Infoblox

Deployment Guide

Cisco ISE PxGrid 2.0 Deployment Guide

Table of Contents

Executive Summary

Cisco ISE stands for Cisco Identity Services Engine. It is a centralized security policy management platform that automates and enforces security access to network resources. In other words, it is a network access controller (NAC) that can be automated to allow or restrict network access to devices based on certain rules/policies.
Cisco pxGrid (platform exchange grid) Controller is a layer on top of Cisco ISE. It is the layer that communicates with other third-party vendors (i.e. Infoblox) to get specific information to allow or restrict the network access in addition to the static rules/policies configured on ISE and the dynamic rules/policies discovered by Cisco. It is also the grid that we will be connecting to in order to send and get information to and from the ISE server.
Infoblox NIOS acts as a client to the pxGrid Controller and will be subscribing to information from the Cisco ISE box such as usernames, domain names, SSID, VLANs, etc. NIOS also publishes information that it has acquired via DHCP to Cisco ISE. NIOS also publishes events triggered as a result of ADP/DNS Firewall rules being hit.

This document goes over the steps to configure NIOS 8.5 to integrate with Cisco ISE 2.4 and above using PxGrid 2.0. The integration is different in that NIOS 8.5 uses outbound API to communicate with Cisco ISE.

Features of integrating with Cisco ISE/pxGrid include:

- The ability to get (i.e., subscribe) to session notifications from the Cisco ISE server.
- The ability to publish RPZ, IPAM, and DHCP data to the Cisco ISE server.
- Quarantining clients when an RPZ entry is hit.

Supported Platforms

Cisco ISE integration is supported on the following Infoblox appliances:

- IB-1415
- IB-1425
- IB-2215
- IB-2225
- IB-4015
- IB-4025

Prerequisites

The following are prerequisites for the Infoblox and Cisco ISE/pxGrid integration:

- NIOS 8.5 or later
- Grid master and Grid Master Candidate

Licenses

- VNIOS license if using VNIOS
- DNS license
- DHCP license
- RPZ license
- Security Ecosystem license
- MS Management license if using Grid to manage MS servers
- Threat protection license if using Advanced DNS Protection services

Certificate

- Client certificate created by the Cisco ISE administrator
- CA Root Certificate from the Customer and it is already in the Cisco ISE trusted certificate store
- Grid Master, Grid Master Candidate, MS AD Server, and Cisco ISE appliance must be in the same domain name

NOTE: Usually Cisco ISE is deployed in multiple nodes in a production environment with separate nodes for primary admin node (PPAN), primary monitoring node (PMNT), secondary admin node (SPAN), secondary monitoring node (SMNT), primary pxGrid node (pxGrid1), and secondary pxGrid node (pxGrid2)—with policy service nodes (PSN). The certificates come from the primary monitoring node. However, if the ISE server is limited to one server, then client certificate and CA certificate come from the ISE server at the following ISE GUI path: Administration --> pxGrid Services --> Certificates.

Assumptions

- Cisco ISE and pxGrid are installed properly.
- Cisco ISE certificates are installed properly.
- Root Certificate is installed properly on Cisco ISE.
- Auto registration must be turned on or clients must be explicitly approved on the Cisco ISE side.
- When DHCP/IPAM data is published to Cisco ISE, the dynamic topic (Infoblox_DHCP or Infoblox_IPAM) must be authorized.
- Time must be synchronized between the Cisco ISE server and the managing Infoblox member.
- You are running Active Directory authentication and have added the AD server to Cisco ISE. This means the Cisco ISE appliances are in the main DNS zone as A records.
- You have a Cisco ISE expert configuring the ISE appliance.
- Ethernet switch is configured correctly to communicate with the Cisco ISE appliance.

The Information Exchange from Cisco ISE to NIOS Grid

Data	**Infoblox Object**	**Value**
Device OS	Discovery	Compliments DHCP Fingerprinting and Network Insight.
Security Group	Discovery	Important security state information now available to the network admin.
Session State	Discovery	Important security state information now available to the network admin.
SSID	Discovery	Currently not discovered via Network Insight.
VLAN	Discovery	Compliments Network Insight.

TrustSEC Tag	Discovery	Important security state information now available to the network admin.
User Name	Network User	Compliments MSFT Identity Management.
Domain Name	Network User	Compliments MSFT Identity Management.
Account Session ID	Extensible Attribute	Important security state information now available to the network admin.
Audit Session ID	Extensible Attribute	Important security state information now available to the network admin.
EPS Status	Extensible Attribute	Important security state information now available to the network admin.
IP Address	Extensible Attribute	Published by Cisco, but most likely not used.
MAC Address	Extensible Attribute	Published by Cisco, but most likely not used.
NAS IP Address	Extensible Attribute	Important security state information now available to the network admin.
NAS Port ID	Extensible Attribute	Important security state information now available to the network admin.
Posture Status	Extensible Attribute	Important security state information now available to the network admin.
Posture Time Stamp	Extensible Attribute	Important security state information now available to the network admin.

Information Published by Infoblox for Action (ie notifications) by Cisco ISE

Event	Filter	Filter	Filter	Filter
DNS RPZ	RPZ Name	Rule Name	Action Policy	Source IP
Security - ADP	Rule Severity	SID	Rule Message	Source IP
DHCP Leases	Lease State			

Information Published by Infoblox to Cisco ISE

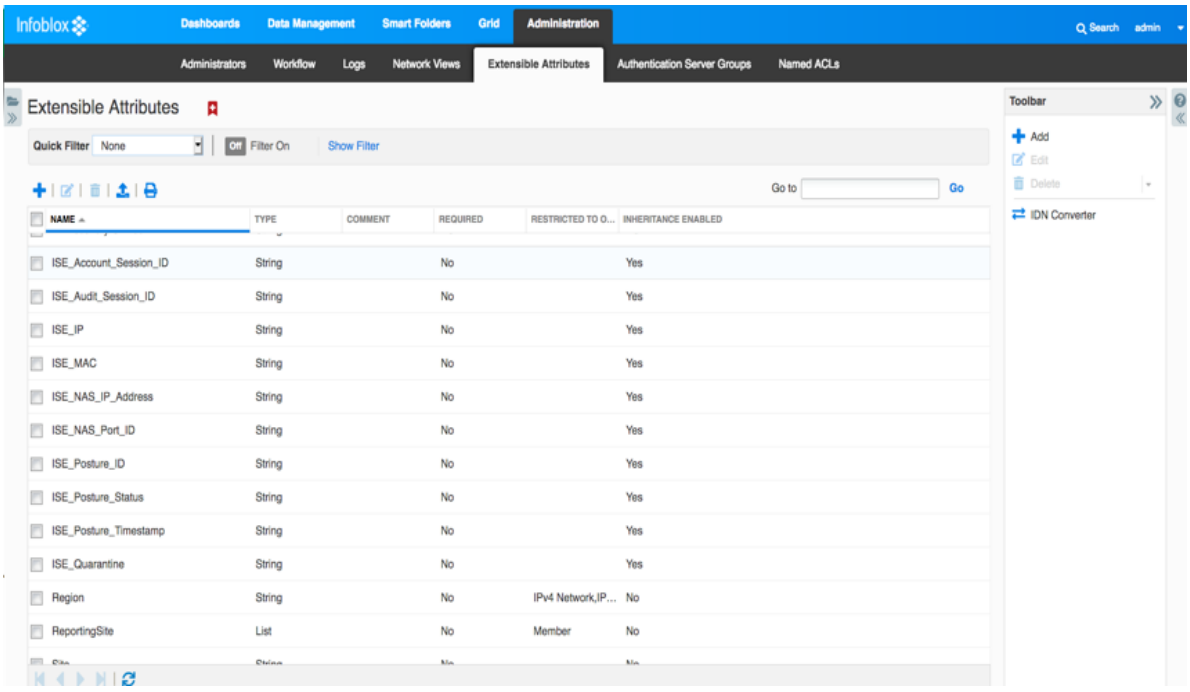
Data	IPAM Source
Attached Device Name	Network Insight
Attached Device Port	Network Insight
Attached Device Model	Network Insight
Attached Device Type	Network Insight
Attached Device Vendor	Network Insight
First Discovered	Network Insight
NetBIOS Name	Network Insight
Port Link	Network Insight
Port Speed	Network Insight
Port Status	Network Insight
VLAN Description	Network Insight
State	Network Insight
Client ID	DHCP

Fingerprint	DHCP
Infoblox Member	DHCP
Lease Start Time	DHCP
Lease State	DHCP
IP Address	IPAM and DHCP
MAC or DUID	IPAM and DHCP
Host Name	DNS

Configuring Extensible Attributes

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. To make it easier to distinguish attributes for ISE subscribed data, preface each name with the name “ISE.”

1. On the grid master, navigate to Administration → Extensible Attributes.



2. Add each extensible attribute that is prefaced by ‘ISE’. Attribute ‘ISE_Quarantine’ will be assigned to the data type EPS_status later in this document. Here are examples of the extensible attributes:

- ISE_Account_Session_ID
- ISE_Audit_Session_ID
- ISE_IP
- ISE_MAC
- ISE_NAS_IP_Address
- ISE_NAS_Port_ID

- ISE_Posture_ID
- ISE_Posture_Status
- ISE_Posture_Timestamp
- ISE_Quarantine

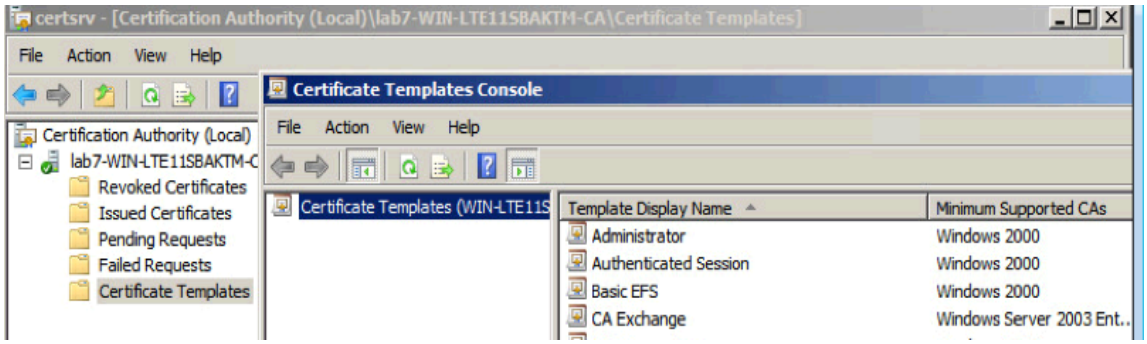
Configuring Certificates using a Certificate Authority

In this example, we will use a Microsoft Certificate Authority. The summary of instructions are:

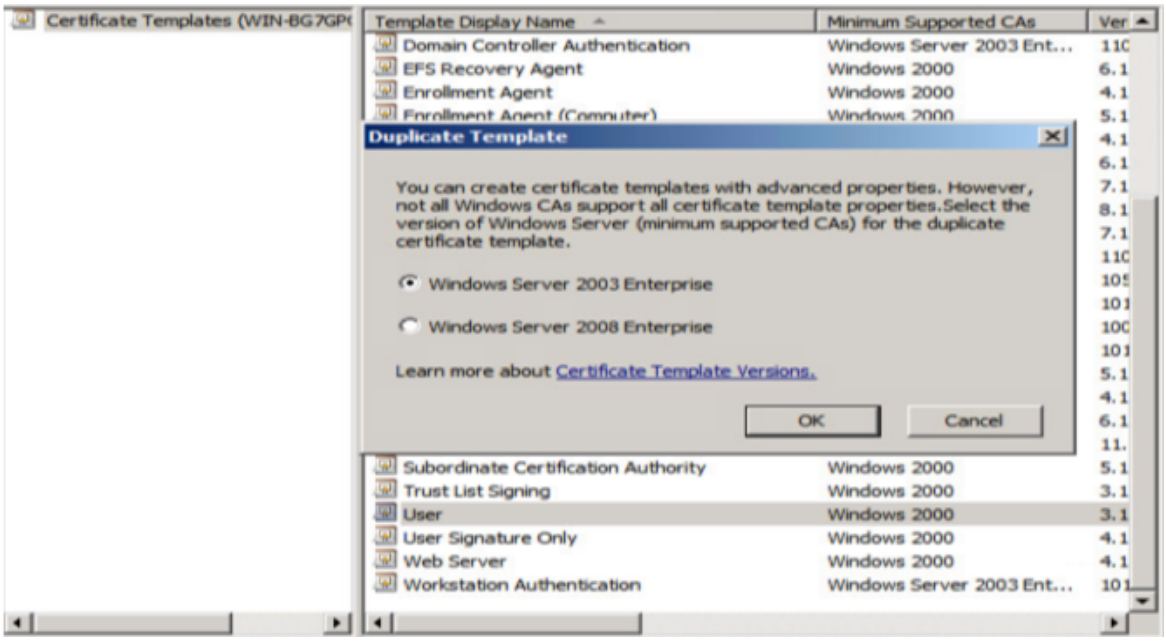
- Configuring a pxgrid template for CA-signed operation.
- Configuring the Infoblox Grid Master for CA-signed certificates.
- Signing the certificate.
- Configuring ISE ecosystem settings on the grid master.

Configuring a pxgrid template for CA-signed operation

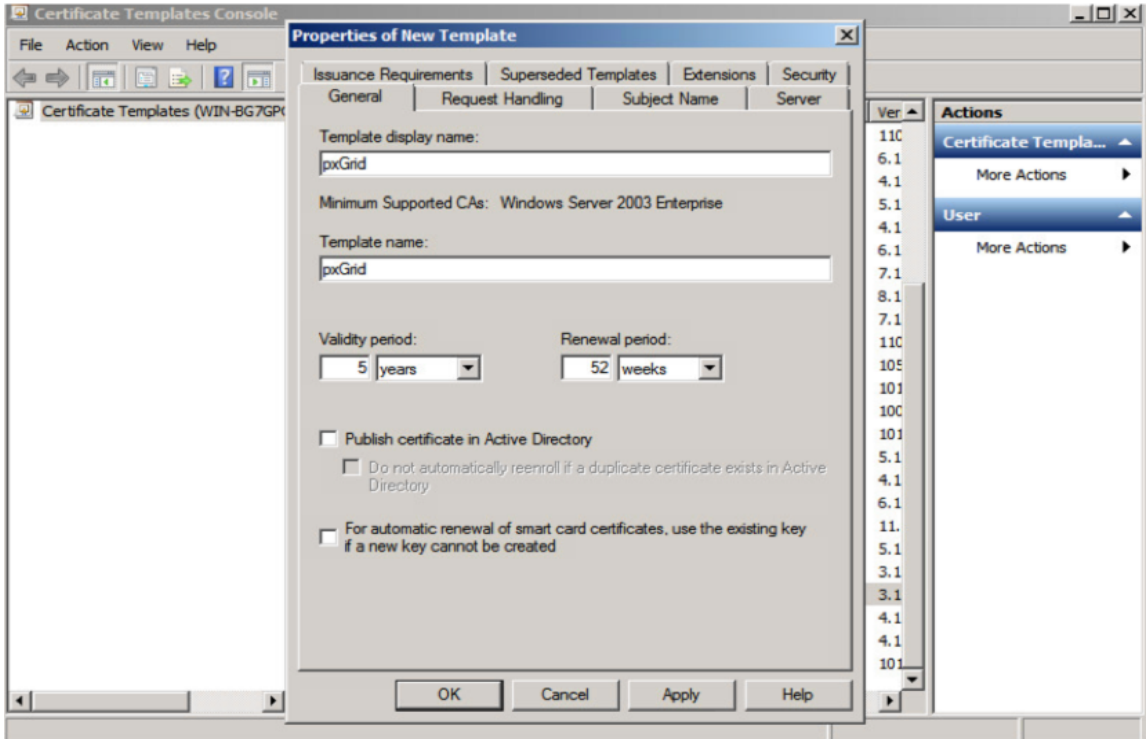
1. Select Administrative Tools->Certificate Authority-> “+” dropdown next to CA server->Right-Click on Certificate Templates->Manage.



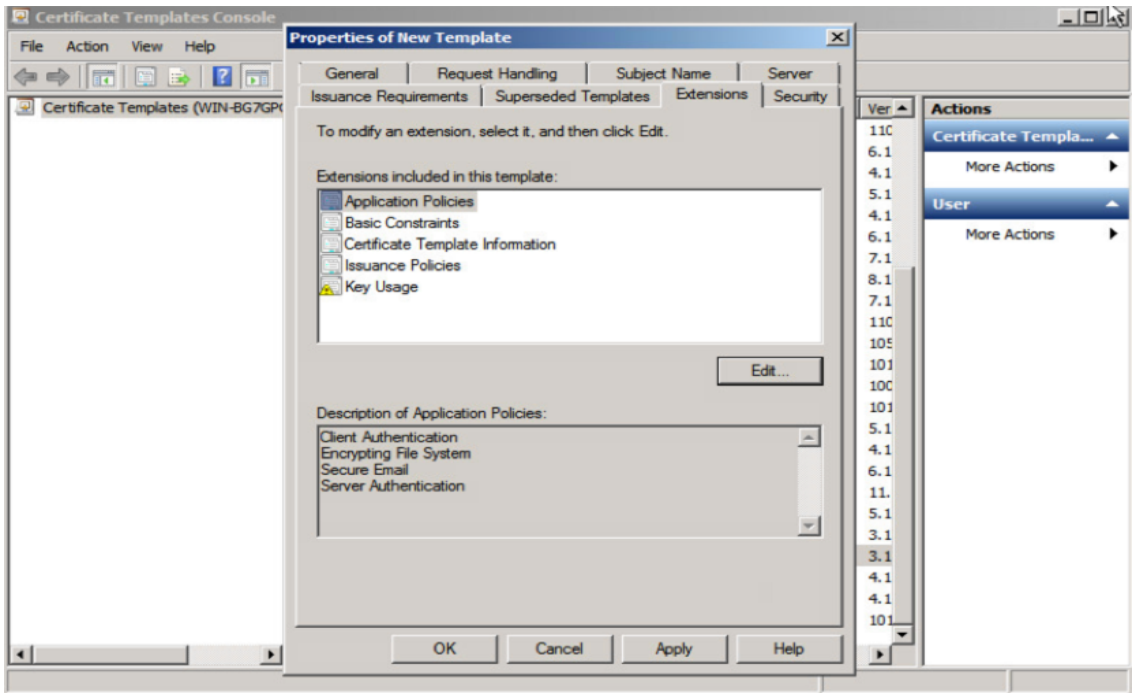
2. Right-Click and Duplicate User template->Windows 2003 Enterprise->OK.



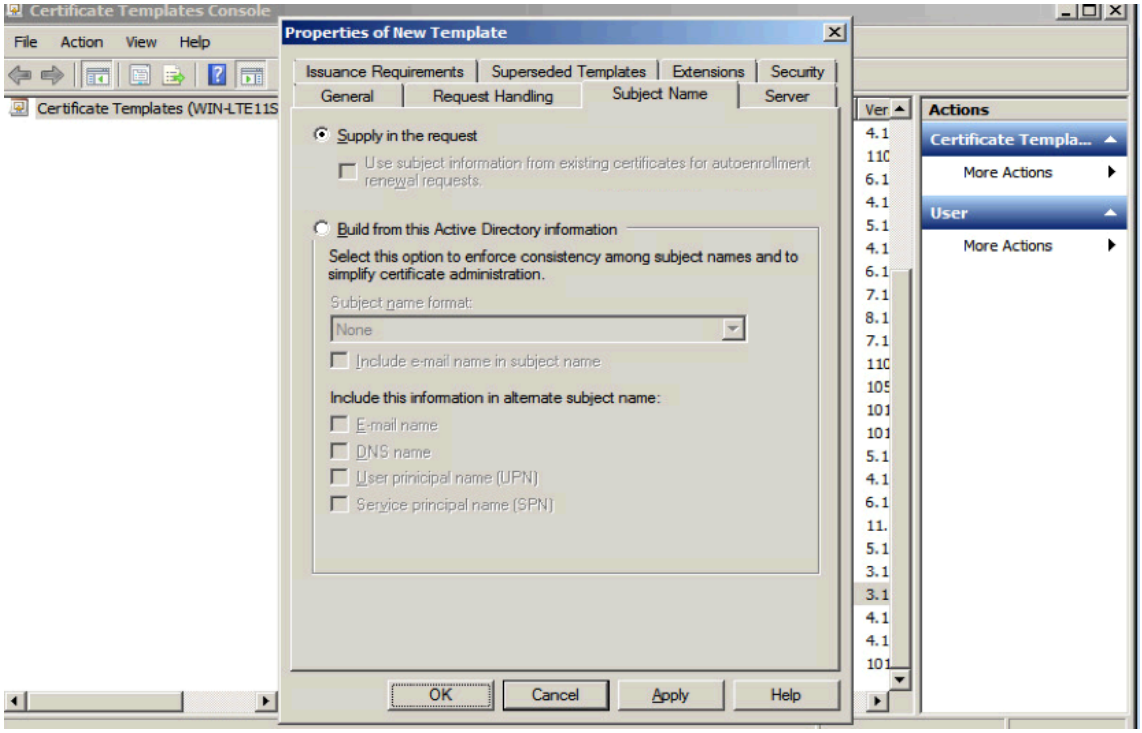
3. Enter name of certificate template, uncheck “Publish certificate in Active Directory”, and provide validity period and renewal period.



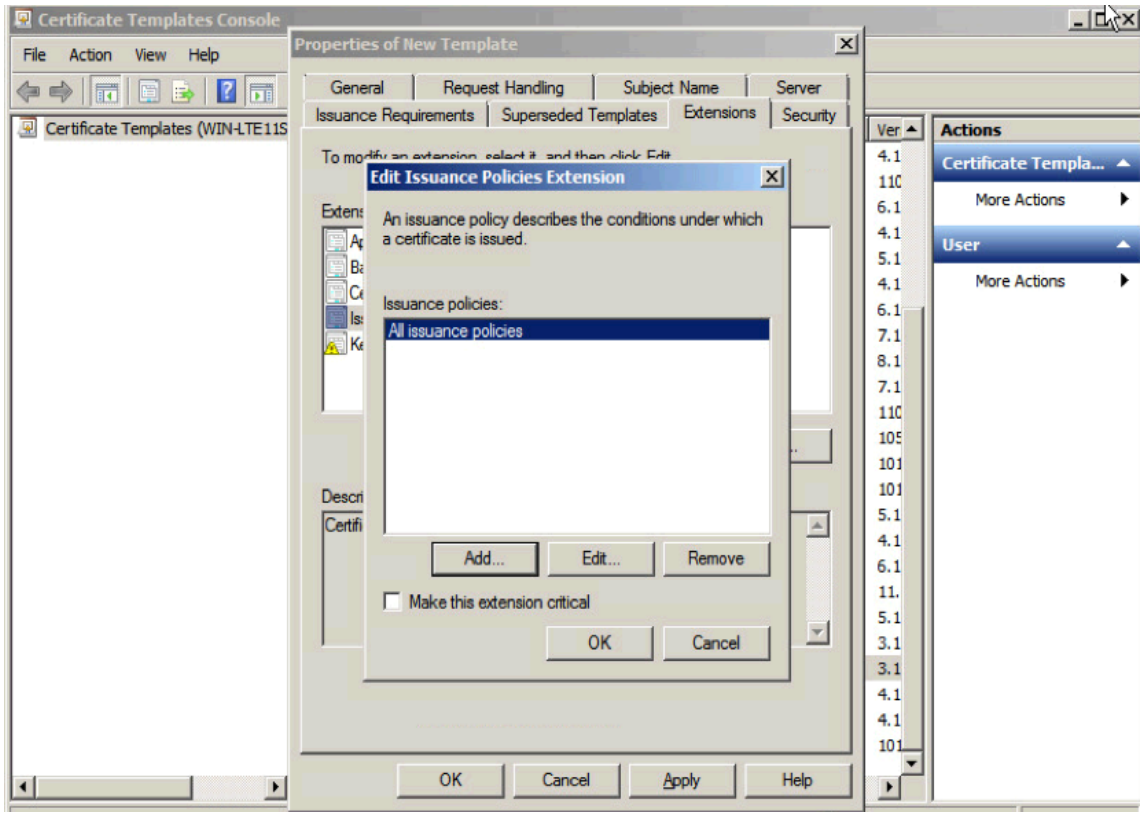
4. Click on Extensions->Add->Server Authentication->Ok->Apply.



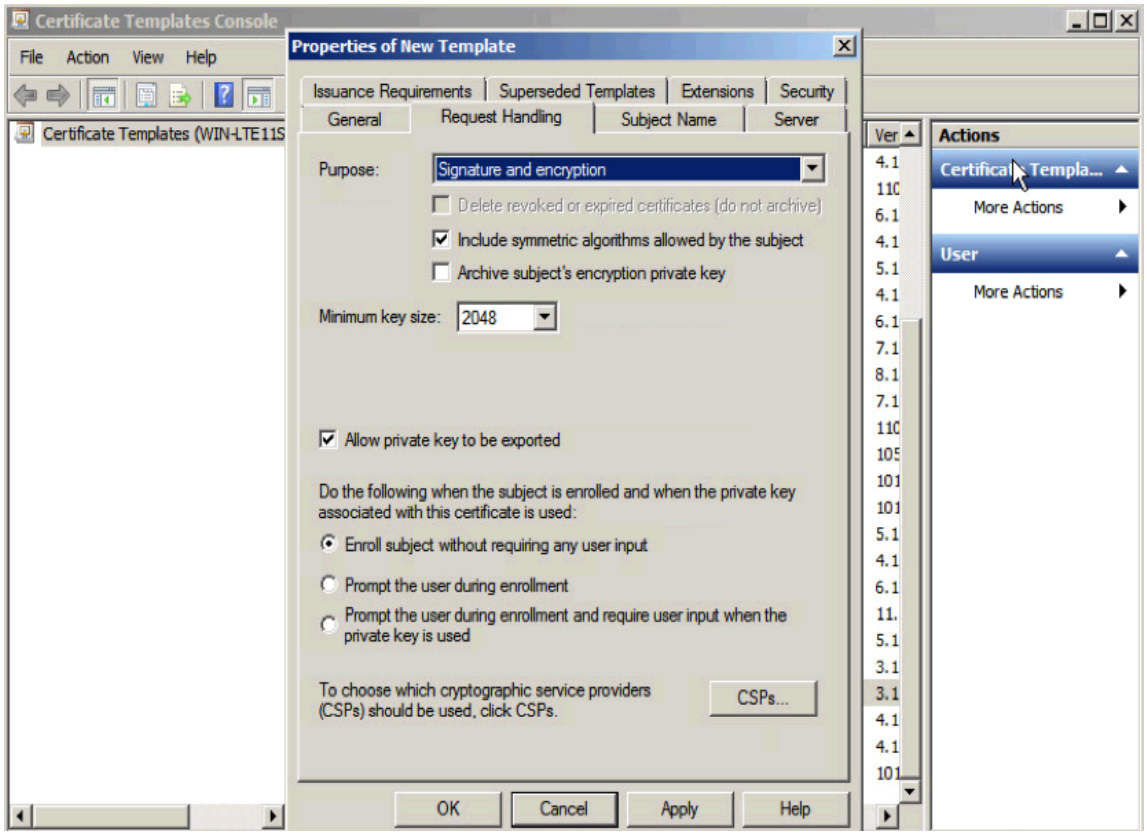
5. Click on Subject name, enable “Supply in the request”.



