Cisco FireSIGHT and ISE Rapid Threat Containment Solution
# Table of Contents

About this Document .................................................................................................................. 4  
Technical Overview .................................................................................................................. 5  
FireSIGHT Realm Configuration ................................................................................................. 8  
  Configure LDAP Connection .................................................................................................... 8  
  Sample User LDAP Information .............................................................................................. 10  
Configuring ISE for Self-Signed Certificates in a Stand-Alone Environment using pxGrid ......................................................... 11  
  Export the ISE identity-self-signed certificate into the ISE trusted certificate store .............. 11  
Configuring FireSIGHT Management Center for Self-Signed Certificates ................................. 13  
  Configuring pxGrid agent using self-signed certs ................................................................. 18  
Customized pxGrid template for CA-signed operation ................................................................ 21  
Configuring ISE for CA-Signed Certificates in a Stand-Alone Environment using pxGrid .......................... 24  
Configuring FireSIGHT Management Center for CA-Signed Certificates ............................... 27  
  Configuring pxGrid agent using CA-signed certs ............................................................... 28  
FireSIGHT pxGrid remediation module ...................................................................................... 31  
  Uploading FireSIGHT pxGrid remediation module .............................................................. 31  
  Create new instance ............................................................................................................. 31  
  Create FireSIGHT pxGrid mitigation types ......................................................................... 32  
    Quarantine ......................................................................................................................... 32  
    portBounce ....................................................................................................................... 32  
    reAuthenticate .................................................................................................................. 33  
    shutDown ........................................................................................................................ 33  
    terminate .......................................................................................................................... 34  
    unQuarantine ................................................................................................................... 34  
FireSIGHT pxGrid Intrusion Policy ............................................................................................ 36  
FireSIGHT Connection Rule ....................................................................................................... 40  
Configuring ISE EPS Service and Quarantine Authorization Policies ........................................... 43  
FireSIGHT Management Center Correlation Policies ................................................................ 45  
  Quarantine .......................................................................................................................... 45  
  Testing .................................................................................................................................. 47  
  portBounce .......................................................................................................................... 49  
    Testing ............................................................................................................................... 51  
    portShutdown .................................................................................................................... 54  
    Testing ............................................................................................................................... 56
reAuthenticate..................................................................................................................58
Testing..........................................................................................................................60
Terminate.......................................................................................................................63
Testing..........................................................................................................................63

Unquarantine Correlation Policy ..................................................................................67
Testing..........................................................................................................................69

Troubleshooting..............................................................................................................72
ISE pxGrid Services do not come up ............................................................................72
pxGrid agent certificate error messages .......................................................................72
FireSiGHT Management Center not communicating with ISE ....................................72
No correlation events appear in the FireSiGHT Management Center .......................72
FireSiGHT failed mitigation attempts .........................................................................72
Mitigation "lookup failure" attempts .............................................................................72
pxGrid connection failure attempts syslog error messages from FireSiGHT Management Console........73
Verifying self-signed certs by importing into ISE system store ....................................74

Solution Caveats.............................................................................................................76
pxGrid & Identity mapping service restart .....................................................................76
Active pxGrid node is not reflected in the GUI; It is reflected in CLI .............................76

References 77
About this Document

This document is intended for Cisco engineers and customers who are interested in deploying FireSIGHT Management Center (5.4) with Cisco Identity Service Engine (ISE 1.3 or higher) using (platform exchange Grid) pxGrid’s Adaptive Network Control (ANC) mitigation actions to take action on the endpoint. Please note that this is for FireSIGHT Management Center 5.4 only and not for FireSIGHT Management Center 6.0.

This document provides details on the configuration of FireSIGHT Management Center using ISE in a stand-alone environment using self-signed certificates and also using Certificate Authority (CA)-signed certificates with pxGrid enabled. The pxGrid remediation module, pxGrid agent installation and configuration details are covered. The pxGrid remediation module provides the pxGrid ANC mitigation features: quarantine, portbounce, portshut, reauthenticate, terminate and unquarantine. The pxGrid agent provides the certificate information and ISE pxGrid node connection information between the FireSIGHT Management Center and the ISE pxGrid node. Correlation policies, rules, remediation types are defined for each ANC mitigation action type.

The reader should have some familiarity with the FireSIGHT Management Center and the Identity Service Engine (ISE) access control system. It is assumed that FireSIGHT Management Center 5.4 and a standalone ISE 1.3 or ISE 1.4 environment is installed. FireSIGHT Management Center 5.4 was also tested on ISE 2.0.

The following software versions were used for the testing of this document:

- FireSIGHT Management Center 5.4
- FireSIGHT Appliance Virtual Sensor 5.4
- Cisco Identity Services Engine ISE 1.3 and ISE 1.4
- FireSIGHT pxGrid remediation module 1.0
- FireSIGHT pxGrid Agent 1.0
- Microsoft CA 2008 R2 Enterprise

For configuring ISE pxGrid in a Distributed ISE environment, please see the link in the References section. Also included are links to How-To Deployment guides using CA-signed certificates and self-signed certificates using a MAC as a pxGrid client as reference.
Technical Overview

Cisco’s Platform Exchange Grid (pxGrid) enables multivendor, cross platform network system collaboration among the IT infrastructure. It allows such as security monitoring and detection system, network policy platforms, asset and configuration management, identity and access management platforms, and virtually any other IT operations platform. pxGrid uses the Identity Service Engine (ISE) policy server to provide Authentication, Authorization and Access control (AAA).

The pxGrid framework consists of the following:

pxGrid Publisher - publishes topics of interest or capabilities
pxGrid Controller - manages all pxGrid client authentications, authorizations, capabilities and subscription list
pxGrid Subscriber (also called a pxGrid client) - subscribes to the published pxGrid topics.

The FireSIGHT ISE Remediation Module is a pxGrid client and provides mitigation actions via the ISE publish/subscribe method.

ISE publishes Session Directory and Endpoint Protection Services. The Session Directory exposes the existing attributes in the ISE Session directory for pxGrid session objects. These include:

- Session State
- IP Address
- Username
- User AD domain
- MAC
- NAS IP Address
- TrustSec Security Group Name
- Endpoint Profile Name
- Profiling policy name
- Posture Status
- Audit Session ID
- Acct Session IP (In the RADIUS AV Pair, Last Update Time)
The Endpoint Protection Service exposes the following pxGrid ANC mitigation objects:

- Quarantine
- Unquarantine
- Terminate
- Port Bounce
- Shutdown

The FireSIGHT agent registers to the ISE pxGrid node as a pxGrid client and subscribes to the EndpointProtection Service topic and EPS session group for performing the pxGrid ANC mitigation actions.

