TREND MICRO™

txOne™ networks

# 1.0 TXOne StellarOne™ for StellarProtect

## Administrator's Guide

All-terrain protection for mission critical assets

Windows

Endpoint Security

# TXOne StellarOne™

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

Document Part No.: SLEM19269/210330

Release Date: May 4th, 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..........................................................................16**

***Chapter 2 .......................................................................................... 18***

**Agents..........................................................................................18**

**Managing StellarProtect Devices ..........................................................................19**

Group Management.......................................................................................... 20

View ICS Items.......................................................................................... 27

Policy Management.......................................................................................... 28

Device Action Commands .......................................................................................... 46

***Chapter 3 .......................................................................................... 49***

**Dashboard, Events, and Logs ..........................................................................49**

**Overview..........................................................................................50**

**Dashboard..........................................................................................51**

StellarProtect Top Endpoints with Blocked Events .......................................................... 52

StellarProtect Top Blocked Files ........ 55

CPU Usage ........ 56

Memory Usage ........ 57

Disk Usage ........ 57

**Events ........ 58**

Agent Events ........ 60

Server Events ........ 66

System Logs ........ 70

Audit Logs ........ 73

***Chapter 4 ........ 78***

**Administration ........ 78**

**Overview ........ 79**

**Account Management ........ 80**

**System Time ........ 87**

**Proxy ........ 89**

**Downloads / Updates ........ 93**

**License ........ 95**

Specify Activation Code ........ 96

Seat Count ........ 97

*Chapter 5 ........ 98*

**Technical Support ........ 98**

**Troubleshooting Resources ........ 99**

**Using the Support Portal ........ 99**

**Threat Encyclopedia ........ 100**

**Contacting Trend Micro ........ 100**

**Speeding Up the Support Call ........ 101**

**Sending Suspicious Content to Trend Micro ........ 102**

Email Reputation Services ........ 102

File Reputation Services ........ 103

Web Reputation Services ........ 103

Other Resources ........ 104

**Download Center ........ 104**

**Documentation Feedback ........ 104**

# 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 |
| *Italics* | References to other documents |
| Monospace | Sample command lines, program code, web URLs, file names, and program output |
| **Navigation** > **Path** | The navigation path to reach a particular screen<br>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 2. 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<br>managed endpoints | The hosts running the StellarProtect program that are known to the StellarOne server program |
| target endpoints | The hosts where the StellarOne managed agents will be installed |
| administrator (or StellarOne administrator) | The person managing the StellarOne server |
| 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 1-1. 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.<br>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:<br>1. Account Management<br>2. System Time<br>3. Proxy<br>4. Downloads / Updates<br>5. License |

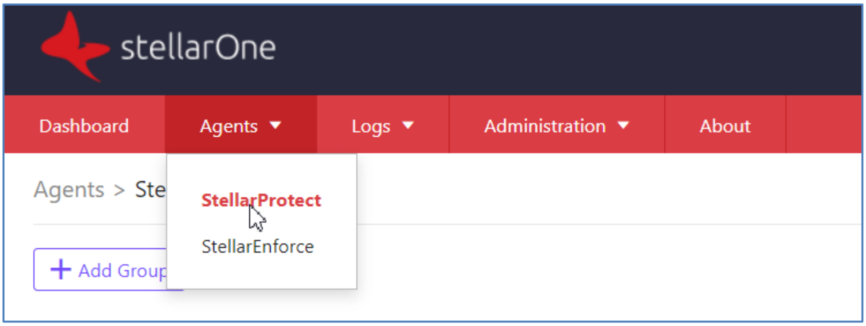
# Chapter 2

## 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.

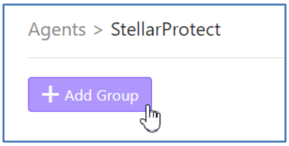
These agents will be managed with global policy. You can also create groups of agents (each endpoint is considered as an "agent" managing the endpoint) and then configure those groups with group policies.

# 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

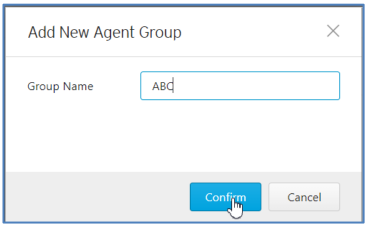
Please click ‘Add Group’ to create a new group.



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

Note

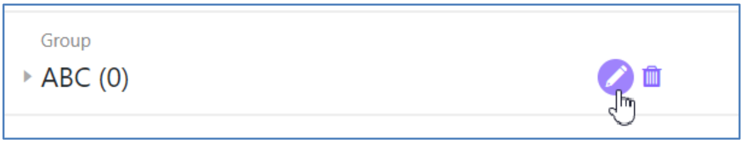
Group Name cannot be the same as the system default group name.


Add New Agent Group

Group Name: ABC

## Rename a Group

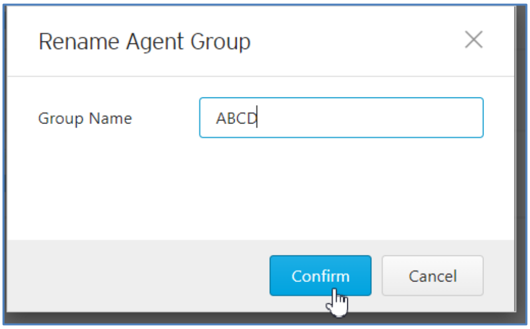
If you need to modify the name of the group, click the pencil icon of the group as shown below.



Group

ABC (0)

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

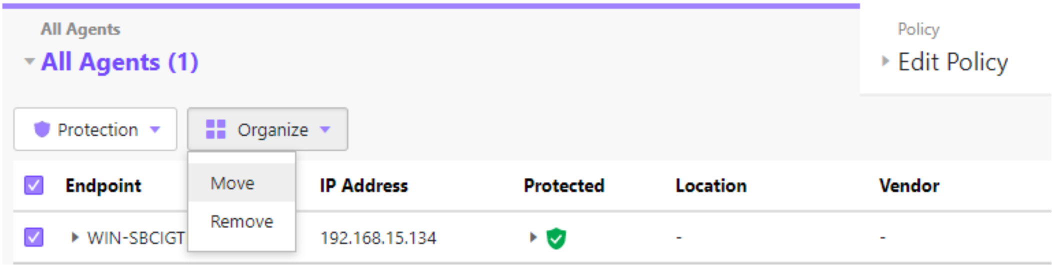


Rename Agent Group

Group Name: ABCD

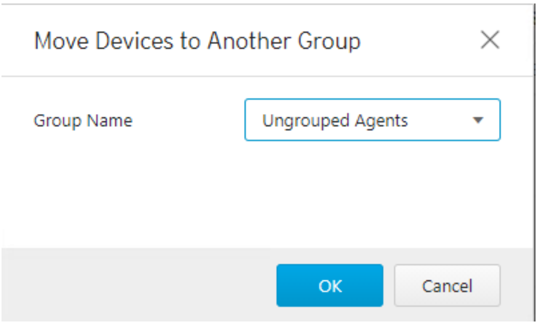
## Move a Device to a Group

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



| ☑ | Endpoint | IP Address | Protected | Location | Vendor |
|---|---|---|---|---|---|
| ☑ | WIN-SBCIGT | 192.168.15.134 | ✓ | - | - |

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

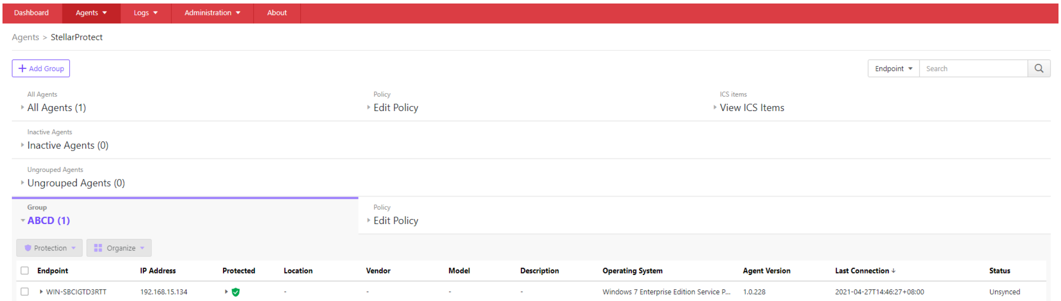


Group Name: Ungrouped Agents

Click the ‘OK’ button to confirm the settings.

## Expand a Group

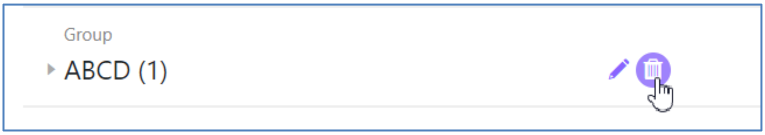
When all default values of the group have been collapsed, you can click on the group name and the group will expand as shown below:



| □ | Endpoint | IP Address | Protected | Location | Vendor | Model | Description | Operating System | Agent Version | Last Connection ↓ | Status |
|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | WIN-SBCIGTD3RTT | 192.168.15.134 | ✓ | - | - | - | - | Windows 7 Enterprise Edition Service P... | 1.0.228 | 2021-04-27T14:46:27+08:00 | Unsynced |

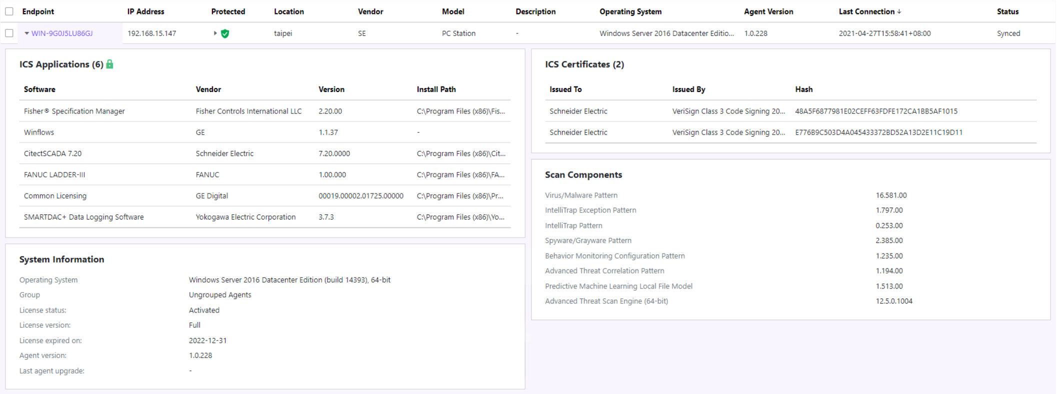
## Delete a Group

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 | Protected | Location | Vendor | Model | Description | Operating System | Agent Version | Last Connection ↓ | Status |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | ▾ WIN-9G0J5LU86GJ | 192.168.15.147 | ▸ ✓ | taipei | SE | PC Station | - | Windows Server 2016 Datacenter Editio... | 1.0.228 | 2021-04-27T15:58:41+08:00 | Synced |

**ICS Applications (6)**

| Software | Vendor | Version | Install Path |
|---|---|---|---|
| Fisher® Specification Manager | Fisher Controls International LLC | 2.20.00 | C:\Program Files (x86)\Fis... |
| Winflows | GE | 1.1.37 | - |
| CitectSCADA 7.20 | Schneider Electric | 7.20.0000 | C:\Program Files (x86)\Cit... |
| FANUC LADDER-III | FANUC | 1.00.000 | C:\Program Files (x86)\FA... |
| Common Licensing | GE Digital | 00019.00002.01725.00000 | C:\Program Files (x86)\Pr... |
| SMARTDAC+ Data Logging Software | Yokogawa Electric Corporation | 3.7.3 | C:\Program Files (x86)\Yo... |

**ICS Certificates (2)**

| Issued To | Issued By | Hash |
|---|---|---|
| Schneider Electric | VeriSign Class 3 Code Signing 20... | 48A5F6877981E02CEFF63FDFE172CA1BB5AF1015 |
| Schneider Electric | VeriSign Class 3 Code Signing 20... | E776B9C503D4A045433372BD52A13D2E11C19D11 |

**System Information**

| | |
|---|---|
| Operating System | Windows Server 2016 Datacenter Edition (build 14393), 64-bit |
| Group | Ungrouped Agents |
| License status: | Activated |
| License version: | Full |
| License expired on: | 2022-12-31 |
| Agent version: | 1.0.228 |
| Last agent upgrade: | - |

**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 |

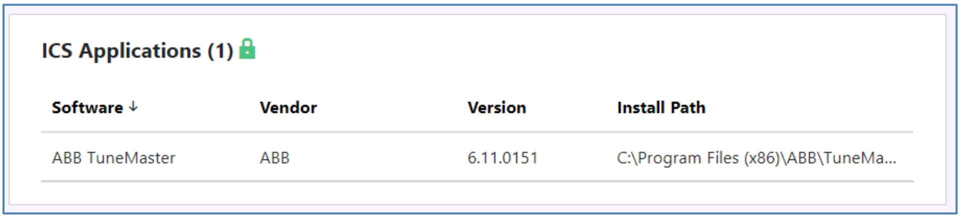
Device information includes the following:

- ICS application
- ICS certificate
- System information
- Scan component

## 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.

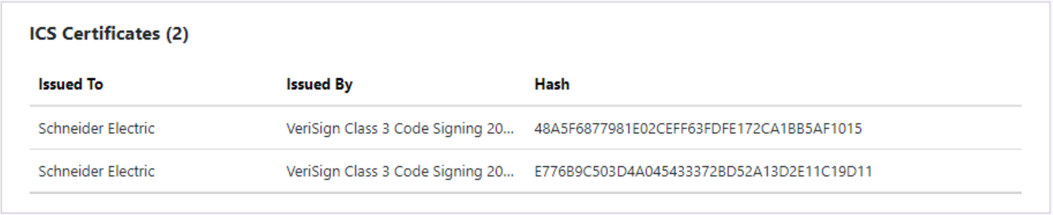


ICS Applications (1) 🔒

| 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.

