N-Partner

N-REPORTER

How to receive McAfee IntruShield IDS Audit Log with N-Reporter

V1.1.2

(01-01-01-001) 2013/08/06

Preface

This document is to introduce how to receive McAfee IntruShield Syslog with N-Reporter. It emphasizes on how to set up McAfee IntruShield Syslog Forwarding, for N-Reporter to process McAfee IntruShield Syslog correctly.

N-Reporter is a product of N-Partner. It is one of the main Syslog analyzer in the industry. It is able to calculate and analyze received Syslog, and produce all kinds of professional reports.

McAfee IntruShield IDS is a device of Network Intrusion Detection. It sends analyzed results of network current situation to N-Reporter through Syslog.

P.S. McAfee IntruShield IDS is the registered trademark of McAfee company.

Contents

Setting up McAfee IntruShield Syslog Forwarding

McAfee IntruShield IDS is able to send Syslog through Fault Notification Syslog Forwarder to the third party syslog application. For example: N-Reporter.

Perform the following steps:

►**step1:** Please log in IntruShield IDS with administrator authorization.

►**step2:** Open the syslog forwarder interface.

►**step3:** Set up the following options and key-in the needed value.

- ✓ Enable Syslog Forwarder: Yes
- ✓ Forward Alerts: With Severity low and above
- ✓ Syslog Server: Please key-in the IP address of the N-Reporter device.
- ✓ Port: 514

►**step4:** Select Message Preference: Customized. Then, click **Edit**, enter the interface for customized edit syslog messages.

►**step5:** Please copy and paste the following text.

category="$IV_CATEGORY$", sub_category="$IV_SUB_CATEGORY$", attack_name="IV_ATTACK_NAME", attack_severity=$IV_ATTACK_SEVERITY$, interface=$IV_INTERFACE$, source_ip=IV_SOURCE_IP, source_port=IV_SOURCE_PORT,destination_ip=$IV_DESTINATION_IP$,destination_port=$IV_DESTINATION_PORT$, network_protocol=$IV_NETWORK_PROTOCOL$,attack_count=IV_ATTACK_COUNT

Note: The format above does not contain any line break.

►**step6:** Click **Save**.

►**step7:** Click **Apply**.

►**step8:** Set up complete. IntruShield IDS will generate and send Syslog to N-Reporter.

Setting up McAfee Network Security Manager Syslog forwording

► **step1:** Please log in with administrator authorization.

Network Security Manager➔IPS Setting➔Alert Notification➔Syslog。

► **step2:** Open the syslog forwarder interface.

► **step3:** Set up the following options and key-in the needed value.

- ✓ Enable Syslog Forwarder：Yes
- ✓ Server Name or IP Address：Please key-in the IP address of the N-Reporter machine.
- ✓ UDP Port：514
- ✓ Send Notification IF：Check The following notification filter is matched: Severity Informational and above

► **step4:** Select Message Preference: Customized. Then, click **Edit**, enter the interface for customized edit syslog messages.

► **step5:** Please copy and paste the following text.

```
category="$IV_CATEGORY$", sub_category="$IV_SUB_CATEGORY$", attack_name="$IV_ATTACK_NAME$", attack_severity=$IV_ATTACK_SEVERITY$, interface=$IV_INTERFACE$, source_ip=$IV_SOURCE_IP$, source_port=$IV_SOURCE_PORT$,destination_ip=$IV_DESTINATION_IP$,destination_port=$IV_DESTINATION_PORT$, network_protocol=$IV_NETWORK_PROTOCOL$,attack_count=$IV_ATTACK_COUNT$
```