The actual FireSIGHT pxGrid integration occurs by uploading the pxGrid agent and pxGrid remediation module to FireSIGHT management center.

The pxGrid agent installation serves three functions:

Installation of pxGrid services and supporting libraries

- pxGrid connection parameter configuration - such as pxGrid node IP address, host/identity certificate, host private key certificate and the trusted CA root
- Starts the pxGrid services and handles the mitigation action requests from pxGrid remediation module and sends the information over to the ISE pxGrid node.
- The pxGrid remediation module hands off all pxGrid interactions to the pxGrid service and receives notification results from the ISE pxGrid node.

The FireSIGHT pxGrid remediation module sends the pxGrid ANC mitigation action requests to the FireSIGHT pxGrid service which processes these requests based on the pxGrid GCL libraries and then sends this information over to the ISE pxGrid node. A Microsoft AD realm will be configured with Network discovery turned on for hosts and users in order for the FireSIGHT Management center to obtain user logon/logoff information and operating system details of the endpoint.
Cisco Sourcefire and pxGrid Integration

Remediation Module

pxGrid Node

Connection parameters for CA-signed FireSIGHT cert
- IP Address ISE pxGrid node
- Identity (Host certificate)
- CA Root Certificate
- Private key password

External Authentication Complete
Register SourcefireAgent & subscribe to EndpointProtectionService
Authenticated SASL successfully
Successfully Subscribed
Processes request GLC libraries, and sends information

Mitigation successful

Send Mitigation Action Request
Mitigation action=quarantine, IP=10.0.0.18
FireSIGHT Realm Configuration

An authentication server is defined that provides LDAP user information. In addition, user awareness is enabled and network discovery turned on to provide user logon/logoff details and host information and operating system details.

Configure LDAP Connection

Step 1  Policies->Users->Add LDAP Connection, enter the following:

Step 2  Enable->User/Group Access Control Parameters->Fetch Groups

Note: Include all groups for User Awareness

Step 3  Test and Save
**Step 4**  
Activate LDAP connection, **Click->button** below  

![Image of the LDAP connection page](image1)  

**Step 5**  
You should see this:  

![Image of the successful LDAP connection](image2)  

**Step 6**  
Enable Network Discovery for hosts, users and applications  
**Policies->Network Discovery->** and **Click->Pencil->select Hosts, Users and Applications->Save**  

![Image of the Network Discovery page](image3)
Sample User LDAP Information

The User Activity screen displays the end-user information

In addition, if you click on the PC icon below, you will receive the “host profile” for the IP address below

This host profile contains user history information, host protocol can vulnerability information.
Configuring ISE for Self-Signed Certificates in a Stand-Alone Environment using pxGrid

This section steps through the process of configuring ISE using self-signed certificates in a stand-alone environment using pxGrid.

Export the ISE identity-self-signed certificate into the ISE trusted certificate store

This is required for ISE to trust the self-signed certificate.

**Note:** Please note that this is not required in ISE 2.0. By default, when pxGrid is enabled in ISE, the published nodes will appear and connectivity to the ISE pxGrid node will be established. This ISE identity self-signed certificate is trusted.

**Step 1** Select->Administration->System->Certificates->System Certificates->select ISE self-signed identity certificate

**Step 2** Export the certificate only, Click->Export

**Step 3** Import the ISE identity self-signed certificate into the ISE trusted store
Select->Administration->System->Certificates->Trusted Certificates->Import ->the ISE identity self-signed certificate (PEM)->Enable Trust for authentication within ISE->Submit
Step 4  Enable pxGrid on the ISE node
Administration->System->Deployment->select node->Enable pxGrid, and then Save

Note: This may take a couple of seconds before you see connected
Configuring FireSIGHT Management Center for Self-Signed Certificates

In this section, the FireSIGHT Management Center (FMC) is configured for using self-signed certificates for ISE pxGrid node operation. An internal FMC certificate authority is created on the FireSIGHT Management Center and the public/private key pair exported and imported into the ISE certificate system store. The internal FMC public certificate will be exported into the ISE certificate trusted system store. The ISE identity self-signed public certificate will be imported into the FireSIGHT Management Center Trusted CA store.

Step 1 Select->Objects > Object Management > PKI -> Internal CAs ->Generate CA-> provide the certification information below:
In this example, FMC2, was the name given to the internal CA

Step 2 Click->Generate self-signed CA
Step 3 Download the CA certificate file, Click->Pencil below:
Step 4  Select Download

Step 5  Enter encryption password, then click OK. In this example, cisco123 was used.

Step 6  Save the .p12 file locally.

Step 7  Rename the .p12 filename to make it easier to work with. In this example, fmc2.p12 was the renamed file.
Step 8  Use WinSCP or another method to upload the file to the FireSIGHT Management Console

<table>
<thead>
<tr>
<th>Name</th>
<th>Ext</th>
<th>Size</th>
<th>Type</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sourcefire_3D_Device_VirtualBox_Vmware_0</td>
<td></td>
<td>542 MB</td>
<td>GZ File</td>
<td>9/7/2015</td>
</tr>
<tr>
<td>Sourcefire_Defense_Center_VirtualBox_Vmware_0</td>
<td></td>
<td>677 MB</td>
<td>GZ File</td>
<td>9/7/2015</td>
</tr>
<tr>
<td>Sourcefire_Defense_Center_VirtualBox_Vmware_0</td>
<td></td>
<td>1,044 B</td>
<td>LE File</td>
<td>9/7/2015</td>
</tr>
<tr>
<td>Sourcefire_Defense_Center_VirtualBox_Vmware_0</td>
<td></td>
<td>1,049 B</td>
<td>LE File</td>
<td>9/7/2015</td>
</tr>
</tbody>
</table>

Step 9  SSH to the FireSIGHT Management Console

Step 10  Convert the .p12 file into CER and KEY files, by typing the following commands:

Note: the CER and KEY filenames are random. The original.p12 file was renamed to fmc2.p12

```
sudo openssl pkcs12 -nokeys -clcerts -in fmc2.p12 -out fmc2.cer
```

Enter Import Password:
MAC verified OK
admin@sd:~$

```
sudo openssl pkcs12 -nocerts -in fmc2.p12 -out fmc2.key
```

Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
admin@sd:~$

Step 11  WinSCP was used to copy the fmc2.cer and fmc2.key files from the FireSIGHT Management Center to the local PC.

```
sudo openssl pkcs12 -nocerts -in fmc2.p12 -out fmc2.key
```

Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
admin@sd:~$

Step 12  The FireSIGHT Management internal CA public certificate was exported into the ISE certificate trust store
Administration->System->Certificates->Trusted Certificates->Browse and upload fmc2.cer

Step 13  Enable “Trust for authentication within ISE”->Submit

Step 14  Export both the ISE identity self-signed public certificate and private key from the ISE Trusted Certificates store. You will only need to export the ISE identity self-signed public certificate into the FireSIGHT Management trusted CA store. The FireSIGHT Management Console recognizes this as being a trusted certificate.

