



1.1 TXOne StellarOne™ for StellarProtect

Administrator's Guide

All-terrain protection for mission critical assets

Windows



Endpoint Security

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>

© 2020 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.: SLEM19395/210826

Release Date: September 2021

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 may be 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	13
Introduction	13
About the TXOne™ Stellar™ series and StellarOne™	14
Agent Features and Benefits	15
What's New	16
System Migration	17
Chapter 2	20
Agents	20
Managing StellarProtect Devices	21
Group Management	22
View ICS Items	30
Policy Management	31
Device Action Commands	49
Chapter 3	53
Dashboard, Events, and Logs	53
Overview	54
Dashboard	55

StellarProtect Top Endpoints with Blocked Events.....	55
StellarProtect Top Blocked Files	58
CPU Usage.....	59
Memory Usage.....	59
Disk Usage.....	60
Events.....	61
Agent Events	63
Server Events	69
System Logs.....	73
Audit Logs.....	76
Chapter 4.....	80
Administration	80
Overview	81
Account Management	82
Single Sign-On	88
System Time	89
Proxy	92
Downloads / Updates.....	95
SSL Certification	99

License	100
Specify Activation Code	102
Seat Count	102
Log Purge	103
Automatic Purge.....	103
Syslog Forwarding	104
SMTP Settings	104
Notification	106
Warning Level Agent Events	106
Outbreak	106
Firmware	107
<i>Chapter 5</i>	<i>108</i>
Log Description Reference	108
StellarProtect Agent Event Log Descriptions	109
StellarProtect Server Event Log Descriptions	116
StellarOne Server Event Log Descriptions	118
<i>Chapter 6</i>	<i>119</i>
Technical Support.....	119

Troubleshooting Resources.....	120
Using the Support Portal	120
Threat Encyclopedia	121
Contacting Trend Micro	121
Speeding Up the Support Call	122
Sending Suspicious Content to Trend Micro	123
Email Reputation Services.....	123
File Reputation Services	124
Web Reputation Services	124
Other Resources.....	125
Download Center	125
Documentation Feedback.....	125

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, file names, and program output
Navigation > Path	The navigation path to reach a particular screen For example, File > Save means, click File and then click Save on the interface
 Note	Configuration notes
 Tip	Recommendations or suggestions
 Important	Information regarding required or default configuration settings and product limitations
 WARNING	Critical actions and configuration options

Terminology

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

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: <ol style="list-style-type: none">1. Account Management2. Single Sign-On3. System Time4. Proxy5. Downloads / Updates6. SSL Certification7. License8. Log Purge9. Firmware

What's New

TXOne StellarOne 1.1 includes the following new features and enhancements.

Table 2-2. What's New in TXOne StellarOne 1.1

Feature	Description
Group RBAC	StellarOne now supports defining account privileges by selected groups.
SAML SSO	StellarOne now includes Windows AD Authentication via SAML SSO.
Proxy settings enhancement	Proxy settings for StellarOne to connect to the internet can now be customized.
Update source enhancement	The StellarProtect and StellarEnforce Agents can now be updated from either Trend Micro Active Update or StellarOne.
StellarOne self-update	A new interface was added to allow future updates to be carried out within StellarOne without conducting a system migration.
StellarOne web console certificate updates	StellarOne's web console certificate can now be updated.

System Migration



Important

StellarOne must be upgraded before the StellarProtect agent is upgraded.

For StellarOne 1.1, a feature was added to allow the migration of settings of StellarOne 1.0 into StellarOne 1.1. This is done by attaching the external disk of the old instance of StellarOne 1.0 to the new StellarOne 1.1 instance. The migration of settings can include:

- The UUID
- System configurations including license, account information, security policies, and so on
- Security event logs

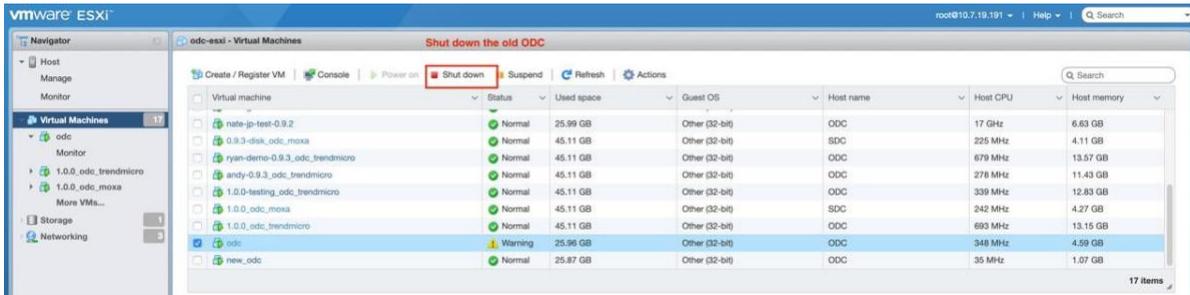


Important

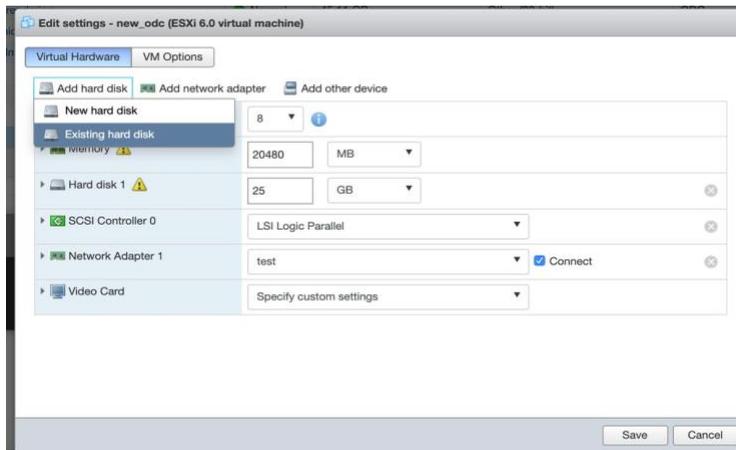
Before conducting a system migration, please take a VMware snapshot or back up your StellarOne data.

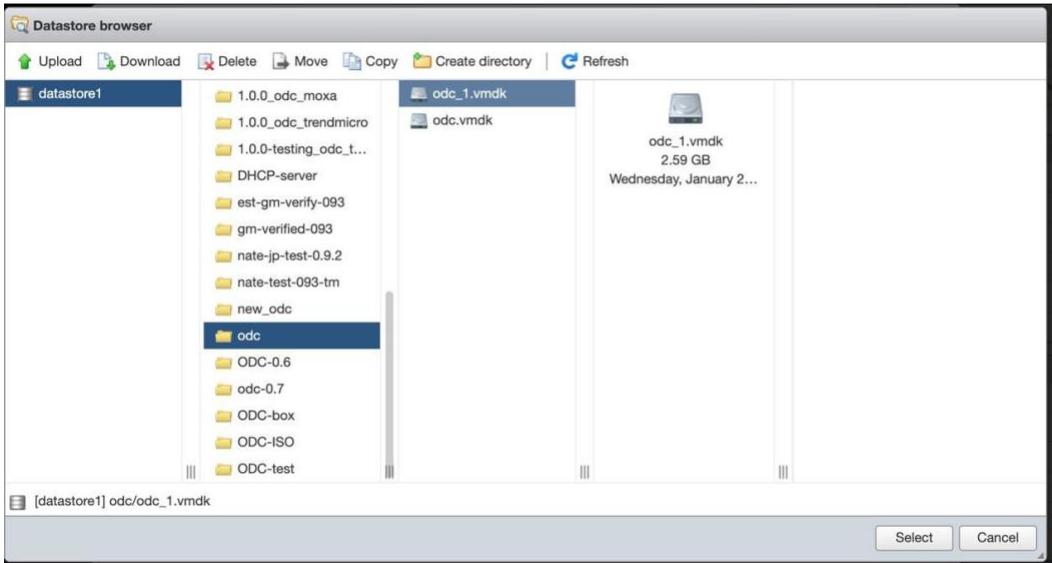
Procedure

1. Launch the new StellarOne instance (refer to section “Deploying StellarOne”).
2. Close the old instance of StellarOne.



3. Attach the external disk of the old StellarOne to the new StellarOne.





4. The information from the old instance of StellarOne will be migrated into the new instance of StellarOne.
5. Check and, if necessary, configure the IP address of the new StellarOne to be the same as the IP address for the old instance of StellarOne. After this is configured, communications between the new instance of StellarOne and agents will be reconnected and proceed as normal. The next time agents sync their status, they will report to the new StellarOne. By default, agents will sync every 20 minutes.
6. If the proxy or scan component update source is already defined in the old instance of StellarOne, please define it again in the UI of the new instance of StellarOne.

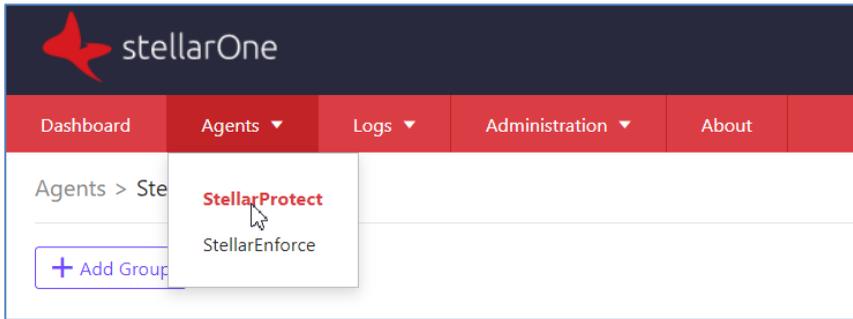
Chapter 2

Agents

This chapter introduces how to manage StellarProtect agents through StellarOne.

Managing StellarProtect Devices

While StellarOne can manage StellarProtect and StellarEnforce devices, this administration guide is focused on StellarProtect devices.



StellarProtect devices can be managed from Agents > StellarProtect.

The device installs StellarProtect, which it will then register to StellarOne automatically. It will then be listed under All Agents.

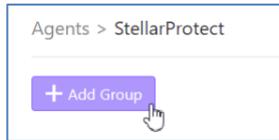
These agents will be managed with global policy. You can also create groups of agents (each endpoint is considered as an “agent” managing the endpoint) and then configure those groups with group policies.

Group Management

Group management is a policy-oriented management mechanism. You can select some devices in the group as well as configure policies by group.

Add a New Group

Please click 'Add Group' to create a new group.

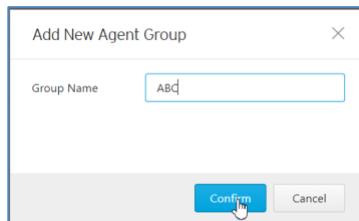


Then, you can enter the group name according to the dialog box, and then click 'Confirm' to complete the group creation.



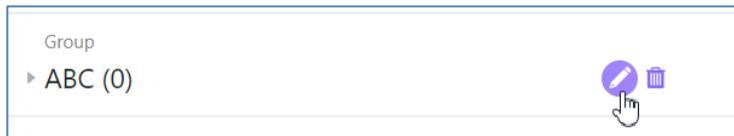
Note

Group names cannot be the same as the system default group name.

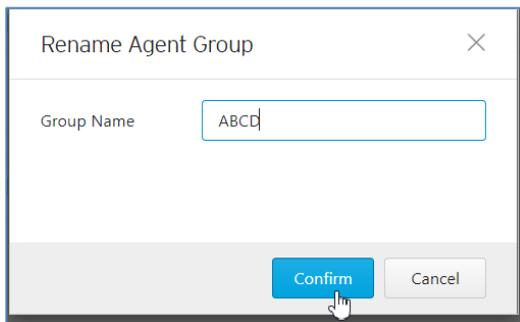


Rename a Group

If you need to modify the name of the group, click the pencil icon of the group as shown below.



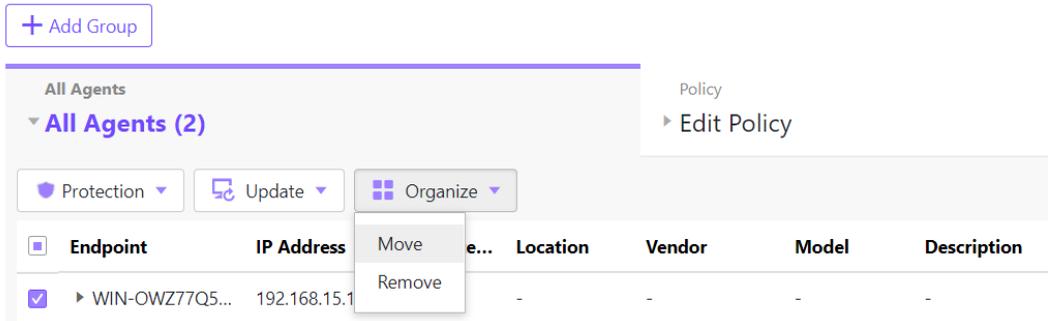
After entering the new name, click 'Confirm' to complete the group name modification.