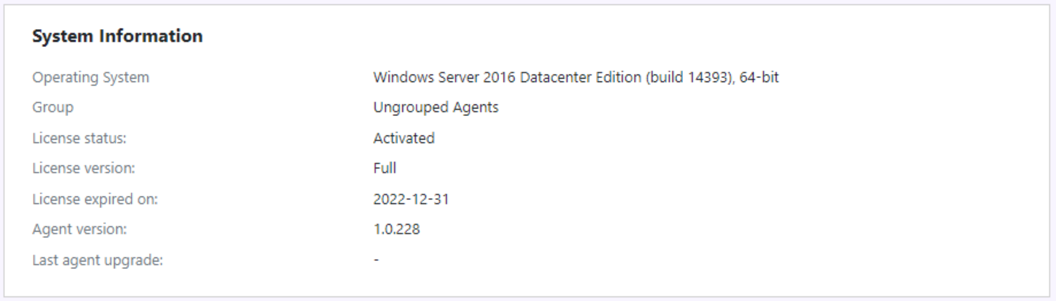


ICS Certificates (2)

| Issued To | Issued By | Hash |
|---|---|---|
| Schneider Electric | VeriSign Class 3 Code Signing 20... | 48A5F6877981E02CEFF63FDFE172CA1BB5AF1015 |
| 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.

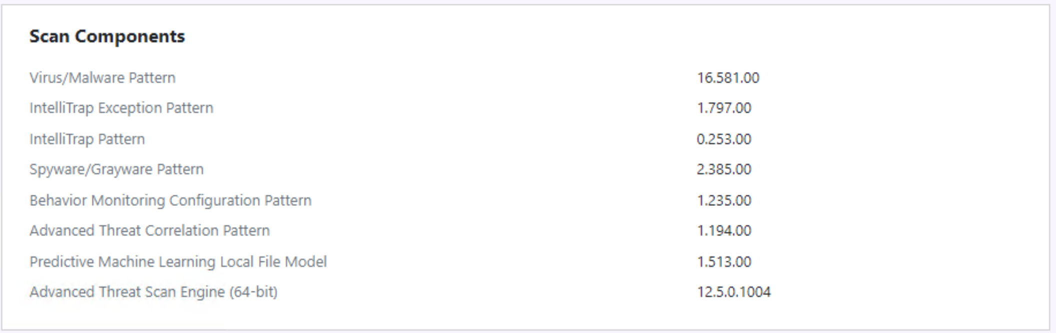


**System Information**

| | |
|---|---|
| Operating System | Windows Server 2016 Datacenter Edition (build 14393), 64-bit |
| Group | Ungrouped Agents |
| License status: | Activated |
| License version: | Full |
| License expired on: | 2022-12-31 |
| Agent version: | 1.0.228 |
| Last agent upgrade: | - |

## Scan Components

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

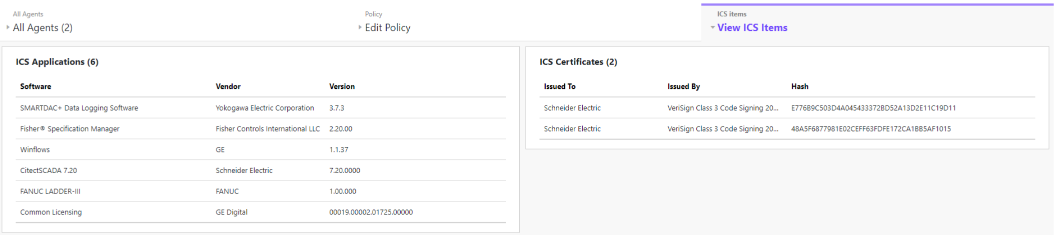


**Scan Components**

| | |
|---|---|
| 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 |

# 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.



**ICS Applications (6)**

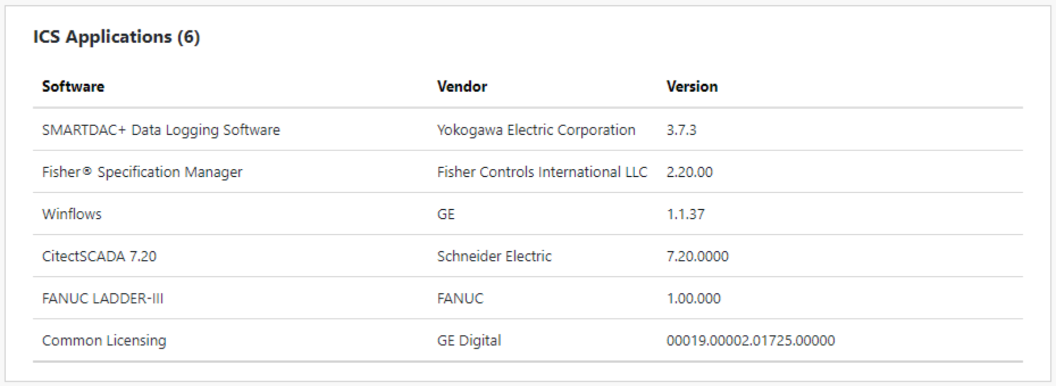
| Software | Vendor | Version |
|---|---|---|
| SMARTDAC+ Data Logging Software | Yokogawa Electric Corporation | 3.7.3 |
| Fisher® Specification Manager | Fisher Controls International LLC | 2.20.00 |
| Winflows | GE | 1.1.37 |
| CitectSCADA 7.20 | Schneider Electric | 7.20.0000 |
| FANUC LADDER-III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

**ICS Certificates (2)**

| Issued To | Issued By | Hash |
|---|---|---|
| Schneider Electric | VeriSign Class 3 Code Signing 20... | E776B9C503D4A045433372BD52A13D2E11C19D11 |
| Schneider Electric | VeriSign Class 3 Code Signing 20... | 48A5F6877981E02CEFF63FDFE172CA1BB5AF1015 |

# ICS Applications

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

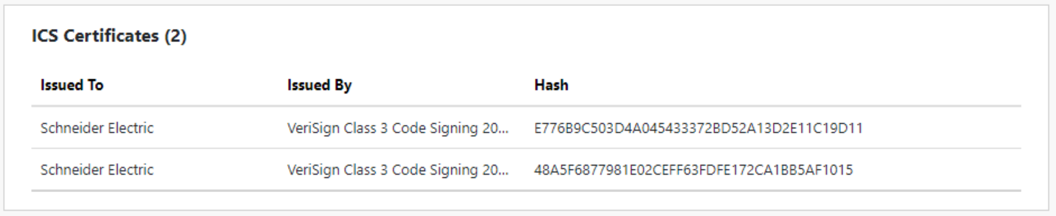


ICS Applications (6)

| 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)

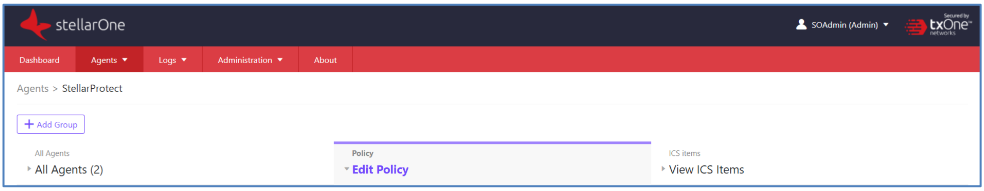
| Issued To | Issued By | Hash |
|---|---|---|
| Schneider Electric | VeriSign Class 3 Code Signing 20... | E776B9C503D4A045433372BD52A13D2E11C19D11 |
| Schneider Electric | VeriSign Class 3 Code Signing 20... | 48A5F6877981E02CEFF63FDFE172CA1BB5AF1015 |

## 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.

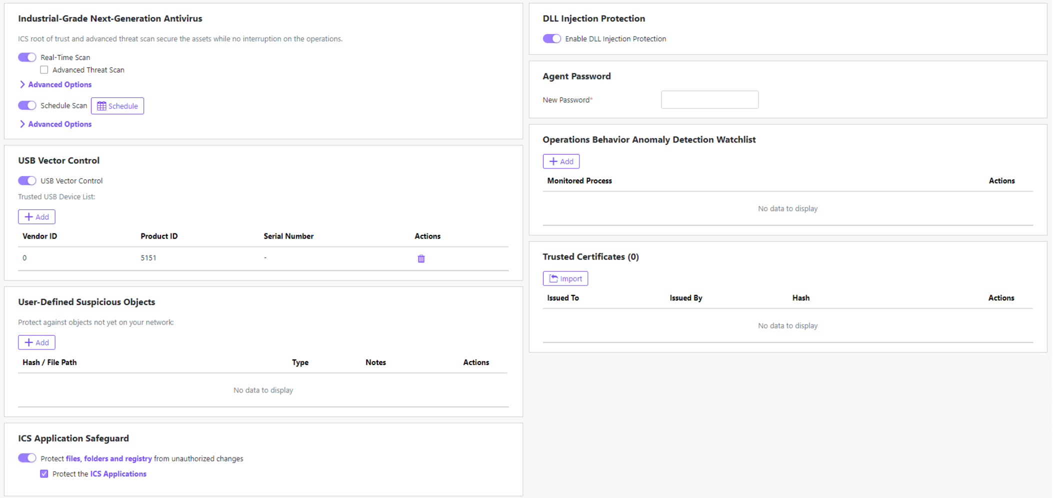
## Global Policy

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



### Industrial-Grade Next-Generation Antivirus

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

● Real-Time Scan

☐ Advanced Threat Scan

> Advanced Options

● Schedule Scan  Schedule

> Advanced Options

### USB Vector Control

● USB Vector Control

Trusted USB Device List:

+ Add

| Vendor ID | Product ID | Serial Number | Actions |
|---|---|---|---|
| 0 | 5151 | - | 🗑 |

### User-Defined Suspicious Objects

Protect against objects not yet on your network:

+ Add

| Hash / File Path | Type | Notes | Actions |
|---|---|---|---|
| No data to display | | | |

### ICS Application Safeguard

● Protect **files**, **folders and registry** from unauthorized changes

☑ Protect the **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 | |

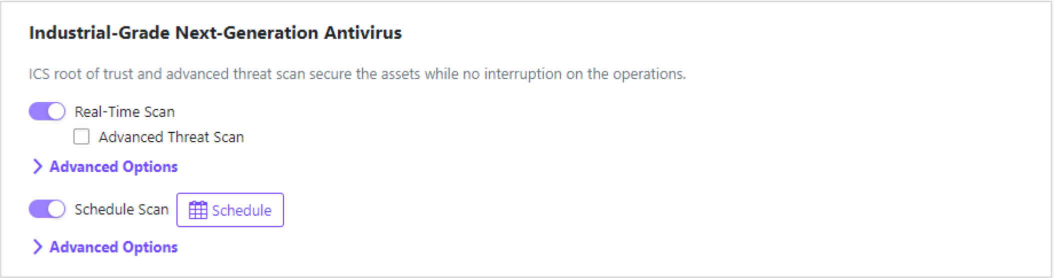
### Trusted Certificates (0)

Import

| Issued To | Issued By | Hash | Actions |
|---|---|---|---|
| No data to display | | | |

