

Splunk & pxGrid Adaptive Network Control (ANC) Mitigation Workflow Actions

Table of Contents

About this Document	4
Splunk Add-on GUI Setup	5
EPS Workflow Actions	6
pxGrid ANC Workflow Mitigation Actions	7
Customizing Workflow Actions	8
ISE EPS RESTful API and pxGrid Workflow Actions	8
Customizing EPS RESTful API Workflow Actions	9
Quarantine by IP Address.....	9
Quarantine by MACAddress	10
Quarantine by Framed IP Address	11
Unquarantine by IP Address	12
Unquarantine by MAC Address	13
Customizing pxGrid ANC Workflow Mitigation Actions.....	14
ANC Quarantine by IP Address	14
ANC Quarantine by MAC Address.....	15
ANC UnQuarantine by IP Address.....	16
ANC UnQuarantine by MAC Address	17
Enabling ISE for EPS (Endpoint Protection Service)	18
Enabling the ISE Restful APIs.....	18
Create Authorization Policy for Quarantine	19
Configuring Logging Categories in ISE	20
Introduction to pxGrid client Java Keystores	21
ISE pxGrid and Splunk pxGrid client certificate generation	22
Introduction	22
ISE pxGrid persona configuration	23
pxGrid client certificate configuration	25
Configuring Splunk to Receive Syslog Events from ISE	31
Splunk pxGrid ANC Testing	32
pxGrid Operation.....	33

Troubleshooting	34
Cannot connect to ISE pxGrid node.....	34
Check keystoreFilename and password	34
Check the Splunk pxGrid log file	35
References	36

About this Document

This document is intended for Cisco engineers, partners and customers deploying Splunk-for ISE Add-on with pxGrid & Cisco Identity Service Engine (ISE) 1.3. The reader should be familiar with Splunk and ISE. It is assumed that Splunk Enterprise 6.1 or 6.2 , the Splunk-for-ISE Add-on with pxGrid and ISE has been installed.

The Splunk-for-ISE Add-on with pxGrid currently works on only Linux or MAC platforms. It does not work on Windows platforms due to limited API support for the encryption of stored pxGrid credentials.

Introduction

Splunk is a powerful tool for analyzing information in your organization by collecting, storing, alerting, reporting, and analyzing machine data. With Cisco platform Exchange Grid (pxGrid) Splunk is able to proactively act on received network security syslog events and quarantine/unquarantine an endpoint, by issuing pxGrid Adaptive Network Control (ANC) workflow actions.

The Splunk-for-ISE Add-on 2.1 or higher features an automated setup GUI for ISE EPS (Endpoint Protection Service) RESTful APIs and pxGrid ANC (Adaptive Network Control) mitigation actions via Splunk workflow actions.

The ISE EPS workflow actions work with ISE 1.2 and with ISE 1.3. The pxGrid ANC mitigation actions work with ISE 1.3.

The initial release of Splunk for ISE Add-on 2.1 for pxGrid operation requires additional Cisco files, please see your Cisco Account team.

In this document ISE will be configured for pxGrid operation in a stand-alone environment using the self-signed ISE identity certificates and creating and generating self-signed certificates for the pxGrid client, Splunk.

Please see “Deploying pxGrid in an ISE Distributed Environment” for deploying ISE in a productional environment using Certificate Authority (CA) signed certificates.

All EPS and ANC workflow actions can be customized as illustrated in this document. ISE logging categories have been enabled to trigger the syslog events sent to Splunk. These events contain the real IP or MAC addresses in the Framed_IP_Address, IPAddress, MacAddress field received by Splunk and are defined in the workflow actions.

This document includes the self-signed pxGrid client certificate generation process for Splunk. A use case is also covered whereby Splunk registers to the ISE pxGrid node as a pxGrid client and subscribes to the EndpointProtection capability topic to perform a quarantine mitigation action on the endpoint with results seen in ISE. Please note that ISE will be deployed in a Stand-alone environment.

This document also covers workflow customizations based on the enabled ISE logged categories followed by a troubleshooting and reference section.

Splunk Add-on GUI Setup

The Splunk Add-on GUI setup provides an automated way to configure the ISE EPS RESTful APIs and ISE pxGrid ANC mitigation workflow actions. You can choose to enable either one or all of the workflow actions.

EPS Workflow Actions

Step 1 Enabling ISE EPS RESTful API workflow actions
Splunk->Apps->Splunk Add-on for Cisco ISE->Setup

The “host” value for the workflow actions represents the IP address or FQDN for ISE in a stand-alone deployment.

Note: The host IP address or FQDN of ISE should be the ISE MnT node in an ISE distributed deployment.

You can enable the ISE desired ISE version for ISE 1.2 or ISE 1.3 from the drop-down menus as well as the workflow actions. These workflow actions can be customized under Settings->Fields->Workflow actions.

Configure Remediation Workflow Actions for ISE

Host for EPS_Quarantine_By_Framed_IP_Address	<input type="text" value="mwt1.lab6.com"/>
Version for EPS_Quarantine_By_Framed_IP_Address	<input type="text" value="1.3"/>
<input checked="" type="checkbox"/> Enable EPS_Quarantine_By_Framed_IP_Address	
Host for EPS_QuarantineByIPAddress	<input type="text" value="mwt1.lab6.com"/>
Version for EPS_QuarantineByIPAddress	<input type="text" value="1.3"/>
<input checked="" type="checkbox"/> Enable EPS_QuarantineByIPAddress	
Host for EPS_QuarantineByMAC	<input type="text" value="mwt1.lab6.com"/>
Version for EPS_QuarantineByMAC	<input type="text" value="1.3"/>
<input checked="" type="checkbox"/> Enable EPS_QuarantineByMAC	
Host for EPS_UnquarantineByIPAddress	<input type="text" value="mwt1.lab6.com"/>
Version for EPS_UnquarantineByIPAddress	<input type="text" value="1.3"/>
<input checked="" type="checkbox"/> Enable EPS_UnquarantineByIPAddress	
Host for EPS_UnquarantineByMAC	<input type="text" value="mwt1.lab6.com"/>
Version for EPS_UnquarantineByMAC	<input type="text" value="1.3"/>
<input checked="" type="checkbox"/> Enable EPS_UnquarantineByMAC	

pxGrid ANC Workflow Mitigation Actions

Step 1 Enabling pxGrid connections and pxGrid ANC Mitigation workflow actions
 Splunk->Apps->Splunk Add-on for Cisco ISE->Setup

Below is a summary of the connection parameters for ISE pxGrid operation:

- **Host:** defines the IP address or FQDN of the pxGrid primary node.
- **Username:** defines the pxGrid registered client name
- **Keystore File:** defines the keystoreFilename (JKS) from the identity client certificates
- **Truststore File:** defines the truststoreFilename (JKS) from the CA root certificate and/or self-signed ISE certificate
- **Password for the keystore file:** defines the password for the keystoreFilename
- **Password for the truststore file:** defined the password for the truststoreFilename
- **pxGrid Workflow Actions:** Available pxGrid mitigation actions

pxGrid Setup

Host: ← primary pxGrid node

Username: ← pxGrid client name

Keystore File (*.jks): ← keystoreFilename

Truststore File (*.jks): ← truststoreFilename

Password for keystore file: ← keystorePassword

Confirm password:

Password for truststore file: ← tuststorePassword

Confirm password:

Enable pxGrid_QuarantineByIP

Enable pxGrid_UnQuarantineByIP

Enable pxGrid_QuarantineByMAC

Enable pxGrid_UnQuarantineByMAC

← Enable pxGrid Workflow Actions

Customizing Workflow Actions

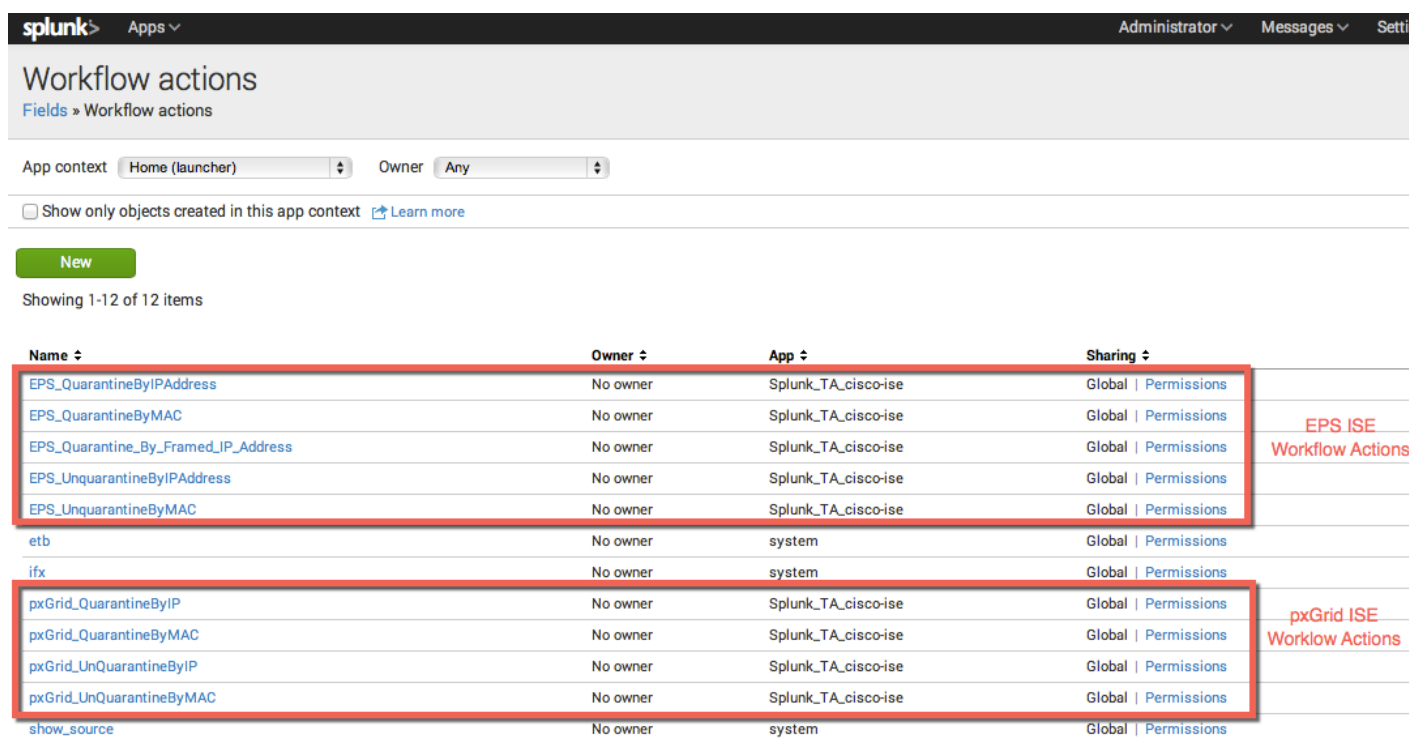
The ISE EPS RESTful workflow actions and pxGrid ANC mitigation workflow actions can be customized to use different real IP or MAC addresses based on Splunk variables or fields received by syslog events. In this document, the ISE logging categories will contain the real IP or real MAC addresses in the Framed_IP_Address, IpAddress, MacAddress fields in these syslog events send to Splunk.

