

Cisco ISE pxGrid App 1.0 for IBM QRadar SIEM

Author: John Eppich

Table of Contents

| | |
|---|----|
| About This Document..... | 4 |
| Solution Overview..... | 5 |
| Technical Details..... | 6 |
| Cisco ISE pxGrid Installation..... | 7 |
| Generating the Cisco ISE pxGrid App Certificate..... | 9 |
| Installing Cisco ISE pxGrid App..... | 11 |
| Configuring pxGrid Integration..... | 13 |
| Cisco ISE pxGrid App Dashboard Panels..... | 16 |
| Passed Authentications..... | 16 |
| Failed Authentications..... | 19 |
| User Panel..... | 20 |
| Failure Reason Panel..... | 22 |
| Device Type Panel..... | 24 |
| Locations Panel..... | 26 |
| Devices..... | 28 |
| Compliance..... | 31 |
| TrustSec..... | 33 |
| Mobile Device Management (MDM)..... | 35 |
| ANC Details..... | 36 |
| Configuring Cisco ISE Adaptive Network Control Policies..... | 37 |
| Configuring Default ANC policies for Cisco ISE pxGrid App..... | 37 |
| Adding ANC Policies to ISE Policy Sets..... | 38 |
| Performing Cisco ISE ANC Mitigation Actions Through Cisco ISE pxGrid App Dashboard Panel..... | 40 |
| Configuring IBM QRadar for Cisco ISE Syslog Events..... | 46 |
| Configuring Cisco ISE Syslog Events..... | 47 |
| Performing ISE ANC Mitigation Actions Through IBM QRadar Syslog Events..... | 49 |
| Creating Custom Field for Framed IP Address ISE Syslog Event..... | 49 |
| ANC Mitigation Syslog Event Example..... | 54 |
| Hovering Over IBM QRadar Syslog IP Address for ISE Contextual Information..... | 58 |
| IBM QRadar Cisco ISE pxGrid Offense Rule..... | 59 |
| Verify pxGrid offense rule via Log Activity..... | 60 |
| Verify pxGrid offense rule via Offenses Dashboard..... | 62 |
| Taking ISE ANC mitigations from Offenses Dashboard..... | 62 |

Appendices 66

| | |
|---|----|
| Cisco ISE pxGrid App pxGrid client not showing under ISE pxGrid Client View | 66 |
| Cisco ISE pxGrid App pxGrid client not showing under ISE pxGrid Web Client View | 66 |
| Cisco ISE pxGrid Dashboards not populating with ISE Contextual Information | 66 |
| ANC Mitigation Actions not appearing in Dashboards | 66 |

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 v1.0 for IBM the QRadar SIEM. The supported platforms are: IBM QRadar SIEM 7.2.8 patch 9 and greater versions, Cisco ISE 2.4 and greater versions as well.

In this document, the Cisco ISE pxGrid app was installed on IBM QRadar SIEM 7.2.8 Patch 9 along with Cisco ISE 2.4. Cisco ISE 2.4 was installed in a Stand-Alone deployment, and the ISE internal CA was used for generating the pxGrid certificates for the Cisco ISE pxGrid App.

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 mitigation 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 ISE.

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 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 use 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 register 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.

| 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 |

Subscribed Topics 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 Cisco ISE pxGrid app pxGrid client subscribes to the Session Directory, RADIUS failure, MDM endpoint, 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. In the initial Cisco ISE 2.4 release, only the compliance and registration status attributes are available. In later releases of Cisco ISE after 2.4, the MDM attributes: Manufacturer, UDID, Serial Number, Encryption Status, Jail Broken Status, Pin Lock Status will be available.

The RADIUS failure topic includes failure reason attributes such as “invalid password” and drill downs based on location and wired and 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 WebSockets, REST API and STOMP messaging protocol for pxGrid operation and thus supported in Cisco ISE 2.4 or greater.

Cisco ISE pxGrid Installation

This assumes that Cisco Identity Services (ISE) 2.4 or greater has been installed and is in a stand-alone deployment. If this is a productional ISE deployment, ensure the Cisco ISE pxGrid node is on a dedicated node, please see: How to Configure pxGrid in ISE Production Environments: <https://communities.cisco.com/docs/DOC-68284>

Step 1 Select Administration->System Deployment->edit the ISE node->Enable pxGrid

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

Role **STANDALONE** Make Primary

Administration

Monitoring
 Role PRIMARY
 Other Monitoring Node [REDACTED]

Policy Service
 Enable Session Services *i*
 Include Node in Node Group None *i*

Enable Profiling Service *i*

Enable Threat Centric NAC Service *i*

Enable SXP Service *i*

Enable Device Admin Service *i*

Enable Passive Identity Service *i*

pxGrid *i*

Step 2 Select Save You should see:

| Hostname | Personas | Role(s) | Services | Node Status |
|----------|--|------------|------------------|-------------------------------------|
| ise24k | Administration, Monitoring, Policy Service, pxGrid | STANDALONE | SESSION,PROFILER | <input checked="" type="checkbox"/> |

Step 3 Select **Administration->pxGrid Services**
Verify the published nodes appear

Identity Services Engine Administration > pxGrid Services

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

| Client Name | Client Description | Capabilities | Status | Client Group(s) | Auth Method | Log |
|-------------------|--------------------|----------------------------|---------------|-----------------|-------------|----------------------|
| ise-fanout-ise24k | | Capabilities(0 Pub, 0 Sub) | Online (XMPP) | Internal | Certificate | View |
| ise-bridge-ise24k | | Capabilities(0 Pub, 4 Sub) | Online (XMPP) | Internal | Certificate | View |
| ise-mnt-ise24k | | Capabilities(2 Pub, 1 Sub) | Online (XMPP) | Internal | Certificate | View |
| ise-admin-ise24k | | Capabilities(6 Pub, 2 Sub) | Online (XMPP) | Internal | Certificate | View |
| ise-pubsub-ise24k | | Capabilities(0 Pub, 0 Sub) | Online (XMPP) | Internal | Certificate | View |

and you have connectivity

Connected to pxGrid ise24k.lab10.com

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

Identity Services Engine Administration > pxGrid Services > Web Clients

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

Rows/Page: 6 / 1 / 1 Go 6 Total Rows

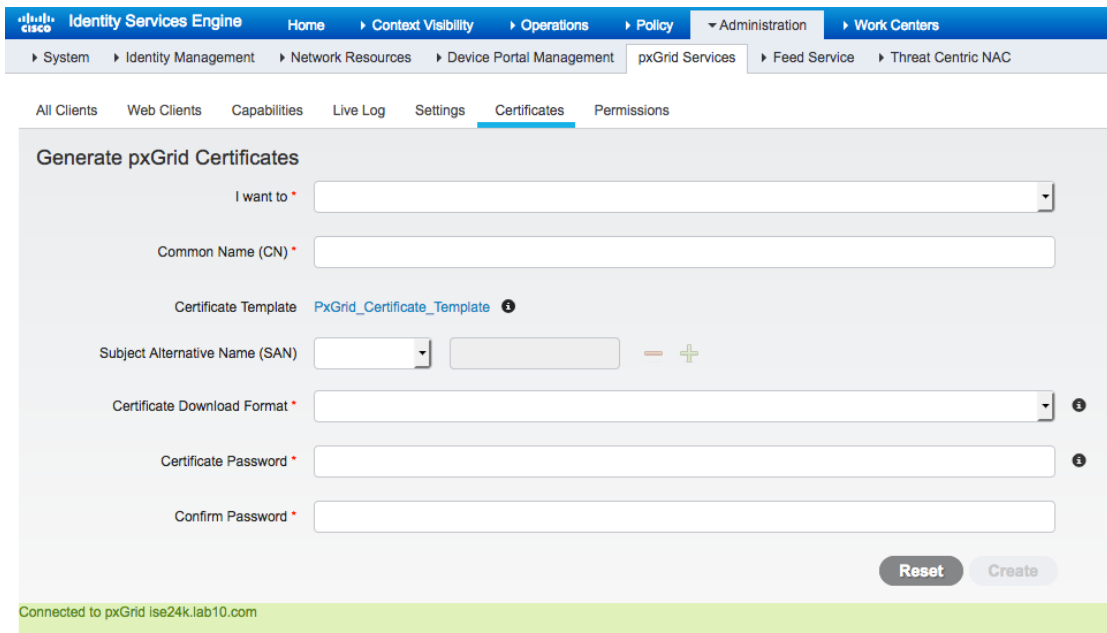
| Client Name | Connect To | Session Id | Certificate | Subscriptions | Publications | IP Address | Status | Start time | Duratio... |
|-------------------|------------|------------|-------------|--------------------------|--------------------------|------------|--------|-------------------------|-------------|
| ise-fanout-ise24k | ise24k | ise24k:0 | CN=... | /api/wildcard | | 127.0.0.1 | ON | 2018-03-08 14:31:45 UTC | 01:13:12:08 |
| ise-mnt-ise24k | ise24k | ise24k:4 | CN=... | /api/com.cisco.ise.se... | /api/com.cisco.ise.se... | | ON | 2018-03-08 14:32:55 UTC | 01:13:10:58 |
| ise-fanout-ise24k | ise24k | ise24k:7 | CN=... | /api/distributed | /api/distributed | | ON | 2018-03-08 16:25:46 UTC | 01:11:18:05 |
| ise-bridge-ise24k | ise24k | ise24k:9 | CN=... | | /api/com.cisco.ise.se... | | ON | 2018-03-08 19:37:22 UTC | 01:08:06:29 |
| ise-admin-ise24k | ise24k | ise24k:12 | CN=... | | /api/com.cisco.ise.co... | | ON | 2018-03-09 07:52:34 UTC | 00:19:51:17 |

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: https://communities.cisco.com/docs/DOC-68284](https://communities.cisco.com/docs/DOC-68284)

Please note that 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 ISE Administration console interface. The breadcrumb navigation is: Administration > pxGrid Services > Certificates. The main content area is titled 'Generate pxGrid Certificates' and contains the following fields and controls:

- 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 green status bar at the bottom indicates 'Connected to pxGrid ise24k.lab10.com'.

Step 2 Type the following:
I want to: Generate a single certificate (without a certificate signing request)
Common Name (FQDN): qradar. [REDACTED]
Description: QRadar
Certificate Template: Pxgrid_Certificate_Template
Subject Alternative Name (FQDN): qradar [REDACTED]
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: Please make sure your browser Pop-Up blocker is disabled, when generating certificates

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

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

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

qradar.████████_qradar.████████.cer and qradar.████████_qradar.████████.key

The CertificateServicesRootCA-ise24k_.cer is the ISE internal Root CA certificate

Step 5 Run the following to remove the encryption password when importing into the Cisco ISE pxGrid App

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

```
cp qradar.████████_qradar.████████.key qradar.lab10.com_qradar.████████.key.org  
openssl rsa -in qradar.████████.com.key.org cp -out qradar.████████.com.key  
(you will be prompted to enter the encryption password when generating the certificate in ISE)
```

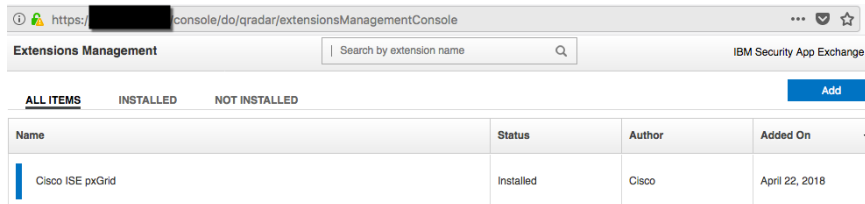
Step 6 You will need to upload these 6 certificates when configuring the Cisco ISE pxGrid App for pxGrid integration.

Installing Cisco ISE pxGrid App

This section steps the reader through the Cisco ISE pxGrid App Installation.

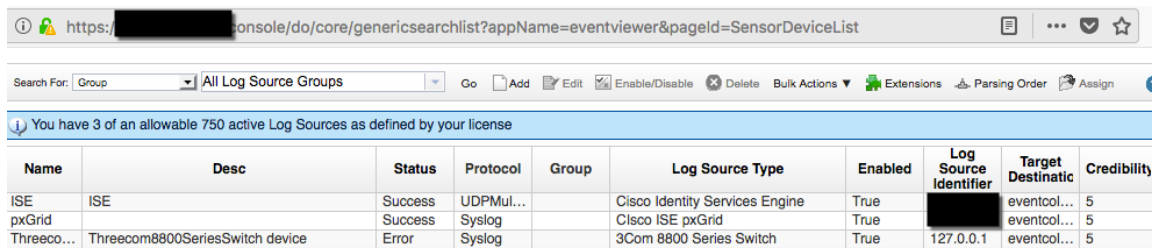
Note: It is assumed that QRadar ver 7.28 has been installed along with Patch 9 (<http://www-01.ibm.com/support/docview.wss?uid=swg27050133>)

- Step 1** From IBM QRadar, select **Admin->Extensions Management->Add->**upload the signed **Cisco ISE pxGrid App** and select **Install Immediately**
After the install, you should see:



| Name | Status | Author | Added On |
|------------------|-----------|--------|----------------|
| Cisco ISE pxGrid | Installed | Cisco | April 22, 2018 |

- Step 2** Refresh the browser
Step 3 **Double-Click Admin->Log Sources->Name->pxGrid**



| Name | Desc | Status | Protocol | Group | Log Source Type | Enabled | Log Source Identifier | Target Destination | Credibility |
|------------|---------------------------------|---------|-----------|-------|--------------------------------|---------|-----------------------|--------------------|-------------|
| ISE | ISE | Success | UDPMul... | | Cisco Identity Services Engine | True | | eventcol... | 5 |
| pxGrid | | Success | Syslog | | Cisco ISE pxGrid | True | | eventcol... | 5 |
| Threeco... | Threecom8800SeriesSwitch device | Error | Syslog | | 3Com 8800 Series Switch | True | 127.0.0.1 | eventcol... | 5 |

- Step 4** Edit the **Log Source Identifier** and type in the **IP Address** of the IBM QRadar instance.

https://[redacted]console/do/sem/maintainSensorDevice?dispatch=ec

Edit a log source

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

Log Source Name: pxGrid

Log Source Description: [empty]

Log Source Type: Cisco ISE pxGrid

Protocol Configuration: Syslog

Log Source Identifier: [redacted]

Enabled:

Credibility: 5

Target Event Collector: eventcollector0 :: qradar3

Coalescing Events:

Incoming Payload Encoding: UTF-8

Store Event Payload:

Log Source Language: [empty]

Log Source Extension: CiscosepGridCustom_ext

Extension Use Condition: Parsing Override

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

- Step 5** Select **Save**
- Step 6** Select **Admin->Authorized Services->Add Authorized Service->**type: **pxGridService** for the **Service name:**
- Step 7** Select **Admin** for both the **User Role** and **Security Profile** drop-downs
- Step 8** Enable **No** for Expiry

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

- Step 9** Select **Create Service**
- Step 10** Note the authentication token, you will need to paste this into the token installation window when configuring the Cisco ISE pxGrid App for pxGrid integration.

