



Cisco ISE pxGrid App 2.0.0 for IBM QRadar SIEM

Updated: Jason Kunst

Updated - February 2021

Table of Contents

About This Document.....	4
Solution Overview	5
Technical Details	6
Cisco ISE pxGrid Installation.....	8
Generating the Cisco ISE pxGrid App Certificate	12
Installing Cisco ISE pxGrid App.....	16
Configuring pxGrid Integration on QRadar	23
Setup Indexing in QRadar	28
Cisco ISE pxGrid App Dashboard Panels	30
Search Functionality	30
Passed Authentications	32
Failed Authentications	35
User Panel	36
Failure Reason Panel	38
Device Type Panel.....	40
Locations Panel.....	43
Devices	46
Compliance	50
TrustSec	53
Mobile Device Management (MDM)	55
ANC Details.....	56
Configuring Cisco ISE Adaptive Network Control Policies	57
Configuring Default ANC policies for Cisco ISE pxGrid App	57
Adding ANC Policies to ISE Policy Sets	59
Performing Cisco ISE ANC Mitigation Actions Through Cisco ISE pxGrid App Dashboard Panel	61

Configuring IBM QRadar for Cisco ISE Syslog Events	67
Configuring Cisco ISE Syslog Events.....	69
Performing ISE ANC Mitigation Actions Through IBM QRadar Syslog Events	72
Creating Custom Field for Framed IP Address ISE Syslog Event.....	72
ANC Mitigation Syslog Event Example	80
Hovering Over IBM QRadar Syslog IP Address for ISE Contextual Information	86
IBM QRadar Cisco ISE pxGrid Offense Rule.....	87
Verify pxGrid offense rule via Log Activity	88
Verify pxGrid offense rule via Offenses Dashboard	90
Taking ISE ANC mitigations from Offenses Dashboard.....	90
Addendums.....	96
Adding Log Activity Filter to View Session Information	96
Using an External Certificate Authority	97
Generating IBM QRadar Certificate from ISE Internal CA	100
Troubleshooting	105
Cisco ISE pxGrid App pxGrid client not showing under ISE pxGrid Client View	105
Cisco ISE pxGrid App pxGrid client not showing under ISE pxGrid Web Client View	105
Cisco ISE pxGrid Dashboards not populating with ISE Contextual Information.....	105
ANC Mitigation Actions not appearing in Dashboards	105
Using the IBM QRadar pxGrid App Logs for Troubleshooting.....	106
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 v2.0+ for IBM the QRadar SIEM.

The supported platforms are:

- IBM QRadar SIEM 7.3.1 patch 7 and higher
- Cisco ISE 2.4 and higher with latest patch

Note: Please keep up with latest patches and recommended releases, as of October 2020 it is ISE 2.7 patch 2

Validation has been done with the following for this release:

- The ISE internal CA was used for generating the pxGrid certificates for the Cisco ISE pxGrid App.
- ISE 2.4 Standalone with IBM QRadar SIEM 7.3.1 Patch 7
- ISE 2.7 patch 2 standalone/distributed with IBM QRadar SIEM 7.4.0, should work with 7.4.x

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

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 be 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 authentication 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/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 installs, 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.

At the bottom of the screen, you should see a connection for distributed deployment:

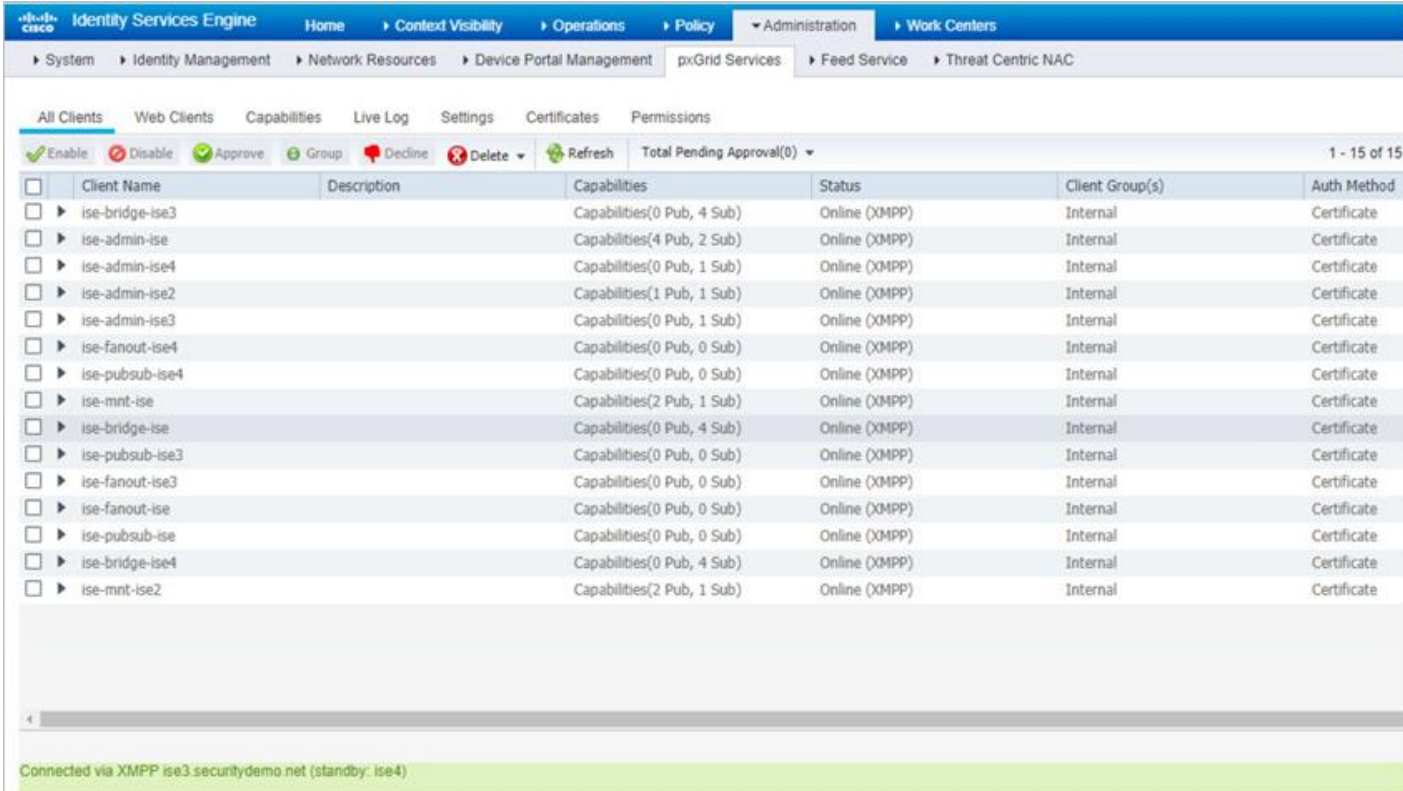
Connected via XMPP ise3.securitydemo.net (standby: ise4)

The following image is a single standalone:

Client Name	Connect To	Session Id	Certificate	Subscriptions	Publications	IP Address	Status
ise-fanout-ise24k	ise24k	ise24k:0	CN=ise24k	/topic/wildcard		127.0.0.1	ON
ise-mnt-ise24k	ise24k	ise24k:1	CN=ise24k	/topic/com.cisco.ise.se...	/topic/com.cisco.ise.se...		ON
ise-fanout-ise24k	ise24k	ise24k:2	CN=ise24k	/topic/distributed	/topic/distributed		ON
ise-admin-ise24k	ise24k	ise24k:3	CN=ise24k				ON
ise-bridge-ise24k	ise24k	ise24k:5	CN=ise24k				ON
CiscoSEpxGridApp	ise24k	ise24k:6	CN=qradar	/topic/com.cisco.ise.se...			ON

Subscriptions for CiscoSEpxGridApp: /topic/com.cisco.ise.session, /topic/com.cisco.ise.radius.failure, /topic/com.cisco.ise.config.anc.status, /topic/com.cisco.ise.mdm.endpoint

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



Client Name	Description	Capabilities	Status	Client Group(s)	Auth Method
ise-bridge-ise3		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate
ise-admin-ise		Capabilities(4 Pub, 2 Sub)	Online (XMPP)	Internal	Certificate
ise-admin-ise4		Capabilities(0 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate
ise-admin-ise2		Capabilities(1 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate
ise-admin-ise3		Capabilities(0 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate
ise-fanout-ise4		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
ise-pubsub-ise4		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
ise-mnt-ise		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate
ise-bridge-ise		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate
ise-pubsub-ise3		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
ise-fanout-ise3		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
ise-fanout-ise		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
ise-pubsub-ise		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
ise-bridge-ise4		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate
ise-mnt-ise2		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate

Connected via XMPP ise3.securitydemo.net (standby: ise4)

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 done was 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.

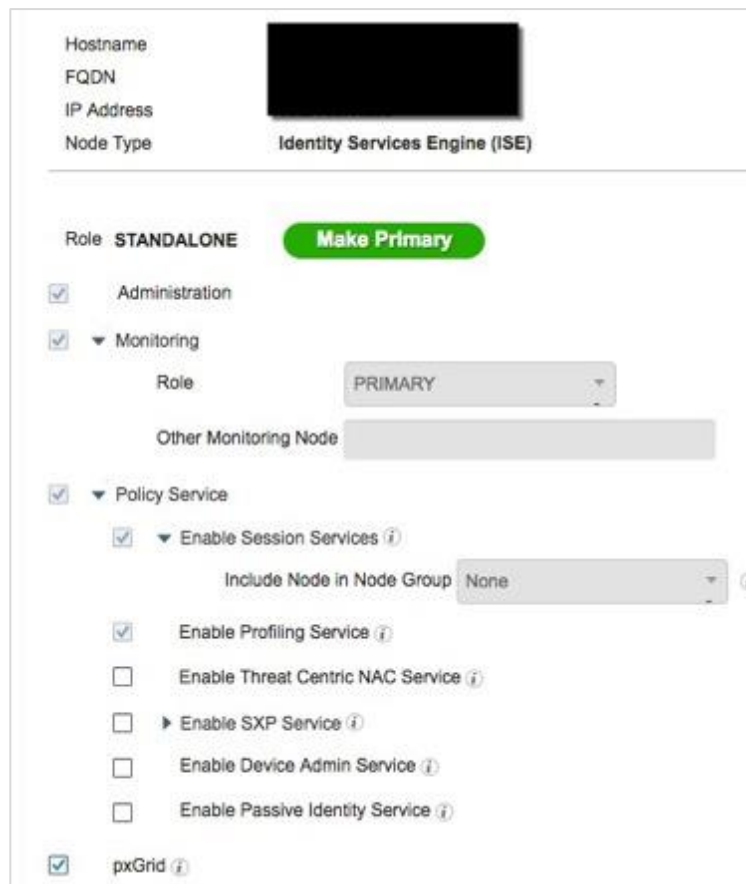
The Cisco ISE pxGrid App uses pxGrid 2.0, which uses WebSocket, REST API, and STOMP messaging protocol for pxGrid operation and thus supported since Cisco ISE 2.

Cisco ISE pxGrid Installation

Make sure that you have installed Cisco Identity Services (ISE) 2.4 or higher and it is in a stand-alone 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 [How to Configure pxGrid in ISE Production Environments](#).

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.

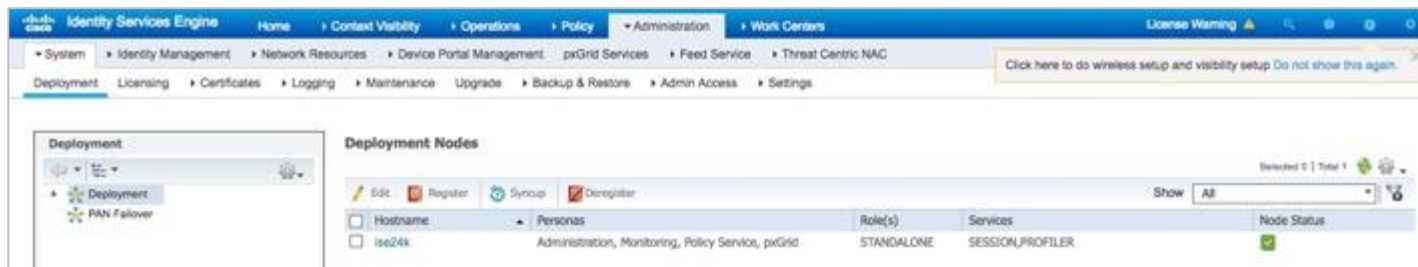
Step 1 Select **Administration > System Deployment > Edit the ISE node > Enable pxGrid**



The screenshot shows the configuration page for an Identity Services Engine (ISE) node. The node type is 'Identity Services Engine (ISE)'. The role is set to 'STANDALONE', and there is a 'Make Primary' button. The 'Administration' role is checked. Under 'Monitoring', the role is set to 'PRIMARY'. Under 'Policy Service', 'Enable Session Services' is checked, and 'Include Node in Node Group' is set to 'None'. Other services like 'Enable Profiling Service', 'Enable Threat Centric NAC Service', 'Enable SXP Service', 'Enable Device Admin Service', and 'Enable Passive Identity Service' are unchecked. The 'pxGrid' checkbox is checked.

Step 2 Select **Save**

You should see the following:



Recommended Distributed deployment example:



Step 3 Select **Administration > pxGrid Services**

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

Note: XMPP is for pxGrid 1.0 and for releases prior to ISE 3.0 the All Clients page doesn't provide the best view. You should look at the Web Clients view below.

Step 4 Select **Web Clients** and verify the published nodes appear:

Note: This is validating pxGrid 2.0 connections. You should see admin, mnt, and pxGrid nodes have connections with each other. They should all be **ON**.

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 [How to Configure pxGrid in ISE Production Environments](#).

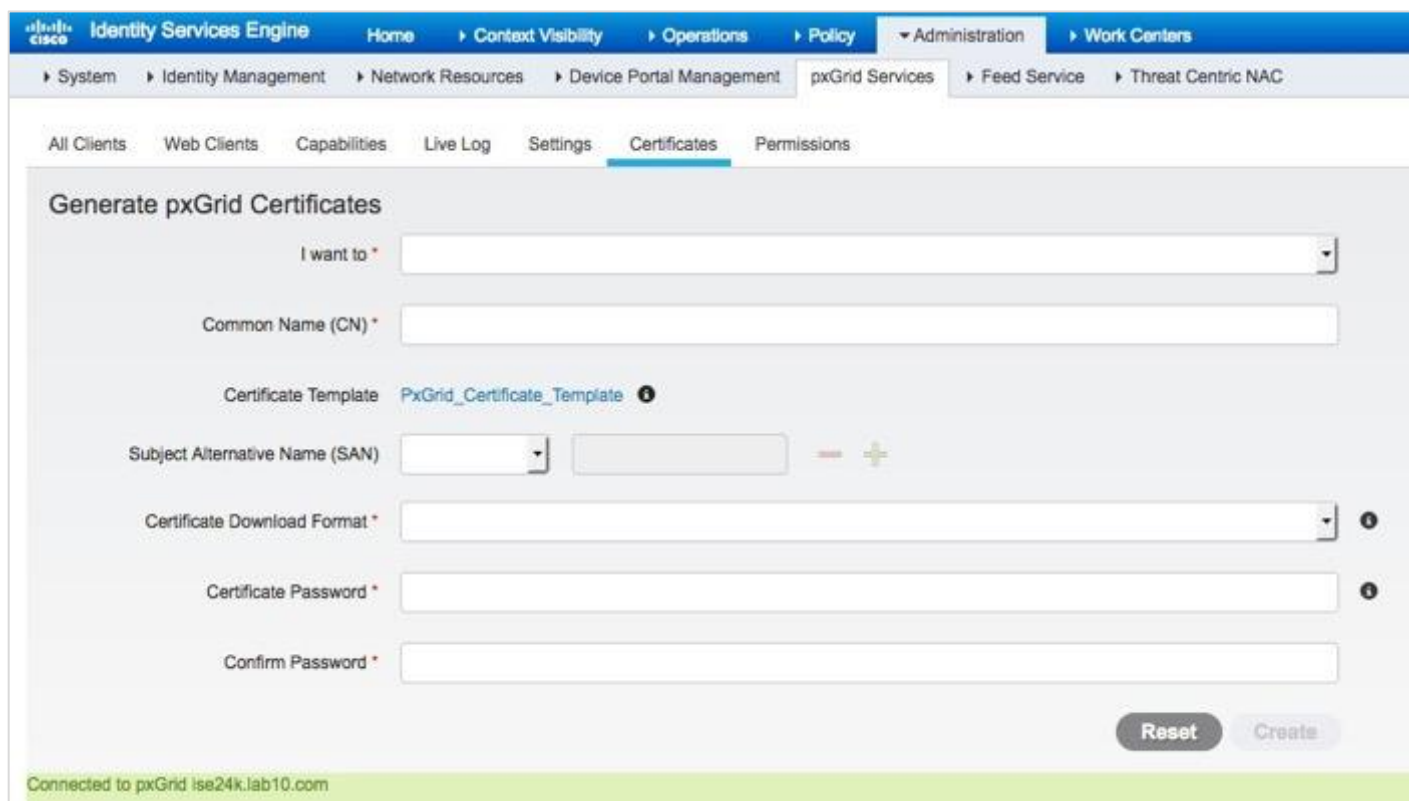
For more information on certificates please reference [this section](#) under [cs.co/ise-guides](#).

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

PKCS12 files are not supported. This is due to non-support in the Python libraries used in the Cisco ISE pxGrid client.

Step 1 Select **Administration > pxGrid Services > Certificates**

You should see the following:



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Administration > pxGrid Services > Certificates. The 'Generate pxGrid Certificates' form is displayed with the following fields and options:

- I want to ***: A dropdown menu.
- Common Name (CN) ***: A text input field.
- Certificate Template**: A dropdown menu showing 'PxGrid_Certificate_Template' with an information icon.
- Subject Alternative Name (SAN)**: A dropdown menu, a text input field, and '+' and '-' buttons.
- Certificate Download Format ***: A dropdown menu with an information icon.
- Certificate Password ***: A text input field with an information icon.
- Confirm Password ***: A text input field.

At the bottom right of the form are 'Reset' and 'Create' buttons. A status bar at the bottom left indicates 'Connected to pxGrid ise24k.lab10.com'.

Step 2 Type the following:

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

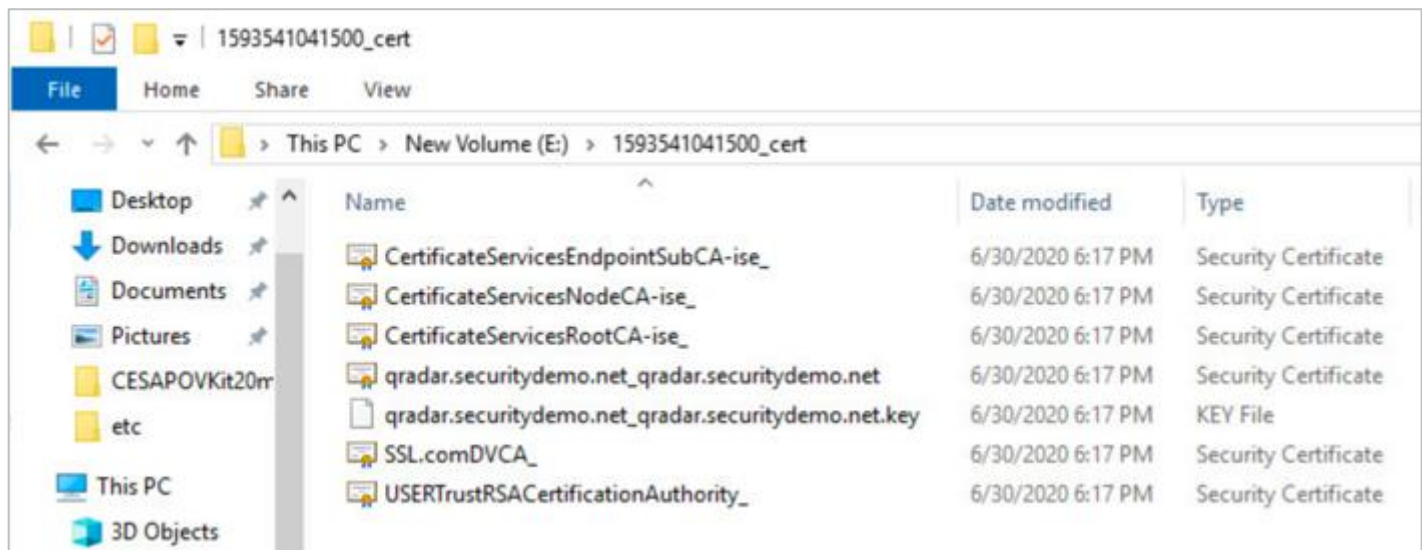
Confirm Password: xxxxxx

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:



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

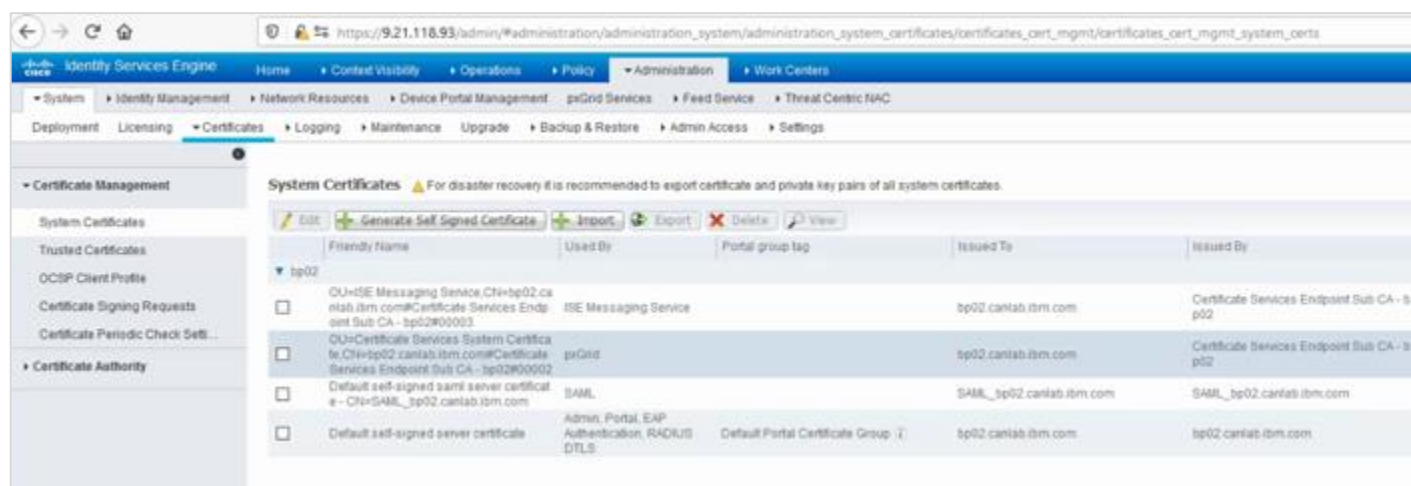
```
qradar.securitydemo.net_qradar.securitydemo.net.cer
qradar.securitydemo.net_qradar.securitydemo.net.key
```

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 best practice. If it is move 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 as ISE is aware of the certificates it issues and the associated certificate chain.



Step 5 Decrypt the file on the QRadar box:

- a. Using WinSCP Copy the `qradar.securitydemo.net_qradar.securitydemo.net.key` to the QRadar Setup

Note: The certificate might also have the IP address since it was part of the SAN above.

- b. SSH to your QRadar setup and make sure you're in the root directory
- c. Run the following to remove the encryption password when importing into the Cisco ISE pxGrid App:

```
mv qradar.securitydemo.net_qradar.securitydemo.net.key
qradar.securitydemo.net_qradar.securitydemo.net.key.old
openssl rsa -in qradar.securitydemo.net_qradar.securitydemo.net.key.old-out
qradar.securitydemo.net_qradar.securitydemo.net.key
```

You will be prompted to enter the encryption password when generating the certificate in ISE

Note: The Cisco ISE pxGrid App does not support encryption due to the Python libraries

d. Refresh your WinSCP and copy the key file back (not the .org) to the same windows location overwriting the key file

e. Close your WinSCP and SSH sessions to QRadar server

Note: You will need to upload these six certificates when configuring the Cisco ISE pxGrid App for pxGrid integration

Installing Cisco ISE pxGrid App

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

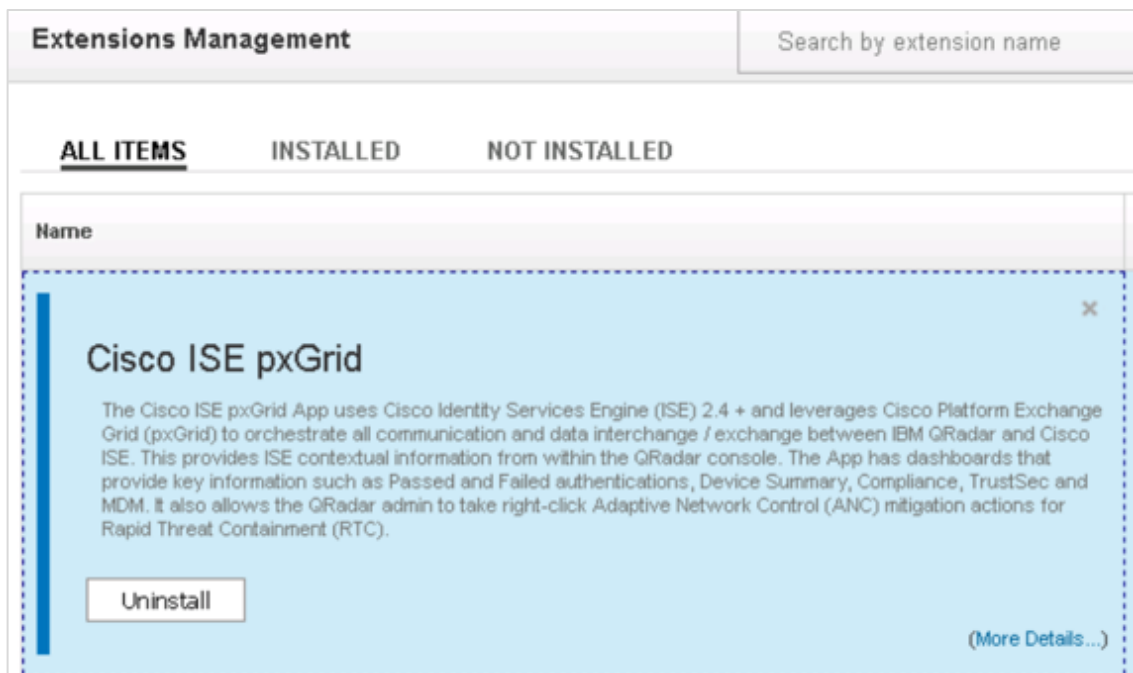
To download the app, please visit the [IBM App Exchange](#).

Note: It is assumed that [QRadar Ver 7.3.1p7](#) and above has been installed along with Patch 7.

If user is upgrading the Cisco ISE pxGrid QRadar App from ver1.x.x, we recommend users to uninstall the old app (1.x.x) and install the latest version.