Move a Device to a Group

If you want to move any device to an existing group, click the 'Organize' icon and select 'Move'.

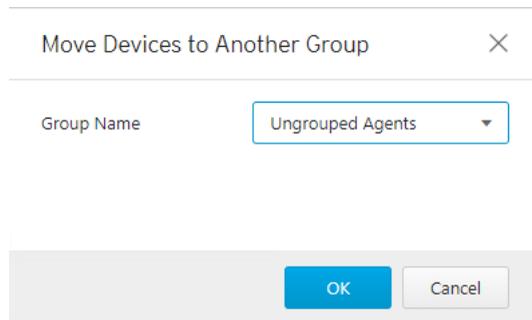
Agents > StellarProtect



The screenshot shows the StellarProtect interface. At the top left, there is a '+ Add Group' button. Below it, the 'All Agents' section is expanded to show 'All Agents (2)'. To the right of this section, there is a 'Policy' dropdown menu with an 'Edit Policy' option. Below the 'All Agents' section, there are three buttons: 'Protection', 'Update', and 'Organize'. The 'Organize' button is open, showing a dropdown menu with 'Move' and 'Remove' options. Below the buttons is a table with columns: Endpoint, IP Address, Location, Vendor, Model, and Description. The first row in the table is selected, and the 'Move' option is highlighted in the dropdown menu.

Endpoint	IP Address	Location	Vendor	Model	Description
WIN-OWZ77Q5...	192.168.15.1	-	-	-	-

Then, you can select a group name from the drop-down list.

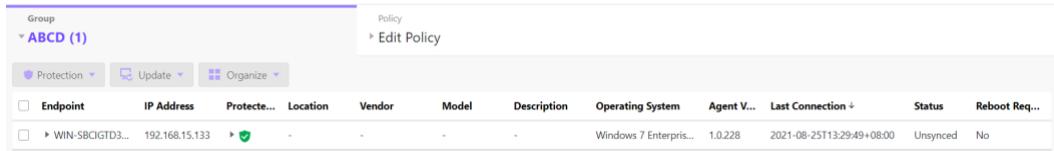


The screenshot shows a dialog box titled 'Move Devices to Another Group'. It has a close button (X) in the top right corner. Below the title, there is a 'Group Name' label and a dropdown menu. The dropdown menu is open, showing 'Ungrouped Agents' as the selected option. At the bottom of the dialog box, there are two buttons: 'OK' and 'Cancel'.

Click the **OK** button to confirm the settings.

Expand a Group

When all default values of the group have been collapsed, you can click on the group name and the group will expand as shown below:

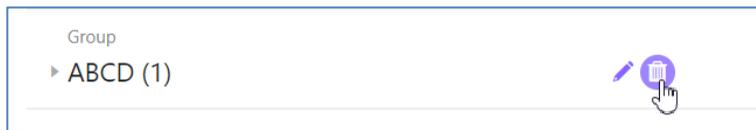


The screenshot shows a user interface for managing a group. At the top, there is a 'Group' header with a dropdown arrow next to 'ABCD (1)'. To the right, there is a 'Policy' section with an 'Edit Policy' link. Below these are three buttons: 'Protection', 'Update', and 'Organize'. A table below displays the group's details. The table has columns for Endpoint, IP Address, Protection Status, Location, Vendor, Model, Description, Operating System, Agent Version, Last Connection, Status, and Reboot Requirement. The first row shows a group named 'WIN-SBCIGTD3...' with IP address '192.168.15.133', a green checkmark for protection, and various system details.

Endpoint	IP Address	Protecte...	Location	Vendor	Model	Description	Operating System	Agent V...	Last Connection +	Status	Reboot Req...
▶ WIN-SBCIGTD3...	192.168.15.133	▶	-	-	-	-	Windows 7 Enterpris...	1.0.228	2021-08-25T13:29:49+08:00	Unsynced	No

Delete a Group

You can click the recycle bin icon of a group to delete the group.



Device Information

If you want to look at device information, you can click the device name and the listing will expand as shown below.

Endpoint	IP Address	Protecte...	Location	Vendor	Model	Description	Operating System	Agent V...	Last Connection	Status	Reboot Req...
WIN-OWZ77Q5...	192.168.15.129		-	-	-	-	Windows Server 200...	1.1.1089	2021-08-25T09:38:13+08:00	Synced	No

ICS Applications (5)			
Software	Vendor	Version	Install Path
Beckhoff TwinCAT Multiuser	Beckhoff Automation	1.0.9.0	C:\TwinCAT\Func...
TF5210-CNC-Export	Beckhoff Automation	3.1.3070.0	C:\TwinCAT\Func...
Beckhoff TwinCAT 3.1 (Build 4024)	Beckhoff Automation	3.1.4024.10	C:\TwinCAT\
Beckhoff TwinCAT Multiuser Git	Beckhoff Automation	1.0.5.0	C:\TwinCAT\Func...
Bürkert Communicator	Bürkert	5.0	C:\Program Files...

ICS Certificates (2)		
Issued To	Issued By	Hash
Beckhoff Automation ...	DigiCert SHA2 High A...	8020A777057887B7A5FD0B17DEE9711954F0FE4A
Buerkert Werke Gmb...	Sectigo RSA Code Sig...	75E681DD8DA601AD298C1DC18C075B59DDE0...

System Information	
Operating System	Windows Server 2008 Datacenter Edition Service Pack 2 (build 6002), 32-bit
Group	Ungrouped Agents
License status:	Activated
License version:	Trial
License expired on:	2021-12-31
Agent version:	1.1.1089

Scan Components	
Virus Pattern	16.581.00
IntelliTrap Exception Pattern	1.797.00
IntelliTrap Pattern	0.253.00
Spyware/Grayware Pattern	2.385.00
Behavior Monitoring Configuration Pattern	1.235.00
Advanced Threat Correlation Pattern	1.194.00
Predictive Machine Learning Local File Model	1.513.00
Advanced Threat Scan Engine (32-bit)	12.5.0.1004

Device information includes the following:

- ICS Applications
- ICS Certificates
- System Information
- Scan Component
- Reboot Required

ICS Applications

Under 'ICS Applications', the ICS applications currently installed on the device will be displayed, along with the software name, vendor, version, and installation path of the application.

This information allows the user to identify ICS applications for management.

ICS Applications (1) 			
Software ↓	Vendor	Version	Install Path
ABB TuneMaster	ABB	6.11.0151	C:\Program Files (x86)\ABB\TuneMa...

ICS Certificates

The trusted certificates installed on the device are displayed here. Certificates listed here are the ICS certificates that StellarOne can recognize.

ICS Certificates (2)		
Issued To	Issued By	Hash
Schneider Electric	VeriSign Class 3 Code Signing 20...	48A5F6877981E02CEFF63FD0E172CA1BB5AF1015
Schneider Electric	VeriSign Class 3 Code Signing 20...	E776B9C503D4A045433372BD52A13D2E11C19D11

System Information

Under 'system information' you can find the operating system, group, license status, license version, license expiration date, agent version, and the date

on which the agent was last upgraded.

System Information

Operating System	Windows 7 Enterprise Edition Service Pack 1 (build 7601), 32-bit
Group	ABCD
License status:	Activated
License version:	Trial
License expired on:	2021-12-31
Agent version:	1.0.228

Scan Components

Under 'scan components', versions are listed for engines and patterns used in security scans.

Scan Components	
Virus/Malware Pattern	16.581.00
IntelliTrap Exception Pattern	1.797.00
IntelliTrap Pattern	0.253.00
Spyware/Grayware Pattern	2.385.00
Behavior Monitoring Configuration Pattern	1.235.00
Advanced Threat Correlation Pattern	1.194.00
Predictive Machine Learning Local File Model	1.513.00
Advanced Threat Scan Engine (64-bit)	12.5.0.1004

Reboot Required

Some version upgrades for the agent will include a driver update, which will require the system to be restarted once the update is complete. This column is here to remind the user to restart the device when it's necessary after an update.

View ICS Items

If you want to browse all current ICS application systems and certificates, you can click 'View ICS Items' to view the recognized ICS applications and the certificates of all devices currently managed by StellarOne.

The screenshot shows the StellarOne interface with two main sections: 'ICS Applications (6)' and 'ICS Certificates (2)'. The 'ICS Applications' section contains a table with columns for Software, Vendor, and Version. The 'ICS Certificates' section contains a table with columns for Issued To, Issued By, and Hash. A 'View ICS Items' link is visible in the top right corner.

Software	Vendor	Version
SMARTDAC+ Data Logging Software	Yokogawa Electric Corporation	3.7.3
Fisher® Specification Manager	Fisher Controls International LLC	2.20.00
Winflows	GE	1.1.37
CitectSCADA 7.20	Schneider Electric	7.20.0000
FANUC LADDER-III	FANUC	1.00.000
Common Licensing	GE Digital	00019.00002.01725.00000

Issued To	Issued By	Hash
Schneider Electric	VeriSign Class 3 Code Signing 20...	E776B9C303D4AD4543372B052A13D0E11C19D11
Schneider Electric	VeriSign Class 3 Code Signing 20...	4BA3F8B77981E02CEFF63FD9E172CA18E5AF1015

ICS Applications

Under 'ICS Applications', ICS software name, vendor and version will be listed. This will include all versions currently in use.

ICS Applications (6)		
Software	Vendor	Version
SMARTDAC+ Data Logging Software	Yokogawa Electric Corporation	3.7.3
Fisher® Specification Manager	Fisher Controls International LLC	2.20.00
Winflows	GE	1.1.37
CitectSCADA 7.20	Schneider Electric	7.20.0000
FANUC LADDER-III	FANUC	1.00.000
Common Licensing	GE Digital	00019.00002.01725.00000

ICS Certificates

This will list all the certificates trusted by StellarOne, and display the issuing unit ('Issued by'), certificate owner ('Issued to'), and hash value of each certificate.

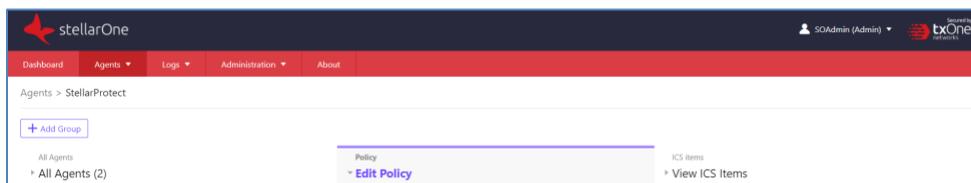
ICS Certificates (2)		
Issued To	Issued By	Hash
Schneider Electric	VeriSign Class 3 Code Signing 20...	E776B9C503D4A04543372BD52A13D2E11C19D11
Schneider Electric	VeriSign Class 3 Code Signing 20...	48A5F6877981E02CEFF63FDFE172CA18B5AF1015

Policy Management

Policies are divided into global policies and group policies. Global policies apply to all devices, while group policies apply to specific groups. If the group policy is different from the global policy, the group policy will take precedence.

Global Policy

The global policy applies to all devices and contains various settings. Click **Edit Policy** next to **All Agents** to set global policy.



The following figure shows the global policy settings, including:

- Industrial-Grade Next-Generation Antivirus
- USB Vector Control

- User-Defined Suspicious Objects
- DLL Injection Protection
- Agent Password
- Operations Behavior Anomaly Detection
- ICS Application Safeguard
- Trusted Certificates
- Patch

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

Schedule Scan [Schedule](#)

[Advanced Options](#)

USB Vector Control

Allow only trusted USB devices by vendor ID, serial number, and product ID.

Trusted USB devices list:

[+ Add](#)

Vendor ID	Product ID	Serial Number	Actions
No data to display.			

User-Defined Suspicious Objects

Protect agent objects not yet on your network.

[+ Add](#)

Hash / File Path	Type	Notes	Actions
No data to display.			

ICS Application Safeguard

Protect files, folders or registry from unauthorized changes
 Protect ICS applications

DLL Injection Protection

Enable DLL Injection Protection

Agent Password

New Password?

Operations Behavior Anomaly Detection Watchlist

[+ Add](#)

Monitored Process	Actions
No data to display.	

Trusted Certificates (0)

[+ Import](#)

Issued To	Issued By	Hash	Actions
No data to display.			

Patches

Apply the following patch in this group:

File Name	Version
No data to display.	

You can import new patches for the agent on the [Upload](#) page.

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 [Schedule](#)

> [Advanced Options](#)

Real-Time Scan

When 'Real-Time Scan' is enabled, all devices will activate real-time virus protection. File access and process creation will trigger security scanning.

Advanced Threat Scan

You can click **Advanced Threat Scan** to enable aggressive antivirus protection.

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  Schedule

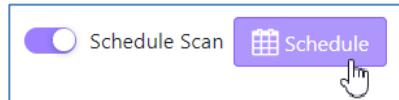
> **Advanced Options**

Important

Advanced Threat Scan is configured to support all scan types, included scheduled scans.

