



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	4
Introduction 5	
Technical Theory	7
Configuring the Infoblox Grid Master (GM) and Network Discovery (ND) Member	8
Configuring the Infoblox Grid Master	8
Creating Temporary Licenses	8
Configure Network Settings	9
Configuring the ND Grid Member	10
Creating Temporary Licenses	10
Configure Network Settings	10
Provisioning Grid Member to the Grid Master	11
Configuring for CA-signed Operation	12
Customized pxGrid template for CA-signed operation	12
Configuring Cisco ISE pxGrid Node	16
Configuring Infoblox Grid Master (GM)	22
Generating a public-private key pair certs for Infoblox	22
Configuring ISE Ecosystem settings	23
Configuring for Self-Signed Certificate Operation	28
Configuring Cisco ISE pxGrid Node	28
Configuring Infoblox Grid Master	29
Generating a public-private key pair cert, CSR Request and self-signed certificate for Infoblox	29
Importing Infoblox certificate into ISE trusted system store	30
Import ISE self-signed certificate into Infoblox trusted system store	31
Creating Infoblox Extensible Attributes for ISE	36
Enabling Data Management Network Users View	38
Dynamic Topics	40
Create IPAM Dynamic Topic	40
Create DHCP Dynamic Topic	43
Configuring DNS Services	47
Enabling DNS Service on Grid Master	47
Creating DNS Zone and DNS Zone for Dynamic Addresses	48
Configuring DNS Zone Properties	55
Add Policy Response Zone	60

cisco.

	Specifying Syslog Server for Notifications	64
	Adding RPZ Notification	65
Configuring	DHCP Services	67
	Configuring DHCP	67
Configuring	IPAM Table	78
Adding ISE E	PS Quarantine Authorization Rule	80
Testing	81	
Troubleshoo	ting	85
	Infoblox Grid Master ISE Ecosystem Status Error	85
	Adaptive Network Control (ANC) Mitigation Quarantine Mitigation Actions Not Showing Up ISE	85
	No Active User are Displayed under Infoblox Grid Maser Network Users	85
	Infoblox published Dynamic Topics do not Appear in ISE Capabilities Menu	85
References	86	

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 <u>www.yahoo.com</u>, 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 <u>https://communities.cisco.com/docs/DOC-68284</u>

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
<u>ClientID</u>
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.

dentity Serv	ices Engine H	Home	ns + Policy	For the second seco	ess - Administ	tration • Worl	Centers	0	Licens	e Warning	a 🔺	Q,
System Identit	ty Management 🔹 I	Network Resources	Device Portal M	Management	pxGrid Services	Feed Service	Identity Mappin	g				
Clients Live	Log								●Enable Aut	to-Registr	ation	Disable Vie
🖌 Enable 🛛 Ø Disable	e 😋 Approve 😝 🤇	Group 🎈 Decline 👩	Delete 👻 🛞 R	Refresh Total	Pending Approval(0)	*			1-5 of 5	Show 2	5 - 1	per page
Client Name		Client Description	(Capabilities		Status		Client Group(s	5)		Log	
ise-admin-ise2	201self		(Capabilities(4 Pu	ub, 2 Sub)	Online		Administrator			View	
□ ► ise-mnt-ise20	1self		(Capabilities(2 Pu	ub, 1 Sub)	Online		Administrator			View	
□ ▶ infoblox clier	nt publish 323223	infoblox cisco ise cli	ient (Capabilities(0 Pu	ub, 1 Sub)	Online		EPS,Infoblox	IPAM Publish	.Info	View	
infoblox_clier	nt_subscribe_3232	infoblox cisco ise cli	ient (Capabilities(0 Pu	ub, 2 Sub)	Online		EPS			View	
	Capability Detail						1 - 2 of 2	Show 25	 per page 	Page	1 🗘	
	Capability Name	e (Capability Version		Messaging Role		Message Filter					
	O Core	1	1.0		Sub							
	O SessionDirecto	ry 1	1.0		Sub							
	4	Test		Canabilitias/A.P.	(h. 0.0.(h))	offline		Consider		_	Maria	,
□ ▶ infoblox_che	ck_connectivity	Test	(Capabilities(0 Pt	JD, O SUD)	Offline		Session			View	



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 standalone node or to join a Grid.

Enter IP address: **192.168.1.88** Enter netmask: [Default: 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



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



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 Properties of New Template	×	
Careeral Dependent Version Science Requirements		
Certificate Templates (WIN-BG7GP(Certificate Templates (WIN-BG7GP(Ver 🔺	Actions
Template display name:	110	Certificate Templa 🔺
pxGrid	6.1	More Actions
Minimum Sunnarted CAs: Windows Server 2003 Enterrise	9.1	
Himman Supported Cris. Himatria Server 2005 Enterprise	4.1	User 🔺
Template name:	6.1	More Actions
pxGrid	7.1	
	8.1	
Validity particular Benergy and address	7.1	
5 mars 5 mars 5	105	
J years _ J JZ weeks _	101	
	100	
Publish certificate in Active Directory	101	
Do not automatically reenroll if a duplicate certificate exists in Active	5.1	
Directory	4.1	
Fas a domatic second of smart and antificates use the existing law	11	
For audoinate renewal or smart card centificates, use the existing Key	5.1	
	3.1	
	3.1	
	4.1	
	4.1	
		1
OK Cancel Apply Help		1

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

Certificate Templates Console		
File Action View Help	Properties of New Template	
Certificate Templates Console File Acton View Help Certificate Templates (WIN-BG7GP4 Certificate Templates (WIN-BG7GP4	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. Extensions included in this template: Basic Constraints Certificate Template Information Issuance Policies Key Usage Edit Description of Application Policies: Dient Authentication Secure Email Server Authentication	Ver Actions 110 Certificate Templa ^ 6.1 More Actions > 4.1 More Actions > 5.1 User ^ 4.1 More Actions > 10 10 101 10 105 10 101 10 102 10 103 1 4.1 4.1
· · ·	OK Cancel Apply Help	

Step 5 Click on Subject name, enable "Supply in the request"

🚇 Certificate Templates Console		1	
File Action View Help	Properties of New Template	×	
	Issuance Requirements Superseded Templates Extensions Security		
Certificate Templates (WIN-LTE11S	General Request Handling Subject Name Server © 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 game format: Image: Constance of the subject name in subject name in subject name. Include this information in alternate subject name. Image: Constance of the subject name. Subject principal name (UPNI) Sergice principal name (UPNI) © Sergice principal name (SPNI) Sergice principal name (SPNI)	Ver ▲ 4.1 110 6.1 7.1 8.1 7.1 8.1 7.1 8.1 7.1 105 101 105 101 5.1 4.1 5.1 4.1 1.1 5.1 4.1 1.1 5.1 4.1 1.1 1.1 1.1 1.1 1.1 1.1 1	Actions Certificate Templa More Actions More Actions
	Carricel Apply Help		

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

🖳 Certificate Templates Console		×
File Action View Help	Properties of New Template	1
	General Request Handling Subject Name Server Issuance Requirements Superseded Templates Extensions Security	
Certificate remplates (WIN-LIE11	To mortfix an extension related it and than olick Edit Edit Issuance Policies Extension Extent An issuance policy describes the conditions under which Ar a certificate is issued. Br Gr Gr issuance noticies:	Ver Actions 4.1 Certificate Templa ▲ 110 More Actions ▶ 4.1 User ▲ 5.1 More Actions ▶ 4.1 User ▲
	Is Issuance policies A All issuance policies	6.1 7.1 8.1 7.1 110 105
	Descri Cettfi Add Edt Remove	101 101 5.1 4.1 6.1
	Make this extension critical OK Cancel	11. 5.1 3.1 3.1 4.1
		4.1 101
	Cancel Apply Help	

Step 7 Leave the defaults for request handling

🖳 Certificate Templates Console		_ 🗆 🗙
File Action View Help	Properties of New Template	
Certificate Templates (WIN-LTE11S	Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name Server	Ver Actions
	Purpose: Signature and encryption	4.1 Certifical Templa 110 6.1 More Actions
	 Include symmetric algorithms allowed by the subject Archive subject's encryption private key 	4.1 5.1 Mare Actions
	Minimum key size: 2048	4.1 More Actions F 6.1 1 7.1 8.1 7.1
	Allow private key to be exported	11C 105
	Do the following when the subject is enrolled and when the private key associated with this certificate is used:	101 101
	Enroll subject without requiring any user input	5.1 4.1
	C Prompt the user during enrollment C Prompt the user during enrollment and require user input when the	6.1 11.
	private key is used	5.1 3.1
	Io choose which cryptographic service providers CSPs	3.1 4.1 4.1 101
۲ – •	OK Cancel Apply Help	×

- Step 8 Right-click on Certificate Templates
- Step 9 Select New Template to issue and select pxGrid



Step 10 You should see the pxGrid template

a certsrv - [Certification Authority	(Local)\lab7-WIN-LTE115BAKTM-CA\Cert	ificate Templates]
<u>File Action View Help</u>		
🗢 🔿 🙎 🖪 😫 👔		
Certification Authority (Local)	Name	Intended Purpose
🖃 🚽 lab7-WIN-LTE11SBAKTM-CA	🖳 pxGrid	Server Authentication, Secure Email, Encry
Revoked Certificates	R CEP Encryption	Certificate Request Agent
Issued Certificates	Rechange Enrollment Agent (Offline req	Certificate Request Agent
Pending Requests	IPSec (Offline request)	IP security IKE intermediate
Failed Requests	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
	Representation Authority	<all></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:

dentity Services Engine	Home ► Operations ► Policy ► Guest Access	✓Administration	nters		1	License
▼System → Identity Management →	Network Resources	Grid Services + Feed Service + I	dentity Mapping			
Deployment Licensing - Certificate	es + Logging + Maintenance Upgrade Backup &	Restore + Admin Access + Set	tings	8		
0						
✓ Certificate Management	Certificate Signing Requests					
Overview	Generate Certificate Signing Requests (CSR)					
System Certificates	A Certificate Signing Requests (CSRs) must be sent to a	nd signed by an external authority. Clic	k "export" to downlo	ad one or more CS	Rs so tha	at they ma
Endpoint Certificates	request has been signed, CICK "bind" to bind the request	to the signed certificate issued by that	authority. Once a C	SR is bound, it will	be remov	ed from ti
Trusted Certificates	PView Export XDelete Bind Certificate					Sh
OCSP Client Profile	Friendly Name	Certificate Subject	Key Length	Portal group t	Timestan	np
Certificate Signing Requests			No data available			
Certificate Periodic Check Settings						
Certificate Authority						

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 A	Alternative Name (SAN)	 iseinfo.lab10.com 	= +	٢
Step 7	Leave the defaults for Key Length, Digests to	Sign With and nothing for Certif	ficate 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
	Export
Step 9	Select Export



dentity Services Engine	tome Operations Policy Guest Access Administration Work Centers	0
▼System → Identity Management → I	Network Resources	
Deployment Licensing - Certificates	► Logging → Maintenance Upgrade Backup & Restore → Admin Access → Settings	
Cortificato Managoment	iseinfoAdmin - Notepad	
• Certificate management	File Edit Format View Help	
Overview	BEGIN CERTIFICATE REQUEST MIIC5jCCAC4CAQAwHDEaMBGEAUEAXMRaXNIaW5mby5sYWIXMC5jb20wggEiMA0G C5gC5Tb3DDEBA0UAA4TBDwawageKADTBA0Cx9buy/DbgirD+2e5xCot5DXFEz/C0P8aEUb+	÷.
System Certificates	+kv5kllewFGOPt2DmfNckOMsluij17R18yr6Sluwzq5xVq2Yk+EwC7HAA nNhgzP5pvBxiH36kmTt5quuTD725kFeJ+sb19rJxOS1BjimGCLJ5KXMILQOZUKSUOT	
Endpoint Certificates	+uElwxYTbnyYb1fG5WxjNvVptMGW6gd9+DY+p8XtKl1kEYPPpWbFKEufQAz6VA X5e4dydK2hDnWetqP5W93Vzzz8jyB2+R4A8Vo5I5aEeM10Mpf2E <u>tnVipMyeIm3Xn8bB0rXpukv9ra</u>	
Trusted Certificates	+V12ZXHTNEa6Ma3PLr/paPY5+Y/090XSaxDbHkpODx5AgMBAAGg gYOwgYEGCSgGSIb3D0EJDiF0MHIwHAYDVR0RBBUwE4IRaxNlaW5mbv5sYWIXMC51	
OCSP Client Profile	δ2ÔwĊwYDVRŮPBAQDAgXgMϐOGA1UdDgQWBBTaOaPuXmtLDTJVv++VYϐiQr9gHCTAŤ BgNVHSUEDDAKBggrBgEFBQCDATARBg1ghkgBhvhCAQEEBAMCBKAwDQYJKoZIhvCN	
Certificate Signing Requests	AQELBQADggEBACFGnWPZWEOT4Y56XK7rEMZRSyBUqVBh8+onczAZ8YExSmg3tsuy 2jfKZ3vvUxHpBqvzbYhDSBq3q1yvNfh7yagNC0GnQkgjiDxXIQrNQVPUeYorEjCd2rkAsWk6BHD	
Certificate Periodic Check Settings	+56463nonaxzyPLQUGBbgsozxS3qtum1RsvKE/y8jmB1nB/83/ytR+vANzAHa1rmo5IUBA4tQZj +zBjTUYXyZrV2qochA+tpJkV1XpT5UD4JhyatH4Xf6	
Certificate Authority	9NGp51188Hkxwha7lvs/2D4cfxEe75gyaqY=END_CERTIFICATE_REQUEST	

