TREND MICRO | txOne networks

1.1 TXOne StellarOne™ for StellarEnforce

Administrator's Guide

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

Windows

Endpoint Security

TXOne StellarOne for StellarEnforce

Administrator's Guide

Document Part No.: SLEM19393/210826

Release Date: September 2021

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

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

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

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

Evaluate this documentation on the following site:

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

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
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 1.1 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.

What's new

TXOne StellarOne 1.1 includes the following new features and enhancements.

Table 1-1. What's New in TXOne StellarOne 1.1

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

System Migration

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

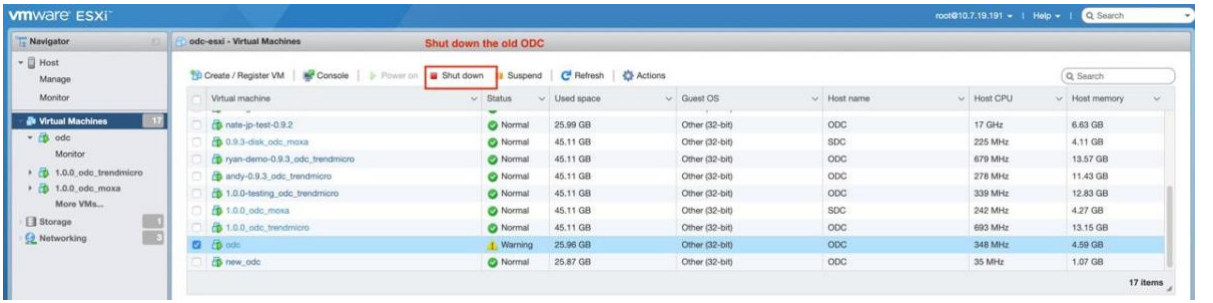
- The UUID
- The system configuration including license, accounting information, security policies, and so on.
- Security event logs

Important

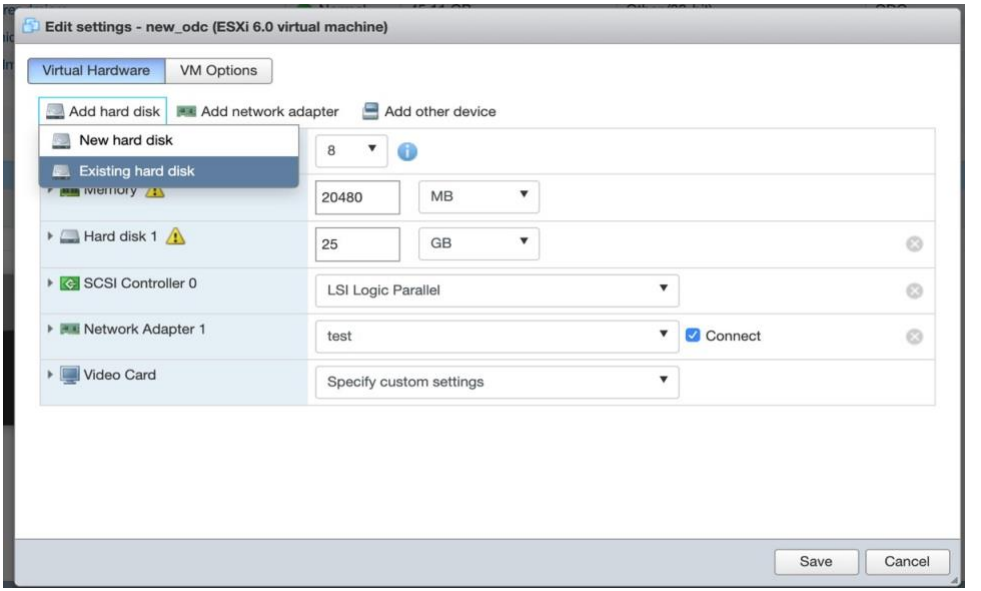
Before conducting a system migration, please take a VMware snapshot or back up your StellarOne data.