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

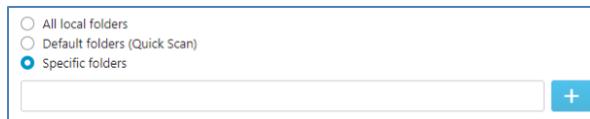
You can configure the following settings for industrial-grade next-generation antivirus under ‘advanced options’:

- 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 screenshot shows a settings panel 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, indicated by a blue dot. Below the radio buttons is a text input field and a blue button with a white plus sign.

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

Select files, folders or extensions to exclude from scans.

Folders:



Files:

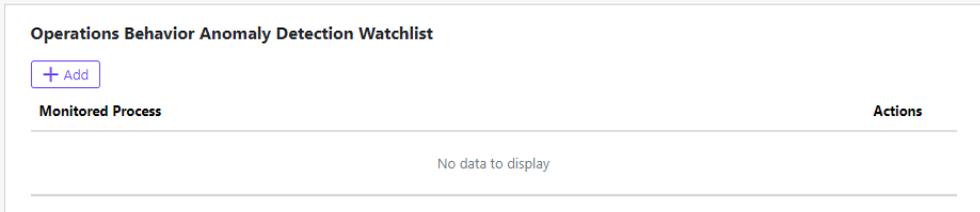


File extensions:



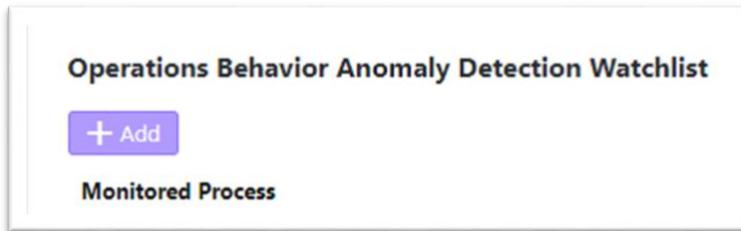
Operations Behavior Anomaly Detection

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

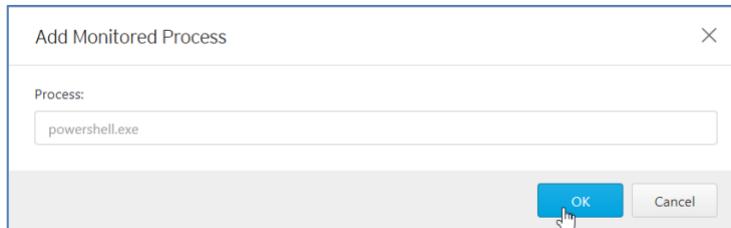


Monitored Processes

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.



USB Vector Control

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

USB Vector Control

Allows only trusted USB devices by vendor ID, serial number, and product ID

Trusted USB Device List:

[+ Add](#)

Vendor ID	Product ID	Serial Number	Actions
No data to display			

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

OK Cancel

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

USB Vector Control

Allows only trusted USB devices by vendor ID, serial number, and product ID

Trusted USB Device List:

[+ Add](#)

Vendor ID	Product ID	Serial Number	Actions
4c5	1526	11f79522	

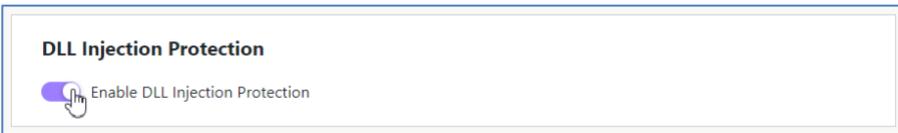
DLL Injection Protection

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'.



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.

User-Defined Suspicious Objects

Protect against objects not yet on your network:

[+ Add](#)

Hash / File Path	Type	Notes	Actions
No data to display			

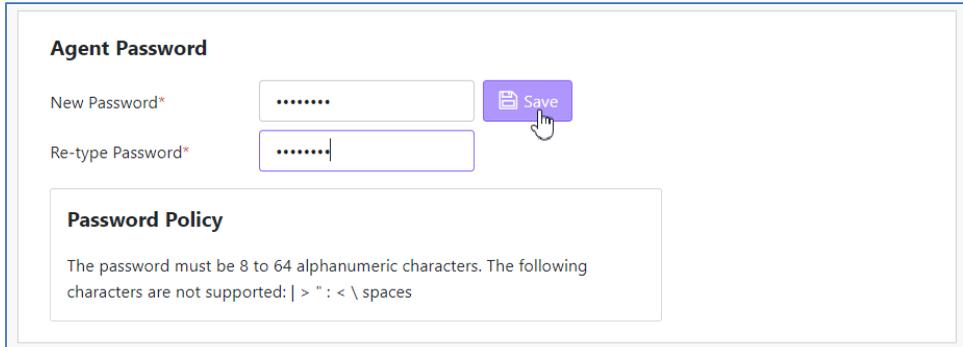
Agent Password

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.



The screenshot shows a web interface for configuring an Agent Password. It features two input fields for 'New Password*' and 'Re-type Password*', both containing masked characters. A purple 'Save' button is positioned to the right of the first field, with a mouse cursor hovering over it. Below the input fields is a 'Password Policy' section with a text box containing the following text: 'The password must be 8 to 64 alphanumeric characters. The following characters are not supported: | > " : < \ spaces'.

ICS Application Safeguard

ICS Application Safeguard is industrial-based change control protection.

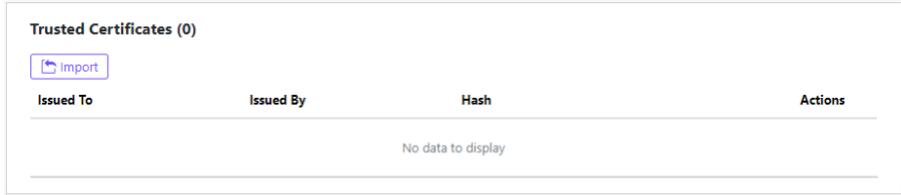
Users can enable this protection to make sure StellarProtect-recognized ICS applications can be updated without being blocked or restricted.

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

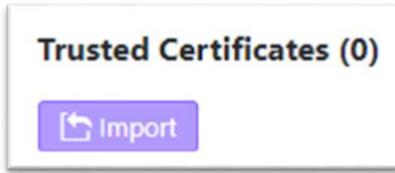
Trusted Certificates

The policy **Trusted Certificates** provides an import function allowing

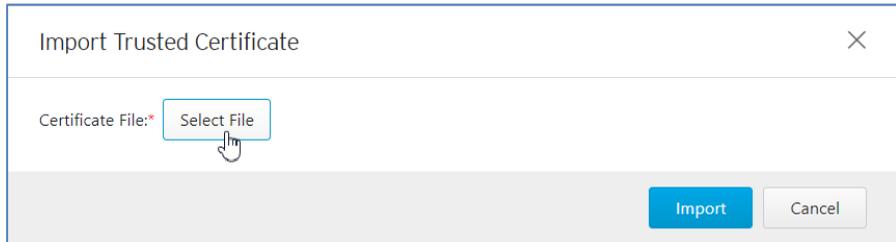
the administrator to add new trusted certificates.



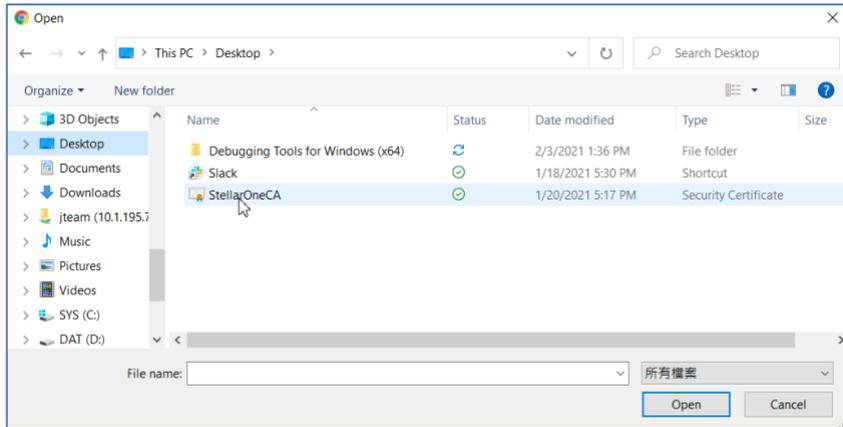
Click the 'Import' icon to import a new trusted certificate.



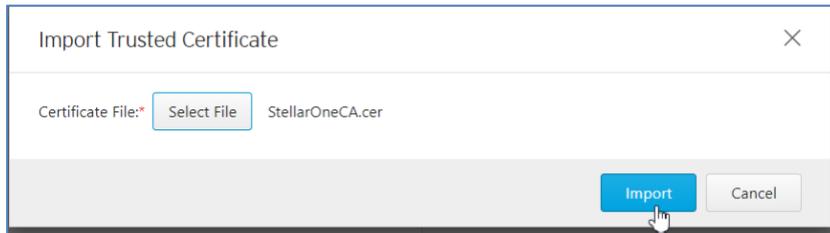
Click 'Select File' to browse certificate files.



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	<input type="button" value="Remove"/>

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 and patches listed will be filtered based on the current agent version – only valid patches for current agents will be displayed.



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. Group policy will be applied after an agent is moved to a group. If a group's policy is set to an agent version lower than that of the global policy, StellarOne will be unable to apply the patch. StellarOne only shows agent versions which are higher than or equal to that of the current endpoint, so we suggest setting higher agent versions using group policy.
3. 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.

Group Policy

StellarOne uses global policy by default. The administrator can also decide to disable group policy.

Group Policy privilege is higher than Global Policy.

If you would like to configure the Group Policy, please click 'Edit Policy' on any group.

Individual Setting

If you change individual agent settings using the send agent command or local configuration, the individual agent setting will be kept until the settings are disabled.

Device Action Commands

Protection

Configure Change Window

The change window is necessary for changes in ICS endpoint operations. During the change window, all newly-added files will be updated through real-time virus scanning. StellarProtect can then learn updated or newly added applications and ensure the execution of these newly updated applications under protected conditions. The user should perform the necessary application updates before the change window reaches its assigned time to close.

Please note, 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 virus patterns, check **Aggressive scan**.

The server will send a notification to the selected StellarProtect agents. You can check the logs for the scan status.

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 web console. The Agents screen will appear.
2. Select one or more endpoints.
3. Select **Protection > Update Agent Components**.
4. Click **OK**.

Update

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

5. Go to **Agents > StellarProtect**. The Agents screen will appear.
6. Select one or more agents.
7. Click **Update > Deploy Agent Patch**.
8. Select the available patch file for deployment. Only patches that are valid for the currently selected agent(s) will be displayed.
9. Click **OK**.

Organize

Move

Group agents according to location, type, or purpose to help you manage multiple agents.

Procedure

1. Go to **Agents** in the navigation at the top of the StellarOne console. The Agents screen will appear.
2. Select one agent, and then select **Organize > Move**.
3. Check the group list.
4. Select a group on the list, then click **OK**.

Remove

Remove agents from the StellarOne server.

StellarProtect will attempt to unregister agents from StellarOne during uninstallation. However, if StellarProtect is not connected to StellarOne, it will not be able to unregister the agents you are removing.

if you are unable to uninstall an agent before removing it from the environment, the agent may continue to appear on the Agents screen. To remove the endpoints that StellarOne no longer manages from the list of monitored agents, use the Remove feature to 'unregister' those agents.

Procedure

1. Go to **Agents** in the navigation at the top of the StellarOne console. The Agents screen will appear.
2. Select the endpoints in the list that you want to remove.
3. Click **Organize > Remove**.
4. Confirm that you want to remove the selected items. StellarOne will remove the selected agents from the list.

Chapter 3

Dashboard, Events, and Logs

This chapter introduces TXOne StellarOne event and log management.

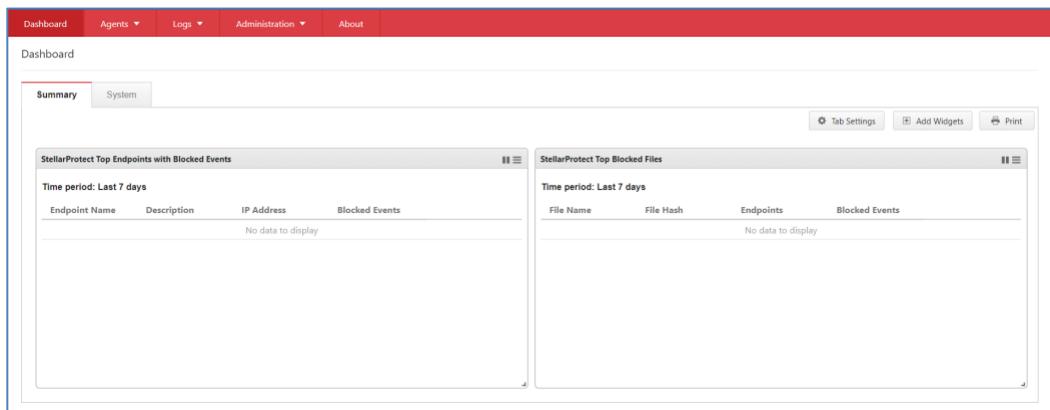
Overview

StellarOne provides a dashboard with 2 lists of events and 2 lists of logs for user reference including Agent Events, Server Events, System Logs and Audit Logs.

