+

How-To Integrate Infoblox and Cisco Identity Services Engine (ISE) using Cisco Platform Exchange Grid (pxGrid)

Author: John Eppich

Table of Contents

About This Document

This document is for Cisco engineers and customers who are planning to integrate Infoblox NIOS and Cisco Identity Service Engine (ISE) 2.1 using Cisco Platform Exchange Grid (pxGrid). Infoblox NIOS version 7.3.6 software was used for both the virtual Grid Master and Network Discovery (ND) member.

This document includes:

- Configuring Infoblox and the ISE pxGrid node for both Self-signed and CA-signed certificates
- Configuring the Infoblox Grid Master (GM) and Infoblox Network Discovery (ND) member
- Configuring DHCP and DNS services on the Infoblox GM
- Configuring Infoblox ISE Ecosystem parameters and connecting to the ISE pxGrid node
- Creating Infoblox DHCP and IPAM notifications for publishing Dynamic Topic information
- Creating Infoblox RPZ notifications to send blocked DNS responses to the ISE pxGrid
- Creating ISE EPS Quarantine Authorization policy
- Populating Infoblox IPAM table with pxGrid session information
- Quarantining an endpoint due to an Infoblox RPZ violation

The reader will observe and become familiar with the ISE user session information that will populate the IPAM table for more contextual information around IP events. Additionally, a RPZ (Response Policy Zone) will be created for blocking www.yahoo.com , with the results the of the endpoint being quarantined.

ISE was configured in a Stand-alone environment for testing. For configuring ISE in a distributed environment, please see https://communities.cisco.com/docs/DOC-68284

Introduction

Infoblox is an integrated security, and centrally managed DNS, DHCP, and IP address management (DDI) solution supporting current and evolving IT needs while providing the highest standards for service uptime, operational efficiencies, security and IT ecosystem integration.

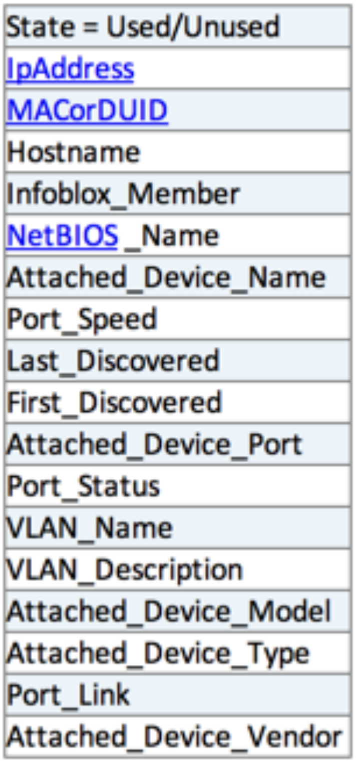
Infoblox Grid Master contains the managed IPAM, DNS, DHCP network services, while Insight Manager or Network Discovery member provides L3 or L2 network visibility around the IPAM and DHCP events.

Cisco ISE (Identity Services Engine) is an identity solution, providing ISE 802.1X authentication for wired, wireless and virtual environments. In addition, ISE can perform additional functions such as Guest, Posture, and incorporate SGT (Security Group Tags), which is a component for the Cisco TrustSec Solution. When a user or device authenticates to the network, there is rich contextual information that is available from these authenticated session. This session information may include the username, IP address, MAC address, posture status, SGT, and endpoint profile information that provides more information around the IP event.

Cisco pxGrid is a framework for this context-sharing of ISE information and makes this session information available to Infoblox and other Cisco Ecosystem partners. Starting with Cisco ISE 2.0, context sharing can be bi-directional, where Infoblox and other Cisco Ecosystem partners can share information on topics with each other while registered and connected to the grid. This bi-directional context sharing is called Dynamic Topics.

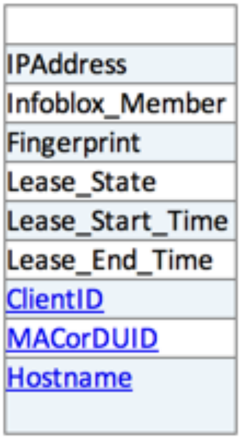
Infoblox publishes IPAM and DHCP dynamic topics and makes this information available as attributes.

Available IPAM attributes in IPAM Dynamic Topic



State = Used/Unused
IpAddress
MACorDUID
Hostname
Infoblox_Member
NetBIOS _Name
Attached_Device_Name
Port_Speed
Last_Discovered
First_Discovered
Attached_Device_Port
Port_Status
VLAN_Name
VLAN_Description
Attached_Device_Model
Attached_Device_Type
Port_Link
Attached_Device_Vendor

Available DHCP attributes in DHCP Dynamic Topic



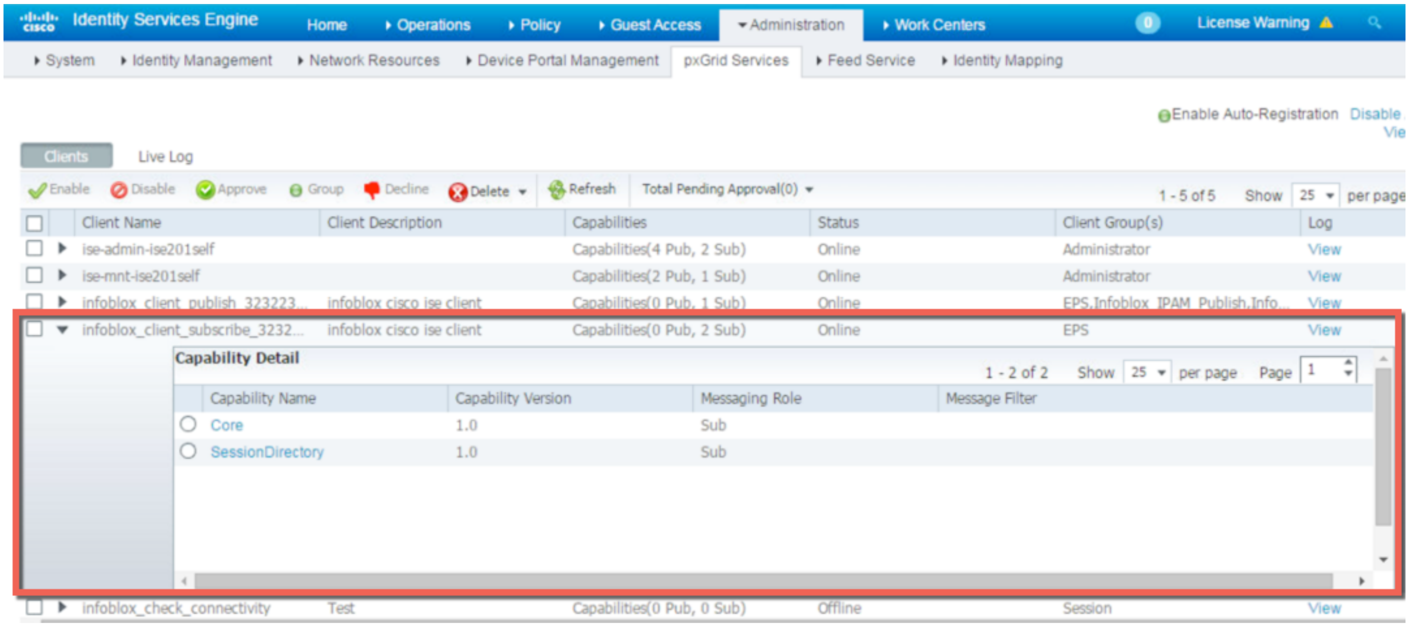
IPAddress
Infoblox_Member
Fingerprint
Lease_State
Lease_Start_Time
Lease_End_Time
ClientID
MACorDUID
Hostname

Cisco pxGrid also provides Adaptive Network Control (ANC) mitigation actions such as quarantining an endpoint due to a violation with the security solution's organizational security policy. This is implemented in Infoblox via RPZ rule violations based on the DNS service policy.

Technical Theory

The Infoblox (GM) Grid Master will authenticate, connect and register to the ISE pxGrid node as a pxGrid client either using either self-signed or CA-signed certificates. The Infoblox Grid Master (GM) will subscribe to the ISE Session Directory Topic and obtain the username, Audit Session ID, EPS Status, NAS IP Address, MAC address, IP Address, Quarantine Status, Security Group Tag, Posture Timestamp, Posture Status. The Infoblox Grid Master will also subscribe to the EndpointProtection Service Capability to perform Adaptive Network Control (ANC) mitigation actions such as quarantining an endpoint. Unquarantining the endpoint must be done manually via ISE using the Adaptive Network Control unquarantine menu or via the ISE EPS Unquarantine RESTful API.

Infoblox is the first ecosystem partner to become a publisher of Dynamic Topics. Infoblox will publish the IPAM and DHCP attributes to other pxGrid clients connected to the grid. These pxGrid clients must subscribe to these topics to consume this information.

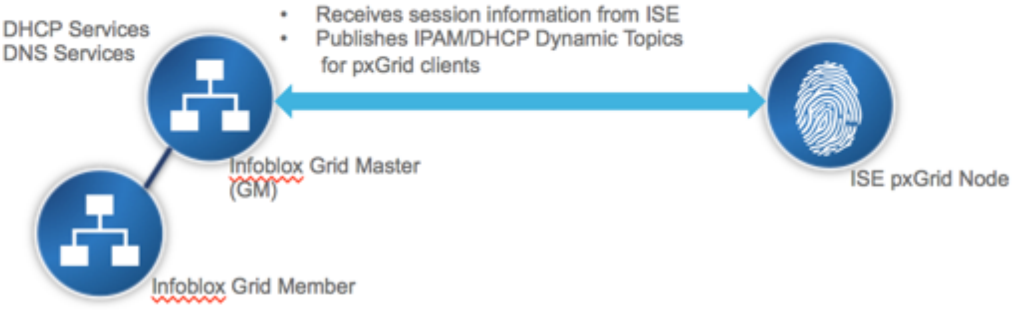


□		Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	▸	ise-admin-ise201self		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	▸	ise-mnt-ise201self		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	▸	infoblox_client_publish_323223...	infoblox cisco ise client	Capabilities(0 Pub, 1 Sub)	Online	EPS,Infoblox_IPAM_Publish,Info...	View
□	▾	infoblox_client_subscribe_3232...	infoblox cisco ise client	Capabilities(0 Pub, 2 Sub)	Online	EPS	View
□	▸	infoblox_check_connectivity	Test	Capabilities(0 Pub, 0 Sub)	Offline	Session	View

Capability Detail

1 - 2 of 2 Show 25 per page Page 1

	Capability Name	Capability Version	Messaging Role	Message Filter
○	Core	1.0	Sub	
○	SessionDirectory	1.0	Sub	


DHCP Services
DNS Services
Receives session information from ISE
Publishes IPAM/DHCP Dynamic Topics for pxGrid clients
Infoblox Grid Master (GM)
ISE pxGrid Node
Infoblox Grid Member

Configuring the Infoblox Grid Master (GM) and Network Discovery (ND) Member

This section describes the installation of the Infoblox Grid Master (GM) and the Infoblox Network Discovery (ND) member. Please note that the installation of both the Infoblox Grid Master and the Infoblox Network Discovery member will be on virtual appliances. This section also describes the procedures for creating temporary licenses, creating the network configuration and for joining the Infoblox ND member to the Infoblox GM.

Configuring the Infoblox Grid Master

Creating Temporary Licenses

This procedure steps the reader through setting up the 60-day temporary licenses

Step 1 Type the following to set your temporary licenses on the Grid Master

```
set temp_license
 1. DNSone (DNS, DHCP)
 2. DNSone with Grid (DNS, DHCP, Grid)
 3. Network Services for Voice (DHCP, Grid)
 4. Add DNS Server License
 5. Add DHCP Server License
 6. Add Grid License
 7. Add Microsoft Management License
 8. Add VNIOS License
 9. Add Mult-Grid Management License
 10.Add Query Redirection License
 11.Add Load Balancer License
 12.Add Response Policy Zones License
 13.Add FireEye license
 14.Add DNS Traffic Control License
 15.Add Cloud Network Automation License
 16.Add Security Ecosystem License
 17.Add Threat Analytics License

Select License (1-17) or q to quit:
```

Step 2 Select licenses individually: **2, 8, 12, 16**

Note: Most licenses will restart the GUI, adding the VNIOS license will restart the VM

Configure Network Settings

This section steps the reader through configuring the network settings and browser configuration settings for the Infoblox GM

Step 1 Configure the network settings

```
set network

NOTICE: All HA Configurations are performed from the GUI.  This interface is used only to configure a stand-
alone node or to join a Grid.

Enter IP address: 192.168.1.88
Enter netmask: [Default: 255.255.255.0]: 255.255.255.0
Enter gateway address [Default: 10.1.1.1]: 192.168.1.1
Become Grid member? [Y or n]:n
```

Step 2 Open browser and connect to https:// {ip_address} i.e. **https://192.168.1.88**

Step 3 Login with the default credentials, username/password: **admin/infoblox**

Step 4 Review the End-User License Agreement and click **I Accept**

Step 5 In the *Grid Setup* Wizard select **Configure a Grid Master** and click **Next**

Step 6 Enter the following Grid Master properties

- **Grid name:** (i.e. **niosgm2**), this is Grid Master name that members will connect to.
- **Shared Secret:** (i.e. **cisco123**) this is the shared secret for joining members to the Grid Master.
- **Show Password:** Select this to display the password.
- **Hostname:** (i.e. **niosgm2.lab10.com**) Enter a FQDN for the GM.
- **Is the Grid Master a HA pair**: Select **No**

Note: We will not cover configuring Infoblox in a HA pair

Step 7 Select **Next**

Step 8 Enter the following network settings for the Grid Master:

- **IP address:** (i.e. **192.168.1.88**)
- **Subnet Mask:** (i.e. **255.255.255.0**)
- **Gateway:** (i.e. **192.168.1.1**)
- **Port Settings:** The default is **Automatic.**

Note: You cannot change the port settings in a VNIOS appliance

Step 9 Select **Next**

Step 10 Set the admin password for changing the default admin/infoblox web GUI password

Step 11 Select **Next**.

Step 12 Enable NTP and specify the NTP Server

Step 13 Verify settings are correct and click **Finish.** The application will restart

Configuring the ND Grid Member

Creating Temporary Licenses

This procedure steps the reader through setting up the 60-day temporary licenses

Step 1 Type the following:

```
set temp_license
 1. Add Grid License
 2. Add vNIOS License
 3. Add Discovery License

Select license (1-3) or q to quit:
```

Step 2 Select licenses individually: **1,2,3**

Note: selecting vNIOS license will reboot the virtual appliance

Configure Network Settings

This section steps the reader through configuring the network settings and browser configuration settings for the Infoblox GM.

Step 1 Select the network settings and join the vNIOS appliance to the Grid. Use the CLI command **set network** to configure the network settings and specify the Grid

```
set network
NOTICE: All HA Configurations are performed from the GUI.  This interface is used only to configure a stand-
alone node or to join a Grid.

Enter IP address: 192.168.1.89
Enter netmask: [Default: 255.255.255.0]: 255.255.255.0
Enter gateway address [Default: 10.1.1.1]: 192.168.1.1
Enter VLAN tag [Default: Untagged]
Configure IPv6 network settings? (y or n):n
Become Grid member? [Y or n]:y
Enter Grid Master VIP: 192.168.1.88
Enter Grid Name:niosgm2
Enter Grid Shared Secret: cisco123
WARNING: Joining a Grid will replace all the data on this node:
IS this correct? ( y or n): y
Are you sure? (y or no): y
The network settings have been applied
```

Provisioning Grid Member to the Grid Master

Before adding additional members to the Grid, they must be defined on the Grid Master, as follows:

Step 1 Login to the Infoblox GM

Step 2 From the **Grid** tab, select the **Grid Manager** tab->**Members** tab, and then click **Add->Add Grid Member** from the Toolbar

Step 3 In the *Add Grid Member* wizard, enter the following:

- **Member Type:** Select **Virtual NIOS**
- **Hostname:** (i.e. **niosnd2.lab10.com**) this will be the FQDN of the new Grid Member
- **Time Zone:** If the vNIOS Grid member is in a different time zone from the Grid, click **Override** and select a time zone.
- **Comment:** optional

Step 4 Click **Next**

Step 5 Enter the following information about the member that you want to add to the Grid:
For a single Grid Member:

- **Standalone Member**: Select this option
- **Address:** (i.e. **192.168.1.89**) this will be the IP address of the new Grid Member
- **Subnet Mask:** (i.e. **255.255.255.0**) the netmask of the new member
- **Gateway:** (i.e. **192.168.1.1**) the default route of the new member
- **Port Settings:** The default is **Automatic**.

Note: You cannot change port settings for vNIOS appliances

Note: Configuring a vNIOS HA pair is not covered in this document

Step 6 Select **Next**

Step 7 There are no extensible attributes that need to be defined.

Step 8 Save the configuration and click **Refresh** 🔄

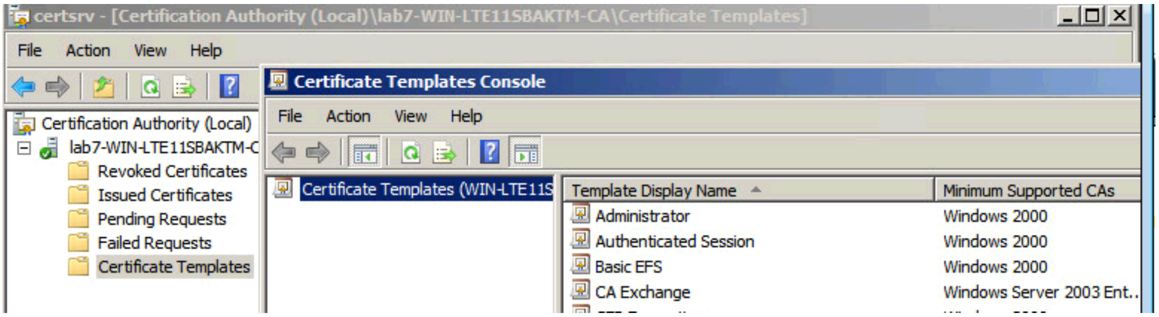
Configuring for CA-signed Operation

This section steps through CA-signed certificate operation for both the Infoblox GM and the ISE pxGrid node. Please note that ISE is deployed in a Stand-alone configuration. For a distributed ISE deployment, please see https://communities.cisco.com/docs/DOC-68284. A customized pxGrid template having an EKU of both client and server authentication is required and is included in this section as well.

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, Infoblox Grid Master and the ISE pxGrid node. This is required for a Certificate Authority (CA)-signed environment where both the Infoblox Grid Master Center and the ISE pxGrid node are signed by the same CA.

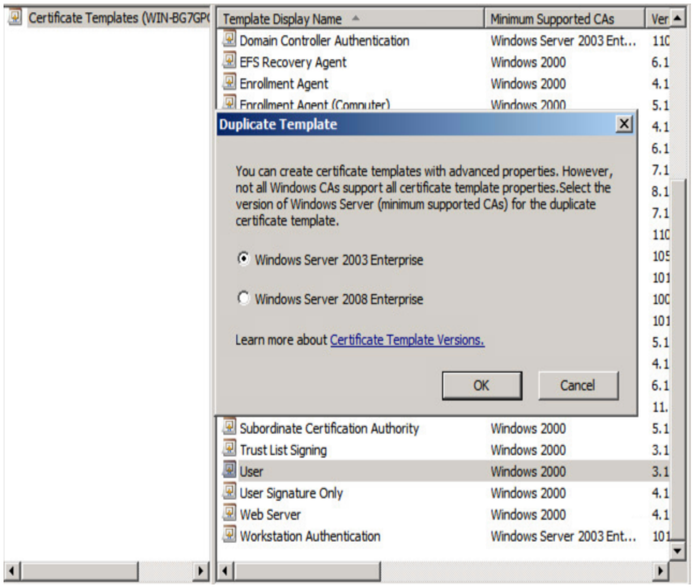
Step 1 Select **Administrative Tools->Certificate Authority-> "+" dropdown next to CA server->Right-Click on Certificate Templates->Manage**



certsrv - [Certification Authority (Local)\lab7-WIN-LTE11SBAKTM-CA\Certificate Templates]

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

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



Template Display Name	Minimum Supported CAs	Ver
Domain Controller Authentication	Windows Server 2003 Ent...	110
EFS Recovery Agent	Windows 2000	6.1
Enrollment Agent	Windows 2000	4.1
Enrollment Agent (Computer)	Windows 2000	5.1
		4.1
		6.1
		7.1
		8.1
		7.1
		110
		105
		101
		100
		101
		5.1
		4.1
		6.1
		11.
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

Duplicate Template

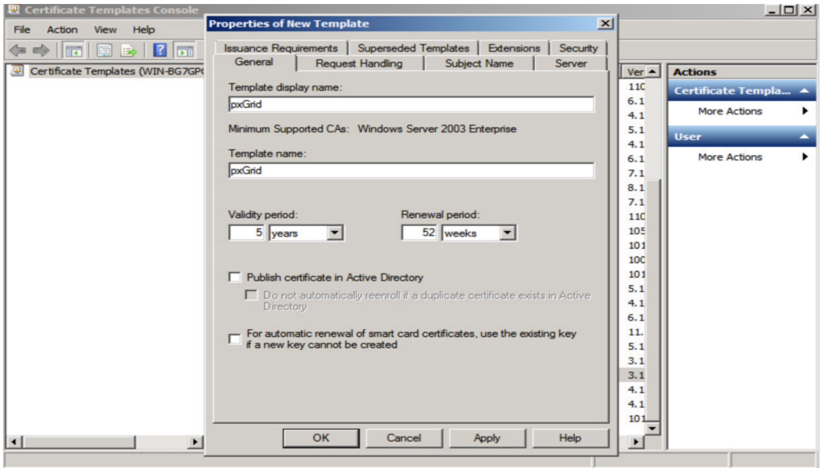
You can create certificate templates with advanced properties. However, not all Windows CAs support all certificate template properties.Select the version of Windows Server (minimum supported CAs) for the duplicate certificate template.

● Windows Server 2003 Enterprise

○ Windows Server 2008 Enterprise

Learn more about Certificate Template Versions.

Step 3 **Enter name of certificate template**, **uncheck** “Publish certificate in Active Directory”, and **provide validity period and renewal period**.


Certificate Templates Console
File Action View Help
Certificate Templates (WIN-BG7GP
Properties of New Template
Issuance Requirements | Superseded Templates | Extensions | Security
General | Request Handling | Subject Name | Server
Actions
Certificate Templa...
More Actions
User
More Actions
OK Cancel Apply Help

Template display name: pxGrid

Minimum Supported CAs: Windows Server 2003 Enterprise

Template name: pxGrid

Validity period: 5 years

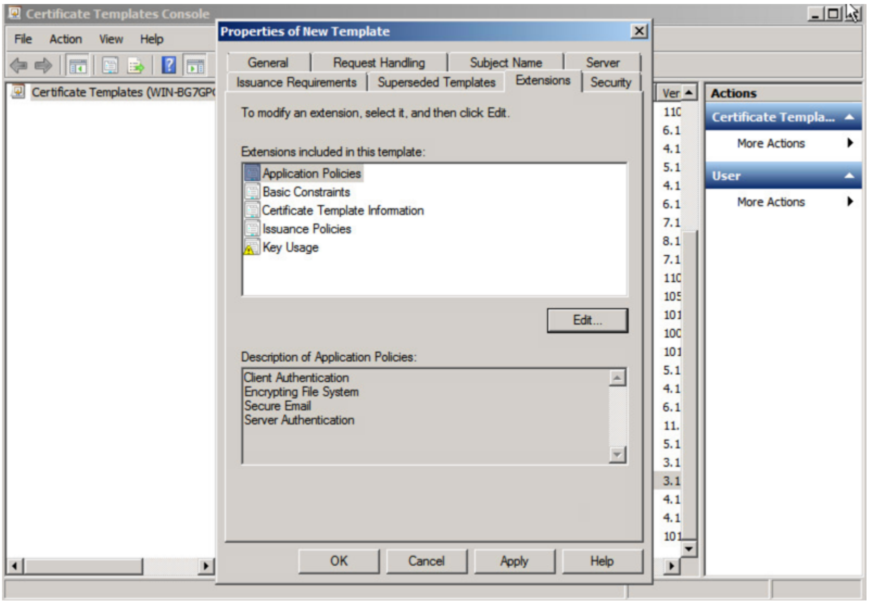
Renewal period: 52 weeks

□ 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 4 Click on **Extensions->Add->Server Authentication->Ok->Apply**


Certificate Templates Console
File Action View Help
Certificate Templates (WIN-BG7GP
Properties of New Template
General | Request Handling | Subject Name | Server
Issuance Requirements | Superseded Templates | Extensions | Security
Edit...
Actions
Certificate Templa...
More Actions
User
More Actions
OK Cancel Apply Help

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

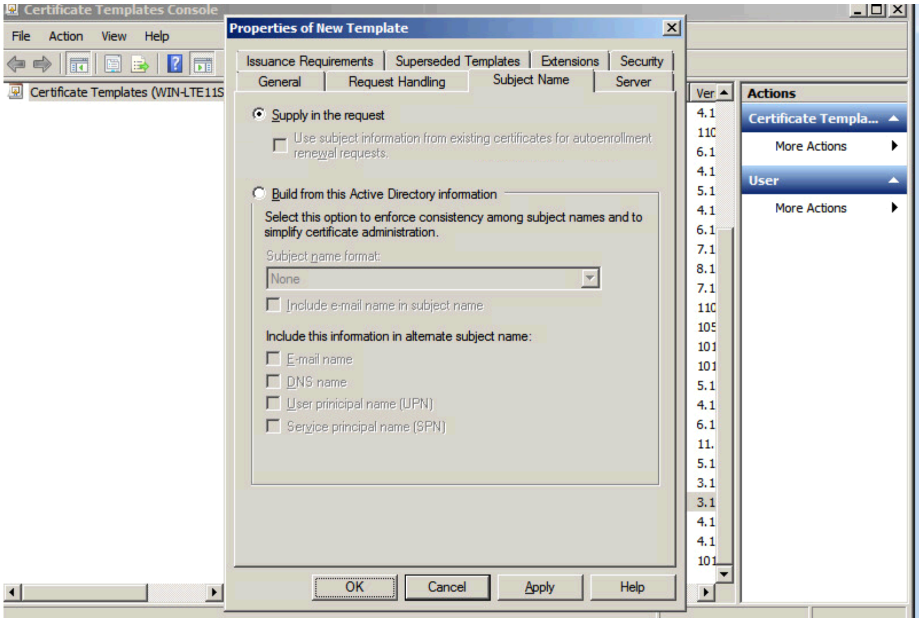
Extensions included in this template:

- 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 5 Click on Subject name, **enable** "Supply in the 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:

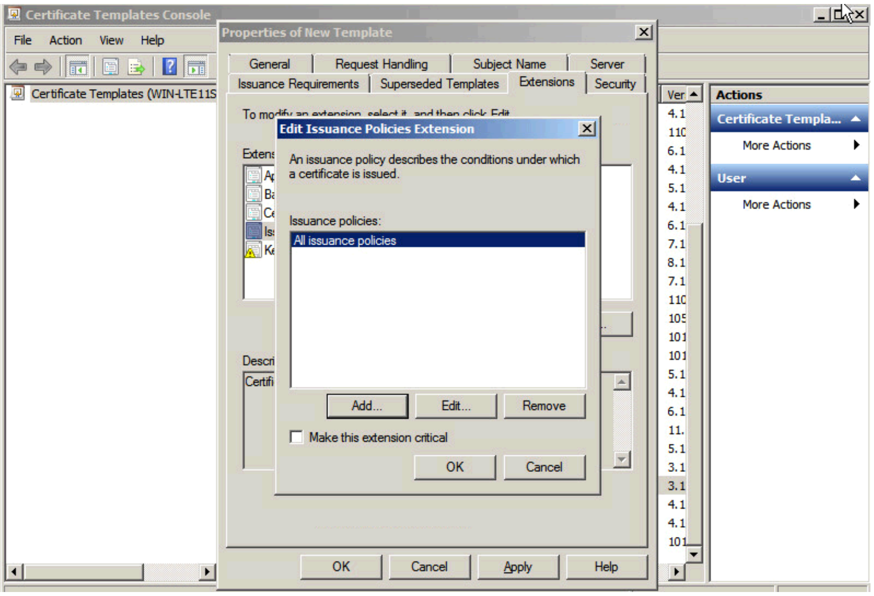
□ E-mail name

□ DNS name

□ User principal name (UPN)

□ Service principal name (SPN)

Step 6 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

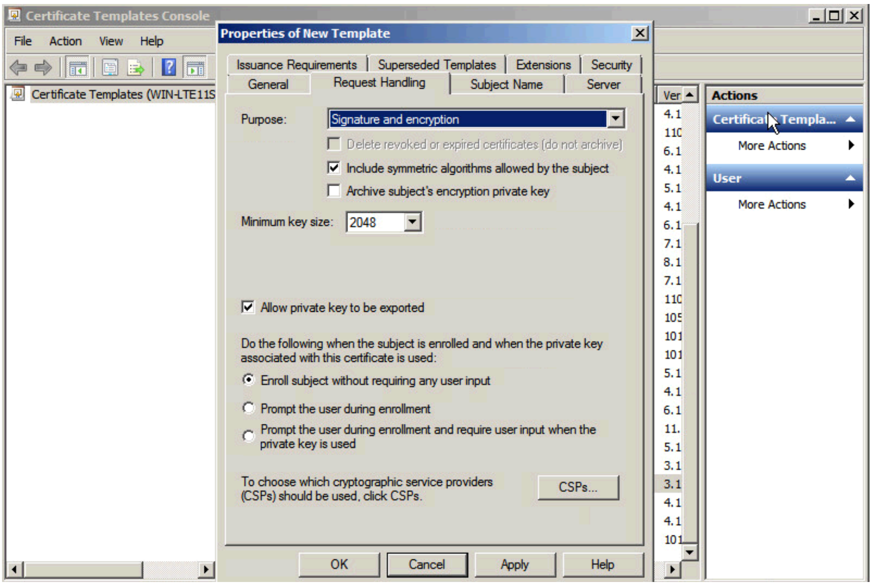
An issuance policy describes the conditions under which a certificate is issued.

Issuance policies:

All issuance policies

□ Make this extension critical

Step 7 Leave the defaults for request handling



Properties of New Template

Issuance Requirements | Superseded Templates | Extensions | Security | General | Request Handling | Subject Name | Server

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

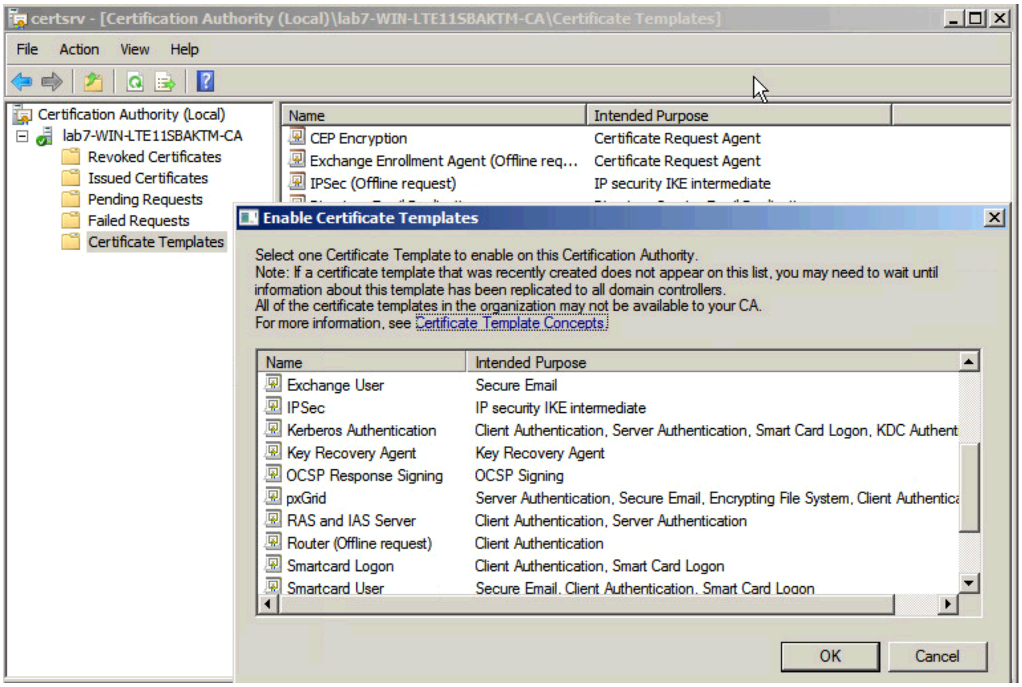
○ Prompt the user during enrollment and require user input when the private key is used

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

OK Cancel Apply Help

Step 8 Right-click on **Certificate Templates**

Step 9 Select **New Template to issue and select pxGrid**



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

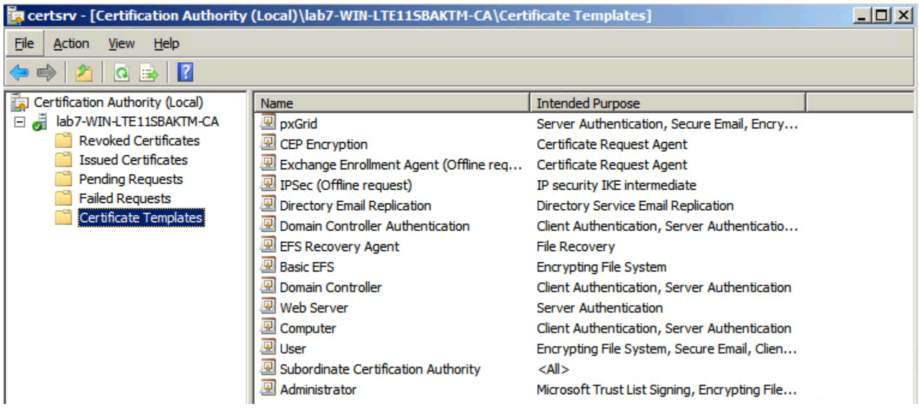
Enable Certificate Templates

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

OK Cancel

Step 10 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 Cisco ISE pxGrid Node

This section details the procedure for configuring the ISE pxGrid node for CA-Signed Certificate operation.

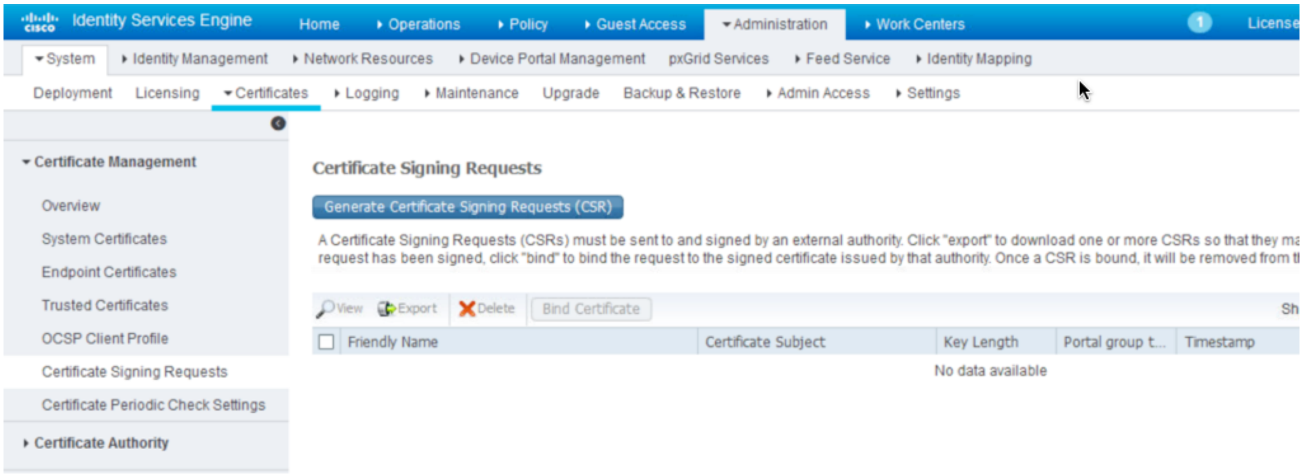
This includes:

- Creating the initial ISE pxGrid node certificate signing request (CSR)
- Generating the certificate from a Microsoft 2008 Enterprise R2 CA server

Note: The pxGrid template is a customized template containing an EKU for both client authentication and server authentication

- Uploading the root CA certificate into the ISE trusted certificate store
- Uploading the ISE pxGrid node certificate into the ISE system certificate store
- Enabling the ISE node for pxGrid operation.

Step 1 Select **Administration->System->Certificates->Certificate Management->Certificate Signing Requests->Generate Certificate Signing Request (CSR)**
You should see the following:



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 ma
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 tl

□ Friendly Name	Certificate Subject	Key Length	Portal group t...	Timestamp

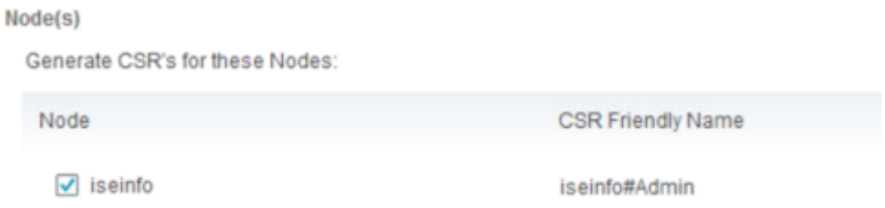
No data available

Step 2 Select **Generate Certificate Signing Requests (CSR)**

Step 3 Under "Usage" Certificate(s) will be used for select **Admin** from the drop-down tab

Note: Admin is selected because Infoblox uses bulk session downloads

Step 4 Select the ise node, (i.e.**iseinfo)**

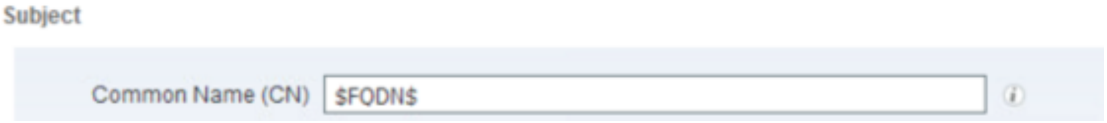


Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☑ iseinfo	iseinfo#Admin

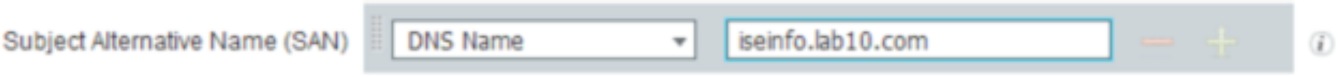
Step 5 Leave the defaults for the FQDN



Subject

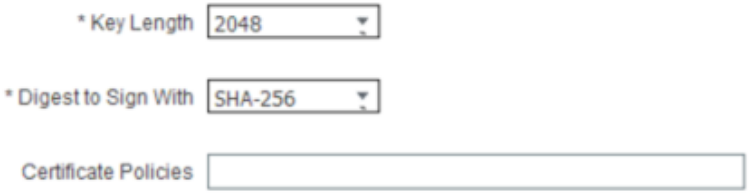
Common Name (CN) $FQDN$

Step 6 Under Subject Alternative Name (SAN), select **DNS name**



Subject Alternative Name (SAN) DNS Name iseinfo.lab10.com

Step 7 Leave the defaults for **Key Length**, **Digests to Sign With** and nothing for Certificate Policies

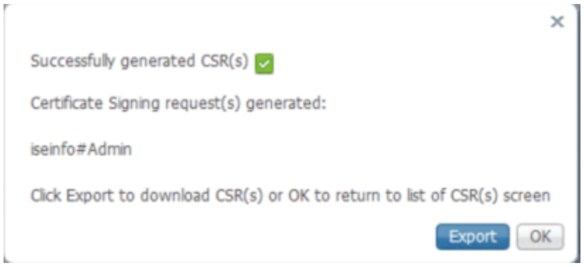


* Key Length 2048

* Digest to Sign With SHA-256

Certificate Policies

Step 8 Select **Generate**



Successfully generated CSR(s) ✓

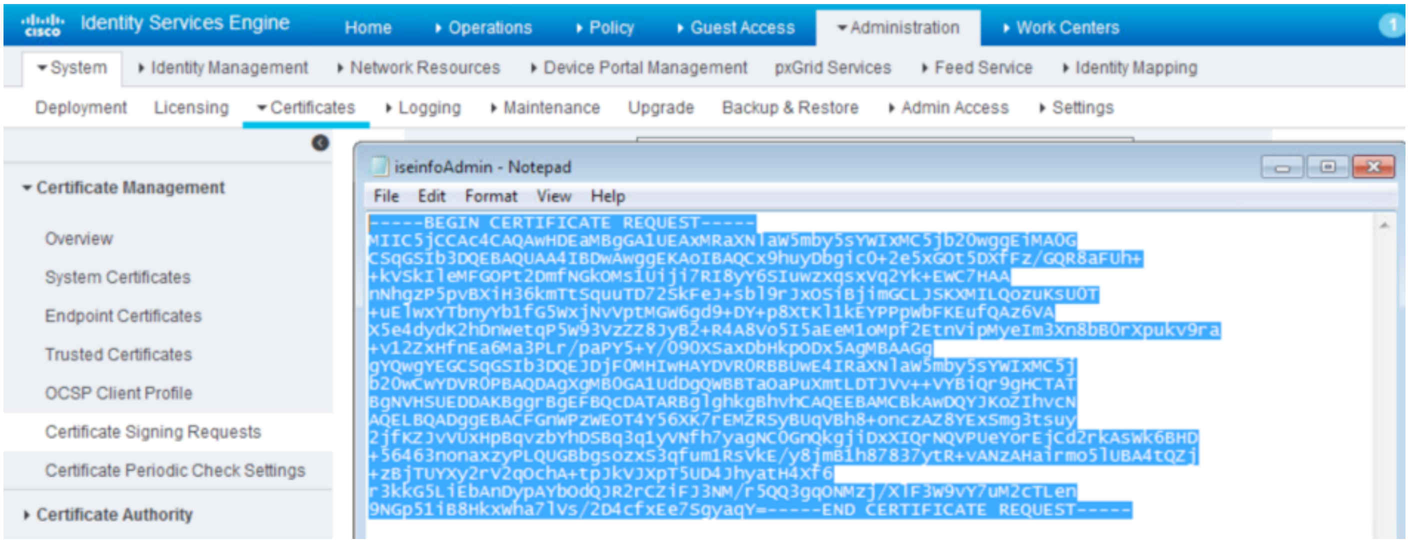
Certificate Signing request(s) generated:

iseinfo#Admin

Click Export to download CSR(s) or OK to return to list of CSR(s) screen

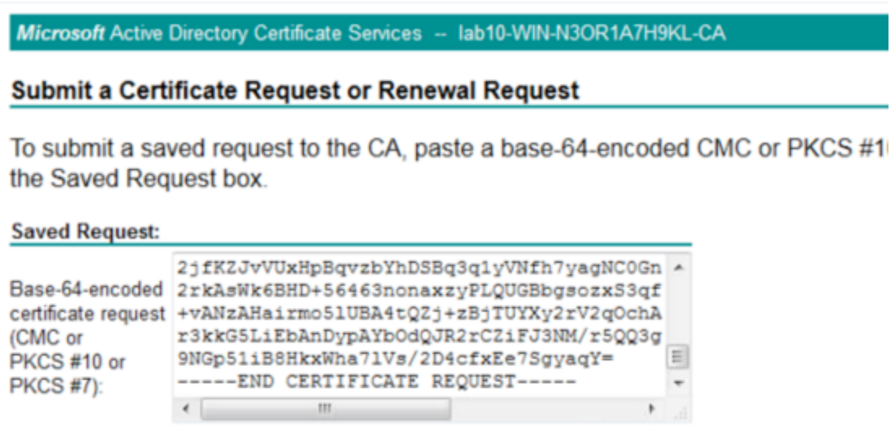
Step 9 Select **Export**

Step 10 Open the certificate using **Notepad,** copy the CSR request



```
-----BEGIN CERTIFICATE REQUEST-----
MIIC5jCCAc4CAQAwHDEaMBgGA1UEAxMRaXNlaW5mby5sYWIxMC5jb20wggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCx9huyDbgic0+2e5xGOt5DXfFz/GQR8aFUh+
+kVSkIleMFGOPt2DmfNGkOMs1Uiji7RI8yY6SIuwzxqsxVq2Yk+EWC7HAA
nNhgzP5pvBXiH36kmTtSquuTD72SkFeJ+sbl9rJxOSiBjimGCLJSKXMILQozuKsUOT
+uElwxYTbnyYb1fG5WxjNvVptMGW6gd9+DY+p8XtKl1kEYPPpWbFKEufQAz6VA
X5e4dydK2hDnwetqP5W93VzZZ8JyB2+R4A8Vo5I5aEeM1oMpf2EtnVipMyeIm3Xn8bB0rXpukv9ra
+v12ZxHfnEa6Ma3PLr/paPY5+Y/090XSaxDbHkpODx5AgMBAAGg
gYQwgYEGCSqGSIb3DQEJDjF0MHIwHAYDVR0RBBUwE4IRaXNlaW5mby5sYWIxMC5j
b20wCwYDVR0PBAQDAgXgMB0GA1UdDgQWBBTaOaPuXmtLDTJVv++VYBiQr9gHCTAT
BgNVHSUEDDAKBggrBgEFBQcDATARBglghkgBhvhCAQEEBAMCBkAwDQYJKoZIhvcN
AQELBQADggEBACFGnWPzWEOT4Y56XK7rEMZRSyBUqVBh8+onczAZ8YExSmg3tsuy
2jfKZJvVUxHpBqvzbYhDSBq3q1yVNfh7yagNC0GnQkgjiDxXIQrNQVPUeYorEjCd2rkAsWk6BHD
+56463nonaxzyPLQUGBbgsozxS3qfum1RsVkE/y8jmB1h87837ytR+vANzAHairmo5lUBA4tQZj
+zBjTUYXy2rV2qOchA+tpJkVJXpT5UD4JhyatH4Xf6
r3kkG5LiEbAnDypAYbOdQJR2rCZiFJ3NM/r5QQ3gqONMzj/XlF3W9vY7uM2cTLen
9NGp51iB8HkxWha71vs/2D4cfxEe7SgyaqY=-----END CERTIFICATE REQUEST-----
```

Step 11 Open MS CA Authority, **Request a certificate->Advanced Certificate Request->paste in Base-64-encoded… Saved Request field**


Microsoft Active Directory Certificate Services -- lab10-WIN-N3OR1A7H9KL-CA

Submit a Certificate Request or Renewal Request

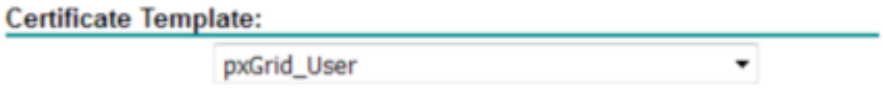
To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #1 the Saved Request box.

