Cisco ISE pxGrid App 1.0 for IBM QRadar SIEM

Author: John Eppich

Table of Contents

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

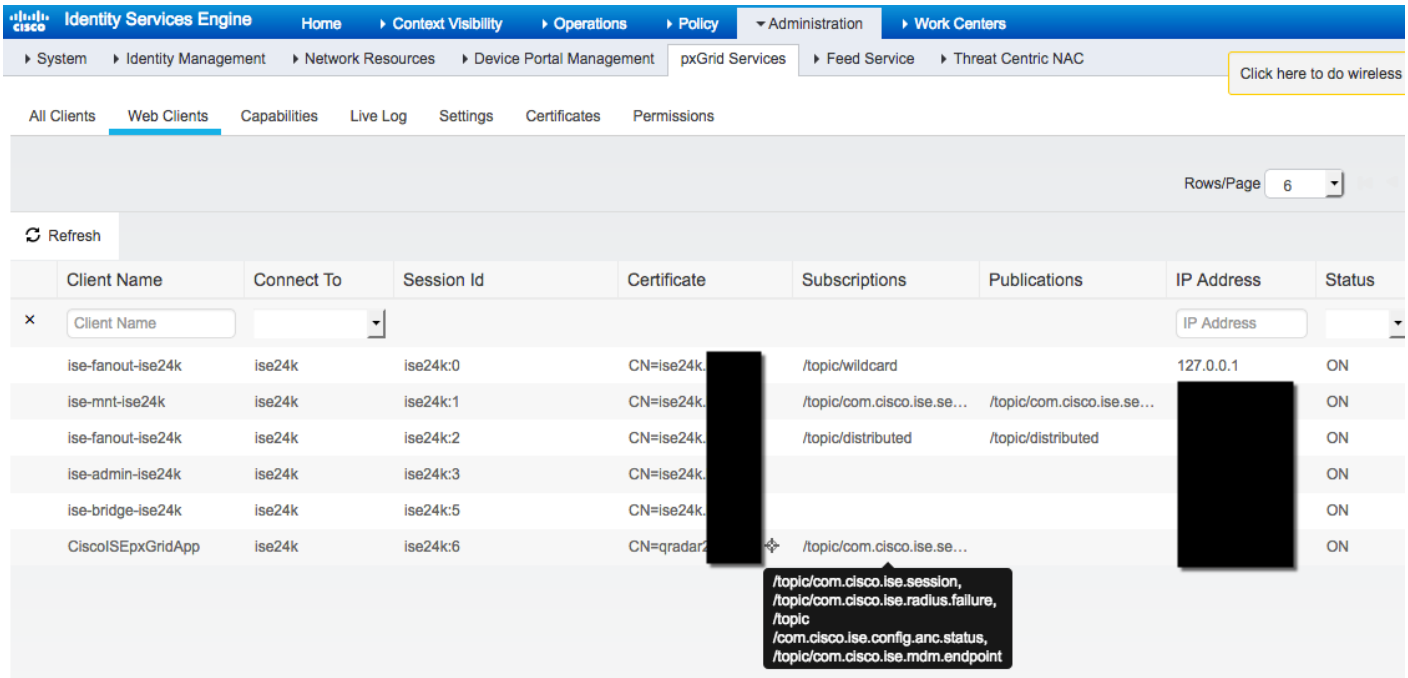
IBM® QRadar® SIEM detects anomalies, uncovers advanced threats and removes false positives. It consolidates log events and network flow data from thousands of devices, endpoints and applications distributed throughout a network. It then uses an advanced Sense Analytics engine to normalize and correlate 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, gust 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.



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.

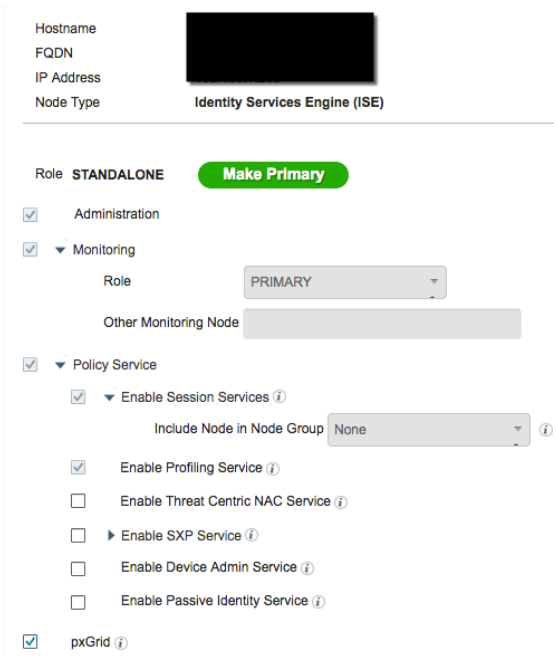
The Config ANC Status Topic provides the Cisco ISE pxGrid client app to perform ISE Adaptive Network Control (ANC) mitigation actions on the endpoints.

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.

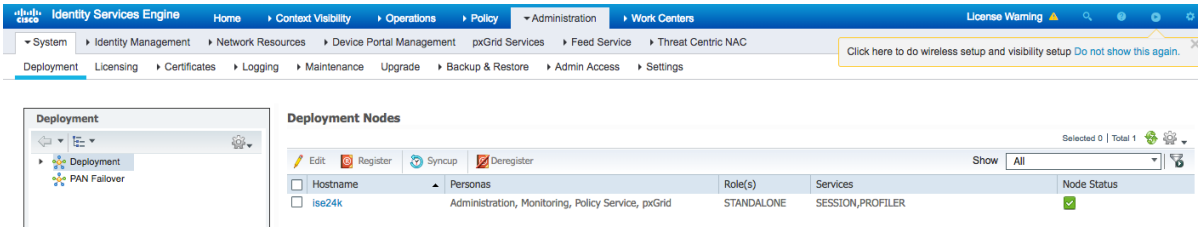
Cisco ISE pxGrid Installation

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

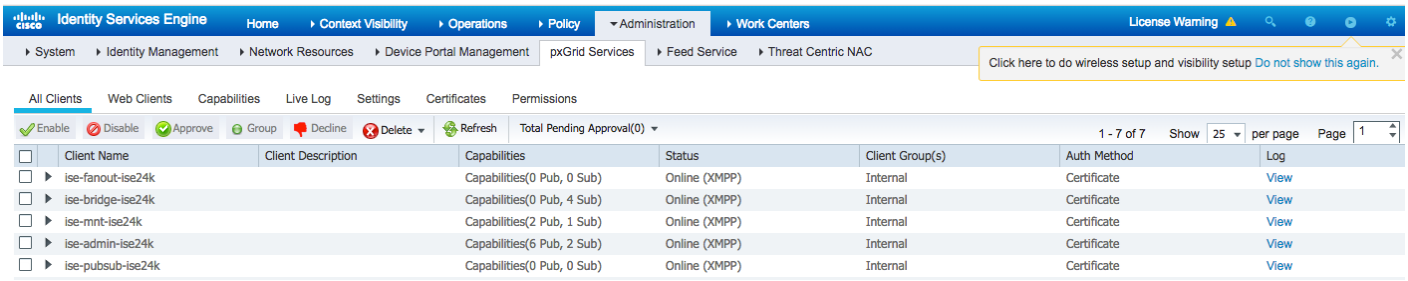
Step 1 Select **Administration->System Deployment->edit the ISE node->Enable pxGrid**



Step 2 Select **Save**
You should see:

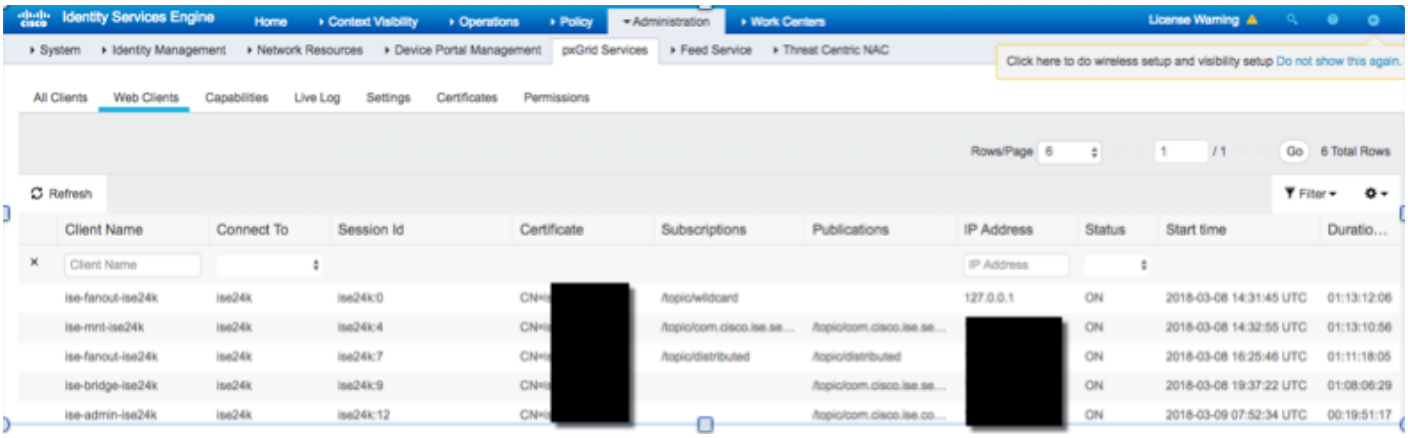


Step 3 Select **Administration->pxGrid Services**
Verify the published nodes appear



and you have connectivity

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

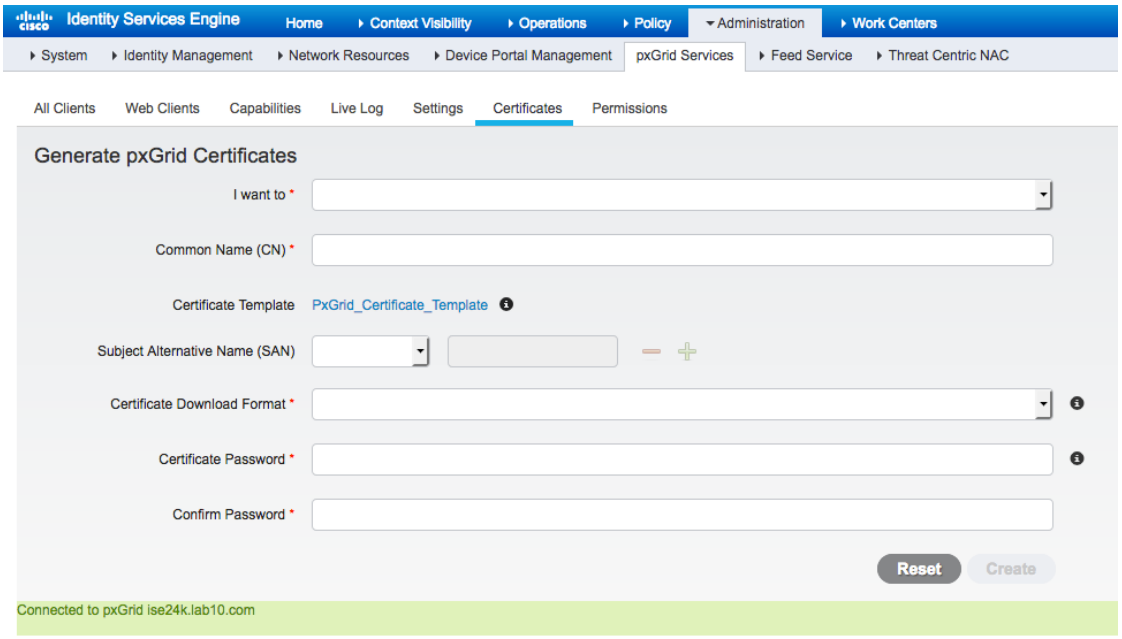


Generating the Cisco ISE pxGrid App Certificate

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

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:



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:

```
CertificaeServicesEndpointSubCA-ise24k_.cer
CertificateServicesNodeCA-is24k_.cer
CertificateServicesRootCA-ise24k_.cer
ise24k.[redacted]cer
qradar.lab10.com_qradar.[redacted].cer
qradar.lab10.com_qradar.[redacted].key
```

The Qradar identity certificate consists of the public private key-pair: qradar.[redacted]_qradar.[redacted].cer and qradar.[redacted]_qradar.[redacted].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.[redacted]_qradar.[redacted].key qradar.lab10.com_qradar.[redacted].key.org
openssl rsa –in qradar.[redacted].com.key.org cp –out qradar.[redacted].com.key
(you will be prompted to enter the encryption password when generating the certificate in ISE)
```

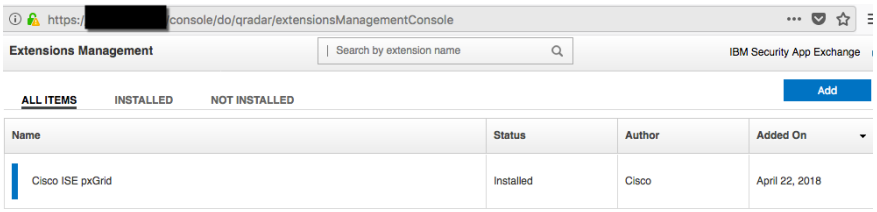
Step 6 You will need to upload these 6 certificates when configuring the Cisco ISE pxGrid App for pxGrid integration.

Installing Cisco ISE pxGrid App

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

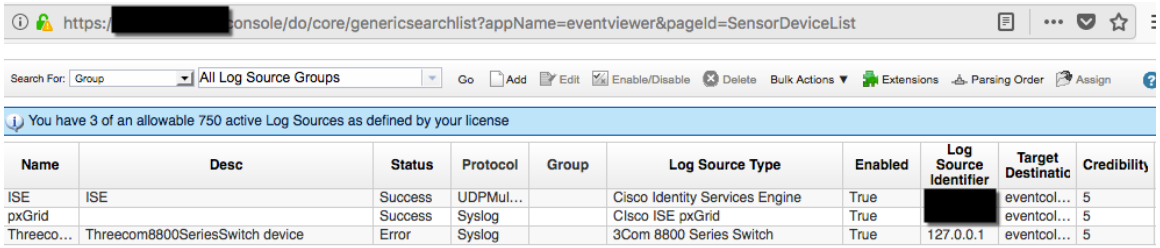
Note: It is assumed that QRadar ver 7.28 has been installed along with Patch 9 (http://www-01.ibm.com/support/docview.wss?uid=swg27050133)

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:

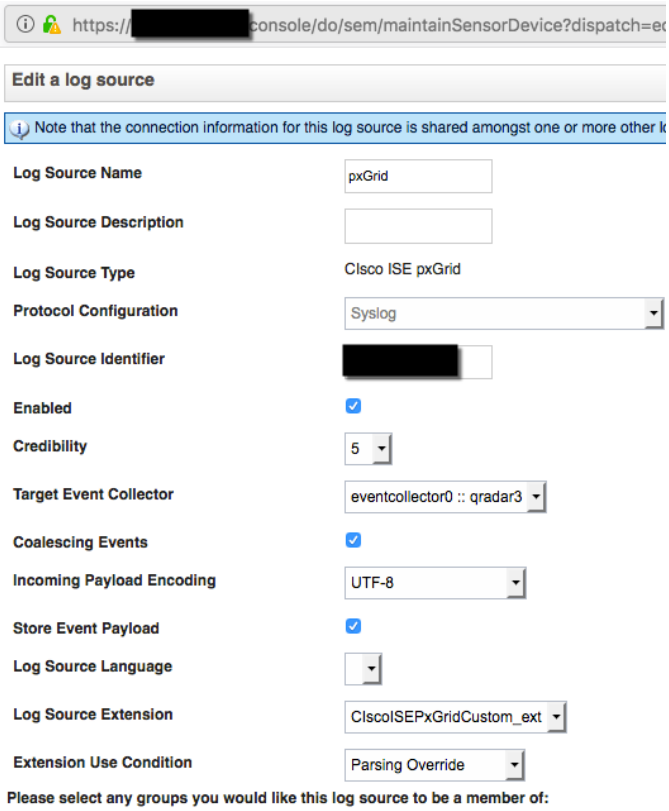


Step 2 Refresh the browser

Step 3 **Double-Click Admin->Log Sources->Name->pxGrid**



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



Step 5 Select **Save**

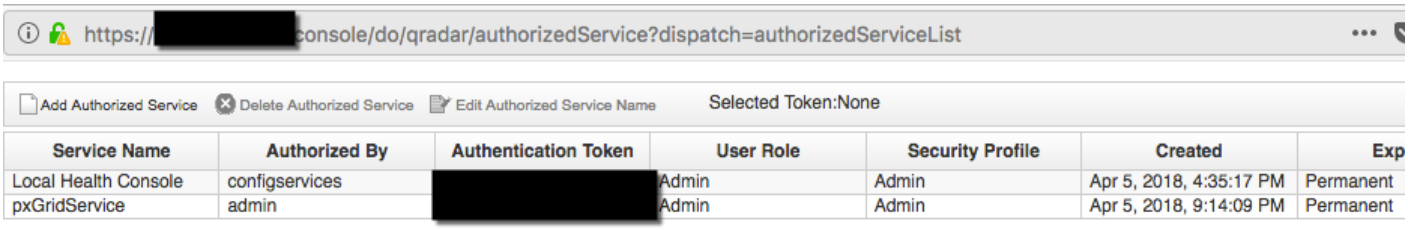
Step 6 Select **Admin->Authorized Services->Add Authorized Service->**type: **pxGridService** for the **Service name**:

Step 7 Select **Admin** for both the **User Role** and **Security Profile** drop-downs

Step 8 Enable **No** for Expiry

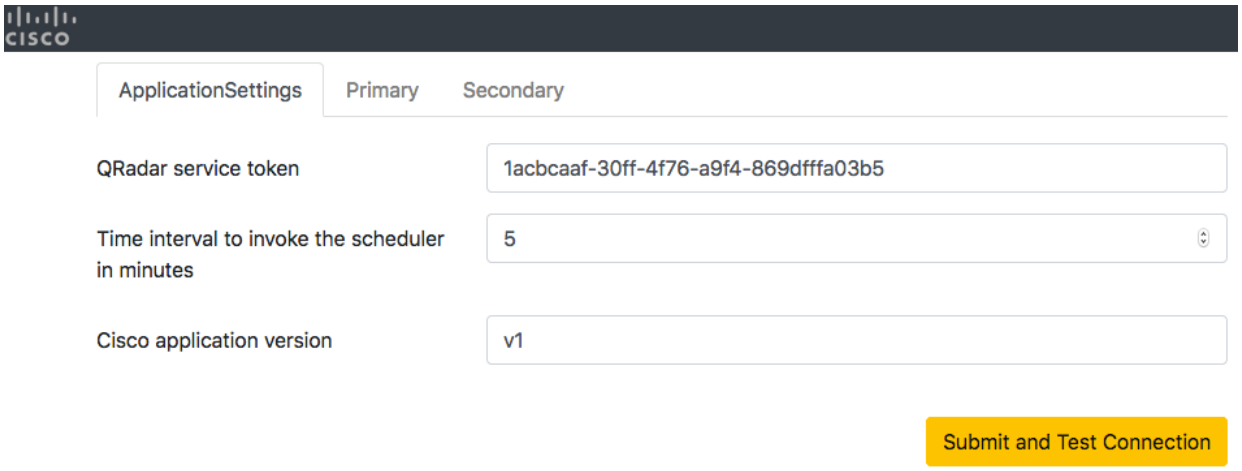
Step 9 Select **Create Service**

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.



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**



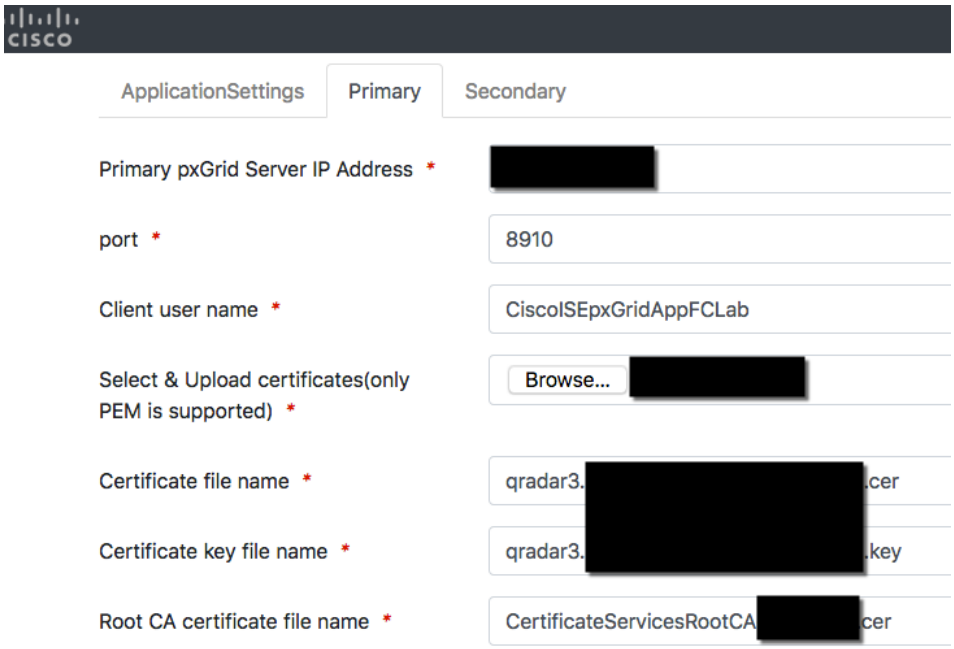
Step 2 Select **Submit and Test Connection,** you should see a successful connection.
Step 3 Select **Primary,** and type the **IP address** of the ISE pxGrid node
Step 4 Leave **8910**, as the port default
Step 5 Enter the **Client user name (i.e. Augas0221)**

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)**

