



# Cisco ISE pxGrid App 3.0.0 for IBM QRadar SIEM

Author: Jason Kunst

October 2021

# Table of Contents

<b>About This Document</b> .....	<b>4</b>
<b>Solution Overview</b> .....	<b>5</b>
<b>Technical Details</b> .....	<b>6</b>
<b>Cisco ISE pxGrid Installation</b> .....	<b>8</b>
<b>Generating the Cisco ISE pxGrid App Certificate</b> .....	<b>12</b>
<b>Installing Cisco ISE pxGrid App</b> .....	<b>15</b>
Configuring pxGrid Integration on QRadar .....	22
Setup Indexing in QRadar .....	29
App installation on QROC .....	31
<b>Cisco ISE pxGrid App Dashboard Panels</b> .....	<b>33</b>
Search Functionality .....	40
Passed Authentications .....	42
Devices .....	45
Failed Authentications .....	48
User Panel .....	48
Failure Reason Panel .....	50
Auth Type Panel.....	51
Locations Panel.....	53
Compliance .....	55
TrustSec .....	57
Mobile Device Management (MDM) .....	59
ANC Details.....	60
<b>Configuring Cisco ISE Adaptive Network Control Policies</b> .....	<b>61</b>
Configuring Default ANC policies for Cisco ISE pxGrid App .....	62
Adding ANC Policies to ISE Policy Sets .....	63
<b>Performing Cisco ISE ANC Mitigation Actions Through Cisco ISE pxGrid App Dashboard Panel</b> .....	<b>64</b>

---

<b>Configuring IBM QRadar for Cisco ISE Syslog Events .....</b>	<b>70</b>
<b>Configuring Cisco ISE Syslog Events.....</b>	<b>72</b>
<b>Performing ISE ANC Mitigation Actions Through IBM QRadar Syslog Events .....</b>	<b>75</b>
Creating Custom Field for Framed IP Address ISE Syslog Event.....	75
ANC Mitigation Syslog Event Example .....	84
<b>Hovering Over IBM QRadar Syslog IP Address for ISE Contextual Information .....</b>	<b>88</b>
<b>IBM QRadar Cisco ISE pxGrid Offense Rule.....</b>	<b>89</b>
Verify pxGrid offense rule via Log Activity .....	91
Verify pxGrid offense rule via Offenses Dashboard .....	93
Taking ISE ANC mitigations from Offenses Dashboard.....	93
<b>Addendums.....</b>	<b>98</b>
Adding Log Activity Filter to View Session Information .....	98
Using an External Certificate Authority .....	99
Generating IBM QRadar Certificate from ISE Internal CA .....	101
<b>Troubleshooting .....</b>	<b>107</b>
Cisco ISE pxGrid App pxGrid client not showing under ISE pxGrid Client View .....	107
Cisco ISE pxGrid App pxGrid client not showing under ISE pxGrid Web Client View .....	107
Cisco ISE pxGrid Dashboards not populating with ISE Contextual Information.....	107
Using the IBM QRadar pxGrid App Logs for Troubleshooting.....	107
Here are some more log issues with connectivity:.....	109
TCP Dump to Analysis Failed Certificate Exchange in ISE.....	111
TCP Dump to Check if pxGrid Logs are Available in QRadar .....	112
Uploading Logs with the case .....	112

## About This Document

This document is for Cisco System Engineers, IBM Engineers, Partners, and Customers deploying the Cisco Identity Services Engine (ISE) Cisco Platform Exchange Grid (pxGrid) App v3.0+ for IBM the QRadar SIEM.

The supported platforms are:

- IBM QRadar – As per recommendations for python 3 (python 2 is end of support), this is supported on the following versions – 7.3.3 FP6, 7.4.1 FP2, and 7.4.2 or later.
- Cisco ISE 2.4 and higher with latest patch (check latest recommended release for newest code).

For this release, validation has been done with the following:

- The ISE internal CA was used for generating the pxGrid certificates for the Cisco ISE pxGrid App.
- Various tests with 7.3.3 FP7, 7.4.1 FP2 and 7.4.2, and ISE Version 2.4, 2.7, 3.0 (with latest patches).
- Standalone and hybrid distributed deployments.

It is also assumed that the reader is familiar with both IBM QRadar SIEM and Cisco ISE.

**Note:** As of July 2021, this guide is written using ISE 3.0 and 7.4.2 as a reference. If you're looking for older version of guide and screenshots, please use app version guide 2.x at <http://cs.co/ise-guides>. The screens for ISE 3.x are slightly different but operationally the same.

This document provides the details of installing and configuring the Cisco ISE pxGrid App for the IBM QRadar SIEM. The Cisco ISE pxGrid App provides Dashboards for Passed Authentications, Failed Authentications, Devices, Compliances, TrustSec, Mobile Device Management (MDM), and Currently Assigned ANC Policies.

Cisco Adaptive Network Control (ANC) mitigation actions can be taken directly from the Dashboards to quarantine endpoints according to an organization's security policy. These ANC mitigations can also be enforced via IBM QRadar SIEM syslog events as long as the endpoint has been authenticated through ISE.

The Cisco ISE pxGrid App contains an IBM QRadar pxGrid offense rule which is based on pxGrid RADIUS failure topic events.

The contextual information can be obtained from the IP Address of syslog events as long as the endpoint has been authenticated through IS.

## Solution Overview

IBM® QRadar® SIEM detects anomalies, uncovers advanced threats, and removes false positives. It consolidates log events and network flow data from thousands of devices, endpoints, and applications distributed throughout a network. It then uses an advanced Sense Analytics engine to normalize and correlate this data and identifies security offenses requiring investigation. As an option, it can incorporate IBM X-Force® Threat Intelligence which supplies a list of potentially malicious IP addresses including malware hosts, spam sources, and other threats. QRadar SIEM is available on premises and in a cloud environment.

Cisco Identity Services Engine (ISE) is a security policy management and identity access management solution. ISE provides centralized management by defining, issuing, or enforcing 802.1X authentications, guest access management, policies, posture, client provisioning, and TrustSec policies. The ISE session directory contains a wealth of information about the endpoint that is published by Cisco Platform Exchange Grid (pxGrid).

ISE also simplifies access control and security compliance for wired, wireless, and VPN connectivity and supports corporate security policy initiatives such as BYOD.

Cisco Platform Exchange Grid (pxGrid) enables multivendor, cross platform network system collaboration among parts of the IT infrastructure such as security monitoring and system detection, network policy platforms, asset and virtually configuration management identity and access management platforms and other IT solutions. pxGrid uses a pub/sub model to publish the contextual information received from ISE, and other security solutions will subscribe to this topic, providing more visibility into security operations. Other security solutions can use pxGrid to enforce their security policies.

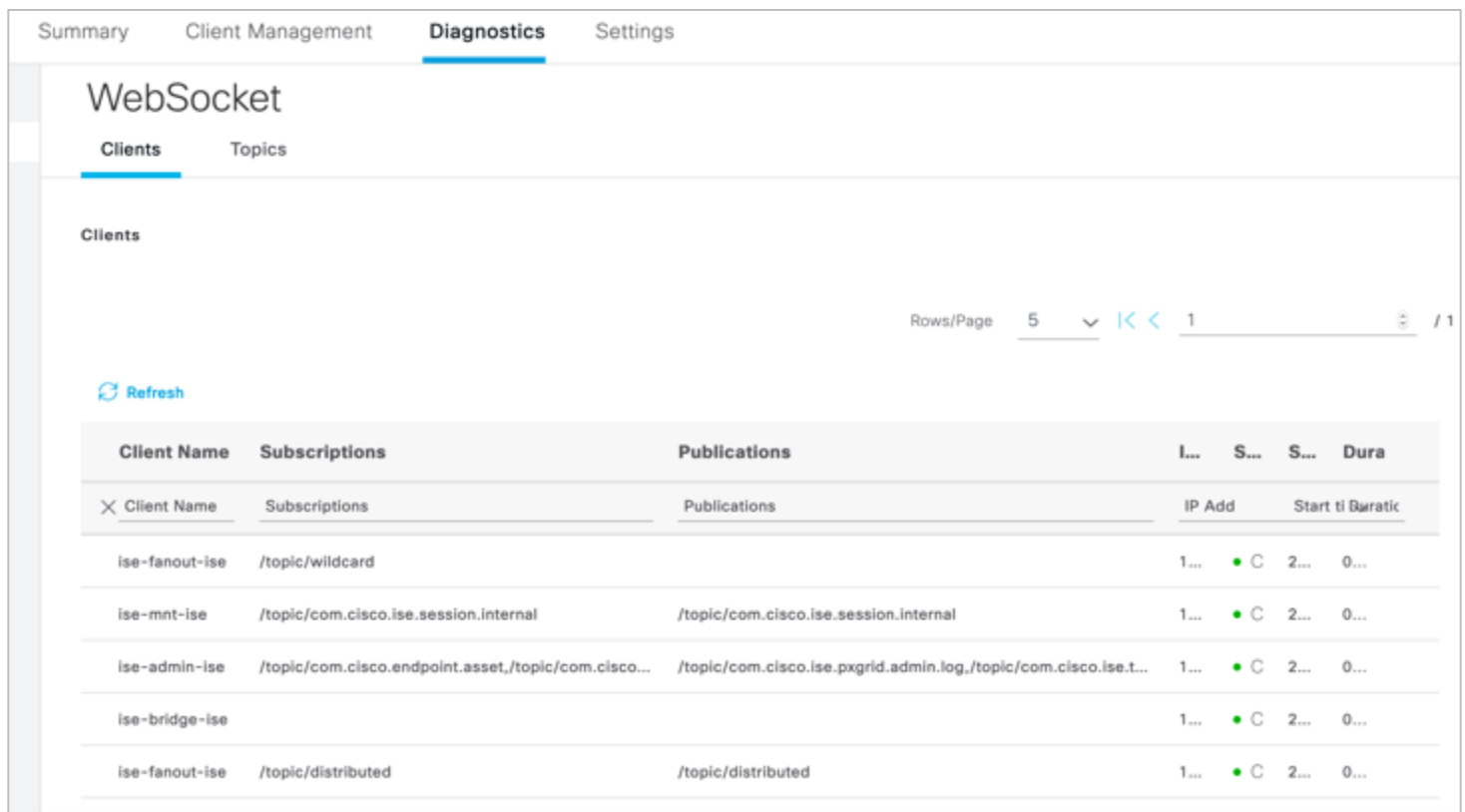
## Technical Details

The Cisco ISE pxGrid App installs on an IBM QRadar SEIM instance as an IBM signed app. Once the app is installed, the Cisco ISE pxGrid App will be registered as a pxGrid client to the ISE pxGrid node and subscribe to topics and consume contextual information to populate the Dashboards and take Adaptive Network Control (ANC) mitigation actions.

The following image is a single standalone ISE 3.0:

- Go to Administration > pxGrid Services > Diagnostics > WebSocket.

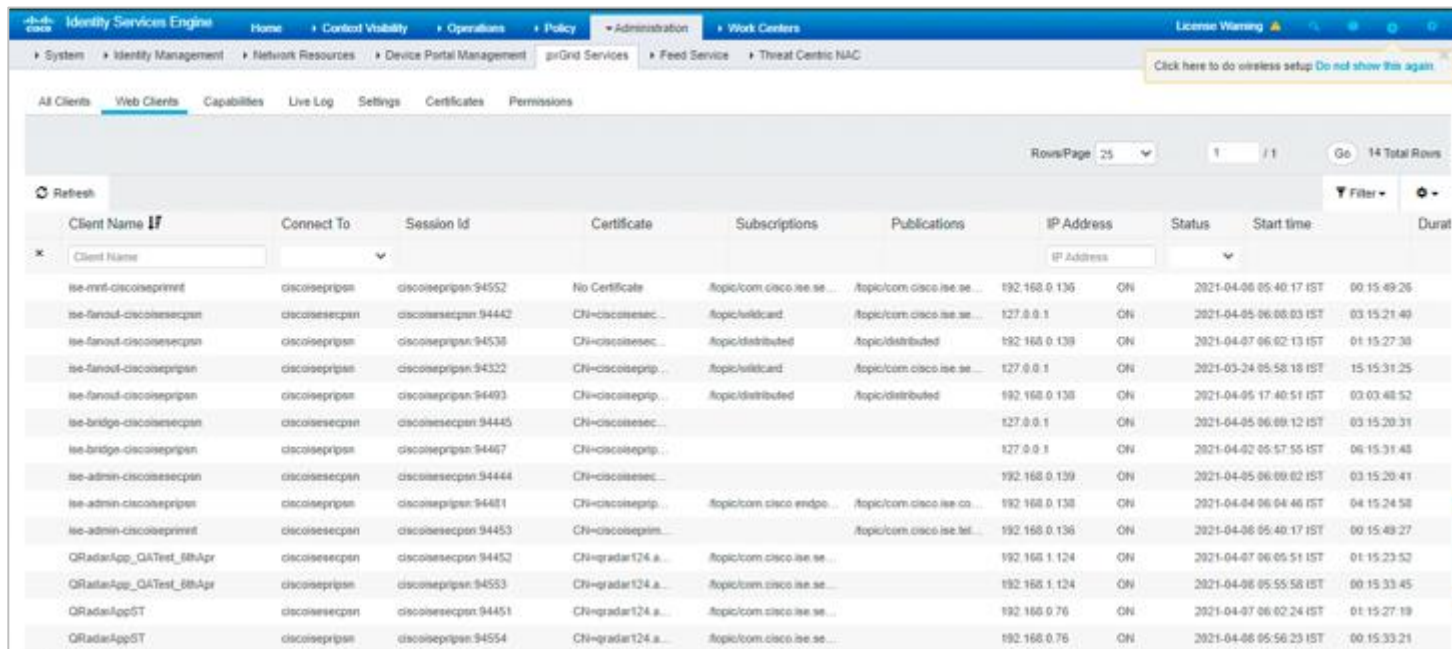
Note: This system is using pxGrid 2.0 which is based on WebSockets. XMPP is for pxGrid 1.0 and is not used and will be deprecated in ISE 3.1.



The screenshot displays the 'Clients' tab under the 'WebSocket' section in the 'Diagnostics' menu. It shows a table of registered clients with the following data:

Client Name	Subscriptions	Publications	IP Add	Status	Start ti	Duratic
ise-fanout-ise	/topic/wildcard		1...	● C	2...	0...
ise-mnt-ise	/topic/com.cisco.ise.session.internal	/topic/com.cisco.ise.session.internal	1...	● C	2...	0...
ise-admin-ise	/topic/com.cisco.endpoint.asset,/topic/com.cisco...	/topic/com.cisco.ise.pxgrid.admin.log,/topic/com.cisco.ise.t...	1...	● C	2...	0...
ise-bridge-ise			1...	● C	2...	0...
ise-fanout-ise	/topic/distributed	/topic/distributed	1...	● C	2...	0...

The following image is for a distributed deployment of PAN, MNT, and 2 PSN/pxGrid Nodes on ISE 2.7:



Client Name	Connect To	Session Id	Certificate	Subscriptions	Publications	IP Address	Status	Start time	Duration
ise-mnt-ciscoisepmmt	ciscoisepmmt	ciscoisepmmt94552	No Certificate	/topic/com.cisco.ise.se...	/topic/com.cisco.ise.se...	192.168.0.136	ON	2021-04-06 05:40:17 IST	00:15:49:26
ise-fanout-ciscoisecpnt	ciscoisecpnt	ciscoisecpnt94442	CN=ciscoisec...	/topic/wirecard	/topic/com.cisco.ise.se...	127.0.0.1	ON	2021-04-05 06:00:03 IST	03:15:21:49
ise-fanout-ciscoisecpnt	ciscoisepmmt	ciscoisepmmt94538	CN=ciscoisec...	/topic/distributed	/topic/distributed	192.168.0.138	ON	2021-04-07 06:02:13 IST	01:15:27:38
ise-fanout-ciscoisepmmt	ciscoisepmmt	ciscoisepmmt94322	CN=ciscoisep...	/topic/wirecard	/topic/com.cisco.ise.se...	127.0.0.1	ON	2021-03-24 05:58:18 IST	15:15:31:25
ise-fanout-ciscoisepmmt	ciscoisepmmt	ciscoisepmmt94493	CN=ciscoisep...	/topic/distributed	/topic/distributed	192.168.0.138	ON	2021-04-05 17:40:51 IST	03:03:48:52
ise-bridge-ciscoisecpnt	ciscoisecpnt	ciscoisecpnt94445	CN=ciscoisec...			127.0.0.1	ON	2021-04-05 06:09:12 IST	03:15:20:31
ise-bridge-ciscoisepmmt	ciscoisepmmt	ciscoisepmmt94467	CN=ciscoisep...			127.0.0.1	ON	2021-04-02 05:57:55 IST	06:15:31:48
ise-admin-ciscoisecpnt	ciscoisecpnt	ciscoisecpnt94444	CN=ciscoisec...			192.168.0.139	ON	2021-04-05 06:09:02 IST	03:15:20:41
ise-admin-ciscoisepmmt	ciscoisepmmt	ciscoisepmmt94481	CN=ciscoisep...	/topic/com.cisco.eme...	/topic/com.cisco.ise.co...	192.168.0.138	ON	2021-04-04 06:04:46 IST	04:15:24:58
ise-admin-ciscoisepmmt	ciscoisecpnt	ciscoisecpnt94453	CN=ciscoisep...		/topic/com.cisco.ise.ist...	192.168.0.136	ON	2021-04-06 05:40:17 IST	00:15:49:27
QRadarApp_QATest_BNApp	ciscoisecpnt	ciscoisecpnt94452	CN=qradar124.a...	/topic/com.cisco.ise.se...		192.168.1.124	ON	2021-04-07 06:05:51 IST	01:15:23:52
QRadarApp_QATest_BNApp	ciscoisepmmt	ciscoisepmmt94553	CN=qradar124.a...	/topic/com.cisco.ise.se...		192.168.1.124	ON	2021-04-06 05:55:58 IST	00:15:33:45
QRadarAppST	ciscoisecpnt	ciscoisecpnt94451	CN=qradar124.a...	/topic/com.cisco.ise.se...		192.168.0.76	ON	2021-04-07 06:02:24 IST	01:15:27:19
QRadarAppST	ciscoisepmmt	ciscoisepmmt94554	CN=qradar124.a...	/topic/com.cisco.ise.se...		192.168.0.76	ON	2021-04-06 05:56:23 IST	00:15:33:21

The Cisco ISE pxGrid app pxGrid client subscribes to the Session Directory, RADIUS failure, MDM endpoint, and ANC configuration Topics.

The Session Directory topics consist of user contextual information, such as username, MAC address, IP Address, endpoint device, posture status and provides wired and wireless connection type information. Wired connection type information includes the NAS Port ID, NAS IP Address, NAS Port Type, Location, and Device Type attributes. Wireless connection type information includes WLAN, Calling Station ID, Called Station ID, NAS IP, Device Type, Location, and NAS Identifier attributes.

The MDM topic consists of compliance and registration status and is dependent on having an external MDM solution configured in Cisco ISE. In this document, the Cisco Meraki Solution was used as the external MDM solution. The testing was done with ISE 2.4 initial release so only the compliance and registration status attributes were available. In later releases of Cisco ISE after 2.4, the MDM attributes are available as follows: Manufacturer, UDID, Serial Number, Encryption Status, Jail Broken Status, Pin Lock Status.

The RADIUS failure topic includes failure reason attributes, such as "invalid password" and drill downs based on location and wired/wireless connection types.

The Config ANC Status Topic provides the Cisco ISE pxGrid client app to perform ISE Adaptive Network Control (ANC) mitigation actions on the endpoints.

The Cisco ISE pxGrid App uses pxGrid 2.0, which uses WebSocket, REST API, and STOMP messaging protocol for pxGrid operation and thus supported since Cisco ISE 2.4.

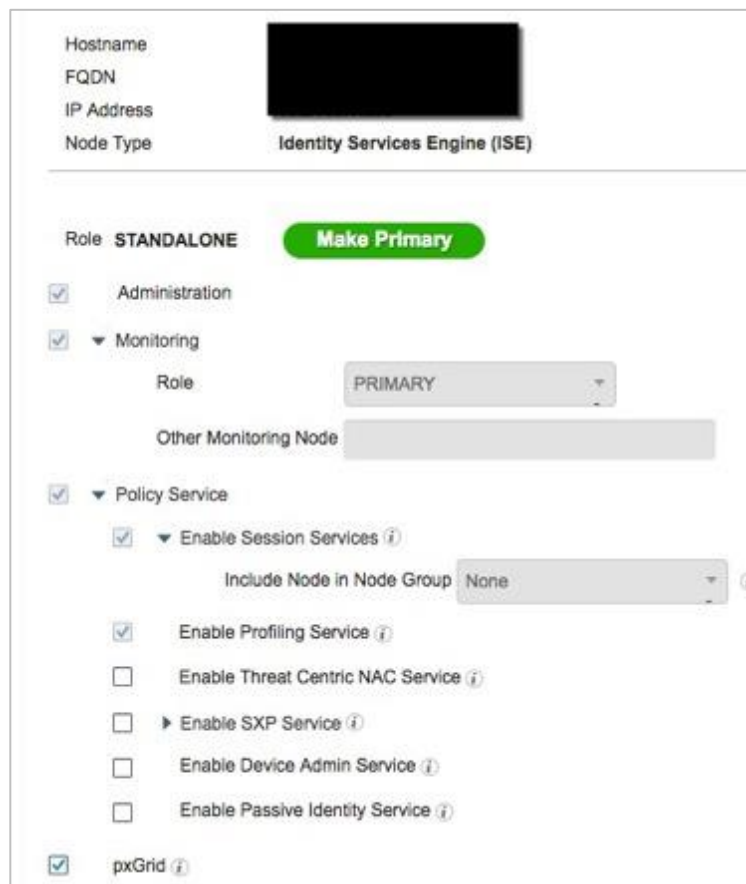
## Cisco ISE pxGrid Installation

Make sure that you have installed Cisco Identity Services (ISE) 2.4 or higher and it is in a standalone deployment (also supports other deployment methods). If this is a production ISE deployment, ensure the Cisco ISE pxGrid node is on a dedicated node. See the [pxGrid section](#) of ISE Guides for more information.

At minimum, it is recommended to have two standalone nodes for HA purposes. Both nodes would be running all personas, including pxGrid. Depending on the number of clients and architecture requirements, you may expand into other architecture designs. Please consult with your ISE integrator on recommended deployment model.

Step 1 Go to **Administration > System Deployment > Edit the ISE node > Enable pxGrid**.

This image is for ISE 2.7. For ISE 3.0, the image doesn't fit well on a screen. You would need to scroll down to the bottom and enable pxGrid.



Hostname [REDACTED]  
FQDN [REDACTED]  
IP Address [REDACTED]  
Node Type Identity Services Engine (ISE)

Role **STANDALONE** [Make Primary](#)

Administration

Monitoring

Role PRIMARY

Other Monitoring Node [REDACTED]

Policy Service

Enable Session Services ⓘ

Include Node in Node Group None ⓘ

Enable Profiling Service ⓘ

Enable Threat Centric NAC Service ⓘ

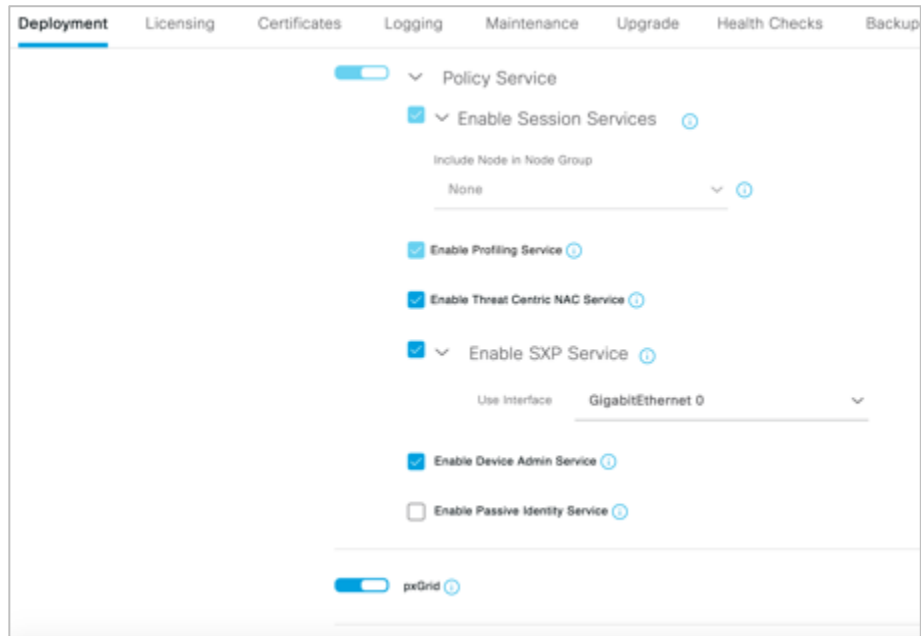
Enable SXP Service ⓘ

Enable Device Admin Service ⓘ

Enable Passive Identity Service ⓘ

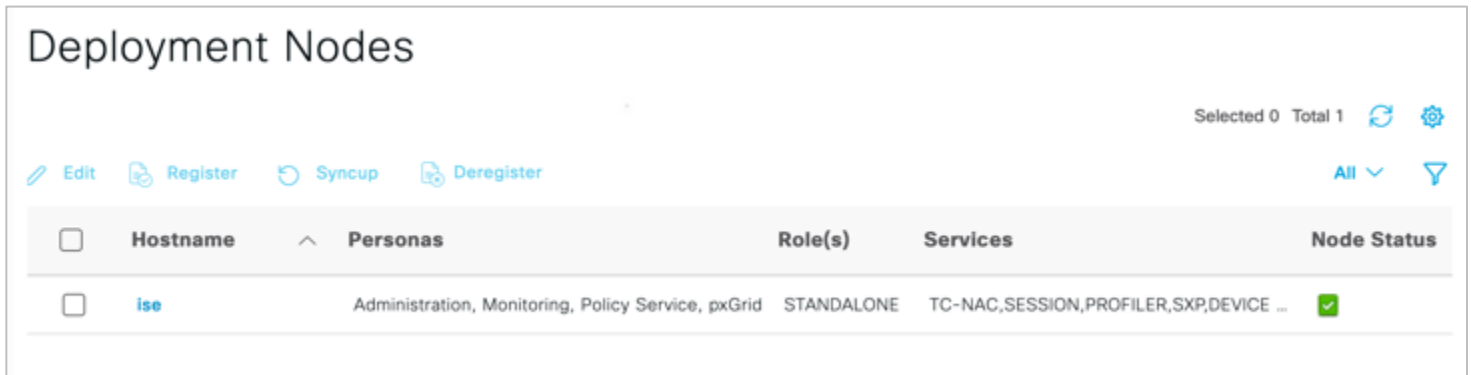
pxGrid ⓘ



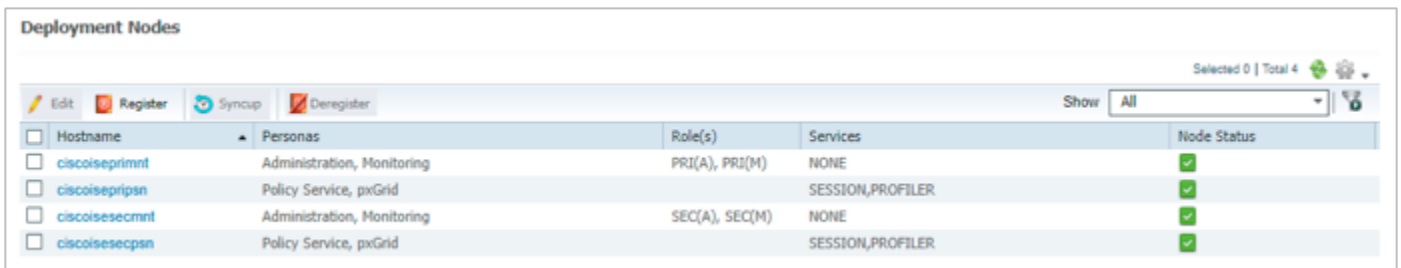


Step 2 Select **Save**.

You should see the following (ISE 3.0):



Recommended Distributed deployment example (ISE 2.4+):

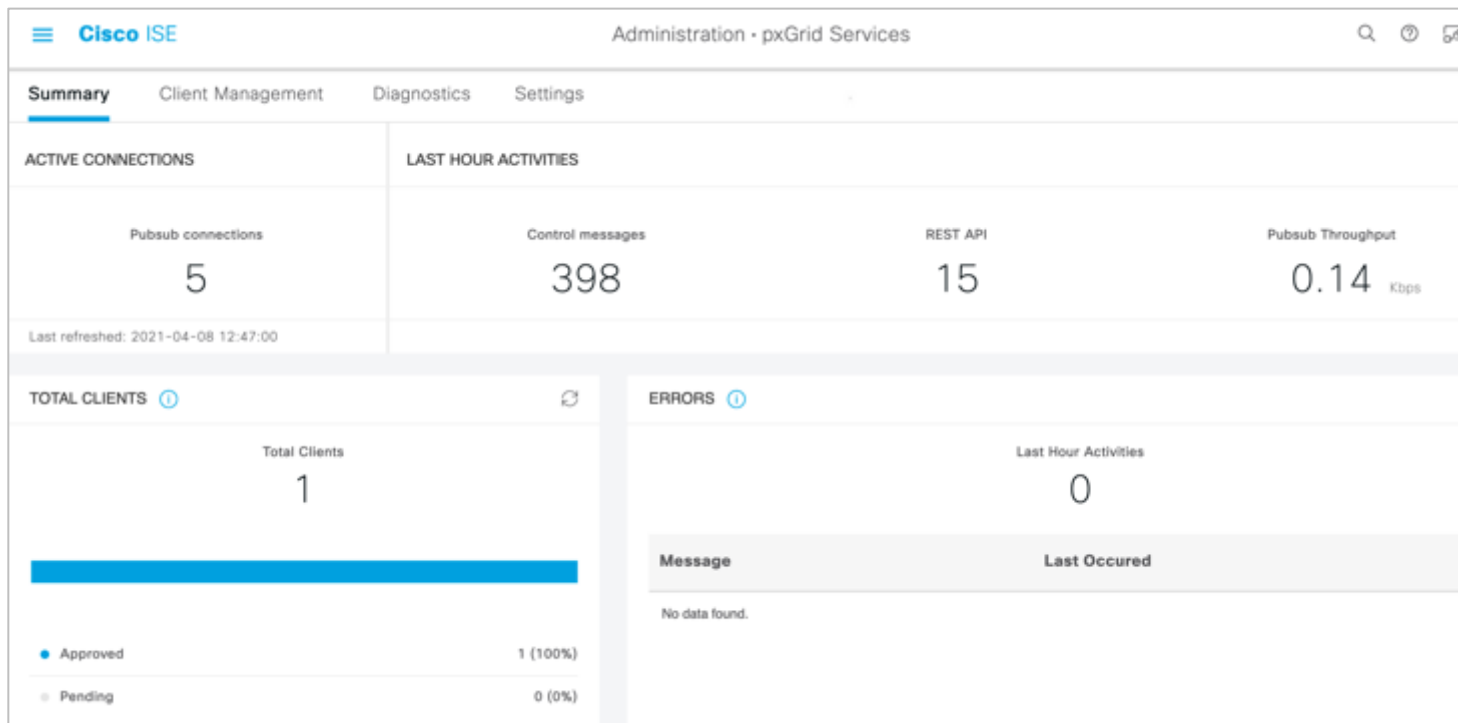


Step 3 Select **Administration > pxGrid Services > Summary**.

Verify that the published nodes appear. All nodes running pxGrid will have a fanout & pubsub.

Note: In ISE 3.0, you may see services not available. This is fixed in patch 3.

The screenshot below shows that 1 pxGrid client is connected (this is a current setup with another vendor that we are showcasing with 5 pubsub connections (internally and to 1 client)).



Step 4 Select **Web Clients (Diagnostics > WebSockets in ISE 3.x)** and verify that the published nodes appear:

Note: This is validating pxGrid 2.0 connections. You should see that admin, mnt, and pxGrid nodes have connections with each other. They should all be **ON**. This is from a 4-node deployment.

Identity Services Engine								
		Home	Context Visibility	Operations	Policy	Administration	Work Centers	
		System	Identity Management	Network Resources	Device Portal Management	pxGrid Services	Feed Service	Threat Centric NAC
Client Name							IP Address	
ise-mnt-ise	ise4	ise4.1	No Certificate	/topic/com.cisco.ise.s...	/topic/com.cisco.ise.s...		10.1.100.21	ON
ise-admin-ise	ise4	ise4.2	CN=ise.security...				10.1.100.21	ON
ise-admin-ise3	ise4	ise4.3	CN=ise3.securit...				10.1.100.23	ON
ise-admin-ise2	ise4	ise4.4	No Certificate				10.1.100.22	ON
ise-admin-ise4	ise4	ise4.6	CN=ise4.securit...				10.1.100.24	ON
ise-fanout-ise4	ise4	ise4.8	CN=ise4.securit...	/topic/wildcard	/topic/com.cisco.ise.s...		127.0.0.1	ON
ise-fanout-ise3	ise3	ise3.0	CN=ise3.securit...	/topic/wildcard	/topic/com.cisco.ise.s...		127.0.0.1	ON
ise-bridge-ise3	ise3	ise3.1	CN=ise3.securit...				127.0.0.1	ON
ise-fanout-ise3	ise3	ise3.2	CN=ise3.securit...	/topic/distributed	/topic/distributed		10.1.100.23	ON
ise-fanout-ise4	ise3	ise3.4	CN=ise4.securit...	/topic/distributed	/topic/distributed		10.1.100.24	ON
ise-mnt-ise2	ise3	ise3.5	No Certificate	/topic/com.cisco.ise.s...	/topic/com.cisco.ise.s...		10.1.100.22	ON

## Generating the Cisco ISE pxGrid App Certificate

A certificate for the Cisco ISE pxGrid App will be generated from the ISE internal CA so the App will register and connect to the ISE pxGrid node. If you are using an external CA server for pxGrid operation, please see [pxGrid section](#) of the ISE Guides.

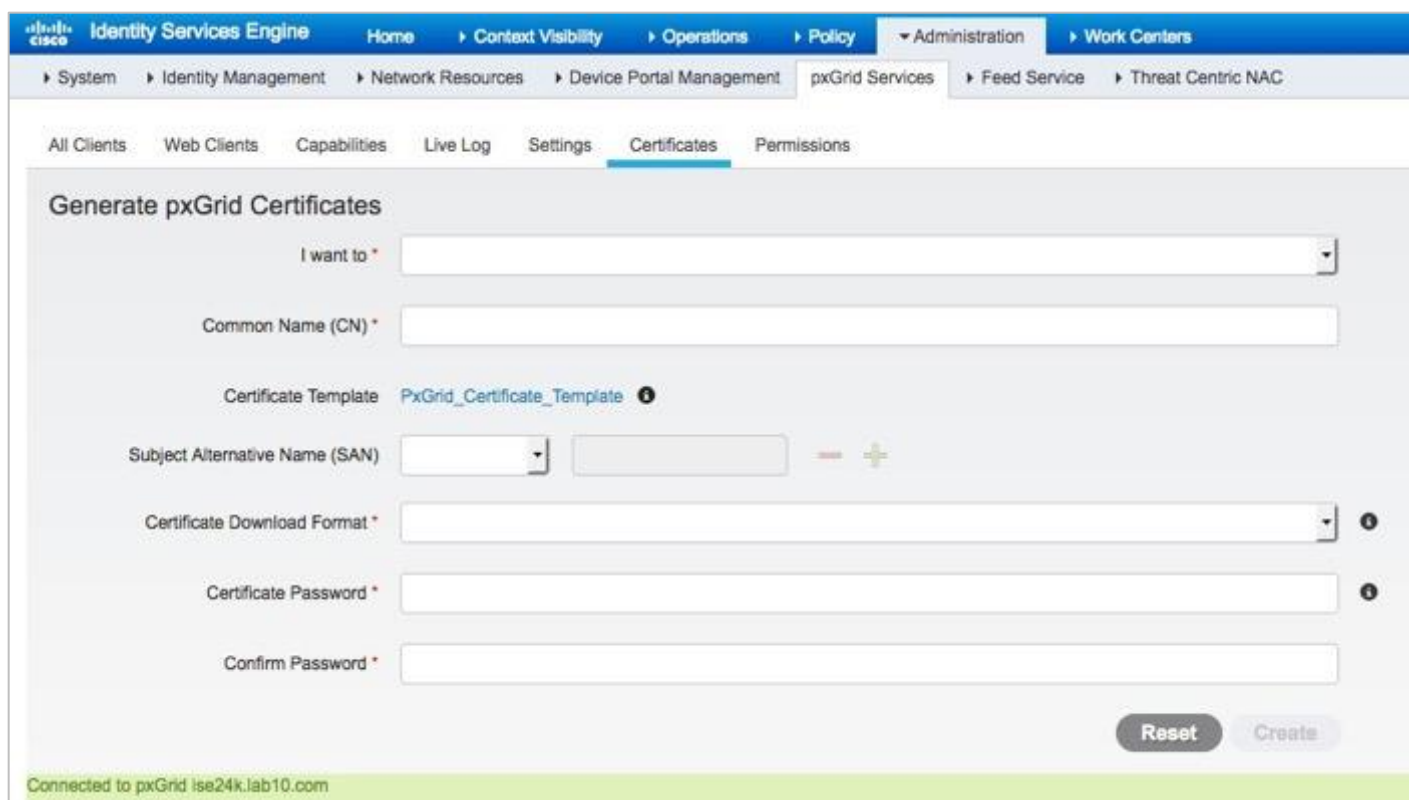
For more information on certificates, please refer to [this section](#) under [cs.co/ise-guides](#).

Note: When deploying certificates to your ISE nodes, make sure that the root that is installed on the pxGrid node is that of the certificate issued to your pxGrid nodes.

PKCS12 files are supported in version 3.0 of the QRadar App. Recommend using PEM with ISE internal CA unless there is some reason you must use PKCS12 (not discussed in this guide).

Step 1 Select **Administration > pxGrid Services > Certificates** (ISE 2.4+) or **Administration > pxGrid Services > Client Management > Certificates** (ISE 3.x).

You should see the following:



The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation path is: Administration > pxGrid Services > Certificates. The main heading is "Generate pxGrid Certificates". The form includes the following fields and controls:

- "I want to \*": A dropdown menu.
- "Common Name (CN) \*": A text input field.
- "Certificate Template": A dropdown menu with "PxGrid\_Certificate\_Template" selected.
- "Subject Alternative Name (SAN)": A dropdown menu, a text input field, and a "+" button.
- "Certificate Download Format \*": A dropdown menu.
- "Certificate Password \*": A text input field.
- "Confirm Password \*": A text input field.
- "Reset" and "Create" buttons at the bottom right.

At the bottom left, a status bar indicates "Connected to pxGrid ise24k.lab10.com".

Step 2 Type the following:

**It is recommended to use the full name of the server ex: qradar.securitydemo.net.**

Note: This is the IP address and FQDN of your QRadar system. You are generating a certificate here to install on QRadar app so it can present when communicating with ISE.