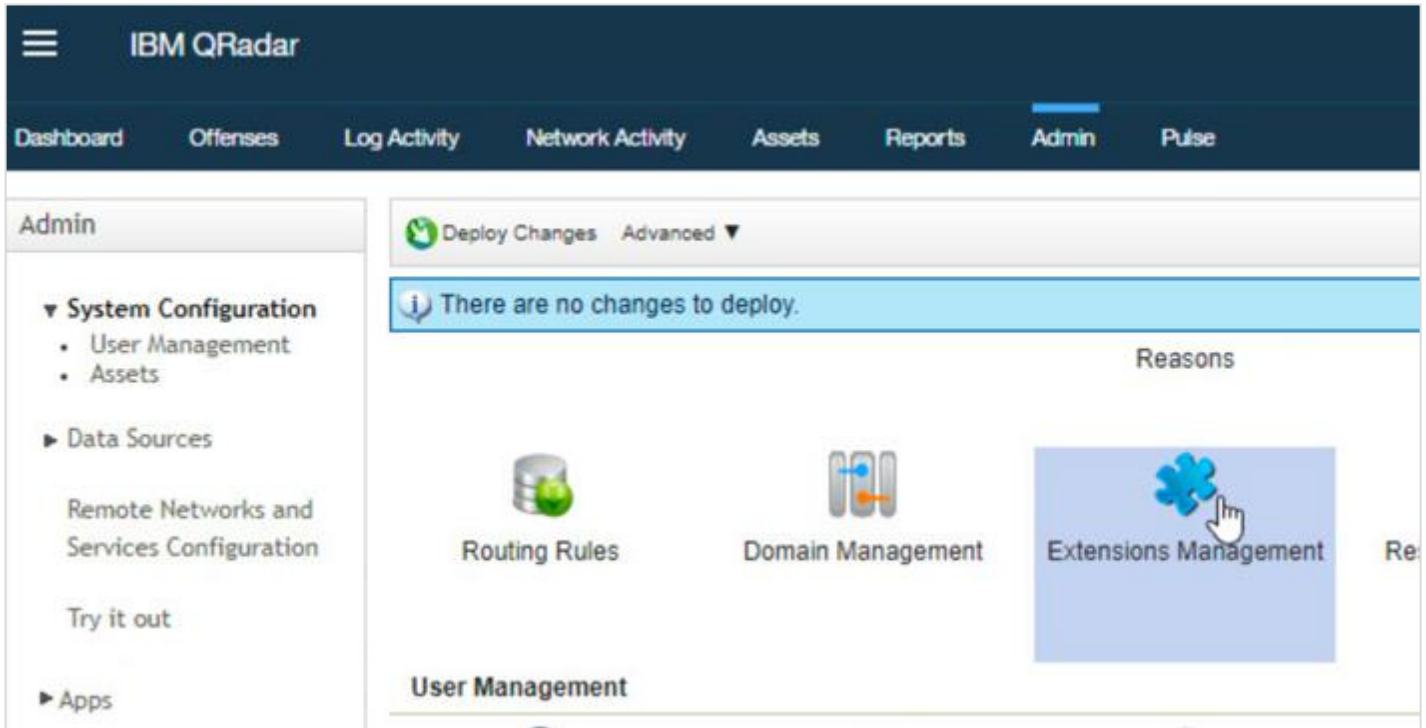
To uninstall the old app:

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

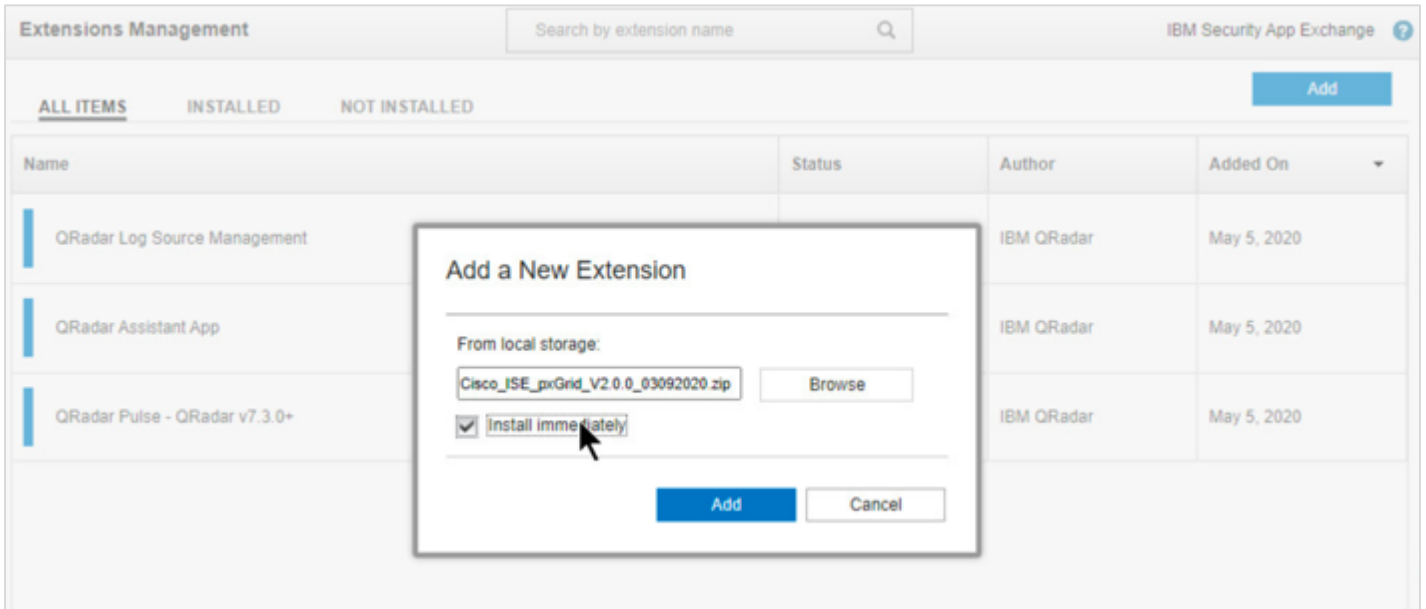


Step 1 Install the extension:

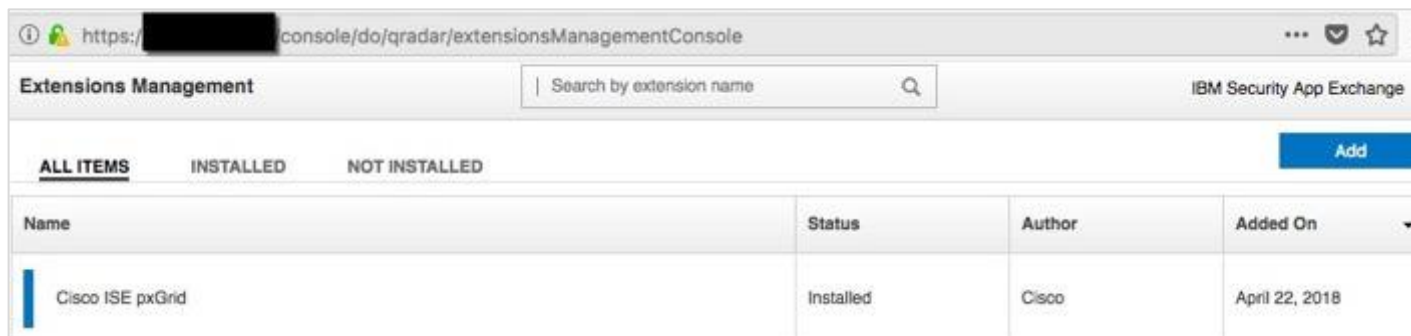
- a. From IBM QRadar, select **Admin > Extensions Management**



b. Click **Add** > Upload the signed Cisco ISE pxGrid App > Select **Install Immediately**



c. After the install, you should see the following:



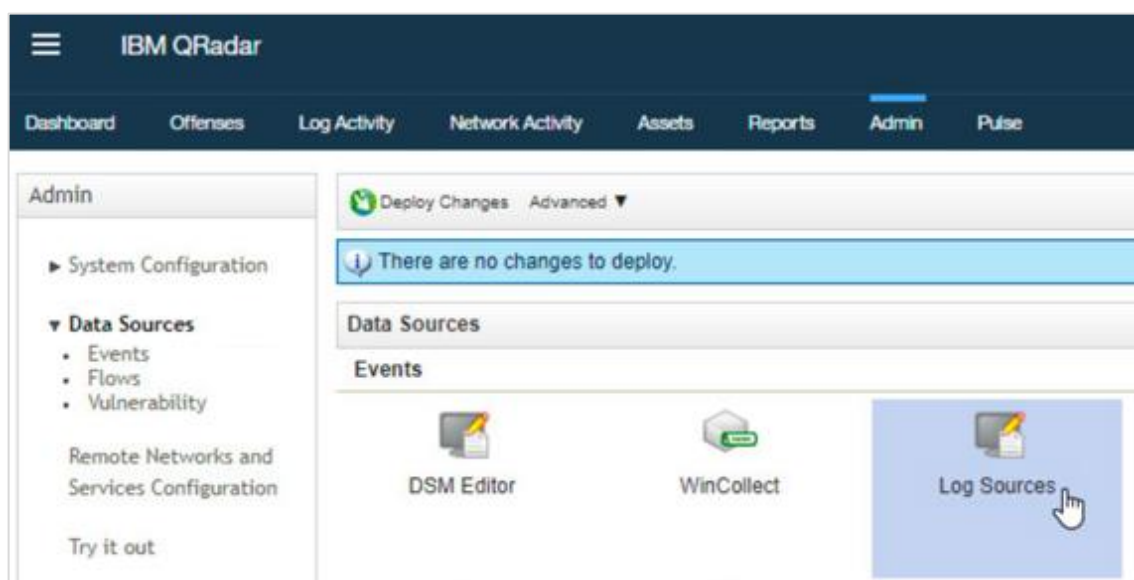
Extensions Management			
Search by extension name			
ALL ITEMS			INSTALLED
NOT INSTALLED			Add
Name	Status	Author	Added On
Cisco ISE pxGrid	Installed	Cisco	April 22, 2018

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 button

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

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

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

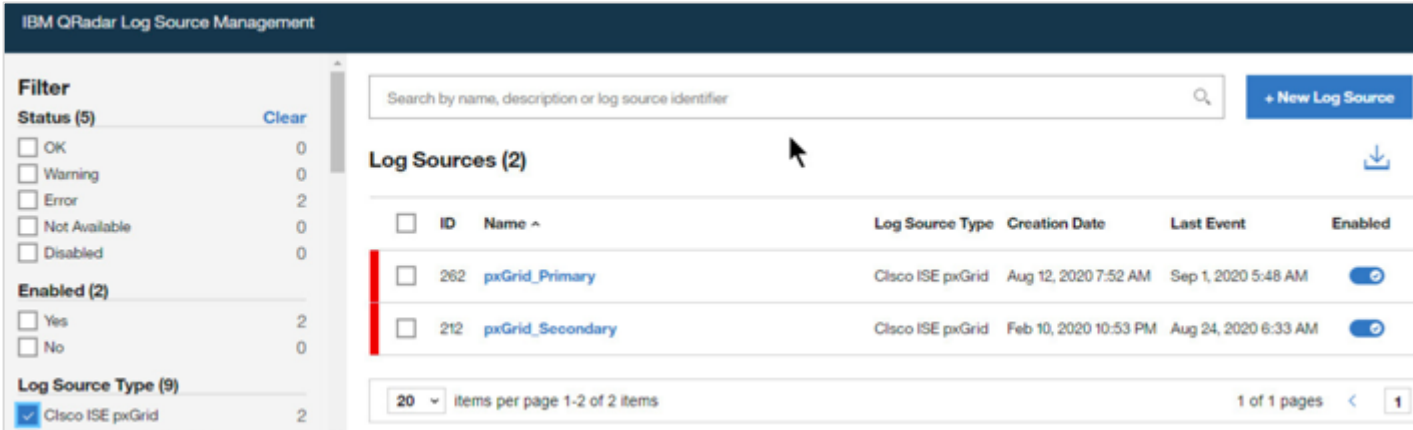
ERROR - Events have not been received from this Log Source in over 720 minutes.

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

Filter

Status (5) [Clear](#)

- OK 0
- Warning 0
- Error 2
- Not Available 0
- Disabled 0

Enabled (2)

- Yes 2
- No 0

Log Source Type (9)

- Cisco ISE pxGrid 2

Search by name, description or log source identifier

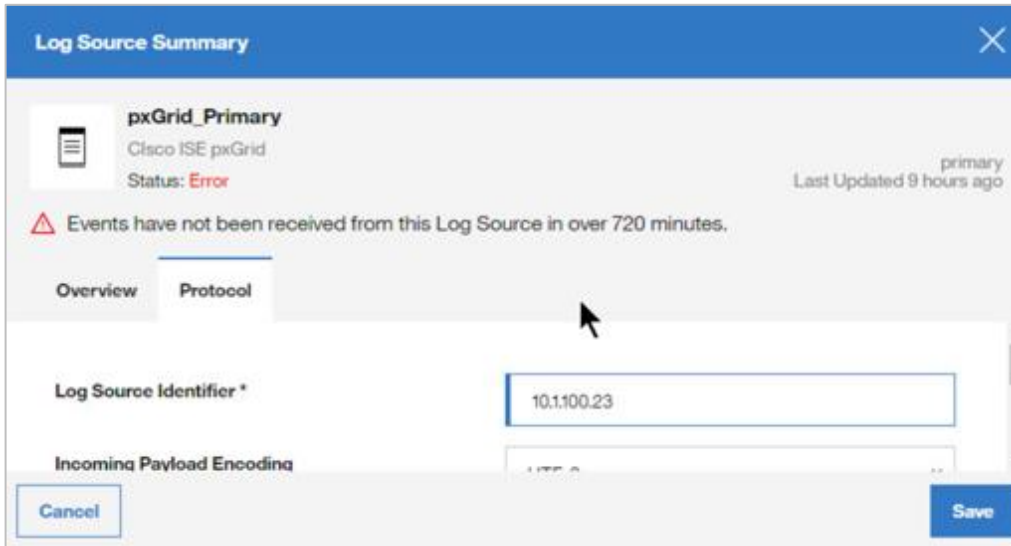
Log Sources (2)

<input type="checkbox"/>	ID	Name ^	Log Source Type	Creation Date	Last Event	Enabled
<input type="checkbox"/>	262	pxGrid_Primary	Cisco ISE pxGrid	Aug 12, 2020 7:52 AM	Sep 1, 2020 5:48 AM	<input checked="" type="checkbox"/>
<input 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.



Log Source Summary

pxGrid_Primary
Cisco ISE pxGrid
Status: **Error** primary
Last Updated 9 hours ago

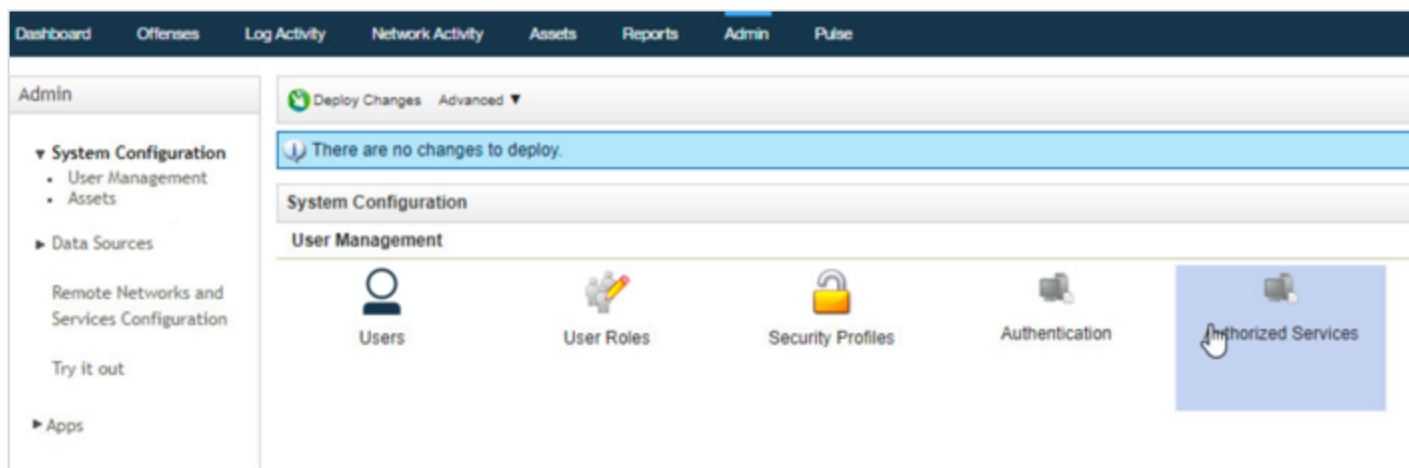
Events have not been received from this Log Source in over 720 minutes.

Overview **Protocol**

Log Source Identifier *

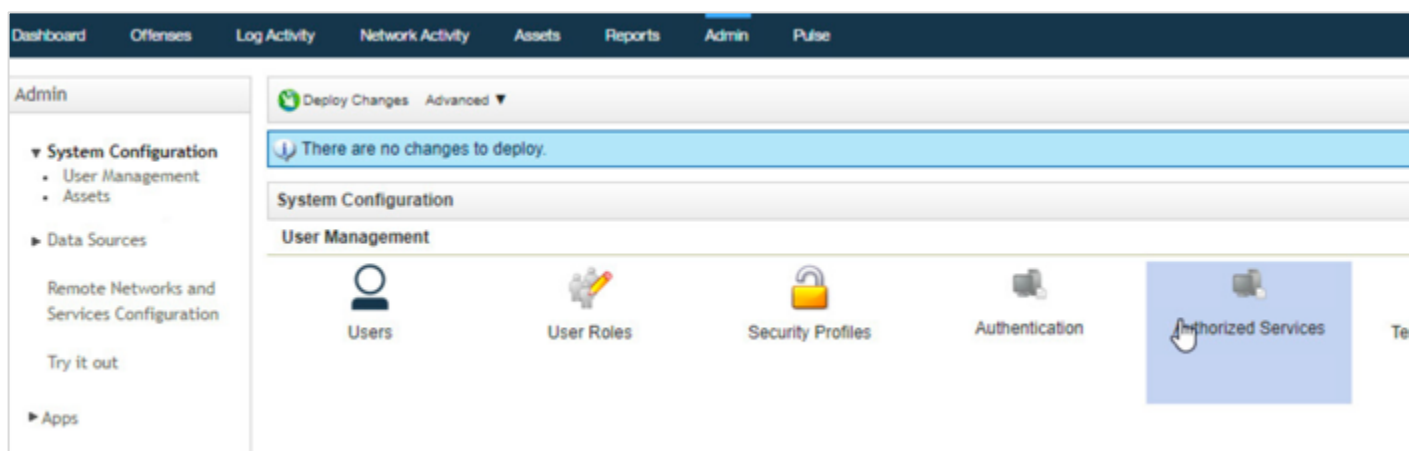
Incoming Payload Encoding

- Close 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**
- For both the User Role and Security Profile drop-down list boxes, select **Admin** (default)
- Enable **No for Expiry**

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

c. Click **Create Service**

d. Copy the authentication token into the notepad

Service Name	Authorized By	Authentication Token	User Role	Security Profile	Created	
Local Health Console	configservices	51402167-3daf-49d6-8a2f-7f0a9eefac5	Admin	Admin	Aug 4, 2018, 11:55:00 ...	Perman
AAPS	admin	617ed99a-a536-441f-902b-a68e9491fe3c	Admin	Admin	Aug 4, 2018, 10:21:34 ...	Perman
pxGridService	admin	9b0fe499-3ab2-4f47-9f8a-0ccb179f3ab3	Admin	Admin	Sep 27, 2018, 2:35:45 ...	Perman
WinCollect Agent	admin	e18fc295-da10-4aa1-8623-168bc7a46277	WinCollect	Admin	Sep 27, 2018, 10:45:24 ...	Perman
AdminToken	admin	70a0defee-f9e0-44a0-a95-86b3261f258	Admin	Admin	Feb 28, 2020, 11:57:50 ...	Feb 4,
pxgrid	admin	b72cfcac-3c5b-42c1-b065-80752eb270e2	Admin	Admin	Jul 1, 2020, 3:55:54 PM	Perman

Selected Token: da9df225-26b8-4ec5-868e-b424971c3ca8

Token: da9df225-26b8-4ec5-868e-b424971c3ca8

Authorized service added. Click Deploy Changes to apply the changes.

Service Name	Authorized By	Authentic... Token	User Role	Security Profile	Created	Expires
pxGridService	admin	da9df225-2...	Admin	Admin	Sep 24, 202...	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

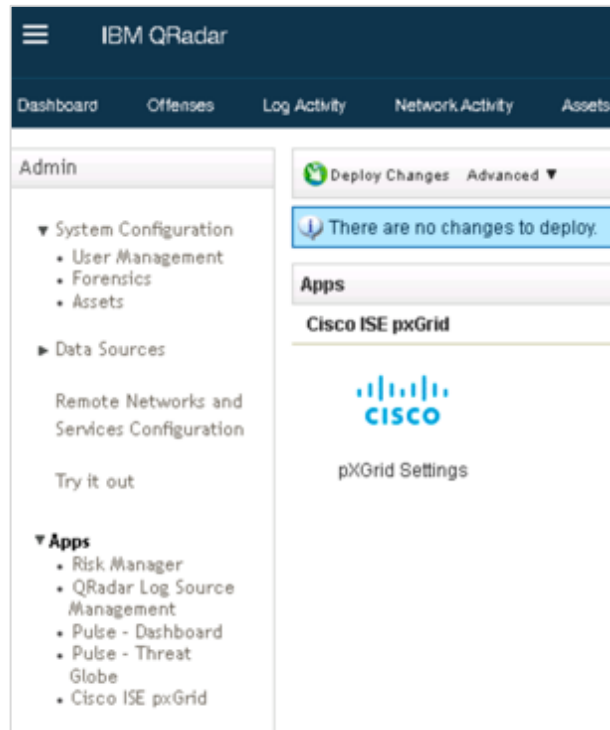
Advanced ▼

! There are undeployed changes. Click 'Deploy Changes' to deploy them. [View Details](#)

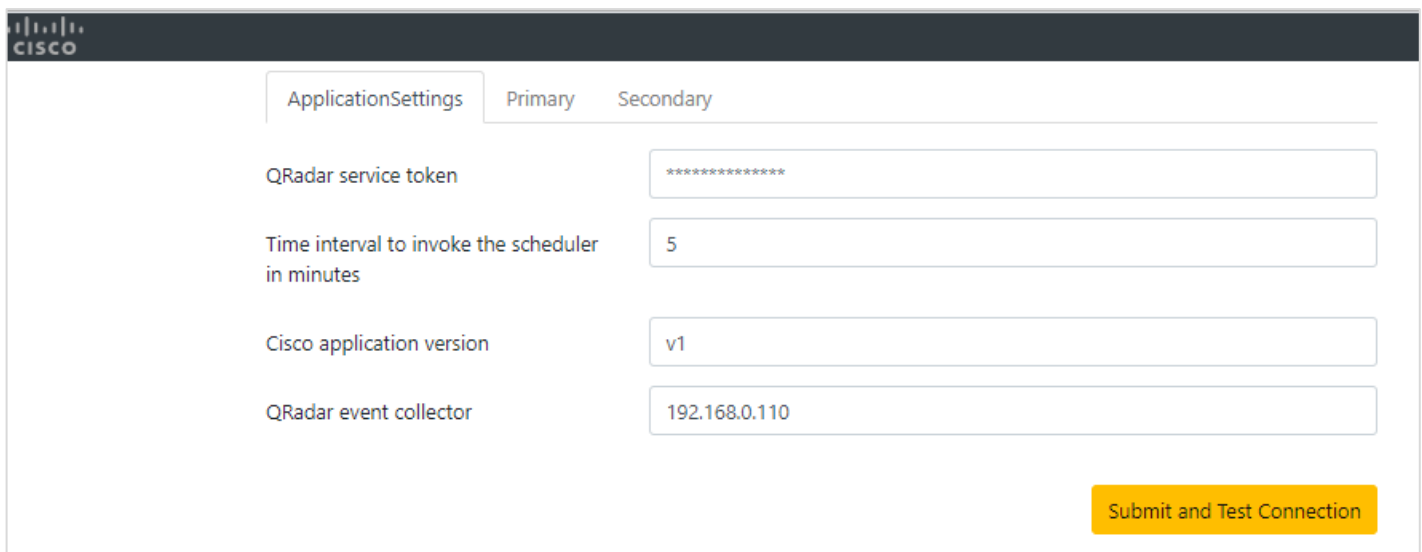
Configuring pxGrid Integration on QRadar

Step 1 Setup pxGrid settings:

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



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



The screenshot displays the 'QRadar Service Token' configuration window. It features a 'Cisco' logo at the top left and a 'Primary' tab selected. The configuration fields are as follows:

Field Name	Value
QRadar service token	*****
Time interval to invoke the scheduler in minutes	5
Cisco application version	v1
QRadar event collector	192.168.0.110

A yellow 'Submit and Test Connection' button is located at the bottom right of the form.

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

Step 3 Select **Submit and Test Connection**, you should see a successful connection in a pop-up window

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

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

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 Upload all (selecting all in the browse windows at once) the Cisco ISE pxGrid App certificates in PEM format under **Select and Upload Certificates (only PEM is supported)** application settings page

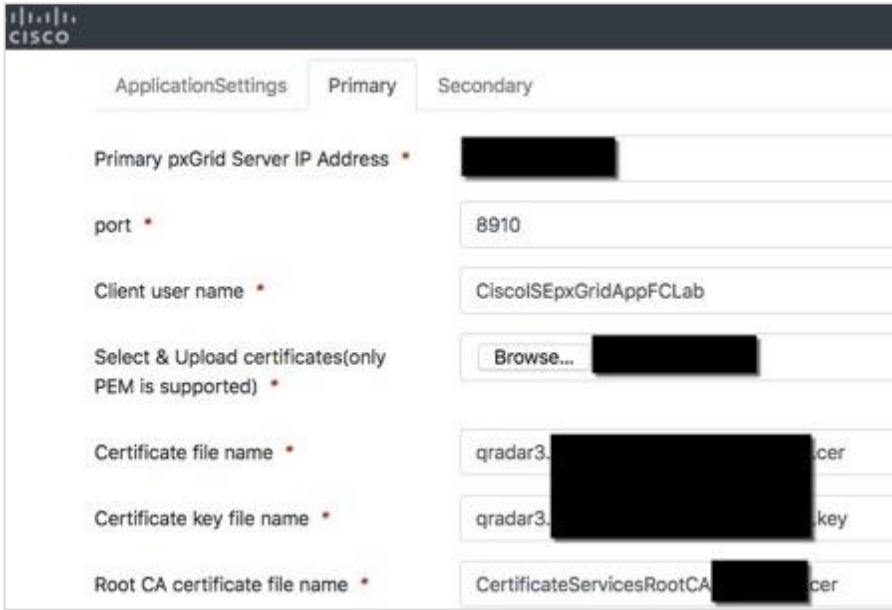
```
CertificateServicesEndpointSubCA-ise24k_.cer  
CertificateServicesNodeCA-ise24k_.cer  
CertificateServicesRootCA-ise24k_.cer  
ise24k.lab10.com.cer  
qradar.lab10.com_qradar.lab10.com.cer  
qradar.lab10.com_qradar.lab10.com.key
```

Step 8 Type in the Cisco ISE pxGrid App Certificate file name:
qradar.lab10.com_qradar.lab10.com.cer

Step 9 Type in the Cisco ISE pxGrid App Certificate key file name:
qradar.lab10.com_qradar.lab10.com.key

Step 10 Type in the Cisco ISE Internal Root Certificate Root CA certificate file name:
qradar.lab10.com_qradar.lab10.com.key

You will see the following:



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 multi certificates for different roles personas.
- The admin node with an internal PKI cert 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 the [ISE Guides page for certificates](#) and the [ISE 2.7 Certificate Section of Admin Guide](#).

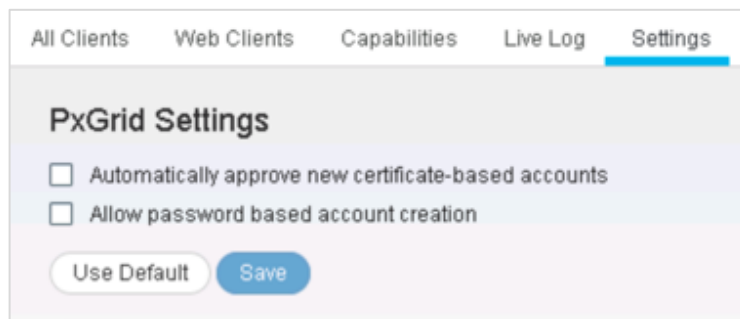
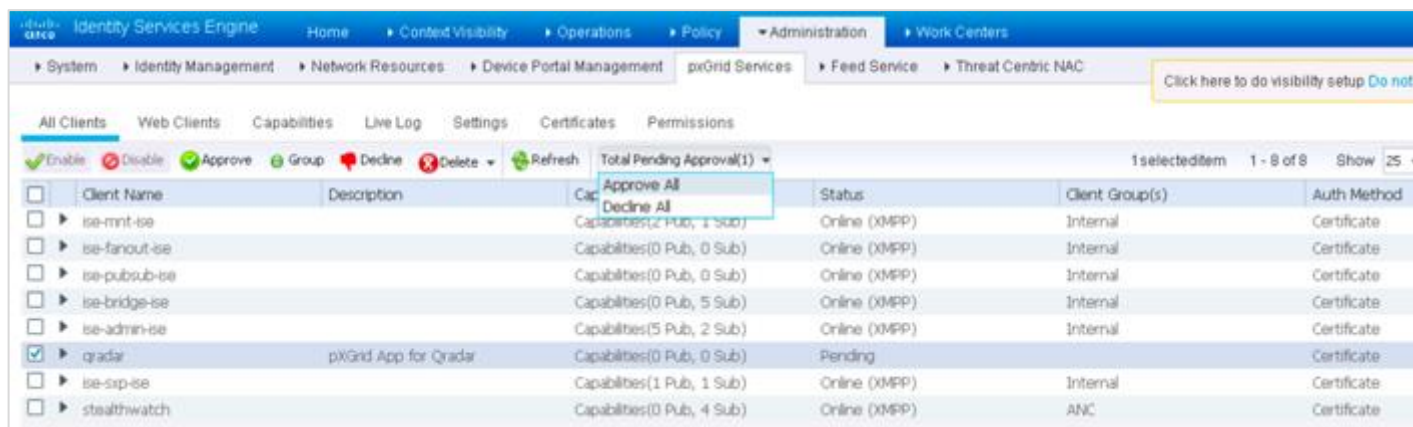
Step 11 At the bottom of the page, select **Submit and Test Connection**. Then you should see a successful connection message. If a secondary connection exists, do the same.

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 12 Validate the pxGrid client on ISE:

- a. In your browser, open ISE and log in
- b. Select **Administration > pxGrid Services**
- c. On the **All Clients** tab, you should see your **QRadar pxGrid client** (pending)

Note: The visibility of QRadar pxGrid client depends on the setting under **pxGrid > Settings for automatic approval of cert accounts**. If that setting is disabled, then you will need to manually approve it.

Client Name	Description	Cap	Status	Client Group(s)	Auth Method
ise-mnt-ise		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate
ise-fanout-ise		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
ise-pubsub-ise		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
ise-bridge-ise		Capabilities(0 Pub, 5 Sub)	Online (XMPP)	Internal	Certificate
ise-admin-ise		Capabilities(5 Pub, 2 Sub)	Online (XMPP)	Internal	Certificate
qradar	pxGrid App for Qradar	Capabilities(0 Pub, 0 Sub)	Pending	Internal	Certificate
ise-sip-ise		Capabilities(1 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate
stealthwatch		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	ANC	Certificate

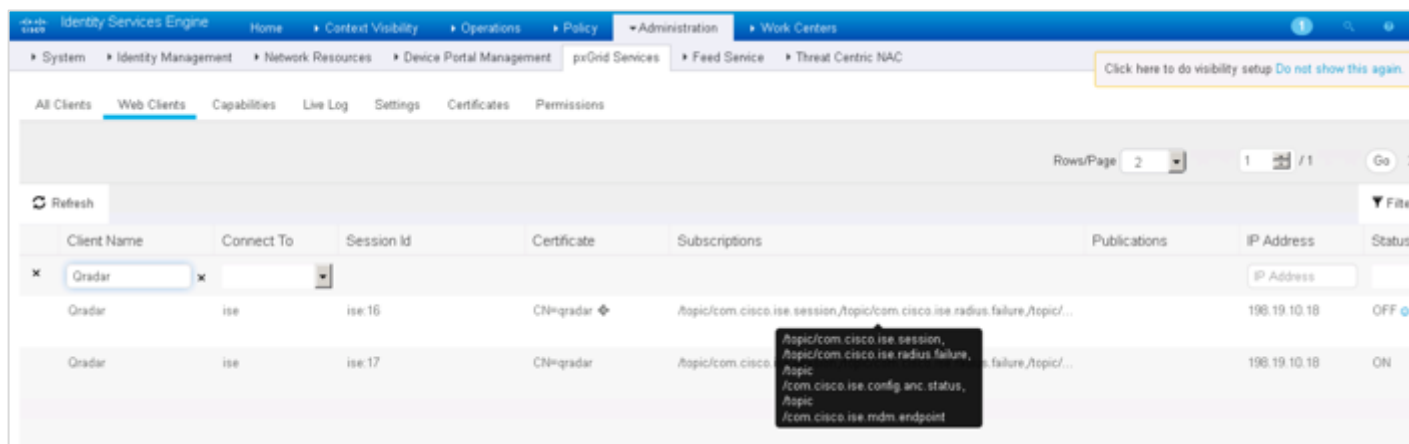
d. Click **Approve All** as you should see just one pending client

Note: 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 has a different view to better represent the setting, but we don't address it here.