Other real IP or MAC addresses can be used however, the endpoint must have an active authenticated IEEE 802.X session.

ISE EPS RESTful API and pxGrid Workflow Actions

The below screen represents both categories of workflow actions

Step 1 Viewing Splunk EPS and pxGrid Workflow Actions Settings->Field->Workflow actions



The screenshot shows the Splunk interface for viewing workflow actions. The page title is "Workflow actions" and the breadcrumb is "Fields » Workflow actions". The app context is "Home (launcher)" and the owner is "Any". There is a "New" button and a "Showing 1-12 of 12 items" indicator. The table below lists the workflow actions, with two groups highlighted by red boxes and labels on the right: "EPS ISE Workflow Actions" and "pxGrid ISE Workflow Actions".

Name	Owner	App	Sharing
EPS_QuarantineByIPAddress	No owner	Splunk_TA_cisco-ise	Global Permissions
EPS_QuarantineByMAC	No owner	Splunk_TA_cisco-ise	Global Permissions
EPS_Quarantine_By_Framed_IP_Address	No owner	Splunk_TA_cisco-ise	Global Permissions
EPS_UnquarantineByIPAddress	No owner	Splunk_TA_cisco-ise	Global Permissions
EPS_UnquarantineByMAC	No owner	Splunk_TA_cisco-ise	Global Permissions
etb	No owner	system	Global Permissions
ifx	No owner	system	Global Permissions
pxGrid_QuarantineByIP	No owner	Splunk_TA_cisco-ise	Global Permissions
pxGrid_QuarantineByMAC	No owner	Splunk_TA_cisco-ise	Global Permissions
pxGrid_UnQuarantineByIP	No owner	Splunk_TA_cisco-ise	Global Permissions
pxGrid_UnQuarantineByMAC	No owner	Splunk_TA_cisco-ise	Global Permissions
show_source	No owner	system	Global Permissions

Customizing EPS RESTful API Workflow Actions

Quarantine by IP Address

The EPS Quarantine by IP Address uses the real IP address contained in the IpAddress field or in the \$IpAddress\$ Splunk variable of the received syslog event from the following ISE enabled logging categories.

- Posture and Client Provisioning Audit
- Passed Authentications
- Failed Attempts
- Guest

Label *



Label appears in Event drop down window with real IP address

Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing the field name in dollar signs, e.g. 'Search for ticket number : Stick

Apply only to the following fields



URI link appears in events when IpAddress field is received in syslog event

Specify a comma-separated list of fields that must be present in an event for the workflow action to apply to it. When fields are specified, the workflow action or menus for those fields; otherwise it appears in all field menus.

Apply only to the following event types

Specify a comma-separated list of event types that an event must be associated with for the workflow action to apply to it.

Show action in



URI link appears in both Events and Actions Drop-down menu

Action type *

Link configuration

URI *



URI ISE EPS RESTful QuarantineByIP link to ISE MnT Node

Enter the location to link to. Optionally, specify fields by enclosing the field name in dollar signs, e.g. http://www.google.com/search?q=\$host\$.

Open link in

Link method

Quarantine by MACAddress

The EPS Quarantine by MAC Address uses the real MAC address contained in the MacAddress field or in the \$MacAddress\$ variable of the received syslog event from the following ISE enabled logging categories.

- Posture and Client Provisioning Audit
- Passed Authentications
- Administrative and Operational Audit
- Failed Attempts
- Guest
- Profiler

Label *

EPS Quarantine By MACAddress \$MacAddress\$



Label appears in Event drop down window with real MAC address

Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing the field name in dollar signs, e.g. 'Search for ticket number : \$ticket'

Apply only to the following fields

MacAddress



URI link appears in events when MacAddress field is received in syslog event

Specify a comma-separated list of fields that must be present in an event for the workflow action to apply to it. When fields are specified, the workflow action only menus for those fields; otherwise it appears in all field menus.

Apply only to the following event types

Specify a comma-separated list of event types that an event must be associated with for the workflow action to apply to it.

Show action in

Both



URI link appears in both Events and Actions Drop-down menu

Action type *

link

Link configuration

URI *

https://mnt1.lab6.com/admin/API/eps/QuarantineByMac/\$MacAddress\$



URI ISE EPS RESTful QuarantineByMac link to ISE MnT Node

Enter the location to link to. Optionally, specify fields by enclosing the field name in dollar signs, e.g. http://www.google.com/search?q=\$host\$.

Open link in

New window

Link method

get

Quarantine by Framed IP Address

The EPS Quarantine by Framed IP Address uses the real IP address contained in the Framed_IP_Address field or in the \$Framed_IP_Address\$ variable of the received syslog event from the following ISE enabled logging categories.

- Passed Authentications
- Failed Attempts
- RADIUS Accounting
- RADIUS Diagnostics
- Profiler

Label *

Label appears in Event drop down window with real IP address

Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing the field name in dollar signs, e.g. 'Search for ticket number : \$ticketnum\$'

Apply only to the following fields

URI link appears in events when Framed_IP_Address field is received in syslog event

Specify a comma-separated list of fields that must be present in an event for the workflow action to apply to it. When fields are specified, the workflow action only appears for those fields; otherwise it appears in all field menus.

Apply only to the following event types

Specify a comma-separated list of event types that an event must be associated with for the workflow action to apply to it.

Show action in

URI link appears in both Events and Actions Drop-down menu

Action type *

Link configuration

URI *

URI ISE EPS RESTful QuarantineByIP link to ISE MNT Node

Enter the location to link to. Optionally, specify fields by enclosing the field name in dollar signs, e.g. http://www.google.com/search?q=\$host\$.

Open link in

Link method

Unquarantine by IP Address

The EPS UnQuarantine by IP Address uses the real IP address contained in the IpAddress field or in the \$IpAddress\$ variable of the received syslog event from the following ISE enabled logging categories.

- Posture and Client Provisioning Audit
- Passed Authentications
- Failed Attempts
- Guest

Label *



Label appears in Event drop down window with real IP address

Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing the field name in dollar signs, e.g. 'Search for ticket number : \$ticketnum\$'.

Apply only to the following fields



URI link appears in events when IpAddress field is received in syslog event

Specify a comma-separated list of fields that must be present in an event for the workflow action to apply to it. When fields are specified, the workflow action only appears for those fields; otherwise it appears in all field menus.

Apply only to the following event types

Specify a comma-separated list of event types that an event must be associated with for the workflow action to apply to it.

Show action in



URI link appears in both Events and Actions Drop-down menu

Action type *

Link configuration

URI *



URI ISE EPS RESTful UnQuarantineByIP link to ISE Mnt Node

Enter the location to link to. Optionally, specify fields by enclosing the field name in dollar signs, e.g. [http://www.google.com/search?q=\\$host\\$](http://www.google.com/search?q=$host$).

Open link in

Link method

Unquarantine by MAC Address

The EPS UnQuarantine by MAC Address uses the real MAC address contained in the MacAddress field or in the \$MacAddress\$ variable of the received syslog event from the following ISE enabled logging categories.

- Posture and Client Provisioning Audit
- Passed Authentications
- Administrative and Operational Audit
- Failed Attempts
- Guest
- Profiler

Label *

EPS UnQuarantine By MACAddress \$MacAddress\$



Label appears in Event drop down window with real MAC address

Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing the field name in dollar signs, e.g. 'Search for ticket number : \$Ticket\$'.

Apply only to the following fields

MacAddress



URI link appears in events when MacAddress field is received in syslog event

Specify a comma-separated list of fields that must be present in an event for the workflow action to apply to it. When fields are specified, the workflow action o menus for those fields; otherwise it appears in all field menus.

Apply only to the following event types

Specify a comma-separated list of event types that an event must be associated with for the workflow action to apply to it.

Show action in

Both



URI link appears in both Events and Actions Drop-down menu

Action type *

link

Link configuration

URI *

https://mnt1.lab6.com/admin/API/eps/UnQuarantineByMac/\$MacAddress\$



URI ISE EPS RESTful UnQuarantineByMac link to ISE MnT Node

Enter the location to link to. Optionally, specify fields by enclosing the field name in dollar signs, e.g. http://www.google.com/search?q=\$host\$.

Open link in

New window

Link method

get

Customizing pxGrid ANC Workflow Mitigation Actions

ANC Quarantine by IP Address

The ANC Quarantine by IP Address calls the pxGrid script using the real IP address contained in the IpAddress field or in the \$IpAddress\$ variable of the received syslog event from the following ISE enabled logging categories.