6. Click on Extensions->Issuance Policies->Edit->All Issuance Policies.

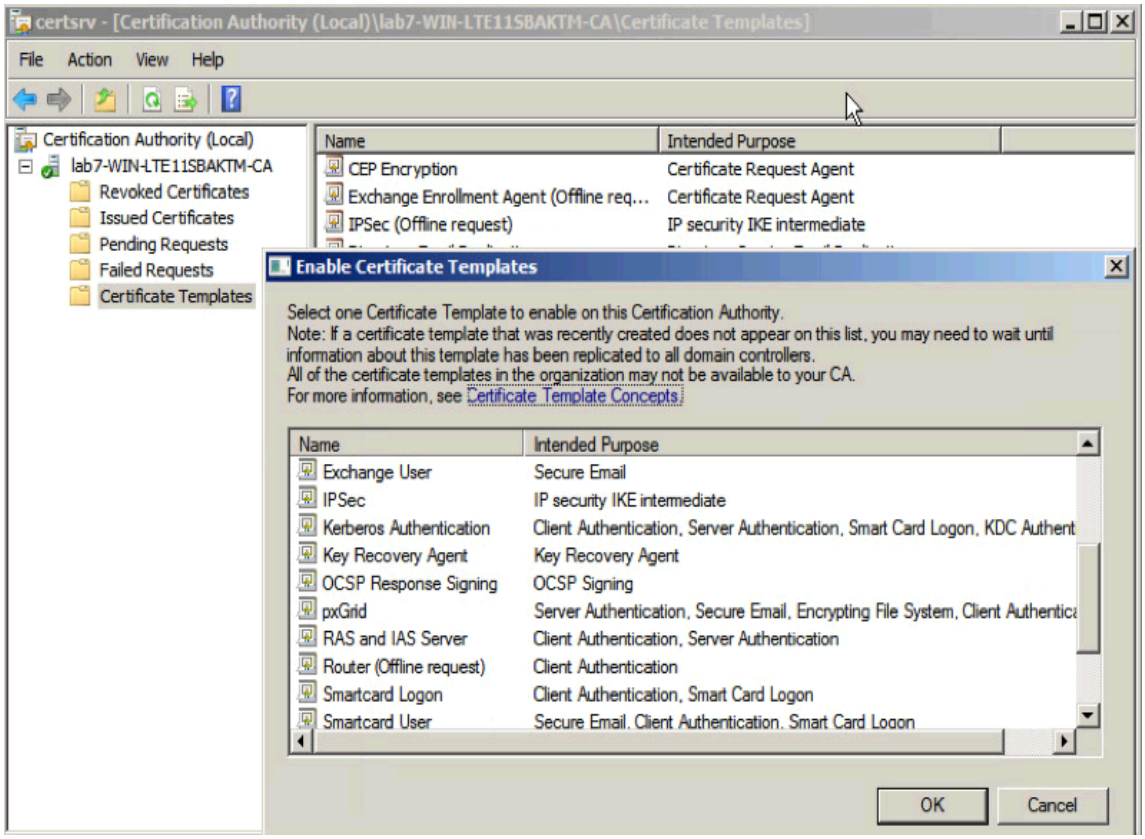


7. Leave the defaults for request handling.

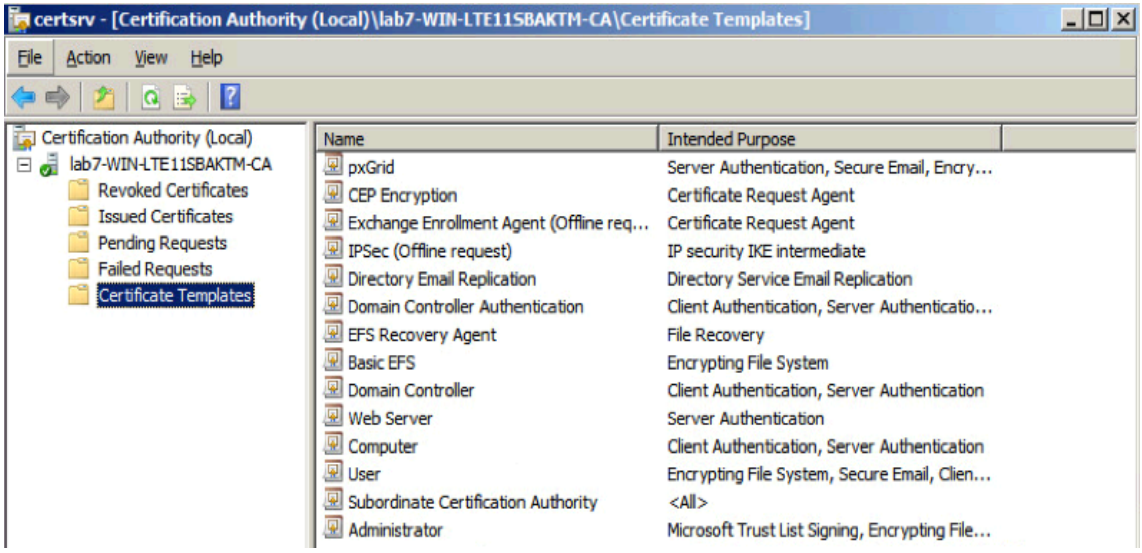


8. Right-click on Certificate Templates.

9. Select New Template to issue and select pxGrid.



10. You should see the pxGrid template.



Configuring Infoblox Grid Master (GM) for CA-signed certificates

This section provides instructions for configuring the Infoblox GM for CA-signed certificate operation.
The instructions are:

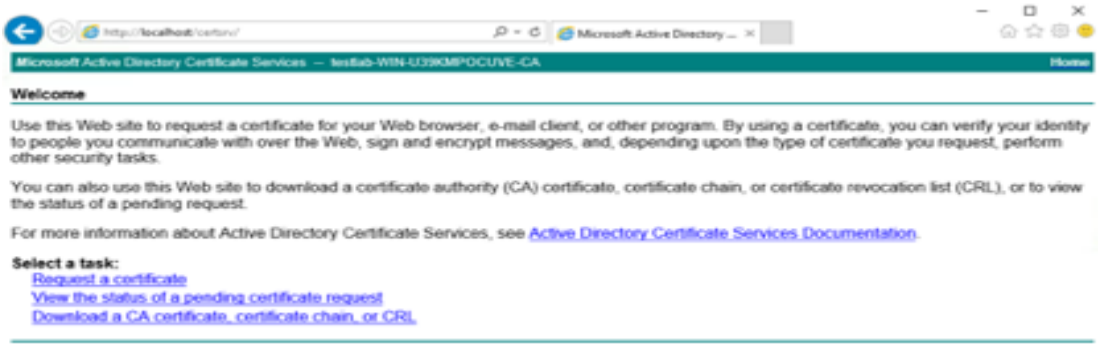
1. Generating a public-private key pair and CSR request for the Infoblox GM. You must use the name of the Grid Master during the creation of the key pair and CSR.
2. Generating the certificate from the Microsoft CA server.
3. Uploading the root CA certificate into the Infoblox trusted store.
4. Configuring ISE ecosystem parameter settings with the Infoblox concatenated certificate and ISE pxGrid node IP address.

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.

Note: The following commands are executed on a MAC or Linux system.

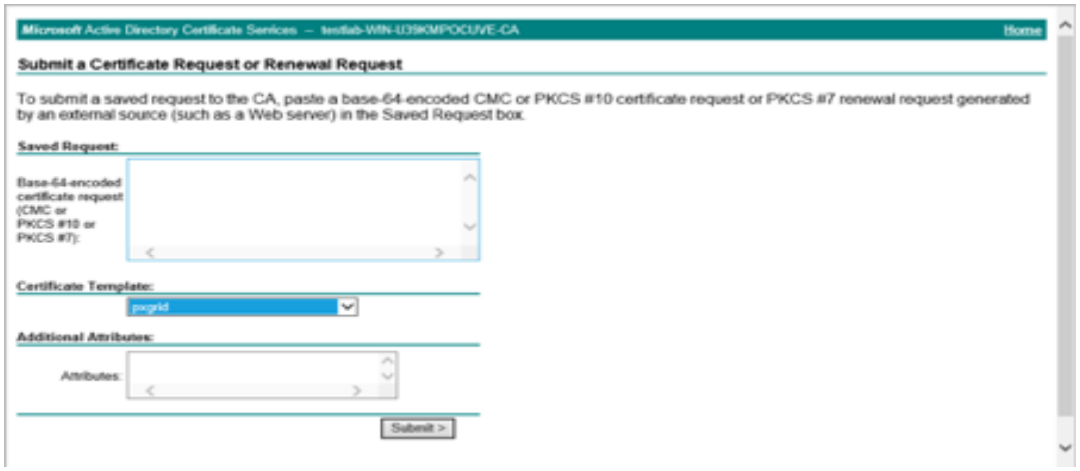
1. Execute the following command to generate the private key: openssl genrsa -out <key filename> 4096.
2. Execute the following command to generate the CSR request: openssl req -new -key <key filename> -out <CSR filename>. Answer all of the prompts**. The most important prompt is Common Name. This has to be the name of the grid master or grid member. Ensure all of the components in this ISE deployment (ie grid master, CA server, and ISE environment) all have the same domain name.**
3. Open the CSR file in an editor and highlight and copy the CSR information including the header and footer or upload this file to the Microsoft CA server.
4. Bring up the CA server from a browser in the Microsoft GUI.



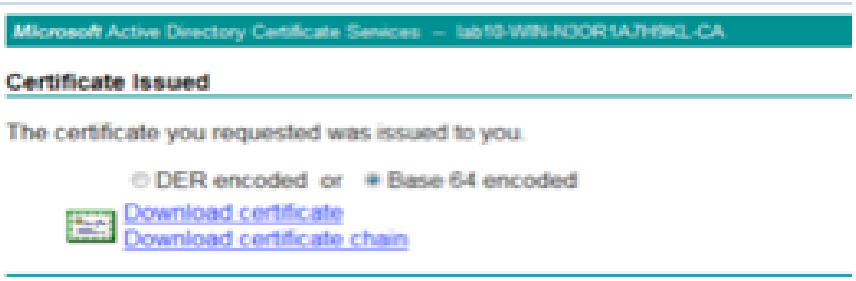
5. Click on ‘Request a certificate’.

6. Click on ‘advanced certificate request’.

7. Click on ‘Submit a certificate request’.

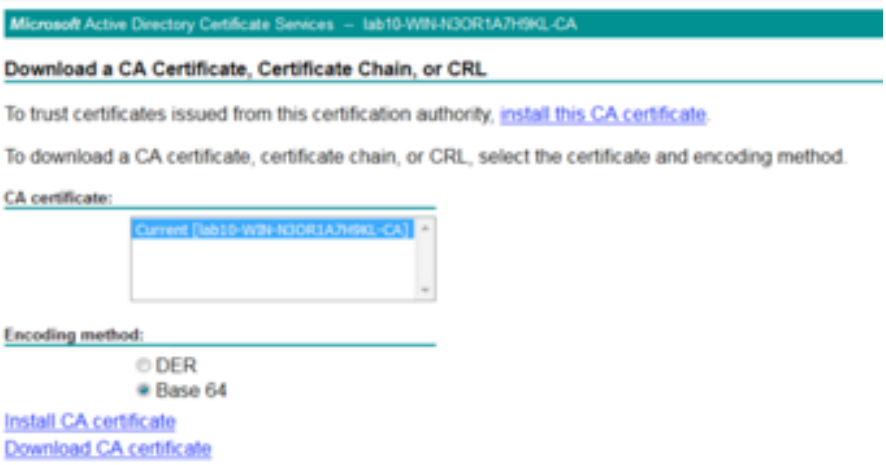


8. Paste the information in the CSR into the ‘Saved Request’ box. Select the newly created certificate template. Click Submit.
9. Select Base 64-encoded.



10. Select ‘Download certificate’.
11. Download the root certificate. This root certificate should be in the ISE certificate trusted store.

12. Download the certificate in Base 64 format.

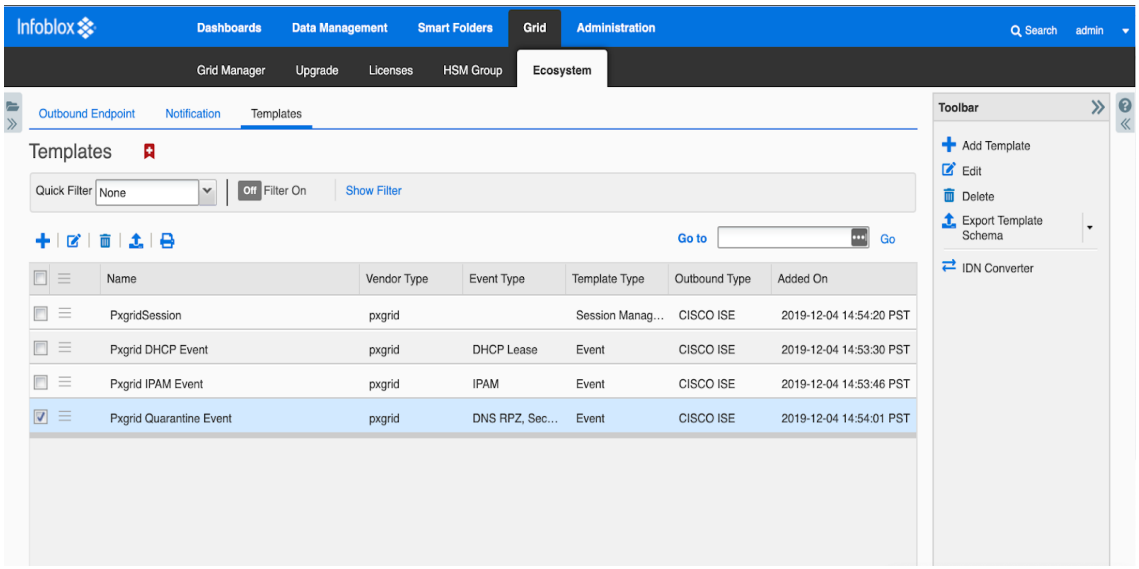


13. Select ‘Download CA certificate’.

14. Concatenate the private key and public certificate into one file with the following command: cat <signed certificate filename from CA server> <key filename> > <filename.pem>. **You must concatenate in this order.**
15. Upload this certificate to the ISE server trusted store.

Configuring ISE ecosystem settings on the grid master or grid master candidate.

1. Navigate to Grid → Ecosystem → Templates.



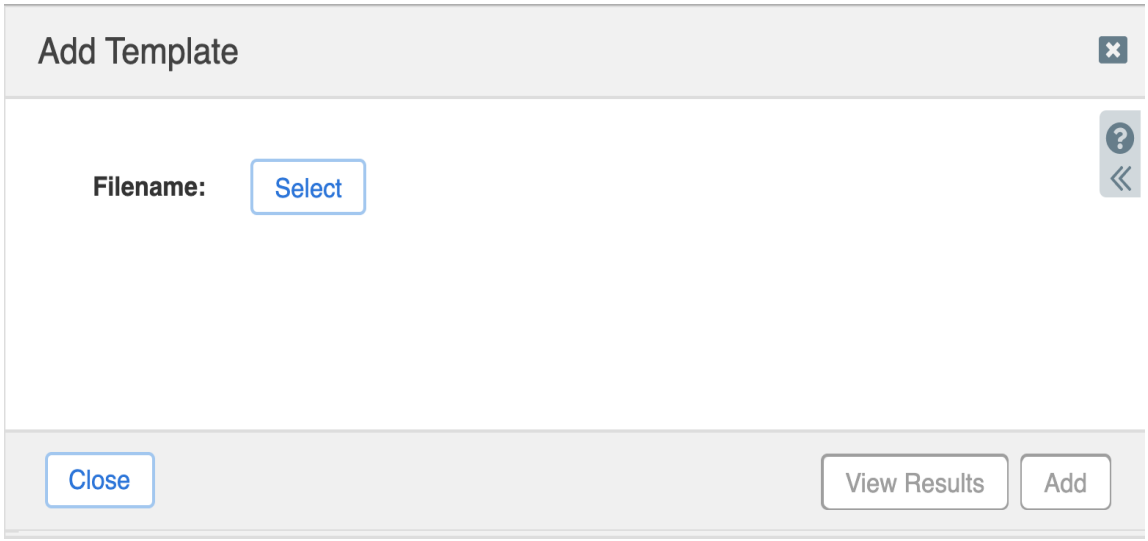
2. Create the following outbound notification templates in a text file.:

```
PxgridSession
	{
	"version": "6.0",
	"vendor_identifier": "pxgrid",
	"name": "PxgridSession",
	"type": "PXGRID_ENDPOINT",
	"comment": "Pxgrid session template",
	"path": "/wapi/v2.9/",
	"override_path": true,
	"timeout": 123,
	"keepalive": true,
	"retry": 4,
	"retry_template": 2,
	"rate_limit": 200
}
Pxgrid DHCP Event
{
	"version": "6.0",
	"name": "Pxgrid DHCP Event",
	"type": "PXGRID_EVENT",
	"event_type": ["LEASE"],
	"action_type": "Pxgrid Action IPAM",
	"comment": "Pxgrid template",
	"content_type": "application/json",
	"vendor_identifier": "pxgrid",
	"headers": {
	"User-Agent": "Outbound API 0.1 rrtest"
	},
	"transport": {
	"path": "/wapi/v2.9",
	"content_type": "application/json",
	"override_path": true
	},
	"steps":
	[
	{
		"name": "DHCP event",
		"operation": "PX_SEND_DHCP_LEASES"
	}
	]
}
Pxgrid IPAM Event
{
	"version": "6.0",
	"name": "Pxgrid IPAM Event",
	"type": "PXGRID_EVENT",
```

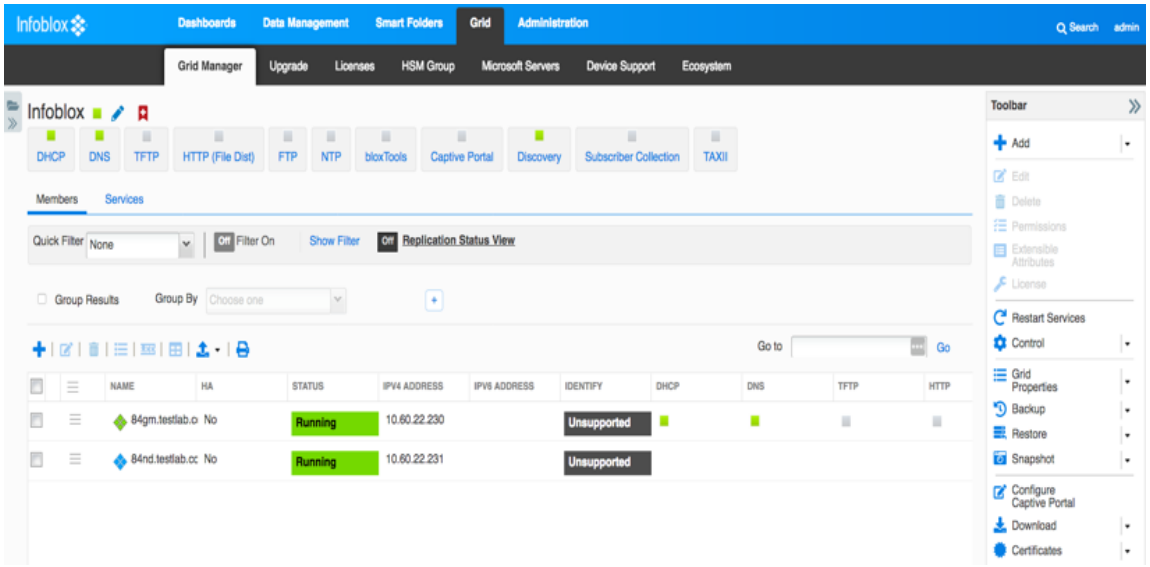
```
        "event_type": ["IPAM"],
        "action_type": "Pxgrid Action IPAM",
        "comment": "Pxgrid template",
        "content_type": "application/json",
        "vendor_identifier": "pxgrid",
        "headers": {
        "User-Agent": "Outbound API 0.1 rrtest"
        },
        "transport": {
        "path": "/wapi/v2.9",
        "content_type": "application/json",
        "override_path": true
        },
        "steps":
        [
        {
                "name": "IPAM event",
                "operation": "PX_SEND_IPAM"
        }
        ]
}
        Pxgrid Quarantine Event
        {
        "version": "6.0",
        "name": "Pxgrid Quarantine Event",
        "type": "PXGRID_EVENT",
        "event_type": ["RPZ","ADP"],
        "action_type": "Pxgrid Action IPAM",
        "comment": "Pxgrid template",
        "content_type": "application/json",
        "vendor_identifier": "pxgrid",
        "headers": {
        "User-Agent": "Outbound API 0.1 rrtest"
        },
        "transport": {
        "path": "/wapi/v2.9",
        "content_type": "application/json",
        "override_path": true
        },
        "steps":
        [
        {
                "name": "Quarantine",
                "operation": "PX_SEND_QUARANTINE"
        }
        ]
```

```
}
```

3. Click on the '+' button to add the templates.

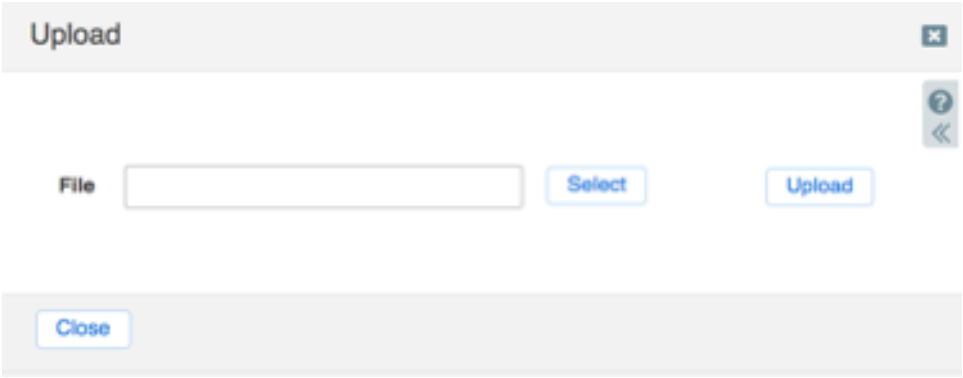


4. Navigate Grid --> Grid Manager --> Members --> Toolbar -->Certificates.

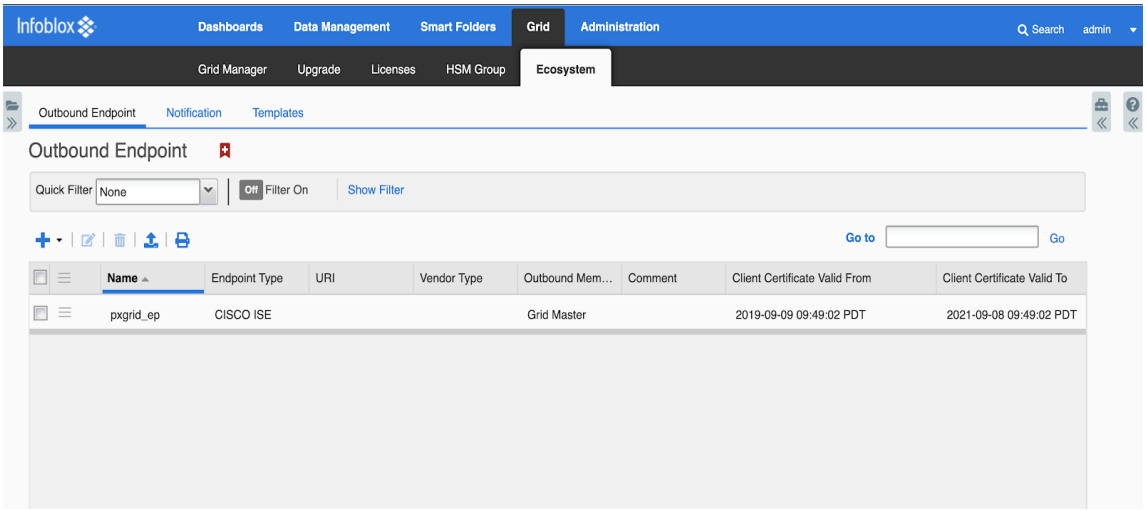


5. From the Certificates drop down menu, select 'Manage Certificates'.

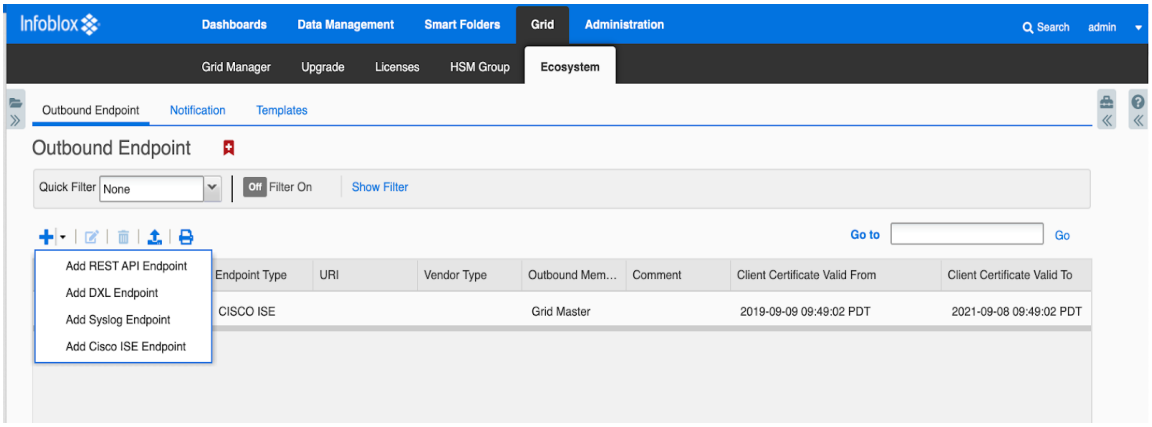
6. Click on the '+' button to add the root certificate.



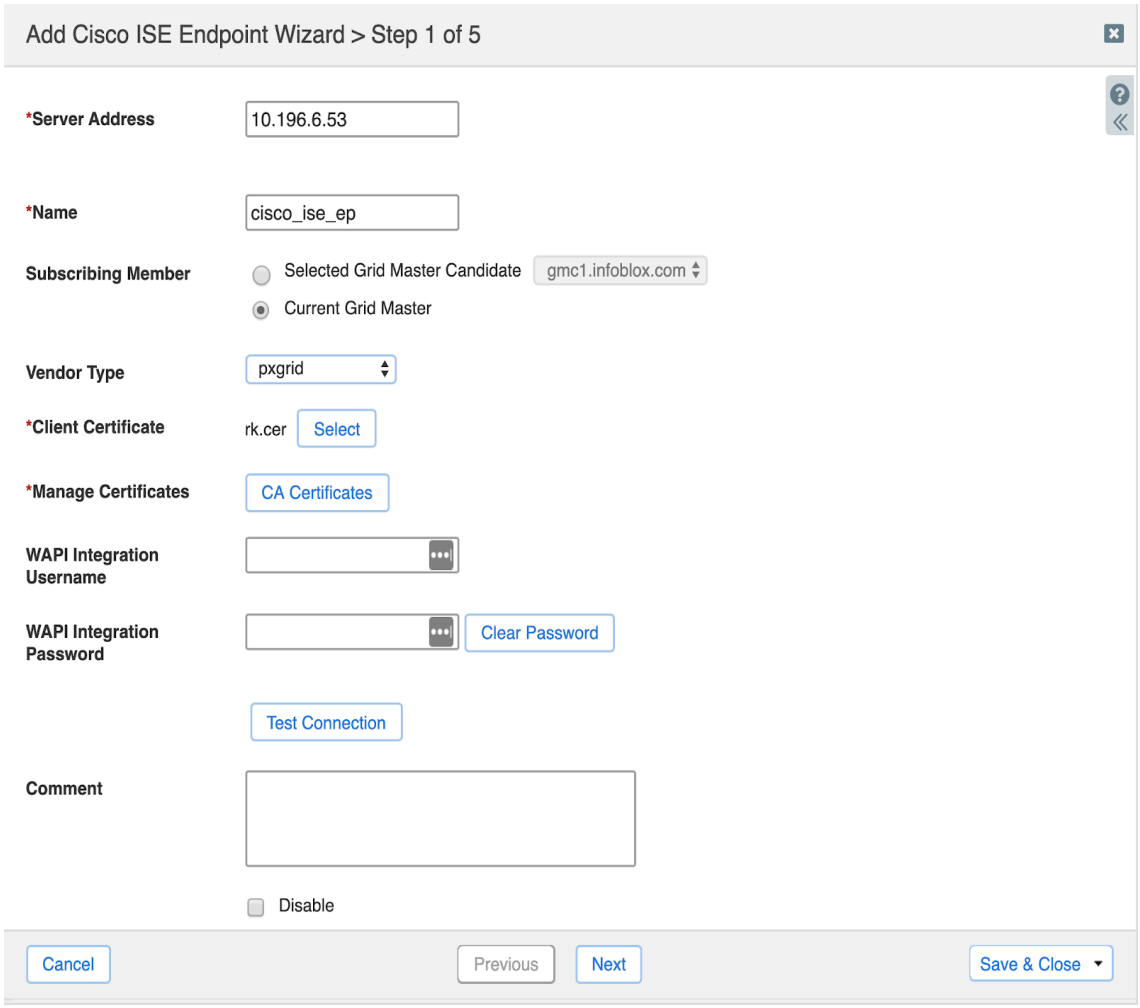
7. Click on the 'Select' button to file the root certificate. Click 'Upload'.
8. Click 'Close'.
9. Navigate to Grid → Ecosystem → Outbound Endpoint.



