



# VARONIS DATALEERT APP FOR IBM QRADAR

## Integration Guide

Publishing Information

Software version	2.0
Document version	1
Publication date	October 9, 2018

Copyright © 2005 - 2018 Varonis Systems Inc.

All rights reserved.

This information shall only be used in conjunction with services contracted for with Varonis Systems, Inc. and shall not be used to the detriment of Varonis Systems, Inc. in any manner. User agrees not to copy, reproduce, sell, license, or transfer this information without prior written consent of Varonis Systems, Inc.

This app incorporated parts of CEFUtils - Common Event Format Extraction Utilities by Igor Sher.

Other brands and products are trademarks of their respective holders.

---

# CONTENTS

<b>Chapter 1: Overview</b> .....	1
Prerequisites.....	1
Related Documentation.....	1
Target Audience.....	1
Support.....	1
<b>Chapter 2: Configuring DatAlert to Send Alerts to IBM QRadar</b> .....	3
Configuring Syslog Message Forwarding.....	3
Defining a New Template.....	4
Defining a Template for DatAlert Versions 6.3.170 to 6.4.174.....	4
Defining a Template for DatAlert Versions Prior to 6.3.170.....	6
Selecting an Alert Method for a Single Rule.....	9
Selecting an Alert Method for Multiple Rules.....	9
<b>Chapter 3: Uploading and Installing the Varonis App for IBM QRadar</b> .....	11
Downloading the Varonis App for IBM QRadar from IBM® Security App Exchange.....	11
Uploading the Varonis App to the IBM QRadar System.....	11
Installing the Varonis App for IBM QRadar.....	12
Retrieving the List of Collector IP Addresses.....	12
Configuring the Predefined Varonis Log Source.....	13
Configuring a Predefined Log Source.....	15
Adding a Bulk Log Source.....	17
Defining App Settings.....	18
Verifying the Installation.....	19
<b>Chapter 4: Mapping User-Defined DatAlert Rules to QRadar Events</b> .....	20
<b>Chapter 5: Using the Varonis App for IBM QRadar</b> .....	21
Accessing the Varonis App for IBM QRadar.....	21
Understanding the Alert Dashboard.....	22
Viewing Alerts Over Time.....	22
Viewing Alerts Per Entity.....	23
Viewing Detailed Information About Alerts.....	25
<b>Appendix A: Alert Field Mapping</b> .....	27
<b>Appendix B: Alerts</b> .....	35
<b>Appendix C: Troubleshooting</b> .....	36
No Data in Varonis DatAlert App for IBM QRadar.....	36
Outgoing Links from Detailed Dashboard Pages are Not Linking to the Varonis Web UI.....	36
Clicking a Row in a Dashboard Widget Does Not Direct Me to the Detailed Dashboards.....	37
Null Values Are Displayed in the DatAlert App for IBM QRadar.....	37
Determining Whether the Syslog Message Originally Included NULL Values.....	38
Determining Whether the Custom Event Properties are Accurately Defined.....	38

# 1

## OVERVIEW

This document describes the installation, configuration, and standard usage of the Varonis DatAlert App for IBM QRadar®.

This app enables integrating the Varonis DatAlert functionality into IBM QRadar. Using the app, you can locate notable Varonis alerts directly from the IBM QRadar console, and then drill down to view additional insights into the alert and the context in which it was generated. Additionally, the app includes field extractions that assist users in querying and visualizing Varonis alerts using QRadar and that enable correlating these alerts with other events collected by QRadar.

### Prerequisites

Before following the procedures described in this guide, ensure that you meet the following prerequisites:

- The following must be installed and running on your company's server:
  - IBM QRadar version 7.3.0 patch 2 or higher
  - DatAdvantage 6.3.256
  - To view a detailed analysis of each alert, the Varonis Web Interface 6.3.150 or higher must be installed. If the Varonis Web Interface is not installed, the Varonis **Alert Info** page will not be displayed.
- To configure DatAlert to send alerts to IBM QRadar, the user must have the *DatAlert Configuration user* and *Reports View user* role or the *Web UI user* role.
- To configure the Varonis App for IBM QRadar, the user must be the admin user.

### Related Documentation

- DatAlert User Guide
- DatAdvantage User Guide
- Varonis Web Interface User Guide
- DatAlert Triage Guide

### Target Audience

This user guide is intended for the following users:

- System Administrators managing the organization's deployments
- Security Analysts using IBM QRadar to manage security alerts
- Information Security management

### Support

For information on how to contact support, refer to the Varonis Support page at:

<https://www.varonis.com/services/support>.

## 2

# CONFIGURING DATALEERT TO SEND ALERTS TO IBM QRADAR

The following procedures detail the required workflow for configuring DatAlert to send alerts to the Varonis App for IBM QRadar:

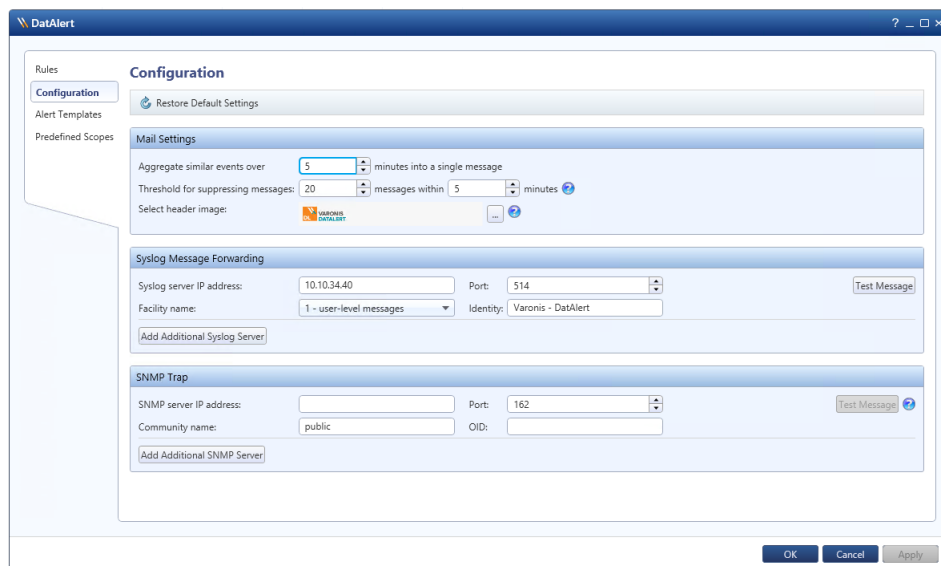
- [Configuring Syslog Message Forwarding](#)
- [Defining a New Template](#)
- [Selecting an Alert Method for a Single Rule](#)
- [Selecting an Alert Method for Multiple Rules](#)

**Note:** To configure DatAlert to send alerts to IBM QRadar, the user must have the *DatAlert Configuration user* and *Reports View user* role or the *Web UI user* role.

## Configuring Syslog Message Forwarding

To configure the Syslog server address in DatAlert:

1. In DatAdvantage, select **Tools > DatAlert**.  
The **DatAlert** window is displayed.
2. From the left menu, select **Configuration**.



The screenshot shows the DatAlert Configuration window. The left sidebar has 'Configuration' selected. The main area is titled 'Configuration' and contains three sections: 'Mail Settings', 'Syslog Message Forwarding', and 'SNMP Trap'. The 'Syslog Message Forwarding' section is highlighted and contains the following fields: 'Syslog server IP address' (10.10.34.40), 'Port' (514), 'Facility name' (1 - user-level messages), and 'Identity' (Varonis - DatAlert). There are 'Test Message' and 'Add Additional Syslog Server' buttons. The 'SNMP Trap' section has 'SNMP server IP address', 'Port' (162), 'Community name' (public), and 'OID' fields, with 'Test Message' and 'Add Additional SNMP Server' buttons. At the bottom right are 'OK', 'Cancel', and 'Apply' buttons.

3. In the Syslog Message Forwarding pane, set the following:
  - *Syslog server IP address* - The IP address of the IBM QRadar server on which to collect events.
  - *Port* - Enter **514**.
4. Click **OK**.

## Defining a New Template

Templates define the format of the alert messages sent from DatAlert, using Syslog, to IBM QRadar. This section describes how to define a relevant template that provides the information in the format expected by the Varonis App for IBM QRadar.

Depending on the installed version, the following templates are available:

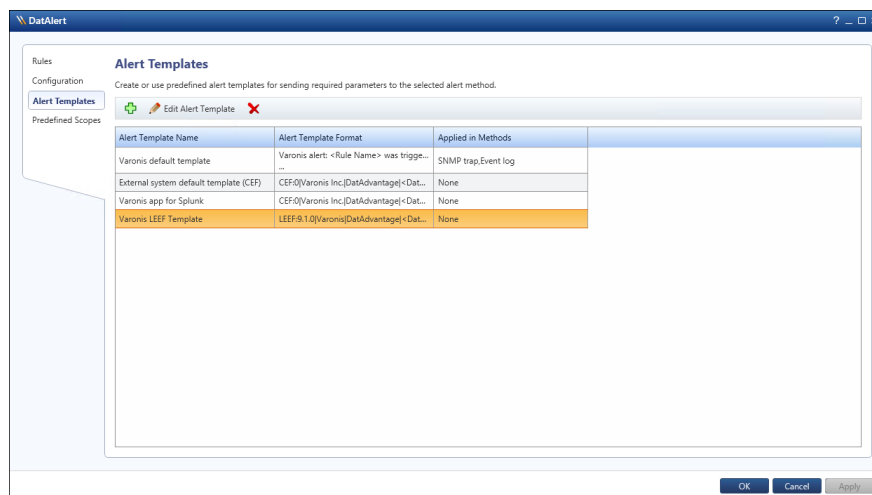
Installed Version	Template	Relevant Procedure
DatAlert versions 6.3.200 and higher	Varonis LEEF Template	<a href="#">Defining a Template for DatAlert Versions 6.3.258, 6.4.175, and Higher</a>
DatAlert versions 6.3.170 up to (and not including) 6.3.200	A template must be defined	<a href="#">Defining a Template for DatAlert Versions 6.3.170 to 6.4.174</a>
DatAlert versions prior to 6.3.170	A template must be defined	<a href="#">Defining a Template for DatAlert Versions Prior to 6.3.170</a>