```
CertificaeServicesEndpointSubCA-ise24k_.cer
CertificateServicesNodeCA-is24k_.cer
CertificateServicesRootCA-ise24k_.cer
ise24k.[redacted]cer
qradar.lab10.com_qradar.[redacted].cer
qradar.lab10.com_qradar.[redacted].key
```

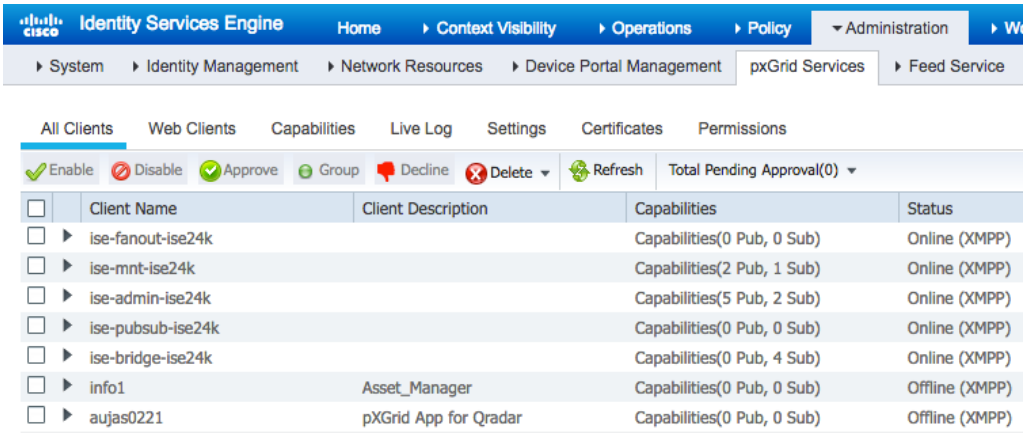
Step 7 Type in the Cisco ISE pxGrid App Certificate file name**: qradar.[redacted]_qradar.[redacted].cer**
Step 8 Type in the Cisco ISE pxGrid App Certificate key file name: **qradar.[redacted].key**
Step 9 Type in the Cisco ISE Internal Root Certificate Root CA certificate file name: **CertificateServicesRootCA-ise24k_.cer**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



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.

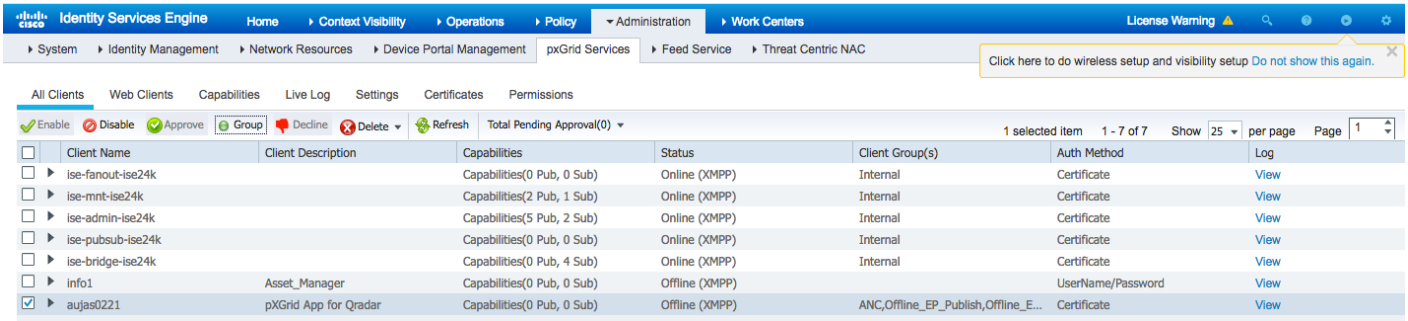


Step 13 Select **Web Clients,** you will see registered Cisco ISE pxGrid QRadar app client Aujas 0221

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



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 polices 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.

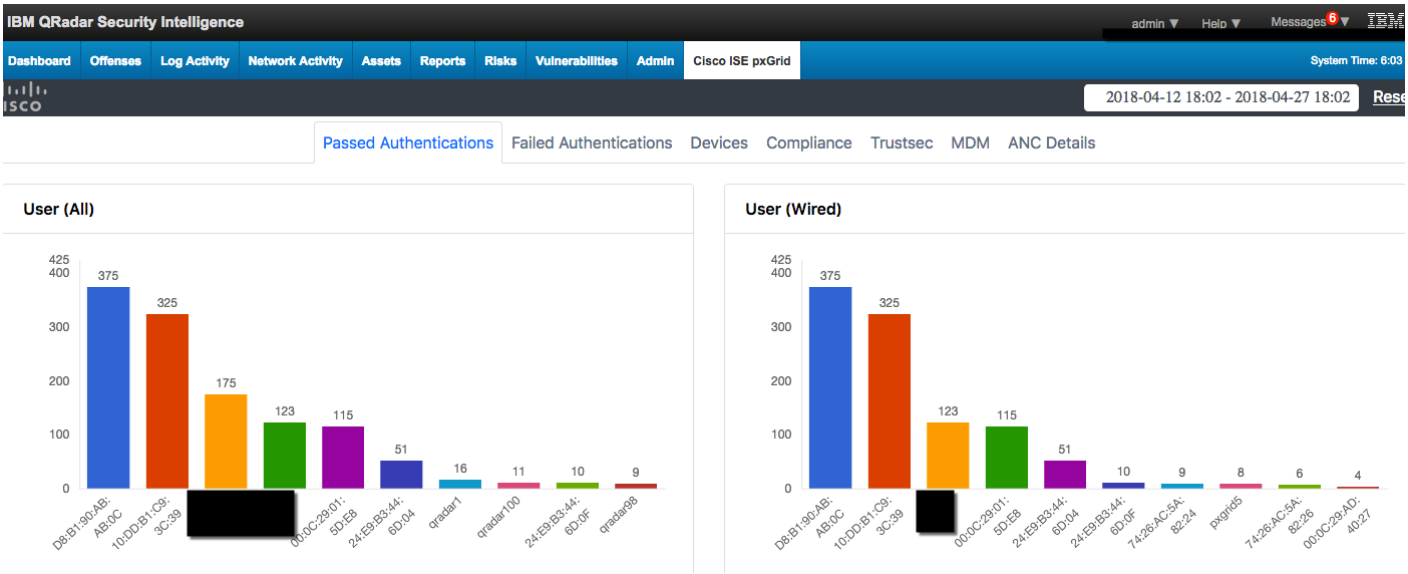
Passed Authentications

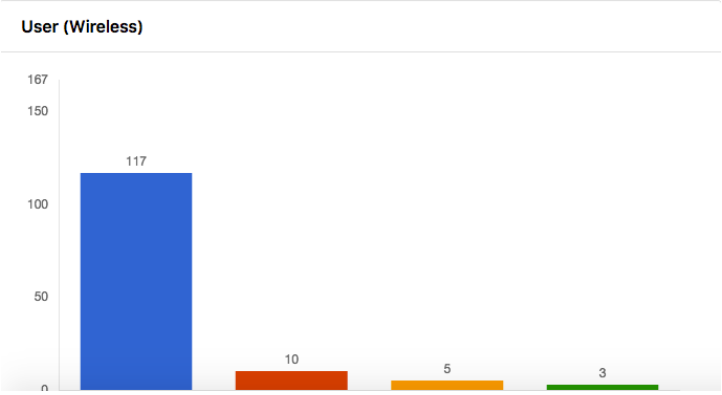
The Passed Authentications Dashboard View provides visibility into successful machine and user authentications across an organization and by wired and wireless connection type. This provides the admin with a view of how employees are connecting to the network, are they connecting over a wired or wireless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

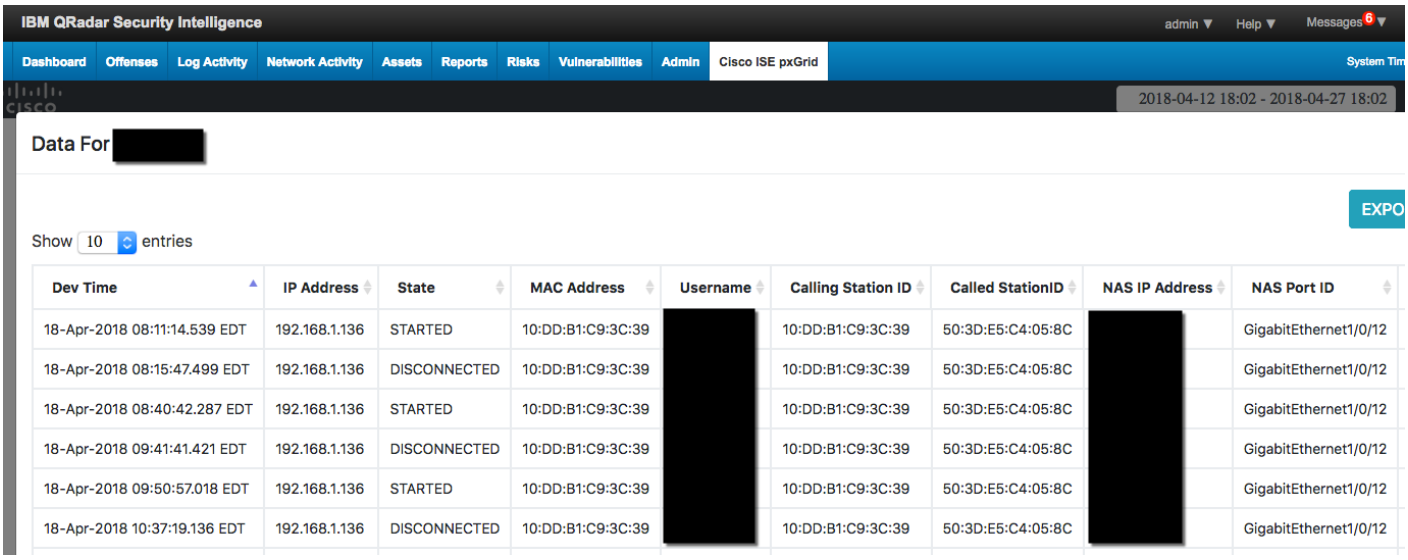
The AD resolvable user and host identities provide a consistent name format when different EAP methods are used, i.e. EAP Chaining.

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



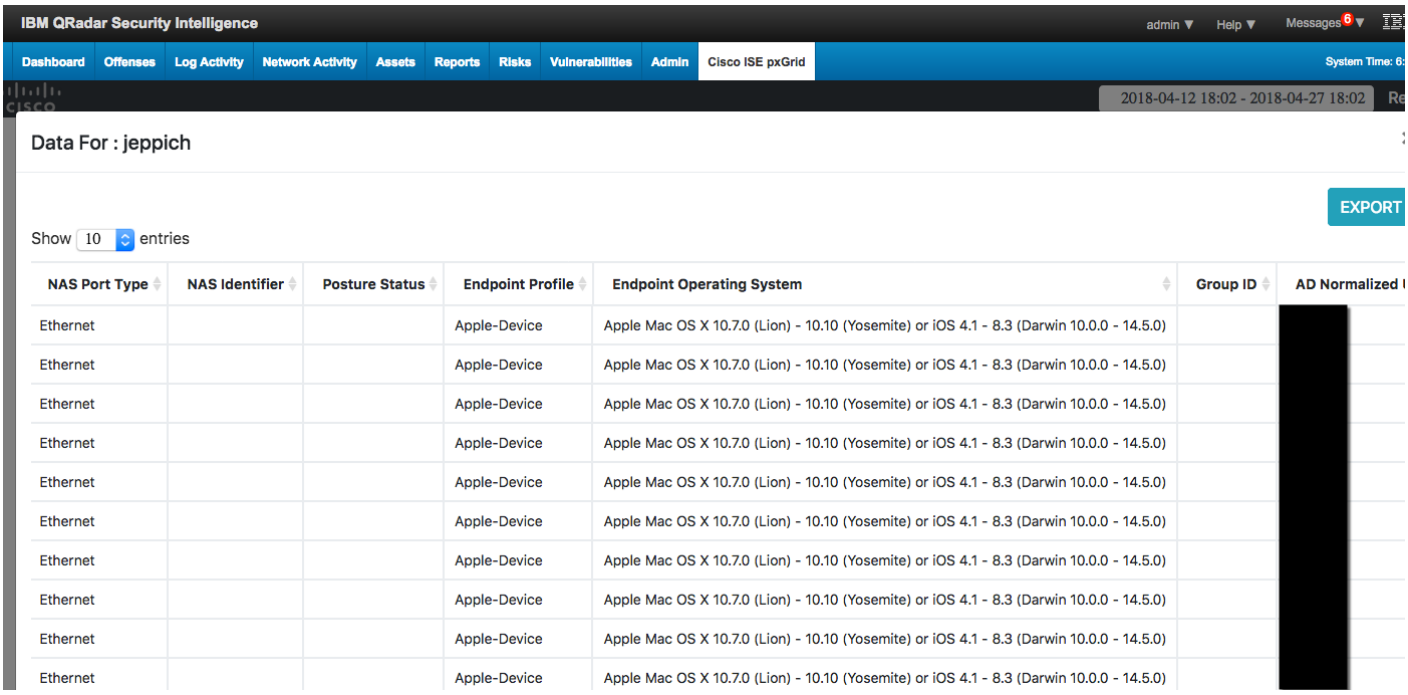


Step 2 Select an **end-user**, this provides a tabular view of the following contextual information:



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

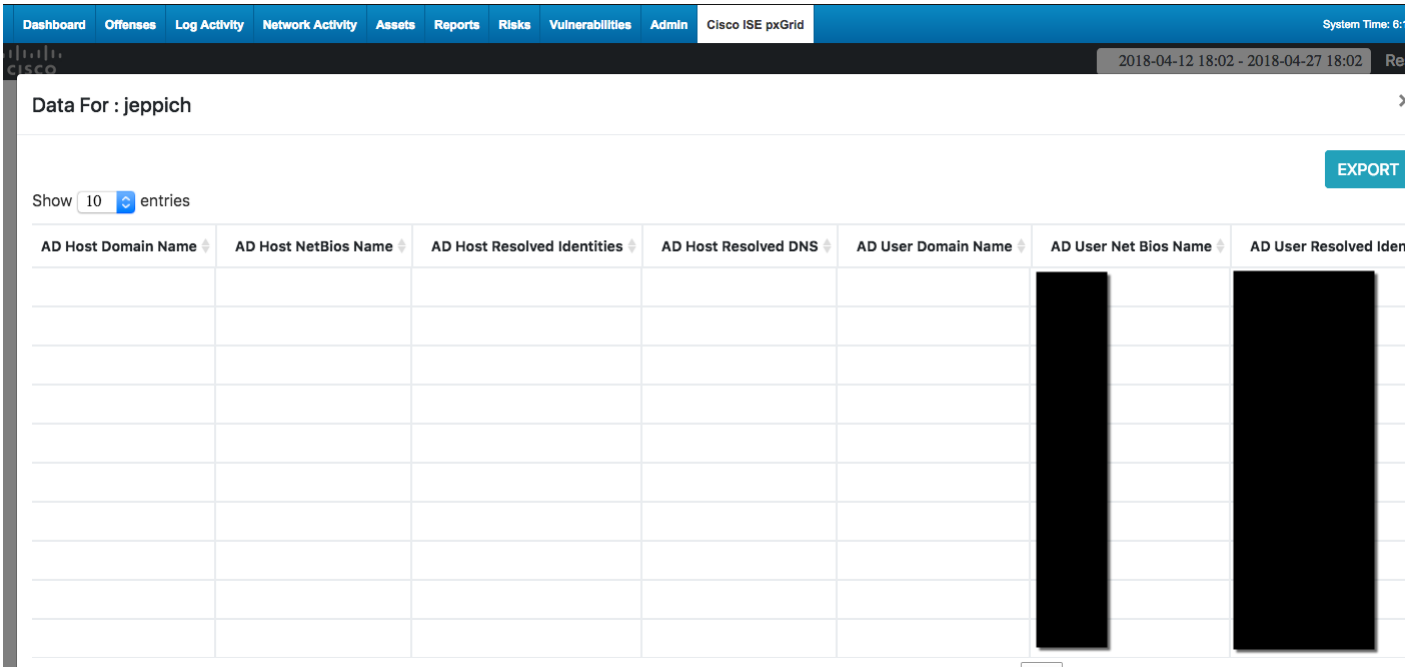
The **Endpoint Profile, Endpoint Operating System** and the **AD Normalized User Name** provide the endpoint information for the user.



Data For : jeppich

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

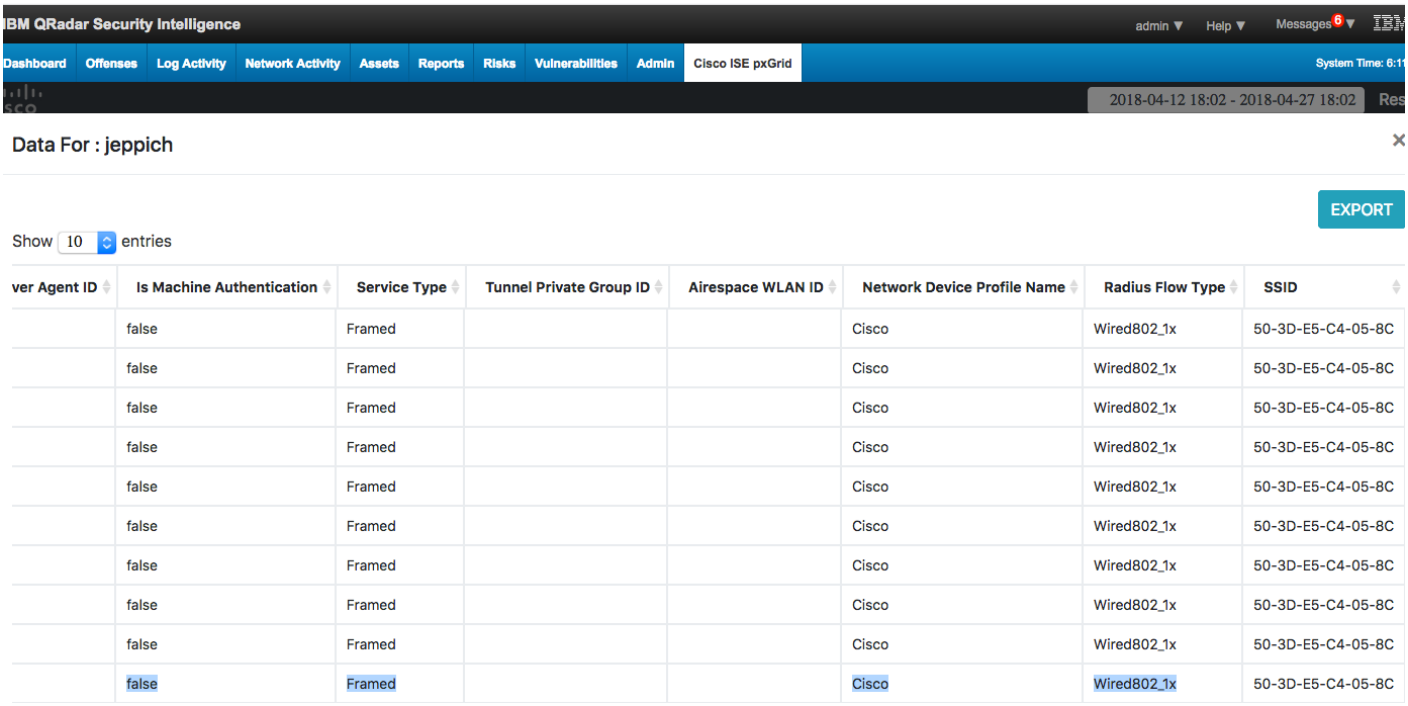
The **AD user Resolved Identities** and **AD User Resolved DNS** provides the consistent identities of the end-user.



Data For : jeppich

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 Iden
					[redacted]	[redacted]
					[redacted]	[redacted]
					[redacted]	[redacted]
					[redacted]	[redacted]
					[redacted]	[redacted]
					[redacted]	[redacted]
					[redacted]	[redacted]
					[redacted]	[redacted]
					[redacted]	[redacted]
					[redacted]	[redacted]

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.



Data For : jeppich

Show 10 entries

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

Failed Authentications

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

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

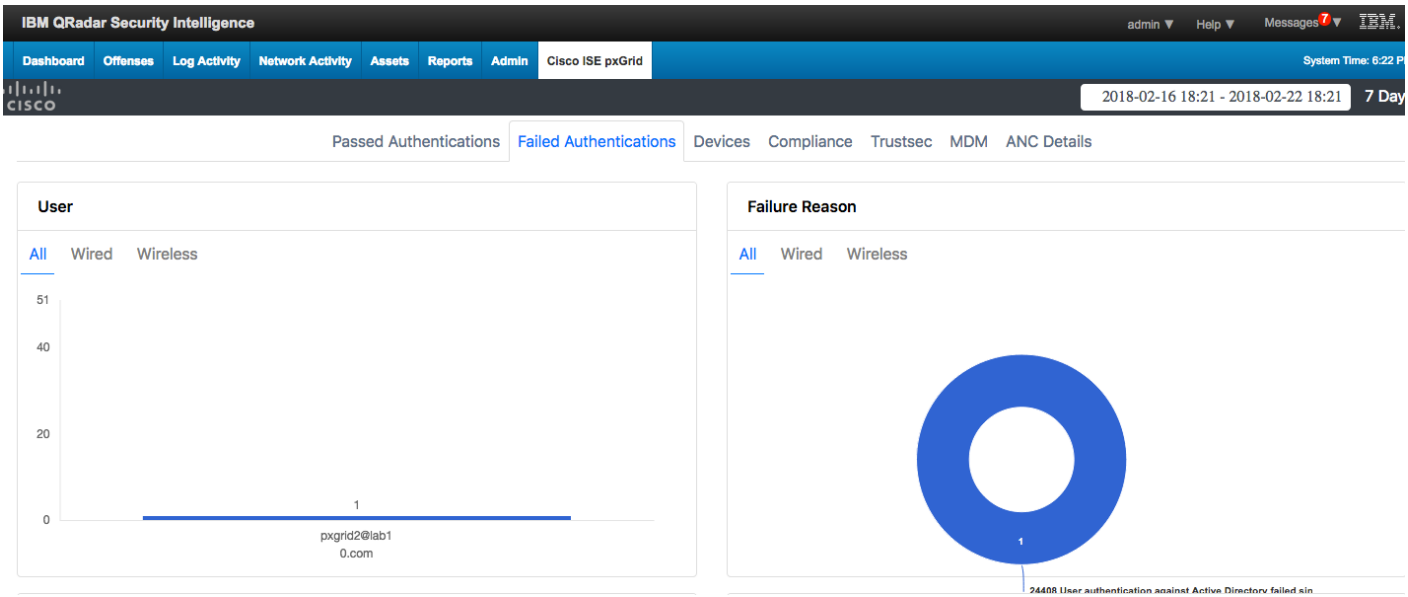
The other panels provide a breakdown by failure reason, device type and location and provide the admin insight to how these failed authentications occur. The same contextual information from the user panel is available in these panel breakdowns.

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

User Panel

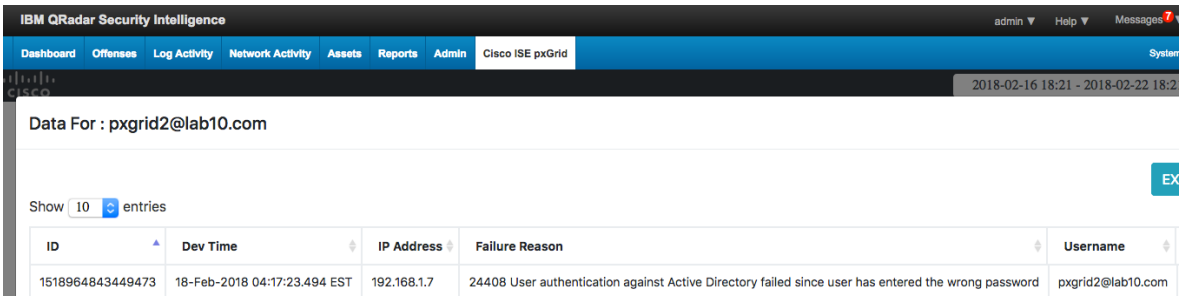
The user panel provides a breakdown by username

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

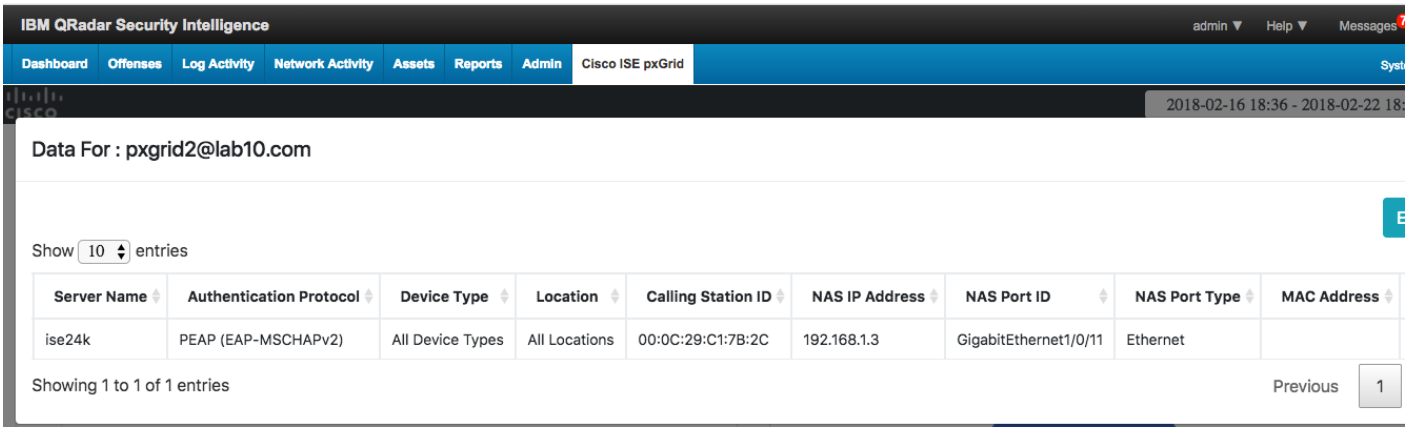


Step 2 Select **Cisco ISE pxGrid->Failed Authentications->User-> pxGrid2@[redacted]**

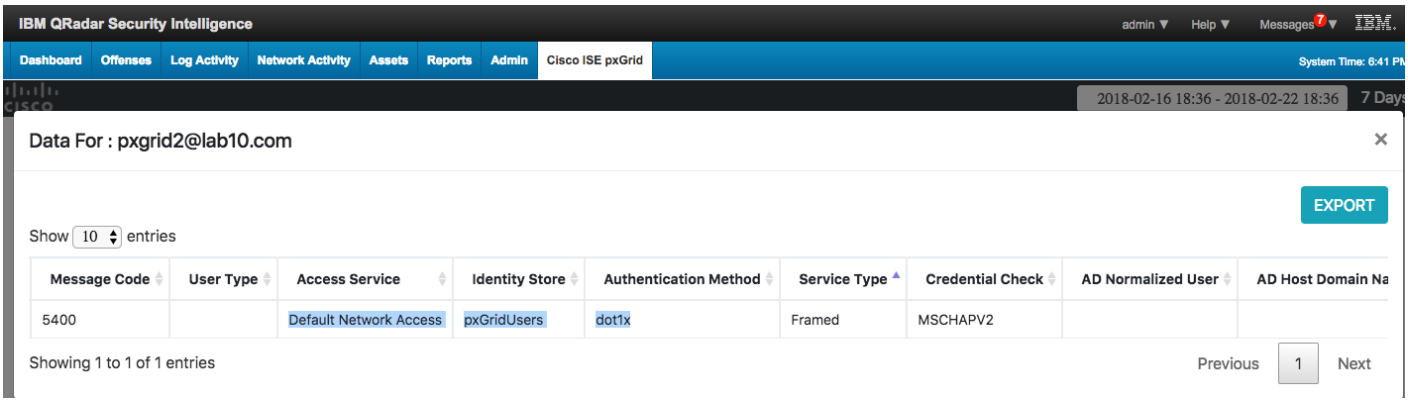
The **IP Address**, **Failure Reason, Username** attributes provide information into failed authentication attempts.



