



1.2 TXOne StellarOne™ for StellarProtect

Patch 1

Administrator's Guide

All-terrain protection for mission critical assets

Windows

TXOne StellarOne[™] for StellarProtect

Administrator's Guide

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

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

© 2022 TXOne Networks Incorporated. All rights reserved. TXOne, and TXOne StellarOne are trademarks or registered trademarks of TXOne Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Document Part No.: APEM19539/220624
Release Date: June 2022
Protected by U.S. Patent No.: Patents pending.

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

Detailed information about how to use specific features within the product maybe available at the TXOne Online Help Center and/or the TXOne Knowledge Base.

TXOne always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any TXOne document, please contact us at

docs@trendmicro.com.

Evaluate this documentation on the following site:

<http://docs.trendmicro.com/en-us/survey.aspx>

Privacy and Personal Data Collection Disclosure

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

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

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

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

<https://www.trendmicro.com/privacy>

Table of Contents

Chapter 1	1
Introduction.....	1
About the TXOne™ Stellar™ series and StellarOne™	2
Agent Features and Benefits	3
What's New	4
Chapter 2	5
Agents.....	5
About the Agents Screen	6
Manage the Agent Tree.....	7
Add Groups.....	7
Rename Groups.....	8
Remove Groups / Unregister Agents	8
Search for Agents/Groups	9
Chapter 3	11
Policy Management.....	11
Manage Group/Agent Policy	12

Industrial-Grade Next-Generation Antivirus	13
Real-Time Scan	13
Schedule Scan	14
Advanced Options	17
Operations Behavior Anomaly Detection	20
DLL Injection Protection	22
OT Application Safeguard	22
Trusted Certificates	24
Device Control	26
Edit Trusted USB Devices	28
Remove Trusted USB Devices by Setting Policy	28
User-Defined Suspicious Objects	29
Agent Password	29
Patch	30
<i>Chapter 4</i>	32
Agent Protection	32
Configure Maintenance Mode	33
Scan Now	33
<i>Chapter 5</i>	35

Agent Update	35
Update Agent Components.....	36
Deploy Agent Patch.....	36
Chapter 6	37
Monitoring StellarProtect	37
About the Dashboard.....	38
Top Endpoints with Blocked Events	38
Top Blocked Files.....	40
CPU Usage	41
Memory Usage.....	42
Disk Usage	42
Add Widgets.....	43
Using Widgets.....	45
About the Agent Events Screen	48
Querying Agent Event Logs	50
Exporting Agent Events	51
About the Server Events Screen	52
Querying Server Event Logs.....	52
Exporting Server Event Logs	53
About the System Log Screen.....	54

Querying Server Logs.....	54
Exporting System Logs.....	55
About the Audit Log Screen.....	56
Querying Audit Logs	56
Exporting Audit Logs.....	59
Chapter 7	60
Administration	60
About the Account Management Screen	61
Server Accounts Overview.....	62
Adding Accounts.....	64
Edit Accounts.....	67
Delete Accounts	69
Single Sign-On.....	71
Resolving the SSO Issue.....	72
System Time	75
Date and Time	75
Time Zone.....	76
Syslog Forwarding.....	77
Agent event format.....	78
StellarProtect Server event format.....	81

StellarOne Server event format	82
Log Purge Settings	84
Purge Now	84
Automatic Purge	85
Notification Settings	86
Warning Level Agent Events.....	88
Outbreak.....	88
SMTP Settings	90
Proxy Settings	91
Download / Update Settings	94
Group Mapping	95
Firmware.....	97
SSL Certification.....	99
License Management.....	101
Changing Activation Code	102
<i>Chapter 8</i>	<i>104</i>
Log Description Reference	104
StellarProtect Agent Event Log Descriptions.....	105
StellarProtect Server Event Log Descriptions.....	111

StellarOne Server Event Log Descriptions	113
<i>Chapter 9</i>	114
Technical Support.....	114
Troubleshooting Resources	115
Using the Support Portal.....	116
Threat Encyclopedia.....	117
Contacting Trend Micro.....	118
Speeding Up the Support Call.....	119
Sending Suspicious Content to Trend Micro.....	120
Email Reputation Services	120
File Reputation Services	120
Web Reputation Services	120
Other Resources.....	121
Download Center.....	121
Documentation Feedback	121

Preface

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

Audience

TXOne StellarOne documentation is intended for users responsible for StellarOne management including agent installation, management, and the command line interface. Administrators are expected to have advanced networking and server management knowledge

Document Conventions

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

Table 1. Document Conventions

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

Terminology

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

Table 1. StellarOne Terminology

Terminology	Description
server	The StellarOne console server program
server endpoint	The host where the StellarOne server is installed
agents	The hosts running the StellarProtect program
NAT agents	The agents that are built under the routers with the Network Address Translation (NAT) function enabled
managed agents managed endpoints	The hosts running the StellarProtect program that are known to the StellarOne server program
target endpoints	The hosts where the StellarOne managed agents will be installed
Administrator (or StellarOne administrator)	The person managing the StellarOne server
Stellar console	The user interface for configuring and managing StellarOne settings and managed agents
CLI	Command Line Interface
license activation	Includes the type of StellarOne server installation and the allowed period of usage that you can use the application

Chapter 1

Introduction

This chapter introduces TXOne StellarOne and how it manages agents providing Industrial-Grade Next-Generation Antivirus protection to your assets. An overview of management functions is provided here.

About the TXOne[™] Stellar[™] series and StellarOne[™]

TXOne's Stellar series is a first-of-its-kind OT endpoint protection platform, allowing protection for modernized and legacy systems running side-by-side to be coordinated and maintained from the same management console, which includes:

- **StellarOne**[™], the ONE console for Stellar series products
- **StellarProtect**[™], the Industrial-Grade Next-Generation Antivirus
- **StellarEnforce**[™], for application lockdown with on-demand AV scan

Field devices in OT production can be categorized into modernized and legacy machines, with legacy machines making up the majority. On systems running legacy OSes, which are also likely to have limited computing resources, **StellarEnforce** is a perfect fit for ICS customers.

For the modern machines being brought into the OT environment more intelligence and flexibility are necessary! For this reason, TXOne Networks' engineers developed a new ICS endpoint protection platform, **StellarProtect**. **StellarProtect** & **StellarEnforce** work in concert to provide comprehensive endpoint protection for ICS assets, managed from the **StellarOne** console.

Agent Features and Benefits

TXOne™ StellarOne™ includes the following features and benefits.

Table 2-1. Features and Benefits

Feature	Benefit
Dashboard	StellarOne provides a configurable dashboard from which customers can get real-time StellarProtect information, including the endpoints with the most blocked events, top blocked files, CPU usage, memory usage, and disk usage.
Device Management	When the device installs StellarProtect it will register to StellarOne automatically. These agents will be managed by StellarOne, and you can add a group or groups to manage agents as well as configure them with individual or group-based policies.
Events/Logs Management	StellarOne has 4 types of events and logs, which provide users with analysis and management functions. Using the notification function, administrators and auditors can query and analyze events to quickly find the root cause of the problem.
Administration Management	StellarOne supports several functions specifically for managing endpoints running StellarProtect: 1. Account Management 2. Single Sign-On 3. System Time 4. Proxy 5. Downloads / Updates 6. SSL Certification 7. License 8. Log Purge 9. Firmware

What's New

TXOne StellarOne 1.2 Patch 1 includes the following new features and enhancements.

Table 2-2. What's New in TXOne StellarOne 1.2 Patch 1

Feature	Description
Group Mapping	User can register StellarProtect agent to a specific group directly via StellarOne web console.

Chapter 2

Agents

This chapter introduces how to manage StellarProtect agents through StellarOne.

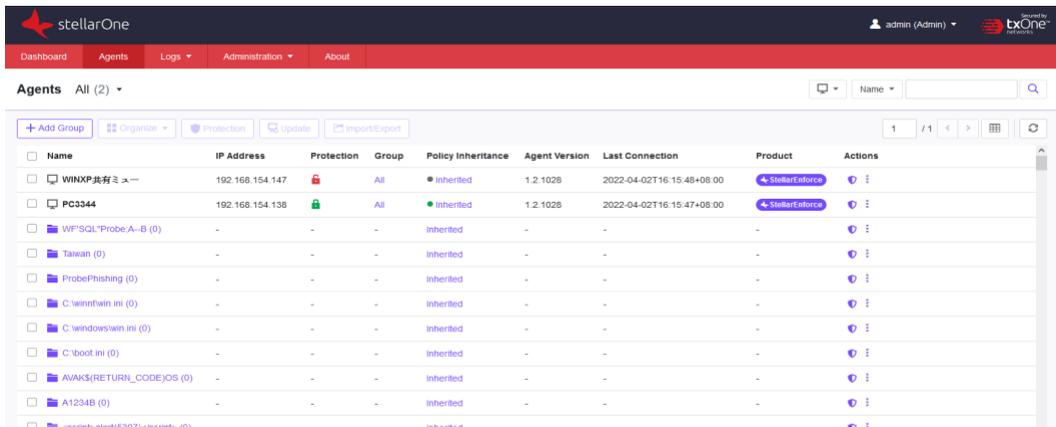
About the Agents Screen

To display the Agents screen, go to **Agents** in the navigation at the top of the web console. This screen displays a list of agents managed by StellarOne console and allows you to perform configuration tasks.



Note:

All agents are under the All group by default.  icon indicates a group and  icon indicates an agent.



Name	IP Address	Protection	Group	Policy Inheritance	Agent Version	Last Connection	Product	Actions
 WINXP共有ミュー	192.168.154.147		All	● inherited	1.2.1028	2022-04-02T16:15:48+08:00	StellarEnforce	 
 PC3344	192.168.154.138		All	● inherited	1.2.1028	2022-04-02T16:15:47+08:00	StellarEnforce	 
 WPFSQL*ProbeA-B (0)	-	-	-	● inherited	-	-	-	 
 Taiwan (0)	-	-	-	● inherited	-	-	-	 
 ProbePhishing (0)	-	-	-	● inherited	-	-	-	 
 C:\winnt\win.ini (0)	-	-	-	● inherited	-	-	-	 
 C:\windows\win.ini (0)	-	-	-	● inherited	-	-	-	 
 C:\boot.ini (0)	-	-	-	● inherited	-	-	-	 
 AVAKS(RETURN_CODE)OS (0)	-	-	-	● inherited	-	-	-	 
 A1234B (0)	-	-	-	● inherited	-	-	-	 
 %script>alert(3073)&crnet% (0)	-	-	-	● inherited	-	-	-	 

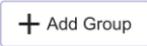
Manage the Agent Tree

StellarOne allows you to organize the agent tree and manage StellarProtect agent information.

Task	Detail
Add agent groups	Create groups according to location, type, or purpose to help you manage multiple agents.
Reorganize agent groups	Reorganize groups. (Suggested to add the section about the task.)
Rename agent groups	Change the names of groups.
Remove agent groups/ Unregister agents	Remove groups or unregister agents from the StellarOne console.
Search for agents or groups	Search for agents/groups with additional search criteria.

Add Groups

Procedure

1. Go to **Agents** in the navigation at the top of the web console. The Agents screen will appear.
2. Start from the **All** group on the **Agent view**.
3. Click the group name to navigate to a target parent group to create a new group.
4. Click  button on the above control area.
5. The **Add Group** window will appear.

Input the group name and select **Confirm**



Note:

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

Rename Groups

Procedure

1. Go to **Agents** in the navigation at the top of the web console. The Agents screen will appear.
2. Select the target group you want to rename.
3. Click  , **More** icon of **Actions** and click **Rename**.
4. The **Rename Group** window will appear.
5. Input the new name you want to use and click **Confirm**.



Note:

The group name cannot be the same as the same level.

Remove Groups / Unregister Agents

Procedure

1. Go to **Agents** in the navigation at the top of the web console. The Agents screen will appear.
2. Select the target groups you want to remove or the agents you want to unregister.
3. Click  , **More** icon of **Actions** and click **Remove**.
4. The **Remove Items** confirmation window will appear.
5. Click **Confirm** that you want to remove the group or unregister the agent.


Note:

If the target group is not empty (with any groups or assets), it cannot be removed.

Search for Agents/Groups

Procedure

1. Go to **Agents** in the navigation at the top of the web console. The Agents screen will appear.
2. Search for specific endpoints by selecting criteria from the drop-down list and specify additional search criteria as required.

Option	Description
Agent	The name of the agent. Type the full or partial endpoint host name to locate the specific agent.
IP Address	Type the IPv4 address.
IP Range	Type the IPv4 address range.
Group	The name of the group. Select the available group.
Policy Inheritance	The mode of Policy Inheritance. Select Inherited or Customized .
Policy Deployment	The status of policy deployment from StellarOne to Agents. Select Completed or In Progress .
Agent Version	Type the Agent Version.
Last Connection	Last connection time. Select the default time range or select Custom to specify your own range. Default time range: <ul style="list-style-type: none"> • Last 1 hour

Option	Description
	<ul style="list-style-type: none">• Last 24 hours• Last 7 days• Last 30 days
Product	Select StellarEnforce or StellarProtect .
Operating System	Select an operating system.
Description	Type the full or partial description to query specific endpoints.