10. Click on the '+' button and select 'Add Cisco ISE Endpoint

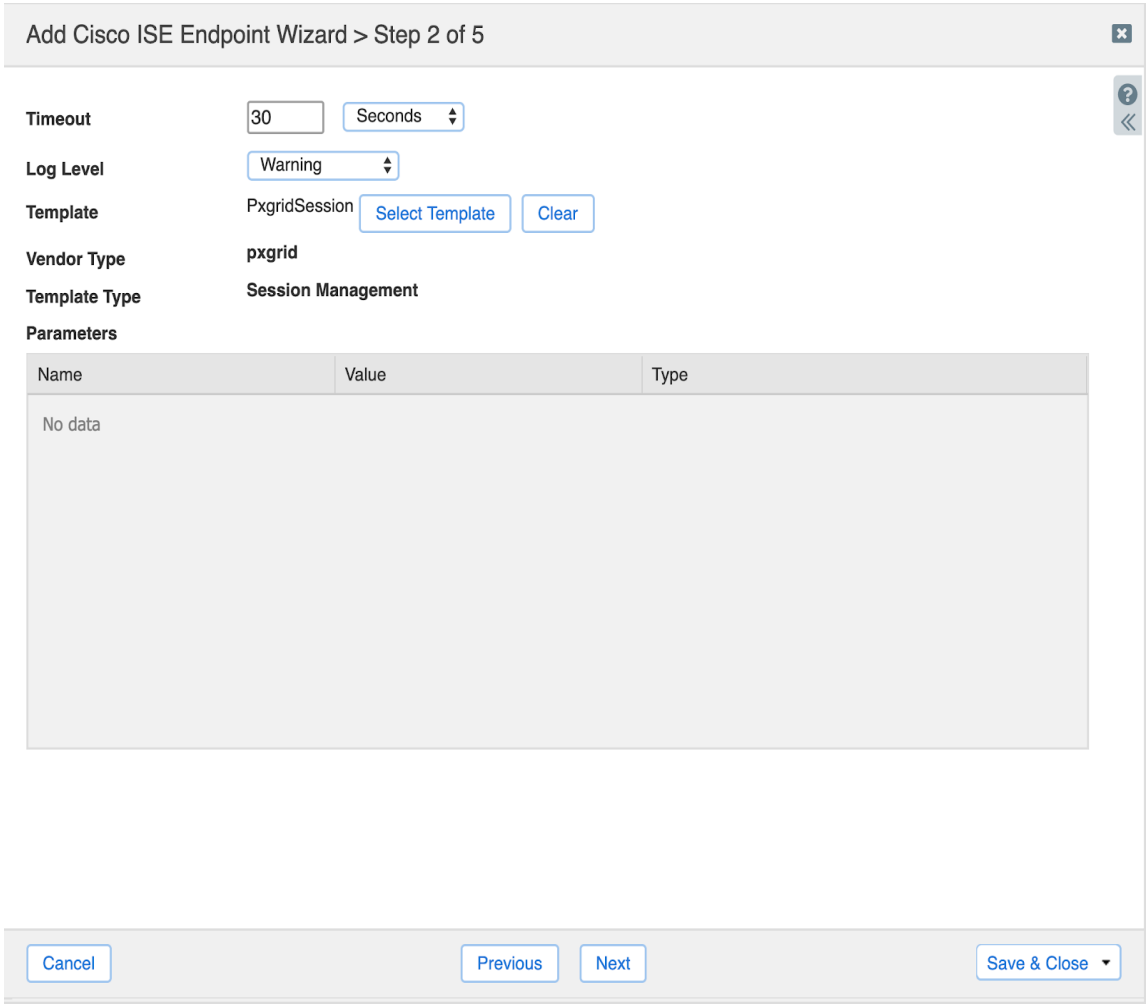


11. You will see the following screen.

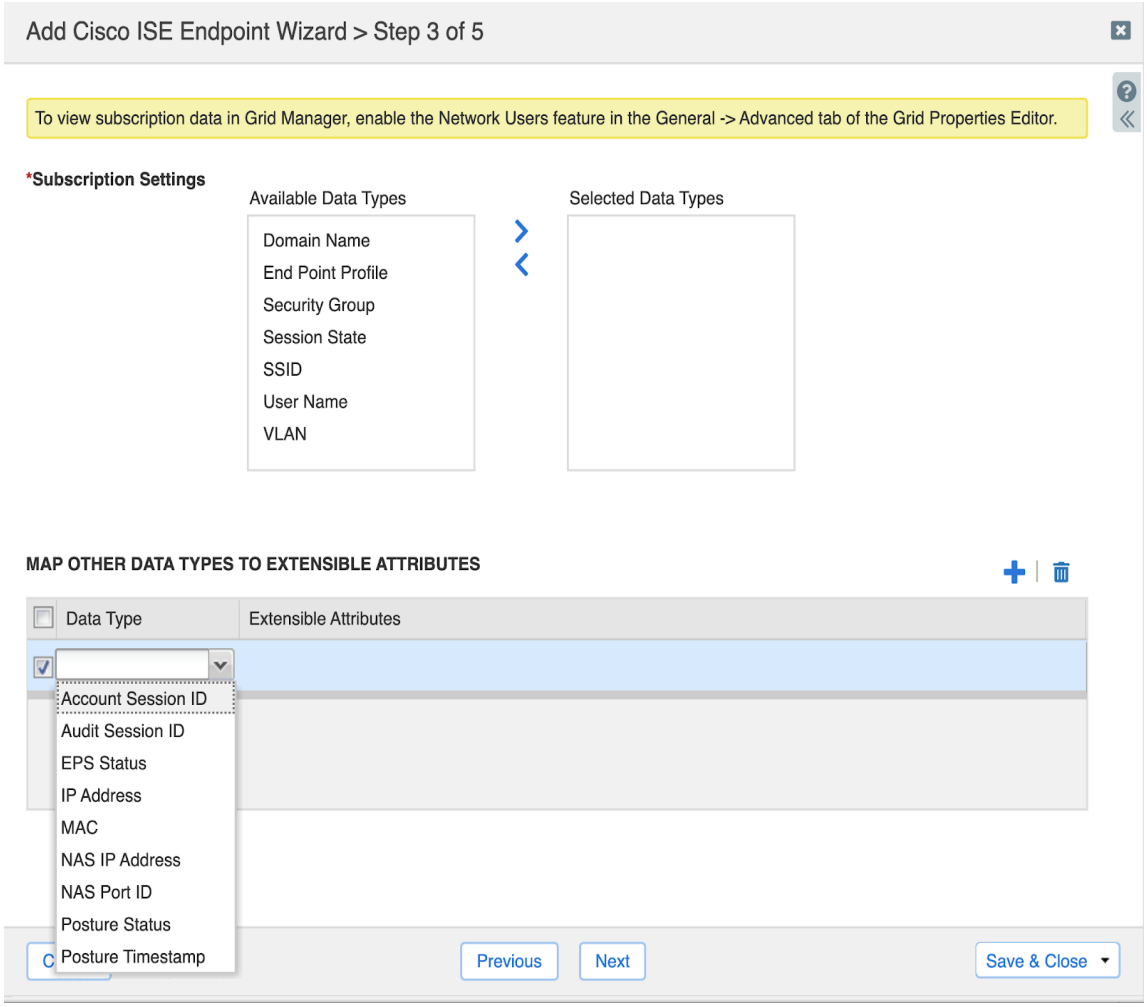


12. Add the Cisco ISE server IP address or host name. If you are running a multi-node pxgrid, then the IP address of the ISE server will be the primary pxGrid node. Enter the name of this entry. Selected member will be responsible for subscribing/publishing information from/to Cisco ISE server. Client certificate should be uploaded accordingly. Select ‘pxgrid’ as ‘Vendor Type’. Upload the client certificate. Enter the WAPI Integration Username. Enter the WAPI Integration Password. Note: if you have included at least one "wapi" related field in your action template, you must configure WAPI integration; otherwise the WAPI step fails due to an authorization error. Enter the username of the admin user you want to designate for Cisco ISE outbound notifications. The appliance ignores the **Auth Username** and **Auth Password** for WAPI related steps in any action templates if WAPI integration is configured.
13. You can now click ‘Test Credentials’ button. It should come back as successful. If not, then check that you have uploaded the client certificate and root certificate to the ISE server certificate trusted store. Leave the timeout section and log level at default or change it. Click on ‘Select

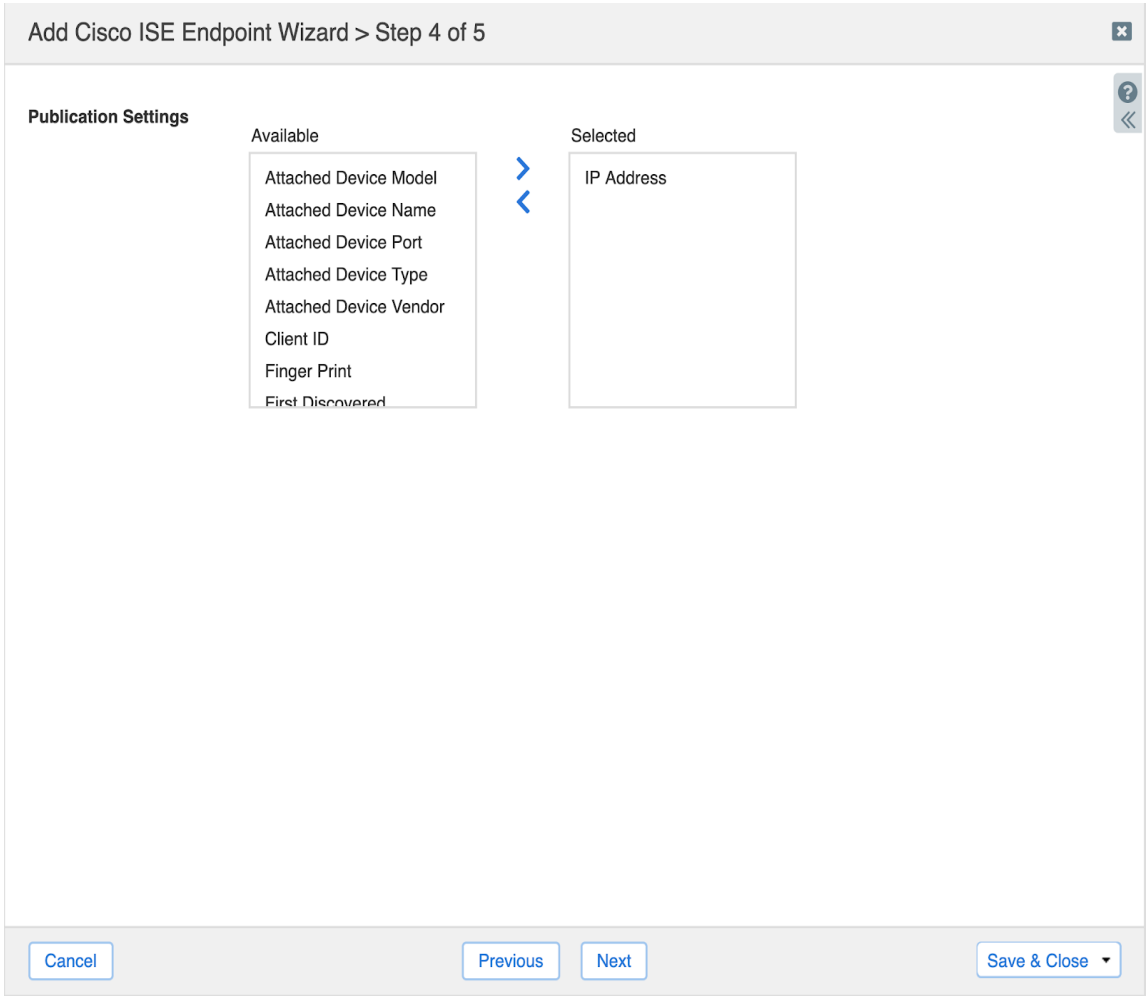
Template’ button. Click Next.



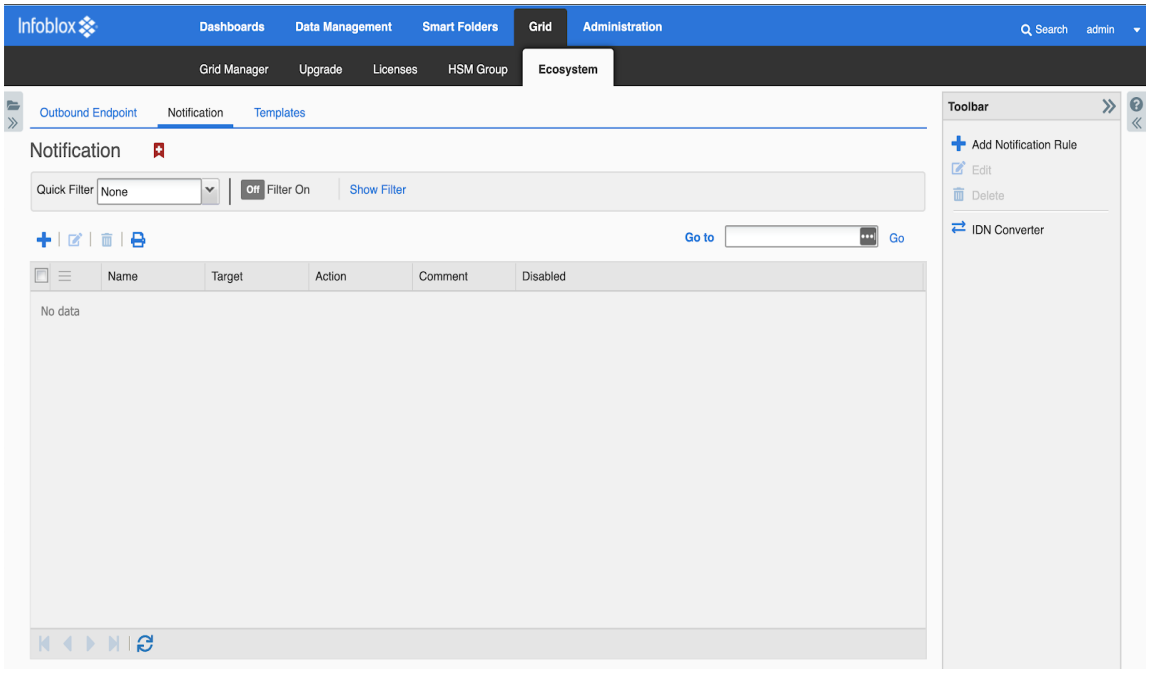
14. Select the Data Types that you want to subscribe and map any or all data types to extensible attributes. These extensible attributes can be used in the IPAM GUI. Click Next.



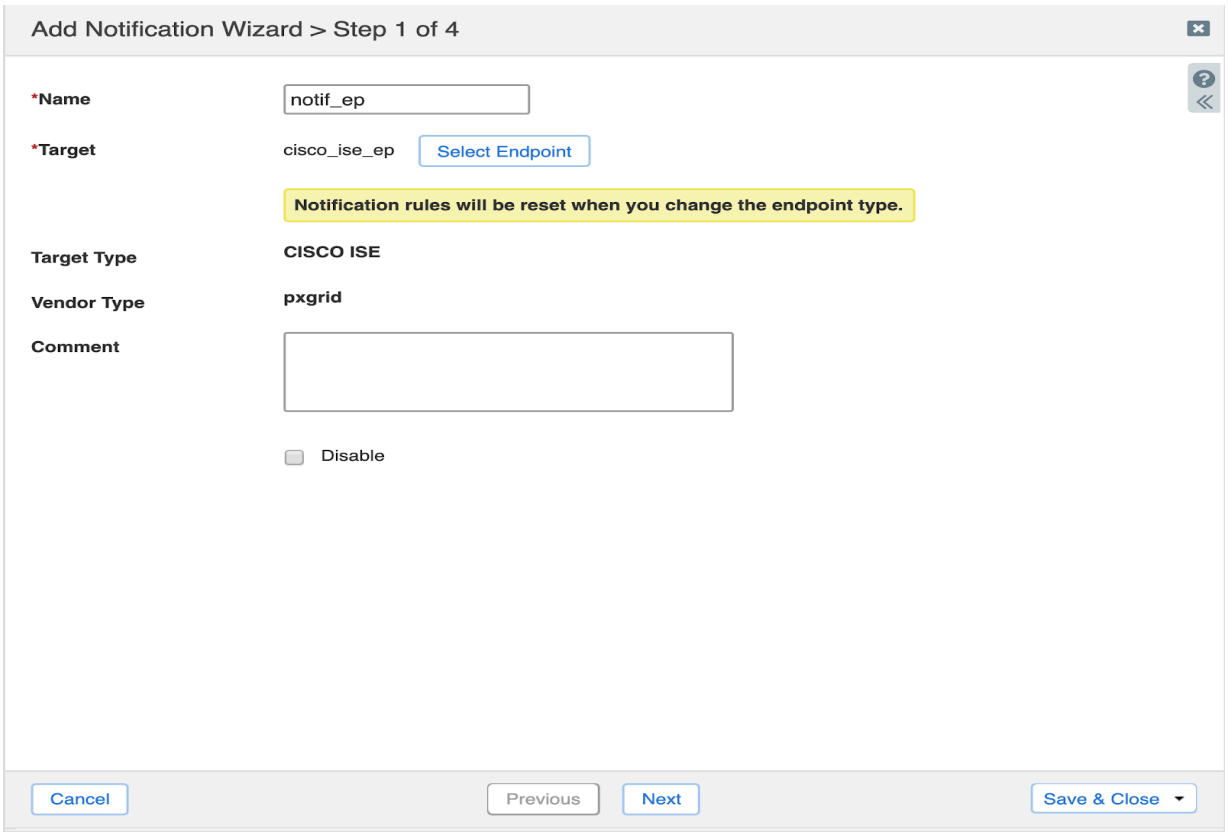
15. Select the items that you want to publish to the PxGrid. Click ‘Save & Close’.



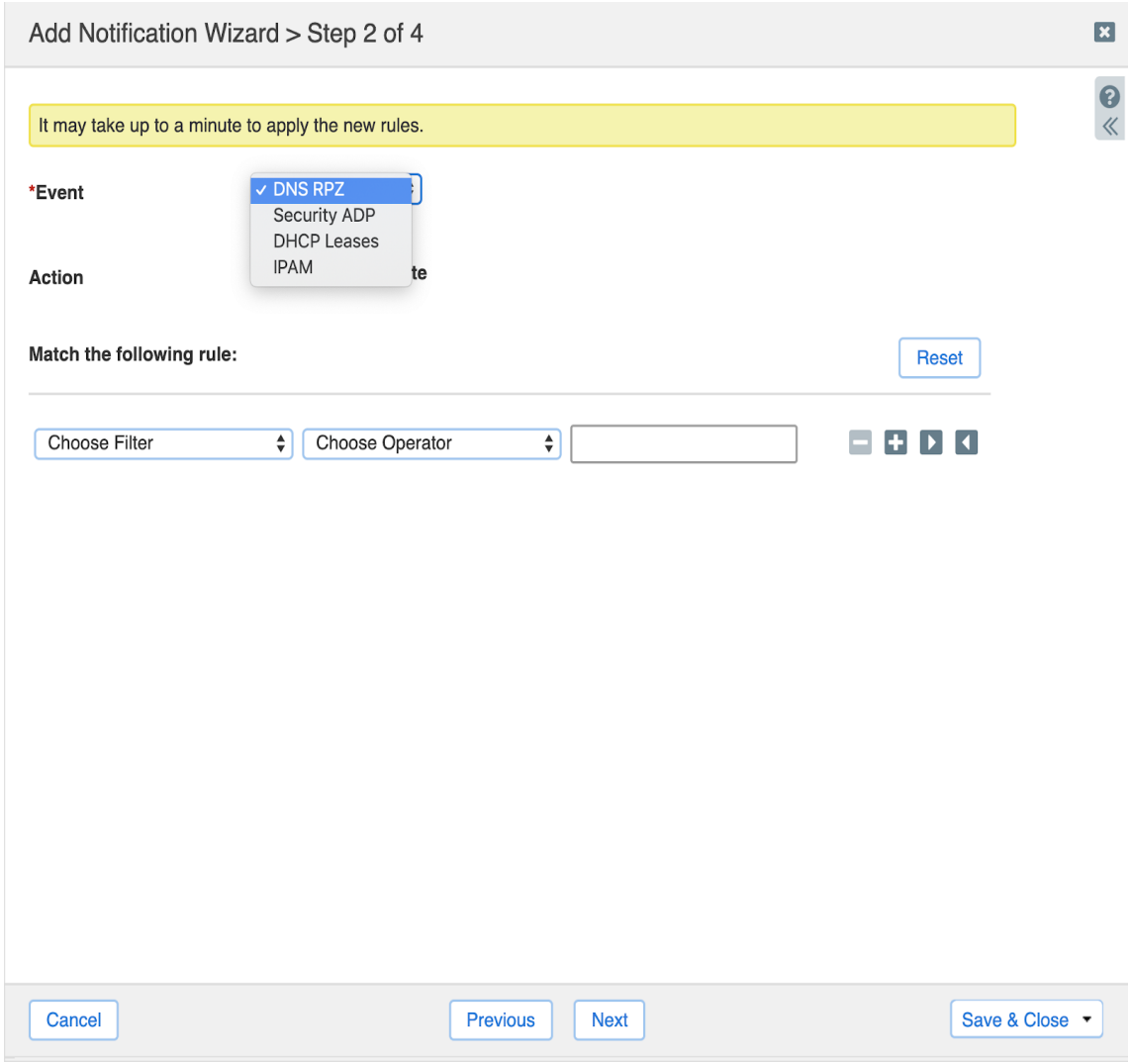
16. Click on the Notification tab.



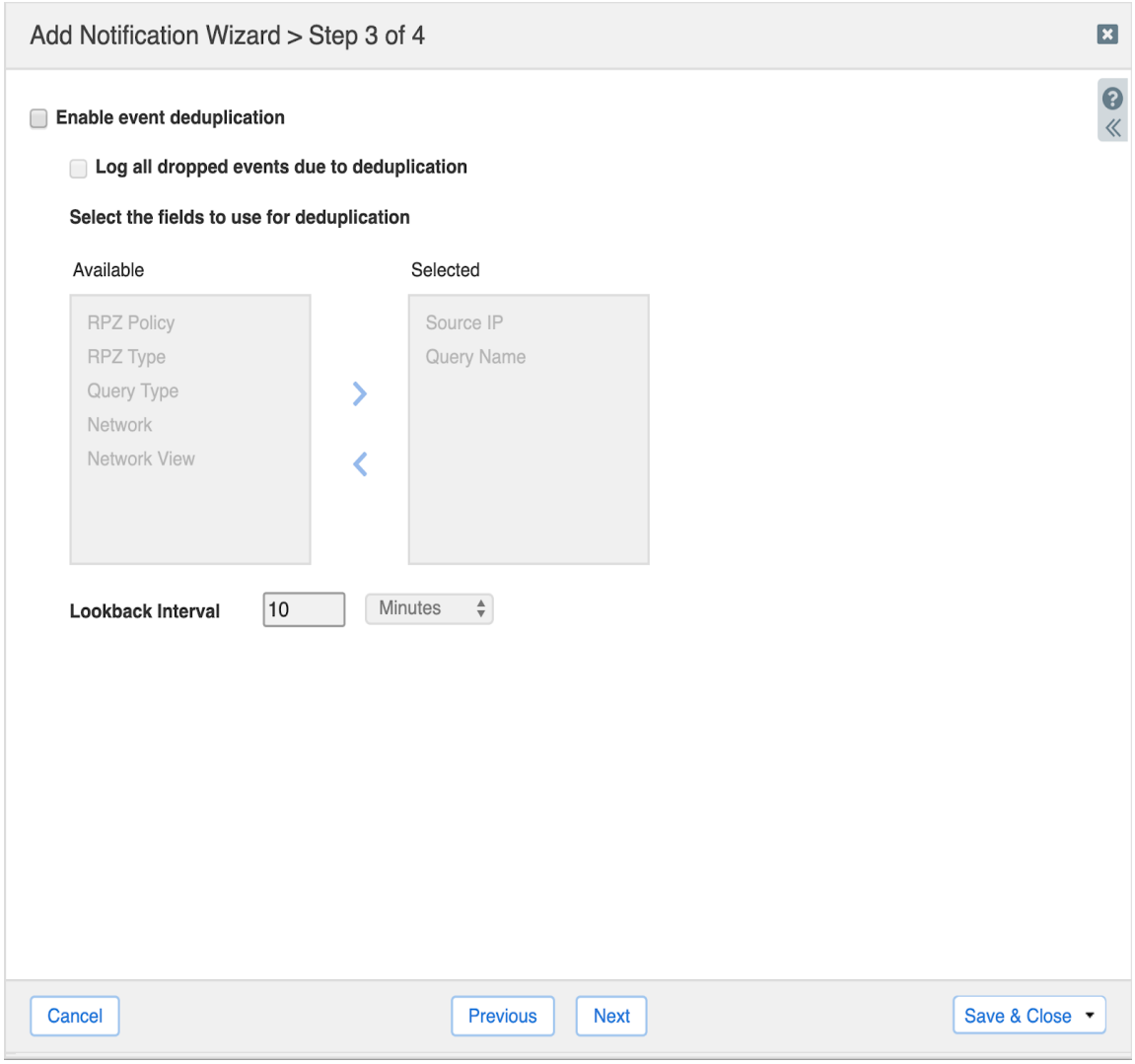
17. Click on '+' button to add a notification. Type in the name. Select the endpoint. Click Next.



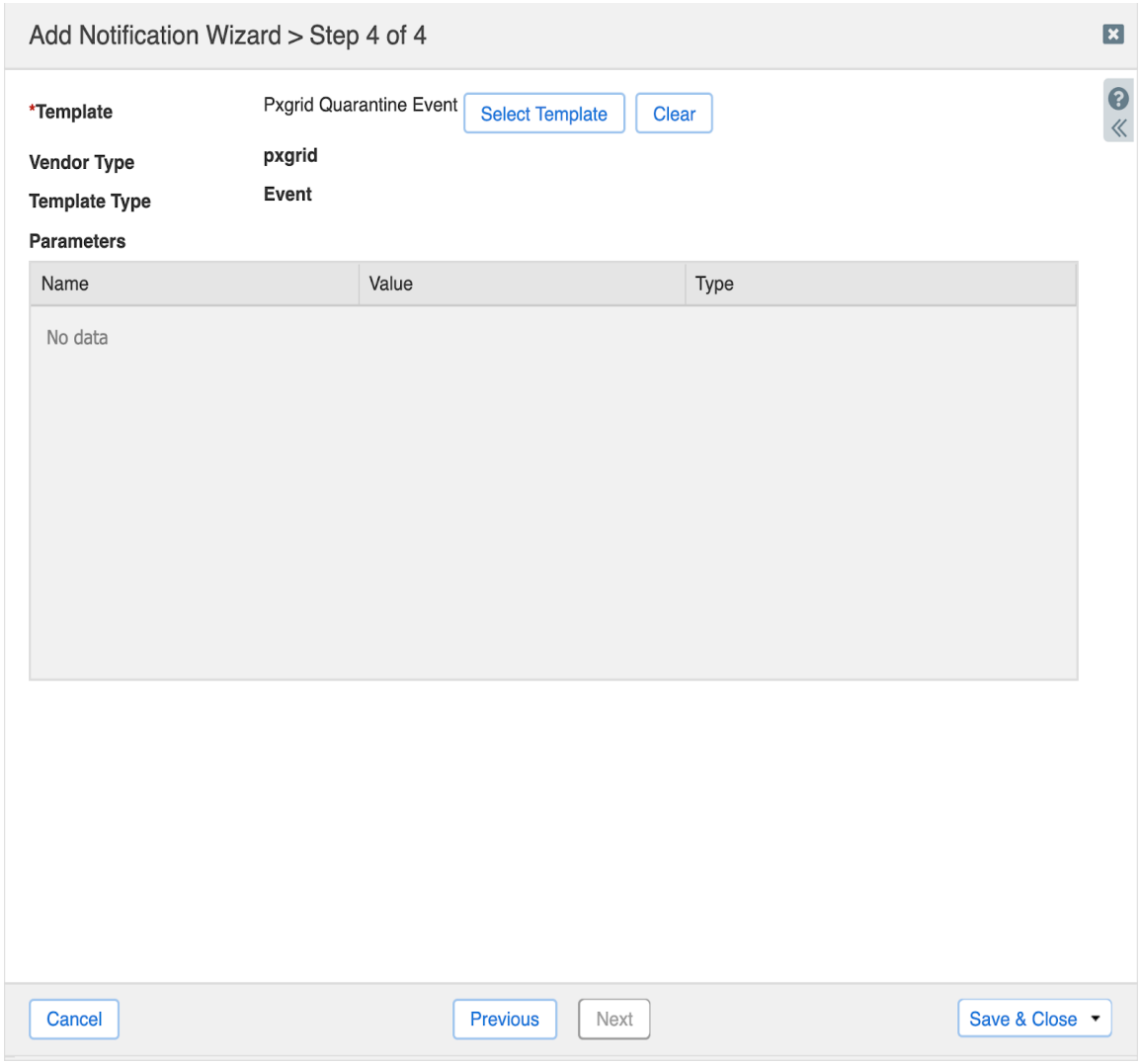
18. Select the event type. The actions and rule template will change accordingly. Fill in the actions or rules. Click Next



19. Enable event deduplication if you wish. It is only relevant for DNS RPZ, Security ADP events, Click Next.



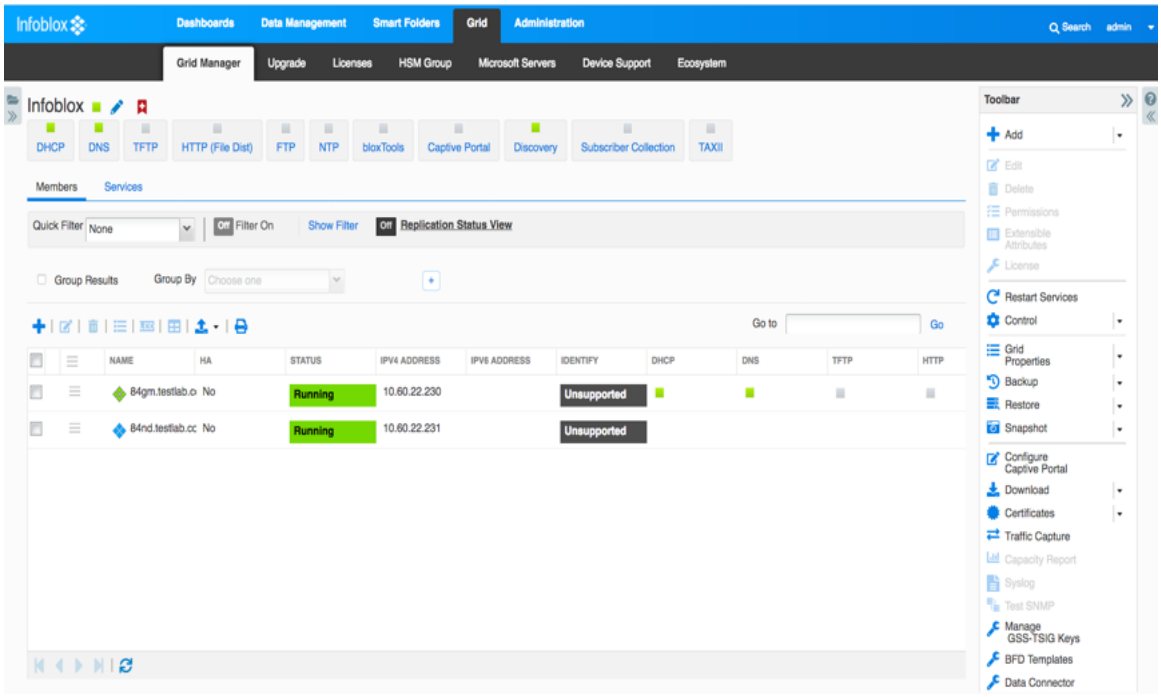
20. Click on Select Template. Click ‘Save and Close’.