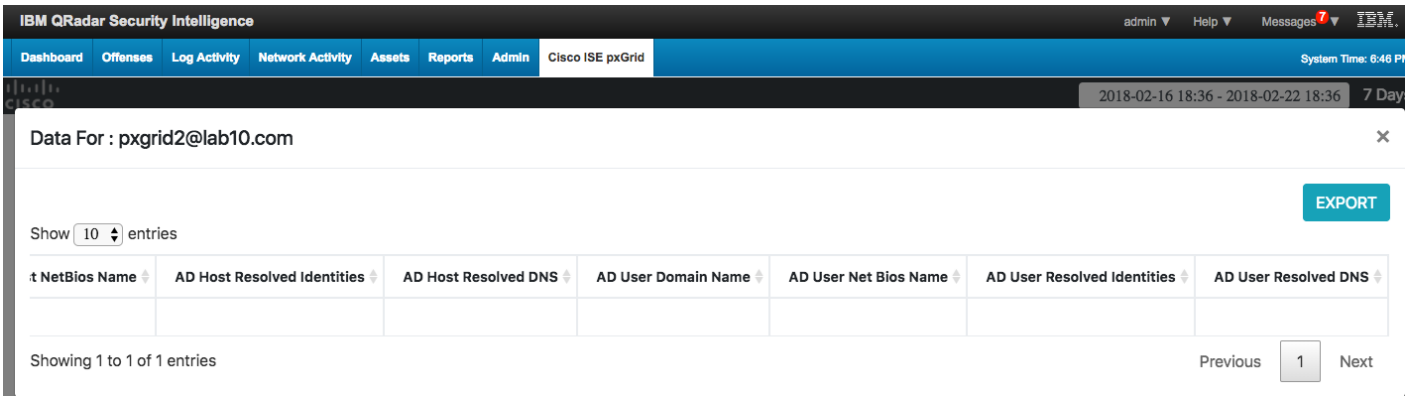
The **Server Name, Authentication Protocol, Device Type, Location, Calling Station ID**, NAS **IP Address, NAS Port ID, NAS Port Type** attributes provide more authentication details and location information of failed authentication attempts.

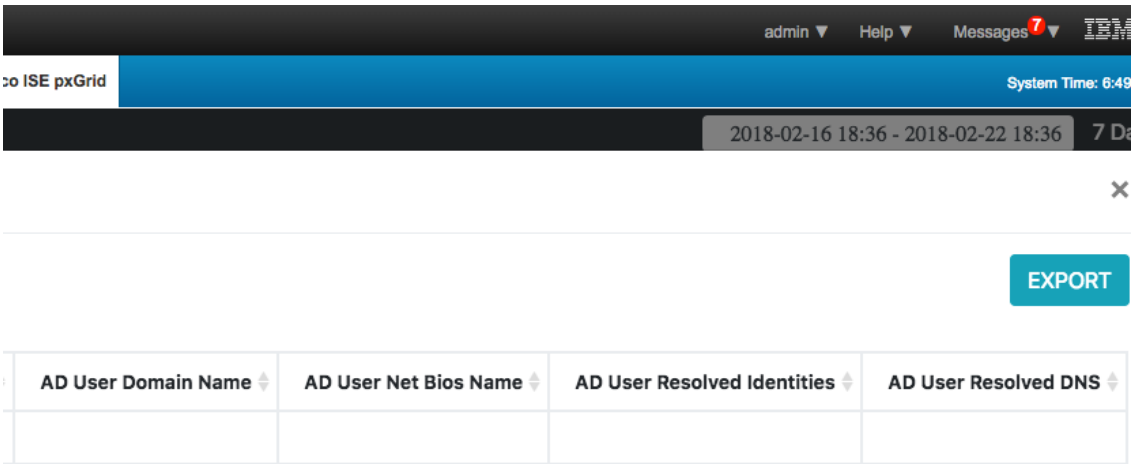


The **Access Service** attribute provide the ISE allowed protocol rules, the **Identity Store** attribute provides the back-end credential database of the end-user in question, the **Authentication Method** attribute provides the ISE authentication rule, and the **Credit Check** attribute provides the EAP authentication method



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.



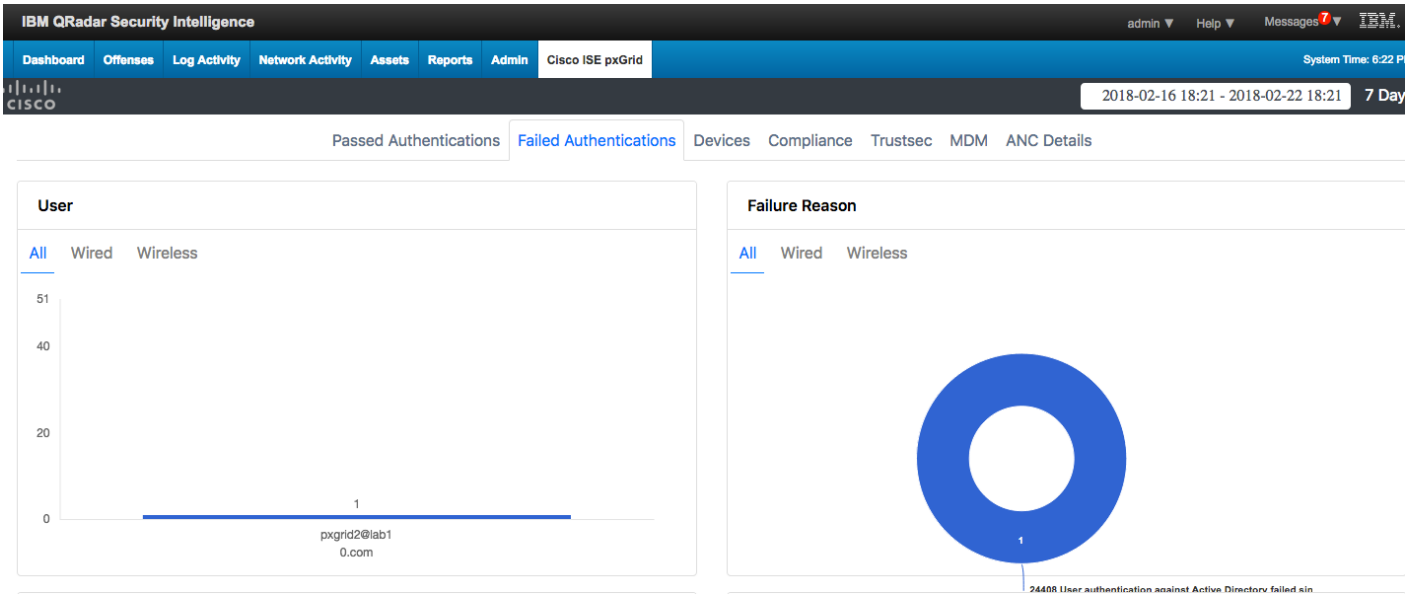


Failure Reason Panel

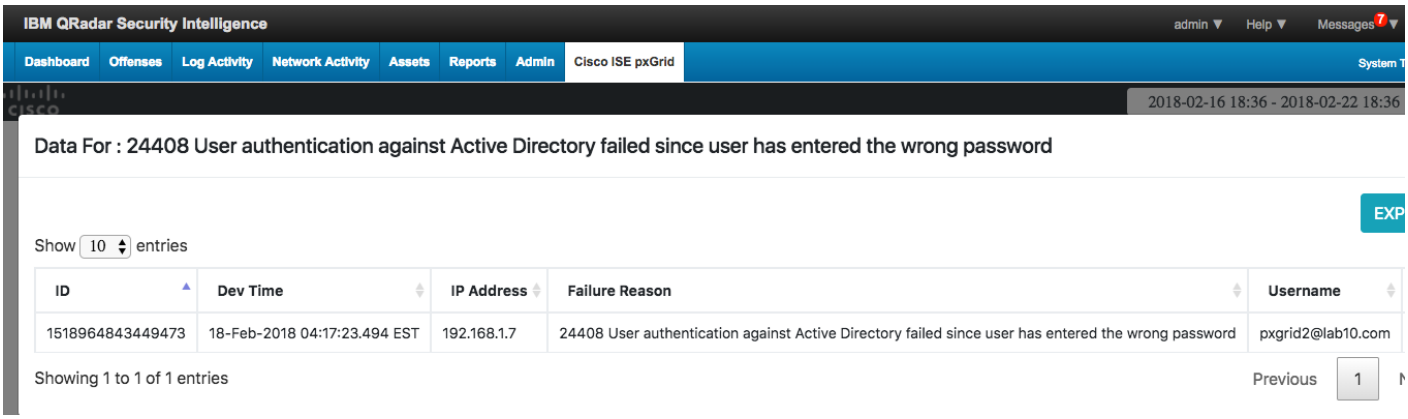
The failure reason panel provides a breakdown by failure reason

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

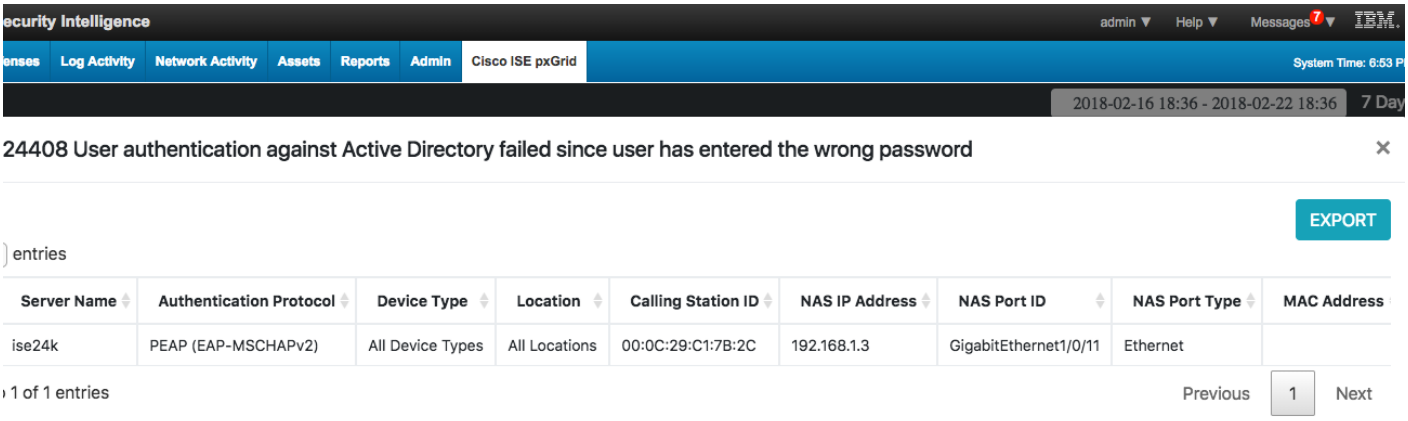
Step 2 Select **Failure Reason->24408 User authentication against Active Directory failed since user has entered the wrong password**



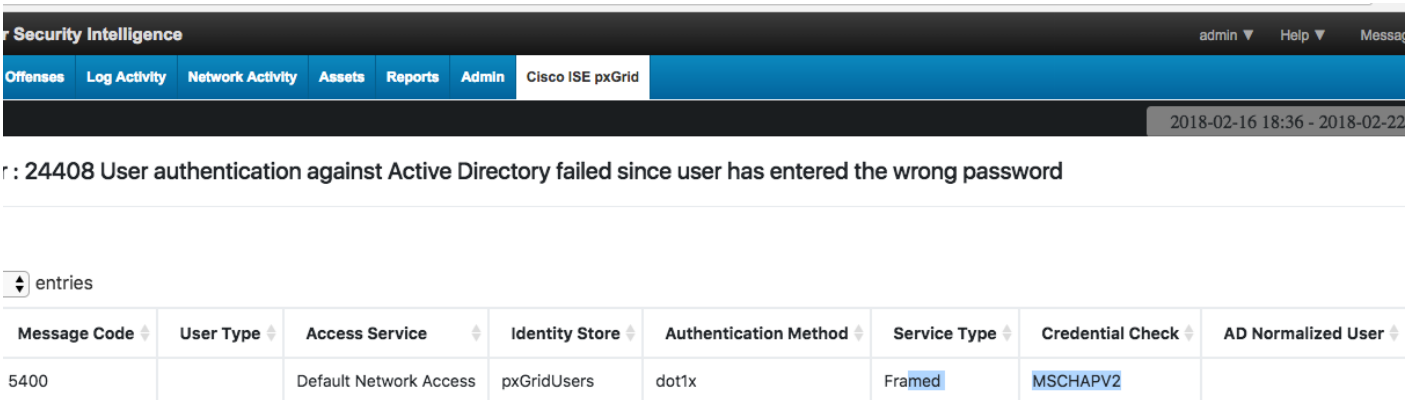
The **IP Address**, **Calling Station ID**, Username attributes, provide basic information for end-users associated with failure reasons



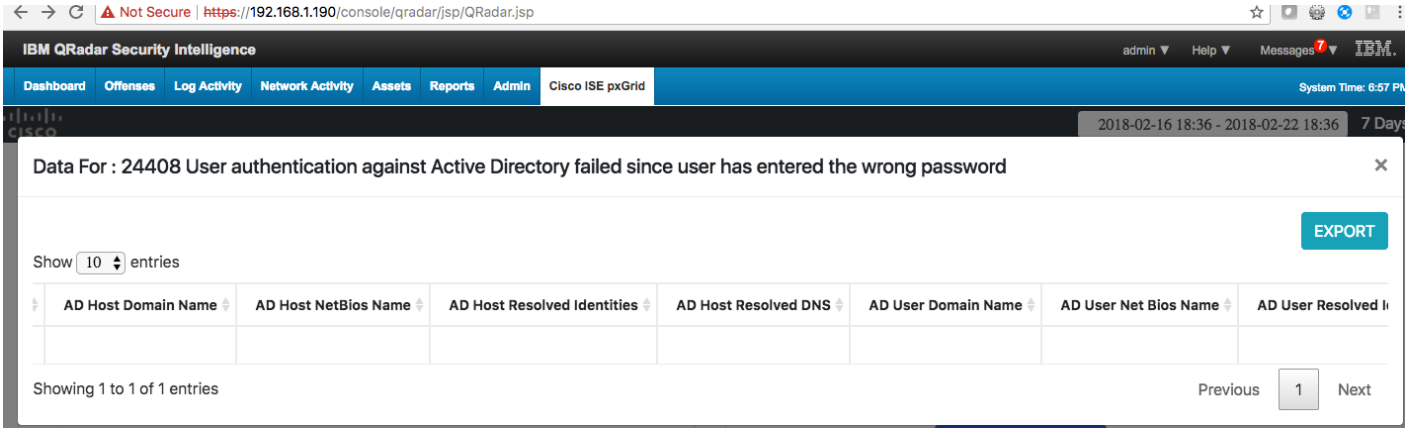
The **Server Name, Authentication Protocol, Device Type, Location, Calling Station ID**, NAS **IP Address, NAS Port ID, NAS Port Type** attributes provide more authentication details and location information of failed authentication attempts.



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



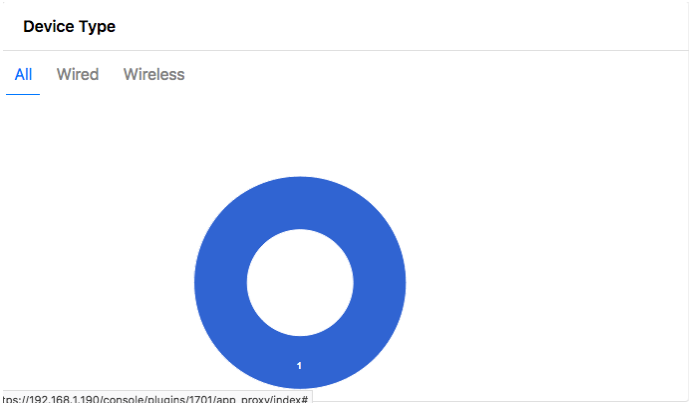
The **AD Host/User Resolved Identities, AD Host/User Resolved DNS, AD User Domain, AD User Net BIOS Name Host** attributes in the following screenshots provide additional context around the host and user identities.



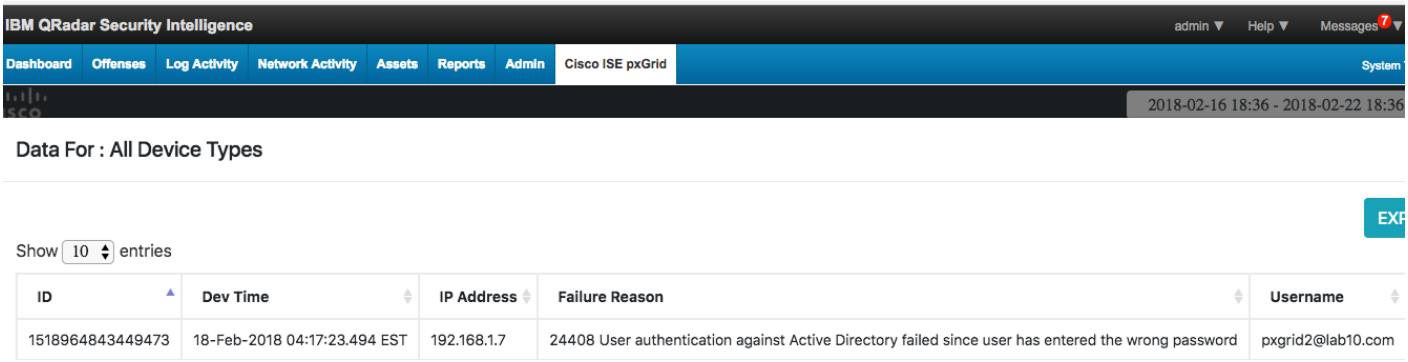
Device Type Panel

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**

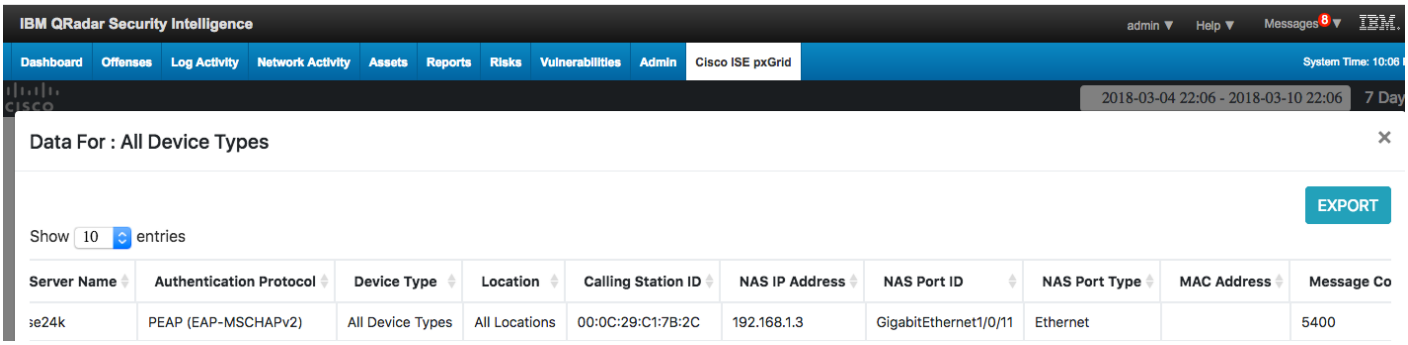


The **IP Address**, **Calling Station ID**, Username attributes, provide basic information for end-users associated with failure reasons



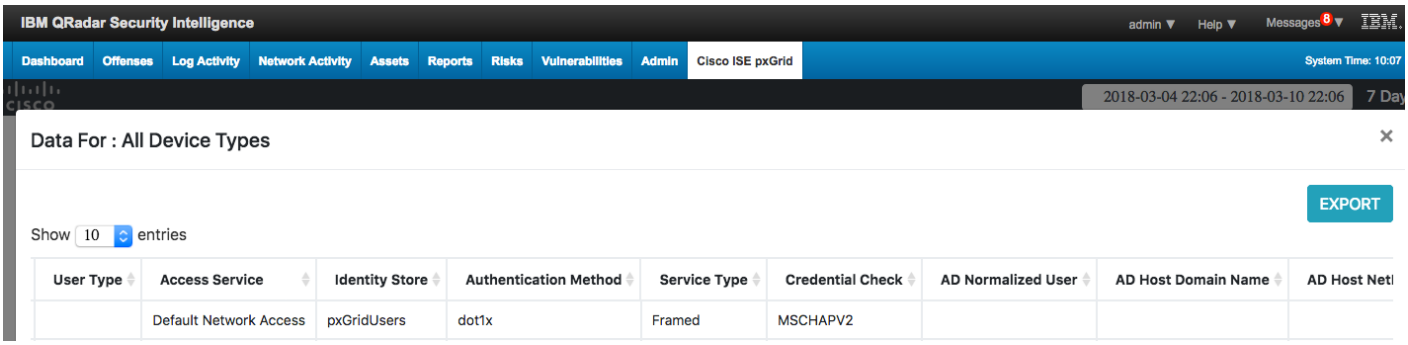
ID	Dev Time	IP Address	Failure Reason	Username
1518964843449473	18-Feb-2018 04:17:23.494 EST	192.168.1.7	24408 User authentication against Active Directory failed since user has entered the wrong password	pxgrid2@lab10.com

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



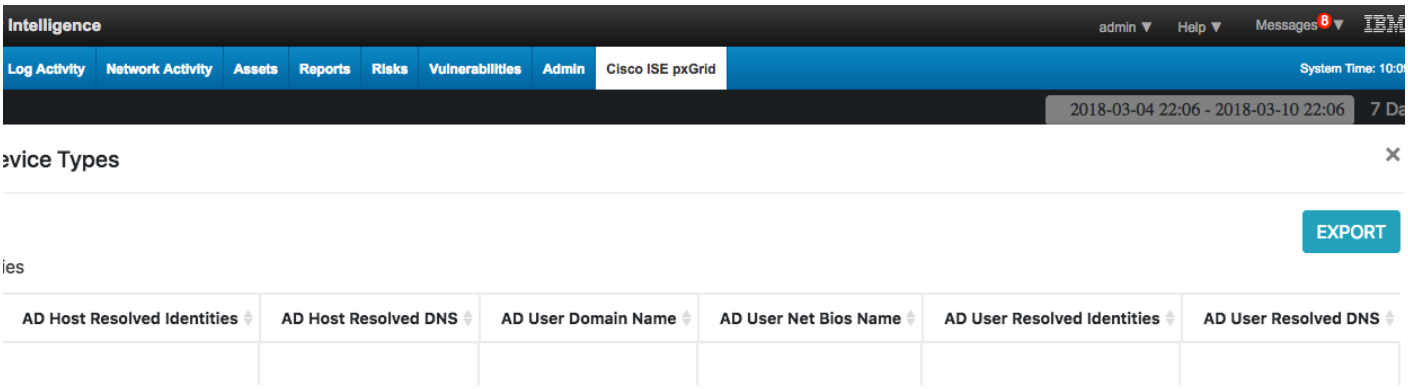
Server Name	Authentication Protocol	Device Type	Location	Calling Station ID	NAS IP Address	NAS Port ID	NAS Port Type	MAC Address	Message Co
se24k	PEAP (EAP-MSCHAPv2)	All Device Types	All Locations	00:0C:29:C1:7B:2C	192.168.1.3	GigabitEthernet1/0/11	Ethernet		5400

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



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

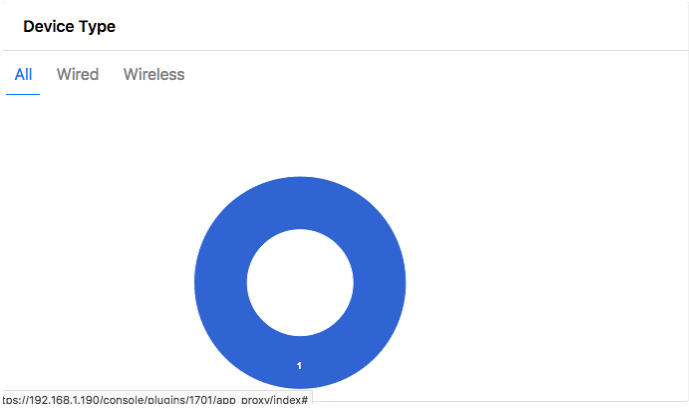
The **AD Host/User Resolved Identities, AD Host/User Resolved DNS, AD User Domain, AD User Net BIOS Name Host** attributes in the following screenshots provide additional context around the host and user identities

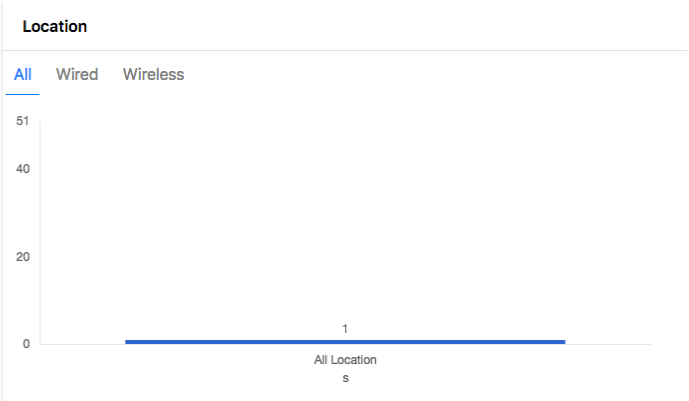


Locations Panel

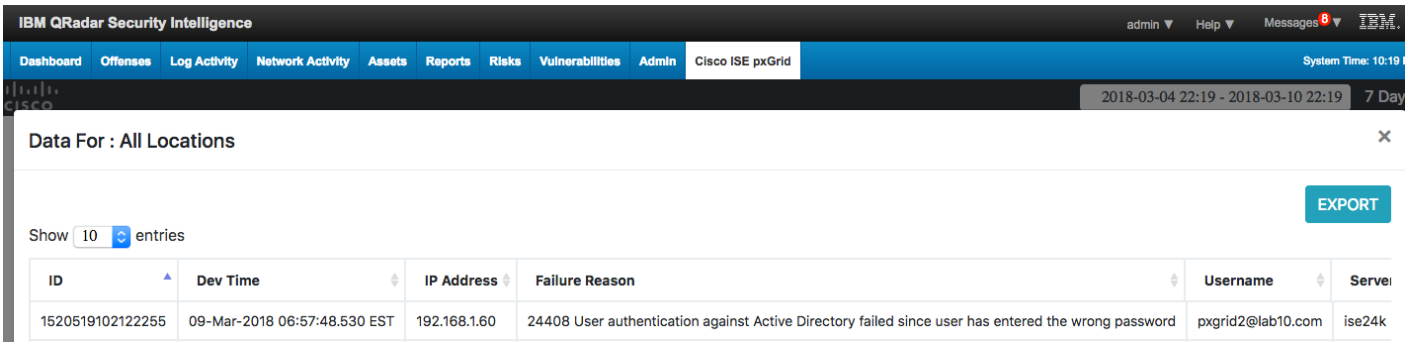
The location panel provides insight into attempted by failures by NAD location type and provides a drill-down based on Locations

Step 1 Select **Cisco ISE pxGrid->Failed Authentications**
Step 2 Select **Location->All->All Location**

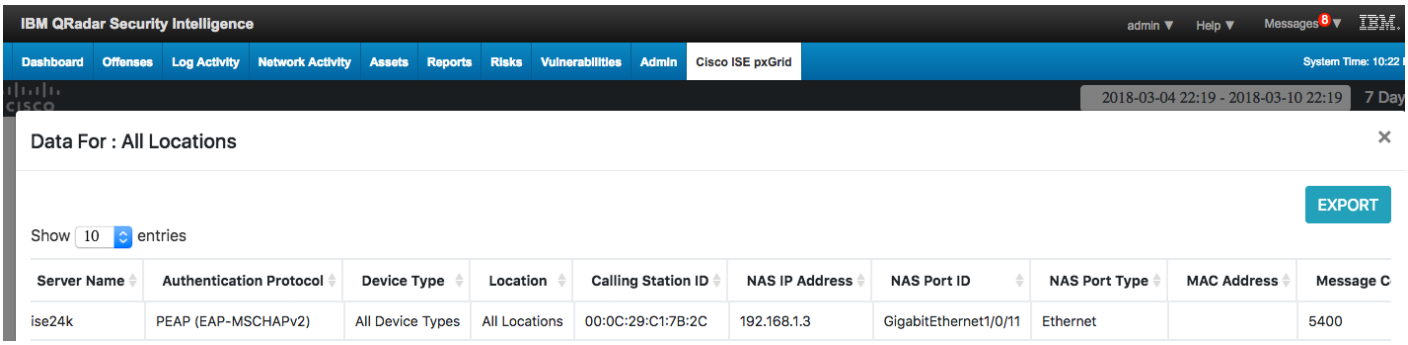




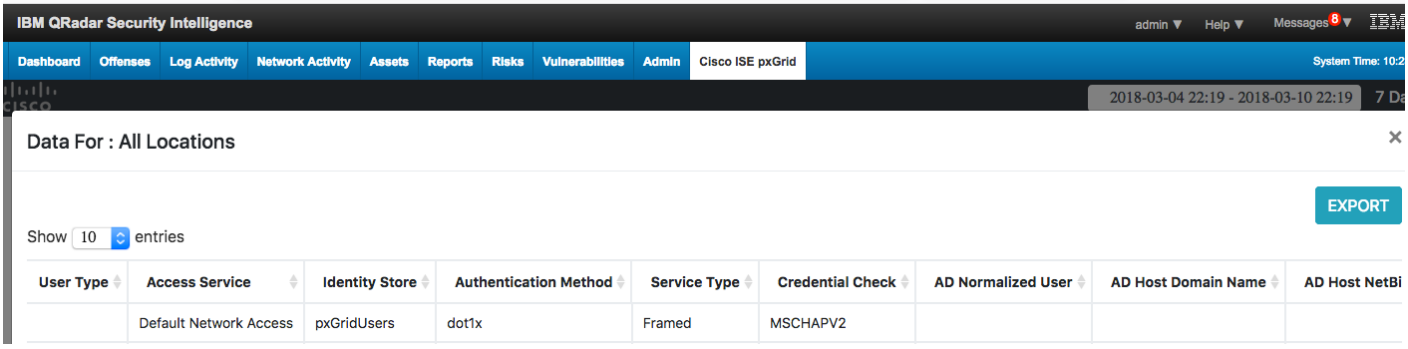
The **IP Address**, **Calling Station ID**, Username attributes, provide basic information for end-users associated with failure reasons

