txOne networks | Keep the Operation Running

**2.2** TXOne StellarOne
Administrator's Guide

Unify your cyber security posture with one centralized console

SC 2022 awards EUROPE
WINNER

# Privacy and Personal Data Collection Disclosure

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

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

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

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

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

# Table of Contents

## Chapter 5: Policy Management

## Chapter 6: Logs

## Chapter 7: Administration

## Chapter 8: Technical Support

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.

v

# Preface

## Preface

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

Topics in this chapter include:

# 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:<br><br>https://kb.txone.com/<br><br>http://success.trendmicro.com |

# Audience

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

# Document Conventions

The documentation uses the following conventions.

**TABLE 1. Document Conventions**

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

# 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 StellarProtect™: an OT/ICS-compatible, high performance and zero touch endpoint protection solution, and StellarProtect (Legacy Mode)™: a simple, no-maintenance solution to lock down and protect fixed-function computers, helping protect businesses against security threats and increase productivity.

Topics in this chapter include:

# About TXOne Stellar

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

- StellarOne™ , the centralized management console designed to streamline administration of both StellarProtect for modernized systems and StellarProtect (Legacy Mode) for legacy systems.

- StellarProtect™, the unified agent with industrial-grade next-generation antivirus and application lockdown endpoint security deployment for modernized OT/ICS endpoints.

- StellarProtect (Legacy Mode)™, for trust-list based application lockdown of legacy and fixed-use OT/ICS endpoints with anti-malware or on-demand AV scan.

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

# Key Features and Benefits

The TXOne 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 | StellarOne allows administrators to perform the following tasks:<br><br>• Monitor StellarProtect/StellarProtect (Legacy Mode) agent status<br><br>• Examine connection status<br><br>• View configurations<br><br>• Collect agent logs on-demand or by policy (Legacy Mode only)<br><br>• Turn agent Application Lockdown on or off<br><br>• Enable or disable agent Device Control<br><br>• Configure agent Maintenance Mode settings<br><br>• Update agent components<br><br>• Initialize the Approved List<br><br>• Deploy agent patches<br><br>• Add trusted files and USB devices<br><br>• Export agents' information<br><br>• Import/Export agents' configuration settings or Approved List (Legacy Mode only) |
| 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. StellarOne provides event management features that let administrators quickly know about and take action on the 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™ 2.2 provides following new features and enhancements.

**TABLE 1-2. What's New in TXOne StellarOne™ 2.2**

| FEATURE | BENEFIT |
|---|---|
| Enhanced dashboard | Adds one type of blocked events, Malware Scan, to be displayed in the Blocked Event History widget on the dashboard. |
| Adding Lockdown features for StellarProtect | You can now remotely configure the sub-features and trusted hash values settings of Application Lockdown for StellarProtect agents. |
| Agent's User password management | In addition to existing Agent's Administrator password, you can also manage Agent's User password remotely from StellarOne web console. |
| New update command button for StellarProtect - Check Connections | This new button for StellarProtect allows you to check connections between the selected endpoints and StellarOne. |
| New update command button - Apply Policies | This new button allows you to apply policies immediately to the selected endpoints. |
| Policy refresh interval | You can now set how often you want StellarOne to apply policies to the managed endpoints. |
| Performance settings for Scheduled Scan and Scan Now | These settings allow you to select the appropriate mode of CPU usage to balance between the scan and the available CPU resources under different circumstances. |
| Time sync with NTP | In addition to manually modifying StellarOne system time, the option to configure StellarOne for automatically synchronizing system time with an NTP server is available now. |
| Enhanced email security | Provides protocol command options such as STARTTLS and SMTPS to secure transmissions of email notifications of warning or outbreak events. |
| Enhanced CLI command | Add a new vShell command for configuring StellarOne FQDN setting to allow communication with agents or SSO (Single Sign-On) login |

# Chapter 2

## Getting Started

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

Topics in this chapter include:

- *About the Web Console on page 2-2*

- *Opening StellarOne Management Console on page 2-2*

# About the Web Console

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

> **Note**
>
> Supported browsers:
>
> - Google Chrome 87 or later versions
> - Microsoft Edge 79 or later versions
> - Mozilla Firefox 78 or later versions

For users who log on StellarOne for the first time, please refer to *Opening StellarOne Management Console on page 2-2*.

For more details about the installation for StellarOne, please refer to the StellarOne Installation Guide.

# Opening StellarOne Management Console

**Procedure**

1. In a web browser, type the address of the StellarOne in the following format: `https://<targetserver IP address>`. The log on screen appears.

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

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

   - User ID: `admin`

- Password: `txone`

3. Click **Log On**.

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

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

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

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

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

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

   d. Choose one of the ways to activate the license based on the license data available from your support provider:

      - **License Key**

        i. Click **License Key**.

        ii. Specify your license key in the text field.

      - **License File**:

        i. Click **License File**.

        ii. Select the license file (a `.txt` file) to import.

        ---

        📝 **Note**

        If you don't have the license file on hand, refer to *Getting the License File on page 7-30*.

        ---

   e. Click **Apply**.

f.   The **License key is valid** message appears. Click **Continue**.
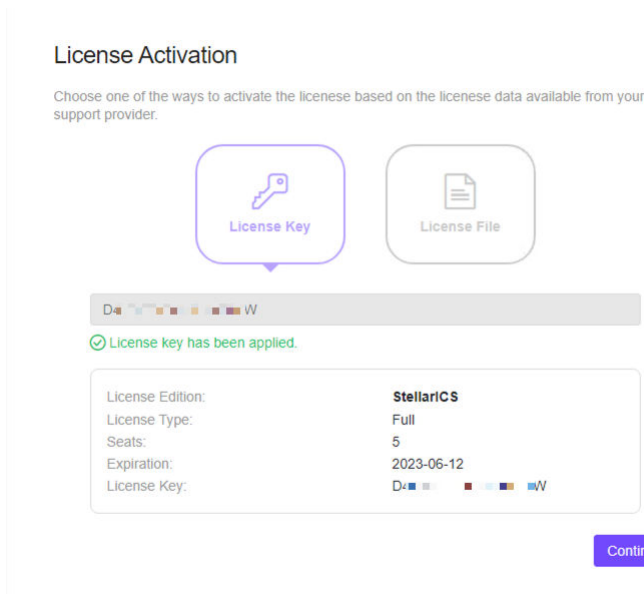


g.   A success message appears. License information also appears at the bottom of the **License Activation** window. Check if it matches the license data provided by your support provider.

h.   Click **Continue**.

i.   The **End User License Agreement and TXOne OT Intelligent Trust** window appears. Click the links to read the documents carefully and click the checkboxes to proceed to next step.

> **Note**
>
> It is advisory to enable **TXOne OT Intelligent Trust** to enhance security deployment. Please refer to *OT Intelligent Trust on page 7-39* for more details.

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

k. The StellarOne console is ready for use now.

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

5. (Optional) You can change your password by clicking the ID icon at the top right corner of the screen, and then selecting **Change Password**.

6. (Optional) For security reasons, you can manually log off by clicking the ID icon at the top right corner of the screen.

   a. A pop-up **Log Off** window appears. Click **Yes** to log out of StellarOne.

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

# Chapter 3

## Dashboard

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

Topics in this chapter include:

# About the Dashboard Screen

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.
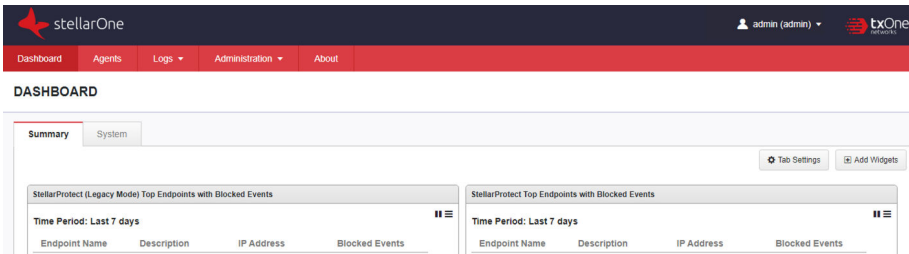


**FIGURE 3-1. The Dashboard Screen**

**TABLE 3-1. About the Dashboard Screen**

| FUNCTION | DESCRIPTION |
|---|---|
| **Summary** | Under this tab, two widgets for monitoring StellarProtect and three for StellarProtect (Legacy Mode) agent events can be added:<br><br>• **Blocked Event History** (Legacy Mode only)<br><br>• **Top Endpoints with Blocked Events**<br><br>• **Top Blocked Files**<br><br>Please refer to *Widgets for Monitoring Agents on page 3-3* and *Add Widgets on page 3-6* for more details.<br><br>---<br><br>📝 **Note**<br>By default the **Summary** tab page is set as the landing page of the **Dashboard**. |

| Function | Description |
|---|---|
| **System** | Under this tab, you can check StellarOne console's system status related to: <br><br> • CPU Usage <br><br> • Memory Usage <br><br> • Disk Usage |
| **Tab Settings** | This button allows you to customize your own tab names. By simply clicking this button, specifying the desired tab name in the **Tab Name** field, and clicking **OK**, you can easily change the tab name. |
| **Add Widgets** | This button allows you to add desired widgets to the **Dashboard** screen. Please refer to *Add Widgets on page 3-6* for more details. |

## Widgets for Monitoring Agents

Two widgets for monitoring StellarProtect and three for StellarProtect (Legacy Mode) agent events can be added under the **Summary** tab of the **Dashboard** screen.

- **Blocked Event History** (Legacy Mode only): This widget displays a summary of blocked events for the specified time period. By default, the widget is displayed on the **Summary** tab page of the **Dashboard**.
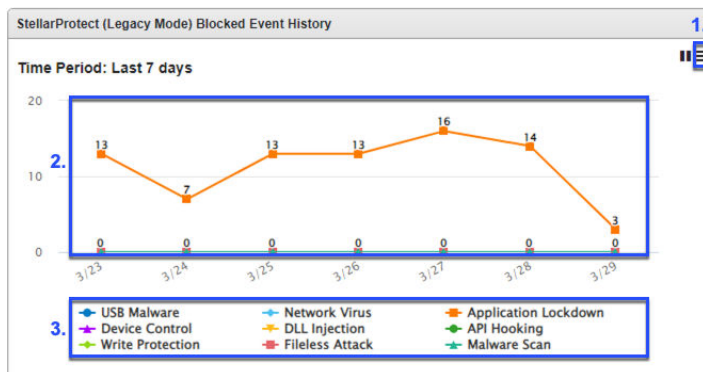
1. Select from the **Time Period** drop-down menu at the top right corner of this widget to display the events occuring within a specified period. Refer to the *Tips* below this section for more details.

2. Click a value on the chart to be directed to the **Agents Events** logs for more details about the blocked event.

3. Click an entry on the legend to show or hide data for that event type.

- **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 page of the **Dashboard**.



1. Select from the **Time Period** drop-down menu at the top right corner of this widget to display the events occuring within a specified period. Refer to the *Tips* below this section for more details.

2. Click an endpoint name to be directed to the **General Info** page for more details about the endpoint.

3. Click a value on the chart to be directed to the **Agents Events** logs for more details about the blocked event.

**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 triggered by the file |
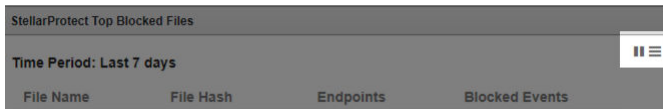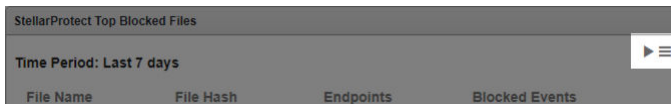
> **Tip**
>
> | StellarProtect Top Blocked Files | | | ► ≡ |
> | --- | --- | --- | --- |
> | Time Period: Last 7 days | | | |
> | File Name | File Hash | Endpoints | Blocked Events |
>
> | StellarProtect Top Blocked Files | | | II ≡ |
> | --- | --- | --- | --- |
> | Time Period: Last 7 days | | | |
> | File Name | File Hash | Endpoints | Blocked Events |
>
> - Click the play button to start auto refresh. Click the pause button to pause auto refresh.
> - The drop-down button provides two functions:
>   - **Widget Settings**:
>     - **Widget Name**: allows you to edit the name for the widget.
>     - **Time Period**: allows you 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 you to change the setting to manual refresh or to configure the auto refresh frequency (The default value is **Every 5 minutes**).
>   - **Remove Widget**: allows you 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 you 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, you 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

## Agents

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

Topics in this chapter include:

# About the Agents Screen

The StellarOne console facilitates agent management by allowing you to organize agents into various groups and build up multi-level hierarchy among the groups (parent groups above child groups), forming an agent/group tree structure.

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

---

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

---
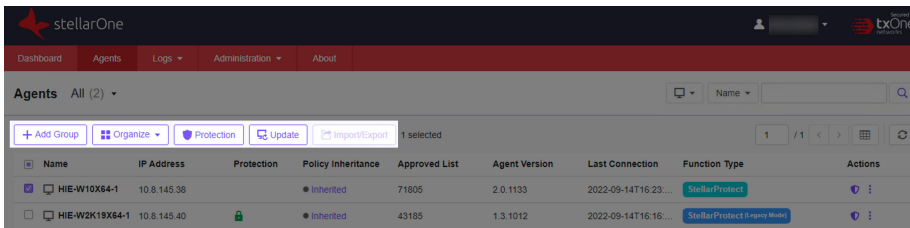


**FIGURE 4-1. The Agents Screen - Toolbar**

**TABLE 4-1. Toolbar**

| TOOLS | DESCRIPTION |
|---|---|
| **+Add Group** | This tool allows you to create groups according to location, type, or purpose for better multi-agent management. See *Add Groups on page 4-6* for more details. |
| **Organize** | This tool allows you to edit description for agent(s), move agent(s) to another group, and remove agent(s)/group(s). See *Edit Description for Agents on page 4-6* and *Organize Agents/Groups on page 4-7* for more details. |

| Tools | Description |
|---|---|
| **Protection** | This tool allows you to configure Maintenance Mode, update Approved List when the Application Lockdown feature is enabled, and customize file scan settings. See *Configure Maintenance Mode on page 4-11*, *Update Approved List on page 4-14*, and *Scan Now on page 4-16* for more details. |
| **Update** | This tool allows you to update components and deploy patches for agents, as well as check connections with endpoints, apply group/agent policies immediately, and collect event logs (Legacy Mode only). See *Update Agent Components on page 4-19*, *Deploy Agent Patches on page 4-20*, *Check Connections on page 4-21*, *Apply Policies on page 4-22*, and *Collect Event Logs on page 4-23* for more details. |
| **Import/Export** | This tool allows you to export an agent config file (Legacy Mode only) or Approved List (Legacy Mode only), and then import it to apply the settings specified in the config file or Approved List to a batch of target agents/groups. You can also export information about the selected or all agents. See *Agent Export/Import Settings on page 4-25* for more details. |



**FIGURE 4-2. The Agents Screen - Column Headings**

**TABLE 4-2. Column Headings**

| Headings | Description |
|---|---|
| **Name** | • 🖥 : Indicates an agent<br><br>• 📁 : Indicates a group |
| **IP Address** | Indicates the IP Address of the endpoint (one IP address corresponds to a single agent) |

| Headings | Description |
|---|---|
| **Protection** | • 🔒 : Indicates the Application Lockdown is enabled<br><br>• 🛡️ : Indicates the agent protection feature is enabled<br><br>• 🔧 : Indicates the agent is in maintenance mode<br><br>• 🔧: Indicates a maintenance period has been scheduled but not started yet<br><br>• ❌ : Indicates the agent protection feature is disabled and the endpoint may be vulnerable to security threats |
| **Policy Inheritance** | • **Inherited**: Indicates the policy settings for the agent/group are inherited from its parent group<br><br>• **Customized**: Indicates the policy settings for the agent/group are customized by administrators<br><br>• **Self-managed**: Indicates the agent/group is free from the StellarOne web console's policy management and its feature settings should be configured on the local console<br><br>• ●: Indicates the agent's feature settings synchronize with the StellarOne console policy settings<br><br>• ●: Indicates the agent's feature settings do not synchronize with the StellarOne console policy settings<br><br>• ⚙?: Indicates the agent/group is free from the StellarOne web console's policy management and its feature settings should be configured on the local console |
| **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 |

| HEADINGS | DESCRIPTION |
|---|---|
| **Function Type** | Indicates two function types of StellarProtect: <br><br> • StellarProtect: for devices with Windows 7 or later versions <br><br> • StellarProtect (Legacy Mode): for devices with legacy platforms such as Windows XP/2000 |
| **Actions** | Under this heading, you can: <br><br> • click ● , the **Policy** icon, for linking to the **General Info** policy page. <br><br> • click the three dots **More actions** menu, for organizing agents and renaming/removing groups. See *Edit Description for Agents on page 4-6* and *Organize Agents/Groups on page 4-7* for more details. |
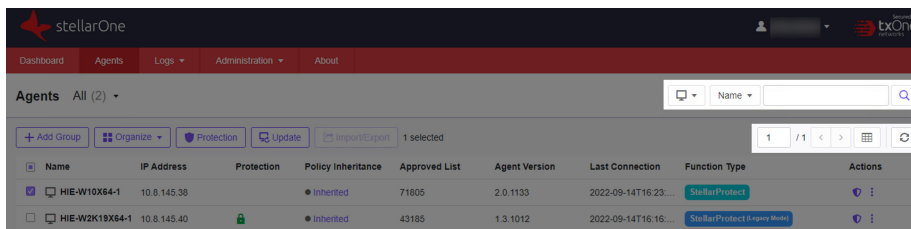


**FIGURE 4-3. The Agents Screen - Other Tools**

**TABLE 4-3. Other Tools**

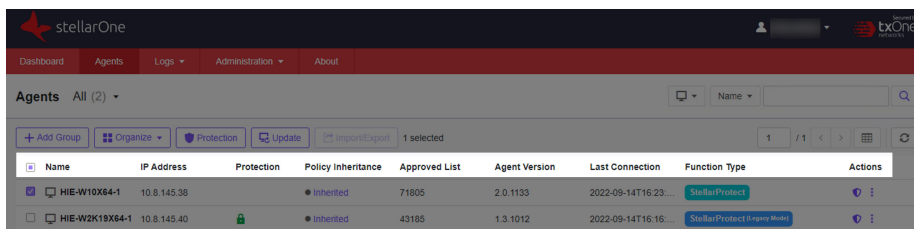| TOOLS | DESCRIPTION |
|---|---|
| **Filter** | [🖵 ▾] [Name ▾] [_____] [🔍] : This tool allows you to quickly find the agents/groups by sorting and searching. See *Filter Options for Agents/Groups on page 4-9* for more details. |

| Tools | Description |
|---|---|
| **Table Display Settings** | `1` `/1` `<` `>` `▦`  `↻` : This tool allows you to customize the table display settings by:<br><br>• going back and forth between the display pages<br><br>• selecting how many agents/groups to be displayed per page and specifying only certain contents to be displayed in the **Customize Table Display** setting<br><br>• 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 main screen of the local agent, follow below procedures.

**Procedure**

1.  Go to **Agents** in the top navigation bar of the StellarOne web console.

2.  Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.

3.  There are two ways to edit descriptions for agent(s):

    •   To edit description for multiple agents at the same time, click the checkboxes next to the target agents. Click the **Organize** tool on the toolbar.

    •   To edit description for a single agent, find the target agent and click its three dots **More actions** menu under the **Actions** header.

4.  A drop-down menu appears. Click **Edit Description** and then a window appears.

5.  Specify the description for the agent(s) in the text field.

6.  Click **Confirm** to complete this task.

## Organize Agents/Groups

You can organizing agents/groups by:

•   renaming groups

•   removing groups

•   removing agents from groups

•   moving agents to another group

**Procedure**

1.  Go to **Agents** in the top navigation bar of the StellarOne web console.

2.  Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.

3. To rename a group, click the three dots **More actions** menu of the target group under the **Actions** header. A drop-down menu appears. Select **Rename** and then a pop-up window appears. Delete the old group name and replace it with a new one. Click **Confirm** to complete this task.

---

📝 **Note**

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

---

4. There are two ways to remove groups or agents:

   • To remove multiple agents or groups at the same time, click the checkboxes next to the target agents or groups. Click the **Organize** tool on the toolbar and select **Remove**. Click **Confirm** to remove the agents/groups.

   ---

   ⚠ **Important**

      • To remove agent(s): The agent(s) will be unregistered from the server.

      • To remove group(s): The group(s) and the configuration of the group(s) will be removed.

   ---

   • To remove a single agent or group, click the three dots **More actions** menu of the target agent/group under the **Actions** header. A drop-down menu appears. Select **Remove** to remove the agent/group.

   ---

   ⚠ **Important**

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

   ---

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

   • To move multiple agents to another group at the same time, click the checkboxes next to the target agents. Click the **Organize** tool on the toolbar.

   • To move a single agent to another group, click the three dots **More actions** menu of the target agent under the **Actions** header.

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

## Search for Agents/Groups

**Procedure**

1.  Go to **Agents** in the top navigation bar of the StellarOne web console.

2.  At the top-right corner of the screen, search for specific endpoints by selecting criteria from the drop-down list and specify additional search criteria as required.