Saved Request:

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

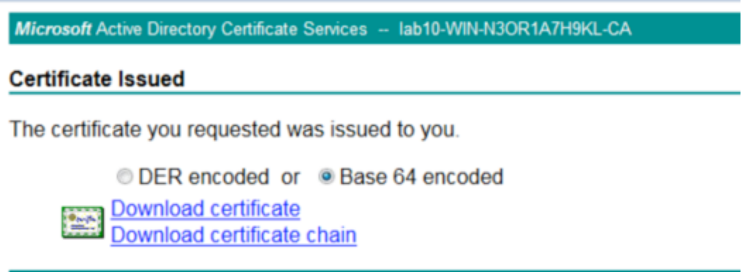
```
2jfKZJvVUxHpBqvzbYhDSBq3q1yVNfh7yagNC0Gn
2rkAsWk6BHD+56463nonaxzyPLQUGBbgsozxS3qf
+vANzAHairmo5lUBA4tQZj+zBjTUYXy2rV2qOchA
r3kkG5LiEbAnDypAYbOdQJR2rCZiFJ3NM/r5QQ3g
9NGp51iB8HkxWha71Vs/2D4cfxEe7SgyaqY=
-----END CERTIFICATE REQUEST-----
```

Step 12 Select customized pxGrid template


Certificate Template: pxGrid_User

Step 13 Select **Submit**

Step 14 Select **Base 64-encoded**



Microsoft Active Directory Certificate Services -- lab10-WIN-N3OR1A7H9KL-CA

Certificate Issued

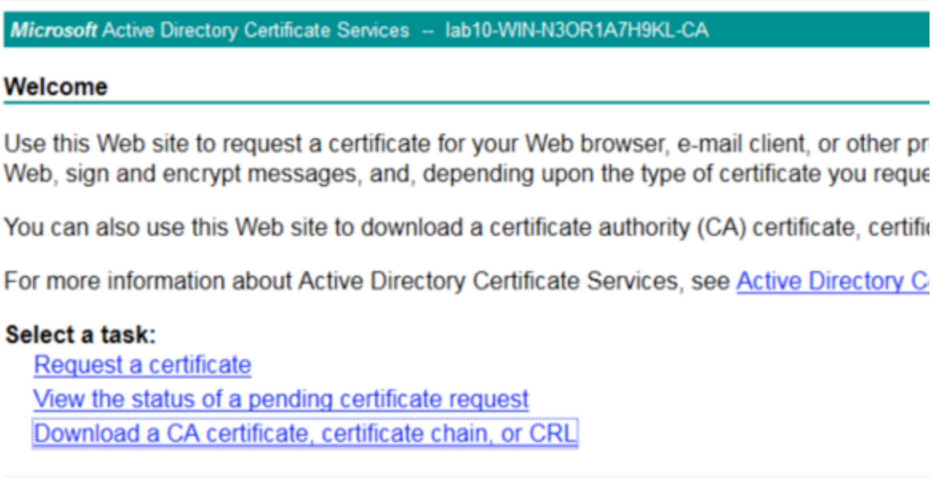
The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Download certificate
Download certificate chain

Step 15 Select **Download certificate**

Step 16 You will also need to download the root certificate



Microsoft Active Directory Certificate Services -- lab10-WIN-N3OR1A7H9KL-CA

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other pr
Web, sign and encrypt messages, and, depending upon the type of certificate you reque

You can also use this Web site to download a certificate authority (CA) certificate, certifi

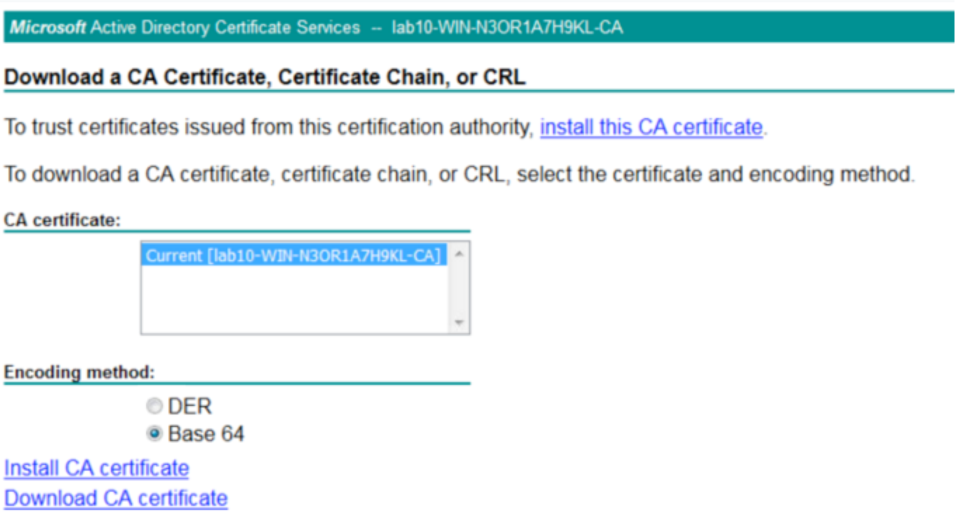
For more information about Active Directory Certificate Services, see Active Directory C

Select a task:

Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

Step 17 Select **Download a CA certificate….** and rename to iseinfo.cer

Step 18 Download in **Base 64** format



Microsoft Active Directory Certificate Services -- lab10-WIN-N3OR1A7H9KL-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 [lab10-WIN-N3OR1A7H9KL-CA]

Encoding method:

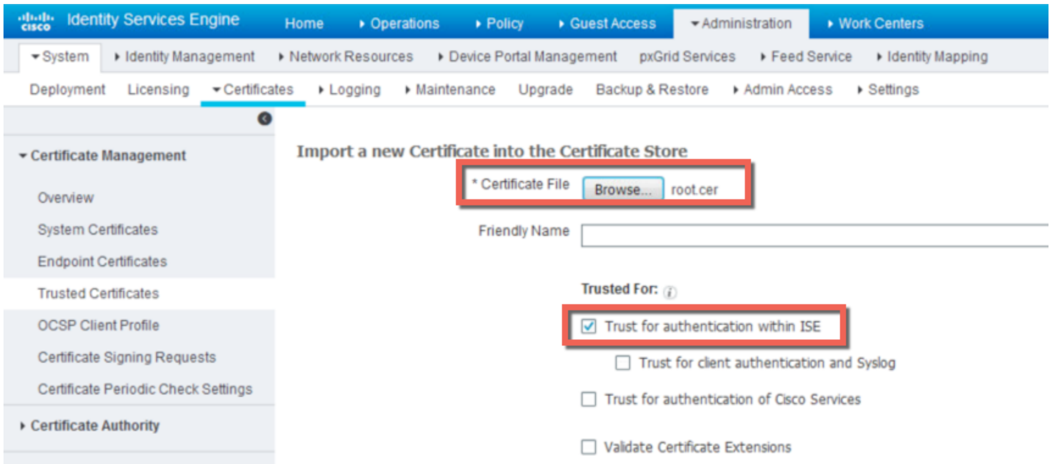
○ DER
● Base 64

Install CA certificate
Download CA certificate

Step 19 Select **Download CA certificate** and rename to root.cer

Step 20 Upload trusted CA root certificate (root.cer) into ISE
Select->**Administration->System->Certificates->Trusted Certificates->Import and upload the root.cer**

Step 21 **Enable** Trust for Authentication within ISE



Import a new Certificate into the Certificate Store

* Certificate File root.cer

Friendly Name

Trusted For:

☑ Trust for authentication within ISE

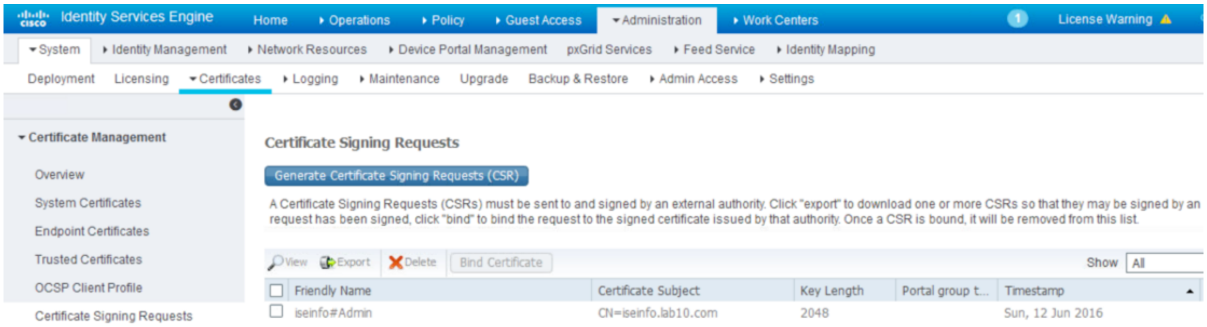
□ Trust for client authentication and Syslog

□ Trust for authentication of Cisco Services

□ Validate Certificate Extensions

Step 22 Select **Submit**

Step 23 Select **Administration->System->Certificates->Certificate Signing Requests (CSR)**
You will see the following:

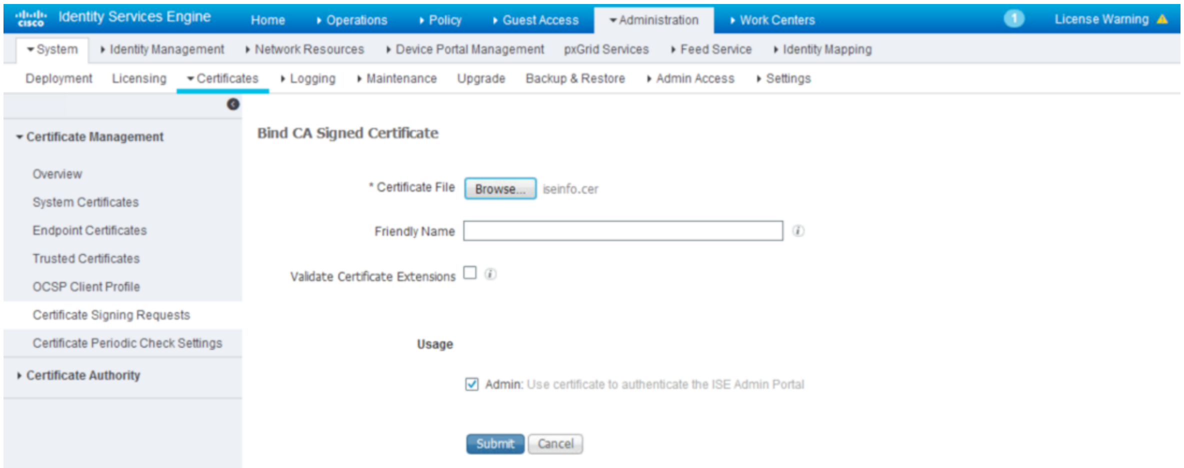


Certificate Signing Requests

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 may be signed by an 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 this list.

□	Friendly Name	Certificate Subject	Key Length	Portal group t...	Timestamp
□	iseinfo#Admin	CN=iseinfo.lab10.com	2048		Sun, 12 Jun 2016

Step 24 Select the **iseinfo#Admin node** and **Bind Certificate** and upload the ISE pxGrid node certificate



Bind CA Signed Certificate

* Certificate File iseinfo.cer

Friendly Name

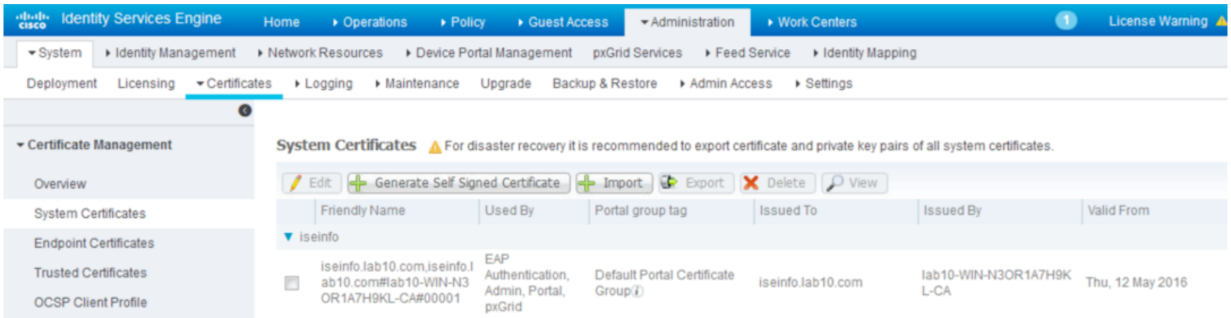
Validate Certificate Extensions □

Usage

☑ Admin: Use certificate to authenticate the ISE Admin Portal

Step 25 Select **Submit**

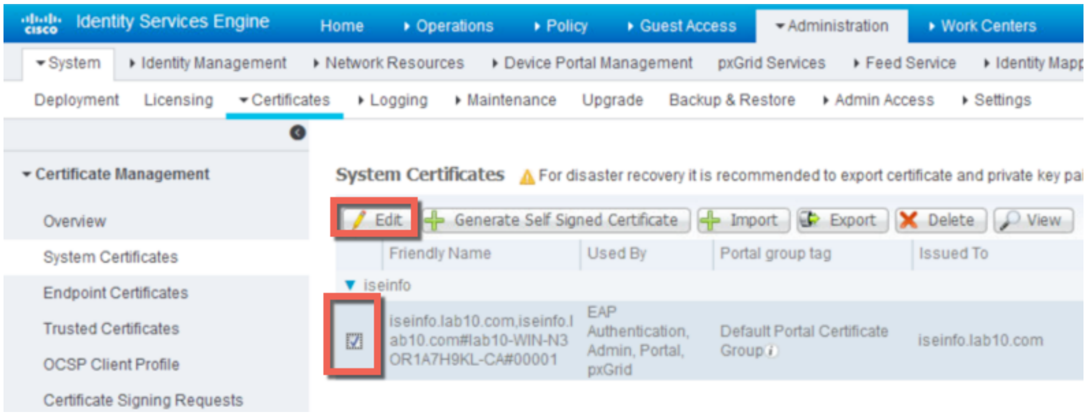
Step 26 Also check to make sure the certificate has pxGrid enabled
Administration->System->Certificates->System Certificates



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	Valid From
▼ iseinfo						
□	iseinfo.lab10.com,iseinfo.lab10.com#lab10-WIN-N3OR1A7H9KL-CA#00001	EAP Authentication, Admin, Portal, pxGrid	Default Portal Certificate Group	iseinfo.lab10.com	lab10-WIN-N3OR1A7H9KL-CA	Thu, 12 May 2016

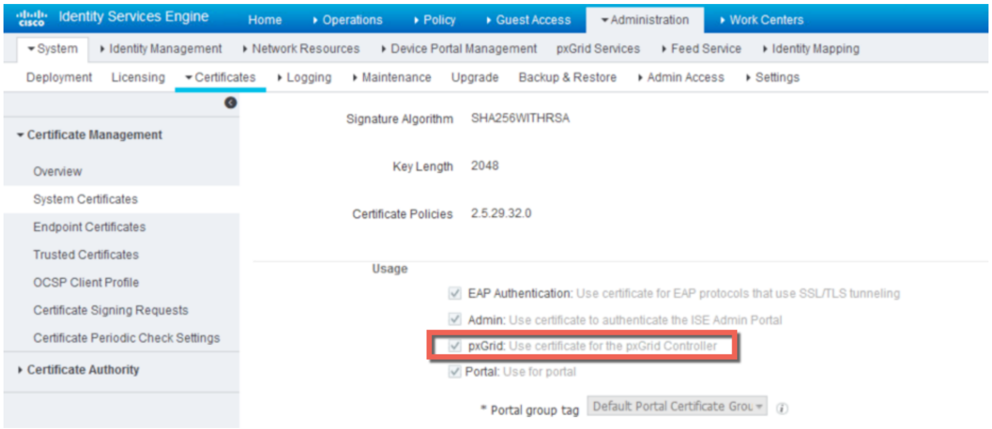
Step 27 If not, you can **select** the certificate and **Edit**



System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pa

	Friendly Name	Used By	Portal group tag	Issued To
▼ iseinfo				
☑	iseinfo.lab10.com,iseinfo.lab10.com#lab10-WIN-N3OR1A7H9KL-CA#00001	EAP Authentication, Admin, Portal, pxGrid	Default Portal Certificate Group	iseinfo.lab10.com

Step 28 **Enable** pxGrid



Signature Algorithm SHA256WITHRSA

Key Length 2048

Certificate Policies 2.5.29.32.0

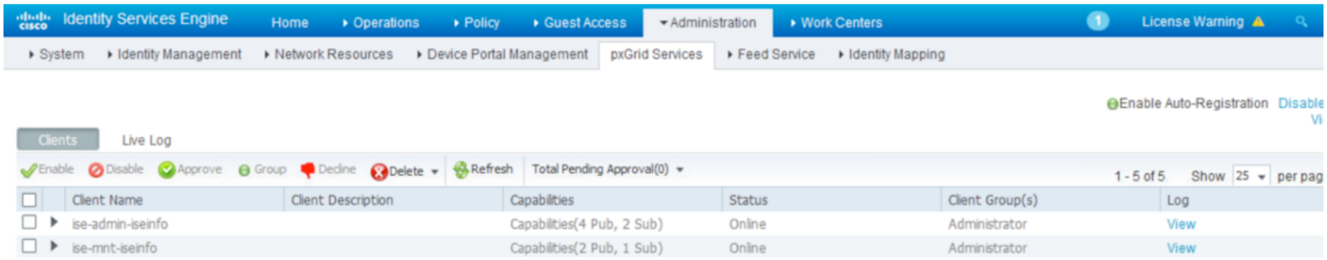
Usage

☑ EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
☑ Admin: Use certificate to authenticate the ISE Admin Portal
☑ pxGrid: Use certificate for the pxGrid Controller
☑ Portal: Use for portal

* Portal group tag Default Portal Certificate Grou

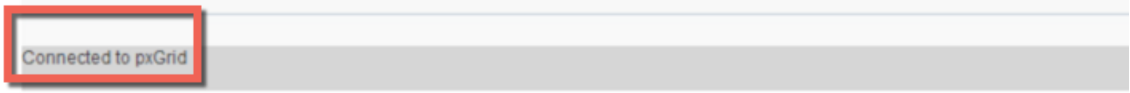
Step 29 Select **Save**

Step 30 Select **Administration->pxGrid Services**
You should see the ISE published nodes



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

Step 31 Verify that there is connectivity


Connected to pxGrid

Configuring Infoblox Grid Master (GM)

This section steps through the procedure for configuring the Infoblox GM for CA-Signed Certificate operation.

This includes:

- Generating a private key and CSR request for the Infoblox GM
- Generating the certificate from a Microsoft 2008 Enterprise R2 CA server

Note: The pxGrid template is a customized template containing an EKU for both client authentication and server authentication

- Uploading the root CA certificate into the Infoblox trusted store
- Configuring ISE ecosystem parameter settings with the Infoblox concatenated certificate, the ISE bulk download certificate and the ISE pxGrid node IP address

Note: The public-private key pair will be concatenated. The ISE bulk download certificate will be the CA root file, since the same CA server signed both the ISE pxGrid node and the Infoblox Grid Master certificate.

- Uploading the root CA certificate into the ISE trusted certificate store
-

Generating a public-private key pair certs for Infoblox

The private key pair and CSR request were created on a MAC with Oracle JDK installed. Once the CSR request was signed by the CA server using the customized pxGrid template, the Infoblox public certificate and private key were concatenated to a PEM file and uploaded to the Infoblox GM.

Step 1 Type the following to generate the private key

```
openssl genrsa -out info.key 4096
```

Step 2 Type the following to generate the CSR request

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

Step 3 Get CSR request signed by pxGrid template and download in base 64 encoded format

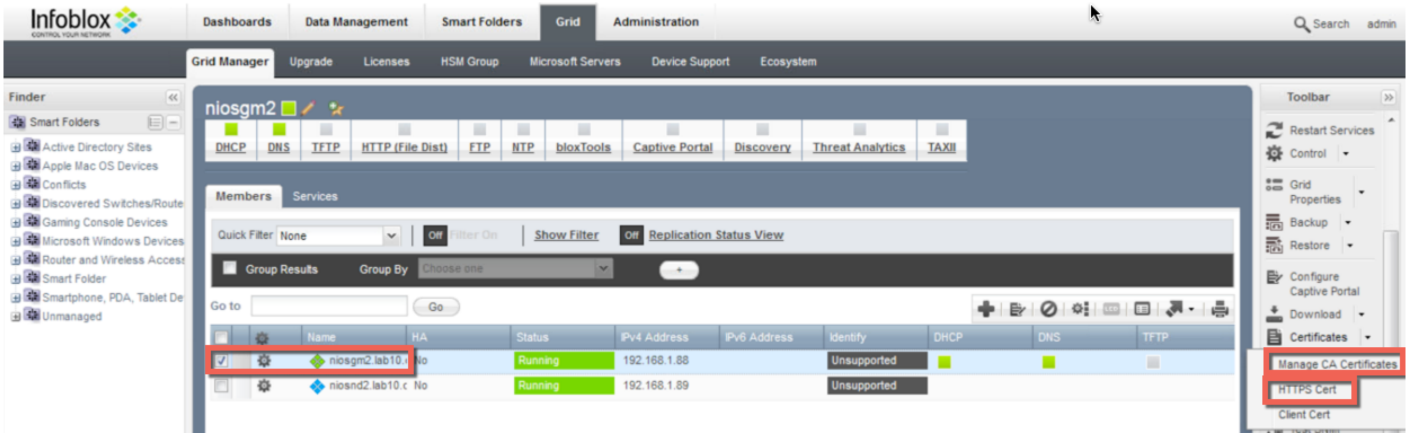
Step 4 You will need to concatenate the private key and public cert into one file. Since base 64 encoded is in PEM format you can simply use cat Linux function

```
cat info.cer info.key > infoblox.pem
```

Configuring ISE Ecosystem settings

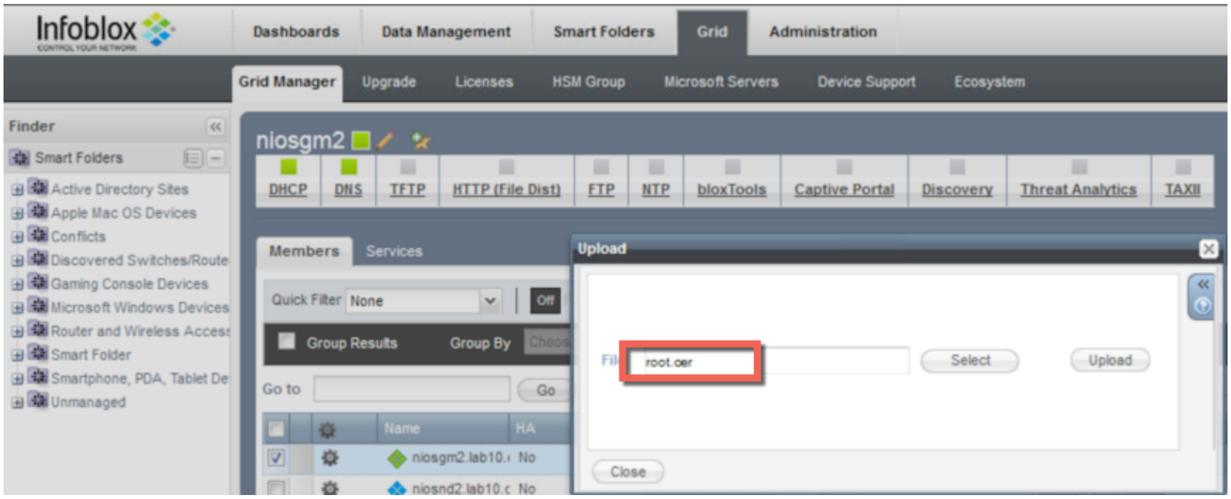
This section configures the Infoblox GM ISE Ecosystem settings used for connecting and registering with the ISE pxGrid node.

Step 1 Upload the CA root certificate into the Infoblox Grid Master
Select **Grid->Grid Manager->Members->Grid Master->Certificates->Manage CA Certificates**



☐	Name	HA	Status	IPv4 Address	IPv6 Address	Identify	DHCP	DNS	TFTP
☑	niosgm2.lab10.c	No	Running	192.168.1.88		Unsupported	🟩	🟩	☐
☐	niosnd2.lab10.c	No	Running	192.168.1.89		Unsupported			

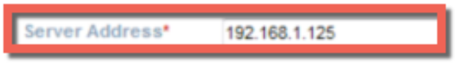
Step 2 Select **"+" Add,** and **upload** the CA root certificate, then **Close**



File root.cer

Step 3 Select **Grid->Ecosystem->+-> add the ISE pxGrid node->General**

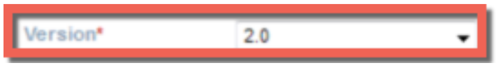
Step 4 Enter the **IP address** of the ISE pxGrid node



Server Address* 192.168.1.125

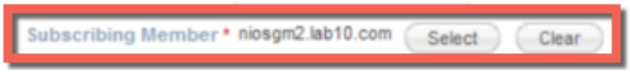
Step 5 Select the **ISE version number**

Note: This will work for ISE 2.0 and ISE 2.1



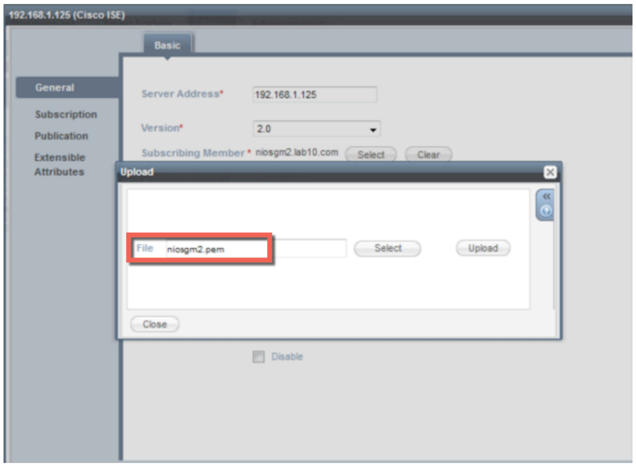
Version* 2.0

Step 6 Select the **Infoblox subscribing member** which is the Infoblox GM



Subscribing Member * niosgm2.lab10.com

Step 7 Upload the Infoblox concatenated PEM file for **Client Certificate**



Server Address* 192.168.1.125

Version* 2.0

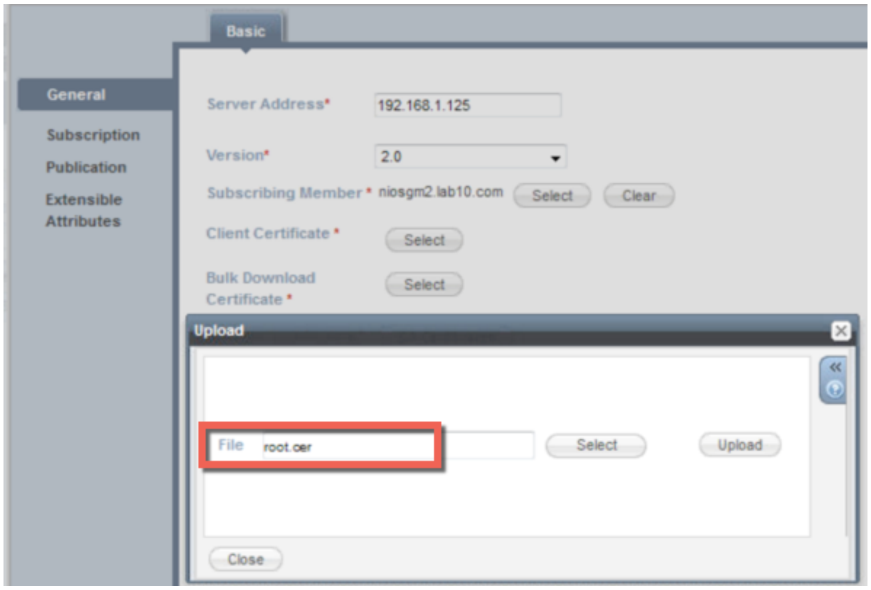
Subscribing Member * niosgm2.lab10.com

File niosgm2.pem

□ Disable

Step 8 Upload the CA-root certificate for the **Bulk Download Certificate**

Note: You will need to export the CA-signed identity cert (here is where the admin purpose cert comes in) and import this cert for the Bulk Download cert



Server Address* 192.168.1.125

Version* 2.0

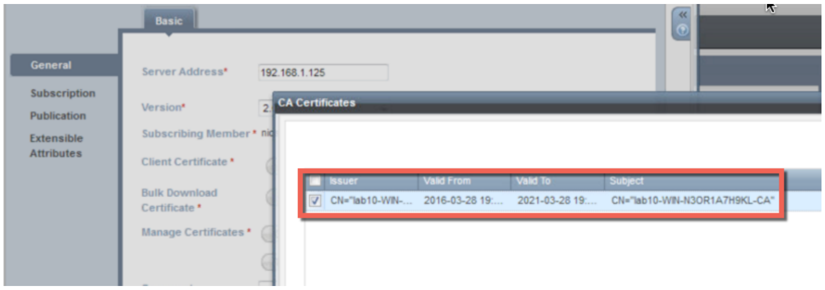
Subscribing Member* niosgm2.lab10.com

Client Certificate*

Bulk Download Certificate*

File root.cer

Step 9 Select the CA-root certificate for **Manage Certificates**



Server Address* 192.168.1.125

Version* 2

Subscribing Member* nio

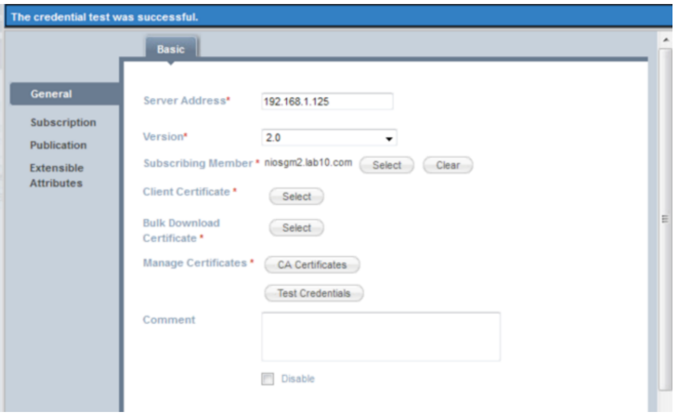
Client Certificate*

Bulk Download Certificate*

Manage Certificates*

	Issuer	Valid From	Valid To	Subject
☑	CN="lab10-WIN-...	2016-03-28 19:...	2021-03-28 19:...	CN="lab10-WIN-N3OR1A7H9KL-CA"

Step 10 Select **Test Credentials**, you should see the message "The credential test was successful.



The credential test was successful.

Server Address* 192.168.1.125

Version* 2.0

Subscribing Member* niosgm2.lab10.com

Client Certificate*

Bulk Download Certificate*

Manage Certificates*

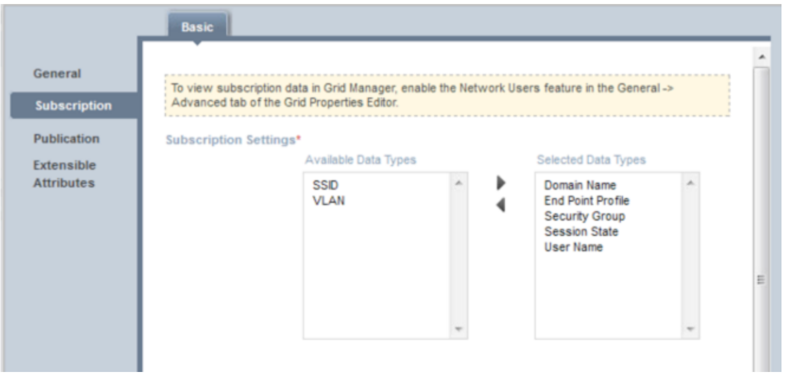
Comment

□ Disable

Step 11 Select -> **Next**

Step 12 Move the following **Available Data Types** into the **Selected Data Types**

Note: The selected data type information is the ISE session information that will be retrieved from ISE. This session attribute information will be populated in the IPAM table and provide additional contextual information around the IP Address. Also note, the SSID and VLAN values are not available as attributes in pxGrid



To view subscription data in Grid Manager, enable the Network Users feature in the General -> Advanced tab of the Grid Properties Editor.

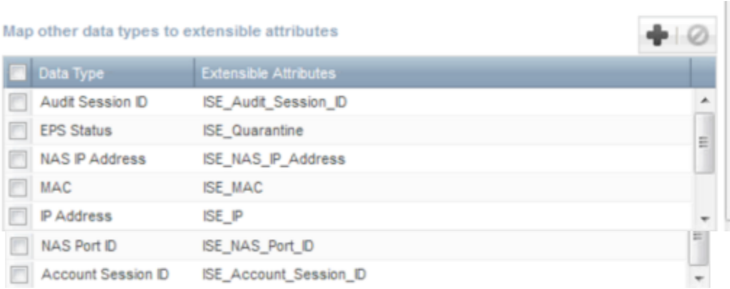
Subscription Settings*

Available Data Types: SSID, VLAN

Selected Data Types: Domain Name, End Point Profile, Security Group, Session State, User Name

Step 13 Add the following Data Types and associated Extensible Attributes below:

Note: You need to define the ISE extensible attributes first.



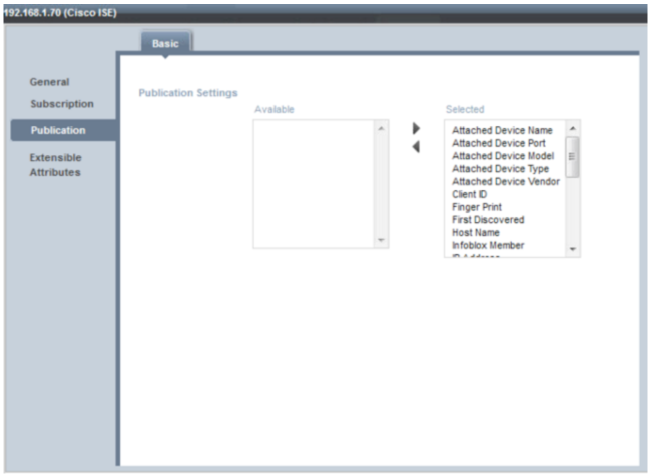
Map other data types to extensible attributes

☐ Data Type	Extensible Attributes
☐ Audit Session ID	ISE_Audit_Session_ID
☐ EPS Status	ISE_Quarantine
☐ NAS IP Address	ISE_NAS_IP_Address
☐ MAC	ISE_MAC
☐ IP Address	ISE_IP
☐ NAS Port ID	ISE_NAS_Port_ID
☐ Account Session ID	ISE_Account_Session_ID

Step 14 Select -> **Next**

Step 15 Select -> **Publication**

Step 16 Move all the available attributes into the Selected Column



Publication Settings

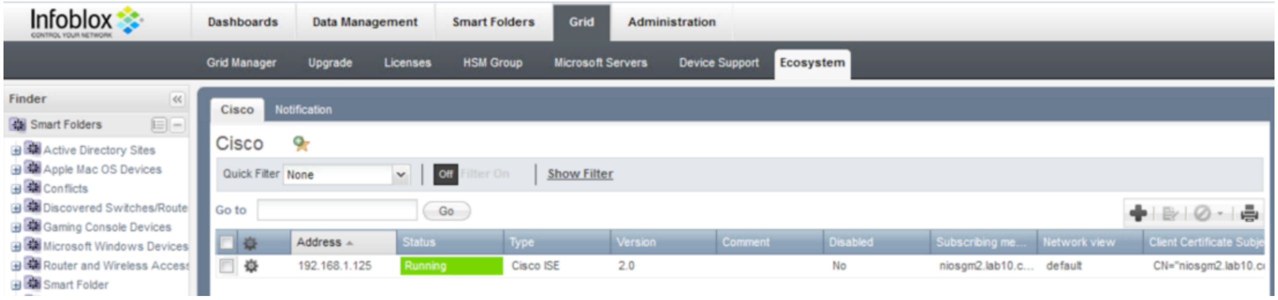
Available

Selected: Attached Device Name, Attached Device Port, Attached Device Model, Attached Device Type, Attached Device Vendor, Client ID, Finger Print, First Discovered, Host Name, Infoblox Member

Step 17 Select **Next**

Step 18 Select **Extensible Attributes**, leave the defaults which are empty, then **Save and Close**

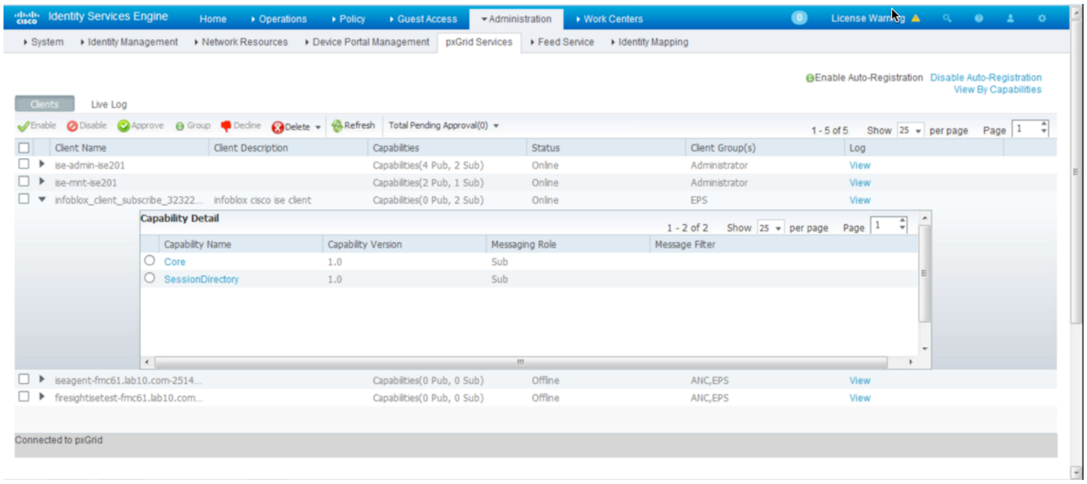
You should see a **running** status connection.



Address	Status	Type	Version	Comment	Disabled	Subscribing me...	Network view	Client Certificate Subje
192.168.1.125	Running	Cisco ISE	2.0		No	niosgm2.lab10.c...	default	CN="niosgm2.lab10.c

Step 19 You can also verify in ISE

Select **Administration->pxGrid Services**



Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
ise-admin-ise201		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
ise-mnt-ise201		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
infoblox_client_subscribe_32322...	infoblox cisco ise client	Capabilities(0 Pub, 2 Sub)	Online	EPS	View
iseagent-fmc61.lab10.com-2514...		Capabilities(0 Pub, 0 Sub)	Offline	ANC,EPS	View
firesightisetest-fmc61.lab10.com...		Capabilities(0 Pub, 0 Sub)	Offline	ANC,EPS	View

Capability Detail

Capability Name	Capability Version	Messaging Role	Message Filter
Core	1.0	Sub	
SessionDirectory	1.0	Sub	

Connected to pxGrid

Configuring for Self-Signed Certificate Operation

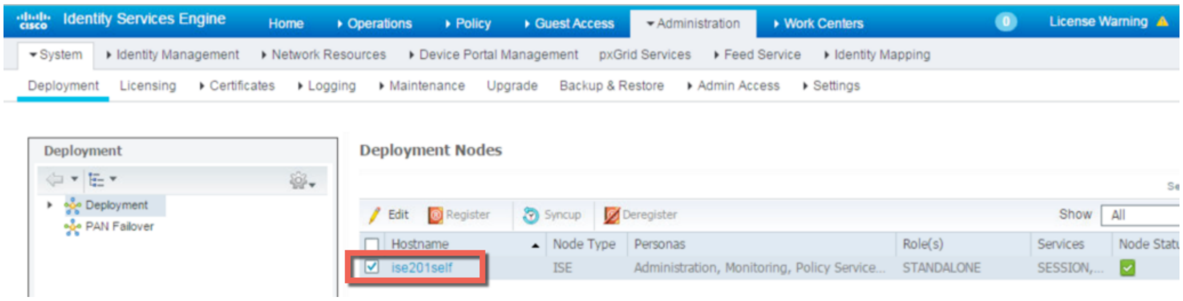
This section steps through self-signed operation for both Infoblox Grid Master (GM) the ISE pxGrid node. Please note that ISE is deployed in a Stand-alone configuration and self-signed certificates are for POC environments only.

Configuring Cisco ISE pxGrid Node

This section details the procedure for configuring the ISE pxGrid node for self signed certificates for ISE 2.1

Note: For ISE 1.3 and ISE 1.4, the ISE self-signed certificate needs to be imported into the ISE trusted certificate store.

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

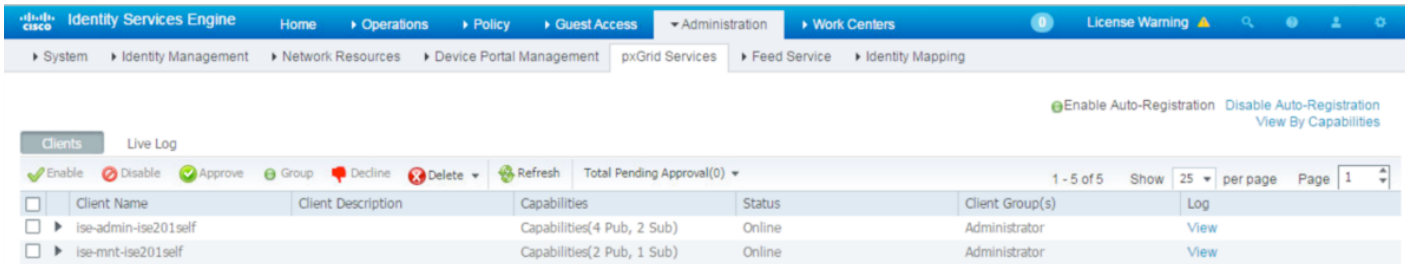


☐	Hostname	Node Type	Personas	Role(s)	Services	Node Statu
☑	ise201self	ISE	Administration, Monitoring, Policy Service...	STANDALONE	SESSION,...	✓

Step 2 Enable **pxGrid**

Step 3 Select **Save**

Step 4 Select **Administration->pxGrid Services** to view the ISE published nodes



☐	Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
☐	ise-admin-ise201self		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
☐	ise-mnt-ise201self		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View

Configuring Infoblox Grid Master

This section steps through the procedure for configuring the Infoblox GM for self signed certificates for ISE 2.1.

Generating a public-private key pair cert, CSR Request and self-signed certificate for Infoblox

The private key pair and CSR request were created on a MAC with Oracle JDK installed. Once the certificate is generated, the Infoblox public certificate and private key were concatenated to a PEM file and uploaded to the Infoblox GM.

