DEPLOYMENT GUIDE

Infoblox Universal DDI™ Agent for Microsoft

Table of Contents

Introduction

Organizations running Microsoft DNS and DHCP natively on Active Directory (AD) servers face escalating challenges. Server-bound tools create silos, forcing administrators to manage each environment in isolation. Tight coupling with AD adds complexity, making automation risky and troubleshooting slower. Fragmented workflows—multiple logins, brittle scripts, and manual operations—waste skilled staff time and drive-up operational costs. At the same time, forgotten DNS records expose systems to cyberthreats, and siloed NetOps, CloudOps, and SecOps lack a single source of truth, delaying remediation and complicating compliance. As hybrid and multi-cloud initiatives expand, these issues only get worse, limiting agility and slowing business outcomes.

The Infoblox Universal DDI™ Agent for Microsoft addresses these challenges by extending the Universal DDI platform to Microsoft environments. With a lightweight native agent and two-way sync, Microsoft DNS and DHCP can be managed in place—no rip-and-replace required. Administrators gain a single API and dashboard to unify control across hybrid and multi-cloud, with consistent policy enforcement that reduces errors and accelerates deployments.

In addition to DNS and DHCP management, the Infoblox Universal DDI Agent provides context to both Infoblox Threat Defense™ and Infoblox Universal Asset Insights™. User and device data, sourced from Microsoft, enriches network and security data, giving SecOps teams stronger visibility and faster incident response. The result is simplified workflows, reduced overhead, stronger security posture, and the agility to modernize Microsoft services at your own pace—all within the same Universal DDI platform that powers enterprise-wide network services.

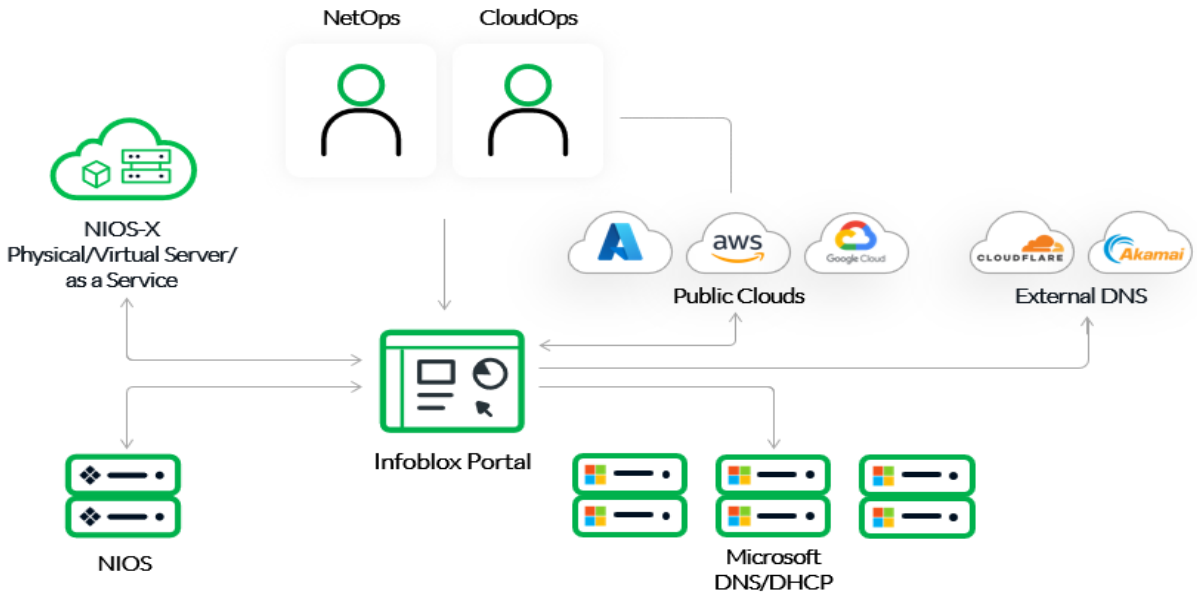


Figure 1. The Infoblox Portal acts as the management plane for Universal DDI and all integrated DDI platforms

Prerequisites

Before configuring the Universal DDI Agent for Microsoft, ensure that you have the following required permissions, access to management tools and open ports on your Microsoft Server(s).

Administrative Privileges

- Must be a Domain Administrator or have delegated permissions to manage Group Policy, DNS, and WMI configurations.
- Must have Local Administrator rights on each server (Domain Controller or Member Server) hosting DNS.
- Must have Administrator rights on the Infoblox Agent host (client machine) to configure CredSSP and modify local Group Policy.

Access to Management Tools

1. **Active Directory Users and Computers (ADUC)** for managing accounts and groups.
2. **ADSIEdit.msc** for editing AD-integrated DNS zone permissions (Domain Controllers only).
3. **wmimgmt.msc** for configuring WMI permissions.
4. **gpedit.msc or Group Policy Management Console (GPMC)** for editing local or domain Group Policies.
5. **Regedit** for updating local registry permissions for DNS Server configuration.
6. **PowerShell** run as administrator; to execute administrative commands.

Network and Connectivity Requirements

For DNS and DHCP use cases, TCP 5985 (WinRM HTTP) and 5986 (WinRM HTTPS) must be open between the Infoblox Agent host and all DNS and DHCP servers.

1. All systems must be in the same AD forest. Management of multiple forests from a single Infoblox Agent is not supported.
2. Time synchronization between client and DNS servers must be within five minutes.

Workflow

1. Create a Join Token via the Infoblox Portal.
2. Install the Universal DDI Agent on Select Windows member servers:
3. Install RSAT modules.
    a. Download the Universal DDI Agent.
4. Install the Universal DDI Agent.

Depending on the requirements, your workflow may change. Perform one or many of the following subsections as per your requirements.

DNS Management

1. Create a Domain User and add the user to the following built-in user groups:
    - DNS Admins
    - Remote Management Users
    - Domain Users
2. Prepare DNS Server(s) for the integration:
    - Configure WMI Permissions for DNS management
3. Prepare Domain controller(s):
4. Enable Windows Remote Management (WinRM) and Credential Security Support Provider protocol (CredSSP) on each Domain Controller.
5. Prepare the Universal DDI Agent client:
6. Run PowerShell commands for WSMan and CredSSP.
7. Enable and configure local Group Policy objects for credentials.
8. (Optional) Prepare the Domain Controller for Zone management via the integration with Infoblox:
9. Attach write, delete, and modify permissions to the Domain for DNS Admins via Active Directory Service Interfaces (ADSI).
10. Create a Microsoft: DNS Discovery Job.

DHCP Management

1. Create a Domain User and add the user to the following built-in user groups:
    - DHCP Administrators
    - Remote Management Users
    - Domain Users
2. Prepare DHCP Server(s) for the Integration:
3. Configure WMI Permissions for DHCP management.
4. Prepare Domain controller(s):
5. Enable Windows Remote Management (WinRM) and Credential Security Support Provider protocol (CredSSP) on each Domain Controller.
6. Prepare the Universal DDI Agent client:

7. Run PowerShell commands for WSMan and CredSSP.
8. Enable and configure local Group Policy objects for credentials.
9. Create a Microsoft: DHCP Discovery Job.

Cataloging Domain Assets and Enriching Asset Insights and Threat Defense with User Data

1. Create a Domain User and add the user to the following built-in user groups:
    - Domain Users
2. Configure a Windows Event Collector (WEC):
3. Information on how to configure a WEC server can be found here.
4. Create a Microsoft: Active Directory Discovery Job.
5. Create a Microsoft: Event Log Discovery Job.

Universal DDI Agent

The Universal DDI Agent is a lightweight agent that securely connects Microsoft DNS, DHCP, and AD services to the Infoblox Cloud platform. It enables centralized visibility and management of DDI (DNS, DHCP, IP address management) infrastructure, discovery of AD objects (users, computers, groups, sites), and collection of security event logs for enhancing asset attribution and threat detection.

The Universal DDI Agent can be configured to acquire the following information from Microsoft:

- Microsoft Event logs via a Windows Event Collector (WEC)
- Microsoft Active Directory (AD) objects via an AD Discovery member server

The Universal DDI Agent also allows for create, read, update and delete operations on DNS and DHCP objects in Microsoft Server.

Please note that with the current iteration of the Universal DDI Agent only one of the above use cases may be configured per instance of Universal DDI Agent. For example, a single agent may not perform DNS and DHCP management, two separate instances of the agent must be deployed on two different Windows Member servers. For the full Infoblox and Windows Server integration, four agents are required.

Before installation on a Windows Server device, the Universal DDI Agent requires the following RSAT modules installed (installation is accomplished via PowerShell, covered later in this guide):

1. RSAT-AD-PowerShell
2. RSAT-DNS-Server
3. RSAT-DHCP

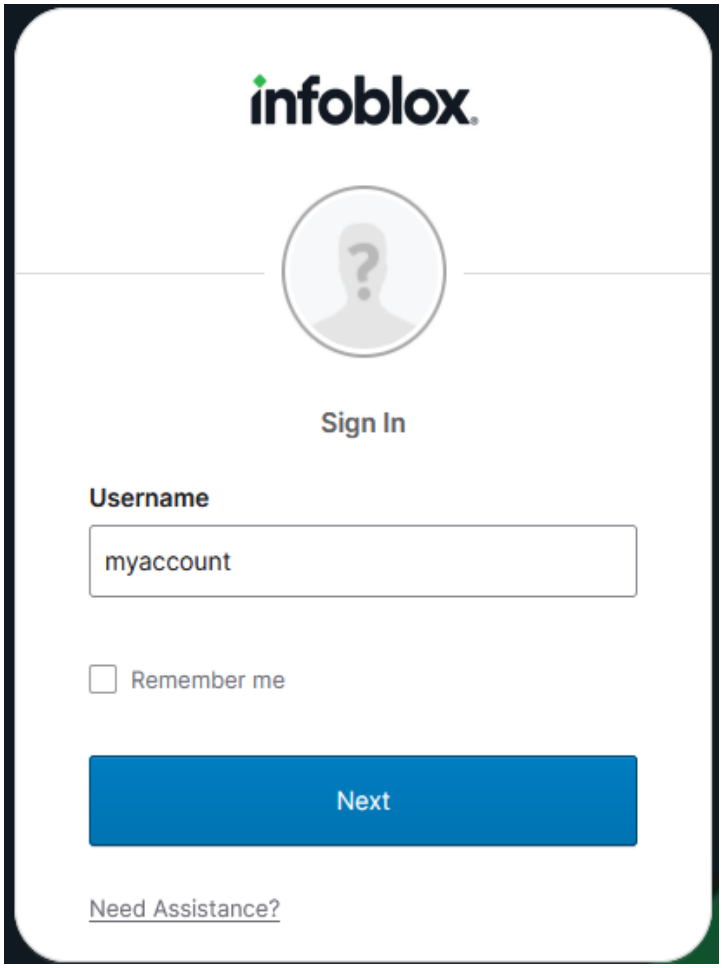
Universal DDI Agent Download and Installation

The Universal DDI Agent enables data transfer between Microsoft server and the Infoblox Portal. To install this agent, perform the following steps:

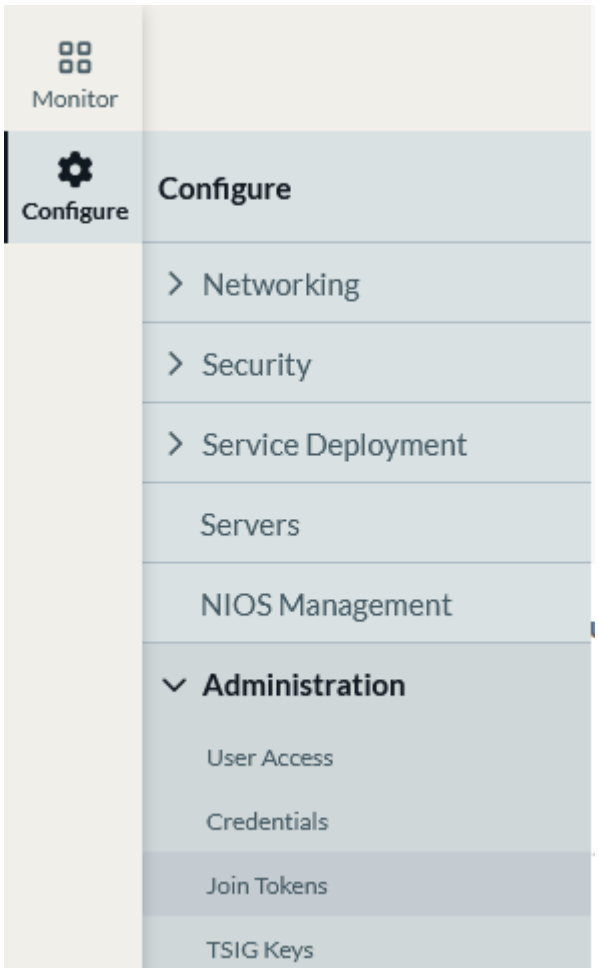
Acquire a Join Token

To properly install the agent, a Join Token from the Infoblox Portal is required. To acquire a Join Token, perform the following steps:

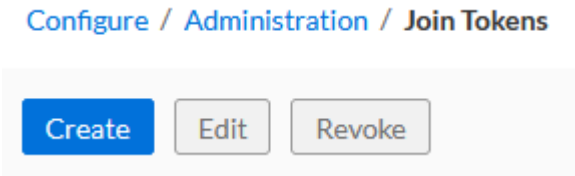
1. **Log in** to the Infoblox Portal.



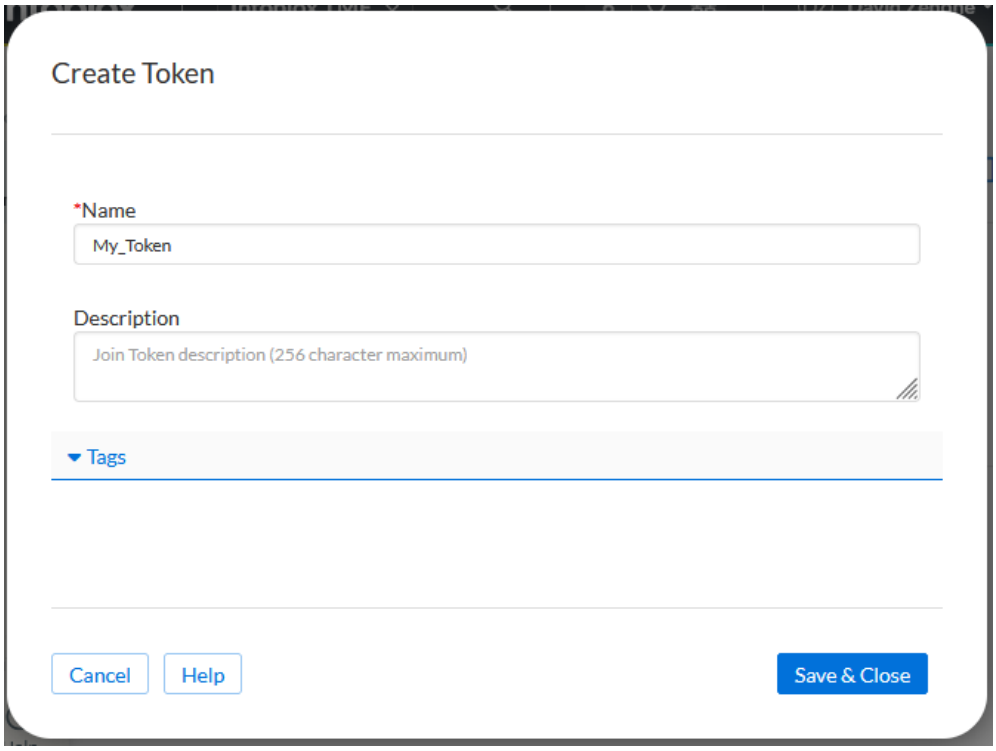
2. Navigate to the **Join Tokens** page. Highlight **Configure**, expand **Administration**, and click **Join Tokens**.



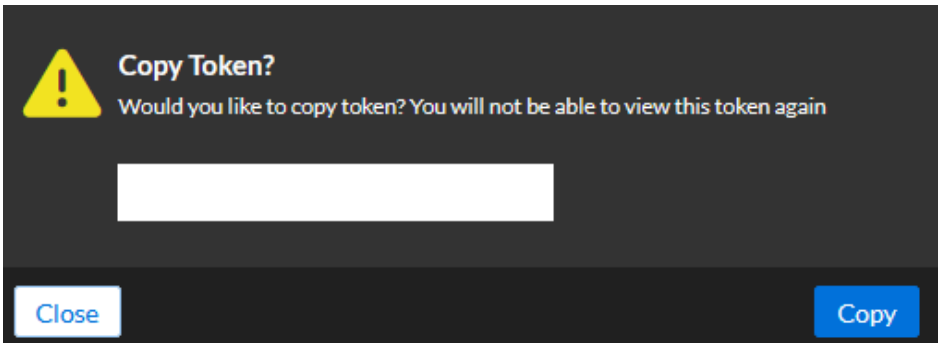
3. On the Join Tokens page, click **Create**.



4. In the **Create Token** panel, give the new Join Token a **Name**. Then, click **Save & Close**.



5. In the dialogue box that appears, click **Copy**.



6. **Save** the Join Token to a text document for use later in this guide.

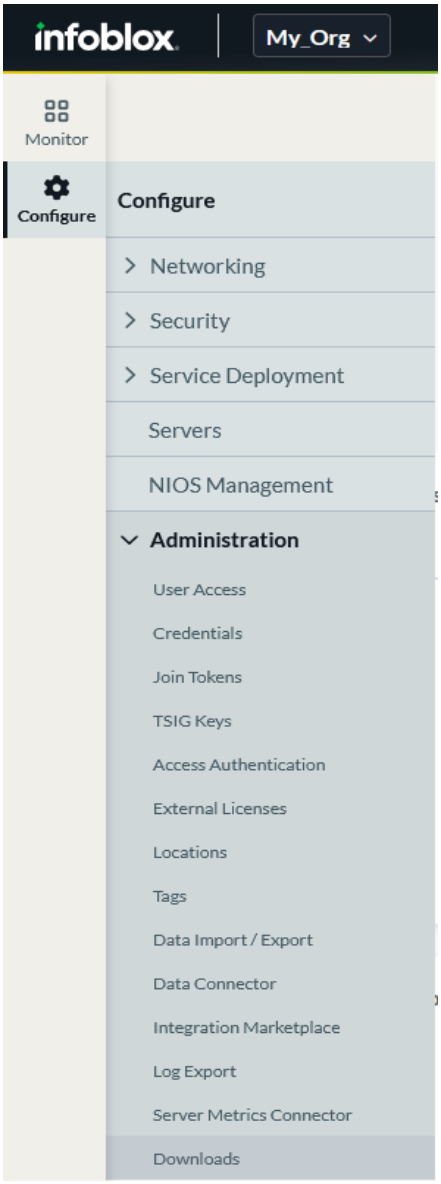
Install RSAT Modules

1. In the Windows Server where the Universal DDI Agent will be installed, input the following commands on a PowerShell console with elevated permissions:

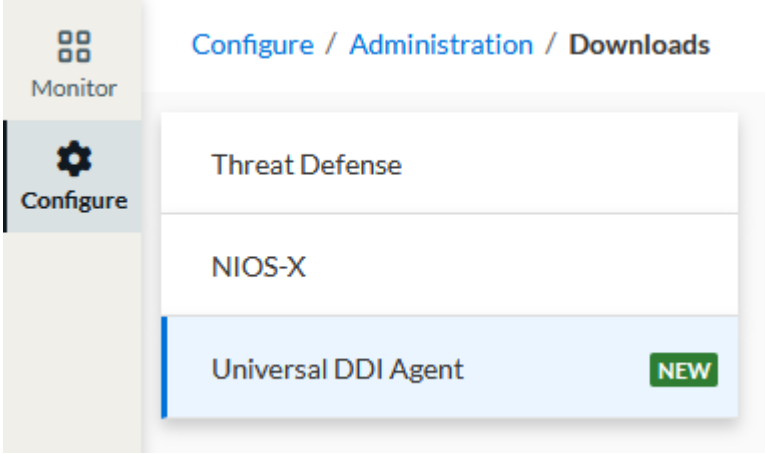
```
Install-WindowsFeature -Name RSAT-AD-PowerShell

Install-WindowsFeature -Name RSAT-DNS-Server

Install-WindowsFeature -Name RSAT-DHCP
```

Download and Install the Universal DDI Agent

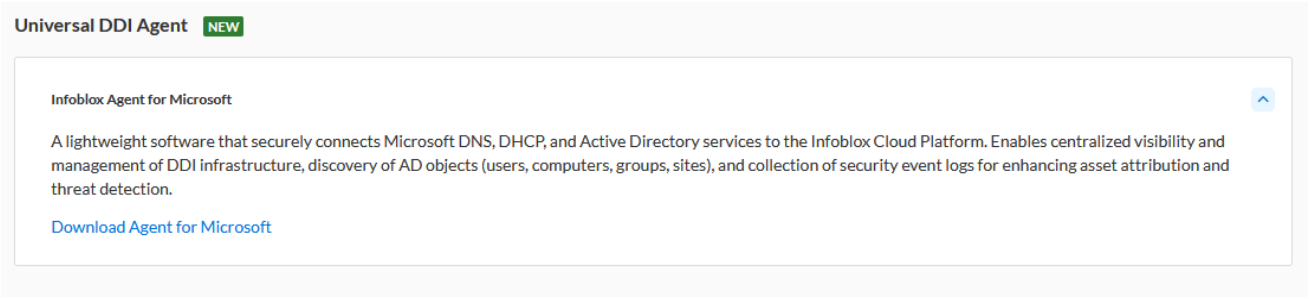
1. On the Infoblox Portal, navigate to the **Downloads** page. Highlight **Configure**, expand **Administration**, and click **Downloads**.



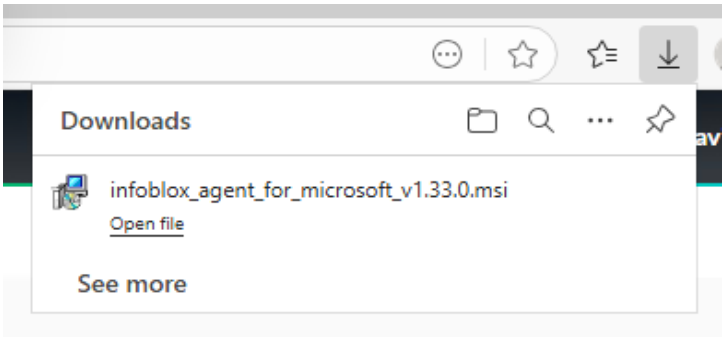
2. On the Downloads page, select **Universal DDI Agent**.



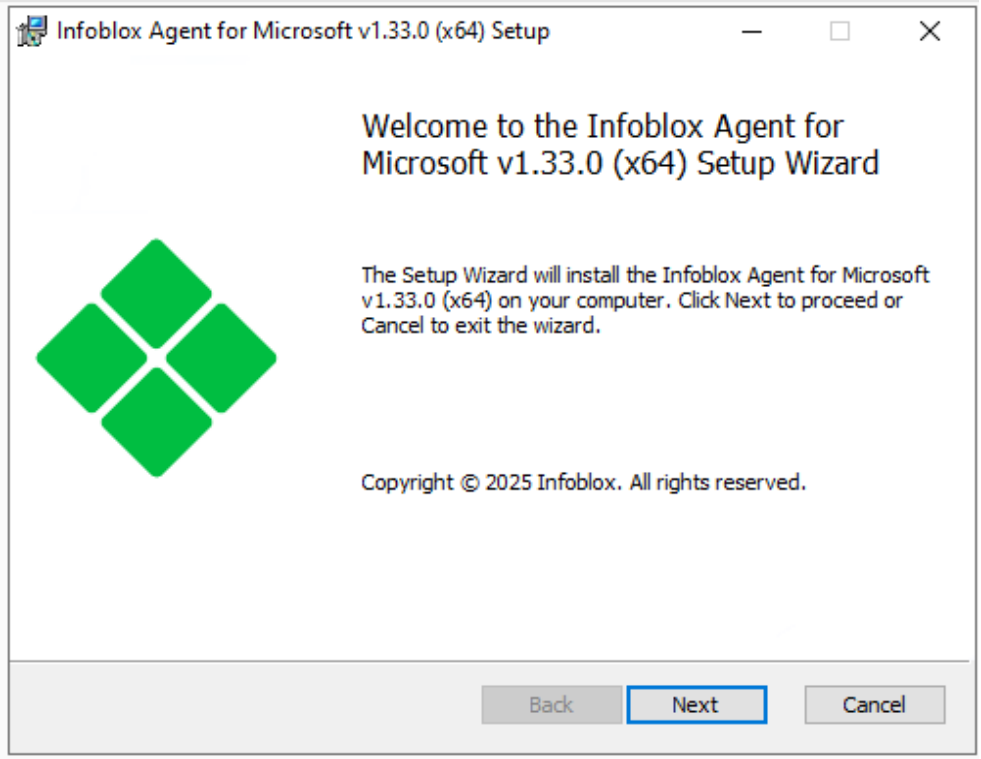
3. Click **Download Agent for Microsoft** and download the agent.



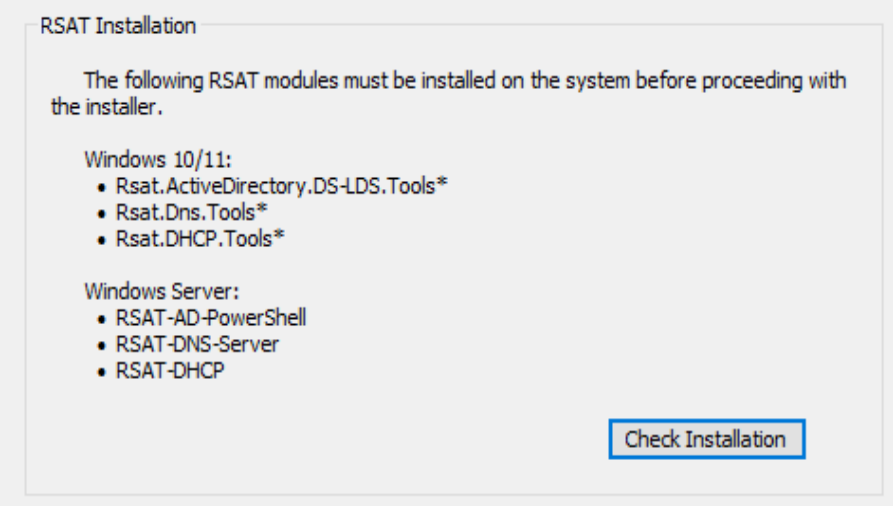
4. Once the download is complete, **run** the downloaded MSI file.



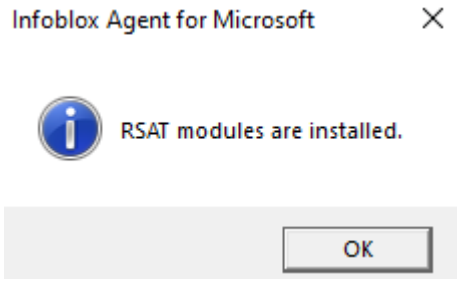
5. In the **Infoblox Agent for Microsoft Setup** panel, click **Next**.



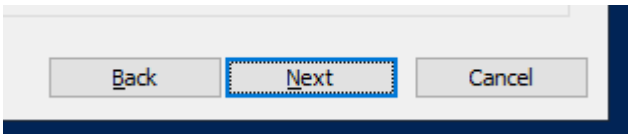
6. Verify that the RSAT modules have been installed. Click **Check Installation** to verify that the RSAT modules exist on the system where you are installing the agent. ***Note:*** *The agent requires **all** three RSAT modules to operate. If the modules are not installed, perform the steps in the Install RSAT Modules section of this guide.*



7. If the RSAT modules are found, the following prompt will appear. Click **OK** to continue:

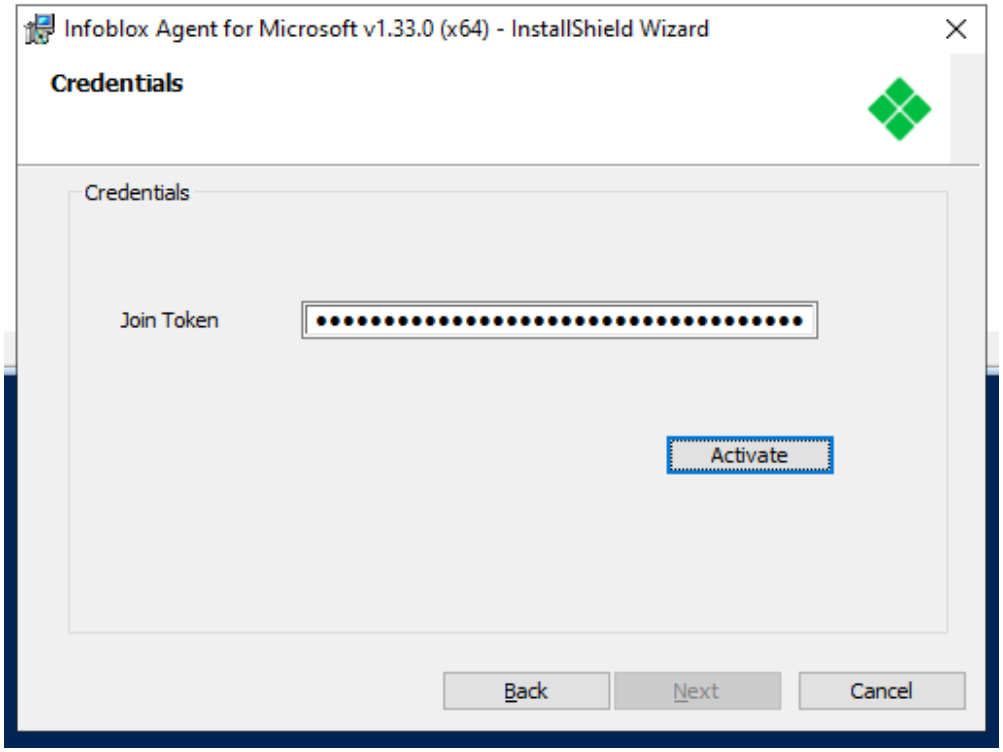


8. Click **Next**.

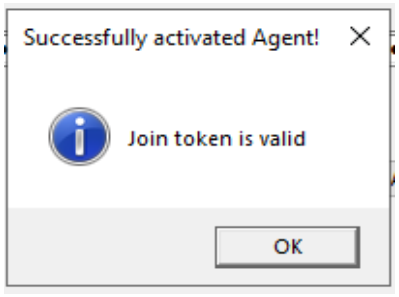


9. Input a Join Token acquired from the Infoblox Portal in the **Join Token** text field.

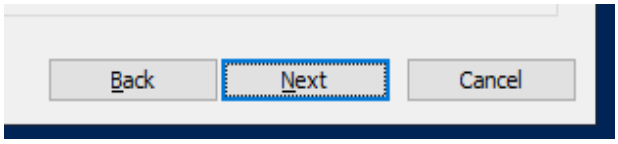
10. Click **Activate**.



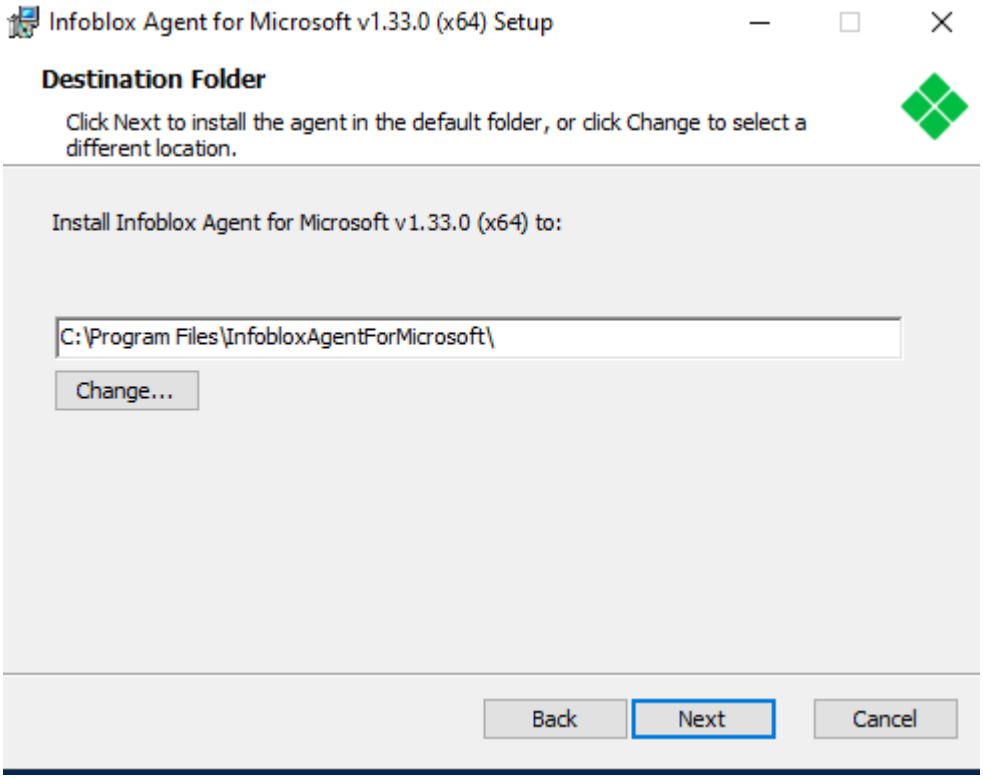
11. If the **Join Token** is accepted, the following dialog will appear. Click **OK** to continue.



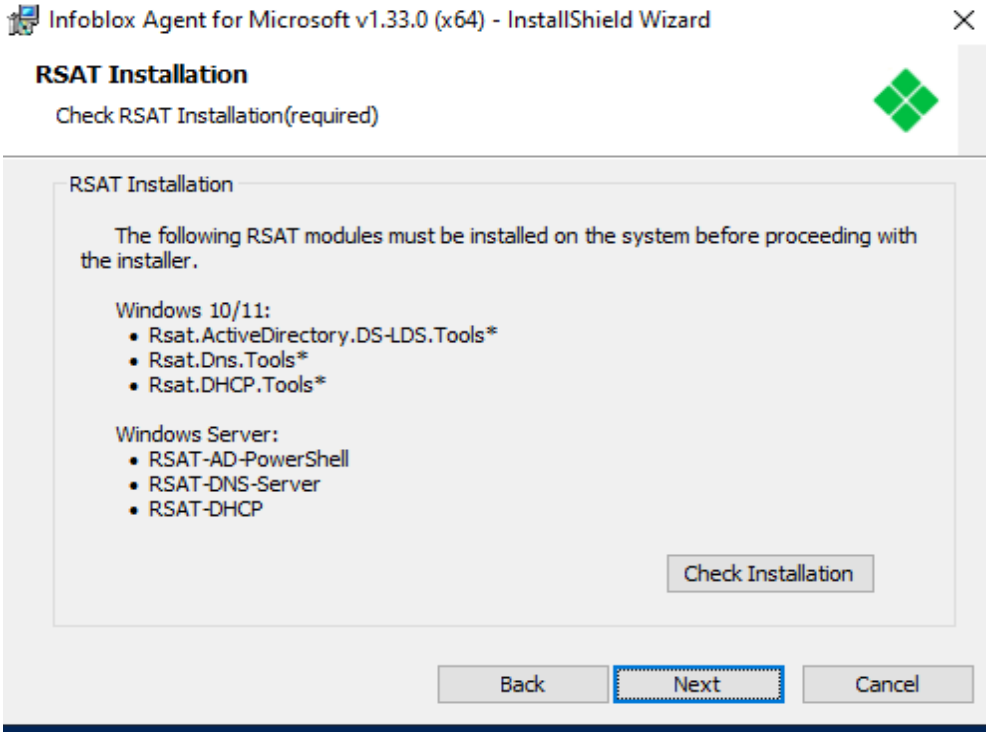
12. Click **Next**.



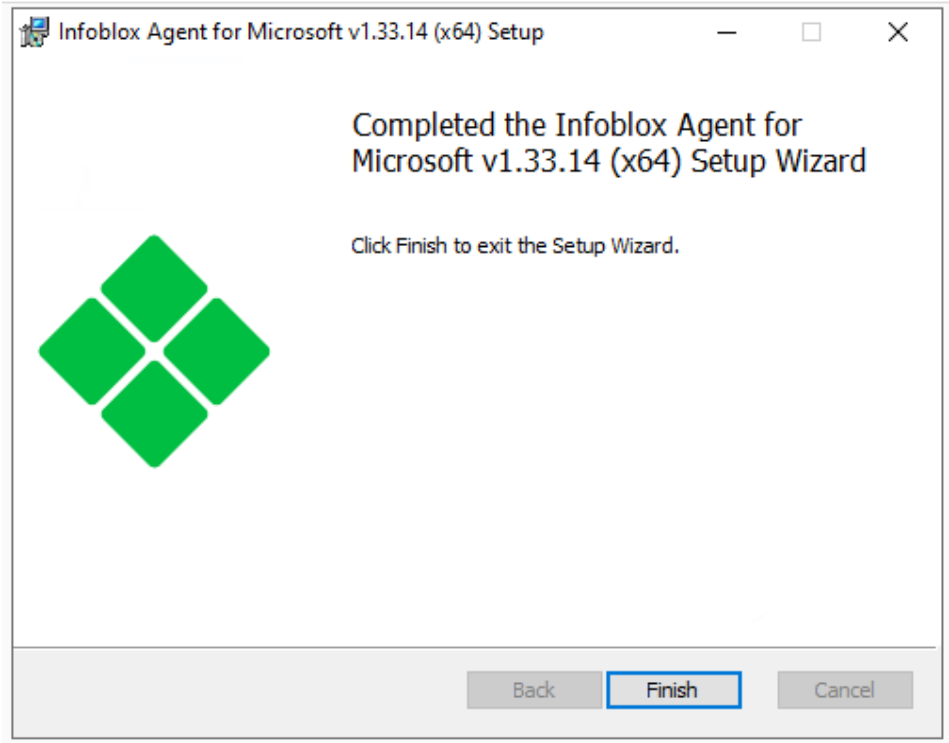
13. If desired, change the installation location with the **Change...** button. Otherwise, click **Next**.



14. Click **Next**.

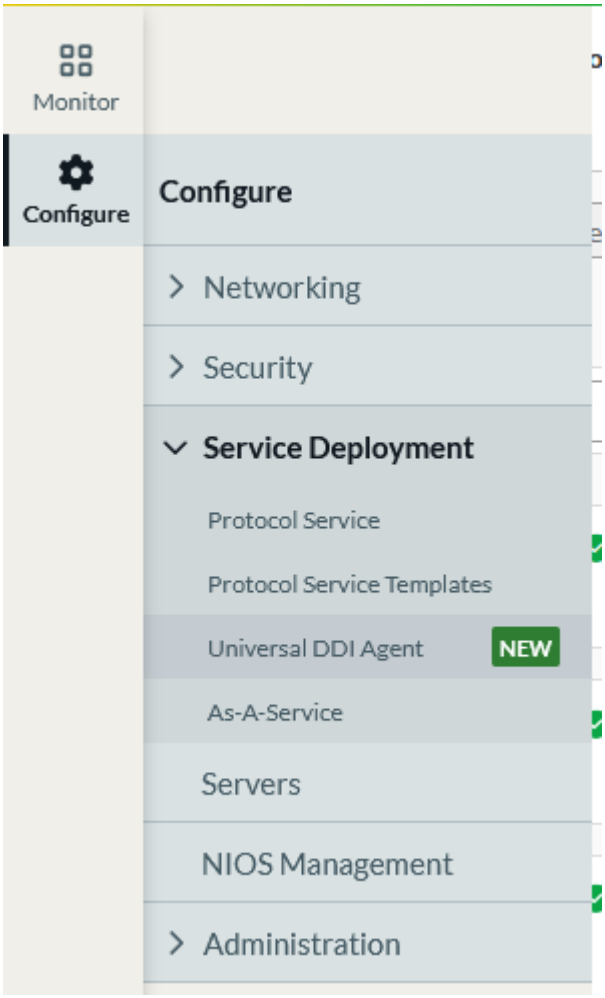


15. Wait for the installation of the agent to finish. Then, click **Finish**.

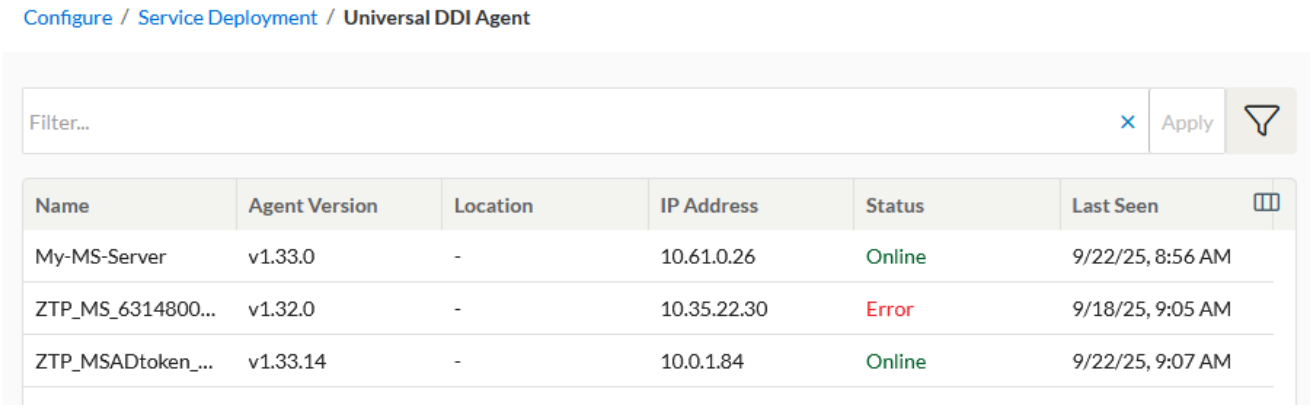


16. (Optional) Complete the sections Install RSAT Modules and Download and Install the Universal DDI Agent with any additional member servers desired.

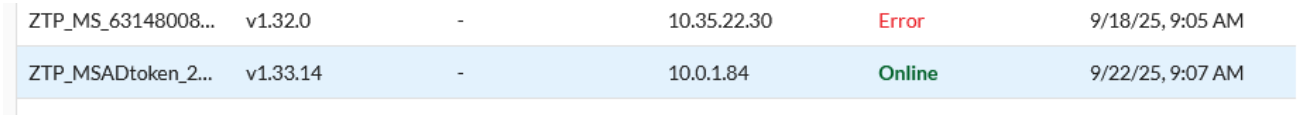
17. Navigate to the Universal DDI Agent page on the **Infoblox Portal**. Highlight **Configure,** expand **Service Deployment**, then click **Universal DDI Agent** in the dropdown list.



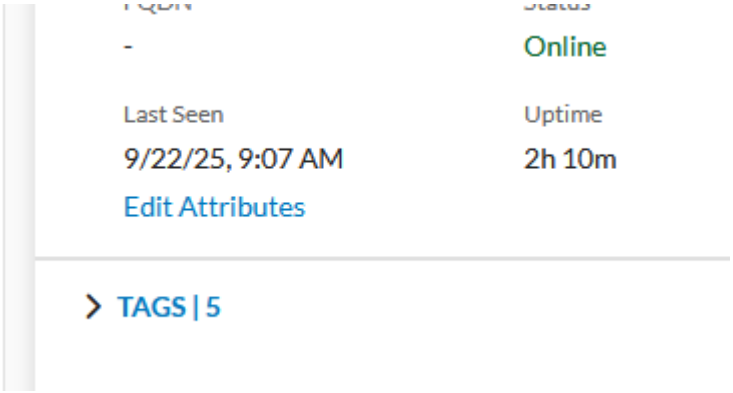
18. The table on the Universal DDI Agent page is a table of all existing Universal DDI Agents attached to this Infoblox Portal account.



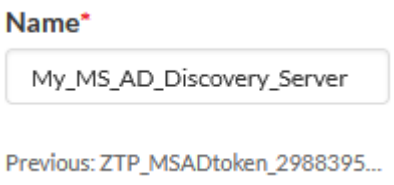
19. Locate and **click** the Universal DDI Agent that was just installed. ***Note:*** *The name will always begin with "ZTP_" and then the name of the Join Token that was provided for the installation.*



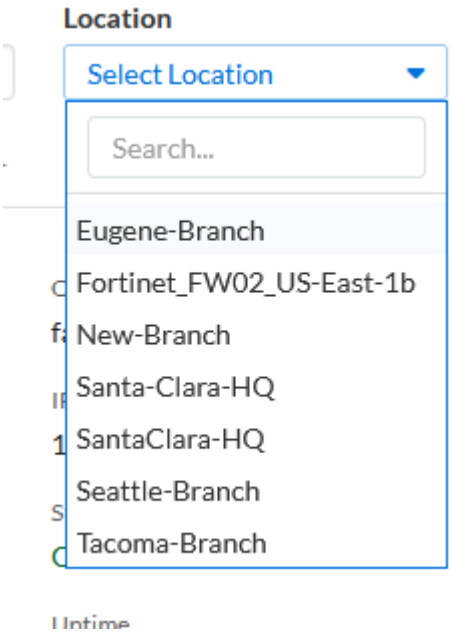
20. In the side panel that is revealed, click **Edit Attributes**.



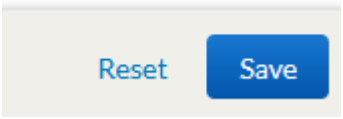
21. Provide a **Name** in the **Name** textbox.



22. (Optional) If desired, provide a **Location** for the Agent.



23. Click **Save** to confirm the new name.



24. (Optional) Repeat the previous steps to rename all newly installed Universal DDI Agent Installations.

Create Discovery Jobs

Discovery Jobs act as a set of parameters for discovery processes that sync data between Infoblox and other platforms. For guidance on how to create Discovery Jobs for the Universal DDI Agent refer to the following sections.

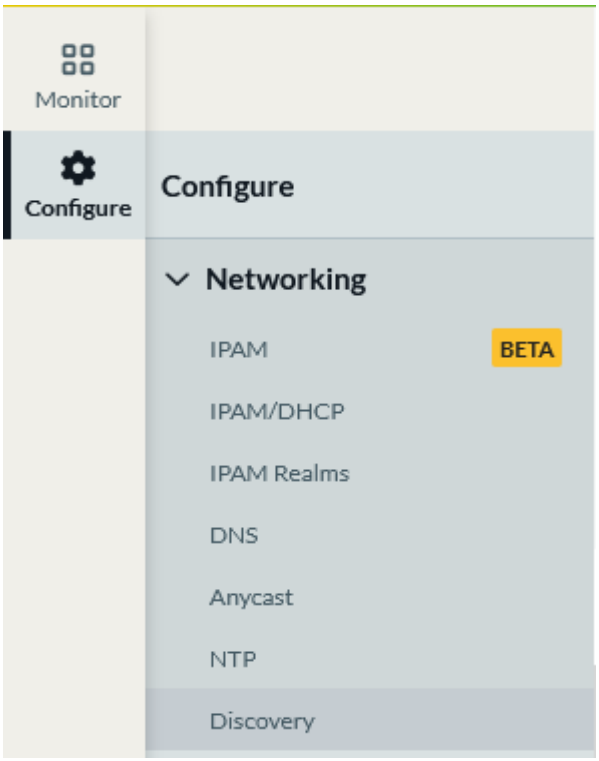
Please note that with the current iteration of the Universal DDI Agent only one Discovery Job may be configured per instance of Universal DDI Agent. For example, an agent may not perform Discovery Jobs for both DNS and DHCP. Two separate instances of the agent must be deployed on two different Windows Member servers.

Discovery Job for WEC Windows Member Server

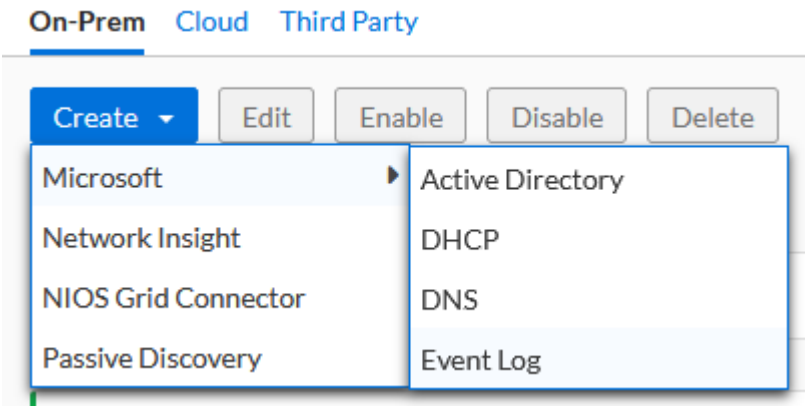
This section is intended to guide administrators through the creation of a Discovery Job which syncs Windows Event logs to the Infoblox Portal. This Discovery Job acquires Windows Security events by means of the Universal DDI Agent installed on a Windows Server that is configured as a Windows Event Collection (WEC) server. Infoblox then correlates user login information to Assets in the Asset Inventory based on the data collected.

For more information on how to deploy a Windows Event Collector, please view the Infoblox docs page located here.

1. Navigate to the **Discovery** page by highlighting **Configure**. Expand **Networking**, then click **Discovery** in the dropdown list.

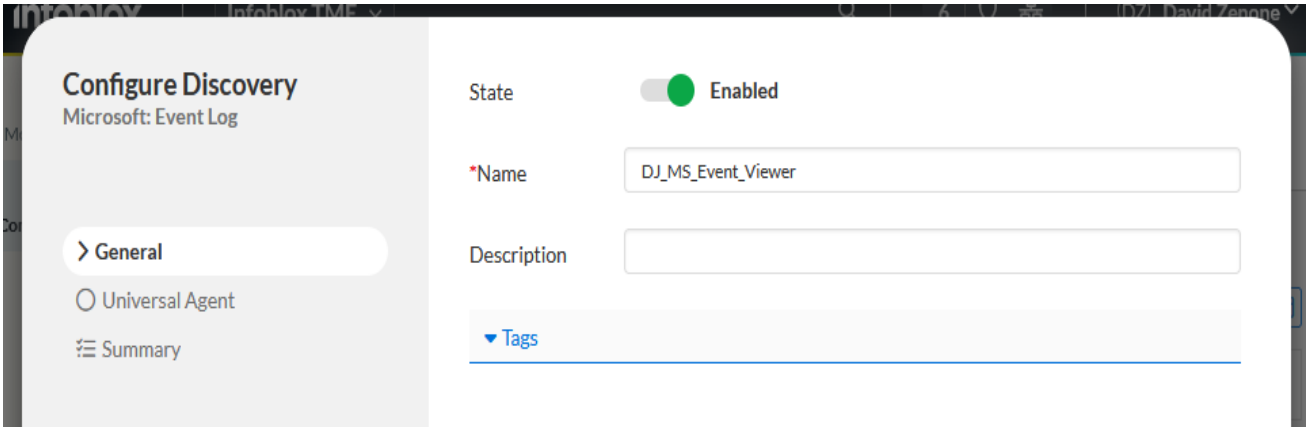


2. On the Discovery page, ensure that you are on the **On-Prem** tab. Click **Create**, highlight **Microsoft**, then click **Event Log** in the list that is revealed.

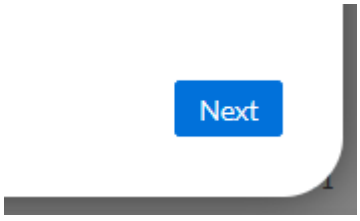


3. On the Configure Discovery Microsoft: Event Log panel, ensure the **State** toggle switch is set to **Enabled** for the new Discovery Job.

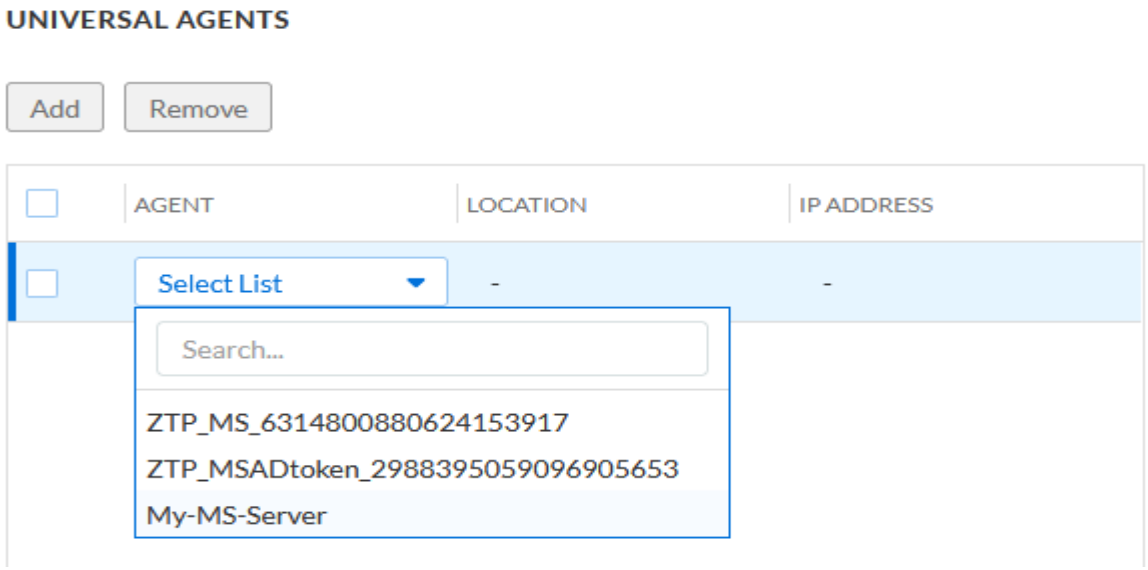
4. Input a **Name**.



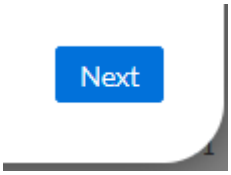
5. Click **Next**.



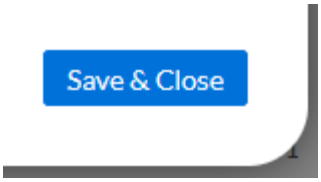
6. Click the **dropdown list** associated with the **AGENT** column and select the **Agent** associated with the WEC member.



7. Click **Next**.



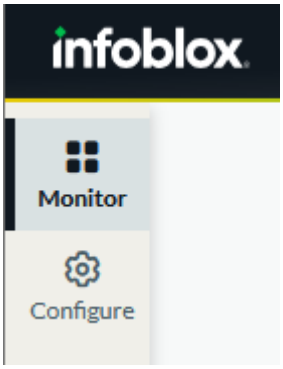
8. Click **Save & Close** to confirm the creation of the new Discovery Job.



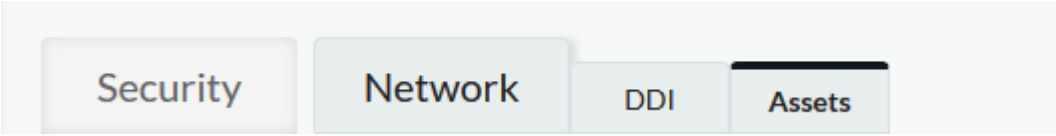
Viewing User Login Data in the Infoblox Portal

Once a WEC member has a Universal DDI Agent installed on it, and an associated Discovery Job has been created, User data can be viewed in the portal. ***Note:*** *This use case requires an associated AD object collection agent and Discovery Job as described in this section.* To view user data associated with a discovery AD object, perform the following steps:

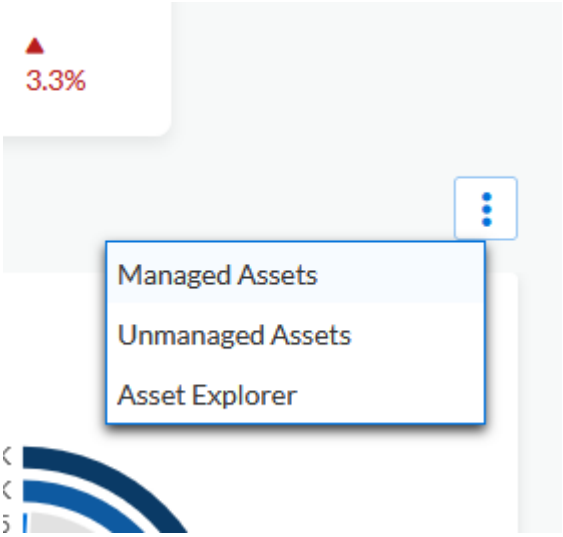
1. In the Infoblox Portal, navigate to the **Monitor** page by clicking the **Monitor** button in the navigation sidebar.



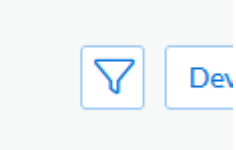
2. Once on the Monitor page, ensure that you are on the **Assets** tab.



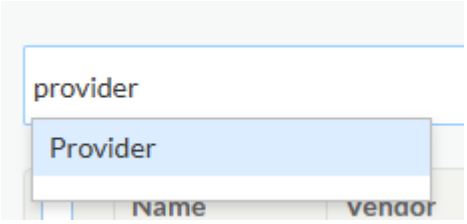
3. Near the top right of the Assets page, click the **kebab menu**. Then, click **Managed Assets** in the dropdown list.



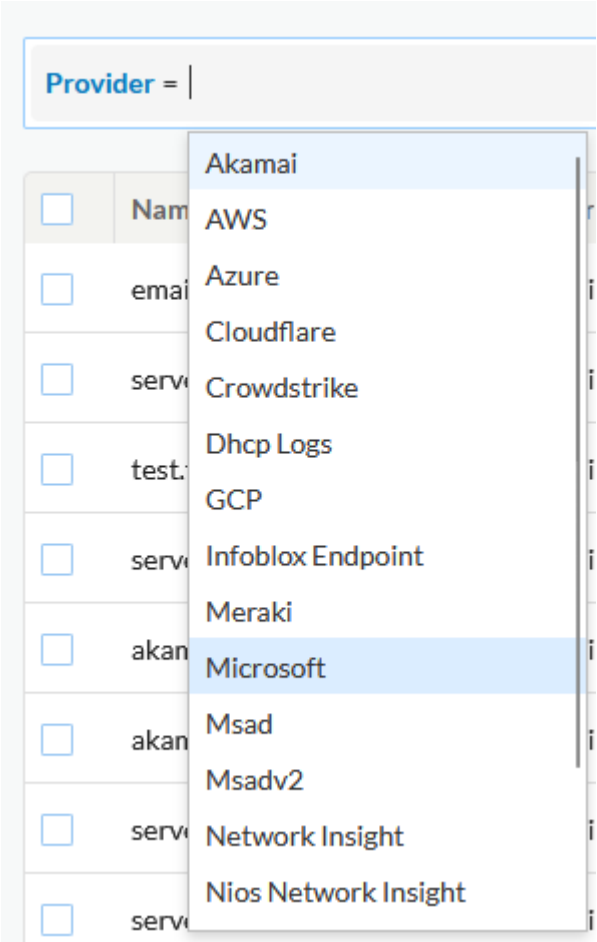
4. Wait for the asset inventory data to populate, then click the **filter** icon near the top right of the page.



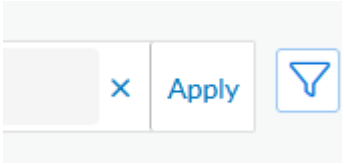
5. In the filter and search text field that is revealed, type ***Provider***. Then, click **Provider** below the text field.



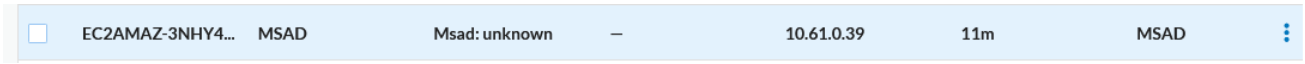
6. Then, click **Microsoft** in the dropdown list.



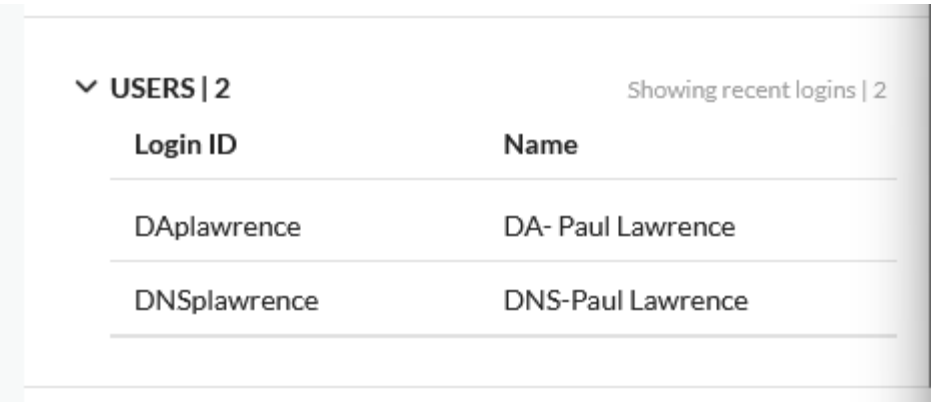
7. Click **Apply**.



8. Click on a discovered AD object in the list.



9. Scroll down in the side panel that is revealed. Under the **USERS** header, user data will be populated with recent logins.



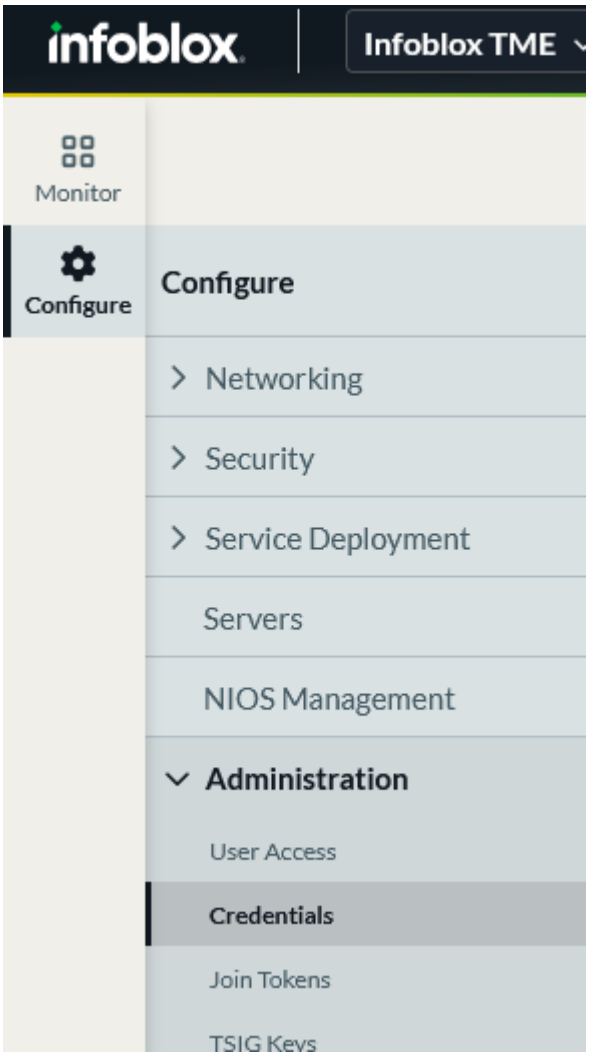
Discovery Job for Active Directory Object Discovery

This section is intended to guide administrators through the creation of a Discovery job for AD object collection. This Discovery Job when paired with the Event Log Discovery Job provides user and device context to both Asset Insights and Threat Defense. This section requires that you have an existing installation of the Universal DDI Agent on a Windows Member server. This Discovery Job acquires Active Discovery data by means of the Agent which is installed on a Windows Member Server.

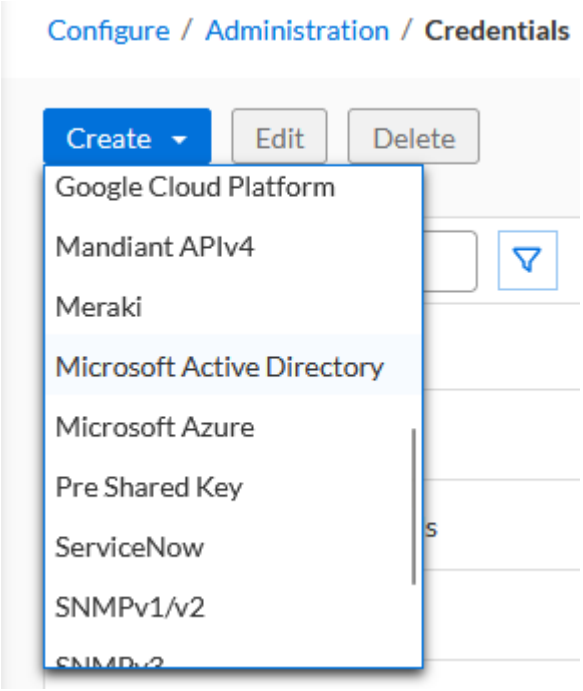
Create Credentials for AD Object Discovery

To sync AD objects with the Infoblox Portal, credentials for an AD User in the **Domain Users built-in group** must be added to the Infoblox Portal.

1. Log in to the Infoblox Portal. Highlight **Configure**, expand **Administration**, then click **Credentials** in the dropdown list.

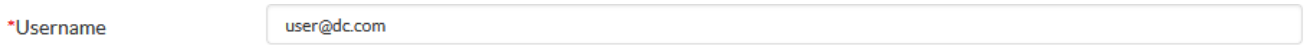


2. Click **Create**, then click **Microsoft Active Directory** in the dropdown list.



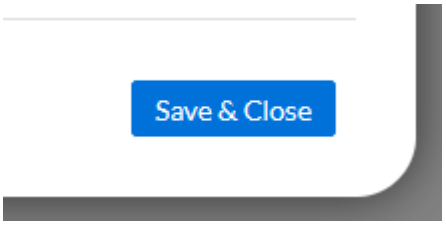
3. Input a **Name** for the Microsoft AD Credentials.

4. Input a Microsoft AD User in the **Username** text field. ***Note:*** *This user must be in the Domain Users built-in group.*



5. Input the password associated with the AD user in the **Password** text field.

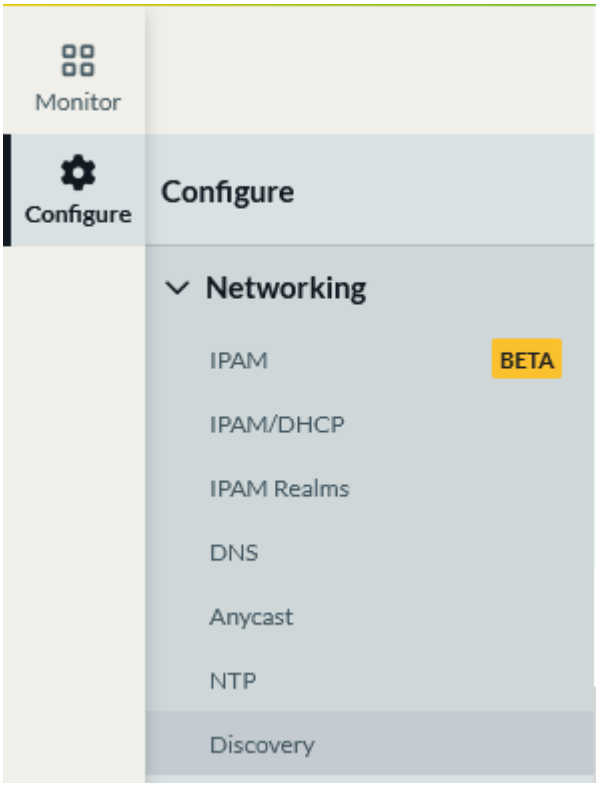
6. Click **Save & Close**.



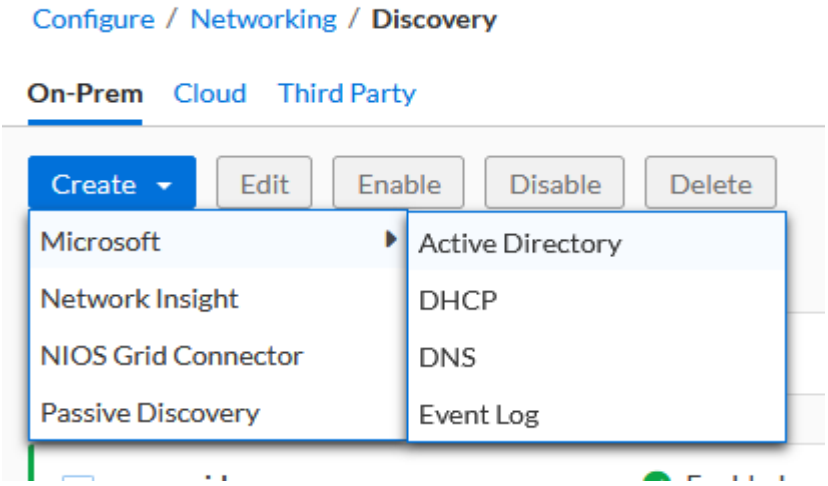
Create a Microsoft AD Discovery Job

Once you have installed the Universal DDI Agent and created a Domain User for AD object discovery, a Discovery Job can be created. To create a Discovery Job for AD object discovery, perform the following steps:

1. Navigate to the **Discovery** page by highlighting **Configure**. Expand **Networking**, then click **Discovery** in the dropdown list.



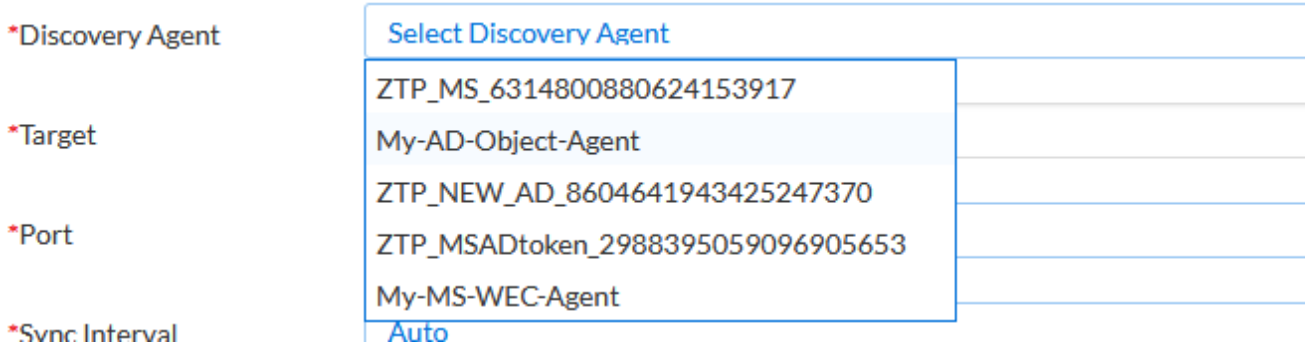
2. On the Discovery page, ensure that you are on the **On-Prem** tab. Click **Create**, highlight **Microsoft**, then click **Active Directory** in the list that is revealed.



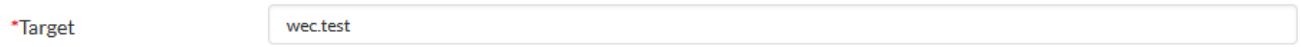
3. Ensure that the **State** toggle switch is set to **Enabled**.

4. Give the Discovery Job a **Name**.

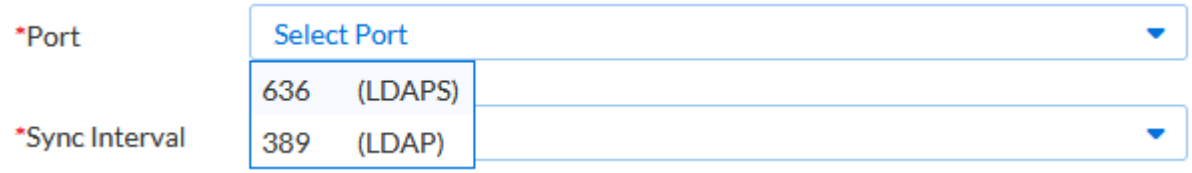
5. Select the appropriate Discovery Agent via the **Select Discovery Agent** dropdown list.



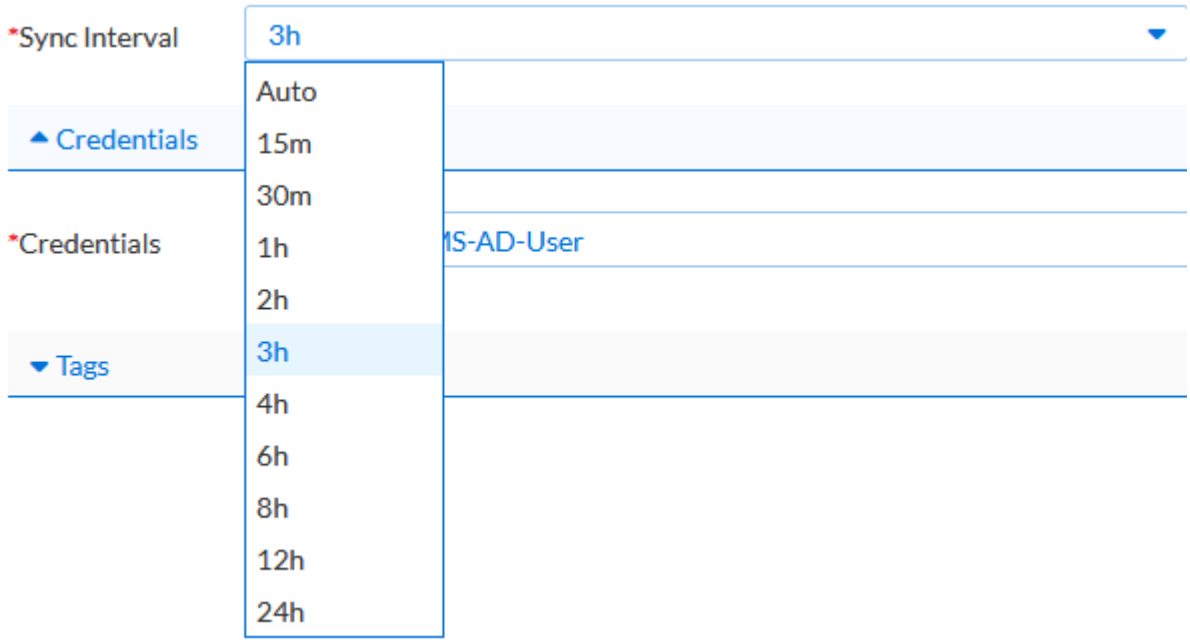
6. Provide the domain name in the **Target** text field.



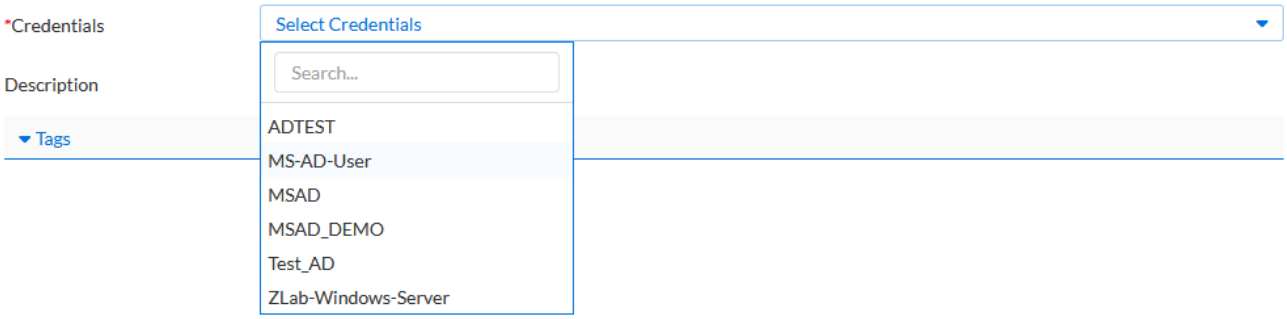
7. For the **Port**, select **636 (LDAPS)**. ***Note:*** *LDAPS requires the domain controller of this domain to have the Active Directory Certificate Services running. The LDAP port 389 is less secure and is not suggested but exists as an option if AD DS is disabled.*



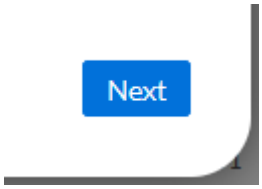
8. (Optional) Change the sync interval via the **Sync Interval** dropdown list. ***Note:*** *It is considered a best practice to set the Sync Interval to* ***3h*** *(three hours).*



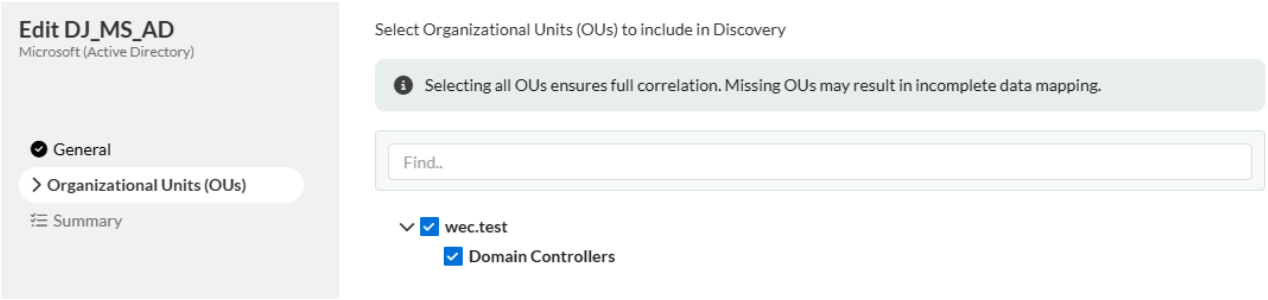
9. Locate and select the appropriate credentials that were created for MS AD object collection from the **Select Credentials** dropdown list.



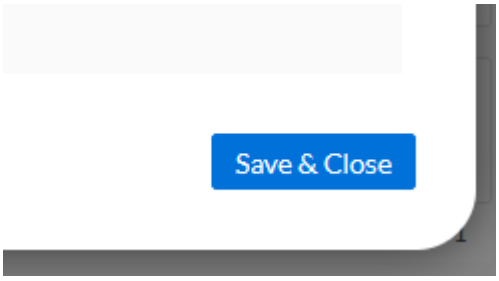
10. Click **Next**.



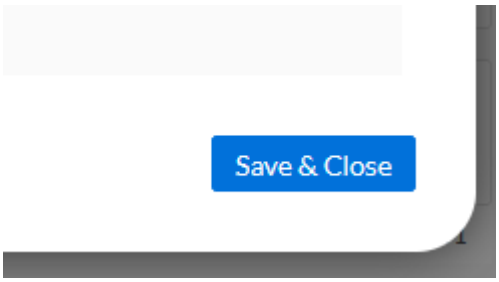
11. On the Organization Units (OUs) page, select the OUs that you wish to include for AD object collection. ***Note:*** *It is suggested to include all OUs when configuring this Discovery Job. If one or more OUs are omitted there may be gaps in synced data.*



12. Click **Next**.



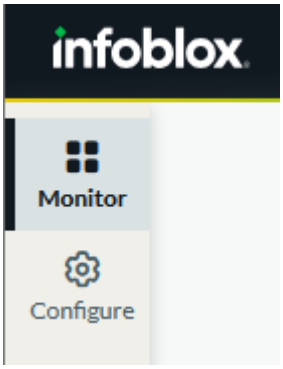
13. Click **Save & Close** to confirm the creation of the Discovery Job.



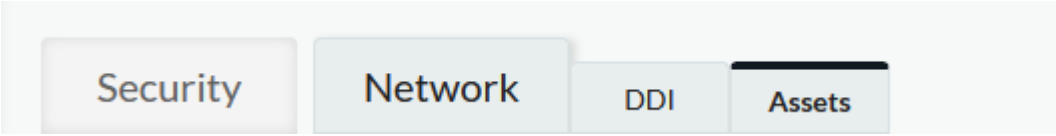
Viewing AD Objects with Asset Insights

Once the Universal DDI Agent and Discovery Job have been properly configured for AD object collection assets will begin populating in Asset Insights. To locate and view these objects, perform the following steps:

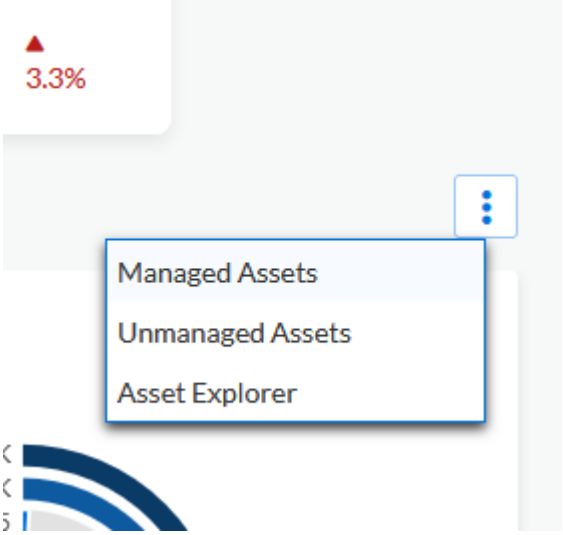
1. In the Infoblox Portal, navigate to the **Monitor** page by clicking the **Monitor** button in the navigation sidebar.



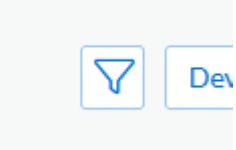
2. Once on the Monitor Page, ensure that you are on the **Assets** tab.



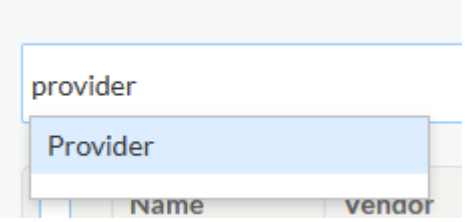
3. Near the top right of the Assets page, click the **kebab menu**. Then, click **Managed Assets** in the dropdown list.



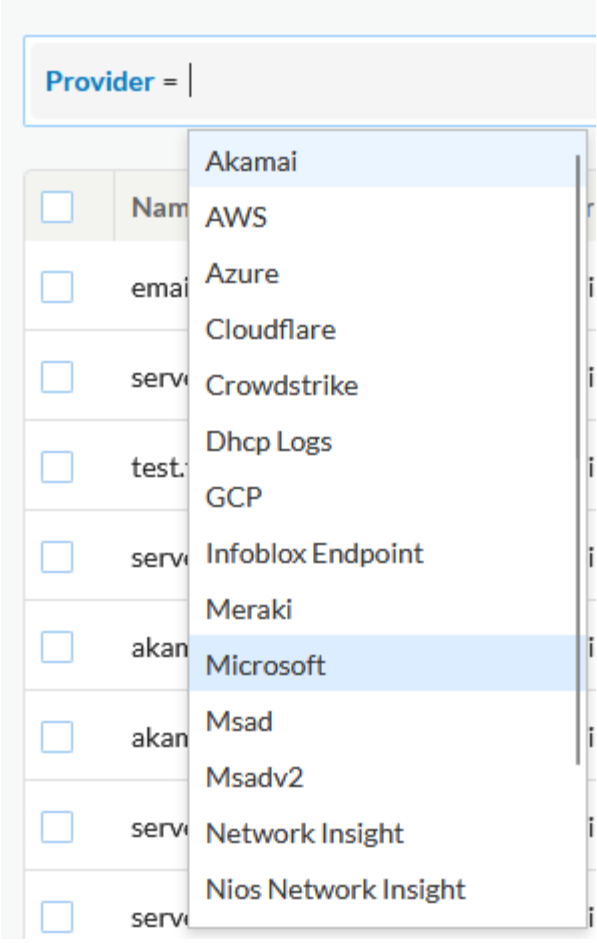
4. Wait for the asset inventory data to populate, then click the **filter** icon near the top right of the page.



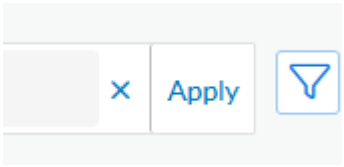
5. In the filter and search text field, type ***Provider***. Then, click **Provider** below the text field.



6. Then, click **Microsoft** in the dropdown list.



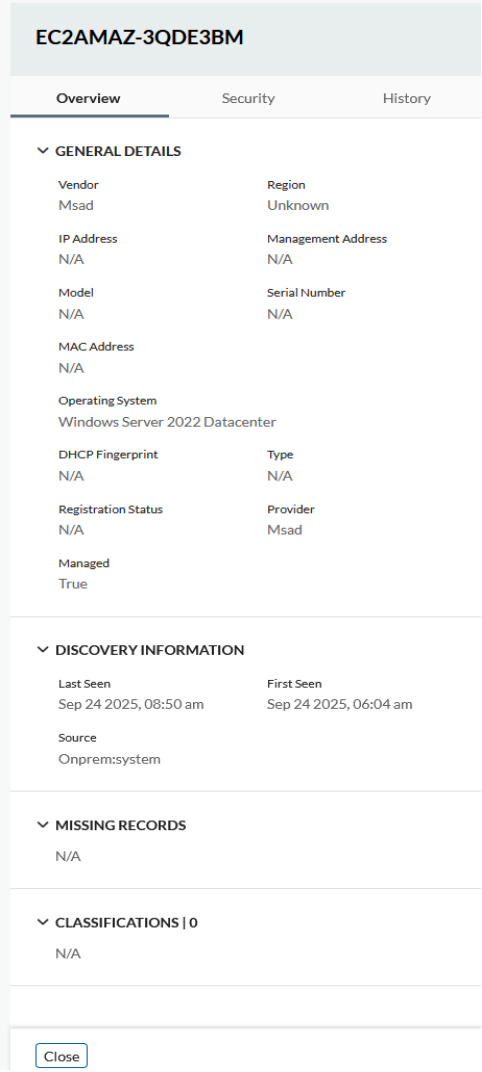
7. Click **Apply**.



8. Objects from the Discovery Job will populate in the list below. **Click** any line item to show additional data.

	Unnamed	MSAD	Msad: unknown	–	10.61.0.13	15m	MSAD
	EC2AMAZ-3QDE3...	**Msad**	**Msad: unknown**	**–**	**–**	**5m**	**MSAD**
	EC2AMAZ-3QDE3...	Msad	Msad: unknown	–	–	5m	MSAD

Example screenshot of object data:

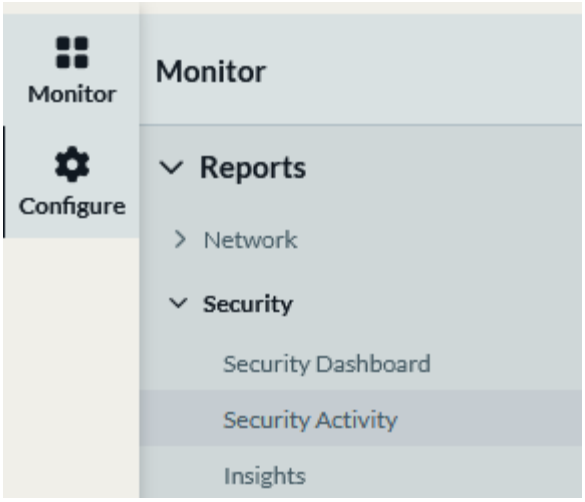


Enriching Infoblox Threat Defense with User Context

Another benefit of the Infoblox integration with Microsoft Server is the automatic application of User and Device data to DNS events. This section shows how to find an example of user data when a malicious query occurs and is blocked by Threat Defense.

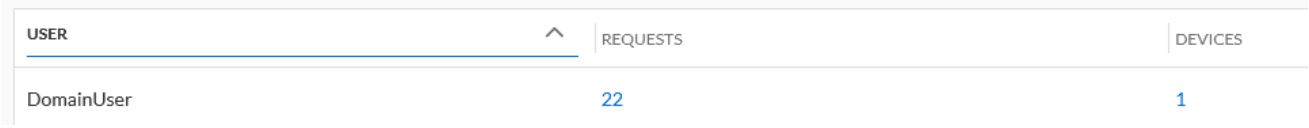
Note: *In the current iteration of Threat Defense and Universal DDI agent, this section only applies to DNS queries that have been resolved by an Infoblox DNS Forwarding Proxy.*

1. Log in to the Infoblox Portal and navigate to **Security Activity**. Highlight **Monitor**, expand **Security**, then click **Security Activity** from the dropdown list.

