txOne networks | Keep the Operation Running

2.0 TXOne StellarOne for StellarEnforce

Administrator's Guide

The trust list-based solution for locking down fixed-function computers

Windows

SC 2022 awards EUROPE WINNER

TXOne Networks Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available at:
http://docs.trendmicro.com/en-us/enterprise/txone-stellarenforce.aspx

Document Part No.: APEM139610/220926
Release Date: September 2022
Protected by U.S. Patent No.: Patents pending.

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

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

Privacy and Personal Data Collection Disclosure

Certain features available in TXOne 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 Networks is subject to the conditions stated in the TXOne Networks Privacy Notice:

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

Table of Contents

Preface

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

Audience

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

Document Conventions

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

Table 1. Document Conventions

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

Terminology

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

Terminology	Description
server	The StellarOne server program
server endpoint	The host where the StellarOne server is installed
agents	The hosts running the StellarEnforce program
managed agents managed endpoints	The hosts running the StellarEnforce 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
web 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
agent installation folder	The folder on the host that contains the StellarEnforce agent files. If you accept the default settings during installation, you will find the installation folder at the following location: "c:\Program Files\TXOne\StellarEnforce"

Chapter 1 - Introduction

Overview

TXOne StellarOne is a centralized management console designed to streamline administration of both TXOne StellarEnforce for legacy systems and TXOne StellarProtect for modernized systems. This manual will focus on its use for TXOne StellarEnforce: a simple, no-maintenance solution to lock down and protect fixed-function computers, helping protect businesses against security threats and increase productivity.

About TXOne StellarOne

TXOne StellarOne provides centralized monitoring and management of StellarEnforce agent deployment, status, and events. For example, administrators can create agent Approved Lists and change agent Application Lockdown states.

Server Features and Benefits

TXOne StellarOne includes the following features and benefits.

Feature	Benefit
Dashboard	The web console dashboard provides summarized information about monitored StellarEnforce agents. Administrators can check deployed StellarEnforce agent status easily, and can generate security reports related to StellarEnforce agent activity for specified periods.
Centralized Agent Management	TXOne StellarOne allows administrators to perform the following tasks: • Monitor StellarEnforce agent status • Examine connection status • View configurations • Collect agent logs on-demand or by policy • Turn agent Application Lockdown on or off • Enable or disable agent Device Control • Configure agent Maintenance Mode settings • Update agent components • Initialize the Approved List • Deploy agent patches • Add trusted files and USB devices
Centralized Event Management	On endpoints protected by StellarEnforce agents, administrators can monitor status and events, as well as respond when files are blocked from running. StellarOne provides event management features that let administrators quickly know about and take action on blocked file events.
Server Event Auditing	Operations performed by StellarOne web console accounts are logged. StellarOne records an operating log for each account, tracking who logs on, who deletes event logs, and more.

What’s New

TXOne StellarOne for StellarEnforce 2.0 includes the following new features and enhancements.

Feature	Description
Self-management Group Policy	This newly-added group policy allows the operators on site to configure the agents' policy settings on their own. Once being switched to the self-management status, the local agents are free from the StellarOne console's policy management.
Open API	Provides open API for users to query data from agents. Users can also generate API keys and set the expiration dates for different user accounts for account management.

Chapter 2 – Agent / Group Management

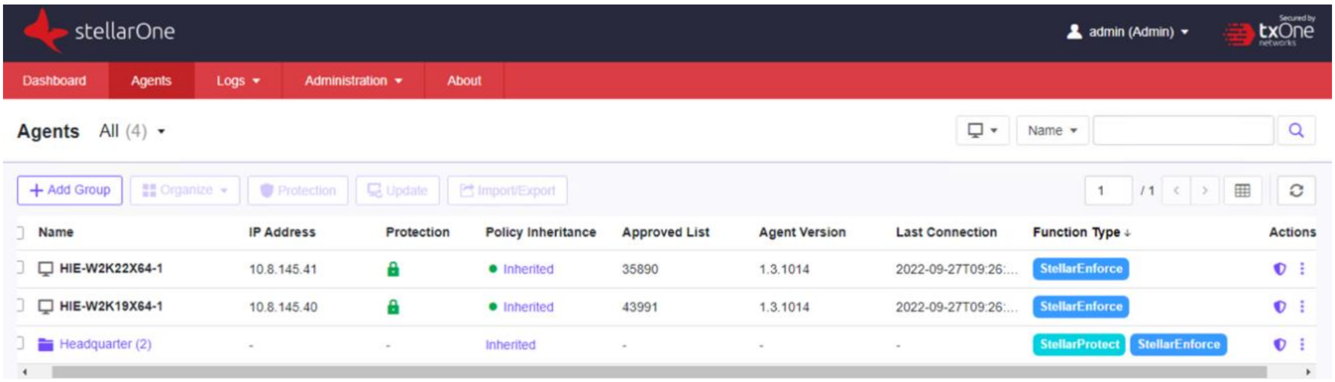
Managing StellarEnforce Agents

This chapter introduces the web console screen for agent management.

About the Agents Screen

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

> **Note:** All agents are under the **All** group by default. 📁 icon indicates a group and 🖥 icon indicates an agent.



Name	IP Address	Protection	Policy Inheritance	Approved List	Agent Version	Last Connection	Function Type ↓	Actions
HIE-W2K22X64-1	10.8.145.41	🔒	● Inherited	35890	1.3.1014	2022-09-27T09:26:...	StellarEnforce	⋮
HIE-W2K19X64-1	10.8.145.40	🔒	● Inherited	43991	1.3.1014	2022-09-27T09:26:...	StellarEnforce	⋮
Headquarter (2)	-	-	Inherited	-	-	-	StellarProtect StellarEnforce	⋮

Manage the Agent Tree

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

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

Add Groups

Procedure

1. Go to **Agents** in the navigation at the top of the web console. The Agents screen will appear.
2. Start from the **All** group on the **Agent view**.
3. Click the group name to navigate to a target parent group to create a new group.

4. Click + Add Group button on the above control area.
5. The **Add Group** window will appear.
6. Input the group name and select **Confirm**

Note:

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

Rename Groups

Procedure

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

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

Remove Groups / Unregister Agents

Procedure

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

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

Search for Agents/Groups

Procedure

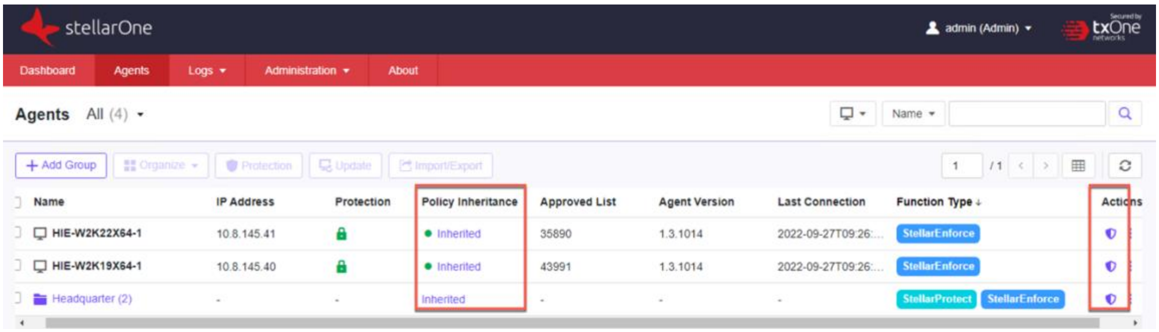
1. Go to **Agents** in the navigation at the top of the web console. The Agents screen will appear.
2. Search for specific endpoints by selecting criteria from the drop-down list and specify additional search criteria as required.

Option	Description
Name	The name of the agent. Type the full or partial endpoint host name to locatethe specific agent.
IP Address	Type the IPv4 address.
IP Range	Type the IPv4 address range.
Group	The name of the group. Select the available group.
Policy Inheritance	The mode of Policy Inheritance. Select **Inherited** or **Customized**.
Policy Deployment	The status of policy deployment from StellarOne to Agents. Select **Completed** or **In Progress**.
Agent Version	Type the Agent Version.
Last Connection	Last connection time. Select the default time range or select Custom to specify your own range. Default time range: • Last 1 hour • Last 24 hours • Last 7 days • Last 30 days
Function Type	Select **StellarEnforce** or **StellarProtect.**
Operating System	Select an operating system.
Description	Type the full or partial description to query specific endpoints.

Chapter 3 – Policy Management

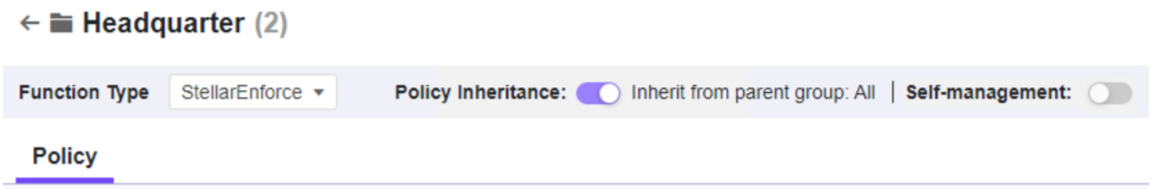
Manage Group/Agent Policy

- The user can add the group with agents, and then inherit **Group Policy** from the parent group or customize its own Group Policy.
- The agent can also have its own customized **Agent Policy** instead of inheriting from the parent group.



Name	IP Address	Protection	Policy Inheritance	Approved List	Agent Version	Last Connection	Function Type ↓	Actions
HIE-W2K22X64-1	10.8.145.41	🔒	● Inherited	35890	1.3.1014	2022-09-27T09:26:...	StellarEnforce	
HIE-W2K19X64-1	10.8.145.40	🔒	● Inherited	43991	1.3.1014	2022-09-27T09:26:...	StellarEnforce	
Headquarter (2)	-	-	Inherited	-	-	-	StellarProtect StellarEnforce	

- For a group with agents, the user can switch between the Function Type (StellarProtect or StellarEnforce) to display its **Policy**.

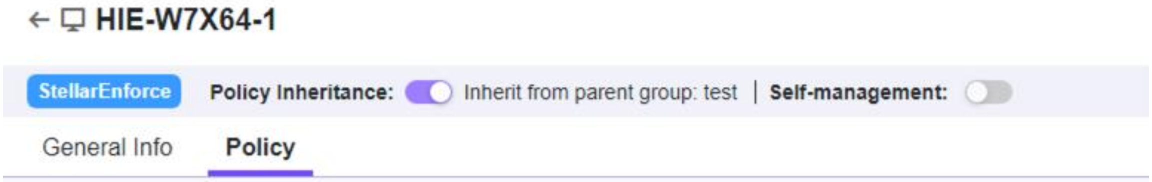


← Headquarter (2)

Function Type: StellarEnforce

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

- For an agent, the user can switch between tabs to display its **General Info** and **Policy**.



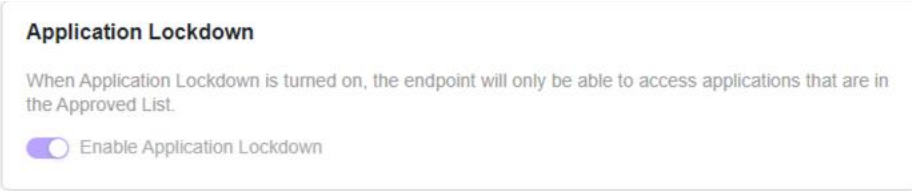
← HIE-W7X64-1

StellarEnforce

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

Configure Application Lockdown

When Application Lockdown is turned on, the Agent will only be able to access applications that are in the Approved List. The Approved List can be configured in the **Lockdown Exclusions** which is elaborated in the following sections.



Application Lockdown

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

Enable Application Lockdown

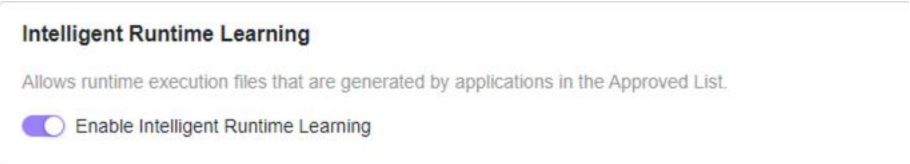
Procedure

1. Navigate to the target agent or agent group on the **Agent view**.
2. Enter the **Policy view** in either method listed below:
   - Click the Policy Inheritance link.
   - Click 🛡, the Policy icon of Actions.
3. Find the **Application Lockdown** pane in the **Policy view**.
4. Click the **Toggle Switch** to disable **Inherit from parent group**.
5. Click the **Toggle Switch** to enable or disable Application Lockdown.

Note: StellarEnforce agent administrators can also change the Application Lockdown status from the StellarEnforce agent console.

Configure Intelligent Runtime Learning

When Intelligent Runtime Learning is turned on, the Agent will allow runtime executable files that are generated by applications in the Trust List.



Intelligent Runtime Learning

Allows runtime execution files that are generated by applications in the Approved List.

Enable Intelligent Runtime Learning

Procedure

1. Navigate to the target agent or agent group on the **Agent view**.
2. Use any of the following methods to enter the **Policy view**:

   - Clcik the **Policy Inheritance** link.
   - Click 🛡, the **Policy** icon of **Actions**.

3. Find the **Application Lockdown** pane in the **Policy view**.
4. Click the Toggle Switch to disable **Inherit from parent group**.
5. Click the **Toggle Switch** to enable or disable Intelligent Runtime Learning.

Configure Lockdown Exclusions

Lockdown Exclusions are used to configure the exclusions from **Application Lockdown**, i.e. user-defined settings of specified applications to be blocked out. The Approved List configured here includes the settings of **Trusted Hash Values**, **Trusted Certificates**, **Exception Paths**, and **Write Protection** from the **Lockdown Exclusions** pane in the **Policy view**.

Trusted Hash Values Settings

Remotely allow applications and files to run on managed assets using hash values.

Calculate Hash Values

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

Procedure

1. Download File Hash Generator tool from the **Trusted Hash Values** area.
2. Execute **WKFileHashGen.exe** from the downloaded folder. The File Hash Generator screen will appear.
3. Use any of the following methods to select files and calculate hash values:

    - Drag and drop folders or files to the File Hash Generator screen.
    - Click the **drop-down** button and click **Add Files** to select files you want to add.
    - Click the **drop-down** button and click **Add Folder** to add all the files in the selected folder.

    Hash values will appear in the File Hash (**SHA-1**) column.

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

Note: To ensure that all necessary files are calculated for hash values, it is recommended to add the root folder of the target application to the **File Hash Generator** for calculation.

Notice that the Add Folder button will only calculate installer files, script files, and files in the **PE** (Portable Executable) format.

Add Trusted Hash Values

Procedure

1. Navigate to the target agent or agent group on the **Agent view**.
2. Use any of the following methods to enter the **Policy view**:

- Clcik the **Policy Inheritance** link.
- Click 🛡, the **Policy** icon of **Actions**.

3. Find the **Trusted Hash Values** section from the **Lockdown Exclusions** pane in the **Policy view**.
4. Fill in hash values and notes.
5. To allow files which are created or modified by trusted installation packages to be automatically added to the Approved List, click the **Toggle Switch** to enable the installer.
6. Click the **Add** button to add a single hash value and the previously-saved settings.

Note: To allow files which are created or modified by trusted installation packages to be automatically added to the Approved List, select application installers in the **Installer** column.

Import Trusted Hash Values

Procedure

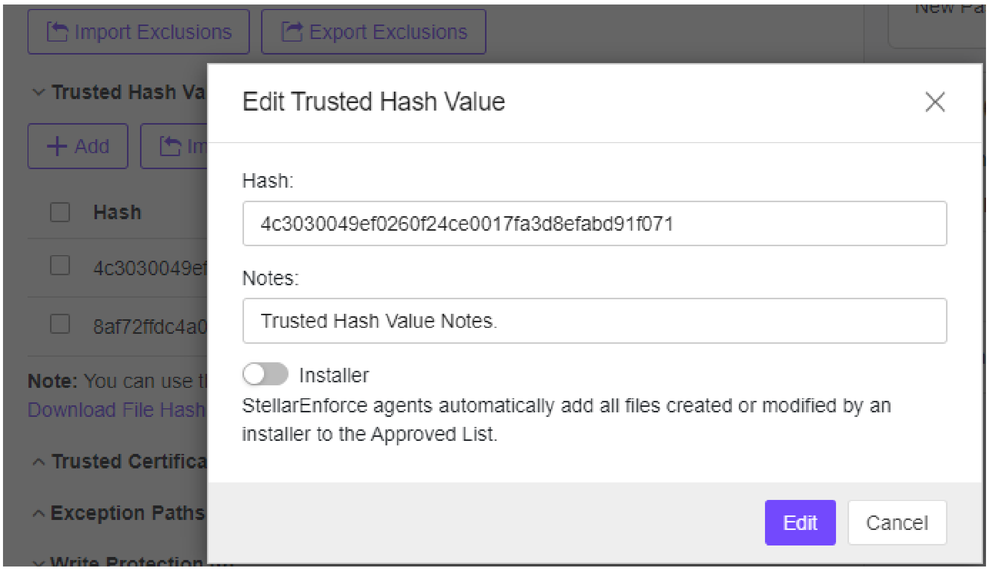
1. Find the **Trusted Hash Values** section from the **Lockdown Exclusions** pane in the **Policy view**.
2. Click the **Import** button to add a batch of hash values.
3. Enable the **Installer** toggle switch to automatically add all files created or modified by the trusted installer to the Approved List.

Note: StellarOne supports the batch import/export of .txt files containing lists of trusted hash values where the installer flag has been marked. However, the import/export process automatically converts any tab character in the Notes field (as displayed on the trusted hash deployment window) to a space character.

Edit Trusted Hash Values

Procedure

1. Find the **Trusted Hash Value section** from the **Lockdown Exclusions** pane in the **Policy view**.
2. Select the hash value you want to edit.
3. Click the **Edit** button and the **Edit Trusted Hash Value** dialog window will appear.
4. After modification, click the **Save** button to save the settings.



Note: You can use t
Download File Hash

Hash: 4c3030049ef0260f24ce0017fa3d8efabd91f071

Notes: Trusted Hash Value Notes.

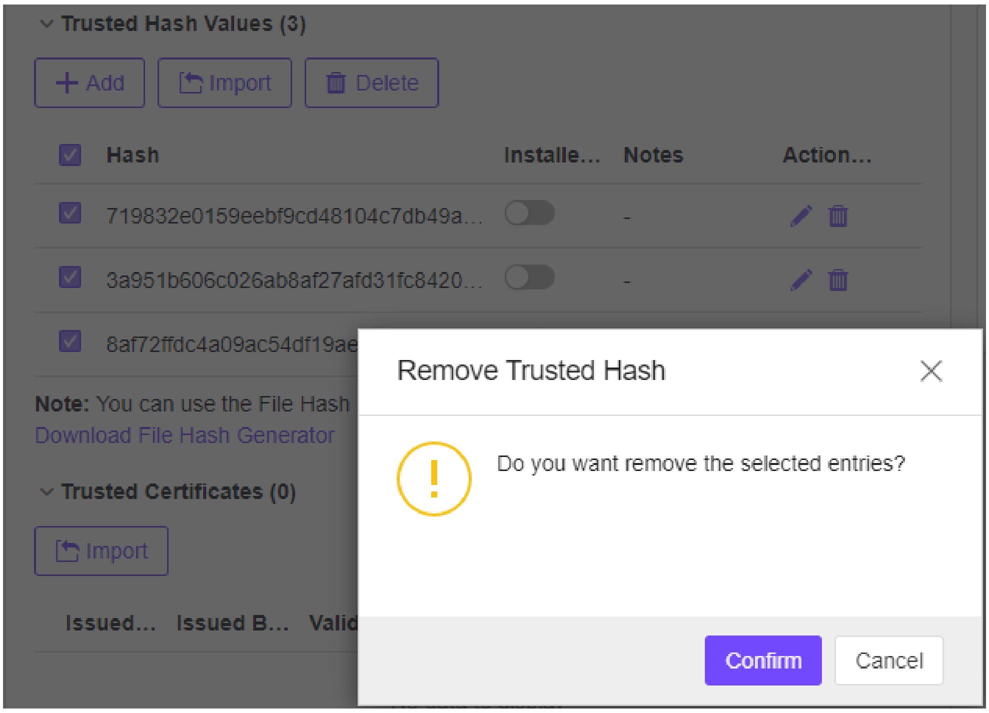
○ Installer

StellarEnforce agents automatically add all files created or modified by an installer to the Approved List.

Remove Trusted Hash Values

Procedure

1. Find the **Trusted Hash Value** section from **Lockdown Exclusions** pane in the **Policy view**.
2. Select the hash values you want to remove.
3. Click the **Delete** button and the dialog window will appear.
4. Click the **Confirm** button that you want to remove the selected entries.



☑	Hash	Installe...	Notes	Action...
☑	719832e0159eebf9cd48104c7db49a...	○	-	✎ 🗑
☑	3a951b606c026ab8af27afd31fc8420...	○	-	✎ 🗑
☑	8af72ffdc4a09ac54df19ae			

Note: You can use the File Hash
Download File Hash Generator

Do you want remove the selected entries?

Trusted Certificates Settings

Similar to hash values, trusted certificates are made by the application vendors or organizations to allow StellarEnforce to know which applications are trustworthy.

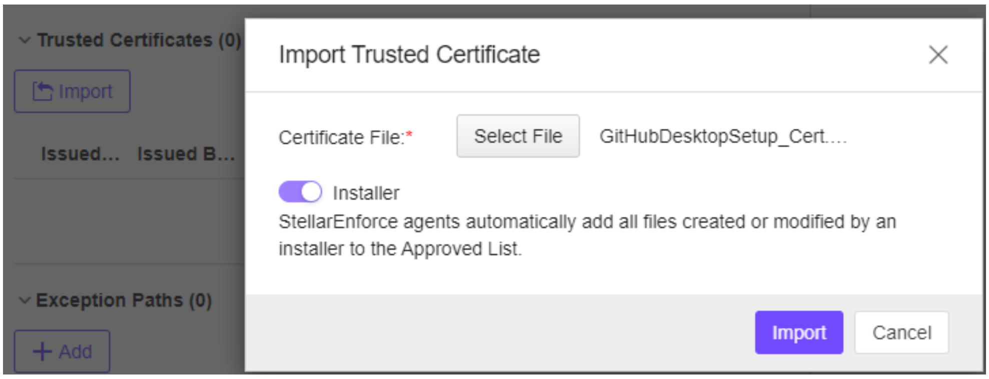
Import Trusted Certificates

Procedure

1. Navigate to the target agent or agent group on the **Agent view**.
2. Use any of the following methods to enter the **Policy view**:

   - Clcik the **Policy Inheritance** link.
   - Click 🛡, the Policy icon of Actions.

3. Find the **Trusted Certificates section** from **Lockdown Exclusions** pane in the **Policy view**.
4. Click **Select File** button, find the certificate you want to add, and click it.
5. Enable the **Installer** toggle switch to automatically add all files created or modified by the trusted installer to the **Approved List**.
6. Click the **Import** button to add the trusted certificate and the settings will be saved.



Certificate File:* GitHubDesktopSetup_Cert.…

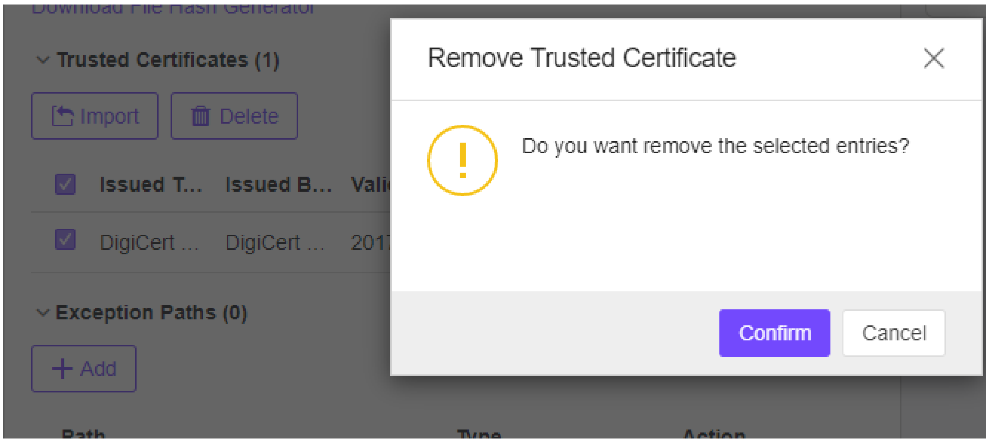
Installer

StellarEnforce agents automatically add all files created or modified by an installer to the Approved List.

Delete Trusted Certificates

Procedure

1. Find the **Trusted Certificates** section from the **Lockdown Exclusions** pane in the **Policy view**.
2. Select the trusted certificates you want to remove.
3. Click the **Delete** button and the **Remove Trusted Certificate** dialog window will appear.
4. Click the **Confirm** button that you want to remove the selected entries.



Remove Trusted Certificate

Do you want remove the selected entries?

Exception Paths Settings

Exception paths are used to point StellarEnforce to your file or file folder directly so that it can approve the file’s execution.

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

Procedure

1. Navigate to the target agent or agent group on the **Agent view**.
2. Use any of the following methods to enter the **Policy view**:

   - Click the **Policy Inheritance** link.
   - Click 🛡, the Policy icon of Actions.

3. Find the **Exception Paths** section from the **Lockdown Exclusions** pane in the **Policy view**.
4. Click the **Add** button and the **Add Exception Path** dialog window will appear.
5. Select the exception type, **File**, **Folder**, or **Regular Expression**.
6. Input the file system **path** for your exception.
7. Click the **Add** button to add a single exception path and the settings will be saved.

Edit Exception Path

Procedure

1. Select the exception path you want to edit.
2. Click the **Edit** button and the **Add Exception Path** dialog window will appear.
3. After modifying a single Exception Path, click **Edit** button and the settings will be saved.

Remove Exception Path

Procedure

1. Select the Exception Path you want to remove.
2. Click the **Delete** button and the **Remove Exception Path** dialog will appear.
3. Click the **Confirm** button that you want to remove the selected entries.

Write Protection Settings

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

Add a File, Folder, Registry Key, or Registry Value to WriteProtection

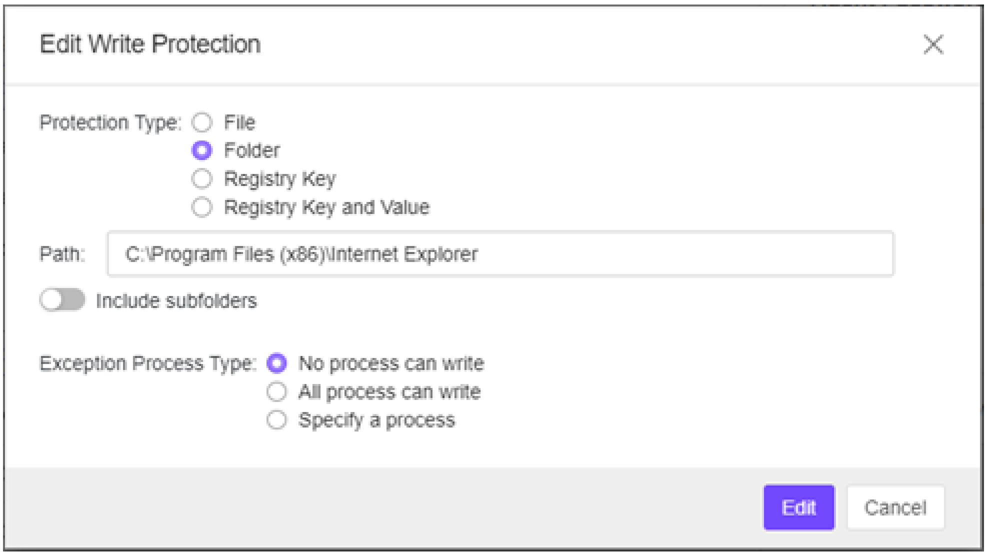
Procedure

1. Navigate to the target agent or agent group on the **Agent view**.
2. Use any of the following methods to enter the **Policy view**:
   - Click the **Policy Inheritance** link.
   - Click 🛡, the **Policy** icon of **Actions**.
3. Find the **Write Protection** section from **Lockdown Exclusions** pane in the **Policy view**.
4. Click the **Add** button and the **Add Write Protection** dialog window will appear.
5. Select the protection type, **File**, **Folder**, or **Regular Expression**.
6. Input the path to the target object to be write protected.
7. Set the **Exception Process Type**.
   - No processes can write
   - All processes can write
   - Specify a process that can write
8. Click the **Add** button and the settings will be saved.

Edit Write Protection

Procedure

1. Find the **Write Protection** section from **Lockdown Exclusions** pane in the **Policy view**.
2. Select the protection type you want to edit.
3. Click the **Edit** button and the settings will be saved.



Edit Write Protection

Protection Type: ○ File
● Folder
○ Registry Key
○ Registry Key and Value

Path: C:\Program Files (x86)\Internet Explorer

Include subfolders

Exception Process Type: ● No process can write
○ All process can write
○ Specify a process

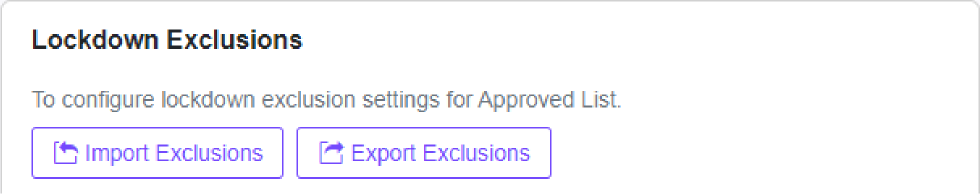
Remove Write Protection

Procedure

1. Find the **Write Protection** section from the **Lockdown Exclusions** pane in the **Policy view**.
2. Select the protection type you want to remove.
3. Click the **Delete** button and the **Remove Write Protection** dialog will appear.
4. Click the **Confirm** button that you want to remove the selected entries.

Import Exclusions

Importing exclusions allows you to move StellarEnforce's hash values, trusted certificates, exception paths, and write protection settings from one group to another.



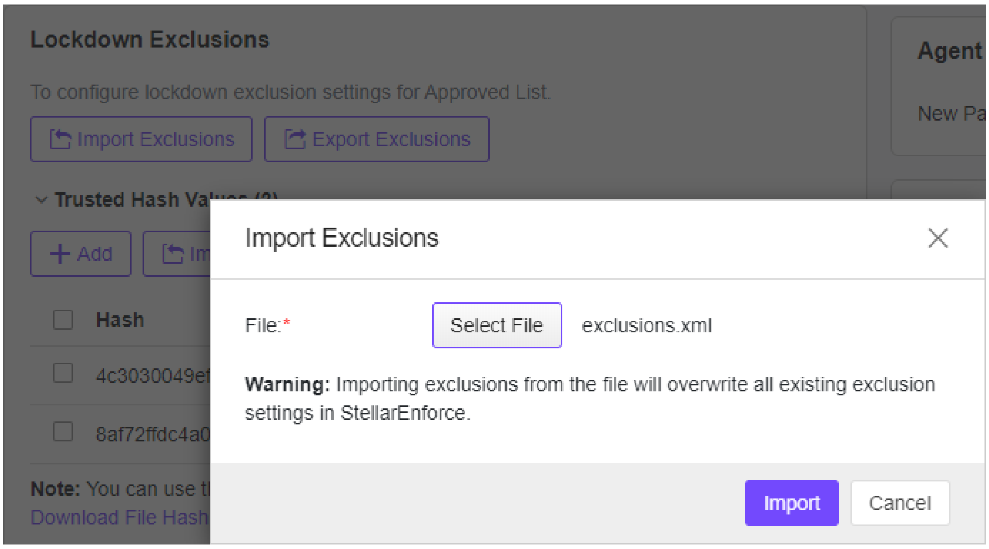
Lockdown Exclusions

To configure lockdown exclusion settings for Approved List.

Procedure

1. Navigate to the target agent or agent group on the **Agents view**.
2. Use any of the following methods to enter the **Policy view**:
   - Click the **Policy Inheritance** link.
   - Click 🛡, the **Policy** icon of **Actions**.
3. Find the **Import Exclusions** button from **Lockdown Exclusions** pane on the **Policy view**.

4. Click the **Import Exclusions** button, and the **Import Exclusions** dialog window will appear.
5. Click the **Select File** button and find the file (e.g. **exclusion.xml**) carrying your exported settings.
6. Click the **Import** button.



Lockdown Exclusions

To configure lockdown exclusion settings for Approved List.

Import Exclusions

File:* exclusions.xml

Warning: Importing exclusions from the file will overwrite all existing exclusion settings in StellarEnforce.

Export Exclusions

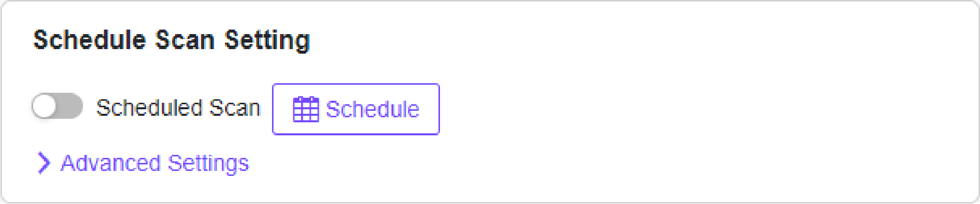
Procedure

1. Find the **Export Exclusions** section from **Lockdown Exclusions** pane in the **Policy view**.
2. Click **Export Exclusions** button and your exclusion settings will be downloaded through your browser.