### Defining a Template for DatAlert Versions 6.3.170 to 6.4.174

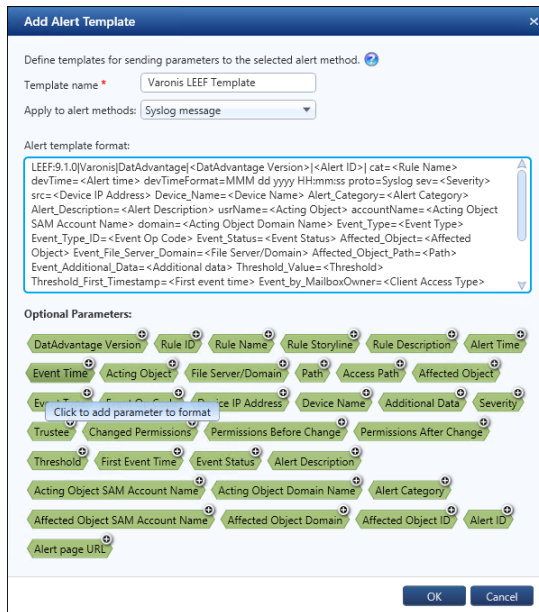
To define a template for DatAlert versions 6.3.170 to 6.4.174:

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.



3. Click the green plus sign . The **Add Alert Template** dialog box is displayed.

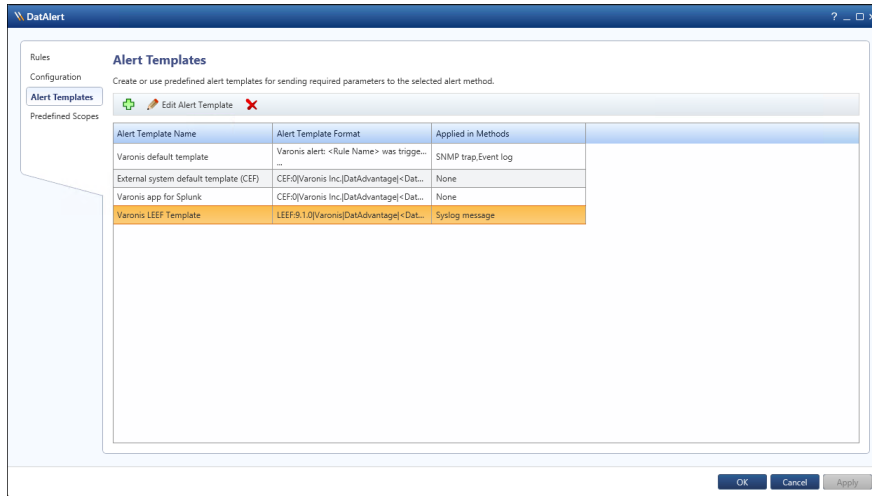


4. Set the following:
  - *Template name* - Enter a unique name for the alert template (for example, Varonis LEEF Template), comprising up to 40 characters.
  - *Apply to alert methods* - From the drop-down list, select **Syslog message**.
5. Go to <https://info.varonis.com/hubfs/docs/qradar/Varonis-QRadar-LEEF-Template.txt> and download the template file.
6. Copy and paste the string in the file into the **Alert template format** text box (the template includes dynamic parameters that are replaced with the actual data when the alert is sent).



7. In the **Add Alert Template** dialog box, click **OK**.
8. Verify that the new template is displayed in the templates table:





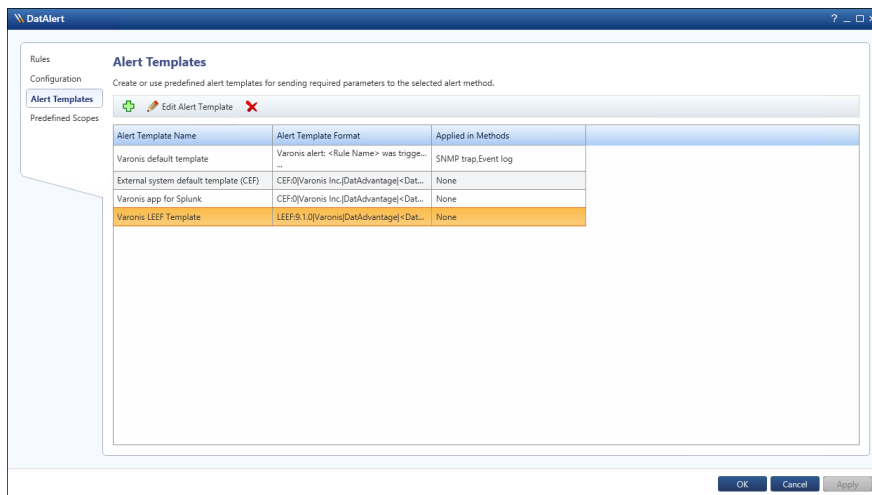
9. Click **OK**.

### Defining a Template for DatAlert Versions Prior to 6.3.170

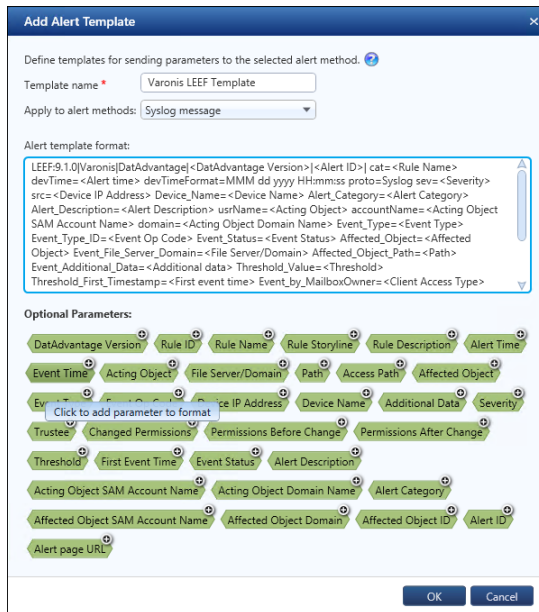
To define a template for DatAlert versions prior to 6.3.170:

1. Ensure that you have followed the procedure in [Configuring Syslog Message Forwarding](#).
2. In DatAlert, from the left menu, click **Alert Templates**.

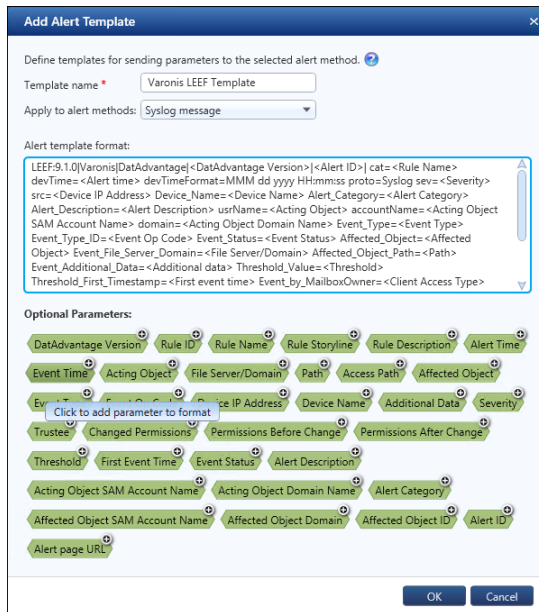
The **Alert Templates** window is displayed.



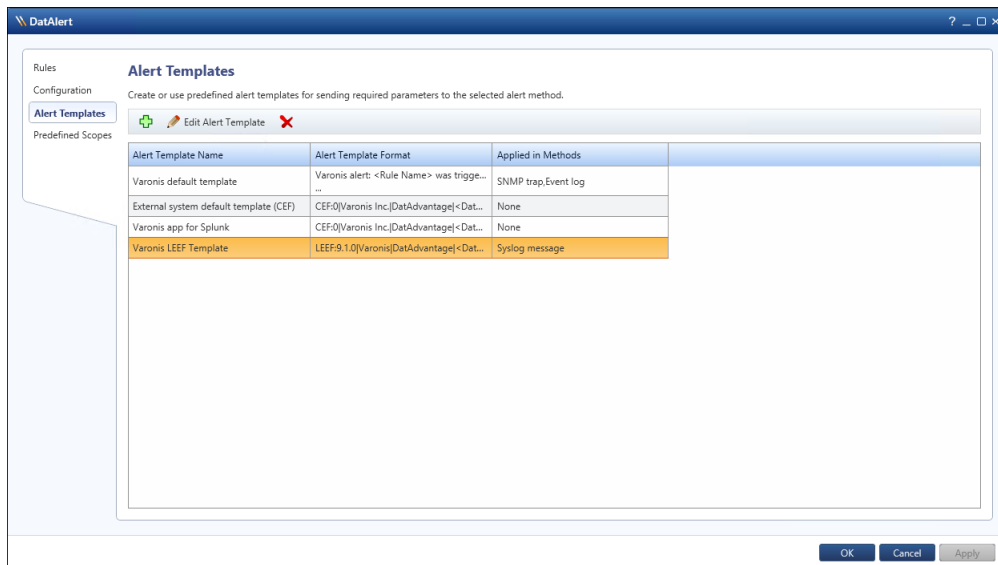
3. Click the green plus sign .
- The **Add Alert Template** dialog box is displayed.