*I want to: Generate a single certificate (without a certificate signing request)*

*Common Name (FQDN): qradar.securitydemo.net*

*Description: QRadar*

*Certificate Template: Pxgrid\_Certificate\_Template*

*Subject Alternative Name (IP Address): 10.1.100.27*

*Subject Alternative Name (FQDN): qradar.securitydemo.net*

*Certificate Download Format: Certificate in Privacy Enhanced Mail (PEM) format, key in PKCS8 PEM format including certificate chain*

*Certificate Password: xxxxxxxx*

*Confirm Password: xxxxxx*

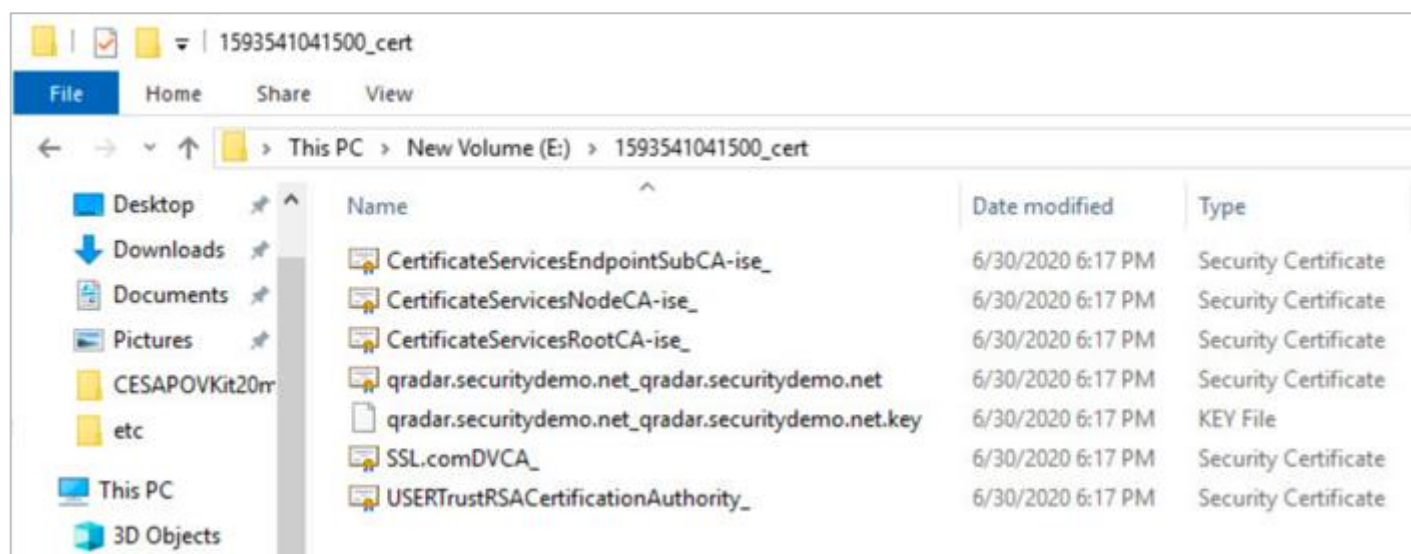
### Step 3 Select **Create**.

This will create a zipped file 1520701037382\_cert.zip.

Note: Make sure your browser pop-up blocker is disabled when generating certificates.

### Step 4 Unzip the file, you will see the following files:

Note: Keep the original zip, we are exporting here to just look at the contents and discuss the certificate. However, the QRadar App is able to import the zip package with its key as well.



The QRadar identity certificate consists of the public private key-pair:

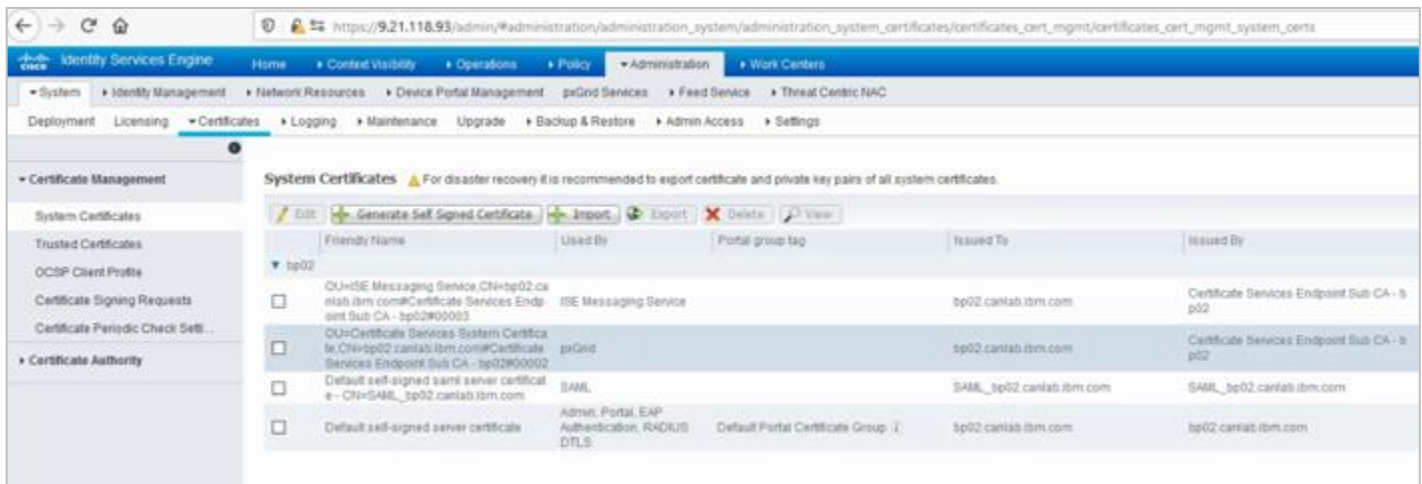
```
qradar.securitydemo.net_qradar.securitydemo.net.cer
qradar.securitydemo.net_qradar.securitydemo.net.key
```

The `CertificateServicesRootCA-ise_.cer` is the ISE internal Root CA certificate.

Depending on your setup, you may have certificates being used for different ISE personas in your environment. If pxGrid is not assigned to the local Certificate services endpoint, as seen below, then make sure that you export the root certificate chain that was used to sign it. For example, if you have ISE signed up an external identity source.

Don't assign pxGrid to the self-signed certificate of ISE. This is not the best practice. If it moves pxGrid back to the Certificate Services Endpoint Sub CA as you can see in the image below. If for some reason you need this, then you will need to manually export this certificate and upload as package with the internal CA generated cert and key to QRadar and choose that as the root. The relevant certificates from the internal CA won't matter even though they are in the package.

In the following example, the pxGrid certificate is signed by the same ISE internal CA. When ISE communicates to QRadar system, it will present this as part of the communication. When you generate the certificate on ISE in the above steps, it gives you a package that includes the certificate chain from ISE internal CA. When QRadar talks to ISE, its certificate is automatically accepted because ISE is aware of the certificates it issues and the associated certificate chain.



## Installing Cisco ISE pxGrid App

In this section, you will learn how to install the Cisco ISE pxGrid App.

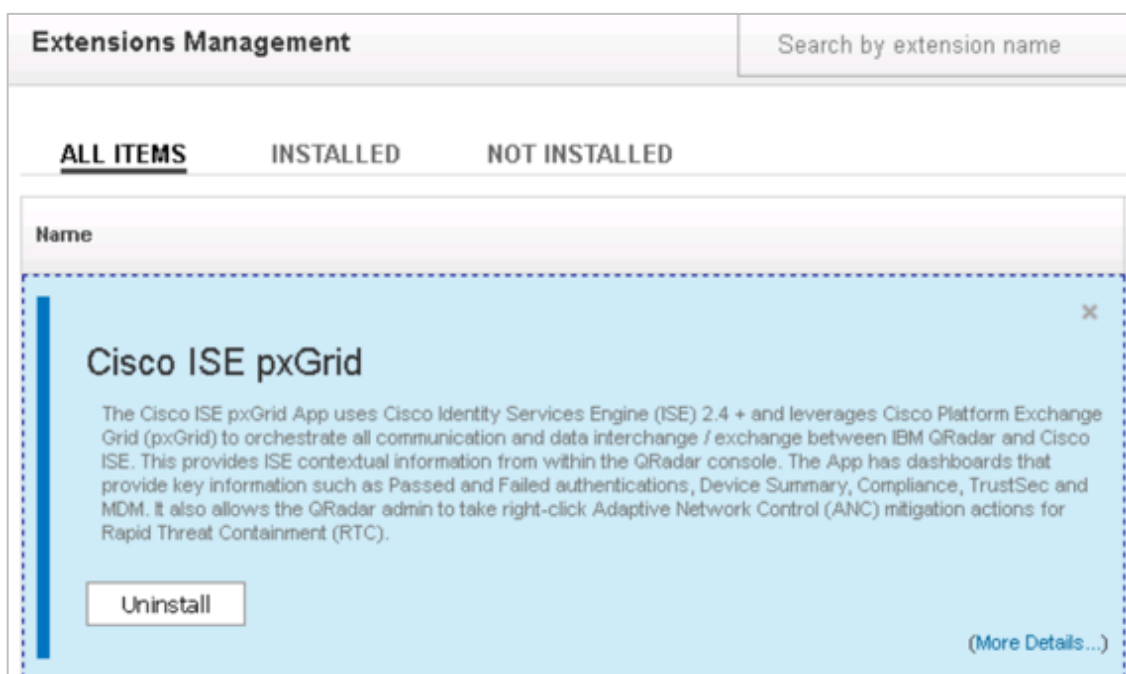
To download the app, please visit the [IBM App Exchange](#).

Note: It is assumed that you're running recommended release of IBM QRadar (see notes at the beginning of this document).

If user is upgrading the Cisco ISE pxGrid QRadar App, we recommend users to uninstall the old app and install the latest version.

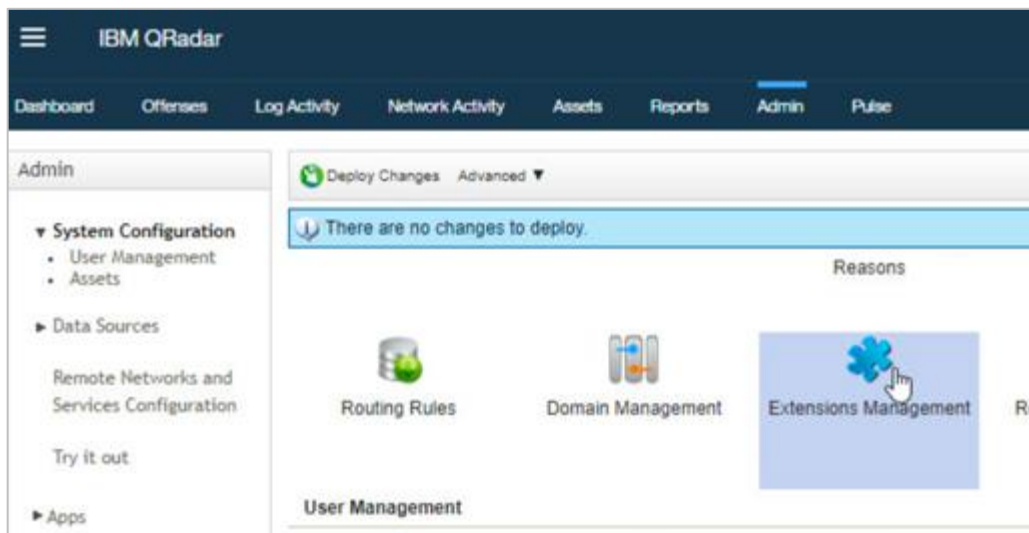
To uninstall the old app:

1. Go to **Admin > System Config > Extensions Mgmt.**
2. Select **Cisco ISE pxGrid**, and then click **Uninstall**.

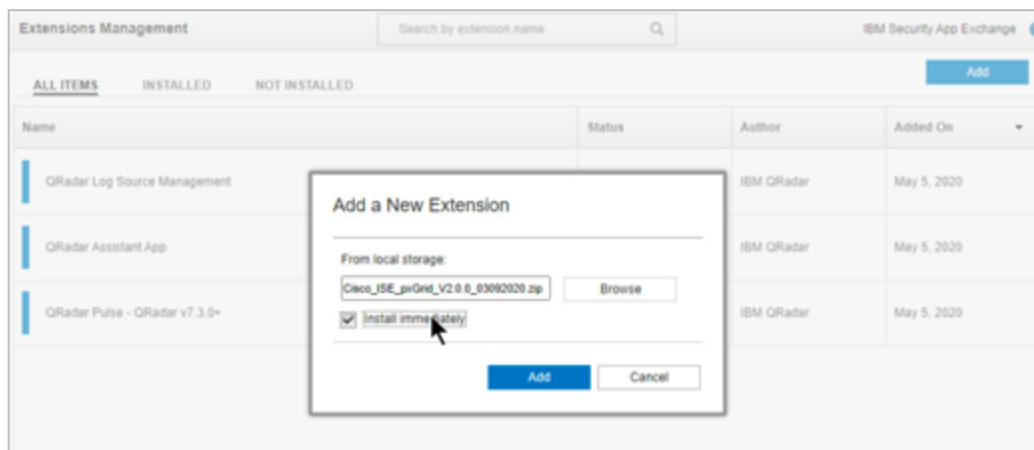


Step 1 Install the extension:

- a. In IBM QRadar, select **Admin > Extensions Management**.

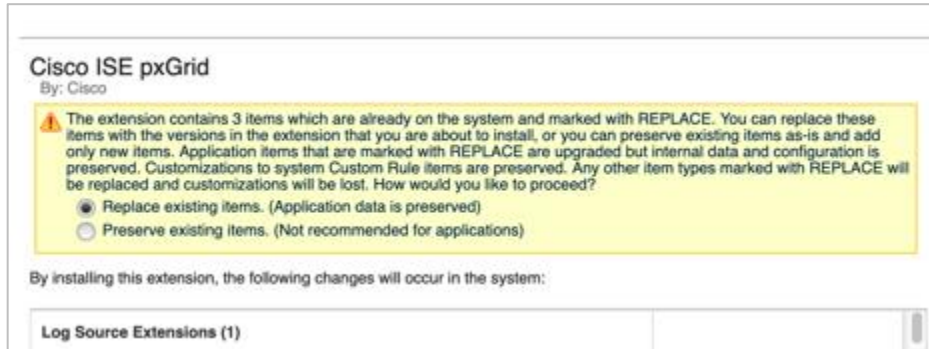


- b. Click **Add a New Extension**, upload the signed Cisco ISE pxGrid App, and select the **Install Immediately** checkbox.





Note: If asked the following, select the Replace option to install new components, and click Install at the very bottom.

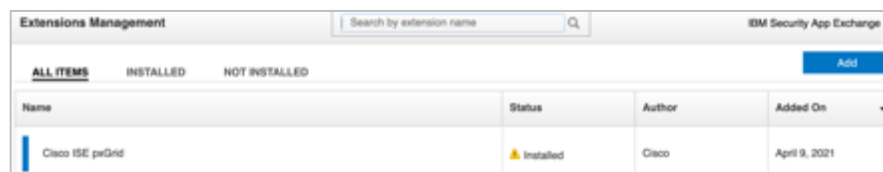


Next you may see this: Click OK.



c. After installation, you should see the following:

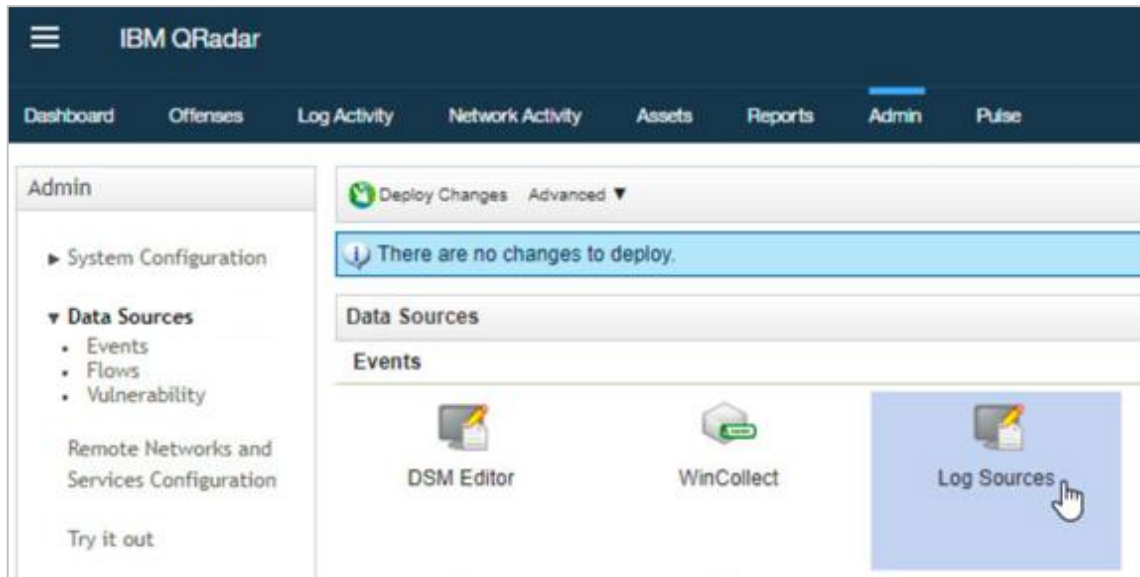
Note: This is showing an exclamation mark as we were testing with an unsigned copy before posting to IBM app exchange.



d. Clear the browser cache, close the browser, launch the app, and login again.

Step 2 Configure the logging IP address for the primary/secondary nodes:

- a. On QRadar, in the upper-left corner, click the **hamburger**.
- b. Navigate to **Admin > Data Sources > Events > Log Sources**.



c. Change your log source identifiers QRadar 7.3 (see 7.4 below this section).

Choose **Name** > **pxGrid\_Primary/pxGrid\_Secondary**.

Edit and change the **Log Source Identifier** to corresponding ISE IP for Primary and Secondary accordingly.

You may disable the secondary if you don't need it.

Log Sources - Google Chrome

192.168.1.233/console/do/sem/maintainSensorDevice

Search For: Group All Log Source Groups Go Add Edit Enable/Disable Delete Bulk Actions

Name	Desc	Status	Protocol	G...	Log Source Type	Enabled	Log Source Identifier	Target Destination	Credibi	Autodiscov
pxGrid_Primary	Cisco ISE ...	Success	Syslog		Cisco ISE pxGrid	True	primary	eventcolle...	5	False
pxGrid_Secondary	Cisco ISE ...	Success	Syslog		Cisco ISE pxGrid	True	secondary	eventcolle...	5	False

Note: You will see Status as Error since there are no logs coming in because we are still working on the system configuration.

Search For: Name pxGrid Go Add Edit Enable/Disable Delete Bulk Actions Extensions Parsing Order Assign

Name ▲	Desc	Status	Protocol	Group	Log Source Type	Enabled	Log Source Identifier	Target Destination
pxGrid	Cisco ISE pxGrid Log Source for pri...	Error	Syslog		Cisco IS...	True	primary	eventcoll...
pxGrid	Cisco ISE pxGrid Log Source for se...	Error	Syslog		Cisco IS...	True	secondary	eventcoll...

Note: If you double-click one of the items, you will see the error details.

### Edit a log source

**Note** that the connection information for this log source is shared amongst one or more other log sources.

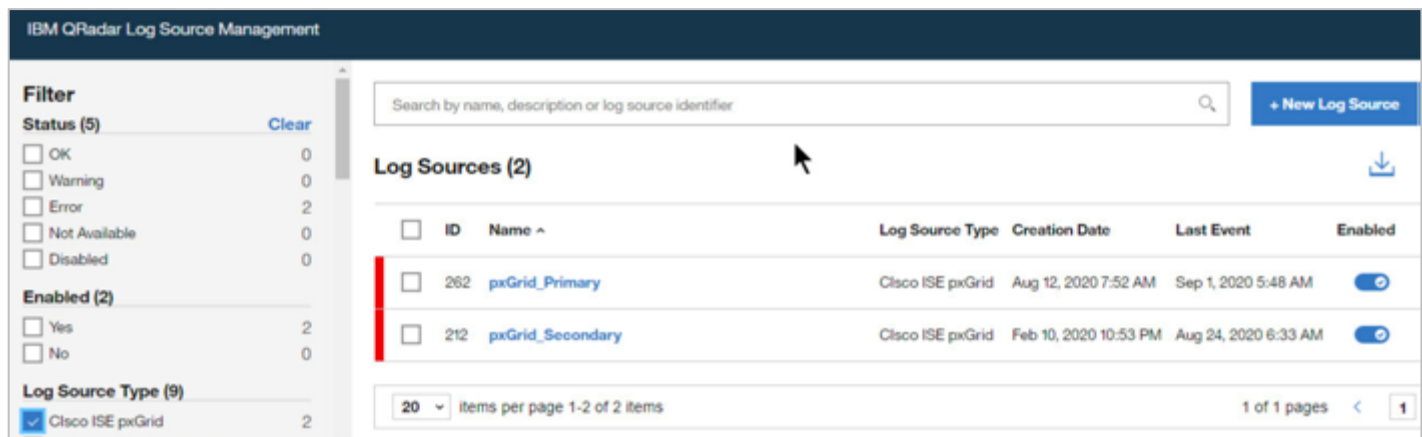
**ERROR** - Events have not been received from this Log Source in over 720 minutes.

**Log Source Name**

**Log Source Description**

d. Change your log source identifiers for **QRadar 7.4**.

- The app opens in a new window.
- Choose Log source type to filter on pxGrid.



IBM QRadar Log Source Management

Search by name, description or log source identifier

+ New Log Source

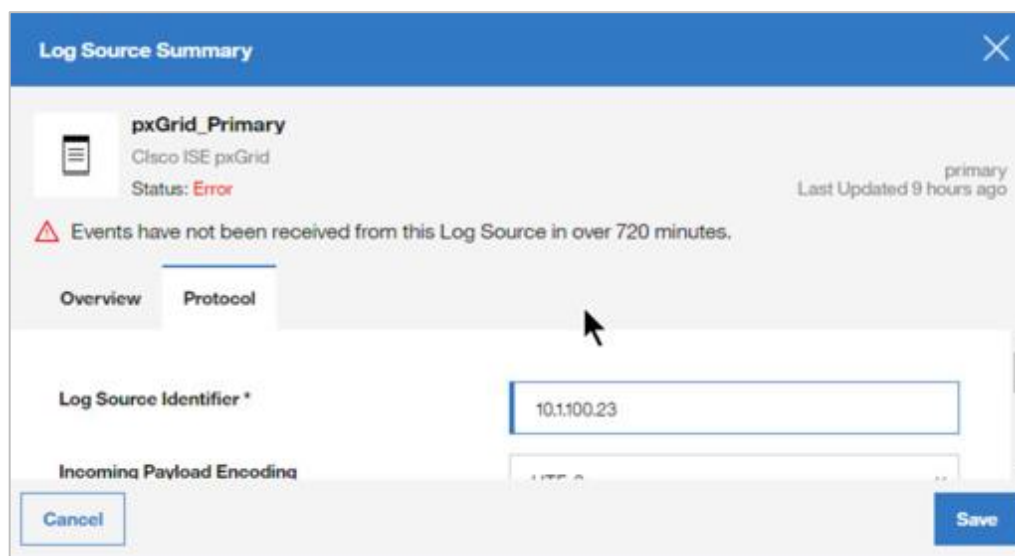
**Log Sources (2)**

ID	Name	Log Source Type	Creation Date	Last Event	Enabled
262	pxGrid_Primary	Cisco ISE pxGrid	Aug 12, 2020 7:52 AM	Sep 1, 2020 5:48 AM	<input checked="" type="checkbox"/>
212	pxGrid_Secondary	Cisco ISE pxGrid	Feb 10, 2020 10:53 PM	Aug 24, 2020 6:33 AM	<input checked="" type="checkbox"/>

20 items per page 1-2 of 2 items 1 of 1 pages

- Change the primary and secondary log source identifier.
- Click on the **primary**, edit, and then choose protocol. Change **Primary** to actual ISE pxGrid node IP, and then click **Save**.

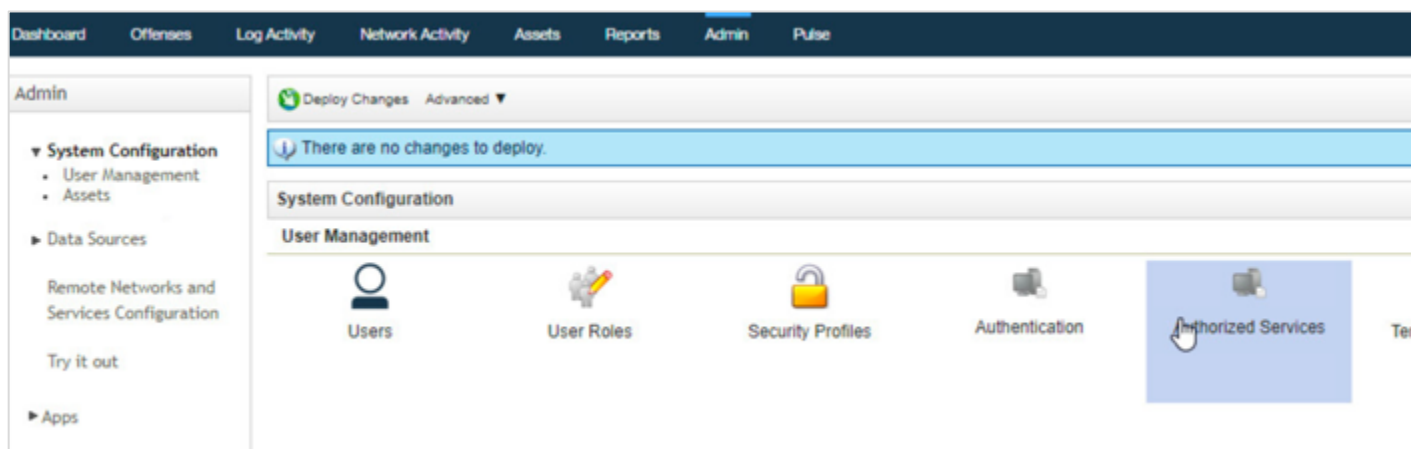
Note: Do the same for the secondary. If one is not used, then disable the toggle slider as in the image above.



- Close the edit window, and then the second browser tab.

Step 3 Configure the **Authorized Services** in QRadar:

- a. Select **Admin > System Configuration > User Mgmt > Authorized Services**.



b. Add Authorized Service:

- In the **Service name** box, enter **pxGridService**.
- In the **User Role** and **Security Profile** dropdown lists, select **Admin** (default).
- Select the **No Expiry** checkbox.

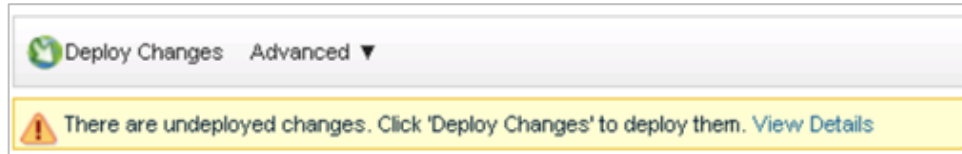
Service Name:	pxGridService
User Role:	Admin
Security Profile:	Admin
Expiry Date:	2/13/2018 / <input checked="" type="checkbox"/> No Expiry

- c. Click **Create Service**.
- d. Copy the authentication token into the notepad.

<input type="checkbox"/> Add Authorized Service		<input checked="" type="checkbox"/> Delete Authorized Service	<input type="checkbox"/> Edit Authorized Service Name	Selected Token: <a href="#">c8342c8c-fb96-48bd-ab93-912754c56872</a>		
Service Name	Authorized By	Authentication Token	User Role	Security Profile	Created	Expires
pxGridService	admin	c8342c8c-fb96-48bd-a...	Admin	Admin	Apr 9, 2021, 8:09:27 PM	Permanent

Note: This is later used for Cisco ISE pxGrid App for pxGrid integration.

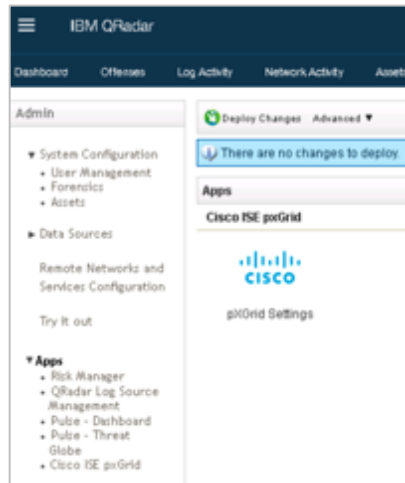
- e. Close the Authorized Service browser window.
- f. Make sure to **deploy changes** at this point.



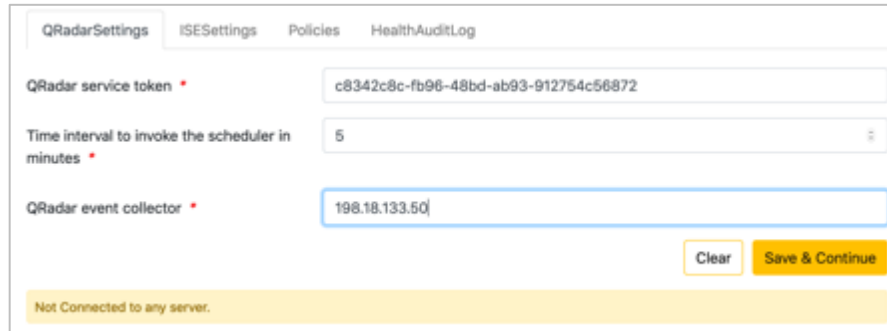
## Configuring pxGrid Integration on QRadar

Step 1 Setup pxGrid settings:

- a. Select **Admin > Apps > Cisco ISE pxGrid > pxGrid Settings**.



- b. **Copy** and paste the authentication token into the **QRadar Service Token Window**.



Note: When going through the setup, you will notice the following message at the bottom of the app. This is due to the config not being completed. You won't see it change to green until all configuration is completed and polling is done via HealthAuditLog.

Note: If you continue to see this after putting all the settings in and ISE shows Enabled then clear your browser cache to refresh.

**Problem in connecting the ISE servers - ISE Settings are missing in the app.**

Step 2 Enter the QRadar Event collector (EC) IP / QRadar Console IP (If EC is not available).

Step 3 Select **Save & Continue**, this will move you to the **ISESettings** tab.

Step 4 Select **Primary and** type the **IP address** of the ISE pxGrid node.

Step 5 Leave **8910** as the default port.

Step 6 Enter the Client username (for example, QRadar App).

Note: This will be the unique registered pxGrid client name displayed on ISE.

Step 7 Select the certificate format type. You can choose between PEM or Pkcs12(.p12).

Step 8 You may upload the zip package you generated from ISE certificate services (ISE internal CA); otherwise, if you're using your own internal PKI, you can upload all (selecting all in the browse windows at once) the Cisco ISE pxGrid App certificates in the PEM format under **Select and Upload Certificates (only PEM is supported)** application settings page.

```
CertificaeServicesEndpointSubCA-ise24k_.cer  
CertificateServicesNodeCA-is24k_.cer  
CertificateServicesRootCA-ise24k_.cer  
ise24k.lab10.com.cer  
qradar.lab10.com_qradar.lab10.com.cer  
qradar.lab10.com_qradar.lab10.com.key
```

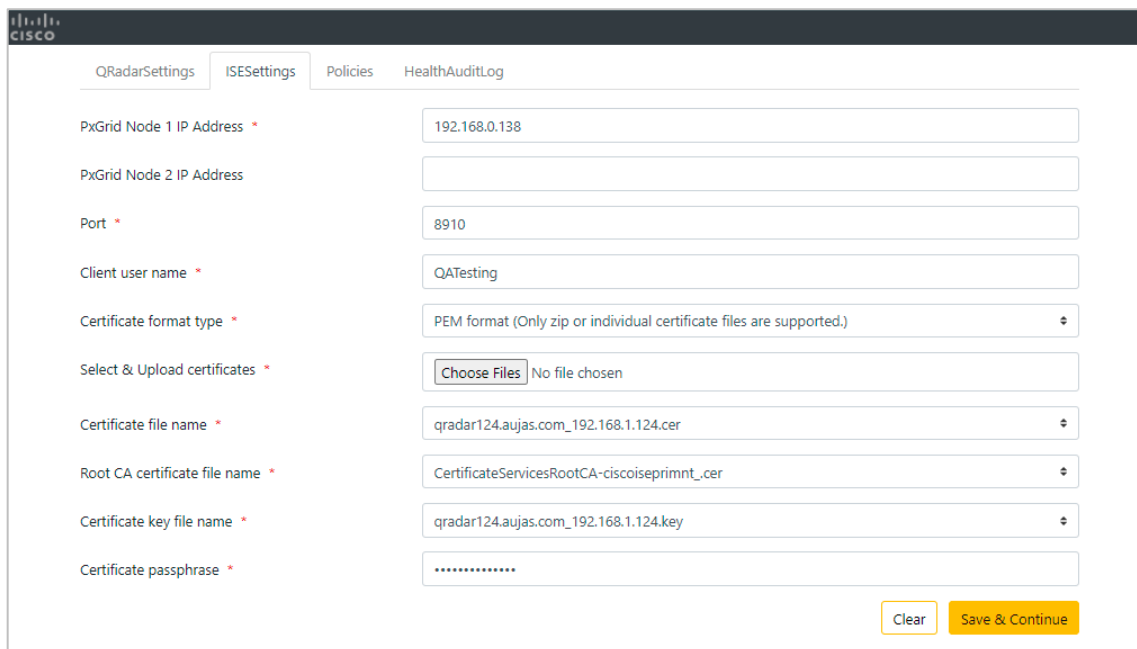
Step 9 Choose the Cisco ISE pxGrid App Certificate file name:  
**qradar.lab10.com\_qradar.lab10.com.cer.**

Step 10 Choose the Cisco ISE pxGrid App Certificate key file name:  
**qradar.lab10.com\_qradar.lab10.com.key.**

Step 11 Choose the Cisco ISE Internal Root Certificate Root CA certificate file name:  
**qradar.lab10.com\_qradar.lab10.com.cer.**

**Step 12 Enter the certificate pass phrase.**

You will see the following if PEM format is selected:



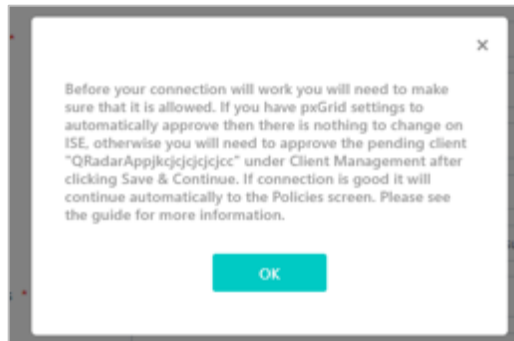
When working with certificates, you must understand where the certificate was issued for your pxGrid nodes. Here are some criteria:

- On any ISE deployment, you could have multiple certificates for different roles personas.
- The admin node with an internal PKI certificate so that your admin machines with the root trust them.
- Portals for guest services would likely have a well-known certificate so that any client coming in off the street can trust the portal.
- Your pxGrid node will likely be side either by ISE internal CA or a well-known certificate root, depending on how you certificate trust is set up. Carefully choose your Root in the setup settings.
- All nodes running pxGrid should have the same root.
- See more about certificates at [ISE Guides page for certificates](#) and [ISE 2.7 Certificate Section of Admin Guide](#).

**Note:** If adding a secondary pxGrid node, provide the secondary pxGrid Server IP Address, the Client username and identity certificate, and public private key-pair. The root certificate will remain the same as in Primary.



Step 13 At the bottom of the page, select **Save and Continue**.

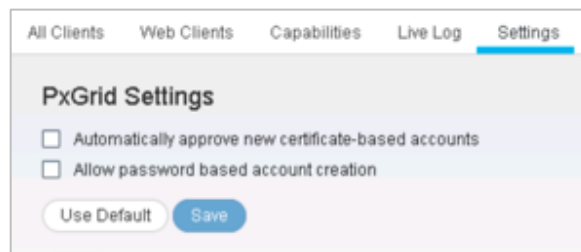
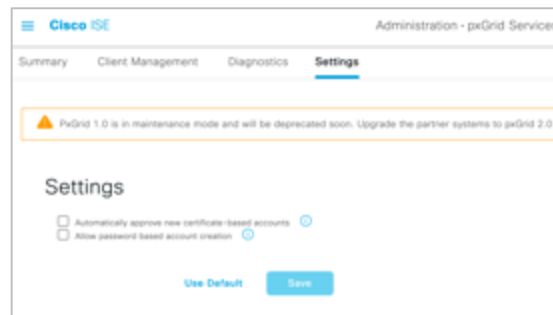


You will be provided with a message to approve client connection. You can ignore if auto approve is enabled. Steps to approve client connection in provided below.

Note: At this point you will see a screen to show pxGrid policies. It will be empty since ISE comes out of box not accepting new account creations. For security, unless you're adding a bunch of clients or testing, you should probably leave these unchecked.

**Administration > pxGrid Services > Settings (ISE 3.x)**

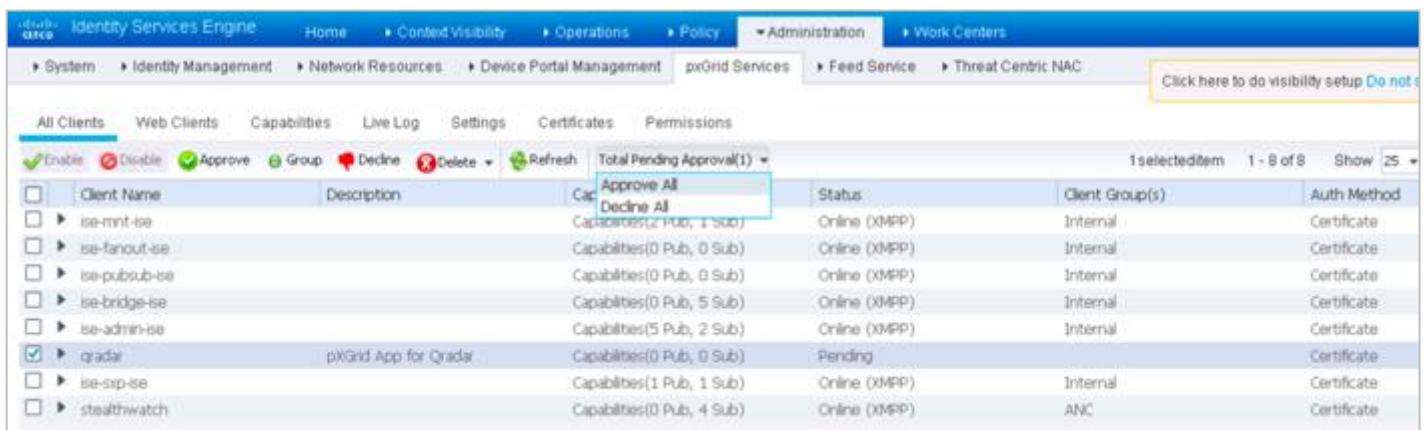
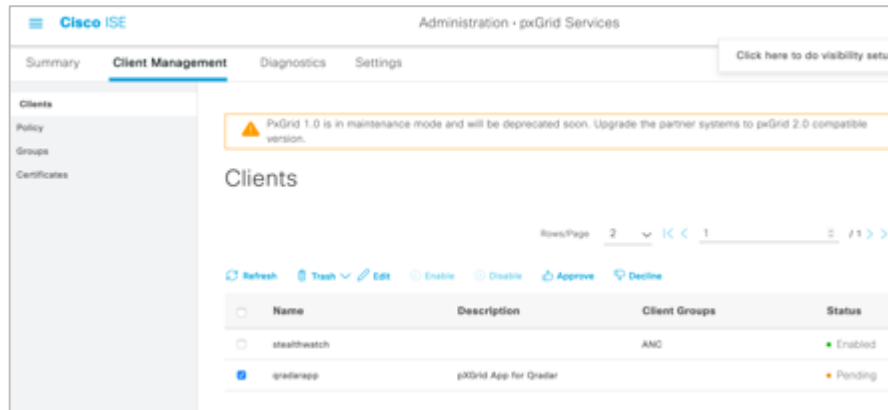
**Administration > pxGrid > Settings (ISE 2.4+)**



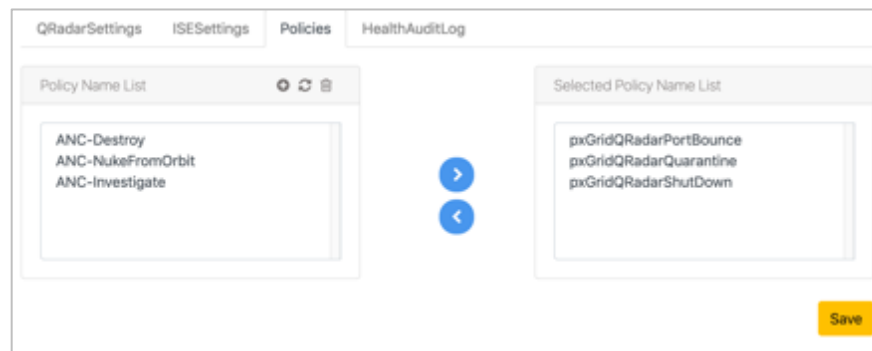
Step 14 Let's allow the connection manually:

**Admin > pxGrid Services > Client Management (ISE 3.x)**, and click to **Approve** the qradarapp.

**Admin > pxGrid Services > All Clients (ISE 2.4+)**, click **Approve all**.



Step 15 Navigate back to the QRadar ISE pxGrid app ui and refresh the policy list UI. Either create or select the policies you want to use in your environment. Click **Save**.



