VARONIS DATALERT APP AND TECHNOLOGY ADD-ON FOR SPLUNK®

Publishing Information

Software version	2.0
Document version	3
Publication date	October 25, 2018

CONTENTS

1 ABOUT THE VARONIS DATALERT APP AND TECHNOLOGY ADD-ON FOR SPLUNK®

The Varonis Technology Add-on (TA) for Splunk® and the Varonis DatAlert App for Splunk® enable integrating the Varonis DatAlert functionality into Splunk Enterprise.
Both the Varonis DatAlert App and TA provide field extractions and dashboards that enable you to locate notable Varonis alerts directly from the Splunk user interface, and then drill down into Varonis DatAlert to get additional insights into the alert and the context in which it was generated. Additionally, they include field extractions that assist users in querying and visualizing Varonis alerts using Splunk Enterprise.

The Varonis DatAlert App and TA are Splunk CIM compliant, which enables correlating the Varonis alerts with other events collected by Splunk Enterprise. This also enables incorporating Varonis alerts in Splunk Enterprise Security (ES).

The Varonis Technology Add-on for Splunk has incorporated parts of CEFUtils - Common Event Format Extraction Utilities by Igor Sher (*https://splunkbase.splunk.com/app/487/*).

Prerequisites

Various prerequisites are required to install and configure the Varonis Technology Add-on and App for Splunk and configure DatAlert to send alerts to Splunk.
Ensure you meet the following prerequisites:

- The following must be installed and running on your company's server:
  - Splunk Enterprise 7.1
  - Data Security Platform versions 6.2 and higher (DatAlert must be installed)
- To configure DatAlert to send alerts to Splunk (see *Configuring DatAlert to Send Alerts to Splunk*), the user must have the DL configuration role.
- To configure the Varonis DatAlert App for Splunk, the user must be the Splunk admin user.

Support

For information on how to contact support, refer to the Varonis Support page (*https://www.varonis.com/services/support*).

2 CONFIGURING DATALERT TO SEND ALERTS TO SPLUNK

You can configure DatAlert to send alerts to the Varonis DatAlert App for Splunk.

- *Configuring Syslog Message Forwarding*
- *Defining a New Template*
  - *Defining a Template for DatAlert Versions Prior to 6.3.170*
  - *Using the Pre-Defined Splunk Template*
- *Selecting an Alert Method for a Single Rule*
- *Selecting an Alert Method for Multiple Rules*

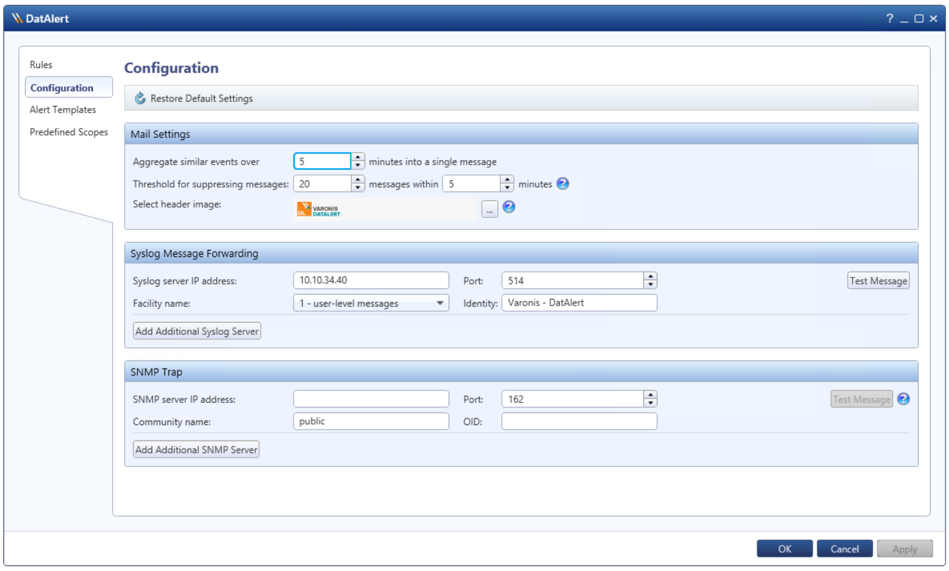
> Note: To configure DatAlert to send alerts to Splunk (*Configuring DatAlert to Send Alerts to Splunk*), the user must have the DL configuration role.

Configuring Syslog Message Forwarding

You can configure the Syslog server address in DatAlert so that alerts are sent to Splunk.

To configure the Syslog server address in DatAlert:

1. In DatAdvantage, select **Tools > DatAlert**.
   DatAlert is displayed.
2. From the left menu, select **Configuration**.
3. In Syslog Message Forwarding, do as follows:
   - Syslog server IP address - The IP address of the Splunk server on which you plan to set up a UDP listener.
   - Port - The port on which the Splunk server will be listening.



Aggregate similar events over 5 minutes into a single message

Threshold for suppressing messages: 20 messages within 5 minutes

Select header image:

Syslog server IP address: 10.10.34.40 Port: 514

Facility name: 1 - user-level messages Identity: Varonis - DatAlert

SNMP server IP address: Port: 162

Community name: public OID:

4. Click **OK**.

Defining a New Template

You can define an alert template that provides the information in the format expected by the Splunk App.

Templates define the format of the alert messages sent from DatAlert, using Syslog, to Splunk.

The procedure is version-specific:

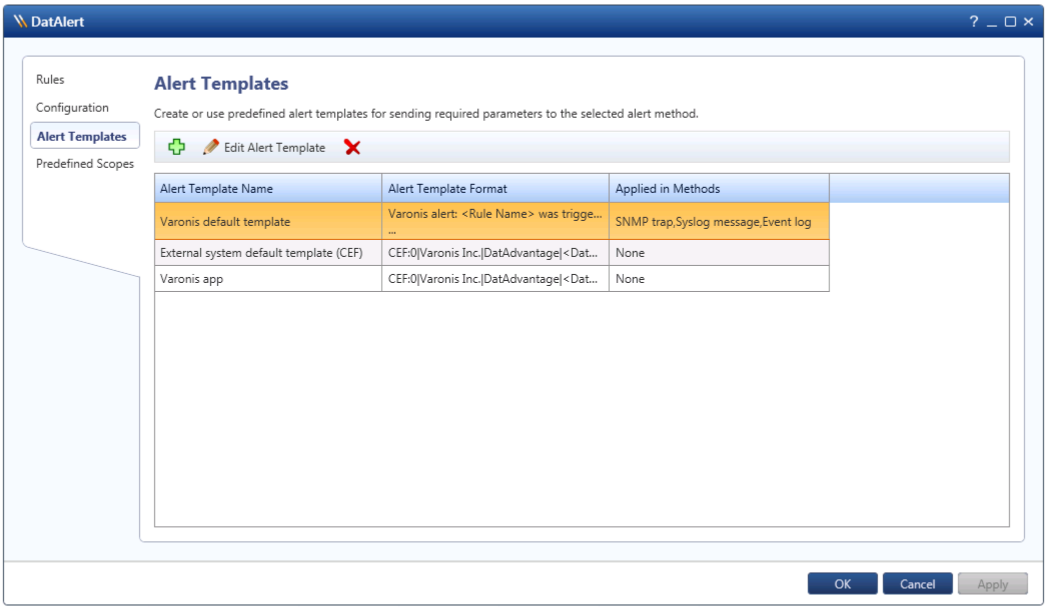
- For DatAlert versions before 6.3.170, refer to *Defining a Template for DatAlert Versions Prior to 6.3.170*.
- For DatAlert version 6.3.170 and above, refer to *Using the Pre-Defined Splunk Template*.

Defining a Template for DatAlert Versions Prior to 6.3.170

For DatAlert versions up to and including 6.3.170, you can define a template which includes the format of the alert messages sent from DatAlert to Splunk, using Syslog.

To define a template for DatAlert versions up to and including 6.3.170:

1. Ensure that you have followed the procedure in *Configuring Syslog Message Forwarding*.
2. In DatAlert, from the left menu, click **Alert Templates**.
   The **Alert Templates** window is displayed.



Alert Templates

Create or use predefined alert templates for sending required parameters to the selected alert method.

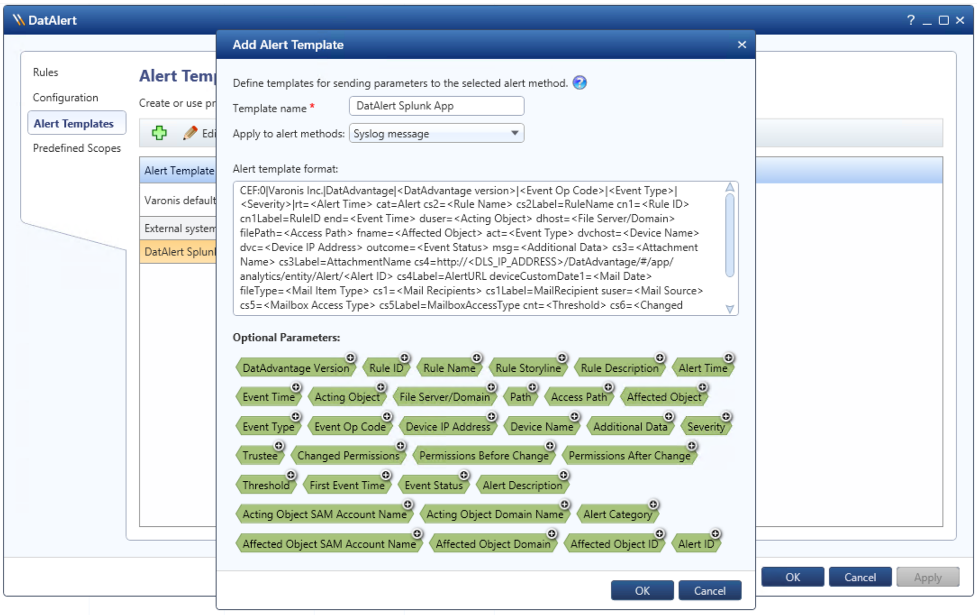
Alert Template Name	Alert Template Format	Applied in Methods
Varonis default template	Varonis alert: <Rule Name> was trigge... ...	SNMP trap,Syslog message,Event log
External system default template (CEF)	CEF:0|Varonis Inc.|DatAdvantage|<Dat...	None
Varonis app	CEF:0|Varonis Inc.|DatAdvantage|<Dat...	None

3. Click the green plus sign ✚.
   The **Add Alert Template** dialog box is displayed.
4. Do the following:
   - Alert template name - Enter a unique name for the alert template (for example, DatAlert Splunk App), comprising up to 40 characters.
   - Apply to alert methods - From the drop-down list, select **Syslog message**.
5. In Alert Template Format, do as follows:

a. Go to *https://info.varonis.com/hubfs/docs/splunk-app/varonis_splunk_syslog_cef_template.txt* and download the template file.

b. Open the downloaded file.

c. Copy and paste the string in the file into the **Alert template format** area for the required alert format (the template includes dynamic parameters that are replaced with the actual data when the alert is sent).



Add Alert Template

Define templates for sending parameters to the selected alert method.