4. Do the following:
  - *Template name* - Enter a unique name for the alert template (for example, Varonis LEEF Template), comprising up to 40 characters.
  - *Apply to alert methods* - From the drop-down list, select **Syslog message**.
5. Go to <https://info.varonis.com/hubfs/docs/qradar/Varonis-QRadar-LEEF-Template.txt> and download the template file.
6. In the **Alert template format** text box, do the following:
  - a. Copy and paste the string in the file into the **Alert template format** text box (the template includes dynamic parameters that are replaced with the actual data when the alert is sent).



- b. In the **Alert template format** text box, manually edit the string as follows:
  - Change `<Alert page URL>` to `<PROTOCOL>://<DLS_IP_ADDRESS>/DatAdvantage/#/app/analytics/entity/Alert/<Alert ID>`
    - Where `<PROTOCOL>` is either HTTP or HTTPS, depending on whether Varonis Web UI uses HTTPS or HTTP
    - Where `<DLS_IP_ADDRESS>` is the IP address or host name of the server running the Varonis Web UI
    - Where `AlertID` is the ID of the triggered alert within DatAlert.
7. In the **Add Alert Template** dialog box, click **OK**.
8. Verify that the new template is displayed in the Alerts Templates table:



9. Click **OK**.

## Selecting an Alert Method for a Single Rule

An alert method is the means by which the alert is transferred. For the Varonis App for IBM QRadar, the alert is transferred by creating a Syslog message.

To select an alert method for a single rule:

1. Ensure that you have followed the procedure in [Configuring Syslog Message Forwarding](#).
2. In DatAlert, in the Rules table, select the relevant rule and then from the toolbar, click **Edit Rule**.

The **Edit Rule** window for the selected rule is displayed.

3. From the left menu, select **Alert Method**.

The **Alert Method** pane is displayed.

4. Select **Syslog message**.

The screenshot shows the 'Add Rule' dialog box with the 'Alert Method' tab selected. On the left, a navigation menu lists 'General', 'Who (Acting Object)', 'Where (Affected Object)', 'What (Event Details)', 'When (Event Time)', and 'Alert Method'. The 'Alert Method' pane contains the following options:

- Mail to recipients: [Text Field] (Use comma as separator) [Send Test Mail]
- Event log
- Syslog message
- SNMP trap
- Include in DatAdvantage reports
- Executable Script

Below these options, there is a section for running a script:

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

Script path: [Text Field] [Browse]

Run the script with credentials:

User name: [Text Field] [Browse]

Password: [Text Field] [Browse]

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

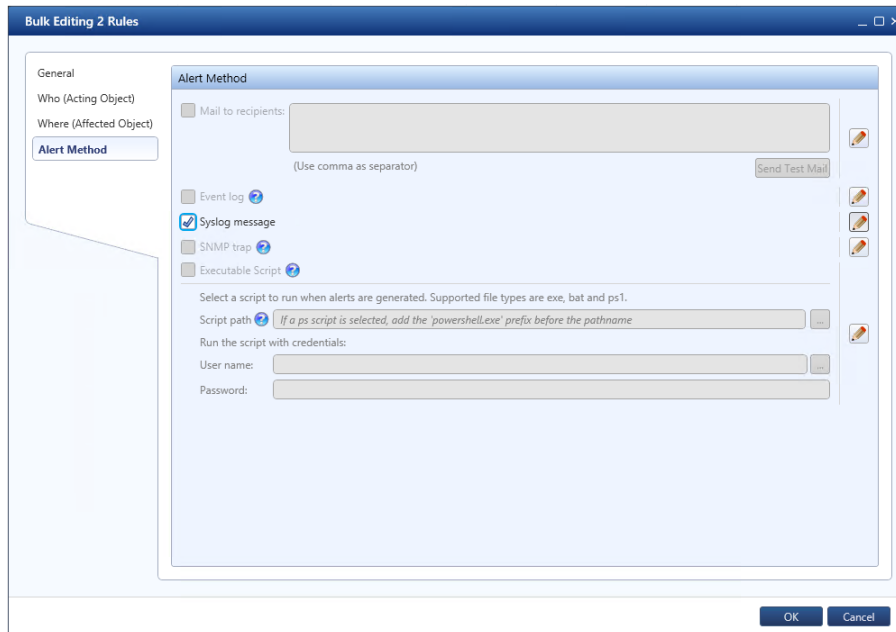
5. Click **OK**.

## Selecting an Alert Method for Multiple Rules

You can select an alert method for multiple rules simultaneously. (For a single rule only, refer to [Selecting an Alert Method for a Single Rule](#)).

To select an alert method for multiple rules:

1. Ensure that you have followed the procedure in [Configuring Syslog Message Forwarding](#).
2. In DatAlert, in the rules table, select the rules and then from the toolbar, click **Edit Rule**. The **Edit Rule** window 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.



5. Click **OK**.

# 3

## UPLOADING AND INSTALLING THE VARONIS APP FOR IBM QRADAR

- [Downloading the Varonis App for IBM QRadar from IBM® Security App Exchange](#)
- [Uploading the Varonis App to the IBM QRadar System](#)
- [Installing the Varonis App for IBM QRadar](#)
- [Retrieving the List of Collector IP Addresses](#)
- [Configuring a Predefined Log Source](#)
- [Defining App Settings](#)
- [Verifying the Installation](#)

### Downloading the Varonis App for IBM QRadar from IBM® Security App Exchange

To download the Varonis App for IBM QRadar from IBM Security App Exchange:

1. Ensure that you have followed the procedures in [Configuring DatAlert to Send Alerts to IBM QRadar](#).
2. From IBM Security App Exchange, click the following link to download the ZIP file containing the Varonis App for QRadar:  

```
https://exchange.xforce.ibmcloud.com/hub/extension/7d7d4f706e8f6f251cc42cfb6b01928f
```
3. Save the ZIP file in a temporary folder.

### Uploading the Varonis App to the IBM QRadar System

To upload the Varonis App to the IBM QRadar console:

**Note:** For more information about uploading apps using the IBM® Security QRadar® Extension Management tool, see [https://www.ibm.com/support/knowledgecenter/SS42VS\\_7.3.1/com.ibm.apps.doc/t\\_Qapps\\_upload.html](https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.apps.doc/t_Qapps_upload.html).

1. Ensure that you have followed the procedure in [Downloading the Varonis App for IBM QRadar from IBM® Security App Exchange](#).
2. In the IBM QRadar Security Intelligence console, select the Admin tab.
3. In the Admin tab, select **Extensions Management**.  
The **Extensions Management** window is displayed.
4. In **Extensions Management** window, do the following:
  - a. Click **Add**.  
The **Add a New Extension** dialog box is displayed.
  - b. Browse to and select the previously downloaded ZIP file.
  - c. To install the app immediately, select the *Install immediately* check box.
  - d. Click **Add**.

The app is uploaded. If you have chosen to install the app immediately, the contents of the app are displayed and the app is installed.

## Installing the Varonis App for IBM QRadar

To install the Varonis App for IBM QRadar:

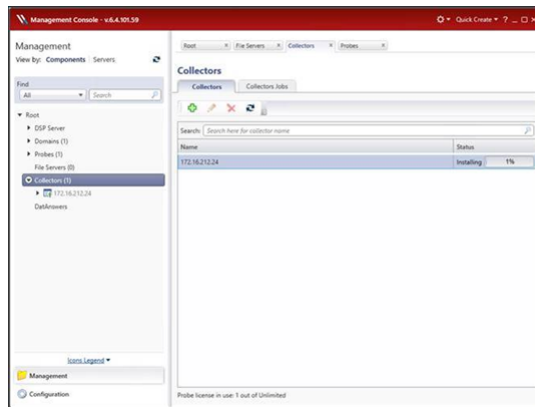
**Note:** The following procedure is relevant only for users who did *not* immediately install the app following upload. For more information about installing apps using the IBM® Security QRadar® Extension Management tool, see [https://www.ibm.com/support/knowledgecenter/en/SS42VS\\_7.3.1/com.ibm.apps.doc/t\\_Qapps\\_install.html](https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.1/com.ibm.apps.doc/t_Qapps_install.html).

1. Ensure that you have followed the procedure in [Uploading the Varonis App to the IBM QRadar System](#).
2. In the IBM QRadar Security Intelligence console, select the Admin tab.
3. In the Admin tab, select **Extensions Management**.  
The **Extensions Management** window is displayed.
4. From the **Extensions Management** window, select the Varonis App and click **Install**.  
The app's contents are compared to the contents found in deployment. If an item already exists, you can select to overwrite the item or keep the existing item.
5. The app is installed and displayed in the **Extensions Management** window.
6. Prior to using the app, clear your browser cache and refresh the browser.

## Retrieving the List of Collector IP Addresses

This procedure describes how to (manually) retrieve the list of Collector IP addresses in the Management Console.

1. In the Management Console, from the navigation pane, select **Management > Root > Collectors** and then **Root > Probes**.



2. Review the Collectors and Probes. For each, determine its IP address. If listed using a host name, use the command `nslookup <hostname>` to retrieve the IP address.
3. Do one of the following:
  - If there is one Collector installed on the Varonis Data Security Platform, configure a standard log source. Refer to [Configuring a Predefined Log Source](#).
  - If there is at least one Collector or Probe that is not installed on the Varonis DNS Server, configure a bulk log source. Refer to [Adding a Bulk Log Source](#).