- Posture and Client Provisioning Audit
- Passed Authentications
- Failed Attempts
- Guest

Label *

Label appears in Event drop down window with real IP address

Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing the field name in dollar signs, e.g. 'Search for ticket number : \$ticketnum\$'

Apply only to the following fields

URI link appears in events when IpAddress field is received in syslog event

Specify a comma-separated list of fields that must be present in an event for the workflow action to apply to it. When fields are specified, the workflow action only appears in menus for those fields; otherwise it appears in all field menus.

Apply only to the following event types

Specify a comma-separated list of event types that an event must be associated with for the workflow action to apply to it.

Show action in

URI link appears in both Events and Actions Drop-down menu

Action type *

Search configuration

Search string *

Calls pxGrid ANC Quarantine script using IP Address

Enter the search for this action. Optionally, specify fields as \$fieldname\$, e.g. sourcetype=rails controller=\$controller\$ error=*

Run in app

Runs pxGrid ANC Quarantine script in Splunk search window

Choose an app for the search to run in. Defaults to the current app.

ANC Quarantine by MAC Address

The ANC Quarantine by MAC Address calls the pxGrid script using the real MAC address contained in the MacAddress field or in the \$MacAddress\$ variable of the received syslog event from the following ISE enabled logging categories.

- Posture and Client Provisioning Audit
- Passed Authentications
- Administrative and Operational Audit
- Failed Attempts
- Guest
- Profiler

Label *

ANC Quarantine by mac \$MacAddress\$



Label appears in Event drop down window with real MAC address

Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing the field name in dollar signs, e.g. 'Search for ticket number : \$ticketnum

Apply only to the following fields

MacAddress



URI link appears in events when MacAddress field is received in syslog event

Specify a comma-separated list of fields that must be present in an event for the workflow action to apply to it. When fields are specified, the workflow action only appears for those fields; otherwise it appears in all field menus.

Apply only to the following event types

Specify a comma-separated list of event types that an event must be associated with for the workflow action to apply to it.

Show action in

Event menu



URI link appears in both Events and Actions Drop-down menu

Action type *

search

Search configuration

Search string *

| pxgremediate xgridAction=quarantine xgridType=mac xgridTarget="\$SM



Calls pxGrid ANC Quarantine script using MAC address

Enter the search for this action. Optionally, specify fields as \$fieldname\$, e.g. sourcetype=rails controller=\$controller\$ error=*

Run in app

search



Runs pxGrid ANC Quarantine script in Splunk search window

Choose an app for the search to run in. Defaults to the current app.

ANC UnQuarantine by IP Address

The ANC UnQuarantine by IP Address calls the pxGrid script using the real IP address contained in the IpAddress field or in the \$IpAddress\$ variable of the received syslog event from the following ISE enabled logging categories.

- Posture and Client Provisioning Audit
- Passed Authentications
- Failed Attempts
- Guest

Label *

ANC Un-Quarantine by ip \$IpAddress\$

Label appears in Event drop down window with real IP address

Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing the field name in dollar signs, e.g. 'Search for ticket number : \$ticketNumber\$'

Apply only to the following fields

IpAddress

URI link appears in events when IpAddress field is received in syslog event

Specify a comma-separated list of fields that must be present in an event for the workflow action to apply to it. When fields are specified, the workflow action only appears for those fields; otherwise it appears in all field menus.

Apply only to the following event types

Specify a comma-separated list of event types that an event must be associated with for the workflow action to apply to it.

Show action in

Event menu

URI link appears in both Events and Actions Drop-down menu

Action type *

search

Search configuration

Search string *

| pxgremediate xgridAction=unquarantine xgridType=ip xgridTarget="\$IpAddress\$"

Calls pxGrid ANC UnQuarantine script using IP address

Enter the search for this action. Optionally, specify fields as \$fieldname\$, e.g. sourcetype=rails controller=\$controller\$ error=*

Run in app

search

Runs pxGrid ANC UnQuarantine script in Splunk search window

Choose an app for the search to run in. Defaults to the current app.

ANC UnQuarantine by MAC Address

The ANC UnQuarantine by MAC Address calls the pxGrid script using the real MAC address contained in the MacAddress field or in the \$MacAddress\$ variable of the received syslog event from the following ISE enabled logging categories.

- Posture and Client Provisioning Audit
- Passed Authentications
- Administrative and Operational Audit
- Failed Attempts
- Guest
- Profiler

Label *

ANC Un-Quarantine by mac \$MacAddress\$

Label appears in Event drop down window with real MAC address

Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing the field name in dollar signs, e.g. 'Search for ticket number : \$ticket\$'

Apply only to the following fields

MacAddress

URI link appears in events when MacAddress field is received in syslog event

Specify a comma-separated list of fields that must be present in an event for the workflow action to apply to it. When fields are specified, the workflow action only menus for those fields; otherwise it appears in all field menus.

Apply only to the following event types

Specify a comma-separated list of event types that an event must be associated with for the workflow action to apply to it.

Show action in

Event menu

URI link appears in both Events and Actions Drop-down menu

Action type *

search

Search configuration

Search string *

| pxgridmediate xgridAction=unquarantine xgridType=mac xgridTarget="!

Calls pxGrid ANC UnQuarantine script using MAC address

Enter the search for this action. Optionally, specify fields as \$fieldname\$, e.g. sourcetype=rails controller=\$controller\$ error=*

Run in app

search

Runs pxGrid ANC UnQuarantine script in Splunk search window

Choose an app for the search to run in. Defaults to the current app.

Open in view

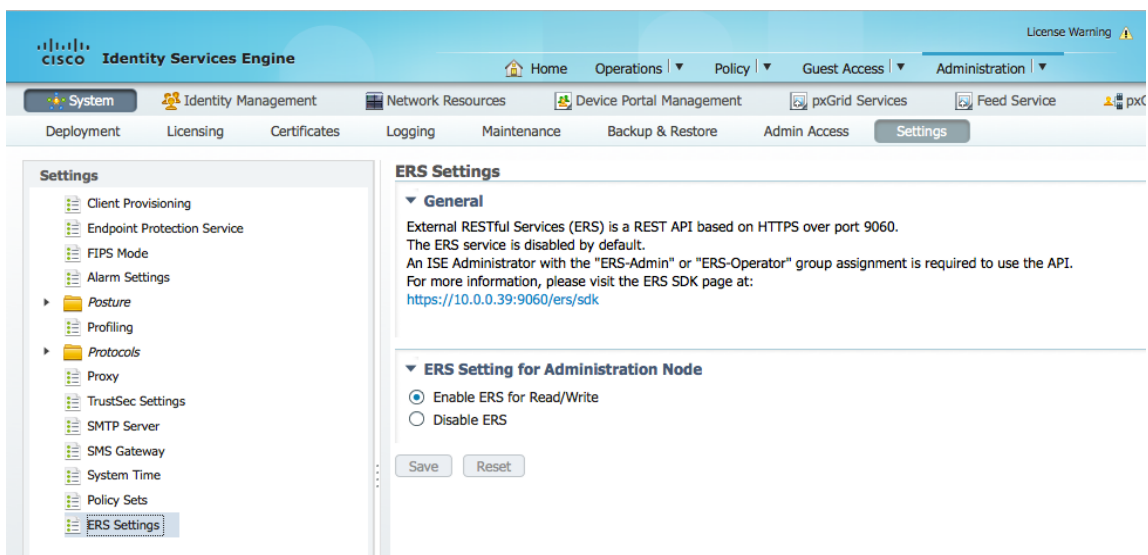
Enabling ISE for EPS (Endpoint Protection Service)

ISE will be configured to enable the RESTful APIs and Endpoint Protection Service to work. In addition an authorization profile and authorization profile for quarantining the endpoint will be created.

Enabling the ISE Restful APIs

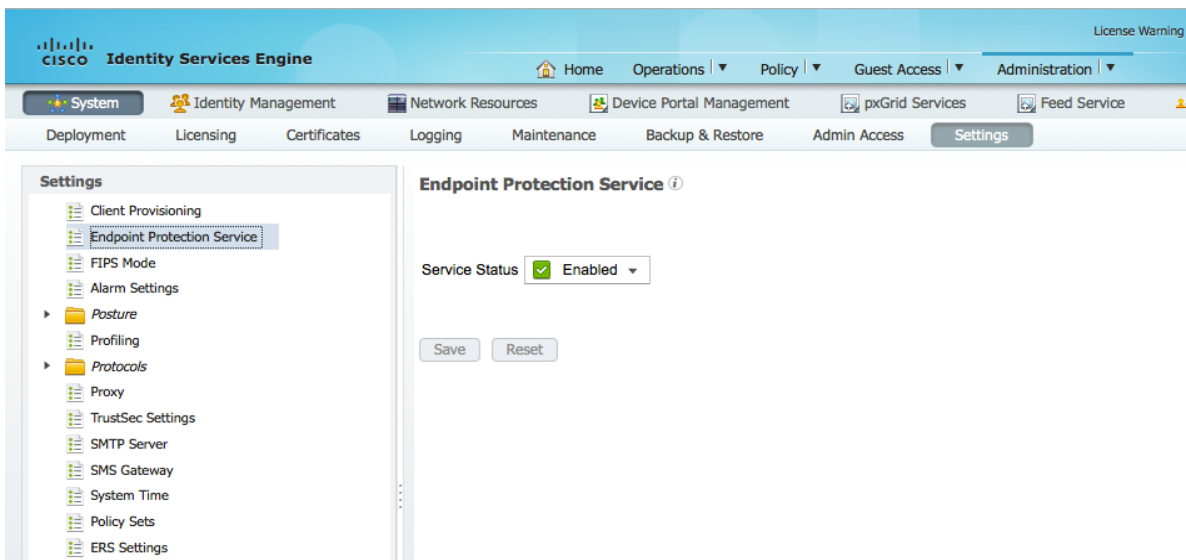
Step 1 Enable ERS Settings
Administration->System->Settings->ERS Settings then Save

Note: In a distributed ISE environment, you will also want to "enable" ERS settings for all other nodes



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The left sidebar contains a 'Settings' menu with 'ERS Settings' selected. The main content area displays the 'ERS Settings' configuration page. Under the 'General' section, there is a text block explaining that External RESTful Services (ERS) is a REST API based on HTTPS over port 9060, which is disabled by default. It also states that an ISE Administrator with the 'ERS-Admin' or 'ERS-Operator' group assignment is required to use the API. Below this, the 'ERS Setting for Administration Node' section has two radio buttons: 'Enable ERS for Read/Write' (which is selected) and 'Disable ERS'. 'Save' and 'Reset' buttons are visible at the bottom of the configuration area.