Step 13 Select **Web Clients** 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).

If you see gai error in the app.log, check if your ISE IP address and its FQDN entry is present in /etc/hosts in pxGrid Docker Container inside QRadar.



Note: You will see the client connected twice if there are two pxGrid (primary/secondary) nodes. Only one entry for single pxGrid nodes.

Step 14 Assign the QRadar client to the ANC Group permissions

- a. Select **All Clients > Check the QRadar Client**
- b. **Group > Add > ANC**
- c. Click **Save**



Note: You should see the pxGrid client Group ANC assigned to the Cisco ISE pxGrid client

Setup Indexing in QRadar

Following are the steps to Index CEPs in QRadar.

Step 15 Return to the IBM QRadar

Step 16 Navigate to **Admin** tab, and then click **Index Management**



Step 17 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, 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**

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.

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 display 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.

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.??.* ,DE:??:DF:*

Passed Authentications

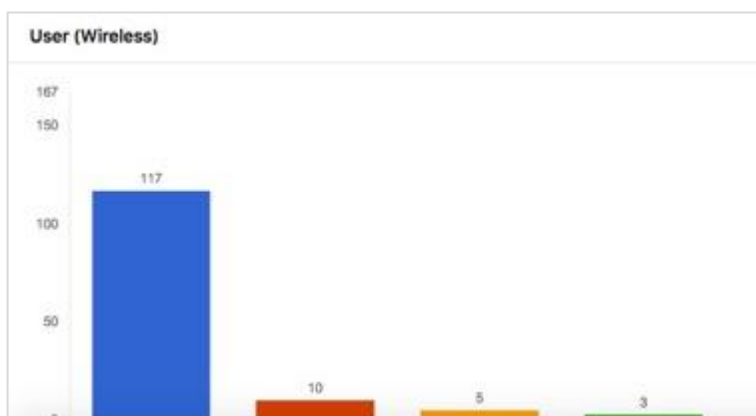
The Passed Authentications Dashboard View provides visibility into successful machine and user authentications across an organization and by wired and wireless connection type. This provides the admin with a view of how employees are connecting to the network, are they connecting over a wired or wireless connection, 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.

Step 1 Select Cisco ISE pxGrid > Passed Authentications





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

IBM QRadar Security Intelligence

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

2018-04-12 18:02 - 2018-04-27 18:02

Data For [Redacted]

Show 10 entries

Dev Time	IP Address	State	MAC Address	Username	Calling Station ID	Called StationID	NAS IP Address	NAS Port ID
18-Apr-2018 08:11:14.639 EDT	192.168.1.136	STARTED	10-DD:B1:C9:3C:39	[Redacted]	10-DD:B1:C9:3C:39	50:3D:E5:C4:06:8C	[Redacted]	GigabitEthernet1/0/12
18-Apr-2018 08:15:47.499 EDT	192.168.1.136	DISCONNECTED	10-DD:B1:C9:3C:39	[Redacted]	10-DD:B1:C9:3C:39	50:3D:E5:C4:06:8C	[Redacted]	GigabitEthernet1/0/12
18-Apr-2018 08:40:42.287 EDT	192.168.1.136	STARTED	10-DD:B1:C9:3C:39	[Redacted]	10-DD:B1:C9:3C:39	50:3D:E5:C4:06:8C	[Redacted]	GigabitEthernet1/0/12
18-Apr-2018 09:41:41.421 EDT	192.168.1.136	DISCONNECTED	10-DD:B1:C9:3C:39	[Redacted]	10-DD:B1:C9:3C:39	50:3D:E5:C4:06:8C	[Redacted]	GigabitEthernet1/0/12
18-Apr-2018 09:50:57.018 EDT	192.168.1.136	STARTED	10-DD:B1:C9:3C:39	[Redacted]	10-DD:B1:C9:3C:39	50:3D:E5:C4:06:8C	[Redacted]	GigabitEthernet1/0/12
18-Apr-2018 10:37:19.136 EDT	192.168.1.136	DISCONNECTED	10-DD:B1:C9:3C:39	[Redacted]	10-DD:B1:C9:3C:39	50:3D:E5:C4:06:8C	[Redacted]	GigabitEthernet1/0/12

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

IBM QRadar Security Intelligence

admin Help Messages

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin Cisco ISE pxGrid System Time: 6:00

2018-04-12 18:02 - 2018-04-27 18:02

Data For : jeppich

Show 10 entries

EXPORT

NAS Port Type	NAS Identifier	Posture Status	Endpoint Profile	Endpoint Operating System	Group ID	AD Normalized
Ethernet			Apple-Device	Apple Mac OS X 10.7.0 (Lion) - 10.10 (Yosemite) or iOS 4.1 - 8.3 (Darwin 10.0.0 - 14.5.0)		
Ethernet			Apple-Device	Apple Mac OS X 10.7.0 (Lion) - 10.10 (Yosemite) or iOS 4.1 - 8.3 (Darwin 10.0.0 - 14.5.0)		
Ethernet			Apple-Device	Apple Mac OS X 10.7.0 (Lion) - 10.10 (Yosemite) or iOS 4.1 - 8.3 (Darwin 10.0.0 - 14.5.0)		
Ethernet			Apple-Device	Apple Mac OS X 10.7.0 (Lion) - 10.10 (Yosemite) or iOS 4.1 - 8.3 (Darwin 10.0.0 - 14.5.0)		
Ethernet			Apple-Device	Apple Mac OS X 10.7.0 (Lion) - 10.10 (Yosemite) or iOS 4.1 - 8.3 (Darwin 10.0.0 - 14.5.0)		
Ethernet			Apple-Device	Apple Mac OS X 10.7.0 (Lion) - 10.10 (Yosemite) or iOS 4.1 - 8.3 (Darwin 10.0.0 - 14.5.0)		
Ethernet			Apple-Device	Apple Mac OS X 10.7.0 (Lion) - 10.10 (Yosemite) or iOS 4.1 - 8.3 (Darwin 10.0.0 - 14.5.0)		
Ethernet			Apple-Device	Apple Mac OS X 10.7.0 (Lion) - 10.10 (Yosemite) or iOS 4.1 - 8.3 (Darwin 10.0.0 - 14.5.0)		
Ethernet			Apple-Device	Apple Mac OS X 10.7.0 (Lion) - 10.10 (Yosemite) or iOS 4.1 - 8.3 (Darwin 10.0.0 - 14.5.0)		
Ethernet			Apple-Device	Apple Mac OS X 10.7.0 (Lion) - 10.10 (Yosemite) or iOS 4.1 - 8.3 (Darwin 10.0.0 - 14.5.0)		

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

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin Cisco ISE pxGrid System Time: 6:00

2018-04-12 18:02 - 2018-04-27 18:02

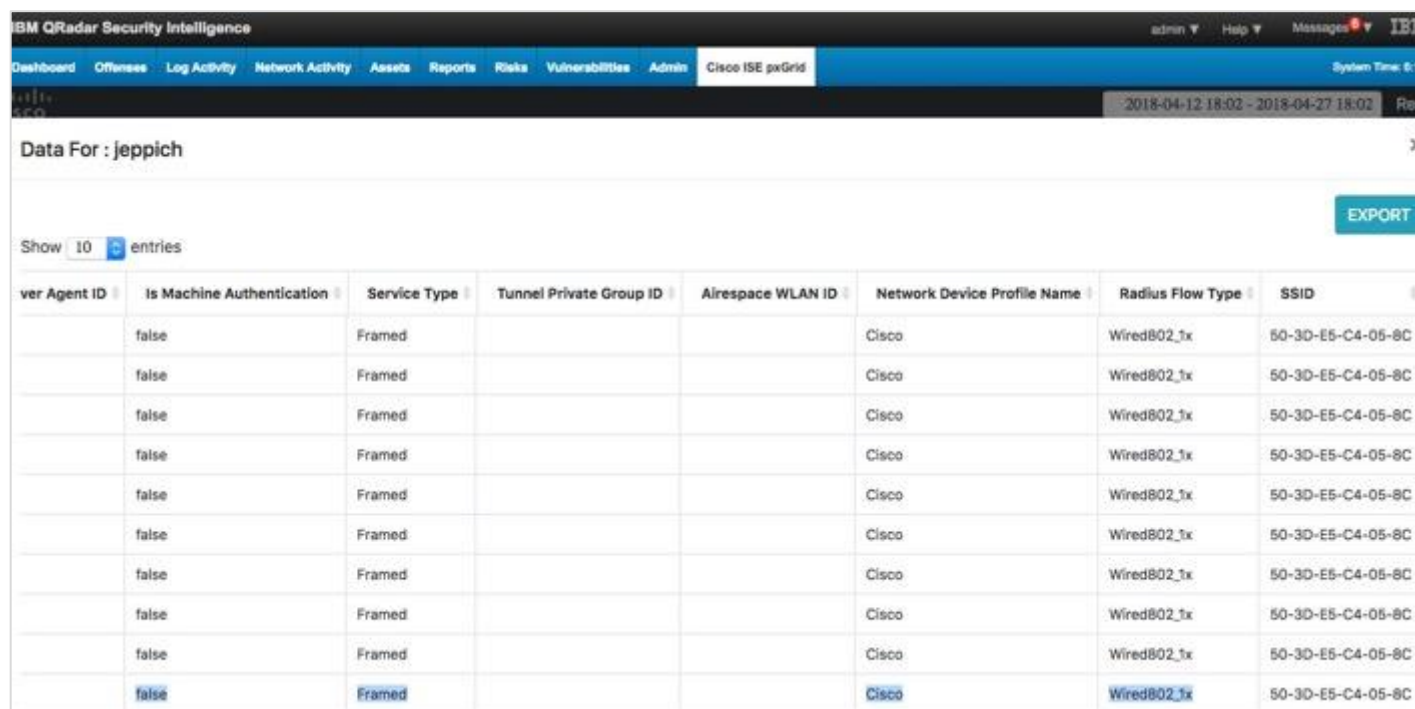
Data For : jeppich

Show 10 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

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.



IBM QRadar Security Intelligence

admin Help Messages System Time: 6:11

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

2018-04-12 18:02 - 2018-04-27 18:02

Data For : jeppich

Show 10 entries

EXPORT

User Agent ID	Is Machine Authentication	Service Type	Tunnel Private Group ID	Airespace WLAN ID	Network Device Profile Name	Radius Flow Type	SSID
	false	Framed			Cisco	Wired802_1x	50-3D-E5-C4-05-8C
	false	Framed			Cisco	Wired802_1x	50-3D-E5-C4-05-8C
	false	Framed			Cisco	Wired802_1x	50-3D-E5-C4-05-8C
	false	Framed			Cisco	Wired802_1x	50-3D-E5-C4-05-8C
	false	Framed			Cisco	Wired802_1x	50-3D-E5-C4-05-8C
	false	Framed			Cisco	Wired802_1x	50-3D-E5-C4-05-8C
	false	Framed			Cisco	Wired802_1x	50-3D-E5-C4-05-8C
	false	Framed			Cisco	Wired802_1x	50-3D-E5-C4-05-8C
	false	Framed			Cisco	Wired802_1x	50-3D-E5-C4-05-8C
	false	Framed			Cisco	Wired802_1x	50-3D-E5-C4-05-8C

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.

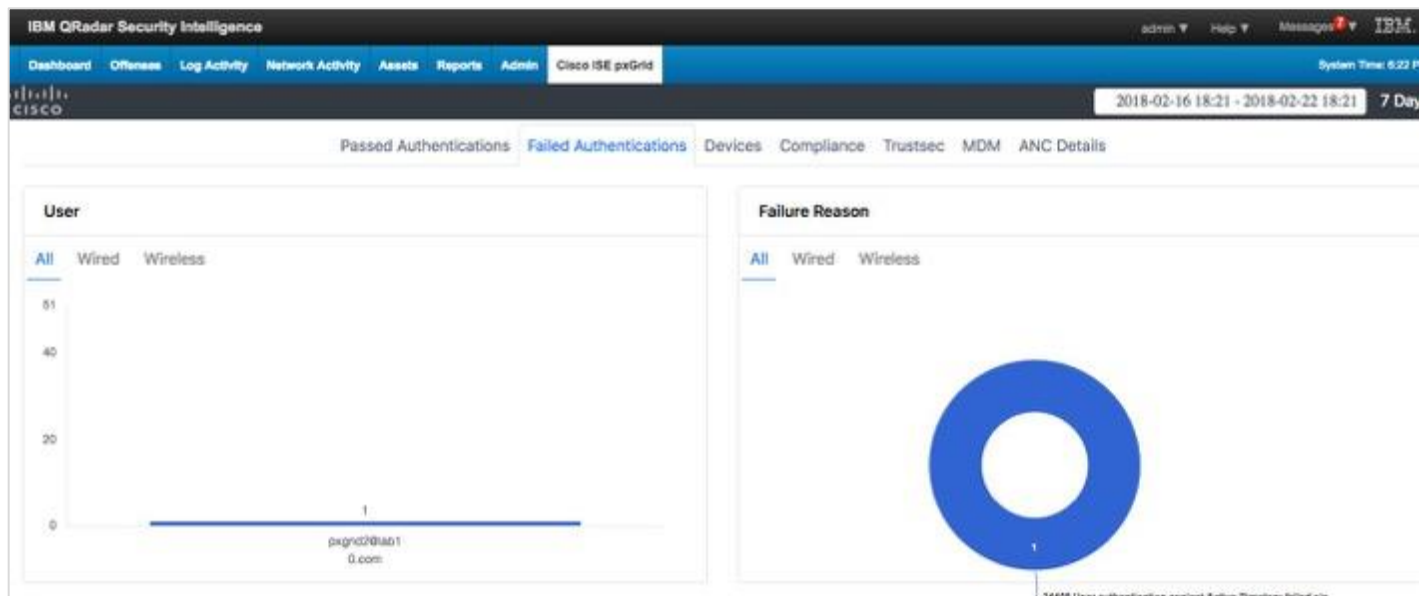
The other panels provide a breakdown by failure reason, device type and location, and provide the admin insight to how these failed authentications occur. The same contextual information from the user panel is available in these panel breakdowns.

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

User Panel

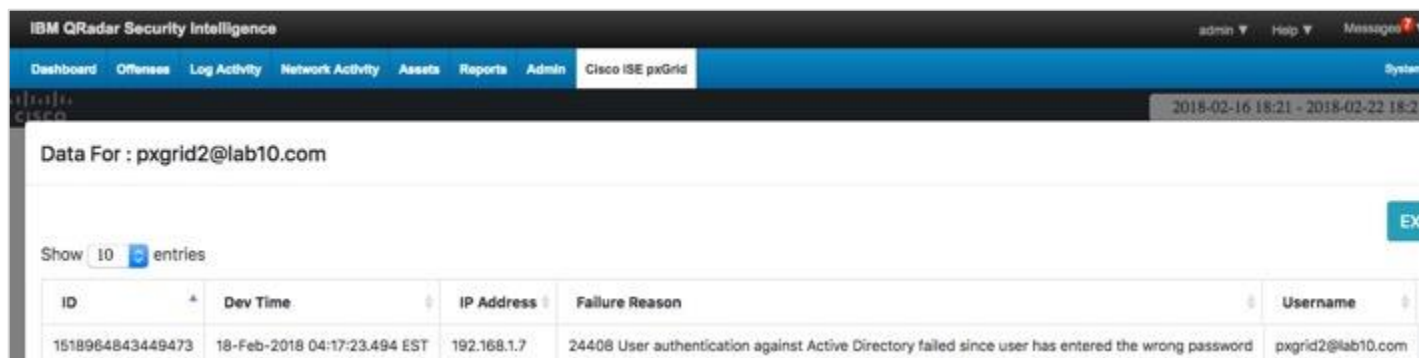
The user panel provides a breakdown by username.

Step 1 Select **Cisco ISE pxGrid > Failed Authentications**



Step 2 Select **Cisco ISE pxGrid > Failed Authentications > User > pxGrid2@** [REDACTED]

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



ID	Dev Time	IP Address	Failure Reason	Username
1518964843449473	18-Feb-2018 04:17:23.494 EST	192.168.1.7	24408 User authentication against Active Directory failed since user has entered the wrong password	pxgrid2@lab10.com

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.

IBM QRadar Security Intelligence

admin Help Messages

Dashboard Offenses Log Activity Network Activity Assets Reports Admin Cisco ISE pxGrid

2018-02-16 18:36 - 2018-02-22 18:36

Data For : pxgrid2@lab10.com

Show 10 entries

Server Name	Authentication Protocol	Device Type	Location	Calling Station ID	NAS IP Address	NAS Port ID	NAS Port Type	MAC Address
ise24k	PEAP (EAP-MSCHAPv2)	All Device Types	All Locations	00-0C-29-C1-7B-2C	192.168.1.3	GigabitEthernet1/0/11	Ethernet	

Showing 1 to 1 of 1 entries

Previous 1

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.

IBM QRadar Security Intelligence

admin Help Messages

Dashboard Offenses Log Activity Network Activity Assets Reports Admin Cisco ISE pxGrid

System Time: 8:41 PM

2018-02-16 18:36 - 2018-02-22 18:36 7 Day

Data For : pxgrid2@lab10.com

EXPORT

Show 10 entries

Message Code	User Type	Access Service	Identity Store	Authentication Method	Service Type	Credential Check	AD Normalized User	AD Host Domain Na
5400		Default Network Access	pxGridUsers	dot1x	Framed	MSCHAPV2		

Showing 1 to 1 of 1 entries

Previous 1 Next

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

IBM QRadar Security Intelligence

admin Help Messages

Dashboard Offenses Log Activity Network Activity Assets Reports Admin Cisco ISE pxGrid

System Time: 8:46 PM

2018-02-16 18:36 - 2018-02-22 18:36 7 Day

Data For : pxgrid2@lab10.com

EXPORT

Show 10 entries

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

Showing 1 to 1 of 1 entries

Previous 1 Next

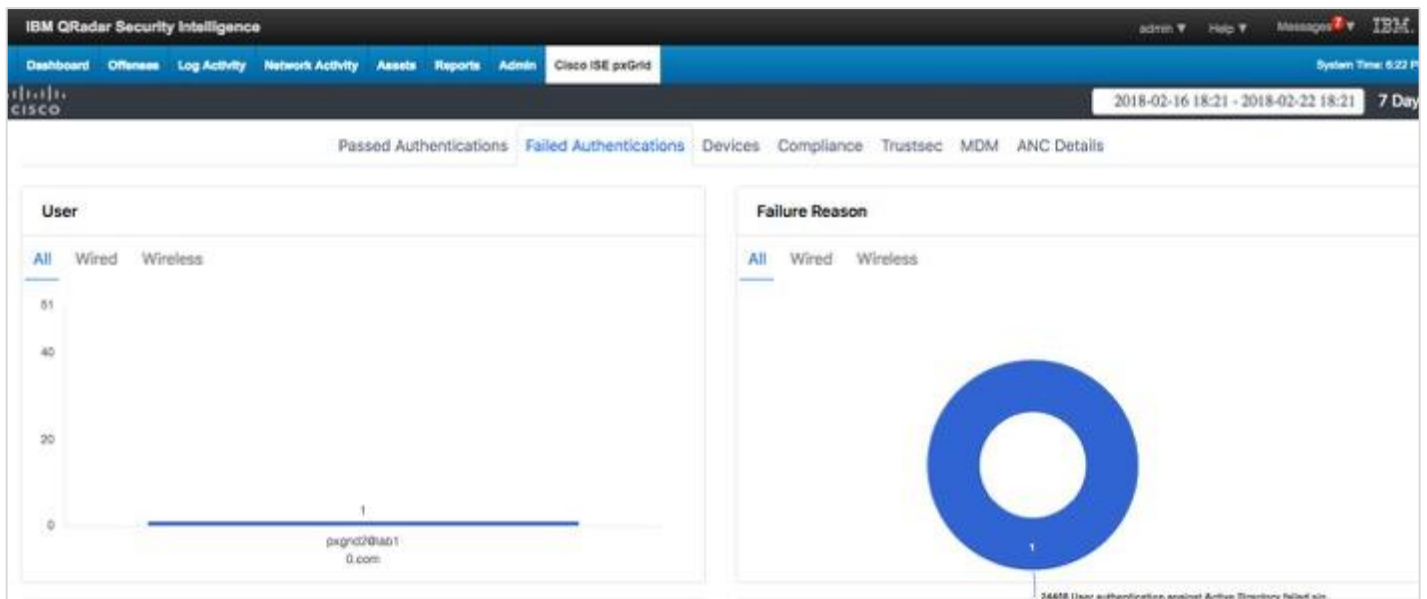
AD User Domain Name	AD User Net Bios Name	AD User Resolved Identities	AD User Resolved DNS

Failure Reason Panel

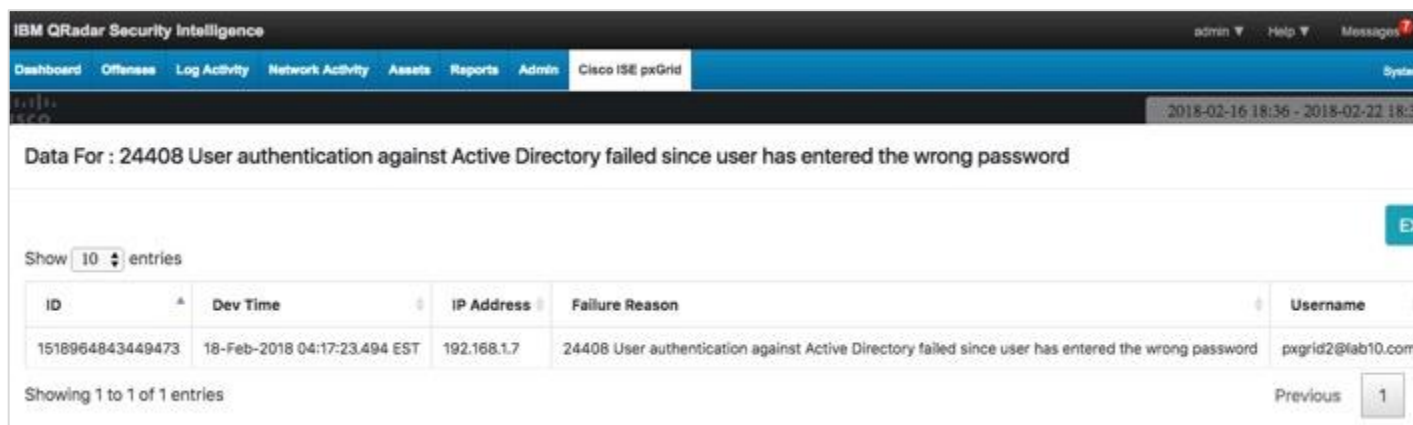
The Failure Reason panel provides a breakdown by failure reason.

Step 1 Select **Cisco ISE pxGrid > Failed Authentications**

Step 2 Select **Failure Reason > 24408 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.



IBM QRadar Security Intelligence

admin Help Messages

Dashboard Offenses Log Activity Network Activity Assets Reports Admin Cisco ISE pxGrid System

2018-02-16 18:36 - 2018-02-22 18:36

Data For : 24408 User authentication against Active Directory failed since user has entered the wrong password

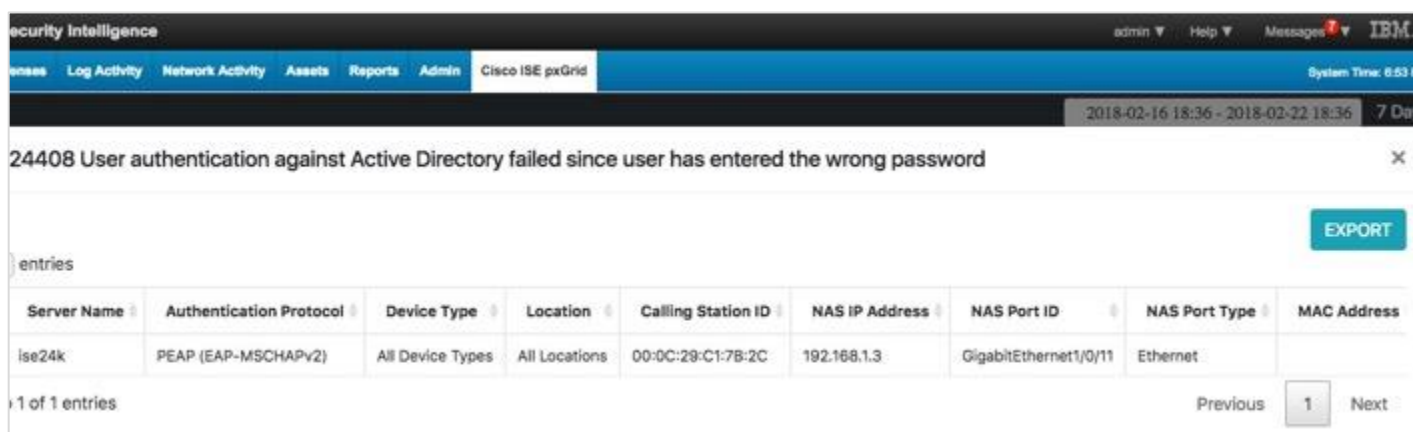
Show 10 entries

ID	Dev Time	IP Address	Failure Reason	Username
1518964843449473	18-Feb-2018 04:17:23.494 EST	192.168.1.7	24408 User authentication against Active Directory failed since user has entered the wrong password	pxgrid2@iab10.com

Showing 1 to 1 of 1 entries

Previous 1

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.



Security Intelligence

admin Help Messages IBM

Offenses Log Activity Network Activity Assets Reports Admin Cisco ISE pxGrid System Time: 8:53 PM

2018-02-16 18:36 - 2018-02-22 18:36 7 Day

24408 User authentication against Active Directory failed since user has entered the wrong password

EXPORT

entries

Server Name	Authentication Protocol	Device Type	Location	Calling Station ID	NAS IP Address	NAS Port ID	NAS Port Type	MAC Address
ise24k	PEAP (EAP-MSCHAPv2)	All Device Types	All Locations	00:0C:29:C1:7B:2C	192.168.1.3	GigabitEthernet1/0/11	Ethernet	

1 of 1 entries

Previous 1 Next

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.



Security Intelligence

admin Help Messages

Offenses Log Activity Network Activity Assets Reports Admin Cisco ISE pxGrid

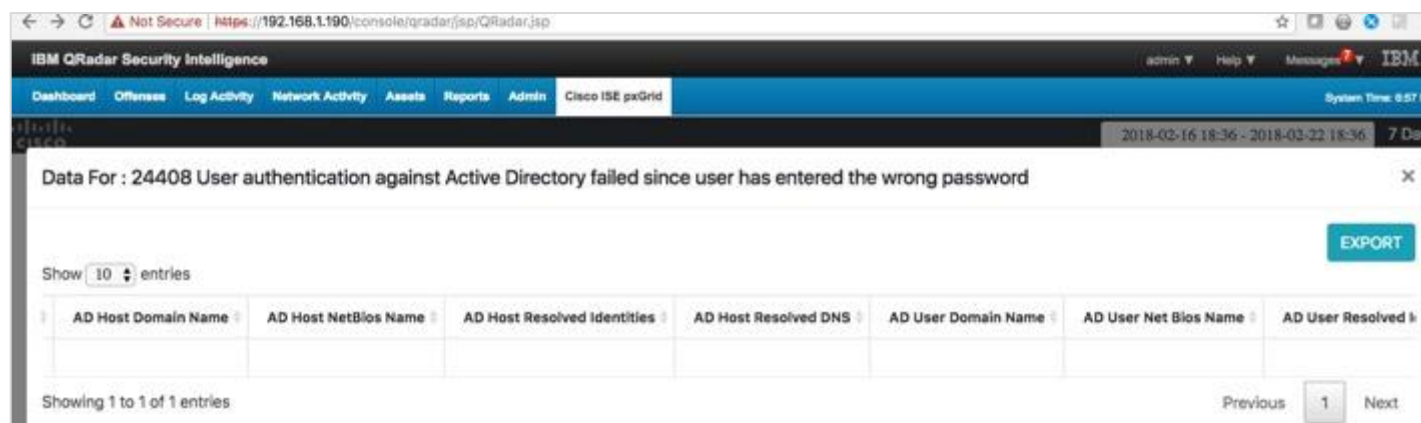
2018-02-16 18:36 - 2018-02-22

: 24408 User authentication against Active Directory failed since user has entered the wrong password

entries

Message Code	User Type	Access Service	Identity Store	Authentication Method	Service Type	Credential Check	AD Normalized User
5400		Default Network Access	pxGridUsers	dot1x	Framed	MSCHAPV2	

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



IBM QRadar Security Intelligence

admin Help Messages

Dashboard Offenses Log Activity Network Activity Assets Reports Admin Cisco ISE pxGrid

System Time: 8:57

2018-02-16 18:36 - 2018-02-22 18:36 7 Da

Data For : 24408 User authentication against Active Directory failed since user has entered the wrong password

EXPORT

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

Showing 1 to 1 of 1 entries

Previous 1 Next

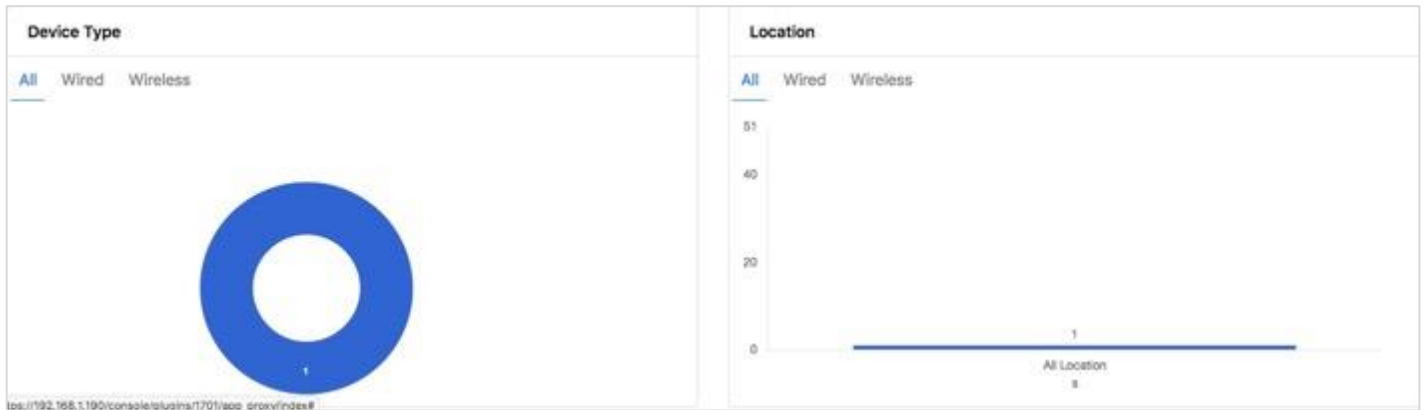
Device Type Panel

The **Device 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 Select **Cisco ISE pxGrid > Failed Authentications**

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



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



IBM QRadar Security Intelligence

Dashboard Offenses Log Activity Network Activity Assets Reports Admin Cisco ISE pxGrid System

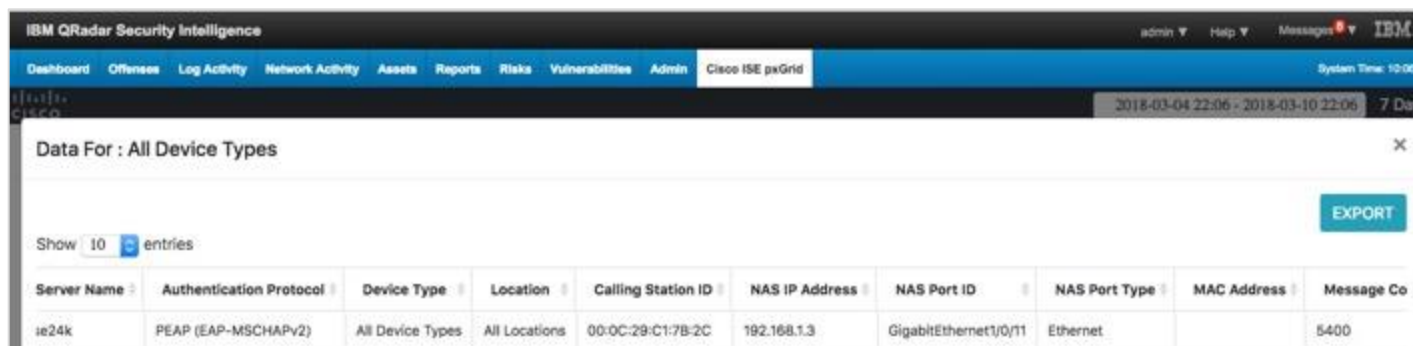
2018-02-16 18:36 - 2018-02-22 18:36

Data For : All Device Types

Show 10 entries

ID	Dev Time	IP Address	Failure Reason	Username
1518964843449473	18-Feb-2018 04:17:23.494 EST	192.168.1.7	24408 User authentication against Active Directory failed since user has entered the wrong password	pxgrid2@lab10.com

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.