Administration->System-Certificates->Certificate Management->Trusted Certificates->select ISE certificate ->Export both the public and private key, provide a password

Note: This procedure is still the same for ISE 2.0

Step 15  Import the ISE self-signed identity cert into the FireSIGHT Management trusted CA store

Objects->Object Management->PKI->Trusted CAs->Add Trusted CA->enter the name->Save.
Step 16  Import the FireSIGHT Management internal CA public/private key pair into the FireSIGHT Management Center’s Internal Certs store
Select->Objects->Object Management->PKI->Internal Certs->Add Internal Cert
Follow the same procedure for the private key

Note: Delete Bag Attributes until you get to "---Begin Certificates"

Step 17  Delete the Bag attributes for the key file until you are just before “---Begin….”

Step 18  Also delete </no> and enter the encrypted password

Step 19  You should see the following, click OK to complete
Configuring pxGrid agent using self-signed certs

The pxGrid agent is responsible for the certificate configuration and communication between the FireSIGHT Management center and the ISE pxGrid node. The IP address of the ISE pxGrid node will be required. The FireSIGHT Management Center’s public certificate and key files will be required for the next steps.

The FireSIGHT Management Center’s public certificate will serve as the host certificate. The ISE identity self-signed certificate will serve as the CA certificate.

The FireSIGHT Management Center’s private key file will be the host key. The password of the key will also be required.

**Step 1** Upload the pxGrid agent to the FireSIGHT Management Console using WinSCP or another SCP/SFTP client of your choosing.

**Step 2** Upload the FireSIGHT internal CA public cert, the internal CA key to FireSIGHT MC /Volume/home/admin, using WinSCP or other method

**Note:** Upper/lowercase syntax is maintained

**Step 3** SSH into the FireSIGHT Management Center and type:

```
sudo bash sfdc-pxgrid_agent_v1.0.35.sh
```
Please see below for a sample script:

Verifying archive integrity... All good.
Uncompressing Cisco pxGrid Agent Installer......
Installing the agent....
Installing the pxGrid libraries and Perl module...
Setting up the agent to be managed by PM...
Installation done!

Configuring pxGrid...

Below you will be asked a series of questions relating to your pxGrid install and the files supporting it. Health alerts WILL be generated by PM until the configuration is completed, however. The answers to these questions will populate the /etc/sf/pxgrid/pxgrid.conf configuration file, which can be manually modified later at any time. A configuration example is provided in the same directory with the filename pxgrid.conf.example.

To get this all to work, the agent will need to connect to a pxGrid server. This is typically your Cisco Identity Services Engine instance, which must also have the pxGrid service enabled.

What is the IP address of your pxGrid server
> 192.168.1.71

Every agent connecting to pxGrid must have a unique host certificate which will be used to identify the agent host. Associated key and CA certs must also be provided.

What is the full path and filename to the host certificate?
> /Volume/home/admin/fmc2.cer
What is the full path and filename to the host key?
> /Volume/home/admin/fmc2.key
What is the host key password?
> cisco123
What is the full path and filename to the CA certificate?
> /Volume/home/admin/ise14lab.pem

Configuration written to /etc/sf/pxgrid/pxgrid.conf
Step 4  Select->System->Monitoring->Syslog to see that FireSIGHT Management Center has successfully registered as a client to the ISE pxGrid node and subscribed to the EPS topic

Step 5  To view in ISE, select->Administration->pxGrid Services. Note the FireSIGHT Management Console has registered to the ISE pxGrid node EndpointProtectionService Capability
Customized pxGrid template for CA-signed operation

A customized pxGrid template having an Enhanced Key Usage (EKA) of both client authentication and server authentication is required for pxGrid operation between the pxGrid client, the FireSIGHT Management Center and the ISE pxGrid node. This is required for a Certificate Authority (CA)-signed environment where both the FireSIGHT Management Center and the ISE pxGrid node are signed by the same CA.

Step 1  Select->Administrative Tools->Certificate Authority->“+” dropdown next to CA server->Right->Click on Certificate Templates->Manage

Step 2  Right-Click and Duplicate User template->Select->Windows 2003 Enterprise->OK

Step 3  Enter name of certificate template, uncheck “Publish certificate in Active Directory”, and provide validity period and renewal period.
Step 4  Click on Extensions->Add->Server Authentication->OK->Apply

Step 5  Click on Subject name, Enable Supply in request

Step 6  Click on Extensions->Issuance Policies->Edit->All Issuance Policies
Step 7  Leave the defaults for request handling

Step 8  Right-click on Certificate templates

Step 9  Select New Template to issue and select pxGrid

Step 10  You should see the pxGrid template
Configuring ISE for CA-Signed Certificates in a Stand-Alone Environment using pxGrid

In this section, the ISE pxGrid node is configured for a Certificate Authority (CA) signed environment. Initially, a “pxGrid” CSR request is generated from the ISE node and signed by the CA server using the pxGrid customized template. The certificate will be bound to the initial ISE CSR request.

The CA root certificate will be imported into the ISE certificate trusted store. The ISE identity certificate will be exported in the ISE certificate system store. The ISE node will be enabled for pxGrid operation.

Step 1 Generate a CSR request for the ISE node which will become the ISE pxGrid node
Administration->System->Certificates->Certificate Signing Requests->Generate

Note: The certificate usage can either be admin, multipurpose, or pxGrid as long as the template is a pxGrid customized one.