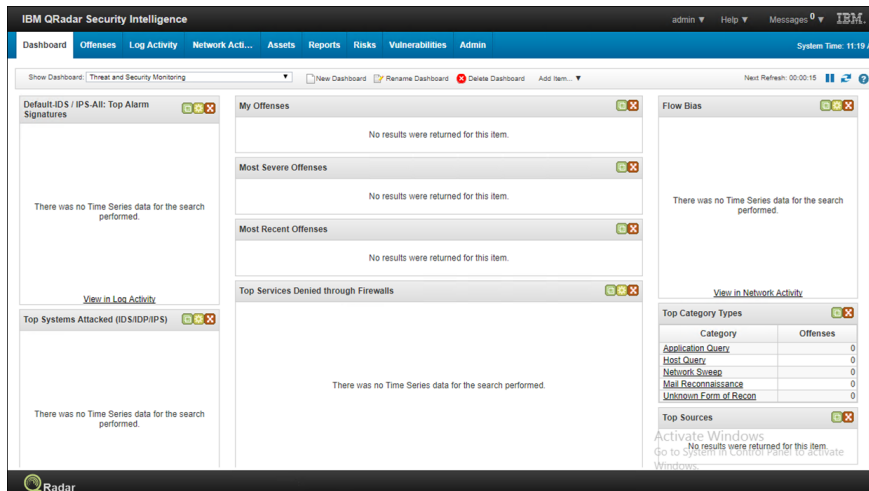
## Configuring the Predefined Varonis Log Source

**Important:** You must configure Log Sources for the Data Security Platform and for each Collector. Real-time alerts are generated from Collectors, whereas DatAlert Analytics alerts are generated from the Data Security Platform; therefore both are required. Varonis recommends creating two Log Sources for each device; one where the Log Source Identifier is set as the IP, and the other is set as the HOSTNAME. For example, a Collector named **Varonis-Collector** with IP **10.0.0.1**, will have two log sources. The first Log Source will have **Varonis-Collector**, whereas the second one will have **10.0.0.1**.

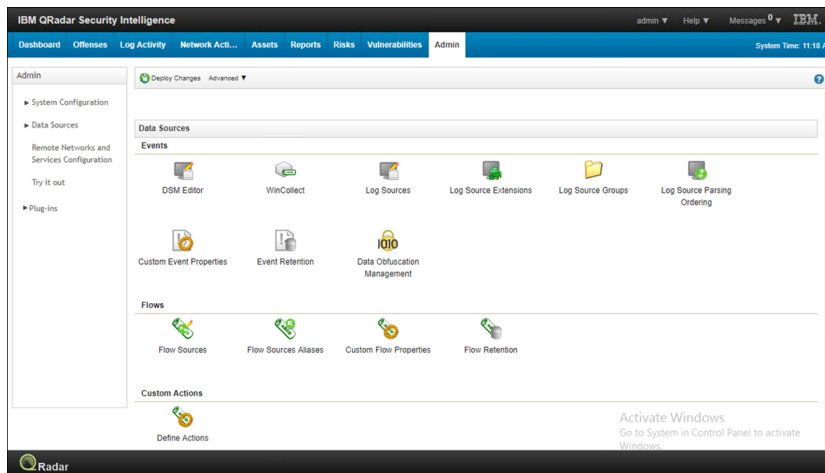
To configure the predefined Varonis Log Source:

1. Open IBM QRadar and enter your access credentials.  
The **IBM QRadar Security Intelligence** window is displayed, open to the Dashboard.

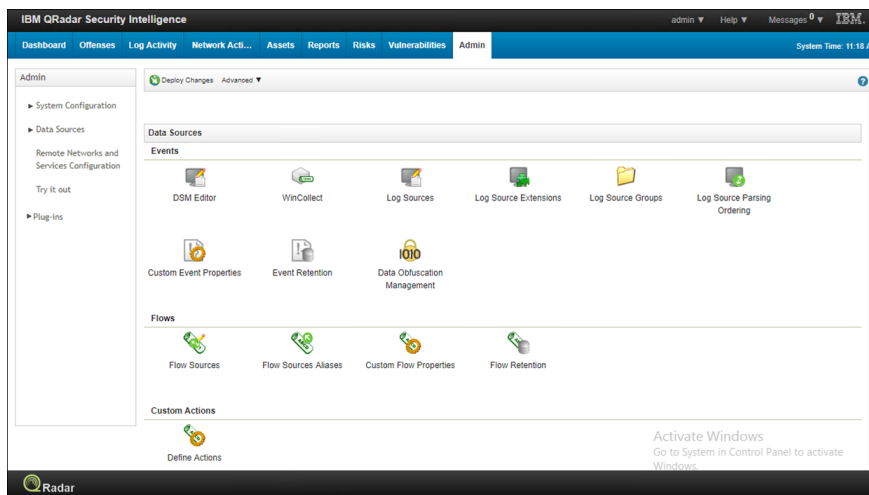




2. Click the **Admin** tab.



3. In the **Data Sources** area, in the **Events** row, click **Log Sources**.



The **Log Sources** window is displayed.

4. Locate the Varonis DatAlert log source.
5. Edit the Log Source Identifier to be the IP of the DSP.
6. Click **Save**.

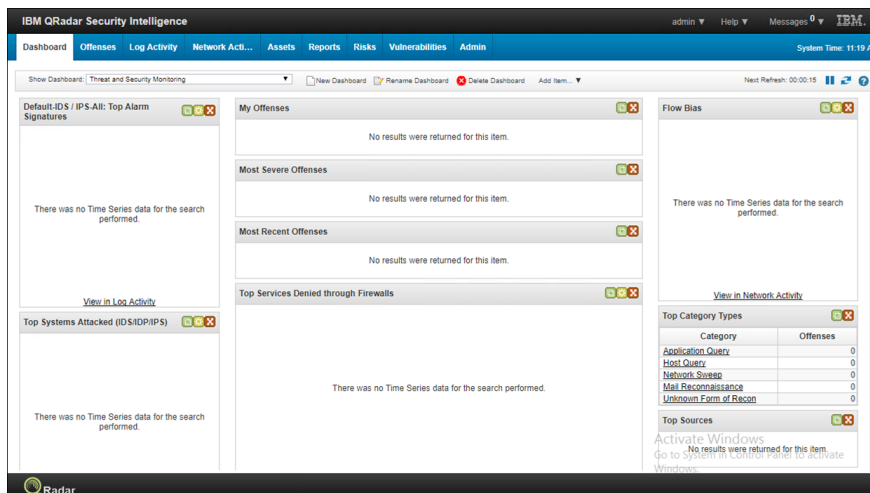
## Configuring a Predefined Log Source

**Important:** You must configure **Log Sources** for the **Data Security Platform** and for each **Collector**. Real-time alerts are generated from **Collectors**, whereas **DatAlert Analytics** alerts are generated from the **Data Security Platform**; therefore both are required. **Varonis** recommends creating two **Log Sources** for each device; one where the **Log Source Identifier** is set as the **IP**, and the other is set as the **HOSTNAME**. For example, a Collector named **Varonis-Collector** with IP **10.0.0.1**, will have two log sources. The first Log Source will have **Varonis-Collector**, whereas the second one will have **10.0.0.1**.

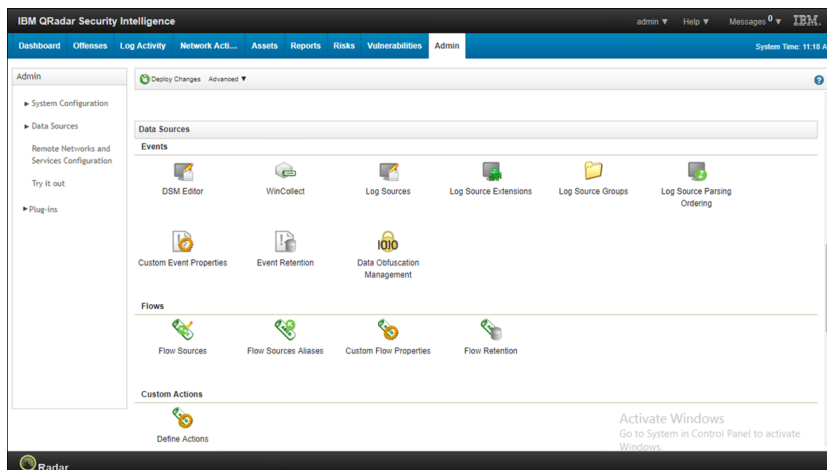
To configure a predefined log source, do as follows:

1. Open IBM QRadar and enter your access credentials.

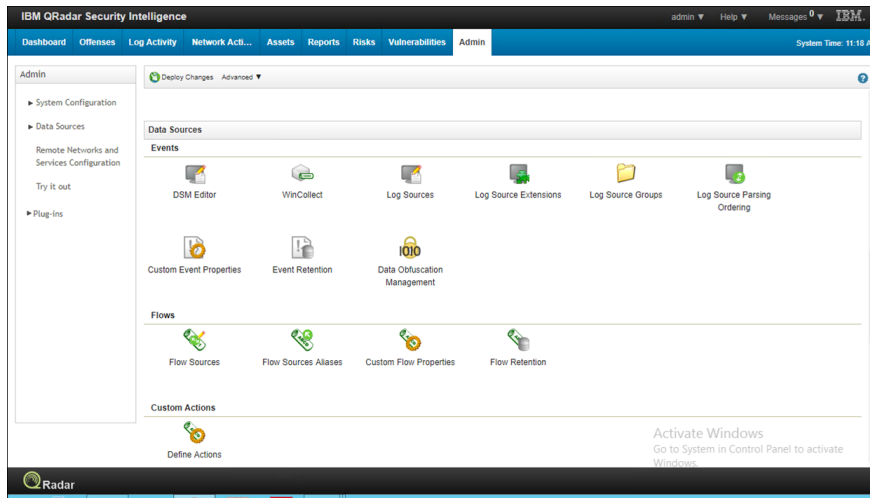
The **IBM QRadar Security Intelligence** window is displayed, open to the **Dashboard**.



2. Click the **Admin** tab.



3. In the **Data Sources** area, in the **Events** row, click **Log Sources**.



The **Log Sources** window is displayed.

4. Click **Add**.

The **Add a Log Source** dialog box is displayed.

