

How to- Configure Varonis to forward logs to EventTracker

EventTracker v9.2 and later

Abstract

This guide provides instructions to retrieve the **Varonis** events via syslog. Once the logs start coming into EventTracker, reports, dashboards, alerts and saved searches can be configured.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.2 or above and **Varonis 6.3.190 and above**.

Audience

Administrators who are assigned the task to monitor **Varonis** events using EventTracker.

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

This document is for informational purposes only. Netsurion 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 Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion 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 Netsurion, 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.

© 2020 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

1. Overview.....	3
2. Prerequisites.....	3
3. Integrating Varonis with EventTracker.....	3
3.1 Configuring syslog message forwarding	3
3.2 Configuring syslog format.....	4
3.3 Configuring alerts for single or multiple rules	6

1. Overview

Varonis is a Data Security Platform that detects insider threats and cyberattacks by analyzing data, account activity and user behavior. It prevents and limits disaster by locking sensitive, and stale data and efficiently sustains a secure state with automation.

Varonis integrates with EventTracker SIEM application to provide security analytics with deep data context, so that organizations can be confident in their data security strategy. Benefits include scheduled reports, integrated Varonis dashboards and alerts for streamlined investigation.

Reports contain a detailed summary of events associated with exchange server activity, CIFS and NFS activity, share-point activity, and active directory activity.

Alerts are triggered as soon as critical events are received by EventTracker for Varonis, such as file permission change, file/folder deletion, password change or update, user lockout etc.

Dashboard is a graphical representation of all the activities happening in Varonis. These include event categories with cumulative log counts or percentage or by timeline.

These attributes or configurations of EventTracker allows administrators to quickly take appropriate actions against any threat/adversaries trying to jeopardize an organizations normal operation.

2. Prerequisites

- EventTracker v9.2 and above should be installed.
- Administrative/root access to Varonis UI.
- Syslog port (e.g. 514) should be allowed in firewall.
- EventTracker Manager public IP address (if Varonis is cloud based).

3. Integrating Varonis with EventTracker

3.1 Configuring syslog message forwarding

User can configure the syslog server address in DatAlert so that alerts are sent to EventTracker.

1. Login into your Varonis UI using admin credentials.
2. In DatAdvantage, select **Tools > DatAlert**. (DatAlert is displayed)
3. From the left menu, select **Configuration**.
4. In **syslog message forwarding**, do as follows.

- **Syslog server IP address** - The IP address of the EventTracker server on which you plan to setup a UDP listener.
 - **Port** - The port on which the EventTracker server will be listening
5. In the top-right corner, click **Syslog Settings**.

The screenshot shows the 'DatAlert' application window with the 'Configuration' tab selected. The left sidebar contains 'Rules', 'Configuration', 'Alert Templates', and 'Predefined Scopes'. The main area is titled 'Configuration' and includes a 'Restore Default Settings' button. Below this are three sections: 'Mail Settings', 'Syslog Message Forwarding', and 'SNMP Trap'.

Mail Settings:

- Aggregate similar events over: 5 minutes into a single message
- Threshold for suppressing messages: 20 messages within 5 minutes
- Select header image: Varonis DataAlert logo

Syslog Message Forwarding:

- Syslog server IP address: 10.10.34.40
- Port: 514
- Facility name: 1 - user-level messages
- Identity: Varonis - DatAlert
- Buttons: Add Additional Syslog Server, Test Message

SNMP Trap:

- SNMP server IP address: (empty)
- Port: 162
- Community name: public
- OID: (empty)
- Buttons: Add Additional SNMP Server, Test Message

At the bottom right are buttons for 'OK', 'Cancel', and 'Apply'.