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

or PKCS #1

-

•

Microsoft Active Directory Certificate Services lab10-WIN-N3OR1A7H9KL-CA						
Submit a Cert	ificate Request or Renewal Request					
To submit a sat the Saved Req Saved Request:	ved request to the CA, paste a base-64-encoduest box.	ed CMC				
Base-64-encoded certificate request (CMC or PKCS #10 or	2jfKZJvVUxHpBqvzbYhDSBq3q1yVNfh7yagNCOGn 2rkAsWk6BHD+56463nonaxzyPLQUGBbgsozxS3qf +vANzAHairmo51UBA4tQZj+zBjTUYXy2rV2qOchA r3kkG5LiEbAnDypAYbOdQJR2rCZiFJ3NM/r5QQ3g 9NGp51iB8HkxWha71Vs/2D4cfxEe7SgyaqY=	A III				

-----END CERTIFICATE REQUEST-----

111

Step 12 Select customized pxGrid template

4

Certificate Template:

PKCS #7):

pxGrid_User

Step 13 Select Submit

Step 14 Select Base 64-encoded

Microsoft Active Directory Certificate Services -- Iab10-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 -- Iab10-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, certific

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 -- Iab10-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 meth	od:	
	© DER	
	Base 64	
Install CA cer	tificate	
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

dentity Services Engine	Home Operations Policy Guest Access Administration Work Centers
▼System → Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Identity Mapping
Deployment Licensing - Certifica	tes → Logging → Maintenance Upgrade Backup & Restore → Admin Access → Settings
Certificate Management Overview	Import a new Certificate into the Certificate Store * Certificate File Browse root.cer
System Certificates	Friendly Name
Endpoint Certificates	
Trusted Certificates	Trusted For: 👔
OCSP Client Profile	✓ Trust for authentication within ISE
Certificate Signing Requests	Trust for client authentication and Syslog
Certificate Periodic Check Settings	Trust for authentication of Cisco Services
Certificate Authority	Validate Certificate Extensions

Step 22 Select Submit

 Step 23
 Select Administration->System->Certificates->Certificate Signing Requests (CSR)

 You will see the following:

dentity Services Engine	Home	Access Administration Work Cent	lers	1 License Warning 🔺			
▼System → Identity Management → Network Resources → Device Portal Management pxGrid Services → Feed Service → Identity Mapping							
Deployment Licensing - Certifica	Deployment Licensing - Certificates + Logging + Maintenance Upgrade Backup & Restore + Admin Access + Settings						
0							
✓ Certificate Management	Certificate Management Certificate Signing Requests						
Overview	Generate Certificate Signing Requests (CSR)						
System Certificates	A Certificate Signing Requests (CSRs) must be s	ent to and signed by an external authority. Click	"export" to download one or more C	SRs so that they may be signed by an			
Endpoint Certificates	Endpoint Certificates 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.						
Trusted Certificates	Niew @Export XDelete Bind Certificate			Show All			
OCSP Client Profile	Friendly Name	Certificate Subject	Key Length Portal group t	Timestamp 🔺			
Certificate Signing Requests	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

dentity Services Engine	Home	y → Guest Access → Administration → Work Centers	1	License Warning 🔺
▼System → Identity Management	Network Resources Device Port	al Management pxGrid Services + Feed Service + Identity Mapping		
Deployment Licensing - Certifica	tes + Logging + Maintenance	Upgrade Backup & Restore + Admin Access + Settings		
♥ ▼ Certificate Management	Bind CA Signed Certificate			
Overview System Certificates	* Certificate File	Browse iseinfo.cer		
Endpoint Certificates	Friendly Name			
Trusted Certificates				
OCSP Client Profile	Validate Certificate Extensions			
Certificate Signing Requests				
Certificate Periodic Check Settings	Usage			
Certificate Authority		Admin: Use certificate to authenticate the ISE Admin Portal		
		Submit Cancel		

Step 25 Select Submit

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

dentity Services Engine	Home	olicy + Guest Access	 Administration 	Work Centers		License Warning 🔺
System Identity Management	Network Resources Device F	Portal Management pxGr	id Services Feed S	ervice Identity Mapping		
Deployment Licensing - Certificat	es + Logging + Maintenance	Upgrade Backup & R	testore + Admin Acce	ess • Settings		
0						
✓ Certificate Management	System Certificates 🛕 For	disaster recovery it is recor	mmended to export cert	ificate and private key pairs of	of all system certificates.	
Overview	🕖 Edit 🕂 Generate Self S	Signed Certificate 🛛 🕂 Im	port 💽 Export 🔀	🕻 Delete 🔎 View		
System Certificates	Friendly Name	Used By Port	al group tag	Issued To	Issued By	Valid From
Endpoint Certificates	▼ iseinfo					
Trusted Certificates	iseinfo.lab10.com,iseinfo ab10.com#lab10-WIN-N3	Authentication, Defa	ault Portal Certificate	iseinfo.lab10.com	lab10-WIN-N3OR1A7H9K	Thu, 12 May 2016
OCSP Client Profile	OR1A7H9KL-CA#00001	pxGrid Grou	nbŵ		L-GA	

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

dentity Services Engine	Home > Operations >	Policy Guest Access	- Administration	Work Centers	
▼System ► Identity Management	Network Resources Device	ce Portal Management pxGri	d Services + Feed	Service Identity Mapp	
Deployment Licensing - Certification	tes + Logging + Maintenan	ce Upgrade Backup & R	estore	ess + Settings	
0					
- Certificate Management	System Certificates 🛕	For disaster recovery it is recor	nmended to export cer	tificate and private key pai	
Overview	📝 Edit 🕂 Generate Se	elf Signed Certificate) 🕂 Imp	ort 💽 Export	🕻 Delete 🔎 View	
System Certificates	Friendly Name	Used By Porta	al group tag	Issued To	
Endpoint Certificates	▼ iseinfo				
Trusted Certificates	iseinfo.lab10.com,ise ab10.com#lab10-WIN	info.I EAP I-N3 Authentication, Defa	ult Portal Certificate	iseinfo.lab10.com	
OCSP Client Profile	OR1A7H9KL-CA#000	01 pxGrid Grou	p. <u>(</u>)		
Certificate Signing Requests					

Step 28 Enable pxGrid



Step 29 Select Save



Step 30 Select Administration->pxGrid Services

You should see the ISE published nodes

dentity Services Engine	Home	Guest Access - Admin	stration • Work Centers	0) 🛛 License Warning 🔺 🔍
System Identity Management	Network Resources Device Porta	al Management pxGrid Services	Feed Service Identity Mappin	g	
Clients Live Log					€Enable Auto-Registration Disable
✓Enable ØDisable ØApprove ⊕G	iroup 👎 Decline 🚷 Delete 👻 🛞 Refre	sh Total Pending Approval(0) 👻			1-5 of 5 Show 25 - per pag
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 1Upload the CA root certificate into the Infoblox Grid Master
Select Grid->Grid Manager->Members->Grid Master->Certificates->Manage CA Certificates



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

	Dashboards	Data Ma	inagement S	mart Folde	ers	Grid A	dministration			
	Grid Manager	Upgrade	Licenses H	SM Group	Micro	osoft Servers	Device Suppo	rt Ecosysi	em	
Finder «	niosgm2	. / x								
Active Directory Sites Active Directory Sites Apple Mac OS Devices	DHCP DN	<u>s</u> <u>tftp</u>	HTTP (File Dist)	ETP	NTP	bloxTools	Captive Portal	Discovery	Threat Analytics	TAXII
Gaming Console Devices	Members Quick Filter	Services	V Off	Upload	-	-	_	_	_	×
Reversion of the second s	Group	Results	Group By Chee	FI	root.cer			Select	Upload	
Com Smartphone, PDA, Tablet De De De De De Do Do	Go to	Name	Go							
	V \$	🔶 nios	sgm2.lab10.(No	Clos	se					

- Step 3 Select Grid->Ecosystem->+-> add the ISE pxGrid node->General
- **Step 4** Enter the **IP address** of the ISE pxGrid node



Step 5 Select the ISE version number

Note: This will work for ISE 2.0 and ISE 2.1



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

Subscribing Member * niosgm2.lab10.com Select Clear

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

192.168.1.125 (Cisco ISE	Destance destruction and the second
	Basic
General Subscription Publication Extensible Attributes	Server Address* 192 168.1.125 Version* 2.0 Subscribing Member * niosgm2 lab10 com Select Clear Upload
	File niosgm2.pem Select Upload
	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

	Basic		
General Subscription Publication Extensible Attributes	Server Address* Version* Subscribing Member * Client Certificate *	192.168.1.125 2.0 - niosgm2 lab10.com Select Clear Select	
	Certificate *	Select	
	File root.cer	Select Up	load

Step 9 Select the CA-root certificate for Manage Certificates

	Basic							«	7
General Subscription Publication Extensible	Server Address* Version* Subscribing Member	192.168 2. CA • nic	3.1.125 Certifi	icates					=
Attributes	Client Certificate	0		Issuer CN="lab10-WIN	Valid From 2016-03-28 19:	Valid To 2021-03-28 19:	Subject CN="lab10-V	/N-N3OR1A7H	KL-CA"
	Manage Certificates	0							

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

	Basic	
General	Server Address* 192.168.1.125	
Subscription Publication	Version* 2.0 •	
Extensible Attributes	Subscribing Member * niosgn2.lab10.com Select Clear Client Certificate * Select	
	Bulk Download Certificate • Select	
	Manage Certificates * CA Certificates	
	Comment	
	Disable	

Step 11 Select -> Next

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

<u>Note:</u> 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



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

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

ap other data types t	+ 0		
Data Type	Extensible Attributes		
Audit Session ID	ISE_Audit_Session_ID	A	
EPS Status	ISE_Quarantine	-	
NAS IP Address	ISE_NAS_IP_Address	1	
MAC	ISE_MAC		
IP Address	ISE_IP	-	
NAS Port ID	ISE_NAS_Port_ID	-	
Account Session D	ISE_Account_Session_ID		

- Step 14 Select -> Next
- Step 15 Select -> Publication
- **Step 16** Move all the available attributes into the Selected Column

92.168.1.70 (Cisco ISE)	Basic		_		
General Subscription Publication Extensible Attributes	Publication Settings	Avalable	*	Selected Attached Device Name Attached Device Port Attached Device Model Attached Device Wendor Client D Friger Prior Friger Prior Prior Prior Wender Infolox 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.

Infoblox 💸	Dashboards	Data Manage	ment Smart Fo	olders Grid	Administration	1				
	Grid Manager	Upgrade I	Licenses HSM G	roup Microsoft	Servers Device	Support Ecosys	item			
Finder	Cisco No	tification								
Smart Folders	01									
Active Directory Sites	Cisco	9								
Apple Mac OS Devices Conflicts	Quick Filter	None	✓ Off Filter 0	Show Filte	<u>n</u>					
Discovered Switches/Route	Go to		Go						1	BO-12
Gaming Console Devices	_									
🕀 🌆 Microsoft Windows Devices		Address A	Status							Client Certificate Subje
Router and Wireless Access		192.168.1.125	Running	Cisco ISE	2.0		No	niosgm2.lab10.c	default	CN="niosgm2.lab10.cr
Smart Folder										

Step 19You can also verify in ISESelect Administration->pxGrid Services

	ns		/ork Centers	🕕 🛛 License Warning 🔺	9. 0 1 0 4
System Identity Management Network Resources	Device Portal Management pxGrid	Services Feed Servic	e 🔸 Identity Mapping		
Clients Live Log				eEnable Auto-Registration Dis	sable Auto-Registration View By Capabilities
√Enable Ø Disable Ø Approve G Group P Dedine O Dedine	lete 👻 😵 Refresh 🛛 Total Pending Approval	(0) -		1-5 of 5 Show 25 - pe	rpage Page 1 ‡
Client Name Client Description	Capabilities	Status	Client Group(s)	Log	
□ ► ise-admin-ise201	Capabilities(4 Pub, 2 Sul	o) Online	Administrator	View	-
□ ▶ ise-mnt-ise201	Capabilities(2 Pub, 1 Sul	o) Online	Administrator	View	
infoblox_client_subscribe_32322 infoblox cisco ise client	ient Capabilities(0 Pub, 2 Sul	o) Online	EPS	View	
Capability Detail			1 - 2 of 2 Show 25 💌 p	er page Page 1 🗘	
Capability Name	Capability Version	Messaging Role	Message Filter		
O Core	1.0	Sub			
O SessionDirectory	1.0	Sub			
•					
□ ▶ iseagent-fmc61.lab10.com-2514	Capabilities(0 Pub, 0 Sul	b) Offline	ANC, EPS	View	
fresightisetest-fmc61.lab10.com	Capabilities(0 Pub, 0 Sul	b) Offline	ANC, EPS	View	_
onineces in prone					