Chapter 3

Policy Management

This chapter introduces how to manage StellarProtect agents with policy.

Manage Group/Agent Policy

- The user can add the group with agents, and then *inherit* **Group Policy** from the parent group or *customize* its own Group Policy.
- The agent can also have its own customized **Agent Policy** instead of inheriting from the parent group.
- The user can switch the product (StellarProtect or StellarEnforce) to display its **Policy** and **General Info**.

Agent	IP Address	Protect...	Policy	Agent ...	Operating System	Last Connection	Product	Actions
<input type="checkbox"/> PC3344	192.168.154.138		● Customized	1.2.1014	Windows 7 Professional Service Pack 1 build 7...	2022-02-24T16:3...	← StellarEnforce	
<input type="checkbox"/> PC2008	192.168.68.129		● Inherited	1.2.1064	Windows Server 2008 R2 Enterprise Edition (b...	2022-02-24T13:2...	← StellarProtect	
<input type="checkbox"/> PC2003	192.168.154.145		● Inherited	1.1.1014	Windows Server 2003 R2, Enterprise Edition S...	2022-02-24T16:3...	← StellarEnforce	

← Taoyuan (3)

Product

Policy Inheritance Inherit from parent group: Taiwan

← PC2003

← StellarEnforce

Policy Inheritance Inherit from parent group: Taoyuan

Industrial-Grade Next-Generation Antivirus

The industrial-grade next-generation antivirus settings include 'Real-Time Scan' and 'Schedule Scan'. The settings are as follows:

Industrial-Grade Next-Generation Antivirus

ICS root of trust and advanced threat scan secure the assets while no interruption on the operations.

Real-time malware scanning
 Advanced Threat Scan

> [Advanced Options](#)

Schedule Scan 

> [Advanced Options](#)

Real-Time Scan

Real-time Scan is a persistent and ongoing scan. Each time a file is received, opened, downloaded, copied, or modified, Real-time Scan scans the file for security risks. If the Security Agent does not detect a security risk, users can proceed to access the file. If the Security Agent detects a security risk or a probable virus/malware, a notification message displays indicating the name of the infected file and the specific security risk.

Real-time Scan maintains a persistent scan cache which reloads each time the Security Agent starts. The Security Agent tracks any changes to files or folders that occurred since the Security Agent unloaded and removes these files from the cache.

Predictive Machine Learning

Predictive Machine Learning uses advanced machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks through digital DNA fingerprinting, API mapping, and other file features. 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 environment from unidentified threats and zero-day attacks.

Industrial-Grade Next-Generation Antivirus

ICS root of trust and advanced threat scan secure the assets while no interruption on the operations.

Real-time malware scanning
 Advanced Threat Scan

> [Advanced Options](#)

Schedule Scan

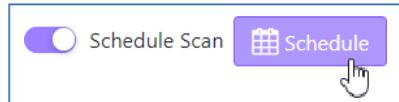
> [Advanced Options](#)

Important

Advanced Threat Scan is configured to support all scan types, including scheduledscans.

Schedule Scan

If you want to set an antivirus scan schedule, click 'Schedule Scan', and then click the 'Schedule' icon to set the date and time.



The schedule settings are as follows:

- Frequency
 - Daily
 - Weekly, and choose a day from Monday to Sunday
 - Monthly, and choose a day of the month (keeping in mind that for monthly scanning to proceed each month that day must exist in every month, for example scanning set to take place on the 30th would not proceed in February)
- Start time
 - Set the hour and minutes

Schedule ✕

Frequency: Daily
 Weekly, every Sunday ▾
 Monthly, on day 01 ▾

Start time: 04 ▾ : 00 ▾

Confirm Cancel

Advanced Options

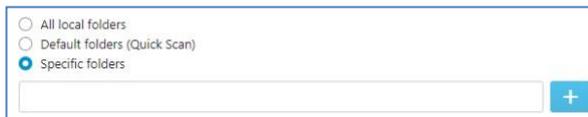
You can configure the following settings for industrial-grade next-generation antivirus under 'advanced options':

- Files to Scan

You can choose one of the following scopes to adjust for scan targeting:

- All local folders
- Default folders for quick scan
- Specific folders

If you select "Specific folders", then you can add a folder list by clicking the '+'.



The image shows a configuration window for 'Files to Scan'. It contains three radio button options: 'All local folders', 'Default folders (Quick Scan)', and 'Specific folders'. The 'Specific folders' option is selected. Below the options is a text input field and a blue '+' button.

You can enable 'scan removable drives' when you need the endpoint to scan connected external storage devices.

The 'Scan compressed files. Maximum layers:' setting allows multiple layers of compressed files to be scanned, providing better scan coverage.

Scanning large files might cause performance issues, so you can configure the file size limit to skip files over a certain size.

Files to Scan	
<input checked="" type="checkbox"/>	Scan compressed files. Maximum layers: <input type="text" value="1"/> ▼
<input checked="" type="checkbox"/>	Skip files larger than <input type="text" value="30"/> MB (1-9999)

Scan Action	
<input checked="" type="radio"/>	Quarantine
<input type="radio"/>	No action

If threats are detected in any file, you will be prompted to choose a scan action.

You can choose an action as follows:

- Quarantine
- No action

You also can choose some folders or files with config file extensions. StellarProtect will skip these folders and files to meet OT environment requirements.

Scan Exclusions

Exclusion can be configured for Realtime scan and Schedule scan: you can add multiple folders, files and file extensions for excluding in scan.

Exclusion folder will include its subfolders. For example, **C:\Windows** will also exclude all folder/files in **C:\Windows\Temp** and other folders. In short, it excludes all files/folders inside **C:\Windows**

Wildcard is not necessary for all exclusions, input your desired setting is enough.

File extension exclusions: don't need "." Or "*" In front of the file extension.

Currently, remote path exclusions are not supportable. For example, **Error! Hyperlink reference not valid.** nor `\\[Hostname]` are not supportable yet.

Operations Behavior Anomaly Detection

As fileless attacks can cause serious damage, StellarProtect provide 'Operations Behavior Anomaly Detection' to prevent such attacks.

Operation Behavior Anomaly Detection

- Learn: Add unrecognized calls from monitored operations and processes to the Approved List
- Detect: Create a log of unrecognized calls from monitored operations and processes
- Enforce: Block unrecognized calls from monitored operations and processes
- Disable

Aggressive Mode
StellarProtect will apply policies more strenuously to the actions of applications.

[Watchlist \(0\)](#)
Manually add commonly-abused applications to the Watchlist for monitoring cyber threats.

Learn Mode

After activating this function, StellarProtect will monitor unrecognized program calls and add them to the approved list to learn more about ICS-related program call behaviors.

Detect Mode

After activating this function, StellarProtect will monitor unrecognized program calls and log them for future analysis.

Enforce Mode

After activating this function, StellarProtect will monitor unrecognized program calls and block them to secure the endpoint.

Disable

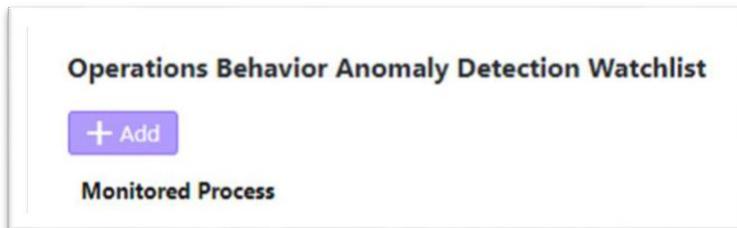
When Operations Behavior Anomaly Detection is set to Disable, protection is turned off.

The Operations Behavior Anomaly Detection function additionally has an **Aggressive Mode**, and can activate protection through process parameter recognition.

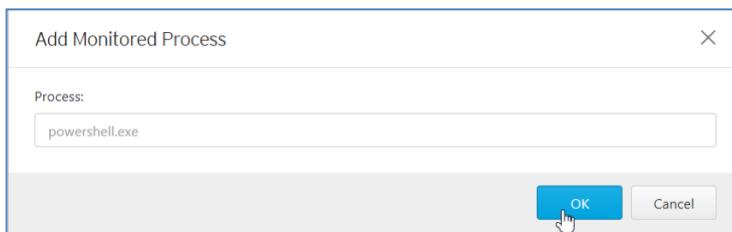
Users can check the process and parameters under monitoring.

Watchlist / Monitored Processes

You can add more processes to be monitored. StellarProtect will monitor **Powershell.exe**, **wscript.exe**, **cscript.exe**, **mshta.exe**, and **psexec.exe** by default.

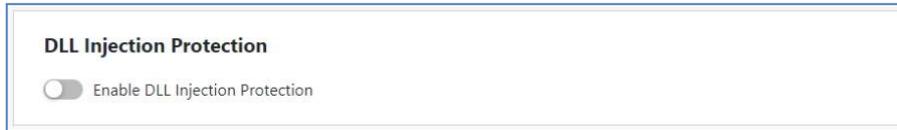


Please input the process name and click 'OK' to confirm.



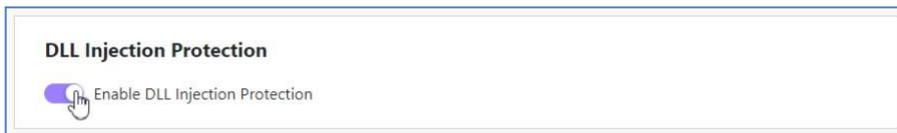
DLL Injection Protection

DLL injection prevention is an important and well-known form of endpoint security.



Block DLL Injection

To enable this protection, click 'Enable DLL Injection Protection'.



OT Application Safeguard

OT Application Safeguard is industrial-based change control protection.

Users can enable this protection to make sure StellarProtect-recognized ICS applications can be updated without being blocked or restricted.

In addition, you can enable ICS application protection to secure recognized ICS application executable binary files.

Basically, StellarProtect will auto-detect currently-installed OT/ICS application and put them under protection. Note that OT/ICS application showing in **General info tab**, this indicates StellarProtect recognizes this application.

For newly-installed OT/ICS applications, be sure to enable “Maintenance Mode” before installing the new application. After the installation process is completed, disable the Maintenance mode and then it will auto re-scan OT/ICS applications. If any new applications are found, they will be added into the OT/ICS Application Safeguard list.

If your OT/ICS application doesn’t show, the administrator can manually add **installation path** for the application under Safeguard’s protection.

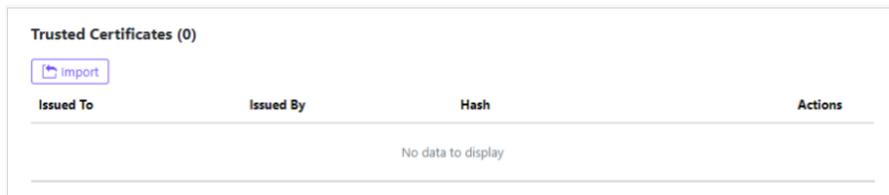
In OT/ICS Application Safeguard policy setting pane, click File/Folders. Then manually add application installation path. The default is to protect this folder/subfolder PE file (.exe & .dll), if you want to protect all files inside this folder, there is also have one option “**Executable file only**” can be disabled to protect **all files** inside this folder. Administrator can also protect their secret files/configurations or other files from being modified with the untrusted applications.

Administrator can also set other application to be the trusted application to modify the protected file by adding the Authorized process. However, please note that if any malicious file has been set into the Authorized process, Stellar Protect cannot prevent this file from modifying OT/ICS application since it is already become excluded from the StellarProtect’s monitor process. Make sure this process is safe before adding the Authorized Process.

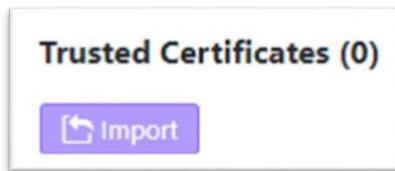
Trusted Certificates

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

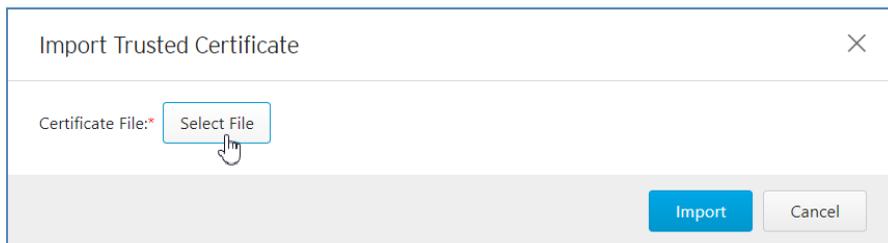
Process with trusted certificate can modify / update / change Protected file/folders.