## 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 Scan

□ Advanced Threat Scan

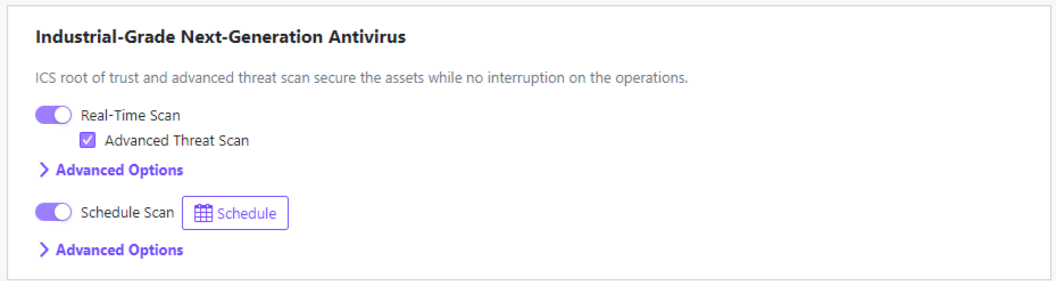
● Schedule Scan

### 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 Scan

☑ Advanced Threat Scan

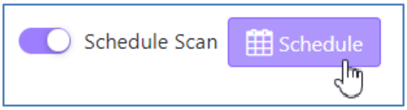
> Advanced Options

Schedule Scan Schedule

> Advanced Options

## Schedule Scan

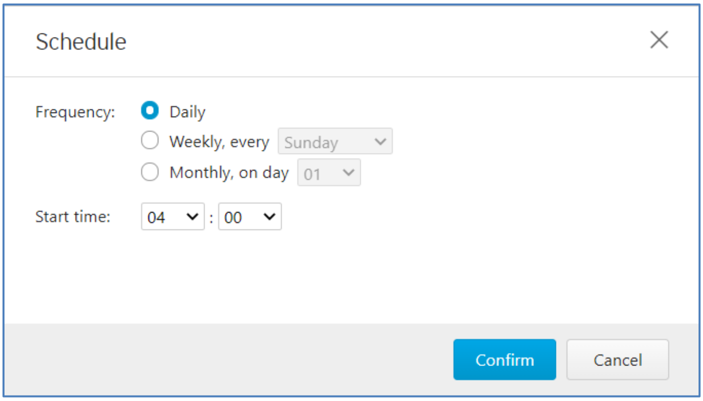
If you want to set an antivirus scan schedule, click ‘Schedule Scan’, and then click the ‘Schedule’ icon to set the date and time.



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

## Advanced Options

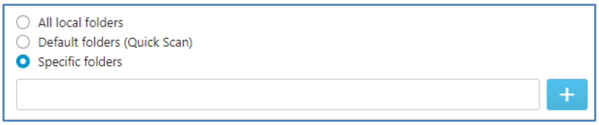
You can configure the following settings for industrial-grade next-generation antivirus under 'advanced options':

- 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 '+'.

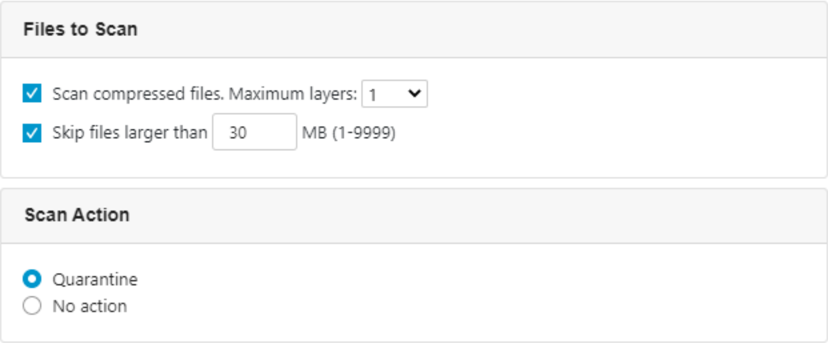


○ All local folders
○ Default folders (Quick Scan)
● Specific folders

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

☑ Scan compressed files. Maximum layers: 1

☑ Skip files larger than 30 MB (1-9999)

Scan Action

● Quarantine

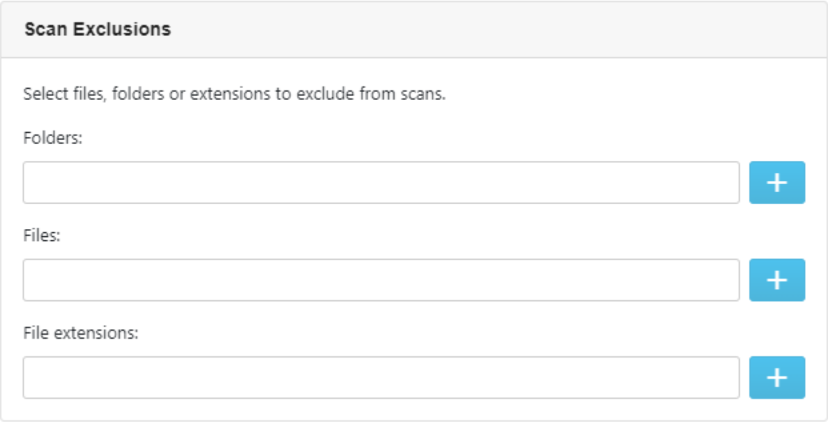
○ No action

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.

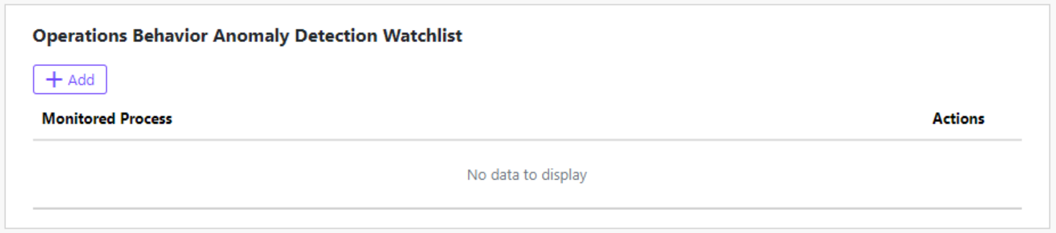
Folders:

Files:

File extensions:

## Operations Behavior Anomaly Detection

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

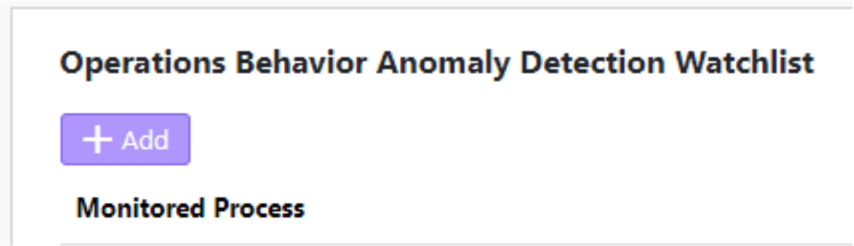


Operations Behavior Anomaly Detection Watchlist

| Monitored Process | Actions |
|---|---|
| No data to display | |

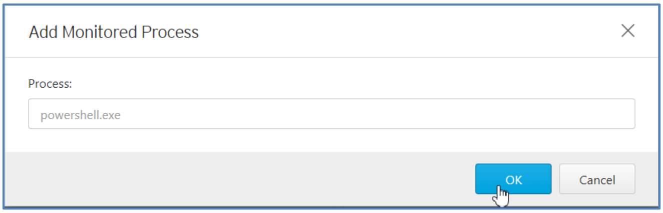
### Monitored Processes

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



Operations Behavior Anomaly Detection Watchlist

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

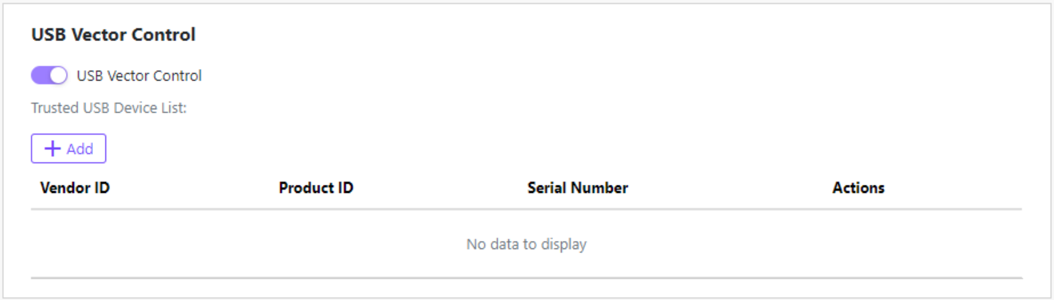


Add Monitored Process

Process: powershell.exe

## 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

USB Vector Control

Trusted USB Device List:

| Vendor ID | Product ID | Serial Number | Actions |
|---|---|---|---|

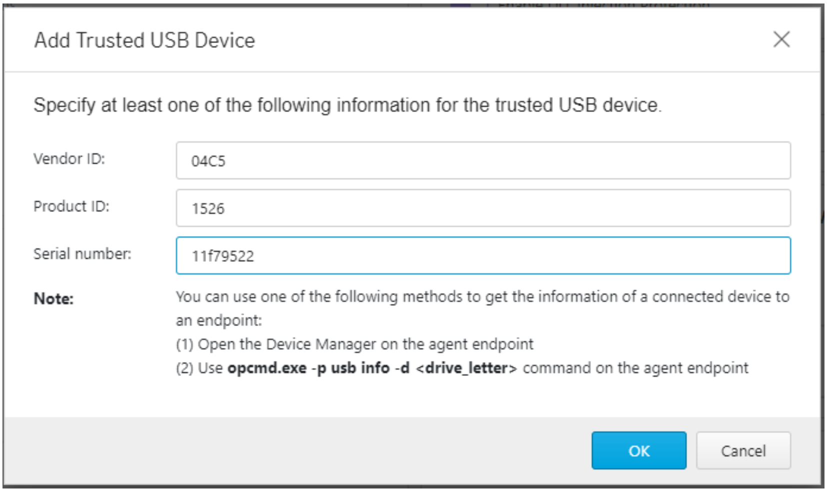
No data to display

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.

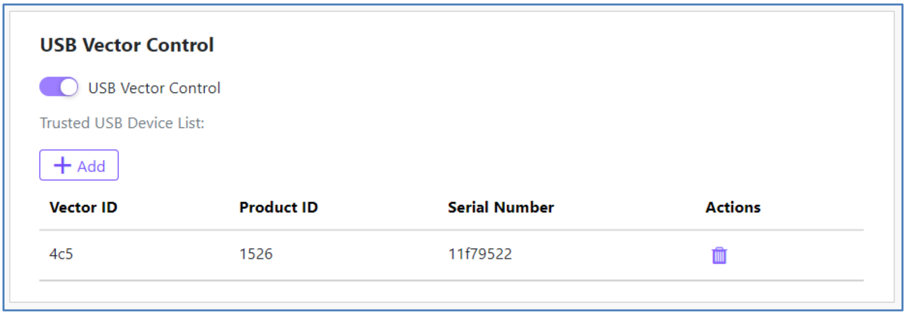
Vendor ID: 04C5

Product ID: 1526

Serial number: 11f79522

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

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



**USB Vector Control**

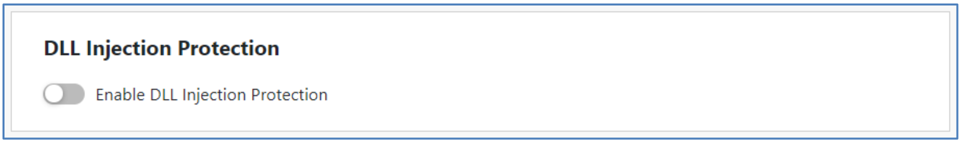
USB Vector Control

Trusted USB Device List:

| Vector 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.

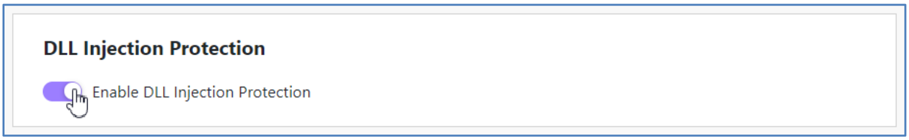


DLL Injection Protection

○ Enable DLL Injection Protection

### Block DLL Injection

To enable this protection, click ‘Enable DLL Injection Protection’.