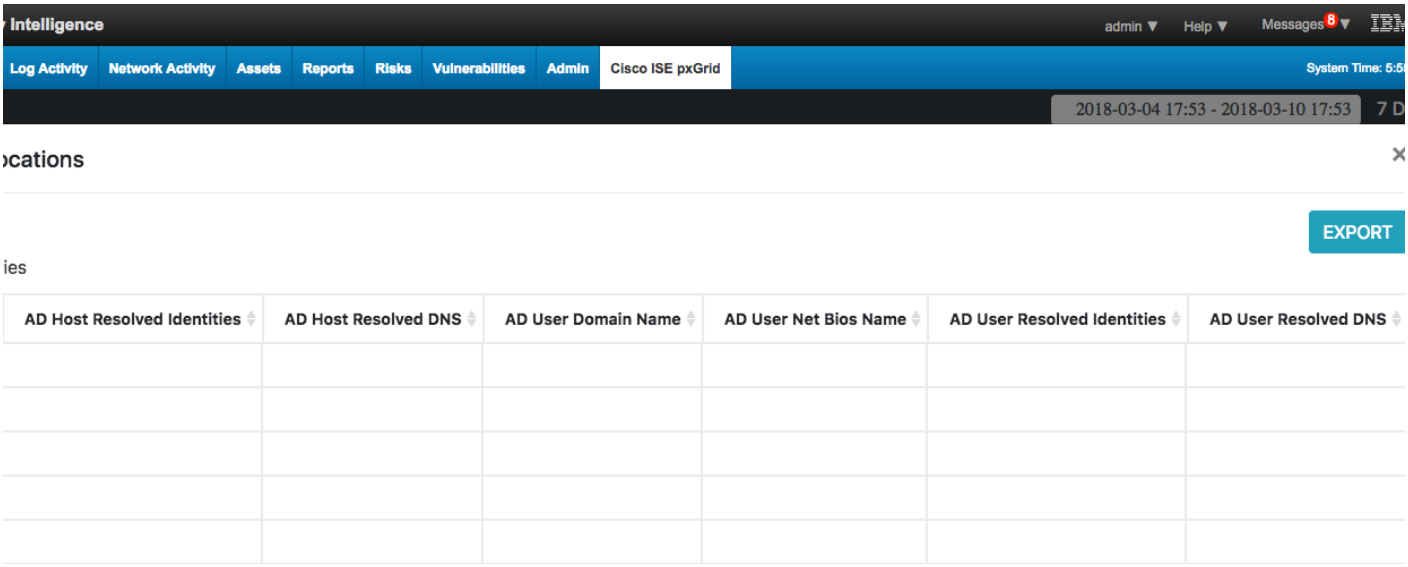


The **Server Name, Authentication Protocol, Device Type, Location, Calling Station ID**, NAS **IP Address, NAS Port ID, NAS Port Type** attributes provide more authentication details and location information of failed authentication attempts



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





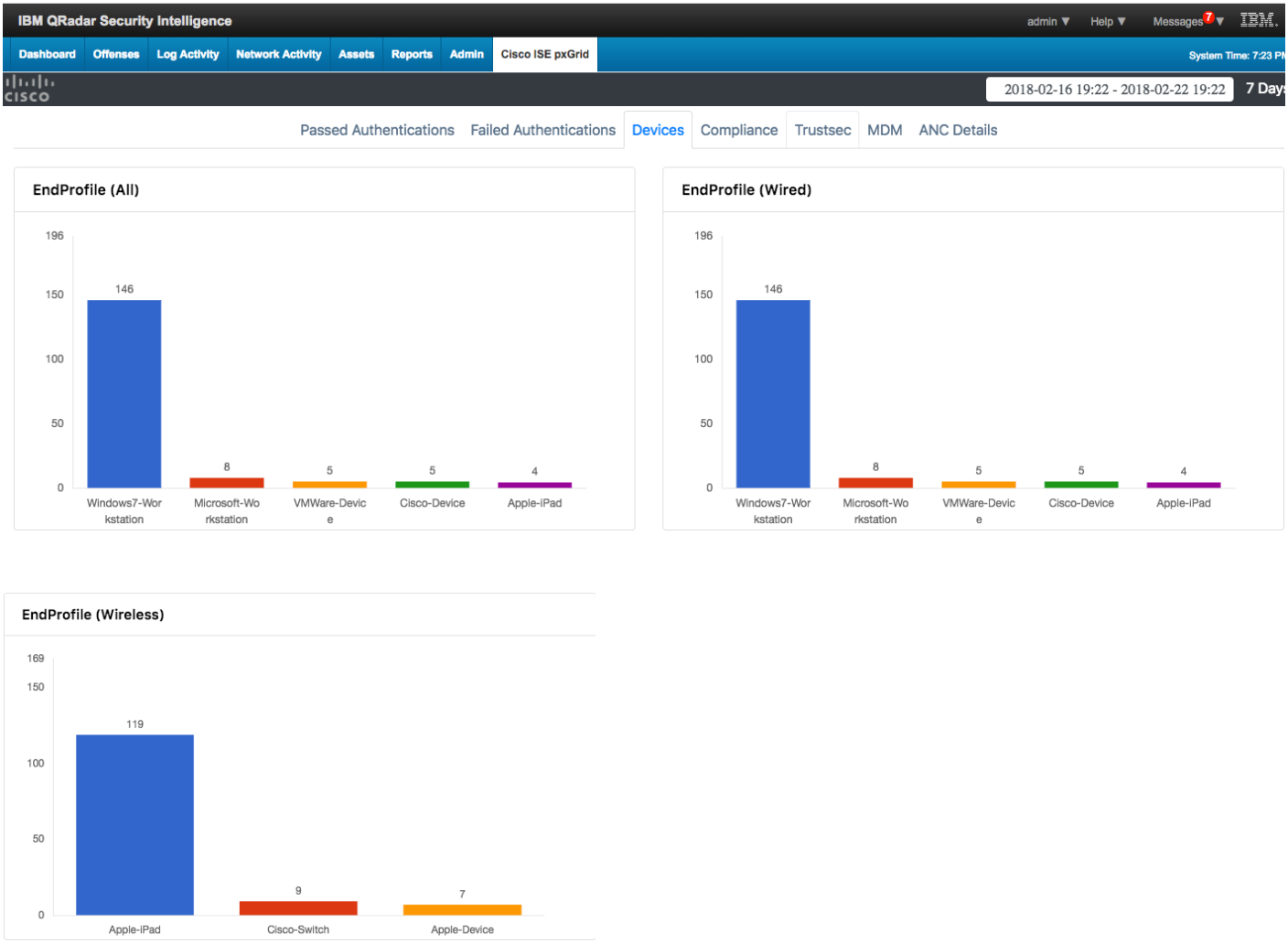
Devices

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.

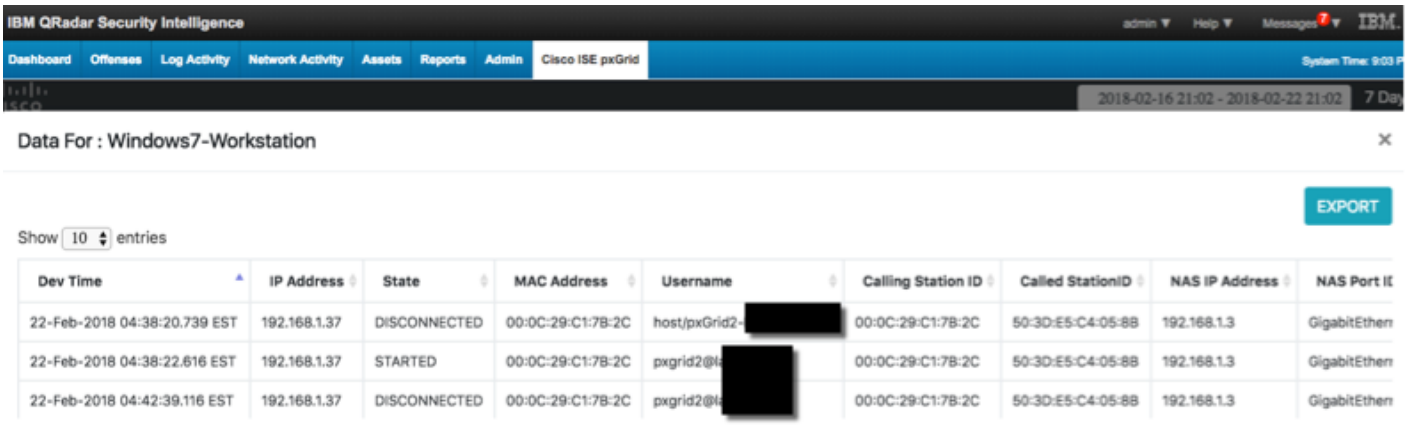
The admin drills down on the endpoint profile and obtains the following contextual information: endpoint device information, MAC Address, IP Address, posture status, NAS Port Type, NAS Port ID, NAS Identifier, NAS IP Address, WLAN Information, Calling Station ID, Called Station ID, AD resolvable user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

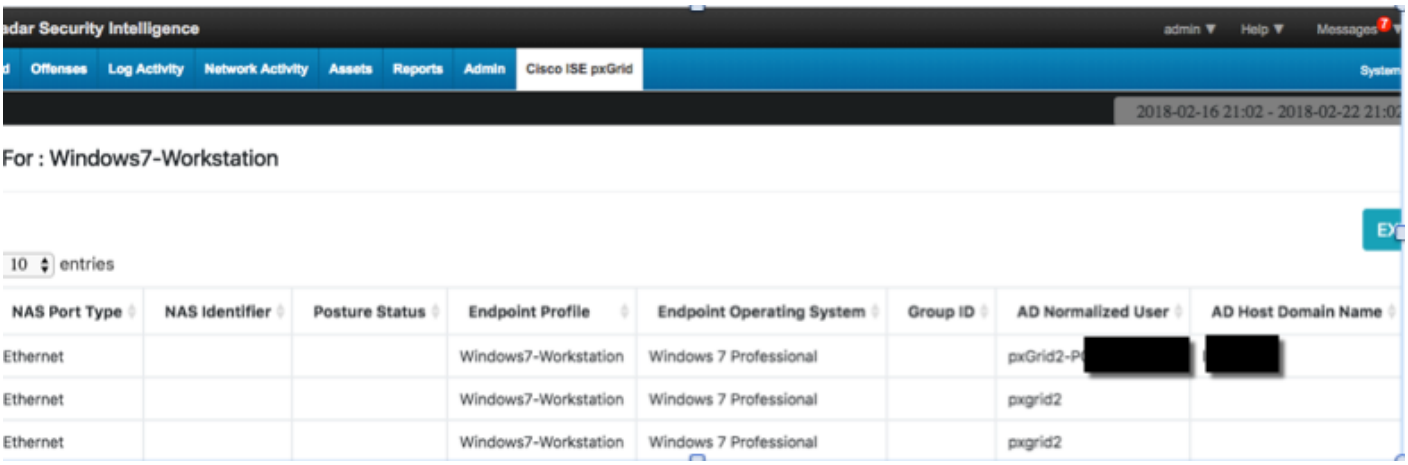


The **Username, IP address and MAC address** attributes are associated with the device.
The **NAS IP, NAS Port ID and NAS Port Type** attributes contain the connection type information



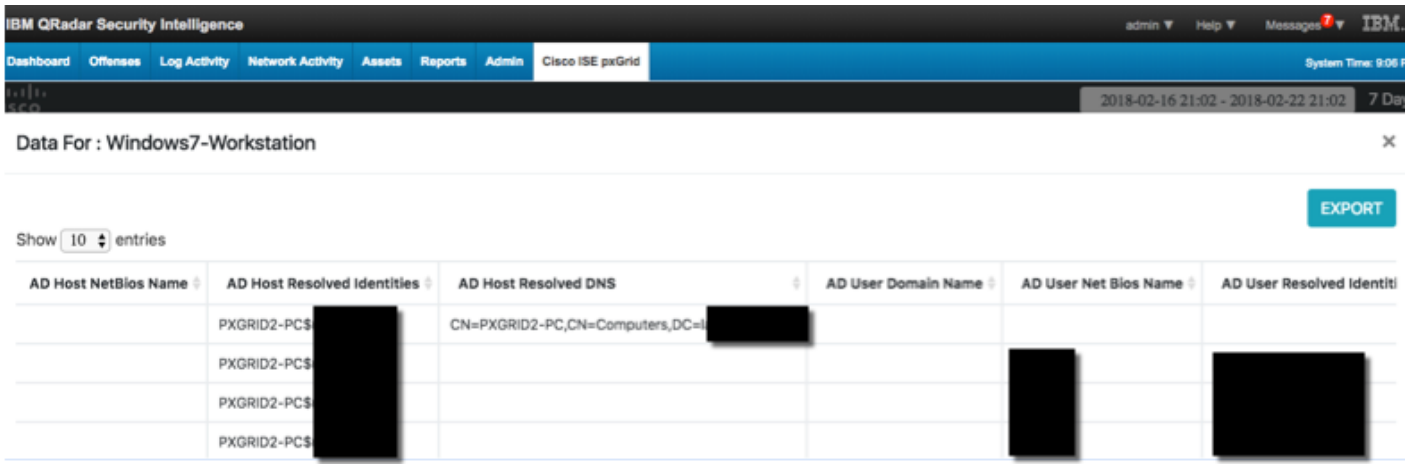
Dev Time	IP Address	State	MAC Address	Username	Calling Station ID	Called StationID	NAS IP Address	NAS Port ID
22-Feb-2018 04:38:20.739 EST	192.168.1.37	DISCONNECTED	00:0C:29:C1:7B:2C	host/pxGrid2-[redacted]	00:0C:29:C1:7B:2C	50:3D:E5:C4:05:8B	192.168.1.3	GigabitEthern
22-Feb-2018 04:38:22.616 EST	192.168.1.37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

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

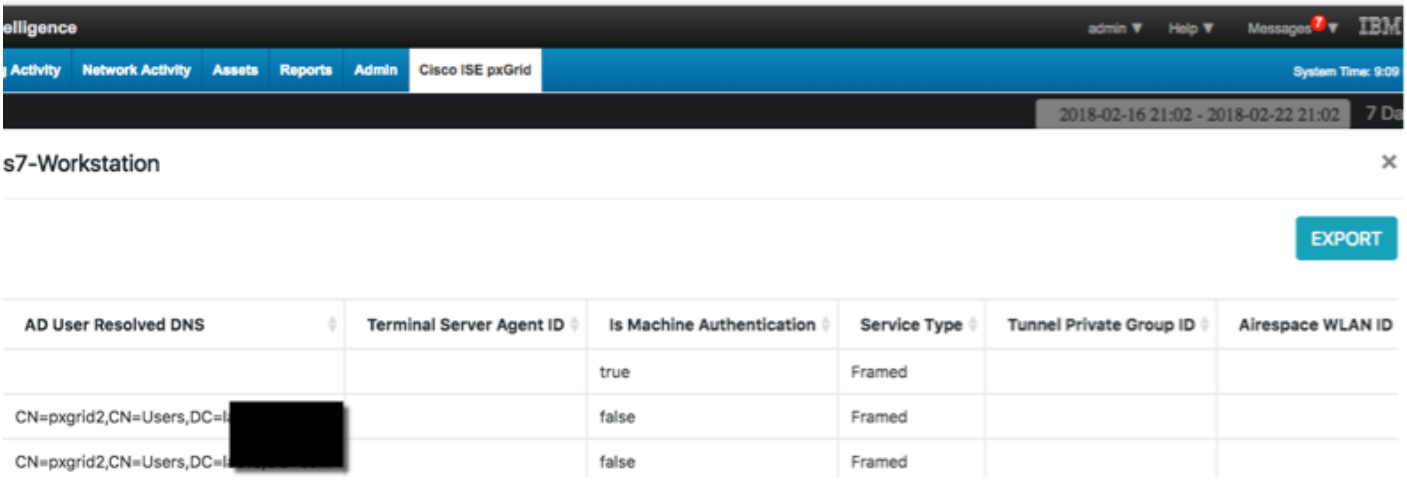


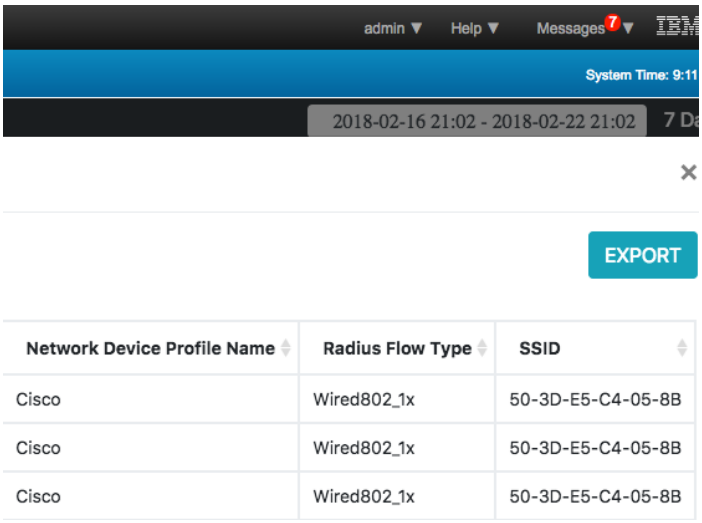
NAS Port Type	NAS Identifier	Posture Status	Endpoint Profile	Endpoint Operating System	Group ID	AD Normalized User	AD Host Domain Name
Ethernet			Windows7-Workstation	Windows 7 Professional		pxGrid2-P[redacted]	[redacted]
Ethernet			Windows7-Workstation	Windows 7 Professional		pxgrid2	
Ethernet			Windows7-Workstation	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.



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





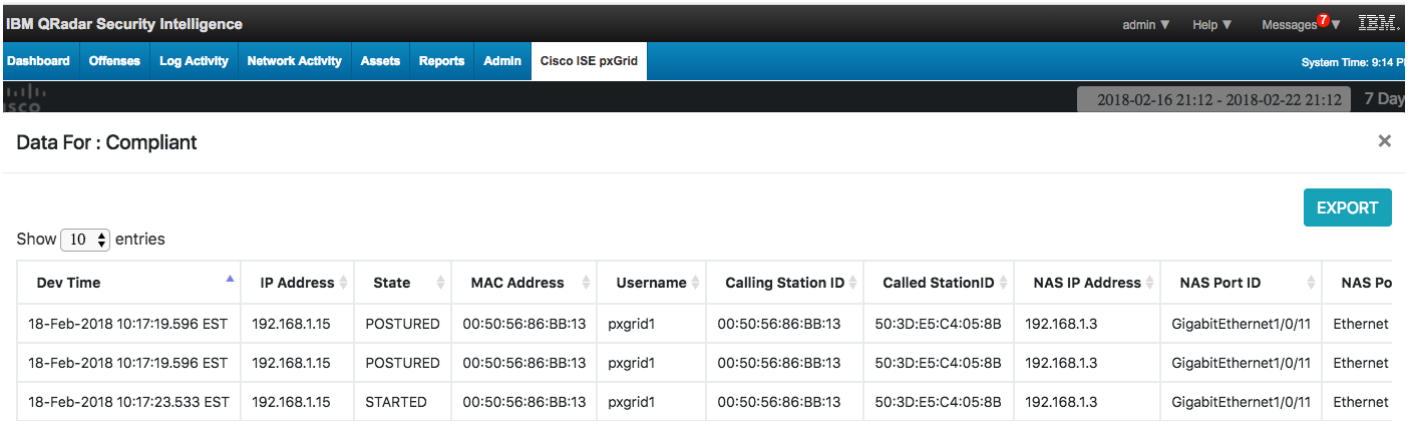
Compliance

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 there are not the case, than 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.

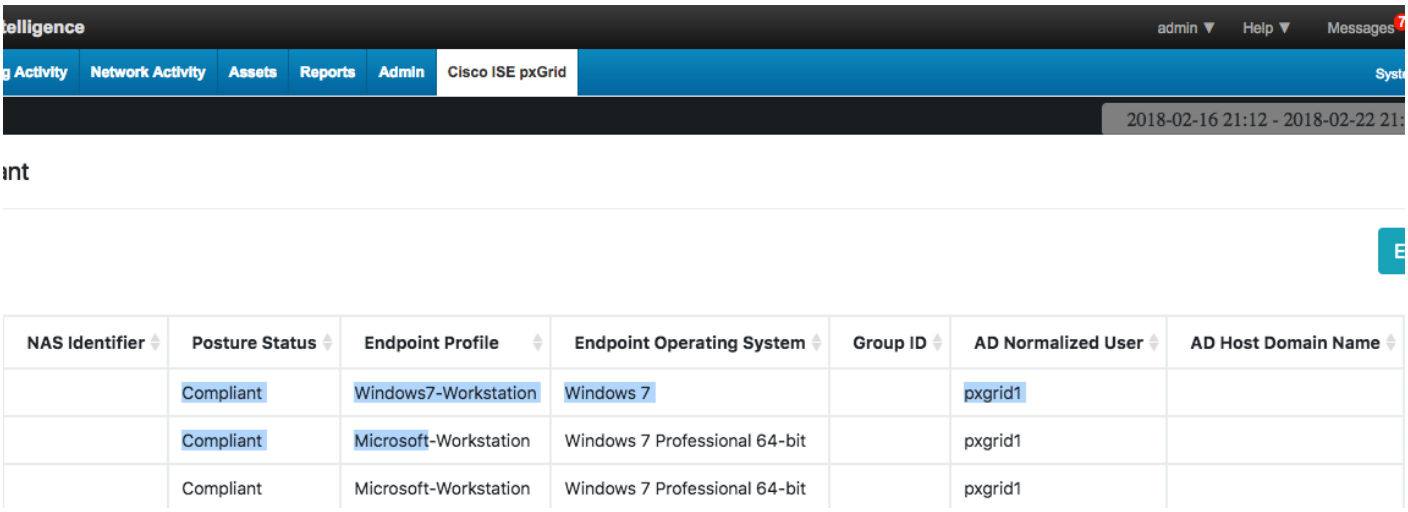
The **IP address, MAC address**, **Username, Calling Station ID** and **Posture Status** attributes provide the basic user information. The **NAS Port ID**, **NAS Port Type**, **NAS IP Address** attributes contain the location and connection-type information. The **State attribute** determines the Postured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



Dev Time	IP Address	State	MAC Address	Username	Calling Station ID	Called StationID	NAS IP Address	NAS Port ID	NAS Po
18-Feb-2018 10:17:19.596 EST	192.168.1.15	POSTURED	00:50:56:86: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

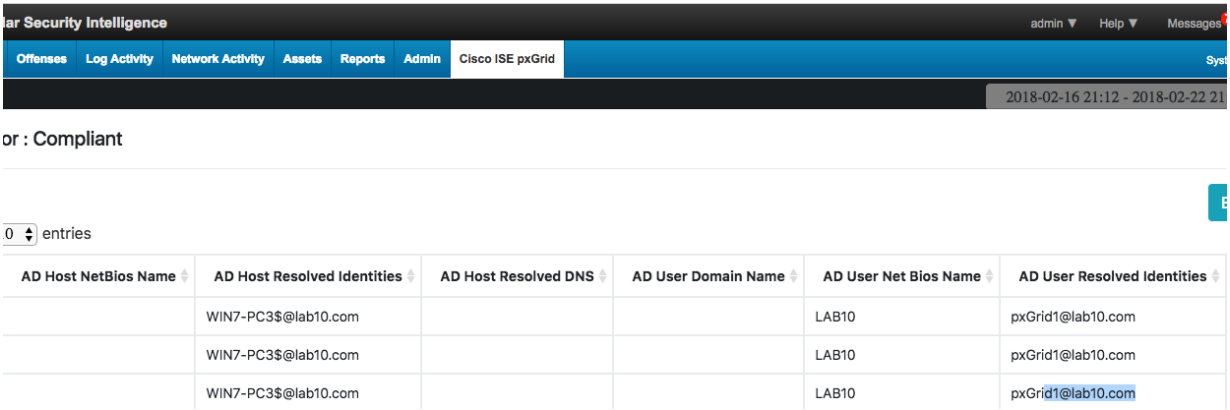
The **Posture Status attribute** contains the value of the posture status, compliant, non-compliance, pending.

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



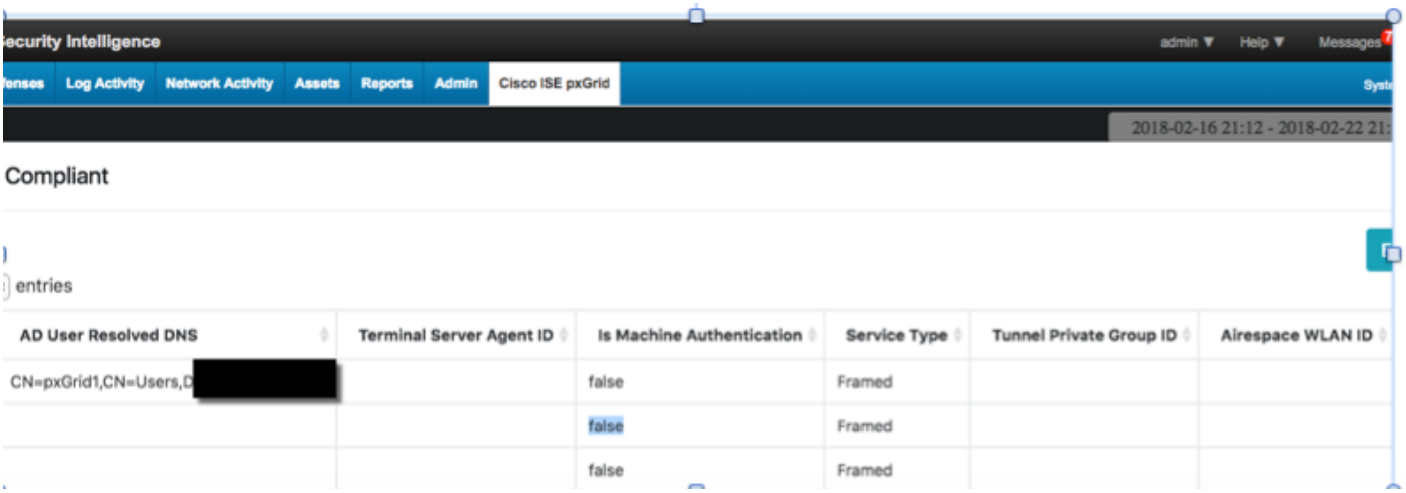
NAS Identifier	Posture Status	Endpoint Profile	Endpoint Operating System	Group ID	AD Normalized User	AD Host Domain Name
	Compliant	Windows7-Workstation	Windows 7		pxgrid1	
	Compliant	Microsoft-Workstation	Windows 7 Professional 64-bit		pxgrid1	
	Compliant	Microsoft-Workstation	Windows 7 Professional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

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



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

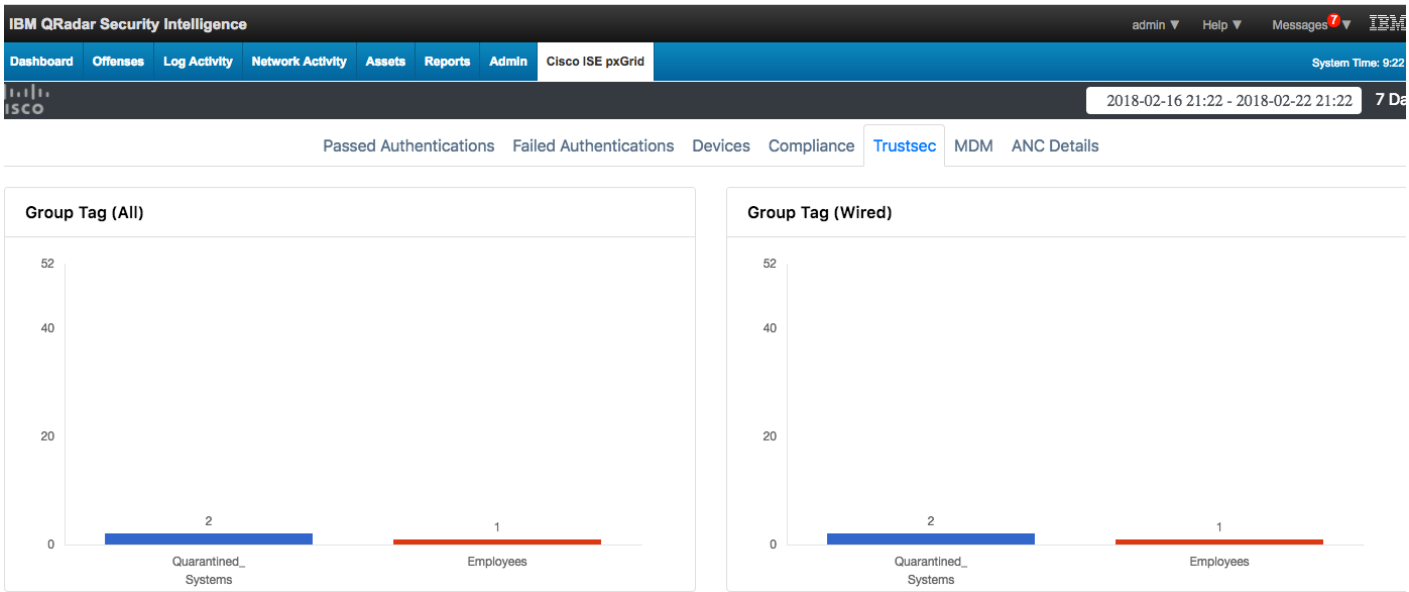
The **Is Machine Authentication** attribute if set to “true” denotes that this is machine authentication. If set to “false” denotes user authentication



