

QRadar Universal Application Integration Guide

QUA v1.0.0 - 2024-09-13

Legal notices

Information about the Nozomi Networks copyright and use of third-party software in the Nozomi Networks product suite.

Copyright

Copyright © 2013-2024, Nozomi Networks. All rights reserved. Nozomi Networks believes the information it furnishes to be accurate and reliable. However, Nozomi Networks assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of Nozomi Networks except as specifically described by applicable user licenses. Nozomi Networks reserves the right to change specifications at any time without notice.

Third Party Software

Nozomi Networks uses third-party software, the usage of which is governed by the applicable license agreements from each of the software vendors. Additional details about used third-party software can be found at https://security.nozominetworks.com/licenses.

Contents

Chapter 1. Introduction	5
Overview	7
Chapter 2. Requirements	9
Requirements	11
Chapter 3. Configuration	
Install the QRadar Universal Application	15
Create the log source	16
Generate an API key in Vantage	22
Generate an OpenAPI key in a sensor	24
Chapter 4. Troubleshooting	
Troubleshooting	29
Glossary	31



1 - Introduction

Chapter 1. Introduction



Overview

This documentation describes the **QRadar Integration for Nozomi Networks Vantage and Sensor** (**QRadar Universal Application**) with the Nozomi Networks platform.

The **QRadar Universal Application** is designed to enhance your security infrastructure. This solution uses the *hypertext transfer protocol (HTTP)* OpenAPI to gather critical information from both the Vantage and the sensor environments. This lets you efficiently monitor asset data and respond to security alerts.

The key features are shown below.

Unified alert management

The **QRadar Universal Application** provides a unified platform that lets you manage alerts and assets that originate from Nozomi Networks platform. Through the consolidation of data from both of these environments, security teams gain a holistic view of the security posture of their network.

HTTP OpenAPI integration

Through the use of the *HTTP* OpenAPI, the **QRadar Universal Application** ensures seamless communication between Nozomi Networks and QRadar. This means that data retrieval and synchronization are efficient and hassle-free, ensuring real-time awareness of security events.

Standardized data format

The data obtained from Vantage and the sensor products is shown in a consistent format that is easy to understand. This uniformity simplifies the monitoring and analysis process, which makes it easier to identify potential security threats.

Alert mapping to QRadar events

All alerts from Nozomi Networks are mapped to QRadar events within the system. This mapping ensures that each alert is treated as a distinct event, which allows for customized alert handling and analysis.

Automatic offense generation

When specific types of alerts are detected, such as Nozomi Networks incident alerts, the **QRadar Universal Application** raises QRadar offenses. This automated response makes sure that potential security incidents are quickly escalated for further investigation.

User-friendly GUI

The **QRadar Universal Application** has an intuitive *graphical user interface (GUI)* that gives a clear and organized view of all alert events. You can easily navigate through the alerts and apply various filters to narrow down the results, to make it easier to identify critical security events.

QRadar workflow integration

Users can easily configure LogSources to collect asset and alert data with the workflows available in the IBM QRadar GitHub repository.



Chapter 2. Requirements



Requirements

A description of the requirements for the use of the **QRadar Universal Application**.

You need:

- QRadar 7.5.0, or later
- To install the Log Source Management application

Note:

The Universal Cloud REST API protocol requires the Log Source Management application.



Chapter 3. Configuration



Install the QRadar Universal Application

Before you can configure the **QRadar Universal Application**, you must download and install it.

Procedure

- 1. Open the IBM X-Force Exchange.
- 2. In the search field, search for Nozomi Networks Universal App



- 3. Download the package.
- 4. To install it in your QRadar instance, upload it in Extensions Management.

Create the log source

Learn how to set up a Nozomi Networks universal log source in QRadar. This covers navigation, selection, and configuration of log source parameters, including type, name, and unique identifiers, sourced from the IBM QRadar GitHub repository.

Procedure

- 1. Open QRadar.
- 2. Select Admin > Apps.
- 3. In the Apps section, select QRadar Log Source Management.

≡	IBM QRadar										
Dashbo	ard Offenses	Log Activity	Network Activity	Assets	Reports	Admin	Pulse	Assistant	Use Case Manager	Pre-Validation	Nozomi Networks Universal
Admin System Date:	stem Configuration ta Sources	C Deplo	e are no changes to c	eploy.							
Re Se Try ► App	mote Networks and rvices Configuration / it out 25	Remote	Networks and Serv	ices Config	juration						
		Apps									
		QRada	r Log Source Manag	jement							
		QRad Ma	QRadar Log Source Management	vlanagement	1						
		Pulse -	Dashboard								
			W.,								

- 4. In the pane on the left, select **Select Log Source Type**.
- 5. In the search field, search for and then select: Nozomi Networks Universal.