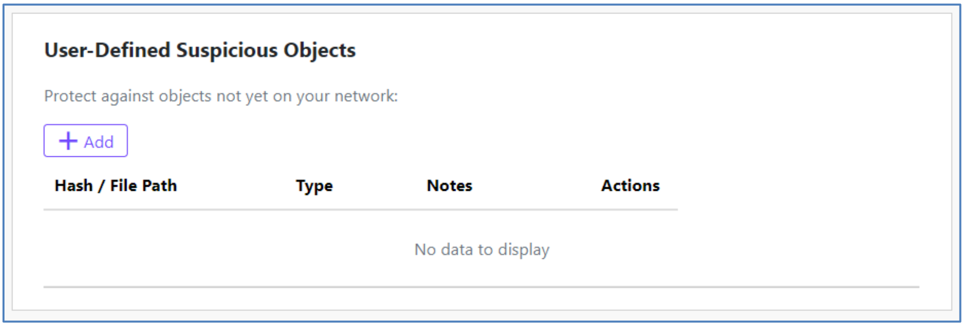


DLL Injection Protection

● Enable DLL Injection Protection

## User-Defined Suspicious Objects

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



User-Defined Suspicious Objects

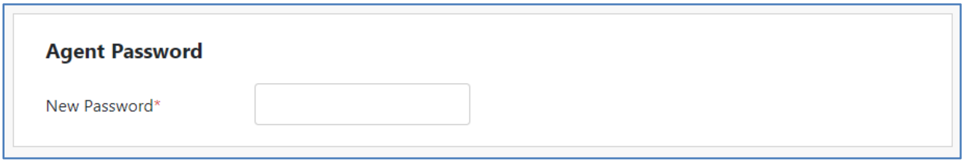
Protect against objects not yet on your network:

| Hash / File Path | Type | Notes | Actions |
|---|---|---|---|

No data to display

## Agent Password

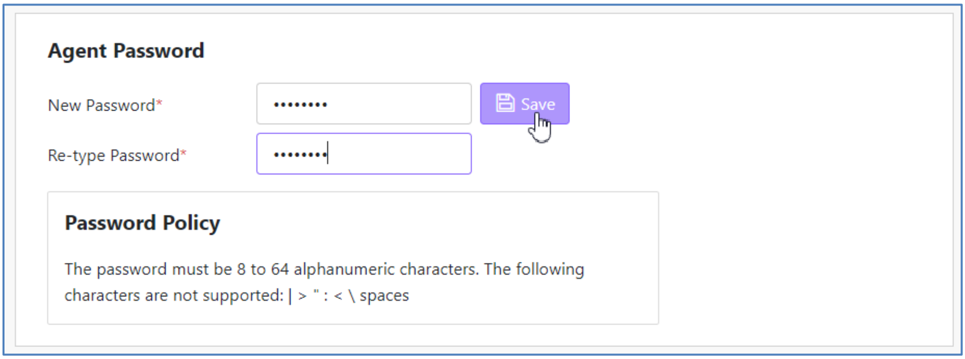
This function allows OT administrators to change the StellarProtect admin password for all connected endpoints via StellarOne.



Agent Password

New Password*

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



**Agent Password**

New Password* ••••••••

Re-type Password* ••••••••

**Password Policy**

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

## ICS Application Safeguard

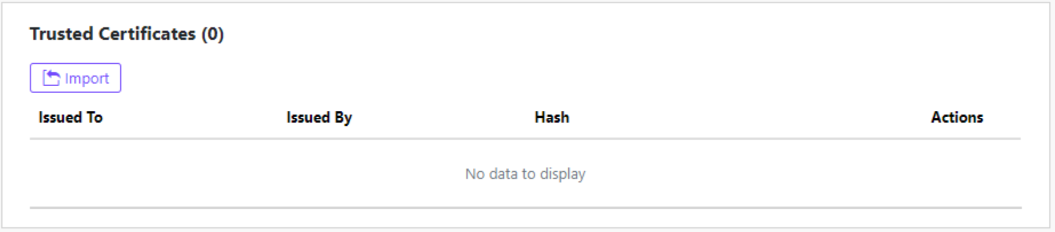
ICS Application Safeguard is industrial-based change control protection.

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

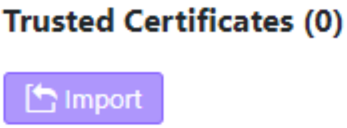
The policy 'Trusted Certificates' provides an import function allowing the administrator to add new trusted certificates.


Trusted Certificates (0)

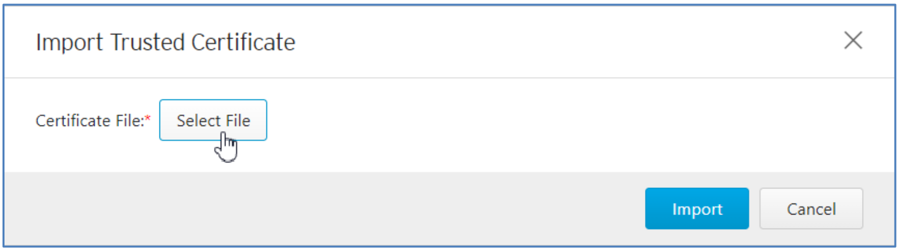
| Issued To | Issued By | Hash | Actions |
|---|---|---|---|

No data to display

Click the ‘Import’ icon to import a new trusted certificate.

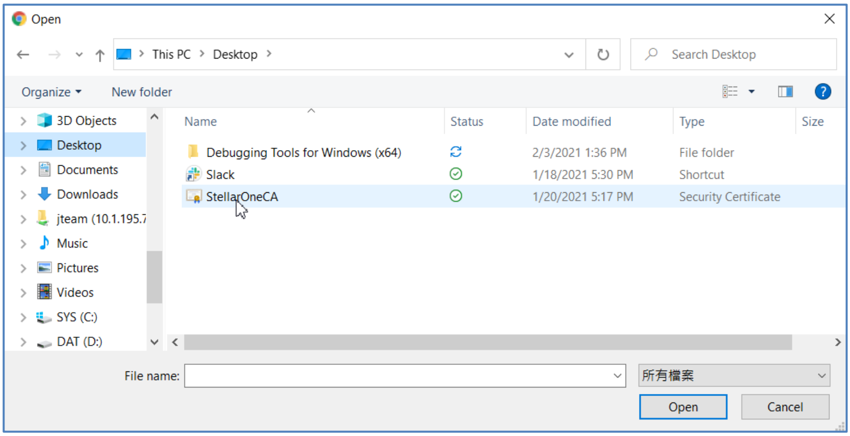

Trusted Certificates (0)

Click ‘Select File’ to browse certificate files.


Import Trusted Certificate

Certificate File:*

Select the specific certificate file.



Open

This PC > Desktop >

Search Desktop

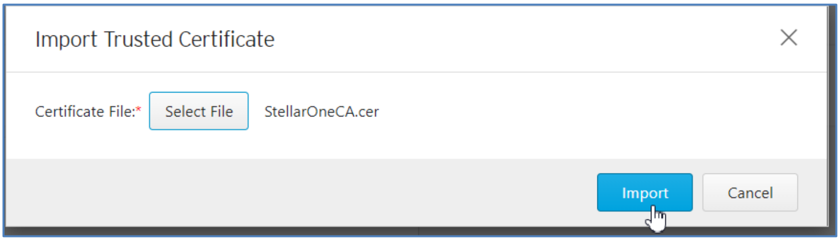
Organize ▾ New folder

| Name | Status | Date modified | Type | Size |
|---|---|---|---|---|
| Debugging Tools for Windows (x64) | | 2/3/2021 1:36 PM | File folder | |
| Slack | | 1/18/2021 5:30 PM | Shortcut | |
| StellarOneCA | | 1/20/2021 5:17 PM | Security Certificate | |

File name:

所有檔案

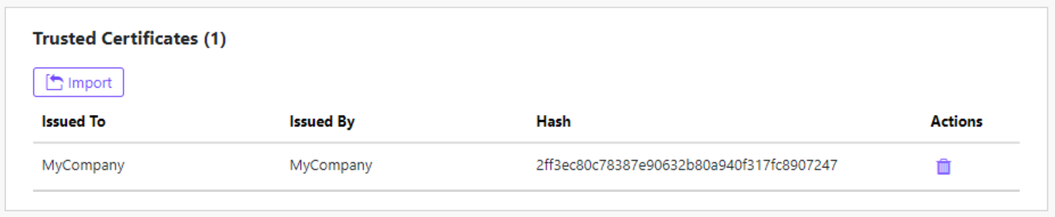
Then click the ‘Import’ button to finish the function.



Import Trusted Certificate

Certificate File:* Select File StellarOneCA.cer

You can have an updated certificate list here.



Trusted Certificates (1)

| Issued To | Issued By | Hash | Actions |
|---|---|---|---|
| MyCompany | MyCompany | 2ff3ec80c78387e90632b80a940f317fc8907247 | 🗑 |

## 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.

#### Initiating Scan Now

You can initiate ‘Scan Now’ on one or more agent endpoints that you suspect to be infected.

**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’.

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

## 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’.

## Delete

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.

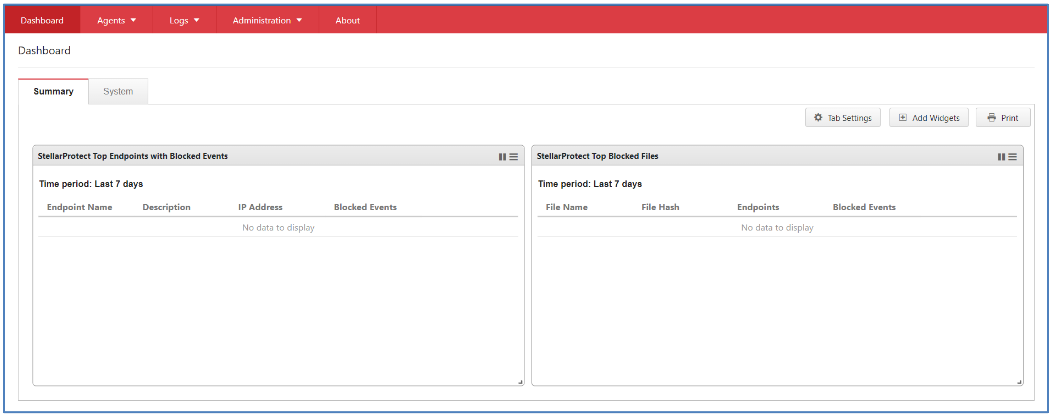
# Overview

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

Time period: Last 7 days

| Endpoint Name | Description | IP Address | Blocked Events |
|---|---|---|---|
| No data to display | | | |

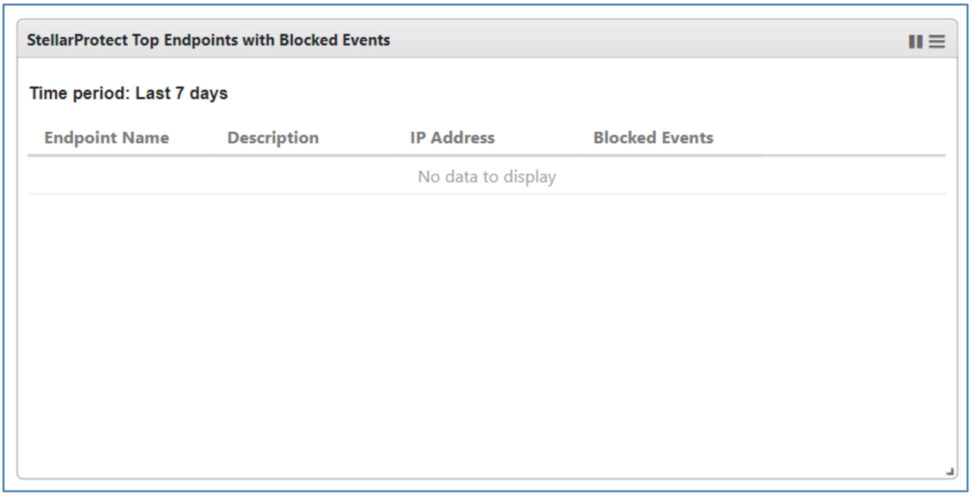
StellarProtect Top Blocked Files

Time period: Last 7 days

| File Name | File Hash | Endpoints | Blocked Events |
|---|---|---|---|
| No data to display | | | |

## 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**.



StellarProtect Top Endpoints with Blocked Events

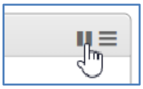
Time period: Last 7 days

| Endpoint Name | Description | IP Address | Blocked Events |
|---|---|---|---|
| No data to display | | | |

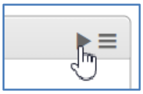
Column descriptions are as follows:

| 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 |

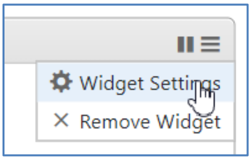
The dashboard will be refresh automatically. You can click the pause icon to stop the automatic refresh.



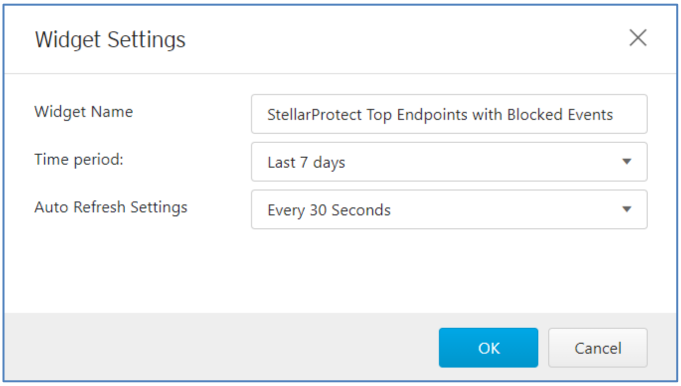
Click the start icon to enable the automatic refresh.