Step 2 Copy/paste the CSR information into Request a certificate->Advanced Certificate request selecting the customized pxGrid template, then Submit

Microsoft Active Directory Certificate Services – lab7-WIN-LTE11SBAKTM-CA
Submit a Certificate Request or Renewal Request
To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request
Request box:

Saved Request:
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

Certificate Template:
pxGrid

Additional Attributes:
Submit >
**Step 3** Download the CA root in base-64 encoded format

![Download CA Certificate](image1)

**Step 4** Upload the CA root into the ISE certificate trusted system store

Select -> Administration -> System -> Certificates -> Trusted Certificates -> upload the CA root certificate

![ISE Certificate Trusted System Store](image2)

**Step 5** Enable “Trust for authentication within ISE, then Submit

**Step 6** Upload the ISE pxGrid node certificate into the ISE certificate system store

Select -> Administration -> System -> Certificate Signing Requests and Bind certificate to the CSR request

![Certificate Signing Requests](image3)
Step 7  Browse and upload the ISE pxGrid node certificate, then Submit

Step 8  Enable pxGrid on the ISE node
Select-Administration->System-Deployment->highlight ISE node and enable pxGrid persona

Step 9  Verify that the pxGrid services are running and Enable “Enable Auto Registration”
Administration->pxGrid services

Note: The pxGrid service may take a few seconds to appear
Configuring FireSIGHT Management Center for CA-Signed Certificates

In this section, the FireSIGHT Management Center (FMC) is configured for Certificate Authority (CA)-signed operation. The FireSIGHT Management Center private key and CSR request are created from the FireSIGHT Management Center console (FMC). The CA server signs the CSR request and provides the FMC identity certificate using the customized pxGrid template.

Both the FMC certificate and FMC key are uploaded into FMC internal certs store. The CA root certificate is uploaded into the FMC trusted CA store.

**Step 1** Generate a FireSIGHT private key

**Note:** the password here will be defined in the pxGrid agent configuration

```
openssl genrsa -des3 -out sourcefire.key 4096
```

**Step 2** Generate a CSR request

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

**Step 3** Use WinSCP to copy the file from the FireSIGHT Management Center (FMC) locally to the PC

**Step 4** Copy/Paste FMC CSR request into Request a certificate->Advanced User request using the customized pxGrid template, then submit. Download the certificate in base-64 encoded format

![Certificate Request Image]
Step 5  Download the CA root certificate in base-64 encoded format

Step 6  Upload the CA root cert into the FireSIGHT Management trusted CA store
Select->Objects->Object Management->PKI->Trusted CAs->Add Trusted CA-> provide a name and upload root CA cert, then Save

Step 7  Upload the FireSIGHT Management center public certificate and private key to the FMC internal cert store
Select->Objects->Object Management->PKI->Internal Certs->add the Sourcefire CER file and Sourcefire KEY files, then Save

Configuring pxGrid agent using CA-signed certs

The pxGrid agent is responsible for the certificate configuration and communication between the FireSIGHT Management center and the ISE pxGrid node. The IP address of the ISE pxGrid node will be required. The FireSIGHT Management Center’s public certificate and key files will be required.

The FireSIGHT Management Center’s public certificate will serve as the host certificate. The CA root certificate will serve as the CA certificate.

The FireSIGHT key file will be the host key. The password of the key will also be required.

Step 1  Upload the pxGrid agent to the FireSIGHT Management Console using winSCP
**Step 2**  
Upload the FireSIGHT public cert, the FireSIGHT CA key and CA root certificate to FireSIGHT MC /Volume/home/admin, using WinSCP or other method

*Note:* Upper/lowercase syntax is maintained

**Step 3**  
SSH into the FireSIGHT Management Center and type:

```
sudo bash sfdc-pxgrid_agent_v1.0.35.sh
```

Please see below for a sample script:

```
Verifying archive integrity... All good.
Uncompressing Cisco pxGrid Agent Installer......
Installing the agent...  
Installing the pxGrid libraries and Perl module...
Setting up the agent to be managed by PM...
Installation done!
Configuring pxGrid...

Below you will be asked a series of questions relating to your pxGrid install and the files supporting it. Health alerts WILL be generated by PM until the configuration is completed, however. The answers to these questions will populate the /etc/sf/pxgrid/pxgrid.conf configuration file, which can be manually modified later at any time. A configuration example is provided in the same directory with the filename pxgrid.conf.example.

To get this all to work, the agent will need to connect to a pxGrid server. This is typically your Cisco Identity Services Engine instance, which must also have the pxGrid service enabled.

What is the IP address of your pxGrid server
> 10.0.0.15

Every agent connecting to pxGrid must have a unique host certificate which will be used to identify the agent host. Associated key and CA certs must also be provided.

What is the full path and filename to the host certificate?
> /Volume/home/admin/sourcefire.cer
What is the full path and filename to the host key?
> /Volume/home/admin/sourcefire.key
What is the host key password?
> cisco123
What is the full path and filename to the CA certificate?
> /Volume/home/admin/root.cer

Configuration written to /etc/sf/pxgrid
```
Step 4  The FireSIGHT Management Center should have successfully registered as a pxGrid client and subscribed to the EPS published topic
Select Administration->pxGrid Services
FireSIGHT pxGrid remediation module

In this section, the pxGrid mitigation remediation module is uploaded into the FireSIGHT Management Center. A pxGrid instance is created and the remediation types defined. These remediation types provide the pxGrid ANC functionality when assigned as responses to their respective correlation policies.

These remediation types consist of:

- **Quarantine**- quarantines an endpoint based on source ip address
- **portBounce**- temporarily bounces the endpoint or host port
- **Terminate**- terminates the end-user session
- **Shutdown**- initiates a host port shutdown, this will insert a “shutdown” command on the switch port configuration
- **reAuthenticate**- reAuthenticates the end-user
- **UnQuarantine**- unquarantines the endpoint

Uploading FireSIGHT pxGrid remediation module

**Step 1**  
Upload the pxGrid remediation module to the FireSIGHT Management Center  
Select Policies->Actions->Remediations->Modules-Install a new module browse and upload the module, the pxGrid_Mitigation_Remediation_v1.0.tgz file.