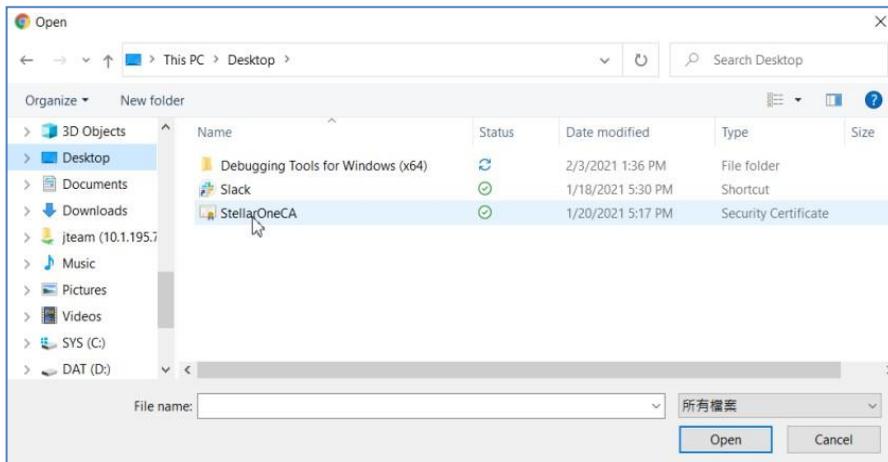
Click the 'Import' icon to import a new trusted certificate.



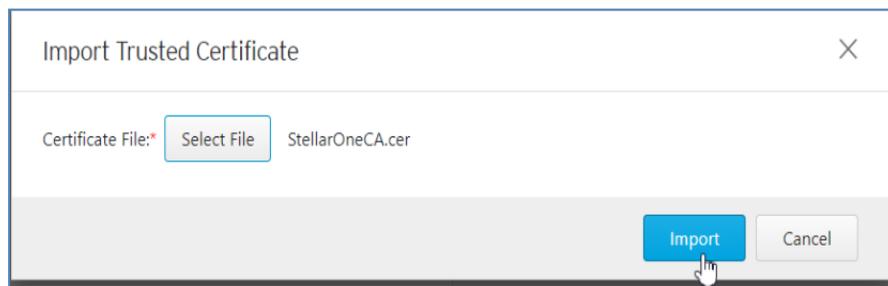
Click 'Select File' to browse certificate files.



Select the specific certificate file.



Then click the 'Import' button to finish the function.



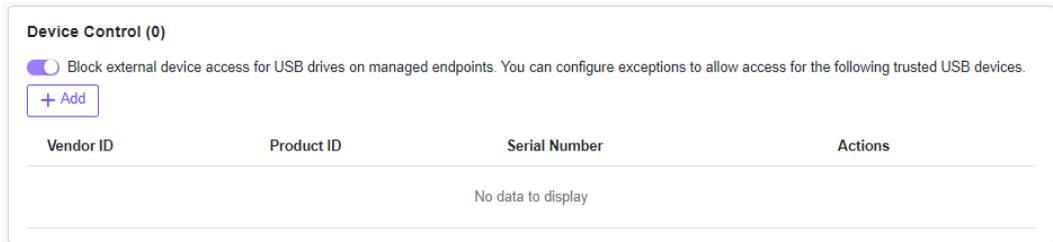
You can have an updated certificate list here.

Trusted Certificates (1)			
Issued To	Issued By	Hash	Actions
MyCompany	MyCompany	2ff3ec80c78387e90632b80a940f317fc8907247	

Device Control

USB vector control is one of the foundations of endpoint protection, by which StellarProtect supports USB storage device access control.

In StellarProtect agent side, when USB device control been enabled, every time plug-in USB device, will prompt one dialog to confirm if admin really want to access this device. But the confirm will need check every time, only add the USB info into this list, will make this device always can directly access without check.



You can add specific drivers to the approved list.

StellarProtect supports VID (Vendor ID), PID (Product ID), and SN (Serial Number) as conditions for USB vector control approval, and the administrator can choose one, two, or all to be used.

Please click 'Add' to add a new device.



You can input one or all of VID, PID and SN.

Add Trusted USB Device ✕

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

Vendor ID:

Product ID:

Serial number:

Note: You can use one of the following methods to get the information of a connected device to an endpoint:
 (1) Open the Device Manager on the agent endpoint
 (2) Use `opcmd.exe -p usb info -d <drive_letter>` command on the agent endpoint

You can check the updated USB vector list to confirm that the vector was added successfully.

Device Control (1)

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

<input type="checkbox"/>	Vendor ID	Product ID	Serial Number	Actions
<input type="checkbox"/>	4C5	1526	11f79522	

Edit Trusted USB Devices

Procedure

1. Find the **Device Control** pane in the **Policy view**.
2. Click the **Toggle Switch** to enable “Block external device access for USB drives on managed endpoints. You can configure exceptions to allow access for the following trusted USB devices”. The **Trusted USB Device List** will appear.
3. Select the Trusted USB Device you want to edit.
4. Click the **Edit** button and the dialog window will appear.
5. Click the **Confirm** button and the settings will be saved.

Remove Trusted USB Devices by Setting Policy

Procedure

1. Find the **Device Control** pane in the **Policy view**.
2. Click the **Toggle Switch** to enable “Block external device access for USB drives on managed endpoints. You can configure exceptions to allow access for the following trusted USB devices”. The **Trusted USB Device List** will appear.
3. Select the Trusted USB Device you want to delete.
4. Click the **Delete** button and the **Remove Trusted USB Device** dialog window will appear.
5. Click the **Confirm** button and the settings will be saved.

User-Defined Suspicious Objects

Sometimes we can receive new IOC (Indicators Of Compromise), including file hash (SHA-1 or SHA-2) or path. You can add them and make sure all managed endpoints are free of these infected files.

If there have new threat want to block, can set the file hash into User-Defined suspicious object to block file been executed.

User-Defined Suspicious Objects

Protect against objects not yet on your network:

[+ Add](#)

Hash / File Path	Type	Notes	Actions
No data to display			

Agent Password

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

Agent Password

New Password*

Please input your new password twice and click 'Save' to finish policy setting.

Agent Password

New Password*

Re-type Password*

Password Policy

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

Patch

The **Patch** function allows the administrator to upgrade all agents under the same group policy to upgrade to a new version. The patching process will be conducted remotely and automatically using policy sync.

Only one patch (Agent version) is allowed under each unit policy.



Note:

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

1. Global policy is the default agent landing policy, so every agent will apply this policy first before moving to other groups. We suggest that the global policy should use lower agent version as its base policy.
2. If you don't want to set any agent version to be patched, please remember to clear all checkboxes in 'agent version' under the Patch function.



Important

StellarProtect Agent 1.0 does not support Remote Patch, as it does not have any available remote patches.

Chapter 4

Agent Protection

This chapter introduces how to manage StellarProtect Protection feature command.

Configure Maintenance Mode

The maintenance mode is necessary for changes in OT endpoint operations. During the Maintenance mode, all newly-added files will be updated through real-time virus scanning. Thus, StellarProtect can learn the newly-added applications and ensure the execution of these newly-added applications under the protected conditions. The user should perform the necessary application updates before the Change Window reaches its assigned time to close. Please note that StellarProtect will still prevent malware infection during the Change Window.

Scan Now

You can initiate ‘Scan Now’ through the StellarOne console and can target one or several StellarProtect agent endpoints.

Procedure

1. Go to **Agents** in the navigation at the top of the StellarOne console.
2. Select one or more entries and then click **Protection > Scan Now**.
3. When the confirmation screen appears, confirm your settings and then click **OK**.
 - a. To scan compressed files, check **Scan compressed files** and choose the desired number of layers.
 - b. To skip files larger than a certain size, check **Skip files larger**

than and specify the size at which files should be skipped.

- c. To scan with no trust rules, scanning everything with current viruspatterns, check **Aggressive scan**.

The server will send a notification to the selected StellarProtect agents.

You can check the logs for the scan status.

Chapter 5

Agent Update

This chapter introduces how to update StellarProtect scan component and agent itself.

Update Agent Components

You can start the agent component update process on selected endpoints from StellarOne. The agent will then download the latest component updates.

Update agent components regularly to protect endpoints from the latest security risks.

Procedure

1. Go to **Agents > StellarProtect** in the navigation at the top of the webconsole. The Agents screen will appear.
2. Select one or more endpoints.
3. Select **Protection > Update Agent Components**.
4. Click **OK**.

Deploy Agent Patch

You can update agents directly from the web console page by using StellarOne to deploy an uploaded patch file to selected StellarProtect agents.

Procedure

1. Go to **Agents > StellarProtect**. The Agents screen will appear.
2. Select one or more agents.
3. Click **Update > Deploy Agent Patch**.
4. Select the available patch file for deployment.
5. Click **OK**.

Chapter 6

Monitoring StellarProtect

This chapter introduces TXOne StellarOne monitoring feature.

About the Dashboard

Monitor events from the Dashboard using the overview provided under the Summary tab. This tab is added to the Dashboard by default when there are no user-defined tabs.

Default widgets included in the **Summary** and **System** tabs with Blocked Event History, Top Endpoints with Blocked Events, CPU Usage, Memory Usage, and Disk Usage.

Top Endpoints with Blocked Events

This widget displays the endpoints with the most blocked events. By default, the widget is displayed on the Event Overview tab of the Dashboard.

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

StellarProtect Top Endpoints with Blocked Events

Time Period: Last 7 days

Endpoint Name	Description	IP Address	Blocked Events
TC	-	192.168.15.138	1

Use the Time Period drop-down to display only the event data for the period specified. To specify the number of events to display, open the Widget Settings dialog, then select a different value for Events to display.

Top Blocked Files

This widget displays a list of files that triggered the most blocked events, and it will NOT be listed in the Dashboard by default.

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	Number of endpoints which reported a blocked event for the file
Blocked Events	Total number of blocked events reported for the file

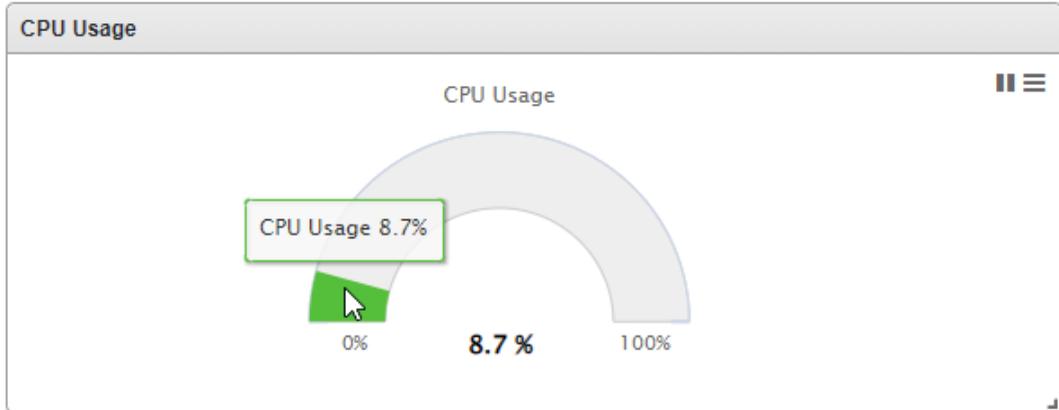
StellarProtect Top Blocked Files

Time Period: Last 7 days ☰

File Name	File Hash	Endpoints	Blocked Events
C:\test\eicar\eicar.com	275a021bbfb6489e54d471899f	1	1

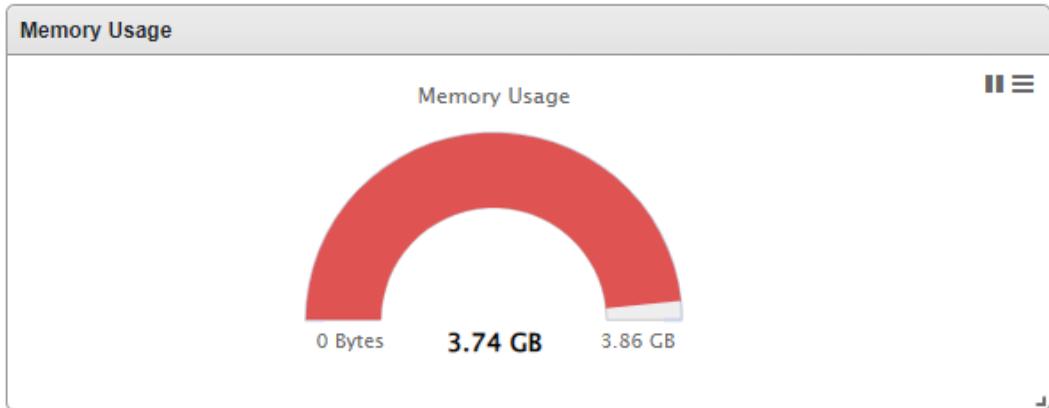
CPU Usage

This widget displays CPU usage information.



