TREND MICRO | txOne networks

1.0 TXOne StellarOne™ for StellarEnforce

Administrator's Guide

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

Windows

Endpoint Security

StellarOne for StellarEnforce

v 1.0

Administrator's Guide

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

http://docs.trendmicro.com/en-us/enterprise/txone-stellarenforce.aspx

Document Part No.: SLEM19271/210330

Release Date: May 4th, 2021

Protected by U.S. Patent No.: Patents pending.

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

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

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

Evaluate this documentation on the following site:

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

Privacy and Personal Data Collection Disclosure

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

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

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

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

https://www.trendmicro.com/privacy

Table of Contents

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:

Table 2. StellarOne Terminology

Terminology	Description
server	The StellarOne server program
server endpoint	The host where the StellarOne server is installed
agents	The hosts running the StellarEnforce program
NAT agents	The agents that are built under the routers with the Network Address Translation (NAT) function enabled
managed agents managed endpoints	The hosts running the 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

TXOne StellarOne 1.0 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.

Table 1-1. 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

Feature	Benefit
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.
Anti-malware Scanning	Security risk is the collective term for viruses/malware and spyware/grayware. StellarOne protects endpoints from security risks by scanning files and then performing a specific action for each security risk detected. Notifications and logs help you keep track of security risks and alert you if you need to take immediate action.

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 Required
Dashboard	• Admin • Operator • Viewer
Configure application lockdown	• Admin • Operator
Configure maintenance mode	• Admin • Operator
Configure device control	• Admin • Operator
Add trusted USB devices	• Admin • Operator
Scan now	• Admin • Operator
Update approved list	• Admin • Operator
Update agent components	• Admin • Operator
Deploy agent patch	• Admin • Operator

Check connection	• Admin • Operator • Viewer
Collect event logs	• Admin • Operator
Import / Export (approved list / agent configuration)	• Admin • Operator
Export selected / all agents	• Admin • Operator • Viewer
Organize (edit description / move / delete)	• Admin • Operator
Configure group policy	• Admin • Operator
Configure global policy	• Admin • Operator
Monitor agent event logs	• Admin • Operator • Viewer
Monitor server event logs	• Admin • Operator
Monitor system logs	• Admin • Operator

Monitor audit logs	• Admin • Operator
Account management	• Admin • Operator
System time	• Admin • Operator
Syslog forwarding	• Admin • Operator
Log purge	• Admin • Operator
Schedule report	• Admin • Operator • Viewer
Notification settings	• Admin • Operator • Viewer
SMTP settings	• Admin • Operator
Proxy settings	• Admin • Operator
Updates	• Admin • Operator

Download TXOne StellarEnforce agent installer image	• Admin • Operator • Viewer
License management	• Admin • Operator

Chapter 2

Managing StellarEnforce Agents

This chapter introduces the web console screen for agent management.

About the Agent Screen

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

Managing the Agent Group

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

Table 2-1. Agent Tree Management Tasks

Task	Details
Create agent groups	Create groups according to location, type, or purpose to help you manage multiple agents.
Delete agent groups	Delete groups.
Rename agent groups	Change the names of groups.

Creating Groups

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

Procedure

1. Go to **Agents > StellarEnforce** in the navigation at the top of the web console.

   The **Agents** screen will appear.

2. Click  icon.
3. Enter group name and select "Confirm".

   Note: *The group name must be less than 64 characters.*

Rename Group

Procedure

1. Click the three vertical dots icon next to the group you want to rename.
2. The **Rename** window will appear.
3. Type in the new name you want, and click **Confirm**.

Delete Group

Procedure

1. Click the three vertical dots icon next to the group you want to delete.
2. The delete confirmation window will appear.
3. Click **OK** that you want to delete the group.

Configuring Agent Settings

You can use the **Send Command** menu located on the **Agent** screen to control agent configuration settings.