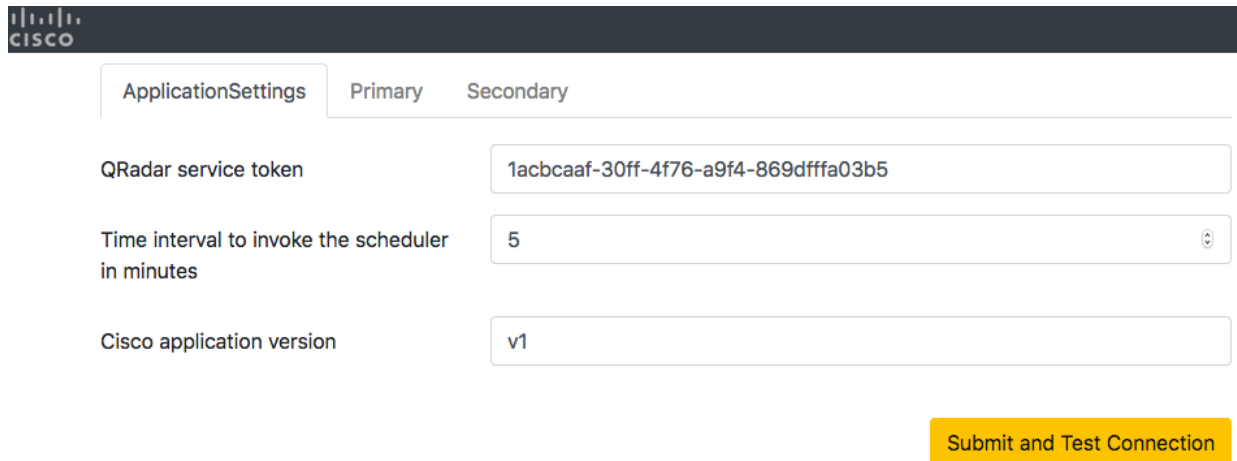
https://[redacted]console/do/qradar/authorizedService?dispatch=authorizedServiceList

Add Authorized Service Delete Authorized Service Edit Authorized Service Name Selected Token:None

| Service Name | Authorized By | Authentication Token | User Role | Security Profile | Created | Exp |
|----------------------|----------------|----------------------|-----------|------------------|-------------------------|-----------|
| Local Health Console | configservices | [redacted] | Admin | Admin | Apr 5, 2018, 4:35:17 PM | Permanent |
| pxGridService | admin | [redacted] | Admin | Admin | Apr 5, 2018, 9:14:09 PM | Permanent |

Configuring pxGrid Integration

- Step 1** Select **Admin->Plug-Ins->Cisco pxGrid->pxGrid Settings**, and copy/paste the authentication token from step 11 into the **QRadar Service Token Window**



- Step 2** Select **Submit and Test Connection**, you should see a successful connection.
Step 3 Select **Primary**, and type the **IP address** of the ISE pxGrid node
Step 4 Leave **8910**, as the port default
Step 5 Enter the **Client user name (i.e. Augas0221)**

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

- Step 6** Upload the Cisco ISE pxGrid App certificates in PEM format under **Select and Upload Certificates (only PEM is supported)**

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

- Step 7** Type in the Cisco ISE pxGrid App Certificate file name: **qradar.██████████_qradar.██████████.cer**
Step 8 Type in the Cisco ISE pxGrid App Certificate key file name: **qradar.██████████.key**
Step 9 Type in the Cisco ISE Internal Root Certificate Root CA certificate file name:
CertificateServicesRootCA-ise24k_.cer
Step 10 You should see the following:

CISCO

ApplicationSettings

Primary

Secondary

Primary pxGrid Server IP Address *

port *

8910

Client user name *

CiscoISEpxGridAppFCLab

Select & Upload certificates(only PEM is supported) *

Certificate file name *

qradar3. .cer

Certificate key file name *

qradar3. .key

Root CA certificate file name *

CertificateServicesRootCA .cer

Step 11 Select **Submit and Test Connection**, you should see a successful connection message.

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

Step 12 On ISE, select **Administration->pxGrid Services**, you should see the registered Cisco ISE pxGrid App client **Aujas0221** as the client.

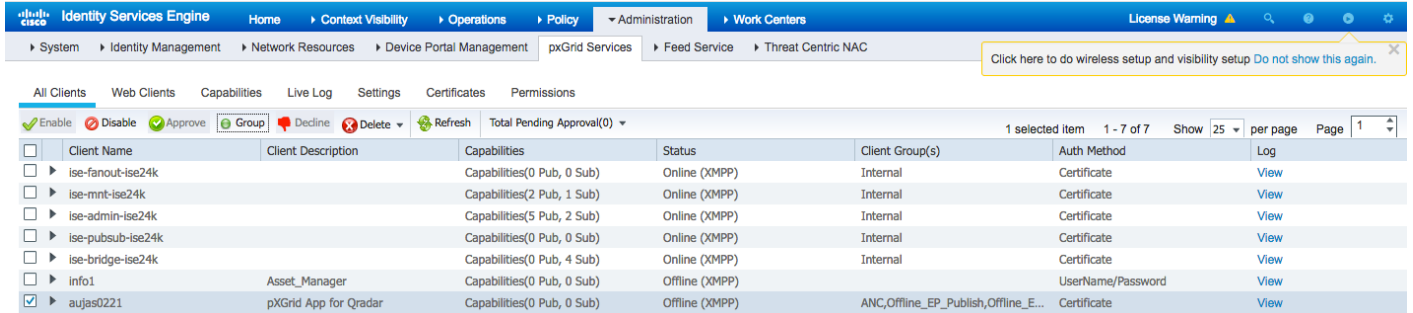
| Client Name | Client Description | Capabilities | Status |
|-------------------|-----------------------|----------------------------|----------------|
| ise-fanout-ise24k | | Capabilities(0 Pub, 0 Sub) | Online (XMPP) |
| ise-mnt-ise24k | | Capabilities(2 Pub, 1 Sub) | Online (XMPP) |
| ise-admin-ise24k | | Capabilities(5 Pub, 2 Sub) | Online (XMPP) |
| ise-pubsub-ise24k | | Capabilities(0 Pub, 0 Sub) | Online (XMPP) |
| ise-bridge-ise24k | | Capabilities(0 Pub, 4 Sub) | Online (XMPP) |
| info1 | Asset_Manager | Capabilities(0 Pub, 0 Sub) | Offline (XMPP) |
| aujas0221 | pXGrid App for Qradar | Capabilities(0 Pub, 0 Sub) | Offline (XMPP) |

Step 13 Select **Web Clients**, you will see registered Cisco ISE pxGrid QRadar app client Aujas 0221

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

Step 14 Select **All Clients->Aujas0221->Group->Add->ANC->Offline_EP_Publish->Offline_EP_Subscribe->Offline_EP_Subscribe->Offline_EP_Action->Save**

Step 15 You should see the pxGrid client Groups assigned to the Cisco ISE pxGrid client



The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is: System > Identity Management > Network Resources > Device Portal Management > pxGrid Services. The 'pxGrid Services' page displays a table of client groups. The 'Group' button is highlighted in the top toolbar. The table below shows the details for the selected client group 'aujas0221'.

| Client Name | Client Description | Capabilities | Status | Client Group(s) | Auth Method | Log |
|-------------------|------------------------------|-----------------------------------|-----------------------|--|--------------------|-----------------------------|
| ise-fanout-ise24k | | Capabilities(0 Pub, 0 Sub) | Online (XMPP) | Internal | Certificate | View |
| ise-mnt-ise24k | | Capabilities(2 Pub, 1 Sub) | Online (XMPP) | Internal | Certificate | View |
| ise-admin-ise24k | | Capabilities(5 Pub, 2 Sub) | Online (XMPP) | Internal | Certificate | View |
| ise-pubsub-ise24k | | Capabilities(0 Pub, 0 Sub) | Online (XMPP) | Internal | Certificate | View |
| ise-bridge-ise24k | | Capabilities(0 Pub, 4 Sub) | Online (XMPP) | Internal | Certificate | View |
| info1 | Asset_Manager | Capabilities(0 Pub, 0 Sub) | Offline (XMPP) | | UserName/Password | View |
| aujas0221 | pxGrid App for Qradar | Capabilities(0 Pub, 0 Sub) | Offline (XMPP) | ANC,Offline_EP_Publish,Offline_E... | Certificate | View |

Cisco ISE pxGrid App Dashboard Panels

The Dashboards and Panels are populated with contextual information from ISE via pxGrid. This contextual information provides the security or network admin visibility into who is connecting to the network and how they are connecting. What type of devices are connecting to the network and how they are connecting, also who is the owner of these devices. Are users in the organization compliant or non-compliant with the organization’s security policy. Does the organization incorporate Bring Your Own Device (BYOD) security policies and do 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 Dashboards, with the exception of TrustSec and Currently Assigned ANC Dashboards.

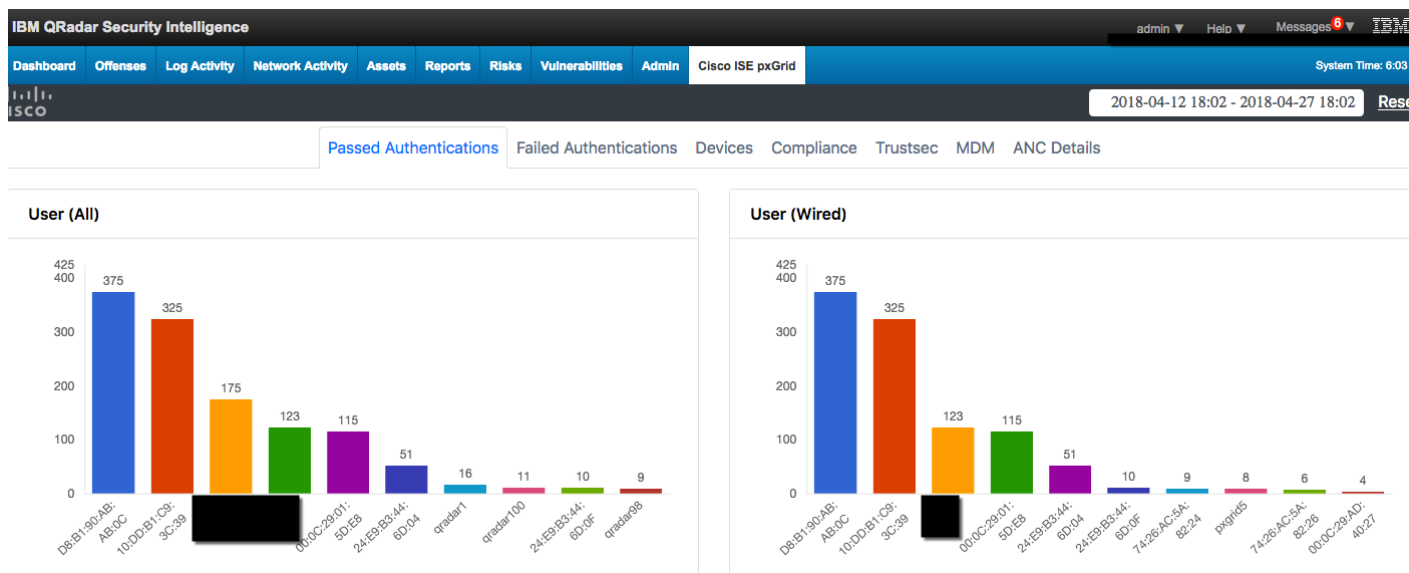
Passed Authentications

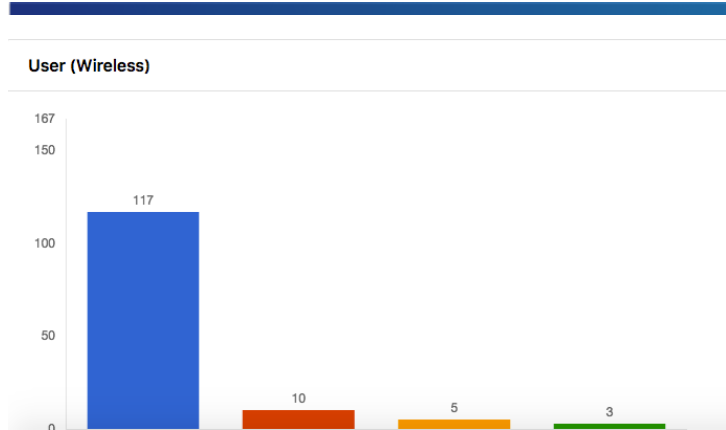
The Passed Authentications Dashboard View provides visibility into successful machine and user authentications across an organization and by wired and wireless connection type. This provides the admin with a view of how employees are connecting to the network, are they connecting over a wired or wireless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

admin Help Messages

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

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 08:11:14.539 EDT | 192.168.1.136 | STARTED | 10-DD:B1:C9:3C:39 | [Redacted] | 10-DD:B1:C9:3C:39 | 50:3D:E5:C4:05:8C | [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:C4:05:8C | [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:C4:05:8C | [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:C4:05:8C | [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:C4:05:8C | [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:C4:05:8C | [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 6 System Time: 8:02

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

| NAS Port Type | NAS Identifier | Posture Status | Endpoint Profile | Endpoint Operating System | Group ID | AD Normalized I |
|---------------|----------------|----------------|------------------|---|----------|-----------------|
| 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** provides the consistent identities of the end-user.