Step 1 Type the following to generate the private key

```
openssl genrsa -out infoself.key 4096
```

Step 2 Type the following to generate the CSR request

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

Step 3 Generate the self-signed certificate

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

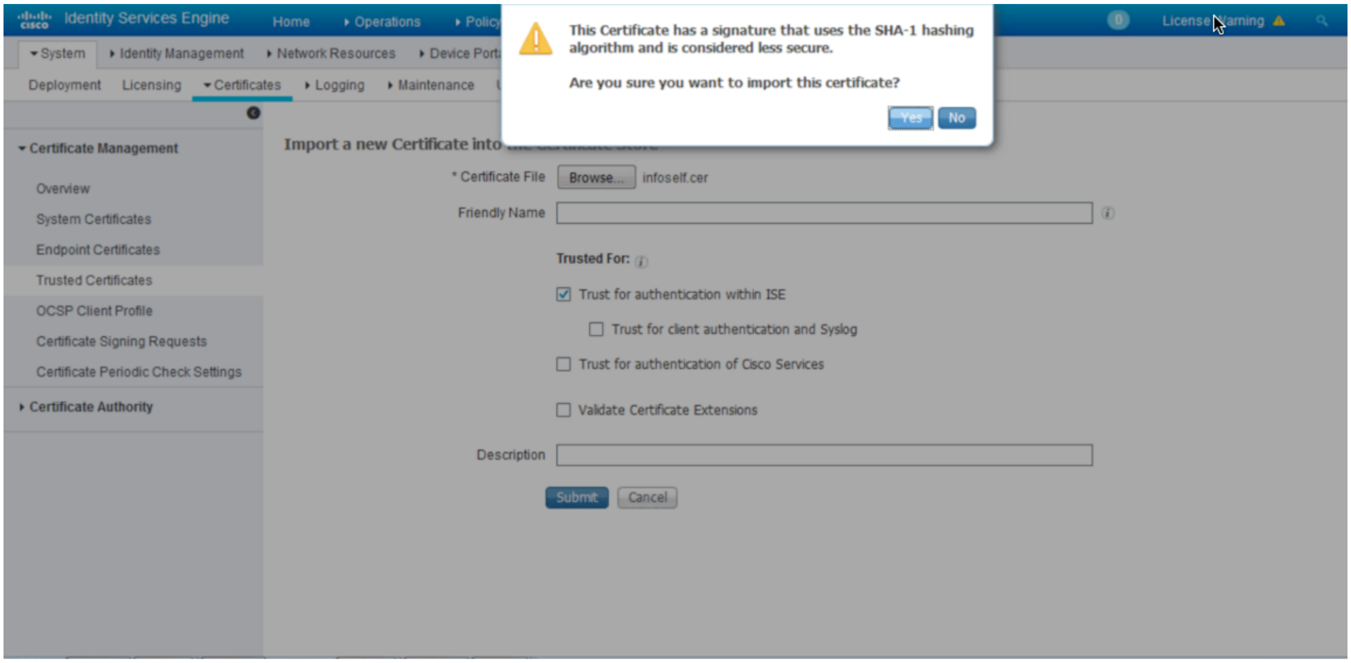
Step 4 You will need to concatenate the private ley and public cert into one file. Since base 64 encoded is in PEM format you can simply use cat Linux function

```
cat infoself.cer infoself.key > infoself.pem
```

Importing Infoblox certificate into ISE trusted system store

Step 1 Import the Infoblox identity self-signed certificate into the ISE trusted system certificate store
Select **Administration->System->Certificates->Trusted Certificates->Import the infoself.pem file->Submit-Yes**

Note: Ensure Trust for authentication with ISE is enabled



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?

Yes No

Import a new Certificate into

* Certificate File Browse... infoself.cer

Friendly Name

Trusted For:

☑ Trust for authentication within ISE

☐ Trust for client authentication and Syslog

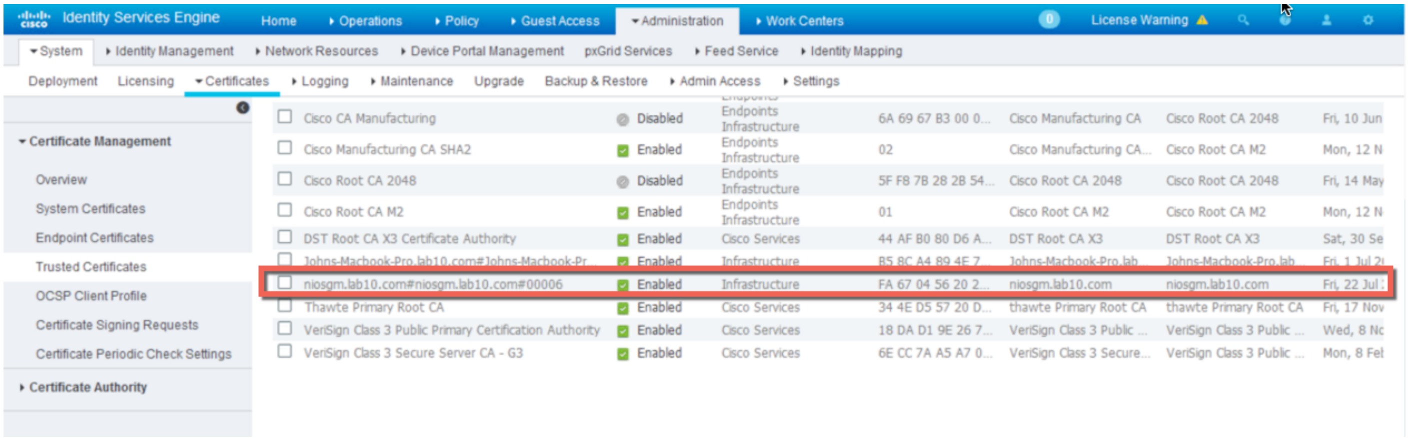
☐ Trust for authentication of Cisco Services

☐ Validate Certificate Extensions

Description

Submit Cancel

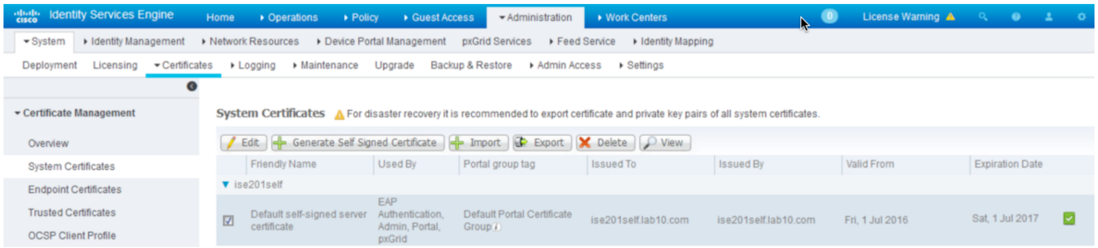
Step 2 You should see the certificate under the ISE trusted certificate store



☐	Cisco CA Manufacturing	Disabled	Endpoints Infrastructure	6A 69 67 B3 00 0...	Cisco Manufacturing CA	Cisco Root CA 2048	Fri, 10 Jun
☐	Cisco Manufacturing CA SHA2	✓ Enabled	Endpoints Infrastructure	02	Cisco Manufacturing CA...	Cisco Root CA M2	Mon, 12 N
☐	Cisco Root CA 2048	Disabled	Endpoints Infrastructure	5F F8 7B 28 2B 54...	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May
☐	Cisco Root CA M2	✓ Enabled	Endpoints Infrastructure	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 N
☐	DST Root CA X3 Certificate Authority	✓ Enabled	Cisco Services	44 AF B0 80 D6 A...	DST Root CA X3	DST Root CA X3	Sat, 30 Se
☐	Johns-Macbook-Pro.lab10.com#Johns-Macbook-Pr...	✓ Enabled	Infrastructure	B5 8C A4 89 4E 7...	Johns-Macbook-Pro.lab...	Johns-Macbook-Pro.lab...	Fri, 1 Jul 2
☐	niosgm.lab10.com#niosgm.lab10.com#00006	✓ Enabled	Infrastructure	FA 67 04 56 20 2...	niosgm.lab10.com	niosgm.lab10.com	Fri, 22 Jul
☐	Thawte Primary Root CA	✓ Enabled	Cisco Services	34 4E D5 57 20 D...	thawte Primary Root CA	thawte Primary Root CA	Fri, 17 Nov
☐	VeriSign Class 3 Public Primary Certification Authority	✓ Enabled	Cisco Services	18 DA D1 9E 26 7...	VeriSign Class 3 Public ...	VeriSign Class 3 Public ...	Wed, 8 Nc
☐	VeriSign Class 3 Secure Server CA - G3	✓ Enabled	Cisco Services	6E CC 7A A5 A7 0...	VeriSign Class 3 Secure...	VeriSign Class 3 Public ...	Mon, 8 Fel

Import ISE self-signed certificate into Infoblox trusted system store

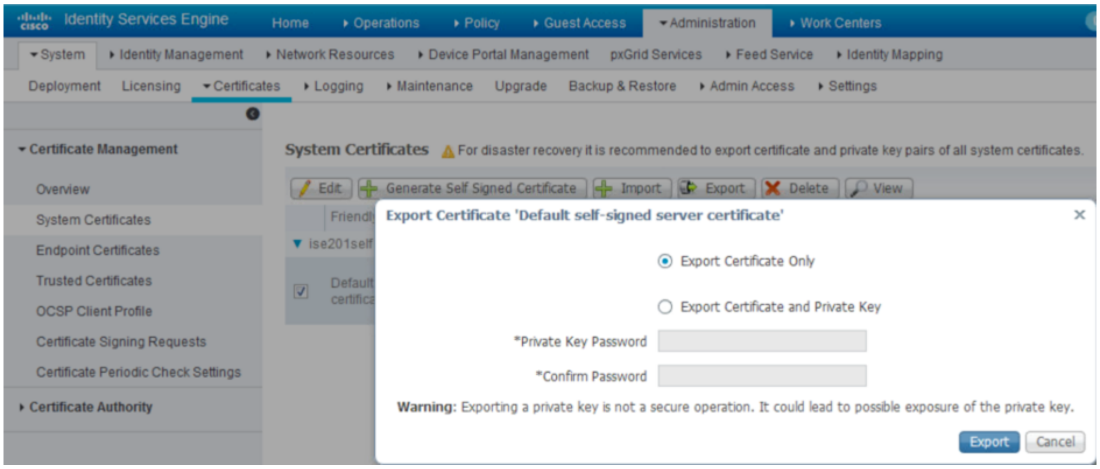
Step 1 Import the ISE self-signed certificate into the Infoblox GM Trusted Certificate Store
Select **Administration->System->Certificates->System Certificates->and select the ISE self-signed certificate**



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	Valid From	Expiration Date	
▼ ise201self								
☑	Default self-signed server certificate	EAP Authentication, Admin, Portal, pxGrid	Default Portal Certificate Group	ise201self.lab10.com	ise201self.lab10.com	Fri, 1 Jul 2016	Sat, 1 Jul 2017	✓

Step 2 Select **Export** and **Export Certificate Only** to export the public key of Cisco ISE



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

Export Certificate 'Default self-signed server certificate'

● Export Certificate Only

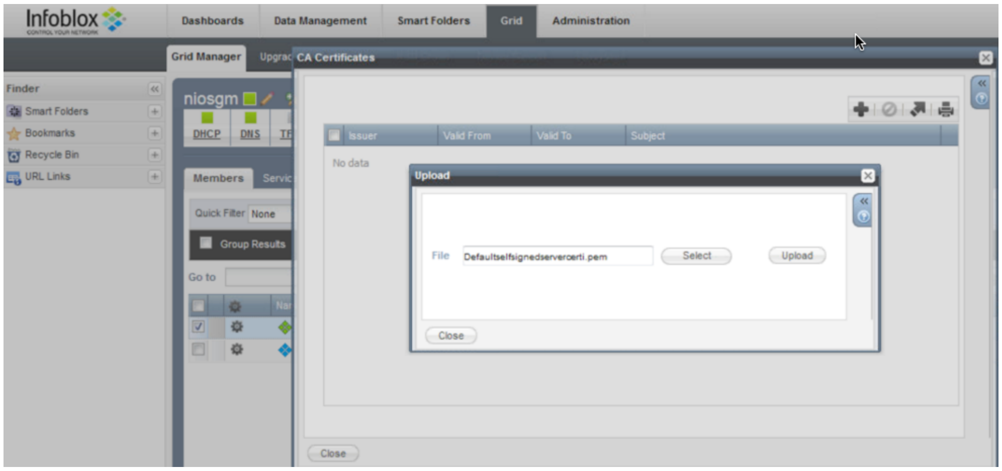
○ Export Certificate and Private Key

*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.

Step 3 Select the **Export** button and save the Defaultsignedservercerti.pem file.
Step 4 Upload the ISE self-signed certificate into the Infoblox trust store
Select **Grid->Grid Manager->Members->Grid Master->Certificates->Manage CA Certificates->** "+" **->Select** the ISE self-signed certificate



CA Certificates

Issuer	Valid From	Valid To	Subject

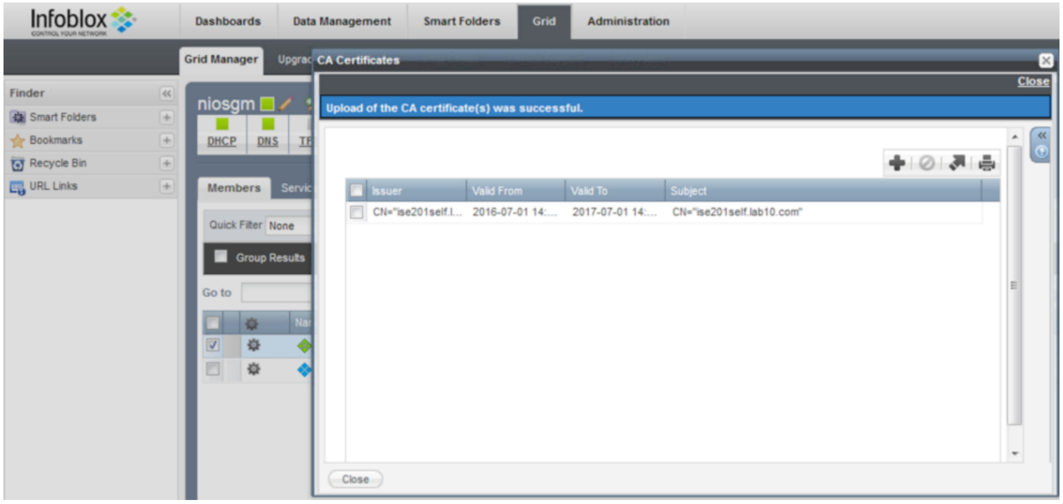
No data

Upload

File Defaultselfsignedservercerti.pem

Step 5 Select **Upload**

Step 6 You should see that the upload was successful



CA Certificates

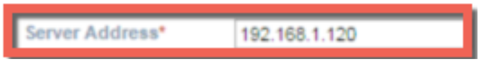
Upload of the CA certificate(s) was successful.

Issuer	Valid From	Valid To	Subject
CN="ise201self.l...	2016-07-01 14:...	2017-07-01 14:...	CN="ise201self.lab10.com"

Step 7 Select **Close**

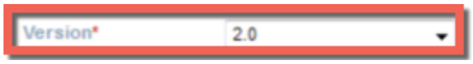
Step 8 Select **Grid->Ecosystem->+-> add the ISE pxGrid node->General**

Step 9 Enter the **IP address** of the ISE pxGrid node



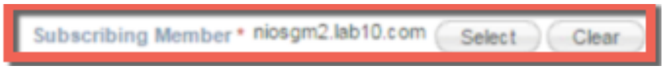
Server Address* 192.168.1.120

Step 10 Select the **ISE version number**



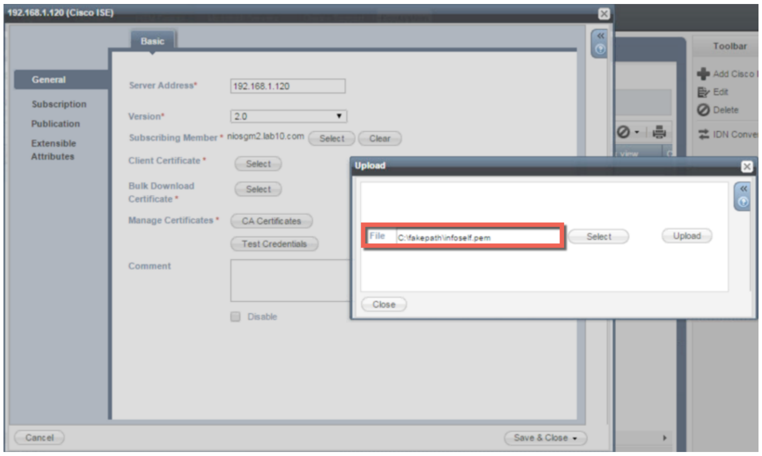
Version* 2.0

Step 11 Select the **Infoblox subscribing member** which is the Infoblox Grid Master



Subscribing Member * niosgm2.lab10.com

Step 12 Upload the Infoblox concatenated PEM file for **Client Certificate**



192.168.1.120 (Cisco ISE)

Server Address* 192.168.1.120

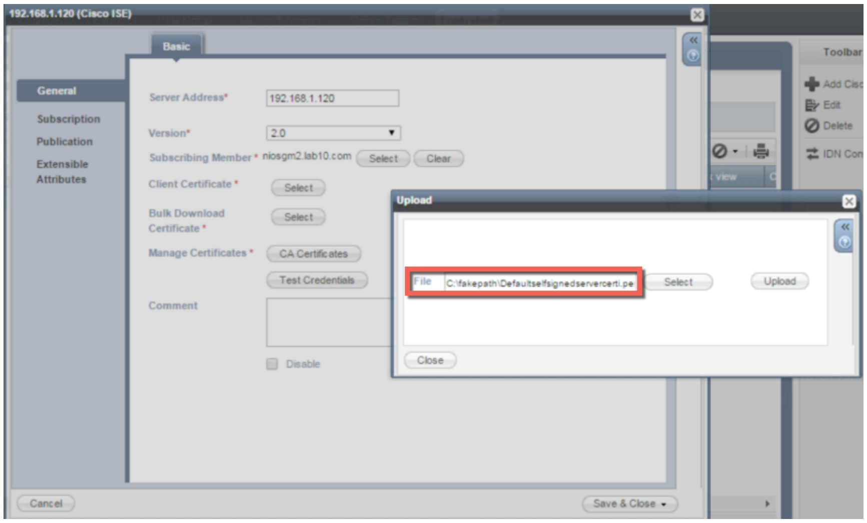
Version* 2.0

Subscribing Member * niosgm2.lab10.com

Upload

File C:\fakepath\infoself.pem

Step 13 Upload the exported ISE certificate for the **Bulk Download Certificate**



192.168.1.120 (Cisco ISE)

Server Address* 192.168.1.120

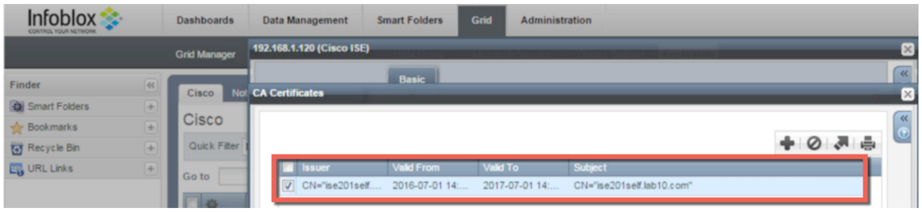
Version* 2.0

Subscribing Member* niosgm2.lab10.com

Upload

File C:\fakepath\Defaultselfsignedservercerti.pe

Step 14 Select the exported ISE certificate for **Manage Certificates CA Certificates**

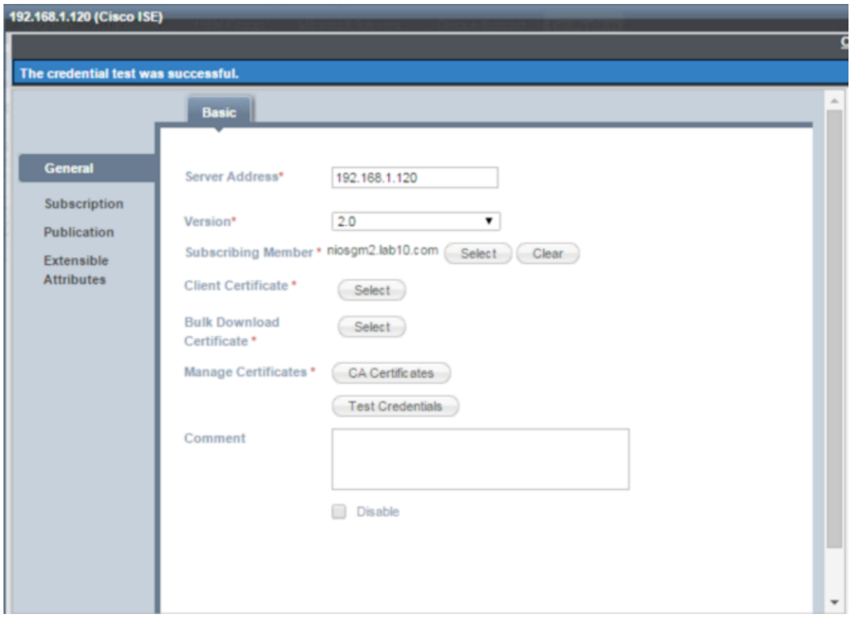


192.168.1.120 (Cisco ISE)

CA Certificates

☐	Issuer	Valid From	Valid To	Subject
☑	CN="ise201self....	2016-07-01 14:...	2017-07-01 14:...	CN="ise201self.lab10.com"

Step 15 Select **Test Credentials**, you should see the message "The credential test was successful.



192.168.1.120 (Cisco ISE)

The credential test was successful.

Server Address* 192.168.1.120

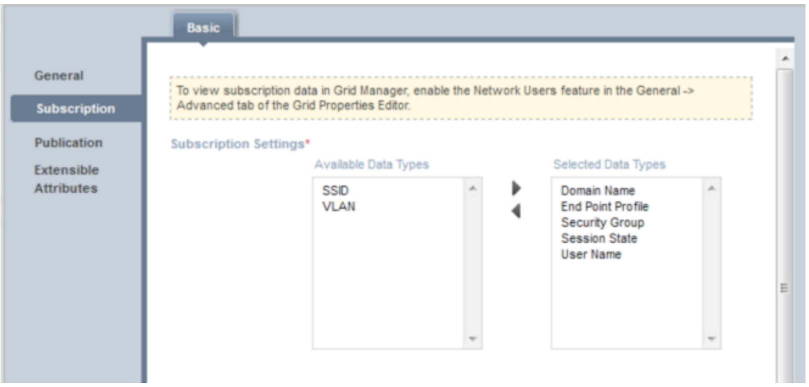
Version* 2.0

Subscribing Member* niosgm2.lab10.com

Step 16 Select Next

Step 17 Move the following **Available Data Types** into the **Selected Data Types**

Note: The selected data type information is the ISE session information that will be retrieved from ISE. This session attribute information will be populated in the IPAM table and provide additional contextual information around the IP Address. Also note, the SSID and VLAN values are not available as attributes in pxGrid



To view subscription data in Grid Manager, enable the Network Users feature in the General -> Advanced tab of the Grid Properties Editor.

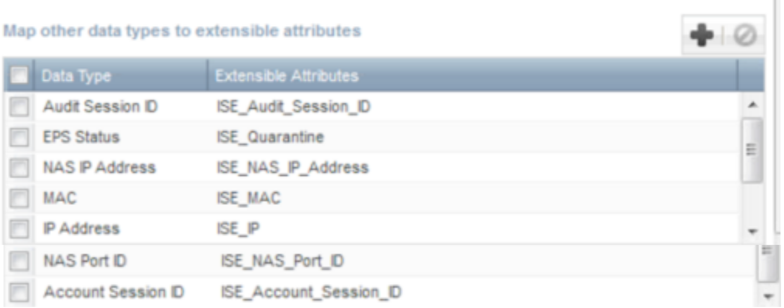
Subscription Settings*

Available Data Types: SSID, VLAN

Selected Data Types: Domain Name, End Point Profile, Security Group, Session State, User Name

Step 18 Add the following Data Types and associated Extensible attributes below:

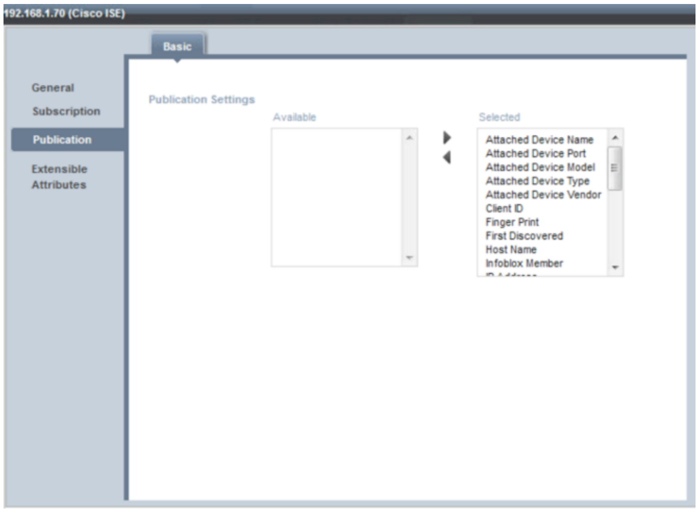
Note: You need to define the ISE extensible attributes first.



Map other data types to extensible attributes

Data Type	Extensible Attributes
Audit Session ID	ISE_Audit_Session_ID
EPS Status	ISE_Quarantine
NAS IP Address	ISE_NAS_IP_Address
MAC	ISE_MAC
IP Address	ISE_IP
NAS Port ID	ISE_NAS_Port_ID
Account Session ID	ISE_Account_Session_ID

Step 19 Select -> **Next**
Step 20 Select -> **Publication**
Step 21 Move all the available attributes into the Selected Column



Publication Settings

Available

Selected: Attached Device Name, Attached Device Port, Attached Device Model, Attached Device Type, Attached Device Vendor, Client ID, Finger Print, First Discovered, Host Name, Infoblox Member

Step 22 Select **Next**

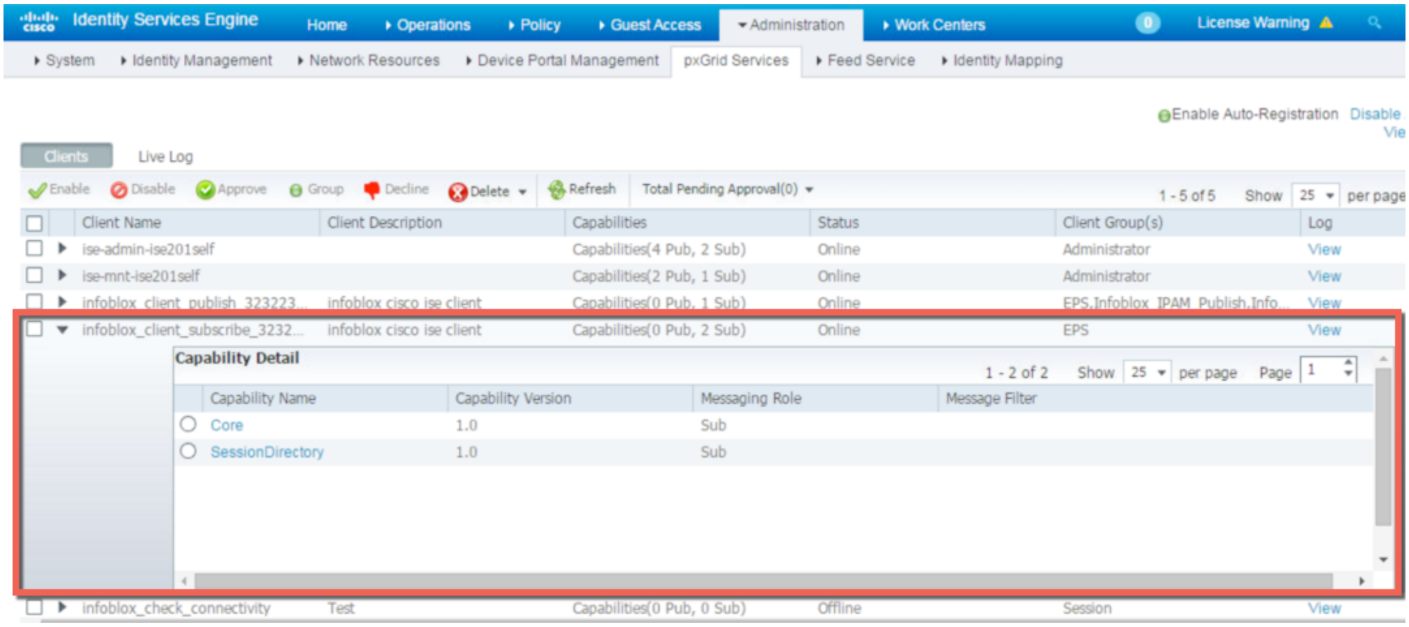
Step 23 Select **Extensible Attributes**, leave the defaults which are empty, then **Save and Close**

Step 24 You can also verify in ISE

Select **Administration->pxGrid Services**

Note: The Infoblox client publish client will appear after the admin approval of the DHCP and IPAM topics

Ensure that Auto-Registration is enabled; otherwise, the Infoblox client will remain in a pending state until the admin selects the client and then selects **Approve** from the pxGrid menu.



□		Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	▸	ise-admin-ise201self		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	▸	ise-mnt-ise201self		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	▸	infoblox_client_publish_323223...	infoblox cisco ise client	Capabilities(0 Pub, 1 Sub)	Online	EPS,Infoblox_IPAM_Publish,Info...	View
□	▾	infoblox_client_subscribe_3232...	infoblox cisco ise client	Capabilities(0 Pub, 2 Sub)	Online	EPS	View
□	▸	infoblox_check_connectivity	Test	Capabilities(0 Pub, 0 Sub)	Offline	Session	View

Capability Detail

	Capability Name	Capability Version	Messaging Role	Message Filter
○	Core	1.0	Sub	
○	SessionDirectory	1.0	Sub	

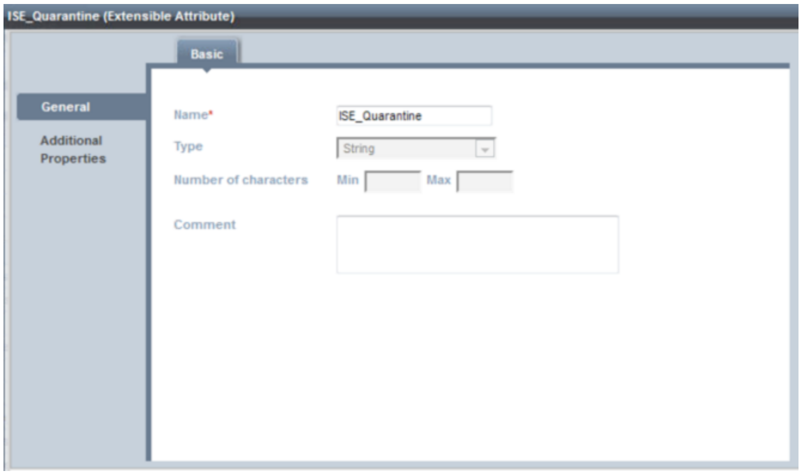
Creating Infoblox Extensible Attributes for ISE

You need to create extensible attributes and values for all of the subscribed attributes and map these to the data types in the subscription process during the initial ISE Ecosystem configuration.

Note: To make it easier to distinguish attributes for ISE subscribed data. Preface each name with the name "ISE."

Step 1 Select **Administration->Extensible Attributes**

Step 2 Click the add **(+)** icon to add an extensible attribute, and enter the **name**, and select **string**



ISE_Quarantine (Extensible Attribute)

Name* ISE_Quarantine

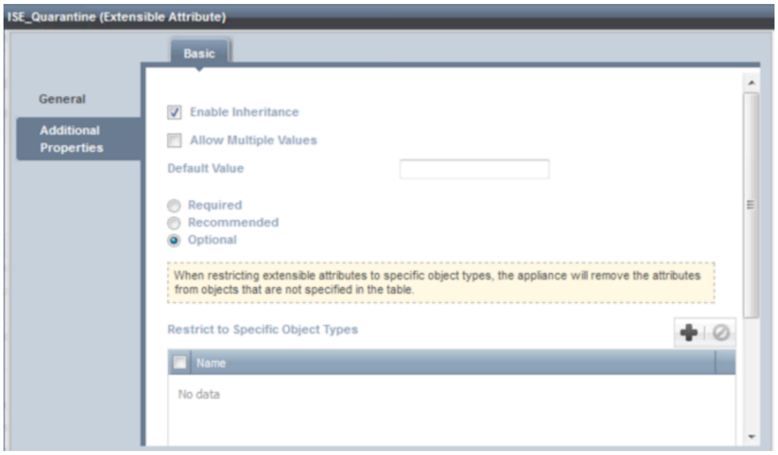
Type String

Number of characters Min Max

Comment

Step 3 Select **Next**

Step 4 Enable **"Enable Inheritance"** and select **"Optional"**



ISE_Quarantine (Extensible Attribute)

☑ Enable Inheritance

□ Allow Multiple Values

Default Value

○ Required

○ Recommended

● Optional

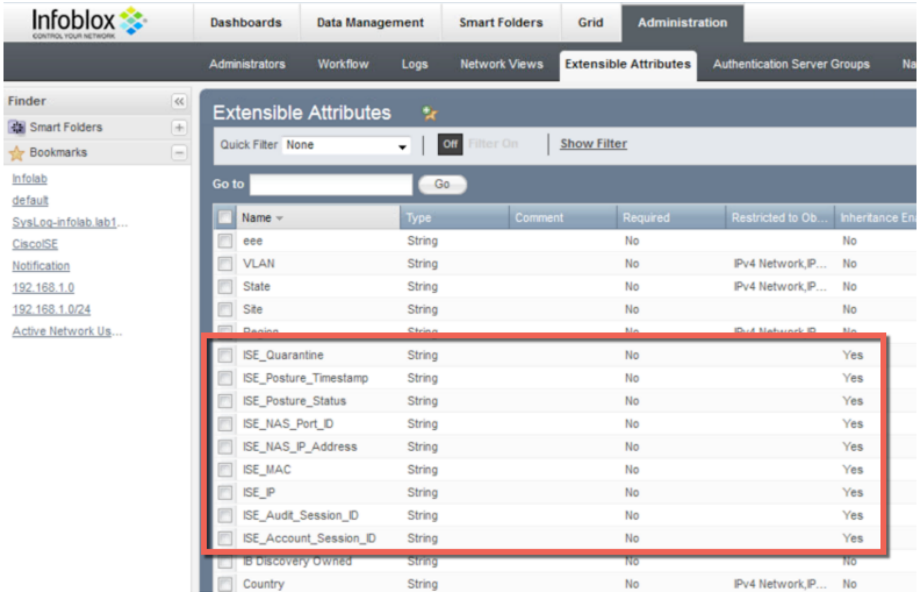
When restricting extensible attributes to specific object types, the appliance will remove the attributes from objects that are not specified in the table.

Restrict to Specific Object Types

□ Name
No data

Step 5 Select **Save and Close**

Step 6 Repeat steps 2 through 5 to add the following: ISE_Posture_Timestamp, ISE_Posture_Status, ISE_NAS_Port_ID, ISE_NAS_IP_Address, ISE_MAC, ISE_IP, ISE_Audit_Session_ID, ISE_Account_Session_ID



Extensible Attributes

Quick Filter: None

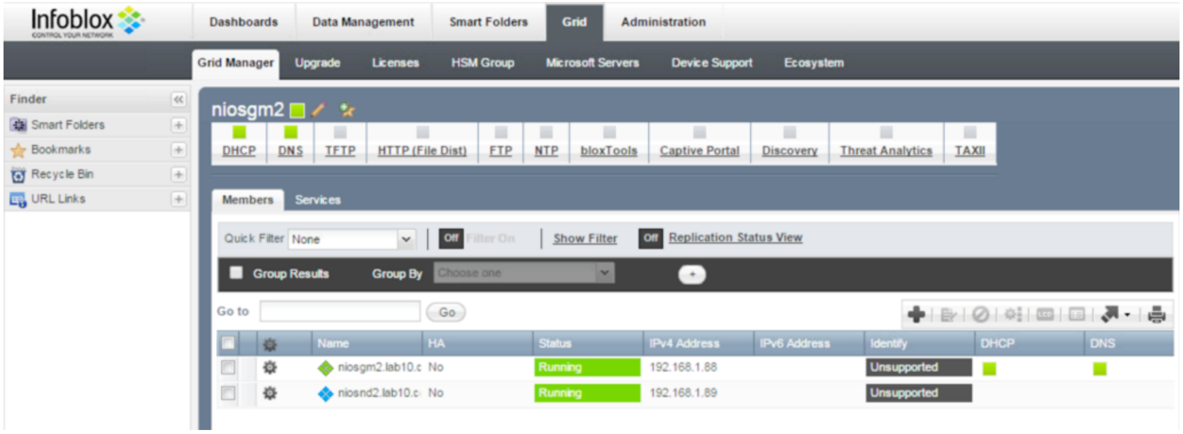
Go to

Name	Type	Comment	Required	Restricted to Ob...	Inheritance En
eee	String		No		No
VLAN	String		No	IPv4 Network,IP...	No
State	String		No	IPv4 Network,IP...	No
Site	String		No		No
Region	String		No	IPv4 Network,IP...	No
ISE_Quarantine	String		No		Yes
ISE_Posture_Timestamp	String		No		Yes
ISE_Posture_Status	String		No		Yes
ISE_NAS_Port_ID	String		No		Yes
ISE_NAS_IP_Address	String		No		Yes
ISE_MAC	String		No		Yes
ISE_IP	String		No		Yes
ISE_Audit_Session_ID	String		No		Yes
ISE_Account_Session_ID	String		No		Yes
IB Discovery Owned	String		No		No
Country	String		No	IPv4 Network,IP...	No

Enabling Data Management Network Users View

This section steps through enabling the Data Management Network Users View on the Grid Master so the Infoblox admin can view the active users from the authenticated ISE sessions.

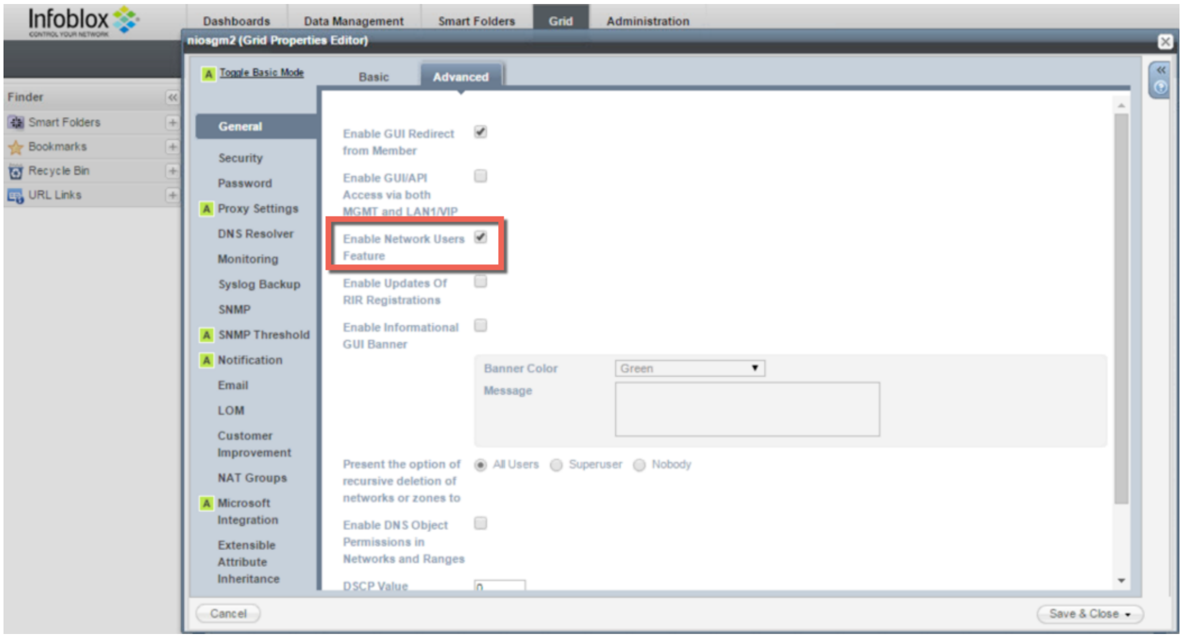
Step 1 Select **Grid -> Grid Manager -> Members**



Quick Filter: None

		Name	HA	Status	IPv4 Address	IPv6 Address	Identify	DHCP	DNS
□	⚙	niosgm2.lab10.c	No	Running	192.168.1.88		Unsupported	🟩	🟩
□	⚙	niosnd2.lab10.c	No	Running	192.168.1.89		Unsupported		

Step 2 From the Toolbar, select **Grid Properties->Edit->Advanced->enable** the **Enable Network Users Feature**



Enable GUI Redirect from Member ☑

Enable GUI/API Access via both MGMT and LAN1/VIP ☐

Enable Network Users Feature ☑

Enable Updates Of RIR Registrations ☐

Enable Informational GUI Banner ☐

Banner Color: Green

Message:

Present the option of recursive deletion of networks or zones to ● All Users ○ Superuser ○ Nobody

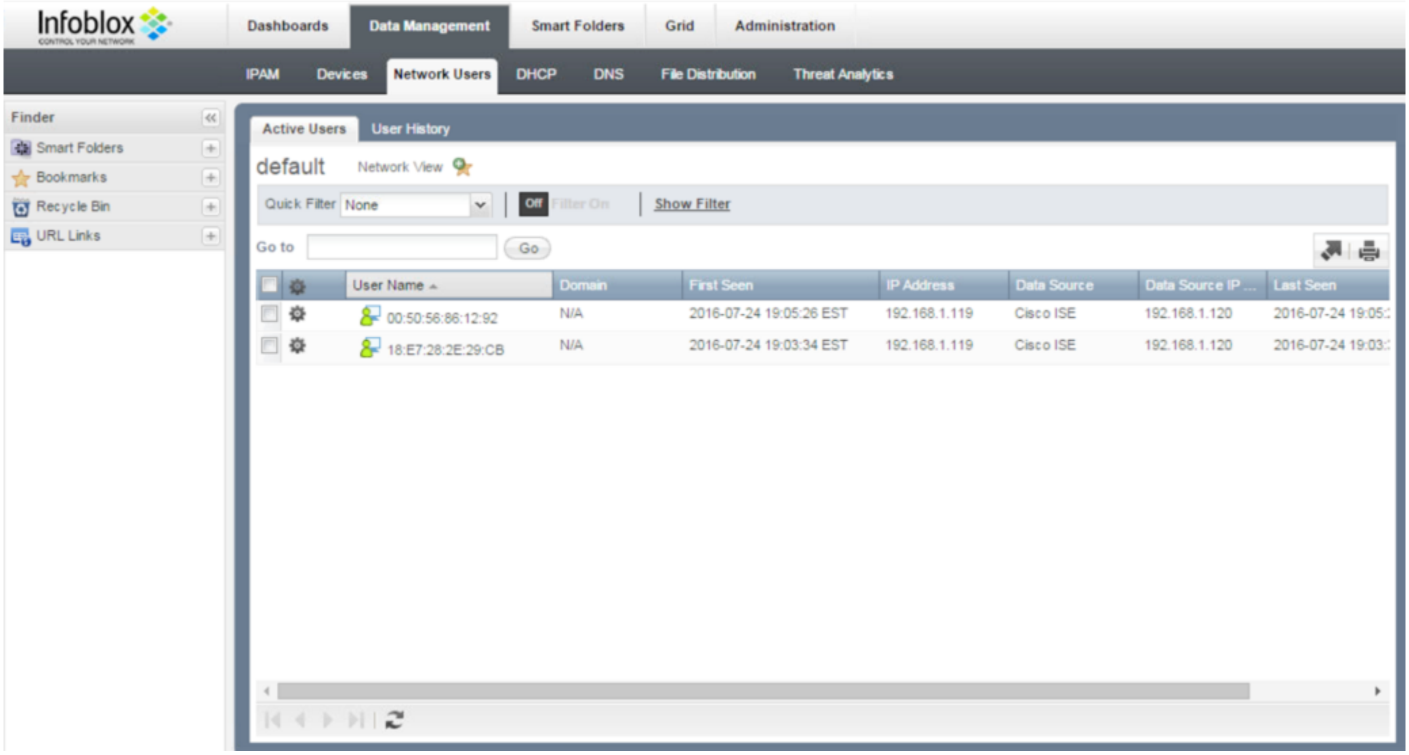
Enable DNS Object Permissions in Networks and Ranges ☐

DSCP Value: 0

Step 3 Select **Save and Close**

Step 4 Select **Data Management->Network Users**, you should see the activity screen

Note: The activity screen displays the ISE authenticated user information



		User Name	Domain	First Seen	IP Address	Data Source	Data Source IP ...	Last Seen
□		00:50:56:86:12:92	N/A	2016-07-24 19:05:26 EST	192.168.1.119	Cisco ISE	192.168.1.120	2016-07-24 19:05:
□		18:E7:28:2E:29:CB	N/A	2016-07-24 19:03:34 EST	192.168.1.119	Cisco ISE	192.168.1.120	2016-07-24 19:03:

Dynamic Topics

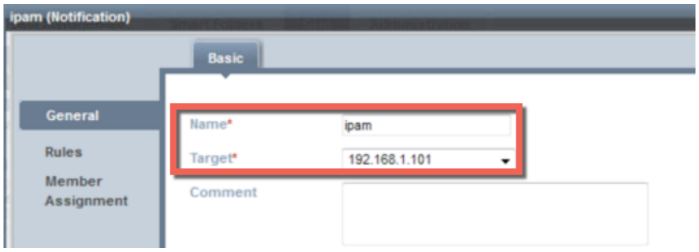
Infoblox has the ability to publish DHCP and IPAM dynamic topics. DHCP and IPAM notifications are created on the Infoblox GM. These topics need to be approved by the ISE pxGrid admin and assigned to the appropriate publisher, subscription and action groups for other clients connected to the grid to consume this information.

Create IPAM Dynamic Topic

Step 1 Create IPAM Notifications

Note: IF-MAP must be disabled to publish DHCP notifications

Step 2 On the Infoblox Grid Master, select **Grid->Ecosystem->Notification->+** add the notification name and the IP address of the ISE pxGrid node



ipam (Notification)

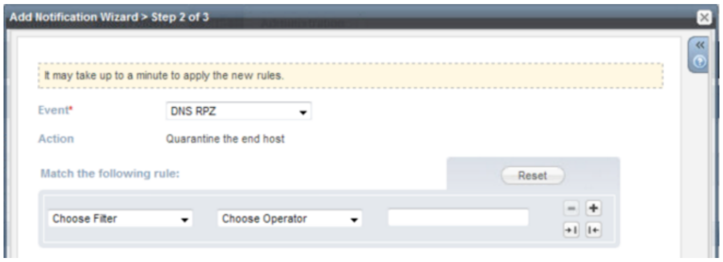
Name* ipam

Target* 192.168.1.101

Comment

Step 3 Select ->**Next**

Step 4 You should see the following



Add Notification Wizard > Step 2 of 3

It may take up to a minute to apply the new rules.