Table 2-2. StellarEnforce Agent Commands

Task	Details
Configure Application Lockdown	Change the status of Application Lockdown.
Configure Maintenance Mode	Configure Maintenance Mode settings to enable patch updates on endpoints without blocking new file operations.
Configure Device Control	Allow or block storage devices (CD/DVD drives, floppy disks, and USB storage device) from accessing the managed endpoint.
Add Trusted Files	Configure agents to allow all files and installers added to the list to run based on hash values
Add Trusted USB Device	Configure agents to allow access of trusted USB devices on endpoints based on the device information.
Scan Now	Initiate a manual scan on selected endpoints and configure scan settings to deploy to endpoints
Update Approved List	Update the Approved List on selected agents by performing an inventory scan
Update Agent Components	Start the agent component update process on the selected agent. The agent will download the latest component updates
Deploy Agent Patch	Upgrade selected agents by uploading a patch file
Check Connection	Check the connection status of selected StellarEnforce agents

Collect Event Logs	Collecting event logs updates the StellarOne database with the latest information from the selected agents.
Import Settings	Import the Approved List or configuration settings for selected agents
Export Settings	Export the Approved List or configuration settings for selected agents
Export Selected Agents	Export selected agent information
Export All Agents	Export all agent information

Configure Application Lockdown

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

Procedure

1. Go to **Agents > StellarEnforce** in the navigation at the top of the web console.
2. Click the checkbox next to the endpoint you want to configure for Application Lockdown.
3. Under **Protection**, click **Configure Application Lockdown**. There, you can select from two options:

- **Turn Application Lockdown On:** select **Lock**
- **Turn Application Lockdown Off:** select **Unlock**

4. Select the desired option and click **OK**.
5. And system will show the description of the function for confirmation. Please click Yes to confirm or No to back.

Configuring 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 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 agent 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. Go to **Agents > StellarEnforce** in the navigation at the top of the web console.
2. The **Agents** screen will appear.
3. Select one or more endpoints by clicking the checkbox next to them.
4. Click **Configure Maintenance Mode**. The **Configure Maintenance Mode** screen will appear.
5. Click **Enable** to configure the Maintenance Mode settings.

   Click **Disable** to stop Maintenance Mode or cancel the scheduled maintenance period on endpoints.
6. You can choose either **Start Now** or **Schedule**. If you choose **Schedule**, you must specify the duration of the maintenance period.
7. If you select **Scan endpoints when Maintenance Mode is stopped**, StellarEnforce will scan endpoints for threats when the maintenance period is over.

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

8. If you decided to **Scan endpoints when Maintenance Mode is stopped**, select if you want detected files to be **Quarantined** or **Added to the Approved List**.
9. Click **OK** to deploy the settings to the selected agents or groups.
10. The system will show the command deployment with status, user can click the Close button.

Configuring Device Control

Procedure

1. Go to **Agents > StellarEnforce** in the navigation at the top of the web console. The **Agents** screen will appear.
2. Select which endpoints you want to configure by clicking the checkboxes next to their names.
3. Under **Protection**, click **Configure Device Control**.
4. Select to **Allow** or **Block** external device access for

USB drives, CD/DVD drives, and floppy disks on managed endpoints.

5. Click **OK** to confirm your settings.

Adding Trusted Files

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

Procedure

1. Go to **Agents > StellarEnforce** in the navigation at the top of the web console.

   The **Agents** screen will appear.

2. Select one or more endpoints by clicking the checkboxes next to each name.

3. Under **Protection** click **Add Trusted Files**. The **Add Trusted Files** screen will appear.

4. Click **Download File Hash Generator** to download the tool for calculating hash values.

5. Click **Add** to add a single hash value or click **Import** to add a batch of hash values.

6. To allow files created or modified by trusted installation packages to be automatically added to the Approved List, click the switch in the **Installer** column.

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.

Calculating the Hash Values

Use the File Hash Generator to calculate hash values.

Procedure

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

Note

- To ensure that all necessary files are calculated for hash values, TXOne recommends adding the root folder of the target application to the File Hash Generator for calculation.
- The **Add Folder** button will only calculate installer files, script files, and files in the Portable Executable format.

- Drag and drop folders or files to the File Hash Generator screen.
- Click the drop-down button and click **Add Files** to select files.
- Click the drop-down button and click **Add Folder**

to add all the files in the selected folder.

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

3. 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.

Add Trusted USB Devices

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

Procedure

1. Go to **Agents > StellarEnforce** in the navigation at the top of the web console.

   The **Agents** screen will appear.

2. Select one or more endpoints.

3. Click **Add Trusted USB Device**. The **Add Trusted USB Device** screen will appear.

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

   - Vendor ID
   - Product ID
   - Serial number

5. Click **Deploy** to deploy the setting to the selected agents or groups.

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

Removing Trusted USB Devices

After adding trusted USB devices, you can remove one or more trusted USB devices on an agent endpoint or using the StellarOne web console.

