



Pulse Policy Secure: Admission Control using IBM QRadar

Deployment Guide

Published

February, 2021

Document Version

2.0

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

www.pulsesecure.net

© 2021 by Pulse Secure, LLC. All rights reserved.

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Pulse Policy Secure: Admission Control using IBM QRadar

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at <http://www.pulsesecure.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Revision History

The following table lists changes made to this document:

Document Revision	Release	Date	Changes
2.0		February, 2021	Added Adding Root/Intermediate CA certificate.

Contents

PURPOSE OF THIS GUIDE	1
PREREQUISITES.....	1
ALERT-BASED ADMISSION CONTROL WITH IBM QRADAR	3
OVERVIEW OF ALERT-BASED ADMISSION CONTROL WITH IBM QRADAR	3
SUMMARY OF CONFIGURATION	4
CONFIGURING PPS WITH IBM QRADAR.....	4
ADMISSION CONTROL TEMPLATE.....	5
ADMISSION CONTROL CLIENT.....	6
ADMISSION CONTROL POLICIES.....	7
CONFIGURING IBM QRADAR.....	10
ADDING ROOT/INTERMEDIATE CA CERTIFICATE	10
INSTALL PULSE POLICY SECURE ALERT ADD-ON FOR IBM QRADAR	11
SENDING OFFENSE INFORMATION TO PPS	13
ALERT ACTION BASED ON SOURCE IP/MAC ADDRESS.....	15
TROUBLESHOOTING	16

Purpose of this Guide

This guide describes how to configure Pulse Policy Secure (PPS) to provide Alert-based admission control protection for your network using IBM QRadar.

Prerequisites

This guide assumes you are familiar with the use of the following products and their related terminology.

Note: Root/Intermediate CA certificate should be present in IBM QRadar Trust store and PPS should use this CA issued certificate.

- Pulse Policy Secure at version 9.1R3.
- IBM QRadar at version 7.3.2 Build 20190705120852
- Palo Alto Firewall (IBM QRadar configured as syslog Server)
- Pulse Secure app at version 1.0.0
- 802.1X/RADIUS CoA supported Switch/WLC

Alert-Based Admission Control with IBM QRadar

• Overview of Alert-Based Admission Control with IBM QRadar	3
• Summary of Configuration.....	4
• Configuring PPS with IBM QRadar	4
• Configuring IBM QRadar.....	10
• Troubleshooting	16

This section describes how to integrate IBM QRadar SIEM device with PPS to support alert-based admission control in your network.

Overview of Alert-Based Admission Control with IBM QRadar

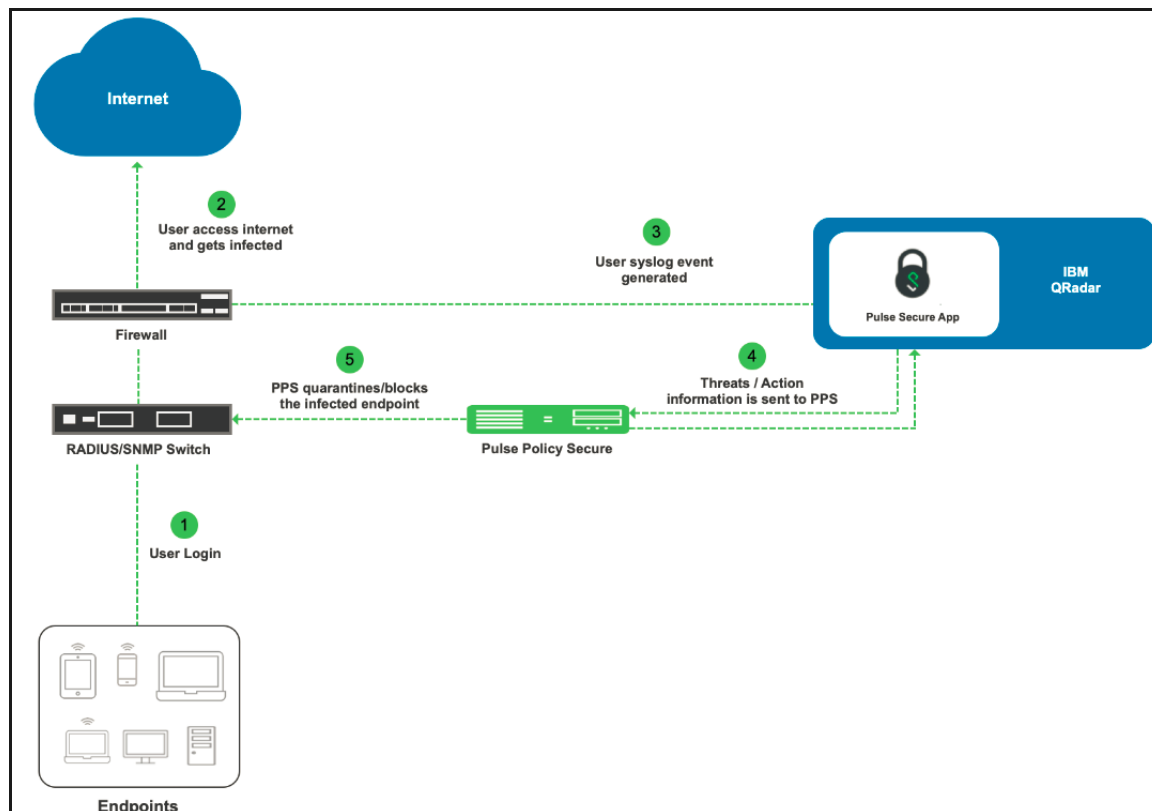
Pulse Policy Secure (PPS) integration with the IBM QRadar provides complete visibility of network endpoints, including unmanaged endpoints and provide end to end network security. The PPS integration with IBM QRadar integration allows Admin to perform user access control based on alerts received from the IBM QRadar.