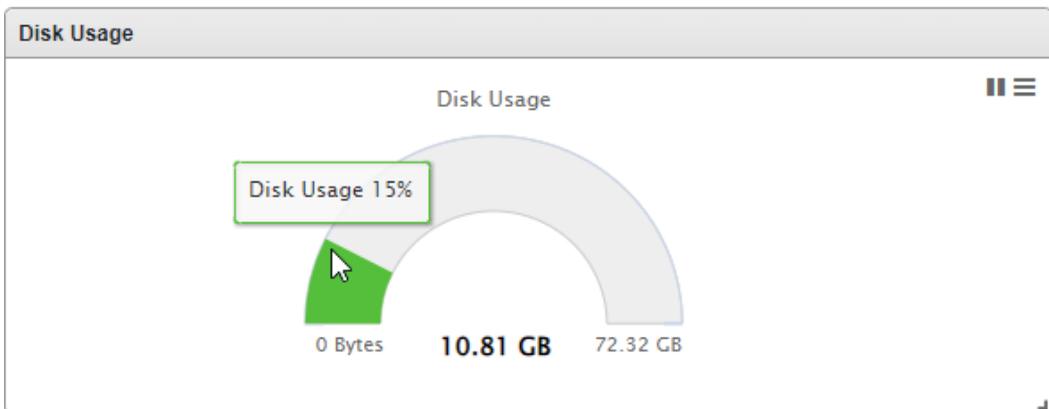
Memory Usage

This widget displays memory usage information.



Disk Usage

This widget displays disk usage information.



Add Widgets

The number of widgets that you can add to a tab depends on the layout for the tab.

Once the tab contains the maximum number of widgets, you must remove a widget from the tab 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) on the dashboard that you want to add the widget to.
3. Click **Add Widgets** and the screen appears.



Dashboard Agents Logs Administration About

Dashboard

Assets (5)
System (3)

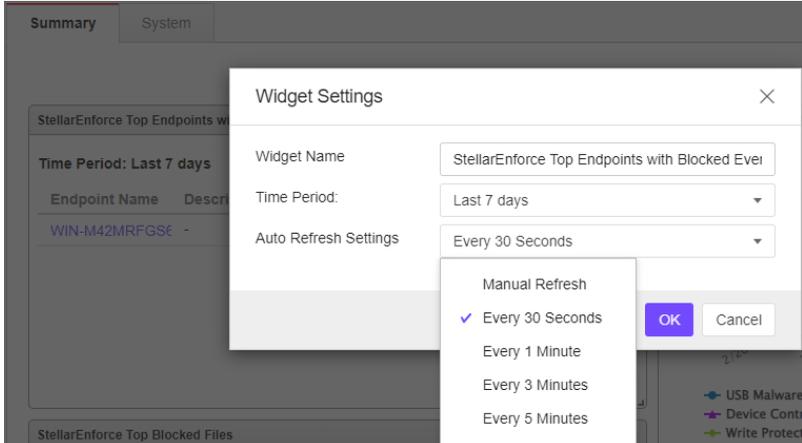
- StellarEnforce Top Endpoints with Blocked Events
Displays the endpoints that triggered the highest number of blocked events.
- StellarEnforce Blocked Event History
Displays blocked events during a specified time period.
- StellarEnforce Top Blocked Files
Displays the most frequently blocked files.

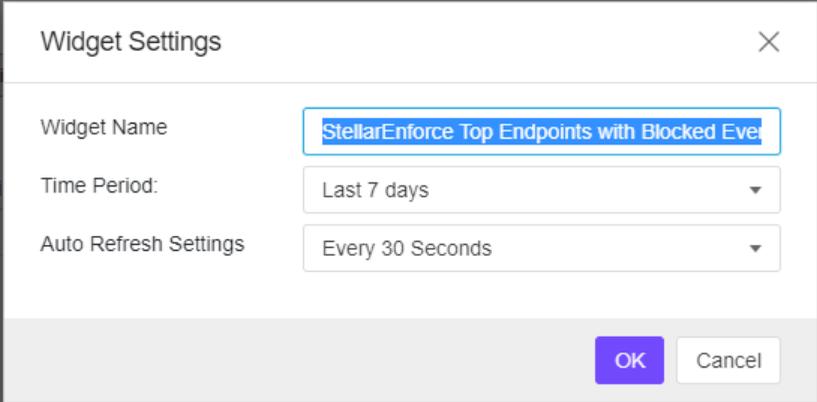
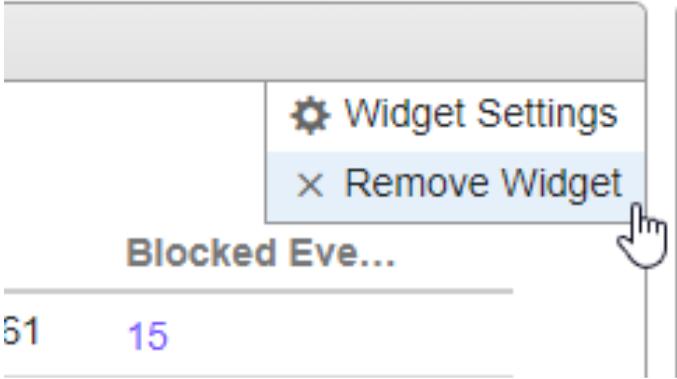
Add Cancel Currently selected widgets in this tab (3/10).

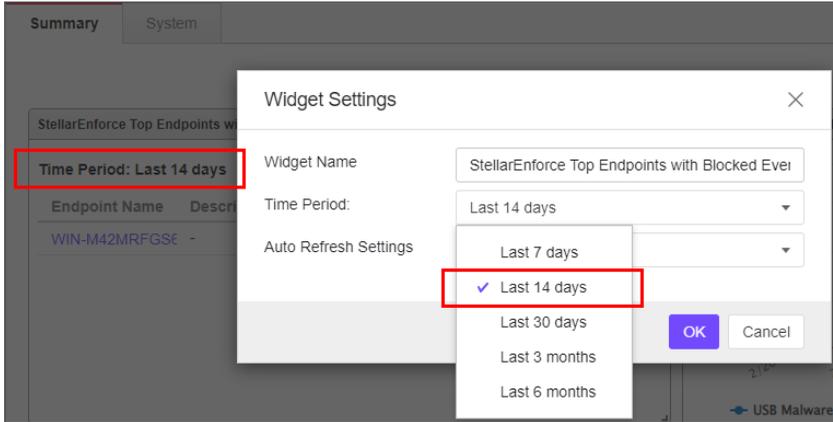
4. Select one or more widgets to add to the current tab and then click **Add**.

Using Widgets

Perform the following tasks on each widget:

Task	Steps
Move a widget	Move widgets on tabs by clicking and holding on the title bar at the top of the widget and dragging to various locations on a tab.
Resize a widget	Drag the edge of each widget to resize.
Refresh widget data	<p>Config the Auto Refresh Settings under Widget Settings first. (Default value is Every 30 Seconds)</p> 

Task	Steps
Rename a widget	<ol style="list-style-type: none"> 1. Click the More Options icon at the top of the widget. 2. Select Widget Settings. The Widget Settings screen appears. 3. Type a meaningful widget name for the widget. 
Close a widget	<ol style="list-style-type: none"> 1. Click the More Options icon at the top of the widget. 2. Select Remove Widget. 

Task	Steps
Set Time Period	<p>Displays the data during the specified time period. (Default value is Last 7 days)</p>  <p>The screenshot shows a 'Widget Settings' dialog box with the following fields:</p> <ul style="list-style-type: none"> Widget Name: StellarEnforce Top Endpoints with Blocked Ever Time Period: Last 14 days (dropdown menu is open, showing options: Last 7 days, Last 14 days (checked), Last 30 days, Last 3 months, Last 6 months) Auto Refresh Settings: (dropdown menu) <p>Buttons: OK, Cancel</p>

About the Agent Events Screen

To display the Agent Events screen, go to **Logs > Agent Events** in the navigation at the top of the web console. This screen displays a list of events related to detection and activity monitored on agents managed by StellarOne.

Depending on the feature status, StellarProtect generates a log and performs the action for the events listed in the following table.

Event	Feature Status	StellarProtect Action
A threat file landing or try to run	Real time scan disabled	Allows the file to landing/execute.
	Real time scan enabled	First action in configure will be taken and prompt for user a chance to change action.
A USB storage device attempts to access the endpoint	Device Control disabled	Allows access for the device
	Device Control enabled	Denies access for the device (when the device type is removable device) and prompts for user action
Unknown call of monitored process	Operation Behavior Anomaly Detection disabled	Allows call trigger monitored process.
	Operation Behavior Anomaly Detection enabled	Block or Allow depend on mode setting and prompt for user action.

The following table describes the user actions for the events.

User Action	Description
Add to Approved List	Add the threat file to Approved List.
Restore & Add to Approved List	Restore the quarantined file and add it to Approved List to prevent detection of the same file.
Quarantine	Quarantine the threat file.
Add to Approved Operations	Add unknown process chains to Operation Behavior Anomaly Detection's Approved List.
Allow one-time USB device access	Allow blocked USB device access until next plug-in.

Querying Agent Event Logs

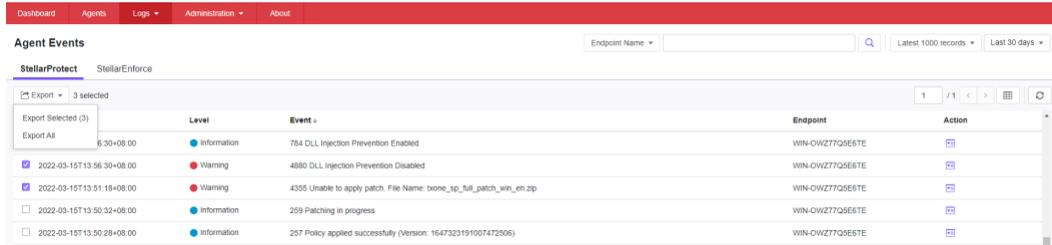
Querying refines the list of displayed agent event logs.

Procedure

1. Go to Logs > Agent Events in the navigation at the top of the web console. The Agent Events screen will appear.
2. To filter by period, click the Time Period drop down, which defaults to Last 30 days, and pick a time period. Perform one of the following:
 - Click a listed time range.
 - Click Custom, specify a time range, and click Search.
3. To filter by Endpoint Name, Agent Group, IP Address, IP Range, Description, Event Type, Severity Level, click the drop-down to the left of the search bar and specify a criteria.
 - Endpoint Name: Specify the name of the endpoint you're looking for.
 - Agent Group: Specify the name of the group you're looking for.
 - IP Address: Specify the IP address of the agent you're looking for.
 - IP Range: Specify a range of Ips to search for agents within.
 - Description: Specify the description assigned to the endpoint
 - Event Type: Select a specific event and click Apply.
 - Severity Level: Select Information or Warning as the event level.
4. The table displays only the entries that match the filters selected.

Exporting Agent Events

Save data about selected agent event log entries as a **CSV** file.



The screenshot shows the 'Agent Events' page in the web console. The navigation bar at the top includes 'Dashboard', 'Agents', 'Logs', 'Administration', and 'About'. The 'Agent Events' section is active, displaying a table of event logs. A dropdown menu is open on the left, showing 'Export Selected (3)' and 'Export All' options. The table contains five rows of event data:

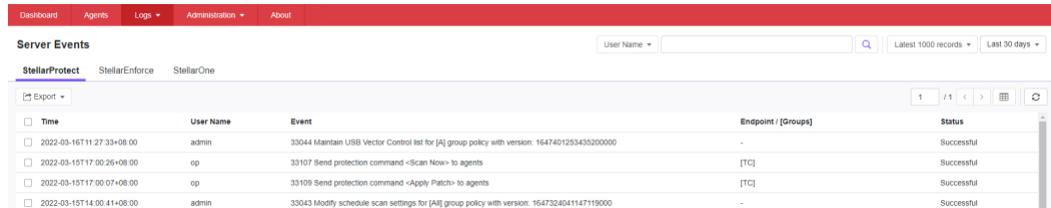
Level	Event	Endpoint	Action
Information	784 DLL Injection Prevention Enabled	WIN-OIWZ77Q9E6TE	[Action]
Warning	4890 DLL Injection Prevention Disabled	WIN-OIWZ77Q9E6TE	[Action]
Warning	4355 Unable to apply patch. File Name: boone_sp_full_patch_win_en.zip	WIN-OIWZ77Q9E6TE	[Action]
Information	259 Patching in progress	WIN-OIWZ77Q9E6TE	[Action]
Information	257 Policy applied successfully (Version: 1647323191007472506)	WIN-OIWZ77Q9E6TE	[Action]

Procedure

1. Go to **Logs > Agent Events** in the navigation at the top of the web console. The **Agent Events** screen will appear.
2. Select the agent log entries in the list that you want to export information for.
3. To export all entries, click the **Export All** on the upper-right.
4. To export selected entries only, select the entries you wish to export, then click the **Export Selected** button in the upper-left.
5. Save the file.