Template name *: DatAlert Splunk App

Apply to alert methods: Syslog message

Alert template format:

```
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=AlertURL 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
```

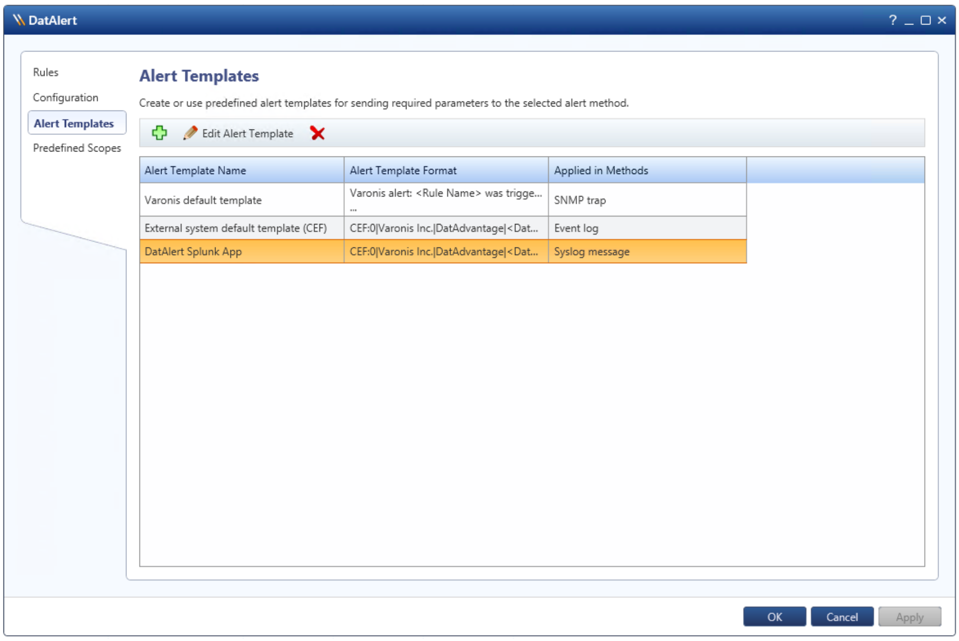
Optional Parameters:

d. Manually edit the cs4 section of the string as follows:

- Where `DLS_IP_ADDRESS` is the IP address or host name of the server running the Varonis Web UI
- Where `PROTOCOL` is either HTTP or HTTPS depending on whether Varonis Web UI uses HTTPS or HTTP

6. In the **Add Alert Template** dialog box, click **OK**.

7. Verify that the new template is displayed in the templates table:



Alert Templates

Create or use predefined alert templates for sending required parameters to the selected alert method.

Alert Template Name	Alert Template Format	Applied in Methods
Varonis default template	Varonis alert: <Rule Name> was trigge... ...	SNMP trap
External system default template (CEF)	CEF:0|Varonis Inc.|DatAdvantage|<Dat...	Event log
DatAlert Splunk App	CEF:0|Varonis Inc.|DatAdvantage|<Dat...	Syslog message

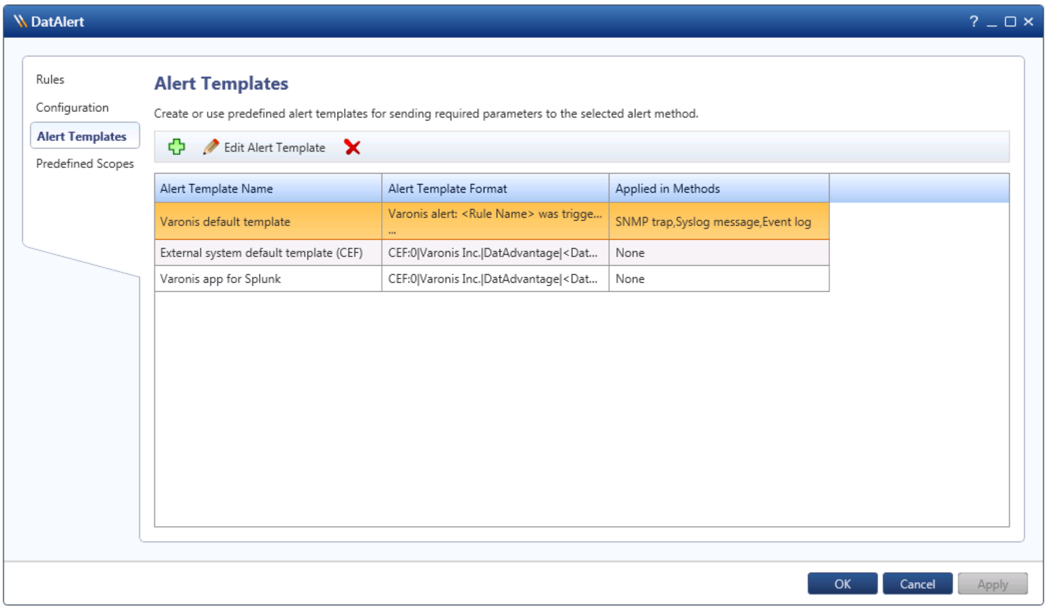
8. Click **OK**.

Using the Pre-Defined Splunk Template

For DatAlert versions higher than 6.3.170, DatAlert provides a predefined alert template for Splunk.

To define a template for DatAlert versions higher than 6.3.170:

1. Ensure that you have followed the procedure in *Configuring Syslog Message Forwarding*.
2. In DatAlert, from the left menu, click **Alert Templates**.
   The **Alert Templates** window is displayed.



Alert Templates

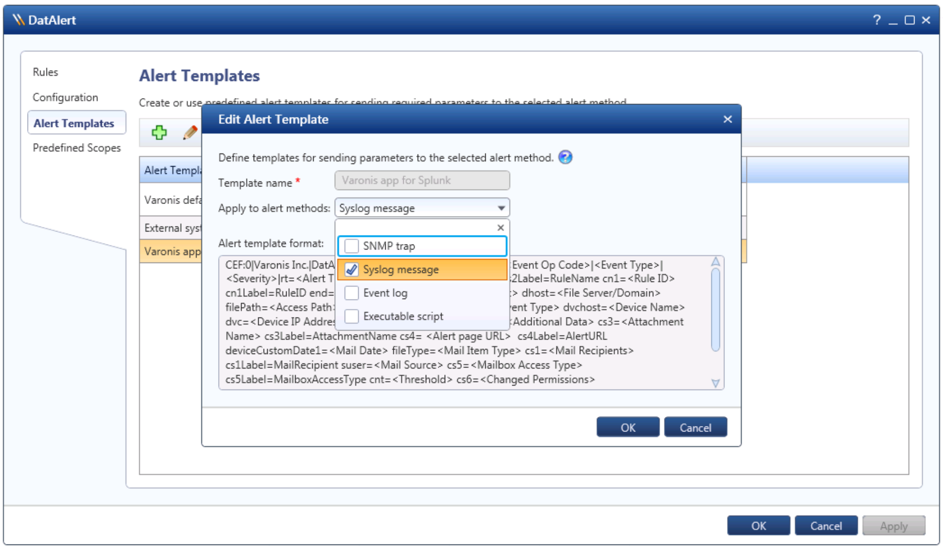
Create or use predefined alert templates for sending required parameters to the selected alert method.

Alert Template Name	Alert Template Format	Applied in Methods
Varonis default template	Varonis alert: <Rule Name> was trigge... ...	SNMP trap,Syslog message,Event log
External system default template (CEF)	CEF:0|Varonis Inc.|DatAdvantage|<Dat...	None
Varonis app for Splunk	CEF:0|Varonis Inc.|DatAdvantage|<Dat...	None

3. In the table, select **Varonis App for Splunk**.
4. In the toolbar, click **Edit Alert Template**.

The **Edit Alert Template** dialog box is displayed.

5. In Apply to Alert Templates, select **Syslog message**.



Define templates for sending parameters to the selected alert method.

Template name * Varonis app for Splunk

Apply to alert methods: Syslog message

- □ SNMP trap
- ☑ Syslog message
- □ Event log
- □ Executable script

Alert template format:

```
CEF:0|Varonis Inc.|DatA                     Event Op Code>|<Event Type>|
<Severity>|rt=<Alert T                     2Label=RuleName cn1=<Rule ID>
cn1Label=RuleID end=                       > dhost=<File Server/Domain>
filePath=<Access Path:                     ent Type> dvchost=<Device Name>
dvc=<Device IP Addres                      Additional Data> cs3=<Attachment
Name> cs3Label=AttachmentName cs4= <Alert page URL>  cs4Label=AlertURL
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>
```

6. Click **OK**, and then **OK** again.

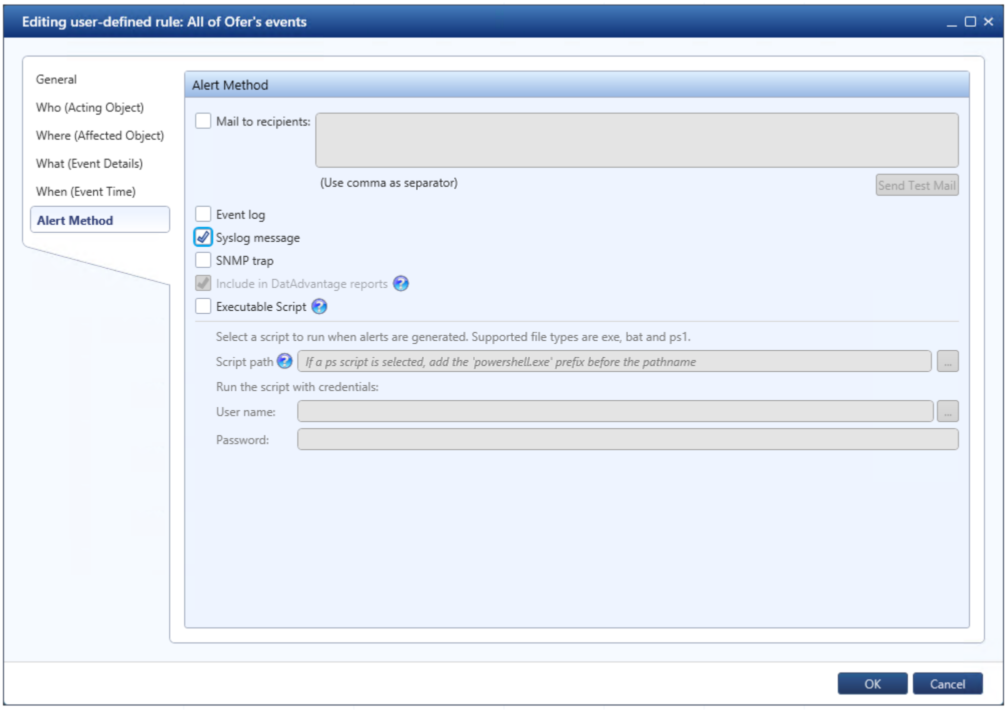
Selecting an Alert Method for a Single Rule

You can select the *alert method*, which is the means by which the alert is transferred.

For the Varonis App for Splunk, the alert is transferred by creating a Syslog message.

To select an alert method for a single rule, do as follows:

1. Ensure that you have followed the procedure in *Defining a New Template*.
2. In DatAlert, in the rules table, select the rule and then from the toolbar, click **Edit Rule** ✎.
   The rule editing menu is displayed.
3. From the left menu, select **Alerts Method**.
   The **Alert Method** window is displayed.
4. Select **Syslog message**.



Alert Method

☐ Mail to recipients:

(Use comma as separator)

☐ Event log

☑ Syslog message

☐ SNMP trap

☑ Include in DatAdvantage reports

☐ 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:

5. Click **OK**.

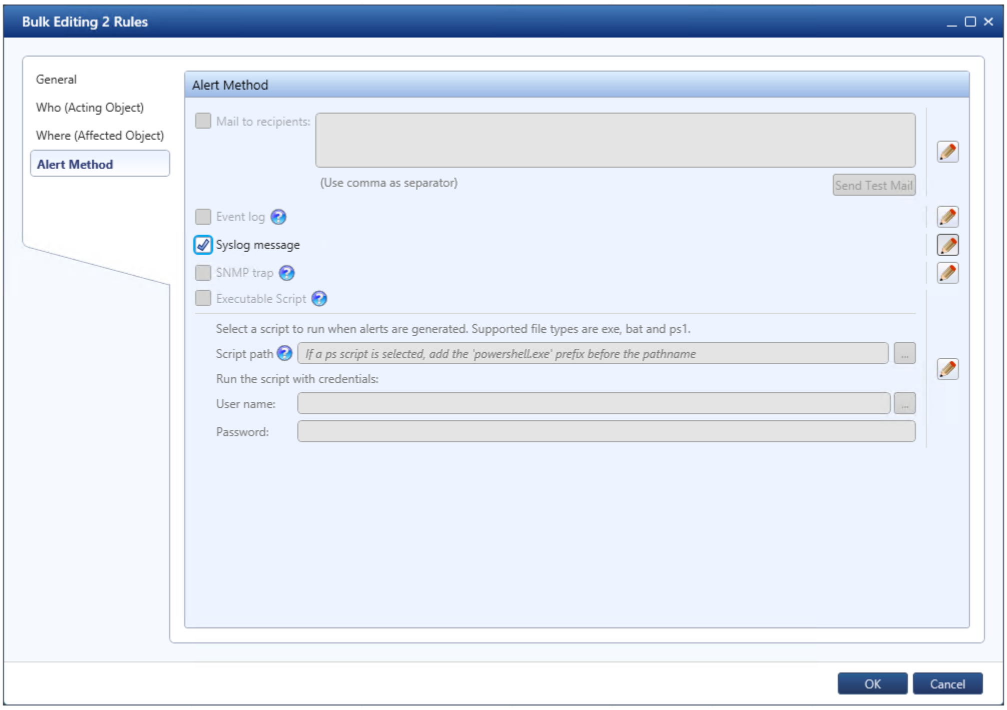
Selecting an Alert Method for Multiple Rules

You can select the alert method for multiple rules simultaneously.

