



Cisco ISE pxGrid App 2.0.0 for IBM QRadar SIEM

Updated: Jason Kunst

Updated - February 2021



Table of Contents

About This Document
Solution Overview
Technical Details
Cisco ISE pxGrid Installation
Generating the Cisco ISE pxGrid App Certificate 12
Installing Cisco ISE pxGrid App 16
Configuring pxGrid Integration on QRadar23
Setup Indexing in QRadar28
Cisco ISE pxGrid App Dashboard Panels
Search Functionality
Passed Authentications
Failed Authentications 35 User Panel 36 Failure Reason Panel 38 Device Type Panel 40 Locations Panel 43
Devices
Compliance
TrustSec
Mobile Device Management (MDM)55
ANC Details
Configuring Cisco ISE Adaptive Network Control Policies
Configuring Default ANC policies for Cisco ISE pxGrid App57
Adding ANC Policies to ISE Policy Sets59
Performing Cisco ISE ANC Mitigation Actions Through Cisco ISE pxGrid App Dashboard Panel 61

cisco.

Configuring IBM QRadar for Cisco ISE Syslog Events67
Configuring Cisco ISE Syslog Events
Performing ISE ANC Mitigation Actions Through IBM QRadar Syslog Events
Creating Custom Field for Framed IP Address ISE Syslog Event
Hovering Over IBM QRadar Syslog IP Address for ISE Contextual Information
IBM QRadar Cisco ISE pxGrid Offense Rule
Verify pxGrid offense rule via Log Activity88
Verify pxGrid offense rule via Offenses Dashboard90
Taking ISE ANC mitigations from Offenses Dashboard90
Addendums
Adding Log Activity Filter to View Session Information96
Using an External Certificate Authority97
Generating IBM QRadar Certificate from ISE Internal CA100
Troubleshooting
Cisco ISE pxGrid App pxGrid client not showing under ISE pxGrid Client View
Cisco ISE pxGrid App pxGrid client not showing under ISE pxGrid Web Client View
Cisco ISE pxGrid Dashboards not populating with ISE Contextual Information105
ANC Mitigation Actions not appearing in Dashboards105
Using the IBM QRadar pxGrid App Logs for Troubleshooting106
TCP Dump to Analysis Failed Certificate Exchange in ISE111
TCP Dump to Check if pxGrid Logs are Available in QRadar112
Uploading Logs with the case112

About This Document

This document is for Cisco System Engineers, IBM Engineers, Partners, and Customers deploying the Cisco Identity Services Engine (ISE) Cisco Platform Exchange Grid (pxGrid) App v2.0+ for IBM the QRadar SIEM.

The supported platforms are:

- IBM QRadar SIEM 7.3.1 patch 7 and higher
- Cisco ISE 2.4 and higher with latest patch
- Note: Please keep up with latest patches and recommended releases, as of October 2020 it is ISE 2.7 patch 2

Validation has been done with the following for this release:

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

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

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

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

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

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

Solution Overview

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

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

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

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

Technical Details

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

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

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

The following image is a single standalone:

cisco	Identity Services Eng	gine Home	Context Visibility	Operations	+ Policy + Adi	ministration + Work Co	nlers		
+ Sy	stem 🔸 Identity Manag	ement Network F	Resources + Device	e Portal Managemer	nt pxGrid Services	+ Feed Service + Th	eat Centric NAC	Click he	re 1o do wireles
All	Clients Web Clients	Capabilities Liv	e Log Settings	Certificates Pr	ermissions				
								Rows/Page 6	J
C I	Refresh								
	Client Name	Connect To	Session Id	Ce	ertificate	Subscriptions	Publications	IP Address	Status
×	Client Name		<u>.</u>					IP Address	
	ise-fanout-ise24k	ise24k	ise24kc0	CN	(=ise24k	/topic/wildcard		127.0.0.1	ON
	ise-mnt-ise24k	ise24k	ise24k:1	Ch	l=ise24k.	/topic/com.cisco.ise.se	/topic/com.cisco.ise.se		ON
	ise-fancut-ise24k	ise24k	ise24k2	Ch	∉≕se24k.	/topic/distributed	/topic/distributed		ON
	ise-admin-ise24k	ise24k	ise24kc3	CN	l≈ise24k.				ON
	ise-bridge-ise24k	ise24k	ise24k:5	Ch	l≈ise24k.				ON
	CiscolSEpxGridApp	ise24k	ise24k:6	Ch	v=qradar	/topic/com.cisco.ise.se			ON
					ha ha ha ha	pioloom.cisco.ise.session, pioloom.cisco.ise.radius.faih pic ym.cisco.ise.config.anc.statu pioloom.cisco.ise.mdm.endp	ure, s, point		

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

dentes Iden	ntity Services Engine	Home Conte	xt Visibility > Operations	▶ Policy ▼Admi	nistration • Work Center	5	
 System 	Identity Management	Network Resources	Device Portal Managem	nent pxGrid Services	+ Feed Service + Threat	Centric NAC	
All Clients	s Web Clients Capat	bilities Live Log	Settings Certificates	Permissions			
Senable	O Disable O Approve	😝 Group 🏾 🎈 Decline	🕄 Delete 👻 🛞 Refresh	Total Pending Approval(0)	*		1 - 15 of 15
Chi	ent Name	Description	Capabilit	ies	Status	Client Group(s)	Auth Method
D 🕨 ise	-bridge-ise3		Capabilit	ies(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate
D 🕨 ise	i-admin-ise		Capabilit	ies(4 Pub, 2 Sub)	Online (XMPP)	Internal	Certificate
D 🕨 ise	-admin-ise4		Capabilit	ies(0 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate
🗆 🕨 ise	i-admin-ise2		Capabilit	ies(1 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate
□ ► ise	-admin-ise3		Capabilit	ies(0 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate
🗆 🕨 ise	-fanout-ise4		Capabilit	ies(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
□ ► ise	-pubsub-ise4		Capabilit	ies(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
□ ► ise	-mnt-ise		Capabilit	ies(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate
🗆 🕨 ise	-bridge-ise		Capabilit	ies(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate
🗆 🕨 ise	-pubsub-ise3		Capabilit	ies(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
□ ► ise	-fanout-ise3		Capabilit	ies(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
□ ► ise	-fanout-ise		Capabilit	ies(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
□ ► ise	-pubsub-ise		Capabilit	ies(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
🗆 🕨 ise	-bridge-ise4		Capabilit	ies(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate
D 🕨 ise	-mnt-ise2		Capabilit	ies(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate
4							
Connected v	via XMPP ise3 securitydemo	net (standby: ise4)					

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

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

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

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

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

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

Cisco ISE pxGrid Installation

Make sure that you have installed Cisco Identity Services (ISE) 2.4 or higher and it is in a stand-alone deployment (also supports other deployment methods). If this is a production ISE deployment, ensure the Cisco ISE pxGrid node is on a dedicated node, see <u>How to Configure pxGrid in ISE Production</u> <u>Environments</u>.

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



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

Step 2 Select Save



You should see the following:



ace Identity Services Engine Home	+ Context Visibility + Operations + Policy + Administration + Work Century	-	00	nse Warning 🔺	- 4. O	0 9
System + Identity Management + Network Deployment Licensing + Certificates +	KResources + Device Portal Management pxGrid Services + Feed Service + Thread Cogging + Meintenance Upgrade + Backup & Restore + Admin Access + Settings	Sentric NAC	Click here to do wireless setup	and visibility se	tup Do not show	this again.
Deployment	Deployment Nodes				Belected 0 Total	**.
	🖉 fidit 🔯 Register 🧑 Syncup 🖉 Deregistar		Sh	All we		1.0.0
 Deployment 						. 0
Deployment Selector PAN Failover	Hostname + Personas	Role(s)	Services		Node Status	. 0

Recommended Distributed deployment example:

				Selected 0 Total 4
/ Edit 🔯 Register	Syncup Deregister		Show	Al
Hostname	 Personas 	Role(s)	Services	Node Status
ise ise	Administration, Monitoring	PRI(A), PRI(NONE	S
ise2	Administration, Monitoring	SEC(A), SEC	NONE	
ise3	Policy Service, pxGrid		SESSION, PROFILER	2
ise4	Policy Service, pxGrid		SESSION, PROFILER, DEVICE AD	MIN 🔽

Step 3 Select Administration > pxGrid Services

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

- Note: XMPP is for pxGrid 1.0 and for releases prior to ISE 3.0 the All Clients page doesn't provide the best view. You should look at the Web Clients view below.
- Step 4 Select **Web Clients** and verify the published nodes appear:
 - **Note:** This is validating pxGrid 2.0 connections. You should see admin, mnt, and pxGrid nodes have connections with each other. They should all be **ON**.

SECURE ACCESS HOW-TO GUIDES



alsola casco	Identity Services E	ngine Ho	me + Context Visib	olity Operations	Policy Administration	Work Centers		
+ Sy	stem 🔹 Identity Man	agement + Ne	twork Resources	Device Portal Management	pxGrid Services + Feed	Service + Threat Centric M	NAC .	
×	Client Name		¥				IP Address	~
	ise-mnt-ise	ise4	ise4.1	No Certificate	Apploicom.cisco.ise.s.	Appicicom.cisco.ise.s	10.1.100.21	ON
	ise-admin-ise	ise4	ise4:2	CN=ise security			10.1.100.21	ON
	ise-admin-ise3	ise4	ise4:3	CN=ise3.securit			10.1.100.23	ON
	ise-admin-ise2	ise4	1504.4	No Certificate			10.1.100.22	ON
	ise-admin-ise4	ise4	ise4.6	CN=ise4.securit			10.1.100.24	ON
	ise-fanout-ise4	ise4	ise4:8	CN=ise4.securit	.#opic/wildcard	Appicicom cisco ise s	127.0.0.1	ON
	ise-fanout-ise3	ise3	ise3:0	CN=ise3.securit	Appic/wildcard	Appic/com.cisco.ise.s	127.0.0.1	ON
	ise-bridge-ise3	ise3	ise3:1	CN=ise3.securit			127.0.0.1	ON
	ise-fanout-ise3	ise3	ise3:2	CN=ise3.securit	/topic/distributed	AppicIdistributed	10.1.100.23	ON
	ise-fanout-ise4	ise3	ise3:4	CN=ise4.securit	Apploidistributed	Apploidistributed	10.1.100.24	ON
	ise-mnt-ise2	ise3	ise3:5	No Certificate	Appicicom cisco ise s	Appiolcom cisco ise s	10.1.100.22	ON

Generating the Cisco ISE pxGrid App Certificate

A certificate for the Cisco ISE pxGrid App will be generated from the ISE internal CA so the App will register and connect to the ISE pxGrid node. If you are using an external CA server for pxGrid operation, please see <u>How to Configure pxGrid in ISE Production Environments</u>.

For more information on certificates please reference this section under cs.co/ise-guides.

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

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

Step 1 Select Administration > pxGrid Services > Certificates

dentity Services Engine	Home	Operations Policy Adm	inistration Work Centers
System Identity Management	Network Resources	Portal Management pxGrid Services	Feed Service Threat Centric NAC
All Clients Web Clients Capabiliti	es Live Log Settings	Certificates Permissions	
Generate pxGrid Certificate	S		
I want to	• [·
Common Name (CN)	•		
Certificate Templat	e PxGrid_Certificate_Templati	0	
Subject Alternative Name (SAN) 🔄 🗌	- +	
Certificate Download Format	•		· 0
Certificate Password	•		0
Confirm Password	•		
			Reset Create
Connected to pxGrid ise24k.lab10.com			

You should see the following:

Step 2 Type the following:

Recommended to use the full name of the server ex: qradar.securitydemo.net

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

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

Common Name (FQDN): qradar.securitydemo.net

Description: QRadar

Certificate Template: Pxgrid_Certificate_Template

Subject Alternative Name (IP Address): 10.1.100.27

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

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

Certificate Password: xxxxxxx

Confirm Password: xxxxxx

Step 3 Select Create

This will create a zipped file 1520701037382_cert.zip

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

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



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

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

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

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

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

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

€ → ୯ û	🛛 🔏 😂 https://9.21.118.93/admin/#administration/administration_system/administration_system_certificates/certificates_cert_mgmt/certificates_cert_mgmt_system_certs						
dealer Identity Services Engine	Home	+ Context Visibility + Operations +	Policy Administratio	m + Work Centers			
System + Identity Management	+ Network F	Resources + Device Portal Management	peGod Seneces + Fee	d Service + Threat Centric NAC			
Deployment Licensing Certific	ates + Log	gging + Maintenance Upgrade + Ba	ckup & Restore + Admin	Access + Settings			
Certificate Management System Certificates	System	n Certificates 🛕 For disaster recovery # 1	s recommended to export o	certificate and private key pairs of all syste X Deleter P Vew	m certificates.		
Trusted Certificates		Friendly Name	UsedBy	Ponal group tag	Issued To	Numer By	
OCSP Client Profile	▼ tp0.	1					
Certificate Signing Requests		OU+ISE Messaging Senice, CN+bp02.ca nlab.itm.com#Certificate Senices Endp oint Sub CA - bp02#00003.	ISE Messaging Service		bp02.cantab.itm.com	Certificate Services Endpaint Sub CA - 8 p52	
Certificate Periodic Check Sett Certificate Authority	OU=Certificate Services System Certificate to CH+tp02 cantals item com#Certificate Insurant Endexent But C4 - te02900002		psGnd		6p02 canitab ibm com	Certificate betwices Endpoint But CA- p52	
		Default self-signed sami server certificat + - CNsrG488, 3x002 castab ibm com	DAML.		SAML_bp02 caniab ibm com	SAML_bp02.carilati.ibm.com	
		Default self-argred server certificate	Admin, Portal, EAP Authentication, RADRUS DTLS	Default Portal Certificate Group T	bp02 caniab itm.com	bp02 cantab /bm.com	

- Step 5 Decrypt the file on the QRadar box:
 - **a.** Using WinSCP Copy the gradar.securitydemo.net_gradar.securitydemo.net.key to the QRadar Setup

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

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

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

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

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

- **d.** Refresh your WinSCP and copy the key file back (not the .org) to the same windows location overwriting the key file
- e. Close your WinSCP and SSH sessions to QRadar server
- Note: You will need to upload these six certificates when configuring the Cisco ISE pxGrid App for pxGrid integration

Installing Cisco ISE pxGrid App

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

To download the app, please visit the <u>IBM App Exchange</u>.

Note: It is assumed that <u>QRadar Ver 7.3.1p7</u> and above has been installed along with Patch 7.

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

To uninstall the old app:

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

Extensions Management	Search by extension name
ALL ITEMS INSTALLED NOT INSTALLED	
Name	
Cisco ISE pxGrid The Cisco ISE pxGrid App uses Cisco Identity Services Engine (ISE) 2.4 + Grid (pxGrid) to orchestrate all communication and data interchange / exc ISE. This provides ISE contextual information from within the QRadar com provide key information such as Passed and Failed authentications, Devi MDM. It also allows the QRadar admin to take right-click Adaptive Networ Rapid Threat Containment (RTC).	and leverages Cisco Platform Exchange change between IBM QRadar and Cisco sole. The App has dashboards that ce Summary, Compliance, TrustSec and k Control (ANC) mitigation actions for
	(More Details)

Step 1 Install the extension:

a. From IBM QRadar, select Admin > Extensions Management



≡ IBM QRadar							
Dashboard Offenses	Log Activity	Network Activity	Assets	Reports	Admin	Pulse	
Admin	() Deple	oy Changes Advanced	•				
▼ System Configuration	(j) Ther	e are no changes to	deploy.				
 User Management Assets 						Reasons	
► Data Sources		-	001	n		-90	
Remote Networks and		E	12			S and a second s	
Services Configuration	Ro	outing Rules	Domain Man	agement	Extensi	ons Management	Re
Try it out							
► Apps	User N	lanagement					

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

Extensions Management	Search by extension name	Q	IBM Security App Excha							
ALL ITEMS IN STALLED NOT INSTALLED Add										
Name		Status	Author	Added On 👻						
QRadar Log Source Management	a New Extension		IBM QRadar	May 5, 2020						
QRadar Assistant App	n local storage:		IBM QRadar	May 5, 2020						
QRadar Pulse - QRadar v7.3.0+	io_ISE_pxGrid_V2.0.0_03092020.zip	Browse	IBM QRadar	May 5, 2020						
	Add	Cancel								

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

① 🗞 https://	nsionsManagementConsole			🛡 🕁 🗄
Extensions Management	Search by extension name	٩		IBM Security App Exchange
ALL ITEMS INSTALLED NOT INSTALLED				Add
Name		Status	Author	Added On 🗸
Cisco ISE pxGrid		Installed	Cisco	April 22, 2018

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

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

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

≡ IBM QRadar							
Dashboard Offenses	Log Activity	Network Activity	Assets	Reports	Admin	Pulse	
Admin • System Configuration	C Deploy	Changes Advanced are no changes to	deploy.				
Data Sources Events Flows	Data Sources Events						
 Vulnerability Remote Networks and Services Configuration Try it out 	DS	M Editor	WinCo	ollect	L	og Sources	

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

Choose Name > pxGrid_Primary/pxGrid_Secondary

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

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



🚯 Log Sources - Go	💱 Log Sources - Google Chrome —									
Not secure 192.168.1.233/console/do/sem/maintainSensorDevice										
Search For: Group 🗸 All Log Source Groups 💿 Go 🗋 Add 💕 Edit 🖾 Enable/Disable 🔕 Delete Bulk Actions 🔻									0	
Name	Desc	Status	Protocol	G	Log Source Type	Enabled	Log Source Identifier	Target Destination	Credibi	Autodiscov
pxGrid_Primary	Cisco ISE	Success	Syslog		Clsco ISE pxGrid	True	primary	eventcolle	5	False
pxGrid_Secondary	Cisco ISE	Success	Syslog		Clsco ISE pxGrid	True	secondary	eventcolle	5	False

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

Search For: Name	_ gx0nid	Go Add Fat Enabl	e.Disable 🙆 Delete Bulk	Actions 🔻 🍃	Edensions	📥 Parsing Ord	er 🍘 Assign	0
Name 🔺	Desc	Status	Protocol	Group	Log Source Type	Enabled	Log Source Identifier	Target Destinatio
pxGrid	Cisco ISE pxGrid Log Source for pri	Error	Syslog		Clsco IS	True	primary	eventcoll
pxGrid	Cisco ISE pxGrid Log Source for se	Error	Syslog		Clsco IS	True	secondary	eventcoll

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

Edit a log source							
When the connection information for this log source is shared amongst one or more other log sources.							
ERROR - Events have not been received from this Lo	ERROR - Events have not been received from this Log Source in over 720 minutes.						
Log Source Name	pxGrid						
Log Source Description	Cisco ISE pxGrid Log						

- d. Change your log source identifiers for QRadar 7.4
- The app opens in a new window.
- Choose Log source type to filter on pxGrid.



IBM QRadar Log Source M	anagement				
Filter Status (5)	Clear 0	Search by name, description or log source identifie	ĸ	Q	+ New Log Source
Warning	0	Log Sources (2)	7		<u> </u>
Not Available	0	D Name ^	Log Source Type	Creation Date Last Eve	nt Enabled
Enabled (2)	0	262 pxGrid_Primary	Clsco ISE pxGrid	Aug 12, 2020 7:52 AM Sep 1, 20	20 5:48 AM 🛛 📀
Ves	2 0	212 pxGrid_Secondary	Clsco ISE pxGrid	Feb 10, 2020 10:53 PM Aug 24, 2	2020 6:33 AM 🛛 📀
Log Source Type (9)	2	20 v items per page 1-2 of 2 items			1 of 1 pages < 1

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

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

Log Source Summary		×
E Claco ISE pxGrid Status: Error	L	primary ast Updated 9 hours ago
Events have not been received from Overview Protocol	n this Log Source in over 720 minutes.	
	*	1
Log Source Identifier*	10.1.100.23	
Incoming Payload Encoding	1177 A	
Cancel		Save

• Close the second browser tab.

SECURE ACCESS HOW-TO GUIDES



Dashboard	Offenses	Log Activity	Network Activity	Assets	Reports	Admin	Pulse			
Admin • System (Configuration	O Depk	oy Changes Advanced to changes to c	leploy.						
 User M Assets Data Sou 	lanagement	System User M	Configuration lanagement							
Remote Services Try it ou	Networks and Configuration t		Users	0 User	Roles	Sec	urity Profiles	Authentication	Christian Services	
► Apps										

Step 3 Configure the Authorized Services in QRadar:

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

Dashboard	Offenses	Log Activity	Network Activity	Assets	Reports	Admin	Pulse			
Admin • System (• User M • Assets	Configuration lanagement	C Depic	oy Changes Advanced e are no changes to Configuration	deploy.						
 Data Sou Remote 1 Services Try it out Apps 	rces Networks and Configuration t	User M	Users	i User	Roles	Sec	urity Profiles	Authentication	Conthorized Services	Ten

- b. Add Authorized Service:
- In the Service name box, enter pxGridService
- For both the User Role and Security Profile drop-down list boxes, select Admin (default)
- Enable No for Expiry

Service Name:	pxGridService		
User Role:	Admin 🔸		
Security Profile:	Admin 🚽		
Expiry Date:	2/13/2018	*	/ 🗹 No Expiry

c. Click Create Service

d. Copy the authentication token into the notepad

Add Authorized Service	O Delete Authorized Service	Edit Authorized Service Name Selected To	ken b72cfcac-3c5b-42c1-b0	65-80752eb270e2		0
Service Name	Authorized By	Authentication Token	User Role	Security Profile	Created	
Local Health Console	configservices	51402167-3daf-49d6-8a2f-7ffDa9eefac5	Admin	Admin	Aug 4, 2018, 11:55:00	Permar
APPS	admin	617ed99a-a536-441f-9f2b-a68e9491fe3c	Admin	Admin	Aug 4, 2018, 10:21:34	Permar
pxGridService	admin	9b0fe499-3ab2-4f47-9f8a-0ccb179f3ab3	Admin	Admin	Sep 27, 2018, 2:35:45	Permar
WinCollect Agent	admin	e18fc295-da10-4aa1-8623-168bc7a46277	WinCollect	Admin	Sep 27, 2018, 10:45:24	Permar
AdminToken	admin	70a0efee-f9e0-44a0-af95-86bf3261f258	Admin	Admin	Feb 28, 2020, 11:57:50	Feb 4,
pxgrid	admin	b72cfcac-3c5b-42c1-b065-80752eb270e2	Admin	Admin	Jul 1, 2020, 3:55:54 PM	Permar

						0
Add Authoria	ted Service 🙆 D	elete Authorized Se 8e-b424971c3c	rvice 📝 Edit Au a8	thorized Service Na	me Select	ed
(1) Authorized	I service added.	Click Deploy Ch	anges to apply	the changes.		
Service Name	Authorized By	Authentic Token	User Role	Security Profile	Created	Expires
pxGridService	admin	da9dt225-2	Admin	Admin	Sep 24, 202	Permanent

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

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



Configuring pxGrid Integration on QRadar

- Step 1 Setup pxGrid settings:
- a. Select Admin > Apps > Cisco ISE pxGrid > pxGrid Settings



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

uluulu cisco		
	ApplicationSettings Primary Sec	condary
	QRadar service token	*****
	Time interval to invoke the scheduler in minutes	5
	Cisco application version	v1
	QRadar event collector	192.168.0.110
		Submit and Test Connection

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

- Step 3 Select **Submit and Test Connection**, you should see a successful connection in a pop-up window
- Step 4 Select **Primary**, and type the **IP address** of the ISE pxGrid node
- Step 5 Leave **8910** as the port default
- Step 6 Enter the Client username (for example, QRadar App)

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

Step 7 Upload all (selecting all in the browse windows at once) the Cisco ISE pxGrid App certificates in PEM format under **Select and Upload Certificates** (only PEM is supported) application settings page

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

- Step 8 Type in the Cisco ISE pxGrid App Certificate file name: qradar.lab10.com_qradar.lab10.com.cer
- Step 9 Type in the Cisco ISE pxGrid App Certificate key file name: qradar.lab10.com_qradar.lab10.com.key
- Step 10 Type in the Cisco ISE Internal Root Certificate Root CA certificate file name: qradar.lab10.com_qradar.lab10.com.key

You will see the following:

ApplicationSetting	s Primary	Secondary		
Primary pxGrid Serve	r IP Address			
port •		8910		
Client user name		CiscolSEpxGridAppFCLab		
Select & Upload cert PEM is supported)	ificates(only	Browse		
Certificate file name		gradar3.	cer	
Certificate key file na	ime *	qradar3.	key	
Root CA certificate fi	le name *	CertificateServicesRootCA	cer	

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

- On any ISE deployment you could have multi certificates for different roles personas.
- The admin node with an internal PKI cert so that your admin machines with the root trust them.
- Portals for guest services would likely have a well-known certificate so that any client coming in off the street can trust the portal.
- Your pxGrid node will likely be side either by ISE internal CA or a well-known certificate root, depending on how you certificate trust is set up. Carefully choose your Root in the setup settings.
- All nodes running pxGrid should have the same root.
- See more about certificates at the <u>ISE Guides page for certificates</u> and the <u>ISE 2.7 Certificate</u> <u>Section of Admin Guide</u>.
- Step 11 At the bottom of the page, select **Submit and Test Connection**. Then you should see a successful connection message. If a secondary connection exists, do the same.
- Note: If adding a secondary pxGrid node, provide the secondary pxGrid Server IP Address, the Client username and identity certificate, and public private key-pair. The root certificate will remain the same as in Primary.
- Step 12 Validate the pxGrid client on ISE:
- a. In your browser, open ISE and log in
 - b. Select Administration > pxGrid Services
 - c. On the All Clients tab, you should see your QRadar pxGrid client (pending)

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



dentity Services E	ngine Home + Context Visibilit	Y + Operations + Polic	Administration	Vork Centers	
System Identity Man All Clients Web Clients	agement + Network Resources + De s Capabilities Live Log Setting	vice Portal Management gxG s Certificates Permissi	rid Services + Feed Service	Threat Centric NAC Click here	to do visibility setup Do not s
Inable ODisable OAp	oprove 🔒 Group 🁎 Decline 🔞 Delete 🔹	Refresh Total Pending Appr	oval(1) =	1 selecteditern	1-8 of 8 Show 25 +
Client Name	Description	Cap Approve Al	Status	Client Group(s)	Auth Method
Ise-mnt-ise		Capacitorio Ad	Sub) Online (XMPP)	Internal	Certificate
Ise-fanout-ise		Capabilities(0 Pub, 0	Sub) Online (XMPP)	Internal	Certificate
Ise-pubsub-ise		Capabilities(0 Pub, 0	Sub) Online (XMPP)	Internal	Certificate
ise-bridge-ise		Capabilities(0 Pub, 5	Sub) Online (XMPP)	Internal	Certificate
Ise-adminise		Capabilities (5 Pub, 2	Sub) Online (XMPP)	Internal	Certificate
🗹 🕨 qradar	pXGrid App for Qradar	Capabilities(0 Pub, 0	Sub) Pending		Certificate
□ ► ise-srp-ise		Capabilities(1 Pub, 1	Sub) Online (XMPP)	Internal	Certificate
Stealthwatch		Capabilities(0 Pub, 4	Sub) Online (XMPP)	ANC	Certificate

- d. Click Approve All as you should see just one pending client
- Note: On the All Clients tab, the Client Status can be Offline (XMPP). This is for pxGrid 1.0 and doesn't represent any value. ISE 3.0 has a different view to better represent the setting, but we don't address it here.