Figure 1

6. Click OK.

3.2 Configuring syslog format

1. In **DatAlert**, from the left menu, click **Alert Templates**.

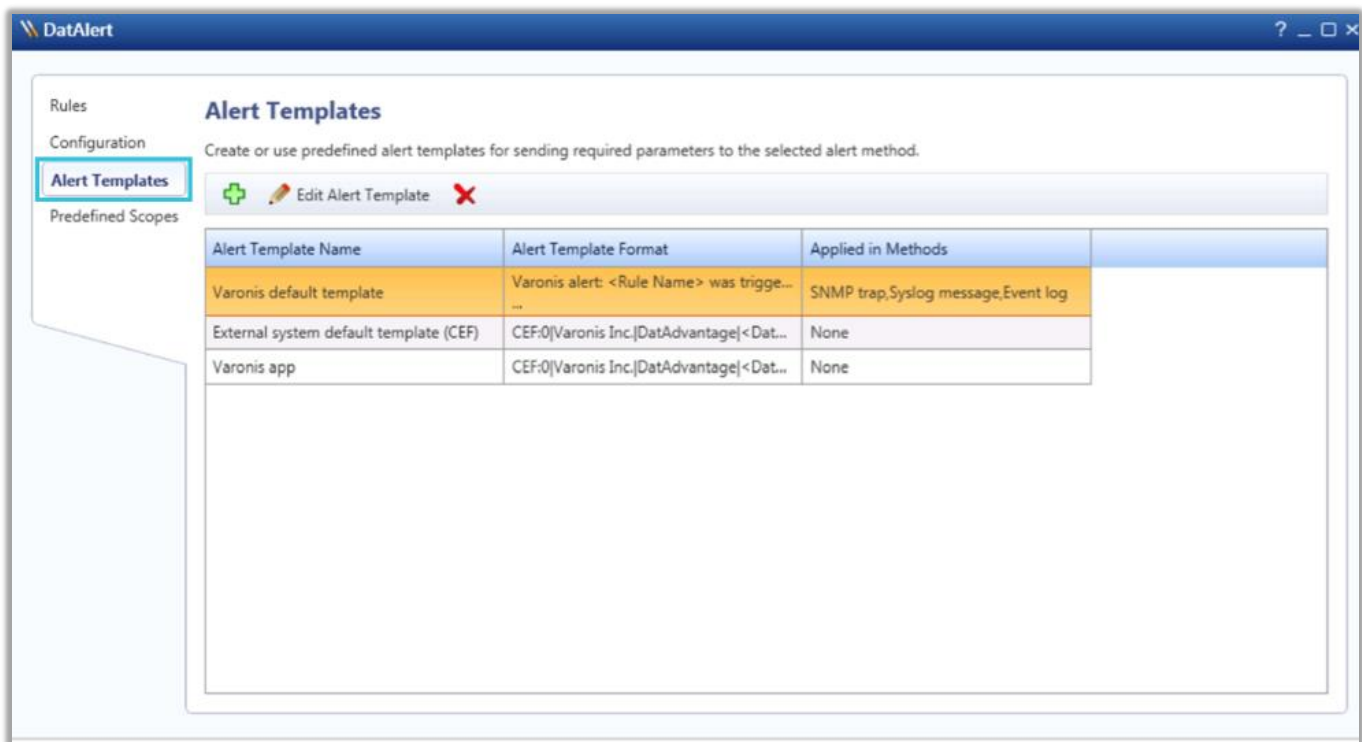


Figure 2

2. Click the green plus sign to add a new alert template:
 - Enter a **template name**. e.g. EventTracker syslog (CEF)
 - Open the **Apply to alert methods** dropdown list and select **Syslog message**.
 - Create a new **Alert Template Format** using the example templates below:
 - Manually edit the cs4 section, where DLS_IP_ADDRESS is the IP address or host name of the server running the Varonis Web UI.

```
CEF:0|Varonis Inc.|DatAdvantage|<DatAdvantage version>|<Event Op Code>|<Event
Type>|<Severity>|rt=<Alert Time> cat=Alert cs2=<Rule Name> cs2Label=RuleName cn1=<Rule
ID> cn1Label=RuleID end=<Event Time> duser=<Acting Object> dhost=<File Server/Domain>
filePath=<Access Path> fname=<Affected Object> act=<Event Type> dvchost=<Device Name>
dvc=<Device IP Address> outcome=<Event Status> msg=<Additional Data> cs3=<Attachment
Name> cs3Label=AttachmentName cs4=
http://<DLS_IP_ADDRESS>/DatAdvantage/#/app/analytics/entity/Alert/<Alert ID>
cs4Label=ClientAccessType deviceCustomDate1=<Mail Date> fileType=<Mail Item Type>
cs1=<Mail Recipients> cs1Label=MailRecipient suser=<Mail Source> cs5=<Mailbox Access
Type> cs5Label=MailboxAccessType cnt=<Threshold> cs6=<Changed Permissions>
cs6Label=ChangedPermissions oldFilePermission=<Permissions Before Change>
filePermission=<Permissions After Change> dpriv=<Trustee> start=<First Event Time>
```

e.g.