Dashboard

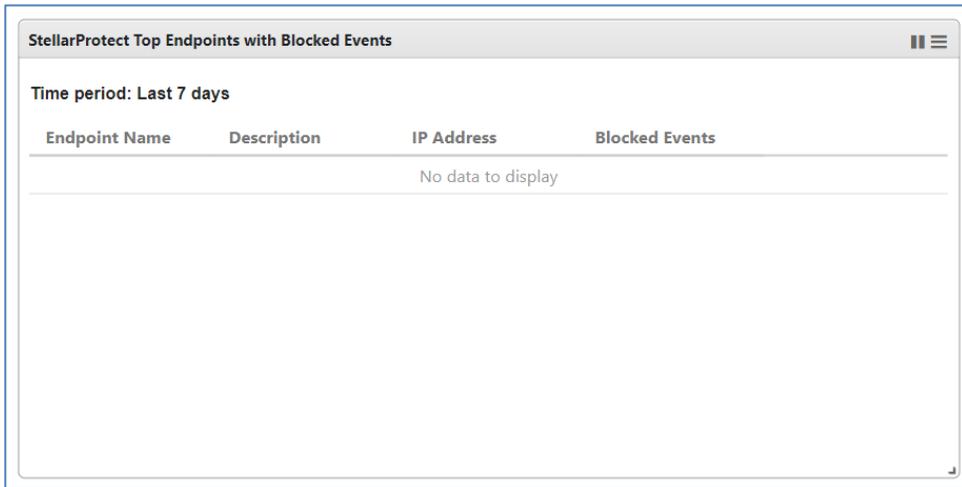
Monitor events from the Dashboard using the overview provided under the Summary tab. This tab is added to the Dashboard by default when there are no user-defined tabs.

StellarProtect widgets include Top Endpoints with Blocked Events, Top Blocked Files under the Summary tab, and then CPU Usage, Memory Usage and Disk Usage under the System tab. (Default widgets are StellarProtect Top Endpoints with Blocked Events, StellarEnforce Top Endpoints with Blocked Events, StellarEnforce Blocked Event History)



StellarProtect Top Endpoints with Blocked Events

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



Endpoint Name	Description	IP Address	Blocked Events
No data to display			

Column descriptions are as follows:

Column	Description
Endpoint Name	Name of the endpoint
Description	The endpoint description.
IP Address	IP address of the endpoint
Blocked Events	Total number of events blocked on the endpoint

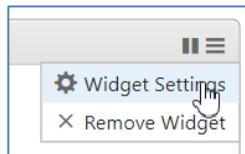
The dashboard will be refresh automatically. You can click the pause icon to stop the automatic refresh.



Click the start icon to enable the automatic refresh.



You can select the 'Widget Settings' for any dashboard widget.



You can change the widget name here, as well as configure the time period for shown data or auto refresh settings.

Widget Settings ✕

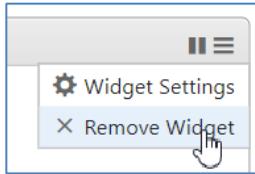
Widget Name: StellarProtect Top Endpoints with Blocked Events

Time period: Last 7 days ▼

Auto Refresh Settings: Every 30 Seconds ▼

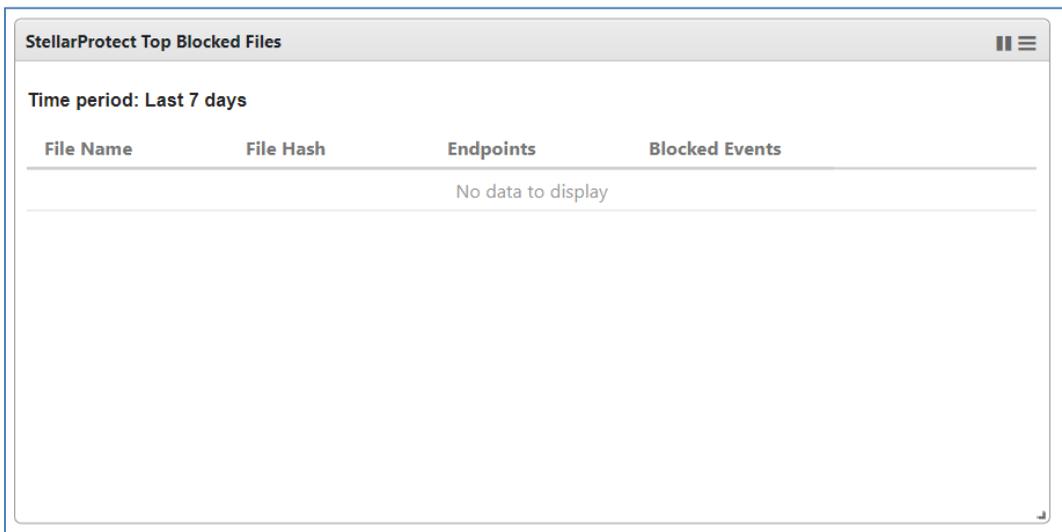
OK Cancel

If you need to remove a Widget, you can also find 'Remove Widget' here.



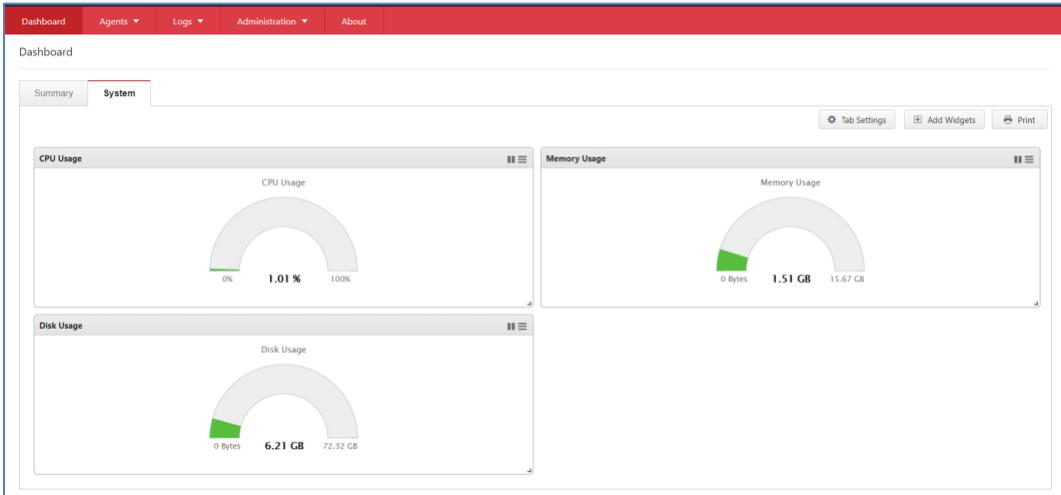
StellarProtect Top Blocked Files

This widget displays the endpoints with the most blocked files.



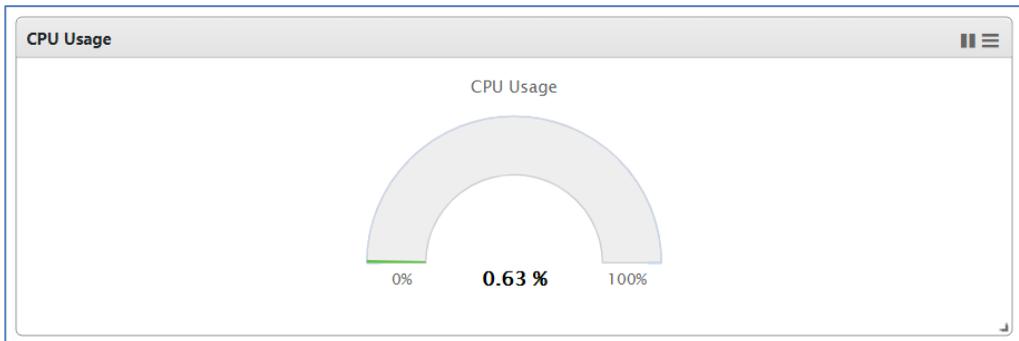
This widget will show the blocked file name, hash value (in SHA-2 standard), the endpoint's name, and any related blocked events.

There are 3 widgets for displaying StellarOne system status. By default, the widget is displayed on the **System** tab of the **Dashboard**.



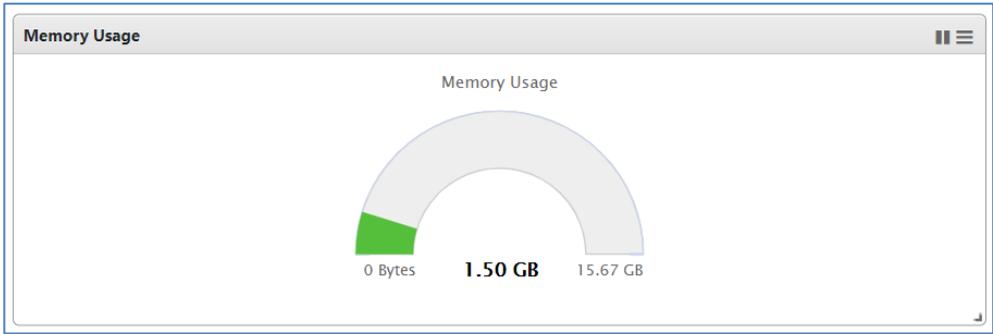
CPU Usage

This widget displays CPU usage information.



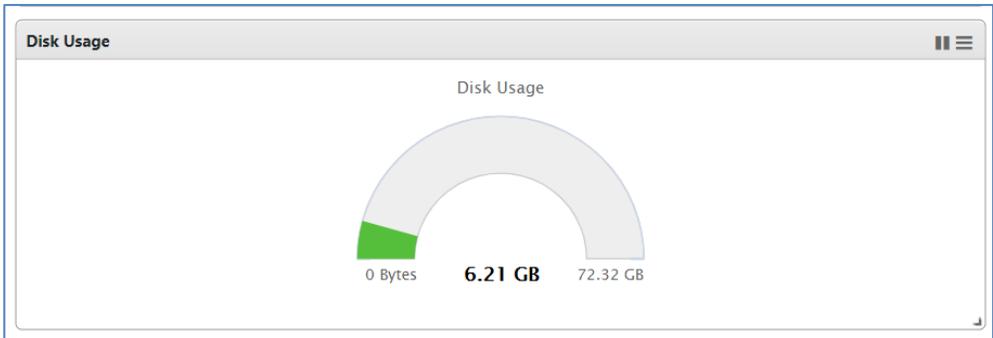
Memory Usage

This widget displays memory usage information.



Disk Usage

This widget displays disk usage information.



Events

StellarOne has 2 types of events and 2 types of logs, which provide users with analysis and management functions, especially intended for support usage after an incident. Using the notification function, an administrator or auditor can query and analyze events to quickly find the root cause of the problem.

The 2 types of events and 2 types of logs are as follows:

- Agent Events

When an event is triggered by a device, the event and device information will be sent to StellarOne. According to the severity, the events are classified as 'warning', 'critical', or 'information'. A 'warning' indicates that a serious security incident has occurred on the device and immediate action is recommended. 'Critical' indicates events related to changes in StellarProtect's settings as well as threat detection events where the user is suggested to take action. If action has been taken, it is recommended to check what happened, judge the current status of the situation, and perform any necessary further actions. The 'information' label refers to general events that usually do not compromise safety.

It is recommended to collect, analyze, and archive events regularly.

- Server Events

This event list shows StellarOne management events, especially events triggered by StellarOne management functions or automatic processing.

- System Logs

This is the system log of StellarOne, which includes information such as system time zone changes.

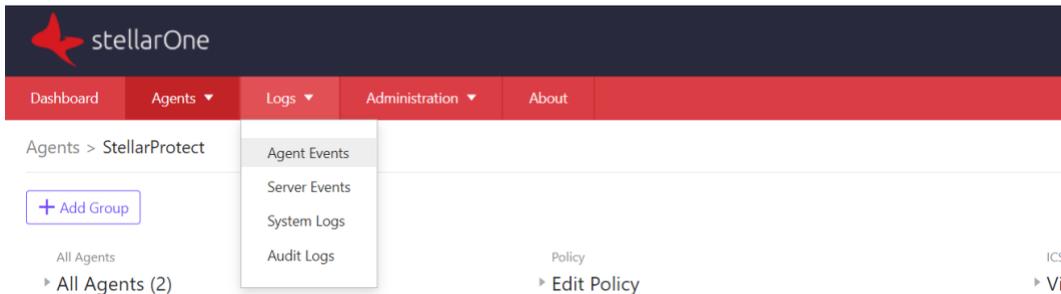
- Audit Logs

This includes logs related to StellarOne security audits, usually related to information security. This includes modifications to important parameters, account creation, account deletion, and password changes.