IBM QRadar receives log or threat information from various log sources such as Palo Alto Network firewall. Based on the offense rules configured on IBM QRadar an offense is created to trigger alerts to PPS. PPS takes action on user session by blocking or quarantining the user.

The authentication process is described below:

1. User downloads a file from the Internet. The perimeter firewall scans the file and, based on user-defined policies, sends the file for analysis.
2. Firewall detects that the file contains malware and a threat alert syslog gets generated and sent to IBM QRadar.
3. Based on the offense rules configured on IBM QRadar. It generates alerts and this has to be manually sent to PPS with the help of Pulse Secure App.
4. The offense includes severity, credibility and other information for the affected endpoint.
5. The PPS server quarantines/blocks the endpoint based on the configured Admission control policies.

Figure 1 Deployment using PPS, IBM QRadar and Palo Alto Networks Firewall



In this example, the endpoint is connected to a third-party switch. The switch has 802.1X/MAB authentication enabled. As an alternate, SNMP enforcement mechanism can also be used.

Summary of Configuration

To prepare your network to perform alert-based admission control using Pulse Policy Secure, IBM QRadar and Firewall, perform the following tasks:

The following sections describe each of these steps in detail.

- [“Configuring PPS with IBM QRadar” on page 4](#)
- [“Configuring IBM QRadar” on page 10](#)

Configuring PPS with IBM QRadar

The PPS configuration requires defining the IBM QRadar as a client in PPS. PPS acts as a REST API server for IBM QRadar.

A high-level overview of the configuration steps needed to set up and run the integration is described below:

- The Administrator configures the basic PPS configurations such as creating an authentication server, authentication realm, user roles, and role mapping rules.

- Configure IBM QRadar as a client in PPS. PPS acts as a REST API Server for IBM QRadar. The REST API access for the admin user needs to be enabled by accessing the serial console or alternatively from the PPS admin UI (Authentication > Auth Server > Administrators > Users > click “admin”, enable Allow access to REST APIs).
- Configure PPS to block/quarantine the endpoint based on the threat prevention policy.
- Configure the Switches/WLC as RADIUS Client in PPS (Endpoint Policy > Network Access > Radius Clients > New Radius Client). Switch should be configured with PPS as a RADIUS server.
- Configure RADIUS return attribute policies to define the action upon receiving the event.

Note: Ensure that PPS has the endpoint IP Address for the enforcement to work correctly.

This section covers the following topics:

- [“Admission Control Template” on page 5](#)
- [“Admission Control Client” on page 6](#)
- [“Admission Control Policies” on page 7](#)

Admission Control Template

The admission control template provides the list of possible events that can be received from the network security device along with regular expression to parse the message. The template also provides possible actions that can be taken for an event. PPS is loaded with default templates for IBM QRadar.

To view the admission control template in PPS:

1. Select Endpoint Policy > Admission Control > Templates.

Figure 2 IBM QRadar Template

templates

Configure

Templates

New Template...

Delete...

Restore Factory Default...

10 records per page

Search:

	Name	File Name	Protocol Type	Vendor	Device Type
1	fortianalyzer-text.itmpl Syslog integration with FortiAnalyzer using text format messages.	fortianalyzer-text.itmpl	Syslog	Fortinet	Analyzer
2	paloaltonetworksfw-ietf-bsd.itmpl Syslog integration with Palo Alto Networks Firewall using IETF/BSD format messages.	paloaltonetworksfw-ietf-bsd.itmpl	Syslog	Palo Alto Networks	Firewall
3	fortianalyzer-cef.itmpl Syslog integration with Forti Analyzer using CEF format messages.	fortianalyzer-cef.itmpl	Syslog	Fortinet	Analyzer
4	fortigate-cef.itmpl Syslog integration with Fortinet Firewall using CEF format messages.	fortigate-cef.itmpl	Syslog	Fortinet	Firewall
5	fortigate-text.itmpl Syslog integration with Fortinet Fortigate Firewall using text format messages.	fortigate-text.itmpl	Syslog	Fortinet	Firewall
6	juniper-policy-enforcer-http.itmpl Integration with Juniper's Policy Enforcer which sends endpoint control commands to PPS	juniper-policy-enforcer-http.itmpl	HTTP	Juniper Networks	Policy Enforcer
7	nozomi-scadaguardian-cef.itmpl Syslog integration with Nozomi Network's SCADAGuardian using CEF format messages.	nozomi-scadaguardian-cef.itmpl	Syslog	Nozomi Networks	SCADAGuardian
8	ibm-qradar-http.itmpl Integration with IBM Qradar which sends endpoint control commands/offenses to PPS	ibm-qradar-http.itmpl	HTTP	IBM Qradar	SIEM

Admission Control Client

The admission control clients are the network security devices on which the syslog forwarding is enabled. The messages are received by the syslog server module running on PPS.