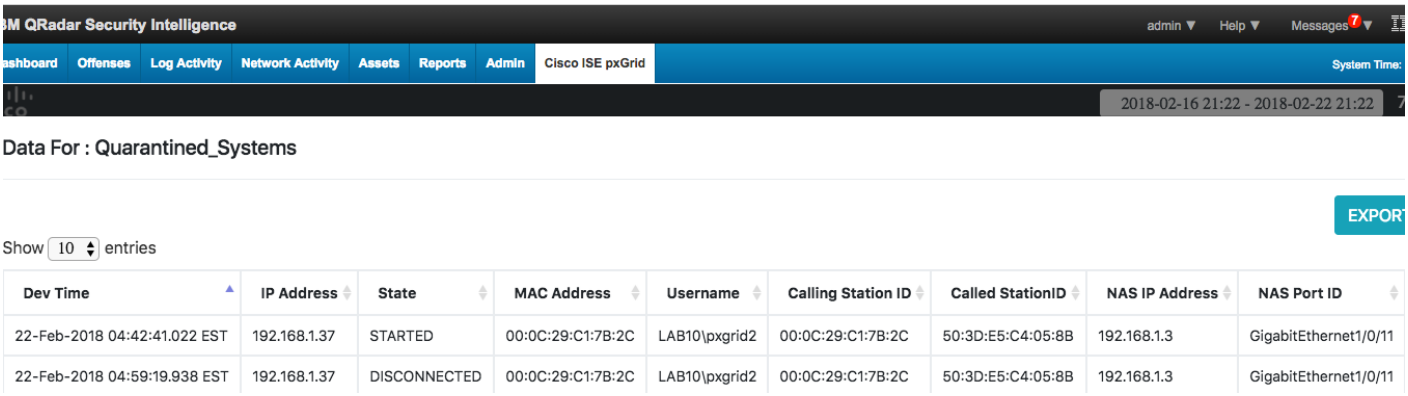
TrustSec

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**

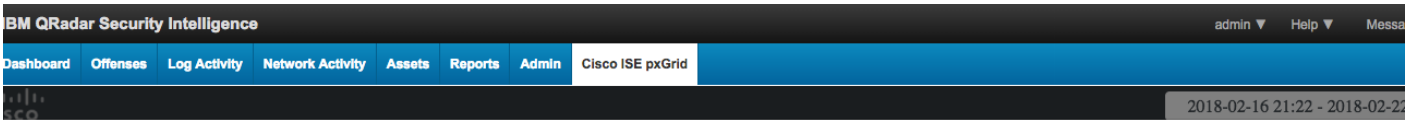


This provides the end-user information associated with the SGT. Here we see the **Username**, **IP Address, MAC Address** attributes. We also see the **NAS IP Address**, **NAS Port ID,** and **NAS Port type** attributes to determine the location and connection type



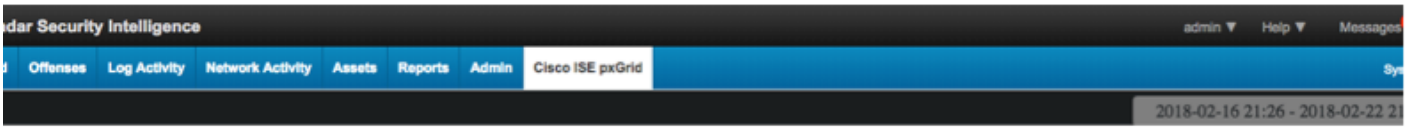
Dev Time	IP Address	State	MAC Address	Username	Calling Station ID	Called StationID	NAS IP Address	NAS Port ID
22-Feb-2018 04:42:41.022 EST	192.168.1.37	STARTED	00:0C:29:C1:7B:2C	LAB10\pxgrid2	00:0C:29:C1:7B:2C	50:3D:E5:C4:05:8B	192.168.1.3	GigabitEthernet1/0/11
22-Feb-2018 04:59:19.938 EST	192.168.1.37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



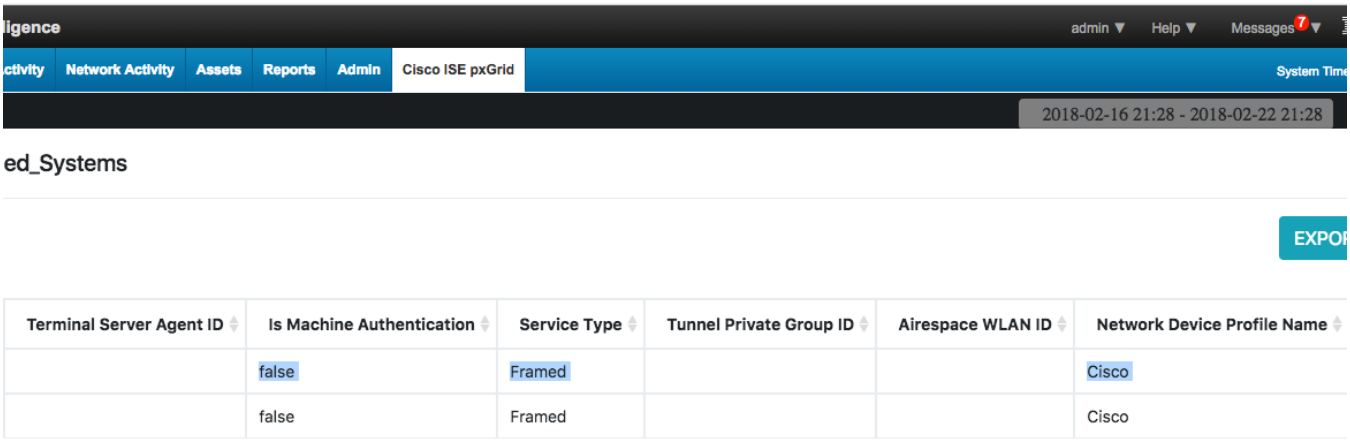
NAS Port Type	NAS Identifier	Posture Status	Endpoint Profile	Endpoint Operating System	Group ID	AD Normalized User	AD Host Domain Name
Ethernet			Windows7-Workstation	Windows 7 Professional		pxgrid2	
Ethernet			Windows7-Workstation	Windows 7 Professional		pxgrid2	

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



AD Host NetBios Name	AD Host Resolved Identities	AD Host Resolved DNS	AD User Domain Name	AD User Net Bios Name	AD User Resolved Identities
	PXGRID2-PC$@[redacted]			LAB10	[redacted]
	PXGRID2-PC$@[redacted]			LAB10	[redacted]

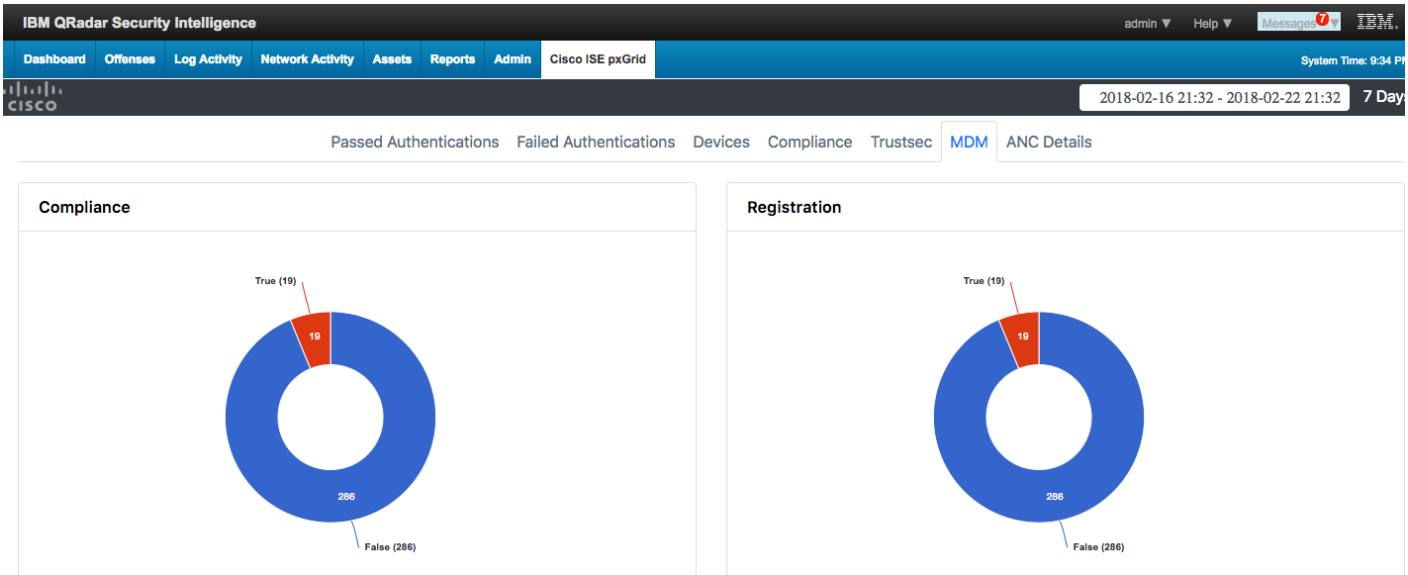
The **Is Machine Authentication** attribute if set to "true" denotes that this is machine authentication. If set to "false" denotes user authentication.



Mobile Device Management (MDM)

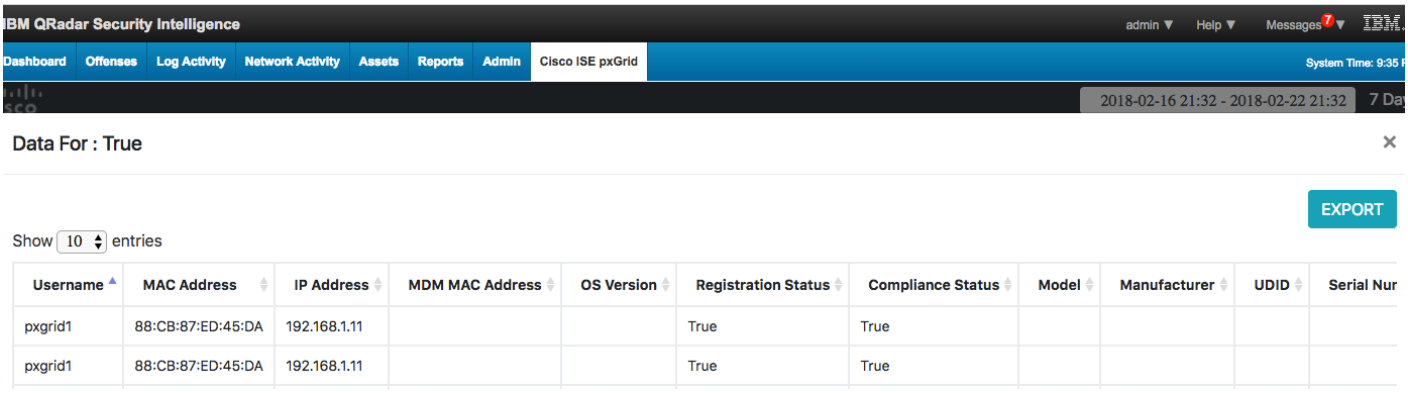
The MDM Dashboard provides the admin with the visibility to look into an organizations MDM security policy. In the ISE 2.4 initial release, only the registration and compliance status are available.

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.

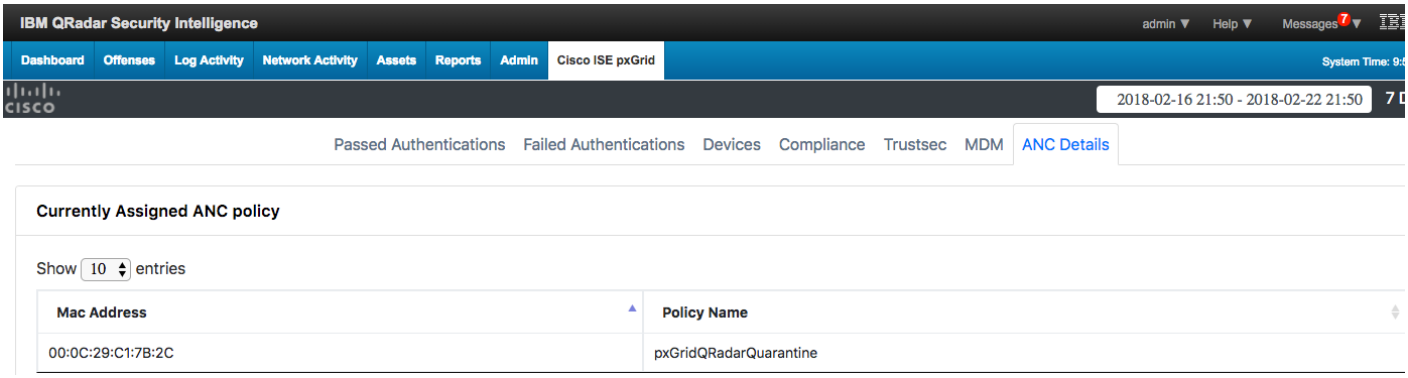
Note: It is assumed that MDM is already configured in ISE. In this example, Cisco Meraki is used.



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**



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:**

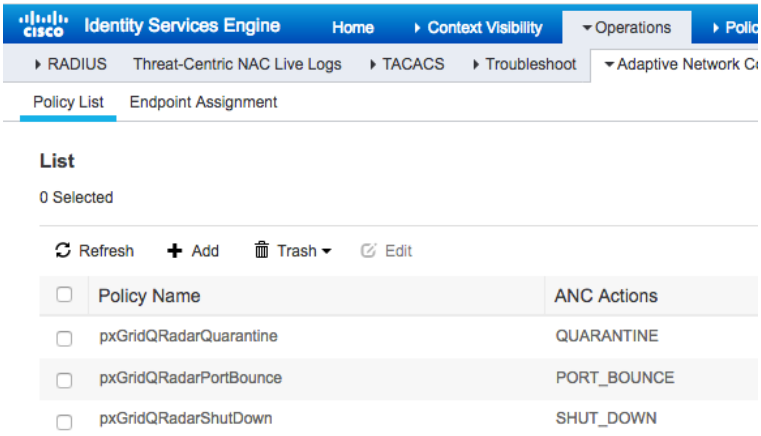
Step 2 **pxGridQRadarQuaratine**, **QUARANTINE**

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:



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.

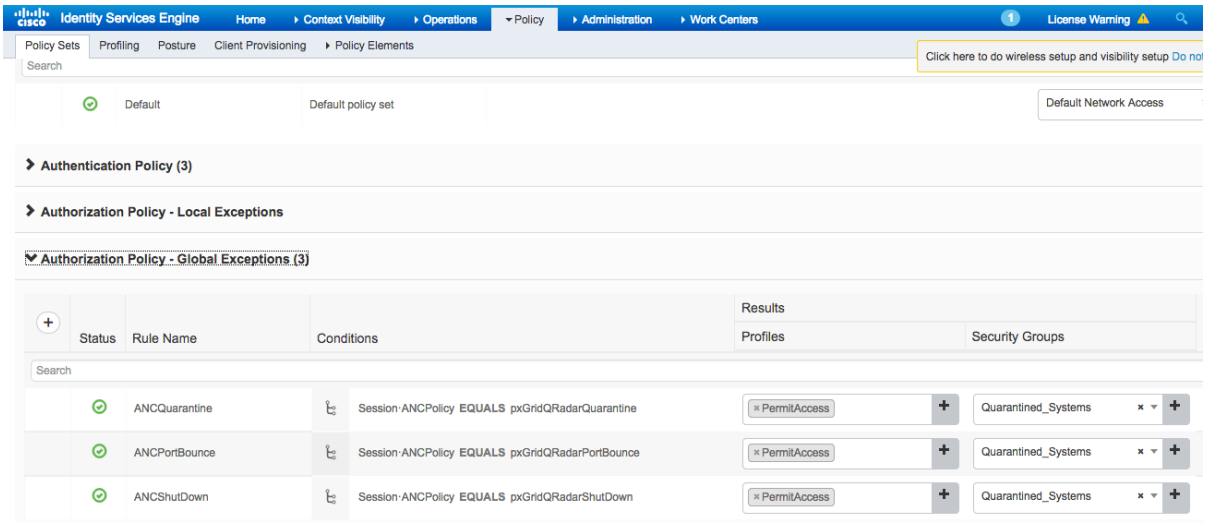
Step 1 Select **Policy->Policy Sets->Default>”>”->Authorization Policy->Global Exceptions->”+”**
Step 2 Under **Rule Name**, type: **ANCQuarantine**
Step 3 Under **Conditions**, select “**+**”
Step 4 Select “**x**” close the introductory screen
Step 5 Under **Dictionary,** select **Session->ANCPolicy->Equals->pxGridQRadarQuarantine**
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

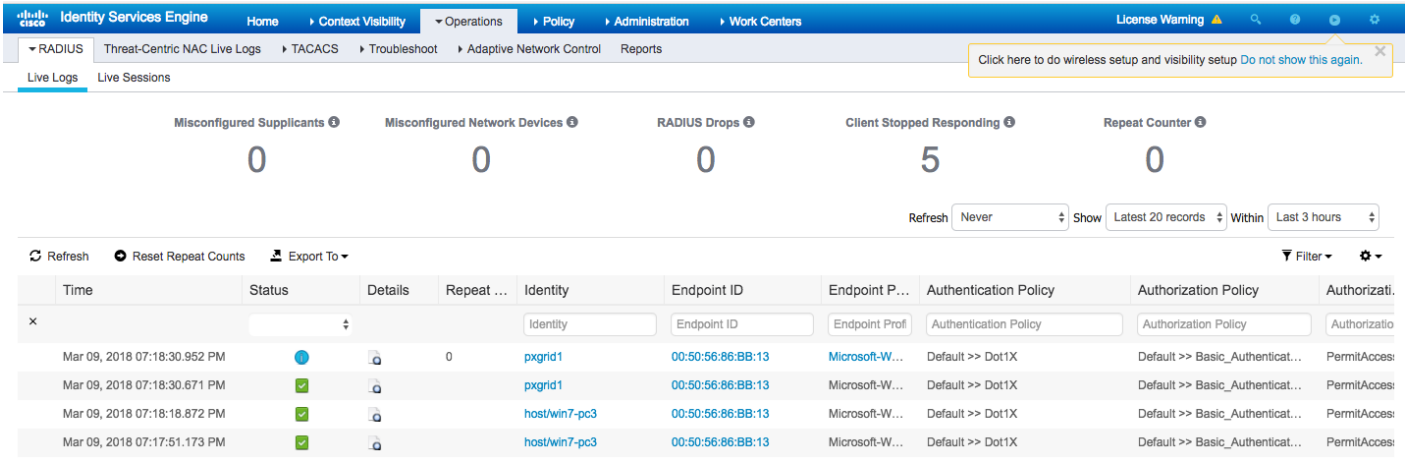
Step 12 You should see the following:


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
License Warning
Policy Sets
Profiling
Posture
Client Provisioning
Policy Elements
Search
Click here to do wireless setup and visibility setup Do not
Default
Default policy set
Default Network Access
Authentication Policy (3)
Authorization Policy - Local Exceptions
Authorization Policy - Global Exceptions (3)
Results
Status
Rule Name
Conditions
Profiles
Security Groups
Search
ANCQuarantine
Session·ANCPolicy EQUALS pxGridQRadarQuarantine
PermitAccess
Quarantined_Systems
ANCPortBounce
Session·ANCPolicy EQUALS pxGridQRadarPortBounce
PermitAccess
Quarantined_Systems
ANCShutDown
Session·ANCPolicy EQUALS pxGridQRadarShutDown
PermitAccess
Quarantined_Systems

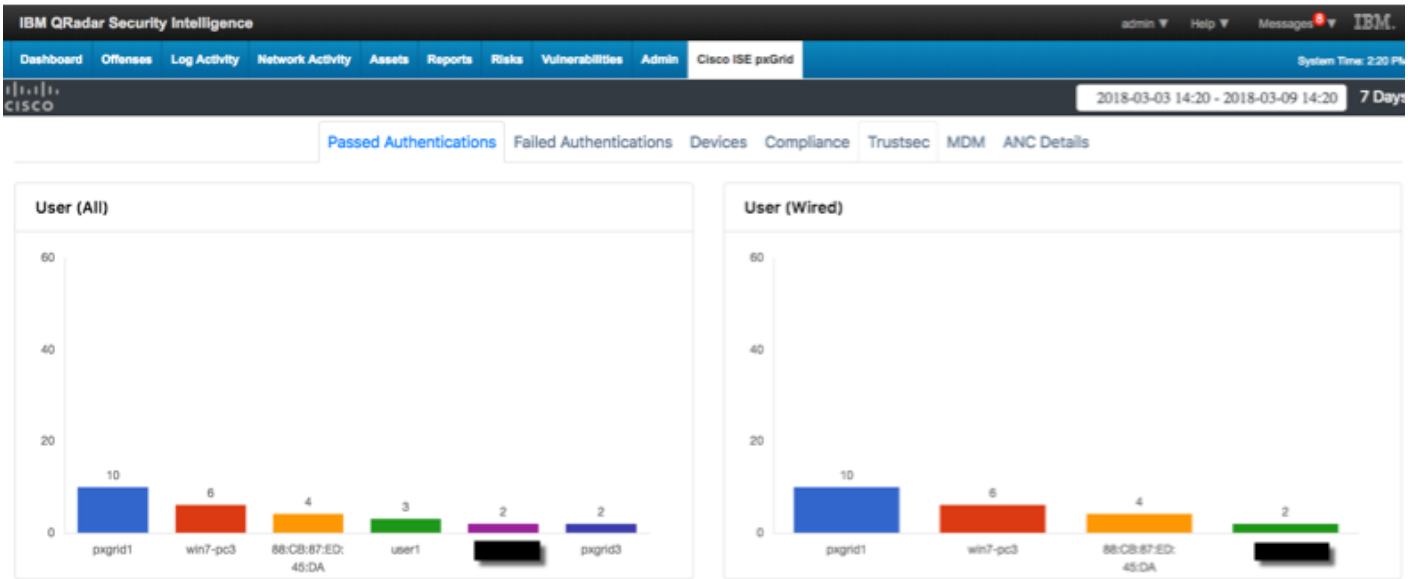
Performing Cisco ISE ANC Mitigation Actions Through Cisco ISE pxGrid App Dashboard Panel