About the Server Events Screen

To display the Server Events screen, go to **Logs > Server Events** in the navigation at the top of the web console.



Time	User Name	Event	Endpoint (Groups)	Status
2022-03-16T11:27:33+08:00	admin	33044 Maintain USB Vector Control list for [A] group policy with version: 1547401253435200000	-	Successful
2022-03-15T17:00:26+08:00	op	33107 Send protection command -<Scan Now> to agents	[TC]	Successful
2022-03-15T17:00:07+08:00	op	33109 Send protection command -<Apply Patch> to agents	[TC]	Successful
2022-03-15T14:00:41+08:00	admin	33043 Modify schedule scan settings for [All] group policy with version: 1547324041147119000	-	Successful

This screen displays a log of audited StellarOne user account activity for StellarProtect, StellarEnforce, and StellarOne.



Note:

Server event logs contain collected information about actions taken by StellarOne web console account users and policies.

Querying Server Event Logs

Querying refines the list of displayed server event logs.

Procedure

1. Go to **Logs > Server Events** in the navigation at the top of the web console. The Server Events screen will appear.
2. Click the drop-down list under **Server Events**. A list of search criteria will appear.
3. Select the desired search criteria. Appropriate search fields appear for the selected criteria.
4. Follow the appropriate steps depending on the selected criteria:

Option	Description
Time Period	Do one of the following: <ul style="list-style-type: none"> • Select a listed time range. • Specify a custom time range. <ol style="list-style-type: none"> a. Go to Custom in the list. b. Specify your custom time range. c. Click Apply.
User Name	Displays all events logged by a specific user.
Endpoint Name	Type the endpoint host name (first few letters or complete name), and click Search.
Group Name	Displays all events logged by the specific groups.
Event Type	Select a specific event.

Your search results will appear in the list of server event logs.

Exporting Server Event Logs

Save data about selected server event log entries as a CSV file.

Procedure

1. Go to Logs > Server Events in the navigation at the top of the web console. The Server Events screen will appear.
2. Select the server log entries in the list that you want to export information for.
3. To export all entries, click the Export icon.
4. To export selected entries only, select the entries you wish to export then click Export Selected.
5. Save the file.

About the System Log Screen

To display the System Log screen, go to Logs > System Logs in the navigation at the top of the web console. This screen displays a log of adjustable StellarOne web console settings.

Querying Server Logs

Querying refines the list of displayed server event logs.

Procedure

1. Go to Logs > System Logs in the navigation at the top of the web console. The System Log screen will appear.
2. Select the desired search criteria. Appropriate search fields appear for the selected criteria.
3. Follow the appropriate steps depending on the selected criteria:

Option	Description
Time Period	Do one of the following: <ul style="list-style-type: none"> • Select a listed time range. • Specify a custom time range. <ol style="list-style-type: none"> a. Go to Custom in the list. b. Specify your custom time range. c. Click Search.

Option	Description
Severity	Select one of the criteria below and click Search. <ul style="list-style-type: none">• Emergency• Alert• Critical• Error• Warning• Notice• Information• Debug

Your search results will appear in the list of system logs.

Exporting System Logs

Save data about selected system log entries as a CSV file.

Procedure

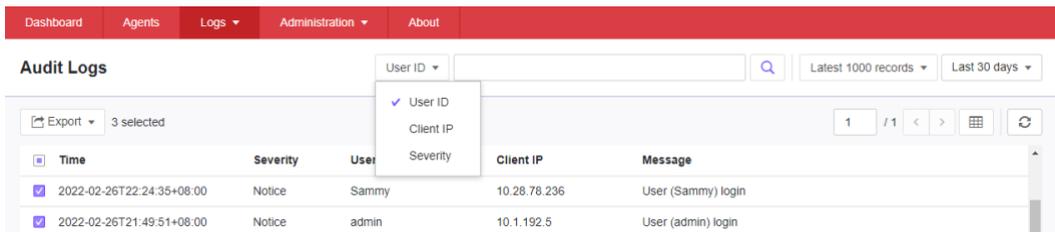
1. Go to Logs > System Logs in the navigation at the top of the web console. The System Logs screen will appear.
2. Select the system log entries in the list that you want to export information for.
 - To export all entries, click the Export icon.
 - To export selected entries only, select the entries you wish to export then click Export Selected.

About the Audit Log Screen

To display the Audit Log screen, go to Logs > Audit Logs in the navigation at the top of the web console. This screen displays StellarOne’s audit logs.

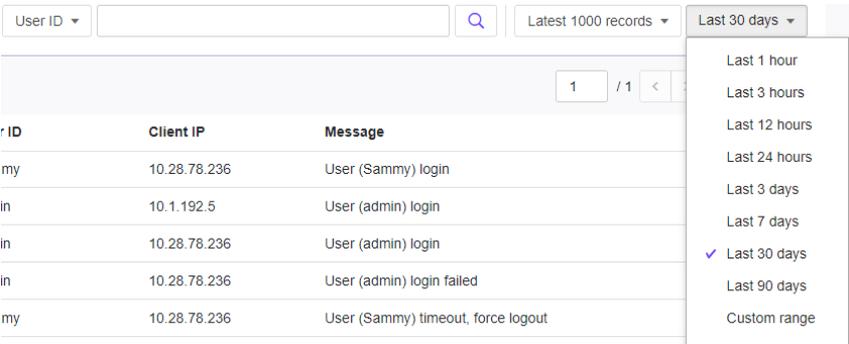
Querying Audit Logs

Querying refines the list of displayed server event logs.



Procedure

1. Go to Logs > Audit Logs in the navigation at the top of the web console. The Audit Log screen will appear.
2. Select the desired search criteria. Appropriate search fields appear for the selected criteria.
3. Follow the appropriate steps depending on the selected criteria:

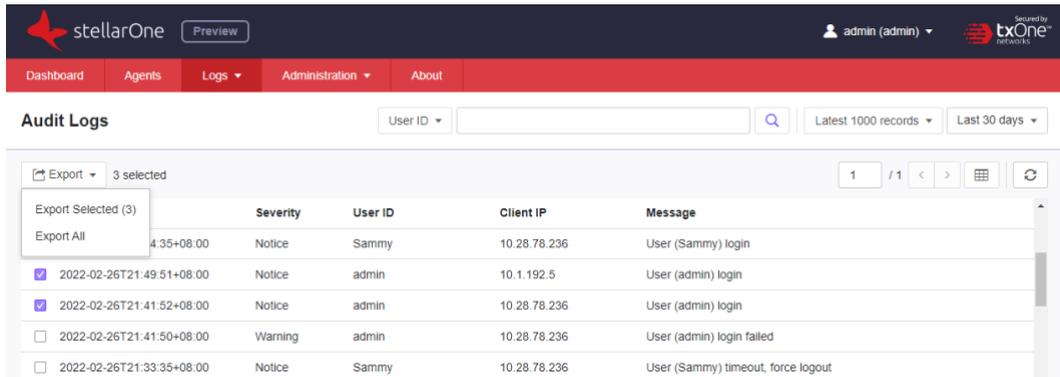
Option	Description
Time Period	 <p>Do one of the following:</p> <ul style="list-style-type: none"> • Select a listed time range. • Specify a custom time range. <ol style="list-style-type: none"> a. Go to Custom in the list. b. Specify your custom time range. c. Click Search.
User ID	Type user ID and click Search.
Client IP	Type client IP number and click Search.
Severity	<p>Select one of the criteria below and click Search.</p>  <ul style="list-style-type: none"> • Emergency • Alert • Critical • Error

Option	Description
	<ul style="list-style-type: none"><li data-bbox="341 250 508 277">• Warning<li data-bbox="341 285 481 313">• Notice<li data-bbox="341 321 545 349">• Information<li data-bbox="341 357 481 384">• Debug

Your search results will appear in the list of audit logs.

Exporting Audit Logs

Save data about selected server event log entries as a CSV file.



The screenshot shows the stellarOne interface with the 'Audit Logs' section active. A table of log entries is displayed with columns for Severity, User ID, Client IP, and Message. An 'Export' menu is open, showing options for 'Export Selected (3)' and 'Export All'. The table contains the following data:

	Severity	User ID	Client IP	Message
<input type="checkbox"/>	Notice	Sammy	10.28.78.236	User (Sammy) login
<input checked="" type="checkbox"/>	Notice	admin	10.1.192.5	User (admin) login
<input checked="" type="checkbox"/>	Notice	admin	10.28.78.236	User (admin) login
<input type="checkbox"/>	Warning	admin	10.28.78.236	User (admin) login failed
<input type="checkbox"/>	Notice	Sammy	10.28.78.236	User (Sammy) timeout, force logout

Procedure

1. Go to Logs > Audit Logs in the navigation at the top of the web console. The Audit Logs screen will appear.
2. Select the system log entries in the list that you want to export information for.
 - To export all entries, click the **Export All**.
 - To export selected entries only, select the entries you wish to export then click **Export Selected**.

Chapter 7

Administration

This chapter introduces TXOne StellarOne administration settings.

About the Account Management Screen

To display the Account Management screen, go to **Administration > Account Management** in the navigation at the top of the web console.

Use this screen to manage StellarOne web console accounts. TXOne StellarOne web console accounts have the following privileges:

Account Type	Privileges
Admin (Full Control)	<ul style="list-style-type: none"> a. Manage StellarOne: The privilege of configuring system settings. b. Manage Group: The privilege of creating, moving, or deleting groups. c. Account Management: The privilege of managing StellarOne accounts. d. Policy Configuration: The privilege of defining policy for Agents such as USB Control and Intelligent Runtime Learning.
Operator (Asset Control)	<ul style="list-style-type: none"> a. Manage Group: The privilege of creating, moving, or deleting groups. b. Policy Configuration: The privilege of defining policy for Agents such as USB Control and Intelligent Runtime Learning.
Viewer (Read Only)	<ul style="list-style-type: none"> a. Read only for Dashboard, Policy Configuration, and Agent Events. b. Agent installer package download available. c. Modify their 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.

Task	Account Privilege Allowed		
	Admin	Operator	Viewer
Dashboard	V	V	V
Configure application lockdown	V	V	
Configure maintenance mode	V	V	
Configure device control	V	V	
Add trusted files	V	V	
Add trusted USB devices	V	V	
Scan now	V	V	
Update approved list	V	V	
Update agent components	V	V	
Deploy agent patch	V	V	
Check connection	V	V	V
Collect event logs	V	V	
Import / Export (approved list / agent configuration)	V	V	
Organize (edit description / move / delete)	V	V	
Configure group policy	V	V	

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

Adding Accounts

Procedure

1. Log on to the web console using an administrator account.
(Please note that information entered here is case-sensitive)
2. Go to **Administration > Account Management** in the navigation at the top of the web console. The Account Management screen will appear.
3. Click **Add User** button, and the **Add User Account** screen will appear.
4. Specify the **Authentication Source**. (Local or SMAL Identity Provider)
 - To add a local user, specify the **ID** and **Name**. (Please note that information entered here is case-sensitive)

Add User Account

Authentication Source	Local
Role	Viewer
ID*	Joseph
Name*	Joseph Lin

- To add an **SAML Identity Provider** user, specify Email for SAML Account Mapping and Name. (Please note that information entered here is case-sensitive)

Add User Account ×

Authentication Source ▼
[Single Sign On Configuration](#)

Role ▼

Email for SAML Account Mapping*
Type the same letter case as the account on your authentication server.

Name*

- Role:** Specify the privileges for the account as among **Admin**, **Operator** or **Viewer** (Default).

Add User Account

Authentication Source ▼

Role ▼

ID*

Name*

Local Password*

Admin

Operator

✓ Viewer

- For a **Local** user, specify and re-type the Local Password.

- Group Control:** Specify the Group Control you want for the target account to access.

Group Control*

- All (0)
 - Admin-G1 (0)
 - msmith-G1 (0)
 - ▼ Orson-G1 (0)
 - ▼ Orson-G2 (0)
 - Orson-G3 (0)
 - Oscar-G1 (0)
 - Sammy-G1 (0)

7. Optionally, type an account **Description**.
8. Click **Confirm** button, and the target user account will be created.

Account Management

Users Roles

[+ Add User](#) [Delete](#) 1 / 1 [<](#) [>](#) [Grid](#)

<input type="checkbox"/> ID ↑	Name	Role	Authentication Source	Group Control	Description	Actions	
<input type="checkbox"/>	Alice	Admin-01	Admin	Local	-	-	✎ 🗑
<input type="checkbox"/>	Orson	Operator-01	Operator	Local	-	-	✎ 🗑
<input type="checkbox"/>	Oscar	Operator-02	Operator	Local	-	-	✎ 🗑

Edit Accounts

Procedure

1. Log on to the web console using an account with **Admin** role.
(Please note that information entered here is case-sensitive)
2. Go to **Administration > Account Management** in the navigation at the top of the web console. The Account Management screen will appear.
3. Click **Edit** icon from Actions, and the **Edit User Account** screen will appear.
4. For a **Local** user, you can specify the *account Role, Name, Password, Group Control, and Description*.
5. For a **SAML Identity Provider** user, you can specify the account *Role, Name, Group Control, and Description*.
6. Click Confirm.