Create new instance

**Step 1**  
Create new pxGrid instance  
Select Policies->Actions->Remediations->Instances->Add a new Instance->Module type->Talos Labs-pxGrid mitigation->Add->Instance Name->pxGrid->Create
Create FireSIGHT pxGrid mitigation types

These remediation types define the pxGrid ANC mitigation actions that are assigned as responses to the correlation rules that invoke remediation action on endpoints

**Note:** Click on Magnifying Glass to select

**Quarantine**

Create quarantine mitigation action based on mitigate source

**Step 1** Policies->Actions->Remediations->Modules->Talos Labs- pxGrid Mitigation->pxGrid under Configured Instances

**Step 2** Click on the “magnifying glass”->Add a new remediation type based on Mitigate Source

**Step 3** Enter the remediation name: Quarantine_SourceIP

**Step 4** For mitigation action, select quarantine from the drop-down menu

**Step 5** Click Save

**portBounce**

Create portBounce mitigation action based on mitigate source

**Step 1** Policies->Actions->Instances, click the magnifying glass next to “pxGrid” under Configured Instances

**Step 2** Choose Mitigate Source from the drop-down and click Add

**Step 3** Enter the remediation name: portBounce

**Step 4** For mitigation action, select portBounce from the drop-down menu

**Step 5** Click Save
**reAuthenticate**

Create reAuthenticate mitigation action based on mitigate source

**Step 1**  Policies->Actions->Instances, click the magnifying glass next to “pxGrid” under Configured Instances

**Step 2**  Choose **Mitigate Source** from the drop-down and click **Add**

**Step 3**  Enter the remediation name: **reAuthenticate**

**Step 4**  For mitigation action, select **reAuthenticate** from the drop-down menu

**Step 5**  Click **Save**

---

**shutDown**

Create shutdown mitigation action based on mitigate source

**Step 1**  Policies->Actions->Instances, click the magnifying glass next to “pxGrid” under Configured Instances

**Step 2**  Choose **Mitigate Source** from the drop-down and click **Add**

**Step 3**  Enter the remediation name: **Shutdown**

**Step 4**  For mitigation action, select **shutdown** from the drop-down menu

**Step 5**  Click **Save**
terminate
Create terminate mitigation action based on mitigate source

Step 1  Policies->Actions->Instances, click the magnifying glass next to “pxGrid” under Configured Instances
Step 2  Choose Mitigate Source from the drop-down and click Add
Step 3  Enter the remediation name: Terminate
Step 4  For mitigation action, select terminate from the drop-down menu
Step 5  Click Save

unQuarantine
Create unquarantine mitigation action based on mitigate source

Step 1  Policies->Actions->Instances, click the magnifying glass next to “pxGrid” under Configured Instances
Step 2  Choose Mitigate Source from the drop-down and click Add
Step 3  Enter the remediation name: UnQuarantine_SourceIP
Step 4  For mitigation action, select unquarantine from the drop-down menu
Step 5  Click Save
In this section, the pxGrid Intrusion Policy is created and deployed to the FireSIGHT sensor. This policy contains “SERVER IIS CMD.EXE access” rule, when the end-user types in: www.yahoo.com/cmd.exe in their browser, this will generate an intrusion event based on the correlation policies, with the exception of the unquarantine correlation policy.

**Step 1** Navigate to Policies->Intrusion->Intrusion Policy  
**Step 2** Click on Create Policy  
**Step 3** Name the new policy pxGrid_Intrusion_Policy  
**Step 4** Click Create Policy

**Step 5** Click->pxGrid_Intrusion_Policy to edit

**Step 6** Click->Rules and filter on: cmd.exe, and select the rules below
**SECURE ACCESS HOW-TO GUIDES**

**Step 7**  
Click on Rule State > Generate Events, then OK

**Step 8**  
You should see a success message for “successfully set the rule state for 3 rules”

**Step 9**  
Click Policy Information

**Step 10**  
Then click “Commit Changes”
Step 11  Click OK
Step 12  Select and edit Policies->Access Control Policies->Default Intrusion Prevention

Step 13  Under Default actions, from the dropdown select the pxGrid_Intrusion_Policy

Step 14  Click on Save
Step 15  Click on the Logging icon at the bottom right of the table

Step 16  Enable logging at the Beginning and End of a connection. Select Defense Center as the destination
Step 17  Click OK
Step 18  Click Save and Apply
Step 19  You should see the following:

Step 20  Click Apply All
Step 21  You should see the task has been queued

Step 22  Click Ok
Step 23  Select System->Monitoring->Task Status for results, notice the task was completed successfully
FireSIGHT Connection Rule

In this section we define a connection rule to add to the Default Access policy. This Default access policy also includes the pxGrid Intrusion Policy. This connection rule monitors connection events over HTTP/HTTPS and logs these connection details to FireSIGHT Management Center. This connection rule will be used by the UnQuarantine Policy to monitor connection events that trigger the unquarantine remediation type.

**Step 1** Navigate to **Policies->Access Control**

**Step 2** Edit **Default Intrusion Prevention** by clicking on the pencil

**Step 3** Click **Add Rule**

**Step 4** Name the rule “HTTP Checks”

**Step 5** Select the **Ports** Tab

**Step 6** Select **HTTP** and **HTTPS** as destination ports

**Step 7** Click on **IPS** and select the **pxGrid_Intrusion_Policy**
Step 8  Select Logging

Step 9  You should see the following

Step 10  Select Save

Step 11  Select Save and Apply
**Step 12**  Click **Apply All**

**Step 13**  You should see “Policy apply task queued, click **OK**”
Configuring ISE EPS Service and Quarantine Authorization Policies

This section illustrates the steps for enable EPS in ISE and the creation of the quarantine authorization policies in ISE. In ISE 1.4, the Endpoint Protection Service is renamed to Adaptive Network Control. In ISE 2.0, this is enabled by default, there is no Adaptive Network Control service setting under Administration.

**Note:** The Adaptive Network Control Policies in ISE 2.0 are dependent on pxGrid clients that register to the AdaptiveNetworkControl Capability. This is not the case with the FireSIGHT Management Center. The FireSIGHT Management Center registers to the EndpointProtectionService Capability and relies on the ISE authorization policies. Please note that in ISE 2.0, unquarantining the endpoint must be done using the pxGrid GCL EPS_unquarantine script. This is performed in the FireSIGHT Management Center by creating an unquarantine correlation policy, uncorrelation rule, and assigning the unquarantined mitigation response to the unquarantine correlation policy.