Step 2 Enable Endpoint Protection Service
Administration->System->Settings->enable Service Status then Save



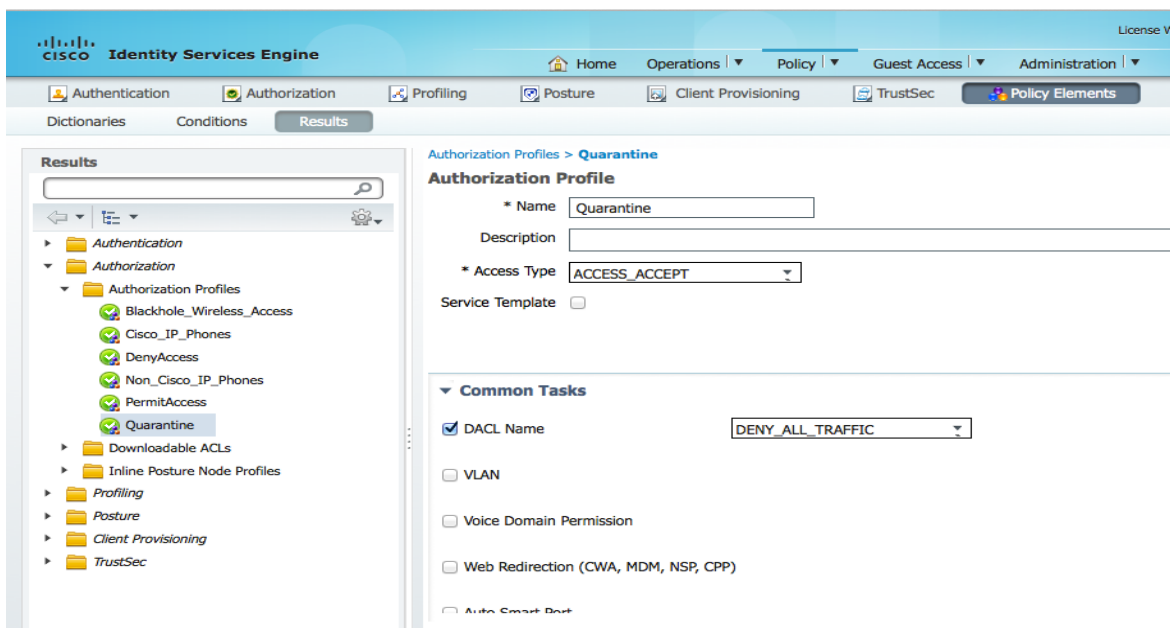
The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The left sidebar contains a 'Settings' menu with 'Endpoint Protection Service' selected. The main content area displays the 'Endpoint Protection Service' configuration page. The 'Service Status' is set to 'Enabled' with a green checkmark icon. 'Save' and 'Reset' buttons are visible at the bottom of the configuration area.

Create Authorization Policy for Quarantine

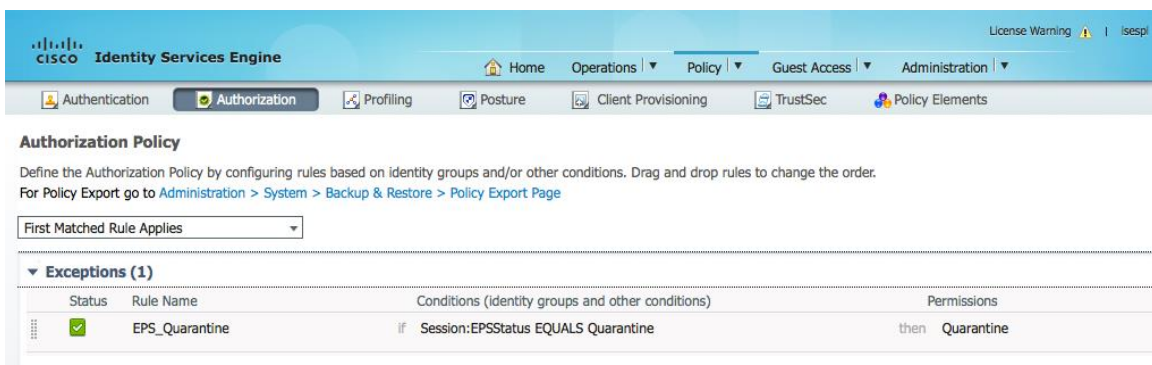
Here we create the EPS Quarantine Authorization Profile and Authorization Policy for quarantining the endpoint.

- Step 3** Create the Quarantine Authorization Profile
 Policy->Policy Elements->Results->Authorization->Authorization Profiles->Add the Quarantine profile, then Submit

Note: You can elect to DENY or ALLOW all traffic for testing. The Authorization policy profile results will still be “Quarantine” in the ISE Operation Authentication Views



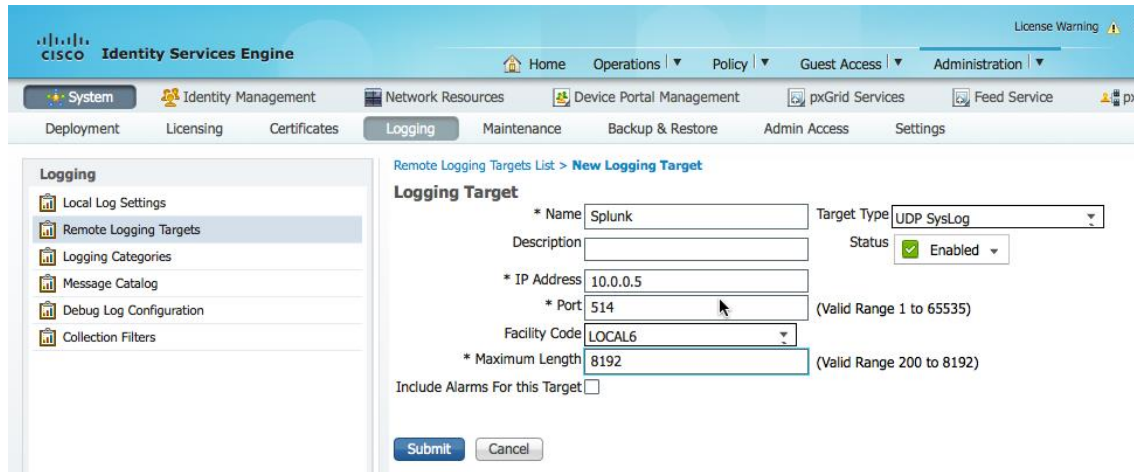
- Step 4** Create the EPS Quarantine Authorization Policy
 Policy->Authorization->Exceptions and create a new rule with the following:
- Provide the Rule Name: EPS_Quarantine
 - Create new Condition: Session:Equals:Quarantine
 - Permissions: Quarantine from Standard Profile
- Click->Done->Save



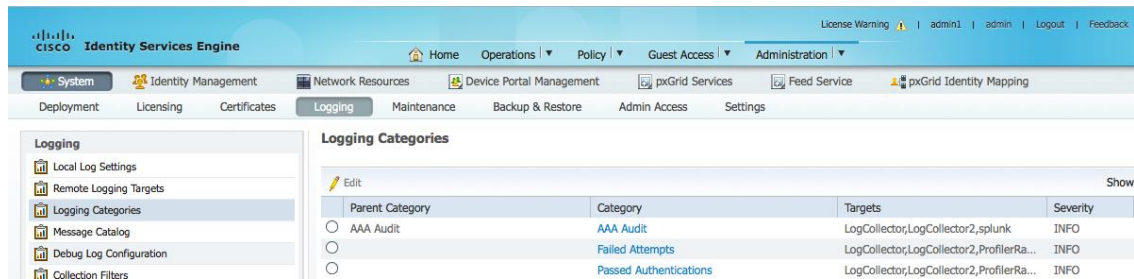
Configuring Logging Categories in ISE

Here we configure logging categories for ISE

Step 1 Administration->System->Logging->Remote Logging Targets->Add and enter the remote Splunk server settings, then Submit



Step 2 Add remote logging categories
Administration->System->Logging->Logging Categories->select the categories via edit and select Splunk as the logging target, then save



Introduction to pxGrid client Java Keystores

Java keystores contain the public/private key pairs of certificates, such as the CA root certificate, host identity or pxGrid client certificate, self-signed certificate. The java keystore itself is a PKCS #12 format (JKS).

The certificates themselves are either in a PEM or CER format, and converted over to DER and imported into the java keystore.

The keystoreFilename contains the pxGrid client identity certificate in JKS format.

The truststoreFilename can contain the CA root certificate, MnT node, self-signed ISE identity certificate in JKS format.

Note: In this example, we will only use the ISE identity certificate for the truststoreFilename

The keystorePassword contains the password of the pxGrid client identity certificate when converted to DER and imported into the keystoreFilename

The truststorePassword contains the password of the CA root certificate, MnT node certificate certificate, self-signed ISE identity certificate when converted to DER and imported into the truststoreFilename.