IBM QRadar Security Intelligence

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin Cisco ISE pxGrid System Time: 10:08

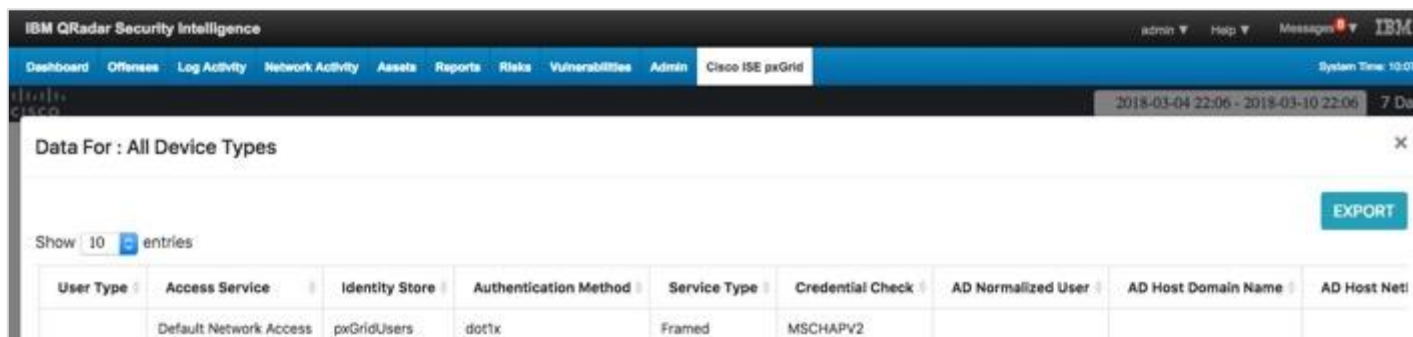
2018-03-04 22:06 - 2018-03-10 22:06 7 Day

Data For : All Device Types

Show 10 entries

Server Name	Authentication Protocol	Device Type	Location	Calling Station ID	NAS IP Address	NAS Port ID	NAS Port Type	MAC Address	Message Co
ie24k	PEAP (EAP-MSCHAPV2)	All Device Types	All Locations	00:0C:29:C1:7B:2C	192.168.1.3	GigabitEthernet1/0/11	Ethernet		5400

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.



IBM QRadar Security Intelligence

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin Cisco ISE pxGrid System Time: 10:07


2018-03-04 22:06 - 2018-03-10 22:06 7 Day

Data For : All Device Types

Show 10 entries

User Type	Access Service	Identity Store	Authentication Method	Service Type	Credential Check	AD Normalized User	AD Host Domain Name	AD Host Net
	Default Network Access	pxGridUsers	dot1x	Framed	MSCHAPV2			

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



The screenshot shows the Cisco ISE pxGrid interface. The top navigation bar includes 'Intelligence', 'Log Activity', 'Network Activity', 'Assets', 'Reports', 'Risks', 'Vulnerabilities', 'Admin', and 'Cisco ISE pxGrid'. The main content area displays a table with columns for various AD attributes. An 'EXPORT' button is visible in the top right corner of the table area.

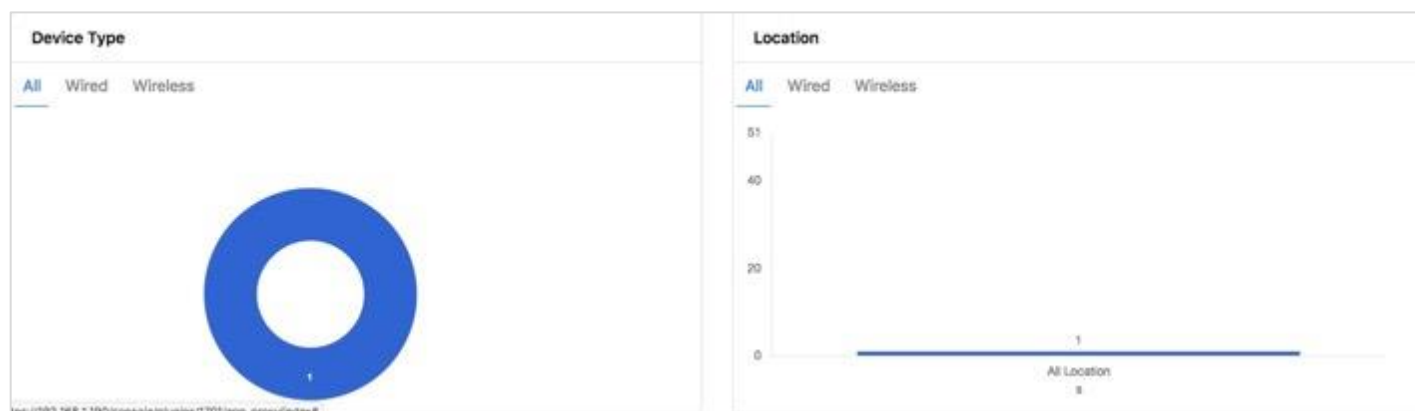
AD Host Resolved Identities	AD Host Resolved DNS	AD User Domain Name	AD User Net Bios Name	AD User Resolved Identities	AD User Resolved DNS

Locations Panel

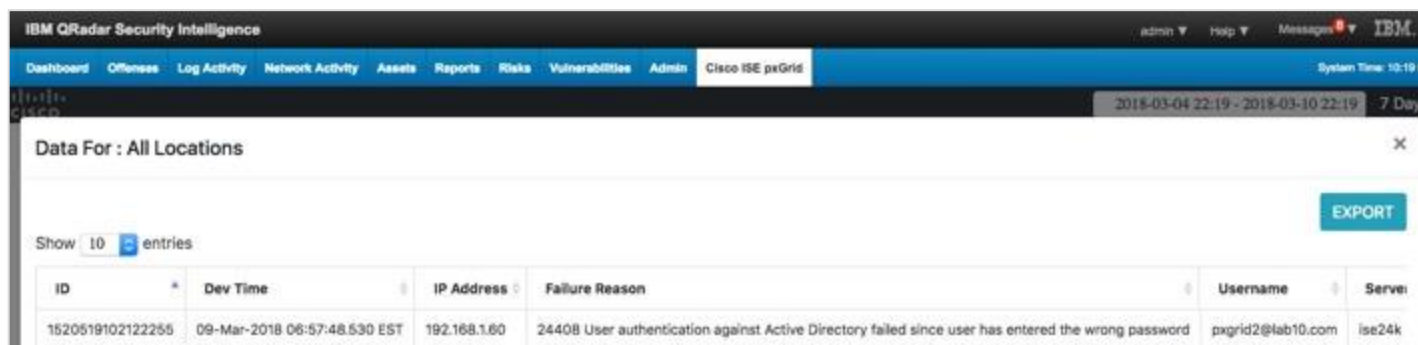
The location panel provides insight into attempted by failures by NAD location type and provides a drill-down based on Locations.

Step 1 Select **Cisco ISE pxGrid > Failed Authentications**

Step 2 Select **Location > All > All Location**



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



IBM QRadar Security Intelligence

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

System Time: 10:19

2018-03-04 22:19 - 2018-03-10 22:19 7 Day

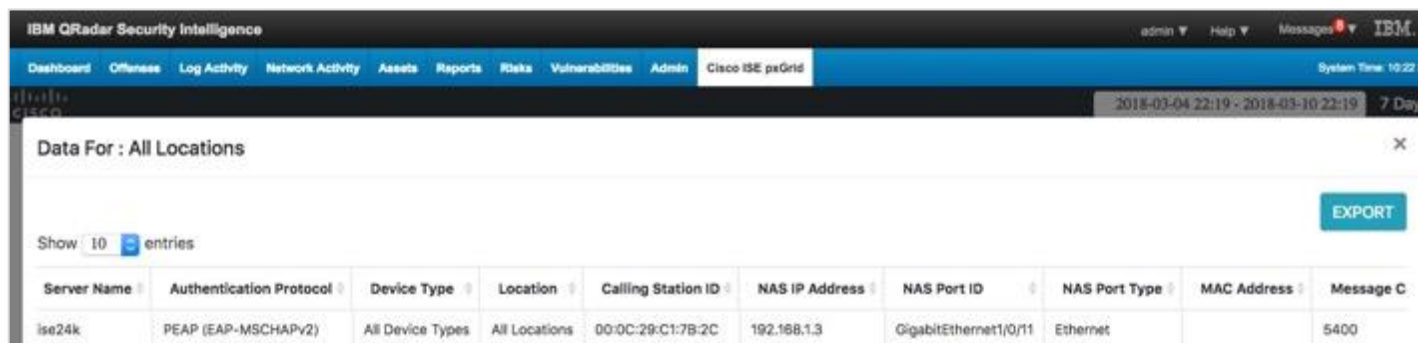
Data For : All Locations

Show 10 entries

ID	Dev Time	IP Address	Failure Reason	Username	Server
1520519102122255	09-Mar-2018 06:57:48.530 EST	192.168.1.60	2440B User authentication against Active Directory failed since user has entered the wrong password	pxgrid2@lab10.com	ise24k

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.



IBM QRadar Security Intelligence

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

System Time: 10:22

2018-03-04 22:19 - 2018-03-10 22:19 7 Day

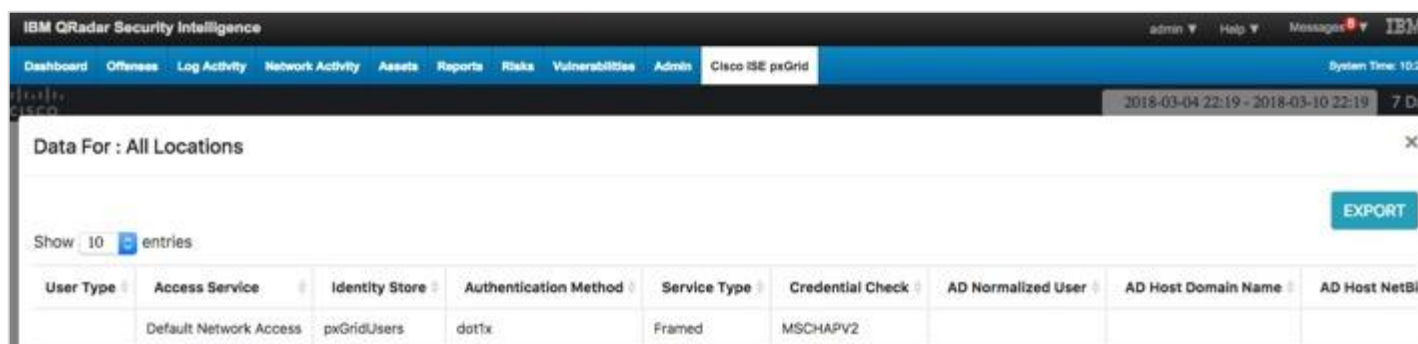
Data For : All Locations

Show 10 entries

Server Name	Authentication Protocol	Device Type	Location	Calling Station ID	NAS IP Address	NAS Port ID	NAS Port Type	MAC Address	Message C
ise24k	PEAP (EAP-MSCHAPV2)	All Device Types	All Locations	00:0C:29:C1:7B:2C	192.168.1.3	GigabitEthernet1/0/11	Ethernet		5400

EXPORT

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.



IBM QRadar Security Intelligence

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

System Time: 10:22

2018-03-04 22:19 - 2018-03-10 22:19 7 Day

Data For : All Locations

Show 10 entries

User Type	Access Service	Identity Store	Authentication Method	Service Type	Credential Check	AD Normalized User	AD Host Domain Name	AD Host NetBI
	Default Network Access	pxGridUsers	dot1x	Framed	MSCHAPV2			

EXPORT

Intelligence admin ▾ Help ▾ Messages 0 ▾ IB3

Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin Cisco ISE pxGrid System Time: 5:5

2018-03-04 17:53 - 2018-03-10 17:53 7 D

Locations X

[EXPORT](#)

ies

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 ▾

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.

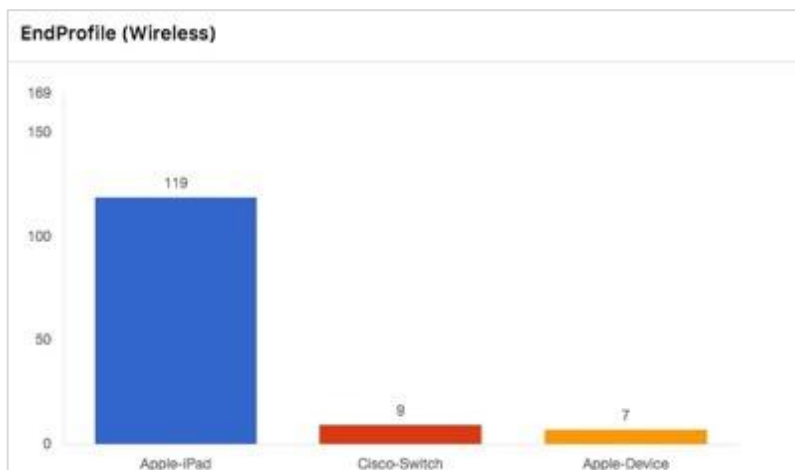
The admin drills down on the endpoint profile and obtains the following contextual information: endpoint device information, MAC Address, IP Address, posture status, NAS Port Type, NAS Port ID, NAS Identifier, NAS IP Address, WLAN Information, Calling Station ID, Called Station ID, AD resolvable user 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 Select **Cisco ISE pxGrid > Devices**

Step 2 Select **EndProfile (All) > Windows7-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

IBM QRadar Security Intelligence

Dashboard Offenses Log Activity Network Activity Assets Reports Admin Cisco ISE pxGrid System Time: 9:03 PM

2018-02-16 21:02 - 2018-02-22 21:02 7 Days

Data For : Windows7-Workstation

Show 10 entries

Dev Time	IP Address	State	MAC Address	Username	Calling Station ID	Called StationID	NAS IP Address	NAS Port ID
22-Feb-2018 04:38:20.739 EST	192.168.1.37	DISCONNECTED	00:0C:29:C1:7B:2C	host\pxGrid2- [REDACTED]	00:0C:29:C1:7B:2C	50:3D:E5:C4:05:8B	192.168.1.3	GigabitEthen
22-Feb-2018 04:38:22.616 EST	192.168.1.37	STARTED	00:0C:29:C1:7B:2C	pxgrid2@ [REDACTED]	00:0C:29:C1:7B:2C	50:3D:E5:C4:05:8B	192.168.1.3	GigabitEthen
22-Feb-2018 04:42:39.116 EST	192.168.1.37	DISCONNECTED	00:0C:29:C1:7B:2C	pxgrid2@ [REDACTED]	00:0C:29:C1:7B:2C	50:3D:E5:C4:05:8B	192.168.1.3	GigabitEthen

EXPORT

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.

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-PC\$	
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 Identity
PXGRID2-PC\$		CN=PXGRID2-PC,CN=Computers,DC=			
PXGRID2-PC\$					
PXGRID2-PC\$					
PXGRID2-PC\$					

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.

Intelligence admin Help Messages IBM

Activity Network Activity Assets Reports Admin Cisco ISE pxGrid System Time: 9:09

2018-02-16 21:02 - 2018-02-22 21:02 7 D

s7-Workstation

EXPORT

AD User Resolved DNS	Terminal Server Agent ID	Is Machine Authentication	Service Type	Tunnel Private Group ID	Airspace WLAN ID
		true	Framed		
CN=pxgrid2,CN=Users,DC=		false	Framed		
CN=pxgrid2,CN=Users,DC=		false	Framed		

admin Help Messages IBM

System Time: 9:1

2018-02-16 21:02 - 2018-02-22 21:02 7 D

s7-Workstation

EXPORT

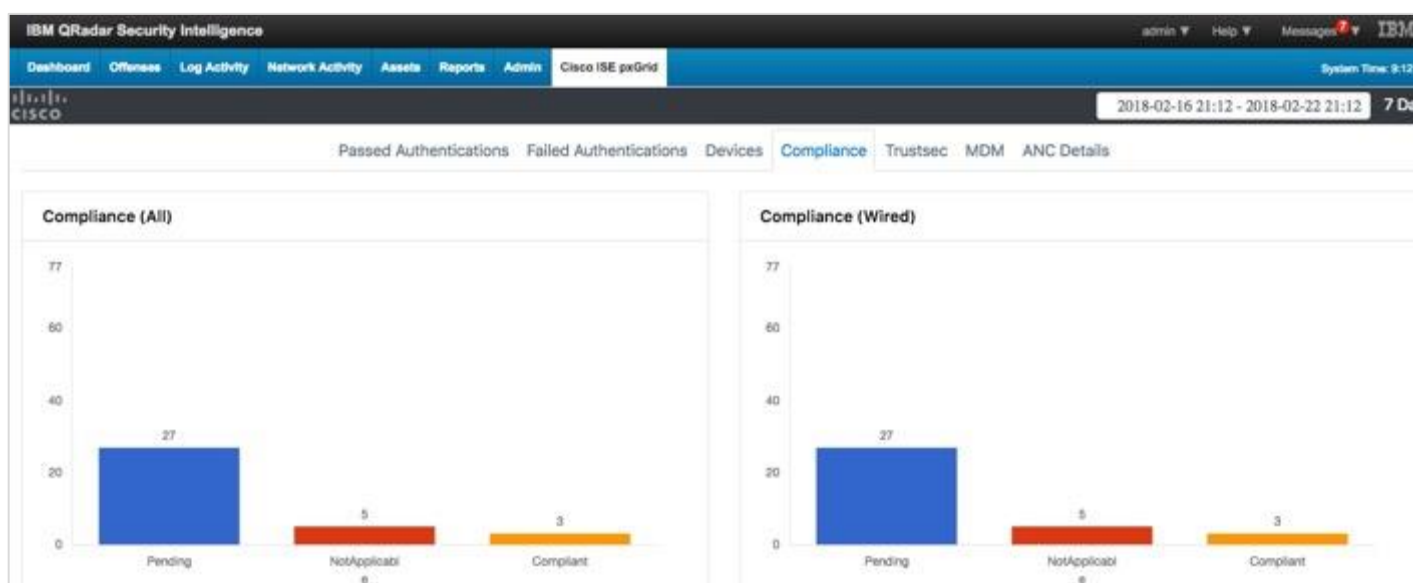
Network Device Profile Name	Radius Flow Type	SSID
Cisco	Wired802_1x	50-3D-E5-C4-05-8B
Cisco	Wired802_1x	50-3D-E5-C4-05-8B
Cisco	Wired802_1x	50-3D-E5-C4-05-8B

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 Select **Cisco pxGrid > Compliance (All)**

Step 2 Select **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.

IBM QRadar Security Intelligence admin Help Messages IBM

Dashboard Offenses Log Activity Network Activity Assets Reports Admin Cisco ISE pxGrid System Time: 9:14 P

2018-02-16 21:12 - 2018-02-22 21:12 7 Day

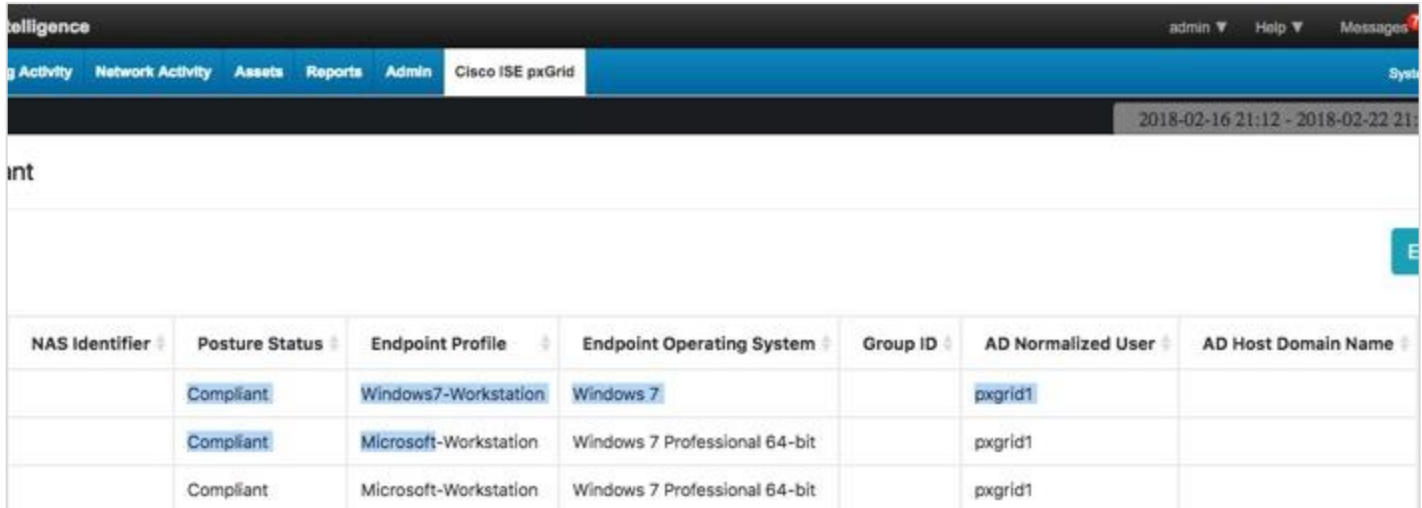
Data For : Compliant X

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

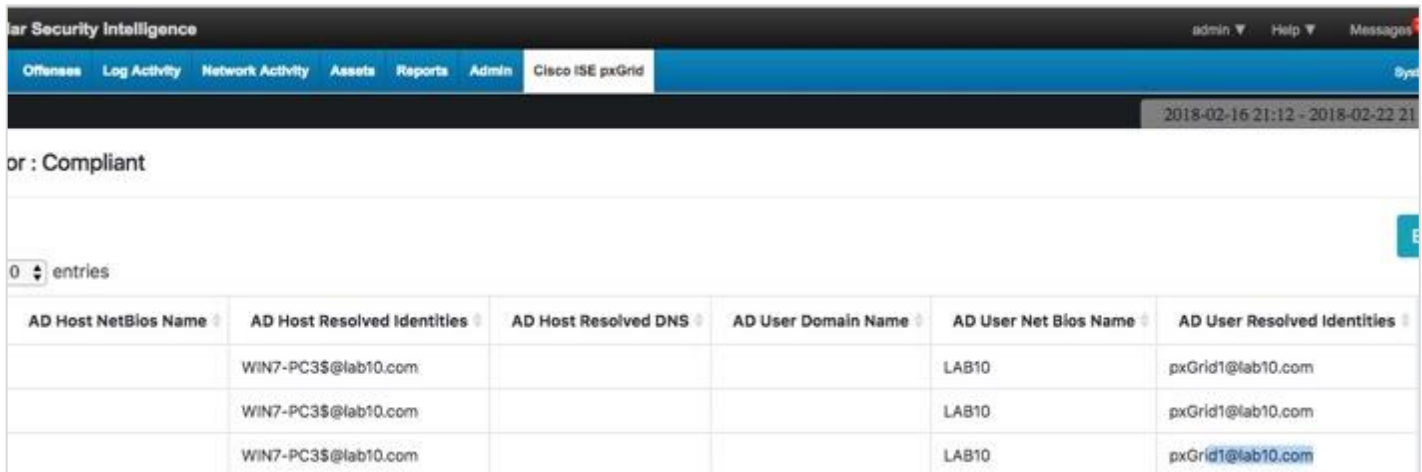
The Posture Status attribute contains the value of the posture status, compliant, non-compliance, and pending.

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	Airspace WLAN ID
CN=pxGrid1,CN=Users,...		false	Framed		
		false	Framed		
		false	Framed		

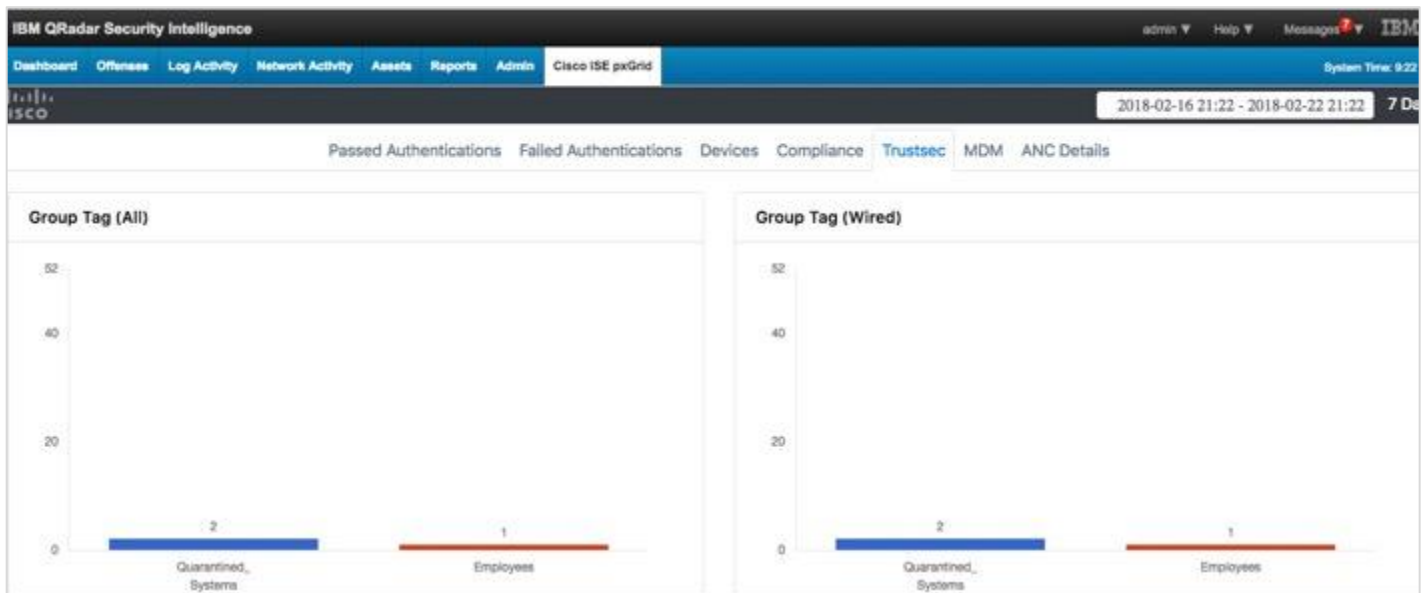
TrustSec

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 Select **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.

IBM QRadar Security Intelligence

admin Help Messages

Dashboard Offenses Log Activity Network Activity Assets Reports Admin Cisco ISE pxGrid System Time

2018-02-16 21:22 - 2018-02-22 21:22

Data For : Quarantined_Systems

Show 10 entries

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.

IBM QRadar Security Intelligence

admin Help Messages

Dashboard Offenses Log Activity Network Activity Assets Reports Admin Cisco ISE pxGrid System Time

2018-02-16 21:22 - 2018-02-22 21:22

Data For : Quarantined_Systems

Show 10 entries

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.