### Filter Options for Agents/Groups
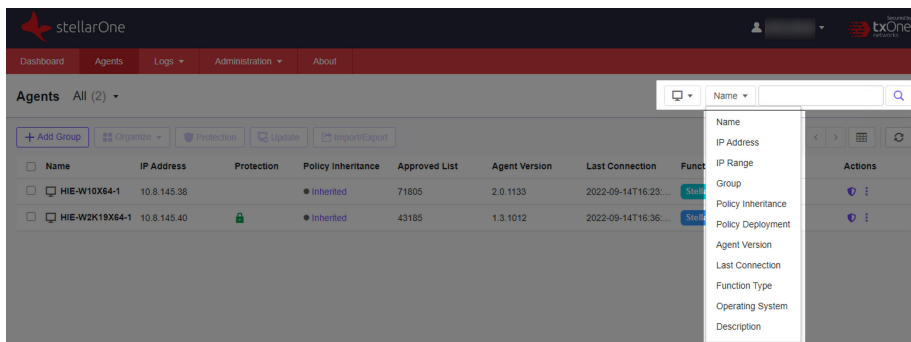


**FIGURE 4-4. Filter Options for Agents/Groups**

**TABLE 4-4. Filter Options for Agents/Groups**

| OPTIONS | DESCRIPTIONS |
|---------|--------------|
| 🖵 ▾ | This icon provides three filter options:<br><br>• Active Agents: the agents with license seats<br><br>• Inactive Agents: the agents without license seats<br><br>• Ungrouped Agents: the agents that are not grouped. |
| Name | The name of the agent. Type the full or partial endpoint host name to locate the specific agent. |
| IP Address | Type the IPv4 address. |
| IP Range | Type the IPv4 address range. |
| Group | The name of the group. Please ensure that you select the available group. |
| Policy Inheritance | Three options -- **Customized**, **Inherited**, and **Self-managed**, are available for selection. |
| Policy Deployment | The status of policy deployment from StellarOne to Agents. Select **Completed** or **In Progress**. |
| Agent Version | Type the build version of the target agents. |
| Last Connection | The last time the agents were connected with StellarOne. Select the default time period or select **Custom range** to specify a time period. Default time period available for selection includes:<br><br>• Last 1 hour<br><br>• Last 24 hours<br><br>• Last 7 days<br><br>• 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. |

# Protection

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

Topics in this chapter include:

## Configure Maintenance Mode

To perform file updates on endpoints, you can configure Maintenance Mode to define a period when the agents allow all file executions and add all files that are created, executed, or modified to the Approved List. Besides, the agents can ensure the execution of these applications are under the protected conditions by performing malware scanning before adding new or changed files to the Approved List. You can also define the action to take after suspicious files are detected.

---

> ⚠️ **Important**
>
> Before using Maintenance Mode, apply the required updates on the following supported platforms for StellarProtect (Legacy Mode) agents:
>
> - For Windows 2000 Service Pack 4, apply the update KB891861 from the Microsoft Update Catalog website.
>
> - For Windows XP SP1, upgrade to Windows XP SP2.

---

---

> ✎ **Note**
>
> - If you change the policy settings of Application Lockdown, OT Application Safeguard, Real-Time Malware Scan, or Anti-malware Scanning during maintenance period, the policy settings will not be implemented until the maintenance period is ended.
>
> - During the maintenance period, you cannot perform agent patch updates on endpoints. In addition, the StellarProtect (Legacy Mode) agent does not support Windows updates that require restarting an endpoint during the maintenance period.
>
> - To run an installer that deploys files to a network folder during the maintenance period, StellarProtect (Legacy Mode) must have access permission to the network.

---

**Procedure**

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

2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.

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

4. Click the **Protection** button from the Tool Bar at the top of the **Agents** screen.

5. A pop-up window appears. Click the **Configure Maintenace Mode** option.

6. Click **Confirm**.

7. The configuration window appears. Please read the notice carefully before you check the **Disable** or **Enable** radio button.

   - Click **Disable** > **OK** to end Maintenance Mode. This will cancel the scheduled maintenance period on endpoints.

      a. A warning message appears. Please read carefully before proceeding to next step.

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

b. Click **OK** to end Maintenance Mode. A pop-up window appears showing the deployment status of stopping Maintenance Mode on endpoints.

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

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

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

> **Note**
>
> • Agents can start one scheduled maintenance period at a time. If you configure a new maintenance period, the system overwrites the existing maintenance schedule that has not started yet.
>
> • When the agent is about to leave Maintenance Mode, restarting the endpoint prevents StellarProtect (Legacy Mode) from adding files in the queue to the Approved List.

• Click the **Schedule** radio button, and then click the edit icon to select the start date and specify the start time for Maintenance Mode. After that, specify the duration of the maintenance period in **Maintenance Mode will be ended after**.

• Click the **Start now** radio button, and then specify the duration of the maintenance period in **Maintenance Mode will be ended after**.

9. A **Scan** toggle switch is added at the bottom and is set **enabled** by default.

> **Note**
>
> - If you disable scan feature in the policy settings, TXOne Networks suggests you enable the scan function here to ensure all the new or changed files go through the malware scanning before they're added to the Approved List. After the maintenance, the original policy settings (in which the scan feature is disabled) will still apply.
>
> - The scan toggle should not appear on the StellarOne console with StellarOEM license edition. See *License Editions on page 7-33* for more details.

10. Select one of the actions to take if suspicious files are detected during scanning:

    - **Quarantine detected files**

    - **Add detected files to Approved List**

11. Click **OK** to deploy the settings to the selected agents or groups.

12. The **Command Deployment** window appears showing the deployment status. Click the **Close** button to close the window.

> **Note**
>
> On the **Agents** screen, in the **Protection** column of the selected agents/groups:
>
> - The 🔧 will appear indicating a maintenance period has been scheduled but not started yet if you select **Schedule** in *Step 8* and deploy related settings.
>
> - The 🔧 icon will appear indicating the agents/groups are currently in maintenance mode if you select **Start now** in *Step 8* and deploy related settings.

## Update Approved List

This function allows you to update the Approved List on selected agents/groups by several simple clicks. Updating the Approved List performs an

inventory scan on selected endpoints and adds any new applications found on the endpoints to the global Approved List. The Approved List must be periodically updated so the newly-added applications can run on the endpoints when the Application Lockdown feature is turned on.

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

**Procedure**

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

2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.

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

4. Click the **Protection** button from the Tool Bar at the top of the **Agents** screen.

5. A pop-up window appears. Click the **Update Approved List** option.

6. Click **Confirm**.

7. A pop-up **Update Approved List** window appears. Click **OK** to start the Approved List update process.

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

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

## Scan Now

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

**Procedure**

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

2.  Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.

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

4.  Click the **Protection** button from the Tool Bar at the top of the **Agents** screen.

5.  A pop-up window appears. Click the **Scan Now** option.

6.  Click **Confirm**.

7.  The configuration window appears.

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

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

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

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

- (Optional and StellarProtect (Legacy Mode) only) Check **Scan removable drives** to allow scanning files in removable drives

- (Optional) Check **Scan compressed files** and select the **Maximum layers** between 1 and 20 for the compressed files.

- (Optional) To skip files over a certain size, check **Skip files larger than** and specify the file size between 1 and 2048 MB. Files exceeding the specified file size will not be scanned.

- (Optional and StellarProtect only) Check **Aggressive scan (include all OT applications and CA files)** to allow scanning files in existing trusted list.

b. The **CPU Usage** settings allow you to select the appropriate mode of CPU usage to balance between the scan and the available CPU resources depednding on situations. There are two options available:

- Click **Normal** to reduce the impact on the service performance, which allows you to perform other tasks while scanning but the scan may take longer to complete.

- Click **High** to reduce scan time, which requires higher CPU usage and may affect the system performance.

c. In the **Scan Action** section, you can pre-define the action to take after threats are detected. Select **Quarantine** to place the suspicious or infected files detected in an isolated folder for further checking. Select **No action** to produce only a readout of results with no actions taken on the suspicious files.

> **Note**
>
> The StellarProtect (Legacy Mode) agents provide more choices such as:
>
> - **Use ActiveAction**: The pre-configured scan actions, which are best to use if you are not familiar with scan actions or if you are not sure which scan action is suitable.
>
> - **Clean, or delete if the clean action is unsuccessful**: To delete the target file if it cannot be recovered.
>
> - **Clean, or quarantine if the clean action is unsuccessful**: To quarantine the target file if it cannot be recovered.
>
> - **Clean, or ignore if the clean action is unsuccessful**: To ignore the target file if it cannot be recovered.

d. (Optional) The **Scan Exclusions** section allows you to exclude certain folders, files, or file extensions from being scanned.

- **Folders**: specify a path to the folders that do not require scanning.

- **Files**: specify a path to the files that do not require scanning.

- **File Extensions**: specify the file extension of certain files that do not require scanning.

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

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

9.  Click **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.

# Update

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

Topics in this section include:

- *Update Agent Components on page 4-19*

- *Deploy Agent Patches on page 4-20*

- *Check Connections on page 4-21*

- *Apply Policies on page 4-22*

- *Collect Event Logs on page 4-23*

> 📝 **Note**
>
> Only StellarProtect (Legacy Mode) supports the Collect Event Logs feature.

## Update Agent Components

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

**Procedure**

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

2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.

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

4. Click the **Update** button from the Tool Bar at the top of the **Agents** screen.

5. A pop-up window appears. Click **Update Agent Components** option.

6. Click **Confirm**.

7. The **Update Agent Components** window appears. Click **OK** to start the update.

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

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

## Deploy Agent Patches

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

**Procedure**

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

2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.

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

4. Click the **Update** button from the Tool Bar at the top of the **Agents** screen.

5. A pop-up window appears. Click the **Deploy Agent Patches** option.

6. Click **Confirm**.

7. A pop-up **Deploy Agent Patches** window with the patch list appears. Select the version of the patch for deployment and click the checkbox next to it.
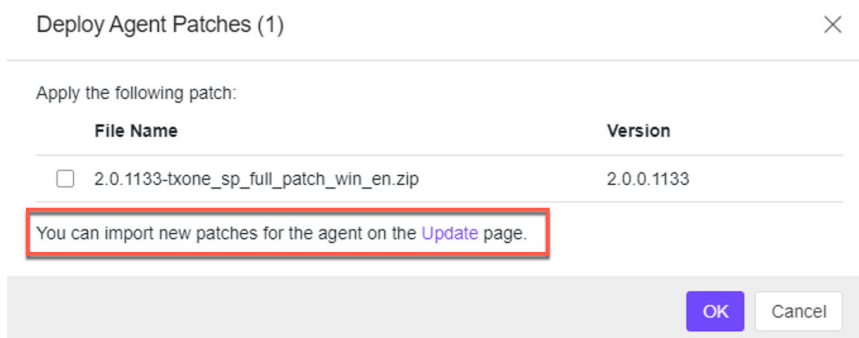


**FIGURE 4-5. Select the Patch Version**

> 📝 **Note**
>
> By clicking the **Update** link, you will be directed to the *Downloads/Updates on page 7-20* page for importing new patches for agents.

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

## Check Connections

You can check the connection status of the selected agents.

**Procedure**

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

2.   Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.

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

4.   Click the **Update** button from the Tool Bar at the top of the **Agents** screen.

5.   A pop-up window appears. Click the **Check Connections** option.

6.   Click **Confirm**.

7.   A pop-up **Command Deployment** window with the endpoint list appears. The **Status** column shows if the agents are succesfully connected to the StellarOne server.

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

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

## Apply Policies

You can manually apply policy updates to the selected endpoints.

**Procedure**

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

2.   Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.

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

4. Click the **Update** button from the Tool Bar at the top of the **Agents** screen.

5. A pop-up window appears. Click the **Apply Policies** option.

6. Click **Confirm**.

7. A pop-up **Command Deployment** window with the endpoint list appears. The **Status** column shows if the StellarOne policies are succesfully applied to the target agents.

---

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

---

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

## Collect Event Logs

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

---

> **Note**
>
> Only StellarProtect (Legacy Mode) supports this function.

---

**Procedure**

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

2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.

3. Select the target agents by clicking the checkboxes next to them.

4. Click the **Update** button from the Tool Bar at the top of the **Agents** screen.

5. A pop-up window appears. Click the **Collect Event Logs** option.

6. Click **Confirm**.

7. A pop-up **Command Deployment** window with the endpoint list appears. The **Status** column shows if the event logs are successfully collected.

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

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

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

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

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

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

- On the StellarOne console, export the agent's configuration file and change the value of `InformationLog Enable` to `yes`. Import the modified configuration file to the selected agent. Refer to *Export Agent Configurations on page 4-26* and *Import Agent Configurations on page 4-28* for more detailed instructions.

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

**FIGURE 4-6. Snippet of the Configuration File**

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

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

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

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

## Agent Export/Import Settings

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

Topics in this section include:

- *Export Agent Settings on page 4-26*

- *Import Agent Settings on page 4-27*

- *Export Selected Agents Info on page 4-30*

- *Export all Agents Info on page 4-31*

---

📝 **Note**

Only StellarProtect (Legacy Mode) supports Export/Import Agent Settings, which are only for agent level. When you select any group from the list, the function should be disabled.

---

## Export Agent Settings

You can remotely obtain the StellarProtect (Legacy Mode) Agent Configuration settings and Approved List by exporting and downloading them from the StellarOne console.

---

📝 **Note**

Only StellarProtect (Legacy Mode) supports this functions.

---

## Export Agent Configurations

---

**Procedure**

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

2.  Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.

3.  Select the target agent by clicking the checkbox next to it.

4.  Click the **Import/Export** button from the Tool Bar at the top of the **Agents** screen.

5. Click the **Export Agent Configurations** option.

6. Click **Confirm**.

7. A pop-up **Command Deployment** window appears. The **Status** shows if the agent configuration is exported successfully.

8. Click the **Download** link to download the target agent's configuration file.

**Export Approved List**

**Procedure**

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

2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.

3. Select the target agent by clicking the checkbox next to it.

4. Click the **Import/Export** button from the Tool Bar at the top of the **Agents** screen.

5. Click the **Export Approved List** option.

6. Click **Confirm**.

7. A pop-up **Command Deployment** window appears. The **Status** shows if the agent's approved list is exported successfully.

8. Click the **Download** link to download the target agent's approved list.

## Import Agent Settings

You can remotely obtain the StellarProtect (Legacy Mode) Agent Configuration settings and Approved List by exporting and downloading them from the StellarOne console.

> **Note**
>
> Only StellarProtect (Legacy Mode) supports this functions.

## Import Agent Configurations

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

- Remotely overwrite agent configuration

- Remotely overwrite Approved List

Remember to prepare a customized agent configuration file or Approved List first:

- Export and download an agent configuration file or Approved List.

- Customize the downloaded file

> **Note**
>
> To ensure a successful import, verify that the file to import meets the following requirements:
>
> - For Approved List, file is in the CSV format and uses UTF-8 encoding
>
> - The maximum file size supported is **20 MB**
>
> - For Agent Configuration file, file is in the XML format and the maximum file size supported is **1 MB**

**Procedure**

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

2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.

3. Select the target agents by clicking the checkboxes next to them.

4. Click the **Import/Export** button from the Tool Bar at the top of the **Agents** screen.

5.  Click the **Import Agent Configurations** option.

6.  Click **Confirm**.

7.  A pop-up **Import Agent Configurations** window appears. Click **Select File**.

8.  Select the file to import and click **OK**.

9.  A pop-up **Command Deployment** window appears. The **Status** shows if the agent configurations are imported to the target endpoints successfully.

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

## Import Approved List

**Procedure**

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

2.  Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.

3.  Select the target agents by clicking the checkboxes next to them.

4.  Click the **Import/Export** button from the Tool Bar at the top of the **Agents** screen.

5.  Click the **Import Approved List** option.

6.  Click **Confirm**.

7.  A pop-up **Import Approved List** window appears. Click **Select File**.

8.  Select the file to import and click **OK**.

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

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

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

## Export Selected Agents Info

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

**Procedure**

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

2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.

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

4. Click the **Import/Export** button from the Tool Bar at the top of the **Agents** screen.

5. A pop-up window appears. Click the **Export Selected Agents Info** option.

6. Click **Confirm**.

7. A `.csv` file is downloaded.

## Export all Agents Info

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

**Procedure**

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

2.  Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.

3.  Click the **Import/Export** button from the Tool Bar at the top of the **Agents** screen.

4.  A pop-up window appears. Click the **Export all Agents Info** option.

5.  Click **Confirm**.

6.  A `.csv` file is downloaded.

# Chapter 5

## Policy Management

Unlike the configurations available on the **Agents** screen (which are one-time commands for triggering immediate actions), the policy management on the **Policy** page are for pattern deployment to the agents.

After you organize agents into various groups and build up multi-level hierarchy among the groups (parent groups above child groups), two types of policy management are available for choice:

- Policy **Inherited**: The group policy is inherited from the parent group

- Policy **Customized**: The group policy is customized for specific agents/groups by the StellarOne administrators

---

📝 **Note**

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

---

Topics in this chapter include:

# About the Policy Screen

Topics in this chapter include:

- *Go to the Policy Screen on page 5-2*

- *Options Available on the Policy Screen on page 5-3*

## Go to the Policy Screen
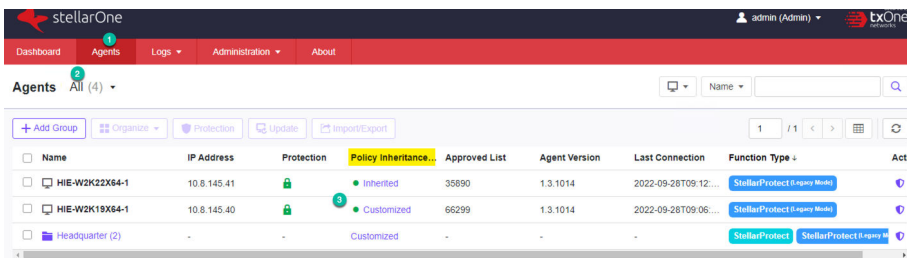


**Procedure**

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

2.  Click the **All** group, and then a screen displays the second level of groups/agents managed by StellarOne.

3.  Navigate to the target agent or group. Go to the Policy page by either way listed below.

    - Click the link (**Inherited**, **Customized**, or **Self-managed**) in the **Policy Inheritance** column.

    - Click the Policy icon in the **Actions** column, and then click the **Policy** tab.

    The **Policy** screen appears.

> **Note**
>
> You can also click the corresponding **Policy Inheritance** link of the **All** group to check its policy settings.

## Options Available on the Policy Screen
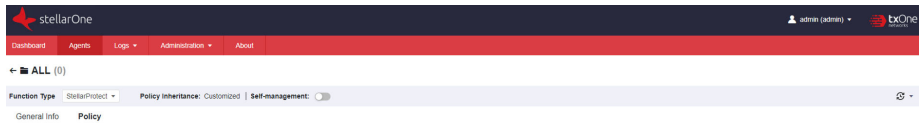


**FIGURE 5-1. Switch Options of the Policy Screen**

| Options | Description |
|---|---|
| **Function Type** | The dropdown button next to the **Function Type** allows you to switch between **StellarProtect** and **StellarProtect (Legacy Mode)**. |
| **Policy Inheritance** | The toggle button allows you to enable or disable the group policy inheritance from the parent group. If the toggle is on, policy settings for the agent/group are inherited from the parent group; otherwise, policy settings for the agent/group are customized by the server administrators. <br><br> > **Note** <br> > <br> > When the toggle is on or off, the **Inherited** or **Customized** status will be displayed in the **Policy Inheritance** column on the **Agents** screen. |
| **Self-management** | The toggle button allows you to enable or disable the agent's self-managementl. When the toggle is on, the agent will be set free from StellarOne console's policy management and the on-site operators can configure the agent's policy settings on their own. |
| **General Info**/**Policy** | The tabs allow you to switch between the displays of General Information or Policy settings. |

| Options | Description |
|---|---|
| <br><br>Set policy refresh interval | This button allows you to specify how often the StellarOne policy is applied to the agent/group. See *Set Policy Refresh Interval on page 5-4* for more details. |

## Set Policy Refresh Interval

You can specify how often the StellarOne policy is applied to the agent/group.

**Procedure**

1. Navigate to the target agent or group, and then go to its **Policy** page. For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

2. Find the refresh icon in the upper-right corner of the screen.

3. Click the refresh icon and the **Set Policy Refresh Interval** window appears

4. Click the **Refresh Interval** menu and select among the given options:

   - **5 Minutes**

   - **10 Minutes**

   - **20 Minutes** (default setting)

   - **60 Minutes**

> **Important**
>
> Frequent refresh might interfere with your work and increase network traffic. See the list below as the recommended policy refresh interval regarding the number of agents managed:

| Policy Refresh Interval | No. of Agents Managed |
|---|---|
| 5 minutes | 5000 |
| 10 minutes | 10000 |
| 20 minutes | 20000 |
| 60 minuties | 60000 |

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

## Policy Settings

On the **Policy** screen, the **Function Type** menu allows you to switch between the policy settings for **StellarProtect** and **StellarProtect (Legacy Mode)**.