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

System Time: 8:02

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 Identi |
|---------------------|----------------------|-----------------------------|----------------------|---------------------|-----------------------|-------------------------|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

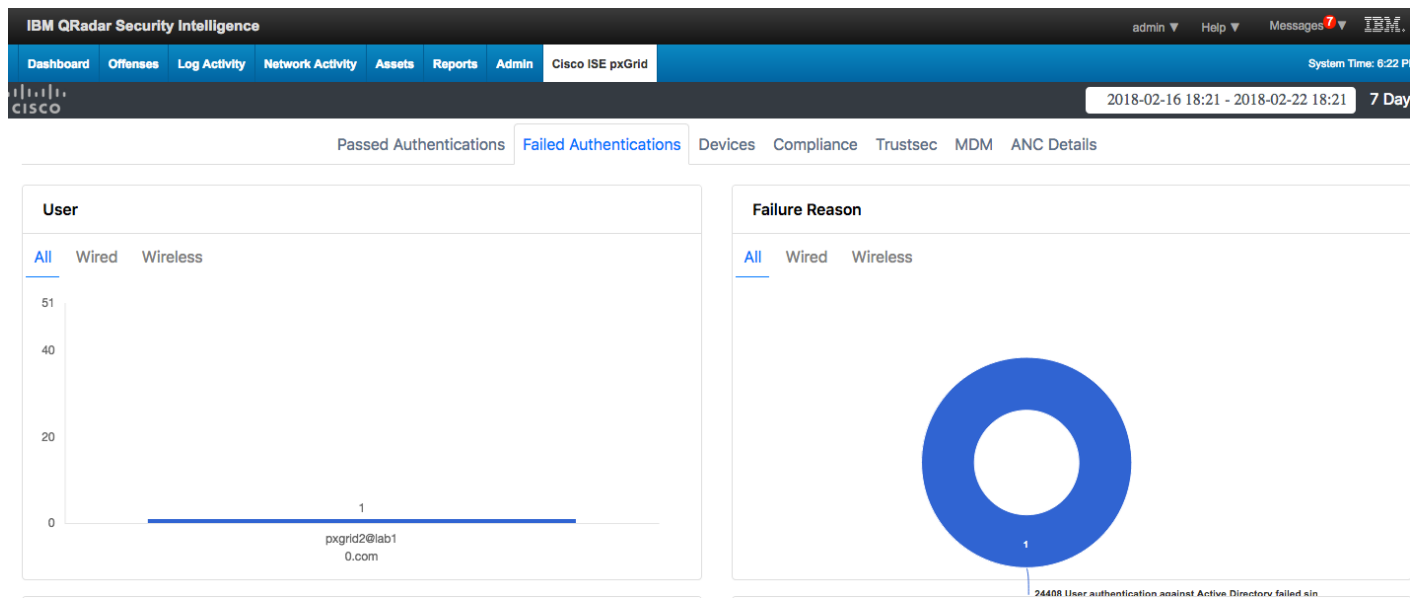
The **Is Machine Authentication** attribute determines if this machine authentication or user authentication. If this attribute is set to “true”, then this is machine authentication, if this is set to “false”, then this is user authentication.

The AD resolvable user and host identities provide a consistent name format when different EAP methods are used, i.e. 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 IBM

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

System Time: 6:41 PM

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

Data For : pxgrid2@lab10.com

Show 10 entries EXPORT

| Message Code | User Type | Access Service | Identity Store | Authentication Method | Service Type | Credential Check | AD Normalized User | AD Host Domain Name |
|--------------|-----------|------------------------|----------------|-----------------------|--------------|------------------|--------------------|---------------------|
| 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** attributes in the following screenshots provide additional context around the host and user identities.

IBM QRadar Security Intelligence

admin Help Messages IBM

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

System Time: 6:48 PM

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

Data For : pxgrid2@lab10.com

Show 10 entries EXPORT

| 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

admin Help Messages 7 System Time: 6:49

ISE pxGrid System Time: 6:49

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

EXPORT

| 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**

IBM QRadar Security Intelligence admin Help Messages 7 System Time: 6:22 P

Dashboard Offenses Log Activity Network Activity Assets Reports Admin Cisco ISE pxGrid System Time: 6:22 P

2018-02-16 18:21 - 2018-02-22 18:21 7 Day

Passed Authentications **Failed Authentications** Devices Compliance Trustsec MDM ANC Details

User

All Wired Wireless

| User | Count |
|-------------------|-------|
| pxgrid2@lab10.com | 1 |

Failure Reason

All Wired Wireless

| Failure Reason | Count |
|---|-------|
| 24408 User authentication against Active Directory failed since user has entered the wrong password | 1 |

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 Admin Cisco ISE pxGrid

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@lab10.com |

Showing 1 to 1 of 1 entries

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

Security Intelligence

Offenses Log Activity Network Activity Assets Reports Admin Cisco ISE pxGrid

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

EXPORT

| 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

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

Security Intelligence

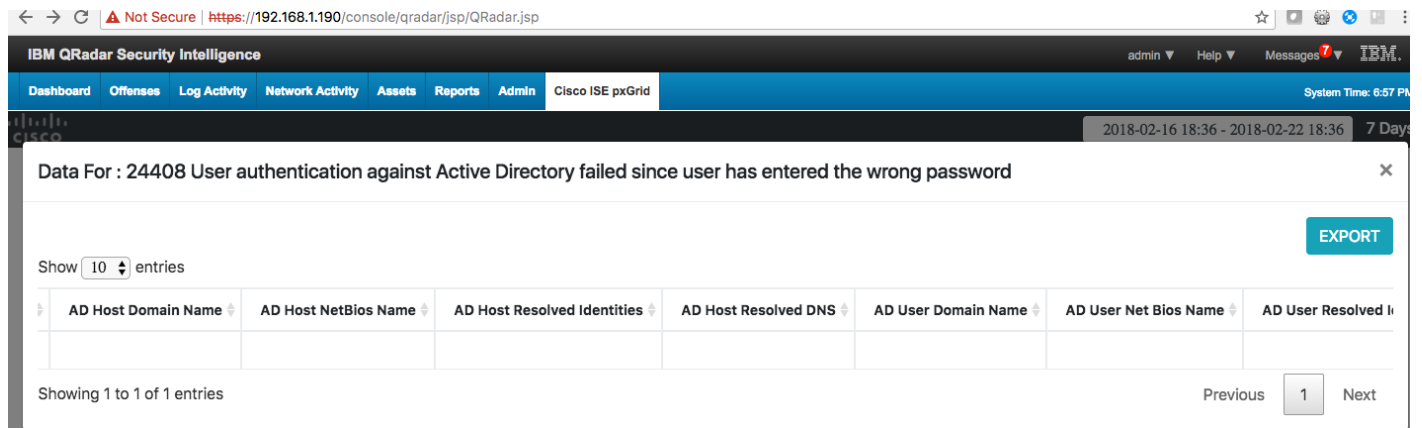
Offenses Log Activity Network Activity Assets Reports Admin Cisco ISE pxGrid

r : 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 screenshots provide additional context around the host and user identities.

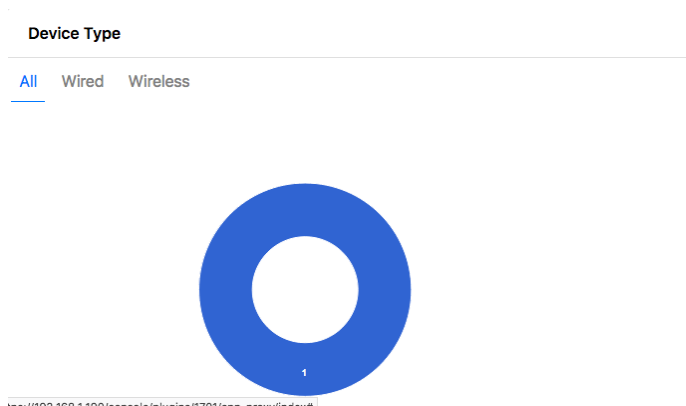


Device Type Panel

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

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

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



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 7

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 |

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

admin Help Messages 8

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

| Server Name | Authentication Protocol | Device Type | Location | Calling Station ID | NAS IP Address | NAS Port ID | NAS Port Type | MAC Address | Message Co |
|-------------|-------------------------|------------------|---------------|--------------------|----------------|-----------------------|---------------|-------------|------------|
| se24k | 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 **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 8

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 | | | |

EXPORT

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

The screenshot shows the 'Cisco ISE pxGrid' view in IBM QRadar. A table titled 'Device Types' is displayed with an 'EXPORT' button. The table has the following columns:

| 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 first screenshot shows a 'Device Type' donut chart with 'All' selected. The chart consists of a single blue ring representing 100% of the data.

The second screenshot shows a 'Location' bar chart with 'All' selected. The y-axis ranges from 0 to 51. A single bar for 'All Locations' reaches the value of 1.

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

The screenshot shows the 'Data For : All Locations' view in IBM QRadar. A table is displayed with the following columns and one row of data:

| ID | Dev Time | IP Address | Failure Reason | Username | Server |
|------------------|------------------------------|--------------|---|-------------------|--------|
| 1520519102122255 | 09-Mar-2018 06:57:48.530 EST | 192.168.1.60 | 24408 User authentication against Active Directory failed since user has entered the wrong password | pxgrid2@lab10.com | ise24k |

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 8 System Time: 10:22

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

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

Data For : All Locations

Show 10 entries

EXPORT

| 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 |

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 8 System Time: 10:22

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

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

Data For : All Locations

Show 10 entries

EXPORT

| 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 | | | |

Intelligence

admin Help Messages 8 System Time: 5:55

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

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

Locations

Show 10 entries

EXPORT

| 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 |
|-----------------------------|----------------------|---------------------|-----------------------|-----------------------------|----------------------|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

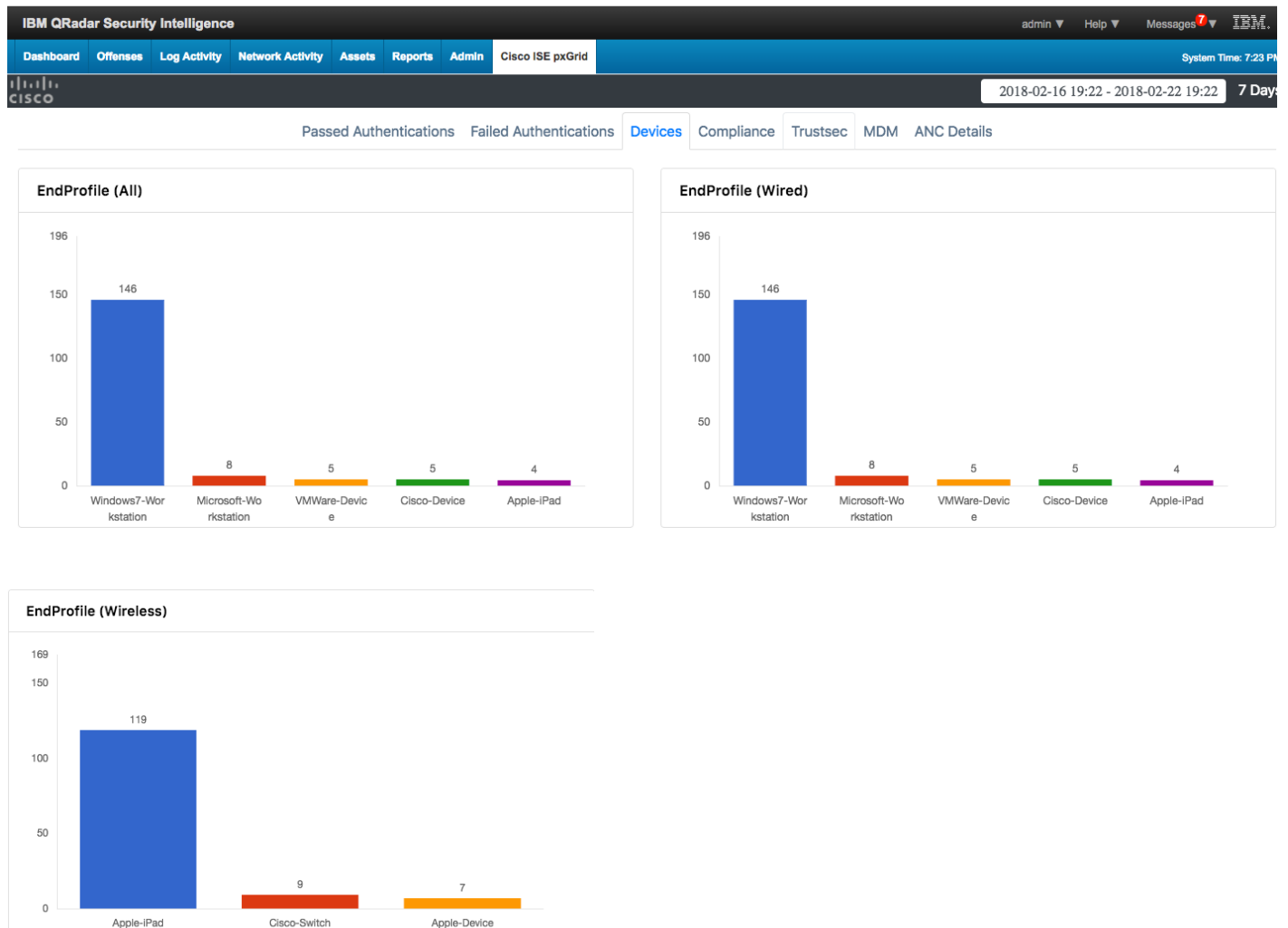
Devices

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 who the owner of these devices are and where they are located. 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, i.e. 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

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 | GigabitEthernet |
| 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 | GigabitEthernet |
| 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 | GigabitEthernet |

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.