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.



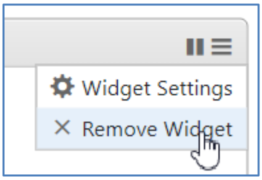
Widget Settings

Widget Name: StellarProtect Top Endpoints with Blocked Events

Time period: Last 7 days

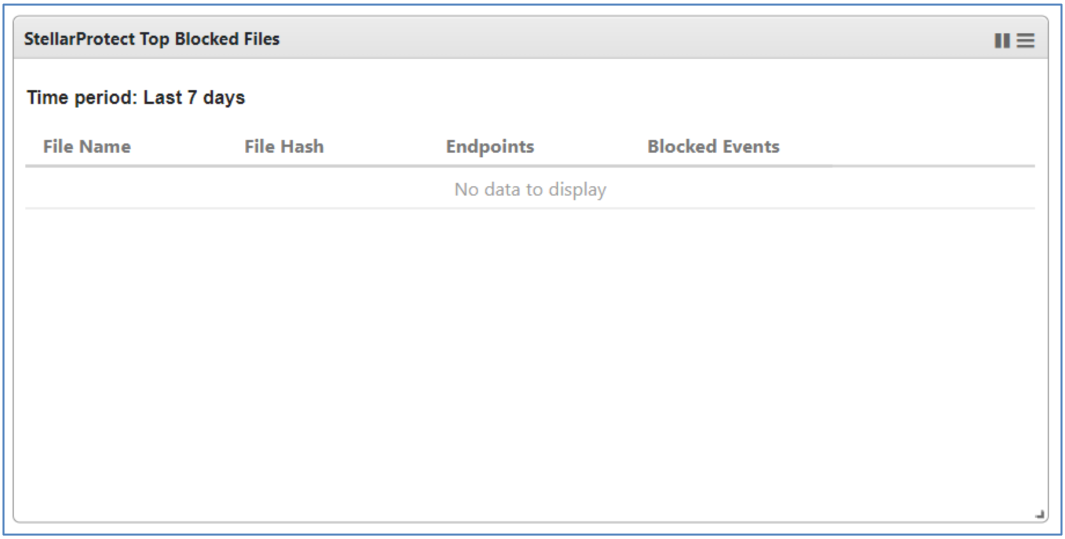
Auto Refresh Settings: Every 30 Seconds

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.



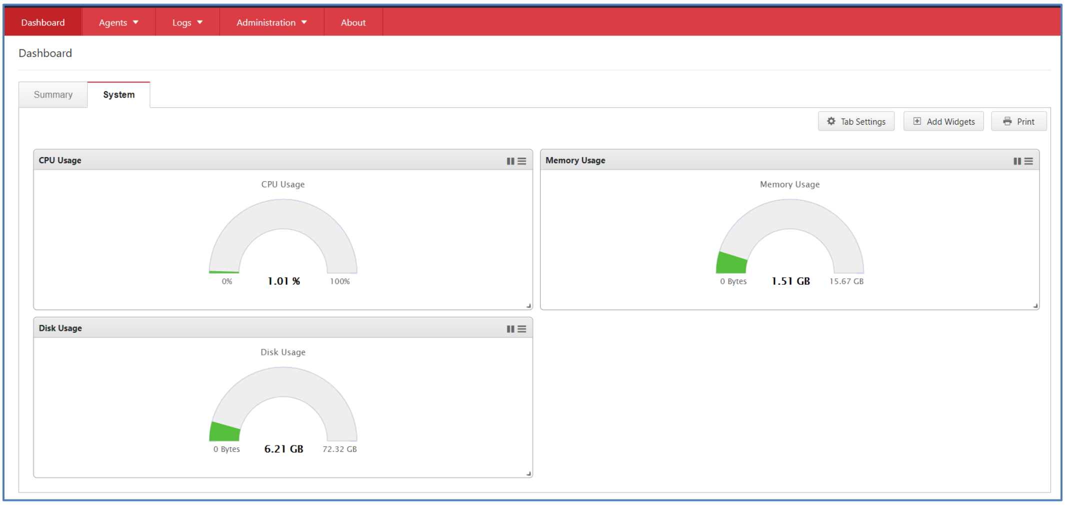
StellarProtect Top Blocked Files

Time period: Last 7 days

| File Name | File Hash | Endpoints | Blocked Events |
|---|---|---|---|
| No data to display | | | |

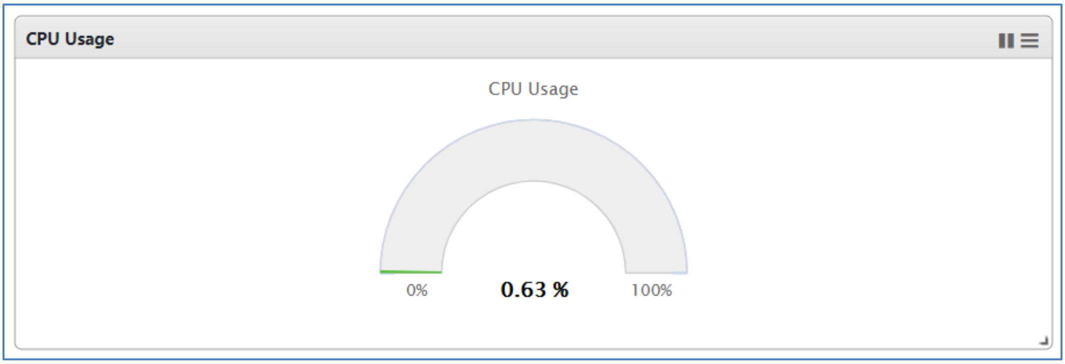
This widget will show the blocked file name, hash value (in SHA-2 standard), endpoint's name, and any related blocked events.

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



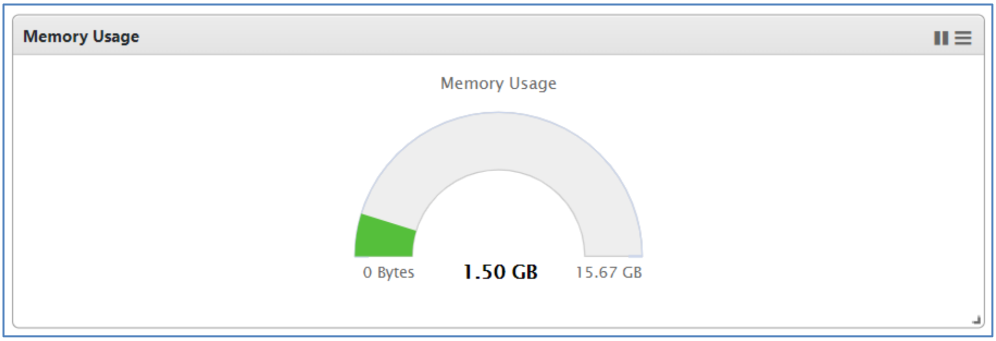
## CPU Usage

This widget displays CPU usage information.



## Memory Usage

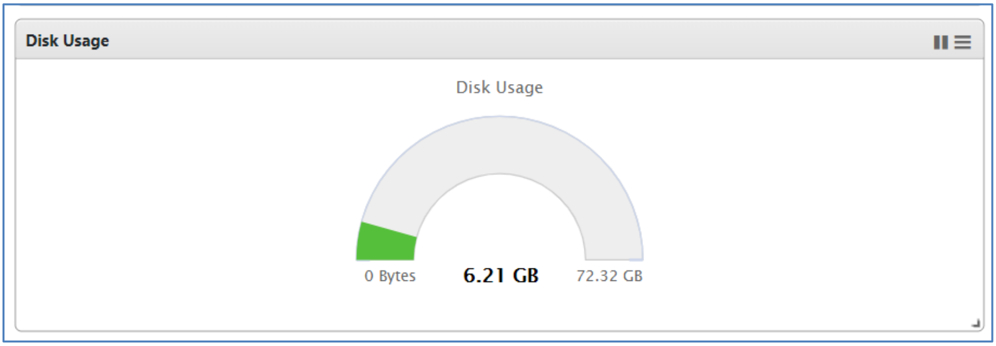
This widget displays memory usage information.



Memory Usage

## Disk Usage

This widget displays disk usage information.



Disk Usage

# 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.

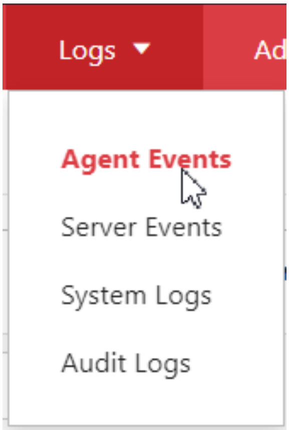
- Audit Logs

  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

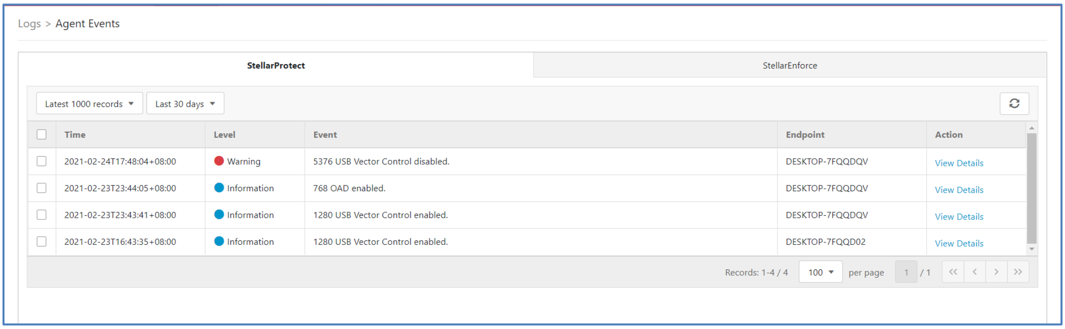
Event and device information will be sent to StellarOne periodically, which includes data about every time an event is triggered by the device. According to the severity, the events will be labeled ‘warning’, ‘critical’ or ‘information’. A ‘warning’ indicates that a serious security incident has occurred 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. If a modification is made, it is recommended to judge whether it is correct and perform post-processing. ‘Information’ refers to general events that usually do not compromise safety.

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

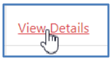
**StellarProtect** | StellarEnforce

Latest 1000 records ▾ | Last 30 days ▾

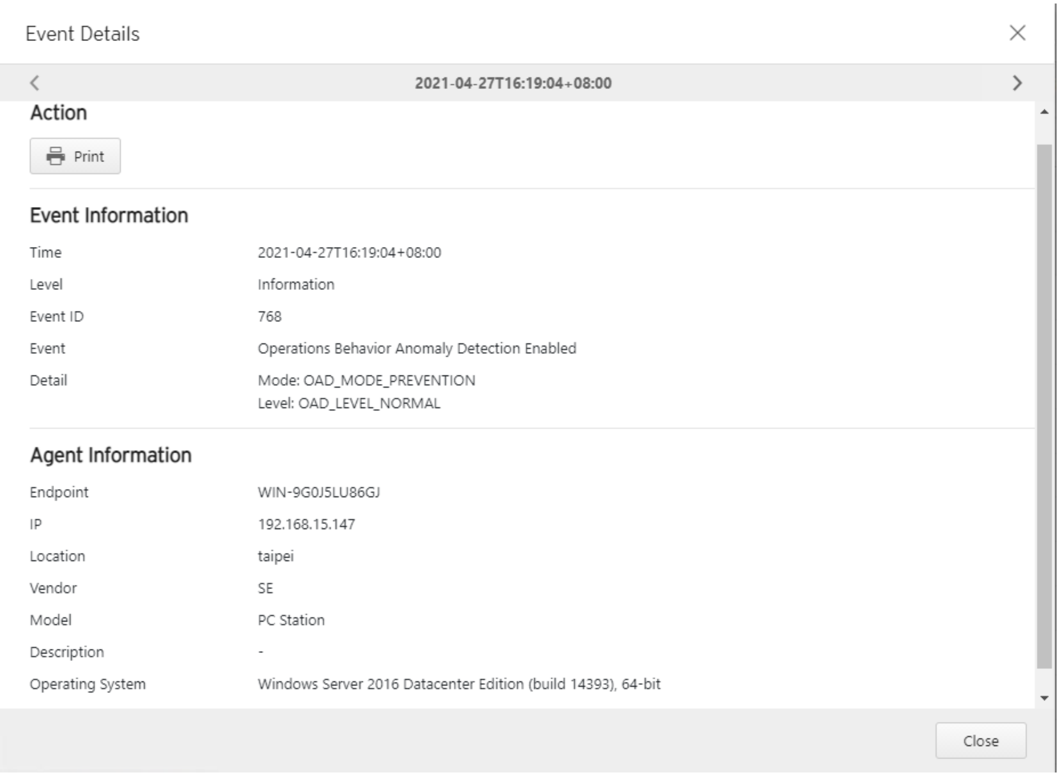
| □ | Time | Level | Event | Endpoint | Action |
|---|---|---|---|---|---|
| □ | 2021-02-24T17:48:04+08:00 | ● Warning | 5376 USB Vector Control disabled. | DESKTOP-7FQQDQV | View Details |
| □ | 2021-02-23T23:44:05+08:00 | ● Information | 768 OAD enabled. | DESKTOP-7FQQDQV | View Details |
| □ | 2021-02-23T23:43:41+08:00 | ● Information | 1280 USB Vector Control enabled. | DESKTOP-7FQQDQV | View Details |
| □ | 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 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<br>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 |

## 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

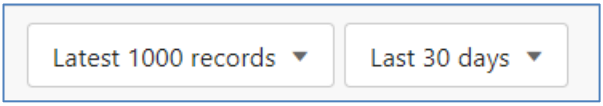
   The description of the endpoint, which might include the ICS product critical description or relative information.