The keystoreFilename, keystorePassword, truststoreFilename, truststorePassword are used in the pxGrid scripts for SASL authentication and connection to the pxGrid persona.

In the case of Splunk, the pxGrid script, pxgremediate python script, is called from a pxGrid.jar file which invokes the pxGrid ANC workflow mitigation actions in the Splunk search bar.

ISE pxGrid and Splunk pxGrid client certificate generation

This illustrates the steps required to setup pxGrid with ISE 1.3 in a Proof of Concept (POC) Environment. Here we create and generate self-signed certificates for Splunk and we use the self-signed ISE Identity Certificate for pxGrid Operation. ISE is configured in a Stand-Alone environment.

Please note in a productional ISE environment, Certificate Authority (CA) signed certificates will be used to sign both the pxGrid client and ISE certificates, please see: <https://cisco.box.com/s/o6jt09pkvo9sew4novnnvbqyfvx63h9b> for more information.

Introduction

You should have openssl, or keytool on your Linux or MAC server. If ether of these are missing, consult your Linux Operating System for installation of these files.

As a requirement, please download the Oracle Java Development Kit for your Linux operating system:

<http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html>

In order to install the Oracle Java Development Kit, you must uninstall the older version of Java that exists on your system.

Note: If you are using a MAC for testing, please see: https://www.java.com/en/download/help/mac_uninstall_java.xml for uninstalling Java
If you are using Centos 6.5, please refer to the Appendices **Removing Java and Installing JDK 8.0 on Centos 6.5**

Please ensure that “keytool” is included in the path:

Note: You will have to do this for Centos 64

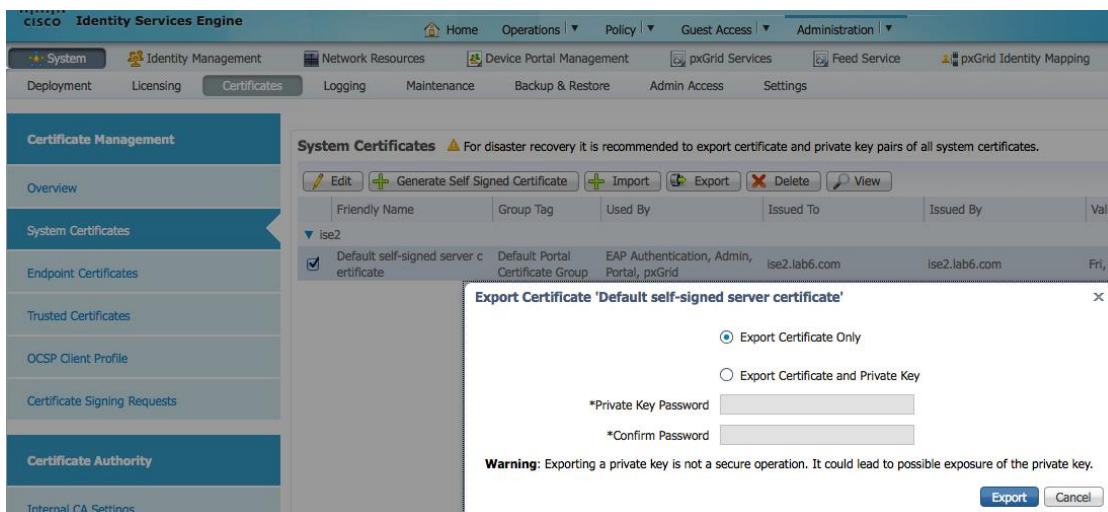
```
Append the "../jdk1.7._51/bin" to PATH
```

```
export
PATH=/usr/lib64/qt3.3/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/sbin:/usr/sbin:/sbin:/home/jeppich/bin:/usr
/java/jdk1.7.0_51/bin
```

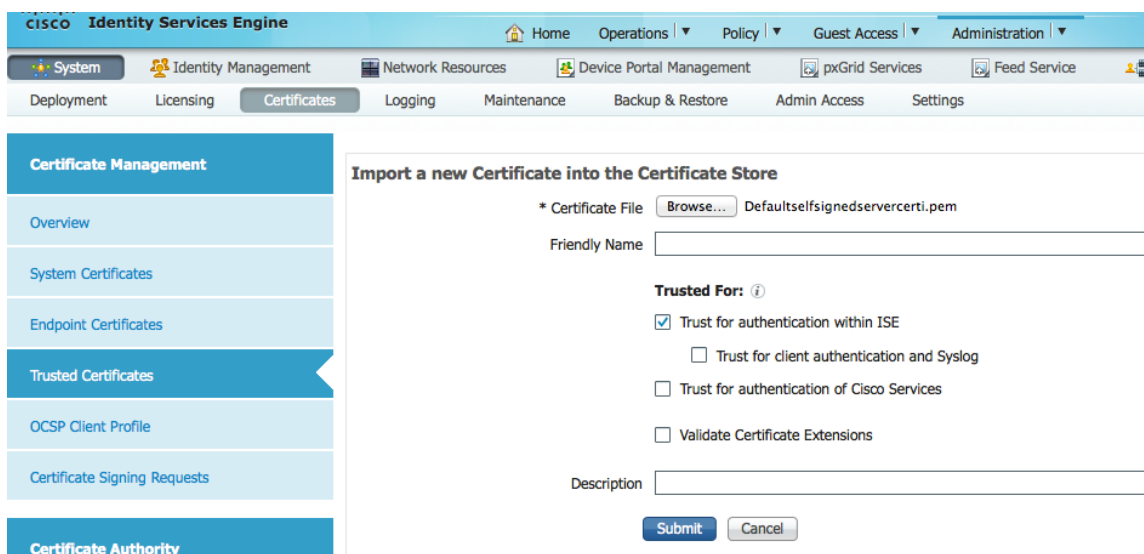
ISE pxGrid persona configuration

The Self-Signed ISE Identity certificate will be exported from the system certificate store and imported into the ISE trusted certificates store. Once the ISE Identity certificate is imported into the trusted certificate store, the pxGrid persona on the ISE node will be enabled. The pxGrid ISE node will become the primary node.

- Step 1** Export the Self Signed ISE identity certificate and save as a .pem file.
Administration->System->Certificates->select ISE identity cert->Export (public key only)



- Step 2** Import the saved ISE .pem file into the ISE trusted certificate store
Administration->System->Certificates->Trusted Certificates->Browse and upload file->Submit
Enable “trust for authentication within ISE”



You will see the imported ISE Identity certificate in the trusted certificate store

Trusted Certificates						
Edit + Import Export Delete						
<input type="checkbox"/>	Friendly Name	Status	Trusted For	Serial Number	Issued To	
<input type="checkbox"/>	Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust	
<input type="checkbox"/>	Certificate Services Endpoint Sub CA - ise2#00001	Enabled	Infrastructure Endpoints	0B A4 C8 E2 A9 A4...	Certificate Services E	
<input type="checkbox"/>	Certificate Services OCSP Responder - ise2#00003	Enabled	Infrastructure	1A E3 25 3B 98 CA...	Certificate Services C	
<input type="checkbox"/>	Certificate Services Root CA - ise2#00002	Enabled	Infrastructure Endpoints	0D 9F C1 A1 C1 9D...	Certificate Services R	
<input type="checkbox"/>	Cisco CA Manufacturing	Disabled	Endpoints Infrastructure	6A 69 67 B3 00 00 ...	Cisco Manufacturing	
<input type="checkbox"/>	Cisco Root CA 2048	Disabled	Endpoints Infrastructure	5F F8 7B 28 2B 54 ...	Cisco Root CA 2048	
<input type="checkbox"/>	ise2.lab6.com#ise2.lab6.com#00004	Enabled	Infrastructure	54 8A 31 DD 00 00...	ise2.lab6.com	
<input type="checkbox"/>	Thawte Primary Root CA	Enabled	Cisco Services	34 4E D5 57 20 D5...	thawte Primary Root	

Step 3 Enable the pxGrid persona in ISE.
Administration->System->Deployment->Enable pxGrid->Change role to Primary->Save

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is Administration > System > Deployment > Edit Node. The node name is 'ise2'. The configuration shows the following details:

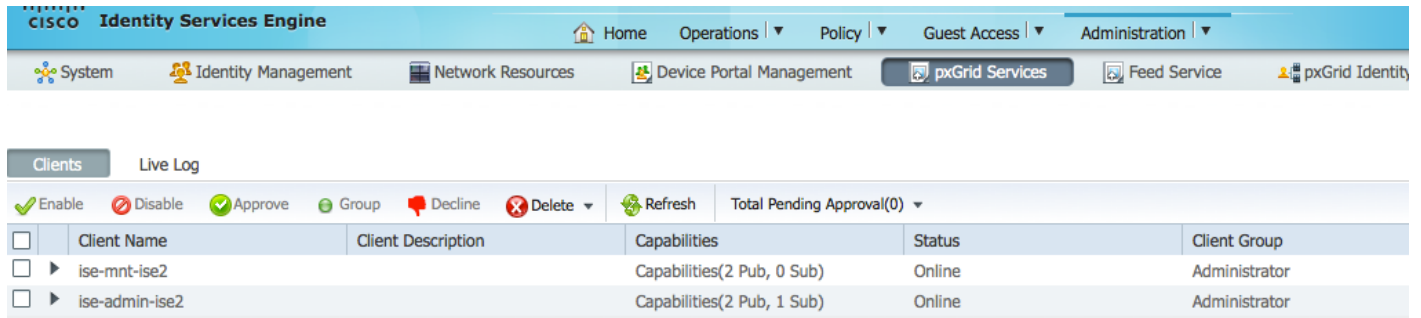
- Hostname: ise2
- FQDN: ise2.lab6.com
- IP Address: 10.0.0.94
- Node Type: Identity Services Engine (ISE)

In the 'Personas' section, the following services are enabled:

- Administration: Role PRIMARY (Make Standalone button)
- Monitoring: Role PRIMARY (Other Monitoring Node dropdown)
- Policy Service:
 - Enable Session Services: [checked] (Include Node in Node Group: None)
 - Enable Profiling Service: [checked]
- pxGrid: [checked]

Note: It is not required to change the role to primary

Step 4 Verify that the published services have started.
Administration->pxGrid Services



Client Name	Client Description	Capabilities	Status	Client Group
ise-mnt-ise2		Capabilities(2 Pub, 0 Sub)	Online	Administrator
ise-admin-ise2		Capabilities(2 Pub, 1 Sub)	Online	Administrator

Note: There may be a delay before the ISE publishing nodes appear. The certificates must be installed before the pxGrid persona is enabled.

pxGrid client certificate configuration

A self-signed certificate will be created and generated on the pxGrid client, Splunk.