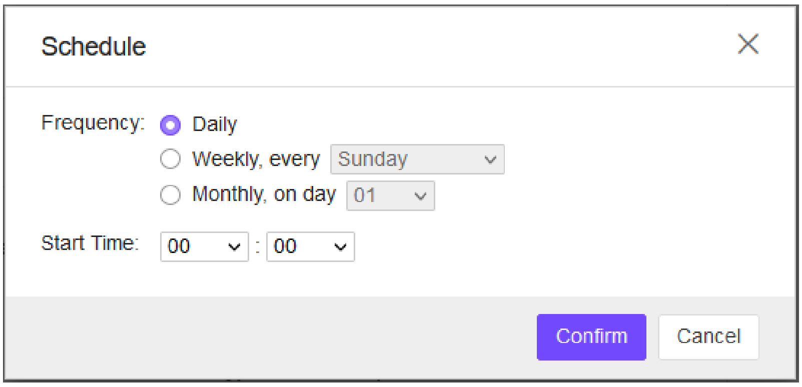
Configure Scheduled Scan Settings

From **Scheduled Scan** Settings pane, you can configure scan frequency and component update settings before a scan, i.e., which files to scan, what actions to take during a scan, and what files to exclude from a scan.

Note: Scan function is only available for StellarEnforce AV Edition and StellarMIX license.



Schedule Scan Setting


Schedule

Frequency: ● Daily
○ Weekly, every Sunday
○ Monthly, on day 01

Start Time: 00 : 00

Scheduled Scan

Procedure

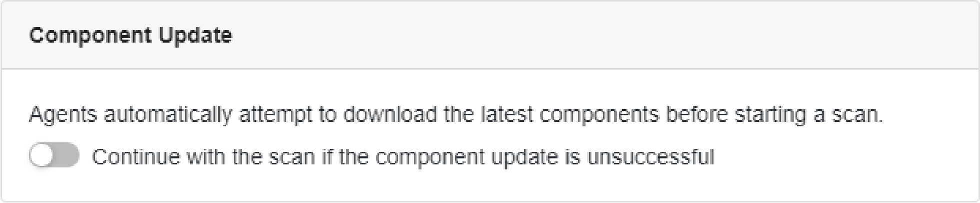
1. Navigate to the target agent or agent group on the **Agent view**.
2. Use any of the following methods to enter the **Policy view**:
    - Click the **Policy Inheritance** link.
    - Click 🛡, the **Policy** icon of **Actions**.
3. Find the **Schedule** button from **Scheduled Scan Settings** pane in the **Policy view**.
4. Set the **Frequency** (Daily, Weekly, or Monthly) and **Start time**.
5. Click the **Confirm** button.

Component Update

Procedure

1. Find **Advanced Settings** from the **Scheduled Scan Settings** pane in the **Policy view**.
2. Find the **Component Update** section.
3. Check the checkbox to continue with the scan even if the component update is unsuccessful.

Note: If the checkbox is left unchecked, the scan will not be conducted so StellarEnforce cannot update its components.


Component Update

Agents automatically attempt to download the latest components before starting a scan.

○ Continue with the scan if the component update is unsuccessful

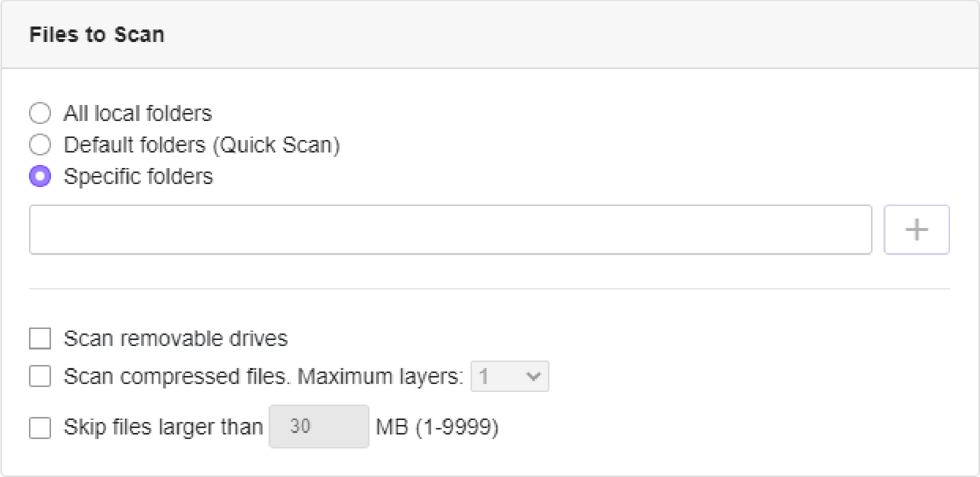
Files to Scan

Procedure

1. Find **Advanced Settings** from the **Scheduled Scan Settings** pane in the **Policy view**.
2. Find the **Files to Scan** section.
3. Select **All local folders**, **Default folders (Quick Scan)**, or select **Specific folders** and enter paths to the folders you want to scan.
4. To scan all **removable drives**: check the checkbox next to **Scan Removable Drives**.
5. To scan all **compressed files**: check the checkbox next to **Scan Compressed Files**.

Note: Under this checkbox, you can select how many layers deep to scan compressed files.

6. To skip files over a certain size, you can check **Skip files larger than** and enter a file size between **1** and **9999** MB.



Files to Scan

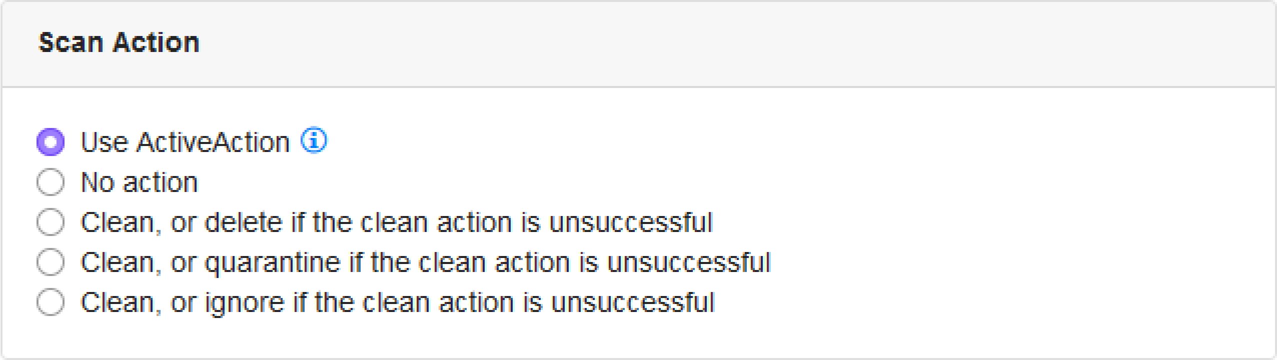
○ All local folders
○ Default folders (Quick Scan)
● Specific folders

□ Scan removable drives
□ Scan compressed files. Maximum layers: 1
□ Skip files larger than 30 MB (1-9999)

Scan Actions

Procedure

1. Find **Advanced Settings** from the **Scheduled Scan Settings** pane in the **Policy view**.
2. Find the **Scan Action** section.



Scan Action

● Use ActiveAction ⓘ
○ No action
○ Clean, or delete if the clean action is unsuccessful
○ Clean, or quarantine if the clean action is unsuccessful
○ Clean, or ignore if the clean action is unsuccessful

- Select **Active Action** to use pre-configured scan actions, which are best to use if you arenot familiar with scan actions or if you are not sure which scan action is suitable.
- Select **No Action** if you want a scan that just produces a readout of results, with no actionstaken on the discovered files.
- Select **Clean** or **Delete if the Clean Action is Unsuccessful** to default to **Delete** the target file if it cannot be recovered.
- Select **Clean** or **Quarantine if the Clean Action is Unsuccessful** to default to **Quarantine** the target file if it cannot be recovered.
- Select **Clean**, or **Ignore if the Clean Action is Unsuccessful** to default to **Ignore** thetarget file if it cannot be recovered.

Scan Exclusions

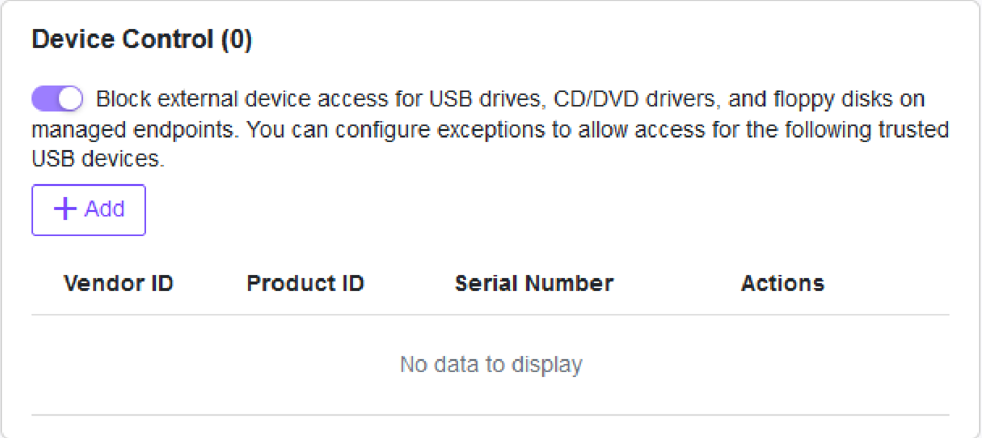
Procedure

1. Find **Scan Exclusions** from **Scheduled Scan Settings** pane in the **Policy view**.
2. Specify files, folders, or extensions that will not be scanned.

- **Folders**: specify a path of the folder you do not want it be scanned.
- **Files**: specify a path of the file you do not want it be scanned.
- **File Extensions**: specify a type of file by their file extension that you do not want it be scanned.

Configure Device Control

Allow or block external device access on managed endpoints, including USB drives, CD/DVD drives, and floppy disks. You can also configure exceptions to allow access trusted USB devices.



Device Control (0)

Block external device access for USB drives, CD/DVD drivers, and floppy disks on managed endpoints. You can configure exceptions to allow access for the following trusted USB devices.

Vendor ID	Product ID	Serial Number	Actions

No data to display

Get Device Information

Use one of the following methods to get the information of a connected device to the endpoint:

- Open the **Device Manager** on the endpoint.
- Use the **SLCmd.exe** to show USB info command on the endpoint as the command listed in the next section.
- Go to the **Agent Events** screen for agent events on StellarOne console and View Event details for removable devices with **Agent Event ID 5001**.

Trusted USB Device Commands

Configure the trusted USB device list using the Command Line Interface by typing your commands in the following format on StellarEnforce agent:

```
SLCmd.exe -p <admin_password> <command> <parameter> <value>
```

The following table lists the available abbreviated forms of parameters:

Parameter	Abbreviation	Use
trustedusbdevice	tud	Manage the trusted USB device list

The following table lists the commands, parameters, and values available:

Command	Parameter	Description
show usbinfo	<drive_letter>	Display the identifiers (VID/PID/SN) of a USB storage device For example, if the USB is in D drive, type: SLCmd.exe -p <admin_password> show usbinfo d
show trustedusbdevice		Display all trusted USB storage devices For example, type: SLCmd.exe -p <admin_password> show trustedusbdevice
add trustedusbdevice	[-vid <VID>] [-pid <PID>] [-sn <SN>]	Add a trusted USB storage device with the specified identifiers. You must specify at least one device identifier. For example, type: SLCmd.exe -p <admin_password> add trustedusbdevice -sn 123456
remove trustedusbdevice	[-vid <VID>] [-pid <PID>] [-sn <SN>]	Remove a trusted USB storage device with the specified identifiers. You must specify at least one device identifier. For example, type: SLCmd.exe -p <admin_password> remove trustedusbdevice -sn 123456

Add Trusted USB Devices

You can specify USB storage devices that are allowed to access managed endpoints based on the device information.

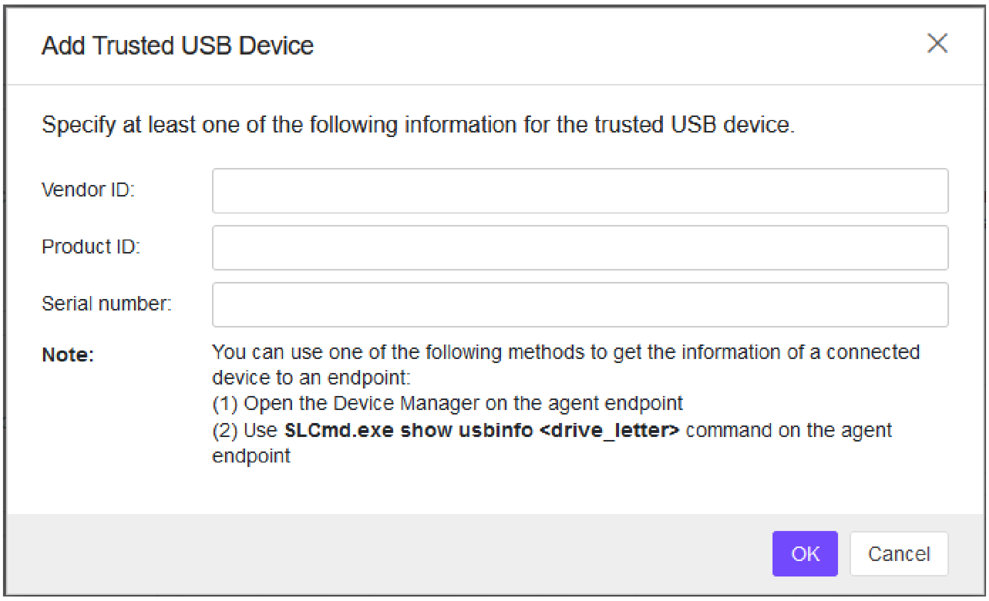
Procedure

1. Navigate to the target agent or agent group on the **Agent list**.
2. Use any of the following methods to enter the **Policy view**:

    - Click the **Policy Inheritance** link.
    - Click ⛉, the **Policy** icon of **Actions**.

3. Find the **Device Control** pane in the **Policy view**.
4. Click the **Toggle Switch** to enable "Allows only trusted USB devices by vendor ID, serial number, and product ID**"**. The **Trusted USB Device** List will appear.
5. Click the **Add** button and the **Add Trusted USB Device** dialog window will appear.
6. Specify at least one of the following information for the trusted USB device, and click the **OK** button:

    - **Vendor ID**
    - **Product ID**
    - **Serial number**



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 **SLCmd.exe show usbinfo <drive_letter>** command on the agent endpoint

Note:
To view the list of trusted USB devices on an endpoint, export the agent settings. To manually configure the trusted USB device list on an endpoint, do one of the following: Export agent settings, make changes, or import an updated settings file Using the SLCmd command.

Edit Trusted USB Devices

Procedure

1. Find the **Device Control** pane in the **Policy view**.
2. Click the **Toggle Switch** to enable "Allows only trusted USB devices by vendor ID, serial number, and product ID". The **Trusted USB Device List** will appear.
3. Select the Trusted USB Device you want to edit.
4. Click the **Edit** button and the dialog window will appear.

5. Click the **Confirm** button and the settings will be saved.

Remove Trusted USB Devices by Setting Policy

Procedure

1. Find the **Device Control** pane in the **Policy view**.
2. Click the **Toggle Switch** to enable “Allows only trusted USB devices by vendor ID, serial number, and product ID”. The **Trusted USB Device List** will appear.
3. Select the Trusted USB Device you want to delete.
4. Click the **Delete** button and the **Remove Trusted USB Device** dialog window will appear.
5. Click the **Confirm** button and the settings will be saved.

Remove Trusted USB Devices by Importing Config

Procedure

1. go to **Agents** in the navigation at the top of the web console. The Agents screen will appear.
2. Select one or more endpoints.
3. Click **Import / Export** > **Export Agent Configuration**.
4. Click the **Download** link in the **Status** field to download the agent configuration file on your computer.
5. Open the agent configuration file using a text editor and locate the **<DeviceException>** section.

The following figure shows an example where the <DeviceException> section is empty when no trusted USB device is added.

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

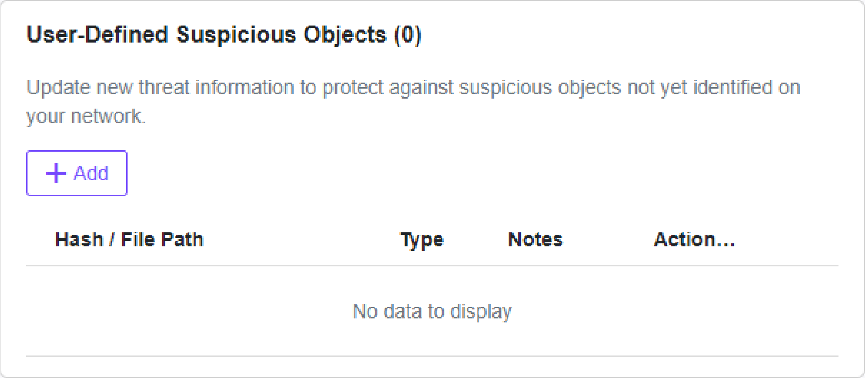
The following figure shows an example where the <DeviceException> section contains two entries for the added trusted USB devices.

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

6. Delete the entries for the trusted USB devices you want to remove and save the agent configuration file.
7. Import the updated agent configuration file.

Configure User-Defined Suspicious Objects

By setting User-Defined Suspicious Objects, you can protect your system against malware discovered by TXOne's researchers.



User-Defined Suspicious Objects (0)

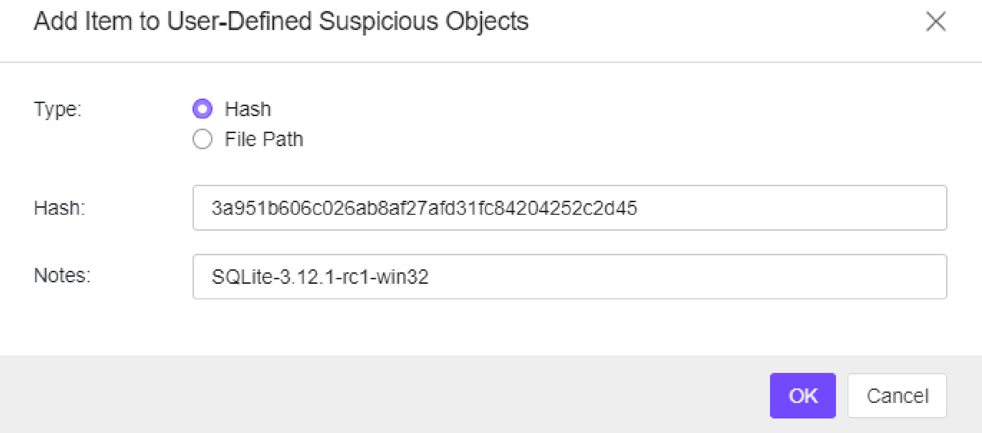
Update new threat information to protect against suspicious objects not yet identified on your network.

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

Add User-Defined Suspicious Objects

Procedure

1. Navigate to the target agent or agent group on the **Agent list**.
2. Use any of the following methods to enter the **Policy view**:
   - Click the **Policy Inheritance** link.
   - Click 🛡, the **Policy** icon of **Actions**.
3. Find the **User-Defined Suspicious Objects** pane in the **Policy view**.
4. Click **Add** button and the **Add Item to User-Defined Suspicious Objects** dialog will appear.
5. After modification, click the **OK** button and the settings will be saved.



Add Item to User-Defined Suspicious Objects

Type: ● Hash ○ File Path

Hash: 3a951b606c026ab8af27afd31fc84204252c2d45

Notes: SQLite-3.12.1-rc1-win32

Remove User-Defined Suspicious Objects

Procedure

1. Find the User-Defined Suspicious Objects pane in the Policy view.
2. Select the Hash / File Path you want to remove.
3. Click the Delete button and the dialog window will appear.
4. Click the Confirm button that you want to remove the selected items.

Set Agent Password

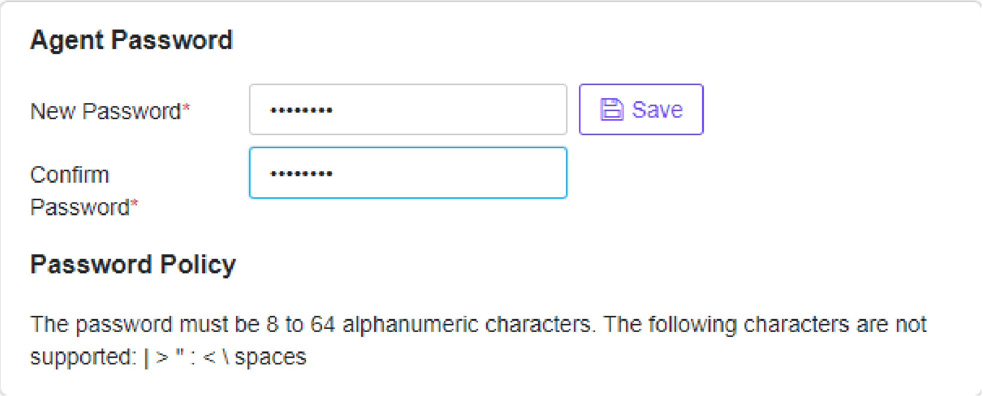
Update StellarEnforce agent password remotely using StellarOne console. It does not require the old agent password to create a new one.

Procedure

1. Navigate to the target agent or agent group on the **Agent list**.
2. Use any of the following methods to enter the **Policy view**:

   - Click the **Policy Inheritance** link.
   - Click 🛡, the **Policy** icon of **Actions**.

3. Find the **Agent Password** pane in the **Policy view**.
4. Input **New Password** and **Confirm Password**.
5. Click the **Save** button and the settings will be saved.



Agent Password

New Password* ••••••••

Confirm Password* ••••••••

Password Policy

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

Note: This function is only available for users with privileges of Admins or Operators. They can change agent admin password remotely.

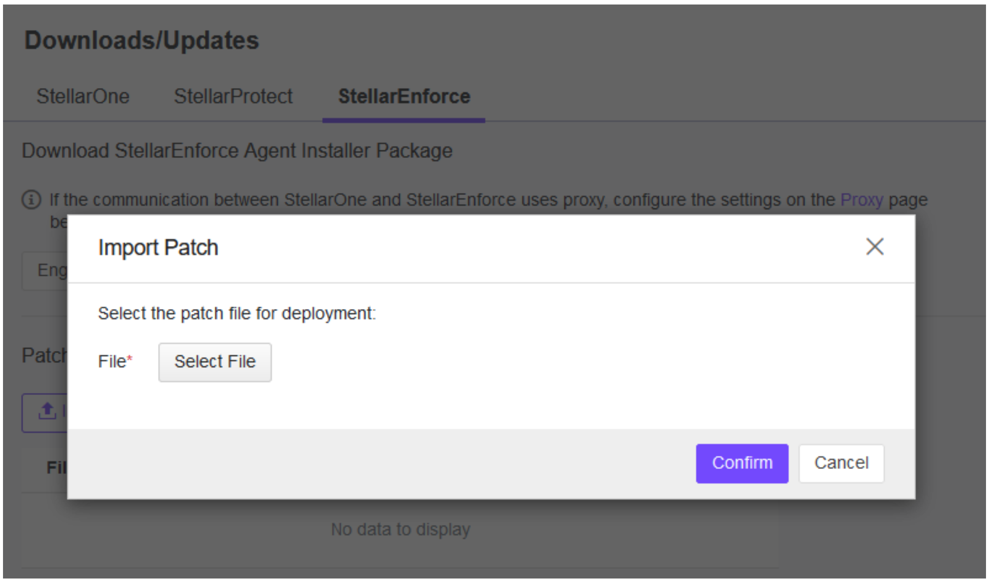
Configure Patch Settings

Procedure

1. Navigate to the target agent or agent group on the **Agent list**.
2. Use any of the following methods to enter the **Policy view**:

    - Click the **Policy Inheritance** link.
    - Click 🛡, the **Policy** icon of **Actions**.

3. Find the **Patch** pane in the **Policy view**.
4. Select the checkbox next to the patch or patches you want to apply.
5. Click the **Update** link to import a new patch.
6. Click the link to go to the **Downloads / Updates** page.
7. Click the **Confirm** button and the settings will be saved.



Downloads/Updates

Download StellarEnforce Agent Installer Package

If the communication between StellarOne and StellarEnforce uses proxy, configure the settings on the Proxy page be

Import Patch

Select the patch file for deployment:

File*

No data to display

Note: If the version of the patch is lower than the current agent, the patch should not be applied and the status will keep un-synced and other policy will also not be deployed. It needs to wait for the next 20 minutes, and other policy could be applied to the agent.

Chapter 4 – Agent Protection and Update

Configure Maintenance Mode Settings

To perform updates on endpoints, you can configure Maintenance Mode settings to define a period when StellarEnforce allows all file executions and adds all files that are created, executed, or modified to the Approved List.

For example, if Mozilla Firefox needs to be installed or updated, enable the Maintenance Mode to allow the installation or update, and also add any files created or modified in the process to the Approved List.

For added security, you can enable **file scanning** and select the **scan action** after the maintenance period.

Important:

Before using Maintenance Mode, apply the required updates on the following supported platforms:

- For Windows 2000 Service Pack 4, apply the update KB891861 from the Microsoft Update Catalog website.
- For Windows XP SP1, upgrade to Windows XP SP2.

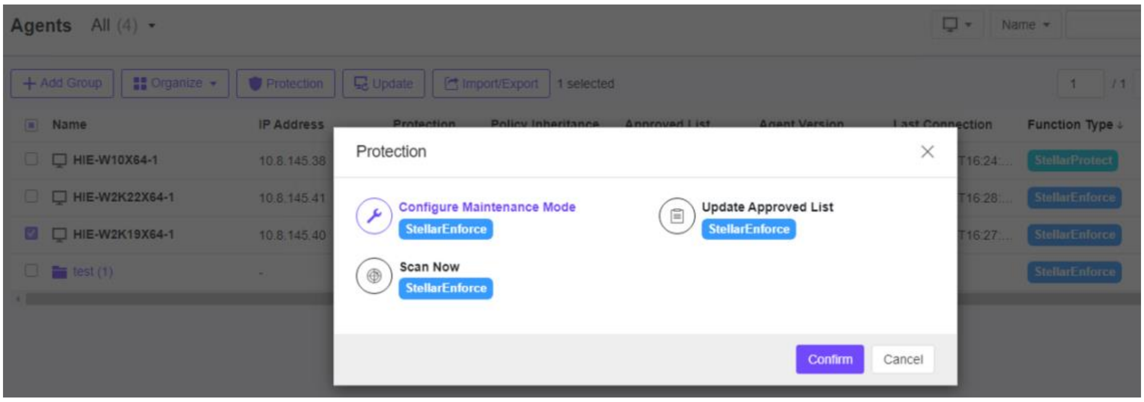
Note:

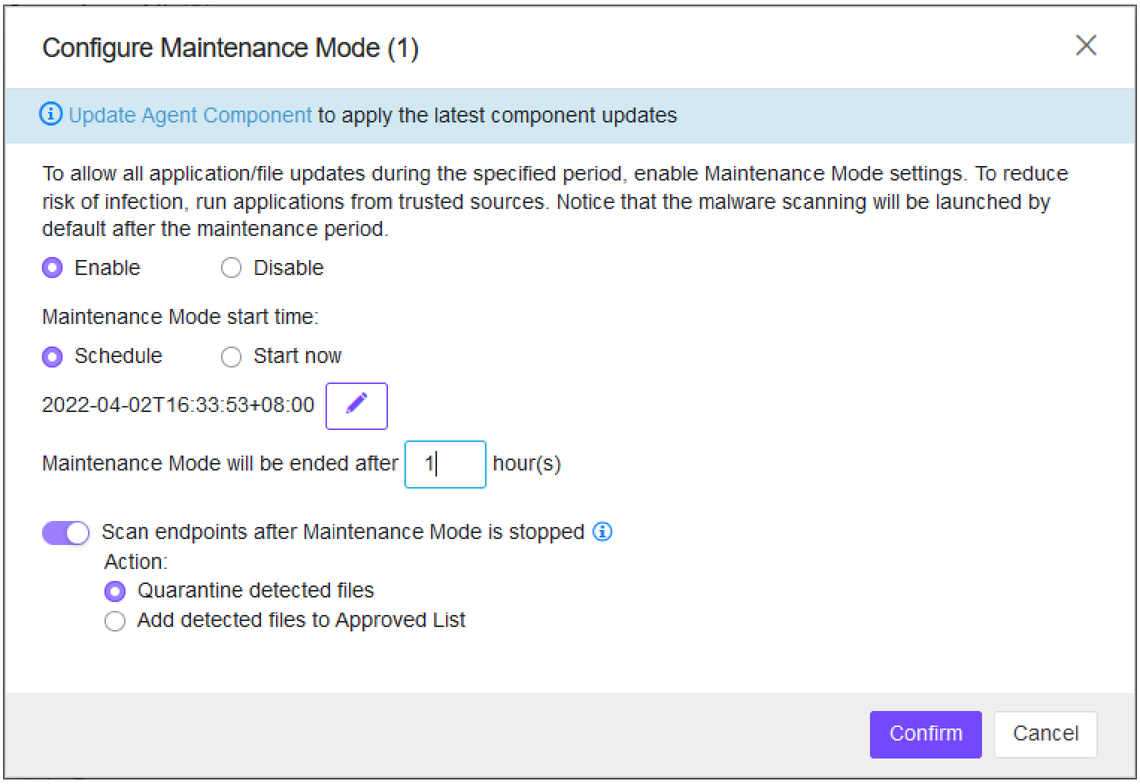
- To reduce risk of infection, run only applications from trusted sources on endpoints during the maintenance period.
- Agents can start one scheduled maintenance period at a time. If you configure a new maintenance period, the system overwrites the existing maintenance schedule that has not started yet.
- When the agent is about to leave Maintenance Mode, restarting the endpoint prevents StellarEnforce from adding files in the queue to the Approved List.
- During the maintenance period, you cannot perform agent patch updates on endpoints.
- When Maintenance Mode is enabled, StellarEnforce does not support Windows updates that require restarting an endpoint during the maintenance period.
- To run an installer that deploys files to a network folder during the maintenance period, StellarEnforce must have access permission to the network folder.

Procedure

1. Navigate to the target agent or agent group on the **Agent view**.
2. Select one or more endpoints (or groups) by clicking the checkboxes next to them.

3. Click the Protection button from the Tool Bar at the top of the **Agents** screen.
4. Click the **Configure Maintenance Mode** option and then click the **Confirm** button on the **Protection** menu window. The configuration window will appear.





Configure Maintenance Mode (1)

Update Agent Component to apply the latest component updates

To allow all application/file updates during the specified period, enable Maintenance Mode settings. To reduce risk of infection, run applications from trusted sources. Notice that the malware scanning will be launched by default after the maintenance period.

● Enable ○ Disable

Maintenance Mode start time:

● Schedule ○ Start now

2022-04-02T16:33:53+08:00

Maintenance Mode will be ended after 1 hour(s)

Scan endpoints after Maintenance Mode is stopped

Action:

● Quarantine detected files

○ Add detected files to Approved List

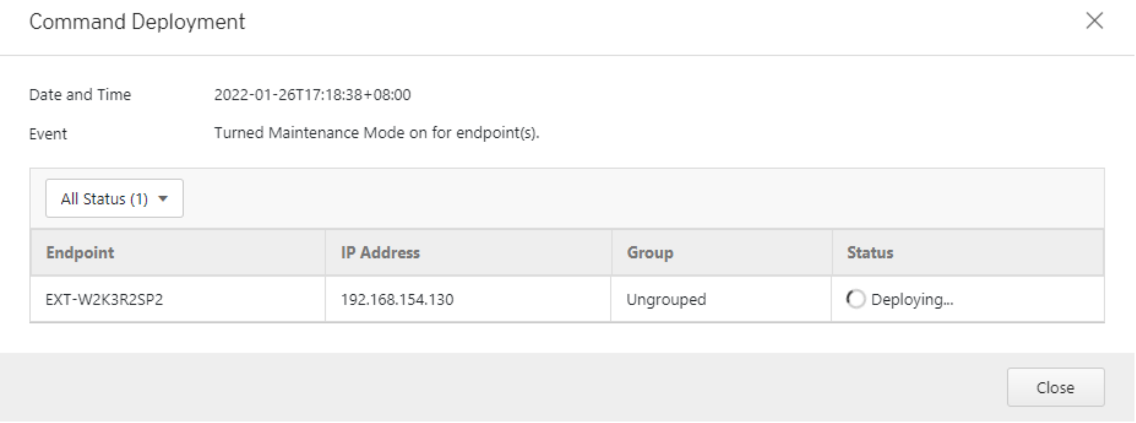
5. Choose either **Enable** or **Disable**.
   - Click **Enable** to start the Maintenance Mode settings.
   - Click **Disable** to stop Maintenance Mode or cancel the scheduled maintenance period on endpoints.
6. Choose either **Schedule** or **Start Now**.
   - If you choose **Schedule**, you must specify the duration of the maintenance period.