Removing Trusted USB Devices on StellarOne

This section describes how to remove trusted USB devices using the StellarOne web console.

Procedure

1. Go to **Agents > StellarEnforce** 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**.

The **Details** screen will appear.

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.

Removing Trusted USB Devices on StellarEnforce Agent Endpoints

This section describes how to remove trusted USB devices on a StellarEnforce agent endpoint using the Command Line Interface (CLI).

Procedure

1. Open a command window as an administrator and go to the StellarEnforce installation folder.
2. Type slcmd.exe show tud to display the current trusted USB device list.
3. Type the remove command in the following format to remove a trusted USB device:

   slcmd.exe remove tud [-vid <VID>] [-pid <PID>] [-sn <SN>]
4. Type slcmd.exe show tud to verify the trusted USB device is removed from the list.

Scan Now

You can initiate Scan Now through the StellarOne web console and can target one or several StellarEnforce agent endpoints.

Initiating Scan Now

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

Procedure

1. Go to **Agents > StellarEnforce** in the navigation at the top of the web console.
2. Select one or more entries and click **Protection** > **Scan Now**.

3. On the confirmation screen that will appear, click **Scan**.

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

Configuring Scan Now Settings

Procedure

1. In the **Scan Now** section, first select if StellarEnforce should continue to scan if the component update is unsuccessful.
2. Configure what StellarEnforce scans on endpoints.

Option	Description
All local folders	Select this option to scan all folders on the target endpoint.
Default folders	Select this option to scan only the folders most vulnerable to system threats: ● Fixed drivers root (e.g. C:\, D:\) ● System root folder (e.g. C:\Windows) ● System folder (e.g. C:\Windows\system) ● System32 folder (e.g. C:\Windows\system32) ● Driver folder (e.g. C:\Windows\system\drivers) ● Temp folder (e.g. C:\Users\AppDate\Local\Temp) ● Desktop folder include sub folders and files (e.g. c:\Users\Desktop)
Specific folders	Select this option to scan only the folders you specify.
Scan removable drives	Select this option to scan any removable media devices connected to the endpoint.
Scan compressed files	Select this option to scan the specified number of compression layers within an archived file. **Note** Scanning through more layers may detect malware intentionally buried within a compressed archive, but the scan may affect system performance.

Skip files	Select this option to bypass files that are larger than the specified size (in MB).

3. In the Actions section, specify the action to perform when detections occur.

Option	Description
Use ActiveAction	ActiveAction is a set of pre-configured scan actions for different types of security risks. If you are unsure which scan action is suitable for a certain type of security risk, TXOne recommends using ActiveAction. ActiveAction settings are constantly updated in the pattern files to protect endpoints against the latest security risks and the latest methods of attacks.
Customize scan actions	Select this option if you want the same action performed on all types of security risks. If you choose "Clean" as the first action, select a second action that StellarEnforce performs if cleaning is unsuccessful.

4. In the Scan Exclusions section, configure scan exclusions to increase scanning performance by skipping files that are known to be harmless.

Scan Exclusion List	Description
Folders	Click **Add** and specify a folder path. For example, C:\temp \ExcludeDir. StellarEnforce will not scan all files in the specified folders. **Note** Click **Delete** to remove one or more selected entries from the list.
Files	Click **Add** and specify the file path. For example, C:\temp \ExcludeDir\ExcludeDoc.hlp. **Note** Click **Delete** to remove one or more selected entries from the list.
File extensions	Type one or more file extensions, separating entries with a comma. StellarEnforce will not scan a file if its file extension matches any of the extensions in this list.

Updating 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.

Procedure

1. Go to **Agents > StellarEnforce** in the navigation at the top of the web console.

   The **Agents** screen will appear.
2. Select one or more endpoints.
3. Select **Update & Check > Update Approved List**. The **Update Approved List** screen will appear.
4. Click **OK** to begin inventorying the selected agents.

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

You can monitor the status of the Approved List update using the **Details** screen. The icons on the **Approved List** column display the current progress status.

Updating Agent Components

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

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

Procedure

1. Go to **Agents > StellarEnforce** in the navigation at the top of the web console. The **Agents** screen will appear.
2. Select one or more endpoints.
3. Select **Update & Check > Update Agent Components**.
4. Click **OK**.

