



**STORMSHIELD**



TECHNICAL NOTE

**STORMSHIELD NETWORK SECURITY**

# INTEGRATING SNS LOGS IN IBM QRADAR

Product concerned: SNS 3.7.x and higher, SNS 4.x

Document last update: December 23, 2020

Reference: [sns-en-integrating\\_SNS\\_logs\\_in\\_IBM\\_QRadar\\_technical\\_note](#)



# Table of contents

Getting started .....	3
About this document .....	3
Requirements and compatibility .....	3
Installing the SNS extension in IBM QRadar .....	4
Downloading the DSM .....	4
Importing the DSM into QRadar .....	4
Configuring the log source .....	5
Adapting the size of syslog UDP messages in QRadar .....	6
Changing the payload size of syslog messages in QRadar .....	7
Configuring the SNS firewall to send logs to IBM QRadar .....	8
Using QRadar with the SNS DSM .....	9
Support .....	10



## Getting started

Of all the cybersecurity components that can be deployed to secure a network, Stormshield's SNS firewalls and IBM's Security QRadar come together to ensure that security operations center (SOC) analysts and administrators can fully trust the defenses that are implemented and obtain relevant information about events occurring on their networks.

As a cybersecurity vendor, Stormshield has protected organizations that host critical and highly sensitive infrastructures for the past 20 years with its firewall range. Thanks to Stormshield firewalls, administrators are able to secure their networks, monitor the nature of data that their users share, and encrypt data through IPSec VPN tunnels. As for all the routine events that take place every day, Stormshield firewalls generate logs that keep administrators informed as soon as events occur on the network. Stormshield SNS firewalls' ability to organize and categorize logs gives administrators a deeper understanding of what their firewalls process.

IBM's Security QRadar Device Support Module (DSM) offers administrators and SOCs the possibility of integrating SNS firewall logs into IBM Security QRadar so that they can obtain relevant information in their security information and event management (SIEM) solution. With this combination, security teams can analyze network behavior in real time and detect threats that target their organization.

The IBM Security QRadar DSM for Stormshield firewalls makes it possible to analyze the following log categories:

- Authentication,
- Firewall,
- Intrusion prevention (IPS),
- Threat management (UTM),
- Sandboxing,
- System events,
- Alarms.

### About this document

IBM QRadar is a security information and event management (SIEM) solution that enables the real-time analysis of security alerts generated by network-based applications and solutions.

This document explains how to integrate the Stormshield Network Security DSM into IBM QRadar.

### Requirements and compatibility

- SNS DSM version: 1.0.0 (published: October 2020),
- IBM QRadar 7.3.2 and higher,
- SNS 3.7 and higher.



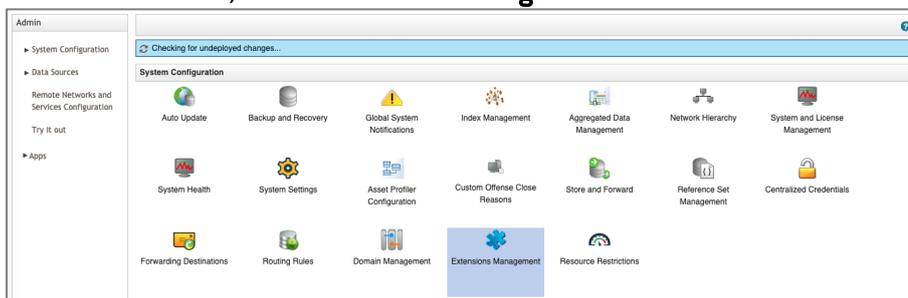
# Installing the SNS extension in IBM QRadar

To install the extension:

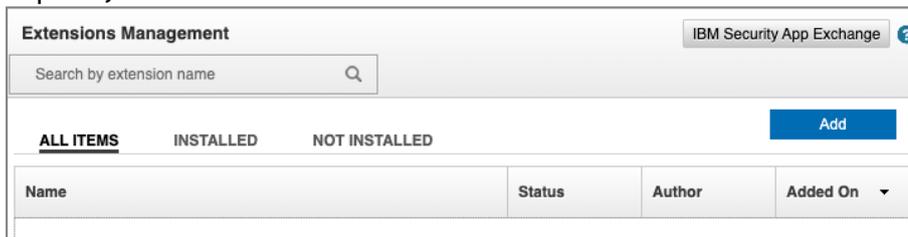
- Download the Stormshield Network Security DSM from the [IBM application store](#),
- Import the DSM into QRadar,
- Configure a log source that accepts and maps syslog messages from the SNS firewall to the DSM.