≡	IBM QRadar Log Source Management	t - Add a Single Log Source	\times
0	Select Log Source Type		
2	Select Protocol Type	Select a Log Source type	
3	Configure Log Source Parameters	nozomi X Q.	
4	Configure Protocol Parameters	Nozomi Networks Universal	
5	Test Protocol Parameters		
		Step 2: Select Protocol Type	

6. In the bottom right corner, select **Step 2: Select Protocol Type**.

Result: The Select a protocol type page opens.

7. In the search field, search for and then select: Universal Cloud REST API.

≡	IBM QRadar Log Source Managemer	nt - Add a Single Log Source		\times
0	Select Log Source Type			
2	Select Protocol Type	Select a protocol type		
3	Configure Log Source Parameters	uri	x ्	
4	Configure Protocol Parameters	Universal Cloud REST API		
5	Test Protocol Parameters			
		Step 1: Select Log Source Type Step 2: Configure Log Source F	arameters	

8. In the bottom right corner, select Step 3: Configure Log Source Parameters.

Result: The Configure the Log Source parameters page opens.

9. In the **Name** field, enter the name of the log source.

≡	IBM QRadar Log Source Managemer	nt - Add a Single Log Source		×
0	Select Log Source Type			
0	Select Protocol Type	Configure the Log Source para	meters	
3	Configure Log Source Parameters	Name * The name of the log source.	host_keyname_Alert	
4	Configure Protocol Parameters Test Protocol Parameters	Description An optional description of the log source.		
		Enabled Indicates whether the log source should be enabled.		
		Groups • The groups that this log source will belong to.	Other × + Add Group	Q
		Extension Log Source Extensions perform post-processing of events after default pansing has occurred. + Show More	NozomiNetworksUniversalCustom_ext	X *
		Step 2: Select Protocol Type		Step 4: Configure Protocol Parameters

10. In the **Extension** field, enter: NozomiNetworksUniversalCustom_ext

Note:	
If you do not add the extension, the QRadar system will automatically	
assign it.	

11. In the bottom right corner, select Step 4: Configure Protocol Parameters.

=	IBM QRadar Log Source Manageme	nt - Add a Single Log Source	X
0	Select Log Source Type		
0	Select Protocol Type	Configure the protocol para	meters
0	Configure Log Source Parameters	Log Source Identifier *	
0	Configure Protocol Parameters	Workflow *	<qnsresolutiontest host="\$\/host]"></qnsresolutiontest> <tlcpconnectiontest host="\$\/host]"></tlcpconnectiontest>
5	Test Protocol Parameters		<sslhandhake(test host="5/host)"></sslhandhake(test> <htlcgonnectiontonoughprov test="" uni="https://5/host)"></htlcgonnectiontonoughprov>
		Workflow Parameter Values	••••••
		Allow Untrusted Certificates Enable this option to allow self-signed or otherwise untrusted certificates. + Show More	
		Use Proxy Select this check box if the API is accessed by using a proxy. + Show More	
		Step 3: Configure Log Source Parameters	Step 5: Test Protocol Parameters

Result: The Configure the protocol parameters page opens.

12. In the Log Source Identifier field, enter an identifier. Concatenate the Nozomi Networks endpoint with the key_name, followed by either Alert or Asset string: nozominetworkscom.customers.eul.io_AKdf6123_Alert The Log Source Identifier should be unique and should be similar to:

\${/host}_\${/key_name}_Alert \${/host}_\${/key_name}_Asset

host is the Vantage endpoint like:

nozominetworkscom.customers.eul.xxx.nozominetworks.io

key_name is the key_name generated in Vantage.

_Asset and _Alert are just strings.

LogSourceIdentifier examples:

- o nozominetworkscom.customers.eul.xxx.nozominetworks.io_AK023XXX_Alert
- $^\circ nozominetworkscom.customers.eu1.xxx.nozominetworks.io_AK023XXX_Asset$
- 13. In the **Workflow** field, enter the value.

You can get the latest version from the IBM QRadar GitHub repository.

Note:

There are two types of workflow: Alerts and Assets.

14. In the Workflow Parameter Values field, enter the value.

You can get the latest version from the IBM QRadar GitHub repository.