Step 16 Validate the HealthAuditLog in the app. Notice it shows enabled as the last status. This may take a bit to update the polling. Perhaps 1-2 min. There is Refresh and Poll now.

On clicking the **refresh** button, the latest status of the node will be read from the **internal App Db** and updated on the table, by default the page refreshed every 5 min.

The **Poll now** button will send a request to the nodes to poll the status of the node.

**You may now close the app window.**

ISE Node	Response Time	Last Health Check Time	HTTP Status Code	Status
Node1	0.0325427981872586	2021-05-17 23:40:34.539936	200	ENABLED
Node1	0.030228853229708008	2021-05-17 23:40:26.374261	200	ENABLED
Node1	0.030719757060078125	2021-05-17 23:39:34.556419	200	ENABLED
Node1	0.0312821849508179371	2021-05-17 23:39:34.518222	200	ENABLED
Node1	0.03184247018906738	2021-05-17 23:29:34.558597	200	ENABLED
Node1	0.031603396394228516	2021-05-17 23:20:34.558713	200	ENABLED
Node1	0.0349047998046875	2021-05-17 23:19:34.421255	200	ENABLED
Node1	0.03082968162536621	2021-05-17 23:10:34.397989	200	ENABLED
Node1	0.0304415225962666	2021-05-17 23:09:34.397063	200	ENABLED
Node1	0.2781148406431255	2021-05-17 23:00:34.643534	200	ENABLED

Step 17 Validate the pxGrid client on ISE:

Note: In ISE 2.4+ On the All Clients tab, the Client Status can be Offline (XMPP). This is for pxGrid 1.0 and doesn't represent any value. ISE 3.0 shows XMPP and WebSockets screens.

Step 18 Admin > pxGrid Services > Web Clients (2.4+).

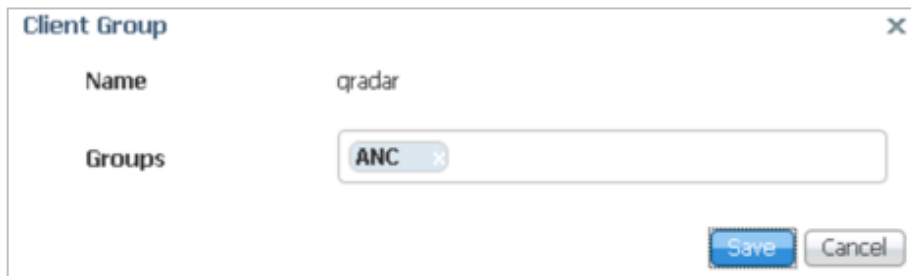
Admin > pxGrid Services > Diagnostics > WebSocket (3.0) and see registered Cisco ISE pxGrid QRadar app client.

Note: If you do not see the pxGrid registered client, ensure the ISE pxGrid QRadar app client is using Fully Qualified Domain Name (FQDN).

Client Name	Connect To	Session Id	Certificate	Subscriptions	Publications	IP Address	Status
QRadar	ise	ise:16	CN=qradar	/topic/com.cisco.ise.session,/topic/com.cisco.ise.radius.failure,/topic/...		198.19.10.18	OFF
QRadar	ise	ise:17	CN=qradar	/topic/com.cisco		198.19.10.18	ON

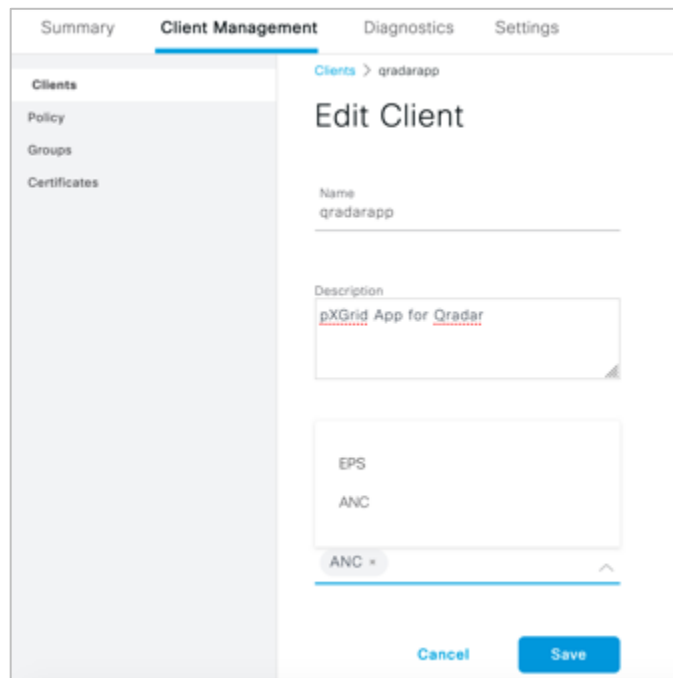
Step 19 You will see the client connected twice if there are two pxGrid (primary/secondary) nodes. Only one entry for single pxGrid nodes. Assign the QRadar client to the ANC Group permissions:

- Select **All Clients** (Admin > pxGrid Services > Client Management > Clients (ISE 3.x) > **Check the QRadar Client**.
- Go to Group > **Add** > **ANC**.
- Click **Save**.



A dialog box titled "Client Group" with a close button (X) in the top right corner. It contains two fields: "Name" with the value "qradar" and "Groups" with a dropdown menu showing "ANC" and a close button (X). At the bottom right, there are "Save" and "Cancel" buttons.

Note: You should see the pxGrid client Group ANC assigned to the Cisco ISE pxGrid client, the below image is of ISE 3.x (above is 2.x).



A screenshot of the Cisco ISE 3.x web interface. The "Client Management" tab is active, and the "Edit Client" page is displayed for the client "qradarapp". The page shows the following fields:

- Name: qradarapp
- Description: pxGrid App for Qradar
- Groups: ANC

At the bottom, there are "Cancel" and "Save" buttons.

## Setup Indexing in QRadar

Following are the steps to Index CEPs in QRadar.

Step 1 **Return to the IBM QRadar Web Console.**

Step 2 **Navigate to Admin tab, and then click Index Management.**



Step 3 **To setup the Indexes for use with pxGRid:**

- a. Search for **pxgrid** indexes: in the upper-left corner, enter pxgrid into the search window, and then search.



- b. Sort by Property:

Indexed	Property
	pxGrid_accessService (custom)
	pxGrid_adHostDomainName (custom)
	pxGrid_adHostNetBiosName (custom)
	pxGrid_adHostResolvedDns (custom)
	pxGrid_adHostResolvedIdentities (custom)
	pxGrid_adNormalizedUser (custom)
	pxGrid_adUserDomainName (custom)

- c. To Index the CEPs Packaged with the app, **right-click** on the property name, and then **Enable Index**.

Recommended CEPs to be indexed are the following:

- pxGrid\_adNormalizedUser

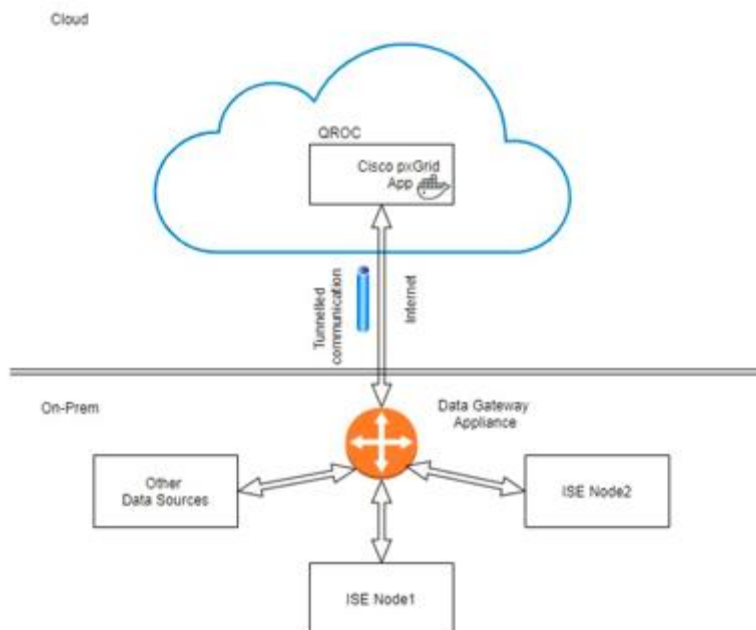
- pxGrid\_auditSessionId
- pxGrid\_EventName
- pxGrid\_macAddress
- pxGrid\_nasPortType
- pxGrid\_src

d. Click **Save**.

## App installation on QROC

Cisco pxGrid QRadar App is certified 'QRadar on cloud ready' by IBM.

The following image shows data sources on your network that send information to your gateway appliance. The gateway appliance then communicates with an instance of QRadar that is running in the IBM cloud.



The pxGrid QRadar App installation on QROC is very similar to the QRadar enterprise .

NOTE: Use the QRadar® on Cloud [Self Serve app](#) to perform administrative tasks that are related to the provisioning and configuration of your QRadar on Cloud instance. The Self Serve app is installed on all QRadar on Cloud Consoles by default.

Log on to the QRadar console(QROC) from a web browser to install and access Cisco ISE pxGrid QRadar App, just as you would with QRadar deployed on your premises.

Step 1: Follow all the steps under the section "[Generating the Cisco ISE pxGrid App Certificate](#)" to download the certificates but ensure to use the Data Gateway IP and FQDN instead of QRadar console details.

Step 2: Follow all the steps under the section "[Installing Cisco ISE pxGrid App](#)" to install the app on QROC.

A QRadar cloud user should ensure, that both the ISE Nodes IPs should be whitelisted on data gateway. This can be directly done in QROC UI with the help of “Self-serve app” provided by default in QROC.

### **Allowlisting an IP address**

Performing the below steps should whitelist ISE server and allow communication between ISE Server and QROC.

Users can allowlist an IP address by adding the classless inter-domain routing (CIDR) value to the Allowlist Management page. Here user should allowlist the ISE IP here.

1. Open the Admin settings and click QRadar on Cloud Self Serve.
2. Click Allowlist Management.
3. Click Add.
4. Enter the CIDR.
5. Click Save.
6. Click Submit, and then click Confirm

Refer [here](#) for more details.

If the communication is still not ON, whitelist 8910 (pxGrid Service) port as well.



## Cisco ISE pxGrid App Dashboard Panels

The dashboards and panels are populated with contextual information from ISE via pxGrid. This contextual information includes:

- Security or network admin visibility into who is connecting to the network and how they are connecting
- Type of devices connecting to the network, how they are connecting, and the owners of these devices
- Users' compliance with the organization's security policy
- Data on the incorporation of Bring Your Own Device (BYOD) security policies within the organization and whether they include external Mobile Device Management (MDM) vendors

The dashboards and panels are designed or provide investigative insight across the entire organization or by connection-type such as wired or wireless. These dashboards include: Passed Authentications, Failed Authentications, Devices, Compliance, MDM, TrustSec, and Currently Assigned ANC policies.

The admin can also take ISE ANC mitigative actions on the endpoint through these all QRadar ISE pxGrid App dashboards, except for TrustSec and Currently Assigned ANC Dashboards under ANC Details.

Tab Name			Description	Search Criteria
Passed Authentications	User	All	Top ten users with passed auth	<ul style="list-style-type: none"> <li>▪ Select by pxGrid_adNormalizedUser</li> <li>▪ pxGrid_EventName as User Sessions</li> </ul>
		Wired	Top ten Wired users with passed auth	<ul style="list-style-type: none"> <li>▪ Select by pxGrid_adNormalizedUser</li> <li>▪ pxGrid_EventName as User Sessions</li> <li>▪ pxGrid_nasPortType as Ethernet</li> </ul>
		Wireless	Top ten Wireless users with passed auth	<ul style="list-style-type: none"> <li>▪ Select by pxGrid_adNormalizedUser</li> <li>▪ pxGrid_EventName as User Sessions</li> <li>▪ pxGrid_nasPortType as Wireless</li> </ul>

Tab Name		Description	Search Criteria
	VPN	Top ten VPN users with passed auth	<ul style="list-style-type: none"> <li>▪ Select by pxGrid_adNormalizedUser</li> <li>▪ pxGrid_EventName as User Sessions</li> <li>▪ pxGrid_nasPortType as Virtual</li> </ul>
	WebAuth	Top ten WebAuth (MAB+Guest) users with passed auth	<ul style="list-style-type: none"> <li>▪ Select by pxGrid_username</li> <li>▪ pxGrid_EventName as User Sessions</li> <li>▪ pxGrid_radiusFlowType as wiredMAB or wirelessMAB</li> <li>▪ pxGrid_username as a valid name, not MAC ID</li> </ul>
Device	All	Top ten endPointProfile	<ul style="list-style-type: none"> <li>▪ Select by pxGrid_endPointProfile</li> <li>▪ pxGrid_EventName as User Sessions</li> </ul>
	Wired	Top ten Wired endPointProfile	<ul style="list-style-type: none"> <li>▪ Select by pxGrid_endPointProfile</li> <li>▪ pxGrid_EventName as User Sessions</li> <li>▪ pxGrid_nasPortType as Ethernet</li> </ul>
	Wired Dot1x	Top ten Wired Dot1x endPointProfile	<ul style="list-style-type: none"> <li>▪ Select by pxGrid_endPointProfile</li> <li>▪ pxGrid_EventName as User Sessions</li> <li>▪ pxGrid_nasPortType as Ethernet</li> <li>▪ pxGrid_serviceType as Framed</li> </ul>
	Wired MAB	Top ten Wired MAB endPointProfile	<ul style="list-style-type: none"> <li>▪ Select by pxGrid_endPointProfile</li> <li>▪ pxGrid_EventName as User Sessions</li> <li>▪ pxGrid_nasPortType as Ethernet</li> <li>▪ pxGrid_serviceType as Call Check</li> </ul>
	Wireless	Top ten Wireless endPointProfile	<ul style="list-style-type: none"> <li>▪ Select by pxGrid_endPointProfile</li> <li>▪ pxGrid_EventName as User Sessions</li> <li>▪ pxGrid_nasPortType as Wireless</li> </ul>
	Wireless Dot1x	Top ten Wireless Dot1x endPointProfile	<ul style="list-style-type: none"> <li>▪ Select by pxGrid_endPointProfile</li> <li>▪ pxGrid_EventName as User Sessions</li> <li>▪ pxGrid_nasPortType as Wireless</li> <li>▪ pxGrid_serviceType as Framed</li> </ul>

Tab Name		Description	Search Criteria
	Wireless MAB	Top ten Wireless MAB endPointProfile	<ul style="list-style-type: none"> <li>▪ Select by pxGrid_endPointProfile</li> <li>▪ pxGrid_EventName as User Sessions</li> <li>▪ pxGrid_nasPortType as Wireless</li> <li>▪ pxGrid_serviceType as Call Check</li> </ul>
	VPN	Top ten VPN endPointProfile	<ul style="list-style-type: none"> <li>▪ Select by pxGrid_endPointProfile</li> <li>▪ pxGrid_EventName as User Sessions</li> <li>▪ pxGrid_nasPortType as Virtual</li> </ul>
	WebAuth	Top ten WebAuth (MAB+Guest) endPointProfile	<ul style="list-style-type: none"> <li>▪ Select by pxGrid_endPointProfile</li> <li>▪ pxGrid_EventName as User Sessions</li> <li>▪ pxGrid_radiusFlowType as wiredMAB or wirelessMAB</li> <li>▪ pxGrid_username as a valid name, not MAC ID</li> </ul>
Failed Authentications	User	All	<ul style="list-style-type: none"> <li>▪ Top ten users with failed auth</li> <li>▪ Select by pxGrid_username</li> <li>▪ pxGrid_EventName as Radius Failure</li> </ul>
		Wired	<ul style="list-style-type: none"> <li>▪ Top ten Wired users with failed auth</li> <li>▪ Select by pxGrid_username</li> <li>▪ pxGrid_EventName as Radius Failure</li> <li>▪ pxGrid_nasPortType as Ethernet</li> </ul>
		Wireless	<ul style="list-style-type: none"> <li>▪ Top ten Wireless users with failed auth</li> <li>▪ Select by pxGrid_username</li> <li>▪ pxGrid_EventName as Radius Failure</li> <li>▪ pxGrid_nasPortType as Wireless</li> </ul>
		VPN	<ul style="list-style-type: none"> <li>▪ Top ten VPN users with failed auth</li> <li>▪ Select by pxGrid_username</li> <li>▪ pxGrid_EventName as Radius Failure</li> <li>▪ pxGrid_nasPortType as Virtual</li> </ul>
		WebAuth	<ul style="list-style-type: none"> <li>▪ Top ten WebAuth (MAB+Guest) users with failed auth</li> <li>▪ Select by pxGrid_username</li> <li>▪ pxGrid_EventName as Radius Failure</li> <li>▪ pxGrid_radiusFlowType as wiredMAB or wirelessMAB</li> <li>▪ pxGrid_username as a valid name, not MAC ID</li> </ul>

Tab Name		Description	Search Criteria	
Failure reasons	All	Top ten Failure reason with failed auth	<ul style="list-style-type: none"> <li>Select by pxGrid_failureReason</li> <li>pxGrid_EventName as Radius Failure</li> </ul>	
	Wired	Top ten Failure Reason for wired user with failed auth	<ul style="list-style-type: none"> <li>Select by pxGrid_failureReason</li> <li>pxGrid_EventName as Radius Failure</li> <li>pxGrid_nasPortType as Ethernet</li> </ul>	
	Wireless	Top ten Failure Reason for wireless user with failed auth	<ul style="list-style-type: none"> <li>Select by pxGrid_failureReason</li> <li>pxGrid_EventName as Radius Failure</li> <li>pxGrid_nasPortType as Wireless</li> </ul>	
	VPN	Top ten Failure Reason for VPN users with failed auth	<ul style="list-style-type: none"> <li>Select by pxGrid_failureReason</li> <li>pxGrid_EventName as Radius Failure</li> <li>pxGrid_nasPortType as Virtual</li> </ul>	
	WebAuth	Top ten Failure Reason for WebAuth (MAB+Guest) with failed auth	<ul style="list-style-type: none"> <li>Select by pxGrid_failureReason</li> <li>pxGrid_EventName as Radius Failure</li> <li>pxGrid_radiusFlowType as wiredMAB or wirelessMAB</li> <li>pxGrid_username as a valid name, not MAC ID</li> </ul>	
	Auth Type	All	Top ten deviceType by Failed Auth with failed auth	<ul style="list-style-type: none"> <li>Select by pxGrid_deviceType</li> <li>pxGrid_EventName as Radius Failure</li> </ul>
		Wired	Top ten deviceType for Wired users with failed auth	<ul style="list-style-type: none"> <li>Select by pxGrid_deviceType</li> <li>pxGrid_EventName as Radius Failure</li> <li>pxGrid_nasPortType as Ethernet</li> </ul>
		Wireless	Top ten deviceType for Wireless users with failed auth	<ul style="list-style-type: none"> <li>Select by pxGrid_deviceType</li> <li>pxGrid_EventName as Radius Failure</li> <li>pxGrid_nasPortType as Wireless</li> </ul>
		VPN	Top ten deviceType for VPN users with failed auth	<ul style="list-style-type: none"> <li>Select by pxGrid_deviceType</li> <li>pxGrid_EventName as Radius Failure</li> <li>pxGrid_nasPortType as Virtual</li> </ul>
		WebAuth	Top ten deviceType WebAuth (MAB+Guest) users with failed auth	<ul style="list-style-type: none"> <li>Select by pxGrid_deviceType</li> <li>pxGrid_radiusFlowType as wiredMAB or wirelessMAB</li> </ul>

Tab Name		Description		Search Criteria
				<ul style="list-style-type: none"> <li>pxGrid_username as a valid name, not MAC ID</li> </ul>
	Location	All	Top ten locations with failed auth	<ul style="list-style-type: none"> <li>Select by pxGrid_location</li> <li>pxGrid_EventName as Radius Failure</li> </ul>
		Wired	Top ten locations of Wired users with failed auth	<ul style="list-style-type: none"> <li>Select by pxGrid_location</li> <li>pxGrid_EventName as Radius Failure</li> <li>pxGrid_nasPortType as Ethernet</li> </ul>
		Wireless	Top ten locations of Wireless users with failed auth	<ul style="list-style-type: none"> <li>Select by pxGrid_location</li> <li>pxGrid_EventName as Radius Failure</li> <li>pxGrid_nasPortType as Wireless</li> </ul>
		VPN	Top ten locations of VPN users with failed auth	<ul style="list-style-type: none"> <li>Select by pxGrid_location</li> <li>pxGrid_EventName as Radius Failure</li> <li>pxGrid_nasPortType as Virtual</li> </ul>
		WebAuth	Top ten location of WebAuth (MAB+Guest) users with failed auth	<ul style="list-style-type: none"> <li>Select by pxGrid_location</li> <li>pxGrid_EventName as Radius Failure</li> <li>pxGrid_radiusFlowType as wiredMAB or wirelessMAB</li> <li>pxGrid_username as a valid name, not MAC ID</li> </ul>
Compliance	All	Top ten postureStatus	<ul style="list-style-type: none"> <li>Select by pxGrid_postureStatus</li> </ul>	
	Wired	Top ten postureStatus of Wired users	<ul style="list-style-type: none"> <li>Select by pxGrid_postureStatus</li> <li>pxGrid_nasPortType as Ethernet</li> </ul>	
	Wired MAB	Top ten postureStatus of Wired MAB users	<ul style="list-style-type: none"> <li>Select by pxGrid_postureStatus</li> <li>pxGrid_nasPortType as Ethernet</li> <li>pxGrid_serviceType as Call Check</li> </ul>	
	Wireless	Top ten postureStatus of Wireless users	<ul style="list-style-type: none"> <li>Select by pxGrid_postureStatus</li> <li>pxGrid_nasPortType as Wireless</li> </ul>	
	Wireless MAB	Top ten postureStatus of Wireles MAB users	<ul style="list-style-type: none"> <li>Select by pxGrid_postureStatus</li> <li>pxGrid_nasPortType as Wireless</li> <li>pxGrid_serviceType as Call Check</li> </ul>	

Tab Name		Description	Search Criteria	
	VPN	Top ten postureStatus of VPN users	<ul style="list-style-type: none"> <li>Select by pxGrid_postureStatus</li> <li>pxGrid_nasPortType as Virtual</li> </ul>	
TrustSec	Group Tag	All	<ul style="list-style-type: none"> <li>Top ten ctsSecurityGroup</li> </ul>	<ul style="list-style-type: none"> <li>Select by pxGrid_ctsSecurityGroup</li> </ul>
		Wired	Top ten ctsSecurityGroup of Wired users	<ul style="list-style-type: none"> <li>Select by pxGrid_ctsSecurityGroup</li> <li>pxGrid_nasPortType as Ethernet</li> </ul>
		Wired MAB	Top ten ctsSecurityGroup of Wired MAB users	<ul style="list-style-type: none"> <li>Select by pxGrid_ctsSecurityGroup</li> <li>pxGrid_nasPortType as Ethernet</li> </ul>
		Wireless	Top ten ctsSecurityGroup of Wireless users	<ul style="list-style-type: none"> <li>Select by pxGrid_ctsSecurityGroup</li> <li>pxGrid_nasPortType as Wireless</li> </ul>
		Wireless MAB	Top ten ctsSecurityGroup of Wireles MAB users	<ul style="list-style-type: none"> <li>Select by pxGrid_ctsSecurityGroup</li> <li>pxGrid_nasPortType as Wireless</li> </ul>
		VPN	Top ten ctsSecurityGroup of vpn users	<ul style="list-style-type: none"> <li>Select by pxGrid_ctsSecurityGroup</li> <li>pxGrid_nasPortType as Virtual</li> </ul>
		WebAuth	Top ten ctsSecurityGroup of WebAuth (MAB+Guest) users	<ul style="list-style-type: none"> <li>Select by pxGrid_ctsSecurityGroup</li> <li>pxGrid_radiusFlowType as wiredMAB or wirelessMAB</li> <li>pxGrid_username as a valid name, not MAC ID</li> </ul>
MDM	Compliance	Top ten mdmComplianceStatus	<ul style="list-style-type: none"> <li>Select by pxGrid_mdmComplianceStatus</li> <li>pxGrid_EventName as User Sessions</li> </ul>	
	Registration	Top ten mdmRegistrationStatus	<ul style="list-style-type: none"> <li>Select by pxGrid_mdmRegistrationStatus</li> <li>pxGrid_EventName as User Sessions</li> </ul>	



## Search Functionality

The Search tab is the first tab on the page where user can enter the search details. While clicking on the tab the search page should be displayed with a search box, dropdown to select the type of event (Session, Radius, or both) to search, and a date-picker adjacent.

When the user enters text in the search box and clicks the Search' button, the date field should be populated with the existing date range from the application window by default. The end users should be able to change its according to their needs. If the search returns more than 200 (TBD) records the user should get an acknowledgement saying "This search returns too many records" and displaying the first 200 records. In such cases, the user should narrow down their search by using the event type filter and the minimum time span.

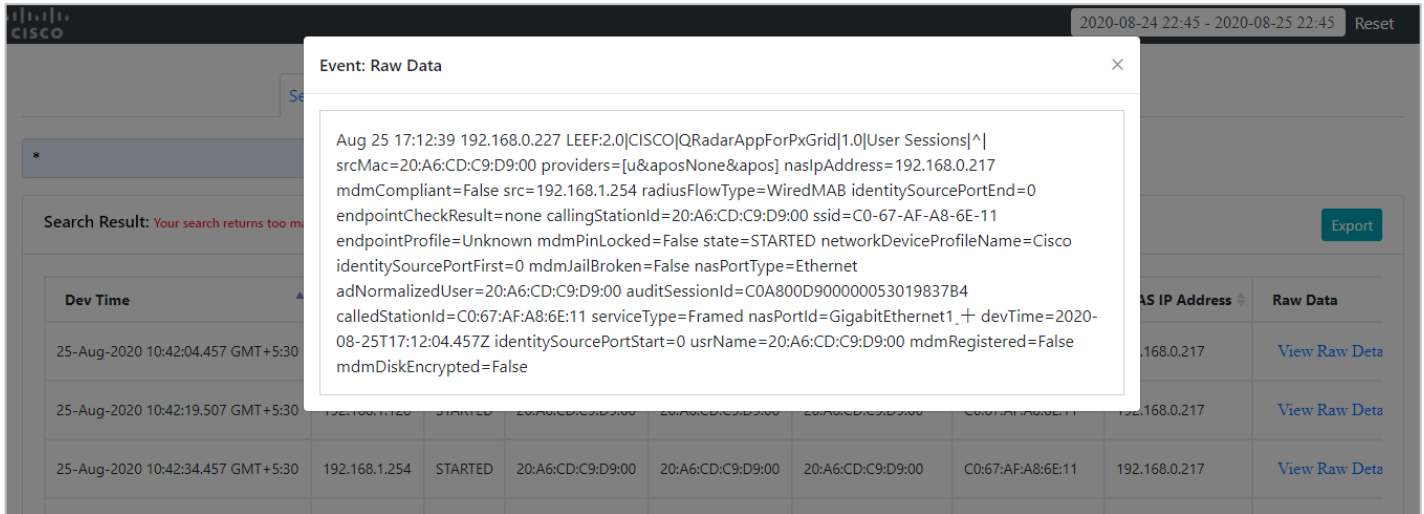
In the search window, the user should be able to enter IP Address, MAC Address and Session ID. When the user clicks the search button, the results should be displayed in a tabular format with pagination. The result's displayed format will be same as the current window displayed with details while clicking on the existing graph in dashboard.

There should be an option (hyperlink) provided at the end of the table to view the raw event associated with the selected event. The request data from the UI should be validated for security and valid request format.

The screenshot shows the IBM QRadar search interface. At the top, there is a navigation bar with various tabs like Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Admin, Pre-Validation, and Cisco ISE pxGrid. A search bar is present with a date range of 2020-09-02 14:27 - 2020-09-03 14:27. Below the search bar, there are tabs for Search, Passed Authentications, Failed Authentications, Devices, Compliance, Trustsec, MDM, and ANC Details. The search criteria are set to "Session" and the date range is "September 2, 2020 14:27 - September 3, 2020 14:27". A "Search" button is visible. Below the search bar, a message states "Search Result: Search criteria return more records. The first 200 records are displayed." and there is an "Export" button. The search results are displayed in a table with the following columns: Dev Time, IP Address, State, MAC Address, Username, Calling Station ID, Called StationID, NAS IP Address, and Raw Data. The table contains five rows of data, each with a "View Raw Details" link.

Dev Time	IP Address	State	MAC Address	Username	Calling Station ID	Called StationID	NAS IP Address	Raw Data
02-Sep-2020 09:12:19.597 GMT+5:30	192.168.1.254	STARTED	20:A6:CD:C9:D9:00	20:A6:CD:C9:D9:00	20:A6:CD:C9:D9:00	C0:67:AF:A8:6E:11	192.168.0.217	<a href="#">View Raw Details</a>
02-Sep-2020 09:12:26.564 GMT+5:30	192.168.1.128	STARTED	20:A6:CD:C9:D9:00	20:A6:CD:C9:D9:00	20:A6:CD:C9:D9:00	C0:67:AF:A8:6E:11	192.168.0.217	<a href="#">View Raw Details</a>
02-Sep-2020 09:12:41.085 GMT+5:30	10.235.24.6	STARTED	02:8F:A5:7E:9C:8A	02:8F:A5:7E:9C:8A	02:8F:A5:7E:9C:8A	C0:67:AF:A8:6E:11	192.168.0.217	<a href="#">View Raw Details</a>
02-Sep-2020 09:12:49.602 GMT+5:30	192.168.1.254	STARTED	20:A6:CD:C9:D9:00	20:A6:CD:C9:D9:00	20:A6:CD:C9:D9:00	C0:67:AF:A8:6E:11	192.168.0.217	<a href="#">View Raw Details</a>
02-Sep-2020 09:12:54.749 GMT+5:30	192.168.0.42	STARTED	02:8F:A5:7E:9C:8A	02:8F:A5:7E:9C:8A	02:8F:A5:7E:9C:8A	C0:67:AF:A8:6E:11	192.168.0.217	<a href="#">View Raw Details</a>





**Accepted Search format:**

- IP Address      X.X.X.X
- MAC Address    X:X:X:X
- Session ID     XXXX

**Partial Search Criteria:**

- IP Address should begin with X.
- Mac Address should begin with X:

**Accepted Wildcard characters:**

Wildcard Character	Description	Example
*	Matches a string of zero or more characters	*.*,*:*,192.*,192.168.*.*,AE:BC:*
?	Matches any single character	192.???.???.???,192.168.???.124,DE:?:DF:*

## Passed Authentications

The Passed Authentications dashboard view provides visibility into successful machine and user authentications across an organization and by wired and wireless connection type. This provides the admin with a view of how employees are connecting to the network, are they connecting over Wired, Wireless, VPN or Guest and where are they connecting from. This information is obtained from the Cisco ISE pxGrid App pxGrid client subscribing to the Session Directory topic.

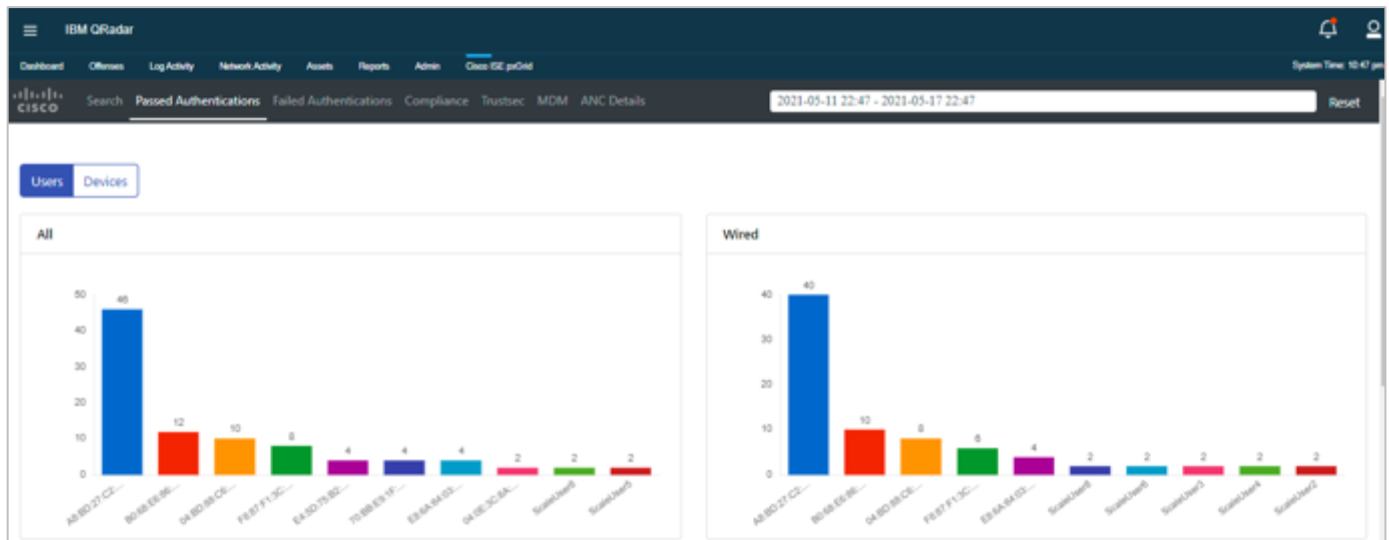
The admin drills down on the user or host and obtains the following contextual information: endpoint device information, MAC Address, IP Address, posture status, NAS Port Type, NAS Port ID, NAS Identifier, NAS IP Address, WLAN Information, Calling Station ID, Called Station ID, AD resolvable user and host identities.

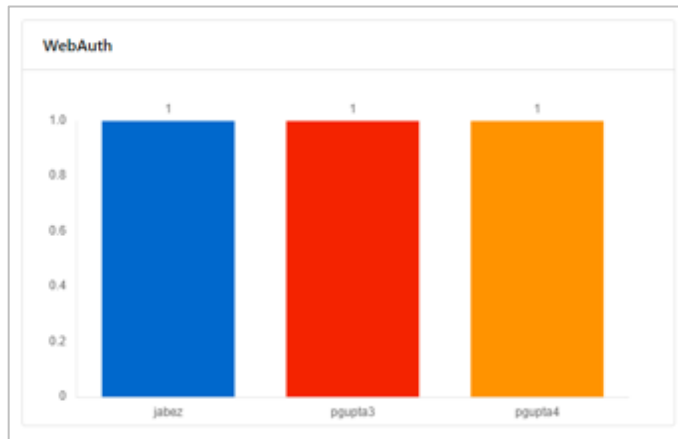
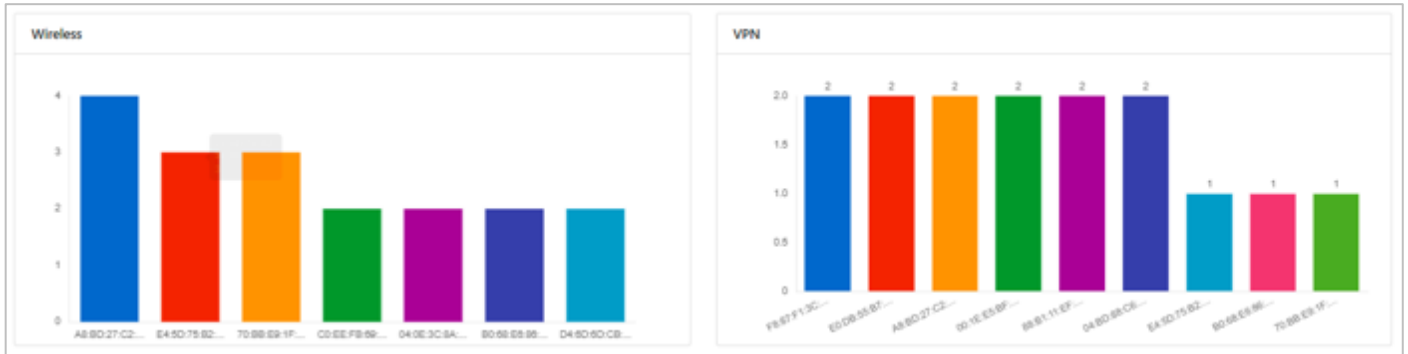
The AD resolvable user and host identities provide a consistent name format when different EAP methods are used, for example, EAP Chaining.

For the WebAuth (guest & employee access) portion we show the credentialed authentication flow. We don't show Hotspot (basic MAB).

Note: Some fields for WebAuth may not apply as they're using Guest users.

Step 1 Go to **Cisco ISE pxGrid > Passed Authentications**.





Step 2 Select an end-user, this provides a tabular view of the following contextual information:

Data For : ScaleUser7

Show 10 entries

Dev Time	IP Address	State	MAC Address	Username	Calling Station ID	Called StationID	NAS IP Address	NAS Port ID	NAS Port Type	NAS Identifier	Posture State
06-Jul-2021 09:46:19.274 GMT+5:30	21.0.0.15	STARTED	95:70:28:E4:00:06	ScaleUser7	95:70:28:E4:00:06	None	1.1.1.1	GigabitEthernet1/	Ethernet	None	None
06-Jul-2021 09:46:19.274 GMT+5:30	21.0.0.15	STARTED	95:70:28:E4:00:06	ScaleUser7	95:70:28:E4:00:06	None	1.1.1.1	GigabitEthernet1/	Ethernet	None	None

Showing 1 to 2 of 2 entries

The **Endpoint Profile**, **Endpoint Operating System**, and the **AD Normalized User Name** provide the endpoint information for the user.

Data For : ScaleUser7

Show 10 entries

atus	Endpoint Profile	Endpoint Operating System	Group ID	AD Normalized User	AD Host Domain Name	AD Host NetBios Name	AD Host Resolved Identifies	AD Host Resolved DNS	AD User Domain N.
	Unknown	None	None	ScaleUser7	None	None	None	None	None
	Unknown	None	None	ScaleUser7	None	None	None	None	None

Showing 1 to 2 of 2 entries

The **AD user Resolved Identities** and **AD User Resolved DNS** provide the consistent identities of the end user.

AD User Domain Name	AD User Net Bios Name	AD User Resolved Identities	AD User Resolved DNS
ddcloud.cisco.com	D\CLOUD	doctor@ddcloud.cisco.com	CN=Doctor,OU=Demo Users,DC=ddcloud,DC=cisco,DC=com
ddcloud.cisco.com	D\CLOUD	doctor@ddcloud.cisco.com	CN=Doctor,OU=Demo Users,DC=ddcloud,DC=cisco,DC=com
ddcloud.cisco.com	D\CLOUD	doctor@ddcloud.cisco.com	CN=Doctor,OU=Demo Users,DC=ddcloud,DC=cisco,DC=com
ddcloud.cisco.com	D\CLOUD	doctor@ddcloud.cisco.com	CN=Doctor,OU=Demo Users,DC=ddcloud,DC=cisco,DC=com

The **Is Machine Authentication** attribute determines if this is machine authentication or user authentication. If this attribute is set to **"true"**, then this is machine authentication, if this is set to **"false"**, then this is user authentication.