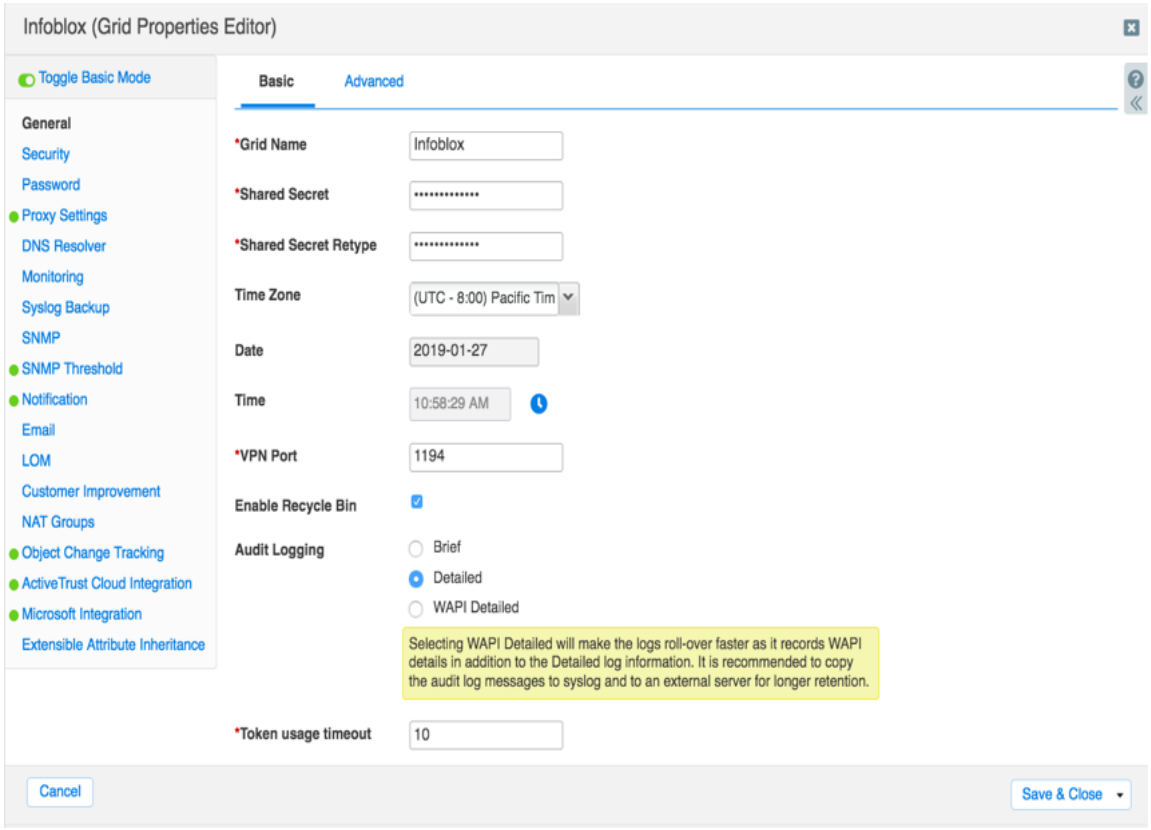
Enabling Data Management Network Users

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

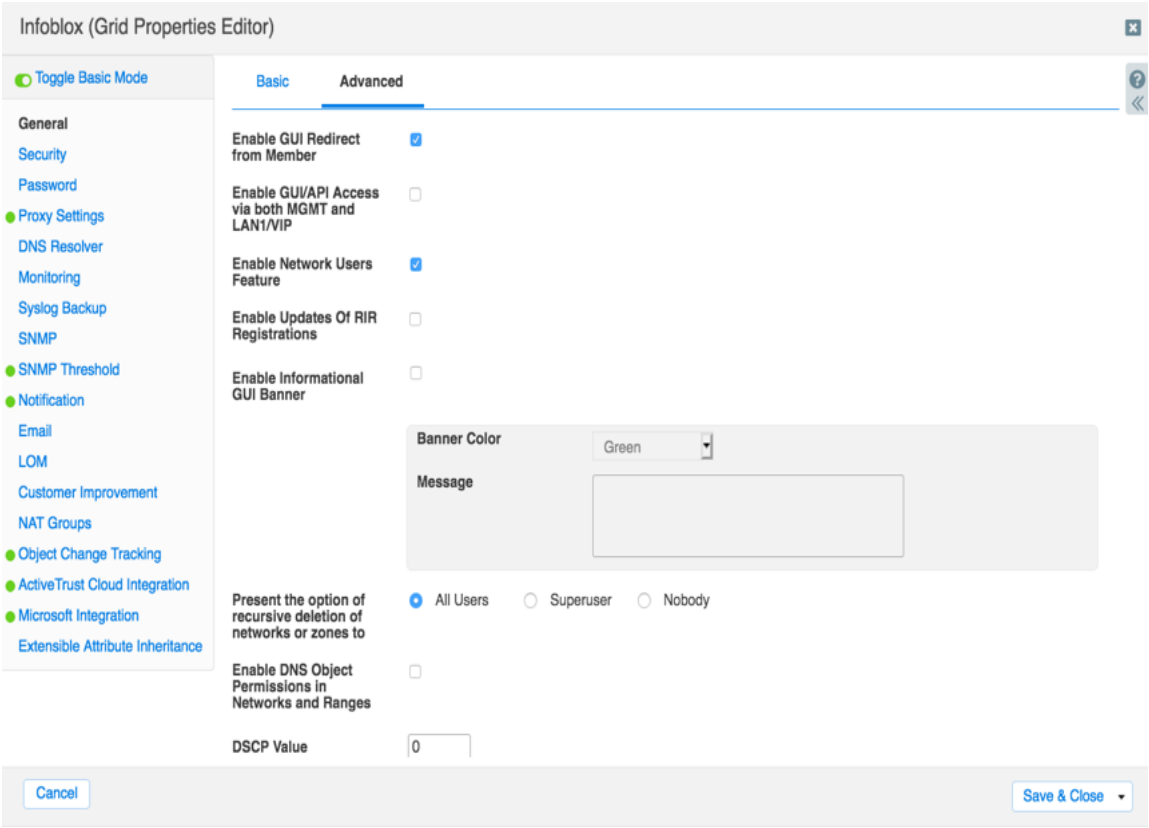
1. Navigate to Grid → Grid Manager--> Members.



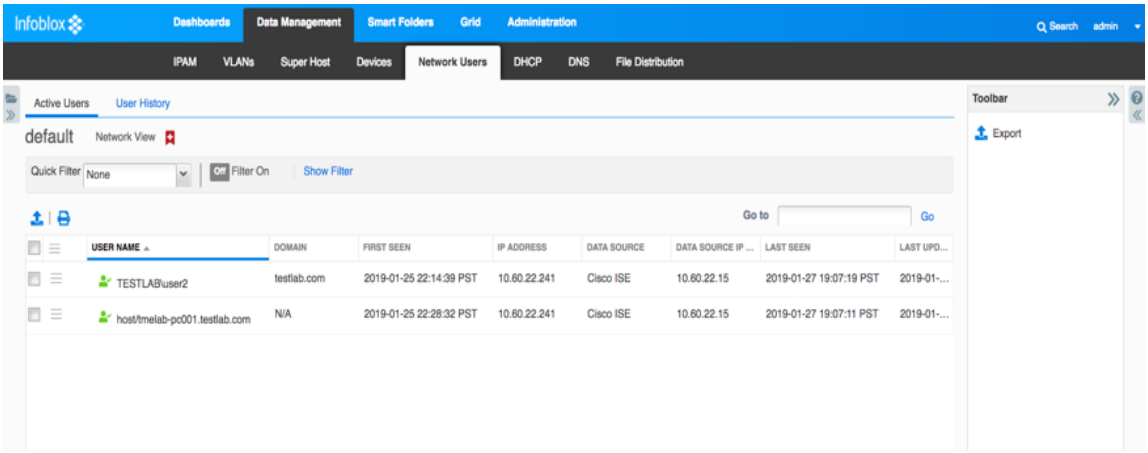
2. Navigate to Toolbar --> Grid Properties à Edit.



3. Click on the ‘Advanced’ tab.



4. Ensure the ‘Enable Network Users Feature’ button is enabled. Click ‘Save and Close’.
5. Navigate to Data Management à Network Users. This screen shows the ISE authenticated users.

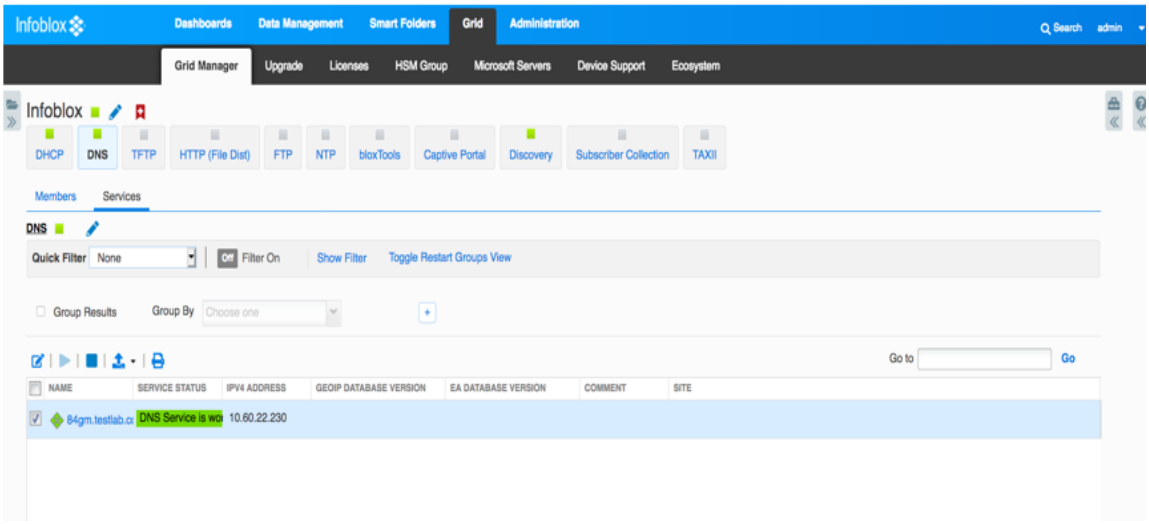


Configuring DNS Services

This section documents enabling DNS services on the Grid Master and creating and configuring DNSzones. A dynamic zone will be created for updating user records dynamically. In addition, an RPZ 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.

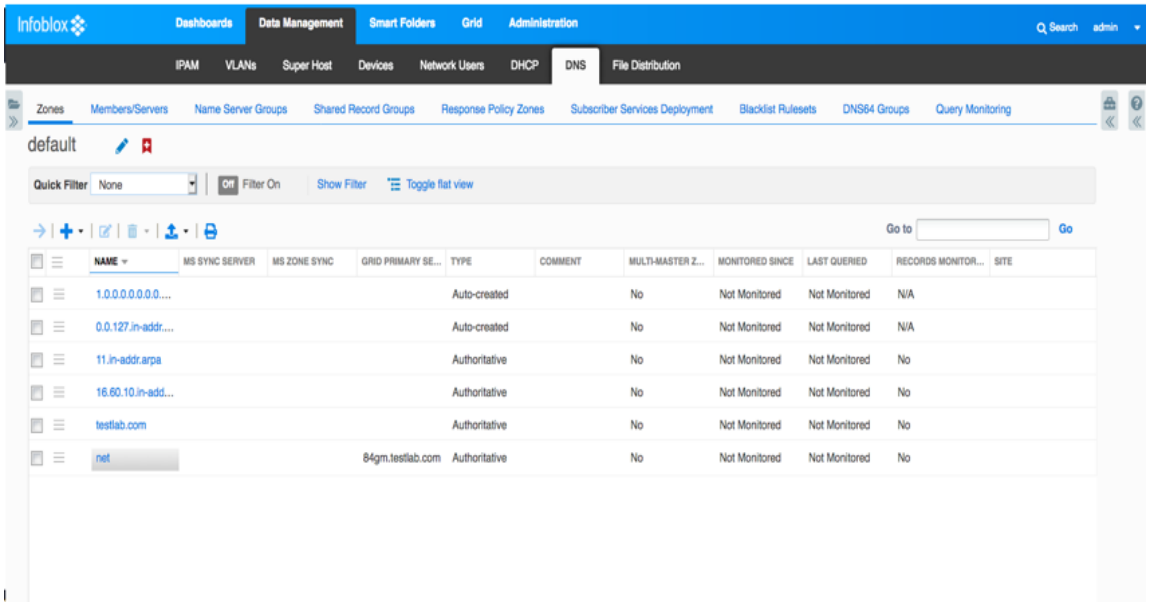
Enabling DNS Service on the Grid Master

1. On the Infoblox GUI, navigate to Grid à Grid Manager à DNS . Select the Grid Master and then click on the play button.

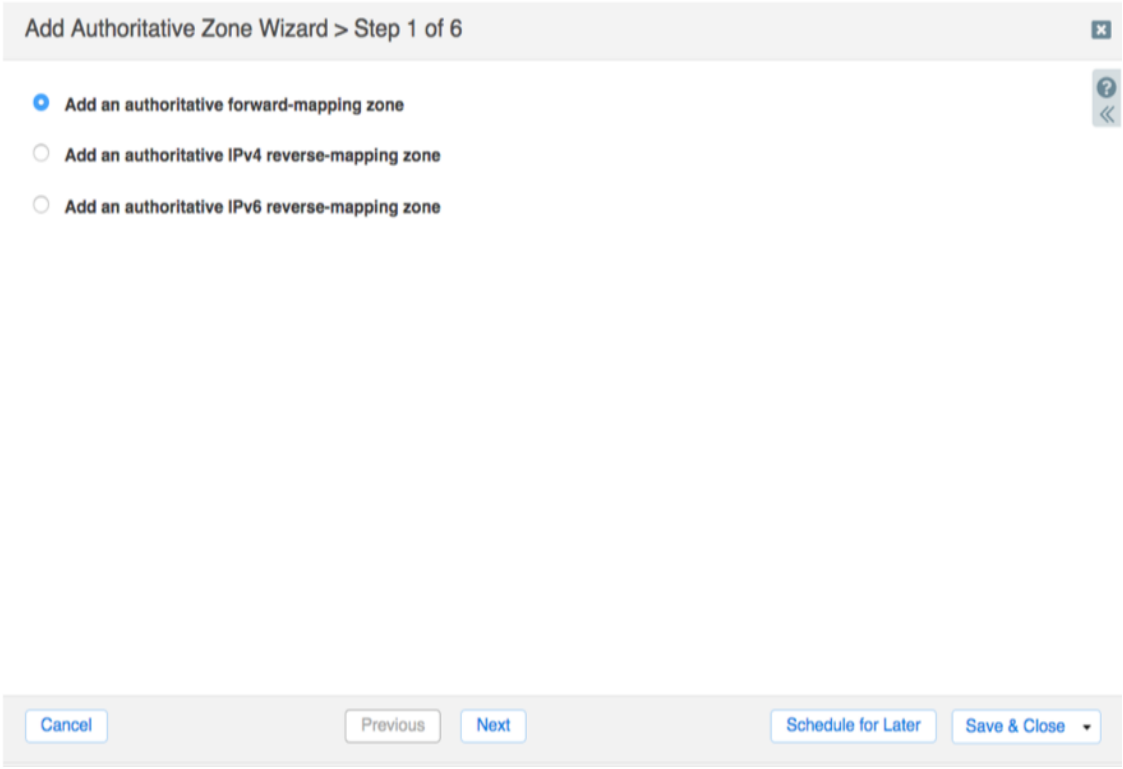


Creating DNS Zone

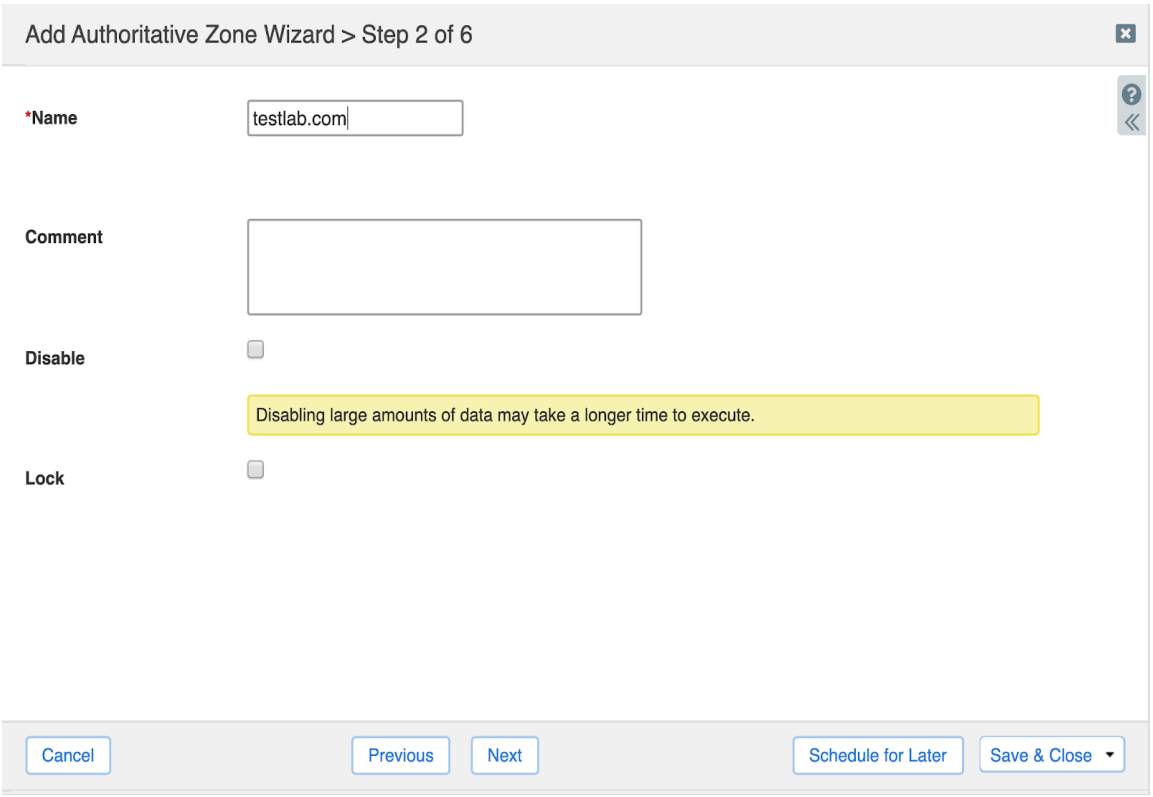
1. Navigate to Data Management --> DNS --> Zones.



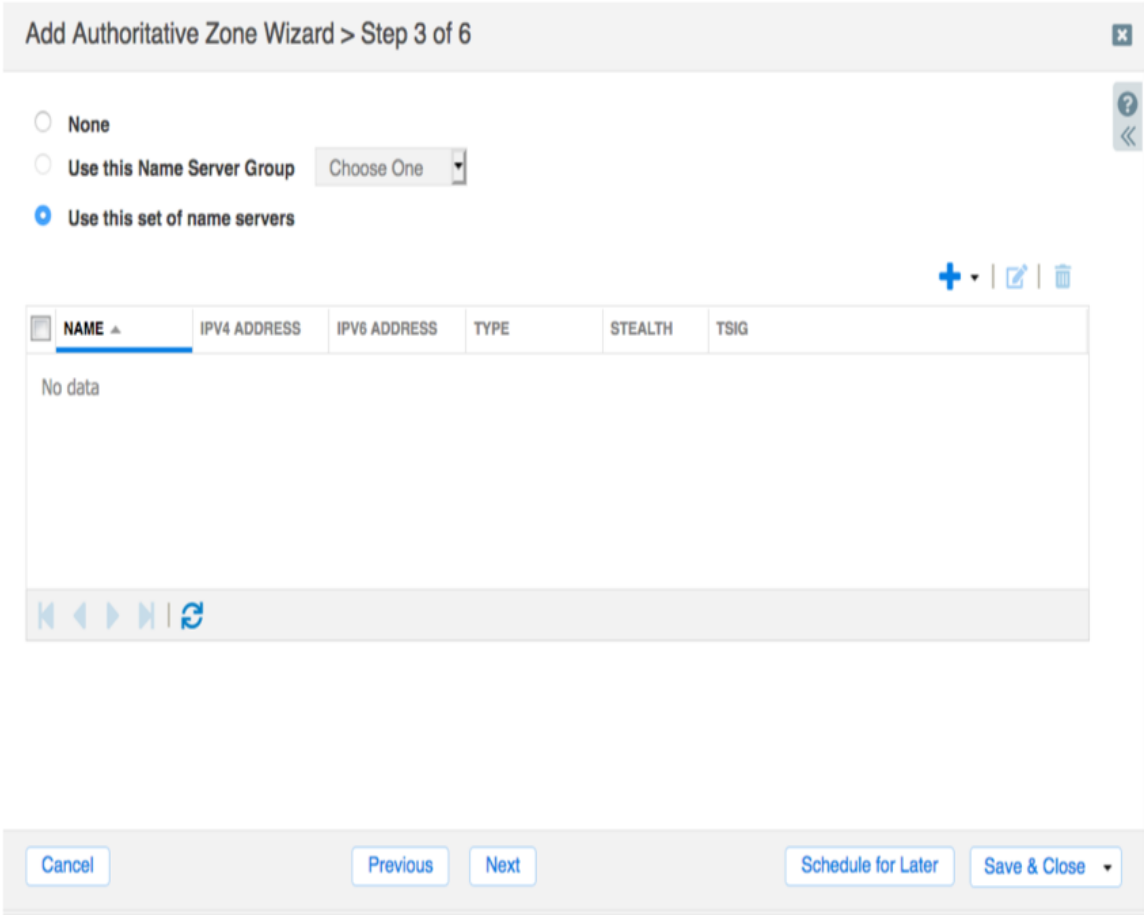
2. Click on the '+' button to add an authoritative forward mapping zone. Click Next.



3. Type in the name of the zone. Add a comment. Click Next.

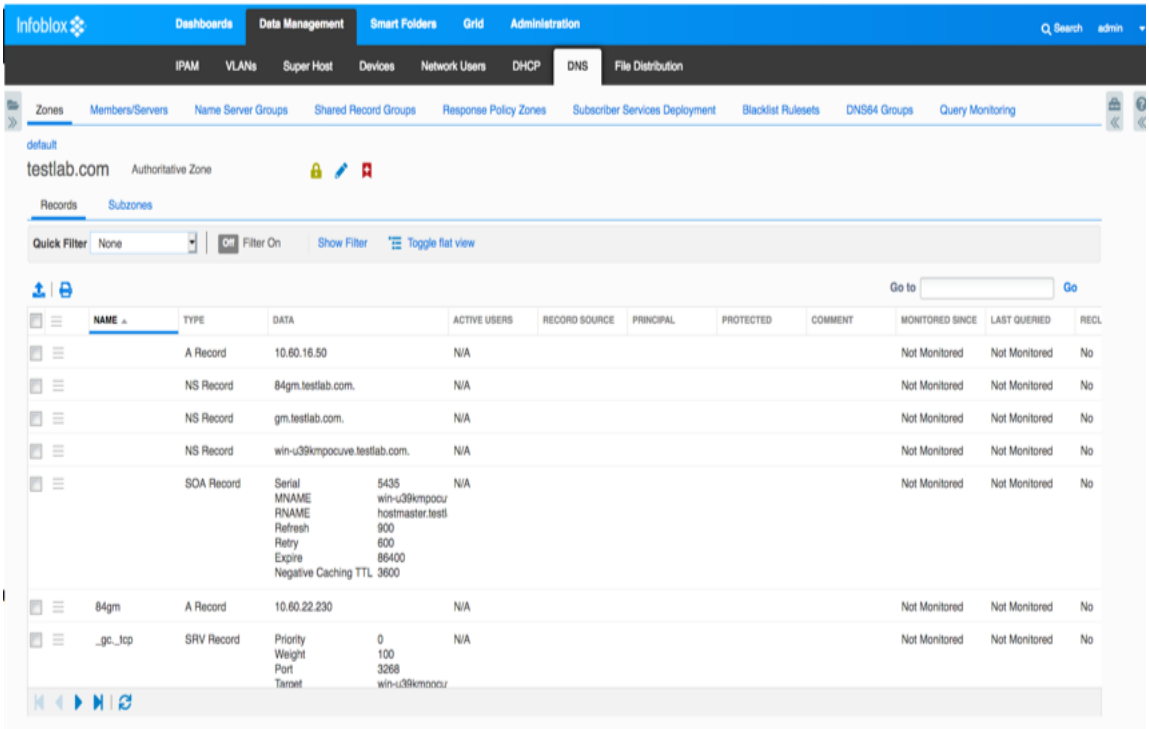


4. Add the name server by clicking on the '+' button and select 'Grid Primary'. Click Save and Close.

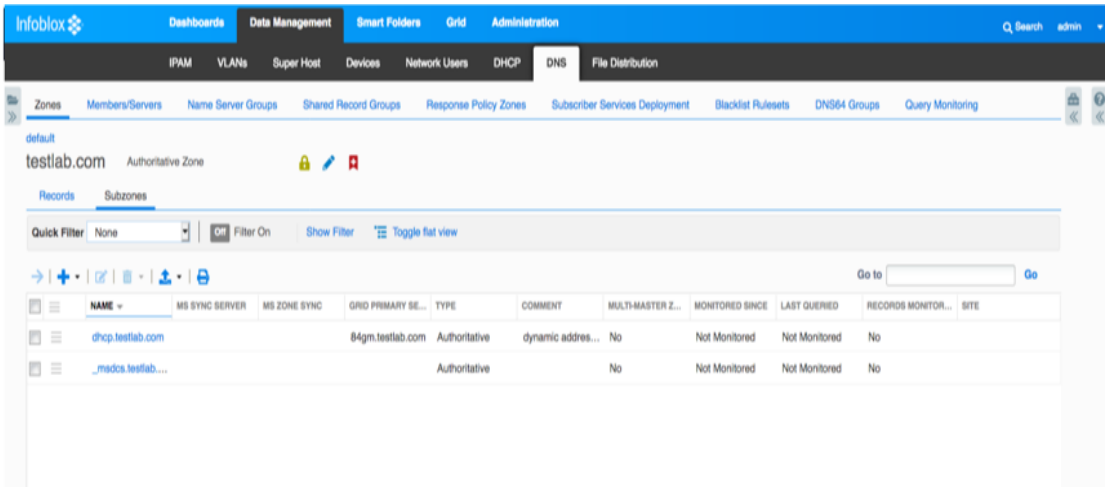


5. At this point, you can enable zone transfer to transfer the zone information from the AD server. Refer to the Infoblox NIOS Administrator Guide to enable zone transfer. The Cisco ISE appliances A records will be transferred in addition to the SRV records needed to point the

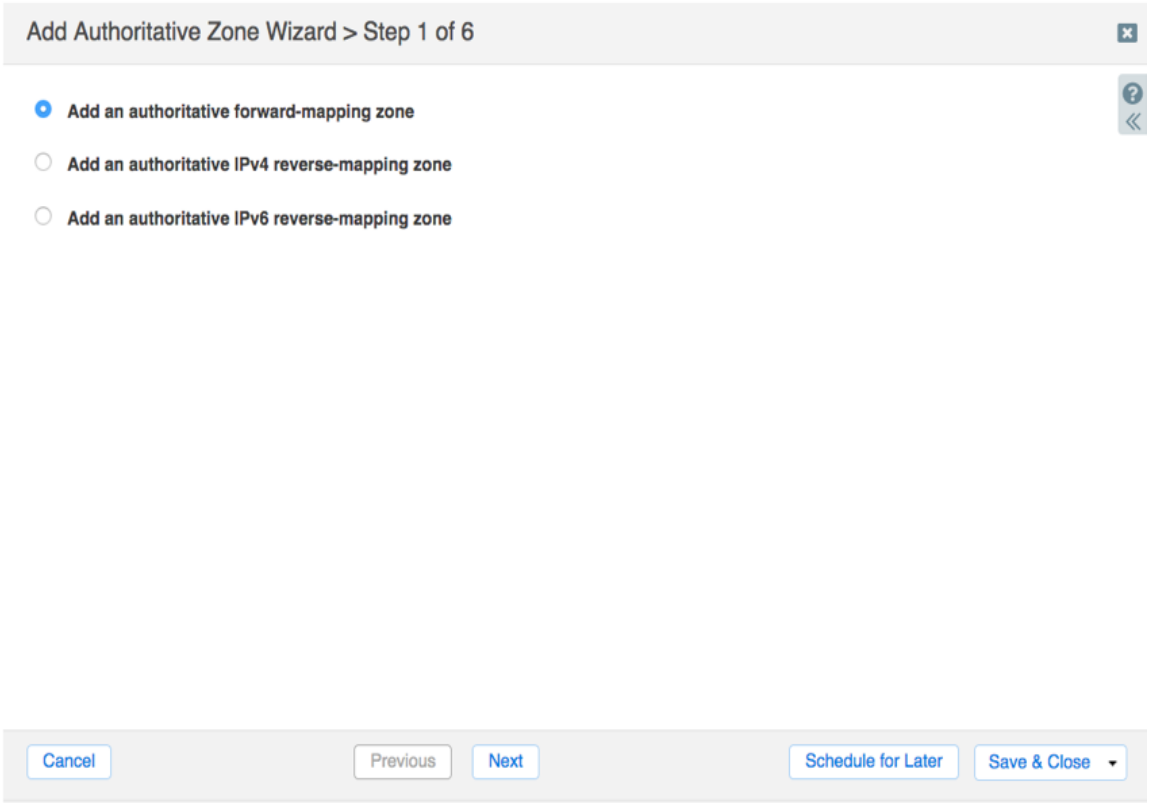
workstations towards the AD server for authentication.