To select the alert method for a single rule only, refer to *Selecting an Alert Method for a Single Rule*.

To select the alert method for multiple rules:

1. Ensure that you have followed the procedure in *Defining a New Template*.
2. In DatAlert, in the rules table, select the rules and then from the toolbar, click **Edit Rule** . The rule editing menu is displayed.
3. From the left menu, select **Alerts Method**. Note that the window's contents are disabled for selection.
4. To enable **Syslog message** for selection, click the edit icon and select the checkbox.



□ Mail to recipients:

(Use comma as separator)

□ 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:

5. Click **OK**.

3 INSTALLING THE VARONIS TECHNOLOGY ADD-ON AND APP FOR SPLUNK

Installing the Varonis Technology Add-on and App for Splunk enables integrating the Varonis DatAlert functionality into Splunk Enterprise.

- *Downloading the Varonis Technology Add-on and DatAlert App for Splunk*
- *Installing the Varonis Technology Add-on for Splunk*
- *Installing the Varonis DatAlert App for Splunk*
- *Configuring a New Splunk UDP Listener*
- *Configuring an Existing Splunk UDP Listener*
- *Optimizing for a Dedicated Index*
- *Verifying the Installation*

Downloading the Varonis Technology Add-on and DatAlert App for Splunk

Prior to installation, you must first download the Varonis Technology Add-on and DatAlert App for Splunk.

To download the Varonis Technology Add-on and DatAlert App for Splunk:

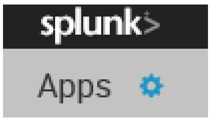
1. Ensure that you have followed the procedures in *Configuring DatAlert to Send Alerts to Splunk*.
2. Browse to *https://www.varonis.com/products/splunk-app*, and download the Varonis app for Splunk and the Varonis Technology Add-on for Splunk.
3. Place the downloaded zip files in a temporary folder.

Installing the Varonis Technology Add-on for Splunk

Installing the Varonis Technology Add-on for Splunk enables integrating the Varonis DatAlert functionality into Splunk Enterprise.

To install the Varonis Technology Add-on for Splunk:

1. Ensure that you have followed the procedure in *Downloading the Varonis Technology Add-on and DatAlert App for Splunk*.
2. In your local Splunk installation, access the main page.
3. Next to Apps, click the gear icon.



The **Apps** window is displayed.

4. Click **Install App from File**.
The **Upload an App** window is displayed.

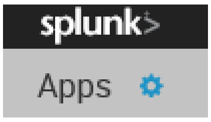
5. Click **Browse** and browse for the Varonis Technology Add-on for Splunk zip file you downloaded in *Downloading the Varonis Technology Add-on and DatAlert App for Splunk*.
6. Select the file and click **Upload**.
7. If you are prompted to restart Splunk Enterprise, then do so.
8. In the **Apps** window, you should have **Technology Add-on for Varonis DatAlert** listed in the list of apps.
   The app is installed.

Installing the Varonis DatAlert App for Splunk

Installing the Varonis DatAlert App for Splunk enables integrating the Varonis DatAlert functionality into Splunk Enterprise.

To install the Varonis DatAlert App for Splunk:

1. Ensure that you have followed the procedure in *Downloading the Varonis App for Splunk*.
2. In your local Splunk installation, access the main page.
3. Next to Apps, click the gear icon.

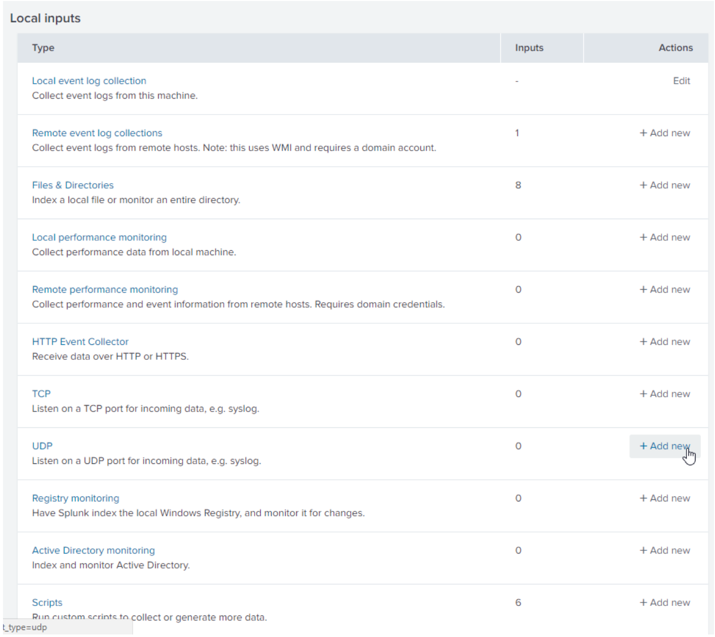
   The **Apps** window is displayed.
4. Click **Install App from File**.
   The **Upload an App** window is displayed.
5. Click **Browse** and browse for the Varonis App for Splunk zip file you downloaded in *Downloading the Varonis Technology Add-on and DatAlert App for Splunk*.
6. Select the file and click **Upload**.
7. If you are prompted to restart Splunk Enterprise, then do so.
8. In the **Apps** window, you should have **Varonis DatAlert App for Splunk** listed in the list of apps.
   The app is installed.

Configuring a New Splunk UDP Listener

You can configure a new UDP listener, enabling the installed app to correctly receive the Syslog messages from DatAlert.

To use an existing listener, refer to *Configuring an Existing Splunk UDP Listener*.

1. Ensure that you have followed the procedure in *Installing the Varonis DatAlert App for Splunk*.
2. In your local Splunk installation, access the main page.
3. From the top menu, select **Settings > Data Inputs**.
   The **Data Inputs** window is displayed.



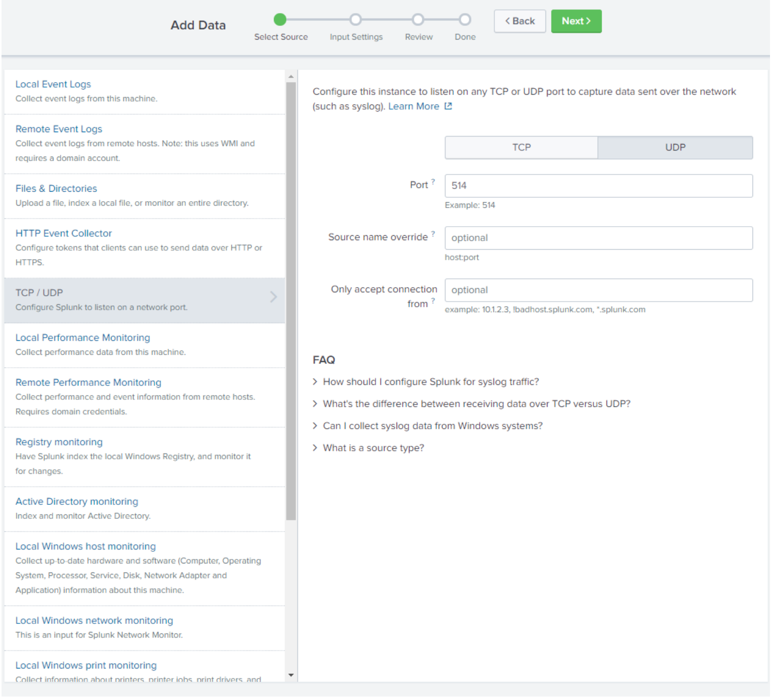
Local inputs

Type	Inputs	Actions
Local event log collection Collect event logs from this machine.	-	Edit
Remote event log collections Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.	1	+ Add new
Files & Directories Index a local file or monitor an entire directory.	8	+ Add new
Local performance monitoring Collect performance data from local machine.	0	+ Add new
Remote performance monitoring Collect performance and event information from remote hosts. Requires domain credentials.	0	+ Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	0	+ Add new
TCP Listen on a TCP port for incoming data, e.g. syslog.	0	+ Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	0	+ Add new
Registry monitoring Have Splunk index the local Windows Registry, and monitor it for changes.	0	+ Add new
Active Directory monitoring Index and monitor Active Directory.	0	+ Add new
Scripts Run custom scripts to collect or generate more data.	6	+ Add new

t_type=udp

4. In the UDP row, on the right, in the Action column, click **Add New**.
   The **Add Data** window is displayed. The TCP and UDP selections are displayed on the right.

5. Enter the port where Syslog messages are sent (as configured in *Configuring Syslog Message Forwarding*).



Local Event Logs
Collect event logs from this machine.

Remote Event Logs
Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure Splunk to listen on a network port.

Local Performance Monitoring
Collect performance data from this machine.

Remote Performance Monitoring
Collect performance and event information from remote hosts. Requires domain credentials.

Registry monitoring
Have Splunk index the local Windows Registry, and monitor it for changes.

Active Directory monitoring
Index and monitor Active Directory.

Local Windows host monitoring
Collect up-to-date hardware and software (Computer, Operating System, Processor, Service, Disk, Network Adapter and Application) information about this machine.

Local Windows network monitoring
This is an input for Splunk Network Monitor.

Local Windows print monitoring
Collect information about printers, printer jobs, print drivers, and

Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). Learn More

TCP | UDP

Port: 514
Example: 514

Source name override: optional
host:port

Only accept connection from: optional
example: 10.1.2.3, !badhost.splunk.com, *.splunk.com

FAQ

> How should I configure Splunk for syslog traffic?
> What's the difference between receiving data over TCP versus UDP?
> Can I collect syslog data from Windows systems?
> What is a source type?

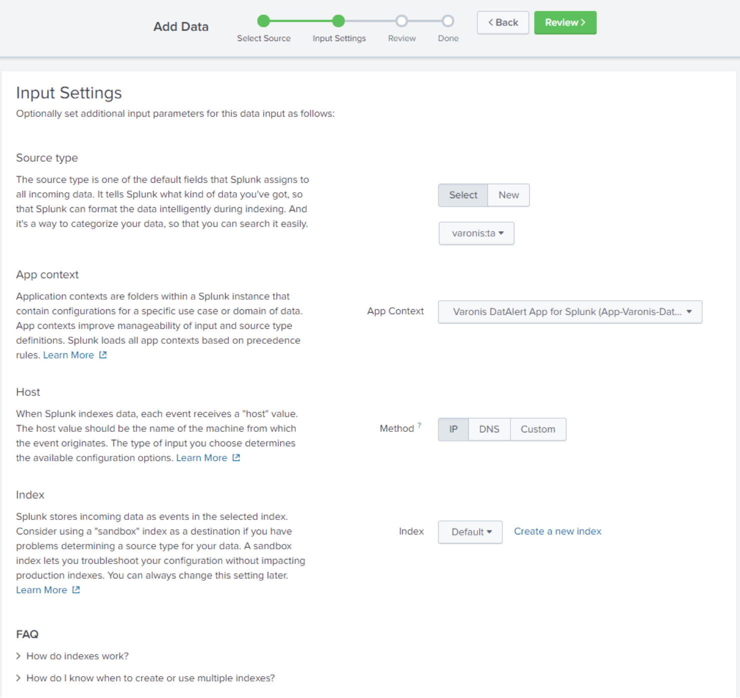
6. Click **Next**.

7. In **Input Settings**, in Source Type, do as follows:

   a. Click **Select**.

   b. From the drop-down list, select **Varonis** > **varonis:ta** or simply type **varonis:ta** in the drop-down field.

8. In App Context, select **Varonis DatAlert App for Splunk**.



Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

The source type is one of the default fields that Splunk assigns to all incoming data. It tells Splunk what kind of data you've got, so that Splunk can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Select | New

varonis:ta

App context

Application contexts are folders within a Splunk instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. Splunk loads all app contexts based on precedence rules. Learn More

App Context: Varonis DatAlert App for Splunk (App-Varonis-Dat...