Data For : ScaleUser7

Show 10 entries EXPORT

AD User Resolved DNS	Terminal Server Agent ID	Is Machine Authentication	Service Type	Tunnel Private Group ID	Addressspace WLAN ID	Network Device Profile Name	Radius Flow Type	SSID	ANC Policy
ne	None	None	None	None	None	Cisco	None	None	None
ne	None	None	None	None	None	Cisco	None	None	None

Showing 1 to 2 of 2 entries Previous 1 Next

## Devices

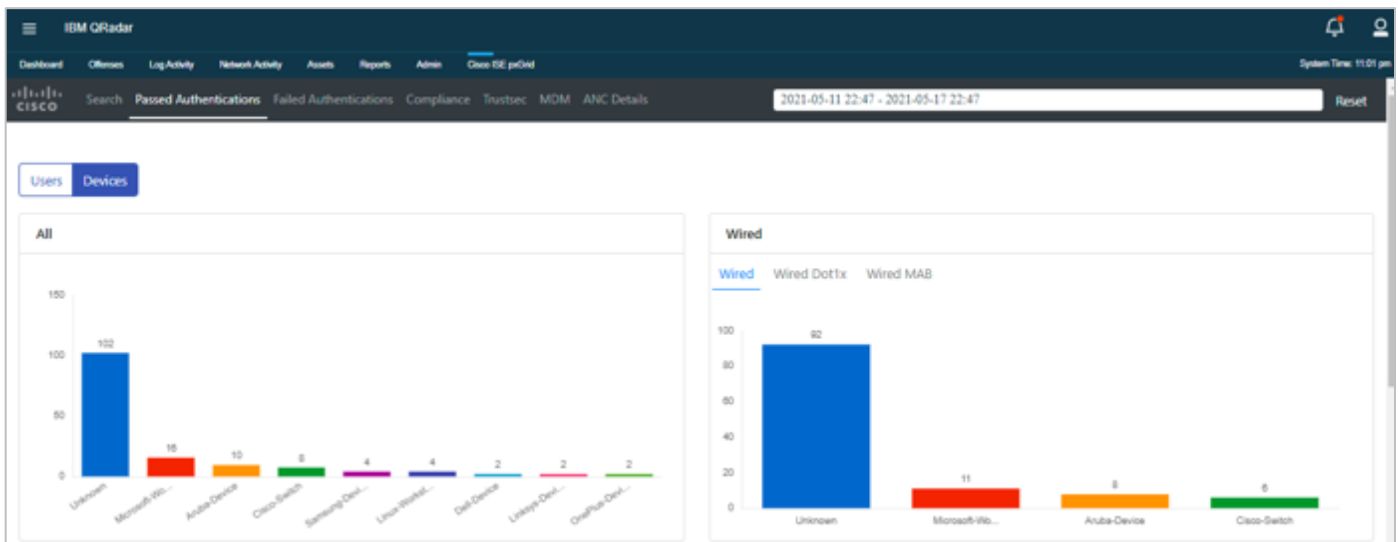
The Devices Dashboard View provides the admin with visibility into the connected devices across the organization or by wired and wireless connection types. An organization may have a security policy about recommended or non-recommended devices for employees. The admin is able to drill down and see the owners of these devices and their location. This information is obtained from the Cisco ISE pxGrid App client subscribing to the Session Directory topic.

The admin drills down on the endpoint profile and obtains the following contextual information: endpoint device information, MAC Address, IP Address, posture status, NAS Port Type, NAS Port ID, NAS Identifier, NAS IP Address, WLAN Information, Calling Station ID, Called Station ID, AD resolvable user and host identities.

The AD resolvable user and host identities provide a consistent name format when different EAP methods are used, for example, EAP Chaining.

Step 1 Go to **Cisco ISE pxGrid > Passed Authentications > Devices**.

Step 2 Select **EndProfile (All) > Microsoft-Workstation**.





The Username, IP address and MAC address attributes are associated with the device.

The NAS IP, NAS Port ID and NAS Port Type attributes contain the connection type information.

Dashboard Overview Log Activity Network Activity Assets Reports Admin Cisco ISE psGat System Time: 11:04 pm

Data For: **Microsoft-Workstation** EXPORT

Show 10 entries

Dev Time	IP Address	State	MAC Address	Username	Calling Station ID	Called StationID	NAS IP Address	NAS Port ID	NAS Port Type	NAS Identifier
06-Jan-2020 03:09:28:567 GMT+5:30	192.168.0.44	DISCONNECTED	4C:8B:58:3E:0D:97	4C:8B:58:3E:0D:97	4C:8B:58:3E:0D:97	C0:67:AF:A8:EE:11	192.168.0.217	GigabitEthernet1/...	Ethernet	None
06-Jan-2020 03:09:29:753 GMT+5:30	192.168.0.56	DISCONNECTED	28:C6:3F:C4:61:93	28:C6:3F:C4:61:93	28:C6:3F:C4:61:93	C0:67:AF:A8:EE:11	192.168.0.217	GigabitEthernet1/...	Ethernet	None
06-Jan-2020 03:09:31:281 GMT+5:30	192.168.0.94	DISCONNECTED	FE:FC:16:61:D7:98	FE:FC:16:61:D7:98	FE:FC:16:61:D7:98	C0:67:AF:A8:EE:11	192.168.0.217	GigabitEthernet1/...	Ethernet	None
06-Jan-2020 03:07:23:510 GMT+5:30	192.168.0.212	STARTED	E8:6A:64:03:83:64	E8:6A:64:03:83:64	E8:6A:64:03:83:64	C0:67:AF:A8:EE:11	192.168.0.217	GigabitEthernet1/...	Ethernet	None
06-Jan-2020 03:07:23:510 GMT+5:30	192.168.0.212	STARTED	E8:6A:64:03:83:64	E8:6A:64:03:83:64	E8:6A:64:03:83:64	C0:67:AF:A8:EE:11	192.168.0.217	GigabitEthernet1/...	Ethernet	None

The NAS Identifier attribute may contain more information about the device such as the MAC address. The EndPoint Profile and Endpoint Operating System attributes provide the type of device and operating system.

Data For : Microsoft-Workstation

Show 10 entries

Posture Status	Endpoint Profile	Endpoint Operating System	Group ID	AD Normalized User	AD Host Domain Name	AD Host NetBios Name	AD Host Resolve
None	Microsoft-Workstation	Microsoft Windows Vista, Windows 7 SP1, or Windows 8.1 Update 1	None	4C8B5B3E0D97	None	None	None
None	Microsoft-Workstation	Microsoft Windows Server 2008 or 2008 Beta 3 (accuracy 93%)	None	2BCE3FC4E193	None	None	None
None	Microsoft-Workstation	Microsoft Windows Longhorn (accuracy 94%)	None	F8C1E61D798	None	None	None
None	Microsoft-Workstation	Microsoft Windows Longhorn (accuracy 95%)	None	EB6A6403B3E4	None	None	None
None	Microsoft-Workstation	Microsoft Windows Longhorn (accuracy 95%)	None	EB6A6403B3E4	None	None	None

The **AD Username/Host** and **AD Resolved Username/Host** identity attributes provide a consistent way of providing the username and hostname despite various EAP authentication types.

Data For : Microsoft-Workstation

Show 10 entries

AD Host Resolved DNS	AD User Domain Name	AD User Net Bios Name	AD User Resolved Identities	AD User Resolved DNS	Terminal Server Agent ID	Is Machine Authentication	Service Type	Tunnel Pri
None	None	None	None	None	None	None	Framed	None
None	None	None	None	None	None	None	Framed	None
None	None	None	None	None	None	None	Framed	None
None	None	None	None	None	None	None	Framed	None
None	None	None	None	None	None	None	Framed	None

The **Is Machine Authentication** attribute if set to "true" denotes that this is machine authentication. If it is set to "false", it denotes user authentication.

Data For : Microsoft-Workstation

Show 10 entries

id DNS	Terminal Server Agent ID	Is Machine Authentication	Service Type	Tunnel Private Group ID	Airspace WLAN ID	Network Device Profile Name	Radius Flow Type	SSID	ANC Policy
None	None	None	Framed	None	None	Cisco	WiredMAB	CO-E7-AF-AS-EE-11	None
None	None	None	Framed	None	None	Cisco	WiredMAB	CO-E7-AF-AS-EE-11	None
None	None	None	Framed	None	None	Cisco	WiredMAB	CO-E7-AF-AS-EE-11	None
None	None	None	Framed	None	None	Cisco	WiredMAB	CO-E7-AF-AS-EE-11	None
None	None	None	Framed	None	None	Cisco	WiredMAB	CO-E7-AF-AS-EE-11	None

## Failed Authentications

The Failed Authentications dashboard view provides visibility into failed authentication attempts across the organization and by wired and wireless connection types. This provides the admin with a view of how these failed authentications occur with panel breakdowns by user, failure reason, device type, and location. This information is obtained from the Cisco ISE pxGrid client App subscribing to the RADIUS failure topic.

The user panel provides a breakdown by user and provides the following contextual information: failure reason, device type, location, endpoint device information, MAC address, IP Address, posture status, NAS IP address, NAS Port Type, NAS Port ID, WLAN information, NAS Identifier, Calling Station ID, Called Station ID, access, identity store, and credit check.

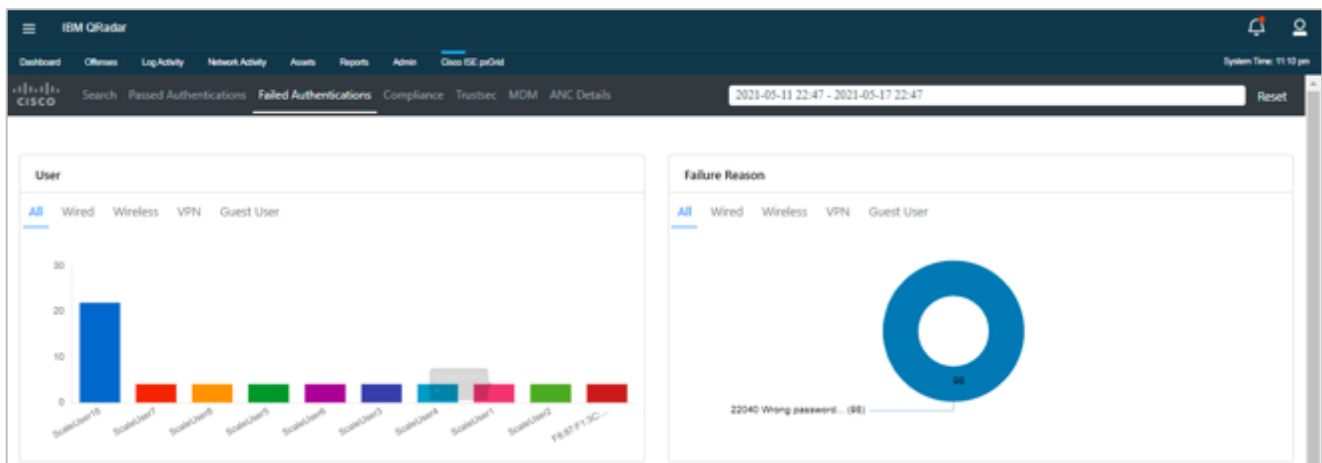
The other panels provide a breakdown by failure reason, device type and location, and provide the admin insight to how these failed authentications occur. The same contextual information from the user panel is available in these panel breakdowns.

The AD resolvable user and host identities provide a consistent name format when different EAP methods are used, for example, EAP Chaining.

### User Panel

The user panel provides a breakdown by username.

Step 1 Go to **Cisco ISE pxGrid > Failed Authentications**.



Step 2 Go to **Cisco ISE pxGrid > Failed Authentications > User > ScaleUser7**.

Step 3 The **IP Address, Failure Reason, Username** attributes provide information into failed authentication attempts.



Data For : ScaleUser7

Show 10 entries

ID	Dev Time	IP Address	Failure Reason	Username	Server Name	Authentication Protocol	Device Type	Location	Calling Station ID
1619632837049804	12-May-2021 04:12:45.681 GMT+5:30	21.0.0.7	22040 Wrong password or invalid shared secret	ScaleUser7	cisco/seprispn	PAP_ASCII	All Device Types	All Locations	95:70:28:E4:00:06
1619632837049804	12-May-2021 04:12:45.681 GMT+5:30	21.0.0.7	22040 Wrong password or invalid shared secret	ScaleUser7	cisco/seprispn	PAP_ASCII	All Device Types	All Locations	95:70:28:E4:00:06
1619632837049948	12-May-2021 05:51:20.159 GMT+5:30	21.0.0.7	22040 Wrong password or invalid shared secret	ScaleUser7	cisco/seprispn	PAP_ASCII	All Device Types	All Locations	95:70:28:E4:00:06
1619632837049948	12-May-2021 05:51:20.159 GMT+5:30	21.0.0.7	22040 Wrong password or invalid shared secret	ScaleUser7	cisco/seprispn	PAP_ASCII	All Device Types	All Locations	95:70:28:E4:00:06

Showing 1 to 4 of 4 entries

The **Server Name**, **Authentication Protocol**, **Device Type**, **Location**, **Calling Station ID**, **NAS IP Address**, **NAS Port ID**, **NAS Port Type** attributes provide more authentication details and location information of failed authentication attempts.

Data For : ScaleUser7

Show 10 entries

NAS IP Address	NAS Port ID	NAS Port Type	MAC Address	Message Code	User Type	Access Service	Identity Store	Authentication Method	Service Type	Credential Check	AD Non
1.1.1.1	GigabitEthernet1	Ethernet	None	5400	User	Default Network Access	Internal Users	PAP_ASCII	None	PAP_ASCII	None
1.1.1.1	GigabitEthernet1	Ethernet	None	5400	User	Default Network Access	Internal Users	PAP_ASCII	None	PAP_ASCII	None
1.1.1.1	GigabitEthernet1	Ethernet	None	5400	User	Default Network Access	Internal Users	PAP_ASCII	None	PAP_ASCII	None
1.1.1.1	GigabitEthernet1	Ethernet	None	5400	User	Default Network Access	Internal Users	PAP_ASCII	None	PAP_ASCII	None

Showing 1 to 4 of 4 entries

The **Access Service** attribute provide the ISE allowed protocol rules, the **Identity Store** attribute provides the back-end credential database of the end-user in question.

The **Authentication Method** attribute provides the ISE authentication rule, and the **Credit Check** attribute provides the EAP authentication method.

Data For : ScaleUser7

Show 10 entries

AD Host Domain Name	AD Host NetBios Name	AD Host Resolved Identities	AD Host Resolved DNS	AD User Domain Name	AD User Net Bios Name	AD User Resolved Identities	AD User Resolved DNS
None	None	None	None	None	None	None	None
None	None	None	None	None	None	None	None
None	None	None	None	None	None	None	None
None	None	None	None	None	None	None	None

Showing 1 to 4 of 4 entries

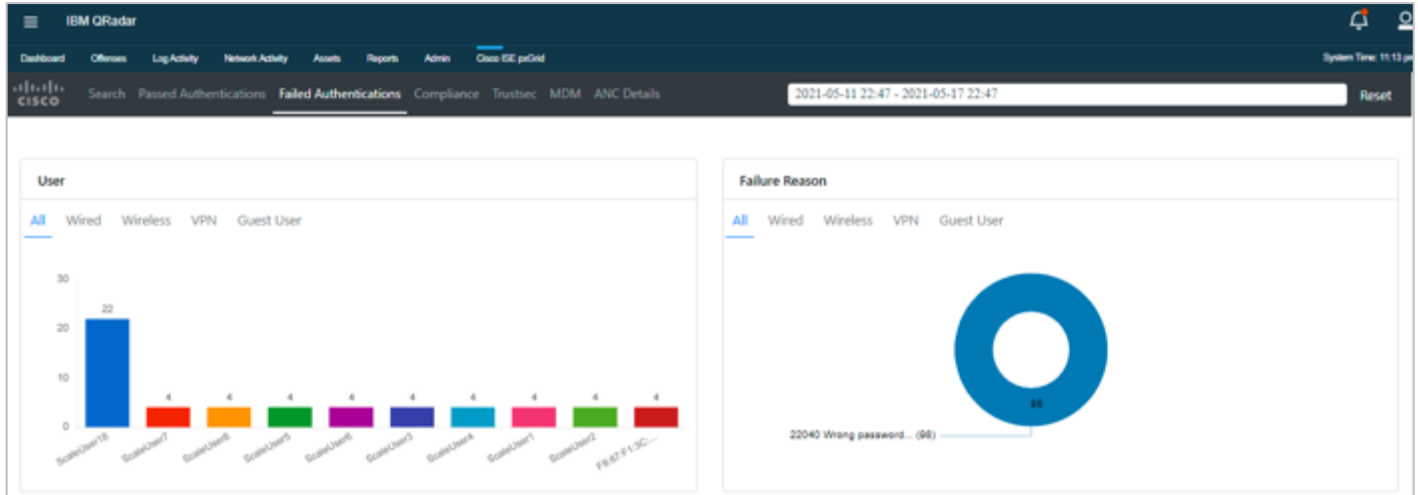
The **AD Host/User Resolved Identities**, **AD Host/User Resolved DNS**, **AD User Domain**, **AD User Net BIOS Name Host** attributes in the screenshots provide additional context around the host and user identities.

## Failure Reason Panel

The Failure Reason panel provides a breakdown by failure reason.

Step 1 Go to **Cisco ISE pxGrid > Failed Authentications**.

Step 2 Select **Failure Reason > 22408 User authentication against Active Directory failed since user has entered the wrong password**.



The **IP Address**, **Calling Station ID**, **Username** attributes provide basic information for end users associated with failure reasons.

Data For : 22040 Wrong password or invalid shared secret

Show 10 entries

ID	Dev Time	IP Address	Failure Reason	Username	Server Name	Authentication Protocol	Device Type	Location	Calling Station ID
1619632837049798	12-May-2021 04:12:45.480 GMT+5:30	21.0.0.1	22040 Wrong password or invalid shared secret	ScaleUser1	ciscoiseprism	PAP_ASCII	All Device Types	All Locations	95:70:2B:E4:00:00
1619632837049799	12-May-2021 04:12:45.505 GMT+5:30	21.0.0.2	22040 Wrong password or invalid shared secret	ScaleUser2	ciscoiseprism	PAP_ASCII	All Device Types	All Locations	95:70:2B:E4:00:01
1619632837049800	12-May-2021 04:12:45.529 GMT+5:30	21.0.0.3	22040 Wrong password or invalid shared secret	ScaleUser3	ciscoiseprism	PAP_ASCII	All Device Types	All Locations	95:70:2B:E4:00:02
1619632837049802	12-May-2021 04:12:45.557 GMT+5:30	21.0.0.5	22040 Wrong password or invalid shared secret	ScaleUser5	ciscoiseprism	PAP_ASCII	All Device Types	All Locations	95:70:2B:E4:00:04

EXPORT

The **Server Name**, **Authentication Protocol**, **Device Type**, **Location**, **Calling Station ID**, **NAS IP Address**, **NAS Port ID**, **NAS Port Type** attributes provide more authentication details and location information of failed authentication attempts.

Data For : 22040 Wrong password or invalid shared secret

Show 10 entries

NAS IP Address	NAS Port ID	NAS Port Type	MAC Address	Message Code	User Type	Access Service	Identity Store	Authentication Method	Service Type	Credential Check	AD Norm
1.1.1.1	GigabitEthernet1/	Ethernet	None	5400	User	Default Network Access	Internal Users	PAP_ASCII	None	PAP_ASCII	None
1.1.1.1	GigabitEthernet1/	Ethernet	None	5400	User	Default Network Access	Internal Users	PAP_ASCII	None	PAP_ASCII	None
1.1.1.1	GigabitEthernet1/	Ethernet	None	5400	User	Default Network Access	Internal Users	PAP_ASCII	None	PAP_ASCII	None
1.1.1.1	GigabitEthernet1/	Ethernet	None	5400	User	Default Network Access	Internal Users	PAP_ASCII	None	PAP_ASCII	None

The **Access Service** attribute provides the ISE allowed protocol rules, the **Identity Store** attribute provides the back-end credential database of the needed end user.

The **Authentication Method** attribute provides the ISE authentication rule, and the **Credit Check** attribute provides the EAP authentication method.

Data For : 22040 Wrong password or invalid shared secret

Show 10 entries

AD Host Domain Name	AD Host NetBios Name	AD Host Resolved Identities	AD Host Resolved DNS	AD User Domain Name	AD User Net Bios Name	AD User Resolved Identities	AD User Resolved DNS
None	None	None	None	None	None	None	None
None	None	None	None	None	None	None	None
None	None	None	None	None	None	None	None
None	None	None	None	None	None	None	None

The **AD Host/User Resolved Identities**, **AD Host/User Resolved DNS**, **AD User Domain**, **AD User Net BIOS Name Host** attributes in the images provide additional context around the host and user identities.

## Auth Type Panel

The **Auth Type** attribute categorizes the NAD device for Network Device Groups that may distinguish by different locations. For example, you may have Cisco Catalysts switches for the North America locations.

To categorize device type:

Step 1 Go to **Cisco ISE pxGrid > Failed Authentications**.

Step 2 Select **Device Type > All Device Types**.

<p>User</p> <p>All Wired Wireless VPN WebAuth</p>	<p>Failure Reason</p> <p>All Wired Wireless VPN WebAuth</p>
---	---



The **IP Address**, **Calling Station ID**, and **Username** attributes provide basic information for end users associated with failure reasons.

Data For : All Device Types

Show 10 entries

ID	Dev Time	IP Address	Failure Reason	Username	Server Name	Authentication Protocol	Device Type	Location	Calling Station ID
1619632837049942	12-May-2021 09:51:20.003 GMT+5:30	21.0.0.1	22040 Wrong password or invalid shared secret	ScaleUser1	cisco/seprispn	PAP_ASCII	All Device Types	All Locations	95:7D:2B:E4:0D:00
1619632837049943	12-May-2021 09:51:20.035 GMT+5:30	21.0.0.2	22040 Wrong password or invalid shared secret	ScaleUser2	cisco/seprispn	PAP_ASCII	All Device Types	All Locations	95:7D:2B:E4:0D:01

The **Server Name**, **Authentication Protocol**, **Device Type**, **Location**, **Calling Station ID**, **NAS IP Address**, **NAS Port ID**, and **NAS Port Type** attributes provide more authentication details and location information of failed authentication attempts.

Data For : All Device Types

Show 10 entries

NAS IP Address	NAS Port ID	NAS Port Type	MAC Address	Message Code	User Type	Access Service	Identity Store	Authentication Method	Service Type	Credential Check	AD Norm
1.1.1.1	GigabitEthernet1/	Ethernet	None	5400	User	Default Network Access	Internal Users	PAP_ASCII	None	PAP_ASCII	None
1.1.1.1	GigabitEthernet1/	Ethernet	None	5400	User	Default Network Access	Internal Users	PAP_ASCII	None	PAP_ASCII	None
1.1.1.1	GigabitEthernet1/	Ethernet	None	5400	User	Default Network Access	Internal Users	PAP_ASCII	None	PAP_ASCII	None

The **Access Service** attribute provides the ISE allowed protocol rules, the **Identity Store** attribute provides the back-end credential database of the needed end user.

The **Authentication Method** attribute provides the ISE authentication rule, and the **Credit Check** attribute provides the EAP authentication method.

Data For : All Device Types

Show 10 entries

AD Host Domain Name	AD Host NetBios Name	AD Host Resolved Identities	AD Host Resolved DNS	AD User Domain Name	AD User Net Bios Name	AD User Resolved Identities	AD User Resolved DNS
None	None	None	None	None	None	None	None
None	None	None	None	None	None	None	None
None	None	None	None	None	None	None	None

The **AD Host/User Resolved Identities**, **AD Host/User Resolved DNS**, **AD User Domain**, **AD User Net BIOS Name Host** attributes in the screenshot provides additional context around the host and user identities.

## Locations Panel

The location panel provides insight into attempted by failures by NAD location type and provides a drill-down based on Locations.

Step 1 Go to **Cisco ISE pxGrid > Failed Authentications**.

Step 2 Go to **Location > All > All Location**.



The **IP Address**, **Calling Station ID**, **Username** attributes provide basic information for end users associated with failure reasons.

Data For : All Locations

Show  entries EXPORT

ID	Dev Time	IP Address	Failure Reason	Username	Server Name	Authentication Protocol	Device Type	Location	Calling Station ID
1619632837049798	12-May-2021 04:12:45.480 GMT+5:30	21.0.0.1	22040 Wrong password or invalid shared secret	ScaleUser1	ciscoisepripsn	PAP_ASCII	All Device Types	All Locations	95:70:28:E4:00:00
1619632837049799	12-May-2021 04:12:45.505 GMT+5:30	21.0.0.2	22040 Wrong password or invalid shared secret	ScaleUser2	ciscoisepripsn	PAP_ASCII	All Device Types	All Locations	95:70:28:E4:00:01
1619632837049800	12-May-2021 04:12:45.529 GMT+5:30	21.0.0.3	22040 Wrong password or invalid shared secret	ScaleUser3	ciscoisepripsn	PAP_ASCII	All Device Types	All Locations	95:70:28:E4:00:02

The **Server Name**, **Authentication Protocol**, **Device Type**, **Location**, **Calling Station ID**, **NAS IP Address**, **NAS Port ID**, **NAS Port Type** attributes provide more authentication details and location information of failed authentication attempts.

Data For : All Locations ✕

Show  entries EXPORT

NAS IP Address	NAS Port ID	NAS Port Type	MAC Address	Message Code	User Type	Access Service	Identity Store	Authentication Method	Service Type	Credential Check	AD Norm
1.1.1.1	GigabitEthernet1_7	Ethernet	None	5400	User	Default Network Access	Internal Users	PAP_ASCII	None	PAP_ASCII	None
1.1.1.1	GigabitEthernet1_7	Ethernet	None	5400	User	Default Network Access	Internal Users	PAP_ASCII	None	PAP_ASCII	None
1.1.1.1	GigabitEthernet1_7	Ethernet	None	5400	User	Default Network Access	Internal Users	PAP_ASCII	None	PAP_ASCII	None

The **AD Host/User Resolved Identities**, **AD Host/User Resolved DNS**, **AD User Domain**, and **AD User Net BIOS Name Host** attributes in the following screenshots provide additional context around the host and user identities.

Data For : All Locations ✕

Show  entries EXPORT

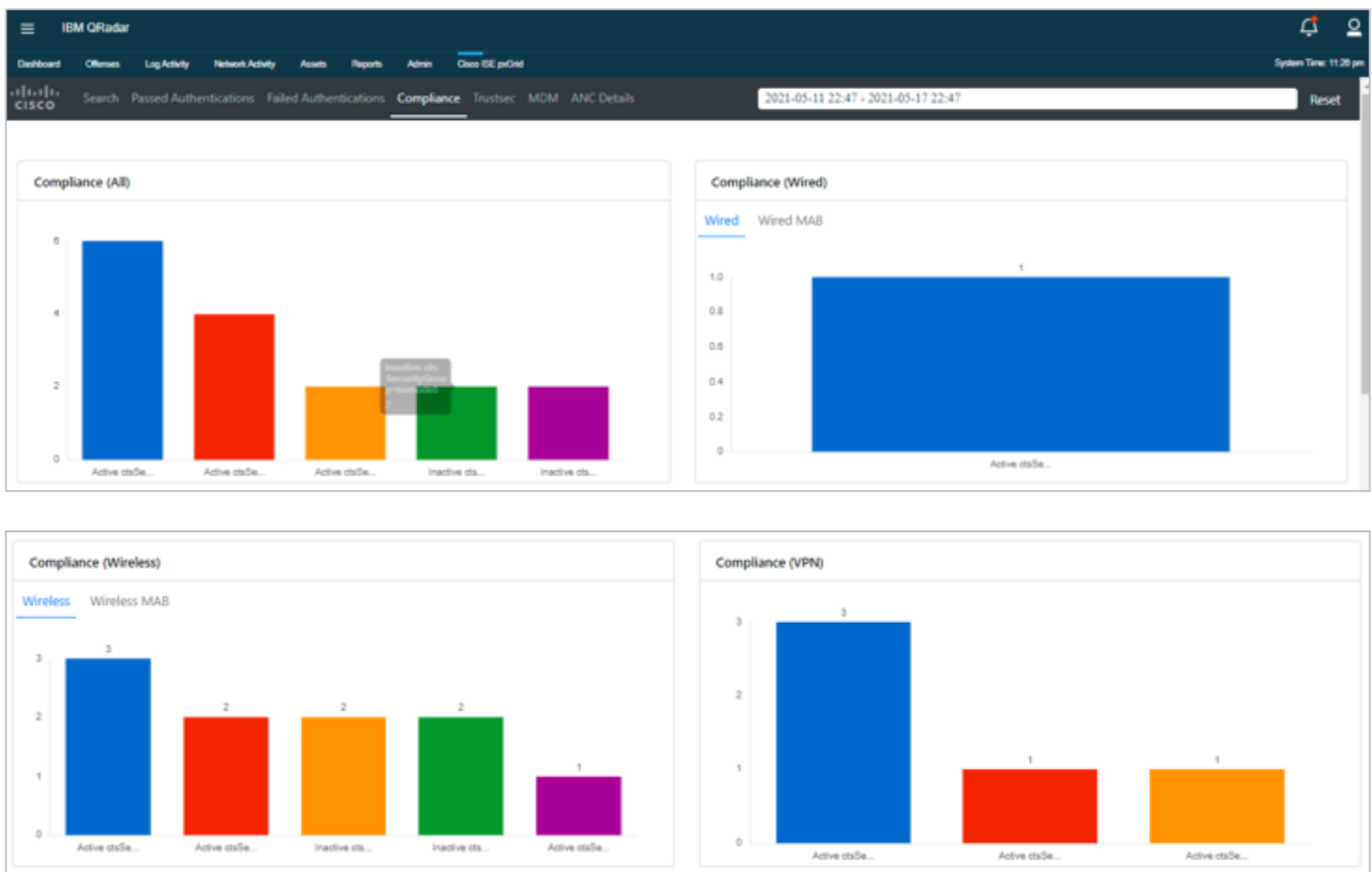
AD Host Domain Name	AD Host NetBios Name	AD Host Resolved Identities	AD Host Resolved DNS	AD User Domain Name	AD User Net Bios Name	AD User Resolved Identities	AD User Resolved DNS
None	None	None	None	None	None	None	None
None	None	None	None	None	None	None	None
None	None	None	None	None	None	None	None

## Compliance

The Compliance Dashboard provides the admin with ISE posture compliant or non-compliant devices across the organization or by wired or wireless connection type. The organization may have security policy for their employees such as ensuring that AV DAT files are up-to-date and AV services must be running for compliance. If either of these are not the case, then the end user is deemed non-compliance.

Step 1 Go to **Cisco pxGrid > Compliance (All)**.

Step 2 Go to **Compliant**.



You will see a list of compliant end users along with the associated contextual information.

The **IP address**, **MAC address**, **Username**, **Calling Station ID** and **Posture Status** attributes provide the basic user information. The **NAS Port ID**, **NAS Port Type**, **NAS IP Address** attributes contain the location and connection-type information. The **State attribute** determines the Postured Status.

Data For : Compliant X

Show 10 entries EXPORT

Dev Time	IP Address	State	MAC Address	Username	Calling Station ID	Called StationID	NAS IP Address	NAS Port ID	NAS Po
18-Feb-2018 10:17:19.596 EST	192.168.1.15	POSTURED	00:50:56:86:8B:13	pxgrid1	00:50:56:86:8B:13	50:3D:E5:C4:05:8B	192.168.1.3	GigabitEthernet1/0/11	Ethernet
18-Feb-2018 10:17:19.596 EST	192.168.1.15	POSTURED	00:50:56:86:8B:13	pxgrid1	00:50:56:86:8B:13	50:3D:E5:C4:05:8B	192.168.1.3	GigabitEthernet1/0/11	Ethernet
18-Feb-2018 10:17:23.533 EST	192.168.1.15	STARTED	00:50:56:86:8B:13	pxgrid1	00:50:56:86:8B:13	50:3D:E5:C4:05:8B	192.168.1.3	GigabitEthernet1/0/11	Ethernet

The **Posture Status** attribute contains the value of the posture status, compliant, non-compliance, and pending.

The **Endpoint Profile** attribute is the device information of the end user along with the **Endpoint Operating System** attribute.

NAS Identifier	Posture Status	Endpoint Profile	Endpoint Operating System	Group ID	AD Normalized User	AD Host Domain Name
	Compliant	Windows7-Workstation	Windows 7		pxgrid1	
	Compliant	Microsoft-Workstation	Windows 7 Professional 64-bit		pxgrid1	
	Compliant	Microsoft-Workstation	Windows 7 Professional 64-bit		pxgrid1	

The **AD Username/Host** and **AD Resolved Username/Host identity** attributes provide a consistent way of providing the username and hostname despite various EAP authentication types.

AD Host NetBios Name	AD Host Resolved Identities	AD Host Resolved DNS	AD User Domain Name	AD User Net Bios Name	AD User Resolved Identities
	WIN7-PC3\$@lab10.com			LAB10	pxGrid1@lab10.com
	WIN7-PC3\$@lab10.com			LAB10	pxGrid1@lab10.com
	WIN7-PC3\$@lab10.com			LAB10	pxGrid1@lab10.com

The **Is Machine Authentication** attribute if set to "true" denotes that this is machine authentication. If set to "false" denotes user authentication.

AD User Resolved DNS	Terminal Server Agent ID	Is Machine Authentication	Service Type	Tunnel Private Group ID	Airespace WLAN ID
CN=pxGrid1,CN=Users,...		false	Framed		
		false	Framed		
		false	Framed		



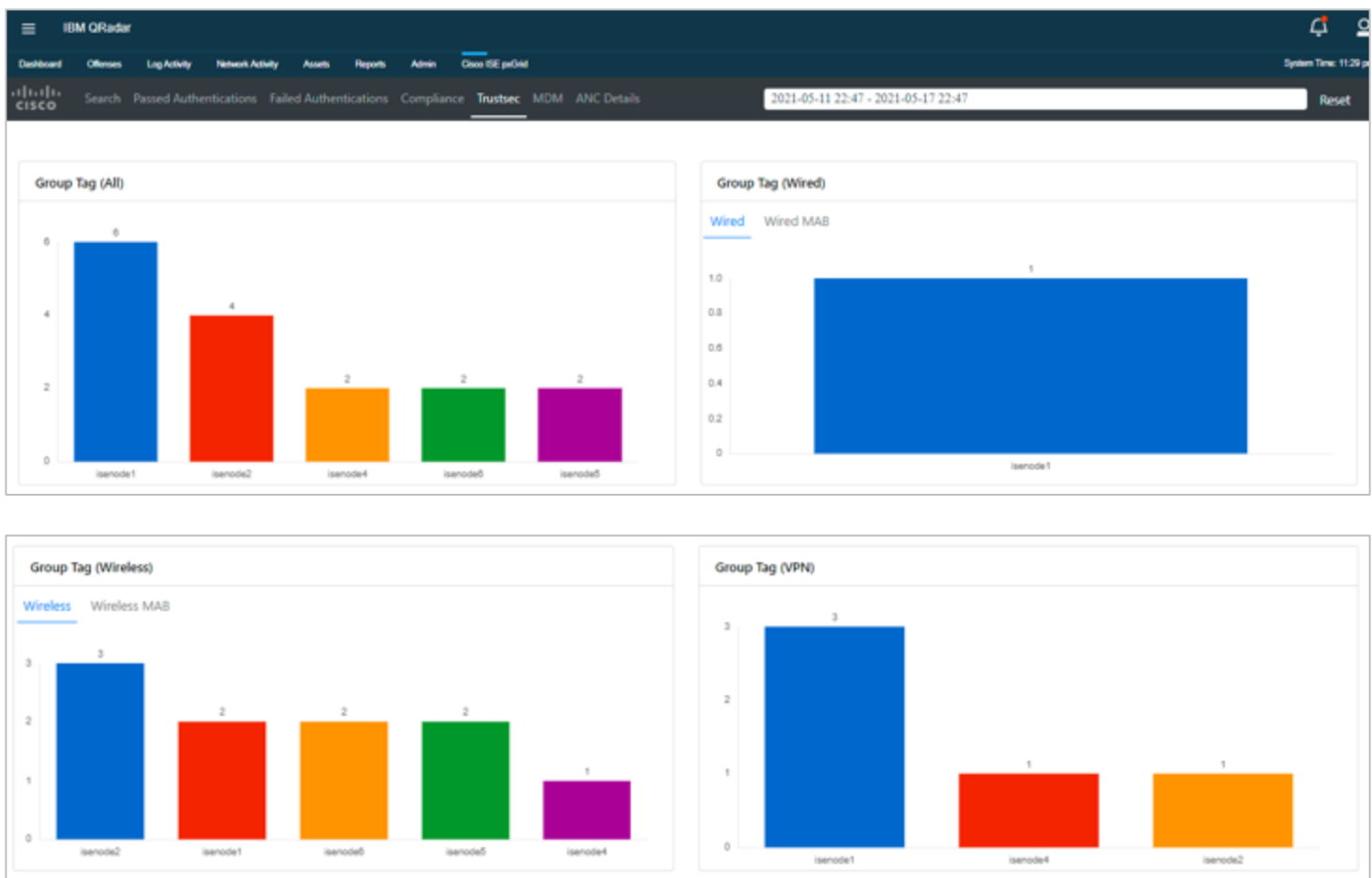
## TrustSec

The TrustSec dashboard contains the Security Group Tag (SGT) Information for assigned end users. This provides the admin with visibility to see which end user is associated with a SGT. For example, a SGT of Quarantined Systems, will provide a view of end users who have been assigned this label.

Step 1 Go to Cisco ISE pxGrid > Trustsec.

Step 2 Select Group Tag (All.)

Step 3 Select Quarantined Systems.



This provides the end-user information associated with the SGT. Here we see the **Username**, **IP Address**, and **MAC Address** attributes. We also see the **NAS IP Address**, **NAS Port ID**, and **NAS Port type** attributes to determine the location and connection type.

Dev Time	IP Address	State	MAC Address	Username	Calling Station ID	Called StationID	NAS IP Address	NAS Port ID
22-Feb-2018 04:42:41.022 EST	192.168.1.37	STARTED	00:0C:29:C1:7B:2C	LAB10\pxgrid2	00:0C:29:C1:7B:2C	50:3D:E5-C4:05-8B	192.168.1.3	GigabitEthernet1/0/11
22-Feb-2018 04:59:19.938 EST	192.168.1.37	DISCONNECTED	00:0C:29:C1:7B:2C	LAB10\pxgrid2	00:0C:29:C1:7B:2C	50:3D:E5-C4:05-8B	192.168.1.3	GigabitEthernet1/0/11

This also provides the **Endpoint Profile**, **Endpoint Operating System** and **AD normalized user/host names** and **AD user/host FQDN identities** attributes.

NAS Port Type	NAS Identifier	Posture Status	Endpoint Profile	Endpoint Operating System	Group ID	AD Normalized User	AD Host Domain Name
Ethernet			Windows7-Workstation	Windows 7 Professional		pxgrid2	
Ethernet			Windows7-Workstation	Windows 7 Professional		pxgrid2	

The **AD Username/Host** and **AD Resolved Username/Host identity** attributes provide a consistent way of providing the username and hostname despite various EAP authentication types.

AD Host NetBios Name	AD Host Resolved Identities	AD Host Resolved DNS	AD User Domain Name	AD User Net Bios Name	AD User Resolved Identities
	PXGRID2-PC\$			LAB10	
	PXGRID2-PC\$			LAB10	

The **Is Machine Authentication** attribute if set to "true" denotes that this is machine authentication. If set to "false" denotes user authentication.