- If you select **Scan endpoints after Maintenance Mode is stopped**, StellarEnforce will scan endpoints for threats when the maintenance period is over.

7. Select the action you want:
    - **Quarantine detected files**
    - **Add detected files to Approved List**

Note: StellarEnforce scans files that are created, executed, or modified on endpoints during the maintenance period.

8. Click the **OK** button to deploy the settings to the selected agents or groups.
9. The system will show the **Command Deployment** window with the deployment status, user can click the **Close** button to close the window.



Command Deployment

Date and Time 2022-01-26T17:18:38+08:00

Event Turned Maintenance Mode on for endpoint(s).

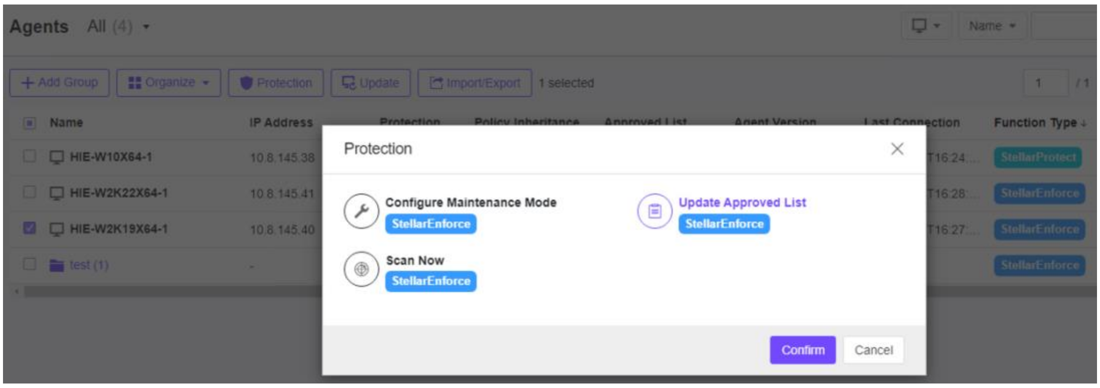
Endpoint	IP Address	Group	Status
EXT-W2K3R2SP2	192.168.154.130	Ungrouped	Deploying...

Update the Approved List

You may want to periodically update the Approved List on StellarEnforce Agents after installing new applications that you want to run during a Lockdown situation. Updating the Approved List performs an inventory scan on selected agents and adds any new applications found on the agent to the global Approved List.

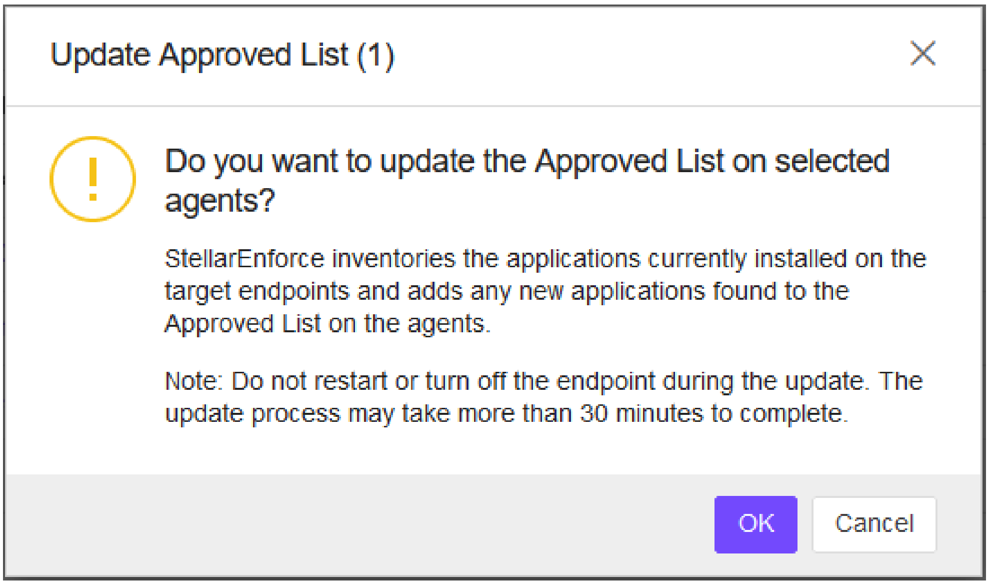
Before StellarEnforce can protect the endpoint, it must check the endpoint for existing applications and files necessary for the system to run correctly. When StellarEnforce Application Lockdown is on, only applications that are in the Approved List will be able to run.

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



Procedure

1. Navigate to the target agent or agent group on the **Agent list**.
2. Select one or more endpoints (or groups) by clicking the checkboxes next to them.
3. Click the Protection button from the Tool Bar at the top of the **Agents** screen.
4. Click the **Update Approved List** option and then click the **Confirm** button on the **Protection** menu window. The confirmation window will appear.
5. Click the **OK** button to update the Approved List.


Update Approved List (1)

Do you want to update the Approved List on selected agents?

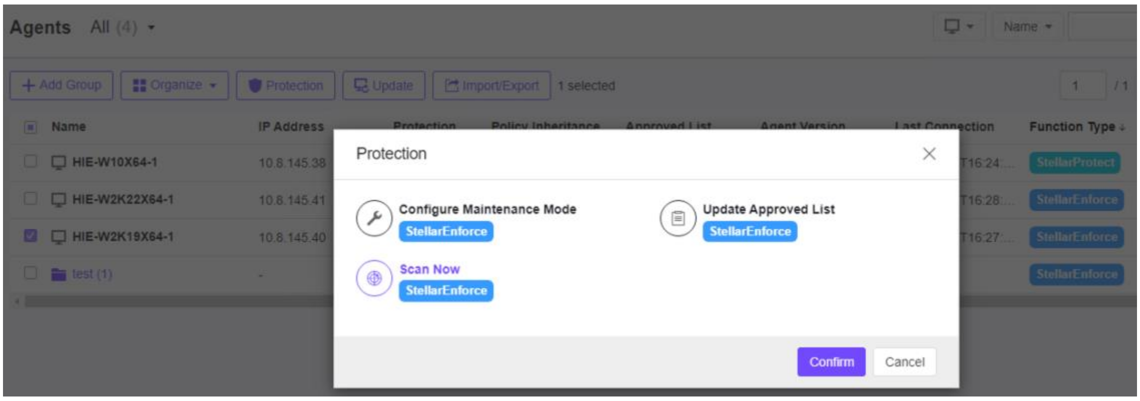
StellarEnforce inventories the applications currently installed on the target endpoints and adds any new applications found to the Approved List on the agents.

Note: Do not restart or turn off the endpoint during the update. The update process may take more than 30 minutes to complete.

Note: Do not restart or turn off the endpoint during the update. The update process may take more than 30 minutes to complete.

Scan Now

You can initiate a manual Scan Now on the selected endpoints and configure the scan settings to deploy one or several StellarEnforce target endpoints.



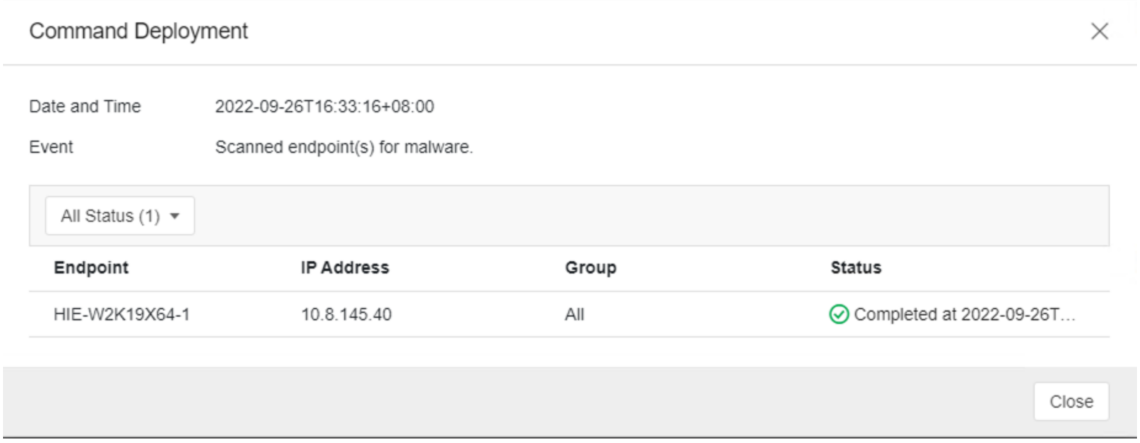
Initiate Scan Now

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

Procedure

1. Navigate to the target agent or agent group on the **Agents list**.
2. Select one or more endpoints (or groups) by clicking the checkboxes next to them.
3. Click the Protection button from the Tool Bar at the top of the **Agents** screen.
4. Click the **Scan Now** option and then click the **Confirm** button on the **Protection** menu window. The confirmation window will appear.
5. After configuring the scan settings, click the **OK** button to initiate Scan Now.

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


Command Deployment

Date and Time 2022-09-26T16:33:16+08:00

Event Scanned endpoint(s) for malware.

All Status (1)

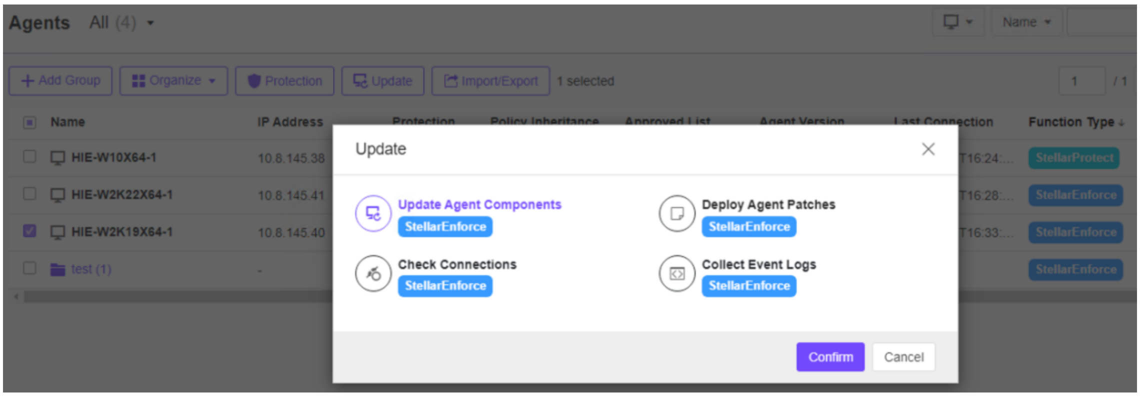
Endpoint	IP Address	Group	Status
HIE-W2K19X64-1	10.8.145.40	All	✓ Completed at 2022-09-26T...

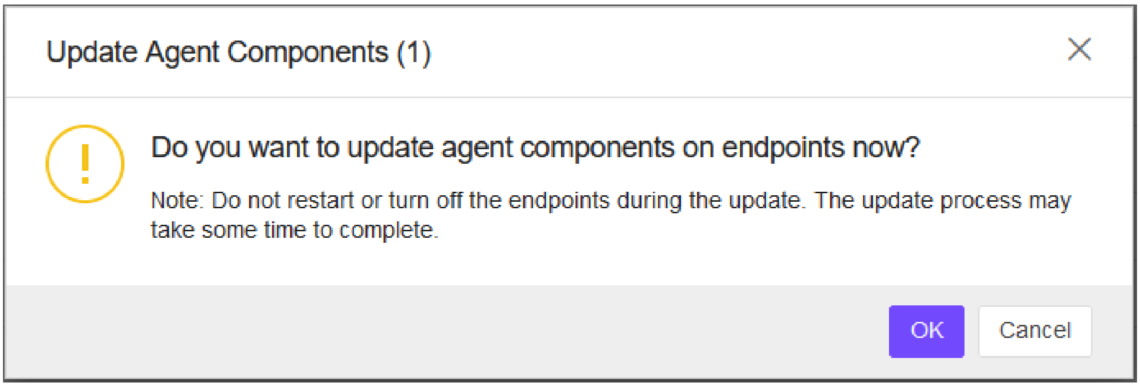
Update Agent Components

You can start the agent component update process on the selected endpoints from StellarOne. The agent will download the latest component updates. Updating agent components regularly can protect endpoints from the latest security risks.

Procedure

1. Navigate to the target agent or agent group within the **Agents** table.
2. Select one or more endpoints (or groups) by clicking the checkboxes next to them.
3. Click the Update button from the Tool Bar at the top of the **Agents** screen.
4. Click the **Update Agent Components option** and then click the **Confirm** button on the **Update** menu window. The confirmation window will appear.
5. Click the **OK** button to update agent components.


Agents All (4)
Name
+ Add Group
Organize
Protection
Update
Import/Export
1 selected
1 / 1
Name
IP Address
Protection
Policy Inheritance
Approved List
Agent Version
Last Connection
Function Type
HIE-W10X64-1 10.8.145.38 T16:24:... StellarProtect
HIE-W2K22X64-1 10.8.145.41 T16:28:... StellarEnforce
HIE-W2K19X64-1 10.8.145.40 T16:33:... StellarEnforce
test (1) - StellarEnforce
Update
Update Agent Components StellarEnforce
Deploy Agent Patches StellarEnforce
Check Connections StellarEnforce
Collect Event Logs StellarEnforce
Confirm
Cancel


Update Agent Components (1)

Do you want to update agent components on endpoints now?

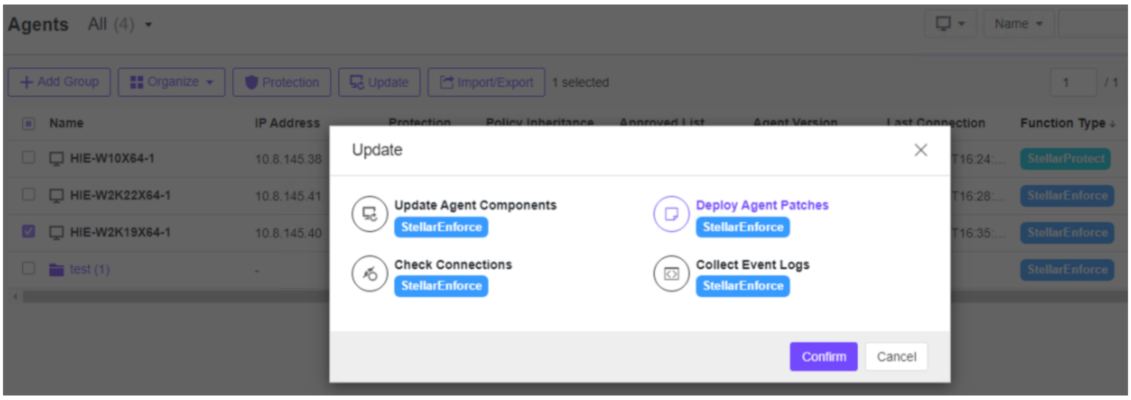
Note: Do not restart or turn off the endpoints during the update. The update process may take some time to complete.

Deploy Agent Patches

You can upgrade agents remotely from the web console by using StellarOne to deploy an uploaded patch file to the selected StellarEnforce agents.

Procedure

1. Navigate to the target agent or agent group on the **Agent list**.
2. Select one or more endpoints (or groups) by clicking the checkboxes next to them.
3. Click the Update button from the Tool Bar at the top of the **Agents** screen.
4. Click the **Deploy Agent Patches** option and then click the **Confirm** button on the **Update** menu window. The confirmation window will appear.
5. After configuring the settings, click the **OK** button.



Wait for the upload process to complete. After StellarOne verifies the validity of the file, it will deploy the patch file to the selected agents.

Note:

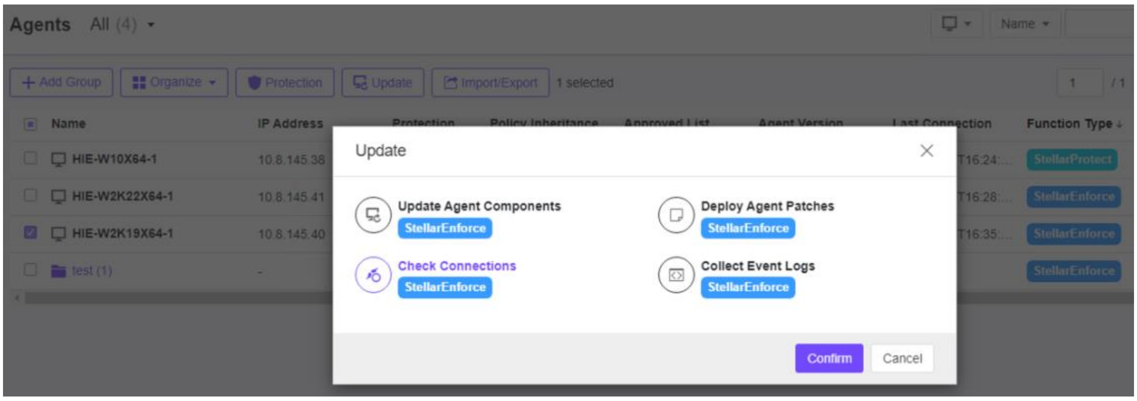
The remote deployment of agent patches to the StellarEnforce 1.0 agent is not supported for Windows 7 SP1 and older versions.

Check Connections

Check the connection status of the selected StellarEnforce agents.

Procedure

1. Navigate to the target agent or agent group on the **Agent list**.
2. Select one or more endpoints (or groups) by clicking the checkboxes next to them.
3. Click the Update button from the Tool Bar at the top of the **Agents** screen.
4. Click the **Check Connections** option and then click the **Confirm** button. The window will appear.
5. Check the connection status by selecting criteria of **Status** or **Products**.

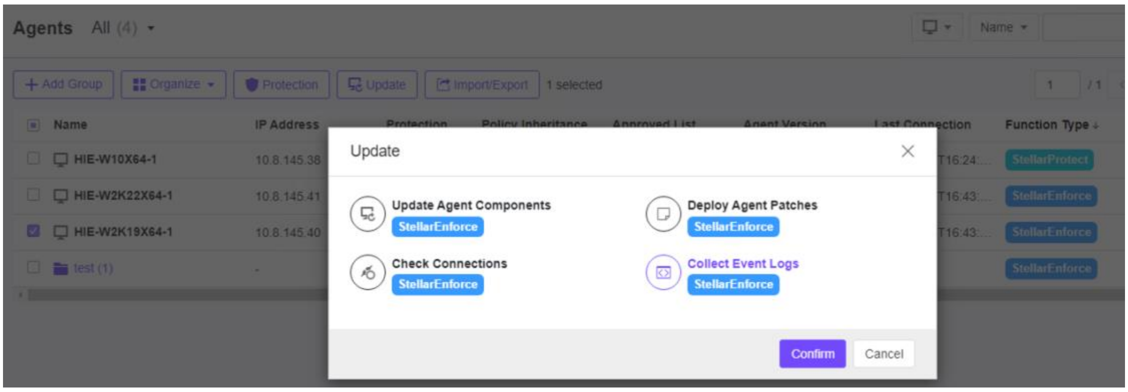


Note:

- After determining which agents cannot be connected to the StellarOne server, TXOne Networks recommends checking the network connectivity of the disconnected agents.
- By default, agents will auto-sync StellarOne console every **20** minutes.

Collect Event Logs

Logs contain information about agent activity. Collecting event logs updates the StellarOne database with the latest information from the selected agents.



☐	Name	IP Address	Protection	Policy Inheritance	Approved List	Agent Version	Last Connection	Function Type ↓
☐	HIE-W10X64-1	10.8.145.38					T16:24:...	StellarProtect
☐	HIE-W2K22X64-1	10.8.145.41					T16:43:...	StellarEnforce
☑	HIE-W2K19X64-1	10.8.145.40					T16:43:...	StellarEnforce
☐	test (1)	-						StellarEnforce

Procedure

1. Navigate to the target agent on the Agent list.
2. Select one or more endpoints by clicking the checkboxes next to them.
3. Click the Update button from the Tool Bar at the top of the Agents screen.
4. Click the **Collect Event Logs** option and then click the **Confirm** button.

StellarOne updates the date and time displayed in the **Last Connection** column after each StellarEnforce agent successfully sends logs and status to StellarOne.

Note:
The user needs to enable Information level (Setup.ini) of Logs below and then contain information about the agent activity.

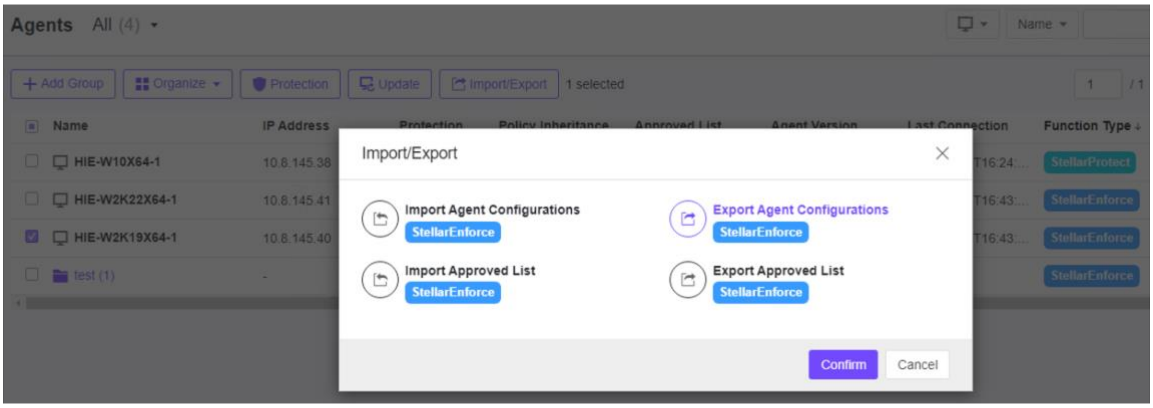
```
[EventLog]
Enable = 1
Level_WarningLog = 1
Level_InformationLog = 1
```

Chapter 5 – Agent Import/Export Settings

The following functions should be only for agent level. When the user selects any group from the list, the function should be disabled.

Export Agent Settings

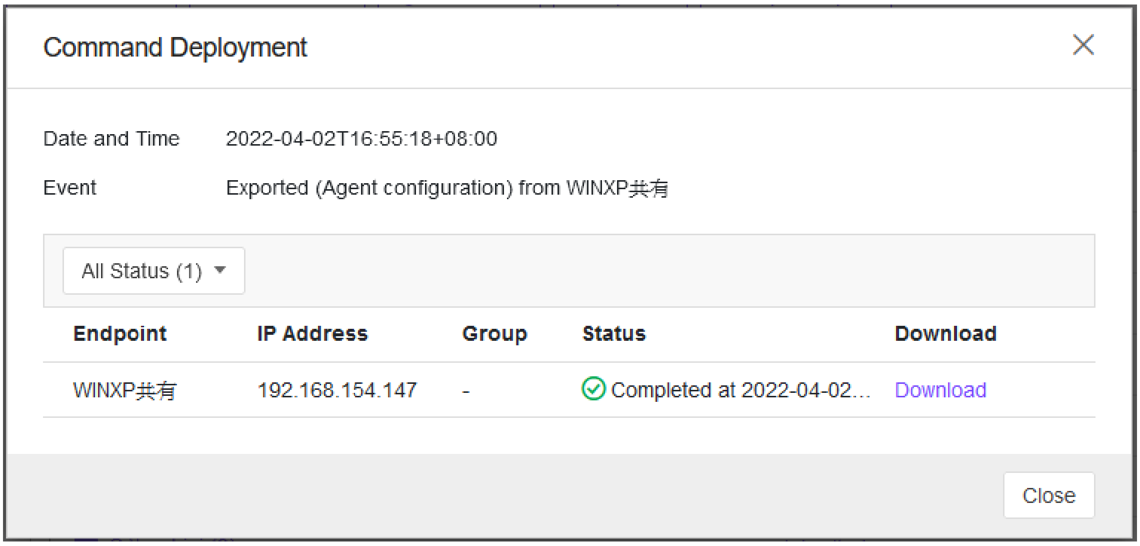
You can remotely obtain Agent Configuration settings and Approved List by exporting and downloading them from the StellarOne console.



Export Agent Configuration

Procedure

1. Navigate to the target agent or agent group on the **Agent list**.
2. Select the target agent by clicking the checkbox next to it.
3. Click the Import / Export button from the Tool Bar at the top of the **Agents** screen.
4. Click the **Export Agent Configuration** option and then click the **Confirm** button on the **Import/Export** menu window. The window will appear.
5. Click the **Download** link to download your agent configuration file. The progress can be viewed from the pop-up details window.



Command Deployment

Date and Time 2022-04-02T16:55:18+08:00

Event Exported (Agent configuration) from WINXP共有

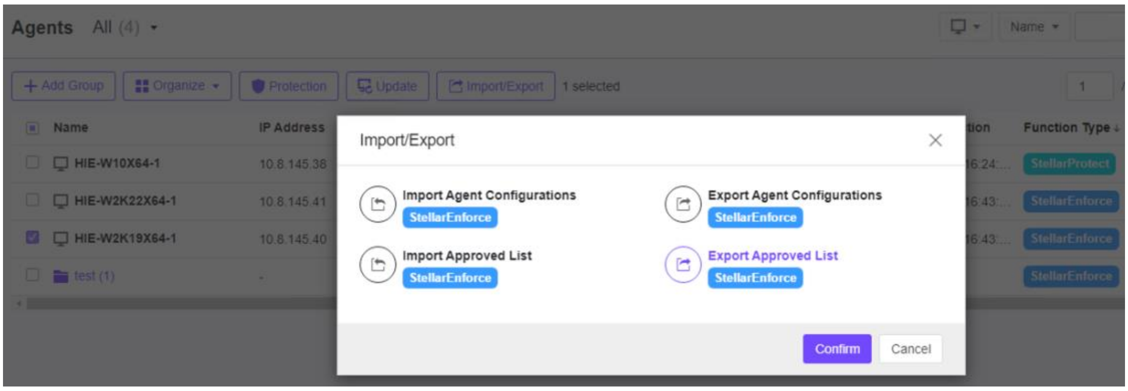
All Status (1)

Endpoint	IP Address	Group	Status	Download
WINXP共有	192.168.154.147	-	✓ Completed at 2022-04-02…	Download

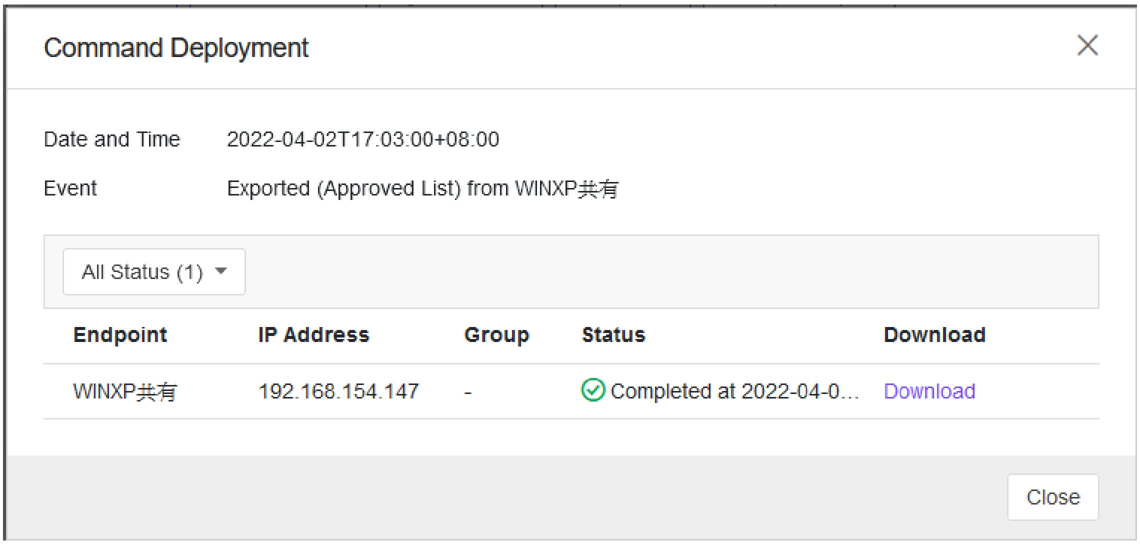
Export Approved List

Procedure

1. Navigate to the target agent or agent group on the **Agent list**.
2. Select the target endpoints by clicking the checkbox next to it.
3. Click the Import / Export button from the Tool Bar at the top of the **Agents** screen.
4. Click the **Export Approved List** option and then click the **Confirm** button on the **Import/Export** menu window. The window will appear



5. Click the **Download** link to download your Approved List file. The progress can be viewed from the pop-up details window.



Command Deployment

Date and Time 2022-04-02T17:03:00+08:00

Event Exported (Approved List) from WINXP共有

All Status (1)

Endpoint	IP Address	Group	Status	Download
WINXP共有	192.168.154.147	-	✓ Completed at 2022-04-0...	Download

Import Agent Settings

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

- Remotely overwrite agent configuration
- Remotely overwrite Approved List

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

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

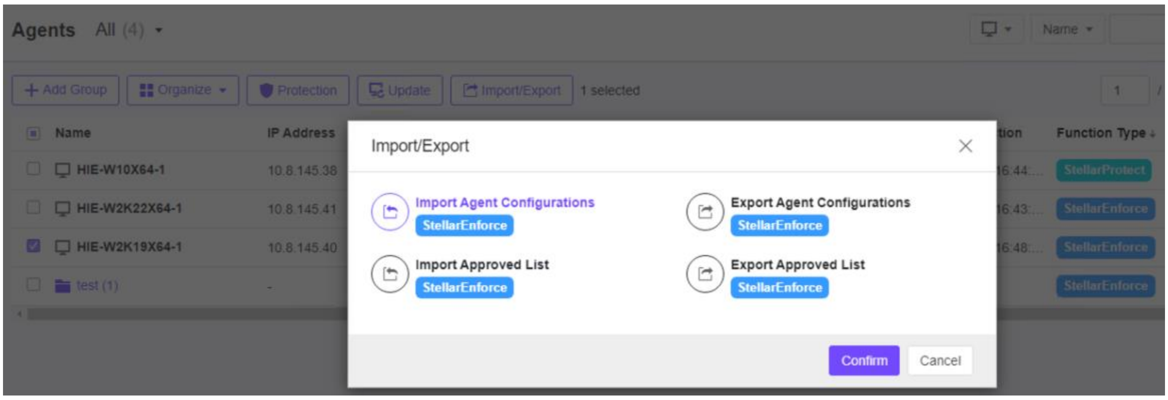
To ensure a successful import, verify that the file to import meets the following requirements:

- For Approved List, file is in the CSV format and uses UTF-8 encoding
- The maximum file size support is **20 MB**
- For Agent Configuration file, file is in the XML format and the maximum file size support is **1 MB**

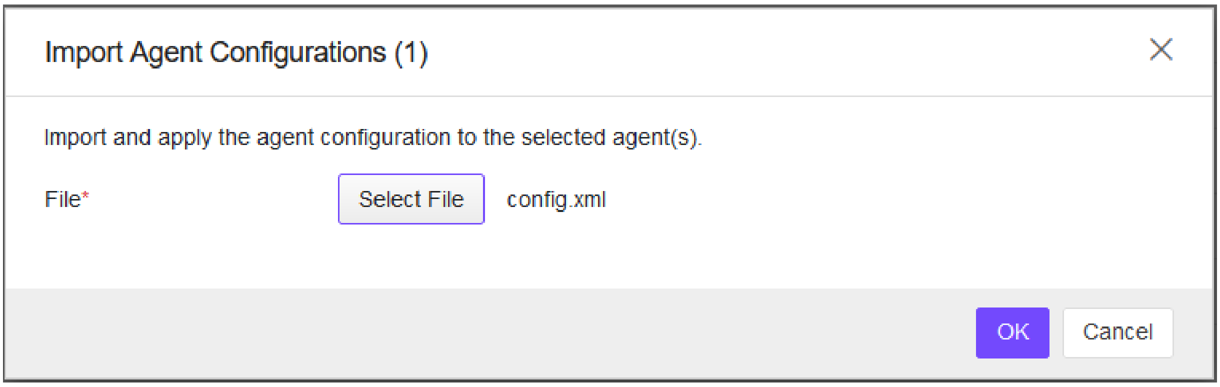
Import Agent Configuration

Procedure

1. Navigate to the target agent or agent group on the **Agent list**.
2. Select the target endpoints by clicking the checkbox next to it.
3. Click the Import / Export button from the Tool Bar at the top of the **Agents** screen.
4. Click the **Import Agent configuration** option and then click the **Confirm** button on the **Import/Export** menu window. The window will appear



5. **Select File** and click the **OK** button to start importing agent configuration.



Import Agent Configurations (1)

Import and apply the agent configuration to the selected agent(s).