**Step 1**
Enable ISE Endpoint Protection Service

Administration->System->Settings->Endpoint Protection Service and enable Endpoint Protection Service->Save

**Note:** Endpoint Protection service is non-applicable in ISE 2.0, it is turned on by default.

**Step 2**
Create Quarantine Authorization Profile

Policy->Policy Elements->Results->Authorization->Authorization Profiles->Add->Name:Quarantine->Save

**Note:** In this example, Access Type was set to ACCESS_ACCEPT to demonstrate the authorization condition profile.

**Step 3**
Create Quarantine Authorization Policy
Policy->Authorization->Exceptions-> and enter the following:
   Rule Name: EPS Quarantine
   Create a new Condition Rule: Session:EPSStatus:EQUALS:Quarantine
   Standard Profile: Quarantine
   Click->Done

Step 4   Click->Save
FireSIGHT Management Center Correlation Policies

In this section the FireSIGHT correlation polices and rules are created for Quarantine, portbounce, reAuthenticate, portshutdown, terminate and unquarantine. These policies are assigned their respective remediation responses, providing the pxGrid ANC mitigation remediation actions on the endpoint.

The correlation policies are created and then the rule modules. The correlation policies will add their respective rule modules. The rule modules will be assigned their respective responses.

For example, the Quarantine Correlation Policy will be created. The Quarantine rule module will be created, such that when an intrusion event occurs, the Source IP address of the endpoint will be quarantined. The Quarantine rule module will be assigned the quarantine remediation type response. When an end-user violates a pxGrid Intrusion Policy, this will trigger an intrusion event, and also a correlation event which initiates the quarantine mitigation action based on the quarantine remediation type response.

The portbounce, reAuthenticate, portshutdown, terminate policies will follow the same flow.

The Unquarantine policy will have an unquarantine rule module that triggers a connection event, when the endpoint access a specific URL site, it will be unquarantined based on the Source IP address of the endpoint.

Quarantine

The quarantine correlation policy is created.

**Step 1**  Policies->Correlation->Policy Management->Create Policy->pxGrid_ANC_Quarantine->Save
Step 2  Policies->Correlation->Rule Management->Create Rule->add rule name->Quarantine_by_SourceIP, and enter the following, then Save

**Note:** This rule provides a proof of concept where the source ip address is quarantined

Step 3  Policies->Correlation->Policy Management->pxGrid ANC Quarantine->Add rules->pxGrid ANC Quarantine->Add

Step 4  Next we will add a response, Click on Responses tab
Step 5  
Move the Quarantine_SourceIP to assigned Responses->Update->Save

Step 6  
Activate the Quarantine correlation policy by clicking on the button

Testing

An end-user will type in their browser window [www.yahoo.com/cmd.exe](http://www.yahoo.com/cmd.exe), which will trigger an intrusion event from a “SERVER-IIS.cmd.exe access” rule violation in FireSIGHT’s pxGrid Intrusion Policy. The endpoint will be quarantined based on the quarantine mitigation response assigned to the quarantine rule as defined in the correlation policy.

Step 1  
End-user enters [www.yahoo.com/cmd.exe](http://www.yahoo.com/cmd.exe) in their browser

Step 2  
This triggers a “web application attack” intrusion event
Step 3  This also triggers a “correlation event”
Note the Source IP address that will be quarantined and the user information based on the FireSIGHT LDAP/User Awareness configuration.

Step 4  As we continue with the same event
Note the destination port and the rule violation as contained in the pxGrid_Intrusion_Policy rule.

Step 5  As we proceed further with the same event
Note the correlation policy and correlation rule that triggered the assigned quarantine mitigation response
SECURE ACCESS HOW-TO GUIDES

Step 6  To view the response in ISE, select Operations->Authentications

portBounce

The portBounce correlation policy is created

Step 1  Policies->Correlation->Policy Management->Create Policy->pxGrid ANC portBounce->Save

Step 2  Policies->Correlation->Rule Management->Create Rule->add rule name->portBounce_by_SourceIP, and enter the following, then Save
Step 3 Policies->Correlation->Policy Management->pxGrid ANC portBounce>Add rules->select “portBounce_by_SourceIP, Add rule

Step 4 Next we will add a response, Click on Responses tab

Step 5 Select Policies->Correlation->portBounce_by_SourceIP, move portBounce to assigned Responses->Update->Save
Step 6  Activate terminate policy, click on **button** below which will turn on the policy

Testing

An end-user will type in their browser window [www.yahoo.com/cmd.exe](http://www.yahoo.com/cmd.exe), which will trigger an intrusion event from a “SERVER-IIS.cmd.exe access” rule violation in FireSIGHT’s pxGrid Intrusion Policy. The port containing the endpoint will be bounced based on the portbounce mitigation response assigned to the rule as defined in the Correlation policy.

**Step 1**  End-user enters [www.yahoo.com/cmd.exe](http://www.yahoo.com/cmd.exe) in their browser

**Step 2**  This triggers a “web application attack” intrusion event

**Step 3**  This also triggers a “correlation event”

The port will be bounced for the host who belongs to the Source IP address.

**Note:** There is no user information, due to Network Discovery hosts and users not being turned on.
Step 4  As we continue with the same event
Note the rule violation as contained in the pxGrid_Intrusion_Policy rule.

Step 5  As we proceed further with the same event
Note the correlation policy and correlation rule that triggered the assigned portbounce mitigation response.

Step 6  To view the response in ISE, select Operations-Authentications
Step 7  By selecting the details button, we see that the port is bounced based on the CiscoAVpair attributes

Step 8  Additionally, you can view the FireSIGHT Management Center syslog events to verify that the portbounce mitigation action was successful
portShutdown

The portShutdown correlation policy is created.

Step 1  Policies->Correlation->Policy Management->Create Policy->pxGrid_ANC_shutdown->Save

Step 2  Policies->Correlation->Rule Management->Create Rule->add rule name->shutdown_by_SourceIP, and enter the following, then Save

Step 3  Policies->Correlation->Policy Management->pxGrid_ANC_shutdown>Add rules->select “shutdown_bySourceIP, Add rule
Step 4  Next we will add a response, Click on Responses tab

![Policy Management interface](image1)

**Step 5**  Select Policies->Correlation->pxGrid_ANC_shutdown, move the Shutdown to assigned Responses->Update->Save

![Policy Management interface](image2)

**Step 6**  Activate terminate policy, click on button below which will turn on the policy

![Policy Management interface](image3)
Testing

An end-user will type in their browser window www.yahoo.com/cmd.exe, which will trigger an intrusion event from a “SERVER-IIS.cmd.exe access” rule violation in FireSIGHT’s pxGrid Intrusion Policy. The endpoint’s port will be shutdown based on the shutdown mitigation response assigned to the rule defined in the correlation policy.