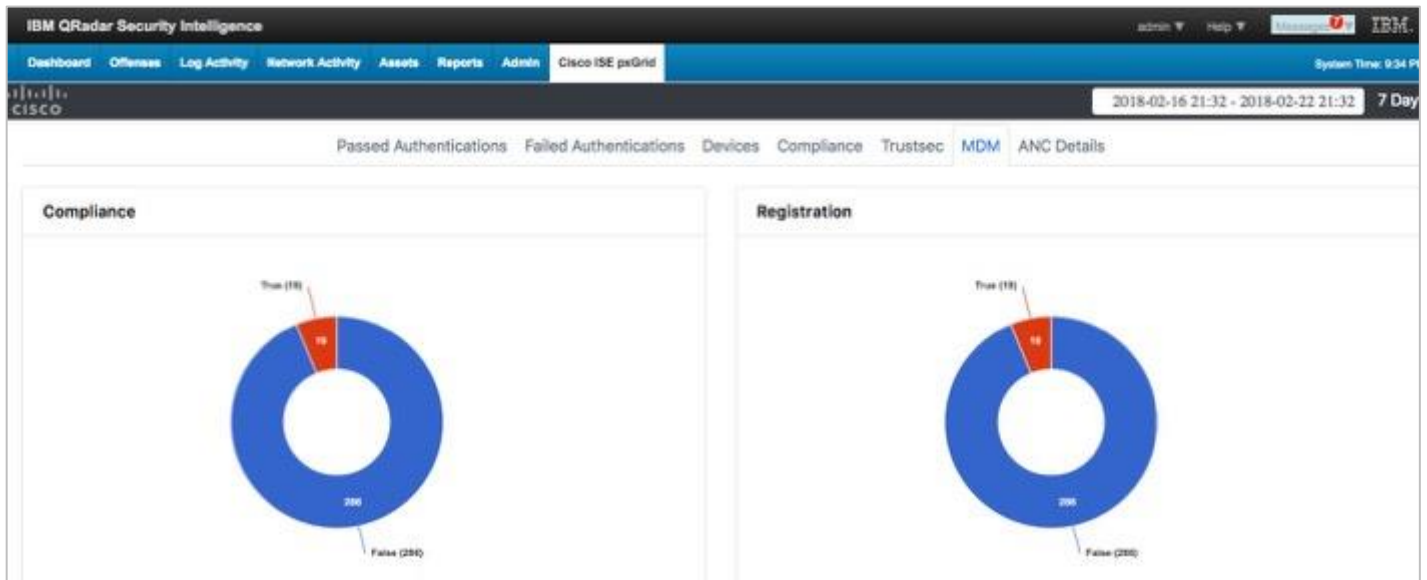
Terminal Server Agent ID	Is Machine Authentication	Service Type	Tunnel Private Group ID	Airespace WLAN ID	Network Device Profile Name
	false	Framed			Cisco
	false	Framed			Cisco

## Mobile Device Management (MDM)

The MDM Dashboard provides the admin with the visibility to look into an organizations MDM security policy. In the ISE 2.4 initial release, only the registration and compliance status are available.

Step 1 Go to **Cisco ISE pxGrid > MDM**.

Step 2 Select **Compliance**.



The **Username, MAC Address, IP Address** and **Registration** and **Compliance Status** attribute are available.

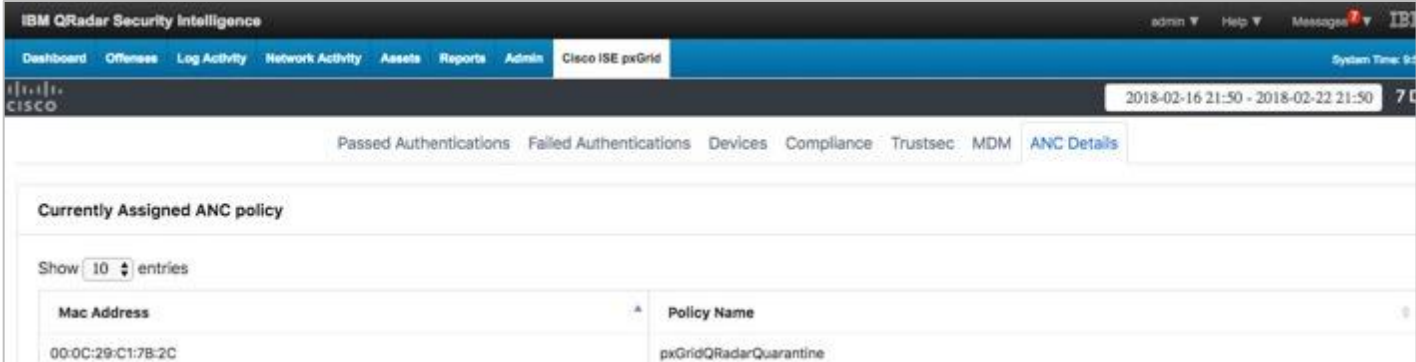
Note: It is assumed that MDM is already configured in ISE. In this example, Cisco Meraki is used.

Username ^	MAC Address	IP Address	MDM MAC Address	OS Version	Registration Status	Compliance Status	Model	Manufacturer	UDID	Serial Nur
pxgrid1	88:CB-87:ED:45:DA	192.168.1.11			True	True				
pxgrid1	88:CB-87:ED:45:DA	192.168.1.11			True	True				

## ANC Details

The ANC Details Dashboard View provides visibility into the ANC policies currently assigned to endpoints MAC address.

Step 1 Go to **Cisco ISE pxGrid > ANC Details**.



The screenshot displays the IBM QRadar Security Intelligence interface. The top navigation bar includes 'Dashboard', 'Offenses', 'Log Activity', 'Network Activity', 'Assets', 'Reports', 'Admin', and 'Cisco ISE pxGrid'. The 'ANC Details' tab is selected. Below the navigation, there are tabs for 'Passed Authentications', 'Failed Authentications', 'Devices', 'Compliance', 'Trustsec', 'MDM', and 'ANC Details'. The main content area shows 'Currently Assigned ANC policy' with a 'Show 10 entries' dropdown. A table lists the following data:

Mac Address	Policy Name
00:0C:29:C1:7B:2C	pxGridQRadarQuarantine

## Configuring Cisco ISE Adaptive Network Control Policies

Cisco ISE Adaptive Network Control (ANC) Policies provide a means of enforcing an organization's security policy by issuing a quarantine, port-bounce, or port-shut on the endpoint. When an endpoint is quarantined, this issues a Change of Authorization (CoA) and the endpoint is quarantined due to the organization's security policy. The security policy may be just to monitor the traffic and take no action. In this case, a Security Group Tag (SGT) can be assigned. SGT are part of the Cisco TrustSec Solution and is used here for assigning labels to an organization's security policy. As an example, Quarantined System SGT will be applied to an ANC quarantine policy to monitor and not enforce network access.

Port-bounce will bounce the port the endpoint is connected, and user will be re-authenticated.

Port-shut will issue a shutdown on the port the endpoint is connected. This is the most severe and may be issued if the endpoint is infected with malware and the malware is in suspect of propagating over file shares.

These ISE ANC policies will be used by the Cisco ISE pxGrid app to enforce mitigation actions on the endpoints from either the Dashboard and Panels or through IBM QRadar system syslog events as long as the endpoint has been authenticated through ISE.

The following Cisco ISE ANC policies will be created:

- pxGridQRadarQuarantine - issues a quarantine
- pxGridQRadarPortBounce - issues a port-bounce
- pxGridQRadarShutDown - issues a shut down

The Cisco ISE pxGrid app will read in the existing ISE ANC policies; however, these default ANC policies need to be configured first. Also, the Cisco ISE pxGrid app pxGrid client will need to be added to the pxGrid ANC Group. You will perform this exercise later, when configuring the Cisco ISE pxGrid for pxGrid integration.

## Configuring Default ANC policies for Cisco ISE pxGrid App

**Note:** When you setup the QRadar, pxGrid app will automatically create default ANC policies if they don't exist. These policies shown in the paragraph about are hard coded and cannot be edited. If you have other policies, you will need to integrate them manually on ISE. These policies are populated after you submit and test the pxGrid app settings in QRadar.

**Step 1** Go to **Operations > Adaptive Network Control > Policy List > Add > The following for the Policy Name and Action:**

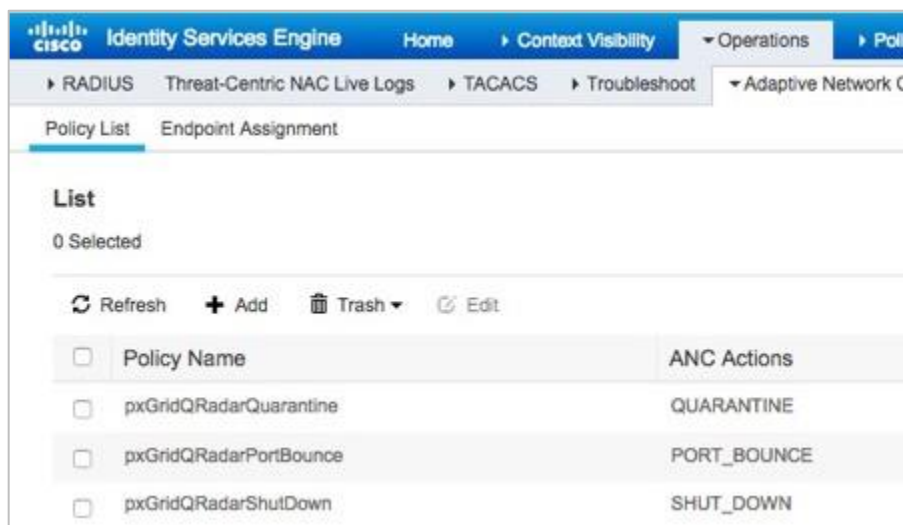
pxGridQRadarQuarantine, QUARANTINE

pxGridQRadarPortBounce, PORT\_BOUNCE

pxGridQRadatShutDown, SHUT\_DOWN,

**Step 2** Select **Save**.

After **Policy Name** and associated action, you should see the following:



Policy Name	ANC Actions
<input type="checkbox"/> pxGridQRadarQuarantine	QUARANTINE
<input type="checkbox"/> pxGridQRadarPortBounce	PORT_BOUNCE
<input type="checkbox"/> pxGridQRadarShutDown	SHUT_DOWN

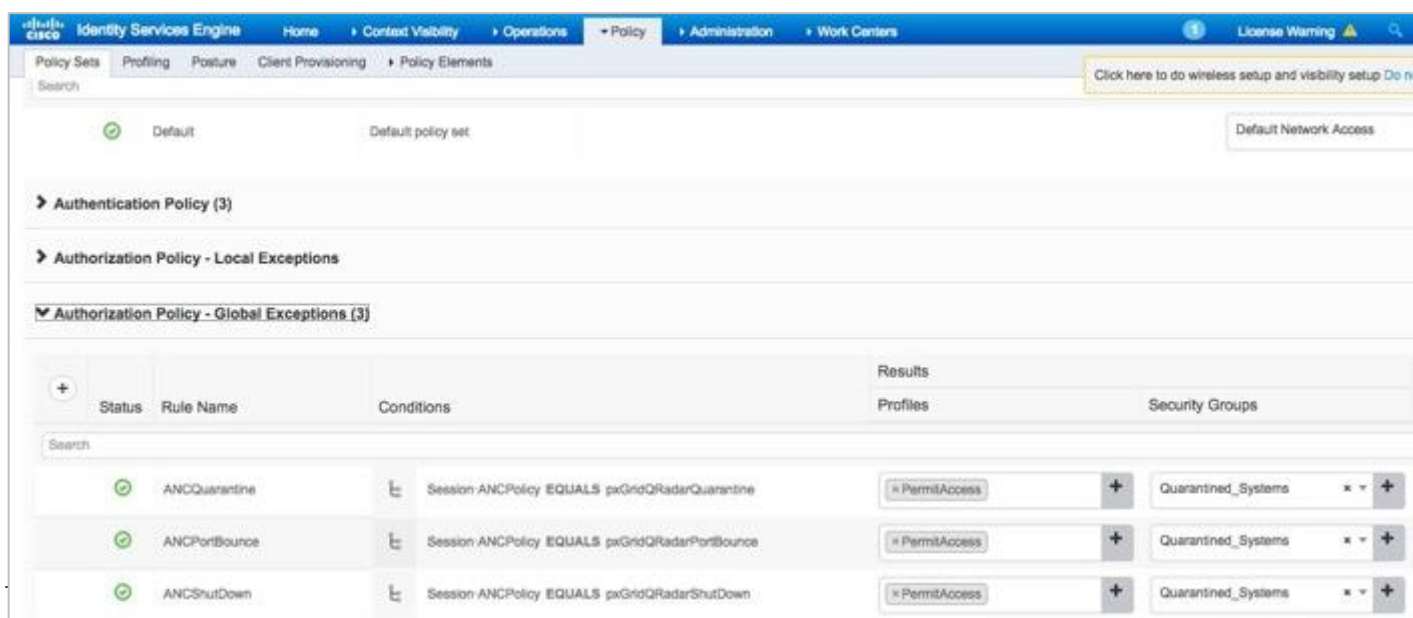
## Adding ANC Policies to ISE Policy Sets

- Step 1 Go to **Policy > Policy Sets > Default > ">" > Authorization Policy > Global Exceptions > "+"**.
- Step 2 Under **Rule Name**, type: **ANC Quarantine**.
- Step 3 Under **Conditions**, select **">"**.
- Step 4 To close the introductory screen, select **"x"**.
- Step 5 Under **Dictionary**, select **Session > ANCPolicy > Equals > pxGridQRadarQuarantine**.
- Step 6 Select **Use**.
- Step 7 Under **Profiles**, select **Permit Access**.
- Step 8 Under **Security Groups**, select **Quarantine\_Systems**.
- Step 9 Select **Save**.
- Step 10 Perform steps 1-9 for the Rule Name ANCShutDown and ANCPolicy pxGridQRadarShutDown.
 

Note: You can also click on the Gear and duplicate line below and add the rule name and ANCPolicy.
- Step 11 Perform steps 1-9 for the Rule Name ANCPortBounce and ANCPolicy pxGridQRadarPorBounce.
 

Note: You can also click the Gear icon and duplicate line below and add the rule name and ANCPolicy.

You should see the following:

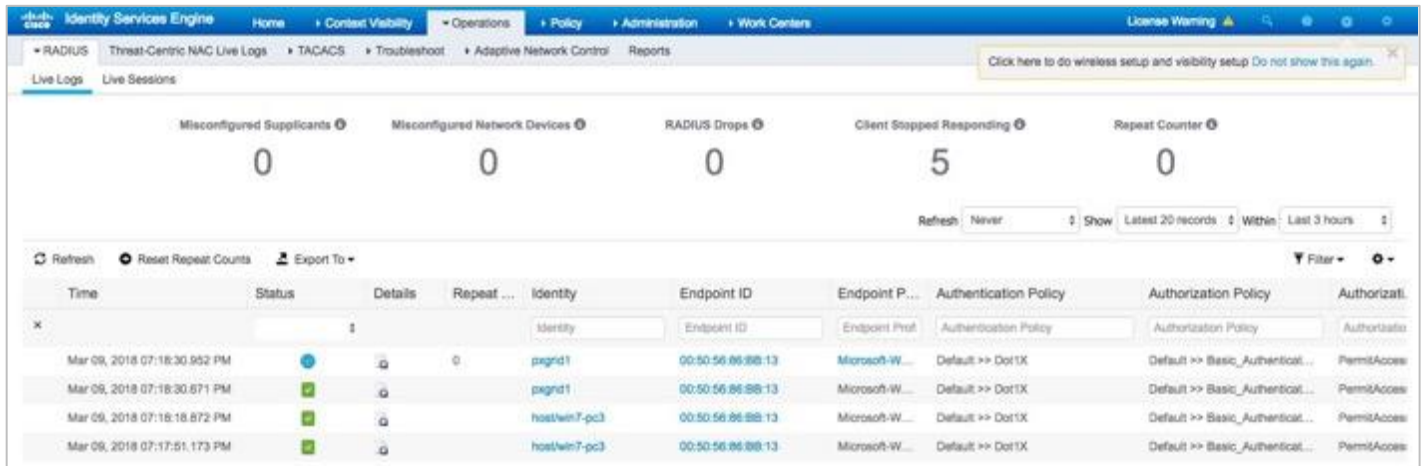


Cisco Identity Services Engine						
Policy						
Authorization Policy - Global Exceptions (3)						
	Status	Rule Name	Conditions	Profiles	Security Groups	
+	✔	ANCQuarantine	Session ANCPolicy EQUALS pxGridQRadarQuarantine	PermitAccess	Quarantine_Systems	+
	✔	ANCPortBounce	Session ANCPolicy EQUALS pxGridQRadarPorBounce	PermitAccess	Quarantine_Systems	+
	✔	ANCShutDown	Session ANCPolicy EQUALS pxGridQRadarShutDown	PermitAccess	Quarantine_Systems	+

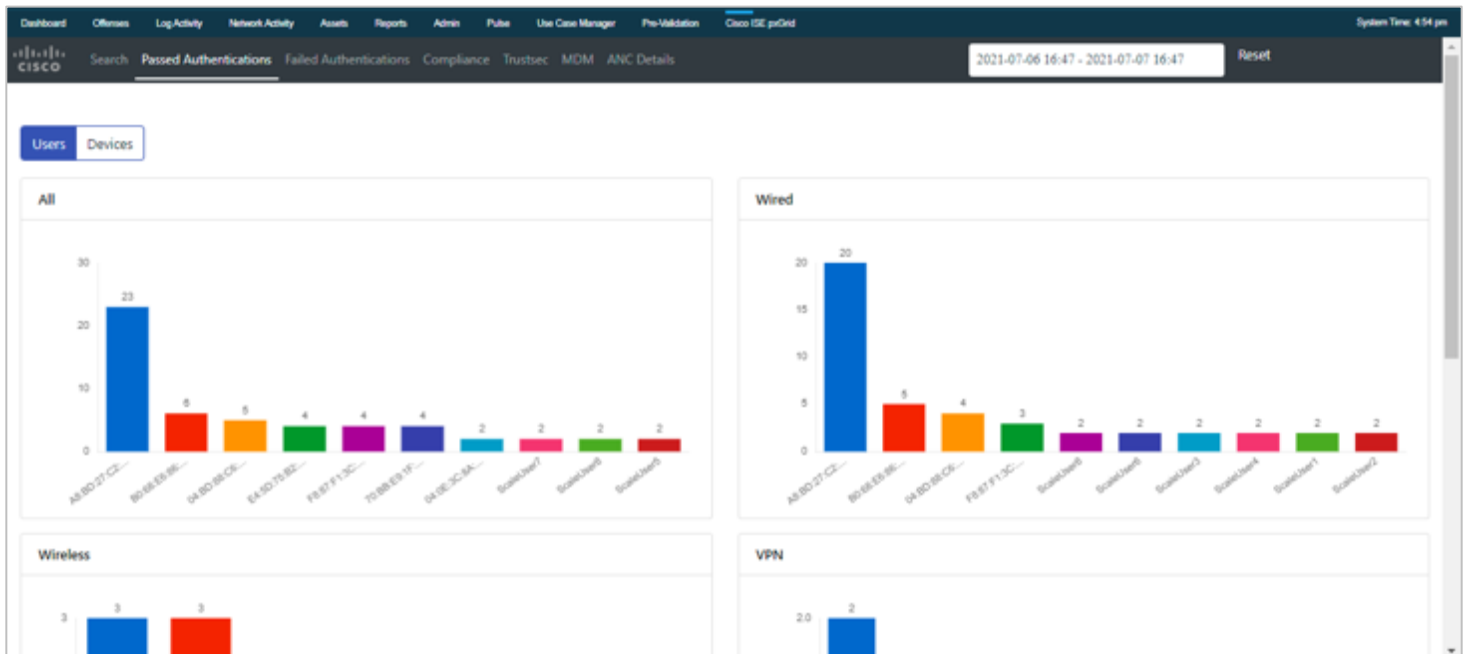
# Performing Cisco ISE ANC Mitigation Actions Through Cisco ISE pxGrid App Dashboard Panel

This section steps the reader through performing ANC mitigation actions on the endpoint from the dashboards and panels.

Step 1 User pxGrid1 authenticates in ISE.



Step 2 Go to Cisco ISE pxGrid > Passed Authentications.





Step 3 Select an end user, ScaleUser7, and then see the following:

Data For : ScaleUser7

Show 10 entries

Dev Time	IP Address	State	MAC Address	Username	Calling Station ID	Called StationID	NAS IP Address	NAS Port ID	NAS Port Type	NAS Identifier	Posture Stat
06-Jul-2021 09:46:19.274 GMT+5:30	21.0.0.15	STARTED	95:70:28:E4:00:06	ScaleUser7	95:70:28:E4:00:06	None	1.1.1.1	GigabitEthernet1_7	Ethernet	None	None
06-Jul-2021 09:46:19.274 GMT+5:30	21.0.0.15	STARTED	95:70:28:E4:00:06	ScaleUser7	95:70:28:E4:00:06	None	1.1.1.1	GigabitEthernet1_7	Ethernet	None	None

Showing 1 to 2 of 2 entries

Step 4 Right-click on the IP address, and then see the ANC policies:

Data For : ScaleUser18

Show 10 entries

ID	Dev Time	IP Address	Failure Reason	Username	Server Name	Authentication Protocol	Device Type	Location	Calling Station ID
1614089477942030	15-Mar-2021 09:03:04.892 GMT+5:30	21.0.0.18	pxGridQRadarShutDown	ScaleUser18	ciscoiseprism	PAP_ASCII	All Device Types	All Locations	95:70:28:E4:00:11
1614089477942030	15-Mar-2021 09:03:04.892 GMT+5:30	21.0.0.18	policy_demoj-09	ScaleUser18	ciscoiseprism	PAP_ASCII	All Device Types	All Locations	95:70:28:E4:00:11
1614089477942030	15-Mar-2021 09:03:04.892 GMT+5:30	21.0.0.18	pxGridQRadarPortBounce	ScaleUser18	ciscoiseprism	PAP_ASCII	All Device Types	All Locations	95:70:28:E4:00:11

Step 5 Select pxGridQRadarPortBounced.

Step 6 You should see a successful status message:

192.168.0.250 says  
Status: RUNNING  
Operation Id: ciscoiseprism.aujas-blr.local:95

Data For : ScaleUser7

Show 10 entries

Dev Time	IP Address	State	MAC Address	Username	Calling Station ID	Called StationID	NAS IP Address	NAS Port ID	NAS Port Type	NAS Identifier	Posture Stat
06-Jul-2021 09:46:19.274 GMT+5:30	21.0.0.15	STARTED	95:70:28:E4:00:06	ScaleUser7	95:70:28:E4:00:06	None	1.1.1.1	GigabitEthernet1_7	Ethernet	None	None
06-Jul-2021 09:46:19.274 GMT+5:30	21.0.0.15	STARTED	95:70:28:E4:00:06	ScaleUser7	95:70:28:E4:00:06	None	1.1.1.1	GigabitEthernet1_7	Ethernet	None	None

Showing 1 to 2 of 2 entries

Step 7 Select OK.

Step 8 To view in ISE, select **Operations > RADIUS LiveLogs**.

Based on the ANCQuarantine Policy, the endpoint has been quarantined:

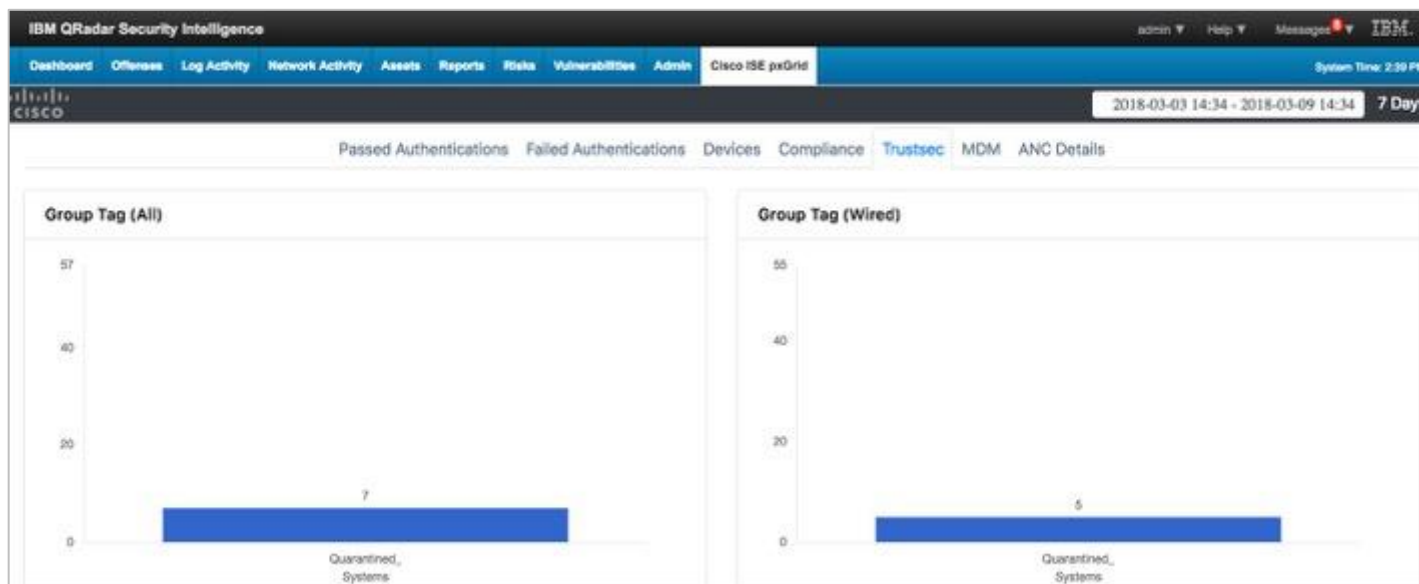
Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorizati
Mar 09, 2018 07:29:29.602 PM	Quarantined		0	pxgrid1	00:50:56:86:8B:13	Microsoft-W...	Default >> Dot1X	Default >> ANCQuarantine	Quarantined
Mar 09, 2018 07:29:29.506 PM	Quarantined			pxgrid1	00:50:56:86:8B:13	Microsoft-W...	Default >> Dot1X	Default >> ANCQuarantine	Quarantined
Mar 09, 2018 07:29:28.709 PM	Quarantined				00:50:56:86:8B:13				

Step 9 To view the quarantine details in the Cisco ISE pxGrid App ANC Dashboard, go to **Cisco ISE pxGrid > ANC Details**.

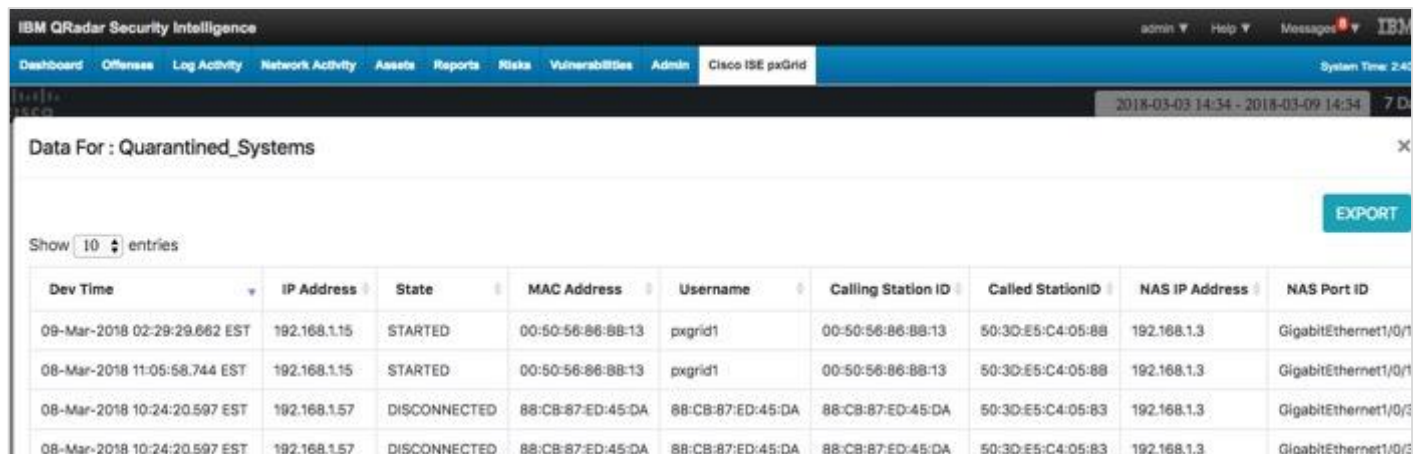
See an example of the MAC Address of the quarantined endpoint:

Mac Address	Policy Name
88:B1:11:EF:F8:12	pxGridQRadarPortBounce
95:70:2B:E4:00:05	policy_demojlc-09
95:70:2B:E4:00:06	pxGridQRadarPortBounce
95:70:2B:E4:00:07	test_ui
95:70:2B:E4:00:08	testaddition
A8:BD:27:C2:61:DC	pxGridQRadarPortBounce
F8:87:F1:3C:58:9E	pxGridQRadarPortBounce

Step 10 To view the details in the Cisco ISE pxGrid App TrustSec Dashboard, go to **Cisco ISE pxGrid > Trusts**.



Step 11 To see the quarantined endpoints, select **Quarantined\_Systems**:



The screenshot shows the 'Data For: Quarantined\_Systems' view in the Cisco ISE pxGrid TrustSec Dashboard. It includes a table with columns for Dev Time, IP Address, State, MAC Address, Username, Calling Station ID, Called Station ID, NAS IP Address, and NAS Port ID. There are four rows of data. An 'EXPORT' button is visible in the top right corner of the table area.

Dev Time	IP Address	State	MAC Address	Username	Calling Station ID	Called Station ID	NAS IP Address	NAS Port ID
09-Mar-2018 02:29:29.662 EST	192.168.1.15	STARTED	00:50:56:86:8B:13	pxgrid1	00:50:56:86:8B:13	50:3D:E5:C4:05:8B	192.168.1.3	GigabitEthernet1/0/1
08-Mar-2018 11:05:58.744 EST	192.168.1.15	STARTED	00:50:56:86:8B:13	pxgrid1	00:50:56:86:8B:13	50:3D:E5:C4:05:8B	192.168.1.3	GigabitEthernet1/0/1
08-Mar-2018 10:24:20.597 EST	192.168.1.57	DISCONNECTED	88:CB:87:ED:45:DA	88:CB:87:ED:45:DA	88:CB:87:ED:45:DA	50:3D:E5:C4:05:83	192.168.1.3	GigabitEthernet1/0/3
08-Mar-2018 10:24:20.597 EST	192.168.1.57	DISCONNECTED	88:CB:87:ED:45:DA	88:CB:87:ED:45:DA	88:CB:87:ED:45:DA	50:3D:E5:C4:05:83	192.168.1.3	GigabitEthernet1/0/3

Step 12 To un-quarantine or clear the endpoint either in the Dashboards or directly in ISE. The endpoint will be un-quarantined from this view.

Step 13 Right-click on the MAC Address:

Data For : ScaleUser7

Show 10 entries

Dev Time	IP Address	State	MAC Address	Username	Calling Station ID	Called StationID	NAS IP Address	NAS Port ID	NAS Port Type	NAS Identifier	Posture Statu
06-Jul-2021 09:46:19.274 GMT+5:30	21.0.0.15	STARTED	95:70:2B:E4:00:06	ScaleUser7	95:70:2B:E4:00:06	None	1.1.1.1	GigabitEthernet1,7	Ethernet	None	None
06-Jul-2021 09:46:19.274 GMT+5:30	21.0.0.15	STARTED	95:70:2B:E4:00:06	ScaleUser7	95:70:2B:E4:00:06	None	1.1.1.1	GigabitEthernet1,7	Ethernet	None	None

Showing 1 to 2 of 2 entries

Step 14 Select pxGridQRadarClear.

Step 15 You should see successful status message:

192.168.0.250 says  
Status : SUCCESS  
Operation Id : ciscoisepripsn.aujas-blr.local96

OK

Data For : ScaleUser7

Show 10 entries

Dev Time	IP Address	State	MAC Address	Username	Calling Station ID	Called StationID	NAS IP Address	NAS Port ID	NAS Port Type	NAS Identifier	Posture Statu
06-Jul-2021 09:46:19.274 GMT+5:30	21.0.0.15	STARTED	95:70:2B:E4:00:06	ScaleUser7	95:70:2B:E4:00:06	None	1.1.1.1	GigabitEthernet1,7	Ethernet	None	None
06-Jul-2021 09:46:19.274 GMT+5:30	21.0.0.15	STARTED	95:70:2B:E4:00:06	ScaleUser7	95:70:2B:E4:00:06	None	1.1.1.1	GigabitEthernet1,7	Ethernet	None	None

Showing 1 to 2 of 2 entries

Step 16 Select OK.

Step 17 To un-quarantine the endpoints and view the results in ISE, go to **Operations > RADIUS > Live Logs**.

Identity Services Engine

Home Context Visibility Operations Policy Administration Work Centers

RADIUS Threat-Centric NAC Live Logs TACACS Troubleshoot Adaptive Network Control Reports

Click here to do wireless setup and visibility setup Do not show this again.

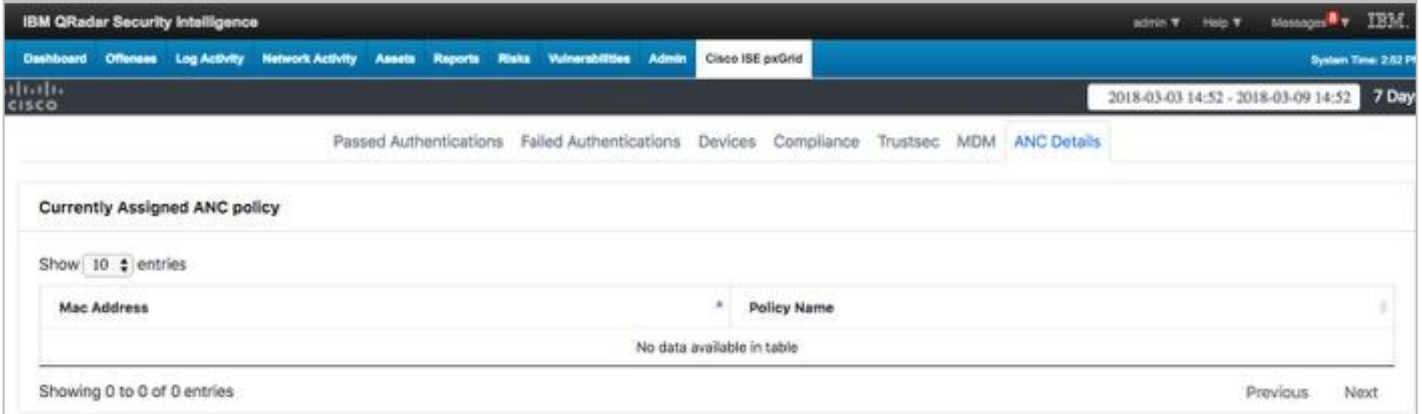
Live Logs Live Sessions

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 0 Client Stopped Responding 5 Repeat Counter 0

Refresh Never Show Latest 20 records Within Last 3 hours

Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorizati
Mar 09, 2018 07:48:43.693 PM	Success	q	0	pxgrid1	00:50:56:86:8B:13	Microsoft-W...	Default >> Dot1X	Default >> Basic_Authentico...	PermiAcces
Mar 09, 2018 07:48:42.916 PM	Success	q	0	pxgrid1	00:50:56:86:8B:13	Microsoft-W...	Default >> Dot1X	Default >> Basic_Authentico...	PermiAcces
Mar 09, 2018 07:45:52.604 PM	Success	q	0	pxgrid1	00:50:56:86:8B:13	Microsoft-W...	Default >> Dot1X	Default >> Basic_Authentico...	PermiAcces

Step 18 Go to **Cisco ISE pxGrid > ANC Details**, you should see the endpoint is no longer assigned to the ANC policy:



IBM QRadar Security Intelligence

admin Help Messages IBM

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin Cisco ISE pxGrid System Time: 2:02 PM

2018-03-03 14:52 - 2018-03-09 14:52 7 Day

Passed Authentications Failed Authentications Devices Compliance Trustsec MDM ANC Details

Currently Assigned ANC policy

Show: 10 entries

Mac Address	Policy Name
No data available in table	

Showing 0 to 0 of 0 entries Previous Next

Note: To un-quarantine or clear in ISE: go to **Operations > Adaptive Network Control > Endpoint Assignment > Select the endpoint MAC address > Tras.**

## Configuring IBM QRadar for Cisco ISE Syslog Events

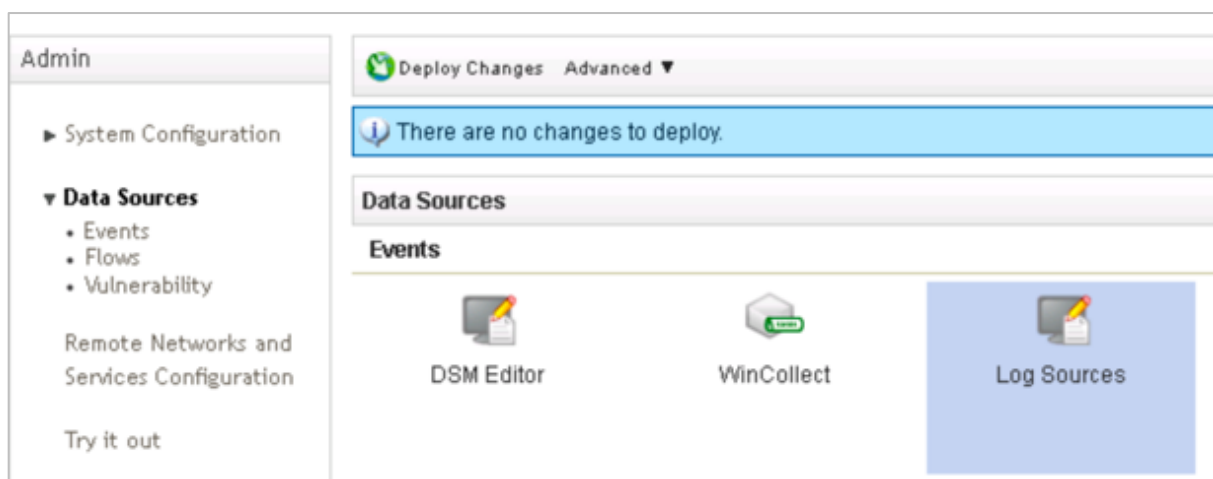
The IBM Device Support Module (DSM) for Cisco Identity Service Engine (ISE) Syslog is installed by default on QRadar. For more information on DSM (beyond the scope of this guide) visit the [DSM guide](#).

Note: Support of DSM comes from IBM Support, this information is added for your benefit but not supported by the ISE QRadar App Team

### Step 1 Configure log source on IBM QRadar.

Note: Configure both primary and secondary MNT log sources in an HA environment.

- a. Open the IBM QRadar Console.
- b. Go to **Admin > Data Sources > Log Sources**.

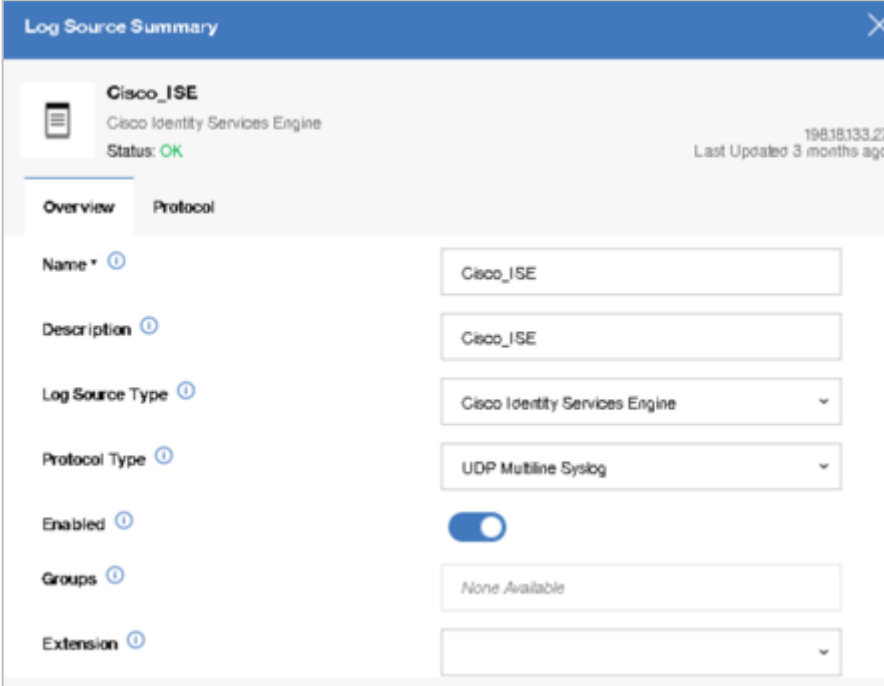


- c. Add in a new log source for Cisco ISE Syslog.