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

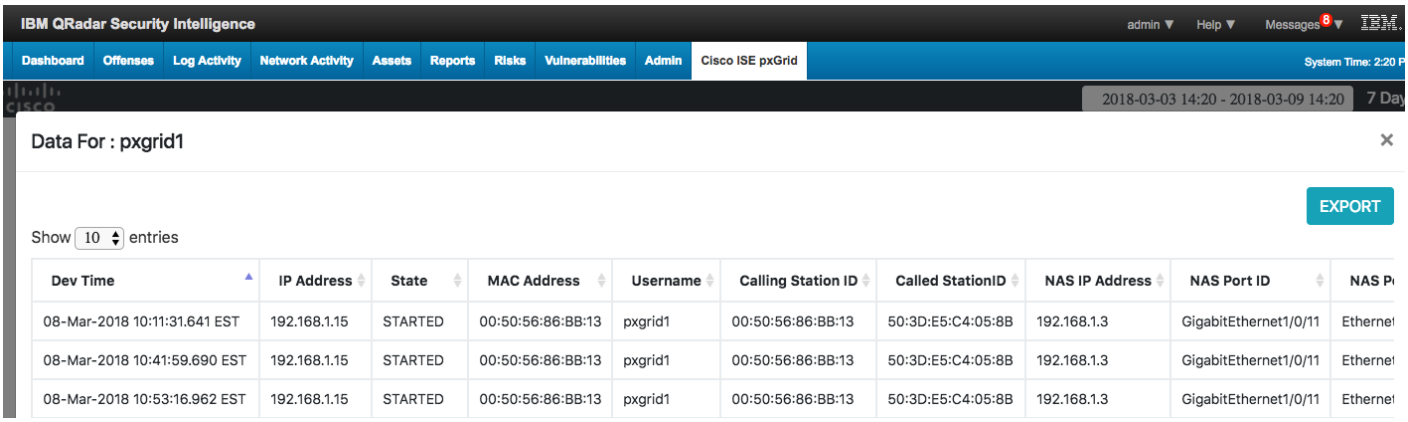
Step 1 User pxGrid1 authenticates in ISE.



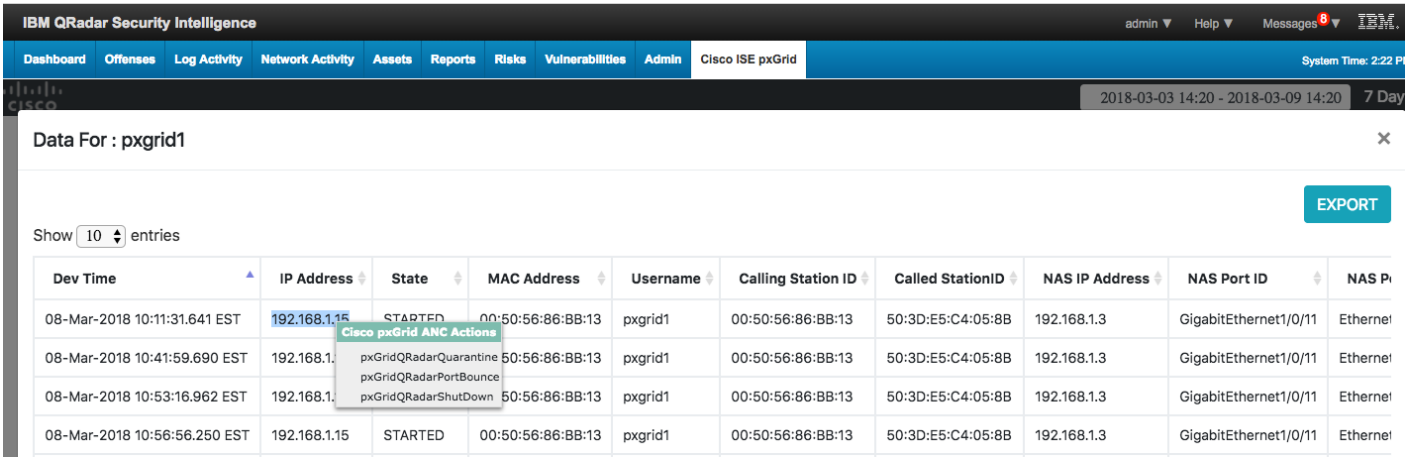
Step 2 Select **Cisco ISE pxGrid->Passed Authentications**



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

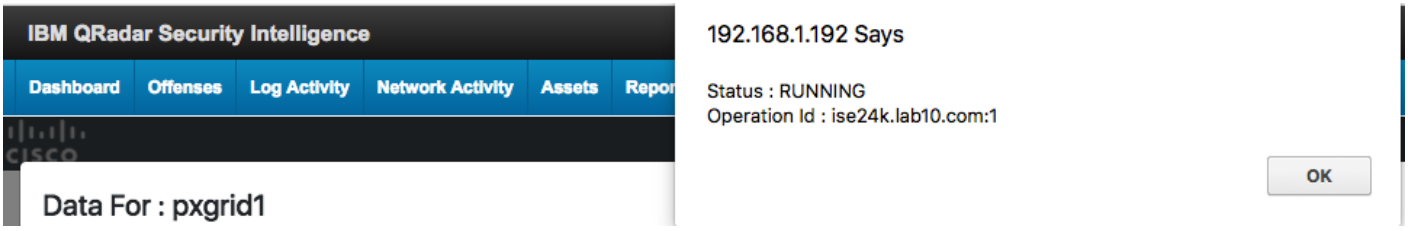


Step 4 **Right-click** on the IP address, you should will the ANC policies



Step 5 Select p**xGridQRadarQuarantine**

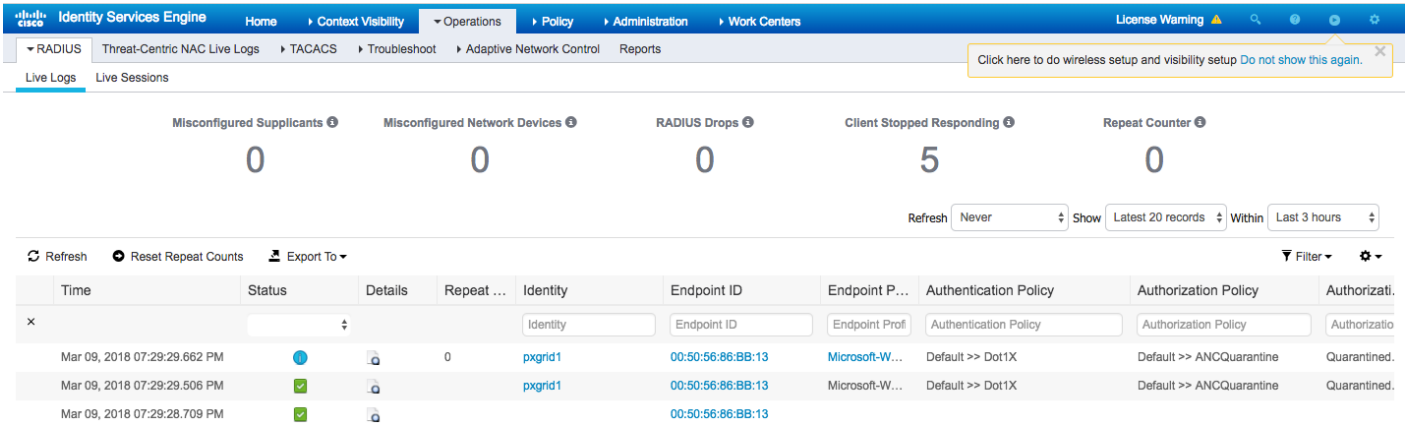
Step 6 You should see a successful status message



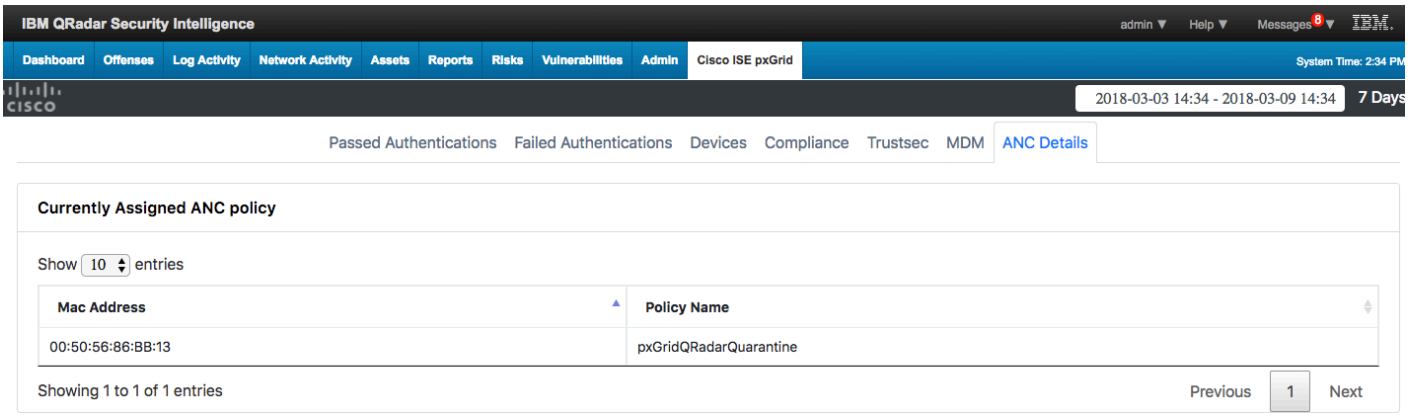
Step 7 Select **OK**

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

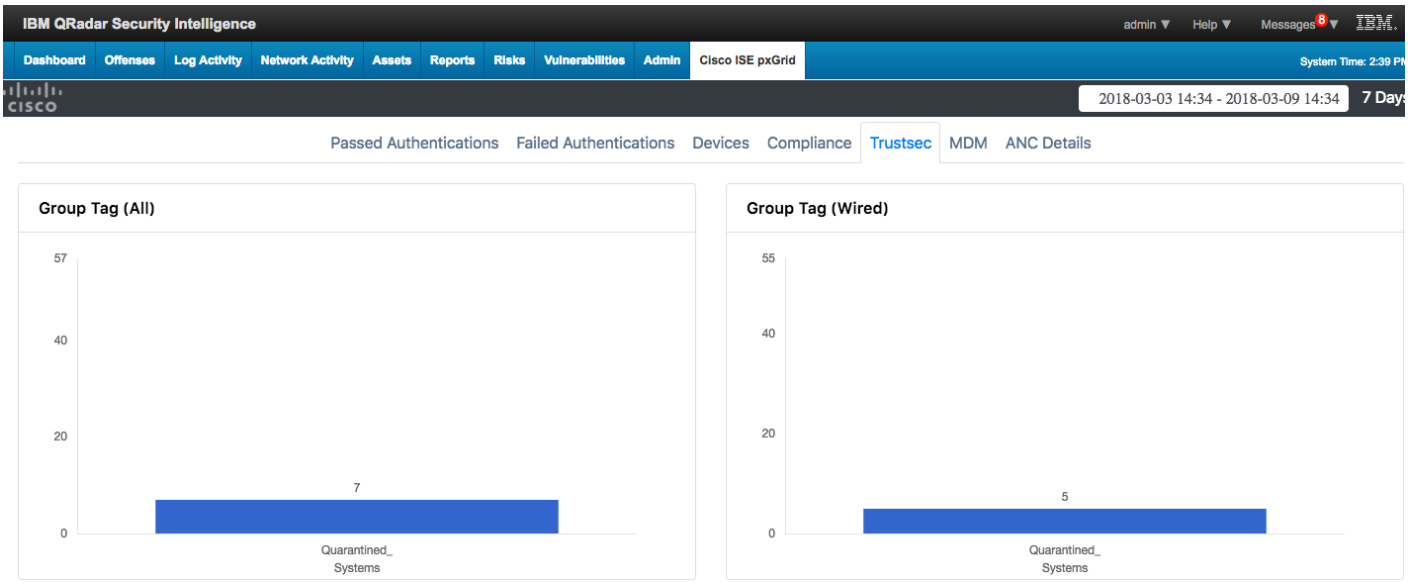
You should see that the endpoint has been quarantined based on the ANCQuarantine Policy



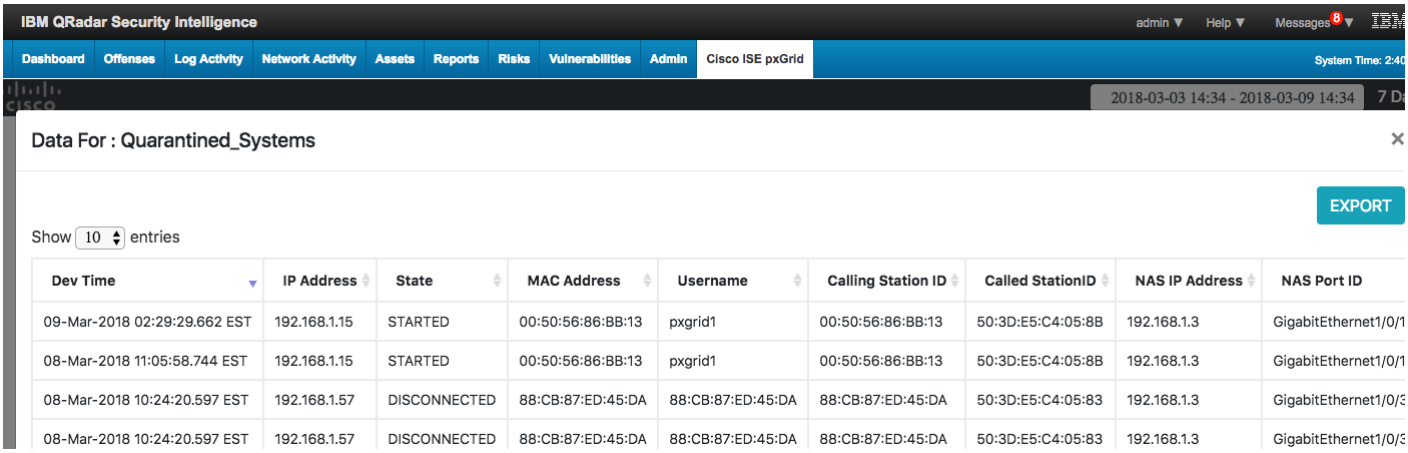
Step 9 To view the quarantine details in the Cisco ISE pxGrid App ANC Dashboard, **select Cisco ISE pxGrid->ANC Details**
Note the MAC Address of the quarantined endpoint.



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



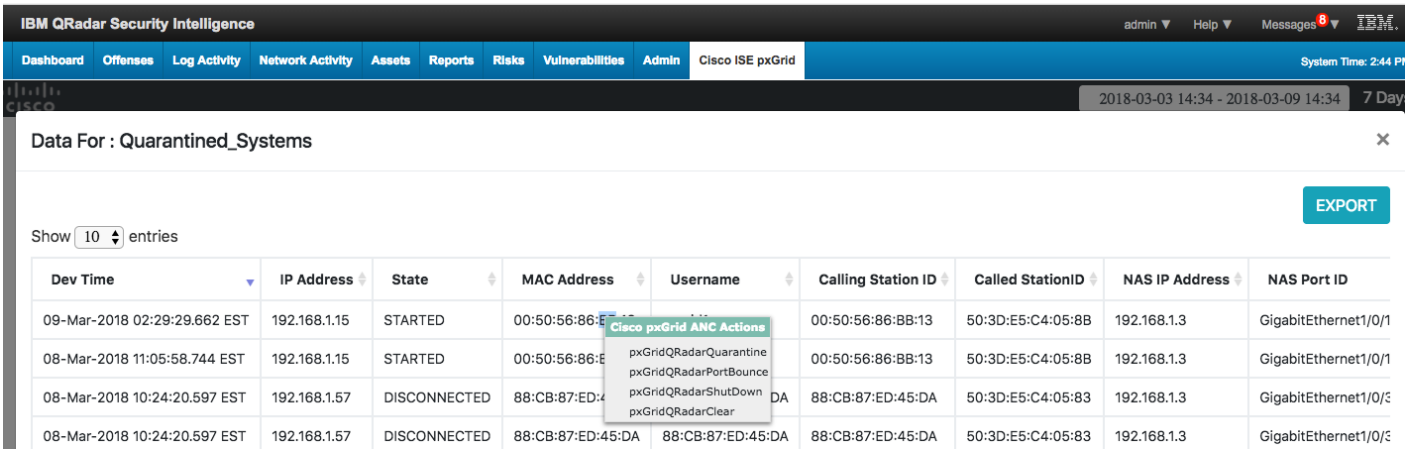
Step 11 Select **Quarantined_Systems**, you should see the quarantined endpoint



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

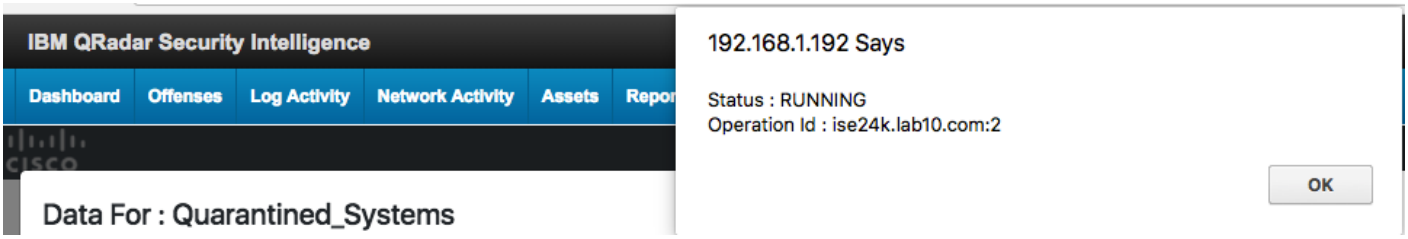
Step 12 You have the option of unquaranting or clearing the endpoint either through the Dashboards or directly in ISE. We will unquarantine the endpoint from this view.

Step 13 Right-click on the MAC Address



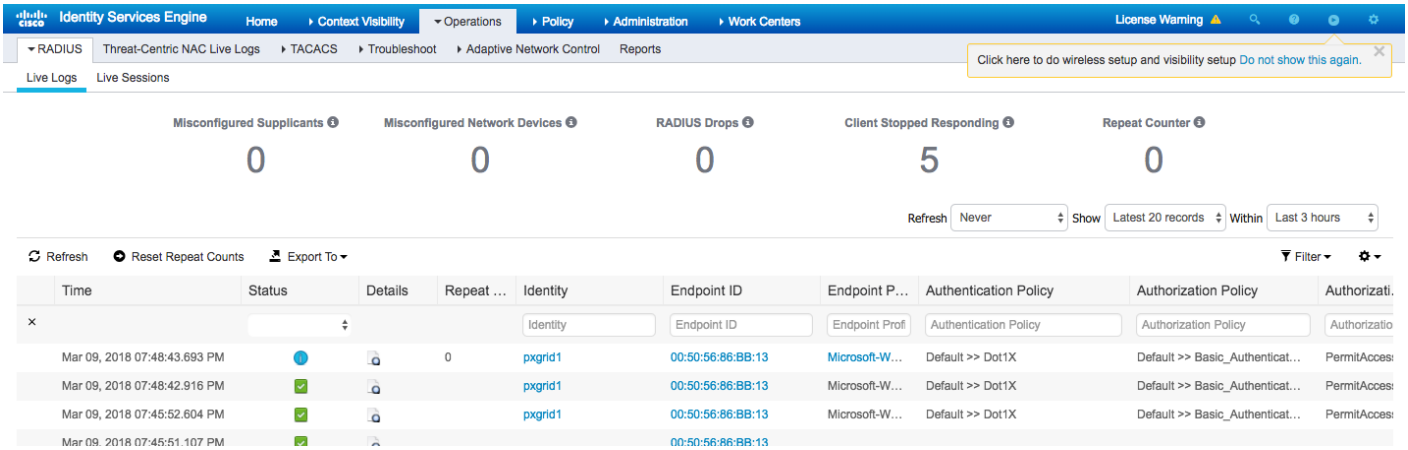
Step 14 Select px**GridQRadarClear**

Step 15 You should see successful status message

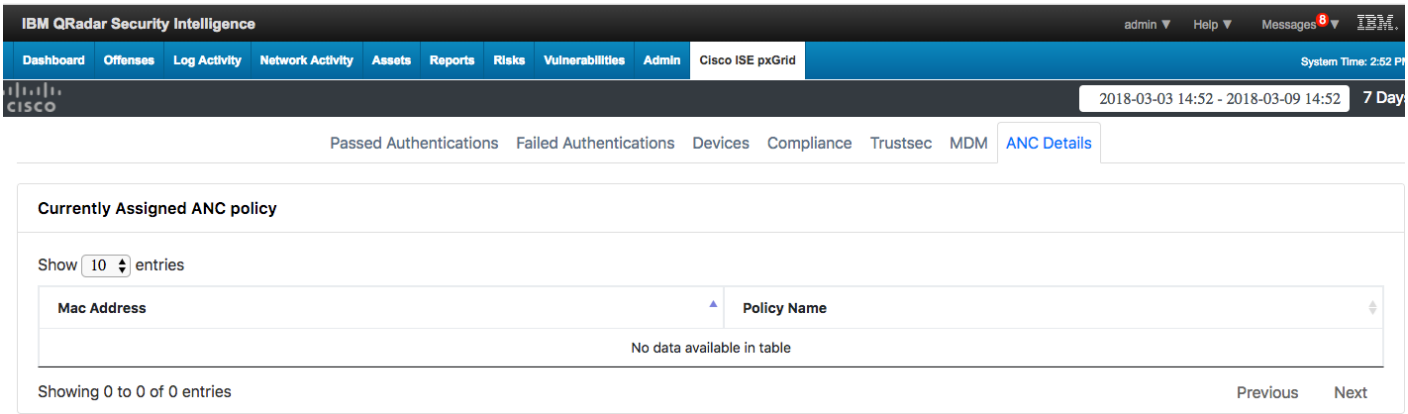


Step 16 Select **OK**

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



Step 18 Select Cisco ISE pxGrid->ANC Details, you should see the endpoint is no longer assigned to the ANC policy.

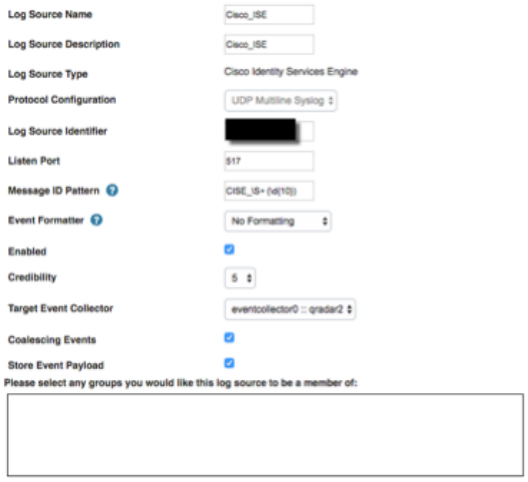


Note: To unquarantine or clear in ISE, select Operations->Adaptive Network Control->Endpoint Assignment->select the endpoint MAC address->Trash

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**



Step 2 Select **Save**

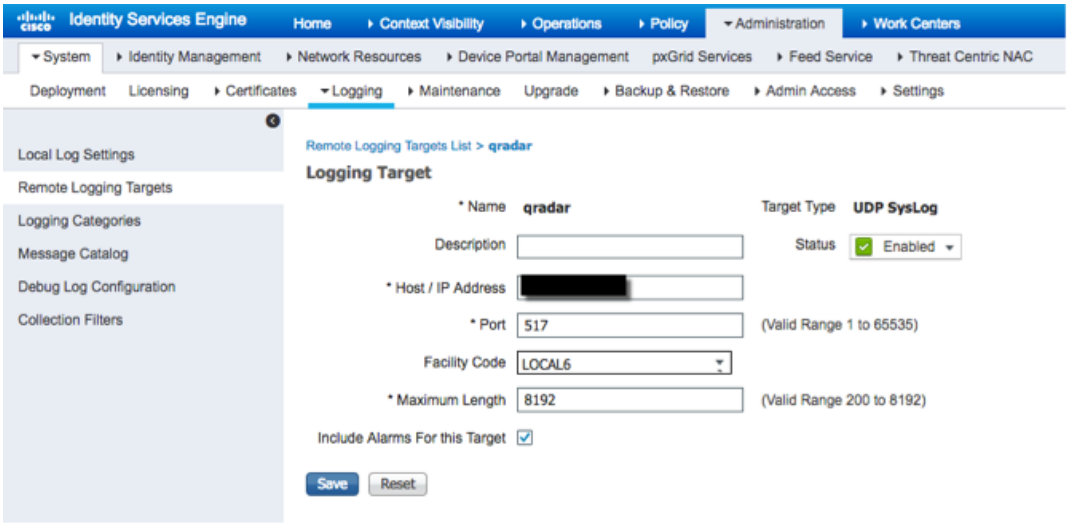
Step 3 Select **Deploy Changes->Deploy**

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.

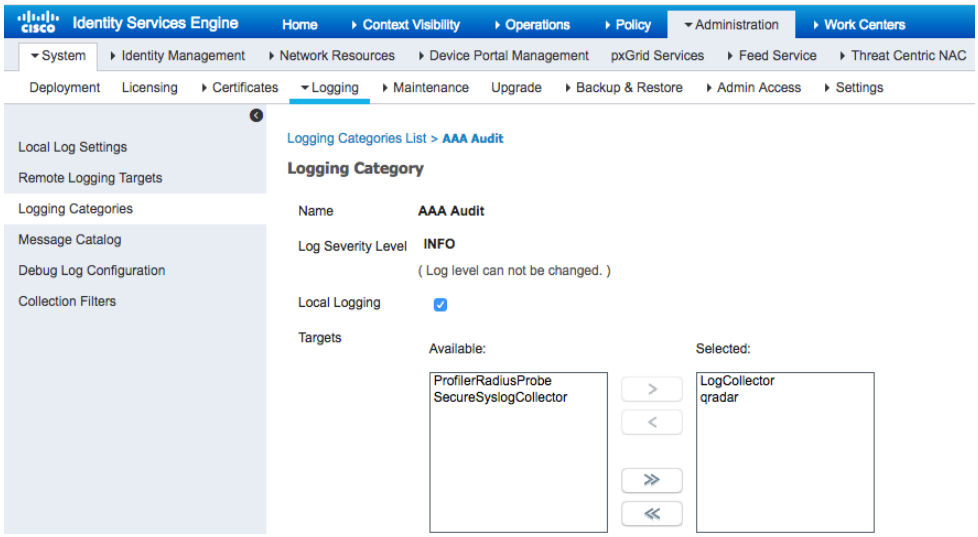
Step 1 Select **Administration->System->Logging->Remote Logging Targets->Add->**type: **Host/ IP address** of IBM QRadar instance and **517** for the **Port**



Step 2 Select **Save**

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

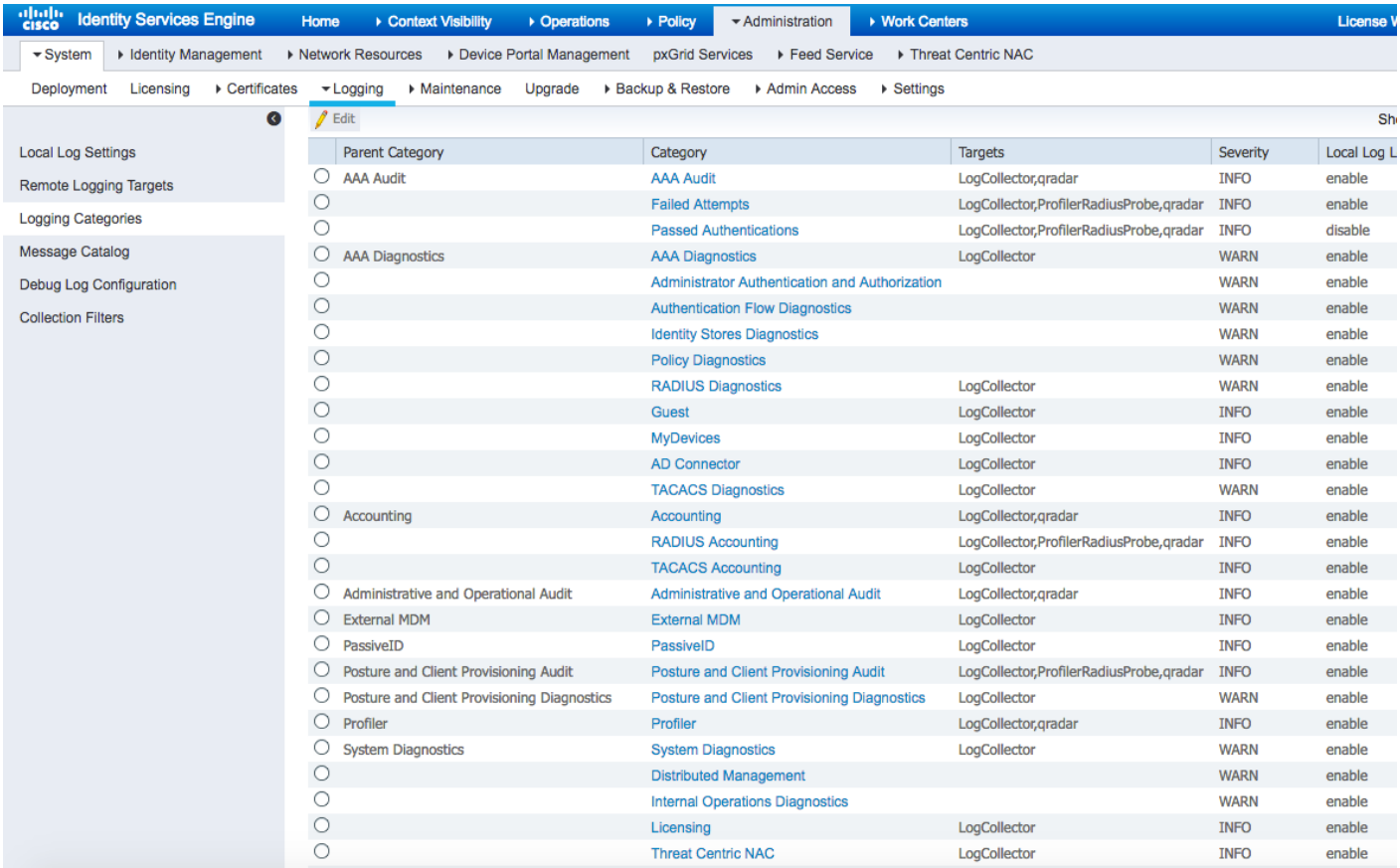
Step 4 Move qRadar from Targets **Available** into the **Selected** column



Step 5 Select **Save**

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

Step 7 When completed, you should see the following:



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

Performing ISE ANC Mitigation Actions Through IBM QRadar Syslog Events

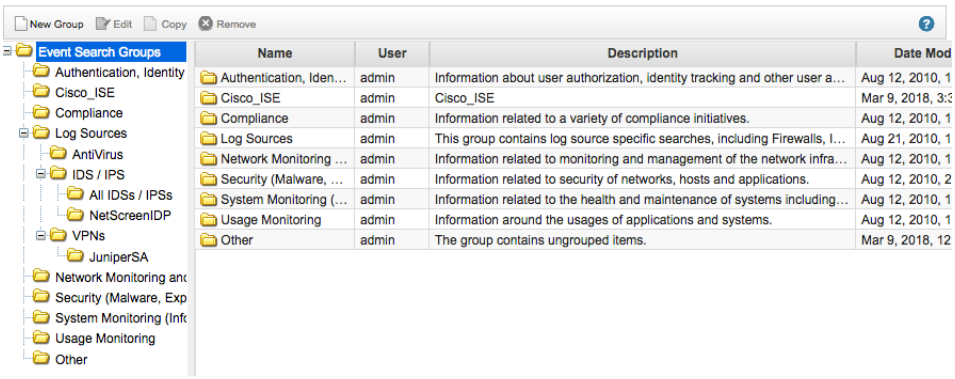
The desired endpoints for performing ANC mitigation actions must have been authenticated through ISE. In this example, we have Cisco ISE Passed Authentication syslog events sent over to IBM QRadar. We have to create a custom FramedIPAddress field to provide the IP address of the endpoint.

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

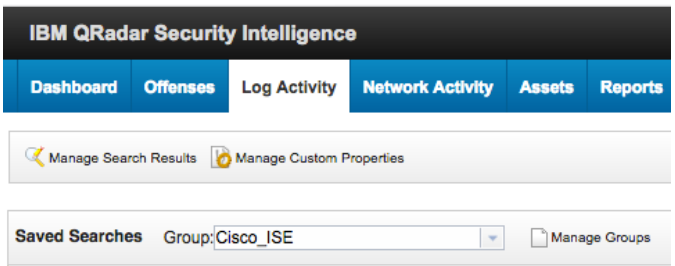
The FramedIPAddress field will be added to the available columns field in the Log Activity Search created for ISE. The FramedIPAddress field will now appear in ISE Log Activity searches.

Creating Custom Field for Framed IP Address ISE Syslog Event

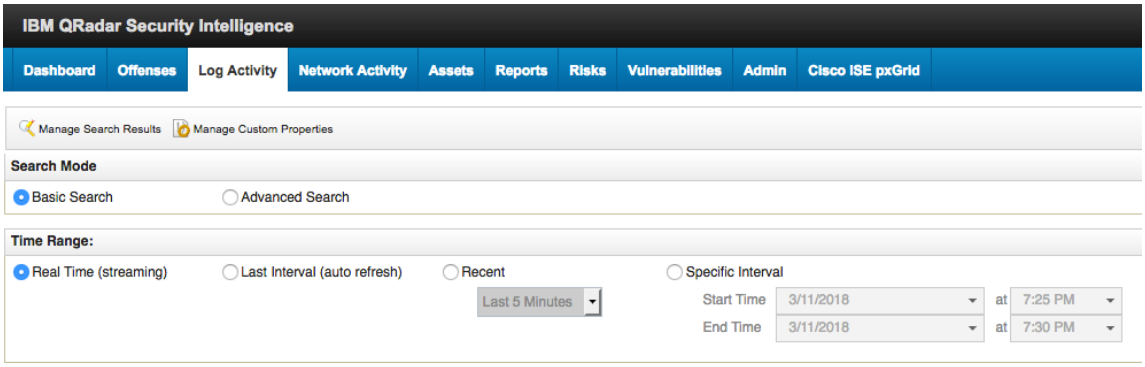
Step 1 In IBM QRadar, select Log Activity->Search->New Search->Manage Groups->New Group->Cisco_ISE You should see the Cisco ISE group