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



- Step 2 Enable **pxGrid**
- Step 3 Select Save
- Step 4 Select Administration->pxGrid Services to view the ISE published nodes

dentity Services Engine	Home	olicy Guest Access Admini	stration • Work Centers	U Licen:	ise Warning 🔺 🔍 🐵 🔳	ø
System Identity Management	Network Resources Device	Portal Management pxGrid Services	Feed Service Identity Mapping			
Clients Live Log				⊜Enable At	uto-Registration Disable Auto-Registratio View By Capabilitie)n BS
🖌 Enable 🕜 Disable 🔮 Approve	😝 Group 🛛 👎 Decline 🛛 🚷 Delete 👻	Refresh Total Pending Approval(0)) -	1-5 of 5	Show 25 v per page Page 1	÷
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 1Import 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

dentity Services Engine	Home	This Certificate has a signature that uses the SHA-1 hashing	0 License Naming 🔺
System Identity Management	Network Resources Povice Port:	algorithm and is considered less secure.	
Deployment Licensing Certific	ates + Logging + Maintenance (Are you sure you want to import this certificate?	
Certificate Management	Import a new Certificate into		
Overview	* Certificate File	Browse infoself.cer	
System Certificates	Friendly Name		0
Endpoint Certificates		Trusted For: (1)	
Trusted Certificates		Trust for authentication within ISE	
OCSP Client Profile		Trust for client authentication and Syslon	
Certificate Signing Requests		Tout for authentication of Circo Sonicos	
Certificate Periodic Check Settings			
Certificate Authority		Validate Certificate Extensions	
	Description]
		Submit Cancel	

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

dentity Services Engine	Home	→ Administra	tion • Work Centers		U License Wa	aming 🔺 🔍 🍣	± 0		
▼System → Identity Management → Network Resources → Device Portal Management pxGrid Services → Feed Service → Identity Mapping									
Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings									
0	Cisco CA Manufacturing	Ø Disabled	Endpoints Infrastructure	6A 69 67 B3 00 0	Cisco Manufacturing CA	Cisco Root CA 2048	Fri, 10 Jun		
✓ Certificate Management	Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure	02	Cisco Manufacturing CA	Cisco Root CA M2	Mon, 12 N		
Overview	Cisco Root CA 2048	Ø Disabled	Endpoints Infrastructure	5F F8 7B 28 2B 54	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May		
System Certificates	Cisco Root CA M2	Enabled	Endpoints Infrastructure	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 N		
Endpoint Certificates	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		
Trusted Certificates	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 21		
0000 Client Profile	niosgm.lab10.com#niosgm.lab10.com#00006	Enabled	Infrastructure	FA 67 04 56 20 2	niosgm.lab10.com	niosgm.lab10.com	Fri, 22 Jul :		
OGSP Client Frome	Thawte Primary Root CA	Enabled	Cisco Services	34 4E D5 57 20 D	thawte Primary Root CA	thawte Primary Root CA	Fri, 17 Nov		
Certificate Signing Requests	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		
Certificate Periodic Check Settings	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		
Certificate Authority									

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

dentity Services Engine	Home	licy + Guest Access	✓ Administration	Work Centers	N 0	License Warning 🔺	Q 0	± 0
▼System → Identity Management →	Network Resources	ortal Management px	Grid Services + Feed	Service Identity Mappin	3			
Deployment Licensing - Certificate	s + Logging + Maintenance	Upgrade Backup &	Restore + Admin Acc	cess + Settings				
0								
✓ Certificate Management	System Certificates 🔥 For	disaster recovery it is rec	commended to export cer	rtificate and private key pairs	of all system certificates.			
Overview	🕖 Edit 🕂 Generate Self S	igned Certificate 🛛 🕂 1	Import 💽 🚱 Export	🕻 Delete 🔎 View				
System Certificates	Friendly Name	Used By Po	ortal group tag	Issued To	Issued By	Valid From	Expiration Date	5
Endpoint Certificates	▼ ise201self							
Trusted Certificates	Default self-signed server	EAP r Authentication, D	efault Portal Certificate	ise201self.lab10.com	ise201self.lab10.com	Fri, 1 Jul 2016	Sat, 1 Jul 2017	
OCSP Client Profile	centricate	Admin, Portal, Gi pxGrid	roup					_

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



Step 3 Select the **Export** button and save the Defaultsignedservercerti.pem file.

Step 4Upload 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

	Dashboards Data Management Smart Folders Grid Administration	
	Grid Manager Upgrac CA Certificates	× 8
Finder	A data and a construction of the second	

Step 5 Select Upload

Step 6 You should see that the upload was successful



- 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



Step 10 Select the ISE version number



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

Subscribing Member * niosgm2.lab10.com Select Clear

Step 12 Upload the Infoblox concatenated PEM file for Client Certificate

192.168.1.120 (Cisco ISE)	Basic				×	
General Subacciption Publication Extensible Attributes	Server Address* Version* Subscribing Member * Client Certificate* Buik Download Certificate * Manage Certificates * Comment	192.168.1.120	Upload File Criskeppthintperf per Close		elect Ur	Add Cisco Er Edx Collecte Collect
Cancel				Save & Close •		

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

192.168.1.120 (Cisco ISE		×
192.108.1.120 (Cisco ISB General Subscription Publication Extensible Attributes	Basic Server Address* 192168.1120 Version* 20 Version* 20 Version* 20 Version* Client Certificate Builk Download Gelect Certificate* Manage Certificates* Test Credentials Test Credentials Test Credentials Test Credentials Test Credentials Test Credentials	Toolbar Add Cisc Edd Delete Z IDN Con View C
Cancel	Disable Close -	

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

Infoblox 📚	Dashboards	Data Management	Smart Folders	Grid Administ	ration	
	Grid Manager	192.168.1.120 (Cisco ISE)	ALC: NO DO		and the state of the Destate of the state of	×
Finder «	Cisco No	CA Certificates	Basic			×
Bookmarks +	Cisco					© »
Recycle Bin +	Quick Filter	lissuer	Valid From	Valid To	Subject	
	Go to	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		CHERRY INCOMENDATION CONTRACTOR	
			2
The credential test wa	s successful.		
	Basic		
General Subscription Publication Extensible Attributes	Server Address* Version* Subscribing Member * Client Certificate * Bulk Download Certificate * Manage Certificates * Comment	192.168.1.120 2.0 • niosgm2 lab10.com Select Clear Select Select CA Certific ates Test Credentials	
		Disable	
			-

Step 16 Select Next

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

<u>Note:</u> 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

General	To view subscription	data in Grid Manager	enable the Netwo	rk Users feature in the Genera	1->
Subscription	Advanced tab of the	Grid Properties Editor.			
Publication	Subscription Settin	igs*			
Extensible		Available Data Typ	es	Selected Data Types	
Attributes		SSID VLAN	*	Domain Name End Point Profile Security Group Session State User Name	^
			-		~



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

ap other data types to	+ 0	
Data Type	Extensible Attributes	
Audit Session ID	ISE_Audit_Session_ID	A
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	1
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

	, i			
General	Publication Settings			
Subscription		Available	Selected	
Publication Extensible Attributes			 Attached Device Name Attached Device Model Attached Device Model Attached Device Vendor Clent D Finger Print First Discovered Host Name Infoliox Member	* III *

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.

dentity Services	Engine Home +	Operations Policy	Guest Access	- Administration	Work Centers	Licer	nse Warning 🔺	Q,
System Identity Ma	anagement • Network Res	ources Device Portal	Management pxGri	d Services + Feed	Service Identity Mapping	g		
Clients Live Log						⊖Enable A	Auto-Registration D	Disable Vie
✓ Enable Ø Disable	😋 Approve 🛛 😝 Group 🛛 👎 De	ecline 😵 Delete 👻 😵	Refresh Total Pending	Approval(0) +		1 - 5 of 5	Show 25 - p	er page
Client Name	Client Desc	cription	Capabilities	Status		Client Group(s)	Log	
□ ► ise-admin-ise201s	elf		Capabilities(4 Pub, 2 S	Sub) Online		Administrator	View	
□ ► ise-mnt-ise201self	F		Capabilities(2 Pub, 1 S	ub) Online		Administrator	View	
□ ► infoblox client p	ublish 323223 infoblox ci	isco ise client	Capabilities(0 Pub, 1 S	ub) Online		EPS.Infoblox IPAM Publ	ish,Info View	
infoblox_client_subscription	ubscribe_3232 infoblox ci	isco ise client	Capabilities(0 Pub, 2 S	Sub) Online		EPS	View	
Cap	pability Detail				1 - 2 of 2	Show 25 🔻 per pag	e Page 1 🌲	Ê
	Capability Name	Capability Version	Me	ssaging Role	Message Filter			
0	Core	1.0	Su	b				
0	SessionDirectory	1.0	Su	b				
								•
Infoblox check of	onnectivity Test		Capabilities(0 Pub, 0 S	ub) Offline		Session	View	

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)				
	Basic			
General Additional Properties	Name* Type Number of characters Comment	ISE_Quarantine		

Step 3 Select Next

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

ISE_Quarantine (Extensible Attribute)					
	Besic				
General Additional Properties					
		-			

Step 5 Select Save and Close
Step 6Repeat 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

	Dashboard	s Data Manag	gement	Smart Folders	Grid Administ	ration	
	Administrato	rs Workflow	Logs	Network Views	Extensible Attributes	Authentication Server	Groups N
Finder Smart Folders Hookmarks	Extens Quick Filte	ible Attribute ^{r None}	s 🕺	H Filter On	Show Filter		
<u>Infolab</u> <u>default</u> <u>SysLoq-infolab.lab1</u>	Go to	v	Go	Comme	nt Required	Restricted to Ob	Inheritance Er
CiscoISE Notification 192.168.1.0	VLAN State		String String String		No No	IPv4 Network,IP IPv4 Network,IP	No No No
<u>192.168.1.0/24</u> Active Network Us	Site Regio	uarantine	String String String		No No	Dud Naturark D	No Yes
	ISE_P	osture_Timestamp osture_Status	String String		No		Yes Yes
	ISE_N	AS_Port_ID AS_IP_Address	String String String		No No		Yes Yes Yes
	ISE_P	udit_Session_ID	String String		No No		Yes Yes
	IB Dis	covery Owned	String String		NO NO 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

		Dashboards	Data Man	agement Sr	nart Folders	Grid	Administration					
		Grid Manager	Upgrade	Licenses H	SM Group	Microsoft Se	ervers Device	e Support Ed	cosystem			
Finder	-	niosam										
Smart Folders	+	niosginz			1.1							
🔶 Bookmarks	+	DHCP	DNS TFTP	HTTP (File Dis	1 FTP	NTP blox	Tools Captive	Portal Disco	very Threat Analy	ics TAXI		
🔯 Recycle Bin	+											
📑 URL Links	+	Members	Services									
		Quick Filte	None	✓ Off	Filter On	Show Filt	er Off Replic	ation Status Vie	w			
		Grou	p Results	Group By	ose one	~	l 📀					
		Go to		Go							¢ 🖬 🗉	· · ·
			Name	HA		Status	IPv4 Addre	ss IPv6 A	ddress Identify	D	HCP	DNS
		A 1	🚸 niosg	m2.lab10.c No		Running	192.168.1.	88	Unsupp	orted		
			🚸 niosr	nd2.lab10.cr No		Running	192.168.1.	89	Unsupp	rted		

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

Infoblox 📚	Dashboards Da	ata Management Smart Folders Grid Administration	
CONTROL YOUR NETWORK	niosgm2 (Grid Propertie	es Editor)	×
	A Toggle Basic Mode	Basic Advanced	×
Finder 🔍			
Smart Folders +	General	Enable GIII Redirect	
🚖 Bookmarks 🛛 🛨	Security	from Member	
🗑 Recycle Bin +	Password	Enable GUI/API	
ஞ URL Links 🛛 +	A Proxy Settings	Access via both	
	DNS Resolver		
	Monitoring	Feature	
	Syslog Backup	Enable Updates Of	
	SNMP	RIR Registrations	
	A SNMP Threshold	Enable Informational	
	A Notification	GUI Banner	
	Email	Banner Color Green	
	LOM	แต่รองผู้ใน	
	Customer		
	Improvement	Present the option of All Users Superuser Nobody	
	NAT Groups	recursive deletion of	
	A Microsoft	networks or zones to	
	Extensible	Enable DNS Object Permissions in	
	Attribute	Networks and Ranges	
	Inheritance	DSCP Value n	-
	Cancel		Save & Close +

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

	Dashboards Data M	anagement Smart Folders	Grid Administration				
	IPAM Devices Net	twork Users DHCP DNS	File Distribution Threat Analy	/tics			
Finder (Image: Smart Folders + Image: Smart Folders +	Active Users User H default Network Quick Filter None Go to	listory View ♀ ♥ Off Filter On Go	Show Filter First Seen	IP Address	Data Source	Data Source IP	Jast Seen
	 ★ ♦ ♦ ♦ 18.5 	0:56:86:12:92 N/A 7:28:2E:29:CB N/A	2016-07-24 19:05:26 EST 2016-07-24 19:03:34 EST	192.168.1.119	Cisco ISE Cisco ISE	192.168.1.120	2016-07-24 19:05: 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



Step 3 Select ->Next

Step 4 You should see the following



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

It may take up to	o a minute to apply the r	new rules.			
Event*	IPAM	.			
Action	Notify the targ	et			
	* •	Attached Device Name Attached Device Port Attached Device Model Attached Device Type Attached Device Vendor Client ID Eincer Devic	* III	Override	
	+	First Discovered Host Name Infoblox Member			

Step 6 Select Next

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

DHCP (Notification)	Basic				
General Rules	Apply rule	to relevant member	s		
Member Assignment	Select Mer	nber(s)			+ 0
	Name	IPv4 Address	IPv6 Address	Comment	
	No data				