To add IBM QRadar as a client:

1. Select **Endpoint Policy > Admission Control > Clients**.
2. Click **New Client**.
3. Enter the name.
4. Enter the description.
5. Enter the IP address of the client.
6. Under Template, select IBM Qradar-SIEM-HTTP-JSON.
7. Click **Save Changes**.

Figure 3 Figure 3: Template

Admission Control > Configure > Clients > New Client

New Client

* Name: Label to reference this client.

Description:

* IP Address: IP Address of this client.

* Template: Template used by the client

Selected Template Details

Template name	Vendor	Device	Protocol	Format	Description
ibm-qradar-http.itmpl	IBM Qradar	SIEM	HTTP	JSON	Integration with IBM Qradar which sends endpoint control commands/offenses to PPS

* indicates required field

Admission Control Policies

The admission control policies define the list of actions to be performed on PPS for the user sessions. The actions are based on the event and the severity information received from the network security device.

To view and add the new integration policy:

1. Select **Endpoint Policy > Admission Control > Policies**.
2. Click **New Policy**.
3. Enter the policy name.
4. Select **IBM QRadar--SIEM-HTTP-JSON** as a template.
5. Under Rule on Receiving, select the event type (block-endpoint, quarantine-endpoint, alert, any) and the severity level. The event types and the severity level are based on the selected template.

The actions on sessions supported are:

- Block Endpoint: Blocks the host MAC Address on the PPS permanently. If admin choose to clear this, it can be cleared either by using IBM QRadar application or by using the PPS Admin UI.
 - Quarantine Endpoint (Change user roles): Changes the roles assigned to the user on PPS so that restriction/privileges for the user can be changed.
 - Offense – Generated based on the Severity level and magnitude of the alert. Specify the magnitude and severity of the offense (High, Information, Low, Medium, Any). Enter the Count Value (1-256)
6. Under then perform this action, select the desired action.
 - Block the endpoint from authenticating the network.

- Put the endpoint into a quarantine network by assigning this role — choose the role to put endpoint in quarantine role. Specify whether to apply the role assignment permanently or only for the session.
- Terminate user session—Terminates the user session on the PPS.
- Ignore (log the event) —Received syslog event details are logged on the PPS and no specific action is taken.

7. Under Roles, specify:

- Policy applies to ALL roles—To apply the policy to all users.
- Policy applies to SELECTED roles—To apply this policy only to users who are mapped to roles in the Selected roles list. You must add roles to this list from the Available roles list.
- Policy applies to all roles OTHER THAN those selected below—To apply this policy to all users except for those who map to the roles in the Selected roles list. You must add roles to this list from the Available roles list.

Figure 4 Configuration Policies

Admission Control > Configure > Policies > Pilo

Pilo

* Name:

* Template:

Template name	Vendor	Device	Protocol	Format	Description
ibm-qradar-http.itmpl	IBM Qradar	SIEM	HTTP	JSON	Integration with IBM Qradar which sends endpoint control commands/offenses to PPS

▼ Rule on receiving

* Events:

* Magnitude (>=): Match when magnitude of the offense is greater than or equal to this value.

* Severity (>=): Match when severity of the offense is greater than or equal to this value.

▼ Count these many times

* Count:

▼ then perform this action

☒ Put the endpoint into a quarantine network by assigning this role:

Make this role assignment

☒ Permanent

☐ For this session only

☐ Block the endpoint from authenticating to the network

☐ Terminate user session

☐ Ignore (just log the event)

▼ Roles

☐ Policy applies to ALL roles

☒ Policy applies to SELECTED roles

☐ Policy applies to all roles OTHER THAN those selected below

Available roles:

- Guest
- Guest Admin
- Guest Sponsor
- Guest Wired Restrict
- LimitedAccessRole

Add ->

Remove

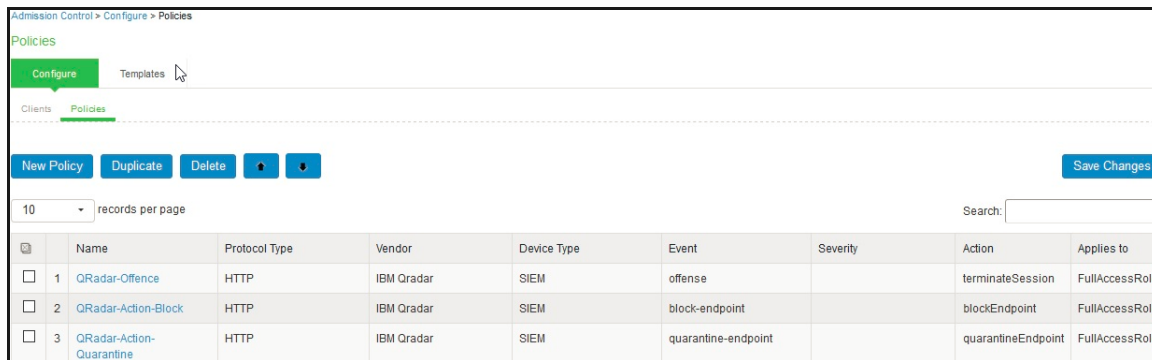
Selected roles:

- FullAccessRole

* indicates required field

8. Click **Save Changes**.

Once the policy is created. You can see the summary page as shown below. The following page shows the different policies created for different events with different user roles.



Configuring IBM QRadar

This section covers the following topics:

- “Adding Root/Intermediate CA Certificate”
- “Install Pulse Policy Secure Alert Add-On for IBM QRadar” on page 11
- “Sending Offense information to PPS” on page 13
- “Alert Action Based on Source IP/MAC Address” on page 15

Adding Root/Intermediate CA Certificate

To add Root/Intermediate CA certificate:

1. Perform an SSH connection to the IBM QRadar as Root User or with equivalent user privilege.
2. Copy the intermediate/Root CA certificate to `/etc/pki/ca-trust/source/anchors`.
3. Run the command `update-ca-trust`.

Note: If the user fails to Add Root/CA intermediate certificate before installing Pulse Secure Alert Add-On, the following additional steps needs to be performed.

```
# Find the Pulse Secure Alert Add-on app process ID.
[root@ibm-qradar-qa anchors]# /opt/qradar/support/recon ps
App-ID Name Managed Host ID Workload ID Service Name AB Container Name CDEGH Port IJKL
1252 Pulse Secure 53 apps qapp-1252 ++ qapp-1252 +++++ 5000 ++++

[root@ibm-qradar-qa anchors]# docker container ls
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
a116cd36dbf1 console.localdeployment:5000/qapp/1252:1.0.0-20210222111523 "sh /
start_container..." 17 minutes ago Up 17 minutes 0.0.0.0:32771->5000/tcp qapp-1252-zwgv1DhV

# Copy the CA certificate (pps.pem)to below mentioned location.
root@ibm-qradar-qa anchors]# docker cp pps.pem a116cd36dbf1:/etc/pki/ca-trust/source/
anchors
# Connect to the Pulse Secure Alert Add-on app Console.
root@ibm-qradar-qa anchors]# /opt/qradar/support/recon connect 1252

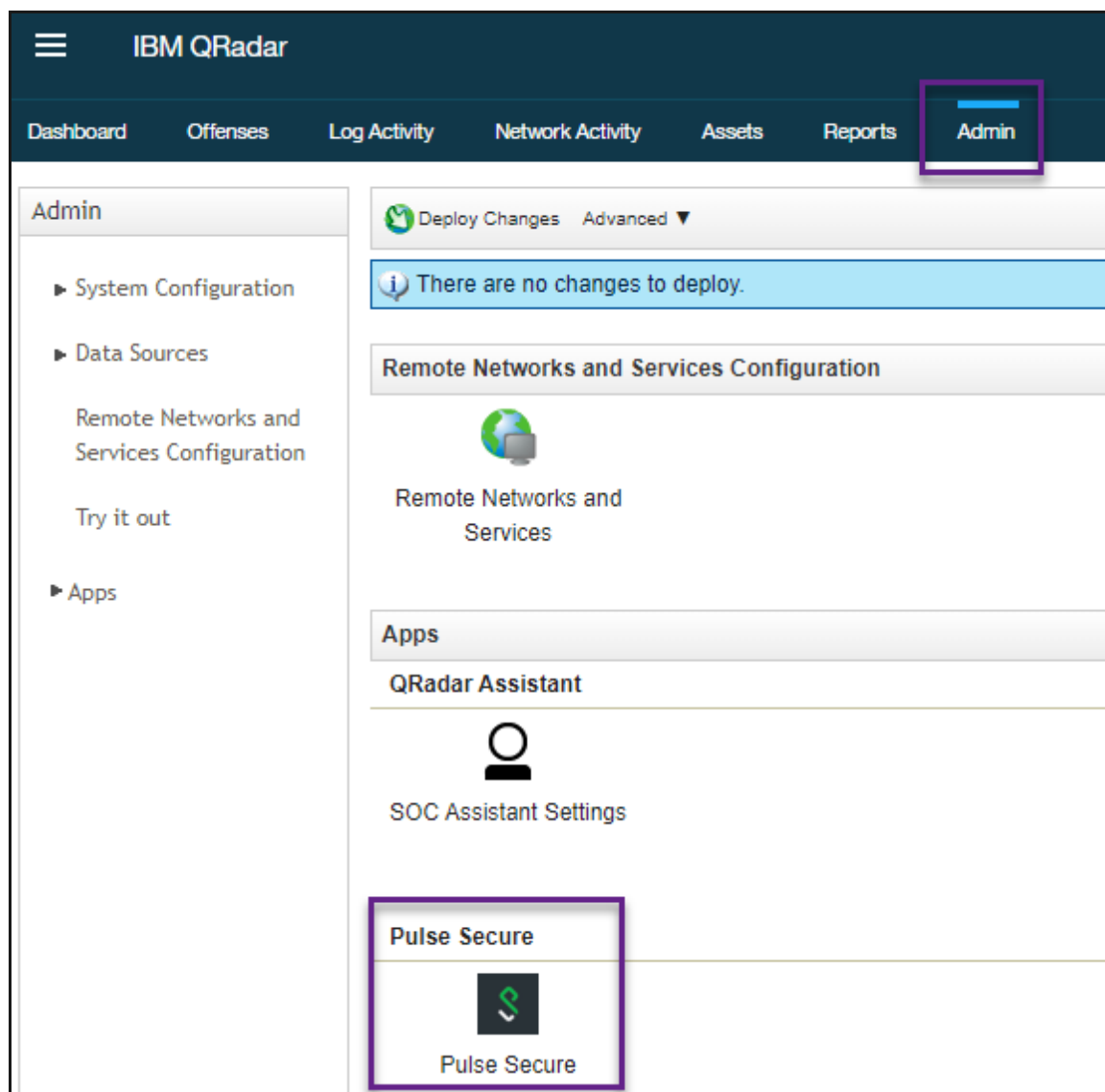
# Update the CA trust.
update-ca-trust
```