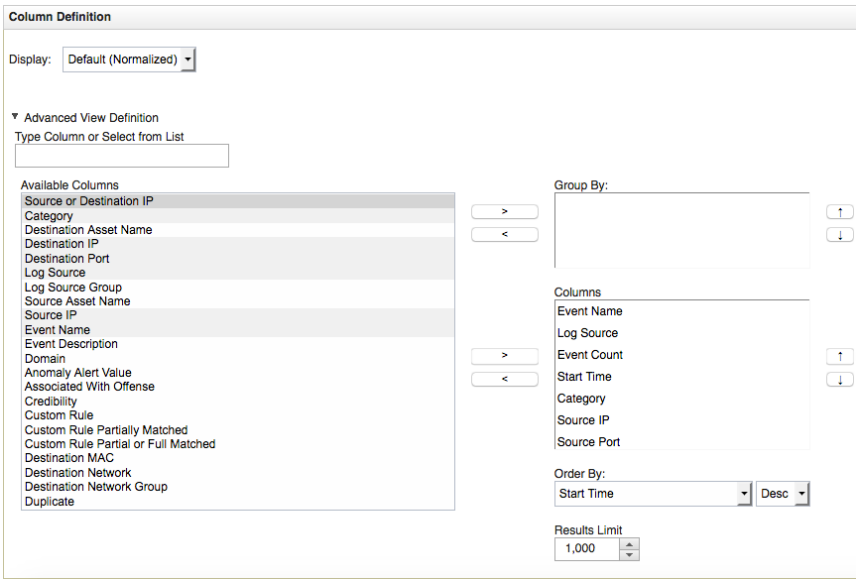
Step 2 Select **Cisco_ISE Group**



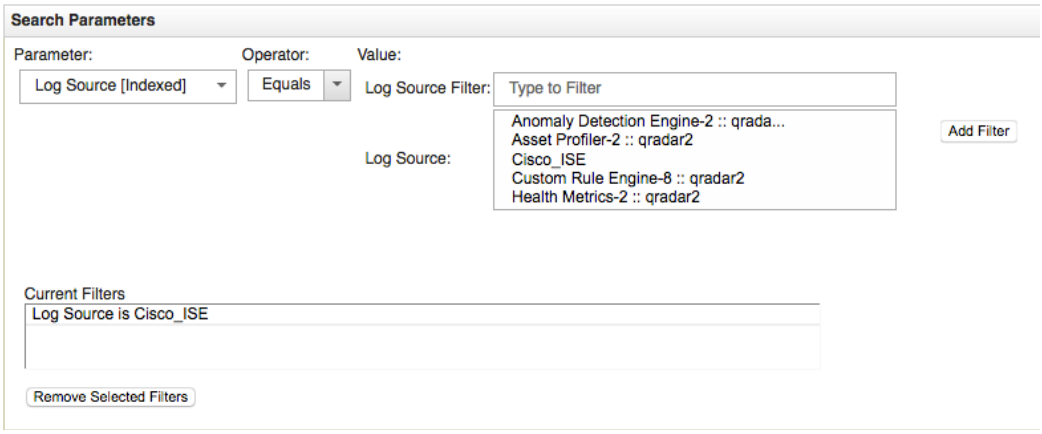
Step 3 Keep the Search defaults



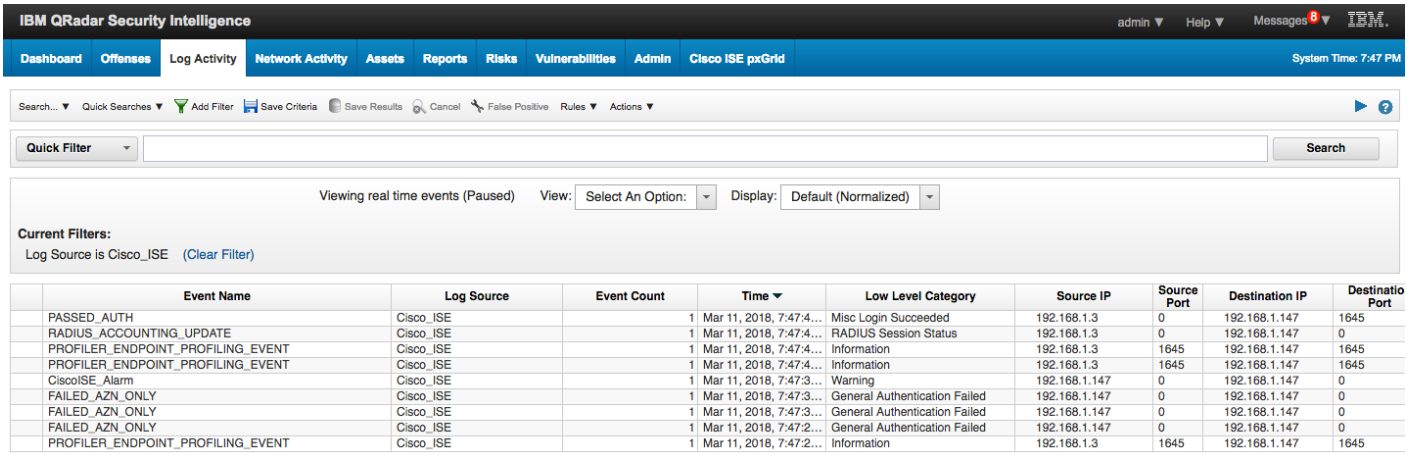
Step 4 Keep the Column defaults



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



Step 6 Select **Filter**



Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destinatio 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

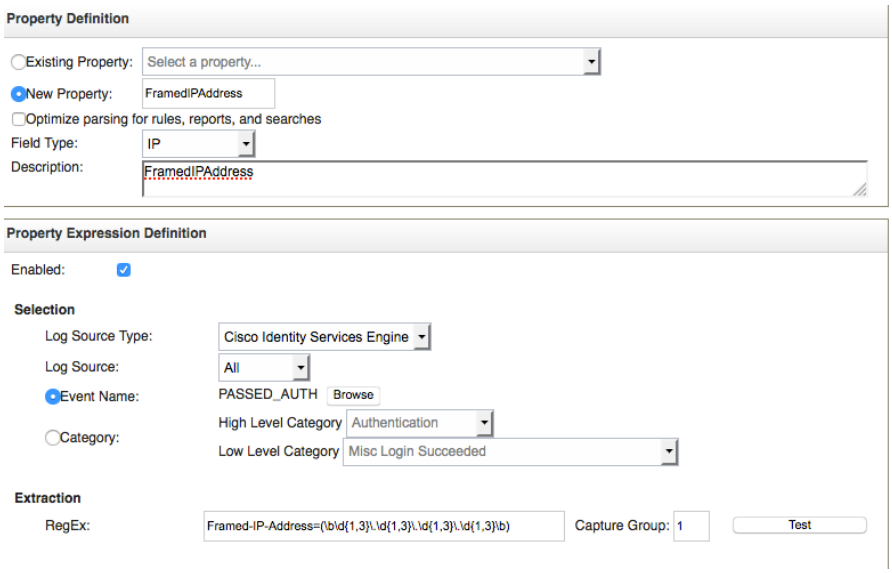
Step 7 Select **Passed Auth->Extract Property**

Step 8 For **New Property**, type: **FramedIPAddress**

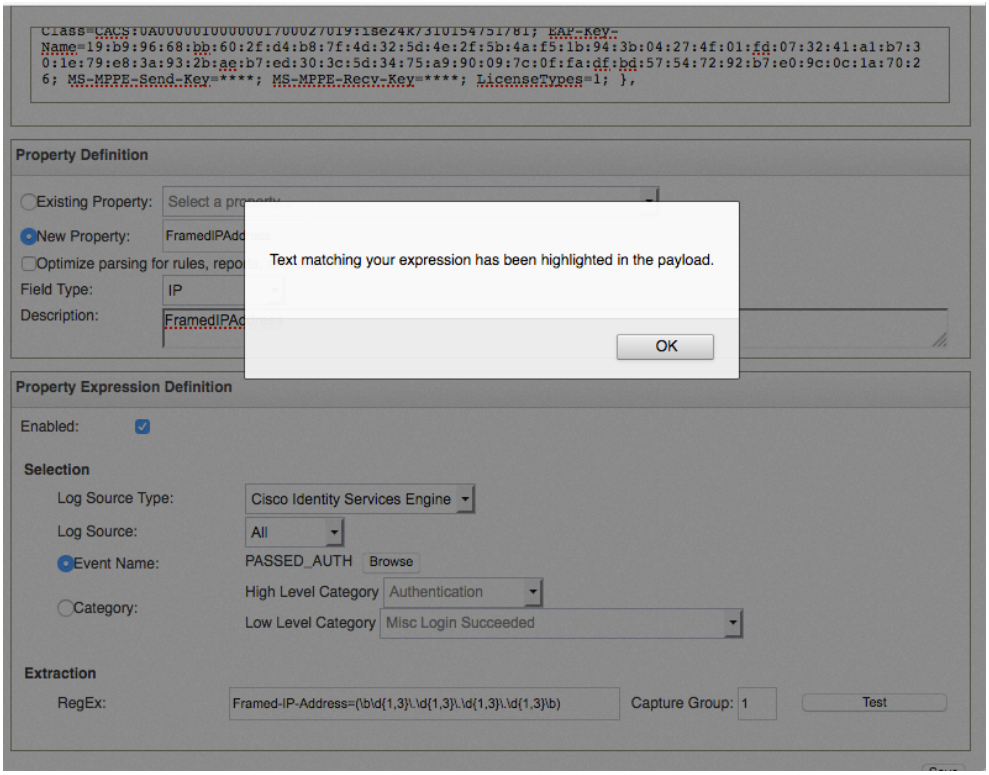
Step 9 For **Field Type**, type: **IP**

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:



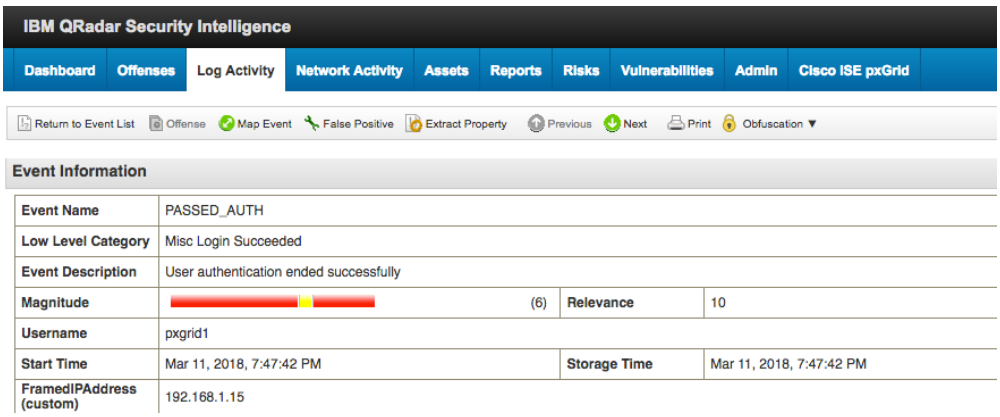
Step 12 Select **Test**
You should see



Step 13 Select **OK**

Step 14 Select **Save**

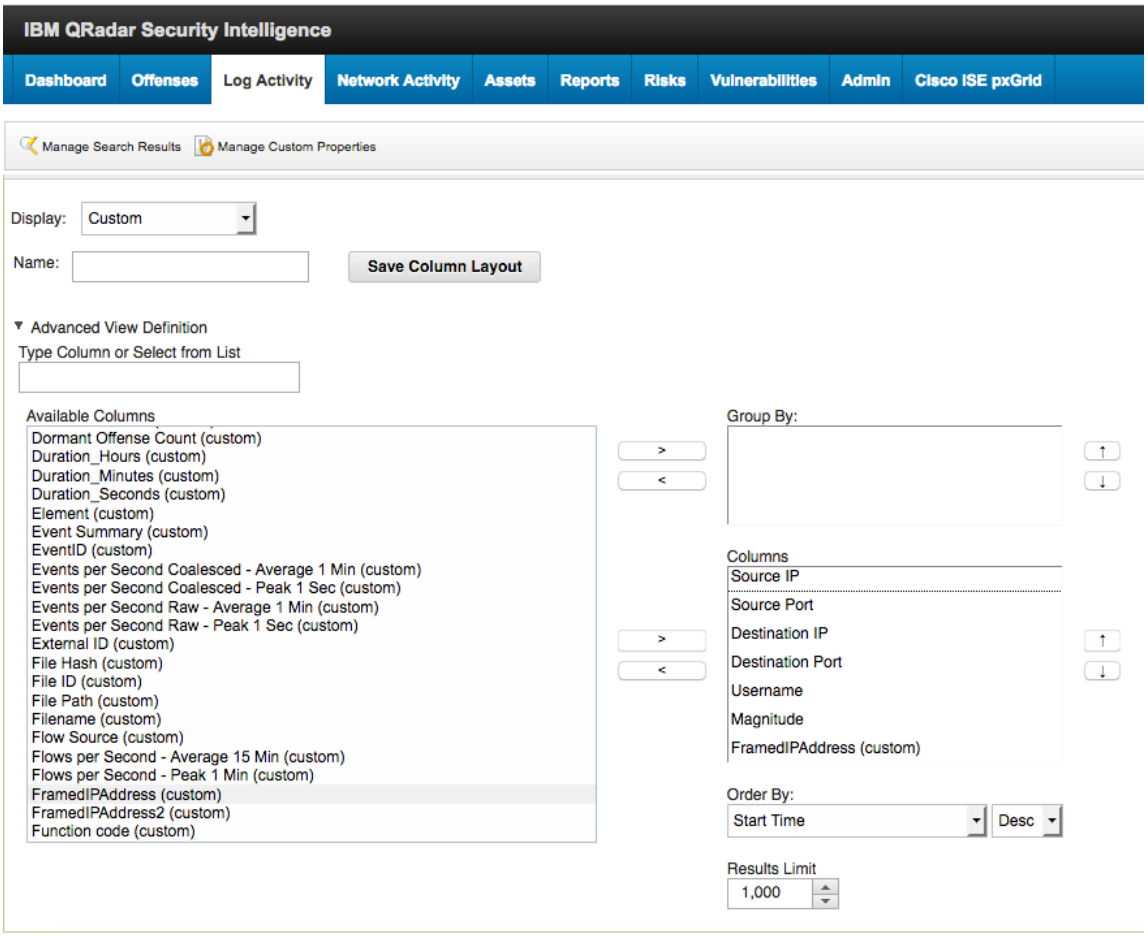
Step 15 Ensure you see you see the **FramedIPAddress** appear



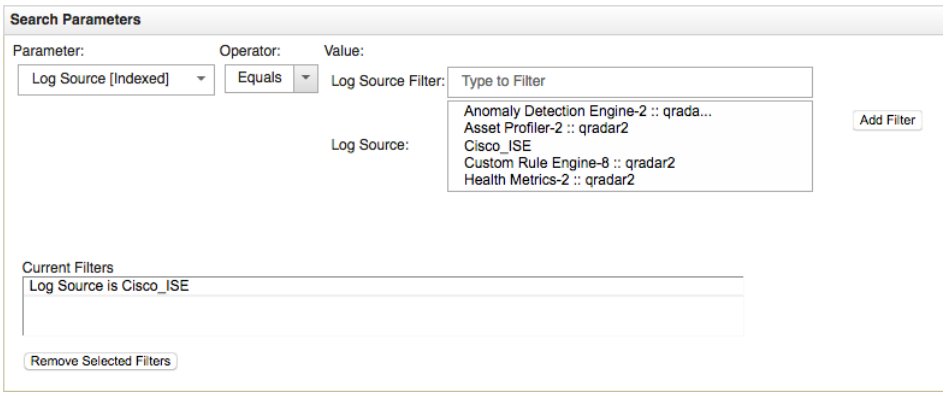
Step 16 Select **Return to Event List**

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 ">"**

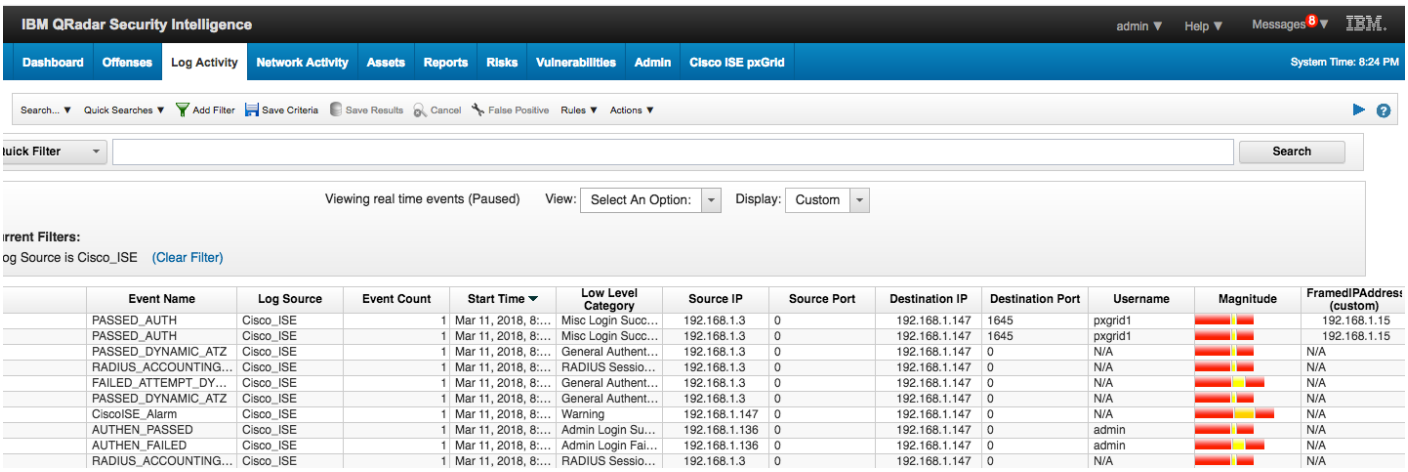


Step 19 Under **Search Parameters->Parameter->Quick Filters->Log Source (Indexed)->Equals->Log Source Filter->Cisco_ISE-Add Filer**



Step 20 Select **Filter**

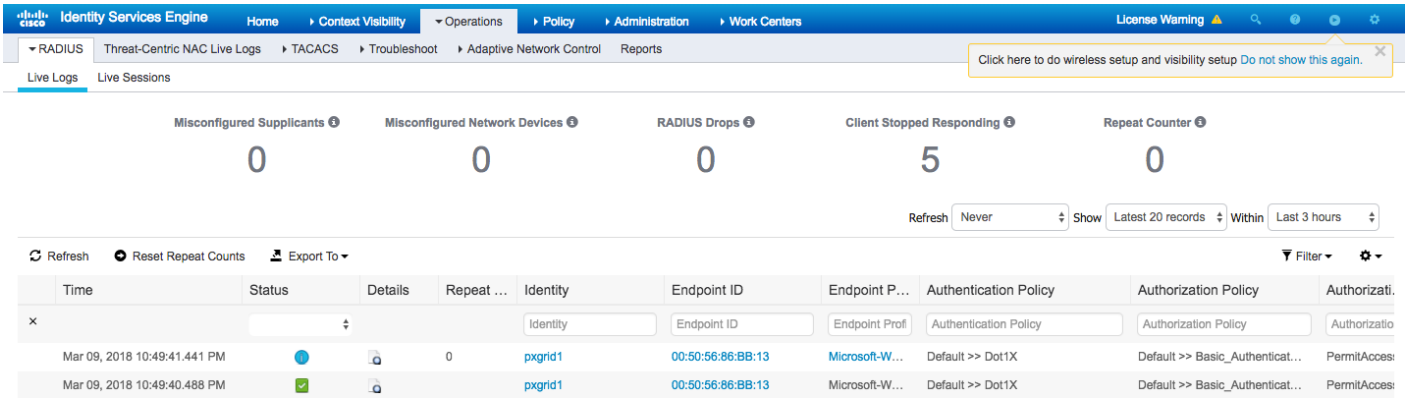
Step 21 You should see the custom FramedIPAddress field



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		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		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		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		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		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		N/A
CiscoISE_Alarm	Cisco_ISE	1	Mar 11, 2018, 8:...	Warning	192.168.1.147	0	192.168.1.147	0	N/A		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		N/A
AUTHEN_FAILED	Cisco_ISE	1	Mar 11, 2018, 8:...	Admin Login Fai...	192.168.1.136	0	192.168.1.147	0	admin		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		N/A

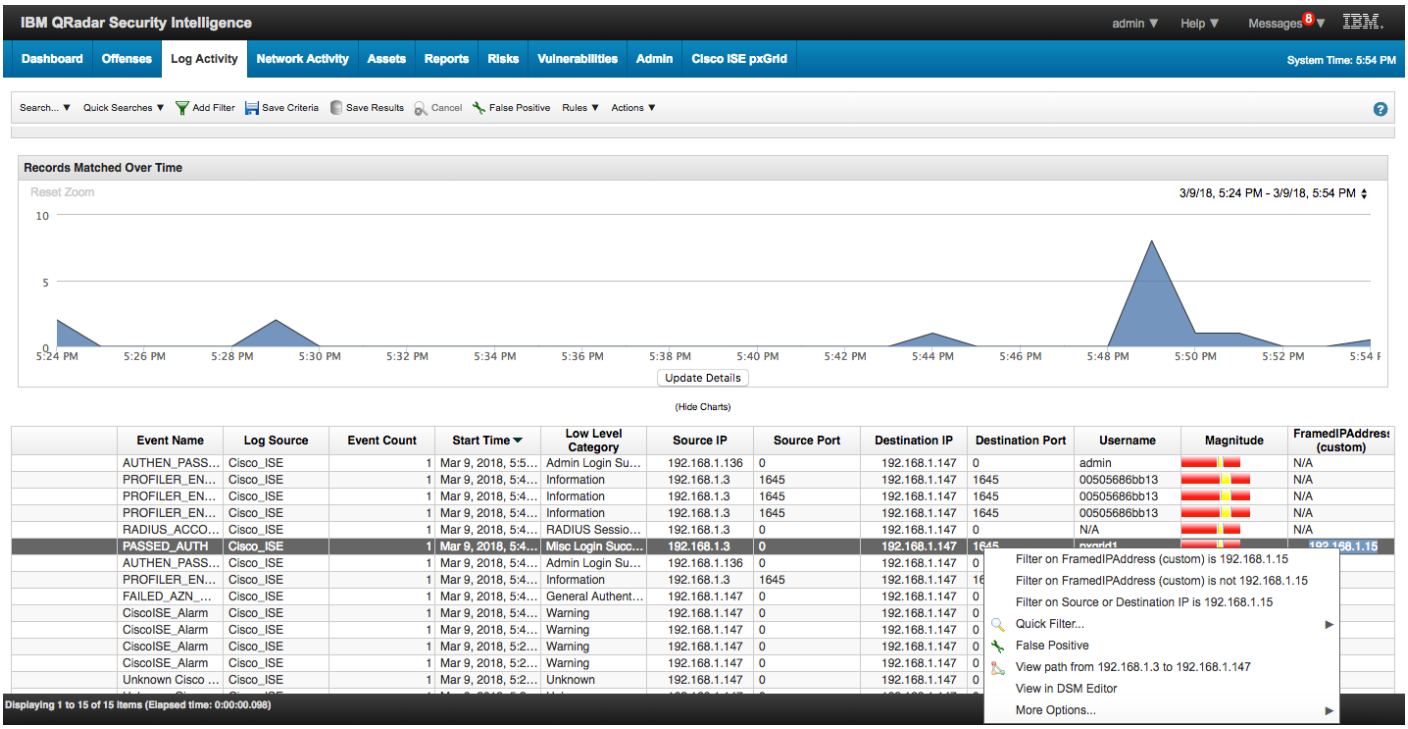
ANC Mitigation Syslog Event Example

Step 1 The user has been successfully authenticated through ISE

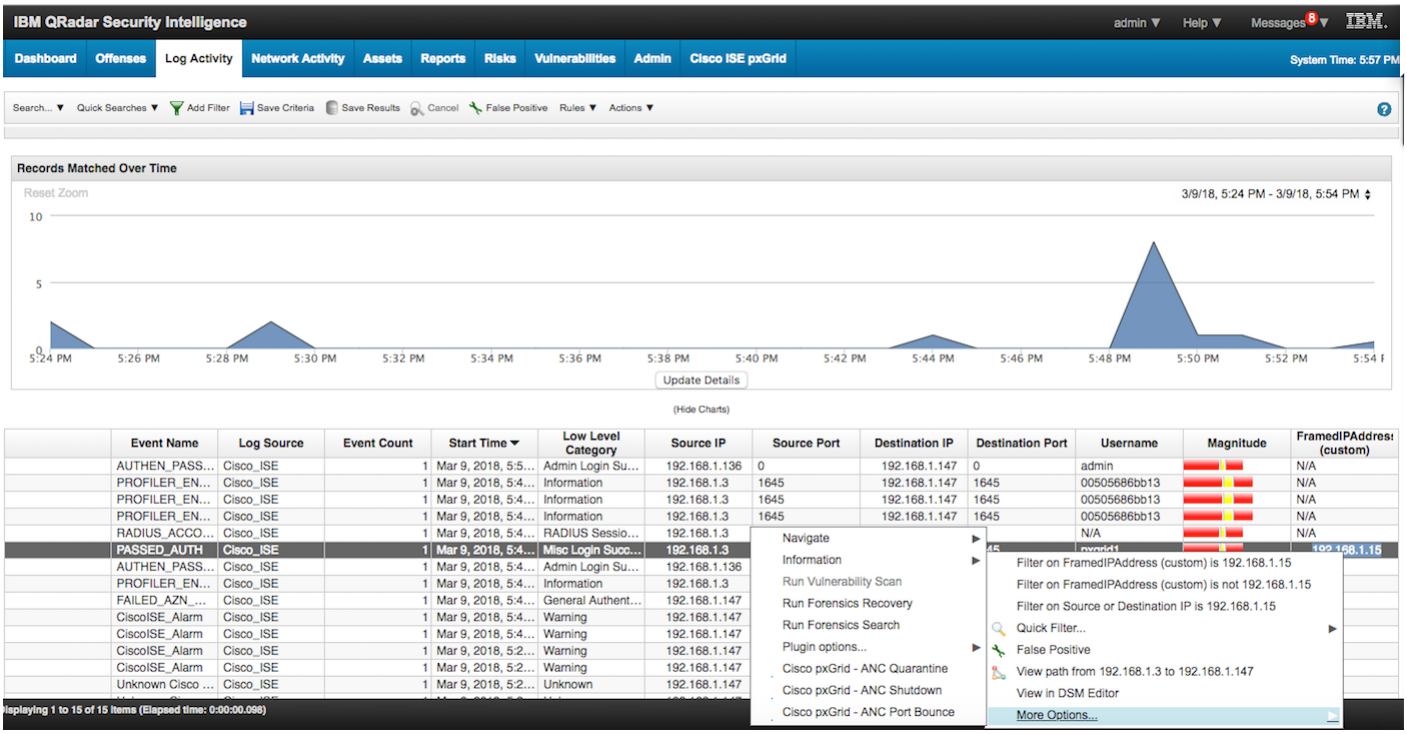


Step 2 In the QRadar, select the syslog event, Right-click on **FramedIPAddress** and select **More Options**
In the example below, a Passed authentication syslog event was received from ISE.

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



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

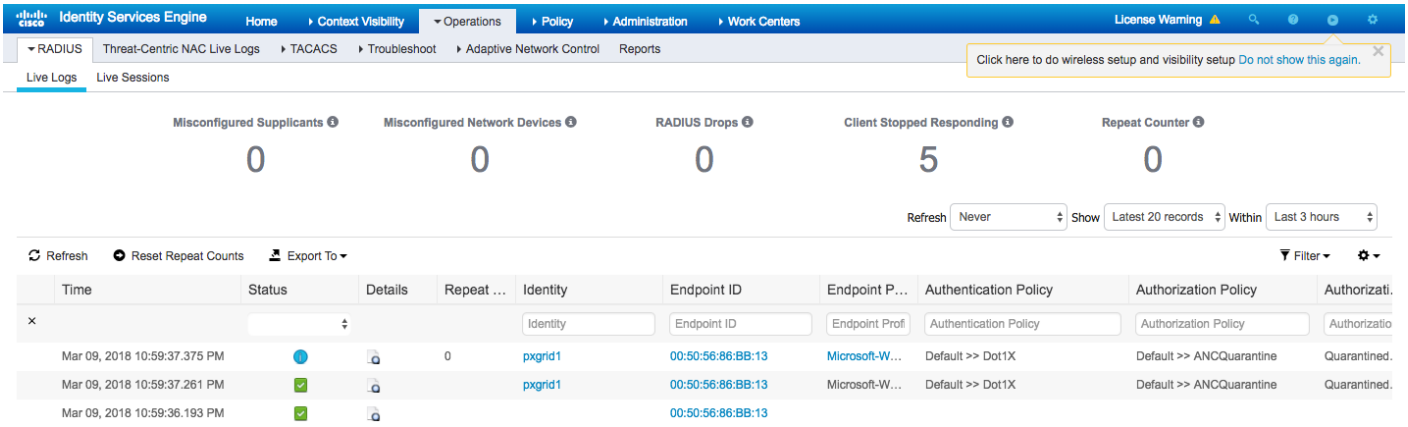


Step 4 You should see a successful status message

Step 5 Select **OK**

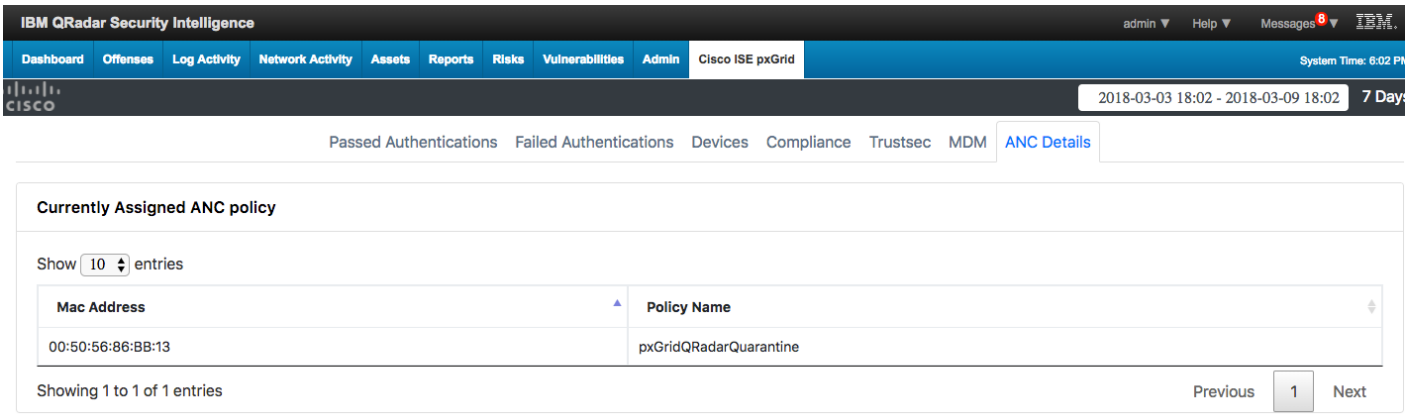
Step 6 To view in ISE, select **Operations->RADIUS->Live Logs**

You should see the quarantined endpoint designated by the ANCQuarantine Policy

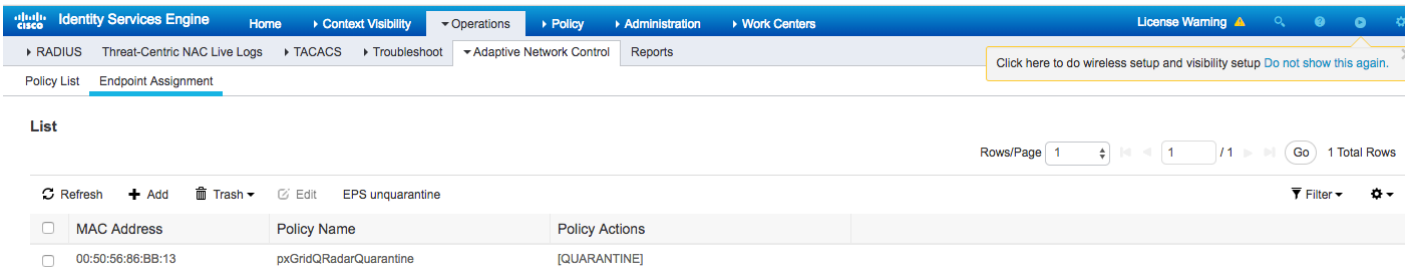


Step 7 To view in Cisco ISE pxGrid ANC Details Dashboard, select **Cisco ISE pxGrid-> ANC Details**

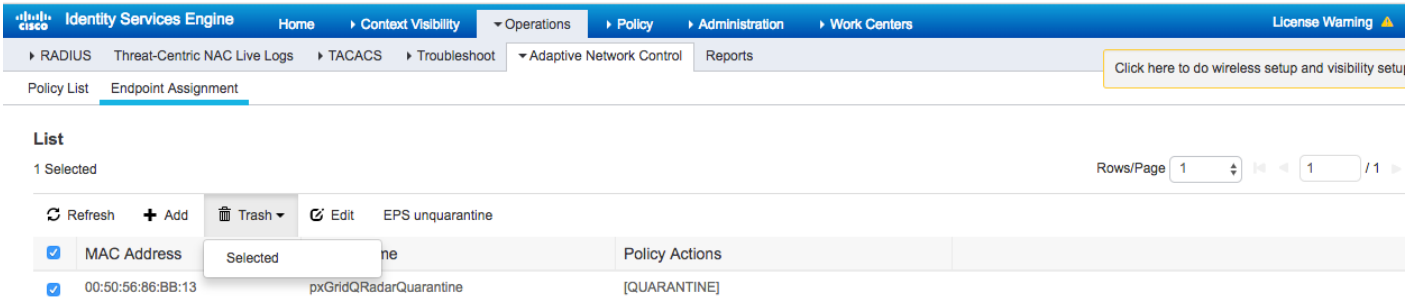
You should see the MAC address assigned to the ISE ANC policy name



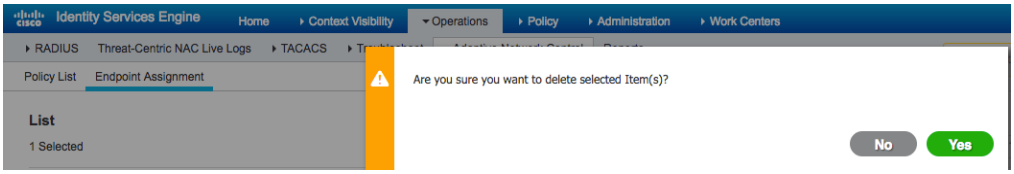
Step 8 To unquarantine, or clear the endpoint,
Select ISE->**Operations->Adaptive Network Control->Endpoint Assignment**



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

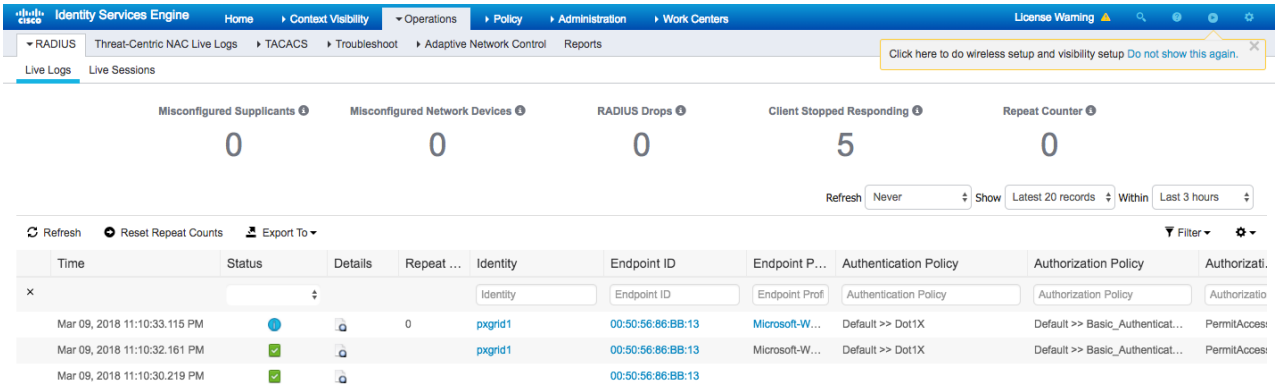


Step 10 Select selected, you should see:



Step 11 Select **Yes**

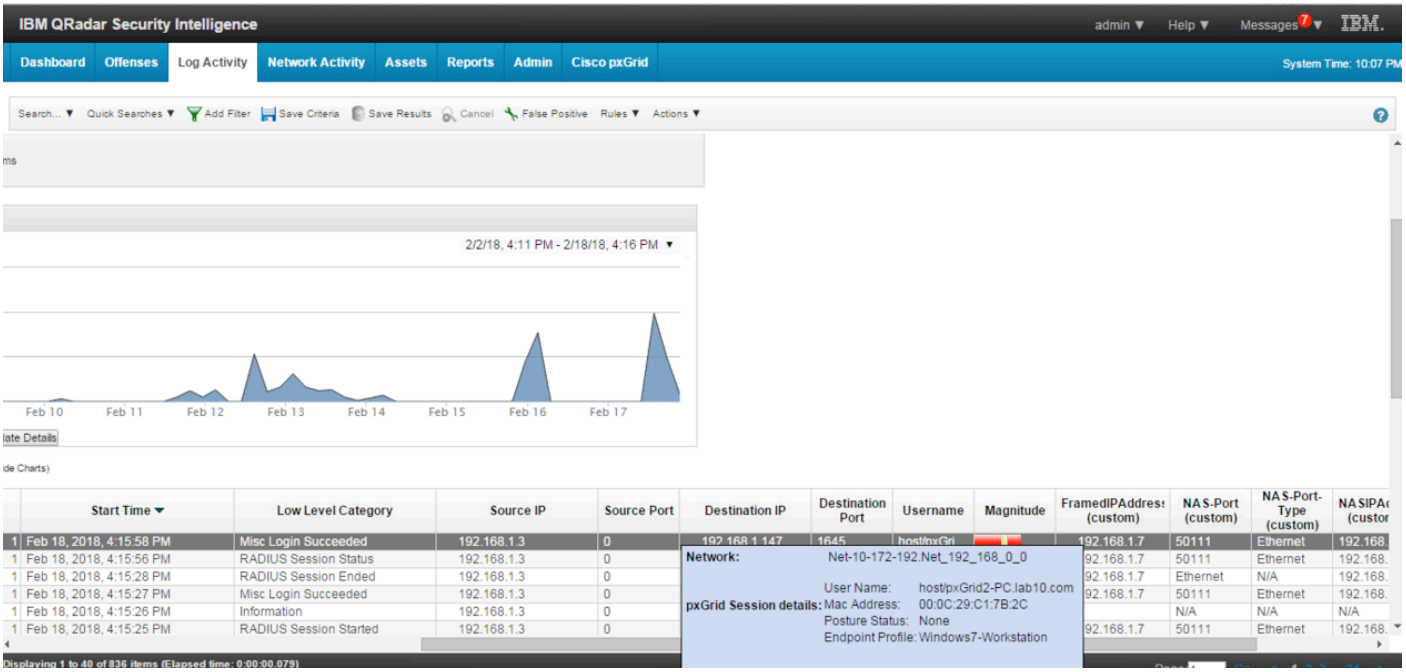
Step 12 In ISE, select **Operations->RADIUS-Live Logs**
You should that the endpoint has been unquarantined



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.



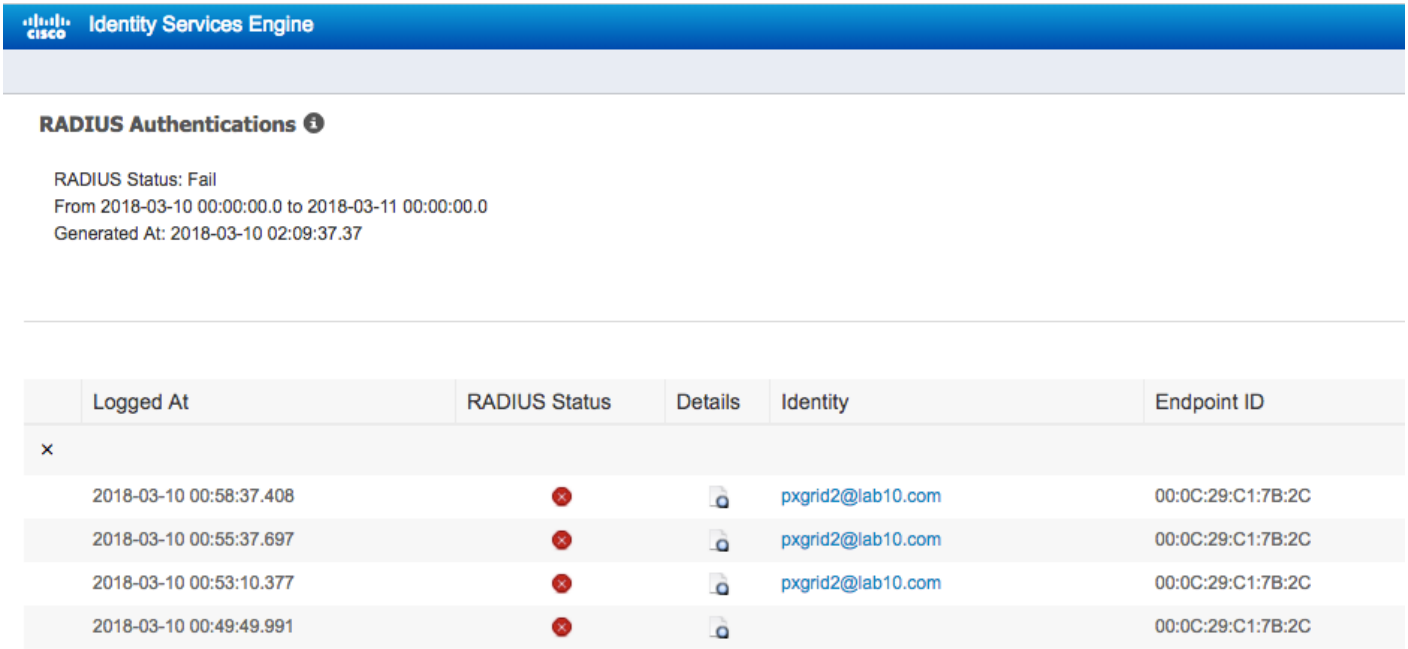
IBM QRadar Cisco ISE pxGrid Offense Rule