Step 8 Select Save and Close

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

•	ili.ili. cisco	Identit	y Services Eng	gine	Home	Operations	Policy	• Guest Ac	cess - Adr	ninistration	Work Centers		0 Lic	ense Warning	9
	• S)	ystem	Identity Manag	ement	Network F	Resources	Device Portal M	anagement	pxGrid Service	Feed Se	rvice 🔹 🕨 Identity Ma	apping			
Ca	pabilt	ties	Live Log									€E	nable Auto	-Registration	1
?En	able	Ø Disable	e 🕑 Approve	Pedine	Oelete	Refresh	Total Pending App	roval(1)				1	- 9 of 9	Show 25 👻	1
T	Ca	apability N	ame	C	apability De	escription		Vendor Pla	tform	Capability Vers	Status	Publisher Count	Subscribe	r Co Supp	po
)	G	ridControl	lerAdminService							1.0	Enabled	0	1	N/A	
)	A A	daptiveNe	tworkControl							1.0	Enabled	1	0	N/A	
) (C C	ore								1.0	Enabled	0	4	N/A	
) (Er	ndpointPr	ofileMetaData							1.0	Enabled	1	0	N/A	
) (Er	ndpointPr	otectionService							1.0	Enabled	1	0	N/A	
2 1	▶ Id	lentitvGro	un							1.0	Enabled	1	0	N/A	
P	In	nfoblox_IP	AM	D)ynamic cap	ability for IPAN	1/DHCP publish	Infoblox		1.0	Pending create	0	0	N/A	
	Se	essionDire	ctory							1.0	Enabled	1	1	Subr	16
)	• Tr	rustSecM	etaData							1.0	Enabled	1	0	N/A	

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

cisco	; 1	dentity Services Engine	Home • O	perations	Policy O	uest Access	◄ Adminis	tration • Wor	k Centers	0	Licens	e Warning
► S	Syste	em 🔹 Identity Management	Network Resource	irces De	vice Portal Manag	ement pxGrid	Services	Feed Service	Identity Mappin	g		
	apa	bilities Live Log								Θ	Enable Au	to-Registral
√ E	nabl	e ⊘ Disable 💽 Approve	Dedine 🚷 Delete	Refresh	Total Pending App	roval(1)			1	selected item 1	- 9 of 9	Show 25
		Capability Name	Capability De	scription		Vendor Platfo	rm	Capability Vers	Status	Publisher Count	Subscrib	ber Co S
0	۲	GridControllerAdminService						1.0	Enabled	0	1	1
0	۲	AdaptiveNetworkControl						1.0	Enabled	1	0	P
0	۲	Core						1.0	Enabled	0	4	1
0	۲	EndpointProfileMetaData						1.0	Enabled	1	0	P
0	۲	EndpointProtectionService						1.0	Enabled	1	0	1
0	۲	IdentityGroup						1.0	Enabled	1	0	1
	►	Infoblox_IPAM	Dynamic cap	ability for IPAI	M/DHCP publish	Infoblox		1.0	Pending create	0	0	1
0	ł	SessionDirectory						1.0	Enabled	1	1	5
0	۲	TrustSecMetaData						1.0	Enabled	1	0	1

Step 11 Note the IPAM Topic is now enabled

-ihid cisco	•• I	dentity Services Engine	Home • Ope	ations	Policy	Guest Acc	ess - Adminis	stration • Work	Centers	0	License	Warning
• 5	Syste	em 🕨 Identity Management	Network Resource	es ⊧Dev	ice Portal Manaç	gement	pxGrid Services	Feed Service	Identity Mapping)		
	Capa	bilties Live Log								ØE	nable Auto	-Registral
√ E	Enabl	le 🧭 Disable 😪 Approve 🛽	P Decline 🛞 Delete 🔸	Refresh	Total Pending Ap	proval(0)				1.	9 of 9	Show 25
		Capability Name	Capability Desc	iption		Vendo	r Platform	Capability Vers	Status	Publisher Count	Subscribe	r Co 5
0	۲	GridControllerAdminService						1.0	Enabled	0	1	1
\bigcirc	۲	AdaptiveNetworkControl						1.0	Enabled	1	0	P
0	۲	Core						1.0	Enabled	0	4	1
\bigcirc	۲	EndpointProfileMetaData						1.0	Enabled	1	0	1
0	۲	EndpointProtectionService						1.0	Enabled	1	0	1
0	►	IdentityGroup						1.0	Enabled	1	0	1
0	•	Infoblox_IPAM	Dynamic capab	lity for IPAN	1/DHCP publish	Infoblo	x	1.0	Enabled	0	0	
0	•	SessionDirectory						1.0	Enabled	1	1	S.
0	۲	TrustSecMetaData						1.0	Enabled	1	0	P

Step 12 Select View By Clients

You should see the following

altalta cisco	Identity Services Engine	Home • Op	erations Policy	Guest Acces	s - Adminis	stration	Work Centers	0	License Warning
▶ Sy	stem Identity Management	Network Resource	rces	Management p	xGrid Services	Feed Servi	ce Identity apping		
Clie	ents Live Log							€En	able Auto-Registral
✓Ena	able 🧭 Disable 😪 Approve 😝 G	roup 🎈 Decline	🐼 Delete 👻 🛞 Refres	n Total Pending Ap	proval(0) 👻			1-5	5 of 5 Show 25
	Client Name	Client Descrip	tion	Capabilities		Status		Client Group(s)	L
	ise-admin-ise201self			Capabilities(4 Pub,	2 Sub)	Online		Administrator	V
	ise-mnt-ise201self			Capabilities(2 Pub,	1 Sub)	Online		Administrator	V
	infoblox_client_subscribe_32322	infoblox cisco	ise client	Capabilities(0 Pub,	2 Sub)	Online		EPS	V
	infoblox_client_publish_3232235	infoblox cisco	ise client	Capabilities(0 Pub,	1 Sub)	Online		EPS	
	infoblox_check_connectivity	Test		Capabilities(0 Pub,	0 Sub)	Offine		Session	V

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

cise	dentity Services Engine	Home • Operations	s ► Policy ► Guest Acces	s ▼Administra	ation • Worl	Centers	License Wa	iming
•	System Identity Management	Network Resources	Device Portal Management	xGrid Services	Feed Service	Identity Mapping		
Clier	its Live Log						⊖Enable Auto-Regis	tratior
✓Enal	ole 🧭 Disable 🔮 Approve 😝 Group	🖣 Decine 🛛 🔞 Delete 👻	Refresh Total Pending Appro	wal(0) +			1-5 of 5 Show	25 👻
	Client Name	Client Description	Capabilities	Sta	tus	Client Group(s)	Log
□►	ise-admin-ise201self		Capabilities(4 Pub, 2	Sub) Onl	line	Administrator		Viev
□ ▶	ise-mnt-ise201self		Capabilities(2 Pub, 1	Sub) Onl	line	Administrator		Viev
□ ▶	infoblox_client_subscribe_32322	infoblox cisco ise client	Capabilities(0 Pub, 2	Sub) Onl	line	EPS		Viev
►	infoblox check connectivity	Test	Capabilities(0 Pub, 0	Sub) Off	ìne	Session		Viev
□ ▶	infoblox_client_publish_3232235	infoblox cisco ise client	Capabilities(0 Pub, 0	Sub) Off	îne	EPS, Infoblox_	IPAM_Publish,Info	Vie

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



- Step 3 Select ->Next
- **Step 4** You should see the following

It may take up t	o a minute to apply the new rule	es.		
Event*	DNS RPZ	•		
Action	Quarantine the end he	ost		
Match the folk	owing rule:		Reset	

Step 5Change the Event from DNS RPZ to DHCP Leases
You should see the following:

CISCO

Event*	DHCP Lease	s 🗸			
Action	Notify the tar	get			
Publication Setti Available	ings	Selected			
	v P	Attached Device Name Attached Device Port Attached Device Model Attached Device Type Attached Device Vendor Clent D Finger Print First Discovered Host Name Infoliox Member	< 🗅	verride	
Inherited from EndPo	pintCiscolSE 192.168.1.	101			

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

Event*	DHCP Leases	•			
Action	Notify the targe	t			
Publication Setti Available	ings	Selected			
	-	Attached Device Name Attached Device Nott Attached Device Model Attached Device Vendor Client D Finger Print First Discovered Host Name Infobiox Member	* III	Override	
Inherited from EndPo	ointCiscoISE 192.168.1.10	1			

- Step 7 Select Next
- **Step 8** Leave the defaults for applying the rule to relevant members

				Basic
+0			relevant members r(s)	Apply rule Select Mer
	Comment	IPv6 Address	IPv4 Address	Name
	Comment	IPv6 Address	IPv4 Address	Name

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.

	cisco	dentity Services Engine	Home • Operation	ns Policy	• Guest Acc	ess -Adn	ninistration	Work Centers	(0 License V	Varning
	۶ (System 🔸 Identity Management	Network Resources	Device Portal M	lanagement	pxGrid Service	Feed Ser	vice 🔹 🕨 Identity Ma	apping		
Ca	apabi	ities Live Log							€E	nable Auto-Regist	tration (
Er	able	🙆 Disable 😪 Approve 👎 Declir	ne 🔞 Delete 😵 Refresh	Total Pending App	oroval(1)				1-1	of 10 Show	25 ¥ g
	C	Capability Name	Capability Description		Vendor Plat	form	Capability Vers	Status	Publisher Count	Subscriber Co	Suppo
)	▶ G	GridControllerAdminService					1.0	Enabled	0	1	N/A
)	► A	AdaptiveNetworkControl					1.0	Enabled	1	0	N/A
)	C	Core					1.0	Enabled	0	4	N/A
)	▶ E	EndpointProfileMetaData					1.0	Enabled	1	0	N/A
)	▶ E	EndpointProtectionService					1.0	Enabled	1	0	N/A
)	▶ 10	dentityGroup					1.0	Enabled	1	0	N/A
	▶ Ir	infoblox_DHCP	Dynamic capability for IPA	M/DHCP publish	Infoblox		1.0	Pending create	0	0	N/A
) -		nfoblox_IPAM	Dynamic capability for IPA	M/DHCP publish	Infoblox		1.0	Enabled	0	0	N/A
)	▶ s	SessionDirectory					1.0	Enabled	1	1	Subne
)	► T	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

cisco	Identity Services Engine	Home • Operations	Policy FGL	uest Access - Admin	istration • Worl	k Centers	۰ 🖈	License Warni	ng
► Sy	stem 🕨 Identity Management 🕨	Network Resources + De	vice Portal Manage	ment pxGrid Services	Feed Service	Identity Mapping	g		
Ca	pabilities Live Log						Ø	nable Auto-Regis	straf
✓En	able 🖉 Disable 🐼 Approve 👎 De	dine 🛞 Delete 🔗 Refresh	Total Pending Appro	oval(1)		1 sel	ected item 1 - 1	0 of 10 Show	25
	Capability Name	Capability Description		Vendor Platform	Capability Vers	Status	Publisher Count	Subscriber Co	5
0	GridControllerAdminService				1.0	Enabled	0	1	1
01	AdaptiveNetworkControl				1.0	Enabled	1	0	1
01	Core				1.0	Enabled	0	4	1
0 1	 EndpointProfileMetaData 				1.0	Enabled	1	0	1
01	 EndpointProtectionService 				1.0	Enabled	1	0	1
01	IdentityGroup				1.0	Enabled	1	0	1
	Infoblox_DHCP	Dynamic capability for IPA	M/DHCP publish	Infoblox	1.0	Pending create	0	0	1
	Infoblox_IPAM	Dynamic capability for IPA	M/DHCP publish	Infoblox	1.0	Enabled	0	0	r.
01	SessionDirectory				1.0	Enabled	1	1	ŝ
0 1	 TrustSecMetaData 				1.0	Enabled	1	0	1

Step 12 Note the DHCP Topic is now enabled

cisco	; I	dentity Services Engine	Home •	Operations	Policy	Guest Access	→ Adminis	stration 🔹 Wo	rk Centers	0	License	e Warnin	g
• 5	Syste	em 🕨 Identity Management	 Network Res 	ources + De	vice Portal Manag	gement pxGr	d Services	Feed Service	Identity Mapping	,			
	Capa	blities Live Log								ØE	nable Auto	o-Regist	al
√ E	inabl	e 🧭 Disable 😪 Approve 🛽	Dedine 🛞 Delet	e 😵 Refresh	Total Pending Ap	proval(0)				1-1	0 of 10	Show	25
		Capability Name	Capability	Description		Vendor Platf	orm	Capability Vers.	Status	Publisher Count	Subscribe	er Co	ç
0	۲	GridControllerAdminService						1.0	Enabled	0	1		ľ
0	۲	AdaptiveNetworkControl						1.0	Enabled	1	0		1
0	۲	Core						1.0	Enabled	0	4		ľ
0	۲	EndpointProfileMetaData						1.0	Enabled	1	0		1
0	۲	EndpointProtectionService						1.0	Enabled	1	0		ľ
0	►	IdentityGroup						1.0	Enabled	1	0		1
0	۲	Infoblox_DHCP	Dynamic c	apability for IPA	M/DHCP publish	Infoblox		1.0	Enabled	0	0		r
0	•	Infoblox_IPAM	Dynamic c	apability for IPA	M/DHCP publish	Infoblox		1.0	Enabled	0	0		1
0	۲	SessionDirectory						1.0	Enabled	1	1		ç
0	۲	TrustSecMetaData						1.0	Enabled	1	0		P