Edit User Account ✕

Authentication Source

Role

Email for SAML Account Mapping*
Type the same letter case as the account on your authentication server.

Name*

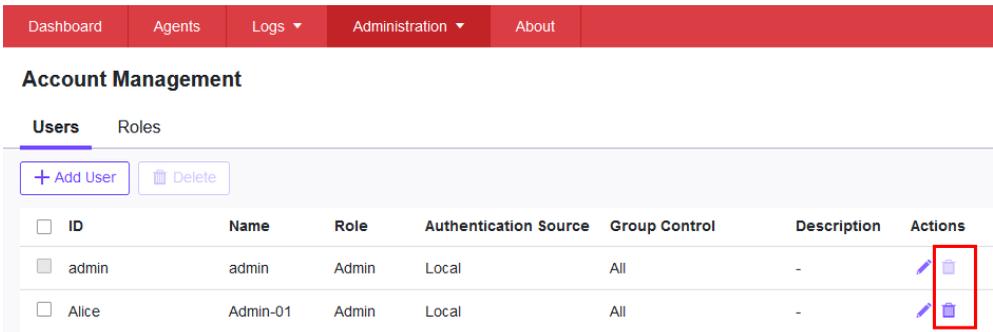
Group Control*
 All (0)
 Admin-G1 (0)
 msmith-G1 (0)
 > Orson-G1 (0)
 Oscar-G1 (0)
 Sammy-G1 (0)

Description

Delete Accounts

Procedure

1. Log on the web console using an administrator account. (Please note that information entered here is case-sensitive)
2. Go to **Administration > Account Management** in the navigation at the top of the web console. The Account Management screen will appear.
3. Select the specific account which you want to delete. (Only the **Master admin** cannot be deleted)



Dashboard Agents Logs Administration About

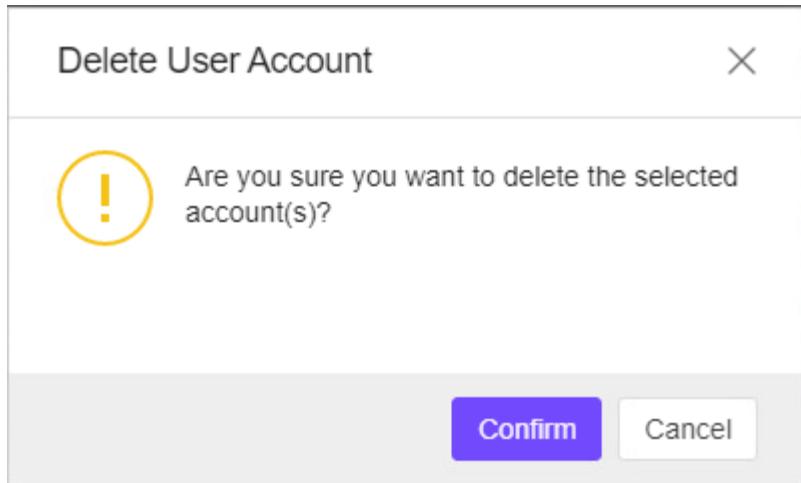
Account Management

Users Roles

+ Add User Delete

ID	Name	Role	Authentication Source	Group Control	Description	Actions
<input type="checkbox"/> admin	admin	Admin	Local	All	-	 
<input type="checkbox"/> Alice	Admin-01	Admin	Local	All	-	 

4. Click **Delete** icon, and the **Delete User Account** dialog will appear.



5. Click **Confirm** button, and the target user account should be deleted from the Account table.

Single Sign-On

Procedure

1. Log on to the web console using an administrator account.
(Please note that information entered here is case-sensitive)
2. Go to **Administration** > **Single Sign-On** in the navigation at the top of the web console.
3. Click **Download** button to download the StellarOne metadata XML file.
4. Upload the StellarOne XML file to your IdP, and then download the IdP metadata XML file.
5. Click **Upload** button to upload the IdP metadata XML file to StellarOne web console and complete the SAML 2.0 single sign-on configuration. The IdP metadata XML file must be re-uploaded if there is a configuration change on the IdP



3 **Upload the IdP metadata XML file**
Upload the IdP metadata XML file to complete the SAML 2.0 single sign-on configuration. The IdP metadata XML file must be re-uploaded if there is a configuration change on the IdP

IdP display name:
Protocol: SAML 2.0/SAML 1.1
IdP Single Sign On URL:
Mapping Attribute: Email Address

6. After the IdP metadata XML file is uploaded, the **Test Connection** button will appear.
7. Click **Test Connection** button to test the IdP connection with StellarOne.

Dashboard Agents Logs Administration About

Single Sign-On

✓ IdP connection test successful. ✕

SAML Configuration

1 **Download the StellarOne metadata XML file**
 Upload the StellarOne XML file to your IdP

[Download](#)

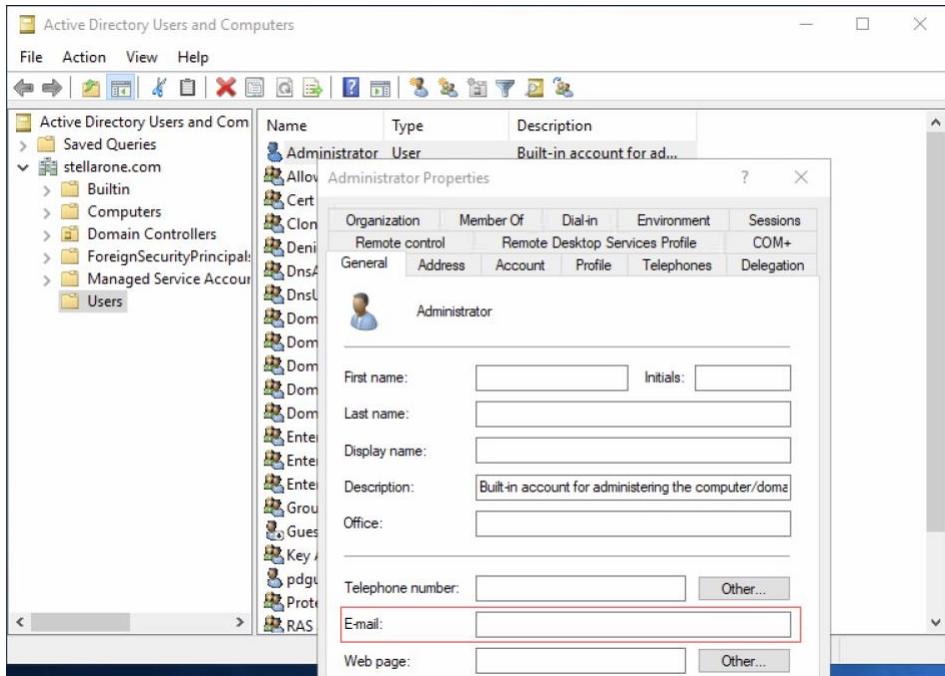
Note:

Invalid logon error message may appear after the SAML configuration is completed. Please refer to [Resolving the SSO Issue](#) 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 Active Directory Users and Computers in IdP server.
2. Right-click on the user account used for SSO, then go to **Properties > General**.
3. Check the E-mail field. Make sure the email input here is consistent with the account email for accessing StellarOne web console.



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 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. Check the box of **Synchronize guest time with host**, and then click **OK**.

Virtual Machine Settings

Hardware Options

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

VMware Tools features

- Synchronize guest time with host

VMware Tools updates

If a new version of VMware Tools is available:

- Update manually (do nothing)
- Update automatically
- Use application default (currently update manually)

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

System Time

Go to Administration > System Time to change system time settings.

Date and Time

Use the Time Period drop-down button to specific system time

Date and Time

Current Time: 2022-02-27T18:19:38+08:00 

Time Zone

Time Zone:

 2022-02-27

 18:19:31

< **February 2022** >

Su	Mo	Tu	We	Th	Fr	Sa
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	1	2	3	4	5
6	7	8	9	10	11	12

Time Zone

Use the drop-down to specific system time zone.

Time Zone

Time Zone: (GMT+08:00) Asia/Taipei 

- (GMT-12:00) Etc/GMT+12
- (GMT-11:00) Etc/GMT+11
- (GMT-11:00) Pacific/Midway
- (GMT-11:00) Pacific/Niue
- (GMT-11:00) Pacific/Pago_Pago
- (GMT-11:00) Pacific/Samoa
- (GMT-11:00) US/Samoa
- (GMT-10:00) Etc/GMT+10
- (GMT-10:00) HST

Syslog Forwarding

You can forward Server and Agent Event logs to an external Syslog server for the additional managing and monitoring 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. Enable **Forward logs to syslog server (CEF only)**.
3. Specify the Protocol, Server Address, and Port of the Syslog server.

Dashboard Agents Logs Administration

Syslog Forwarding

Forward logs to syslog server (CEF only)

Server Address*

Port* ⓘ

Protocol TCP UDP

Agent event format

CEF Field Name	Description	Possible Values
Header		
CEF:Version		CEF:0
Device Vendor		TXOne Networks
Device Product		StellarProtect
Device Version		1.0
Device Event Class ID	Event id	{ }
Name	Event kind	Agent Event
Severity	LOG_CRIT: 2 LOG_WARNING: 4 LOG_INFO: 6	{2, 4, 6}
Extension		
eventTime	StellarEnforce format	Jan 02 2006 15:04:05 GMT+00:00
msg	<string>	
category	OPTION: 0 SYSTEM: 1 INTELLI_AV: 2	

CEF Field Name	Description	Possible Values
	ANOMALY_DETECT: 3 CHANGE_CONTROL: 4 DEVICE_CONTROL: 5 MISC: 15	
agentEndpoint	<string>	
agentIp	<string>	
agentLocation	<string>	
agentVendor	<string>	
agentModel	<string>	
agentOS	<string>	
policyVersion	<string>	
detailMsg	<string>	
targetProcess	<string>	
fileHash	<string>	
threatType	<string>	
threatName	<string>	
filePath	<string>	
actionResult	<int>	
quarantinePath	<string>	

CEF Field Name	Description	Possible Values
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>	
targetFile	<string>	
vid	<int>	
pid	<int>	

CEF Field Name	Description	Possible Values
sn	<string>	
accessImagePath	<string>	
srcPath	<string>	
dstPath	<string>	
errCode	<int>	
patchFileName	<string>	
filePath	<string>	
type	<string>	

StellarProtect Server event format

CEF Field Name	Description	Possible Values
Header		
CEF:Version		CEF:0
Device Vendor		TXOne Networks
Device Product		StellarProtect
Device Version		1.0
Device Event Class ID	Event id	{ }

CEF Field Name	Description	Possible Values
Name	Event kind	Server Event
Severity	LOG_INFO: 6	{6}
Extension		
eventTime	StellarEnforce format	Jan 02 2006 15:04:05 GMT+00:00
msg	<string>	
userName	<string>	
userRole	<string>	
clientIp	<string>	

StellarOne Server event format

CEF Field Name	Description	Possible Values
Header		
CEF:Version		CEF:0
Device Vendor		TXOne Networks
Device Product		StellarOne
Device Version		1.0

CEF Field Name	Description	Possible Values
Device Event Class ID	Event id	{}
Name	Event kind	Console Log
Severity	LOG_INFO: 6	{6}
Extension		
eventTime	StellarEnforce 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, enforce}

Log Purge Settings

Purge older logs to reduce the size of the StellarOne database.

Purge Now

Procedure

1. Go to **Administration** > **Log Purge** in the navigation at the top of the web console. The **Log Purge** screen will appear.
2. Specify the Log Type you want to purge below.
 - All Logs
 - System Log, Audit Log, Agent Events, or Server Events
3. Under **older than**, specify the maximum age of event log entries to keep.
 - 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)
4. Under **Keep at most**, specify the maximum number of event entries to keep.
 - 0 entries
 - 10000 entries, 50000 entries, 100000 entries, 500000 entries, 1000000 entries, 5000000 entries, 10000000 entries
5. Click **Purge Now** button, and the event logs should be purged.

Log Purge

Purge Now

Purge Agent Events ▾ older than no limit ▾ and keep at most 0 entries ▾ Purge Now

Purge Now

Purge Agent Events ▾ older than 1 month(s) ▾ and keep at most 10,000 entries ▾ Purge Now

Automatic Purge

Use these settings to set an automatic purge once per day.