**Step 1**  End-user enters www.yahoo.com/cmd.exe in their browser

**Step 2**  This triggers a “web application attack” intrusion event

**Step 3**  This also triggers a “correlation event”

Note the port that for the host who belongs to the Source IP address will be shutdown

**Note:** There is no user information, due to Network Discovery hosts and users not being turned on.

**Step 4**  As we continue with the same event

Note the rule violation as contained in the pxGrid_Intrusion_Policy rule.
Step 5  As we proceed further with the same event
Note the correlation policy and correlation rule that triggered the assigned portShutdown mitigation response

Step 6  To view the response in ISE, select Operations->Authentications

Step 7  By selecting the details button, we see that the port is disabled based on the CiscoAVpair attributes
Step 8  Additionally, you can view the FireSIGHT Management Center syslog events to verify that the port shutdown mitigation action was successful.

Step 9  Additionally, on the switch you will see “shutdown” on the port.

```bash
interface GigabitEthernet1/0/3
description internal LAN
switchport mode access
shutdown
authentication host-mode multi-auth
authentication open
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication fallback mab
mab
```

**reAuthenticate**

The reAuthenticate policy is created.

**Step 1**  Policies->Correlation->Policy Management->Create Policy->pxGrid ANC reAuthenticate->Save

**Step 2**  Policies->Correlation->Rule Management->Create Rule->add rule name->reAuthenticate_bySourceIP, and enter the following, then Save
Step 3  Policies->Correlation->Policy Management->pxGrid_ANC_reAuthenticate>Add rules->select “reAuthenticate_bySourceIP”, Add rule

Step 4  Next we will add a response, Click on Responses tab
Step 5: Select Policies->Correlation->pxGrid_ANC_reAuthenticate, move reAuthenticate to assigned Responses->Update->Save

Step 6: Activate terminate policy, click on button below which will turn on the policy

Testing

An end-user will type in their browser window www.yahoo.com/cmd.exe, which will trigger an intrusion event from a “SERVER-IIS.cmd.exe access” rule violation in FireSIGHT’s pxGrid Intrusion Policy. The end-user will be reauthenticated based on the reAuthenticate mitigation response assigned to the rule as defined in the correlation policy.

Step 1: End-user enters www.yahoo.com/cmd.exe in their browser
Step 2: This triggers a “web application attack” intrusion event
SECURE ACCESS HOW-TO GUIDES

Events By Priority and Classification

<table>
<thead>
<tr>
<th>Message</th>
<th>Priority</th>
<th>Classification</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERVER-OS cmd exe access (-1.1001)</td>
<td>high</td>
<td>Web Application Attack</td>
<td>1</td>
</tr>
</tbody>
</table>

**Step 3**

This also triggers a “correlation event”

Note that the end-user who belongs to the Source IP address will be reauthenticated.

**Note:** There is no user information, due to Network Discovery hosts and users not being turned on.

**Step 4**

As we continue with the same event

Note the rule violation as contained in the pxGrid_Intrusion_Policy rule.

**Step 5**

As we proceed further with the same event

Note the correlation policy and correlation rule that triggered the assigned reauthenticate mitigation response.
Step 6  To view the response in ISE, select Operations->Authentications

Step 7  By selecting the details button, we see that the port is disabled based on the CiscoAVpair attributes
Step 8  Additionally, you can view the FireSIGHT Management Center syslog events to verify that the reAuthenticate mitigation action was successful.

Terminate

The terminate correlation policy is created.

Step 1  Policies->Correlation->Policy Management->Create Policy->pxGrid ANC Terminate->Save

Step 2  Policies->Correlation->Rule Management->Create Rule->add rule name->Terminate_by_SourceIP, and enter the following, then Save
Step 3  Policies > Correlation > Policy Management > pxGrid ANC Terminate > Add rule > select “Terminate by SourceIP”, Add rule

Step 4  Next we will add a response, Click on Responses tab

Step 5  Select Policies > Correlation > pxGrid_ANC_Terminate, move Terminate to assigned Responses > Update > Save
Step 6  Activate terminate policy, click on **button** below which will turn on the policy

![Image of a policy management interface](image)

**Testing**

An end-user will type in their browser window [www.yahoo.com/cmd.exe](http://www.yahoo.com/cmd.exe), which will trigger an intrusion event from a “SERVER-IIS cmd.exe access” rule violation in FireSIGHT’s pxGrid Intrusion Policy. The end-user’s session will be terminated based on the terminate mitigation response assigned to the rule as defined in the correlation policy.

**Step 1**  End-user enters [www.yahoo.com/cmd.exe](http://www.yahoo.com/cmd.exe) in their browser

**Step 2**  This triggers a “web application attack” intrusion event

**Step 3**  This also triggers a “correlation event”

*Note:* There is no user information, due to Network Discovery hosts and users not being turned on.
Step 4  As we continue with the same event
Note the rule violation as contained in the pxGrid_Intrusion_Policy rule.

Step 5  As we proceed further with the same event
Note the correlation policy and correlation rule that triggered the assigned terminate mitigation response

Step 6  To view the response in ISE, select Operations-Authentications

Step 7  Additionally, you can view the FireSIGHT Management Center syslog events to verify that the terminate mitigation action was successful
Unquarantine Correlation Policy

The unquarantine correlation policy and rule are created as in the same process as the rest of the correlation polices. This only difference is that the correlation rules will be triggered from a “connection event” instead on an “intrusion” event. When the end-user browses to the URL defined in the unquarantine rule, the unquarantine mitigation response will unquarantine the endpoint.

We will also need to create a “connection” rule such that all HTTP/HTTPS traffic is monitored and logged and assigned to the Default Access policy which also contains the pxGrid Intrusion Policy.

Step 1  Policies->Correlation->Policy Management->Create Policy->pxGrid_ANC_Unquarantine->Save

Step 2  Policies->Correlation->Rule Management->Create Rule->add rule name->UnQuarantine_by_DestinationIP, then Save

Step 3  Policies->Correlation->Policy Management->pxGrid_ANC_Unquarantine->Add rules->UnQuarantine_by_DestinationIP, then Save changes
Step 4  Next we will add a response, Click on Responses tab

Step 5  Select Policies->Correlation->UnQuarantine_by_DestinationIP, move the UnQuarantine_SourceIP to assigned Responses->Update->Save
Testing

An end-user will type in their browser window [www.yahoo.com/cmd.exe](http://www.yahoo.com/cmd.exe), which will trigger an intrusion event from a “SERVER-IIS.cmd.exe access” rule violation in FireSIGHT’s pxGrid Intrusion Policy. The endpoint will be unquarantined based on the unquarantine mitigation response assigned to the rule as defined in the correlation policy.