**Add a new log source > Single Source > Source Type: Identity Services Engine.**

- Log Source Name and Description: Cisco\_ISE
- Log Source Type Cisco Identity Services Engine
- Protocol Configuration: UDP Multiline Syslog
- Log Source Identifier: IP Address of your ISE MNT node(s)
- Listen port (leave default 517)
- Message ID Pattern: CISE\_\- Source Name Formatting String (researching)

Note: For version 7.3, there will be a single screen configuration.



The screenshot shows a configuration window titled "Log Source Summary" for a log source named "Cisco\_ISE". The window is divided into two tabs: "Overview" and "Protocol". The "Overview" tab is active, showing the following configuration details:

- Name:** Cisco\_ISE
- Description:** Cisco\_ISE
- Log Source Type:** Cisco Identity Services Engine
- Protocol Type:** UDP Multiline Syslog
- Enabled:** Yes (toggle switch is turned on)
- Groups:** None Available
- Extension:** (empty dropdown menu)

Additional information at the top right of the window includes the IP address "198.18.133.27" and the text "Last Updated 3 months ago". The status is indicated as "OK".

Note: For QRadar 7.4, this will open a new application window and will take you through a guided configuration.

- d. Select **Save** or **Finish**, close the new app window.
- e. Select **Deploy Changes > Deploy**.

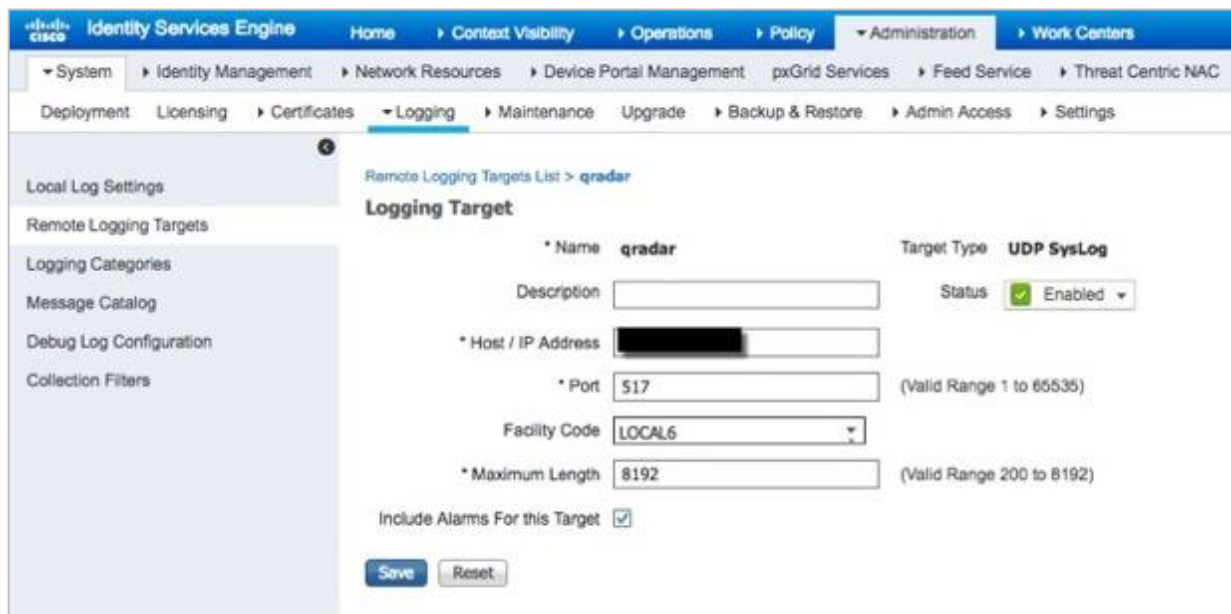
## Configuring Cisco ISE Syslog Events

Cisco ISE will be configured to send syslog information to the IBM QRadar instance. Please make sure you have the QRadar ISE DSM installed. Future releases of the QRadar ISE DSM will include ISE syslog events such as Framed IP Address, IP address, where you can take ANC mitigation actions on the endpoint.

Step 1 Go to **Administration > System > Logging > Remote Logging Targets**.

Step 2 Add in a new Remote logging target - **Host/IP address** of IBM QRadar instance:

- Port - non-default 517 (QRadar UDP multiline listening port)
- Maximum length of 8192 (to see complete logs instead of those truncated)
- Include alarms for this Target (checked)



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Administration > System > Logging > Remote Logging Targets. The page title is "Remote Logging Targets List > qradar". The main content area is titled "Logging Target" and contains the following configuration fields:

- \* Name: qradar
- Target Type: UDP SysLog
- Description: [Empty text box]
- Status:  Enabled
- \* Host / IP Address: [Redacted text box]
- \* Port: 517 (Valid Range 1 to 65535)
- Facility Code: LOCAL6
- \* Maximum Length: 8192 (Valid Range 200 to 8192)
- Include Alarms For this Target:

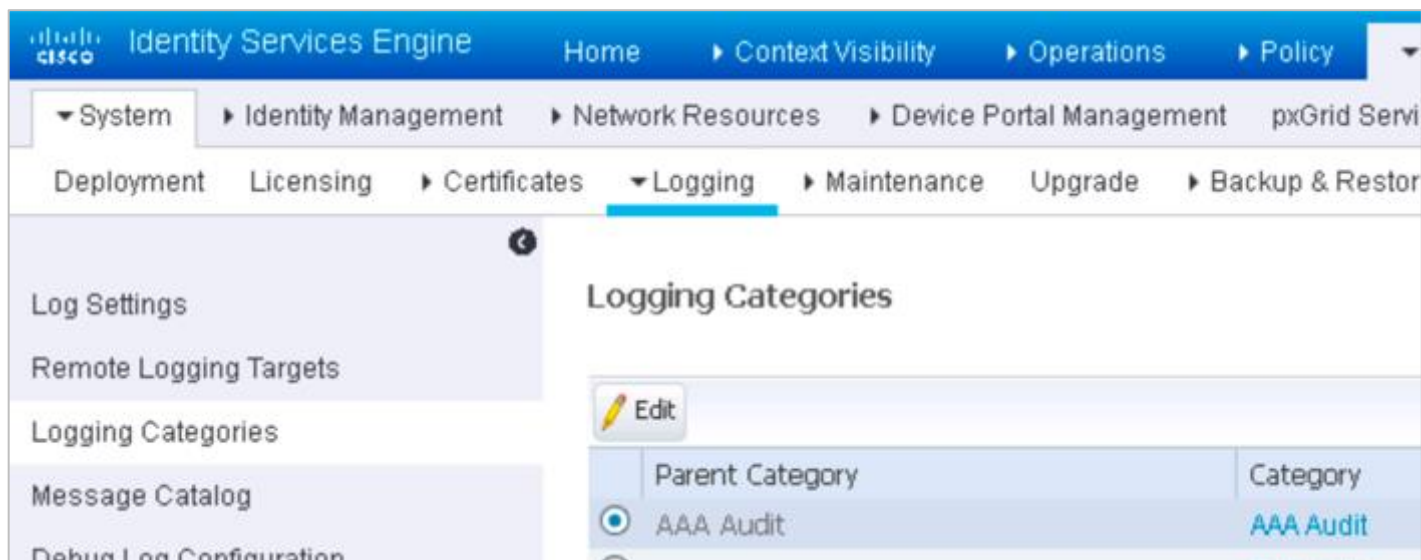
At the bottom of the form are "Save" and "Reset" buttons.

Step 3 Select **Submit/Save**.

Step 4 Configure **Logging Categories**:

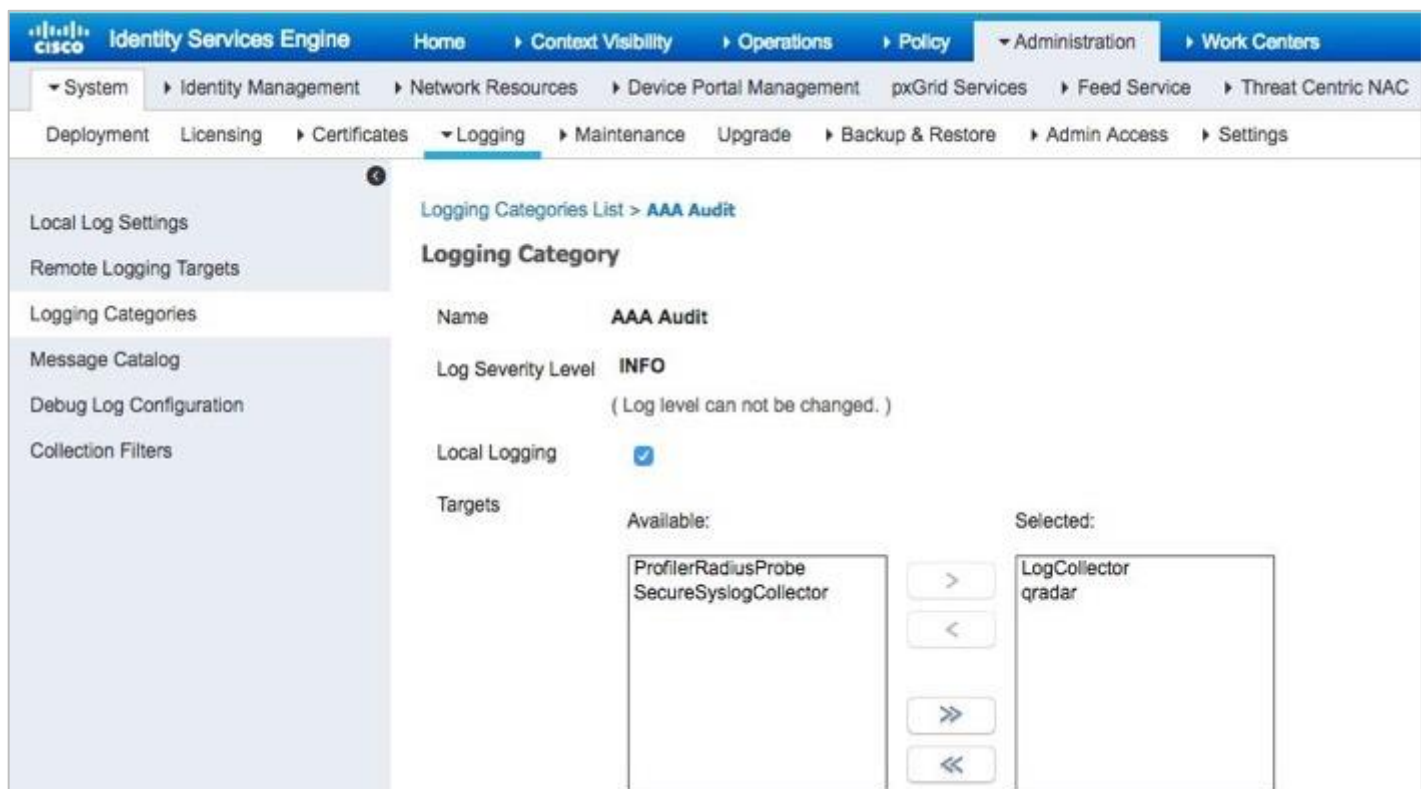
Choose **AAA Audit element > Edit**.





Step 5 Move QRadar from Targets **Available** into the **Selected** column.

Don't worry about the local logging checkbox, leave it alone.



Step 6 Select **Save**.

Step 7 Perform previous steps for additional elements: Passed Authentications, Failed Attempts, Accounting, RADIUS Accounting, Administration and Operational Audit, Posture and Client Provisioning Audit, and Profile.

Step 8 When completed, you should see elements with QRadar listed in the Targets column where appropriate.

Parent Category	Category	Targets	Severity	Local Log L
<input type="radio"/> AAA Audit	AAA Audit	LogCollector,qradar	INFO	enable
<input type="radio"/>	Failed Attempts	LogCollector,ProfilerRadiusProbe,qradar	INFO	enable
<input type="radio"/>	Passed Authentications	LogCollector,ProfilerRadiusProbe,qradar	INFO	disable
<input type="radio"/> AAA Diagnostics	AAA Diagnostics	LogCollector	WARN	enable
<input type="radio"/>	Administrator Authentication and Authorization		WARN	enable
<input type="radio"/>	Authentication Flow Diagnostics		WARN	enable
<input type="radio"/>	Identity Stores Diagnostics		WARN	enable
<input type="radio"/>	Policy Diagnostics		WARN	enable
<input type="radio"/>	RADIUS Diagnostics	LogCollector	WARN	enable
<input type="radio"/>	Guest	LogCollector	INFO	enable
<input type="radio"/>	MyDevices	LogCollector	INFO	enable
<input type="radio"/>	AD Connector	LogCollector	INFO	enable
<input type="radio"/>	TACACS Diagnostics	LogCollector	WARN	enable
<input type="radio"/> Accounting	Accounting	LogCollector,qradar	INFO	enable
<input type="radio"/>	RADIUS Accounting	LogCollector,ProfilerRadiusProbe,qradar	INFO	enable
<input type="radio"/>	TACACS Accounting	LogCollector	INFO	enable
<input type="radio"/> Administrative and Operational Audit	Administrative and Operational Audit	LogCollector,qradar	INFO	enable
<input type="radio"/> External MDM	External MDM	LogCollector	INFO	enable
<input type="radio"/> PassiveID	PassiveID	LogCollector	INFO	enable
<input type="radio"/> Posture and Client Provisioning Audit	Posture and Client Provisioning Audit	LogCollector,ProfilerRadiusProbe,qradar	INFO	enable
<input type="radio"/> Posture and Client Provisioning Diagnostics	Posture and Client Provisioning Diagnostics	LogCollector	WARN	enable
<input type="radio"/> Profiler	Profiler	LogCollector,qradar	INFO	enable
<input type="radio"/> System Diagnostics	System Diagnostics	LogCollector	WARN	enable
<input type="radio"/>	Distributed Management		WARN	enable
<input type="radio"/>	Internal Operations Diagnostics		WARN	enable
<input type="radio"/>	Licensing	LogCollector	INFO	enable
<input type="radio"/>	Threat Centric NAC	LogCollector	INFO	enable

## Performing ISE ANC Mitigation Actions Through IBM QRadar Syslog Events

The desired endpoints for performing ANC mitigation actions must have been authenticated through ISE. In this example, we have Cisco ISE Passed Authentication syslog events sent over to IBM QRadar. We have to create a custom FramedIPAddress field to provide the IP address of the endpoint.

**Note:** IBM will add this later to their DSM collector, so you will not have to add the custom FramedIPAddress field. You may need to add additional fields. These have been included in the Appendices section. This is still required in the version 7.4 of QRadar.

The FramedIPAddress field will be added to the available columns field in the Log Activity Search created for ISE.

The FramedIPAddress field will now appear in ISE Log Activity searches.

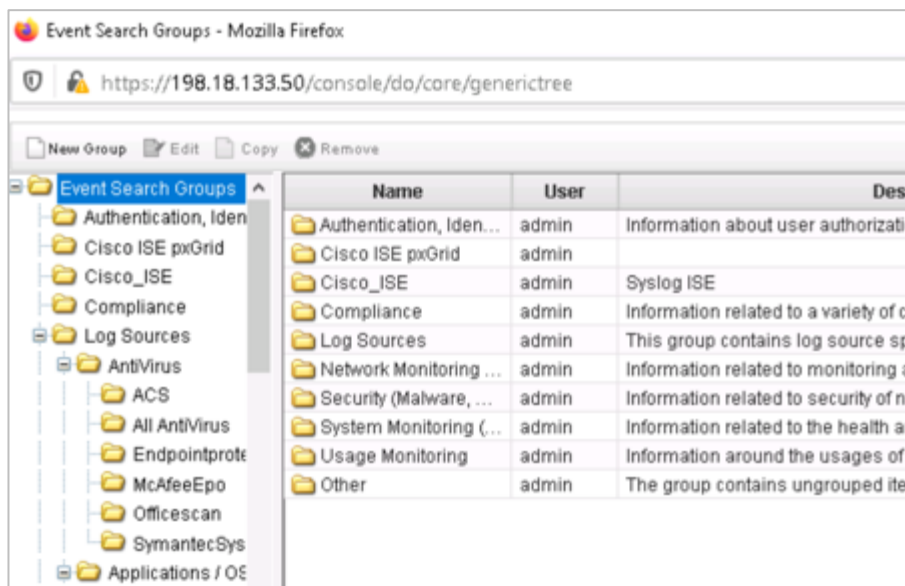
**Note:** You will see a group already created for Cisco ISE pxGrid. This is strictly to use with pxGrid data sources. The following group you're making is for additional support of syslog messages that provide more information than the pxGrid source. This helps you working with additional functionality of QRadar that is beyond the scope of the pxGrid app.

### Creating Custom Field for Framed IP Address ISE Syslog Event

Step 1 In IBM QRadar, go to **Log Activity > Search > New Search > Manage Groups**.

Create **New Group > Cisco\_ISE**.

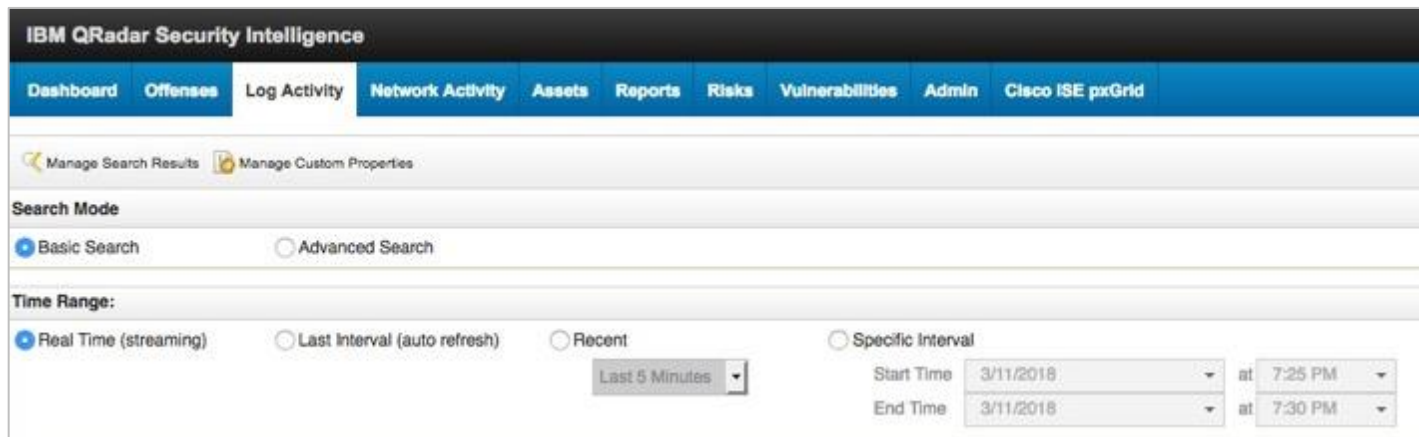
You should see the Cisco ISE group:



Step 2 Close the **Search groups** page and select the newly created **Cisco\_ISE** Group for **Saved Searches**.

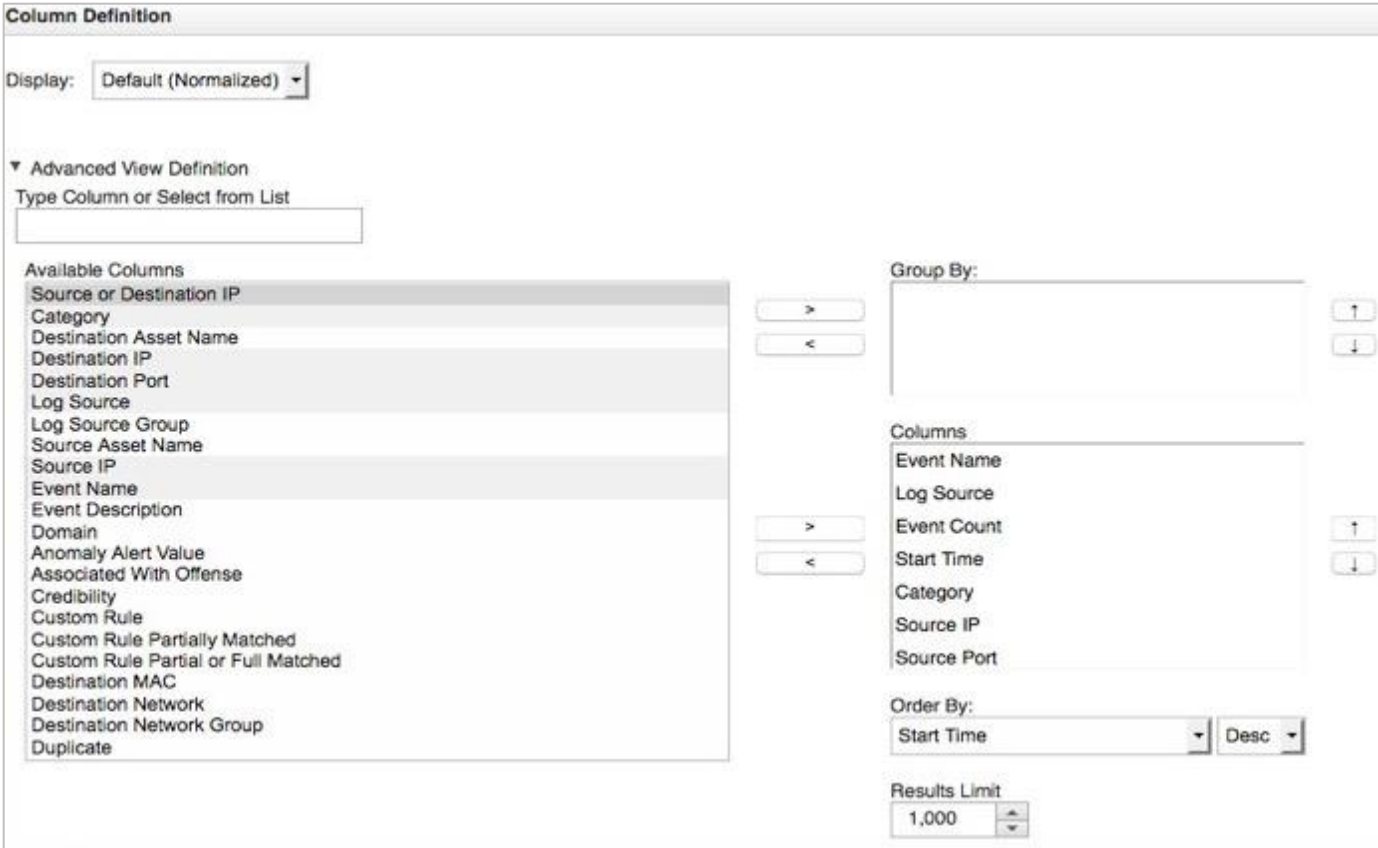


Step 3 Keep the Search defaults.





Step 4 Keep the column defaults.



Column Definition

Display:

▼ Advanced View Definition

Type Column or Select from List

Available Columns

- Source or Destination IP
- Category
- Destination Asset Name
- Destination IP
- Destination Port
- Log Source
- Log Source Group
- Source Asset Name
- Source IP
- Event Name
- Event Description
- Domain
- Anomaly Alert Value
- Associated With Offense
- Credibility
- Custom Rule
- Custom Rule Partially Matched
- Custom Rule Partial or Full Matched
- Destination MAC
- Destination Network
- Destination Network Group
- Duplicate

Group By:

Columns

- Event Name
- Log Source
- Event Count
- Start Time
- Category
- Source IP
- Source Port

Order By:

Start Time Desc

Results Limit

1,000

Step 5 Under **Search Parameters > Parameter > Quick Filters.**

Go to **Log Source (Indexed) > Equals > Log Source Filter > Cisco\_ISE Add Filter.**



**Search Parameters**

Parameter:  Operator:  Value:

Log Source:

**Add Filter**

Current Filters

Log Source is Cisco\_ISE

**Remove Selected Filters**

Step 6 Click **Search**.

IBM QRadar Security Intelligence

admin Help Messages IBM

Dashboard Offenses **Log Activity** Network Activity Assets Reports Risks Vulnerabilities Admin Cisco ISE psGrid System Time: 7:47 PM

Search... Quick Searches Add Filter Save Criteria Save Results Cancel False Positive Rules Actions

Quick Filter  **Search**

Viewing real time events (Paused) View: Select An Option: Display: Default (Normalized)

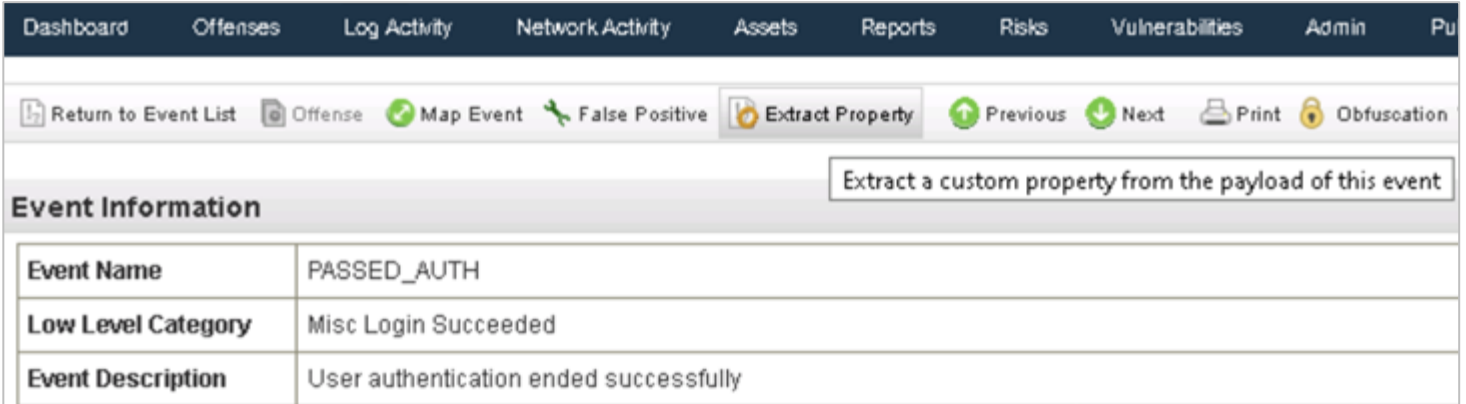
Current Filters:  
Log Source is Cisco\_ISE (Clear Filter)

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port
PASSED_AUTH	Cisco_ISE	1	Mar 11, 2018, 7:47:4...	Misc Logn Succeeded	192.168.1.3	0	192.168.1.147	1645
RADIUS_ACCOUNTING_UPDATE	Cisco_ISE	1	Mar 11, 2018, 7:47:4...	RADIUS Session Status	192.168.1.3	0	192.168.1.147	0
PROFILER_ENDPOINT_PROFILING_EVENT	Cisco_ISE	1	Mar 11, 2018, 7:47:4...	Information	192.168.1.3	1645	192.168.1.147	1645
PROFILER_ENDPOINT_PROFILING_EVENT	Cisco_ISE	1	Mar 11, 2018, 7:47:4...	Information	192.168.1.3	1645	192.168.1.147	1645
CiscoISE_Alarm	Cisco_ISE	1	Mar 11, 2018, 7:47:3...	Warning	192.168.1.147	0	192.168.1.147	0
FAILED_AZN_ONLY	Cisco_ISE	1	Mar 11, 2018, 7:47:3...	General Authentication Failed	192.168.1.147	0	192.168.1.147	0
FAILED_AZN_ONLY	Cisco_ISE	1	Mar 11, 2018, 7:47:3...	General Authentication Failed	192.168.1.147	0	192.168.1.147	0
FAILED_AZN_ONLY	Cisco_ISE	1	Mar 11, 2018, 7:47:2...	General Authentication Failed	192.168.1.147	0	192.168.1.147	0
PROFILER_ENDPOINT_PROFILING_EVENT	Cisco_ISE	1	Mar 11, 2018, 7:47:2...	Information	192.168.1.3	1645	192.168.1.147	1645

Note: The following steps will work with a wired connection, however with a wireless connection you will need to check RADIUS Accounting events.

Step 7 In the upper right corner, click **Pause**, and then double-click **Passed Auth (wired)** or **Radius\_Acct (wireless)**.

Step 8 Click **Extract Property** and for **New Property**, then type: **FramedIPAddress**.



The screenshot shows the Cisco Secure Access interface. At the top, there is a navigation bar with tabs: Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Risks, Vulnerabilities, Admin, and Pu. Below the navigation bar, there is a toolbar with buttons: Return to Event List, Offense, Map Event, False Positive, Extract Property, Previous, Next, Print, and Obfuscation. The 'Event Information' section is highlighted, and a tooltip is visible over the 'Extract Property' button, stating: 'Extract a custom property from the payload of this event'. Below this, there is a table with the following data:

Event Name	PASSED_AUTH
Low Level Category	Misc Login Succeeded
Event Description	User authentication ended successfully

Step 9 For **Field Type**, type: **IP**.

Step 10 For **Description**, type: **FramedIPAddress**.

Step 11 For **Extraction** > **RegEx** > type: **Framed-IP-Address=(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b)**.



You should see:

### Property Definition

Existing Property:

New Property:

Optimize parsing for rules, reports, and searches

Field Type:

Description:

### Property Expression Definition

Enabled:

**Selection**

Log Source Type:

Log Source:

Event Name:

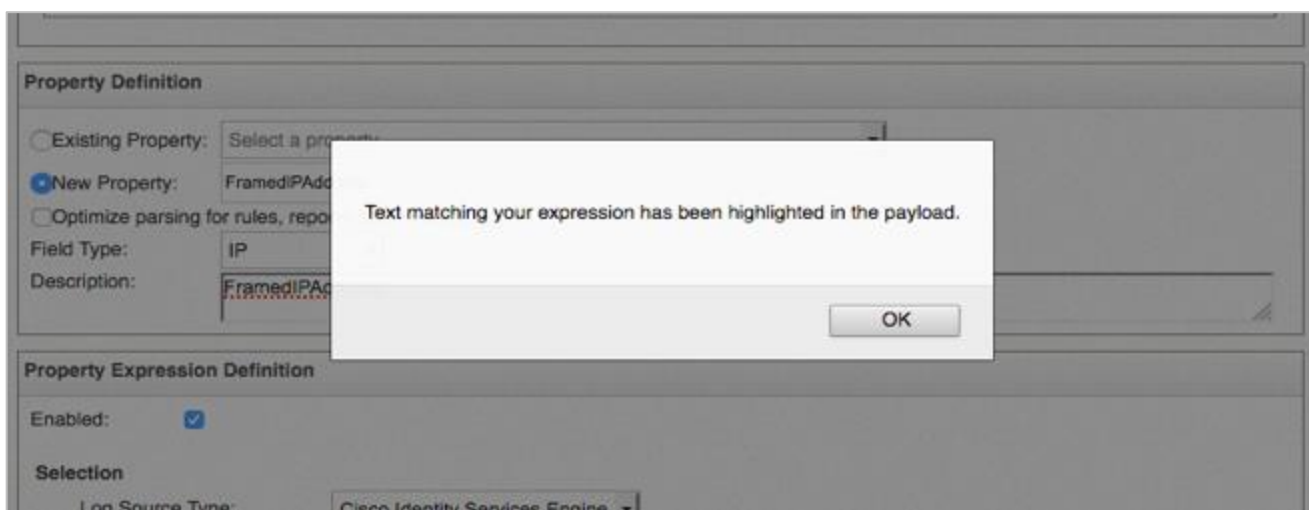
Category:

**Extraction**

RegEx:  Capture Group:

Step 12 Select **Test**.

You should see:



Step 13 Select **OK**.

Step 14 Select **Save**.

Step 15 Ensure the FramedIPAddress appeared:



Event Information			
Event Name	PASSED_AUTH		
Low Level Category	Misc Login Succeeded		
Event Description	User authentication ended successfully		
Magnitude		(5)	Relevance
Username	pxgrid1		
Start Time	Mar 11, 2018, 7:47:42 PM	Storage Time	Mar 11, 2018, 7:47:42 PM
FramedIPAddress (custom)	192.168.1.15		

Step 16 Select **Return to Event List**.

Step 17 Select **Search > Edit Search > Saved Searches > Group: Cisco\_IS**.

Step 18 Scroll down to **Column Definition > Available Columns > FramedIPAddress(Custom) > Move to columns** by selecting ">".

Note: You can search for the value instead of scrolling through list.

**IBM QRadar Security Intelligence**

Dashboard Offenses **Log Activity** Network Activity Assets Reports Risks Vulnerabilities Admin Cisco ISE pxGrid

Manage Search Results Manage Custom Properties

Display: Custom

Name:  Save Column Layout

Advanced View Definition

Type Column or Select from List

Available Columns

- Dormant Offense Count (custom)
- Duration\_Hours (custom)
- Duration\_Minutes (custom)
- Duration\_Seconds (custom)
- Element (custom)
- Event Summary (custom)
- EventID (custom)
- Events per Second Coalesced - Average 1 Min (custom)
- Events per Second Coalesced - Peak 1 Sec (custom)
- Events per Second Raw - Average 1 Min (custom)
- Events per Second Raw - Peak 1 Sec (custom)
- External ID (custom)
- File Hash (custom)
- File ID (custom)
- File Path (custom)
- Filename (custom)
- Flow Source (custom)
- Flows per Second - Average 15 Min (custom)
- Flows per Second - Peak 1 Min (custom)
- FramedIPAddress (custom)
- FramedIPAddress2 (custom)
- Function code (custom)

Group By:

Columns

- Source IP
- Source Port
- Destination IP
- Destination Port
- Username
- Magnitude
- FramedIPAddress (custom)

Order By: Start Time Desc

Results Limit: 1,000

Step 19 Select **Filter**. Now, you should see the custom **FramedIPAddress** field:

**IBM QRadar Security Intelligence**

admin Help Messages IBM

Dashboard Offenses **Log Activity** Network Activity Assets Reports Risks Vulnerabilities Admin Cisco ISE pxGrid System Time: 8:24 PM

Search Quick Searches Add Filter Save Criteria Save Results Cancel Filter Positive Rules Actions

Quick Filter  Search

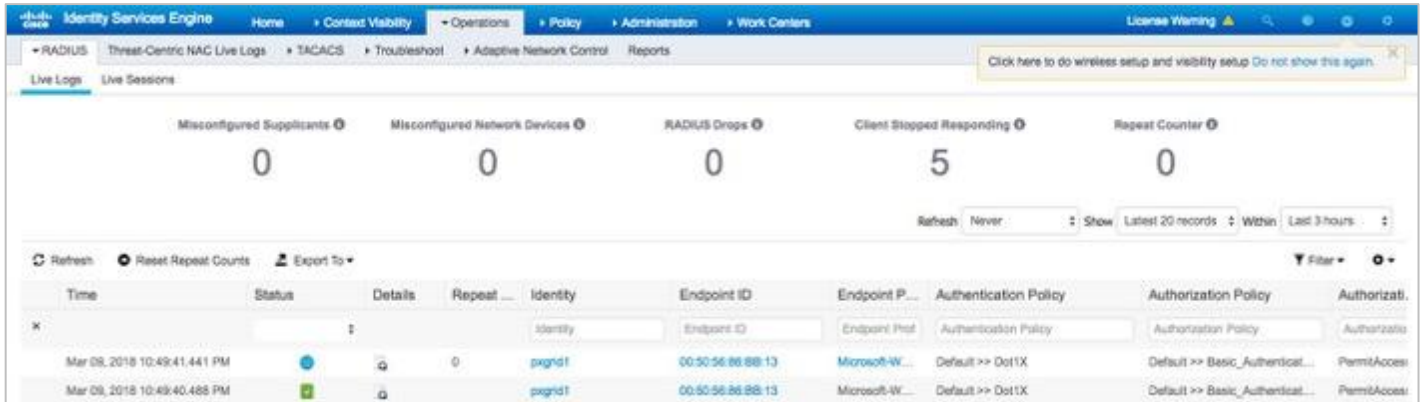
Viewing real time events (Paused) View: Select An Option Display: Custom

Current Filters: Log Source is Cisco\_ISE (Clear Filter)

Event Name	Log Source	Event Count	Start Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude	FramedIPAddress (custom)
PASSED_AUTH	Cisco_ISE	1	Mar 11, 2018, 8:...	Misc Login Succ...	192.168.1.3	0	192.168.1.147	1645	pxgrid1	5	192.168.1.15
PASSED_AUTH	Cisco_ISE	1	Mar 11, 2018, 8:...	Misc Login Succ...	192.168.1.3	0	192.168.1.147	1645	pxgrid1	5	192.168.1.15
PASSED_DYNAMIC_ATZ	Cisco_ISE	1	Mar 11, 2018, 8:...	General Authent...	192.168.1.3	0	192.168.1.147	0	N/A	5	N/A
RADIUS_ACCOUNTING...	Cisco_ISE	1	Mar 11, 2018, 8:...	RADIUS Sessio...	192.168.1.3	0	192.168.1.147	0	N/A	5	N/A
FAILED_ATTEMPT_DY...	Cisco_ISE	1	Mar 11, 2018, 8:...	General Authent...	192.168.1.3	0	192.168.1.147	0	N/A	5	N/A
PASSED_DYNAMIC_ATZ	Cisco_ISE	1	Mar 11, 2018, 8:...	General Authent...	192.168.1.3	0	192.168.1.147	0	N/A	5	N/A
CiscoISE_Alarm	Cisco_ISE	1	Mar 11, 2018, 8:...	Warning	192.168.1.147	0	192.168.1.147	0	N/A	5	N/A
AUTHEN_PASSED	Cisco_ISE	1	Mar 11, 2018, 8:...	Admin Login Su...	192.168.1.136	0	192.168.1.147	0	admin	5	N/A
AUTHEN_FAILED	Cisco_ISE	1	Mar 11, 2018, 8:...	Admin Login Fai...	192.168.1.136	0	192.168.1.147	0	admin	5	N/A
RADIUS_ACCOUNTING...	Cisco_ISE	1	Mar 11, 2018, 8:...	RADIUS Sessio...	192.168.1.3	0	192.168.1.147	0	N/A	5	N/A

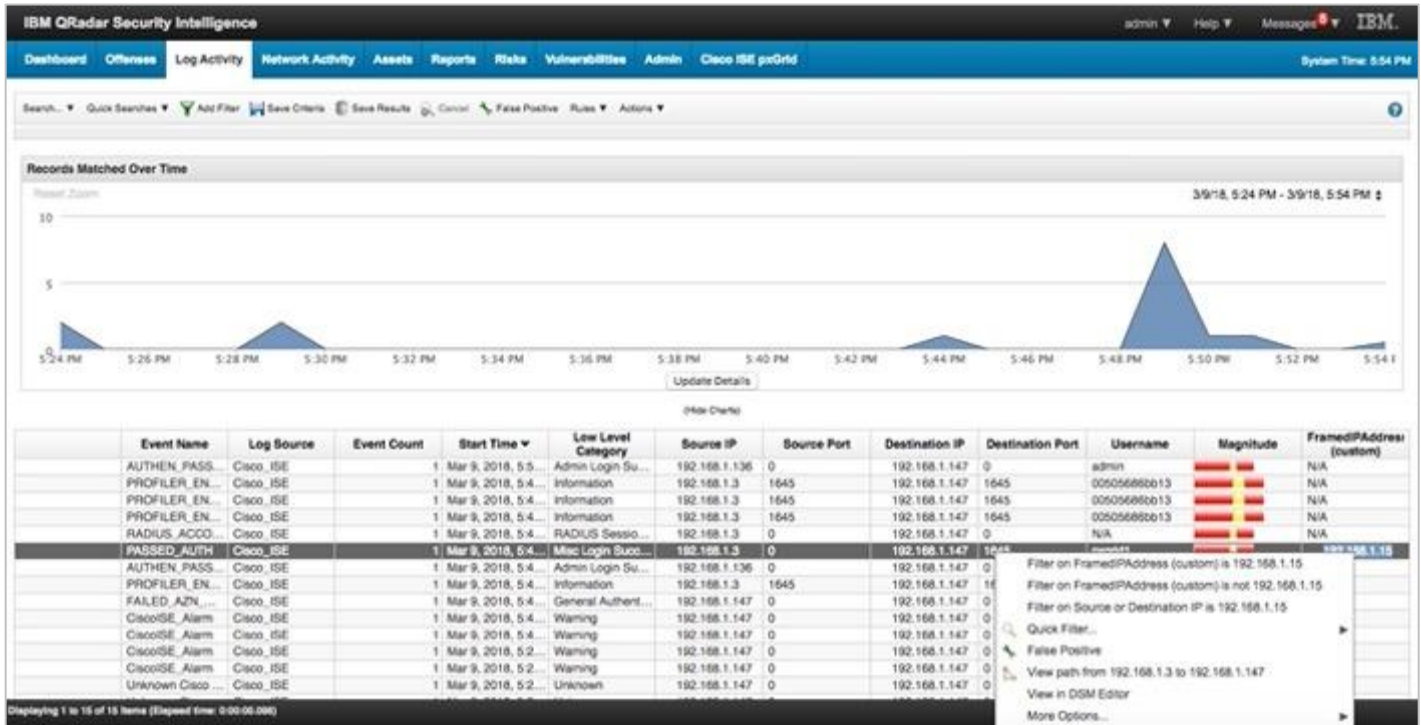
## ANC Mitigation Syslog Event Example

Step 1 The user has been successfully authenticated through ISE.