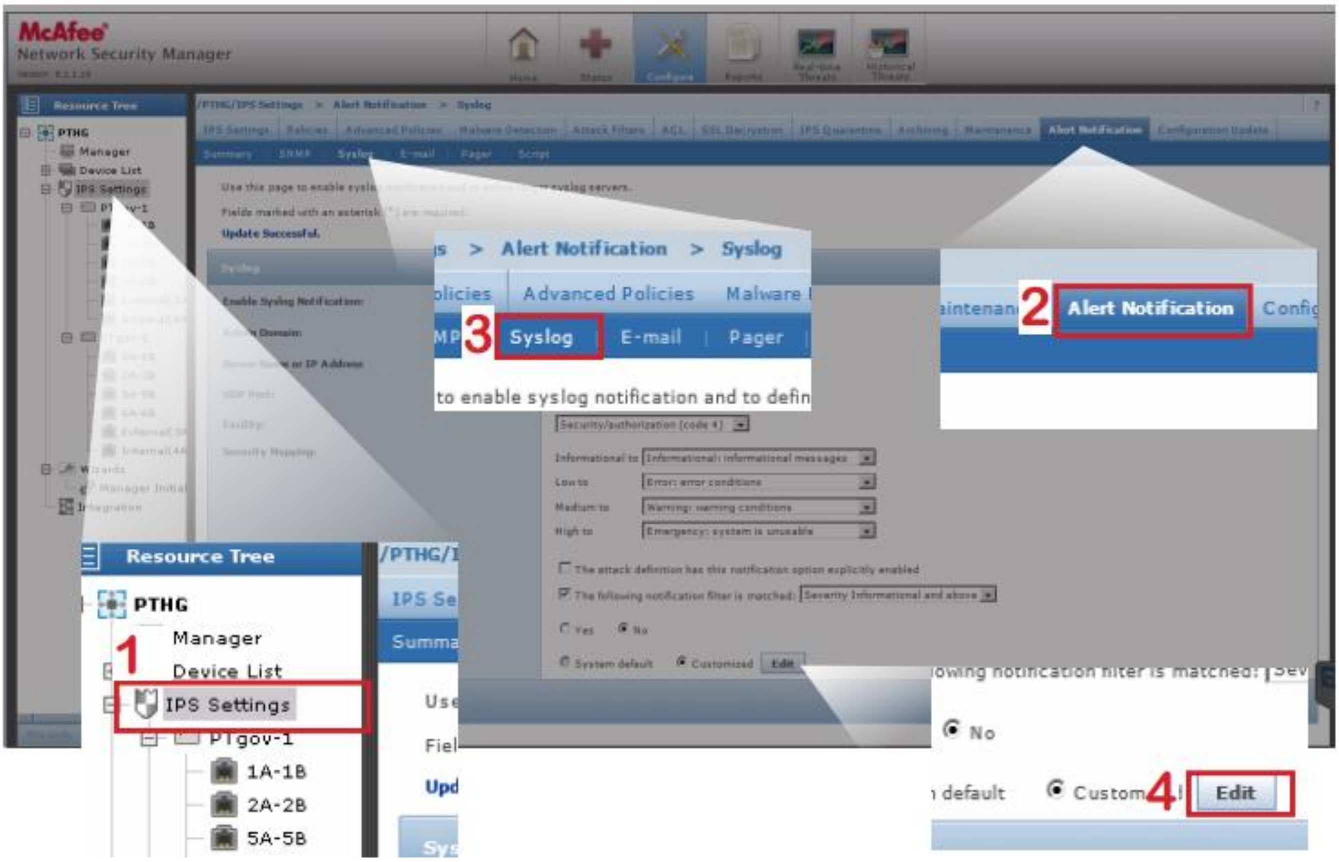
Note: The format above does not contain any line break.

►**step6:** Click **Save**.

►**step7:** Click **Apply**.

►**step8:** Set up complete. IntruShield IDS will generate and send Syslog to N-Reporter.