IBM QRadar Security Intelligence

admin Help Messages

Dashboard Offenses Log Activity Network Activity Assets Reports Admin Cisco ISE pxGrid System Time

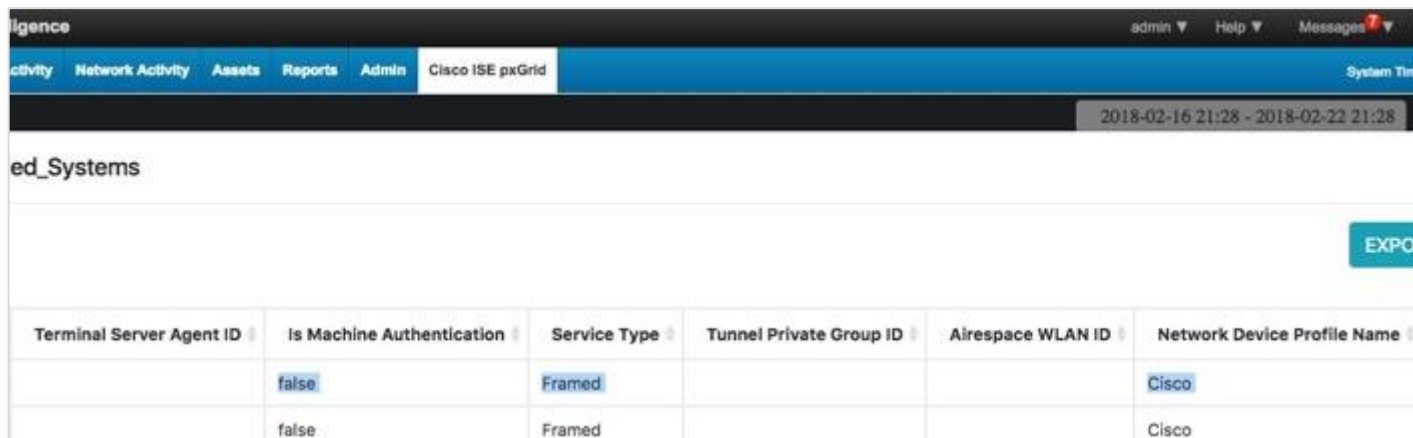
2018-02-16 21:26 - 2018-02-22 21:22

Data For : Quarantined_Systems

Show 10 entries

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-PCSE			LAB10	
	PXGRID2-PCSE			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 Select **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.

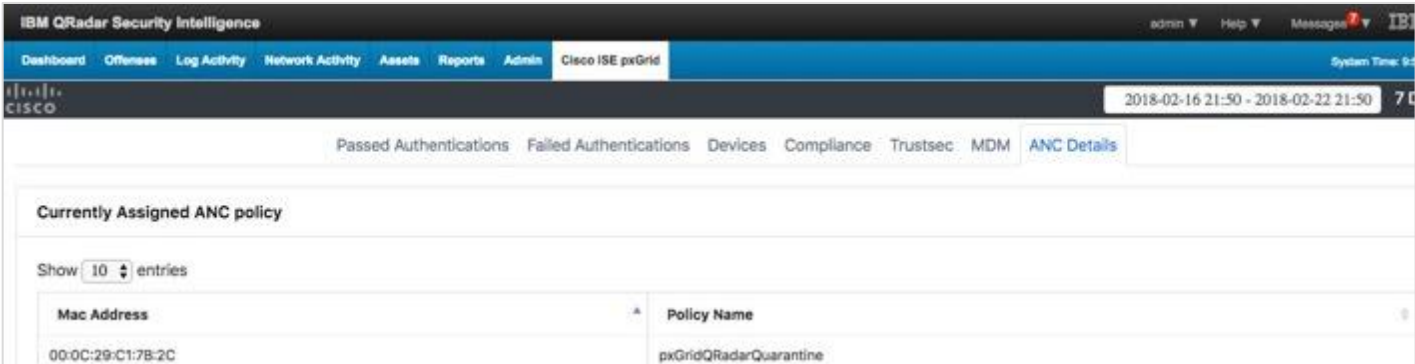


Username ^	MAC Address	IP Address	MDM MAC Address	OS Version	Registration Status	Compliance Status	Model	Manufacturer	UDID	Serial Num
pxgrid1	88:CB-87:ED:45:DA	192.168.1.11			True	True				
pxgrid1	88:CB-87:ED:45:DA	192.168.1.11			True	True				

ANC Details

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

Step 1 Select **Cisco ISE pxGrid > ANC Details**



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 to, and the end-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 on, when configuring the Cisco ISE pxGrid for pxGrid integration.

Configuring Default ANC policies for Cisco ISE pxGrid App

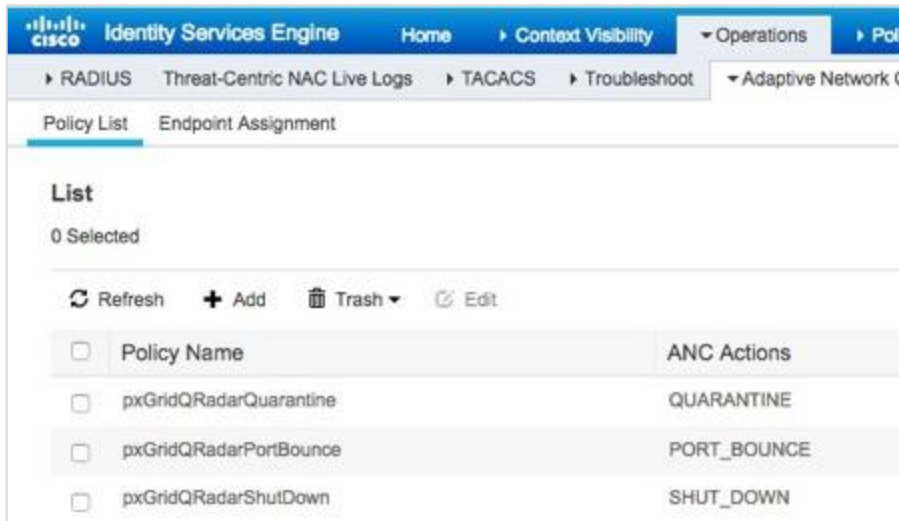
Note: When you setup the QRadar, pxGrid app will automatically create default ANC policies if they don't exist. These policies shown in the paragraph about are hard coded and cannot be edited. If you have other policies, you will need to integrate them manually on ISE. These policies are populated after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

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

pxGridQRadarQuarantine, QUARANTINE

pxGridQRadatShutDown, SHUT_DOWN,

Step 2 Select **Save** after **Policy Name** and associated action, you should see:



Policy Name	ANC Actions
pxGridQRadarQuarantine	QUARANTINE
pxGridQRadarPortBounce	PORT_BOUNCE
pxGridQRadarShutDown	SHUT_DOWN

Adding ANC Policies to ISE Policy Sets

Step 1 Select **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**

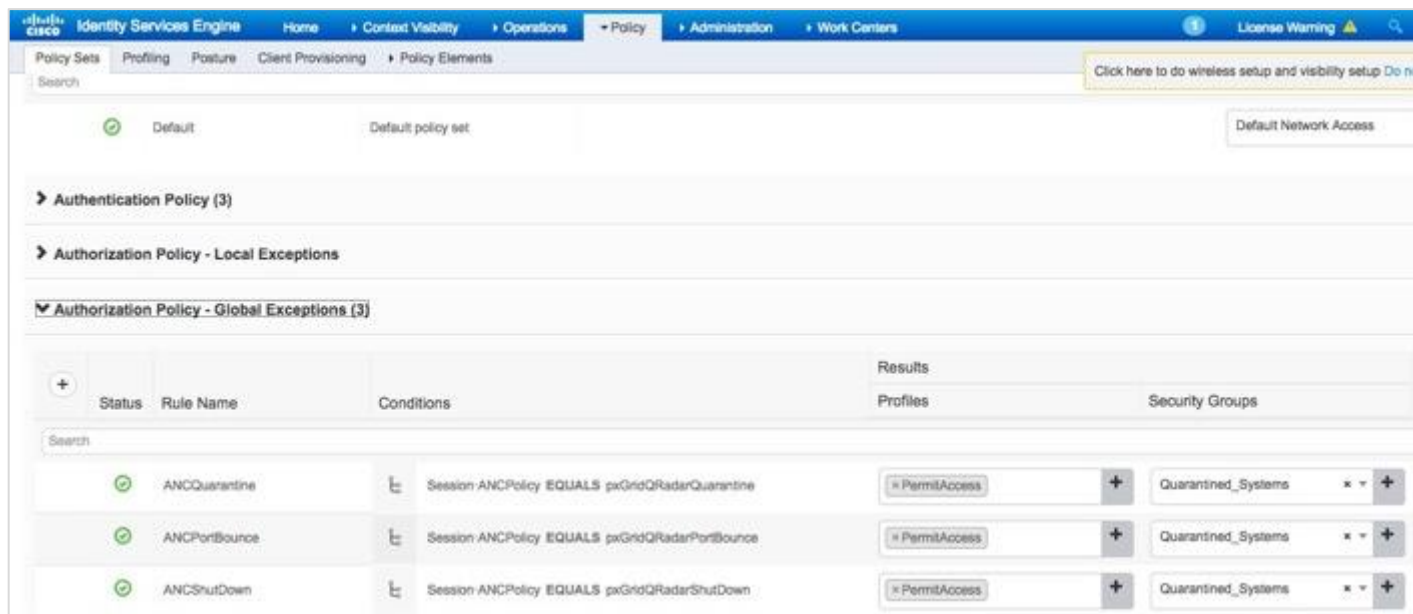
Step 10 Perform steps 1-9 for the Rule Name ANCSHutDown and ANCPolicy pxGridQRadarShutDown

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

Step 12 You should see the following:



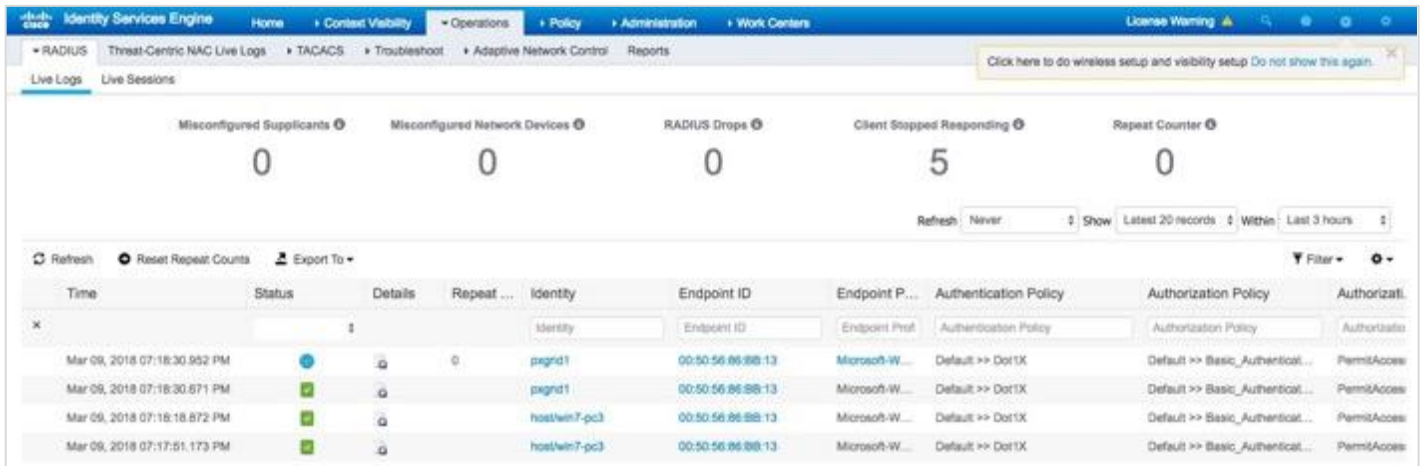
The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Policy' section is active, showing a search bar and a 'Default' policy set. Below this, there are expandable sections for 'Authentication Policy (3)', 'Authorization Policy - Local Exceptions', and 'Authorization Policy - Global Exceptions (3)'. The 'Global Exceptions' section is expanded, revealing a table with the following data:

+	Status	Rule Name	Conditions	Results	
				Profiles	Security Groups
	✔	ANCQuarantine	Session ANCPolicy EQUALS pxGridQRadarQuarantine	PermitAccess	Quarantined_Systems
	✔	ANCPortBounce	Session ANCPolicy EQUALS pxGridQRadarPortBounce	PermitAccess	Quarantined_Systems
	✔	ANCShutDown	Session ANCPolicy EQUALS pxGridQRadarShutDown	PermitAccess	Quarantined_Systems

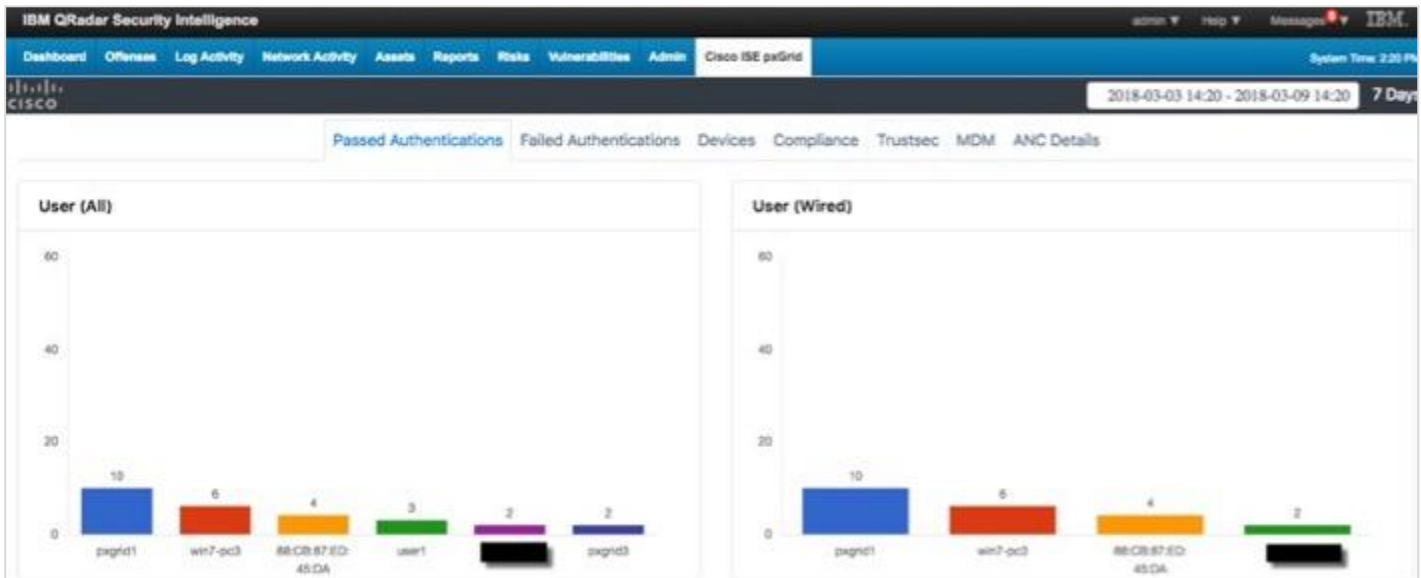
Performing Cisco ISE ANC Mitigation Actions Through Cisco ISE pxGrid App Dashboard Panel

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 Select Cisco ISE pxGrid > Passed Authentications



Step 3 Select an end user, pxGrid1, and then see the following:

Dev Time	IP Address	State	MAC Address	Username	Calling Station ID	Called StationID	NAS IP Address	NAS Port ID	NAS P
08-Mar-2018 10:11:31.641 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
08-Mar-2018 10:41:59.690 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
08-Mar-2018 10:53:16.962 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

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

Dev Time	IP Address	State	MAC Address	Username	Calling Station ID	Called StationID	NAS IP Address	NAS Port ID	NAS P
08-Mar-2018 10:11:31.641 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
08-Mar-2018 10:41:59.690 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
08-Mar-2018 10:53:16.962 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
08-Mar-2018 10:56:56.250 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

Step 5 Select pxGridQRadarQuarantine

Step 6 You should see a successful status message:

192.168.1.192 Says

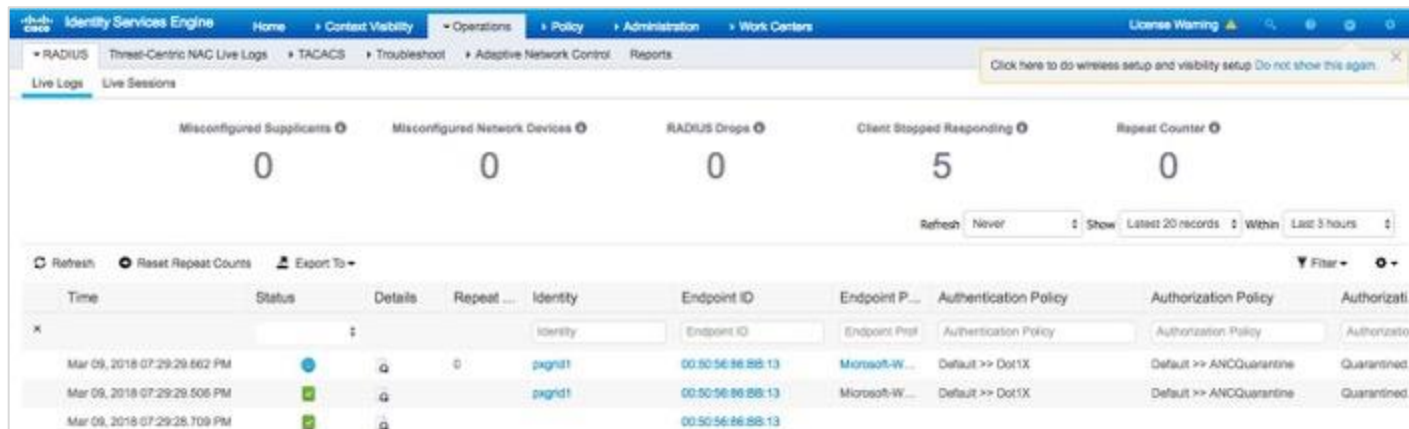
Status : RUNNING
Operation Id : ise24k.lab10.com:1

OK

Step 7 Select OK

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

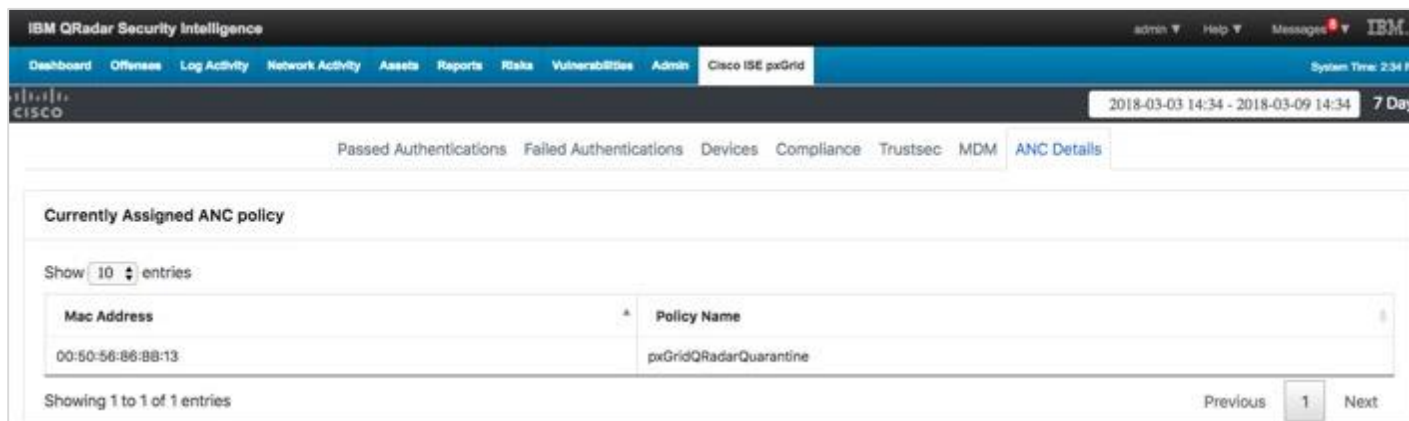
Based on the ANCQuarantine Policy, the endpoint has been quarantined:



Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorizati.
Mar 09, 2018 07:29:28.602 PM	●		0	pxgrid1	00:50:56:86:BB:13	Microsoft-W...	Default >> Dot1X	Default >> ANCQuarantine	Quarantined.
Mar 09, 2018 07:29:29.506 PM	●			pxgrid1	00:50:56:86:BB:13	Microsoft-W...	Default >> Dot1X	Default >> ANCQuarantine	Quarantined.
Mar 09, 2018 07:29:28.709 PM	●				00:50:56:86:BB:13				

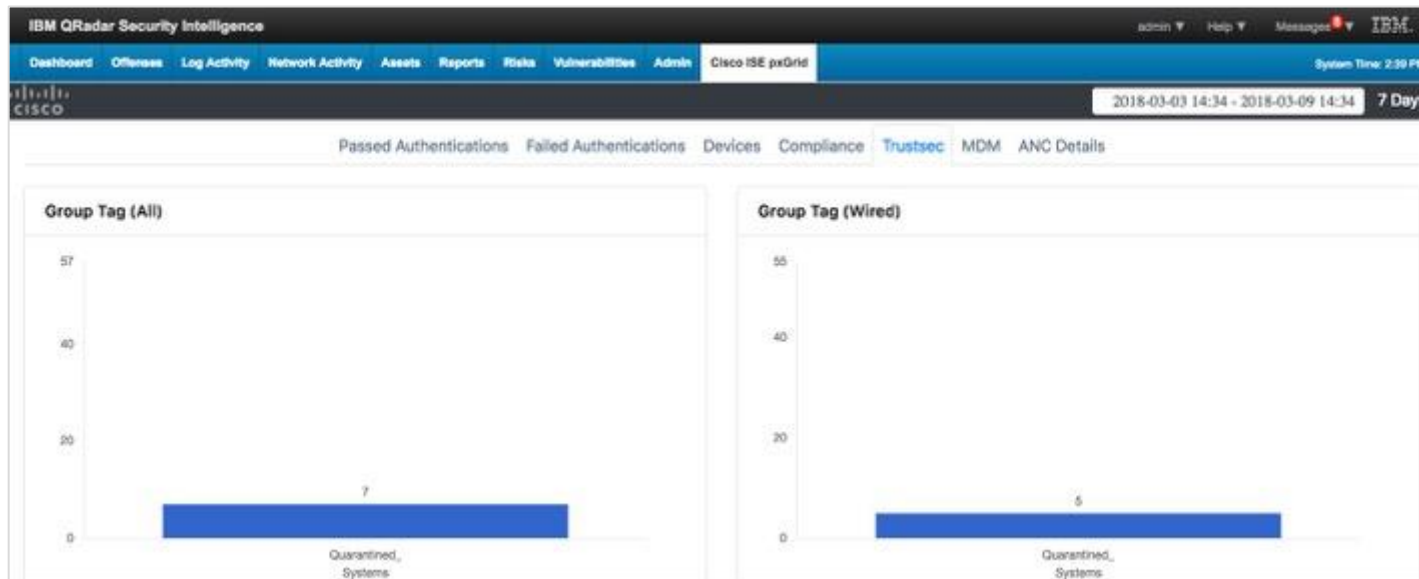
Step 9 To view the quarantine details in the Cisco ISE pxGrid App ANC Dashboard, select **Cisco ISE pxGrid > ANC Details**

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

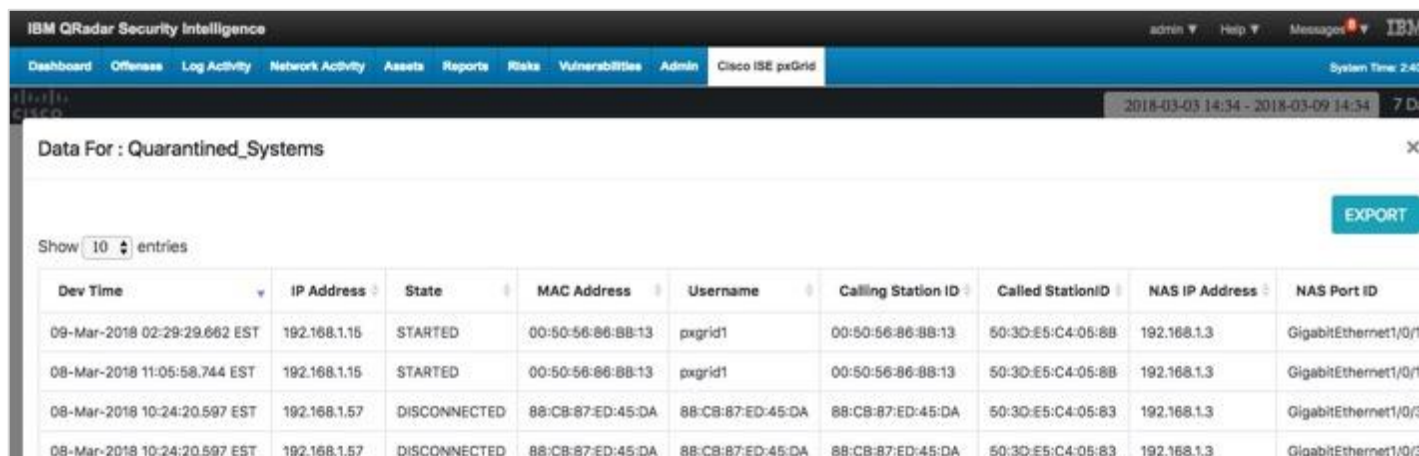


Mac Address	Policy Name
00:50:56:86:BB:13	pxGridQRadarQuarantine

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



Step 11 To see the quarantined endpoints, select **Quarantined_Systems**:



The screenshot shows the IBM QRadar Security Intelligence dashboard with the 'Data For : Quarantined_Systems' view selected. The table displays the following data:

Dev Time	IP Address	State	MAC Address	Username	Calling Station ID	Called StationID	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	GigabitEthernet1/0/5
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	GigabitEthernet1/0/5

Step 12 You have the option of un-quarantine or clearing the endpoint either through the Dashboards or directly in ISE. We will un-quarantine the endpoint from this view.

Step 13 Right-click on the MAC Address:

Dev Time	IP Address	State	MAC Address	Username	Calling Station ID	Called StationID	NAS IP Address	NAS Port ID
09-Mar-2018 02:29:29.662 EST	192.168.1.15	STARTED	00:50:56:86:88:13		00:50:56:86:88:13	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	00:50:56:86:88:13		00:50:56:86:88:13	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	DA	88:CB:87:ED:45:DA	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:C4:05:8B	192.168.1.3	GigabitEthernet1/0/1

Step 14 Select **pxGridQRadarClear**

Step 15 You should see successful status message:

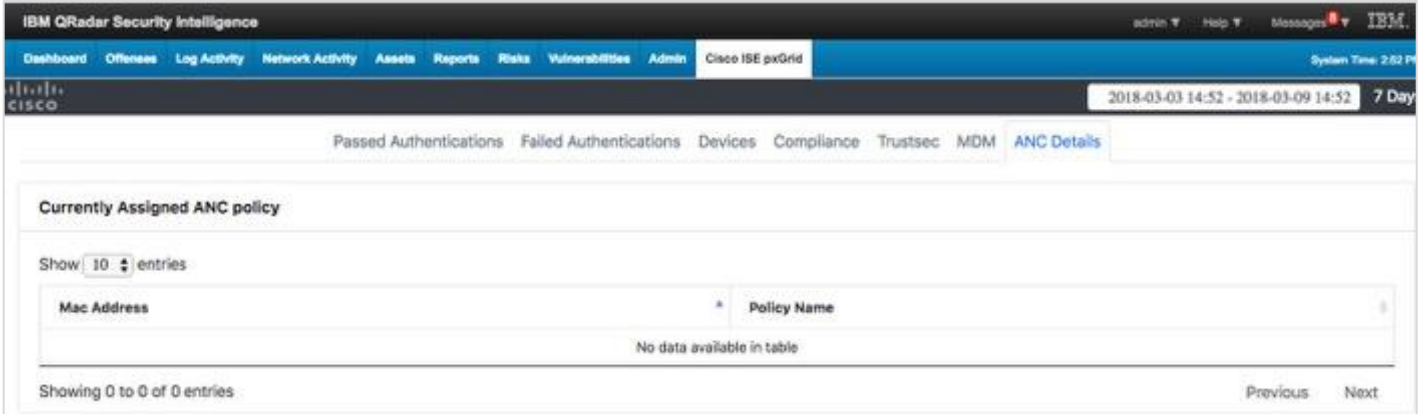
Step 16 Select **OK**

Step 17 To un-quarantine the endpoints and view the results in ISE:

Select **Operations > RADIUS > Live Logs**

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorizat...
Mar 09, 2018 07:48:43.693 PM	●	q	0	pxgrid1	00:50:56:86:88:13	Microsoft-W...	Default >> Dot1X	Default >> Basic_Authenticat...	PermitAccess
Mar 09, 2018 07:48:42.916 PM	●	q		pxgrid1	00:50:56:86:88:13	Microsoft-W...	Default >> Dot1X	Default >> Basic_Authenticat...	PermitAccess
Mar 09, 2018 07:45:52.604 PM	●	q		pxgrid1	00:50:56:86:88:13	Microsoft-W...	Default >> Dot1X	Default >> Basic_Authenticat...	PermitAccess

Step 18 Select **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: select **Operations > Adaptive Network Control > Endpoint Assignment > Select the endpoint MAC address > Tras**

Configuring IBM QRadar for Cisco ISE Syslog Events

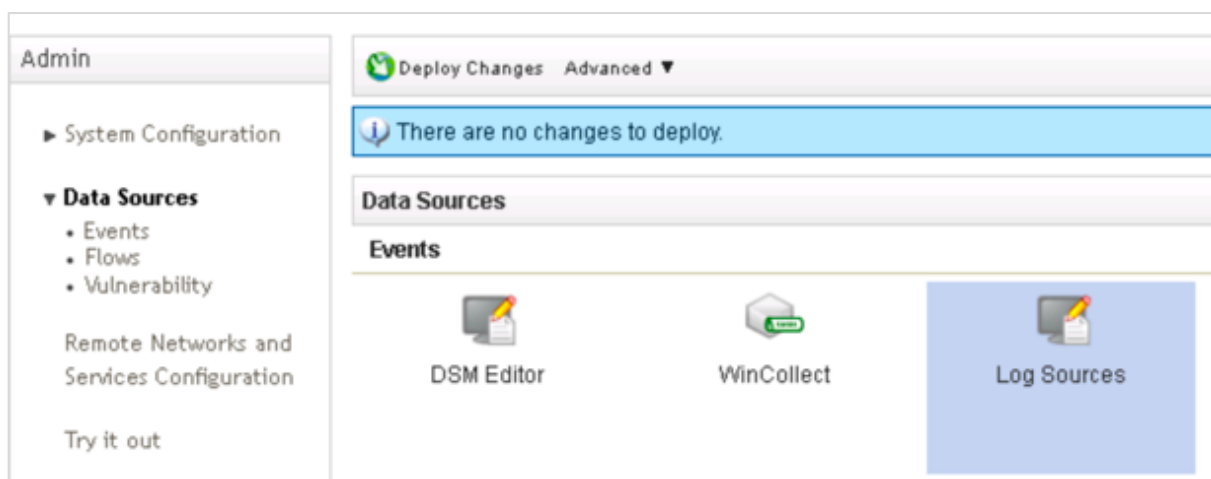
The IBM Device Support Module (DSM) for Cisco Identity Service Engine (ISE) Syslog is installed by default on QRadar. For more information on DSM (beyond the scope of this guide) visit the [DSM guide](#).