Deploy Agent Patch

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

Procedure

1. Go to **Agents > StellarEnforce**.

   The **Agents** screen will appear.
2. Select one or more agents.

3. Click **Update & Check** > **Deploy Agent Patch**.
4. Select the patch file for deployment.
5. Click **OK**.

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

Checking Connections

Procedure

1. Go to **Agents > StellarEnforce** in the navigation at the top of the web console.

   The **Agents** screen will appear.
2. Select one or more endpoints.
3. Click **Update & Check > Check Connection**.

StellarOne will automatically attempt to contact the selected StellarEnforce Agents.

Important

StellarOne is unable to check the connection to NAT agents due to a lack of direct communication.

After the connection check completes, StellarOne will display a list of test results from all agents.

4. Click **Close** to display a complete list of disconnected agents in the agent tree search results.

After determining which agents cannot connect to the

StellarOne server, TXOne recommends checking the network connectivity of the disconnected agents.

Collecting Event Logs

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

Procedure

1. Go to **Agents > StellarEnforce** in the navigation at the top of the web console.

   The **Agents** screen will appear.

2. Select one or more agents.

3. Click **Update & Check** > **Collect Event Logs**.

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

Import Agent Settings

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

- Overwrite agent configurations
- Overwrite Approved Lists

Procedure

1. Prepare a customized agent configuration file or Approved List.
   a. Export and download an agent configuration file or Approved List.
   b. Customize the downloaded file.

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

- File is in the CSV format and uses UTF-8 encoding
- For Approved List, maximum file size supported is 20 MB
- For agent configuration file, maximum file size supported is 1 MB

---

2. Go to **Agents > StellarEnforce**.

   The **Agents** screen will appear.

3. From the Endpoint column, select one or more agents.
4. Click **Import / Export** > **Import Agent Configuration**. The import dialog will appear.
5. The **Command Deployment** window will appear.

6. Click **OK**.

Remotely Exporting Agent Settings

You can remotely obtain agent configuration settings and Approved Lists by exporting and downloading them from the StellarOne.

Procedure

1. Click **Agents > StellarEnforce** from the StellarOne. The **Agents** screen will appear.
2. Select a target endpoint.
3. Select **Import / Export**. The command window will appear.
4. Select one of the following:
   - **Approved List**
   - **Agent Configuration**

   Click the download link to download your approved list or agent configuration file. The progress can be viewed from the pop-up **Details** window.
5. To export more settings, repeat the above steps.
6. Click **View Details** to download the exported settings.

Export Selected Agent Settings

Procedure

1. Go to **Agents > StellarEnforce**. The

   Agents screen will appear.

2. Select a target endpoint.

3. Select **Import / Export** > **Export Selected Agents**.

4. An “exported endpoint info.csv” file will be downloaded to the folder which your browser specifies. It will include the specific agent information.

Export All Agent Settings

Procedure

1. Go to **Agents > StellarEnforce**. The

   Agents screen will appear.

2. Select a target endpoint.

3. Select **Import / Export** > **Export Selected Agents**.

4. An “exported endpoint info.csv” file will be downloaded to the folder which your browser specifies. It includes all agent information.

Edit Description

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

Procedure

1. Go to **Agents > StellarEnforce** in the navigation at the top of the web console. The **Agents** screen will appear.
2. Select one or more agents.
3. Click **Organize** > **Edit Description**.
4. Type or modify the agent tags.
5. Click **OK**.

Move

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

Procedure

1. Go to **Agents > StellarEnforce** in the navigation at the top of the web console.

   The **Agents** screen will appear.
2. Select one agent, and then select **Organize** > **Move**.

3. Check the group list.
4. Select a group on the list, and select **OK**.

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.

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

Procedure

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

Searching for Agents

Procedure

1. Go to **Agents > StellarEnforce** 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 specifying additional search criteria as required.

Tip

StellarOne supports partial string matching.

Option	Description
Endpoint	Type the full or partial endpoint host name to locate the specific endpoint.
Description	Type the description name.
IP Address	Type the IPv4 address.
IP Range	Type the IPv4 address.
Operating System	Select an operating system.
Last Connection	Select from the default time ranges or select **Custom** to specify your own range.
Sync Statue	Select **Synced** or **Unsynced**.