Step 13 Select Web Clients and see registered Cisco ISE pxGrid QRadar app client

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

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



-0.46- 0.007	Identity	Services Engi	ne	Home + C	ontext Visibility	Operations	+ Policy	• Administration	Work Centers			•	o, o
• S)	rstem	 Identity Mana 	geme	ent 🔸 Network Res	sources + Devic	e Portal Manageme	nt pxGrid	Services + Feed	ervice		Click here to do visit	vility setup Do not show	this again.
AI	Clients	Web Clients	c	apabilities Live L	Log Settings	Certificates	Permissions			Rows/	Page 2	1 퀸/1	Go 2
0	Refresh												▼ Filter
	Client	Name		Connect To	Session Id	0	ertificate	Subscri	tions		Publications	IP Address	Status
×	Grada	r	×	•								IP Address	
	Gradar			ise	ise:16	0	N≈qradar Φ	/topic/co	n. cisco. ise. session /lopic/com. cisco Aopic/com. cisco. ise. sessio	ise.radius.failure,/topic/		198.19.10.18	OFF o
	Gradar			ise	ise:17	0	N=qradar	/hopic/co	Appic/com cisco ise radius Appic /com cisco ise config anc.s Appic /com cisco ise mdm endpo	s.failure, s.failure,/topic/ status,		196.19.10.18	ON

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

Step 14 Assign the QRadar client to the ANC Group permissions

a. Select All Clients > Check the QRadar Client

- b. Group > Add > ANC
- c. Click Save

Client Group		×
Name	qradar	
Groups	ANC	
		Save Cancel

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

Setup Indexing in QRadar

Following are the steps to Index CEPs in QRadar.

Step 15 Return to the IBM QRadar

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

	E		200	Cert	~	200	1000
Auto Update	Backup and Recovery	Global System Notifications	Index Management	Aggregated Data Management	Network Hierarchy	System and License Management	System Health
1	国田	18.	8.		<u></u>		
System Settings	Asset Profiler Configuration	Custom Offense Close Reasons	Store and Forward	Reference Set Management	Centralized Credentials	Forwarding Destinations	Routing Rules
	-	6					
Domain Management	Extensions Management	Resource Restrictions					

Step 17 To setup the Indexes for use with pxGRid:

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

🥝 Enable Index 🛛 😣 Dis	able Index pxgri	<u>ب</u> ل
------------------------	------------------	------------

b. Sort by Property:

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

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

Recommended CEPs to be indexed are the following:

- pxGrid_adNormalizedUser
- pxGrid_auditSessionId
- pxGrid_EventName
- pxGrid_macAddress
- pxGrid_nasPortType
- pxGrid_src
- d. Click Save

Cisco ISE pxGrid App Dashboard Panels

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

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

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

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

Search Functionality

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

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

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

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



≡	IBM QRadar									Ļ	<u> </u>
Dast	nboard Offenses Log Activity Network /	Activity Assets	Reports A	Idmin Pre-Validation	Cisco ISE pxGrid					System Time:	2:27 PM
ciso	0 10							2020-09-02 14:27 - 2020	0-09-03 14:27	Reset	
		Search Pa	assed Auther	ntications Failed Au	thentications Devic	es Compliance Trus	tsec MDM ANC D	etails			
*.	*	Ses	ssion	~	September 2, 2020 14	4:27 - September 3, 202	0 14:27 🋗	Search			
	Search Result: Search criteria return more rec	ords. The first 200 rec	ords are display	red.						Export	
	Dev Time	IP Address 🔅	State 🔅	MAC Address	Username 🕴	Calling Station ID 🔅	Called StationID 🔅	NAS IP Address	Raw Data	¢	
	02-Sep-2020 09:12:19.597 GMT+5:30	192.168.1.254	STARTED	20:A6:CD:C9:D9:00	20:A6:CD:C9:D9:00	20:A6:CD:C9:D9:00	C0:67:AF:A8:6E:11	192.168.0.217	View Raw Deta	ails	
	02-Sep-2020 09:12:26.564 GMT+5:30	192.168.1.128	STARTED	20:A6:CD:C9:D9:00	20:A6:CD:C9:D9:00	20:A6:CD:C9:D9:00	C0:67:AF:A8:6E:11	192.168.0.217	View Raw Deta	ails	
	02-Sep-2020 09:12:41.085 GMT+5:30	10.235.24.6	STARTED	02:8F:A5:7E:9C:8A	02:8F:A5:7E:9C:8A	02:8F:A5:7E:9C:8A	C0:67:AF:A8:6E:11	192.168.0.217	View Raw Deta	ails	
	02-Sep-2020 09:12:49.602 GMT+5:30	192.168.1.254	STARTED	20:A6:CD:C9:D9:00	20:A6:CD:C9:D9:00	20:A6:CD:C9:D9:00	C0:67:AF:A8:6E:11	192.168.0.217	View Raw Deta	ails	
	02-Sep-2020 09:12:54.749 GMT+5:30	192.168.0.42	STARTED	02:8F:A5:7E:9C:8A	02:8F:A5:7E:9C:8A	02:8F:A5:7E:9C:8A	C0:67:AF:A8:6E:11	192.168.0.217	View Raw Det	ails	

cisco			020-08-24 22:45	08-25 22:45 Reset					
Se	Event: Raw Da	ata					×		
* Search Result: Your search returns too ma	Aug 25 17:1 srcMac=20: mdmCompl endpointCh endpointPro identitySour	2:39 192.10 A6:CD:C9:D iant=False eckResult= ofile=Unkno ccePortFirst	58.0.227 LEEF:2.0 Cl 9:00 providers=[u8 src=192.168.1.254 r none callingStation own mdmPinLockee =0 mdmJailBroken	SCO QRadarAppFor aposNone'] r adiusFlowType=Wir Id=20:A6:CD:C9:D9: d=False state=STAR =False nasPortType=	PxGrid 1.0 User Sessio aslpAddress=192.168 edMAB identitySourc 00 ssid=C0-67-AF-A8 FED networkDevicePro Ethernet	ons ^ 3.0.217 rePortEnd=0 r-6E-11 ofileName=Cisco			Export
Dev Time	adNormaliz calledStatio	edUser=20 nId=C0:67:	:A6:CD:C9:D9:00 au AF:A8:6E:11 service]	ditSessionId=C0A80	0D900000053019837 rtId=GigabitEthernet	'B4 1 + devTime=2020	AS IP Ad	dress 🔶	Raw Data
25-Aug-2020 10:42:04.457 GMT+5:30	 08-25T17:12:04.457Z identitySourcePortStart=0 usrName=20:A6:CD:C9:D9:00 mdmRegistered=False mdmDiskEncrypted=False 							7	View Raw Deta
25-Aug-2020 10:42:19:507 GMT+5:30	152.100.1.120	JIANILU	20:00:00:00:00	20:00:00:00:000	20:70:00:05:05:00	C0.07.3413(0.0E.11	192.168.0.21	7	View Raw Deta
25-Aug-2020 10:42:34.457 GMT+5:30	192.168.1.254	STARTED	20:A6:CD:C9:D9:00	20:A6:CD:C9:D9:00	20:A6:CD:C9:D9:00	C0:67:AF:A8:6E:11	192.168.0.21	7	View Raw Deta

Accepted Search format:

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

Partial Search Criteria:

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

Accepted Wildcard characters:

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

Passed Authentications

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

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

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



Step 1 Select Cisco ISE pxGrid > Passed Authentications



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

IBM QRadar Security Intelligence							admin 🔻	Halp V Mensages
Dashboard Offenses Log Activity	Network Activity	Assets Reports	Risks Vulnerabilities	Admin Cisco IS	E pxGrid			System Te
hilh Isco							2018-04-12 1	8:02 - 2018-04-27 18:02
Data For								
								×
11227 0000000000000000000000000000000000								EXPO
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:81:C9:3C:39		10:DD:81:C9:3C:39	50:3D:E5:C4:05:8C		GigabitEthernet1/0/12
18-Apr-2018 08:15:47.499 EDT	192.168.1.136	DISCONNECTED	10:DD:81:C9:3C:39		10:DD:B1:C9:3C:39	50:3D:E5:C4:05:8C		GigabitEthemet1/0/12
18-Apr-2018 08:40:42.287 EDT	192.168.1.136	STARTED	10:DD:81:C9:3C:39		10:DD:B1:C9:3C:39	50:3D:E5:C4:05:8C		GigabitEthernet1/0/12
18-Apr-2018 09:41:41.421 EDT	192.168.1.136	DISCONNECTED	10:DD:81:C9:3C:39		10:DD:B1:C9:3C:39	50:3D:E5:C4:05:8C		GigabitEthernet1/0/12
18-Apr-2018 09:50:57.018 EDT	192.168.1.136	STARTED	10:DD:B1:C9:3C:39		10:DD:81:C9:3C:39	50:3D:E5:C4:05:8C		GigabitEthernet1/0/12
	100 100 100	100000000000000000000000000000000000000			100000000000000000000000000000000000000			2012/02/02/02/02/02/02

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



BM QRadar Security	y Intelligence			mba	in 🔻 Help 🔻	Messages T
ashboard Offenses	Log Activity Netwo	rk Activity Assets F	laports Rieks Vulner	abilities Admin Cisco ISE pxGrid		System Time
110 50				2018-0	4-12 18:02 - 201	8-04-27 18:02
Data For : jeppi	ich					
						-
						EXPOR
show 10 🔁 ent	ries					
NAS Port Type	NAS Identifier	Posture Status	Endpoint Profile	Endpoint Operating System	Group ID	AD Normalize
Ethernet			Apple-Device	Apple Mac OS X 10.7.0 (Lion) - 10.10 (Yosemite) or iOS 4.1 - 8.3 (Darwin 10.0.0 - 14.5.0)		
Ethernet			Apple-Device	Apple Mac OS X 10.7.0 (Lion) - 10.10 (Yosemite) or iOS 4.1 - 8.3 (Darwin 10.0.0 - 14.5.0)		
Ethernet			Apple-Device	Apple Mac OS X 10.7.0 (Lion) - 10.10 (Yosemite) or iOS 4.1 - 8.3 (Darwin 10.0.0 - 14.5.0)		
Ethernet			Apple-Device	Apple Mac OS X 10.7.0 (Lion) - 10.10 (Yosemite) or iOS 4.1 - 8.3 (Darwin 10.0.0 - 14.5.0)		
Ethernet			Apple-Device	Apple Mac OS X 10.7.0 (Lion) - 10.10 (Yosemite) or iOS 4.1 - 8.3 (Darwin 10.0.0 - 14.5.0)		
Ethernet			Apple-Device	Apple Mac OS X 10.7.0 (Lion) - 10.10 (Yosemite) or iOS 4.1 - 8.3 (Darwin 10.0.0 - 14.5.0)		
Ethernet			Apple-Device	Apple Mac OS X 10.7.0 (Lion) - 10.10 (Yosemite) or iOS 4.1 - 8.3 (Darwin 10.0.0 - 14.5.0)		
Ethernet			Apple-Device	Apple Mac OS X 10.7.0 (Lion) - 10.10 (Yosemite) or IOS 4.1 - 8.3 (Darwin 10.0.0 - 14.5.0)		
Ethernet			Apple-Device	Apple Mac OS X 10.7.0 (Lion) - 10.10 (Yosemite) or iOS 4.1 - 8.3 (Darwin 10.0.0 - 14.5.0)		
Ethernet			Apple-Device	Apple Mac OS X 10.7.0 (Lion) - 10.10 (Yosemite) or IOS 4.1 - 8.3 (Darwin 10.0.0 - 14.5.0)		

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

Deshboard Offenses Log Ac	stivity Notwork Activity Assets	s Reports Risks Vulnerabilities	Admin Cisco ISE pxGrid			System Time: 6.1
10]16 (\$C0					2018-04-12 18:01	2 - 2018-04-27 18:02 Re
Data For : jeppich						3
Show 10 centries						EXPORT
AD Host Domain Name	AD Host NetBios Name	AD Host Resolved Identities	AD Host Resolved DNS	AD User Domain Name	AD User Net Blos Name	AD User Resolved Iden
					_	

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

IBM QRedar Se	curity Intelligence			admin 🔻 Help	¥ Massages∰¥ IBM		
Owshiboard Offe	nees Log Activity Network Activi	ty Assets Reports	Risks Vulnersbilltles Admi	Cisco ISE pxGrid			System Time: 0.11
6116 550					2018-04-12 18:02 -	2018-04-27 18:02 Ret	
Data For : j	eppich						×
Show 10	entries						EXPORT
ver Agent ID	Is Machine Authentication	Service Type	Tunnel Private Group ID	Airespace WLAN ID	Network Device Profile Name	Radius Flow Type	SSID I
	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_tx	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_tx	50-3D-E5-C4-05-8C
	false	Framed			Cisco	Wired802_1x	50-3D-E5-C4-05-8C

Failed Authentications

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

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

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

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

User Panel

The user panel provides a breakdown by username.

Step 1 Select Cisco ISE pxGrid > Failed Authentications

IBM C	Radar Se	curity Intelligenc	•									admin V	Hep V	Mainages	1814.
Dashba	oard Offe	nees Log Activity	Network Activity	Assets	Reports Ad	Cisco ISE pxGrid								Bystem	Time: 6.22 P
cisco	i i											2018-02-16	18:21 - 20	18-02-22 18:21	7 Day
			Pas	sed Auth	entications	Failed Authentication	bevice	Complian	ce Trustsec	MDM ANO	C Details				
Use	br							Failure Reas	ion						
All	Wired	Wireless					1	II Wired	Wireless						
51															
40															
										6					
20															
0				0						-					
			pxgndb 0.e	om:							/	<i>(</i>			
											24408 Dane au	therdiration and	et Active Time	etsev failed also	

Step 2 Select Cisco ISE pxGrid > Failed Authentications > User > pxGrid2@

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

IBM QRad	ar Security	Intelligenc	0											.85	inin T	Help V	Mossa	ages 🚺
Deshboard	Offenses	Log Activity	Network Activity	Assets R	leporta Ar	dmin Cisco IS	IE pxGrid											System
14114														2018-	02-16	18:21 - 21	018-02-2	2 18:2
Data Fo	or : pxgri	d2@lab1	0.com															
Show	0 📴 entri	es																EX
ID		* Dev Ti	ime	÷ . B	P Address	1 Failure	Reason								4	User	name	- 8
151896	484344947	3 18-Feb	2018 04:17:23.49	4 EST 19	2.168.1.7	24408 U	ser authentica	ation against	Active Direct	tory failed	d since user	r has ente	red the v	wrong pase	isword	pxgrid	2@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 Sec	urity Intelligence						admin ¥	Help 🔻 🔥	kessinger
Dashboard Offens	es Log Activity Network Activity	Assets Reports	Admin Cisco I	SE pxGrid					Syna
kilin Isco			- *				2018-02-16 1	8:36 - 2018-0	2-22 18:
Data For : px	grid2@lab10.com								
Show 10 🛊 e	ntries								
Server Name	Authentication Protocol	Device Type	Location	Calling Station ID	NAS IP Address	NAS Port ID	NAS Port Type	MAC Add	Iress
ise24k	PEAP (EAP-MSCHAPv2)	All Device Types	All Locations	00:0C:29:C1:78:2C	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 QRedar Sec	urity Intelligenc	•					admin ¥ Help 1	Managa 📴 IBM.
Deshboard Offens	es Log Activity	Network Activity Assets Re	eports Admin G	isco ISE paGrid				System Time: 8:411
10110 1550							2018-02-16 18:36 -	2018-02-32 18:36 7 Da
Data For : px	grid2@lab10).com						×
Show 10 ¢ e	ntries							EXPORT
Message Co	le 🕴 User Tyj	Access Service	Identity Stor	Authentication Method	Service Type *	Credential Check	AD Normalized User	AD Host Domain Na
5400		Default Network Access	pxGridUsers	dotta	Framed	MSCHAPV2		
Showing 1 to 1	of 1 entries						Prev	fious 1 Next

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

IBM QRadar Securi	ity Intelligence				aomin ¥	Help * Messages
Deshboard Offenses	Log Activity Network Activity A	ssets Reports Admin Cis	co ISE pxGrid			System Time: 6.46 (
torilia: teco:					2018-02-16 1	8:36 - 2018-02-22 18:36 7.03
Data For : pxg	rid2@lab10.com					×
Show 10 \$ entr	ries					EXPORT
t NetBios Name	AD Host Resolved Identities	AD Host Resolved DNS	AD User Domain Name	AD User Net Blos Name	AD User Resolved Identities	AD User Resolved DNS
Showing 1 to 1 of	1 entries					Previous 1 Next

		admin 🔻	Help 🔻 Messages 🖉 🔻	IBM
ISE pxGrid			System T	ime: 6:41
		2018-02-16 18	:36 - 2018-02-22 18:36	7 D
				×
			EXP	ORT
AD User Domain Name	AD User Net Bios Name	AD User Resolved Identities	AD User Resolved D	ONS 🕴

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 Intelligen	ce	adının 🔻 Haşaya 🚺 🕈 133
Deshboard Offenses Log Activity	Network Activity Assets Reports Admin Cloco ISE pat	Grid System Time 6.2
Isco		2018-02-16 18:21 - 2018-02-22 18:21 7 D
	Passed Authentications Failed Authenti	ications Devices Compliance Trustsec MDM ANC Details
User		Failure Reason
All Wired Wireless		All Wired Wireless
51		
40		
20		
	1	
	pxgnd240ub1 0.com	

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



IBM QRad	ar Securit,	Intelligenc	•				admin V	Help V	Mossages
Dashboard	Offenses	Log Activity	Network Activity	Assets	Reports	Admin	Cisco ISE pxGrid		System
iniju Isco							2018-02-16-18	:36 - 2018-	02-22 18:3
Data Fo	or : 2440	8 User au	uthentication	agains	t Active	Direc	tory failed since user has entered the wrong password		
Show 1	0 🛊 entri	25							EX
ID		* Dev T	ime		IP Addr	ess	Failure Reason 0	Userna	ime
1518964	48434494	73 18-Feb	-2018 04:17:23.49	94 EST	192.168.1	.7 :	24408 User authentication against Active Directory failed since user has entered the wrong password	pxgrid26	Plab10.com
Showing	1 to 1 of 1	entries						Previous	1

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

ecurity Intelli	gence							ximin V Help V	Manager IBM
enses Log Ac	tivity Network Activity	Assets	Reports Admin	Cisco ISE pxGrid					System Time: 0.53 /
							2018	8-02-16 18:36 - 20	18-02-22 18:36 7 Day
24408 Use	er authentication a	gainst	Active Direc	tory failed sir	nce user has entered	d the wrong pass	word		×
									FURDER
entries									EXPORT
Server Nam	Authentication P	Protocol	Device Typ	pe Location	Calling Station ID	NAS IP Address	NAS Port ID	NAS Port Typ	e MAC Address
ise24k	PEAP (EAP-MSCH/	APv2)	All Device T	ypes All Locatio	ons 00:0C:29:C1:7B:2C	192.168.1.3	GigabitEthernet1/0/11	Ethernet	
1 of 1 entries								Previo	us 1 Next

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



Security	Intelligence	•					ŝ	admin 🔻	Help ¥	Mossa
Offenses	Log Activity	Network Activity	y Assets Reports	Admin Cisco ISE	pxGrid					
							201	8-02-16 1	8:36 - 201	8-02-22
: 2440	8 User au	thenticatio	n against Active	Directory faile	ed since user has ente	red the wrong pass	word			
\$ entrie	s									
Message	e Code 🕴	User Type 🕴	Access Service	Identity St	ore Authentication Met	thod Service Type	Credential Check	AD N	ormalized	User
5400			Default Network Acce	ss pxGridUsers	dot1x	Framed	MSCHAPV2			

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

← → C ▲ Not Secure Hitter	://192.168.1.190/console/grad	at/jsp/QRadat.jsp				x 🖬 🛛 🕄 🕅
IBM QRadar Security Intellige	100				admin ¥ Help ¥	Manager IBM.
Dashboard Offenses Log Activit	y Network Activity Assets	Reports Admin Cisco ISE pxGrid				System Time: 0.57
ilitilit cisco					2018-02-16 18:36 - 20	18-02-22 18:36 7 De
Data For : 24408 User	authentication against	Active Directory failed sin	ce user has entered th	e wrong password		×
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 Blos Name	AD User Resolved k
Showing 1 to 1 of 1 entries					Previ	ous 1 Next

Device Type Panel

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

To categorize device type:

- Step 1 Select Cisco ISE pxGrid > Failed Authentications
- Step 2 Select Device Type > All Device Types

SECURE ACCESS HOW-TO GUIDES





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

IBM QRadar	Security	y Intelligence					admin ¥	Help 🔻 Mossages 🚱 🔻
Dashboard (Offenses	Log Activity	Hetwork Activity	Assets	Reports	Admin	Cisco ISE pxGrid	System
inilin Isco							2018-02-16 18	:35 - 2018-02-22 18:36
Data For	: All De	evice Type	es					
Show 10	¢ entri	es						EX
ID		* Dev Ti	me		IP Addr	ess 🤌 💡	Failure Reason	Username
15189648	84344947	73 18-Feb-	2018 04:17:23.49	4 EST	192.168.1	.7	24408 User authentication against Active Directory failed since user has entered the wrong password	pxgrid2@lab10.com

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

IBM QRada	r Security	y Intelligence										admir	▼ Help ₹	Mossager	IBM.
Deshboard	Offenses	Log Activity	Network Activity	Assets	Reports	Risks	Vulnerabilities	Admin	Cisco ISE pxGrid					Dyster	Time: 10.06
liniji. Jisco												2018-03-	04 22:06 - 2	18-03-10 22:0	7 Da
Data Fo	or : All D	evice Typ	es												×
Show 10) 🔁 enti	ries												Ð	PORT
Server Na	me 🤅 🗚	uthenticatio	n Protocol	Device Ty	pe	Locatio	n Callin	g Station	ID NAS IP A	ddress	NAS Port ID	NAS Port Type	MAC Add	ress Mes	sage Co
ie24k	PE	AP (EAP-MS	CHAPv2)	VII Device T	ypes /	All Locati	ons 00:0C	29:C1:78:2	2C 192.168.1.3	3	GigabitEthernet1/0/11	Ethernet		5400	

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

IBM QRada	ar Security Intelligence										admin V	Help V	Messagen	IBM.
Deshboerd	Offenses Log Activity	Network Ac	hity Assets	Reports	Rieks	Vulnerabilities	Admin	Cisco ISE pa	Grid				System 1	Time: 10:07
dialla cisco											2018-03-04	22:06 - 201	8-03-10 22:06	7 Da
Data Fo	or : All Device Typ	es												×
Show 10	entries												EXP	ORT
User T	ype Access Servi	ce i	Identity St	ore A	uthentic	ation Method	Ser	vice Type	Credential Check	AD Normalized User	AD Host D	omain Nar	me AD Ho	ost Neti
	Default Networ	k Access	pxGridUsers	do	etic		Fram	ed	MSCHAPV2					

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

Intelligence						admin 🔻	Holp ¥ Message	0 -	IBM
Log Activity Network Activity As	sets Reports Ris	ska Vulnerabilities	Admin (Cisco ISE pxGrid			97	stern Tim	e; 10:0
			7			2018-03-04-22	106 - 2018-03-10 2	2:06	7 Di
evice Types									×
ies								EXPO	RT
AD Host Resolved Identities	AD Host Resol	Ived DNS AD) User Doma	ain Name	AD User Net Bios Name	AD User Resolved Identities	AD User Resol	ved DN	IS I

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

Device Type	Location
All Wired Wireless	All Wired Wireless
	57
	40
	20
	0 Al Location

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



IBM QRa	dar Security	y Intelligenc	•								admin V	Holp ¥ Messager	 IBM.
Dashboard	Offenses	Log Activity	Network Activity	Assets	Reports	Risks	Vulnerabilities	Admin	Cisco ISE pxGrid			System	en Time: 10:19
http: SCD										2	2018-03-04 3	22:19 - 2018-03-10 22:	19 7 Day
Data F	or : All Lo	ocations											×
Show	t0 📴 enti	ries										ε	XPORT
ID		* Dev Tir	me	1	IP Addre	ISS 0	Failure Reaso	n				Username	Servei

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 QRade	er Security Intell	gence						edmin I	r Help ▼ 1	Acssages 0 v	IBM.
Deshboard	Offenses Log A	thity Network Activ	tty Assets Report	n Rinks Val	nerabilities Admin	Cisco ISE pxGrid				Bystem 1	ine 1022
61560								2018-03-0	4 22:19 - 2018-	13-10 22:19	7 Day
Data Fo	or : All Locatio	ons									×
Show 10	0 📴 entries									EXP	ORT
Server N	lame Auther	tication Protocol	Device Type	Location	Calling Statio	n ID NAS IP Addr	NAS Port ID	NAS Port Type	MAC Addres	s Mes	sage C
ise24k	PEAP (E	P-MSCHAPv2)	All Device Types	All Locations	00:0C:29:C1:78	192.168.1.3	GigabitEthernet1/0/11	Ethernet		5400	

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

IBM QRada	r Security Intelligence						admin 🔻 Help ¥ 🛛 N	essages V	IBN
Dashboard	Offenses Log Activity Netw	ork Activity Assets	Reporte Riska Vulnerabilities	Admin Cisco 158	2 pxGrid			Bystem Th	me: 103
dadh ISCO							2018-03-04 22:19 - 2018-0	3-10 22:19	7 D
Data Fo	r : All Locations								×
Show 10	entries							EXPO	DRT
User Typ	Access Service	Identity Store	Authentication Method	Service Type	Credential Check	AD Normalized User	AD Host Domain Name	AD Host	NetB
	Default Network Acces	s pxGridUsers	dot1x	Framed	MSCHAPV2				



Intelligence		_			admin ¥	Holp 🛛 Messages 🗳 IB)
Log Activity Network Activity Ass	ets Reports Risks	Vulnerabilities Admin	Cisco ISE pxGrid			Bysten Time: 5:5
			a		2018-03-04 17	53 - 2018-03-10 17:53 7 D
ocations						×
ies						EXPORT
AD Host Resolved Identities	AD Host Resolved	DNS AD User Dor	main Name 🕴	AD User Net Bios Name	AD User Resolved Identities	AD User Resolved DNS

Devices

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

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

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

Step 1 Select Cisco ISE pxGrid > Devices

Step 2 Select EndProfile (All) > Windows7-Workstation





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

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

IBM QRadar Se	ecurity Intelligenc	•						n.▼ Hop.▼ Ma	IBM.
Deehboard Offe	mees Log Activity	Hetwork Activity	Assets Reports /	Idmin Cisco ISE peGrid	C				System Time: 2031
nilo Isco							2018-03	-16 21:02 - 2018-02	-22 31-02 7 Day
Data For : \	Windows7-Wo	rkstation							×
Show 10 \$	entries								EXPORT
Dev Time		IP Address	State	MAC Address	Username	Calling Station ID	Called Station/D	NAS IP Address	NAS Port IL
22-Feb-2018	9 04:38:20.739 EST	192.168.1.37	DISCONNECTED	00:00:29:01:78:20	host/pxGrid2-	00.00.29:01:78:20	50:3D:E5:C4:05:88	192.168.1.3	GigabitEtherr
22-Feb-2018	9 04:38:22.616 EST	192.168.1.37	STARTED	00:00:29:01:78:20	pxgrid2@l	00:00:29:01:78:20	50:30:E5:C4:05:88	192.168.1.3	GigabitEtherr
22-Feb-2018	9 04:42:39.116 EST	192.168.1.37	DISCONNECTED	00:00:29:01:78:20	pxgrid2@4	00:00:29:01:78:20	50-30-E5-C4-05-88	192.168.1.3	GigabitEthen

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.



adar Security Intel	lligence		_	1 12 1		ade	is 🔻 Holp 🔻 Moss	
d Offenses Log	Activity Network Activ	ny Assets Reports	Admin Cisco ISE pxGrid					System
						2018-0	2-16 21:02 - 2018-02-2	22 21:0
For : Windows	7-Workstation							
								Ð
10 ¢ entries								
NAS Port Type	NAS Identifier	Posture Status	Endpoint Profile	Endpoint Operating System	Group ID	AD Normalized User	AD Host Domain N	Name
Ethernet			Windows7-Workstation	Windows 7 Professional		pxGrid2-P0		
Ethernet			Windows7-Workstation	Windows 7 Professional		psgrid2		
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 Intellig	gence			admin.V 2	uip V Messager
Deshboard Offenses Log Act	ovity Network Activity Assets Re	ports Admin Claco ISE pxGrid			System Time 200
61[0 \$CO				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 Blos Name	AD User Resolved Identiti
	PXGRID2-PC\$	CN=PXGRID2-PC,CN=Computers,DC=L			
	PXGRID2-PC\$				
	PXGRID2-PC\$				
	PXORID2-PC\$				

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



elligence								admin ¥ Help ¥	Mossager IBM
Activity	Network Activity	Assets	Reports	Admin	Cisco ISE pxGrid				System Time, 9.09
								2018-02-16 21:02 - 2	018-02-22 21:02 7 Da
s7-Wo	rkstation								×
									EXPORT
AD Us	er Resolved DNS		1	Term	inal Server Agent ID	Is Machine Authentication	Service Type	Tunnel Private Group ID	Airespace WLAN ID
						true	Framed		
CN=pxg	grid2,CN=Users,D	C=li		1		faise	Framed		
CN+px	grid2,CN=Users,D	C=la				false	Framed		

	aunan a map i	r messages v	10
		System 1	īme: 9:
	2018-02-16 21:02 -	2018-02-22 21:02	70
			3
		-	0.077
		EXP	ORI
Network Device Profile Name	Radius Flow Type	SSID	OK1
Network Device Profile Name =	Radius Flow Type	SSID 50-3D-E5-C4-0	6 R1
Network Device Profile Name = Cisco Cisco	Radius Flow Type & Wired802_1x Wired802_1x	\$\$10 50-3D-E5-C4-0 50-3D-E5-C4-0	5-88 5-88

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)

nt

IBM QRa	dar Securit	y Intelligence									agmin 🔻	Help ¥	Message	IBM.
Deshboard	Offenses	Log Activity	Network Activity	Assets	Reports Adv	Cisco ISE pxGrid							System	Time: 8:12 P
cisco						5 / A 6					2018-02-16	21:12 - 201	8-02-22 21:12	7 Day
			Pass	ed Authe	entications	Falled Authentication	s Devices	Compliance	Trustsec MDM	ANC Details				
Comp	liance (All)						Compliance (V	Vired)					
π								77						
60								60						
40								40						
20	1	<i>a</i>						20	27					
0					_	3		0		5		_	3	
	Pen	ding	NotApp 0	ficator		Compliant		P	ending	NotApplicat 0		Co	mplant	

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.



IDM GRad	ar Security Intellig	pence							admin	▼ Help ▼ Mess	ous IBM
Deshboard	Offenses Log Act	MRY	Network Activity	Assots Repo	ris Admin Cisco I	iE pxGrid					System Time: 9:14
HILL ISCO									2018-02-	16 21:12 - 2018-02-2	2102 7 De
Data Fo	or : Compliant										×
											EXPORT
Show 1	0 \$ entries										
Show 1 Dev Ti	0 🛊 entries		IP Address	State	MAC Address	Username	Calling Station ID	Called StationID	NAS IP Address	NAS Port ID	I NAS Po
Show 1 Dev Ti 18-Feb	entries me 2018 10:17:19.596	* EST	IP Address 192.168.1.15	State I	MAC Address	Username I pxgrid1	Calling Station ID 00:50:56:86:88:13	Called StationID 6 50:3D:E5:C4:05:8B	NAS IP Address (NAS Port ID GigabitEthernet1/0	NAS Po
Show 1 Dev Ti 18-Feb- 18-Feb-	entries me 2018 10:17:19.596 2018 10:17:19.596	+ EST EST	IP Address 192.168.1.15 192.168.1.15	State II POSTURED POSTURED	MAC Address 00:50:56:86:88:13 00:50:56:86:88:13	Username I pxgrid1 pxgrid1	Calling Station ID 00:50:56:86:88:13 00:50:56:86:88:13	Called StationID 0 50:30:E5:C4:05:88 50:30:E5:C4:05:88	NAS IP Address 1 192.168.1.3 192.168.1.3	NAS Port ID GigabitEthernet1/0 GigabitEthernet1/0	NAS Po 11 Ethernet 11 Ethernet

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

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

telligence						84.			admin 🔻 Help 🔻 Messag	105
g Activity Netw	work Activity	Assets	Reports	Admin Cisco IS	E pxGrid					Syste
								20	18-02-16 21:12 - 2018-02-22	21:
int										
										_
										E
NAS Identif	fier Post	ure State	us 🕴 I	Endpoint Profile	÷. #	Endpoint Operating System	Group ID	AD Normalized User	AD Host Domain Name	÷۹
	Compl	liant	M	/indows7-Worksta	ation V	Vindows 7		pxgrid1		
	Compl	liant	M	licrosoft-Workstat	tion V	Vindows 7 Professional 64-bit		pxgrid1		
	Compl	liant	M	licrosoft-Workstat	tion V	Vindows 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.

lar Security Intelligence					admin.▼ Help ▼ Messages
Offenses Log Activity Net	work Activity Assets Reports Adi	min Cisco ISE pxGrid			Syr
					2018-02-16 21:12 - 2018-02-22 21
or : Compliant					
0 🗘 entries					
AD Host NetBios Name	AD Host Resolved Identities	AD Host Resolved DNS	AD User Domain Name	AD User Net Blos 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.



lecurity	y Intelligence								admin	▼ Help ▼	Messager
tenses	Log Activity	Network Activity	Assets	Reports	Admin	Cisco ISE pa	Grid				Sys
						e 7			2018-02-	16 21:12 - 2	018-02-22 21
Com	pliant										
1											
entri	05										
AD U	iser Resolved	DNS	4	Terminal	Server	Agent ID	Is Machine Authentication	Service Type	Tunnel Private Group ID	Airespac	WLAN ID
CN=p	Grid1,CN=Us	ers,D					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

IBM QRadar Security Intelligence	admin ¥ Help ¥ Messagn 🖏 IBM
Deshboard Offenses Log Activity Network Activity Assets Reports Admin Cisco ISE pxGrid	Bystem Time 9.2
isto	2018-02-16 21:22 - 2018-02-22 21:22 7 D
Passed Authentications Falled Authenticati	ions Devices Compliance Trustsec MDM ANC Details
Group Tag (All)	Group Tag (Wired)
52 ·	
40	40
20	20
2 1 Outarantinėd, Employees Svaterra	0 Quarantined_ Employees Svotoma

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



M QRade	ar Security Intelligenc	•						edmin ¥ He	ip 🔻 Massager 🔐 🖬
eshboard	Offenses Log Activity	Network Activity	Assets Reports	Admin Cisco ISE pxGrid					Bystem Time:
()) 60								2018-02-16 21:2	2 - 2018-02-22 21:22 7
Data Fo	or : Quarantined_S	ystems							
Show 10	entries								EXPOR
Dev Ti	me	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:C1:78:2C	LAB10\pxgrid2	00:0C:29:C1:78:2C	50:3D:E5:C4:05:88	192.168.1.3	GigabitEthemet1/0/11
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:C4:05:88	192.168.1.3	GigabitEthernet1/0/11

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

IBM QRadar S	ecurity Intellig	ince										admin V	Help V	Messa
Dashboard Off	enses Log Acth	ity Netwo	rk Activity	Assets	Reports	Admin	Cisco ISE ;	pxGrid						
64[16 560												2018-02-16	21:22 - 2	018-02-22
Data For :	Quarantined	_Systen	ns											
Show 10 \$	entries													
NAS Port Ty	ype NAS lo	entifier 1	Postur	e Status	End	point Pro	file 0	Endpoint Operat	ing System	Group ID	AD Normalized User	AD Hos	t Domain	Name
Ethernet					Wind	ows7-Wo	rkstation	Windows 7 Profess	ional		pxgrid2			
Ethernet					Wind	ows7-Wo	rkstation	Windows 7 Profess	ional		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.

dar Security Intelligence	والمحروفة والمحروفين				admin 🔻 Help 🔻 Messager
d Ottonses Log Activity N	letwork Activity Assets Reports A	dmin Cisco ISE pxGrid			
		- 4			2018-02-16 21:26 - 2018-02-22 2
For : Quarantined_Sys	stems				
10 🛊 entries					
AD Host NetBios Name	AD Host Resolved Identities	AD Host Resolved DNS	AD User Domain Name	AD User Net Blos Name	AD User Resolved Identities
	PXGRID2-PC\$6			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.



ligence	•		11.000				admin 🔻 Help 🔻	Messages
ctivity	Network Activity Ass	ats Reports	Admin Cisco IS	E pxGrid				System Time
						201	8-02-15 21:28 - 20	18-02-22 21:28
ed_S	ystems							
								EXPO
Ter	minal Server Agent ID	Is Mac	hine Authenticati	on Service Type	Tunnel Private Group ID	Airespace WLAN ID	Network Devic	ce 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

IBM QRadar Security Intelligence	adoin V Hep V Manage 🐓 IBM.
Deshboard Offenses Log Activity Network Activity Assets Reports Admin Cisco ISE psGrid	System Time: 0:34 P1
dhala cisco	2018-02-16 21:32 - 2018-02-22 21:32 7 Day
Passed Authentications Failed Authentications	Devices Compliance Trustsec MDM ANC Details
Compliance	Registration
The (18)	Total (18)

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.



IBM QRadar Sec	urity Intelligence							admin 🔻 Help 1	Messag	IBM.
Deshboerd Offene	es Log Activity Netw	rork Activity Asse	ta Reporta Admin Cia	co ISE pxGrid						lystern Timle: 9:35 f
sco			1					2018-02-16 21:32 -	2018-02-22	21:32 7 Da
Data For : Tr	Je									×
Show 10 \$ e	ntries									EXPORT
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

IBM QRadar Security Intelligence	admin V Help V Messages ²⁰ V IB3
Deshboard Offenses Log Activity Network Activity Assets Reports Admin Cisco ISE pxG	id System Tares 93
iliuliu cisco	2018-02-16 21:50 - 2018-02-22 21:50 70
Passed Authentications Falled Authentic	ations Devices Compliance Trustsec MDM ANC Details
Currently Assigned ANC policy	
Show 10 ¢ entries	
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 reauthenticated.

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

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

The following Cisco ISE ANC policies will be created:

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

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

Configuring Default ANC policies for Cisco ISE pxGrid App

- Note: When you setup the QRadar, pxGrid app will automatically create default ANC policies if they don't exist. These policies shown in the paragraph about are hard coded and cannot be edited. If you have other policies, you will need to integrate them manually on ISE. These policies are populated after you submit and test the pxGrid app settings in QRadar.
- Step 1 Select Operations > Adaptive Network Control > Policy List > Add > The following for the Policy Name and Action:

pxGridQRadarQuarantine, QUARANTINE



pxGridQRadatShutDown, SHUT_DOWN,

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

cisco	Identity Services Engine Ho	ome • Con	text Visibility	Operations Pollo
+ RAD	IUS Threat-Centric NAC Live Logs	+ TACACS	Troubleshoot	- Adaptive Network Co
Policy	List Endpoint Assignment			
List 0 Sele	ected			
c	Refresh 🕂 Add 🏛 Trash 🕶	🖾 Edit		
	Policy Name		ANC	Actions
	pxGrldQRadarQuarantine		QUA	RANTINE
	pxGridQRadarPortBounce		POR	T_BOUNCE
	pxGridQRadarShutDown		SHU	T_DOWN

Adding ANC Policies to ISE Policy Sets

- Step 1 Select Policy > Policy Sets > Default > ">" > Authorization Policy > Global Exceptions > "+"
- Step 2 Under Rule Name, type: ANC Quarantine
- Step 3 Under Conditions, select "+"
- Step 4 To close the introductory screen, select "x"
- Step 5 Under Dictionary, select Session > ANCPolicy > Equals > pxGridQRadarQuarantine
- Step 6 Select Use
- Step 7 Under Profiles, select Permit Access
- Step 8 Under Security Groups, select Quarantine_Systems
- Step 9 Select Save
- Step 10 Perform steps 1-9 for the Rule Name ANCShutDown and ANCPolicy pxGridQRadarShutDown
 - Note: You can also click on the Gear and duplicate line below and add the rule name and ANCPolicy
- Step 11 Perform steps 1-9 for the Rule Name ANCPortBounce and ANCPolicy pxGridQRadarPorBounce

Note: You can also click the Gear icon and duplicate line below and add the rule name andCisco Systems © 202 ANCPolicyPage 59



Step 12 You should see the following:

cisco I	dentity Se	rvices Engine	Home	+ Context Vi	sibility + Operations	+ Policy	+ Administration	+ Work Centers				License Warni	ing 🔺	ġ,
Policy S Search	ets Profi	ling Posture	Client Provision	ning + Poli	cy Elements					Click he	re to do wirele	ss setup and visi	bility setu	p Do n
	0	Default		Default p	olicy set							Default Networ	rk Access	ę.
> Auti	henticatio	n Policy (3)												
> Auti	horization	Policy - Loca	I Exceptions											
M Aut	horization	Policy - Glob	al Exceptions	s (3)										
-								Res	ults					
•	Status	Rule Name		Condit	ions			Prof	lies		Security Gr	oups		
Seet	n													
	0	ANCQuarantin	6	F	Session ANCPolicy EQU	NLS pxGridQ	RadarQuarantine	(*)	PermitAccess	+	Quarantine	d_Systems	* *	+
	0	ANCPortBoun	ce	F	Session ANCPolicy EQU	NLS pxGridQ	RadarPortBounce		PermitAccess	+	Quarantine	d_Systems	* *	+

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

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

Step 1 User pxGric	1 authenticates	in	ISE
--------------------	-----------------	----	-----

dentity Services I	Engine Home + Co	relaxit Visibility	· Operations	+ Policy	+ Administration + Work Centers			License Warning 📣 🕓	
+RADIUS Threat-Cent	ric NAC Live Logs + TACAC	S + Troublesh	oot + Adaptive	Network Control	Reports		Click here to do wi	releas setup and visibility setup Do not si	Now this again
Live Logs Live Sessions	•								
	Misconfigured Supplicants	Miscor	ifigured Network	R Devices 0	RADIUS Drops @	Cilent Stopp	ed Responding O	Repeat Counter 0	
	0		0		0		5	0	
						я	efresh Never 0	Show Latest 20 records ¢ Within L	ist 3 hours [
C Refresh O Reset	Repeat Counts 🕹 Export 1	α •							Filter - 0 -
Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P	Authentication Policy	Authorization Policy	Authorizati.
×		1		Identity	Endpoint ID	Endpord Prof.	Authentication Policy	Authorization Policy	Authoritatio
Mar 09, 2018 07:18	30.952 PM		0	pagnid1	00:50:56:66:88:13	Microsoft-W	Default >> Dot1X	Default >> Basic_Authentica	t PernitAcces
Mar 09, 2018 07:18	30.671 PM	ō		pagnd1	00:50:56:86:88:13	Microsoft-W	Default >> Dot1X	Default >> Basic_Authentica	L PermitAcces
Mar 09, 2018 07:18	18.872 PM	ö		host/win7-pc3	00.50.56.86.88.13	Microsoft-W	Default >> Dot1X	Default >> Basic_Authentical	L PerritAcces
Mar 09, 2018 07:17	51.173 PM	ā		host/win7-pc3	00:50:56:86:88:13	Microsoft-W	Default >> Dot1X	Default >> Basic_Authentica	L. PermitAcces