For : Windows7-Workstation

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-P-[REDACTED] | [REDACTED] |
| 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 7 IBM

Dashboard Offenses Log Activity Network Activity Assets Reports Admin Cisco ISE pxGrid System Time: 9:06 P

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

Data For : Windows7-Workstation

Show 10 entries EXPORT

| AD Host NetBios Name | AD Host Resolved Identities | AD Host Resolved DNS | AD User Domain Name | AD User Net Bios Name | AD User Resolved Identiti |
|----------------------|-----------------------------|--|---------------------|-----------------------|---------------------------|
| PXGRID2-PC\$ | [REDACTED] | CN=PXGRID2-PC,CN=Computers,DC=[REDACTED] | | | |
| PXGRID2-PC\$ | [REDACTED] | | | [REDACTED] | [REDACTED] |
| PXGRID2-PC\$ | [REDACTED] | | | | |
| PXGRID2-PC\$ | [REDACTED] | | | | |

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

elligence admin Help Messages 7 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 Da

s7-Workstation

EXPORT

| AD User Resolved DNS | Terminal Server Agent ID | Is Machine Authentication | Service Type | Tunnel Private Group ID | Airespace WLAN ID |
|-----------------------------------|--------------------------|---------------------------|--------------|-------------------------|-------------------|
| | | true | Framed | | |
| CN=pxgrid2,CN=Users,DC=[REDACTED] | [REDACTED] | false | Framed | | |
| CN=pxgrid2,CN=Users,DC=[REDACTED] | [REDACTED] | false | Framed | | |

admin Help Messages 7 IBM

System Time: 9:11

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

EXPORT

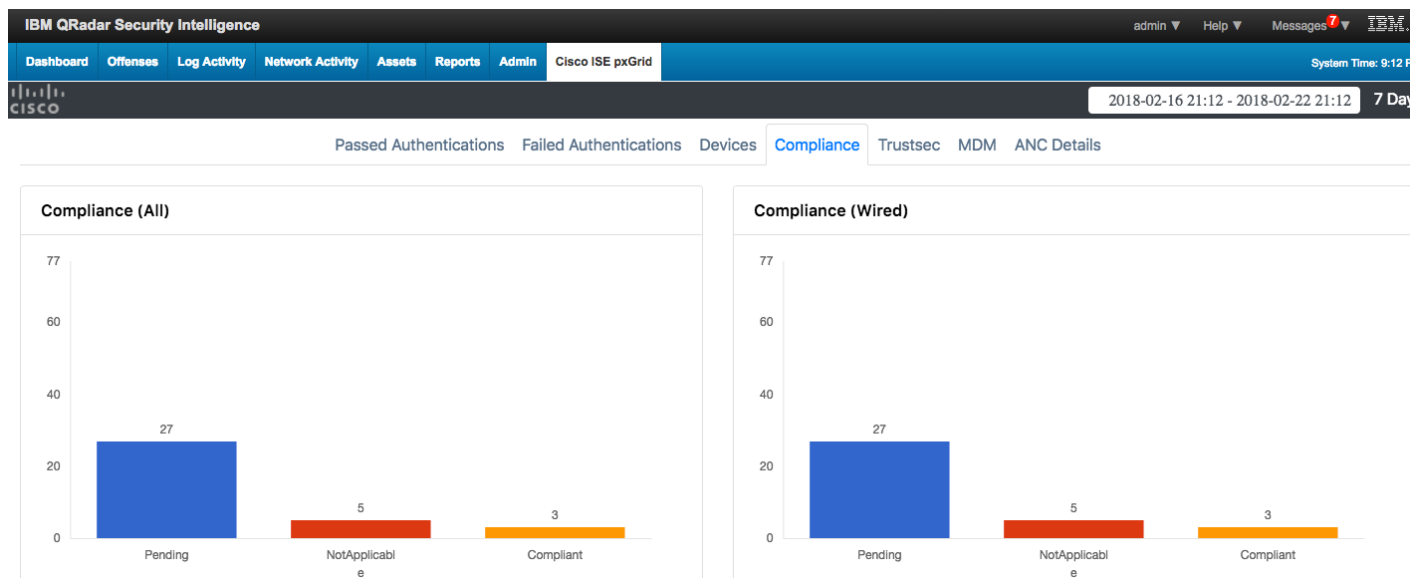
| Network Device Profile Name | Radius Flow Type | SSID |
|-----------------------------|------------------|-------------------|
| Cisco | Wired802_1x | 50-3D-E5-C4-05-8B |
| Cisco | Wired802_1x | 50-3D-E5-C4-05-8B |
| Cisco | Wired802_1x | 50-3D-E5-C4-05-8B |

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**



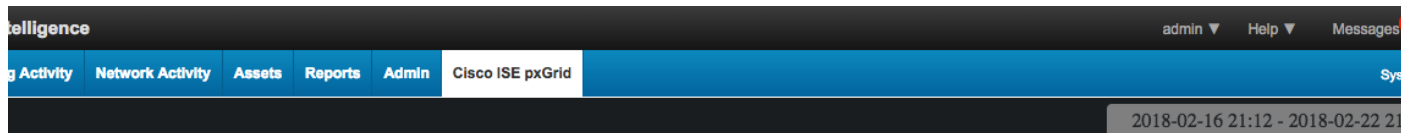
You will see a list of compliant end-users along with the associated contextual information.

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.

| Dev Time | IP Address | State | MAC Address | Username | Calling Station ID | Called Station ID | NAS IP Address | NAS Port ID | NAS Port Type |
|------------------------------|--------------|----------|-------------------|----------|--------------------|-------------------|----------------|-----------------------|---------------|
| 18-Feb-2018 10:17:19.596 EST | 192.168.1.15 | POSTURED | 00:50:56:86:BB:13 | pxgrid1 | 00:50:56:86:BB: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:BB:13 | pxgrid1 | 00:50:56:86:BB: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:BB:13 | pxgrid1 | 00:50:56:86:BB: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, pending.

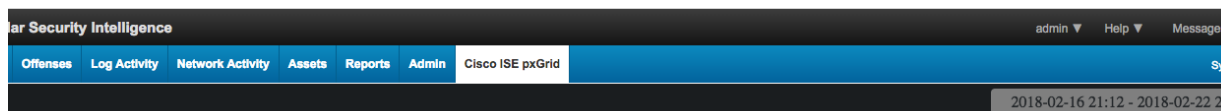
The **Endpoint Profile** attribute is the device information of the end-user along with the **Endpoint Operating System** attribute.



Endpoint

| 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.



or : Compliant

0 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 |
|----------------------|-----------------------------|----------------------|---------------------|-----------------------|-----------------------------|
| | 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

Security Intelligence

admin Help Messages 7

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

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

Compliant

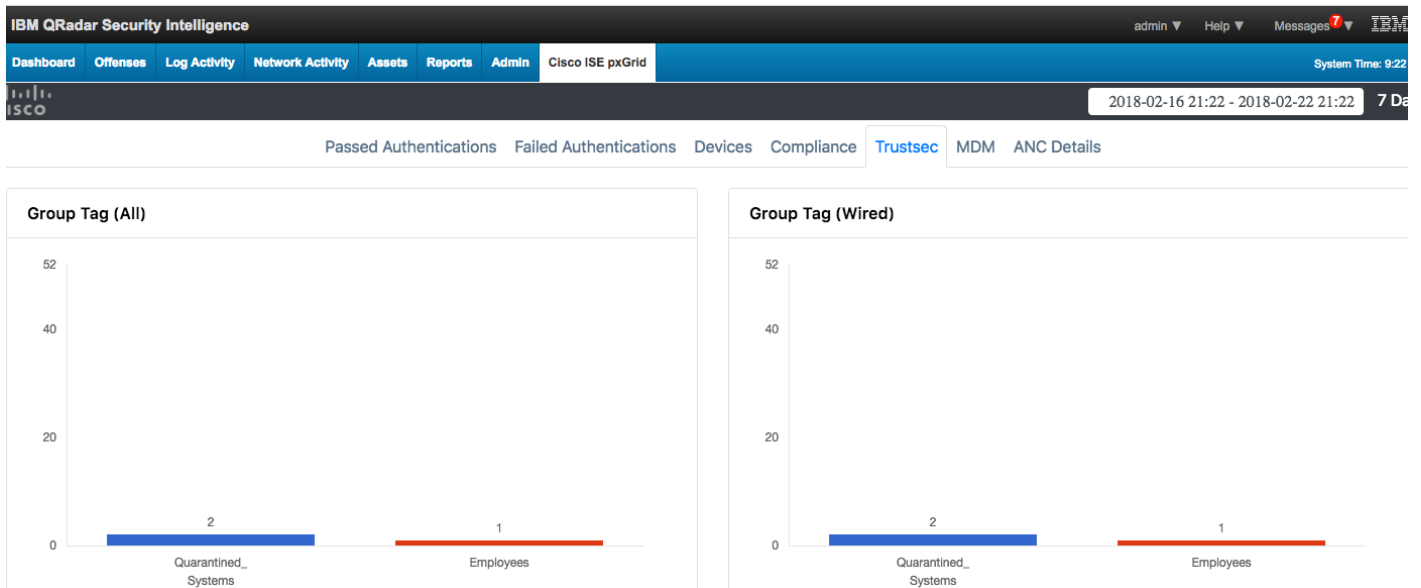
entries

| AD User Resolved DNS | Terminal Server Agent ID | Is Machine Authentication | Service Type | Tunnel Private Group ID | Airspace WLAN ID |
|----------------------------------|--------------------------|---------------------------|--------------|-------------------------|------------------|
| CN=pxGrid1,CN=Users,D [REDACTED] | | 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, 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 7 System Time: 2018-02-16 21:22 - 2018-02-22 21:22

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

Data For : Quarantined_Systems

[EXPORT](#)

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 resolvable identities** attributes.

IBM QRadar Security Intelligence admin Help Messages

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

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

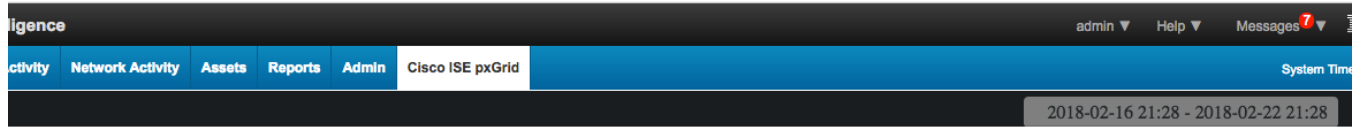
Dashboard Offenses Log Activity Network Activity Assets Reports Admin Cisco ISE pxGrid

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-PC\$ | | | LAB10 | |
| | PXGRID2-PC\$ | | | LAB10 | |

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



ed_Systems

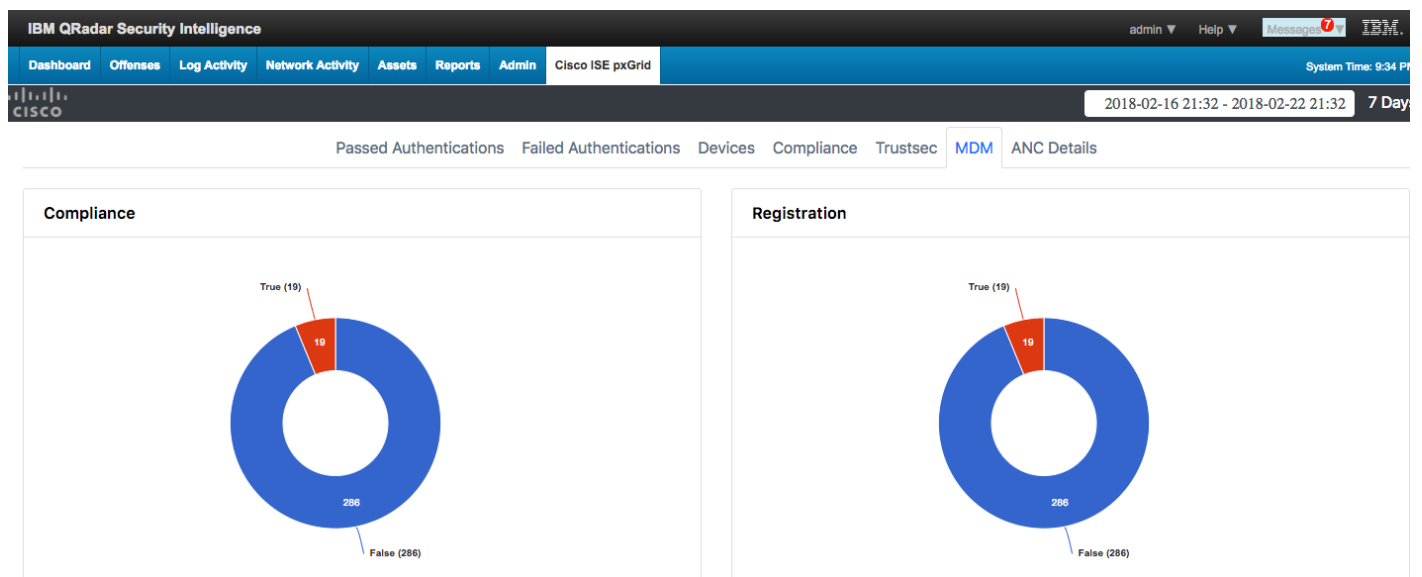
EXPOR

| 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.