Agent Events

Event and device information will be sent to StellarOne periodically, which includes data about every time an event is triggered by the device. According to the severity, events will be labeled **information**, **warning**, **critical**. **Information** refers to general events that usually do not compromise safety. A **warning** indicates that a serious security incident has occurred on the device and immediate action is recommended. **Critical** indicates events related to changes in StellarProtect's settings as well as threat detection events where the user is suggested to take action. If action has been taken, it is recommended to check what happened, judge the current status of the situation, and perform any necessary further actions. If a modification is made, it is recommended to judge whether it is correct and perform post-processing.

It is recommended to collect, analyze, and archive logs regularly. You can check **Logs > Agent Events** to open event management.



When opening agent event management, you can check the **StellarProtect** and **StellarEnforce** tabs to change specific event and log settings or manage events and logs.

Please select StellarProtect and you will see the following list:

Logs > Agent Events

StellarProtect				StellarEnforce	
<input type="checkbox"/>	Time	Level	Event	Endpoint	Action
<input type="checkbox"/>	2021-02-24T17:48:04+08:00	Warning	5376 USB Vector Control disabled.	DESKTOP-7FQQDQV	View Details
<input type="checkbox"/>	2021-02-23T23:44:05+08:00	Information	768 CAD enabled.	DESKTOP-7FQQDQV	View Details
<input type="checkbox"/>	2021-02-23T23:43:41+08:00	Information	1280 USB Vector Control enabled.	DESKTOP-7FQQDQV	View Details
<input type="checkbox"/>	2021-02-23T16:43:35+08:00	Information	1280 USB Vector Control enabled.	DESKTOP-7FQQD02	View Details

Records: 1-4 / 4 100 per page 1 / 1 << < > >>

If you would like to check individual event details, please click the “View Details”.



Then you will have event details as follows:

Event Details ×

< 2021-04-27T16:19:04+08:00 >

Action

 Print

Event Information

Time	2021-04-27T16:19:04+08:00
Level	Information
Event ID	768
Event	Operations Behavior Anomaly Detection Enabled
Detail	Mode: OAD_MODE_PREVENTION Level: OAD_LEVEL_NORMAL

Agent Information

Endpoint	WIN-9G0J5LU86GJ
IP	192.168.15.147
Location	taipei
Vendor	SE
Model	PC Station
Description	-
Operating System	Windows Server 2016 Datacenter Edition (build 14393), 64-bit

Close

Events Details

Event details are as follows:

[Event Information]

1. Time

The event date and time, following the UTC standard format for date and time.

2. Level

Event severity level: 'warning', 'critical', or 'information'.

3. Event ID

The identification number of the event.

4. Event

A brief description of the event. It usually contains important environmental parameters, key activities, and results, some of which will have initiated a follow-up action.

5. Detail

The detailed description of the event, it includes agent side critical setting and details information.

[Agent Information]

1. Endpoint

The name of the device.

2. IP

IPv4 address of the endpoint.

3. Location

The physical location of the endpoint, usually entered in when StellarProtect is installed.

4. Vendor

The endpoint ICS application provider name.

5. Model

The model name or ID of the ICS product or application operating on the endpoint.

6. Description

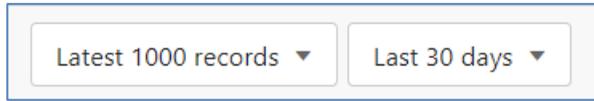
The description of the endpoint, which might include the ICS product critical description or relative information.

7. Operating System

The OS name with version.

Filtering & Refresh

You can filter events based on the number of records and time limit.



The event records will be updated automatically after you change the filter setting.

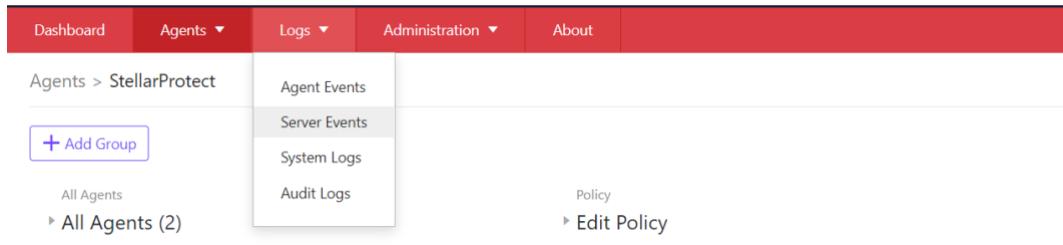
In addition, you can click the **refresh** icon to refresh the event list.



Server Events

This event list shows StellarOne management events, especially events triggered by StellarOne management functions or automatic processing.

You can select **Logs > Server Events**:



Events Details

The event details are:

1. Time

The event date and time, following the UTC standard format for date and time.

2. User Name

Which user triggered the event, or if it was an automatic event it will say **system**.

3. Event

A description of the event, including event ID.

4. Endpoint / [Group]

Endpoint name and its group name.

5. Status

The result of the server event.

<input type="checkbox"/>	Time	User Name	Event	Endpoint / [Groups]	Status
<input type="checkbox"/>	2021-02-24T11:00:00+08:00	System	3001 Automatic purge of agent event logs.		Successful
<input type="checkbox"/>	2021-02-24T11:00:00+08:00	System	3004 Automatic purge of server event logs.		Successful

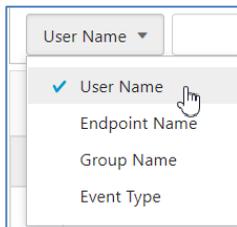


Note

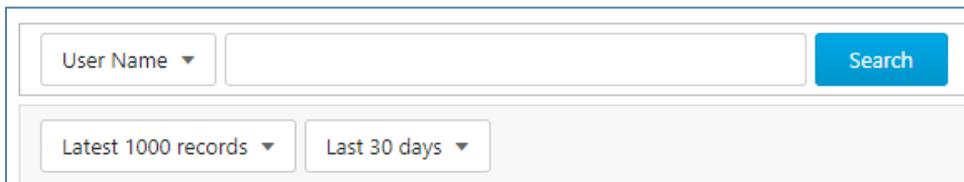
Server event logs contain collected information about actions taken by policies as well as StellarOne console users.

Search & Refresh

You can query events based on specific conditions including user name, endpoint name, group name and event type.



You can filter events using the number of records and a time limit.



Event records will be updated automatically after you change the filter settings.

You can click the 'refresh' icon to refresh the event list.

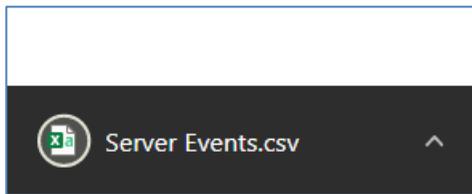


Export

If you would like to download the events you queried, please click the download icon.



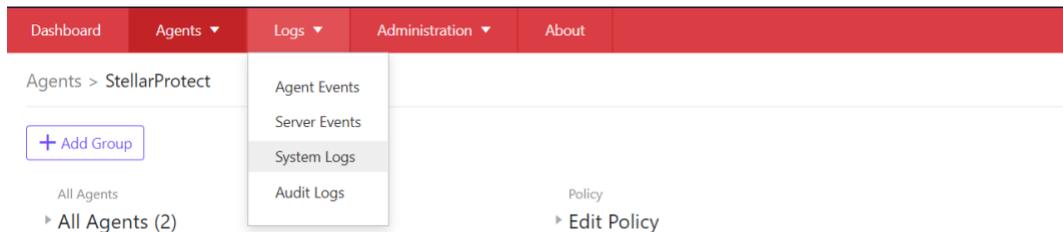
A file named "Server Events.csv" will be prepared for export.



System Logs

This shows the system logs for StellarOne.

You can select Logs > System Logs:



Logs Details

Details are shown as follows:

1. Time

The event date and time, it following the UTC standard format for date and time.

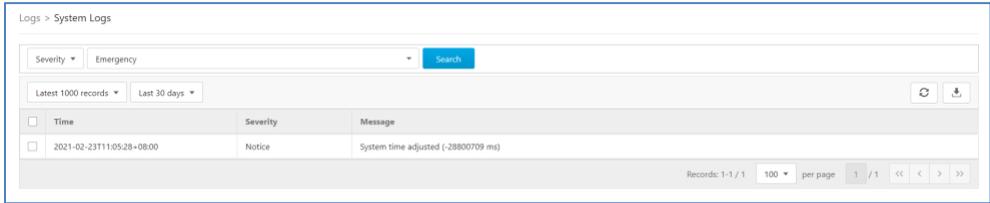
2. Severity

Severity labels include eight different types. These types are **'Emergency'**, **'Alert'**, **'Critical'**, **'Error'**, **'Warning'**, **'Notice'**, **'Information'** and **'Debug'**.

3. Message

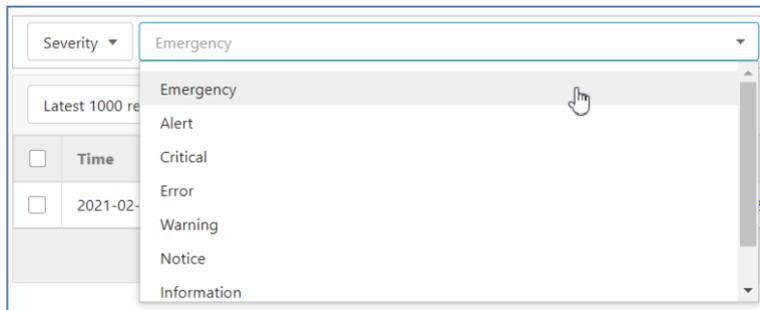
This will be the log message content, which will contain important

environmental parameters, key activities, and results.

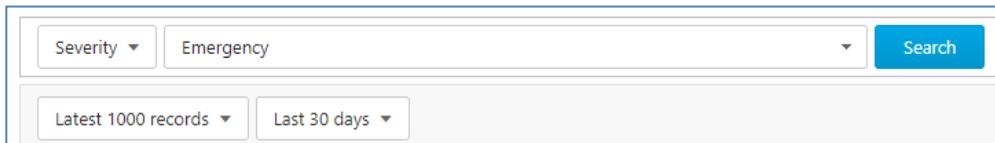


Search & Refresh

You can query events based on severity with different classifications. These types are 'Emergency', 'Alert', 'Critical', 'Error', 'Warning', 'Notice', 'Information' and 'Debug'.



Similarly, you can filter events using the number of records and time limit.



The event records will be updated automatically after you change the filter setting.

You can click the 'refresh' icon to refresh the event list.

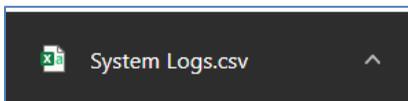


Export

If you would like to download the events you queried, please click the download icon.

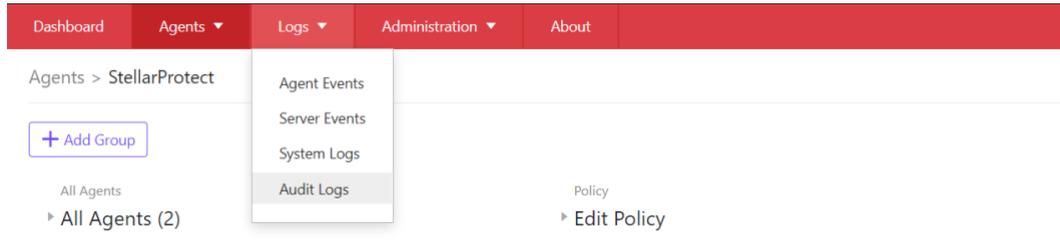


A file named "Server Events.csv" will be prepared for export.



Audit Logs

Under audit logs will be logs related to the StellarOne security audit, usually related to information security. This will include important parameter modifications, account addition and deletion, and password changes.



Logs Details

Details are shown as follows:

1. Time

The event date and time, following UTC standard format for date and time.

2. Severity

Severity labels include eight different classifications. These types are **'Emergency'**, **'Alert'**, **'Critical'**, **'Error'**, **'Warning'**, **'Notice'**, **'Information'** and **'Debug'**.

3. User ID

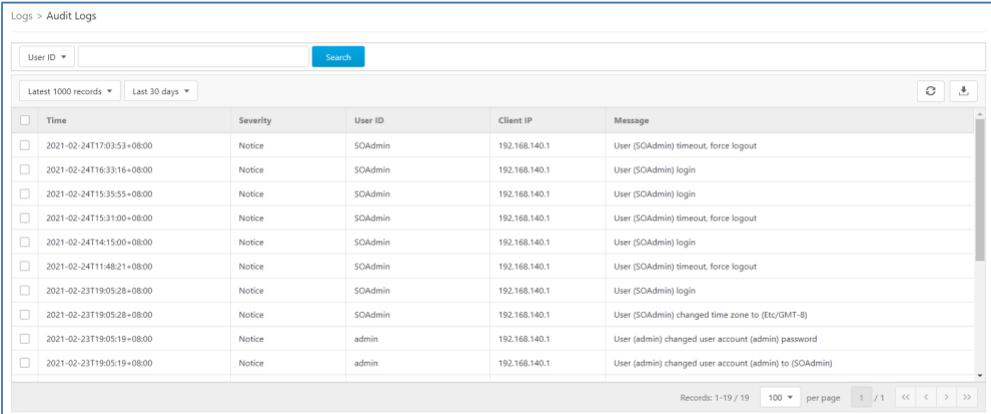
The ID of the user responsible for the change.