Step 2 In QRadar, select the syslog event, right-click **FramedIPAddress**, and then select **More Options**.

In the following example, a Passed authentication (or RADIUS Accounting) syslog event was received from ISE:



Note: You can right-click the **Source IP** and **Destination IP** address. This will also work on customized IP Fields.

Step 3 Select **More Options > Cisco pxGrid – ANC Quarantine**.

The screenshot shows the IBM QRadar Security Intelligence interface. At the top, there are navigation tabs: Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Risks, Vulnerabilities, Admin, and Cisco ISE pxGrid. Below the tabs is a search bar and a toolbar with options like Add Filter, Save Criteria, Save Results, Cancel, False Positive, Rules, and Actions. A line graph titled 'Records Matched Over Time' shows activity between 5:24 PM and 5:54 PM. Below the graph is a table of log events.

Event Name	Log Source	Event Count	Start Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude	FramedIPAddress (custom)
AUTHEN_PASS...	Cisco_ISE	1	Mar 9, 2018, 5:5...	Admin Login Su...	192.168.1.136	0	192.168.1.147	0	admin	High	N/A
PROFILER_EN...	Cisco_ISE	1	Mar 9, 2018, 5:4...	Information	192.168.1.3	1645	192.168.1.147	1645	00505686bb13	High	N/A
PROFILER_EN...	Cisco_ISE	1	Mar 9, 2018, 5:4...	Information	192.168.1.3	1645	192.168.1.147	1645	00505686bb13	High	N/A
PROFILER_EN...	Cisco_ISE	1	Mar 9, 2018, 5:4...	Information	192.168.1.3	1645	192.168.1.147	1645	00505686bb13	High	N/A
RADIUS_ACCO...	Cisco_ISE	1	Mar 9, 2018, 5:4...	RADIUS Sessio...	192.168.1.3				N/A	High	N/A
PASSED_AUTH	Cisco_ISE	1	Mar 9, 2018, 5:4...	Misc Login Succ...	192.168.1.3				N/A	High	N/A
AUTHEN_PASS...	Cisco_ISE	1	Mar 9, 2018, 5:4...	Admin Login Su...	192.168.1.136				N/A	High	N/A
PROFILER_EN...	Cisco_ISE	1	Mar 9, 2018, 5:4...	Information	192.168.1.3				N/A	High	N/A
FAILED_AZN...	Cisco_ISE	1	Mar 9, 2018, 5:4...	General Authent...	192.168.1.147				N/A	High	N/A
CiscoISE_Alarm	Cisco_ISE	1	Mar 9, 2018, 5:4...	Warning	192.168.1.147				N/A	High	N/A
CiscoISE_Alarm	Cisco_ISE	1	Mar 9, 2018, 5:2...	Warning	192.168.1.147				N/A	High	N/A
CiscoISE_Alarm	Cisco_ISE	1	Mar 9, 2018, 5:2...	Warning	192.168.1.147				N/A	High	N/A
Unknown Cisco	Cisco_ISE	1	Mar 9, 2018, 5:2...	Unknown	192.168.1.147				N/A	High	N/A

A context menu is open over the 'PASSED\_AUTH' event, showing options like 'Cisco pxGrid - ANC Quarantine' and 'Cisco pxGrid - ANC Port Bounce'. The 'More Options...' option is selected, opening a sub-menu with filters and actions like 'Filter on FramedIPAddress (custom) is 192.168.1.15' and 'Run Forensics Search'.

Step 4 You should see a successful status message:

The screenshot shows a status message dialog box in the IBM QRadar Security Intelligence interface. The message text reads: '192.168.1.192 Says' followed by 'ANC action returned status: RUNNING'. There is an 'OK' button at the bottom right of the dialog box.

Step 5 Select **OK**.

Step 6 To view in ISE, go to **Operations > RADIUS > Live Logs**.



You should see the quarantined endpoint designated by the ANC Quarantine Policy:

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorizati...
Mar 09, 2018 10:59:37.370 PM	<span style="color: blue;">●</span>	q	0	pxgrid1	00:50:56:86:8B:13	Microsoft-W...	Default >> Dot1X	Default >> ANCQuarantine	Quarantined.
Mar 09, 2018 10:59:37.261 PM	<span style="color: green;">●</span>	q		pxgrid1	00:50:56:86:8B:13	Microsoft-W...	Default >> Dot1X	Default >> ANCQuarantine	Quarantined.
Mar 09, 2018 10:59:36.193 PM	<span style="color: green;">●</span>	q			00:50:56:86:8B:13				

Step 7 To view in Cisco ISE pxGrid ANC Details Dashboard, go to **Cisco ISE pxGrid > ANC Details**.

You should see the MAC address assigned to the ISE ANC policy name:

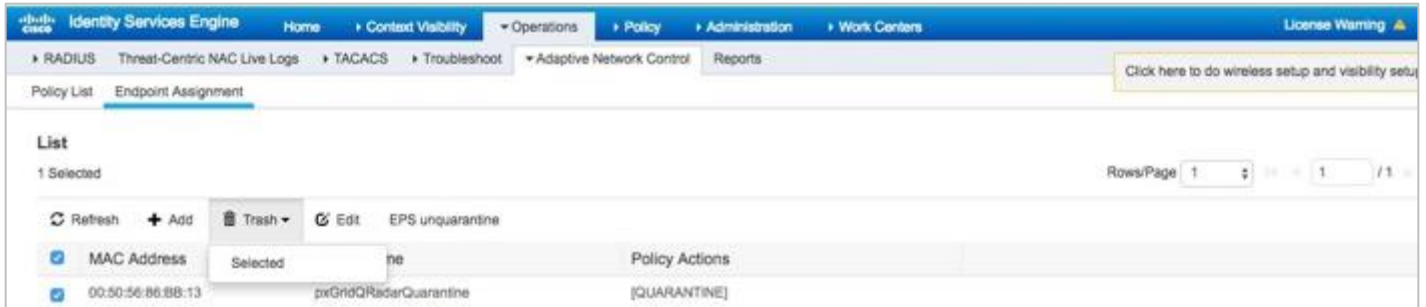
Mac Address	Policy Name
8881118FF812	pxGridRadarPortBounce
957028840005	policy_name-09
957028840006	pxGridRadarPortBounce
957028840007	test_ul
957028840008	testaddition
A88D27C2610C	pxGridRadarPortBounce
F887F13C389E	pxGridRadarPortBounce

Step 8 To un-quarantine or clear the endpoint:

Go to ISE > **Operations > Adaptive Network Control > Endpoint Assignment**.

MAC Address	Policy Name	Policy Actions
<input type="checkbox"/>	00:50:56:86:8B:13	pxGridRadarQuarantine [QUARANTINE]

Step 9 Select the endpoint **MAC address** > **Trash**.



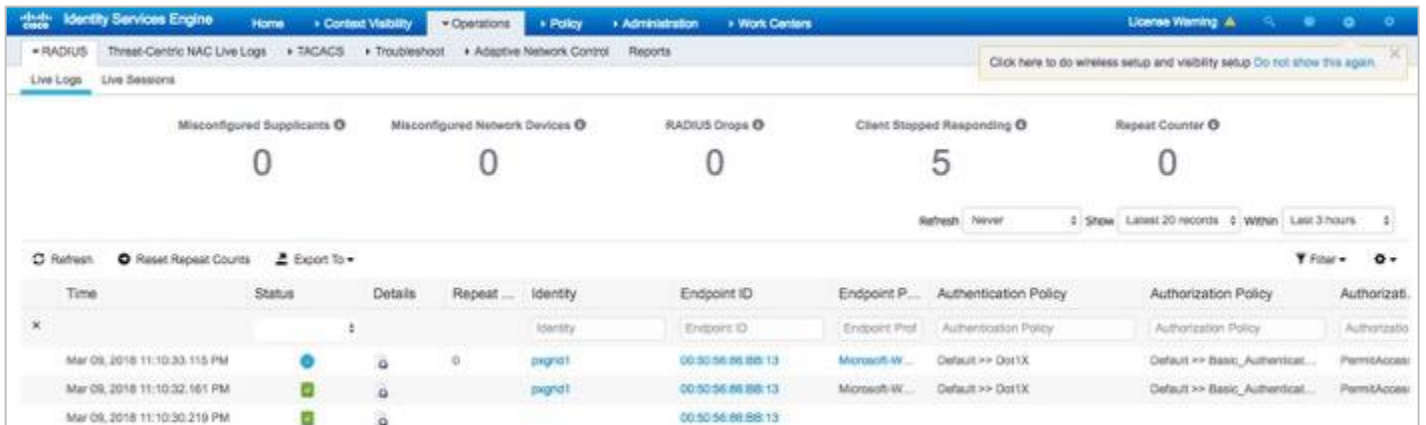
Step 10 Select **Selected**, and then you should see:



Step 11 Select **Yes**.

Step 12 In ISE, go to **Operations > RADIUS-Live Logs**.

You should see that the endpoint has been un-quarantined:



# Hovering Over IBM QRadar Syslog IP Address for ISE Contextual Information

Once the endpoint has been authenticated, you can hover the IP address fields and obtain additional contextual information such as the User Name, Mac Address, Posture Status, and Endpoint Profile.

When you hover over the IP address field, the contextual information is displayed:

The screenshot shows the IBM QRadar Security Intelligence interface. At the top, there are navigation tabs: Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Admin, and Cisco paGrid. Below the navigation is a search bar and a time range selector set to '2Q/18, 4:11 PM - 2/18/18, 4:16 PM'. A line chart shows activity over time from Feb 10 to Feb 17. Below the chart is a table of log entries. A tooltip is displayed over the 'Destination IP' field of the first entry, showing detailed session information.

Start Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude	FramedIPAddress (custom)	NAS-Port (custom)	NAS-Port-Type (custom)	NAS-IP-Address (custom)
1 Feb 18, 2018, 4:15:58 PM	Misc Login Succeeded	192.168.1.3	0	192.168.1.147	1644	hostpxGrid		192.168.1.7	50111	Ethernet	192.168.1.7
1 Feb 18, 2018, 4:15:56 PM	RADIUS Session Status	192.168.1.3	0	<b>Network:</b> Net-10-172-192-Net_192_168_0_0 192.168.1.7 50111 Ethernet N/A 192.168.1.7 192.168.1.7 50111 Ethernet N/A 192.168.1.7 192.168.1.7 50111 Ethernet N/A 192.168.1.7 192.168.1.7 50111 Ethernet N/A 192.168.1.7							
1 Feb 18, 2018, 4:15:28 PM	RADIUS Session Ended	192.168.1.3	0	<b>paGrid Session details:</b> User Name: hostpxGrid2-PC.18010.com Mac Address: 00:0C:29:C1:7B:2C Posture Status: None Endpoint Profile: Windows7-Workstation							
1 Feb 18, 2018, 4:15:27 PM	Misc Login Succeeded	192.168.1.3	0								
1 Feb 18, 2018, 4:15:26 PM	Information	192.168.1.3	0								
1 Feb 18, 2018, 4:15:25 PM	RADIUS Session Started	192.168.1.3	0								



## IBM QRadar Cisco ISE pxGrid Offense Rule

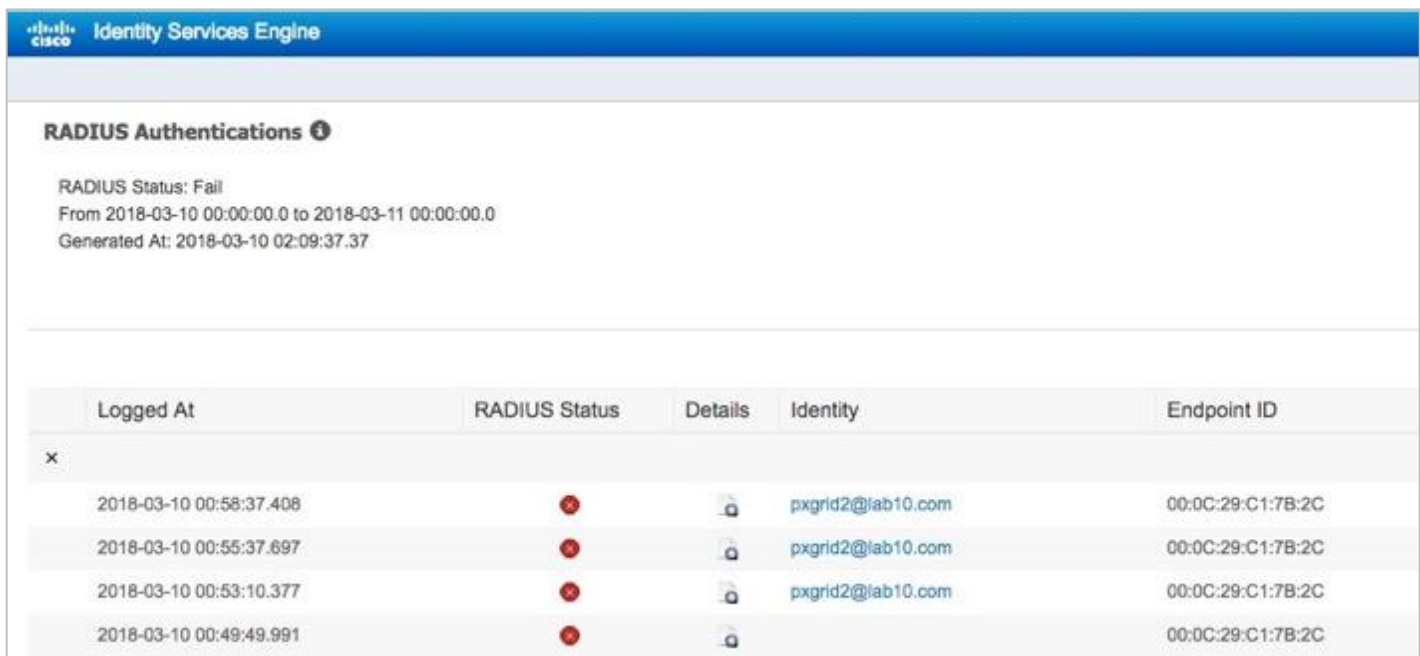
IBM QRadar Custom Rules Engine (CRE) displays the rules and building blocks that are used by IBM QRadar. The CRE provides information about how the rules are groups, the types of tests that the rules perform, and the rule responses. A rule is a collection of tests that triggers an action when specific actions are met.





Offenses are generated when events and flow data pass through the CRE. They are correlated against the rules that are configured and an offense can be generated based on this correlation and viewed on the Offenses tab.

The Cisco pxGrid offense rule gets triggered when an event occurs, the match Radius Failure session or simply three events in the Cisco ISE pxGrid App Failed Authentication Dashboard from the same source IP address that occur within 10 minutes.

As a simple test, you can attempt to log in with an invalid password, and then login successfully. This will trigger a failed event followed by a successful login. Repeat this step three or four times within 10 minutes, and this will trigger the IBM QRadar pxGrid Offense rule.

The following image is an example of ISE authentication failure report that confirms failed authentications.



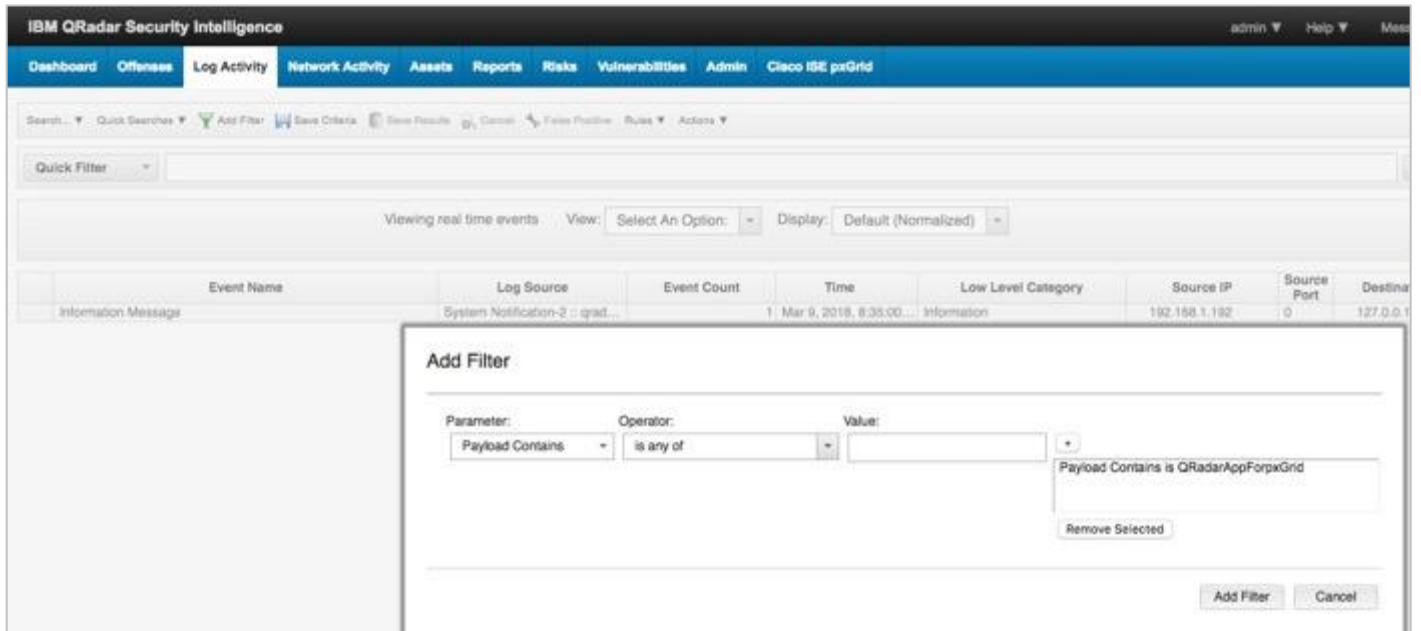
Logged At	RADIUS Status	Details	Identity	Endpoint ID
2018-03-10 00:58:37.408	✖		pxgrid2@lab10.com	00:0C:29:C1:7B:2C
2018-03-10 00:55:37.697	✖		pxgrid2@lab10.com	00:0C:29:C1:7B:2C
2018-03-10 00:53:10.377	✖		pxgrid2@lab10.com	00:0C:29:C1:7B:2C
2018-03-10 00:49:49.991	✖		pxgrid2@lab10.com	00:0C:29:C1:7B:2C

You can also view events in ISE.

Time	Status	Username	IP Address	Device Type	Authentication Policy	Authorization Policy
Mar 10, 2018 01:59:31.302 AM	●	LAB10\pgrnd2	00:0C:29:C1:7B:2C	Windows7...	Default >> Dot1X	Default >> Basic_Authenticat...
Mar 10, 2018 01:59:30.971 AM	●	LAB10\pgrnd2	00:0C:29:C1:7B:2C	Windows7...	Default >> Dot1X	Default >> Basic_Authenticat...
Mar 10, 2018 01:29:06.452 AM	●	LAB10\pgrnd2	00:0C:29:C1:7B:2C	Windows7...	Default >> Dot1X	Default >> Basic_Authenticat...
Mar 10, 2018 01:21:15.684 AM	●	[REDACTED]	10:00:B1:C9:3C:39	Apple-Device	Default >> Dot1X	Default >> Basic_Authenticat...
Mar 10, 2018 01:21:15.160 AM	●	[REDACTED]	10:00:B1:C9:3C:39	Apple-Device	Default >> Dot1X	Default >> Basic_Authenticat...
Mar 10, 2018 01:16:17.167 AM	●	10:00:B1:C9:3C:39	10:00:B1:C9:3C:39	Apple-Device	Default >> MAB	Default >> Basic_Authenticat...
Mar 10, 2018 12:59:44.623 AM	●	pgrnd2@lab10.com	00:0C:29:C1:7B:2C	Windows7...	Default >> Dot1X	Default >> Basic_Authenticat...
Mar 10, 2018 12:59:42.460 AM	●		00:0C:29:C1:7B:2C			
Mar 10, 2018 12:58:37.408 AM	●	pgrnd2@lab10.com	00:0C:29:C1:7B:2C		Default >> Dot1X	Default
Mar 10, 2018 12:58:12.372 AM	●	hostprGnt2-PC1...	00:0C:29:C1:7B:2C	Windows7...	Default >> Dot1X	Default >> Basic_Authenticat...
Mar 10, 2018 12:57:40.226 AM	●	hostprGnt2-PC1...	00:0C:29:C1:7B:2C	Windows7...	Default >> Dot1X	Default >> Basic_Authenticat...
Mar 10, 2018 12:56:36.688 AM	●	pgrnd2@lab10.com	00:0C:29:C1:7B:2C	Windows7...	Default >> Dot1X	Default >> Basic_Authenticat...
Mar 10, 2018 12:55:37.697 AM	●	pgrnd2@lab10.com	00:0C:29:C1:7B:2C		Default >> Dot1X	Default

## Verify pxGrid offense rule via Log Activity

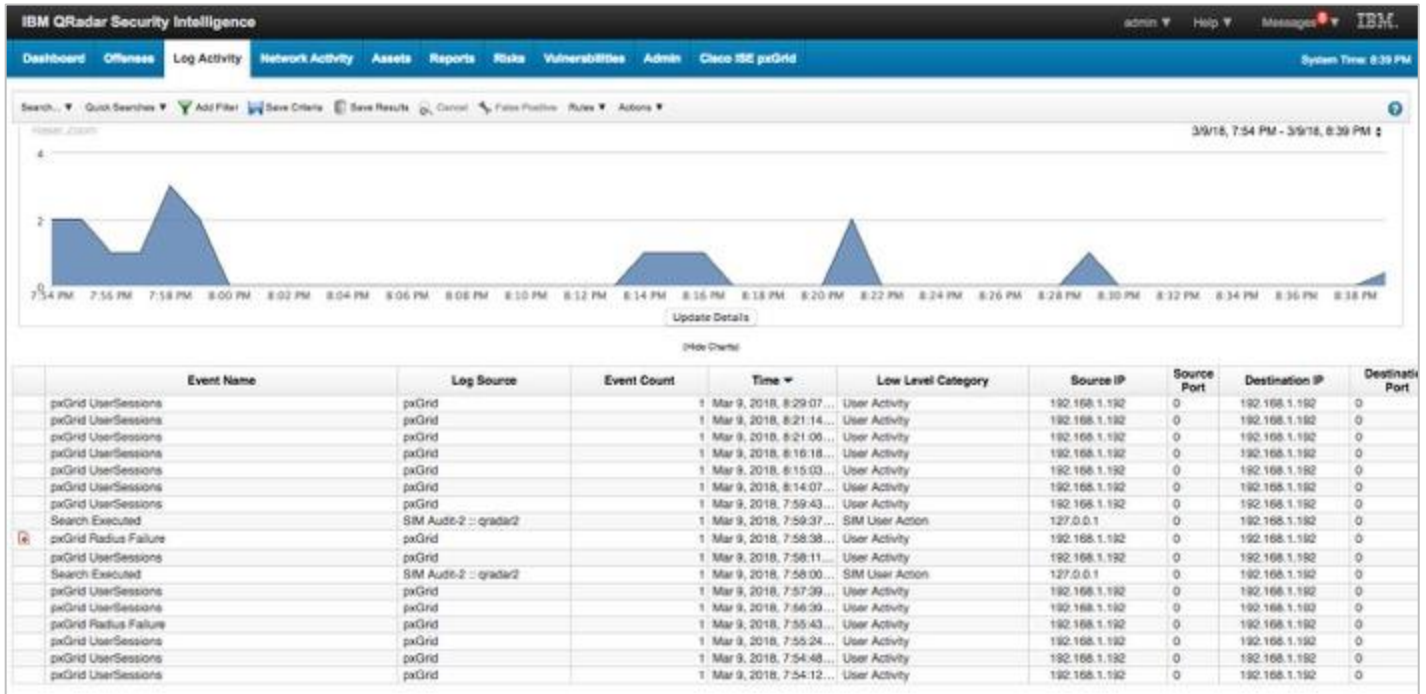
Step 13 Go to Log Activity > Add Filter > Parameter > Payload Contains > Operator > is any of > Value > QRadarAppForPxgrid > "+".



Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination
Information Message	System Notification-2 : grad...		1 Mar 9, 2018, 8:35:00...	Information	192.168.1.192	0	127.0.0.1

Step 14 Select **Add Filter**.

Step 15 Select **View Real Time Events** > Last interval setting, for example, 45 minutes.



Step 16 Click the offense rule

You will see the following:

Offense 1 (All Categories)

**Offense 1** Summary Display Events Connections Flows View Attack Path Actions Print

<b>Magnitude</b>		<b>Status</b>		<b>Relevance</b>	5	<b>Severity</b>	4	<b>Credibility</b>	2
<b>Description</b>	pxGrid Radius Failure	<b>Offense Type</b>	pxGrid_src (custom)						
		<b>Event/Flow count</b>	3 events and 0 flows in 1 categories						
<b>Source IP(s)</b>	192.168.1.192	<b>Start</b>	Mar 9, 2018, 7:53:10 PM						
<b>Destination IP(s)</b>	192.168.1.192	<b>Duration</b>	5m 27s						
<b>Network(s)</b>	Net-10-172-192.Net 192.168.0.0	<b>Assigned to</b>	Unassigned						

**Offense Source Summary**

<b>Custom property value</b>	192.168.1.60		
<b>Offenses</b>	1	<b>Events/Flows</b>	1

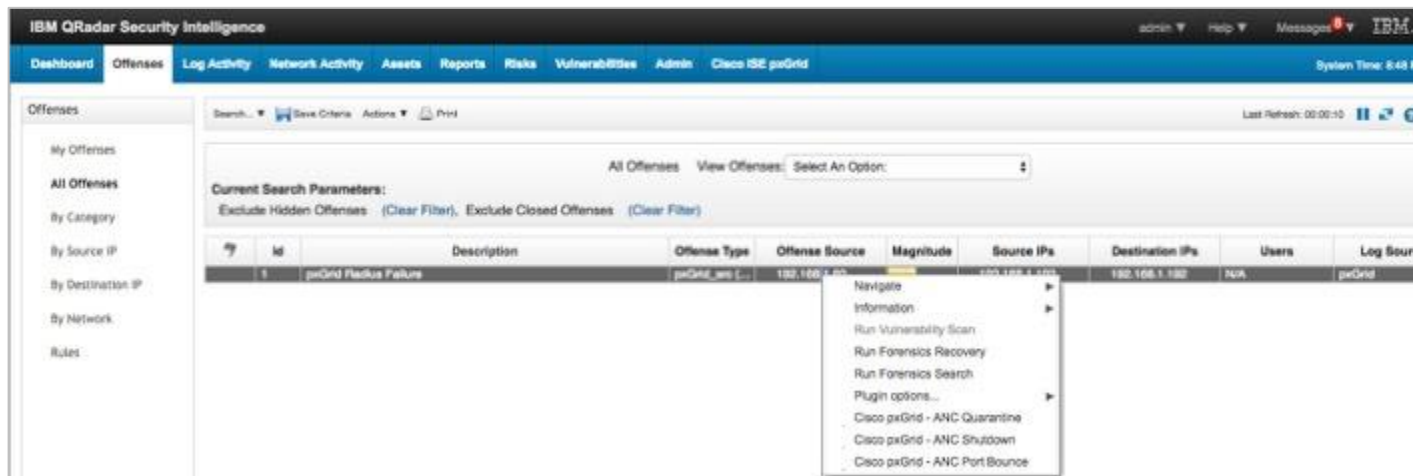
## Verify pxGrid offense rule via Offenses Dashboard

After select **Offenses**, you should see the pxGrid Radius Failure Offense rule:



## Taking ISE ANC mitigations from Offenses Dashboard

Step 1 Under the Offense Source, right-click the IP address, and then select the Cisco pxGrid - ANC Quarantine mitigation action.



Step 2 This will trigger the ANC Quarantine:



Step 3 Select OK.



Step 4 In ISE, select **Operations > RADIUS > Live Logs**.

Note: The endpoint has been quarantined as designated by the ANC Quarantine Authorization Policy.

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorizati.
Mar 10, 2018 02:30:00.432 AM	<span style="color: blue;">●</span>		0	LAB10\pagn2	00:0C:29:C1:7B:2C	WindowsF...	Default >> Dot1X	Default >> ANOQuarantine	Quarantined.
Mar 10, 2018 02:30:00.145 AM	<span style="color: green;">●</span>			LAB10\pagn2	00:0C:29:C1:7B:2C	WindowsF...	Default >> Dot1X	Default >> ANOQuarantine	Quarantined.

Step 5 To un-quarantine or clear, go to **Operations > Adaptive Network Control > Endpoint Assignment**.

MAC Address	Policy Name	Policy Actions
<input type="checkbox"/> 00:0C:29:C1:7B:2C	pxGridQRadarQuarantine	[QUARANTINE]

Step 6 Select the endpoint > **Trash**.

MAC Address	Policy Name	Policy Actions
<input checked="" type="checkbox"/> 00:0C:29:C1:7B:2C	pxGridQRadarQuarantine	[QUARANTINE]

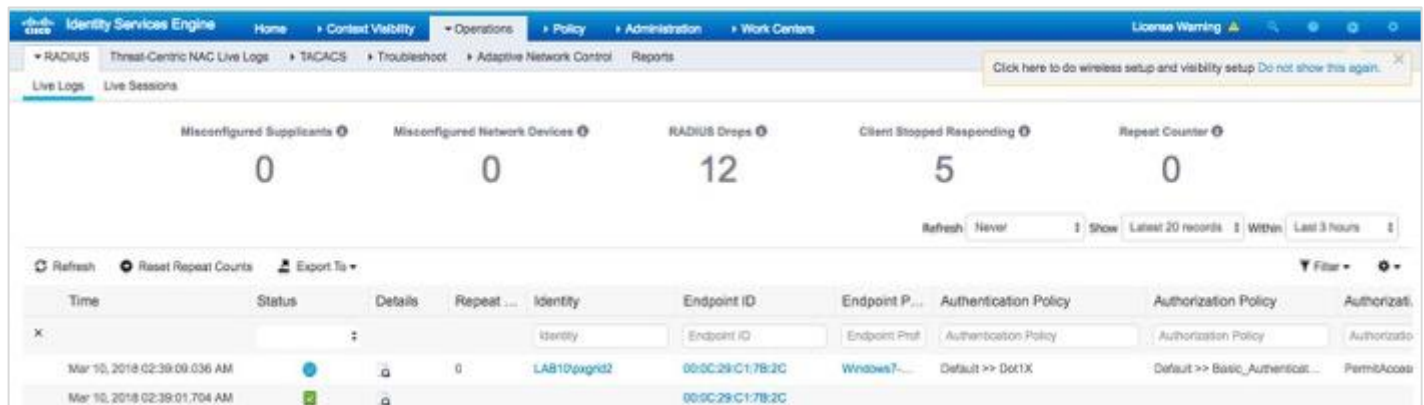


Step 7 **Select > Selected.**

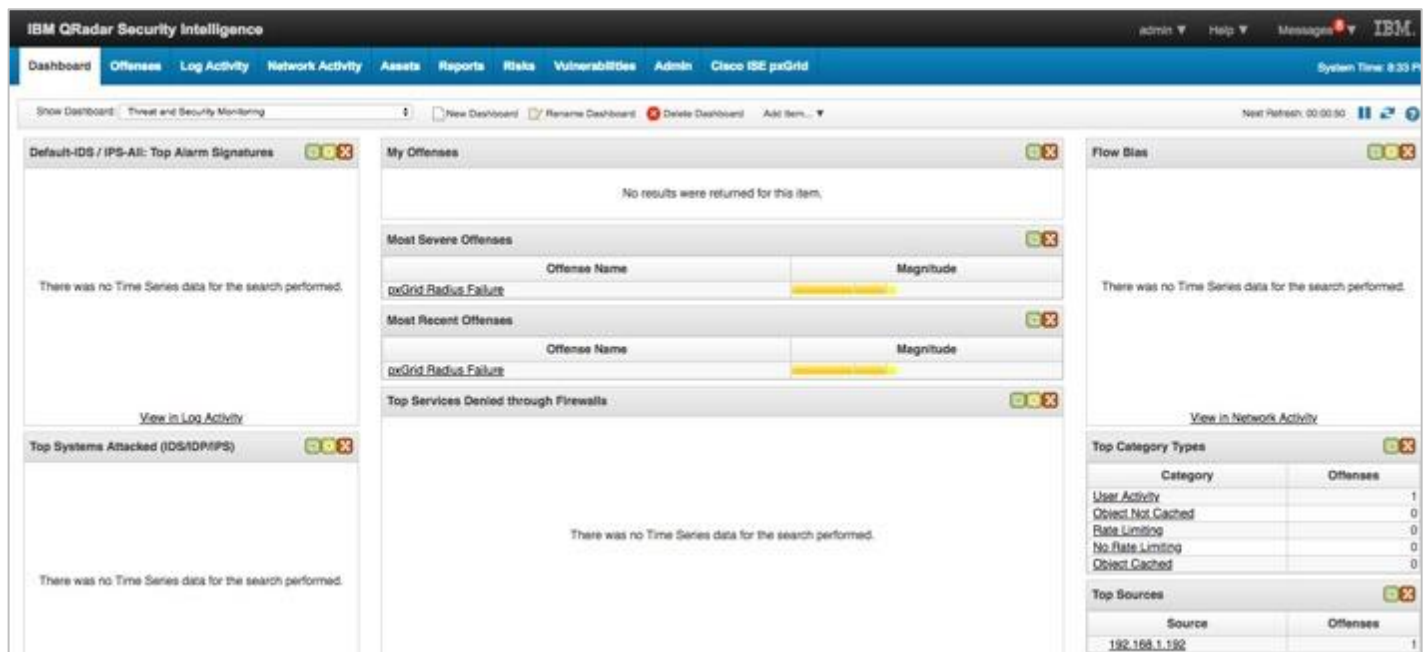


Step 8 **Select Yes.**

Step 9 In ISE, you should see the endpoint has been un-quarantined:



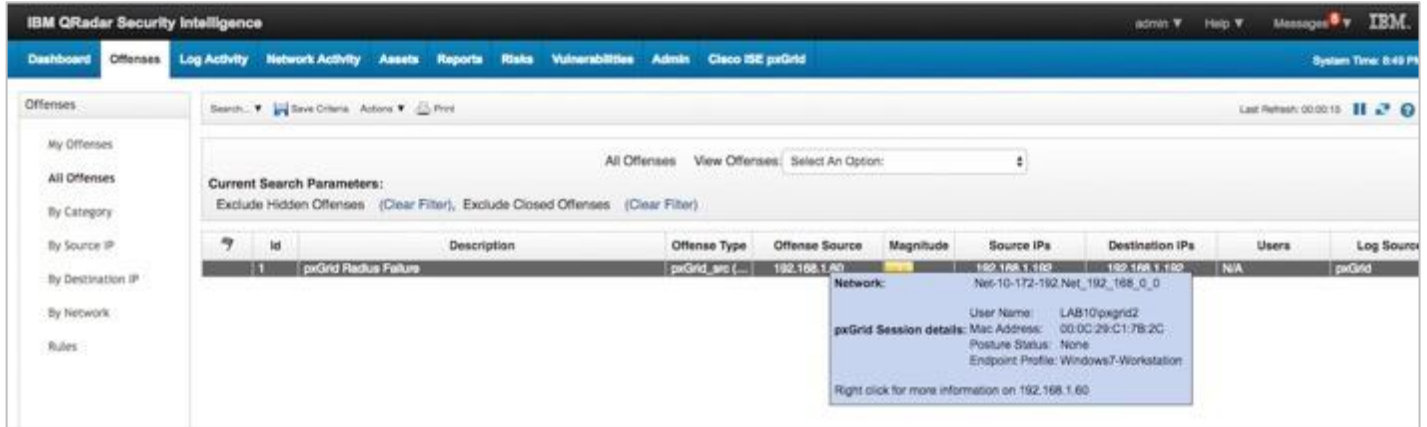
Step 10 **Select Dashboard**





Step 11 Select **pxGrid Radius Failure**.

Step 12 Hover over the **Offense Source IP Address**.