## Downloading the DSM

1. Log in to your IBM QRadar console.
2. In the **Admin** menu, select **Extensions Management**:



3. Click on **IBM Security App Exchange**. Your browser will open the page <https://exchange.xforce.ibmcloud.com/hub/> (IBM ID required).



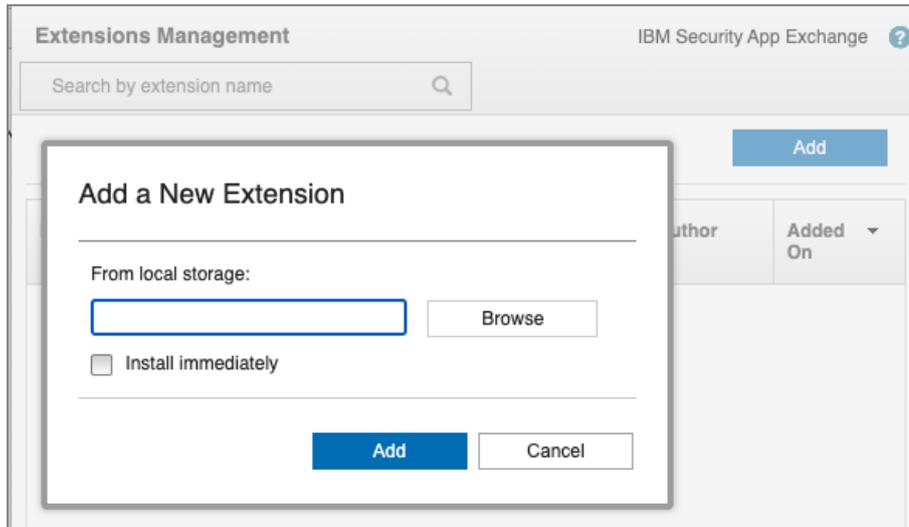
4. Download the "Stormshield Network Security" DSM.

## Importing the DSM into QRadar

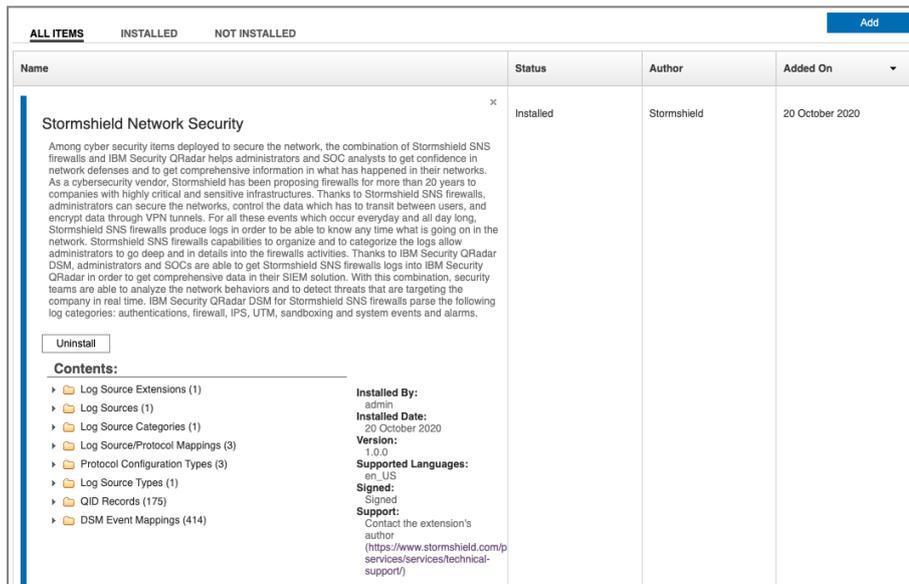
In your IBM QRadar console:



1. Go to **Admin > Extensions Management**.
2. Click on **Add a New Extension**:



3. Select the zip archive downloaded earlier (Stormshield\_Network\_Security\_DSM\_v1.0.0.zip).
4. Click on **Add** to install the extension:



## Configuring the log source

SNS firewalls send their logs to IBM QRadar over the syslog protocol.

1. Log in to your IBM QRadar console.
2. In the **Admin** menu, select **Log Source**.
3. Click on **Add**.
4. Fill in the form to create the Log Source:
  - **Log Source Name** field: enter a name for your new log source (e.g.: *Stormshield SNS device*).
  - **Log Source description** field: enter a description of your new log source.
  - **Protocol Configuration** field: select **Syslog**.