Procedure

1. Go to **Administration > Log Purge** in the navigation at the top of the web console. The **Log Purge** screen will appear.
2. Specify the Log Type you want to purge below.
 - System Log
 - Audit Log
 - Agent Events
 - Server Events
3. Under **older than**, specify the maximum age of event log entries to keep.
 - 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)
4. Under **Keep at most**, specify the maximum number of event entries to keep.
 - 10000 entries
 - 50000 entries

- 100000 entries
 - 500000 entries
 - 1000000 entries
 - 5000000 entries
 - 10000000 entries
5. Click **Save** button.

Automatic Purge

Purge **System Log** older than and keep at most

Purge **Audit Log** older than and keep at most

Purge **Server Events** older than and keep at most

Purge **Agent Events** older than and keep at most

Notification Settings

Enter your e-mail under Email Notifications. Your e-mail will be saved when you Save the page with the rest of your settings.

Procedure

1. First, go to **Administration > SMTP Settings** to specify your SMTP server settings.
2. Go to **Administration > Notification** to change notification settings.
3. Sections under Notification include:
 - Warning Level Agent Events (Default is disabled)

- Outbreak (Default is disabled)
- Email Notifications.

Warning Level Agent Events

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

 TXOne StellarProtect: [Action required] Incoming Files Scanned, Action Taken by Antivirus: C:\Users\Administrator\Desktop\eicar\eicar.com on TC

StellarOne

Action required

TXOne StellarProtect detected a warning event that requires attention. Incoming Files Scanned, Action Taken by Antivirus: C:\Users\Administrator\Desktop\eicar\eicar.com

To manage this event, go to [Agent Event](#).

Event Information

Date and Time:	2022-03-16T07:21:55Z
Level:	Warning
Event ID:	4609
Event:	Incoming Files Scanned, Action Taken by Antivirus: C:\Users\Administrator\Desktop\eicar\eicar.com
Detail:	Incoming files were scanned by antivirus. Action were taken according to settings. File Path: C:\Users\Administrator\Desktop\eicar\eicar.com File Hash: 275a021bb1b6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f Threat Type: Virus Threat Name: Eicar_test_file Action Result: 0 Quarantine Path: C:\Program Files\TXOne\StellarProtect\private\quarantine\8866212f-f9d9-43d5-aa93-36aa8997549f

Agent Information

Endpoint:	TC
IP address:	192.168.15.138
Tags:	
Approved List last updated on:	N/A

Outbreak

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 has appeared in a specified time period.

StellarOne(protect): Outbreak notification

StellarOne

Outbreak on 2022-03-16 07:32:23.113205781 +0000 UTC m=+17362.839585743. There were more than 1 warnings within a 1-minute period.
For details, go to the StellarOne web console at [Agent Event](#)

You can set the number of open warnings in a time period to be considered as an outbreak (1 - 20000), as well as the time period which those warnings will be measured against (1 - 60 minutes).

Outbreak

Send outbreak notifications

Number of warnings in a time period: (1-20000)

The time period of those warnings: (1-60 minutes)

SMTP Settings

This screen allows users to specify SMTP server settings for sending out notifications and scheduled reports.

Procedure

1. Go to **Administration** > **SMTP Settings** in the navigation at the top of the web console. The SMTP Settings screen will appear.
2. Specify **Server address**, **Port**, and **Sender**.
3. If the SMTP server requires authentication, select SMTP server authentication.
4. To send a test email from StellarOne, click the Send Test Email button.
5. Click **Save** button.

The screenshot shows the 'SMTP Settings' page in a web console. At the top is a navigation bar with 'Dashboard', 'Agents', 'Logs', 'Administration', and 'About'. The 'SMTP Settings' title is displayed below the navigation. The form contains several input fields: 'Server address*', 'Port*', and 'Sender*', each with a corresponding text box. A checkbox labeled 'SMTP server requires authentication' is checked. Below this are 'User name*' and 'Password*' fields, each with a text box. At the bottom of the form are three buttons: 'Save' (highlighted in blue), 'Cancel', and 'Send Test Email'.

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 to agents.

Procedure

1. Go to **Administration** > **Proxy** in the navigation at the top of the web console.
2. Specify the Proxy Settings for the following option:
 - Proxy Settings for StellarOne to internet
 - Proxy settings for StellarOne to Agent communications
 - Proxy Settings for agent to StellarOne communicates to agents.
3. To configure proxy settings for updates:
 - (1) Select protocol use HTTPS or HTTP
 - (2) Under Server Address, specify the IPv4 address or FQDN of the proxy server.
 - (3) Specify the Port.
 - (4) If your proxy server requires authentication, select Proxy server authentication and give your credentials.
 - (5) Click Save.

Proxy

Proxy Settings for StellarOne to internet

Proxy Settings for StellarOne to internet

HTTPS HTTP

Server Address*

Port*

Proxy server requires authentication

User name*

Password*

Proxy Settings for StellarOne to Agent communications

Proxy Settings for StellarOne to Agent communications

Proxy Settings for Agent to StellarOne communications

Proxy Settings for Agent to StellarOne communications

 **Tip**

To configure proxy settings used by StellarOne when sending messages to StellarProtect.

Before installation:

Add the proxy information to the configuration file used by the agent installer package. Save the proxy settings. They will now be included in the agent installer after the agent package is repacked.

After installation:

Use the **opcnd.exe** Command Line Interface tool on the local StellarProtect agent administrator guide.

Download / Update Settings

To manage Download / Updates for StellarOne and StellarProtect, go to Administration >

Download / Updates in the navigation at the top of the web console. Here, you have two tabs: StellarOne and StellarProtect.

The following table describes the tasks you can perform on this screen under the StellarOne tab:

Function	Description
Scan Component	Under this section you can click Update Now to downloading latest components. All of the pattern and engine versions are listed here.
Scan Component Update Schedule	Set the frequency and time for scheduled reports to be either daily, weekly, or monthly, as well as which day of the week or month they arrive on and Start time.
Scan Component Update Source (StellarOne)	Specify an update server or download updates directly from the ActiveUpdate server.
Scan Component Update Source (Agents)	You can also specify an update server or downloading them directly from StellarOne.

The following table describes the tasks you can perform on this screen under the StellarProtect tab:

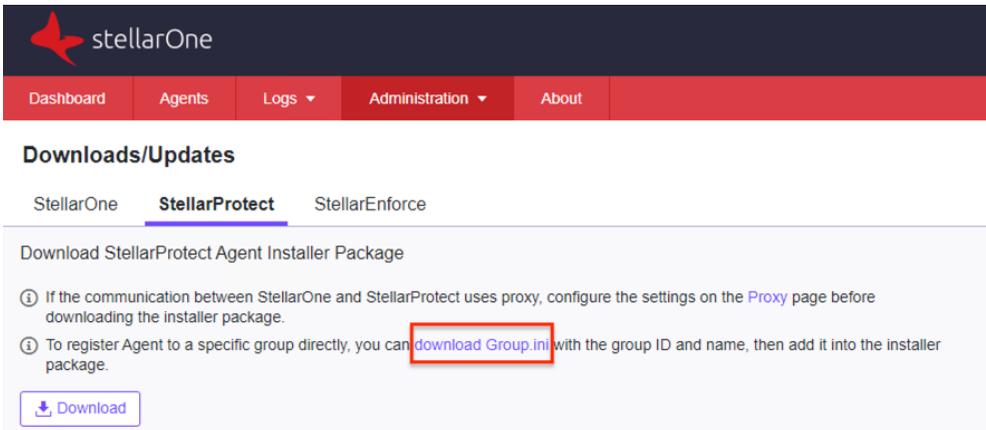
Function	Description
Download StellarProtect Agent Installer Package	Download an up-to-date agent installer package. You can also modify the agent component download source and proxy settings, as well as update to the latest components.

Function	Description
	Download a Group.ini file and add it into the installer package, which enables directly registering StellarProtect agent to a specific group via StellarOne console. For more details, see Group Mapping .
Patch	Here you can click the Import button to import a patch manually, or Delete to remove a StellarProtect patch.

Group Mapping

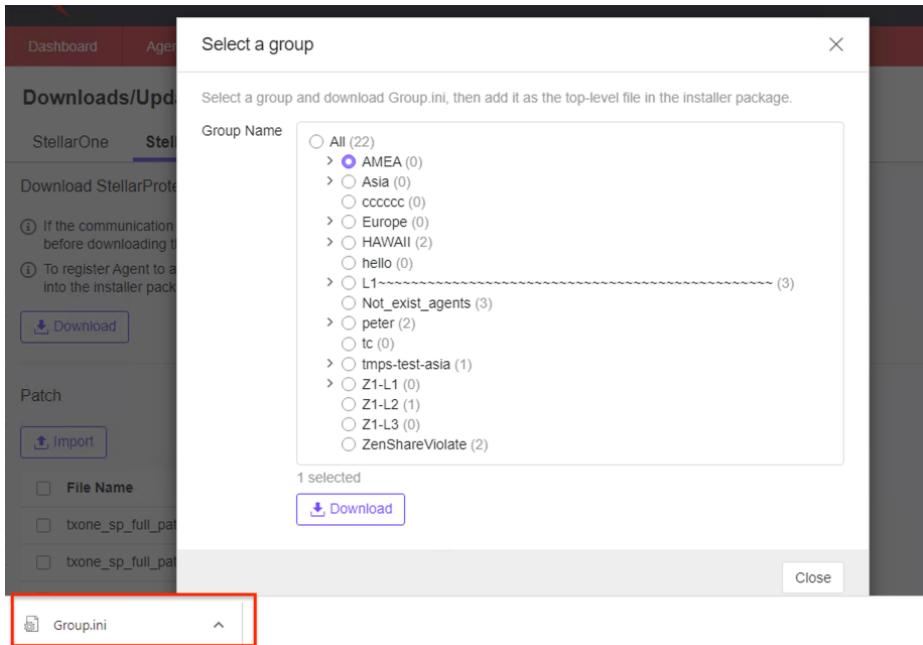
Procedure

1. Go to **Administration > Downloads/Updates** in the navigation at the top of the web console.
2. Select **StellarProtect** tab.
3. After downloading the Installer Package, click on **download Group.ini**.



The screenshot shows the StellarOne web console interface. At the top, there is a navigation bar with the StellarOne logo and menu items: Dashboard, Agents, Logs, Administration, and About. Below this, the 'Downloads/Updates' section is active, with tabs for StellarOne, StellarProtect (selected), and StellarEnforce. The main content area is titled 'Download StellarProtect Agent Installer Package' and contains two informational messages. The second message states: 'To register Agent to a specific group directly, you can [download Group.ini](#) with the group ID and name, then add it into the installer package.' The 'download Group.ini' link is highlighted with a red rectangular box. At the bottom of this section, there is a 'Download' button with a download icon.

4. Select a group for the StellarProtect agent and click **Download**. A file named **Group.ini** is downloaded. Place the Group.ini file as the top-level file in the agent's installer package.

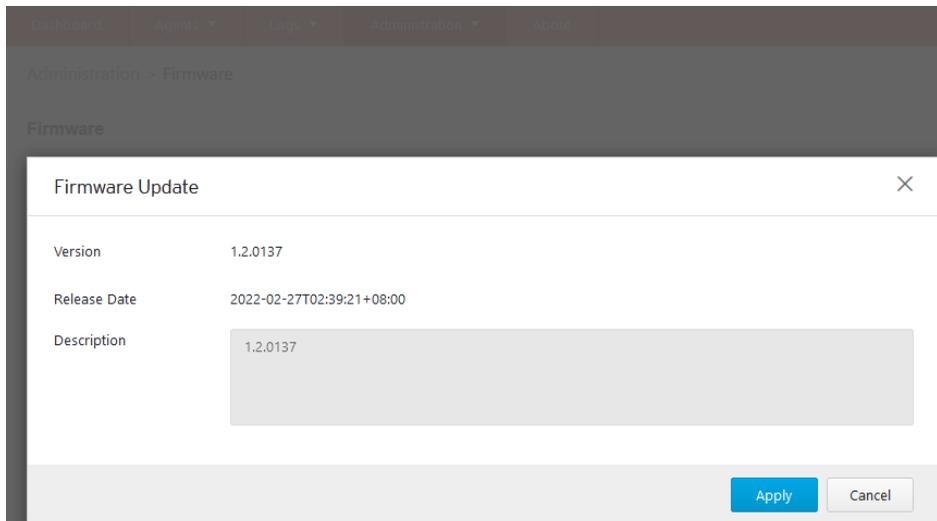


5. User can check StellarOne management console and StellarProtect agent console to see if the agent is successfully registered.

Firmware

Procedure

1. Go to **Administration** > **Firmware** in the navigation at the top of the web console.
2. Click **Import** to specify the firmware patch file (E.g. acus.fw_1.2.0137.acf).
3. Version shows the current StellarOne build version.
4. Release Date and Description show the current information for StellarOne patch fire.



5. When the Firmware Update window pops up, click **Apply** to apply the patch to StellarOne.
6. Confirm the notification description.
7. Click **Install Now** to implement the update or **Abort** to stop updating.

