

Integrate ArrayOS SPX

Abstract

This guide provides instructions to configure ArrayOS to send the syslog events to EventTracker.

Scope

The configurations detailed in this guide are consistent with **EventTracker** version 7.X and later, and ArrayOS SPX series 8.4.6 and later.

Audience

ArrayOS SPX users, who wish to forward syslog events to EventTracker manager.

The information contained in this document represents the current view of EventTracker. on the issues discussed as of the date of publication. Because EventTracker must respond to changing market conditions, it should not be interpreted to be a commitment on the part of EventTracker, and EventTracker cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. EventTracker MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.

EventTracker may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from EventTracker, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2017 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Abstract 1

Pre-requisite 3

Configurations 3

 Partner Product Configuration 3

 Before You Begin 3

 Array SPX Configuration 3

Import ArrayOS SPX knowledge pack into EventTracker 6

 To import Category 6

 To import Alerts..... 6

Verify ArrayOS SPX knowledge pack in EventTracker 7

 Verify ArrayOS categories 7

 Verify ArrayOS SPX alerts 7

Pre-requisite

- EventTracker should be installed
- ArrayOS SPX 8.4.6 (or later) should be installed

Configurations

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Array SPX with EventTracker Enterprise. This document is not intended to suggest optimum installations or configurations. It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products to install the required components.

All Array SPX components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Array SPX Configuration

1. Login to the WebUI.
2. Select **Monitoring** from the column on the left.
3. Select **Enable Logging**. If the check box is grayed out, enter Config mode by clicking the **Config** radio button in the upper left corner.

Array NETWORKS

Username: array Language: English Help | Logout

SPX Host Name: Test2 Save Config

Mode: ☐ Enable ☒ Config

-- Base System --

Global Home

SYSTEM CONFIGURATION

- General Settings
- Basic Networking
- Advanced Networking
- Clustering
- Webwall

ADMINISTRATORS

- Global Admin
- Site Admin
- Admin Roles
- Admin Authentication

GLOBAL RESOURCES

- Local Databases
- SecurID Servers
- SSL Backend Server
- Thin Client Support

ADMIN TOOLS

- System Management
- Config Management

Monitoring

- Troubleshooting
- Change Password

VIRTUAL SITES

- Virtual Sites
- Service Management

Logging **SNMP** **Statistics**

General **Syslog Servers** HTTP Logging L3 VPN Logging ATF Logging Email Buffer

GENERAL SETTINGS

Enable Logging: ☒

Enable Timestamp: ☒ (Check this box to include timestamp on log entry)

Enable Time Zone: ☐ (Check this box to include time zone on log entry)

Facility: LOCAL0

Level: 6: INFO

CLEAR LOG SETTINGS

Clear Log Settings:

* Note: Clearing settings will also set HTTP Logging and Email Alert settings back to the default.

LOG TEST

Generate a Test Log Message:

Figure 1

- Navigate to **Logging->Syslog Servers** and click **Add Server Entry**.

Logging **SNMP** **Statistics**

General **Syslog Servers** HTTP Logging L3 VPN Logging ATF Logging Email Buffer

REMOTE SYSLOG SERVER CONFIGURATION **Delete Server Entry | Add Server Entry**

* Note: The Protocol (TCP or UDP) used for each Remote Syslog Server must be the same for ALL servers.

Host IP	Host Port	Protocol	Source Port	Log Level

Figure 2

- Enter the **Host IP** and **Host Port** information of the EventTracker log server. Select the log levels or leave all the boxes unchecked to enable all log levels.

Logging **SNMP** **Statistics**

General **Syslog Servers** HTTP Logging L3 VPN Logging ATF Logging Email Buffer

ADD SERVER ENTRY Cancel | Save & Add Another | Save

** Note: The Protocol (TCP or UDP) used for each Remote Syslog Server must be the same for ALL servers.*

Host IP:

Protocol: (If Protocol is disabled, this server will use the same protocol from other configured server)

Host Port:

Source Port:

Log Level [Description (Log Number)]: (Default = All log levels if no checkbox below is checked.)

[EMERGENCY (7)]: ☐

[ALERT (6)]: ☐

[CRITICAL (5)]: ☐

[ERROR (4)]: ☐

[WARNING (3)]: ☐

[NOTICE (2)]: ☐

[INFO (1)]: ☐

[DEBUG (0)]: ☐

Figure 3


6. Click **Save**.

The Event Tracker server will now appear in the list.

Import ArrayOS SPX knowledge pack into EventTracker

1. Launch **EventTracker Control Panel**.
2. Double click **Import Export Utility**.
3. Click the **Import** tab.
4. **Import Category/ Alert/ Scheduled reports** as given below.

To import Category

1. Click **Category** option, and then click the browse  button.
 2. Locate the [All ArrayOS group categories.iscat](#) file, and then click the **Open** button.
 3. Click the **Import** button to import the categories.
- EventTracker displays success message.