- **Log Source Identifier** field: enter the host name of your SNS firewall. If no host name has been defined on your firewall, enter its serial number (e.g.: *VMSNSX0000000A1*).
- **Log Source Extension** field: select *StormshieldNetworkSecurityCustom\_ext*.

**Edit a log source** ?

Note that the connection information for this log source is shared amongst one or more other log sources. This log source is a component of a Bulk Log Source, so some of its configuration parameters are not modifiable.

Log Source Name	Stormshield SNS devi
Log Source Description	StormshieldNetworkSi
Log Source Type	Stormshield Network Security
Protocol Configuration	Syslog
Log Source Identifier	SNShostname
Enabled	<input checked="" type="checkbox"/>
Credibility	5
Target Event Collector	eventcollector0 :: ip-10-0-1-25
Coalescing Events	<input checked="" type="checkbox"/>
Incoming Payload Encoding	UTF-8
Store Event Payload	<input checked="" type="checkbox"/>
Log Source Extension	StormshieldNetworkSecurityCustom_ext

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

Save Cancel

5. Click on **Save**.

### Adapting the size of *syslog* UDP messages in QRadar

QRadar uses a default payload size of 1024 bytes for *syslog* UDP messages. When a message exceeds this size, it will be automatically truncated.

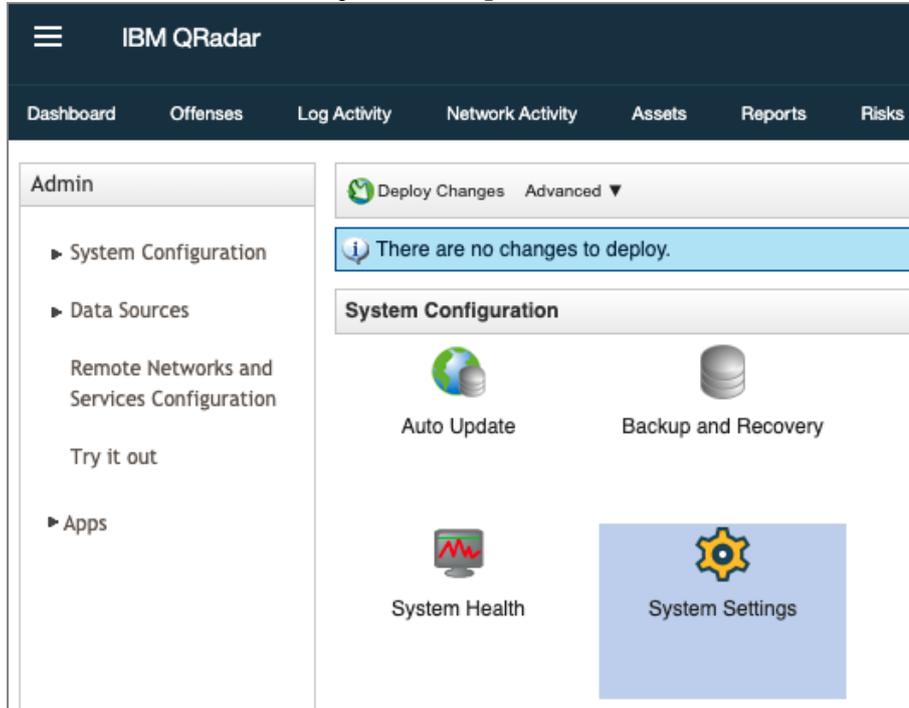
Incidentally, some of the events that SNS firewalls send exceed this size. Since the log type is placed at the end of the line, QRadar will not be able to extract the corresponding event category, and treat these messages as unknown.

The size of *syslog* UDP messages that IBM QRadar accepts must therefore be changed. Increasing the limit to 2048 bytes will sufficiently cover all types of messages that the firewall may send.