The screenshot shows the IBM QRadar Security Intelligence interface. The top navigation bar includes 'Dashboard', 'Offenses', 'Log Activity', 'Network Activity', 'Assets', 'Reports', 'Admin', and 'Cisco ISE pxGrid'. The system time is 9:35 PM. The data range is 2018-02-16 21:32 - 2018-02-22 21:32. The 'Data For' is set to 'True'. There is an 'EXPORT' button. The table shows two entries for 'pxgrid1' with MAC address 88:CB:87:ED:45:DA and IP address 192.168.1.11. Both entries have 'Registration Status' and 'Compliance Status' set to 'True'.

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

ANC Details

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

Step 1 Select Cisco ISE pxGrid->ANC Details

The screenshot shows the IBM QRadar Security Intelligence interface with the 'ANC Details' view selected. The top navigation bar includes 'Passed Authentications', 'Failed Authentications', 'Devices', 'Compliance', 'Trustsec', 'MDM', and 'ANC Details'. The system time is 9:35 PM. The data range is 2018-02-16 21:50 - 2018-02-22 21:50. The 'Currently Assigned ANC policy' section shows one entry for MAC address 00:0C:29:C1:7B:2C with Policy Name 'pxGridQRadarQuarantine'.

| 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:

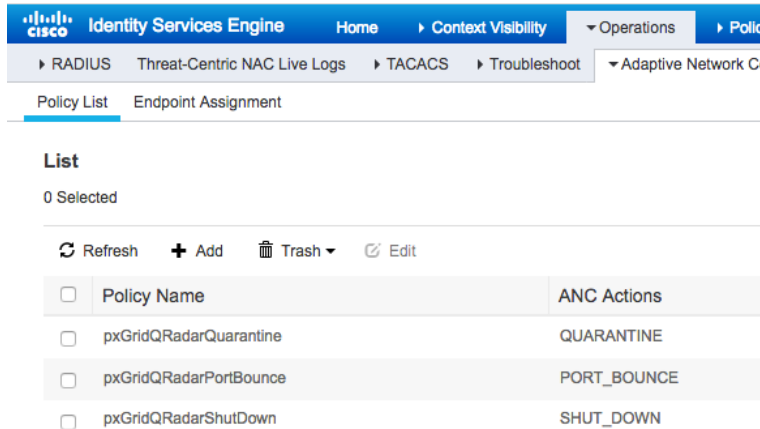
- pxGridQRadarQuarantine- issues a quarantine
- pxGridQRadarPortBounce- issues a port-bounce
- pxGridQRadarShutDown- issues a shut down

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

- Step 1** Select **Operations->Adaptive Network Control->Policy List->Add->**the following for the **Policy Name** and **Action**:
- Step 2** **pxGridQRadarQuarantine, QUARANTINE**
- Step 3** **pxGridQRadarPortBounce, PORT_BOUNCE**
- Step 4** **pxGridQRadatShutDown, SHUT_DOWN,**
- Step 5** Select **Save** after Policy Name and associated action

Step 6 You should see:



List

0 Selected

Refresh + Add Trash Edit

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

Adding ANC Policies to ISE Policy Sets

Configure ISE to send Syslog Events to QRadar.

Note: It is assumed the ISE DSM multiline collector has been installed in QRadar.

- Step 1** Select **Policy->Policy Sets->Default>”>”->Authorization Policy->Global Exceptions->”+”**
- Step 2** Under **Rule Name**, type: **ANCQuarantine**
- Step 3** Under **Conditions**, select “+”
- Step 4** Select “x” close the introductory screen
- 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 on the Gear and duplicate line below and add the rule name and ANCPolicy

- Step 12** You should see the following:

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Policy Sets Profiling Posture Client Provisioning > Policy Elements

Search

Default policy set Default Network Access

> Authentication Policy (3)

> Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions (3)

| + | 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 sections steps the reader through performing ANC mitigation actions on the endpoint from the Dashboards and Panels.

Step 1 User pxGrid1 authenticates in ISE.

| Time | Status | Details | Repeat ... | Identity | Endpoint ID | Endpoint P... | Authentication Policy | Authorization Policy | Authorizati. |
|------------------------------|--------------------------------------|---------|------------|---------------|-------------------|----------------|-----------------------|---------------------------------|----------------|
| Mar 09, 2018 07:18:30.952 PM | ● | | 0 | pxgrid1 | 00:50:56:86:BB:13 | Microsoft-W... | Default >> Dot1X | Default >> Basic_Authenticat... | PermitAcces... |
| Mar 09, 2018 07:18:30.671 PM | ✔ | | | pxgrid1 | 00:50:56:86:BB:13 | Microsoft-W... | Default >> Dot1X | Default >> Basic_Authenticat... | PermitAcces... |
| Mar 09, 2018 07:18:18.872 PM | ✔ | | | host/win7-pc3 | 00:50:56:86:BB:13 | Microsoft-W... | Default >> Dot1X | Default >> Basic_Authenticat... | PermitAcces... |
| Mar 09, 2018 07:17:51.173 PM | ✔ | | | host/win7-pc3 | 00:50:56:86:BB:13 | Microsoft-W... | Default >> Dot1X | Default >> Basic_Authenticat... | PermitAcces... |

Step 2 Select Cisco ISE pxGrid->Passed Authentications

| User | Count |
|-------------------|-------|
| pxgrid1 | 10 |
| win7-pc3 | 6 |
| 88:CB:87:ED:45:DA | 4 |
| user1 | 3 |
| [REDACTED] | 2 |
| pxgrid3 | 2 |

| User | Count |
|-------------------|-------|
| pxgrid1 | 10 |
| win7-pc3 | 6 |
| 88:CB:87:ED:45:DA | 4 |
| [REDACTED] | 2 |

Step 3 Select an end-user, pxGrid1 You should see:

IBM QRadar Security Intelligence

admin Help Messages 0 System Time: 2:20 P

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin Cisco ISE pxGrid 2018-03-03 14:20 - 2018-03-09 14:20 7 Day

Data For : pxgrid1

Show 10 entries

| 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:BB:13 | pxgrid1 | 00:50:56:86:BB: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:BB:13 | pxgrid1 | 00:50:56:86:BB: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:BB:13 | pxgrid1 | 00:50:56:86:BB:13 | 50:3D:E5:C4:05:8B | 192.168.1.3 | GigabitEthernet1/0/11 | Ethernet |

EXPORT

Step 4 Right-click on the IP address, you should will the ANC policies

IBM QRadar Security Intelligence

admin Help Messages 0 System Time: 2:22 P

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin Cisco ISE pxGrid 2018-03-03 14:20 - 2018-03-09 14:20 7 Day

Data For : pxgrid1

Show 10 entries

| 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:BB:13 | pxgrid1 | 00:50:56:86:BB: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:BB:13 | pxgrid1 | 00:50:56:86:BB: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:BB:13 | pxgrid1 | 00:50:56:86:BB: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:BB:13 | pxgrid1 | 00:50:56:86:BB:13 | 50:3D:E5:C4:05:8B | 192.168.1.3 | GigabitEthernet1/0/11 | Ethernet |

EXPORT

Cisco pxGrid ANC Actions

- pxGridQRadarQuarantine
- pxGridQRadarPortBounce
- pxGridQRadarShutDown

Step 5 Select pxGridQRadarQuarantine

Step 6 You should see a successful status message

IBM QRadar Security Intelligence

Dashboard Offenses Log Activity Network Activity Assets Reports

Data For : pxgrid1

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**

You should see that the endpoint has been quarantined based on the ANCQuarantine Policy

The screenshot shows the Cisco ISE pxGrid App ANC Dashboard. 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 says "Click here to do wireless setup and visibility setup Do not show this again." Below the navigation is a summary section with five cards: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (0), Client Stopped Responding (5), and Repeat Counter (0). Below this is a table of records with columns: Time, Status, Details, Repeat..., Identity, Endpoint ID, Endpoint P..., Authentication Policy, Authorization Policy, and Authorizati... The table contains three rows of data, all with a status of 'Quarantined'.

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

Note the MAC Address of the quarantined endpoint.

The screenshot shows the Cisco ISE pxGrid App TrustSec Dashboard. The top navigation bar includes: Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Risks, Vulnerabilities, Admin, and Cisco ISE pxGrid. The current page is 'ANC Details'. Below the navigation is a section titled 'Currently Assigned ANC policy'. It shows a table with two columns: 'Mac Address' and 'Policy Name'. The table contains one entry: Mac Address '00:50:56:86:BB:13' and Policy Name 'pxGridQRadarQuarantine'. Below the table, it says 'Showing 1 to 1 of 1 entries' and has 'Previous', '1', and 'Next' buttons.

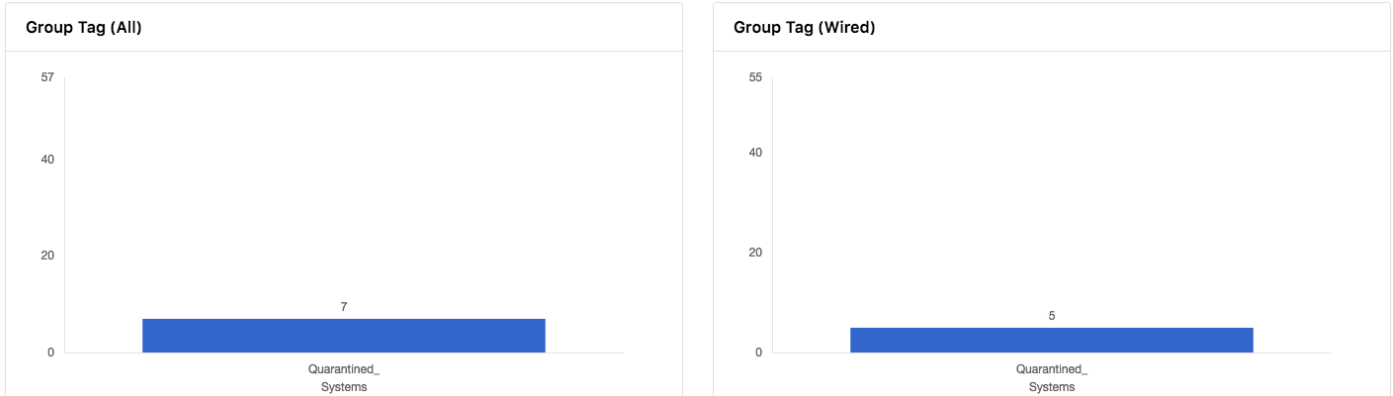
Step 10 To view the details in the Cisco ISE pxGrid App TrustSec Dashboard, select **Cisco ISE pxGrid->Trustsec**

IBM QRadar Security Intelligence admin Help Messages 8 IBM

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin Cisco ISE pxGrid System Time: 2:39 PM

2018-03-03 14:34 - 2018-03-09 14:34 7 Days

Passed Authentications Failed Authentications Devices Compliance Trustsec MDM ANC Details



Step 11 Select **Quarantined_Systems**, you should see the quarantined endpoint

IBM QRadar Security Intelligence admin Help Messages 8 IBM

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin Cisco ISE pxGrid System Time: 2:40 PM

2018-03-03 14:34 - 2018-03-09 14:34 7 Days

Data For : Quarantined_Systems X

Show 10 entries EXPORT

| 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:BB:13 | pxgrid1 | 00:50:56:86:BB: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:BB:13 | pxgrid1 | 00:50:56:86:BB:13 | 50:3D:E5:C4:05:8B | 192.168.1.3 | GigabitEthernet1/0/1 |
| 08-Mar-2018 10:24:20.597 EST | 192.168.1.57 | DISCONNECTED | 88:CB:87:ED:45:DA | 88:CB:87:ED:45:DA | 88:CB:87:ED:45:DA | 50:3D:E5:C4:05:83 | 192.168.1.3 | GigabitEthernet1/0/3 |
| 08-Mar-2018 10:24:20.597 EST | 192.168.1.57 | DISCONNECTED | 88:CB:87:ED:45:DA | 88:CB:87:ED:45:DA | 88:CB:87:ED:45:DA | 50:3D:E5:C4:05:83 | 192.168.1.3 | GigabitEthernet1/0/3 |

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

Step 13 Right-click on the MAC Address

IBM QRadar Security Intelligence

admin Help Messages 8 System Time: 2:44 PM

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin Cisco ISE pxGrid 2018-03-03 14:34 - 2018-03-09 14:34 7 Day

Data For : Quarantined_Systems

Show 10 entries EXPORT

| 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:... | | 00:50:56:86:BB: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:... | | 00:50:56:86:BB: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:... | | 88:CB:87:ED:45:DA | 50:3D:E5:C4:05:83 | 192.168.1.3 | GigabitEthernet1/0/3 |
| 08-Mar-2018 10:24:20.597 EST | 192.168.1.57 | DISCONNECTED | 88:CB:87:ED:... | 88:CB:87:ED:45:DA | 88:CB:87:ED:45:DA | 50:3D:E5:C4:05:83 | 192.168.1.3 | GigabitEthernet1/0/3 |

- Step 14 Select pxGridQRadarClear
- Step 15 You should see successful status message

IBM QRadar Security Intelligence

Dashboard Offenses Log Activity Network Activity Assets Reports

Data For : Quarantined_Systems

192.168.1.192 Says

Status : RUNNING

Operation Id : ise24k.lab10.com:2

OK

- Step 16 Select OK
- Step 17 To view the results in ISE, select **Operations->RADIUS->Live Logs**, you should see that the endpoint has been unquarantined

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

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

Live Logs Live Sessions

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

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

Refresh Never Show Latest 20 records Within Last 3 hours

| Time | Status | Details | Repeat ... | Identity | Endpoint ID | Endpoint P... | Authentication Policy | Authorization Policy | Authorizati... |
|------------------------------|--------|---------|------------|----------|-------------------|----------------|-----------------------|---------------------------------|----------------|
| Mar 09, 2018 07:48:43.693 PM | 🟡 | | 0 | pxgrid1 | 00:50:56:86:BB:13 | Microsoft-W... | Default >> Dot1X | Default >> Basic_Authenticat... | PermitAcces... |
| Mar 09, 2018 07:48:42.916 PM | 🟢 | | | pxgrid1 | 00:50:56:86:BB:13 | Microsoft-W... | Default >> Dot1X | Default >> Basic_Authenticat... | PermitAcces... |
| Mar 09, 2018 07:45:52.604 PM | 🟢 | | | pxgrid1 | 00:50:56:86:BB:13 | Microsoft-W... | Default >> Dot1X | Default >> Basic_Authenticat... | PermitAcces... |
| Mar 09, 2018 07:45:51.107 PM | 🟢 | | | | 00:50:56:86:BB:13 | | | | |