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->



Step 15 Select Save

Step 16 You should see the following:

dentity Servic	es Engine Home	Operations → Po	licy 🔹 🕨 Guest Ac	cess - Admini	stration • Work	Centers	0	License Warn	ing
System Identity	Management • Netwo	rk Resources	ortal Management	pxGrid Services	Feed Service	Identity Mapping			
Clients Live L	og						€Ena	ble Auto-Regi	straf
√Enable ØDisable	😋 Approve 🛛 📵 Group 👎	Decline 😥 Delete 👻 🛞 Ri	efresh Total Pending	g Approval(0) 👻			1-5	of 5 Show	25
Client Name	Clier	nt Description	Capabilities		Status	C	lient Group(s)		L
ise-admin-ise2	1self		Capabilities(4 P	ub, 2 Sub)	Online	A	dministrator		v
□ ► ise-mnt-ise201	self		Capabilities(2 P	ub, 1 Sub)	Online	A	dministrator		v
infoblox_client	_subscribe_32322 info	blox cisco ise client	Capabilities(0 P	ub, 2 Sub)	Online	E	PS		v
□ ▶ infoblox_check	connectivity Tes	t	Capabilities(0 P	ub, 0 Sub)	Offline	S	ession		V
□ ► infoblox_client	_publish_3232235 info	blox cisco ise client	Capabilities(0 P	ub, 0 Sub)	Offine	E	PS,Infoblox_IPAM_	Publish,Info	V

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

Infoblox 💸		Dashboards	Data Manag	jement Smart	Folders Grid	Administration				
		IPAM De	vices Netwo	rk Users DHCf	P DNS File Distrib	ution Threat Analy!	ic s			
Finder	~	Zones M	embers Nam	e Server Groups	Shared Record Groups	Response Policy Zor	ves Blacklist Rules	ets DNS64 Group	a Query Monitorin	a
Smart Folders										
A Bookmarks	+	Members Ho	ome							
Recycle Bin	+	niosgm2	2.lab10.con	1 Member DNS	1 🕺					
URL Links	+	Quick Filter	None	▼ Off Fi	Iter On Show Fil	ter				
	- 1	Go to		Go				+	+. 0	
	- 1		Name +	Grid Primary S	Ser Type	Comment	Multi-master Zone	Monitored Since	Last Queried F	Records Monitored
	- 1		blockyahoo	niosgm2.lab10	.c Response Polic		No	Not Monitored	Not Monitored	No
	- 1	🔄 🕸	dhcp.lab10.cc	niosgm2.lab10	0.c Authoritative	dynamic addres	No	Not Monitored	Not Monitored	No
	- 1		lab10.com	niosgm2.lab10	0.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



Creating DNS Zone and DNS Zone for Dynamic Addresses

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



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

ld Authoritati ve Zon	e Wizard > Step 2 of 6	د ۲
Name*	lab10.com	
Comment		
Disable		-
Lock		
Cancel	Previous Next	Schedule for Later Save & Close •

- Step 3 Select Next
- **Step 4** Select **Use this set of name servers**, the Grid Master

SECURE ACCESS HOW-TO GUIDES

Add Authoritative Zone Wizard > St	ep 3 of 6		_			×
 None Use this Name Server Grou Use this set of name server 	p Choose One V					•
Name 🔺 IPv4 Add	dress IPv6 Address	Туре	Stealth	TSIG		
niosgm2.lab10 192.168.	.1.88	Grid Primary	No	No		
REPER						
Cancel	Previous Nex	đ		Schedule for Later	Save & Close +	

Step 5 Leave the defaults

Extensible Attributes		+ 0
Att	ibute Name Value	Required
No data		

Step 6 Select Next

Step 7 Leave the defaults

uthoritative Zone W	fizard > Step 5 of 6	
low 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 configuratio	n
Save & New	Add this zone and rerun the wizard to create another	
Save & Close	Add this zone and close the wizard	
ancel	Previous	Schedule for Later Save & Close +

Step 8 Select Next

Step 9 Leave the defaults

Id Authoritative Zone	Wizard > Step 6 of 6			×
Schedule Change Now Later Selected tir	ne:			۲
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 (U Canada)	JS and
Cancel	Previo	ous Next	(_Sav	ve & Close 🔹

- 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

		Dashboards	Data Manageme	ent Smart Fo	olders Grid	Administration				
		IPAM Dev	- ices Network U:	sers DHCP	DNS File Distri	bution Threat An	alytics			
Finder	~	Zones M	embers Name Ser	rver Groups Sh	ared Record Groups	Response Policy	Zones Blacklist Ruk	sets DNS64 Gr	oups Query Moni	torina
Smart Folders	+									
1 Bookmarks	+	Members Ho	me							
Recycle Bin	+	niosgm2	.lab10.com	Member DNS 🥖	× 👷					
URL Links	+	Quick Filter	None	▼ Off Filter	r On Show F	ilter				
		Go to		Go					• • • • •	0-13-14
		C 🕸	Name 🔺	Grid Primary Ser			Multi-master Zone	Monitored Since		Records Monitored
			blockyahoo	niosgm2.lab10.c.	Response Polic		No	Not Monitored	Not Monitored	No
		同 改	dhcp.lab10.com	niosom2.lab10.c	Authoritative	dynamic addres	No	Not Monitored	Not Monitored	No
		□ ¢	lab10.com	niosgm2.lab10.c.	Authoritative		No	Not Monitored	Not Monitored	No

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

Records Subzones	_	_	_	_	_	_	
Quick Filter None	Off Filter O	Show Filter	E Toggle flat	view			
Go to	Go					↓ • B/ ()	- . .
Name 🔺	Туре	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 Select Zone Clear
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 At	tributes	+ 0
	Attribute Na Value	Required
No data		

Step 19 Select Next



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

Dash	boards	Data Manager	ment Smart Fo	olders Grid	Administration					
IPAM	Devic	- ces Network L	Jsers DHCP	ONS File Distribution	Threat Analyt	ics				
Zo	nes Me	mbers Name S	Server Groups Sh	ared Record Groups	Response Policy Z	ones Blacklist Ri	ulesets DNS64 G	roups Query Mon	itoring	
lat		me > <u>mosqm</u> 2	re Zone 📾 🥒 🕻	-						
	occorde	Subzasas	e 2011e 🛄 🧨 🦷	•						
	lecorus	Subzones				_	_	_	_	
Qu	iick Filter	None	■ Off Filter	On Show Filter	Toggle fl	at view				
Go	to		Go						↓ • ⊕ (- . - 5
	\$	Name 🔺	Туре	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	NA	System			Auto-created by
	章		NS Record	niosgm2.lab10.com		N/A	System			Auto-created by
	<u>ت</u>	dhcp	NS Record	niosom2.lab10.com		N/A	Svstem			Auto-created by
	Q.	ise201self	A Record	192.168.1.120		0	Static		No	
	\$P ~~	niosgm2	A Record	192.168.1.88		0	System		No	Auto-created by.
	\$2		A Record	182.108.1.89			oystem		NU	Auto-created by.

- **Step 24** Next, create a subzone for dynamic addresses
- Step 25 Select subzone -> "+" -> Authoritative Zone->Add an authoritative forward-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
Туре	Authoritative
Comment	dynamic address will land here
	Disable
	Cock

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 A Pv4 Address Pv6 Address	Туре		TSIG	
niosgm2.lab10 192.168.1.88	Grid Primary	No	No	
R () H 2				

- **Step 30** Leave the Extensible attributes blank
- Step 31 Select Next

SECURE ACCESS HOW-TO GUIDES

Step 32 You should see

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

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 Canad

Step 35 Select Save and Close

Step 36 You should see the following

Dashboards Data Management Smart Folders Grid Administration	
IPAM Devices Network Users DHCP DHS File Distribution Threat Analytics	
Zones Members Name Server Groups Shared Record Groups Response Policy Zones Blacklist Rulesets DNS64 Groups Query Monitoring	
lab10.com Authoritative Zone 👔 🥖 📯	
Records Subzones	
Quick Filter None	
Go to Go	B-0-17-14
Image: Second	Monitored Site
Anter and the second se	
R < → H12	

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)



Step 2 You should see the following:

Toggle Basic Mode	Basic Advan	ced			
General					
Forwarders	Zone Defaults				
Updates	Refresh*	3	Hours	•	
Queries	Retry*	1	Hours		
Zone Transfers	Expire*	4	Weeks	•	
Root Name	Default TTL*	8	Hours	•	
Servers Sort List	Negative-caching	15	Minutes	•	
Blackhole	TTL				
Logging	Email Address (for SOA RNAME field)				
Host Naming					
GSS-TSIG					
DNSSEC					
Blacklist					
DN S64					
RRset Order					
Restart					
Security					
DNS Scavenging					
Cancel					Save & Ck

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

niosgm2 (Grid DNS Pro	perties)	
A Toggle Basic Mode	Basic	
General Forwarders	Forwarders	• 0
Updates	Addresses	
Zone Transfers		
Servers	× ·	
A Blackhole A Logging		

Step 4 Select Save and Close

Step 5 Select Queries and enable Allow recursion

A Toggle Basic Mode	Basic	
General Forwarders	Resolver queries timeout 0 Seconds	-
Updates	Allow queries from	
Queries	Named ACL	E
Zone Transfers	Select Named ACL Clear	
A Root Name Servers	Set of ACEs	
A Sort List		2
A Blackhole	Permission lype Value	
A Logging	No data	
A Host Naming		
A GSS-TSIG		
A DNSSEC		
A Blacklist		
A DNS64	DEVEN MIL	
A RRset Order	18, 8 J. 211	
A Restart	Z Allow resursion	
A Security	- How recursive queries from	
A DNS Scavenging	None	

Step 6 Select **Save and Close**

Step 7 Select the Infoblox Grid Master

Infoblox 📚		Dashboards Data Management Smart Folders Grid Administration	
		Grid Manager Upgrade Licenses HSM Group Microsoft Servers Device Support Ecosystem	
Finder			
Smart Folders	+		
🚖 Bookmarks	+	DHCP DNS TFTP HTTP (File Dist) FTP NTP bloxTools Captive Portal Discovery Threat Analytics TAXII	
Recycle Bin	+		
URL Links	+	Members Services	
		DNS 📕 🥖	
		Quick Filter None	
		Group Results Group By Choose one	
		Go to Go	
		Internet Annuellaber Internet Australia Internet	

Step 8 You should see the following



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

Infoblox 💸		Dashboards	Data Managem	nent Smart Fo	lders Grid	Administration					
		IPAM Devic	es Network U	sers DHCP D	NS File Distributio	on Threat Analy	tics				
Finder		Zones Me	mbers Name S	erver Groups Sha	red Record Groups	Response Policy 2	Zones Blacklist R	ulesets DNS64 G	roups Query I	Monitoring	
Smart Folders	+					nespense reney i			active active		
2 Bookmarks	+	Members Ho	me	_							
Recycle Bin	+	niosgm2	lab10.com	Member DNS	9						
URL Links	+	Quick Filter	None	Off Filter 0	On Show Filt	er					
		Go to		Go						+++e/0	
		· *	Name 🔺	Grid Primary Ser	Туре	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

A Toggle Basic Mode	Basic
General A DNS Views	+ 0
Forwarders	Addresses
Updates	192.168.1.30
Queries	
Zone Transfers	Override
A Root Name Servers	
A Sort List	
A Blackhole	
A Logging	Use Forwarders Only
A Host Naming	Inherited from Grid niosgm2

- Step 11 Select Save and Close
- Step 12 Select dhcp.lab10.com DNS zone

		Dashboards	Data Managem	ent Smart Fo	lders Grid	Administration					
		IPAM Dev	ices Network Us	ers DHCP D	NS File Distributio	on Threat Analy	ics				
Finder		Zones	embers Name Se	rver Groups Sha	red Record Groups	Response Policy 2	ones Blacklist P	ilesets DNS84 Gr	ours Ouery Mo	ntorina	
Smart Folders	+	201100				response roley :			oopo adorymo	moning	
👉 Bookmarks	+	Members H	ome								
Recycle Bin	+	niosgm	2.lab10.com	Member DNS 🥖	9						
URL Links	+	Quick Filter	None	Off Filter 0	Show Filt	er					
		Go to		Go						+-100	- -
	- 1		Name 🔺								Site
	- 1		blockyahoo	niosgm2.lab10.c	Response Polic		No	Not Monitored	Not Monitored	No	
	- 1		dhcp.lab10.com	niosgm2.lab10.c	Authoritative	dynamic addres	No	Not Monitored	Not Monitored	No	
			lab10.com	hiosgm2.lab10.c	Authoritative		No	Not Monitored	Not Monitored	No	

Step 13 Select the **penci**l (edit properties)

Dashboards Data Manage	ement Smart Fo	lders Grid	Administration					
IPAM Devices Network	Users DHCP D	NS File Distribution	Threat Analyt	ics				
Zones Members Name	Server Groups Sha	red Record Groups F	Response Policy Z	Cones Blacklist R	ulesets DNS64 G	roups Query Moni	toring	
Members Home > niosam dhcp.lab10.com A Records Subzones	2.lab10.com Authoritative Zone	<u>/</u> *						
Quick Filter None	Off Filter (On Show Filter	E Toggle fl	lat view				
Go to	Go						↓ • ⊕ (- , - ⊜
name 🔺	Туре	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:

A Toggle Basic Mode	Basic	Advanced	
General	Harris	dhan lab 10 ann	
Name Servers	name	ancp.iab10.com	
Settings	Туре	Authoritative	
Queries	Comment	dynamic address will land here	
Zone Transfers			
Updates		Disable	
Active Directory		E Lock	
A Host Naming			
A Shared Record			
Groups			
A DNSSEC			
A DNS Scavenging			
Extensible Attributes			
Permissions			