Host

When Splunk indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More

Method: IP | DNS | Custom

Index

Splunk stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More

Index: Default Create a new index

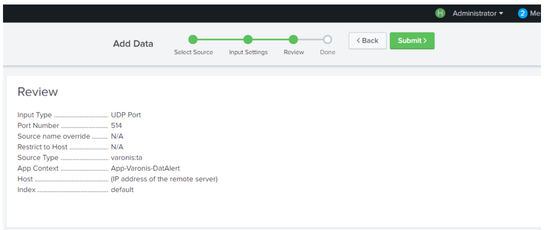
FAQ

› How do indexes work?

› How do I know when to create or use multiple indexes?

> Note: The default values in Host and Index are acceptable; however, they can be modified as needed.

9. At the top, click **Review**. A summary of your settings is displayed.



Review

```
Input Type ............................ UDP Port
Port Number ........................... 514
Source name override .......... N/A
Restrict to Host ..................... N/A
Source Type .......................... varonis:ta
App Context .......................... App-Varonis-DatAlert
Host ........................................ (IP address of the remote server)
Index ...................................... default
```

10. To edit any of the settings, use the back arrow adjacent to the **Submit** button to return to the previous windows to make any necessary changes.

11. If all your settings are satisfactory, click **Submit**.
    Your UDP settings are now configured.

Configuring an Existing Splunk UDP Listener

You can configure an existing UDP listener by verifying the listener's source name and editing the configuration file.

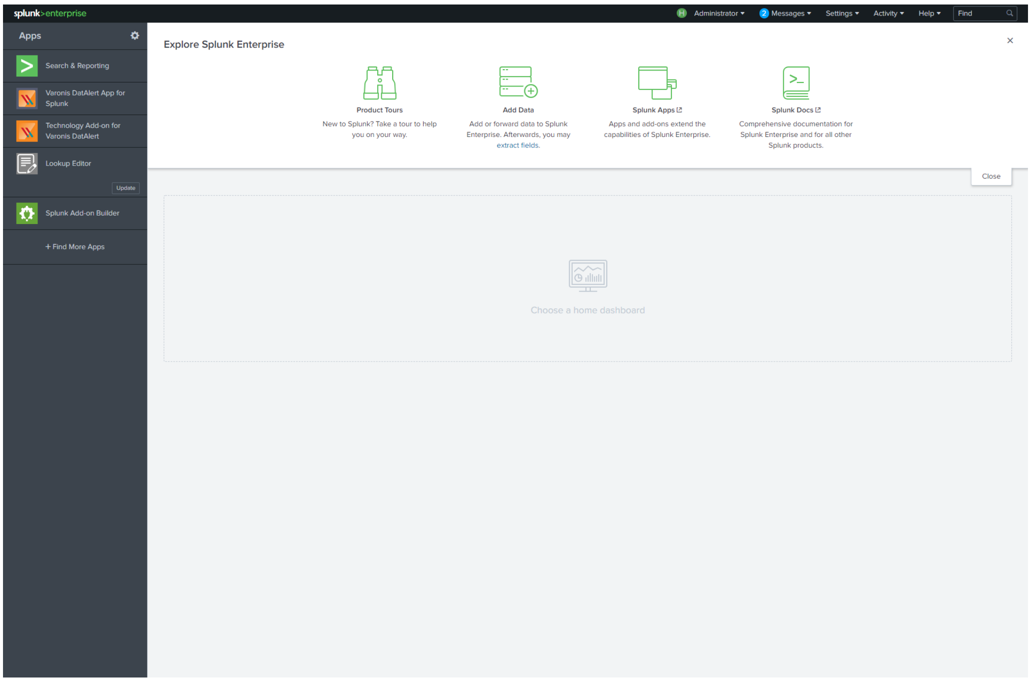
- *Verifying the Listener's Source Name*
- *Editing the Configuration File*

Verifying the Listener's Source Name

You can configure an existing Splunk UDP listener by verifying the listener's source name.

To verify a listener's source name:

1. Ensure that you have followed the procedure in *Installing the Varonis Technology Add-on and App for Splunk*.
2. In your local Splunk installation, access the main page.



Explore Splunk Enterprise

Product Tours
New to Splunk? Take a tour to help you on your way.

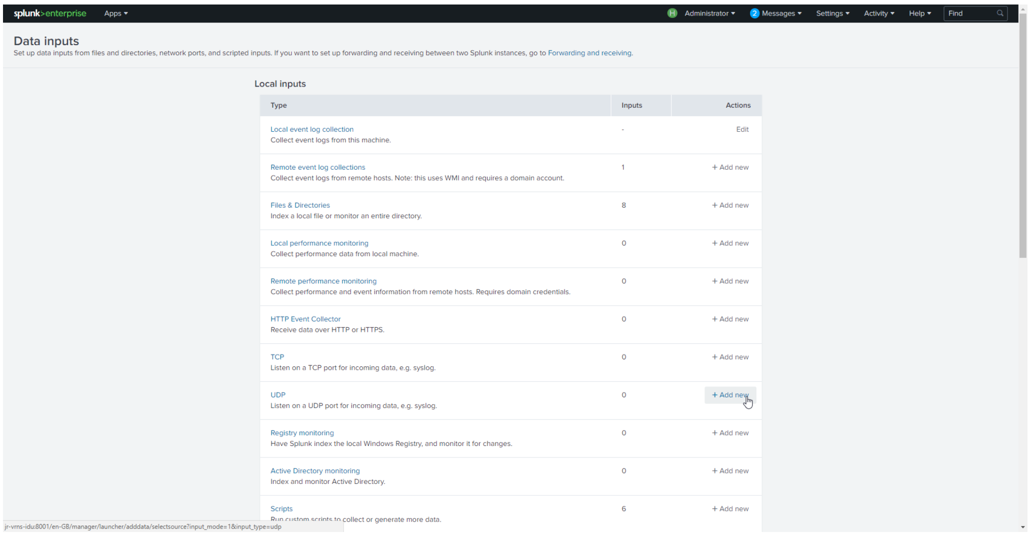
Add Data
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Splunk Apps
Apps and add-ons extend the capabilities of Splunk Enterprise.

Splunk Docs
Comprehensive documentation for Splunk Enterprise and for all other Splunk products.

3. From the menu at the top right of the page, select **Settings > Data Inputs**.

   The **Data Input** window is displayed.


splunk>enterprise
Apps ▾
Administrator ▾
2 Messages ▾
Settings ▾
Activity ▾
Help ▾
Find
jr-vrns-idu:8001/en-GB/manager/launcher/adddata/selectsource?input_mode=1&input_type=udp

Data inputs

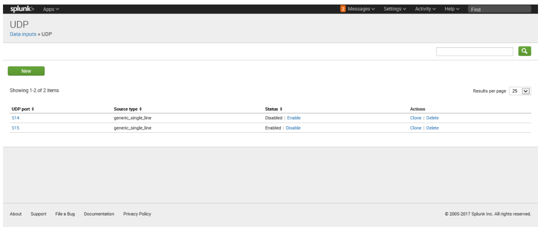
Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to Forwarding and receiving.

Local inputs

Type	Inputs	Actions
Local event log collection Collect event logs from this machine.	-	Edit
Remote event log collections Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.	1	+ Add new
Files & Directories Index a local file or monitor an entire directory.	8	+ Add new
Local performance monitoring Collect performance data from local machine.	0	+ Add new
Remote performance monitoring Collect performance and event information from remote hosts. Requires domain credentials.	0	+ Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	0	+ Add new
TCP Listen on a TCP port for incoming data, e.g. syslog.	0	+ Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	0	+ Add new
Registry monitoring Have Splunk index the local Windows Registry, and monitor it for changes.	0	+ Add new
Active Directory monitoring Index and monitor Active Directory.	0	+ Add new
Scripts Run custom scripts to collect or generate more data.	6	+ Add new

4. From the left menu, click **UDP**.

   The **UDP** window is displayed.



UDP

Data inputs » UDP

Showing 1-2 of 2 items

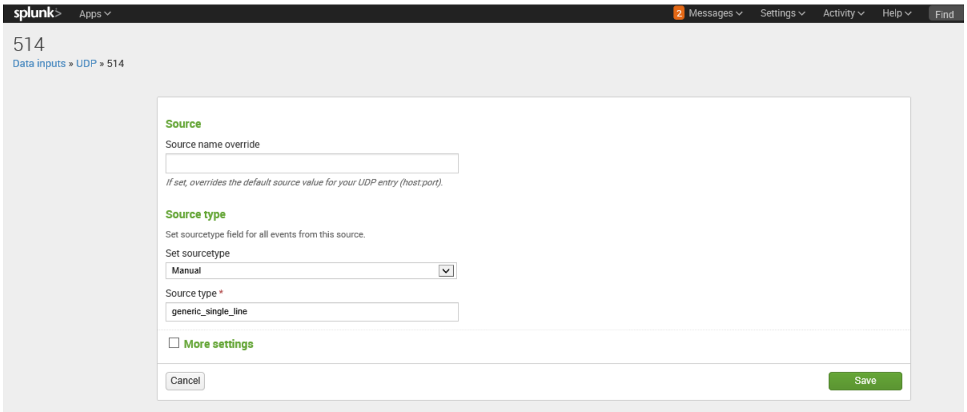
Results per page 25

UDP port	Source type	Status	Actions
514	generic_single_line	Disabled | Enable	Clone | Delete
515	generic_single_line	Enabled | Disable	Clone | Delete

© 2005-2017 Splunk Inc. All rights reserved.

5. In the UDP Port column, select the listener with the same port to where the alerts are sent. The listener's source window is displayed.

6. If the Source field is empty, then the source name is "UDP:<port number>" where port number is replaced by the actual port number. If the name exists (in the Source field), it is the source name to be used.



514

Data inputs » UDP » 514

Source

Source name override

If set, overrides the default source value for your UDP entry (host:port).

Source type

Set sourcetype field for all events from this source.

Set sourcetype: Manual

Source type *: generic_single_line

7. Click **Cancel** and exit the window.

Editing the Configuration File

You can configure an existing Splunk UDP listener by editing the necessary configuration files.

Do as follows:

1. Ensure that you have followed the procedure in *Verifying the Listener’s Source Name*.
2. Go to `$SPLUNK_HOME/etc/system/local`.
3. Open (or create) the **props.conf** file and add the following:

```
[sourcename]
TRANSFORMS-changesourcetype = varonis
```

   (Where `<sourcename>` is the source name of the listener)

4. Save and close the file.
5. Open (or create) the **Transforms.conf** file and add the following:

```
[varonis]
REGEX=DatAdvantage
FORMAT=sourcetype::varonis:ta
DEST_KEY=MetaData:Sourcetype
```

6. Save and close the file.
7. Restart Splunk Enterprise.

Optimizing for a Dedicated Index

If you configured a dedicated index for the app, you can optimize the app to utilize the index.