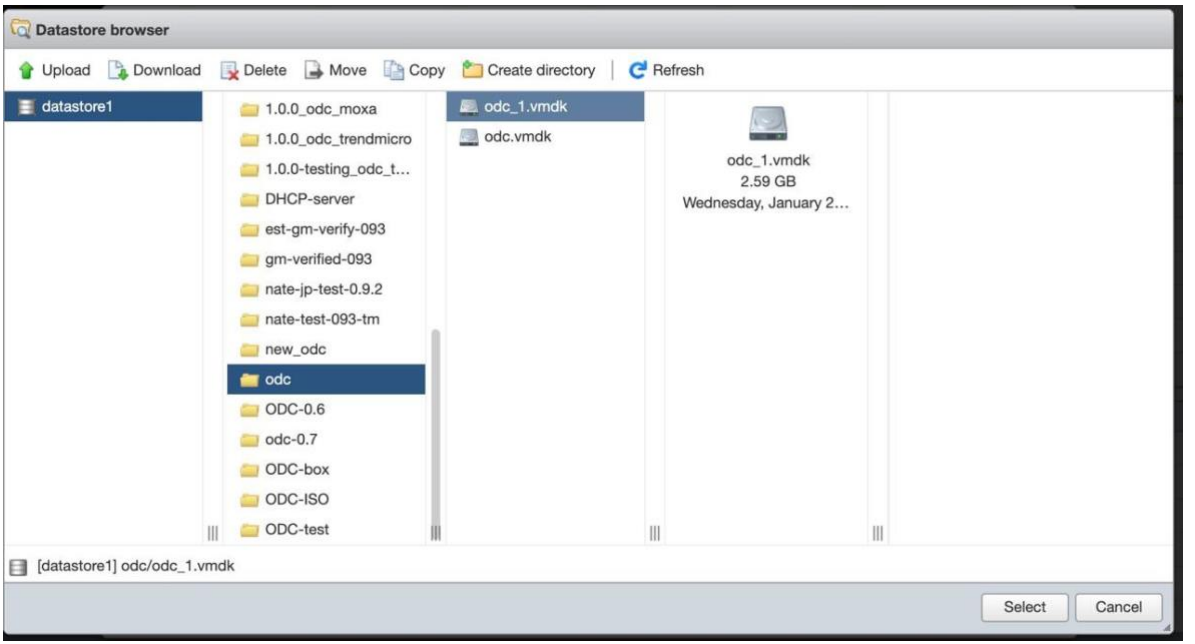
Procedure

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



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





4. The information from the old instance of StellarOne will be migrated into the new instance of StellarOne.

5. Check and, if necessary, configure the IP address of the new StellarOne to be the same as the IP address for the old instance of StellarOne. After this is configured, the communications between the new StellarOne and agents will be reconnected normally. The next time agents sync their status, they will report the new StellarOne. By default, agents will sync every 20 minutes.

6. If the proxy or scan component update source is already defined in the old instance of StellarOne, please define it again in the UI of the new instance of StellarOne.

7. For Japanese-speaking users, please note that you can switch the management console language. For more information, please see: How to Switch Management Console Language

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 files	• 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
Single Sign-On	• Admin

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
Downloads / Updates	• Admin • Operator • Viewer
Firmware	• Admin
SSL Certificate	• Admin
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.
- Please note that maintenance mode does not support the Microsoft Windows Visual Studio debugger.

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

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.

Note : Remote deployment of agent patches to the StellarEnforce 1.0 agent is not supported for Windows 7 SP1 and older versions.

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.

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 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.

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**.

Note: It's highly recommended to apply the agent patch using either group or global policy. If the version of the agent patch in group policy is lower than the version of the agent patch in global policy, it will cause agent status to always show as unsynced, and only the patch in global policy will be applied.

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**.

Note: It's highly recommended to apply the agent patch using either group or global policy. If the version of the agent patch in group policy is lower than the version of the agent patch in global policy, it will cause agent status to always show as unsynced, and only the patch in global policy will be applied.

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 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.

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 **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.

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

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**.

   The **Add User Account** screen will appear.
4. Specify the **Authentication Source**.
5. To add a local user, specify the account **ID** and **Name**. Please note that information entered here is case-sensitive.
6. To add an SAML identity provider user, specify **Email for SAML Account Mapping** and **Name.** Please note that information entered here is case-sensitive.
7. **Role**: Specify the privileges for the account as either **Operator** or **Viewer**.

8. For a local user, specify and re-type the **Local Password**.
9. Specify the **StellarProtect Group Control (All Groups, Custom, None)**.
10. Specify the **StellarEnforce Group Control (All Groups, Custom, None)**.
11. Optionally, type an account **Description**.
12. Click **Confirm**.

Edit Accounts

Procedure

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.

Click  . The **Edit User Account** screen will appear.

Specify the account **Name**. Please note that information entered here is case-sensitive.

Role: Specify the privileges for the account as either **Operator** or **Viewer**.

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

Specify the **StellarProtect Group Control**.

Specify the **StellarEnforce Group Control**.

Optionally, type an account **Description**.

Click **Confirm**.

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.

The **Delete** button will appear.

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

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** > **Authentication Server** in the navigation at the top of the web console.
3. Click **Download** to upload the StellarOne XML file to your IdP.
4. Click **Upload** to upload the IdP metadata XML file and complete the SAML 2.0 single sign-on configuration. The IdP metadata XML file must be re-uploaded if there is a configuration change on the IdP.
5. After the IdP metadata XML file is uploaded, the button **Test Connection** will appear. Click the button to test the IdP connection with StellarOne.

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

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

1. First, go to **Administration** > **SMTP Settings** to specify your SMTP server settings.
2. Go to **Administration** > **Notification** to change notification settings.
3. Sections under **Notification** include **Warning Level, Agent Events, 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, StellarOne 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

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 Settings** in the navigation at the top of the web console.

   Select the Proxy Settings for StellarOne to internet, Proxy settings for StellarOne to Agent communications or **Proxy Settings for agent to StellarOne communicates to agents.**

2. To configure proxy settings for updates:

   a. Select protocol use **HTTPS** or **HTTP**.

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

   c. Specify the **Port**.

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

3. Click Save.

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 StellarOne Server Information	Click **Download** to download the server information from StellarOne.
Patch	Here you can click the **Import** button to import a patch manually, or **Delete** to remove a StellarEnforce patch.

Firmware

Procedure

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

SSL Certification

Procedure

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

License 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

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

Windows Event Log Descriptions

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.

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
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%

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
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.

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
			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.

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
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%

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
			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%

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
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%

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
			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%

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
			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%

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
			[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%

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
			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]

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
			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%

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
			[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%

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
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%

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
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%

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
			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%

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
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%

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
			[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]

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
			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	Warning	Malware detected in Maintenance Mode:

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
	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.

TXOne StellarEnforce Error Code Descriptions

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.

CODE	DESCRIPTION
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)

CODE	DESCRIPTION
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.

Server Event Log Descriptions

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

EVENT ID	SERVER EVENT	DESCRIPTION
		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)
4002	Mark as closed	Marked %num% event(s) closed.
4003	Mark as open	Marked %num% event(s) opened.
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

EVENT ID	SERVER EVENT	DESCRIPTION
		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%
45313	Scan component update now	Scan component update now

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

Chapter 6

Technical Support

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

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

Troubleshooting Resources

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

Using the Support Portal

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

Procedure

1. Go to 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.

   T
   
   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: SLEM19393/210826