**Add a log source**

Log Source Name

Log Source Description

Log Source Type

Protocol Configuration

Log Source Identifier

Enabled

Credibility

Target Event Collector

Coalescing Events

Incoming Payload Encoding

Store Event Payload

Log Source Extension

Please select any groups you would like this log source to be a member of:

5. Do as follows:

- *Log Source Name* - Enter a suitable name (i.e.Varonis DL).
- *Log Source Description* - Enter a brief description of the log source.
- *Log Source Type* - Select Varonis DSM.
- *Protocol Configuration* - Leave at the default (Syslog).
- *Log Source Identifier* - Enter the IP of the DSP that is sending alerts.
- *Enabled, Credibility, Target Event Collector, Coalescing Events, Incoming Payload Encoding, Store Event Payload, Log Source Language* - leave all these at the default.
- *Log Source Extension* - Select **VaronisDSMCustom\_ext**.

6. Click **Save**.  
A new row listing the new log source is displayed in the **Log Sources** window.
7. If a message appears prompting you to deploy changes, click the **Deploy Changes** button at the top.

### Adding a Bulk Log Source

To add multiple log sources, do as follows:

1. Click the **Admin** tab.
2. Under Data Sources, click **Log Sources**.  
The **Log Sources** window is displayed.
3. Click **Bulk Actions**, and in the drop-down list, click **Bulk Add**.  
The **Add a bulk log source** is displayed.
4. Enter the details:
  - *Bulk Log Source Name* - Enter a suitable name (i.e. Varonis DL Bulk).
  - *Log Source Type* - Select **Varonis DSM**.
  - *Protocol Configuration* - Leave at the default (Syslog).
  - *Enabled*, *Credibility*, *Target Event Collector*, *Coalescing Events*, *Store Event Payload*, *Log Source Language* - Leave all these at the default.
  - In the Host table at the bottom, do one of the following:
    - Create a text file that contains one Collector IP address and the IP address of the Varonis DSP server per line and upload it using the File Upload tab.
    - In the Manual tab, enter each collector IP as collected in [Retrieving the List of Collector IP Addresses](#). To do so, enter each IP address in the Host entry box and click the **Add Host** button. The IP address will be displayed in the Host table.

Screenshot:

**Add a bulk log source**

Bulk Log Source Name:

Log Source Type:

Protocol Configuration:

Enabled:

Credibility:

Target Event Collector:

Coalescing Events:

Store Event Payload:

Log Source Language:

File Upload:  Manual:

Enter the host name or IP of the host you wish to add

Host:


Add	Host
<input checked="" type="checkbox"/>	192.168.1.21
<input checked="" type="checkbox"/>	192.168.1.22

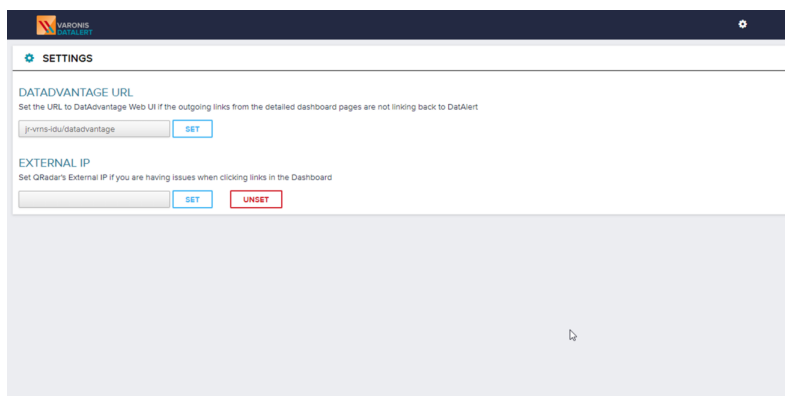
⚠ You have 0 of an allowable 500 saved Log Sources associated with this Bulk Log Source  
You have 2 new Log Sources selected to be added  
Log Sources can be deleted from the Log Sources screen

5. Click **Save**.

## Defining App Settings

To define settings in the Varonis DataAlert App for IBM QRadar:

1. [Access the Varonis App for IBM QRadar.](#)
  2. In the DataAlert dashboard, click the Settings icon .
- The **Settings** window is displayed.



3. To ensure that outgoing links from the detailed dashboard pages are linking back to DataAlert, do the following:
  - a. In the DataAdvantage URL field, enter the URL of the Varonis Web Interface.
  - b. Click **Set**.
4. To resolve issues when clicking links in the dashboard, in the External IP area, enter QRadar's external IP address and click **Set**.

## Verifying the Installation

This procedure describes how to verify the installation. Do as follows:

- Under **Admin > Log Sources**, check that the Varonis DatAlert log source is found. The **Status** column should indicate *success*.

Name	Desc	Status	Protocol	Group	Log Source Type	Enabled	Log Source Identifier	Target Destination	Credibility	Autodisc	Last Event Time	Creation Date	Modification Date
Varonis DL	Varonis DatAlert Alert	Success	Syslog		Varonis	True	192.168...	eventcol...	5	False	Sep 19, 2017	Jul 19, 2017	Aug 23, 2017

- Wait for DatAlert to send a syslog message to IBM QRadar, and in the **Log Activity** tab, search for Varonis DatAlert.

IBM QRadar Security Intelligence

Dashboard | Offenses | Log Activity | Network Activity | Assets | Reports | Risks | Vulnerabilities | Admin | Varonis DL

Search: Quick Search | Save Filters | Save Presets | Control | Filter Presets | Power | Admin

Quick Filter: Varonis DL

Start Time: 9/19/2017 11:05:43 AM | End Time: 9/19/2017 11:10:00 AM | Update

View: Select An Option | Display: Default (Normalized) | Results Limit: 1,000

Current Filter: Quick Filter > Varonis DL (Clear Filter)

Current Statistics: Total Events: 16 (113 MB Total) | Compressed Data Files Searched: 0 (0 MB Total) | Duration: 26.868ms | Data Files Searched: 2 (207.762 Total) | Indexed File Count: 1 (469.162 Total) | [View Details](#)

Records Matched Over Time

Records Matched Over Time

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Severity
Suspicious access activity - non-admin access to system binaries in non-system locations	Varonis DL	1	Sep 19, 2017 11:07:57 AM	User Activity	192.168.1.20	N/A	192.168.1.20	N/A	N/A	High
Creation: automatic forwarding of incoming messages on mailbox	Varonis DL	1	Sep 19, 2017 11:07:57 AM	User Activity	192.168.1.20	N/A	192.168.1.20	N/A	N/A	High
Suspicious mailbox activity: mailbox messages marked as unread by user other than the mailbox owner	Varonis DL	1	Sep 19, 2017 11:07:57 AM	User Activity	192.168.1.20	N/A	192.168.1.20	N/A	N/A	High
Suspicious ransomware intrusion activity	Varonis DL	1	Sep 19, 2017 11:07:57 AM	User Activity	192.168.1.20	N/A	192.168.1.20	N/A	N/A	High
Privilege escalation and handling tools created or modified	Varonis DL	1	Sep 19, 2017 11:07:57 AM	User Activity	192.168.1.20	N/A	192.168.1.20	N/A	N/A	High
System administration tools created or modified	Varonis DL	1	Sep 19, 2017 11:07:57 AM	User Activity	192.168.1.20	N/A	192.168.1.20	N/A	N/A	High
System administration tools accessed	Varonis DL	1	Sep 19, 2017 11:07:57 AM	User Activity	192.168.1.20	N/A	192.168.1.20	N/A	N/A	High
Suspicious access activity: service account access to file containing credentials	Varonis DL	1	Sep 19, 2017 11:07:57 AM	User Activity	192.168.1.20	N/A	192.168.1.20	N/A	N/A	High
Suspicious access activity: non-admin access to backup files and scripts	Varonis DL	1	Sep 19, 2017 11:07:57 AM	User Activity	192.168.1.20	N/A	192.168.1.20	N/A	N/A	High
Suspicious access activity: non-admin access to files containing credentials	Varonis DL	1	Sep 19, 2017 11:07:57 AM	User Activity	192.168.1.20	N/A	192.168.1.20	N/A	N/A	High
Modification: Critical O/S files	Varonis DL	1	Sep 19, 2017 11:07:57 AM	User Activity	192.168.1.20	N/A	192.168.1.20	N/A	N/A	High
Permissions granted directly to user in Windows file system	Varonis DL	1	Sep 19, 2017 11:07:57 AM	User Activity	192.168.1.20	N/A	192.168.1.20	N/A	N/A	High
Security certificate activity by non-administrators	Varonis DL	1	Sep 19, 2017 11:07:57 AM	User Activity	192.168.1.20	N/A	192.168.1.20	N/A	N/A	High

# 4

## MAPPING USER-DEFINED DATALEERT RULES TO QRADAR EVENTS

To map user-defined DataAlert rules to QRadar events:

1. Locate the **Unknown** event in QRadar's Log Activity screen.
2. Right-click the event and select **View in DSM Editor**.  
The DSM Editor opens.
3. Select the **Event Mappings** tab.  
The **Event Mappings** tab is displayed.
4. To create a new event mapping:
  - a. Click the plus sign (+).  
The **Create a new Event Mapping** dialog box opens.
  - b. In the **Event ID** field, enter the name of the relevant rule.
  - c. In the **Category** field, enter the rule category.
  - d. Click the **Choose Event** link to create a new Event Categorization to assign to the rule.  
The **Event Categorizations** dialog box opens.
  - e. In the **Event Categorizations** dialog box, click the **Create New QID Record** button.
  - f. Enter the name and description of the rule in the relevant fields.
  - g. In the **Log Source Type** field, enter your log source. This is usually **Varonis DSM**.
  - h. From the **High Level Category** and **Low Level Category** drop-down lists, select the relevant categories.
  - i. From the **Severity** drop-down list, select the rule's severity. This is the severity defined in Varonis DataAlert.
  - j. Click **Save** to save your changes and close the dialog box.
  - k. In the **Event Categorizations** dialog box, select the added rule from the grid and click **OK**.
  - l. In the **Create a new Event Mapping** dialog box, click **Create**.  
  