7. Operating System

   The OS name with version.

## Filtering & Refresh

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

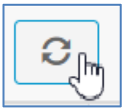


Latest 1000 records ▾

Last 30 days ▾

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

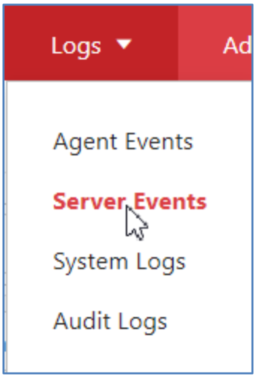
In addition, you can click the ‘refresh’ icon to refresh the event list.



## 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

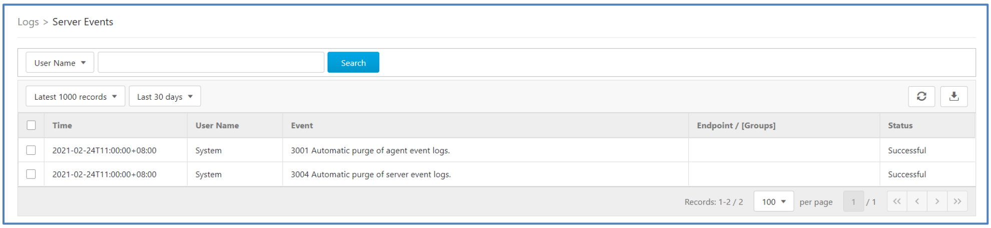
   A description of the event, including event ID.

4. Endpoint / [Group]

   Endpoint name and its group name.

5. Status

   The result of the server event.



Logs > Server Events

| □ | Time | User Name | Event | Endpoint / [Groups] | Status |
|---|---|---|---|---|---|
| □ | 2021-02-24T11:00:00+08:00 | System | 3001 Automatic purge of agent event logs. | | Successful |
| □ | 2021-02-24T11:00:00+08:00 | System | 3004 Automatic purge of server event logs. | | Successful |

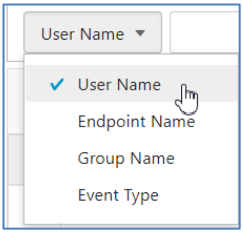
Records: 1-2 / 2   100 ▾ per page   1 / 1

**Note**

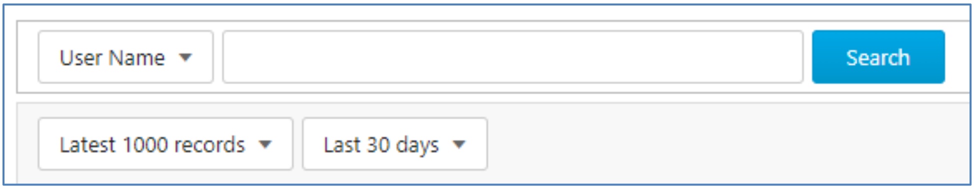
Server event logs contain collected information about actions taken by policies as well as StellarOne console users.

## Search & Refresh

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

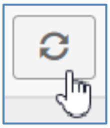


You can filter events using the number of records and a time limit.



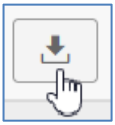
Event records will be updated automatically after you change the filter settings.

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

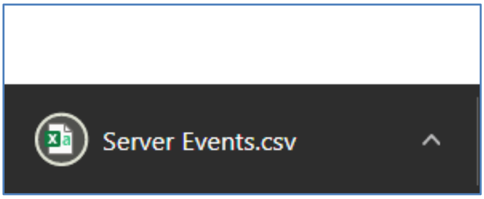


## Export

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.

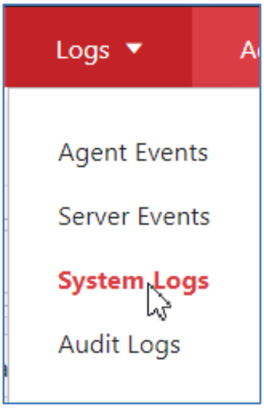


Server Events.csv

## System Logs

This shows the system logs for StellarOne.

You can select Logs > System Logs:



### Logs Details

Details are shown as follows:

1. Time

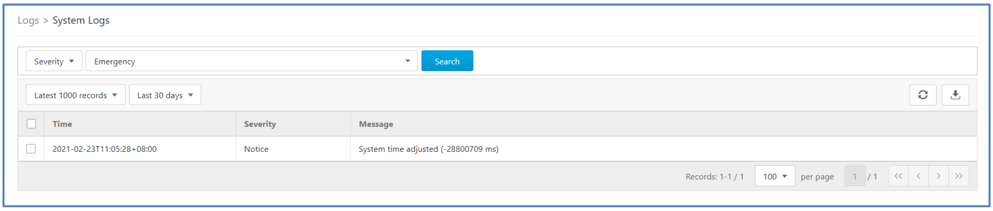
   The event date and time, it following the UTC standard format for date and time.

2. Severity

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

3. Message

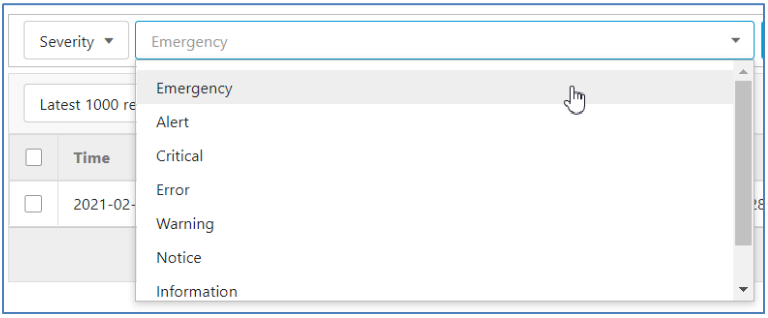
   This will be the log message content, which will contain important environmental parameters, key activities, and results.



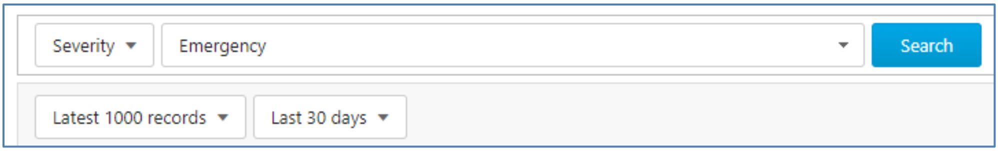
| □ | Time | Severity | Message |
|---|---|---|---|
| □ | 2021-02-23T11:05:28+08:00 | Notice | System time adjusted (-28800709 ms) |

## 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.



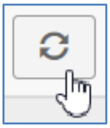
Severity: Emergency

Latest 1000 records

Last 30 days

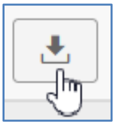
The event records will be updated automatically after you change the filter setting.

You can click the ‘refresh’ icon to refresh the event list.

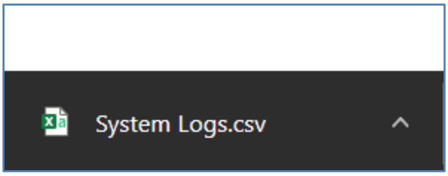


## Export

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

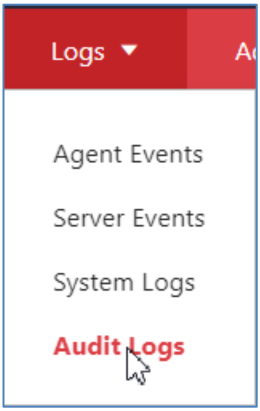


A file named “Server Events.csv” will be prepared for export.



## 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

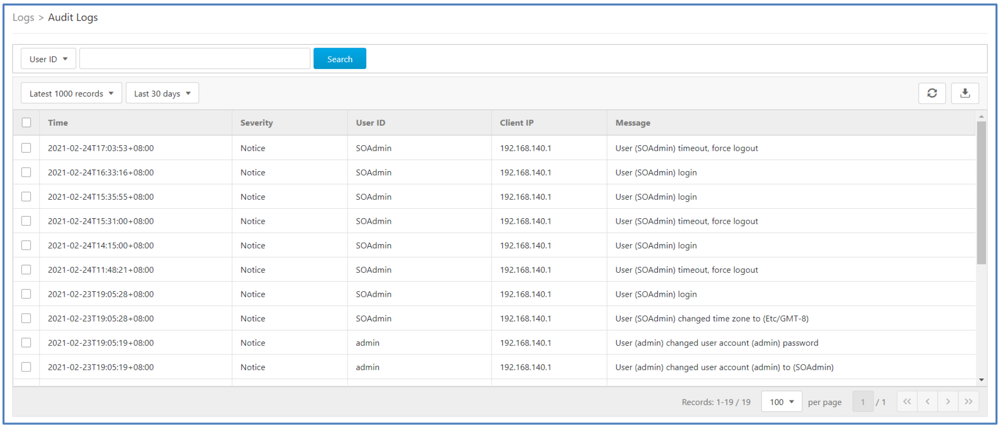
   The ID of the user responsible for the change.

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.



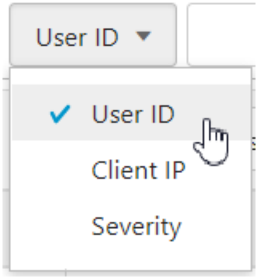
Logs > Audit Logs

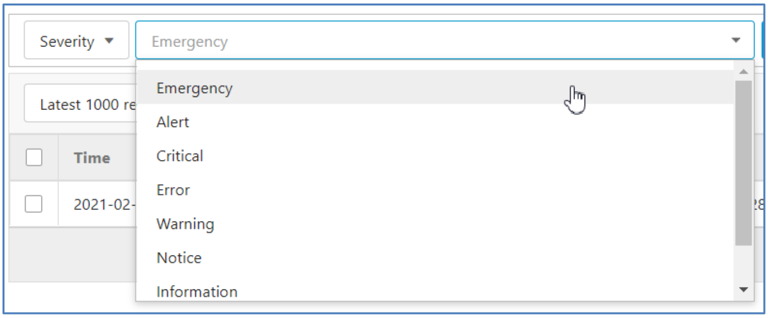
| □ | Time | Severity | User ID | Client IP | Message |
|---|---|---|---|---|---|
| □ | 2021-02-24T17:03:53+08:00 | Notice | SOAdmin | 192.168.140.1 | User (SOAdmin) timeout, force logout |
| □ | 2021-02-24T16:33:16+08:00 | Notice | SOAdmin | 192.168.140.1 | User (SOAdmin) login |
| □ | 2021-02-24T15:35:55+08:00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

Records: 1-19 / 19 100 ▾ per page 1 / 1

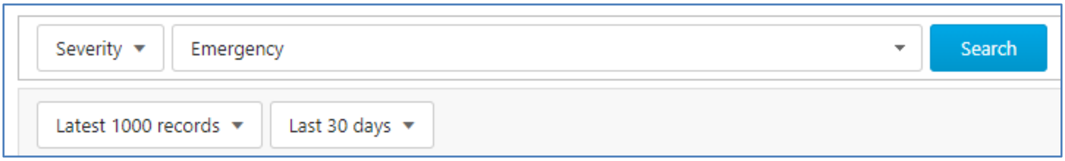
## Search & Refresh

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’.



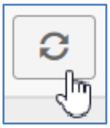


You can also filter events using the number of records and time limit.



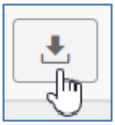
The event records will be updated automatically after you change the filter settings.

You can click the ‘refresh’ icon to refresh the event list.

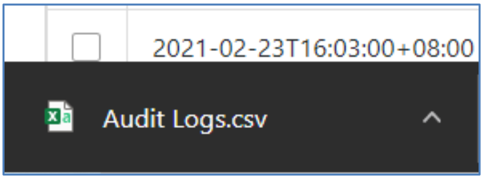


## Export

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.