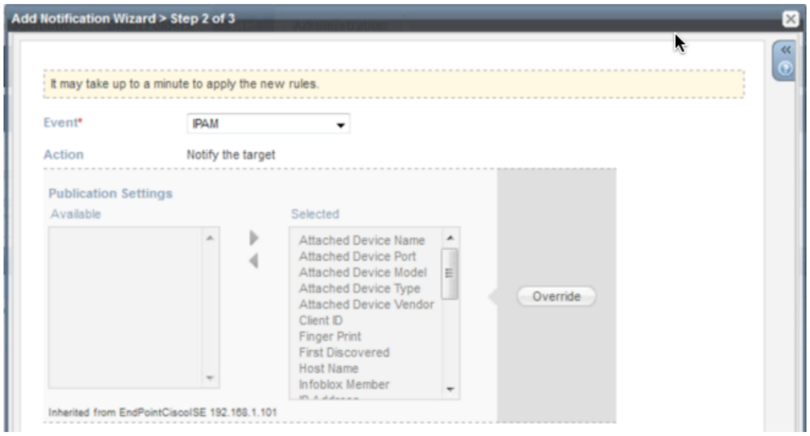
Event* DNS RPZ

Action Quarantine the end host

Match the following rule:

Choose Filter | Choose Operator

Step 5 Change the **Event** from **DNS RPZ** to **IPAM**
You should see the following:



Add Notification Wizard > Step 2 of 3

It may take up to a minute to apply the new rules.

Event*: IPAM

Action: Notify the target

Publication Settings

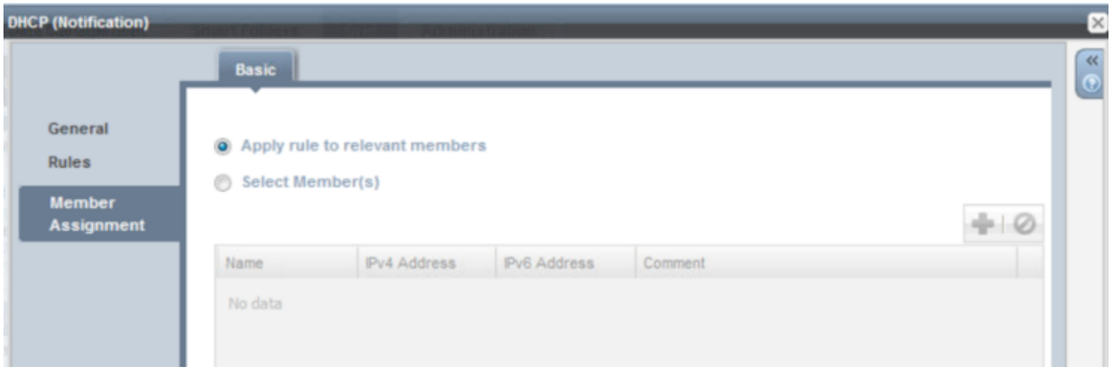
Available:

Selected:
Attached Device Name
Attached Device Port
Attached Device Model
Attached Device Type
Attached Device Vendor
Client ID
Finger Print
First Discovered
Host Name
Infoblox Member

Inherited from EndPointCiscoISE 192.168.1.101

Step 6 Select **Next**

Step 7 Leave the defaults for applying the rule to relevant members



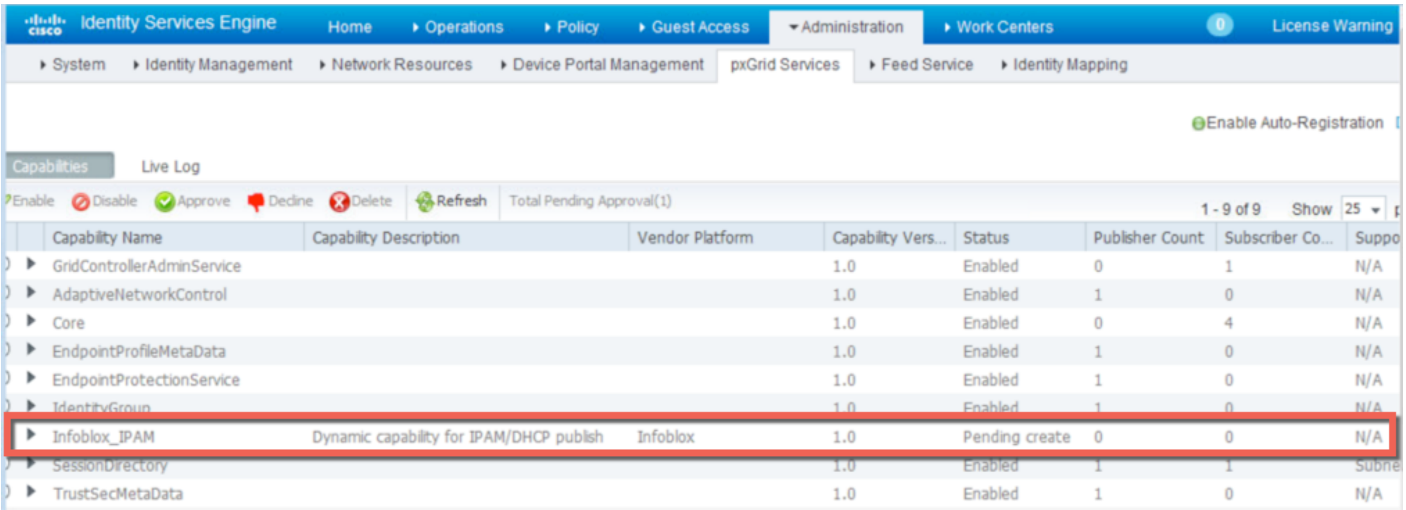
DHCP (Notification)

● Apply rule to relevant members
○ Select Member(s)

Name	IPv4 Address	IPv6 Address	Comment
No data			

Step 8 Select **Save and Close**

Step 9 Go to ISE, **Administration->pxGrid Services-> View by Capabilities**
The admin must approve the IPAM topic before Infoblox is able to publish this topic.

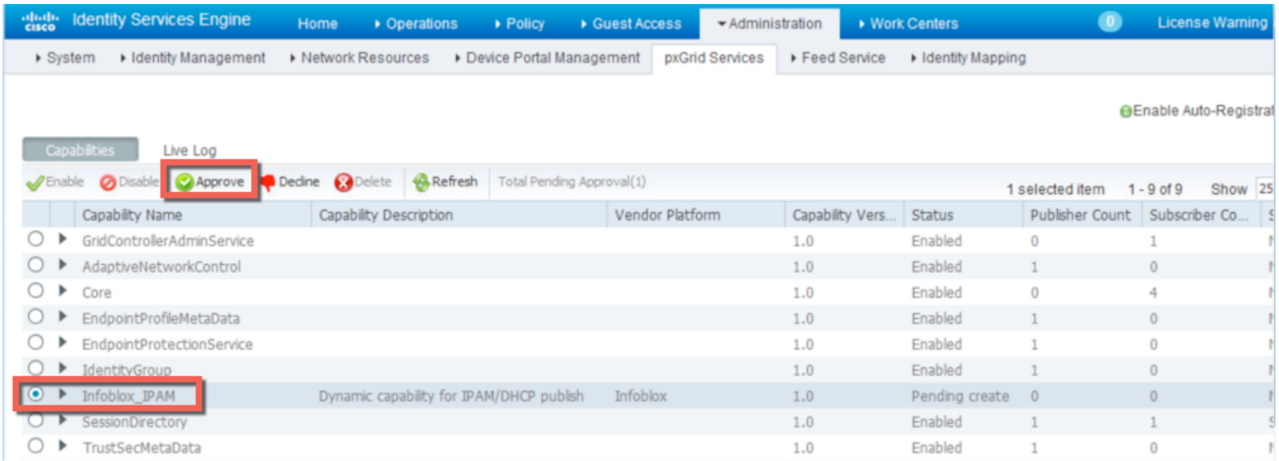


Total Pending Approval(1)

1 - 9 of 9 Show 25

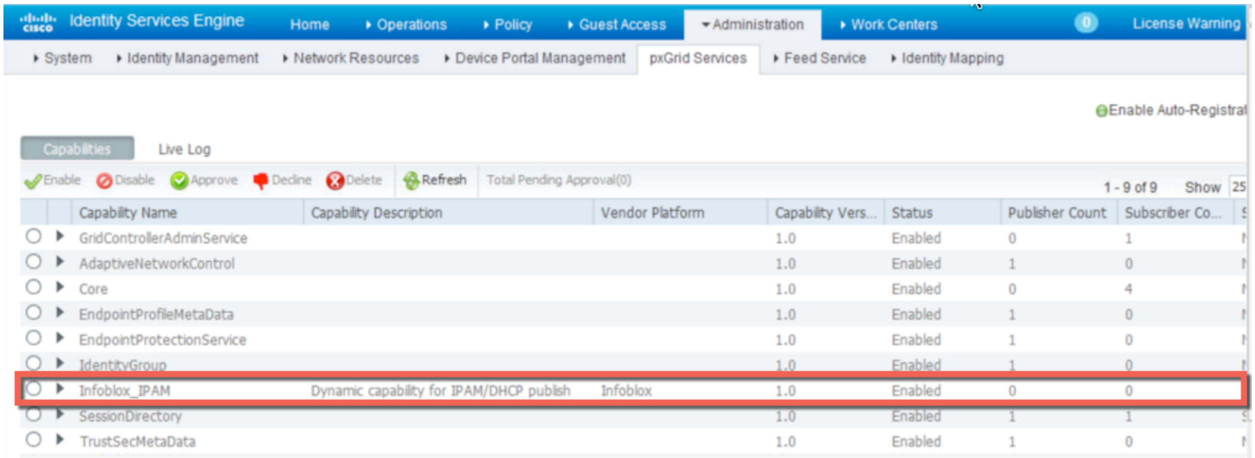
Capability Name	Capability Description	Vendor Platform	Capability Vers...	Status	Publisher Count	Subscriber Co...	Suppo
GridControllerAdminService			1.0	Enabled	0	1	N/A
AdaptiveNetworkControl			1.0	Enabled	1	0	N/A
Core			1.0	Enabled	0	4	N/A
EndpointProfileMetaData			1.0	Enabled	1	0	N/A
EndpointProtectionService			1.0	Enabled	1	0	N/A
IdentityGroup			1.0	Enabled	1	0	N/A
Infoblox_IPAM	Dynamic capability for IPAM/DHCP publish	Infoblox	1.0	Pending create	0	0	N/A
SessionDirectory			1.0	Enabled	1	1	Subne
TrustSecMetaData			1.0	Enabled	1	0	N/A

Step 10 Select **Infoblox_IPAM->Approve,** you will see a message to approve the topic, select ->**yes**



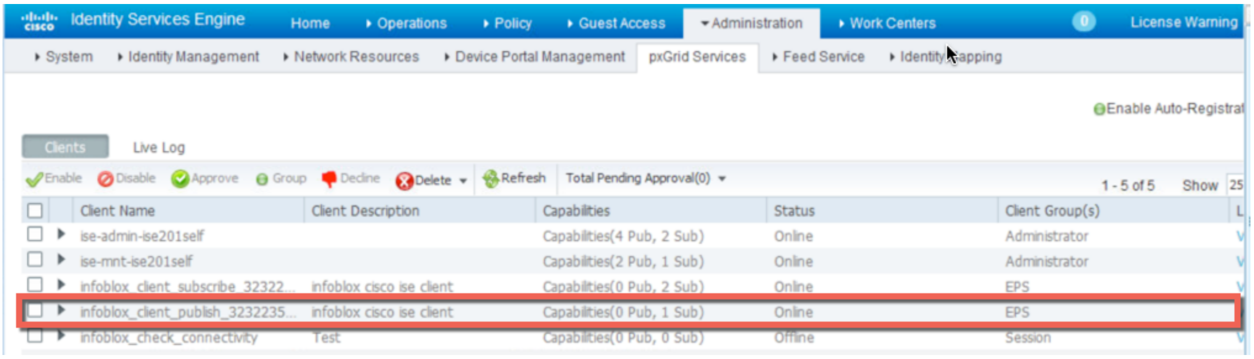
	Capability Name	Capability Description	Vendor Platform	Capability Vers...	Status	Publisher Count	Subscriber Co...
○	GridControllerAdminService			1.0	Enabled	0	1
○	AdaptiveNetworkControl			1.0	Enabled	1	0
○	Core			1.0	Enabled	0	4
○	EndpointProfileMetaData			1.0	Enabled	1	0
○	EndpointProtectionService			1.0	Enabled	1	0
○	IdentityGroup			1.0	Enabled	1	0
●	Infoblox_IPAM	Dynamic capability for IPAM/DHCP publish	Infoblox	1.0	Pending create	0	0
○	SessionDirectory			1.0	Enabled	1	1
○	TrustSecMetaData			1.0	Enabled	1	0

Step 11 Note the IPAM Topic is now enabled



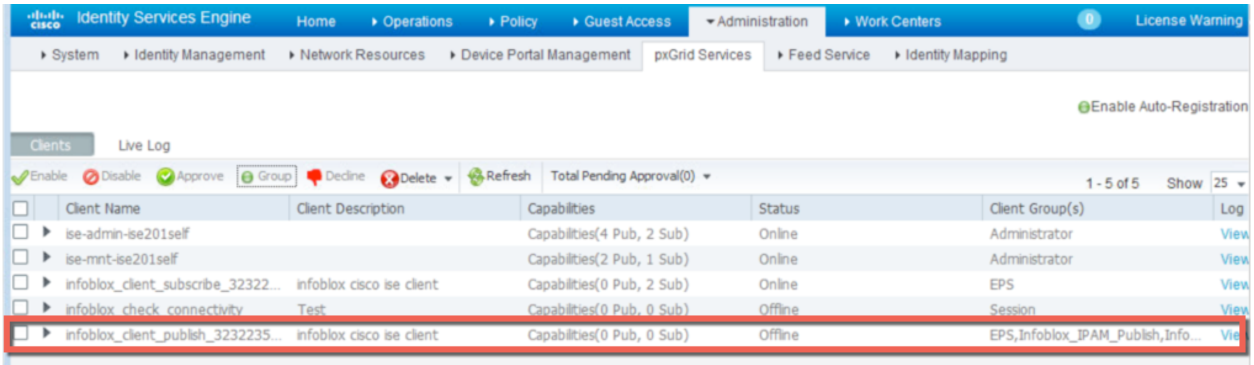
	Capability Name	Capability Description	Vendor Platform	Capability Vers...	Status	Publisher Count	Subscriber Co...
○	GridControllerAdminService			1.0	Enabled	0	1
○	AdaptiveNetworkControl			1.0	Enabled	1	0
○	Core			1.0	Enabled	0	4
○	EndpointProfileMetaData			1.0	Enabled	1	0
○	EndpointProtectionService			1.0	Enabled	1	0
○	IdentityGroup			1.0	Enabled	1	0
○	Infoblox_IPAM	Dynamic capability for IPAM/DHCP publish	Infoblox	1.0	Enabled	0	0
○	SessionDirectory			1.0	Enabled	1	1
○	TrustSecMetaData			1.0	Enabled	1	0

Step 12 Select **View By Clients**
You should see the following



□	Client Name	Client Description	Capabilities	Status	Client Group(s)
□	ise-admin-ise201self		Capabilities(4 Pub, 2 Sub)	Online	Administrator
□	ise-mnt-ise201self		Capabilities(2 Pub, 1 Sub)	Online	Administrator
□	infoblox_client_subscribe_32322...	infoblox cisco ise client	Capabilities(0 Pub, 2 Sub)	Online	EPS
□	infoblox_client_publish_3232235...	infoblox cisco ise client	Capabilities(0 Pub, 1 Sub)	Online	EPS
□	infoblox_check_connectivity	Test	Capabilities(0 Pub, 0 Sub)	Offline	Session

Step 13 You need to add the IPAM publish, IPAM subscribe, and IPAM action groups
Select the **Infoblox client publish**…. client topic, ->**Group-Add->Infoblox_IPAM_Publish, Infoblox_IPAM_Subscribe and Infoblox_IPAM_Action->Save**
You should see the published topic now available to pxGrid subscribers



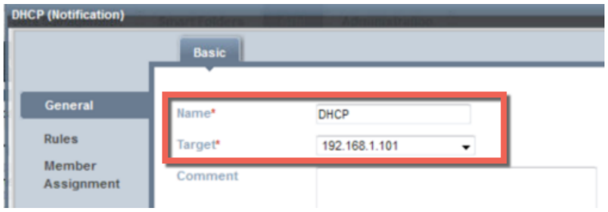
□	Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	ise-admin-ise201self		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	ise-mnt-ise201self		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	infoblox_client_subscribe_32322...	infoblox cisco ise client	Capabilities(0 Pub, 2 Sub)	Online	EPS	View
□	infoblox_check_connectivity	Test	Capabilities(0 Pub, 0 Sub)	Offline	Session	View
□	infoblox_client_publish_3232235...	infoblox cisco ise client	Capabilities(0 Pub, 0 Sub)	Offline	EPS,Infoblox_IPAM_Publish,Info...	View

Create DHCP Dynamic Topic

Step 1 Create DHCP Notifications

Note: IF-MAP must be disabled to publish DHCP notifications

Step 2 On Infoblox Grid Master, select **Grid->Ecosystem->Notification->+** add the notification name and the IP address of the ISE pxGrid node



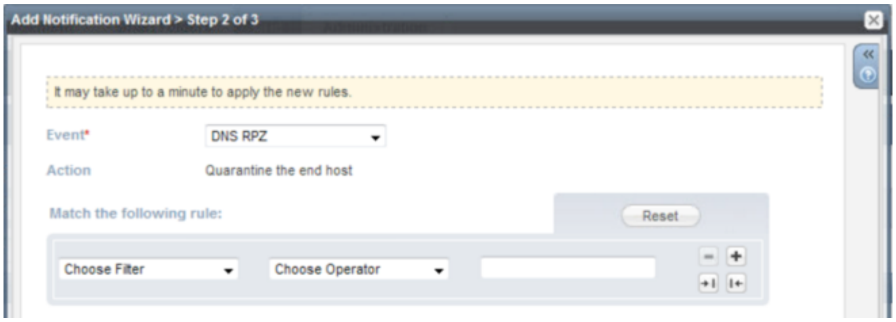
Name* DHCP

Target* 192.168.1.101

Comment

Step 3 Select ->**Next**

Step 4 You should see the following



It may take up to a minute to apply the new rules.

Event* DNS RPZ

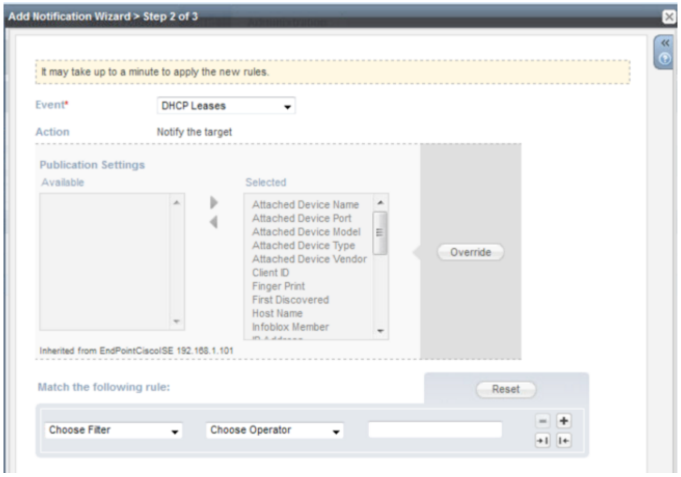
Action Quarantine the end host

Match the following rule:

Choose Filter | Choose Operator

Step 5 Change the **Event** from **DNS RPZ** to **DHCP Leases**

You should see the following:



It may take up to a minute to apply the new rules.

Event* DHCP Leases

Action Notify the target

Publication Settings

Available

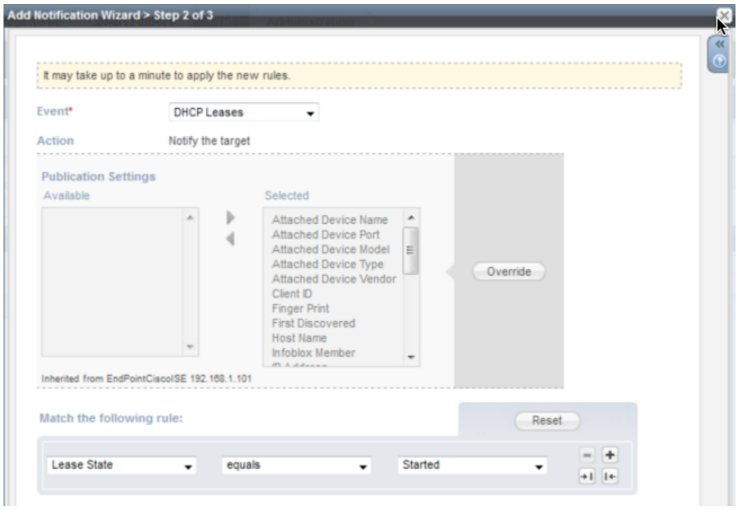
Selected: Attached Device Name, Attached Device Port, Attached Device Model, Attached Device Type, Attached Device Vendor, Client ID, Finger Print, First Discovered, Host Name, Infoblox Member, IP Address

Inherited from EndPointCiscoISE 192.168.1.101

Match the following rule:

Choose Filter | Choose Operator

Step 6 Under Match the following rule: change **Choose Filter** to **Lease State** and select the desired lease state: Started, Expired or Renewed. In this document **Started** was selected



It may take up to a minute to apply the new rules.

Event* DHCP Leases

Action Notify the target

Publication Settings

Available

Selected: Attached Device Name, Attached Device Port, Attached Device Model, Attached Device Type, Attached Device Vendor, Client ID, Finger Print, First Discovered, Host Name, Infoblox Member, IP Address

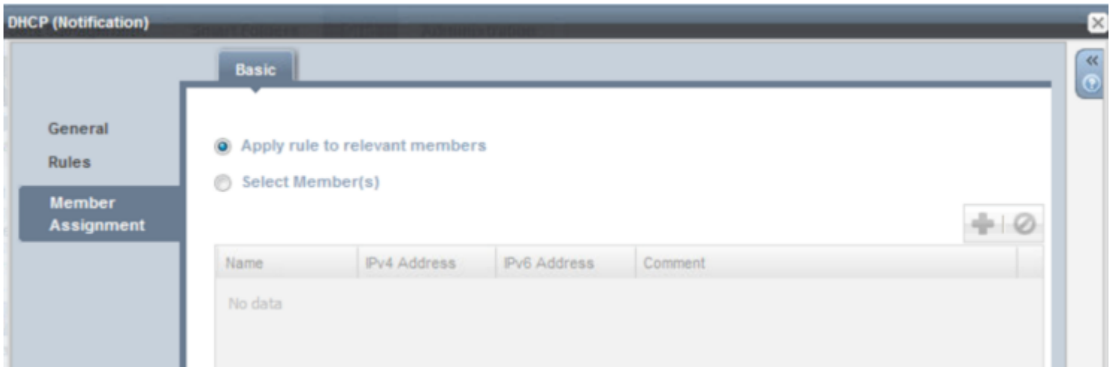
Inherited from EndPointCiscoISE 192.168.1.101

Match the following rule:

Lease State | equals | Started

Step 7 Select **Next**

Step 8 Leave the defaults for applying the rule to relevant members



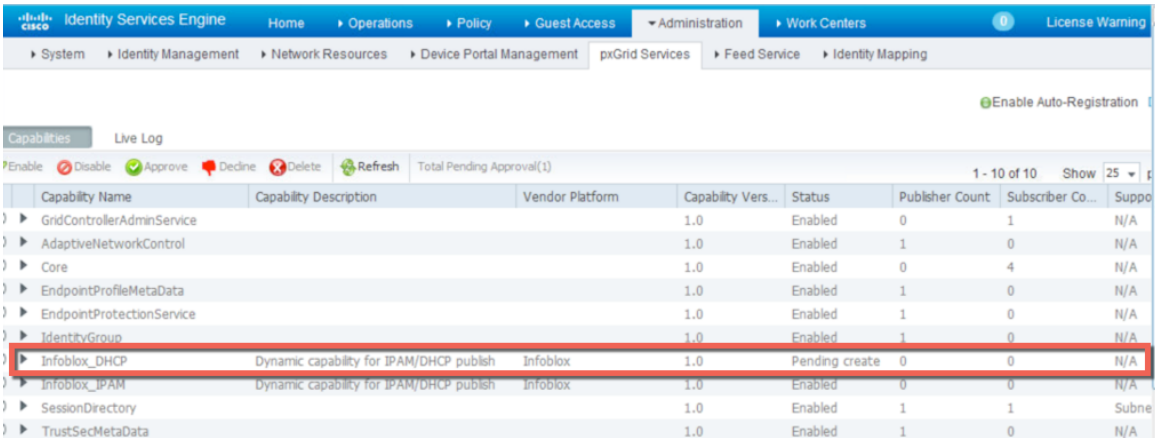
● Apply rule to relevant members

○ Select Member(s)

Name	IPv4 Address	IPv6 Address	Comment
No data			

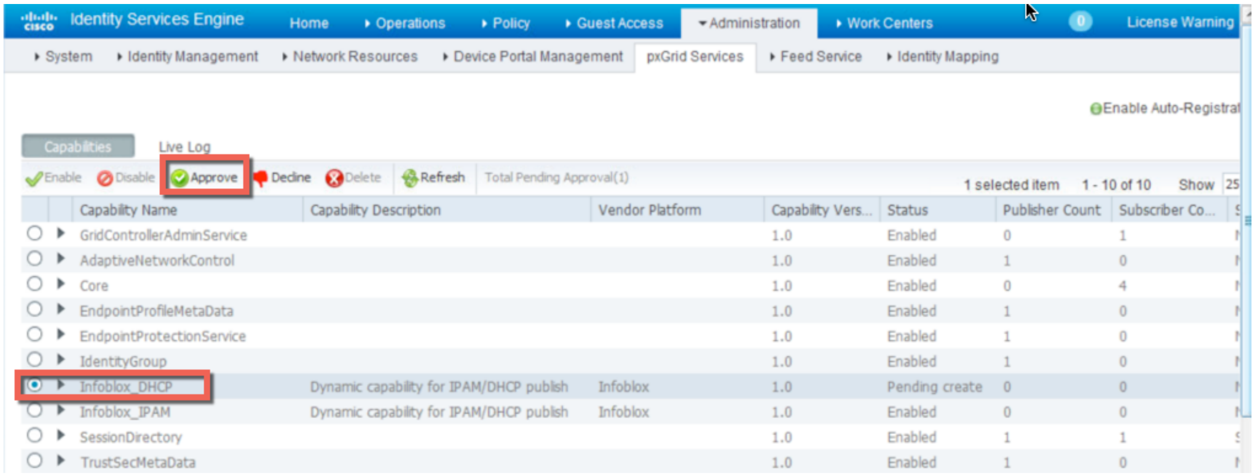
Step 9 Select **Save and Close**

Step 10 Go to ISE, **Administration->pxGrid Services-> View by Capabilities**.
The admin must approve the DHCP topic before Infoblox is able to publish this topic.



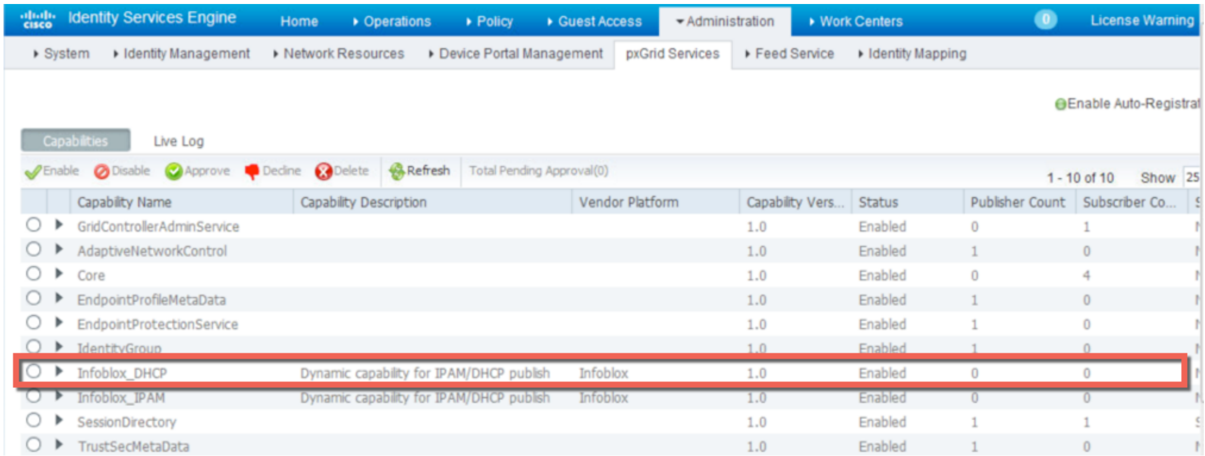
Capability Name	Capability Description	Vendor Platform	Capability Vers...	Status	Publisher Count	Subscriber Co...	Suppo
GridControllerAdminService			1.0	Enabled	0	1	N/A
AdaptiveNetworkControl			1.0	Enabled	1	0	N/A
Core			1.0	Enabled	0	4	N/A
EndpointProfileMetaData			1.0	Enabled	1	0	N/A
EndpointProtectionService			1.0	Enabled	1	0	N/A
IdentityGroup			1.0	Enabled	1	0	N/A
Infoblox_DHCP	Dynamic capability for IPAM/DHCP publish	Infoblox	1.0	Pending create	0	0	N/A
Infoblox_IPAM	Dynamic capability for IPAM/DHCP publish	Infoblox	1.0	Enabled	0	0	N/A
SessionDirectory			1.0	Enabled	1	1	Subne
TrustSecMetaData			1.0	Enabled	1	0	N/A

Step 11 Select **Infoblox_DHCP->Approve,** you will see a message to approve the topic, select **->yes**



	Capability Name	Capability Description	Vendor Platform	Capability Vers...	Status	Publisher Count	Subscriber Co...
○	GridControllerAdminService			1.0	Enabled	0	1
○	AdaptiveNetworkControl			1.0	Enabled	1	0
○	Core			1.0	Enabled	0	4
○	EndpointProfileMetaData			1.0	Enabled	1	0
○	EndpointProtectionService			1.0	Enabled	1	0
○	IdentityGroup			1.0	Enabled	1	0
●	Infoblox_DHCP	Dynamic capability for IPAM/DHCP publish	Infoblox	1.0	Pending create	0	0
○	Infoblox_IPAM	Dynamic capability for IPAM/DHCP publish	Infoblox	1.0	Enabled	0	0
○	SessionDirectory			1.0	Enabled	1	1
○	TrustSecMetaData			1.0	Enabled	1	0

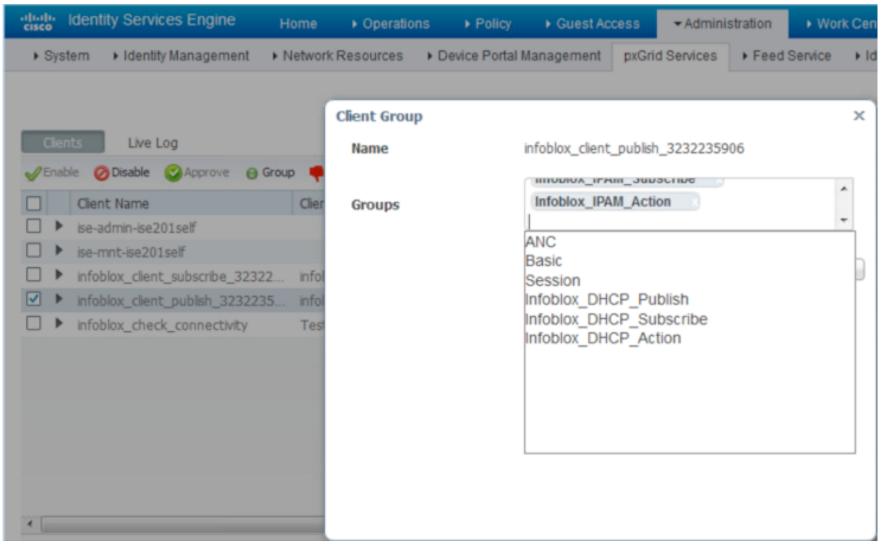
Step 12 Note the DHCP Topic is now enabled



	Capability Name	Capability Description	Vendor Platform	Capability Vers...	Status	Publisher Count	Subscriber Co...
○	GridControllerAdminService			1.0	Enabled	0	1
○	AdaptiveNetworkControl			1.0	Enabled	1	0
○	Core			1.0	Enabled	0	4
○	EndpointProfileMetaData			1.0	Enabled	1	0
○	EndpointProtectionService			1.0	Enabled	1	0
○	IdentityGroup			1.0	Enabled	1	0
○	Infoblox_DHCP	Dynamic capability for IPAM/DHCP publish	Infoblox	1.0	Enabled	0	0
○	Infoblox_IPAM	Dynamic capability for IPAM/DHCP publish	Infoblox	1.0	Enabled	0	0
○	SessionDirectory			1.0	Enabled	1	1
○	TrustSecMetaData			1.0	Enabled	1	0

Step 13 Select **View By Clients**

Step 14 You need to add the DHCP publish, DHCP subscribe, and DHCP action groups
Select the **Infoblox client publish**…. client topic, ->**Group-Add->Infoblox_DHCP_Publish, Infoblox_DHCP_Subscribe and Infoblox_DHCP_Action->**



Client Group

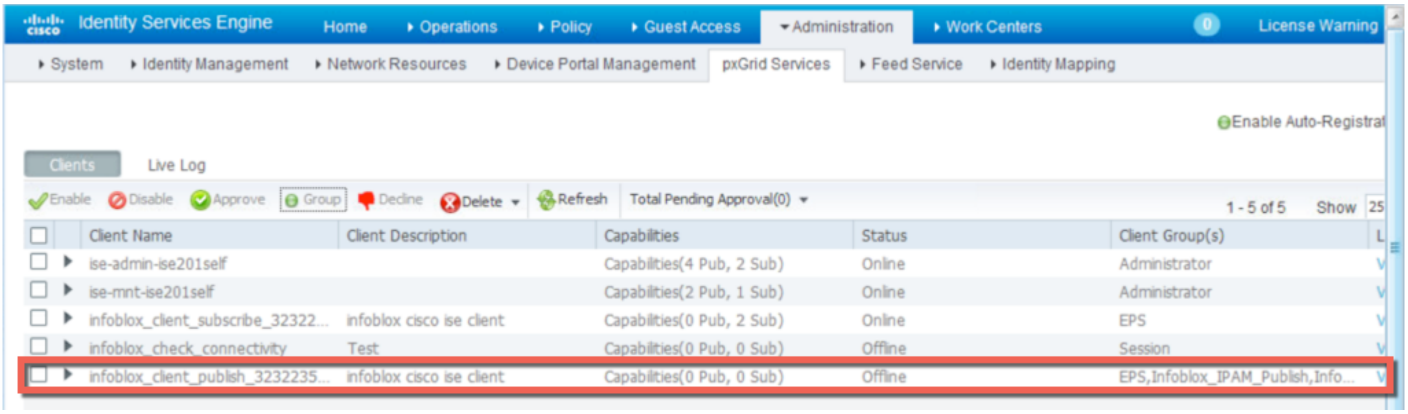
Name infoblox_client_publish_3232235906

Groups Infoblox_IPAM_Subscribe
Infoblox_IPAM_Action

ANC
Basic
Session
Infoblox_DHCP_Publish
Infoblox_DHCP_Subscribe
Infoblox_DHCP_Action

Step 15 Select **Save**

Step 16 You should see the following:

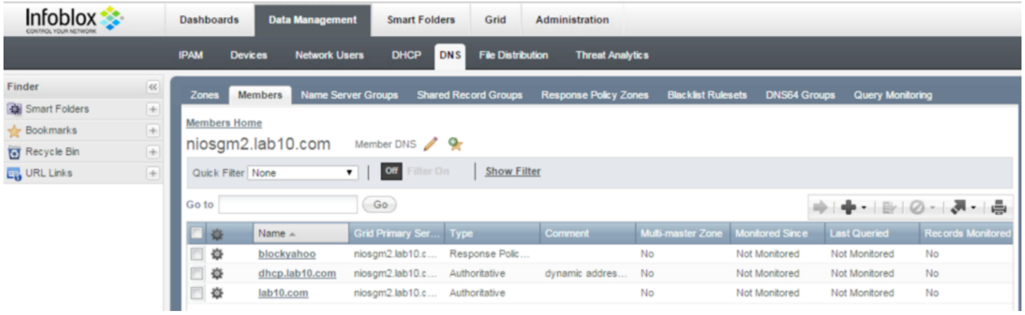


Client Name	Client Description	Capabilities	Status	Client Group(s)
ise-admin-ise201self		Capabilities(4 Pub, 2 Sub)	Online	Administrator
ise-mnt-ise201self		Capabilities(2 Pub, 1 Sub)	Online	Administrator
infoblox_client_subscribe_32322...	infoblox cisco ise client	Capabilities(0 Pub, 2 Sub)	Online	EPS
infoblox_check_connectivity	Test	Capabilities(0 Pub, 0 Sub)	Offline	Session
infoblox_client_publish_3232235...	infoblox cisco ise client	Capabilities(0 Pub, 0 Sub)	Offline	EPS,Infoblox_IPAM_Publish,Info...

Configuring DNS Services

This section takes the reader through enabling DNS services on the Grid Master and creating and configuring DNS zones. A dynamic zone will be created for updating user records dynamically. In addition, a blacklist-zone will be created for blocking the yahoo domain, which will be used later on for demonstrating a RPZ zone violation and quarantining an endpoint.

Note: Each DNS zone configuration is dependent on the specific organization's DNS policy



niosgm2.lab10.com

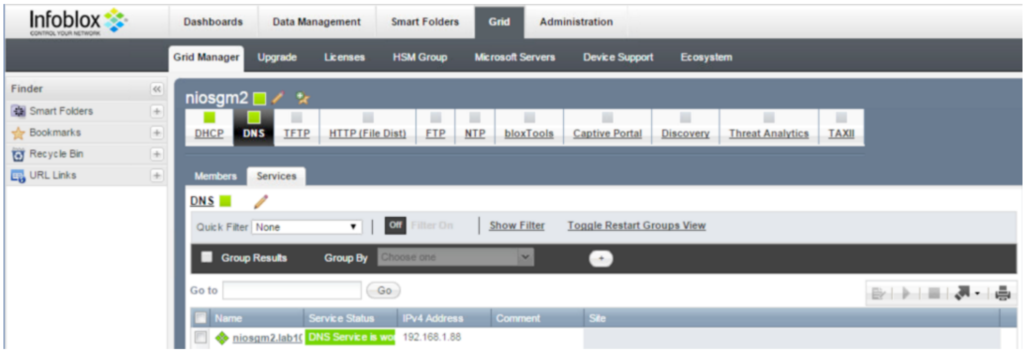
Quick Filter None | Off Filter On | Show Filter

Name	Grid Primary Ser...	Type	Comment	Multi-master Zone	Monitored Since	Last Queried	Records Monitored
blockyahoo	niosgm2.lab10.c...	Response Polic...		No	Not Monitored	Not Monitored	No
dhcp.lab10.com	niosgm2.lab10.c...	Authoritative	dynamic addres...	No	Not Monitored	Not Monitored	No
lab10.com	niosgm2.lab10.c...	Authoritative		No	Not Monitored	Not Monitored	No

Enabling DNS Service on Grid Master

Step 1 Select **Grid->Grid Manager->Members->select the Grid Master->DNS** and **Start** from the Toolbar

Step 2 You should see that the DNS service have started

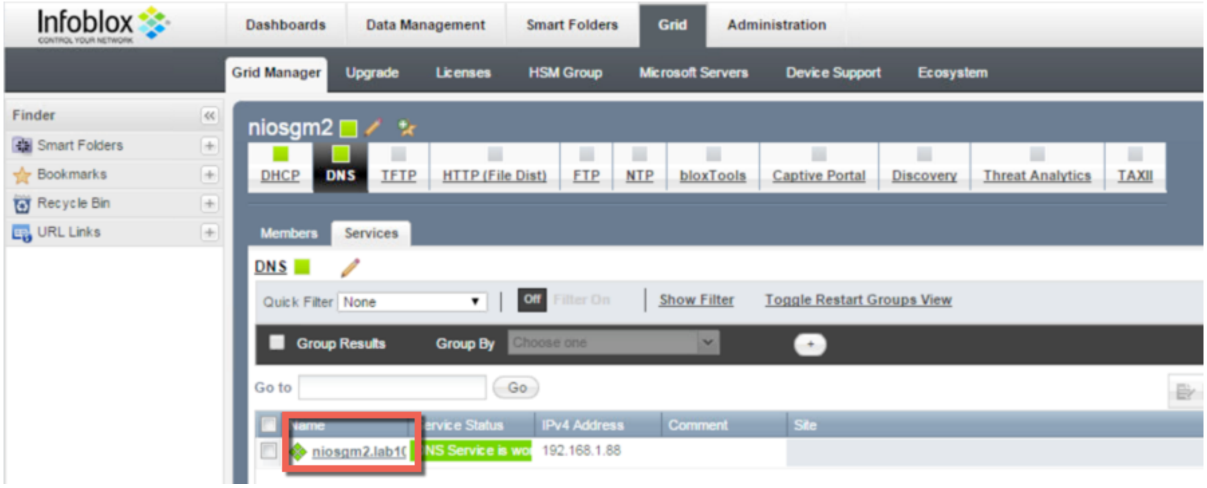


Quick Filter None | Off Filter On

Name	Service Status	IPv4 Address	Comment	Site
niosgm2.lab1(	DNS Service is wo	192.168.1.88		

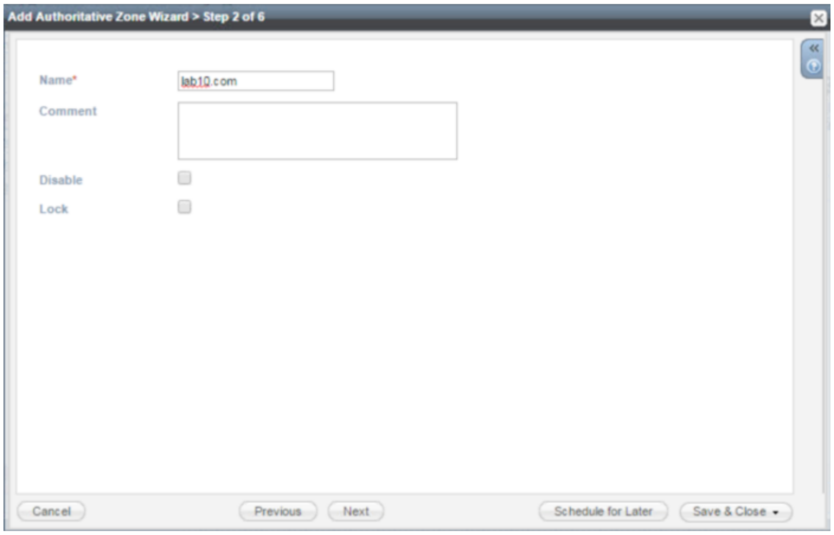
Creating DNS Zone and DNS Zone for Dynamic Addresses

Step 1 Select **Grid-> Grid Manager->DNS->Grid Master**



Name	Service Status	IPv4 Address	Comment	Site
niosgm2.lab1(	NS Service is wo	192.168.1.88		

Step 2 Select **"+"->Authoritative Zone->Add an authoritative forward-mapping zone->Next** enter the name



Name* lab10.com

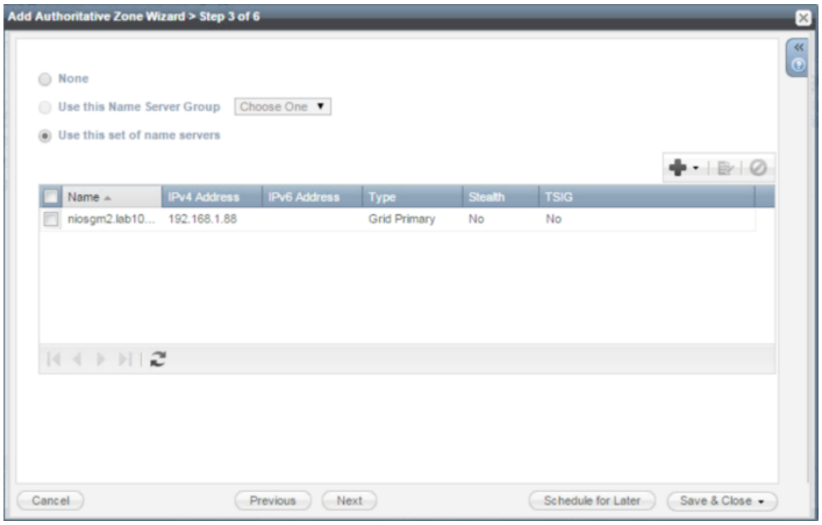
Comment

Disable □

Lock □

Step 3 Select **Next**

Step 4 Select **Use this set of name servers,** the Grid Master



Add Authoritative Zone Wizard > Step 3 of 6

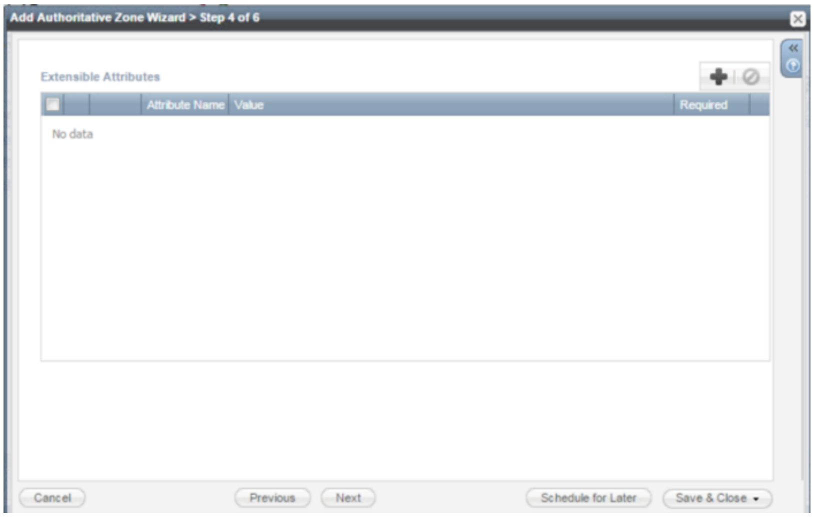
○ None

○ Use this Name Server Group Choose One ▼

● Use this set of name servers

□	Name ▲	IPv4 Address	IPv6 Address	Type	Stealth	TSIG
□	niosgm2.lab10...	192.168.1.88		Grid Primary	No	No

Step 5 Leave the defaults



Add Authoritative Zone Wizard > Step 4 of 6

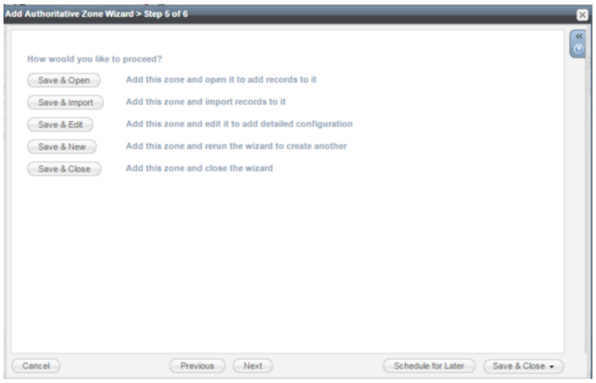
Extensible Attributes

□	Attribute Name	Value	Required

No data

Step 6 Select **Next**

Step 7 Leave the defaults



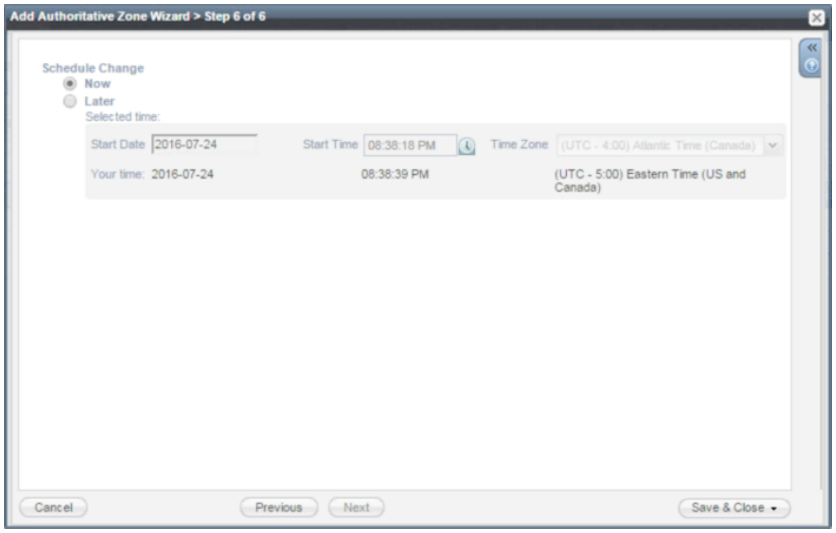
Add Authoritative Zone Wizard > Step 5 of 6

How would you like to proceed?