3. Click the **Search** icon.

   StellarOne will display all hosts that match the search

criteria.

Configuring Agent Group Policy

You can use the **Lockdown Exclusions** menu located on the **Agents** screen under the group's name to control agent configuration settings.

Each type of information – Trusted Hash Values, Trusted Certificates, Exception Paths, and Write Protection – will sync to each group based on its settings.

Enable Group Policy

Procedure

1. To configure group policy, click the gear next to **Device Group** on the **Agents** screen. The settings window will appear.
2. Click the switch to set **Auto Sync** to all devices. When auto sync is on, lockdown exclusions and patches will be synced. When auto sync is off, lockdown exclusions and patches will not be synced.

Trusted Hash Values

Trusted hash values allow StellarEnforce to identify and make rules for different applications running in your system.

Add Trusted Hash Values

Procedure

1. To add trusted hash values, go to your group's name under the **Agents** screen, and click **Lockdown Exclusions**. The **Lockdown Exclusions** screen will appear, showing the **Trusted Hash Values** tab.
2. Click **Add**, and the **Add Trusted Hash Values** window will appear.
3. Type in the hash value and any notes you might want to include on the hash value.

4. Set the **Installer** switch to automatically add all files created or modified by the related installer to the **Approved List**.
5. When you're satisfied with your entries, click **Add**. You will see it in the list under the **Trusted Hash Values** tab.

6. Click **Save**, then **Confirm**.

Import

Procedure

1. Under the **Trusted Hash Values** tab, under **Lockdown Exclusions**, under the name of your group, click **Import**. The **Import** screen will appear.
2. Click **Select File**, select your file, and then click **Import**.
3. Click **Save**, then **Confirm**.

Delete

Procedure

1. Select the checkbox next to the **Hash** you want to delete.
2. Click the **Delete** button on the bar under the tab's name.
3. **Confirm** that you want to delete the selected entries.
4. Click **Save** and then **Confirm**.

Trusted Certificates

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

Import

Procedure

1. Under the **Trusted Certificates** tab under **Lockdown Exclusions** under your group's name on the **Agents** screen, find the **Import** button and click it.
2. Click **Select File**, find the certificate you want to add, and click it.
3. Set the **Installer** switch to automatically add all files created or modified by the related installer to the **Approved List**.
4. Click **Import**.
5. When you're satisfied with the added certificate, click **Save**, and **Confirm**.

Delete

Procedure

1. To select the certificate you want to delete, click the checkbox next to its information under the **Trusted Certificates** tab.
2. Click the **Delete** button at the top of the list.
3. **Confirm** that you want to delete the certificate.
4. Click **Save** and then **Confirm**.

Exception Paths

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. Under **Lockdown Exclusions** under your group's name on the **Agents** screen, click the **Exception Paths** tab.
2. Under that tab, click the **Add** button. The **Add Exception Path** window will appear.
3. Select if it's a file, folder, or regular expression.
4. Under **Path** enter the file system path for the desired exception.
5. Click **Add**.
6. Click **Save**, and then **Confirm**.

Delete

Procedure

1. Under the **Exception Paths** tab, select the checkbox next to the path or paths you want to remove.
2. Click the **Delete** button at the top.
3. **Confirm** that you want to delete the checked values.
4. Click **Save** at the bottom, and then **Confirm**.

Write Protection

Write protection allows you to protect the details in certain files or folders from being

changed by users or other applications.

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

Procedure

1. Find the **Write Protection** tab under **Lockdown Exclusions** under your group name on the **Agents** screen.
2. Click the **Add** button. The **Add Write Protection** window will appear.
3. Select if the protection path is for a file, folder, registry key, or registry value.
4. Next to **Path**, type in the path to the target to be write protected.
5. Set the exception process type, 'No processes can write', 'All processes can write', or 'Specify a process that can write'.
6. Click **Add**.
7. Click **Save** and then **Confirm**.

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.

1. Find **Import Exclusions** on the **Lockdown Exclusions** screen, above the tab bar.
2. Click **Import Exclusions** and the **Import Exclusions** window will come up.
3. Click **Select File** and find the file carrying your exported settings.
4. Click **Import**.
5. Click **Save** and then **Confirm**.

Export Exclusions

1. Find **Export Exclusions** on the **Lockdown Exclusions** screen, above the tab bar.
2. Click **Export Exclusions** and your exclusion settings will be downloaded through your browser.