2021-02-23T16:03:00+08:00

Audit Logs.csv

# Chapter 4

## Administration

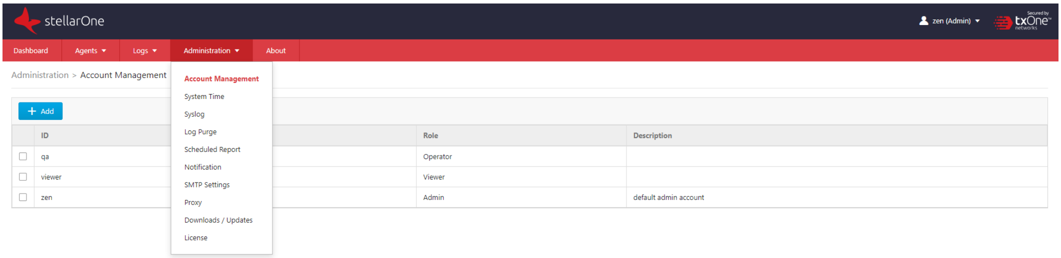
This chapter introduces administration practices for StellarOne.

# Overview

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

1. Account Management
2. System Time
3. Proxy
4. Downloads / Updates
5. License

Users can select one of these functions from the Administration tab of StellarOne. Other functions on this list are for managing StellarEnforce, and are only necessary if StellarOne is also connected to endpoints running StellarEnforce.

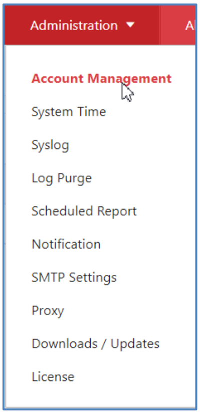


Administration > Account Management

|   | ID | Role | Description |
|---|---|---|---|
| □ | qa | Operator | |
| □ | viewer | Viewer | |
| □ | zen | Admin | default admin account |

# Account Management

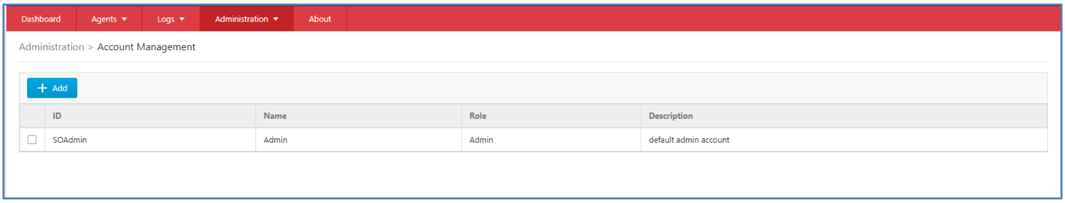
User can select Administration > Account Management to configure or manage StellarOne accounts.



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

| ACCOUNT TYPE | PRIVILEGES |
|---|---|
| Administrator | • Add, edit, enable, disable, or delete StellarOne console accounts from the **Account Management** screen<br>• Modify their own account description and password<br>• Specify actions to take on files blocked by agents<br>• View the StellarOne console **Logs** > **Server Events** screen<br>• Allow or block storage device access on managed endpoints |
| Operator | • Modify their own account description, email address, and password<br>• Specify actions to take on files blocked by agents<br>• View the StellarOne console **Logs & Reports** > **Server Events** screen<br>• Allow or block storage device access on managed endpoints |
| Viewer | • Modify their own account description, email address, and password<br>• View the StellarOne console **Logs & Reports** > **Server Events** screen |

Then system will show you all valid accounts as follows:

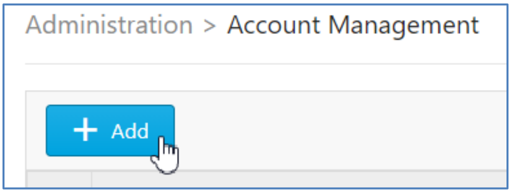


|  | ID | Name | Role | Description |
|---|---|---|---|---|
| □ | SOAdmin | Admin | Admin | default admin account |

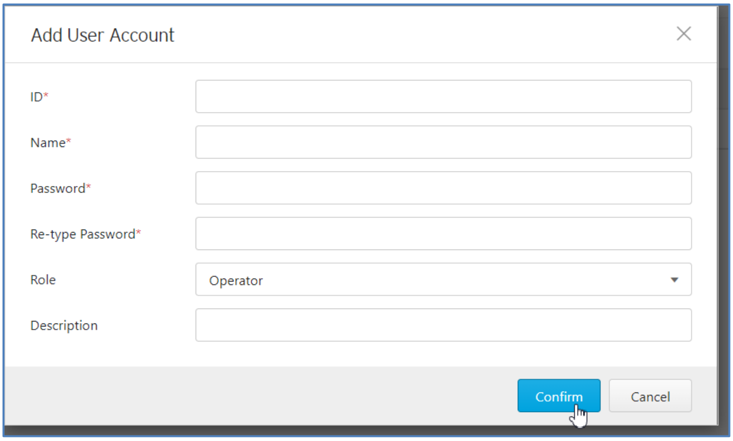
Information shown under account management will include:

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. Description: The description details for this account.

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



A table will appear where you can input ID, name, role, and description, as well as enter the password for the new account twice. Click 'Confirm' to create a new account.



Add User Account

ID*

Name*

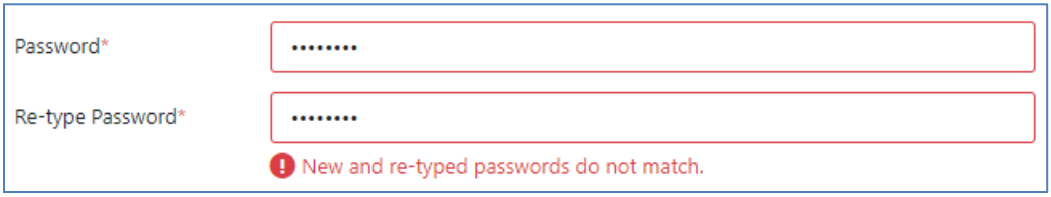
Password*

Re-type Password*

Role: Operator

Description

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.

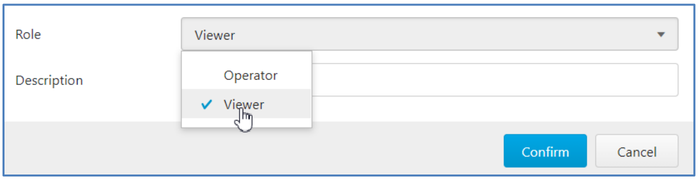


Password*: ••••••••

Re-type Password*: ••••••••

New and re-typed passwords do not match.

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



Role: Viewer

Description

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.

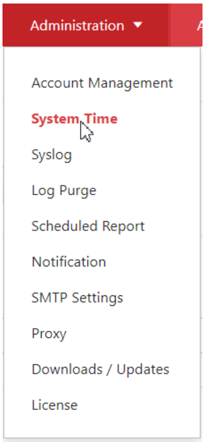
| Task | Account Privilege Required |
|---|---|
| Configure Industrial-Grade Next-Generation Antivirus | • Admin<br>• Operator |
| Configure USB Vector Control | • Admin<br>• Operator |
| Configure User-Defined Suspicious Objects | • Admin<br>• Operator |
| Configure DLL Injection Protection | • Admin<br>• Operator |
| Configure Agent Password | • Admin<br>• Operator |
| Configure Operations Behavior Anomaly Detection | • Admin<br>• Operator |
| Configure ICS application safeguard | • Admin<br>• Operator |

| | |
|---|---|
| Configure Trusted Certifications | • Admin<br>• Operator |
| Configure Group Policy | • Admin<br>• Operator |
| Configure Global Policy | • Admin<br>• Operator |
| Send Configure Change Window Command | • Admin<br>• Operator |
| Send Scan Now Command | • Admin<br>• Operator |
| Organize<br>(Edit Tags/ Move / Delete) | • Admin<br>• Operator |
| Monitor Server Event logs | • Admin<br>• Operator |
| Monitor Agent Event logs | • Admin<br>• Operator<br>• Viewer |
| Account Management | • Admin<br>• Operator |
| System Time | • Admin<br>• Operator |
| Proxy | • Admin<br>• Operator |

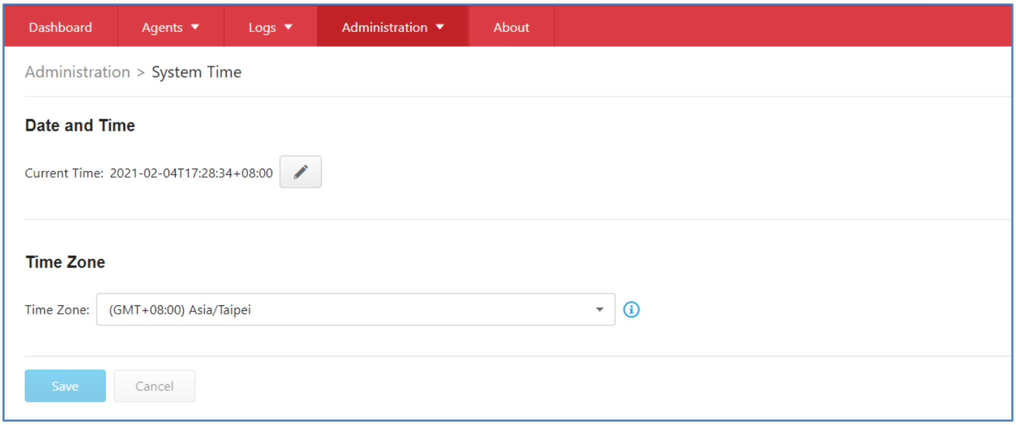
| | |
|---|---|
| Downloads / Updates | • Admin<br>• Operator<br>• Viewer |
| License | • Admin<br>• Operator |

# 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.



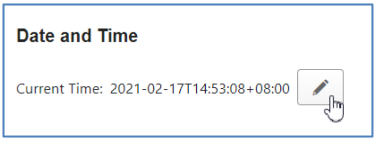
Date and Time

Current Time: 2021-02-04T17:28:34+08:00

Time Zone

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

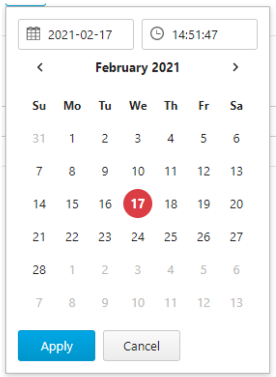
You can modify the Date and Time as below:



Date and Time

Current Time: 2021-02-17T14:53:08+08:00

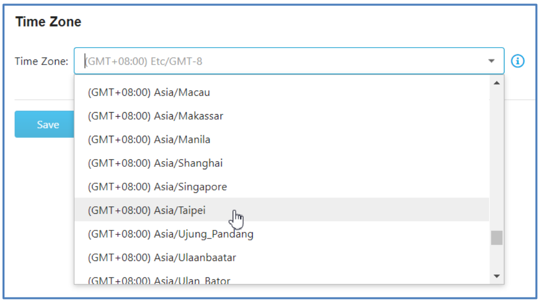
A calendar will appear where you can select the current date and time.