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

A Toggle Basic Mode	Basic	
General Name Servers Settings	 None Use this Name Server Group Choose One Use this set of name servers 	
Zone Transfers		+. 0
Updates	Name A. Pv4 Address Pv6 Address Type Steath TSIG	_
Active Directory	niosgm2.lab10 192.168.1.88 Grid Primary No No	
A Host Naming		
A Shared Record Groups		
A DNSSEC		

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

A Toggle Basic Mode	Basic				
General Name Servers	Extensible A	Attributes	Value		+ 0
Settings		ISE_Account_Session_ID	seed1		
Queries		ISE_Audit_Session_ID	seed2		
Zone Transfers		ISE_IP	seed3		
Updates		ISE_MAC	seed4		
Active Directory		ISE_NAS_IP_Address	seed5		
A Host Naming		ISE_NAS_POIT_ID	seed0		
A Shared Record Groups					
A DNSSEC					
A DNS Scavenging				 	
Extensible Attributes					
Permissions					

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



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

) Add Response Policy Zo	one Feed		

- Step 4 Select Next
- **Step 5** Add the name **blockyahoo**

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

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

Use this Name Server	r Group	Choose One 👻				
) Use this set of name	servers					
					+	• 8
Name A Pv4	4 Address	IPv6 Address	Туре	TSIG		
niosgm2.lab10 192	2.168.1.88		Grid Primary	No		
~						
< -> >1 2						
< > > > > > = 2						
< • > > > 2						

- Step 7 Select Next
- **Step 8** Leave extensible attributes blank
- Step 9 Select Next
- Step 10 Select Schedule Change now



- Step 11 Select Save and Close
- **Step 12** You should see the blockyahoo Response Policy Zone

Dashboards Data Mar	nagement Smart Folders	Grid Administratio	n		
IPAM Devices Netv	vork Users DHCP DNS	File Distribution Threat Ana	lytics		
Zones Members N	lame Server Groups Shared Re	cord Groups Response Polic	v Zones Blacklist Rulesets	DNS64 Groups	Query Monitoring
Members Home					
niosgm2.lab10.co	OM Member DNS 🥖 👷				
Quick Filter None		Show Filter			
Go to	Go				++++
Name 🔺	Grid Primary Ser Type	Comment	Multi-master Zone Moni	tored Since Last Q	ueried Records I
blockyaho	o niosgm2.lab10.c Resp	onse Polic	No Not I	Nonitored Not Mo	nitored No
dhcp.lab10	.com niosgm2.lab10.c Autho	oritative dynamic addres.	No Not I	Monitored Not Mo	nitored No
🗐 🌣 🛛 lab10.com	niosgm2.lab10.c Author	oritative	No Not I	Not Mo	nitored No

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

lame*	www.yahoo.com	.blockyahoo Select Zone Clear
NS View	default	
olicy	Block (No Such Domain)	
Comment		
isable		

- 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 <u>www.yahoo.com</u> blocked domain rule

Dashboards Data Management	Smart Folders Grid	Administration			
IPAM Devices Network Users	DHCP DNS File Distributio	n Threat Analytics			
Zones Members Name Server Grou	ups Shared Record Groups	Response Policy Zones	Blacklist Rulesets	DNS64 Groups	Query Monitoring
Members Home > niosqm2.lab10.com	n				
blockyahoo 🗈 🥖 📯					
Quick Filter None 🗸 🛛	Filter On Show Filter				
Go to G	Go to Threat	Analytics Whitelist view			+· B 0· 3 · B
Name or Address Policy	Data		Comment	Site	
www.yahoo.com Block Do	omain N				

Step 18 Select Grid DNS Properties

Infoblox 📚		Dashboard	s Dat	a Management	Smart Folders	Grid	Administration						1	Search	ad
		IPAM D	evices	Network Users	DHCP DNS	File Distributio	on Threat Analytics								
Finder		Zones	Members	Name Server G	Groups Shared Re	cord Groups	Response Policy Zones	Blacklist Rulesets	DNS64 Groups	Query Monitori	ing		Te	oolbar	
Bookmarks	•	Members	Home >	niosqm2.lab10.c	com								⇒ v	/iew +	
URL Links	*	Quick Filte	er None		Off Filter On	Show Filter	ī						€°н с	lostname Compliance	
		Go to			Go	Go to Threa	t Analytics Whitelist view				+		ŝ, s	icavenge R	ecord
		C 🕸	Name	or Address Policy	y Data			Comment	Site				0 P		
			www	yahoo.com Block	k Domain N								U U	lanage Dyn Ipdate Grou	amic ups
													<u>۱</u>	NSSEC	
														nport Zone Configure A Virectory	
												14	11	love DNS V	liew.
													ii G P	Brid DNS Properties	
													2 R	lestart Serv	ices
													1	SV Import	
		14.4	E ELLA	2										SV JOD Ma	nager
													# 0	ON Converte	êr 👘

Step 19 Select Logging->Enable rpz



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	•			
lode ID	LAN	•			
iource	Any	•			
Severity	Debug	•			
Port*	2000				
Logging Category	 Send all Send selected categor 	ies			
	Available			Selected	
	Active Directory Authent Common Authentication LDAP Authentication Non-system Authentication RADIUS Authentication		Þ	Threat Protection DNS RPZ	*
	TACACS Authentication UI API Authentication		4		
	Cloud API DHCP Process				
	DNS Client	*			w.

Step 3 Select Add

Step 4 You should see the following:

A Toggle Basic Mode	Basic
General	Syslog
Password	Syslog Size (MB)* 300
A Proxy Settings DNS Resolver	Once the syslog file reaches this size, the syslog server rotates the file and opens a new one.
Monitoring Syslog Backup	Servers
SNMP	Address Transport Interface Source Node D Port Severity Category
Threshold	127.0.0.1 UDP LAN Any LAN 2000 Debug Threat Protection, DNS
Email	

- **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

Name*	BlockYahoo	
Target*	192.168.1.125 👻	
Comment		

- Step 2 Select Next
- Step 3 Select DNS Event from the drop-down menu
- Step 4 Select Rule Name->Contains->www.yahoo.com

It may take up t	o a minute to apply the new rules.			
Event*	DNS RPZ	•		
Action	Quarantine the end host	t		
Match the foll	owing rule:		Reset	

Step 5 Select Next

Step 6 You should see the following:

otification Wiz	zard > Step 3 of 3			1	
Apply rule	to relevant member	5			
Select Mer	mber(s)				0
Name	IPv4 Address	IPv6 Address	Comment		
No data					

Step 7 Select Save and Close

Step 8 You should see the following:

Dashboards Data Management Smart Folders Grid Administration Finder Grid Manager Upgrade Licenses HSM Group Microsoft Servers Device Support Ecosystem Finder Grid Manager Cisco Notification Image: Cisco Notification Smart Folders + Motification Image: Cisco Notification Image: Cisco Image: Cisco Walk Filter Image: Cisco Notification Image: Cisco Image: Cisco Image: Cisco WIRL Links + Image: Cisco Image: Cisco Image: Cisco Image: Cisco IVEL Links + Image: Cisco Image: Cisco Image: Cisco Image: Cisco IVEL Links + Image: Cisco Image: Cisco Image: Cisco Image: Cisco IVEL Links + Image: Cisco Image: Cisco Image: Cisco Image: Cisco IVEL Links + Image: Cisco Image: Cisco Image: Cisco Image: Cisco IVEL Links + Image: Cisco Image: Cisco Image: Cisco Image: Cisco IVEL Links + Image: Cisco Image: Cisco Image: Cisco Image: Cisco IVEL Links + Image:	
Grid Manager Upgrade Licenses HSM Group Microsoft Servers Device Support Ecosystem Finder	
Finder Cisco Notification Smart Folders	
Smart Folders	
★ Bookmarks ★ Image: Bookmarks Image: Bookmarks Image: Bookmarks Control of Filter On Image: Bookmarks Target Image: Bookmarks No	
Recycle Bin URL Links Go to PAM </td <td></td>	
Go to Go Variable	
Image Name Target Action Comment Disabled Image IPAM 192.168.1.125 Notify the target No Image DHCP 192.168.1.125 Notify the target No	e 0 4
中 IPAM IP2.168.1.125 Notify the target No 中 DHCP IP2.168.1.125 Notify the target No	
DHCP 192.168.1.125 Notify the target No	
BlockGoogle 192.168.1.125 Quarantine the No	
🔄 🏚 bloxixyahoo 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



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



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

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



Step 4 Select Next

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

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 👻	
	Unimited Lease Line	
	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	Override
	Inherited from Grid niosgm2	
Routers	+ 0	
	IP Address	Quantita
	No data	Overnde
	Inherited from Grid niosgm2	
Domain Name	ab10.com	Override
	Inherited from Grid niosgm2	Overnde

Step 8 Select Next

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

Enable Discovery Discovery Member	niosnd2.lab10.com Select Member Clear
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 Image: The state of the polling
	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:



Step 14 Select the network:

Dashboards Data Management Smart Folders Grid Administration	
IPAM Devices Network Users DHCP DNS File Distribution Threat Analytics	
Networks Members Leases IPv4 Filters Option Spaces Fingerprints Templates	
Members Pv4 DHCP Falover Associations	
Members Home	
niosgm2.lab10.com Member DHCP 🥖 🛠	
Quick Filter None	
Go to Go	
🗌 🥸 Network 🔺 Comment IPv4 DHCP Utilz Active Users Discover Now Site	
💭 🏟 📫 <u>192.168.1.0/24</u> 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) Select Network Clear
Start*	192.168.1.10
End*	192.168.1.120
Name	
Comment	
Disable for DHCP	

Step 18Select NextStep 19Leave the defaults

Served by	None (Reserved Range)
	O Grid Member	None
	 IPv4 DHCP Failover Association 	Select Association

Step 20 Select Next

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

niosnd2.lab10.com Select Member Clear Override
Inherited from Network 192.168.1.0/24
After the range is created, a discovery of the range will be performed unless immediate Discovery
disabled. Enabling Immediate Discovery is recommended.
Basic Polling Settings Simple Settings CLI Collection Port Scanning Profile Device Complete Ping Sweep Complete Ping Sweep KetBloS Scanning Automatic ARP Refresh before Switch Port Polling Switch Port Data Collection Private Polling No schedule has been constant and

- 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:

Dashboards Data Management Smart Folders Grid Administration			
IPAM Devices Network Users DHCP DNS File Distribution Threat Analytics			
Networks Members Leases IPv4 Filters Option Spaces Fingerprints Templates			
Members Pv4 DHCP Falover Associations			
Members Home > niosqm2.lab10.com			
192.168.1.0/24 🕸 IPv4 Network 🥖 🐓 🛛 Go to IPAM View			
Quick Filter None			
Go to Go	+ + · ⊵ ⊘ ·		
🗐 🧔 🛛 PAddress 🔺 Type Name IPv4 DHCP Utiliz Active Users Discover Now	Comment Site		
② 章 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)



Step 27 You should see the following:

niosgm2 (Grid DHCP Pr	operties)
A Toggle Basic Mode	Basic Advanced
General	IPv4 Properties
Fingerprinting	Authoritative V DHCP server is authoritative
IPv4 DHCP Options	Lease Time 5 Minutes -
IPv4 DDNS	Onimited Lease Time
IPv4 DHCP Thresholds	madvertently selecting the Unimited Lease I inter check box or using this option incorrectly could cause a serious network outage in the future when all available leases are allocated
A IPv4 Filters	Microsoft Clients None 🛩
A IPv4 BOOTP/PXE	Coue Page
IPv6 DHCP Options	IPv6 Properties
IPv6 DDNS	Microsoft Clients None 👻
IPv6 Global Prefixes	
A Logging	
A IF-MAP	
A Restart	

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

A Toggle Basic Mode	Basic Advanced	
General Fingerprinting	Routers	0
IPv4 DHCP Options IPv4 DDNS	P Address No data	
IPv4 DHCP Thresholds	Domain Name lab10.com	
A IPv4 Filters	DNS Servers	2
IPv4 BOOTP/PXE IPv6 DHCP Options IPv6 DDNS	P Address 192.168.1.88 192.168.1.30	
IPv6 Global Prefixes	Broadcast Address	
A Logging	Custom DHCP Choose option	
A IF-MAP	Options	
A Restart		

Step 29 Select IPv4 DDNS and enable DDNS updates

A Toggle Basic Mode	Basic Advanced	
General Fingerprinting IPv4 DHCP Options IPv4 DDNS IPv4 DDNS IPv4 DHCP Thresholds A IPv4 Filters A IPv4 BOOTP/PXE	DDNS Updates DDNS Updates DDNS Update TTL 0 Seconds GSS-TSIG Enable GSS-TSIG Updates Manage GSS-TSIG keys Domain Controller (KDC)	
IPv6 DHCP Options IPv6 DDNS	Version Encryption type Last update	+ · · O

Step 30 Select Save and Close
Step 31 Select the link for the Infoblox Grid Master



Step 32 Select pencil (edit properties)

Dashboards Data Management Smart Folders Grid Administration	
IPAM Devices Network Users DHCP DNS File Distribution Threat Analytics	
Networks Members Leases IPv4 Filters Option Spaces Fingerprints Templates	
Members Pv4 DHCP Falover Associations	
Members Home	
niosgm2.lab10.com Member DHC 📝 🛠	
Ouick Filter None	
Go to Go	⇒ + • ⊵ ⊘ • ₹
🗌 🏚 Network 🔺 Comment Pv4 DHCP Utiliz Active Users Discover Now Ste	