The process is described below:

- A private key (i.e. mac.key) is generated for the pxGrid client
- A CSR (Certificate Signing Request) (i.e. mac.csr) is generated from the private key. A challenge key is required which will be used later on for keystore management
- The certificate (mac.cer) will be self-generated from the private key on the Linux host
- A PKCS#12 file (mac.p12) will be created from the public/private key pair and root certificate. This will be used for keystore creation of the keystoreFilename (JKS) and truststoreFilename (JKS)
- The keystoreFilename (JKS) (i.e. mac.jks) will be created
- The truststoreFilename (JKS) (i.e. caroot1.jks) will be created
- Import the self-signed ISE identity certificate from the ISE primary node (isemnt.pem)

Note: In a productional environment, this be imported from the ISE MnT node. This is also used for bulk session downloads but not in the Splunk implementation. This file was also renamed to make it easier to work with.

- Convert the ISE identity certificate PEM file (isemnt.pem) to a DER format (isemnt.der) and add to the keystoreFileName keystore (i.e. mac.jks)
- Import the pxGrid client certificate (i.e. mac.cer) into the keystoreFilename (JKS) (i.e. mac.jks)
- Import the ISE identity certificate (i.e. isemnt.der) into the truststoreFilename (JKS) (i.e. caroot1.jks)
- Copy both keystoreFilename (mac.jks) and truststoreFilename (caroot1.jks) files into the SPLUNK directory (i.e. /Applications/splunk/etc/apps/Splunk_TA_cisco-ise/bin/certs folder)

Step 1 Generate a private key (i.e. mac.key) for the pxGrid client

```
openssl genrsa -out mac.key 4096

Generating RSA private key, 4096 bit long modulus
.....++
.....++
e is 65537 (0x10001)
```

Step 2 Generate the self-signed CSR(mac.csr) request and provide a challenge password (i.e. cisco123)

Note: The challenge password will become the keystoreFilename password

```
openssl req -new -key mac.key -out mac.csr

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:cisco123
An optional company name []:
```

Note: Keep the same password throughout this document, easier to maintain, and cut down on errors

Step 3 Generate self-signed cert public-key pair certificate (i.e. mac.cer)

```
openssl req -x509 -days 365 -key mac.key -in mac.csr -out mac.cer
```

Step 4 A PKCS12 file (i.e. mac.p12) will be created from the private key.

```
openssl pkcs12 -export -out mac.p12 -inkey mac.key -in mac.cer

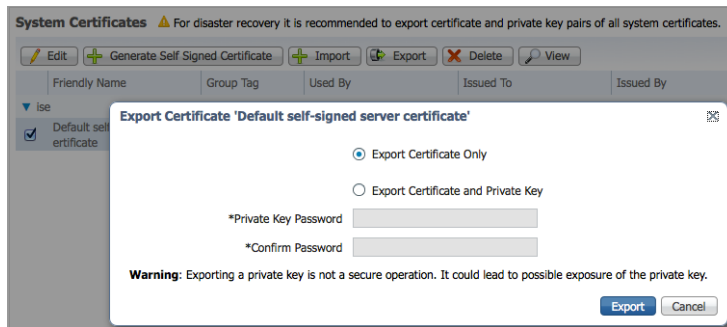
Enter Export Password: cisco123
Verifying - Enter Export Password: cisco123
```

Step 5 The mac.p12 will be imported into the identity keystore (i.e. mac.jks). This can be a random filename with a .jks extension. This will serve as the keystoreFilename and associated keystorePassword in the pxGrid scripts.

```
keytool -importkeystore -srckeystore mac.p12 -destkeystore mac.jks -srcstoretype PKCS12

Enter destination keystore password: cisco123
Re-enter new password: cisco123
Enter source keystore password: cisco123
Entry for alias 1 successfully imported.
Import command completed: 1 entries successfully imported, 0 entries failed or cancelled
```

Step 6 Export only the public ISE Identity certificate into the pxGrid client, note that this will be in .pem format. You can rename the file with .pem extension to make it easier to read, in this example the file was renamed to isemnt.pem.



Step 7 Convert the .pem file to .der format.

```
openssl x509 -outform der -in isemnt.pem -out isemnt.der
```

Step 8 Add the ISE identity cert to the keystoreFilename.

```
keytool -import -alias mnt1 -keystore mac.jks -file isemnt.der

Enter keystore password: cisco123
Owner: CN=ise.lab6.com
Issuer: CN=ise.lab6.com
Serial number: 548502f500000000ec27e53c1dd64f46
Valid from: Sun Dec 07 17:46:29 PST 2014 until: Mon Dec 07 17:46:29 PST 2015
Certificate fingerprints:
    MD5: 04:7D:67:04:EC:D2:F5:BC:DC:79:4D:0A:FF:62:09:FD
    SHA1: 5A:7B:02:E4:07:A1:D2:0B:7D:A5:AE:83:27:3B:E7:33:30:1E:32
    SHA256:
C4:21:6C:6F:5B:06:F3:2C:D7:26:35:CB:BE:2B:1B:FF:0E:EE:09:91:F6:B6:54:0C:6F:63:CB:43:1F:77:F2:37
Signature algorithm name: SHA1withRSA
Version: 3

Extensions:

#1: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
  CA:true
  PathLen:2147483647
]
```

```
#2: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
  clientAuth
]

#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Key_Encipherment
  Key_Agreement
  Key_CertSign
]

#4: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
  SSL server
]

#5: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: C4 F3 1A 9E 7B 1B 14 4F   51 9E A4 88 33 07 7A AC   .....OQ...3.z.
0010: 75 37 36 D4                               u76.
]
]

Trust this certificate? [no]: yes
Certificate was added to keystore
Johns-MacBook-Pro:bin jeppich$
```

Step 9 Import the pxGrid client certificate into the keystoreFilename.

```
keytool -import -alias pxGridclient -keystore mac.jks -file mac.cer

Enter keystore password:
Certificate already exists in keystore under alias <1>
Do you still want to add it? [no]: n
Certificate was not added to keystore
```

Note: If you receive the following message the certificate was already added to a pre-existing keystore, you can say "no" and still be okay. I selected "yes" so we can verify that the certificate was added later on.

Step 10 Import the ISE identity cert into the truststoreFilename (i.e. caroot1.jks) which serves as the truststoreFilename and truststorePassword in the pxGrid scripts.

```
keytool -import -alias root -keystore caroot1.jks -file isemnt.der
Enter keystore password: cisco123
Re-enter new password: cisco123
Owner: CN=ise.lab6.com
Issuer: CN=ise.lab6.com
Serial number: 548502f500000000ec27e53c1dd64f46
Valid from: Sun Dec 07 17:46:29 PST 2014 until: Mon Dec 07 17:46:29 PST 2015
Certificate fingerprints:
    MD5: 04:7D:67:04:EC:D2:F5:BC:DC:79:4D:0A:FF:62:09:FD
```

```
    SHA1: 5A:7B:02:E4:07:A1:D2:0B:7D:A5:AE:83:27:3B:E7:33:33:30:1E:32
    SHA256:
C4:21:6C:6F:5B:06:F3:2C:D7:26:35:CB:BE:2B:1B:FF:0E:EE:09:91:F6:B6:54:0C:6F:63:CB:43:1F:77:F2:37
    Signature algorithm name: SHA1withRSA
    Version: 3

Extensions:

#1: ObjectID: 2.5.29.19 Criticality=false
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#2: ObjectID: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
  clientAuth
]

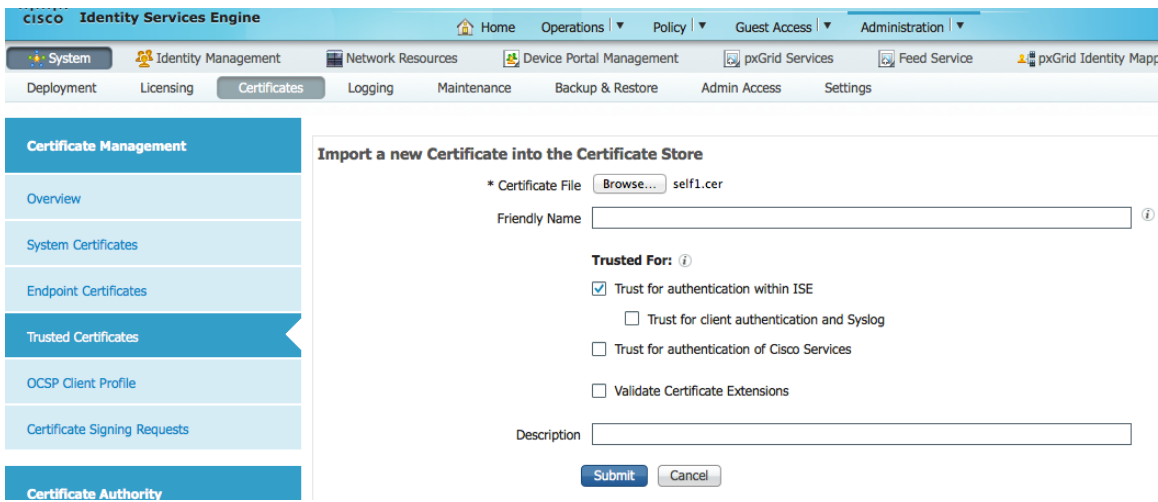
#3: ObjectID: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Key_Encipherment
  Key_Agreement
  Key_CertSign
]

#4: ObjectID: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
  SSL server
]

#5: ObjectID: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: C4 F3 1A 9E 7B 1B 14 4F   51 9E A4 88 33 07 7A AC   .....0Q...3.z.
0010: 75 37 36 D4                               u76.
]
]

Trust this certificate? [no]: yes
Certificate was added to keystore
```