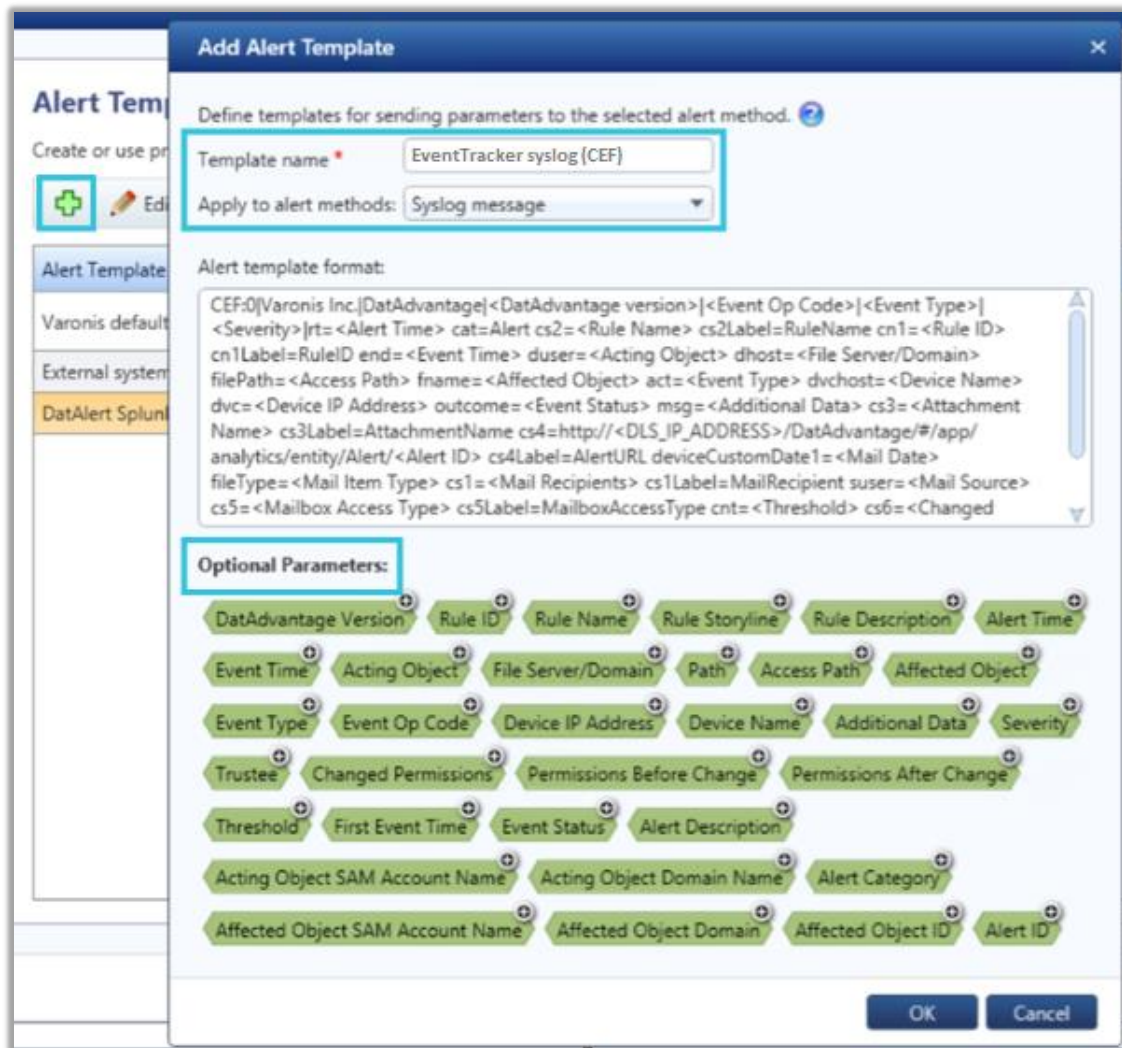


Figure 3

3. Click **OK** and verify that the new template appears in the “**Alert Templates**” table.
4. Click **OK**.

3.3 Configuring alerts for single or multiple rules

To send the events triggered by the rules to EventTracker, the alert must be forwarded by creating a syslog message.

To select the syslog alert method for a single rule:

1. From the DatAlert rules table, select the rule, then click **Edit Rule**. The rule editing menu appears.
2. From the left menu, select **Alerts Method**. The “Alert Method” window appears.