Patch Settings

Under **Patch Settings** you can set which patches should be applied to which group.

1. Find the **Patch** section on the **Agents** screen, under your group name, beneath **Lockdown Exclusions**.
2. Select the checkbox next to the patch or patches you want to apply to agents in this group.
3. To import a new patch, click the link to go to the **Update** page.
4. When you're satisfied with your settings, click **Save** and then **Confirm**.

Configuring Agent Global Policy

On the **Agents** screen, you can go to **All Agents** to set global policy that applies to every agent in every group.

Setting Global Agent Password

1. Find the **Agent Password** section under **All Agents** on the **Agents** screen.
2. Type in your new password, and click **Save**.

Schedule Scan Setting

Under Schedule Scan Setting, you can set scan frequency, component update settings before a scan, which files to scan, what actions to take during a scan, and what files to exclude from a scan.

Setting a Schedule

1. Under **Schedule Scan Setting**, find the **Schedule** section.
2. Set frequency to **Daily**, **Weekly**, or **Monthly**.
3. Set which day the routine should take place on, as well as the start time.

Component Update

1. Under **Schedule Scan Setting**, find the **Component Update** section.
2. Check the checkbox to continue with the scan even if the component update is unsuccessful. If left unchecked, the scan will not be conducted if StellarEnforce cannot update its components.

Files to Scan

1. Under **Schedule Scan Setting**, find the **Files to Scan** section.
2. Select **All Local Folders**, **Default Folders**, or select **Specific Folders** and enter paths to the folders you want to scan.
3. To scan all removable drives, check the checkbox next to **Scan Removable Drives.**
4. To scan all compressed files, check the checkbox next to **Scan Compressed Files**. Under this checkbox, you can also select how many layers deep to scan compressed files.

5. To skip files over a certain size, you can check **Skip Files Larger Than** and enter a file size between 1 and 9999 megabytes.

Scan Action

Under **Schedule Scan Setting**, find the **Scan Action** section.

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

Scan Exclusions

Under **Schedule Scan Setting**, find the **Scan Exclusions** section. Here you can specify files, folders, or extensions that will not be scanned.

- Under **Folders**, you can specify a path to the folder you do not want scanned.
- Under **Files**, you can specify a path to the files you do not want scanned.
- Under **File Extensions**, you can specify specific types of file by their file extension that you do not want scanned.

Intelligent Runtime Learning

When Intelligent Runtime Learning is turned on, the Agent will allow run-time execution files that are generated by applications on the Trust List.

Enable Intelligent Runtime Learning

1. Under **All Agents**, find the **Intelligent Runtime Learning** section.
2. Click the switch to enable **Intelligent Runtime Learning**. **Intelligent Runtime Learning** can also be disabled from this section.
3. Click **Save** and then confirm.

User-Defined Suspicious Objects

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

Adding User-Defined Suspicious Objects

1. Under **All Agents**, find the **User-Defined Suspicious Objects** section.
2. Click **Add**. The **Add Items to User-Defined Suspicious Objects** window will appear.
3. Enter the **Hash** or **File Path** for the object you want to be protected against, and type a note so you can easily identify it later.
4. Click **Confirm**.
5. Click **Save**.

Creating a Global Patch Policy

Previously this guide explained how to set a **Group Patch Policy**, which only applies to one group. In this section, it is shown how to create a **Global Patch Policy**, which applies to all agents regardless of group.

1. Under **All Agents**, find the **Patch** section.
2. Click the checkboxes next to each filename to select which patch or patches you would like to apply to all agents.
3. Click **Save**.

Chapter 3

Monitoring StellarEnforce

This chapter introduces TXOne StellarOne 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** tab are **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.

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

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**.

CPU Usage

This widget displays CPU usage information.

Memory Usage

This widget displays memory usage information.

Disk Usage

This widget displays disk usage information.

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.

Table 3-1. Agent events

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.

Table 3-2. User actions

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 1 Hour**, 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.

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** icon 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.

This screen displays a log of audited StellarOne web console account activity.

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.

   Click the drop-down list under **Server Events**. A list of search criteria 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**.
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.

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	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

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.

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

Chapter 4

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
Operator	• Add user account (Operator or Viewer) • Delete user account
Viewer	• Not able to use account management screen

Adding Accounts

Procedure

1. Log on the web console using an administrator account.
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**.

   The **Add User Account** screen will appear.
4. Specify the account **ID** and **Name**.
5. Specify the **Password**.