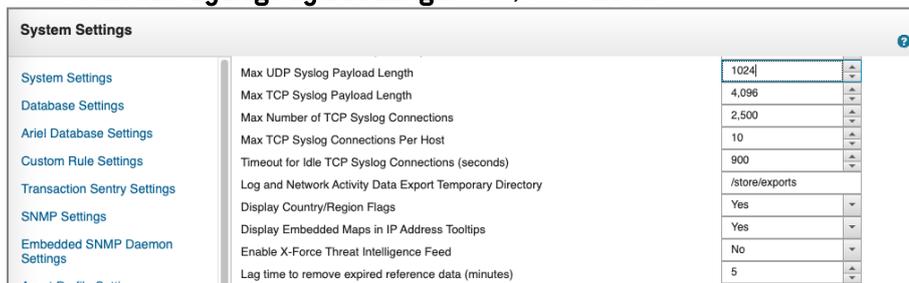


## Changing the payload size of syslog messages in QRadar

1. Log in to your IBM QRadar console.
2. In the **Admin** menu, select **System settings**:



3. Switch the system settings panel from **Basic** to **Advanced** mode.
4. In the **Max UDP Syslog Payload Length** field, enter **2048**:



5. Click on **Save** to save your changes.



# Configuring the SNS firewall to send logs to IBM QRadar

1. Log in to the web administration interface of your SNS firewall.
2. Go to **Configuration > Notifications > Logs - Syslog - IPFIX > SYSLOG** tab.
3. Edit one of the four available SYSLOG profiles.
4. **Name** field: enter a custom name for this profile.
5. **Syslog server** field: select or create a network object representing the IBM QRadar machine.
6. **Protocol** field: select **UDP**.
7. **Port** field: select **syslog**.
8. **Format** field: select **RFC5424**.
9. In **Advanced properties > Logs enabled**, select the log categories to be sent to IBM QRadar.
10. Click on **Apply**.
11. Double-click in a profile's **Status** cell to enable it.

The screenshot shows the Stormshield Network Security v4.0.3 web interface. The user is logged in as 'EVAU' with ID 'VMSNSX08K0014A9'. The navigation menu on the left includes SYSTEM, NETWORK, OBJECTS, USERS, SECURITY POLICY, APPLICATION PROTECTION, VPN, and NOTIFICATIONS. The 'NOTIFICATIONS' section is expanded to 'Logs - Syslog - IPFIX'. The main content area is titled 'NOTIFICATIONS / LOGS - SYSLOG - IPFIX' and has tabs for 'LOCAL STORAGE', 'SYSLOG', and 'IPFIX'. The 'SYSLOG' tab is active, showing a table of 'SYSLOG PROFILES' with columns for 'Status' and 'Name'. The profile 'QRADAR 732' is highlighted and its status is 'Enabled'. To the right, the 'Details' section for this profile is shown, with fields for Name (QRADAR 732), Comments, Syslog server (ip-10-0-1-25), Protocol (UDP), Port (syslog), Certification authority (syslog-ca), Server certificate (syslog.qradar), Client certificate, and Format (RFC5424). Below these fields is the 'Advanced properties' section, which includes 'Backup server', 'Backup port', and 'Category (facility)'. At the bottom of the 'Advanced properties' section is the 'LOGS ENABLED' section, which has 'Enable all' and 'Disable all' buttons and a table of log categories with their status:

Status	Name
Enabled	Alarms
Enabled	Network connections
Enabled	Filter policy
Enabled	HTTP proxy
Enabled	SMTP proxy

The installation is complete – the SNS firewall's logs will be redirected to the IBM QRadar platform.



# Using QRadar with the SNS DSM

1. Log in to your IBM QRadar console.
2. In the **Log Activity** menu, click on **New Search**.
3. Fill in the various fields of the search form:
  - **Parameter** field: select **Log Source Type**,
  - **Operator** field: select **Equals**,
  - **Value** field: select **Stormshield Network Security**.
4. Confirm by clicking on **Add Filter**.
5. Click on **Search**.  
Stormshield logs will appear in the grid.