Install Pulse Policy Secure Alert Add-On for IBM QRadar

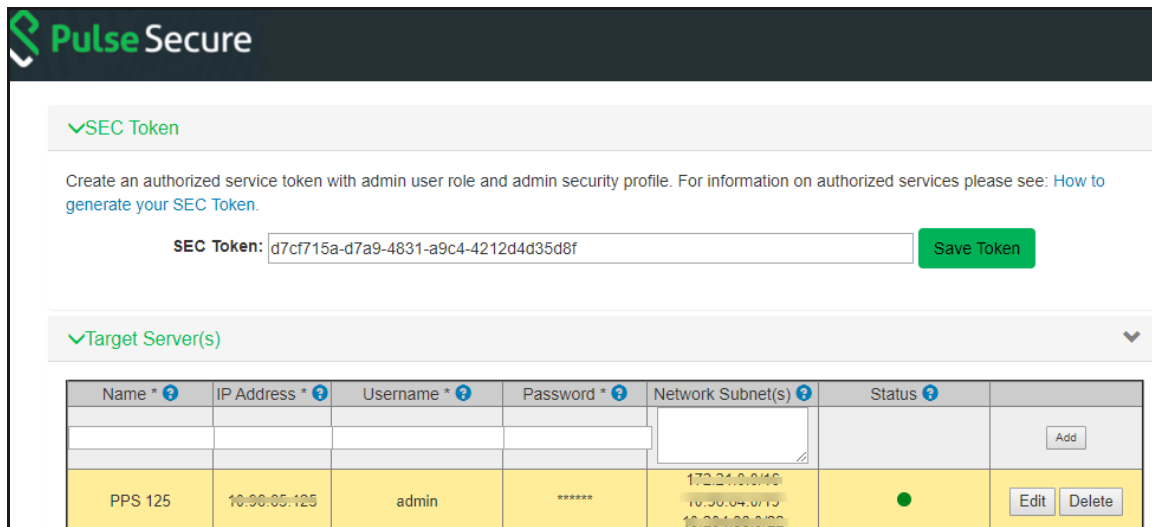
Download the PulseSecureAppForQRadar.zip file from Pulse Secure software downloads location and install them onto your IBM QRadar server. You can also download and install the Pulse Secure app from IBM X-Force exchange site.

To configure the Pulse Policy Secure App:

1. Log into IBM QRadar as an **Admin** user.
2. In the IBM QRadar Dashboard, select the Admin tab.
3. Select **Extension Management**.
4. In the Extensions Management window, click Add and select the app archive that you want to upload to the console
5. Click Browse and upload the Pulse-Secure.zip file to install the Pulse Secure App for IBM QRadar.



6. After installation, Pulse Secure App for IBM QRadar appears in the App section.
7. Select **Authorized Services**, and then select **Add Authorized Service** and follow the wizard to create authorized service.
8. Copy the Authentication Token.
9. Select the Pulse Secure Icon, paste or enter the authentication token and Save.
10. Enter the name, PPS IP address, user name, network subnet to send offenses/action. Click Add.
11. Click **Save**.



✓SEC Token

Create an authorized service token with admin user role and admin security profile. For information on authorized services please see: [How to generate your SEC Token](#).