4. Client IP

The IP address of the client which triggered the log.

5. Message

The log message content, which usually contains important environmental parameters, key activities, and results.



Logs > Audit Logs

User ID

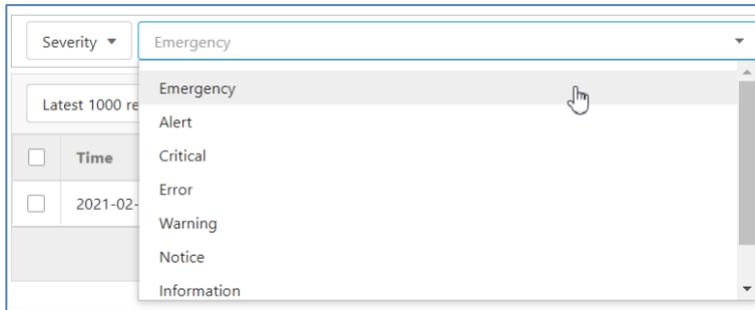
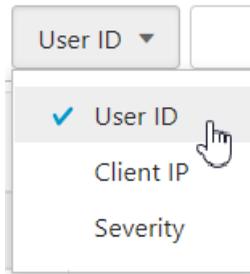
Latest 1000 records ▾ Last 30 days ▾

<input type="checkbox"/>	Time	Severity	User ID	Client IP	Message
<input type="checkbox"/>	2021-02-24T17:03:53+08:00	Notice	SOAdmin	192.168.140.1	User (SOAdmin) timeout, force logout
<input type="checkbox"/>	2021-02-24T16:33:16+08:00	Notice	SOAdmin	192.168.140.1	User (SOAdmin) login
<input type="checkbox"/>	2021-02-24T15:35:55+08:00	Notice	SOAdmin	192.168.140.1	User (SOAdmin) login
<input type="checkbox"/>	2021-02-24T15:31:00+08:00	Notice	SOAdmin	192.168.140.1	User (SOAdmin) timeout, force logout
<input type="checkbox"/>	2021-02-24T14:15:00+08:00	Notice	SOAdmin	192.168.140.1	User (SOAdmin) login
<input type="checkbox"/>	2021-02-24T11:48:21+08:00	Notice	SOAdmin	192.168.140.1	User (SOAdmin) timeout, force logout
<input type="checkbox"/>	2021-02-23T19:05:28+08:00	Notice	SOAdmin	192.168.140.1	User (SOAdmin) login
<input type="checkbox"/>	2021-02-23T19:05:28+08:00	Notice	SOAdmin	192.168.140.1	User (SOAdmin) changed time zone to (Etc/GMT-8)
<input type="checkbox"/>	2021-02-23T19:05:19+08:00	Notice	admin	192.168.140.1	User (admin) changed user account (admin) password
<input type="checkbox"/>	2021-02-23T19:05:19+08:00	Notice	admin	192.168.140.1	User (admin) changed user account (admin) to (SOAdmin)

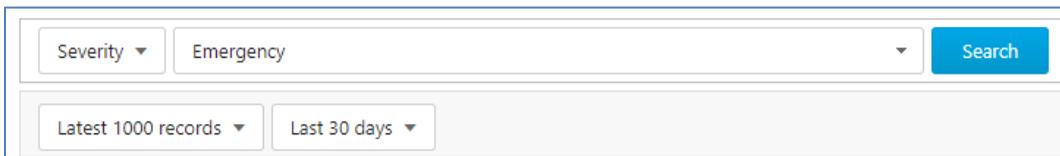
Records: 1-19 / 19 per page 1 / 1 << < > >>

Search & Refresh

You can query events based on User ID, Client IP, and severity classification. These classifications are 'Emergency', 'Alert', 'Critical', 'Error', 'Warning', 'Notice', 'Information' and 'Debug'.



You can also filter events using the number of records and time limit.



The event records will be updated automatically after you change the filter settings.

You can click the **refresh** icon to refresh the event list.

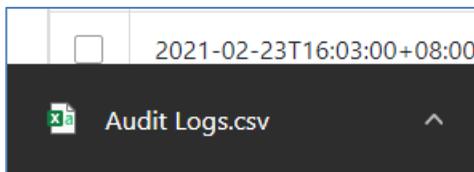


Export

If you would like to download the events you queried, please click the 'download' icon.



A file named "Audit Logs.csv" will be prepared for export.



Chapter 4

Administration

This chapter introduces administration practices for StellarOne.

Overview

There are many functions included in StellarOne for managing StellarProtect. They are as follows:

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
10. Syslog Forwarding
11. SMTP Settings
12. Notification

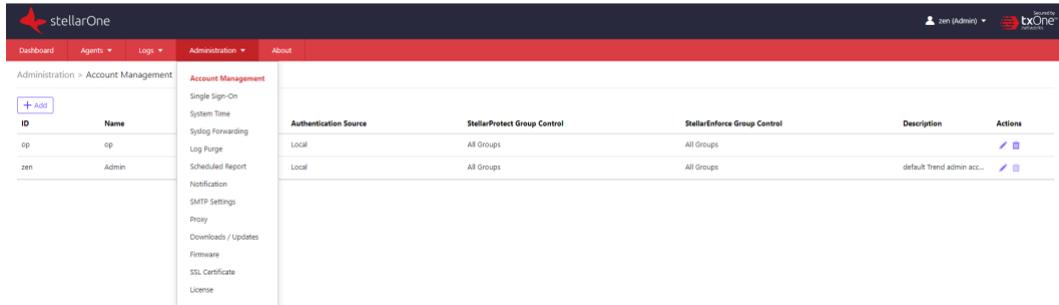
Users can select one of these functions from the Administration tab of StellarOne. Other functions not on this list are for managing StellarEnforce, and are only necessary if StellarOne is also connected to endpoints running StellarEnforce.

Account Management

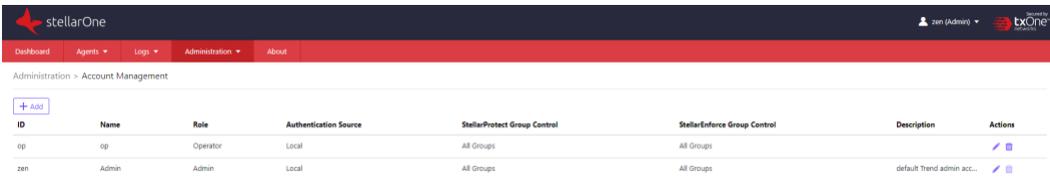
TXOne StellarOne console accounts have privileges by account type, according to the following list of types:

ACCOUNT TYPE	PRIVILEGES
Administrator	<ul style="list-style-type: none">• Add, edit, enable, disable, or delete StellarOne console accounts from the Account Management screen• Modify their own account description and password• Specify actions to take on files blocked by agents• View the StellarOne console Logs > Server Events screen• Allow or block storage device access on managed endpoints
Operator	<ul style="list-style-type: none">• Modify their own account description, email address, and password• Specify actions to take on files blocked by agents• View the StellarOne console Logs & Reports > Server Events screen• Allow or block storage device access on managed endpoints
Viewer	<ul style="list-style-type: none">• Modify their own account description, email address, and password• View the StellarOne console Logs & Reports > Server Events screen

User can select **Administration > Account Management** to configure or manage StellarOne accounts.



Then system will show you all valid accounts as follows:



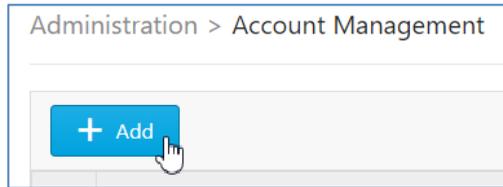
Information shown under account management will include:

1. **ID:** The ID used to log in
2. **Name:** The name of the account user
3. **Role:** The user role of the ID – Admin, Operator or Viewer
4. **Authentication Source:** Local account type or SAML
5. **StellarProtect Group Control:** The StellarProtect group that this account can manage or view
6. **StellarEnforce Group Control:** StellarEnforce group that this account can

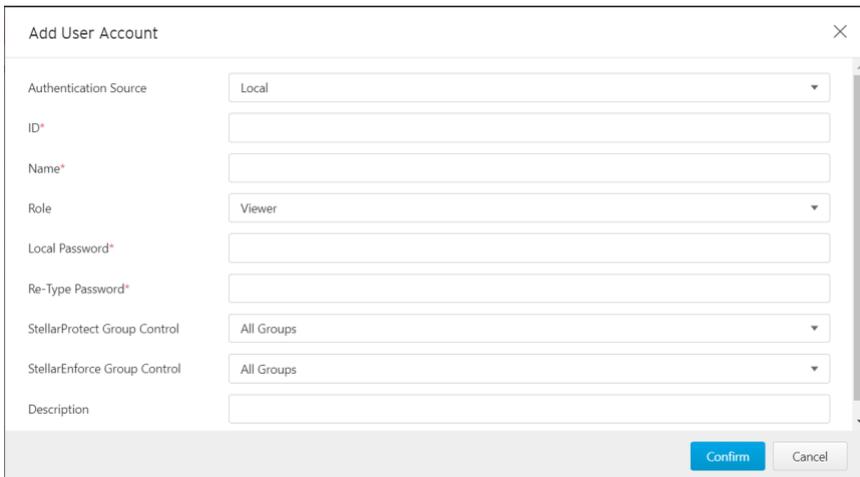
manage or view

7. Description: The description details for this account.

User can click 'Add' to add a new account:



A table will appear where you can enter your account type, including authentication source, input ID, name, role, and description. You will need to enter the password for a new account twice when creating a local account.

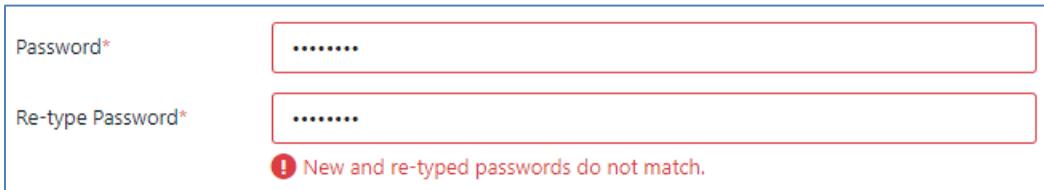
A screenshot of a dialog box titled 'Add User Account' with a close button (X) in the top right corner. The dialog contains several input fields: 'Authentication Source' (dropdown menu with 'Local' selected), 'ID*' (text input), 'Name*' (text input), 'Role' (dropdown menu with 'Viewer' selected), 'Local Password*' (text input), 'Re-Type Password*' (text input), 'StellarProtect Group Control' (dropdown menu with 'All Groups' selected), 'StellarEnforce Group Control' (dropdown menu with 'All Groups' selected), and 'Description' (text input). At the bottom right, there are two buttons: 'Confirm' (blue) and 'Cancel' (gray).

You can also configure which Agent group(s) this account can manage or view. There are three types of group setting available:

- All Groups
- Custom
- None

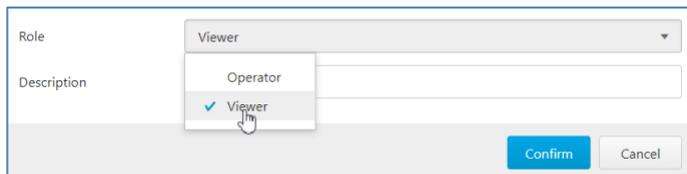
Click **Confirm** to create a new account.

The system will check that the text entered into Password and Re-type Password matches. Please confirm these two passwords are the same before you click **Confirm** again.



A screenshot of a form with two input fields. The first field is labeled "Password*" and contains seven dots. The second field is labeled "Re-type Password*" and also contains seven dots. Below the fields is a red error message: "❗ New and re-typed passwords do not match." The entire form is enclosed in a blue border.

StellarOne has a unique administrator account. The administrator can choose the Operator or Viewer role for new accounts.



A screenshot of a form showing a dropdown menu for the "Role" field. The dropdown is open, showing three options: "Viewer" (selected with a blue checkmark), "Operator", and "Viewer". The "Description" field is empty. At the bottom right, there are "Confirm" and "Cancel" buttons.

TXOne StellarOne features StellarOne console accounts with different privileges and

limitations. Use these accounts to configure StellarOne and to monitor or manage StellarProtect agents. Administrator and Operator accounts have full control while the Viewer can only view data.

The following table outlines typical StellarOne tasks and the account privileges required to perform them.