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:33	Firewall Permit	10.0.100.2	37031	10.0.0.9	636	Jack	High
System Informational	Stormshield SNS device	1	20 Oct 2020, 14:53:32	System Informational	10.0.100.1	0	10.0.1.110	0	N/A	Low
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:30	Firewall Permit	10.0.100.14	36364		443	Jessica	High
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:19	Firewall Permit		59124	10.0.1.25	443	N/A	High
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:28	Firewall Permit	10.0.100.9	23971	10.0.0.8	443	James	High
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:27	Firewall Permit		37503	10.0.0.1	25		High
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:26	Firewall Permit	10.0.1.9	58506		443	N/A	High
Firewall Deny	Stormshield SNS device	1	20 Oct 2020, 14:53:23	Firewall Deny	10.0.100.16	32615		80	Isla	High
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:21	Firewall Permit	10.0.100.5	36429		443	Charlie	High
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:20	Firewall Permit	10.0.100.1	36689	10.0.0.7	443	Oliver	High
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:07	Firewall Permit		59126	10.0.0.37	80	N/A	High
Virus Detected And Blocked	Stormshield SNS device	1	20 Oct 2020, 14:53:18	Virus Detected	10.0.100.16	21343	192.168.100.1	80	Isla	High
Firewall Permit	Stormshield SNS device	2	20 Oct 2020, 14:53:05	Firewall Permit		58893	10.0.1.25	443	N/A	High
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:10	Firewall Permit	10.0.100.12	38897	192.168.13.4	102	Olivia	High
Authentication success on the firewall via SSH	Stormshield SNS device	1	20 Oct 2020, 14:53:07	SSH Login Succeeded	10.0.100.18	28512	10.0.0.9	636	Isabella	High
IPS Deny	Stormshield SNS device	1	20 Oct 2020, 14:53:06	IPS Deny	192.168.11.1	37887	192.168.13.1	502	N/A	High
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:52:53	Firewall Permit		58849	10.0.1.9	443	N/A	High
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:04	Firewall Permit	10.0.100.11	24302		80	Amelia	High
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:52:54	Firewall Permit	10.0.1.9	43148		443	N/A	High
Sandboxing malicious	Stormshield SNS device	1	20 Oct 2020, 14:53:02	Malicious Software	10.0.100.5	26663		80	Charlie	High
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:52:52	Firewall Permit	10.0.1.9	59182		443	N/A	High
System Informational	Stormshield SNS device	3	20 Oct 2020, 14:52:51	System Informational		0	10.0.1.110	0	admin	High
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:01	Firewall Permit	10.0.100.5	39058		80	Charlie	High
Sandboxing malicious	Stormshield SNS device	1	20 Oct 2020, 14:52:59	Malicious Software	10.0.100.1	27372		80	Oliver	High
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:52:57	Firewall Permit	10.0.100.15	35660	10.0.0.11	445	Ava	High
Sandboxing malicious	Stormshield SNS device	1	20 Oct 2020, 14:52:55	Malicious Software	10.0.100.18	21853		80	Isabella	High
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:52:44	Firewall Permit		59052	10.0.0.37	22	N/A	High
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:52:54	Firewall Permit	10.0.1.9	41994		443	N/A	High
Firewall Permit	Stormshield SNS device	2	20 Oct 2020, 14:52:33	Firewall Permit		59123	10.0.1.25	443	N/A	High
Firewall Permit	Stormshield SNS device	2	20 Oct 2020, 14:52:28	Firewall Permit		59107	10.0.1.9	443	N/A	High
Firewall Permit	Stormshield SNS device	5	20 Oct 2020, 14:52:22	Firewall Permit		59103	10.0.1.25	443	N/A	High
Firewall Permit	Stormshield SNS device	2	20 Oct 2020, 14:52:20	Firewall Permit	10.0.1.9	63567		53	N/A	High
Authentication failure on the firewall via SSH	Stormshield SNS device	1	20 Oct 2020, 14:52:22	SSH Login Failed		0	0.0.0.0	0	N/A	High

**NOTE:**  
There are two limitations in version 1.0.0 of the SNS DSM:

- IPv6 values are not taken into account.
- Only standard QRadar fields are used; custom properties to filter by vendor-specific values are not available.

The Stormshield DSM provides the values of the following QRadar standard properties:

- DestinationIp,
- DestinationMAC,
- DestinationPort,
- DestinationIpPreNAT,
- DestinationPortPreNAT,
- DeviceTime,
- EventCategory,
- Protocol,
- SourceIp,



- SourceMAC,
- SourcePort,
- SourceIpPostNAT,
- SourcePortPostNAT,
- UserName.

Following events are categorised by QRadar:

- Connections Pass or Block,
  - Firewall and proxies,
  - Filter policy,
  - Alarms (IPS Permit or Deny),
- Proxies,
  - Virus detection,
  - Sandboxing detection,
- Authentication errors,
- System events.

## Support

If you encounter issues while installing or using the Stormshield Network Security DSM on the IBM QRadar platform, feel free to get in touch with [Stormshield technical support](#).



**STORMSHIELD**

[documentation@stormshield.eu](mailto:documentation@stormshield.eu)

*All images in this document are for representational purposes only, actual products may differ.*

*Copyright © Stormshield 2020. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.*