- 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 8 IBM

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin Cisco ISE pxGrid System Time: 2:52 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 unquarantine or clear in ISE, select Operations->Adaptive Network Control->Endpoint Assignment->select the endpoint MAC address->Trash

Configuring IBM QRadar for Cisco ISE Syslog Events

The IBM Device Support Module (DSM) for Cisco Identity Service Engine needs to be installed in the IBM QRadar instance. For more information, please see IBM DSM Configuration Guide:

ftp://ftp.software.ibm.com/software/security/products/qradar/documents/iTeam_addendum/b_dsm_guide.pdf

Step 1 Select **Admin->Log Sources->Add the following**

| | |
|--|---|
| Log Source Name | <input type="text" value="Cisco_ISE"/> |
| Log Source Description | <input type="text" value="Cisco_ISE"/> |
| Log Source Type | Cisco Identity Services Engine |
| Protocol Configuration | UDP Multiline Syslog |
| Log Source Identifier | <input type="text" value=""/> |
| Listen Port | <input type="text" value="517"/> |
| Message ID Pattern | <input type="text" value="CISE_IS* (s(10))"/> |
| Event Formatter | No Formatting |
| Enabled | <input checked="" type="checkbox"/> |
| Credibility | <input type="text" value="5"/> |
| Target Event Collector | eventcollector0 :: qradar2 |
| Coalescing Events | <input checked="" type="checkbox"/> |
| Store Event Payload | <input checked="" type="checkbox"/> |
| Please select any groups you would like this log source to be a member of: | |
| <input type="text"/> | |

Step 2 Select **Save**

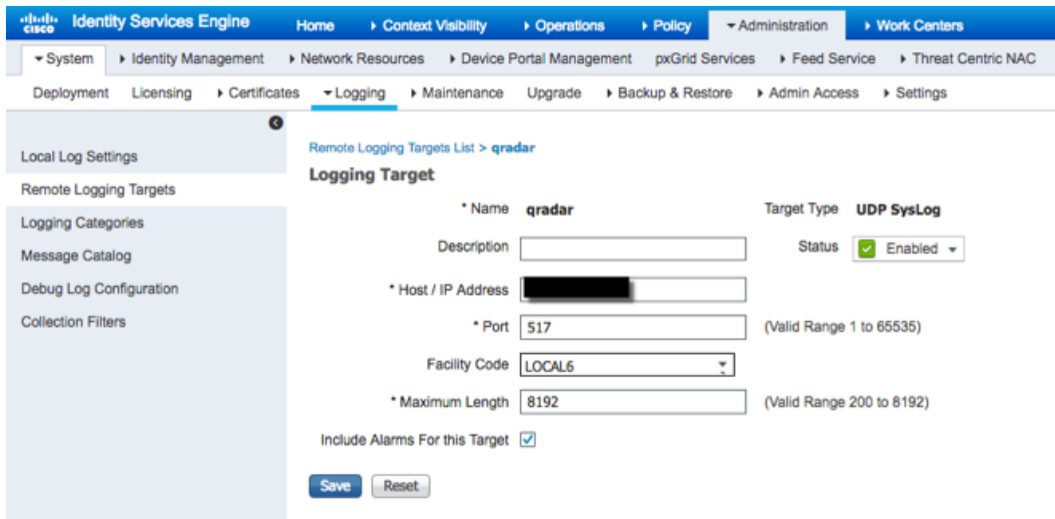
Step 3 Select **Deploy Changes->Deploy**

Step 4 **Administration->System->Logging->Remote Logging Targets->Add->enter Host/ IP address of the IBM QRadar instance**

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, etc, where you can take ANC mitigation actions on the endpoint.

Step 1 Select **Administration->System->Logging->Remote Logging Targets->Add->type: Host/ IP address of IBM QRadar instance and 517 for the Port**



The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is: Administration > System > Logging > Remote Logging Targets > Add > type: Host/ IP address of IBM QRadar instance and 517 for the Port. The page title is "Remote Logging Targets List > qradar". The "Logging Target" configuration form is displayed with the following fields:

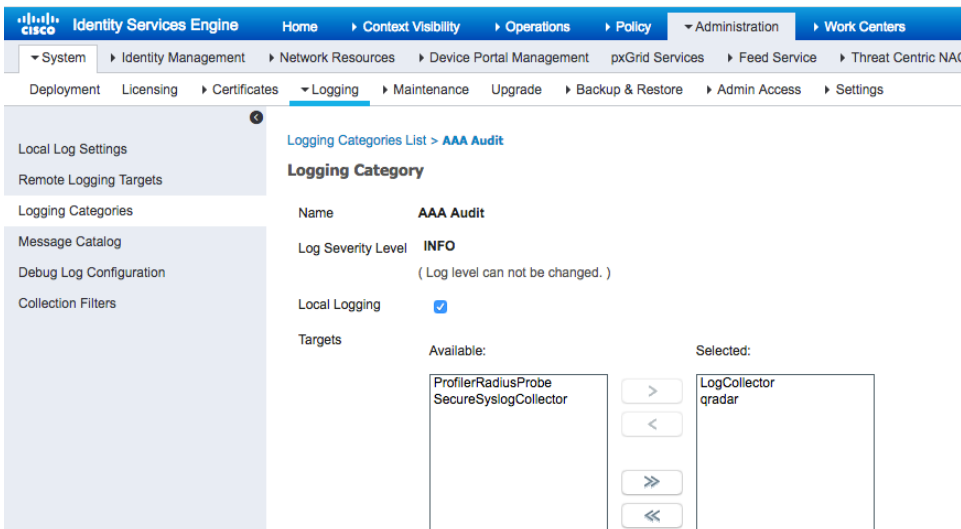
- Name: qradar
- Target Type: UDP SysLog
- Status: Enabled
- Description: (empty)
- * Host / IP Address: (redacted)
- * Port: 517 (Valid Range 1 to 65535)
- Facility Code: LOCAL6
- * Maximum Length: 8192 (Valid Range 200 to 8192)
- Include Alarms For this Target:

Buttons for "Save" and "Reset" are visible at the bottom of the form.

Step 2 Select **Save**

Step 3 Select **Logging Categories->AAA Audit->Edit**

Step 4 Move qRadar from Targets **Available** into the **Selected** column



The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is: Administration > System > Logging > Logging Categories > AAA Audit > Edit. The page title is "Logging Categories List > AAA Audit". The "Logging Category" configuration form is displayed with the following fields:

- Name: AAA Audit
- Log Severity Level: INFO (Log level can not be changed.)
- Local Logging:
- Targets:

| Available: | Selected: |
|--|------------------------|
| ProfilerRadiusProbe SecureSyslogCollector | LogCollector qradar |

Navigation buttons (>, <, >>, <<) are visible between the Available and Selected target lists.

Step 5 Select **Save**

Step 6 Perform this for AAA Audit, Passed Authentications, Failed Attempts, Accounting, RADIUS Accounting, Administrative and Operational Audit, Posture and Client Provisioning Audit, Profiler

Step 7 When completed, you should see the following:

Identity Services Engine Administration Work Centers License V

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Edit

| 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

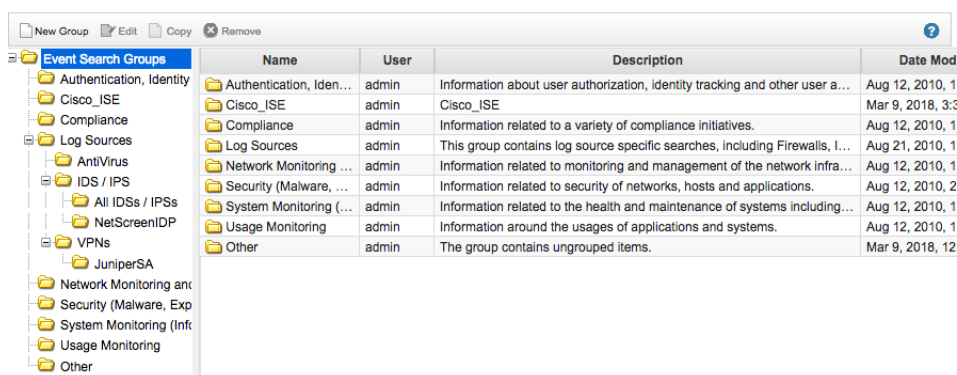
The desired endpoints for performing ANC mitigation actions must have been authenticated through ISE. In this example, we have Cisco ISE Passed Authentication syslog events sent over to IBM QRadar. We have to create a custom FramedIPAddress field to provide the IP address of the endpoint.

Note: IBM will add this later in 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

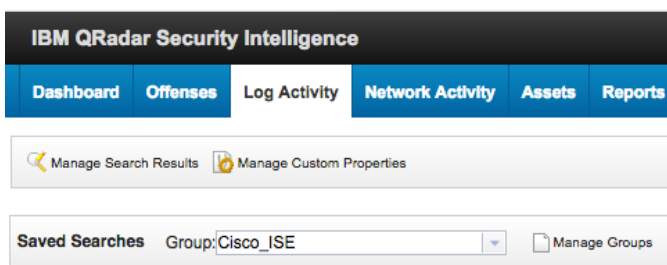
The FramedIPAddress field will be added to the available columns field in the Log Activity Search created for ISE. The FramedIPAddress field will now appear in ISE Log Activity searches.

Creating Custom Field for Framed IP Address ISE Syslog Event

Step 1 In IBM QRadar, select Log Activity->Search->New Search->Manage Groups->New Group->Cisco_ISE
You should see the Cisco ISE group



Step 2 Select Cisco_ISE Group



Step 3 Keep the Search defaults

IBM QRadar Security Intelligence

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

Manage Search Results Manage Custom Properties

Search Mode

Basic Search Advanced Search

Time Range:

Real Time (streaming) Last Interval (auto refresh) Recent Specific Interval

Last 5 Minutes Start Time 3/11/2018 at 7:25 PM
End Time 3/11/2018 at 7:30 PM

Step 4 Keep the Column defaults

Column Definition

Display: Default (Normalized)

Advanced View Definition

Type Column or Select from List

Available Columns

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

Group By:

Columns

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

Order By: Start Time Desc

Results Limit: 1,000

Step 5 Under Search Parameters->Parameter->Quick Filters->Log Source (Indexed)->Equals->Log Source Filter->Cisco_ISE-Add Filter

Search Parameters

Parameter: Log Source [Indexed] Operator: Equals Value: Log Source Filter: Type to Filter

Log Source: Anomaly Detection Engine-2 :: qrada...
Asset Profiler-2 :: qradar2
Cisco_ISE
Custom Rule Engine-8 :: qradar2
Health Metrics-2 :: qradar2

Add Filter

Current Filters

Log Source is Cisco_ISE

Remove Selected Filters

Step 6 Select 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 Login 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 |

Step 7 Select Passed Auth->Extract Property

Step 8 For New Property, type: FramedIPAddress

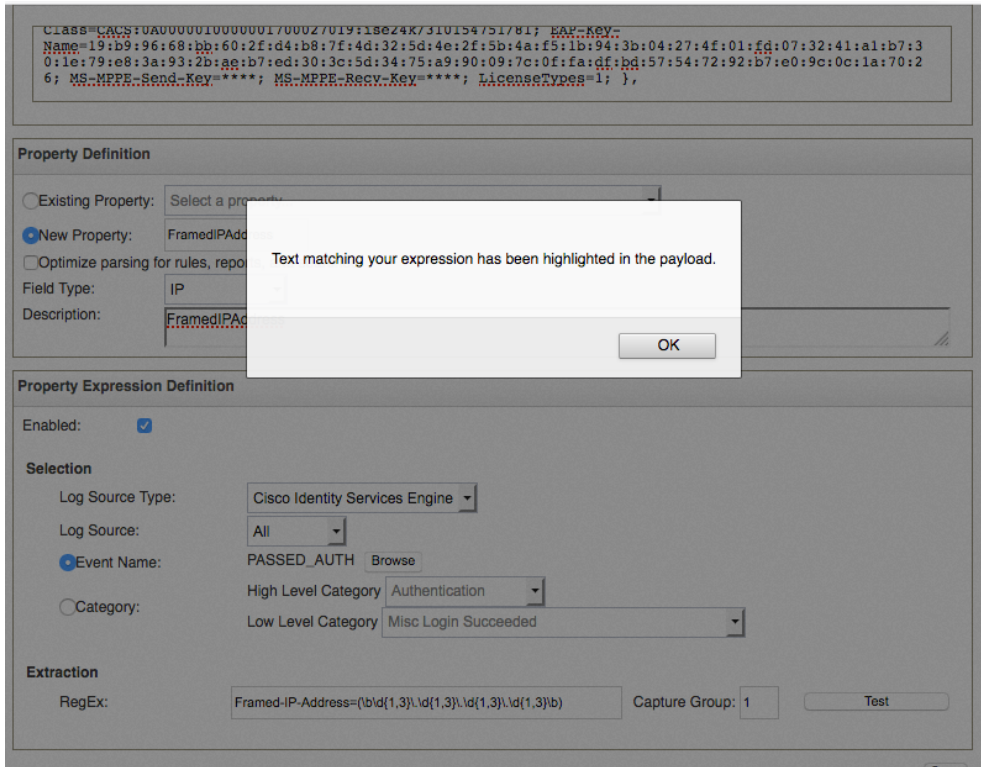
Step 9 For Field Type, type: IP

Step 10 For Description, type: FramedIPAddress

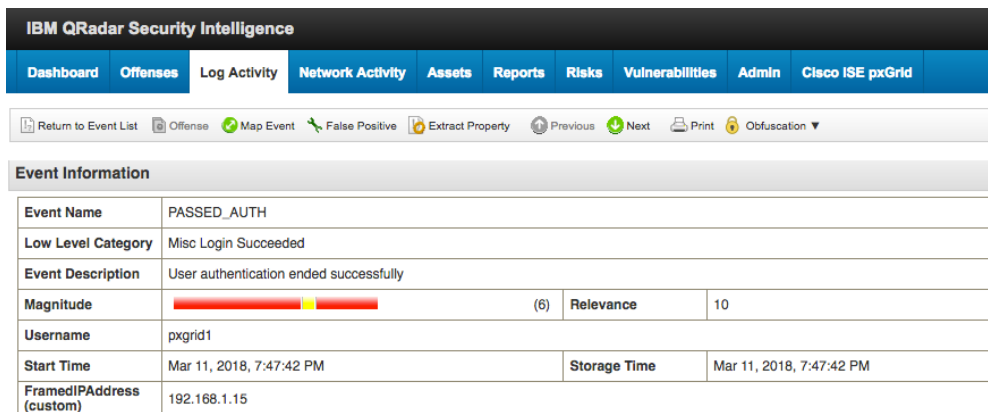
Step 11 For Extraction->RegEx:, type: Framed-IP-Address=(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b)
You should see:

Step 12 Select Test

You should see



- Step 13 Select **OK**
- Step 14 Select **Save**
- Step 15 Ensure you see you see the **FramedIPAddress** appear



- Step 16 Select **Return to Event List**
- Step 17 Select **Search->Edit Search->Saved Searches->Group:Cisco_ISE**

Step 18 Scroll Down to **Column Definition->Available Columns->FramedIPAddress(Custom)->Move to Columns** by selecting “>”

The screenshot shows the 'Advanced View Definition' section of the IBM QRadar Security Intelligence interface. It includes a 'Display' dropdown set to 'Custom', a 'Name' input field, and a 'Save Column Layout' button. Below this is the 'Advanced View Definition' section with a 'Type Column or Select from List' input. The 'Available Columns' list on the left contains various metrics, with 'FramedIPAddress (custom)' highlighted. The 'Columns' list on the right shows the selected columns, including 'FramedIPAddress (custom)'. The 'Order By' dropdown is set to 'Start Time' and 'Desc', and the 'Results Limit' is set to 1,000.

Step 19 Under **Search Parameters->Parameter->Quick Filters->Log Source (Indexed)->Equals->Log Source Filter->Cisco_ISE-Add Filer**

The screenshot shows the 'Search Parameters' configuration page. The 'Parameter:' dropdown is set to 'Log Source [Indexed]', the 'Operator:' is 'Equals', and the 'Value:' is 'Log Source Filter: Type to Filter'. The 'Log Source:' dropdown is open, showing a list of log sources including 'Anomaly Detection Engine-2 :: qrada...', 'Asset Profiler-2 :: qrada2', 'Cisco_ISE', 'Custom Rule Engine-8 :: qrada2', and 'Health Metrics-2 :: qrada2'. The 'Add Filter' button is visible. The 'Current Filters' section shows 'Log Source is Cisco_ISE'.

Step 20 Select **Filter**

Step 21 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 | pxgrid1 | High | 192.168.1.15 |
| PASSED_AUTH | Cisco_ISE | 1 | Mar 11, 2018, 8:... | Misc Login Succ... | 192.168.1.3 | 0 | 192.168.1.147 | 1645 | pxgrid1 | High | 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 | High | 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 | High | 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 | High | 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 | High | N/A |
| CiscoISE_Alarm | Cisco_ISE | 1 | Mar 11, 2018, 8:... | Warning | 192.168.1.147 | 0 | 192.168.1.147 | 0 | N/A | High | N/A |
| AUTHEN_PASSED | Cisco_ISE | 1 | Mar 11, 2018, 8:... | Admin Login Su... | 192.168.1.136 | 0 | 192.168.1.147 | 0 | admin | High | 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 | High | 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 | High | N/A |

ANC Mitigation Syslog Event Example

Step 1 The user has been successfully authenticated through ISE

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

| Time | Status | Details | Repeat ... | Identity | Endpoint ID | Endpoint P... | Authentication Policy | Authorization Policy | Authorizati... |
|------------------------------|---------|---------|------------|----------|-------------------|----------------|-----------------------|---------------------------------|----------------|
| Mar 09, 2018 10:49:41.441 PM | Success | | 0 | pxgrid1 | 00:50:56:86:BB:13 | Microsoft-W... | Default >> Dot1X | Default >> Basic_Authenticat... | PermitAcces... |
| Mar 09, 2018 10:49:40.488 PM | Success | | 0 | pxgrid1 | 00:50:56:86:BB:13 | Microsoft-W... | Default >> Dot1X | Default >> Basic_Authenticat... | PermitAcces... |

Step 2 In the QRadar, select the syslog event, Right-click on **FramedIPAddress** and select **More Options**
In the example below, a Passed authentication syslog event was received from ISE.

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

IBM QRadar Security Intelligence admin Help Messages 8 IBM System Time: 5:54 PM

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

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

Records Matched Over Time 3/9/18, 5:24 PM - 3/9/18, 5:54 PM

(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 | 5 | N/A |
| PROFILER_EN... | Cisco_ISE | 1 | Mar 9, 2018, 5:4... | Information | 192.168.1.3 | 1645 | 192.168.1.147 | 1645 | 00505686bb13 | 5 | N/A |
| PROFILER_EN... | Cisco_ISE | 1 | Mar 9, 2018, 5:4... | Information | 192.168.1.3 | 1645 | 192.168.1.147 | 1645 | 00505686bb13 | 5 | N/A |
| PROFILER_EN... | Cisco_ISE | 1 | Mar 9, 2018, 5:4... | Information | 192.168.1.3 | 1645 | 192.168.1.147 | 1645 | 00505686bb13 | 5 | N/A |
| RADIUS_ACCO... | Cisco_ISE | 1 | Mar 9, 2018, 5:4... | RADIUS Sessio... | 192.168.1.3 | 0 | 192.168.1.147 | 0 | N/A | 5 | N/A |
| PASSED_AUTH... | Cisco_ISE | 1 | Mar 9, 2018, 5:4... | Misc Login Succ... | 192.168.1.3 | 0 | 192.168.1.147 | 1645 | msadrt1 | 5 | 192.168.1.15 |
| AUTHEN_PASS... | Cisco_ISE | 1 | Mar 9, 2018, 5:4... | Admin Login Su... | 192.168.1.136 | 0 | 192.168.1.147 | 0 | | 5 | |
| PROFILER_EN... | Cisco_ISE | 1 | Mar 9, 2018, 5:4... | Information | 192.168.1.3 | 1645 | 192.168.1.147 | 1645 | | 5 | |
| FAILED_AZN... | Cisco_ISE | 1 | Mar 9, 2018, 5:4... | General Authent... | 192.168.1.147 | 0 | 192.168.1.147 | 0 | | 5 | |
| CiscoISE_Alarm | Cisco_ISE | 1 | Mar 9, 2018, 5:4... | Warning | 192.168.1.147 | 0 | 192.168.1.147 | 0 | | 5 | |
| CiscoISE_Alarm | Cisco_ISE | 1 | Mar 9, 2018, 5:4... | Warning | 192.168.1.147 | 0 | 192.168.1.147 | 0 | | 5 | |
| CiscoISE_Alarm | Cisco_ISE | 1 | Mar 9, 2018, 5:2... | Warning | 192.168.1.147 | 0 | 192.168.1.147 | 0 | | 5 | |
| CiscoISE_Alarm | Cisco_ISE | 1 | Mar 9, 2018, 5:2... | Warning | 192.168.1.147 | 0 | 192.168.1.147 | 0 | | 5 | |
| Unknown Cisco ... | Cisco_ISE | 1 | Mar 9, 2018, 5:2... | Unknown | 192.168.1.147 | 0 | 192.168.1.147 | 0 | | 5 | |

Displaying 1 to 15 of 15 Items (Elapsed time: 0:00:00.098)

Step 3 Select More Options->Cisco pxGrid – ANC Quarantine

IBM QRadar Security Intelligence admin Help Messages 8 IBM System Time: 5:57 PM

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

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

Records Matched Over Time 3/9/18, 5:24 PM - 3/9/18, 5:54 PM

(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 | 5 | N/A |
| PROFILER_EN... | Cisco_ISE | 1 | Mar 9, 2018, 5:4... | Information | 192.168.1.3 | 1645 | 192.168.1.147 | 1645 | 00505686bb13 | 5 | N/A |
| PROFILER_EN... | Cisco_ISE | 1 | Mar 9, 2018, 5:4... | Information | 192.168.1.3 | 1645 | 192.168.1.147 | 1645 | 00505686bb13 | 5 | N/A |
| PROFILER_EN... | Cisco_ISE | 1 | Mar 9, 2018, 5:4... | Information | 192.168.1.3 | 1645 | 192.168.1.147 | 1645 | 00505686bb13 | 5 | N/A |
| RADIUS_ACCO... | Cisco_ISE | 1 | Mar 9, 2018, 5:4... | RADIUS Sessio... | 192.168.1.3 | 0 | 192.168.1.147 | 0 | N/A | 5 | N/A |
| PASSED_AUTH... | Cisco_ISE | 1 | Mar 9, 2018, 5:4... | Misc Login Succ... | 192.168.1.3 | 0 | 192.168.1.147 | 1645 | msadrt1 | 5 | 192.168.1.15 |
| AUTHEN_PASS... | Cisco_ISE | 1 | Mar 9, 2018, 5:4... | Admin Login Su... | 192.168.1.136 | 0 | 192.168.1.147 | 0 | | 5 | |
| PROFILER_EN... | Cisco_ISE | 1 | Mar 9, 2018, 5:4... | Information | 192.168.1.3 | 1645 | 192.168.1.147 | 1645 | | 5 | |
| FAILED_AZN... | Cisco_ISE | 1 | Mar 9, 2018, 5:4... | General Authent... | 192.168.1.147 | 0 | 192.168.1.147 | 0 | | 5 | |
| CiscoISE_Alarm | Cisco_ISE | 1 | Mar 9, 2018, 5:4... | Warning | 192.168.1.147 | 0 | 192.168.1.147 | 0 | | 5 | |
| CiscoISE_Alarm | Cisco_ISE | 1 | Mar 9, 2018, 5:4... | Warning | 192.168.1.147 | 0 | 192.168.1.147 | 0 | | 5 | |
| CiscoISE_Alarm | Cisco_ISE | 1 | Mar 9, 2018, 5:2... | Warning | 192.168.1.147 | 0 | 192.168.1.147 | 0 | | 5 | |
| CiscoISE_Alarm | Cisco_ISE | 1 | Mar 9, 2018, 5:2... | Warning | 192.168.1.147 | 0 | 192.168.1.147 | 0 | | 5 | |
| Unknown Cisco ... | Cisco_ISE | 1 | Mar 9, 2018, 5:2... | Unknown | 192.168.1.147 | 0 | 192.168.1.147 | 0 | | 5 | |

Displaying 1 to 15 of 15 Items (Elapsed time: 0:00:00.098)

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 ANCQuarantine Policy

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

Step 8 To unquarantine, or clear the endpoint,
Select ISE->Operations->Adaptive Network Control->Endpoint Assignment

Step 9 Select the endpoint MAC address->Trash

Step 10 Select selected, you should see:

Step 11 Select Yes

Step 12 In ISE, select Operations->RADIUS-Live Logs
You should that the endpoint has been unquarantined

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.

Step 1 Move your cursor over the IP address field and the contextual information will be 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 pxGrid. Below the navigation is a search bar and a filter section. A chart displays network activity over time, with a tooltip for the period 2/2/18, 4:11 PM - 2/18/18, 4:16 PM. Below the chart is a table of log entries. A tooltip is displayed over the 'Destination IP' field of the first row, showing session details for a user named 'hostpxGrid'.

| Start Time | Low Level Category | Source IP | Source Port | Destination IP | Destination Port | Username | Magnitude | FramedIPAddress (custom) | NAS-Port (custom) | NAS-Port-Type (custom) | NASIPAddr (custom) |
|----------------------------|------------------------|-------------|-------------|---|------------------|------------|-----------|--------------------------|-------------------|------------------------|--------------------|
| 1 Feb 18, 2018, 4:15:58 PM | Misc Login Succeeded | 192.168.1.3 | 0 | 192.168.1.147 | 1645 | 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 User Name: hostpxGrid2-PC.lab10.com Mac Address: 00:0C:29:C1:7B:2C Posture Status: None Endpoint Profile: Windows7-Workstation | | | | | | | |
| 1 Feb 18, 2018, 4:15:28 PM | RADIUS Session Ended | 192.168.1.3 | 0 | | | | | 92.168.1.7 | 50111 | Ethernet | 192.168.1.7 |
| 1 Feb 18, 2018, 4:15:27 PM | Misc Login Succeeded | 192.168.1.3 | 0 | | | | | 92.168.1.7 | 50111 | Ethernet | 192.168.1.7 |
| 1 Feb 18, 2018, 4:15:26 PM | Information | 192.168.1.3 | 0 | | | | | 92.168.1.7 | N/A | N/A | N/A |
| 1 Feb 18, 2018, 4:15:25 PM | RADIUS Session Started | 192.168.1.3 | 0 | | | | | 92.168.1.7 | 50111 | Ethernet | 192.168.1.7 |





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 test that triggers an action when specific actions are met. Offenses are generated when events and flow data passes through the CRE, it is correlated against the rules that are configured and an offense can be generated based on this correlation and viewed in the Offenses Tab.