Save & Open	Add this zone and open it to add records to it
Save & Import	Add this zone and import records to it
Save & Edit	Add this zone and edit it to add detailed configuration
Save & New	Add this zone and rerun the wizard to create another
Save & Close	Add this zone and close the wizard

Step 8 Select **Next**

Step 9 Leave the defaults



Add Authoritative Zone Wizard > Step 6 of 6

Schedule Change

● Now
○ Later

Selected time:

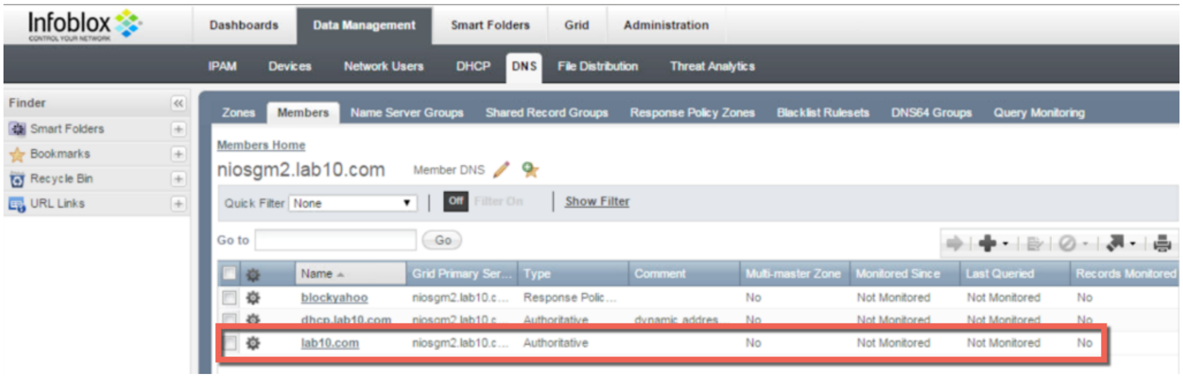
Start Date 2016-07-24 Start Time 08:38:18 PM Time Zone (UTC - 4:00) Atlantic Time (Canada)

Your time: 2016-07-24 08:38:39 PM (UTC - 5:00) Eastern Time (US and Canada)

Step 10 Select **Save and Close**

Step 11 The configuration will require a service restart

Step 12 You should see the configured lab10.com DNS Zone



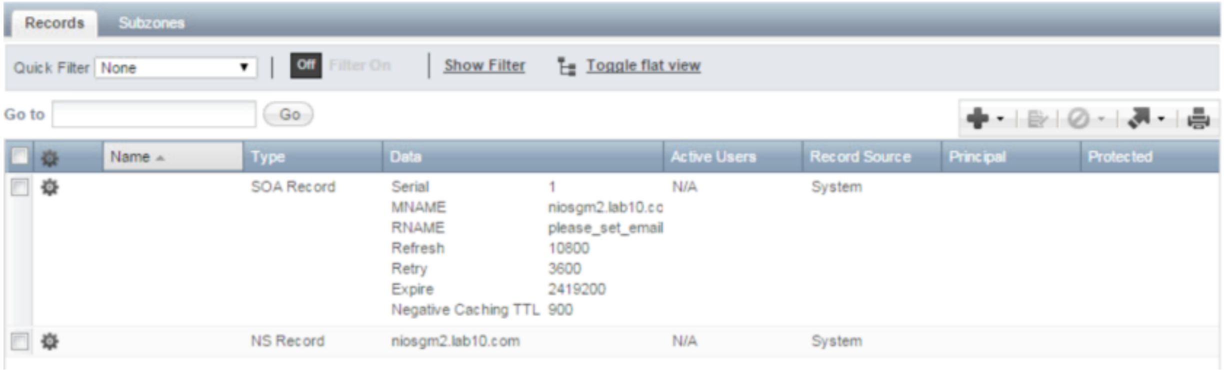
niosgm2.lab10.com Member DNS

Quick Filter None | Off Filter On | Show Filter

Go to Go

Name	Grid Primary Ser...	Type	Comment	Multi-master Zone	Monitored Since	Last Queried	Records Monitored
blockyahoo	niosgm2.lab10.c...	Response Polic...		No	Not Monitored	Not Monitored	No
dhcp.lab10.com	niosgm2.lab10.c...	Authoritative	dynamic addres...	No	Not Monitored	Not Monitored	No
lab10.com	niosgm2.lab10.c...	Authoritative		No	Not Monitored	Not Monitored	No

Step 13 Select the lab10.com DNS zone and select **Records**
You should see the following:



Quick Filter None | Off Filter On | Show Filter | Toggle flat view

Go to Go

Name	Type	Data		Active Users	Record Source	Principal	Protected
	SOA Record	Serial MNAME RNAME Refresh Retry Expire Negative Caching TTL	1 niosgm2.lab10.cc please_set_email 10800 3600 2419200 900	N/A	System		
	NS Record	niosgm2.lab10.com		N/A	System		

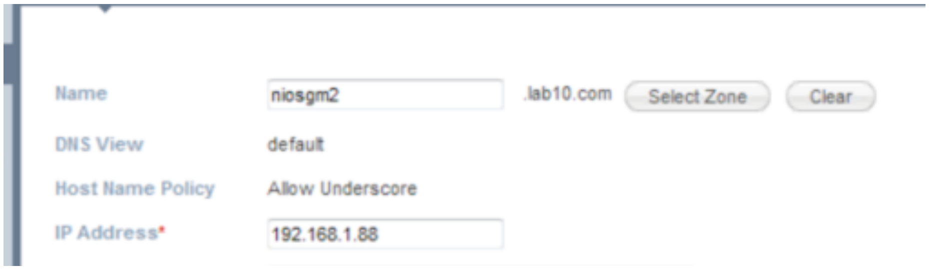
Step 14 Add A records for the ISE pxGrid node, the Infoblox GM, the Infoblox ND Member and a Primary DNS server that the Infoblox GM may forward DNS lookups to.

Note: You may not have a Primary DNS server in your DNS security configuration

Note: Steps 14-21 should have been done automatically if the domain in the FQDN per Grid Master setup matches the Authoritative Zone

Step 15 To add A records, select **"+"->Record->A record**

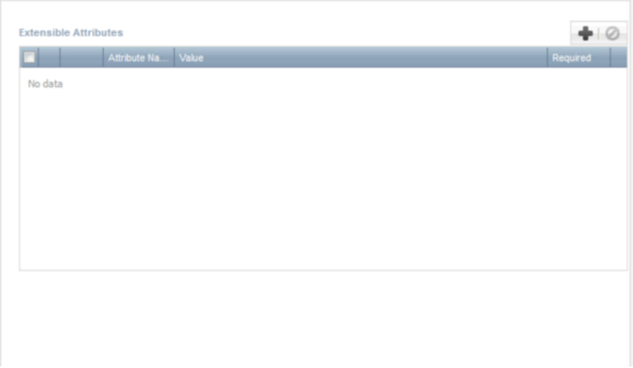
Step 16 Add the host name, the IP address, leave **create associated PTR pointer** enabled



Name: niosgm2 .lab10.com
DNS View: default
Host Name Policy: Allow Underscore
IP Address*: 192.168.1.88

Step 17 Select **Next**

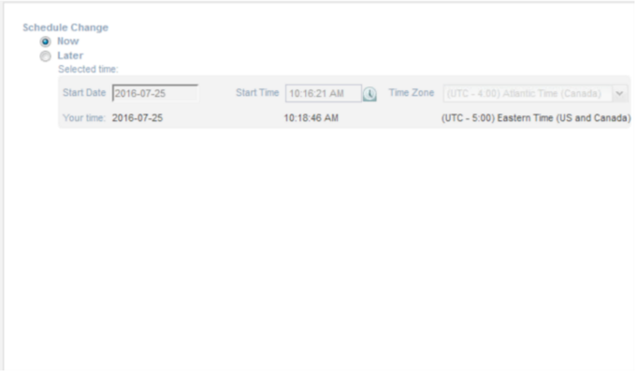
Step 18 Leave the defaults for extensible attributes



Extensible Attributes

□			Attribute Na...	Value	Required
No data					

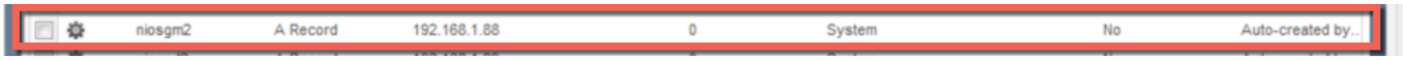
Step 19 Select **Next**



Schedule Change
● Now
○ Later
Selected time:
Start Date 2016-07-25 Start Time 10:16:21 AM Time Zone (UTC - 4:00) Atlantic Time (Canada)
Your time: 2016-07-25 10:18:46 AM (UTC - 5:00) Eastern Time (US and Canada)

Step 20 Select **Save and Close**

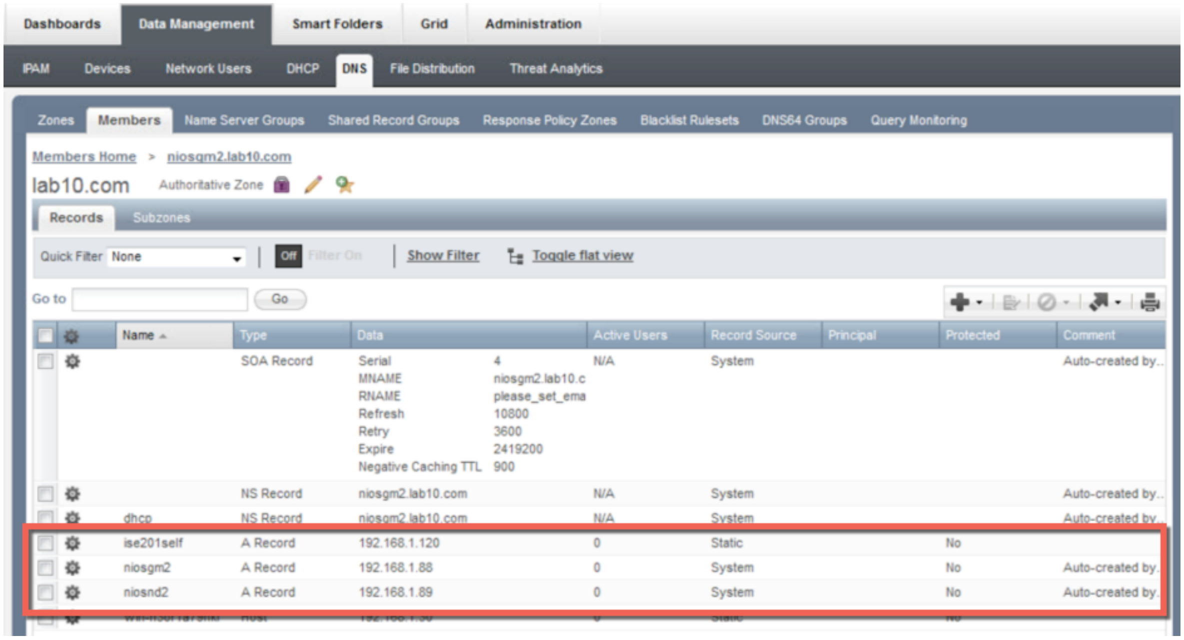
Step 21 You should see the record.



□	niosgm2	A Record	192.168.1.88	0	System	No	Auto-created by...

Step 22 Repeat steps 15-21 for the ISE pxGrid node, the Infoblox GM, the DNS server for forwarding DNS lookups

Step 23 Once completed you should see all the host records



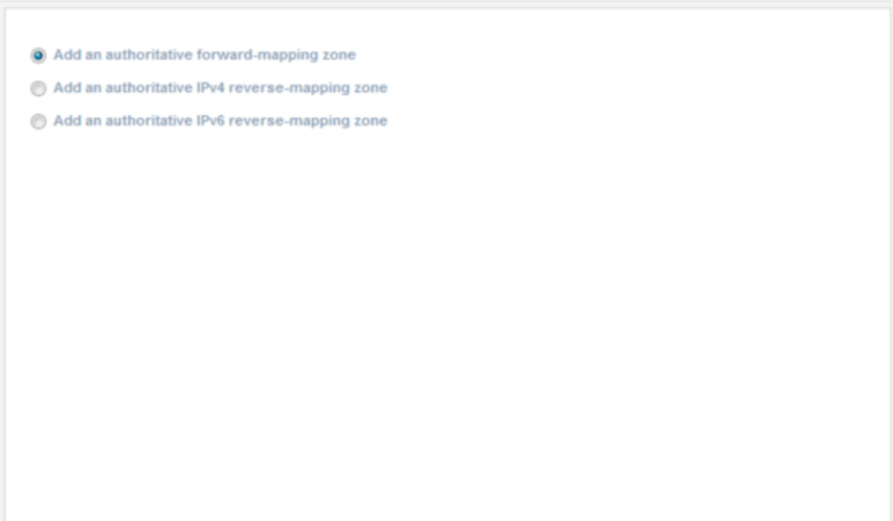
lab10.com Authoritative Zone

Quick Filter None Off Filter On

□	Name ▲	Type	Data		Active Users	Record Source	Principal	Protected	Comment
□		SOA Record	Serial MNAME RNAME Refresh Retry Expire Negative Caching TTL	4 niosgm2.lab10.c please_set_ema 10800 3600 2419200 900	N/A	System			Auto-created by...
□		NS Record	niosgm2.lab10.com		N/A	System			Auto-created by...
□	dhcp	NS Record	niosgm2.lab10.com		N/A	System			Auto-created by...
□	ise201self	A Record	192.168.1.120		0	Static		No	
□	niosgm2	A Record	192.168.1.88		0	System		No	Auto-created by...
□	niosnd2	A Record	192.168.1.89		0	System		No	Auto-created by...

Step 24 Next, create a subzone for dynamic addresses

Step 25 Select **subzone -> "+" -> Authoritative Zone->Add an authoritative forward-mapping zone**



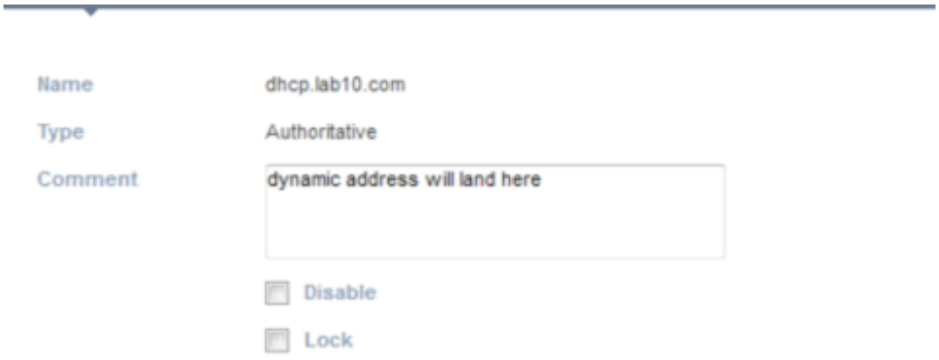
● Add an authoritative forward-mapping zone

○ Add an authoritative IPv4 reverse-mapping zone

○ Add an authoritative IPv6 reverse-mapping zone

Step 26 Select **Next**

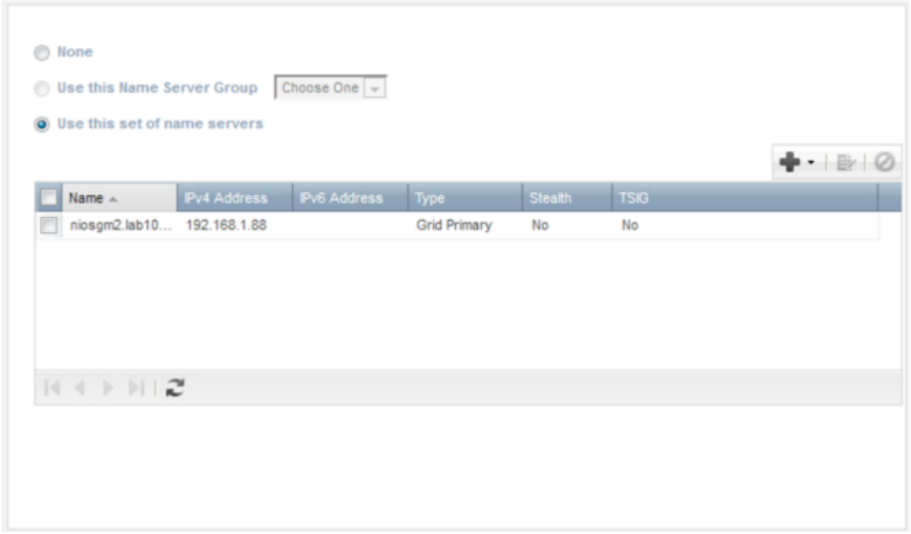
Step 27 Enter name (i.e. **dhcp.lab10.com**) and **dynamic addresses will land here** for comments



Name	dhcp.lab10.com
Type	Authoritative
Comment	dynamic address will land here
	□ Disable
	□ Lock

Step 28 Select **Next**

Step 29 Select **Use this set of name servers**



○ None

○ Use this Name Server Group Choose One

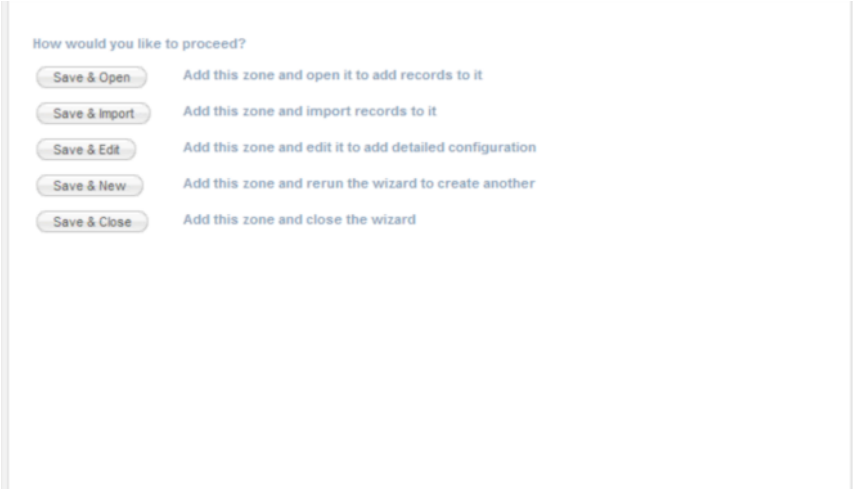
● Use this set of name servers

□	Name	IPv4 Address	IPv6 Address	Type	Stealth	TSIG
□	niosgm2.lab10...	192.168.1.88		Grid Primary	No	No

Step 30 Leave the Extensible attributes blank

Step 31 Select **Next**

Step 32 You should see

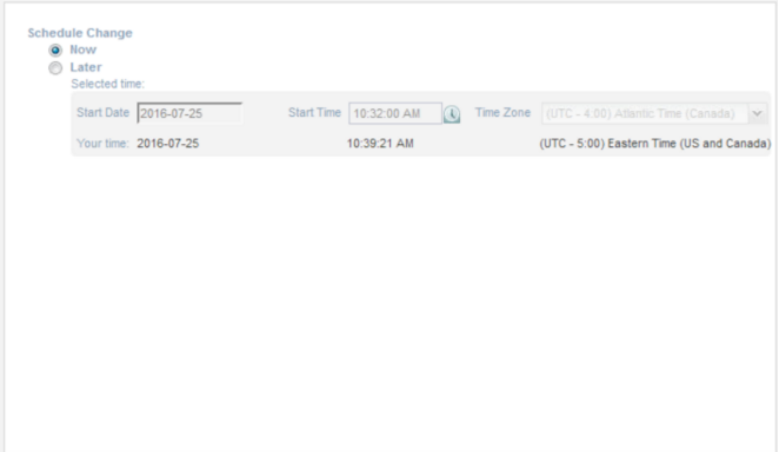


How would you like to proceed?

Save & Open	Add this zone and open it to add records to it
Save & Import	Add this zone and import records to it
Save & Edit	Add this zone and edit it to add detailed configuration
Save & New	Add this zone and rerun the wizard to create another
Save & Close	Add this zone and close the wizard

Step 33 Select **Next**

Step 34 You should see the following



Schedule Change

● Now

○ Later

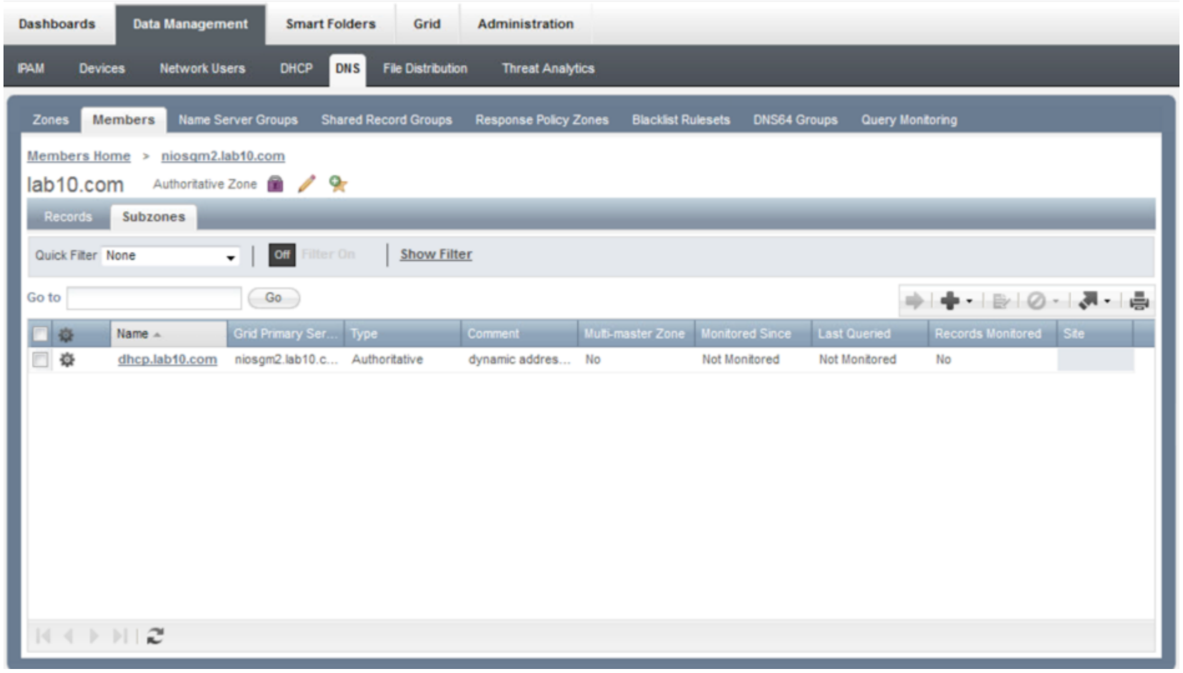
Selected time:

Start Date 2016-07-25 Start Time 10:32:00 AM Time Zone (UTC - 4:00) Atlantic Time (Canada)

Your time: 2016-07-25 10:39:21 AM (UTC - 5:00) Eastern Time (US and Canada)

Step 35 Select **Save and Close**

Step 36 You should see the following

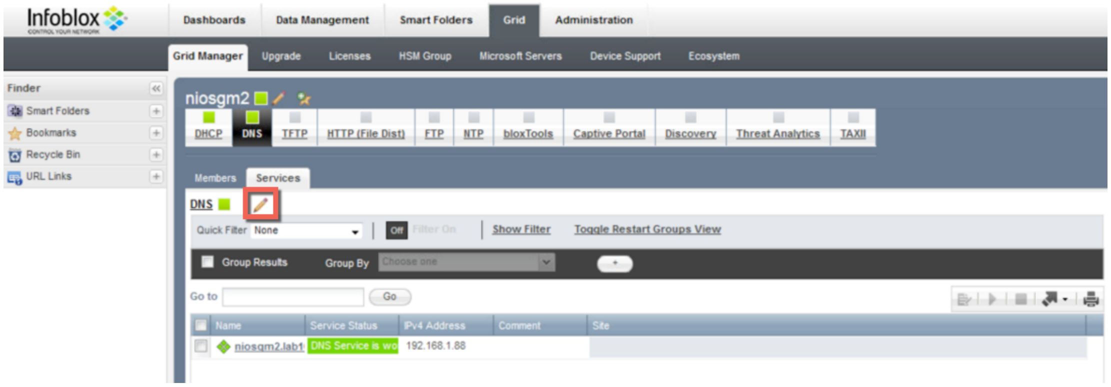


Name	Grid Primary Ser...	Type	Comment	Multi-master Zone	Monitored Since	Last Queried	Records Monitored	Site
dhcp.lab10.com	niosgm2.lab10.c...	Authoritative	dynamic addres...	No	Not Monitored	Not Monitored	No	

Configuring DNS Zone Properties

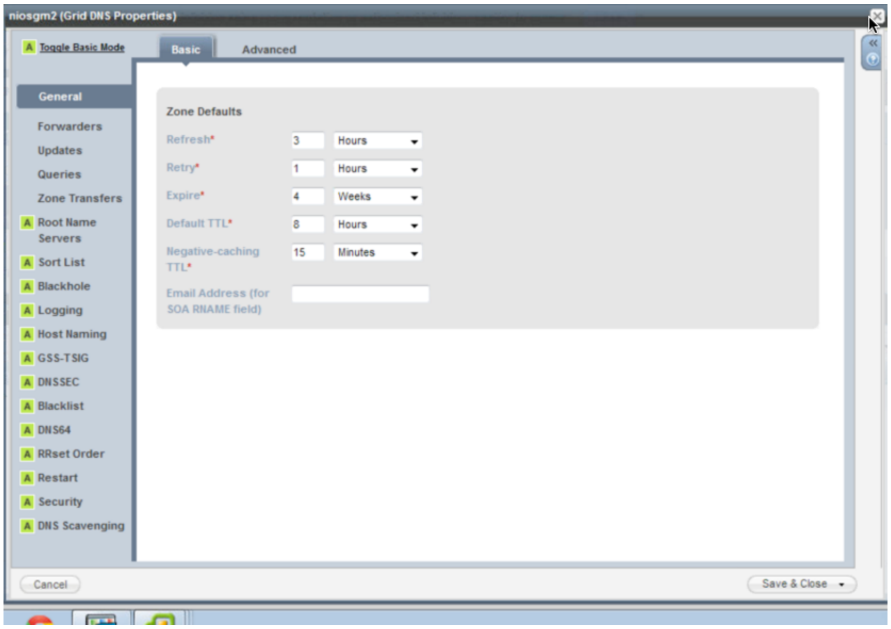
This section steps through DNS Zone properties

Step 1 Select **Grid->Grid Manager->DNS->pencil** (edit DNS properties under Services tab)



Name	Service Status	IPv4 Address	Comment	Site
niosgm2.lab1	DNS Service is wo	192.168.1.88		

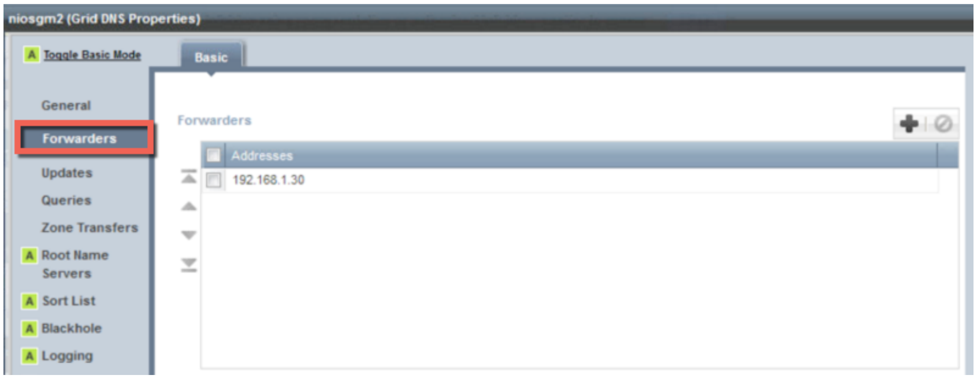
Step 2 You should see the following:



Zone Defaults

Refresh*	3	Hours
Retry*	1	Hours
Expire*	4	Weeks
Default TTL*	8	Hours
Negative-caching TTL*	15	Minutes
Email Address (for SOA RNAME field)		

Step 3 Add a DNS Forwarder if the Infoblox Grid Master should not query root servers or recurs to the internet Select **Forwarders->"+"->add the IP address of the DNS server**

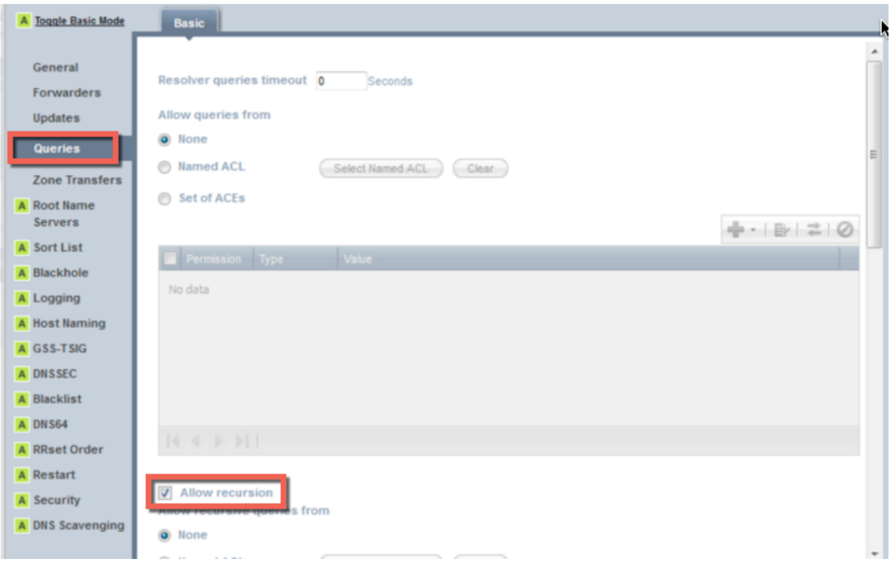


Forwarders

Addresses
192.168.1.30

Step 4 Select **Save and Close**

Step 5 Select **Queries** and **enable Allow recursion**



Resolver queries timeout 0 Seconds

Allow queries from

● None

○ Named ACL

○ Set of ACEs

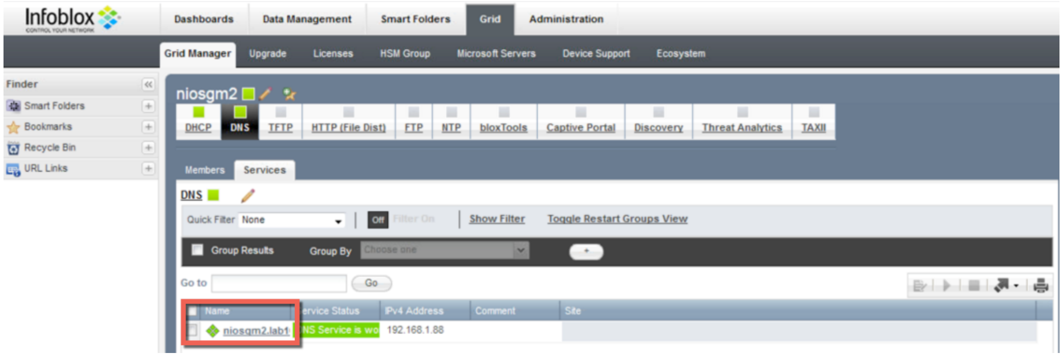
☑ Allow recursion

Allow recursive queries from

● None

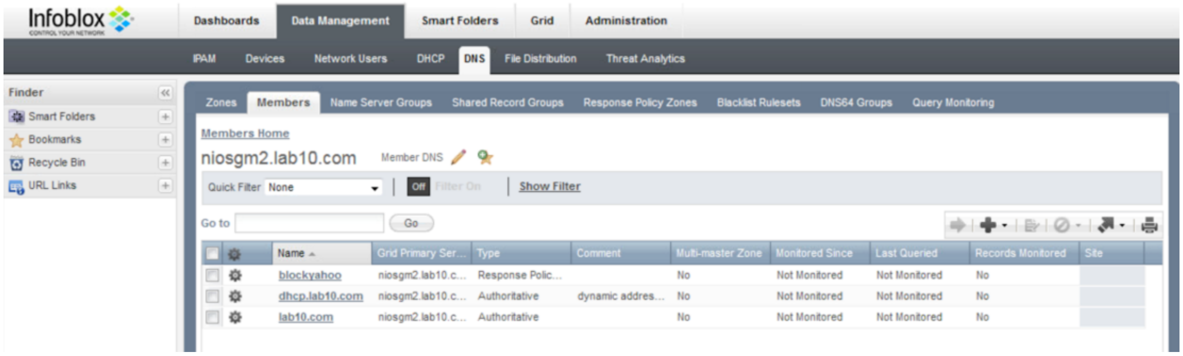
Step 6 Select **Save and Close**

Step 7 Select the Infoblox Grid Master



Name	Service Status	IPv4 Address	Comment	Site
niosgm2.lab1	DNS Service is wo	192.168.1.88		

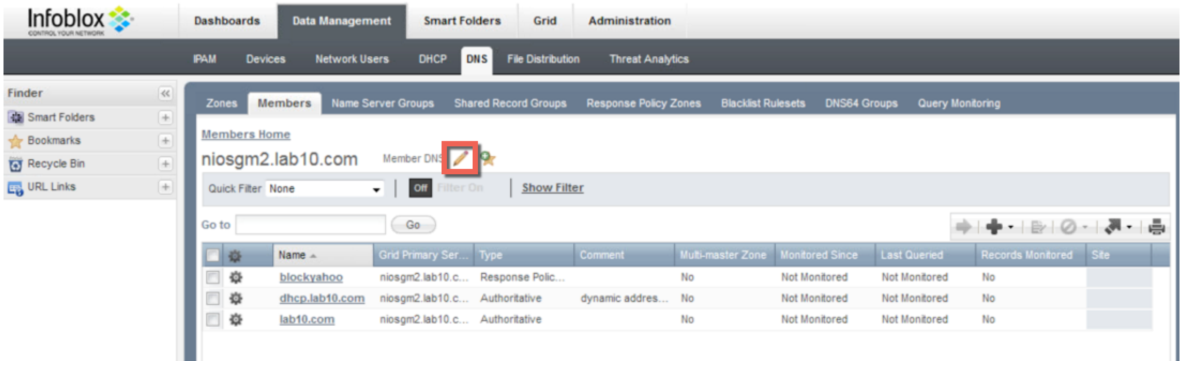
Step 8 You should see the following



niosgm2.lab10.com

Name	Grid Primary Ser...	Type	Comment	Multi-master Zone	Monitored Since	Last Queried	Records Monitored	Site
blockyahoo	niosgm2.lab10.c...	Response Polic...		No	Not Monitored	Not Monitored	No	
dhcp.lab10.com	niosgm2.lab10.c...	Authoritative	dynamic addres...	No	Not Monitored	Not Monitored	No	
lab10.com	niosgm2.lab10.c...	Authoritative		No	Not Monitored	Not Monitored	No	

Step 9 Select the **pencil** (edit properties)

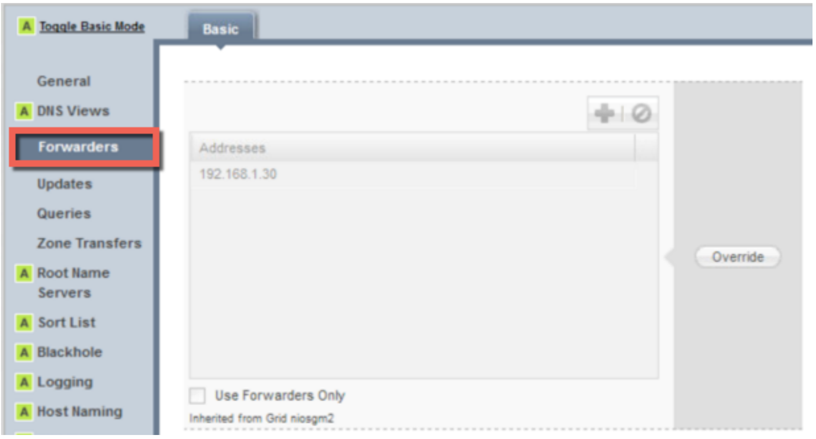


niosgm2.lab10.com

Quick Filter: None | Off

Name	Grid Primary Ser...	Type	Comment	Multi-master Zone	Monitored Since	Last Queried	Records Monitored	Site
blockyahoo	niosgm2.lab10.c...	Response Polic...		No	Not Monitored	Not Monitored	No	
dhcp.lab10.com	niosgm2.lab10.c...	Authoritative	dynamic addres...	No	Not Monitored	Not Monitored	No	
lab10.com	niosgm2.lab10.c...	Authoritative		No	Not Monitored	Not Monitored	No	

Step 10 Verify that you have your DNS forwarder IP Address



Addresses

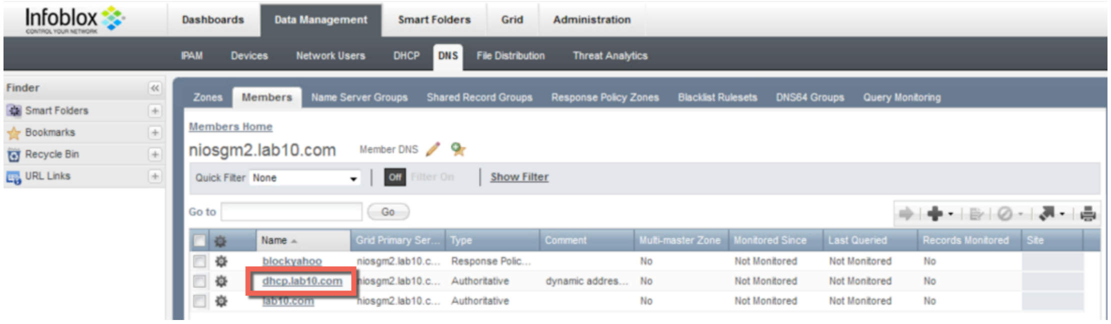
192.168.1.30

□ Use Forwarders Only

Inherited from Grid niosgm2

Step 11 Select **Save** and **Close**

Step 12 Select **dhcp.lab10.com DNS** zone

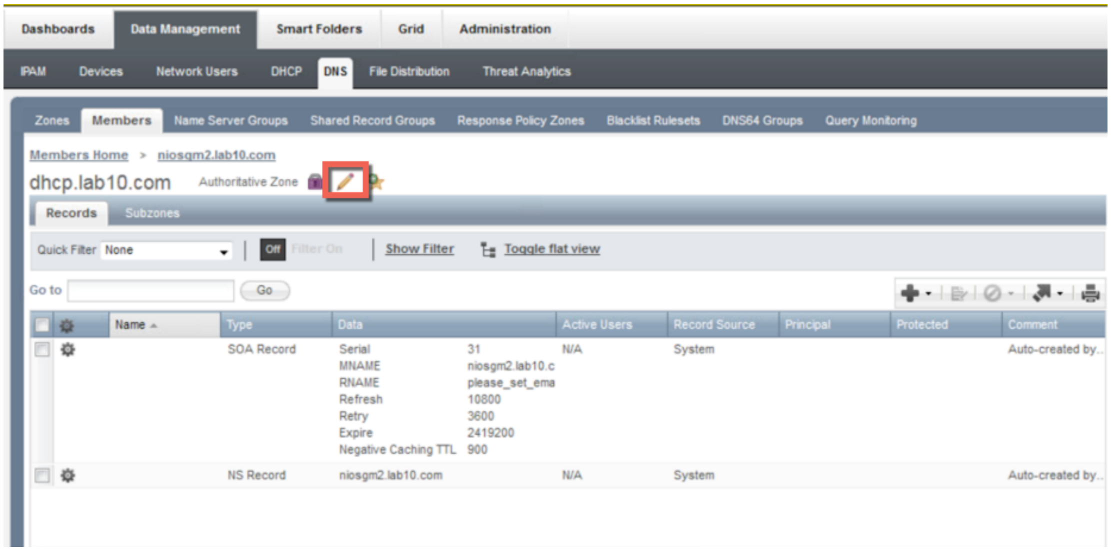


niosgm2.lab10.com

Quick Filter: None | Off

Name	Grid Primary Ser...	Type	Comment	Multi-master Zone	Monitored Since	Last Queried	Records Monitored	Site
blockyahoo	niosgm2.lab10.c...	Response Polic...		No	Not Monitored	Not Monitored	No	
dhcp.lab10.com	niosgm2.lab10.c...	Authoritative	dynamic addres...	No	Not Monitored	Not Monitored	No	
lab10.com	niosgm2.lab10.c...	Authoritative		No	Not Monitored	Not Monitored	No	

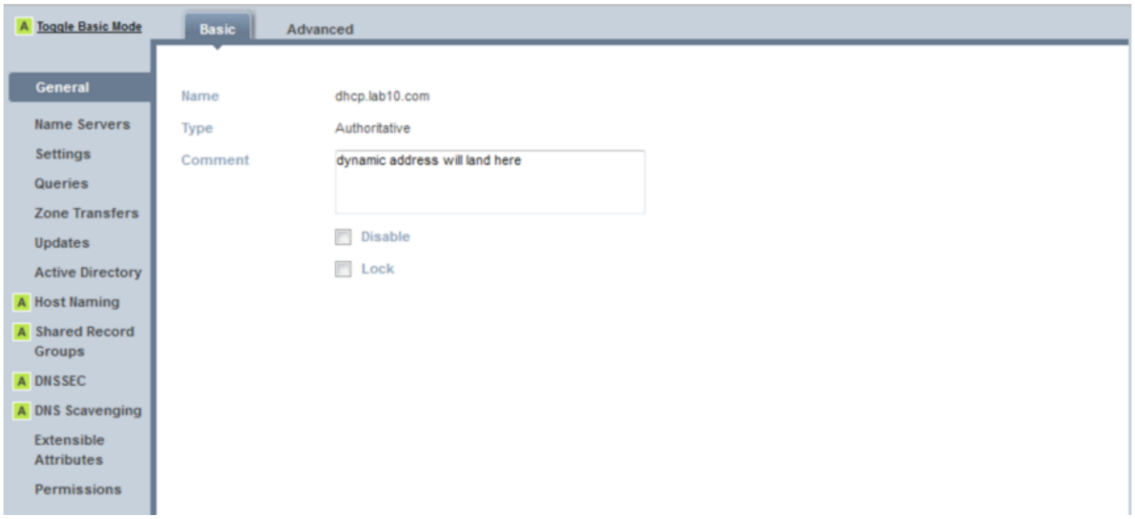
Step 13 Select the **pencil** (edit properties)



dhcp.lab10.com Authoritative Zone

Name	Type	Data		Active Users	Record Source	Principal	Protected	Comment
	SOA Record	Serial MNAME RNAME Refresh Retry Expire Negative Caching TTL	31 niosgm2.lab10.c please_set_ema 10800 3600 2419200 900	N/A	System			Auto-created by...
	NS Record	niosgm2.lab10.com		N/A	System			Auto-created by...