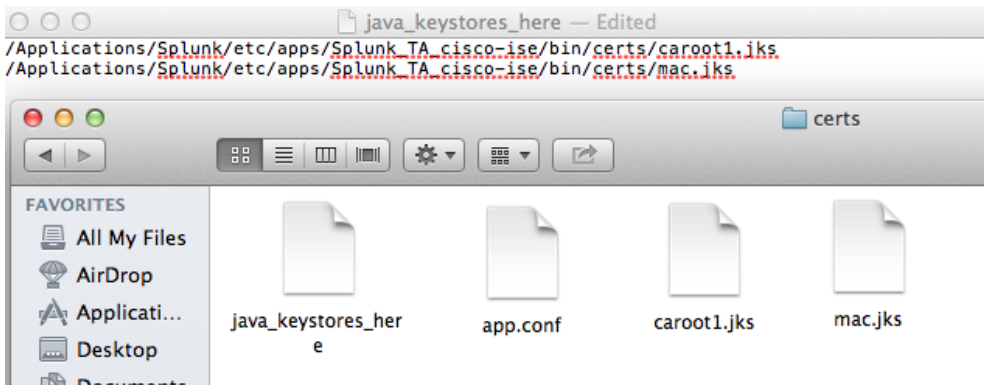
Step 11 Upload the pxGrid client public certificate (mac.cer) into the ISE trusted certificate store.
Administration->System Certificates->Trusted Certificates->Upload the mac.cer from the pxGrid client



Step 12 Copy the identity keystoreFilename (mac.jks) and truststoreFilename (caroot1.jks) into the /Applications/splunk/etc/apps/Splunk_TA_cisco-ise/bin/certs folder

Note: The path is relevant where you installed Splunk

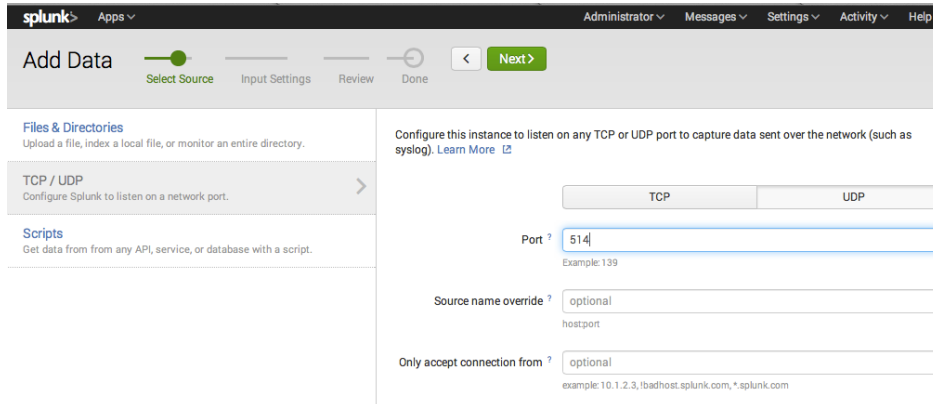
Step 13 Edit the java_keystores_here file and include the path of the truststoreFilename and keystoreFilename



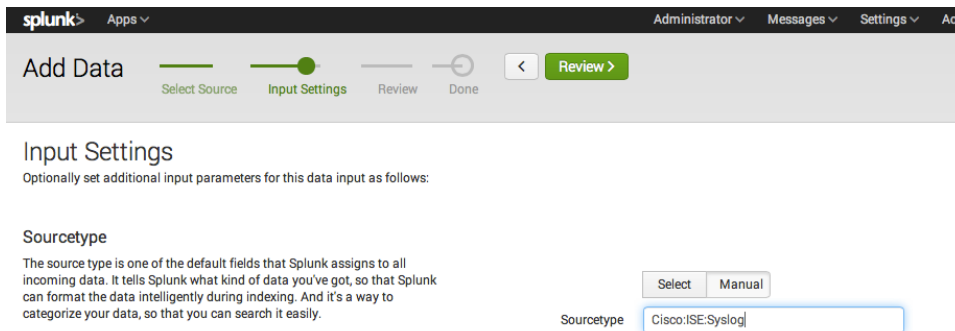
Configuring Splunk to Receive Syslog Events from ISE

The below details the initial configuration for Splunk to receive events, Splunk Enterprise 6.2 was used. If you are using Splunk Enterprise 6.1 set for manual.

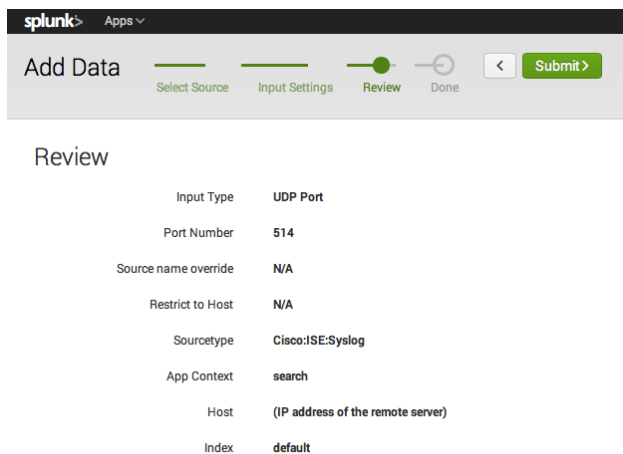
Step 1 Splunk->Settings->Data Inputs->UDP->New and select an available port, then next



Step 2 Select “Manual”, and enter :Cisco:ISE:Syslog



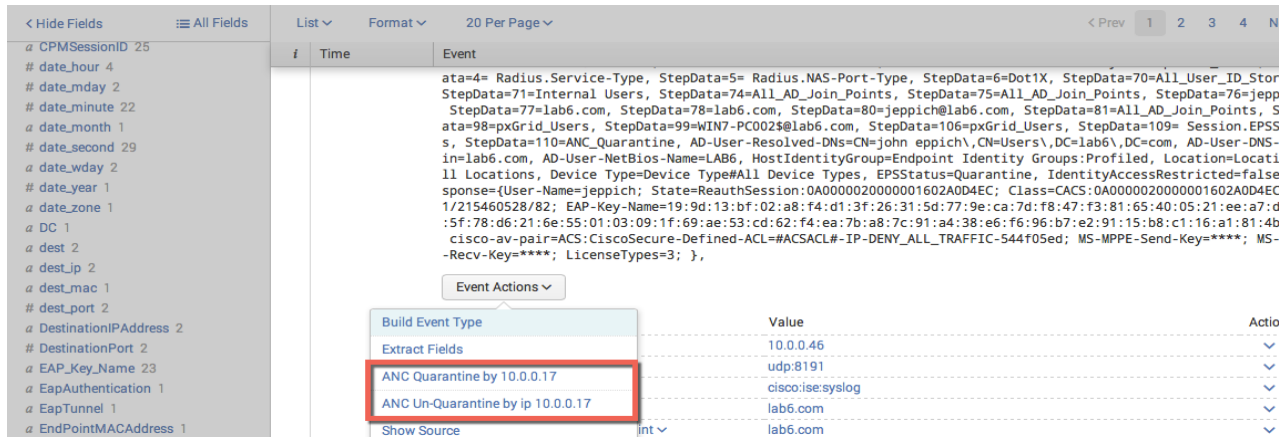
Step 3 Select ->Review->Submit->Done



Splunk pxGrid ANC Testing

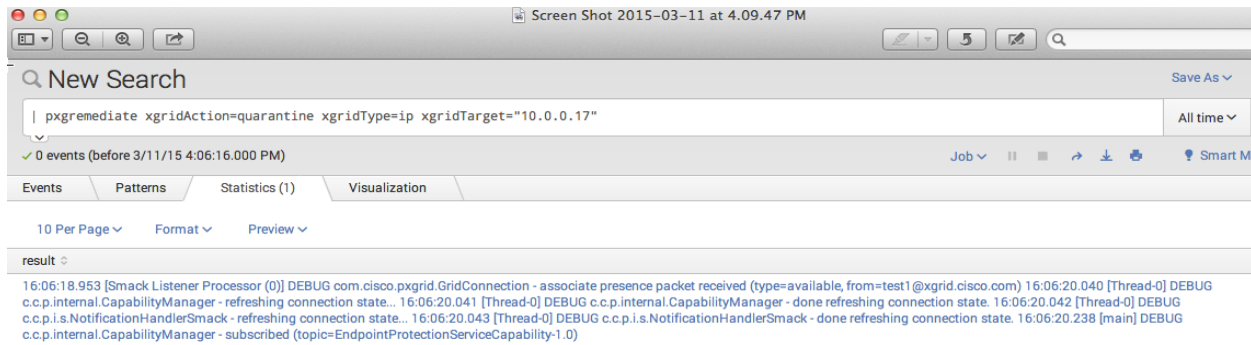
In this example, we will enable the ISE remote logging categories for Passed Authentications for ISE and send these syslog events over to Splunk. We will modify the pxGrid_Quarantine and pxGrid_UnQuarantine workflow actions to include the \$Framed_IP_Address\$ variables.