Topics in this section include:

- *Policy Settings for StellarProtect on page 5-5*

- *Policy Settings for StellarProtect (Legacy Mode) on page 5-26*

- *Other Policy Settings for StellarProtect/StellarProtect (Legacy Mode) on page 5-47*

## Policy Settings for StellarProtect

Policy settings for StellarProtect agent include:

- *Application Lockdown on page 5-6*

- *Industrial-Grade Next-Generation Antivirus on page 5-13*

- *Operations Behavior Anomaly Detection on page 5-19*

- *OT Application Safeguard on page 5-23*

- *DLL Injection Prevention on page 5-25*

- *Trusted Certificates on page 5-26*

See *Other Policy Settings for StellarProtect/StellarProtect (Legacy Mode) on page 5-47* for how to configure Agent Component Update Schedule, Device Control, User-Defined Suspicious Objects, Agent Password, and Agent Patch deployment for StellarProtect agent.

## Application Lockdown

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

**Procedure**

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

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

   > **Note**
   >
   > For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

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

4. 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, see *Exception Paths Settings on page 5-7*.
>
> - For how to configure trusted hash values settings for the Approved List, see *Trusted Hash Values Settings on page 5-9*.

**5.** If you enable the "Detect" mode or "Enforce" mode, the sub-features listed below will appear. By default, the sub-features are enabled. Click the toggles to disable them if needed.

- **DLL/Driver Lockdown**: Prevents unapproved DLLs or drivers from being loaded into the memory of protected endpoints.

- **Script Lockdown**: Prevents unapproved script files from being run on protected endpoints.

- **Intelligent Runtime Learning**: Allows runtime executable files that are generated by applications in the Approved List.

**Exception Paths Settings**

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 you to configure lockdown exclusion settings for the Approved List.

**Procedure**

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

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

> **✎ Note**
>
> For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

3. Find and click the **Exception Paths** at the bottom of the **Application Lockdown** pane.

- For adding exception paths:

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

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

    > **Note**
    >
    > The **Exception Paths** function supports only the real path and hardlink path.

    c. Click **Add** to complete adding the exception paths for the Approved List.

- For editing existing exception paths:

    a. Find the exception path to be edited and click the corresponding Edit icon under the **Actions** header.

    b. A pop-up window appears. Select among **Folder**, **File**, or **Regular Expression** and edit in the corresponding text field.

    c. Click **Save** to complete editing the exception paths for the Approved List.

- For deleting multiple existing exception paths:

    a. Click the checkboxes next to the existing exception paths.

    b. Click the **Delete** button next to the **+Add** button.

    c. A warning message window appears. Click **Confirm** to delete the selected items.

- For deleting single existing exception path:

    a. Find the exception path to be deleted and click the corresponding Delete icon in the **Actions** column.

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

## Trusted Hash Values Settings

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

### Calculate Hash Values

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

**Procedure**

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

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

    > **Note**
    >
    > For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

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

4.  The **Trusted Hash Values** windows appears. Find and click **File Hash Generator** to download the tool.

5.  Execute WKFileHashGen.exe from the downloaded folder. The **File Hash Generator** screen will appear.

6.  Use any of the following methods to select files and calculate hash values:

    •  Drag and drop folders or files to the **File Hash Generator** screen.

- Click the drop-down button and click **Add Files** to select the files to add.

- Click the drop-down button and click **Add Folder** to add all the files in the selected folder.

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

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

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

> **Note**
>
> - To ensure that all necessary files are calculated for hash values, it is advisable to add the root folder of the target application(s) to the **File Hash Generator** for calculation.
>
> - By clicking the **Add Folder** button, only the installer files, script files, and files in the PE (Portable Executable) format will be calculated.
>
> - For the single hash value, see *Add Trusted Hash Values on page 5-11* for how to add the copied hash value to the trusted hash value list.
>
> - For multiple hash values, see *Import Trusted Hash Values on page 5-11* for how to import the file containing the hash values to the trusted hash value list.

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

**Add Trusted Hash Values**

**Procedure**

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

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

    > 📝 **Note**
    >
    > For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

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

4.  Click the **Add** button and fill in the hash values and notes.

**Import Trusted Hash Values**

**Procedure**

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

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

    > 📝 **Note**
    >
    > For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

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

4.  Click the **Import** button to import the .txt file containing a batch of hash values.

> 📝 **Note**
>
> See *Calculate Hash Values on page 5-40* for generating the file containing the list of multiple hash values

**Edit Trusted Hash Values**

### Procedure

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

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

   > 📝 **Note**
   >
   > For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

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

4. Find the trusted hash value to be edited and click the corresponding Edit icon in the **Actions** column.

5. The **Edit Trusted Hash Value** dialog window appears.

6. After modification, click the **Save** button to complete the settings.

**Remove Trusted Hash Values**

### Procedure

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

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

   > 📝 **Note**
   >
   > For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

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

4.  To delete multiple existing trusted hash values:

    a.  Click the checkboxes next to the existing trusted hash values.

    b.  Click the **Delete** button next to the **Import** button.

    c.  A warning message window appears. Click **Confirm** to delete the selected items.

5.  To delete single existing trusted hash values:

    a.  Find the trusted hash value to be deleted and click the corresponding Delete icon in the **Actions** column.

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

## Industrial-Grade Next-Generation Antivirus

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

### Real-Time 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**, you 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.  Go to **Agents** > **All**.

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

    > 📝 **Note**
    >
    > For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

3.  Go to the **Real-time Malware Scan** section in the **Industrial-Grade Next-Generation Antivirus** pane.

4.  Toggle on the **Real-Time Malware Scan**.

    > 📝 **Note**
    >
    > See *Advanced Settings on page 5-16* for instructions on how to configure the types of the files to be scanned, the action to take after possible security risk is detected, and the scan exclusion list.

**Predictive Machine Learning**

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

helps protect your assets and network environment against unidentified threats and zero-day attacks.

To enable **Predictive Machine Learning**, find and click the check box next to it in the section of **Real-Time Malware Scan** in the **Industrial-Grade Next-Generation Antivirus** pane.

### Scheduled Scan

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

**Procedure**

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

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

> **Note**
>
> For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

3. Go to the **Scheduled Scan** in the **Industrial-Grade Next-Generation Antivirus** pane.

4. Toggle the **Scheduled Scan** on.

5. Click the **Schedule** button. A **Schedule** window appears.

6. Select one of the radio buttons listed below for determining the scan frequency.

   - **Daily**: Perform scanning every day

   - **Weekly**: Perform scanning every week (by default it's set as **every Sunday**)

   - **Monthly**: Perform scanning every month (by default it's set as **on day 01**)

---

**Important**

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

---

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

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

---

**Note**

See *Advanced Settings on page 5-18* for instructions on how to configure the types of the files to be scanned, the action to take after possible security risk is detected, and the scan exclusion list.

---

## Advanced Settings

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

---

**Note**

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

---

### 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 2048 MB. Files exceeding the specified file size will not be scanned.

6. In the **Scan Action** section, you can pre-define the action to take after threats are detected during the scanning. Select **Quarantine** to place the suspicious files detected in an isolated folder for 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 allows you to exclude certain folders, files, or file extensions from being scanned.

   - **Folders**: Specify a path to the folders that do not require scanning.

   - **Files**: Specify a path to the files that do not require scanning.

   - **File Extensions**: Specify the file extension of certain files that do not require scanning.

   ---

   **Note**

   - StellarProtect supports only local paths for Scan Exclusions. Remote paths such as an URL or \\[Hostname] are not supported.

   - It is not required to add "." or "*." in front of the file extension.

   ---

   **Tip**

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

   ---

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

---

**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 four sections: **Files to Scan**, **CPU Usage**, **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 2048 MB. Files exceeding the specified file size will not be scanned.

    b. The **CPU Usage** settings allow you to select the appropriate mode of CPU usage to balance between the scan and the available CPU resources depedning on situations. There are two options available:

       • Click **Normal** to reduce the impact on the service performance, which allows you to perform other tasks while scanning but the scan may take longer to complete.

- Click **High** to reduce scan time, which requires higher CPU usage and may affect the system performance.

c. In the **Scan Action** section, you can pre-define the action to take after threats are detected. Select **Quarantine** to place the suspicious or infected files detected in an isolated folder for further checking. Select **No action** to produce only a readout of results with no actions taken on the suspicious files.

d. (Optional) The **Scan Exclusions** section allows you to exclude certain folders, files, or file extensions from being scanned.

- **Folders**: specify a path to the folders that do not require scanning.

- **Files**: specify a path to the files that do not require scanning.

- **File Extensions**: specify the file extension of certain files that do not require scanning.

---

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

---

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

---

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

---

## Operations Behavior Anomaly Detection

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

Navigate to the target agent or group, and then go to its **Policy** page. For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

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

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

- **Learn**: Under this mode, StellarProtect will monitor unrecognized program calls and add them to the approved operations. In this way, the agent will continuously learn more and more OT-related program call behaviors.

- **Detect**: Under this mode, StellarProtect will 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, there is one more option, the **Aggressive Mode**, which is used for stronger threat protection. See *Aggressive Mode on page 5-20* for more details.

- You can manually add commonly-abused applications used in operations and processes to the **Watchlist** for strengthening security monitoring. See *Watchlist on page 5-22* for more details.

---

### Aggressive Mode

In either **Detect** or **Enforce** mode, there is one more option, the **Aggressive Mode,** which is used for stronger threat protection. This feature helps enhance protection by adding parameter identification into the monitoring task, enabling the examination of the operation process and its accompanied changes in parameters.

> **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.

See below as an example of how the **Aggressive Mode** works.

1.  When you 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 you switch to the **Detect** or **Enforce** mode without enabling 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 `script.ps1 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 the **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 `script.ps1 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

You 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, and 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** pane. Enable **Operations Behavior Anomaly Detection** by selecting **Learn**, **Detect**, or **Enforce**.

    > **Note**
    >
    > The default setting for **Operations Behavior Anomaly Detection** is **Disable**. If you 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 you 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**
    >
    > To delete the added application one by one, click the Delete icon in the **Actions** column; to delete multiple applications, click the checkboxes next to them and then click **Delete** > **Confirm**.

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

## OT Application Safeguard

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

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

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

**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 in the **Actions** column.

4. The **General Info** screen appears. Check the OT Applications automatically recognized by the StellarProtect agent.

> **！ Important**
>
> Be sure to enable the **Maintenance Mode** before installing new OT
> applications. After the installation process completes, disable the
> **Maintenance Mode** and then StellarProtect will auto re-scan the newly-
> added OT applications. Any new applications found will be added into the
> OT Application Safeguard list. See *Configure Maintenance Mode on page 4-11*
> for how to enable this function.

5. You 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 the configuration window appears.

   d. Click the **+Add** button, and then select **Folder** or **File** and specify
      the folder or file path in the corresponding text fields.

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

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

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

   f. Click **Add** to complete the setting.

6. You can also add user-defined processes.

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

b.   The configuration window appears. Click the **+Add** button, and then specify the authorized processes in the corresponding text fields.

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

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

## DLL Injection Prevention

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

> **Note**
>
> Only x86 platform supports DLL injection Prevention.

**Procedure**

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

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

> **Note**
>
> For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

3.   Scroll down and find the **DLL Injection Prevention** at the left side of the screen.

**4.** Toggle on **Block DLL Injection** to enable it.

## Trusted Certificates

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

**Procedure**

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

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

> 📝 **Note**
>
> For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

3. Scroll down and find the **Trusted Certificates** at the right side of the screen.

4. Click **Import** to import the selected trusted certificate file.

5. To remove the trusted certificate(s), choose either way listed below.

   - For removing multiple trusted certificates at the same time, select them and click the **Delete** button next to the **+Add** button.

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

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

## Policy Settings for StellarProtect (Legacy Mode)

Policy settings for StellarProtect (Legacy Mode) agent include:

- *Application Lockdown on page 5-27*

- *Intelligent Runtime Learning on page 5-28*

- *Anti-malware Scanning on page 5-28*

- *Exclusions Settings on page 5-35*

See *Other Policy Settings for StellarProtect/StellarProtect (Legacy Mode) on page 5-47* for how to configure Agent Component Update Schedule, Device Control, User-Defined Suspicious Objects, Agent Password, and Agent Patch deployment for StellarProtect (Legacy Mode) agent.

## Application Lockdown

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

**Procedure**

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

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

   > 📝 **Note**
   >
   > For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

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

   > 📝 **Note**
   >
   > See the *Exclusions Settings on page 5-35* for how to configure the exclusions for the Approved List.

### Intelligent Runtime Learning

When **Intelligent Runtime Learning** is enabled, the agent will allow runtime execution files that are generated by applications in the Approved List.

**Procedure**

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

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

   > **Note**
   >
   > For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

3. Find the **Intelligent Runtime Learning**, and then toggle it on.

## Anti-malware Scanning

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

- *Real-Time Scan on page 5-28*

- *Scheduled Scan on page 5-15*

- *Advanced Settings on page 5-16*

### Real-Time Scan

**Real-time Scan** provides persistent and ongoing file scan for the endpoints. Each time a file is received, opened, downloaded, copied, or modified, **Real-time Scan** always scans the file for security assessment. After performing the **Real-Time Scan**, users can proceed to access the file if it does not pose a security threat. However, if a security risk or possible virus/malware has

been detected during the scanning, a notification message appears indicating the name of the infected file and the specific security risk.

Moreover, a persistent scan cache is maintained and reloaded each time the **Real-Time Scan** is executed. The **Real-Time Scan** tracks any changes made to files or folders that have occurred until the function is disabled and the files are unloaded and removed from the scan cache.

**Procedure**

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

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

   > **Note**
   >
   > For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

3. Find the **Real-Time Scan** in the **Anti-Malware Scanning** pane.

4. Toggle **Real-Time Scan** on to enable the function.

   > **Note**
   >
   > See the *Advanced Settings on page 5-31* for instructions on how to configure the types of the files to be scanned, the action to take after possible security risk is detected, and the scan exclusion list.

## Scheduled Scan

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

**Procedure**

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

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

> **Note**
>
> For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

3. Go to the **Scheduled Scan** in the **Anti-Malware Scanning** pane.

4. Toggle the **Scheduled Scan** on.

5. Click the **Schedule** button. A **Schedule** window appears.

6. Select one of the radio buttons listed below for determining the scan frequency.

   - **Daily**: Perform scanning every day

   - **Weekly**: Perform scanning every week (by default it's set as **every Sunday**)

   - **Monthly**: Perform scanning every month (by default it's set as **on day 01**)

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

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

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

> **Note**
>
> See *Advanced Settings for Scheduled Scan on page 5-32* for instructions on how to configure the types of the files to be scanned, the action to take after possible security risk is detected, and the scan exclusion list.

### Advanced Settings

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

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

### Advanced Settings for Real-Time Scan

**Procedure**

1. Go to **Agents** > **Policy** > **Anti-Malware Scanning**.

2. Click the **Advanced Settings** in the **Real-Time Scan** section.

3. The **Advanced Settings** configuration window appears.

4. The configuration window consists of three sections: **Files to Scan**, **Scan Action**, and **Scan Exclusions**.

5. In the **Files to Scan** section:

    - Check **Scan compressed files** and select the **Maximum layers** between 1 and 20 for the compressed files.

    - To skip scanning files over a certain size, check **Skip files larger than** and specify the file size between 1 and 2048 MB. Files exceeding the specified file size will not be scanned.

6. In the **Scan Action** section, you can pre-define the action to take after threats are detected during the scanning. Select **Quarantine** to place the

suspicious files detected in an isolated folder for 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 allows you to exclude certain folders, files, or file extensions from being scanned.

   - **Folders**: Specify a path to the folders that do not require scanning.

   - **Files**: Specify a path to the files that do not require scanning.

   - **File Extensions**: Specify the file extension of certain files that do not require scanning.

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

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

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

**Advanced Settings for Scheduled Scan**

**Procedure**

1. Go to **Agents** > **Policy** > **Anti-Malware Scanning**.

2. Click the **Advanced Settings** in the **Scheduled Scan** section:

3. The **Advanced Settings** configuration window appears.

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

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

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

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

   - (Optional and StellarProtect (Legacy Mode) only) Check **Scan removable drives** to allow scanning files in removable drives

   - (Optional) Check **Scan compressed files** and select the **Maximum layers** between 1 and 20 for the compressed files.

   - (Optional) To skip files over a certain size, check **Skip files larger than** and specify the file size between 1 and 2048 MB. Files exceeding the specified file size will not be scanned.

b.  The **CPU Usage** settings allow you to select the appropriate mode of CPU usage to balance between the scan and the available CPU resources depedning on situations. There are two options available:

   - Click **Normal** to reduce the impact on the service performance, which allows you to perform other tasks while scanning but the scan may take longer to complete.

   - Click **High** to reduce scan time, which requires higher CPU usage and may affect the system performance.

c.  In the **Scan Action** section, you can pre-define the action to take after threats are detected. Select **Quarantine** to place the suspicious or infected files detected in an isolated folder for further checking.

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

---

📝 **Note**

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

- **Use ActiveAction**: The pre-configured scan actions, which are best to use if you are not familiar with scan actions or if you are not sure which scan action is suitable.

- **Clean, or delete if the clean action is unsuccessful**: To delete the target file if it cannot be recovered.

- **Clean, or quarantine if the clean action is unsuccessful**: To quarantine the target file if it cannot be recovered.

- **Clean, or ignore if the clean action is unsuccessful**: To ignore the target file if it cannot be recovered.

---

d.  (Optional) The **Scan Exclusions** section allows you to exclude certain folders, files, or file extensions from being scanned.

- **Folders**: specify a path to the folders that do not require scanning.

- **Files**: specify a path to the files that do not require scanning.

- **File Extensions**: specify the file extension of certain files that do not require scanning.

---

📝 **Note**

- StellarProtect supports only local paths for **Scan Exclusions**. Remote paths such as an URL or \\[Hostname] are not supported.

- It is not required to add "." or ".*" in front of the file extension.

---

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

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

## Exclusions Settings

The Lockdown Exclusions allows users to define trusted certificates, trusted hash values, exception paths, and write protecion list. The trusted certificates defined by users will be bypassed during scanning and will not be blocked by **Application Lockdown**. Meanwhile, the trusted hash values, exception paths, and write protecion allows users to configure lockdown exclusion settings for the Approved List.

**Procedure**

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

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

> **Note**
>
> For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

3.    Scroll down and go to the **Exclusions** section.

4.    Configure the **Exclusions** by Import/Export Exclusions for **Trusted Certificates** and **Trusted Hash Values**:

5.    Manually add lockdown exclusion lists for **Trusted Hash Values**, **Exception Paths**, and **Write Protection**:

   •    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.

---

### Export/Import Exclusions Settings

Exporting and importing exclusions settings allow you to move StellarProtect (Legacy Mode)'s hash values, trusted certificates, exception paths, and write protection settings from one group to another.

> **Tip**
>
> It is advisory to refer to the sections below for configuring the **Trusted Certificates**, **Trusted Hash Values**, **Exception Paths,** and **Write Protection** settings first, and then export the exclusions configuration file from the agent as an template to modify (if needed) and import it to a batch of target agents/ groups.

### Trusted Certificates Settings

Similar to hash values, trusted certificates are made by the application vendors or organizations to allow StellarProtect (Legacy Mode) to know which applications are trustworthy.

#### Import Trusted Certificates

**Procedure**

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

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

   > **Note**
   >
   > For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

3. Go to the **Exclusions** pane.

4. Find **Trusted Certificates** section and then Click **Import**.

5. The **Import Trusted Certificate** window appears. Click **Select File** to import the target certificate.

6. Enable the **Installer** toggle switch to automatically add all files created or modified by the trusted installer to the Approved List.

> 📝 **Note**
>
> By default, the **Installer** toggle is turned off.

7. Click **Import** to add the trusted certificate and the settings will be saved.

**Delete Trusted Certificates**

**Procedure**

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

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

   > 📝 **Note**
   >
   > For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

3. Go to the **Exclusions** pane.

4. Find **Trusted Certificates** section and select the trusted certificates to be removed.

5. Click the **Delete** button and the **Remove Trusted Certificate** dialog window will appear.

6. Click **Confirm** to remove the selected entries.

**Exception Paths Settings**

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

**Add a File, Folder, or Regular Expression as an Exception Path**

**Procedure**

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

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

    > 📝 **Note**
    >
    > For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

3.  Find the **Exception Paths** section from the **Exclusions** pane.

4.  Click the **Add** button and the **Add Exception Path** dialog window will appear.

5.  Select one of the exception types: **File**, **Folder**, or **Regular Expression**.

6.  Input the file system path for your exception.

7.  Click the **Add** button to add a single exception path and the settings will be saved.

**Edit Exception Path**

**Procedure**

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

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

    > 📝 **Note**
    >
    > For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

3.  Find the **Exception Paths** section from the **Exclusions** pane.

4. Check the check box next to the exception path you want to edit.

5. Click the **Edit** button and the **Add Exception Path** dialog window will appear.

6. After modification, click the **Save** button to save the settings.

**Remove Exception Path**

**Procedure**

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

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

   > **Note**
   >
   > For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

3. Find the **Exception Paths** section from the **Exclusions** pane.

4. Check the check box next to the Exception Path you want to remove.

5. Click the **Delete** button and the **Remove Exception Path** dialog window will appear.

6. Click the **Confirm** button to remove the selected entries.

**Trusted Hash Values Settings**

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

**Calculate Hash Values**

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

**Procedure**

1.  Find and click the **Trusted Hash Values** in the **Exclusions** pane.

2.  Download the **File Hash Generator** tool from the **Trusted Hash Values** area.

3.  Execute `WKFileHashGen.exe` from the downloaded folder. The **File Hash Generator** screen will appear.

4.  Use any of the following methods to select files and calculate hash values:

    •   Drag and drop folders or files to the **File Hash Generator** screen.