Task	Account Privilege Required
Configure Industrial-Grade Next-Generation Antivirus	<ul style="list-style-type: none">• Admin• Operator
Configure USB Vector Control	<ul style="list-style-type: none">• Admin• Operator
Configure User-Defined Suspicious Objects	<ul style="list-style-type: none">• Admin• Operator
Configure DLL Injection Protection	<ul style="list-style-type: none">• Admin• Operator
Configure Agent Password	<ul style="list-style-type: none">• Admin• Operator
Configure Operations Behavior Anomaly Detection	<ul style="list-style-type: none">• Admin• Operator
Configure ICS application safeguard	<ul style="list-style-type: none">• Admin• Operator
Configure Trusted Certifications	<ul style="list-style-type: none">• Admin• Operator
Configure Group Policy	<ul style="list-style-type: none">• Admin• Operator
Configure Global Policy	<ul style="list-style-type: none">• Admin

	<ul style="list-style-type: none"> Operator
Send Configure Change Window Command	<ul style="list-style-type: none"> Admin Operator
Send Scan Now Command	<ul style="list-style-type: none"> Admin Operator
Organize (Edit Tags/ Move / Delete)	<ul style="list-style-type: none"> Admin Operator
Monitor Server Event logs	<ul style="list-style-type: none"> Admin Operator
Monitor Agent Event logs	<ul style="list-style-type: none"> Admin Operator Viewer
Account Management	<ul style="list-style-type: none"> Admin Operator
Single Sign-On	<ul style="list-style-type: none"> Admin
System Time	<ul style="list-style-type: none"> Admin Operator
Proxy	<ul style="list-style-type: none"> Admin Operator
Downloads / Updates	<ul style="list-style-type: none"> Admin Operator Viewer

Firmware	<ul style="list-style-type: none"> Admin
SSL Certification	<ul style="list-style-type: none"> Admin
License	<ul style="list-style-type: none"> Admin Operator
Log Purge	<ul style="list-style-type: none"> Admin Operator
Syslog Forwarding	<ul style="list-style-type: none"> Admin Operator
SMTP Settings	<ul style="list-style-type: none"> Admin Operator
Notification	<ul style="list-style-type: none"> Admin Operator Viewer

Single Sign-On

Procedure

1. Log on to the web console using an administrator account.
2. Go to **Administration > Single Sign-On** in the navigation at the top of the web console.
3. Click **Download** to upload the StellarOne XML file to your IdP.

4. Click **Upload** to upload the IdP metadata XML file 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.
5. After the IdP metadata XML file is uploaded, the button **Test Connection** will appear. Click the button to test the IdP connection with StellarOne.
6. Make sure you have created your **SAML Account Mapping** under **Administration > Account Management**.
7. You can now use this account to login.

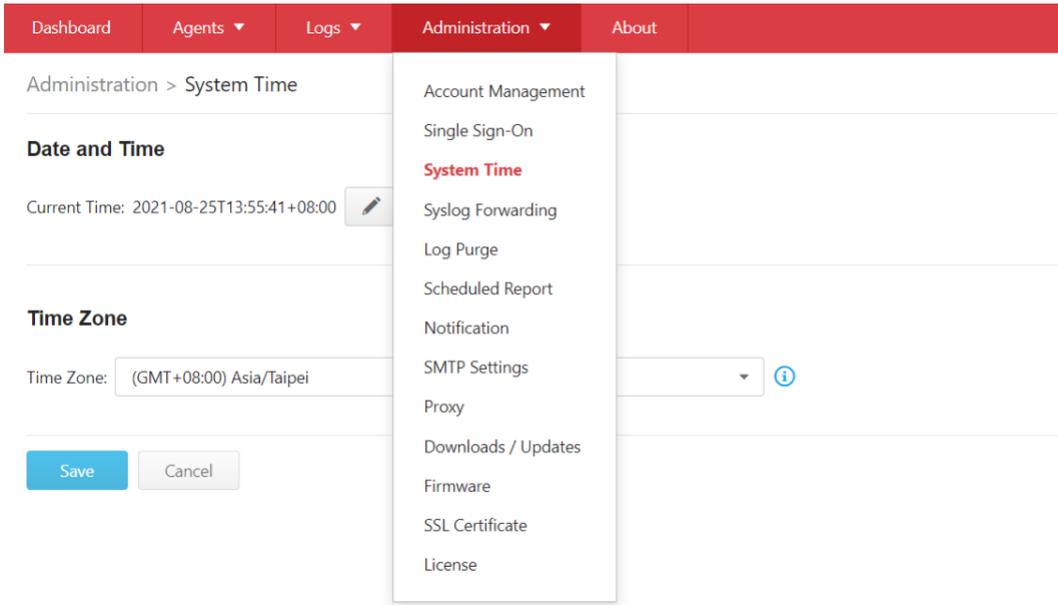


Important

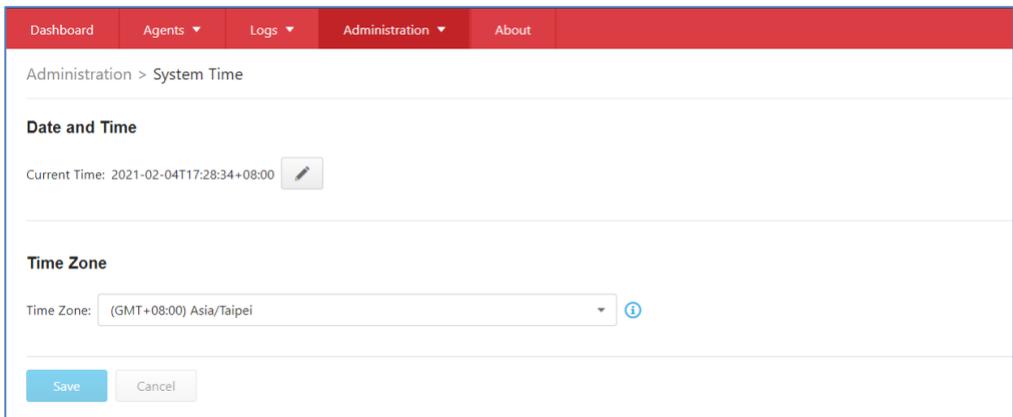
SAML Account Mapping email is case-sensitive.

System Time

The user can change the StellarOne system time by going to Administration > System Time.



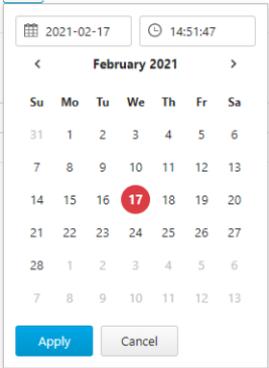
StellarOne can support different time zones around the world, so you can choose the correct time zone and set the date and time based on your location.



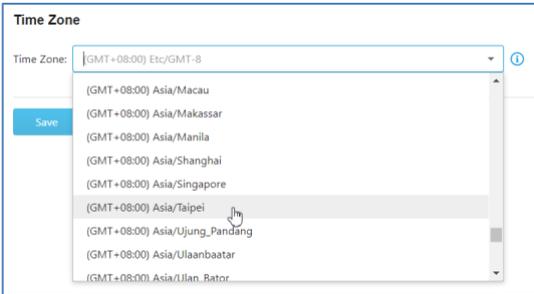
You can modify the Date and Time as below:



A calendar will appear where you can select the current date and time.

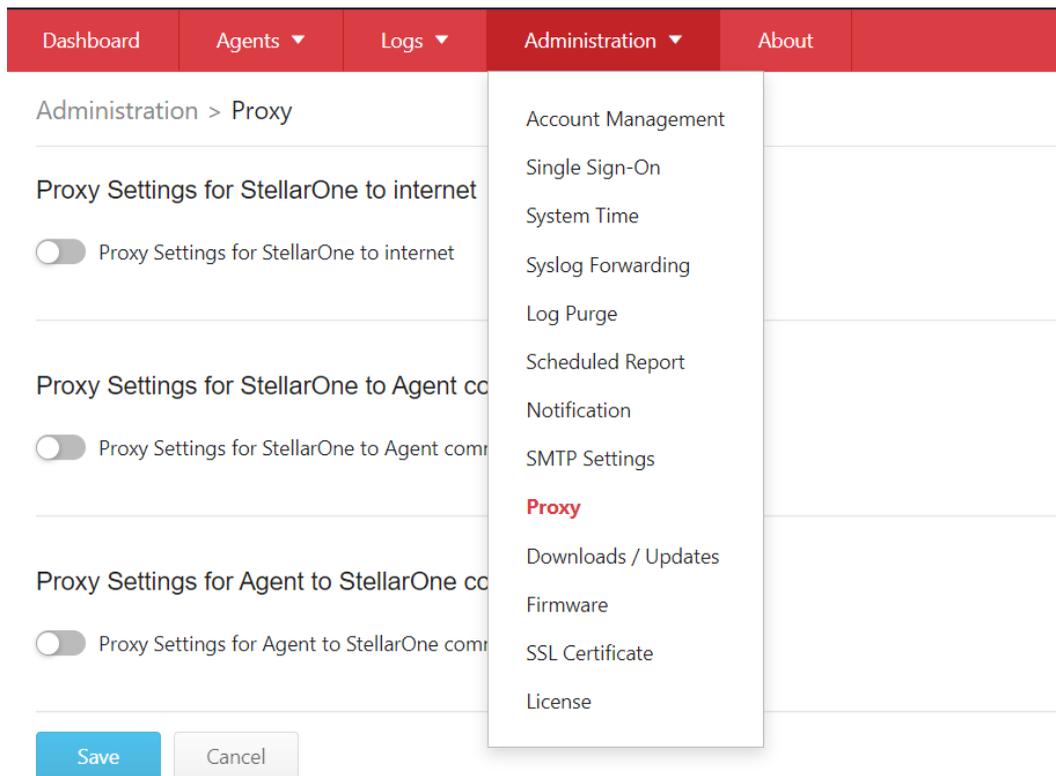


In addition, you can select your time zone from the drop-down list, then click “Save” to confirm the setting.



Proxy

StellarOne supports the use of a proxy for agent communications. Please select **Administration > Proxy** to open proxy settings.



The screenshot shows the StellarOne Administration interface. At the top, there is a red navigation bar with the following tabs: Dashboard, Agents (with a dropdown arrow), Logs (with a dropdown arrow), Administration (with a dropdown arrow), and About. The Administration menu is open, displaying a list of options: Account Management, Single Sign-On, System Time, Syslog Forwarding, Log Purge, Scheduled Report, Notification, SMTP Settings, **Proxy** (highlighted in red), Downloads / Updates, Firmware, SSL Certificate, and License. Below the navigation bar, the breadcrumb path 'Administration > Proxy' is visible. The main content area shows three settings sections, each with a toggle switch and a title: 'Proxy Settings for StellarOne to internet' (toggle off), 'Proxy Settings for StellarOne to Agent co' (toggle off), and 'Proxy Settings for Agent to StellarOne co' (toggle off). At the bottom left, there are two buttons: 'Save' (blue) and 'Cancel' (grey).

A window will appear as follows:

Administration > Proxy

Proxy Settings for StellarOne to internet

Proxy Settings for StellarOne to internet

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

Save

Cancel

There are three types of proxy for different purposes:

- **Proxy Settings for StellarOne to Internet:** This proxy is used by StellarOne for license renewal and Scan Component Updates.
- **Proxy Settings for StellarOne to Agent Communications:** This proxy is used for StellarOne command deployment to agents.
- **Proxy Settings for Agent to StellarOne Communications:** This proxy will be included in created agent installer packages and use by agents to connect to StellarOne.

Procedure

1. Please enable the proxy want to use and finish the server settings including choosing a **protocol** (HTTP or HTTPS) and entering a **server IP address** with **port number**.
2. If the proxy server requires authentication, please input the correct **user name** and **password**.
3. Click **Save** to confirm all settings.

Downloads / Updates

StellarOne supports update services.

Please select **Administration > Downloads / Updates**.

The screenshot displays the StellarOne Administration interface. At the top, a red navigation bar contains the following items: Dashboard, Agents (with a dropdown arrow), Logs (with a dropdown arrow), Administration (with a dropdown arrow), and About. Below the navigation bar, the breadcrumb path "Administration > Downloads / Updates" is visible. The main content area is divided into two columns. The left column shows the "StellarOne" section with a "Scan Component" section containing an "Update Now" button (with an upward arrow icon) and the text "Last Updated: 2021-08-24T...". Below this are sections for "Pattern Version" and "Engine Version". The right column shows the "Administration" dropdown menu, which is open and lists the following options: Account Management, Single Sign-On, System Time, Syslog Forwarding, Log Purge, Scheduled Report, Notification, SMTP Settings, Proxy, Downloads / Updates (highlighted in red), Firmware, SSL Certificate, and License. Below the menu, the "Scan Component Update Schedule" section is visible, featuring a "Schedule Update" toggle switch. At the bottom, the "Scan Component Update Source (StellarOne)" section is partially visible, with the text "Select a download source:".