When a successful IEEE 802.1X authentication occurs, a syslog event will be triggered in Splunk. We will then Search on the event in Splunk, and issue an ANC pxgrid_Quarantine by IP from the Event drop down window.

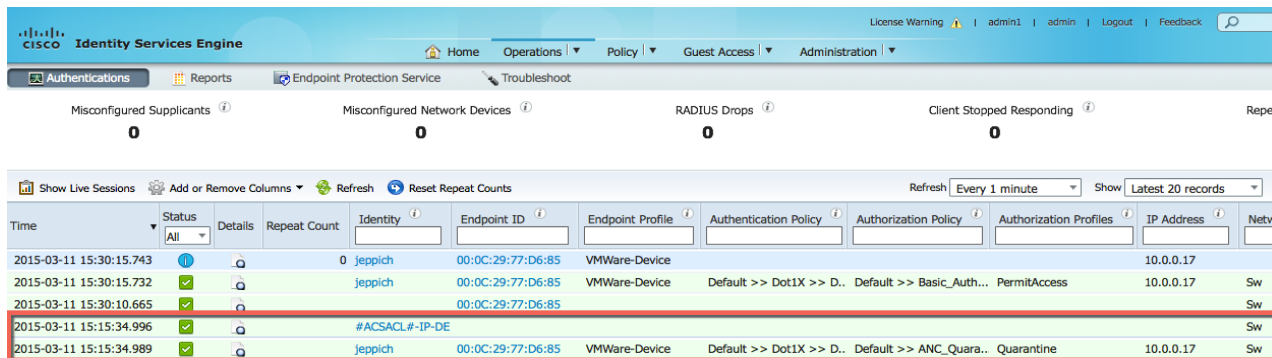


Select the “ANC Un-Quarantine by IP” workflow action

You should see following:



If you review the Operations->Events in ISE, you should see that the endpoint has been quarantined



pxGrid Operation

When the pxGrid workflow is initiated, you should see the Splunk register as the pxGrid client as indicated by the “username” in the Splunk pxGrid setup

Client Name	Client Description	Capabilities	Status	Client Group
ise-admin-admin1		Capabilities(2 Pub, 1 Sub)	Online	Administrator
ise-mnt-mnt1		Capabilities(2 Pub, 0 Sub)	Online	Administrator
ise-admin-mnt1		Capabilities(1 Pub, 0 Sub)	Online	Administrator
ironport.example.com1	pxGrid Connection from WSA	Capabilities(0 Pub, 0 Sub)	Online	Session
ironport.example.com0	pxGrid Connection from WSA	Capabilities(0 Pub, 1 Sub)	Online	Session
ironport.example.com9	pxGrid Connection from WSA	Capabilities(0 Pub, 0 Sub)	Online	Session
ironport.example.com8	pxGrid Connection from WSA	Capabilities(0 Pub, 0 Sub)	Online	Session
ironport.example.com7	pxGrid Connection from WSA	Capabilities(0 Pub, 0 Sub)	Online	Session
ironport.example.com6	pxGrid Connection from WSA	Capabilities(0 Pub, 0 Sub)	Online	Session
ironport.example.com5	pxGrid Connection from WSA	Capabilities(0 Pub, 0 Sub)	Online	Session
ironport.example.com4	pxGrid Connection from WSA	Capabilities(0 Pub, 0 Sub)	Online	Session
ironport.example.com3	pxGrid Connection from WSA	Capabilities(0 Pub, 0 Sub)	Online	Session
ironport.example.com2	pxGrid Connection from WSA	Capabilities(0 Pub, 0 Sub)	Online	Session
ironport.example.com.639505000	pxGrid Connection from WSA	Capabilities(0 Pub, 0 Sub)	Offline	Session
test1		Capabilities(0 Pub, 0 Sub)	Offline	EPS

The pxGrid client will also subscribe to the EndpointProtection Capability to invoke the mitigation quarantine mitigation action

Client Name	Capability Name	Event Type	Timestamp	Other Attributes
test1@xgrid.cisco.com		Client offline	10:07:37 PM EST, Mar 11 2015	
test1@xgrid.cisco.com	EndpointProtectionServiceCapabil...	Client unsubscribed	10:07:37 PM EST, Mar 11 2015	
test1@xgrid.cisco.com	EndpointProtectionServiceCapabil...	Client subscribed	10:07:34 PM EST, Mar 11 2015	
test1@xgrid.cisco.com		Client online	10:07:34 PM EST, Mar 11 2015	

Troubleshooting

Cannot connect to ISE pxGrid node

Ensure that the FQDN of Splunk server is DNS resolvable with ISE

Check keystoreFilename and password

- Ensure that you have the proper path for the keystoreFilename and truststoreFilename
- Run the Splunk search string on the Linux command line to help diagnose the issue

If you see the following:

```
java -jar /Applications/Splunk/etc/apps/Splunk_TA_cisco-ise/bin/lib/pxGrid_Search.jar pxGrid1.lab6.com test1
/Applications/Splunk/etc/apps/Splunk_TA_cisco-ise/bin/certs/mac.jks cisco123
/Applications/Splunk/etc/apps/Splunk_TA_cisco-ise/bin/certs/caroot1.jks cisco123 10.0.0.17 quarantine_ip
17:46:53.596 [Smack Listener Processor (0)] DEBUG com.cisco.pxgrid.GridConnection - associate presence packet
received (type=available, from=test1@xgrid.cisco.com)
17:46:55.266 [Thread-0] DEBUG c.c.p.internal.CapabilityManager - refreshing connection state...
17:46:55.273 [Thread-0] DEBUG c.c.p.internal.CapabilityManager - done refreshing connection state.
17:46:55.290 [Thread-0] DEBUG c.c.p.i.s.NotificationHandlerSmack - refreshing connection state...
17:46:55.291 [Thread-0] DEBUG c.c.p.i.s.NotificationHandlerSmack - done refreshing connection state.
17:46:55.502 [main] DEBUG c.c.p.internal.CapabilityManager - subscribed
(topic=EndpointProtectionServiceCapability-1.0)
```

This means that the pxGrid Quarantine action was successful

Check the Splunk pxGrid log file

The log file can be found at “/Applications/splunk/var/log/splunk/pxgridremediate.log” or wherever path you have Splunk installed.

Details below indicate that the endpoint was successfully unquarantined via Splunk pxGrid_unQuarantine_by_IP workflow action

```
2015-03-11 23:20:51,662 [016929] INFO      root:  Logger Initialized
2015-03-11 23:20:52,084 [016929] INFO      root:
item=pxGrid1.lab6.com|test1|/Applications/Splunk/etc/apps/Splunk_TA_cisco-
ise/bin/certs/mac.jks|/Applications/Splunk/etc/apps/Splunk_TA_cisco-ise/bin/certs/caroot1.jks|
2015-03-11 23:20:52,084 [016929] INFO      root:  xgridHostname=pxGrid1.lab6.com
2015-03-11 23:20:52,084 [016929] INFO      root:  xgridUsername=test1
2015-03-11 23:20:52,084 [016929] INFO      root:
keystoreFilename=/Applications/Splunk/etc/apps/Splunk_TA_cisco-ise/bin/certs/mac.jks
2015-03-11 23:20:52,084 [016929] INFO      root:
truststoreFilename=/Applications/Splunk/etc/apps/Splunk_TA_cisco-ise/bin/certs/caroot1.jks
2015-03-11 23:20:52,411 [016929] INFO      root:  keystorePassword=<password />
2015-03-11 23:20:52,411 [016929] INFO      root:  truststorePassword=<password />
2015-03-11 23:20:52,411 [016929] INFO      root:  xgridAction=unquarantine
2015-03-11 23:20:52,411 [016929] INFO      root:  xgridType=ip
2015-03-11 23:20:52,411 [016929] INFO      root:  xgridTarget=10.0.0.17
2015-03-11 23:20:52,411 [016929] INFO      root:  LAUNCHING: java -jar
/Applications/Splunk/etc/apps/Splunk_TA_cisco-ise/bin/lib/pxGrid_Search.jar pxGrid1.lab6.com test1
/Applications/Splunk/etc/apps/Splunk_TA_cisco-ise/bin/certs/mac.jks cisco123
/Applications/Splunk/etc/apps/Splunk_TA_cisco-ise/bin/certs/caroot1.jks cisco123 10.0.0.17 unquarantine_ip
2015-03-11 23:21:08,792 [016929] INFO      root:  result from java cmd: 23:20:53.968 [Smack Listener Processor
(0)] DEBUG com.cisco.pxgrid.GridConnection - associate presence packet received (type=available,
from=test1@xgrid.cisco.com)
23:21:00.132 [Thread-0] DEBUG c.c.p.internal.CapabilityManager - refreshing connection state...
23:21:00.133 [Thread-0] DEBUG c.c.p.internal.CapabilityManager - done refreshing connection state.
23:21:00.134 [Thread-0] DEBUG c.c.p.i.s.NotificationHandlerSmack - refreshing connection state...
23:21:00.135 [Thread-0] DEBUG c.c.p.i.s.NotificationHandlerSmack - done refreshing connection state.
23:21:00.390 [main] DEBUG c.c.p.internal.CapabilityManager - subscribed
(topic=EndpointProtectionServiceCapability-1.0)
```

References

For more detailed information regarding pxGrid, please see:

http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-84-Configure_and_Test_Integration_with_Cisco_pxGrid.pdf

For Cisco ISE pxGrid deployment guide, please see:

<https://cisco.box.com/s/o6jt09pkvo9sew4novnnvbqyfvx63h9b>

Splunk reference for ISE EPS RESTful workflow actions:

http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-85-Integrating_and_Monitoring_Cisco_ISE_User-Device_Context_in_Splunk.pdf