    •   Click the drop-down button and click **Add Files** to select the files to add.

    •   Click the drop-down button and click **Add Folder** to add all the files in the selected folder.

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

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

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

> **Note**
>
> - To ensure that all necessary files are calculated for hash values, TXOne Networks suggests adding the root folder of the target application to the **File Hash Generator** for calculation.
>
> - By clicking the **Add Folder** button, only the installer files, script files, and files in the PE (Portable Executable) format will be calculated.
>
> - For the single hash value, see *Add Trusted Hash Values on page 5-42* for how to add the copied hash value to the trusted hash value list.
>
> - For multiple hash values, see *Import Trusted Hash Values on page 5-43* for how to import the file containing the hash values to the trusted hash value list.

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

**Add Trusted Hash Values**

**Procedure**

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

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

> **Note**
>
> For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

**3.** Find and click the **Trusted Hash Values** in the **Exclusions** pane.

**4.** Click the **Add** button and fill in the hash values and notes.

**5.** Enable the **Installer** toggle switch to automatically add all files created or modified by the trusted installer to the Approved List.

**Import Trusted Hash Values**

**Procedure**

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

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

   > 📝 **Note**
   >
   > For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

3. Find and click the **Trusted Hash Values** in the **Exclusions** pane.

4. Click the **Import** button to import the .txt file containing a batch of hash values.

   > 📝 **Note**
   >
   > See *Calculate Hash Values on page 5-40* for generating the file containing the list of multiple hash values

5. Enable the **Installer** toggle switches to automatically add all files created or modified by the trusted installer to the Approved List.

**Edit Trusted Hash Values**

**Procedure**

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

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

   > 📝 **Note**
   >
   > For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

3.  Find and click the **Trusted Hash Values** in the **Exclusions** pane.

4.  Find the trusted hash value to be edited and click the corresponding Edit icon in the **Actions** column.

5.  The **Edit Trusted Hash Value** dialog window appears.

6.  After modification, click the **Save** button to complete the settings.

> 📝 **Note**
>
> Enable the **Installer** toggle switches to automatically add all files created or modified by the trusted installer to the Approved List.

**Remove Trusted Hash Values**

**Procedure**

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

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

> 📝 **Note**
>
> For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

3.  Find and click the **Trusted Hash Values** in the **Exclusions** pane.

4.  To delete multiple existing trusted hash values:

    a.  Click the checkboxes next to the existing trusted hash values.

    b.  Click the **Delete** button next to the **Import** button.

    c.  A warning message window appears. Click **Confirm** to delete the selected items.

5.  To delete single existing trusted hash values:

    a.  Find the trusted hash value to be deleted and click the corresponding Delete icon in the **Actions** column.

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

## Write Protection Settings

Write protection allows you to protect the details in certain files or folders from being changed by unauthorized users or applications.

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

**Procedure**

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

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

    > **Note**
    >
    > For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

3.  Find the **Write Protection** section from the **Exclusions** pane.

4.  Click the **Add** button and the **Add Write Protection** dialog window will appear.

5.  Select one of the protection types: **File**, **Folder**, **Registry Key** or **Registry Key and Value**.

6.  Input the path to the target object to be write protected.

7.  Set the **Exception Process Type**.

    •   No processes can write

    •   All processes can write

    •   Specify a process that can write by inputing the path.

**8.** Click the **Add** button and the settings will be saved.

**Edit Write Protection**

**Procedure**

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

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

> 📝 **Note**
>
> For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

**3.** Find the **Write Protection** section from the **Exclusions** pane.

**4.** Check the check box next to the protection type you want to edit.

**5.** Click the **Edit** button and the **Add Write Protection** dialog window will appear.

**6.** After modification, click the **Save** button to save the settings.

**Remove Write Protection**

**Procedure**

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

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

> 📝 **Note**
>
> For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

**3.** Find the **Write Protection** section from the **Exclusions** pane.

4. Check the check box next to the protection type you want to remove.

5. Click the **Delete** button and the **Remove Write Protection** dialog window will appear.

6. Click the **Confirm** button to remove the selected entries.

## Other Policy Settings for StellarProtect/StellarProtect (Legacy Mode)

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

- *Agent Component Update Schedule on page 5-47*

- *Device Control on page 5-49*

- *User-Defined Suspicious Objects on page 5-52*

- *Agent Password on page 5-53*

- *Patch on page 5-54*

### Agent Component Update Schedule

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

> **Note**
>
> StellarOEM license edition does not support this function.

**Procedure**

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

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

> **Note**
>
> For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

3. On the **Policy** page, find the **Schedule Update** in the **Agent Component Update Schedule** pane.

4. (Optional) Click **Go to StellarOne Scan Component Update Schedule** and view the current settings of StellarOne's component update schedule.

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

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

5. Toggle on the **Schedule Update**. Radio buttons for setting the **Frequency** and **Start Time** appear.

   • Click **Daily** to perform the agent component update every day

   • Click **Weekly** to perform the agent component update every week

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

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

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

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

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

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

## Device Control

StellarProtect/StellarProtect (Legacy Mode) 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 privilege 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.

> **Note**
>
> In addition to USB drives, StellarProtect (Legacy Mode) also supports blocking CD/DVD drives and floppy disks on managed endpoints.

**Procedure**

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

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

> ### 📝 Note
>
> For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

3. Make sure the **Device Control** toggle is switched on.

4. Click **Add**. The **Add Trusted USB Device** window appears.

5. Specify at least one of the following information for the trusted USB device.

   - **Vendor ID**

   - **Product ID**

   - **Serial number**

6. Click **OK** to complete the setting.

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

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

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

   - For removing multiple USB devices at the same time, select the USB devices and click the **Delete** button next to the **+Add** button.

   - For removing only one USB devices, click the Delete icon in the **Actions** column.

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

## Get Device Information

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

- Open the **Device Manager** on the endpoint.

- For StellarProtect (Legacy Mode) agent, use the SLCmd.exe command on the endpoint. Refer to [StellarProtect (Legacy Mode) Administrator's Guide](#) for more details.

- On StellarOne, go to the **Logs** > **Agent Events** on StellarOne console to check the event details about removable devices with Agent Event ID 1281/1282 (StellarProtect) or 5000/5001 (StellarProtect (Legacy Mode)).

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

- Export the agent's settings, make changes, and then import the modified settings back to the agent via StellarOne

- Import an updated settings file via StellarOne

- Use the SLCmd.exe command on the StellarProtect (Legacy Mode) agent

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

**Procedure**

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

2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.

3. Select the target agent by clicking the checkbox next to it.

4. Click the **Import/Export** button from the Tool Bar at the top of the **Agents** screen.

5. Click the **Export Agent Configuration** option.

6. Click **Confirm**.

7. A pop-up **Command Deployment** window appears. The **Status** shows if the agent configuration is exported successfully.

8. Click the **Download** link to download the target agent's configuration file.

9. Open the agent configuration file in a text editor and find the `DeviceException` section.

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

**FIGURE 5-2. DeviceException section**

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

```
<StorageDeviceBlocking Enable="no" ActionMode="1" AllowNonMassStorageUSBDevice="no">
    <DeviceException>
        <DeviceGroup name="UserDefined">
            <Device vid="781" pid="5151" sn="2444130A5442A4F5"/>
            <Device vid="951" pid="1666" sn="E03F49AEC0DDF351E913003F"/>
        </DeviceGroup>
    </DeviceException>
</StorageDeviceBlocking>
```

**FIGURE 5-3. Devices added in DeviceException section**

11. You can edit, add, or remove the trusted USB devices by modifying, adding, or deleting the entries for the trusted USB devices and save the agent configuration file.

12. Import the updated agent configuration file to the target agents.

## User-Defined Suspicious Objects

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

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

**Procedure**

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

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

   > **Note**
   >
   > For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

3. Find the **User-Defined Suspicious Object** at the right side of the screen.

4. Click **Add**. The **Add Item to User-Defined Suspicious Objects** window appears.

5. Select **Hash** or **File Path** as the suspicious file type.

6. Specify the file hash or path in the corresponding text field.

7. (Optional) Specify notes in the **Notes** text field.

8. Click **OK** to complete this task.

9. (Optional) To remove a user-defined suspicious object, select the target hash/file path and click the **Delete** button next to the **+Add** button.

10. A pop-up **Notification** window appears. Click **Confirm** to delete the selected item.

## Agent Password

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

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

**Procedure**

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

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

    > 📝 **Note**
    >
    > For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

3.  Scroll down and find the **Agent Password** at the right side of the screen.

4.  Select the **ADMINISTRATOR** or **USER** tab.

5.  Input the new password twice and click **Save** to finish this policy setting.

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

## Patch

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

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

**Procedure**

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

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

   > **✎** **Note**
   >
   > For instructions on how to go to the **Policy** page, see *Go to the Policy Screen on page 5-2*.

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

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

   > **✎** **Note**
   >
   > Users can import new patches for the agent on the *Importing/Deleting Agent's Patch on page 7-24* page.

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

> **Note**
>
> Since StellarOne can apply global policy to all managed agents or certain group policies to group-owned endpoints for conducting the patching process on multiple devices at the same time, before you select agent version, please be aware that:
>
> - By default, the global policy should be applied to every agent. TXOne Networks suggests that you keep lower agent version in the global policy settings.
>
> - If you don't want to set any agent version for patch deployment, please uncheck all checkboxes next to the agent version patch files in the **Patch** pane.

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

# Chapter 6

## Logs

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

# Agent Events

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

**Procedure**

1.  Mouse over the **Logs** tab in the top navigation bar of the StellarOne web console. A drop-down menu appears.

2.  Click the **Agent Events**.

3.  Click the StellarProtect or StellarProtect (Legacy Mode) tab, the corresponding agent event logs appear.

4.  Regarding how to search for the relevant log messages for troubleshooting or analysis. Please refer to *Agent Events Log Filtering on page 6-4* for more details.

> **Note**
>
> - For StellarProtect's event IDs and corresponding log information, refer to *Log Descriptions for StellarProtect on page A-2*.
>
> - For StellarProtect (Legacy Mode)'s event IDs and corresponding log information, refer to *Log Descriptions for StellarProtect (Legacy Mode) on page A-21*
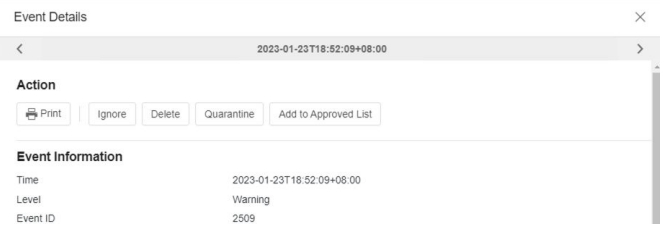
## About Agent Events Screen
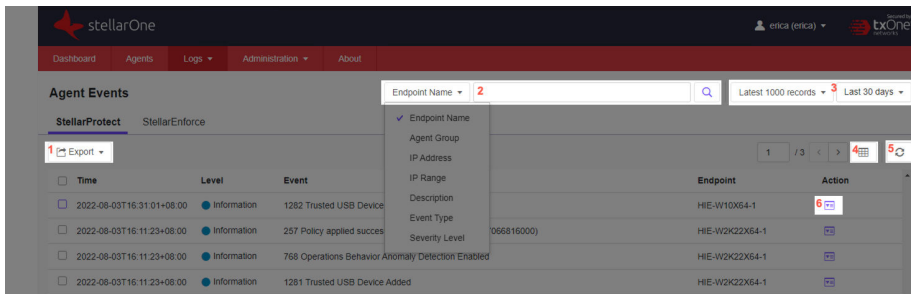


**FIGURE 6-1. StellarProtect Agent Events Logs**

**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:<br><br>• **Export Selected**: This button is activated when users select the checkbox(es) next to the logs to be exported.<br><br>• **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 6-4* for detailed procedures. |
| (3) Log display setting | Users can customize how many logs to be displayed either by:<br><br>• the number of the latest log records<br><br>• the logs generated within a particular period |
| (4) Screen display setting | By clicking this button, users can customize the screen display by:<br><br>• selecting how many logs to be displayed per page<br><br>• hiding certain contents by unchecking **Time**, **Level**, **Event**, or **Endpoint** in the **Cusomize Table Display** window. |

| Item | Description |
|---|---|
| (5) Refresh | The button allows users to manually refresh the screen for the latest log outputs. |
| (6) View Details | For **Information** level logs, this button allows users to view and print event details such as event information, agent information and components version. |
| | For **Critical** level logs, this button allows users to view and print event details such as event information and agent information. |
| | For **Warning** level logs, in addition to viewing and printing event details such as event information and agent information, this button also allows users to apply one of the following actions to the unknown files, such as **Ignore**, **Delete**, **Quarantine**, and **Add to Approved List**. |



**Figure 6-2. Event Details of Warning Level Logs**

## 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 *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 the Agents by StellarOne are logged and shown in the **Server Events** screen.

**Procedure**

1. Mouse hover the **Logs** tab in the top navigation bar of the StellarOne web console. Click the **Server Events** option.

**2.** Click the StellarProtect or StellarProtect (Legacy Mode) tab, the configuration events deployed on the Agents by StellarOne appear.

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

## About Server Events Screen
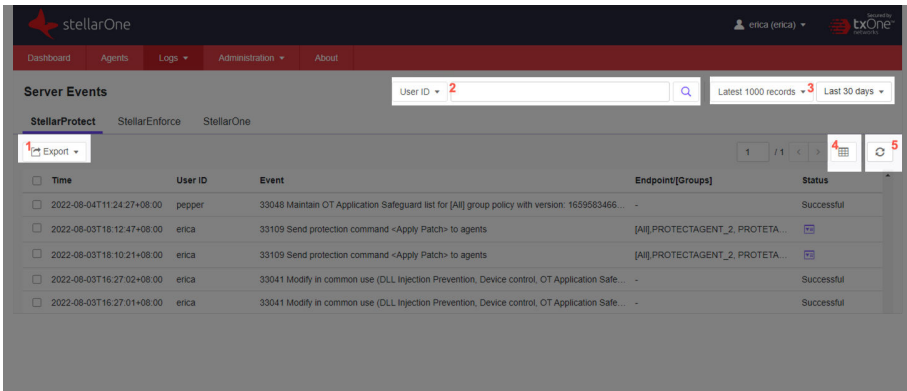


**FIGURE 6-3. Server Events Logs for SterllarProtect**

**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: <br><br> • **Export Selected**: This button is activated when users select the checkbox(es) next to the logs to be exported. <br><br> • **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 *Server Events Log Filtering on page 6-8* for procedures. |

| Item | Description |
|------|-------------|
| (3) Log display setting | Users can customize how many logs to be displayed either by:<br><br>• the number of the latest log records<br><br>• the logs generated within a particular period |
| (4) Screen display setting | By clicking this button, users can customize the screen display by:<br><br>• selecting how many logs to be displayed on one page<br><br>• hiding certain contents by unchecking **Time**, **User ID**, **Event**, **Endpoint/[Groups]**, or **Status** in the **Cusomize Table Display** window. |
| (5) Refresh | The button allows users to manually refresh the screen for the latest log outputs. |



**Figure 6-4. 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:<br><br>• **Export Selected**: This button is activated when users select the checkbox(es) next to the logs to be exported.<br><br>• **Export All**: This button is always activated for users to export all logs. |

| Item | Description |
|------|-------------|
| (2) Screen display setting | By clicking this button, users can customize the screen display by:<br><br>• selecting how many logs to be displayed per page<br><br>• hiding certain contents by unchecking **Time**, **User ID**, **Event**, **Endpoint/[Groups]**, or **Status** 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 *Server Event Log Descriptions for StellarProtect on page A-19* for more details on various event types.

3. Click the search icon next to the search bar and then the screen will display the search result.

4. To clear the search criteria, close the filtering criteria appears above the **Export** button.

> **Note**
>
> Please refer to *Server Event Log Descriptions for StellarProtect on page A-19* and *Server Event Log Descriptions for StellarOne on page A-71* in the Appendices for more details about event IDs and corresponding log information..

## System Logs

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

**Procedure**

1. Mouse over the **Logs** tab in the top navigation bar of the StellarOne web console.

2. Click the **System Logs** option.

3. The **System Logs** screen appears.

# About System Logs Screen
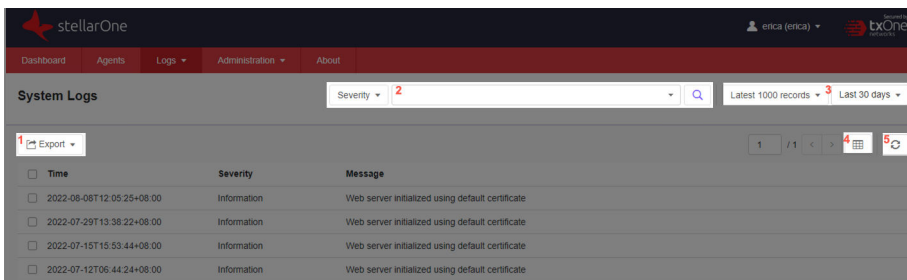


**FIGURE 6-5. System Logs Screen**

**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:<br><br>• **Export Selected**: This button is activated when users select the checkbox(es) next to the logs to be exported.<br><br>• **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:<br><br>• Emergency<br><br>• Alert<br><br>• Critical<br><br>• Error<br><br>• Warning<br><br>• Notice<br><br>• Information<br><br>• Debug<br><br>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:<br><br>• the number of the latest logs records<br><br>• the logs generated within a particular period |
| Screen display setting | By clicking this button, users can customize the screen display by:<br><br>• selecting how many logs to be displayed per page<br><br>• 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
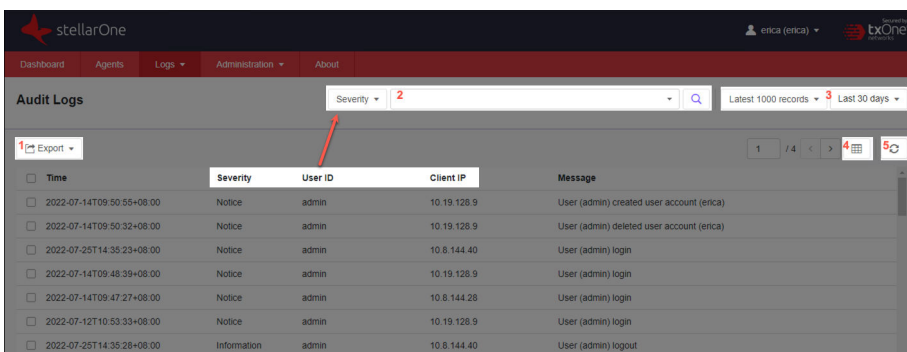


**FIGURE 6-6. Audit Logs Screen**

**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:<br><br>• **Export Selected**: This button is activated when users select the checkbox(es) next to the logs to be exported.<br><br>• **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 6-13* for procedures. |

| Item | Description |
|------|-------------|
| (3) Log display setting | Users can customize how many logs to be displayed either by:<br><br>• the number of the latest logs records<br><br>• the logs generated within a particular period |
| (4) Screen display setting | By clicking this button, users can customize the screen display by:<br><br>• selecting how many logs to be displayed per page<br><br>• 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.

      • Emergency

      • Alert

- Critical

- Error

- Warning

- Notice

- Information

- Debug

3. Click the search icon next to the search bar, and then the screen will display the search result.

4. To clear the search criteria, close the filtering criteria appears above the **Export** button.

# Chapter 7

## Administration

This chapter introduces the StellarOne web console's administration settings, mainly grouped into four categories: **Account**, **Notification**, **Update**, and **System**.

Topics in this chapter includes:

- **Account**
  - *Account Management on page 7-3*
  - *Single Sign-On on page 7-11*
- **Notification**
  - *SMTP Settings and Notification on page 7-14*
  - *Scheduled Report on page 7-16*
  - *Syslog Forwarding on page 7-18*
- **Update**
  - *Proxy Settings on page 7-19*
  - *Downloads/Updates on page 7-20*
  - *Importing Firmware on page 7-25*

- *About the License Screen on page 7-27*

- **System**

    - *System Time on page 7-36*

    - *Log Purge on page 7-36*

    - *Importing SSL Certificate on page 7-38*

    - *OT Intelligent Trust on page 7-39*

    - *Service Integration on page 7-39*

# Account

Topics in this section 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**. One allows users to manage accounts; the other one provides information about different privileges for different accounts.
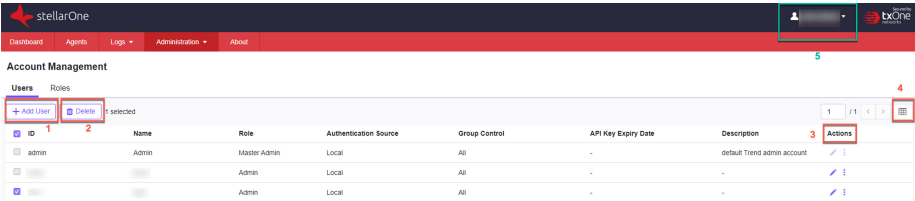


**FIGURE 7-1. Account Management Screen**

**TABLE 7-1. About Account Management Screen - Users**

| ITEM | DESCRIPTION |
|---|---|
| (1) **+Add User** | This button allows you to add account(s) for accessing StellarOne web console. See *Add Accounts on page 7-8* for instructions. |
| (2) **Delete** | This button allows you to delete account(s). See *Delete Accounts on page 7-9* for instructions. |

| Item | Description |
|---|---|
| (3) **Actions** | The **Edit** button allows you to edit a single user account. See *Edit Accounts on page 7-10* for instructions. |
| | The three dots **More Actions** button allows you to: |
| | •   Generate an API Key: see *Generate an API Key on page 7-10* for instructions. |
| | •   Delete a single user account: see *Delete Accounts on page 7-9* for instructions. |
| (4) **Screen display setting** | By clicking this button, you 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** | Click the account icon at the top-right corner of the screen to change your password or log off. |

See *Account Types on page 7-4* for more information about the **Roles** page.