Step 2 Select Cisco ISE pxGrid > Passed Authentications



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

an Gradar security intelligence							admin 1	▼ Holp ¥ Messages	TIBM
eshboard Offenses Log Activity	Network Activity	Assets Repor	ts Risks Vulnerabilit	ies Admin Ci	sco ISE pxGrid			((6))	en Time: 220
ala co							2018-03-0	13 14:20 - 2018-03-09 14:	30 7 Da
Data For : pxgrid1									×
Show 10 \$ entries	IP Address	State	MAC Address	Username	Calling Station ID	Called StationID	NAS IP Address	NAS Port ID	NAS P
Show 10 \$ entries Dev Time * 08-Mar-2018 10:11:31.641 EST	IP Address 192.168.1.15	State I STARTED	MAC Address 00:50:56:86:88:13	Username I	Calling Station ID 00:50:56:86:88:13	Called StationID	NAS IP Address	NAS Port ID GigabitEthernet1/0/11	NAS P
Show 10 ¢ entries Dev Time * 08-Mar-2018 10:11:31.641 EST 08-Mar-2018 10:41:59.690 EST	IP Address 192.168.1.15 192.168.1.15	State STARTED	MAC Address 00:50:56:86:88:13 00:50:56:86:88:83	Username I pxgrid1 pxgrid1	Calling Station ID 00:50:56:86:88:13 00:50:56:88:88:13	Called StationID (50:30:E5:C4:05:88 50:30:E5:C4:05:88	NAS IP Address = 192.168.1.3 192.168.1.3	NAS Port ID GigabitEthernet1/0/11 GigabitEthernet1/0/11	NAS P Etherner

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

IBM QReder Security Intelligence							admin	V Holp V Messages	IBM
Deshboard Offenses Log Activity	Network Activity	Assets Report	s Risks Vulnersbillt	ies Admin Ci	sco ISE pxGrid				en Time: 2:22
16110 1560				100			2018-03-0	3 14:20 - 2918-03-09 14	20 7 Da
Data For : pxgrid1									×
Show 10 \$ entries									XPORT
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	STAPTER	00 50 56 86 88 13	pxgrid1	00:50:56:86:88:13	50:30:E5:C4:05:88	192.168.1.3	GigabitEthemet1/0/11	Ethernel
08-Mar-2018 10:41:59.690 EST	192.168.1. p	wGridQRadarQuara	ntine 50:56:86:88:13	pxgrid1	00:50:56:86:88:13	50:30:E5:C4:05:88	192.168.1.3	GigabitEthemet1/0/11	Etherner
08-Mar-2018 10:53:16.962 EST	192.168.1. p	xGndQRadarFortBi xGndQRadarShutD	Nown 50:56:86:88:13	pxgrid1	00:50:56:86:88:13	50:3D:E5:C4:05:88	192.168.1.3	GigabitEthernet1/0/11	Ethernel
08-Mar-2018 10:56:56 250 EST	192.168.1.15	STARTED	00:50:56:86:88:13	ovorid1	00:50:56:86:88:13	50:30:E5:C4:05:88	192.168.1.3	GipabitPthemet1/0/11	-

Step 5 Select pxGridQRadarQuarantine

Step 6 You should see a successful status message:

IBM QRad	ar Securit	y Intelligenc	ə			192.168.1.192 Says	
Dashboard	Offenses	Log Activity	Network Activity	Assets	Repor	Status : RUNNING Operation Id : ise24k.lab10.com:1	
Data Fo	or : pxgri	id1					ОК

Step 7 Select OK

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

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

theh Identity Services Engine	Home + Contr	ext Visibility	· Operations	+ Policy	+ Administration - Work Centers			License Warning 👍		o o
*RADIUS Threet-Centric NAC UV	e Logs + TAGACS	+ Troublesho	ot + Adaptive	Network Cont	rol Reports		Click here to r	o winters setup and visibility setup Do	not show this i	X
Live Logs Live Sessions							-			
Miscorfi	pured Supplicants O	Miscon	figured Network	Devices O	RADIUS Drops O	Client Stopp	ed Responding O	Repeat Counter O		
	0		0		0		5	0		
						R	eftesh Never	C Show Latest 20 records C Web	n Last 3 hour	s t
C Refresh O Reset Repeat Co	uns 🕹 Export To •								¥ Fitar •	0-
Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P	Authentication Policy	Authorization Policy	A	uthorizati
×				identity.	Endport ID	Endpoint Prof	Authentication Policy	Authorization Palicy	1.0	Authorizatio
Mar 09, 2018 07:29:29:562 PM	•	9	0	pagnat	00.50 56 36 88 13	Microsoft-W	Default >> Dot1X	Default >> ANCQuerer	one Q	Laransned
Mar 09, 2018 07:29:29.505 PM		a		pagridt	00:50:56 86 88:13	Microsoft-W	Default >> Dot1X	Default >> ANCQuaran	one G	karantined
Mar 09, 2018 07:29:28.709 PM	8				00.50.56.66.88.13					

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

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

IBM QRadar Security Intelligence	admin V Help V Messager
Deahboard Offenses Log Activity Network Activity Assets Reports Raka Vulnerabilities	Admin Cisco ISE pxGrid System Tree 234 I
alialia cisco	2018-03-03 14:34 - 2018-03-09 14:34 7 Dat
Passed Authentications Failed Authentic	ations Devices Compliance Trustsec MDM ANC Details
Currently Assigned ANC policy	
Show 10 ¢ entries	
Mac Address *	Policy Name
00:50:56:86:88:13	pxGridQRadarQuarantine
Showing 1 to 1 of 1 entries	Previous 1 Next

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



IBM QRad	ar Security	y Intelligence												admin ¥	Help ¥	Messager	R 3	BM.
Deshboard	Offenses	Log Activity	Hetwork Activity	Assets	Reports	Risks	Vulnerabilities	Admin	Cisco ISE	pxGrid						Syn	es Tina	x 2.90 Pt
cisco								_	1					2018-03-03	14:34 - 20	18-03-09 14:	34	7 Day
			Pas	sed Auth	enticatio	ns Fa	iled Authentic	ations	Devices	Compliance	Trustsec	MDM	ANC Details					
Group	Tag (All)								G	roup Tag (Wi	red)							
57										55								
40										40								
20										20								
0			Quara Syst	7 ntined, terns						0			5 Quarantiner Systems	a_				

Step 11 To see the quarantined endpoints, select Quarantined_Systems:

IBM QRadar Security Intelligence	5	-					admin 🔻 Help 🔻	Messager IBM
Dashboard Offenses Log Activity	Network Activity	Assets Reports P	tiska Vulnerabilities v	Admin Cisco ISE pxGrid				System Time: 2.4
dialo Gisco							2018-03-03 14:34 - 20	18-03-09 14:54 7 D
Data For : Quarantined_Sy	stems							×
Show 10 \$ entries	IP Address	State	MAC Address	Username	Calling Station ID	Called StationID	NAS IP Address	EXPORT NAS Port ID
09-Mar-2018 02:29:29.662 EST	192.168.1.15	STARTED	00:50:56:86:8B:13	pxgrid1	00:50:56:86:88:13	50:3D:E5:C4:05:8B	192.168.1.3	GigabitEthernet1/0/
08-Mar-2018 11:05:58.744 EST	192.168.1.15	STARTED	00:50:56:86:88:13	pxgrid1	00:50:56:86:88:13	50:3D:E5:C4:05:8B	192.168.1.3	GigabitEthernet1/0/
08-Mar-2018 10:24:20.597 EST	192.168.1.57	DISCONNECTED	88:CB:87:ED:45:DA	88:C8:87:ED:45:DA	88:C8:87:ED:45:DA	50:30:E5:C4:05:83	192.168.1.3	GigabitEthernet1/0/
08-Mar-2018 10:24:20.597 EST	192.168.1.57	DISCONNECTED	88:C8:87:ED:45:DA	88:C8:87:ED:45:DA	88:CB:87:ED:45:DA	50:3D:E5:C4:05:83	192.168.1.3	GigabitEthernet1/0/

- Step 12 You have the option of un-quarantine or clearing the endpoint either through the Dashboards or directly in ISE. We will un-quarantine the endpoint from this view.
- Step 13 Right-click on the MAC Address:



IBM QRadar Security Int	elligence							admin Y Help Y	Messages IBM
Dashboard Offenses Log	Activity	Network Activity	Assets Reports I	ilske Vulversbillites	Admin Cisco ISE pxGrid				System Time: 244
isco								2018-03-03 14:34 - 20	18-03-09 14:34 7 Da
Data For : Quarant	ined_Sy	stems							×
Show 10 \$ entries Dev Time		IP Address	State	MAC Address	Username I	Calling Station ID	Called StationID	NAS IP Address	EXPORT NAS Port ID
09-Mar-2018 02:29:29	662 EST	192.168.1.15	STARTED	00:50:56:86:	o puBrid ANC Actions	00:50:56:86:88:13	50:30:E5:C4:05:88	192.168.1.3	GigabitEthernet1/0/1
08-Mar-2018 11:05:58.	744 EST	192.168.1.15	STARTED	00:50:56:86:6	oxGridQRadarQuarantine oxGridQRadarPontBource	00:50:56:86:B8:13	50:3D:E5:C4:05:88	192.168.1.3	GigabitEthernet1/0/1
08-Mar-2018 10:24:20	597 EST	192.168.1.57	DISCONNECTED	88:C8:87:ED:4	oxGridQRadarShutDown DA	88:C8:87:ED:45:DA	50:3D:E5:C4:05:83	192.168.1.3	GigabitEthernet1/0/S
08-Mar-2018 10:24:20	597 EST	192.168.1.57	DISCONNECTED	88:CB-87-ED:45:D/	A 88:C8:87:ED:45:DA	88:CB:87:ED:45:DA	50:3D:E5:C4:05:83	192.168.1.3	GigabitEthernet1/0/5

Step 14 Select pxGridQRadarClear

Step 15 You should see successful status message:

IBM QRadar Security Intelligence					192.168.1.192 Says	
Dashboard	Offenses	Log Activity	Network Activity	Assets	Repor	Status : RUNNING Operation Id : ise24k.lab10.com:2
Data F	or : Quar	antined_S	ystems			

Step 16 Select OK

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

Select Operations > RADIUS > Live Logs

dentity Services E	ngine Home	+ Conter	d Visibility	- Operations	+ Policy	+ Administration + Work Centers			License Warning 📸 🔍		0
+ RADIUS Threat-Centry	NAC Live Logs	IACACS	+ Troublesho	oot + Adaptive	Network Cont	rol Reports		Click here to a	to wireless setup and visibility setup Donot	now this again.	×
Live Logs Uve Sessions											
	Misconfigured Supp	icants O	Miscon	Figured Natwork	Devices 0	RADRUS Drops O	Cilient Stopp	ed Responding O	Repeat Counter O		
	0			0		0		5	0		
								and an orall	de la companya de la		5
								Menesh Never	Show Littlet 20 records 2 Within 1	ant 3 nours 2	9
C Refresh O Reset R	epeat Counts 🖉	Export To ·								Y Filer • O	
Time	Status		Details	Repeat	Identity	Endpoint ID	Endpoint P	Authentication Policy	Authorization Policy	Authoriz	zati.
×		:			identity	Endpoint 10	Endpoint Prof.	Authentication Policy	Authorization Policy	Authoriza	rath
Mer 09, 2018 07:48:4	3.693 PM	•		0	pagrid1	00:50:56:66:88:13	Motorol-W_	Cefault >> Dot1X	Default >> Basic_Authento	el., PerrilAci	00091
Mar 09, 2018 07:48-4	2.916 PM		ä		pagrid1	00.50.56.66.88.13	Morosoft-W	Default >> Dot1X	Default >> Basic_Authentic	at PermitAci	0089
Mar 09, 2018 07:48 5	2.004 PM	2			pagrid1	00:50:56:86:88:13	Microsoft-W	Default >> Dot1X	Default >> Basic_Authentic	al PerritAo	coes
	Contraction of the	-				10 10 10 10 10 10					

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 ¥ Holp ¥ Mosso	pro lo v IBM.			
Dashboard Offenses Log Activity N	Network Activity Assets Reports R	ska Vulnersbilltes Admin Cisco ISI	E pxQrid		System Time: 2.62 P
diala cisco				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 polic	cy				
Show 10 + entries					
Mac Address		* p	folicy Name		
		No data available in	n table		
Showing 0 to 0 of 0 entries				Previous	Next

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

Configuring IBM QRadar for Cisco ISE Syslog Events

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

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

Step 1 Configure log source on IBM QRadar

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

a. Open the IBM QRadar Console

b. Select Admin > Data Sources > Log Sources

Admin	Oeploy Changes Advance	ed ▼				
 System Configuration 	🔱 There are no changes t	to deploy.				
v Data Sources	Data Sources					
Events Flows	Events					
 Vulnerability Remote Networks and Services Configuration 	DSM Editor	WinCollect	Log Sources			
Try it out						

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

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

- Log Source Name and Description: Cisco_ISE
- Log Source Type Cisco Identity Services Engine
- Protocol Configuration: UDP Multiline Syslog
- Log Source Identifier: IP Address of your ISE MNT node(s)
- Listen port (leave default 517)
- Message ID Pattern: CISE_\S+ (\d{10})
- Source Name Formatting String (researching)

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

Log Source Summary	×
Cisco_ISE Cisco Identity Services Engine Status: OK	1983833.27 Last Updated 3 months ago
Over view Protector	
Name * 🕕	Cisco_ISE
Description ()	Cisco_ISE
Log Source Type 🕕	Cisco Identity Services Engine *
Protocol Type ①	UDP Mubline Syslog ~
Enabled ①	
Groups 🛈	None Available
Extension ()	~

- Note: For QRadar 7.4, this will open a new application window and will take you through a guided configuration
- d. Select Save or Finish, close the new app window
- e. Select Deploy Changes > Deploy

Configuring Cisco ISE Syslog Events

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

Step 1 Select Administration > System > Logging > Remote Logging Targets

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

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

dentity Services Engine	Home	Operations Policy A	dministration + Work Centers
System Identity Management	Network Resources Device P	Portal Management pxGrid Service	s + Feed Service + Threat Centric NAC
Deployment Licensing + Certificat	es + Logging + Maintenance	Upgrade + Backup & Restore	Admin Access Settings
CLocal Log Settings	Remote Logging Targets List > grav	dar	
Remote Logging Targets	* Name	qradar	Target Type UDP SysLog
Message Catalog Debug Log Configuration	* Host / IP Address		Status 💟 Enabled 👻
Collection Filters	Port Facility Code	517	(Valid Range 1 to 65535)
	* Maximum Length	8192	(Valid Range 200 to 8192)
	Include Alarms For this Target		

- Step 3 Select Submit/Save
- Step 4 Configure Logging Categories:

Choose AAA Audit element > Edit

dialo Ident	ity Ser∨ices Er	ngine _{Ho}	me 🕨 Cor	ntext Visibility	 Operations 	Policy
	Identity Mana	agement 🕨 Ne	atwork Resour	ces 🕨 Device F	ortal Manager	ient pxGrid Servi
Deploymen	t Licensing	 Certificates 	- Logging	Maintenance	Upgrade	Backup & Restor
Log Settings Remote Logg	ing Targets	G	.ogging Cat	egories		
Logging Cate	gories		/ Edit			
Message Cat	alog		Parent Ca	tegory		Category
Debug Log C	onfiguration		AAA Audit	t		AAA Audit

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

cisco Identity Services Engine	Home + Context	Visibility + Operation	ons + Policy	- Administration	Work Centers
-System + Identity Management +	Network Resources	Device Portal Manag	ement pxGrid Se	rvices + Feed Servi	ice
Deployment Licensing Certificates	s - Logging + Ma	aintenance Upgrade	Backup & Resto	Fre Admin Access	Settings
C Local Log Settings Remote Logging Targets	Logging Categories I Logging Catego	List > AAA Audit ry			
Logging Categories	Name	AAA Audit			
Message Catalog	Log Severity Level	INFO			
Debug Log Configuration		(Log level can not be o	changed.)		
Collection Filters	Local Logging	0			
	Targets	Available:		Selected:	
		ProfilerRadiusProbe SecureSysiogCollect	tor	LogCollector	
			<	1	
			>		
			~		

Step 6 Select Save

- Step 7 Perform previous steps for additional elements: Passed Authentications, Failed Attempts, Accounting, RADIUS Accounting, Administration and Operational Audit, Posture and Client Provisioning Audit, and Profile
- Step 8 When completed, you should see elements with QRadar listed in the Targets column where appropriate

cisco Identity Services Engine	Home + Context Visibility + Operations	+ Policy - Administration + Work Cen	88		License
System + Identity Management + 1	Network Resources	pxGrid Services + Feed Service + Three	t Centric NAC		
Deployment Licensing + Certificates	+Logging + Maintenance Upgrade + Bac	kup & Restore + Admin Access + Settings			
0	🖊 Edit				Sh
Local Log Settings	Parent Category	Category	Targets	Severity	Local Log L
Remote Looping Tamate	O AAA Audit	AAA Audit	LogCollector,gradar	INFO	enable
remote cogging inigers.	0	Failed Attempts	LogCollector, ProfilerRadiusProbe, gradar	INFO	enable
Logging Categories	0	Passed Authentications	LogCollector, ProfilerRadiusProbe, gradar	INFO	disable
Message Catalog	O AAA Diagnostics	AAA Diagnostics	LogCollector	WARN	enable
Debug Log Configuration	0	Administrator Authentication and Authorization		WARN	enable
Collection Ellierr	0	Authentication Flow Diagnostics		WARN	enable
Constant Prints	0	Identity Stores Diagnostics		WARN	enable
	0	Policy Diagnostics		WARN	enable
	0	RADIUS Diagnostics	LogCollector.	WARN	enable
	0	Guest	LogCollector	INFO	enable
	0	MyDevices	LogCollector	INFO	enable
	0	AD Connector	LogCollector	INFO	enable
	0	TACACS Diagnostics	LogCollector	WARN	enable
	O Accounting	Accounting	LogCollector,gradar	INFO	enable
	0	RADIUS Accounting	LogCollector, Profiler Radius Probe, gradar	INFO	enable
	0	TACACS Accounting	LogCollector	INFO	enable
	O Administrative and Operational Audit	Administrative and Operational Audit	LogCollector,gradar	INFO	enable
	O External MDM	External MDM	LogCollector	INFO	enable
	O PassiveID	PassivelD	LogCollector	INFO	enable
	O Posture and Client Provisioning Audit	Posture and Client Provisioning Audit	LogCollector, ProfilerRadiusProbe, gradar	INFO	enable
	O Posture and Client Provisioning Diagnostics	Posture and Client Provisioning Diagnostics	LogCollector	WARN	enable
	O Profiler	Profiler	LogCollector,gradar	INFO	enable
	O System Diagnostics	System Diagnostics	LogCollector	WARN	enable
	0	Distributed Management		WARN	enable
	0	Internal Operations Diagnostics		WARN	enable
	0	Licensing	LogCollector	INFO	enable
	0	Threat Centric NAC	LogCollector	INFO	enable

Performing ISE ANC Mitigation Actions Through IBM QRadar Syslog Events

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

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

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

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

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

Creating Custom Field for Framed IP Address ISE Syslog Event

Step 1 In IBM QRadar, select Log Activity > Search > New Search > Manage Groups

Create New Group > Cisco_ISE

You should see the Cisco ISE group:
😻 Event Search Groups - Mozilla	• Firefox 50/console/do/core/gene	rictree	
New Group 🔐 Edit 📄 Copy	Remove		
🖃 😂 Event Search Groups 🔺	Name	User	Desc
- 🗀 Authentication, Iden	CAUTA Authentication, Iden	admin	Information about user authorization
- Cisco ISE pxGrid	Cisco ISE pxGrid	admin	
- Cisco_ISE	Cisco_ISE	admin	Syslog ISE
- Compliance	Compliance	admin	Information related to a variety of co
😑 🧀 Log Sources	C Log Sources	admin	This group contains log source sp
🖻 🗀 AntiVirus	Detwork Monitoring	admin	Information related to monitoring a
- CO ACS	C Security (Malware,	admin	Information related to security of ne
- All AntiVirus	C System Monitoring (admin	Information related to the health an
- Endpointprote	C Usage Monitoring	admin	Information around the usages of a
- McAfeeEpo	Cther Other	admin	The group contains ungrouped iter
- Officescan			
SymantecSys			
🖨 🧰 Applications / OS			

Step 2 Close the **Search groups** page and select the newly created **Cisco_ISE Group** for **Saved Searches**

IBM QRad	ar Securit	y Intelligenc	9		
Dashboard	Offenses	Log Activity	Network Activity	Assets	Reports
🏹 Manage Sear	rch Results 👔	Manage Custom F	Properties		
Saved Searche	s Group:C	isco_ISE		Mana	ge Groups

Step 3 Keep the Search defaults

IBM QRad	ar Security	y Intelligenc	•										
Dashboard	Offenses	Log Activity	Network Activity	Assets	Reports	Risks	Vulnerabilities	Admin	Cisco ISE pxGrid				
Kanage Sear	ch Results 🔞	Manage Custom F	roperties										
Search Mode													
O Basic Searc	1	Advanc	ed Search										
Time Range:													
Real Time (s	treaming)	C Last Int	erval (auto refresh)	ORec	ent		O Specific	Interval					
					Last 5 Minut	ers 🔹	Start	Time	3/11/2018	*	at	7:25 PM	*
						_	End 1	lime	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	Group By:
Destination Port Log Source Log Source Group Source Asset Name Source IP	Columns Event Name
Event Name Event Description Domain Anomaly Alert Value Associated With Offense	Log Source
Credibility Custom Rule Custom Rule Partially Matched Custom Rule Partial or Full Matched Destination MAC	Category Source IP Source Port
Destination Network Destination Network Group Duplicate	Order By: Start Time Desc
	Results Limit

Step 5 Under Search Parameters > Parameter > Quick Filters

Select Log Source (Indexed) > Equals > Log Source Filter > Cisco_ISE Add Filter

SECURE ACCESS HOW-TO GUIDES

Search Parameters				
Parameter:	Operator:	Value:		
Log Source [Indexed] +	Equals -	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				
Remove Selected Filters				