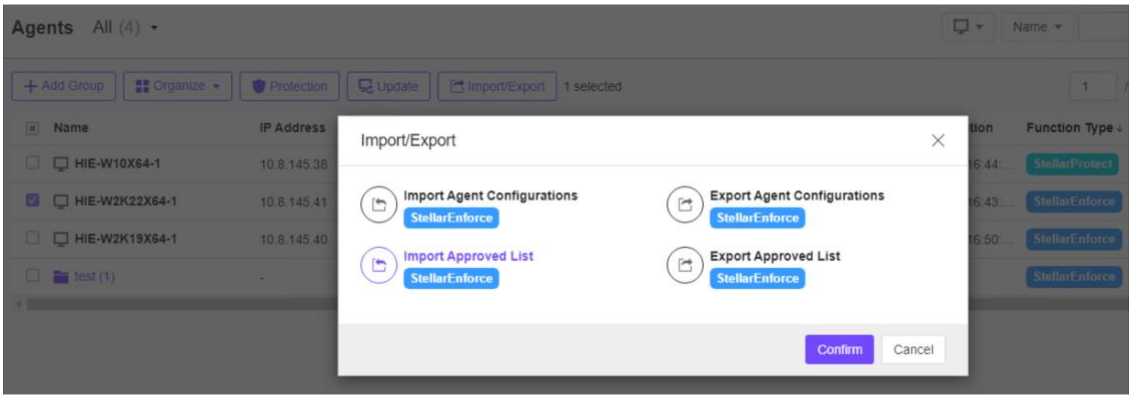
File* Select File config.xml

OK Cancel

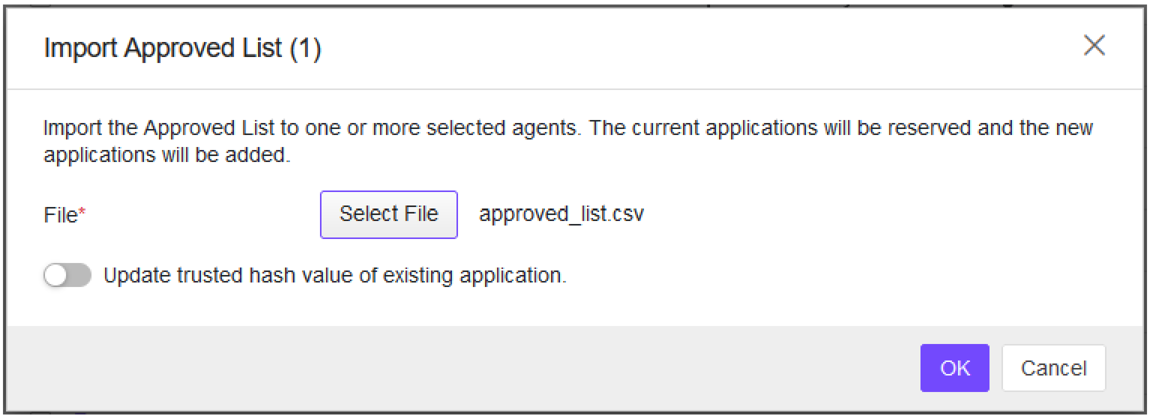
Import Approved List

Procedure

1. Navigate to the target agent or agent group on the **Agent list**.
2. Select the target endpoints by clicking the checkbox next to it.
3. Click the Import / Export button from the Tool Bar at the top of the **Agents** screen.
4. Click the **Import Agent configuration** option and then click the **Confirm** button on the **Import/Export** menu window. The window will appear



5. **Select File** and click the **OK** button to start importing Approved List.



Import Approved List (1)

Import the Approved List to one or more selected agents. The current applications will be reserved and the new applications will be added.

File* Select File approved_list.csv

○ Update trusted hash value of existing application.

Note:

The switch toggle, “Update trusted hash values of existing application” is used for overwriting the existing trusted hash values (in Approved List).

Actions for Endpoints

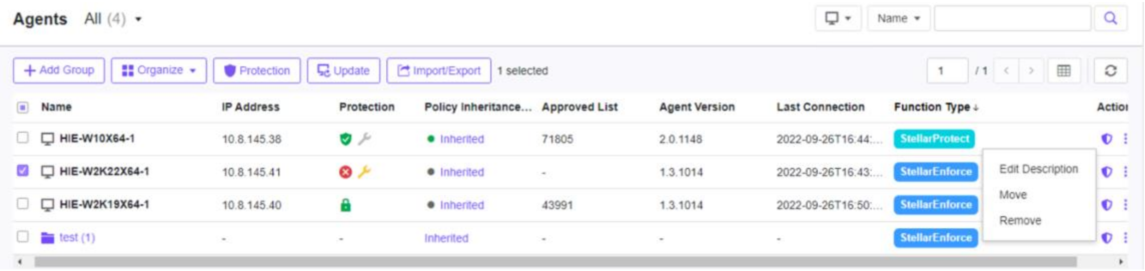
Edit Description

You can edit tags to help you identify and search for agents. To edit tags, follow the steps below.

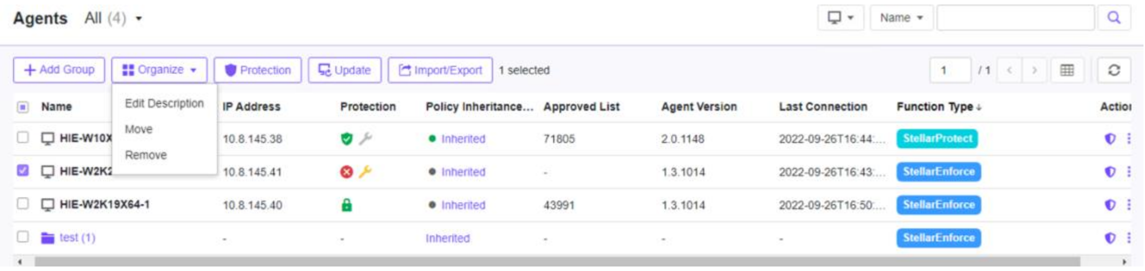
- Actions for Endpoints
- Edition Description from Organize

Procedure

1. Navigate to the **Agents** page.
2. Select one or more endpoints by clicking the checkbox next to them.
3. Click **More actions** icon from **Action** field.
4. Click **Edition Description** and Type or modify the content.
5. Click **Confirm** button.



	Name	IP Address	Protection	Policy Inheritance...	Approved List	Agent Version	Last Connection	Function Type ↓	Actio
□	HIE-W10X64-1	10.8.145.38		● Inherited	71805	2.0.1148	2022-09-26T16:44:...	StellarProtect	
☑	HIE-W2K22X64-1	10.8.145.41	☒	● Inherited	-	1.3.1014	2022-09-26T16:43:...	StellarEnforce	
□	HIE-W2K19X64-1	10.8.145.40		● Inherited	43991	1.3.1014	2022-09-26T16:50:...	StellarEnforce	
□	test (1)	-	-	Inherited	-	-	-	StellarEnforce	



	Name	IP Address	Protection	Policy Inheritance...	Approved List	Agent Version	Last Connection	Function Type ↓	Actio
□	HIE-W10X	10.8.145.38		● Inherited	71805	2.0.1148	2022-09-26T16:44:...	StellarProtect	
☑	HIE-W2K2	10.8.145.41	☒	● Inherited	-	1.3.1014	2022-09-26T16:43:...	StellarEnforce	
□	HIE-W2K19X64-1	10.8.145.40		● Inherited	43991	1.3.1014	2022-09-26T16:50:...	StellarEnforce	
□	test (1)	-	-	Inherited	-	-	-	StellarEnforce	

Move

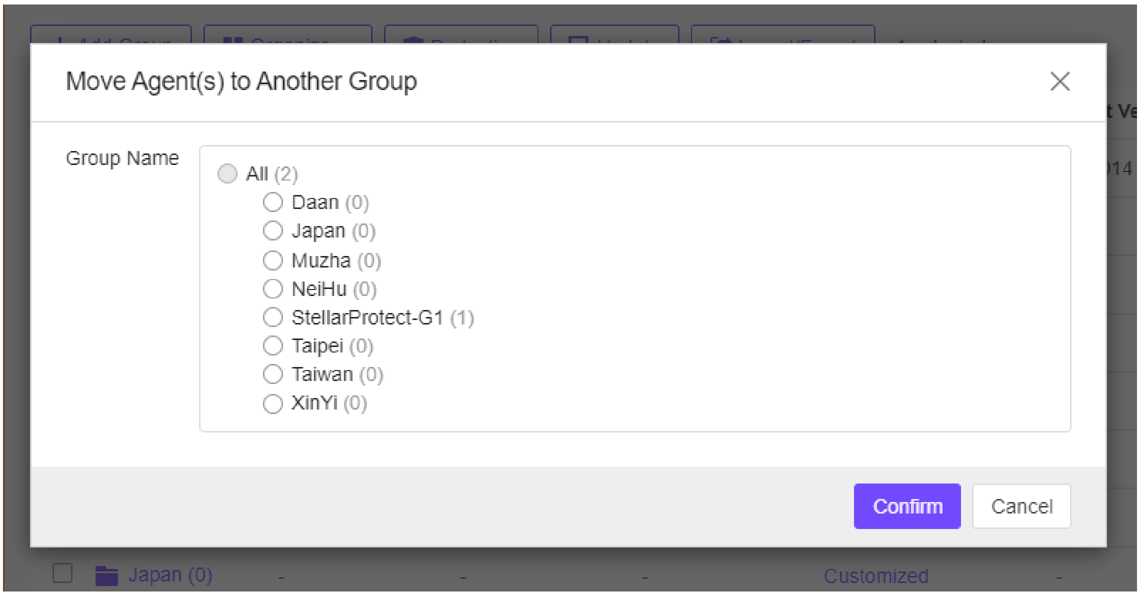
Group agents according to location, type, or purpose to help you manage multiple agents.

- Actions for Endpoints
- Edition Description from Organize

Procedure

1. Navigate to the **Agents** page.
2. Select one or more endpoints by clicking the checkbox next to them.
3. Click **More actions** icon from **Action** field.

4. Click **Move** and select the target **group name**.



Move Agent(s) to Another Group

Group Name

○ All (2)
○ Daan (0)
○ Japan (0)
○ Muzha (0)
○ NeiHu (0)
○ StellarProtect-G1 (1)
○ Taipei (0)
○ Taiwan (0)
○ XinYi (0)

5. Click **Confirm** button.

Remove

Remove agents from the StellarOne server.

StellarEnforce will attempt to unregister agents from StellarOne during uninstallation. However, if StellarEnforce is not connected to the 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” the agents.

Procedure

1. Navigate to the **Agents** page.
2. Select one or more endpoints by clicking the checkbox next to them.
3. Click **More actions** icon from **Action** field.
4. Click **Remove** and select the target group name.
5. Click **Confirm** button that you want to remove the selected items. StellarOne will remove the agents from the list.

Note: Removing an agent from the list of monitored agents does not delete any preexisting agent event logs.

Chapter 6 – Monitoring StellarEnforce

Monitoring StellarEnforce

This chapter introduces StellarOne console monitoring practices.

About the Dashboard

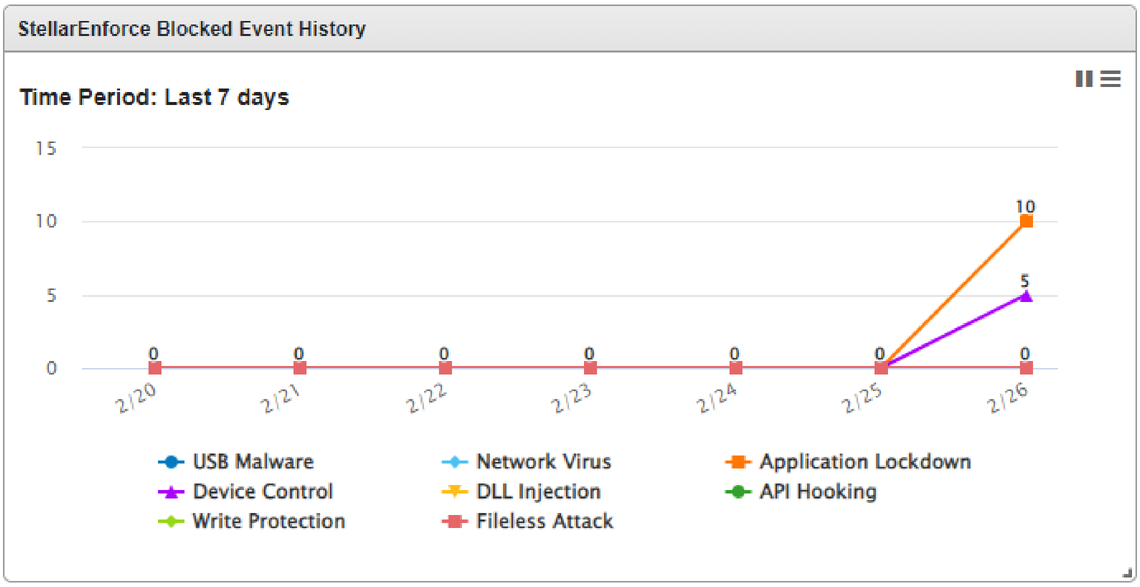
Monitor events from the Dashboard using the overview provided under the Summary tab. This tab is added to the Dashboard by default when there are no user-defined tabs.

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

Blocked Event History

This widget displays a summary of blocked events for the specified time period. By default, the widget is displayed on the Event Overview tab of the Dashboard. Click the display icons to display the data as a pie chart or a line chart.

- Use the Time Period drop-down to display only the event data for the period specified.
- Click an entry on the legend to show or hide data for that event.
- Click a value on the chart to view more details about the blocked event.

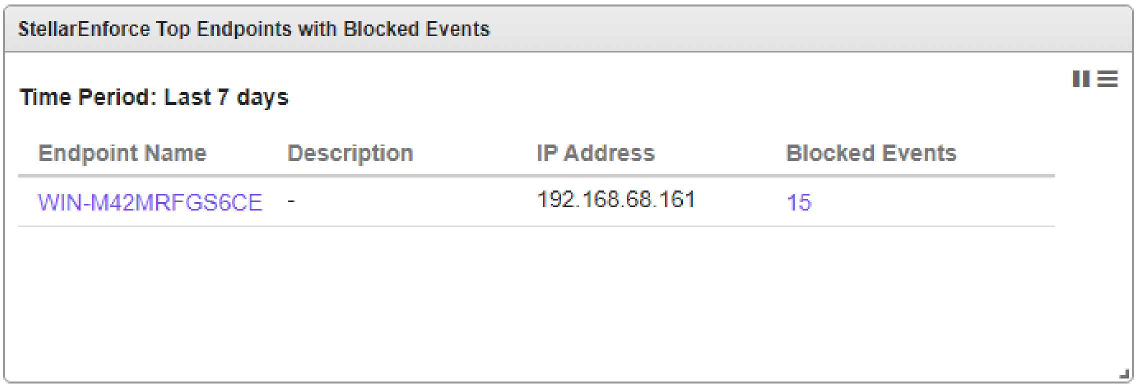

StellarEnforce Blocked Event History

Time Period: Last 7 days

Top Endpoints with Blocked Events

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

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



StellarEnforce Top Endpoints with Blocked Events

Time Period: Last 7 days

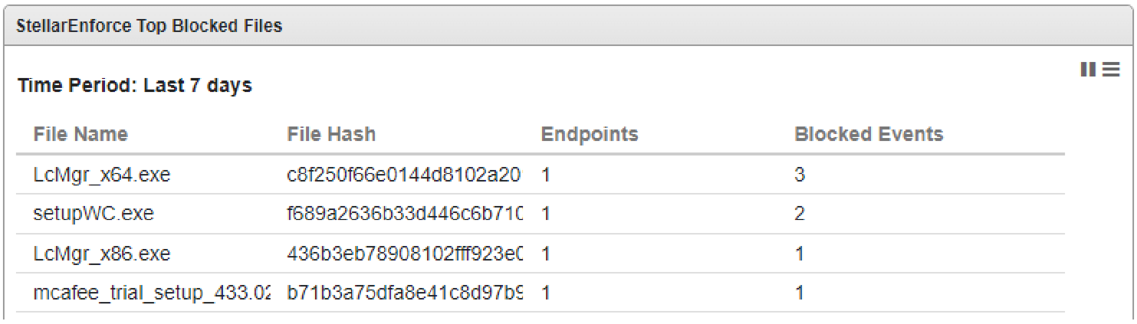
Endpoint Name	Description	IP Address	Blocked Events
WIN-M42MRFGS6CE	-	192.168.68.161	15

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

Top Blocked Files

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

Column	Description
File Name	Name of the file that triggered the blocked events
File Hash	SHA1 hash of the file that triggered the blocked events
Endpoints	Number of endpoints which reported a blocked event for the file
Blocked Events	Total number of blocked events reported for the file



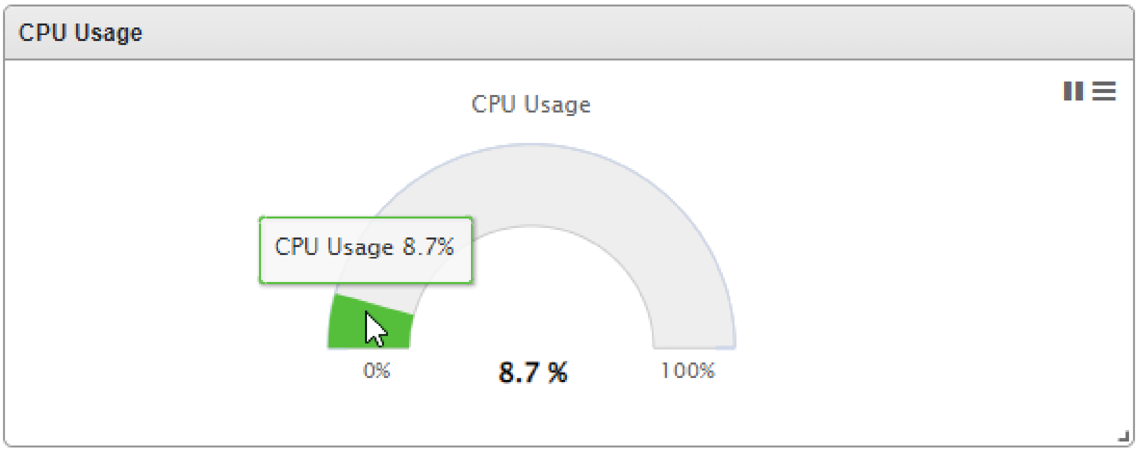
StellarEnforce Top Blocked Files

Time Period: Last 7 days

File Name	File Hash	Endpoints	Blocked Events
LcMgr_x64.exe	c8f250f66e0144d8102a20	1	3
setupWC.exe	f689a2636b33d446c6b71(	1	2
LcMgr_x86.exe	436b3eb78908102fff923e(	1	1
mcafee_trial_setup_433.0:	b71b3a75dfa8e41c8d97b9	1	1

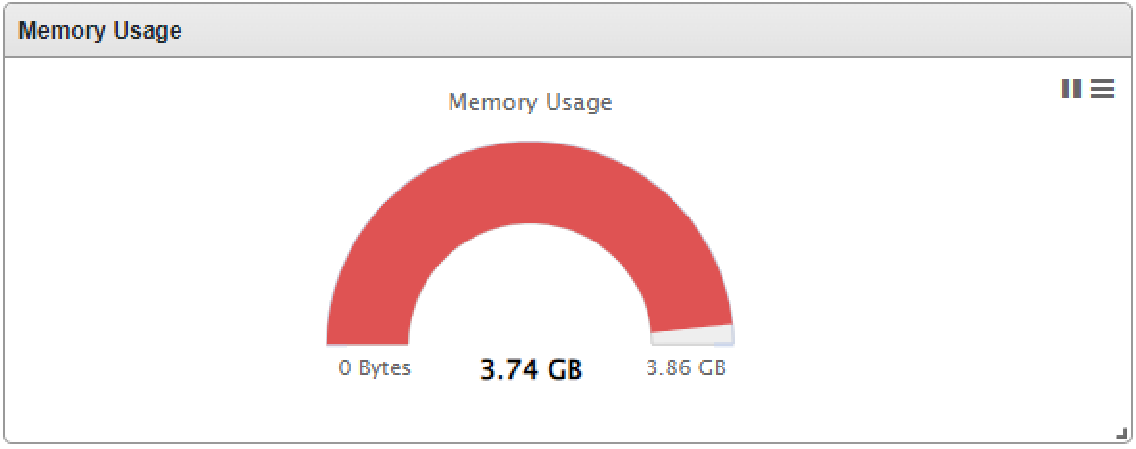
CPU Usage

This widget displays CPU usage information.



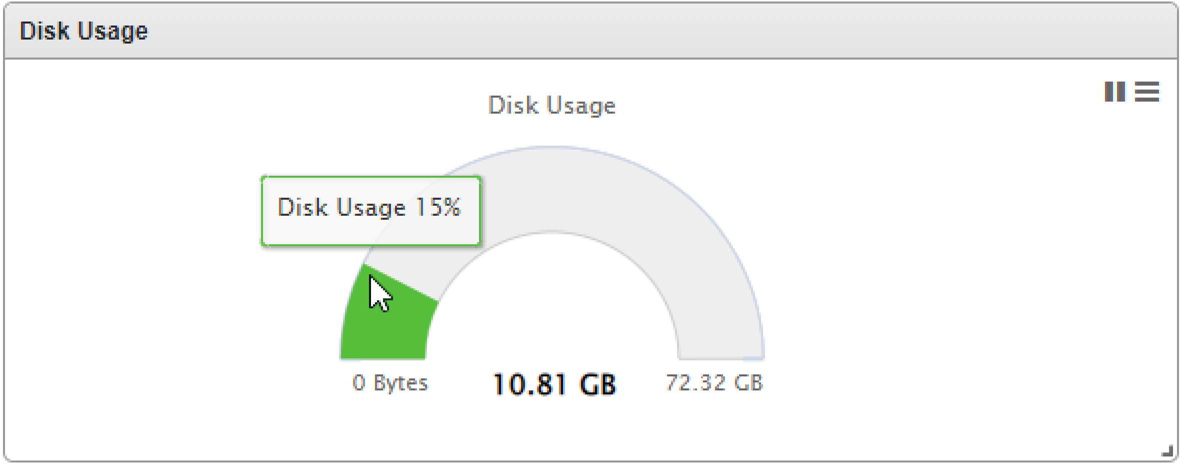
Memory Usage

This widget displays memory usage information.



Disk Usage

This widget displays disk usage information.

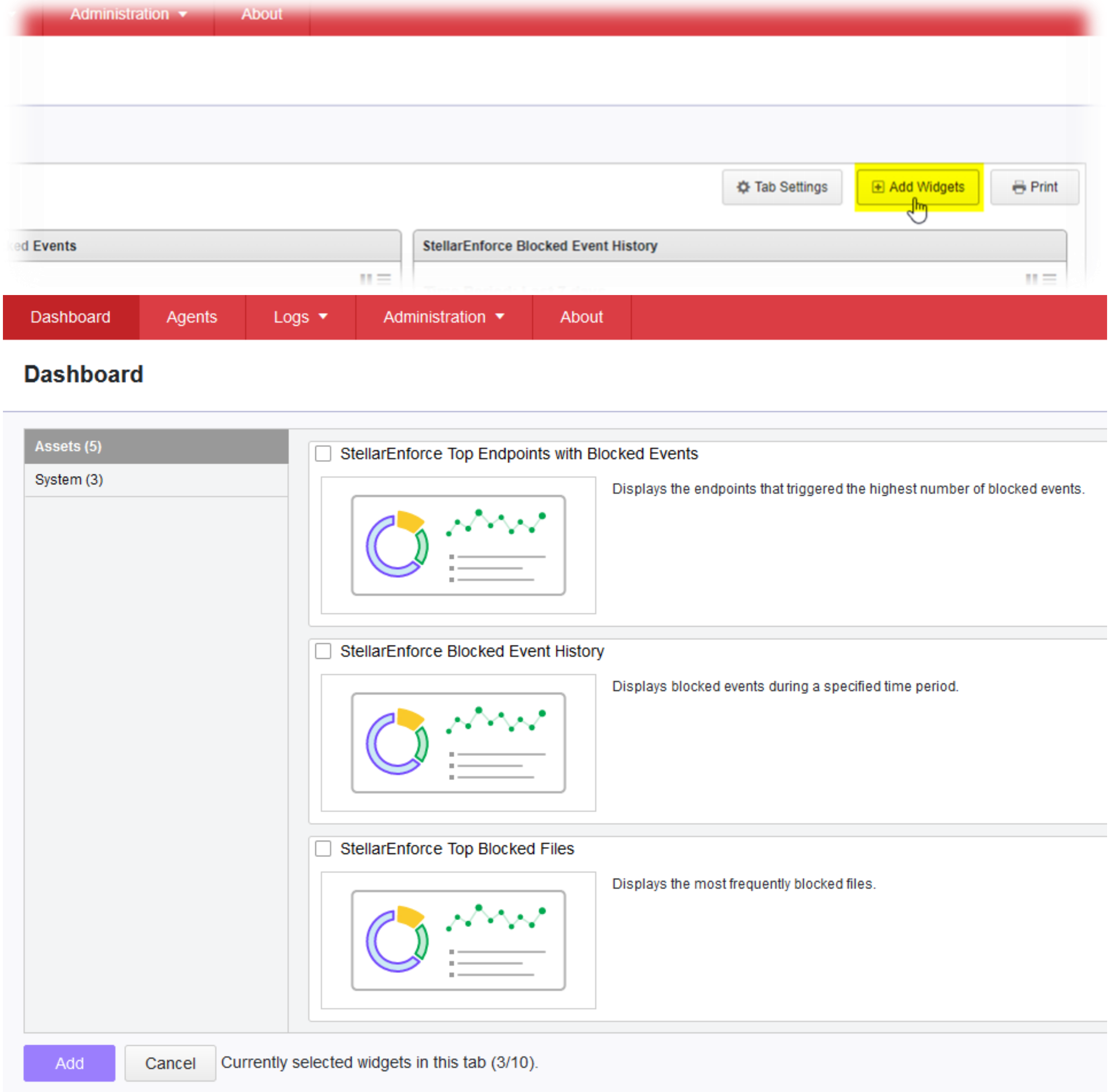


Add Widgets

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

Procedure

1. Go to **Dashboard** in the navigation at the top of the web console.
2. Go to the tab (**Summary** or System) on the dashboard that you want to add the widget to.
3. Click **Add Widgets** and the screen appears.



□ StellarEnforce Top Endpoints with Blocked Events

Displays the endpoints that triggered the highest number of blocked events.

□ StellarEnforce Blocked Event History

Displays blocked events during a specified time period.

□ StellarEnforce Top Blocked Files

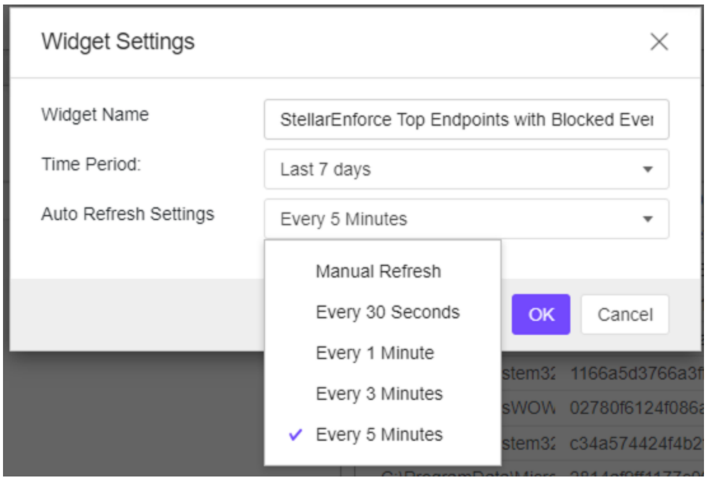
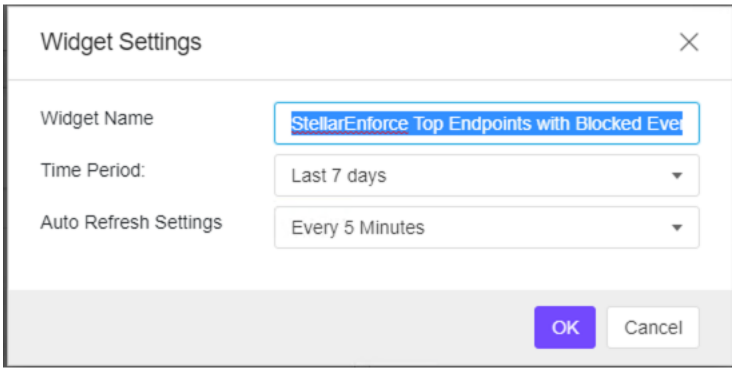
Displays the most frequently blocked files.

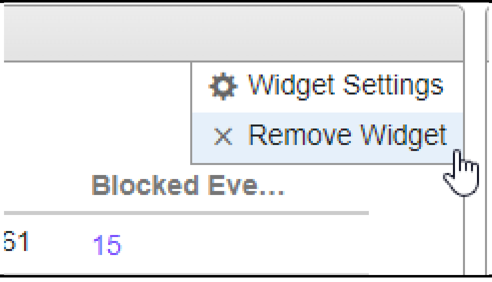
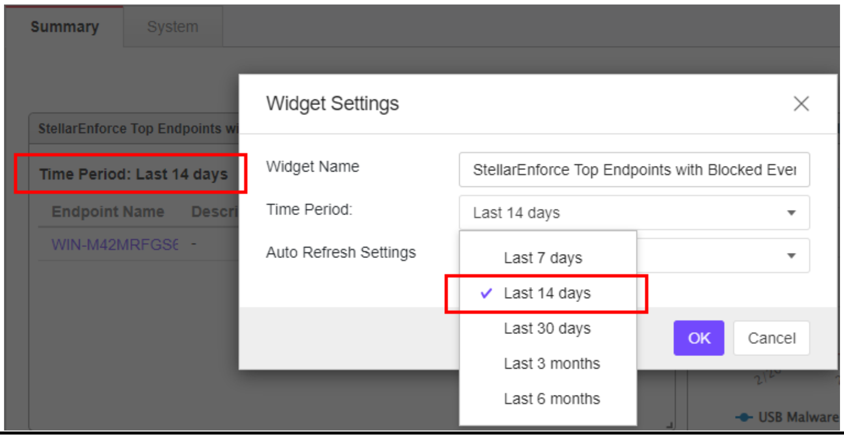
Currently selected widgets in this tab (3/10).

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

Using Widgets

Perform the following tasks on each widget:

Task	Steps
Move a widget	Move widgets on tabs by clicking and holding on the title bar at the top of the widget and dragging to various locations on a tab.
Resize a widget	Drag the edge of each widget to resize.
Refresh widget data	Config the **Auto Refresh Settings** under **Widget Settings** first. (Default value is **Every 5 minutes**)  Widget Settings Widget Name: StellarEnforce Top Endpoints with Blocked Ever Time Period: Last 7 days Auto Refresh Settings: Every 5 Minutes Manual Refresh Every 30 Seconds Every 1 Minute Every 3 Minutes ✓ Every 5 Minutes
Rename a widget	1. Click the More Options icon at the top of the widget. 2. Select Widget Settings. The Widget Settings screen appears. 3. Type a meaningful **widget name** for the widget.  Widget Settings Widget Name: StellarEnforce Top Endpoints with Blocked Eve Time Period: Last 7 days Auto Refresh Settings: Every 5 Minutes
Close a widget	1. Click the More Options icon at the top of the widget. 2. Select **Remove Widget**.

	 Widget Settings Remove Widget Blocked Eve... 61 15
Set Time Period	Displays the data during the specified time period. (Default value is **Last 7 days**)  Summary System StellarEnforce Top Endpoints wi Time Period: Last 14 days Endpoint Name Descri WIN-M42MRFGS6 - Widget Settings Widget Name StellarEnforce Top Endpoints with Blocked Evei Time Period: Last 14 days Auto Refresh Settings Last 7 days ✓ Last 14 days Last 30 days Last 3 months Last 6 months OK Cancel USB Malware

About the Agent Events Screen

To display the Agent Events screen, go to **Logs** > **Agent Events** in the navigation at the top of the web console. This screen displays a list of events related to applications not in the Approved List on agents managed by StellarOne.

Depending on the feature status, StellarEnforce generates a log and performs the action for the events listed in the following table. Event logs contain information from managed agents about files not in the Approved List and any action taken.

Event	Feature Status	StellarEnforce Action
A file not on an agent's Approved List attempts to run or make changes to the endpoint	Lockdown disabled	Allows the file to run
	Lockdown enabled	Blocks the file and prompts for user action
A storage device (CD/DVD drive, floppy disk, or USB device) attempts to access the endpoint	Device Control disabled	Allows access for the device
	Device Control enabled	Denies access for the device (when the device type is removable device) and prompts for user action

The following table describes the user actions for the events.

User Action	Description
Add to Approved List	Prevent the file from executing or deny the USB device access to the endpoint for this instance but add the file or USB device to the agent's Approved List. This allows the file to execute or USB device access for subsequent detections.
Ignore	Prevent the file from executing but do not move or change the file.
Quarantine	Prevent the file from executing and hold the file in quarantine for later analysis.
Delete	Prevent the file from executing and delete the file.

Querying Agent Event Logs

Querying refines the list of displayed agent event logs.