## Account Types

StellarOne user accounts are categorized into three types as listed below.

**Table 7-2. StellarOne Account Types**

| Account Types | Access Rights | Privileges |
|---|---|---|
| Admin | Full control | •   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 |

| Account Types | Access Rights | Privileges |
|---|---|---|
| Operator | Asset control | • Manage Group: The privilege of creating, moving, or deleting groups<br><br>• 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.<br><br>• Allowed to download the Agent's installer package and `Group.ini` file<br><br>• 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 | √ | √ | |

| Task | Account Privilege Allowed | | |
|---|---|---|---|
| | Admin | Operator | Viewer |
| Configure Device Control | √ | √ | |
| Add trusted files | √ | √ | |
| Add trusted USB devices | √ | √ | |
| Scan now | √ | √ | |
| Update Approved List | √ | √ | |
| Update agent components | √ | √ | |
| Deploy agent patch | √ | √ | |
| Check connection | √ | √ | |
| Deploy policies | √ | √ | |
| Policy refresh interval | √ | √ | |
| Collect event logs | √ | √ | |
| Import / Export (Approved List / agent configuration) | √ | √ | |
| Organize (edit description / move / delete) | √ | √ | |
| Configure group policy | √ | √ | |
| Configure global policy | √ | √ | |

| Task | Account Privilege Allowed | | |
|---|---|---|---|
| | Admin | Operator | Viewer |
| 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 | √ | √ | |
| Scheduled report | √ | √ | √ |
| Notification settings | √ | √ | √ |
| SMTP settings | √ | √ | |
| Proxy settings | √ | √ | |
| Downloads / Updates | √ | √ | √ |
| Firmware update | √ | | |
| SSL Certificate | √ | | |
| License management | √ | √ | |

## Add Accounts

This section describes how to add user accounts for accessing StellarOne web console.

**Procedure**

1.  Log on to the web console using an account with the **Admin** role.

    > **Note**
    >
    > - The logon credentials entered here are case-sensitive.
    > - Only the account with the **Admin** role can manage user accounts.

2.  Go to **Administration** > **Account Management**.

3.  Click **Add User** button, and then the **Add User Account** window appears.

4.  Specify the **Authentication Source** (**Local** or **SAML Identity Provider**).

    - To add a **Local** user, specify the **ID** and **Name**.

    - To add an **SAML Identity Provider** user, specify **Email for SAML Account Mapping** and **Name**.

        > **Note**
        >
        > To allow an SAML Identity Provider user to log in using Single Sign-On (SSO), click the **Single Sign On Configuration** link. Please refer to *Single Sign-On on page 7-11* for procedures.

        > **Note**
        >
        > The **ID**, **Name**, and **Email for SAML Account Mapping** entered here are case-sensitive.

5.  **Role**: Select among the account roles **Admin**, **Operator** or **Viewer** (Default). Please refer to *Account Types on page 7-4* for more details on the account privileges.

- For a **Local** user, specify the **Local Password** and re-type it for confirmation.

6.  **Group Control**: Select the groups the target account is allowed to access or view.

7.  Click **Confirm** to complete the user account creation.

## Delete Accounts

This section describes how to 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).

## Edit Accounts

This section describes how to edit user accounts that have been created.

**Procedure**

1. Log on to the web console using an account with the **Admin** role.

   > **Note**
   >
   > - The logon credentials entered here are case-sensitive.
   >
   > - Only the account with the **Admin** role can manage user accounts.

2. Go to **Administration** > **Account Management**.

3. Under the **Actions** column, click the edit icon corresponding to the target user account.

4. The **Edit User Account** window appears.

   - For a **Local** user, the **Role**, **Name**, **Password**, **Group Control**, and **Description** of an account can be edited.

   - For an **SAML Identity Provider** user, the **Role**, **Name**, **Group Control**, and **Description** of an account can be edited.

     > **Note**
     >
     > To allow an SAML Identity Provider user to log in using Single Sign-On (SSO), click the **Single Sign On Configuration** link. Please refer to *Single Sign-On on page 7-11* for procedures.

5. Click **Confirm** to complete editing user account(s).

## Generate an API Key

Users can generate API keys and query data from agents via the open API. The expiration dates of the API keys can be set for different user accounts to increase account management efficiency.

**Procedure**

1.  Log on to the web console using an account with the **Admin** role.

    > **Note**
    >
    > •   The logon credentials entered here are case-sensitive.

2.  Go to **Administration** > **Account Management**.

3.  Under the **Users** tab, find the user ID you want to modify and go to the kebab menu under **Actions** at the right of the screen.

4.  Click on the kebab menu, and then select the **Generate an API Key** option.

5.  The **Generate an API Key** window appears. Click the date picker and choose an expiration date on the pop-up calendar. Click **Confirm**.

6.  An API key is generated. Click the clipboard for copying the generated API key.

    > **Important**
    >
    > Make sure to back up the copied API key before proceeding to the next step. The API key will not be displayed again for security reasons.

7.  Click **OK**.

8.  Check the result under the **API Key Expiry Date** or mouse over above the kebab menu of the user account, and the expiration date of the API key will appear.

## Single Sign-On

Users who log on with the SAML Identity Provider 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 7-13* 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.
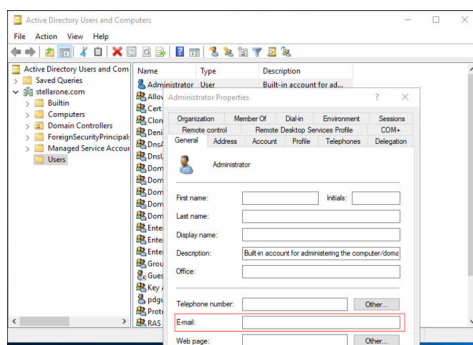


**FIGURE 7-2. Resolving SSO Issue - Email Check**

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**.
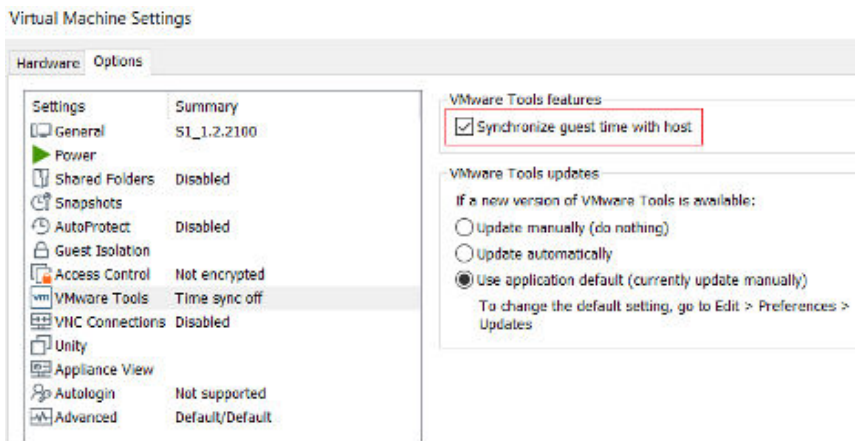
**FIGURE 7-3. Virtual Machine Settings - Time Synchronization**

# Notification

Topics in this section includes:

## SMTP Settings and Notification

The settings allow users to receive notifications of warning or outbreak events by emails.

**Procedure**

1.  Go to **Administration** > **SMTP Settings** for specifying the SMTP server setting required for notification sending.

2. Specify the **Server address**, **Port**, and **Sender**.

3. Specify the Security mode by clicking **STARTTLS**, **SMTPS**, or **None**.

4. (Optional) If the SMTP server requires authentication, click the checkbox next to **SMTP server requires authentication**. Specify the **User name** and **Password** as the SMTP server authentication credential.

5. Click the **Send Test Email** button to send a test email from StellarOne (This step is essential for *Step 13*).

6. Click **Save** to complete the SMTP setting.

7. Go to **Administration** > **Notification** for notification criteria and email setting.

8. Under the **Warning Level Agent Events**, click the **Send warning level agent events** toggle to enable it.

> **Note**
>
> When the 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.

9. 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.

10. Define an outbreak by the number of detections and the detection period.

   • Specify the number of occurrences of an event in the field of **Number of warnings in a time period** (1- 20000).

   • Specify the time frame during which the event has occurred in the field of **The time period of those warnings** (1 - 60 minutes).

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

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

13. Go to the specified email box to check if you receive the test email sent from StellarOne (see *Step 5*).

## Scheduled Report

By configuring the **Scheduled Report**, users can receive a list of all reports that automatically generate on a user-defined schedule. The **Scheduled Report** screen also provides basic information about previously configured schedules and recipients, as well as allows users to enable and disable sending scheduled reports

**Note**

Only StellarProtect (Legacy Mode) supports this function.

**Procedure**

1. Go to **Administration** > **Scheduled Report**.

2. Toggle on **Send scheduled reports**.

**Note**

By default, the **Scheduled Report** is disabled.

3. Three available settings appear on the **Scheduled Report** screen.

| Settings | Description |
|---|---|
| **Report content** | Event Type:<br><br>• StellarProtect (Legacy Mode) Blocked Event History<br><br>• StellarProtect (Legacy Mode) Top 10 Endpoints with Blocked Events<br><br>• StellarProtect (Legacy Mode) Top 10 Blocked Files<br><br>Time Period: A drop-down menu for users to choose preferred time period during which the above-mentioned events occur<br><br>• Last 7 days<br><br>• Last 14 days<br><br>• Last 30 days<br><br>• Last 3 months<br><br>• Last 6 months |
| **Schedule** | Set the frequency and start time for the scheduled reports on a daily, weekly, or monthly basis.<br><br>**Note**<br>It is advisable 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. |
| **Recipients** | A valid email address is required for specifying the report recipient.<br><br>**Note**<br>When entering muiltiple email addresses, be sure to use the semicolon character to separate them. |

4. Click **Save** to save the settings.

## Syslog Forwarding

Users can forward the Server and Agent Event logs to an external Syslog server for increasing monitoring and management capabilities. TXOne StellarOne console forwards logs in the Common Event Format (CEF). Make sure your Syslog server supports the Common Event Format (CEF).

**Procedure**

1. Go to **Administration** > **Syslog Forwarding**.

2. Click the **Forward logs to syslog server (CEF only)** toggle to switch on the function.

3. Specify the **Server Address**, **Port**, and **Protocol** of the Syslog server.

4. Click **Save** to complete the settings.

   Please refer to *StellarProtect Agent Event Format on page A-72*, *StellarProtect Server Event Format on page A-75*, or *StellarOne Server Event Format on page A-78* in the Appendices for details about the logs forwarded in the Common Event Format (CEF).

# Update

Topics in this section includes:

- *Proxy Settings on page 7-19*

- *Downloads/Updates on page 7-20*

- *Importing Firmware on page 7-25*

- *License on page 7-26*

## 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 or SLCmd.exe Command Line Interface tool on the local StellarProtect or StellarProtect (Legacy Mode) Agent.

## Downloads/Updates

The **Downloads/Updates** page allows users to execute below tasks:

- Configuring scan component for StellarOne

- Downloading the Agent Installer Package or Group.ini file for *Group Mapping on page 7-23*.

- Importing or deleting patch files for the agents

## Configuring Scan Component for StellarOne

**Procedure**

1. Go to **Administration** > **Downloads/Updates** > **StellarOne**.

2. To start the component update for StellarOne immediately, click the **Update Now** button in the **Scan Component** section.

> **Note**
>
> - By clicking the **Update Now**, StellarOne will download and update the latest components. All of the pattern and engine versions available are listed under the **Update Now** button.
>
> - You can refer to the **Last Updated:** near the **Update Now** button for the last time the scan component was updated.

**3.** To schedule for the component update, find and click the **Scan Component Update Schedule (StellarOne)** at the bottom of the screen.

   a. The **Scan Component Update Schedule (StellarOne)** window appears.

   b. Toggle on the **Schedule Update**.

   c. Click the radio buttons next to **Frequency** to set the frequency by **Daily**, **Weekly**, or **Monthly**.

   > **Important**
   >
   > It is advisable NOT to select the date 29th, 30th, or 31st for monthly update frequency. This helps prevent the system from bypassing the update in the month that does not contain the date 29th, 30th, or 31st.

   d. Click the **Start Time** to determine when to start the scheduled scan component update.

**4.** To specify the download source for StellarOne regarding different network configurations, find and click the **Scan Component Update Source** at the bottom of the screen.

   a. The **Scan Component Update Source** window appears.

   b. In the **Scan Component Update Source (StellarOne)** section:

   - If the StellarOne server can connect to the ActiveUpdate server, select the **ActiveUpdate server**, the component update will be downloaded directly from the ActiveUpdate server.

- If the StellarOne server can not connect to the ActiveUpdate server or if users host an update server in an internal network, select **Other update source** and specify the URL address in the text field.

5. To specify the download source for agents regarding different network configurations or agent types, find and click the **Scan Component Update Source** at the bottom of the screen.

   a. The **Scan Component Update Source** window appears.

   b. In the **Scan Component Update Source (Agents)** section:

   - If the agents can connect to StellarOne server, select **Update from StellarOne** to download the component update directly from the StellarOne server.

   - If the agents can not connect to StellarOne server or if they are standalone agents, select **Other update source** and specify the URL address in the text field.

## Downloading Agent Installer Package/Group.ini File

**Procedure**

1. Go to **Administration** > **Downloads/Updates** > **Agent**.

2. To download the latest Agent Installer Package. Click **Download**.

**FIGURE 7-4. Downloads/Updates Screen**

A zipped folder is downloaded. Extract the folder and proceed with the installation for the agents. Please refer to the [StellarProtect Installation Guide](#) for more details.

3. (Optional) If the StellarOne uses proxy to communicate with the agents, click the **Proxy** link or go to **Administration** > **Proxy** to complete the proxy configuration before downloading the installer package. Please refer to *Proxy Settings on page 7-19* for detailed procedures.

4. (Optional) To directly register the agent to a specific group via StellarOne console, click the **download a Group.ini** link and add it into the agent's installer package. Please refer to *Group Mapping on page 7-23* for more details.

## Group Mapping

This function allows users to directly register agent to a specific group via the StellarOne web console.

**Procedure**

1.  Go to **Administration** > **Downloads/Updates**.

2.  Select the **Agent** tab.

3.  Click **Download** to download the Installer Package.

4.  Click the **download Group.ini** link.

5.  The **Select a group** window appears.

6.  Select a group for the target agent and click **Download**. Click the **Close** button to close the window.

7.  A file named Group.ini has been downloaded. Place the Group.ini file as the top-level file in the installer package of the target agent.

8.  Run the installation on the target agent. Make sure the agent is connected to StellarOne console during the installation process.

9.  Users can check the StellarOne console and the on-site target agent to see if the agent is successfully registered.

## Importing/Deleting Agent's Patch

**Procedure**

1.  Go to **Administration** > **Downloads/Updates** > **Agent** > **Patch**.

2.  Select **StellarProtect** or **StellarProtect (Legacy Mode)** to determine the target agent.

3.  Click **Import** to import the target patch file.

4.  A **Import Patch** window appears. Click the radio button to determine the target agent.

5.  Click **Select File** to select the patch file to import.

6. To remove existing patch files on StellarOne, select the target files and then the **Delete** button appears next to the **Import** button. Click **Delete** to remove the selected entries.

## Importing Firmware

**Procedure**

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

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

3. The **Firmware Update** window appears. The **Version** shows the current StellarOne build version, the **Release Date** and **Description** show the information for the StellarOne patch file.

4. Click **Apply** to apply the patch to StellarOne.

5. Read the upgrade notice carefully.

6. Click **Install Now** to implement the update or **Abort** to stop the update.

**FIGURE 7-5. Firmware Update Notice**

## License

Topcis in this section includes:

## About the License Screen

Go to **Administration** > **License**. Below table lists details about the **License** page.



**FIGURE 7-6. The License Screen**

**TABLE 7-4. About the License Screen**

| ITEM | DESCRIPTION |
|---|---|
| **Renew License Key** | This button is for license renewal using the same license key. Refer to *Renew License with the same License Key on page 7-30* for more details. |
| **New License Key/ File** | This button is for license activation using new license key or license file. Refer to *New License Key/File on page 7-32* for more details. |
| | 📝 **Note**<br><br>This button can also be used for other purpose: license renewal using the license file. Refer to *Renew License by Importing License File on page 7-30* for more details. |
| **License Edition** | Displays current license edition for Stellar product. Refer to *License Editions on page 7-33* for more details. |
| **License Type** | • Full: a full version that is officially authorized.<br><br>• Trial: a trial version with excluded features or limited functions.<br><br>• Perpetual: provides permanent use and 5-year technical support. |
| **Seats** | Specifies current number of agents managed by StellarOne and the total number of agents that can be managed by StellarOne. For example, **Seats: 2/10** means:<br><br>• 2 agents are currently managed<br><br>• Up to 10 agents can be managed |
| | 📝 **Note**<br><br>Overseat is triggered when seat in use exceeds the seat count; the agents that can not be managed by StellarOne due to overseat will be classified as "Inactive Agents" on the **Agents** screen. See *Filter Options for Agents/Groups on page 4-9* for more details. |

| Item | Description |
|---|---|
| **Status** | • Activated: The existing license is effective.<br><br>• Expired: The existing license is out of date.<br><br>---<br>📝 **Note**<br>It is advisory to renew license promptly to protect your devices against cybersecurity threats. Refer to one of the methods listed below for license renewal.<br><br>• *Renew License with the same License Key on page 7-30*<br><br>• *Renew License by Importing License File on page 7-30* |
| **Expiration** | Displays the effective date of existing license. |
| **License Key** | The license key that is required for activating StellarOne. |
| **Last Updated** | Displays the last time the License Key is updated. |
| **Learn More** | The link directs users to the Online Help web page for more details on license. |
| **Download the Latest License File** | The link is used to download the latest license file to renew license for standalone agents. |

## License Management

Users can renew license or activate new license via the StellarOne web console.

### License Renewal

Choose one of the ways to renew license based on the license data available from your support provider:

- *Renew License with the same License Key on page 7-30*

- *Renew License by Importing License File on page 7-30*

**Renew License with the same License Key**

**Procedure**

1. Go to **Administration** > **License**

2. Click the **Renew License Key** button.

3. A message with **The License has been updated successfully** appears. The **Last Updated** shows the latest license renewal date and time.

**Renew License by Importing License File**

**Procedure**

1. Go to **Administration** > **License**

2. Click the **New License Key / File** button.

3. The **New License** window appears.

4. Click **License File**.

5. Select the license file (a `.txt` file) to import.

   > **Note**
   >
   > If you don't have the license file on hand, refer to *Getting the License File on page 7-30*.

6. Click **Apply**.

7. A success message appears. The updated license information will be shown on the **License** page.

**Getting the License File**

The license file can be used for license renewal or new license activation. To get a license file, follow below precedures.

**Procedure**

1. Go to **Administration** > **License**

2. Click the **New License Key / File** button.

3. The **New License** window appears.

4. Click **License File**.

5. Click **Copy Download Link for getting the License File** at the bottom of the **New License** window.
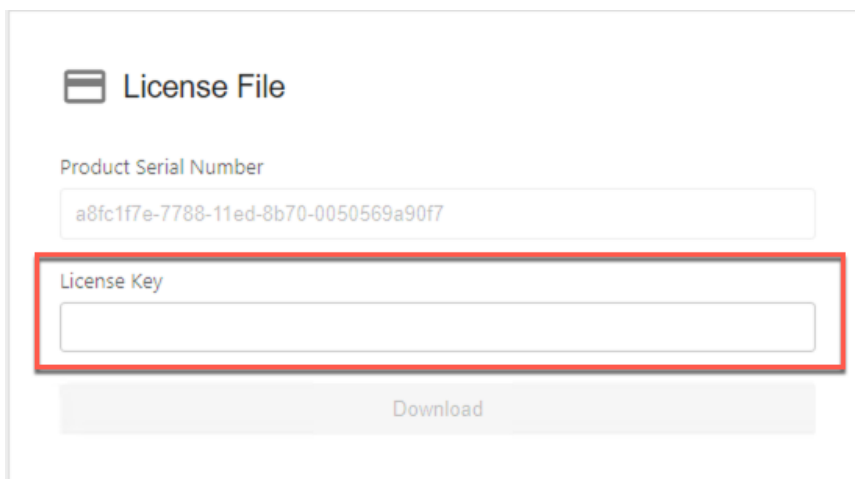
> ⚠️ **Important**
>
> A license key is required for downloading a license file.
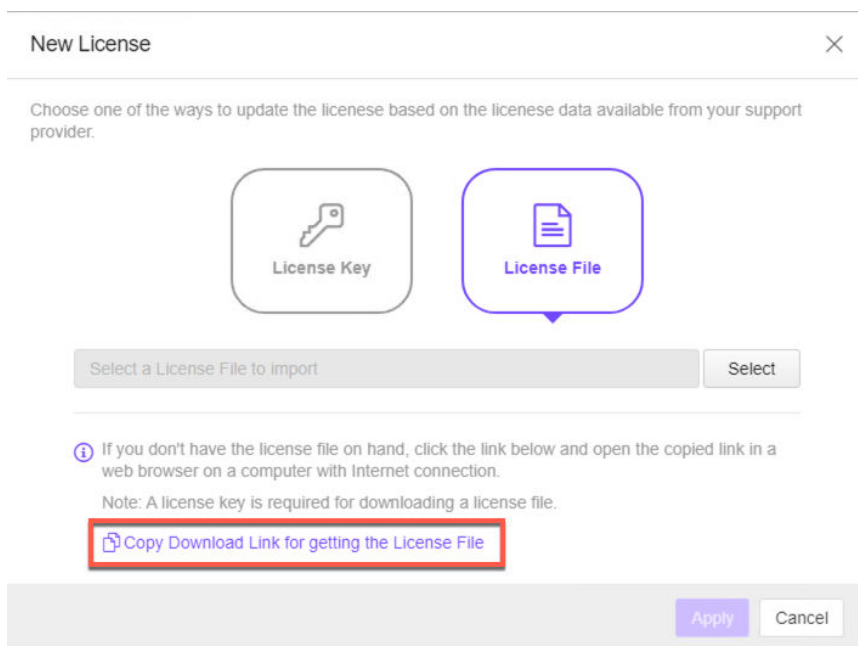


**FIGURE 7-7. Copy Download Link for License File**

6.  **The Download Link has been copied** toast message appears.