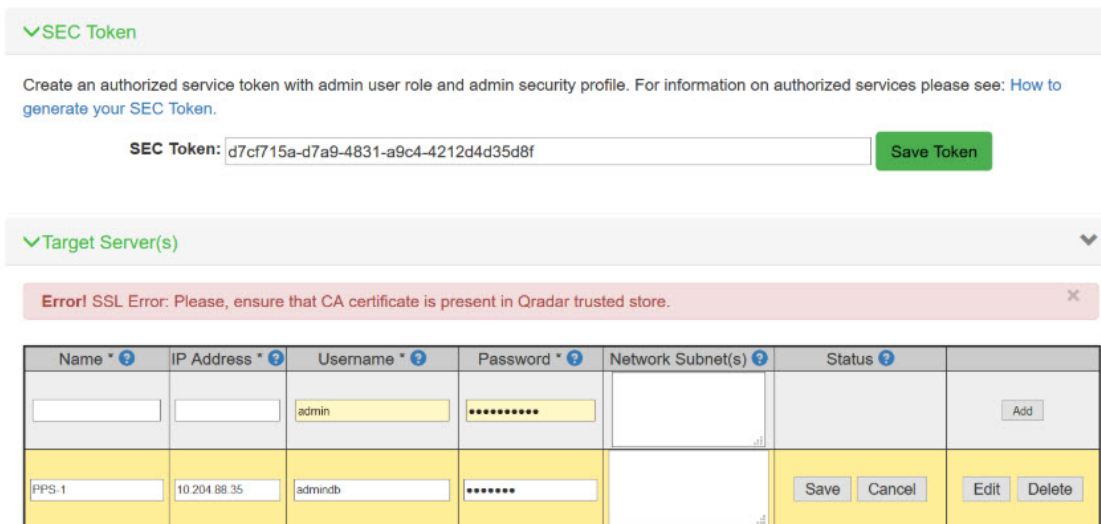
SEC Token:

✓Target Server(s)

Name *	IP Address *	Username *	Password *	Network Subnet(s) *	Status *	
						<input type="button" value="Add"/>
PPS 125	10.90.05.125	admin	*****	172.24.0.0/16 10.30.04.0/15 10.30.03.0/22	●	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Note: If the user gets the SSL error "Please ensure that CA certificate is present in QRadar trusted store" follow the steps mentioned in ["Adding Root/Intermediate CA Certificate"](#).

Figure 5 SSL Error



✓SEC Token

Create an authorized service token with admin user role and admin security profile. For information on authorized services please see: [How to generate your SEC Token](#).

SEC Token:

✓Target Server(s)

Error! SSL Error: Please, ensure that CA certificate is present in Qradar trusted store.

Name *	IP Address *	Username *	Password *	Network Subnet(s) *	Status *	
		admin	*****			<input type="button" value="Add"/>
PPS-1	10.204.88.35	admindb	*****			<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

Sending Offense information to PPS

To send the offense information to PPS:

1. Login to the IBM QRadar console and click **Offenses**.
2. In the left pane, select **All Offenses**. The full list of offenses is displayed.
3. Double-click on an offense. The Offense detail page opens. The Relevance, Severity and Credibility values are listed in the right corner.
 - High Credibility and (High) Severity events – By default the last offense credibility is set to 8, 9, and 10.

- Medium Credibility and (Medium) Severity events - By default the last offense credibility is set to 4, 5, 6, and 7.
- Low Credibility and (Low) Severity events - By default the last offense credibility is set to 1, 2, and 3

Offense 10 Summary

Magnitude		Status		Relevance	0	Severity	7	Credibility	3
Description	FileType Detected			Offense Type	Source IP				
Source IP(s)	10.20.71.100			Event/Flow count	3 events and 0 flows in 1 categories				
Destination IP(s)	10.20.10.114			Start	Sep 9, 2019, 1:13:03 PM				
Network(s)	Net-10-170-102.Net_10_0_0_0			Duration	9m 14s				
				Assigned to	Unassigned				

Offense Source Summary

IP	10.20.71.100	Location	Net-10-170-102.Net_10_0_0_0
Magnitude		Vulnerabilities	0
Username	Unknown	MAC Address	Unknown NIC
Host Name	Unknown		
Asset Name	Unknown	Weight	0
Offenses	1	Events/Flows	3

- Click **Send to Pulse Policy Secure**. The Success or Failure message is displayed based on the action.