The Cisco pxGrid offense rule gets triggered when an event occurs the match Radius Failure session or simply 3 event s 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 login with an invalid password, than login successfully, this will trigger a failed event followed by a successful login. Repeat this step 3 or 4 times within 10 minutes, and this will trigger the IBM QRadar pxGrid Offense rule

Below is a sample ISE authentication failure report that can be run to be used to confirm 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 the events in ISE

| Time | Status | Source | Destination | Protocol | Authentication Policy | Authorization 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 01:29:06.492 AM | Success | LAB10pxgrid2 | 00:0C:29:C1:7B:2C | Windows7... | Default >> Dot1X | Default >> Basic_Authenticat... |
| Mar 10, 2018 01:21:15.884 AM | Success | [Redacted] | 10:00:B1:C9:3C:39 | Apple-Device | Default >> Dot1X | Default >> Basic_Authenticat... |
| Mar 10, 2018 01:21:15.160 AM | Success | [Redacted] | 10:00:B1:C9:3C:39 | Apple-Device | Default >> Dot1X | Default >> Basic_Authenticat... |
| Mar 10, 2018 01:16:17.167 AM | Success | 10:00:B1:C9:3C:39 | 10:00:B1:C9:3C:39 | Apple-Device | Default >> MAB | Default >> Basic_Authenticat... |
| Mar 10, 2018 12:59:44.623 AM | 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 | pxgrid2@lab10.com | 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 | host/pxGrid2-PC1... | 00:0C:29:C1:7B:2C | Windows7... | Default >> Dot1X | Default >> Basic_Authenticat... |
| Mar 10, 2018 12:57:40.226 AM | Success | host/pxGrid2-PC1... | 00:0C:29:C1:7B:2C | Windows7... | Default >> Dot1X | Default >> Basic_Authenticat... |
| Mar 10, 2018 12:56:38.688 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 1 Select **Log Activity->Add Filter->Parameter->payload contains->Operator->is any of->Value->QRadarAppForPxgrid->"+"**

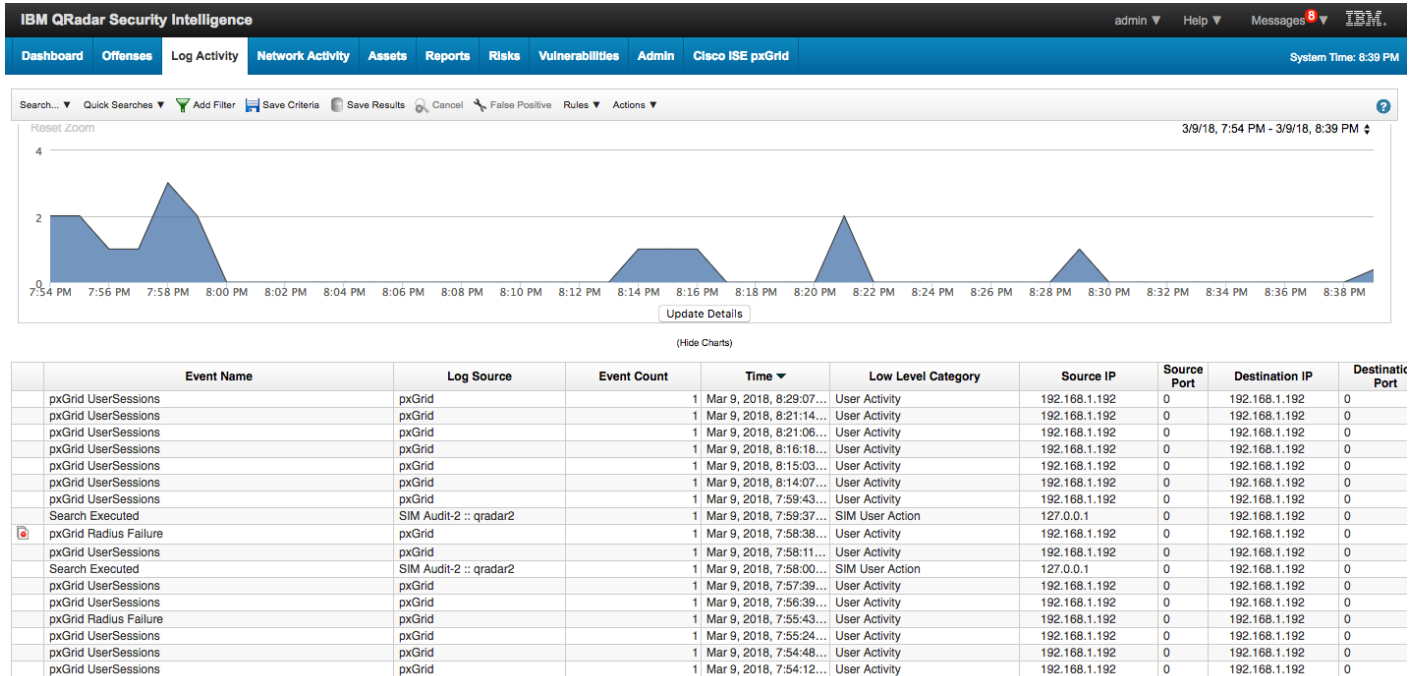
The screenshot shows the IBM QRadar Security Intelligence interface. The 'Log Activity' tab is selected. Below the navigation bar, there are search and filter options. An 'Add Filter' dialog box is open, showing the following configuration:

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

Buttons for 'Add Filter' and 'Cancel' are visible at the bottom of the dialog.

Step 2 Select **Add Filter**

Step 3 Select **View Real Time Events->last interval setting (i.e. 45 minutes)**



Step 4 Click on the offense rule
You will see



Offense 1 (All Categories)

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

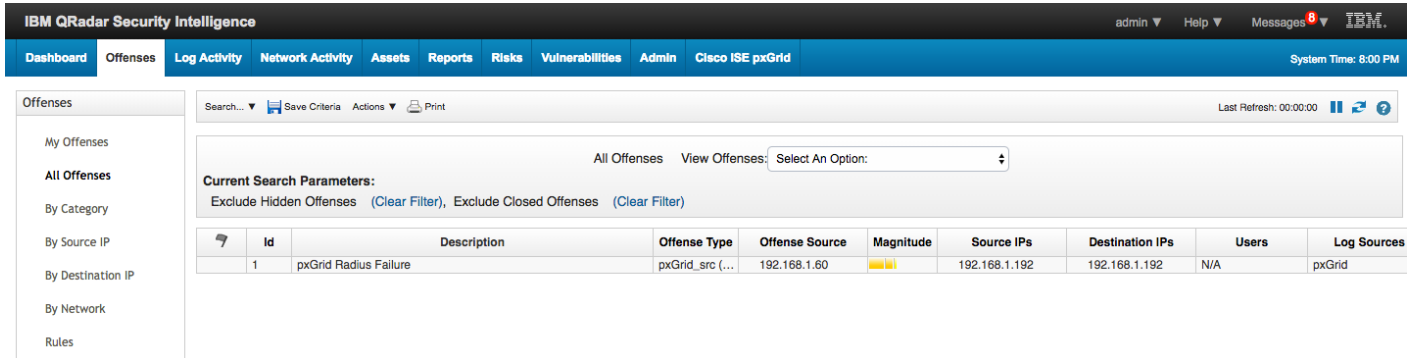
| | | | | | |
|--------------------------|--------------------------------|-------------------------|--------------------------------------|-------------------|----------------------|
| Magnitude | | Status | Relevance 5 | Severity 4 | Credibility 2 |
| Description | pxGrid Radius Failure | Offense Type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

Offense Source Summary

| | | | |
|------------------------------|--------------|---------------------|---|
| Custom property value | 192.168.1.60 | | |
| Offenses | 1 | Events/Flows | 1 |

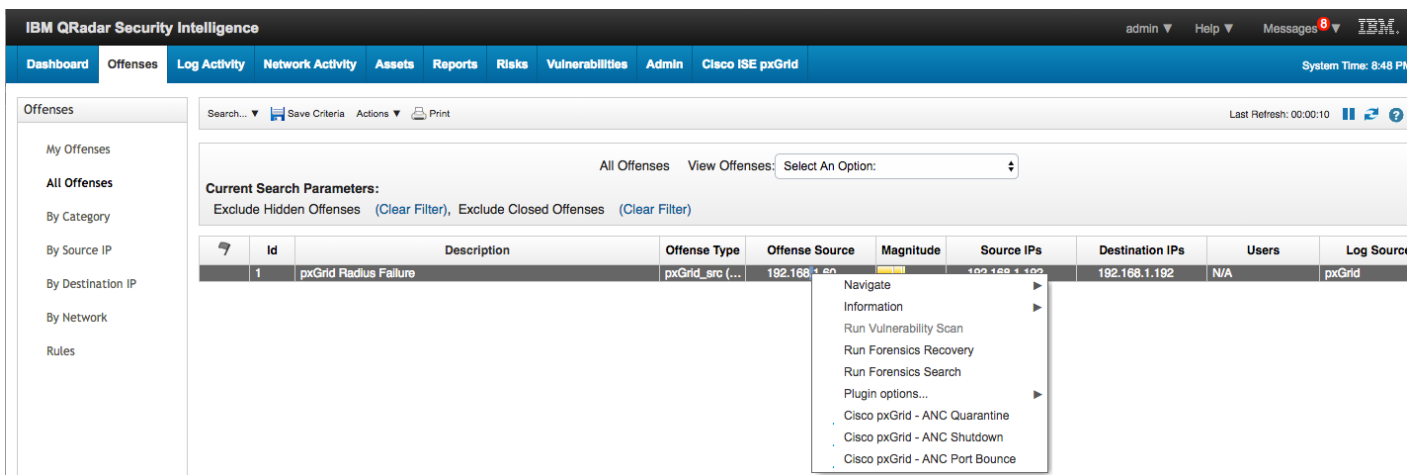
Verify pxGrid offense rule via Offenses Dashboard

Step 1 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 on the IP address, and select the Cisco pxGrid –ANC Quarantine mitigation action.



Step 2 This will trigger the ANC Quarantine, you should see



Step 3 Select **OK**

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

Note the endpoint has been quarantined as designated by the ANCQuarantine 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\pxgrid2 | 00:0C:29:C1:7B:2C | Windows7-... | Default >> Dot1X | Default >> ANCQuarantine | Quarantined. |
| Mar 10, 2018 02:30:00.145 AM | | | | LAB10\pxgrid2 | 00:0C:29:C1:7B:2C | Windows7-... | Default >> Dot1X | Default >> ANCQuarantine | Quarantined. |

Step 5 To unquarantine or clear, select **Operations->Adaptive Network Control->Endpoint Assignment**

Policy List **Endpoint Assignment**

List

Refresh Add Trash Edit EPS unquarantine

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

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

Policy List **Endpoint Assignment**

List

1 Selected

Refresh Add **Trash** Edit EPS unquarantine

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

Step 7 Select->**Selected**

Policy List **Endpoint Assignment**

List

1 Selected

Are you sure you want to delete selected Item(s)?

No Yes

Step 8 Select Yes

Step 9 In ISE, you should see the endpoint has been unquarantined

The screenshot shows the Cisco Identity Services Engine (ISE) dashboard. At the top, there are navigation tabs: Home, Context Visibility, Operations, Policy, Administration, and Work Centers. A notification box says "Click here to do wireless setup and visibility setup Do not show this again." Below the navigation, there are five summary cards: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (12), Client Stopped Responding (5), and Repeat Counter (0). Below these cards is a table of events with columns for Time, Status, Details, Repeat, Identity, Endpoint ID, Endpoint P..., Authentication Policy, Authorization Policy, and Authorizati. Two rows of data are visible, both with a status of 'Success' (green checkmark).

| Time | Status | Details | Repeat | Identity | Endpoint ID | Endpoint P... | Authentication Policy | Authorization Policy | Authorizati. |
|------------------------------|---------|---------|--------|---------------|-------------------|---------------|-----------------------|---------------------------------|--------------|
| Mar 10, 2018 02:39:09.036 AM | Success | | 0 | LAB10\pxgrid2 | 00:0C:29:C1:7B:2C | Windows7... | Default >> Dot1X | Default >> Basic_Authenticat... | PermitAcces |
| Mar 10, 2018 02:39:01.704 AM | Success | | | | 00:0C:29:C1:7B:2C | | | | |

Step 10 Select Dashboard

The screenshot shows the IBM QRadar Security Intelligence dashboard. The top navigation bar includes Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Risks, Vulnerabilities, Admin, and Cisco ISE pxGrid. The main content area is divided into several panels:

- Default-IDS / IPS-All: Top Alarm Signatures:** Shows "There was no Time Series data for the search performed." with a "View in Log Activity" link.
- Top Systems Attacked (IDS/DP/PS):** Shows "There was no Time Series data for the search performed."
- My Offenses:** Shows "No results were returned for this item." Below this are sections for "Most Severe Offenses" and "Most Recent Offenses", both containing a table with columns for "Offense Name" and "Magnitude". The only entry in both is "pxGrid Radius Failure".
- Top Services Denied through Firewalls:** Shows "There was no Time Series data for the search performed."
- Flow Bias:** Shows "There was no Time Series data for the search performed." with a "View in Network Activity" link.
- Top Category Types:** A table showing categories and their corresponding offense counts.

| Category | Offenses |
|-------------------|----------|
| User Activity | 1 |
| Object Not Cached | 0 |
| Rate Limiting | 0 |
| No Rate Limiting | 0 |
| Object Cached | 0 |
- Top Sources:** A table showing sources and their corresponding offense counts.

| Source | Offenses |
|---------------|----------|
| 192.168.1.192 | 1 |

- 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_src (...) | 192.168.1.60 | High | 192.168.1.192 | 192.168.1.192 | N/A | pxGrid |

Network: Net-10-172-192-Net_192_168_0_0

pxGrid Session details: User Name: LAB10pxgrid2
 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

Appendices

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 filename.

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

Cisco ISE pxGrid Dashboards not populating with ISE Contextual Information

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

ANC Mitigation Actions not appearing in Dashboards

Ensure you have the following ISE policies created:

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