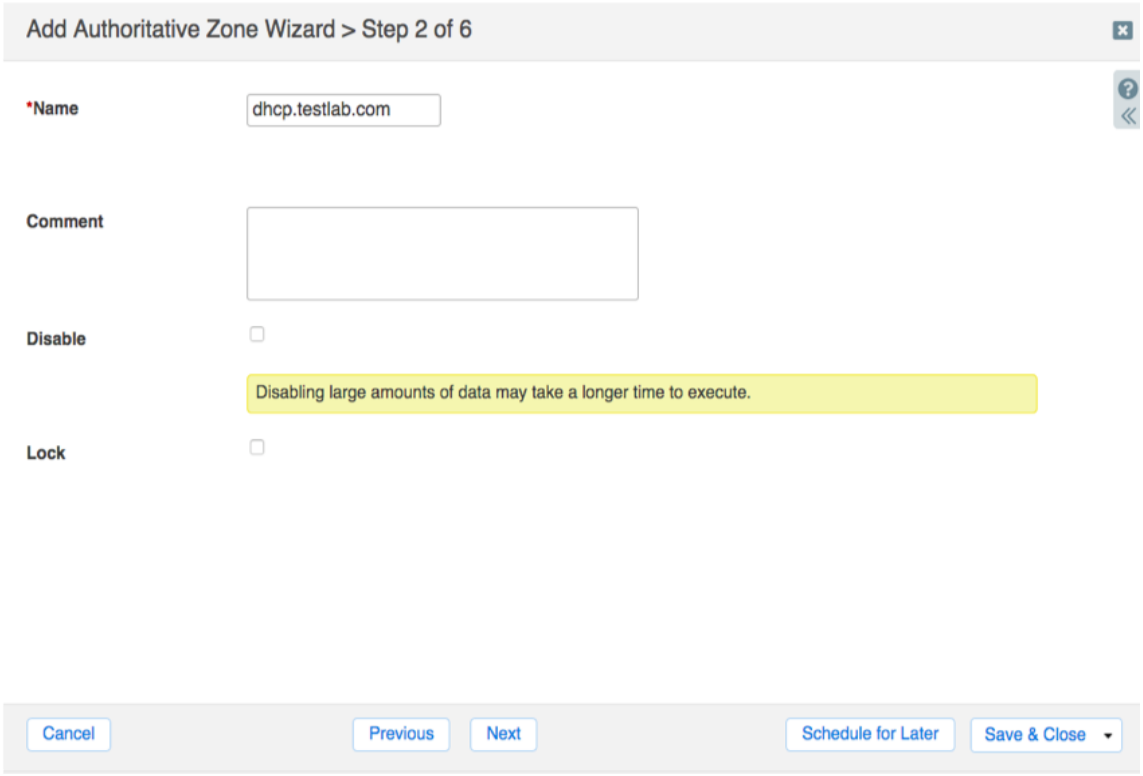
6. Click on Subzones. Create a subzone for dynamic addresses.



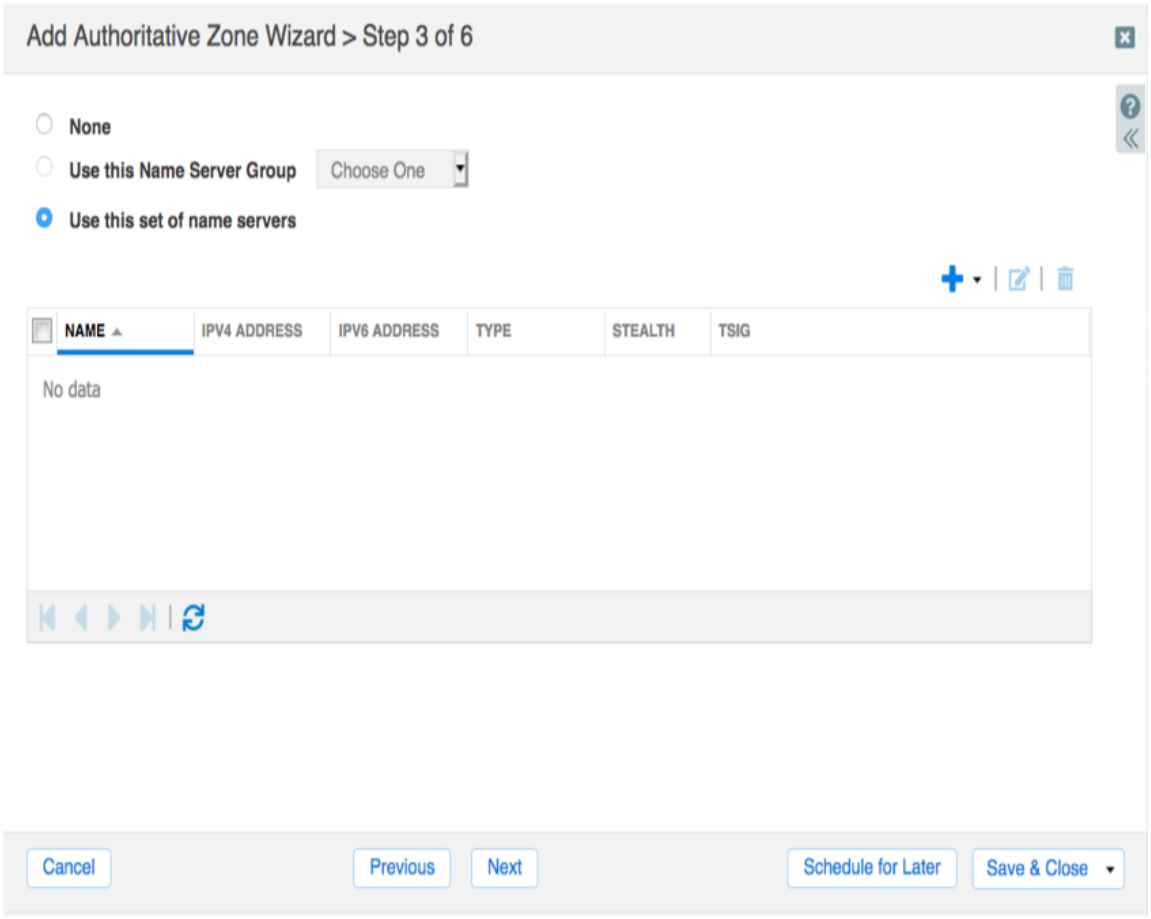
7. Click on the '+' button to add an authoritative forward mapping zone. Click 'Next'.



8. Type in the name of the zone. Click 'Next'.



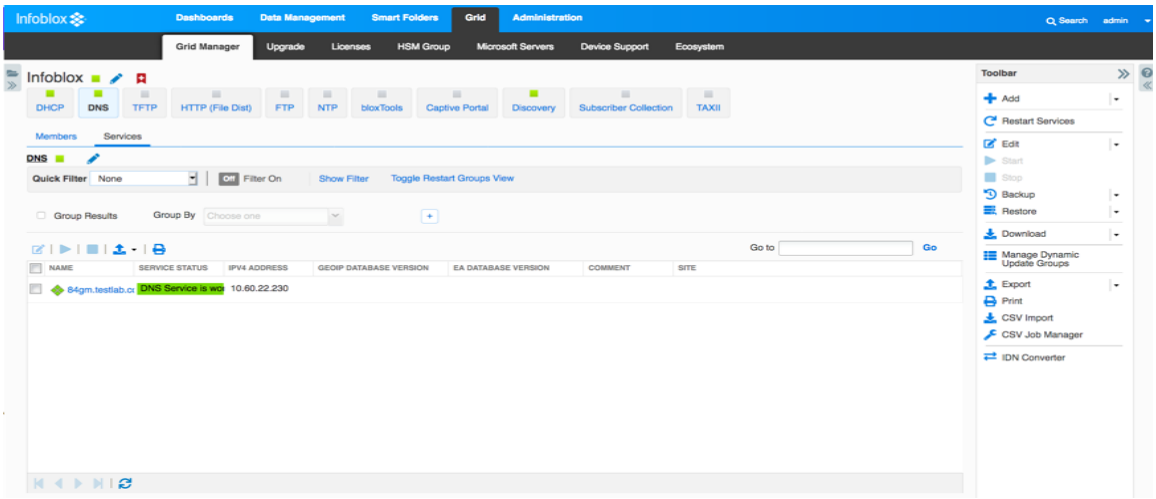
9. Add the name server. Click ‘Save and Close’.



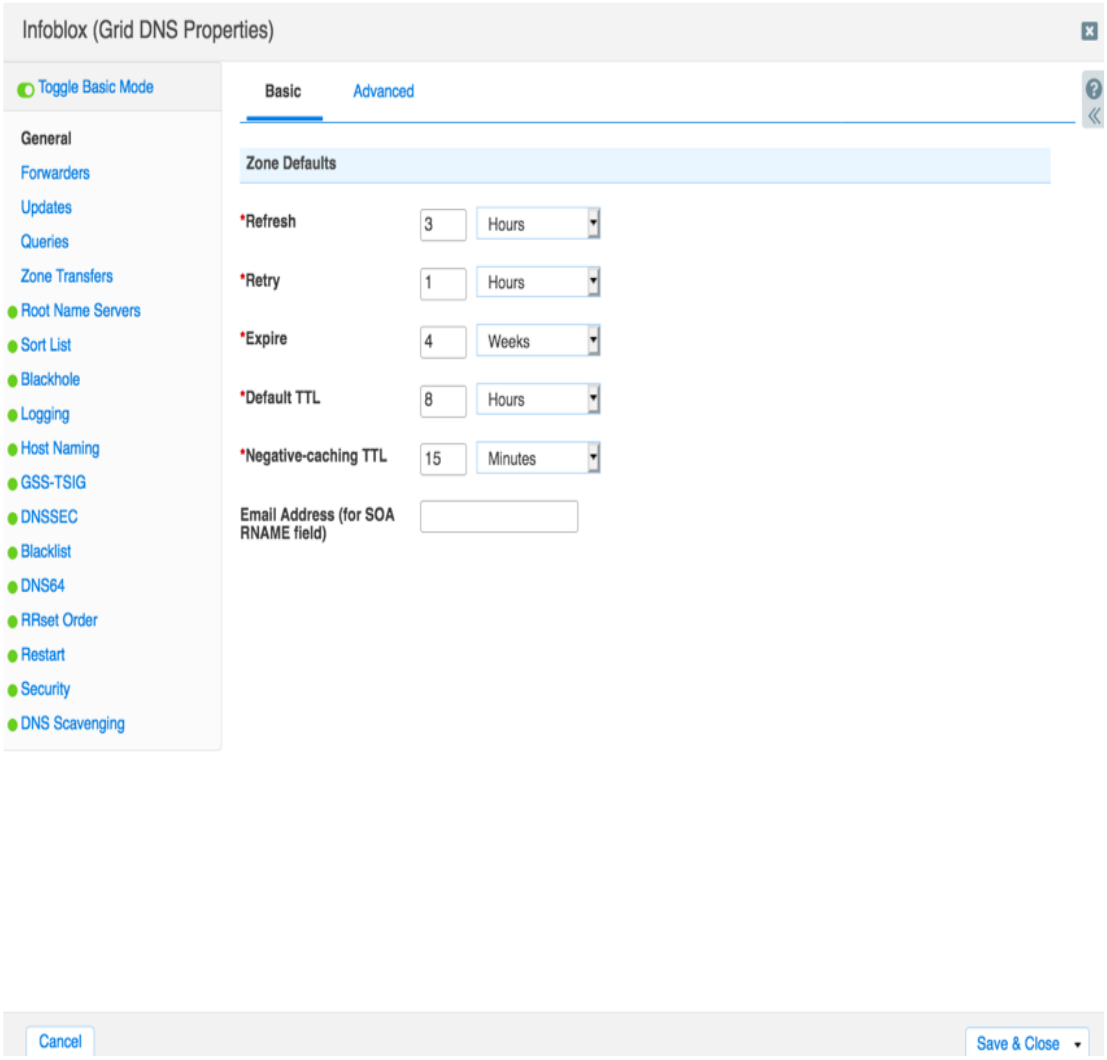
Configure DNS Properties

This section provides instructions on configuring forwarder address and recursion.

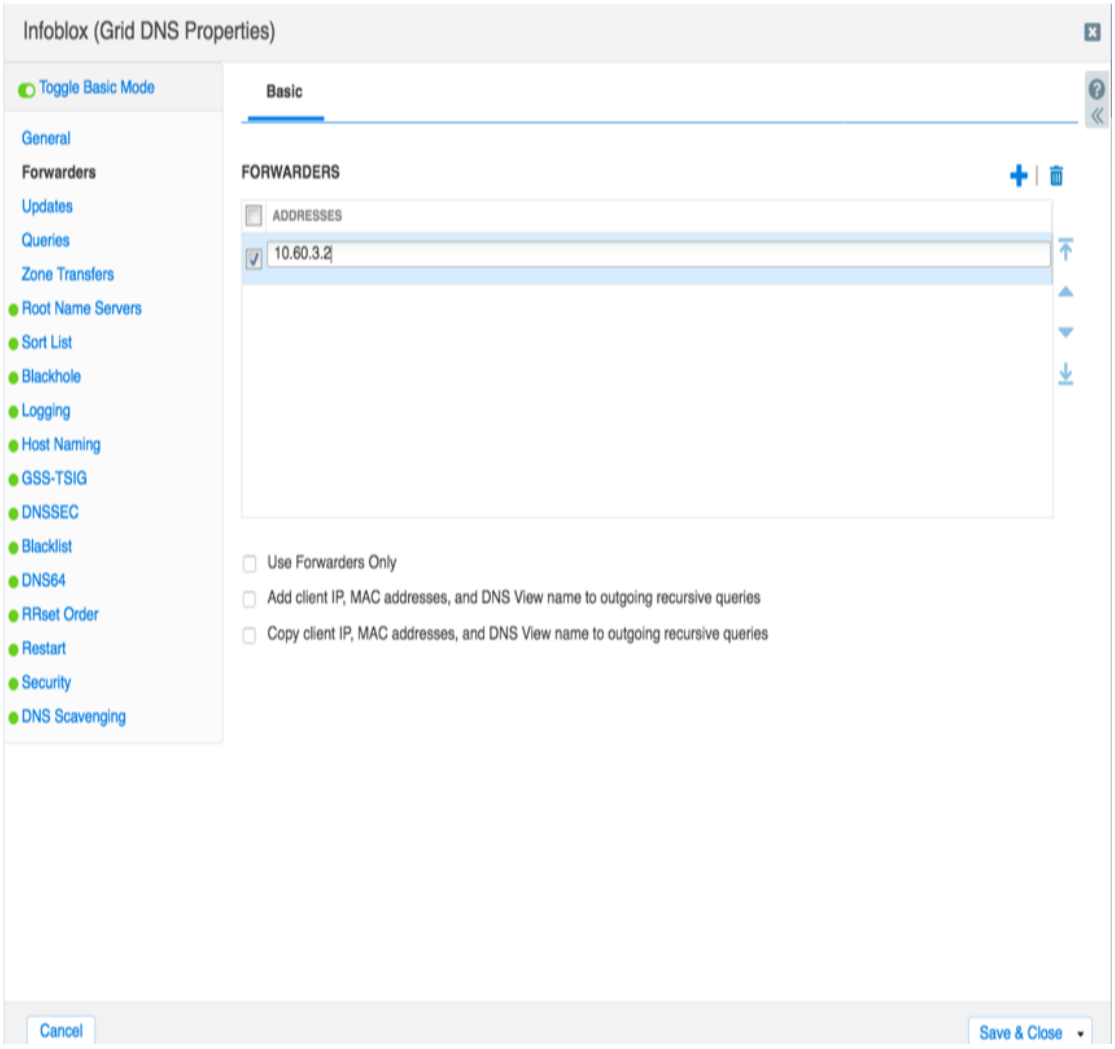
1. Navigate to Grid --> Grid Manager --> DNS.



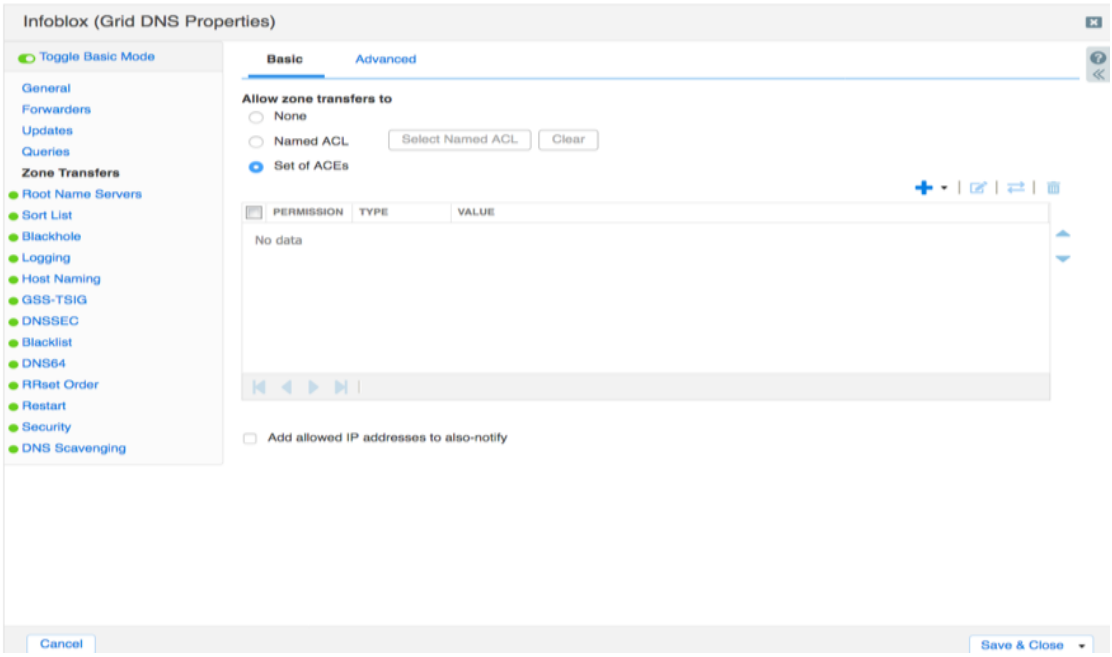
2. Click on Toolbar --> Edit → Grid DNS Properties.



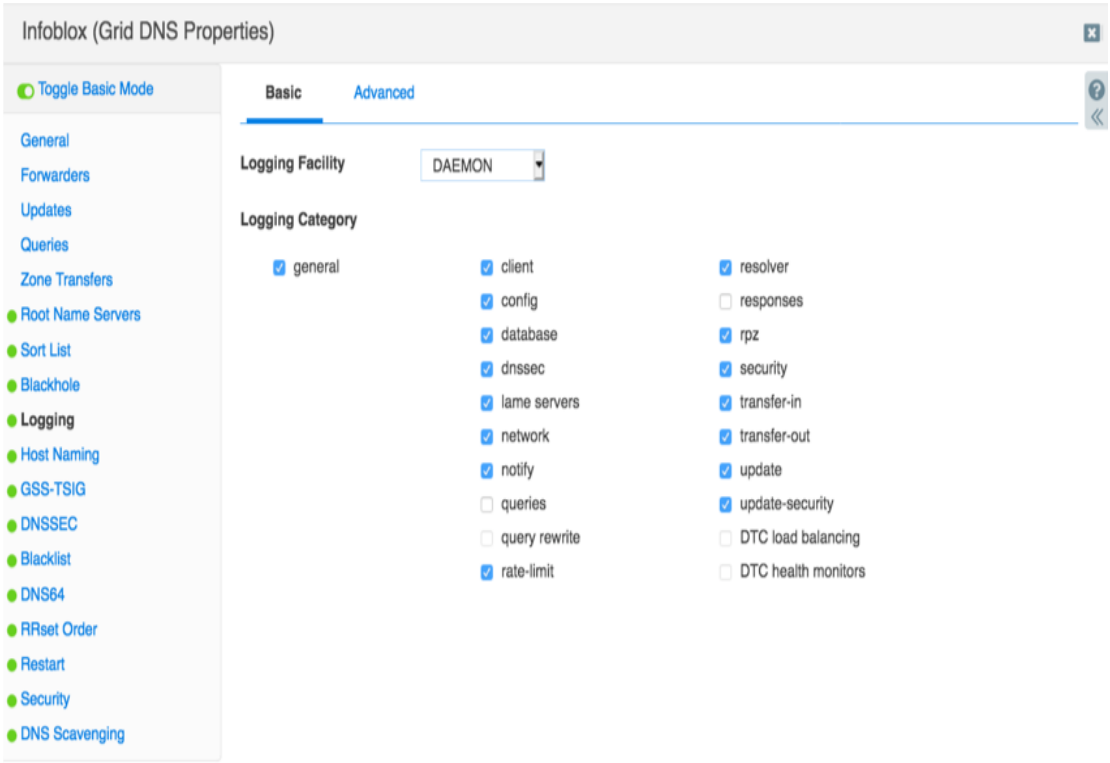
3. If you wish to forward queries to another DNS server, click on the ‘Forwarders’ tab and add a forwarding address.



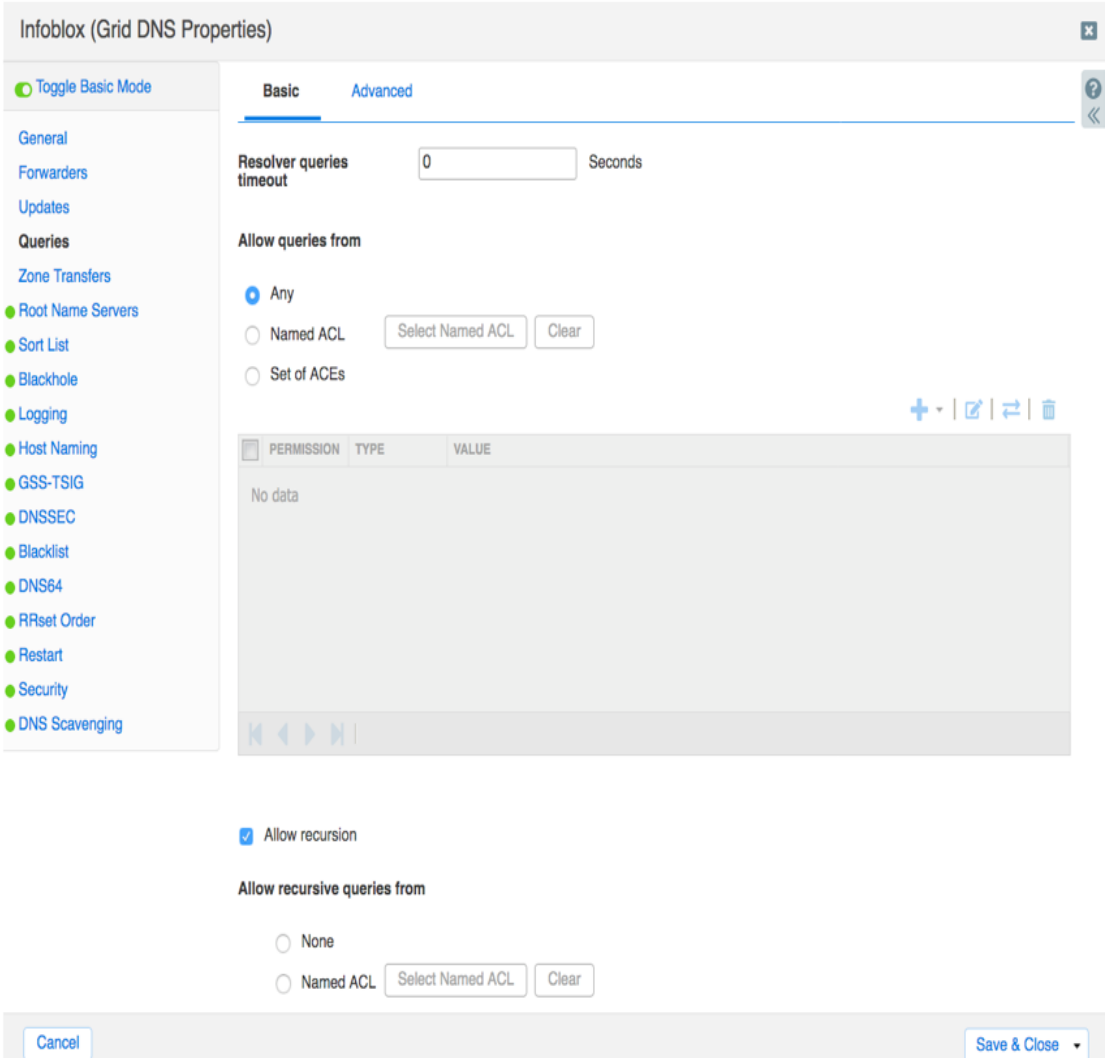
4. Click on Zone Transfers to transfer zone information from the AD DNS Server. Click on ‘Set of ACEs’ and add the Grid Master or Grid Member that will accept a zone transfer.



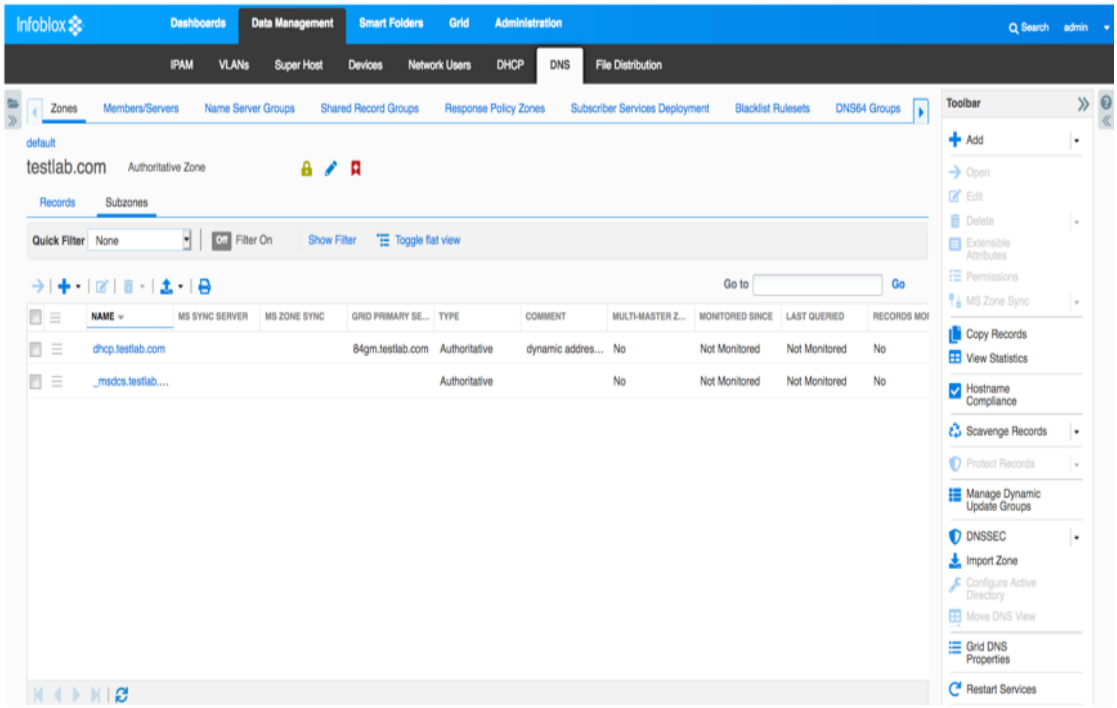
5. Click on Logging and click on RPZ to enable logging of RPZ events in the syslog.



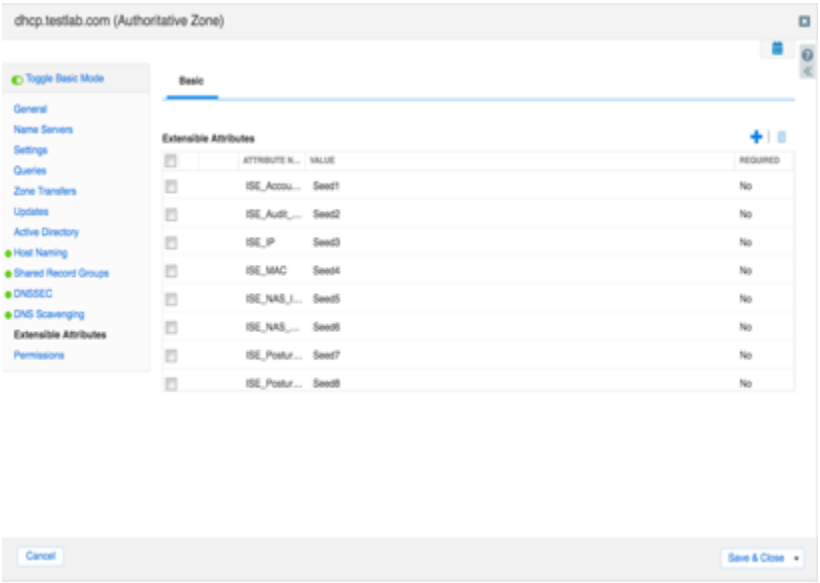
6. Click on Queries and Click on ‘Allow Recursion’ to enable recursion. Click ‘Save and Close’ .