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.

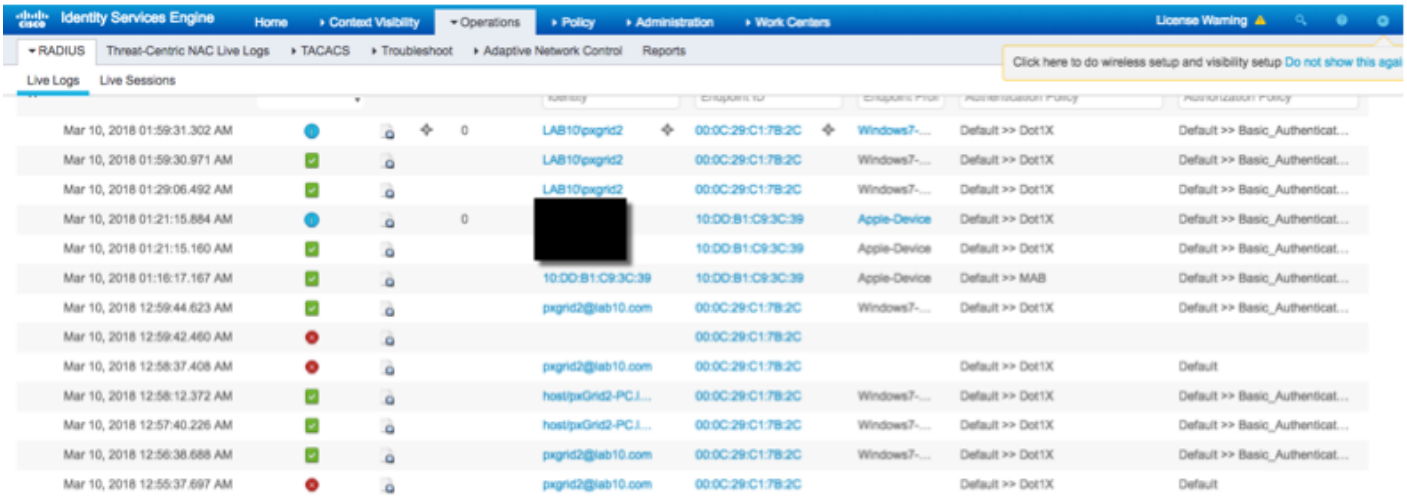
The Cisco pxGrid offense rule gets triggered when an event occurs the match Radius Failure session or simply 3 event s in the Cisco ISE pxGrid App Failed Authentication Dashboard from the same source IP address that occur within 10 minutes.

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

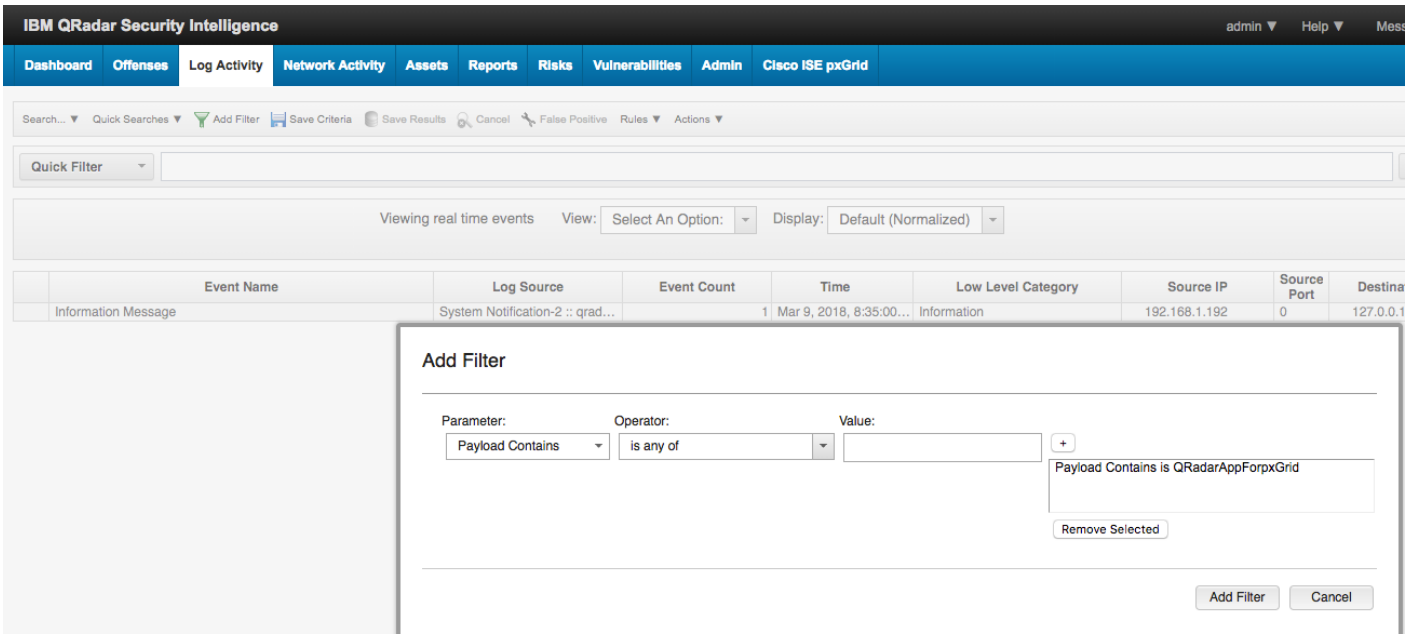


You can also view the events in ISE



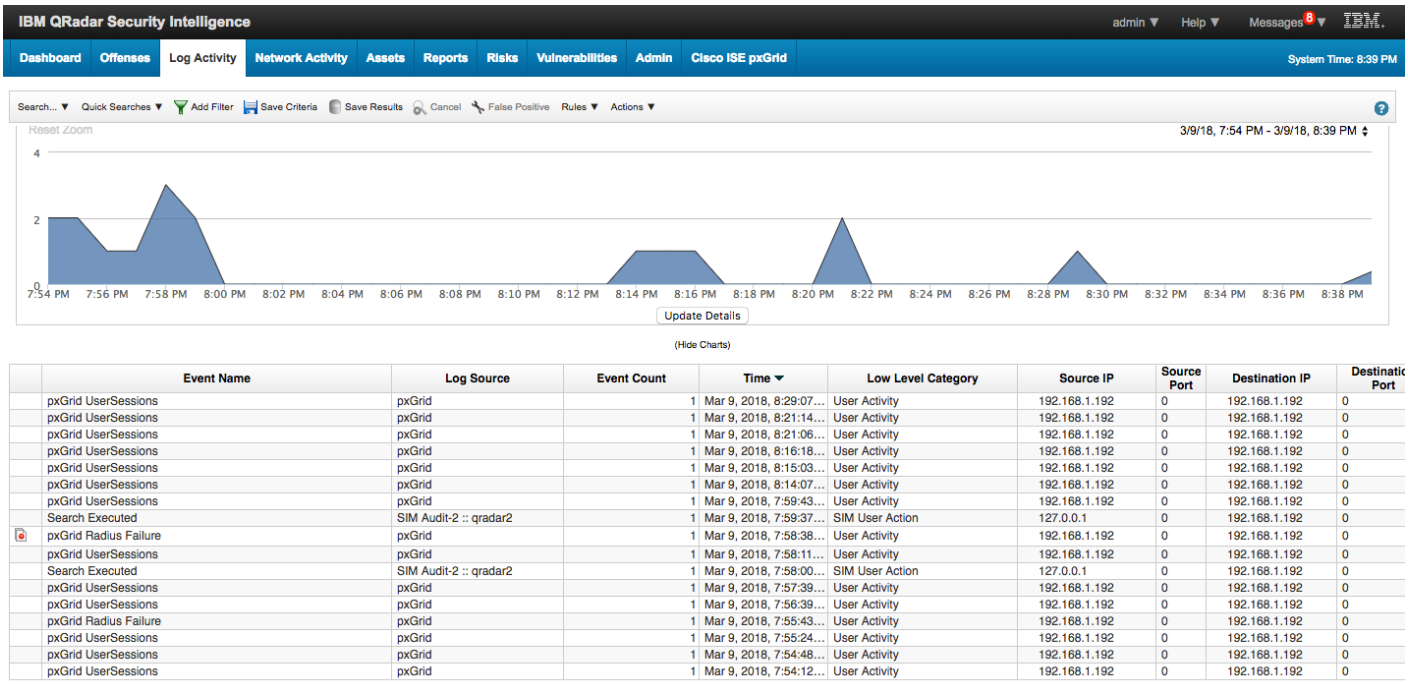
Verify pxGrid offense rule via Log Activity

Step 1 Select **Log Activity->Add Filter->Parameter->payload contains->Operator->is any of->Value->QRadarAppForPxgrid->"+"**



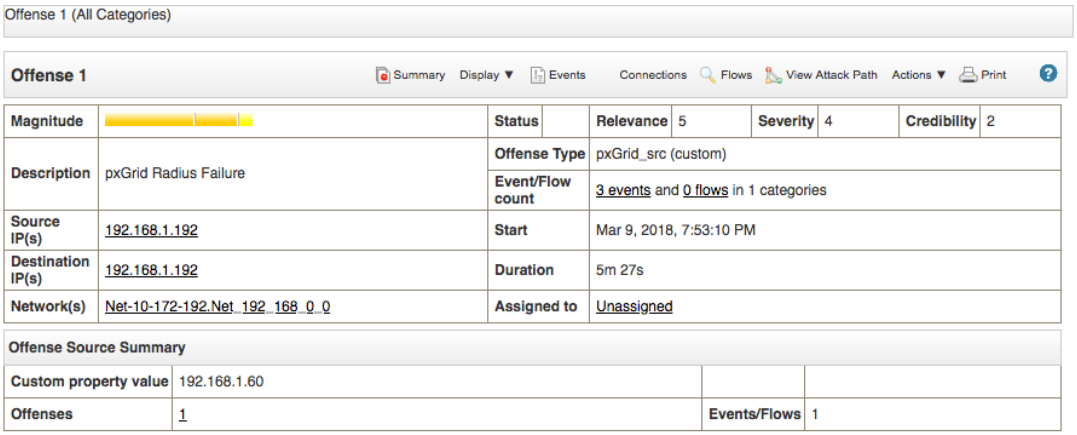
Step 2 Select **Add Filter**

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



	Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destinatio Port
	pxGrid UserSessions	pxGrid	1	Mar 9, 2018, 8:29:07...	User Activity	192.168.1.192	0	192.168.1.192	0
	pxGrid UserSessions	pxGrid	1	Mar 9, 2018, 8:21:14...	User Activity	192.168.1.192	0	192.168.1.192	0
	pxGrid UserSessions	pxGrid	1	Mar 9, 2018, 8:21:06...	User Activity	192.168.1.192	0	192.168.1.192	0
	pxGrid UserSessions	pxGrid	1	Mar 9, 2018, 8:16:18...	User Activity	192.168.1.192	0	192.168.1.192	0
	pxGrid UserSessions	pxGrid	1	Mar 9, 2018, 8:15:03...	User Activity	192.168.1.192	0	192.168.1.192	0
	pxGrid UserSessions	pxGrid	1	Mar 9, 2018, 8:14:07...	User Activity	192.168.1.192	0	192.168.1.192	0
	pxGrid UserSessions	pxGrid	1	Mar 9, 2018, 7:59:43...	User Activity	192.168.1.192	0	192.168.1.192	0
	Search Executed	SIM Audit-2 :: qradar2	1	Mar 9, 2018, 7:59:37...	SIM User Action	127.0.0.1	0	192.168.1.192	0
	pxGrid Radius Failure	pxGrid	1	Mar 9, 2018, 7:58:38...	User Activity	192.168.1.192	0	192.168.1.192	0
	pxGrid UserSessions	pxGrid	1	Mar 9, 2018, 7:58:11...	User Activity	192.168.1.192	0	192.168.1.192	0
	Search Executed	SIM Audit-2 :: qradar2	1	Mar 9, 2018, 7:58:00...	SIM User Action	127.0.0.1	0	192.168.1.192	0
	pxGrid UserSessions	pxGrid	1	Mar 9, 2018, 7:57:39...	User Activity	192.168.1.192	0	192.168.1.192	0
	pxGrid UserSessions	pxGrid	1	Mar 9, 2018, 7:56:39...	User Activity	192.168.1.192	0	192.168.1.192	0
	pxGrid Radius Failure	pxGrid	1	Mar 9, 2018, 7:55:43...	User Activity	192.168.1.192	0	192.168.1.192	0
	pxGrid UserSessions	pxGrid	1	Mar 9, 2018, 7:55:24...	User Activity	192.168.1.192	0	192.168.1.192	0
	pxGrid UserSessions	pxGrid	1	Mar 9, 2018, 7:54:48...	User Activity	192.168.1.192	0	192.168.1.192	0
	pxGrid UserSessions	pxGrid	1	Mar 9, 2018, 7:54:12...	User Activity	192.168.1.192	0	192.168.1.192	0

Step 4 Click on the offense rule 
You will see

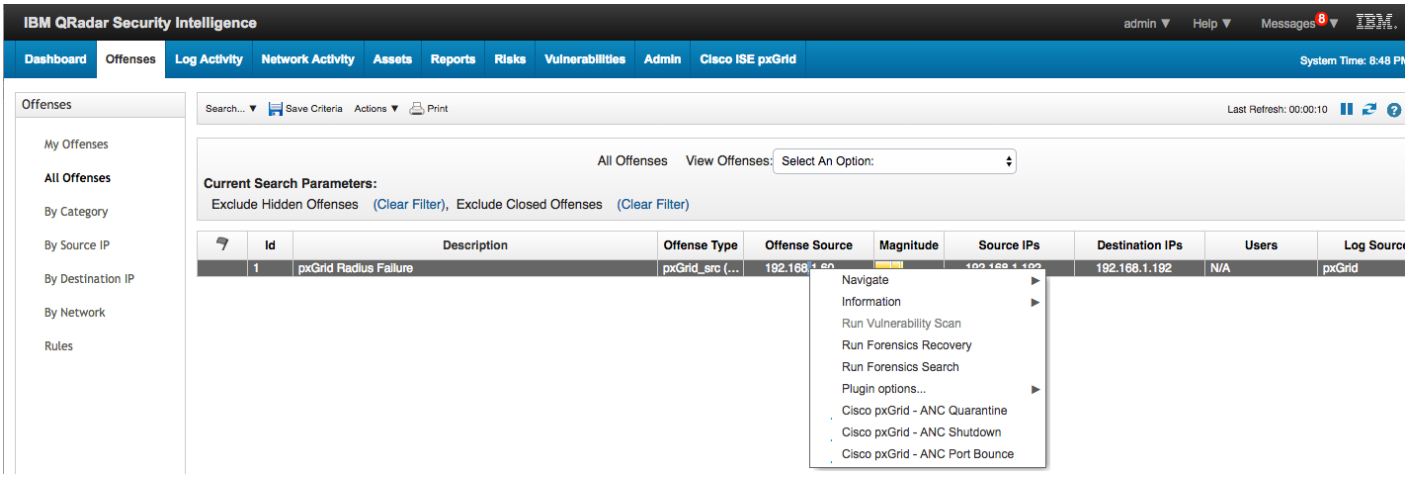


Verify pxGrid offense rule via Offenses Dashboard

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.

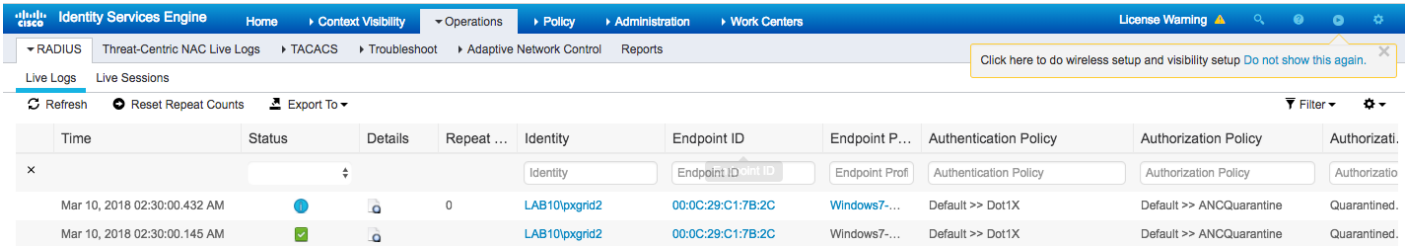


Step 2 This will trigger the ANC Quarantine, you should see

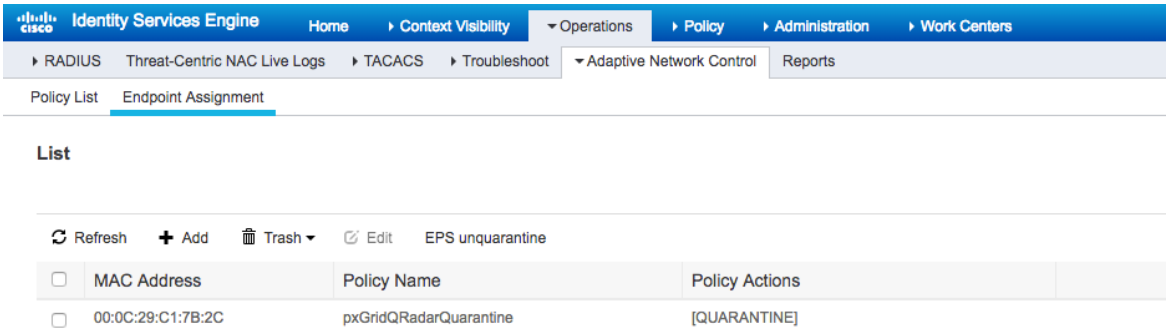
Step 3 Select **OK**

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

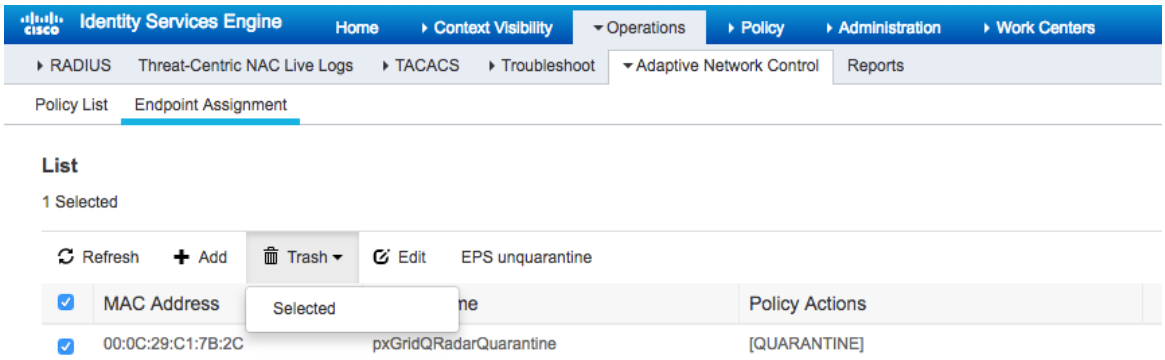
Note the endpoint has been quarantined as designated by the ANCQuarantine Authorization Policy



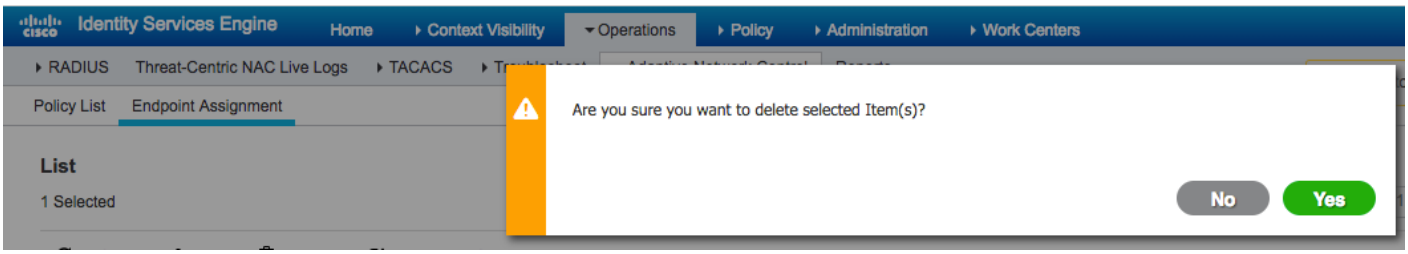
Step 5 To unquarantine or clear, select Operations->Adaptive Network Control->Endpoint Assignment



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

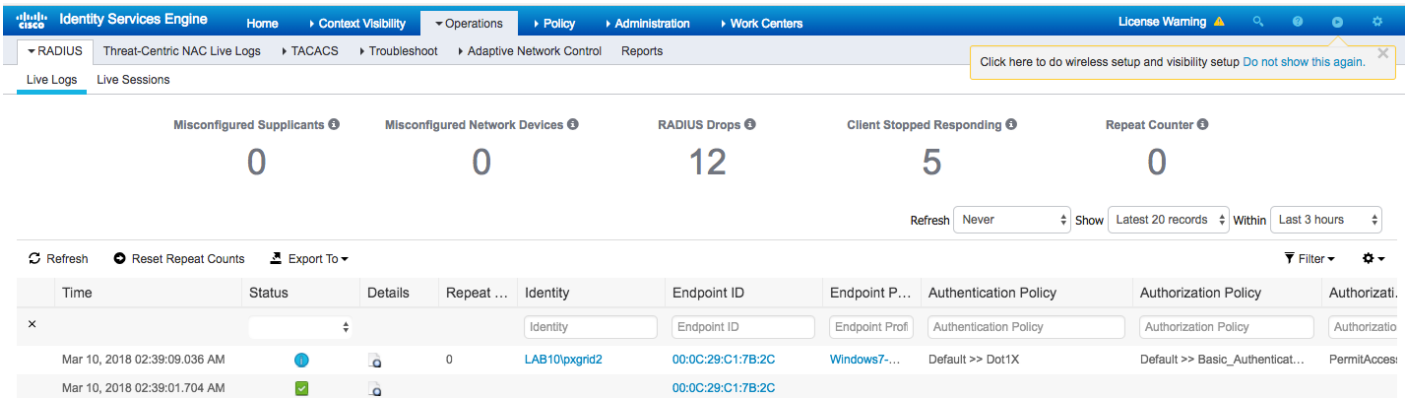


Step 7 Select->**Selected**

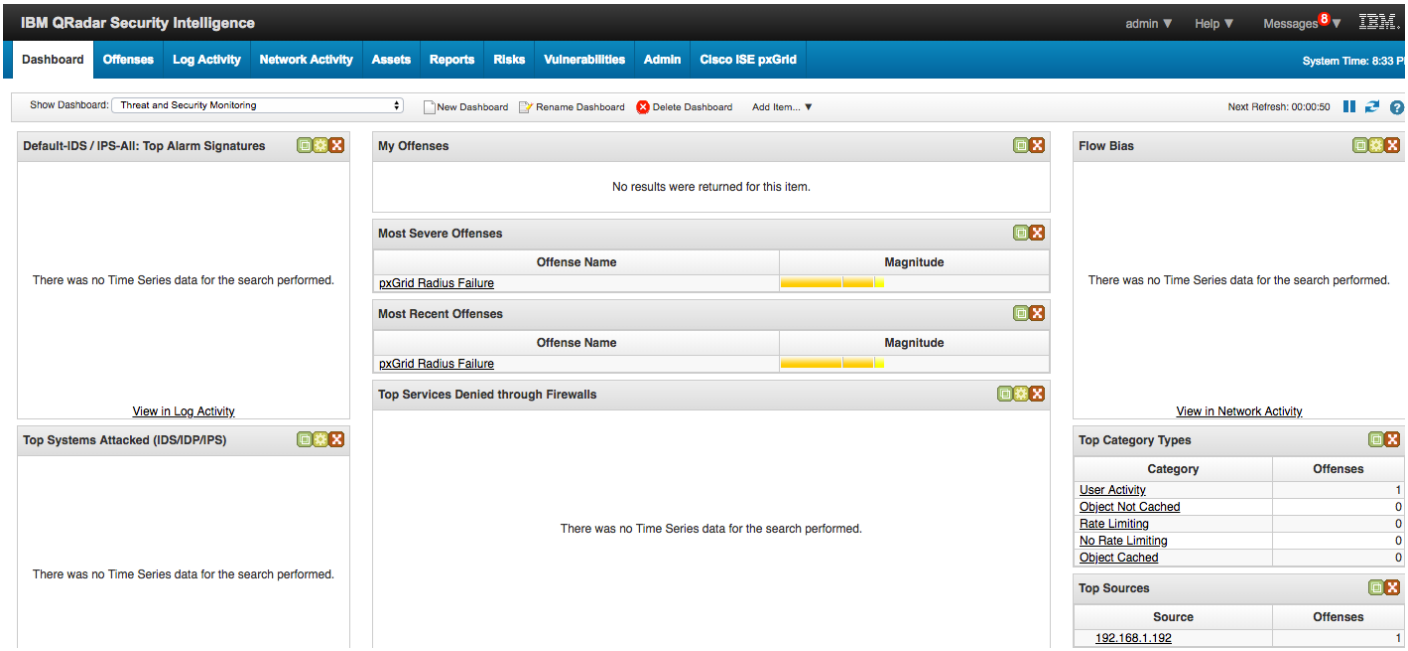


Step 8 Select **Yes**

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

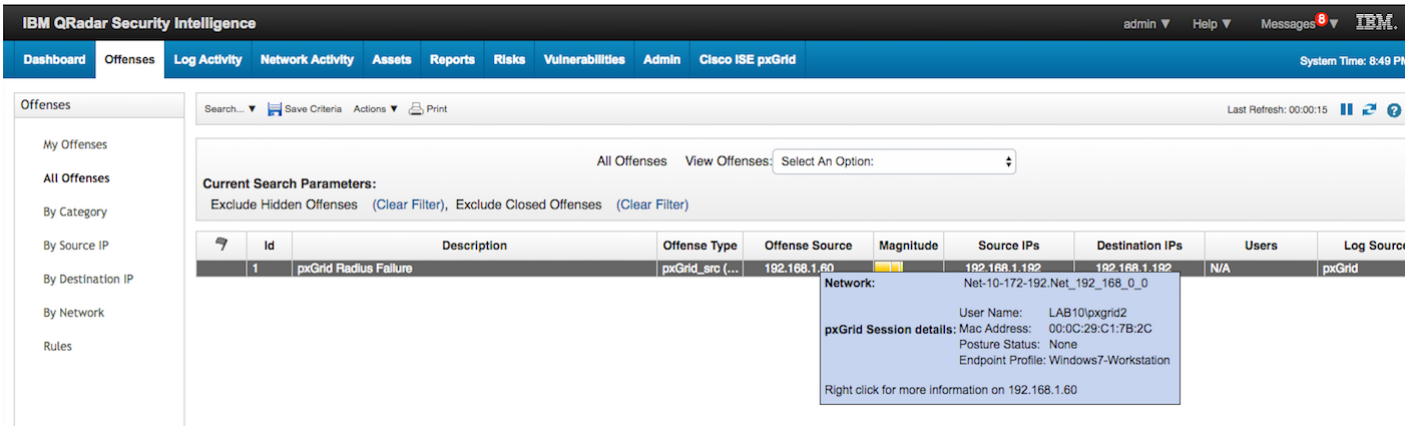


Step 10 Select **Dashboard**



Step 11 Select **pxGrid Radius Failure**

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



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