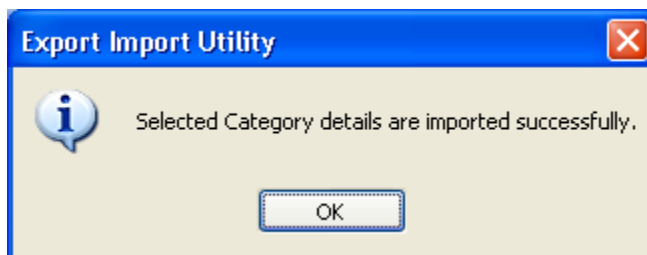



Figure 4

4. Click **OK** and then click the **Close** button.

To import Alerts

1. Click **Alert** option, and then click the browse  button.
 2. Locate the [All ArrayOS group alerts.isalt](#) file, and then click the **Open** button.
 3. Click the **Import** button to import the alerts.
- EventTracker displays success message.

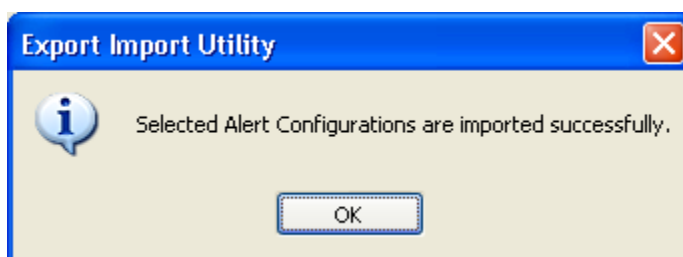


Figure 5

4. Click **OK** and then click the **Close** button.

Verify ArrayOS SPX knowledge pack in EventTracker

Verify ArrayOS categories

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and then click **Categories**.
3. In the **Category Tree**, expand **ArrayOS SPX** group folder to see the imported categories.

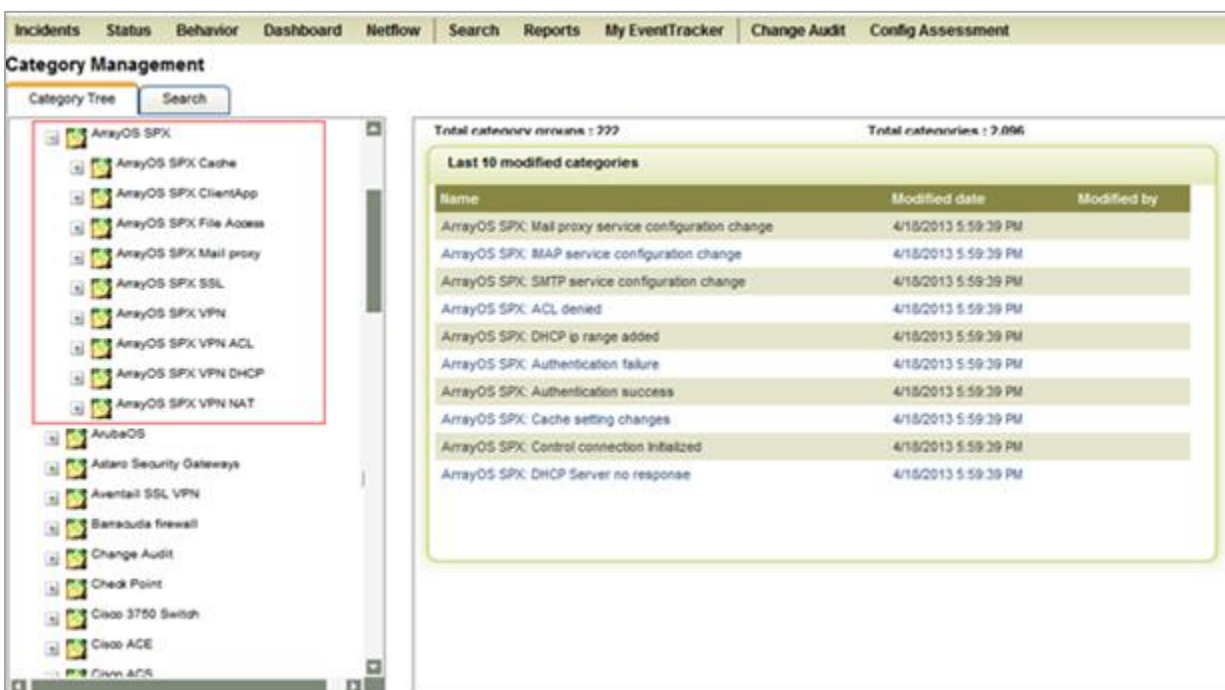


Figure 6

Verify ArrayOS SPX alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and then click **Alerts**.
3. In the **Search** field, type 'ArrayOS SPX', and then click the **Go** button.
Alert Management page will display all the imported ArrayOS SPX alerts.



Figure 7

4. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

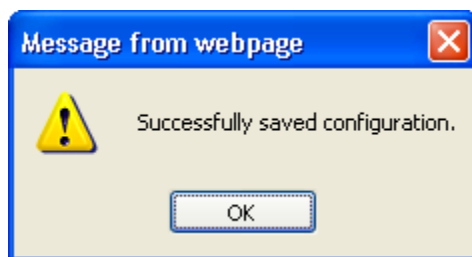


Figure 8

5. Click the **OK** button, and then click the **Activate now** button.
- NOTE:** You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.