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. Select **Admin > Data Sources > Log Sources**

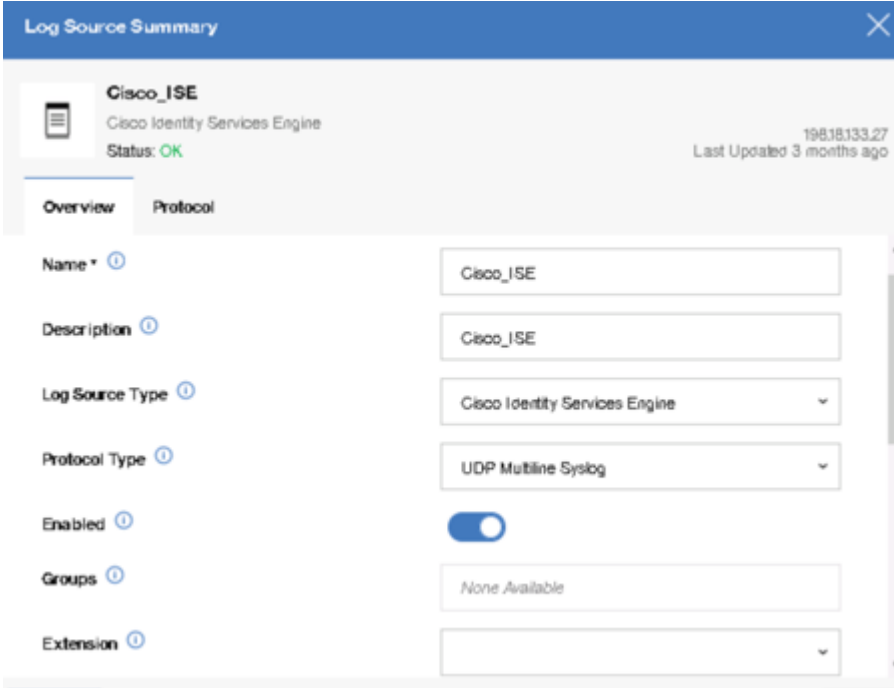


- c. Add in a new log source for Cisco ISE Syslog

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.



Log Source Summary

Cisco_ISE
Cisco Identity Services Engine
Status: OK
198.18.133.27
Last Updated 3 months ago

Overview Protocol

Name *

Description

Log Source Type

Protocol Type

Enabled

Groups

Extension

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**

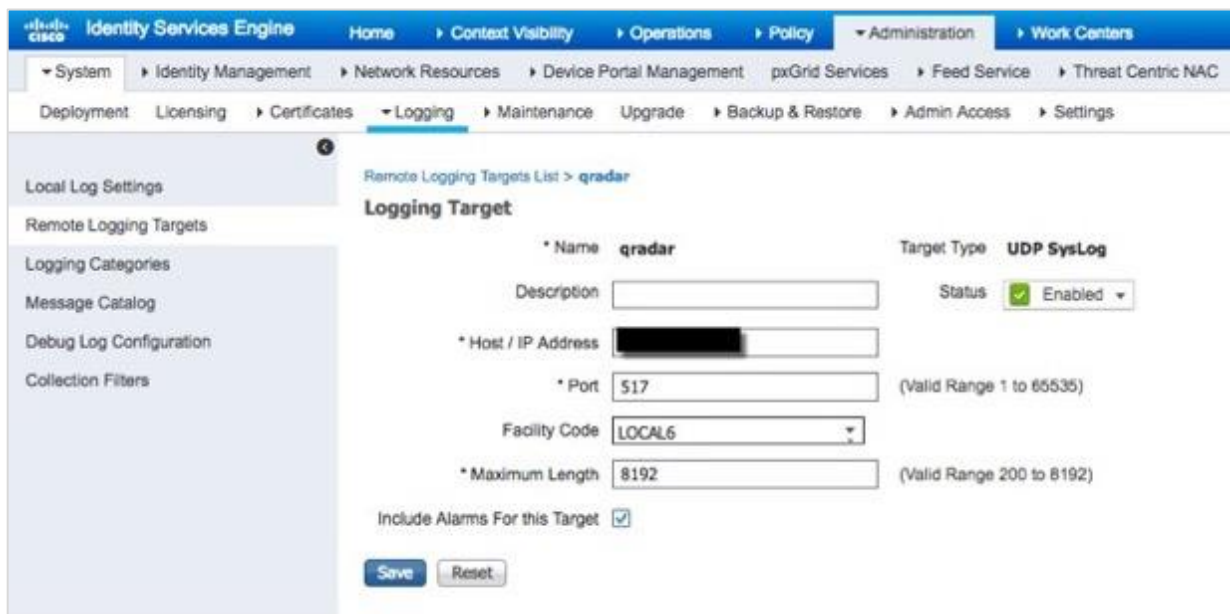
Configuring Cisco ISE Syslog Events

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 Select **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 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:

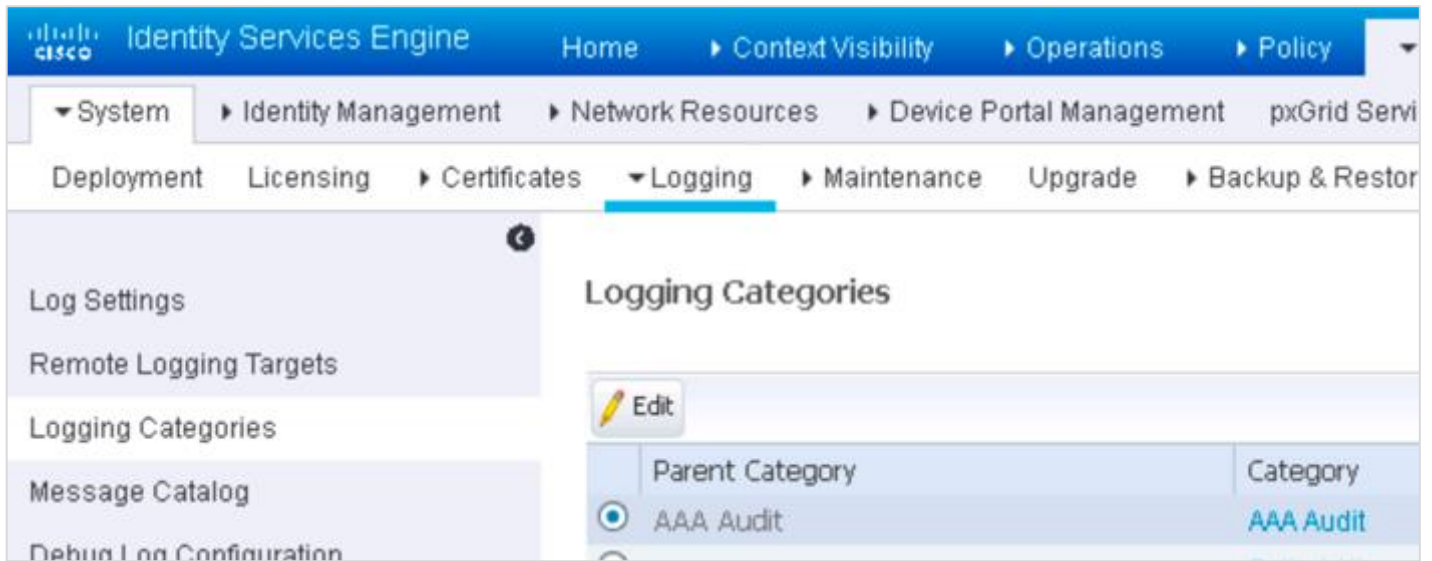
* Name	qradar	Target Type	UDP SysLog
Description	<input type="text"/>	Status	<input checked="" type="checkbox"/> Enabled
* Host / IP Address	<input type="text"/>		
* Port	517	(Valid Range 1 to 65535)	
Facility Code	LOCAL6		
* Maximum Length	8192	(Valid Range 200 to 8192)	
Include Alarms For this Target	<input checked="" type="checkbox"/>		

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

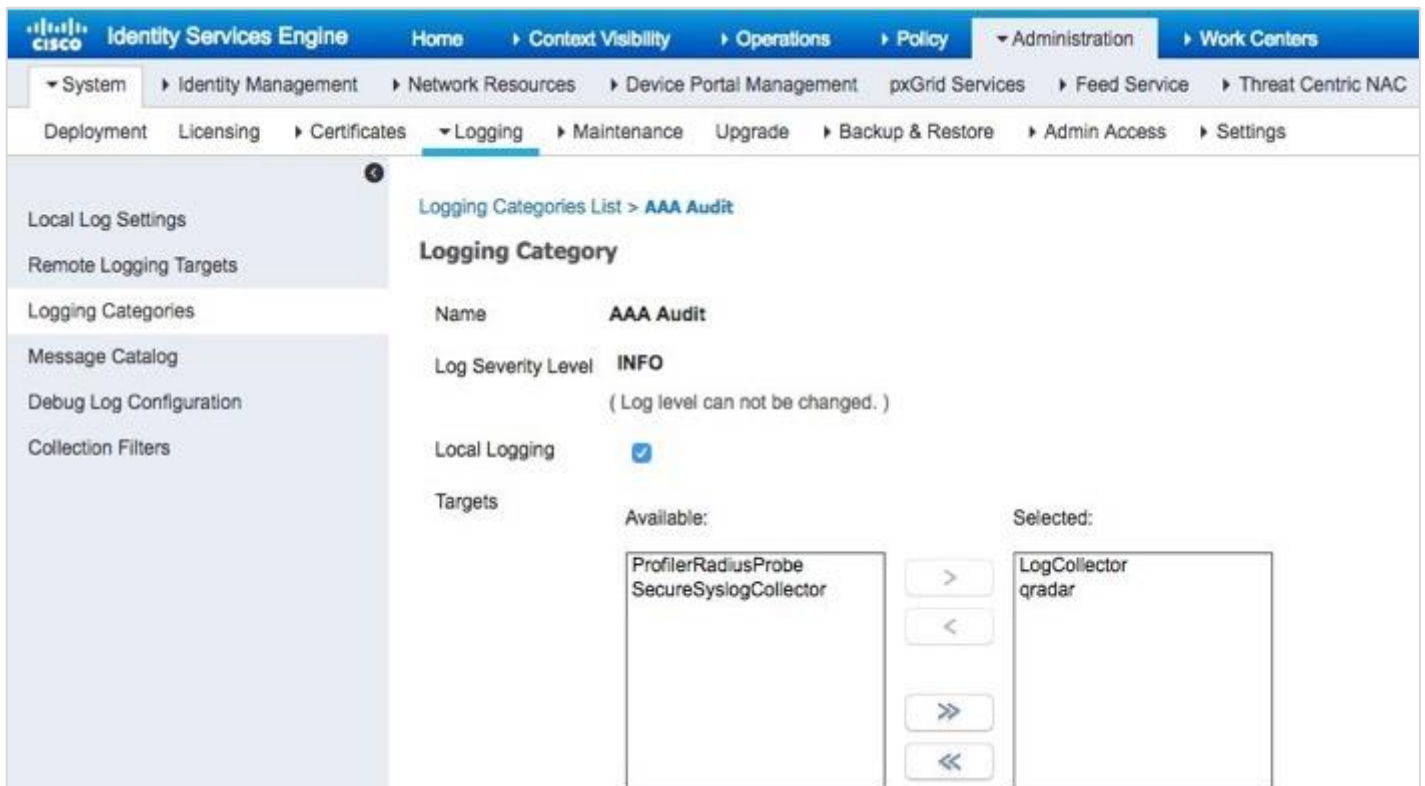
Step 3 Select **Submit/Save**

Step 4 Configure **Logging Categories**:

Choose **AAA Audit element > Edit**



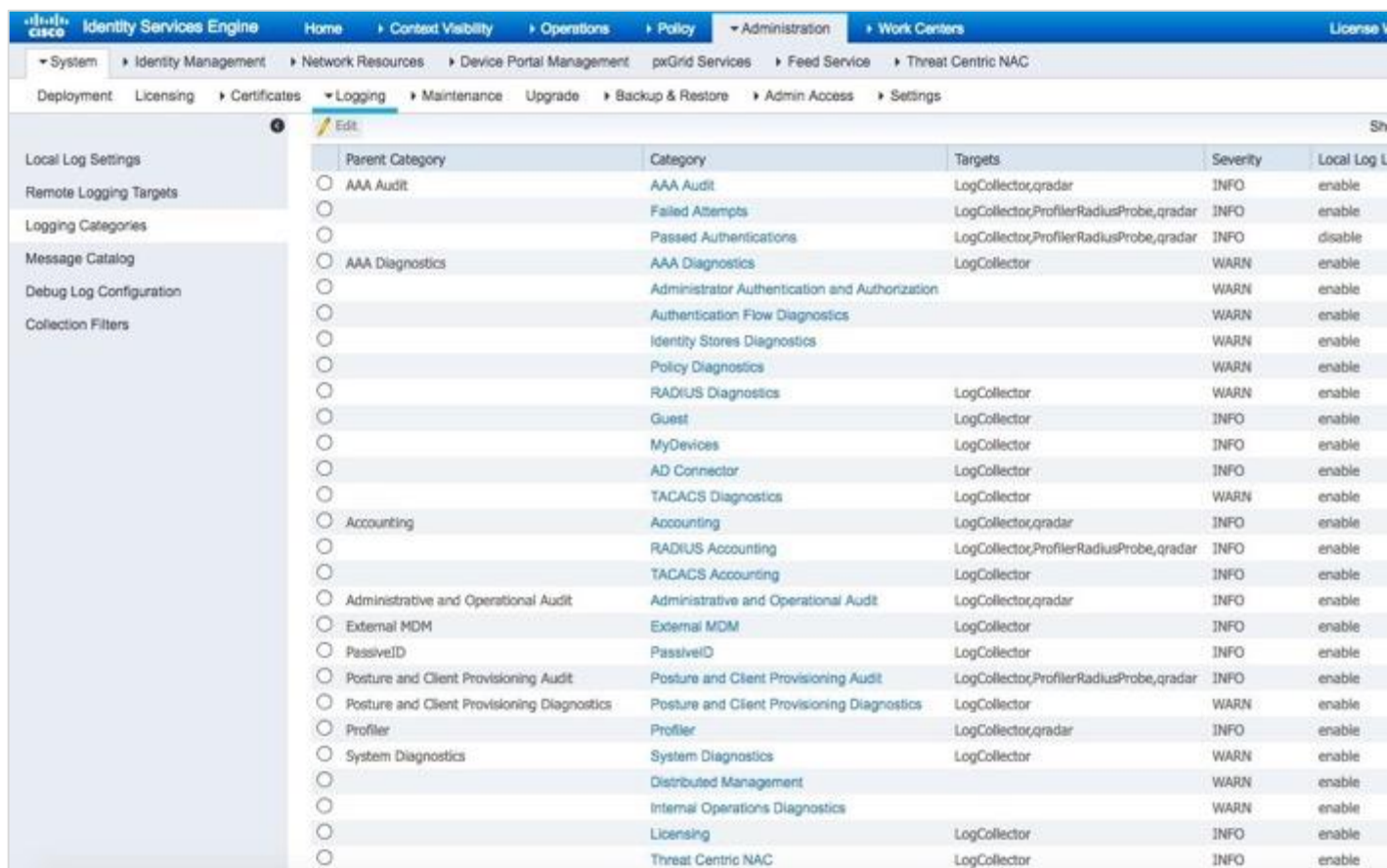
Step 5 Move QRadar from Targets **Available** into the **Selected** column. Don't worry about the local logging checkbox, leave it alone.



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.

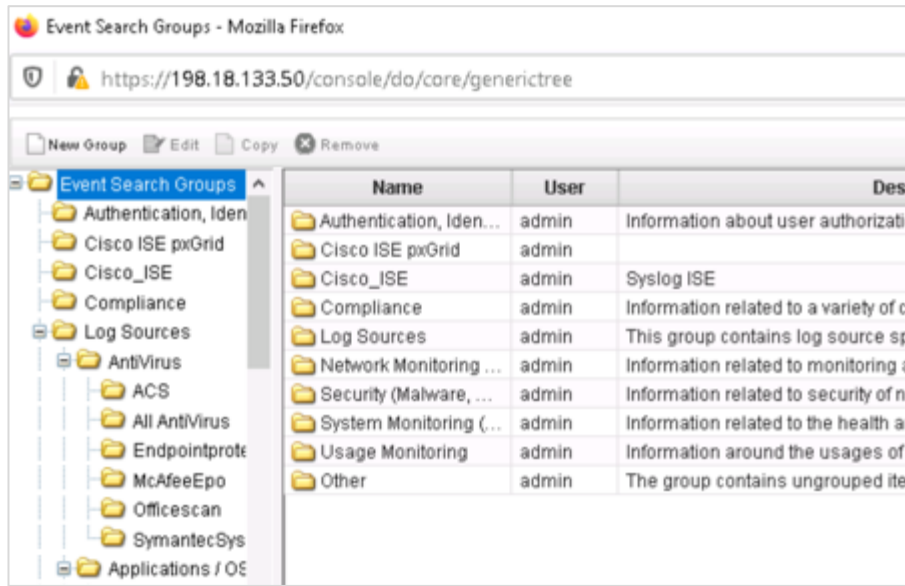
Note: You will see a group already created for Cisco ISE pxGrid. This is strictly to use with pxGrid data sources. The following group you're making is for additional support of syslog messages that provide more information than the pxGrid source. This helps you working with additional functionality 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, select **Log Activity > Search > New Search > Manage Groups**

Create **New Group > Cisco_ISE**

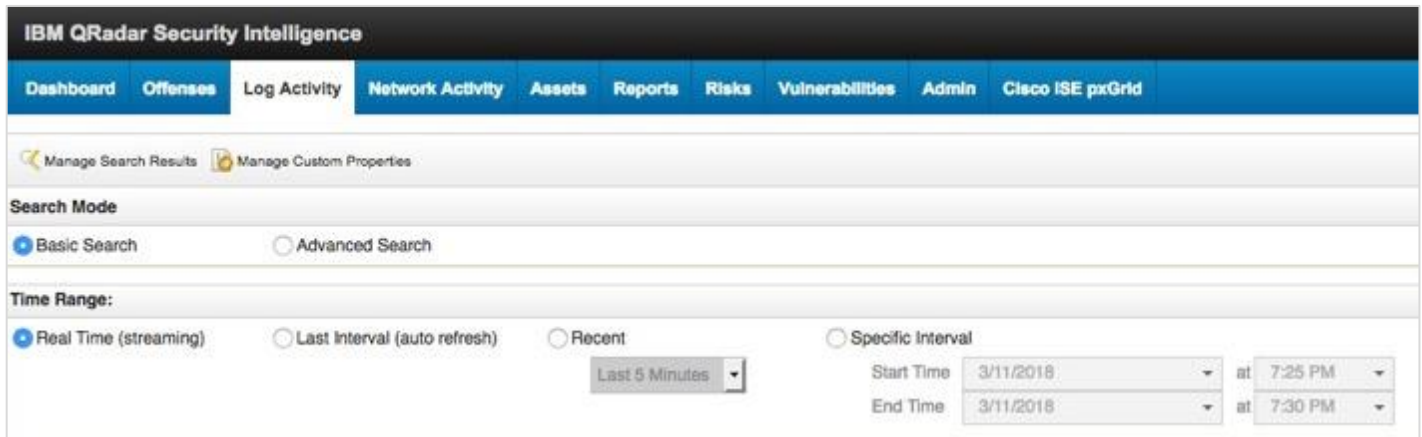
You should see the Cisco ISE group:



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:

Results Limit

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

Select **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: Display:

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**

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin Pu

Return to Event List Offense Map Event False Positive Extract Property Previous Next Print Obfuscation

Extract a custom property from the payload of this event

Event Information

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: Select a property...
 New Property: FramedIPAddress
 Optimize parsing for rules, reports, and searches
 Field Type: IP
 Description: FramedIPAddress

Property Expression Definition

Enabled:

Selection

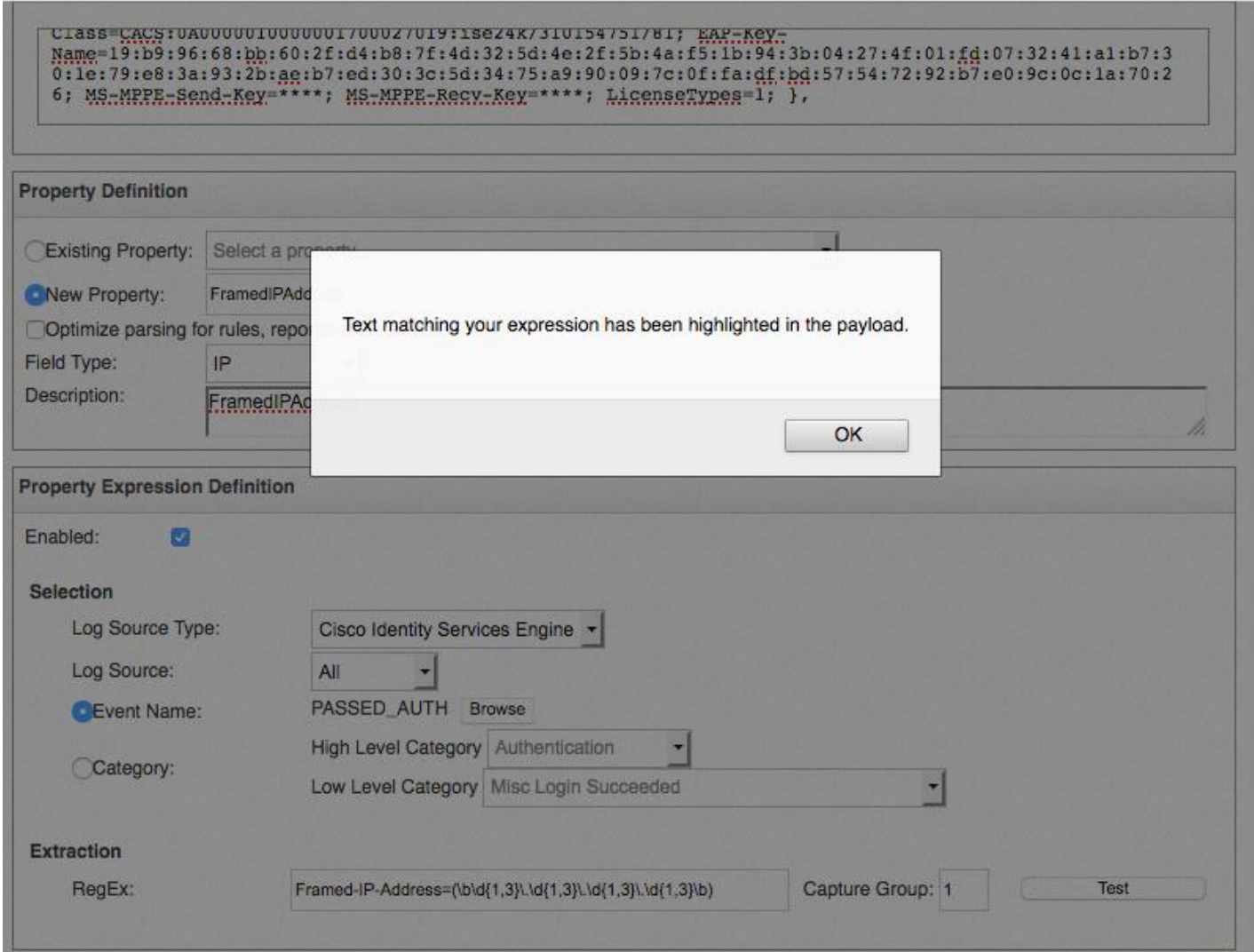
Log Source Type: Cisco Identity Services Engine
 Log Source: All
 Event Name: PASSED_AUTH Browse
 Category: High Level Category: Authentication
 Low Level Category: Misc Login Succeeded

Extraction

RegEx: Framed-IP-Address=(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b) Capture Group: 1 Test

Step 12 Select **Test**

You should see:



The screenshot displays the configuration interface for a property definition. At the top, a text box contains a JSON payload with several fields highlighted in red, including `MS-MPPE-Send-Key`, `MS-MPPE-Recv-Key`, and `LicenseTypes`. Below this is the **Property Definition** section, where the **New Property** radio button is selected, and the field type is set to **IP**. A dialog box is overlaid on the interface, displaying the message: "Text matching your expression has been highlighted in the payload." with an **OK** button. The **Property Expression Definition** section is also visible, showing the **Enabled** checkbox checked, the **Log Source Type** set to **Cisco Identity Services Engine**, and the **Event Name** set to **PASSED_AUTH**. The **Extraction** section shows a **Regex** expression: `Framed-IP-Address=(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b)` and a **Capture Group** of **1**. A **Test** button is present at the bottom right of the configuration area.

Step 13 Select **OK**Step 14 Select **Save**

Step 15 Ensure you see you see the FramedIPAddress appear:



The screenshot shows the IBM QRadar Security Intelligence interface. The top navigation bar includes 'Dashboard', 'Offenses', 'Log Activity', 'Network Activity', 'Assets', 'Reports', 'Risks', 'Vulnerabilities', 'Admin', and 'Cisco ISE pxGrid'. Below the navigation bar is a toolbar with icons for 'Return to Event List', 'Offense', 'Map Event', 'False Positive', 'Extract Property', 'Previous', 'Next', 'Print', and 'Obfuscation'. The main content area is titled 'Event Information' and contains a table with the following data:

Event Name	PASSED_AUTH			
Low Level Category	Misc Login Succeeded			
Event Description	User authentication ended successfully			
Magnitude		(5)	Relevance	10
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

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	pxgnd1	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_FAILED	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 Fal...	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

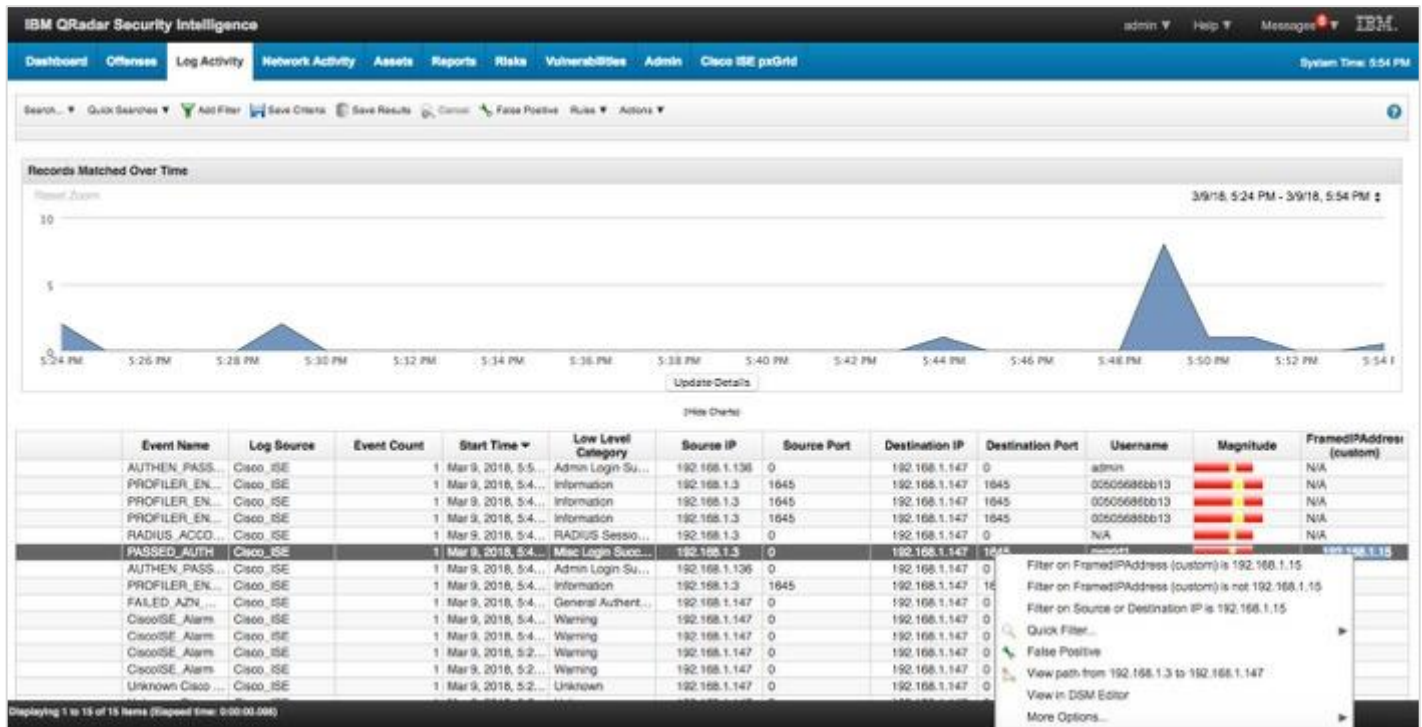
ANC Mitigation Syslog Event Example

Step 1 The user has been successfully authenticated through ISE

Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorizati.
Mar 08, 2018 10:49:41.441 PM	Success		0	pxgnd1	00:50:56:86:88:13	Microsoft-W...	Default >> Dot1X	Default >> Basic_Authenticat...	PermitAcces...
Mar 08, 2018 10:49:40.488 PM	Success		0	pxgnd1	00:50:56:86:88:13	Microsoft-W...	Default >> Dot1X	Default >> Basic_Authenticat...	PermitAcces...