6. **Re-type Password**. Enter the password a second time.
7. **Role**: Specify the privileges for the account. **Operator** or **Viewer**.
8. Optionally, type an account **Description**.
9. Click **Confirm**.

Delete Accounts

Procedure

1. Log on the web console using an administrator account.
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.

   The **Delete** button will appear.
4. Click **Delete** button then the **Delete User Account** will appear.
5. Click **Yes**.

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

Time Zone

Use the drop-down to specific system time zone.

Syslog Settings

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

Procedure

1. Go to **Administration** > **Syslog**.
2. Select **Forward Logs to Syslog Server**.
3. Specify the protocol, IP address, and port of the syslog server.

Log Purge Settings

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

Procedure

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

   The **Log Purge** screen will appear.

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

Automatic Purge

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

Procedure

1. Find **Automatic Purge** under **Log Purge**
2. In the first dropdown box, select log type.
3. In the second dropdown box, select time frame for purging based on **Older Than** (Do not keep logs older than …).
4. In the third dropdown box, select the maximum number of log files to be kept.

5. When you're sure, click **Purge Now**.

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.
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 time for the scheduled reports on a daily, weekly, or monthly basis.  **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.

Notification Settings

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

Go to **Administration** > **Notification** to change notification settings.

Sections under **Notification** include **Warning Level Agent Events, Outbreak**, and **Email Notifications**.

Warning Level Agent Events

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

Outbreak

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

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).

Check the checkbox at the bottom to enable a notification to appear on the physical StellarOne.

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. To configure proxy settings for updates:

   a. Under **Server Address**, the IP address or fully qualified domain name (FQDN) of the SMTP server in the SMTP server field.

   b. Specify the **Port**.

   c. Specify the sender's email address in the **Sender** field. StellarOne uses this address as the sender address.

   d. If the SMTP server requires authentication, select **SMTP server requires authentication.**

   e. To send a test email from StellarOne, click the Send Test Email button.

3. Click **Save**.

Proxy Settings

Procedure

1. Go to **Administration** > **Proxy Settings** in the navigation at the top of the web console.

   The **Proxy Settings** screen will appear.

2. To configure proxy settings for updates:

   a. Under **Server Address**, specify the IPv4 address or FQDN of the proxy server.

   b. Specify the port.

   c. If your proxy server requires authentication, select **Proxy server authentication** and give your credentials.

3. Click Save.

Tip:

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

- **Before installation:** Add the proxy information to the configuration file used by the agent installer package.
- **After installation:** Use the SLCmd.exe Command Line Interface tool on the local StellarEnforce agent.

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
Patch	Here you can click the **Import** button to import a patch manually, or **Delete** to remove a StellarOne patch.

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.
Patch	Here you can click the **Import** button to import a patch manually, or **Delete** to remove a StellarEnforce patch.
Scan Component Update Source	Here, you can update components by downloading them directly from TXOne Server. You can also specify an update server that does not require authentication.

License Management

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

The following details appear on this screen:

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

Changing Activation Codes

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**.

3. Type your new TXOne StellarOne Activation Code.

Note

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

Chapter 5

Technical Support

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

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

Troubleshooting Resources

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

Using the Support Portal

The Trend Micro Support Portal is a 24/7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to 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 Trend Micro support engineer will investigate the case and respond in 24 hours or less.

Threat Encyclopedia

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

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

Go to http://about-threats.trendmicro.com/us/threatencyclopedia#malware to learn more about:

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

Contacting Trend Micro

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

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

- Worldwide support offices:

  http://www.trendmicro.com/us/about-

  us/contact/index.html

- TXOne product documentation:
  http://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

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

- Exact text of any error message received

Sending Suspicious Content to Trend Micro

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

Email Reputation Services

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

https://ers.trendmicro.com/

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

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

File Reputation Services

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

http://esupport.trendmicro.com/solution/en-

us/1059565.aspx

Please record the case number for tracking

purposes.

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

http://global.sitesafety.trendmicro.com/

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

Download Center

From time to time, TXOne may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

http://www.trendmicro.com/download/

If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.

Documentation Feedback

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

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

TREND MICRO INCORPORATED

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

www.trendmicro.com

Item Code: SLEM19271/210330