Step 6 Click Search

A CONTRACT OF A					edr	un V Hol	p w Messages	IBM.
Dashboard Offenses Log Attivity Network Activity	Assats Reports Risks Val	nenblittes Admin	Cieco ISE pxGrid				Spile	Tele TATPA
Search	Sava Reads 👸 Carner 🤸 False Poster	Rules V Actors V						► 0
Quick Filter +							Se	arch
Current Filters:	ing real time events (Paused) Vi	ew Select An Option	Display: Defau	ut (Normalized)				
and a second second second second								
Event Name	Log Source	Event Count	Time 🕶	Low Level Category	Source IP	Source Part	Destination IP	Destinatio
Event Name PASSED_AUTH	Log Source Cisco_ISE	Event Count	Time -	Low Level Category Misc Login Succeeded	Source IP	Source Port 0	Destination IP 192.168.1.147	Destinatio Port 1645
Event Name PASSED AUTH RADIUS ACCOUNTING UPDATE	Log Source Cisco, ISE Cisco, ISE	Event Count	Time ¥ 1 Mar 11, 2018, 7:47:4 1 Mar 11, 2018, 7:47:4	Low Level Category Misc Login Succeeded PADRUS Session Status	Source IP 192 108 1.3 192 108 1.3	Source Port 0 0	Destination IP 192.168.1.147 192.168.1.147	Destinatio Port 1645 0
Event Name PASSED_AUTH RADIUS_ACCOUNTING_UPDATE PROFILER_ENDPOINT_PROFILING_EVENT	Log Source Cisco, ISE Cisco, ISE Cisco, ISE	Event Count	Time ¥ 1 Mar 11, 2018, 7:47:4 1 Mar 11, 2018, 7:47:4 1 Mar 11, 2018, 7:47:4	Low Level Category Misc Login Succeeded RADRUS Session Status Information	Source IP 192 168 1.3 192 168 1.3 192 168 1.3	Source Port 0 0 1645	Destination IP 192.188.1.147 192.168.1.147 192.168.1.147	Destinatio Port 1645 0 1645
Event Name PASSED, AUTH RADIUS, ACCOUNTING, LPDATE PROFILER, ENDPOINT, PROFILING, EVENT PROFILER, ENDPOINT, PROFILING, EVENT	Log Source Cisco, ISE Cisco, ISE Cisco, ISE Cisco, ISE	Event Count	Time ¥ 1 Mar 11, 2018, 7.474 1 Mar 11, 2018, 7.474 1 Mar 11, 2018, 7.474 1 Mar 11, 2018, 7.474	Low Level Category Misc Login Successed RABIUS Session Status Information	Source IP 1992 168 1.3 1992 168 1.3 1992 168 1.3 1992 168 1.3	Source Part 0 0 1645 1645	Destination IP 192.168.1.147 192.168.1.147 192.168.1.147 192.168.1.147	Destinatio Port 1945 0 1945 1945
Event Name PASSED_AUTH RADIUS_ACCOUNTING_UPDATE PROFILER_END/PONT_PROFILING_EVENT PROFILER_END/PONT_PROFILING_EVENT Cikel/SE_Alam	Log Source Cace, ISE Cace, ISE Cace, ISE Cace, ISE Cace, ISE	Event Count	Time * 1 Mar 11, 2018, 7:47:4 1 Mar 11, 2018, 7:47:4 1 Mar 11, 2018, 7:47:4 1 Mar 11, 2018, 7:47:4 1 Mar 11, 2018, 7:47:3	Low Level Category Misc Login Successed RADRUS Session Status Information Information Warning	Source IP 192 198.1.3 192 198.1.3 192 198.1.3 192 198.1.3 192 198.1.3 192 198.1.3	Source Port 0 1645 1645 0	Destination IP 192.168.1.147 192.168.1.147 192.168.1.147 192.168.1.147 192.168.1.147	Destinatio Port 1945 0 1945 1945 1945 0
Event Name PASSED_AUTH RADIUS_ACCOUNTING_UPDATE PROFILER_ENDPOINT_PROFILING_EVENT PROFILER_ENDPOINT_PROFILING_EVENT Classifies_Alarm FALED_ADN_ONLY	Log Source Cisco, ISE Cisco, ISE Cisco, ISE Cisco, ISE Cisco, ISE Cisco, ISE Cisco, ISE	Event Count	Time V 1 Mar 11, 2018, 7.47.4. 1 Mar 11, 2018, 7.47.4. 1 Mar 11, 2018, 7.47.4. 1 Mar 11, 2018, 7.47.4. 1 Mar 11, 2018, 7.47.3. 1 Mar 11, 2018, 7.47.3.	Low Level Category Misc Login Succended PADIDS Selector Status Information Information Watming General Authentication Patied	Source IP 102.168.1.3 102.168.1.3 102.168.1.3 102.168.1.3 102.168.1.47 102.168.1.147	Source Part 0 1645 1645 0 0	Destination IP 192.168.1.147 192.168.1.147 192.168.1.147 192.168.1.147 192.168.1.147 192.168.1.147	Destinatio Part 1945 0 1645 1645 0 0
Event Name PASSED, AUTH RADIUS, ACCOUNTING, LPDATE PROFILER, ENDPOINT, PROFILING, EVENT PROFILER, ENDPOINT, PROFILING, EVENT CISCIDE, AIAM FALED, AZN, ONLY FALED, AZN, ONLY	Log Source Clace, 155 Clace, 155 Clace, 155 Clace, 155 Clace, 155 Clace, 155 Clace, 155 Clace, 155	Event Count	Time ¥ 1 Mar 11, 2018, 7.47.4. 1 Mar 11, 2018, 7.47.3.	Low Level Category Misc Login Succeeded RADIXS Session Status Information Information Warring General Authentication Failed General Authentication Failed	Source IP 102.168.1.3 102.168.1.3 102.168.1.3 102.168.1.3 102.168.1.47 102.168.1.147 102.168.1.147	Source Part 0 1545 1545 0 0 0	Destination IP 192, 168, 1, 147 192, 168, 1, 147	Destinatio 1645 0 1645 1645 0 0 0
Event Name PASSED_AUTH RADIUS_ACCOUNTING_UPDATE PROFILER_ENDPOINT_PROFILING_EVENT Describe_Alam FALED_ADN_ONLY FALED_ADN_ONLY FALED_ADN_ONLY	Log Source Caco, ISE Caco, ISE Caco, ISE Caco, ISE Caco, ISE Caco, ISE Caco, ISE Caco, ISE Caco, ISE Caco, ISE	Event Count	Time ¥ 1 Mar 11, 2018, 7:47:4 1 Mar 11, 2018, 7:47:3	Low Level Category Nisc Login Successed AdDrud Season Status Information Information Varining General Authentication Failed General Authentication Failed General Authentication Failed	Source (# 192168.1.3 192168.1.3 192168.1.3 192168.1.3 192168.1.147 192168.1.147 192168.1.147	Source Part 0 1545 1545 0 0 0 0 0	Destination IP 192:168.1.147 192:168.1.147 192:168.1.147 192:168.1.147 192:168.1.147 192:168.1.147 192:168.1.147 192:168.1.147	Destinatio Port 1645 0 1645 0 0 0 0 0 0

- Note: The following steps will work with a wired connection, however with a wireless connection you will need to check RADIUS Accounting events
- Step 7 In the upper right corner, click **Pause**, and then double-click **Passed Auth (wired)** or **Radius_Acct (wireless)**
- Step 8 Click Extract Property and for New Property, then type: FramedIPAddress





Dashboard	Offenses	Log Activity	Network Activity	Network Activity Assets		Risks	Vulnerabili	ties	Admin	Pu
12 Return to	o Event List 🛛 🕼	Offense 📀 Map Ev	rent 🤸 False Positive	o Extrac	t Property	🕜 Previous	🕙 Next 🔮	Print	🔒 Obfus	ation
Event In	formation				Extract a c	ustom prop	erty from the	e payload	l of this e	vent
Event Na	me	PASSED_AUTH								
Low Leve	el Category	Misc Login Succ	eeded							
Event De:	scription	User authenticat	ion ended successfu	ully						

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}\.\d{1,3}\.\d{1,3}\.

You should see:

Property Definition					
Existing Property:	Select a p	operty		-	
ONew Property:	FramedIPA	tress			
Optimize parsing f	for rules, rep	rts, and searches			
Field Type:	IP	•			
Description:	FramedIP	Idress			h
Property Expression	n Definition				
Enabled: Selection Log Source Ty;	pe:	Cisco Identity Services Engine +			
Log Source:		All I			
Event Name	:	PASSED_AUTH Browse			
Category:		High Level Category Authentication Low Level Category Misc Login Succe	- eded	•	
Extraction					
RegEx:		ramed-IP-Address=(\b\d{1,3}\.\d{1,3}\.\d{1,3}	\.\d(1,3)\b)	Capture Group: 1	Test



Step 12 Select Test

You should see:

Property Definition		
Existing Property:	Select a pr	prostu _]
New Property:	FramedIPAd	
Optimize parsing f	or rules, repo	Text matching your expression has been highlighted in the payload.
Field Type:	IP	
Description:	FramedIPA	
		OK
Property Expression	Definition	
Enabled:		
Selection		
Log Source Ty	be:	Cisco Identity Services Engine
Log Source:		Ali
Cupat Mana		PASSED_AUTH Browse
event Name		
Ocvent Name		High Level Category Authentication -
Category:		High Level Category Authentication
Category:		High Level Category Authentication Low Level Category Misc Login Succeeded
Category:		High Level Category Authentication

Step 13 Select OK

Step 14 Select Save

Step 15 Ensure you see you see the FramedIPAddress appear:

IBM QRadar Security Intelligence											
Dashboard Offen	Log Activity	Network Activity	Assets	Reports	Risks	Vulnerabilities	Admin	Cisco ISE pxGrid			
Return to Event List	Offense 🙆 Map Even	t 🔸 False Positive	Extract Pr	operty 😡	Previous	Next Brint	🔒 Oblusca	lon ¥			
Event Information											
Event Name	PASSED_AUTH										
Low Level Category	Misc Login Succeed	ed									
Event Description	User authentication	anded successfully									
Magnitude	-			(6)	Releva	ance 10)				
Username	pxgrid1										
Start Time	Mar 11, 2018, 7:47:4	2 PM			Storag	je Time M	ar 11, 2018	3, 7:47:42 PM			
FramedIPAddress (custom)	192.168.1.15										

- Step 16 Select Return to Event List
- Step 17 Select Search > Edit Search > Saved Searches > Group: Cisco_IS
- Step 18 Scroll down to Column **Definition** > **Available Columns** > **FramedIPAddress(Custom)** > Move to columns by selecting ">"
- Note: You can search for the value instead of scrolling through list

SECURE ACCESS HOW-TO GUIDES



Dashboard	Offenses	Log Activity	Network Activity	Assets	Reports	Risks	Vulnerabilities	Admin	Cisco ISE pxGrid	
🕻 Manage Ser	rch Results 🛛 👔	Manage Custom F	roperties							
iplay: Cus	tom	·	Save Column	Layout						
Available Co Dormant Of Duration_H Duration_M Duration_S Element (ou Event Sum EventID (cu Events per	umns ense Count (c purs (custom) nutes (custor conds (custor stom) stom) stom) Second Coale:	bustom) n) m) sced - Average 1	I Min (custom)			>	Group By:			0
Events per 3 Events per 3 External ID File Hash (of File ID (cust File Path (ci Filename (of Flow Source Flows per S Flows per S	Second Coale: Second Raw - Second Raw - (custom) ustom) om) (stom) (custom) (custom) (custom) econd - Avera econd - Peak	Average 1 Min (Peak 1 Sec (cu: ge 15 Min (custor) 1 Min (custor)	ec (custom) custom) stom)			> <	Source Port Destination IP Destination Po Username Magnitude FramedIPAdd	ort ress (custo	m)	0
FramedIPAG FramedIPAG Function co	dress (custon dress2 (custo de (custom)	n) vm)					Order By: Start Time		- Desc	-

Step 19 Select Filter

Now, you should see the custom FramedIPAddress field

IBM QR	idar Security Intelliger	nce								admin ¥	Help ¥ Messa	m Ov IBM.
Dashboar	differences Log Activit	y Network Activit	y Assets Re	queta Riaka Vu	Anerstoffittee Admit	n Cless IBE part	hid					Dyslam Time: 8:24 PM
Search*	Quick Searches • ¥ All File	- Manadana E	Same Romains 🙀 G	aron 🔖 Fala Poston	Rules V. Addres V							► 0
luick Filter											Se	arch
		Ve	wing real time e	vents (Paused) N	New: Select An Op	tion: • Displ	ay: Custom +					
og Source is	Cisco_ISE (Clear Filter)											
	Event Name	Log Source	Event Count	Start Time *	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude	FramediPAddress (custom)
	PASSED_AUTH	Cisco_ISE		1 Mar 11, 2018, 8	Misc Login Succ	192.168.1.3	0	192.168.1.147	1645	pxgrid1		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	And and a state	182.168.1.15
	PASSED_DYNAMIC_ATZ	Cisco_ISE		1 Mar 11, 2018, B	General Authent	192.168.1.3	0	192.168.1.147	0	NA	Address to the	N/A.
	RADIUS_ACCOUNTING	Cisco_ISE		1 Mar 11, 2018, B	RADIUS Sessio	192.168.1.3	0	192.168.1.147	0	NA	Address to the	NA
	FAILED_ATTEMPT_DY	Cisco_iSE		1 Mar 11, 2018, 8	General Authent	192.168.1.3	0	192.168.1.147	Ô.	NA		NOA.
	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.
	CiscolSE_Alarm	Cisco_ISE		1. Mar 11, 2018, B	Warning	192.168.1.147	0	192.168.1.147	0	N/A	Statement of the local	NOA.
	AUTHEN PASSED	Cisco_ISE		1 Mar 11, 2018, B	Admin Login Su	192.168.1.136	0	102.168.1.147	0	admin		NIA
	AUTHEN_FAILED	Cisco_ISE		1 Mar 11, 2018, B	Admin Login Fal	192.168.1.136	0	192.168.1.147	0	admin		N/A.
	RADIUS_ACCOUNTING	Cisco_ISE		1 Mar 11, 2018, B	PADIUS Sessio	192.168.1.3	0	192.168.1.147	0	NA	And and a second second	NA.

ANC Mitigation Syslog Event Example

Step 1 The user has been successfully authenticated through ISE

dentity Services Engine	Home + Conte	ot Visibility	Operations	+ Policy	+ Administration + Work Centers				License Warning 🔺	- a,	-0-4	5 0
+RADIUS Threat-Centric NAC	Uve Logs + TACACS	+ Troublesh	ool + Adaptive	Network Contr	ol Reports		Click	here to do wireler	is setup and visibility set	tup Do re	st show this	egen X
Live Logs Live Sessions												
Misco	enfigured Supplicants O	Miscor	vfigured Network	Devices O	RADIUS Drops O	Client Stopp	ed Responding	0	Repeat Counter O			
	0		0		0		5		0			
							aftesh Never	: Show	Latest 20 records \$	Within	Last 3 hos	
C Refresh O Reset Report	Counts 🕹 Export To •										Y Filter •	••
Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P	Authenticatio	n Policy	Authorization	Policy	1	Authorizat
ж				identity.	Endport 10	Endpoint Prof.	Authenticebor	Paloy	Authorization P	alicy		Authoriza)
Mar 09, 2018 10:49:41,441	РМ 🔵	a	0	pagndt	00.50.56 86 88 13	Microsoft-W	Default >> Dot	ux.	Default >> Basic	Authen	tost. F	4emitAcce
Mar 09, 2018 10:49:40.488	PM 🚦	.o		pagrid1	00.60.56.86.88.13	Microsoft-W	Default >> Dot	tx	Default >> Basic	Autor	feat. F	harmitAcce

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

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



	Security Intellig	ence								admin V	Help T Mos	anges IBM.
Destitional C	Choses Log Acti	vity Hebwork Acti	nty Assess P	Reports Risks	Volversbillities	Admin Cisco ISE	pxGrid					- Bystern Tiese, 0.54 Ph
Bearon, * Guide	claarchas V Y Aat F	mer 🙀 Sava Crista	E Save Rosats (2),	Carrow 👆 Fares Poe	live Ruiss ¥ Activ	ni ¥						0
Records Match	ed Over Time											
Renet Augen											3/9/18.5:24 PM -	3/9/18, 5:54 PM :
10												
		\wedge									1	
53+ PM	5:26 PM 5	28 PM 5 30 P	5.32 PM	5.34 PM	5-36.PM	3-38 PM S- Update Details PHite Overla	40 PM 5:42 P	5.44 PM	5:46 PM	S-48.PM	5.50 PN 5	52 PM 5:54 I
5Serve	5.25 FM 5	28 PM 5 30 P	N 5:32 PM	5.34 PM	S.35.PM	S 38 PM S Update Cetails 2Hite Durse Source IP	40 PM 5.42 F	Destination IP	5:46 PM Destination Port	S.4E.PM	5.50 FM 5. Magnitude	52 PM 5-54 I
5Serm	5.25 FM 5	28 PM 5 30 P	W 5:32 PM	5-34 PM Start Time * 1 Mar 9, 2018, 5-5	5:35.PM Low Level Category Admin Login Su	5-38 PM 5- Update Details PHite Darba Bourse IP 192,105,1,138	40 PM 5 42 P Source Port	Destination IP 192,108,1,147	5:46 PM Destination Port	5.48 PM	S SO PH S	52 PM 5.54 I
s3+m	5.26 FM 5	Log Source Cisco, ISE Cisco, ISE	W 5:32 PM	5.34 PM Start Time * 1 Mar 9, 2016, 5.5. 1 Mar 9, 2016, 5.5.	5.35.74 Low Level Category Admin Login Su.	5:38 PM 5- Update Details PHile Darke Bourse IP 192:105.1.138 192:105.1.38	40 PM 5 42 P Source Port 0 1645	Destination IP 192,108,1,147 192,108,1,147	5:46 PM Destination Port 0 1045	S-4E PM Username admin 00505686bb13	Magnitude	52 PM 5:54 I Framedi ⁵ Address (custom) N/A
s3+m	5.26 FM 5 Event Name AUTHEN, PASS, PROFILER, EN,	Log Source Cisco, ISE Cisco, ISE Cisco, ISE	W 5:32 PM	5.34 PM Start Time * 1 Mar 9, 2018, 5-5 1 Mar 9, 2018, 5-4. 1 Mar 9, 2018, 5-4.	5.35.PW Low Level Category Adma Login Su. Information	5.38 PM 5. Update Details PHile Darbs Bourse IP . 192.105.1.30 192.105.1.3 192.105.1.3	5 42 7 Source Port 0 1645	Destination IP 192 108 1.147 192 108 1.147 192 108 1.147	5.46 PM Destination Port 0 1045 1045	S-4E PM Username admin 00505686bb13 00505666bb13	S SO PW S	52 PM 5:54 I FramediPAddress (custom) N/A N/A N/A
53+ PM	526 FM 5 Event Name AUTHEN PASS. PROFILER, EN. PROFILER, EN.	28 FW 5-30 F Log Source Cisco, ISE Cisco, ISE Cisco, ISE Cisco, ISE	S 5:32 PM	5 34 PM Start Time * 1 Mar 9, 2018, 54, 1 Mar 9, 2018, 54, 1 Mar 9, 2018, 54, 1 Mar 9, 2018, 54,	5.35.PM Low Level Category Admin Login Su. Information Information	5.38 PM 5- Update/Detalts PHile Detal 50uree (P 192.108.1.38 192.108.1.3 192.108.1.3	50 mi 5.42 f Source Port 0 1645 1645 1645	Destination IP 192.106.1.147 192.106.1.147 192.106.1.147 192.106.1.147	5:46 PM Destination Port 0 1645 1645	5.46 PM Username admin 005056866013 005056866013 005056866013	S SO PM S	FramediPAddress (custom) N/A N/A N/A N/A
5-2+ PM	S-28 PM S Event Name AUTHEN PASS. PROFILER, EN. PROFILER, EN. RADIUS ACCO.	28 PM 5.30 P Log Source Cisco, ISE Cisco, ISE Cisco, ISE Cisco, ISE Cisco, ISE Cisco, ISE	W 5:32 PM	5 34 PM Start Time * 1 Mar 9, 2018, 54 1 Mar 9, 2018, 54 1 Mar 9, 2018, 54 1 Mar 9, 2018, 54 1 Mar 9, 2018, 54	5.35.PM Low Level Category Admin Login Su. Information Information Information RADIUS Sessio.	3.38 PM 5- Update/Details PHer/Owene 50urce IP 192 108.1.138 192 108.1.3 192 108.1.3 192 108.1.3	5 PM 5.42 P Source Port 0 1645 1645 0 0	Destination IP 192.108.1.147 192.108.1.147 192.108.1.147 192.108.1.147 192.108.1.147	5:46 PM Destination Port 0 1045 1045 1045 0	Username admin 005005886bb13 00505886bb13 00505886bb13 NA	S SO PM S	FramediPAddress (custom) NVA NVA NVA NVA NVA NVA
534 PM	5-26 FM 5 Event Name AUTHEN PKSS PROFILER, EN, PROFILER, EN, PROFILER, EN, PROFILER, EN, PROFILER, EN, PROFILER, EN, PROFILER, EN, FASSED, AUTH	28 PM 5-30 P Log Source Cisco, 85E Cisco, 85E Cisco, 85E Cisco, 85E Cisco, 85E Cisco, 85E Cisco, 85E	W 5:32 PM	5 34 PM Start Time * Mar 9, 2018, 55 Mar 9, 2018, 54, Mar 9, 2018, 54,	5-35.PM Cohegory Admin Login Su, Information Information Information RADU(5 Setsion	5.38 PM 5- Update Details PHite Durse Source IP 192 108.1.30 192 108.1.3 192 108.1.3 192 108.1.3 192 108.1.3 192 108.1.3	500 mil 5.42 f 500/ce Port 0 1645 1645 1645 0 10 10 10 10 10 10 10 10 10	Destination IP 192 108 1,147 192 108 1,147 192 108 1,147 192 108 1,147 192 108 1,147 192 108 1,147	5:46 PM Destination Port 0 1045 1045 1045 0 0 1045	Userhame admin Obciosebeh13 Obciosebb13 Obciosebb13 Obciosebb13 NiA	S-SO PM S	FramediPAddress (custom) N/A N/A N/A N/A N/A N/A
<u>19</u> a ma	S-26 FM S Event Name AUTHEN, PASS, PROFILER, EN, PROFILER, EN, PROFILER, EN, PROSEQUATION AUTHEN, PASS	28 PM 5.30 P Log Source Cisco, ISE Cisco, ISE Cisco, ISE Cisco, ISE Cisco, ISE Cisco, ISE	W 5-32 PM	5.34 PM Start Time * Mar 9, 2016, 5-5, Mar 9, 2016, 5-4, Mar 9, 2018, 5-4, Mar 9, 20	5.36.794 Low Level Category Admin Logn Su. Information Information RADIUS Serso. Ming Arole Serso. Admin Logn Su.	3.38 PM 5- Update-Details PHIs Overte Source IP 192,108,1,39 192,108,1,3 192,108,1,3 192,108,1,3 192,108,1,3 192,108,1,38	50 mil 5-42 f 50 mil 5-42 f 50 1645 1645 1645 0 0 0	M 5:44 INF Destination IP 192.108.1.147 192.108.1.147 192.108.1.147 192.108.1.147 192.108.1.147 192.108.1.147	5:46 PM Destination Port 0 1045 1645 0 1645 0 1645 0 Filter on Fi	S-4E PM Username admin 055056826b13 055056826b13 055056826b13 N/A umet/PAddress (o	S-S0 IM S: Magnitude	FramedPAddress (custom) N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A
<u>5</u> 24 PM	S-26 PM S Event Name AUTHEN PASS PROFILER, EN. PROFILER, EN. PROFILER, EN. PASSED, AUTH AUTHEN, PASS PROFILER, EN.	28 M 5.30 P	N 5.32 PM	5 34 PM Start Time * 1 Mar 9, 2016, 5:5. 1 Mar 9, 2016, 5:4. 1 Mar 9, 2018, 5:4.	5-36 PM Low Level Category Admit Logions, Information Information PADIUS Sessio, Man Logi Stud. Admit Login Su, Manadon	3.38 PM 5- Update/Details (Hite Overal) 500cmt (P) 192 108.1.38 192 108.1.3 192 108.1.3 192 108.1.3 192 108.1.3 192 108.1.3 192 108.1.3	5-42 / 5-42 /	M 5,44 PM Destination IP 192,108,1,147 192,108,1,147 192,108,1,147 192,108,1,147 192,108,1,147 192,108,1,147	5.46 PM Destination Port 0 1645 1645 0 1745 0 Fitter on Pi Fitter on Pi	S-4E PM Username admin 05505682bb13 05505682bb13 NA mmediPAddress (o tamediPAddress (o	S-SO IM S: Magnitude ustom) is 192, 160, 1 ustom) is not 192, 11	52 PM 5.54 I FramediPAddress (custom) NVA NVA NVA NVA NVA Sector 10 15
534 PM	S-26 FM S Event Name AUTHEN PKSS PROFILER EN PROFILER EN PADEUS ACCO. PASSED AUTH AUTHEN PKSS. PROFILER EN FALED ADN	28 PM 5.30 P Log Source Caso, ISE Caso, ISE Caso, ISE	S 32 PM	5 34 PM Start Time + Mar 9, 2016, 5-5. Mar 9, 2016, 5-4. Mar 9, 2016, 5-4.	5.36 PM Low Level Category Admin Logn Su. Information Information RADIUS Sesso. Ministrony Sesso. Mi	3.38 PM 5- Update-Octaits PHIN Chefts 500000 PH 192:108.1.38 192:108.1.3 192:108.1.3 192:108.1.3 192:108.1.3 192:108.1.3 192:108.1.3 192:108.1.3 192:108.1.34	5.42 / Source Port 0 1645 1645 0 0 0 1845 0 0	M 5,44 IVM Destination IP 192,108,1,147 192,108,1,147 192,108,1,147 192,108,1,147 192,108,1,147 192,108,1,147 192,108,1,147 192,108,1,147	5.46 PM Destination Port 0 1645 1645 0 0 1645 1645 0 0 1645 1645 0 0 1645 1645 0 0 1645 1645 0 0 1645 1645 0 0 1645 1645 0 0 1645 1645 0 0 0 1645 1645 0 0 0 0 0 0 0 0 0 0 0 0 0	S-4E PM Username admin 00500686b13 00500566b13 00500566b13 N/A tamediPAddress (o tamediPAddress (o	S SO INV S	52 mil 5.54 l
5.54 PM	S 28 FM S Event Name AUTHEN, PASS, PROFILER, EN, PROFILER, EN, PROFILER, EN, PROFILER, EN, PROFILER, EN, PASSEQ AUTH AUTHEN, PASS, PROFILER, EN, Casorise, Alarm	28 PM 5.38 P Log Source Cisoo, ISE Cisoo, ISE Cisoo, ISE	S 32 PM	5 34 PM Start Time + Mar 8, 2016, 5-5. Mar 9, 2018, 5-4. Mar 9, 2018, 5-4.	5.36 PM Low Level Category Adma Logray Information Information Information RADIUS Sesso. Mitternation Admin Login Su. Mitternation General Authent, Warning	3.38 PM 5- Update-Details Prim Overke Source IP 192:108.1.39 192:108.1.3 192:108.1.3 192:108.1.3 192:108.1.30 192:108.1.30 192:108.1.30 192:108.1.107	5-42 / Source Part 0 1645 1645 0 1645 0 1645 0 1645 0 0 0 0 0 0 0 0 0 0 0 0 0	M 5,44 PM Destination IP 192,108,1,147 192,108,1,147 192,108,1,147 192,108,1,147 192,108,1,147 192,108,1,147 192,108,1,147 192,108,1,147 192,108,1,147	5.46 PM Destination Port 0 1945 1945 0 1945 1945 0 1945 1945 0 1945 1945 0 1945 1945 0 1945 1945 0 1945 1945 0 1945 1945 0 1945 1945 0 1945 1945 0 1945	S-4E PM Username admin 05505682b13 05505682b13 05505682b13 N/A umediPAddress (o namediPAddress (o namediPAddress (o	S-S0 PM S: Magnitude ustom) is 192 100.1 ustom) is not 192.10	52 PN 5.54 I Framed/PAddress (custom) NVA NVA NVA NVA
5.34 PM	S-26 FM S Event Name AUTHEN PASS. PROFILER, EN. PROFILER, EN. PROFILER, EN. PROFILER, EN. FALED, ADN. CasoSE Airm CasoSE Airm	28 PM 5.30 P Log Source Cisco, ISE Cisco, ISE Cisco, ISE	Event Count	5 34 PM Start Time • 1 Mar 9, 2016, 5-5, Mar 9, 2016, 5-4, Mar 9, 2016, 5-4, 1 Mar 9, 2018, 5-4, 1 Mar 9, 5-4, 1 Mar 9, 5-4,	5.36 PM Low Level Crangory Admin Login Su. Information Information PADIUS Sessio. Admin Login Su. Information Ceneral Authors. Warning Warning	3.38 PM 5- Update Details PHIII Details PHIII Details 192 108.1.38 192 108.1.3 192 108.1.3 193 108.1.3	50 mi 5.42 / Source Part 0 1645 1645 0 1645 0 1645 0 0 0 0 0 0 0 0 0 0 0 0 0	M 5,44 PM Destination IP 102,108,1,147 103,147 103,14	S.46 PM Destination Port 0 1645 1645 0 1645 0 1645 0 1647 0 1648 0 1647 0 1648 0 1649	S-4E PM Username atime occossable 13 occossable 13 occossable 13 occossable 13 N/A unned IPAddress (o ource or Destination K_	S SO INV S	52 PM 5.54 I
5.Serve	S 28 FM S Event Name AUTHEN PKSS PROFILER, EN, PROFILER, EN, PASED AUTH AUTHEN, PKSS, PROFILER, EN, FALED ADN, CasolSE, Alarm CasolSE, Alarm	28 PM 5.30 P Log Source Gaoo, 65E Caoo, 65E Caoo, 55E Caoo, 55E Caoo, 55E	Event Count	5 34 PM Start Time + Mar 9, 2016, 5-5. Mar 9, 2016, 5-4. Mar 9, 2016, 5-4.	5.36 PM Low Level Zalegory Admit Logn Su- Information Information Information Information RADIUS Setsio. Mind Logn Su- Information General Authent, Warning Warning	3.38 PM 5- Update-Details JHim Overhil Source IP 192,108,1,138 192,108,1,3 192,108,1,3 192,108,1,3 192,108,1,3 192,108,1,37 192,108,1,147 192,108,1,147 192,108,1,147	5.42 / Source Part 0 1645 1645 0 0 0 1845 0 0 0 0 0 0 0 0 0 0 0 0 0	M 5,44 PM Destination IP 192,108,1,142 192,108,1,147 193,108,1,147 194,108,108,108,108 194,108,108,108 194,108,108,108 194,108,108 1	S.46 PM Destination Port 0 1645 1645 0 7047 1845 0 70 71 72 73 74 74 74 74 74 74 74 74 74 74 74 74 74 74 74	S.4EPM Username admin 005005805b13 005005805b13 005005805b13 N/A ramediPAddress (o ourse or Destination r	S SO IN S Magnitude ustom) is 192 100.1 ustom) is not 192 100.1.15	Framed/PAddress (custom) NVA NVA NVA NVA NVA NVA NVA NVA NVA NVA
5.Serve	S 28 FM S Event Name AJTHEN, PASS, PROFILER, EN, PROFILER, EN, PROFILER, EN, PROFILER, EN, PROFILER, EN, PROFILER, EN, Casolise, Alarm Casolise, Alarm Casolise, Alarm Casolise, Alarm	28 PM 5.30 P Log Source Cisoo, iSE Cisoo, ISE Cisoo, ISE	S 32 PM	5 34 PM Start Time + Mar 8, 2016, 5-5. Mar 9, 2018, 5-4. Mar 9, 2018, 5-5. Mar 9, 2018, 5-5. Mar 9, 2018, 5-5. Mar 9, 2018, 5-5.	5.36 PM Low Level Category S. Adma Logry S. Information Information Information RADIUS Sesso. Material Sesso.	3.38 PM 5- Update-Details Prim Overke Source IP 192:108.1.39 192:108.1.3 192:108.1.3 192:108.1.3 192:108.1.33 192:108.1.35 192:108.1.35 192:108.1.347 192:108.1.147 192:108.1.147	5-42 / Source Part 0 1645 1645 0 1645 0 1645 0 1645 0 0 0 0 0 0 0 0 0 0 0 0 0	M 5,44 PM Destination IP 192,108,1,147 192,108,1,147 192,108,1,147 192,108,1,147 192,108,1,147 192,108,1,147 192,108,1,147 192,108,1,147 192,108,1,147 192,108,1,147 192,108,1,147	5.46 PM Destination Port 0 1645 1645 0 1645 1645 0 1645 1645 0 1645 1645 0 1645 1645 0 1645 0 1645 1645 0 1645 1645 0 1645 1645 0 1645 164	S-4E PM Username admin 05505682b13 05505682b13 05505682b13 N/A unnetiPAddress (o numetiPAddress (o num	5.50 PM 5. Magnitude ustom) is 192 168.1 ustom) is not 192.1 192.168.1.147	52 PM 5.54 I
5.Serve	S-26 FM S Event Name AUTHEN PASS PROFILER EN. PROFILER EN. PROFILER EN. PROFILER EN. PROFILER EN. PASSED AUTH AUTHEN PASS AUTHEN PASS AUTHEN PASS PROFILER EN. PALED ADN Classifie Alarm Classifie Alarm Classifie Alarm Classifie Alarm Classifie Alarm	28 PM 5.30 P Log Source Caso, ISE Caso, ISE Caso, ISE	Event Count	5 34 PM Start Time * 1 Mar 9, 2016, 5-5, Mar 9, 2016, 5-4, Mar 9, 2016, 5-4, 1 Mar 9, 2018, 5-2, 1 Mar 9, 2016, 5-2, 1 Mar 9, 20	5.36 PM Low Level Category Admin Logn Su. Information Information Mormation RADIUS Sesso. Mormation Consult Authorst. Warning Warning Warning Unknown	3.38 PM 5- Update-Octaits PHIN Outling 5000000 PHIN 000000 1922108.1.30 1922108.1.30 1922108.1.30 1922108.1.30 1922108.1.30 1922108.1.30 1922108.1.30 1922108.1.31 1922108.1.147 1922108.1.147 1922108.1.147	5.42 / 5.42 /	M 5,44 PM Destination IP 192,108,1,147 193,108 193	S.46 PM Destination Port 0 1645 1645 1645 1645 1645 0 Filter on F 0 Filter on F 0 Filter on F 0 Quick Filter 0 S. False Poil	S.4E PM Username admin opposeb 13 opposeb 13 opposeb 13 opposeb 13 nvA sumetiPAdress (o rumetiPAdress to rumetiPAdress to rum	5.50 PM 5. Magnitude ustom) is 192.168.1 ustom) is not 192.1 P is 192.168.1.15	52 mil 5.54 l