15. In the bottom right corner, select Step 5: Test Protocol Parameters.

Result: The Test Protocol Parameters page opens.

16. To make sure that the parameters of the log source configuration are correct, select **Start Test**.

≡	IBM QRadar Log Source Managemen	t - Add a Single Log Source	
Ø	Select Log Source Type		
0	Select Protocol Type	Test Protocol Parameters	
0	Configure Log Source Parameters	¢	
0	Configure Protocol Parameters	Test this log source configuration to ensure that the parameters are correct.	
6	Test Protocol Parameters	The test runs from the host specified by the Target Event Collector parameter. If there is high network latency between the console and this host, it may take a moment for the results to appear.	
		The test collects sample event data from the target system. This feature can be disabled in the settings.	
		Start Test	
		Slep 4: Configure Protocol Parameters Skip Test and Finial	1

Figure 1. Test protocol parameters page

17. If the configuration is correct, a positive result will show.

=	IBM QRadar Log Source Managemen	nt - Add a Single Log Source	×
0	Select Log Source Type		
0	Select Protocol Type	Test Protocol Parameters	
0	Configure Log Source Parameters	÷ الح الم	
0	Configure Protocol Parameters		
6	Test Protocol Parameters	Pestert	
		Results (3):	
		> 🗸 Testing DNS resolution of	
		> 🗸 Testing TCP connection to	
		> 🗸 Testing SSL connection to	
		Events (5):	
		Log Source identifier Payload	
		Biop & Configure Protocol Parameters	

Figure 2. Successful result

18. If the configuration is not correct, a negative result will show.

 statut ug kovers Type Statut Protocol Parameters Configure 1 og kovers Parameters Configure 1 og kovers Parameters Tet Protocol Parameters Tet Para	E IBM QRadar Log Source Manageme	nt - Add's Single Log Source
	Select Log Source Type	
Contractive to go downer homeneters Contractive to downer homeneters The Produce Presenters	Select Protocol Type	Test Protocol Parameters
Configure Mondool Rewardsets Text Protocol Rewardsets	Configure Log Source Parameters	← ₹ ®
Tet Protocol Parameters Image: Control Cont	Configure Protocol Parameters	×
Results (3): × Y Testing DNS resolution of Error: Unable to resulte × O × O × O × Events (0): Error: 00 or are tests have failed - cancelling sample event collection	5 Test Protocol Parameters	Retar
		Results (8): * X Testing MSP resolution of Brance State State • ① Testing TOP connection to • ② Testing SSL connection to

Figure 3. Unsuccessful result

19. If there is an authentication error, the **Error 401** page will show.

This might be because the key_name and/or the key_token are not valid (incorrect or expired).

≡	IBM QRadar Log Source Manageme	nt - Add a Single Log Source
Ø	Select Log Source Type	
0	Select Protocol Type	Test Protocol Parameters
0	Configure Log Source Parameters	← ₹ @
0	Configure Protocol Parameters	×
0	Test Protocol Parameters	401
		Pestart
		Results (3):
		> 🗸 Testing DNS resolution of
		> 🗸 Testing TCP connection to
		> 🗸 Testing SSL connection to
		Events (0): Error: 445
		Step 4: Configure Protocol Parameters

Figure 4. Error 401

20. Select Finish.

Generate an API key

Before you can use an API key, you must generate one.

Before you begin

Before you do this procedure, make sure that you have:

- Created a user to associate with your third-party application
- Assigned the user a role that grants the necessary permissions and scope within Vantage

About this task

Once an *application programming interface (API)* key has been created, you cannot edit it. You can only revoke it.

Procedure

- 1. Log into Vantage as the user who will own the API key.
- 2. In the top navigation bar, select $^{\textcircled{0}}$ > **Profile**.
- 3. Select API Keys.

Result: The API Keys page opens.

4. In the **Description** field, enter a description for the API key.

Give a human-friendly descri	tion to the API key.				
Allowed IPs					
Example IP ranges: 1.2.3.4/	4 or 1.2.3.4/24,2.	3.4.5/16.			
If no IP range is defined, the r If an IP range is defined, it co	inge defined in gene trols OVER the one o	ral settings conti lefined in genera	ols. I settings.		
Organization					
Acme					
Default Organization linked t	this ApiKey. It will b	e used by reques	t authenticated by th	is API Key.	
If no Organization is sent in t	e request header, th	e default Organiz	ation will be used.		

Note:

Nozomi Networks recommends that the description includes the name of the application that will connect with the <u>API</u> key.