Procedure

1. Go to Logs > Agent Events in the navigation at the top of the web console. The Agent Events screen will appear.
2. To filter by period, click the Time Period drop down, which defaults to Last 30 days, and pick a time period. Perform one of the following:

   - Click a listed time range.
   - Click Custom, specify a time range, and click Search.

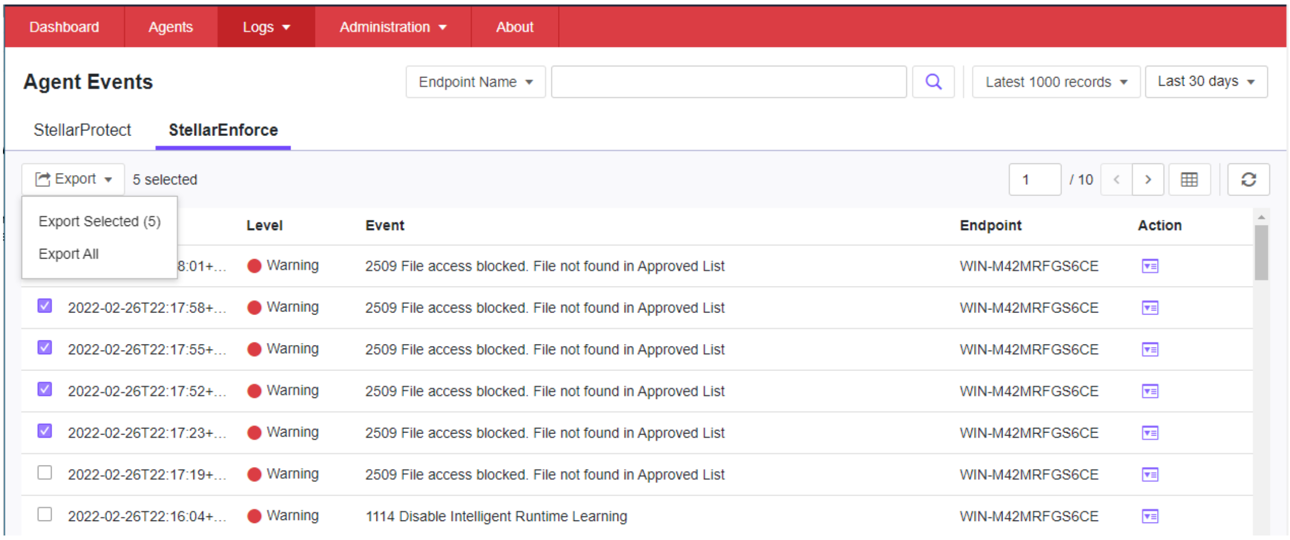
3. To filter by Endpoint Name, Group Name, IP Address, IP Range, Tag, Event Type, Severity Level, Integrity Monitoring, Blocked File, or Malware Detection, click the drop-down to the left of the search bar and specify a criteria.

   - Endpoint Name: Specify the name of the endpoint you’re looking for.
   - Group Name: Specify the name of the group you’re looking for.
   - IP Address: Specify the IP address of the agent you’re looking for.
   - IP Range: Specify a range of IPs to search for agents within.
   - Description: Specify the description assigned to the endpoint
   - Event Type: Select a specific event and click Apply.
   - Severity Level: Select Information or Warning as the event level.
   - Integrity Monitoring: Select File or Folder or Registry Key or Value, and click Search. File or Folder searches support partial string matching.
   - Blocked File: Select File Name or File Hash (SHA-1), and click Search. File Name searches support partial string matching.
   - Malware Detection: Select All Detections, Unsuccessful actions, Cleaned, Quarantined, Deleted, Ignored or Rolled Back.

4. The table displays only the entries that match the filters selected.

Exporting Agent Events

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



		Level	Event	Endpoint	Action
	8:01+...	● Warning	2509 File access blocked. File not found in Approved List	WIN-M42MRFGS6CE	
☑	2022-02-26T22:17:58+...	● Warning	2509 File access blocked. File not found in Approved List	WIN-M42MRFGS6CE	
☑	2022-02-26T22:17:55+...	● Warning	2509 File access blocked. File not found in Approved List	WIN-M42MRFGS6CE	
☑	2022-02-26T22:17:52+...	● Warning	2509 File access blocked. File not found in Approved List	WIN-M42MRFGS6CE	
☑	2022-02-26T22:17:23+...	● Warning	2509 File access blocked. File not found in Approved List	WIN-M42MRFGS6CE	
□	2022-02-26T22:17:19+...	● Warning	2509 File access blocked. File not found in Approved List	WIN-M42MRFGS6CE	
□	2022-02-26T22:16:04+...	● Warning	1114 Disable Intelligent Runtime Learning	WIN-M42MRFGS6CE	

Procedure

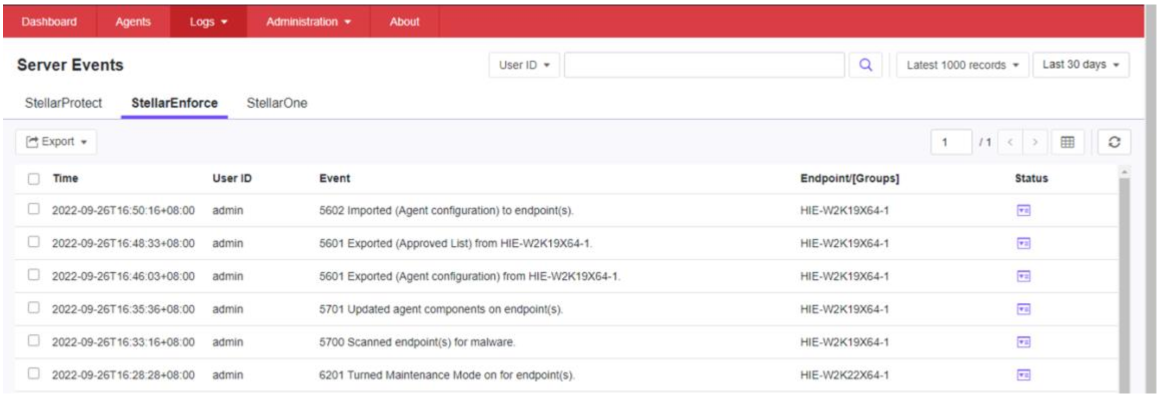
1. Go to **Logs** > **Agent Events** in the navigation at the top of the web console. The **Agent Events** screen will appear.
2. Select the agent log entries in the list that you want to export information for.

   - To export all entries, click the **Export All** on the upper-right.
   - To export selected entries only, select the entries you wish to export, then click the **Export Selected** button in the upper-left.

3. Save the file.

About the Server Events Screen

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



□	Time	User ID	Event	Endpoint/[Groups]	Status
□	2022-09-26T16:50:16+08:00	admin	5602 Imported (Agent configuration) to endpoint(s).	HIE-W2K19X64-1	
□	2022-09-26T16:48:33+08:00	admin	5601 Exported (Approved List) from HIE-W2K19X64-1.	HIE-W2K19X64-1	
□	2022-09-26T16:46:03+08:00	admin	5601 Exported (Agent configuration) from HIE-W2K19X64-1.	HIE-W2K19X64-1	
□	2022-09-26T16:35:36+08:00	admin	5701 Updated agent components on endpoint(s).	HIE-W2K19X64-1	
□	2022-09-26T16:33:16+08:00	admin	5700 Scanned endpoint(s) for malware.	HIE-W2K19X64-1	
□	2022-09-26T16:28:28+08:00	admin	6201 Turned Maintenance Mode on for endpoint(s).	HIE-W2K22X64-1	

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

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

Querying Server Event Logs

Querying refines the list of displayed server event logs.

Procedure

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

Option	Description
Time Period	Do one of the following: • Select a listed time range. • Specify a custom time range. a. Go to Custom in the list. b. Specify your custom time range.

	c. Click Apply.
User Name	Displays all events logged by a specific user.
Endpoint Name	Type the endpoint host name (first few letters or complete name), and click Search.
Group Name	Displays all events logged by the specific groups.
Event Type	Select a specific event.

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

Exporting Server Event Logs

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

Procedure

1. Go to Logs > Server Events in the navigation at the top of the web console. The Server Events screen will appear.
2. Select the server log entries in the list that you want to export information for.

   - To export all entries, click the Export icon.
   - To export selected entries only, select the entries you wish to export then click Export Selected.

3. Save the file.

About the System Log Screen

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

Querying Server Logs

Querying refines the list of displayed server event logs.

Procedure

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

Option	Description
Time Period	Do one of the following: • Select a listed time range. • Specify a custom time range. a. Go to Custom in the list. b. Specify your custom time range. c. Click Search.
Severity	Select one of the criteria below and click Search. • Emergency • Alert • Critical • Error • Warning • Notice • Information • Debug

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

Exporting System Logs

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

Procedure

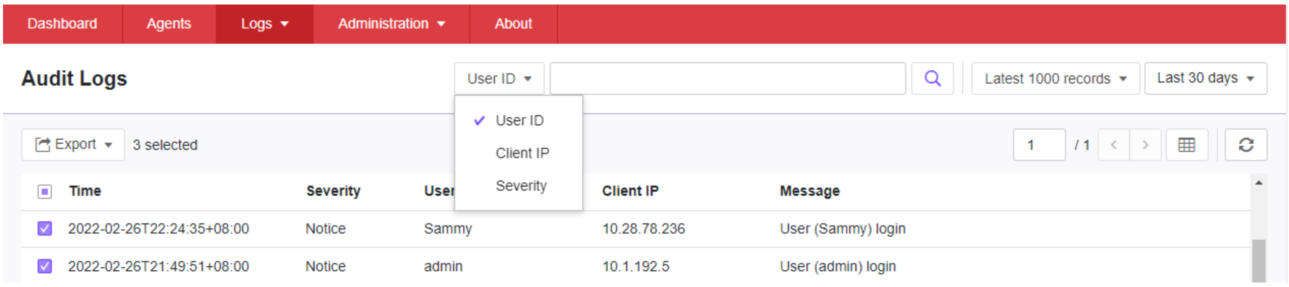
1. Go to Logs > System Logs in the navigation at the top of the web console. The System Logs screen will appear.
2. Select the system log entries in the list that you want to export information for.
    - To export all entries, click the Export icon.
    - To export selected entries only, select the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

About the Audit Log Screen

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

Querying Audit Logs

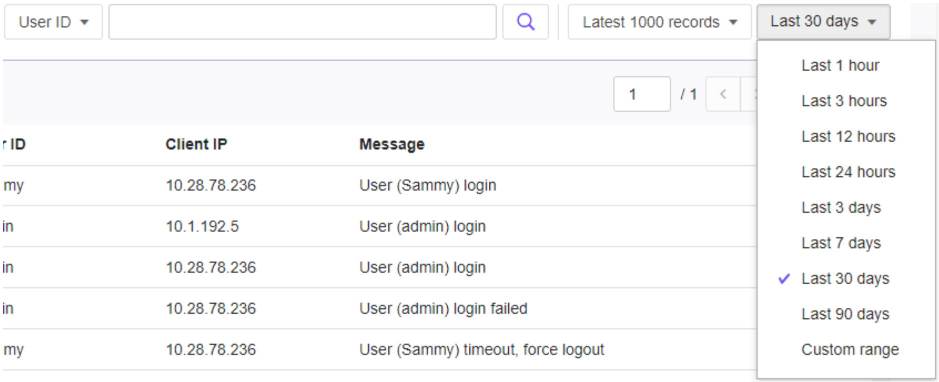
Querying refines the list of displayed server event logs.



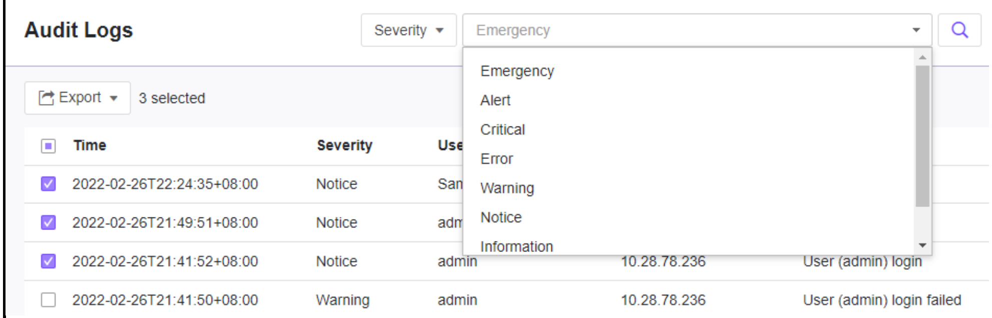
☑	Time	Severity	User	Client IP	Message
☑	2022-02-26T22:24:35+08:00	Notice	Sammy	10.28.78.236	User (Sammy) login
☑	2022-02-26T21:49:51+08:00	Notice	admin	10.1.192.5	User (admin) login

Procedure

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

Option	Description
Time Period	

ID	Client IP	Message
my	10.28.78.236	User (Sammy) login
in	10.1.192.5	User (admin) login
in	10.28.78.236	User (admin) login
in	10.28.78.236	User (admin) login failed
my	10.28.78.236	User (Sammy) timeout, force logout

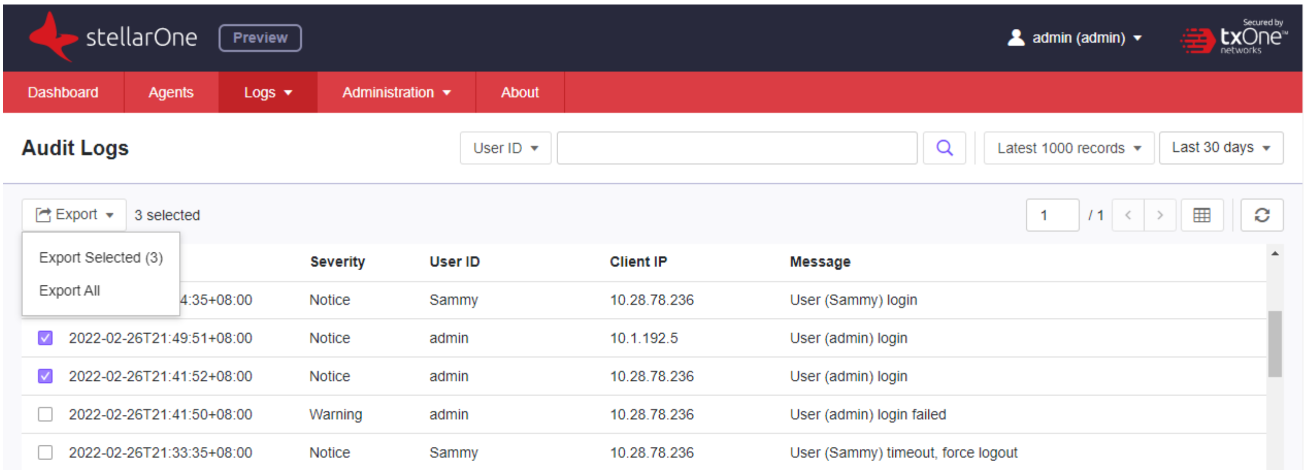
	Do one of the following: - Select a listed time range. - Specify a custom time range. a. Go to Custom in the list. b. Specify your custom time range. c. Click Search.
User ID	Type user ID and click Search.
Client IP	Type client IP number and click Search.
Severity	Select one of the criteria below and click Search.  - Emergency - Alert - Critical - Error - Warning - Notice - Information - Debug

☐	Time	Severity	Use		
☑	2022-02-26T22:24:35+08:00	Notice	San		
☑	2022-02-26T21:49:51+08:00	Notice	adm		
☑	2022-02-26T21:41:52+08:00	Notice	admin	10.28.78.236	User (admin) login
☐	2022-02-26T21:41:50+08:00	Warning	admin	10.28.78.236	User (admin) login failed

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

Exporting Audit Logs

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



		Severity	User ID	Client IP	Message
	4:35+08:00	Notice	Sammy	10.28.78.236	User (Sammy) login
☑	2022-02-26T21:49:51+08:00	Notice	admin	10.1.192.5	User (admin) login
☑	2022-02-26T21:41:52+08:00	Notice	admin	10.28.78.236	User (admin) login
☐	2022-02-26T21:41:50+08:00	Warning	admin	10.28.78.236	User (admin) login failed
☐	2022-02-26T21:33:35+08:00	Notice	Sammy	10.28.78.236	User (Sammy) timeout, force logout

Procedure

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

Chapter 7 - Configuring Administration Settings

This chapter introduces TXOne StellarOne administration settings.

About the Account Management Screen

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

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

Account Type	Privileges
Admin (Full Control)	a. Manage StellarOne: The privilege of configuring system settings. b. Manage Group: The privilege of creating, moving, or deleting groups. c. Account Management: The privilege of managing StellarOne accounts. d. Policy Configuration: The privilege of defining policy for Agents such as USB Control and Intelligent Runtime Learning.
Operator (Asset Control)	a. Manage Group: The privilege of creating, moving, or deleting groups. b. Policy Configuration: The privilege of defining policy for Agents such as USB Control and Intelligent Runtime Learning.
Viewer (Read Only)	a. Read only for Dashboard, Policy Configuration, and Agent Events. b. Agent installer package download available. c. Modify their own account password.

Server Accounts Overview

TXOne StellarOne features web console accounts with different privileges and limitations. Use these accounts to configure StellarOne and to monitor or manage StellarEnforce agents. The following table outlines typical StellarOne tasks and the account privileges required to perform them.

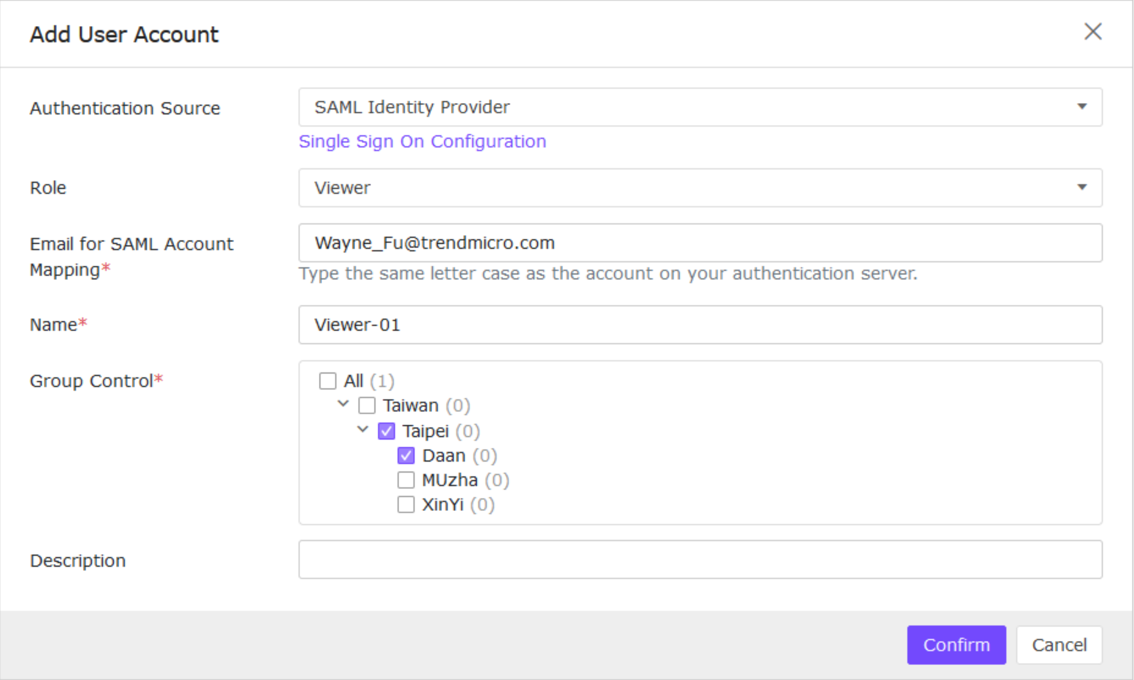
Task	Account Privilege Allowed		
	Admin	Operator	Viewer
Dashboard	V	V	V
Configure application lockdown	V	V	
Configure maintenance mode	V	V	
Configure device control	V	V	
Add trusted files	V	V	

Add trusted USB devices	V	V	
Scan now	V	V	
Update approved list	V	V	
Update agent components	V	V	
Deploy agent patch	V	V	
Check connection	V	V	V
Collect event logs	V	V	
Import / Export (approved list / agent configuration)	V	V	
Organize (edit description / move / delete)	V	V	
Configure group policy	V	V	
Configure global policy	V	V	
Monitor agent event logs	V	V	V
Monitor server event logs	V	V	
Monitor system logs	V	V	
Monitor audit logs	V	V	
Account management	V		
Single Sign-On	V		
System time	V	V	
Syslog forwarding	V	V	
Log purge	V	V	
Schedule report	V	V	V
Notification settings	V	V	V
SMTP settings	V	V	
Proxy settings	V	V	
Downloads / Updates	V	V	V
Firmware	V		
SSL Certificate	V		
License management	V	V	

Adding Accounts

Procedure

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



Add User Account

Authentication Source: SAML Identity Provider

Single Sign On Configuration

Role: Viewer

Email for SAML Account Mapping*: Wayne_Fu@trendmicro.com

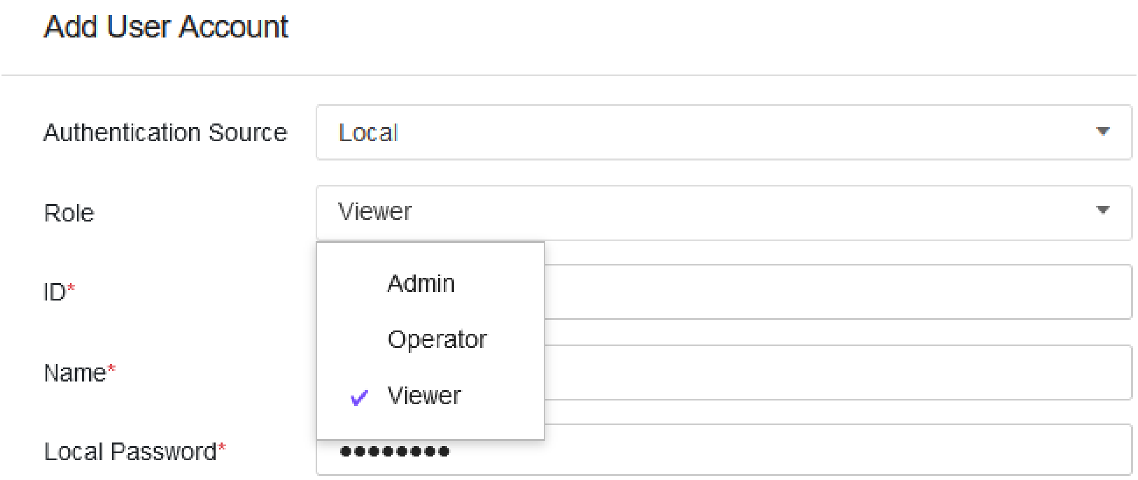
Type the same letter case as the account on your authentication server.

Name*: Viewer-01

Group Control*:
- □ All (1)
  - □ Taiwan (0)
    - ☑ Taipei (0)
      - ☑ Daan (0)
      - □ MUzha (0)
      - □ XinYi (0)

Description:

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



Add User Account

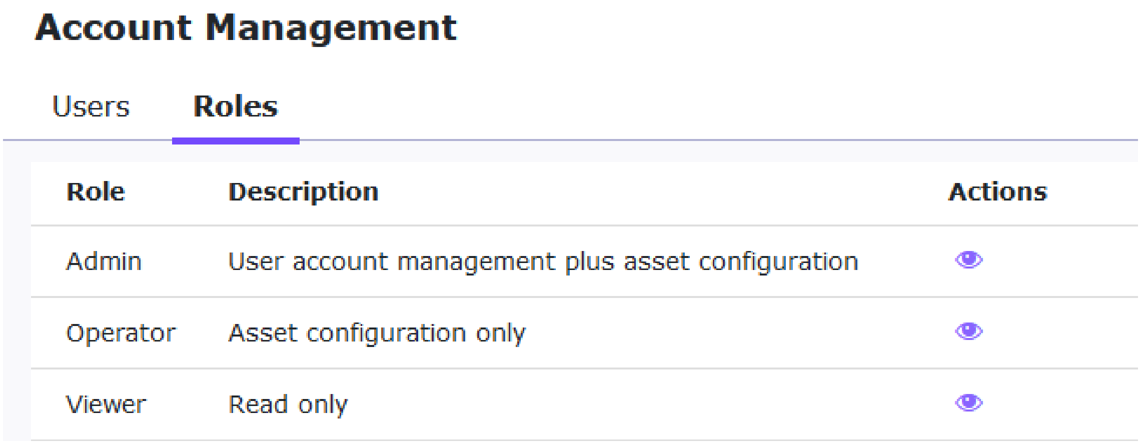
Authentication Source: Local

Role: Viewer

ID*

Name*

Local Password*: ●●●●●●●●●



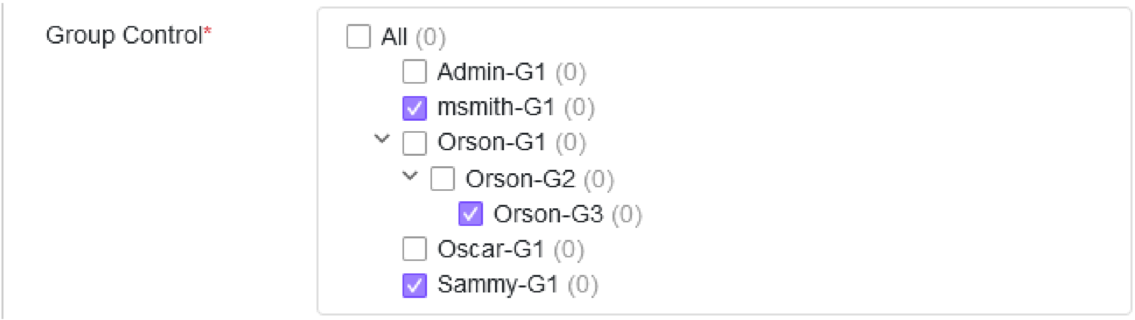
Account Management

Users | **Roles**

Role	Description	Actions
Admin	User account management plus asset configuration	👁
Operator	Asset configuration only	👁
Viewer	Read only	👁

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

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



Group Control*

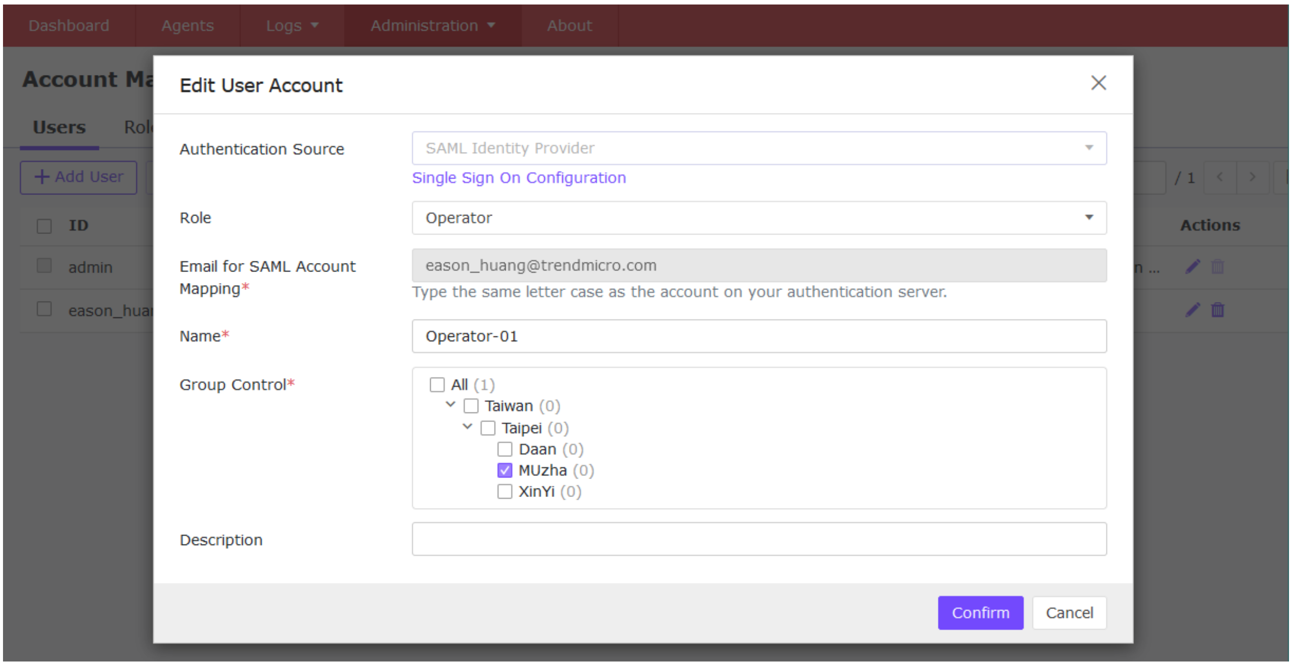
- ☐ All (0)
  - ☐ Admin-G1 (0)
  - ☑ msmith-G1 (0)
  - ☐ Orson-G1 (0)
    - ☐ Orson-G2 (0)
      - ☑ Orson-G3 (0)
  - ☐ Oscar-G1 (0)
  - ☑ Sammy-G1 (0)

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

Edit Accounts

Procedure

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



Edit User Account

Authentication Source: SAML Identity Provider

Single Sign On Configuration

Role: Operator

Email for SAML Account Mapping*: eason_huang@trendmicro.com

Type the same letter case as the account on your authentication server.

Name*: Operator-01

Group Control*:

- ☐ All (1)
  - ☐ Taiwan (0)
    - ☐ Taipei (0)
      - ☐ Daan (0)
      - ☑ MUzha (0)
      - ☐ XinYi (0)

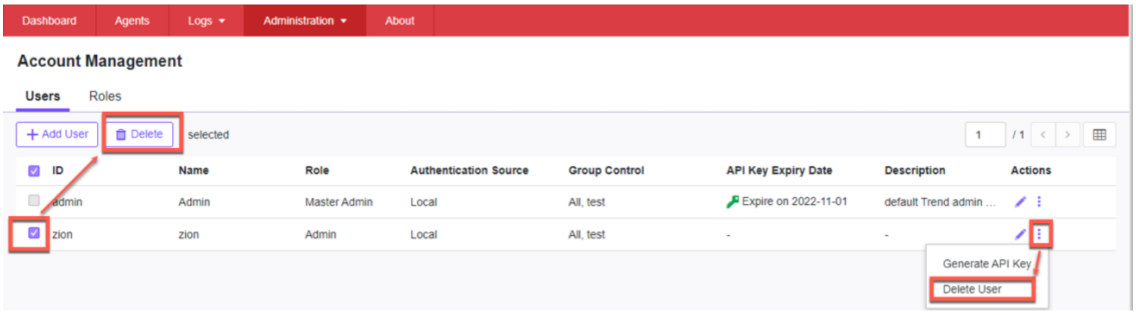
Description:

Confirm | Cancel

Delete Accounts

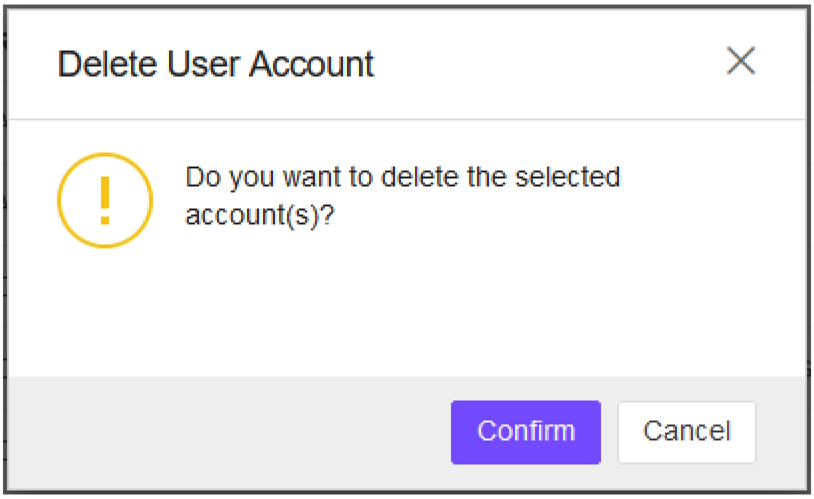
Procedure

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



☑ ID	Name	Role	Authentication Source	Group Control	API Key Expiry Date	Description	Actions
□ admin	Admin	Master Admin	Local	All, test	Expire on 2022-11-01	default Trend admin ...	⋮
☑ zion	zion	Admin	Local	All, test	-	-	⋮

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



Do you want to delete the selected account(s)?

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

Generate an API Key

Users can generate API keys and query data from agents via the open API. The expiration dates of the API keys can be set for different user accounts to increase account management efficiency.

Procedure

1. Log on the web console using an administrator account. (Please note that information entered here is case-sensitive)
2. Go to **Administration** > **Account Management** in the navigation at the top of the web console. The Account Management screen will appear.
3. Under the Users tab, find the user ID you want to modify and go to thekebab menu under **Actions** at the right of the screen.
4. Click on the kebab menu, and then select the **Generate an API Key** option.
5. The **Generate an API Key** window appears. Click the date picker and choose an expiration date on the pop-up calendar. Click **Confirm**.
6. An API key is generated. Click the clipboard for copying the generated API key.