Step 14 You should see the following:



Name dhcp.lab10.com

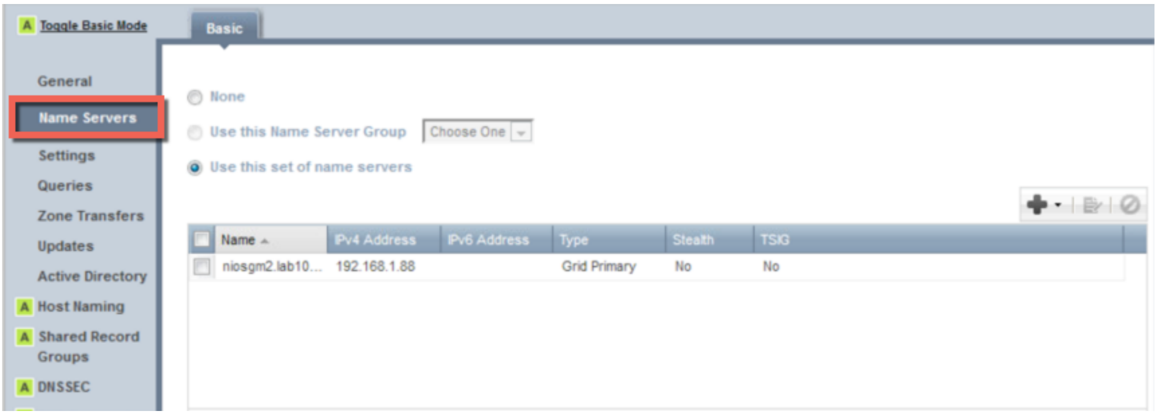
Type Authoritative

Comment dynamic address will land here

□ Disable

□ Lock

Step 15 Select **Name Servers** and verify that you see the Infoblox GM as the name server



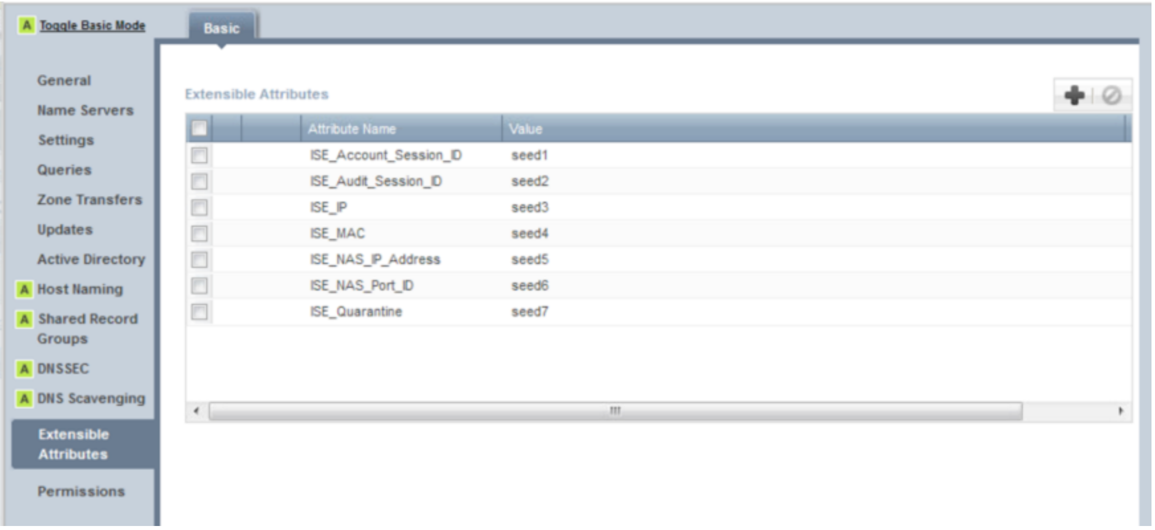
○ None

○ Use this Name Server Group Choose One

● Use this set of name servers

Name	IPv4 Address	IPv6 Address	Type	Stealth	TSIG
niosgm2.lab10...	192.168.1.88		Grid Primary	No	No

Step 16 Select -> **Extensible Attributes -> "+"** add the following under **attribute name** and **value:**



Extensible Attributes

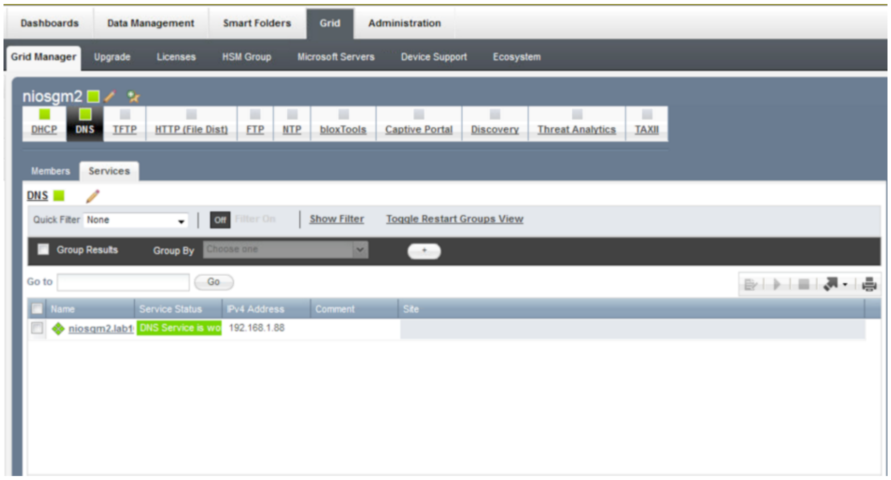
Attribute Name	Value
ISE_Account_Session_ID	seed1
ISE_Audit_Session_ID	seed2
ISE_IP	seed3
ISE_MAC	seed4
ISE_NAS_IP_Address	seed5
ISE_NAS_Port_ID	seed6
ISE_Quarantine	seed7

Step 17 Select **Save and Close**

Add Policy Response Zone

This section steps through adding the Policy Response Zone for blocking www.yahoo.com

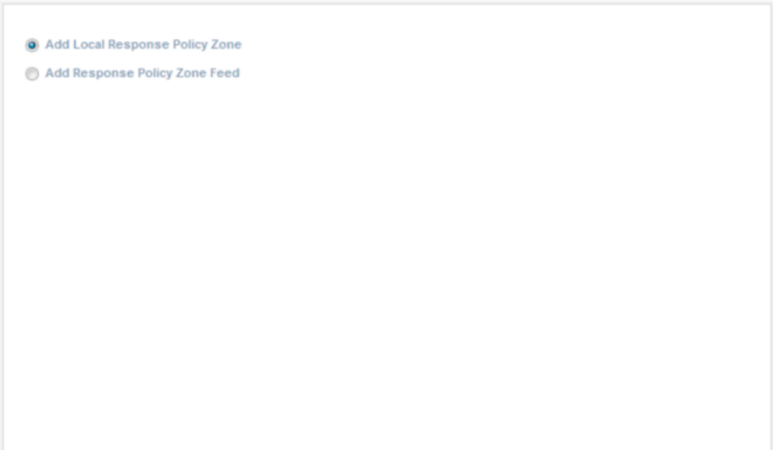
Step 1 Select **Grid->Grid Manager->DNS**
Step 2 You should see the infoblox Grid Master



Quick Filter: None

Name	Service Status	IPv4 Address	Comment	Site
niosgm2.labt	DNS Service is wo	192.168.1.88		

Step 3 Select the **Infoblox Grid Master->"+"-> Response Zone Policy->Add a Local Response Policy**

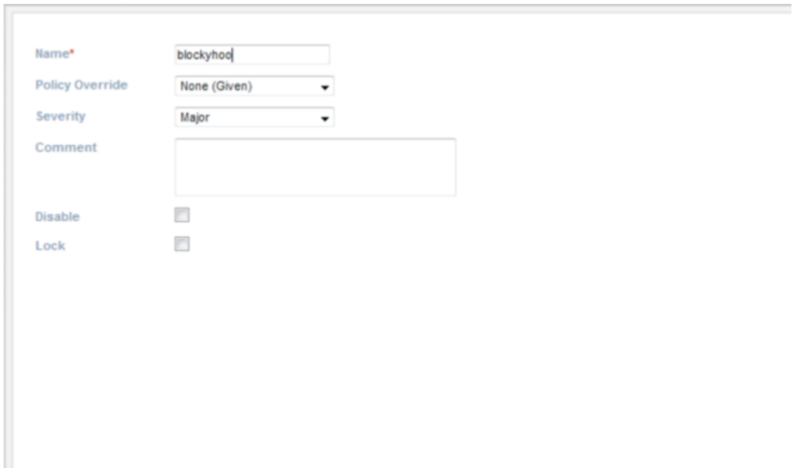


● Add Local Response Policy Zone

○ Add Response Policy Zone Feed

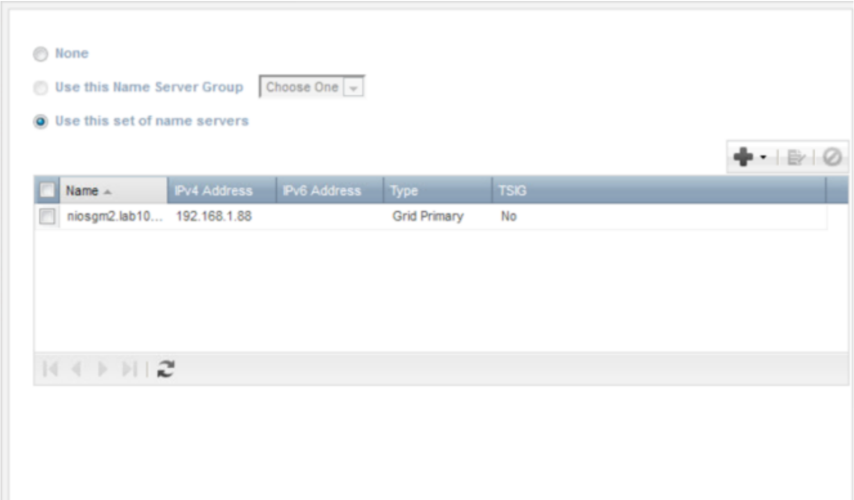
Step 4 Select **Next**

Step 5 Add the name **blockyahoo**



Name*	blockyhoo
Policy Override	None (Given)
Severity	Major
Comment	
Disable	□
Lock	□

Step 6 Verify that you have the Infoblox Grid Master for the named server



○ None

○ Use this Name Server Group Choose One

● Use this set of name servers

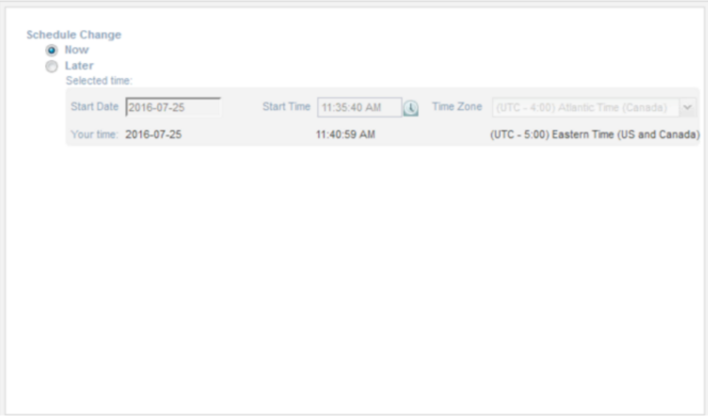
□	Name	IPv4 Address	IPv6 Address	Type	TSIG
□	niosgm2.lab10...	192.168.1.88		Grid Primary	No

Step 7 Select **Next**

Step 8 Leave extensible attributes blank

Step 9 Select **Next**

Step 10 Select **Schedule Change now**



Schedule Change

● Now
○ Later

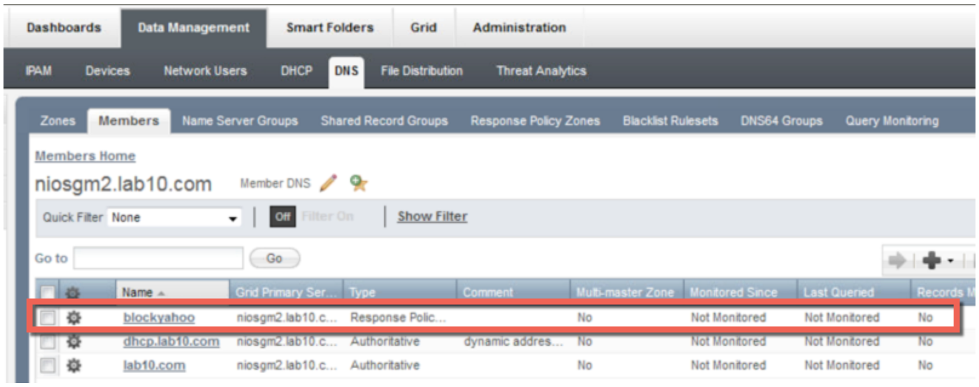
Selected time:

Start Date 2016-07-25 Start Time 11:35:40 AM Time Zone (UTC - 4:00) Atlantic Time (Canada)

Your time: 2016-07-25 11:40:59 AM (UTC - 5:00) Eastern Time (US and Canada)

Step 11 Select **Save and Close**

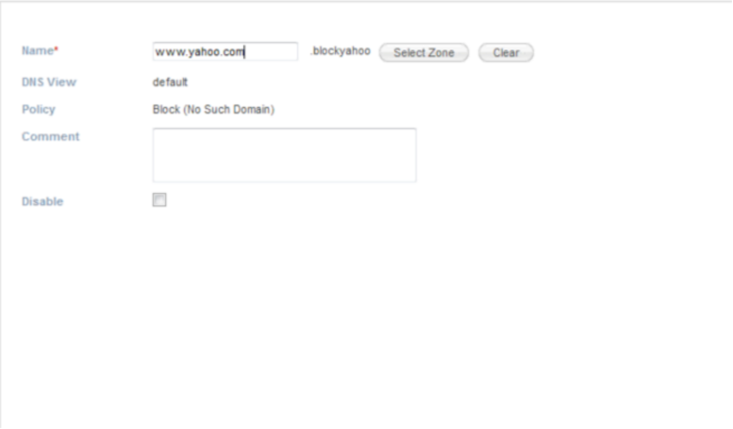
Step 12 You should see the blockyahoo Response Policy Zone



niosgm2.lab10.com

Name	Grid Primary Ser...	Type	Comment	Multi-master Zone	Monitored Since	Last Queried	Records M
blockyahoo	niosgm2.lab10.c...	Response Polic...		No	Not Monitored	Not Monitored	No
dhcp.lab10.com	niosgm2.lab10.c...	Authoritative	dynamic addres...	No	Not Monitored	Not Monitored	No
lab10.com	niosgm2.lab10.c...	Authoritative		No	Not Monitored	Not Monitored	No

Step 13 Select **blockyahoo -> "+"-> Block (no such domain rule)->Block Domain (no such domain rule)** and enter www.yahoo.com for name



Name* www.yahoo.com .blockyahoo

DNS View default

Policy Block (No Such Domain)

Comment

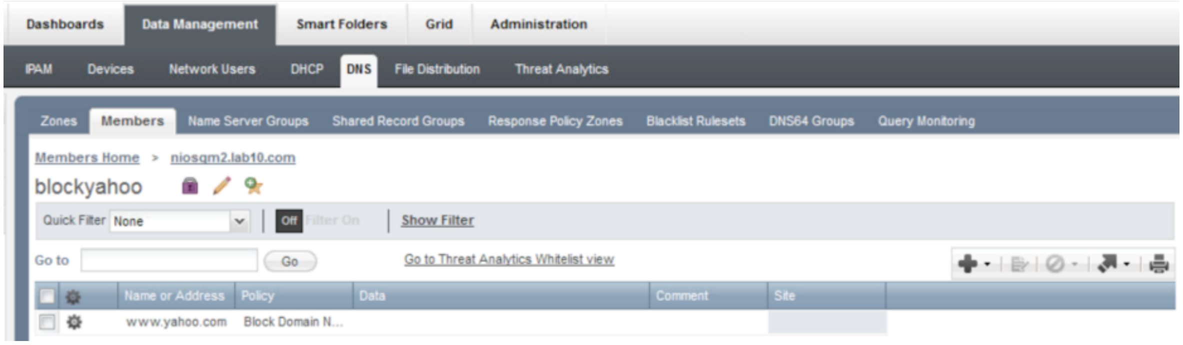
Disable □

Step 14 Select **Next**

Step 15 Leave Extensible attributes blank, select **Next**

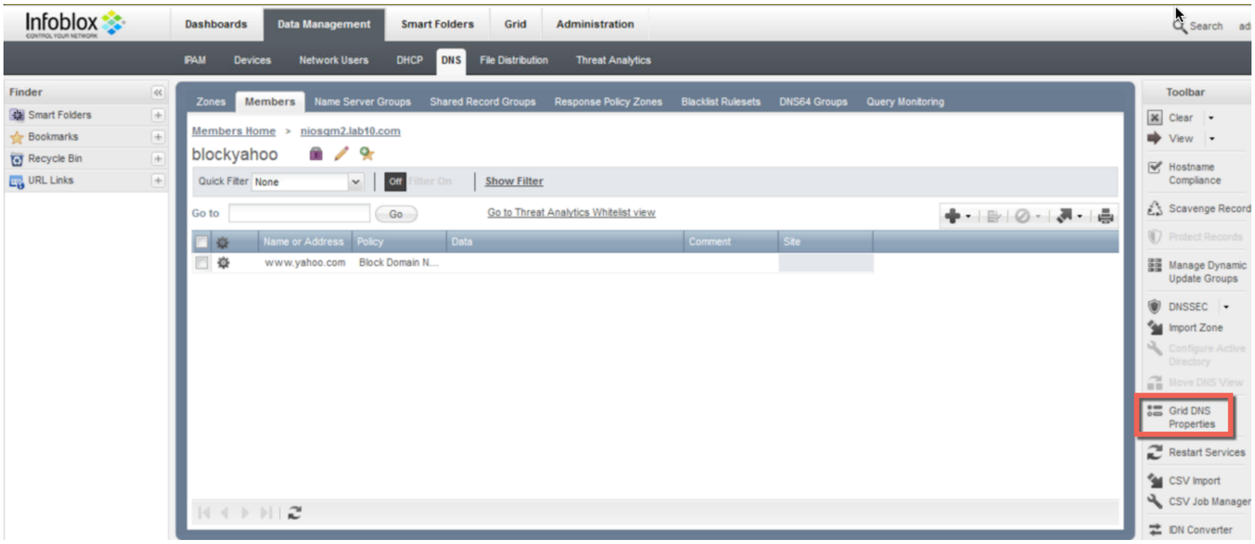
Step 16 Select Schedule Change Now, select **Save and Close**

Step 17 You should see the www.yahoo.com blocked domain rule



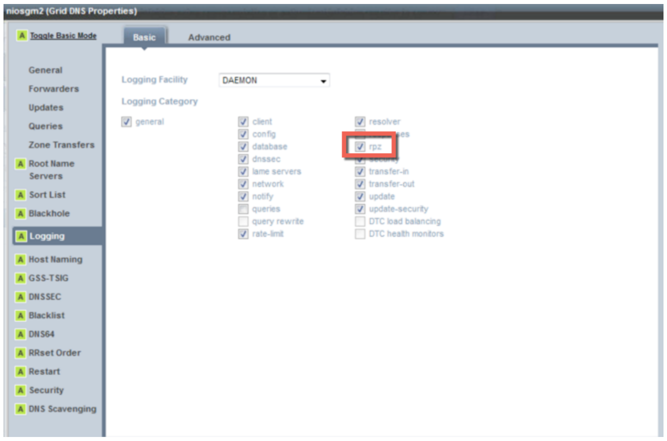
Name or Address	Policy	Data	Comment	Site
www.yahoo.com	Block Domain N...			

Step 18 Select **Grid DNS Properties**



Name or Address	Policy	Data	Comment	Site
www.yahoo.com	Block Domain N...			

Step 19 Select **Logging->Enable rpz**



Logging Facility: DAEMON

Logging Category

☑ general

☑ client
☑ config
☑ database
☑ dnssec
☑ lame servers
☑ network
☑ notify
☐ queries
☐ query rewrite
☑ rate-limit

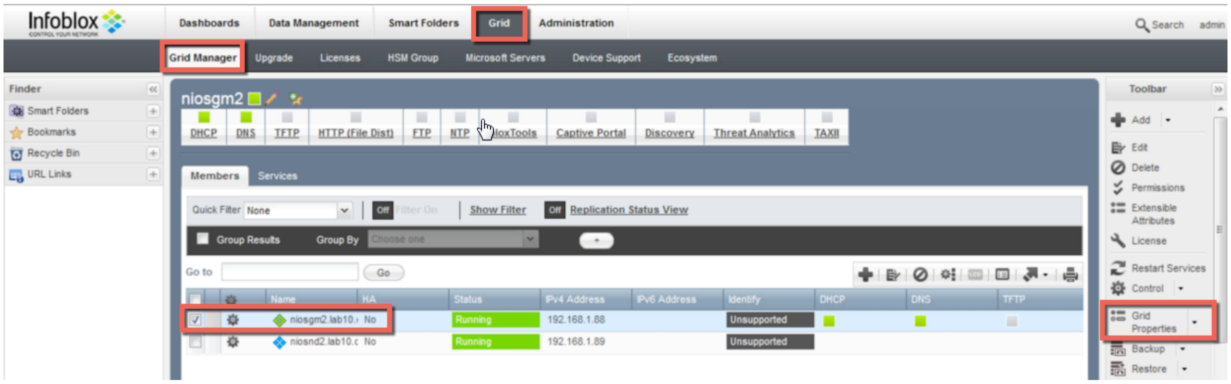
☑ resolver
☐ ...es
☑ rpz
☑ security
☑ transfer-in
☑ transfer-out
☑ update
☑ update-security
☐ DTC load balancing
☐ DTC health monitors

Step 20 Select **Save and Close**

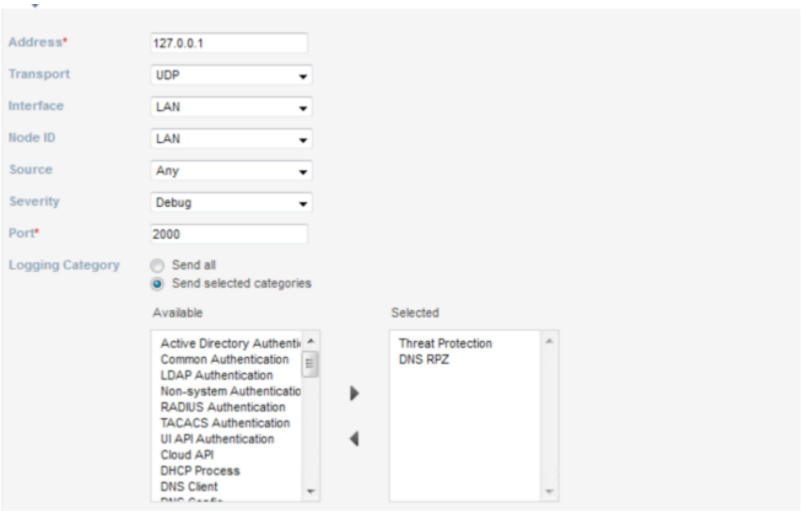
Specifying Syslog Server for Notifications

You must configure the syslog server to which the appliance logs RPZ and threat protection events. This is required for publishing RPZ and threat protection notifications to the Cisco ISE pxGrid node. The appliance generates notifications about these events and analyzes the data before sending it to the Cisco ISE pxGrid node. When setting up the syslog server, ensure you select DNS RPZ and Threat Protection logging categories so all events related to RPZ and threat protection hits are logged to the syslog.

Step 1 Select **Grid-> Grid Manager-> infoblox Grid Master (i.e. niosgm2.lab10.com)->Grid Properties**



Step 2 Select **Monitoring->"+" (add) the following**:



Address*	127.0.0.1
Transport	UDP
Interface	LAN
Node ID	LAN
Source	Any
Severity	Debug
Port*	2000
Logging Category	○ Send all ● Send selected categories

Available:

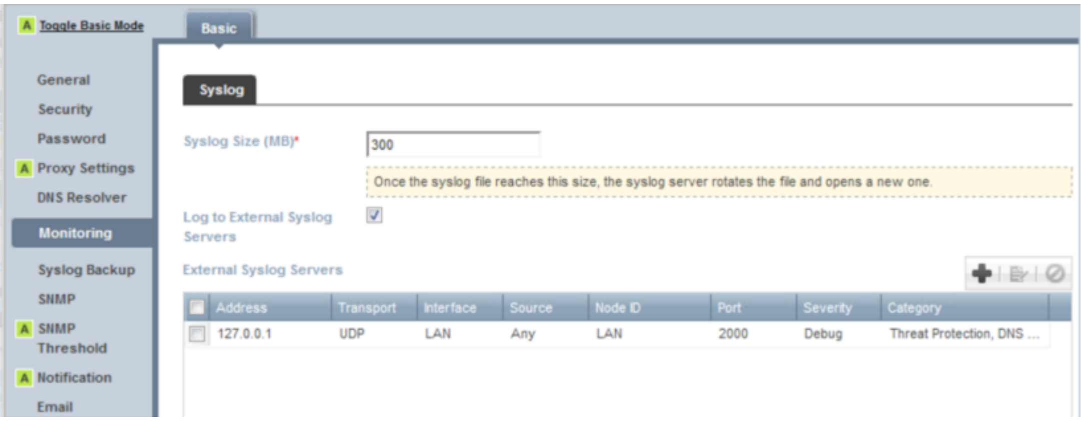
Active Directory Authenti
Common Authentication
LDAP Authentication
Non-system Authenticatio
RADIUS Authentication
TACACS Authentication
UI API Authentication
Cloud API
DHCP Process
DNS Client

Selected:

Threat Protection
DNS RPZ

Step 3 Select **Add**

Step 4 You should see the following:



Syslog Size (MB)* 300

Once the syslog file reaches this size, the syslog server rotates the file and opens a new one.

Log to External Syslog Servers ☑

External Syslog Servers

Address	Transport	Interface	Source	Node ID	Port	Severity	Category
127.0.0.1	UDP	LAN	Any	LAN	2000	Debug	Threat Protection, DNS ...

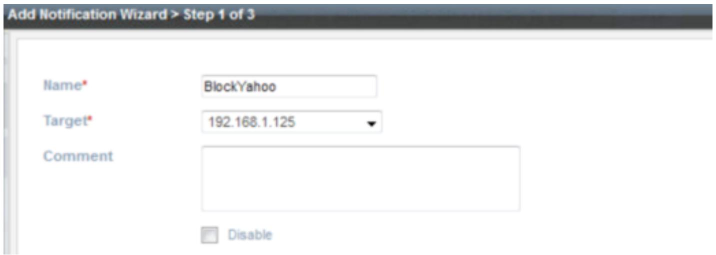
Step 5 Select **Save and Close**

Step 6 Select Restart, the configuration will require a restart.

Adding RPZ Notification

Configure RPZ Notification rules for ISE to quarantine the endpoint based on the RPZ rule violation.

Step 1 Select **Grid->Ecosystem>Notification->"+" (add),** name of the RPZ rule notification, IP address of the ISE pxGrid node


Add Notification Wizard > Step 1 of 3

Name* BlockYahoo

Target* 192.168.1.125

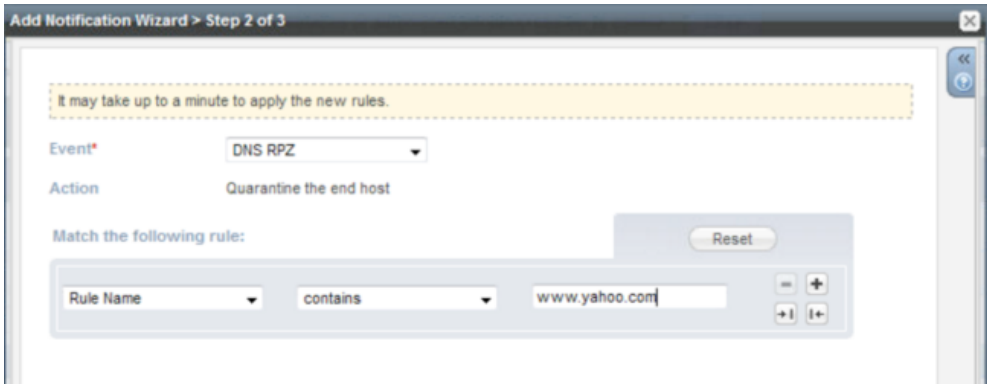
Comment

□ Disable

Step 2 Select **Next**

Step 3 Select **DNS Event** from the drop-down menu

Step 4 Select **Rule Name->Contains->www.yahoo.com**


Add Notification Wizard > Step 2 of 3

It may take up to a minute to apply the new rules.

Event* DNS RPZ

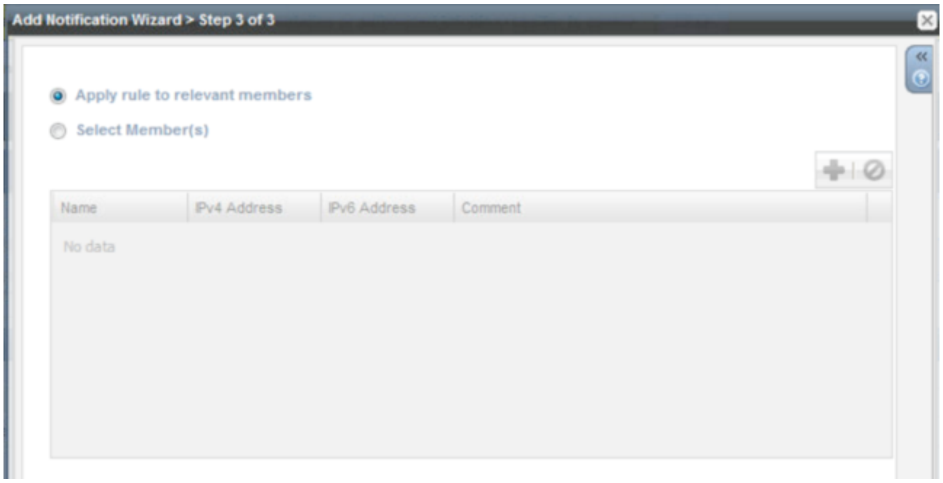
Action Quarantine the end host

Match the following rule:

Rule Name | contains | www.yahoo.com

Step 5 Select **Next**

Step 6 You should see the following:



Add Notification Wizard > Step 3 of 3

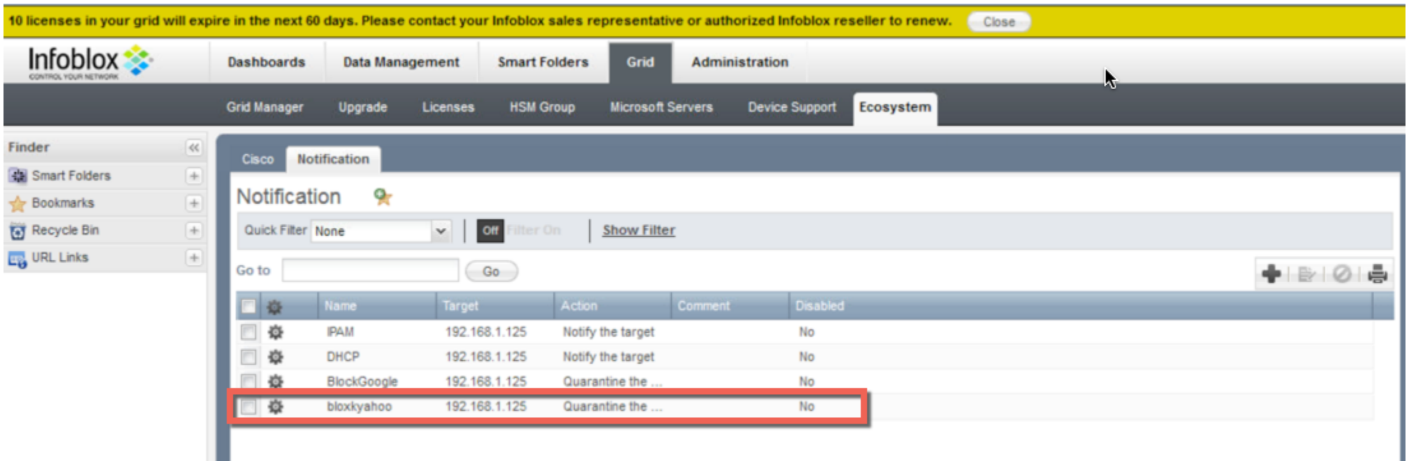
● Apply rule to relevant members

○ Select Member(s)

Name	IPv4 Address	IPv6 Address	Comment
No data			

Step 7 Select **Save and Close**

Step 8 You should see the following:



10 licenses in your grid will expire in the next 60 days. Please contact your Infoblox sales representative or authorized Infoblox reseller to renew. Close

Notification

Quick Filter None | Off Filter On | Show Filter

Go to Go

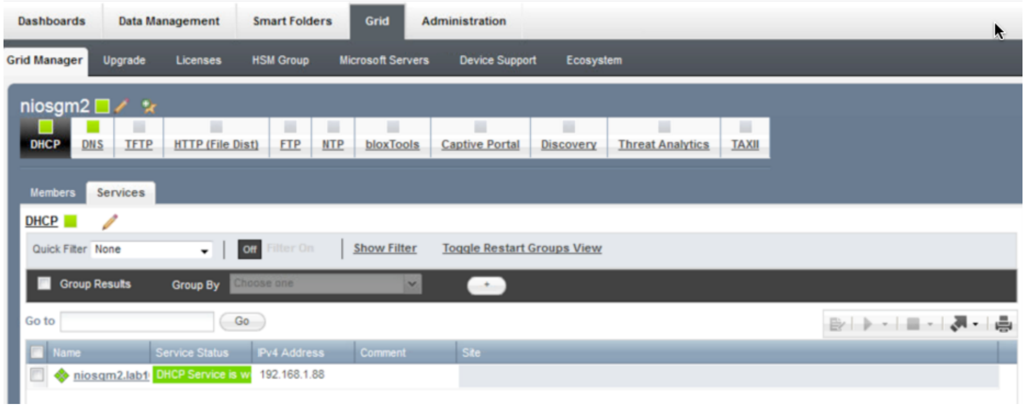
		Name	Target	Action	Comment	Disabled
□	⚙	IPAM	192.168.1.125	Notify the target		No
□	⚙	DHCP	192.168.1.125	Notify the target		No
□	⚙	BlockGoogle	192.168.1.125	Quarantine the ...		No
□	⚙	bloxkyahoo	192.168.1.125	Quarantine the ...		No

Configuring DHCP Services

This section steps through configuring DHCP Services and creating a range of networks.

Step 1 Select **Grid->Grid Manager->Members->**select the Infoblox Grid Master->**DHCP** and **Start** from the Toolbar

Step 2 You should see that the DHCP service have started



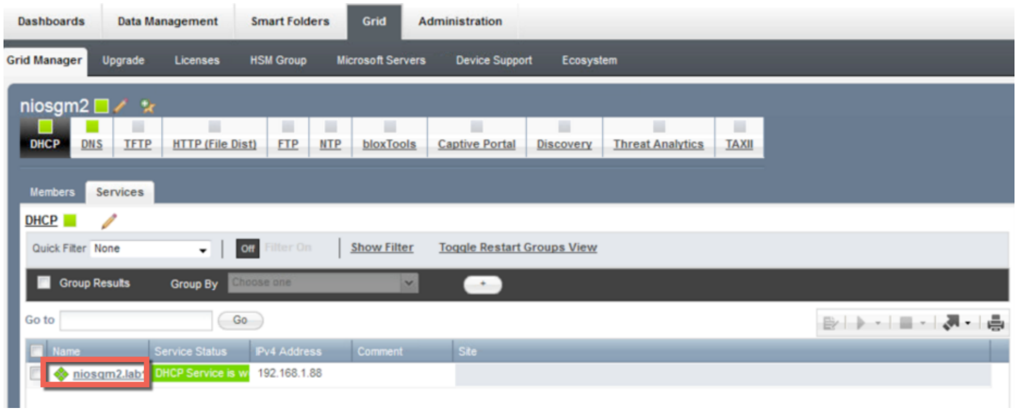
Name	Service Status	IPv4 Address	Comment	Site
niosgm2.lab1.	DHCP Service is w	192.168.1.88		

Step 3 You should see that the DHCP service have started

Configuring DHCP

This sections steps through creating a range of network for DHCP.

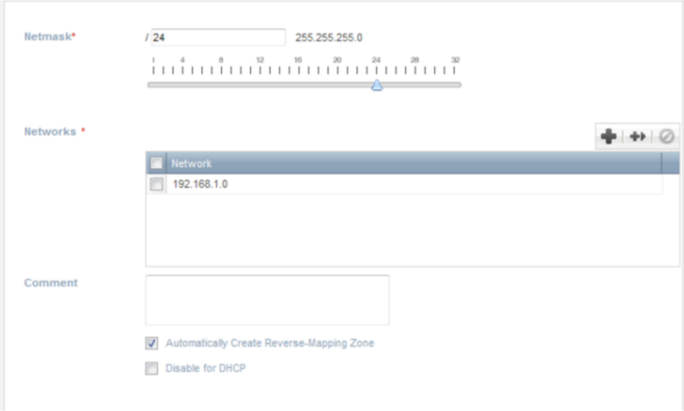
Step 1 Select the Infoblox Grid Master



Name	Service Status	IPv4 Address	Comment	Site
niosgm2.lab	DHCP Service is w	192.168.1.88		

Step 2 Select **"+" ->IPV4 network->Add Network->next**

Step 3 Enter **Networks** and **enable Automatically create Reverse-Mapping Zones**



Netmask* / 24 255.255.255.0

Networks *

□	Network
□	192.168.1.0

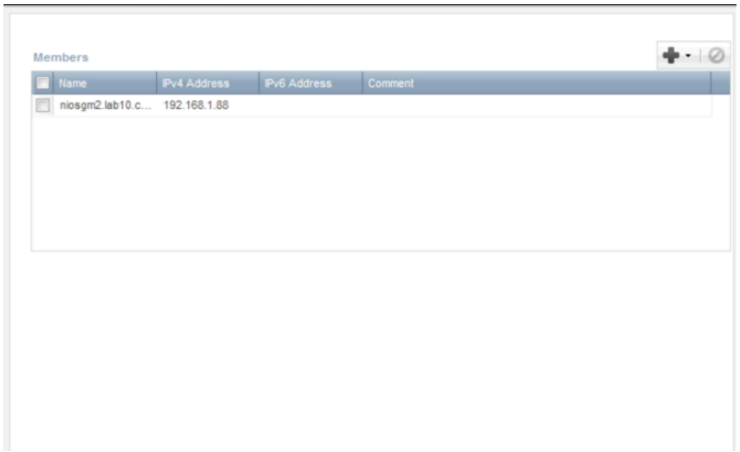
Comment

☑ Automatically Create Reverse-Mapping Zone

□ Disable for DHCP

Step 4 Select **Next**

Step 5 Verify you see the Infoblox Grid Master as a member

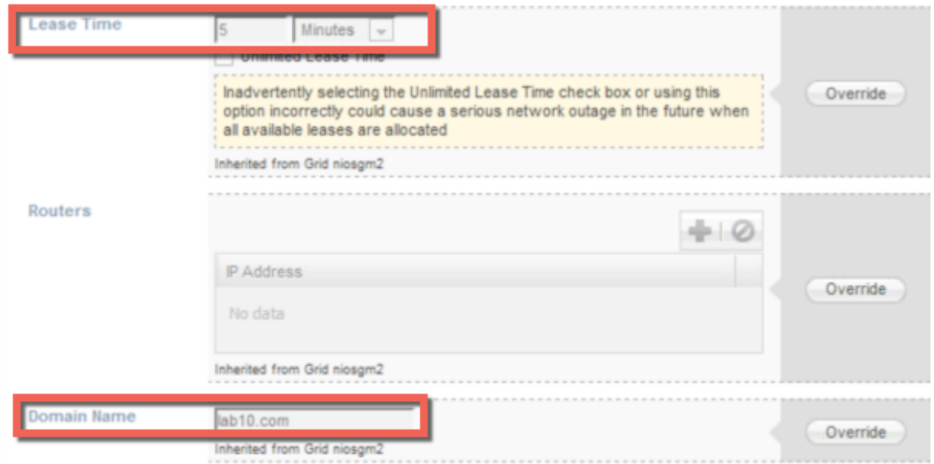


Members

□	Name	IPv4 Address	IPv6 Address	Comment
□	niosgm2.lab10.c...	192.168.1.88		

Step 6 Select **Next**

Step 7 Select **Override** and change the Lease time to 5 minutes and add the domain name



Lease Time 5 Minutes

□ Unlimited Lease Time

Inadvertently selecting the Unlimited Lease Time check box or using this option incorrectly could cause a serious network outage in the future when all available leases are allocated

Inherited from Grid niosgm2

Routers

IP Address
No data

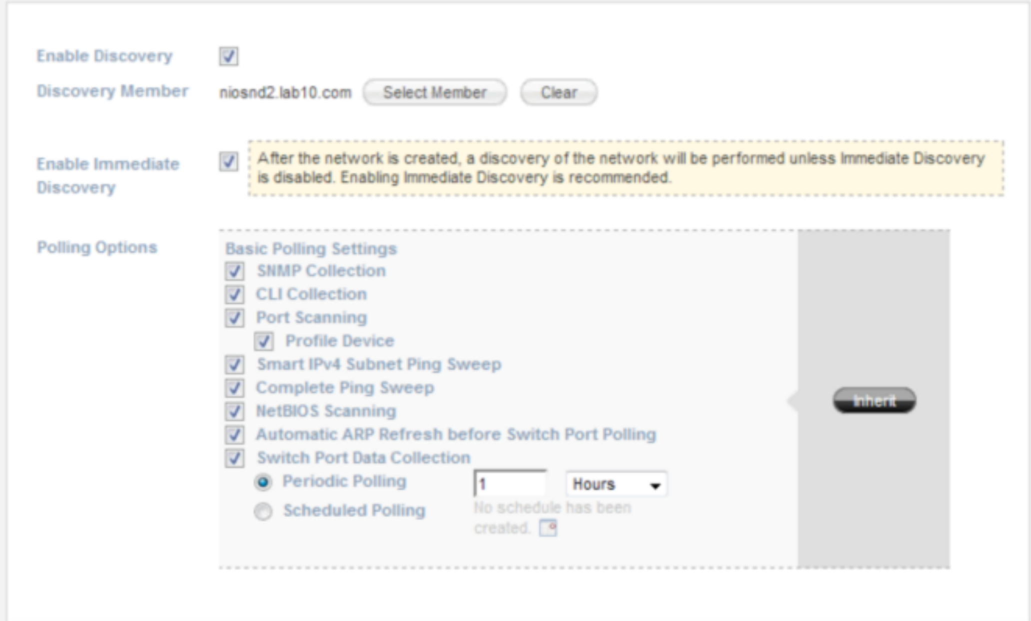
Inherited from Grid niosgm2

Domain Name lab10.com

Inherited from Grid niosgm2

Step 8 Select **Next**

Step 9 Enable **Discovery, select Member, Override** and select the following:



Enable Discovery ☑

Discovery Member niosnd2.lab10.com

Enable Immediate Discovery ☑ After the network is created, a discovery of the network will be performed unless Immediate Discovery is disabled. Enabling Immediate Discovery is recommended.