**Step 1**  
End-user enters http://192.168.1.14/Unquarantine/unquarantine.htm in their browser

**Step 2**  
This triggers a “connection” event

**Step 3**  
Here’s a continuation of the connection event
Step 4  This also triggers a “correlation event”
Note the Source IP address will be unquarantined.

Step 5  As we continue with the same event
Note the connection event.

Step 6  As we proceed further with the same event
Note the correlation policy and correlation rule that triggered the assigned quarantine mitigation response
Step 7  To view the response in ISE, select **Operations->Authentications**

![Image of ISE interface showing operations and authentications](image1)

Step 8  Additionally, you can view the FireSIGHT Management Center syslog events to verify that the unquarantine mitigation action was successful

![Image of FireSIGHT Management Center syslog events](image2)
Troubleshooting

**ISE pxGrid Services do not come up**
Resolution: Run stop “application stop ise” on the ISE pxGrid node.

**pxGrid agent certificate error messages**
Resolution: View FireSIGHT Management Center Syslog messages for certificate error messages.
Ensure that the full path to the certificate is correct: /Volume/home/admin/…
Ensure time is synced between the FireSIGHT Management Center and the ISE pxGrid node.
FireSIGHT, ISE pxGrid node, and endpoint should all be DNS resolvable

**FireSIGHT Management Center not communicating with ISE**
Resolution: FireSIGHT, ISE pxGrid node, and endpoint should all be DNS resolvable
Ensure time is synced between the FireSIGHT Management Center, Sensor and the ISE pxGrid node.
Reboot FireSIGHT Management Center

**No correlation events appear in the FireSIGHT Management Center**
Resolution: Ensure time is synced between the FireSIGHT Management Center, Sensor and the ISE pxGrid node

**FireSIGHT failed mitigation attempts**
Resolution: Ensure time is synced between the FireSIGHT Management Center, Sensor and the ISE pxGrid node.
Reboot FireSIGHT Management Center

**Mitigation “lookup failure” attempts**
Resolution: Ensure the IP address of the device is has been authenticated through ISE. The remediation type has been configured for source.
pxGrid connection failure attempts syslog error messages from FireSIGHT Management Console

Resolution: Ensure the ISE pem file contains the certificate by running the following on the FireSIGHT Management Console CLI

```
openssl x509 -noout -text -in ise14lab.pem
```

The pem file should contain the certificate

```
Certificate:  
Data:  
   Version: 3 (0x2)  
   Serial Number:  
      56:19:bf:90:00:00:00:00:00:ab:b7:4f:a0:57:21:a0:03  
   Signature Algorithm: sha1WithRSAEncryption  
   Issuer: CN=ise14.lab8.com  
   Validity  
      Not Before: Oct 11 01:46:56 2015 GMT  
      Not After : Oct 10 01:46:56 2016 GMT  
   Subject: CN=ise14.lab8.com  
   Subject Public Key Info:  
      Public Key Algorithm: rsaEncryption  
      Public-Key: (2048 bit)  
         Modulus:  
            38:5b:dd:2f:cc:2d:6e:90:02:8e:5a:9f:7a:2d:dc:44:  
            a6:93:1b:b0:00:c3:9b:bc:c4:98:45:af:79:1b:9c:55:  
            11:d5:58:0d:00:aa:26:3a:5f:c3:08:1c:dc:a0:26:  
            e8:87  
         Exponent: 65537 (0x10001)  
X509v3 extensions:  
 X509v3 Basic Constraints:  
   CA:TRUE  
X509v3 Key Usage:  
   Digital Signature, Key Encipherment, Key Agreement, Certificate Sign  
X509v3 Subject Key Identifier:  
X509v3 Extended Key Usage:  
   TLS Web Server Authentication, TLS Web Client Authentication  
Netscape Cert Type:  
   SSL Server  
Signature Algorithm: sha1WithRSAEncryption  
```
If you do not see this, export the ISE identity self-signed public-private key pair, provide the password, add the ISE identity self-signed certificate to the FMC trusted CA store.

### Verifying self-signed certs by importing into ISE system store

**Resolution:** This is not necessarily a problem, however, the vendor’s public/private key pair can be imported into the ISE trusted system store. This is due to using ISE sample certs from the pxGrid SDK and should be for testing only, not recommended for productional use. Please use the steps in Configuring FireSIGHT Management Center for Self-Signed Certificates for configuring self-signed certificates.

**Step 1** Import the FireSIGHT internal CA public/private key pair into the ISE certificate system store. The private key password will be required.

Administration->System->Certificates->System Certificates and import the FireSIGHT internal public/private key pair. Enter the private key password.

**Step 2** Select pxGrid for certificate “usage”, then Submit

**Step 3** You should see the following:
Secure Access How-to Guides

Certificate Management

System Certificates

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

Default self-signed server certificate - generated by the Identity Services Engine.

Default Portal Certificate

Several certificate types are present:

- CSR (Certificate Signing Request)
- PEM (Privacy Enhanced Mail)
- DER (Distinguished Encoding Rules)
- PFX (Personal Information Exchange)

Export:

- CSR
- PEM
- DER
- PFX

Import:

- CSR
- PEM
- DER
- PFX
Solution Caveats

pxGrid & Identity mapping service restart

**Description**: pxGrid & Identity mapping service restart on ISE pxGrid node when ever a cert is imported/deleted from the trust store of ISE deployment

**Defect filed**: CSCuv43145

**Work around**: None needed as the service will be automatically restarted but while the service is in the restart state new quarantine events will not be processed.

**Resolution plan**: ISE Carlsbad release spring 2016

Active pxGrid node is not reflected in the GUI; It is reflected in CLI

**Description**: When two pxGrid nodes are available in a pxGrid HA deployment, one is active and the other is standby. Identifying which is active, and administrator needs to review the pxGrid status in the CLI. The status is not visible in the UI Deployment page. This addition will be made in Carlsbad.

**Work around**: Use the CLI to determine active/passive status

**Resolution plan**: ISE Carlsbad release spring 2016
References

Configuring pxGrid in a Distributed ISE Environment:
