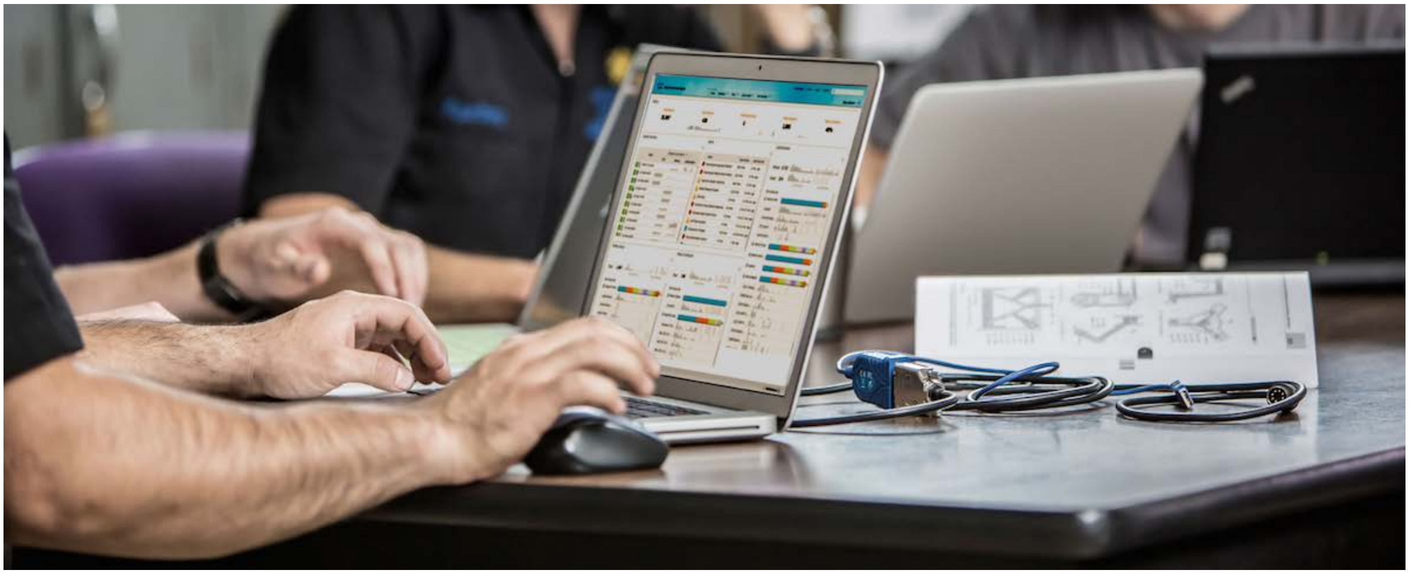


How to Integrate Cisco Firepower Management Center 6.0 With ISE and TrustSec Through pxGrid

Table of Contents

About This Document

This document is intended for Cisco engineers and customers who are interested in deploying Cisco Firepower Management Center (FMC) 6.0 with Cisco Identity Service Engine (ISE 1.3 or higher) using (platform exchange Grid) pxGrid.

Please note that pxGrid remediation is not supported in Cisco Firepower Management Center FMC 6.0.

Cisco Firepower Management Center (FMC) 6.0 can now enforce an organizations security policy based on ISE session attribute information available through pxGrid. These security policies can be applied to and enforced by the Cisco Firepower to managed NGIPS sensors and/or an ASA with Firepower services. The ASA with Firepower services vsm also manage these policies locally via ASDM.

This document provides the details of configuring Cisco Firepower Management Center (FMC) 6.0 and pxGrid integration with ISE in an ISE Stand-Alone environment using self-signed certificates or using CA (Certificate Authority)- signed certificates. If deploying pxGrid in an ISE production environment, please see http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-88-Configuring-pxGrid-in-an-ISE-Distributed-Environment.pdf

In this document an ASA with Firepower services will be configured with the ASA Firepower (sfr) module and register with Cisco Firepower Management Center (FMC) 6.0 to use the centrally managed Cisco Firepower Management Center policy. The ASA with Firepower services will also be configured on-box with the Firepower intrusion policy and access control rule independent of the FMC.

The Cisco Firepower Management Center managed security policy and ASA on box Firepower Management policy will consist of an intrusion policy and Employee SGT access control rule for denying access to specific web categories.

The reader should have some familiarity with ISE, Cisco Firepower Management Center and pxGrid.

.

Solution Introduction Cisco Management Center 6.0 with TrustSec Using pxGrid with ISE

Cisco Firepower Management Center (FMC) 6.0 centrally manages and enforces an organizations security policy by applying intrusion policies and access controls rules to the NGIPS sensors and the ASA with Firepower services.

FMC 6.0 uses network discovery to obtain the user identity information. In addition, the SFUA (Sourcefire User Agent) is used to obtain more granular details for the user. The SFUA is used to obtain the user-to-ip mapping. Either the SFUA or ISE can be used at a time.

End-users authenticate against an AD or LDAP realm, a default policy containing an organization's security policy is applied to the Cisco Firepower NGIPS sensors or ASA with Firepower services based on the user group information. The security policy can encompass an intrusion policy, where pre-set levels of balanced security can be enforced, as well as access control rules specific to user group.

Cisco (Platform Exchange Grid) pxGrid provides additional ISE attributes: security group tag (SGT), endpoint profile device information, location IP to be used in the Cisco Firepower Management 6.0 access control rule policies.

SGT (Security Group Tags) are a component of TrustSec, and are defined in ISE and are implemented in ISE as authorization policies based on an organization's security policy for identity access. As an example, all wired users using recommended corporate recommended devices area are tagged with an Employee SGT once successfully authenticated through ISE. Wireless users using nonrecommended corporate devices are tagged with Non-Employee SGT once successfully authenticated. These users must exist in the Firepower Management Center ISE realm.

The FMC 6.0 can then apply access control rules based on these security group tags. In addition FMC 6.0 can also include the additional ISE pxGrid attributes to make the Firepower Management Center 6.0 policy context-aware.

Cisco Identity Service Engine (ISE) provides the identity solution and Cisco (Platform Exchange Grid) pxGrid framework.

Cisco Firepower Management Center 6.0

The Cisco Firepower Management Center provides a centralized management console with web interface to manage Firepower Appliances (NGIPS) and Firepower Services. It can be used to perform administrative, management, analysis, and reporting tasks. It automatically aggregates and correlates intrusion, file, malware, discovery, connection, and performance data, assessing the impact of events on particular hosts and tagging hosts with indications of compromise.

Cisco TrustSec

Security Group Tags (SGT) are part of the Cisco TrustSec solution. SGTs are defined in ISE and applied at ingress (inbound to the network). SGTs can represent a grouping of users, endpoint devices, line of business, etc. SGTs can then be applied to a network access policy and used by network devices to make forwarding decisions and share access control policies across the network infrastructure. A SGT is a unique 16-bit security group number assigned to a security group. Security groups can also have descriptive naming.

SGTs are defined and implemented as authorization profiles in an ISE authorization policy consisting of condition rules defining an organizations security policy.

SGTs can make an organization's security policy uniform or global across the network.

In this document, an ISE authorization policy will be created such that all successfully authenticated end-users belonging to the /users/domain Windows group will receive an employee SGT. This employee SGT will be used in a Cisco Firepower managed access control rule policy denying access to streaming media, peer-to-peer applications, hacking, malware sites, and gambling categories.

Cisco Identity Service Engine (ISE)

Identity Service Engine (ISE) is a security policy management and identity access management platform solution. ISE provides centralized management by defining/issuing/enforcing 802.1x authentications, guest management policies, posture, client provisioning and TrustSec policies. The ISE session directory provides rich contextual information for IEEE 802.1x authenticated users that can be used in security solutions to include context-aware policies via pxGrid.

In addition ISE simplifies access control and security compliance for wired, wireless, and VPN connectivity and supports corporate security policy initiatives.

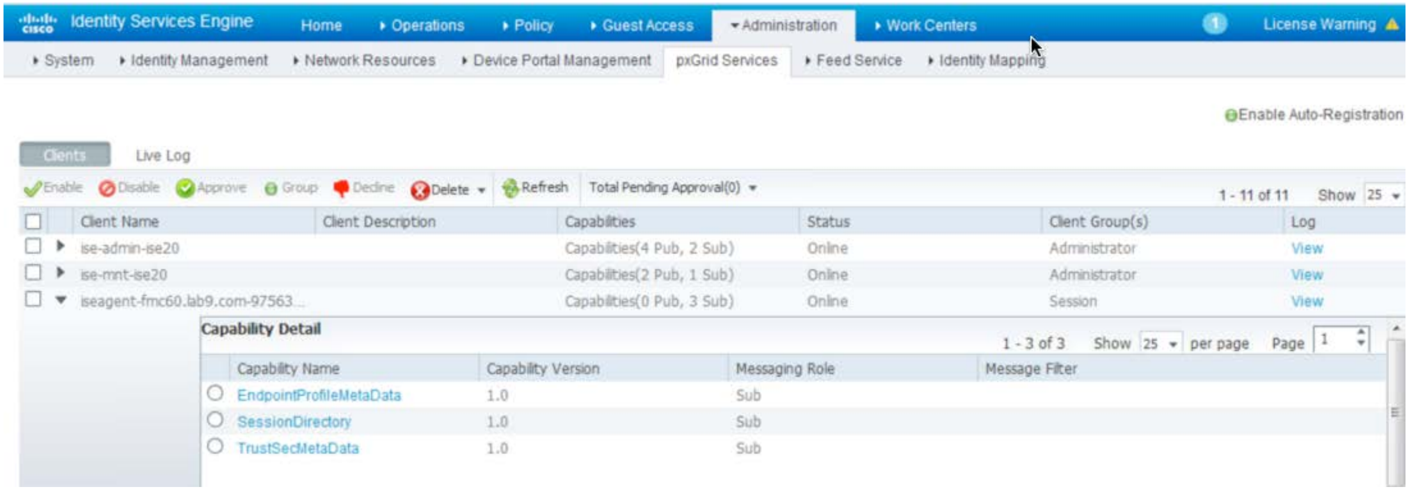
Cisco pxGrid

Cisco (Platform Exchange Grid) pxGrid enables multivendor, cross platform network system collaboration among parts of the IT infrastructure such as security monitoring and detection system, network policy platforms, asset and virtually configuration management, identity and access management platforms, and virtually and other IT operations platform.

When business or operational needs arise, Cisco's Security Solutions such as Firepower Management Center 6.0 and ecosystem partners can use pxGrid to exchange contextual information via a publish/subscribe method.

Technical Overview

Cisco Firepower Management Center 6.0 will register as a pxGrid client to the ISE pxGrid node and subscribe to ISE published topics or capabilities to receive ISE session information. This session information includes: Security Group Tags (SGT), endpoint profile device information, endpoint location to be used in Firepower Management Center's 6.0 access control roles.



☐		Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
☐	▸	ise-admin-ise20		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
☐	▸	ise-mnt-ise20		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
☐	▾	iseagent-fmc60.lab9.com-97563...		Capabilities(0 Pub, 3 Sub)	Online	Session	View

Capability Detail

1 - 3 of 3 Show 25 per page Page 1

	Capability Name	Capability Version	Messaging Role	Message Filter
○	EndpointProfileMetaData	1.0	Sub	
○	SessionDirectory	1.0	Sub	
○	TrustSecMetaData	1.0	Sub	

The function of these topics are:

- TrustsecMetadata information which exposes the security group tag umber and description

```
SecurityGroup : id=150138d0-cfc7-11e3-9e0e-000c29e66166, name=Engineering, desc=, tag=3
```

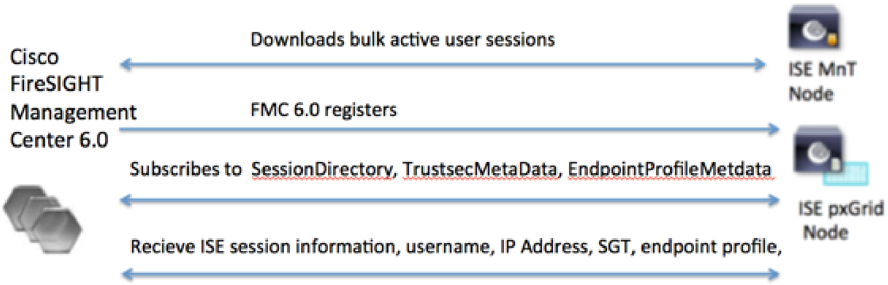
- EndpointProfileMetadata which provides ISE endpoint policy information such as changes/modifications to the ISE profiling policy

```
Endpoint Profile : id=886f7570-bd0c-11e3-a88b-005056bf2f0a, name=Apple-iDevice, fqname Apple-Device:Apple-
iDevice
```

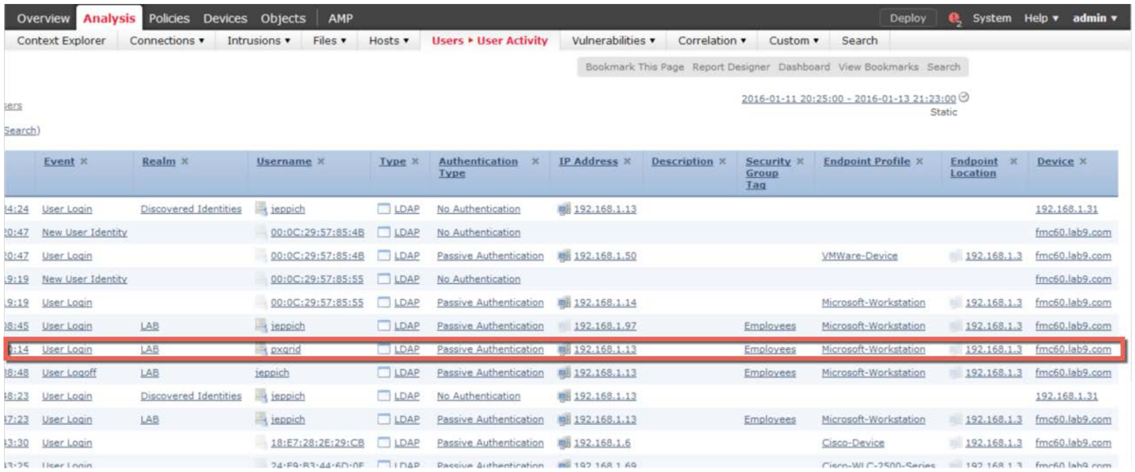
- SessionDirectory exposes the authenticated use session attribute information such as the username and device information

```
session (ip=192.168.1.14, Audit Session Id=0A0301030000001E00FEBAD7, User Name=jsmith, Domain=lab4.com,
Calling station id=00:0C:29:77:A8:C7, Session state= STARTED, Epsstatus=null,Security Group=Engineering,
Endpoint Profile=Microsoft-Workstation, NAS IP=192.168.1.2, NAS Port=GigabitEthernet1/0/9, RADIUSAVPairs=[
Acct-Session-Id=00000027], Posture Status=null, Posture Timestamp=, Session Last Update Time=Tue Apr 29
15:11:46 GMT-05:00 2014
```

Active user sessions bulk downloads occur upon Cisco Firepower Management Center startup or reboots. Bulk downloads of session information is downloaded from the ISE MNT node via the ISE RESTful API. This session information includes: username, IP address, SGT, endpoint profile. If there are any updates such as recently authenticated ISE users, or modifications of existing SGT, these changes will occur in real-time due to the Cisco Firepower Management Center's topic subscription:


Cisco FireSIGHT Management Center 6.0
Downloads bulk active user sessions
ISE MnT Node
FMC 6.0 registers
Subscribes to SessionDirectory, TrustsecMetaData, EndpointProfileMetdata
ISE pxGrid Node
Recieve ISE session information, username, IP Address, SGT, endpoint profile,

The ISE session information from ISE can be seen under the Firepower Management Center's user activity screen.



2016-01-11 20:25:00 - 2016-01-13 21:23:00
Static

	Event	Realm	Username	Type	Authentication Type	IP Address	Description	Security Group Tag	Endpoint Profile	Endpoint Location	Device
34:24	User Login	Discovered Identities	jeppich	LDAP	No Authentication	192.168.1.13					192.168.1.31
20:47	New User Identity		00:0C:29:57:85:4B	LDAP	No Authentication						fmc60.lab9.com
20:47	User Login		00:0C:29:57:85:4B	LDAP	Passive Authentication	192.168.1.50			VMWare-Device	192.168.1.3	fmc60.lab9.com
19:19	New User Identity		00:0C:29:57:85:55	LDAP	No Authentication						fmc60.lab9.com
19:19	User Login		00:0C:29:57:85:55	LDAP	Passive Authentication	192.168.1.14			Microsoft-Workstation	192.168.1.3	fmc60.lab9.com
08:45	User Login	LAB	jeppich	LDAP	Passive Authentication	192.168.1.97		Employees	Microsoft-Workstation	192.168.1.3	fmc60.lab9.com
0:14	User Login	LAB	pxgrid	LDAP	Passive Authentication	192.168.1.13		Employees	Microsoft-Workstation	192.168.1.3	fmc60.lab9.com
38:48	User Logoff	LAB	jeppich	LDAP	Passive Authentication	192.168.1.13		Employees	Microsoft-Workstation	192.168.1.3	fmc60.lab9.com
48:23	User Login	Discovered Identities	jeppich	LDAP	No Authentication	192.168.1.13					192.168.1.31
47:23	User Login	LAB	jeppich	LDAP	Passive Authentication	192.168.1.13		Employees	Microsoft-Workstation	192.168.1.3	fmc60.lab9.com
43:30	User Login		18:E7:28:2E:29:CB	LDAP	Passive Authentication	192.168.1.6			Cisco-Device	192.168.1.3	fmc60.lab9.com
13:25	User Login		24:F9:B3:44:6D:0F	LDAP	Passive Authentication	192.168.1.69			Cisco-WLC-2500-Series	192.168.1.3	fmc60.lab9.com

Please note that only IEEE 802.1X user authentication usernames from ISE can be applied to a FMC 6.0 policy and must exist in the Firepower ISE realm. IEEE 802.1X machine authentication hostnames, or MAC address usernames cannot by applied to the FMC 6.0 policy.

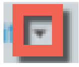
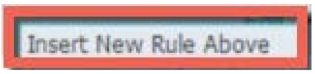
Cisco Identity Service Engine Dynamic Security Group Tags

Organizations security policies can be defined based on security group tags (SGT). This allows an organization to have uniform and global security policies across the network. If Cisco TrustSec is enabled on the organization switches, these security group tags can also be enforced on the network. Typically, security group tags of 2 are given to network devices such as switches, routers, and firewalls.

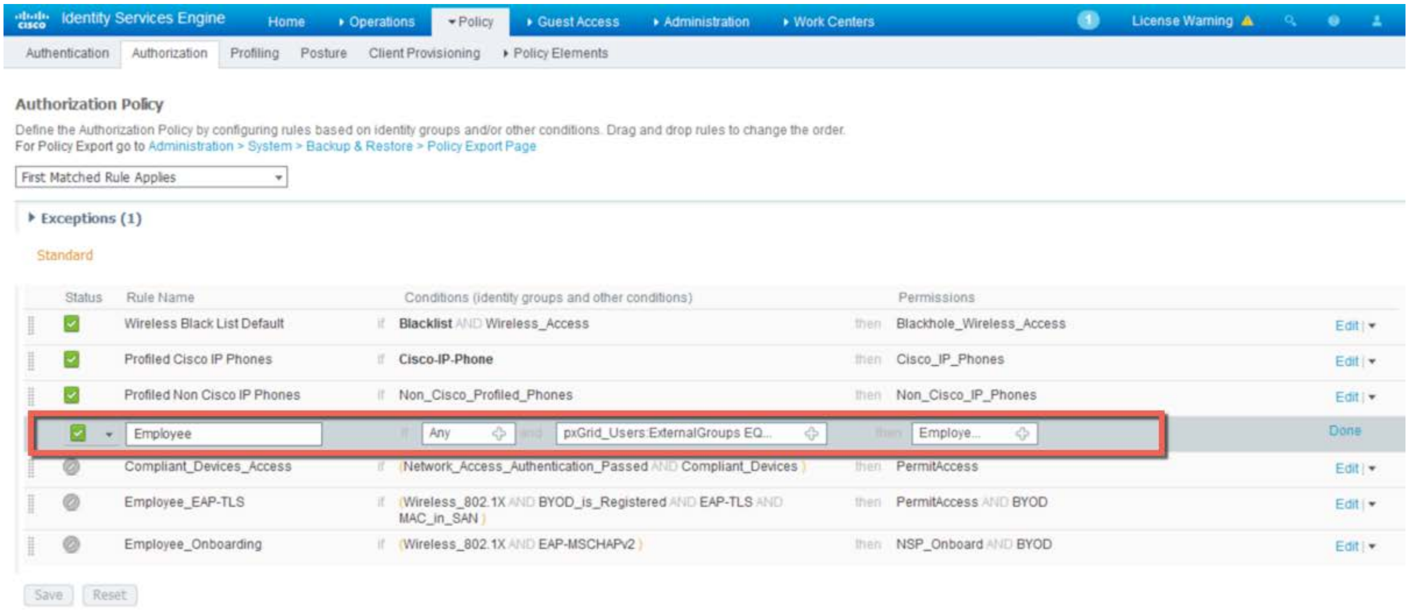
In this document, a dynamic SGT of “employee” will be assigned to successfully authenticated end-users belonging to the Windows user’s domain group. The SGT will then be applied to a Firepower Management access control rule that will be applied to and enforced by the Firepower NGIPS virtual sensor and ASA with Firepower services.

Please note that additional security group tags can be directly configured from the ISE authorization policy or directly from ISE via Work Center->TrustSec->Components->Security Groups menu.

Step 1 Create an Employee Security tag

Select Policy->Authorization->  ->  and enter the following:

Rule Name: Employee;
New Condition: External Groups:equals:pxGrid_Users
Authorization Profile(s): Employee and Permit Access



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

Exceptions (1)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
✓	Wireless Black List Default	if	Blacklist AND Wireless_Access	then	Blackhole_Wireless_Access	Edit | ▾
✓	Profiled Cisco IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phones	Edit | ▾
✓	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones	Edit | ▾
✓	Employee	if	Any and pxGrid_Users:ExternalGroups EQ...	then	Employe...	Done
⊘	Compliant_Devices_Access	if	(Network_Access_Authentication_Passed AND Compliant_Devices)	then	PermitAccess	Edit | ▾
⊘	Employee_EAP-TLS	if	(Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN)	then	PermitAccess AND BYOD	Edit | ▾
⊘	Employee_Onboarding	if	(Wireless_802.1X AND EAP-MSCHAPv2)	then	NSP_Onboard AND BYOD	Edit | ▾

Step 2 Select **Done**

Select **Save**

Self-Signed Certificate Operation

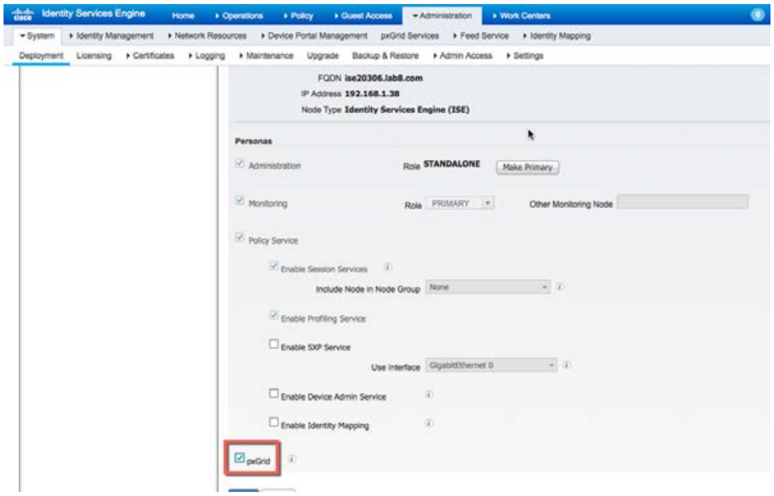
Self-signed certificate operation is used for POC environments only. This section is optional if you are deploying CA signed certificates.

Configuring ISE 2.0

Self-signed certificates are used in a POC environment. In this configuration ISE is deployed in standalone configuration.

Note: The ISE self-signed identity certificate is no longer required to be exported into the ISE certificate trusted store as in ISE 1.3 and ISE 1.4.

Step 1 Select **Administration->System->Deployment, select the node->Edit->enable pxGrid**



FQDN **ise20306.lab8.com**
IP Address **192.168.1.38**
Node Type **Identity Services Engine (ISE)**

Personas

☑ Administration Role **STANDALONE**

☑ Monitoring Role PRIMARY Other Monitoring Node

☑ Policy Service

☑ Enable Session Services

Include Node in Node Group None

☑ Enable Profiling Service

☐ Enable SXP Service

Use Interface GigabitEthernet 0

☐ Enable Device Admin Service

☐ Enable Identity Mapping

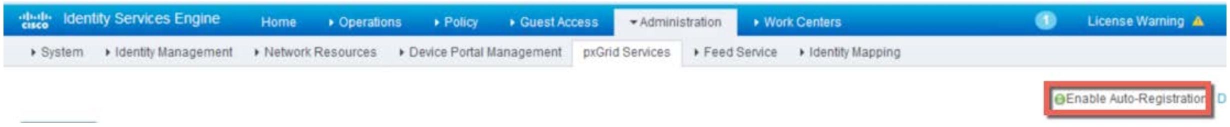
☑ pxGrid

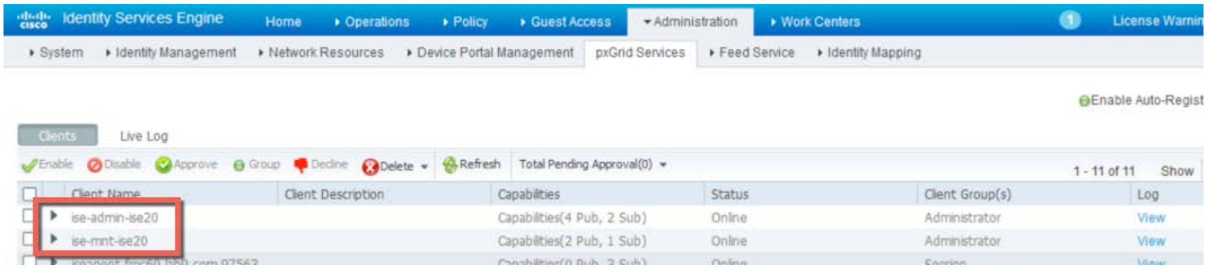
Step 2 Select **Save**

Step 3 Verify that the published nodes appear under pxGrid Services and there is connectivity. **Administration->pxGrid Services**

Note: The published nodes may take a while to appear. Verify that pxGrid services have started by running: **sh application status ise** on the ISE VM node.

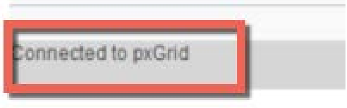
Step 4 Enable **Enable Auto-Registration**





Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
ise-admin-ise20		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
ise-mnt-ise20		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
iseagent-fmc60.lab9.com-97563		Capabilities(0 Pub, 2 Sub)	Online	Session	View

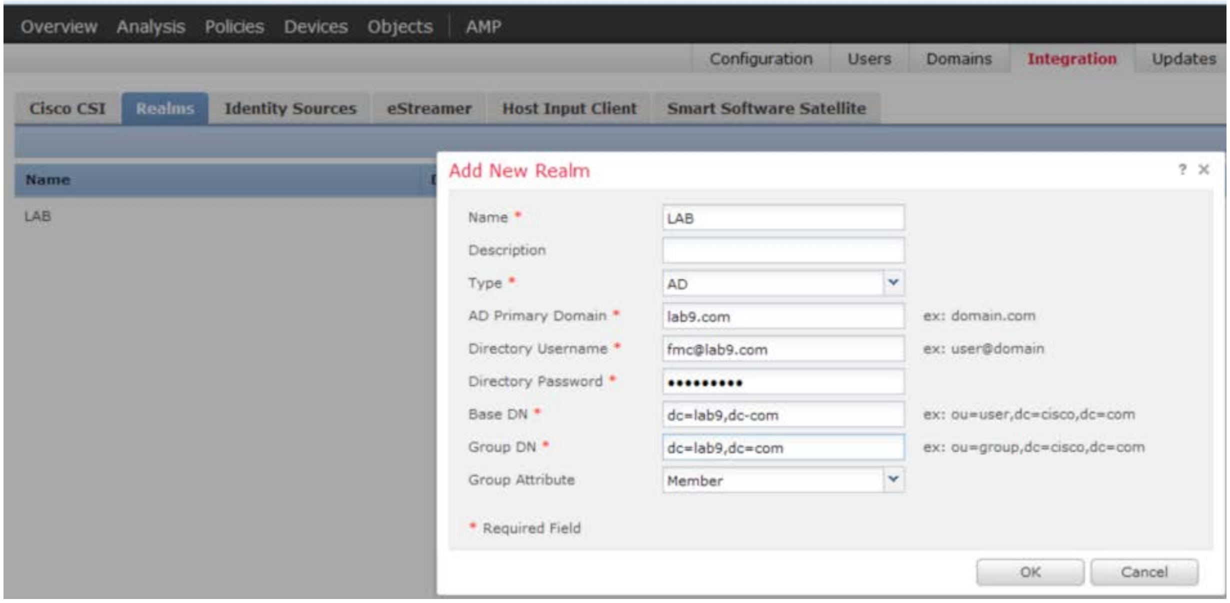
Step 5 Verify that you are **connected to pxGrid**


Connected to pxGrid

Creating Firepower ISE Realm

The ISE Realm is used for ISE authentication and will be used in the Firepower Management Center’s 6.0 Identity Policy.

Step 1 Select **System->Integration->Realms->New Realm**



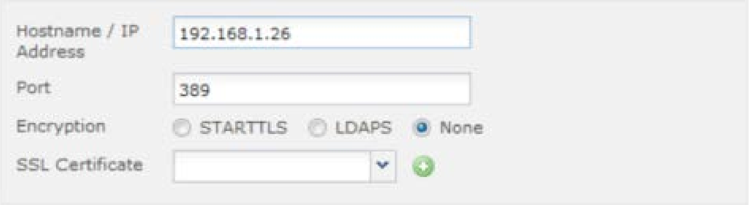
Add New Realm

Name *	LAB	
Description		
Type *	AD	
AD Primary Domain *	lab9.com	ex: domain.com
Directory Username *	fmc@lab9.com	ex: user@domain
Directory Password *	•••••••••	
Base DN *	dc=lab9,dc-com	ex: ou=user,dc=cisco,dc=com
Group DN *	dc=lab9,dc=com	ex: ou=group,dc=cisco,dc=com
Group Attribute	Member	

* Required Field

Step 2 Select **OK**

Step 3 Select **Add Directory,** enter the FQDN hostname or information



Hostname / IP Address	192.168.1.26
Port	389
Encryption	○ STARTTLS ○ LDAPS ● None
SSL Certificate	

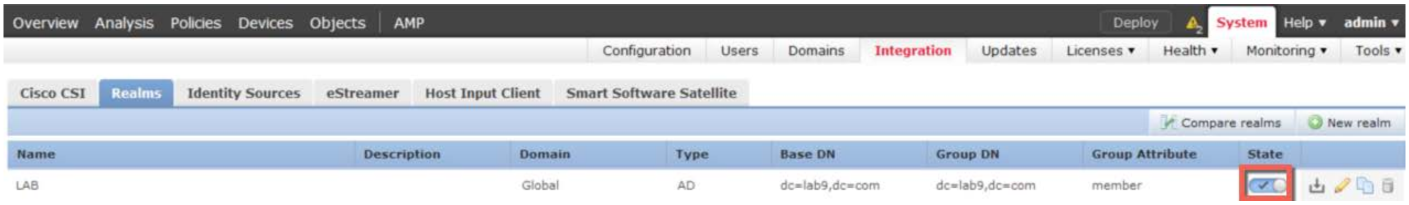
Step 4 Select **Test,** you should see that the: **Test Connection has succeeded,** select **OK**

Note: If you see a returned failed attempt, ensure that the directory username and directory password are correct in the Realm Configuration.

Step 5 Select **OK**

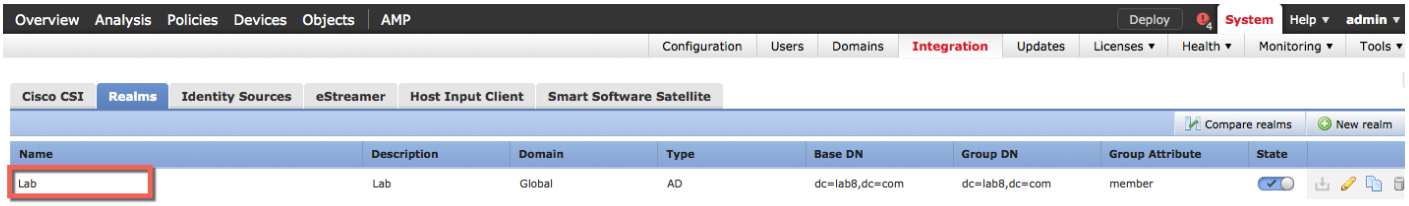
Step 6 Select **Save**

Step 7 Enable the state by selecting



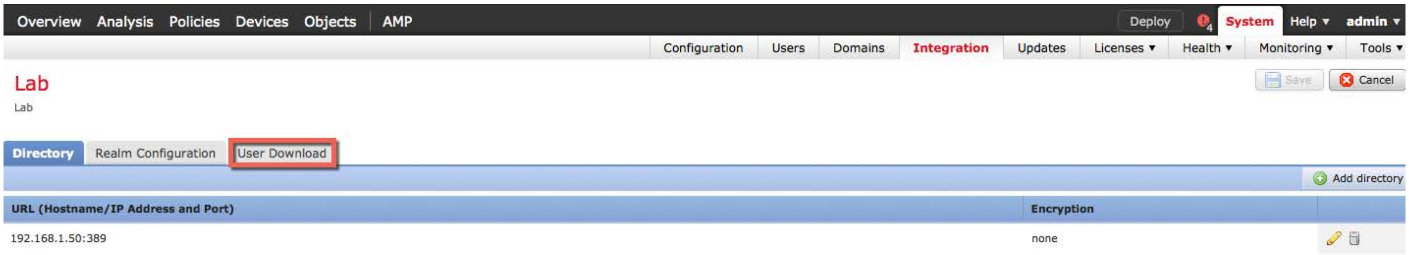
Name	Description	Domain	Type	Base DN	Group DN	Group Attribute	State
LAB		Global	AD	dc=lab9,dc=com	dc=lab9,dc=com	member	✓

Step 8 Click->**Realm name**



Name	Description	Domain	Type	Base DN	Group DN	Group Attribute	State
Lab	Lab	Global	AD	dc=lab8,dc=com	dc=lab8,dc=com	member	✓

Step 9 Click->**User Download**



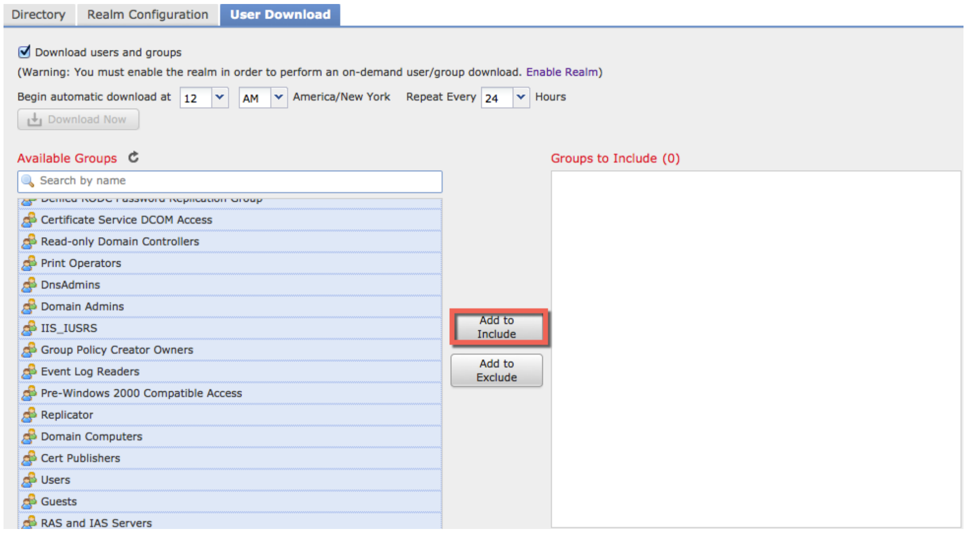
Lab

Lab

URL (Hostname/IP Address and Port)	Encryption
192.168.1.50:389	none

Step 10 Enable **Download users and groups**

Step 11 Highlight all Available Groups select **Add to Include**



☑ Download users and groups

(Warning: You must enable the realm in order to perform an on-demand user/group download. Enable Realm)

Begin automatic download at 12 AM America/New York Repeat Every 24 Hours

Available Groups

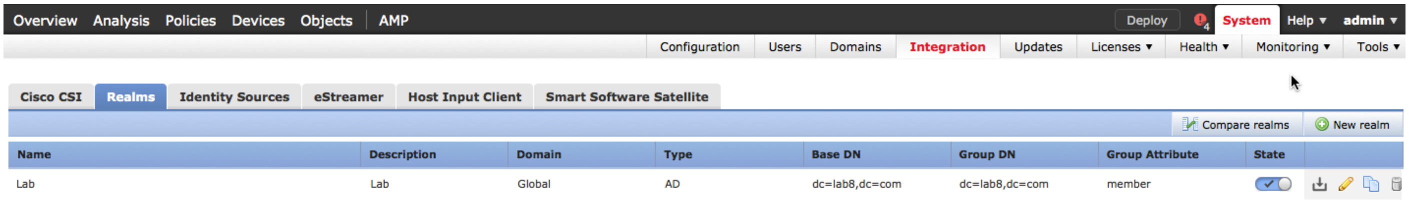
Search by name

- Denied RODC Password Replication Group
- Certificate Service DCOM Access
- Read-only Domain Controllers
- Print Operators
- DnsAdmins
- Domain Admins
- IIS_IUSRS
- Group Policy Creator Owners
- Event Log Readers
- Pre-Windows 2000 Compatible Access
- Replicator
- Domain Computers
- Cert Publishers
- Users
- Guests
- RAS and IAS Servers

Groups to Include (0)

Step 12 Select **Save**

Step 13 You should see the following:

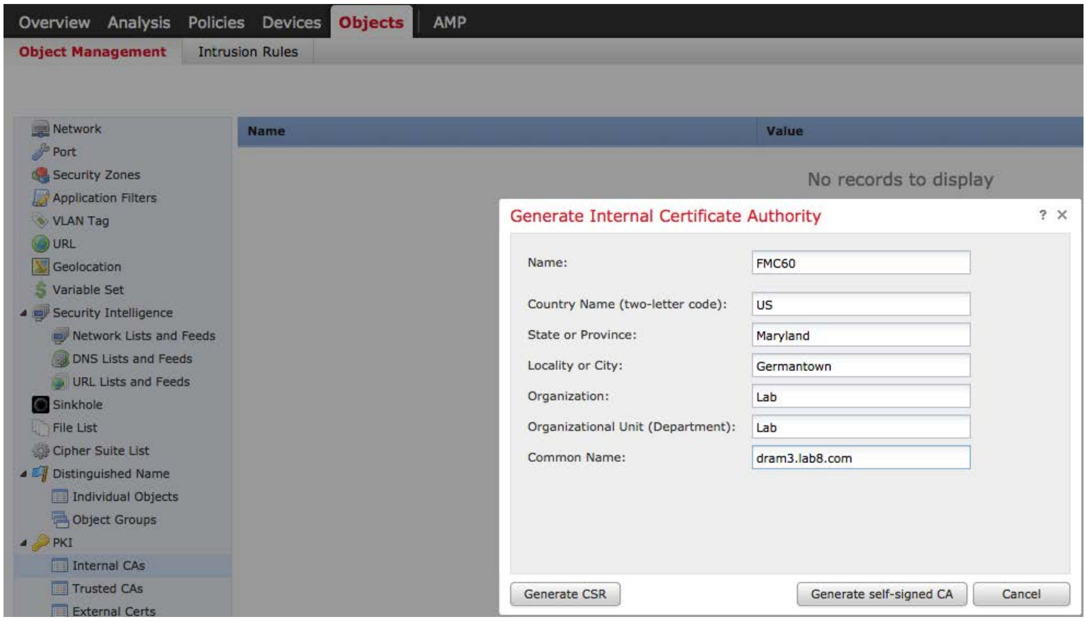


Name	Description	Domain	Type	Base DN	Group DN	Group Attribute	State
Lab	Lab	Global	AD	dc=lab8,dc=com	dc=lab8,dc=com	member	

Configuring Firepower Management Center 6.0

In this section, the Firepower Management Center (FMC) is configured for using self-signed certificates for ISE pxGrid node operation. An internal FMC certificate authority is created on the Firepower Management Center and converted into certificate and imported into the Firepower Management Center's internal certificate 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 Firepower Management Center Trusted CA store.

Step 1 Select **Objects->Object Management->PKI->Internal CAs->Generate CA->** provide the certification information below:
In this example, FMC60, was the name given to the internal CA

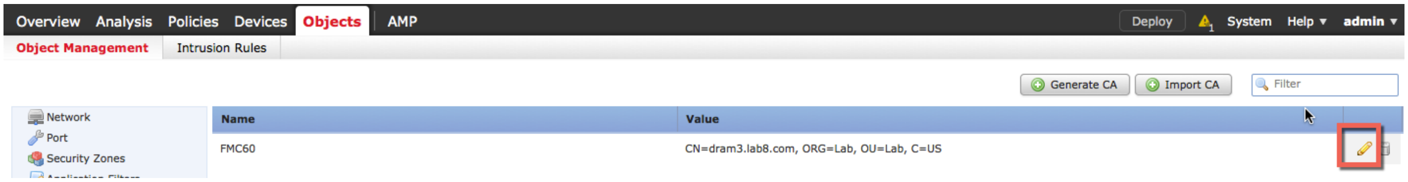


Generate Internal Certificate Authority

Name:	FMC60
Country Name (two-letter code):	US
State or Province:	Maryland
Locality or City:	Germantown
Organization:	Lab
Organizational Unit (Department):	Lab
Common Name:	dram3.lab8.com

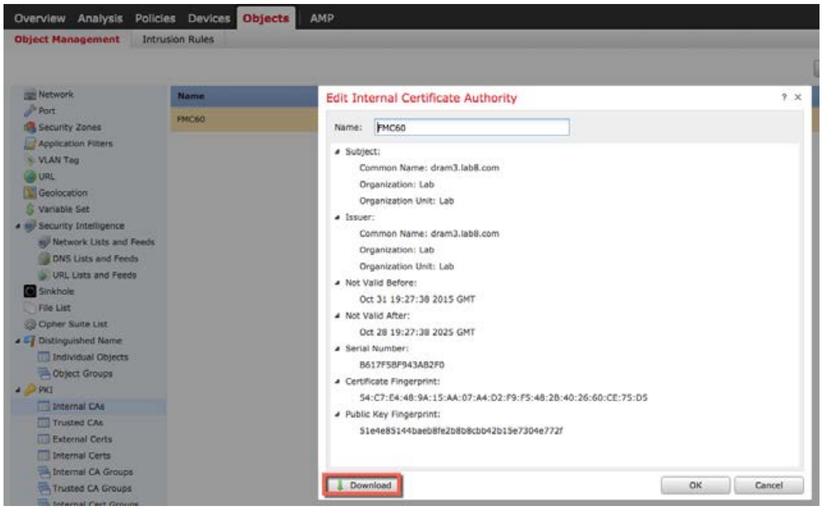
Step 2 Select **Generate self-signed CA**

Step 3 Download the CA certificate file by clicking on the “pencil” below



Name	Value
FMC60	CN=dram3.lab8.com, ORG=Lab, OU=Lab, C=US

Step 4 Select **Download**

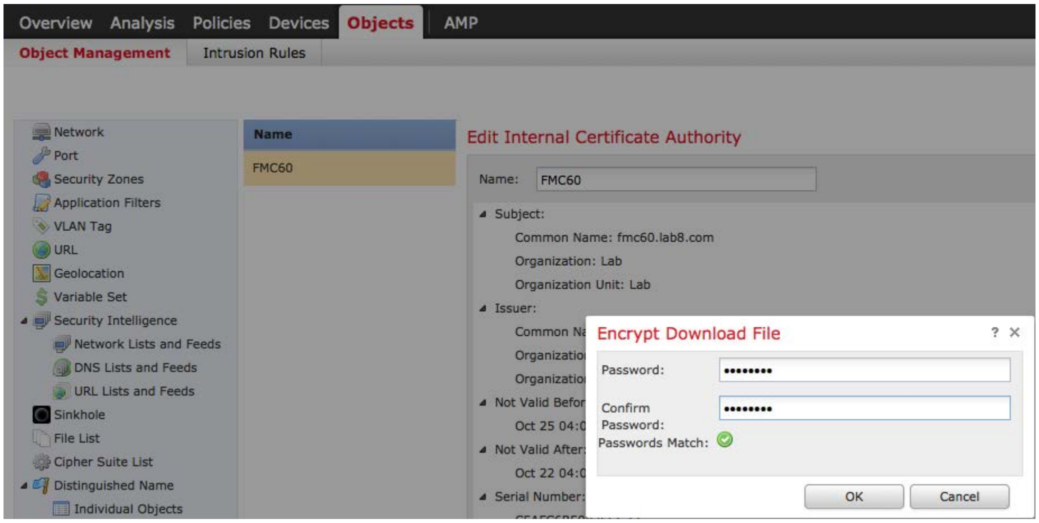


Edit Internal Certificate Authority

Name: FMC60

- Subject:
  - Common Name: dram3.lab8.com
  - Organization: Lab
  - Organization Unit: Lab
- Issuer:
  - Common Name: dram3.lab8.com
  - Organization: Lab
  - Organization Unit: Lab
- Not Valid Before:
  - Oct 31 19:27:38 2015 GMT
- Not Valid After:
  - Oct 28 19:27:38 2025 GMT
- Serial Number:
  - B617F5BF943AB2F0
- Certificate Fingerprint:
  - 54:C7:E4:48:9A:15:AA:07:A4:D2:F9:F5:48:2B:40:26:60:CE:75:D5
- Public Key Fingerprint:
  - 51e4e85144baeb8fe2b8b8cbb42b15e7304e772f

Step 5 Enter encryption password, select **OK**. In this example, cisco123 was used



Edit Internal Certificate Authority

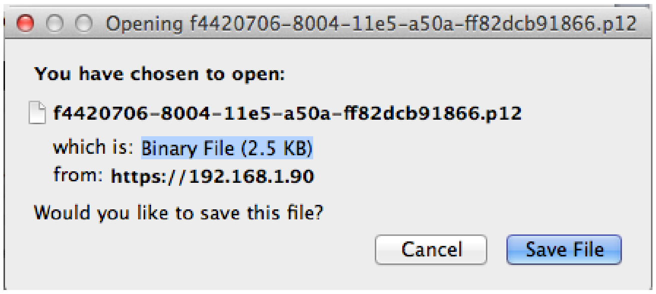
Name: FMC60

Subject:
Common Name: fmc60.lab8.com
Organization: Lab
Organization Unit: Lab
Issuer:
Common Na
Organizatio
Organizatio
Not Valid Befor
Oct 25 04:0
Not Valid After
Oct 22 04:0
Serial Number:

Encrypt Download File

Password: ••••••••
Confirm Password: ••••••••
Passwords Match: ✓

Step 6 Save the .p12 file locally



Opening f4420706-8004-11e5-a50a-ff82dcb91866.p12

You have chosen to open:

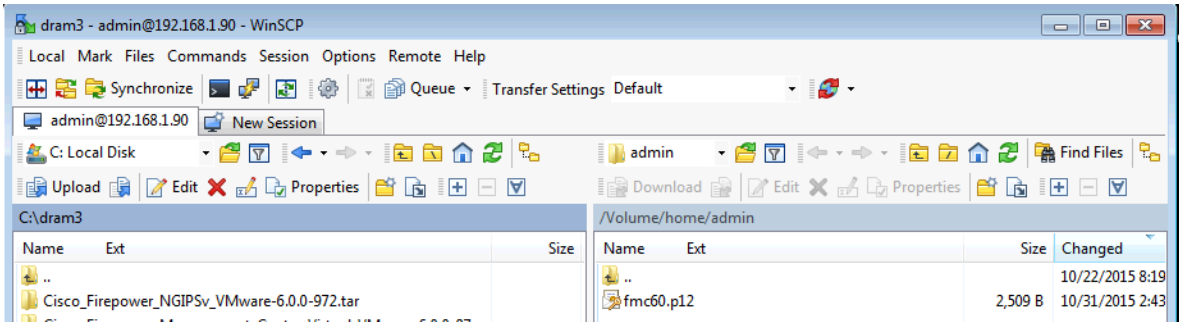
f4420706-8004-11e5-a50a-ff82dcb91866.p12

which is: Binary File (2.5 KB)
from: **https://192.168.1.90**

Would you like to save this file?

Step 7 Rename the .p12 filename to make it easier to work with. In this example, fmc60.p12 was the renamed file.

Step 8 Use WinSCP or another method to upload the file to the Firepower Management Console



dram3 - admin@192.168.1.90 - WinSCP

C:\dram3

Name	Ext	Size
..		
Cisco_Firepower_NGIPSv_VMware-6.0.0-972.tar		

/Volume/home/admin

Name	Ext	Size	Changed
..			10/22/2015 8:19
fmc60.p12		2,509 B	10/31/2015 2:43

Step 9 SSH to the Firepower Management Console

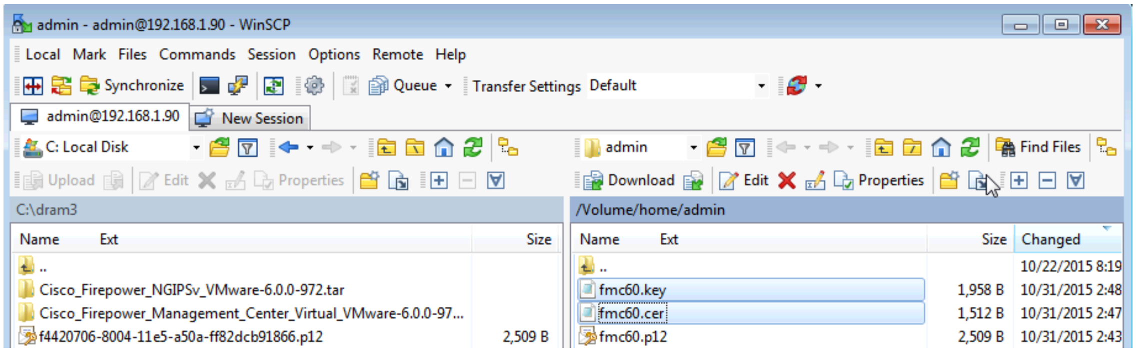
Step 10 Convert the .p12 file into CER and KEY files, by typing the following commands:

Note: the CER and KEY filenames are random. The original.p12 file was renamed to fmc60.p12. Initially you will be prompted for the sudo password. The import password, PEM passphrase will be the encryption key password you typed in earlier.

```
sudo openssl pkcs12 -nokeys -clcerts -in fmc60.p12 -out fmc60.cer
Enter Import Password:
MAC verified OK
admin@sd:~$


sudo openssl pkcs12 -nocerts -in fmc60.p12 -out fmc601.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 fmc60.cer and fmc60.key files from the Firepower Management Center to the local PC.



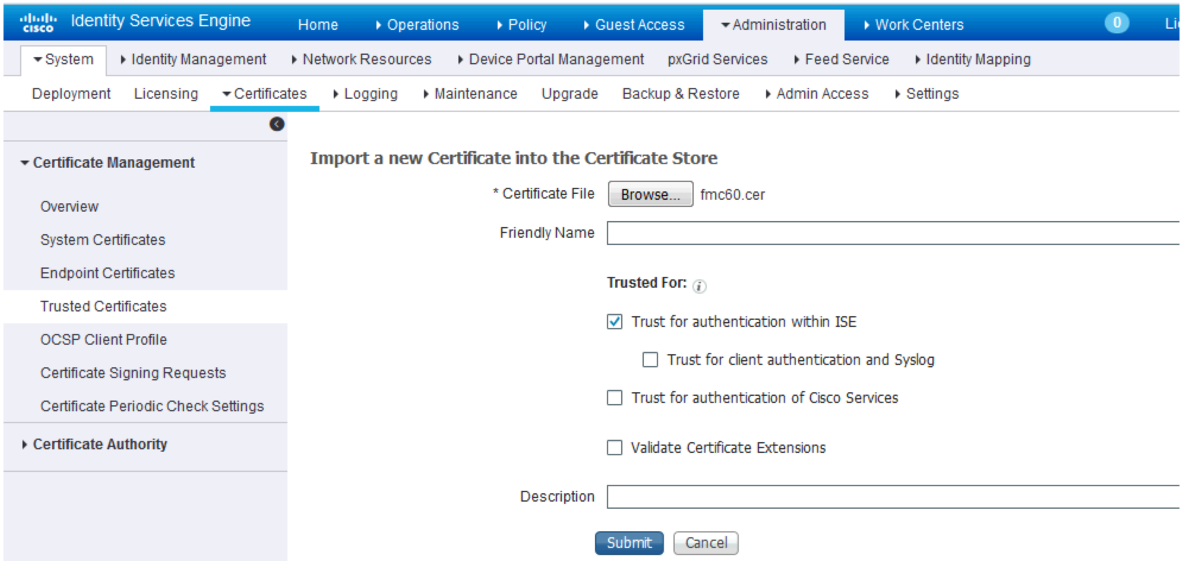
C:\dram3

Name	Ext	Size
..		
Cisco_Firepower_NGIPSv_VMware-6.0.0-972.tar		
Cisco_Firepower_Management_Center_Virtual_VMware-6.0.0-97...		
f4420706-8004-11e5-a50a-ff82dcb91866.p12		2,509 B

/Volume/home/admin

Name	Ext	Size	Changed
..			10/22/2015 8:19
fmc60.key		1,958 B	10/31/2015 2:48
fmc60.cer		1,512 B	10/31/2015 2:47
fmc60.p12		2,509 B	10/31/2015 2:43

Step 12 The Firepower Management internal CA public certificate was exported into the ISE certificate trust store Select->**Administration->System->Certificates->Trusted Certificates->Browse** and upload fmc60.cer



Import a new Certificate into the Certificate Store

* Certificate File Browse... fmc60.cer

Friendly Name

Trusted For:

☑ Trust for authentication within ISE

□ Trust for client authentication and Syslog

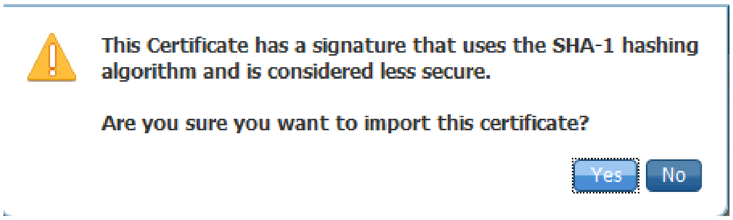
□ Trust for authentication of Cisco Services

□ Validate Certificate Extensions

Description

Step 13 Enable “Trust for authentication within ISE”, then **Submit**

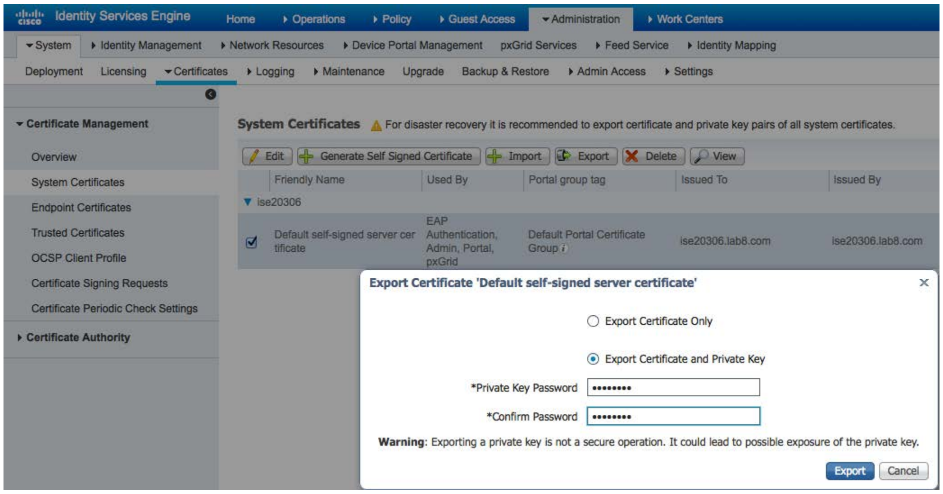
Step 14 You will see the following when importing the FMC certificate, select **Yes**



This Certificate has a signature that uses the SHA-1 hashing algorithm and is considered less secure.

Are you sure you want to import this certificate?

Step 15 Select **Administration->System->Certificates->select the ISE identity self-signed certificates->Export** both public and private key



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

	Friendly Name	Used By	Portal group tag	Issued To	Issued By
▼ ise20306					
☑	Default self-signed server certificate	EAP Authentication, Admin, Portal, pxGrid	Default Portal Certificate Group	ise20306.lab8.com	ise20306.lab8.com

Export Certificate 'Default self-signed server certificate'

○ Export Certificate Only

● Export Certificate and Private Key

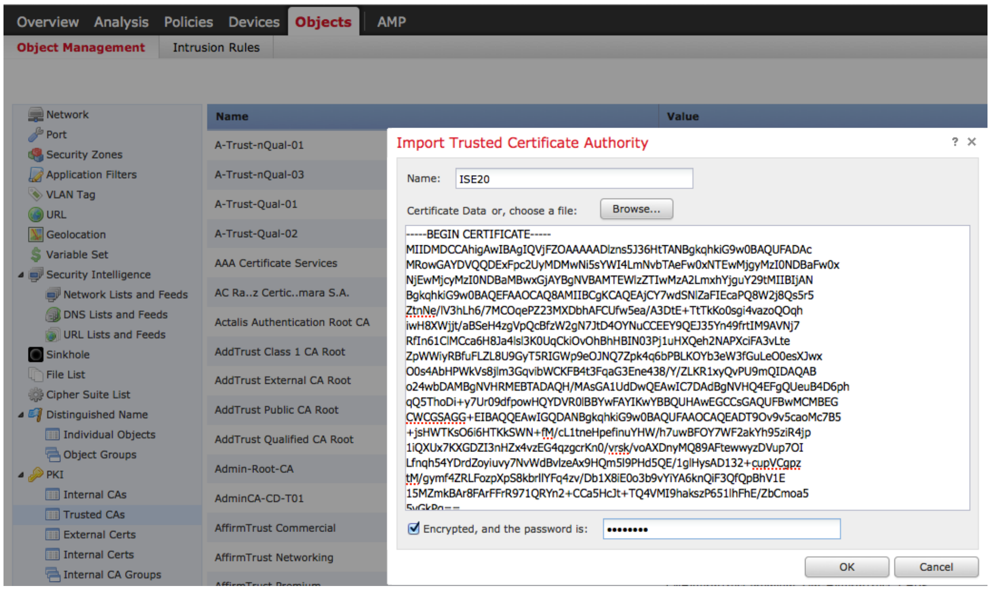
*Private Key Password ••••••••

*Confirm Password ••••••••

Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.

Note: The file will be saved as Defaultserversignedcerti.zip file. Unzip the file and export only the public certificate the PEM file to the FMC trusted store. You can also rename the file to ISE2.0.pem to make it easier to work with.

Step 16 Import the ISE self-signed identity cert into the Firepower Management trusted CA store
Select **Objects->Object Management->PKI->Trusted CAs->Add Trusted CA->**enter the name. In this example, ISE was used.
Enter the encryption key password for ISE ->**OK**



Name	Value
A-Trust-nQual-01	
A-Trust-nQual-03	
A-Trust-Qual-01	
A-Trust-Qual-02	
AAA Certificate Services	
AC Ra..z Certic..mara S.A.	
Actalis Authentication Root CA	
AddTrust Class 1 CA Root	
AddTrust External CA Root	
AddTrust Public CA Root	
AddTrust Qualified CA Root	
Admin-Root-CA	
AdminCA-CD-T01	
AffirmTrust Commercial	
AffirmTrust Networking	

Import Trusted Certificate Authority

Name: ISE20

Certificate Data or, choose a file: Browse...

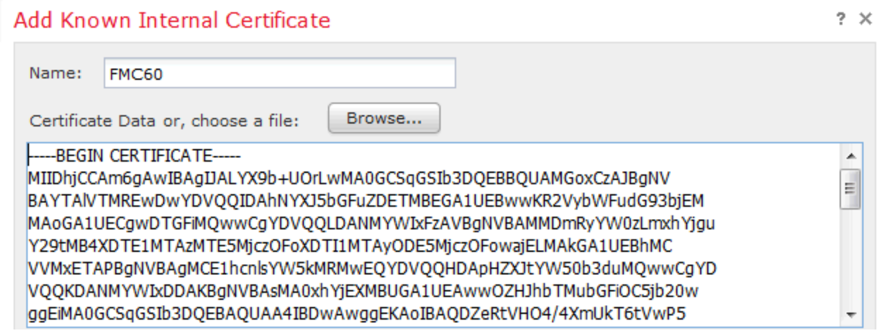
```
-----BEGIN CERTIFICATE-----
MIIDMDCCAhigAwIBAgIQVjFZOAAAAADlzns5J36HtTANBgkqhkiG9w0BAQUFADAc
MRowGAYDVQQDExFpc2UyMDMwNi5sYWI4LmNvbTAeFw0xNTEwMjgyMzI0NDBaFw0x
NjEwMjcyMzI0NDBaMBwxGjAYBgNVBAMTEWlzZTIwMzA2LmxhYjguY29tMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAjCY7wdSNlZaFIEcaPQ8W2j8Qs5r5
ZtnNe/lV3hLh6/7MCOqePZ23MXDbhAFCUfw5ea/A3DtE+TtTkKo0sgi4vazoQOqh
iwH8XWjjt/aBSeH4zgVpQcBfzW2gN7JtD4OYNuCCEEY9QEJ35Yn49frtIM9AVNj7
RfIn61ClMCca6H8Ja4lsl3K0UqCkiOvOhBhHBIN03Pj1uHXQeh2NAPXciFA3vLte
ZpWWiyRBfuFLZL8U9GyT5RIGWp9eOJNQ7Zpk4q6bPBLKOYb3eW3fGuLeO0esXJwx
O0s4AbHPWkVs8jlm3GqvibWCKFB4t3FqaG3Ene438/Y/ZLKR1xyQvPU9mQIDAQAB
o24wbDAMBgNVHRMEBTADAQH/MAsGA1UdDwQEAwIC7DAdBgNVHQ4EFgQUeuB4D6ph
qQ5ThoDi+y7Ur09dfpowHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMBEG
CWCGSAGG+EIBAQQEAwIGQDANBgkqhkiG9w0BAQUFAAOCAQEADT9Ov9v5caoMc7B5
+jsHWTKsO6i6HTKkSWN+fM/cL1tneHpefinuYHW/h7uwBFOY7WF2akYh95ziR4jp
1iQXUx7KXGDZI3nHZx4vzEG4qzgcrKn0/vrsk/voAXDnyMQ89AFtewwyzDVup7OI
Lfnqh54YDrdZoyiuvy7NvWdBvlzeAx9HQm5l9PHd5QE/1glHysAD132+cupVCgpz
tM/gymf4ZRLFozpXpS8kbrllYFq4zv/Db1X8iE0o3b9vYiYA6knQiF3QfQpBhV1E
15MZmkBAr8FArFFrR971QRYn2+CCa5HcJt+TQ4VMI9hakszP651lhFhE/ZbCmoa5
5vGkPg==
```

☑ Encrypted, and the password is: ••••••••

OK Cancel

Step 17 Import the Firepower Management internal CA public/private key pair into the Firepower Management Center's Internal Certs store
Select **Objects->PKI->Internal Certs->Add Internal Cert**
Follow the same procedure for the private key

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

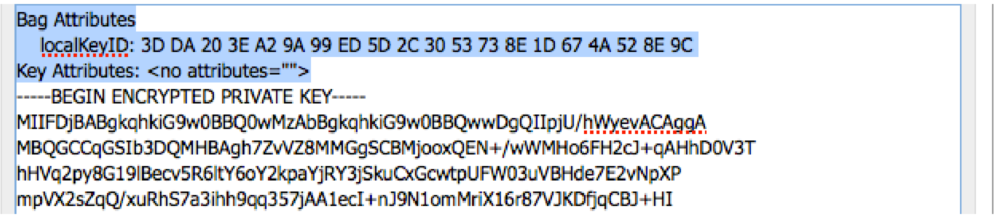

Add Known Internal Certificate

Name: FMC60

Certificate Data or, choose a file: Browse...

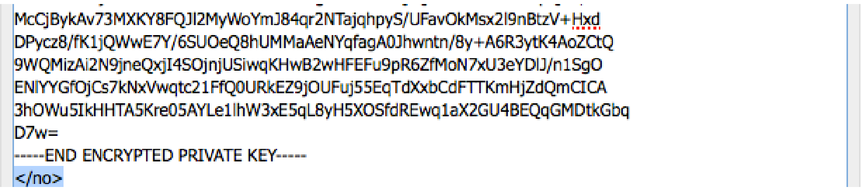
```
-----BEGIN CERTIFICATE-----
MIIDhjCCAm6gAwIBAgIJALYX9b+UOrLwMA0GCSqGSIb3DQEBBQUAMGoxCzAJBgNV
BAYTAlVTMREwDwYDVQQIDAhNYXJ5bGFuZDETMBEGA1UEBwwKR2VybWFudG93bjEM
MAoGA1UECgwDTGFiMQwwCgYDVQQLDANMYWIxFzAVBgNVBAMMDmRyYW0zLmxhYjgu
Y29tMB4XDTE1MTAzMTE5MjczOFoXDTI1MTAyODE5MjczOFowajELMAkGA1UEBhMC
VVMxETAPBgNVBAgMCE1hcnlsYW5kMRMwEQYDVQQHDApHZXJtYW50b3duMQwwCgYD
VQQKDANMYWIxDDAKBgNVBAsMA0xhYjEXMBUGA1UEAwwOZHJhbTMubGFiOC5jb20w
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDZeRtVHO4/4XmUkT6tVwP5
```

Step 18 Delete the Bag attributes for the key file until you are just before “---Begin….”



```
Bag Attributes
    localKeyID: 3D DA 20 3E A2 9A 99 ED 5D 2C 30 53 73 8E 1D 67 4A 52 8E 9C
Key Attributes: <no attributes="">
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIIpjU/hWyevACAggA
MBQGCCqGSIb3DQMHBAgh7ZvVZ8MMGgSCBMjooxQEN+/wWMHo6FH2cJ+qAHhD0V3T
hHVq2py8G19lBecv5R6ltY6oY2kpaYjRY3jSkuCxGcwtpUFW03uVBHde7E2vNpXP
mpVX2sZqQ/xuRhS7a3ihh9qq357jAA1ecI+nJ9N1omMriX16r87VJKDfjqCBJ+HI
```

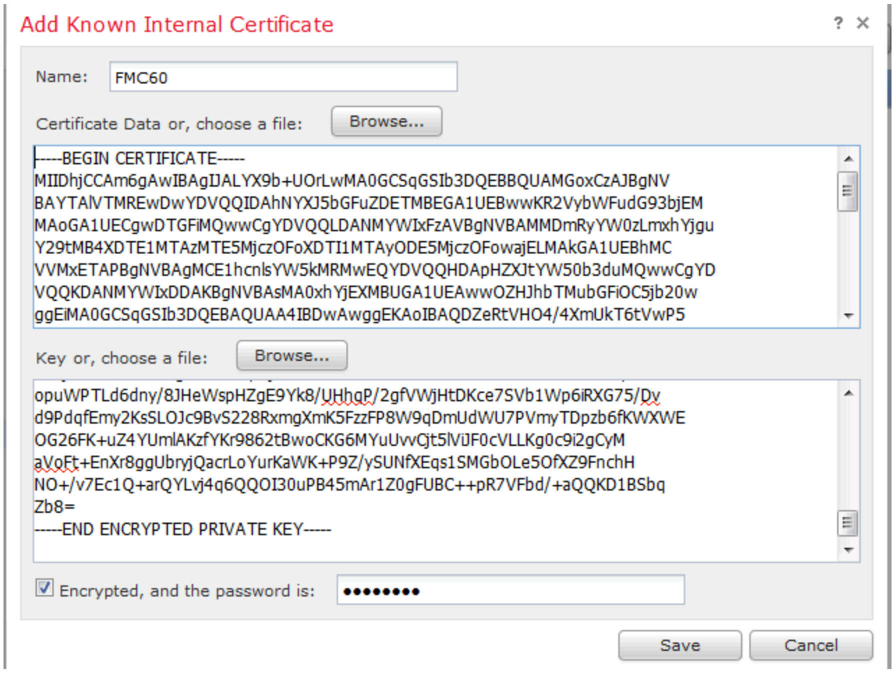
Step 19 Also delete </no>



```
McCjBykAv73MXKY8FQJl2MyWoYmJ84qr2NTajqhpyS/UFavOkMsx2l9nBtzV+Hxd
DPycz8/fK1jQWwE7Y/6SUOeQ8hUMMaAeNYqfagA0Jhwntn/8y+A6R3ytK4AoZCtQ
9WQMizAi2N9jneQxjI4SOjnjUSiwqKHwB2wHFEFu9pR6ZfMoN7xU3eYDlJ/n1SgO
ENlYYGfOjCs7kNxVwqtc21FfQ0URkEZ9jOUFuj55EqTdXxbCdFTTKmHjZdQmCICA
3hOWu5IkHHTA5Kre05AYLe1lhW3xE5qL8yH5XOSfdREwq1aX2GU4BEQqGMDtkGbq
D7w=
-----END ENCRYPTED PRIVATE KEY-----
</no>
```

Step 20 Enter the encrypted password

Step 21 You should see the following:



Name: FMC60

Certificate Data or, choose a file:

```
-----BEGIN CERTIFICATE-----
MIIDhjCCAm6gAwIBAgIJALYX9b+UOrLwMA0GCSqGSIb3DQEBBQUAMGoxCzAJBgNV
BAYTAlVTMREwDwYDVQQIDAhNYXJ5bGFuZDETMBEGA1UEBwwKR2VybWFudG93bjEM
MAoGA1UECgwDTGFiMQwwCgYDVQQLDANMYWIxFzAVBgNVBAMMDmRyYW0zLmxhYjgu
Y29tMB4XDTE1MTAzMTE5MjczOFoXDTI1MTAyODE5MjczOFowajELMAkGA1UEBhMC
VVMxETAPBgNVBAgMCE1hcnlsYW5kMRMwEQYDVQQHDApHZXJtYW50b3duMQwwCgYD
VQQKDANMYWIxDDAKBgNVBAsMA0xhYjEXMBUGA1UEAwwOZHJhbTMubGFiOC5jb20w
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDZeRtVHO4/4XmUkT6tVwP5
```

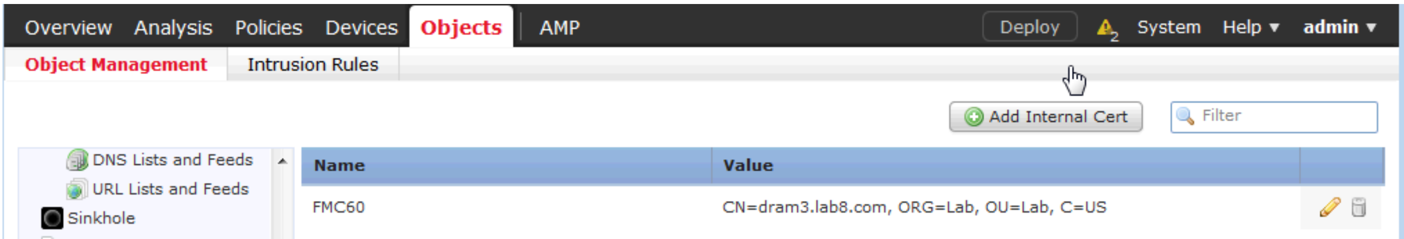
Key or, choose a file:

```
opuWPTLd6dny/8JHeWspHZgE9Yk8/UHhqP/2gfVWjHtDKce7SVb1Wp6iRXG75/Dv
d9PdqfEmy2KsSLOJc9BvS228RxmgXmK5FzzFP8W9qDmUdWU7PVmyTDpzb6fKWXWE
OG26FK+uZ4YUmlAKzfYKr9862tBwoCKG6MYuUvvCjt5lViJF0cVLLKg0c9i2gCyM
aVoFt+EnXr8ggUbryjQacrLoYurKaWK+P9Z/ySUNfXEqs1SMGbOLe5OfXZ9FnchH
NO+/v7Ec1Q+arQYLvj4q6QQOI30uPB45mAr1Z0gFUBC++pR7VFbd/+aQQKD1BSbq
Zb8=
-----END ENCRYPTED PRIVATE KEY-----
```

☑ Encrypted, and the password is: ●●●●●●●●●

Step 22 Select **Save**

You should see the following:



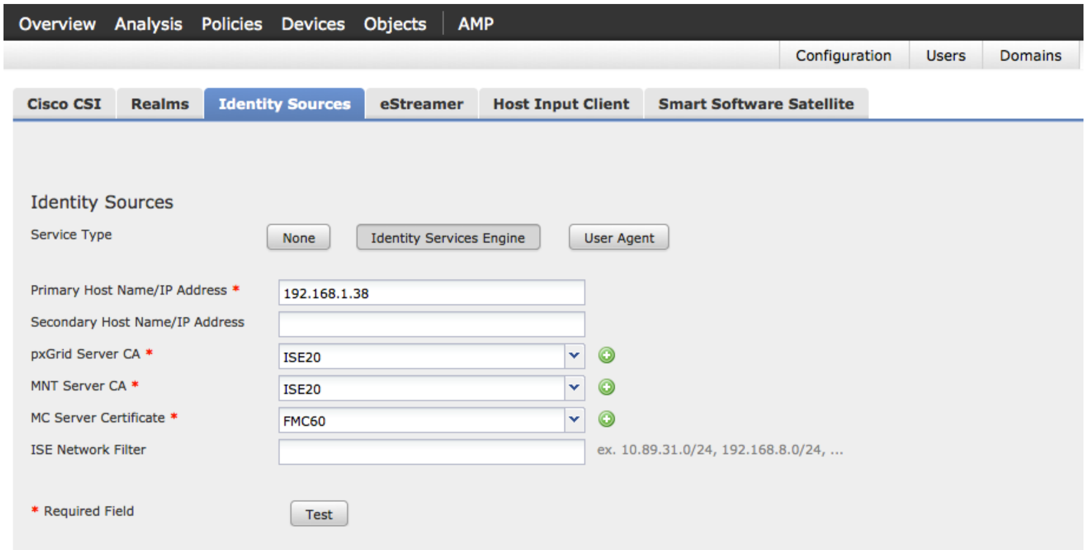
Name	Value
FMC60	CN=dram3.lab8.com, ORG=Lab, OU=Lab, C=US

Configuring Firepower ISE Identity Sources

The Identity Sources Engine configuration defines the ISE pxGrid node connection parameters, ISE MnT node certificates and FMC 6.0 identity certificate.

Step 1 Select **System->Integration->Identity Sources->Identity Services Engine**

Primary Host Name/IP Address- primary FQDN pxGrid name or IP address
Secondary Host Name/IP address- secondary FQDN pxGrid name or IP address
**pxGrid Server CA*- ISE pxGrid node certificate (imported ISE self-signed identity certificate)
**mnt Server CA*- ISE pxGrid node certificate (imported ISE self-signed identity certificate)
MC Server Certificate- identity certificate of FMC (imported internal cert)



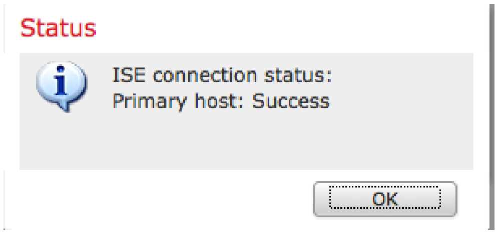
Identity Sources

Service Type: Identity Services Engine

Primary Host Name/IP Address *: 192.168.1.38
Secondary Host Name/IP Address:
pxGrid Server CA *: ISE20
MNT Server CA *: ISE20
MC Server Certificate *: FMC60
ISE Network Filter: ex. 10.89.31.0/24, 192.168.8.0/24, ...

* Required Field

Step 2 Select **Test**
You should see the following



Status

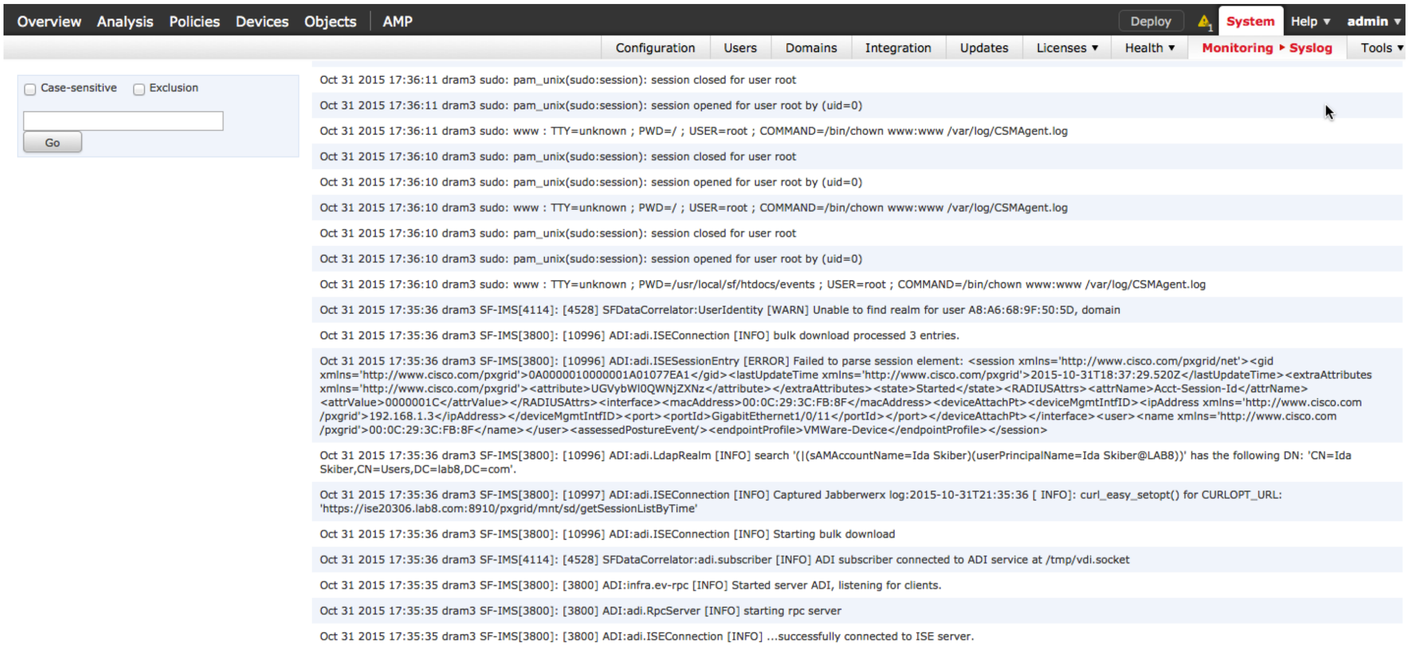
ISE connection status:
Primary host: Success

Step 3 Select **OK**

Step 4 Select **Save**

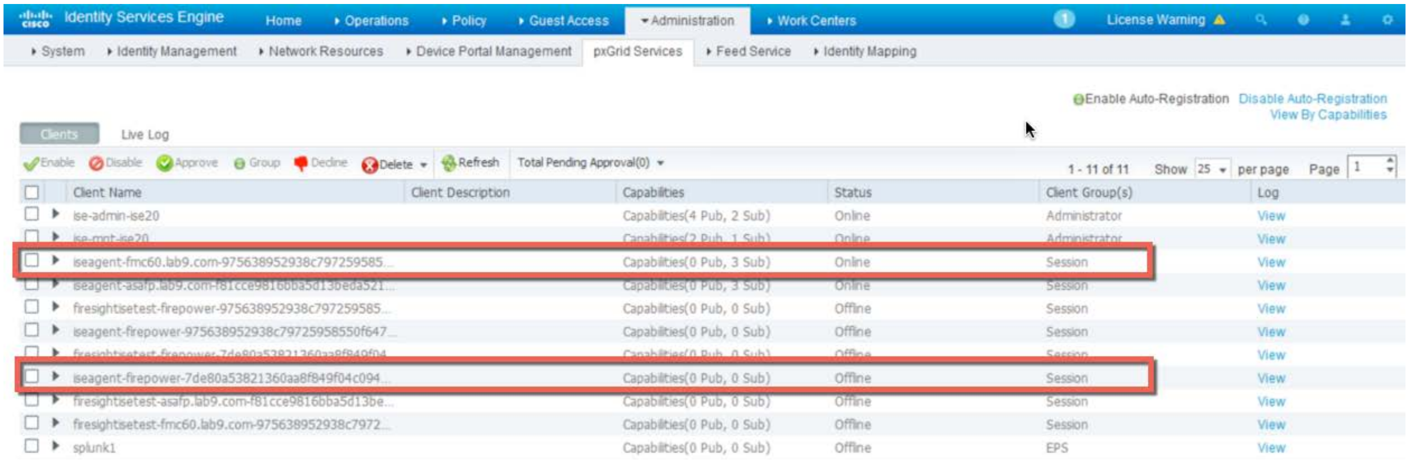
Step 5 Select **System->Monitoring->Syslog**

Note the FMC has successfully connected to the ISE server



```
Oct 31 2015 17:36:11 dram3 sudo: pam_unix(sudo:session): session closed for user root
Oct 31 2015 17:36:11 dram3 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Oct 31 2015 17:36:11 dram3 sudo: www : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/bin/chown www:www /var/log/CSMAgent.log
Oct 31 2015 17:36:10 dram3 sudo: pam_unix(sudo:session): session closed for user root
Oct 31 2015 17:36:10 dram3 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Oct 31 2015 17:36:10 dram3 sudo: www : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/bin/chown www:www /var/log/CSMAgent.log
Oct 31 2015 17:36:10 dram3 sudo: pam_unix(sudo:session): session closed for user root
Oct 31 2015 17:36:10 dram3 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Oct 31 2015 17:36:10 dram3 sudo: www : TTY=unknown ; PWD=/usr/local/sf/htdocs/events ; USER=root ; COMMAND=/bin/chown www:www /var/log/CSMAgent.log
Oct 31 2015 17:35:36 dram3 SF-IMS[4114]: [4528] SFDataCorrelator:UserIdentity [WARN] Unable to find realm for user A8:A6:68:9F:50:5D, domain
Oct 31 2015 17:35:36 dram3 SF-IMS[3800]: [10996] ADI:adi.ISEConnection [INFO] bulk download processed 3 entries.
Oct 31 2015 17:35:36 dram3 SF-IMS[3800]: [10996] ADI:adi.ISESessionEntry [ERROR] Failed to parse session element: <session xmlns='http://www.cisco.com/pxgrid/net'><gid
xmlns='http://www.cisco.com/pxgrid'>0A0000010000001A01077EA1</gid><lastUpdateTime xmlns='http://www.cisco.com/pxgrid'>2015-10-31T18:37:29.520Z</lastUpdateTime><extraAttributes
xmlns='http://www.cisco.com/pxgrid'><attribute>UGVybWl0QWNjZXNz</attribute></extraAttributes><state>Started</state><RADIUSAttrs><attrName>Acct-Session-Id</attrName>
<attrValue>0000001C</attrValue></RADIUSAttrs><interface><macAddress>00:0C:29:3C:FB:8F</macAddress><deviceAttachPt><deviceMgmtIntfID><ipAddress xmlns='http://www.cisco.com
/pxgrid'>192.168.1.3</ipAddress></deviceMgmtIntfID><port><portId>GigabitEthernet1/0/11</portId></port></deviceAttachPt></interface><user><name xmlns='http://www.cisco.com
/pxgrid'>00:0C:29:3C:FB:8F</name></user><assessedPostureEvent/><endpointProfile>VMWare-Device</endpointProfile></session>
Oct 31 2015 17:35:36 dram3 SF-IMS[3800]: [10996] ADI:adi.LdapRealm [INFO] search '(|(sAMAccountName=Ida Skiber)(userPrincipalName=Ida Skiber@LAB8))' has the following DN: 'CN=Ida
Skiber,CN=Users,DC=lab8,DC=com'.
Oct 31 2015 17:35:36 dram3 SF-IMS[3800]: [10997] ADI:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-10-31T21:35:36 [ INFO]: curl_easy_setopt() for CURLOPT_URL:
'https://ise20306.lab8.com:8910/pxgrid/mnt/sd/getSessionListByTime'
Oct 31 2015 17:35:36 dram3 SF-IMS[3800]: [10996] ADI:adi.ISEConnection [INFO] Starting bulk download
Oct 31 2015 17:35:36 dram3 SF-IMS[4114]: [4528] SFDataCorrelator:adi.subscriber [INFO] ADI subscriber connected to ADI service at /tmp/vdi.socket
Oct 31 2015 17:35:35 dram3 SF-IMS[3800]: [3800] ADI:infra.ev-rpc [INFO] Started server ADI, listening for clients.
Oct 31 2015 17:35:35 dram3 SF-IMS[3800]: [3800] ADI:adi.RpcServer [INFO] starting rpc server
Oct 31 2015 17:35:35 dram3 SF-IMS[3800]: [3800] ADI:adi.ISEConnection [INFO] ...successfully connected to ISE server.
```

Step 6 You should see the following in ISE



□	Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	ise-admin-ise20		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	ise-mnt-ise20		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	iseagent-fmc60.lab9.com-975638952938c797259585...		Capabilities(0 Pub, 3 Sub)	Online	Session	View
□	iseagent-asafp.lab9.com-f81cce9816bba5d13beda521...		Capabilities(0 Pub, 3 Sub)	Online	Session	View
□	firesightisetest-firepower-975638952938c797259585...		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
□	iseagent-firepower-975638952938c79725958550f647...		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
□	firesightisetest-firepower-7de80a53821360aa8f849f04		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
□	iseagent-firepower-7de80a53821360aa8f849f04c094...		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
□	firesightisetest-asafp.lab9.com-f81cce9816bba5d13be...		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
□	firesightisetest-fmc60.lab9.com-975638952938c7972...		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
□	splunk1		Capabilities(0 Pub, 0 Sub)	Offline	EPS	View

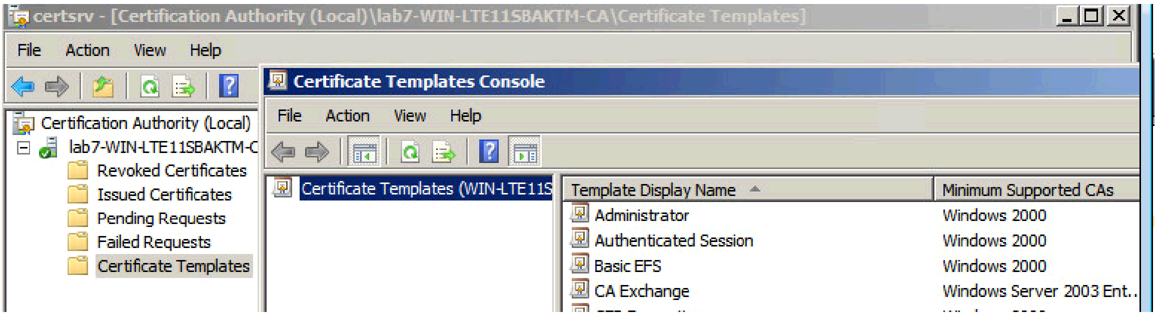
CA (Certificate Authority)- Signed Certificate Operation

This section provides configuration details for deploying ISE 2.0 and Cisco Firepower Management Center 6.0 in an ISE stand-alone environment. This section is optional if you are deploying self-signed certificates.

Customized pxGrid Template for CA-Signed Operation

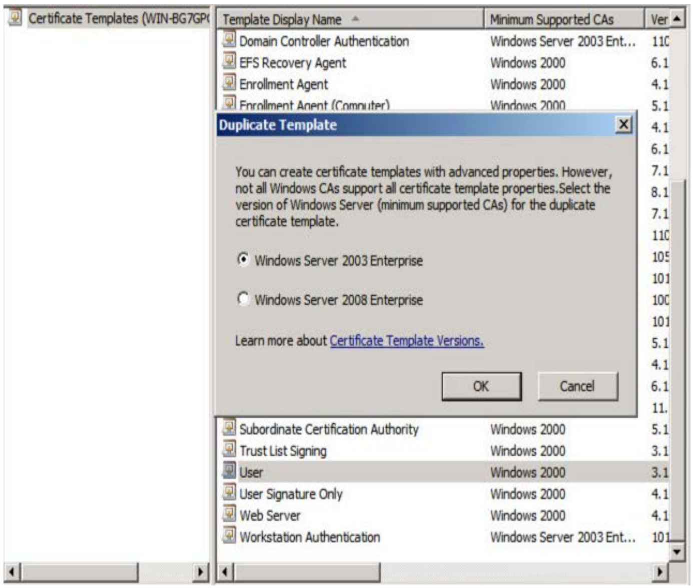
A customized pxGrid template having an Enhanced Key Usage (EKU) of both client authentication and server authentication is required for pxGrid operation between the pxGrid client, the Firepower Management Center and the ISE pxGrid node. This is required for a Certificate Authority (CA)-signed environment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

Step 7 Select **Administrative Tools->Certificate Authority-> "+" dropdown next to CA server->Right-Click on Certificate Templates->Manage**


certsrv - [Certification Authority (Local)\lab7-WIN-LTE11SBAKTM-CA\Certificate Templates]
File
Action
View
Help
Certification Authority (Local)
lab7-WIN-LTE11SBAKTM-C
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Certificate Templates Console
File
Action
View
Help
Certificate Templates (WIN-LTE11S

Template Display Name	Minimum Supported CAs
Administrator	Windows 2000
Authenticated Session	Windows 2000
Basic EFS	Windows 2000
CA Exchange	Windows Server 2003 Ent...

Step 8 Right-Click and Duplicate User template->Select->**Windows 2003 Enterprise->OK**



Template Display Name	Minimum Supported CAs	Ver
Domain Controller Authentication	Windows Server 2003 Ent...	11C
EFS Recovery Agent	Windows 2000	6.1
Enrollment Agent	Windows 2000	4.1
Enrollment Agent (Computer)	Windows 2000	5.1
Subordinate Certification Authority	Windows 2000	5.1
Trust List Signing	Windows 2000	3.1
User	Windows 2000	3.1
User Signature Only	Windows 2000	4.1
Web Server	Windows 2000	4.1
Workstation Authentication	Windows Server 2003 Ent...	101

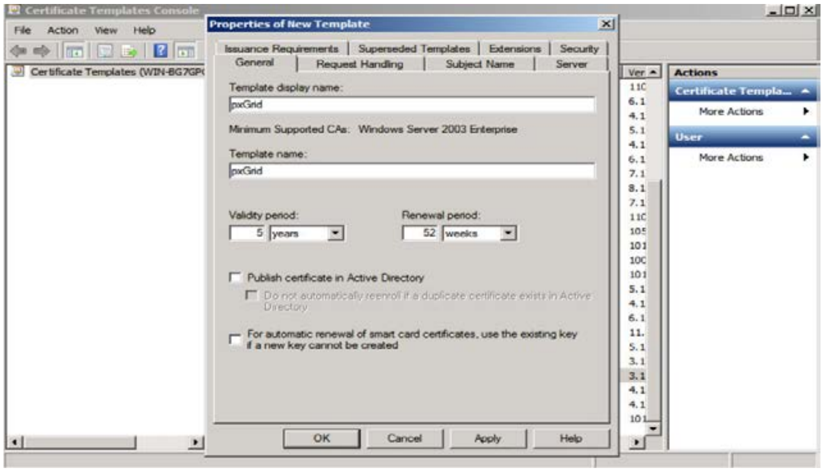
You can create certificate templates with advanced properties. However, not all Windows CAs support all certificate template properties.Select the version of Windows Server (minimum supported CAs) for the duplicate certificate template.

● Windows Server 2003 Enterprise

○ Windows Server 2008 Enterprise

Learn more about Certificate Template Versions.

Step 9 Enter name of certificate template, uncheck “Publish certificate in Active Directory”, and provide validity period and renewal period.



Template display name: pxGrid

Minimum Supported CAs: Windows Server 2003 Enterprise

Template name: pxGrid

Validity period: 5 years

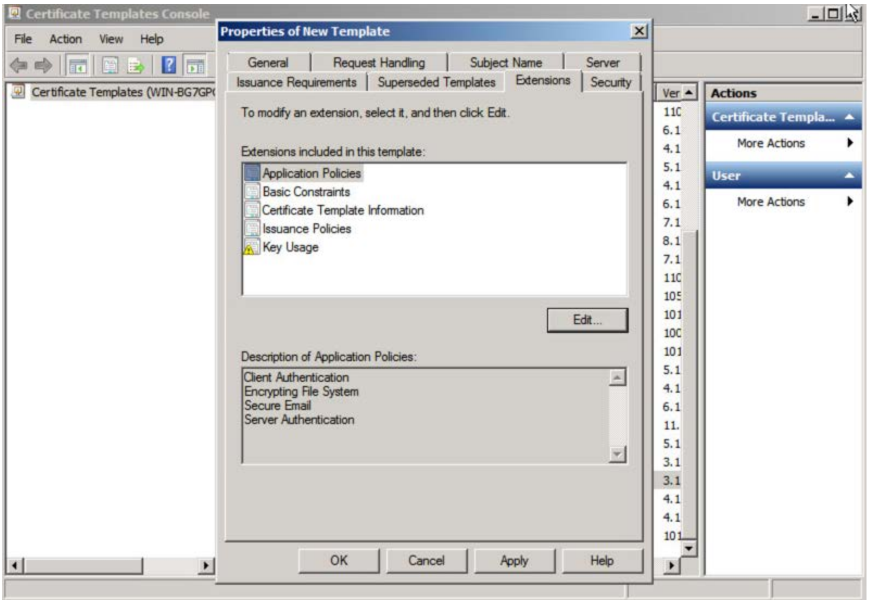
Renewal period: 52 weeks

□ Publish certificate in Active Directory

□ Do not automatically reenroll if a duplicate certificate exists in Active Directory

□ For automatic renewal of smart card certificates, use the existing key if a new key cannot be created

Step 10 Click on Extensions->**Add->Server Authentication->Ok->Apply**



To modify an extension, select it, and then click Edit.

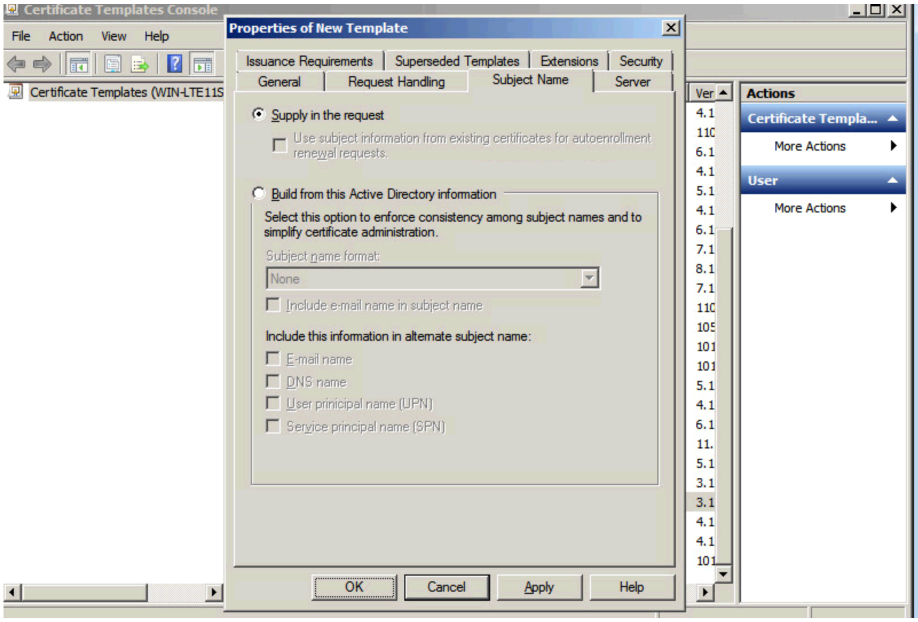
Extensions included in this template:

Application Policies
Basic Constraints
Certificate Template Information
Issuance Policies
Key Usage

Description of Application Policies:

Client Authentication
Encrypting File System
Secure Email
Server Authentication

Step 11 Click on Subject name, Enable Supply in request


Certificate Templates Console
File Action View Help
Certificate Templates (WIN-LTE11S
Properties of New Template
Issuance Requirements | Superseded Templates | Extensions | Security
General | Request Handling | Subject Name | Server
Ver
Actions
Certificate Templa...
More Actions
User
More Actions
OK Cancel Apply Help

● Supply in the request

□ Use subject information from existing certificates for autoenrollment renewal requests.

○ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

None

□ Include e-mail name in subject name

Include this information in alternate subject name:

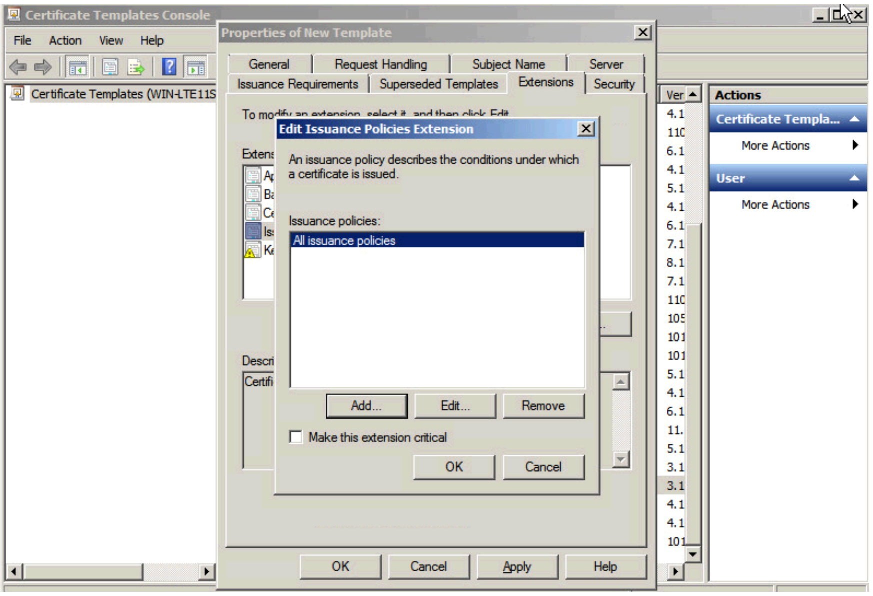
□ E-mail name

□ DNS name

□ User principal name (UPN)

□ Service principal name (SPN)

Step 12 Click on **Extensions->Issuance Policies->Edit->All Issuance Policies**


Certificate Templates Console
File Action View Help
Certificate Templates (WIN-LTE11S
Properties of New Template
General | Request Handling | Subject Name | Server
Issuance Requirements | Superseded Templates | Extensions | Security
To modify an extension, select it, and then click Edit.
Extens
Ap
Ba
Ce
Is
Ke
Descri
Certifi
Edit Issuance Policies Extension
Add... Edit... Remove
OK Cancel
OK Cancel Apply Help
Ver
Actions
Certificate Templa...
More Actions
User
More Actions

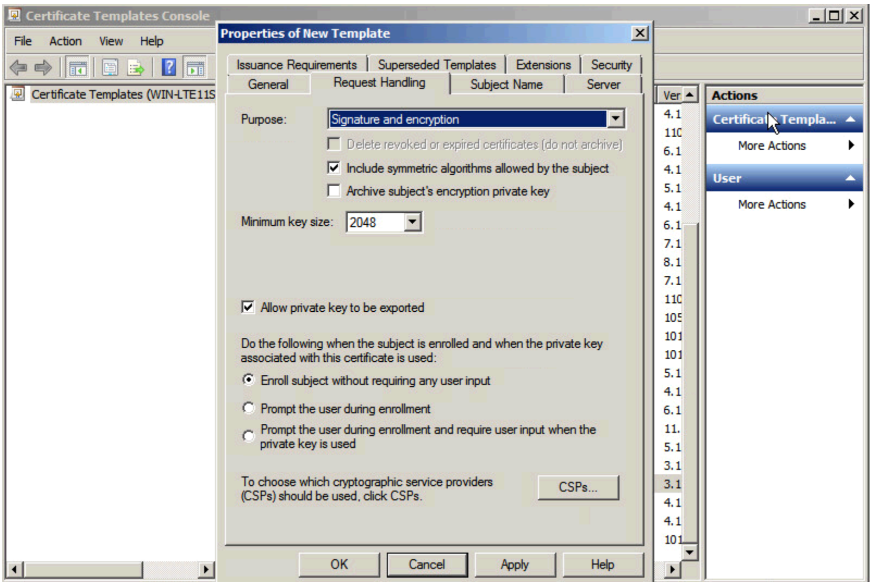
An issuance policy describes the conditions under which a certificate is issued.

Issuance policies:

All issuance policies

□ Make this extension critical

Step 13 Leave the defaults for request handling


Certificate Templates Console
File Action View Help
Certificate Templates (WIN-LTE11S
Properties of New Template
Issuance Requirements | Superseded Templates | Extensions | Security
General | Request Handling | Subject Name | Server
Ver
Actions
Certificate Templa...
More Actions
User
More Actions
OK Cancel Apply Help

Purpose: Signature and encryption

□ Delete revoked or expired certificates (do not archive)

☑ Include symmetric algorithms allowed by the subject

□ Archive subject's encryption private key

Minimum key size: 2048

☑ Allow private key to be exported

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

● Enroll subject without requiring any user input

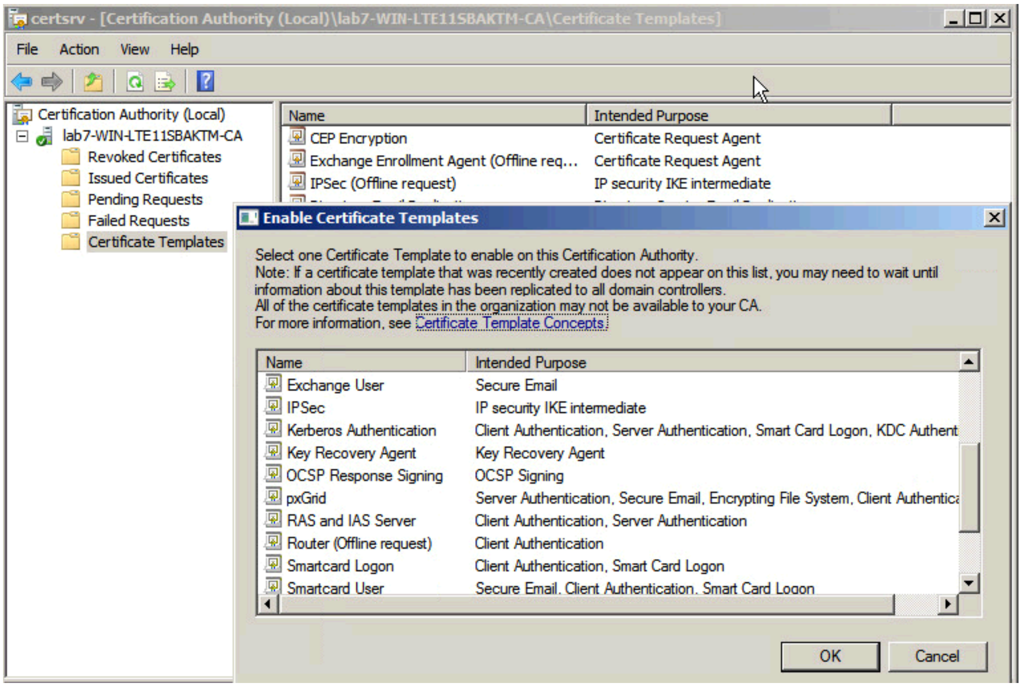
○ Prompt the user during enrollment

○ Prompt the user during enrollment and require user input when the private key is used

To choose which cryptographic service providers (CSPs) should be used, click CSPs. CSPs...

Step 14 Right-click on Certificate templates

Step 15 Select->**New Template to issue and select pxGrid**

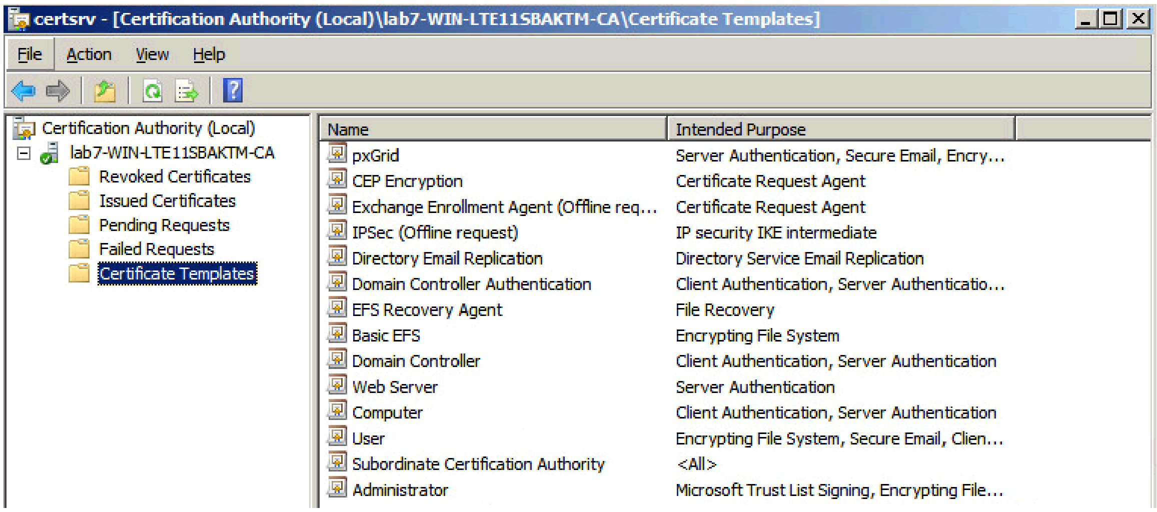

certsrv - [Certification Authority (Local)\lab7-WIN-LTE11SBAKTM-CA\Certificate Templates]
File
Action
View
Help
Certification Authority (Local)
lab7-WIN-LTE11SBAKTM-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Enable Certificate Templates
OK
Cancel

Name	Intended Purpose
CEP Encryption	Certificate Request Agent
Exchange Enrollment Agent (Offline req...	Certificate Request Agent
IPSec (Offline request)	IP security IKE intermediate

Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

Name	Intended Purpose
Exchange User	Secure Email
IPSec	IP security IKE intermediate
Kerberos Authentication	Client Authentication, Server Authentication, Smart Card Logon, KDC Authent
Key Recovery Agent	Key Recovery Agent
OCSP Response Signing	OCSP Signing
pxGrid	Server Authentication, Secure Email, Encrypting File System, Client Authentica
RAS and IAS Server	Client Authentication, Server Authentication
Router (Offline request)	Client Authentication
Smartcard Logon	Client Authentication, Smart Card Logon
Smartcard User	Secure Email, Client Authentication, Smart Card Logon

Step 16 You should see the pxGrid template



Name	Intended Purpose
pxGrid	Server Authentication, Secure Email, Encry...
CEP Encryption	Certificate Request Agent
Exchange Enrollment Agent (Offline req...	Certificate Request Agent
IPSec (Offline request)	IP security IKE intermediate
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authenticatio...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentication
Web Server	Server Authentication
Computer	Client Authentication, Server Authentication
User	Encrypting File System, Secure Email, Clien...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting File...

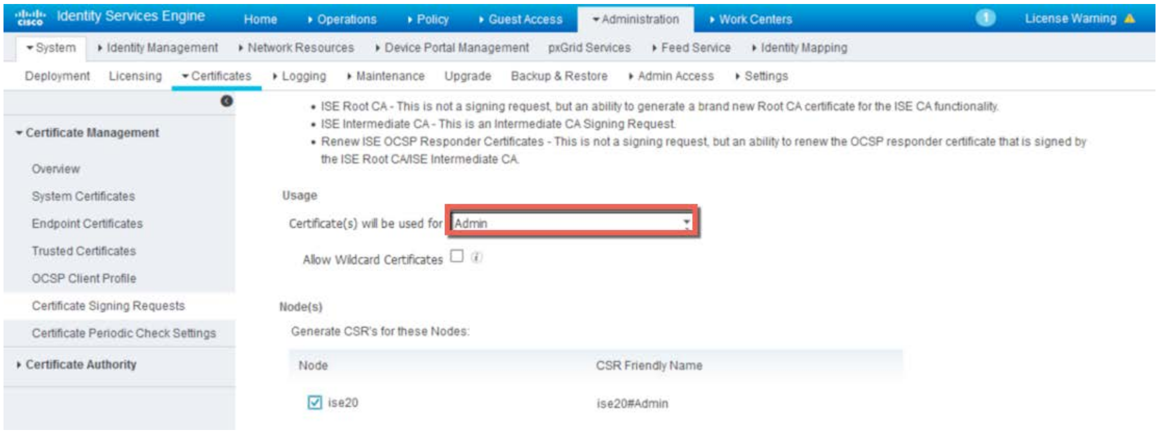
Configuring ISE 2.0

The ISE pxGrid node is configured for a Certificate Authority (CA) signed environment in a stand-alone configuration. 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 should be admin. This is required for FMC 6.0 for active bulk download sessions



- ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality.
- ISE Intermediate CA - This is an Intermediate CA Signing Request.
- Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by the ISE Root CA/ISE Intermediate CA.

Usage

Certificate(s) will be used for: Admin

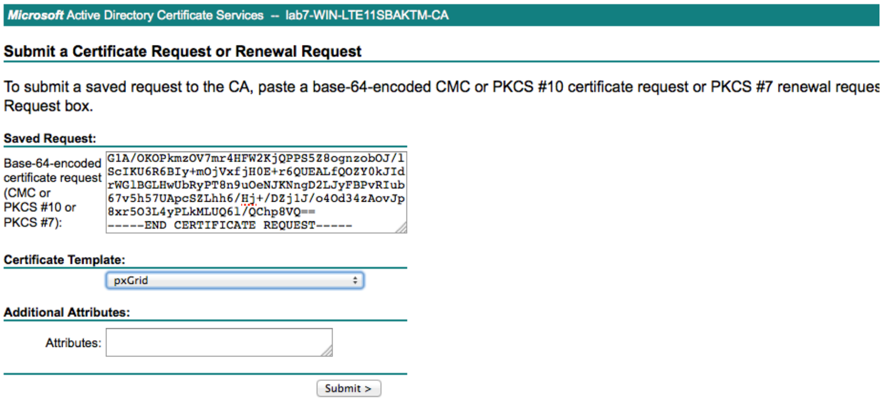
Allow Wildcard Certificates □

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☑ ise20	ise20#Admin

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 >

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 reques Request box.

Saved Request:

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

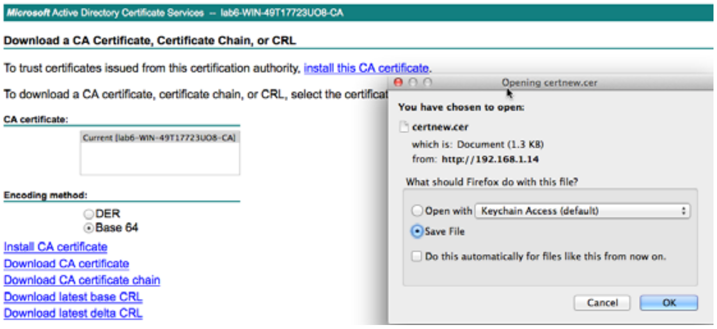
```
GlA/OKOPkmzOV7mr4HFW2KjQPPS5Z8ognzobOJ/l
ScIKU6R6BIy+mOjVxfjH0E+r6QUEALfQOZY0kJId
rWGlBGLHwUbRyPT8n9uOeNJKNngD2LJyFBPvRIub
67v5h57UApcSZLhh6/Hj+/DZj1J/o4Od34zAovJp
8xr5O3L4yPLkMLUQ6l/QChp8VQ==
-----END CERTIFICATE REQUEST-----
```

Certificate Template: pxGrid

Additional Attributes:

Attributes:

Step 3 Download the CA root in base-64 encoded format


Microsoft Active Directory Certificate Services -- lab6-WIN-49T17723UO8-CA
Install CA certificate
Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL
Opening certnew.cer
Cancel
OK

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate.

To download a CA certificate, certificate chain, or CRL, select the certificat

CA certificate: Current [lab6-WIN-49T17723UO8-CA]

Encoding method:
○ DER
● Base 64

You have chosen to open:

certnew.cer
which is: Document (1.3 KB)
from: http://192.168.1.14

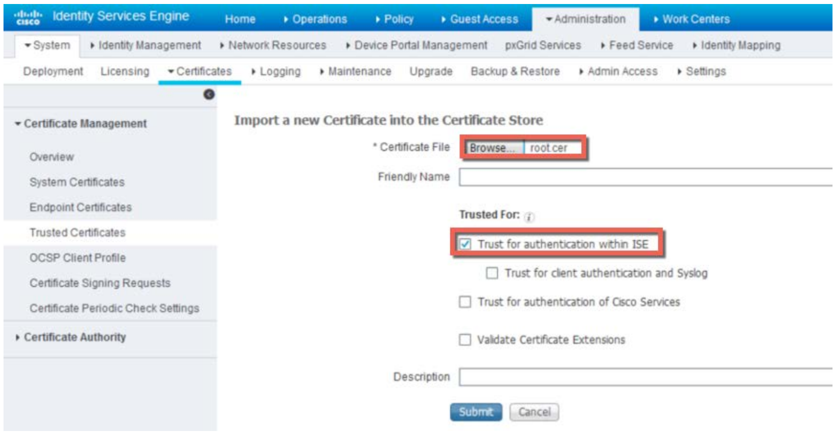
What should Firefox do with this file?

○ Open with Keychain Access (default)
● Save File

□ Do this automatically for files like this from now on.

Step 4 Upload the CA root into the ISE certificate trusted system store
Select->**Administration->System->Certificates->Trusted Certificates->upload the CA root certificate**

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



Import a new Certificate into the Certificate Store

* Certificate File: Browse... root.cer

Friendly Name:

Trusted For:

☑ Trust for authentication within ISE

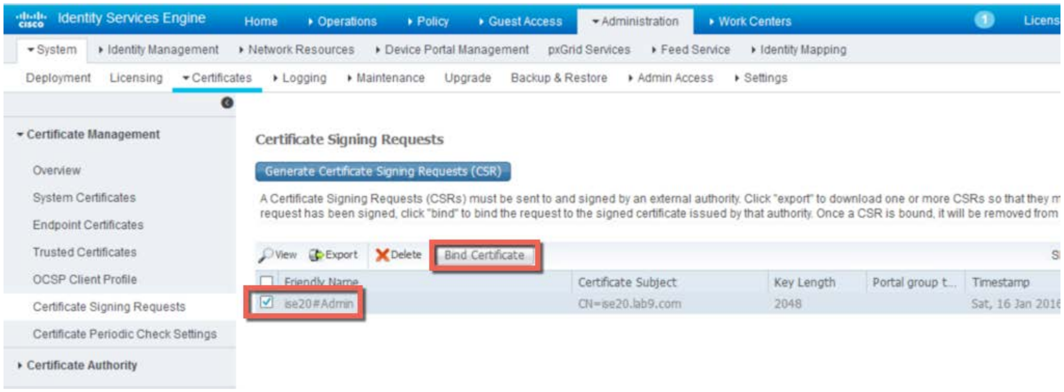
□ Trust for client authentication and Syslog

□ Trust for authentication of Cisco Services

□ Validate Certificate Extensions

Description:

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

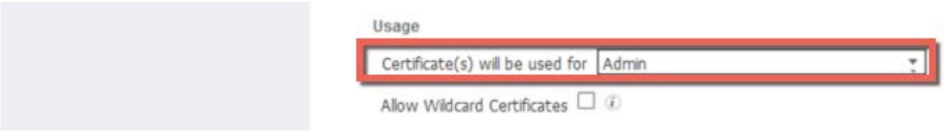


Certificate Signing Requests

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they m
request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from

	Friendly Name	Certificate Subject	Key Length	Portal group t...	Timestamp
☑	ise20#Admin	CN=ise20.lab9.com	2048		Sat, 16 Jan 2016

Step 7 Select **Administration->System->Certificates->Certificate Management->Certificate Signing Request->Generate Certificate Signing Requests (CSR)->Admin** for certificate usage

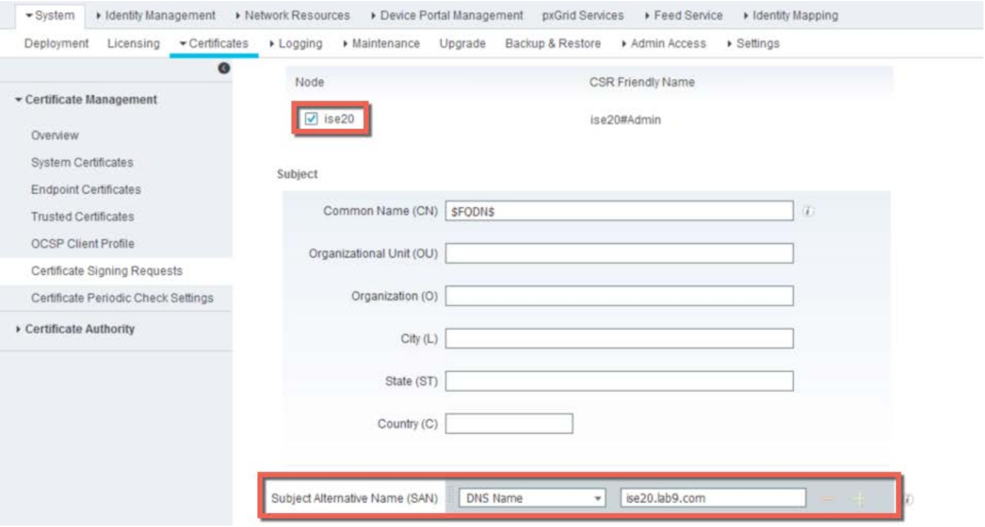


Certificate(s) will be used for: Admin

Allow Wildcard Certificates □

Step 8 Select **Node**

Step 9 Select **DNS name for the Subject Alternative Name (SAN)** and add the **DNS name**



Node	CSR Friendly Name
☑ ise20	ise20#Admin

Subject

Common Name (CN): $FQDN$

Organizational Unit (OU):

Organization (O):

City (L):

State (ST):

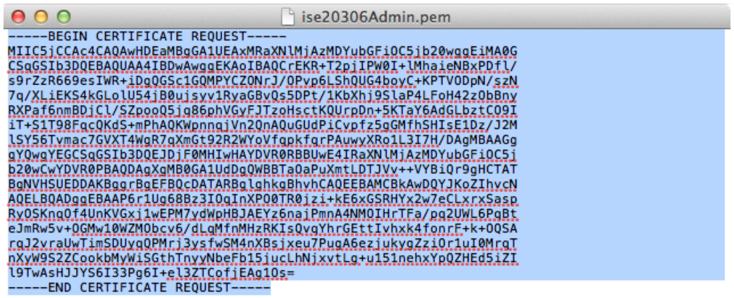
Country (C):

Subject Alternative Name (SAN): DNS Name ise20.lab9.com

Step 10 Select **Generate**

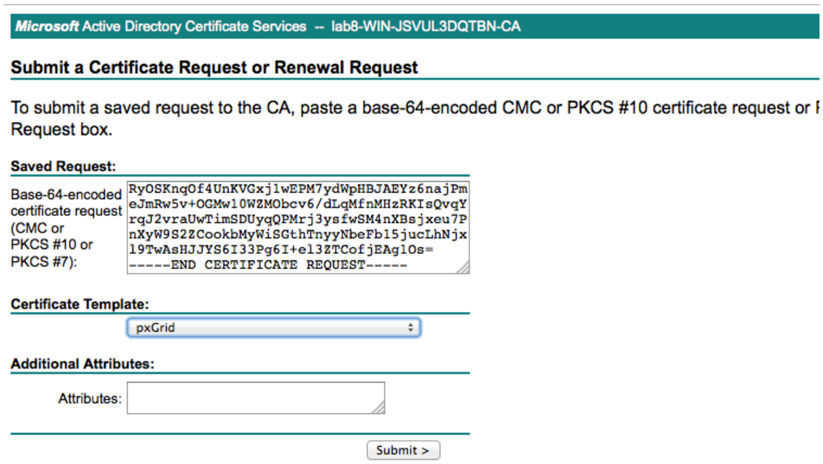
Step 11 Select **Export**

Step 12 Open the pem file and copy/paste the csr request into the customized pxGrid template



```
-----BEGIN CERTIFICATE REQUEST-----
MIIC5jCCAc4CAQAwHDEaMBgGA1UEAxMRaXNlMjAzMDYubGFiOC5jb20wggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCrEKR+T2pjIPW0I+lMhaieNBxPDfl/
s9rZzR669esIWR+iDgQGSc1GQMPYCZONrJ/OPvp6LShQUG4boyC+KPTVODpN/szN
7q/XLiEKS4kGLolU54jB0ujsyv1RyaGBvQs5DPt/1KbXhj9SlaP4LFoH42zObBny
RXPaf6nmBDjCl/SZpooQ5jq86phVGyFJTzoHsctKQUrpDn+5KTaY6AdGLbztCO9I
iT+S1T98FqcQKdS+mPhAQKWpnnqjVn2QnAQuGUdPiCvpfz5gGMfhSHIsE1Dz/J2M
lSY56Tvmac7GVXT4WgR7qXmGt92R2WYoVfqpkfqrPAuwyXRo1L3I7H/DAgMBAAGg
gYQwgYEGCSqGSIb3DQEJDjF0MHIwHAYDVR0RBBUwE4IRaXNlMjAzMDYubGFiOC5j
b20wCwYDVR0PBAQDAgXgMB0GA1UdDgQWBBTaOaPuXmtLDTJVv++VYBiQr9gHCTAT
BgNVHSUEDDAKBggrBgEFBQcDATARBglghkgBhvhCAQEEBAMCBkAwDQYJKoZIhvcN
AQELBQADggEBAAP6r1Ug68Bz3IOqInXPO0TR0jzi+kE6xGSRHYx2w7eCLxrxSasp
RyOSKnqOf4UnKVGxj1wEPM7ydWpHBJAEYz6najPmnA4NMOIHrTFa/pq2UWL6PqBt
eJmRw5v+OGMw10WZMObcv6/dLqMfnMHzRKIsQvqYhrGEttIvhxk4fonrF+k+OQSA
rqJ2vraUwTimSDUyqQPMrj3ysfwSM4nXBsjxeu7PugA6ezjukygZziOr1uI0MrqT
nXyW9S2ZCookbMyWiSGthTnyyNbeFb15jucLhNjxvtLg+u151nehxYpQZHEd5iZI
l9TwAsHJJYS6I33Pg6I+el3ZTCofjEAg1Os=
-----END CERTIFICATE REQUEST-----
```

Step 13 Paste into Request a Certificate->Advanced Certificate Request, select customized pxGrid template->Submit



Microsoft Active Directory Certificate Services -- lab8-WIN-JSVUL3DQTBN-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 I Request box.

Saved Request:

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

```
RyOSKnqOf4UnKVGxjlwEPM7ydWpHBJAEYz6najPm
eJmRw5v+OGMwl0WZMObcv6/dLqMfnMHzRKIsQvqY
rqJ2vraUwTimSDUyqQPMrj3ysfwSM4nXBsjxeu7P
nXyW9S2ZCookbMyWiSGthTnyyNbeFbl5jucLhNjx
l9TwAsHJJYS6I33Pg6I+el3ZTCofjEAglOs=
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

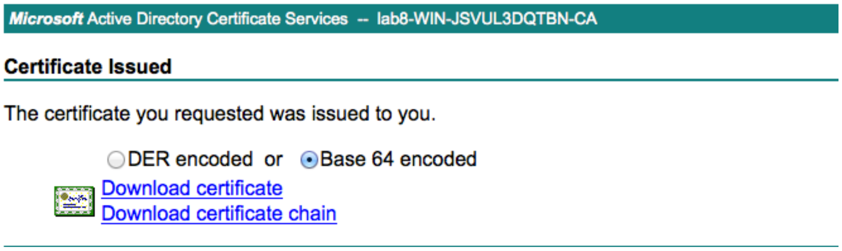
pxGrid

Additional Attributes:

Attributes:

Step 14 Select **Submit**

Step 15 Download certificate in base 64 encoded format



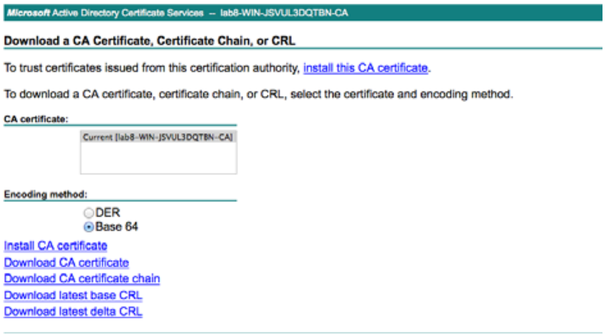
Microsoft Active Directory Certificate Services -- lab8-WIN-JSVUL3DQTBN-CA

Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Step 16 Download CA root certificate in Base 64 format



Microsoft Active Directory Certificate Services -- lab8-WIN-JSVUL3DQTBN-CA

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

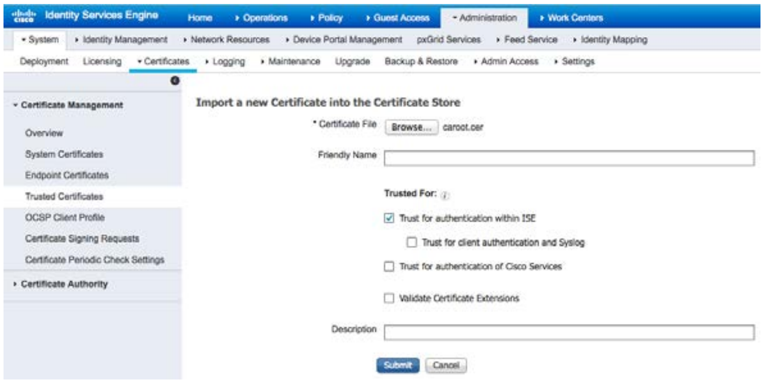
Current [lab8-WIN-JSVUL3DQTBN-CA]

Encoding method:

○ DER
● Base 64

Step 17 Administration **System->Certificates->Certificate Management->Trusted Certificates->Import the root certificate**

Step 18 Enable **Trust for authentication within ISE**



Import a new Certificate into the Certificate Store

* Certificate File: caroot.cer

Friendly Name:

Trusted For:

☑ Trust for authentication within ISE

☐ Trust for client authentication and Syslog

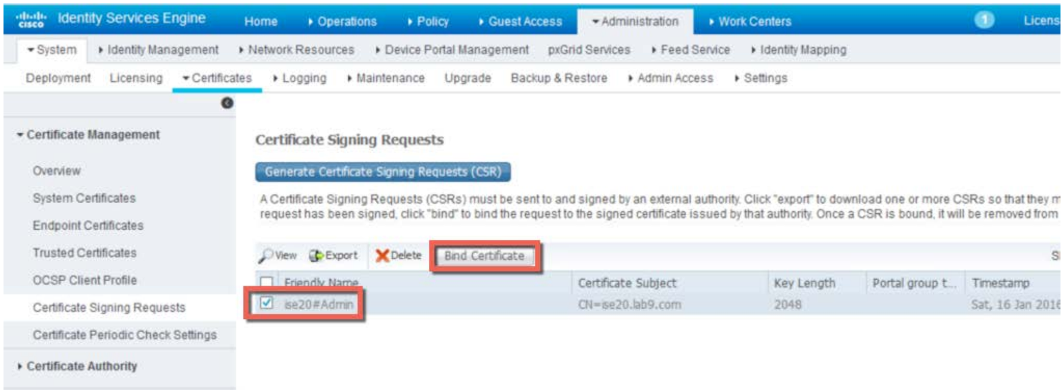
☐ Trust for authentication of Cisco Services

☐ Validate Certificate Extensions

Description:

Step 19 Select **Submit**

Step 20 Select **Administration->Certificates->Certificate Management->System Certificates->Certificate Signing Requests->select CSR request->Bind Certificate**

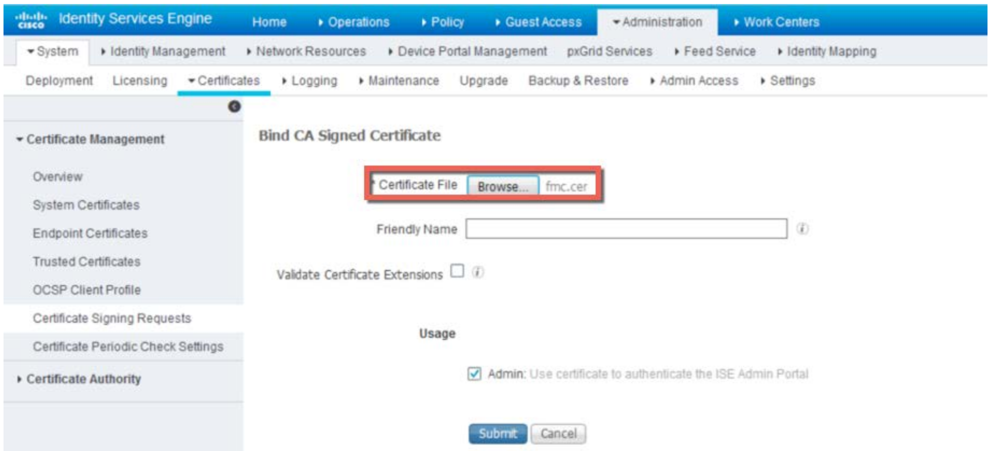


Certificate Signing Requests

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they m request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from

	Friendly Name	Certificate Subject	Key Length	Portal group t...	Timestamp
☑	ise20#Admin	CN=ise20.lab9.com	2048		Sat, 16 Jan 2016

Step 21 Upload the ISE CA-signed identity certificate



Bind CA Signed Certificate

* Certificate File fmc.cer

Friendly Name

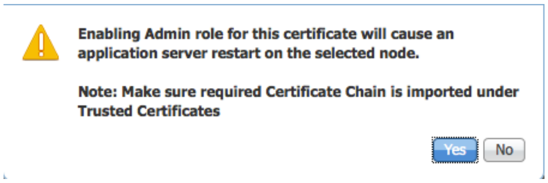
Validate Certificate Extensions ☐

Usage

☑ Admin: Use certificate to authenticate the ISE Admin Portal

Step 22 Select **Submit**

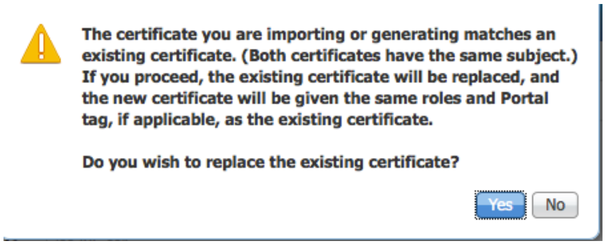
Step 23 Select **Yes,** when you see the following message:



Enabling Admin role for this certificate will cause an application server restart on the selected node.

Note: Make sure required Certificate Chain is imported under Trusted Certificates

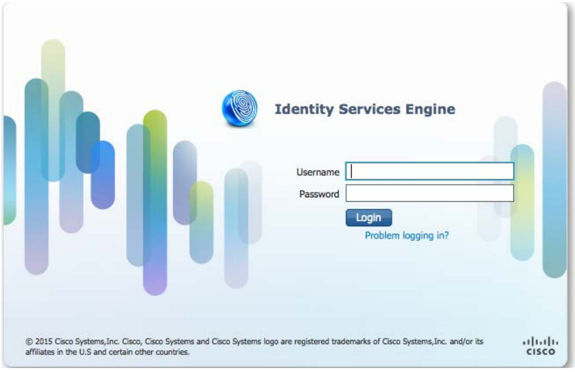
Step 24 Select **YES**, when you see the following message



The certificate you are importing or generating matches an existing certificate. (Both certificates have the same subject.) If you proceed, the existing certificate will be replaced, and the new certificate will be given the same roles and Portal tag, if applicable, as the existing certificate.

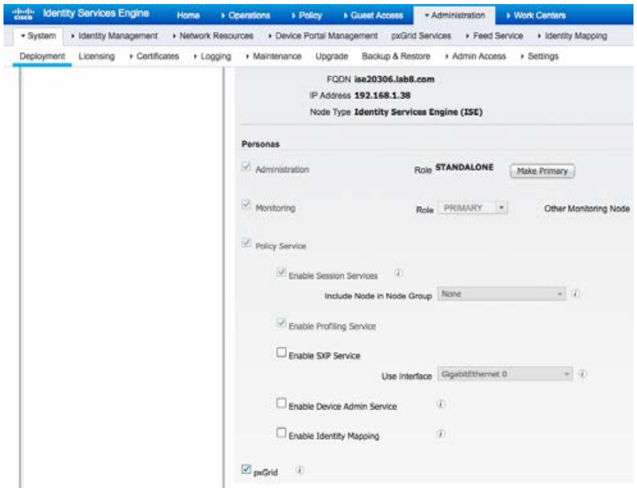
Do you wish to replace the existing certificate?

Step 25 You will see that the system will be restarting and will take you back to the GUI



© 2015 Cisco Systems,Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems,Inc. and/or its affiliates in the U.S and certain other countries.

Step 26 Select **Administration->System->Deployment->edit the Hostname->enable pxGrid**



FQDN **ise20306.lab8.com**
IP Address **192.168.1.38**
Node Type **Identity Services Engine (ISE)**

Personas

☑ Administration Role **STANDALONE**

☑ Monitoring Role PRIMARY Other Monitoring Node

☑ Policy Service

☑ Enable Session Services

Include Node in Node Group None

☑ Enable Profiling Service

□ Enable SXP Service

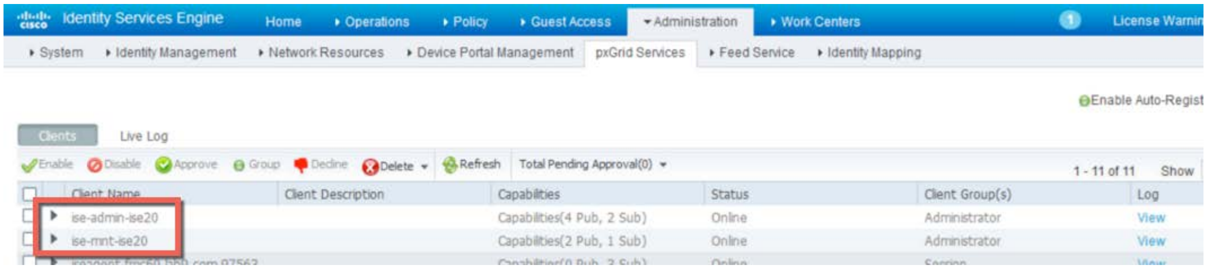
Use Interface GigabitEthernet 0

□ Enable Device Admin Service

□ Enable Identity Mapping

☑ pxGrid

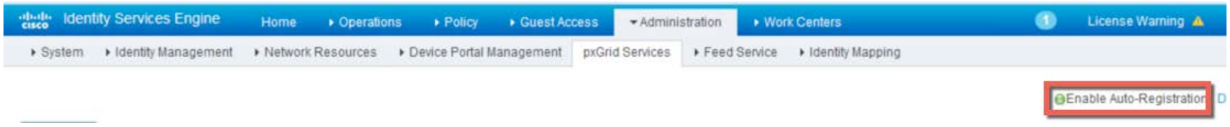
Step 27 Select **Save**
Step 28 Select **Administration->pxGrid Services,** verify that you see the published services



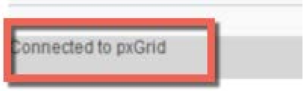
Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
ise-admin-ise20		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
ise-mnt-ise20		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View

Note: This may take a few seconds to appear, verify that the pxGrid services are initializing by running “sh application status ise” on the ISE VM

Step 29 Enable **Enable Auto Registration**



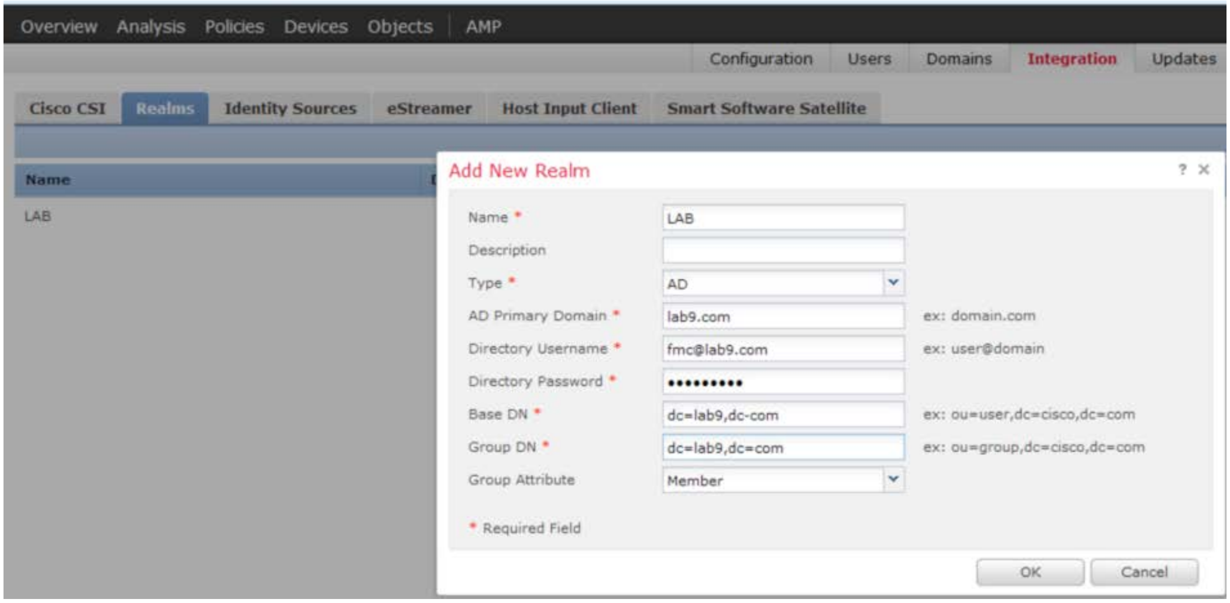
Step 30 Verify that you are **connected to pxGrid**



Creating Firepower ISE Realm

The ISE Realm is used for ISE authentication and will be used in the Firepower Management Center's 6.0 Identity Policy.

Step 1 Select **System->Integration->Realms->New Realm**



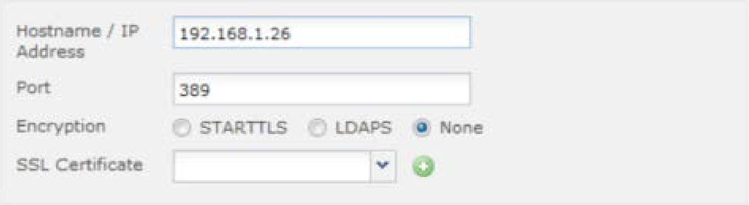
Add New Realm

Name *	LAB	
Description		
Type *	AD	
AD Primary Domain *	lab9.com	ex: domain.com
Directory Username *	fmc@lab9.com	ex: user@domain
Directory Password *	••••••••••	
Base DN *	dc=lab9,dc-com	ex: ou=user,dc=cisco,dc=com
Group DN *	dc=lab9,dc=com	ex: ou=group,dc=cisco,dc=com
Group Attribute	Member	

* Required Field

Step 2 Select **OK**

Step 3 Select **Add Directory,** enter the FQDN hostname or information



Hostname / IP Address	192.168.1.26
Port	389
Encryption	○ STARTTLS ○ LDAPS ● None
SSL Certificate	

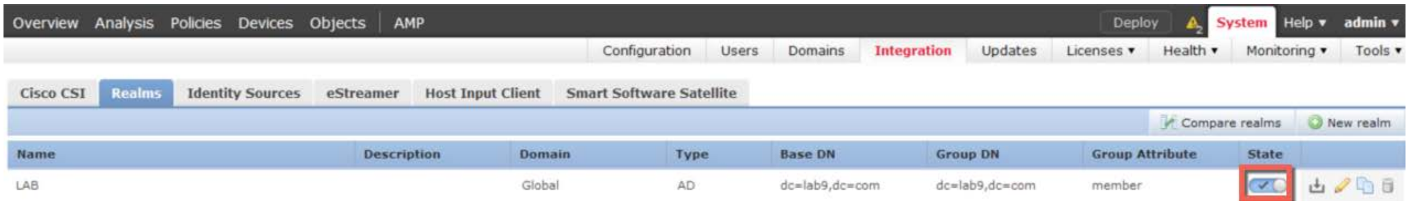
Step 4 Select **Test,** you should see that the: **Test Connection has succeeded,** select **OK**

Note: If you see a returned failed attempt, ensure that the directory username and directory password are correct in the Realm Configuration.

Step 5 Select **OK**

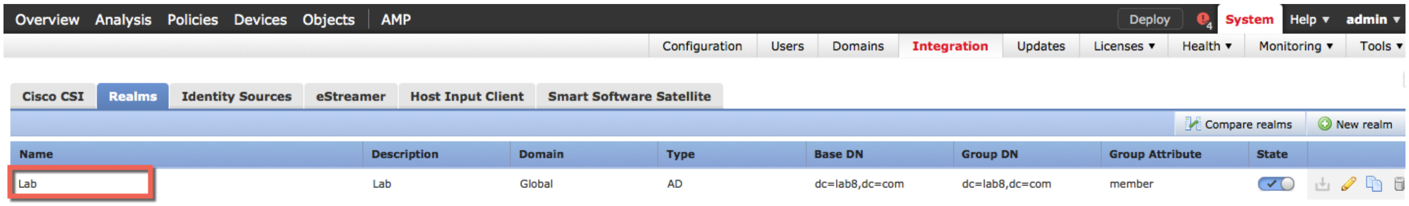
Step 6 Select **Save**

Step 7 Enable the state by selecting ✓


Overview Analysis Policies Devices Objects AMP
Deploy System Help ▾ admin ▾
Configuration Users Domains Integration Updates Licenses ▾ Health ▾ Monitoring ▾ Tools ▾
Cisco CSI Realms Identity Sources eStreamer Host Input Client Smart Software Satellite
Compare realms New realm

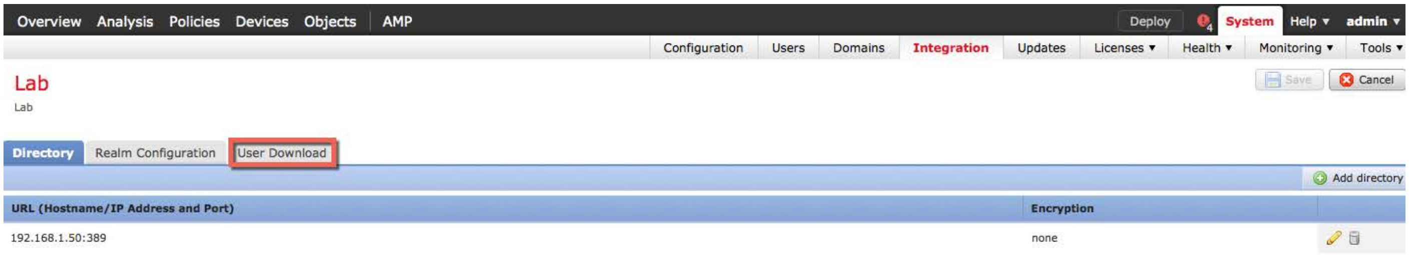
Name	Description	Domain	Type	Base DN	Group DN	Group Attribute	State
LAB		Global	AD	dc=lab9,dc=com	dc=lab9,dc=com	member	

Step 8 Click->**Realm name**


Overview Analysis Policies Devices Objects AMP
Deploy System Help ▾ admin ▾
Configuration Users Domains Integration Updates Licenses ▾ Health ▾ Monitoring ▾ Tools ▾
Cisco CSI Realms Identity Sources eStreamer Host Input Client Smart Software Satellite
Compare realms New realm

Name	Description	Domain	Type	Base DN	Group DN	Group Attribute	State
Lab	Lab	Global	AD	dc=lab8,dc=com	dc=lab8,dc=com	member	

Step 9 Click->**User Download**

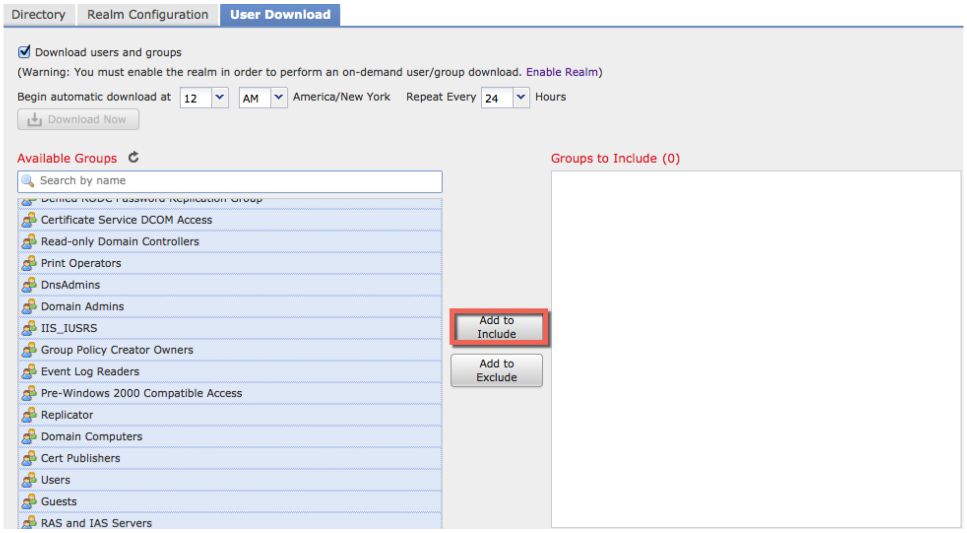

Overview Analysis Policies Devices Objects AMP
Deploy System Help ▾ admin ▾
Configuration Users Domains Integration Updates Licenses ▾ Health ▾ Monitoring ▾ Tools ▾
Save Cancel
Directory Realm Configuration User Download
Add directory

Lab
Lab

URL (Hostname/IP Address and Port)	Encryption
192.168.1.50:389	none

Step 10 Enable **Download users and groups**

Step 11 Highlight all Available Groups select **Add to Include**



☑ Download users and groups

(Warning: You must enable the realm in order to perform an on-demand user/group download. Enable Realm)

Begin automatic download at 12 AM America/New York Repeat Every 24 Hours

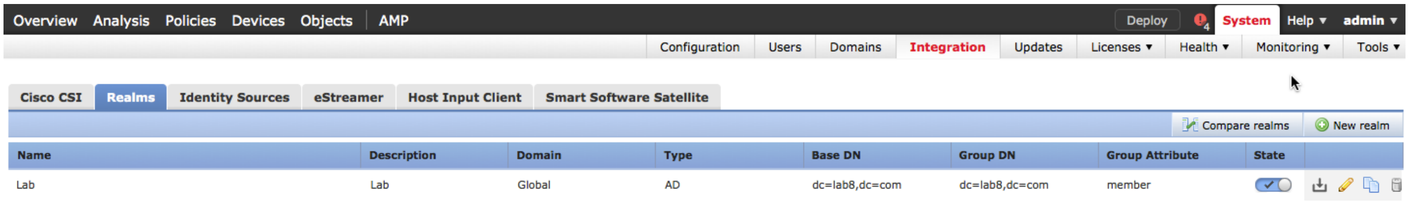
Available Groups

- Denied RODC Password Replication Group
- Certificate Service DCOM Access
- Read-only Domain Controllers
- Print Operators
- DnsAdmins
- Domain Admins
- IIS_IUSRS
- Group Policy Creator Owners
- Event Log Readers
- Pre-Windows 2000 Compatible Access
- Replicator
- Domain Computers
- Cert Publishers
- Users
- Guests
- RAS and IAS Servers

Groups to Include (0)

Step 12 Select **Save**

Step 13 You should see the following:



Name	Description	Domain	Type	Base DN	Group DN	Group Attribute	State
Lab	Lab	Global	AD	dc=lab8,dc=com	dc=lab8,dc=com	member	✓

Configuring Firepower Management Center 6.0

The Firepower Management Center (FMC) is configured for Certificate Authority (CA)-signed operation. The Firepower Management Center private key and CSR request are created from the Firepower 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 Firepower private key

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

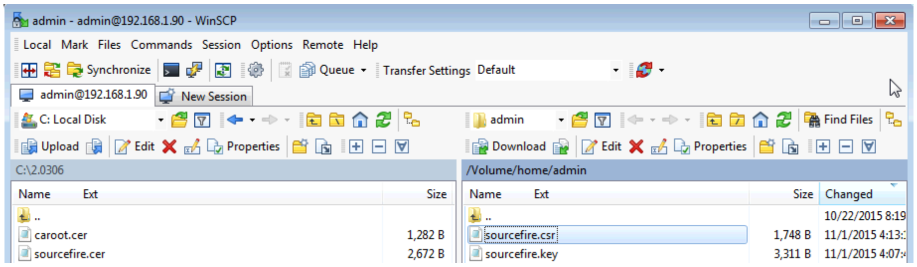
```
openssl genrsa -des3 -out sourcefire.key 4096
```

Step 2 Generate a CSR request

Note: you will be prompted for a password; this will be the same password as you entered previously

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

Step 3 Use WinSCP to copy sourcefire.csr and sourcefire.key file from the Firepower Management Center (FMC) locally to the PC



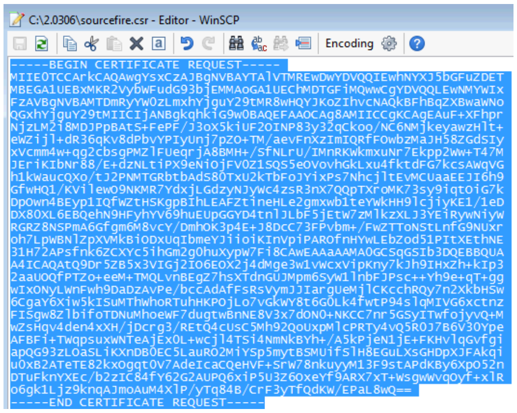
C:\2.0306

Name	Ext	Size
..		
caroot.cer		1,282 B
sourcefire.cer		2,672 B

/Volume/home/admin

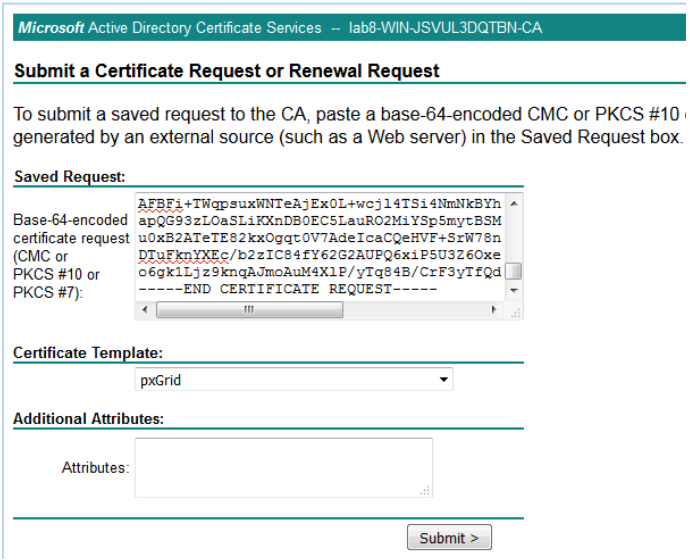
Name	Ext	Size	Changed
..			10/22/2015 8:19
sourcefire.csr		1,748 B	11/1/2015 4:13:
sourcefire.key		3,311 B	11/1/2015 4:07:

Step 4 Open the CSR request using editor copy the CSR request



```
-----BEGIN CERTIFICATE REQUEST-----
MIIE0TCCArkCAQAwgYsxCzAJBgNVBAYTAlVTMREwDwYDVQQIEwhNYXJ5bGFuZDET
MBEGA1UEBxMKR2VybWFudG93bjEMMAoGA1UEChMDTGFiMQwwCgYDVQQLEwNMYWIx
FzAVBgNVBAMTDmRyYW0zLmxhYjguY29tMR8wHQYJKoZIhvcNAQkBFhBqZXBwaWNo
QGxhYjguY29tMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAuF+XFhpr
NjzLM2i8MDJPpBAtS+FePF/J3oX5kiUF2OINP83y32qCkoo/NC6NMjkeyawzHlt+
eWZijl+dR36qKv8dPbvYPIyUnj7pZO+TM/aevFnXzImIQRfFOwbzMaJH58ZGdSIy
xVcmm4w+qg2cbsgPMZlFUeqrjA8BMH+/SfNLrU/IMnRKWkmxuNr7Ekpp2Ww+T47M
JEriKIbNr88/E+dzNLtiPX9eNiOjFV0Z1SQS5eOVovhGkLxu4fktdFG7kcsAWqVG
h1kWaucQXo/tJ2PNMTGRbtbAdS80TxU2kTbFoJYixPs7NhcjltEvMCUaaEEJI6h9
GfwHQ1/KVilewO9NKMR7YdxjLGdzyNJyWc4zsR3nX7QQpTXroMK73sy9iqtOiG7k
DpOwn4BEyp1IQfWZtHSKgpBIhLEAFZtineHLe2gmxwb1teYWkHH9lcjiyKE1/1eD
DX80XL6EBQehN9HFyhYV69huEUpGGYD4tnlJLbF5jEtW7zMlkzXLJ3YEiRywNiyW
RGRZ8NSPmA6Gfgm6M8vcY/DmhOK3p4E+J8DcC73FPvbm+/FwZTToNStLnfG9NUxr
oh7LpWBNlZpXVMkBiODxUqIbmeYJiioiKInVpiPAROfnHYwLEbZod51PItXEthNE
31H72APsfnk6ZCXYc5ihGm2g0huXypW7Fi8CAwEAAaAAMA0GCSqGSIb3DQEBBQUA
A4ICAQAtQ9Dr5ZB5x3VIGj2IO6EOX2j4dMge3w1vWcxVipKny7kJh9IHxZh+kIp3
2aaUOQfPTZo+eeM+TMQLvnBEgZ7hsXTdnGUJMpm6SyW1lnbFJPsc++Yh9e+qT+gg
wIxONyLWnFwh9DaDzAvPe/bcCAdAfFsRsVymJJIargUeMjlCKcchRQy7n2XkbHSw
6CgaY6Xiw5kISuMThwhoRTuhHKPOjLo7vGkWY8t6G0Lk4fwtP94slqMIVG6xctnz
FISgw8ZlbifoTDNuMhoeWF7dugtwBnNE8V3x7dON0+NKCC7nr5GSyITwfojyvQ+M
wZsHqv4den4xXH/jDcrg3/REtQ4cUsC5Mh92QoUxpMlcPRTy4vQ5R0J7B6V3OYpe
AFBFi+TWqpsuxWNTeAjEx0L+wcjl4TSi4NmNkBYh+/A5kPjeN1jE+FKHvlqGvfgi
apQG93zLOaSLiKXnDB0EC5LauRO2MiYSp5mytBSMUifSlH8EGuLXsGHDpXJFAkqi
u0xB2ATeTE82kxOgqt0V7AdeIcaCQeHVF+SrW78nkuyyM13F9stAPdKBy6XpO52n
DTuFknYXEc/b2zIC84fY62G2AUPQ6xiP5U3Z6OxeYf9ARX7xT+WsgwWvqOyf+xlR
o6gk1Ljz9knqAJmoAuM4XlP/yTq84B/CrF3yTfQdKW/EPaL8wQ==
-----END CERTIFICATE REQUEST-----
```

Step 5 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



Microsoft Active Directory Certificate Services -- lab8-WIN-JSVUL3DQTBN-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 or generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

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

```
AFBFi+TWqpsuxWNTeAjEx0L+wcjl4TSi4NmNkBYh
apQG93zLOaSLiKXnDB0EC5LauRO2MiYSp5mytBSM
u0xB2ATeTE82kxOgqt0V7AdeIcaCQeHVF+SrW78n
DTuFknYXEc/b2zIC84fY62G2AUPQ6xiP5U3Z6Oxe
o6gk1Ljz9knqAJmoAuM4XlP/yTq84B/CrF3yTfQd
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

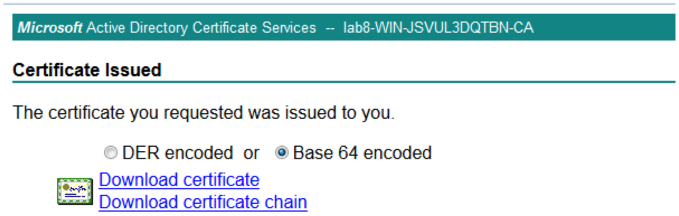
pxGrid

Additional Attributes:

Attributes:

Step 6 Select **Submit**

Step 7 Download the certificate in base 64-format



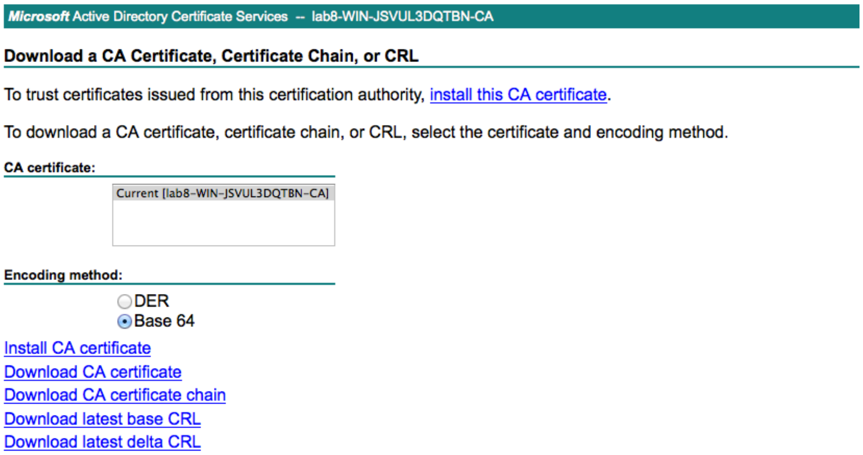
Microsoft Active Directory Certificate Services -- lab8-WIN-JSVUL3DQTBN-CA

Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Step 8 Download the CA root certificate in base-64 encoded format



Microsoft Active Directory Certificate Services -- lab8-WIN-JSVUL3DQTBN-CA

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

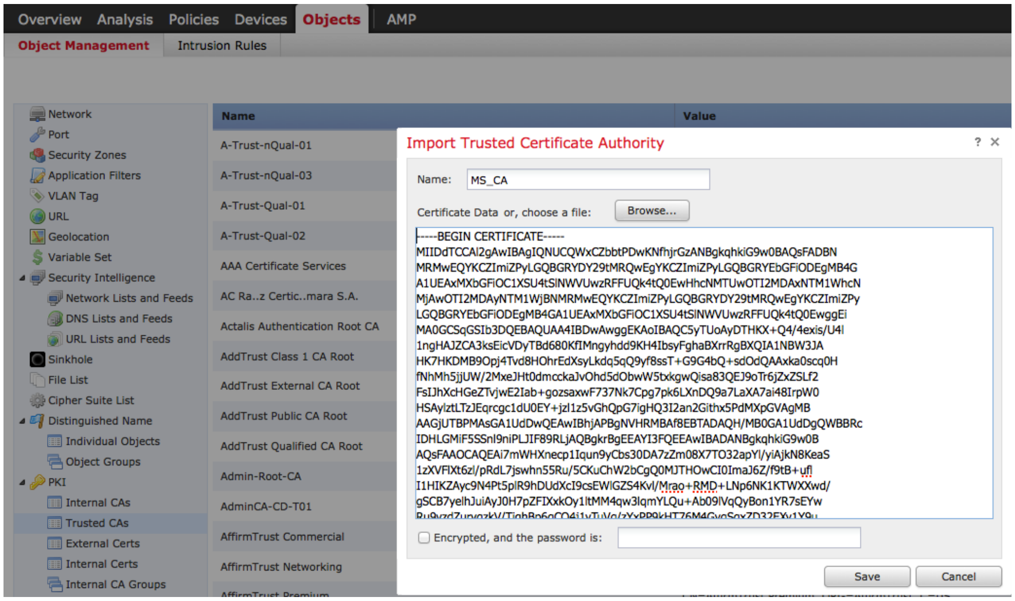
Current [lab8-WIN-JSVUL3DQTBN-CA]

Encoding method:

○ DER
● Base 64

Install CA certificate
Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

Step 9 Upload the CA root cert into the Firepower Management trusted CA store
Select **Objects->PKI->Trusted CAs->Add Trusted CA-> provide a name and upload root CA cert, then Save**



Import Trusted Certificate Authority

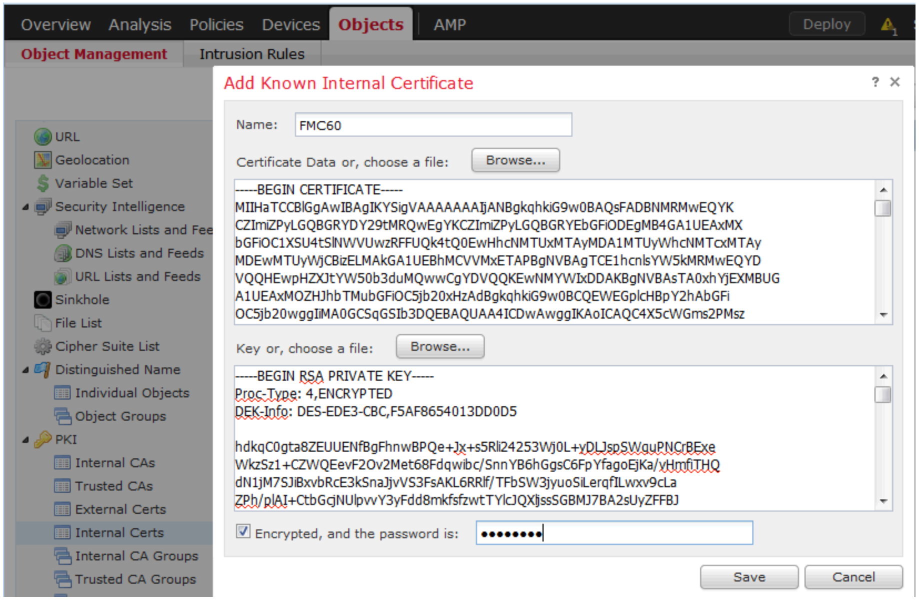
Name: MS_CA

Certificate Data or, choose a file:

```
-----BEGIN CERTIFICATE-----
MIIDdTCCAl2gAwIBAgIQNUCQWxCZbbtPDwKNfhjrGzANBgkqhkiG9w0BAQsFADBN
MRMwEQYKCZImiZPyLGQBGRYDY29tMRQwEgYKCZImiZPyLGQBGRYEbGFiODEgMB4G
A1UEAxMXbGFiOC1XSU4tSlNWVUwzRFFUQk4tQ0EwHhcNMTUwOTI2MDAxNTM1WhcN
MjAwOTI2MDAyNTM1WjBNMRMwEQYKCZImiZPyLGQBGRYDY29tMRQwEgYKCZImiZPy
LGQBGRYEbGFiODEgMB4GA1UEAxMXbGFiOC1XSU4tSlNWVUwzRFFUQk4tQ0EwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC5yTUoAyDTHKX+Q4/4exis/U4l
1ngHAJZCA3ksEicVDyTBd680KfIMngyhdd9KH4IbsyFghaBXrrRgBXQIA1NBW3JA
HK7HKDMB9Opj4Tvd8HOhrEdXsyLkdq5qQ9yf8ssT+G9G4bQ+sdOdQAAxka0scq0H
fNhMh5jjUW/2MxeJHt0dmcckaJvOhd5dObwW5txkgwQisa83QEJ9oTr6jZxZSLf2
FsIJhXcHGeZTvjwE2Iab+gozsaxwF737Nk7Cpg7pk6LXnDQ9a7LaXA7ai48IrpW0
HSAylztLTzJEqrcgc1dU0EY+jzl1z5vGhQpG7igHQ3I2an2Githx5PdMXpGVAgMB
AAGjUTBPMAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBRc
IDHLGMiF5SSnl9niPLJIF89RLjAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0B
AQsFAAOCAQEAi7mWHXnecp1Iqun9yCbs30DA7zZm08X7TO32apYl/yiAjkN8KeaS
1zXVFlXt6zl/pRdL7jswhn55Ru/5CKuChW2bCgQ0MJTHOwCI0ImaJ6Z/f9tB+ufl
I1HIKZAyc9N4Pt5plR9hDUdXcI9csEWlGZS4Kvl/Mrao+RMD+LNp6NK1KTWXXwd/
gSCB7yelhJuiAyJ0H7pZFIXxkOy1ltMM4qw3lqmYLQu+Ab09lVqQyBon1YR7sEYw
```

□ Encrypted, and the password is:

Step 10 Upload the Firepower Management center public certificate and private key to the FMC internal cert store
Select **Objects->PKI->Internal Certs->add the Sourcefire CER file and Sourcefire KEY files and password, then Save**



Add Known Internal Certificate

Name: FMC60

Certificate Data or, choose a file:

```
-----BEGIN CERTIFICATE-----
MIIHaTCCBlGgAwIBAgIKYSigVAAAAAAAIjANBgkqhkiG9w0BAQsFADBNMRMwEQYK
CZImiZPyLGQBGRYDY29tMRQwEgYKCZImiZPyLGQBGRYEbGFiODEgMB4GA1UEAxMX
bGFiOC1XSU4tSlNWVUwzRFFUQk4tQ0EwHhcNMTUxMTAyMDA1MTUyWhcNMTcxMTAy
MDEwMTUyWjCBizELMAkGA1UEBhMCVVMxETAPBgNVBAgTCE1hcnlsYW5kMRMwEQYD
VQQHEwpHZXJtYW50b3duMQwwCgYDVQQKEwNMYWIxDDAKBgNVBAsTA0xhYjEXMBUG
A1UEAxMOZHJhbTMubGFiOC5jb20xHzAdBgkqhkiG9w0BCQEWEGplcHBpY2hAbGFi
OC5jb20wggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQC4X5cWGms2PMsz
```

Key or, choose a file:

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,F5AF8654013DD0D5

hdkqC0gta8ZEUUENfBgFhnwBPQe+Jx+s5Rli24253Wj0L+yDLJspSWquPNCrBExe
WkzSz1+CZWQEevF2Ov2Met68Fdqwibc/SnnYB6hGgsC6FpYfagoEjKa/yHmfiTHQ
dN1jM7SJiBxvbRcE3kSnaJjvVS3FsAKL6RRlf/TFbSW3jyuoSiLerqfILwxv9cLa
ZPh/plAI+CtbGcjNUlpvvY3yFdd8mkfsfzwtTYlcJQXljssSGBMJ7BA2sUyZFFBJ
```

☑ Encrypted, and the password is: ••••••••

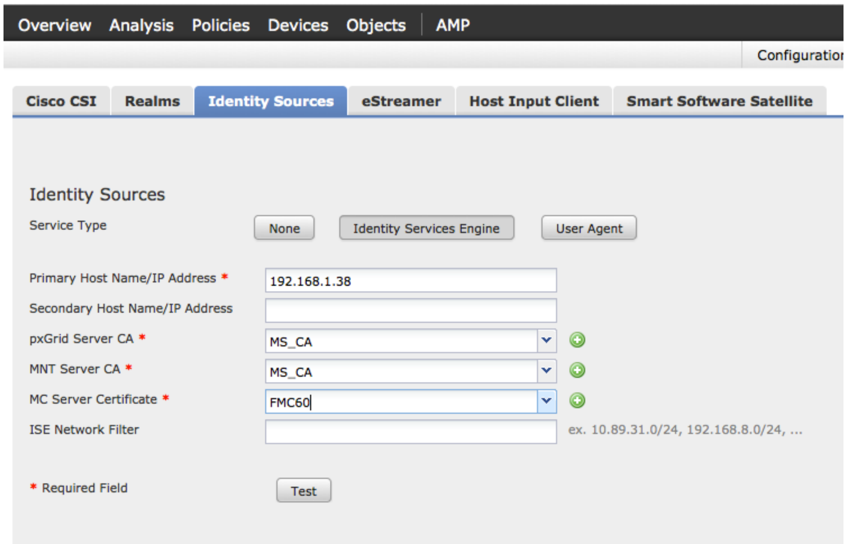
ISE Identity Sources CA-Signed Certificate Configuration

The Identity Sources Engine configuration defines the ISE pxGrid node connection parameters, ISE MnT node certificates and FMC identity certificate. Note that this configuration will be for a CA-signed environment for an ISE stand-alone environment.

Step 1 Select **System->Integration->Identity Sources->Identity Services Engine**

Primary Host Name/IP Address- primary FQDN pxGrid name or IP address
Secondary Host Name/IP address- secondary FQDN pxGrid name or IP address
**pxGrid Server CA*- root CA-signed both ISE pxGrid node and FMC
**mnt Server CA*- root CA-signed both ISE pxGrid node and FMC
MC Server Certificate- CA-signed identity certificate of FMC

**CA Signed Environment*

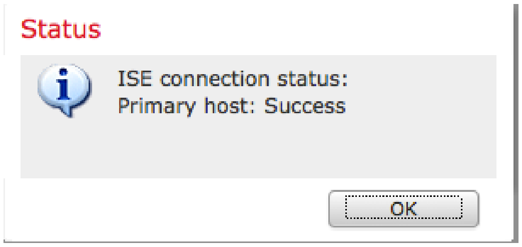


Identity Sources

Service Type	Identity Services Engine
Primary Host Name/IP Address *	192.168.1.38
Secondary Host Name/IP Address	
pxGrid Server CA *	MS_CA
MNT Server CA *	MS_CA
MC Server Certificate *	FMC60
ISE Network Filter	ex. 10.89.31.0/24, 192.168.8.0/24, ...

* Required Field

Step 2 Select **Test**
You should the following:

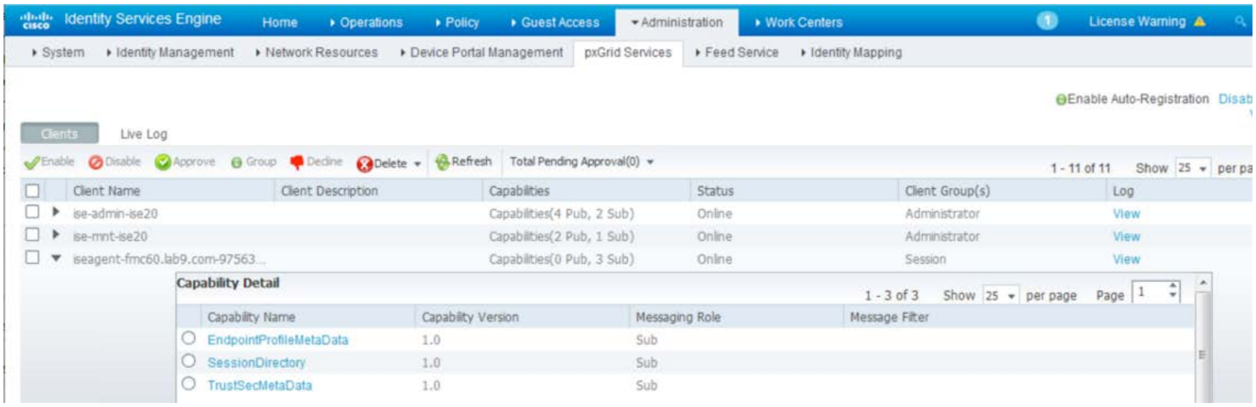


Status

ISE connection status:
Primary host: Success

Step 3 Select **Save**

Step 4 You should see the following on the ISE pxGrid node
Select **Administration->pxGrid Services**



☐		Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
☐	▸	ise-admin-ise20		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
☐	▸	ise-mnt-ise20		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
☐	▾	iseagent-fmc60.lab9.com-97563...		Capabilities(0 Pub, 3 Sub)	Online	Session	View

Capability Detail

	Capability Name	Capability Version	Messaging Role	Message Filter
○	EndpointProfileMetaData	1.0	Sub	
○	SessionDirectory	1.0	Sub	
○	TrustSecMetaData	1.0	Sub	

The FMC has successfully registered to the ISE pxGrid node and subscribed to the EndPointProfileMetada, SessionDirectory and TrustsecMetaData capabilities.

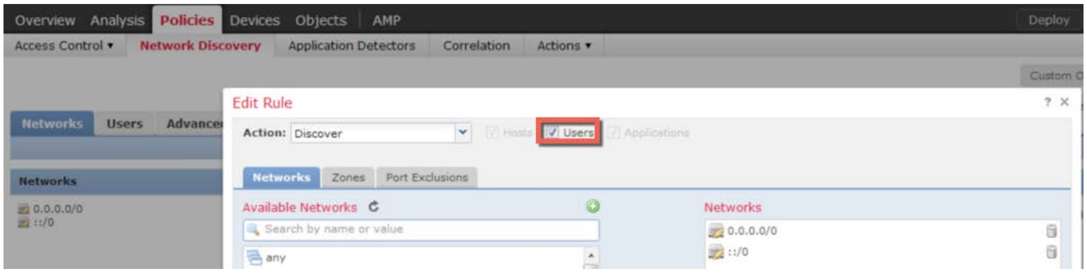
Firepower Management Center

Enabling Network Discovery

Enabling Network discovery provides user identity information

Step 1 Select Policies->Network Discovery->Edit Rule by clicking

Step 2 Enable Users

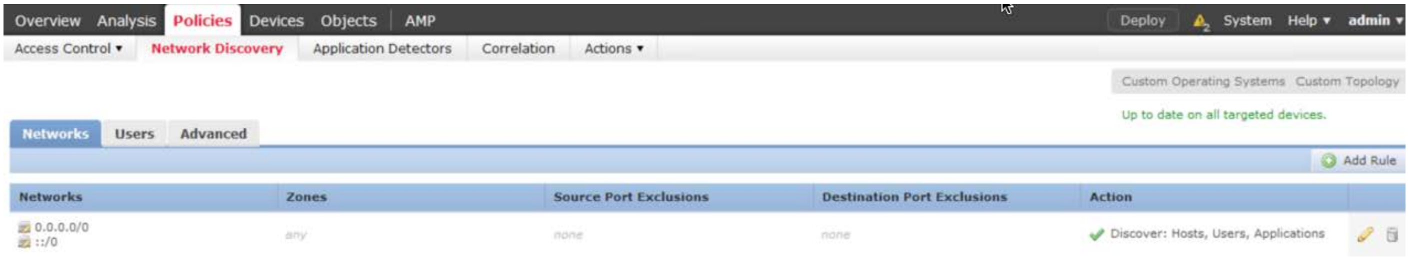


Action: Discover

☑ Hosts ☑ Users ☑ Applications

Step 3 Select **Save**

You should see the following



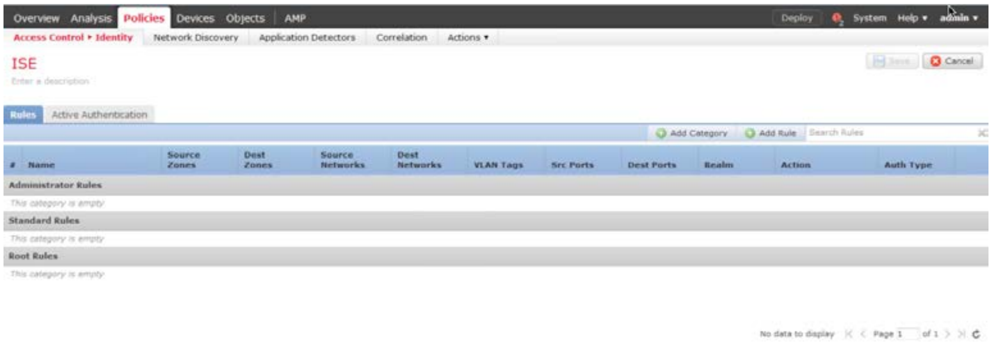
Networks	Zones	Source Port Exclusions	Destination Port Exclusions	Action
0.0.0.0/0 ::/0	any	none	none	✓ Discover: Hosts, Users, Applications

ISE Identity Policy

The ISE Identity policy is used in the Firepower Management center's default access control policy to allow passive ISE authentication.

Step 1 Select **Policies**->**Access Control**->**Identity**->**New Policy**->**New Identity Policy**->provide a name->**Save**

You should see the following:



ISE

Enter a description

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Src Ports	Dest Ports	Realm	Action	Auth Type
Administrator Rules											
This category is empty											
Standard Rules											
This category is empty											
Root Rules											
This category is empty											

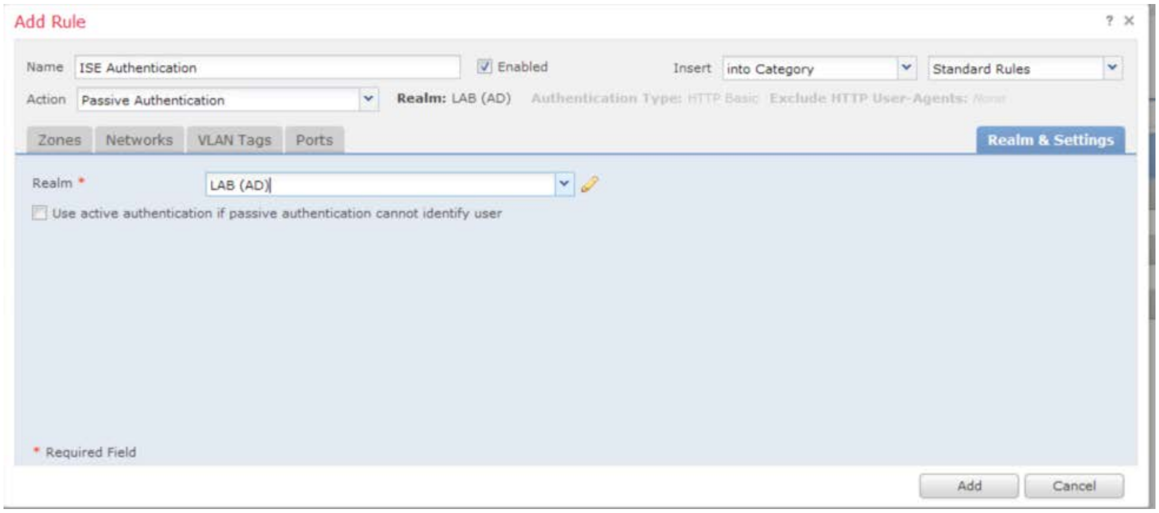
No data to display Page 1 of 1

Step 2 Select **Add Rule**

Step 3 Enter Name: **ISE Authentication**

Step 4 Enter Action: **Passive Authentication**

Step 5 Select **Realm**, then **Add,** select the ISE realm you defined earlier
You should see the following below



Name: ISE Authentication ☑ Enabled Insert: into Category Standard Rules

Action: Passive Authentication **Realm:** LAB (AD) Authentication Type: HTTP Basic Exclude HTTP User-Agents: None

Realm *: LAB (AD)

□ Use active authentication if passive authentication cannot identify user

* Required Field

Step 6 **Save** the changes

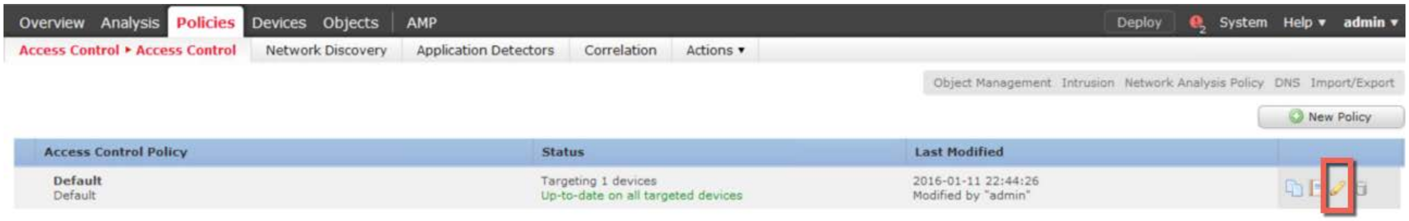
Default Access Control Policy

The default access control policy contains the ISE identity policy, the transport/network layer/preprocessor settings to block transactions, access control rules and Firepower Management Center’s intrusion policies.

Adding ISE Identity Policy

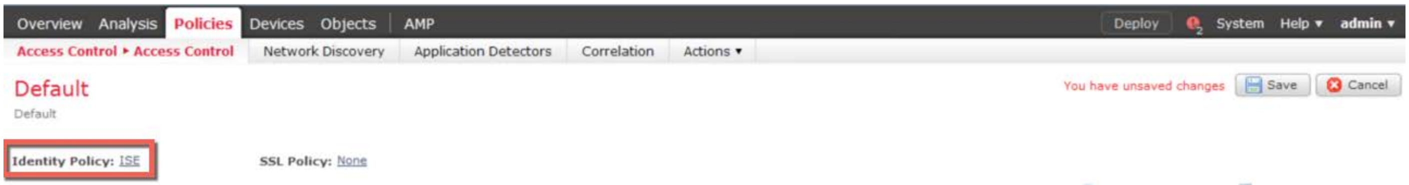
Add the ISE identity policy to the default access policy

Step 1 Select **Policies->Access Control->edit the default access policy**



Access Control Policy	Status	Last Modified
Default Default	Targeting 1 devices Up-to-date on all targeted devices	2016-01-11 22:44:26 Modified by "admin"

Step 2 Click **None -> Identity Policy** select ISE from the drop-down menu



Default

Default

Identity Policy: ISE

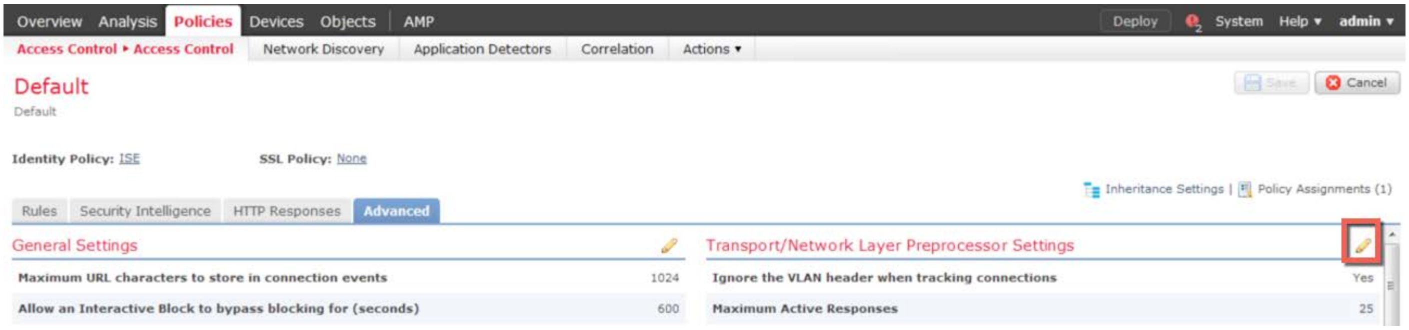
SSL Policy: None

Step 3 Select **Save**

Transport/Network Layer Preprocessor Settings

These settings were modified to for blocking traffic enforced by the Firepower managed intrusion policy.

Step 1 Edit the Transport/Network Layer/Preprocessor Settings



Default

Default

Identity Policy: ISE

SSL Policy: None

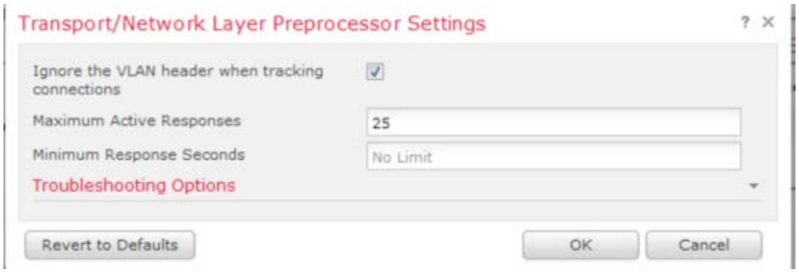
General Settings

Maximum URL characters to store in connection events	1024
Allow an Interactive Block to bypass blocking for (seconds)	600

Transport/Network Layer Preprocessor Settings

Ignore the VLAN header when tracking connections	Yes
Maximum Active Responses	25

Step 2 Provide the following settings



Transport/Network Layer Preprocessor Settings

Ignore the VLAN header when tracking connections ☑

Maximum Active Responses: 25

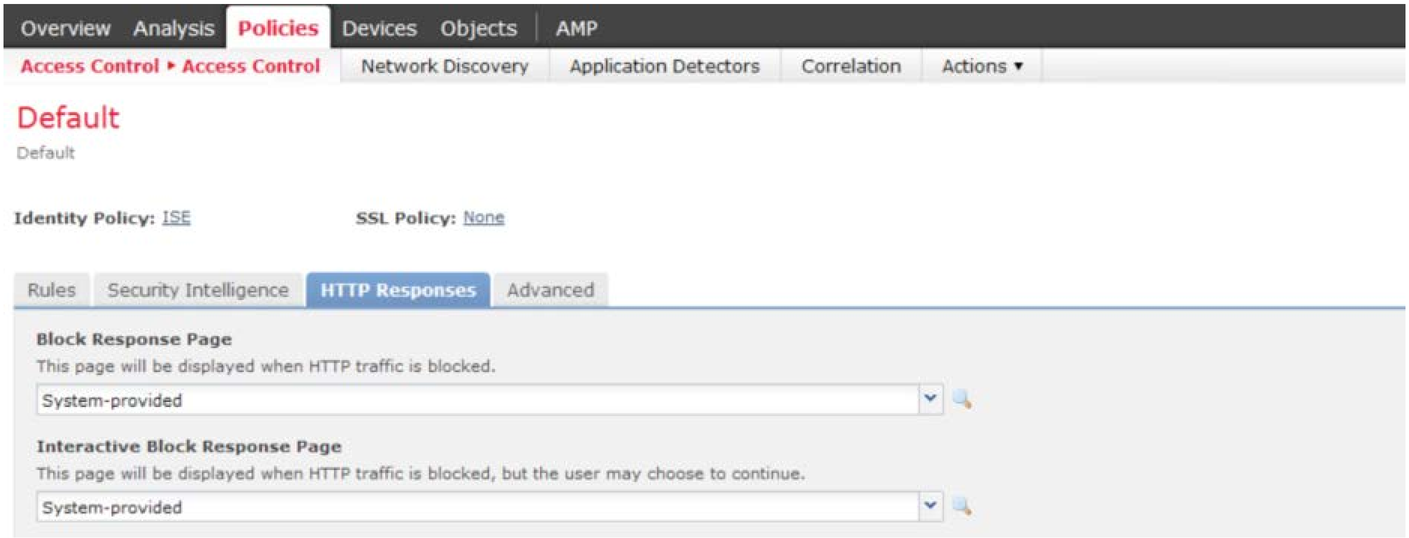
Minimum Response Seconds: No Limit

Step 3 Select ->Ok

Adding Block Response Page

The system-provided block response page will be added to the blocked web categories based on Firepower Management Center's access control policy.

Step 1 Select **HTTP Responses,** and provide the following settings for the response pages



Default

Default

Identity Policy: ISE   SSL Policy: None

Block Response Page

This page will be displayed when HTTP traffic is blocked.

System-provided

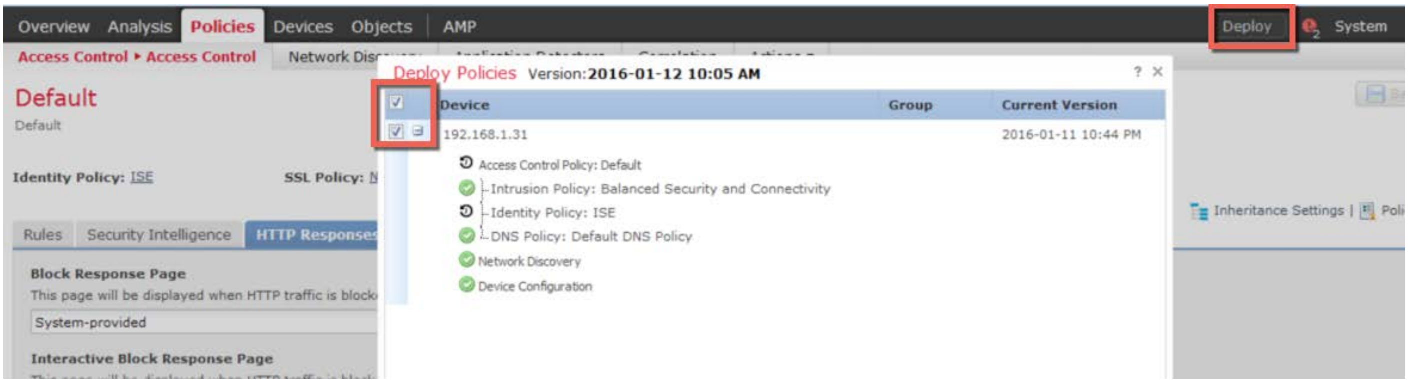
Interactive Block Response Page

This page will be displayed when HTTP traffic is blocked, but the user may choose to continue.

System-provided

Step 2 **Save** the changes

Step 3 Select **Deploy,** and **deploy** the changes to the sensor


Overview Analysis Policies Devices Objects AMP
Deploy
System
Access Control ▸ Access Control
Network Disc
Rules Security Intelligence HTTP Responses
Inheritance Settings | Poli

Default
Default

Identity Policy: ISE SSL Policy: N

Block Response Page
This page will be displayed when HTTP traffic is block
System-provided

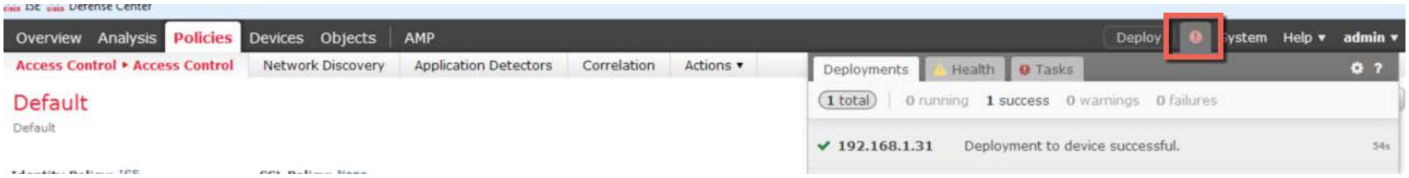
Interactive Block Response Page

Deploy Policies Version:2016-01-12 10:05 AM

☑	Device	Group	Current Version
☑	192.168.1.31		2016-01-11 10:44 PM

- Access Control Policy: Default
- Intrusion Policy: Balanced Security and Connectivity
- Identity Policy: ISE
- DNS Policy: Default DNS Policy
- Network Discovery
- Device Configuration

Step 4 Select the Deploy status bar to see the progress



Default
Default

1 total 0 running 1 success 0 warnings 0 failures

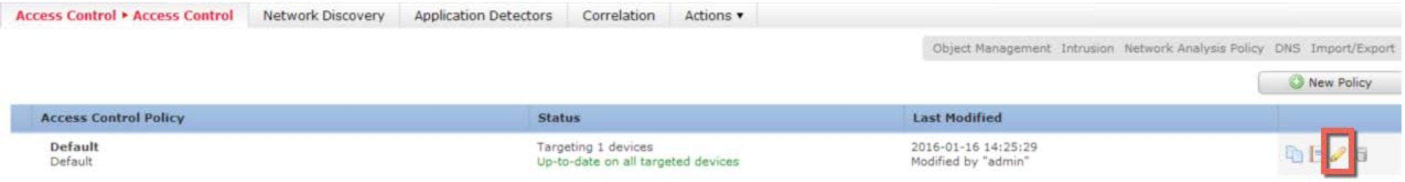
✓ 192.168.1.31 Deployment to device successful. 54s

Create Employee SGT tag Access Control rules

An Employee SGT access control policy will be created simulating an organization's acceptable usage policy.

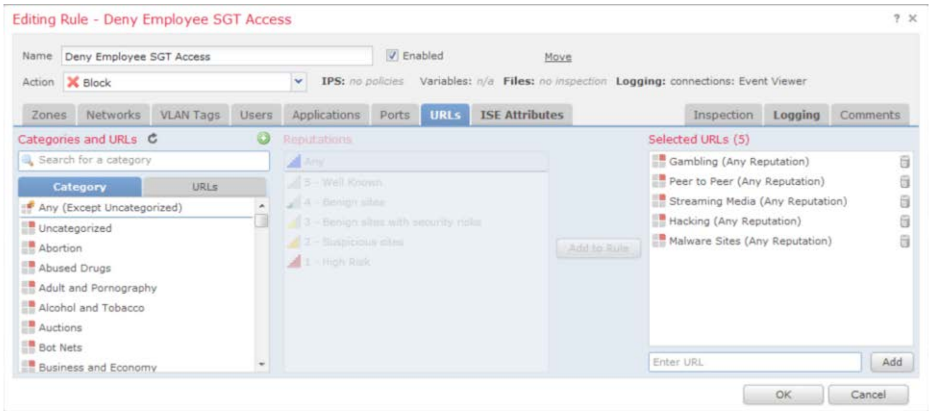
This acceptable usage policy will deny users access to gambling sites, hacking sites, streaming media, social media and peer-to-peer applications.

Step 1 Select **Policies->Access Control->Access Control->Rules**, edit clicking on ✎


Access Control ▸ Access Control
Network Discovery
Application Detectors
Correlation
Actions ▾
Object Management Intrusion Network Analysis Policy DNS Import/Export
New Policy

Access Control Policy	Status	Last Modified
Default Default	Targeting 1 devices Up-to-date on all targeted devices	2016-01-16 14:25:29 Modified by "admin"

Step 2 Select->**Add Rule, enter name: Deny Employee SGT Access->action->Block->IPS->pxGrid intrusion policy->URLs->Category>Gambling, Peer-to-Peer, Streaming Video, Hacking->Add to Rule**



Editing Rule - Deny Employee SGT Access

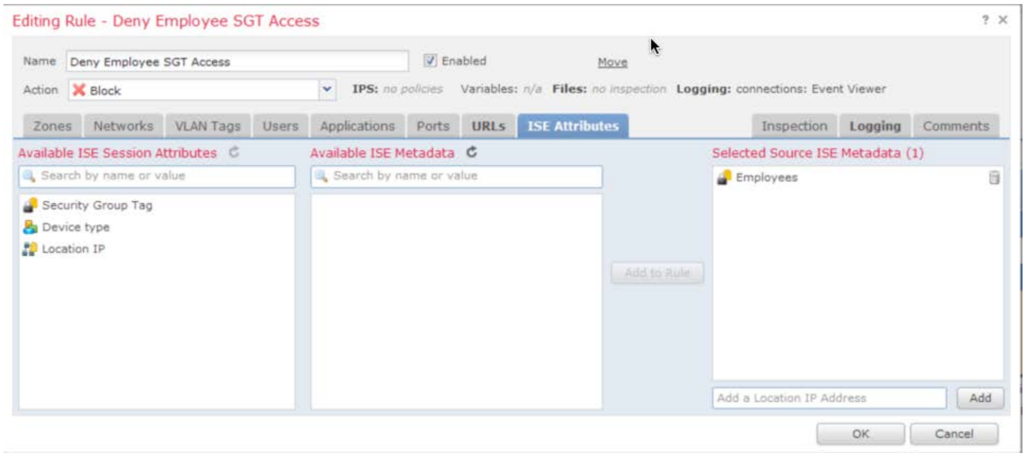
Name: Deny Employee SGT Access ☑ Enabled Move

Action: Block IPS: no policies Variables: n/a Files: no inspection Logging: connections: Event Viewer

Selected URLs (5)

- Gambling (Any Reputation)
- Peer to Peer (Any Reputation)
- Streaming Media (Any Reputation)
- Hacking (Any Reputation)
- Malware Sites (Any Reputation)

Step 3 Select ISE Attributes->**Available ISE session attributes->Security Group Tag->Available Metadata->Employees->Add to rule**



Editing Rule - Deny Employee SGT Access

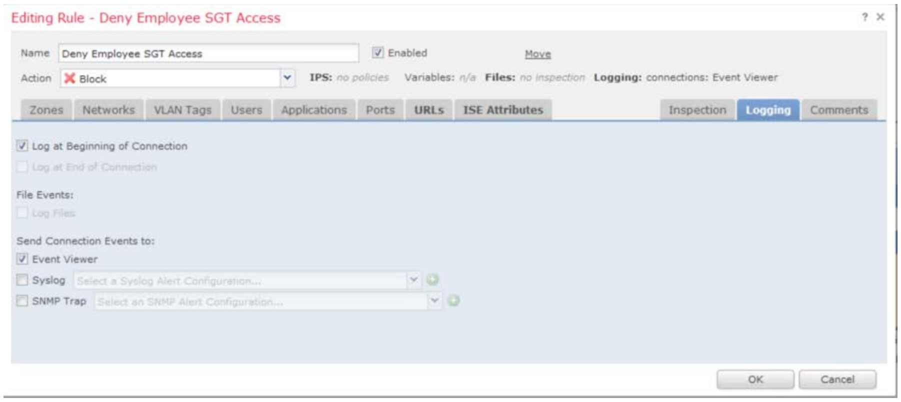
Name: Deny Employee SGT Access ☑ Enabled Move

Action: Block IPS: no policies Variables: n/a Files: no inspection Logging: connections: Event Viewer

Selected Source ISE Metadata (1)

- Employees

Step 4 Select **Logging and configure the following settings**



Editing Rule - Deny Employee SGT Access

Name: Deny Employee SGT Access ☑ Enabled Move

Action: Block IPS: no policies Variables: n/a Files: no inspection Logging: connections: Event Viewer

☑ Log at Beginning of Connection

□ Log at End of Connection

File Events:

□ Log Files

Send Connection Events to:

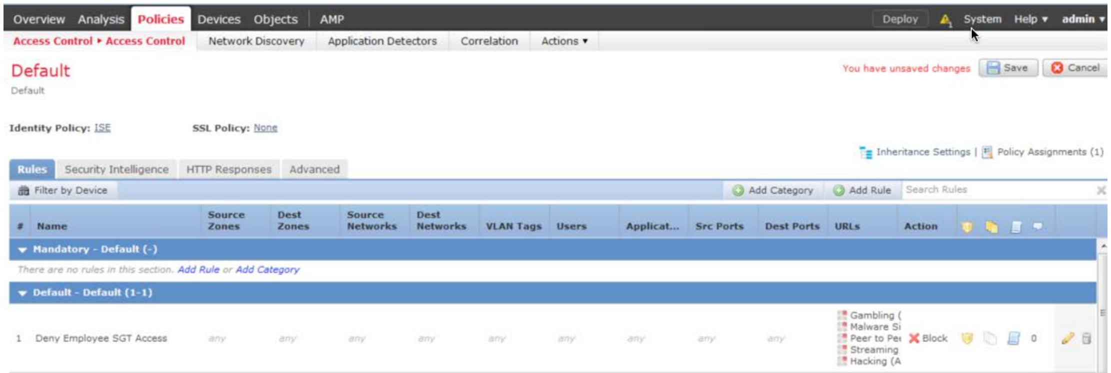
☑ Event Viewer

□ Syslog Select a Syslog Alert Configuration...

□ SNMP Trap Select an SNMP Alert Configuration...

Step 5 Select **OK**

You should see the following



Default
Default

You have unsaved changes

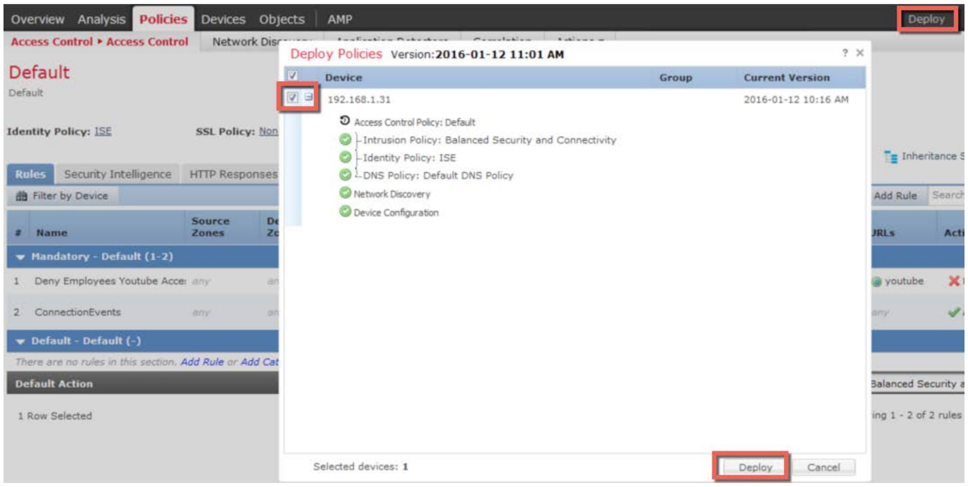
Identity Policy: ISE SSL Policy: None

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Src Ports	Dest Ports	URLs	Action
▾ Mandatory - Default (-)												
There are no rules in this section. Add Rule or Add Category												
▾ Default - Default (1-1)												
1	Deny Employee SGT Access	any	any	any	any	any	any	any	any	any	Gambling (Malware Si Peer to Pe Streaming Hacking (A	✗ Block

Step 6 Select **Save**

Step 7 Deploy the changes to the sensor

Select **Deploy->sensor->Deploy**



Default
Default

Identity Policy: ISE SSL Policy: Non

Deploy Policies Version:2016-01-12 11:01 AM

☑	Device	Group	Current Version
☑	192.168.1.31		2016-01-12 10:16 AM

- Access Control Policy: Default
  - Intrusion Policy: Balanced Security and Connectivity
  - Identity Policy: ISE
  - DNS Policy: Default DNS Policy
- Network Discovery
- Device Configuration

Selected devices: 1

#	Name	Source Zones	URLs	Acti
▾ Mandatory - Default (1-2)				
1	Deny Employees Youtube Acce:	any	youtube	✗
2	ConnectionEvents	any	any	✓
▾ Default - Default (-)				
There are no rules in this section. Add Rule or Add Cat				

Default Action Balanced Security a

1 Row Selected ing 1 - 2 of 2 rules

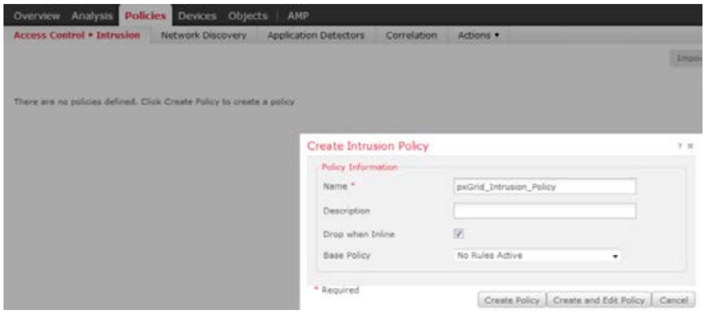
Step 8 Click on , to see Task Status, and verify that the operation has succeeded.

Firepower pxGrid Intrusion Policy

The pxGrid Intrusion Policy is created and deployed to the Firepower NGIPS virtual 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 trigger an intrusion event that will be dropped in line and event generated to the Firepower Management Console under Analysis Intrusion Events. In this document, the pxGrid intrusion policy will also centrally manage the ASA with Firepower Services.

In this document, this policy will also be created on-box via ASDM with ASA with Firepower services.

Step 1 Select Policies **Intrusion->Intrusion Policy->Create Policy->pxGrid_Intrusion_Policy**, enable **Drop when Inline**



There are no policies defined. Click Create Policy to create a policy

Create Intrusion Policy

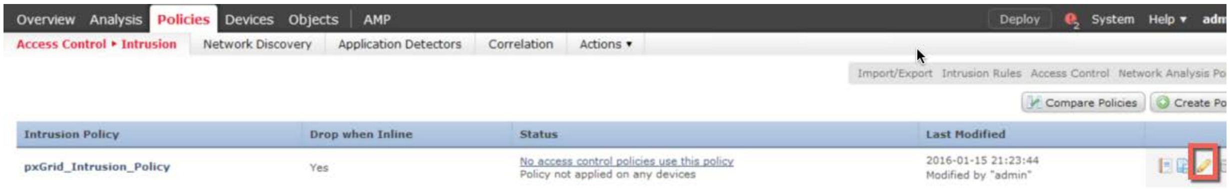
Policy Information

Name *	pxGrid_Intrusion_Policy
Description	
Drop when Inline	☑
Base Policy	No Rules Active

* Required

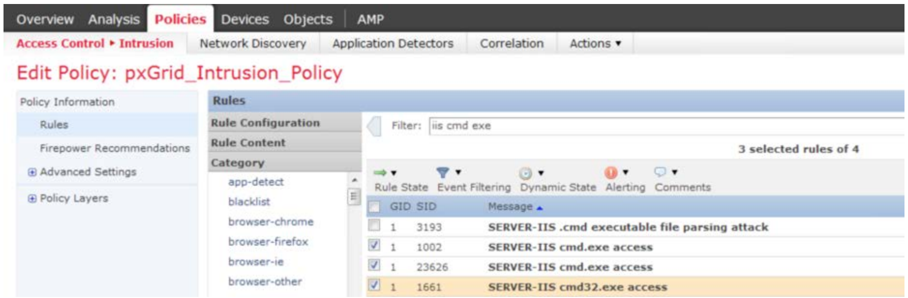
Step 2 Click **Create Policy**

Step 3 Edit the policy by clicking on ✎



Intrusion Policy	Drop when Inline	Status	Last Modified
pxGrid_Intrusion_Policy	Yes	No access control policies use this policy Policy not applied on any devices	2016-01-15 21:23:44 Modified by "admin"

Step 4 Click on **Rules->filter: iis cmd exe** and select the following



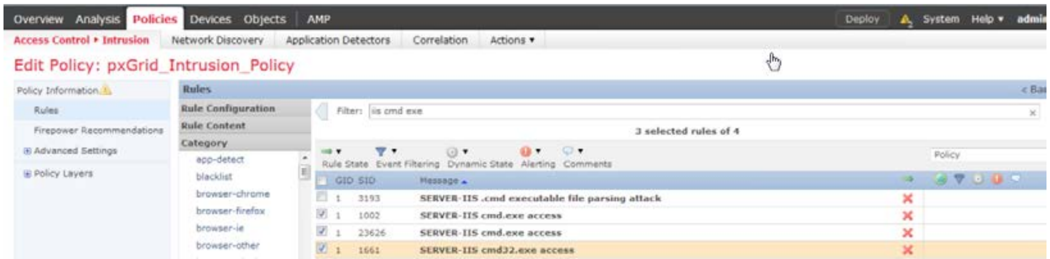
Edit Policy: pxGrid_Intrusion_Policy

Filter: iis cmd exe

3 selected rules of 4

	GID	SID	Message ▴
☐	1	3193	SERVER-IIS .cmd executable file parsing attack
☑	1	1002	SERVER-IIS cmd.exe access
☑	1	23626	SERVER-IIS cmd.exe access
☑	1	1661	SERVER-IIS cmd32.exe access

Step 5 Click **Rule State->Drop and Generate Events->OK**
You should see the following:



Edit Policy: pxGrid_Intrusion_Policy

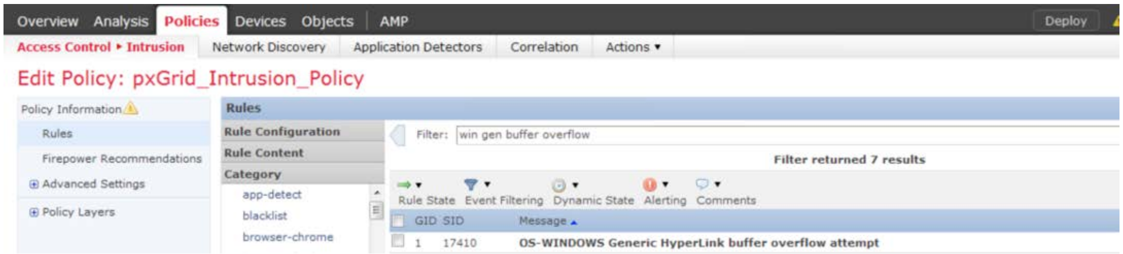
Rules

Filter: iis cmd exe

3 selected rules of 4

	GID	SID	Message ▴	
□	1	3193	SERVER-IIS .cmd executable file parsing attack	✕
☑	1	1002	SERVER-IIS cmd.exe access	✕
☑	1	23626	SERVER-IIS cmd.exe access	✕
☑	1	1661	SERVER-IIS cmd32.exe access	✕

Step 6 Next filter on: **win gen buffer overflow** and select**->OS-Windows Generic Hyperlink BufferOverflow Attempt**



Edit Policy: pxGrid_Intrusion_Policy

Rules

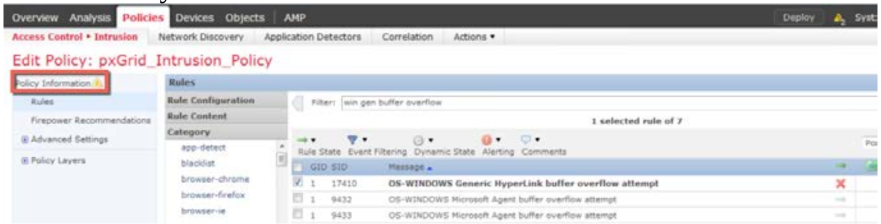
Filter: win gen buffer overflow

Filter returned 7 results

	GID	SID	Message ▴
□	1	17410	OS-WINDOWS Generic HyperLink buffer overflow attempt

Step 7 Rule State**->Drop and Generate Events->OK**

Step 8 Click Policy Information



Edit Policy: pxGrid_Intrusion_Policy

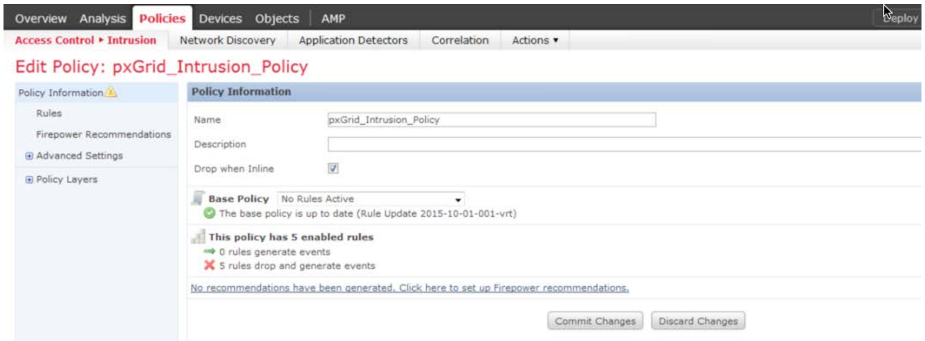
Rules

Filter: win gen buffer overflow

1 selected rule of 7

	GID	SID	Message ▴	
☑	1	17410	OS-WINDOWS Generic HyperLink buffer overflow attempt	✕
□	1	9432	OS-WINDOWS Microsoft Agent buffer overflow attempt	⇒
□	1	9433	OS-WINDOWS Microsoft Agent buffer overflow attempt	⇒

Step 9 You should see the following:



Edit Policy: pxGrid_Intrusion_Policy

Policy Information

Name: pxGrid_Intrusion_Policy

Description:

Drop when Inline ☑

Base Policy: No Rules Active

The base policy is up to date (Rule Update 2015-10-01-001-vrt)

This policy has 5 enabled rules

⇒ 0 rules generate events

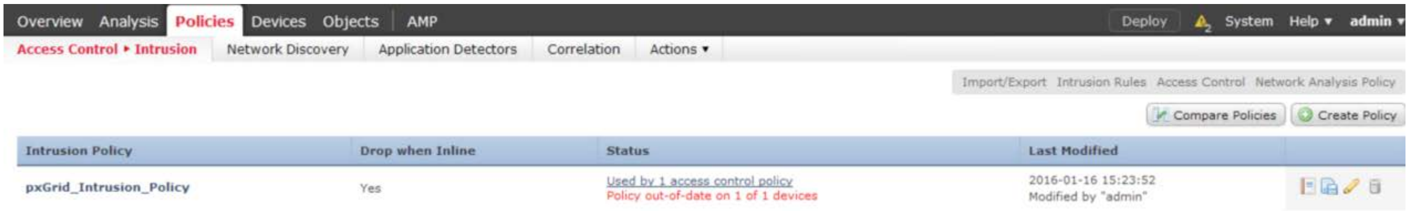
✕ 5 rules drop and generate events

No recommendations have been generated. Click here to set up Firepower recommendations.

Step 10 Select **Commit Changes**

Step 11 Click OK

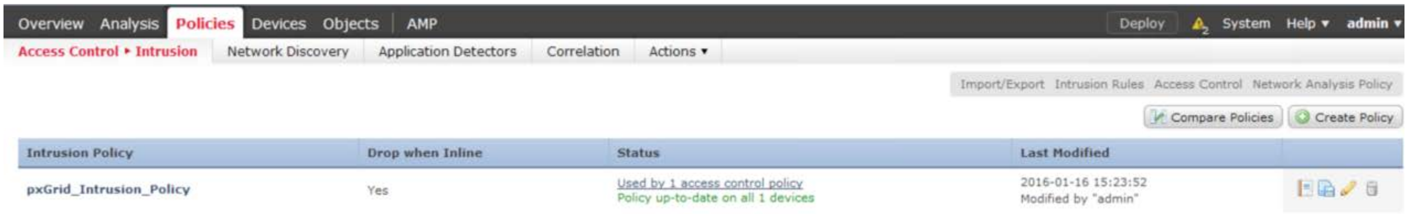
You should see the following



Intrusion Policy	Drop when Inline	Status	Last Modified
pxGrid_Intrusion_Policy	Yes	Used by 1 access control policy Policy out-of-date on 1 of 1 devices	2016-01-16 15:23:52 Modified by "admin"

Step 12 Select Deploy, the sensor, and Deploy again

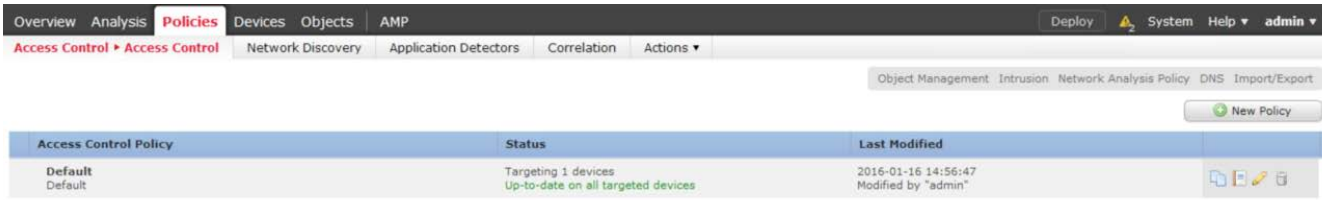
Step 13 Select **Policies->Access Control->Intrusion Access Control**, you should see the following:



Intrusion Policy	Drop when Inline	Status	Last Modified
pxGrid_Intrusion_Policy	Yes	Used by 1 access control policy Policy up-to-date on all 1 devices	2016-01-16 15:23:52 Modified by "admin"

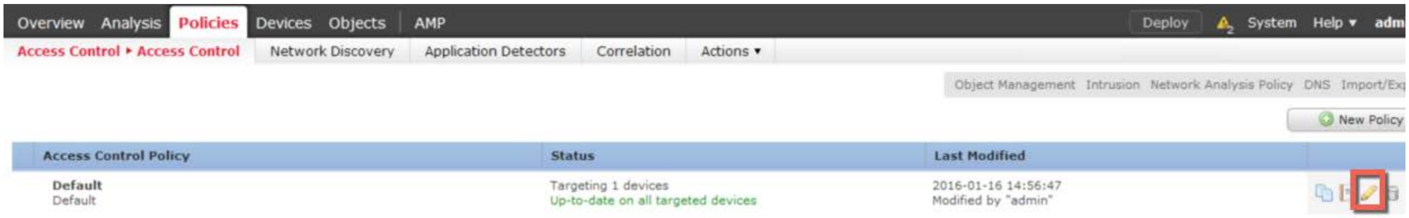
Step 14 Select **Policies->Access Control->Access Control**

You should see the default access policy



Access Control Policy	Status	Last Modified
Default Default	Targeting 1 devices Up-to-date on all targeted devices	2016-01-16 14:56:47 Modified by "admin"

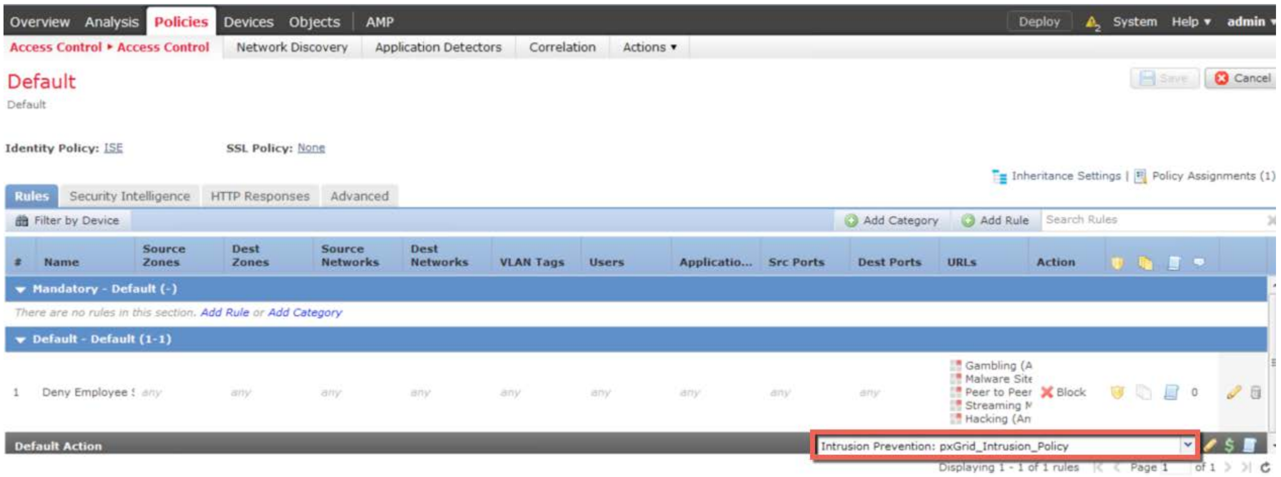
Step 15 Edit the default access policy by clicking on ✎



Access Control Policy	Status	Last Modified
Default Default	Targeting 1 devices Up-to-date on all targeted devices	2016-01-16 14:56:47 Modified by "admin"

Step 16 Under Default actions, from the dropdown select the pxGrid_Intrusion_Policy

You should see the following



Default

Default

Identity Policy: ISE SSL Policy: None

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicatio...	Src Ports	Dest Ports	URLs	Action
▾ Mandatory - Default (-)												
There are no rules in this section. Add Rule or Add Category												
▾ Default - Default (1-1)												
1	Deny Employee !	any	any	any	any	any	any	any	any	any	Gambling (A Malware Site Peer to Peer Streaming M Hacking (An	✖ Block

Default Action: Intrusion Prevention: pxGrid_Intrusion_Policy

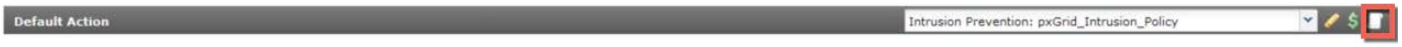
Displaying 1 - 1 of 1 rules Page 1 of 1

Note: you may be prompted to add access control policies. These will be added later on based on the Employee SGT

Step 17 Click **Save**

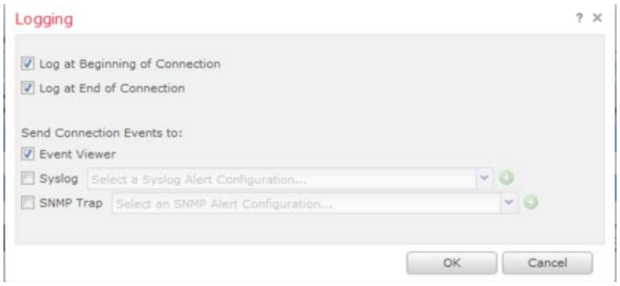
Step 18 Edit the SGT Access control policy to include the pxGrid Intrusion Policy

Step 19 Click on **Logging**, by clicking on



Default Action: Intrusion Prevention: pxGrid_Intrusion_Policy

Step 20 Configure the following settings->**OK**



Logging

☑ Log at Beginning of Connection

☑ Log at End of Connection

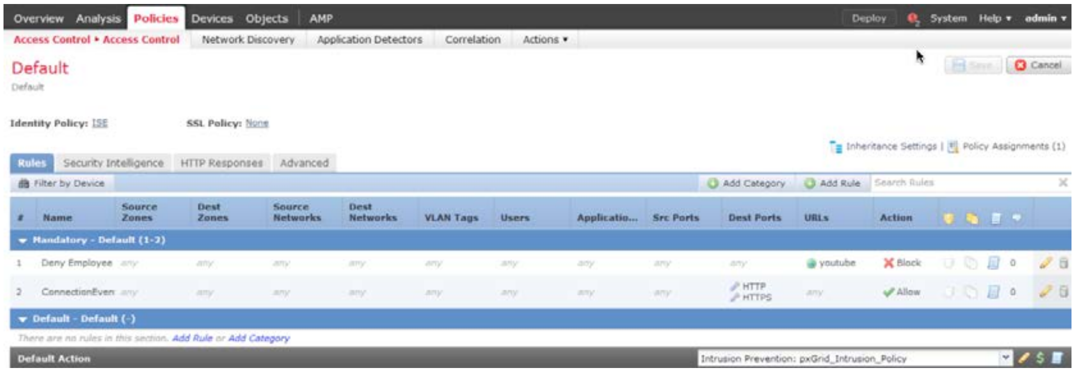
Send Connection Events to:

☑ Event Viewer

☐ Syslog Select a Syslog Alert Configuration...

☐ SNMP Trap Select an SNMP Alert Configuration...

Step 21 Click **Save**



Default

Default

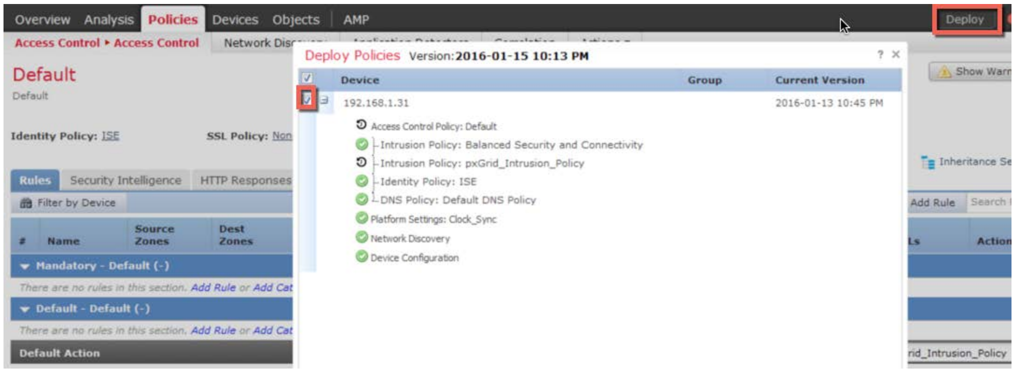
Identity Policy: ISE SSL Policy: None

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicatio...	Src Ports	Dest Ports	URLs	Action
Mandatory - Default (1-2)												
1	Deny Employee	any	any	any	any	any	any	any	any	any	youtube	✗ Block
2	ConnectionEven	any	any	any	any	any	any	any	any	HTTP HTTPS	any	✓ Allow
Default - Default (-)												

There are no rules in this section. Add Rule or Add Category

Default Action: Intrusion Prevention: pxGrid_Intrusion_Policy

Step 22 Click **Deploy,** select the device



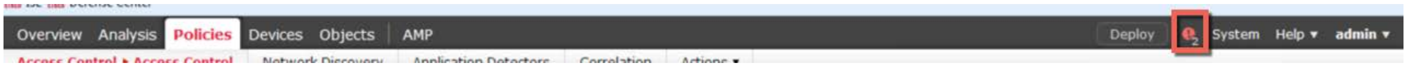
Deploy Policies Version:**2016-01-15 10:13 PM**

☑	Device	Group	Current Version
☑	192.168.1.31		2016-01-13 10:45 PM

- Access Control Policy: Default
  - Intrusion Policy: Balanced Security and Connectivity
  - Intrusion Policy: pxGrid_Intrusion_Policy
  - Identity Policy: ISE
  - DNS Policy: Default DNS Policy
- Platform Settings: Clock_Sync
- Network Discovery
- Device Configuration

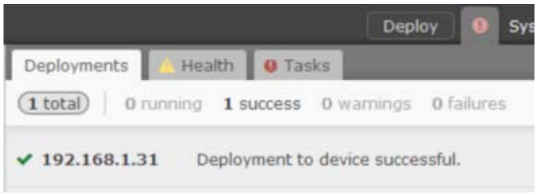
Step 23 Select **Deploy**

Step 24 Click on , to see Task Status



Note: Click on Task Status to see deployment cycle status

You should see deployment to the sensor as successful



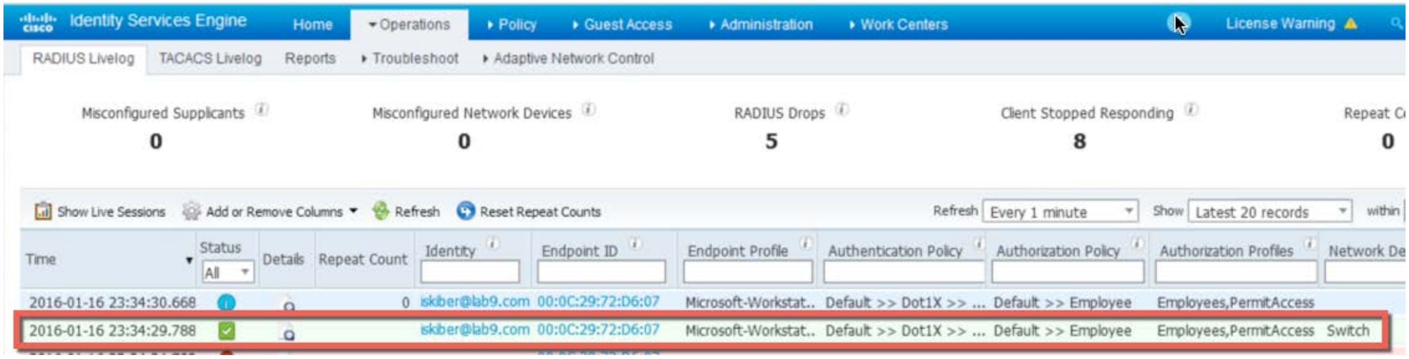
1 total | 0 running 1 success 0 warnings 0 failures

✓ 192.168.1.31 Deployment to device successful.

Testing User with Employee SGT via Firepower Virtual Sensor

In this use case, the end-user is assigned an Employee SGT and received the Firepower Management Center's access control policy, denying SGT tagged employees access to hacking sites, gambling sites, peer-to-peer applications, streaming media applications. Also the intrusion policy is enforced and access to compromised web servers are denied.

The end-user successfully authenticates via IEEE 802.1X and is assigned an Employee SGT as shown below

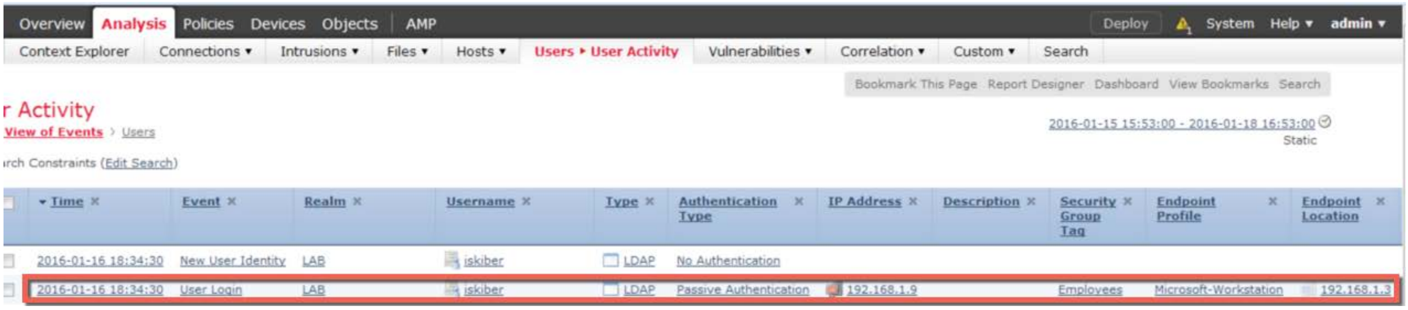


Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat C
0	0	5	8	0

Refresh Every 1 minute Show Latest 20 records within

Time	Status All	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network De
2016-01-16 23:34:30.668	●		0	iskiber@lab9.com	00:0C:29:72:D6:07	Microsoft-Workstat..	Default >> Dot1X >> ...	Default >> Employee	Employees,PermitAccess	
2016-01-16 23:34:29.788	☑			iskiber@lab9.com	00:0C:29:72:D6:07	Microsoft-Workstat..	Default >> Dot1X >> ...	Default >> Employee	Employees,PermitAccess	Switch

Firepower Management Center 6.0 obtains the ISE session information and displays the information in the User Activity Screen



r Activity

View of Events › Users

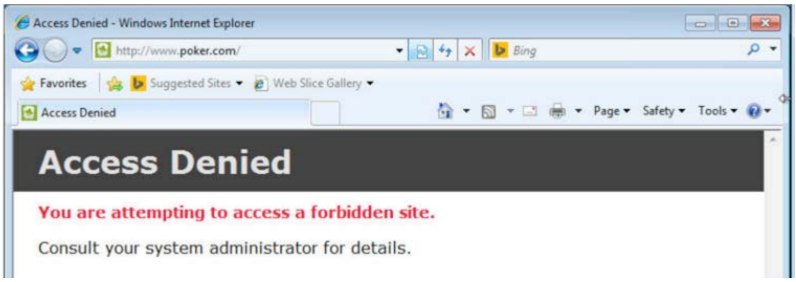
2016-01-15 15:53:00 - 2016-01-18 16:53:00
Static

ırch Constraints (Edit Search)

Time	Event	Realm	Username	Type	Authentication Type	IP Address	Description	Security Group Tag	Endpoint Profile	Endpoint Location
2016-01-16 18:34:30	New User Identity	LAB	iskiber	LDAP	No Authentication					
2016-01-16 18:34:30	User Login	LAB	iskiber	LDAP	Passive Authentication	192.168.1.9		Employees	Microsoft-Workstation	192.168.1.3

Note the ISE session attributes: username, security group tag, endpoint profile and endpoint location. The security group tag attribute was used to create a FMC access control policy.

The end-user opens their browser and accesses poker.com. Note the blocked transaction and the Firepower Management Center displayed page.



Access Denied - Windows Internet Explorer

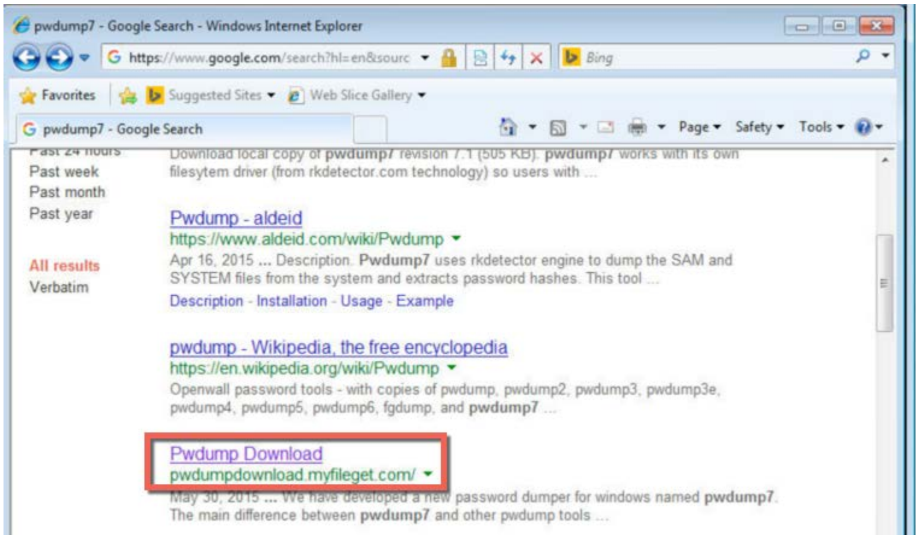
http://www.poker.com/

Access Denied

You are attempting to access a forbidden site.

Consult your system administrator for details.

The end-user opens their browser and wants to download pwdump7.



pwdump7 - Google Search - Windows Internet Explorer

https://www.google.com/search?hl=en&sourc

Past 24 hours
Past week
Past month
Past year

All results
Verbatim

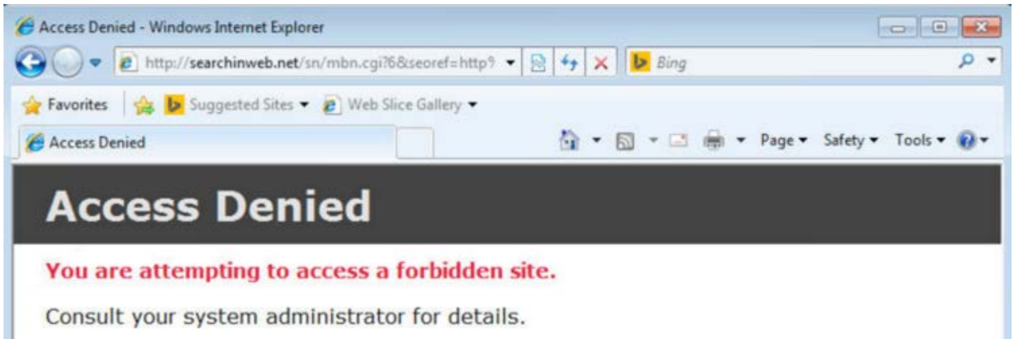
Download local copy of **pwdump7** revision 7.1 (505 KB). **pwdump7** works with its own filesytem driver (from rkdetector.com technology) so users with ...

Pwdump - aldeid
https://www.aldeid.com/wiki/Pwdump
Apr 16, 2015 ... Description. **Pwdump7** uses rkdetector engine to dump the SAM and SYSTEM files from the system and extracts password hashes. This tool ...
Description - Installation - Usage - Example

pwdump - Wikipedia, the free encyclopedia
https://en.wikipedia.org/wiki/Pwdump
Openwall password tools - with copies of pwdump, pwdump2, pwdump3, pwdump3e, pwdump4, pwdump5, pwdump6, fgdump, and **pwdump7** ...

Pwdump Download
pwdumpdownload.myfileget.com/
May 30, 2015 ... We have developed a new password dumper for windows named **pwdump7**. The main difference between **pwdump7** and other pwdump tools ...

The end-user is redirected to the web page and is denied access



Access Denied - Windows Internet Explorer

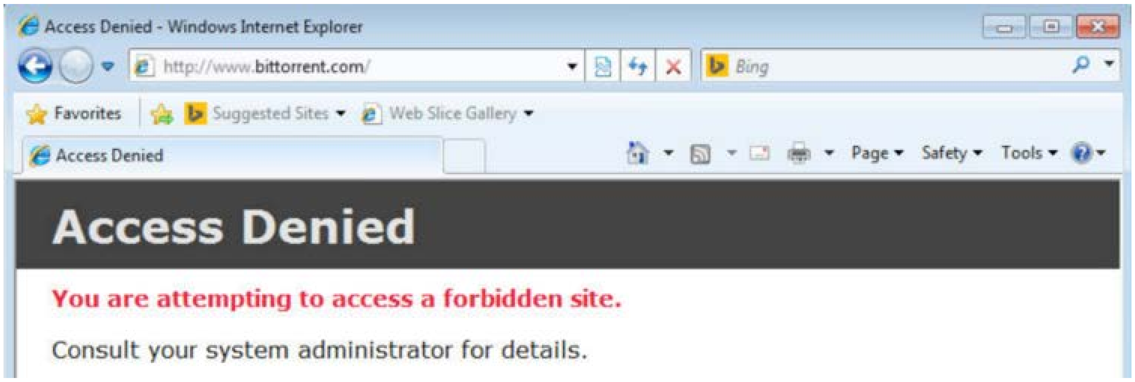
http://searchinweb.net/sn/mbn.cgi?6&seoref=http?

Access Denied

You are attempting to access a forbidden site.

Consult your system administrator for details.

The end-user attempts to access bittorrent and is denied access.

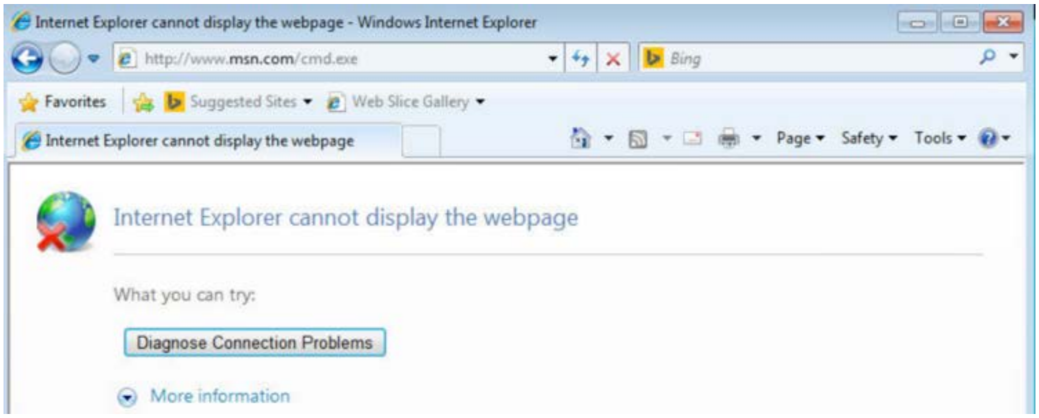


Access Denied

You are attempting to access a forbidden site.

Consult your system administrator for details.

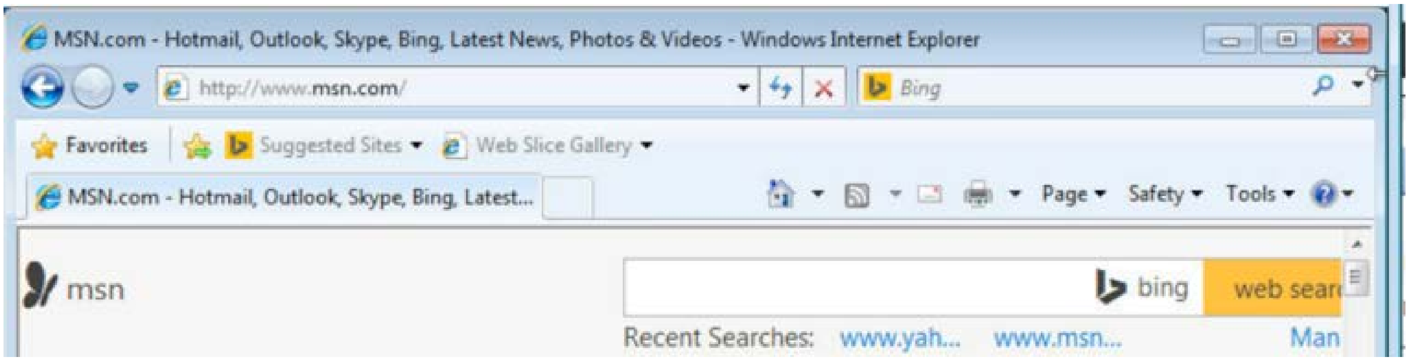
The end-user inserts cmd.exe into the website to simulate a compromised web server and is denied access


Internet Explorer cannot display the webpage - Windows Internet Explorer
http://www.msn.com/cmd.exe
Bing
Favorites
Suggested Sites
Web Slice Gallery
Internet Explorer cannot display the webpage
Page
Safety
Tools
Diagnose Connection Problems
More information

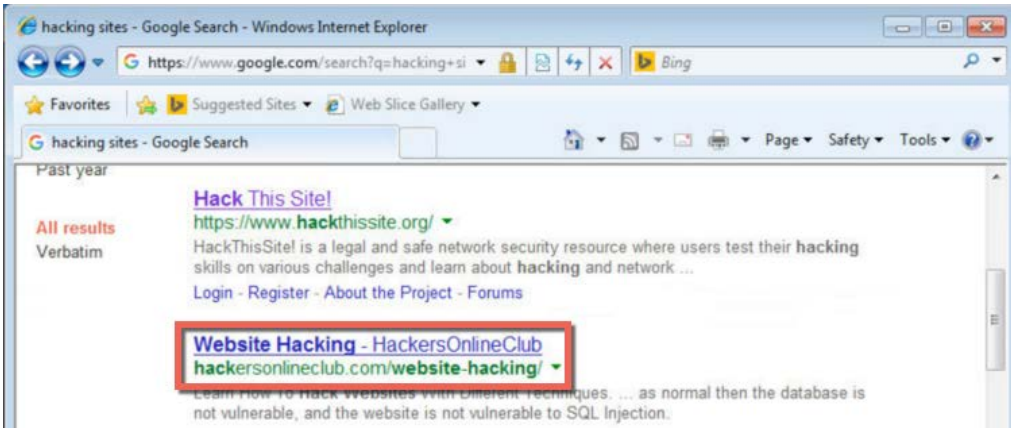
Internet Explorer cannot display the webpage

What you can try:

Just to prove that all is well. The end-user can access a valid website


MSN.com - Hotmail, Outlook, Skype, Bing, Latest News, Photos & Videos - Windows Internet Explorer
http://www.msn.com/
Bing
Favorites
Suggested Sites
Web Slice Gallery
MSN.com - Hotmail, Outlook, Skype, Bing, Latest...
Page
Safety
Tools
msn
bing
web searc
Recent Searches:
www.yah...
www.msn...
Man

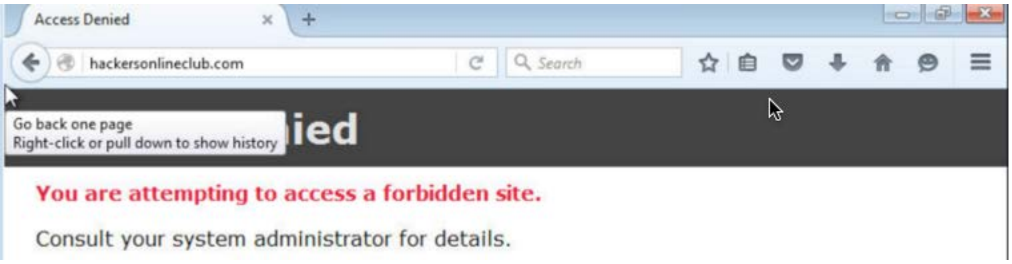
The end-user tries to join a hacking club and is denied access


hacking sites - Google Search - Windows Internet Explorer
https://www.google.com/search?q=hacking+si
Bing
Favorites
Suggested Sites
Web Slice Gallery
hacking sites - Google Search
Page
Safety
Tools
Past year
All results
Verbatim

Hack This Site!
https://www.hackthissite.org/
HackThisSite! is a legal and safe network security resource where users test their hacking skills on various challenges and learn about hacking and network ...
Login - Register - About the Project - Forums

Website Hacking - HackersOnlineClub
hackersonlineclub.com/website-hacking/
Learn How To Hack Websites with Different Techniques. ... as normal then the database is not vulnerable, and the website is not vulnerable to SQL Injection.

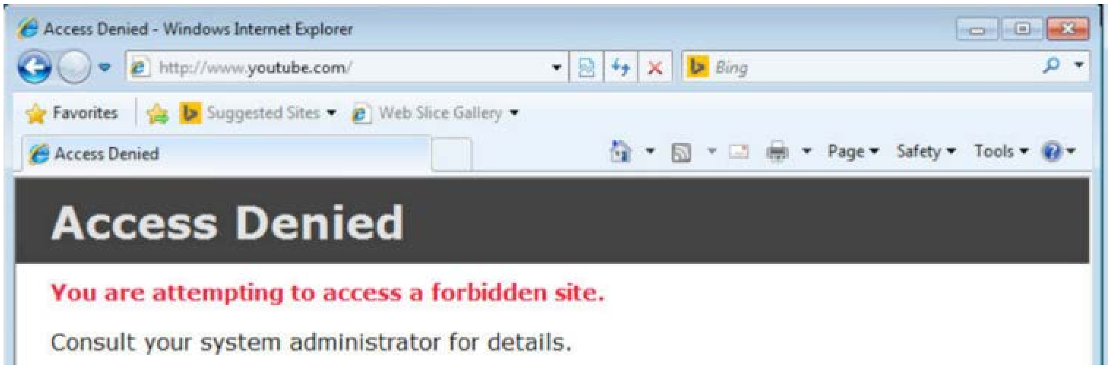
When the end-user attempts to join the hacking club he is denied access



You are attempting to access a forbidden site.

Consult your system administrator for details.

When the end-user attempts to access www.youtube.com he is denied

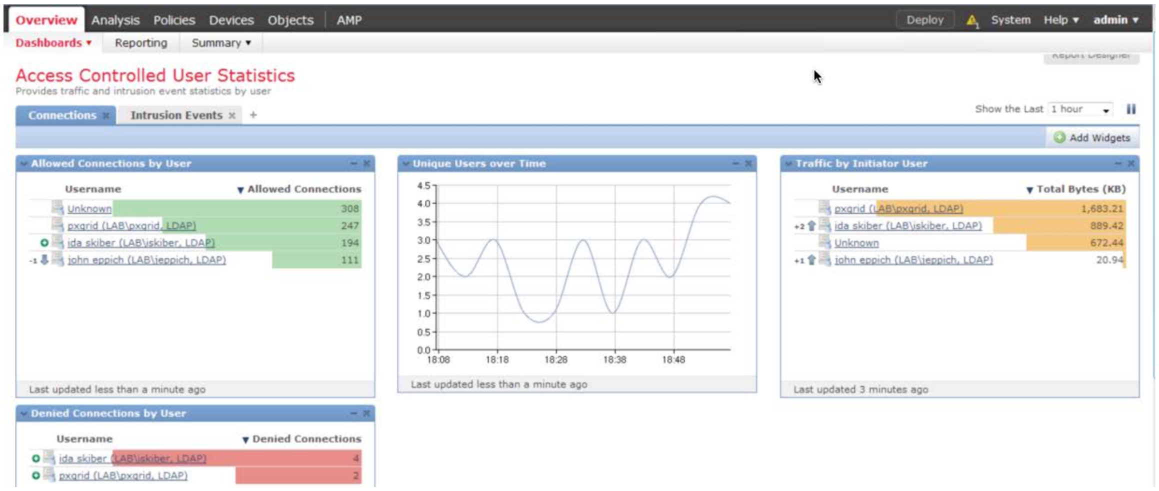


Access Denied

You are attempting to access a forbidden site.

Consult your system administrator for details.

On the Firepower Management Center Access Controlled User Statistics Dashboard, you can view the denied connections from the user iskiber



Access Controlled User Statistics

Provides traffic and intrusion event statistics by user

Allowed Connections by User

	Username	▾ Allowed Connections
	Unknown	308
	pxgrid (LAB\pxgrid, LDAP)	247
○	ida skiber (LAB\iskiber, LDAP)	194
-1 ⬇	john eppich (LAB\jeppich, LDAP)	111

Last updated less than a minute ago

Traffic by Initiator User

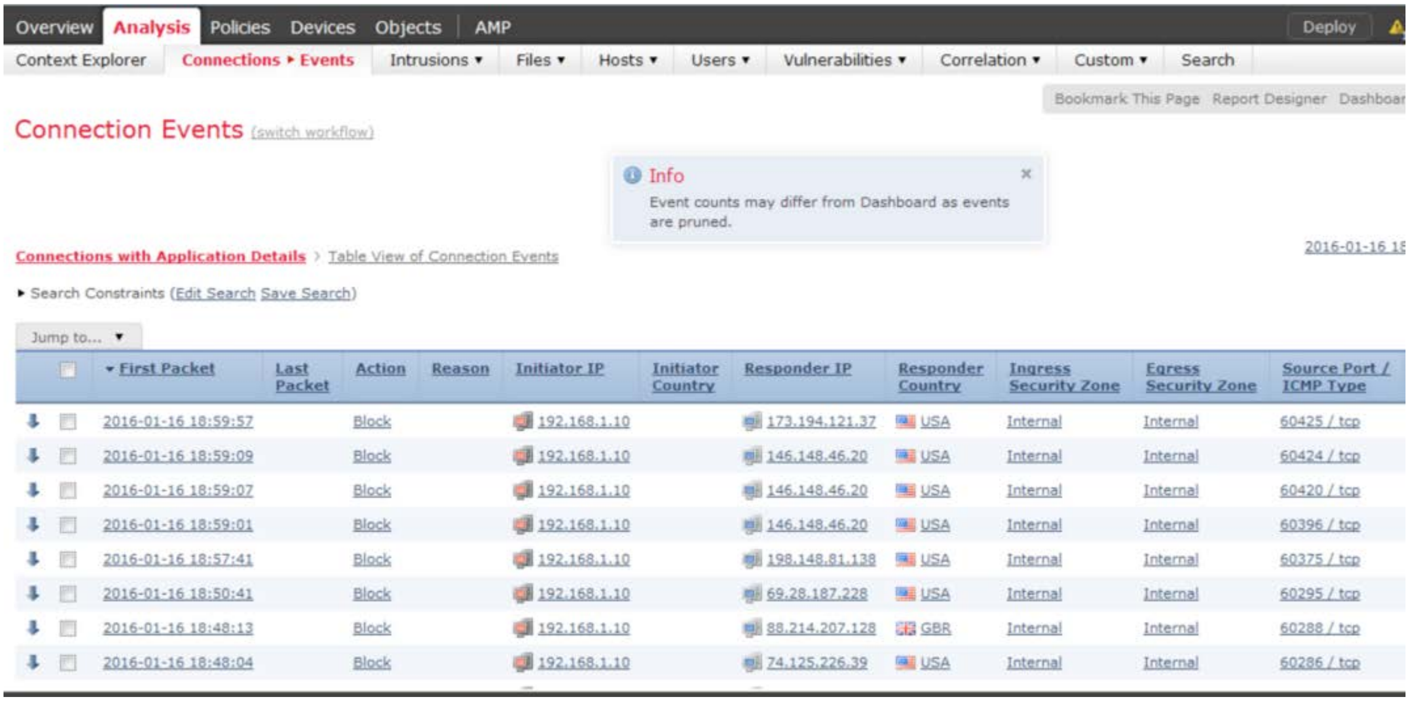
	Username	▾ Total Bytes (KB)
	pxgrid (LAB\pxgrid, LDAP)	1,683.21
+2 ⬆	ida skiber (LAB\iskiber, LDAP)	889.42
	Unknown	672.44
+1 ⬆	john eppich (LAB\jeppich, LDAP)	20.94

Last updated 3 minutes ago

Denied Connections by User

	Username	▾ Denied Connections
○	ida skiber (LAB\iskiber, LDAP)	4
○	pxgrid (LAB\pxgrid, LDAP)	2

If you click on denied connections by iskiber, note the denied URL categories. These denied categories represent the URL categories as defined in the “Deny Employee SGT Access” Firepower Management Center’s access control rule



Connection Events (switch workflow)

Info
Event counts may differ from Dashboard as events are pruned.

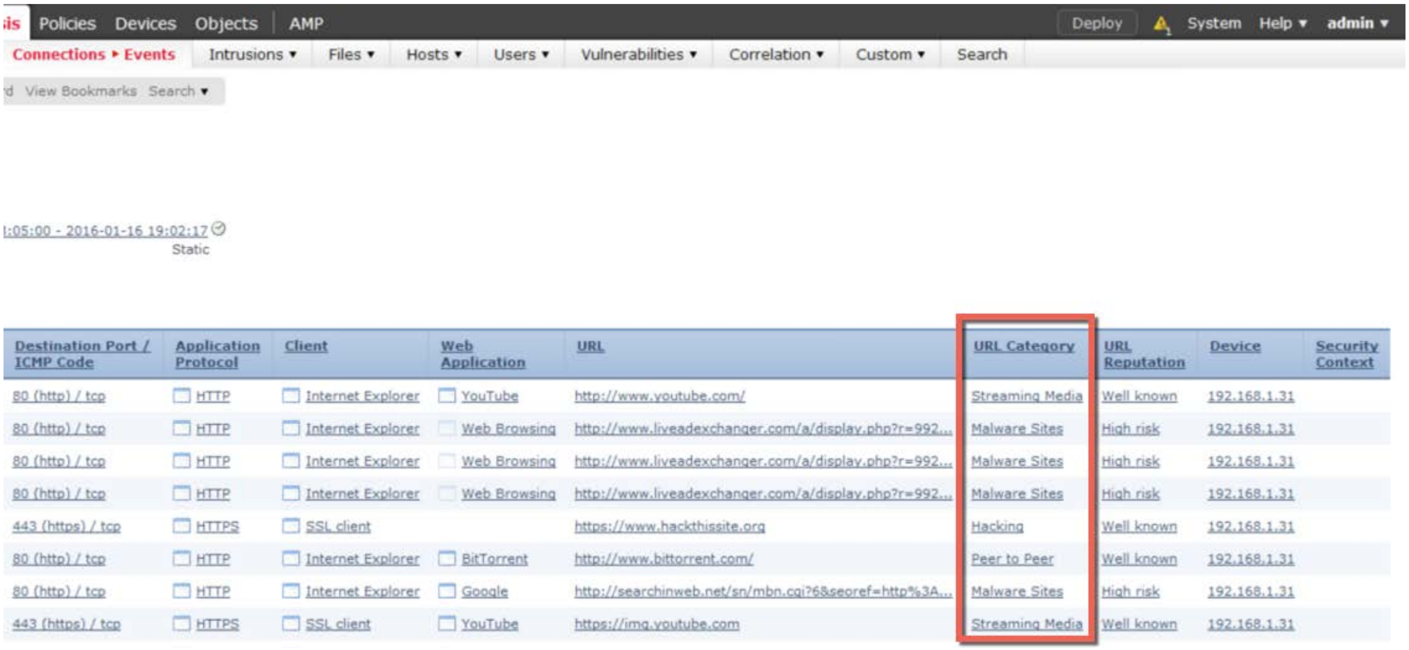
Connections with Application Details > Table View of Connection Events

2016-01-16 1

▸ Search Constraints (Edit Search Save Search)

	□	▾ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type
⬇	□	2016-01-16 18:59:57		Block		192.168.1.10		173.194.121.37	USA	Internal	Internal	60425 / tcp
⬇	□	2016-01-16 18:59:09		Block		192.168.1.10		146.148.46.20	USA	Internal	Internal	60424 / tcp
⬇	□	2016-01-16 18:59:07		Block		192.168.1.10		146.148.46.20	USA	Internal	Internal	60420 / tcp
⬇	□	2016-01-16 18:59:01		Block		192.168.1.10		146.148.46.20	USA	Internal	Internal	60396 / tcp
⬇	□	2016-01-16 18:57:41		Block		192.168.1.10		198.148.81.138	USA	Internal	Internal	60375 / tcp
⬇	□	2016-01-16 18:50:41		Block		192.168.1.10		69.28.187.228	USA	Internal	Internal	60295 / tcp
⬇	□	2016-01-16 18:48:13		Block		192.168.1.10		88.214.207.128	GBR	Internal	Internal	60288 / tcp
⬇	□	2016-01-16 18:48:04		Block		192.168.1.10		74.125.226.39	USA	Internal	Internal	60286 / tcp

Below is a screen continuation



:05:00 - 2016-01-16 19:02:17
Static

Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL	URL Category	URL Reputation	Device	Security Context
80 (http) / tcp	HTTP	Internet Explorer	YouTube	http://www.youtube.com/	Streaming Media	Well known	192.168.1.31	
80 (http) / tcp	HTTP	Internet Explorer	Web Browsing	http://www.liveadexchanger.com/a/display.php?r=992...	Malware Sites	High risk	192.168.1.31	
80 (http) / tcp	HTTP	Internet Explorer	Web Browsing	http://www.liveadexchanger.com/a/display.php?r=992...	Malware Sites	High risk	192.168.1.31	
80 (http) / tcp	HTTP	Internet Explorer	Web Browsing	http://www.liveadexchanger.com/a/display.php?r=992...	Malware Sites	High risk	192.168.1.31	
443 (https) / tcp	HTTPS	SSL client		https://www.hackthissite.org	Hacking	Well known	192.168.1.31	
80 (http) / tcp	HTTP	Internet Explorer	BitTorrent	http://www.bittorrent.com/	Peer to Peer	Well known	192.168.1.31	
80 (http) / tcp	HTTP	Internet Explorer	Google	http://searchinweb.net/sn/mbn.cgi?6&seoref=http%3A...	Malware Sites	High risk	192.168.1.31	
443 (https) / tcp	HTTPS	SSL client	YouTube	https://img.youtube.com	Streaming Media	Well known	192.168.1.31	

ASA with Firepower Services

In this document an ASA 5506W was used for testing. The ASA Firepower (sfr) module was installed and was tested in the following:

- Managed Firepower pxGrid Intrusion policy and Employee SGT access control rule
- On-Box managed Firepower pxGrid Intrusion policy and Employee SGT access control rile.

Using Centralized Firepower Management Center Policy

Here we install the ASA Firepower (sfr) module. Once configured we will register the ASA to the Firepower Management Console where the ASA will enforce the managed Cisco Firepower policy.

Note: Please make sure you install either smart or classic license for the managed ASA with Firepower services.

ASA Firepower (sfr) Installation and registering to Firepower Management Center

Step 1 Download ASDM 7.5.2, and ASA 9.5.2 and upload them to ASA

Step 2 Install the ASA Firepower module

```
ciscoasa# sw-module module sfr recover configure image disk0:/asasfr-5500x-6.0.0.img
```

Step 3 Turn on debugging, this will make it easier if error messages occur

```
ciscoasa# sh debug
ciscoasa# debug module
```

Step 4 Load the ASA Firepower boot image

```
ciscoasa# sw-module module module sfr recover boot
```

Step 5 Wait approximately 5-15 minutes for the ASA Firepower to boot up, open a console session to the now-running ASA Firepower boot image. You may press enter a couple of times and type the following

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is ‘CTRL_^X’.

Cisco ASA SFR Boot Image 5.3.1
asasfr login:admin
Password: Admin123
```

Step 6 Install the software system image using the system install command, ftp was used in the following example:

```
asa-boot>system install http://jeppich:password@192.168.1.8/asasfr-5500x-6.0.0.img
```

The system will go down for a reboot when complete. This may take awhile for sfr to come up; it may take longer than 30 minutes as was the case with my ASA 5506. Check by typing the following

```
sh module sfr
```

You should see the module as up, if it is still in the recover state, the module is still installing

Step 7 Open a session to the ASA Firepower module

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is ‘CTRL- ^X’.

Sourcefire3D login: admin
Password: Admin123
```

Step 8 Read and accept the EULA and complete the system configuration

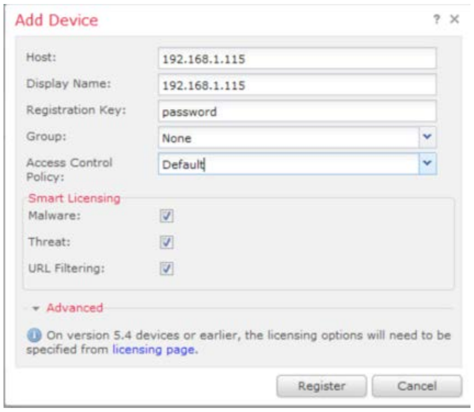
Step 9 Add the ASA Firepower services to the Firepower Management 6.0

```
> configure manager add (ip address of Cisco Firepower Management Console) password
```

Step 10 Ensure that you have the proper licenses installed for the ASA

Step 11 Add ASA Firepower device to the Firepower Management Center 6.0 and enter the device information and enable the license

Select **Devices->Device Management->Add->Add Device**



Add Device

Host:	192.168.1.115
Display Name:	192.168.1.115
Registration Key:	password
Group:	None
Access Control Policy:	Default

Smart Licensing

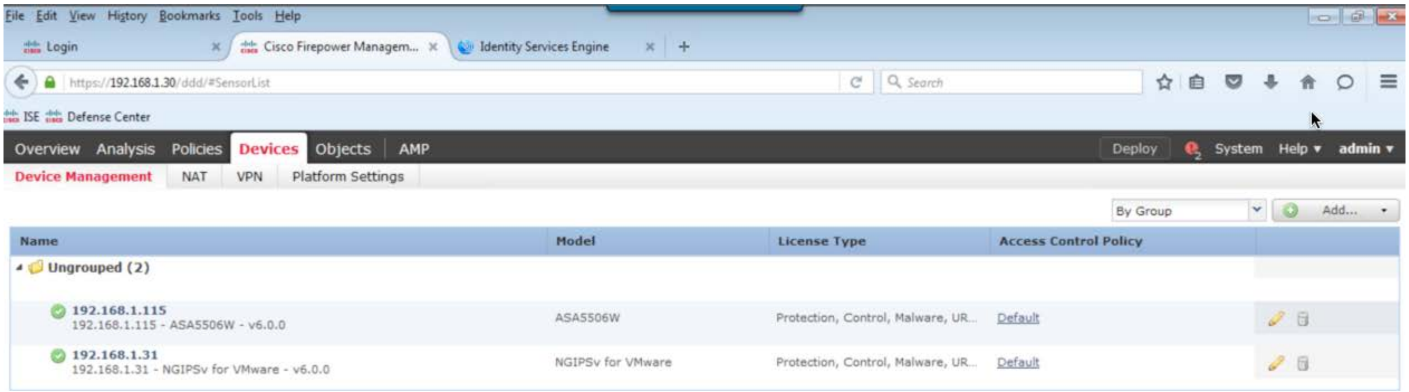
Malware:	☑
Threat:	☑
URL Filtering:	☑

▾ Advanced

On version 5.4 devices or earlier, the licensing options will need to be specified from licensing page.

Step 12 Select Register

Step 13 After the ASA Firepower has successfully registered you should see the following:

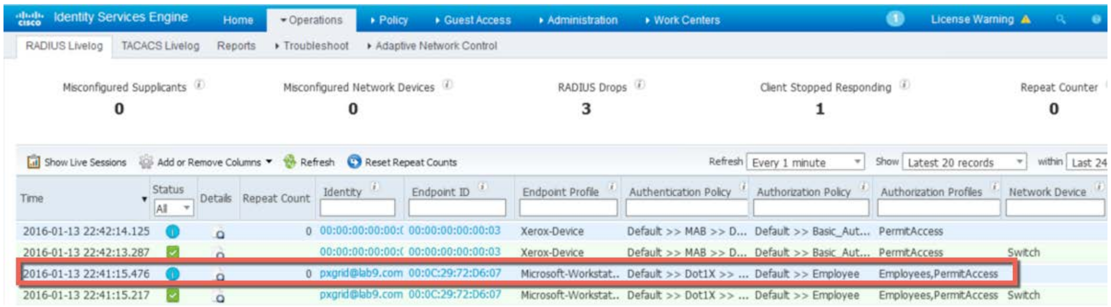


File Edit View History Bookmarks Tools Help
Login
Cisco Firepower Managem...
Identity Services Engine
https://192.168.1.30/ddd/#SensorList
Search
ISE Defense Center
Overview Analysis Policies Devices Objects AMP
Deploy System Help admin
Device Management NAT VPN Platform Settings
By Group
Add...

Name	Model	License Type	Access Control Policy
Ungrouped (2)			
192.168.1.115 192.168.1.115 - ASA5506W - v6.0.0	ASA5506W	Protection, Control, Malware, UR...	Default
192.168.1.31 192.168.1.31 - NGIPSv for VMware - v6.0.0	NGIPSv for VMware	Protection, Control, Malware, UR...	Default

Testing User with Employee SGT from managed Firepower Management Policy

Here we test the FMC 6.0 policy we created for an end-user tagged as employee. The end-user is tagged as having an Employee SGT after a successful 802.1X authentication based on the ISE authorization policy.

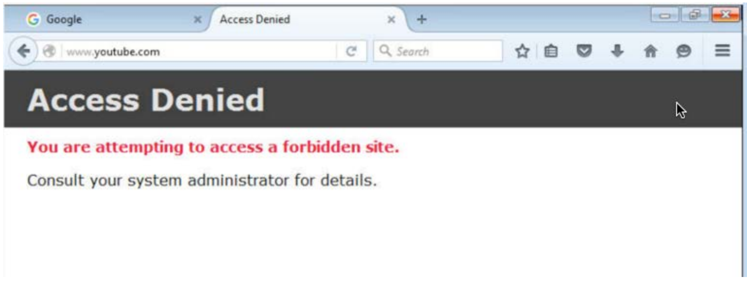


Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	3	1	0

Refresh Every 1 minute Show Latest 20 records within Last 24

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device
	All									
2016-01-13 22:42:14.125			0	00:00:00:00:00:(	00:00:00:00:00:03	Xerox-Device	Default >> MAB >> D...	Default >> Basic_Aut...	PermitAccess	
2016-01-13 22:42:13.287	✓			00:00:00:00:00:(	00:00:00:00:00:03	Xerox-Device	Default >> MAB >> D...	Default >> Basic_Aut...	PermitAccess	Switch
2016-01-13 22:41:15.476			0	pxgrid@lab9.com	00:0C:29:72:D6:07	Microsoft-Workstat..	Default >> Dot1X >> ...	Default >> Employee	Employees,PermitAccess	
2016-01-13 22:41:15.217	✓			pxgrid@lab9.com	00:0C:29:72:D6:07	Microsoft-Workstat..	Default >> Dot1X >> ...	Default >> Employee	Employees,PermitAccess	Switch

The end-user opens their browser and accesses www.youtube.com and is denied access

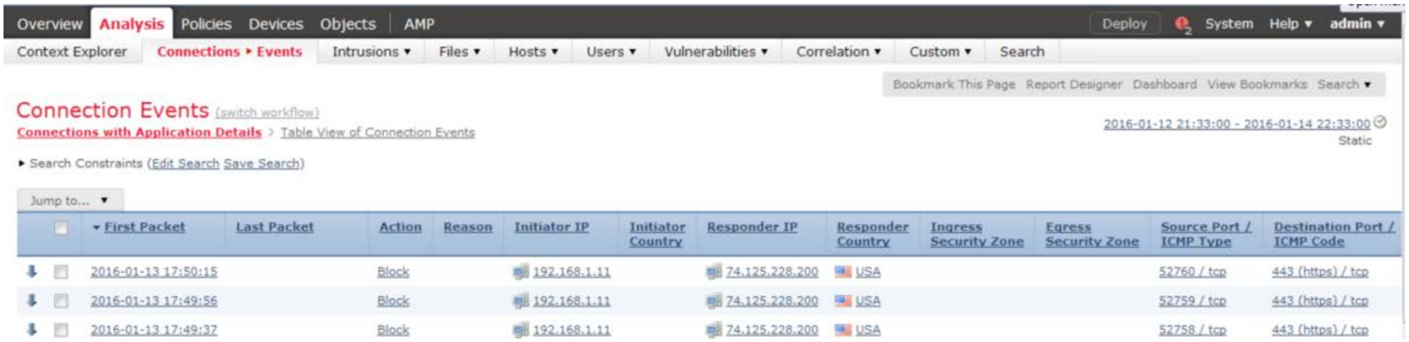


Access Denied

You are attempting to access a forbidden site.

Consult your system administrator for details.

On the Firepower Management Center, s elect **Analysis->Connection->Events** to see the details of blocked transactions



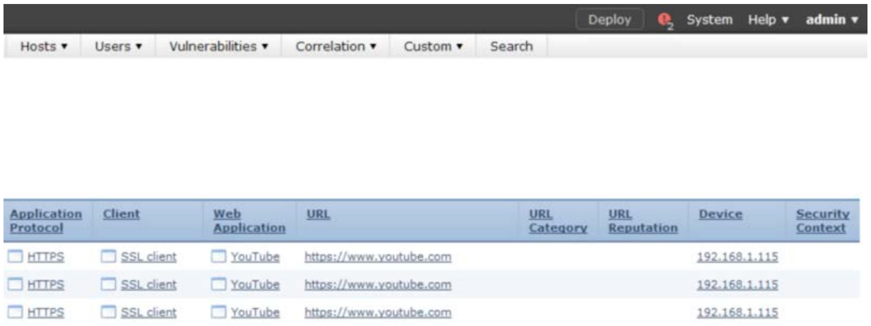
Connection Events (switch workflow)
Connections with Application Details > Table View of Connection Events

2016-01-12 21:33:00 - 2016-01-14 22:33:00
Static

▸ Search Constraints (Edit Search Save Search)

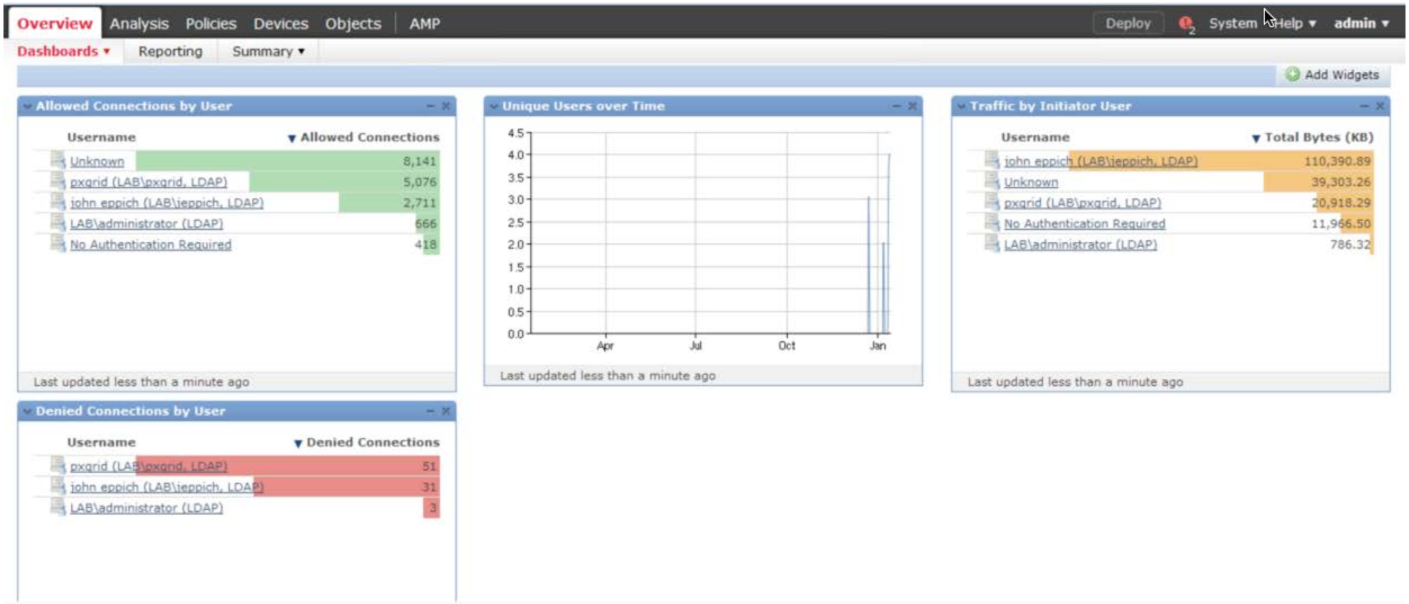
		▾ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
⬇	□	2016-01-13 17:50:15		Block		192.168.1.11		74.125.228.200	USA			52760 / tcp	443 (https) / tcp
⬇	□	2016-01-13 17:49:56		Block		192.168.1.11		74.125.228.200	USA			52759 / tcp	443 (https) / tcp
⬇	□	2016-01-13 17:49:37		Block		192.168.1.11		74.125.228.200	USA			52758 / tcp	443 (https) / tcp

Continuation of screen below note that we see www.youtube.com



Application Protocol	Client	Web Application	URL	URL Category	URL Reputation	Device	Security Context
HTTPS	SSL client	YouTube	https://www.youtube.com			192.168.1.115	
HTTPS	SSL client	YouTube	https://www.youtube.com			192.168.1.115	
HTTPS	SSL client	YouTube	https://www.youtube.com			192.168.1.115	

On Firepower Management center, select **Overview->Dashboards->Access Controlled User Statistics** and click on **Denied Connections** by User for pxGrid



Allowed Connections by User

Username	▾ Allowed Connections
Unknown	8,141
pxgrid (LAB\pxgrid, LDAP)	5,076
john eppich (LAB\jeppich, LDAP)	2,711
LAB\administrator (LDAP)	666
No Authentication Required	418

Last updated less than a minute ago

Traffic by Initiator User

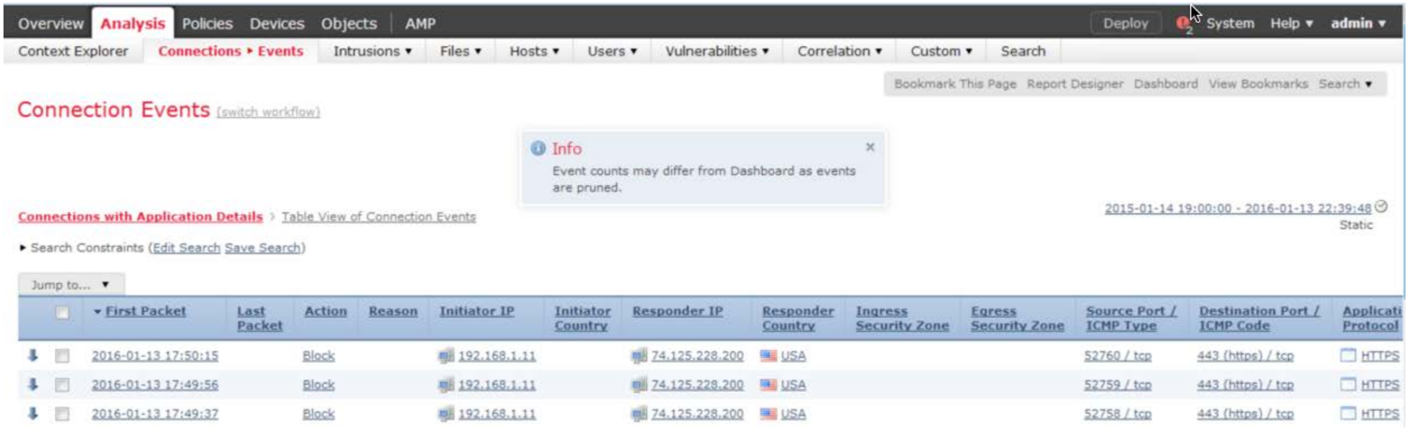
Username	▾ Total Bytes (KB)
john eppich (LAB\jeppich, LDAP)	110,390.89
Unknown	39,303.26
pxgrid (LAB\pxgrid, LDAP)	20,918.29
No Authentication Required	11,966.50
LAB\administrator (LDAP)	786.32

Last updated less than a minute ago

Denied Connections by User

Username	▾ Denied Connections
pxgrid (LAB\pxgrid, LDAP)	51
john eppich (LAB\jeppich, LDAP)	31
LAB\administrator (LDAP)	3

You will see the blocked connection events for www.youtube.com



Connection Events (switch workflow)

Info
Event counts may differ from Dashboard as events are pruned.

Connections with Application Details > Table View of Connection Events

2015-01-14 19:00:00 - 2016-01-13 22:39:48
Static

▸ Search Constraints (Edit Search Save Search)

Jump to... ▾

	□	▾ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Applicati Protocol
⬇	□	2016-01-13 17:50:15		Block		192.168.1.11		74.125.228.200	USA			52760 / tcp	443 (https) / tcp	HTTPS
⬇	□	2016-01-13 17:49:56		Block		192.168.1.11		74.125.228.200	USA			52759 / tcp	443 (https) / tcp	HTTPS
⬇	□	2016-01-13 17:49:37		Block		192.168.1.11		74.125.228.200	USA			52758 / tcp	443 (https) / tcp	HTTPS

On-Box Firepower Policy Management

This section provides details for on-box management for the ASA with Firepower services via ASDM. Please note that you will need separate licenses for the on-box ASA using Firepower policies via ASDM. Also the ASA with Firepower services was configured for a CA-signed environment.

Delete the ASA from the Firepower Management Center 6.0

Step 1 Delete the ASA5500 device from the Firepower Management Center 6.0

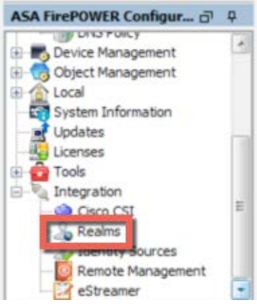
Select **Devices->Device Management->Delete the ASA 5500 Sensor** by clicking on 🗑

Note: If your ASA device has not been deleted from FMC 6.0, the ASDM will not be able to see the ASA Firepower Configuration Details. This will require a separate set of licenses for on-box registration

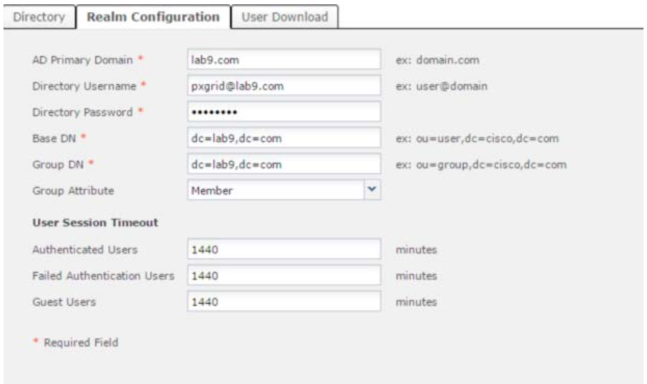
ISE Realm Configuration

Here we configure the ISE Realm on ISE

Step 1 Select **ASA Firepower Configuration->Realms**



Step 2 Select **New Realm,** enter the realm configuration details



AD Primary Domain * lab9.com ex: domain.com

Directory Username * pxgrid@lab9.com ex: user@domain

Directory Password * ••••••••

Base DN * dc=lab9,dc=com ex: ou=user,dc=cisco,dc=com

Group DN * dc=lab9,dc=com ex: ou=group,dc=cisco,dc=com

Group Attribute Member

User Session Timeout

Authenticated Users 1440 minutes

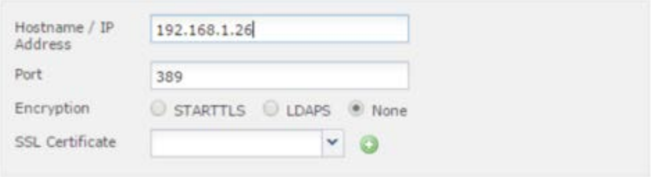
Failed Authentication Users 1440 minutes

Guest Users 1440 minutes

* Required Field

Step 3 Select **OK,** enable the Realm by clicking **State**

Step 4 Select **Add Directory**, enter the information below



Hostname / IP Address 192.168.1.26

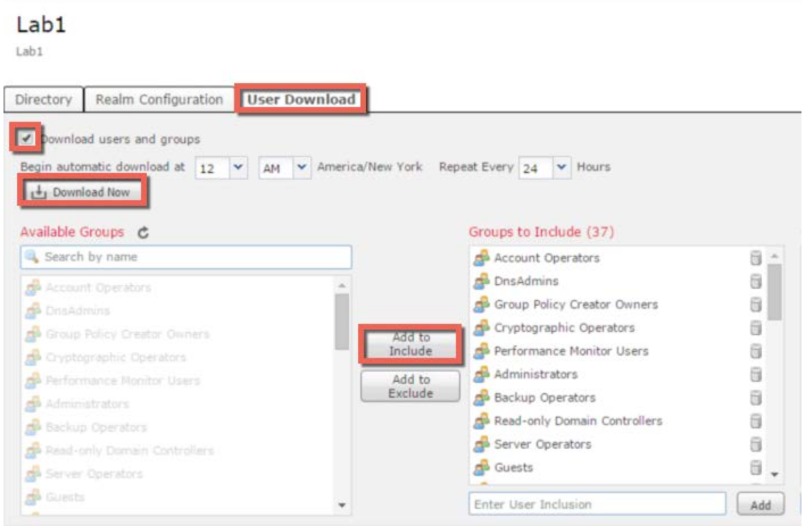
Port 389

Encryption ○ STARTTLS ○ LDAPS ● None

SSL Certificate

Step 5 Select **Test**, you should see operation succeeded

Step 6 Click **User Download->enable Download users and groups->Download Now->Add to Include**



☑ Download users and groups

Begin automatic download at 12 AM America/New York Repeat Every 24 Hours

Groups to Include (37)

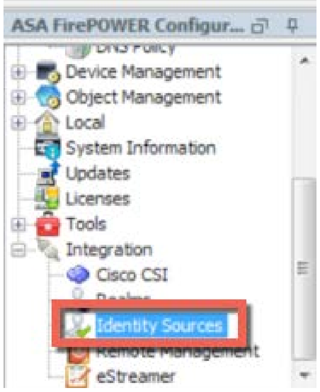
- Account Operators
- DnsAdmins
- Group Policy Creator Owners
- Cryptographic Operators
- Performance Monitor Users
- Administrators
- Backup Operators
- Read-only Domain Controllers
- Server Operators
- Guests

Step 7 Click **Store ASA Firepower Changes**

ISE Identity Sources Configuration

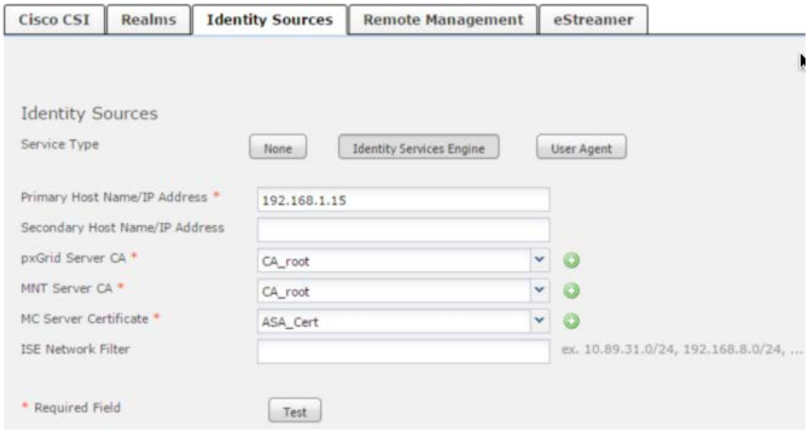
The identity sources configuration contains the connection parameters between the ASA with Firepower services and the ISE pxGrid node. Please note that the ASA has a signed CA-signed certificate. Please refer to CA-signed operation if you are not familiar with the certificate installation

Step 1 Select **ASA Firepower Configuration Changes->Identity Sources**



Step 2 Select **Identity Services Engine,** and provide the ISE pxGrid configuration below:

Note: Please provide the proper certificate information for self-signed or CA-signed certificates

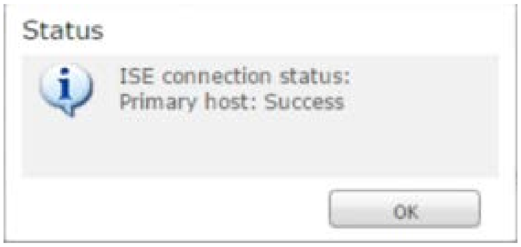


Identity Sources

Service Type	Identity Services Engine
Primary Host Name/IP Address *	192.168.1.15
Secondary Host Name/IP Address	
pxGrid Server CA *	CA_root
MNT Server CA *	CA_root
MC Server Certificate *	ASA_Cert
ISE Network Filter	ex. 10.89.31.0/24, 192.168.8.0/24, ...

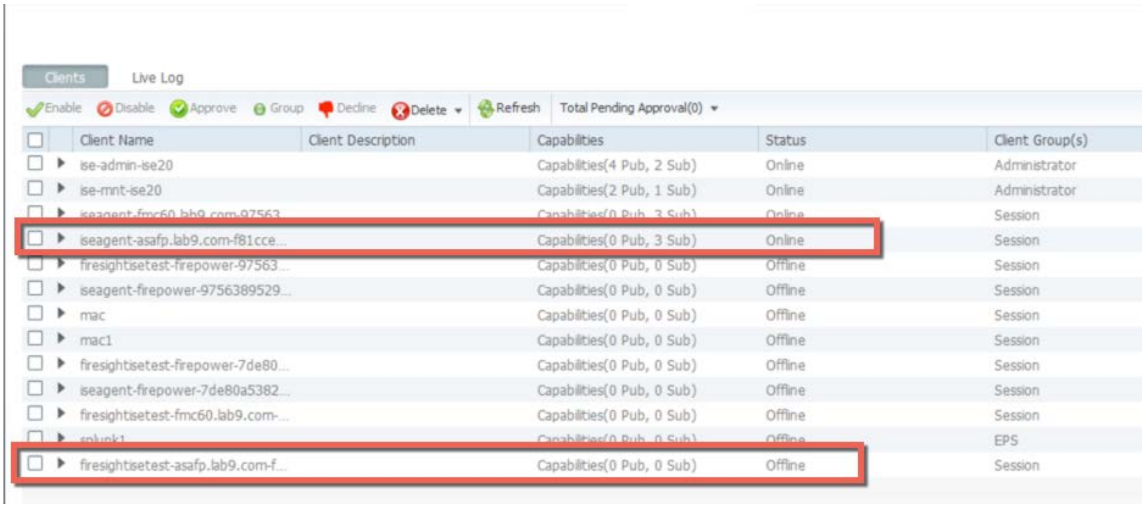
* Required Field

Step 3 Select **Test,** to verify connectivity to the ISE pxGrid node, you should see



ISE connection status:
Primary host: Success

Step 4 You should see that the ASA Firepower has successfully registered as a pxGrid client
Select **Administration->pxGrid Services**



☐	Client Name	Client Description	Capabilities	Status	Client Group(s)
☐	ise-admin-ise20		Capabilities(4 Pub, 2 Sub)	Online	Administrator
☐	ise-mnt-ise20		Capabilities(2 Pub, 1 Sub)	Online	Administrator
☐	iseagent-fmc60.lab9.com-97563		Capabilities(0 Pub, 3 Sub)	Online	Session
☐	iseagent-asafp.lab9.com-f81cce...		Capabilities(0 Pub, 3 Sub)	Online	Session
☐	firesightisetest-firepower-97563...		Capabilities(0 Pub, 0 Sub)	Offline	Session
☐	iseagent-firepower-9756389529...		Capabilities(0 Pub, 0 Sub)	Offline	Session
☐	mac		Capabilities(0 Pub, 0 Sub)	Offline	Session
☐	mac1		Capabilities(0 Pub, 0 Sub)	Offline	Session
☐	firesightisetest-firepower-7de80...		Capabilities(0 Pub, 0 Sub)	Offline	Session
☐	iseagent-firepower-7de80a5382...		Capabilities(0 Pub, 0 Sub)	Offline	Session
☐	firesightisetest-fmc60.lab9.com-...		Capabilities(0 Pub, 0 Sub)	Offline	Session
☐	splunk1		Capabilities(0 Pub, 0 Sub)	Offline	EPS
☐	firesightisetest-asafp.lab9.com-f...		Capabilities(0 Pub, 0 Sub)	Offline	Session

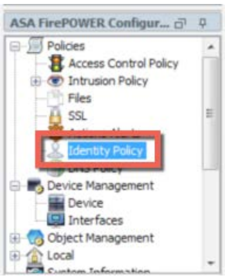
Step 5 If there you have an unsuccessful attempts,
Step 6 Select Monitoring->**ASA Firepower Monitoring,** this should provide some details

Note: Failures are mostly due to certificate issues

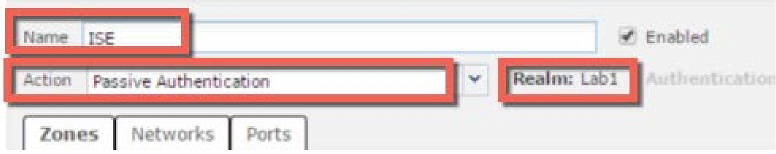
ISE Identity Policy

The ISE Identity Policy will be configured for passive authentication and will be used in the Firepower Management Center default access control rule for ISE authentication.

Step 1 Select ASA Firepower Configuration->**Policies->Identity Policy**



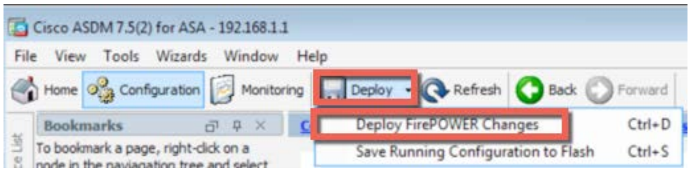
Step 2 Click **Add Rule,** enter name->**Passive Authentication->Realm**



Name ISE
☑ Enabled
Action Passive Authentication
Realm: Lab1

Step 3 Select Store **ASA Firepower Changes**

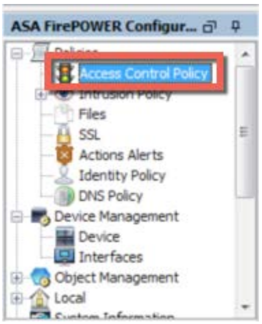
Step 4 Select **Deploy->Deploy Firepower Changes->Deploy-Ok**


Cisco ASDM 7.5(2) for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Deploy Refresh Back Forward
Bookmarks
To bookmark a page, right-click on a node in the navigation tree and select
Deploy FirePOWER Changes Ctrl+D
Save Running Configuration to Flash Ctrl+S

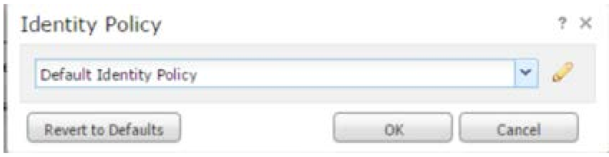
Adding ISE Identity Policy

The ISE identity policy is added to the Firepower Management Center's default access policy

Step 1 Select **ASA Firepower Configuration->Policies->Access Control Policy**



Step 2 Select **ASA Firepower->Add Rule->Identity Policy->None,** select **Default Identity Policy** from the drop-down



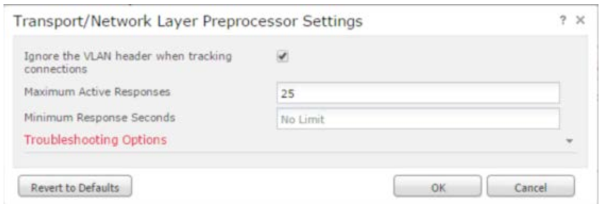
Step 3 Select **OK**

Step 4 Click **Store ASA Firepower Changes**

Transport and Network Layer Preprocessor Settings

These settings have been modified to block network access based on the Firepower intrusion policy.

Step 1 Click **Advanced->Transport/Network Layer Preprocessor Settings** ✎, provide the following settings:


Transport/Network Layer Preprocessor Settings

Ignore the VLAN header when tracking connections ☑

Maximum Active Responses: 25

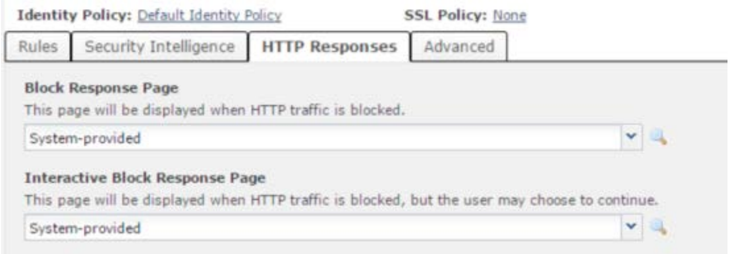
Minimum Response Seconds: No Limit

Step 2 Select **OK**

Adding Block Response Page

The system-provided block response page has been added as a blocked response to the Firepower access control file.

Step 1 Click **HTTP Responses,** and provide the following:


Identity Policy: Default Identity Policy SSL Policy: None

Block Response Page

This page will be displayed when HTTP traffic is blocked.

System-provided

Interactive Block Response Page

This page will be displayed when HTTP traffic is blocked, but the user may choose to continue.

System-provided

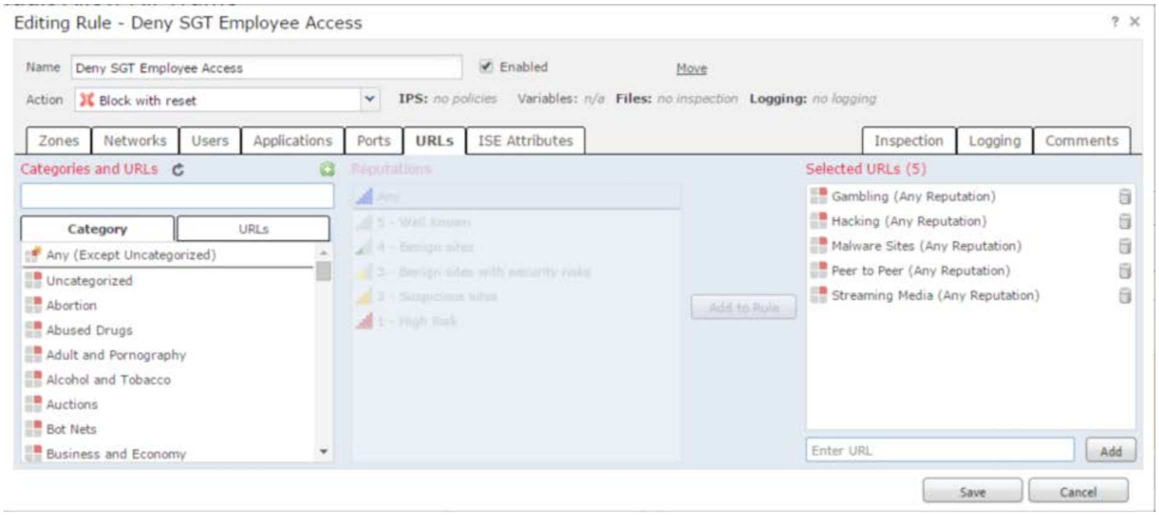
Step 2 Click **Store ASA Firepower Changes**

ASA Create Employee SGT Access Control Rules

These Employee SGT tag access control rules set a corporate acceptable usage policy denying access to: hacking sites, streaming media, peer-to-peer applications, malware and gambling sites

Step 1 Select ASA Firepower Configuration->Access Control Policy->**ASA Firepower-Add rule**

Step 2 Select **Add Rule, enter name: Deny Employee SGT Access->action->Block with reset->IPS->pxGrid intrusion policy->URLs->Category>Gambling, Peer-to-Peer, Streaming Video, Hacking->Save**



Editing Rule - Deny SGT Employee Access

Name: Deny SGT Employee Access ☑ Enabled

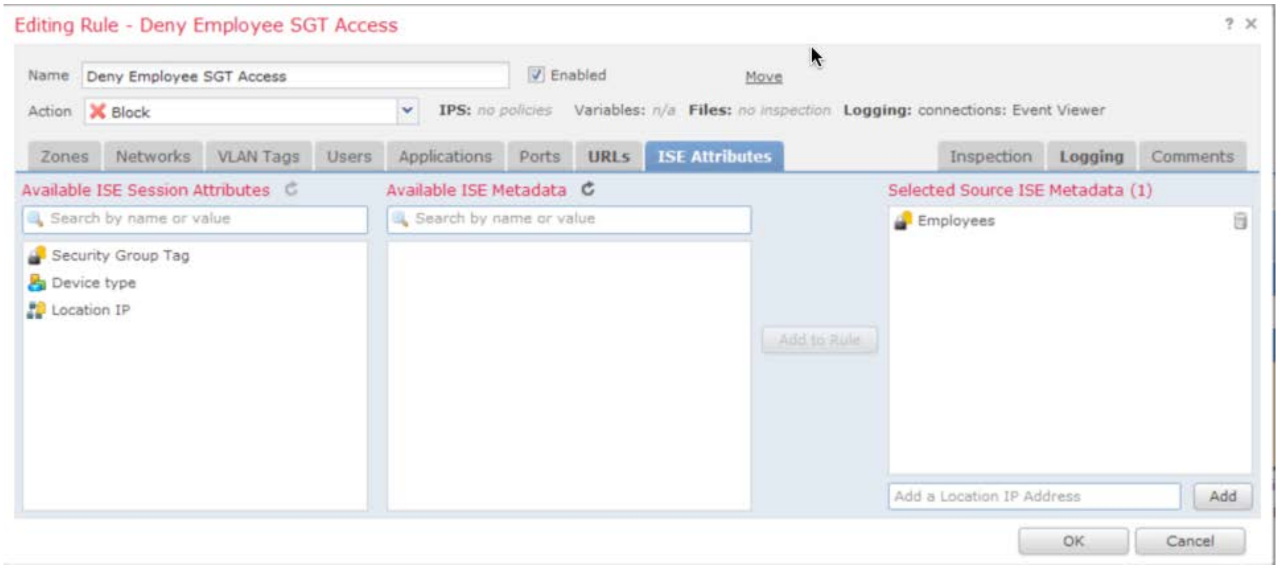
Action: Block with reset

IPS: *no policies* Variables: *n/a* Files: *no inspection* Logging: *no logging*

Selected URLs (5)

- Gambling (Any Reputation)
- Hacking (Any Reputation)
- Malware Sites (Any Reputation)
- Peer to Peer (Any Reputation)
- Streaming Media (Any Reputation)

Step 3 Select ISE **Attributes->Available ISE session attributes->Security Group Tag->Available Metadata->Employees->Add to rule**



Editing Rule - Deny Employee SGT Access

Name: Deny Employee SGT Access ☑ Enabled

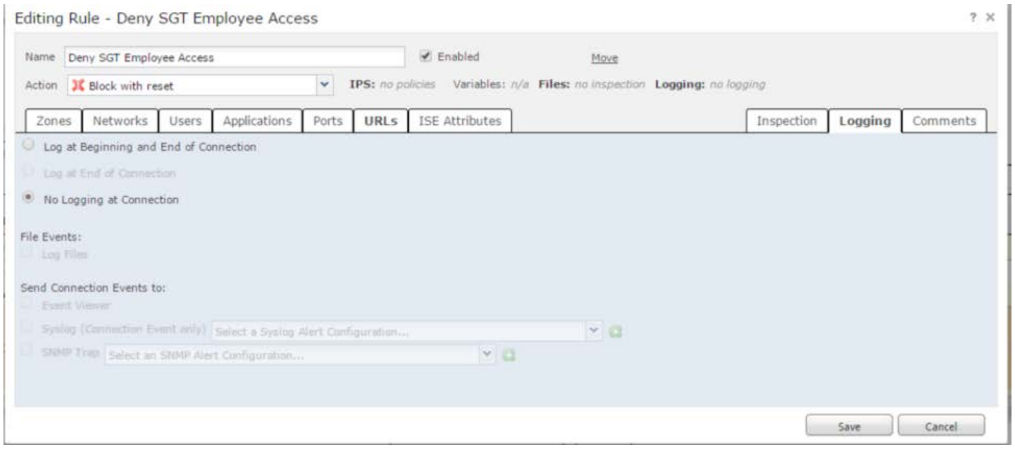
Action: Block

IPS: *no policies* Variables: *n/a* Files: *no inspection* Logging: connections: Event Viewer

Selected Source ISE Metadata (1)

- Employees

Step 4 Select Logging and configure the following settings



Editing Rule - Deny SGT Employee Access

Name: Deny SGT Employee Access ☑ Enabled Move

Action: Block with reset IPS: *no policies* Variables: *n/a* Files: *no inspection* Logging: *no logging*

○ Log at Beginning and End of Connection

○ Log at End of Connection

● No Logging at Connection

File Events:

□ Log Files

Send Connection Events to:

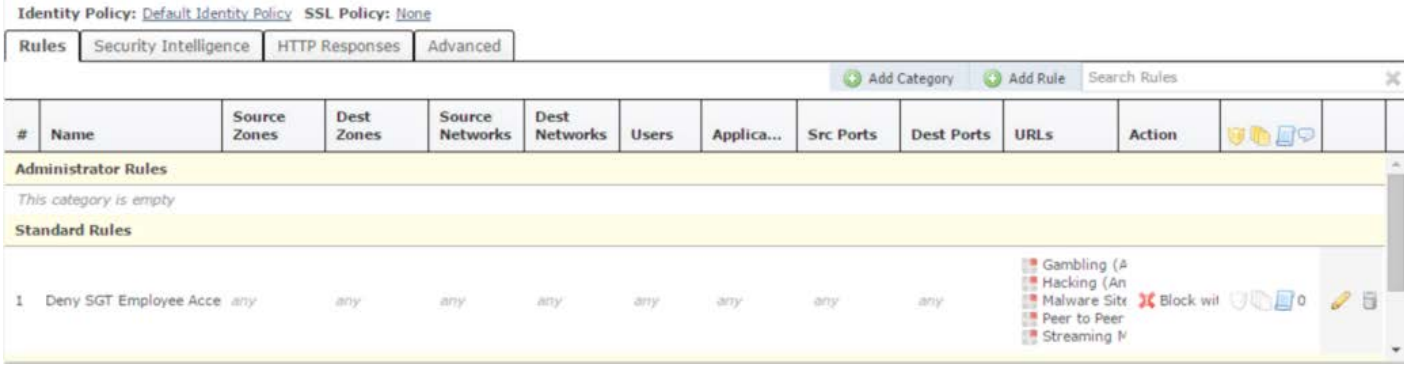
□ Event Viewer

□ Syslog (Connection Event only) Select a Syslog Alert Configuration...

□ SNMP Trap Select an SNMP Alert Configuration...

Step 5 Select **Save**

You should see the following



Identity Policy: Default Identity Policy SSL Policy: None

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	Users	Applica...	Src Ports	Dest Ports	URLs	Action		
Administrator Rules													
This category is empty													
Standard Rules													
1	Deny SGT Employee Acce	*any*	*any*	*any*	*any*	*any*	*any*	*any*	*any*	Gambling (A Hacking (An Malware Site Peer to Peer Streaming M	Block wit	0	

Step 6 Select **Save**

Step 7 Select **store ASA Firepower changes**

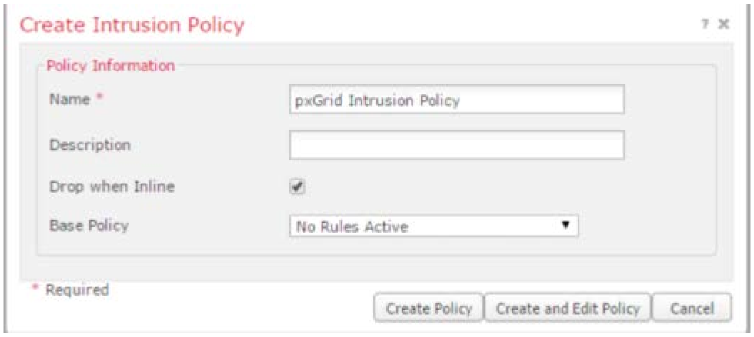
Step 8 Select **Deploy->Deploy Firepower changes->Deploy-OK**

Step 9 Select **Monitoring->ASA Firepower Monitoring->Task Status to view deployment status**

ASA FirePOWER pxGrid Intrusion Policy

In this section, the pxGrid Intrusion Policy is created and deployed to the Firepower 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 trigger an intrusion event that will be dropped in line and event generated to the Firepower Management Console under Analysis Intrusion Events

Step 1 Select ASA Firepower Configuration->Intrusion Policy->Create Policy and configure the following:



Create Intrusion Policy

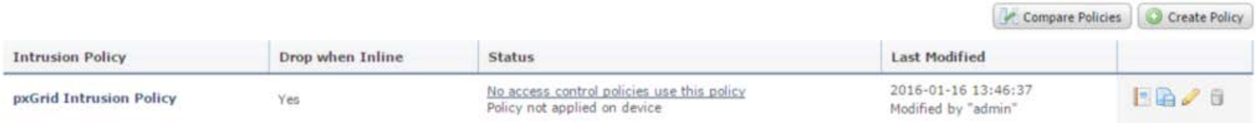
Policy Information

Name *	pxGrid Intrusion Policy
Description	
Drop when Inline	☑
Base Policy	No Rules Active

* Required

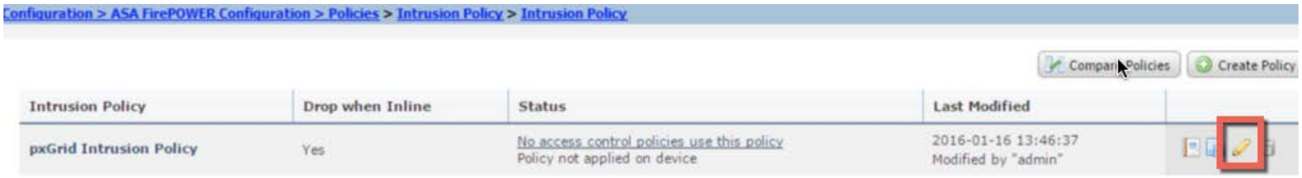
Step 2 Click **Create Policy**

Step 3 You should see the following



Intrusion Policy	Drop when Inline	Status	Last Modified
pxGrid Intrusion Policy	Yes	No access control policies use this policy Policy not applied on device	2016-01-16 13:46:37 Modified by "admin"

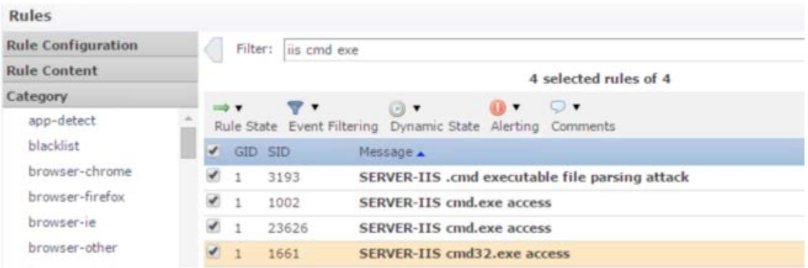
Step 4 Edit the policy by clicking on ✎



Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy

Intrusion Policy	Drop when Inline	Status	Last Modified
pxGrid Intrusion Policy	Yes	No access control policies use this policy Policy not applied on device	2016-01-16 13:46:37 Modified by "admin"

Step 5 Click on **Rules->filter: iis cmd exe** and select the following

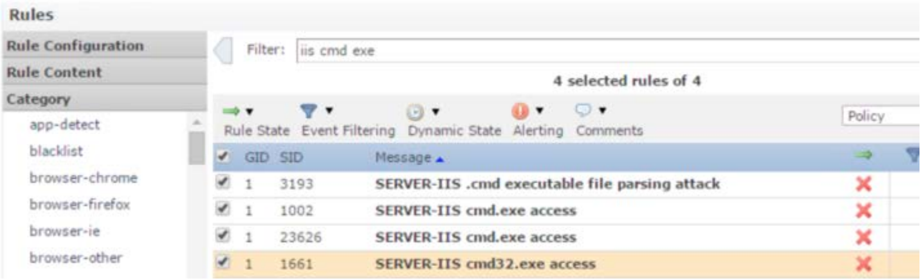


Filter: iis cmd exe

4 selected rules of 4

☑	GID	SID	Message ▲
☑	1	3193	SERVER-IIS .cmd executable file parsing attack
☑	1	1002	SERVER-IIS cmd.exe access
☑	1	23626	SERVER-IIS cmd.exe access
☑	1	1661	SERVER-IIS cmd32.exe access

Step 6 Click **Rule State->Drop and Generate Events->OK**
You should see the following:

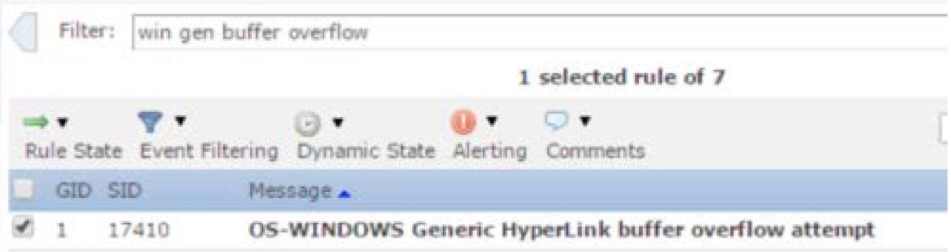


Filter: iis cmd exe

4 selected rules of 4

☑	GID	SID	Message	
☑	1	3193	SERVER-IIS .cmd executable file parsing attack	✗
☑	1	1002	SERVER-IIS cmd.exe access	✗
☑	1	23626	SERVER-IIS cmd.exe access	✗
☑	1	1661	SERVER-IIS cmd32.exe access	✗

Step 7 Next filter on: **win gen buffer overflow** and select->**OS-Windows Generic Hyperlink BufferOverflow Attempt**

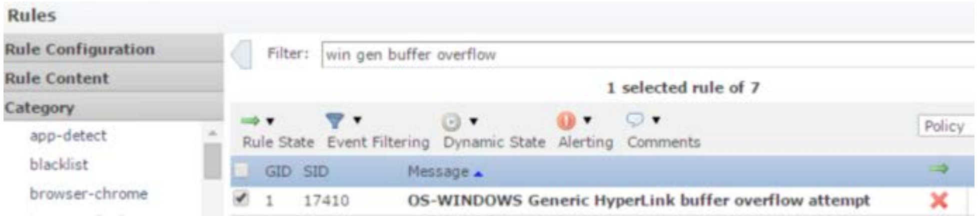


Filter: win gen buffer overflow

1 selected rule of 7

□	GID	SID	Message
☑	1	17410	OS-WINDOWS Generic HyperLink buffer overflow attempt

Step 8 **Rule State->Drop and Generate Events->OK**

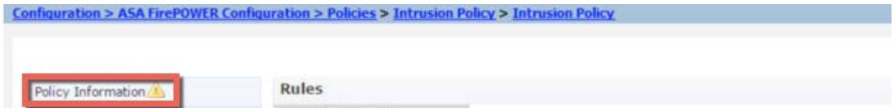


Filter: win gen buffer overflow

1 selected rule of 7

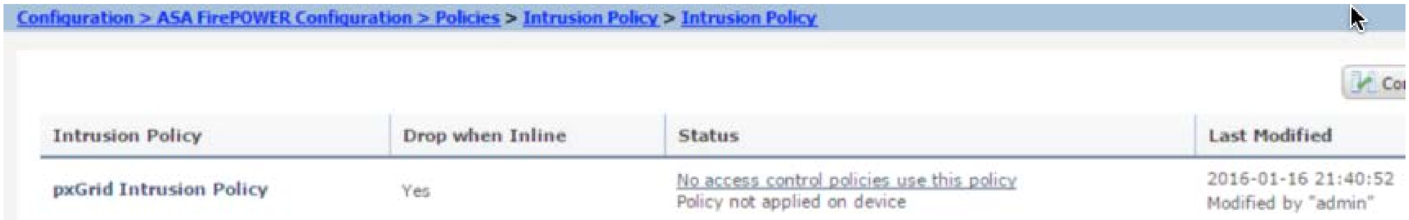
□	GID	SID	Message	
☑	1	17410	OS-WINDOWS Generic HyperLink buffer overflow attempt	✗

Step 9 Click Policy Information to commit changes



Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy
Policy Information
Rules

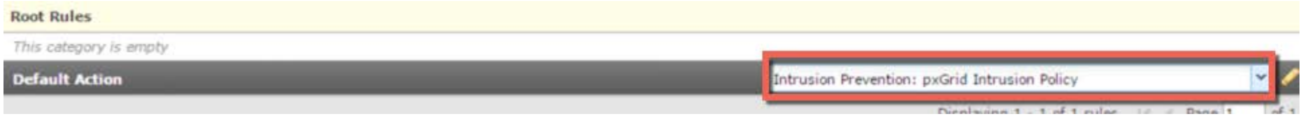
Step 10 Click->Commit Changes->Ok
Step 11 You should see the following



Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy

Intrusion Policy	Drop when Inline	Status	Last Modified
pxGrid Intrusion Policy	Yes	No access control policies use this policy Policy not applied on device	2016-01-16 21:40:52 Modified by "admin"

Step 12 Add pxGrid intrusion policy to default access control policy Select->ASA Firepower configuration->Policies->Access Control Policy->Intrusion Prevention:pxGrid intrusion policy from the drop-down

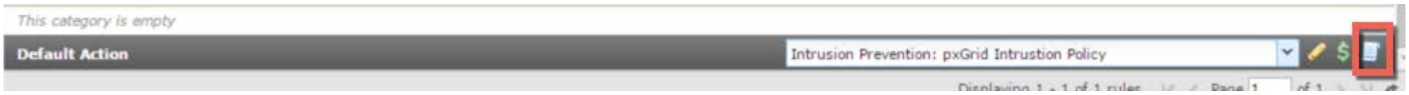


Root Rules

This category is empty

Default Action: Intrusion Prevention: pxGrid Intrusion Policy

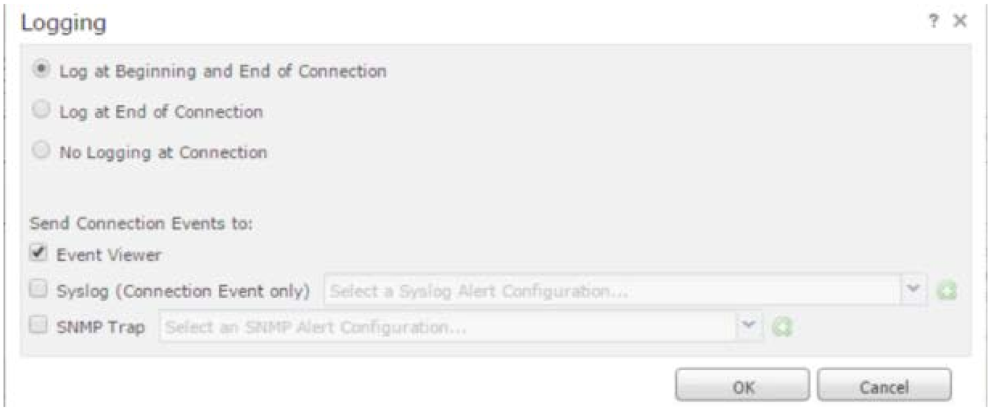
Step 13 Configure logging, by selecting 📄



This category is empty

Default Action: Intrusion Prevention: pxGrid Intrusion Policy

Step 14 Configure the following logging settings



Logging

● Log at Beginning and End of Connection

○ Log at End of Connection

○ No Logging at Connection

Send Connection Events to:

☑ Event Viewer

□ Syslog (Connection Event only) Select a Syslog Alert Configuration...

□ SNMP Trap Select an SNMP Alert Configuration...

Step 15 Click OK

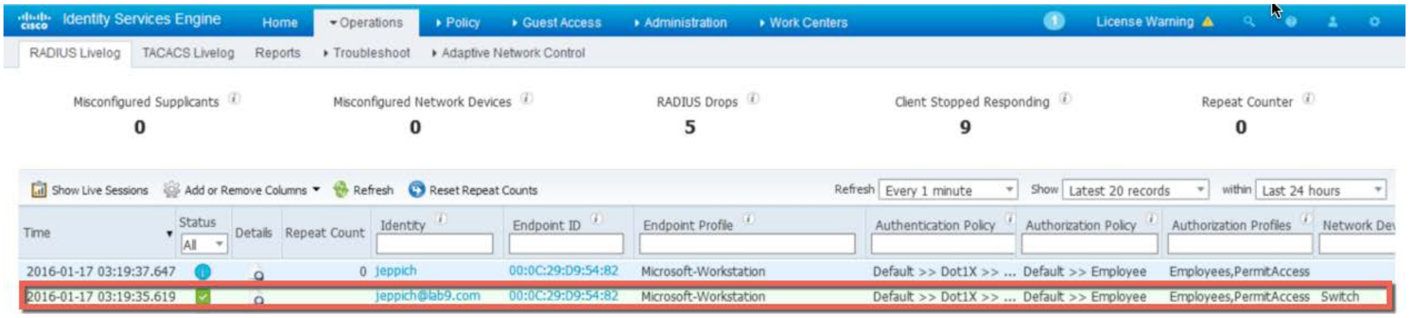
Step 16 Click Store ASA Firepower Changes

Step 17 Click Deploy->Deploy Firepower Changes->Deploy->OK

Step 18 Click Monitoring->ASA Firepower Monitoring->Task to view the deployment status

Testing User Employee SGT Using On-Box Firepower Management Policy

The employee has successfully authenticated to ISE and received an Employee SGT.

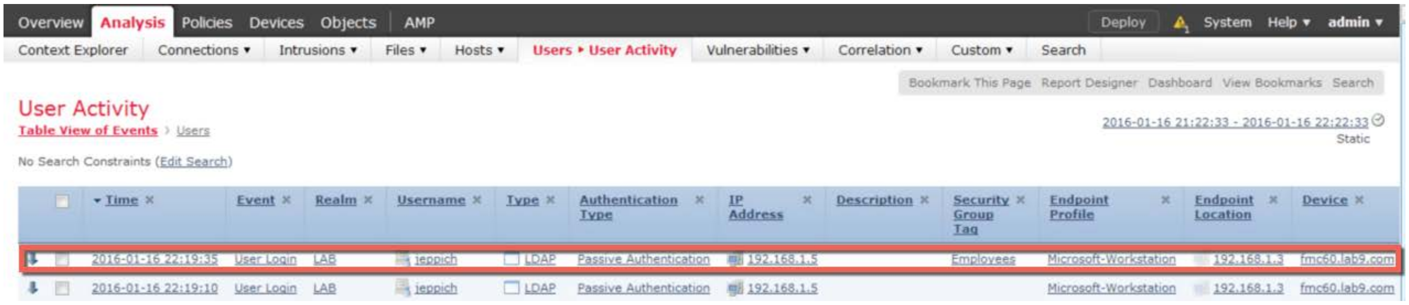


Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	5	9	0

Refresh: Every 1 minute · Show: Latest 20 records · within: Last 24 hours

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Dev
2016-01-17 03:19:37.647	●		0	jeppich	00:0C:29:D9:54:82	Microsoft-Workstation	Default >> Dot1X >> ...	Default >> Employee	Employees,PermitAccess	
2016-01-17 03:19:35.619	✓			jeppich@lab9.com	00:0C:29:D9:54:82	Microsoft-Workstation	Default >> Dot1X >> ...	Default >> Employee	Employees,PermitAccess	Switch

We see that Firepower Management Center has obtained the user session



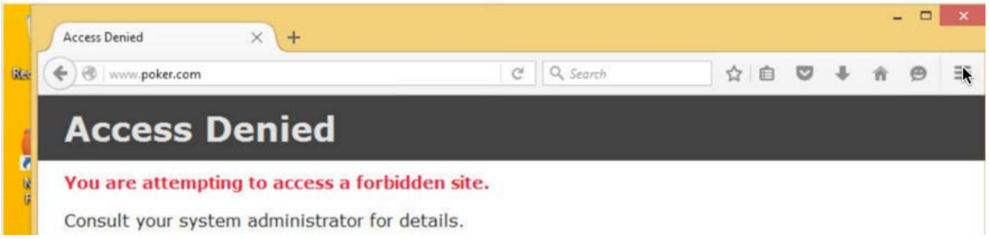
User Activity
Table View of Events › Users

2016-01-16 21:22:33 - 2016-01-16 22:22:33
Static

No Search Constraints (Edit Search)

Time	Event	Realm	Username	Type	Authentication Type	IP Address	Description	Security Group Tag	Endpoint Profile	Endpoint Location	Device
2016-01-16 22:19:35	User Login	LAB	jeppich	LDAP	Passive Authentication	192.168.1.5		Employees	Microsoft-Workstation	192.168.1.3	fmc60.lab9.com
2016-01-16 22:19:10	User Login	LAB	jeppich	LDAP	Passive Authentication	192.168.1.5			Microsoft-Workstation	192.168.1.3	fmc60.lab9.com

Note that when the employee accesses www.poker.com he is denied

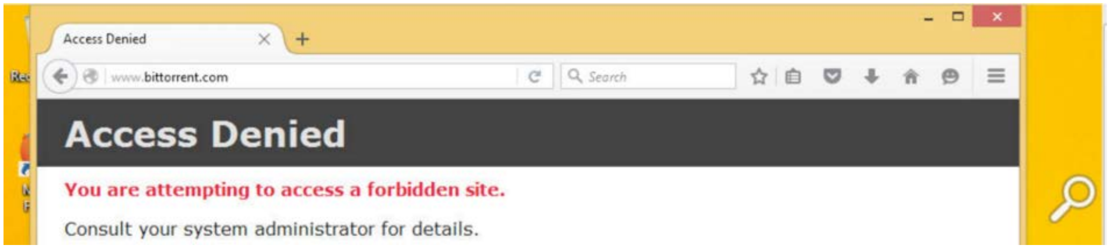


Access Denied

You are attempting to access a forbidden site.

Consult your system administrator for details.

When the employee accesses www.bittorent.com he is denied

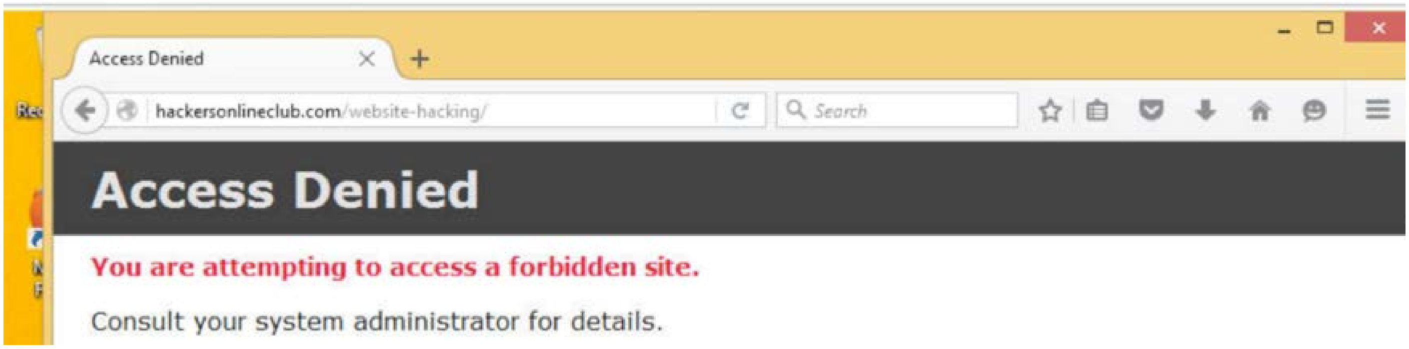


Access Denied

You are attempting to access a forbidden site.

Consult your system administrator for details.

When the employee tries to join a hacking club www. hackersonlineclub.com he is denied

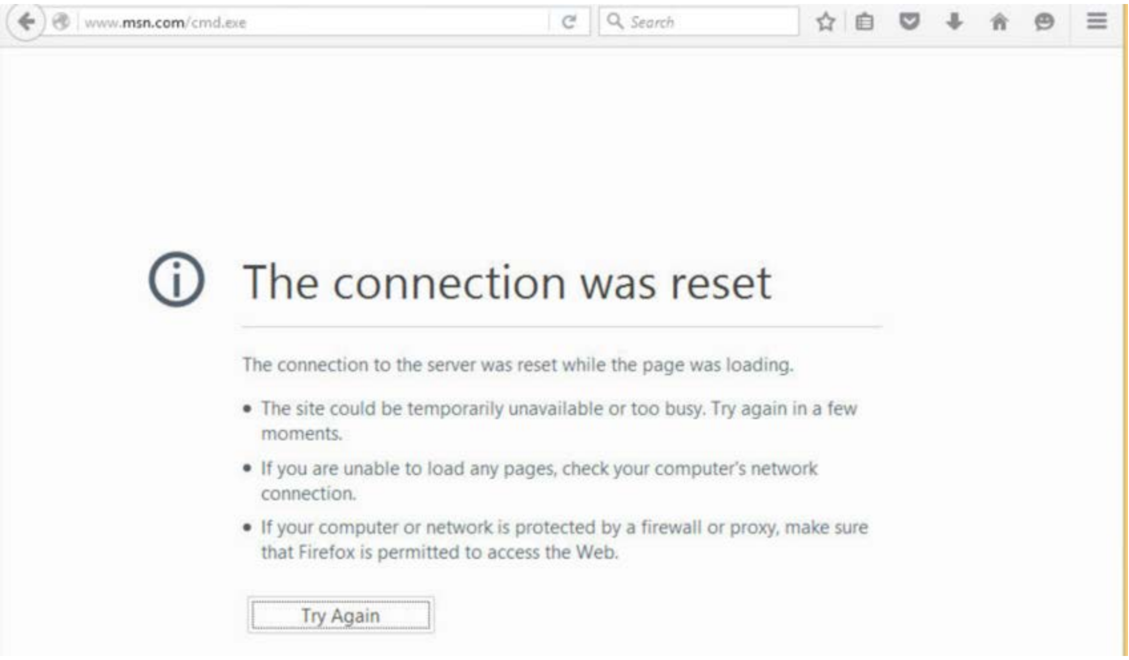


Access Denied

You are attempting to access a forbidden site.

Consult your system administrator for details.

Also when he tries to insert www.msn.com/cmd.exe into his browser, he is denied access.

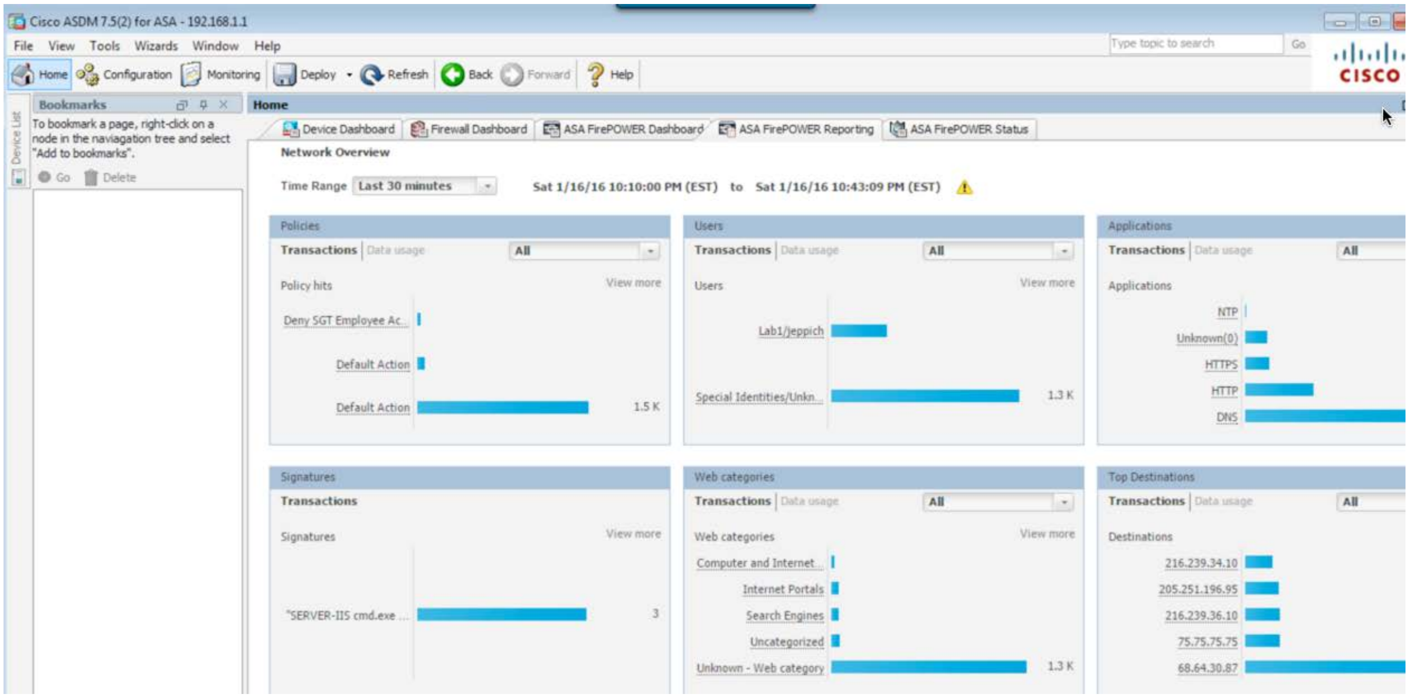


The connection was reset

The connection to the server was reset while the page was loading.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

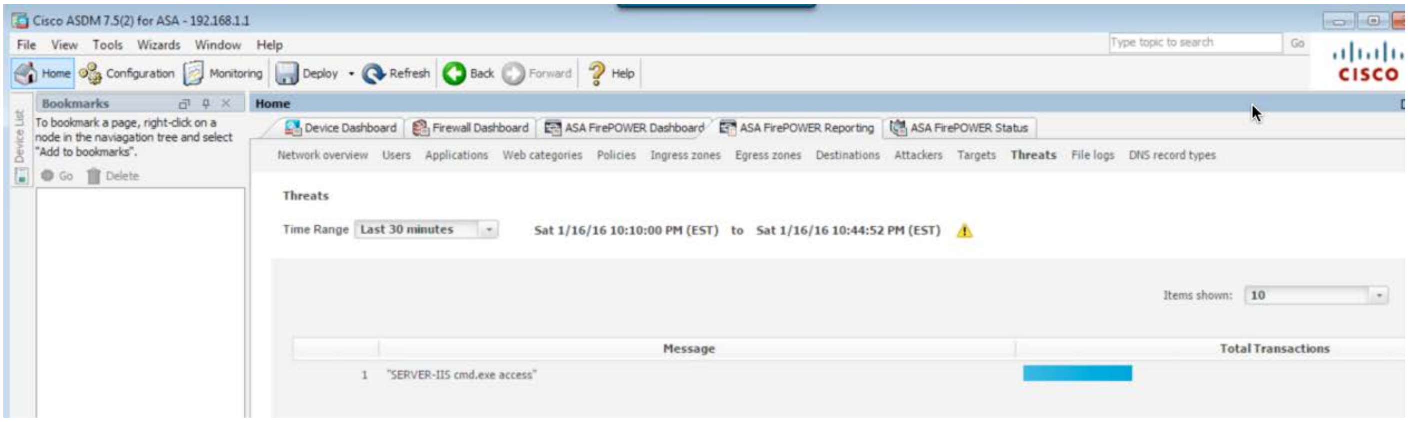
You can view the report on the ASA Firepower Reporting. Note the denied web category transactions and the server IIS- Web signature that fired.


Cisco ASDM 7.5(2) for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search Go
Home Configuration Monitoring Deploy Refresh Back Forward Help
Bookmarks
To bookmark a page, right-click on a node in the naviagation tree and select "Add to bookmarks".
Go Delete
Home
Device Dashboard Firewall Dashboard ASA FirePOWER Dashboard ASA FirePOWER Reporting ASA FirePOWER Status
Policies
Transactions | Data usage All
Policy hits View more
Deny SGT Employee Ac...
Default Action
Default Action 1.5 K
Users
Transactions | Data usage All
Users View more
Lab1/jeppich
Special Identities/Unkn... 1.3 K
Applications
Transactions | Data usage All
Applications
NTP
Unknown(0)
HTTPS
HTTP
DNS
Signatures
Transactions
Signatures View more
"SERVER-IIS cmd.exe ... 3
Web categories
Transactions | Data usage All
Web categories View more
Computer and Internet...
Internet Portals
Search Engines
Uncategorized
Unknown - Web category 1.3 K
Top Destinations
Transactions | Data usage All
Destinations
216.239.34.10
205.251.196.95
216.239.36.10
75.75.75.75
68.64.30.87

Network Overview

Time Range Last 30 minutes Sat 1/16/16 10:10:00 PM (EST) to Sat 1/16/16 10:43:09 PM (EST)

If you click under Threat reports note the signature for SERVER-IIS


Cisco ASDM 7.5(2) for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search Go
Home Configuration Monitoring Deploy Refresh Back Forward Help
Bookmarks
To bookmark a page, right-click on a node in the naviagation tree and select "Add to bookmarks".
Go Delete
Home
Device Dashboard Firewall Dashboard ASA FirePOWER Dashboard ASA FirePOWER Reporting ASA FirePOWER Status
Network overview Users Applications Web categories Policies Ingress zones Egress zones Destinations Attackers Targets Threats File logs DNS record types

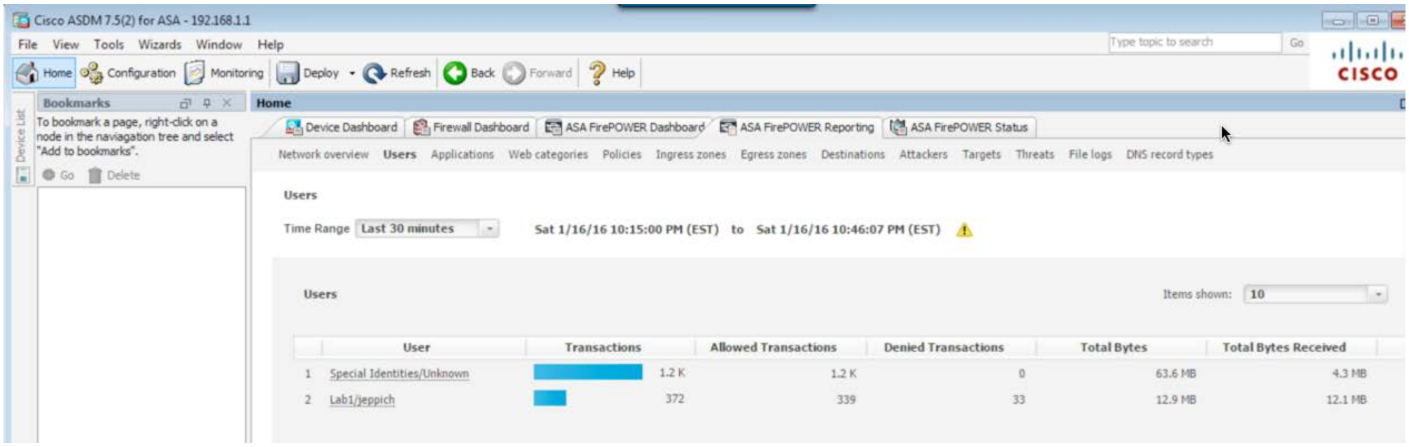
Threats

Time Range Last 30 minutes Sat 1/16/16 10:10:00 PM (EST) to Sat 1/16/16 10:44:52 PM (EST)

Items shown: 10

	Message	Total Transactions
1	"SERVER-IIS cmd.exe access"	

If you select Reports by users, and click on jeppich


Cisco ASDM 7.5(2) for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Deploy Refresh Back Forward Help
Bookmarks
To bookmark a page, right-click on a node in the navigation tree and select "Add to bookmarks".
Go Delete
Home
Device Dashboard
Firewall Dashboard
ASA FirePOWER Dashboard
ASA FirePOWER Reporting
ASA FirePOWER Status
Network overview Users Applications Web categories Policies Ingress zones Egress zones Destinations Attackers Targets Threats File logs DNS record types

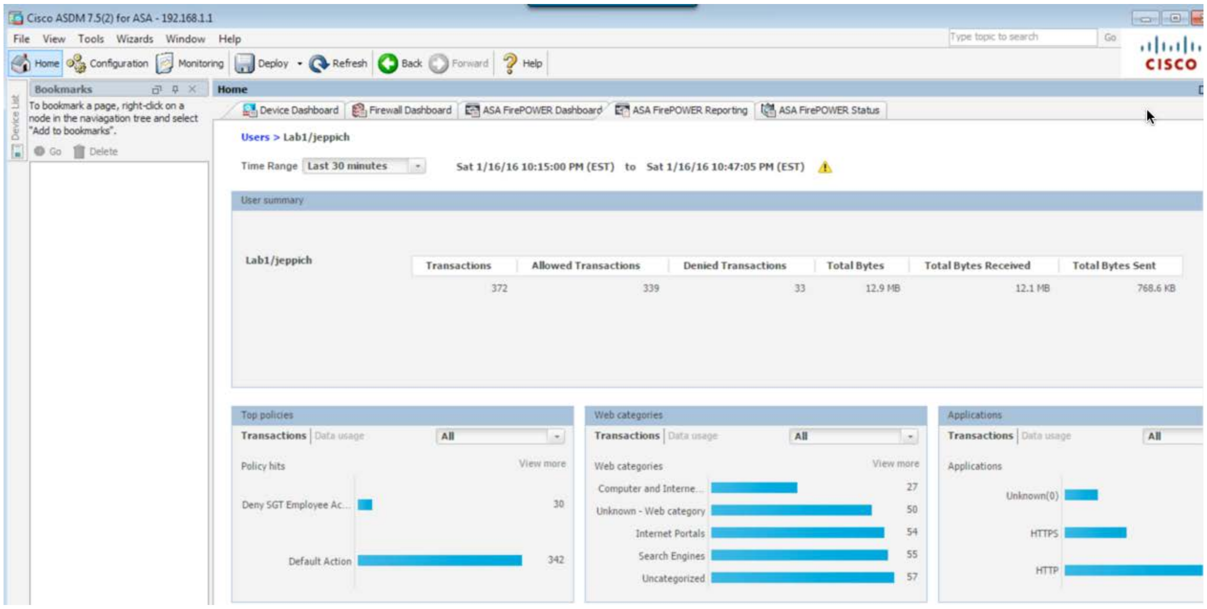
Users

Time Range: Last 30 minutes   Sat 1/16/16 10:15:00 PM (EST) to Sat 1/16/16 10:46:07 PM (EST)

Users   Items shown: 10

	User	Transactions	Allowed Transactions	Denied Transactions	Total Bytes	Total Bytes Received
1	Special Identities/Unknown	1.2 K	1.2 K	0	63.6 MB	4.3 MB
2	Lab1/jeppich	372	339	33	12.9 MB	12.1 MB

You will see the top transactions, web categories, and applications


Cisco ASDM 7.5(2) for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Deploy Refresh Back Forward Help
Bookmarks
To bookmark a page, right-click on a node in the navigation tree and select "Add to bookmarks".
Go Delete
Home
Device Dashboard
Firewall Dashboard
ASA FirePOWER Dashboard
ASA FirePOWER Reporting
ASA FirePOWER Status

Users > Lab1/jeppich

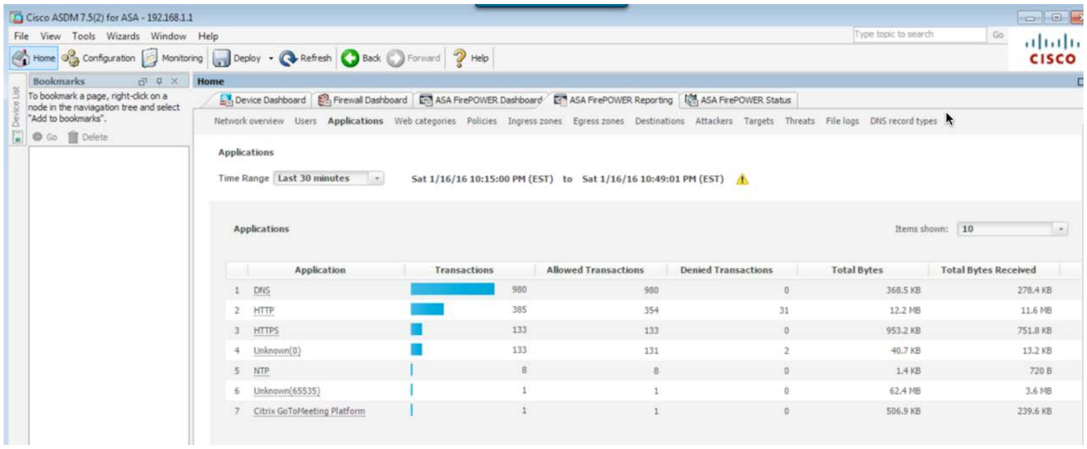
Time Range: Last 30 minutes   Sat 1/16/16 10:15:00 PM (EST) to Sat 1/16/16 10:47:05 PM (EST)

User summary

	Transactions	Allowed Transactions	Denied Transactions	Total Bytes	Total Bytes Received	Total Bytes Sent
Lab1/jeppich	372	339	33	12.9 MB	12.1 MB	768.6 KB

Top policies
Transactions | Data usage
All
Policy hits
View more
Deny SGT Employee Ac... 30
Default Action 342
Web categories
Transactions | Data usage
All
Web categories
View more
Computer and Interne... 27
Unknown - Web category 50
Internet Portals 54
Search Engines 55
Uncategorized 57
Applications
Transactions | Data usage
All
Applications
Unknown(0)
HTTPS
HTTP

You also have reports to view Applications



To bookmark a page, right-click on a node in the naviagation tree and select "Add to bookmarks".

Applications

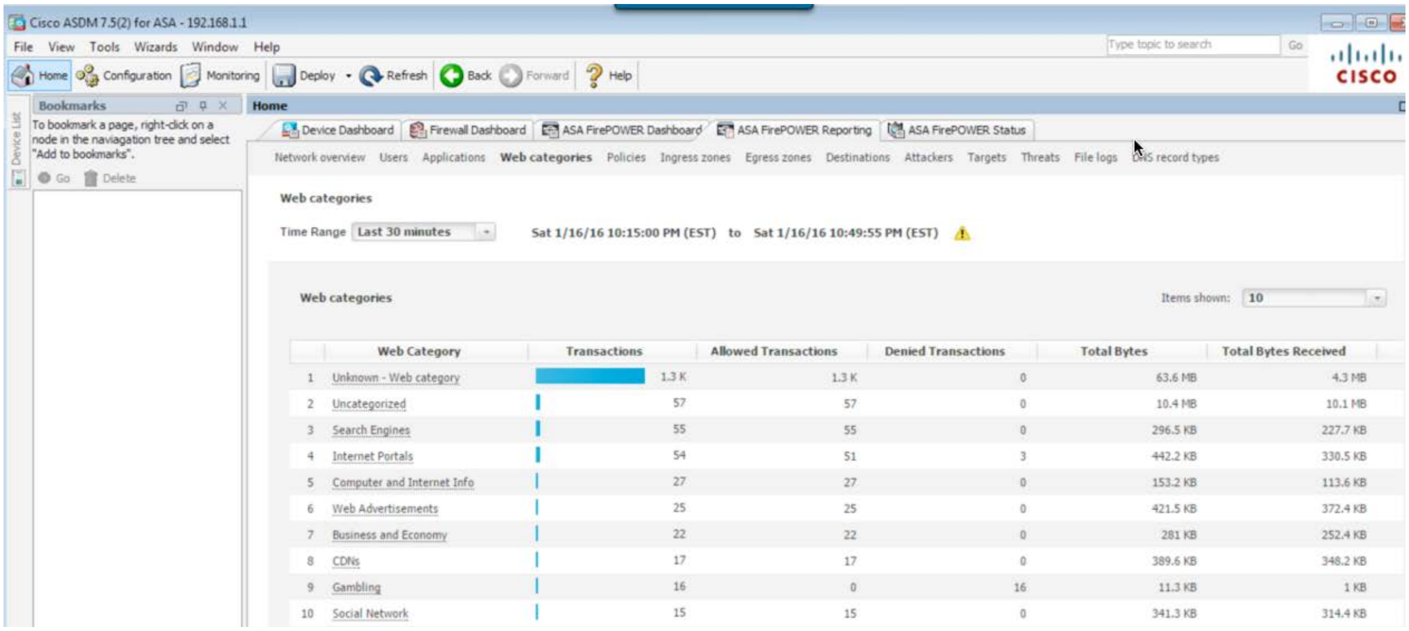
Time Range: Last 30 minutes   Sat 1/16/16 10:15:00 PM (EST) to Sat 1/16/16 10:49:01 PM (EST)

Applications

Items shown: 10

	Application	Transactions	Allowed Transactions	Denied Transactions	Total Bytes	Total Bytes Received
1	DNS	980	980	0	368.5 KB	278.4 KB
2	HTTP	385	354	31	12.2 MB	11.6 MB
3	HTTPS	133	133	0	953.2 KB	751.8 KB
4	Unknown(0)	133	131	2	40.7 KB	13.2 KB
5	NTP	8	8	0	1.4 KB	720 B
6	Unknown(65535)	1	1	0	62.4 MB	3.6 MB
7	Citrix GoToMeeting Platform	1	1	0	506.9 KB	239.6 KB

You can also view reports based on policy



To bookmark a page, right-click on a node in the naviagation tree and select "Add to bookmarks".

Web categories

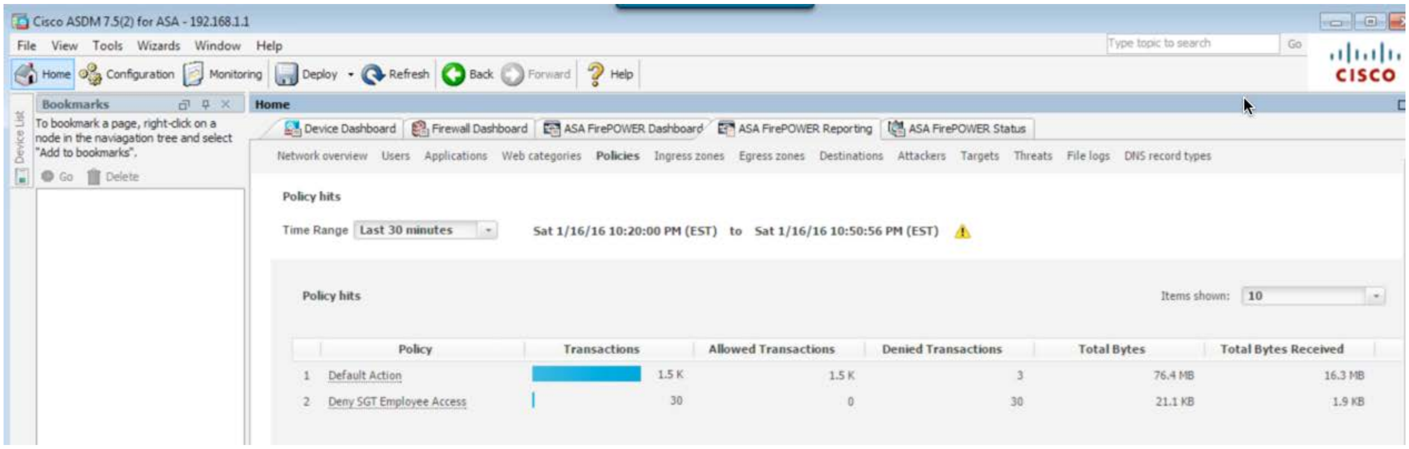
Time Range: Last 30 minutes   Sat 1/16/16 10:15:00 PM (EST) to Sat 1/16/16 10:49:55 PM (EST)

Web categories

Items shown: 10

	Web Category	Transactions	Allowed Transactions	Denied Transactions	Total Bytes	Total Bytes Received
1	Unknown - Web category	1.3 K	1.3 K	0	63.6 MB	4.3 MB
2	Uncategorized	57	57	0	10.4 MB	10.1 MB
3	Search Engines	55	55	0	296.5 KB	227.7 KB
4	Internet Portals	54	51	3	442.2 KB	330.5 KB
5	Computer and Internet Info	27	27	0	153.2 KB	113.6 KB
6	Web Advertisements	25	25	0	421.5 KB	372.4 KB
7	Business and Economy	22	22	0	281 KB	252.4 KB
8	CDNs	17	17	0	389.6 KB	348.2 KB
9	Gambling	16	0	16	11.3 KB	1 KB
10	Social Network	15	15	0	341.3 KB	314.4 KB

and policy hits



Cisco ASDM 7.5(2) for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Deploy Refresh Back Forward Help
Bookmarks
To bookmark a page, right-click on a node in the navigation tree and select "Add to bookmarks".
Go Delete
Device List
Home
Device Dashboard
Firewall Dashboard
ASA FirePOWER Dashboard
ASA FirePOWER Reporting
ASA FirePOWER Status
Network overview Users Applications Web categories Policies Ingress zones Egress zones Destinations Attackers Targets Threats File logs DNS record types

Policy hits

Time Range Last 30 minutes Sat 1/16/16 10:20:00 PM (EST) to Sat 1/16/16 10:50:56 PM (EST)

Policy hits

Items shown: 10

	Policy	Transactions	Allowed Transactions	Denied Transactions	Total Bytes	Total Bytes Received
1	Default Action	1.5 K	1.5 K	3	76.4 MB	16.3 MB
2	Deny SGT Employee Access	30	0	30	21.1 KB	1.9 KB

Troubleshooting

ISE pxGrid Node

pxGrid published nodes do not appear and there is no pxGrid connectivity

- If using self-signed certs with ISE 1.3/1.4, make sure that you have export the ISE self-signed Identity certificate into the ISE system trusted store, before enabling pxGrid.
- If use CA-signed certs ensure that the customized pxGrid template has an EKU of both server authentication an client authentication, before enabling pxGrid
- If deploying pxGrid in a productional environment and the dedicated ISE pxGrid node has its public/private key pair imported into the PPAN and PMNT nodes. If pxGrid-Active Standby is implemented, the secondary pxGrid nodes should have a public/private key imported into the secondary SPAN and secondary SMNT nodes.
  Only on pxGrid node can be active, run application status ise to ensure that the ISE pxGrid node is the active one.
- power down/up ISE Run **application stop ise/application start ise.** You may also disable pxGrid from the ISE node, before stopping the ISE service; Once ISE is back up enable for pxGrid.
- Downloaded certificates should be in base 64 encoded format

Firepower Management Center 6.0

System Integration ISE certificate test fails

- If using ISE 1.3/1.4 in a stand-alone POC environment using self-signed certs and if you have not set as primary, there is a known bulk download session bug that can resolve FQDN issue. Promote to primary to resolve. This is not an issue with ISE 2.0
- If using ISE in a stand-alone environment for CA-signed cert operation, make sure the purpose of the CSR request is admin and NOT pxGrid. This is required for active bulk download record sessions.
- For CA-signed operation:
- For self-signed operation:
- FMC 6.0, ISE pxGrid node, devices should be all DNS resolvable

Not Seeing Correlation Events from ISE

- Ensure time is synced between FMC and ISE. Time should also be synced between the FMC and all the registered devices

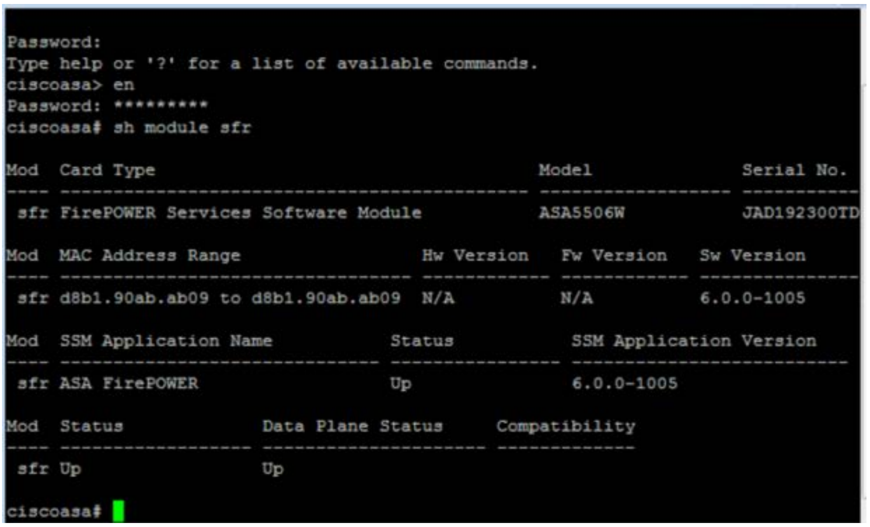
ASA with Firepower Services

Cannot Modify registered ASA device parameters on Firepower Management Center

- Ensure you have the proper device licenses for the proper ASA model on the Firepower Management center

SFR is still in the recovery state

- Re-run SFR installation, this takes awhile. On my ASA 5506 it took over 30 minutes. Run sh module sfr to ensure that is up



```
Password:
Type help or '?' for a list of available commands.
ciscoasa> en
Password: *********
ciscoasa# sh module sfr

Mod  Card Type                                    Model              Serial No.
---- -------------------------------------------- ------------------ -----------
 sfr FirePOWER Services Software Module           ASA5506W           JAD192300TD

Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
 sfr d8b1.90ab.ab09 to d8b1.90ab.ab09  N/A          N/A          6.0.0-1005

Mod  SSM Application Name           Status           SSM Application Version
---- ------------------------------ ---------------- --------------------------
 sfr ASA FirePOWER                  Up               6.0.0-1005

Mod  Status             Data Plane Status     Compatibility
---- ------------------ --------------------- -------------
 sfr Up                 Up

ciscoasa#
```

No traffic on ASA Firepower reports

- Configure all traffic to the ASA Firepower Services
- Below is a sample configuration

```
ciscoasa# conf t
ciscoasa(config)# sh run policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
```

```
!
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class class-default
ciscoasa(config-pmap-c)# sfr fail-open
ciscoasa(config-pmap-c)#
ciscoasa(config-pmap-c)# sh service-policy

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 5531, lock fail 0, drop 0, reset-drop 0, 5-min-

pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: ftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: h323 h225 _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0,

5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: h323 ras _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5

-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: rsh, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: rtsp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: esmtp _default_esmtp_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-

min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: sqlnet, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: skinny , packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: sunrpc, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: xdmcp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: sip , packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: netbios, packet 15, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: tftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: ip-options _default_ip_options_map, packet 0, lock fail 0, drop 0, reset-

drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
    Class-map: class-default

      Default Queueing      SFR: card status Up, mode fail-open
        packet input 250, packet output 250, drop 0, reset-drop 0
ciscoasa(config-pmap-c)#
ciscoasa(config-pmap-c)
ciscoasa(config-pmap-c)# sh service-policy sfr

Global policy:
  Service-policy: global_policy
    Class-map: class-default
      SFR: card status Up, mode fail-open
        packet input 264, packet output 264, drop 0, reset-drop 0
ciscoasa(config-pmap-c)# sh service-policy sfr

Global policy:
  Service-policy: global_policy
    Class-map: class-default
      SFR: card status Up, mode fail-open
        packet input 290, packet output 290, drop 0, reset-drop 0
ciscoasa(config-pmap-c)#
```

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: http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-88-Configuring-pxGrid-in-an-ISE-Distributed-Environment.pdf

How-To Deploying Certificates with Cisco pxGrid: Configuring CA-Signed ISE pxGrid Node and CA-Signed pxGrid client: http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-89-CA_signed_pxGridISEnode_CAsigned_pxGridclient.pdf

How-To Deploying Certificates with Cisco pxGrid: Self-Signed Certs with ISE pxGrid Node and pxGrid client: http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-90-Self_signed_pxGridClient_selfsigned_pxGrid.pdf

Cisco Firepower Management Center 6.0 Configuration Guide

http://www.cisco.com/c/en/us/td/docs/security/Firepower/60/configuration/guide/fpmc-config-guide-v60.html