Step 33 You should see the following:

niosgm2.lab10.com (M	ember DHCP Properties)		
A Toggle Basic Mode	Basic Adva	nced	
General	DHCP Interfaces		^
Fingerprinting	IPv4 IPv6		-
Multi-master DDNS	LAN1 V		
IPv4 DHCP Options	IPv4 Properties		
IPv4 DDNS	irvertoperdes		- 1
IPv4 DHCP Thresholds	Authoritative	DHCP server is authoritative Override Override	E
A IPv4 Filters	Lease Time	5 Minutes 🖵	
A IPv4 Authenticated DHCP		Indivertently selecting the Unlimited Lease Time check box or using this option incorrectly could cause a serious network outage in the future when all available bases are allocated	
IPv6 DHCP Options		Inherited from Grid niosgm2	
IPv6 DDNS	Microsoft Clients Code Page	None V Override Override	
A Logging		innentea from ona nosgraz	
A IF-MAP Permissions	IPv6 Properties		_
	Server DUID		-

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

A Toggle Basic Mode Basic Ad	vanced	
General		
Fingerprinting		+ 0
Multi-master DDNS	IP Address	Override
IPv4 DHCP Options	No data	
options	Inherited from Grid niosgm2	
IPv4 DDNS Domain Name	ab10 com	
IPv4 DHCP Thresholds	Inherited from Grid niosgm2	Override
A IPv4 Filters DNS Servers		
A IPv4 BOOTP/PXE		+ 0
A IPv4	IP Address	
Authenticated	192.168.1.88	Override
DHCP	192.168.1.30	
IPv6 DHCP Options	Inherited from Grid niosgm2	
IPv6 DDNS Broadcast Address	3	
A Logging	Inherited from Grid niosgm2	Override
A IF-MAP		
Permissions Options	Choose option 👻	

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

A Toggle Basic Mode	Basic Advar	nced	÷
General Fingerprinting	Overridden DDNS settin	ngs will not take effect unless "Enable DDNS' is also overridden and set at this level.	
Multi-master DDNS	DDNS Updates	Enable DDNS Updates Inherited from Grid nicegm2 Override	
IPv4 DHCP Options	DDNS Domain Name	Inherited from Grid niosgm2	
IPv4 DDNS IPv4 DHCP Thresholds	DDNS Update TTL	0 Seconds - Override	
A IPv4 Filters	GSS-TSIG	Inherited from Grid mager2 D Enable GSS-TSIG Updates Override	
A IPv4 Authenticated DHCP		Inherited from Grid nosgen2 Manage GSS-TSIG keys	
IPv6 DHCP Options		Domain Controller (KDC)	
IPv6 DDNS		Version Encryption type Last update	
A IF-MAP Permissions			
		Override	-

Step 36 Select Save and Close

Step 37 Select the network

Dashboards Data Management Smart Folders	Grid Adminis	stration			
IPAM Devices Network Users DHCP DNS F	ile Distribution Thre	eat Analytics			
Networks Members Leases IPv4 Filters Option	Spaces Fingerprints	Templates			
Members IPv4 DHCP Failover Associations					
Members Home					
niosgm2.lab10.com Member DHCP 🥖 🛠					
Quick Filter None Off Filter On	Show Filter				
Go to Go					++· =/0· J · 4
🗌 🕸 Network 🔺 Comment	IPv4 DHCP Utiliz	Active Users	Discover Now	Site	
	0.0% (0/111)	0			

Step 38 Select pencil (edit properties)

Dashboards Data Management Smart Folders Grid Administration	
IPAM Devices Network Users DHCP DNS File Distribution Threat Analytics	
Networks Members Leases IPv4 Filters Option Spaces Fingerprints Templates	
Members Pv4 DHCP Falover Associations	
Members Home > niosgm2.lab10.com	
192.168.1.0/24 🔅 IPv4 Networ 🧪 📴 Go to IPAM View	
Quick Filter None	
Go to Go	++· < 0 ·
🗌 🕸 🛛 P 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

				×
A Toggle Basic Mode	Basic Ad	vanced		
General Member Assignment	Lease Time	5 Minutes 🖵 Dinimited Lease Time		Î
IPv4 DHCP Options Discovery		Indivertently selecting the Unlineted 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 Grd nissgm2	Override	
Discovery Exclusions Discovery	Routers	+0		
Blackout DHCP Forwarding		No data	Override	н
A IPv4 DDNS		Inherited from Grid niosgm2		
A IPv4 BOOTP/PXE A IPv4 DHCP	Domain Name	ab10.com Inherited from Grid nicegm2	Override	[
A IPv4 Filters	DNS Servers	+0		
A IPv4 IPAM Utilization		IP Address 192.168.1.88 192.168.1.30	Override	

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

A Toggle Basic Mode	Basic		
General	Overridden DDNS settin	gs will not take effect unless 'Enable DDNS' is also overridden and set	at this level.
Assignment	DDNS Updates	Enable DDNS Updates	Override
Options	DDNS Domain Name	DDNS Domain Name	
Discovery		Inherited from Grid niosgm2	Override
Discovery Blackout	DDNS Update TTL	0 Seconds v Inherited from Grid niosgm2	Override
DHCP Forwarding	Generate Hostname	Generate Hostname if not Sent by Client Inherited from Grid nicsgm2	Override
A IPv4 DDNS A IPv4 BOOTP/PXE	Fixed Address Updates	Update Fixed Addresses Inherited from Grid nicsgm2	Override
A IPv4 DHCP Thresholds A IPv4 Filters	Option 81 Support	Enable Option 81 Support B DHCP server always updates DNS DHCP server updates DNS if requested by client	Override
A IPv4 IPAM Utilization Notification	Lease Renewal Update	Inherited from Grd niosgm2 Update DNS on DHCP Lease Renewal Inherited from Grd niosgm2	Override

Step 41 Select IP address range

PAM Devices Network L Networks Members Lea Members Pv4 DHCP Fas Members Home > niosam2 192.168.1.0/24 🛠 Pv4	Users DHCP DNS Fi ases Pv4 Fitters Option S liover Associations	ile Distribution Th	hreat Analytics s Templates				
Networks Members Lea Members Pv4 DHCP Fail Members Home > niosan2 192.168.1.0/24 \$ Pv4	ases IPv4 Filters Option S liover Associations 2.lab10.com	spaces Fingerprints	s Templates				
Members Pv4 DHCP Fail Members Home > niosqm2 192.168.1.0/24 Pv4	lover Associations 2.lab10.com		_	-	-	_	_
Members Home > niosqm2 192.168.1.0/24 📚 Pv4	2.lab10.com						
192.168.1.0/24 📚 🕬	A Matural d 💁 Catal						
	4 Network 🧨 🌪 Gotor	PAM View					
Quick Filter None	Off Filter On	Show Filter					
Go to	Go					+++	₽ 0 - 1,7 -
P Address 🔺	Туре	Name	IPv4 DHCP Utiliz	Active Users		Comment	Site
192.168.1.10-192	2.168.1.120 IPv4 DHCP Rang	ge dhcprange	0.0% (0/111)	0			

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

Dashboards Data Man	agement Smar	t Folders Grid	Administratio	'n		
IPAM Devices Netw	ork Users DHCP	DNS File Distrib	ution Threat An	alytics		
Networks Members	Leases IPv4 Filters	Option Spaces	Fingerprints Ten	plates		
Members Pv4 DHC	P Failover Associations					
Members Home > nios	gm2.lab10.com > 1	92.168.1.0/24				
192.168.1.10-192	2.168.1.120	IPv4 DHCP Range 💋	· 🗛			
Quick Filter None	▼ Off Fill	er On Show I	Filter			
Go to	Go					+ · 🔄 🖉 · 🗶 🚚
P Address +	Туре	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:

A Toggle Basic Mode	Basic Adva	ced	-
General	Start*	192.168.1.10	
Member Assignment	End*	192.168.1.120	
IPv4 DHCP	Name	dhcprange	
Discovery	Comment		-
Discovery Blackout	Disable for DHCP		
A IPv4 DDNS			
A IPv4 BOOTP/PXE			
A Exclusion Ranges			ľ
A IPv4 DHCP Thresholds			
A IPv4 Filters			

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

A Toggle Basic Mode	Basic Ad	dvanced
General Member Assignment	Lease Time	5 Minutes w Unimted Lease Time
IPv4 DHCP Options		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 neagen2
Discovery Discovery Blackout	Routers	
A IPv4 DDNS A IPv4 BOOTP/PXE		P Address 192.168.1.1
Ranges	Domain Name	
A IPv4 Filters	e e mainte	dhcp.ab10.com

Step 45 Select IPv4 DDNS and verify DDNS updates are enabled

General			
Member Assignment	Overridden DDNS settin	igs will not take effect unless 'Enable DDNS' is also overridden a	and set at this level.
IPv4 DHCP Options	Don's opulates	V Enable DDNS Updates Inherited from Grid niosgm2	Override
Discovery	DDNS Domain Name	DDNS Domain Name	Override
Blackout	Generate Hostname	Generate Hostname if not Sent by Client	Override
IPv4 BOOTP/PXE	Lease Renewal	Inherited from Grid niesgm2	Countin
Exclusion Ranges	Update	Inherited from Grid niosgm2	Overnde
IPv4 DHCP Thresholds			

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

Assignment				N	
IPv4 DHCP		ISE_Account_Session_ID	seed1	*	No Parent
Options		ISE_Audit_Session_ID	seed2		No Parent
Discovery		ISE_IP	seed3		No Parent
Discovery		ISE_MAC	seed4		No Parent
Blackout		ISE_NAS_IP_Address	seed5		No Parent
A IPv4 DDNS		ISE_NAS_Port_ID	seed6		No Parent
A IPv4 BOOTP/PXE		ISE_Quarantine	seed7		No Parent
A Exclusion Ranges					
A IPv4 DHCP Thresholds	•				
A IPv4 Filters	Modify (descendant actions for selected inhe	ritable extensible attributes.		
A IF-MAP					
A Cisco ISE					
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

Dashboards	Data Management	Smart Folders	Grid Admin	istration		
IPAM Devices	Network Users	DHCP DNS	File Distribution Th	reat Analytics		
default 1	Network View 👷					
Quick Filter Not	ne 🗸	Off Filter On	Show Filter	Toggle flat view		
Go to		Go				⇒ + • ₽ ⊘• ₹ • ₫
1 🥸 N	letwork 🔺	Comment	PAM Utilization			
□ ¢ 🔤	• <u>192.168.1.0/24</u>		4 <mark>5.2%</mark>	0		

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

Discovered Data		01
Cisco ISE Session State: Cisco ISE Security Group:	Cisco ISE End Point Profile:	_

Step 3 Ensure you have the following

Discovered D	ata					٥	
Available	NetBIOS Name OS Discovered MAC Address Last Discovered	•		Cisco ISE Session State Cisco ISE End Point Profile Cisco ISE Security Group	*	Selected	
	First Discovered Discovered Name		►			*	
	Discoverer Attached Device Description Attached Device Address Attached Device Model Attached Device Name Attached Device Port Description		4		+	•	

Step 4 Select the Configuration Tab to Close

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

Das	hboards	Data Managemer	t Smart Fold	iers Grid	Administration					
IPAM	Devices	Network Users	DHCP DNS	File Distributio	n Threat Analyti	cs				
194 19	<u>M Home</u> 2.168.1.1 ⁹ Map List	D/24 🐥 IPv4 Net	work 🥖 🛠 S	<u> So to DHCP View</u>						
E					Fir	gerprint:				
P	Discovered D	lata	_	_			_	_		8
L	Cisco ISE Set	ssion State: curity Group:				Cisco ISE End Point Pr	rofile:			
Į.	Related Obje	Audit Histo	iry	_			_	_		_
L		_						81 4 -	B 0 · 1	- I A I
	□ ☆	Name	iype	Active Users	ISE_Quarantine	ISE_NAS_Port_ID	ISE_NAS_IP_Ad	ISE_MAC	ISE_P	ISE_A
L	No data	- T	Sort Ascending Sort Descending							
			Columns	- P						

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

Dashboards Data Ma	inagement Smart Folde	ers Grid Administration			
PAM Devices Netwo	rk Users DHCP DNS	Edit Columns			×
		Column	Width	Sortable	Visible
IPAM Home		Name	107	No	V
192 168 1 0/24 🕏	IPv4 Network 🥖 🐄 G	Туре	100	No	V
IR Map		Active Users	100	No	
ir map tot		ISE_Quarantine	100	Yes	V
		ISE_NAS_Port_ID	100	Yes	V
		ISE_NAS_IP_Address	100	Yes	V
Discovered Data		ISE_MAC	100	Yes	V
		ISE_IP	100	Yes	V
Cisco ISE Session State	e.	ISE_Audit_Session_ID	100	Yes	V
Cisco ISE Security Grou	up:	ISE_Account_Session_ID	100	Yes	V
		DNS View	100	No	
		Comment	100	Yes	
Related Objects	Audit History	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

Related Object	ts Audit Histor	y						_	_
							B + - B	0. 2.	周島
ne	Туре	Active Users	ISE_Quarantine	ISE_NAS_Port_ID	ISE_NAS_P_Ad	ISE_MAC	ISE_IP	ISE_Audit_Sessi	ISE_A

then Quarantined_Systems AND PermitAccess

Adding ISE EPS Quarantine Authorization Rule

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

Step 1	Select Policy->Authorization->I	Exceptions->	Insert New Rule above	
Step 2	For Rule Name enter EPS_Qua	rantine		
		Conditions (identity gro	oups and other conditions)	
Step 3	Create new condition rule by sel	ecting if Any \diamondsuit and	Condition(s)	
Step 4	Under Description, Select Attri	bute select Session:EPS	Status:Equals:Quarantine	
		Permissions		
Step 5	Select the Authorization profile		->Security Group->Quarantined System	ns
Step 6	Select "+"			
Step 7	Select Standard->Under Profi	e select Standard->Per	rmit Access->Done	
Step 8	You should see the following			
Status	Rule Name Cond	itions (identity groups and other condit	tions) Permissions	

