

Infoblox NIOS Integration Guide

Infoblox Network Identity Operating System (NIOS) is the operating system that powers Infoblox core network services, ensuring non-stop operation of network infrastructure. This on-prem network management tool unifies DNS, DHCP, and IP address management (IPAM) and helps organizations improve security, operational efficiency, and service uptime.

Deployment Type

This integration supports **vendor cloud** deployments through 443.

If you already know that your environment supports this deployment type, continue to the next step. If you are unsure whether your organization supports vendor cloud deployments, please ensure your organization's compatibility before continuing.

Required Information and Setup

To integrate GreyMatter with Infoblox NIOS, collect the following details:

- URL - <https://10.220.21.25/wapi/v2.13.1/>
- Admin Username
- Admin Password

See instructions below to gather the required information.

Create a Role

1. Within Infoblox, click **Administration** in the top navigation.
2. Select **Roles** at the top of the **Administrators** tab.
3. Click the **Add Role** button to create a role, then enter a custom name (e.g., GreyMatter Integration).
4. Click **Save**.

Add Permissions

5. Click the **Permissions** link at the top of the **Administrators** tab.
6. In the **Roles** section, select the new role.
7. Click the **Add** icon.
8. Select the **Role Permission** option and select the new role from the drop-down menu.
9. Select **DNS Permissions** from the **Permission Type** drop-down menu and mark the checkboxes for the following permissions:
 - a. All Hosts – Read-Only
 - b. All IPv4 Host Addresses – Read-Only
 - c. All IPv6 Host Addresses – Read-Only
 - d. All Response Policy Zones – Read/Write

Infoblox NIOS Integration Guide

Manage Global Permissions

☐ Group Permission

Choose One

☒ Role Permission

Min Perm

Permission Type

DNS Permissions

Resources/Functions	Read/Write	Read-Only	Deny
Grid DNS Properties	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All DNS Views	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All DNS Zones	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All Hosts	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
All IPv4 Host Addresses	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
All IPv6 Host Addresses	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
All A Records	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Cancel

Save & Close

Manage Global Permissions

☐ Group Permission

Choose One

☒ Role Permission

Min Perm

Permission Type

DNS Permissions

Resources/Functions	Read/Write	Read-Only	Deny
All DNS64 Synthesis Groups	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All Response Policy Zones	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All Response Policy Rules	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All DTC LBDN Records	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All DTC LBDNs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All DTC Pools	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All DTC Servers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

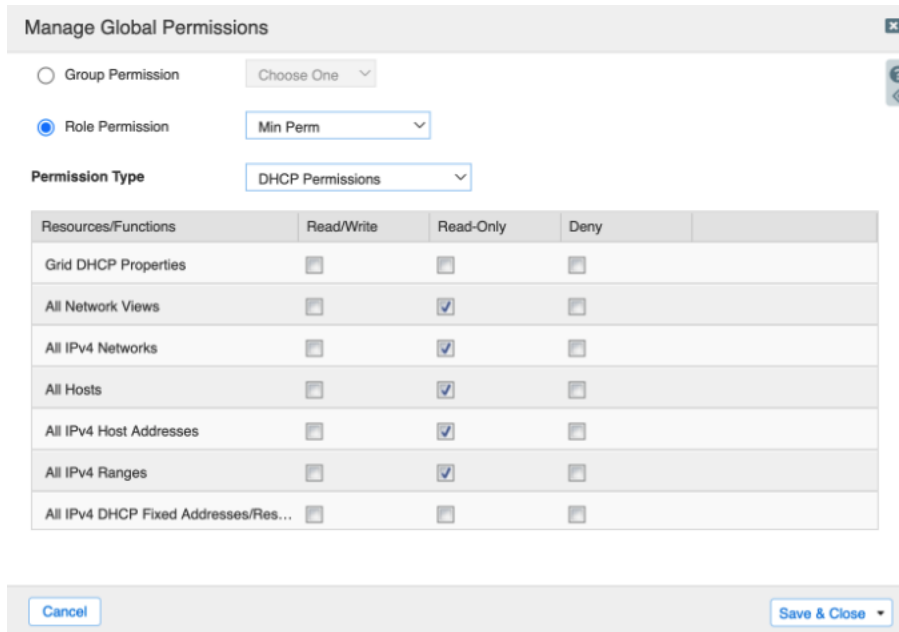
Cancel

Save & Close

10. Select **DHCP Permissions** from the **Permission Type** drop-down menu and mark the checkboxes for the following permissions:

- a. All Network Views – Read-Only
- b. All IPv4 Networks – Read-Only
- c. All Hosts – Read-Only
- d. All IPv4 Host Addresses – Read-Only
- e. All IPv4 Ranges – Read-Only

Infoblox NIOS Integration Guide



Manage Global Permissions

☐ Group Permission
 ☒ Role Permission

Choose One

Min Perm

Permission Type: DHCP Permissions

Resources/Functions	Read/Write	Read-Only	Deny
Grid DHCP Properties	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All Network Views	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
All IPv4 Networks	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
All Hosts	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
All IPv4 Host Addresses	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
All IPv4 Ranges	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
All IPv4 DHCP Fixed Addresses/Res...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

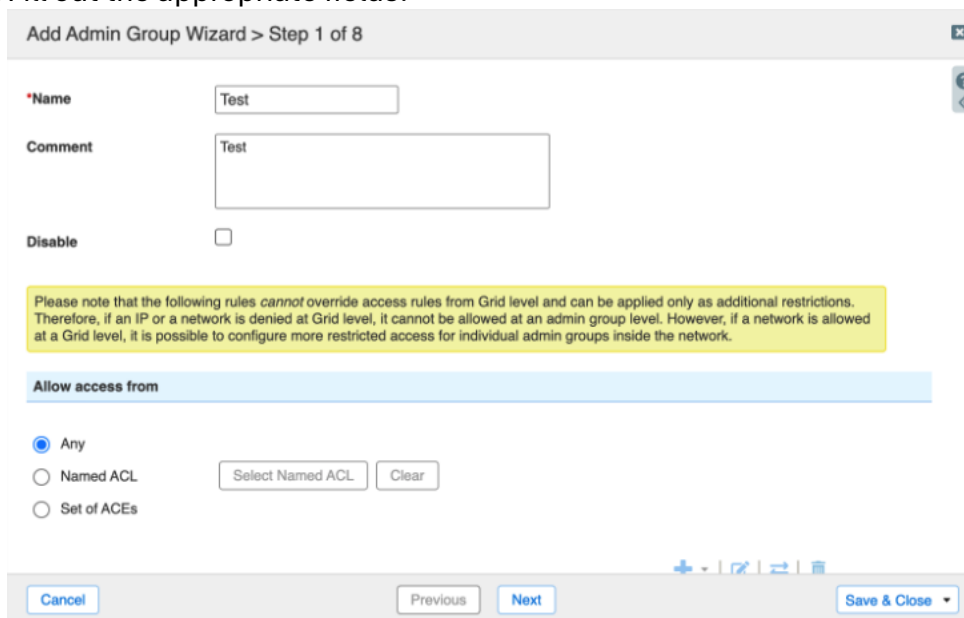
Cancel Save & Close

11. Click **Save & Close**.

Create a Group

12. Click the **Groups** link at the top of the **Administrators** tab.

13. Fill out the appropriate fields.



Add Admin Group Wizard > Step 1 of 8

*Name: Test

Comment: Test

Disable: ☐

Please note that the following rules cannot override access rules from Grid level and can be applied only as additional restrictions. Therefore, if an IP or a network is denied at Grid level, it cannot be allowed at an admin group level. However, if a network is allowed at a Grid level, it is possible to configure more restricted access for individual admin groups inside the network.

Allow access from

☒ Any
 ☐ Named ACL
 ☐ Set of ACEs

Select Named ACL Clear

Cancel Previous Next Save & Close

14. Click **Save & Close**.

Add Permissions

15. Select the **Admins** link at the top of the **Administrators** tab.

16. Click **+ Add**.

- Note:** This Admin will only have permissions related to this integration.

Infoblox NIOS Integration Guide

Add Administrator Wizard > Step 1 of 2

Authentication Type: Local

Credentials

*Login:

*Password:

*Confirm Password:

Password must contain at least 4 characters, including at least 1 lowercase character, 1 uppercase character, 1 numeric character, 1 symbol character.

Use AWS SSH authentication keys: ☐

Authentication Method: Key pair

Cancel Previous Next Save & Close

17. Select the new Admin Group.

Add Administrator Wizard > Step 1 of 2

Email Address:

*Admin Group:

Comment:

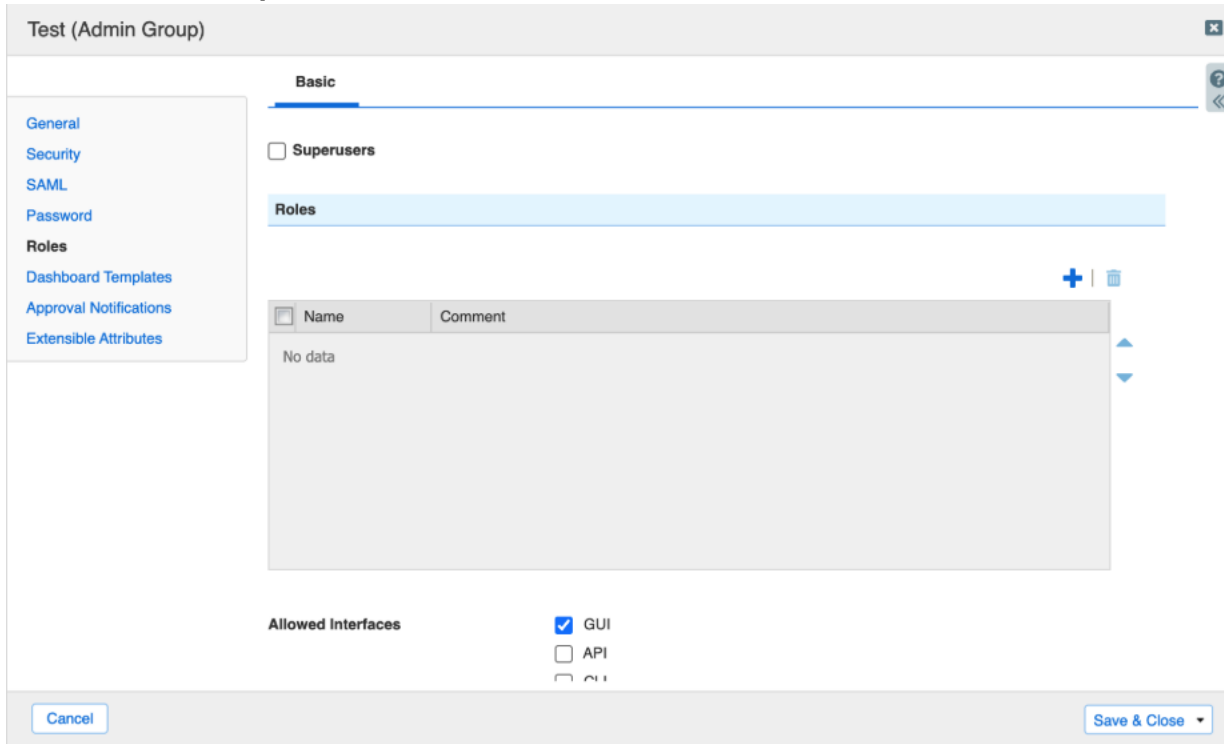
Disable: ☐

Status

Cancel Previous Next Save & Close

Infoblox NIOS Integration Guide

18. Go to **Admin Group**, then click **Edit**.



Test (Admin Group)

Basic

☐ Superusers

Roles

Name	Comment
No data	

Allowed Interfaces

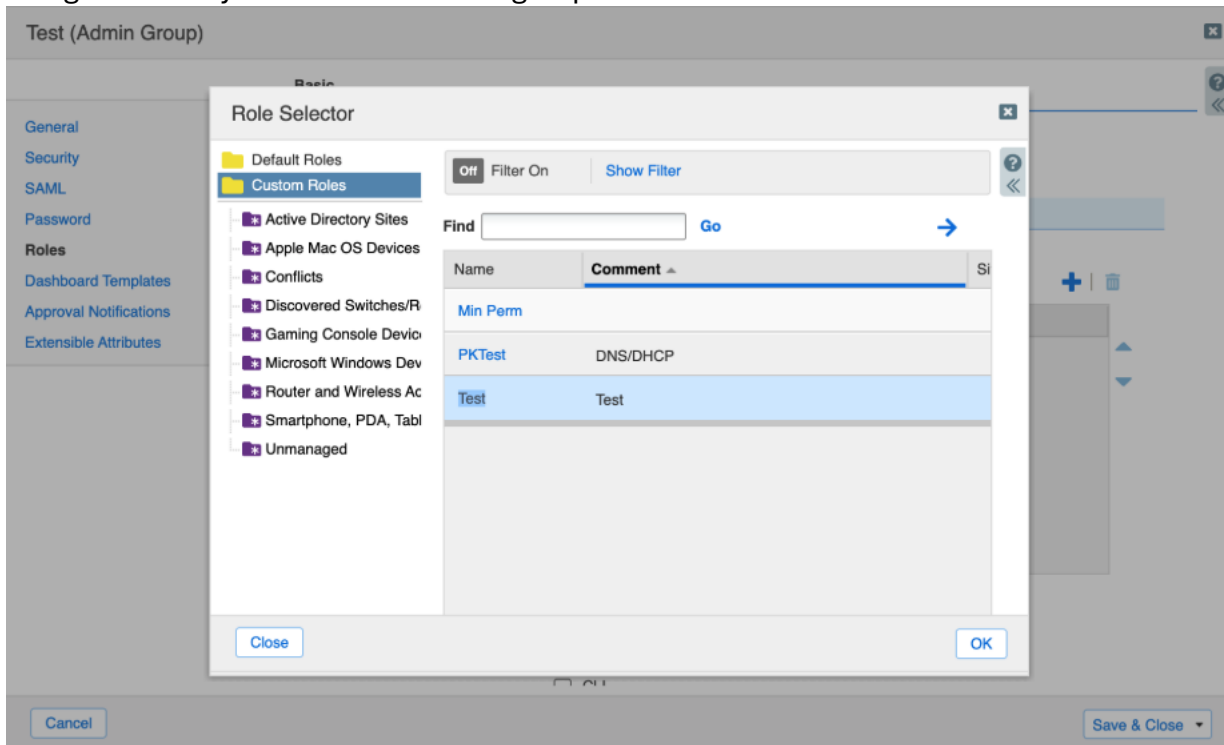
☒ GUI

☐ API

☐ CLI

Cancel Save & Close

19. Assign the newly created **Role** to the group created above.



Test (Admin Group)

Basic

Role Selector

Default Roles

Custom Roles

- Active Directory Sites
- Apple Mac OS Devices
- Conflicts
- Discovered Switches/R
- Gaming Console Devic
- Microsoft Windows Dev
- Router and Wireless Ac
- Smartphone, PDA, Tabl
- Unmanaged

Find Go

Name	Comment
Min Perm	
PKTest	DNS/DHCP
Test	Test

Close OK

Cancel Save & Close

[Vendor Documentation](#)

Infoblox NIOS Integration Guide

Permissions and Functionality

Permissions

Infoblocks Documentation: [About Administration Permissions](#)

GreyMatter Capability	Action(s)	Required Permission
Respond	Enrich Host	All Hosts All Network views All IPv4 Ranges All Hosts
	Enrich IP	All IPV4 Host Addresses All IPV6 Host Addresses All IPV4 Networks All IPV6 Networks
	Block IP	DNS Permission - Response Policy Zone (R/W)
	Block Domain	DNS Permission - Response Policy Zone (R/W)
	Unblock IP	DNS Permission - Response Policy Zone (R/W)
	Unblock Domain	DNS Permission - Response Policy Zone (R/W)

Respond

Playbook Name	Required Input	Result
Enrich Host	A Device Hostname Example: DESKTOP-GPSLRIB	Pulls details on the hosts that are managed by Infoblox.
Enrich IP	IPv4 or IPv6 Address <ul style="list-style-type: none"> IPv4 Example: 10.11.23.125 IPv6 Example: 2001:db8:3333:4444:5555:6666:7777:8888 	Pulls details on the hosts through IP address that are managed by Infoblox.
Block IP	A Device Hostname Example: 10.10.10.20	Block IP address in the Network.
Block Domain	A Domain Name Example: infoblox.com	Block Domain in the Network.
Unblock IP	A Device Hostname Example: 10.10.10.20	Unblocks IP address in the Network.
Unblock Domain	A Domain Name Example: infoblox.com	Unblock Domain in the Network.

Disclaimer: All customer data is classified and handled as 'Confidential' (as outlined in our Data Classification & Handling Policy). Customer data is restricted to authorized personnel only based on their business need. ReliaQuest uses least privilege and role-based access controls via Active Directory to provision and manage access. Please see our Access Control Policy for more information. ReliaQuest employees are also required to sign confidentiality agreements as part of their employment.