Do as follows:

1. Go to `$SPLUNK_HOME/etc/apps/varonisdls/default`.
2. Open the macros.conf file and edit the following line by replacing "*****" with your index name:

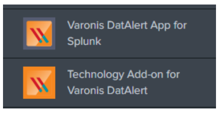
   ```
   definition = index=*
   ```

Verifying Installation

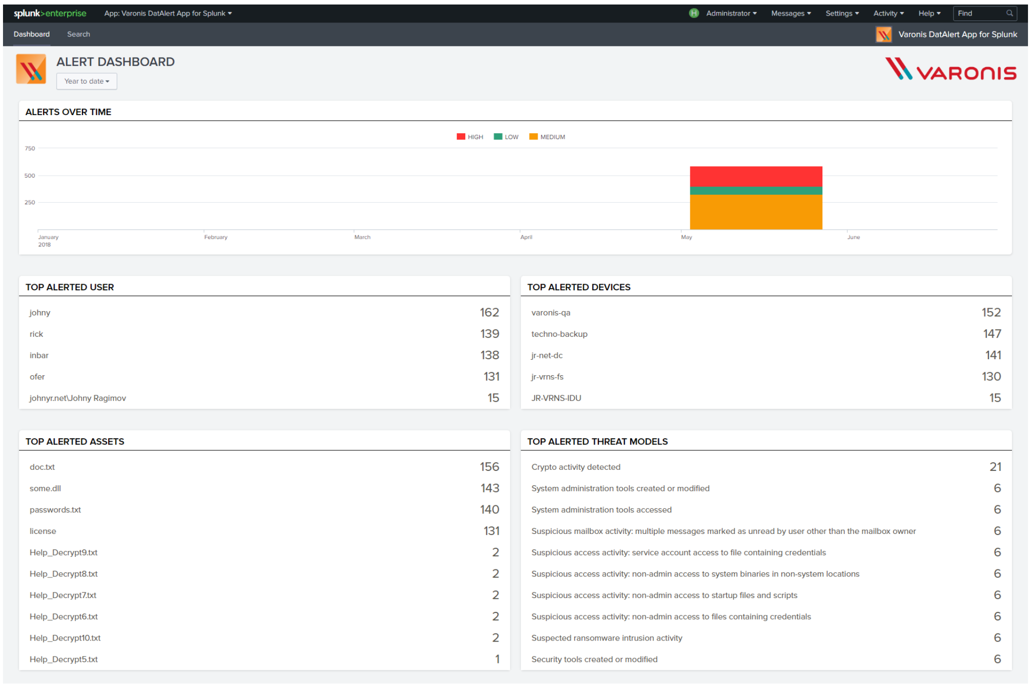
When you are done installing and configuring the apps, you should verify that the processes have been performed correctly.

When you are sure alerts are expected to arrive (hence the dashboard will contain data), do as follows:

1. Ensure that you have followed the procedure in *Configuring a New Splunk UDP Listener* or *Configuring an Existing Splunk UDP Listener*.
2. In your local Splunk installation, access the main page.
3. Verify that **Varonis DatAlert App for Splunk** and **Technology Add-on for Varonis DatAlert** are displayed on the left.


Varonis DatAlert App for Splunk
Technology Add-on for Varonis DatAlert

4. If the **Varonis DatAlert App for Splunk** is displayed, click it. The Alert dashboard is displayed.



TOP ALERTED USER

johny	162
rick	139
inbar	138
ofer	131
johnyr.net\Johny Ragimov	15

TOP ALERTED DEVICES

varonis-qa	152
techno-backup	147
jr-net-dc	141
jr-vrns-fs	130
JR-VRNS-IDU	15

TOP ALERTED ASSETS

doc.txt	156
some.dll	143
passwords.txt	140
license	131
Help_Decrypt9.txt	2
Help_Decrypt8.txt	2
Help_Decrypt7.txt	2
Help_Decrypt6.txt	2
Help_Decrypt10.txt	2
Help_Decrypt5.txt	1

TOP ALERTED THREAT MODELS

Crypto activity detected	21
System administration tools created or modified	6
System administration tools accessed	6
Suspicious mailbox activity: multiple messages marked as unread by user other than the mailbox owner	6
Suspicious access activity: service account access to file containing credentials	6
Suspicious access activity: non-admin access to system binaries in non-system locations	6
Suspicious access activity: non-admin access to startup files and scripts	6
Suspicious access activity: non-admin access to files containing credentials	6
Suspected ransomware intrusion activity	6
Security tools created or modified	6

5. If **Varonis DatAlert App for Splunk** is not displayed, or the dashboard is empty, review your installation procedures, or see *Troubleshooting*.

4 USING THE VARONIS DATALERT APP FOR SPLUNK

The Varonis DatAlert App for Splunk provides field extractions and dashboards that enable you to locate notable Varonis alerts directly from the Splunk user interface, and then drill down into Varonis DatAlert to get additional insights into the alert and the context in which it was generated.

Note: Before you start using the Varonis App for Splunk, ensure that it is installed and configured as described in *Installing the Varonis Technology Add-on and App for Splunk*.

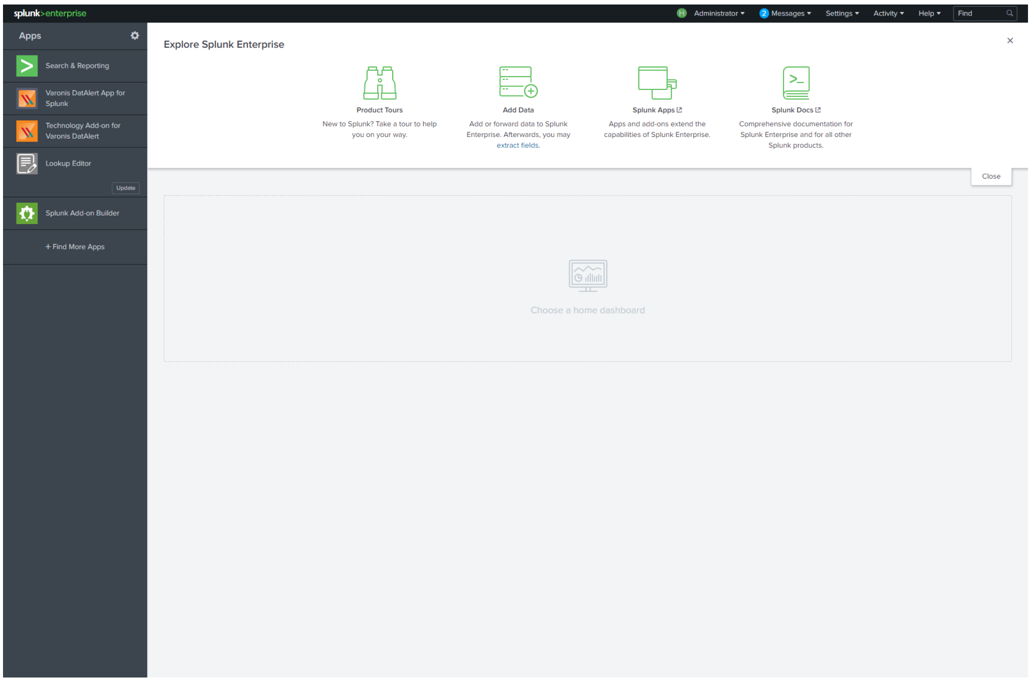
Note: To configure the Varonis DatAlert App for Splunk, the user must be the admin user.

Accessing the Varonis App for Splunk

You can access the Varonis App for Splunk to view its dashboards, locate notable Varonis alerts, and drill down into Varonis DatAlert.

To access the Varonis App for Splunk:

1. Ensure that you have followed the procedures in *Installing the Varonis Technology Add-on and App for Splunk*.
2. In your local Splunk installation, access the main page.



Explore Splunk Enterprise

Product Tours
New to Splunk? Take a tour to help you on your way.

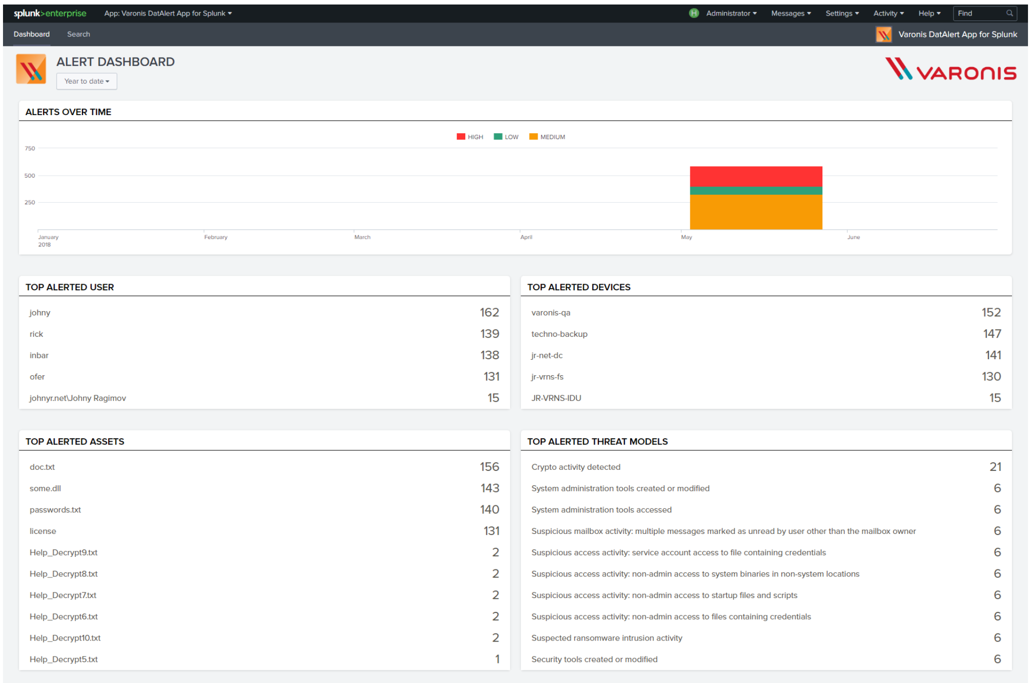
Add Data
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Splunk Apps
Apps and add-ons extend the capabilities of Splunk Enterprise.

Splunk Docs
Comprehensive documentation for Splunk Enterprise and for all other Splunk products.

3. From the left, click **Varonis DatAlert App for Splunk**.

   The **Alert Dashboard** is displayed.



ALERT DASHBOARD

ALERTS OVER TIME

TOP ALERTED USER	
johny	162
rick	139
inbar	138
ofer	131
johnyr.net\Johny Ragimov	15

TOP ALERTED DEVICES	
varonis-qa	152
techno-backup	147
jr-net-dc	141
jr-vrns-fs	130
JR-VRNS-IDU	15

TOP ALERTED ASSETS	
doc.txt	156
some.dll	143
passwords.txt	140
license	131
Help_Decrypt9.txt	2
Help_Decrypt8.txt	2
Help_Decrypt7.txt	2
Help_Decrypt6.txt	2
Help_Decrypt10.txt	2
Help_Decrypt5.txt	1

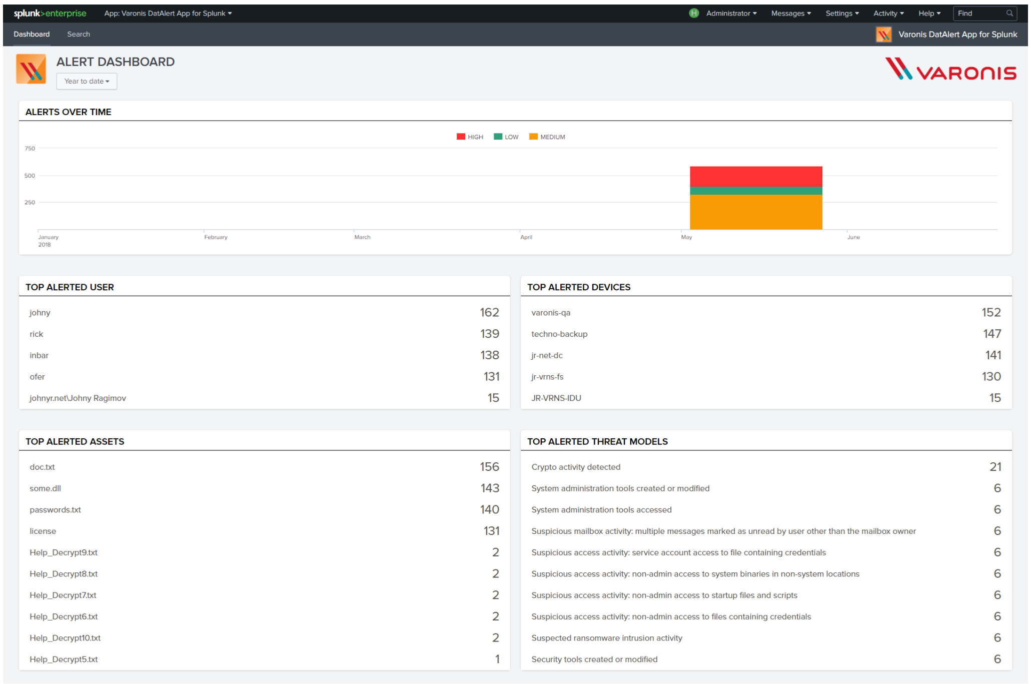
TOP ALERTED THREAT MODELS	
Crypto activity detected	21
System administration tools created or modified	6
System administration tools accessed	6
Suspicious mailbox activity: multiple messages marked as unread by user other than the mailbox owner	6
Suspicious access activity: service account access to file containing credentials	6
Suspicious access activity: non-admin access to system binaries in non-system locations	6
Suspicious access activity: non-admin access to startup files and scripts	6
Suspicious access activity: non-admin access to files containing credentials	6
Suspected ransomware intrusion activity	6
Security tools created or modified	6

Understanding the Alert Dashboard Window

The **Alert Dashboard** enables you to view "at a glance" the top alerted users, assets, devices, and threat models that match the specified search criteria/timeframe.

It enables you to quickly view and detect suspicious activity for further analysis. The Top Alerted Users, Top Alerted Assets, Top Alerted Devices and Top Alerted Threat Models areas of the dashboard each display *entities*, sorted by the number of alerts generated for that entity. The entity with the most alerts appears at the top of each list. The color represents the alert with the highest severity on this entity.

To view the **Alert Dashboard** window, ensure that you have accessed the Alerts Dashboard as described in *Accessing the Varonis App for Splunk*.



TOP ALERTED USER

johny	162
rick	139
inbar	138
ofer	131
johnyr.net\Johny Ragimov	15

TOP ALERTED DEVICES

varonis-qa	152
techno-backup	147
jr-net-dc	141
jr-vrns-fs	130
JR-VRNS-IDU	15

TOP ALERTED ASSETS

doc.txt	156
some.dll	143
passwords.txt	140
license	131
Help_Decrypt9.txt	2
Help_Decrypt8.txt	2
Help_Decrypt7.txt	2
Help_Decrypt6.txt	2
Help_Decrypt10.txt	2
Help_Decrypt5.txt	1

TOP ALERTED THREAT MODELS

Crypto activity detected	21
System administration tools created or modified	6
System administration tools accessed	6
Suspicious mailbox activity: multiple messages marked as unread by user other than the mailbox owner	6
Suspicious access activity: service account access to file containing credentials	6
Suspicious access activity: non-admin access to system binaries in non-system locations	6
Suspicious access activity: non-admin access to startup files and scripts	6
Suspicious access activity: non-admin access to files containing credentials	6
Suspected ransomware intrusion activity	6
Security tools created or modified	6

The **Alert Dashboard** comprises the following *elements*:

- Alerts Over Time - A stacked bar chart illustrating the dispersion of alerts matching the defined timeframe.
- Top Alerted Users - A list of the top alerted users sorted by the number of alerts.
- Top Alerted Assets - A list of the top alerted assets sorted by the number of alerts.
- Top Alerted Threat Models - A list of the top alerted threat models sorted by the number of alerts.
- Top Alerted Devices

> Note: The elements are independent of one another. For instance, the top alerted user may not be associated with the top alerted asset or threat model.

For additional options that you can perform on the elements, refer to the following (more information regarding these and other options can be found in the Splunk documentation): - A list of up the top alerted devices sorted by the number of alerts.

- ⤓ - Export a list of all alerts in the table to a CSV file.
- ⟳ - Refresh the contents of the list.

For more details, refer to the following:

- For information about **Alerts Over Time**, refer to *Viewing Alerts Over Time*.

- For information about the users, assets, threat models, and devices, refer to *Viewing the Drill-Down Dashboards*.

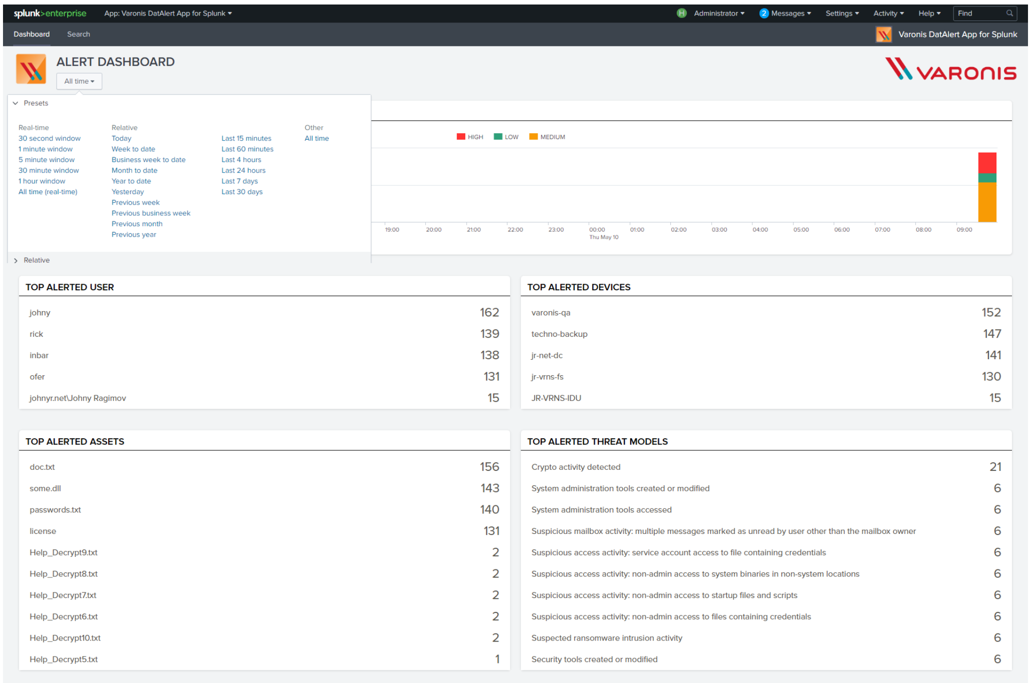
Understanding the Time Filters

Time filters enable setting time boundaries on your searches.

You can restrict a search with preset time ranges, create custom time ranges, specify time ranges based on date or date and time, or work with advanced features in the time filters.

> Note: Only a summary of the time filtering functionality is presented here. For a complete picture, refer to Splunk's documentation.

To access the time filters, from the top of the dashboard, click **All Time**. The time filter is displayed.



TOP ALERTED USER

johny	162
rick	139
inbar	138
ofer	131
johnyr.net\Johny Ragimov	15

TOP ALERTED DEVICES

varonis-qa	152
techno-backup	147
jr-net-dc	141
jr-vrns-fs	130
JR-VRNS-IDU	15

TOP ALERTED ASSETS

doc.txt	156
some.dll	143
passwords.txt	140
license	131
Help_Decrypt9.txt	2
Help_Decrypt8.txt	2
Help_Decrypt7.txt	2
Help_Decrypt6.txt	2
Help_Decrypt10.txt	2
Help_Decrypt5.txt	1

TOP ALERTED THREAT MODELS

Crypto activity detected	21
System administration tools created or modified	6
System administration tools accessed	6
Suspicious mailbox activity: multiple messages marked as unread by user other than the mailbox owner	6
Suspicious access activity: service account access to file containing credentials	6
Suspicious access activity: non-admin access to system binaries in non-system locations	6
Suspicious access activity: non-admin access to startup files and scripts	6
Suspicious access activity: non-admin access to files containing credentials	6
Suspected ransomware intrusion activity	6
Security tools created or modified	6

- Presets - Built-in time ranges options. You can select from a list of real-time windows, relative time ranges, or All Time (no time filtering).

  > Note: The remaining options are all custom time filters.

- Relative - Specify a custom time range for your search that is relative to the current time. You can select from the list of time range units, for example, *seconds ago*, *minutes ago*, etc.
- Real Time - Specify the start time for your real-time time range window.
- Date Range - Specify calendar dates in your search. You can choose among options to return events: *Between* a beginning and end date, *Before* a date, and *Since* a date.
- Date and Time Range - Specify calendar dates and times for the beginning and ending of your search.

- Advanced - Enables you to perform a more advanced search.

Viewing Alerts Over Time

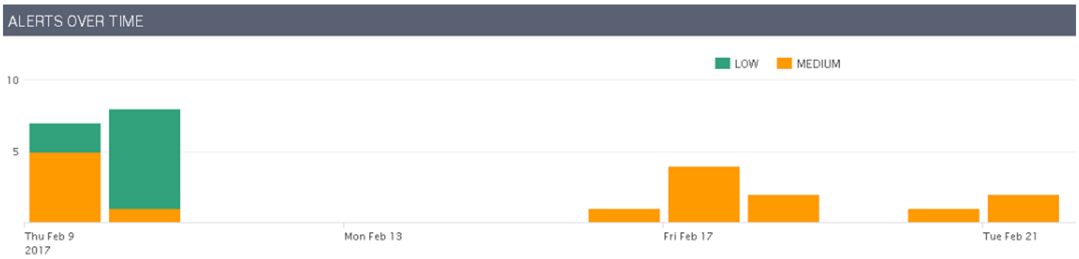
The Alerts dashboard enables you to view a stacked bar chart illustrating the dispersion of alerts over a specified period of time.

Each bar in the chart displays up to three severities, divided into stacks. Each stack represents a different severity - high, medium or low. The color code represents the severity of the alert:

- Red - High severity. Alerts with a severity of Emergency, Alert or Critical.
- Orange - Medium severity. Alerts with a severity of Error or Warning.
- Green - Low severity. Alerts with a severity of Notice, Informational and Debug.

To view alerts over time, do as follows:

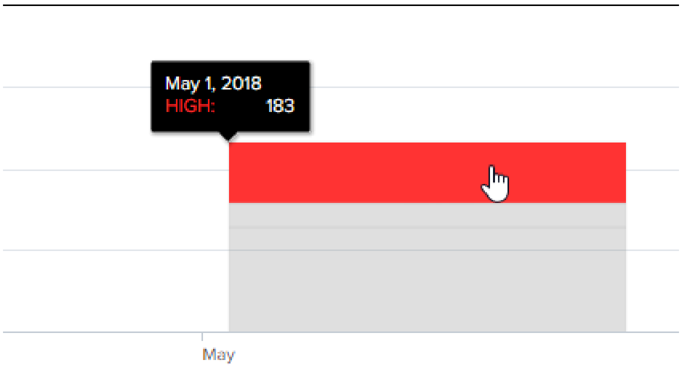
1. Ensure that you have followed the previous procedures in this chapter.
2. Access the Varonis App for Splunk, as described in *Accessing the Varonis App for Splunk*. The **Alerts Dashboard** window is displayed. The Alerts Over Time area is at the top.



3. To remove one or more severities from the bar chart, click the relevant severity from the legend on top of the chart. The severity is removed from the bar chart.

> Note: This may be useful if you want to focus on high severities only.

4. To view the number of alerts retrieved per severity, hover the mouse over the relevant bar. The number of alerts per severity is displayed.



5. To change the timeframe, click the **All time** drop-down list on the top of the page, and select one of the options. Refer to *Understanding the Time Filters*.

Viewing the Drill-Down Dashboards

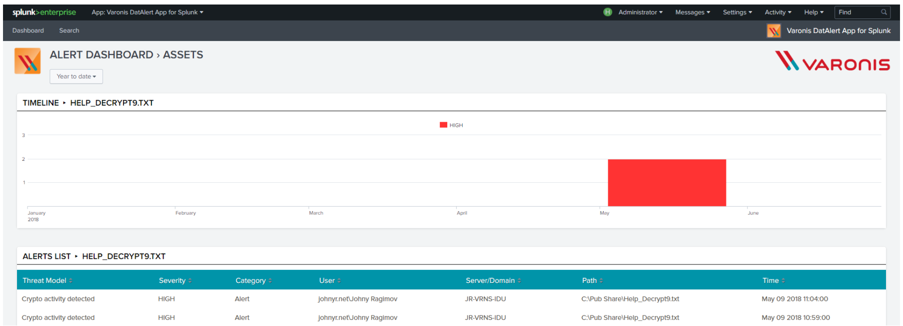
The drill-down dashboards enable you to take a closer look at selected entities in the Alerts dashboard.

By selecting a top alerted entity, either asset, user, threat model, or device, you can access a complete list of all alerts on that entity within the selected timeframe.

> Note: Alerts might be available in Splunk before they are available in the Varonis Web UI. If this is so, attempting to view the drill-down dashboards in the Varonis Web UI will display an error message.

To view the drill-down dashboards, do as follows:

1. Ensure that you have followed the procedure in *Viewing Alerts Over Time*.
2. Access the Varonis App for Splunk, as described in *Accessing the Varonis App for Splunk*.
   The **Alerts Dashboard** window is displayed.
3. Click the row of an entity for which you want a closer look.
   The drill-down dashboard for that entity is displayed. For example:



Threat Model	Severity	Category	User	Server/Domain	Path	Time
Crypto activity detected	HIGH	Alert	johnyr.net\Johny Ragimov	JR-VRNS-IDU	C:\Pub Share\Help_Decrypt9.txt	May 09 2018 11:04:00
Crypto activity detected	HIGH	Alert	johnyr.net\Johny Ragimov	JR-VRNS-IDU	C:\Pub Share\Help_Decrypt9.txt	May 09 2018 10:59:00

   The window comprises two areas:
   - Timeline - An "alerts over time" graph for the selected entity and timeframe.
   - Alerts List - A list of all alerts for that entity, listed with the user, severity, and rule.
4. If needed, change the timeframe of the alerts. Refer to *Understanding the Time Filters*.
5. To view detailed information regarding the alert, click the relevant alert in the list. Refer to *Viewing Detailed Information About Alerts*.

> Note: This step is only for customers running the Varonis Web Interface.

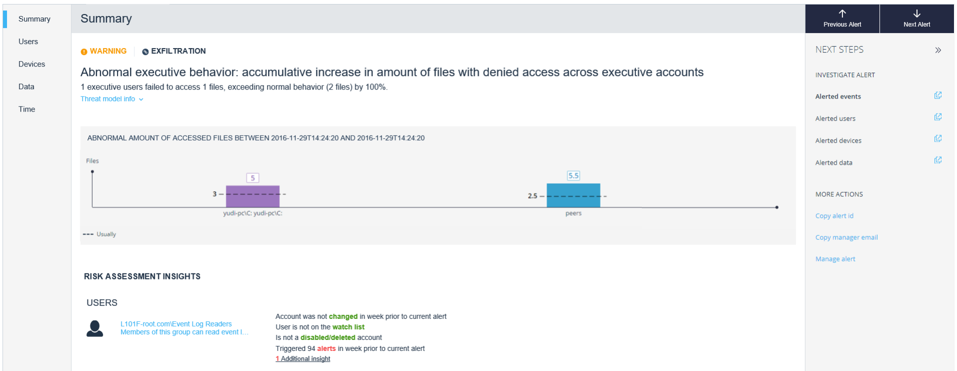
Viewing Detailed Information About Alerts

The Varonis Web Interface enables you view relevant information regarding alerts.

To view the detailed information about alerts:

1. Ensure that have followed the procedure in *Viewing the Drill-Down Dashboards*.
2. From the relevant drill-down dashboard, click the relevant alert.
   The Varonis Web Interface displays the **Alert Info** page. This window enables you to drill down and analyze the details of each alert that matches your search criteria. It enables you

to streamline your investigation and make a quick and informed decision regarding whether the activity is malicious or legitimate.



Abnormal executive behavior: accumulative increase in amount of files with denied access across executive accounts

1 executive users failed to access 1 files, exceeding normal behavior (2 files) by 100%.

ABNORMAL AMOUNT OF ACCESSED FILES BETWEEN 2016-11-29T14:24:20 AND 2016-11-29T14:24:20

L101F-root.com\Event Log Readers
Members of this group can read event l…

Account was not changed in week prior to current alert
User is not on the watch list
Is not a disabled/deleted account
Triggered 94 alerts in week prior to current alert

5 EVENT MAPPING

This list maps extracted Splunk fields to their Splunk CIM field and to the original DatAlert field that they represent.

Splunk Field	CIM Field	DatAlert Field	Description
act	N/A	Event Type	The type of event performed on the affected object.
cat	N/A	Always *Alert*	N/A
cef_Name	N/A	Event Type	The type of event performed on the affected object.
cef_Product	N/A	Always *DatAdvantage*	N/A
cef_Severity	severity	Severity	The severity of the DatAlert threat model which triggered the alert.

Splunk Field	CIM Field	DatAlert Field	Description
cef_Signature	N/A	Event Op Code	The ID of the event type. It enables searching and filtering log events by ID and not by the description provided in the event type. This placeholder is available but has no corresponding button. It must be added manually to the template.
cef_Vendor	N/A	Always *Varonis Inc.*	N/A
cef_cefVersion	N/A	Always *CEF:0*	Version is an integer and identifies the version of the CEF format. Use this information to determine what the other fields represent. The current CEF version is 0 (CEF:0).
cef_Version	N/A	DatAdvantage version	N/A
cn1	id	Rule ID	The unique identifier of the DatAlert threat model which triggered the alert.
cn1Label	N/A	Always *RuleID*	Used as a guideline as to the value stored in the corresponding custom field.

Splunk Field	CIM Field	DatAlert Field	Description
cnt	N/A	Threshold	The number of events which triggered the alert.
cs1	recipient	Mail Recipients	The recipients (to, cc and bcc) of the mail on which the event which triggered the alert occurred. Data is not collected for all event types. This placeholder is available but has no corresponding button. It must be added manually to the template.
cs1abel	N/A	Always *MailRecipients*	Used as a guideline as to the value stored in the corresponding custom field.
cs2	Signature, subject	Rule Name	The name of the DatAlert threat model which triggered the alert. For a complete list of threat models, see *#unique_34*.
cs2Label	N/A	Always *RuleName*	Used as a guideline as to the value stored in the corresponding custom field.

Splunk Field	CIM Field	DatAlert Field	Description
cs3	N/A	Attachment Name	The file name of the email attachment in the event which triggered the alert. Data is not collected for all event types. This placeholder is available but has no corresponding button. It must be added manually to the template.
cs3Label	N/A	Always *AttachmentName*	The file name of the email attachment in the event which triggered the alert. Data is not collected for all event types. This placeholder is available but has no corresponding button. It must be added manually to the template.
cs4	url	N/A	N/A
cs4label	N/A	Always *ClientAccessType*	Used as a guideline as to the value stored in the corresponding custom field.

Splunk Field	CIM Field	DatAlert Field	Description
cs5	N/A	Mailbox Access Type	Whether the acting object is the mailbox owner. Data is not collected for all event types. This placeholder is available but has no corresponding button. It must be added manually to the template.
cs5label	N/A	MailboxAccessType	Used as a guideline as to the value stored in the corresponding custom field.
cs6	file_acl, object_attrs	Changed Permissions	The specified changes in permissions. Data is not collected for all event types.
cs6label	N/A	Always *ChangedPermissions*	Used as a guideline as to the value stored in the corresponding custom field.
DatAdvantage	N/A	DatAdvantage version	N/A

Splunk Field	CIM Field	DatAlert Field	Description
deviceCustomDate1	N/A	Mail Date	The date and time of the mail on which the event which triggered the alert occurred. Data is not collected for all types of events. Format is according to the local time format of the Varonis server which issued the alert by the DSP Server/Probe/Collector. This placeholder is available but has no corresponding button. It must be added manually to the template.
dhost	src_nt_domain	File Server/Domain	Hostname of the machine on which the event which triggered the alert took place. Domain name for Directory Services events.
dpriv	user	Trustee	The account for which the permissions were changed. Data is not collected for all event types.
duser	User, src_user	Acting Object	The object name of the user/ computer that generated the event which triggered the alert.

Splunk Field	CIM Field	DatAlert Field	Description
dvc	src	Device IP Address	The IP address of the user from where the event originated.
dvchost	src	Device Name	The resolved host name of the Device IP, from where the event originated.
end	N/A	Event Time	The date and time of the event which triggered the alert. Format is according to the local time format of the Varonis server which issued the alert by the DSP Server/Probe/Collector.
externalId	id	Alert ID	The ID of the triggered alert within DatAlert.
filePath	file_path, uri_path, object_path	Access Path	N/A
filePermission	N/A	Permissions After Change	The permissions after the change. Data is not collected for all event types.

Splunk Field	CIM Field	DatAlert Field	Description
fileType	N/A	Mail Item Type	The Exchange object's item type on which the event which triggered the alert occurred. Data is not collected for all event types. This placeholder is available but has no corresponding button. It must be added manually to the template.
fname	file_name, object, query, url	Affected Object	The name of the object on which the event which triggered the alert occurred. For events on files, this is the file name and extension.
msg	url, body	Additional Data	The description of the event which triggered the alert, including event details such as date, time, etc..
oldFilePermission	N/A	Permissions Before Change	The permissions before the change. Data is not collected for all event types.
outcome	action, status, result	Event Status	Whether the event which triggered the alert succeeded or failed.

Splunk Field	CIM Field	DatAlert Field	Description
rt	N/A	Alert Time	The date and time at which the alert was triggered. Format is according to the local time format of the Varonis server which issued the alert by the DSP Server/Probe/Collector.
start	_timestamp	First Event Time	The date and time at which the first event to trigger the threshold alert occurred. Empty for alerts on single events. Format is according to the local time format of the Varonis server which issued the alert by the DSP Server/Probe/Collector.
suser	N/A	Mail Source	The sender (from) of the mail on which the event which triggered the alert occurred. Data is not collected for all event types. This placeholder is available but has no corresponding button. It must be added manually to the template.

6 CIM DATA MODEL MAPPING

Each DatAlert threat model is mapped to one or more Splunk CIM data models, matching the type of threat it detects. The DatAlert fields are therefore mapped to the target Splunk data models. For a list of DatAlert fields, see *Event Mapping*.

The following list displays the DatAlert threat models that are mapped to each Splunk CIM data model:

- **Intrusion Detection**
  - Abnormal access behavior: possible credential stuffing attack from a single source
  - Abnormal access behavior: possible distributed credential stuffing attack
  - Abnormal admin behavior: accumulative increase in amount of devices accessed
  - Abnormal admin behavior: accumulative increase in lockouts across admin accounts
  - Abnormal admin behavior: accumulative increase in lockouts for individual admin accounts
  - Abnormal admin behavior: atypical access to platform from geolocation
  - Abnormal admin behavior: unusual amount of devices accessed
  - Abnormal admin behavior: unusual amount of lockouts across admin accounts
  - Abnormal behavior: accumulative increase in amount of devices accessed
  - Abnormal behavior: accumulative increase in amount of public devices accessed
  - Abnormal behavior: accumulative increase in lockouts across end-user accounts
  - Abnormal behavior: accumulative increase in lockouts for individual end-user accounts
  - Abnormal behavior: accumulative increase in the amount of logons to devices
  - Abnormal behavior: accumulative increase in the number of logons to personal devices
  - Abnormal behavior: activity from blacklisted geolocation
  - Abnormal behavior: activity from new geolocation to the organization
  - Abnormal behavior: unreasonable geo-hopping
  - Abnormal behavior: unusual amount of configuration and backup files accessed

- Abnormal behavior: unusual amount of devices accessed
- Abnormal behavior: unusual amount of lockout across end-user accounts
- Abnormal behavior: unusual amount of logons to devices
- Abnormal behavior: unusual amount of logons to personal devices
- Abnormal behavior: unusual amount of public devices accessed
- Abnormal behavior: unusual amount of script files accessed
- Abnormal behavior: unusual amount of system files accessed
- Abnormal behavior: unusual number of failed DNS Queries
- Abnormal behavior: unusual number of users attempted to connect from a single external IP
- Abnormal computer behavior: accumulative increase in amount of devices accessed
- Abnormal computer behavior: computer account attempted to access a personal device for the first time
- Abnormal computer behavior: unusual amount of devices accessed
- Abnormal DNS reverse lookup requests to different IPs
- Abnormal executive behavior: accumulative increase in amount of script, configuration and backup files accessed across executive accounts
- Abnormal executive behavior: unusual amount of script, configuration and backup files accessed
- Abnormal service behavior: a dormant service account was reactivated
- Abnormal service behavior: accumulative increase in amount of devices accessed
- Abnormal service behavior: accumulative increase in lockouts across service accounts
- Abnormal service behavior: accumulative increase in lockouts for individual service accounts
- Abnormal service behavior: atypical access to platform from geolocation
- Abnormal service behavior: service account attempted to access a personal device for the first time
- Abnormal service behavior: service account logged on to a personal device for the first time
- Abnormal service behavior: unusual amount of devices accessed
- Abnormal service behavior: unusual amount of logons to personal devices
- Abnormal service behavior: unusual amounts of lockouts across service accounts
- Abnormal user behavior: password reset by an administrator followed by access to a computer other than the user’s personal computer

  - Abnormal user behavior: password reset by an administrator followed by access to a computer to which the user does not normally access
  - Credentials stuffing attack from an external source
  - DNS cache poisoning (birthday attack)
  - DNS cache snooping attack
  - Encryption downgrade attack
  - Failed privilege escalation was detected via vulnerability in Kerberos
  - Lockout: Multiple accounts locked out
  - Operation on a security tool failed
  - Operation on a system administration tool failed
  - Potential brute-force attack targeting a specific account
  - Potential identity theft based on downgraded encryption
  - Rapid brute-force attack targeting a specific account
  - Reconnaissance using DNS Zone Transfer
  - Security certificate activity by non-administrators
  - Security tools accessed
  - Security tools created or modified
  - Successful brute-force attack targeting a specific account
  - Successful login to an application by a user with a disabled Active Directory account
  - Successful privilege escalation was detected via vulnerability in Kerberos
  - Suspicious access activity: non-admin access to files containing credentials
  - Suspicious access activity: non-admin access to startup files and scripts
  - Suspicious access activity: service account access to file containing credentials
  - Suspicious mailbox activity: multiple messages marked as unread by user other than the mailbox owner
  - System administration tools accessed
  - System administration tools created or modified
- **Data Loss Prevention**

  - Abnormal admin behavior: access to atypical mailboxes
  - Abnormal behavior: access to an unusual amount of idle data
  - Abnormal behavior: access to an unusual amount of idle sensitive data
  - Abnormal behavior: accumulative increase in amount of idle and sensitive data accessed
  - Abnormal behavior: accumulative increase in amount of idle data accessed
  - Abnormal behavior: unusual amount of emails sent to a single recipient
  - Abnormal behavior: unusual amount of files with denied access
  - Abnormal behavior: unusual number of files deleted
  - Abnormal behavior: unusual number of messages marked as unread by a user other than the mailbox owner
  - Abnormal behavior: unusual number of sensitive files deleted
  - Abnormal executive behavior: accumulative increase in amount of files with denied access across executive accounts
  - Abnormal executive behavior: unusual amount of files with denied access across executive accounts
  - Abnormal service behavior: access to atypical files
  - Abnormal service behavior: access to atypical folders
  - Abnormal service behavior: access to atypical folders containing GDPR data
  - Abnormal service behavior: access to atypical mailboxes
  - Abnormal service behavior: atypical actions performed on mailbox owned by other users
  - Abnormal service behavior: atypical failure to access data
  - Access to an unusual number of idle GDPR files
  - Unusual number of GDPR files deleted or modified
  - Unusual number of GDPR files with denied access
- **Email**
  - Abnormal admin behavior: access to atypical mailboxes
  - Abnormal behavior: unusual amount of emails sent to a single recipient
  - Abnormal behavior: unusual number of messages marked as unread by a user other than the mailbox owner
  - Abnormal service behavior: access to atypical mailboxes

  - Abnormal service behavior: atypical actions performed on mailbox owned by other users
  - Creation: automatic forwarding of incoming messages on mailbox
  - Suspicious mailbox activity: multiple messages marked as unread by user other than the mailbox owner
- **Alerts**
  - Administrative or service account disabled or deleted
  - Administrative or service account reset
  - Creation: automatic forwarding of incoming messages on mailbox
  - Deletion: Active Directory containers, Foreign Security Principal, or GPO
  - Deletion: Multiple directory service objects
  - Executive account locked-out/disabled/deleted/password reset
  - Low and slow increase in number of idle GDPR files accessed
  - Membership changes: admin groups
  - Membership Changes: Service Accounts
  - Modification: Critical GPOs
  - Modification: Critical Organizational Units
  - Modification: GPO Security Settings
  - Permission changes on OU
  - Permission changes: Global Access Groups added to folder with significant GDPR data
  - Permission changes: global access groups added/removed
  - Permissions granted directly to user in directory services
  - Permissions granted directly to user in Windows file system
  - Successful login to an application by a user with a disabled Active Directory account
- **Change Analysis**
  - Administrative or service account disabled or deleted
  - Administrative or service account reset
  - Deletion: Active Directory containers, Foreign Security Principal, or GPO

  - Deletion: Multiple directory service objects
  - Executive account locked-out/disabled/deleted/password reset
  - Membership changes: admin groups
  - Membership Changes: Service Accounts
  - Modification: Critical GPOs
  - Modification: Critical Organizational Units
  - Modification: GPO Security Settings
  - Permission changes on OU
  - Permission changes: Global Access Groups added to folder with significant GDPR data
  - Permission changes: global access groups added/removed
  - Permissions granted directly to user in directory services
  - Permissions granted directly to user in Windows file system

- **Change Analysis (Account)**
  - Administrative or service account disabled or deleted
  - Administrative or service account reset
  - Deletion: Active Directory containers, Foreign Security Principal, or GPO
  - Deletion: Multiple directory service objects
  - Executive account locked-out/disabled/deleted/password reset
  - Membership changes: admin groups
  - Membership Changes: Service Accounts
  - Modification: Critical GPOs
  - Modification: Critical Organizational Units
  - Modification: GPO Security Settings
  - Permission changes on OU
  - Permissions granted directly to user in directory services

- **Change Analysis (Endpoint)**
  - Executive account locked-out/disabled/deleted/password reset
  - Permission changes: Global Access Groups added to folder with significant GDPR data
  - Permission changes: global access groups added/removed
  - Permissions granted directly to user in Windows file system
- **Malware**
  - Crypto activity detected
  - Data exfiltration via DNS tunneling
  - Encryption of multiple files
  - Exploitation software accessed
  - Exploitation software created or modified
  - File encrypted by ransomware
  - Immediate pattern detected: user actions resemble ransomware
  - Modification: Hosts file
  - Operation on a penetration testing or hacking tool failed
  - Operation on an exploitation tool failed
  - Past ransomware activity indicated by a residual ransomware note
  - Penetration testing and hacking tools accessed
  - Penetration testing and hacking tools created or modified
  - Suspected ransomware intrusion activity
  - Suspicious access activity: non-admin access to system binaries in non-system locations

7 ALERTS

You can view a description of the alerts received from DatAlert.

To view the alert descriptions, see *Behavioral Threat Model Quick Reference Chart*.

8 TROUBLESHOOTING

Learn about the common problems that may arise when installing, configuring, and using the Varonis App for Splunk, along with possible causes and solutions.

Connectivity Problems

Learn about common connectivity problems that may occur, along with possible causes and solutions.

No Alerts Displayed in App: Port and Protocol for Syslog Do Not Match

If no alerts are received by Splunk, ensure that the port and protocol match.

Problem	No alerts are received by Splunk.
Cause	Syslog can use both TCP and UDP and any port number. The ports for DatAlert and Splunk must be the same, and the protocol must be UDP. Therefore, a problem might arise if the user selected to use an existing listener with a different port or protocol.
Diagnosing the Problem	• Verify if alerts are received by searching in Splunk for `DatAdvantage`. • Check if the port and protocol are the same. Refer to *Configuring Syslog Message Forwarding* and *Configuring an Existing Splunk UDP Listener* (existing or new) for details.
Fixing the Problem	Ensure that the port and protocol match. Setting up a dedicated Splunk listener makes it easier to ensure a common port and protocol.

No Alerts Displayed in App: No Communication is Possible from Collectors to Splunk

If no alerts are received by Splunk, check with a network expert if communication using UDP on the selected port is possible between the Varonis Collector and the DSP, and the Splunk server.

Problem	No alerts are received by Splunk.
Cause	The network does not allow Syslog messages to be sent by the Varonis Connector and the DSP to the Splunk server, either due to routing issues or because a firewall blocks access.

Diagnosing the Problem	- Verify if alerts are received by searching in Splunk for `DatAdvantage`. - Try using the ping function from the DSP and from any Collector expected to send alerts to the Splunk server. If it works, use the logger tool (click *here*) to try to send a syslog message to Splunk using the command "`logger -l <splunk_address> -a <port> datAlert test`. Search Splunk for `DatAlert` to see if the message was received. - Use Wireshark to test if the alerts are sent by DatAlert. It is recommended to leave this step to your organization's networking experts.
Fixing the Problem	Check with a network expert if communication using UDP on the selected port is possible between the Varonis Collector and the DSP, and the Splunk server.

No Alerts Displayed in App: Source Type Identification Not Set Up When Using a Common Splunk Listener

If you are using a common listener and alerts are received by Splunk but are not displayed in the App, you can set up a dedicated Splunk listener for Varonis on a separate port.

Problem	The user selected to use a common listener and so alerts are received by Splunk but are not displayed in the App.
Cause	If the user needs to utilize a shared listener that will accept alerts from multiple sources, additional configuration must be applied in configuration files to help Splunk set the "sourcetype" correctly for the Varonis alerts.
Diagnosing the Problem	- Check if the user selected to use a common Splunk listener. - Verify that alerts are received by searching in Splunk for `DatAdvantage` - Verify that source type is not identified by searching for `sourcetype=varonis:ta`.
Fixing the Problem	- Set up a dedicated Splunk listener for Varonis on a separate port. - If the user must use a shared listener, refer to *Configuring an Existing Splunk UDP Listener*.

No Alerts Displayed in App: No Source Type Selected for a Dedicated Splunk Listener

If a dedicated listener is used and alerts are received by Splunk but are not presented in the App, you can reconfigure the dedicated Splunk listener.

Problem	The user selected to use a dedicated listener, and alerts are received by Splunk but are not presented in the App.
Cause	The user did not set the sourcetype correctly when configuring the listener.
Diagnosing the Problem	• Check if the user selected to use a dedicated Splunk listener. • Verify that alerts are received by searching in Splunk for `DatAdvantage`. • Verify that source type is not identified by searching for `sourcetype=varonis:ta`.
Fixing the Problem	Set up a dedicated Splunk listener.

Drill-Down Problems

Learn about common drill-down problems that may occur while using the Varonis App for Splunk.

"This Site Can't be Reached" or "Page Not Found" Errors When Drilling-Down to Varonis Web UI: Wrong Syslog Template

If you cannot drill down to view details about the alert in the Varonis Web UI, you may need to redefine the Syslog template.

Problem	The user is not able to drill down from an alert in Splunk to the Alert page in Varonis Web UI. The browser displays an error such as *This site can’t be reached* or *page not found*.
Cause	The user did not manually edit the Syslog template configured in DatAlert with the details regarding the Varonis Web UI.
Fixing the Problem	Refer to the step regarding manually editing the cs4 section of the template in *Defining a New Template*.

"This Site Can't be Reached" or "Page Not Found" Errors When Drilling-Down to DatAlert Web UI: Alerts Not Yet Available in the Varonis Web UI

If you cannot drill down to view details about an alert in the Varonis Web UI, the alerts may not be available yet in the Web UI.

Problem	The user is not able to drill down from an alert in Splunk to the Alert page in the Varonis Web UI. The browser displays an error such as *This site can’t be reached* or *page not found*.
Cause	Splunk received alerts as they are generated (real time for RTA, daily for UBA). For RTA alerts, Splunk therefore receives alerts before they arrive to the DSP and therefore to the Varonis Web UI.
Fixing the Problem	Wait until the alerts are available in the Web UI.

Escalation Requirements

Before escalating any issues that you have encountered, you are required to prepare details about the problem and configuration information.

Before escalating a ticket, prepare to do the following:

Connectivity Problems:

- Provide the Syslog template used in the DatAlert configuration.

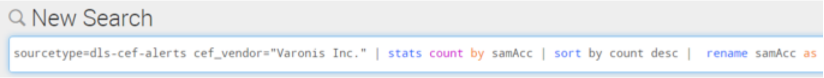
Drill-Down Problems:

- Provide the URL that the app tried to open when drilling-down.
- Provide the PROTOCOL (HTTP or HTTPS) and IP used by the Varonis Web UI.

Dashboard Problems:

At the bottom of the relevant pane (that does not work), do as follows:

- Click **Export** ⤓, and export the pane to CSV.
- Click **Open in Search** 🔍, and copy the search string.



```
sourcetype=dls-cef-alerts cef_vendor="Varonis Inc." | stats count by samAcc | sort by count desc |  rename samAcc as
```