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**

IBM QRadar Security Intelligence admin Help Messages IBM

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin Cisco ISE pxGrid System Time: 5:57 PM

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

Records Matched Over Time

Reset Zoom 3/9/18, 5:24 PM - 3/9/18, 5:54 PM

Update Details (Hide Charts)

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	3	N/A
PROFILER_EN...	Cisco_ISE	1	Mar 9, 2018, 5:4...	Information	192.168.1.3	1645	192.168.1.147	1645	00505686bb13	3	N/A
PROFILER_EN...	Cisco_ISE	1	Mar 9, 2018, 5:4...	Information	192.168.1.3	1645	192.168.1.147	1645	00505686bb13	3	N/A
PROFILER_EN...	Cisco_ISE	1	Mar 9, 2018, 5:4...	Information	192.168.1.3	1645	192.168.1.147	1645	00505686bb13	3	N/A
RADIUS_ACCO...	Cisco_ISE	1	Mar 9, 2018, 5:4...	RADIUS Sessio...	192.168.1.3				N/A	3	N/A
PASSED_AUTH...	Cisco_ISE	1	Mar 9, 2018, 5:4...	Miss Login Succ...	192.168.1.3					3	192.168.1.15
AUTHEN_PASS...	Cisco_ISE	1	Mar 9, 2018, 5:4...	Admin Login Su...	192.168.1.136					3	
PROFILER_EN...	Cisco_ISE	1	Mar 9, 2018, 5:4...	Information	192.168.1.3					3	
FAILED_AZN...	Cisco_ISE	1	Mar 9, 2018, 5:4...	General Authent...	192.168.1.147					3	
CiscoISE_Alarm	Cisco_ISE	1	Mar 9, 2018, 5:4...	Warning	192.168.1.147					3	
CiscoISE_Alarm	Cisco_ISE	1	Mar 9, 2018, 5:4...	Warning	192.168.1.147					3	
CiscoISE_Alarm	Cisco_ISE	1	Mar 9, 2018, 5:2...	Warning	192.168.1.147					3	
CiscoISE_Alarm	Cisco_ISE	1	Mar 9, 2018, 5:2...	Warning	192.168.1.147					3	
Unknown Cisco...	Cisco_ISE	1	Mar 9, 2018, 5:2...	Unknown	192.168.1.147					3	

Displaying 1 to 15 of 15 items (Elapsed time: 0:00:06.096)

Filter on FramedIPAddress (custom) is 192.168.1.15

Filter on FramedIPAddress (custom) is not 192.168.1.15

Filter on Source or Destination IP is 192.168.1.15

Quick Filter...

False Positive

View path from 192.168.1.3 to 192.168.1.147

View in DSM Editor

More Options...

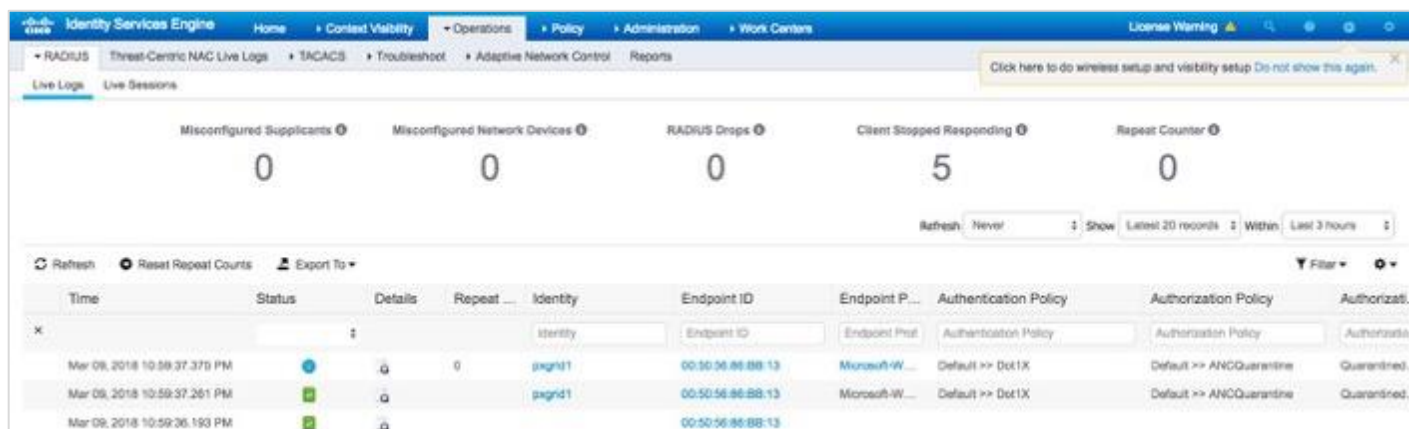
Step 4 You should see a successful status message:



Step 5 Select OK

Step 6 To view in ISE, select **Operations > RADIUS > Live Logs**

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

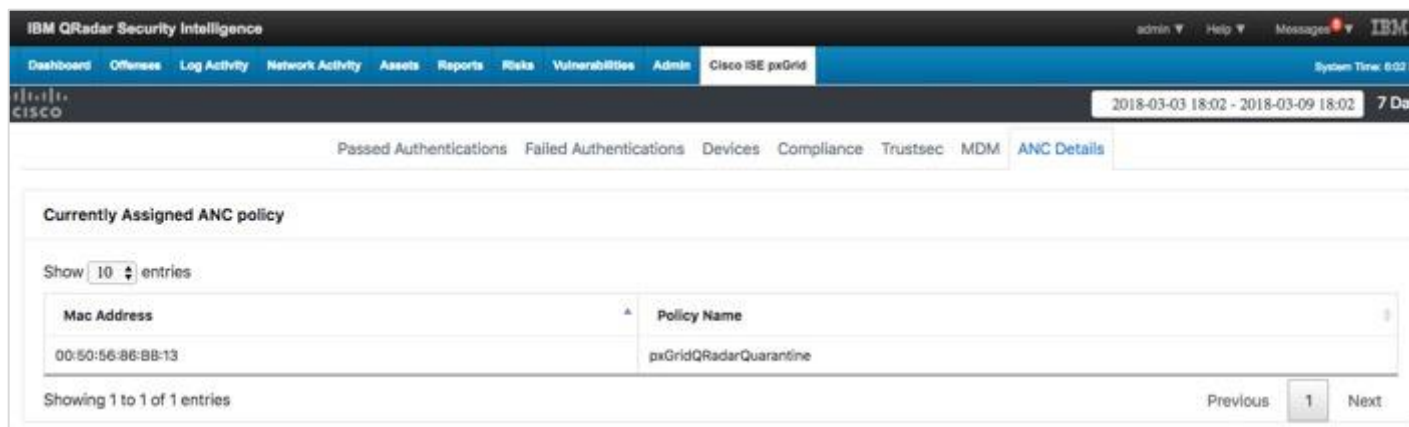


The screenshot shows the Cisco ISE RADIUS Live Logs interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Operations' tab is selected, and the 'Live Logs' sub-tab is active. The main content area displays a table of live logs with columns for Time, Status, Details, Repeat, Identity, Endpoint ID, Endpoint P..., Authentication Policy, Authorization Policy, and Authorizati... The table shows three entries, all with a status of 'Quarantined' and an identity of 'pxGrid1'. The first entry is highlighted with a red 'X' in the first column.

Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorizati...
Mar 09, 2018 10:59:37.370 PM	Quarantined	q	0	pxGrid1	00:50:56:86:BB:13	Microsoft-W...	Default >> Dot1X	Default >> ANCQuarantine	Quarantined
Mar 09, 2018 10:59:37.261 PM	Quarantined	q		pxGrid1	00:50:56:86:BB:13	Microsoft-W...	Default >> Dot1X	Default >> ANCQuarantine	Quarantined
Mar 09, 2018 10:59:36.193 PM	Quarantined	q			00:50:56:86:BB:13				

Step 7 To view in Cisco ISE pxGrid ANC Details Dashboard, select **Cisco ISE pxGrid > ANC Details**

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

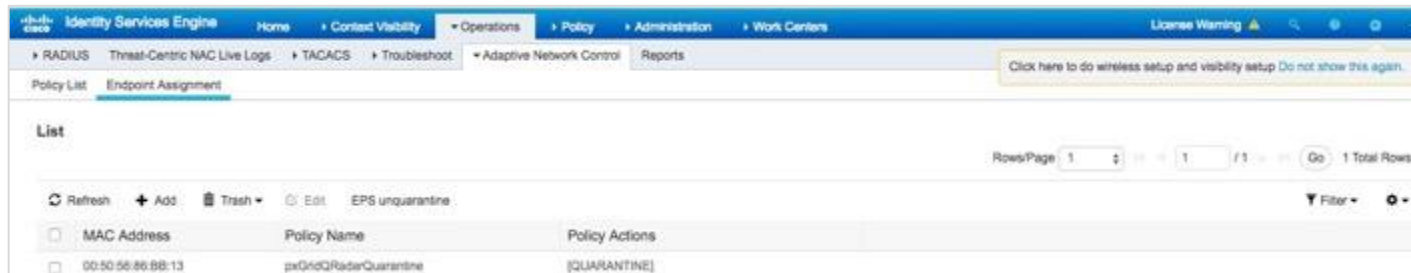


The screenshot shows the Cisco ISE pxGrid ANC Details Dashboard. The top navigation bar includes 'Dashboard', 'Offenses', 'Log Activity', 'Network Activity', 'Assets', 'Reports', 'Risks', 'Vulnerabilities', 'Admin', and 'Cisco ISE pxGrid'. The 'Cisco ISE pxGrid' tab is selected, and the 'ANC Details' sub-tab is active. The main content area displays the 'Currently Assigned ANC policy' section. The 'Show' dropdown is set to '10' entries. The table shows one entry with a Mac Address of '00:50:56:86:BB:13' and a Policy Name of 'pxGridQRadarQuarantine'.

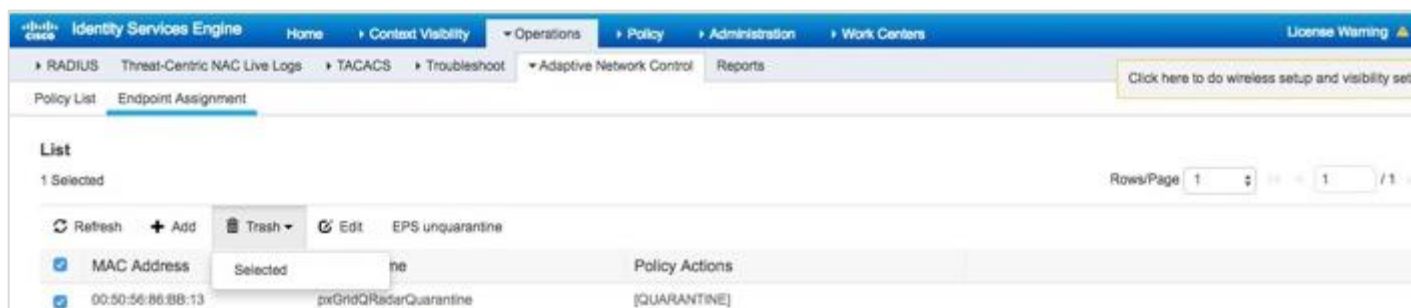
Mac Address	Policy Name
00:50:56:86:BB:13	pxGridQRadarQuarantine

Step 8 To un-quarantine or clear the endpoint:

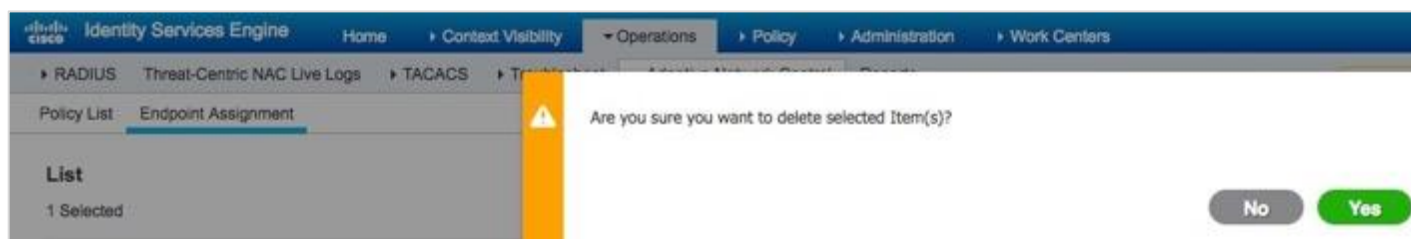
Select **ISE > Operations > Adaptive Network Control > Endpoint Assignment**



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, select **Operations > RADIUS-Live Logs**

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

The screenshot shows the Cisco Identity Services Engine (ISE) interface. At the top, there are navigation tabs: Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Below these are sub-tabs: RADIUS, Threat-Centric NAC Live Logs, TACACS, Troubleshoot, Adaptive Network Control, and Reports. A notification banner at the top right says "Click here to do wireless setup and visibility setup. Do not show this again." Below the navigation is a summary section with five metrics: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (0), Client Stopped Responding (5), and Repeat Counter (0). Below this is a table of live sessions.

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorizat.
Mar 09, 2018 11:10:33.115 PM	●		0	pgnd1	00:50:56:86:88:13	Microsoft-W...	Default >> Dot1X	Default >> Basic_Authenticat...	PermitAccess
Mar 09, 2018 11:10:32.161 PM	■			pgnd1	00:50:56:86:88:13	Microsoft-W...	Default >> Dot1X	Default >> Basic_Authenticat...	PermitAccess
Mar 09, 2018 11:10:30.216 PM	■				00:50:56:86:88:13				

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 displays activity over time from Feb 10 to Feb 17. Below the chart is a table of log entries. A tooltip is visible over the 'Destination IP' field of the first entry, displaying contextual 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	Network: Net-10-172-192-Net_192_168_0_0 192.168.1.7 50111 Ethernet Ethernet 192.168.1.7 192.168.1.7 50111 Ethernet N/A 192.168.1.7 192.168.1.7 50111 Ethernet 192.168.1.7 192.168.1.7 50111 Ethernet N/A N/A 192.168.1.7 192.168.1.7 50111 Ethernet 192.168.1.7							
1 Feb 18, 2018, 4:15:28 PM	RADIUS Session Ended	192.168.1.3	0	paGrid Session details: 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

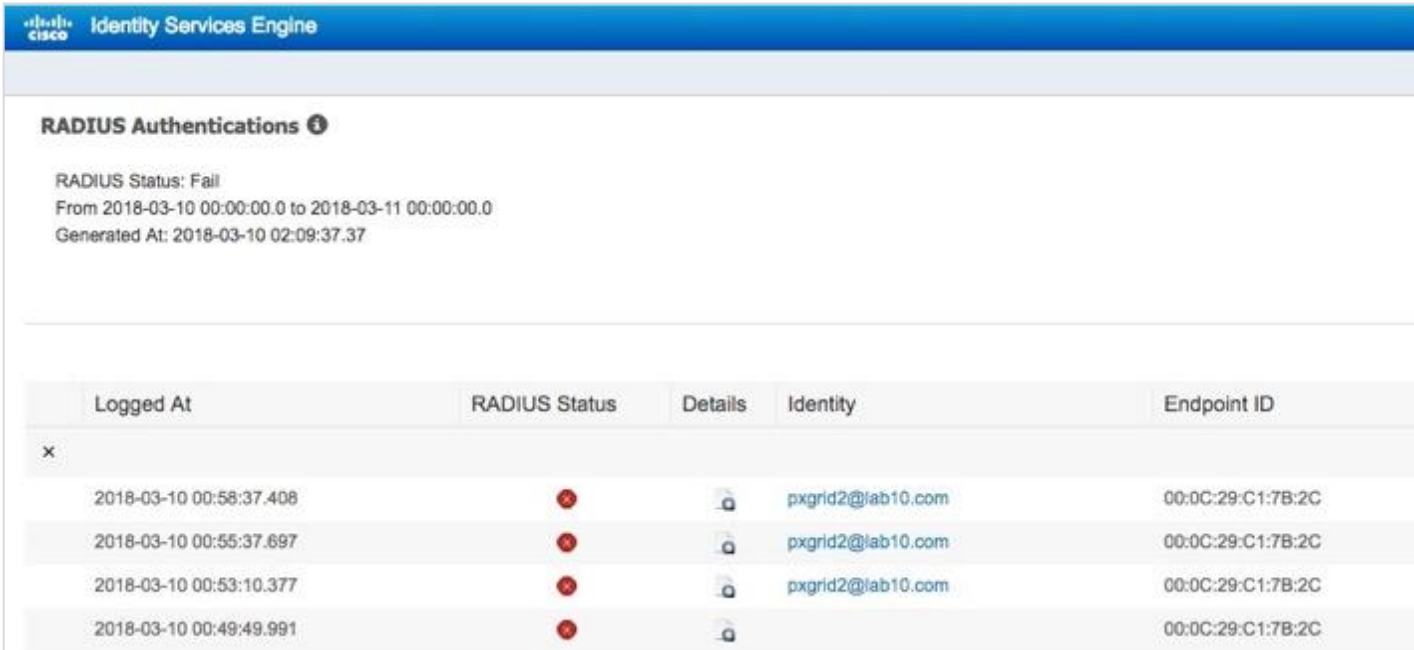
IBM QRadar Custom Rules Engine (CRE) displays the rules and building blocks that are used by IBM QRadar. The CRE provides information about how the rules are groups, the types of tests that the rules perform, and the rule responses. A rule is a collection of tests that triggers an action when specific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



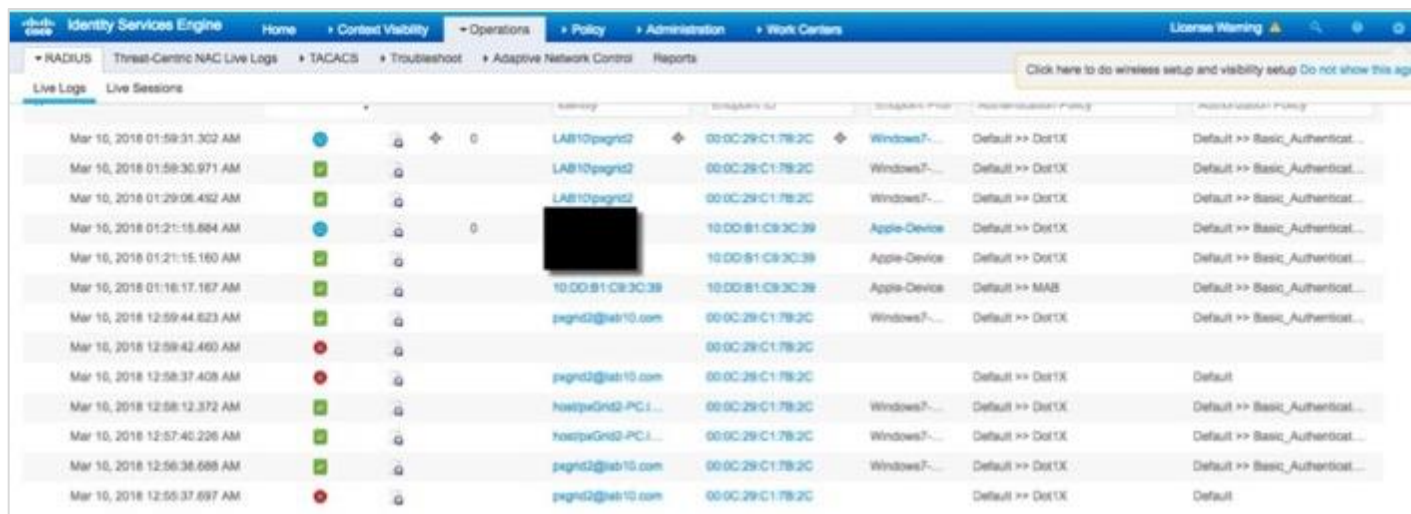
Identity Services Engine

RADIUS Authentications ⓘ

RADIUS Status: Fail
 From 2018-03-10 00:00:00.0 to 2018-03-11 00:00:00.0
 Generated At: 2018-03-10 02:09:37.37

Logged At	RADIUS Status	Details	Identity	Endpoint ID
x				
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

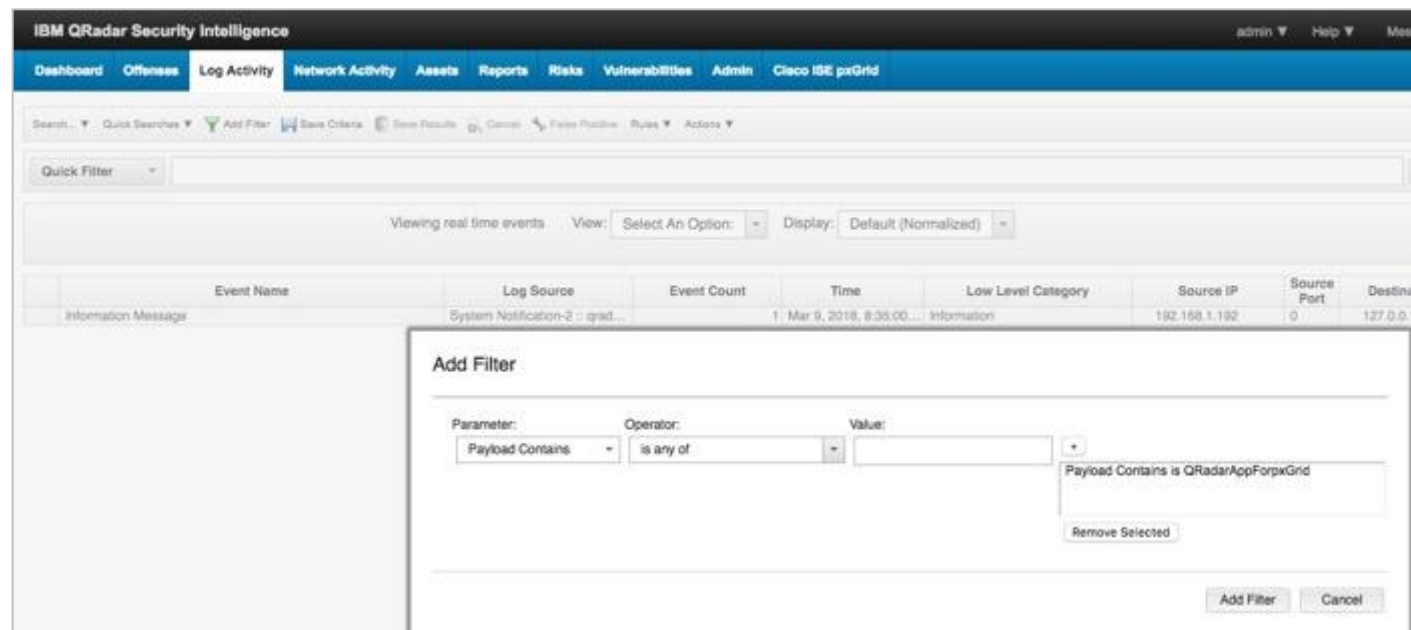
You can also view events in ISE.



Time	Status	Source IP	Source Port	Destination IP	Destination Port	Policy	Authentication Policy
Mar 10, 2018 01:59:31.302 AM	Success	LAB10pxgrid2	00:0C:29:C1:7B:2C	Windows7...	Default >> Dot1X	Default >> Basic_Authenticat...	
Mar 10, 2018 01:59:30.971 AM	Success	LAB10pxgrid2	00:0C:29:C1:7B:2C	Windows7...	Default >> Dot1X	Default >> Basic_Authenticat...	
Mar 10, 2018 01:29:06.452 AM	Success	LAB10pxgrid2	00:0C:29:C1:7B:2C	Windows7...	Default >> Dot1X	Default >> Basic_Authenticat...	
Mar 10, 2018 01:21:15.684 AM	Success	[REDACTED]	10:00:B1:C8:3C:39	Apple-Device	Default >> Dot1X	Default >> Basic_Authenticat...	
Mar 10, 2018 01:16:17.167 AM	Success	[REDACTED]	10:00:B1:C8:3C:39	Apple-Device	Default >> Dot1X	Default >> Basic_Authenticat...	
Mar 10, 2018 01:16:17.167 AM	Success	10:00:B1:C8:3C:39	10:00:B1:C8:3C:39	Apple-Device	Default >> MAB	Default >> Basic_Authenticat...	
Mar 10, 2018 12:59:44.623 AM	Success	pxgrid2@lab10.com	00:0C:29:C1:7B:2C	Windows7...	Default >> Dot1X	Default >> Basic_Authenticat...	
Mar 10, 2018 12:59:42.460 AM	Failure	[REDACTED]	00:0C:29:C1:7B:2C	Windows7...	Default >> Dot1X	Default	
Mar 10, 2018 12:58:37.408 AM	Failure	pxgrid2@lab10.com	00:0C:29:C1:7B:2C	Windows7...	Default >> Dot1X	Default	
Mar 10, 2018 12:58:12.372 AM	Success	hostpxGrid-PC1...	00:0C:29:C1:7B:2C	Windows7...	Default >> Dot1X	Default >> Basic_Authenticat...	
Mar 10, 2018 12:57:40.226 AM	Success	hostpxGrid-PC1...	00:0C:29:C1:7B:2C	Windows7...	Default >> Dot1X	Default >> Basic_Authenticat...	
Mar 10, 2018 12:56:36.688 AM	Success	pxgrid2@lab10.com	00:0C:29:C1:7B:2C	Windows7...	Default >> Dot1X	Default >> Basic_Authenticat...	
Mar 10, 2018 12:55:37.697 AM	Failure	pxgrid2@lab10.com	00:0C:29:C1:7B:2C	Windows7...	Default >> Dot1X	Default	

Verify pxGrid offense rule via Log Activity

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



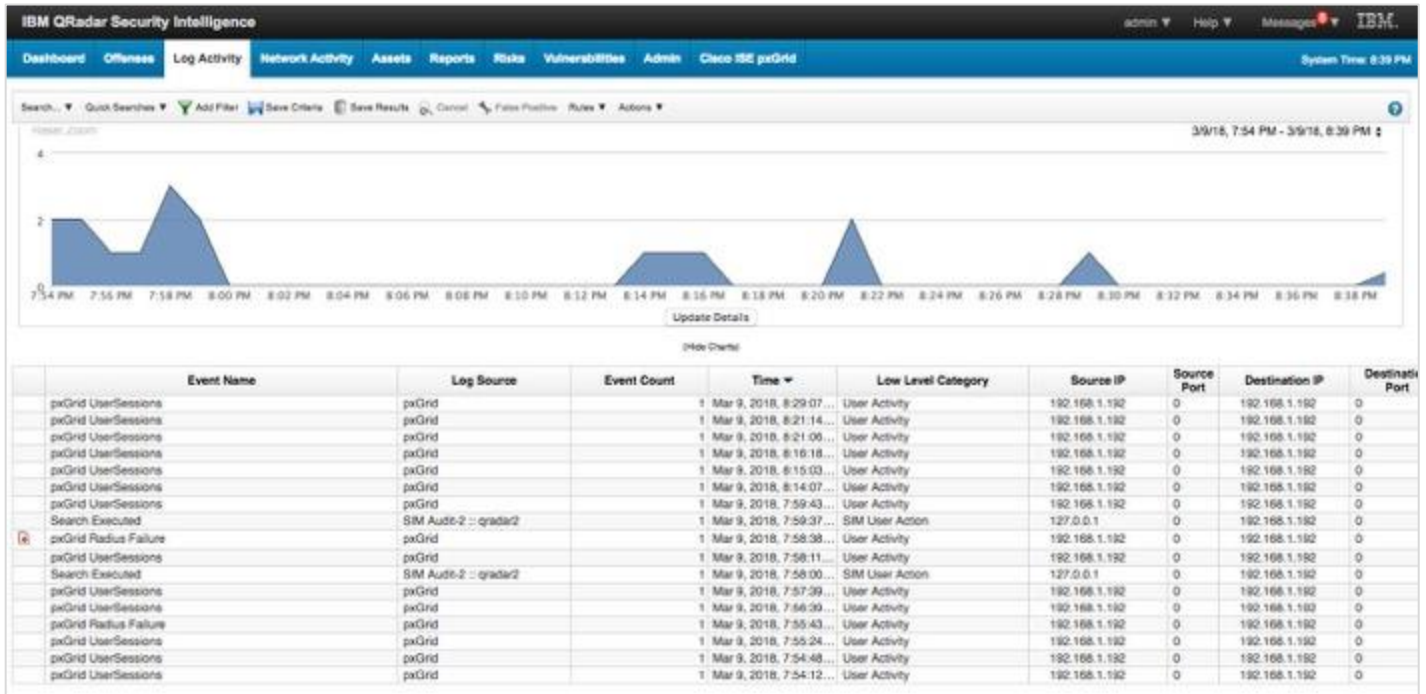
The screenshot shows the IBM QRadar Security Intelligence interface. The 'Log Activity' tab is selected. A table of log events is visible, with one event highlighted. An 'Add Filter' dialog box is open, showing the following configuration:

- Parameter: Payload Contains
- Operator: is any of
- Value: QRadarAppForPxGrid

The dialog box also includes a 'Remove Selected' button and 'Add Filter' and 'Cancel' buttons at the bottom.

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:

Offense 1 (All Categories)

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

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

Offense Source Summary

Custom property value	192.168.1.60		
Offenses	1	Events/Flows	1

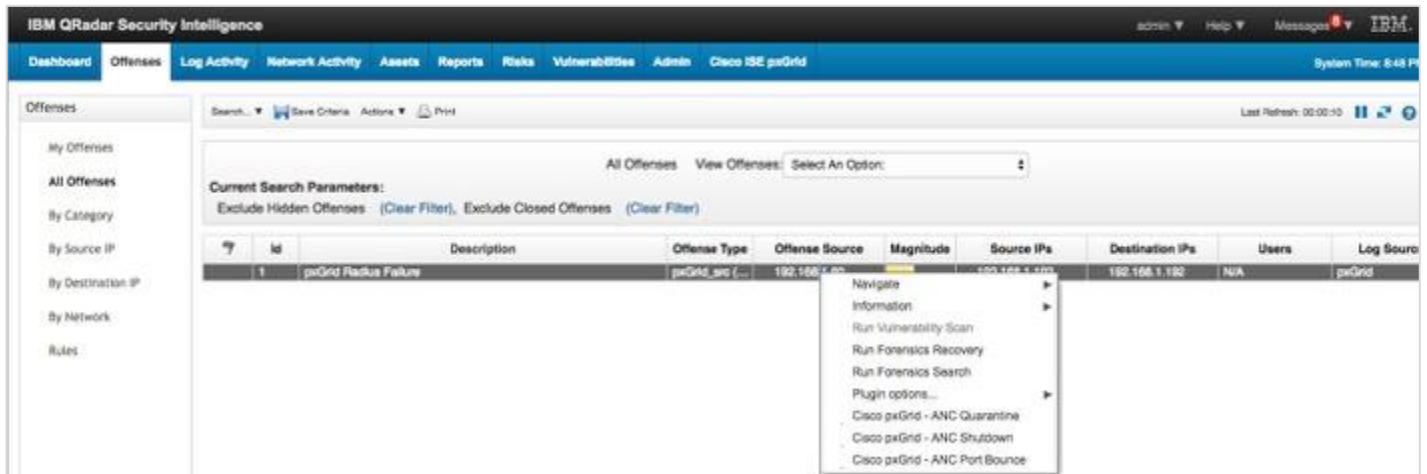
Verify pxGrid offense rule via Offenses Dashboard

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	●		0	LAB10/cpgrnd2	00:0C:29:C1:7B:2C	Windows7...	Default >> Dot1X	Default >> ANQQuarantine	Quarantined.
Mar 10, 2018 02:30:00.145 AM	●			LAB10/cpgrnd2	00:0C:29:C1:7B:2C	Windows7...	Default >> Dot1X	Default >> ANQQuarantine	Quarantined.