Important:

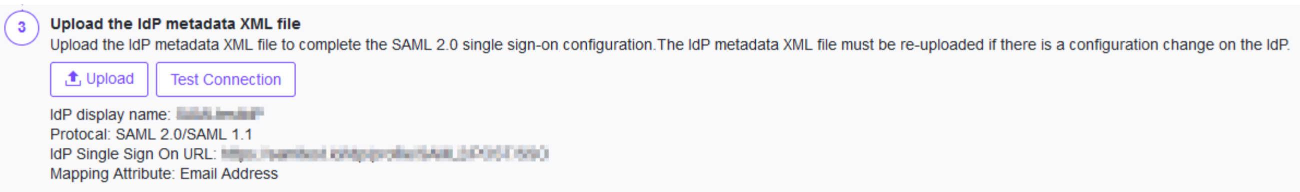
Make sure to back up the copied API key before proceeding to the next step. The API key will not be displayed again for security reasons.

7. Click **OK**.

Single Sign-On

Procedure

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

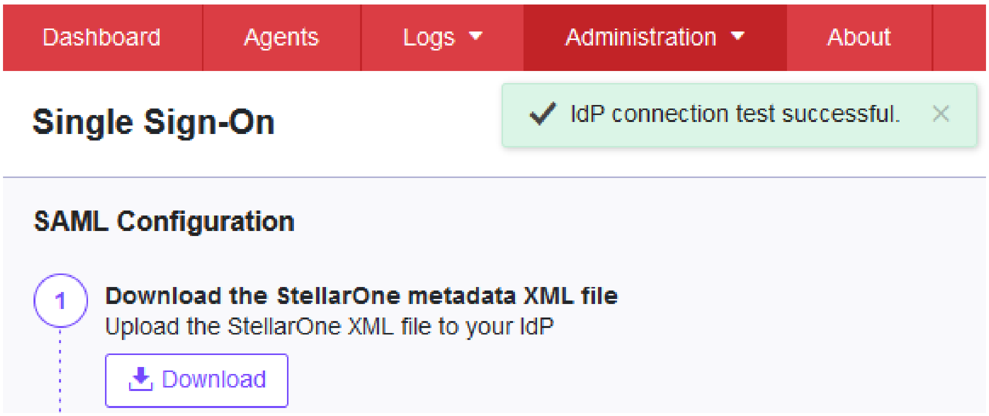


3 **Upload the IdP metadata XML file**

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

IdP display name: [redacted]
Protocal: SAML 2.0/SAML 1.1
IdP Single Sign On URL: [redacted]
Mapping Attribute: Email Address

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



Single Sign-On

✓ IdP connection test successful.

SAML Configuration

1 **Download the StellarOne metadata XML file**

Upload the StellarOne XML file to your IdP

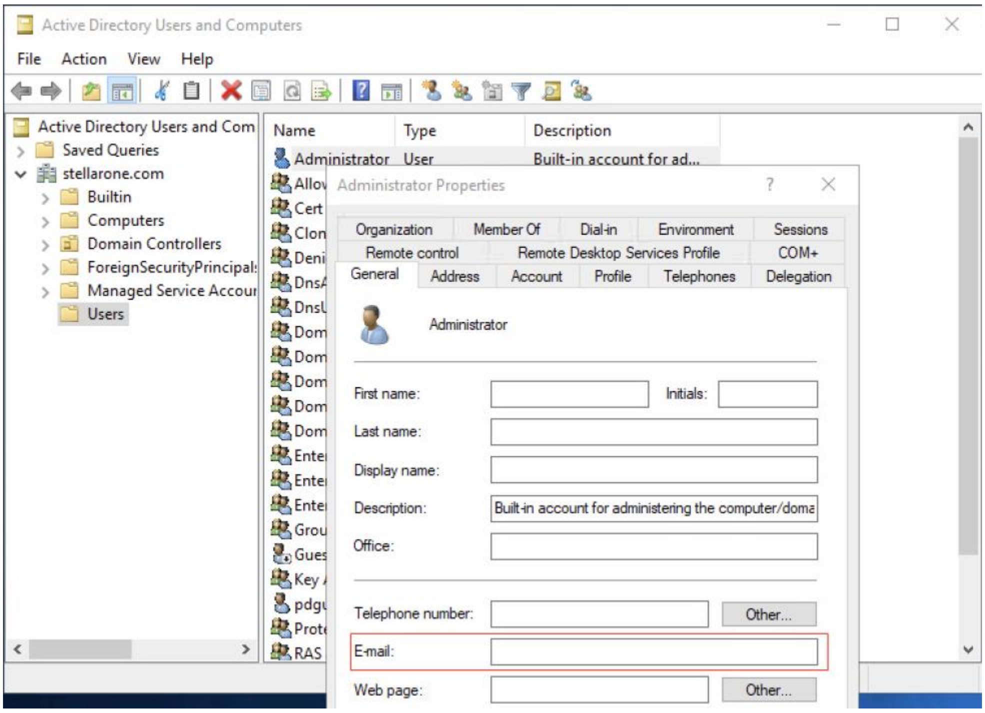
Note:

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

Resolving the SSO Issue

Procedure

1. Open the **Users** folder under **Active Directory Users and Computers** in IdP server.
2. Right-click on the user account used for SSO, then go to **Properties** > **General**.
3. Check the E-mail field. Make sure the email input here is consistent with the account email for accessing StellarOne web console.

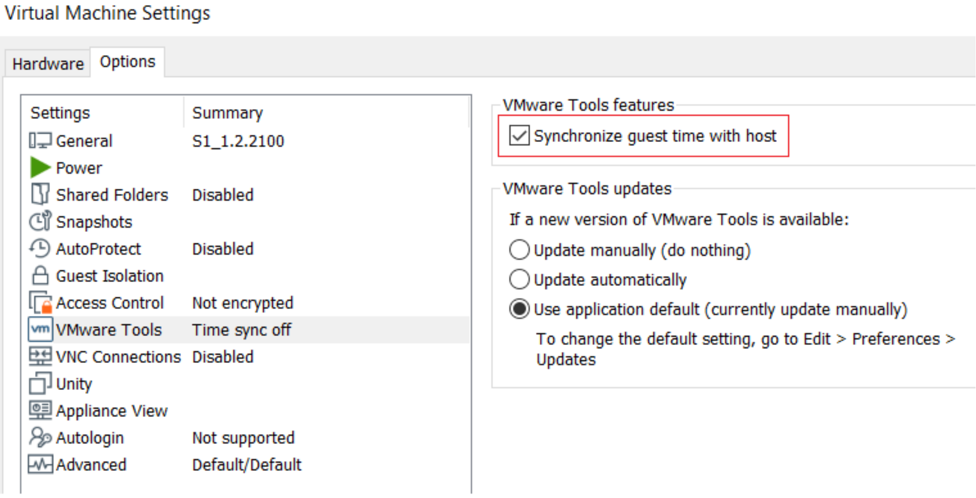


Name	Type	Description
Administrator	User	Built-in account for ad...

Administrator

First name:
Initials:
Last name:
Display name:
Description: Built-in account for administering the computer/doma
Office:
Telephone number:
E-mail:
Web page:

4. Make sure the system time in IdP and StellarOne servers are synchronized. Below are suggested procedures for time synchronization setting.
   a. Ensure the time in IdP server synchronizes with the host PC that runs the StellarOne Virtual Machine (VM).
   b. Open the VM settings of StellarOne. Go **to Options** > **VMware Tools**.
   c. Check the box of **Synchronize guest time with host**, and then click **OK**.



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

VMware Tools features

☑ Synchronize guest time with host

VMware Tools updates

If a new version of VMware Tools is available:

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

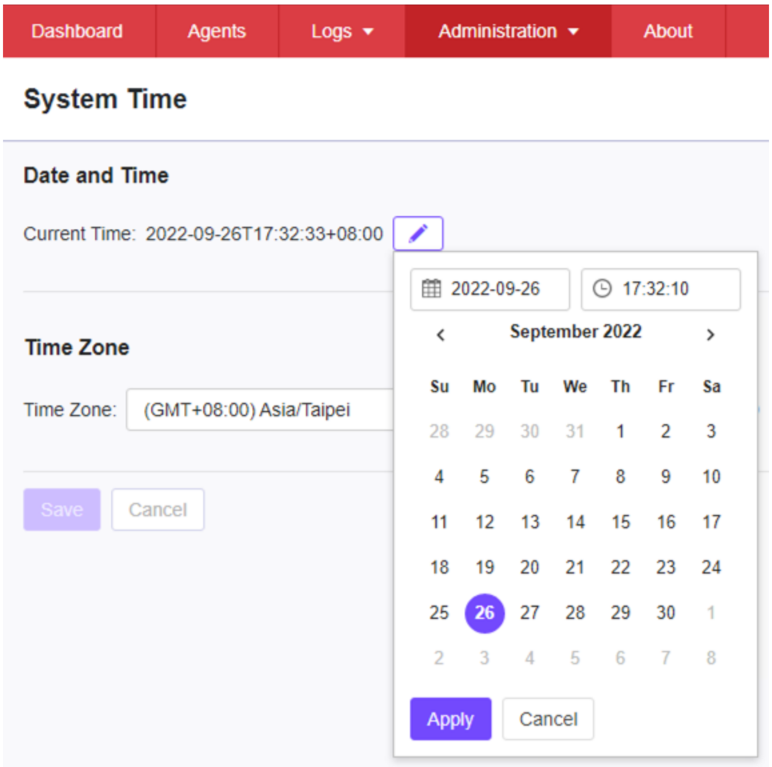
To change the default setting, go to Edit > Preferences > Updates

System Time

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

Date and Time

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



Current Time: 2022-09-26T17:32:33+08:00

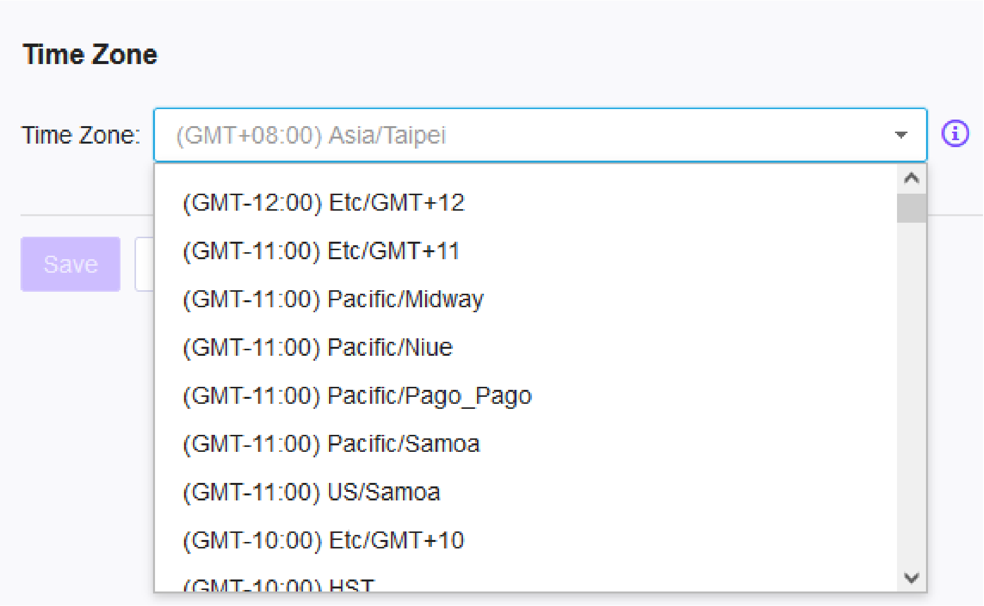
2022-09-26 17:32:10

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

Su	Mo	Tu	We	Th	Fr	Sa
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	1
2	3	4	5	6	7	8

Time Zone

Use the drop-down to specific system time zone.



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

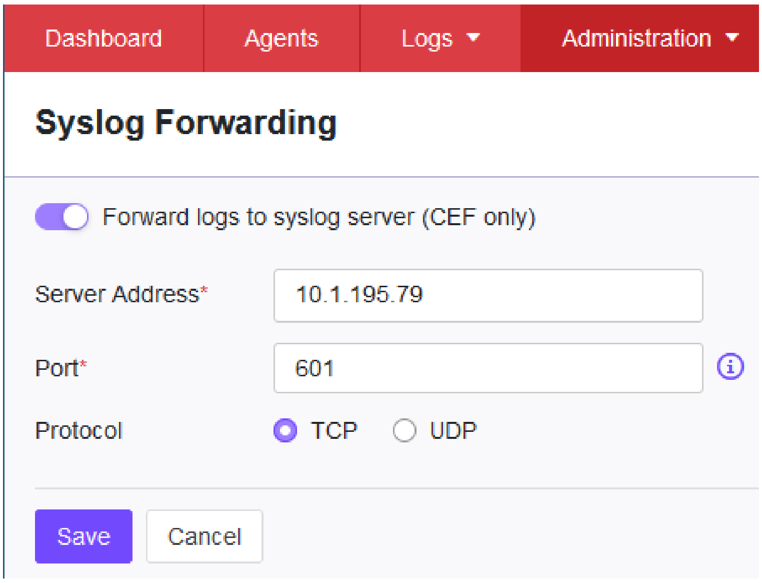
(GMT-12:00) Etc/GMT+12
(GMT-11:00) Etc/GMT+11
(GMT-11:00) Pacific/Midway
(GMT-11:00) Pacific/Niue
(GMT-11:00) Pacific/Pago_Pago
(GMT-11:00) Pacific/Samoa
(GMT-11:00) US/Samoa
(GMT-10:00) Etc/GMT+10
(GMT-10:00) HST

Syslog Forwarding

You can forward Server and Agent Event logs to an external Syslog server for the additional managing and monitoring capabilities. TXOne StellarOne console forwards logs in the Common Event Format (CEF). Make sure your Syslog server supports the Common Event Format (CEF).

Procedure

1. Go to **Administration** > **Syslog Forwarding**.
2. Enable **Forward logs to syslog server (CEF only)**.
3. Specify the Protocol, Server Address, and Port of the Syslog server.



Forward logs to syslog server (CEF only)

Server Address* 10.1.195.79

Port* 601

Protocol ● TCP ○ UDP

Syslog Format

CEF Key	Description	Value
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Device Vendor	Example: TXOne Networks
Header (pname)	Device Product	Example: StellarOne, StellarEnforce
Header (pver)	Device Version	Example: 1.2.0171
Header (eventid)	Device Event Class ID	Example: 2509、6005
Header (eventName)	Name	Example: Agent Event, Server Event, Console Log
Header (severity)	Severity	Example: 4

rt	Logged Time	Example: Apr 02 2022 13:31:51 GMT+00:00
msg	Event Id mapped message	Example: File access blocked. File not found in Approved List
dvchost	Computer name	Example: Localhost
dvc	IP address	Example: 192.168.154.137
cs1Label	Detailed Event Message	Detailed Event Message
cs1	Event ID mapped detailed message	Example: File access blocked: C:\\Documents and Settings\\Administrator\\Local Settings\\Temp\\is-D5V0T.tmp\\is-H7K4O.tmp Malware detected: Quarantine. File path: C:\\eicar\\EICAR_TEST_FILE.exe
cs2Label	Client OS	Client OS
cs2	OS description	Example: Microsoft Windows 7 Enterprise Edition Service Pack 1 build 7601, 64-bit
cs3Label	Client Description	Client Description
cs3	Description	-
suser	Login User	Example: PC1688\\Administrator
act	Action Type	Example: ACTION_TYPE_BLOCKED
fileHash	SHA1	Example: 2201589AA3ED709B3665E4FF979E10C6AD5137FC
filePath	File path	Example: C:\\Documents and Settings\\Administrator\\Local Settings\\Temp\\is-D5V0T.tmp\\is-H7K4O.tmp
fileCreateTime	File create time	Example: 04 02 2022 14:00:21
fileModificationTime	File modified time	Example: 04 02 2022 14:00:21
logGuid	Log GUID	Example: F43500BB-1F8A-4589-A292-144A9DA343AA、{56B7345A-B6D3-4BBB-A515-4AFFAE04092F}
ServerIP	Server IP	Example: 10.8.145.157

Example:

```
Message: CEF:0|TXOne Networks|StellarEnforce|1.2.0171|2509|Agent Events|4|rt=Apr
02 2022 14:09:29 GMT+00:00 msg=File access blocked. File not found in Approved List
dvchost=PC1688 dvc=192.168.154.137 logGuid={CEFD0E54-7693-4B3F-9DDA-
3E6F40A9384E} cs1Label=Detailed Event Message cs1=File access blocked:
```

```
C:\\eicar\\EICAR_TEST_FILE.gz.vbs cs2Label=Client OS cs2=Windows XP Professional
Service Pack 3 build 2600, 32-bit cs3Label=Client Description cs3=
suser=PC1688\\Administrator act=ACTION_TYPE_BLOCKED
fileHash=7dd27fab1f11084e984b631a614a5120c8e25598
filePath=C:\\eicar\\EICAR_TEST_FILE.gz.vbs fileCreateTime=09 13 2007 23:57:52
fileModificationTime=09 13 2007 23:57:52
```

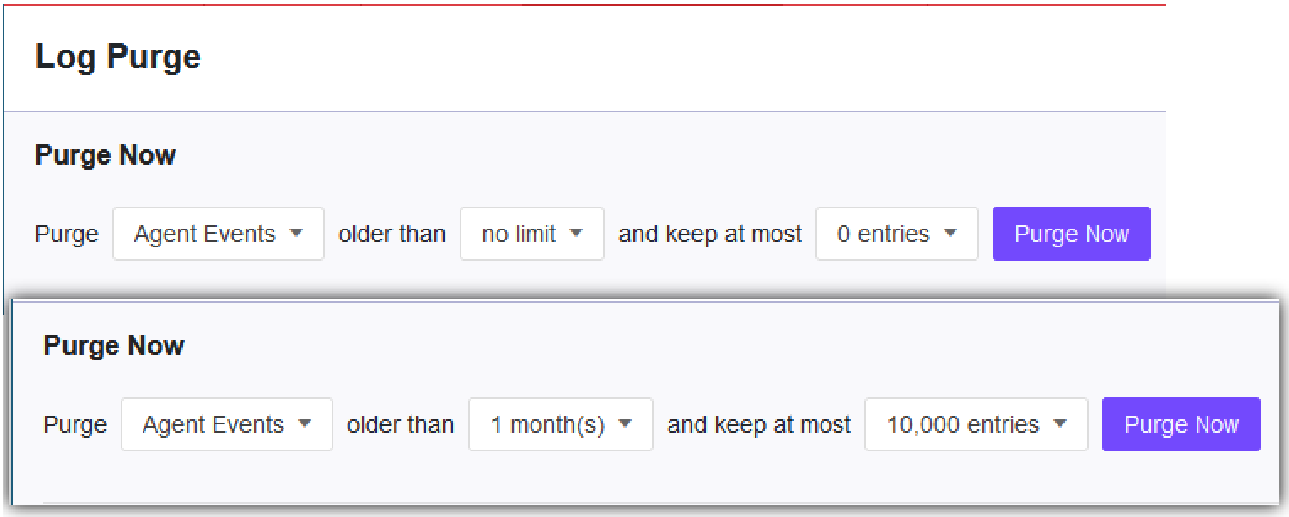
Log Purge Settings

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

Purge Now

Procedure

1. Go to **Administration** > **Log Purge** in the navigation at the top of the web console. The **Log Purge** screen will appear.
2. Specify the Log Type you want to purge below.
   - All Logs
   - System Log, Audit Log, Agent Events, or Server Events
3. Under **older than**, specify the maximum age of event log entries to keep.
   - No limit
   - 1 month(s), 2 months(s), 3 months(s), 6 months(s), 12 months(s), 18 months(s), 24 months(s), 36 months(s), 48 months(s), 60 months(s)
4. Under **Keep at most**, specify the maximum number of event entries to keep.
   - 0 entries
   - 10000 entries, 50000 entries, 100000 entries, 500000 entries, 1000000 entries, 5000000 entries, 10000000 entries
5. Click **Purge Now** button, and the event logs should be purged.



Log Purge

Purge Now

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

Purge Now

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

Automatic Purge

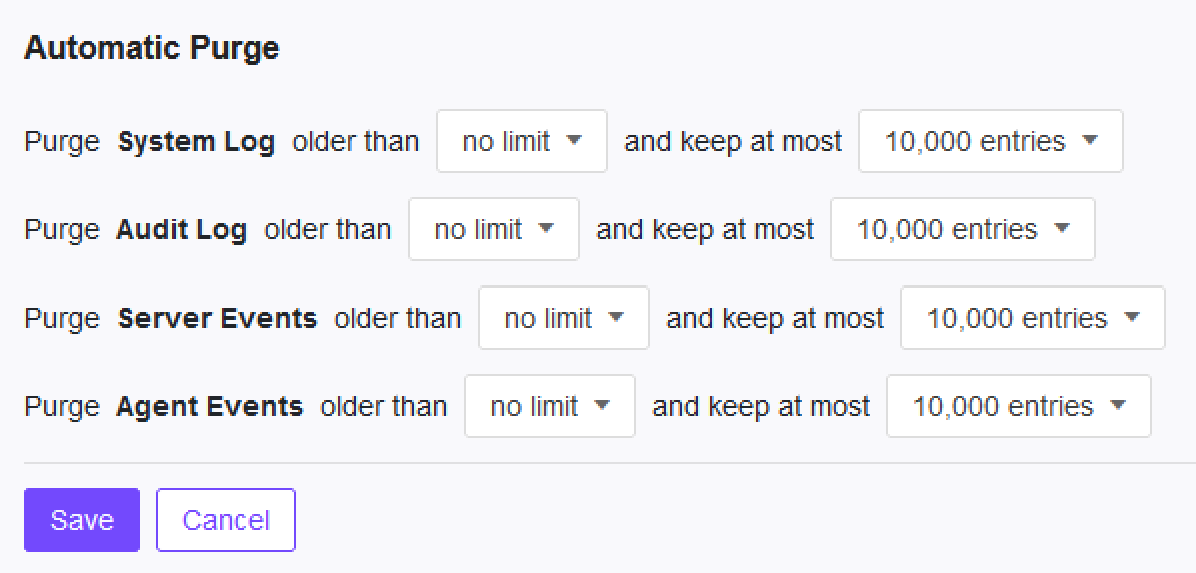
Use these settings to set an automatic purge once per day.

Procedure

1. Go to **Administration** > **Log Purge** in the navigation at the top of the web console. The **Log Purge** screen will appear.
2. Specify the Log Type you want to purge below.
   - System Log

    - Audit Log
    - Agent Events
    - Server Events

3. Under **older than**, specify the maximum age of event log entries to keep.
    - No limit
    - 1 month(s), 2 months(s), 3 months(s), 6 months(s), 12 months(s), 18 months(s), 24 months(s), 36 months(s), 48 months(s), 60 months(s)
4. Under **Keep at most**, specify the maximum number of event entries to keep.
    - 10000 entries
    - 50000 entries
    - 100000 entries
    - 500000 entries
    - 1000000 entries
    - 5000000 entries
    - 10000000 entries
5. Click **Save** button.



Automatic Purge

Purge **System Log** older than no limit and keep at most 10,000 entries

Purge **Audit Log** older than no limit and keep at most 10,000 entries

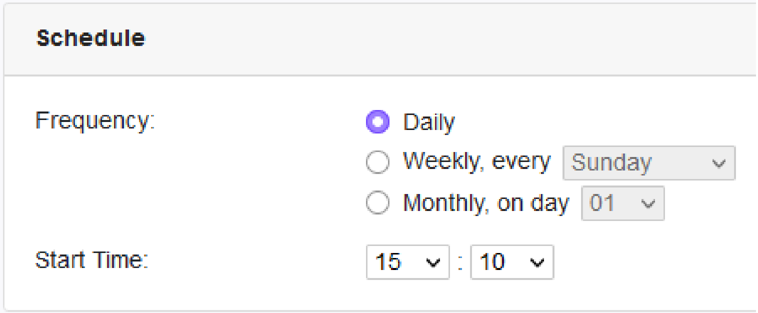
Purge **Server Events** older than no limit and keep at most 10,000 entries

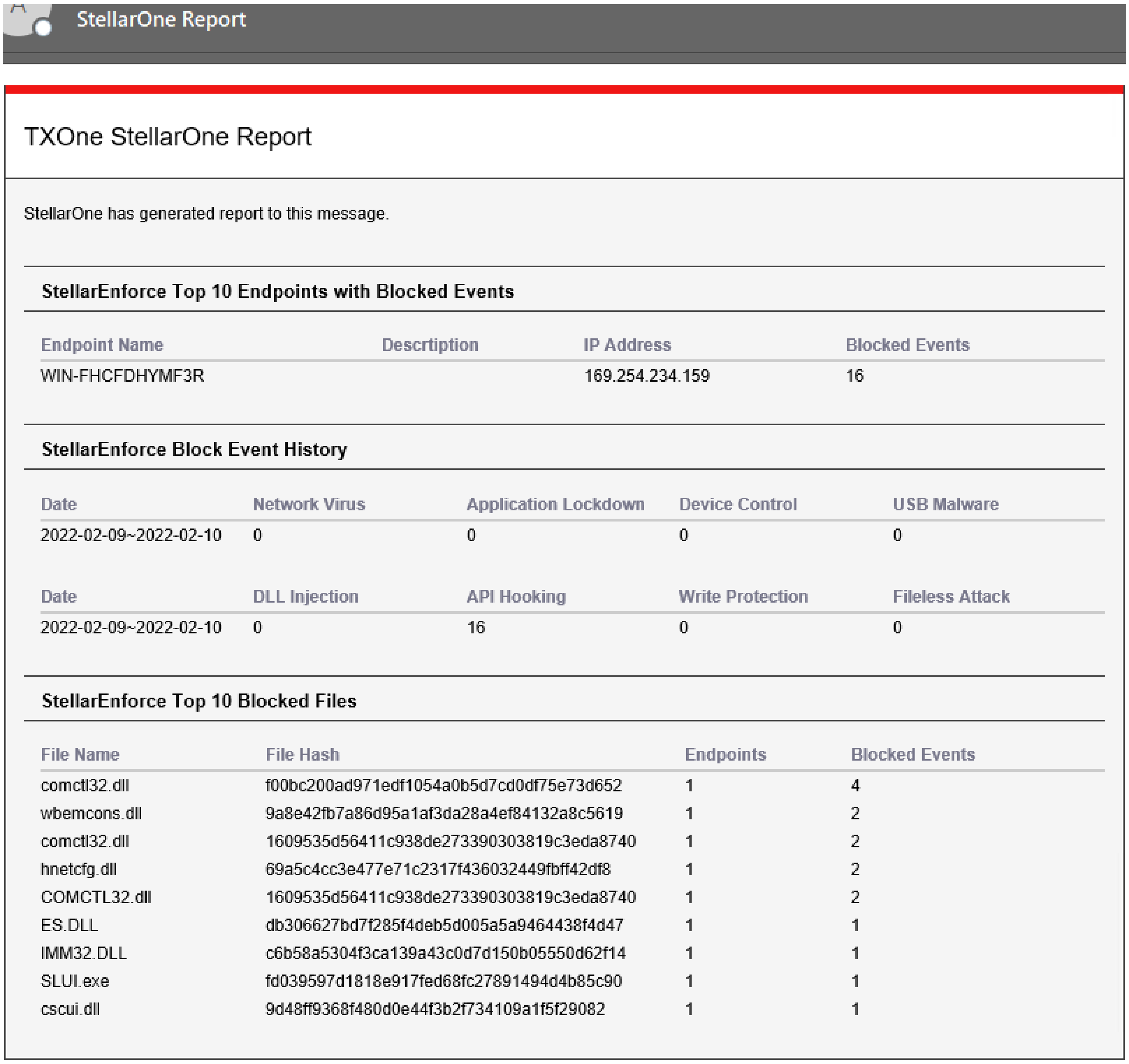
Purge **Agent Events** older than no limit and keep at most 10,000 entries

Scheduled Report Settings

The Scheduled Reports screen, under **Administration** > **Scheduled Report**, provides a list of all reports that automatically generate on a user-defined schedule. You can use this screen to view basic information about previously configured scheduled reports, recipients, as well as enabling and disabling scheduled reports.

The following table outlines the available tasks on the Scheduled Reports screen.

Task	Description
Send Scheduled Reports	Select the **Send scheduled reports** check box to enable scheduled reports. (Default is disabled)
Report Content	Event Type: • StellarEnforce Blocked Event History • StellarEnforce Top 10 Endpoints with Blocked Events • StellarEnforce Top 10 Blocked Files Time Period: • Last 7 days • Last 14 days • Last 30 days • Last 3 months • Last 6 months
Scheduled	Set the frequency and start time for the scheduled reports on a daily, weekly, or monthly basis.  **Schedule** Frequency: ● Daily ○ Weekly, every Sunday ○ Monthly, on day 01 Start Time: 15 : 10 **Note**: Scheduled tasks will be skipped for the months that do not contain the specific day. To carry out the task regularly, we recommend avoiding the 29th, 30th, or 31st.
Recipients	A valid email address is required for specifying the report recipients.



StellarOne Report

TXOne StellarOne Report

StellarOne has generated report to this message.

StellarEnforce Top 10 Endpoints with Blocked Events

Endpoint Name	Descrtiption	IP Address	Blocked Events
WIN-FHCFDHYMF3R		169.254.234.159	16

StellarEnforce Block Event History

Date	Network Virus	Application Lockdown	Device Control	USB Malware
2022-02-09~2022-02-10	0	0	0	0

Date	DLL Injection	API Hooking	Write Protection	Fileless Attack
2022-02-09~2022-02-10	0	16	0	0

StellarEnforce Top 10 Blocked Files

File Name	File Hash	Endpoints	Blocked Events
comctl32.dll	f00bc200ad971edf1054a0b5d7cd0df75e73d652	1	4
wbemcons.dll	9a8e42fb7a86d95a1af3da28a4ef84132a8c5619	1	2
comctl32.dll	1609535d56411c938de273390303819c3eda8740	1	2
hnetcfg.dll	69a5c4cc3e477e71c2317f436032449fbff42df8	1	2
COMCTL32.dll	1609535d56411c938de273390303819c3eda8740	1	2
ES.DLL	db306627bd7f285f4deb5d005a5a9464438f4d47	1	1
IMM32.DLL	c6b58a5304f3ca139a43c0d7d150b05550d62f14	1	1
SLUI.exe	fd039597d1818e917fed68fc27891494d4b85c90	1	1
cscui.dll	9d48ff9368f480d0e44f3b2f734109a1f5f29082	1	1

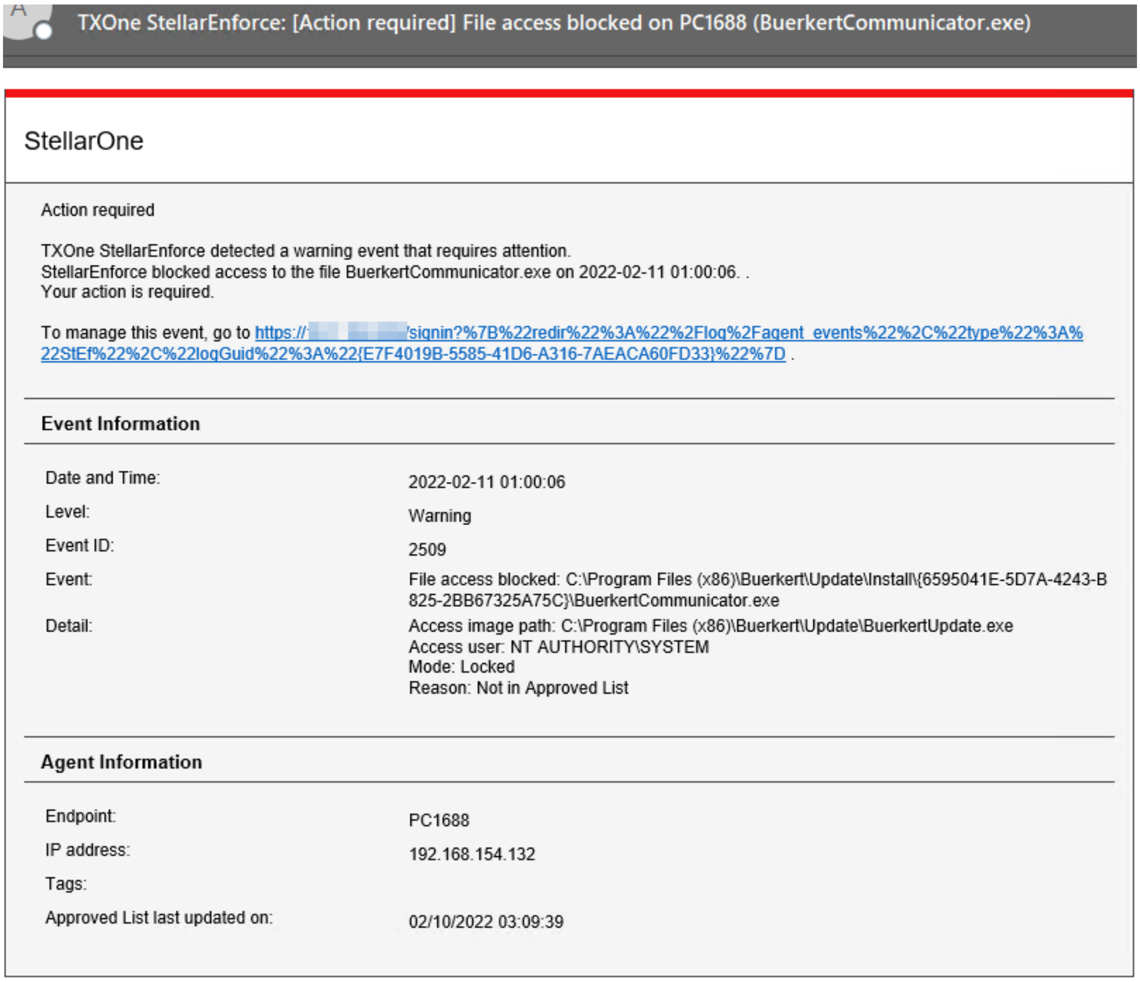
Notification Settings

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

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

Warning Level Agent Events

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



TXOne StellarEnforce: [Action required] File access blocked on PC1688 (BuerkertCommunicator.exe)

StellarOne

Action required

TXOne StellarEnforce detected a warning event that requires attention.
StellarEnforce blocked access to the file BuerkertCommunicator.exe on 2022-02-11 01:00:06. .
Your action is required.