3. Select **syslog message**.
4. Click **OK**.

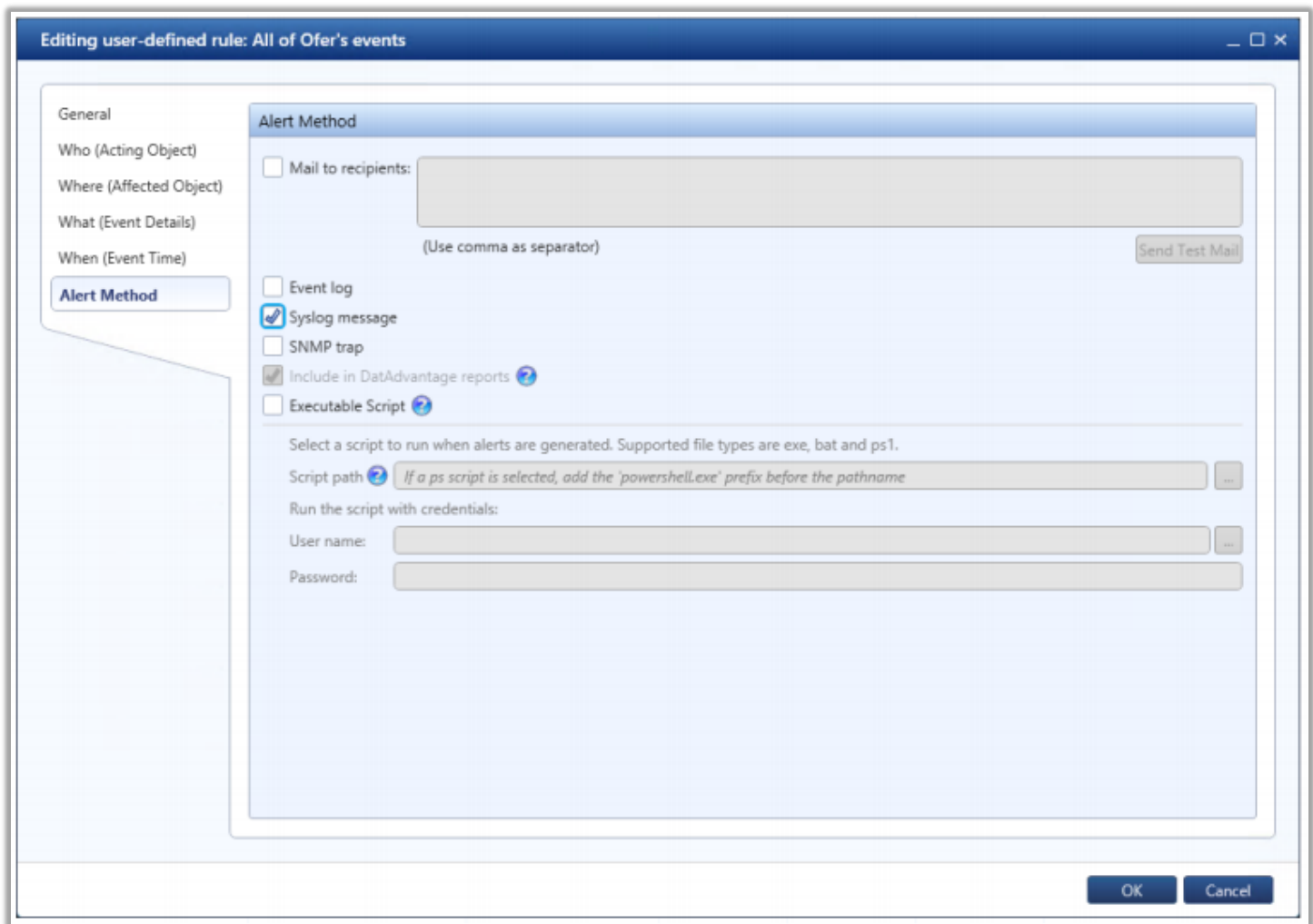



Figure 4

To select the syslog alert method for multiple rules:

1. From the DatAlert rules table, select the rules, then click **Edit Rule**. The rule editing menu appears.
2. From the left menu, select **Alerts Method**. Note that the window's contents are disabled for selection.
3. To enable **syslog message** for selection, click the edit  icon and select the checkbox.
4. Click **OK**.

Bulk Editing 2 Rules

General

Who (Acting Object)

Where (Affected Object)

Alert Method

☐ Mail to recipients:
(Use comma as separator) Send Test Mail

☐ Event log

☒ Syslog message

☐ SNMP trap

☐ Executable Script

Select a script to run when alerts are generated. Supported file types are exe, bat and ps1.

Script path ... *If a ps script is selected, add the 'powershell.exe' prefix before the pathname*

Run the script with credentials:

User name: ...

Password: ...

OK Cancel

Figure 5