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

Step 3 Select More Options > Cisco pxGrid - ANC Quarantine

cisco.

	Security Intellig	ence					_			edmin V	Help ¥ Me	IBM.
Deshboard (Monsee Log Act	vity Hetwork Act	with Assets R	eporta Rieka	Vulnerabilities A	udmin Claco IBE	pxGrid					System Time: 5:57 (
Barch. ¥ Guid	Searches • ¥Ass7	ther 🙀 Save Orberts	E Save Results (6), (Carroni 🐁 False Poet	tun Ruins V Actions							0
Records Match	ed Over Time											
8aaani 2aaani 10											3/9/18, 5:24 PM	- 3/9/18, 5:54 PM \$
5								- 55				
534 PM	5:26.PM 5	28 PM \$ 30 I	PM. 5:32.9M	5:34 PM	5:36 PM	5.38 PM So Update Details	45 PM 5.42 P	M 5.44 PM	5:46 PM	5.48 PM	5.50 PM	5:52 PM 5:54 I
stam.	5:26 PM 5	(28 PM 5.30 I	PM. 5:32 PM	5:34 PM	5:36 PM	5.38 PM S- Update Details (Has Chanc)	65 PM 3:42 P	M 5:44 PM	5:46 PM	5.48 PM	5.50 PM	5:52 PM 5:54
stam.	5:26.PM 5	28 PM 5 30 1	PM 5:32 PM	5:34 PM Start Time •	5:36 PM	5.38 PM 5- Update Details (Hor Chang) Source IP	Source Port	M S.44 PM Destination IP	5:46 PM	5.48 PM	5.50 PM	FramediPAddre (custom)
sBa M	S-26 PM S Event Name AUTHEN, PASS. PROFILER, EN. PROFILER, EN.	28 PM 5:301 Log Source Cisco, ISE Cisco, ISE Cisco, ISE Cisco, ISE Cisco, ISE	PM 5:32 PM Event Count 1 1 1 1	5:34 PM Start Time ~ Mar 9, 2018, 54 Mar 9, 2018, 54 Mar 9, 2018, 54	5:36 PM Low Level Category Admin Login Bu- Information Information	5.38 PM 5- Update Details (Hos Chung) Source IP 192.168.1.36 192.168.1.3 192.168.1.3	0 PM 3.42 P Source Port 0 1645 1645	Destination IP 192 168 1 147 192 168 1 147 192 168 1 147 192 168 1 147	5:46 PM Destination Port 0 1645 1645	5.48 PM Username admin 00505686bb13 00505686bb13 00505686bb13	S SO PM	FramediPAddre (custom) N/A N/A N/A N/A

Step 4 You should see a successful status message:



Step 5 Select OK

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

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

-deter Identity Services Engine	Home + Conte	ed Visibility	+ Operations	+ Policy	+ Administration + Work Centers			License Warning 🍓 🔍	• •	•
+ RADIUS Threat-Centric NAC	Live Logs + 1ACACS	+ Troublesho	ot. + Adeptive	Network Contr	ol Reports		Click here to do	wireless setup and visibility setup Ds-n	of show this as	X Net
Live Logs Uve Sessions										
Miscor	rfigured Supplicants O	Miscon	figured Network	Devices 0	RADRUS Drops O	Client Stopp	ed Responding O	Repeat Counter O		
	0		0		0		5	0		
	170						0 5 0			
							latresh Nevor	Show Latest 20 records 3 Within	Last 3 hours	a 🔹
C Refresh O Reset Repeat 0	Counts 🕹 Export To •								¥ Filer •	••
Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P	Authentication Policy	Authorization Policy	Au	thorizati.
×				identity	Endprint ID	Endpoint Prof.	Authentication Policy	Authorization Policy	A	uthorizantia
Mar 08, 2018 10:58:37.375	м о	.0	0	page101	00.50.56.66.88.13	Microsoft-W_	Default >> Dot1X	Default >> ANCQuarant	ne Qu	variantimed.
Mar 09, 2018 10:59:37 261 F	PM 🖬	à		pagrid1	00.50.56.86.88.13	Microsoft-W	Default >> Dot1X	Default >> ANCQuarant	ne Qu	arantined.
Mar 09, 2018 10:59:36.193 F	PM 🖸	0			00:50:56:86:88:13					

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

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

IBM QRadar Security Intelligence	admin 🔻 Help 🔻 Mossages 🗣 IBM.
Dashboerd Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities	Admin Cisco ISE pxOrld System Tine: 802 P
diala cisco	2018-03-03 18:02 - 2018-03-09 18:02 7 Day
Passed Authentications Failed Authentic	cations Devices Compliance Trustsec MDM ANC Details
Currently Assigned ANC policy Show 10 + entries	
Mac Address *	Policy Name 0
00:50:56:86:88:13	pxGridQRadarQuarantine
Showing 1 to 1 of 1 entries	Previous 1 Next

Step 8 To un-quarantine or clear the endpoint:

Select ISE > Operations > Adaptive Network Control > Endpoint Assignment

thete identity Services Engine Home + C	Context Visibility • Operations	+ Policy + Administration	+ Work Centers	License Warning 🛕 🔍 🔍	• •
+ RADIUS Threat-Centric NAC Live Logs + TACAO	CS + Troubleshoot + Adaptive 1	Network Control Reports		Click here to do wireless setup and visibility setup Do not show this	s again.
Policy List Endpoint Assignment					
List					
				RowsPage 1 = 1 /1 = 00 110	tal Rows
🗘 Refresh 🔸 Add 📋 Trash • 🔅 Edit.	EPS unquarantine			¥ Filter •	۰.
MAC Address Policy N	ame	Policy Actions			
D 00:50 56:86:88:13 pxQ6dQR	tadarQuarantine	(QUARANTINE)			

Step 9 Select the endpoint MAC address > Trash

dentity Services En	gine Home + C	Context Visibility + Opi	erations Policy	Administration	Work Centers	License Warning 🔺
+ RADIUS Threat-Centric	NAC Live Logs + TACA	CS + Troubleshoot	Adaptive Network Control	Reports		Click here to do wireless setup and visibility setup
Policy List Endpoint Assig	nment					<u>k</u>
List						
1 Selected						Rows/Page 1 + 1 /1 =
	1000					
C Retresh + Add		EPS unquarantine				
MAC Address	Selected	ne	Policy Ac	tions		
00:50:56:86:88:13	pxGridQF	RedarQuarantine	QUARAN	TINE]		

Step 10 Select Selected, and then you should see:



Step 11 Select Yes

Step 12 In ISE, select Operations > RADIUS-Live Logs

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

dentity Services Engine	Home + Cont	ext Visibility	· Operations	+ Policy	Administration Work Centers			License Warning 📥 🔍		• •
RADIUS Threat-Centric NAC UV	e Logs + TACACS	 Troublesh 	oot + Adeptive	Network Cont	ol Reports		Click here to	do wheless setup and vielbility setup Do t	ot show the	a again X
Live Logs Live Sessions										
Misconfig	pured Supplicants O	Miscor	figured Network	k Devices O	RADIUS Drops O	Client Stopp	ed Responding O	Repeat Counter O		
	0		0		0		5	0		
							efresh Never	d Stow Latest 20 records d Wither	Lest 3 no	urs a
C Refresh O Reset Repeat Co.	uits 🛓 Expert To-								Y Filter	- 0-
Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P	Authentication Poli	cy Authorization Policy		Authorizat
×				Identity	Engoire D	Endpoint Prof	Authentication Policy	Authorization Policy		Authorizab
Mar 09, 2018 11:10:30 115 PM	•	ē.	0	pagnat	00.50 56 85 88 13	Microsoft-W_	Default >> Dot1X	Oefault >> Basic_Author	nicat	PermitAcce
Mar 09, 2018 11:10:32.161 PM		0		paged1	00:00:56:66 88:13	Monseh-W	Default >> Doi1X	Osfault >> Basic_Auther	idcal	ParmitAcce
Mar 09, 2018 11:10:30 219 PM					00.50.56.88.88.13					

Hovering Over IBM QRadar Syslog IP Address for ISE Contextual Information

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

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

IBM QRadar Security Intelli	gence							admin 🔻	Help ¥ 1	lessages	IBM.
Destboard Offenses Log Ac	Bvilly Network Activiliy Assets	Reports Admin	Cisco parGrid							System 1	me 10.671
Search	të Filar 🕌 Sava Otlaria 🔋 Sava Pasuti	G. Connel 🔸 Falsa Pea	itve Rules ¥ Attor								0
-											
		20/18.4.11 PM-2	UTB/18, 4 16 PM •								
Feb 10 Feb 11 Feb 1 Inte Details	2 Feb 13 Feb 14	feb 15 Feb 16	Feb 17								
de Chata)											
Start Time 🕶	Low Level Category	Source IP	Source Port	Destination (P	Destination Port	Username	Magnitude	FramediPAddres: (custom)	NAS-Port (custom)	NAS-Port- Type (custom)	NA SIPA
1 Fob 58, 2018, 415 58 FM 1 Fob 18, 2018, 413 56 FM 1 Fob 18, 2018, 413 56 FM 1 Fob 18, 2018, 415 27 FM 1 Fob 18, 2018, 415 26 FM 1 Fob 18, 2018, 415 25 FM 4	Mac Login Succeeded RADUS Session Status RADUS Session Ended Mac Login Succeeded Information RADIUS Session Stated	192,198,13 192,168,13 192,168,13 192,168,13 192,168,13 192,168,13	0	152 Stort Say Network: pxGrid Session detail	Viet-10-172- User Name Is: Mac Address Posture Statu Endpoint Pro	192 Net_192 hostip://ir 00.9C 29 s: None file: Windows?	168_0_0 Id2-PC iab10.cc C1.7B.2C 7-Workstation	9223668.17 92.168.1.7 92.168.5.7 92.168.1.7 92.168.1.7	20111 50111 Ethemet 50111 N/A 50111	Ethernet N/A Ethernet N/A Ethernet	192 168 192 168 192 168 192 168 N/A 192 168

IBM QRadar Cisco ISE pxGrid Offense Rule

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

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

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

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

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

dentity Services Engine				
RADIUS Authentications ()				
RADIUS Status: Fail From 2018-03-10 00:00:00.0 to 2018-03 Generated At: 2018-03-10 02:09:37.37	-11 00:00:00.0			
Logged At	RADIUS Status	Details	Identity	Endpoint ID
×				
2018-03-10 00:58:37.408	0	à	pxgrid2@lab10.com	00:0C:29:C1:7B:2C
2018-03-10 00:55:37.697	0	0	pxgrid2@lab10.com	00:0C:29:C1:7B:2C
2018-03-10 00:53:10.377	0	0	pxgrid2@lab10.com	00:0C:29:C1:7B:2C
2018-03-10 00:49:49.991	0	0		00:0C:29:C1:7B:2C

You can also view events in ISE.

the identity Services Engine Ho	me + Conte	d Visibility	-	Operationa	+ Policy +	Adminis	wition + Work Car	-			License Warning 💩 🔍 0 0
RADIUS Threat-Centric NAC Live Logs	+ TACACE	+ Troubl	eshoot	+ Adaptive	Network Control	Heport				Click here to do wit	siess setup and visibility setup Do not show this age
Live Logs Live Sessions					10.00						
							English at			Contraction of the second second	and bands rough
Mar 10, 2018 01:59:31.302 AM	•		+	0	LAB10 pages?	+	00:00:29:01:78:20	٠	Windows7-	Default >> Dot1X	Default >> Basic_Authenticat
Mar 10, 2018 01:58:30.971 AM		à			LAB10 pageid2		00:00:28:01:78:20		Windows7	Default >> Dot1X	Default >> Basic_Authenticat
Mar 10, 2018 01:29:06.452 AM		ö			LABIOpignE2		00100/29-01 78-20		Windows7	Default >> Dot1X	Default >> Basic_Authenticat
Mar 10, 2018 01:21:15.884 AM		à.		0			10.00.01.00.00.39		Apple-Device	Default >> Det1X	Default >> Basic_Authentical
Mar 10, 2018 01:21:15:160 AM		o					10.00/61 C0 20:39		Apple-Device	Default >> Dot1X	Default >> Basic_Authenticat
Mar 10, 2018 01:10:17.167 AM		ä			10.00.91 (9.30)	39	10.00-81 C9.3C 39		Appa-Device	Default >> MAB	Default >> Basic_Authenticat
Mer 10, 2018 12:59:44.623 AM		ā			1+g+d2@ub10.0	100	00.00.29.01.78.20		Windows7	Default >> Dot1X	Default >> Basic_Authenticat
Mer 10, 2018 12:58:42.460 AM	•						00:00:29:01:78:20				
Mar 10, 2018 12:58:37:408 AM	•	ā			pagenet2(glast=10.cs	an.	00.0C/29-C1 78-2C			Default >> Dot1X	Default
Mar 10, 2018 12:58:12:372 AM		-			Nontradia PC	Li.	00.0C 29-C1 78-2C		Windows?	Default >> DottX	Default >> Basic_Authenticat
Mar 10, 2018 12:57:40:228 AM					KompyGrid2-PC	i.	001002910178120		Windows7	Default >> Dot1X	Default >> Basic_Authenticat
Mar 10, 2018 12:56:36.686 AM		à			pagrid2@iib10.co	ini .	00.0C 29.C1 78.2C		Windows7	Default >> DoctX	Default >> Basic_Authenticat
Mar 10, 2018 12:55 37.697 AM	•	ö			p+g+d2dp+b10.0	-	00.00.29-0178-20			Default >= Dot1X	Default

Verify pxGrid offense rule via Log Activity

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

IBM QRadar Security Intelligence					admin	V Holp V	Mes
Deshboard Offenses Log Activity Network Activity	Assets Reports Risks Vul	nerabilities Admin	Ciaco ISE pxGrid				
Search. Y. Guith Searches Y. 🖞 Add Filter 🔐 Searchara 🕼 S	na fanda 👸 Garati 🔩 Fain Patha	Rules W. Actors W					
Guick Fitter *							
v	lewing real time events View:	Select An Option: -	Display: Default (No	rmakzad) =			
		(A second			Source	1001000
Event Name Information Message	Egg Source System Notification-2 : grad	Event Count	Time 1 Mar 9, 2018, 8:35:00	Low Level Category Information	Source IP 192,158.1.192	Port	Destina 127.0.0
	Add Filter						
	Parameter:	Operator:	Value:	1.2			
	Payload Contains +	is any of		Payload Co	ontains is QRadarAppForp	wGrid	
				Remove S	elected		
	2				Add Filter	Cano	el