To manage this event, go to https://[redacted]/signin?%7B%22redir%22%3A%22%2Flog%2Fagent_events%22%2C%22type%22%3A%22StEf%22%2C%22logGuid%22%3A%22{E7F4019B-5585-41D6-A316-7AEACA60FD33}%22%7D .

Event Information

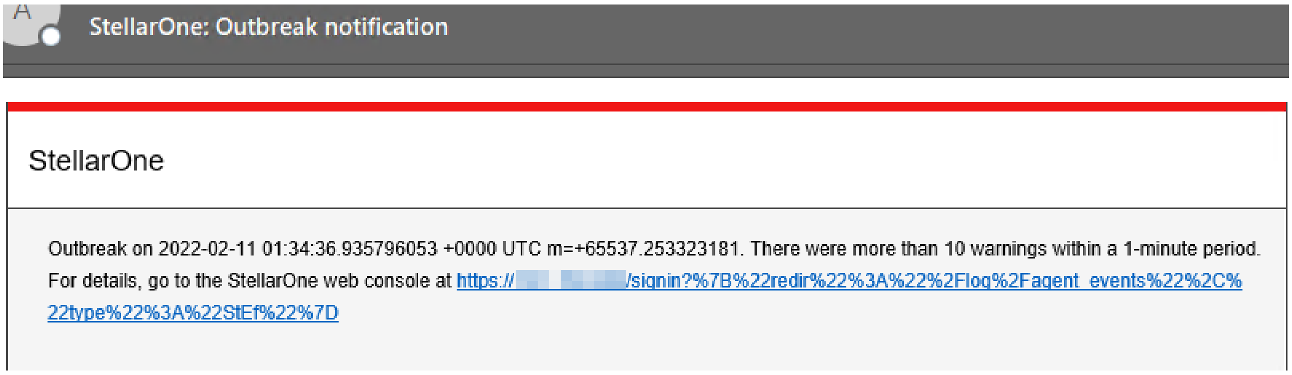
Date and Time:	2022-02-11 01:00:06
Level:	Warning
Event ID:	2509
Event:	File access blocked: C:\Program Files (x86)\Buerkert\Update\Install\{6595041E-5D7A-4243-B825-2BB67325A75C}\BuerkertCommunicator.exe
Detail:	Access image path: C:\Program Files (x86)\Buerkert\Update\BuerkertUpdate.exe Access user: NT AUTHORITY\SYSTEM Mode: Locked Reason: Not in Approved List

Agent Information

Endpoint:	PC1688
IP address:	192.168.154.132
Tags:	
Approved List last updated on:	02/10/2022 03:09:39

Outbreak

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

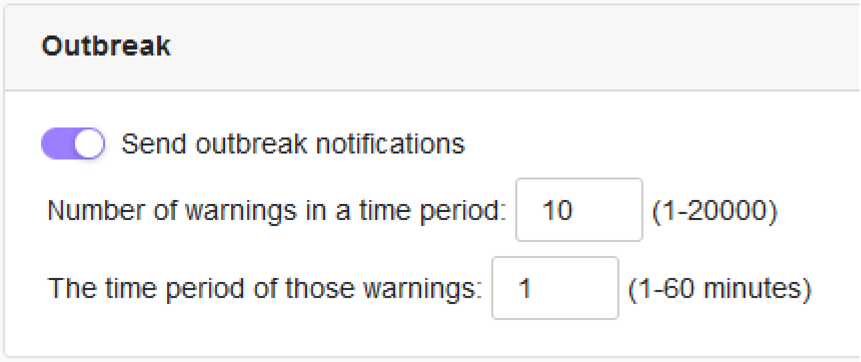


StellarOne: Outbreak notification

StellarOne

Outbreak on 2022-02-11 01:34:36.935796053 +0000 UTC m=+65537.253323181. There were more than 10 warnings within a 1-minute period. For details, go to the StellarOne web console at https://[redacted]/signin?%7B%22redir%22%3A%22%2Flog%2Fagent_events%22%2C%22type%22%3A%22StEf%22%7D

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



Outbreak

Send outbreak notifications

Number of warnings in a time period: 10 (1-20000)

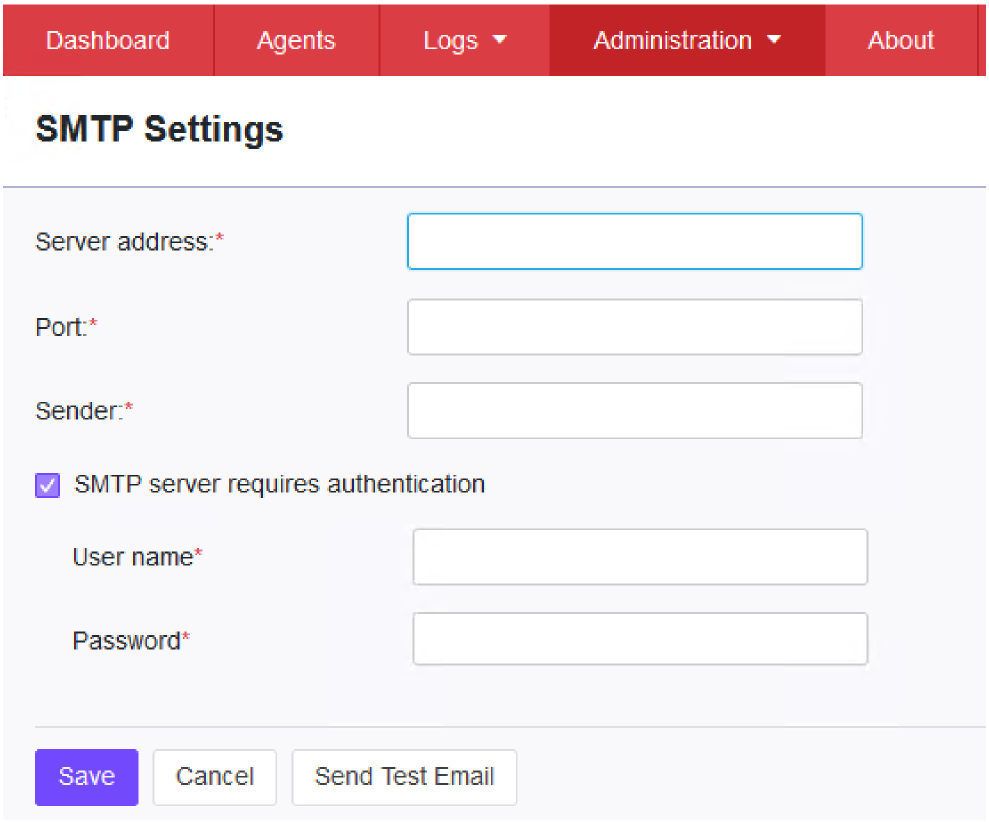
The time period of those warnings: 1 (1-60 minutes)

SMTP Settings

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

Procedure

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



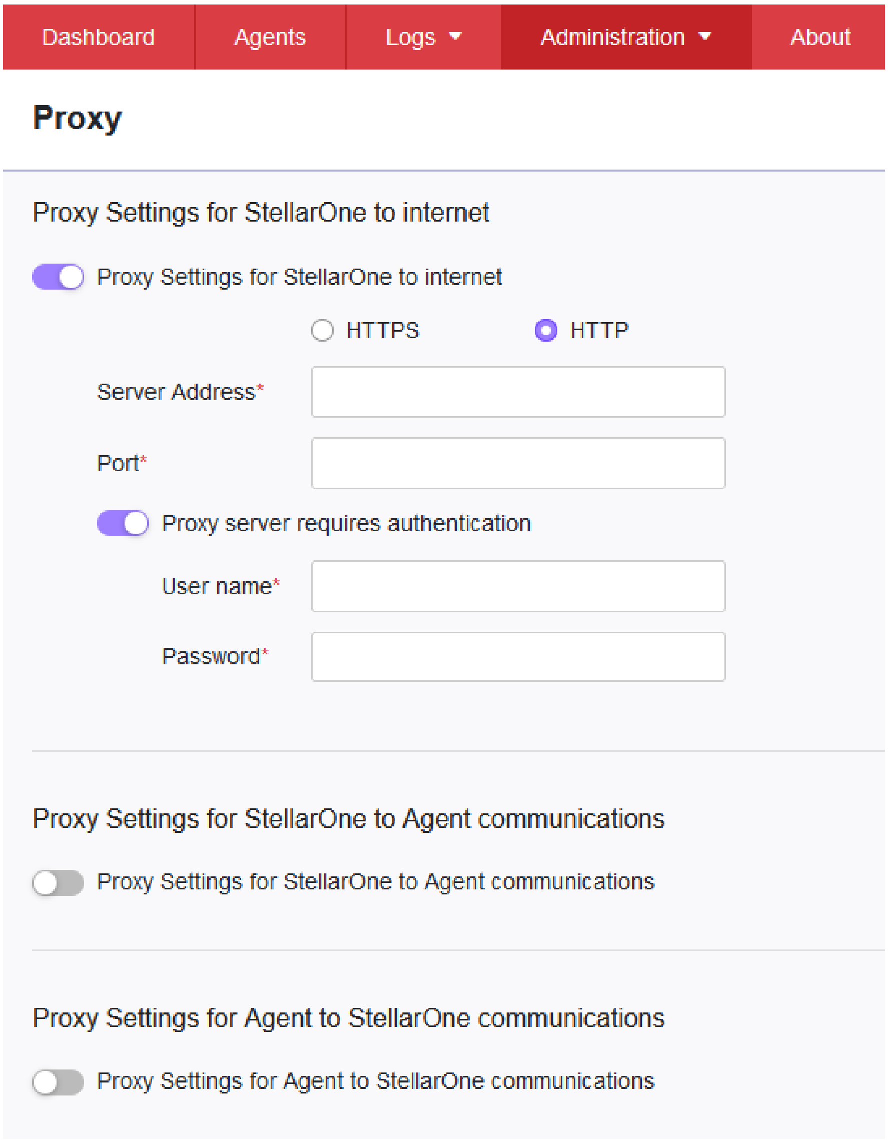
Proxy Settings

There are three proxy settings, Proxy Settings for StellarOne to internet, Proxy settings for StellarOne to Agent communications and Proxy Settings for agent to StellarOne communicates to agents.

Procedure

1. Go to **Administration** > **Proxy** in the navigation at the top of the web console.
2. Specify the Proxy Settings for the following option:
    - Proxy Settings for StellarOne to internet
    - Proxy settings for StellarOne to Agent communications
    - Proxy Settings for agent to StellarOne communicates to agents.
3. To configure proxy settings for updates:

    (1) Select the HTTPS or HTTP protocol.
    Note: For **Proxy Settings for Agent to StellarOne communications**, since currently the StellarEnforce does not support HTTPS proxy, if the destination is an HTTPS server, please use the HTTP proxy for connection.
    (2) Under Server Address, specify the IPv4 address or FQDN of the proxy server.
    (3) Specify the Port.
    (4) If your proxy server requires authentication, select Proxy server authentication and give your credentials.
    (5) Click Save.



Proxy

Proxy Settings for StellarOne to internet

Proxy Settings for StellarOne to internet

○ HTTPS ● HTTP

Server Address*

Port*

Proxy server requires authentication

User name*

Password*

Proxy Settings for StellarOne to Agent communications

Proxy Settings for StellarOne to Agent communications

Proxy Settings for Agent to StellarOne communications

Proxy Settings for Agent to StellarOne communications

Tip: To configure proxy settings used by StellarOne when sending messages to StellarEnforce.

Before installation:
Add the proxy information to the configuration file used by the agent installer package. Save the proxy settings. They will now be included in the agent installer after the agent package is repacked.
After installation:
Use the **SLCmd.exe** Command Line Interface tool on the local StellarEnforce agent administrator guide.

Download / Update Settings

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

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

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

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

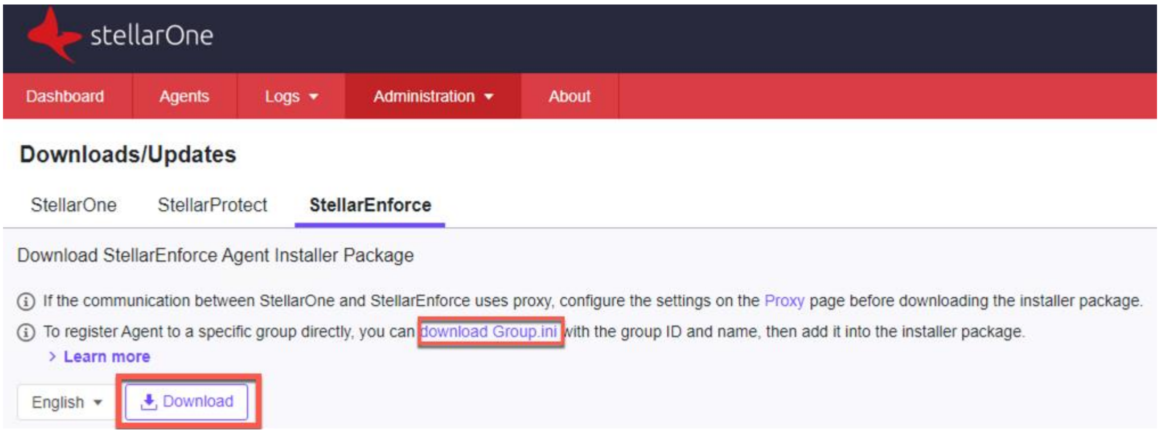
The following table describes the tasks you can perform on this screen under the StellarEnforce tab:

Function	Description
Download StellarEnforce Agent Installer Package	• Download an up-to-date agent installer package. You can also modify the agent component download source and proxy settings, as well as update to the latest components. • Download a Group.ini file and add it into the installer package, which enables directly registering StellarEnforce agent to a specific group via StellarOne console. For more details, see *Group Mapping.*
Patch	Here you can click the Import button to import a patch manually, or Delete to remove a StellarEnforce patch.

Group Mapping

Procedure

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



Downloads/Updates

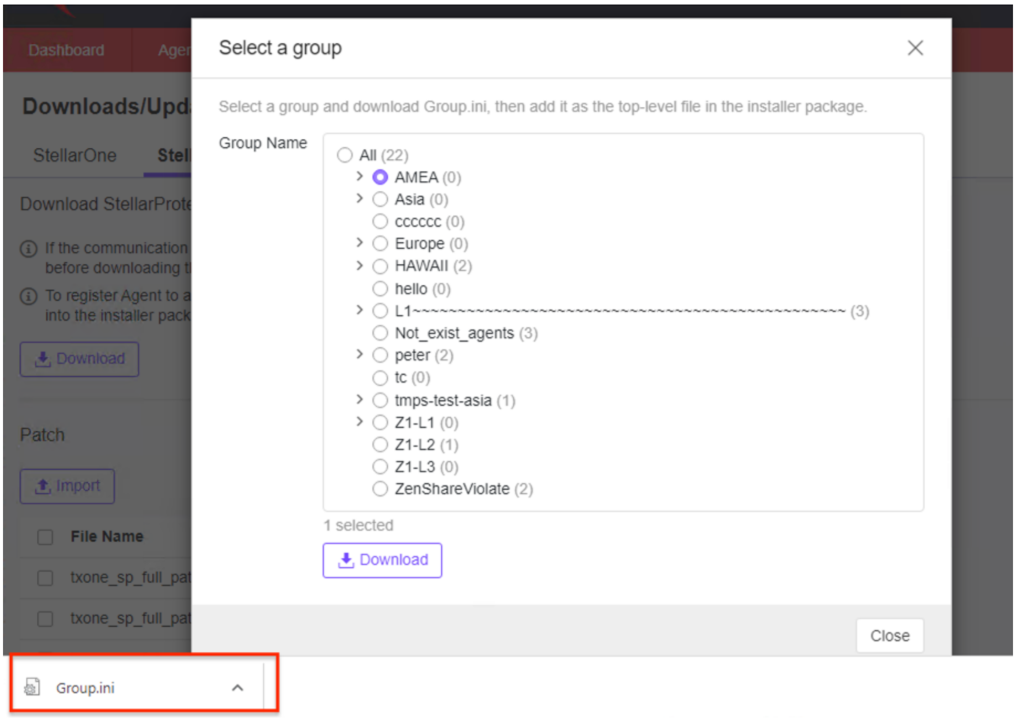
Download StellarEnforce Agent Installer Package

ⓘ If the communication between StellarOne and StellarEnforce uses proxy, configure the settings on the Proxy page before downloading the installer package.

ⓘ To register Agent to a specific group directly, you can download Group.ini with the group ID and name, then add it into the installer package.

› Learn more

4. Select a group for the StellarEnforce agent and click **Download**. A file named **Group.ini** is downloaded. Place the Group.ini file as the top-level file in the agent's installer package.
5. Run the installation on the target agent. Make sure the agent is connected to StellarOne console during the installation process.



Select a group

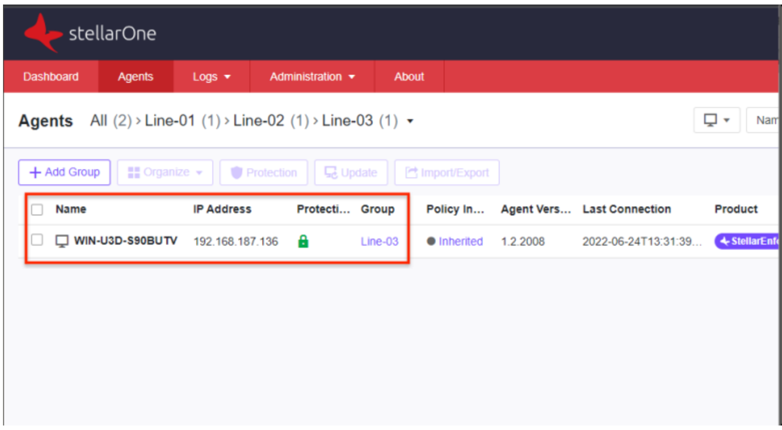
Select a group and download Group.ini, then add it as the top-level file in the installer package.

Group Name

- ○ All (22)
  - ● AMEA (0)
  - ○ Asia (0)
  - ○ cccccc (0)
  - ○ Europe (0)
  - ○ HAWAII (2)
  - ○ hello (0)
  - ○ L1~~~~~~ (3)
  - ○ Not_exist_agents (3)
  - ○ peter (2)
  - ○ tc (0)
  - ○ tmps-test-asia (1)
  - ○ Z1-L1 (0)
  - ○ Z1-L2 (1)
  - ○ Z1-L3 (0)
  - ○ ZenShareViolate (2)

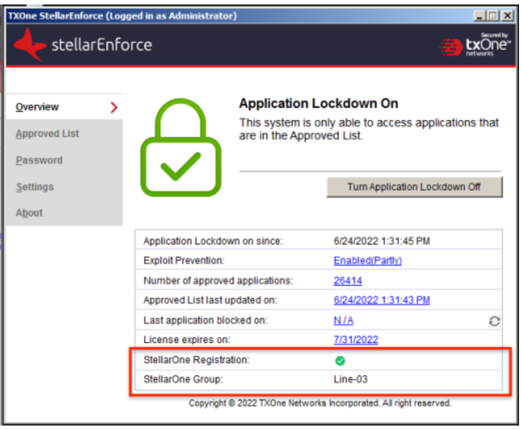
1 selected

6. Users can check the StellarOne management console and the StellarEnforce agent console to see if the agent is successfully registered.



Agents All (2) › Line-01 (1) › Line-02 (1) › Line-03 (1)

	Name	IP Address	Protecti...	Group	Policy In...	Agent Vers...	Last Connection	Product
□	WIN-U3D-S90BUTV	192.168.187.136	🔒	Line-03	● Inherited	1.2.2008	2022-06-24T13:31:39...	StellarEnf


TXOne StellarEnforce (Logged in as Administrator)
stellarEnforce
Secured by txOne networks
Overview
Approved List
Password
Settings
About
Turn Application Lockdown Off

Application Lockdown On

This system is only able to access applications that are in the Approved List.

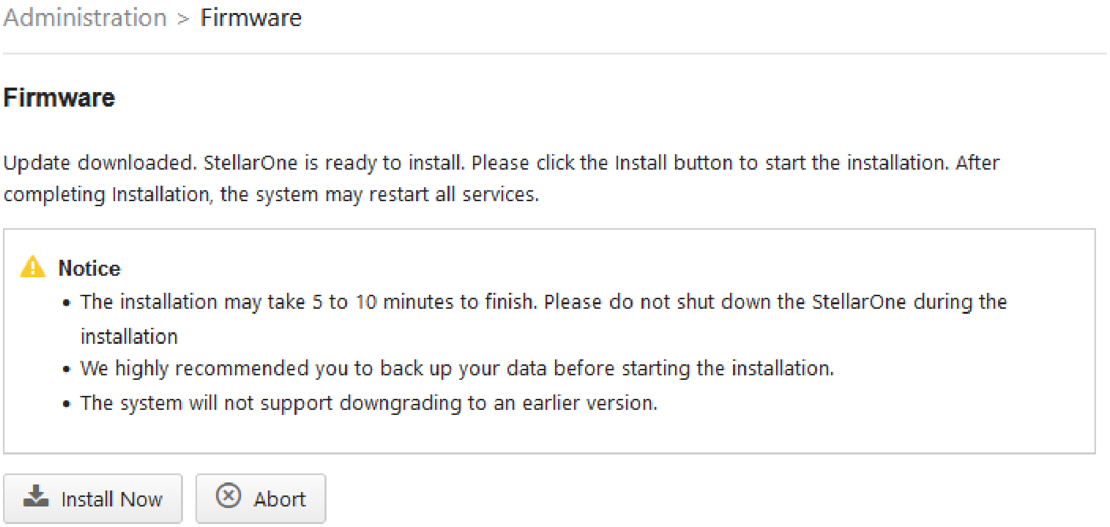
Application Lockdown on since:	6/24/2022 1:31:45 PM
Exploit Prevention:	Enabled(Partly)
Number of approved applications:	26414
Approved List last updated on:	6/24/2022 1:31:43 PM
Last application blocked on:	N/A
License expires on:	7/31/2022
StellarOne Registration:	✓
StellarOne Group:	Line-03

Copyright © 2022 TXOne Networks Incorporated. All right reserved.

Firmware

Procedure

7. Go to **Administration** > **Firmware** in the navigation at the top of the web console.
8. Click **Import** to specify the firmware patch file (E.g. acus.fw_2.0.1137.acf).
   - Version shows the current StellarOne build version.
   - Release Date and Description show the current information for StellarOne patch fire.
9. When the Firmware Update window pops up, click **Apply** to apply the patch to StellarOne.
10. Confirm the notification description.
11. Click **Install Now** to implement the update or Abort to stop updating.



Firmware

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

⚠ Notice

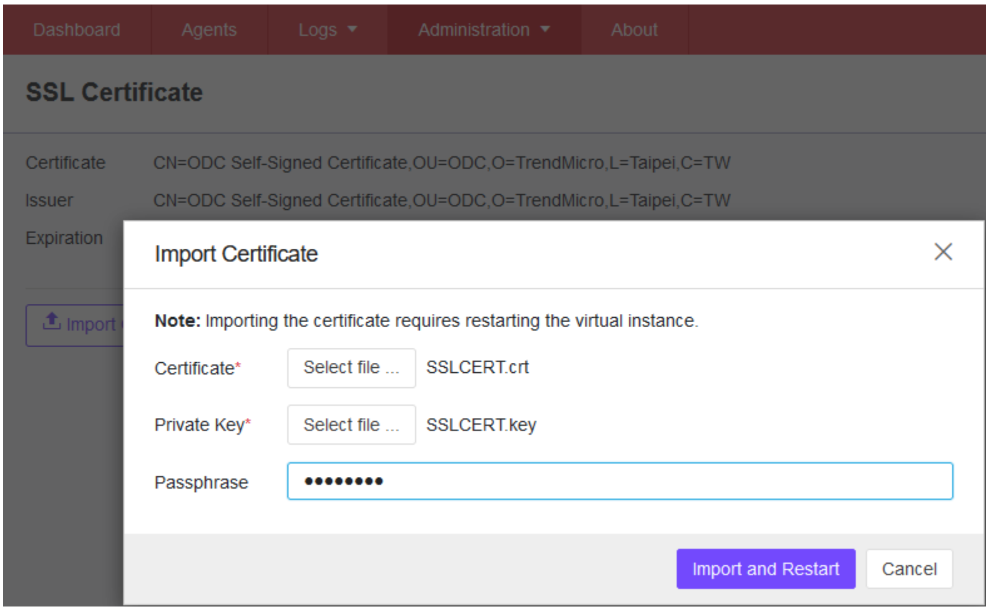
- The installation may take 5 to 10 minutes to finish. Please do not shut down the StellarOne during the installation
- We highly recommended you to back up your data before starting the installation.
- The system will not support downgrading to an earlier version.

SSL Certification

Procedure

1. Go to **Administration** > **SSL Certification** in the navigation at the top of the web console.
2. Select the desired **Import Certificate**.
3. Importing the certificate requires restarting the virtual instance.

   (1) Use the 'Select file…' dropdown next to Certificate to select the desired certificate to import.
   (2) Use the 'Select file…' dropdown next to Private Key to select the desired Private Key.
   (3) Specify the Passphrase. (Optional)



SSL Certificate

Certificate CN=ODC Self-Signed Certificate,OU=ODC,O=TrendMicro,L=Taipei,C=TW

Issuer CN=ODC Self-Signed Certificate,OU=ODC,O=TrendMicro,L=Taipei,C=TW

Expiration

Import Certificate

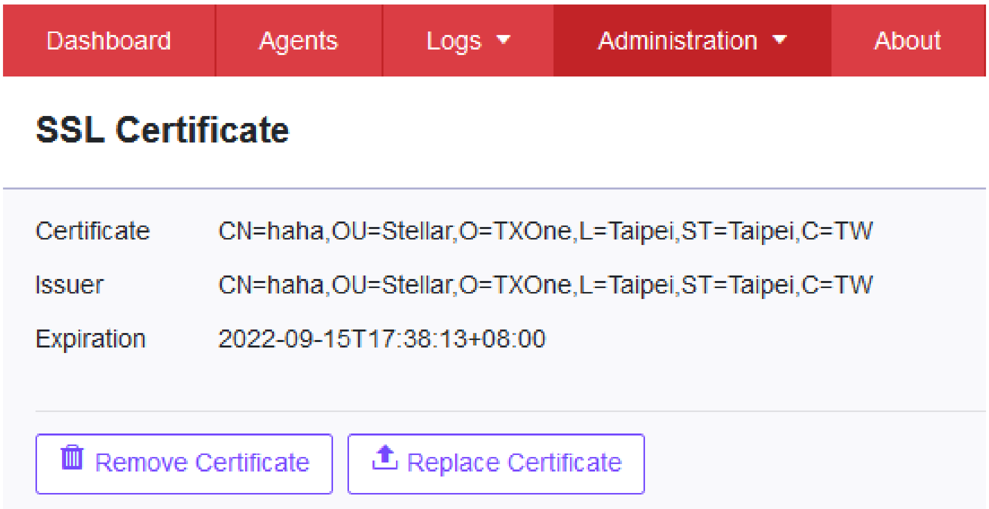
Note: Importing the certificate requires restarting the virtual instance.

Certificate* SSLCERT.crt

Private Key* SSLCERT.key

Passphrase ••••••••

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



SSL Certificate

Certificate CN=haha,OU=Stellar,O=TXOne,L=Taipei,ST=Taipei,C=TW

Issuer CN=haha,OU=Stellar,O=TXOne,L=Taipei,ST=Taipei,C=TW

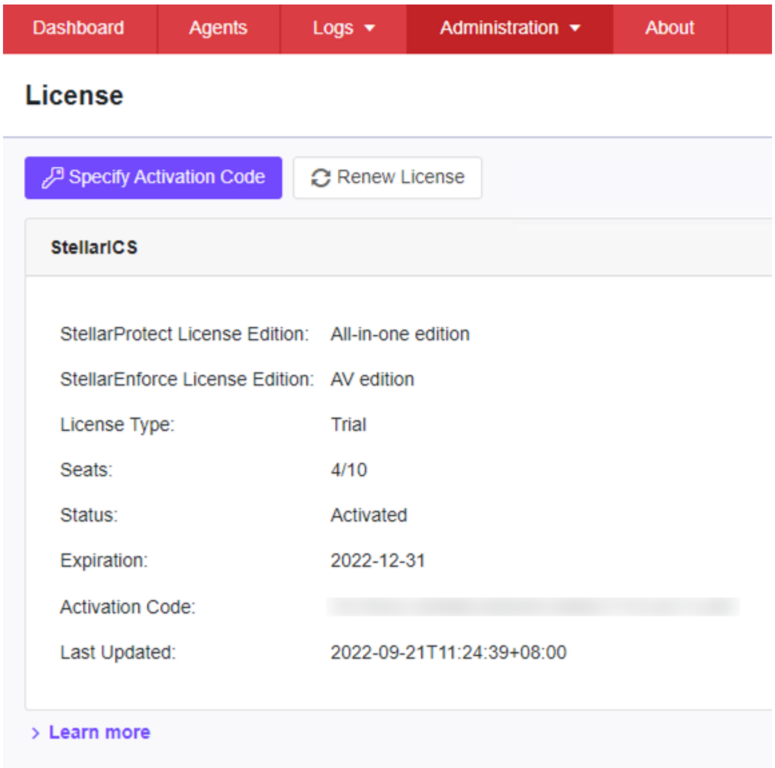
Expiration 2022-09-15T17:38:13+08:00

License Management

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

Item	Description
License Edition	Displays current license edition for StellarEnforce and/or StellarProtect.
License Type	Full: a full version that is officially authorized. Trial: a trial version with excluded features or limited functions. Perpetual: provides permanent use and 5-year technical support.
Seats	Specifies current number of agents registered to StellarOne and the total number of agents that can be registered to StellarOne.
Status	Activated: The existing license is effective. Expired: The existing license is out of date. Note: It is recommended to renew license promptly in order to protect your devices from virus threat.
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
Learn More	Click the link to go to the online help web page for more license details.

Changing Activation Code



License

StellarICS

StellarProtect License Edition:	All-in-one edition
StellarEnforce License Edition:	AV edition
License Type:	Trial
Seats:	4/10
Status:	Activated
Expiration:	2022-12-31
Activation Code:	[redacted]
Last Updated:	2022-09-21T11:24:39+08:00

Procedure

1. Go to **Administration** > **License** in the navigation at the top of the web console. The License Management screen will appear.
2. Click **Specify Activation Code** button.
3. Input the target new Activation Code to renew for StellarOne console.

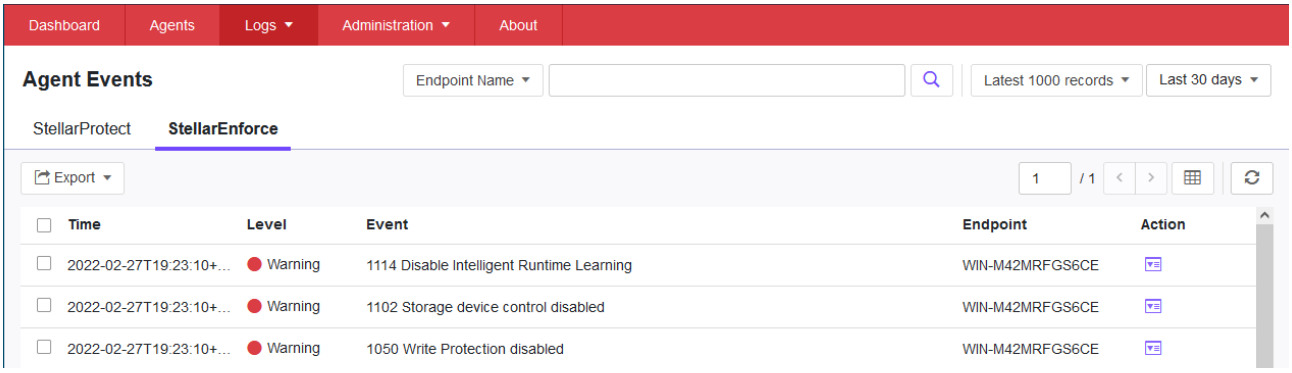
Note: Click **Renew License** button to update your product license. The connection with the TXOne Product License server is required.