Step 5 To un-quarantine or clear, select **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**

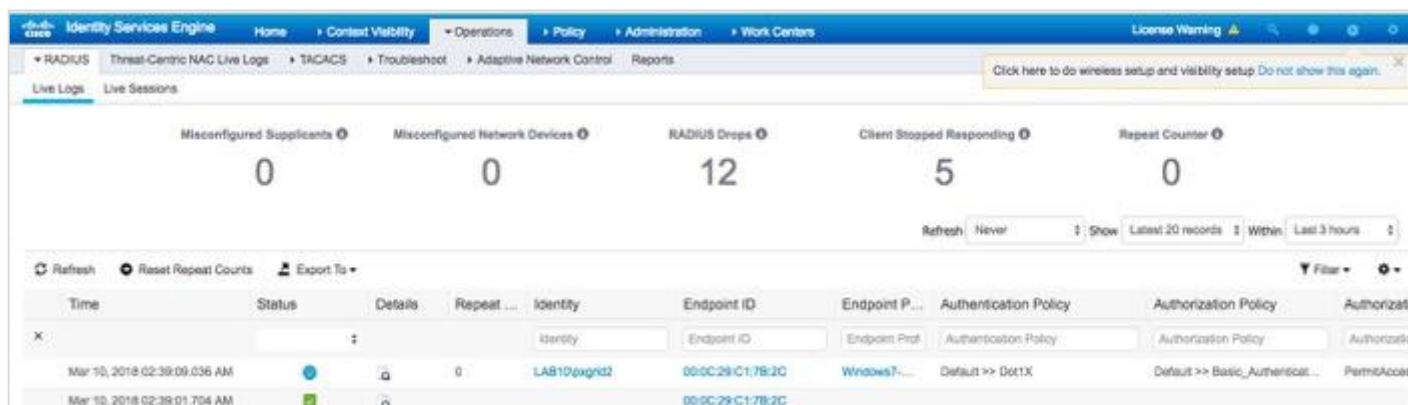
MAC Address	Policy Name	Policy Actions
<input checked="" type="checkbox"/> 00:0C:29:C1:7B:2C	pxGridQRadarQuarantine	[QUARANTINE]

Step 7 **Select > Selected**

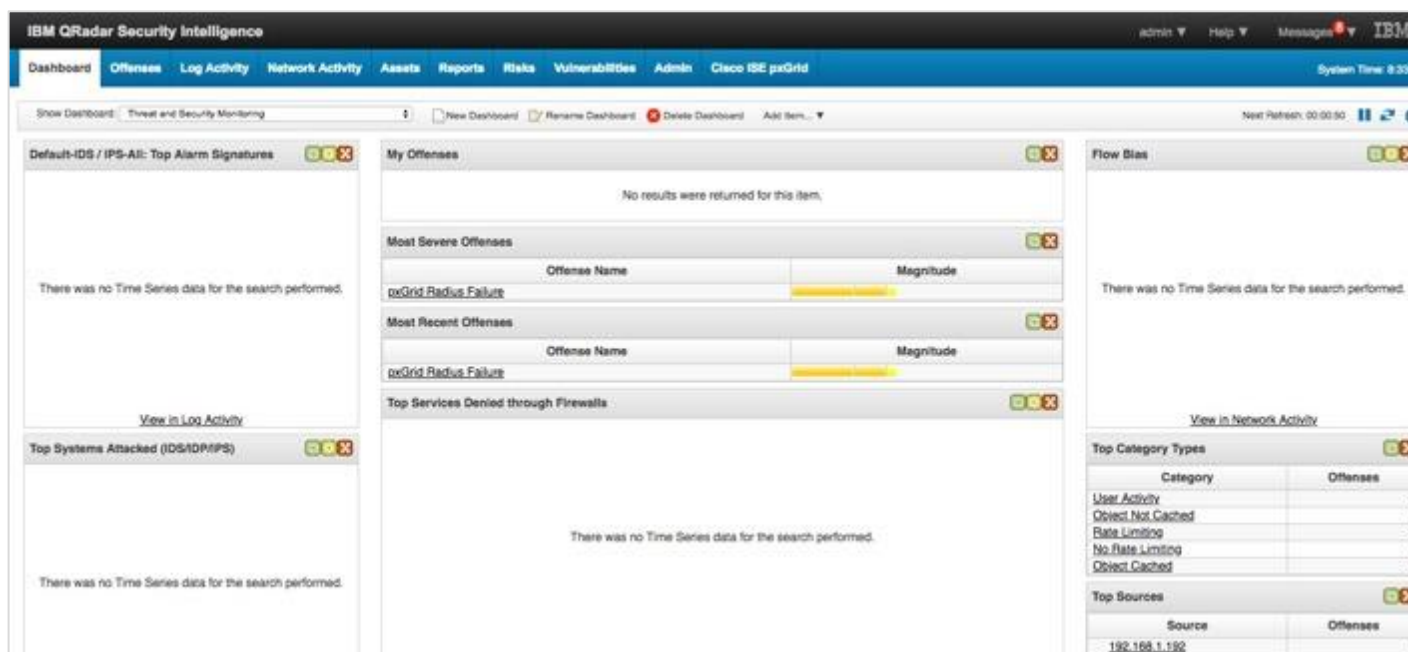


Step 8 **Select Yes**

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 top navigation bar includes 'Dashboard', 'Offenses', 'Log Activity', 'Network Activity', 'Assets', 'Reports', 'Risks', 'Vulnerabilities', 'Admin', and 'Cisco ISE pxGrid'. The 'Offenses' section 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

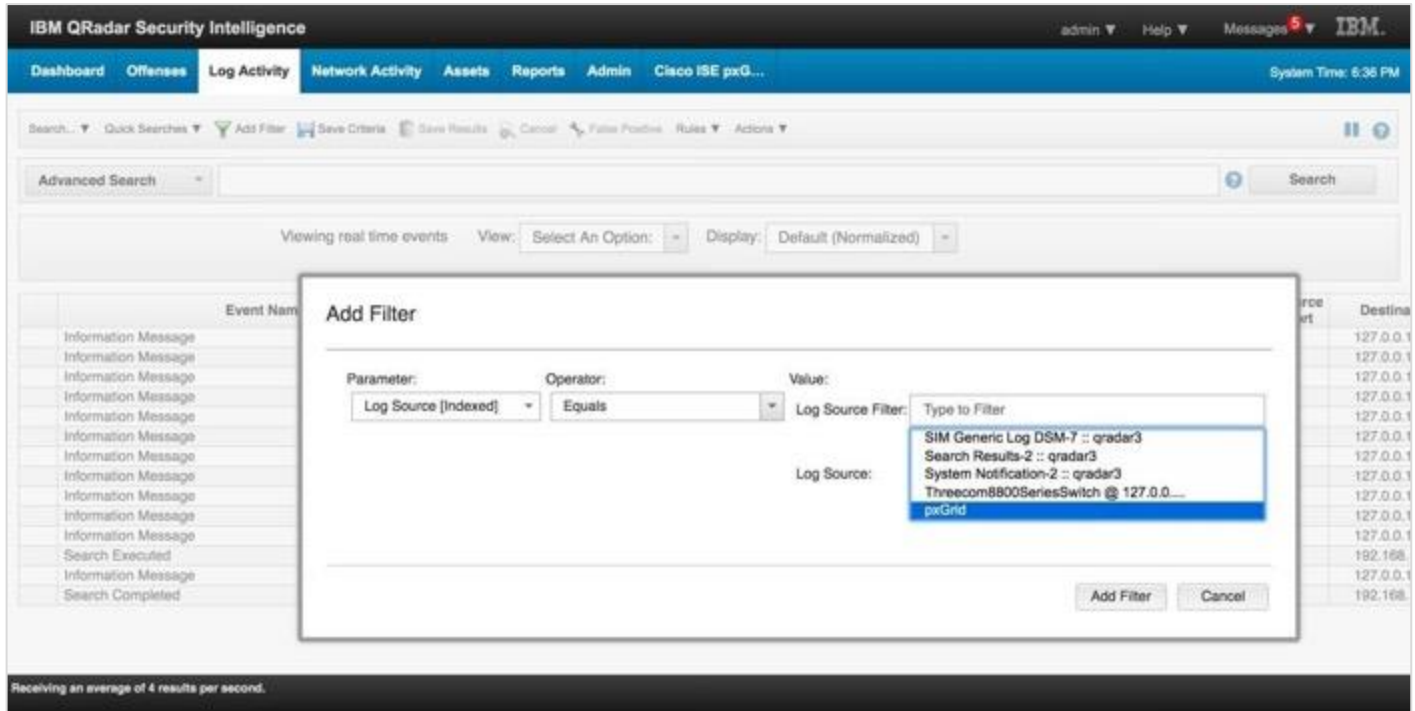
Network:
 Net: 10-172-192-Net_192_168_0_0
 User Name: LAB10\pxgrid2
pxGrid Session details: Mac Address: 00:0C:29:C1:7B:2C
 Posture Status: None
 Endpoint Profile: Windows7-Workstation
 Right click for more information on: 192.168.1.60

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

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 :: qradar3	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
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
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
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
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
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
Information Message	System Notification-2 :: qradar3	1	Apr 19, 2019, 6:14:3...	Information	192.168.1.249	0	127.0.0.1
Information Message	System Notification-2 :: qradar3	1	Apr 19, 2019, 6:14:3...	Information	192.168.1.249	0	127.0.0.1
Information Message	System Notification-2 :: qradar3	1	Apr 19, 2019, 6:14:3...	Information	192.168.1.249	0	127.0.0.1
Information Message	System Notification-2 :: qradar3	1	Apr 19, 2019, 6:14:3...	Information	192.168.1.249	0	127.0.0.1
Information Message	System Notification-2 :: qradar3	1	Apr 19, 2019, 6:14:3...	Information	192.168.1.249	0	127.0.0.1

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 node, the ISE Admin and ISE MNT nodes are signed by the external CA Server

Select **Administration > System > Certificate > System > Certificates > System Certificates**

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

System Certificates ⚠️ For disaster recovery it is recommended to export certificate and private key pairs of all 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#00002	Not in use		ise26.lab10.com	Certificate Services Endpoint Sub CA - ise26	Tue, 5 Mar 2019	Tue, 6 Mar 2029
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#00003	Admin, Portal, EAP Authentication, pxGrid, RADIUS DTLS	Default Portal Certificate Group (2)	ise26.lab10.com	lab10-WIN-N3OR1A7H9KL-CA	Sat, 23 Mar 2019	Tue, 23 Mar 2021
OU=ISE Messaging Service, CN=ise26.lab10.com#Certificate Services Endpoint Sub CA - ise26#00001	ISE Messaging Service		ise26.lab10.com	Certificate Services Endpoint Sub CA - ise26	Tue, 5 Mar 2019	Tue, 6 Mar 2029

Step 2 Verify the pxGrid certificate is signed by the external CA server and ensure that the admin certificate is signed by the external CA server as well

System Certificates ⚠️ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date
Default self-signed saml server certificate - CN=SAML_ise26ca.lab10.com	SAML		SAML_ise26ca.lab10.com	SAML_ise26ca.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-N3OR1A7H9KL-CA#00003	Admin, Portal, EAP Authentication, pxGrid, RADIUS DTLS	Default Portal Certificate Group (2)	ise26ca.lab10.com	lab10-WIN-N3OR1A7H9KL-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: Select **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
firesightsetest-fmc63.lab10.com...		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate
qradar5	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
ncadtest		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate

Connected via XMPP ise26.lab10.com (standby: ise26ca)

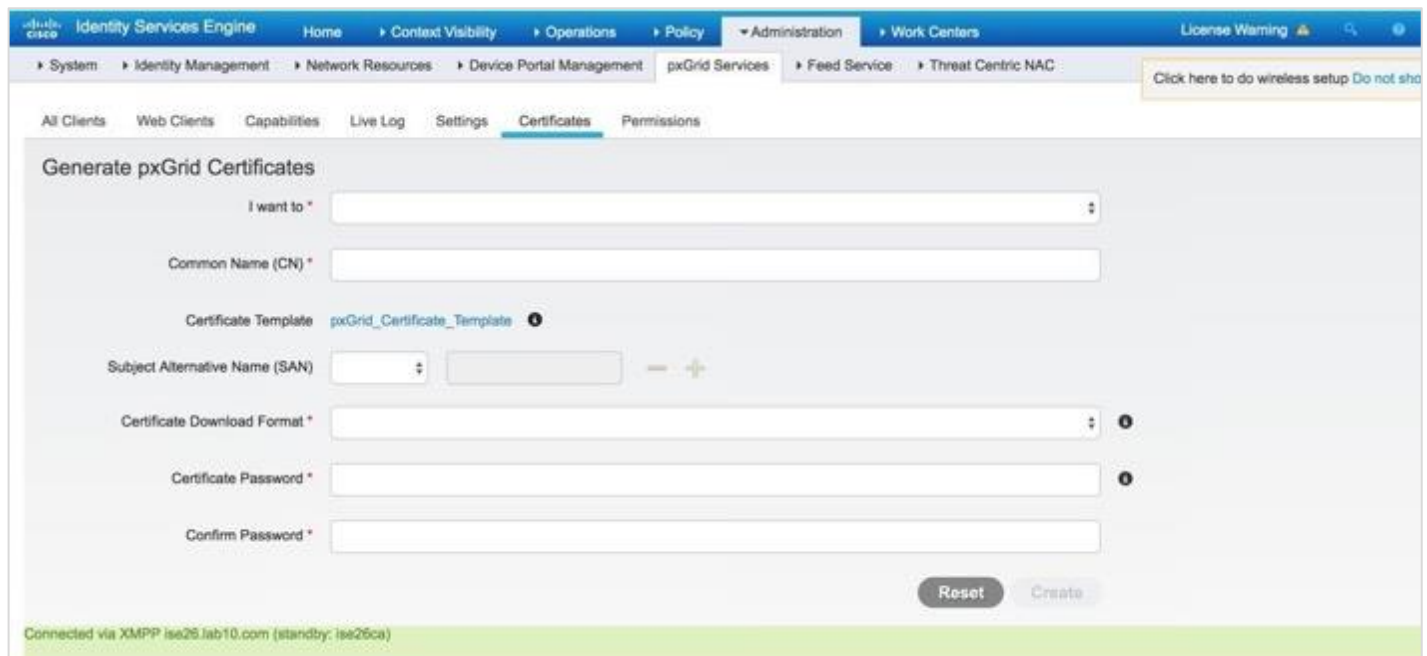
Step 4 Ensure that there is pxGrid connectivity. If in the lower-left corner you see "no connectivity", there is a certificate issue with the ISE pxGrid node, the ISE admin and MNT nodes.

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:

Select **Administration > pxGrid Services > Certificates**



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Administration > pxGrid Services > Certificates. The page title is "Generate pxGrid Certificates". The form includes the following fields and options:

- I want to ***: A dropdown menu.
- Common Name (CN) ***: A text input field.
- Certificate Template**: A dropdown menu showing "pxGrid_Certificate_Template".
- Subject Alternative Name (SAN)**: A list of options with a plus sign to add more.
- Certificate Download Format ***: A dropdown menu.
- Certificate Password ***: A text input field.
- Confirm Password ***: A text input field.

At the bottom right, there are "Reset" and "Create" buttons. A status bar at the bottom indicates "Connected via XMPP isa25.lab10.com (standby: isa26ca)".

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

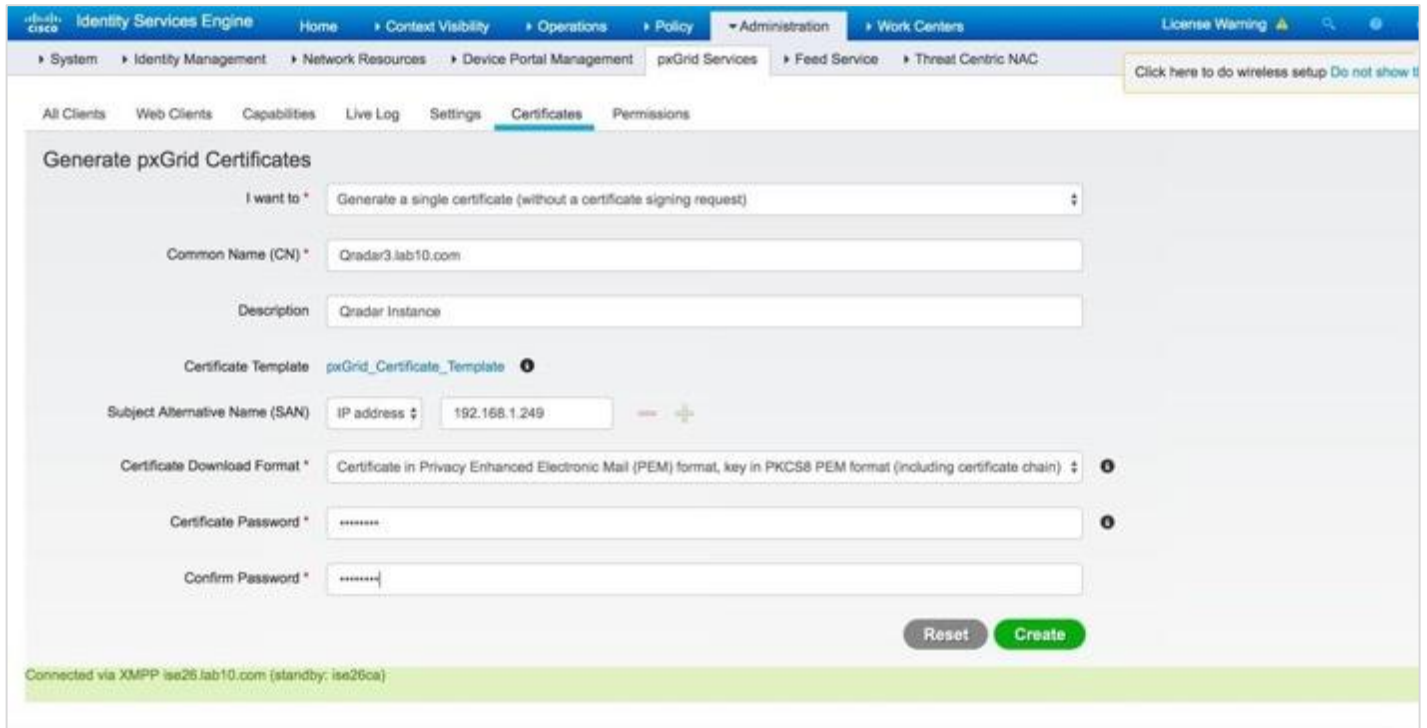
Step 4 From the **Subject Alternative Name (SAN)** list, select the **IP Address**, and then enter the IP address of the QRadar instance

Step 5 Provide a description name

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

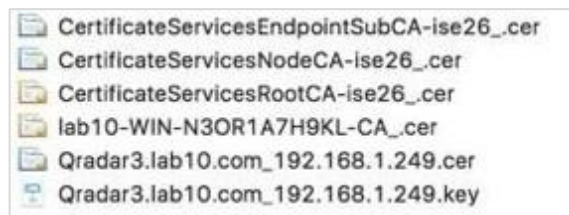
Step 7 In the **Certificate Password** box, enter the encryption password

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
```

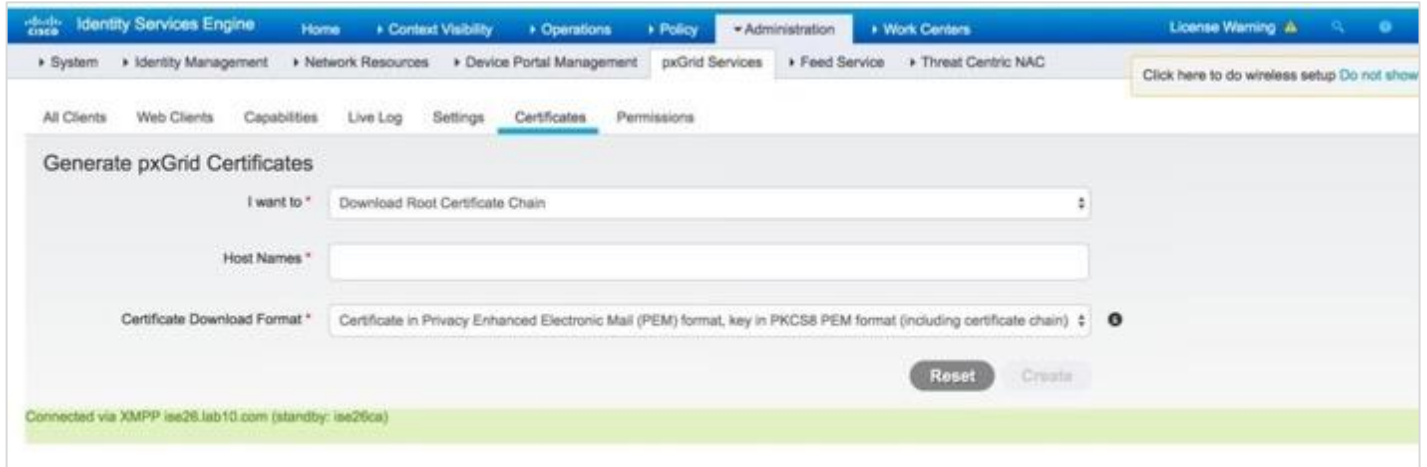
Then, run openssl to remove the encryption password from the key.org file. You will get an unencrypted file as defined by the -out parameter. The unencrypted key will be the .key file.

```
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

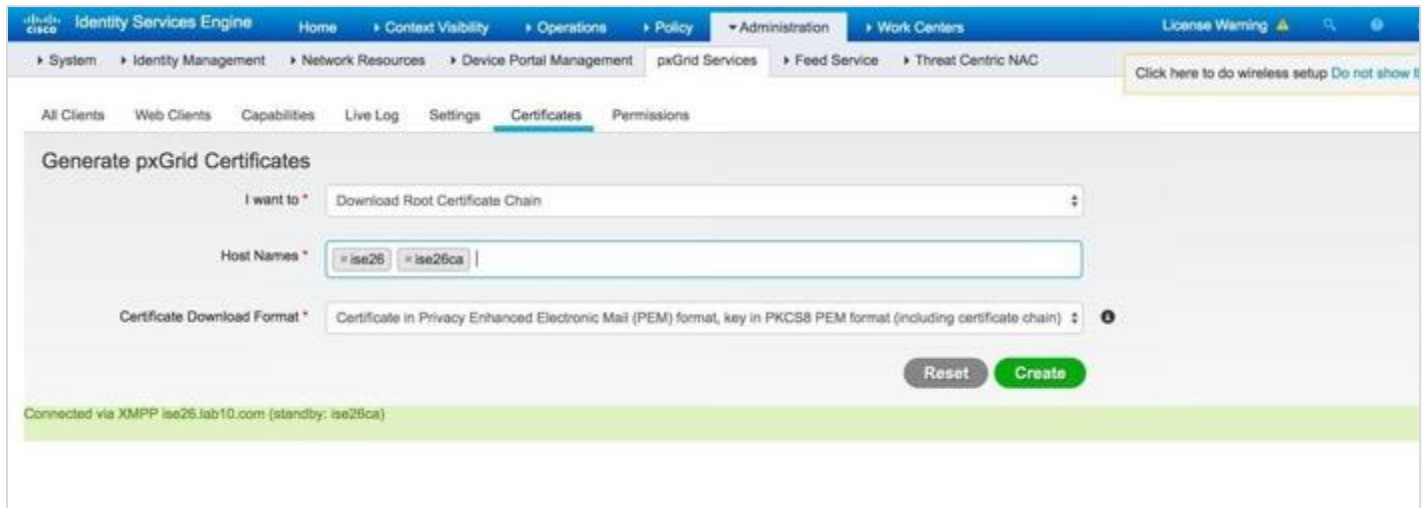
Step 12 To download the certificate root chain:

Select **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**:



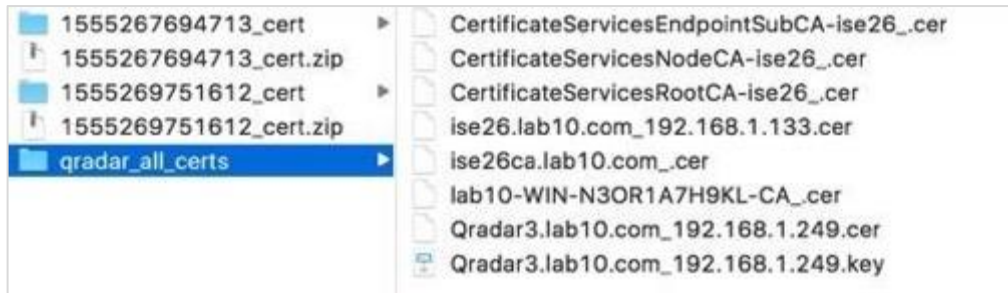
Step 15 From the **Certificate Downloaded Format** list, select **PEM** format

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.

Troubleshoot inside QRadar:

1. Take an SSH to the PxGrid Docker Container on QRadar

- In QRadar versions 7.3.2 and above run the commands:

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

- In QRadar versions 7.3.1 run the commands:

```
1> /opt/qradar/support/qapp_utils_730.py ps
2> /opt/qradar/support/qapp_utils_730.py connect <App ID>
```

2. Once you are inside the PxGrid docker container, enter the following command:

- `echo <ISE IP Address> <FQDN> >> /etc/hosts`
e.g `echo 11.0.50.90 xyc.org.uk >> /etc/hosts` (Please Verify the ISE Ip Address and FQDN on your deployment from administration>>system>>deployment>>hostname in ISE)

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.

ANC Mitigation Actions not appearing in Dashboards

Ensure the app created the following ISE policies and you have them:

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

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>

For QRadar versions 7.3.1, run the commands:

- 1> /opt/qradar/support/qapp_utils_730.py ps
- 2> /opt/qradar/support/qapp_utils_730.py 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
socker .....

```

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 happening 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
```

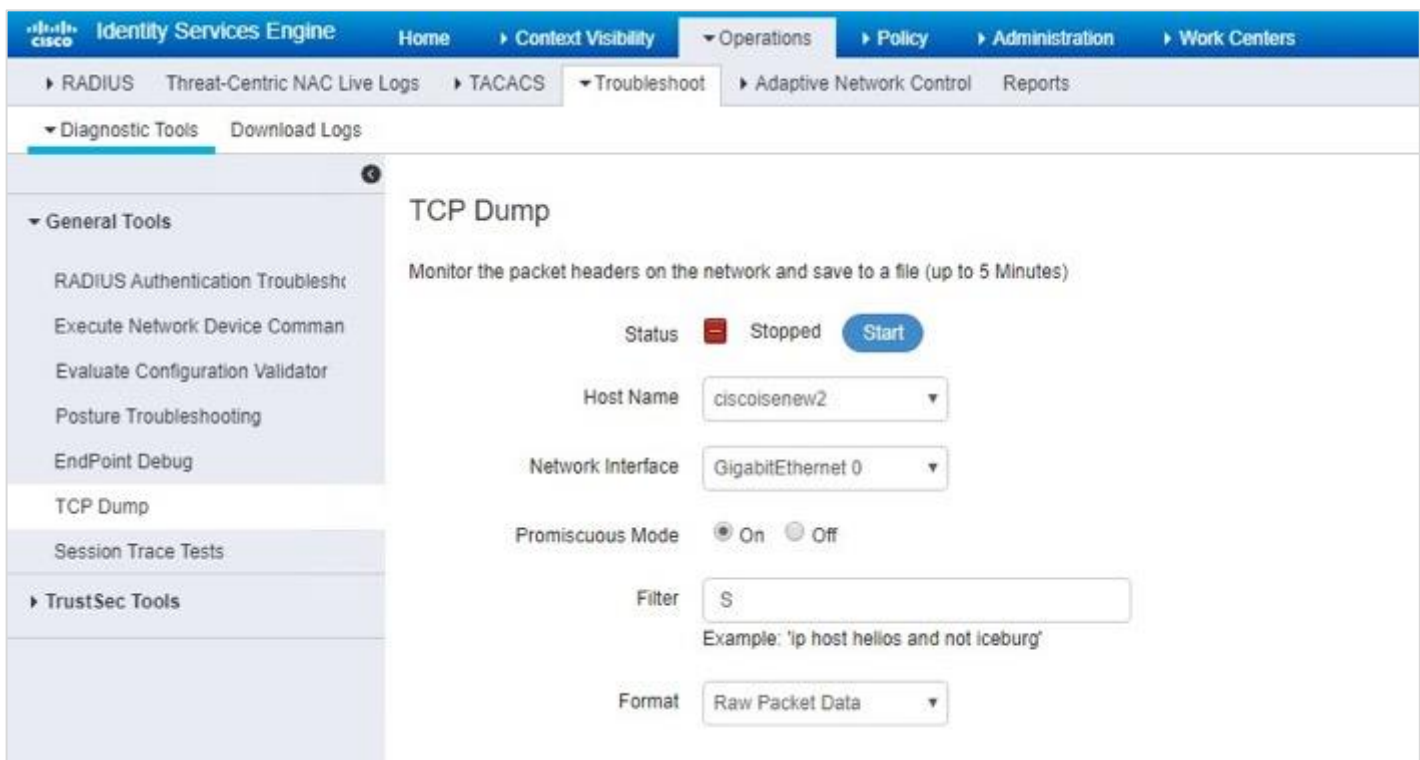
```
2021-02-02 17:25:00,036 [abstract_qpylib.log] [Thread-718] [INFO]
- 127.0.0.1[APP_ID/1102][NOT:0000006000] Checking connection with primary server using PROTOCOL_SSLv23
```

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:

Step 1 Login to QRadar console (putty/terminal)

Step 2 Get the pxGrid APP ID execute this command: `/opt/qradar/support/recon ps`

Step 3 The startup.log and app.log are available in this location: **/store/docker/volumes/qapp-<<App ID>>/log**

Step 4 Replace App ID with pxGrid App ID from Step 2

For example: `/store/docker/volumes/qapp-110`