7. Navigate to Data Management → DNS--> Zones --> <ISE zone> --> Subzones <DHCP subzone>.



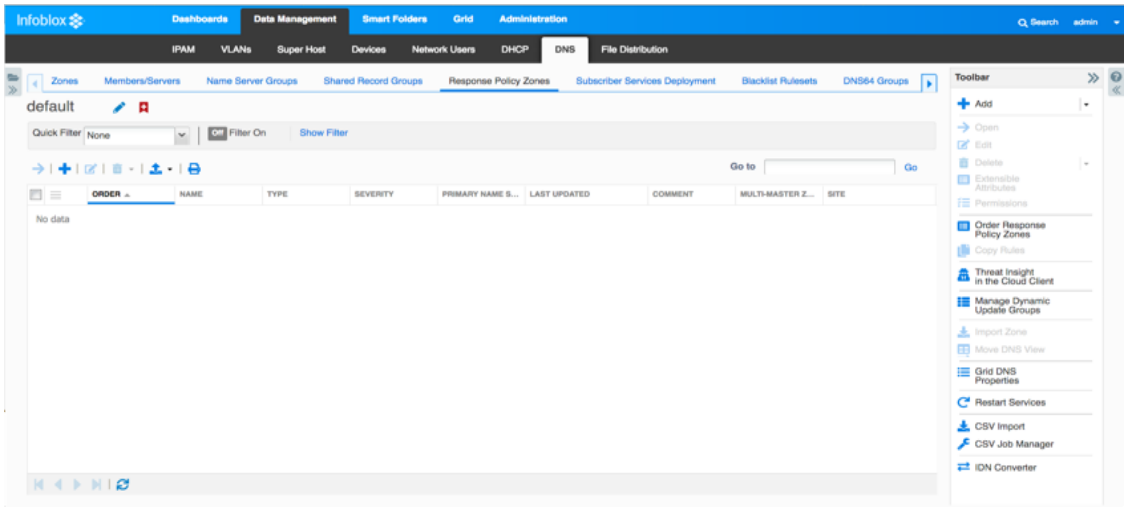
8. Select the newly created subzone and edit the subzone. Select ‘Extensible Attributes’ and add all of the extensible attributes that were created earlier in this document. Click ‘Save and Close’.



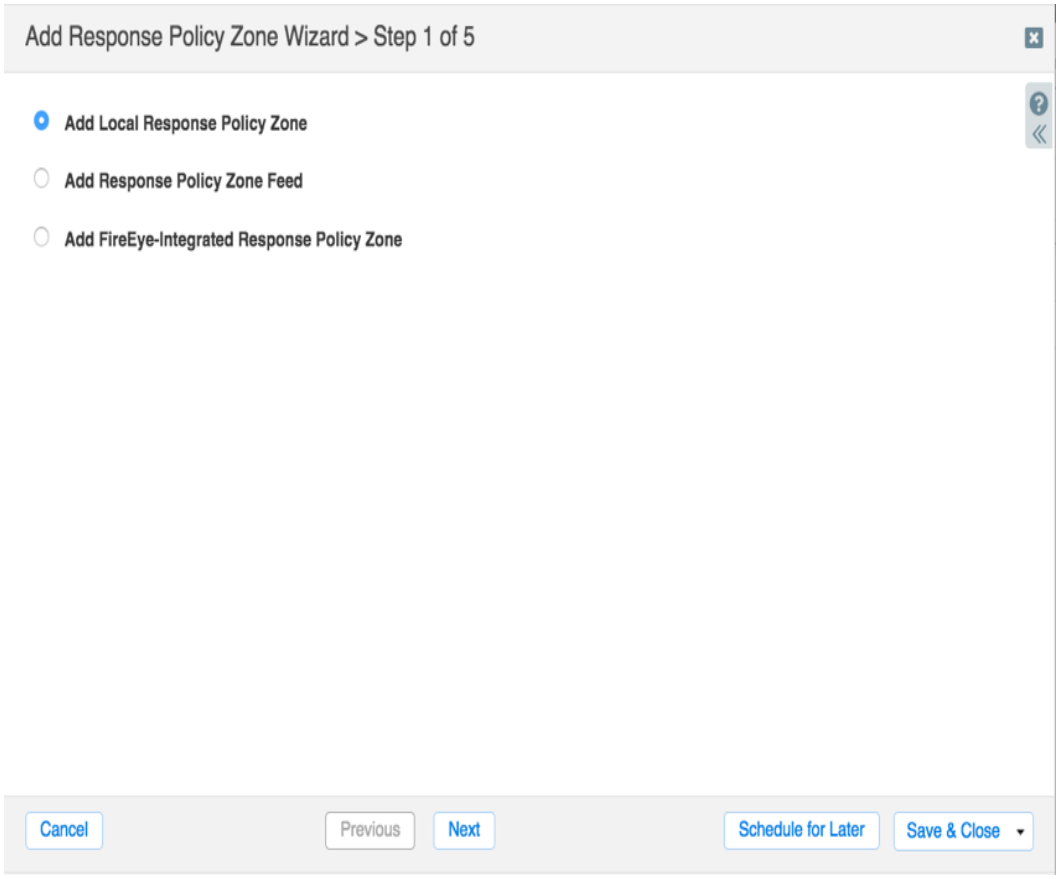
Add Response Policy Zone

These instructions show you how to create a response policy zone. The response policy zone contains a list of known bad sites. The list can be generated manually or by a zone transfer from a threat feed source like Infoblox's BloxOne Threat Feeds. When a workstation tries to resolve one of these domains, the Infoblox appliance will block if configured to do so and then send a notification to ISE appliance to quarantine the workstation. For this document, we will create a local response policy zone to block www.yahoo.com.

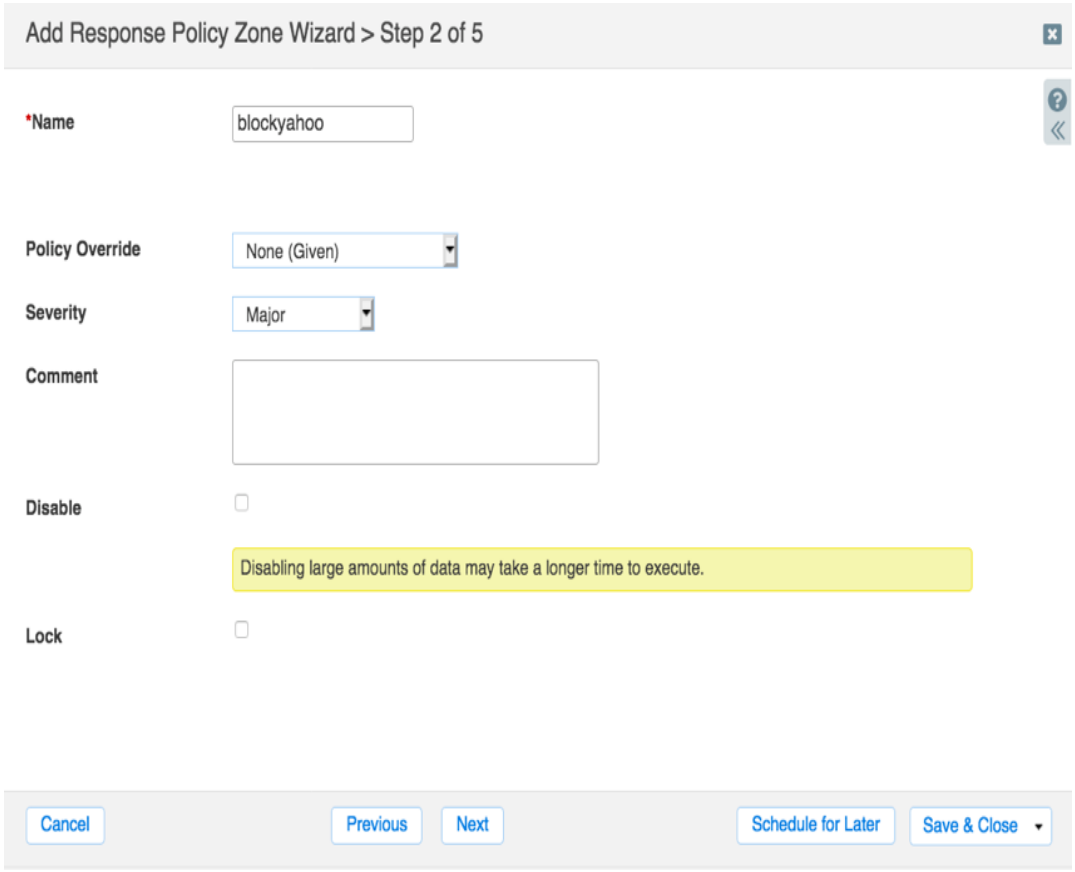
1. Navigate to Data Management à DNS à Response Policy Zones



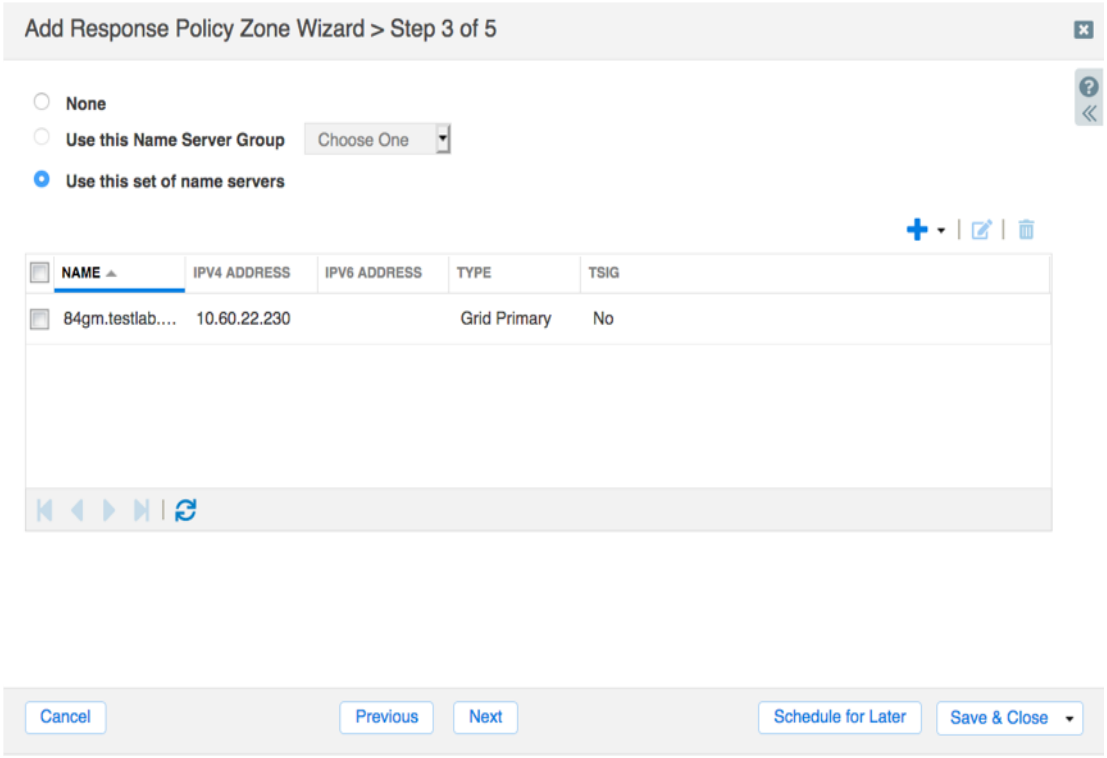
2. Click on the ‘+’ button to add an RPZ. Click Next.



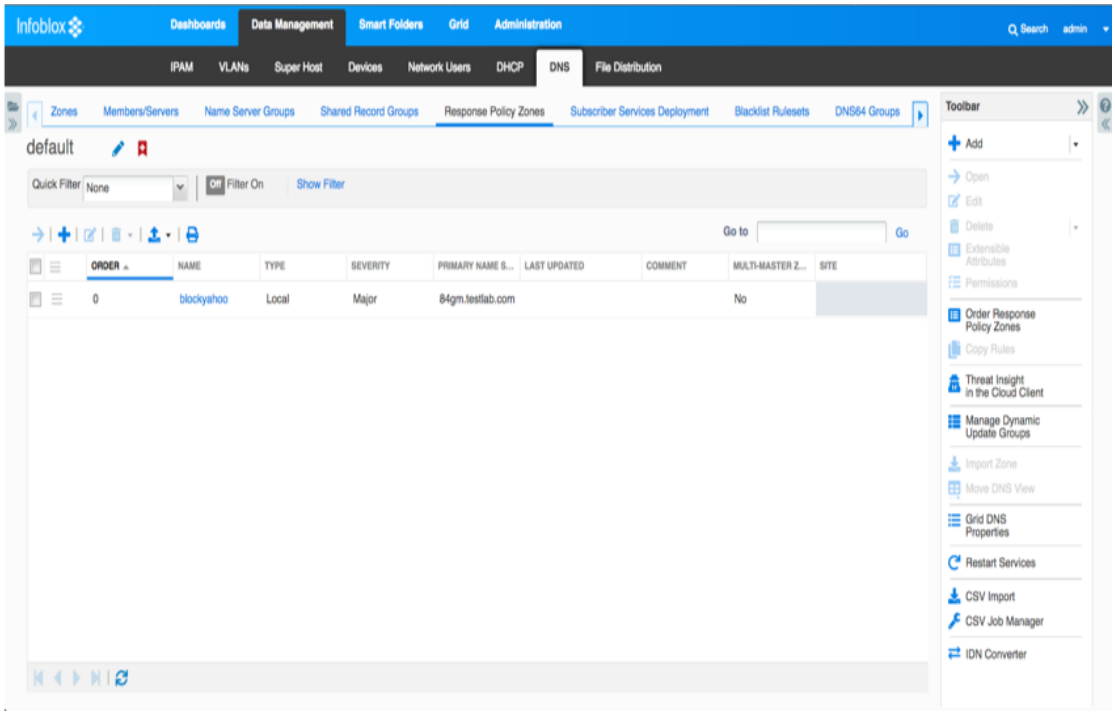
3. Type in the name of the RPZ. Click Next.



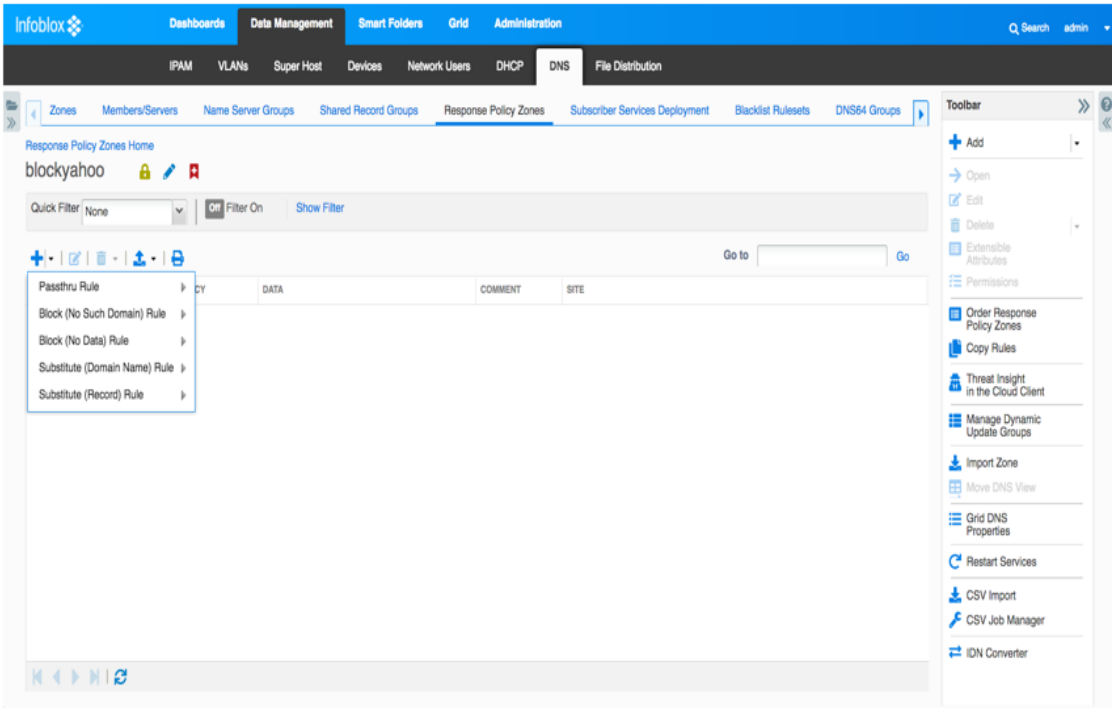
4. Add the name server. Click ‘Save and Close’



5. This brings you back to the main RPZ screen.



6. Click on the RPZ name and then click on the drop-down arrow for the '+' button.



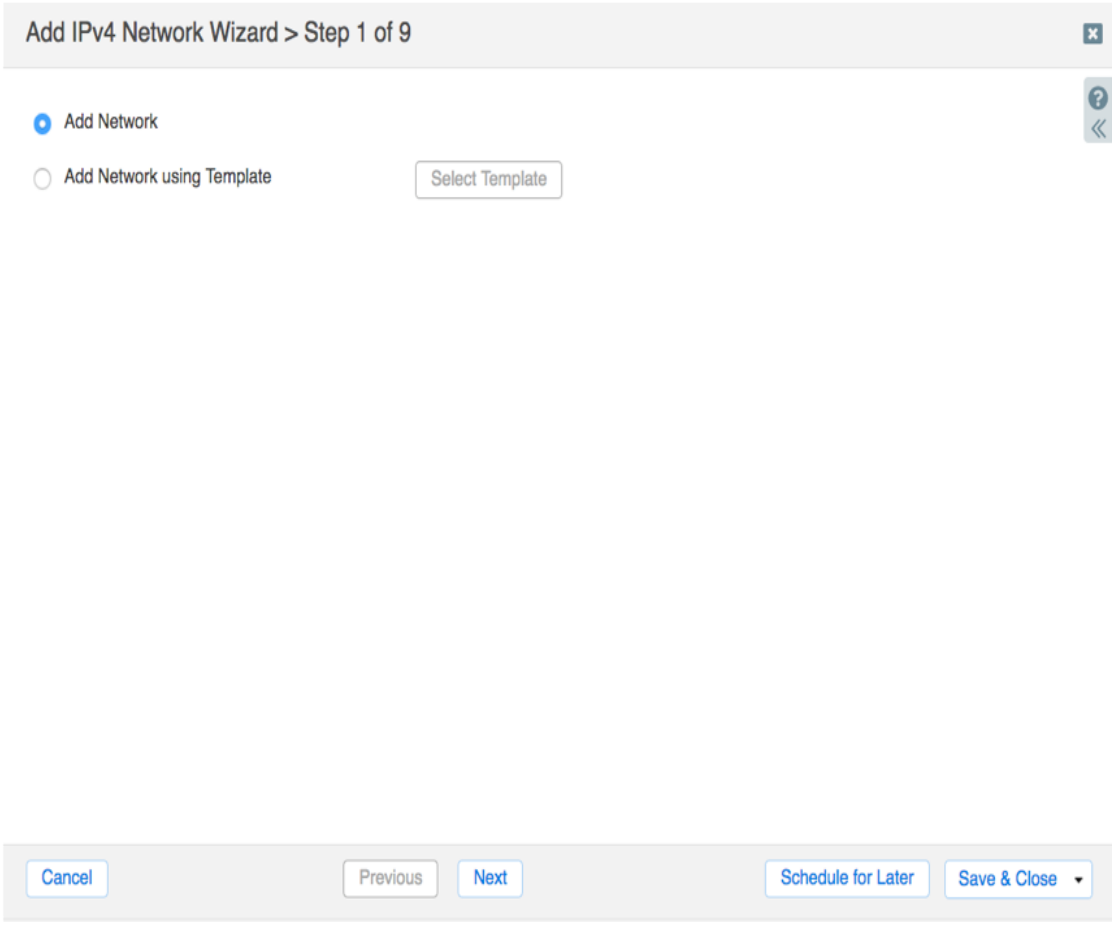
7. Select 'Block (No Such Domain) Rule'. Type in 'www.yahoo.com'. Click 'Save and Close'.

Configuring DHCP

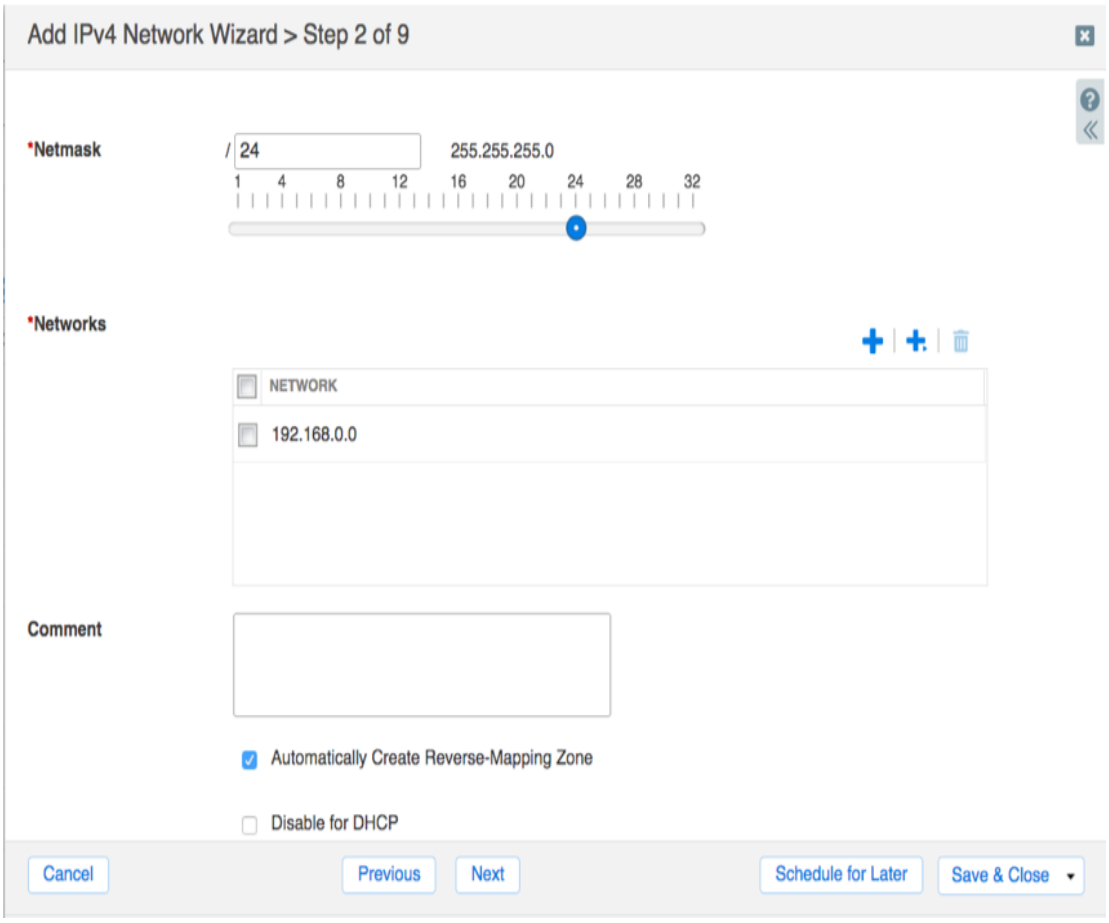
These instructions show you how to create a DHCP range for the clients that will be authenticated by AD via Cisco ISE.

1. If the discovery appliance has not discovered your networks, then you need to manually add networks for DHCP use. Navigate to Data Management --> DHCP --> Networks --> '+'

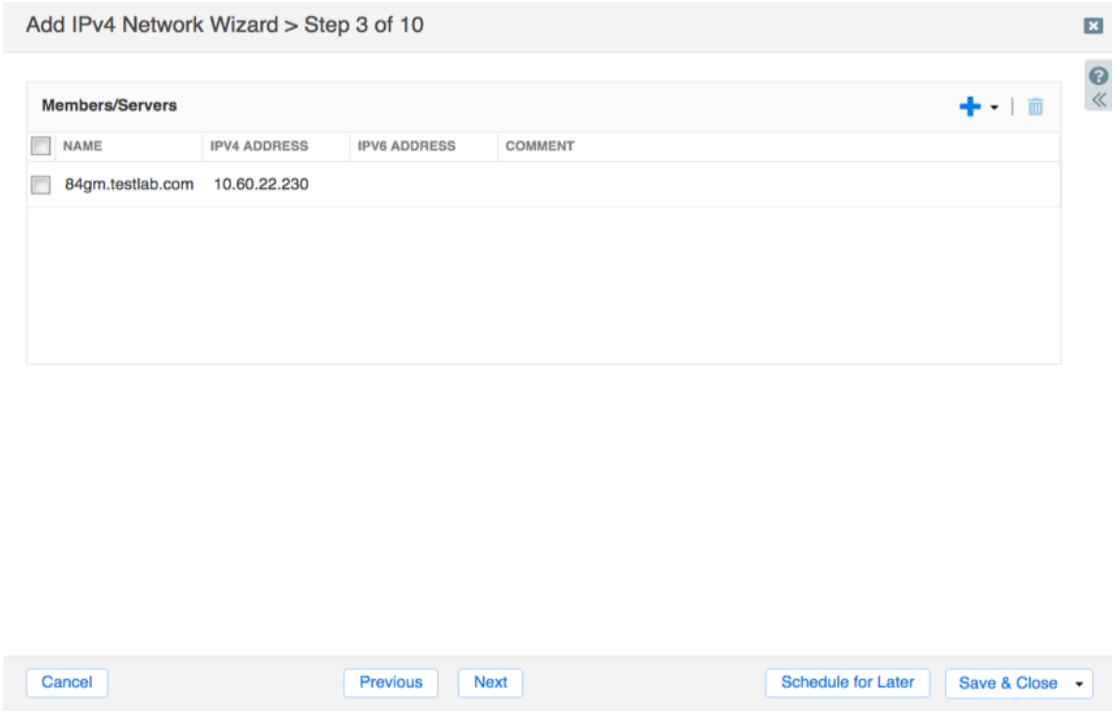
-->IPv4 Network.



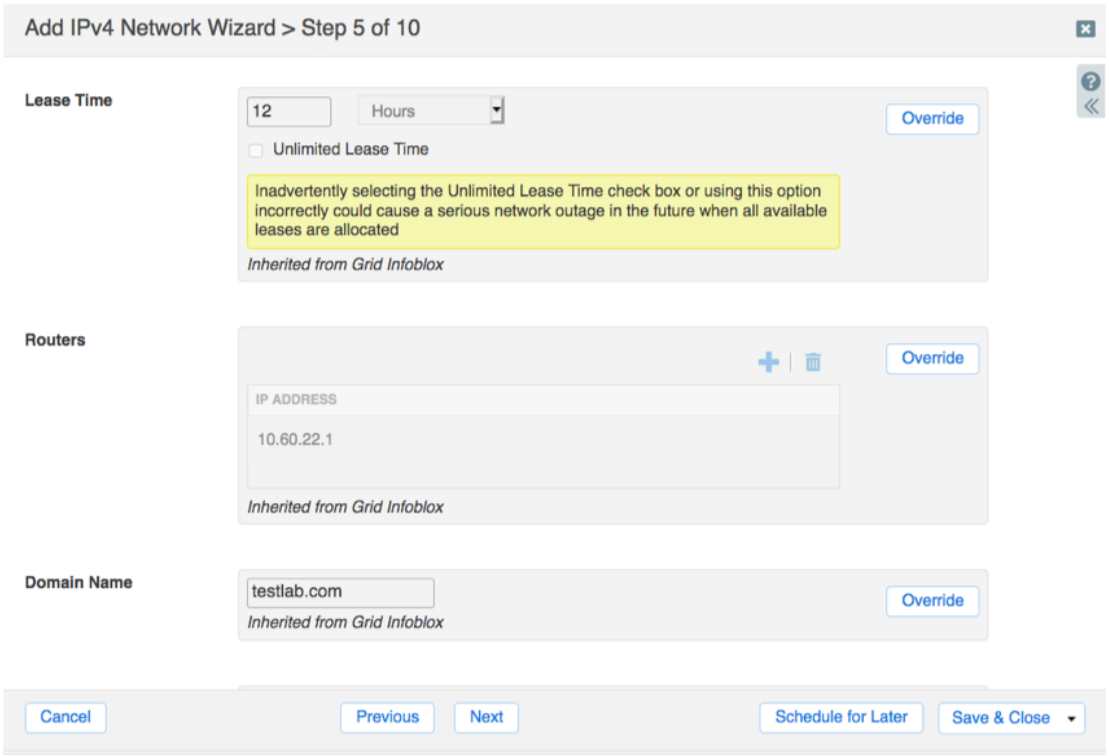
2. Click Next.
3. Adjust the Netmask bar accordingly to your IP address scheme. Click on the left '+' button to add a network and then input the IP subnet. Click to add a reverse mapping zone. Click 'Next'


Add IPv4 Network Wizard > Step 2 of 9
*Netmask
/ 24
255.255.255.0
1 4 8 12 16 20 24 28 32
*Networks
NETWORK
192.168.0.0
Comment
Automatically Create Reverse-Mapping Zone
Disable for DHCP
Cancel
Previous
Next
Schedule for Later
Save & Close

4. Click on the '+' button to assign the grid member to provide DHCP services. In this case it is the grid master. Click 'Next'.