Scan Component

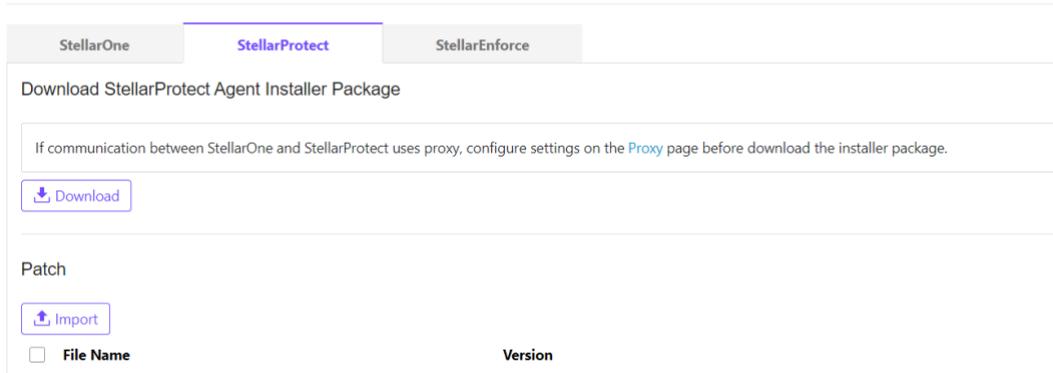
The following table describes the tasks you can perform on this screen:

Function	Description
Scan Component	Under this section you can click Update Now to download latest components. All of the pattern and engine versions are listed here.
Scan Component Update Schedule	Set the frequency and time for scan component updates to be either daily , weekly , or monthly , including 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)	Specify an update server or download updates directly from StellarOne.

Installer Package

If you would like to create an installation package for installing StellarProtect on devices to be managed, please go to **StellarProtect** tab and click **Download**.

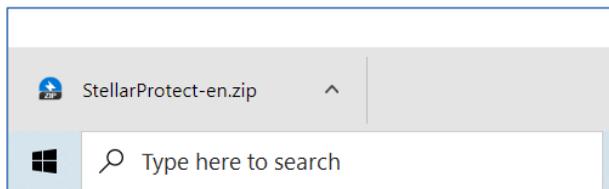
Administration > Downloads / Updates



The screenshot shows a web interface with three tabs: StellarOne, StellarProtect (selected), and StellarEnforce. Below the tabs, the heading reads "Download StellarProtect Agent Installer Package". A note states: "If communication between StellarOne and StellarProtect uses proxy, configure settings on the Proxy page before download the installer package." Below this note is a "Download" button. Underneath is a "Patch" section with an "Import" button. At the bottom, there is a table header with a checkbox, "File Name", and "Version".

A compressed file named **StellarProtect-en.zip** will be prepared for download.

It can be decompressed and used to install an agent on devices intended to be managed by StellarOne.



Patch

You can upload a StellarProtect remote patch file (zip file) to StellarOne for remote deployment.

Procedure

1. Go to **Administration > Downloads / Updates**
2. Go to tab **StellarProtect**
3. Click **Import > Select File** and select the zip patch file you get from **Download Center**
4. Click **Confirm**

You can delete the patch when no longer needed.

Procedure

1. Go to **Administration > Downloads / Updates**
2. Go to tab **StellarProtect**
3. Select the patch file you want to delete
4. Click **Delete**

SSL Certification

Procedure

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

License

If you would like to view or add additional licenses, please select Administration > License.

The screenshot shows the StellarMix administration interface. At the top, there is a red navigation bar with the following items: Dashboard, Agents (with a dropdown arrow), Logs (with a dropdown arrow), Administration (with a dropdown arrow), and About. Below the navigation bar, the breadcrumb path "Administration > License" is displayed. The main content area features a blue button labeled "+ Specify Activation Code" and a grey button labeled "Renew License" with a circular refresh icon. Below these buttons, the license details for "StellarMix" are shown in a table format:

Status:	Activated
Type:	Trial
Expiration:	2021-12-31
Seats:	2/10
Activation Code:	TE-
Last Updated:	2021-08-03T14:43:49+08:00

Overlaid on the right side of the interface is the "Administration" dropdown menu, which contains the following options: Account Management, Single Sign-On, System Time, Syslog Forwarding, Log Purge, Scheduled Report, Notification, SMTP Settings, Proxy, Downloads / Updates, Firmware, SSL Certificate, and License (highlighted in red).

The following details will be shown on this screen:

Item	Description
Status	Displays "Activated" or "Expired"
Type	Displays "Full" or "Trial"
Expiration	Displays the date when features and support end
Activation Code	Displays the activation code
Last Updated	Displays the last time the activation code was updated

Current license information will be shown as follows.

Administration > License

+ Specify Activation Code

 Renew License

StellarMix

Status: Activated

Type: Trial

Expiration: 2021-12-31

Seats: 2/10

Activation Code: TE-

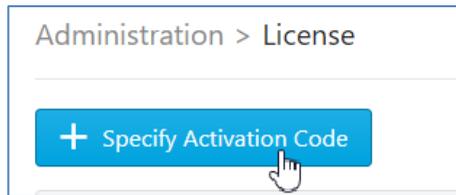
Last Updated: 2021-08-03T14:43:49+08:00



Click **Refresh** to update your product license. A connection with the TXOne product license server is required.

Specify Activation Code

If you'd like to add another license named Activation Code, please click the "Specify Activation Code"



Input a correct Activation Code and click "Save" to verify and confirm the new license.

A screenshot of a dialog box titled "Specify Activation Code". The dialog has a close button (X) in the top right corner. Inside the dialog, there is a label "New Activation Code:" followed by a text input field containing the text "TE-". At the bottom right of the dialog, there are two buttons: "Save" and "Cancel".

Seat Count

Any agent exceeding the available seat count won't be able to be managed by StellarOne.

Log Purge

This function allows the user to purge older logs to reduce the size of the StellarOne database.

Procedure

1. Go to **Administration > Log Purge** in the navigation at the top of the web console.

The **Log Purge** screen will appear.

2. In the first dropdown box, select log type.
3. In the second dropdown box, select time frame for purging based on **Older Than** (Do not keep logs older than ...).
4. In the third dropdown box, select the maximum number of log files to be kept.
5. When you're sure, click **Purge Now**.

Automatic Purge

You can also schedule log purges to occur automatically.

Procedure

1. Find **Automatic Purge** under **Log Purge**
2. Purges are defined according to each type of log listed on the left.
3. In the second dropdown box, select the time frame for purging by adjusting the drop-down box next to 'older than' (Do not keep logs older than ...).
4. In the third dropdown box, next to 'and keep at most', select the number of log files to be kept after the purge.
5. When you're sure, click **Save**.

Syslog Forwarding

You can forward server and agent event logs to an external syslog server for additional managing and monitoring capabilities.

Procedure

1. Go to **Administration > Syslog Forwarding**.
2. Select **Forward logs to syslog server (CEF only)**.
3. Specify the protocol, server address, and port of the syslog server.
4. **Save** your settings.

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 navigation at the top of the web console.

The **SMTP Settings** screen will appear.

2. To configure SMTP settings for email notification:
 - a. Under **Server Address**, the IP address or fully qualified domain name (FQDN) of the SMTP server.
 - b. Specify the **Port**.
 - c. Specify the sender's email address in the **Sender** field. StellarOne uses this address as the sender address.
 - d. If the SMTP server requires authentication, select **SMTP server requires authentication** and provide the authentication information.
 - e. To send a test email from StellarOne, click the **Send Test Email** button.
3. Click **Save**.

Notification

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. Go to **Administration > SMTP Settings** to specify your SMTP server settings first.
2. Go to **Administration > Notification** to change notification settings.
3. Sections under **Notification** include **Warning Level Agent Events**, **Outbreak** and **Email Notifications**.

Warning Level Agent Events

When the switch under **Warning Level Agent Events** is 'on', StellarOne will send a notification to your e-mail when an incident happens that triggers a "**Warning**" or "**Critical**" agent event.

Outbreak

When the switch under **Outbreak** is 'on', StellarOne will send a notification to your e-mail if more than a specified number of open warning and critical messages has appeared in a specified time period.

You can set the number of open events 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).

Firmware

Starting from StellarOne 1.1, you can upgrade StellarOne to new versions using this feature.

Procedure

1. Go to **Administration > Firmware** in the navigation at the top of the web console. Click **Import**.
2. **Version** shows the current StellarOne build version. **Release Date** and **Description** show the current information for StellarOne.
3. Click **Import** and specify the update patch .
4. When the Firmware Update window pops up, click **Apply** to apply the patch to StellarOne.
5. Confirm the notification description. Click **Install Now** to implement the update or **Abort** to stop updating.

Chapter 5

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	
4352	Warning	system	Service stopped	
257	Information	system	Policy applied successfully (Version: %version%)	
4353	Warning	system	Unable to apply policy (Version: %version%)	
513	Information	intelli_av	ICS Inventory List Update Succeeded	
514	Information	intelli_av	Real Time Scan Enabled	
8706	Critical	intelli_av	Real Time Scan Disabled	
4615	Warning	intelli_av	Application Execution Blocked By Antivirus: %PATH%	Application execution was blocked by antivirus. Target Process: %PATH% File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING%

Event ID	Level	Category	Event Content	Event Details
4617	Warning	intelli_av	Application Execution Blocked By Next-Generation Antivirus: %PATH%	Application execution was blocked by next- generation antivirus. Target Process: %PATH% File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING%
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:

Event ID	Level	Category	Event Content	Event Details
				%STRING% Action Result: %INTEGER% Quarantine Path: %PATH%
4611	Warning	intelli_av	Local Files Scanned, Action Taken by Antivirus: %PATH%	Local files were scanned by antivirus. Actions were taken according to settings. File Path: %PATH% File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING% Action Result: %INTEGER% Quarantine Path: %PATH%
4612	Warning	intelli_av	Local Files Scanned, Action Taken by Next-Generation Antivirus: %PATH%	Local files were scanned by next- generation antivirus. Actions were taken according to settings. File Path: %PATH% File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING% Action Result: %INTEGER% Quarantine Path: %PATH%

Event ID	Level	Category	Event Content	Event Details
4613	Warning	intelli_av	Suspicious Program Execution Blocked: %PATH%	Suspicious program execution was blocked. File Path: %PATH% File Hash: %STRING%
768	Information	anomaly_detect	Operations Behavior Anomaly Detection Enabled	Mode: %Mode% Level: %Level%
4864	Warning	anomaly_detect	Operations Behavior Anomaly Detection Disabled	
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%

Event ID	Level	Category	Event Content	Event Details
				% ARGUMENT% Parent Process 4: % PATH% % ARGUMENT%
4865	Warning	anomaly_detect	Process Allowed by Operations Behavior Anomaly Detection: % PATH% % ARGUMENT%	Access User: % USERNAME% Parent Process 1: % PATH% % ARGUMENT% Parent Process 2: % PATH% % ARGUMENT% Parent Process 3: % PATH% % ARGUMENT% Parent Process 4: % PATH% % ARGUMENT% Mode: Detection
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: Protection
9216	Critical	change_control	Change Window Start	
9217	Critical	change_control	Change Window End	
5120	Warning	change_control	ICS File Change Blocked by SafeGuard: % PATH%	ICS File change to executable file were blocked by SafeGuard. Blocked Process: % PATH%

Event ID	Level	Category	Event Content	Event Details
				Target File: %PATH%
1280	Information	device_control	USB Vector Control Enabled	
5376	Warning	device_control	USB Vector Control Disabled	
1281	Information	device_control	Trusted USB Device Added	Vendor ID: %HEX% Product ID: %HEX% Serial Number: %STRING% Type: permanent or onetime
1282	Information	device_control	Trusted USB Device Removed	Vendor ID: %HEX% Product ID: %HEX% Serial Number: %STRING%
5377	Warning	device_control	USB Access Blocked: %PATH% %	Access Image Path: %PATH% Access User: %USERNAME% Vendor ID: %HEX% Product ID: %HEX% Serial Number: %STRING%
4354	Warning	system	Unable to update file: %dst_path%	Unable to update file. Source Path: %src_path% Destination Path: %dst_path% Error Code: %err_code%
258	Information	system	Patch applied. File Name:	Patch applied. File Name:

Event ID	Level	Category	Event Content	Event Details
			%file_name%	%file_name%
4355	Warning	system	Unable to apply patch. File Name: %file_name%	Unable to apply patch. File Name: %file_name% Error Code: %err_code%

StellarProtect Server Event Log Descriptions

Server Event Log Descriptions

ID	Content
33025	Inherit global policy for group [%s]
33026	Customize policy for group [%s] with version: %s
33027	Switch agent (%s) to policy mode
33028	Switch agent (%s) to individual mode
33041	Modify in common use (DLL Injection Prevention, USB Vector Control, ICS Application Safeguard) setting for [%s] group policy with version: %s
33042	Modify real-time scan settings for [%s] group policy with version: %s
33043	Modify schedule scan settings for [%s] group policy with version: %s
33044	Maintain USB Vector Control list for [%s] group policy with version: %s
33045	Maintain User Defined Suspicious Object list for [%s] group policy with version: %s
33046	Maintain Operations Behavior Anomaly Detection Watch List for [%s] group policy with version: %s
33047	Maintain Trusted Certification list for [%s] group policy with version: %s

ID	Content
33048	Maintain ICS Application Safeguard list for [%s] group policy with 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

Chapter 6

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 <http://about-threats.trendmicro.com/us/threatencyclopedia#malware> 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 by phone or email:

Address	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
Website	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: SLEM19395/210826