5. **Optional:** Enter a range of allowed *internet protocol (IP)* addresses in the **Allowed IPs** field. Only applications within this range will be permitted to connect with this key.

Note:

For these settings, you must use comma-delimited entries, in format. Values here will override the values in the **SECURITY** section on the **General** page.

6. In the **Organization** field, select the organization that will be the default for this *API* key.



If an <u>API</u> request that uses this key doesn't include an organization, the default organization is used.

7. Select Generate.

Result: Vantage generates a key and displays its:

- Key name
- Key token
- $^{\circ}$ Allowed ips
- Linked organization

Important:

8.

You will need some of these values when you configure your third-party application. While the name is shown in the Vantage after this point, the token is not shown again. If you lose this data, you must generate a new *API* key.

Record these details:

- Key name
- Key token
- $^{\circ}$ Allowed ips

Generate an OpenAPI key

The profile settings menu lets you generate an OpenAPI key.

Procedure

1. In the top navigation bar, select $^{\textcircled{0}}$

Result: A menu shows.

- 2. Select Other actions.
- 3. Select Edit OpenAPI keys.

Result: A dialog shows.

4. In the top right, select + Generate.

Edit OpenAPI keys							
Page 1 of 1, 0 entries					O Live	+ Generate	
ACTIONS	NAME	DESCRIPTION	ALLOWED IPS	LAST SIGN IN IP	LAST SIGN IN TIME	REVOKE TIME	
						Close	

Result: A dialog shows.

5. In the **Description** field, enter a description for the OpenAPI key.

Generate OpenAPI key								
Ор	OpenAPI key for web user admin							
De	Description							
	bwed IPs							
ì	Examples of IP ranges for allowed IPs: 1.2.3.4/24 or 1.2.3.4/24,2.3.4.5/16. If no IP range is defined all IPs are allowed.							
	Generate Cance							

- 6. In the **Allowed IPs** field, enter the details of the allowed *IP* addresses.
- 7. Select **Generate**.

Results

Your OpenAPI key has been generated.



Chapter 4. Troubleshooting



Troubleshooting

A description of the best way to troubleshoot problems with your integration.

Logs

The QRadar logs are the best way to troubleshoot problems with the integration. You can find the applicable log files:

- /var/log/qradar.log
- /var/log/qradar.error



Glossary



Application Programming Interface

An API is a software interface that lets two or more computer programs communicate with each other.

Cyber threat intelligence

CTI collects and analyzes information on cyber threats and vulnerabilities, providing insights for organizations to proactively understand, prevent, and mitigate cyberattacks. To do this, it learns about the tactics, techniques, and procedures of attackers.

Graphical User Interface

A GUI is an interface that lets humans interact with electronic devices through graphical icons.

Hypertext Transfer Protocol

HTTP is an application layer protocol in the Internet protocol suite model for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access, for example by a mouse click or by tapping the screen in a web browser.

Identifier

A label that identifies the related item.

Internet of Things

The IoT describes devices that connect and exchange information through the internet or other communication devices.

Internet Protocol

An Internet Protocol address, or IP address, identifies a node in a computer network that uses the Internet Protocol to communicate. The IP label is numerical.

Open Virtual Appliance

An OVA file is an open virtualization format (OVF) directory that is saved as an archive using the .tar archiving format. It contains files for distribution of software that runs on a virtual machine. An OVA package contains a .ovf descriptor file, certificate files, an optional .mf file along with other related files.

Operational Technology

OT is the software and hardware that controls and/ or monitors industrial assets, devices and processes.

Security Information and Event Management

SIEM is a field within the computer security industry, where software products and services combine security event management (SEM) and security information management (SIM). SIEMs provide real-time analysis of security alerts.

Structured Threat Information Expression

STIX[™] is a language and serialization format for the exchange of cyber threat intelligence (CTI). STIX is free and open source.

Tactics, techniques, and procedures

TTPs are the patterns of behavior that describe how cyber adversaries operate, encompassing their strategies (tactics), tools and methods (techniques), and specific procedures for executing attacks. Understanding TTPs aids in predicting and defending against future cyber threats.

Trusted Automated Exchange of Indicator Information

TAXII is a protocol for the exchange of cyber threat intelligence (CTI) online. It is often used with Structured Threat Information Expression (STIX) to share detailed threat information.

Uniform Resource Locator

An URL is a reference to a resource on the web that gives its location on a computer network and a mechanism to retrieving it.