The screenshot shows the IBM QRadar Security Intelligence interface. The 'Offenses' tab is active, displaying a table of offenses. A tooltip is visible over the 'Offense Source' column of the first row, providing details for the 'pxGrid Radius Failure' event.

id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Source
1	pxGrid Radius Failure	pxGrid_spo (...)	192.168.1.60	High	192.168.1.100	192.168.1.100	N/A	pxGrid

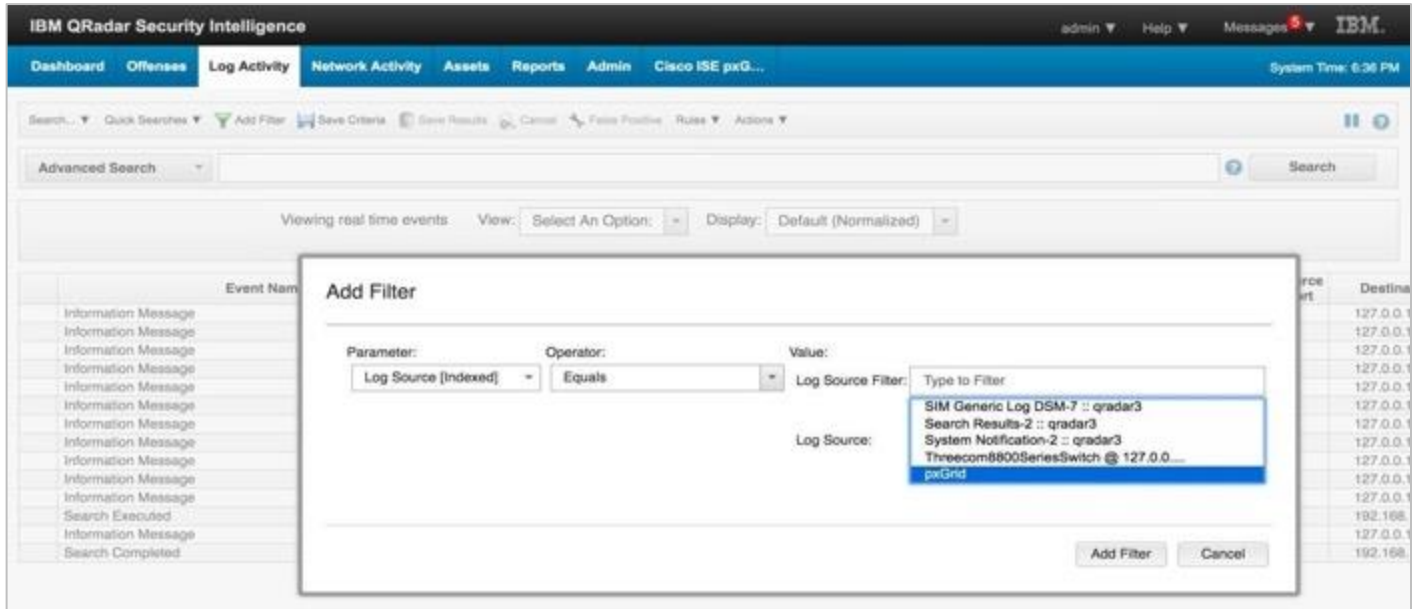
**Network:**  
 Net: 10-172-192-Net\_192\_168\_0\_0  
 User Name: LAB10\pxgrid2  
**pxGrid Session details:** Mac Address: 00:0C:29:C1:7B:2C  
 Posture Status: None  
 Endpoint Profile: Windows7-Workstation  
 Right click for more information on: 192.168.1.60

# Addendums

## Adding Log Activity Filter to View Session Information

In this section, a pxGrid app filter is created to view the incoming session information.

Step 1 Select **Log Activity** > **Add Filter** > Select the following:



Step 2 Add the following search criteria:

```
SELECT "pxGrid_adNormalizedUser" AS 'label' , COUNT("pxGrid_adNormalizedUser") AS 'value' FROM
events WHERE LOGSOURCENAME(logsourceid)='pxGrid' AND "pxGrid_EventName"='User Sessions' GROUP
BY "pxGrid_adNormalizedUser" ORDER BY value DESC LIMIT 10 LAST 1 DAYS
```

Step 3 Click **Search**.

Step 4 You should see the **Cisco ISE pxGrid User Sessions**.

Advanced Search: `cid='pxgrid' AND "pxGrid_EventName"='User Sessions' GROUP BY "pxGrid_odNormalizedUser" ORDER BY value DESC LIMIT 10`

Viewing real time events View: Select An Option: Display: Default (Normalized)

Current Filters: Log Source is pxGrid (Clear Filter)

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination
Cisco ISE pxGrid User Sessions	pxGrid	1	Apr 19, 2019, 6:24:1...	User Activity	169.254.2.2	0	169.254.2.2
Cisco ISE pxGrid User Sessions	pxGrid	1	Apr 19, 2019, 6:23:3...	User Activity	169.254.2.2	0	169.254.2.2
Cisco ISE pxGrid User Sessions	pxGrid	1	Apr 19, 2019, 6:16:0...	User Activity	169.254.2.2	0	169.254.2.2
Information Message	System Notification-2 :: qradar...	1	Apr 19, 2019, 6:14:3...	Information	192.168.1.249	0	127.0.0.1
User Logout	SIM Audit-2 :: qradar3	1	Apr 19, 2019, 6:14:3...	SIM User Authentication	169.254.2.2	0	192.168.1.249

## Using an External Certificate Authority

This section illustrates generating certificates for the IBM QRadar pxGrid App, using the ISE internal CA. It is assumed that the ISE pxGrid node and the other ISE nodes are signed by an external CA server. In this example, there are two ISE instances. The ISE26.lab20.com node is the primary ISE instance, and contains the Primary Admin, Primary MNT, Primary pxGrid node, and PSN personas.

The ISE26ca.lab10.com node is the secondary ISE instance, and contains the Secondary Admin, Secondary MNT, Secondary pxGrid, and PSN personas.

Step 1 Verify that the ISE pxGrid, the ISE Admin and ISE MNT nodes are signed by the external CA Server.

Go to **Administration > System > Certificate > System > Certificates > System Certificates**.

Note: The ISE pxGrid and ISE Primary Admin nodes are signed by an external CA Server.

System Certificates

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date
OU=Certificate Services System Certificate, CN=ise26.lab10.com#Certificate Services Endpoint Sub CA - ise26#0002	Not in use		ise26.lab10.com	Certificate Services Endpoint Sub CA - ise26	Tue, 5 Mar 2019	Tue, 6 Mar 2020
Default self-signed saml server certificate - CN=SAML_ise26.lab10.com	SAML		SAML_ise26.lab10.com	SAML_ise26.lab10.com	Wed, 6 Mar 2019	Thu, 5 Mar 2020
CN=ise26.lab10.com#lab10-WIN-N3OR1A7H9KL-CA#0003	Admin, Portal, EAP Authentication, pxGrid, RADIUS DTLS	Default Portal Certificate Group	ise26.lab10.com	lab10-WIN-N3OR1A7H9KL-CA	Sat, 23 Mar 2019	Tue, 23 Mar 2020
OU=ISE Messaging Service, CN=ise26.lab10.com#Certificate Services Endpoint Sub CA - ise26#0001	ISE Messaging Service		ise26.lab10.com	Certificate Services Endpoint Sub CA - ise26	Tue, 5 Mar 2019	Tue, 6 Mar 2020

Step 2 Verify the pxGrid and Admin certificates are signed by the external CA server.

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date
Default self-signed saml server certificate - CN=SAML_ise26.lab10.com	SAML		SAML_ise26.lab10.com	SAML_ise26.lab10.com	Wed, 6 Mar 2019	Thu, 5 Mar 2020
Default self-signed saml server certificate - CN=SAML_ise26ca.lab10.com	Not in use		SAML_ise26ca.lab10.com	SAML_ise26ca.lab10.com	Wed, 6 Mar 2019	Thu, 5 Mar 2020
CN=ise26ca.lab10.com#lab10-WIN-NSOR1A7H9KL-CA#00003	Admin, Portal, EAP Authentication, pxGrid, RADIUS DTLS	Default Portal Certificate Group (j)	ise26ca.lab10.com	lab10-WIN-NSOR1A7H9KL-CA	Wed, 6 Mar 2019	Sat, 6 Mar 2021
OU=Certificate Services System Certificate, CN=ise26ca.lab10.com#Certificate Services Endpoint Sub CA - ise26ca#00004	Not in use		ise26ca.lab10.com	Certificate Services Endpoint Sub CA - ise26ca	Fri, 22 Mar 2019	Tue, 6 Mar 2029
OU=ISE Messaging Service, CN=ise26ca.lab10.com#Certificate Services Endpoint Sub CA - ise26ca#00004	ISE Messaging Service		ise26ca.lab10.com	Certificate Services Endpoint Sub CA - ise26ca	Fri, 22 Mar 2019	Tue, 6 Mar 2029

Step 3 Ensure that the published pxGrid nodes appear and you have pxGrid node connectivity:

Go to **Administration > pxGrid Services**.

Now, you see the following:

Client Name	Description	Capabilities	Status	Client Group(s)	Auth Method
ise-fanout-ise26		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
ise-mnt-ise26ca		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate
ise-pubsub-ise26ca		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
ise-admin-ise26ca		Capabilities(1 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate
ise-fanout-ise26ca		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
ise-bridge-ise26		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate
ise-admin-ise26		Capabilities(4 Pub, 2 Sub)	Online (XMPP)	Internal	Certificate
ise-pubsub-ise26		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
wsa1.lab10.com_start_test_613	ISED	Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate
wsa1.lab10.com613	ISED	Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate
wsa1.lab10.com497	ISED	Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate
wsa1.lab10.com498	ISED	Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate
wsa1.lab10.com315	ISED	Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate
firesightstest-fmc63.lab10.com...		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate
qradar6	pxGrid App for Qradar	Capabilities(0 Pub, 0 Sub)	Offline (XMPP)	ANC	Certificate
iseagent-fmc63.lab10.com-285faf...	GCL for C sample	Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate
pxgridtest		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate

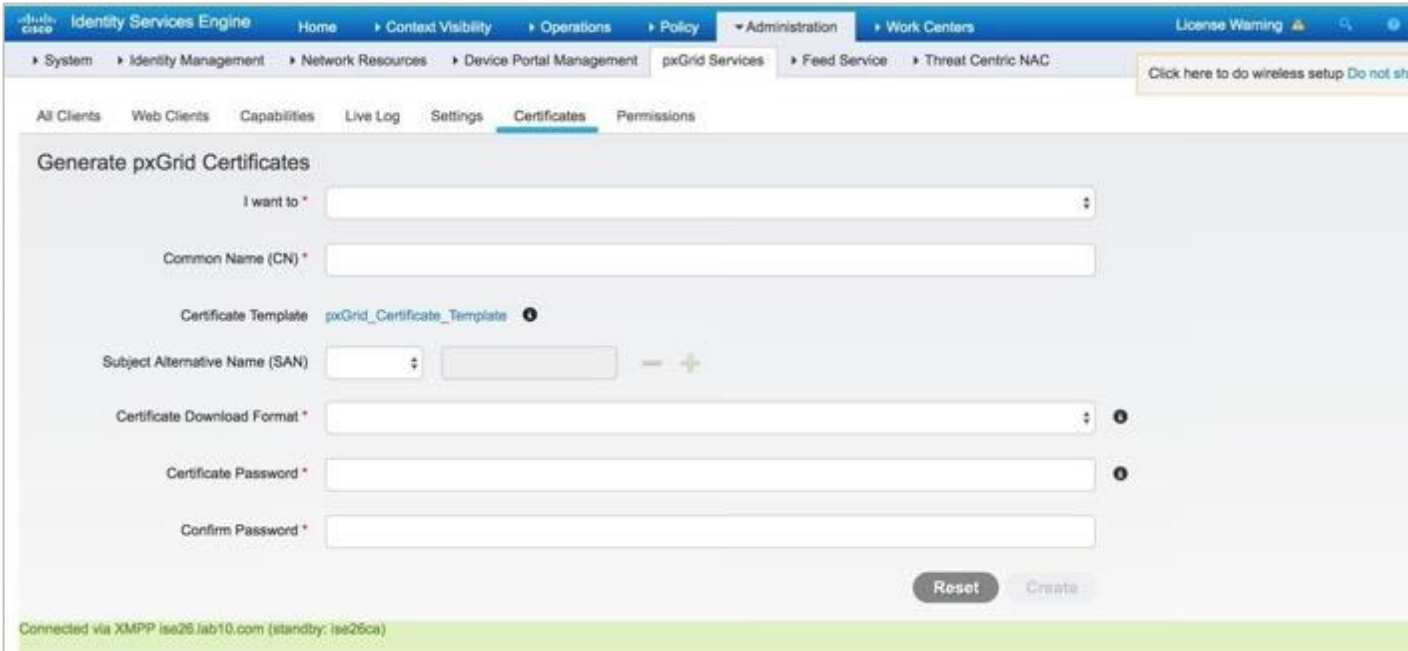
Step 4 Ensure that there is pxGrid connectivity. If in the lower-left corner you see "no connectivity", there is a certificate issue with the ISE pxGrid node, the ISE admin and MNT nodes.

## Generating IBM QRadar Certificate from ISE Internal CA

In this example, the certificate is generated for the IBM QRadar instance using the ISE Internal CA. You can also use opens to create the private key, generate a Certificate Signing Request (CSR), and get this signed by the same customized template that was used for the ISE pxGrid node. To summarize, the customized template must have an EKU of both client and server authentication.

Step 1 Create and generate certificate for the IBM QRadar instance:

Go to **Administration > pxGrid Services > Certificates**.



The screenshot shows the 'Generate pxGrid Certificates' form in the Cisco ISE Administration console. The form is titled 'Generate pxGrid Certificates' and has several input fields and a list. The 'I want to' field is a dropdown menu. The 'Common Name (CN)' field is a text input. The 'Certificate Template' is a dropdown menu showing 'pxGrid\_Certificate\_Template'. The 'Subject Alternative Name (SAN)' field is a list with a dropdown menu and a text input. The 'Certificate Download Format' is a dropdown menu. The 'Certificate Password' and 'Confirm Password' fields are text inputs. At the bottom right, there are 'Reset' and 'Create' buttons. The status bar at the bottom indicates 'Connected via XMPP ise25.lab10.com (standby: ise25ca)'.

Step 2 From the **I want to** list, select **Generate a single certificate without a signing request**.

Step 3 In the **Common Name (CN)** box, enter the Fully Qualified Domain Name (FQDN) of the QRadar Instance.

Step 4 From the **Subject Alternative Name (SAN)** list, select the **IP Address**, and then enter the IP address of the QRadar instance.

Step 5 Provide a description name.

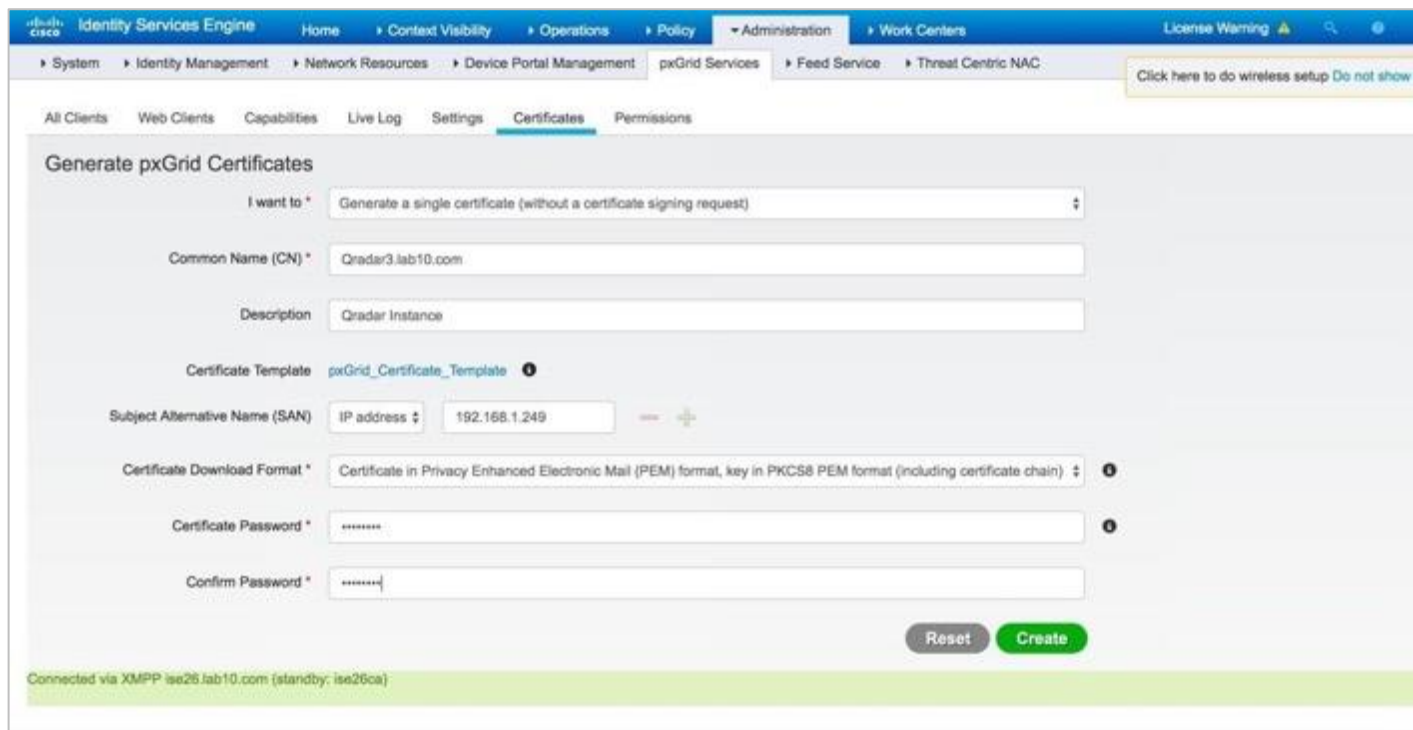
Step 6 From the **Certificate Download Format** list, select the **PEM** format.

Step 7 In the **Certificate Password** box, enter the encryption password.



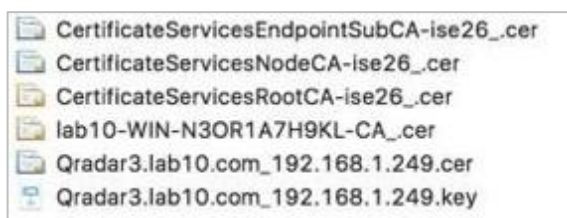


Step 8 In the **Confirm Password** box, enter the password once again.



Step 9 Select **Create**.

Step 10 Copy the zipped file into a folder and unzip the files:



Step 11 Unencrypt the QRadar private key:

Copy the original QRadar .key file to QRadar.key.org file:

```
cp Qradar3.lab10.com_192.168.1.249.key QRadar3.lab10.com_192.168.1.249.key.org
```

Then, run openssl to remove the encryption password from the key.org file. You will get an unencrypted file as defined by the -out parameter. The unencrypted key will be the .key file.

```
QRadar3.lab10.com_192.168.1.249.key.org -out QRadar3.lab10.com_192.168.1.249.key Enter pass phrase for QRadar3.lab10.com_192.168.1.249.key.org:(enter passphrase used when generating certificate) writing RSA key
```

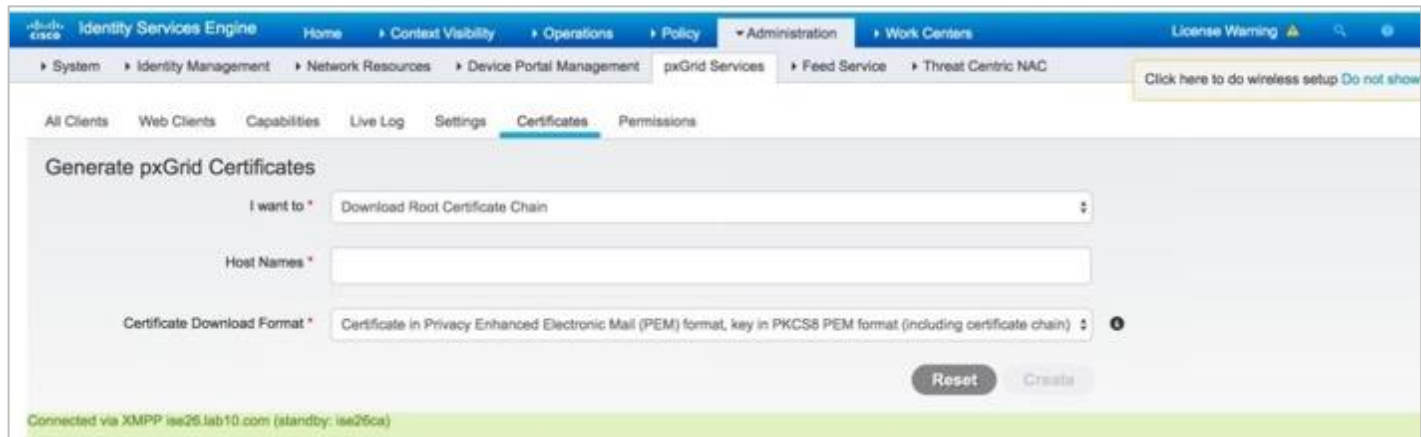
**Note:** Open SSL is on most Linux and MAC operating systems.





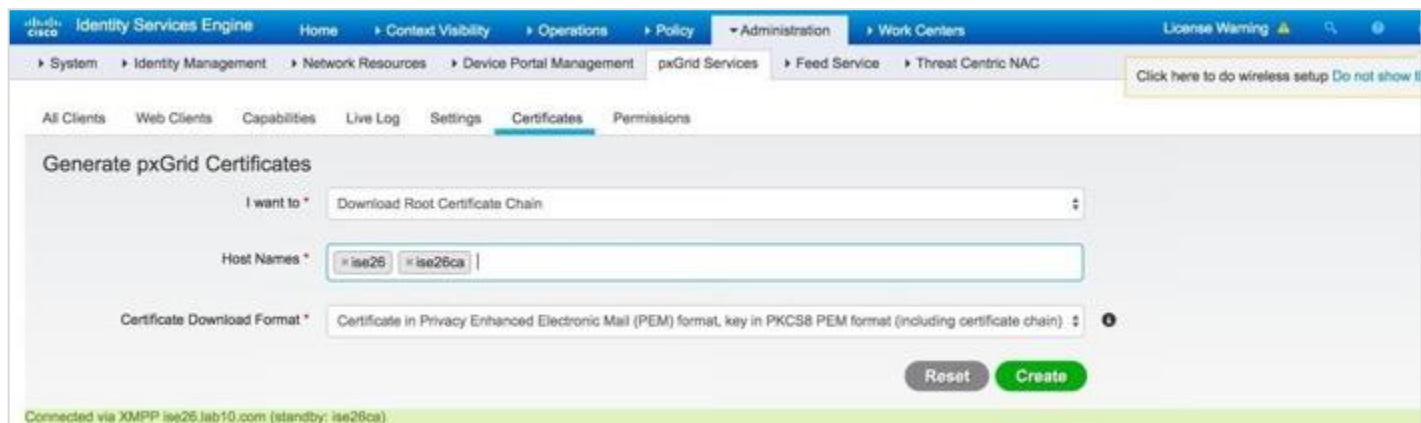
Step 12 To download the certificate root chain:

Go to **Administration > pxGrid services > Certificates**.



Step 13 From the **I want to** list, select **Download Root Certificate Chain**.

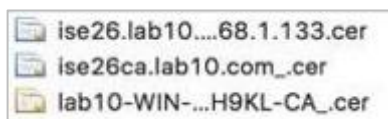
Step 14 In the **Host Names** box, select the **ISE PAN Nodes**:



Step 15 From the **Certificate Downloaded Format** list, select **PEM** format.

Step 16 Select **Create**.

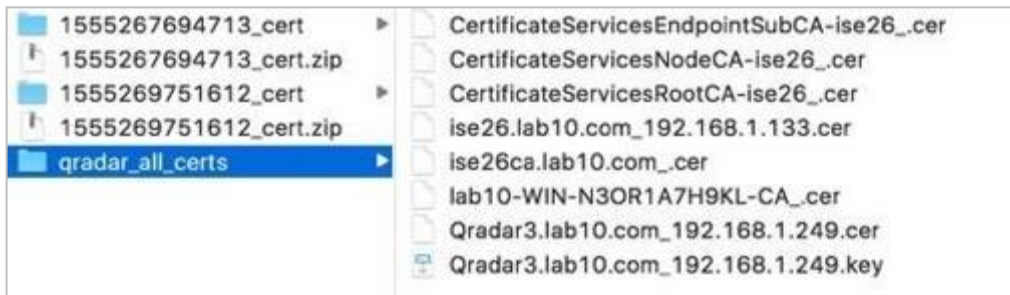
Step 17 Download the zipped file into the same folder where you downloaded the QRadar certificate zipped files. Now, you see the following files:



Step 18 Create a new folder, for example, QRadar\_all\_certs.

Then, copy the ISE identity certificates, for example, ise26.lab10.cer and ise26ca.lab10.com,

the QRadar certificate key-pair files, the external root CA, and the ISE certificate files into this new folder.



Note: Please DO NOT copy the encrypted key.org file into the new folder.

## Troubleshooting

### Cisco ISE pxGrid App pxGrid client not showing under ISE pxGrid Client View

If using an external CA server, upload the CA root certificate and include it in Root CA Certificate file name.

### Cisco ISE pxGrid App pxGrid client not showing under ISE pxGrid Web Client View

Ensure that both the IBM QRadar SIEM and the Cisco ISE pxGrid node are FQDN are resolvable.

Make sure the Forward and Reverse DNS for ISE is defined on the network, And FQDN is resolvable completely from QRadar.

Troubleshoot inside QRadar:

1. Take an SSH to the PxGrid Docker Container on Qradar.
2. For QRadar versions 7.3.3 and above run the commands:

```
1> /opt/qradar/support/recon ps
2> /opt/qradar/support/recon connect <App ID>
```

### Cisco ISE pxGrid Dashboards not populating with ISE Contextual Information

Ensure that the Cisco ISE pxGrid App appears under the ISE pxGrid Web Client View.

### Using the IBM QRadar pxGrid App Logs for Troubleshooting

The QRadar app logs are used for troubleshooting the connection between the QRadar pxGrid App and the ISE pxGrid node.

For example, if the QRadar pxGrid client does not appear under the ISE pxGrid Clients View, you can view the QRadar app log to see if the secure web socket connection is established between the QRadar app and the ISE pxGrid node.

Step 1 To see the QRadar apps, type the following:

```
[root@QRadar3 support]# /opt/qradar/support/recon ps
```

PORT	CONTAINER	IMAGE	STATUS	appID	NAME
32768	28ac62f3a3d8	2cabd65ea8554650b3990bbdd83f59d8	RUNNING	1201	Cisco ISE pxGrid

Step 2 Use **Recon connect** to retrieve the container contents:

```
[root@QRadar3 support]# /opt/qradar/support/recon connect <<appID>> bash-4.1# ls
```

```
App  Dev          home lib64 opt    root  selinux  start_container.sh Sys      Usr
Bin  etc            init  media  proc    run.py  src_deps  start_flask.sh  Tmp      var
boot executeapp.bat lib   mnt    qpython sbin    srv      store          upgradePath.sh
```

**Note:** For QRadar versions 7.3.2 and above, run the commands:

```
1> /opt/qradar/support/recon ps
2> /opt/qradar/support/recon connect <App ID>
```

Use tail to view the app.log: `bash-4.1# tail -f store/log/app.log`

**Step 3** A successful connection will look like this:

```
2019-04-14 21:14:43,812 [abstract_qpylib.log] [Thread-1] [INFO] - 127.0.0.1
[APP_ID/1201][NOT:0000006000] Primary Server: ise26.lab10.com 2019-04-14 21:14:43,812
[abstract_qpylib.log] [Thread-1] [INFO] - 127.0.0.1
[APP_ID/1201][NOT:0000006000] Secondary Server: 192.168.1.138
2019-04-14 21:14:43,813 [abstract_qpylib.log] [Thread-1] [INFO] - 127.0.0.1
[APP_ID/1201][NOT:0000006000] Current Active Server: primary
2019-04-14 21:14:48,933 [abstract_qpylib.log] [Thread-1] [INFO] - 127.0.0.1
[APP_ID/1201][NOT:0000006000] Account Activation Status: 200
2019-04-14 21:14:48,933 [abstract_qpylib.log] [Thread-1] [INFO] - 127.0.0.1
[APP_ID/1201][NOT:0000006000] Performing service lookup for:com.cisco.ise.pubsub
19-04-14 21:14:49,280 [abstract_qpylib.log] [Thread-1] [INFO] - 127.0.0.1
[APP_ID/1201][NOT:0000006000] Creating WebSocketClient...
2019-04-14 21:14:49,282 [abstract_qpylib.log] [Thread-1] [INFO] - 127.0.0.1
[APP_ID/1201][NOT:0000006000]
Connecting to websocket
2019-04-14 21:14:49,321 [abstract_qpylib.log] [Thread-1] [INFO] - 127.0.0.1
[APP_ID/1201][NOT:0000006000] Connected and about to running for ever...
2019-04-14 21:14:49,322 [abstract_qpylib.log] [WebSocketClient] [INFO] - 127.0.0.1
[APP_ID/1201][NOT:0000006000] Subscribe request sent to websocket for
/topic/com.cisco.ise.session
2019-04-14 21:14:49,322 [abstract_qpylib.log] [WebSocketClient] [INFO] - 127.0.0.1
[APP_ID/1201][NOT:0000006000] Subscribe request sent to websocket for
/topic/com.cisco.ise.radius.failure
2019-04-14 21:14:49,323 [abstract_qpylib.log] [WebSocketClient] [INFO] - 127.0.0.1
[APP_ID/1201][NOT:0000006000] Subscribe request sent to websocket for
/topic/com.cisco.ise.config.anc.status
2019-04-14 21:14:49,324 [abstract_qpylib.log] [WebSocketClient] [INFO] - 127.0.0.1
[APP_ID/1201][NOT:0000006000] Subscribe request sent to websocket for
/topic/com.cisco.ise.mdm.endpoint
```

**Note:** You should see a successful connection to the primary server connection and an activation status. You should also see a subscription to the pxGrid topic over a secure Websockets connection. Please disregard the \*crypto messages and the unauthorized messages.

**Step 4** If you do not see a successful connection where there is no Primary server response, or the connection keeps switching between the primary and secondary pxGrid nodes, this can be an indication that some of the services have not started or may be in an inconsistent state.

```

2019-04-14 20:20:57,799 [abstract_qpylib.log] [Thread-100] [INFO] - 127.0.0.1
[APP_ID/1201][NOT:0000006000] Primary Server Response: None
2019-04-14 20:22:08,369 [abstract_qpylib.log] [Thread-103] [INFO] - 127.0.0.1
[APP_ID/1201][NOT:0000006000] Received request to test primary files
2019-04-14 20:22:08,374 [abstract_qpylib.log] [Thread-103] [INFO] - 127.0.0.1
[APP_ID/1201][NOT:0000006000] Trying http connection ..... 2019-04-14 20:22:13,380
[abstract_qpylib.log] [Thread-103] [INFO] - 127.0.0.1 [APP_ID/1201][NOT:0000006000] Wrapping SSL
socket .....

```

You can stop or restart your app by using the IBM QRadar GUI Application Framework REST API endpoints. As a reference, see [this page](#).

#### Step 5 Stop the pxGrid App:

```
POST /api/gui_app_framework/applications/{app_id}?status="STOPPED"
```

#### Step 6 Start or restart the pxGrid app:

a. Start the app: `POST /api/gui_app_framework/applications/{app_id}?status="RUNNING"`

b. Restart the app:

1. Copy the PxGrid app ID: `ssh to QRadar >> /opt/qradar/support/recon ps.`
2. In the GUI, open the QRadar Menu bar.
3. Click the **Interactive API for Developer**.
4. Click the drop button of the latest version `>>gui_app_framework>>applications>>application_id.`
5. Under POST, enter the **application\_id**.
6. Update the status to **STOPPED**, then **RUNNING**, to stop and start the app.

Step 7 Review the QRadar app log again or check to see if the pxGrid client appears under Web Clients on the ISE pxGrid node view.

Step 8 If you are stuck in the loading page, click **Reset** and change the date, to reflect a day before and a day after. There should be real-time authentications in ISE, so the session information can be seen in the IBM QRadar App.

## Here are some more log issues with connectivity:

### pxGrid app pending state in the logs due to ISE pxGrid client not being approved.

This is showing the QRadar ISE pxGrid app as pending. You can see this under `admin > pxGrid > All Clients`. You should not see the app listed under Web Clients as it hasn't been approved. You can manually approve it in the All clients page (this was noted in the setup section of the guide).

**Note:** In order to automatically approve, for future connections you can allow under `pxGrid > Settings >` check the box to automatically approve certificate based connections. This is entirely up to the administrator choice depending on security concerns. Someone would have to create a certificate that ISE trusts either through external or internal PKI.

```
2021-02-02 17:35:00,088 [abstract_qpylib.log] [Thread-740] [INFO]
- 127.0.0.1[APP_ID/1102][NOT:0000006000] Checking response got from primary server
2021-02-02 17:35:00,088 [abstract_qpylib.log] [Thread-740] [INFO]
- 127.0.0.1[APP_ID/1102][NOT:0000006000] Checking status from primary server: 200
2021-02-02 17:35:00,088 [abstract_qpylib.log] [Thread-740] [INFO]
- 127.0.0.1[APP_ID/1102][NOT:0000006000] Checking response from primary server:
{"accountState":"PENDING","version":"2.0.3.14"}
```

### After its connected.

```
2021-02-02 20:40:00,097 [abstract_qpylib.log] [Thread-1193] [INFO]
- 127.0.0.1[APP_ID/1102][NOT:0000006000] Checking response from primary server:
{"accountState":"ENABLED","version":"2.0.3.14"}
```

### Not able to connect to ISE node from Qradar ISE pxGrid app.

These logs were seen when pointing Qradar ISE pxGrid app to the admin node of ISE (should be pointing to a pxGrid node).

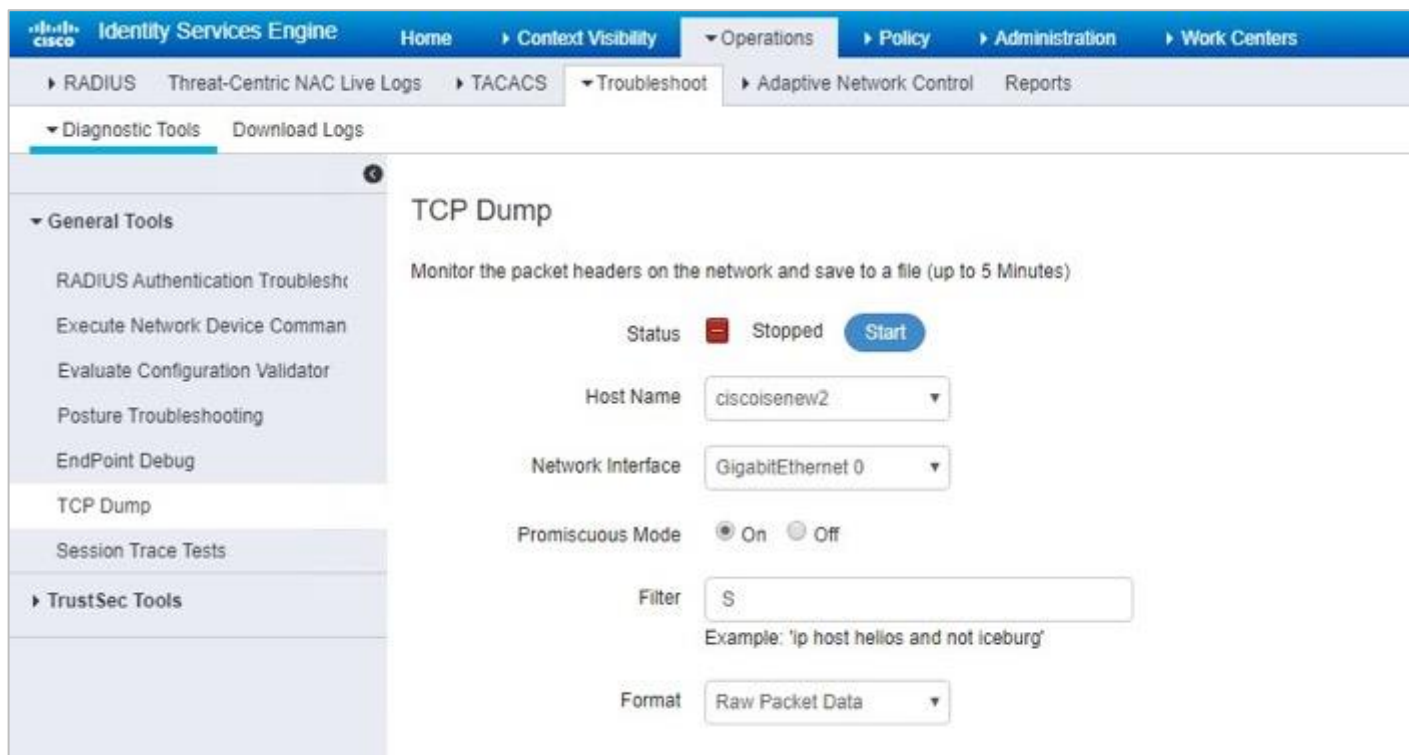
```
2021-02-02 17:20:04,148 [abstract_qpylib.log] [Thread-707] [INFO]
- 127.0.0.1[APP_ID/1102][NOT:0000006000] Client Name Jabe02022021
2021-02-02 17:20:04,148 [abstract_qpylib.log] [Thread-707] [INFO]
- 127.0.0.1[APP_ID/1102][NOT:0000006000] URL /pxgrid/control/ServiceLookup
2021-02-02 17:20:04,148 [abstract_qpylib.log] [Thread-707] [INFO]
- 127.0.0.1[APP_ID/1102][NOT:0000006000] Service Name com.cisco.ise.pubsub
2021-02-02 17:20:04,191 [abstract_qpylib.log] [Thread-707] [ERROR]
- 127.0.0.1[APP_ID/1102][NOT:0000003000] Exception reported from invoke_cisco_ws_api method: <type
'exceptions.ValueError'>
2021-02-02 17:20:04,191 [abstract_qpylib.log] [Thread-707] [ERROR]
- 127.0.0.1[APP_ID/1102][NOT:0000003000] Exception reported from invoke_cisco_ws_api method: No JSON
object could be decoded
2021-02-02 17:20:04,191 [abstract_qpylib.log] [Thread-707] [ERROR]
- 127.0.0.1[APP_ID/1102][NOT:0000003000] Exception reported from subscribefromwebsocket method: <type
'exceptions.ValueError'>
2021-02-02 17:20:04,192 [abstract_qpylib.log] [Thread-707] [ERROR]
- 127.0.0.1[APP_ID/1102][NOT:0000003000] Exception reported from subscribefromwebsocket method: No JSON
object could be decoded
2021-02-02 17:25:00,032 [abstract_qpylib.log] [Thread-718] [INFO]
- 127.0.0.1[APP_ID/1102][NOT:0000006000] Checking http connection with primary server
2021-02-02 17:25:00,036 [abstract_qpylib.log] [Thread-718] [INFO]
- 127.0.0.1[APP_ID/1102][NOT:0000006000] Checking connection with primary server using PROTOCOL_SSLv23
```

## TCP Dump to Analysis Failed Certificate Exchange in ISE

In this section, we are going to see how we can download .pcap file for analysis from ISE, in case the certificate exchange fails, or the Client is not subscribing to topics.

Step 1 Navigate to **Operation > Troubleshoot > Diagnostic Tools > TCP Dump**.

Step 2 From the **Format** drop-down list, select the **Raw Packet Data**, and then click **Start**.



Step 3 While you keep the TCP Dump running, log in to QRadar and reconfigure the App settings page.

Step 4 Stop the dump collection and download the .pcap file.

Step 5 Analyze the .pcap file using Wireshark and observe if there are any packets being dropped, Certificate exchange failing, or Unknown CA alert.



## TCP Dump to Check if pxGrid Logs are Available in QRadar

In this section, we are going to run few tcpdump commands in QRadar, to verify if pxGrid Logs are available in QRadar database, if the pxGrid Dashboard is not loading with data, or the Log Activity search does not show the pxGrid Events.

Step 1 Take SSH to QRadar console.

Step 2 Find the PxGrid docker IP:

```
/opt/qradar/support/recon ps  
  
/opt/qradar/support/recon connect <<App ID>>  
  
ifconfig (Ip associates with the inet addr)
```

Step 3 Run this command `> tcpdump -nnAs0 -i any host <<PxGrid Docker Ip Address>> and port 514`. Wait for few minutes if the Events are available on your ISE for the subscribed topic, then you should see events showing up in LEEF Format.

## Uploading Logs with the case

Upload the following logs with the case can help our engineers assist you further:

- qradar.error
  - startup.log
  - app.log
1. To get **qradar.error** logs, first we need to SSH to QRadar Console.  
QRadar error logs are available in this location: **/var/log/qradar.error**
  2. To get **startup.log** and **app.log**, first we need to get inside pxGrid App docker:
    1. Login to QRadar console (putty/terminal).
    2. Get the pxGrid APP ID execute this command: `/opt/qradar/support/recon ps`.
    3. The startup.log and app.log are available in this location: **/store/docker/volumes/qapp-<<App ID>>/log**.
    4. Replace App ID with pxGrid App ID from Step 2.
    5. For example: `/store/docker/volumes/qapp-110`.