IBM Security QRadar
Version 7.1.0 (MR1)

Configuring Custom Email Notifications Technical Note

Note: Before using this information and the product that it supports, read the information in Notices and Trademarks on page 9.

CONTENTS

1 CUSTOM EMAIL NOTIFICATIONS

When configuring rules using IBM Security QRadar SIEM, you can specify that each time the rule generates a response, an email notification is sent to recipients providing useful information, such as event or flow properties. These properties are specified in the alert-config.xml file, which is the default template. To meet the requirements of your organization, you can customize the content included in the email notification rule response.

This technical note provides information on how to customize your email notifications.

Unless otherwise noted, all references to QRadar SIEM refer to QRadar SIEM, IBM Security QRadar Log Manager, and IBM Security QRadar Network Anomaly Detection. References to flows do not apply to QRadar Log Manager.

This section includes the following topics:

Customizing Email Notifications

You must create a temporary directory in which you can safely edit your copy of the files, without risk of overwriting the default files. After you edit and save the alert-config.xml file, you must run a script that validates your changes. The validation script automatically applies your changes to a staging area, from where you can deploy the changes using the QRadar SIEM user interface.

To customize email notifications:

Step 1 Using SSH, log into the QRadar SIEM Console as the root user.

Username: **`root`**

Password: **`<password>`**

Step 2 To create a new temporary directory, type the following command:

```
mkdir <directory_name>
```

Where **<directory_name>** is the name of the temporary directory you use to edit copies of the default files.

Step 3 To copy the files stored in the **custom_alerts** directory to the temporary directory, type the following command:

```
cp /store/configservices/staging/globalconfig/templates/
custom_alerts/*.* <directory_name>
```

Where **<directory_name>** is the name of the directory you created in **Step 2**.

Step 4 Confirm the files were copied successfully:

a To list the files in the directory, type the following command:

```
ls -lah
```

b Verify the following file is listed:

alert-config.xml

Step 5 Open the alert-config.xml file.

For an example of the alert-config.xml file, see **Example Configuration File**.

Step 6 Optional. If you want to create multiple templates, copy the <template></template> property, including tags and the contents, and then paste it below the existing <template></template> property.

NOTE You can add multiple templates, however, QRadar SIEM only supports one event and one flow template type to be set to **True** in the `Active` property.

Step 7 Edit the contents of the `<template></template>` property:

a Specify the template type using the following XML property:

```
<templatetype></templatetype>
```

Where possible values include **event** or **flow**. This field is mandatory.

b Specify the template name using the following XML property:

```
<templatename></templatename>
```

c Set Active property to true:

```
<active>true</active>
```

d Edit the Subject property, if required.

e Add or remove parameters from the Body property. For more information on accepted parameters, see **Accepted Parameters**.

f Repeat these steps for each template you want to add.

Step 8 Save and close the file.

Step 9 To validate your changes, type the following command:

```
/opt/qradar/bin/runCustAlertValidator.sh <directory_name>
```

Where **<directory_name>** is the name of the directory you created in the **Customizing Email Notifications** procedure.

If the script validates the changes successfully, the following message is displayed:

```
File alert-config.xml was deployed successfully to staging!
```

Step 10 Log in to the QRadar SIEM user interface.

Step 11 Click the **Admin** tab.

Step 12 Select **Advanced > Deploy Full Configuration**.

Your custom email notifications are now complete. Rules that have an email notification set as the rule response will generate emails using the custom parameters you specified.

Example Configuration File

Example of the alert-config.xml default file:

NOTE When you upgrade from QRadar SIEM 7.0 MR5 to QRadar SIEM 7.1, the default alert-config.xml file displays the 7.0 MR5 configuration. If you have installed QRadar SIEM 7.1, the alert-config.xml file displays the example below.

```
<?xml version=”1.0” encoding=”UTF-8?>
<templates>
<template>
<templatename>Default Event</templatename>
<templatetype>event</templatetype>
<active>true</active>
<filename></filename>
<subject>
${RuleName} Fired
</subject>
<body>

The following is an automated response sent to you by the
${AppName} event custom rules engine:

$[StartTime]

Rule Name: ${RuleName}
Rule Description: ${RuleDescription}
Source IP: ${SourceIP}
Source Port: ${SourcePort}
SourceUsername: ${UserName}
Source Network: ${SourceNetNoDefault}
Destination IP: ${DestinationIP}
Destination Port: ${DestinationPort}
Destination Username: ${DestinationUserName}
Destination Network: ${DestinationNetNoDefault}
Protocol: ${Protocol}
QID: ${Qid}
```

```
Event Name: ${EventName}
Event Description: ${EventDescription}
Category: ${Category}
DataSource ID: ${DeviceID}
Device Name" ${DeviceName}
Payload: ${Payload}

CustomPropertiesList: ${CustomPropertiesList}

</body>
<from></from>
<to></to>
<cc></cc>
<bcc></bcc>
</template>
</templates>
```

Using Custom Parameters

The accepted email notification parameters are listed in **Table 1**. To use the body.CustomProperty and body.CalculatedProperty parameters, you must create a custom event or custom property. For more information, see the *IBM Security QRadar SIEM Users Guide*.

To use custom parameters in your custom email notification:

Step 1 Open the alert-config.xml file for editing. See **Step 1** to **Step 5**.

Step 2 Add one or both of the following lines to the alert-config.xml file.

- **`body.CustomProperty <Property Name>`**
- **`body.CalculatedProperty <Property Name>`**

  Where **`<Property Name>`** is the name used to create the custom property.

If you have configured custom properties and included custom parameters in your template, QRadar SIEM will generate emails using the custom parameters you specified.

Accepted Parameters

The following parameters can be used in custom email notifications:

Table 1 Accepted Notification Parameters

Common Parameters	Event Parameters	Flow Parameters
AppName	EventCollectorID	Type
RuleName	DeviceId	CompoundAppID
RuleDescription	DeviceName	FlowSourceIDs
EventName	DeviceTime	SourceASNList
EventDescription	DstPostNATPort	DestinationASNList
EventProcessorId	SrcPostNATPort	InputIFIndexList
Qid	DstMACAddress	OutputIFIndexList

Table 1 Accepted Notification Parameters (continued)

Common Parameters	Event Parameters	Flow Parameters
Category	DstPostNATIPAddress	AppId
RemoteDestinationIP	DstPreNATIPAddress	Host
Payload	SrcMACAddress	Port
Credibility	SrcPostNATIPAddress	SourceBytes
Relevance	SrcPreNATIPAddress	SourcePackets
Source	SrcPreNATPort	Direction
SourcePort	DstPreNATPort	SourceTOS
SourceIP		SourceDSCP
Destination		SourcePrecedence
DestinationPort		DestinationTOS
DestinationIP		DestinationDSCP
DestinationUserName		SourceASN
Protocol		DestinationASN
StartTime		InputIFIndex
Duration		OutputIFIndex
StopTime		FirstPacketTime
EventCount		LastPacketTime
SourceV6		TotalSourceBytes
DestinationV6		TotalDestinationBytes
UserName		TotalSourcePackets
DestinationNetwork		TotalDestinationPackets
SourceNetwork		SourceQOS
Severity		DestinationQOS
CustomPropertiesList		SourcePayload
body.CustomProperty("< Property Name>")		DestinationPayload
body.CalculatedProperty("<Prope rty Name>")		

A NOTICES AND TRADEMARKS

What's in this appendix:

This section describes some important notices, trademarks, and compliance information.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the

capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at *http:\\www.ibm.com/legal/copytrade.shtml*.