The dialog box closes and the **DSM Editor** window is displayed.
5. In the DSM Editor, click **Save**.

# 5

## USING THE VARONIS APP FOR IBM QRADAR

The following procedures provide instructions on using the Varonis App for IBM QRadar. Refer to the following sections:

- [Accessing the Varonis App for IBM QRadar](#)
- [Understanding the Alert Dashboard](#)
- [Viewing Alerts Over Time](#)
- [Viewing Alerts Per Entity](#)
- [Viewing Detailed Information About Alerts](#)

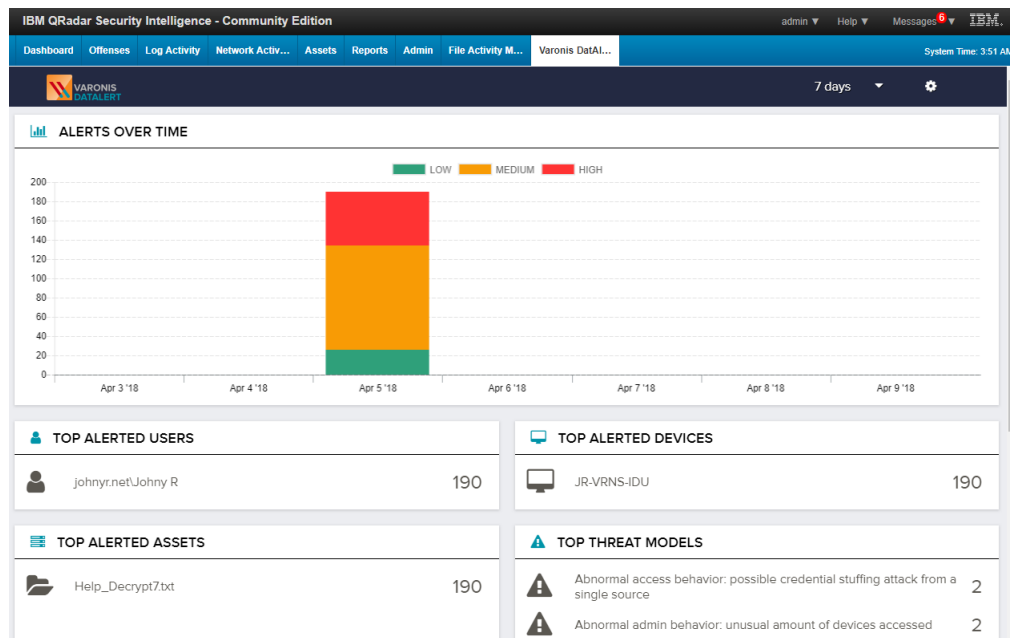
**Note:** Ensure that the Varonis App for QRadar is installed, as described in [Uploading and Installing the Varonis App for IBM QRadar](#).

### Accessing the Varonis App for IBM QRadar

To access the Varonis App for IBM QRadar:

1. Ensure that you have followed the procedures in [Uploading and Installing the Varonis App for IBM QRadar](#).
2. In the IBM QRadar Security Intelligence console, select the Varonis DataAlert tab at the top of the page.

The Varonis DataAlert app opens, displaying the dashboard.





## Understanding the Alert Dashboard

The DatAlert dashboard provides an "at a glance" view of the top alerted users, assets, devices and threat models that match the specified search timeframe. It enables you to quickly view and detect suspicious activity for further analysis.

The 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* - A list of up the top alerted devices sorted by the number of alerts.

In the Top Alerted Users, Assets, Devices and Threat Models widgets, the entity with the most alerts appears at the top of each list.

**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.

## Viewing Alerts Over Time

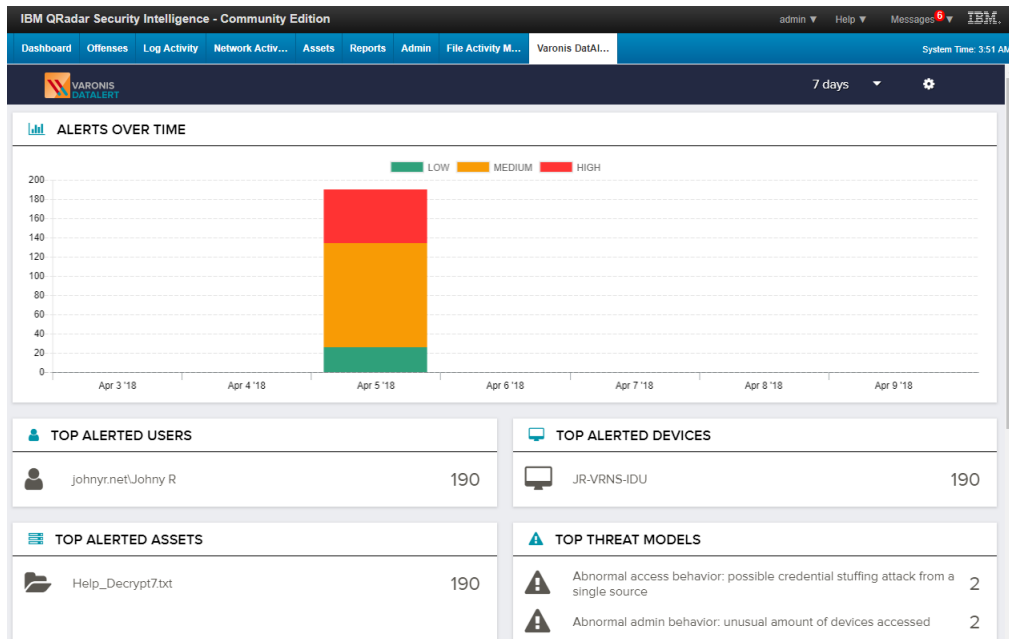
You can view a stacked bar chart illustrating the dispersion of alerts over a specified period of time. Each bar in the chart displays up to three severities, divided into stacks. Each stack represents a different severity - high, medium or low. The color code represents the severity of the alert:

- *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

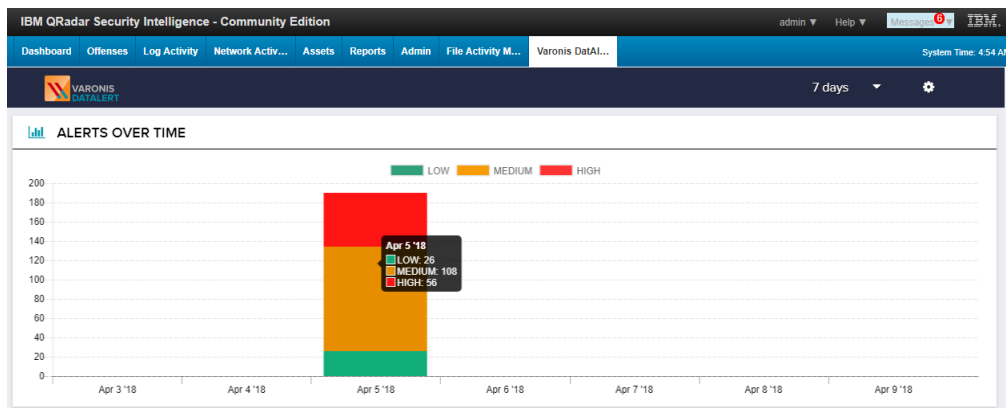
Depending on the timeframe specified, a bar in the chart can represent a single day (minimal display) or a month (maximum display).

To view alerts over a specified timeframe:

1. [Access the Varonis App for IBM QRadar.](#)  
The dashboard is displayed. The Alerts Over Time area is at the top of the page.



2. To change the timeframe, select the relevant time period from the Time drop-down list at the top of the page.
3. To view the number of alerts retrieved per severity, hover the mouse over the relevant bar. The number of alerts per severity is displayed.