7.  Open the copied link in a web browser on a computer with Internet connection.

8.  You will be directed to the TXOne **License File Management** screen. Specify your license key in the **License Key** field, and then click **Download**.



**FIGURE 7-8. TXOne License File Management**

9.  A pop-up window appears showing the license information. Read it carefully and click **Yes** for downloading the license file.

**New License Key/File**

If users need to activate a new license key or license file, follow below procedures.

**Procedure**

1.  Go to **Administration** > **License**.

2. Click **New License Key / File**.

3. The **New License** window appears. Choose one of the ways:

   - Click **License Key** and specify the new license key in the text field below.

   - Click **License File** and select the license file (a `.txt` file) to import.

   > **Note**
   >
   > If you don't have the license file on hand, refer to *Getting the License File on page 7-30*.

4. Click **Apply**.

5. A message with **The License is activated successfully** appears.

## License Editions

See below as the three kinds of license editions for the TXOne Stellar 2.2. 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:<br>• Anti-Virus (Real-Time Malware Scan)<br>• Application Lockdown<br><br>StellarProtect (Legacy Mode) Agent:<br>• Anti-Malware Scan<br>• Application Lockdown | Annual |

| EDITION | PRIMARY FUNCTION | DURATION |
|---------|-----------------|----------|
| StellarKiosk | StellarProtect Agent:<br><br>• Anti-Virus (Real-Time Malware Scan)<br><br>StellarProtect (Legacy Mode) Agent:<br><br>• Anti-Malware Scan<br><br>• Application Lockdown | Annual<br><br>**Note**<br>StellarKiosk was named StellarMix before the TXOne Stellar version 2.0. |
| StellarOEM | StellarProtect Agent:<br><br>• Application Lockdown<br><br>StellarProtect (Legacy Mode) Agent:<br><br>• Application Lockdown | Perpetual<br><br>**Note**<br>• StellarOEM provides permanent use and 5-year technical support for the TXOne Stellar.<br><br>• This license edition does not support features such as scan and agent component update.<br><br>• StellarOEM was named Perpetual before the TXOne Stellar version 2.0. |

**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 | √ | √ | √ |

## System

Topics in this section includes:

## System Time

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

**Procedure**

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

2. Two options are available for configuring StellarOne system time. In the **Date and Time** section:

   - If you want to set the system time manually, click the Edit icon to specify the date and time, and then click **Apply** to save the setting.

   - If you want to align StellarOne system time with an NTP server, click the **Synchronize system time with an NTP server** toggle to enable it. Click **Test Synchronization** to check if the sync was successful.

     > **Note**
     >
     > The default NTP server is pool.ntp.org.

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

4. Select the appropriate time zone for the system, and then click **Save** to complete the settings.

## Log Purge

This feature allows users to manage the volume of log files for optimizing 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 Now** 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 want 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.

- 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.

## Importing SSL Certificate

**Procedure**

1. Go to **Administration** > **SSL Certificate**.

2. Click **Import Certificate**, and then the **Import Certificate** window appears.

- Click the **Select file...** next to the **Certificate** option to select the target certificate.

- Click the **Select file...** next to the **Private Key** option to select the target private key.

- (Optional) Specify the passphrase in the **Passphrase** text field.

> **✎ Note**
>
> Supported certificate and private key formats include:
>
> - Certificate and private key in PEM format
>
> - Private key in PKCS #1 format with or without encryption
>
> - Private key in PKCS #8 format without encryption

3.  Click **Import and Restart** to start importing the target certificate.

> **✎ Note**
>
> Importing the certificate requires restarting the StellarOne console.

## OT Intelligent Trust

When enabled, TXOne OT Intelligent Trust shares anonymous threat information with the Smart Protection Network, allowing TXOne to rapidly indentify and address new threats. You can disable TXOne OT Intelligent Trust anytime on this console.

**Procedure**

1.  Go to **Administration** > **OT Intelligent Trust** .

2.  Click the **Learn More** for visiting TXOne's OT threat research website.

3.  To enable TXOne OT Intelligent Trust, toggle on the **Enable TXOne OT Intelligent Trust (recommended)**.

## Service Integration

## Integrate with Trend Micro Vision One

Users can query for StellarOne malware detection logs via Trend Micro Vision One Search app.

---

> ⚠️ **Important**
>
> Be sure to complete the deployment of Trend Micro Vision One Service Gateway and enable **Forward proxy** function first, and then obtain the information for Service Gateway settings required in *Step 2* and *Step 3*. Please contact your support provider for more information.

---

**Procedure**

1. On StellarOne console, go to **Administration** > **Service Integration**.

2. Specify the IP address and API key of Trend Micro Vision One Service Gateway in **Service Gateway Address** and **Service Gateway API Key**.

   ---

   > 📝 **Note**
   >
   > The IP address and API key should be obtained from the Trend Micro Vision One Service Gateway Virtual Appliance.

   ---

3. Specify the Trend Micro Vision One enrollment token in **Product Connector Enrollment Token**.

   ---

   > 📝 **Note**
   >
   > The enrollment token is required to register StellarOne to Trend Micro Vision One. The enrollment token will expire within 24 hours if not used after generated from the Vision One Product Connector app.

   ---

4. Click **Test Connection** and a success message should appear.

5. Find **Forward Logs to Vision One** section, and then toggle on **Send StellarOne malware detection logs to Vision One**.

6. The **Log Sending Interval** menu appears. Select the frequency in the drop-down menu for sending StellarOne detection logs to Trend Micro Vision One.

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

> **Note**
>
> If StellarOne has connected with Trend Micro Vision One successfully, the **Vision One Onboarding Status** should display **Connected**.

# Chapter 8

## Technical Support

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

Learn about the following topics:

# Troubleshooting Resources

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

## Using the Support Portal

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

**Procedure**

1.  Go to https://success.trendmicro.com.

2.  Select from the available products or click the appropriate button to search for solutions.

3.  Use the **Search Support** box to search for available solutions.

4.  If no solution is found, click **Contact Support** and select the type of support needed.

    > **Tip**
    >
    > To submit a support case online, visit the following URL:
    >
    > https://success.trendmicro.com/smb-new-request

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

## Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro and TXOne combats this complex malware with products that create a custom

defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

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

- Malware and malicious mobile code currently active or "in the wild"

- Correlated threat information pages to form a complete web attack story

- Internet threat advisories about targeted attacks and security threats

- Web attack and online trend information

- Weekly malware reports

# Contacting Trend Micro and TXOne

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

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

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

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

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

- Worldwide support offices:

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

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

- Trend Micro product documentation:

    https://docs.trendmicro.com

## Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem

- Appliance or network information

- Computer brand, model, and any additional connected hardware or devices

- Amount of memory and free hard disk space

- Operating system and service pack version

- Version of the installed agent

- Serial number or Activation Code

- Detailed description of install environment

- Exact text of any error message received

# Sending Suspicious Content to Trend Micro

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

## Email Reputation Services

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

https://ers.trendmicro.com/

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

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

## File Reputation Services

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

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

Record the case number for tracking purposes.

## Web Reputation Services

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

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

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

# Other Resources

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

## Download Center

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

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

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

# Appendix A

## Appendices

Topics in this section include:

- *Log Descriptions on page A-2*
- *Syslog Content - CEF on page A-72*

# Log Descriptions

Topics in this section include:

## Log Descriptions for StellarProtect

Topics in this section include:

### Agent Event Log Descriptions for StellarProtect

This table details the Windows event log descriptions for StellarProtect.

| EVENT ID | LEVEL | CATEGORY | EVENT | DETAILS |
|----------|-------|----------|-------|---------|
| 256 | Information | System | Service has started. | |
| 257 | Information | System | Policy has been applied successfully. (Version: %version%) | |
| 258 | Information | System | Patch has been applied. File Name: %file_name% | |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| 259 | Information | System | Patching in progress | After the earlier-applied patch is completed, the system will automatically try to apply this patch: %deferred_file_name%. |
| 513 | Information | intelli_av | Application vault update was successful | |
| 514 | Information | intelli_av | Real Time Scan has been enabled. | |
| 515 | Information | intelli_av | A scheduled scan has started. | |
| 516 | Information | intelli_av | A scheduled scan has ended. | Folders scanned: %1<br><br>Symbolic links: %2<br><br>Regular files: %3<br><br>Files scanned: %4<br><br>Files passed: %5<br><br>Threats detected: %6 |
| 517 | Information | intelli_av | A manually launched scan has started. | |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| 518 | Information | intelli_av | A manually launched scan has ended. | Folders scanned: %1<br><br>Symbolic links: %2<br><br>Regular files: %3<br><br>Files scanned: %4<br><br>Files passed: %5<br><br>Threats detected: %6 |
| 519 | Information | intelli_av | A scheduled scan has been enabled. | Next scan will be on %NextScan %. |
| 520 | Information | intelli_av | A scheduled scan has been disabled. | |
| 521 | Information | intelli_av | A scan manually launched by local user has started. | |
| 522 | Information | intelli_av | A scan manually launched by local user has ended. | Folders scanned: %1<br><br>Symbolic links: %2<br><br>Regular files: %3<br><br>Files scanned: %4<br><br>Files passed: %5<br><br>Threats detected: %6 |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| 768 | Information | anomaly_detect | Operations Behavior Anomaly Detection Enabled | Mode: %Mode%<br><br>Level: %Level% |
| 769 | Information | anomaly_detect | An operational process has been added to the approved operations of Operations Behavior Anomaly Detection. | Access User: %USERNAME%<br><br>ID: %ID%<br><br>Target Process: %PATH% %ARGUMENT%<br><br>Parent Process 1: %PATH% %ARGUMENT%<br><br>Parent Process 2: %PATH% %ARGUMENT%<br><br>Parent Process 3: %PATH% %ARGUMENT%<br><br>Parent Process 4: %PATH% %ARGUMENT% |

| EVENT ID | LEVEL | CATEGORY | EVENT | DETAILS |
|---|---|---|---|---|
| 770 | Information | anomaly_detect | An operational process has been removed from the approved operations of Operations Behavior Anomaly Detection. | ID: %ID%<br><br>Target Process: %PATH% %ARGUMENT%<br><br>Parent Process 1: %PATH% %ARGUMENT%<br><br>Parent Process 2: %PATH% %ARGUMENT%<br><br>Parent Process 3: %PATH% %ARGUMENT%<br><br>Parent Process 4: %PATH% %ARGUMENT% |
| 784 | Information | anomaly_detect | DLL Injection Prevention has been enabled. | |
| 1280 | Information | device_control | Device Control has been enabled. | |
| 1281 | Information | device_control | Trusted USB device has been added. | Vendor ID: %HEX%<br><br>Product ID: %HEX%<br><br>Serial Number: %STRING%<br><br>Type: permanent or one time |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| 1282 | Information | device_control | Trusted USB device has been removed. | Vendor ID: %HEX% <br><br> Product ID: %HEX% <br><br> Serial Number: %STRING% |
| 1792 | Information | lockdown | File access has been allowed: %PATH% | Access Image Path: %PATH% <br><br> Access User: %USERNAME% <br><br> Mode: %MODE% <br><br> List: %LIST% |
| 1793 | Information | lockdown | A new file has been added to Approved List in Maintenance Mode. | Path: %PATH% <br><br> Hash: %SHA256_HEXSTR% |
| 1794 | Information | lockdown | The hash of an existing file in Approved List has been updated in Maintenance Mode. | Path: %PATH% <br><br> Hash: %SHA256_HEXSTR% |
| 1795 | Information | lockdown | Approved List initialization has started. | |
| 1796 | Information | lockdown | Approved List initialization has completed | Count: %COUNT% |
| 1797 | Information | lockdown | Application Lockdown has been enabled | Mode: %MODE% |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| 1798 | Information | lockdown | DLL/Driver Lockdown has been enabled. | |
| 1799 | Information | lockdown | Script Lockdown has been enabled. | |
| 1800 | Information | lockdown | Intelligent Runtime Learning has been enabled. | |
| 2048 | Information | update | Component update has started. | |
| 2049 | Information | update | Component update has ended. | |
| 2050 | Information | update | Scheduled component update has been enabled. Next update will be on %NEXT_UPDATE_LOCAL_TIME_STR% (agent's local system time). | |
| 2051 | Information | update | Scheduled component update has been disabled. | |
| 3840 | Information | misc | User account has been enabled. | |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| 3841 | Information | misc | User account has been disabled. | |
| 3842 | Information | misc | User password has been changed. | |
| 4352 | Warning | system | Service has stopped. | |
| 4353 | Warning | system | Unable to apply policy (Version: %version%) | |
| 4354 | Warning | system | Unable to update file. | Source Path: %src_path%<br><br>Destination Path: %dst_path%<br><br>Error Code: %err_code% |
| 4355 | Warning | system | Unable to apply patch. | File Name: %file_name%<br><br>Error Code: %err_code% |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| 4609 | Warning | intelli_av | Incoming Files Scanned, Action Taken by Antivirus: %PATH% | Incoming files were scanned by antivirus. Action was taken according to settings. File Path: %PATH% File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING% Action Result: %INTEGER% Quarantine Path: %PATH% |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| 4610 | Warning | intelli_av | Incoming Files Scanned, Action Taken by Next-Generation Antivirus: %PATH% | Incoming files were scanned by next-generation antivirus. Action was taken according to settings.<br><br>File Path: %PATH%<br><br>File Hash: %STRING%<br><br>Threat Type: %STRING%<br><br>Threat Name: %STRING%<br><br>Action Result: %INTEGER%<br><br>Quarantine Path: %PATH% |

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

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

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

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

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

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| 4880 | Warning | anomaly_detect | DLL Injection Prevention has been disabled. | |
| 5120 | Warning | change_control | Change to an ICS file was blocked by OT Application Safeguard. | Blocked Process: %PATH%<br><br>Target File: %PATH% |
| 5121 | Warning | change_control | Manipulation to existing ICS process was blocked by OT Application Safeguard. | Blocked Process: %PATH%<br><br>Target Process: %PATH% |
| 5376 | Warning | device_control | Device Control has been disabled. | |
| 5377 | Warning | device_control | USB access has been blocked: %PATH% | Access Image Path: %PATH%<br><br>Access User: %USERNAME%<br><br>Vendor ID: %HEX%<br><br>Product ID: %HEX%<br><br>Serial Number: %STRING% |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| 5888 | Warning | lockdown | File access has been allowed: %PATH% | Access Image Path: %PATH%<br><br>Access User: %USERNAME%<br><br>Mode: %MODE%<br><br>Reason: %ALLOWED_REASON%<br><br>File hash allowed: %SHA256_HEXSTR%<br>%THROTTLING_INFO_MSG% |
| 5889 | Warning | lockdown | File access has been blocked: C:\object_file_path | Access Image Path: %PATH%<br><br>Access User: %USERNAME%<br><br>Mode: %MODE%<br><br>Reason: %BLOCKED_REASON%<br><br>File hash blocked: %SHA256_HEXSTR%<br>%THROTTLING_INFO_MSG% |
| 5890 | Warning | lockdown | Unable to add to or update Approved List: %PATH% | |

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

## Server Event Log Descriptions for StellarProtect

This table lists the server event log descriptions for StellarProtect.

| Event ID | Event |
|---|---|
| 33027 | Switch agent (%s) to policy mode |
| 33028 | Switch agent (%s) to individual mode |
| 33029 | Deploy policy with version: %s |
| 33041 | Modify in common use (DLL Injection Prevention, Device Control, OT Application Safeguard, OBAD) setting for [%s] group policy with version: %s |
| 33042 | Modify real-time scan settings for [%s] group policywith version: %s |
| 33043 | Modify schedule scan settings for [%s] group policywith version: %s |
| 33044 | Maintain Device Control list for [%s] group policy with version: %s |
| 33045 | Maintain User-Defined Suspicious Object list for [%s] group policy with version: %s |
| 33046 | Maintain Operations Behavior Anomaly Detection Watch List for [%s] group policy with version: %s |
| 33047 | Maintain Trusted Certification list for [%s] group policy with version: %s |
| 33048 | Maintain OT Application Safeguard list for [%s] group policy with version: %s |
| 33049 | Modify agent password for [%s] group policy with version: %s |
| 33056 | Modify available patch setting for [%s] group policy with version: %s |
| 33057 | Maintain an authorized process for [%s] group policy with version: %s |
| 33058 | Modify schedule update settings for [%s] group policy with version: %s |
| 33059 | Modify lockdown config for [%s] group policy with version: %s |
| 33105 | Send individual command to agent (%s) |
| 33106 | Send protection command <Configure Maintenance Mode> to agents |
| 33107 | Send protection command <Scan Now> to agents |
| 33108 | Send update command <Update Agent Component> to agents |

| Event ID | Event |
|----------|-------|
| 33109 | Send update command <Deploy Agent Patches> to agents |
| 33110 | Send protection command <Initialize Lockdown Approved List> to agents |
| 33111 | Send update command <Check Connections> to agents |
| 33112 | Send update command <Apply Policies> to agents |
| 33121 | Apply event action to agent (%AGENT_NAME%) |
| 33122 | Apply event action <%ACTION_TYPE%> to agent(s) |
| 37122 | Set activation code with policy version: %s |
| 37123 | Active agents |
| 37124 | Inactive agents |

## Log Descriptions for StellarProtect (Legacy Mode)

Topics in this section include:

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

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

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

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| 1003 | Warning | System | Application Lockdown Turned Off | |
| 1004 | Information | System | Disabled | |
| 1005 | Information | System | Administrator password changed | |
| 1006 | Information | System | User password changed | |
| 1007 | Information | System | User account enabled | |
| 1008 | Information | System | User account disabled | |
| 1009 | Information | System | Product activated | |
| 1010 | Information | System | Product deactivated | |
| 1011 | Warning | System | License Expired. Grace period enabled. | |
| 1012 | Warning | System | License Expired. Grace period ended. | |
| 1013 | Information | System | Product configuration import started: %path% | |
| 1014 | Information | System | Product configuration import completed: %path% | |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| 1015 | Information | System | Product configuration exported to: %path% | |
| 1016 | Information | System | USB Malware Protection set to Allow | |
| 1017 | Information | System | USB Malware Protection set to Block | |
| 1018 | Information | System | USB Malware Protection enabled | |
| 1019 | Warning | System | USB Malware Protection disabled | |
| 1020 | Information | System | Network Virus Protection set to Allow | |
| 1021 | Information | System | Network Virus Protection set to Block | |
| 1022 | Information | System | Network Virus Protection enabled | |
| 1023 | Warning | System | Network Virus Protection disabled | |
| 1025 | Information | System | Memory Randomization enabled | |

| EVENT ID | LEVEL | CATEGORY | EVENT | DETAILS |
|----------|-------|----------|-------|---------|
| 1026 | Warning | System | Memory Randomization disabled | |
| 1027 | Information | System | API Hooking Prevention set to Allow | |
| 1028 | Information | System | API Hooking Prevention set to Block | |
| 1029 | Information | System | API Hooking Prevention enabled | |
| 1030 | Warning | System | API Hooking Prevention disabled | |
| 1031 | Information | System | DLL Injection Prevention set to Allow | |
| 1032 | Information | System | DLL Injection Prevention set to Block | |
| 1033 | Information | System | DLL Injection Prevention enabled | |
| 1034 | Warning | System | DLL Injection Prevention disabled | |
| 1035 | Information | System | Pre-defined Trusted Update enabled | |
| 1036 | Information | System | Pre-defined Trusted Update disabled | |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| 1037 | Information | System | DLL/Driver Lockdown enabled | |
| 1038 | Warning | System | DLL/Driver Lockdown disabled | |
| 1039 | Information | System | Script Lockdown enabled | |
| 1040 | Warning | System | Script Lockdown disabled | |
| 1041 | Information | System | Script added | File extension: %extension%<br><br>Interpreter: %interpreter% |
| 1042 | Information | System | Script removed | File extension: %extension%<br><br>Interpreter: %interpreter% |
| 1044 | Information | System | Exception path enabled | |
| 1045 | Information | System | Exception path disabled | |
| 1047 | Information | System | Trusted certificate enabled | |
| 1048 | Information | System | Trusted certificate disabled | |
| 1049 | Information | System | Write Protection enabled | |
| 1050 | Warning | System | Write Protection disabled | |

| Event ID | Level | Category | Event | Details |
|----------|-------|----------|-------|---------|
| 1051 | Information | System | Write Protection set to Allow | |
| 1052 | Information | System | Write Protection set to Block | |
| 1055 | Information | System | Added file to Write Protection List<br><br>Path: %path% | |
| 1056 | Information | System | Removed file from Write Protection List<br><br>Path: %path% | |
| 1057 | Information | System | Added file to Write Protection Exception List<br><br>Path: %path%<br><br>Process: %process% | |
| 1058 | Information | System | Removed file from Write Protection Exception List<br><br>Path: %path%<br><br>Process: %process% | |
| 1059 | Information | System | Added folder to Write Protection List<br><br>Path: %path%<br><br>Scope: %scope% | |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| 1060 | Information | System | Removed folder from Write Protection List<br><br>Path: %path%<br><br>Scope: %scope% | |
| 1061 | Information | System | Added folder to Write Protection Exception List<br><br>Path: %path%<br><br>Scope: %scope%<br><br>Process: %process% | |
| 1062 | Information | System | Removed folder from Write Protection Exception List<br><br>Path: %path%<br><br>Scope: %scope%<br><br>Process: %process% | |
| 1063 | Information | System | Added registry value to Write Protection List<br><br>Registry Key: %regkey%<br><br>Registry Value Name: %regvalue% | |
| 1064 | Information | System | Removed registry value from Write Protection List | |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
|  |  |  | Registry Key: %regkey% Registry Value Name: %regvalue% |  |
| 1065 | Information | System | Added registry value to Write Protection Exception List Registry Key: %regkey% Registry Value Name: %regvalue% Process: %process% |  |
| 1066 | Information | System | Removed registry value from Write Protection Exception List Registry Key: %regkey% Registry Value Name: %regvalue% Process: %process% |  |
| 1067 | Information | System | Added registry key to Write Protection List Path: %regkey% Scope: %scope% |  |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| 1068 | Information | System | Removed registry key from Write Protection List<br><br>Path: %regkey%<br><br>Scope: %scope% | |
| 1069 | Information | System | Added registry key to Write Protection Exception List<br><br>Path: %regkey%<br><br>Scope: %scope%<br><br>Process: %process% | |
| 1070 | Information | System | Removed registry key from Write Protection Exception List<br><br>Path: %regkey%<br><br>Scope: %scope%<br><br>Process: %process% | |
| 1071 | Information | System | Custom Action set to Ignore | |
| 1072 | Information | System | Custom Action set to Quarantine | |
| 1073 | Information | System | Custom Action set to Ask StellarOne | |
| 1074 | Information | System | Quarantined file is restored. | Original Location: %path%<br><br>Source: %source% |

| EVENT ID | LEVEL | CATEGORY | EVENT | DETAILS |
|---|---|---|---|---|
| 1075 | Information | System | Quarantined file is deleted. | Original Location: %path%<br><br>Source: %source% |
| 1076 | Information | System | Integrity Monitoring enabled | |
| 1077 | Information | System | Integrity Monitoring disabled | |
| 1078 | Information | System | Root cause analysis report unsuccessful | Access Image Path: %path% |
| 1079 | Information | System | Server certification imported: %path% | |
| 1080 | Information | System | Server certification exported: %path% | |
| 1081 | Information | System | Managed mode configuration imported: %path% | |
| 1082 | Information | System | Managed mode configuration exported: %path% | |
| 1083 | Information | System | Managed mode enabled | |
| 1084 | Information | System | Managed mode disabled | |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| 1085 | Information | System | Protection applied to Write Protection List and Approved List while Write Protection is enabled | |
| 1086 | Warning | System | Protection applied to Write Protection List while Write Protection is enabled. | |
| 1088 | Information | System | Windows Update Support enabled | |
| 1089 | Information | System | Windows Update Support disabled | |
| 1094 | Information | System | Applied a patch to agent by StellarOne<br><br>File applied: %file_name% | |
| 1096 | Information | System | Trusted hash enabled | |
| 1097 | Information | System | Trusted hash disabled | |
| 1099 | Information | System | Storage device access set to Allow | |
| 1100 | Information | System | Storage device access set to Block | |

| Event ID | Level | Category | Event | Details |
|----------|-------|----------|-------|---------|
| 1101 | Information | System | Storage device control enabled | |
| 1102 | Warning | System | Storage device control disabled | |
| 1103 | Information | System | Event Log settings changed | Windows Event Log: %ON\|off% |
| | | | | Level: Warning Log: %ON\|off% |
| | | | | Information Log: %ON\|off% |
| | | | | System Log: %ON\|off% |
| | | | | Exception Path Log: %ON\|off% |
| | | | | Write Protection Log: %ON\|off% |
| | | | | List Log: %ON\|off% |
| | | | | Approved Access Log: DllDriver Log: %ON\|off% |
| | | | | Trusted Updater Log: %ON\|off% |
| | | | | Exception Path Log: %ON\|off% |
| | | | | Trusted Certification Log: %ON\|off% |
| | | | | Trusted Hash Log: %ON\|off% |
| | | | | Write Protection Log: %ON\|off% |

| Event ID | Level | Category | Event | Details |
|----------|-------|----------|-------|---------|
| | | | | Blocked Access Log: %ON\|off% |
| | | | | USB Malware Protection Log: %ON\|off% |
| | | | | Execution Prevention Log: %ON\|off% |
| | | | | Network Virus Protection Log: %ON\|off% |
| | | | | Integrity Monitoring Log |
| | | | | File Created Log: %ON\|off% |
| | | | | File Modified Log: %ON\|off% |
| | | | | File Deleted Log: %ON\|off% |
| | | | | File Renamed Log: %ON\|off% |
| | | | | RegValue Modified Log: %ON\|off% |
| | | | | RegValue Deleted Log: %ON\|off% |
| | | | | RegKey Created Log: %ON\|off% |
| | | | | RegKey Deleted Log: %ON\|off% |
| | | | | RegKey Renamed Log: %ON\|off% |

| Event ID | Level | Category | Event | Details |
|----------|-------|----------|-------|---------|
| | | | | Device Control Log: %ON\|off% <br><br> Debug Log: %ON\|off% |
| 1104 | Warning | System | Memory Randomization is not available in this version of Windows. | |
| 1105 | Information | System | Blocked File Notification enabled | |
| 1106 | Information | System | Blocked File Notification disabled | |
| 1107 | Information | System | Administrator password changed remotely | |
| 1111 | Information | System | Fileless Attack Prevention enabled | |
| 1112 | Warning | System | Fileless Attack Prevention disabled | |
| 1500 | Information | List | Trusted Update started. | |
| 1501 | Information | List | Trusted Update stopped. | |
| 1502 | Information | List | Approved List import started: %path% | |

| Event ID | Level | Category | Event | Details |
|----------|-------|----------|-------|---------|
| 1503 | Information | List | Approved List import complete: %path% | |
| 1504 | Information | List | Approved List exported to: %path% | |
| 1505 | Information | List | Added to Approved List: %path% | |
| 1506 | Information | List | Added to Trusted Updater List: %path% | |
| 1507 | Information | List | Removed from Approved List: %path% | |
| 1508 | Information | List | Removed from Trusted Updater List: %path% | |
| 1509 | Information | List | Approved List updated: %path% | |
| 1510 | Information | List | Trusted Updater List updated: %path% | |
| 1511 | Warning | List | Unable to add to or update Approved List: %path% | |
| 1512 | Warning | List | Unable to add to or update Trusted Updater List: %path% | |

| EVENT ID | LEVEL | CATEGORY | EVENT | DETAILS |
|---|---|---|---|---|
| 1513 | Information | System | Added to Exception Path List | Type: %exceptionpathtype%<br><br>Path: %exceptionpath% |
| 1514 | Information | System | Removed from Exception Path List | Type: %exceptionpathtype%<br><br>Path: %exceptionpath% |
| 1515 | Information | System | Added to Trusted Certification List | Label: %label%<br><br>Hash: %hashvalue%<br><br>Type: %type%<br><br>Subject: %subject%<br><br>Issuer: %issuer% |
| 1516 | Information | System | Removed from Trusted Certification List | Label: %label%<br><br>Hash: %hashvalue%<br><br>Type: %type%<br><br>Subject: %subject%<br><br>Issuer: %issuer% |
| 1517 | Information | System | Added to Trusted Hash List.%n | Label : %label%<br><br>Hash : %hashvalue%<br><br>Type : %type% |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| | | | | Add to Approved List: %yes\|no% |
| | | | | Path : %path% |
| | | | | Note: %note% |
| 1518 | Information | System | Removed from Trusted Hash List.%n | Label : %label% |
| | | | | Hash : %hashvalue% |
| | | | | Type : %type% |
| | | | | Add to Approved List: %yes\|no% |
| | | | | Path : %path% |
| | | | | Note: %note% |
| 1519 | Information | List | Removed from Approved List remotely: %path% | |
| 1520 | Warning | List | Unable to create Approved List because an unexpected error occurred during enumeration of the files in %1 %n Error Code: %2 %n | |
| 1521 | Information | System | Added Fileless Attack Prevention exception | Label : %label% |
| | | | | Target Process: %process_name% |
| | | | | Arguments: %arguments% %regex_flag% |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| | | | | Parent Process 1 Image Path: %path% |
| | | | | Parent Process 2 Image Path: %path% |
| | | | | Parent Process 3 Image Path: %path% |
| | | | | Parent Process 4 Image Path: %path% |
| 1522 | Information | System | Removed Fileless Attack Prevention exception | Label : %label% |
| | | | | Target Process: %process_name% |
| | | | | Arguments: %arguments% %regex_flag% |
| | | | | Parent Process 1 Image Path: %path% |
| | | | | Parent Process 2 Image Path: %path% |
| | | | | Parent Process 3 Image Path: %path% |
| | | | | Parent Process 4 Image Path: %path% |
| 1523 | Information | System | Maintenance Mode started | |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| 1524 | Information | System | Leaving Maintenance Mode | |
| 1525 | Information | System | Maintenance Mode stopped | |
| 1526 | Information | List | Added to Approved List in Maintenance Mode<br><br>Path: %1<br><br>Hash: %2 | |
| 1527 | Information | List | Approved List updated in Maintenance Mode<br><br>Path: %1<br><br>Hash: %2 | |
| 2000 | Information | Access Approved | File access allowed: %path% | Access Image Path: %path%<br><br>Access User: %username%<br><br>Mode: %mode%<br><br>List: %list% |
| 2001 | Warning | Access Approved | File access allowed: %path% | Access Image Path: %path%<br><br>Access User: %username%<br><br>Mode: %mode%<br><br>File Hash allowed: %hash% |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| 2002 | Warning | Access Approved | File access allowed: %path% <br><br> Unable to get the file path while checking the Approved List | Access Image Path: %path% <br><br> Access User: %username% <br><br> Mode: %mode% |
| 2003 | Warning | Access Approved | File access allowed: %path% <br><br> Unable to calculate hash while checking the Approved List | Access Image Path: %path% <br><br> Access User: %username% <br><br> Mode: %mode% |
| 2004 | Warning | Access Approved | File access allowed: %path% <br><br> Unable to get notifications to monitor process | |
| 2005 | Warning | Access Approved | File access allowed: %path% <br><br> Unable to add process to non exception list | |
| 2006 | Information | Access Approved | File access allowed: %path% | Access Image Path: %path% <br><br> Access User: %username% <br><br> Mode: %mode% |
| 2007 | Warning | Access Approved | File access allowed: %path% <br><br> An error occurred while checking the Exception Path List | Access Image Path: %path% <br><br> Access User: %username% <br><br> Mode: %mode% |

| Event ID | Level | Category | Event | Details |
|----------|-------|----------|-------|---------|
| 2008 | Warning | Access Approved | File access allowed: %path%<br><br>An error occurred while checking the Trusted Certification List | Access Image Path: %path%<br><br>Access User: %username%<br><br>Mode: %mode% |
| 2011 | Information | Access Approved | Registry access allowed<br><br>Registry Key: %regkey%<br><br>Registry Value Name: %regvalue% | Access Image Path: %path%<br><br>Access User: %username%<br><br>Mode: %mode% |
| 2012 | Information | Access Approved | Registry access allowed<br><br>Registry Key: %regkey% | Access Image Path: %path%<br><br>Access User: %username%<br><br>Mode: %mode% |
| 2013 | Information | Access Approved | Change of File/Folder allowed by Exception List: %path% | Access Image Path: %path%<br><br>Access User: %username%<br><br>Mode: %mode% |
| 2015 | Information | Access Approved | Change of Registry Value allowed by Exception List<br><br>Registry Key: %regkey%<br><br>Registry Value Name: %regvalue% | Access Image Path: %path%<br><br>Access User: %username%<br><br>Mode: %mode% |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| 2016 | Information | Access Approved | Change of Registry Key allowed by Exception List<br><br>Registry Key: %regkey% | Access Image Path: %path%<br><br>Access User: %username%<br><br>Mode: %mode% |
| 2017 | Warning | Access Approved | Change of File/ Folder allowed: %path% | Access Image Path: %path%<br><br>Access User: %username%<br><br>Mode: %mode% |
| 2019 | Warning | Access Approved | Change of Registry Value allowed<br><br>Registry Key: %regkey%<br><br>Registry Value Name: %regvalue%  | Access Image Path: %path%<br><br>Access User: %username%<br><br>Mode: %mode% |
| 2020 | Warning | Access Approved | Change of Registry Key allowed<br><br>Registry Key: %regkey% | Access Image Path: %path%<br><br>Access User: %username%<br><br>Mode: %mode% |
| 2021 | Warning | Access Approved | File access allowed: %path%<br><br>An error occurred while checking the Trusted Hash List | Access Image Path: %path%<br><br>Access User: %username%<br><br>Mode: %mode% |
| 2022 | Warning | Access Approved | Process allowed by Fileless Attack | Access User: %username% |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| | | | Prevention: %path% %argument% | Parent Process 1 Image Path: %path% |
| | | | | Parent Process 2 Image Path: %path% |
| | | | | Parent Process 3 Image Path: %path% |
| | | | | Parent Process 4 Image Path: %path% |
| | | | | Mode: Unlocked |
| | | | | Reason: %reason% |
| 2503 | Warning | Access Blocked | Change of File/Folder blocked: %path% | Access Image Path: %path% |
| | | | | Access User: %username% |
| | | | | Mode: %mode% |
| 2505 | Warning | Access Blocked | Change of Registry Value blocked. Registry Key: %regkey% Registry Value Name: %regvalue% | Access Image Path: %path% |
| | | | | Access User: %username% |
| | | | | Mode: %mode% |
| 2506 | Warning | Access Blocked | Change of Registry Key blocked. Registry Key: %regkey% | Access Image Path: %path% |
| | | | | Access User: %username% |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| | | | | Mode: %mode% |
| 2507 | Information | Access Blocked | Action completed successfully: %path% | Action: %action%<br><br>Source: %source% |
| 2508 | Warning | Access Blocked | Unable to take specified action: %path% | Action: %action%<br><br>Source: %source% |
| 2509 | Warning | Access Blocked | File access blocked: %path% | Access Image Path: %path%<br><br>Access User: %username%<br><br>Mode: %mode%<br><br>Reason: Not in Approved List<br><br>File Hash blocked: %hash% |
| 2510 | Warning | Access Blocked | File access blocked: %path% | Access Image Path: %path%<br><br>Access User: %username%<br><br>Mode: %mode%<br><br>Reason: Hash does not match expected value<br><br>File Hash blocked: %hash% |
| 2511 | Information | Access Blocked | Change of File/Folder blocked: %path% | Access Image Path: %path%<br><br>Access User: %username% |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| | | | | Mode: %mode% |
| 2512 | Warning | Access Blocked | Change of Registry Value blocked.<br><br>Registry Key: %regkey%<br><br>Registry Value Name: %regvalue% | Access Image Path: %path%<br><br>Access User: %username%<br><br>---<br><br>**Note**<br>Enabling the Service Creation Prevention feature triggers Event ID 2512. |
| 2513 | Warning | Access Blocked | Process blocked by Fileless Attack Prevention: %path% %argument% | Access User: %username%<br><br>Parent Process 1 Image Path: %path%<br><br>Parent Process 2 Image Path: %path%<br><br>Parent Process 3 Image Path: %path%<br><br>Parent Process 4 Image Path: %path%<br><br>Mode: locked<br><br>Reason: %reason% |
| 2514 | Warning | Access Blocked | File access blocked: | Access Image Path: |

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

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| 3501 | Warning | Network Virus Protection | Network virus blocked: %name% | Protocol: TCP<br><br>Source IP Address: %ip_address%<br><br>Source Port: %port%<br><br>Destination IP Address: %ip_address%<br><br>Destination Port: 80 |
| 4000 | Warning | Process Protection Event | API Hooking/DLL Injection allowed: %path% | Threat Image Path: %path%<br><br>Threat User: %username% |
| 4001 | Warning | Process Protection Event | API Hooking/DLL Injection blocked: %path% | Threat Image Path: %path%<br><br>Threat User: %username% |
| 4002 | Warning | Process Protection Event | API Hooking allowed: %path% | Threat Image Path: %path%<br><br>Threat User: %username% |
| 4003 | Warning | Process Protection Event | API Hooking blocked: %path% | Threat Image Path: %path%<br><br>Threat User: %username% |
| 4004 | Warning | Process Protection Event | DLL Injection allowed: %path% | Threat Image Path: %path%<br><br>Threat User: %username% |

| EVENT ID | LEVEL | CATEGORY | EVENT | DETAILS |
|---|---|---|---|---|
| 4005 | Warning | Process Protection Event | DLL Injection blocked: %path% | Threat Image Path: %path%<br><br>Threat User: %username% |
| 4500 | Information | Changes in System | File/Folder created: %path% | Access Image Path: %path%<br><br>Access Process Id: %pid%<br><br>Access User: %username% |
| 4501 | Information | Changes in System | File modified: %path% | Access Image Path: %path%<br><br>Access Process Id: %pid%<br><br>Access User: %username% |
| 4502 | Information | Changes in System | File/Folder deleted: %path% | Access Image Path: %path%<br><br>Access Process Id: %pid%<br><br>Access User: %username% |
| 4503 | Information | Changes in System | File/Folder renamed: %path%<br><br>New Path: %path% | Access Image Path: %path%<br><br>Access Process Id: %pid%<br><br>Access User: %username% |
| 4504 | Information | Changes in System | Registry Value modified. | Access Image Path: %path% |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| | | | Registry Key: %regkey% | Access Process Id: %pid% |
| | | | Registry Value Name: %regvalue% | Access User: %username% |
| | | | Registry Value Type: %regvaluetype% | |
| 4505 | Information | Changes in System | Registry Value deleted. | Access Image Path: %path% |
| | | | Registry Key: %regkey% | Access Process Id: %pid% |
| | | | Registry Value Name: %regvalue% | Access User: %username% |
| 4506 | Information | Changes in System | Registry Key created. | Access Image Path: %path% |
| | | | Registry Key: %regkey% | Access Process Id: %pid% |
| | | | | Access User: %username% |
| 4507 | Information | Changes in System | Registry Key deleted. | Access Image Path: %path% |
| | | | Registry Key: %regkey% | Access Process Id: %pid% |
| | | | | Access User: %username% |
| 4508 | Information | Changes in System | Registry Key renamed. | Access Image Path: %path% |
| | | | Registry Key: %regkey% | Access Process Id: %pid% |

| Event ID | Level | Category | Event | Details |
|----------|-------|----------|-------|---------|
| | | | New Registry Key: %regkey% | Access User: %username% |
| 5000 | Warning | Device Control | Storage device access allowed: %PATH% | Access Image path: %PATH% |
| | | | | Access User: %USERNAME% |
| | | | | Device Type: %TYPE% %DEVICEINFO% |
| 5001 | Warning | Device Control | Storage device access blocked: %PATH% | Access Image path: %PATH% |
| | | | | Access User: %USERNAME% |
| | | | | Device Type: %TYPE% %DEVICEINFO% |
| 6000 | Information | System | %Result% | Update Source: %SERVER% |
| | | | | [Original Version] |
| | | | | Virus Pattern: %VERSION% |
| | | | | Spyware Pattern: %VERSION% |
| | | | | Digital Signature Pattern: %VERSION% |
| | | | | Program Inspection Pattern: %VERSION% |
| | | | | Damage Cleanup Template: %VERSION% |