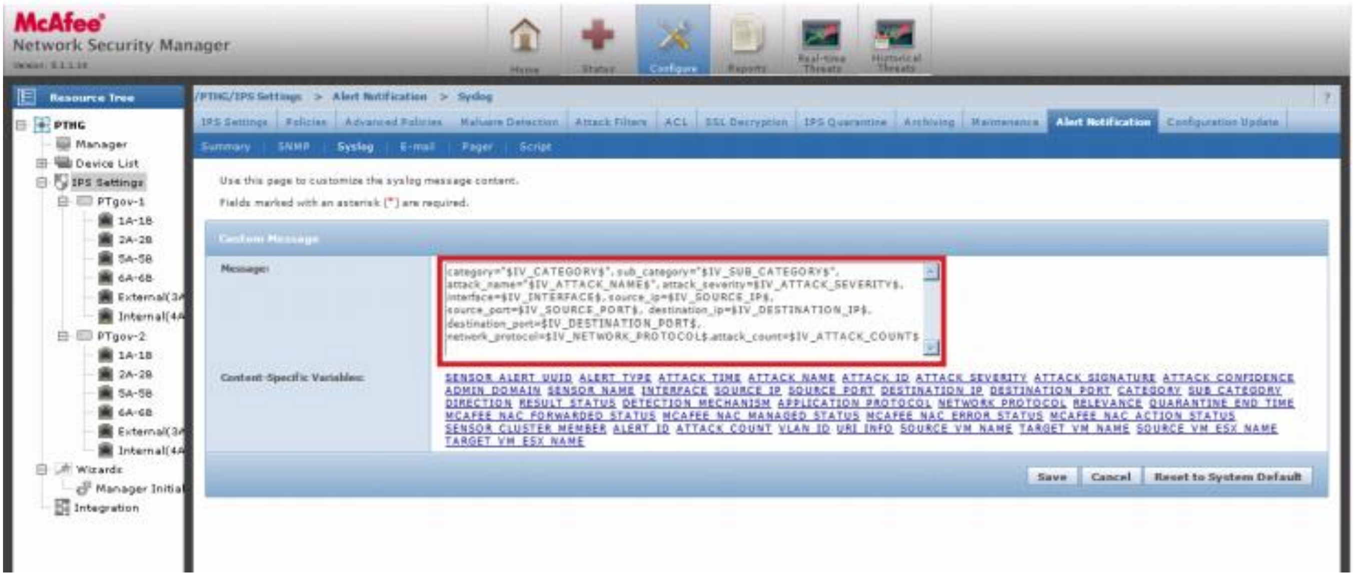
Examples:_



Use this page to enable syslog notification and to define syslog servers.

Fields marked with an asterisk (*) are required.

Update Successful.



Use this page to customize the syslog message content.

Fields marked with an asterisk (*) are required.

Message:

```
category="$IV_CATEGORY$", sub_category="$IV_SUB_CATEGORY$",
attack_name="$IV_ATTACK_NAME$", attack_severity=$IV_ATTACK_SEVERITY$,
interface=$IV_INTERFACE$, source_ip=$IV_SOURCE_IP$,
source_port=$IV_SOURCE_PORT$, destination_ip=$IV_DESTINATION_IP$,
destination_port=$IV_DESTINATION_PORT$,
network_protocol=$IV_NETWORK_PROTOCOL$,attack_count=$IV_ATTACK_COUNT$
```

Content-Specific Variables: SENSOR ALERT UUID ALERT TYPE ATTACK TIME ATTACK NAME ATTACK ID ATTACK SEVERITY ATTACK SIGNATURE ATTACK CONFIDENCE ADMIN DOMAIN SENSOR NAME INTERFACE SOURCE IP SOURCE PORT DESTINATION IP DESTINATION PORT CATEGORY SUB CATEGORY DIRECTION RESULT STATUS DETECTION MECHANISM APPLICATION PROTOCOL NETWORK PROTOCOL RELEVANCE QUARANTINE END TIME MCAFEE NAC FORWARDED STATUS MCAFEE NAC MANAGED STATUS MCAFEE NAC ERROR STATUS MCAFEE NAC ACTION STATUS SENSOR CLUSTER MEMBER ALERT ID ATTACK COUNT VLAN ID URI INFO SOURCE VM NAME TARGET VM NAME SOURCE VM ESX NAME TARGET VM ESX NAME

Purchases and Sales Cooperation: sales@npartnertech.com

Technical Support: support@npartnertech.com

N-Partner