Pulse Secure

Sending offense for the host 10.20.71.100 to the following destinations:

- 10.20.71.100 -
- 10.20.71.100 -
- 10.20.10.114 -

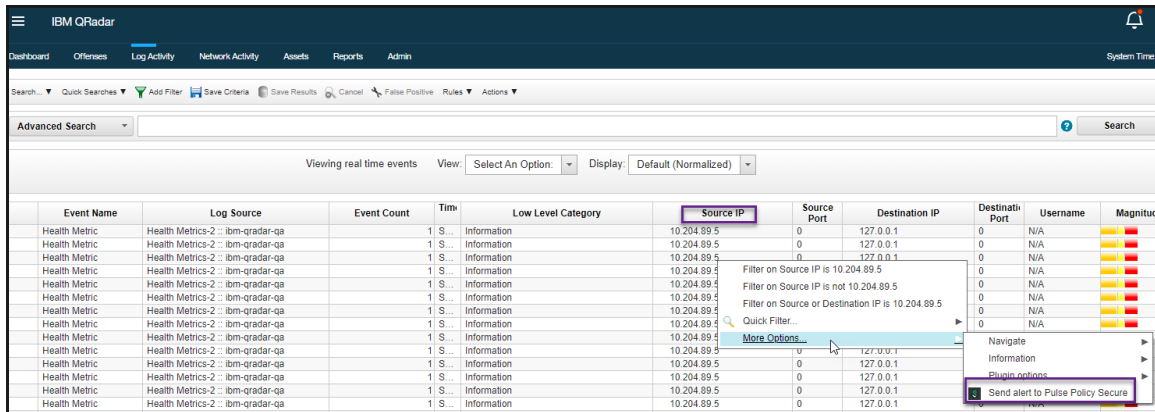
Send **Cancel**

Note: Pulse Secure App supports only four types of offenses: Source/Destination IP address, Source/Destination MAC address.

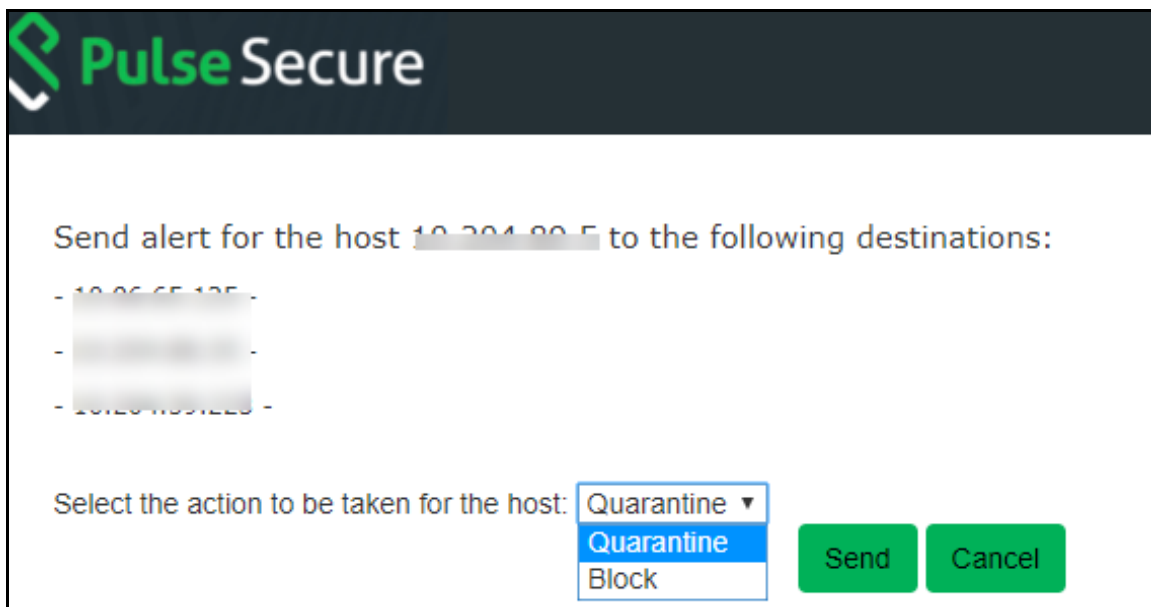
Alert Action Based on Source IP/MAC Address

SIEM provides live streaming of the processed events and flows. SIEM admin live monitors these log and network activity. Expert SIEM admin can identify the malicious host by monitoring these data. Pulse Secure application provides an option for the SIEM admin to take action for such host based on IP Address even if these are not listed under alerts.

1. Click **Log Activity/Network Activity** in IBM QRadar console.
2. Under Source IP column select the host by IP address or MAC address.
3. Click **Send alert to Pulse Policy Secure**.