2021-02-17 | 14:51:47

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

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



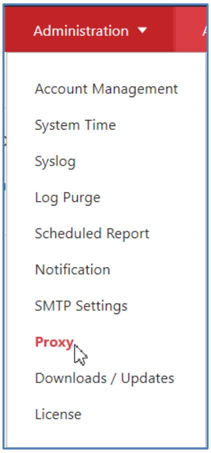
Time Zone

Time Zone: (GMT+08:00) Etc/GMT-8

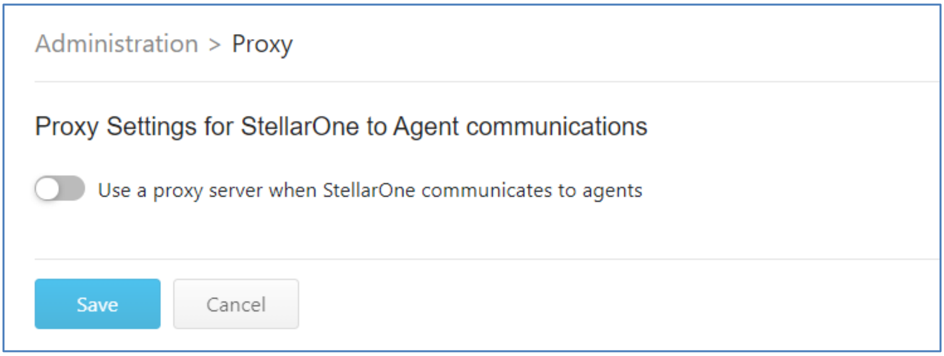
Save
(GMT+08:00) Asia/Macau
(GMT+08:00) Asia/Makassar
(GMT+08:00) Asia/Manila
(GMT+08:00) Asia/Shanghai
(GMT+08:00) Asia/Singapore
(GMT+08:00) Asia/Taipei
(GMT+08:00) Asia/Ujung_Pandang
(GMT+08:00) Asia/Ulaanbaatar
(GMT+08:00) Asia/Ulan_Bator

# Proxy

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



A window will appear as follows:

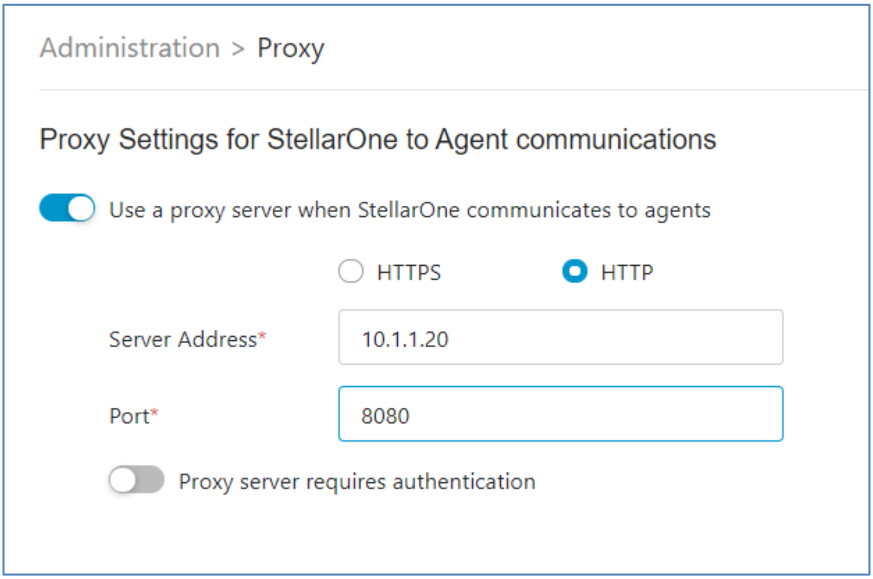


Administration > Proxy

Proxy Settings for StellarOne to Agent communications

○ Use a proxy server when StellarOne communicates to agents

Please enable “Use a proxy server when StellarOne communicates to agents” and finish the server settings including choosing a protocol (HTTP or HTTPS) and entering a server IP address with port number.



Administration > Proxy

Proxy Settings for StellarOne to Agent communications

Use a proxy server when StellarOne communicates to agents

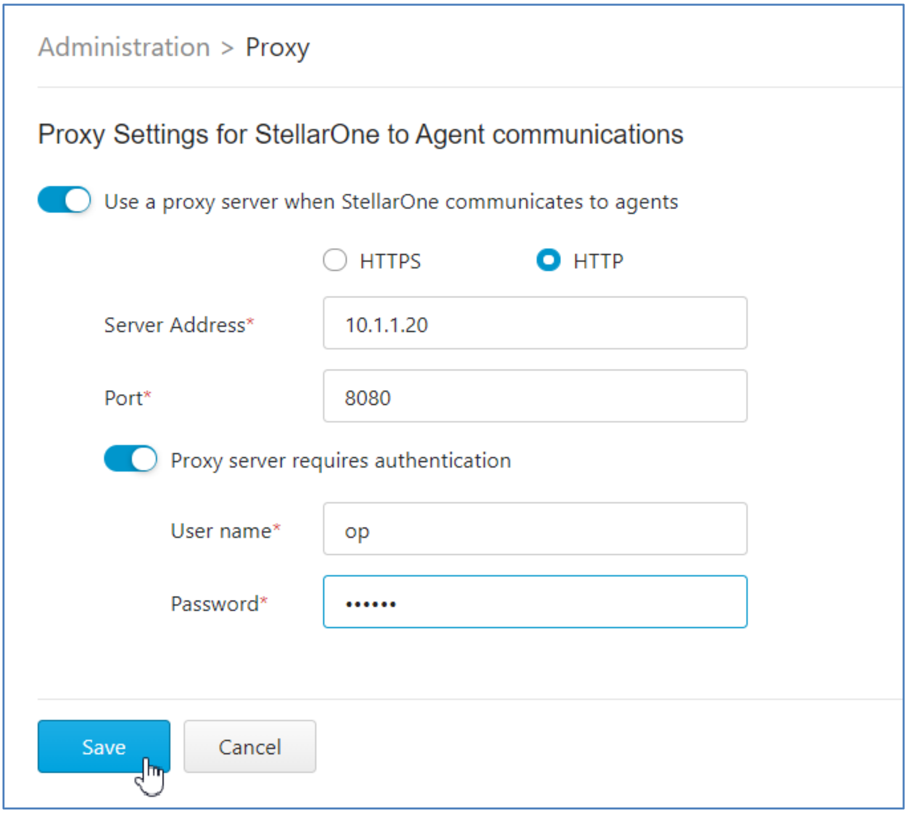
○ HTTPS ● HTTP

Server Address* 10.1.1.20

Port* 8080

Proxy server requires authentication

If the proxy server requires authentication, please input the correct user name and password as follows.



Administration > Proxy

Proxy Settings for StellarOne to Agent communications

Use a proxy server when StellarOne communicates to agents

○ HTTPS ● HTTP

Server Address* 10.1.1.20

Port* 8080

Proxy server requires authentication

User name* op

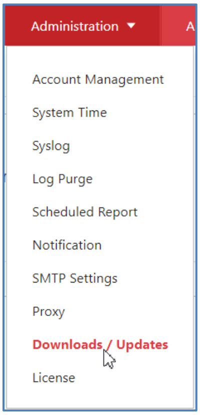
Password* ••••••

Click “Save” to confirm all settings.

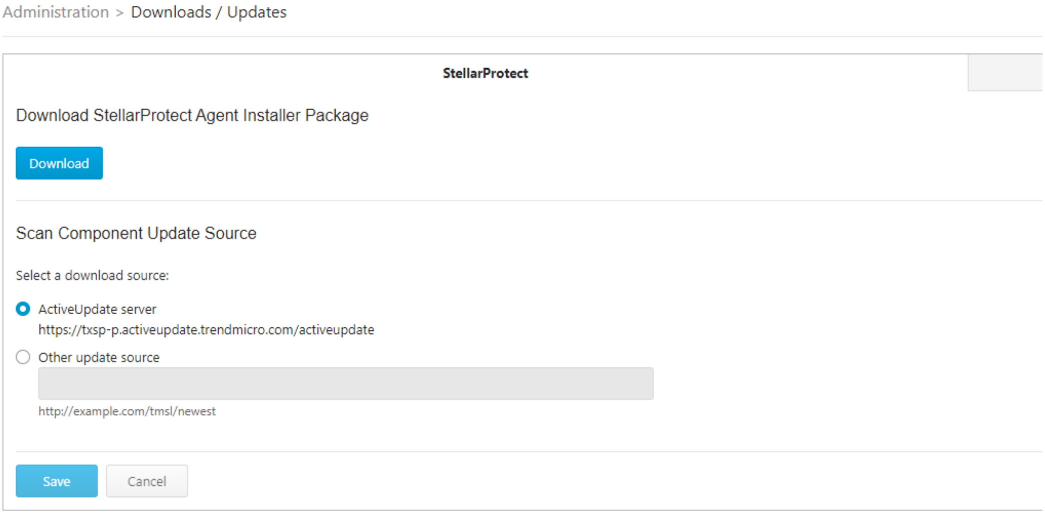
# Downloads / Updates

StellarOne supports update services.

Please select Administration > Downloads / Updates.



If you would like to get an installation package for devices to be managed, please click ‘Download’.



Administration > Downloads / Updates

**StellarProtect**

Download StellarProtect Agent Installer Package

Scan Component Update Source

Select a download source:

● ActiveUpdate server
https://txsp-p.activeupdate.trendmicro.com/activeupdate

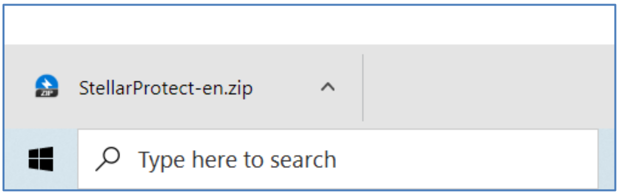
○ Other update source

http://example.com/tmsl/newest

User can configure the update source from this page. When agents attempt to update scan components, they will get the update source information from this setting.

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

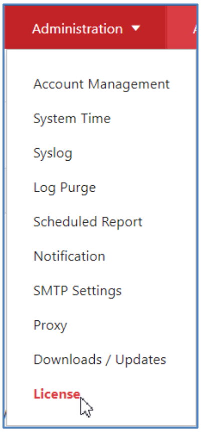
It can be decompressed and used to install an agent on devices intended to be managed by StellarOne.



StellarProtect-en.zip

# License

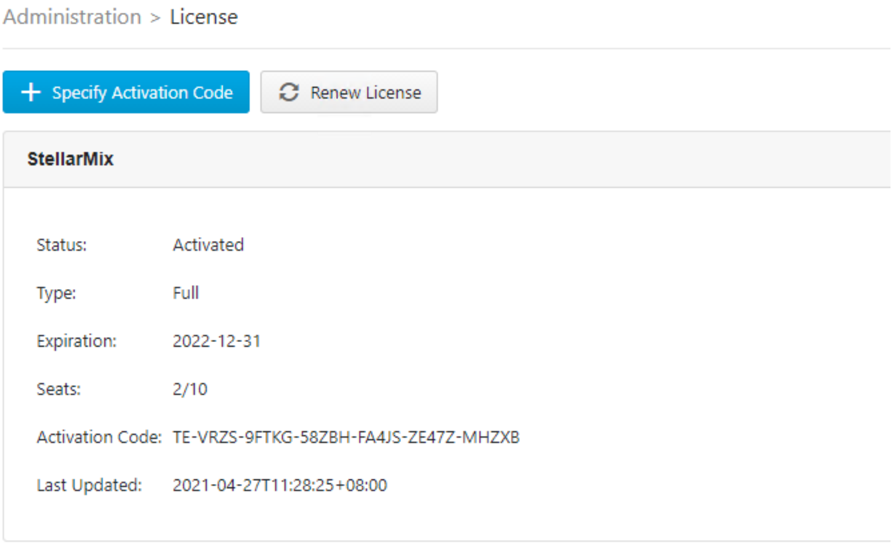
If you would like to view or add additional licenses, please select Administration > License.



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.



StellarMix

Status: Activated

Type: Full

Expiration: 2022-12-31

Seats: 2/10

Activation Code: TE-VRZS-9FTKG-58ZBH-FA4JS-ZE47Z-MHZXB

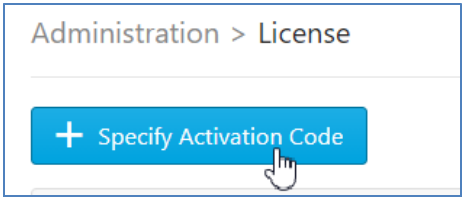
Last Updated: 2021-04-27T11:28:25+08:00

**Note**

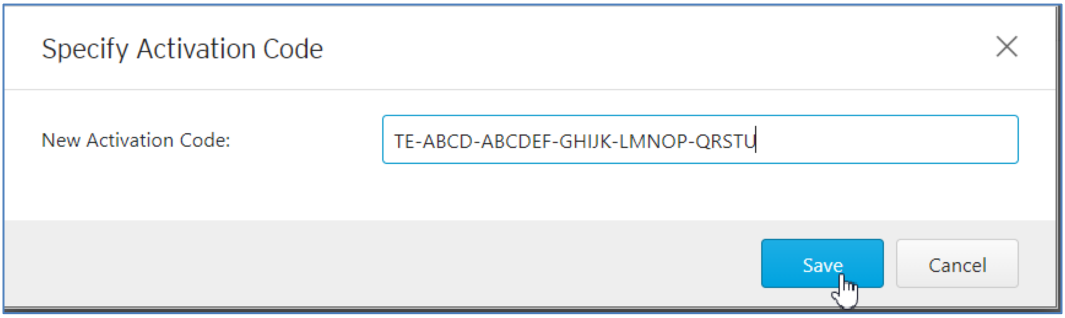
Click **Refresh** to update your product license. A connection with the TXOne product license server is required.

## 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.



New Activation Code: TE-ABCD-ABCDEF-GHIJK-LMNOP-QRSTU

## Seat Count

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

# Chapter 5

## 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<br>225 E. John Carpenter Freeway, Suite 1500<br>Irving, Texas 75062 U.S.A. |
| Phone | Phone: +1 (817) 569-8900<br>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: SLEM19269/210330