Administration > Firmware

Firmware

Update downloaded. StellarOne is ready to install. Please click the Install button to start the installation. After completing Installation, the system may restart all services.

 **Notice**

- The installation may take 5 to 10 minutes to finish. Please do not shut down the StellarOne during the installation
- We highly recommended you to back up your data before starting the installation.
- The system will not support downgrading to an earlier version.

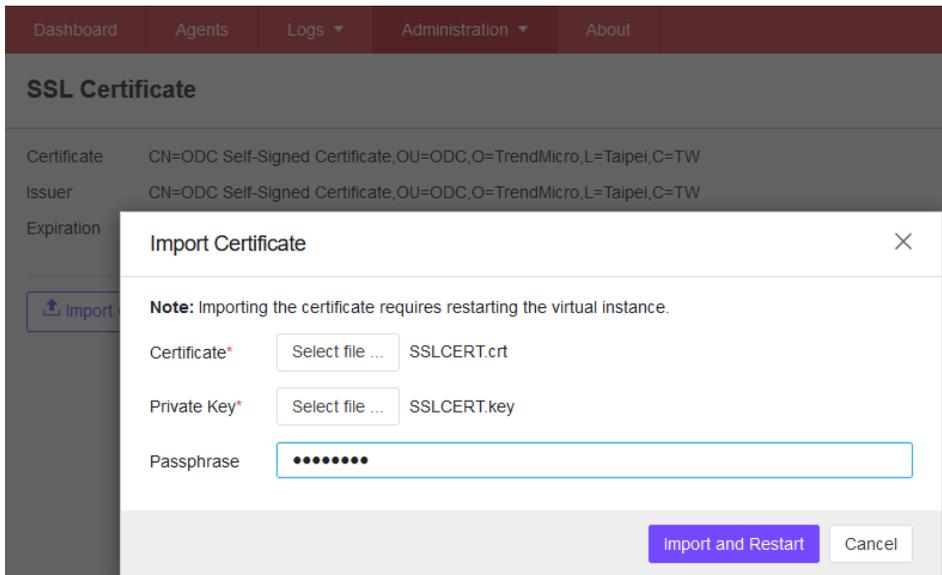
 Install Now

 Abort

SSL Certification

Procedure

1. Go to **Administration > SSL Certification** in the navigation at the top of the web console.
2. Select the desired **Import Certificate**.
3. Importing the certificate requires restarting the virtual instance.
 - (1) Use the 'Select file...' dropdown next to Certificate to select the desired certificate to import.
 - (2) Use the 'Select file...' dropdown next to Private Key to select the desired Private Key.
 - (3) Specify the Passphrase. (Optional)



The screenshot shows the StellarOne console interface. At the top, there is a navigation bar with 'Administration' selected. Below it, the 'SSL Certificate' page is visible. A modal dialog titled 'Import Certificate' is open, displaying the following information:

- Note:** Importing the certificate requires restarting the virtual instance.
- Certificate***: Select file ... SSLCERT.crt
- Private Key***: Select file ... SSLCERT.key
- Passphrase**: [Redacted with dots]

At the bottom of the dialog, there are two buttons: 'Import and Restart' (highlighted in blue) and 'Cancel'.

4. Click **Import and Restart**. (StellarOne console will be reloaded)

Dashboard

Agents

Logs ▾

Administration ▾

About

SSL Certificate

Certificate	CN=haha,OU=Stellar,O=TXOne,L=Taipei,ST=Taipei,C=TW
Issuer	CN=haha,OU=Stellar,O=TXOne,L=Taipei,ST=Taipei,C=TW
Expiration	2022-09-15T17:38:13+08:00

 Remove Certificate

 Replace Certificate

License Management

To display the License Management screen, go to Administration > License in the navigation at the top of the web console. The following details appear on this screen:

Item	Description
Status	Displays “Activated” or “Expired”
Type	Displays “Full” or “Trial”
Expiration	Displays the date when features and support end
Seats	Specifies how many agents can register to StellarOne and current number of registered agents
Activation Code	Displays the Activation Code
Last Updated	Displays the last time the Activation Code was updated



Note:

Click **Renew License** button to update your product license. The connection with the TXOne Product License server is required.

Chapter 8

Log Description Reference

This chapter includes extra information for administrator management. Topics in this chapter include:

- StellarProtect Agent Event Log Descriptions
- StellarProtect Server Event Log Descriptions
- StellarOne Server Event Log Descriptions

StellarProtect Agent Event Log Descriptions

Windows Event Log Descriptions

Event ID	Level	Category	Event Content	Event Details
256	Information	system	Service started	
257	Information	system	Policy applied successfully (Version: %version%)	
258	Information	system	Patch applied. File Name: %file_name%	Patch applied. File Name: %file_name%
259	Information	system	Patching in progress	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	ICS Inventory List Update Succeeded	
514	Information	intelli_av	Real Time Scan Enabled	
515	Information	intelli_av	Scheduled Scan Start	A scheduled scan has started.
516	Information	intelli_av	Scheduled Scan End	A scheduled scan has ended.
517	Information	intelli_av	On-Demand Scan Start	A manually launched scan has started.
518	Information	intelli_av	On-Demand Scan End	A manually launched scan has ended.
519	Information	intelli_av	Scheduled Scan Enabled	Scheduled scan has been enabled. Next scan will be on %NextScan%.
520	Information	intelli_av	Scheduled Scan Disabled	Scheduled scan has been disabled.

Event ID	Level	Category	Event Content	Event Details
768	Information	anomaly_detect	Operations Behavior Anomaly Detection Enabled	Mode: %Mode% Level: %Level%
769	Information	anomaly_detect	Added Operations Behavior Anomaly Detection Approved Operation	Access User: %USERNAME% ID: %ID% Target Process: %PATH% %ARGUMENT% Parent Process 1: %PATH% %ARGUMENT% Parent Process 2: %PATH% %ARGUMENT% Parent Process 3: %PATH% %ARGUMENT% Parent Process 4: %PATH% %ARGUMENT%
770	Information	anomaly_detect	Removed Operations Behavior Anomaly Detection Approved Operation	ID: %ID% Target Process: %PATH% %ARGUMENT% Parent Process 1: %PATH% %ARGUMENT% Parent Process 2: %PATH% %ARGUMENT% Parent Process 3: %PATH% Parent Process 4: %PATH% %ARGUMENT%
784	Information	anomaly_detect	DLL Injection Prevention Enabled	
1280	Information	device_control	Device Control Enabled	
1281	Information	device_control	Trusted USB Device Added	Vendor ID: %HEX% Product ID: %HEX% Serial Number: %STRING% Type: permanent or one time

Event ID	Level	Category	Event Content	Event Details
1282	Information	device_control	Trusted USB Device Removed	Vendor ID: %HEX% Product ID: %HEX% Serial Number: %STRING%
4352	Warning	system	Service stopped	
4353	Warning	system	Unable to apply policy (Version: %version%)	
4609	Warning	intelli_av	Incoming Files Scanned, Action Taken by Antivirus: %PATH%	Incoming files were scanned by antivirus. Actions were taken according to settings. File Path %PATH% File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING% Action Result: %INTEGER% Quarantine Path: %PATH%
4610	Warning	intelli_av	Incoming Files Scanned, Action Taken by Next-Generation Antivirus: %PATH%	Incoming files were scanned by next-generation antivirus. Actions were taken according to settings. File Path: %PATH% File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING% Action Result: %INTEGER% Quarantine Path: %PATH%
4612	Warning	intelli_av	Local Files Scanned, Action Taken by Next-Generation Antivirus: %PATH%	Local files were scanned by next-generation antivirus. Actions were taken according to settings. File Path: %PATH% File Hash: %STRING% Threat Type: %STRING%

Event ID	Level	Category	Event Content	Event Details
				Threat Name: %STRING% Action Result: %INTEGER% Quarantine Path: %PATH%
4613	Warning	intelli_av	Suspicious Program Execution Blocked: %PATH%	Suspicious program execution was blocked. File Path: %PATH% File Hash: %STRING%
4614	Warning	intelli_av	Suspicious Program Currently Running: %PATH%	Suspicious program is currently running. Process Id: %PID% File Path: %PATH% File Hash: %STRING% File Credibility: %STRING%
4615	Warning	intelli_av	Application Execution Blocked By Antivirus: %PATH%	Application execution was blocked by antivirus. Target Process: %PATH% File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING%
4617	Warning	intelli_av	Application Execution Blocked By Next-Generation Antivirus: %PATH%	Application execution was blocked by next-generation antivirus. Target Process: %PATH% File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING%
4864	Warning	anomaly_detect	Operations Behavior Anomaly Detection Disabled	

Event ID	Level	Category	Event Content	Event Details
4865	Warning	anomaly_detect	Process Allowed by Operations Behavior AnomalyDetection: %PATH% %ARGUMENT%	Access User: %USERNAME% Parent Process 1: %PATH% %ARGUMENT% Parent Process 2: %PATH% %ARGUMENT% Parent Process 3: %PATH% %ARGUMENT% Parent Process 4: %PATH% %ARGUMENT% Mode: %Mode%
4866	Warning	anomaly_detect	Process Blocked by Operations Behavior Anomaly Detection: %PATH% %ARGUMENT%	Access User: %USERNAME% Parent Process 1: %PATH% %ARGUMENT% Parent Process 2: %PATH% %ARGUMENT% Parent Process 3: %PATH% %ARGUMENT% Parent Process 4: %PATH% %ARGUMENT% Mode: %Mode%
4880	Warning	anomaly_detect	DLL Injection Prevention Disabled	
5120	Warning	change_control	ICS File Change Blocked by SafeGuard: %PATH%	ICS File change to executable file were blocked by SafeGuard. Blocked Process: %PATH% Target File: %PATH%

Event ID	Level	Category	Event Content	Event Details
5121	Warning	change_control	ICS Process Manipulation Blocked by Safeguard: %PATH%	ICS Process manipulation were blocked by Safeguard: Blocked Process: %PATH% Target Process: %PATH%
5376	Warning	device_control	Device Control Disabled	
5377	Warning	device_control	USB Access Blocked: %PATH%	Access Image Path: %PATH% Access User: %USERNAME% Vendor ID: %HEX% Product ID: %HEX% Serial Number: %STRING%
8706	Critical	intelli_av	Real Time Scan Disabled	
9216	Critical	change_control	Maintenance Mode Start	
9217	Critical	change_control	Maintenance Mode End	

StellarProtect Server Event Log Descriptions

Server Event Log Descriptions

ID	Content
33027	Switch agent (%s) to policy mode
33028	Switch agent (%s) to individual mode
33029	Deploy policy with version: %s
33041	Modify in common use (DLL Injection Prevention, USB Vector Control, ICS 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 USB Vector Control list for [%s] group policywith version: %s
33045	Maintain User Defined Suspicious Object list for [%s] group policy with version: %s
33046	Maintain Operations Behavior Anomaly Detection Watch Listfor [%s] group policy with version: %s
33047	Maintain Trusted Certification list for [%s] group policywith version: %s
33048	Maintain ICS Application Safeguard list for [%s] group policywith version: %s

33049	Modify agent password for [%s] group policy with version: %s
33050	Modify available patch setting for [%s] group policy with version: %s
33105	Send individual command to agent (%s)
33106	Send protection command <Configure Change Window> to agents
33107	Send protection command <Scan Now> to agents
33108	Send protection command <Update Component> to agents
33109	Send protection command <Apply Patch> to agents
33121	Send event action to agent (%s)
37122	Set activation code with policy version: %s
37123	Active agents
37124	Inactive agents

StellarOne Server Event Log Descriptions

Server Event Log Descriptions

ID	Content
45313	Scan component update now
45314	Scan component [%s] update job was 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 needed
45321	Scan component [%s] update was failed with internal error
45322	Scan component [%s] update was failed due to unable to connect to the network
45323	Customize policy
45324	Inherit policy from [%s]

Chapter 9

Technical Support

TXOne Networks is a joint venture of Trend Micro and Moxa, and support for TXOne Networks products is provided by Trend Micro. All technical support goes through Trend Micro engineers.

This chapter includes information about troubleshooting, contacting Trend Micro, sending suspicious content to Trend Micro, and other resources.

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 24/7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to <http://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/sign-in>

A Trend Micro support engineer will investigate the case and respond 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 combat 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/> 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

In the United States, Trend Micro representatives are available byphone or email:

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

- Worldwide support offices: <http://www.trendmicro.com/us/about-us/contact/index.html>
- TXOne product documentation: <http://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 TXOne:

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

File Reputation Services

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

<http://esupport.trendmicro.com/solution/en-us/1059565.aspx>

Please 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):

<http://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 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:

<http://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.

Documentation Feedback

TXOne always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any TXOne document, please go to the following site:

<http://www.trendmicro.com/download/documentation/rating.asp>



TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: APEM19539/220624