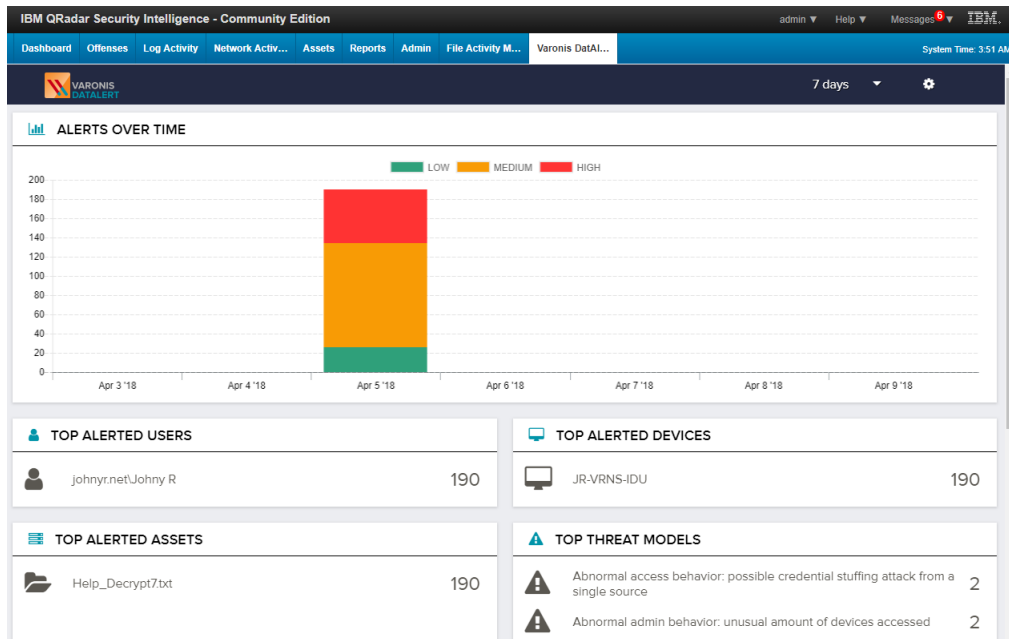


## Viewing Alerts Per Entity

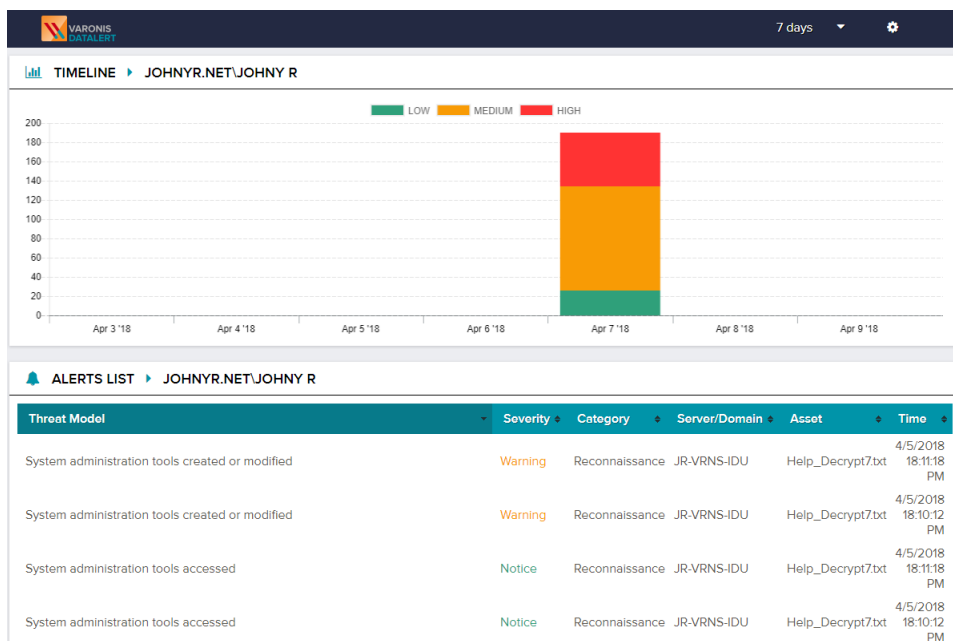
The dashboard enables you to select a top alerted entity to view a complete list of alerts on that entity for the selected timeframe.

To view alerts per entity:

1. [Access the Varonis App for IBM QRadar.](#)  
The dashboard is displayed.



- In the relevant top alerted widget, select the required entity. A new tab opens, displaying a timeline and a complete list of alerts on the selected entity.



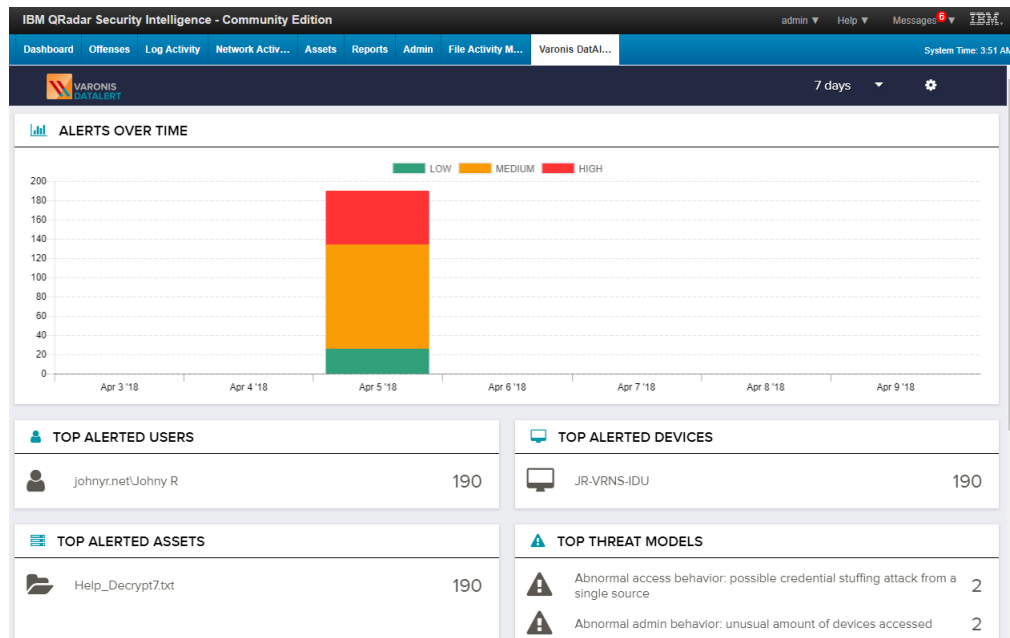
- To change the timeframe, select the relevant time period from the Time drop-down list at the top of the page.
- To sort the table by a specific column, click the column's heading. The table is sorted by the column. A triangle is displayed next to the column's header, to indicate the table is sorted by that column. The sort order (ascending or descending) is indicated by the direction of the triangle.

## Viewing Detailed Information About Alerts

To view detailed information about alerts:

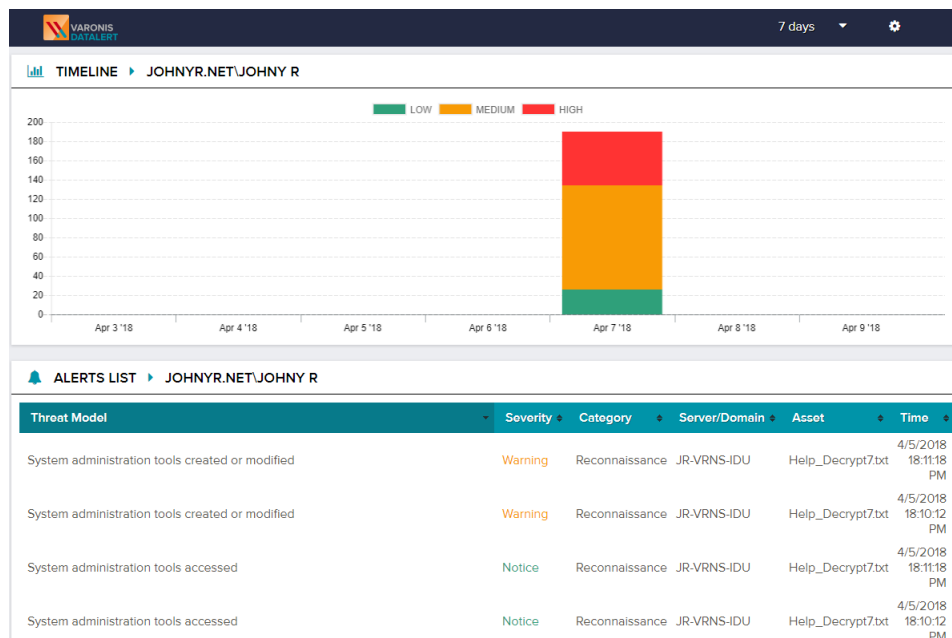
1. [Access the Varonis App for IBM QRadar.](#)

The dashboard is displayed.



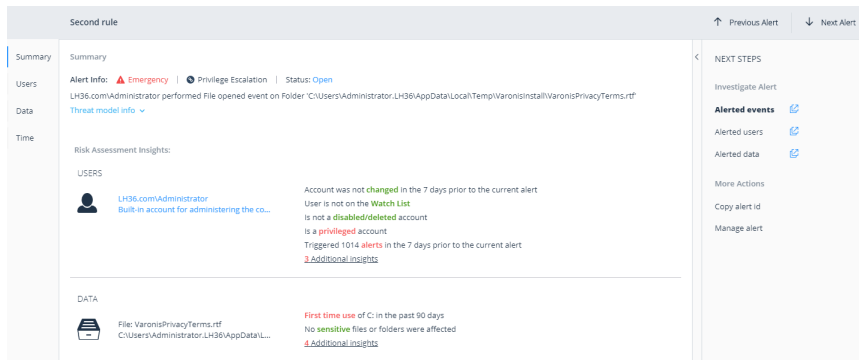
2. In the relevant top alerted widget, select the required entity.

A new tab opens, displaying a timeline and a complete list of alerts on the selected entity.



3. To view detailed information regarding a specific alert, click the relevant alert in the list.

The **Alert Info** page of the Varonis Web Interface opens, displaying detailed information about the alert. This page enables you to streamline your investigation and make a quick and informed decision regarding whether the activity is malicious or legitimate.



**Note:**

- This step is relevant only for customers running the Varonis Web Interface.
- For more information about the **Alert Info** page, see the *Varonis Web Interface User Guide*.

# A ALERT FIELD MAPPING

The following is a list of the fields that are built in to DatAlert's templates:

IBM QRadar Property	LEEF Field	DatAlert Placeholder	Description
Header_Type	LEEF version	Always " <i>LEEF:9.1.0</i> "	The LEEF version information is an integer value that identifies the major and minor version of the LEEF format that is used for the event.
Header_Vendor	Vendor	always " <i>Varonis</i> "	N/A
Header_Product	Product Name	always " <i>DatAdvantage</i> "	N/A
Header_Version	Product Version	<DatAdvantage Version>	The DatAdvantage software version, for use with rules run on HP-NAS devices.
Alert ID	EventID	<Alert ID>	The unique identifier of the DatAlert rule which triggered the alert.
Event ID	cat	<Rule Name>	The name of the DatAlert rule which triggered the alert.