Step 9 Select Save

EPS_Quarantine

~

Step 10 Add a Security Group Tag of Employee to user authenticating in the Domain/Users Group

if Session: EPSStatus EQUALS Quarantine

- **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:

cisc	dentity	Services Engine	Ноп	ne 🕨 C	Context Visibility	r	Operations	▼Policy	Administration	• Work Ce	nters	5	License W
Au	thentication	Authorization F	Profiling	Posture	Client Provis	ioning	Policy Ele	ements					
Aut	thorization	Policy											
For	Policy Export	go to Administration	i > System	> Backup &	& Restore > Po	licy Expo	or other cond ort Page	nuons. Drag a	na arop rules to chanj	ge me order.			
Firs	t Matched R	ule Applies	*										
►	Exceptions	(2)											
	Standard												
	Status	Rule Name			Condi	tions (ide	antity groups	and other con	ditions)			Permissions	
1		Wireless Black Lis	t Default		if Blackli	st AND W	Vireless_Acc	ess	uluons)		then	Blackhole_Wireless_Access	
-		Profiled Cisco IP P	hones		if Cisco-l	P-Phone					then	Cisco_IP_Phones	
-		Profiled Non Cisco	IP Phone	s	if Non_C	isco_Pro	filed_Phone:	s			then	Non_Cisco_IP_Phones	
1	0	VPN			if (DEVIC	E:Device	Type EQUAL	LS All Device 1	iypes#asa AND Radiu	us:NAS-	then	VPN	
Γ	2	Employee			if pxGridU	Jsers:Ext	ternalGroups	EQUALS lab	10.com/Users/Domai	n Users	then	Employees	
1	0	Compliant_Device	s_Access		if (Netwo	rk_Acces	s_Authentica	ation_Passed	AND Compliant_Devi	ices)	then	PermitAccess	
	\bigcirc	Employee_EAP-TL	.s		if (Wirele	ss_802.1	1X AND BYO	D_is_Registe	red AND EAP-TLS AN		then	PermitAccess AND BYOD	
	ave Res	et											

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 <u>www.yahoo.com</u> and is quarantined via pxGrid.

Step 1 Verify user logs into ISE

altalta cisco	Identity Services Engine	Home • Co	ontext Visibility	Operations Policy	Administration	Work Centers	License Warning 🔺	Q 0	± •	
▼RA	DIUS TC-NAC Live Logs	TACACS Report	ts Froublesho	Adaptive Network Con	itrol					
Live	.ogs Live Sessions									
	Misconfigu	red Supplicants 🚯	Misconfigur	red Network Devices	RADIUS Drops 🚯	Client Stopped Responding	g 🛛 Repeat Counter 🕲			
		0		0	1	0	0			
						Refresh Every 1 minute	Show Latest 100 records 💌 With	Last 24 ho	urs 💌	
CR	efresh OReset Repeat Cou	ints 🛛 🚨 Export To	•					T Filt	er 🕶 🗢 🕶	
	Time	Status	Details	Identity	Endp	oint ID Authentication	Policy Authoriza	tion Policy	Auth	or
×			-	Identity	End	ooint ID Authentication P	olicy Authorizat	ion Policy	Auth	hor
	Aug 14, 2016 04:26:29.038 AM	0	0	50:3D:E5:C4:05:8A	50:30	E5:C4:05:8A Default >> MAB >	> Default Default >>	Basic_Authenti	ca Perm	nit∕
	Aug 14, 2016 04:26:27.086 AM	0	0	jeppich@lab10.com	00:00	:29:CF:07:17 Default >> Dot1X	>> Default Default >>	Employe	Empl	loy
	Aug 14, 2016 04:26:26.999 AM		Q	jeppich@lab10.com	00:00	:29:CF:07:17 Default >> Dot1X	>> Default Default >>	Employe	Empl	loy
	Aug 14, 2016 04:26:17.118 AM		0	host/jeppich-PC.lab10.com	00:00	:29:CF:07:17 Default >> Dot1X	>> Default Default >>	Basic_Authentic	ca Perm	nitA

- **Step 2** Open a command prompt on the client and type: **nslookup**
- Step 3 Type: <u>www.yahoo.com</u>
- **Step 4** You should see the following non-existent domain messages



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

sco Iden	tity Services Engine	Home • Conte	xt Visibility		inistration	License	Warning 🔺 🔍 🔍 🛔	•
RADIUS	TC-NAC Live Logs + T	ACACS Reports	Troublesho	ot Adaptive Network Control				
ive Logs	Live Sessions							
					Refresh Every	1 minute Show Latest 100 record	is 👻 Within Last 24 hours	•
CRefresh	Reset Repeat Count	s 🛃 Export To 🕶					T Filter •	۰.
Tim	e	Status	Details	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Author
ĸ		-		Identity	Endpoint ID	Authentication Policy	Authorization Policy	Author
Aug	14, 2016 05:37:08.369 AM	0		LAB10Veppich	00:0C:29:CF:07:17	Default >> Dot1X >> Default	Default >> EPS_Quarantine	Quaran
Aug	14, 2016 05:37:07.868 AM		0	LAB10\jeppich	00:0C:29:CF:07:17	Default >> Dot1X >> Default	Default >> EPS_Quarantine	Quaran
Aug	14, 2016 05:37:07.429 AM		0		00:0C:29:CF:07:17			
Aug	14, 2016 05:37:04.417 AM	0	0		00:0C:29:CF:07:17			

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

Infoblox 😵	Dashboards	Data Management	Smart Folders	Grid Administration					
	IPAM Dev	ices Network Users DH	CP DNS	File Distribution Threat Anal	ytics	ti italianaa	1.4951		
nder Smart Folders	Active User	rs User History							
Bookmarks	+ default	Network View 🧏							
Recycle Bin	+ Quick Filter	None V Off	Filter On	Show Filter					
URL Links	+ Go to	Go							
	- \$	User Name 🔺	Domain				Data Source P		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-
	•	Se 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-
	•	Anost/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
	-	൙ 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

Infoblox 💸		Dashbo	oards	Data Management	Smart Folders	Grid Administration	1					
		IPAM	Devices	Network Users	DHCP DNS	File Distribution Threat An	alytics		CON			
inder	*	Activ	ve Users	User History								
Bookmarks	+	defa	ault 🔹	ietwork View 🤶								
Recycle Bin	+	Quic	k Filter Nor	ne 🗸	Off Filter On	Show Filter						
URL Links	+	Go to			Go						31.5	
			Q. U	ser Name 🔺	Domain	First Seen	P Address	Data Source	Data Source P	Last Seen	La	at i
			¢	A 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	20	16-
		- E +	¢.	⊱ 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	20	16-
			φ.	⊱ 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	20	16-
			¢	⊱ 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	20	16-
		E 1	¢	⊱ 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	20	16-
		- 1	¢	⊱ 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	20	16-
		- +	¢	lost/jeppich-PC.lab	10 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	20	16-
				So To IPAM IP Address D	Details 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	20	16-
		V 1	¢	So To DHCP Network De	tails in 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	20	16-
			¢ (Go To IPAM Network Det	ails Init 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	20	16-
												- 1

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

	Dashboards Data Management Sm	nart Folders Grid Adminis	tration	
	IPAM Devices Network Users DHCP	DNS File Distribution Three	at Analytics	
inder Smart Folders	IPAM Home > <u>192.168.1.0/24</u> 192.168.1.119 Pv4 Address 🛠			
Recycle Bin	Type: A Record, Lease, Pv4 DHCP Ra Comment:	ange	MAC Address: 00:0c:29:c607:17 Name: jeppich-pc.dhcp.lab10.com, jeppich-PC DHCP Microsoft Windows Vista/7 or Server 2008 Fingerprint:	
	Discovered Data Cisco ISE Session State: STARTED Cisco ISE Security Group: Quarantined_Syst	tems	Cisco ISE End Point Profile: Microsoft-Workstation	80
	Related Objects Audit History		B	₽ 0- ≠ - 7 4
	Image: Second	Type Active Users A Record 6 Lease 6	SE_QUarantine SE_INAS_POR_D SE_NAS_P_Ad SE_MAC QUARANTINE GigabitEthernet1 192.168.1.3 00.0C.29	ISE_IP IS CF:07:17 192.168.1.119 04

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

Infoblox 📚	Dashb	oards	Data Management	jeppich-pc.dhcp.lab10.	.com (A Record)	-	_	_	_	alala	×	
Finder Smart Folders Bokomarks Crecycle Bin URL Links	PAM PAM PAM PAM PAM PAM PAM PAM	ands Devices Iome > 168.1 ent: co ISE Se co ISE Se co ISE Se ated Obj	Data Management Network Users DHC 192166.1.0/24 .119 Pv4 Address & A Record, Lease, Pv4 DHCC Data ssion State: STARTED curdy Group: Quarantined_S Pects Audit History Name	General TTL Discovered Data DHS Scavenging Updates Extensible Attributes Permissions	Com (A Record)	Attributes Attributes ISE_Account ISE_Judt_Si ISE_IP ISE_IAS_PO ISE_UAS_PO ISE_Ouarant	to _Session_D ession_D Address rt_D ine 	Value 0000003A 0A00001000002A0382 192.168.1.119 00.0C.29.CF.07.17 192.168.1.3 GigabEthement1/0/11 QUARANTHE SE_INAS_P_Ad	40AF E E Ve & Clos		X C S E_P	
		¢ ¢	jeppich-pc.dhcp.lab10.com jeppich-PC	A Record Lease	6	QUARANTINE	GigabitEthernet1	192.168.1.3 00:00	:29:CF:07	:17 1	92.168	1.119 04

 Step 10
 Unquarantine must be done manually from ISE, type in the URL:

 https://{ISE ipaddress}/admin/API/eps/UnQuarantineByIP/{ipaddress of endpoint}





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

altalia cisco	Identit	ty Services Engine	Home	Conte	ext Visibility	▼Operations	Policy	Administration	• Work Cente	ers		License Warr	ing 🔺	۹ 🛛	
₹R	ADIUS	TC-NAC Live Logs	TACACS	Reports	Troublesh	oot + Adaptive	Network Contro	bl							
Live	Logs	Live Sessions													
									Refresh	Every 1 minute	• Show	Latest 100 records	• Within	Last 24	hou
CF	Refresh	Reset Repeat Cou	ints 🛛 🚨 Ex	port To 👻										▼ F	ilte
	Time		Status		Details	Identity		En	dpoint ID	Authent	ication Policy	Au	thorizatior	n Policy	
×				-		Identity		E	ndpoint ID	Authent	ication Policy	A	nthorization	Policy	
	Aug 14	4, 2016 05:48:22.545 AM		0	9	LAB10\jeppic	1	00	:0C:29:CF:07:17	Default >	> Dot1X >> De	fault De	fault >> Em	ploye	1
	Aug 14	4, 2016 05:48:22.266 AM		~	Q	LAB10\jeppic	1	00	:0C:29:CF:07:17	Default >	> Dot1X >> De	fault De	fault >> Em	ploye	

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

Infoblox 💸		Dashboards	Data Management	Smart Folders	Grid Administration					
		IPAM Dev	ices Network Users	DHCP DNS	File Distribution Threat Ana	lytics				
Finder		Active Use	rs User History							
Smart Folders	+	d a facult								
A Bookmarks	+	default	Network View Y							
Recycle Bin	+	Quick Filter	None Y	off Filter On	Show Filter					
📑 URL Links	+	Go to		Go						第 日春
		2	User Name 🔺	Domain	First Seen	IP Address	Data Source	Data Source IP	Las Last updated	
			8 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	å: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	3:42
			⊱ 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	å: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	3:21
		0 ¢	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	2:00
		C 🕸	Go To IPAM IP Address Det	tails 0.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
		V 🕸	Go To DHCP Network Deta	is hill10.com	2016-07-23 17:28:02 EST	192.168.1.119	Cisco ISE	192.168.1.125	201 2016-08-14 00:20	2:21
		•	Go To IPAM Network Detail	S Into10.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**

Infoblox 💸		Dashboards	Data Management	Smart Folders	Grid Admin	istration		
		IPAM Devices	Network Users (DHCP DNS FI	le Distribution Th	reat Analytics		
Finder Smart Folders Fookmarks Recycle Bin Curl Links	* * *	IPAM Home > 192.168.1 Type: Comment:	192.168.1.0/24 .119 Pv4 Address A Record, Lease, Pv4 D	* HCP Range		MAC Address: Name: DHCP Fingerprint:	00:0c:29:cf:07:17 jeppich-pc.dhcp.lab10.com, jeppich-PC Microsoft Windows Vista/7 or Server 2	
		Discovered (Cisco ISE Se Cisco ISE Se	Data ssion State: DISCONNECT curity Group: Employees	ED		Cisco ISE E	Ind Point Profile: Microsoft-Workstation	0
		Related Obje	Audit History Name jeppich-pc.dhcp.lab10.cor jeppich-PC	Type n A Record Lease	Active Users 6 6	ISE_Quarantine NONE	SE_NAS_Port_0 SE_NAS_P_Ad 8 DigabitEthernet1 192.168.1.3 0	▶ • () • • • • • • • • • •

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