Polling Options

Basic Polling Settings

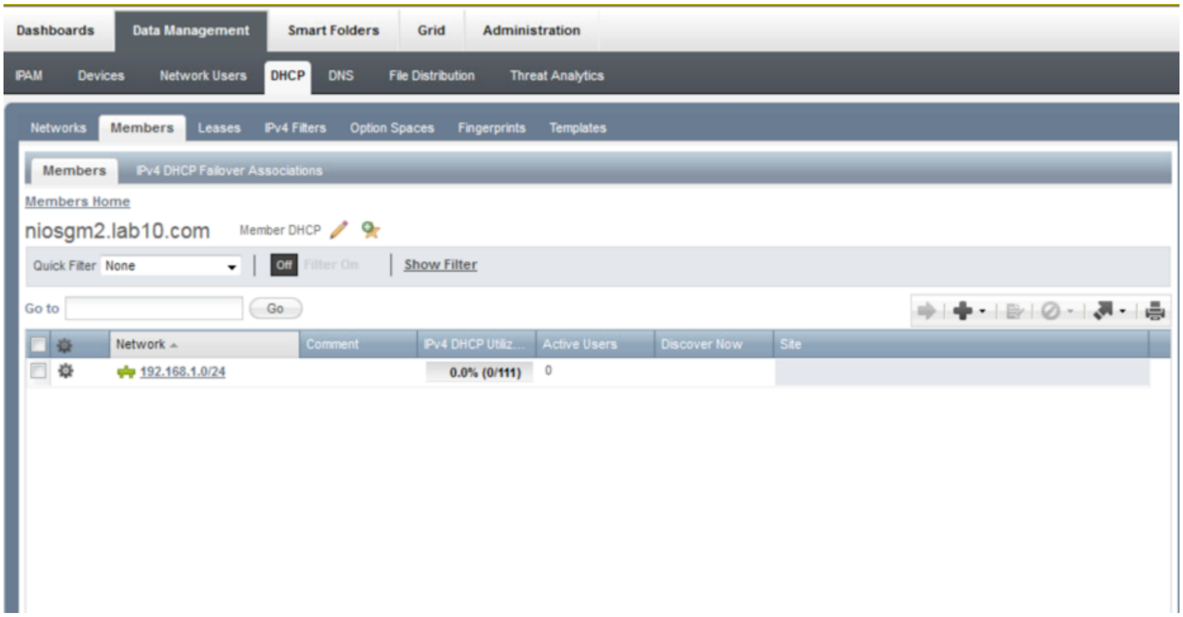
- ☑ SNMP Collection
- ☑ CLI Collection
- ☑ Port Scanning
  - ☑ Profile Device
- ☑ Smart IPv4 Subnet Ping Sweep
- ☑ Complete Ping Sweep
- ☑ NetBIOS Scanning
- ☑ Automatic ARP Refresh before Switch Port Polling
- ☑ Switch Port Data Collection
- ● Periodic Polling 1 Hours
- ○ Scheduled Polling No schedule has been created.

Step 10 Select **Next**

Step 11 Leave the Extensible attributes blank, select Next

Step 12 Schedule Ipv4 network now->**Save and Close**

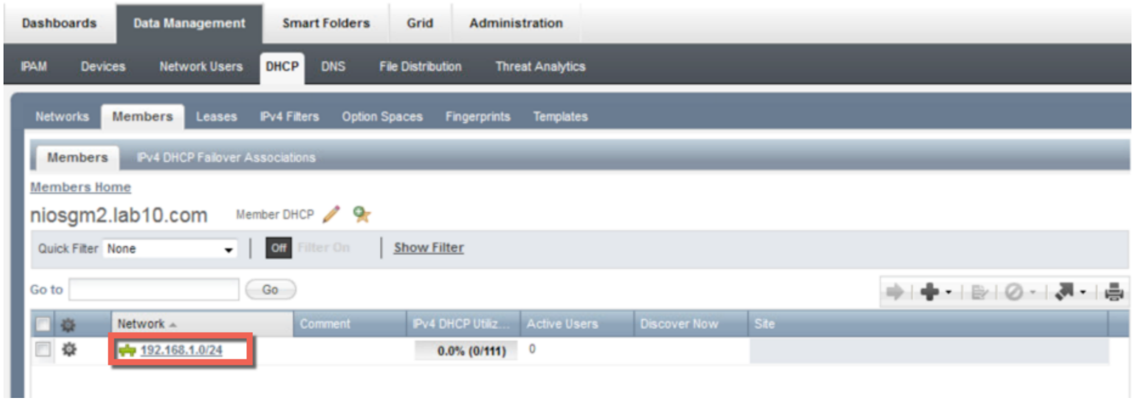
Step 13 You should see the following:



niosgm2.lab10.com Member DHCP

Network	Comment	IPv4 DHCP Utiliz...	Active Users	Discover Now	Site
192.168.1.0/24		0.0% (0/111)	0		

Step 14 Select the network:



niosgm2.lab10.com Member DHCP

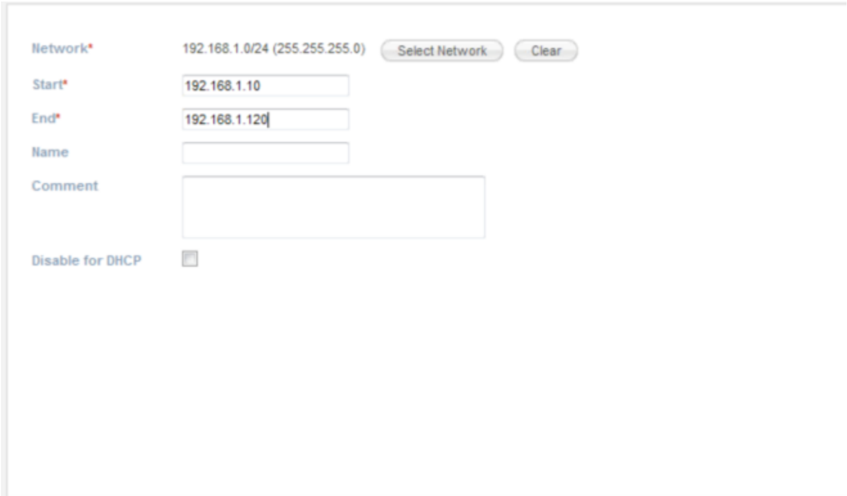
Quick Filter None

Network	Comment	IPv4 DHCP Utiliz...	Active Users	Discover Now	Site
192.168.1.0/24		0.0% (0/111)	0		

Step 15 Select "+" -> **Add Range**

Step 16 Select **Next**

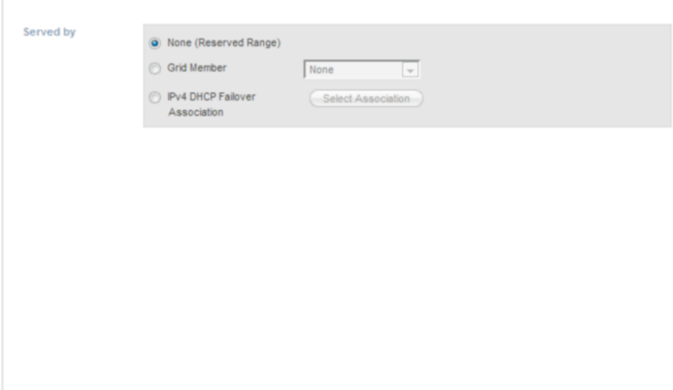
Step 17 Enter the Start and Stop IP addresses



Network*	192.168.1.0/24 (255.255.255.0)
Start*	192.168.1.10
End*	192.168.1.120
Name	
Comment	
Disable for DHCP	□

Step 18 Select **Next**

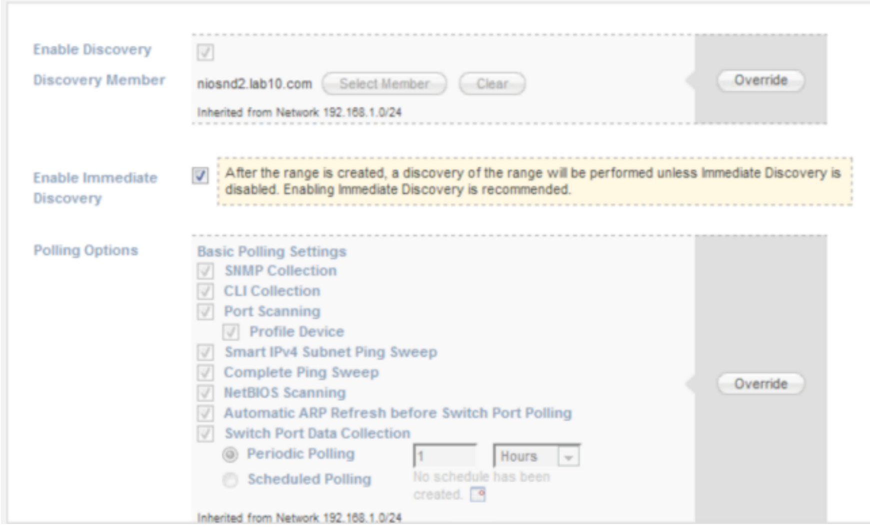
Step 19 Leave the defaults



Served by
● None (Reserved Range)
○ Grid Member None
○ IPv4 DHCP Failover Association

Step 20 Select **Next**

Step 21 Verify the discovery is enabled and you have the following parameters and the Infoblox Grid Master



Enable Discovery ☑

Discovery Member: niosnd2.lab10.com

Inherited from Network 192.168.1.0/24

Enable Immediate Discovery ☑ After the range is created, a discovery of the range will be performed unless Immediate Discovery is disabled. Enabling Immediate Discovery is recommended.

Polling Options

Basic Polling Settings
- ☑ SNMP Collection
- ☑ CLI Collection
- ☑ Port Scanning
  - ☑ Profile Device
- ☑ Smart IPv4 Subnet Ping Sweep
- ☑ Complete Ping Sweep
- ☑ NetBIOS Scanning
- ☑ Automatic ARP Refresh before Switch Port Polling
- ☑ Switch Port Data Collection
- ● Periodic Polling 1 Hours
- ○ Scheduled Polling No schedule has been created.

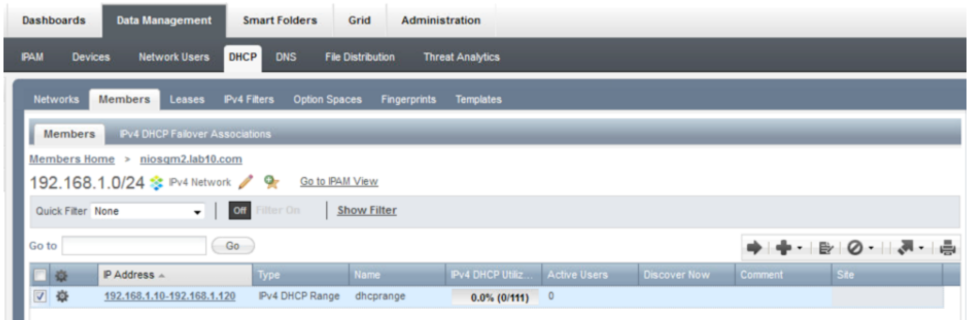
Inherited from Network 192.168.1.0/24

Step 22 Select **Next**

Step 23 Leave Extensible attributes BLANK, select **next**

Step 24 Schedule change now, select **Save and close**

Step 25 You should see the following:



Members Home > niosgm2.lab10.com

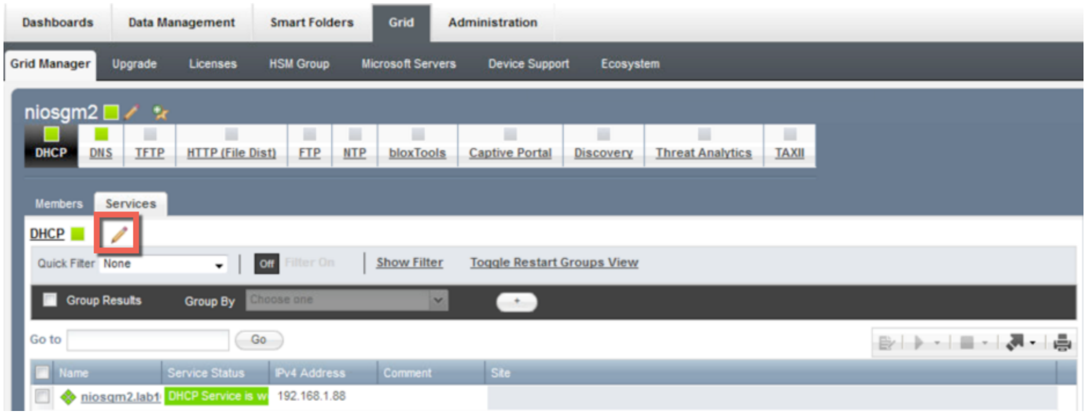
192.168.1.0/24 IPv4 Network

Quick Filter None | Off Filter On | Show Filter

Go to

□		IP Address	Type	Name	IPv4 DHCP Utiliz...	Active Users	Discover Now	Comment	Site
☑		192.168.1.10-192.168.1.120	IPv4 DHCP Range	dhcprange	0.0% (0/111)	0			

Step 26 Select **Grid->Grid Manager->DHCP->select pencil** (edit properties)



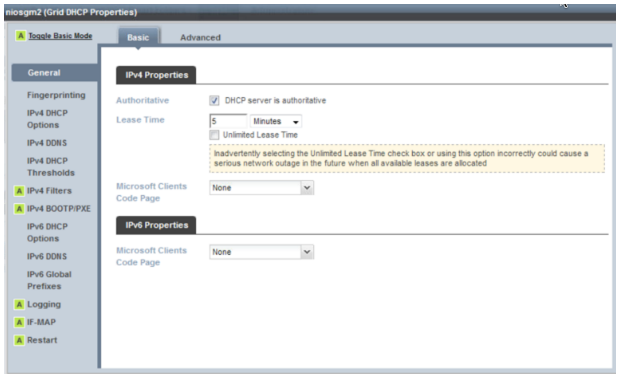
Quick Filter None | Off Filter On | Show Filter Toggle Restart Groups View

□ Group Results Group By Choose one

Go to

□	Name	Service Status	IPv4 Address	Comment	Site
□	niosgm2.lab1	DHCP Service is w	192.168.1.88		

Step 27 You should see the following:



niosgm2 (Grid DHCP Properties)

IPv4 Properties

Authoritative: ☑ DHCP server is authoritative

Lease Time: 5 Minutes

☐ Unlimited Lease Time

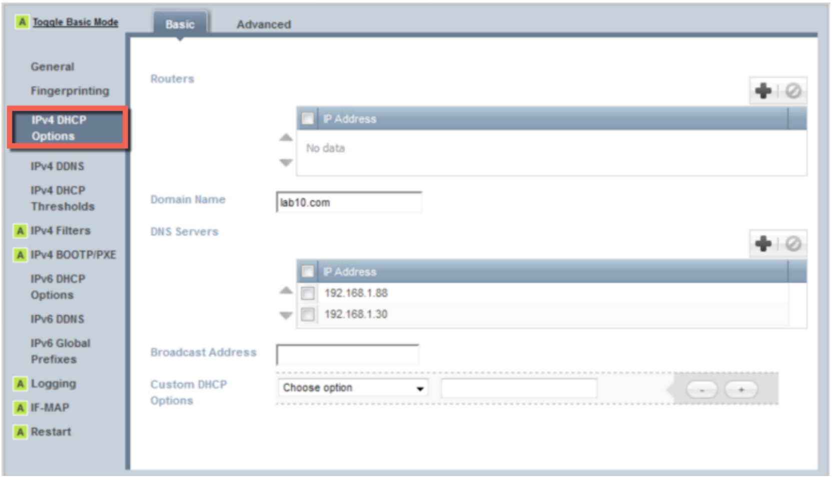
Inadvertently selecting the Unlimited Lease Time check box or using this option incorrectly could cause a serious network outage in the future when all available leases are allocated

Microsoft Clients Code Page: None

IPv6 Properties

Microsoft Clients Code Page: None

Step 28 Under **IPv4 DHCP Options,** enter **the domain name** (i.e. lab10.com), Infoblox Grid Master and DNS server to forward lookups to



Routers

☐ IP Address
No data

Domain Name: lab10.com

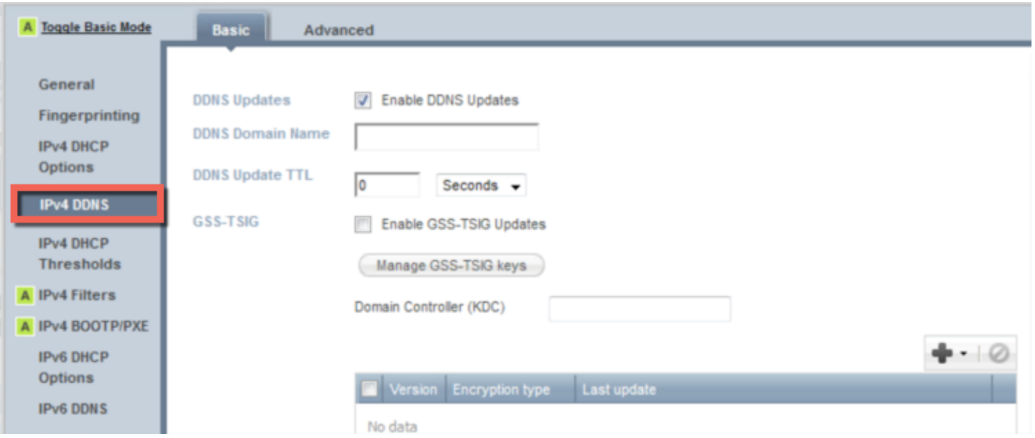
DNS Servers

☐ IP Address
☐ 192.168.1.88
☐ 192.168.1.30

Broadcast Address:

Custom DHCP Options: Choose option

Step 29 Select **IPv4 DDNS** and **enable DDNS updates**



DDNS Updates: ☑ Enable DDNS Updates

DDNS Domain Name:

DDNS Update TTL: 0 Seconds

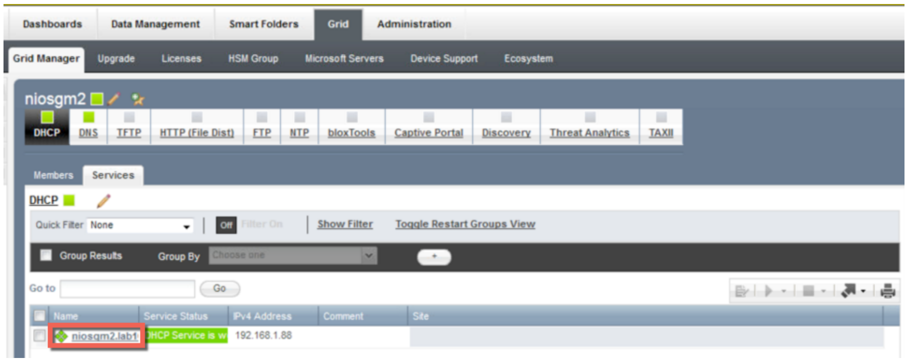
GSS-TSIG: ☐ Enable GSS-TSIG Updates

Domain Controller (KDC):

☐	Version	Encryption type	Last update
No data			

Step 30 Select **Save and Close**

Step 31 Select the link for the Infoblox Grid Master

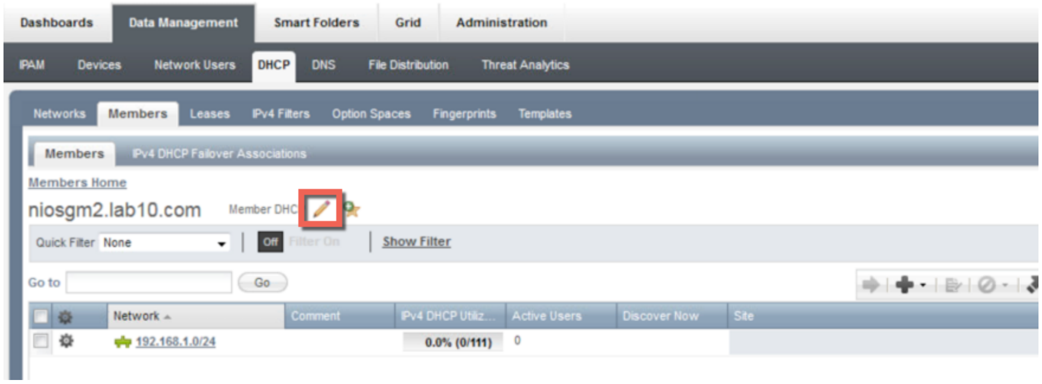


Quick Filter: None

Group By: Choose one

Name	Service Status	IPv4 Address	Comment	Site
niosgm2.lab1	DHCP Service is w	192.168.1.88		

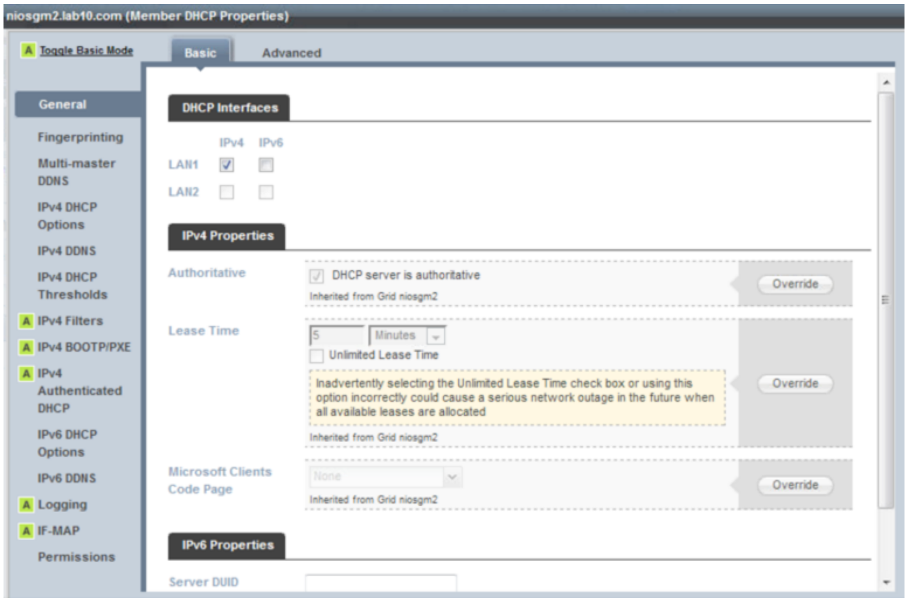
Step 32 Select **pencil** (edit properties)



Quick Filter: None

Network	Comment	IPv4 DHCP Utiliz...	Active Users	Discover Now	Site
192.168.1.0/24		0.0% (0/111)	0		

Step 33 You should see the following:



DHCP Interfaces

	IPv4	IPv6
LAN1	☑	□
LAN2	□	□

IPv4 Properties

Authoritative: ☑ DHCP server is authoritative
Inherited from Grid niosgm2

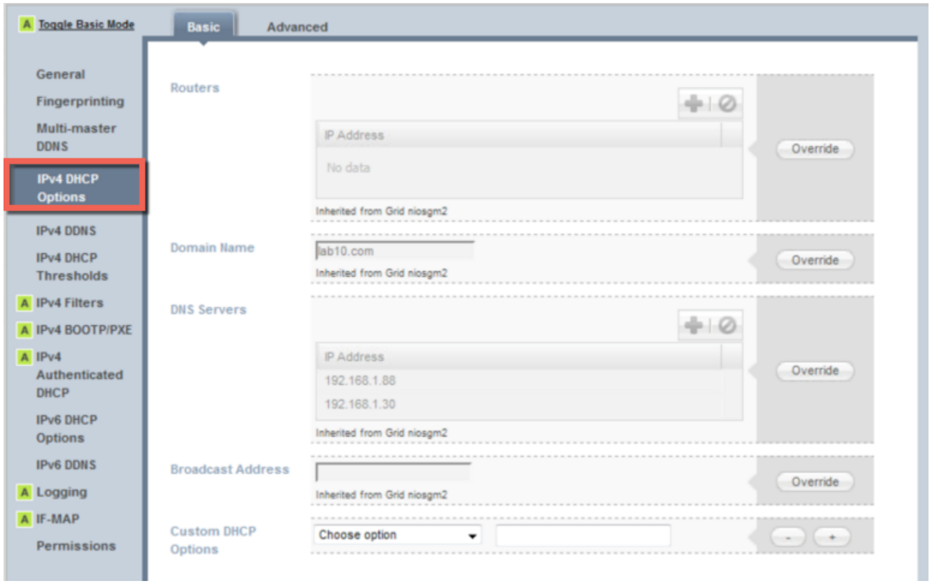
Lease Time: 5 Minutes
□ Unlimited Lease Time
Inadvertently selecting the Unlimited Lease Time check box or using this option incorrectly could cause a serious network outage in the future when all available leases are allocated
Inherited from Grid niosgm2

Microsoft Clients Code Page: None
Inherited from Grid niosgm2

IPv6 Properties

Server DUID

Step 34 Select **IPv4 DHCP Options** and verify the domain name and DNS server information



Routers: IP Address — No data — Inherited from Grid niosgm2

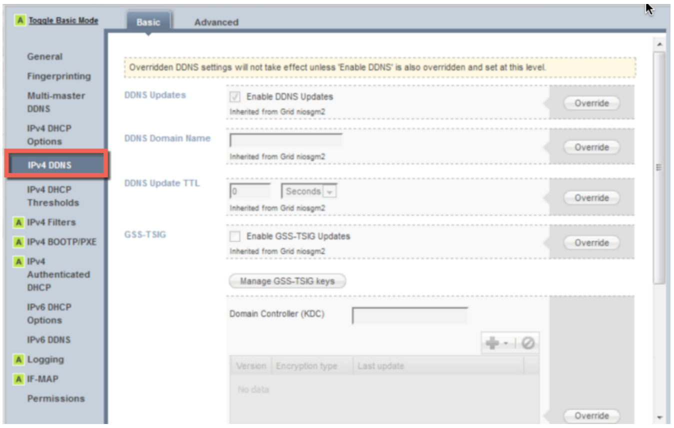
Domain Name: lab10.com — Inherited from Grid niosgm2

DNS Servers: IP Address — 192.168.1.88 — 192.168.1.30 — Inherited from Grid niosgm2

Broadcast Address: — Inherited from Grid niosgm2

Custom DHCP Options: Choose option

Step 35 Select **IPv4 DDNS** and verify that DDNS updates are enabled



Overridden DDNS settings will not take effect unless 'Enable DDNS' is also overridden and set at this level.

DDNS Updates: ☑ Enable DDNS Updates — Inherited from Grid niosgm2

DDNS Domain Name: — Inherited from Grid niosgm2

DDNS Update TTL: 0 Seconds — Inherited from Grid niosgm2

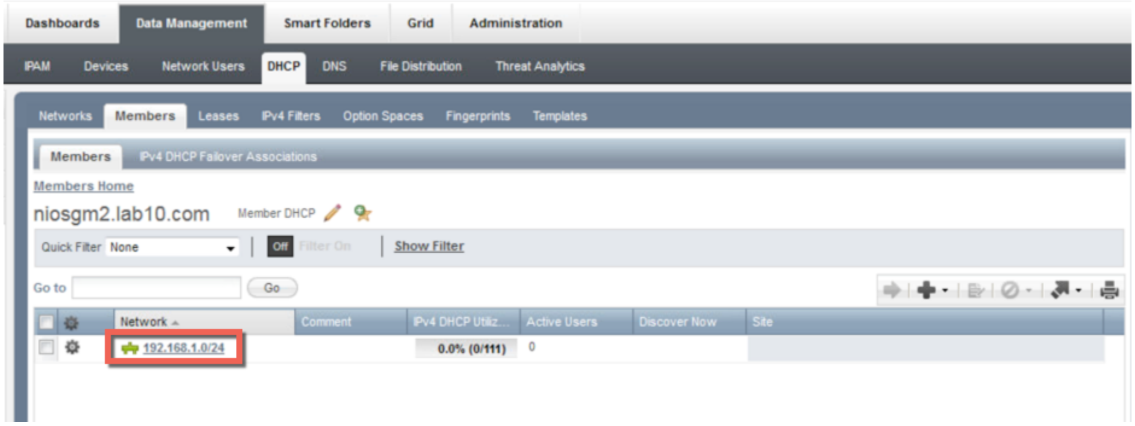
GSS-TSIG: □ Enable GSS-TSIG Updates — Inherited from Grid niosgm2

Domain Controller (KDC):

Version	Encryption type	Last update
No data		

Step 36 Select **Save and Close**

Step 37 Select the network

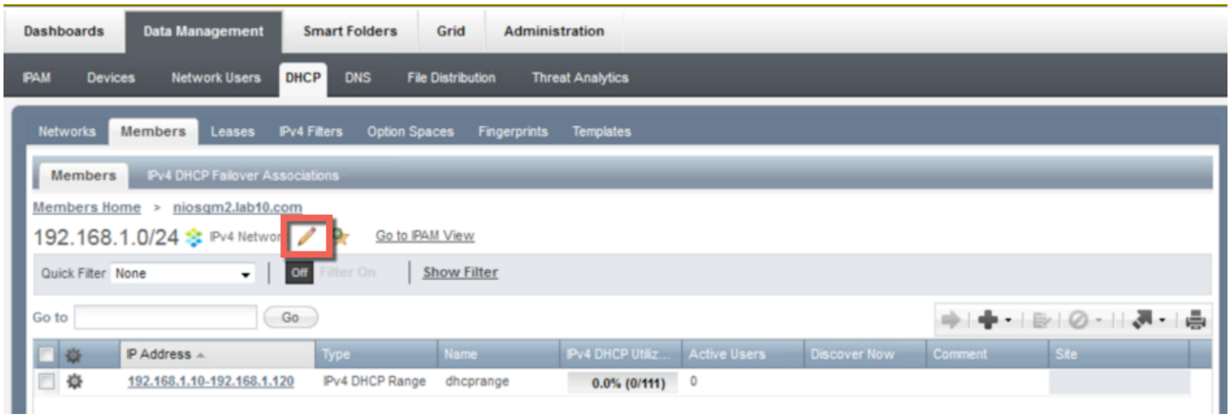


niosgm2.lab10.com

Quick Filter: None

	Network	Comment	IPv4 DHCP Utiliz...	Active Users	Discover Now	Site
□	192.168.1.0/24		0.0% (0/111)	0		

Step 38 Select **pencil (edit properties)**



Members Home > niosgm2.lab10.com

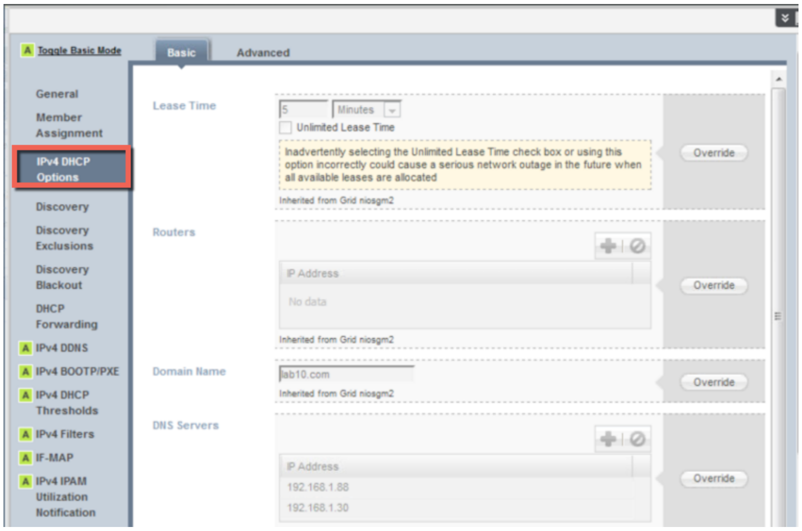
192.168.1.0/24 IPv4 Network

Quick Filter None | Off Filter On

Go to

IP Address	Type	Name	IPv4 DHCP Utiliz...	Active Users	Discover Now	Comment	Site
192.168.1.10-192.168.1.120	IPv4 DHCP Range	dhcprange	0.0% (0/111)	0			

Step 39 Select **IPv4 DHCP Options**, verify that your name servers and domain are correct



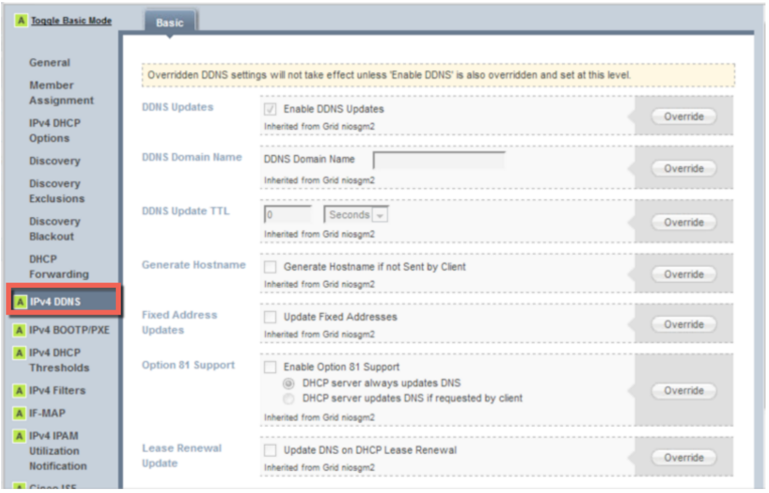
Lease Time: 5 Minutes
□ Unlimited Lease Time
Inadvertently selecting the Unlimited Lease Time check box or using this option incorrectly could cause a serious network outage in the future when all available leases are allocated
Inherited from Grid niosgm2

Routers: IP Address — No data
Inherited from Grid niosgm2

Domain Name: lab10.com
Inherited from Grid niosgm2

DNS Servers: IP Address
192.168.1.88
192.168.1.30

Step 40 Select **IPv4 DDNS** and verify that Enable DDNS Updates are enabled.



Overridden DDNS settings will not take effect unless 'Enable DDNS' is also overridden and set at this level.

DDNS Updates: ☑ Enable DDNS Updates
Inherited from Grid niosgm2

DDNS Domain Name: DDNS Domain Name
Inherited from Grid niosgm2

DDNS Update TTL: 0 Seconds
Inherited from Grid niosgm2

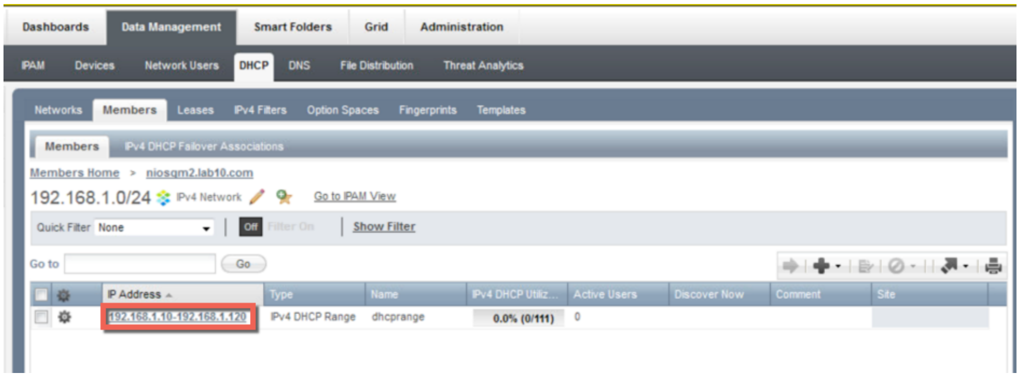
Generate Hostname: □ Generate Hostname if not Sent by Client
Inherited from Grid niosgm2

Fixed Address Updates: □ Update Fixed Addresses
Inherited from Grid niosgm2

Option 81 Support: □ Enable Option 81 Support
● DHCP server always updates DNS
○ DHCP server updates DNS if requested by client
Inherited from Grid niosgm2

Lease Renewal Update: □ Update DNS on DHCP Lease Renewal
Inherited from Grid niosgm2

Step 41 Select **IP address** range



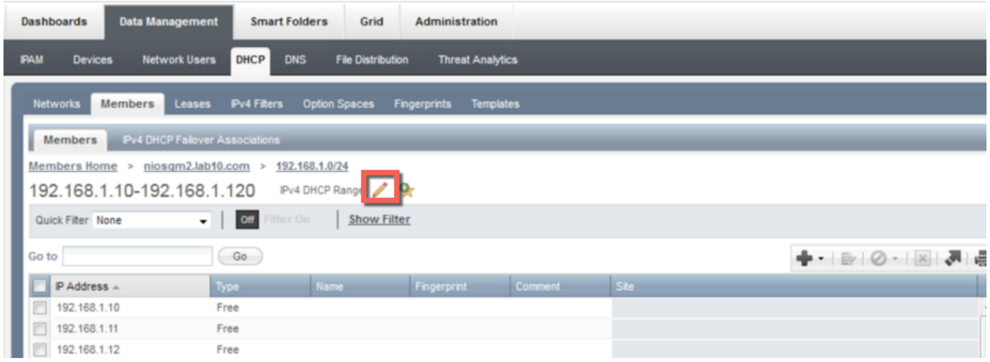
Members Home > niosgm2.lab10.com

192.168.1.0/24 IPv4 Network Go to IPAM View

Quick Filter: None

IP Address	Type	Name	IPv4 DHCP Utiliz...	Active Users	Discover Now	Comment	Site
192.168.1.10-192.168.1.120	IPv4 DHCP Range	dhcprange	0.0% (0/111)	0			

Step 42 Select **pencil** (edit properties)



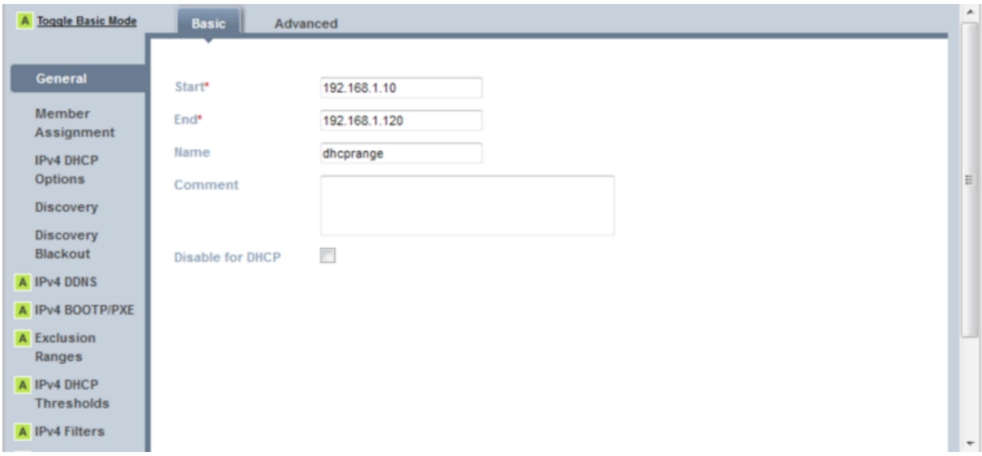
Members Home > niosgm2.lab10.com > 192.168.1.0/24

192.168.1.10-192.168.1.120 IPv4 DHCP Range

Quick Filter: None

IP Address	Type	Name	Fingerprint	Comment	Site
192.168.1.10	Free				
192.168.1.11	Free				
192.168.1.12	Free				

Step 43 You should see the following:



Start*: 192.168.1.10

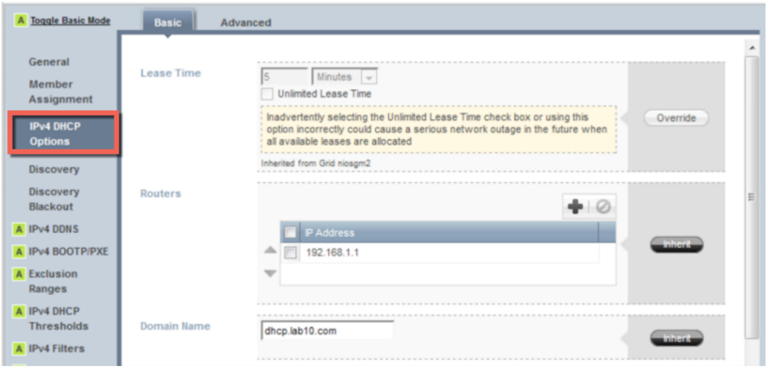
End*: 192.168.1.120

Name: dhcprange

Comment:

Disable for DHCP ☐

Step 44 Select **IPv4 DHCP Options**, and verify the Lease time of 5 minutes, router IP address, domain name and the name servers



Lease Time: 5 Minutes

□ Unlimited Lease Time

Inadvertently selecting the Unlimited Lease Time check box or using this option incorrectly could cause a serious network outage in the future when all available leases are allocated

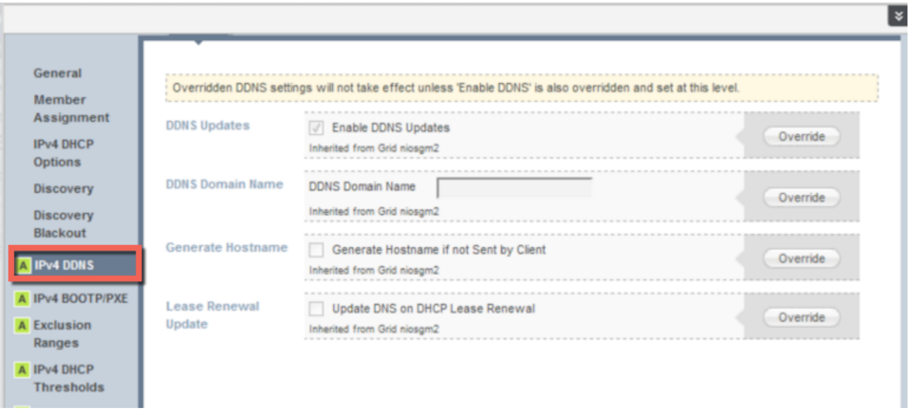
Inherited from Grid niosgm2

Routers:

IP Address
192.168.1.1

Domain Name: dhcp.lab10.com

Step 45 Select **IPv4 DDNS** and verify DDNS updates are enabled



Overridden DDNS settings will not take effect unless 'Enable DDNS' is also overridden and set at this level.

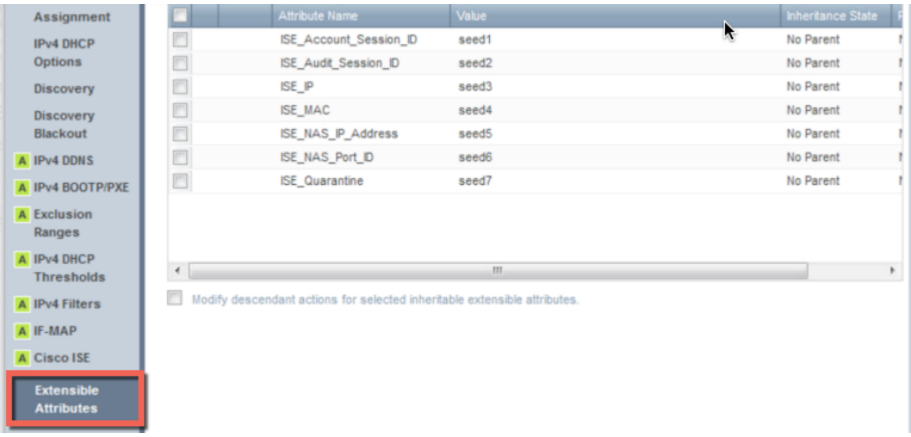
DDNS Updates: ☑ Enable DDNS Updates
Inherited from Grid niosgm2

DDNS Domain Name: DDNS Domain Name
Inherited from Grid niosgm2

Generate Hostname: □ Generate Hostname if not Sent by Client
Inherited from Grid niosgm2

Lease Renewal Update: □ Update DNS on DHCP Lease Renewal
Inherited from Grid niosgm2

Step 46 Select **Extensible Attributes,** and verify that you have the following attributes



Attribute Name	Value	Inheritance State
ISE_Account_Session_ID	seed1	No Parent
ISE_Audit_Session_ID	seed2	No Parent
ISE_IP	seed3	No Parent
ISE_MAC	seed4	No Parent
ISE_NAS_IP_Address	seed5	No Parent
ISE_NAS_Port_ID	seed6	No Parent
ISE_Quarantine	seed7	No Parent

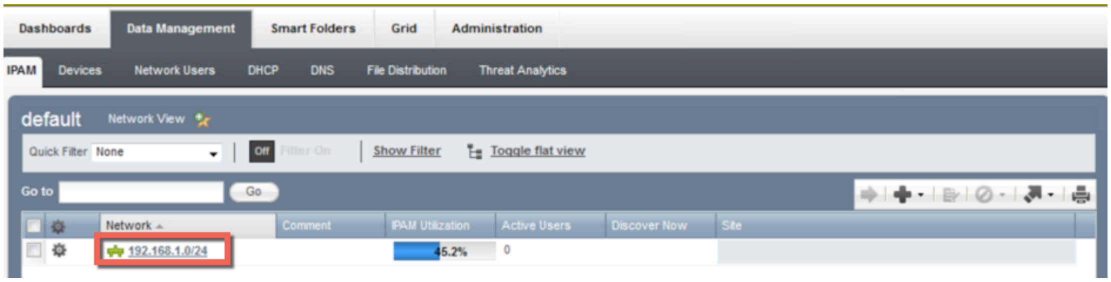
□ Modify descendant actions for selected inheritable extensible attributes.