IBM QRadar Property	LEEF Field	DatAlert Placeholder	Description
devTime	devTime	<Alert time>	Format is according to the local time format of the Varonis server which issued the alert by the DSP Server/Probe/Collector.
devTimeFormat	devTimeFormat	always "MMM dd yyyy HH:mm:ss"	
Protocol	proto	Always "Syslog"	
Severity	sev	<Severity>	The severity of the DatAlert rule which triggered the alert.
src	src	<Device IP Address>	The IP address of the user from where the event originated.
Device_Name	Device_Name	<Device_Name>	The resolved host name of the Device IP, from where the event originated.
Alert_Category	Alert_Category	<Alert Category>	
Alert_Description	Alert_Description	<Alert Description>	The full description of the alert.
usrName	usrName	<Acting Object>	The object name of the user/ computer that generated the event which triggered the alert.

IBM QRadar Property	LEEF Field	DataAlert Placeholder	Description
AccountName	accountName	<Acting Object SAM Account Name>	The logon name of the account that triggered the alert.
AccountDomain	domain	<Acting Object Domain Name>	The domain in which the user/ computer that generated the alerted event resides.
Event_Type	Event_Type	<Event Type>	The type of event performed on the affected object.
Event_Type_ID	Event_Type_ID	<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.
Event_Status	Event_Status	<Event Status>	Whether the event which triggered the alert succeeded or failed.



IBM QRadar Property	LEEF Field	DataAlert Placeholder	Description
Affected_Object	Affected_Object	<AffectedObject>	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.
Event_File_Server_Domain	Event_File_Server_Domain	<File Server/ Domain>	Hostname of the machine on which the event which triggered the alert took place. Domain name for Directory Services events.
Affected_Object_Path	Affected_Object_Path	<Path>	The access path where the affected object resides. For directory service objects, this is the distinguished name.
Event_Additional_Data	Event_Additional_Data	<Additional data>	The description of the event which triggered the alert, including event details such as date, time, etc..
Threshold_Value	Threshold_Value	<Threshold>	The number of events which triggered the alert.

IBM QRadar Property	LEEF Field	DatAlert Placeholder	Description
Threshold_First_Timestamp	Threshold_First_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.
Event_by_MailboxOwner	Event_by_MailboxOwner	<Client Access Type>	Whether the event which triggered the alert was performed by the mailbox owner or not. 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.
Email_Sender	Email_Sender	<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.

IBM QRadar Property	LEEF Field	DatAlert Placeholder	Description
Mailbox_Access_by_Owner	Mailbox_Access_by_Owner	<Mailbox Access Type>	Whether the event which triggered the alert was performed by the mailbox owner or not. 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.
Email_Item	Email_Item	<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.
Email_Attachment_Name	Email_Attachment_Name	<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.

IBM QRadar Property	LEEF Field	DatAlert Placeholder	Description
Email_Recipients	Email_Recipients	<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.
Email_Date	Email_Date	<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.
Account_of_Changed_Permissions	Account_of_Changed_Permissions	<Trustee>	The account for which the permissions were changed. Data is not collected for all event types.

IBM QRadar Property	LEEF Field	DataAlert Placeholder	Description
Permissions_Changes	Permissions_Changes	<Changed Permissions>	The specified changes in permissions. Data is not collected for all event types.
Permissions_before_Change	Permissions_before_Change	<Permissions Before Change>	The permissions before the change. Data is not collected for all event types.
Permissions_after_Change	Permissions_after_Change	<Permissions After Change>	The permissions after the change. Data is not collected for all event types.
Alert_Page_URL	Alert_Page_URL	<Alert page URL>	The URL of the Alerts page in the Varonis Web Interface. This placeholder enables opening the Alerts page directly from email or SIEM services.

## B ALERTS

For a description of the alerts received by DatAlert, refer to the *Behavioral Threat Model Quick Reference Chart* section in the *DatAlert and DatAlert Analytics Reference and Investigation Guide*.

# C TROUBLESHOOTING


This section describes possible problems and their fixes.

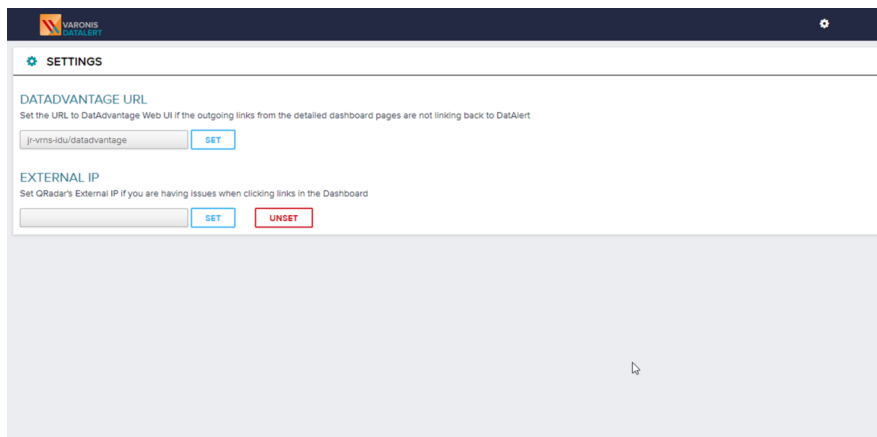
## No Data in Varonis DatAlert App for IBM QRadar

1. In the Log Activity tab, search for *Varonis*. If no results are displayed, alerts may not be received by QRadar.
2. In DatAlert, check that the port and protocol settings for Syslog are correct.
3. Check that the network allows Syslog messages to be sent by the Varonis Connector and DSP to QRadar:
  - Try using the ping function from the DSP and from any Collector that is configured to send alerts to the server.
  - If the ping function works, use the Logger tool (click [here](#)) to send a Syslog message to QRadar, run the `logger -l <qradar_address> -a 514 datAlert test` command, and search for **QRadar for DatAlert** to verify that the message was received.
  - If both attempts fail, consult with your networking expert to resolve the connectivity issue.

## Outgoing Links from Detailed Dashboard Pages are Not Linking to the Varonis Web UI

If outgoing links from the detailed dashboard pages are not linking back to DatAlert:

1. [Access the Varonis App for IBM QRadar.](#)
2. In the DatAlert dashboard, click the Settings icon . The **Settings** window is displayed.



3. Do the following:
  - a. In the DatAdvantage URL field, enter the URL of the Varonis Web Interface. For example:

```
yourServer/DatAdvantage
```


**Note:** http:// is not required.

- b. Click **Set**.

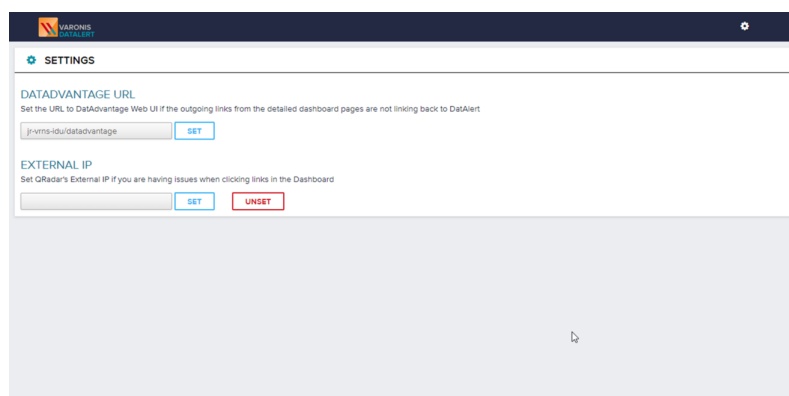
## Clicking a Row in a Dashboard Widget Does Not Direct Me to the Detailed Dashboards

This issue may occur if the QRadar instance is accessed from an external IP. If the internal IP of the QRadar instance is 192.168.1.20, for example, but you are accessing QRadar from 60.50.40.100 (an external IP), you will need to set the external IP from the Settings window.

To set the external IP:

1. [Access the Varonis App for IBM QRadar.](#)
2. In the DatAlert dashboard, click the Settings icon .

The **Settings** window is displayed.



3. In the External IP area, enter QRadar's external IP address and click **Set**.

## Null Values Are Displayed in the DatAlert App for IBM QRadar

NULL values are displayed in the Varonis DatAlert App for IBM QRadar if one or more mandatory fields in the syslog message are not populated.

For example, if the Top Alerted Devices module displays a NULL value, the `device_name` field in the syslog message may be empty.

To determine which fields should be checked when examining NULL values in the Top Alerted modules, see [Syslog Message Fields to Check When Null Values Are Displayed in Modules](#).



## Determining Whether the Syslog Message Originally Included NULL Values

To determine whether the Syslog message originally included NULL values:

1. In QRadar's Log Activity tab, filter the search according to the log sources defined for the DatAlert App for IBM QRadar.
2. Open an event and verify that the properties marked as "custom" properties under Event Information do *not* have the N/A value.
3. In the Payload Information area, select **UTF** and check the field in the syslog message.

## Determining Whether the Custom Event Properties are Accurately Defined

If there are uncertified IBM QRadar Apps in the environment, the App's default Custom Event property settings may be inaccurately defined.

1. To determine which properties require evaluation:
  - a. In QRadar's Admin tab, open the DSM Editor.
  - b. Select **Varonis DSM**.
  - c. Evaluate all properties in the Properties tab.
  - d. Close the window.
2. To determine whether the CEP settings are correct:
  - a. In QRadar's Admin tab, go to **Data Sources > Custom Event Properties**.
  - b. Search for the properties previously located in the Properties tab (for example, Alert ID).
  - c. Double-click the property name.
  - d. In the Property Expression Definition area, ensure that the Log Source Type is set to **Varonis DSM**.

**Important:** The Log Source Type *must* be set to **Varonis DSM**.

- e. Click **Save**.

### Syslog Message Fields to Check When Null Values Are Displayed in Modules

Module	QRadar Custom Event Property	Syslog Field
Top Alerted Users	Username	usrName
Top Alerted Devices	Device name	device_name
Top Alerted Assets	Affected object	affected_object
Top Alerted Threat Models	Rule name	Fifth field in the syslog header