Chapter 8 - Log Description Reference

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

- StellarEnforce Agent Event Log Descriptions
- StellarEnforce Agent Error Code Descriptions
- StellarOne Server Event Log Descriptions

Agent Event Log Descriptions



	Time	Level	Event	Endpoint	Action
□	2022-02-27T19:23:10+...	● Warning	1114 Disable Intelligent Runtime Learning	WIN-M42MRFGS6CE	
□	2022-02-27T19:23:10+...	● Warning	1102 Storage device control disabled	WIN-M42MRFGS6CE	
□	2022-02-27T19:23:10+...	● Warning	1050 Write Protection disabled	WIN-M42MRFGS6CE	

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
1000	System	Information	Service started.
1001	System	Warning	Service stopped.
1002	System	Information	Application Lockdown Turned On.
1003	System	Warning	Application Lockdown Turned Off.
1004	System	Information	Disabled.
1005	System	Information	Administrator password changed.
1006	System	Information	Restricted User password changed.
1007	System	Information	Restricted User account enabled.
1008	System	Information	Restricted User account disabled.
1009	System	Information	Product activated.
1010	System	Information	Product deactivated.
1011	System	Warning	License Expired. Grace period enabled.
1012	System	Warning	License Expired. Grace period ended.

1013	System	Information	Product configuration import started: %path%
1014	System	Information	Product configuration import complete: %path%
1015	System	Information	Product configuration exported to: %path%
1016	System	Information	USB Malware Protection set to Allow.
1017	System	Information	USB Malware Protection set to Block.
1018	System	Information	USB Malware Protection enabled.
1019	System	Warning	USB Malware Protection disabled.
1020	System	Information	Network Virus Protection set to Allow.
1021	System	Information	Network Virus Protection set to Block.
1022	System	Information	Network Virus Protection enabled.
1023	System	Warning	Network Virus Protection disabled.
1025	System	Information	Memory Randomization enabled.
1026	System	Warning	Memory Randomization disabled.
1027	System	Information	API Hooking Prevention set to Allow.
1028	System	Information	API Hooking Prevention set to Block.
1029	System	Information	API Hooking Prevention enabled.
1030	System	Warning	API Hooking Prevention disabled.
1031	System	Information	DLL Injection Prevention set to Allow.
1032	System	Information	DLL Injection Prevention set to Block.
1033	System	Information	DLL Injection Prevention enabled.
1034	System	Warning	DLL Injection Prevention disabled.
1035	System	Information	Pre-defined Trusted Update enabled.
1036	System	Information	Pre-defined Trusted Update disabled.
1037	System	Information	DLL/Driver Lockdown enabled.
1038	System	Warning	DLL/Driver Lockdown disabled.
1039	System	Information	Script Lockdown enabled.
1040	System	Warning	Script Lockdown disabled.
1041	System	Information	Script added. [Details] File extension: %extension% Interpreter: %interpreter%

1042	System	Information	Script removed. [Details] File extension: %extension% Interpreter: %interpreter%
1044	System	Information	Exception path enabled.
1045	System	Information	Exception path disabled.
1047	System	Information	Trusted certification enabled.
1048	System	Information	Trusted certification disabled.
1049	System	Information	Write Protection enabled.
1050	System	Warning	Write Protection disabled.
1051	System	Information	Write Protection set to Allow.
1052	System	Information	Write Protection set to Block.
1055	System	Information	Added file to Write Protection List. Path: %path%
1056	System	Information	Removed file from Write Protection List. Path: %path%
1057	System	Information	Added file to Write Protection Exception List. Path: %path% Process: %process%
1058	System	Information	Removed file from Write Protection Exception List. Path: %path% Process: %process%
1059	System	Information	Added folder to Write Protection List. Path: %path% Scope: %scope%
1060	System	Information	Removed folder from Write Protection List. Path: %path% Scope: %scope%
1061	System	Information	Added folder to Write Protection Exception List. Path: %path% Scope: %scope% Process: %process%
1062	System	Information	Removed folder from Write Protection Exception List. Path: %path% Scope: %scope% Process: %process%
1063	System	Information	Added registry value to Write Protection List. Registry Key: %regkey% Registry Value Name: %regvalue%
1064	System	Information	Removed registry value from Write Protection List. Registry Key: %regkey% Registry Value Name: %regvalue%
1065	System	Information	Added registry value to Write Protection Exception List. Registry Key: %regkey% Registry Value Name: %regvalue% Process: %process%

1066	System	Information	Removed registry value from Write Protection Exception List. Registry Key: %regkey% Registry Value Name: %regvalue% Process: %process%
1067	System	Information	Added registry key to Write Protection List. Path: %regkey% Scope: %scope%
1068	System	Information	Removed registry key from Write Protection List. Path: %regkey% Scope: %scope%
1069	System	Information	Added registry key to Write Protection Exception List. Path: %regkey% Scope: %scope% Process: %process%
1070	System	Information	Removed registry key from Write Protection Exception List. Path: %regkey% Scope: %scope% Process: %process%
1071	System	Information	Custom Action set to Ignore.
1072	System	Information	Custom Action set to Quarantine.
1073	System	Information	Custom Action set to Ask Intelligent Manager
1074	System	Information	Quarantined file is restored. [Details] Original Location: %path% Source: %source%
1075	System	Information	Quarantined file is deleted. [Details] Original Location: %path% Source: %source%
1076	System	Information	Integrity Monitoring enabled.
1077	System	Information	Integrity Monitoring disabled.
1078	System	Information	Root cause analysis report unsuccessful. [Details] Access Image Path: %path%
1079	System	Information	Server certification imported: %path%
1080	System	Information	Server certification exported to: %path%
1081	System	Information	Managed mode configuration imported: %path%
1082	System	Information	Managed mode configuration exported to: %path%
1083	System	Information	Managed mode enabled.
1084	System	Information	Managed mode disabled.
1085	System	Information	Protection applied to Write Protection List and Approved List while Write Protection is enabled
1086	System	Warning	Protection applied to Write Protection List while Write Protection is enabled.

1088	System	Information	Windows Update Support enabled.
1089	System	Information	Windows Update Support disabled.
1094	System	Information	TXOne StellarEnforce updated. File applied: %file_name%
1096	System	Information	Trusted Hash List enabled.
1097	System	Information	Trusted Hash List disabled.
1099	System	Information	Storage device access set to Allow
1100	System	Information	Storage device access set to Block
1101	System	Information	Storage device control enabled
1102	System	Warning	Storage device control disabled
1103	System	Information	Event Log settings changed. [Details] Windows Event Log: %ON|off% Level: Warning Log: %ON|off% Information Log: %ON|off% System Log: %ON|off% Exception Path Log: %ON|off% Write Protection Log: %ON|off% List Log: %ON|off% Approved Access Log: DllDriver Log: %ON|off% Trusted Updater Log: %ON|off% Exception Path Log: %ON|off% Trusted Certification Log: %ON|off% Trusted Hash Log: %ON|off% Write Protection Log: %ON|off% Blocked Access Log: %ON|off% USB Malware Protection Log: %ON|off% Execution Prevention Log: %ON|off% Network Virus Protection Log: %ON|off%
			Integrity Monitoring Log File Created Log: %ON|off% File Modified Log: %ON|off% File Deleted Log: %ON|off% File Renamed Log: %ON|off% RegValue Modified Log: %ON|off% RegValue Deleted Log: %ON|off% RegKey Created Log: %ON|off% RegKey Deleted Log: %ON|off% RegKey Renamed Log: %ON|off% Device Control Log: %ON|off% Debug Log: %ON|off%
1104	System	Warning	Memory Randomization is not available in this version of Windows.
1105	System	Information	Blocked File Notification enabled.
1106	System	Information	Blocked File Notification disabled.
1107	System	Information	Administrator password changed remotely.
1111	System	Information	Fileless Attack Prevention enabled.

1112	System	Warning	Fileless Attack Prevention disabled.
1500	List	Information	Trusted Update started.
1501	List	Information	Trusted Update stopped.
1502	List	Information	Approved List import started: %path%
1503	List	Information	Approved List import complete: %path%
1504	List	Information	Approved List exported to: %path%
1505	List	Information	Added to Approved List: %path%
1506	List	Information	Added to Trusted Updater List: %path%
1507	List	Information	Removed from Approved List: %path%
1508	List	Information	Removed from Trusted Updater List: %path%
1509	List	Information	Approved List updated: %path%
1510	List	Information	Trusted Updater List updated: %path%
1511	List	Warning	Unable to add to or update Approved List: %path%
1512	List	Warning	Unable to add to or update Trusted Updater List: %path%
1513	System	Information	Added to Exception Path List. [Details] Type: %exceptionpathtype% Path: %exceptionpath%
1514	System	Information	Removed from Exception Path List. [Details] Type: %exceptionpathtype% Path: %exceptionpath%
1515	System	Information	Added to Trusted Certification List. [Details] Label: %label% Hash: %hashvalue% Type: %type% Subject: %subject% Issuer: %issuer%
1516	System	Information	Removed from Trusted Certification List. [Details] Label: %label% Hash: %hashvalue% Type: %type% Subject: %subject% Issuer: %issuer%
1517	System	Information	Added to the Trusted Hash List.%n [Details] Label : %label% Hash : %hashvalue% Type : %type% Add to Approved List: %yes|no% Path : %path% Note: %note%

1518	System	Information	Removed from the Trusted Hash List.%n [Details] Label : %label% Hash : %hashvalue% Type : %type% Add to Approved List: %yes|no% Path : %path% Note: %note%
1519	List	Information	Removed from Approved List remotely: %path%
1520	List	Warning	Unable to create Approved List because an unexpected error occurred during enumeration of the files in %1 %n Error Code: %2 %n
1521	System	Information	Added Fileless Attack Prevention exception. [Details] Label : %label% Target Process: %process_name% Arguments: %arguments% %regex_flag% Parent Process 1 Image Path: %path% Parent Process 2 Image Path: %path% Parent Process 3 Image Path: %path% Parent Process 4 Image Path: %path%
1522	System	Information	Removed Fileless Attack Prevention exception. [Details] Label : %label% Target Process: %process_name% Arguments: %arguments% %regex_flag% Parent Process 1 Image Path: %path% Parent Process 2 Image Path: %path% Parent Process 3 Image Path: %path% Parent Process 4 Image Path: %path%
1523	System	Information	Maintenance Mode started
1524	System	Information	Leaving Maintenance Mode
1525	System	Information	Maintenance Mode stopped
1526	List	Information	Added to Approved List in Maintenance Mode. Path: %1 Hash: %2
1527	List	Information	Approved List updated in Maintenance Mode. Path: %1 Hash: %2
2000	Access Approved	Information	File access allowed: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode% List: %list%
2001	Access Approved	Warning	File access allowed: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%

			File Hash allowed: %hash%
2002	Access Approved	Warning	File access allowed: %path% Unable to get the file path while checking the Approved List. [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2003	Access Approved	Warning	File access allowed: %path% Unable to calculate hash while checking the Approved List. [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2004	Access Approved	Warning	File access allowed: %path% Unable to get notifications to monitor process.
2005	Access Approved	Warning	File access allowed: %path% Unable to add process to non exception list.
2006	Access Approved	Information	File access allowed: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2007	Access Approved	Warning	File access allowed: %path% An error occurred while checking the Exception Path List. [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2008	Access Approved	Warning	File access allowed: %path% An error occurred while checking the Trusted Certification List. [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2011	Access Approved	Information	Registry access allowed. Registry Key: %regkey% Registry Value Name: %regvalue% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2012	Access Approved	Information	Registry access allowed. Registry Key: %regkey% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2013	Access Approved	Information	Change of File/Folder allowed by Exception List: %path% [Details] Access Image Path: Access User: %username% Mode: %mode%

2015	Access Approved	Information	Change of Registry Value allowed by Exception List. Registry Key: %regkey% Registry Value Name: %regvalue% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2016	Access Approved	Information	Change of Registry Key allowed by Exception List. Registry Key: %regkey% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2017	Access Approved	Warning	Change of File/Folder allowed: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2019	Access Approved	Warning	Change of Registry Value allowed. Registry Key: %regkey% Registry Value Name: %regvalue% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2020	Access Approved	Warning	Change of Registry Key allowed. Registry Key: %regkey% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2021	Access Approved	Warning	File access allowed: %path% An error occurred while checking the Trusted Hash List. [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2022	Access Approved	Warning	Process allowed by Fileless Attack Prevention: %path% %argument% [Details] Access User: %username% Parent Process 1 Image Path: %path% Parent Process 2 Image Path: %path% Parent Process 3 Image Path: %path% Parent Process 4 Image Path: %path% Mode: Unlocked Reason: %reason%
2503	Access Blocked	Warning	Change of File/Folder blocked: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%

2505	Access Blocked	Warning	Change of Registry Value blocked. Registry Key: %regkey% Registry Value Name: %regvalue% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2506	Access Blocked	Warning	Change of Registry Key blocked. Registry Key: %regkey% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2507	Access Blocked	Information	Action completed successfully: %path% [Details] Action: %action% Source: %source%
2508	Access Blocked	Warning	Unable to take specified action: %path% [Details] Action: %action% Source: %source%
2509	Access Blocked	Warning	File access blocked: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode% Reason: Not in Approved List File Hash blocked: %hash%
2510	Access Blocked	Warning	File access blocked: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode% Reason: Hash does not match expected value File Hash blocked: %hash%
2511	Access Blocked	Information	Change of File/Folder blocked: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2512	Access Blocked	Warning	Change of Registry Value blocked. Registry Key: %regkey% Registry Value Name: %regvalue% [Details] Access Image Path: %path% Access User: %username% Note Enabling the Service Creation Prevention feature triggers Event ID 2512.

2513	Access Blocked	Warning	Process blocked by Fileless Attack Prevention: %path% %argument% [Details] Access User: %username% Parent Process 1 Image Path: %path% Parent Process 2 Image Path: %path% Parent Process 3 Image Path: %path% Parent Process 4 Image Path: %path% Mode: locked Reason: %reason%
2514	Access Blocked	Warning	File access blocked: %BLOCKED_FILE_PATH% [Details] Access Image Path: %PARENT_PROCESS_PATH% Access User: %USER_NAME% Reason: Blocked file is in a folder that has the case sensitive attribute enabled.
3000	USB Malware Protection	Warning	Device access allowed: %path% [Details] Access Image Path: %path% Access User: %username% Device Type: %type%
3001	USB Malware Protection	Warning	Device access blocked: %path% [Details] Access Image Path: %path% Access User: %username% Device Type: %type%
3500	Network Virus Protection	Warning	Network virus allowed: %name% [Details] Protocol: TCP Source IP Address: %ip_address% Source Port: %port% Destination IP Address: %ip_address% Destination Port: 80
3501	Network Virus Protection	Warning	Network virus blocked: %name% [Details] Protocol: TCP Source IP Address: %ip_address% Source Port: %port% Destination IP Address: %ip_address% Destination Port: 80
4000	Process Protection Event	Warning	API Hooking/DLL Injection allowed: %path% [Details] Threat Image Path: %path% Threat User: %username%
4001	Process Protection Event	Warning	API Hooking/DLL Injection blocked: %path% [Details] Threat Image Path: %path% Threat User: %username%

4002	Process Protection Event	Warning	API Hooking allowed: %path% [Details] Threat Image Path: %path% Threat User: %username%
4003	Process Protection Event	Warning	API Hooking blocked: %path% [Details] Threat Image Path: %path% Threat User: %username%
4004	Process Protection Event	Warning	DLL Injection allowed: %path% [Details] Threat Image Path: %path% Threat User: %username%
4005	Process Protection Event	Warning	DLL Injection blocked: %path% [Details] Threat Image Path: %path% Threat User: %username%
4500	Changes in System	Information	File/Folder created: %path% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4501	Changes in System	Information	File modified: %path% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4502	Changes in System	Information	File/Folder deleted: %path% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4503	Changes in System	Information	File/Folder renamed: %path% New Path: %path% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4504	Changes in System	Information	Registry Value modified. Registry Key: %regkey% Registry Value Name: %regvalue% Registry Value Type: %regvaluetype% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4505	Changes in System	Information	Registry Value deleted. Registry Key: %regkey% Registry Value Name: %regvalue% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%

4506	Changes in System	Information	Registry Key created. Registry Key: %regkey% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4507	Changes in System	Information	Registry Key deleted. Registry Key: %regkey% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4508	Changes in System	Information	Registry Key renamed. Registry Key: %regkey% New Registry Key: %regkey% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
5000	Device Control	Warning	Storage device access allowed: %PATH% [Details] Access Image path: %PATH% Access User: %USERNAME% Device Type: %TYPE% %DEVICEINFO%
5001	Device Control	Warning	Storage device access blocked: %PATH% [Details] Access Image path: %PATH% Access User: %USERNAME% Device Type: %TYPE% %DEVICEINFO%
6000	System	Information	%Result% [Details] Update Source: %SERVER% [Original Version] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION% [Updated Version] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION%

			Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
6001	System	Warning	Update failed: %ERROR_MSG% (%ERROR_CODE%) [Details] Update Source: %SERVER% [Original Version] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION% [Updated Version] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
6002	System	Information	Malware scan started: %SCAN_TYPE% [Details] Files to scan: %SCAN_FOLDER_TYPE% Scanned folders: %PATHS% Excluded paths: %PATHS% Excluded files: %PATHS% Excluded extensions: %PATHS% [Components] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%

6003	System	Information	Malware scan completed: %SCAN_TYPE%. Number of infected files: %NUM% [Details] Files to scan: %SCAN_FOLDER_TYPE% Scanned folders: %PATHS% Excluded paths: %PATHS% Excluded files: %PATHS% Excluded extensions: %PATHS% Start date/time: %DATE_TIME% End date/time: %DATE_TIME% Number of scanned files: %NUM% Number of infected files: %NUM% Number of cleaned files: %NUM% Number of files cleaned after reboot: %NUM% [Components] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
6004	System	Warning	Malware scan unsuccessful: %SCAN_TYPE% %ERROR% [Details] Files to scan: %SCAN_FOLDER_TYPE% Scanned folders: %PATHS% Excluded paths: %PATHS% Excluded files: %PATHS% Excluded extensions: %PATHS% Start date/time: %DATE_TIME% End date/time: %DATE_TIME% Number of scanned files: %NUM% Number of infected files: %NUM% Number of cleaned files: %NUM% Number of files cleaned after reboot: %NUM% [Components] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%

6005	System	Information	Malware detected: %ACTION% File path: %PATH% [Details] Reboot required: %NEED_REBOOT% [Scan Result] Threat type: %TYPE% Threat name: %NAME% [Components] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
6006	System	Warning	Malware detected. Unable to perform scan actions: %PATH% [Details] First action: %1ST_ACTION% Second action: %2ND_ACTION% Threat type: %TYPE% Threat name: %NAME% [Components] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
6007	Maintenance Mode	Warning	Malware detected in Maintenance Mode (file quarantine successful): %PATH% [Details] Component versions: Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%

6008	Maintenance Mode	Warning	Malware detected in Maintenance Mode (file quarantine unsuccessful): %PATH% [Details] Component versions: Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
6009	Maintenance Mode	Warning	Malware detected in Maintenance Mode: %PATH% [Details] Component versions: Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
7000	System	Information	Group policy applied [Details] Old Group Name: %GROUP NAME% Old Policy Version: %VERSION% New Group Name: %GROUP NAME% New Policy Version: %VERSION%
7001	System	Warning	Unable to synchronize group policy [Details] Old Group Name: %GROUP NAME% Old Policy Version: %VERSION% New Group Name: %GROUP NAME% New Policy Version: %VERSION% Reason: %Reason%

Agent Error Code Descriptions

This list describes the various error codes used in TXOne StellarEnforce agent.

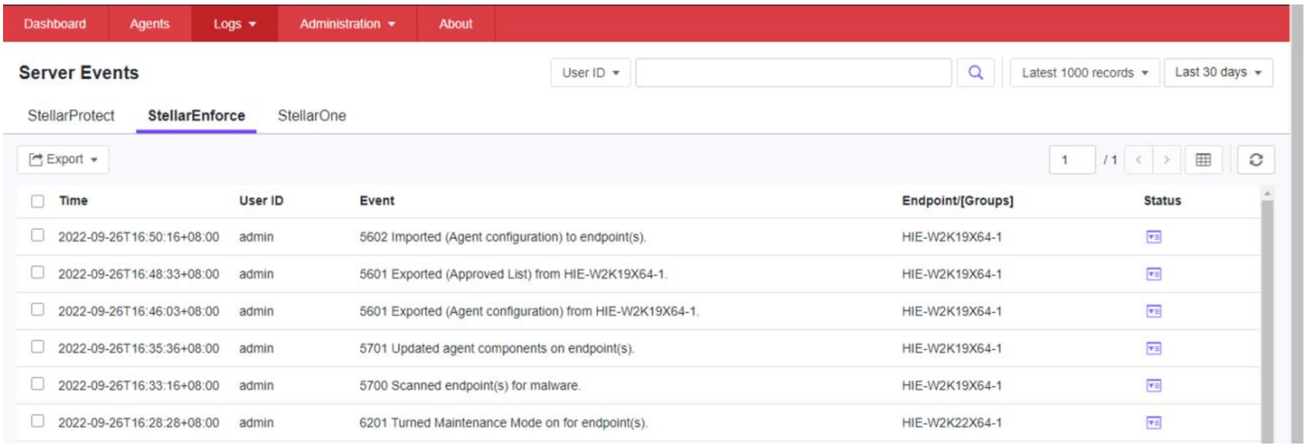
Error Code Descriptions (StellarEnforce)

CODE	DESCRIPTION
0x00040200	Operation successful.
0x80040201	Operation unsuccessful.
0x80040202	Operation unsuccessful.
0x00040202	Operation partially successful.
0x00040203	Requested function not installed.
0x80040203	Requested function not supported.
0x80040204	Invalid argument.
0x80040205	Invalid status.
0x80040206	Out of memory.
0x80040207	Busy. Request ignored.
0x00040208	Retry. (Usually the result of a task taking too long)
0x80040208	System Reserved. (Not used)
0x80040209	The file path is too long.
0x0004020a	System Reserved. (Not used)
0x8004020b	System Reserved. (Not used)
0x0004020c	System Reserved. (Not used)
0x0004020d	System Reserved. (Not used)
0x8004020d	System Reserved. (Not used)
0x0004020e	Reboot required.
0x8004020e	Reboot required for unexpected reason.
0x0004020f	Allowed to perform task.
0x8004020f	Permission denied.
0x00040210	System Reserved. (Not used)
0x80040210	Invalid or unexpected service mode.
0x00040211	System Reserved. (Not used)
0x80040211	Requested task not permitted in current status. Check license.
0x00040212	System Reserved. (Not used)
0x00040213	System Reserved. (Not used)
0x80040213	Passwords do not match.
0x00040214	System Reserved. (Not used)
0x80040214	System Reserved. (Not used)

0x00040215	Not found.
0x80040215	"Expected, but not found."
0x80040216	Authentication is locked.
0x80040217	Invalid password length.
0x80040218	Invalid characters in password.
0x00040219	Duplicate password. Administrator and Restricted User passwords cannot match.
0x80040220	System Reserved. (Not used)
0x80040221	System Reserved. (Not used)
0x80040222	System Reserved. (Not used)
0x80040223	File not found (as expected, and not an error).
0x80040224	System Reserved. (Not used)
0x80040225	System Reserved. (Not used)
0x80040240	Library not found.
0x80040241	Invalid library status or unexpected error in library function.
0x80040260	System Reserved. (Not used)
0x80040261	System Reserved. (Not used)
0x80040262	System Reserved. (Not used)
0x80040263	System Reserved. (Not used)
0x80040264	System Reserved. (Not used)
0x00040265	System Reserved. (Not used)
0x80040265	System Reserved. (Not used)
0x80040270	System Reserved. (Not used)
0x80040271	System Reserved. (Not used)
0x80040272	System Reserved. (Not used)
0x80040273	System Reserved. (Not used)
0x80040274	System Reserved. (Not used)
0x80040275	System Reserved. (Not used)
0x80040280	Invalid Activation Code.
0x80040281	Incorrect Activation Code format.

Server Event Log Descriptions

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



□	Time	User ID	Event	Endpoint/[Groups]	Status
□	2022-09-26T16:50:16+08:00	admin	5602 Imported (Agent configuration) to endpoint(s).	HIE-W2K19X64-1	▤
□	2022-09-26T16:48:33+08:00	admin	5601 Exported (Approved List) from HIE-W2K19X64-1.	HIE-W2K19X64-1	▤
□	2022-09-26T16:46:03+08:00	admin	5601 Exported (Agent configuration) from HIE-W2K19X64-1.	HIE-W2K19X64-1	▤
□	2022-09-26T16:35:36+08:00	admin	5701 Updated agent components on endpoint(s).	HIE-W2K19X64-1	▤
□	2022-09-26T16:33:16+08:00	admin	5700 Scanned endpoint(s) for malware.	HIE-W2K19X64-1	▤
□	2022-09-26T16:28:28+08:00	admin	6201 Turned Maintenance Mode on for endpoint(s).	HIE-W2K22X64-1	▤

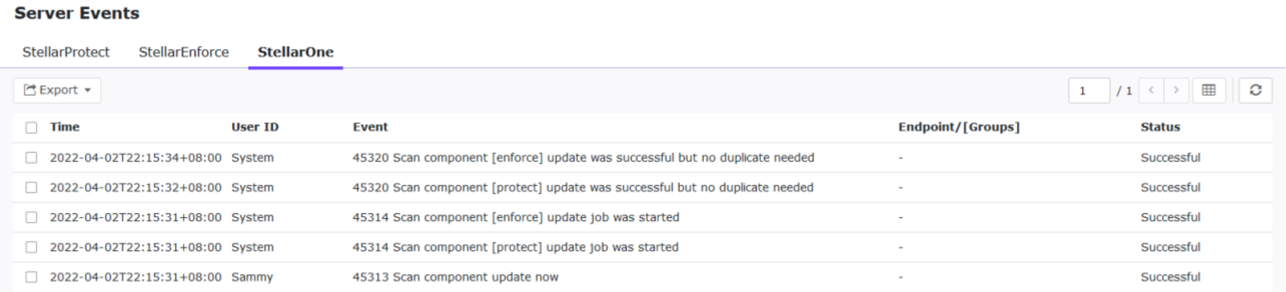
Server Event Log Descriptions (StellarEnforce)

EVENT ID	SERVER EVENT	DESCRIPTION
1001	Log on console	Logged on web console.
1002	Log off console	Logged off web console.
1003	Session timeout	Web console session timed out. Account '%user_name%' was logged off automatically.
1011	Unable to send reports	Unable to send scheduled reports to %email_address%.
1012	Unable to send notifications	Unable to send notifications to %email_address%.
2001	Create account	Created Intelligent Manager account '%user_name%'.
2002	Delete account	Deleted Intelligent Manager account '%user_name%'.
2003	Modify account	Modified Intelligent Manager account '%user_name%' %field_name%.
3001	Purge agent event logs - automatic	Automatic purge of agent event logs.
3002	Purge agent event logs - manual	Manual purge of agent event logs.
3003	Back up agent event logs	Automatic back up of agent event logs. Path: %filepath%.
3004	Purge server event logs - automatic	Automatic purge of server event logs.

3005	Purge server event logs - manual	Manual purge of server event logs.
3006	Back up server event logs	Automatic back up of server event logs. Path: %filepath%.
4001	Take action on unapproved blocked file	Request sent to endpoint(s): Add blocked file to Approved List. File name: %file_name% File hash: %file_hash% (SHA-1) Request sent to endpoint(s): Delete the blocked file. File name: %file_name% File hash: %file_hash% (SHA-1) Request sent to endpoint(s): Ignore the blocked file. File name: %file_name% File hash: %file_hash% (SHA-1) Request sent to endpoint(s): Quarantine the file. File name: %file_name% File hash: %file_hash% (SHA-1) Request sent to endpoint(s): Restore the file from quarantine. File name: %file_name% File hash: %file_hash% (SHA-1)
4004	Release the quarantined malicious file	Request sent to endpoint(s): Restore the file from quarantine. File name: %file_name% File hash: %file_hash% (SHA-1)
4005	Delete the quarantined malicious file	Request sent to endpoint(s): Delete the file from quarantine. File name: %file_name% File hash: %file_hash% (SHA-1)
4006	Take action on unapproved fileless attack	Request sent to endpoint(s): Add blocked process chain and command argument. Process chain: %process_name% Command argument: %parameter% Request sent to endpoint(s): Ignore blocked process chain and command argument. Process chain: %process_name% Command argument: %parameter%
5001	Turn Application Lockdown on	Turned Application Lockdown on for endpoint(s).
5002	Turn Application Lockdown off	Turned Application Lockdown off for endpoint(s).
5011	Add trusted file hashes	Added 1 trusted file hash to endpoint(s). Added %num% trusted file hashes to endpoint(s).
5013	Delete approved files	Removed specified items from the Approved List on endpoint(s) using SLtasks.exe.
5021	Block access from storage devices	Blocked access from storage devices on endpoint(s).
5023	Allow access from storage devices	Allowed access from storage devices on endpoint(s).
5025	Add trusted USB device	Add trusted USB device on selected endpoint(s)

5601	Export agent settings	Exported (%file_desc%) from %endpoint_name%.
5602	Import agent settings	Imported (%file_desc%) to endpoint(s).
5800	Change agent administrator password	Changed password on endpoint(s).
5700	Scan for malware	Scanned endpoint(s) for malware.
5701	Update agent components	Updated agent components on endpoint(s).
5900	Update agent Approved List	Updated Approved List on endpoint(s).
6001	Deploy agent patch	Deploy agent patch to endpoint(s). Patch name: %patch_name%
6101	Agent transfer	Agent transferred to new Intelligent Manager server
6201	Turn Maintenance Mode on	Turned Maintenance Mode on for endpoint(s).
6202	Turn Maintenance Mode off	Turned Maintenance Mode off for endpoint(s).
6301	Deploy group policy	Deploy group policy. Version: %version%.
6302	Cannot connect to ODC server	Cannot connect to ODC server.
6401	Set Intelligent Runtime Learning	Set Intelligent Runtime Learning. Version: %policy_version%
6402	Set Agent Password	Set Agent Password. Version: %policy_version%
6403	Set Schedule Scan Setting.	Set Schedule Scan Setting. Version: %policy_version%
6404	Set User-Defined Suspicious Objects.	Set User-Defined Suspicious Objects. Version: %policy_version%
6405	Set Agent Patch.	Set Agent Patch. Version: %policy_version%

Server Event Log Descriptions (StellarOne)



Server Events

□	Time	User ID	Event	Endpoint/[Groups]	Status
□	2022-04-02T22:15:34+08:00	System	45320 Scan component [enforce] update was successful but no duplicate needed	-	Successful
□	2022-04-02T22:15:32+08:00	System	45320 Scan component [protect] update was successful but no duplicate needed	-	Successful
□	2022-04-02T22:15:31+08:00	System	45314 Scan component [enforce] update job was started	-	Successful
□	2022-04-02T22:15:31+08:00	System	45314 Scan component [protect] update job was started	-	Successful
□	2022-04-02T22:15:31+08:00	Sammy	45313 Scan component update now	-	Successful

EVENT ID	DESCRIPTION
45313	Scan component update now
45314	Scan component [%s] update job was started
45315	Enable scan component scheduled update
45316	Disable scan component scheduled update
45317	Modify Scan component update source for StellarOne
45318	Modify Scan component update source for agents
45319	Scan component [%s] update was successful
45320	Scan component [%s] update was successful but no duplicate needed
45321	Scan component [%s] update was failed with internal error
45322	Scan component [%s] update was failed due to unable to connect to the network
45323	Customize policy
45324	Inherit policy from [%s]

Chapter 9 - Technical Support

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

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

Troubleshooting Resources

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

Using the Support Portal

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

Tip: To submit a support case online, visit the following URL: https://success.trendmicro.com/sign-in

A TXOne Networks or Trend Micro support engineer will investigate the case and respond in 24 hours or less.

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro and TXOne combat this complex malware with products that create a custom defense strategy.

The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

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

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

Contacting TXone and 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

In the United States, TXOne Networks representatives are available by below contact inforamation:

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

- Worldwide support offices:

  https://www.trendmicro.com/us/aboutus/contact/index.html

  https://www.txone.com/contact/
- Trend Micro product documentation:
  https://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

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

Sending Suspicious Content to Trend Micro

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

Email Reputation Services

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

https://ers.trendmicro.com/

Refer to the following Knowledge Base entry to send message samples to TXOne Networks:

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:

https://www.trendmicro.com/en_us/business/products/downloads.html

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

TXONE NETWORKS INCORPORATED

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

www.txone.com

Item Code: APEM139610/220926