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

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

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

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| | | | | Excluded files: %PATHS% |
| | | | | Excluded extensions: %PATHS% |
| | | | | [Components] |
| | | | | Virus Pattern: %VERSION% |
| | | | | Spyware Pattern: %VERSION% |
| | | | | Digital Signature Pattern: %VERSION% |
| | | | | Program Inspection Pattern: %VERSION% |
| | | | | Damage Cleanup Template: %VERSION% |
| | | | | Damage Cleanup Engine Configuration: %VERSION% |
| | | | | Virus Scan Engine: %VERSION% |
| | | | | Damage Cleanup Engine: %VERSION% |
| | | | | Scanner: %VERSION% |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| 6003 | Information | System | Malware scan completed: %SCAN_TYPE%. <br><br> Number of infected files: %NUM% | Files to scan: %SCAN_FOLDER_TYPE% <br><br> Scanned folders: %PATHS% <br><br> Excluded paths: %PATHS% <br><br> Excluded files: %PATHS% <br><br> Excluded extensions: %PATHS% <br><br> Start date/time: %DATE_TIME% <br><br> End date/time: %DATE_TIME% <br><br> Number of scanned files: %NUM% <br><br> Number of infected files: %NUM% <br><br> Number of cleaned files: %NUM% <br><br> Number of files cleaned after reboot: %NUM% <br><br> [Components] <br><br> Virus Pattern: %VERSION% <br><br> Spyware Pattern: %VERSION% |

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

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| | | | | Start date/time: %DATE_TIME% |
| | | | | End date/time: %DATE_TIME% |
| | | | | Number of scanned files: %NUM% |
| | | | | Number of infected files: %NUM% |
| | | | | Number of cleaned files: %NUM% |
| | | | | Number of files cleaned after reboot: %NUM% |
| | | | | [Components] |
| | | | | Virus Pattern: %VERSION% |
| | | | | Spyware Pattern: %VERSION% |
| | | | | Digital Signature Pattern: %VERSION% |
| | | | | Program Inspection Pattern: %VERSION% |
| | | | | Damage Cleanup Template: %VERSION% |
| | | | | Damage Cleanup Engine Configuration: %VERSION% |

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

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

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

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

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| | | | | Scanner: %VERSION% |
| 6009 | Warning | Maintenance Mode | Malware detected in Maintenance Mode: %PATH% | Component versions: Virus Pattern: %VERSION% |
| | | | | Spyware Pattern: %VERSION% |
| | | | | Digital Signature Pattern: %VERSION% |
| | | | | Program Inspection Pattern: %VERSION% |
| | | | | Damage Cleanup Template: %VERSION% |
| | | | | Damage Cleanup Engine Configuration: %VERSION% |
| | | | | Virus Scan Engine: %VERSION% |
| | | | | Damage Cleanup Engine: %VERSION% |
| | | | | Scanner: %VERSION% |
| 7000 | Information | System | Group policy applied | Old Group Name: %GROUP NAME% |
| | | | | Old Policy Version: %VERSION% |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| | | | | New Group Name: %GROUP NAME% |
| | | | | New Policy Version: %VERSION% |
| 7001 | Warning | System | Unable to synchronize group policy | Old Group Name: %GROUP NAME% |
| | | | | Old Policy Version: %VERSION% |
| | | | | New Group Name: %GROUP NAME% |
| | | | | New Policy Version: %VERSION% |
| | | | | Reason: %Reason% |
| 8000 | Information | System | Real Time Scan is enabled. | |
| 8001 | Warning | System | Real Time Scan is disabled. | |
| 8010 | Warning | System | Incoming files were scanned by antivirus. Action was taken according to settings. | File Path: %PATH% |
| | | | | File Hash: %HASH% |
| | | | | Threat Type: %TYPE% |
| | | | | Threat Name: %NAME% |
| | | | | Action Result: %INTEGER% |

| Event ID | Level | Category | Event | Details |
|---|---|---|---|---|
| | | | | Quarantine Path: %PATH% |
| 8011 | Warning | System | Application execution was blocked by antivirus. | Process Image Path: %PATH%<br><br>File Hash: %HASH%<br><br>Threat Type: %TYPE%<br><br>Threat Name: %NAME% |
| 8500 | Information | System | Scheduled component update has been enabled. Next update will be on %TIME% (agent's local system time). | |
| 8501 | Information | System | Scheduled component update has been disabled. | |

## Agent Error Code Descriptions for StellarProtect (Legacy Mode)

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

| Code | Description |
|---|---|
| 0x00040200 | Operation successful. |
| 0x80040201 | Operation unsuccessful. |
| 0x80040202 | Operation unsuccessful. |

| Code | Description |
|---|---|
| 0x00040202 | Operation partially successful. |
| 0x00040203 | Requested function not installed. |
| 0x80040203 | Requested function not supported. |
| 0x80040204 | Invalid argument. |
| 0x80040205 | Invalid status. |
| 0x80040206 | Out of memory. |
| 0x80040207 | Busy. Request ignored. |
| 0x00040208 | Retry. (Usually the result of a task taking too long) |
| 0x80040208 | System Reserved. (Not used) |
| 0x80040209 | The file path is too long. |
| 0x0004020a | System Reserved. (Not used) |
| 0x8004020b | System Reserved. (Not used) |
| 0x0004020c | System Reserved. (Not used) |
| 0x0004020d | System Reserved. (Not used) |
| 0x8004020d | System Reserved. (Not used) |
| 0x0004020e | Reboot required. |
| 0x8004020e | Reboot required for unexpected reason. |
| 0x0004020f | Allowed to perform task. |
| 0x8004020f | Permission denied. |
| 0x00040210 | System Reserved. (Not used) |
| 0x80040210 | Invalid or unexpected service mode. |
| 0x00040211 | System Reserved. (Not used) |

| Code | Description |
|---|---|
| 0x80040211 | Requested task not permitted in current status. Check license. |
| 0x00040212 | System Reserved. (Not used) |
| 0x00040213 | System Reserved. (Not used) |
| 0x80040213 | Passwords do not match. |
| 0x00040214 | System Reserved. (Not used) |
| 0x80040214 | System Reserved. (Not used) |
| 0x00040215 | Not found. |
| 0x80040215 | "Expected, but not found." |
| 0x80040216 | Authentication is locked. |
| 0x80040217 | Invalid password length. |
| 0x80040218 | Invalid characters in password. |
| 0x00040219 | Duplicate password. Administrator and Restricted User passwords cannot match. |
| 0x80040220 | System Reserved. (Not used) |
| 0x80040221 | System Reserved. (Not used) |
| 0x80040222 | System Reserved. (Not used) |
| 0x80040223 | File not found (as expected, and not an error). |
| 0x80040224 | System Reserved. (Not used) |
| 0x80040225 | System Reserved. (Not used) |
| 0x80040240 | Library not found. |
| 0x80040241 | Invalid library status or unexpected error in library function. |
| 0x80040260 | System Reserved. (Not used) |

| Code | Description |
|------|-------------|
| 0x80040261 | System Reserved. (Not used) |
| 0x80040262 | System Reserved. (Not used) |
| 0x80040263 | System Reserved. (Not used) |
| 0x80040264 | System Reserved. (Not used) |
| 0x00040265 | System Reserved. (Not used) |
| 0x80040265 | System Reserved. (Not used) |
| 0x80040270 | System Reserved. (Not used) |
| 0x80040271 | System Reserved. (Not used) |
| 0x80040272 | System Reserved. (Not used) |
| 0x80040273 | System Reserved. (Not used) |
| 0x80040274 | System Reserved. (Not used) |
| 0x80040275 | System Reserved. (Not used) |
| 0x80040280 | Invalid Activation Code. |
| 0x80040281 | Incorrect Activation Code format. |

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

This table lists the server event log descriptions for StellarProtect (Legacy Mode).

| ID | Server Event | Description |
|------|-------------|-------------|
| 1011 | Unable to send reports | Unable to send scheduled reports to %email_address%. |
| 1012 | Unable to send notifications | Unable to send notifications to %email_address%. |

| ID | Server Event | Description |
|---|---|---|
| 3001 | Purge agent event logs - automatic | Automatic purge of agent event logs. |
| 3002 | Purge agent event logs - manual | Manual purge of agent event logs. |
| 3004 | Purge server event logs - automatic | Automatic purge of server event logs. |
| 3005 | Purge server event logs - manual | Manual purge of server event logs. |
| 4001 | Take action on unapproved blocked file | Request sent to endpoint(s): Add blocked file to Approved List. <br><br> File name: %file_name% <br><br> File hash: %file_hash% (SHA-1) <br><br> Request sent to endpoint(s): Delete the blocked file. <br><br> File name: %file_name% <br><br> File hash: %file_hash% (SHA-1) <br><br> Request sent to endpoint(s): Ignore the blocked file. <br><br> File name: %file_name% <br><br> File hash: %file_hash% (SHA-1) <br><br> Request sent to endpoint(s): Quarantine the file. <br><br> File name: %file_name% <br><br> File hash: %file_hash% (SHA-1) <br><br> Request sent to endpoint(s): Restore the file from quarantine. <br><br> File name: %file_name% <br><br> File hash: %file_hash% (SHA-1) |

| ID | Server Event | Description |
|---|---|---|
| 4004 | Release the quarantined malicious file | Request sent to endpoint(s): Restore the file from quarantine.<br><br>File name: %file_name%<br><br>File hash: %file_hash% (SHA-1) |
| 4005 | Delete the quarantined malicious file | Request sent to endpoint(s): Delete the file from quarantine.<br><br>File name: %file_name%<br><br>File hash: %file_hash% (SHA-1) |
| 4006 | Take action on unapproved fileless attack | Request sent to endpoint(s): Add blocked process chain and command argument.<br><br>Process chain: %process_name%<br><br>Command argument: %parameter%<br><br>Request sent to endpoint(s): Ignore blocked process chain and command argument.<br><br>Process chain: %process_name%<br><br>Command argument: %parameter% |
| 5001 | Turn Application Lockdown on | Turned Application Lockdown on for endpoint(s). |
| 5002 | Turn Application Lockdown off | Turned Application Lockdown off for endpoint(s). |
| 5011 | Add trusted file hashes | Added 1 trusted file hash to endpoint(s).<br><br>Added %num% trusted file hashes to endpoint(s). |
| 5013 | Delete approved files | Removed specified items from the Approved List on endpoint(s) using SLtasks.exe. |
| 5021 | Block access from storage devices | Blocked access from storage devices on endpoint(s). |
| 5023 | Allow access from storage devices | Allowed access from storage devices on endpoint(s). |

| ID | SERVER EVENT | DESCRIPTION |
|---|---|---|
| 5025 | Add trusted USB device on selected endpoint(s) | Add trusted USB device on selected endpoint(s) |
| 5601 | Export agent settings | Exported (%file_desc%) from %endpoint_name%. |
| 5602 | Import agent settings | Imported (%file_desc%) to endpoint(s). |
| 5700 | Scan for malware | Scanned endpoint(s) for malware. |
| 5701 | Update agent components | Updated agent components on endpoint(s). |
| 5800 | Change agent administrator password | Changed password on endpoint(s). |
| 5900 | Update agent Approved List | Updated Approved List on endpoint(s). |
| 6001 | Deploy agent patch | Deploy agent patch to endpoint(s). Patch name: %patch_name% |
| 6101 | Agent transferred to new StellarOne server | Agent transferred to new StellarOne server |
| 6201 | Turn Maintenance Mode on | Turned Maintenance Mode on for endpoint(s). |
| 6202 | Turn Maintenance Mode off | Turned Maintenance Mode off for endpoint(s). |
| 6301 | Deploy group policy | Deploy group policy. Version: %version%. |
| 6401 | Set Intelligent Runtime Learning | Set Intelligent Runtime Learning. Version: %policy_version% |
| 6402 | Set Agent Password | Set Agent Password. Version: %policy_version% |

| ID | Server Event | Description |
|---|---|---|
| 6403 | Set Schedule Scan Setting | Set Schedule Scan Setting. Version: %policy_version% |
| 6404 | Set User-Defined Suspicious Objects | Set User-Defined Suspicious Objects. Version: %policy_version% |
| 6405 | Set Agent Patch | Set Agent Patch. Version: %policy_version% |

## Server Event Log Descriptions for StellarOne

This table lists the server event log descriptions for StellarOne.

| ID | Content |
|---|---|
| 45313 | Scan component update now |
| 45314 | Scan component [%s] update task started |
| 45315 | Enable scan component scheduled update |
| 45316 | Disable scan component scheduled update |
| 45317 | Modify scan component update source for StellarOne |
| 45318 | Modify scan component update source for agents |
| 45319 | Scan component [%s] update was successful |
| 45320 | Scan component [%s] update was successful but no duplicate is needed |
| 45321 | Scan component [%s] update failed with internal error |
| 45322 | Scan component [%s] update failed due to unable to connect to the network |
| 45323 | Customize policy |
| 45324 | Inherit policy from [%s] |

| ID | Content |
|---|---|
| 45325 | Scan component [%s] update failed due to <%s> |
| 45569 | Modify sync interval: [%s] Minutes |
| 45824 | Enable forwarding logs to Trend Micro Vision One |
| 45825 | Disable forwarding logs to Trend Micro Vision One |

# Syslog Content - CEF

The following section maps syslog content between StellarOne log output and CEF syslog types.

Topics in this section includes:

- *StellarProtect Agent Event Format on page A-72*

- *StellarProtect Server Event Format on page A-75*

- *StellarProtect (Legacy Mode) Agent/Server Event Format on page A-76*

- *StellarOne Server Event Format on page A-78*

## StellarProtect Agent Event Format

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

**TABLE A-1. StellarProtect Agent Event Format**

| CEF Field Name | Description | Possible Values |
|---|---|---|
| **Header** | | |
| CEF:Version | CEF format version | CEF:0 |
| Device Vendor | Device Vendor | TXOne Networks |

| CEF FIELD NAME | DESCRIPTION | POSSIBLE VALUES |
|---|---|---|
| Device Product | Device Product | StellarProtect |
| Device Version | Device Version | 2.0.1145 |
| Device Event Class ID | Event ID | {} |
| Name | Event category | Agent Event |
| Severity | LOG_CRIT: 2<br><br>LOG_WARNING: 4<br><br>LOG_INFO: 6 | {2, 4, 6} |
| **Extension** | | |
| eventTime | StellarProtect format | Apr 02 2022 13:31:51 GMT +00:00 |
| msg | <string> | |
| category | OPTION: 0<br><br>SYSTEM: 1<br><br>INTELLI_AV: 2<br><br>ANOMALY_DETECT: 3<br><br>CHANGE_CONTROL: 4<br><br>DEVICE_CONTROL: 5<br><br>MISC: 15 | |
| agentEndpoint | <string> | |
| agentIp | <string> | |
| agentLocation | <string> | |
| agentVendor | <string> | |
| agentModel | <string> | |
| agentOS | <string> | |

| CEF Field Name | Description | Possible Values |
|---|---|---|
| policyVersion | \<string\> | |
| detailMsg | \<string\> | |
| targetProcess | \<string\> | |
| fileHash | \<string\> | |
| threatType | \<string\> | |
| threatName | \<string\> | |
| filePath | \<string\> | |
| actionResult | \<int\> | |
| quarantinePath | \<string\> | |
| obadMode | \<string\> | |
| obadLevel | \<string\> | |
| accessUser | \<string\> | |
| processId | \<string\> | |
| parentProcess1 | \<string\> | |
| parentProcess2 | \<string\> | |
| parentProcess3 | \<string\> | |
| parentProcess4 | \<string\> | |
| targetArguments | \<string\> | |
| parentArguments1 | \<string\> | |
| parentArguments2 | \<string\> | |
| parentArguments3 | \<string\> | |
| parentArguments4 | \<string\> | |
| blockedProcess | \<string\> | |

| CEF Field Name | Description | Possible Values |
|---|---|---|
| targetFile | <string> | |
| vid | <int> | |
| pid | <int> | |
| sn | <string> | |
| accessImagePath | <string> | |
| srcPath | <string> | |
| dstPath | <string> | |
| errCode | <int> | |
| patchFileName | <string> | |
| filePath | <string> | |
| type | <string> | |

```
Time: Nov 22 04:00:07
IP: 10.8.145.45
Host:
Facility: local3
Priority: info
Tag: 2022-11-21T20:00:07Z 864c9868f43d Stellar[1]
Message: CEF:0|TXOne Networks|StellarProtect|2.0.1145|515|Agent Event|6|eventTime=Nov 21 2022 20:00:07 GMT+00:00 msg=Scheduled Scan Start
category=2 agentEndpoint=Z-W7X86T1CPSP1 agentIp=10.8.145.170 agentLocation=vC agentVendor=ZzZz agentModel=W7x86_testCrash agentOS=Windows 7
Ultimate Edition Service Pack 1 (build 7601), 32-bit desc=W7SP_remark serverIP=10.8.145.45
```

**FIGURE A-1. Example of StellarProtect Syslog Content**

## StellarProtect Server Event Format

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

**TABLE A-2. StellarProtect Server Event Format**

| CEF Field Name | Description | Possible Values |
|---|---|---|
| **Header** | | |

| CEF FIELD NAME | DESCRIPTION | POSSIBLE VALUES |
|---|---|---|
| CEF:Version | CEF format version | CEF:0 |
| Device Vendor | Device Vendor | TXOne Networks |
| Device Product | Device Product | StellarProtect |
| Device Version | Device Version | 2.2 |
| Device Event Class ID | Event ID | {} |
| Name | Event category | Server Event |
| Severity | LOG_INFO: 6 | {6} |
| **Extension** | | |
| eventTime | StellarProtect format | Apr 02 2023 13:31:51 GMT +00:00 |
| msg | <string> | |
| userName | <string> | |
| userRole | <string> | |
| clientIp | <string> | |

## StellarProtect (Legacy Mode) Agent/Server Event Format

Please refer to below table as StellarProtect (Legacy Mode) agent/server events in the Common Event Format.

**TABLE A-3. Agent Event Format**

| CEF KEY | DESCRIPTION | POSSIBLE VALUES / EXAMPLE |
|---|---|---|
| Header (logVer) | CEF format version | CEF:0 |
| Header (vendor) | Device Vendor | TXOne Networks |

| CEF Key | Description | Possible Values / Example |
|---------|-------------|---------------------------|
| Header (pname) | Device Product | StellarOne, StellarProtect (Legacy Mode) |
| Header (pver) | Device Version | 2.0.1145 |
| Header (eventid) | Device Event Class ID | 2509, 6005 |
| Header (eventName) | Name | Agent Event, Server Event, Console Log |
| Header (severity) | Severity | 4 |
| rt | Logged Time | Apr 02 2022 13:31:51 GMT +00:00 |
| msg | Event Id mapped message | File access blocked. File not found in Approved List |
| dvchost | Computer name | Localhost |
| dvc | IP address | 192.168.154.137 |
| cs1Label | Detailed Event Message | Detailed Event Message |
| cs1 | Event ID mapped detailed message | File access blocked: C:\\Documents and Settings\\Administrator\\Local Settings\\Temp\\isD5V0T.tmp\\is-H7K4O.tmp Malware detected: Quarantine. File path: C:\\eicar\\EICAR_TEST_FILE.exe |
| cs2Label | Client OS | Client OS |
| cs2 | OS description | Microsoft Windows 7 Enterprise Edition Service Pack 1 build 7601, 64-bit |
| cs3Label | Client Description | Client Description |
| cs3 | Description | - |

| CEF KEY | DESCRIPTION | POSSIBLE VALUES / EXAMPLE |
|---------|-------------|---------------------------|
| suser | Login User | PC1688\\Administrator |
| act | Action Type | ACTION_TYPE_BLOCKED |
| fileHash | SHA1 | 2201589AA3ED709B3665E4FF979E10C6AD5137F C |
| filePath | File path | C:\\Documents and Settings\\Administrator\\Local Settings\\Temp\\is-D5V0T.tmp\\is-H7K4O.tmp |
| fileCreateTime | File create time | 04 02 2022 14:00:21 |
| fileModificationTime | File modified time | 04 02 2022 14:00:21 |
| logGuid | Log GUID | : F43500BB-1F8A-4589-A292-144A9DA343AA、{56B7345A-B6D3-4BBB-A515-4AFFAE04092F} |
| ServerIP | Server IP | 10.8.145.157 |

```
Time: Nov 23 20:16:21
IP: 10.8.145.45
Host:
Facility: local3
Priority: warning
Tag: 2022-11-23T12:16:20Z StellarOne  [1]
Message: CEF:0|TXOne Networks |StellarProtect (Legacy Mode)|2.0.1145|2510|Agent Events|4|rt=Nov 23 2022 12:16:15 GMT+00:00 msg=File access blocked. File hash
does not match the expected value of the file with that path in Approved List dvchost=Z-W10IOT-2 dvc=10.8.145.10 logGuid={631219FB-E2C9-4CA2-
8643-38BADD044847} cs1Label=Detailed Event Message cs1=File access blocked: C:\\windows\\system32\\WINHTTP.dll cs2Label=Client OS cs2=Windows 10
build 19044, 64-bit cs3Label=Client Description cs3= suser=NT AUTHORITY\\NETWORK SERVICE act=ACTION_TYPE_BLOCKED
fileHash=091963d9538af4b2b9447180f95edae481f267e filePath=C:\\windows\\system32\\WINHTTP.dll fileCreateTime=10 12 2022 11:02:52
fileModificationTime=10 12 2022 11:02:52 serverIP=10.8.145.45
```

**FIGURE A-2. Example of StellarProtect (Legacy Mode) Syslog Content**

## StellarOne Server Event Format

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

**TABLE A-4. 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 | 2.2 |
| 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} |
| serverIP | StellarOne IP address | 10.8.145.123 |

# Index

www.**txone**.com