4. On the new page, SIEM user needs to decide the action and the PPS server IP.
5. Click **Send**.

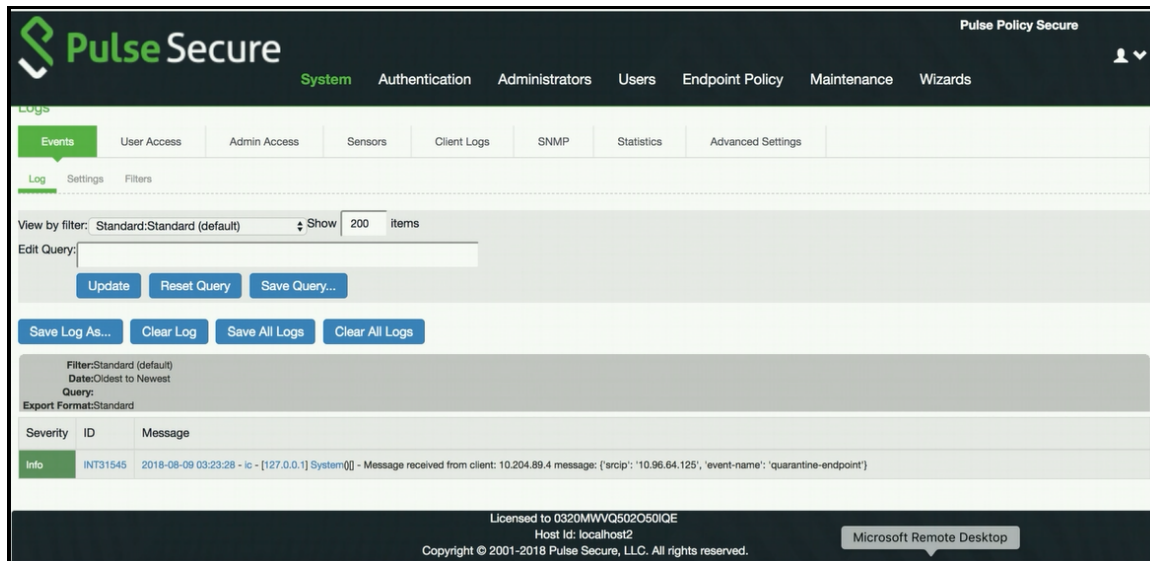


For more information on IBM QRadar configuration, see *IBM QRadar documentation*.

Troubleshooting

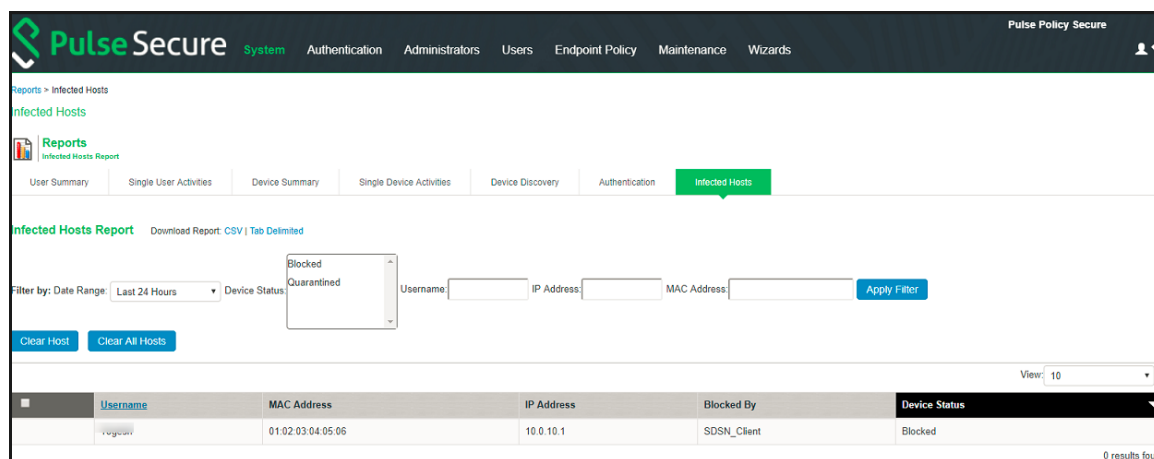
To verify the event logs on PPS, select System > Log/Monitoring > Events. Ensure Admission control events option is enabled in Event logs settings.

You can verify that the event logs are generated every time when an event is received from IBM QRadar.



To verify the user access logs, select System > Logs & Monitoring > User Access to verify the user login related logs like realm, roles, username and IP address.

You can also verify whether the quarantined/blocked host is listed in the Infected Devices report, which lists the mac address, IP address, and the device status. To verify the reports, select System > Reports > Infected Devices.



You can also enable debug logs to troubleshoot any issues. Select Maintenance > Troubleshooting > Monitoring > Debug Log to enable debug logs.

Pulse Secure System Authentication Administrators Users Endpoint Policy **Maintenance** Wizards Pulse Policy Secure on PPS_176

Troubleshooting > Monitoring > Debug Log

Debug Log

User Sessions **Monitoring** Tools System Snapshot Remote Debugging

Debug Log Node Monitor Cluster Diagnostic Logs

Save Changes Reset Save Debug Log Clear Log...

Debug Log Settings

Current Log Size 5078 bytes

Debug Logging On ☒

Max Debug Log Size 200 MB

Debug Log Detail Level 50

Include logs ☒

Process Names:

Event Codes: integrations

System

Import/Export

Push Config

Archiving

Troubleshooting

▼ User Sessions Remote Debugging

Policy Tracing

▼ Monitoring

Debug Log

Node Monitor

Cluster

Diagnostic Logs

▼ Tools

TCP Dump

Commands

Kerberos

System Snapshot

A positive number

Selecting this option will include system logs

Comma separated, list of process names to log

Comma separated, list of events to log