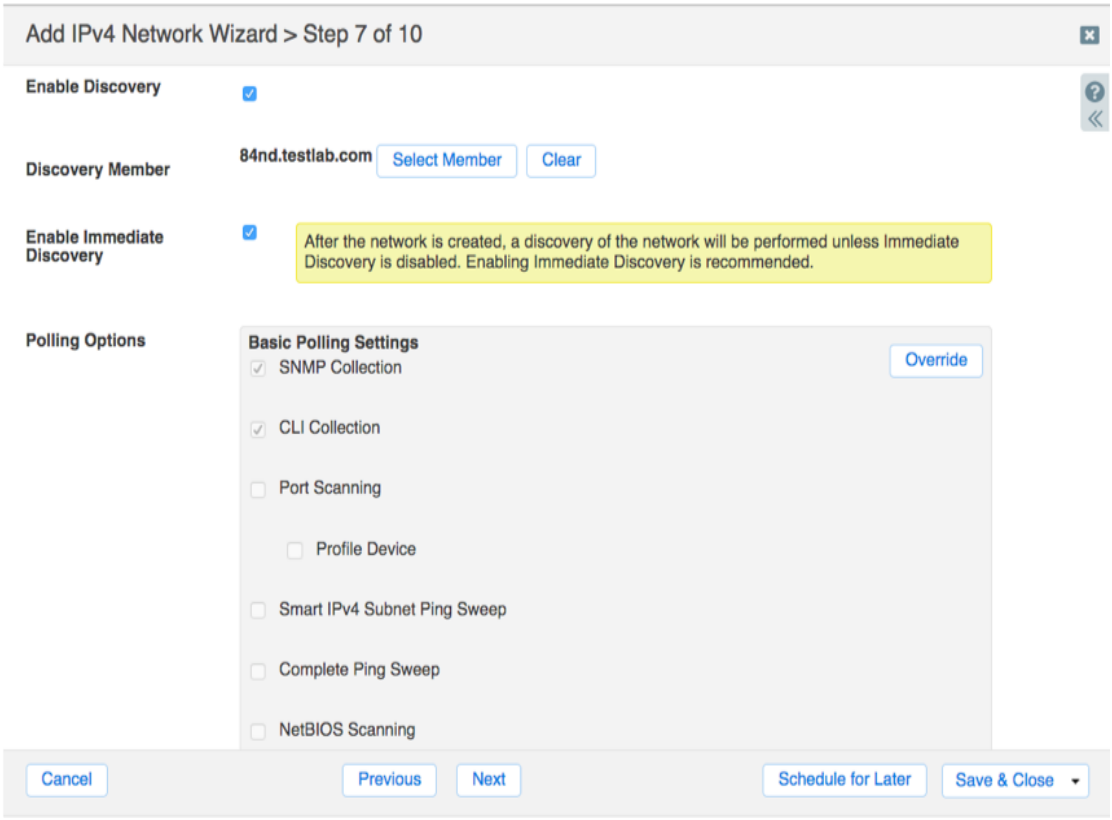


5. Click Next.
6. Ensure the lease time, routers, domain name, and DNS server configurations are correct. Otherwise, click on the respective override button to override the setting. Click 'Next'

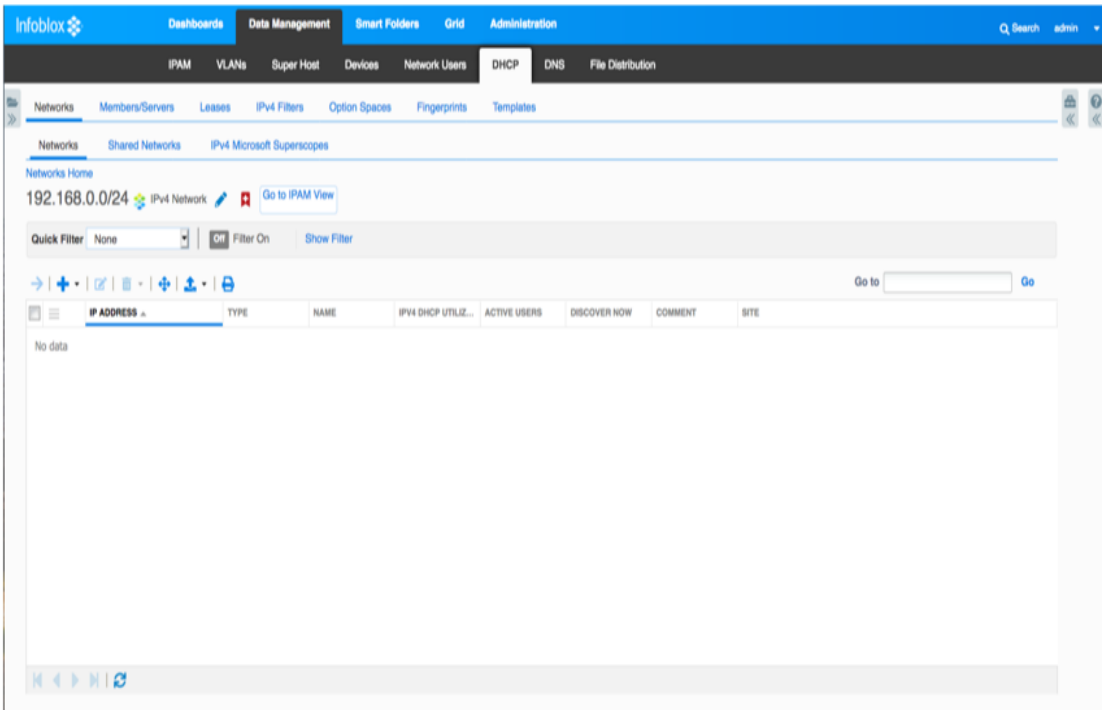


7. Click 'Next'.

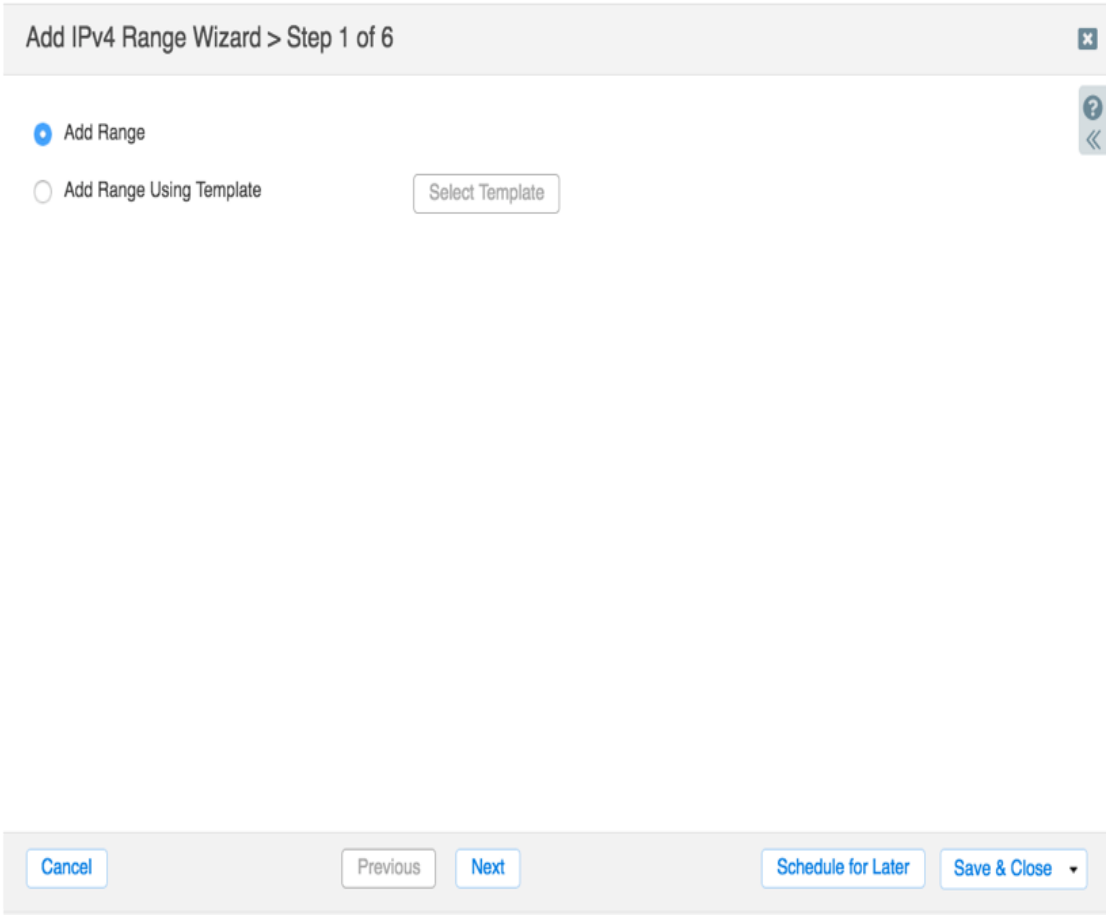
8. Enable discovery. Select the discovery member. Click ‘Next’.



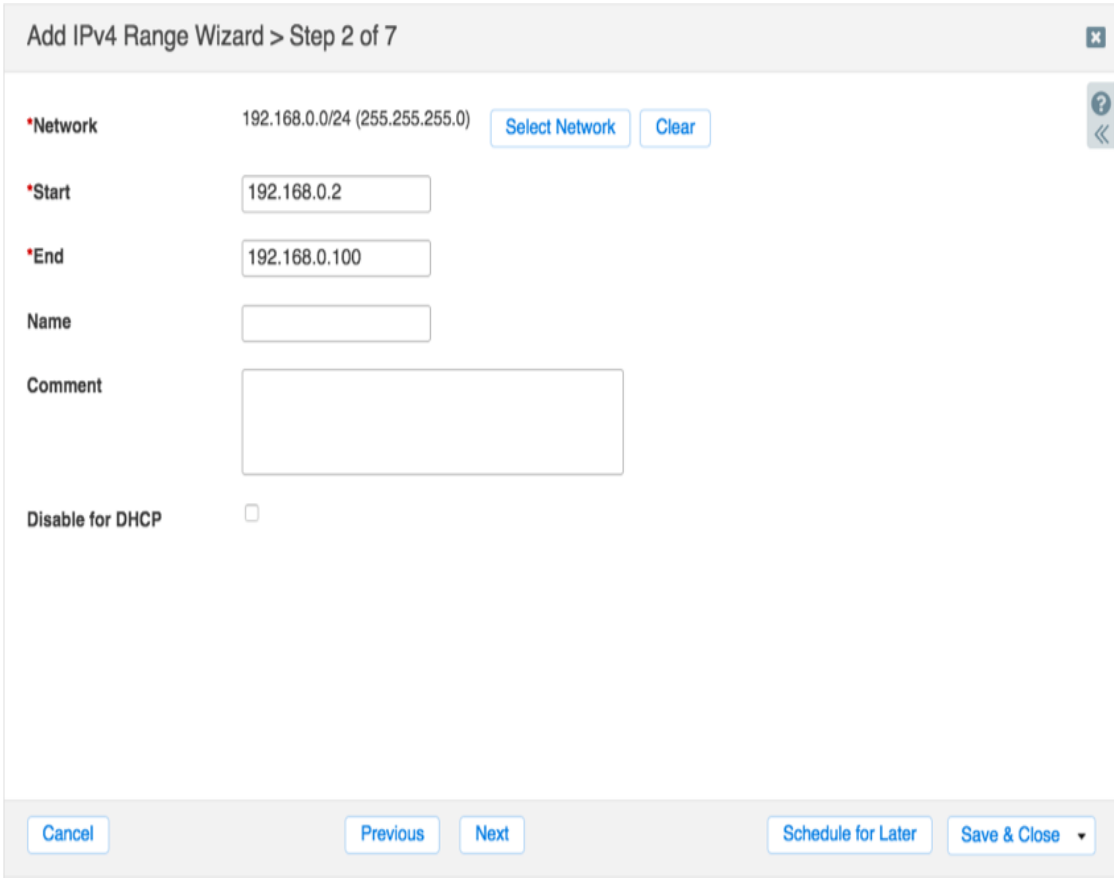
9. Click ‘Save and Close’.
10. Click on the newly created network.



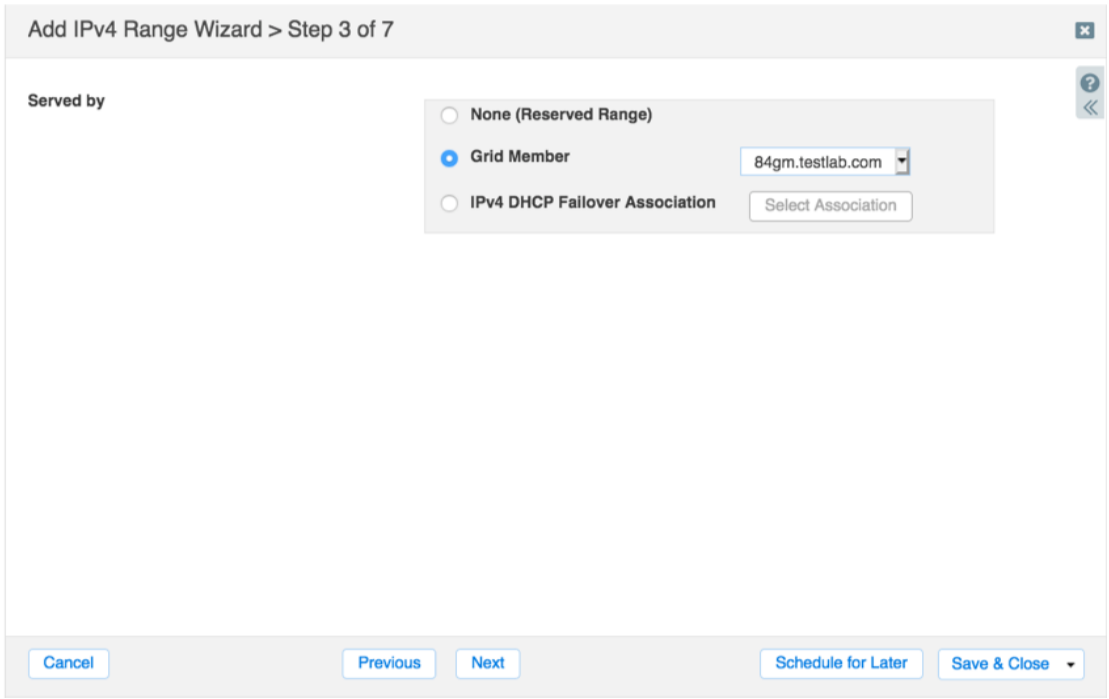
11. Click on the ‘+’ to add a DHCP range. This is the range of addresses that the DHCP server will distribute. Click ‘Next’



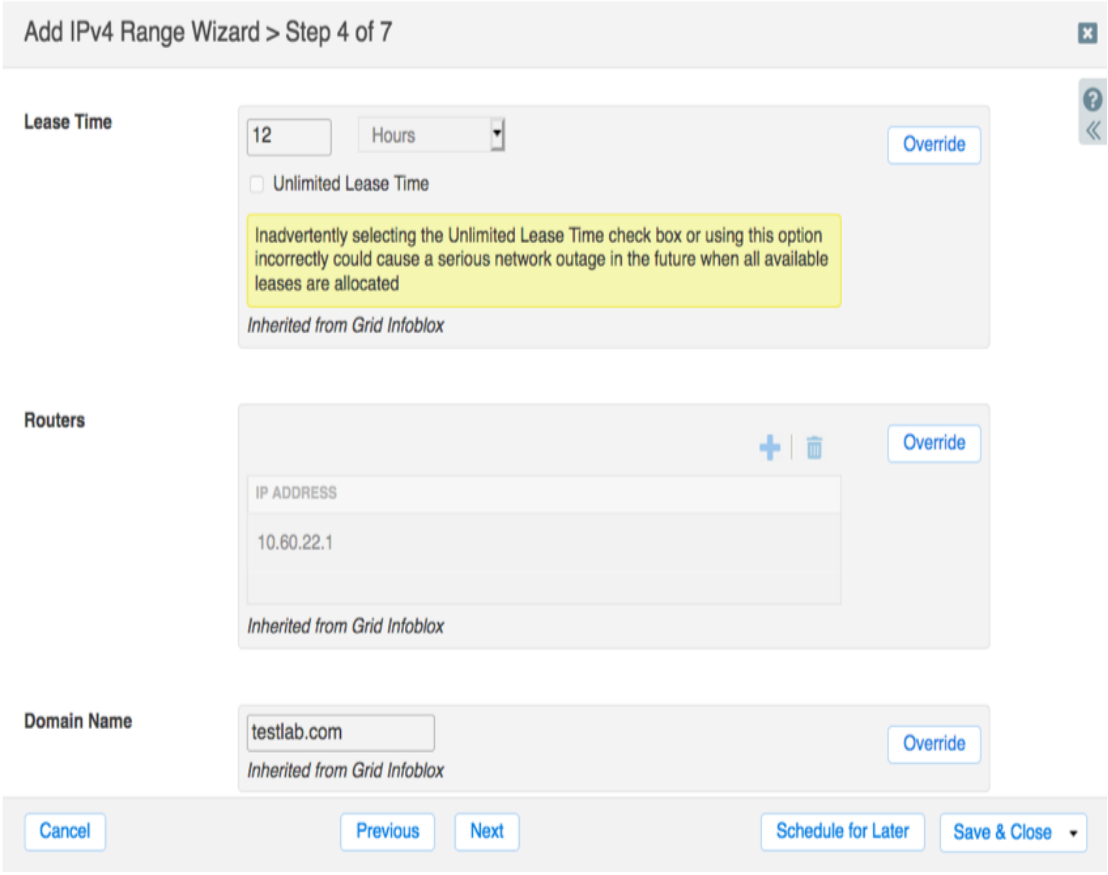
12. Configure the starting and ending addresses. ‘Click Next’.



13. Assign the Grid Member to serve the DHCP range. Click ‘Next’.

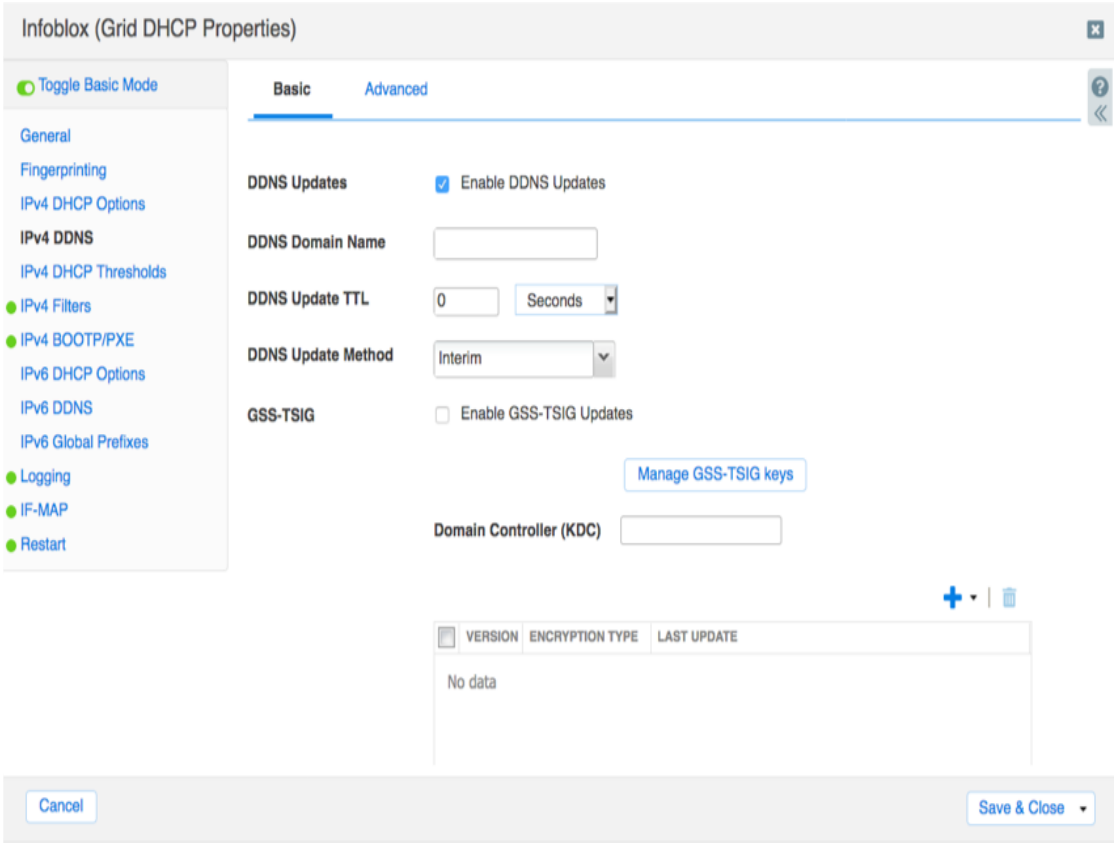


14. Verify the lease time, routers, domain name, and DNS servers. Click ‘Next’



15. Click Save and Close.

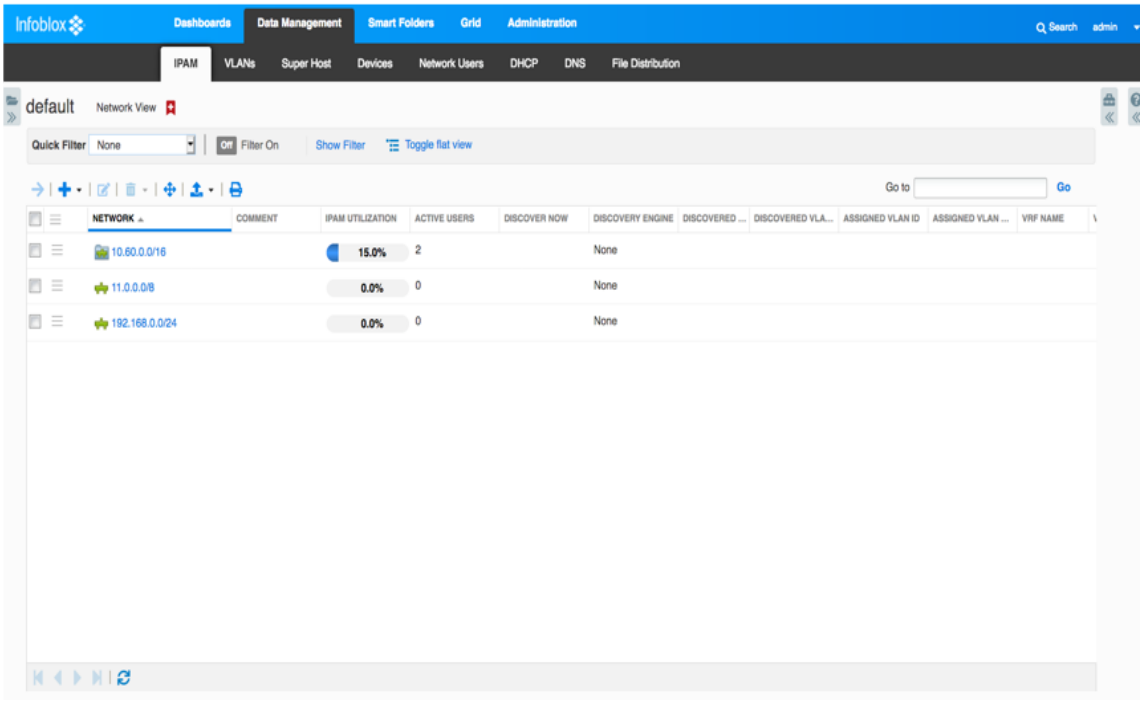
16. Navigate to Grid à Grid Manager à DHCP. Click on the pencil. Click on IPv4 DDNS. Enable DDNS. Click ‘Save and Close’.



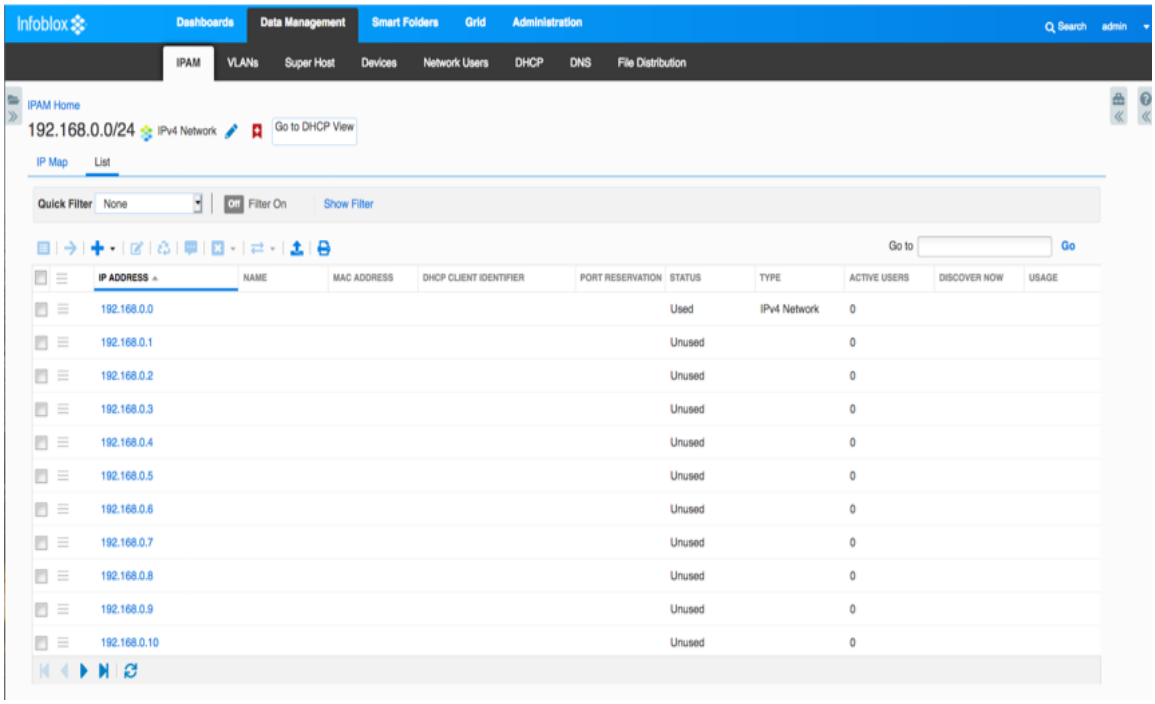
Configuring the display of the IPAM table

This section provides instructions on how to configure the display to show subscribed ISE specific information.

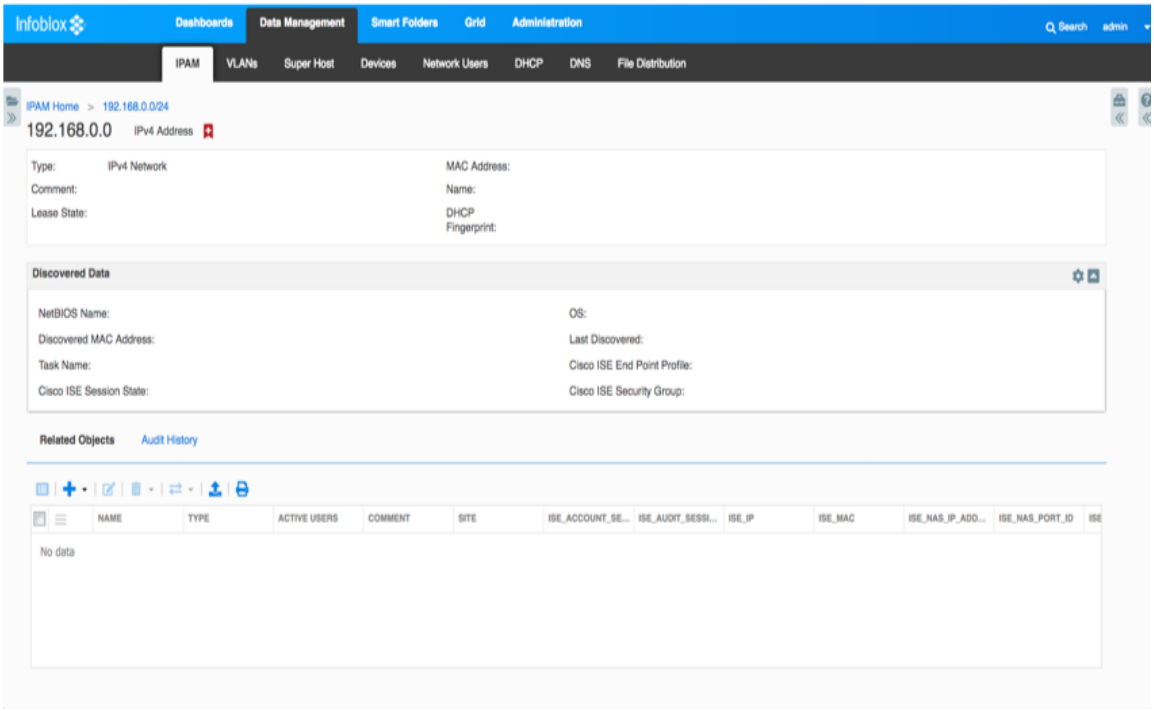
1. Navigate to Data Management --> IPAM



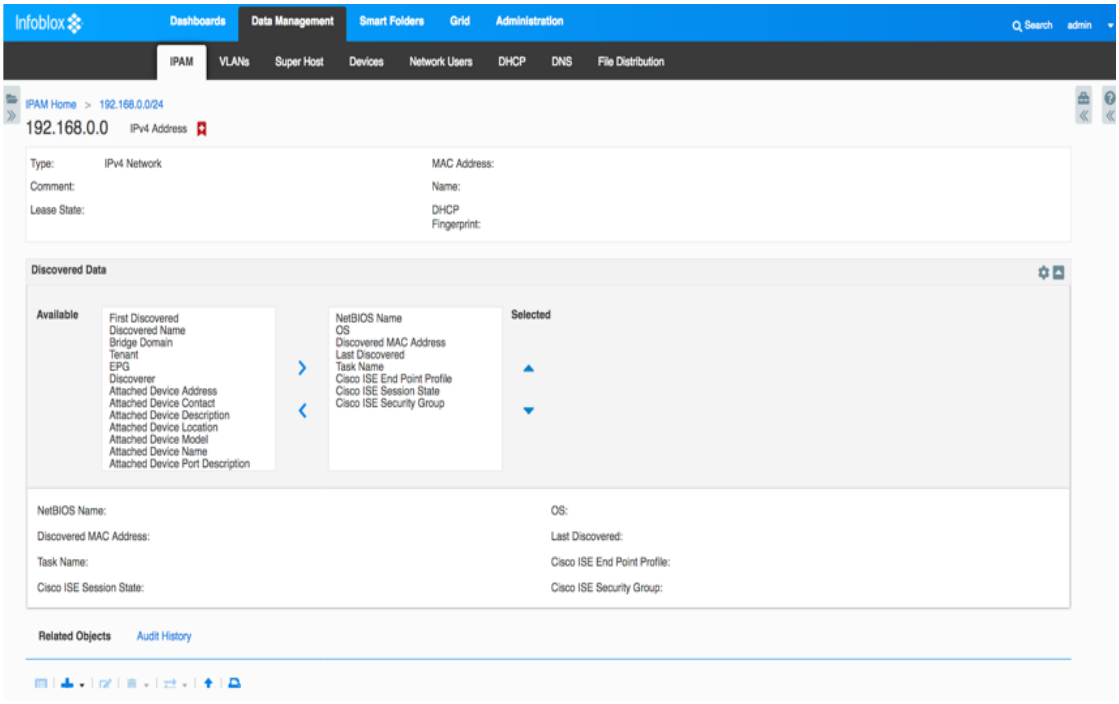
2. In this example, click on the 192.168.0.0 subnet. Click on List tab. A list of IP addresses will appear.