Step 47 Select **Save and Close**

Configuring IPAM Table

This section steps through the IPAM configuration to recognize the pxGrid session information

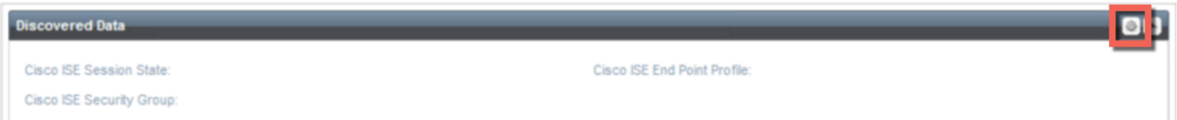
Step 1 Select **Data Management->IPAM->network**



Quick Filter: None

Network	Comment	IPAM Utilization	Active Users	Discover Now	Site
192.168.1.0/24		45.2%	0		

Step 2 Select the **Configure** tab on the Discovered Data bar

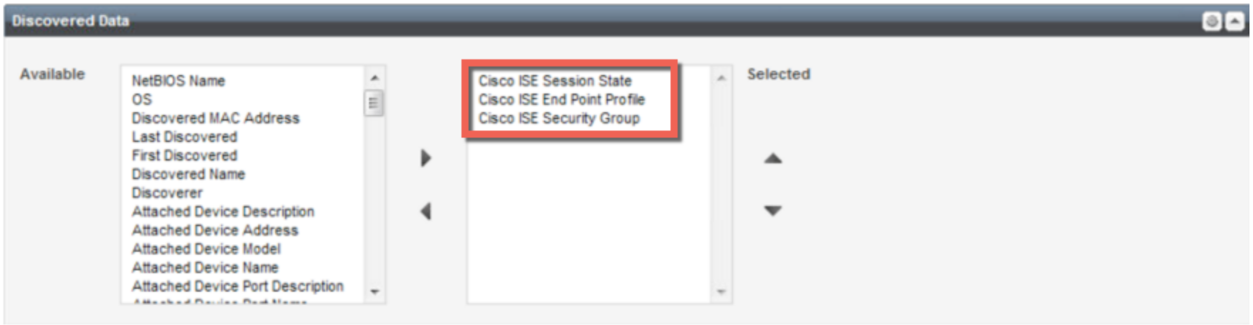


Cisco ISE Session State:

Cisco ISE End Point Profile:

Cisco ISE Security Group:

Step 3 Ensure you have the following



Available

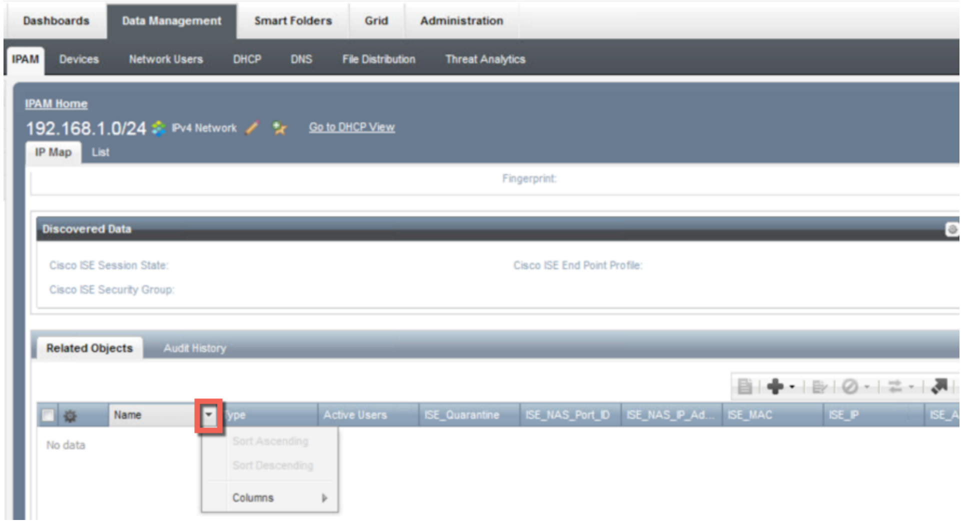
NetBIOS Name
OS
Discovered MAC Address
Last Discovered
First Discovered
Discovered Name
Discoverer
Attached Device Description
Attached Device Address
Attached Device Model
Attached Device Name
Attached Device Port Description

Selected

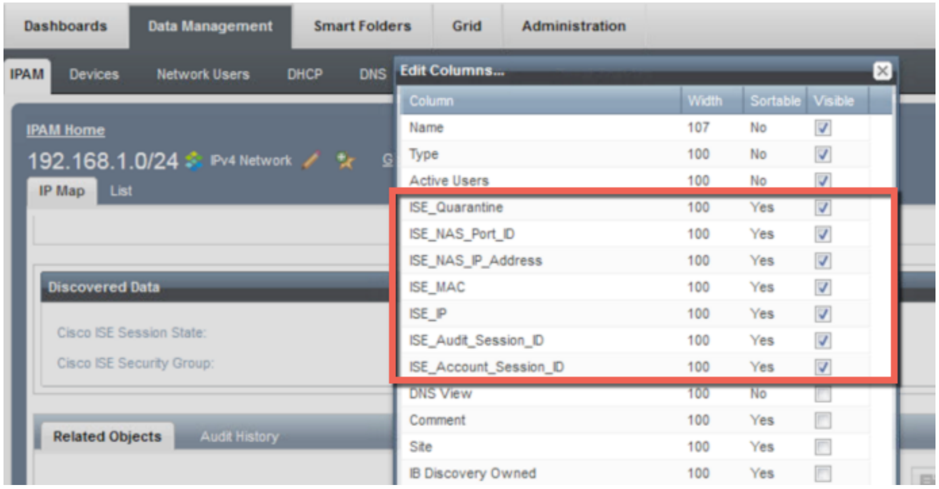
Cisco ISE Session State
Cisco ISE End Point Profile
Cisco ISE Security Group

Step 4 Select the **Configuration Tab** to Close

Step 5 Scroll down to the Name Column and click on the **Down arrow**



Step 6 Select **Columns->Edit Columns** and select the following:

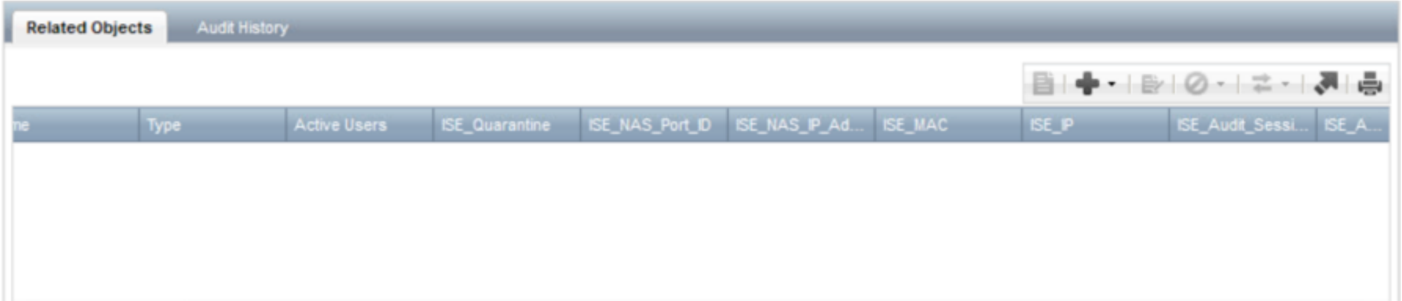


Edit Columns...

Column	Width	Sortable	Visible
Name	107	No	☑
Type	100	No	☑
Active Users	100	No	☑
ISE_Quarantine	100	Yes	☑
ISE_NAS_Port_ID	100	Yes	☑
ISE_NAS_IP_Address	100	Yes	☑
ISE_MAC	100	Yes	☑
ISE_IP	100	Yes	☑
ISE_Audit_Session_ID	100	Yes	☑
ISE_Account_Session_ID	100	Yes	☑
DNS View	100	No	□
Comment	100	Yes	□
Site	100	Yes	□
IB Discovery Owned	100	Yes	□

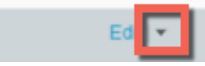
Step 7 Click ->**Apply**

Step 8 You should see the ISE attributes appear in the Column header

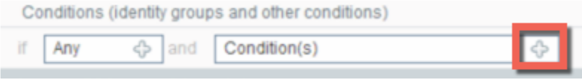


Adding ISE EPS Quarantine Authorization Rule

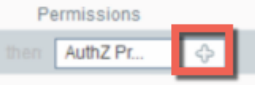
Add the ISE EPS Quarantine Authorization Policy to quarantine the endpoint through ISE.



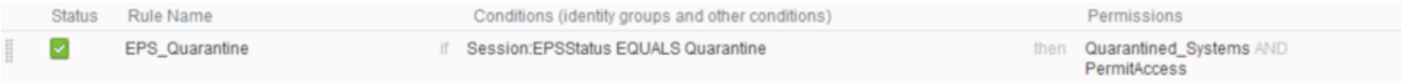
Step 1 Select Policy->Authorization->Exceptions-> Insert New Rule above
Step 2 For Rule Name enter **EPS_Quarantine**



Step 3 Create new condition rule by selecting
Step 4 Under Description, Select **Attribute** select **Session:EPStatus:Equals:Quarantine**

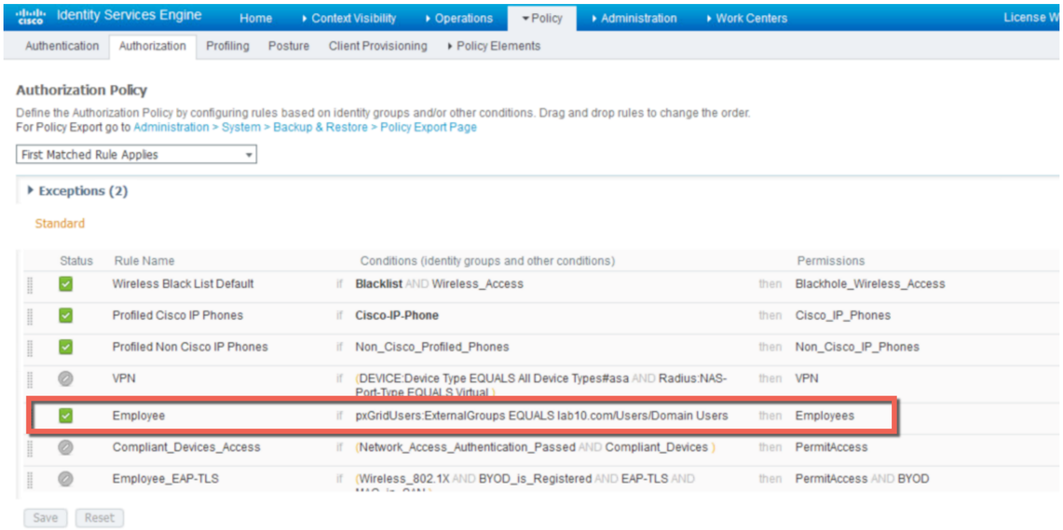


Step 5 Select the Authorization profile **->Security Group->Quarantined Systems**
Step 6 Select **"+"**
Step 7 Select **Standard->Under Profile select Standard->Permit Access->Done**
Step 8 You should see the following



	Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
	✓	EPS_Quarantine	if	Session:EPSStatus EQUALS Quarantine	then	Quarantined_Systems AND PermitAccess

Step 9 Select **Save**
Step 10 Add a Security Group Tag of Employee to user authenticating in the Domain/Users Group
Step 11 Insert a new authorization rule named **Employee**
Step 12 Create a new condition rule: select your AD joint point name (i.e. **pxgridUsers)->External Groups->../Domain/Users**
Step 13 Select **Authorization Profile->Security Group->Employee->Done->Save**
You should see the following:



Authorization Policy

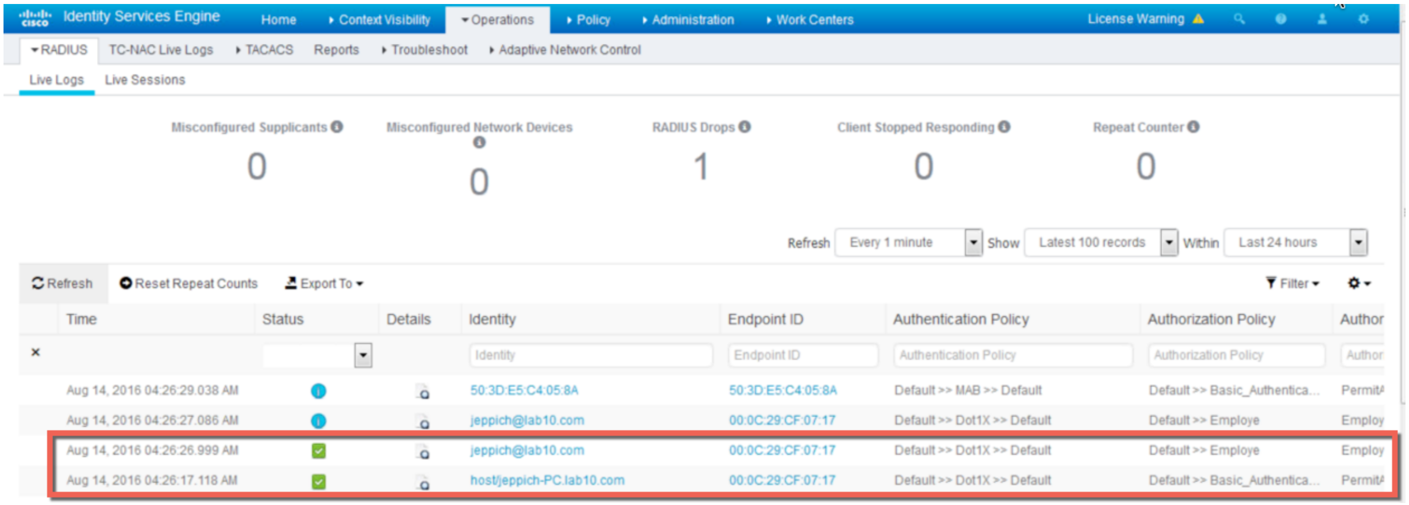
Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Wireless Black List Default	if	Blacklist AND Wireless_Access	then	Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones
⊘	VPN	if	(DEVICE:Device Type EQUALS All Device Types#asa AND Radius:NAS-Port-Type EQUALS Virtual)	then	VPN
✓	Employee	if	pxGridUsers:ExternalGroups EQUALS lab10.com/Users/Domain Users	then	Employees
⊘	Compliant_Devices_Access	if	(Network_Access_Authentication_Passed AND Compliant_Devices)	then	PermitAccess
⊘	Employee_EAP-TLS	if	(Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN)	then	PermitAccess AND BYOD

Testing

Here we step through the use-case of an end-user authenticating to ISE. The Infoblox Grid Master IPAM table will be populated with the pxGrid session information. The other use case is an Infoblox Grid Master RPZ policy violation, where the end-user is denied access to www.yahoo.com and is quarantined via pxGrid.

Step 1 Verify user logs into ISE



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

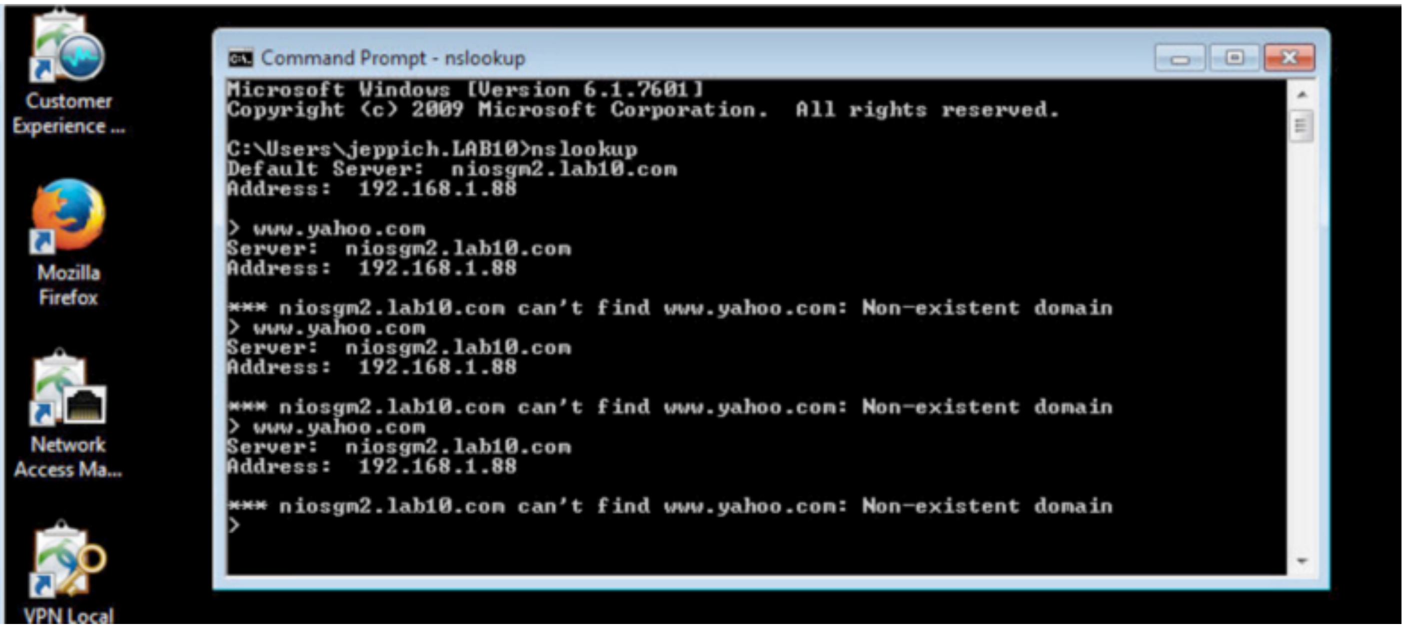
Refresh: Every 1 minute Show: Latest 100 records Within: Last 24 hours

Time	Status	Details	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Author
Aug 14, 2016 04:26:29.038 AM	●		50:3D:E5:C4:05:8A	50:3D:E5:C4:05:8A	Default >> MAB >> Default	Default >> Basic_Authentica...	Permit
Aug 14, 2016 04:26:27.086 AM	●		jeppich@lab10.com	00:0C:29:CF:07:17	Default >> Dot1X >> Default	Default >> Employe	Employ
Aug 14, 2016 04:26:26.999 AM	✓		jeppich@lab10.com	00:0C:29:CF:07:17	Default >> Dot1X >> Default	Default >> Employe	Employ
Aug 14, 2016 04:26:17.118 AM	✓		host/jeppich-PC.lab10.com	00:0C:29:CF:07:17	Default >> Dot1X >> Default	Default >> Basic_Authentica...	Permit

Step 2 Open a command prompt on the client and type: **nslookup**

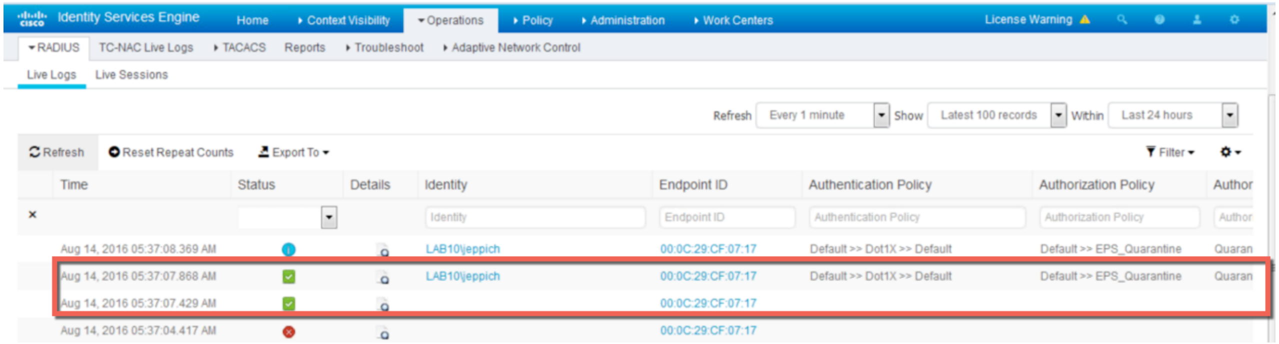
Step 3 Type: www.yahoo.com

Step 4 You should see the following non-existent domain messages



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\jeppich.LAB10>nslookup
Default Server:  niosgm2.lab10.com
Address:  192.168.1.88

> www.yahoo.com
Server:  niosgm2.lab10.com
Address:  192.168.1.88

*** niosgm2.lab10.com can't find www.yahoo.com: Non-existent domain
> www.yahoo.com
Server:  niosgm2.lab10.com
Address:  192.168.1.88

*** niosgm2.lab10.com can't find www.yahoo.com: Non-existent domain
> www.yahoo.com
Server:  niosgm2.lab10.com
Address:  192.168.1.88

*** niosgm2.lab10.com can't find www.yahoo.com: Non-existent domain
>
```

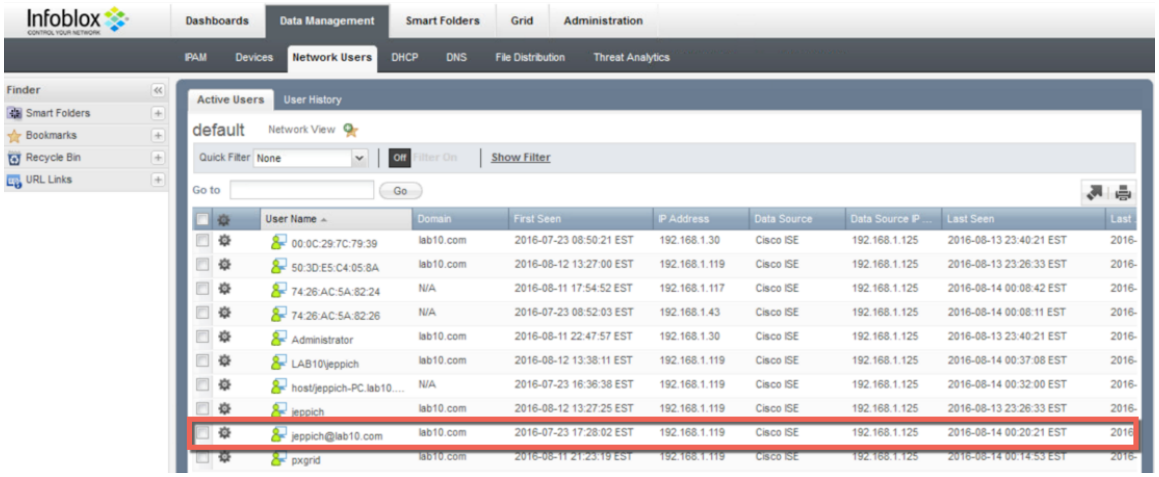
Step 5 To view the logs in ISE, select **Operations->RADIUS->Live Logs**, the endpoint is quarantined



Refresh Every 1 minute Show Latest 100 records Within Last 24 hours

Time	Status	Details	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Author
Aug 14, 2016 05:37:08.369 AM	●		LAB10\jeppich	00:0C:29:CF:07:17	Default >> Dot1X >> Default	Default >> EPS_Quarantine	Quaran
Aug 14, 2016 05:37:07.868 AM	✓		LAB10\jeppich	00:0C:29:CF:07:17	Default >> Dot1X >> Default	Default >> EPS_Quarantine	Quaran
Aug 14, 2016 05:37:07.429 AM	✓			00:0C:29:CF:07:17			
Aug 14, 2016 05:37:04.417 AM	✖			00:0C:29:CF:07:17			

Step 6 On the Infoblox Grid Master, select **Data Management->Network Users->authenticated end-user**

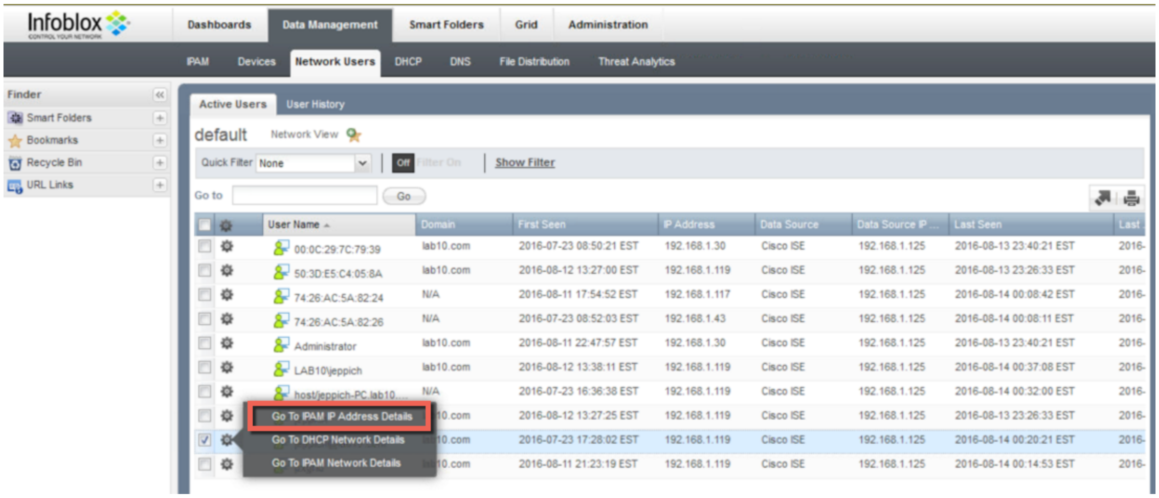


default Network View

Quick Filter None

User Name	Domain	First Seen	IP Address	Data Source	Data Source IP ...	Last Seen	Last
00:0C:29:7C:79:39	lab10.com	2016-07-23 08:50:21 EST	192.168.1.30	Cisco ISE	192.168.1.125	2016-08-13 23:40:21 EST	2016-
50:3D:E5:C4:05:8A	lab10.com	2016-08-12 13:27:00 EST	192.168.1.119	Cisco ISE	192.168.1.125	2016-08-13 23:26:33 EST	2016-
74:26:AC:5A:82:24	N/A	2016-08-11 17:54:52 EST	192.168.1.117	Cisco ISE	192.168.1.125	2016-08-14 00:08:42 EST	2016-
74:26:AC:5A:82:26	N/A	2016-07-23 08:52:03 EST	192.168.1.43	Cisco ISE	192.168.1.125	2016-08-14 00:08:11 EST	2016-
Administrator	lab10.com	2016-08-11 22:47:57 EST	192.168.1.30	Cisco ISE	192.168.1.125	2016-08-13 23:40:21 EST	2016-
LAB10\jeppich	lab10.com	2016-08-12 13:38:11 EST	192.168.1.119	Cisco ISE	192.168.1.125	2016-08-14 00:37:08 EST	2016-
host/jeppich-PC.lab10....	N/A	2016-07-23 16:36:38 EST	192.168.1.119	Cisco ISE	192.168.1.125	2016-08-14 00:32:00 EST	2016-
jeppich	lab10.com	2016-08-12 13:27:25 EST	192.168.1.119	Cisco ISE	192.168.1.125	2016-08-13 23:26:33 EST	2016-
jeppich@lab10.com	lab10.com	2016-07-23 17:28:02 EST	192.168.1.119	Cisco ISE	192.168.1.125	2016-08-14 00:20:21 EST	2016
pxgrid	lab10.com	2016-08-11 21:23:19 EST	192.168.1.119	Cisco ISE	192.168.1.125	2016-08-14 00:14:53 EST	2016-

Step 7 Select the end-user and click on the **go to IPAM IP Address Details** Tab

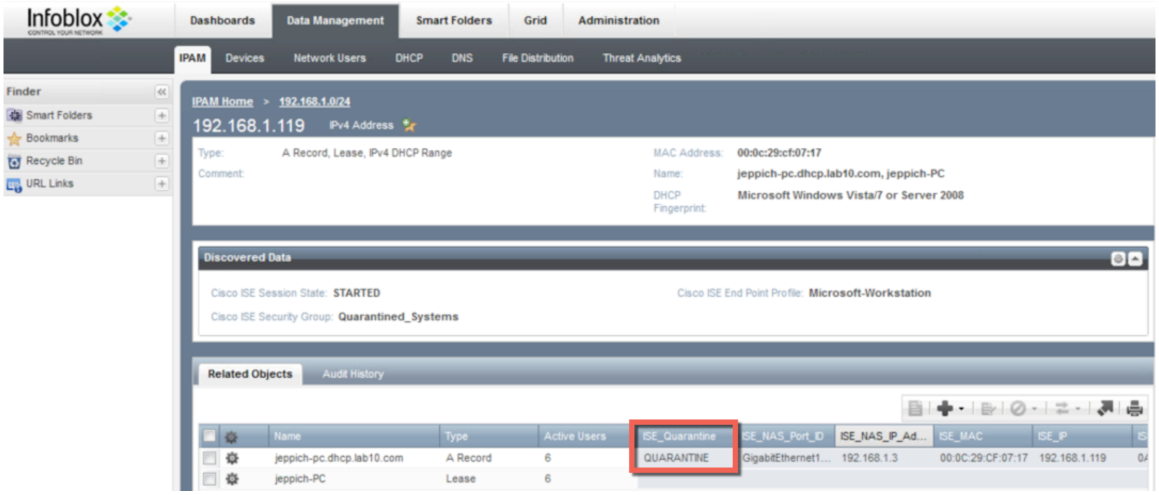


default Network View

Quick Filter None

User Name	Domain	First Seen	IP Address	Data Source	Data Source IP ...	Last Seen	Last
00:0C:29:7C:79:39	lab10.com	2016-07-23 08:50:21 EST	192.168.1.30	Cisco ISE	192.168.1.125	2016-08-13 23:40:21 EST	2016-
50:3D:E5:C4:05:8A	lab10.com	2016-08-12 13:27:00 EST	192.168.1.119	Cisco ISE	192.168.1.125	2016-08-13 23:26:33 EST	2016-
74:26:AC:5A:82:24	N/A	2016-08-11 17:54:52 EST	192.168.1.117	Cisco ISE	192.168.1.125	2016-08-14 00:08:42 EST	2016-
74:26:AC:5A:82:26	N/A	2016-07-23 08:52:03 EST	192.168.1.43	Cisco ISE	192.168.1.125	2016-08-14 00:08:11 EST	2016-
Administrator	lab10.com	2016-08-11 22:47:57 EST	192.168.1.30	Cisco ISE	192.168.1.125	2016-08-13 23:40:21 EST	2016-
LAB10\jeppich	lab10.com	2016-08-12 13:38:11 EST	192.168.1.119	Cisco ISE	192.168.1.125	2016-08-14 00:37:08 EST	2016-
host/jeppich-PC.lab10....	N/A	2016-07-23 16:36:38 EST	192.168.1.119	Cisco ISE	192.168.1.125	2016-08-14 00:32:00 EST	2016-
	10.com	2016-08-12 13:27:25 EST	192.168.1.119	Cisco ISE	192.168.1.125	2016-08-13 23:26:33 EST	2016-
	10.com	2016-07-23 17:28:02 EST	192.168.1.119	Cisco ISE	192.168.1.125	2016-08-14 00:20:21 EST	2016-
	10.com	2016-08-11 21:23:19 EST	192.168.1.119	Cisco ISE	192.168.1.125	2016-08-14 00:14:53 EST	2016-

Step 8 You should see the end-user has been quarantined as denoted by the pxGrid session attribute EPS_Status



IPAM Home > 192.168.1.0/24

192.168.1.119 IPv4 Address

Type: A Record, Lease, IPv4 DHCP Range

Comment:

MAC Address: 00:0c:29:cf:07:17

Name: jeppich-pc.dhcp.lab10.com, jeppich-PC

DHCP Fingerprint: Microsoft Windows Vista/7 or Server 2008

Discovered Data

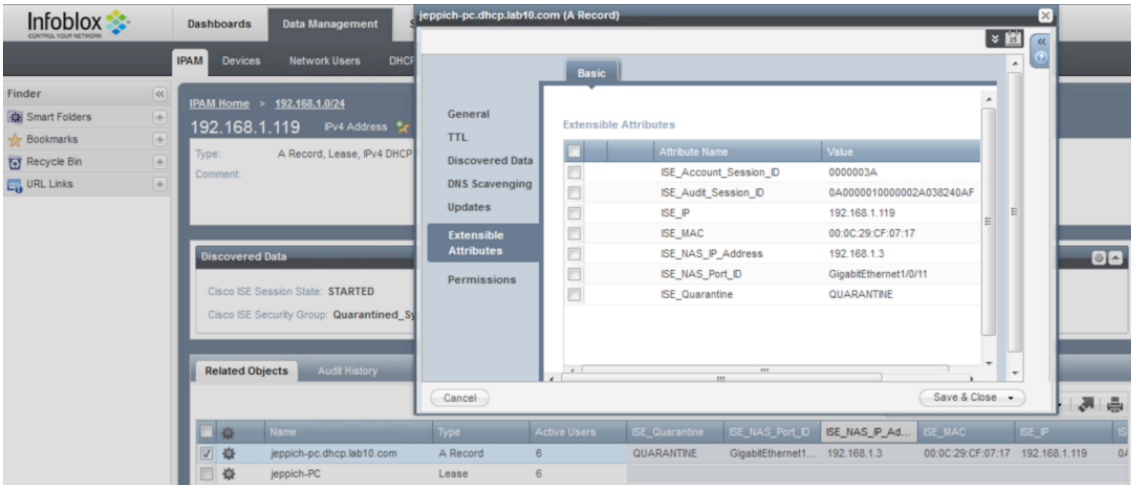
Cisco ISE Session State: STARTED

Cisco ISE End Point Profile: Microsoft-Workstation

Cisco ISE Security Group: Quarantined_Systems

Name	Type	Active Users	ISE_Quarantine	ISE_NAS_Port_ID	ISE_NAS_IP_Ad...	ISE_MAC	ISE_IP
jeppich-pc.dhcp.lab10.com	A Record	6	QUARANTINE	GigabitEthernet1...	192.168.1.3	00:0C:29:CF:07:17	192.168.1.119
jeppich-PC	Lease	6					

Step 9 Select the **end-user->edit** , you will see the pxGrid available attributes

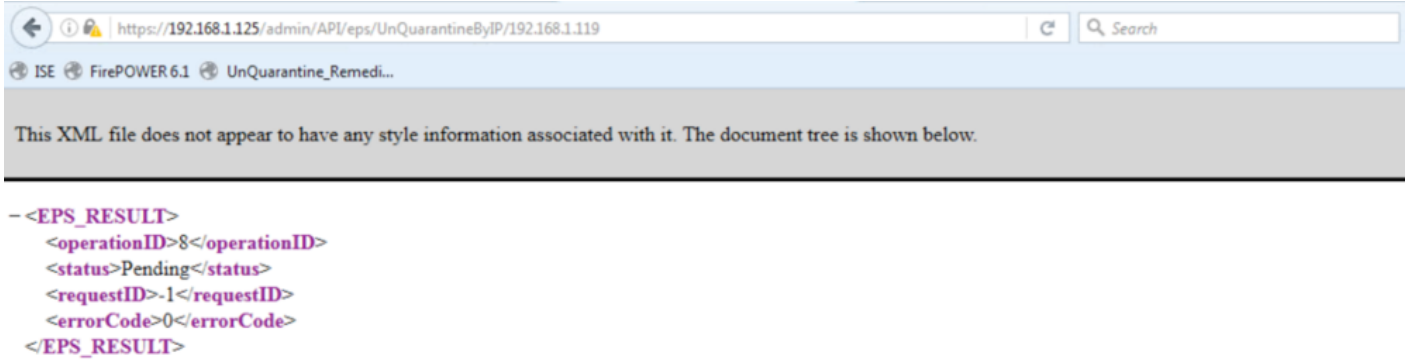


jeppich-pc.dhcp.lab10.com (A Record)

Extensible Attributes

Attribute Name	Value
ISE_Account_Session_ID	0000003A
ISE_Audit_Session_ID	0A0000010000002A038240AF
ISE_IP	192.168.1.119
ISE_MAC	00:0C:29:CF:07:17
ISE_NAS_IP_Address	192.168.1.3
ISE_NAS_Port_ID	GigabitEthernet1/0/11
ISE_Quarantine	QUARANTINE

Step 10 Unquarantine must be done manually from ISE, type in the URL:
https://{ISE ipaddress}/admin/API/eps/UnQuarantineByIP/{ipaddress of endpoint}

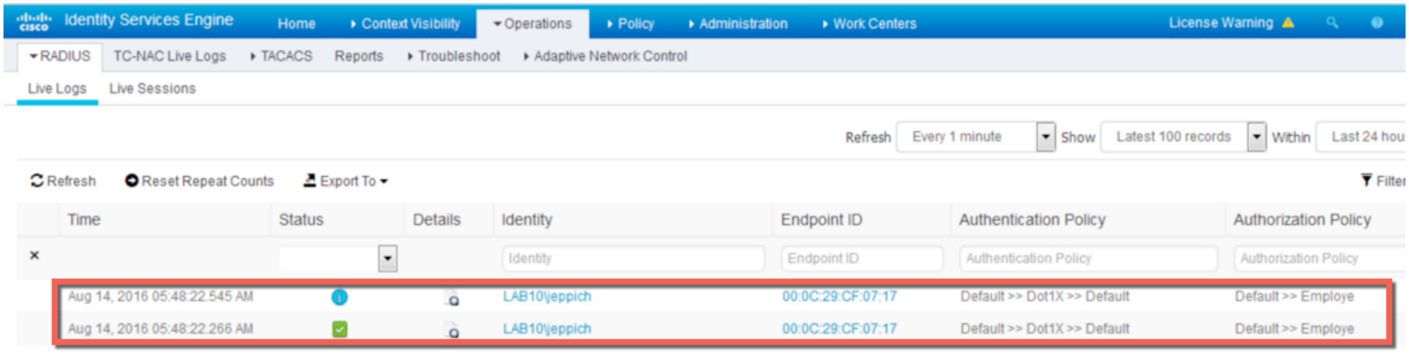


https://192.168.1.125/admin/API/eps/UnQuarantineByIP/192.168.1.119

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
- <EPS_RESULT>
    <operationID>8</operationID>
    <status>Pending</status>
    <requestID>-1</requestID>
    <errorCode>0</errorCode>
  </EPS_RESULT>
```

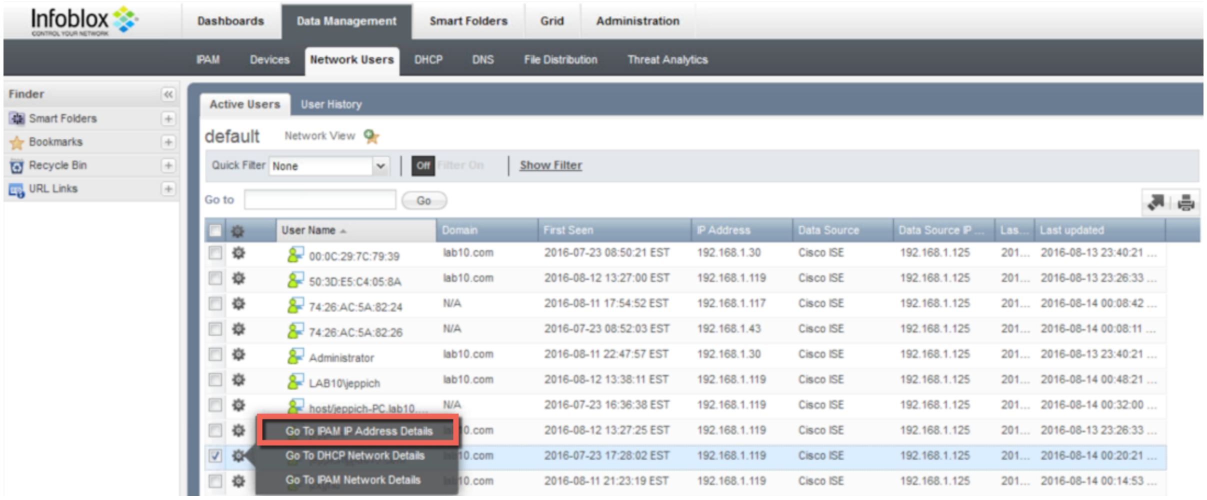
Step 11 To view the unquarantined device in ISE, select **Operations->RADIUS->LiveLogs** You should see the unquarantined endpoint.



Refresh Every 1 minute · Show Latest 100 records · Within Last 24 hou

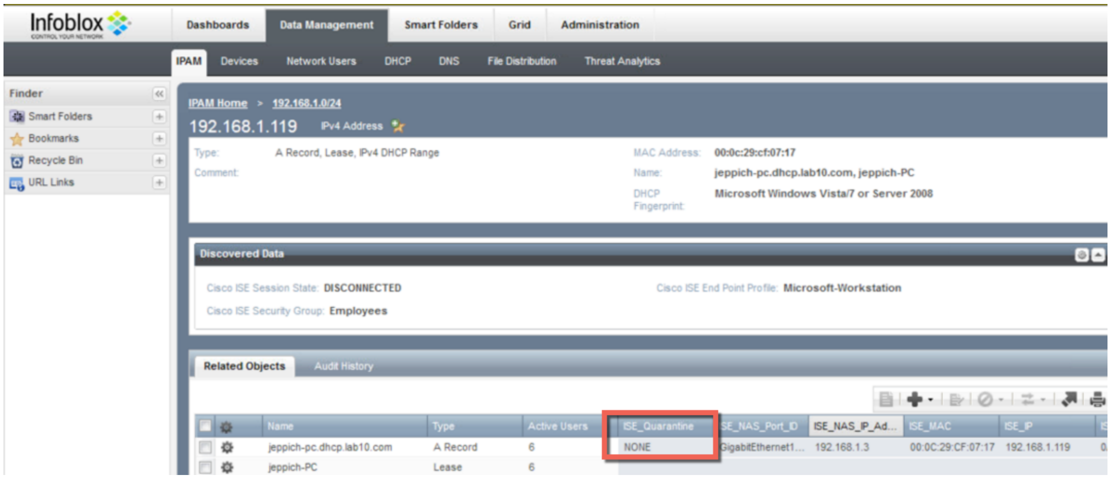
Time	Status	Details	Identity	Endpoint ID	Authentication Policy	Authorization Policy
Aug 14, 2016 05:48:22.545 AM	ℹ	🔍	LAB10\jeppich	00:0C:29:CF:07:17	Default >> Dot1X >> Default	Default >> Employe
Aug 14, 2016 05:48:22.266 AM	✓	🔍	LAB10\jeppich	00:0C:29:CF:07:17	Default >> Dot1X >> Default	Default >> Employe

Step 12 To view the updated quarantine status session information in Infoblox, select **Data Management->Network Users->Active Users->select the same end-user->go to the IPAM IP Address Details tab**



☐	User Name	Domain	First Seen	IP Address	Data Source	Data Source IP ...	Las...	Last updated
☐	00:0C:29:7C:79:39	lab10.com	2016-07-23 08:50:21 EST	192.168.1.30	Cisco ISE	192.168.1.125	201...	2016-08-13 23:40:21 ...
☐	50:3D:E5:C4:05:8A	lab10.com	2016-08-12 13:27:00 EST	192.168.1.119	Cisco ISE	192.168.1.125	201...	2016-08-13 23:26:33 ...
☐	74:26:AC:5A:82:24	N/A	2016-08-11 17:54:52 EST	192.168.1.117	Cisco ISE	192.168.1.125	201...	2016-08-14 00:08:42 ...
☐	74:26:AC:5A:82:26	N/A	2016-07-23 08:52:03 EST	192.168.1.43	Cisco ISE	192.168.1.125	201...	2016-08-14 00:08:11 ...
☐	Administrator	lab10.com	2016-08-11 22:47:57 EST	192.168.1.30	Cisco ISE	192.168.1.125	201...	2016-08-13 23:40:21 ...
☐	LAB10\jeppich	lab10.com	2016-08-12 13:38:11 EST	192.168.1.119	Cisco ISE	192.168.1.125	201...	2016-08-14 00:48:21 ...
☐	host/jeppich-PC.lab10....	N/A	2016-07-23 16:36:38 EST	192.168.1.119	Cisco ISE	192.168.1.125	201...	2016-08-14 00:32:00 ...
☐	[illegible]	lab10.com	2016-08-12 13:27:25 EST	192.168.1.119	Cisco ISE	192.168.1.125	201...	2016-08-13 23:26:33 ...
☑	[illegible]	lab10.com	2016-07-23 17:28:02 EST	192.168.1.119	Cisco ISE	192.168.1.125	201...	2016-08-14 00:20:21 ...
☐	[illegible]	lab10.com	2016-08-11 21:23:19 EST	192.168.1.119	Cisco ISE	192.168.1.125	201...	2016-08-14 00:14:53 ...

Step 13 You should see the Quarantine status set to **None**



192.168.1.119 IPv4 Address

Type: A Record, Lease, IPv4 DHCP Range

Comment:

MAC Address: 00:0c:29:cf:07:17

Name: jeppich-pc.dhcp.lab10.com, jeppich-PC

DHCP Fingerprint: Microsoft Windows Vista/7 or Server 2008

Cisco ISE Session State: DISCONNECTED

Cisco ISE End Point Profile: Microsoft-Workstation

Cisco ISE Security Group: Employees

☐	Name	Type	Active Users	ISE_Quarantine	ISE_NAS_Port_ID	ISE_NAS_IP_Ad...	ISE_MAC	ISE_IP
☐	jeppich-pc.dhcp.lab10.com	A Record	6	NONE	GigabitEthernet1...	192.168.1.3	00:0C:29:CF:07:17	192.168.1.119
☐	jeppich-PC	Lease	6					

Troubleshooting

Please note that all Infoblox Grid Master, Infoblox Grid Member and ISE pxGrid must be FQDN resolvable.

Listed are some common troubleshooting tips:

Infoblox Grid Master ISE Ecosystem Status Error

If you see a red status message of **Error**, re-authenticate an end-user via IEEE 802.1X. Ensure the end-user has successfully logged onto the network via ISE and see if the ISE Ecosystem status is **Running**

Adaptive Network Control (ANC) Mitigation Quarantine Mitigation Actions Not Showing Up ISE

If the endpoint quarantine mitigation actions do not appear in ISE, ensure the DNS response policy zone is set to logging under enable logging on **Adding Policy Response Zone** in this document

No Active User are Displayed under Infoblox Grid Maser Network Users

- Ensure that Infoblox Grid Master Cisco ISE Ecosystem status is Running
- Verify that Infoblox has registered to the ISE pxGrid node and subscribed to the Core and Session Topics.
- Reboot the Infoblox Grid Master
- Apply Infoblox vNIOS 7.3.6 with hotfix to resolve issue with domain\user logins

Infoblox published Dynamic Topics do not Appear in ISE Capabilities Menu

The DHCP and IPAM dynamic topics need admin approval. Select Administration->pxGrid Services-> View by Capabilities and approve the pending topics.

References

Cisco pxGrid Design Guides: https://communities.cisco.com/docs/DOC-64012