Step 14 Select Add Filter

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



IB	M QRadar Security Intelligence						n 🔻 Help	* Motorger	IBM.
De	shboard Offenese Log Activity Network Activ	rty Assets Reports Risks Vul	nersbillbes Admin I	Clace ISE pxGrid				. System	Time 839 PM
5ee	ndh, 🔻 Guidh Seanchais V 🕎 Add Pilter 🙀 Sean Onteria Instant Joseph	🕼 Sans Hanufs 🔗 Connor 🤸 Frans Postion	Plutes ¥ Autoria ¥				3/9/16	, 7.54 PM - 3/918, 8	0 39 PM ¢
1		04 PM 806 PM 808 PM 810 PM	812 M 814 M 81		M 822 PM 824 PM 826 PM	828 PM 8.10 PM	8.32 PM 8	34 PM 8.36 PM 1	E 38 PM
			Upda	te Details					
			240	Owne					
	Event Name	Log Source	Event Count	Time *	Low Level Category	Source IP	Source Port	Destination IP	Destination
	pxGrid UserSessions	pxGrid		Mar 9, 2018, 8:29:07	User Activity	192.168.1.192	0	192.168.1.192	0
	pxQrid UserSessions	pxGrid		Mar 9, 2018, 8:21:14	User Activity	192.168.1.192	0	192.168.1.192	0
	pxGrid UserSessions	pxGrid		Mar 9, 2018, 8:21:06	Upor Activity	192.165.1.192	0	192,168.1.192	0
	pxOrid UserBessions	pxGnd		Mar 9, 2018, 8:10:18	User Activity	192.168.1.192	0	192.168.1.192	0
	pxGrid UserSessions	pxGrid	1	Mar 9. 2018. 6:15:03	User Activity	192.168.1.192	0	192.168.1.192	0
	pxGrid UserSessions	pxGirid	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 :: gradar2		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 :: gradar2	3	Mar 9, 2018, 7:58:00	SIM User Acton	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
	pxOnid UserBessione	pscGrid		Mar 9, 2018, 7:56:30	User Activity	192.168.1.192	0	192.168.1.102	0
	pxOrid Radius Falure	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 0, 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	patGrid	1	Mar 9, 2018, 7:54:12	User Activity	192.168.1.192	0	192.168.1.192	0



You will see:

Offense 1 (All	Categories)										
Offense 1		Summary Disp	olay 🔻 🔓 E	vents	Connectio	ons 🔍 Flows	New /	Attack Path	Actions ¥	Print 🕜	
Magnitude			Status		Relevance 5 Severity 4 Credibility						
	Description pxGrid Radius Failure		Offense 1	ype	pxGrid_src	(custom)					
Description			Event/Flo	w	3 events an						
Source IP(s)	<u>192.168.1</u>	Start		Mar 9, 2018, 7:53:10 PM							
Destination IP(s)	192.168.1	.192	Duration		5m 27s						
Network(s)	Net-10-17	2-192.Net 192 168 0 0	Assigned	to	Unassigned	1					
Offense Sou	rce Summa	iry									
Custom prop	perty value	192.168.1.60									
Offenses	ffenses 1					Events/	Flows 1				

Verify pxGrid offense rule via Offenses Dashboard

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

IBM QRadar Security	Intelligenc	:0								admin T	Holp W Mean	IBM.
Destitioned Offenses	Log Activity	Hete	ork Activity Assats	Reports Hisks	Vulnerabilities	Admin Cisco IS	E piQfil					Rysteen Time: 8:00 PM
Offenses	Search.	• 14	iave Orlana Actiona 🖲 🧴	- Pers							Last Reheat: (0 S 11 00 00 00
My Offenses All Offenses By Category	Curren	nt Searc de Hidd	h Parameters: en Offenses (Clear I	Filter), Exclude Clo	Ail Of	fenses Vew Offer Joar Filter)	ises: Select An Opti	M.	٠			
By Source IP	7	M		Description		Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources
By Destination IP		1	pxGrid Redius Failure			pxGrid_set (192.168.1.60		192.168.1.192	192.168.1.192	NA	pxGrd
By Network												
Rules												

Taking ISE ANC mitigations from Offenses Dashboard

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

IBM QRadar Security	Intelligenc	•							admin V	Help ¥	Massager	IBM.
Deshboard Offenses	Log Activity	Network Activity	Assets Reports Risk	a Vulnerabilities	Admin Cisco ISI	E pæGrid					Syste	n Time: 648 P
Offenses	Dearch.	• 📕 Save Criteria 🗛	allore 🕈 🔝 Print							Leaf	Plathash: 00:00:10	11 2 0
Wy Ottenses All Ottenses By Category	Curren Exclu	t Search Parameter le Hidden Offenses	(Clear Filter), Exclude Cl	All Of	fenses View Offen Sear Filter)	ses: Select An Opti	pr:	•				
By Source IP	7	la la	Description		Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs		Users	Log Sourc
By Destination IP	_	1 pxOxid RadA	ua Failura		[p=Gz4d_av6 (]	102.160 Na	rigalia	*	192.166.1.192	N/A	P	wQind
By Network						Ru	rmation • Vulnerability Sca	· ·				
Rules						Ru	Forensics Recov	ary .				
						Rur	Forenalos Searc	n .				
						Plu	gin opõons					
							co gauno - ANC C	auarantine				
						Ca	co axGrid - ANC P	fort Bounce				

Step 2 This will trigger the ANC Quarantine:

IBM QRad	ar Securit	y Intelligenc	9		
Dashboard	Offenses	Log Activity	Network Activity	Assets	Repor
Offenses		Search	🕈 🕌 Save Criteria 🛛 A	ctions ¥ &	Print
My Offens	194				

Step 3 Select OK

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

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

their identit	y Services Engine	Home Contex	t Vebility	- Operations	+ Policy	+ Administration + Work Centers			License Warning 📥 🔍 0	0 0
* RADIUS	Threat-Centric NAC Live L	ogs + TACACS	+ Troublesho	of + Adaptive	Network Control	Reports		Click here to do wirele	se setup and visibility setup Co nvt sho	w Tris appart
Live Logs	Live Sessions									
C Refresh	C Reset Repeat Counts	差 Export To •							Ψ.	iter • • •
Time		Status	Details	Repeat	Identity	Endpoint ID	Endpoint P	Authentication Policy	Authorization Policy	Authorizati.
×		4			identity.	Endpeinin (Endpoint Prof.	Authentication Policy	Authorization Policy	Authorizatio
Mar 10	AM 52018 02:30:00:432 AM	•	iù.	0	LAB10 paged 2	00.00/29/01/78/20	Windows7-	Default >> Dot1X	Default >> ANCQuarantine	Quarantined.
Mar 1), 2018 02:30:00 145 AM	2	ä		LAB10pxpnt2	00.0C/29/C1.78/2C	Windows?	Default >> Dot1X	Default >> ANCQuarantine	Quarantined.

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

dentity Services Engine Ho	me	Operations Policy	Administration Work Centers
+ RADIUS Threat-Centric NAC Live Logs	+ TACACS + Troubleshoot	- Adaptive Network Control	Reports
Policy List Endpoint Assignment			
List			
C Refresh + Add	C Edit EPS unquarantine		
MAC Address	Policy Name	Policy Ac	tions
00:0C:29:C1:7B:2C	pxGridQRadarQuarantine	[QUARAN	TINE]

Step 6 Select the endpoint > Trash

Identity Services En	gine Home	Context Visibility	Operations Policy	Administration	Work Centers
+ RADIUS Threat-Centric	NAC Live Logs + TAC	CACS + Troubleshoot	- Adaptive Network Control	Reports	
Policy List Endpoint Assign	nment				
List					
1 Selected					
C Refresh + Add	💼 Trash 🕶 🕑 Ed	it EPS unquarantine			
MAC Address	Selected	ne	Policy A	ctions	
00:0C:29:C1:7B:2C	pxGrid	QRadarQuarantine	QUARAM	ITINE]	

Step 7 Select > Selected

enses Identity Services Engine Home → Context Visit	Operations Policy Administration Work Centers
+ RADIUS Threat-Centric NAC Live Logs + TACACS + Tr	And a second descent descent descent
Policy List Endpoint Assignment	Are you sure you want to delete selected Item(s)?
114	
List	
1 Selected	res .

Step 8 Select Yes

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

dentity Services Eng	gine Home + Conte	at Velbilly - Operations	+ Policy + A	dministration + Work Centers	1		License Warning d		• •	• •
*RADIUS Threat-Centric I	NAC Live Logs + TRGACS	+ Troubleshoot + Adapt	e Network Control	Reports		Click here to do	wireless setup and visibility se	itup Do na	they run a	N Mag
Live Logs Live Sessions								N.		
M	isconfigured Suppleants O	Misconfigured Netwo	rk Devices Ø	RADIUS Drops O	Client Stopp	ed Responding O	Repeat Counter O			
	0	0		12		5	0	0		
						efresh Never	\$ Show Latent 20 records	Within	Last 3 hour	s - 2
C Rafresh O Reset Rep	peat Counts 🕹 Export Ta •								¥ Filter •	۰.
Time	Status	Details Repeat	identity	Endpoint ID	Endpoint P	Authentication Policy	Authorization	Policy	A	uthorizati
×			kteroty	Endpoint /D	Endpoint Prof	Authentoston Policy	Autorization	Policy	110	iuthorizatio
Mar 10, 2018 02:39(09)	036 AM	a 0	LAB10/pxgrid2	00:0C/29/C1/78/2C	Wridows7	Default >> Dot1X	Default >> Basi	c_Authent	alt. P	ermitAcces
Mar 10, 2018 02:39:01.7	704 AM	ā		00.0C:29:C1:78:2C						

Step 10 Select Dashboard

IBM QRadar Security Intelligence			admin V Help V	Mensagen		
Dashboard Offenses Log Activity Network Activity	Assets Reports Risks Vulnerabilities Admin Claco ISI	EpxGrid		System Time: 8:33 P		
Show Dashboard Threat and Security Monitoring	1 Device Decisionary 🔐 Reneme Decisionary 🥝 Device Decisionary	Add tern ¥	Net	Permen 02.02.50 11 2 0		
Default-IDS / IPS-All: Top Alarm Signatures	My Offenses	80	Flow Blas	808		
	No results were returned to	or this item,				
	Most Severe Offenses					
There was no Time Series data for the search performed	Offense Name	Megnitude	There was no Time Series data for the search performed.			
There was no Time Series data for the search performed.	Disard Hadus Faiure					
	Most Recent Offenses					
	Offense Name					
	oxGrid Radius Failure	View in Network Activity				
View in Log Activity	Top Services Denied through Firewalls					
Top Systems Attacked (IDS/IDP/IPS)			Top Category Types	8		
			Category	Offenses		
			User Activity	1		
			Object Not Cached	0		
	There was no Time Series data for t	he search performed.	No Bate Limiting	0		
		Object Cached	0			
There was no Time Series data for the search performed.		Top Sources	8			
		Source	Offenses			
			192.168.1.192	1		

Step 11 Select pxGrid Radius Failure

Step 12 Hover over the Offense Source IP Address

IBM QReder Securi	ty Intelligenc	•												admin ¥	Help ¥	Messages	• 11	BM.
Deshtured Offenses	Log Activity	Network	Activity A	Assets 1	Reports R	tisks 1	Admenabilitie	e Admin	Cisco IS	E prGrid						System	n Timer	8.49 M
Offenses	Search.	* Maria	e Oritaria Actor	m ¥ ⊴P	144										Last	Refresh: 00.00.15	11.4	. 0
My Offenses All Offenses By Category	Curren Exclus	t Search P de Hidden	Parameters: Offenses (: (Clear Filte	er), Exclude	Ciosed	All C	Offenses (Clear Filte	View Offer	nes Select	An Optio	n:	•					
By Source IP	9	ld			Description	n		Off	ense Type	Offense S	iource	Magnitude	Source IPs	Destination IPs		Isera	Log	Sourc
By Destination IP By Network Rules		1 p	KGrid Pladius I	Falus				pec.	94d_945 (192.168.1	Networ pxGrid Right ci	rk: I Session details lick for more info	182 168 a 160 Net-10-172-192 User Name (Mac Address) Posture Status Endpoint Profile Imation on 192 168	Net_192_168_0_0 Net_192_168_0_0 AB10psgrid2 20.00_29-01.78:20 Yone Windows7-Workstation 1.60	NA	P	KGrid	

Addendums

Adding Log Activity Filter to View Session Information

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

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

BM QRadar Security Intelligence						admin 🔻 Help 🔻	Messar	985 ¹⁰ T	IRW.
Dashboard Offenses Log Activity	Network Activity As	sets Report	Admin	Cinco ISE pxG			- 6	System Time	e: 6:36 P
beach. 🔻 Guick Searches 🔻 🏹 Add Filter 🕌	Seve Orterta 😰 Garra Par	nils 🖗 Crost	4, ran r	outrie Rules V. Actions	Ŧ				11 0
Advanced Search *							0	Search	
View Event Nam Information Message Information Message Information Message	Add Filter	View: Sele	ect An Opti	on: • Display:	Value:	ŋ -		rce et	Des 127.0 127.0 127.0 127.1
Information Message Information Message Information Message Information Message Information Message Information Message Search Executed	Log Source (ind	Jexedi *	Equals		Log Source Filter:	Type to Filter SIM Generic Log DSM-7 :: gradar3 Search Results-2 :: gradar3 System Notification-2 :: gradar3 Threecom8800SeriesSwitch @ 127.0.0 pxGrid			127.0 127.0 127.0 127.0 127.0 127.0 127.0 127.0 192.
Information Message Search Completed						Add Filter	Cancel		127.0

Step 2 Add the following search criteria:

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

Step 3 Click Search

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

IBM QRadar Security Intelligence				adm	in 🔻 Help 🔻	Messages 5 v	IBM.
Dashboard Offenses Log Activity Network Activity	Assets Reports Admin Cla	ico ISE ;	ржG			System Ti	me: 6:23 PM
Search 🕈 Quick Searches 🕈 🍟 Add Filter 🕌 Bave Oritoria 📳	Save Results 🙀 Carcel 🔸 False Positive	Rules ¥	Actions T				
Advanced Search * ceid)='pxgrid' AND "pxGr	Id_EventNome"="User Sessions"	GROUP	BY "pxGrid_odNormo	lizedUser" ORDER BY value	DESC LIMIT 10 L	Searc	h
Viewing real time ev	ents View: Select An Option:	- Dis	splay: Default (Norm	alized) -			
Current Filters:							
Log Source is pxGrid (Clear Filter)							
Construction of the second							
Event Name	Log Source	Even	Time	Low Level Category	Source IP	Source	Destina
Event Name Cisco ISE pxGrid User Sessions	Log Source	Even Coun	Time Apr 19, 2019, 6:24:1	Low Level Category User Activity	Source IP	Source Port 0	Destina 169.254.3
Event Name Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions	Log Source pxGrid pxGrid	Even Cour 1	Time Apr 19, 2019, 6:24:1 Apr 19, 2019, 6:23:3	Low Level Category User Activity User Activity	Source IP 169.254.2.2 169.254.2.2	Source Port 0	Destina 169.254. 169.254.
Event Name Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions	Log Source pxGrid pxGrid pxGrid	Even Cour 1 1	Time Apr 19, 2019, 6:24:1 Apr 19, 2019, 6:23:3 Apr 19, 2019, 6:16:0	Low Level Category User Activity User Activity User Activity	Source IP 169.254.2.2 169.254.2.2 169.254.2.2	Source Port 0 0	Destina 169.254 169.254 169.254
Event Name Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions Information Message	Log Source pxGrid pxGrid pxGrid System Notification-2 :: grad	Even Cour 1 1 1	Time Apr 19, 2019, 6:24:1 Apr 19, 2019, 6:23:3 Apr 19, 2019, 6:16:0 Apr 19, 2019, 6:16:3	Low Level Category User Activity User Activity User Activity Information	Source IP 169.254.2.2 169.254.2.2 169.254.2.2 169.254.2.2 192.168.1.249	Source Port 0 0 0	Destina 169.254. 169.254. 169.254. 169.254. 127.0.0.1
Event Name Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions Information Message User Lopout	Log Source pxGrid pxGrid pyGrid System Notification-2 :: grad SIM Audit-2 :: gradar3	Even Coun 1 1 1 1	Time Apr 19, 2019, 6:24:1 Apr 19, 2019, 6:23:3 Apr 19, 2019, 6:6:0 Apr 19, 2019, 6:14:3 Apr 19, 2019, 6:14:3	Low Level Category User Activity User Activity User Activity Information SiM User Authentication	Source IP 169,254,2,2 169,254,2,2 169,254,2,2 192,168,1,249 169,254,2,2	Source Port 0 0 0 0 0	Destina 169.254. 169.254. 169.254. 127.0.0.1 192.168.
Event Name Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions Information Message User Logout User Logout	Log Source pxGrid pxGrid System Notification-2 :: grad SIM Audit-2 :: gradar3 SIM Audit-2 :: gradar3	Even Coun 1 1 1 1 1 1 1	Time Apr 19, 2019, 6:24:1 Apr 19, 2019, 6:23:3 Apr 19, 2019, 6:16:0 Apr 19, 2019, 6:14:3 Apr 19, 2019, 6:14:3 Apr 19, 2019, 6:14:3	Low Level Category User Activity User Activity User Activity Information SIM User Authentication SIM User Authentication	Source IP 169.254.2.2 169.254.2.2 169.254.2.2 192.168.1.249 169.254.2.2 169.254.2.2	Source Port 0 0 0 0 0	Destina 169,254.3 169,254.3 169,254.3 127,0,0,1 192,168. 192,168.
Event Name Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions Information Message User Logout User Logout User Logout User Logout	Log Source pxGrid pxGrid System Notification-2 :: grad SIM Audit-2 :: gradar3 SIM Audit-2 :: gradar3 SIM Audit-2 :: gradar3	Even Coun 1 1 1 1 1 1 1 1 1	Time Apr 19, 2019, 6:24:1 Apr 19, 2019, 6:24:3 Apr 19, 2019, 6:14:3 Apr 19, 2019, 6:14:3 Apr 19, 2019, 6:14:3 Apr 19, 2019, 6:14:3 Apr 19, 2019, 6:14:3	Low Level Category User Activity User Activity User Activity Information SIM User Authentication SIM User Authentication SIM User Authentication	Source IP 169,254.2.2 169,254.2.2 169,254.2.2 192,168,1,249 169,254.2.2 169,254.2.2 169,254.2.2 169,254.2.2	Source Port 0 0 0 0 0 0 0 0	Destina 169.254. 169.254. 169.254. 192.168. 192.168. 192.168.
Event Name Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions Information Message User Logout User Logout User Logout User Logout User Logout User Logout User Logout	Log Source pxGrid pxGrid System Notification-2 :: grad SIM Audit-2 :: gradar3 SIM Audit-2 :: gradar3 SIM Audit-2 :: gradar3 SIM Audit-2 :: gradar3	Even Cour 1 1 1 1 1 1 1 1 1 1	Time Apr 19, 2019, 6:24:1 Apr 19, 2019, 6:24:3 Apr 19, 2019, 6:16:0 Apr 19, 2019, 6:14:3 Apr 19, 2019, 6:14:3 Apr 19, 2019, 6:14:3 Apr 19, 2019, 6:14:3 Apr 19, 2019, 6:14:3	Low Level Category User Activity User Activity User Activity Information SiM User Authentication SiM User Authentication SiM User Authentication	Source IP 169.254.2.2 169.254.2.2 169.254.2.2 192.168.1.249 169.254.2.2 169.254.2.2 169.254.2.2 169.254.2.2	Source Port 0 0 0 0 0 0 0 0 0 0 0	Destina 169.254. 169.254. 127.0.0.1 192.168. 192.168. 192.168. 192.168.
Event Name Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions Information Message User Logout	Log Source pxGrid pxGrid System Notification-2 :: grad SIM Audit-2 :: grader3 SIM Audit-2 :: grader3 SIM Audit-2 :: grader3 SIM Audit-2 :: grader3 SIM Audit-2 :: grader3	Even Cour 1 1 1 1 1 1 1 1 1 1 1	Time Apr 19, 2019, 6:24:1 Apr 19, 2019, 6:23:3 Apr 19, 2019, 6:163 Apr 19, 2019, 6:143 Apr 19, 2019, 6:143 Apr 19, 2019, 6:143 Apr 19, 2019, 6:143 Apr 19, 2019, 6:143	Low Level Category User Activity User Activity User Activity Information SIM User Authentication SIM User Authentication SIM User Authentication SIM User Authentication SIM User Authentication	Source IP 169.254.2.2 169.254.2.2 169.254.2.2 169.254.2.2 169.254.2.2 169.254.2.2 169.254.2.2 169.254.2.2 169.254.2.2	Source Port 0 0 0 0 0 0 0 0 0 0 0 0 0	Destina 169.254. 169.254. 169.254. 127.0.0.1 192.168. 192.168. 192.168. 192.168.
Event Name Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions Information Message User Logout Us	Log Source pxGrid pxGrid System Notification-2 :: grad SIM Audit-2 :: gradar3 SIM Audit-2 :: gradar3	Even Cour 1 1 1 1 1 1 1 1 1 1 1 1	Time Apr 19, 2019, 6:24:1. Apr 19, 2019, 6:23:3. Apr 19, 2019, 6:14:3. Apr 19, 2019, 6:14:3.	Low Level Category User Activity User Activity User Activity Information SIM User Authentication SIM User Authentication SIM User Authentication SIM User Authentication SIM User Authentication	Source IP 109.254.2.2 109.254.2.2 199.254.2.2 199.254.2.2 169.254.2.2 169.254.2.2 169.254.2.2 169.254.2.2 169.254.2.2 169.254.2.2	Source Port 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Destina 169.254. 169.254. 169.254. 127.0.0.1 192.168. 192.168. 192.168. 192.168. 192.168.
Event Name Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions Information Message User Logout Information Message	Log Source pxGrid pxGrid System Notification-2 :: grad SIM Audit-2 :: grader3 SIM Audit-2 :: grader3	Even Cour 1 1 1 1 1 1 1 1 1 1 1 1 1	Time Apr 19, 2019, 6:24:1 Apr 19, 2019, 6:24:3 Apr 19, 2019, 6:160 Apr 19, 2019, 6:143 Apr 19, 2019, 6:143	Low Level Category User Activity User Activity User Activity Information SIM User Authentication SIM User Authentication SIM User Authentication SIM User Authentication SIM User Authentication SIM User Authentication SIM User Authentication	Source IP 169.254.2.2 169.254.2.2 169.254.2.2 192.168.1.249 169.254.2.2 169.254.2.2 169.254.2.2 169.254.2.2 169.254.2.2 169.254.2.2 169.254.2.2 169.254.2.2	Source Port 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Destina 169.254. 169.254. 127.0.0.1 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 192.168.
Event Name Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions Information Message User Logout Information Message Information Message Information Message	Log Source pxGrid pxGrid System Notification-2 :: grad SIM Audit-2 :: gradar3 SIM Audit-2 :: gradar3	Even Cour 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Time Apr 19, 2019, 6:24:1 Apr 19, 2019, 6:24:1 Apr 19, 2019, 6:16:0 Apr 19, 2019, 6:14:3 Apr 19, 2019, 6:14:3	Low Level Category User Activity User Activity User Activity Information SIM User Authentication SIM User Authentication SIM User Authentication SIM User Authentication SIM User Authentication SIM User Authentication Information	Source IP 169.254.2.2 169.254.2.2 169.254.2.2 192.168.1.249 169.254.2.2 169.254.2.2 169.254.2.2 169.254.2.2 169.254.2.2 169.254.2.2 169.254.2.2 169.254.2.2 169.254.2.2 169.254.2.2	Source Port 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Destina 169.254. 169.254. 127.0.0.1 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 192.168.
Event Name Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions Information Message User Logout Information Message Information Message Information Message Information Message	Log Source pxGrid pxGrid System Notification-2 :: grad SIM Audit-2 :: grader3 SIM Audit-2 :: grader3 System Notification-2 :: grad System Notification-2 :: grad	Even Court 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Time Apr 19, 2019, 6:24:1 Apr 19, 2019, 6:23:3 Apr 19, 2019, 6:16:0 Apr 19, 2019, 6:14:3 Apr 19, 2019, 6:14:3	Low Level Category User Activity User Activity User Activity Information SIM User Authentication SIM User Authentication SIM User Authentication SIM User Authentication SIM User Authentication Information Information Information	Source IP 109.254.2.2	Source Port 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Destina 169.254. 169.254. 127.0.0.1 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 127.0.0.1 127.0.0.1
Event Name Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions Cisco ISE pxGrid User Sessions Information Message User Logout User Logout User Logout User Logout User Logout User Logout Information Message Comparison Mes	Log Source pxGrid pxGrid pxGrid System Notification-2 :: grad SIM Audit-2 :: gradar3 SIM Audit-2 :: gradar3 System Notification-2 :: grad System Notification-2 :: grad System Notification-2 :: grad System Notification-2 :: grad System Notification-2 :: grad	Even Cour 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Time Apr 19, 2019, 6:24:1 Apr 19, 2019, 6:24:1 Apr 19, 2019, 6:14:3 Apr 19, 2019, 6:14:3	Low Level Category User Activity User Activity User Activity User Activity Information SIM User Authentication SIM User Authentication SIM User Authentication SIM User Authentication SIM User Authentication Information Information	Source IP 109.254.2.2 109.254.2.2 199.254.2.2 199.254.2.2 109.254.2.2 109.254.2.2 109.254.2.2 109.254.2.2 109.254.2.2 109.254.2.2 109.254.2.2 109.254.2.2 109.254.2.2 109.254.2.2 109.254.2.408.1.249 102.108.1.249 102.108.1.249	Source Port 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Destina 169.254. 169.254. 127.0.0.1 192.168. 193.168.168.168.168.168.168.168.168.168.168

Using an External Certificate Authority

This section illustrates generating certificates for the IBM QRadar pxGrid App, using the ISE internal CA. It is assumed that the ISE pxGrid node and the other ISE nodes are signed by an external CA server. In this example, there are two ISE instances. The ISE26.lab20.com node is the primary ISE instance, and contains the Primary Admin, Primary MNT, Primary pxGrid node, and PSN personas. The ISE26ca.lab10.com node is the secondary ISE instance, and contains the Secondary Admin, Secondary MNT, Secondary pxGrid, and PSN personas.