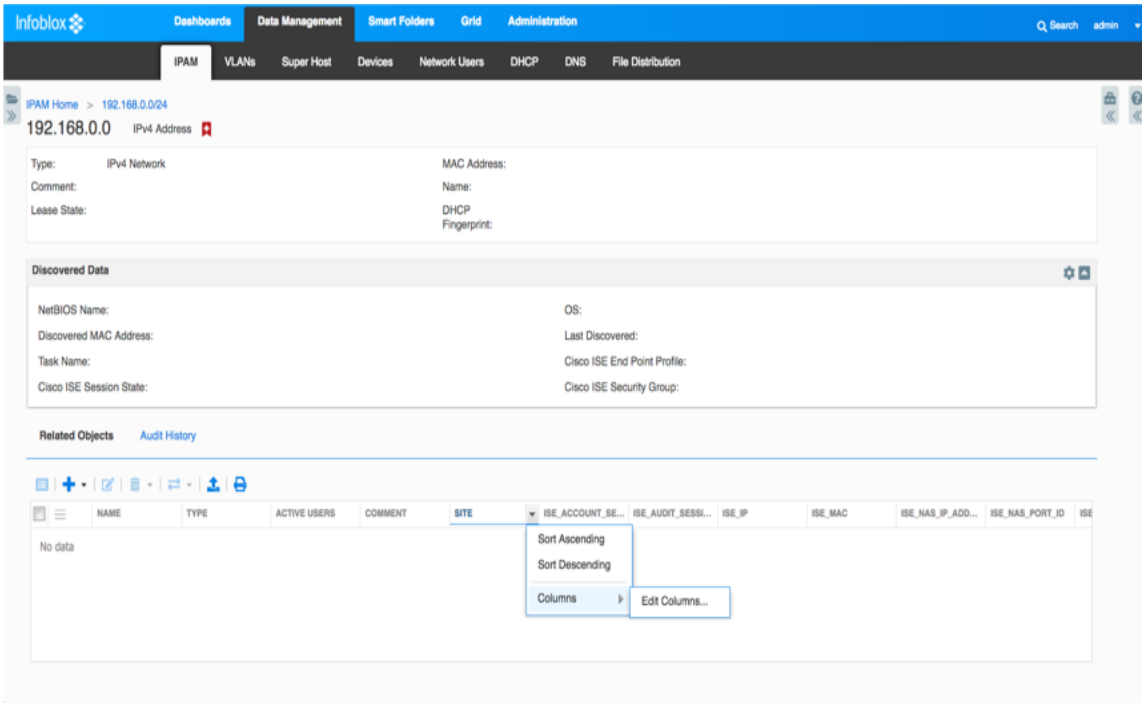
3. Click on any address



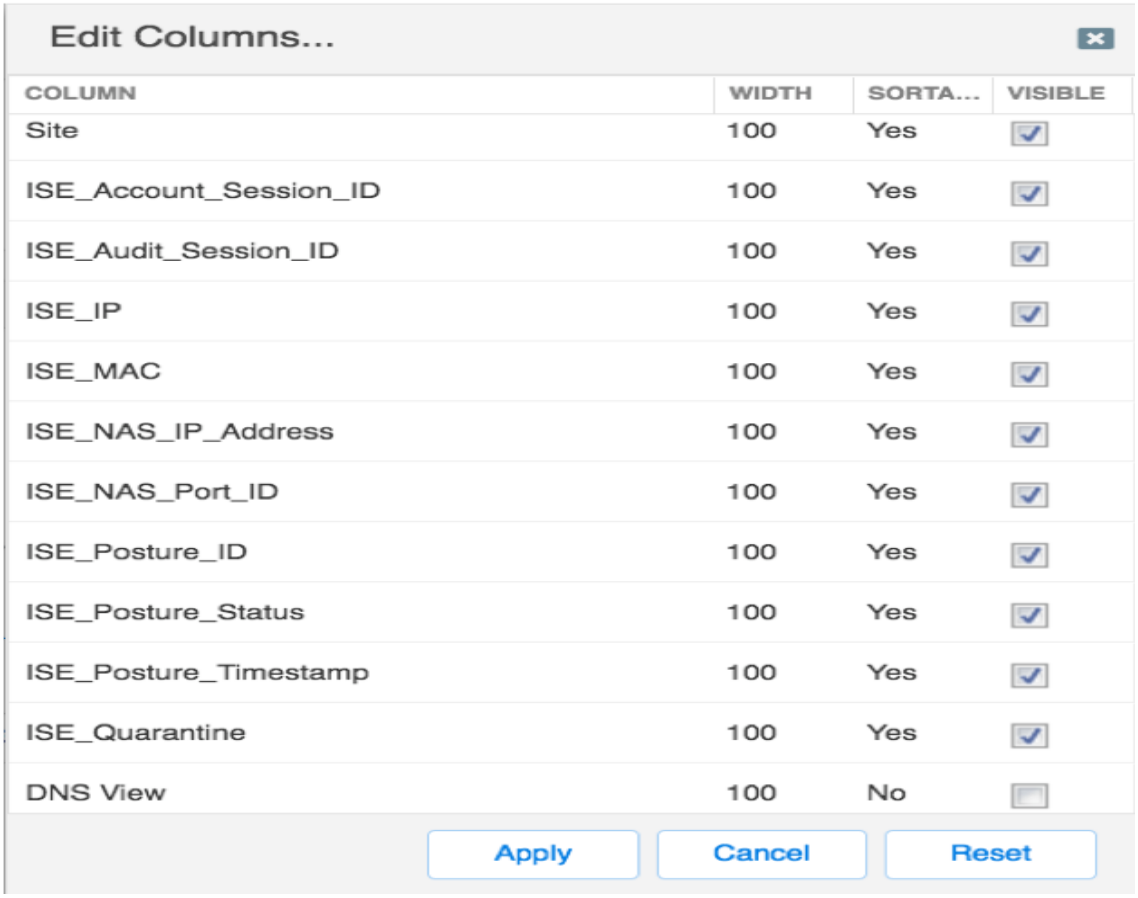
4. In the ‘Discovered Data’ section, you can configure which items discovered data items to display by clicking on the right side wheel and then move items from Available column to Selected column. Click on the wheel again to collapse.



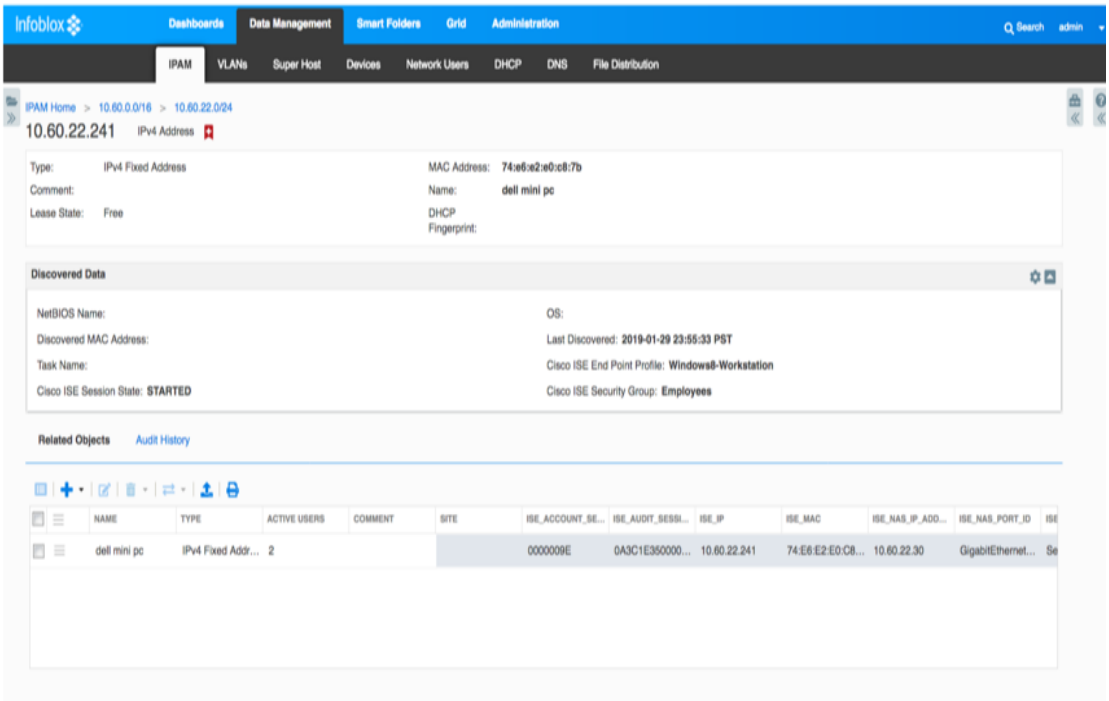
5. In the Related Objects area, you can add or delete columns. There is where you add the ISE related extensible attribute columns. Click on a column name → Columns → Edit Columns.



6. Click on Edit Columns and click ‘Visible’ box on each column you wish to display. Click on ‘Apply’



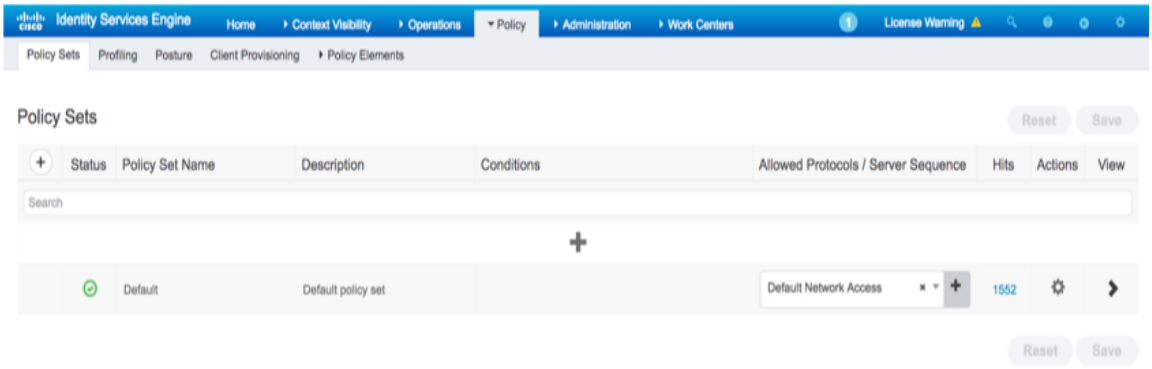
7. This is an example of an IPAM entry with ISE specific attributes.



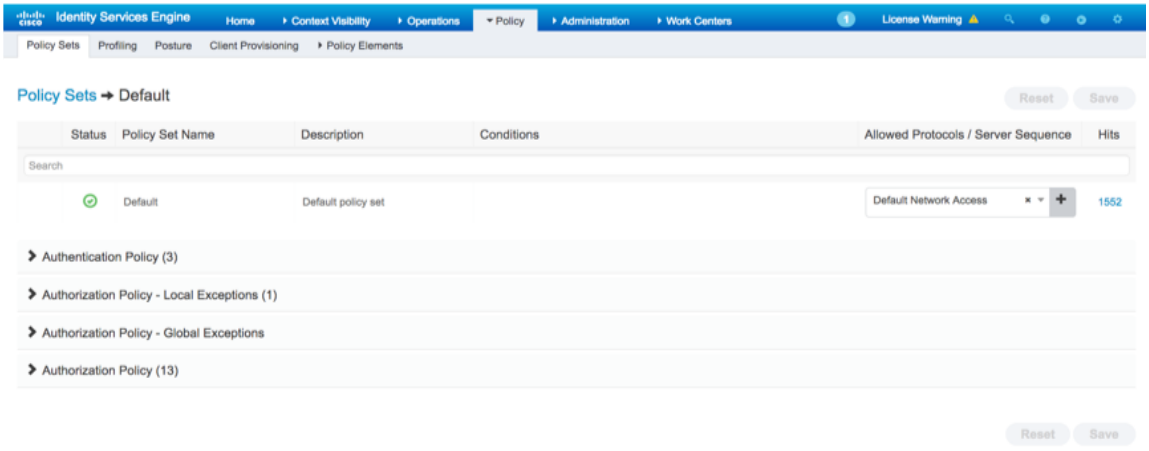
Adding an ISE EPS Quarantine Authorization Rule

This rule will be used to quarantine a client when the Infoblox grid member sends a notification to the ISE appliance when an RPZ entry has been hit by the client. For testing purposes, we will set the action to be permit access. However the status of the client will be in quarantine mode. Note: Please have your Cisco ISE expert configure this section.

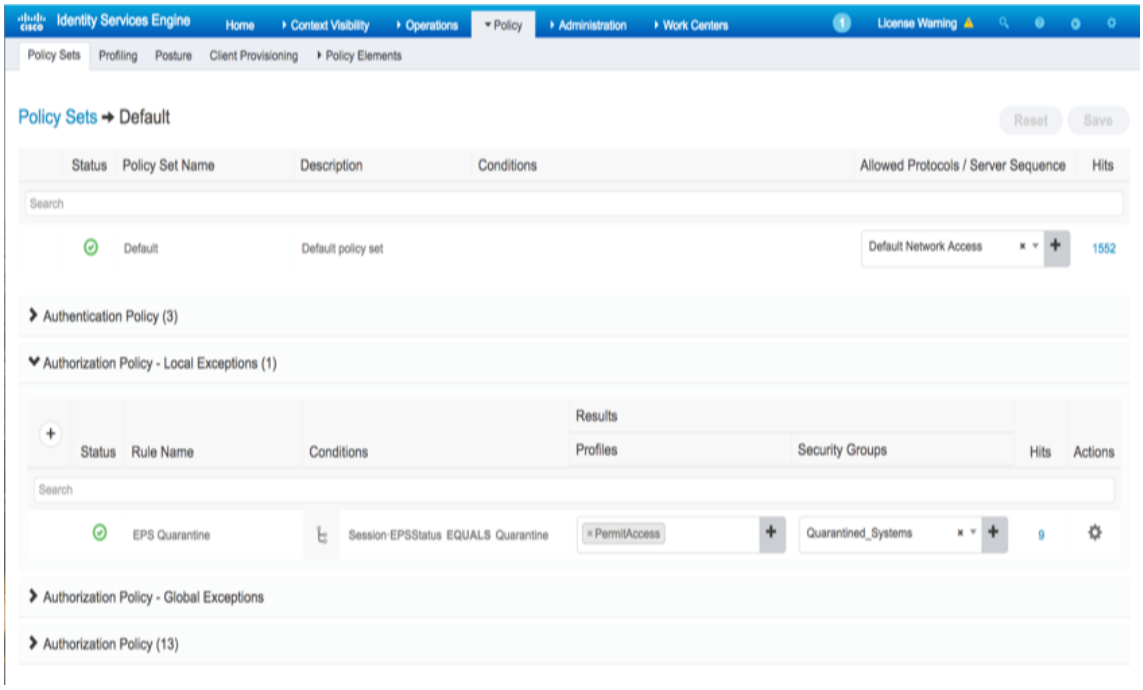
1. On the ISE GUI, navigate to Policy → Policy Sets



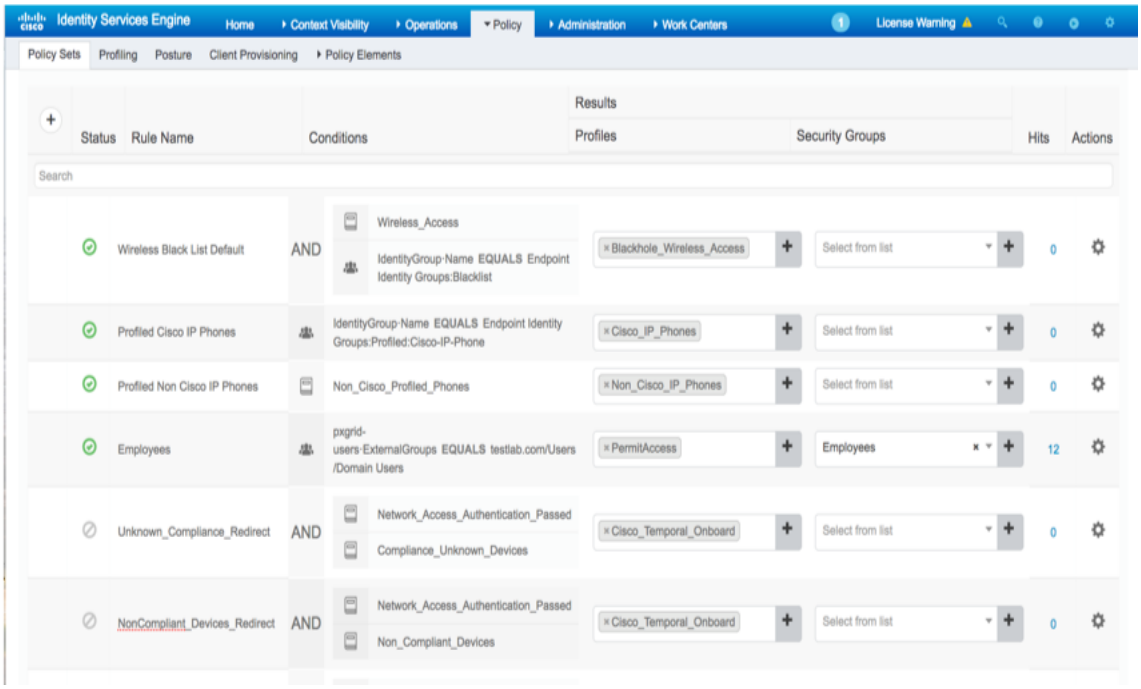
2. Click on the arrow on the right side and the following screen will appear



3. Add a Local Exception rule like the following



4. Go down to regular Authorization Policy and create an external group like Employees



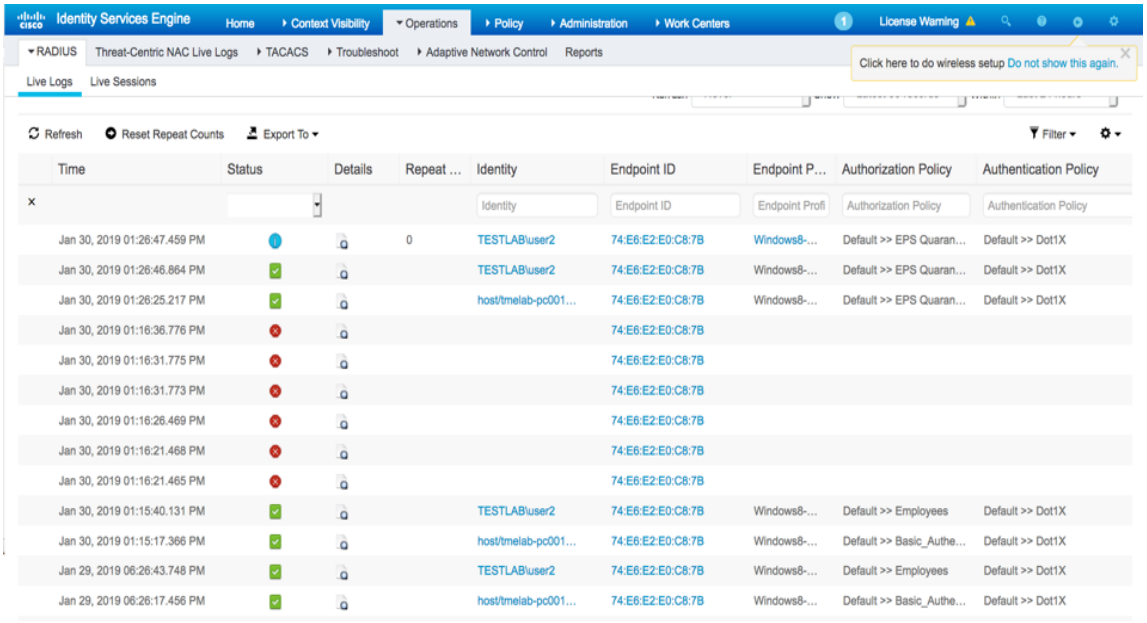
Testing

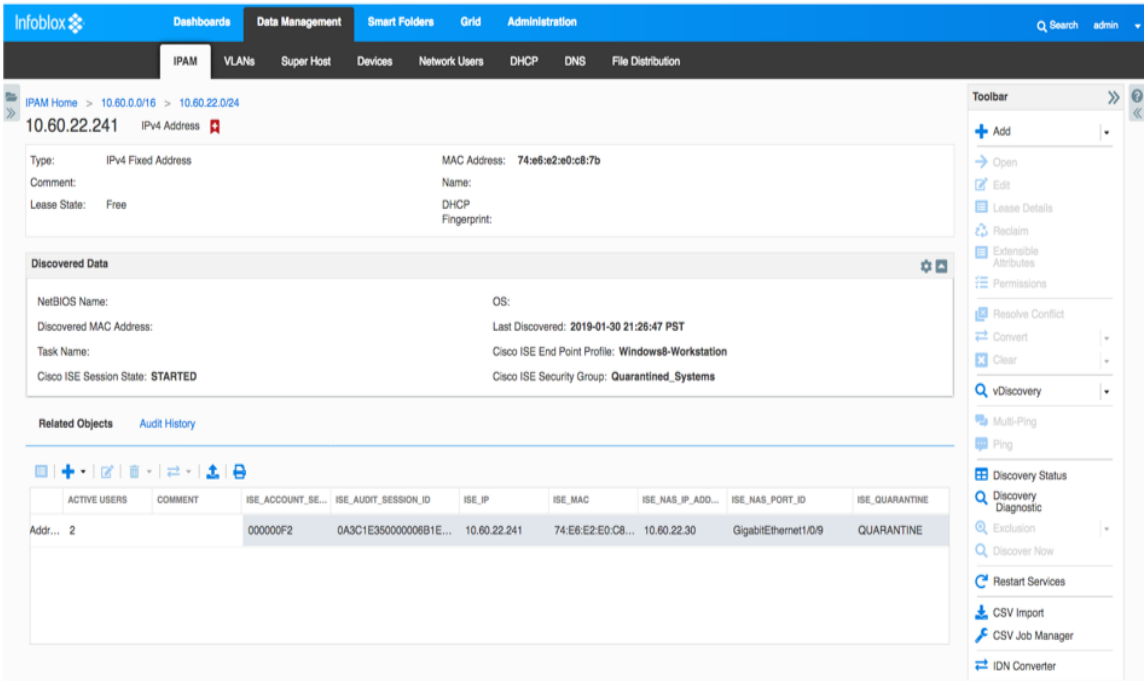
Here are the instructions for testing quarantining of a client that hits an RPZ entry.

1. After authenticating your client, run nslookup on Windows command window against www.yahoo.com or dig on Linux against www.yahoo.com. The commands are:

a. Windows: nslookup www.yahoo.com.
b. Linux: dig www.yahoo.com.

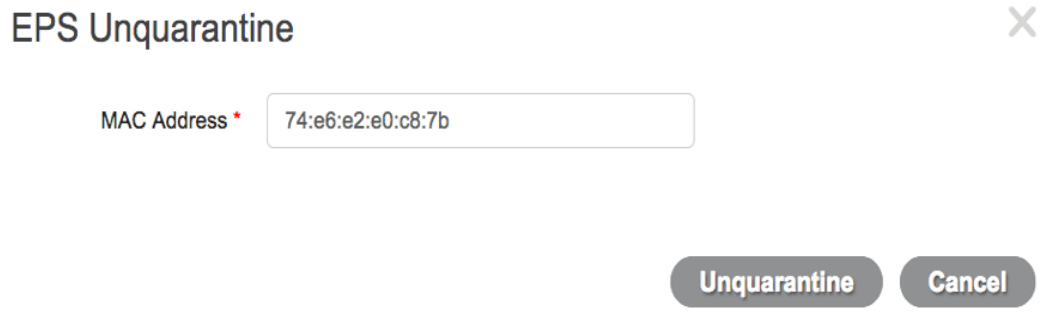
2. You should get an error indicating a non-existent domain.
3. The client should now be in quarantine state but it will not appear in the RADIUS Live Logs until the client is rebooted and the Infoblox IPAM entry for the client will update to quarantine state in the security group and EPS status.





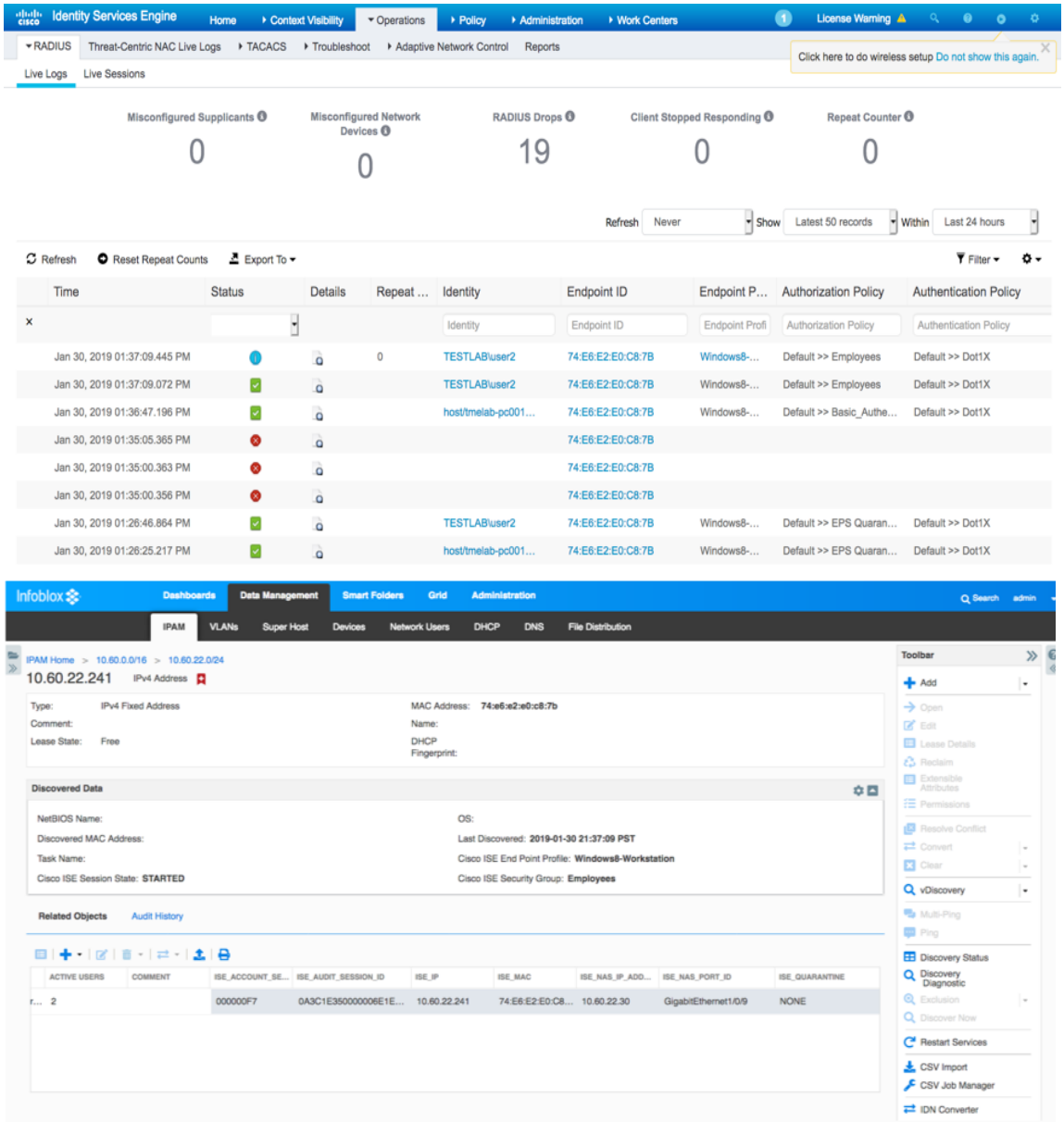
4. To unquarantined the client on the ISE GUI, navigate to Operations à Adaptive Network Control à Endpoint Assignment. Click on EPS unquarantine and type in the MAC address of the client.

Click ‘Unquarantine’.



5. Reboot the client.

6. The RADIUS authentication states for the client return to normal.



Troubleshooting

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

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

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.

Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com