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

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

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

SECURE ACCESS HOW-TO GUIDES

cisco.

dentity Services Engine	Home	ations + Policy + Admini	stration • Work Cente	a	License Warning 🛕	% 0
System Identity Management	Network Resources Device Portal M ates Looping Maintegance Lipper	ta Barkun & Bastom A A	min Annes - Settions	Centric NAC	Click here to do wireless s	etup Do not show
Deployment Edenany + Gerand	aas roogging rimanananon opgi	se i backup a nessure i ra	anni Aconsi 🕴 Geanga			
* Certificate Management	System Certificates 🛕 For deaster	ecovery it is recommended to exp	ort certificate and private ka	ry pairs of all system certific	ates.	
System Certificates	📝 Edit 🛛 👍 Generate Self Signed Cert	icate	🗙 Delete 🔎 View			
Trusted Certificates	Friendly Name Used By	Portal group tag	Issued To	Isound By	Valid From	Expiration Date
OCSP Client Profile Certificate Signing Requests Certificate Periodic Check Setti > Certificate Authority	Vise28 OU#Certificate Services System Certificate Services U#Certificate Services se25.lab10.com#Certific ub CA - ise28400002 Default self-signed saml server certificate - CN+S SAML AML_ise26.lab10.com Admin, P CN=ise26.lab10.com#La CN=ise26.lab10.com#La Admin, P CN=ise26.lab10.	ortal, Default Portal Certificate	ise26.lab10.com SAML_ise26.lab10.com ise26.lab10.com	Certificate Services Endp oint Sub CA - ise26 SAML_tee28.lab10.com lab10-WIN-N3OR1A7H9	Tue, 5 Mar 2019 Wed, 6 Mer 2019 Sat, 23 Mar 2019	Tue, 6 Mar 2029 Thu, 6 Mar 2020 Tue, 23 Mar 202
	L-CA#00003 pxGrid, RADIUS OU=ISE Messaging Ser vice,CN=ips26 lab10.co miRCertificate Services E ndpoint Sub CA - iss2580 00001	aging	ise26.lab10.com	Certificate Services Endp oint Sub CA - ise26	Tue, 5 Mar 2019	Tue, 6 Mar 2029
	▶ іве2бса					

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

System Identity Management Deployment Licensing Certifica	Network Resources Device Portal Mantes Logging Maintenance Upgrad	agement pxGrid Services Backup & Restore + A	Feed Service Threat dmin Access Settings	Centric NAC	Click here to do wineless	setup Do not show
Certificate Management	System Certificates 🛕 For disaster re	covery it is recommended to exp	oort certificate and private ke	y pairs of all system certific	ates.	
System Certificates	/ Edit Generate Self Signed Certifi	ate 🕂 Import 🐼 Export	X Delete P View			
Trusted Certificates	Friendly Name Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date
OCSP Client Profile	▶ ise26					
Certificate Signing Requests	▼ ise26ca					
Certificate Periodic Check Setti	Default self-signed sami server certificate - CN=S SAML AML ise26.lab10.com		SAML_ise26.lab10.com	SAML_iee26.iab10.com	Wed, 6 Mar 2019	Thu, 5 Mar 202
Certificate Authority	Default self-signed saml server certificate - CN+S Not in use AML_ise25ca.lab10.com		SAML_ise25ca.lab10.co m	SAML_ise26ca.lab10.co m	Wed, 6 Mar 2019	Thu, 5 Mar 202
	Admin, Por CN×ise25ca.lab10.com/ll EAP lab10-WIN-N3OR1A7H9 Authentica KL-CA#00003 pxGind, RAD5US D	al, Default Portal Certificate Group ()	ise26ca.lab10.com	lab10-WIN-N3OR1A7H9 KL-CA	Wed, 6 Mar 2019	Sat, 6 Mar 202
	OU=Certificate Services System Certificate, CN=i se25ca lab10.com#Certif icate Services Endpoint Sub CA - ise25ca#0000 4		ise28ca.tab10.com	Certificate Services Endp oint Sub CA - ise25ca	Fri, 22 Mar 2019	Tue, 6 Mar 202
	OU=ISE Messaging Ser vice.CN=Ise28ca.lab10.c om#Certificate Services Endpoint Sub CA - ise28 cat800004	ang	ise26ca.lab10.com	Certificate Services Endp ont Sub CA - Ise26ca	Fri, 22 Mar 2019	Tue, 6 Mar 202

Step 3 Ensure that the published pxGrid nodes appear and you have pxGrid node connectivity: Select Administration > pxGrid Services

Now, you see the following:

-10-	4 1- 160	Identity Services Engine	Home + Go	ontext Visibility	+ Operati	ons + Policy	Administration	+ Work Centers	1	icense Warr	eng 💩 🔍	•
1	Sy	stem Identity Management	Network Resou	rces + Devi	ce Portal Mana	gement pxGrid \$	Services + Feed Ser	vice + Threat Centric NAC	Click	here to do w	vireless setup Do) not show t
Al	Clie	ents Web Clients Capabilitie	E Live Log	Settings	Certificates	Permissions						
VE.	rabi	le 🥝 Disable 🙄 Approve 😝 G	roup 💗 Decline	O Delete +	Refresh	Total Pending App	roval(0) +		1 - 180/18	Show	25 + per page	Page
		Client Name	Description		Capabi	ities	Status	Client Gro	up(s)		Auth Method	
		ise-fanout-ise26			Capabi	ities(0 Pub, 0 Sub)	Online (XMP	P) Internal			Certificate	
		ise-mnt-ise25ca			Capabi	ities(2 Pub, 1 Sub)	Online (XMP	P) Internal			Certificate	
		ise-pubsub-ise26ca			Capabil	Ities(0 Pub, 0 Sub)	Online (XMP	P) Internal			Certificate	
		ise-admin-ise26ca			Capabi	ities(1 Pub, 1 Sub)	Online (XMP	P) Internal			Certificate	
		ise-fanout-ise26ca			Capabi	ities(0 Pub, 0 Sub)	Online (XMP	P) Internal			Certificate	
	•	lse-bridge-ise26			Capabil	ities(0 Pub, 4 Sub)	Online (XMP	P) Internal			Certificate	
		ise-admin-ise26			Capabil	ities(4 Pub, 2 Sub)	Online (XMP	P) Internal			Certificate	
		ise-pubsub-ise26			Capabi	ities(0 Pub, 0 Sub)	Online (XMP	P) Internal			Certificate	
		wsal.lab10.com_start_test_613	15ED		Capabi	ities(0 Pub, 0 Sub)	Offline (XMP	P)			Certificate	
		wsa1.lab10.com613	15ED		Capabi	ities(0 Pub, 0 Sub)	Offline (XMP	P)			Certificate	
		wsa1.lab10.com497	ISED		Capabil	ities(0 Pub, 0 Sub)	Offline (XMP	P)			Certificate	
	•	wsa1.lab10.com498	ISED		Capabil	ities(0 Pub, 0 Sub)	Offline (XMP	PP)			Certificate	
		wsa1.lab10.com315	15ED		Capabi	ities(0 Pub, 0 Sub)	Offline (XMP	PP)			Certificate	
		firesightisetest-fmc63.lab10.com			Capabi	ities(0 Pub, 0 Sub)	Offline (XMP	PP)			Certificate	
		gradar6	pXGrid App for 0	Qradar	Capabil	ities(0 Pub, 0 Sub)	Offline (XMP	P) ANC			Certificate	
	•	iseagent-fmc63.lab10.com-285faf	GCL for C samp	le.	Capabi	ities(0 Pub, 0 Sub)	Offline (XMP	(P)			Certificate	
		nravfiled			Canabi	Hes/0 Pub. 0 Sub1	Offline (XMP	(P)			Certificate	
Conn	ecte	ed via XMPP ise26.lab10.com (ataridi	by: ise26ca)									

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

Generating IBM QRadar Certificate from ISE Internal CA

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

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

dentity Services Engine Hor	ne + Context Visibility	Operations F	Policy Administration	Work Centers	License Warning 👩 🔍 🔍
System Identity Management Net	work Resources + Devic	Portal Management (xGrid Services + Feed S	ervice	Click here to do wireless setup Do not sho
All Clients Web Clients Capabilities	Live Log Settings	Certificates Permiss	lions		
Generate pxGrid Certificates					
I want to *				3	
Common Name (CN) *					
Certificate Template	pxGrid_Certificate_Template	0			
Subject Alternative Name (SAN)					
Certificate Download Format *					0
Certificate Password *					0
Confirm Password *					
				Resot	
Connected via XMPP ise26.lab10.com (standby	: ise26ca)				

Select Administration > pxGrid Services > Certificates

- Step 2 From the I want to list, select Generate a single certificate without a signing request
- Step 3 In the **Common Name (CN)** box, enter the Fully Qualified Domain Name (FQDN) of the QRadar Instance
- Step 4 From the **Subject Alternative Name (SAN)** list, select the **IP Address**, and then enter the IP address of the QRadar instance
- Step 5 Provide a description name
- Step 6 From the Certificate Download Format list, select the PEM format
- Step 7 In the Certificate Password box, enter the encryption password



duals Identity Services Engine Ho	ne		License Warning 🛕	8	0
System Identity Management. Ne	twork Resources		Click here to do wireless se	Hup Do no	ot show t
All Clients Web Clients Capabilities	Live Log Settings Certificates Permissions				
Generate pxGrid Certificates					
I want to *	Generate a single certificate (without a certificate signing request)				
Common Name (CN) *	Gradar3.lab10.com				
Description	Grader Instance				
Certificate Template	pxGrid_Certificate_Template				
Subject Alternative Name (SAN)	IP address \$ 192.168.1.249				
Certificate Download Format *	Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)	0			
Certificate Password *		0			
Confirm Password *	[]				
	Reset Create				
Connected via XMPP ise26.lab10.com (standb)	r ise26ca)				

Step 9 Select Create

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



Step 11 Unencrypt the QRadar private key:

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

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

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

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

Note: Open ssl is on most Linux and MAC operating systems

Step 12 To download the certificate root chain:

Select Administration > pxGrid services > Certificates

-dude Identity Services Engine Hor	te + Context Visibility + Operation	ns I Policy Administratio	Work Centers	License Warning 🎪 🔍 0
System identity Management Net	work Resources + Device Portal Manage	ement pxGrid Services + Feet	Service + Threat Centric NAC	Click here to do wireless setup Do not show
All Clients Web Clients Capabilities	Live Log Settings Certificates	Permissions		
Generate pxGrid Certificates				
I want to *	Download Root Certificate Chain			
Host Names *				
Certificate Download Format *	Certificate in Privacy Enhanced Electronic	: Mail (PEM) format, key in PKCS8 P	EM format (including certificate chain) \$	0
			Roset Create	
Connected via XMPP ise26.lab10.com (standby	ise26ca)			

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

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

ulivelin identity Services Engine Home + Context Visibility + Operations + Policy + Administration + Work Centers	License Warning 🛕 🤼 😐
System + Identity Management + Network Resources + Device Portal Management pxGnd Services + Feed Service + Threat Centric NAC	Click here to do wineless setup Do not show f
All Clients Web Clients Capabilities Live Log Settings Certificates Permissions	
Generate pxGrid Certificates	
I want to * Download Root Certificate Chain \$	
Host Names * Ise26 * ise26ca	
Certificate Download Format * Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain) \$	0
Reset	P
Connected via XMPP ise26.jab10.com (standby: ise26ca)	

- Step 15 From the Certificate Downloaded Format list, select PEM format
- Step 16 Select Create
- Step 17 Download the zipped file into the same folder where you downloaded the QRadar certificate zipped files. Now, you see the following files:

ise26.lab10....68.1.133.cer ise26ca.lab10.com_.cer lab10-WIN-...H9KL-CA_.cer

Step 18 Create a new folder, for example, QRadar_all_certs. Then, copy the ISE identity certificates, for example, ise26.lab10.cer and ise26ca.lab10.com, the QRadar certificate key-pair files, the external root CA, and the ISE certificate files into this new folder.



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

Troubleshooting

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

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

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

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

Troubleshoot inside QRadar:

- 1. Take an SSH to the PxGrid Docker Container on QRadar
- In QRadar versions 7.3.2 and above run the commands:
 - 1> /opt/qradar/support/recon ps
 - 2> /opt/qradar/support/recon connect <App ID>
- In QRadar versions 7.3.1 run the commands:
 - 1> /opt/qradar/support/qapp_utils_730.py ps
 - 2> /opt/qradar/support/qapp_utils_730.py connect <App ID>
- 2. Once you are inside the PxGrid docker container, enter the following command:
- echo <ISE IP Address> <FQDN> >> /etc/hosts

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

Cisco ISE pxGrid Dashboards not populating with ISE Contextual Information

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

ANC Mitigation Actions not appearing in Dashboards

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

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

Using the IBM QRadar pxGrid App Logs for Troubleshooting

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

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

[root@	QRadar3 support]# /opt/qradar/support/recon ps			
PORT	CONTAINER	IMAGE	STATUS	appID	NAME
32768	28ac62f3a3d8	2cabd65ea8554650b3990bbdd83f59d8	RUNNING	1201	Cisco ISE
					pxGrid

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

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

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

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

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

For QRadar versions 7.3.1, run the commands:

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

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

Step 3 A successful connection will look like this:

```
2019-04-14 21:14:43,812 [abstract_qpylib.log] [Thread-1] [INFO] - 127.0.0.1
[APP ID/1201][NOT:0000006000] Primary Server: ise26.lab10.com 2019-04-14 21:14:43,812
[abstract qpylib.log] [Thread-1] [INFO] - 127.0.0.1
[APP ID/1201][NOT:000006000] Secondary Server: 192.168.1.138
2019-04-14 21:14:43,813 [abstract qpylib.log] [Thread-1] [INFO] - 127.0.0.1
[APP ID/1201][NOT:000006000] Current Active Server: primary
2019-04-14 21:14:48,933 [abstract_qpylib.log] [Thread-1] [INFO] - 127.0.0.1
[APP ID/1201][NOT:000006000] Account Activation Status: 200
2019-04-14 21:14:48,933 [abstract_qpylib.log] [Thread-1] [INFO] - 127.0.0.1
[APP_ID/1201][NOT:0000006000] Performing service lookup for:com.cisco.ise.pubsub
19-04-14 21:14:49,280 [abstract_qpylib.log] [Thread-1] [INFO] - 127.0.0.1
[APP_ID/1201][NOT:0000006000] Creating WebSocketClient....
2019-04-14 21:14:49,282 [abstract qpylib.log] [Thread-1] [INFO] - 127.0.0.1
[APP ID/1201][NOT:0000006000]
Connecting to websocket
2019-04-14 21:14:49,321 [abstract qpylib.log] [Thread-1] [INFO] - 127.0.0.1
[APP ID/1201][NOT:000006000] Connected and about to running for ever....
2019-04-14 21:14:49,322 [abstract_qpylib.log] [WebSocketClient] [INFO] - 127.0.0.1
[APP ID/1201][NOT:000006000] Subscribe request sent to websocket for
/topic/com.cisco.ise.session
2019-04-14 21:14:49,322 [abstract qpylib.log] [WebSocketClient] [INFO] - 127.0.0.1
[APP_ID/1201][NOT:0000006000] Subscribe request sent to websocket for
/topic/com.cisco.ise.radius.failure
2019-04-14 21:14:49,323 [abstract qpylib.log] [WebSocketClient] [INFO] - 127.0.0.1
[APP ID/1201][NOT:000006000] Subscribe request sent to websocket for
/topic/com.cisco.ise.config.anc.status
2019-04-14 21:14:49,324 [abstract_qpylib.log] [WebSocketClient] [INFO] - 127.0.0.1
[APP ID/1201][NOT:000006000] Subscribe request sent to websocket for
/topic/com.cisco.ise.mdm.endpoint
```

- Note: You should see a successful connection to the primary server connection and an activation status. You should also see a subscription to the pxGrid topic over a secure Websockets connection. Please disregard the *crypto messages and the unauthorized messages.
- Step 4 If you do not see a successful connection where there is no Primary server response, or the connection keeps switching between the primary and secondary pxGrid nodes, this can be an indication that some of the services have not started or may be in an inconsistent state.

2019-04-14 20:20:57,799 [abstract_qpylib.log] [Thread-100] [INFO] - 127.0.0.1 [APP_ID/1201][NOT:000006000] Primary Server Response: None 2019-04-14 20:22:08,369 [abstract_qpylib.log] [Thread-103] [INFO] - 127.0.0.1 [APP_ID/1201][NOT:000006000] Received request to test primary files 2019-04-14 20:22:08,374 [abstract_qpylib.log] [Thread-103] [INFO] - 127.0.0.1 [APP_ID/1201][NOT:000006000] Trying http connection 2019-04-14 20:22:13,380 [abstract_qpylib.log] [Thread-103] [INFO] - 127.0.0.1 [APP_ID/1201][NOT:000006000] Wraping SSL socker

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

Step 5 Stop the pxGrid App:



POST /api/gui_app_framework/applications/{app_id}?status="STOPPED"
- Step 6 Start or restart the pxGrid app:
 - a. Start the app: POST /api/gui_app_framework/applications/{app_id}?status="RUNNING"
 - **b.** Restart the app:
 - 1. Copy the PxGrid app ID: ssh to QRadar >> /opt/qradar/support/recon ps
 - 2. In the GUI, open the QRadar Menu bar
 - 3. Click the Interactive API for Developer
 - 4. Click the drop button of the latest version >>gui_app_framework>>applications>>application_id
 - 5. Under POST, enter the application_id
 - 6. Update the status to **STOPPED**, then **RUNNING**, to stop and start the app
- Step 7 Review the QRadar app log again, or check to see if the pxGrid client appears under Web Clients on the ISE pxGrid node view
- Step 8 If you are stuck in the loading page, click **Reset** and change the date, to reflect a day before and a day after. There should be real-time authentications happening in ISE, so the session information can be seen in the IBM QRadar App.

Here are some more log issues with connectivity:

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

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

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

```
2021-02-02 17:35:00,088 [abstract_qpylib.log] [Thread-740] [INF0]
- 127.0.0.1[APP_ID/1102][NOT:000006000] Checking response got from primary server
2021-02-02 17:35:00,088 [abstract_qpylib.log] [Thread-740] [INF0]
- 127.0.0.1[APP_ID/1102][NOT:000006000] Checking status from primary server: 200
2021-02-02 17:35:00,088 [abstract_qpylib.log] [Thread-740] [INF0]
- 127.0.0.1[APP_ID/1102][NOT:000006000] Checking response from primary server:
{"accountState":"PENDING","version":"2.0.3.14"}
```

After its connected

2021-02-02 20:40:00,097 [abstract_qpylib.log] [Thread-1193] [INF0]
- 127.0.0.1[APP_ID/1102][NOT:000006000] Checking response from primary server:
{"accountState":"ENABLED","version":"2.0.3.14"}

Not able to connect to ISE node from QRadar ISE pxGrid app

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

```
2021-02-02 17:20:04,148 [abstract_qpylib.log] [Thread-707] [INFO]
- 127.0.0.1[APP ID/1102][NOT:0000006000] Client Name Jabe02022021
2021-02-02 17:20:04,148 [abstract_qpylib.log] [Thread-707] [INFO]
- 127.0.0.1[APP ID/1102][NOT:000006000] URL /pxgrid/control/ServiceLookup
2021-02-02 17:20:04,148 [abstract qpylib.log] [Thread-707] [INF0]
- 127.0.0.1[APP ID/1102][NOT:000006000] Service Name com.cisco.ise.pubsub
2021-02-02 17:20:04,191 [abstract_qpylib.log] [Thread-707] [ERROR]
- 127.0.0.1[APP_ID/1102][NOT:0000003000] Exception reported from invoke_cisco_ws_api method: <type
'exceptions.ValueError'>
2021-02-02 17:20:04,191 [abstract qpylib.log] [Thread-707] [ERROR]
- 127.0.0.1[APP ID/1102][NOT:0000003000] Exception reported from invoke cisco ws api method: No JSON
object could be decoded
2021-02-02 17:20:04,191 [abstract_qpylib.log] [Thread-707] [ERROR]
- 127.0.0.1[APP ID/1102][NOT:0000003000] Exception reported from subscribefromwebsocket method: <type
'exceptions.ValueError'>
2021-02-02 17:20:04,192 [abstract_qpylib.log] [Thread-707] [ERROR]
- 127.0.0.1[APP_ID/1102][NOT:0000003000] Exception reported from subscribefromwebsocket method: No JSON
object could be decoded
2021-02-02 17:25:00,032 [abstract qpylib.log] [Thread-718] [INF0]
- 127.0.0.1[APP ID/1102][NOT:000006000] Checking http connection with primary server
```

2021-02-02 17:25:00,036 [abstract_qpylib.log] [Thread-718] [INFO] - 127.0.0.1[APP_ID/1102][NOT:000006000] Checking connection with primary server using PROTOCOL_SSLv23

TCP Dump to Analysis Failed Certificate Exchange in ISE

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

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

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

dentity Services Engine	Home	Operations Policy Administration Work Centers
RADIUS Threat-Centric NAC Live I	Logs + TACACS - Troublesho	ot Adaptive Network Control Reports
Diagnostic Tools Download Logs		
0		
✓ General Tools	TCP Dump	
RADIUS Authentication Troublesh:	Monitor the packet headers on the	e network and save to a file (up to 5 Minutes)
Execute Network Device Comman	Status	Stopped Start
Evaluate Configuration Validator	Host Name	Cienciesaia
Posture Troubleshooting	Those Harris	LISCUSCIEW2 ·
EndPoint Debug	Network Interface	GigabitEthernet 0 •
TCP Dump		*
Session Trace Tests	Promiscuous Mode	⊛ On ⊖ Off
TrustSec Tools	Filter	S
	Example: 'ip host helios and not iceburg'	Example: 'lp host helios and not iceburg'
	Format	Raw Packet Data

- Step 3 While you keep the TCP Dump running, log in to QRadar and reconfigure the App settings page
- Step 4 Stop the dump collection and download the .pcap file
- Step 5 Analyze the .pcap file using Wireshark and observe if there are any packets being dropped, Certificate exchange failing, or Unknown CA alert

TCP Dump to Check if pxGrid Logs are Available in QRadar

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

- Step 1 Take SSH to QRadar console
- Step 2 Find the PxGrid docker IP:

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

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

Uploading Logs with the case

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

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

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