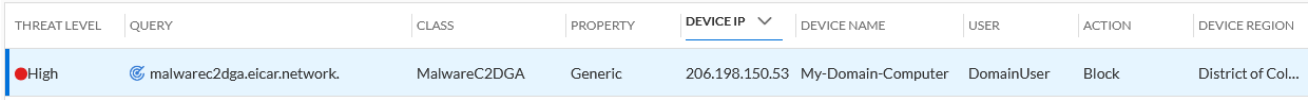


2. Click the **Users** tab located near the top right of the Security Activity page.

3. In the list of users, locate a Domain User and click the **Requests** value associated with this user.
Note: *This list will be empty if no Security Policy hits have occurred in the selected time value. If the list is empty, test the integration by querying a domain listed in the Infoblox Dossier tool while attempting this step again.*



4. Click the **REQUESTS** value to see a filtered list of queries that this user has made.



Discovery Job for DHCP Management

This section is intended to guide administrators through the creation of a Discovery Job for DHCP management of Windows based DNS. Discovery Jobs for DHCP management can be configured as Read Only or Read/Write.

Create Credentials for DHCP Management

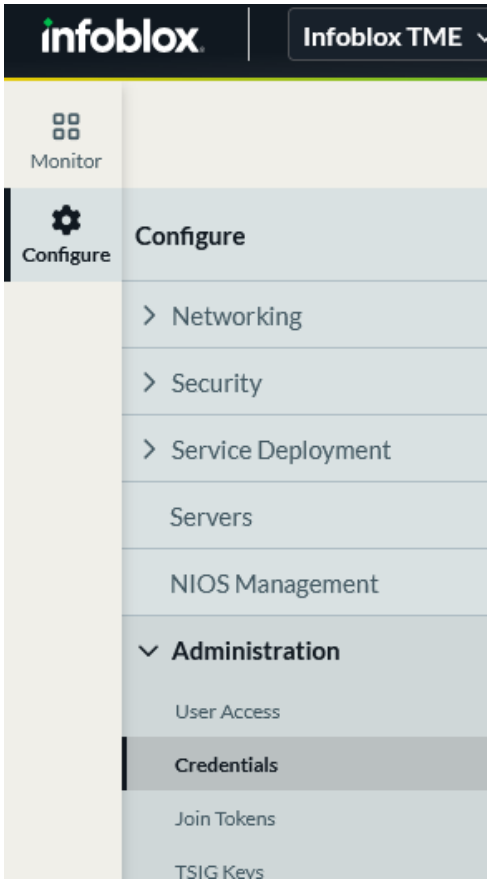
To configure a Discovery Job to manage Windows-based DHCP from the Infoblox Portal, credentials for an AD User must be added to the Infoblox Portal. The user(s) must be added to the appropriate AD groups as listed below:

DHCP Management:

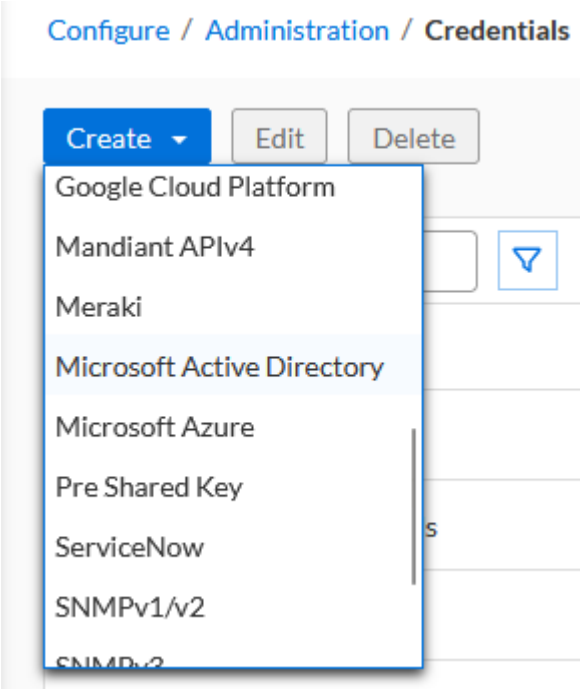
- DHCP Administrator
- Remote Management Users

To add the user to the Infoblox Portal, perform the following steps:

1. Log in to the Infoblox Portal. Highlight **Configure**, expand **Administration**, then click **Credentials** in the dropdown list.

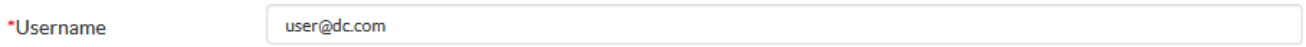


2. Click **Create**, then click **Microsoft Active Directory** in the dropdown list.



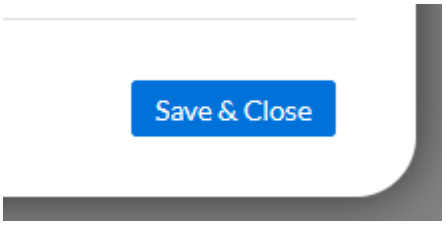
3. Input a **Name** for the Microsoft AD credentials.

4. Input a Microsoft AD User in the **Username** text field. ***Note:*** *This user must be in the DHCP Administrators and Remote Management Users built-in groups.*



5. Input the password associated with the AD user in the **Password** text field.

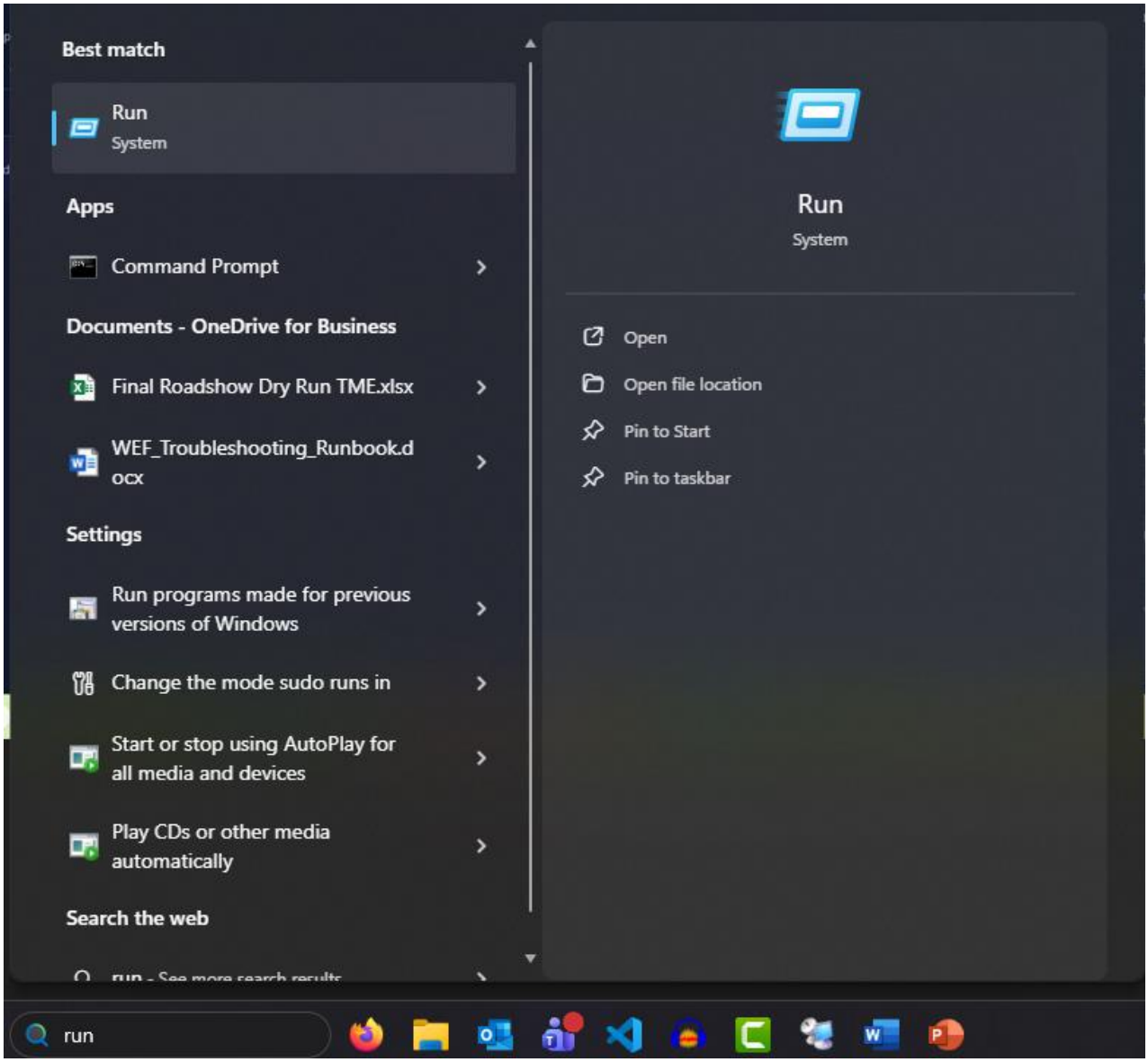
6. Click **Save & Close**.



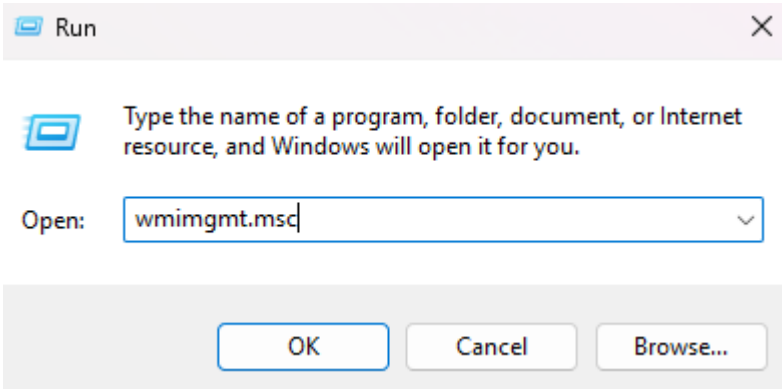
Configure WMI Permissions for DHCP Management

On each Windows DHCP server that will be managed by Infoblox, perform the following steps:

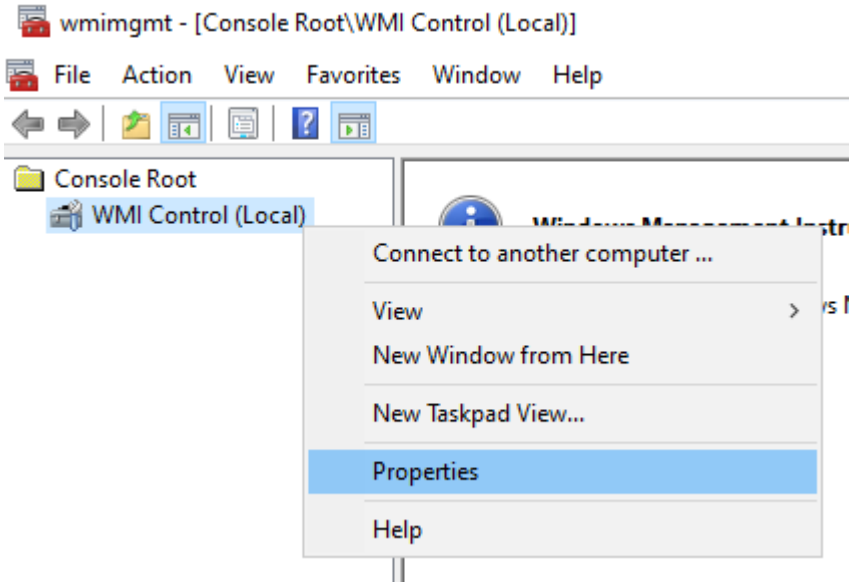
1. Access **Run** by searching for **Run** in the Windows search bar and clicking **Run**.



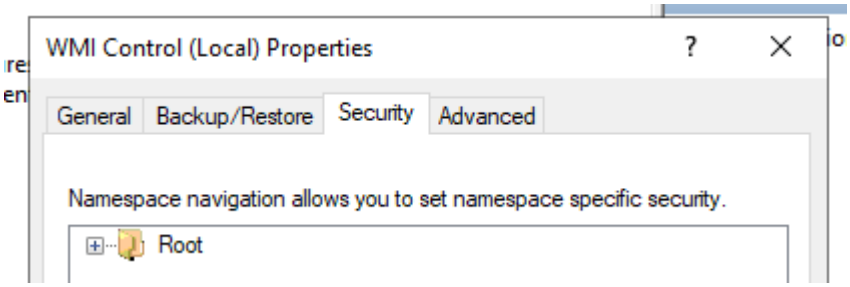
2. Run **wmimgmt.msc** by inputting **wimimgmt.msc** in the **Open** text field and clicking **OK**.



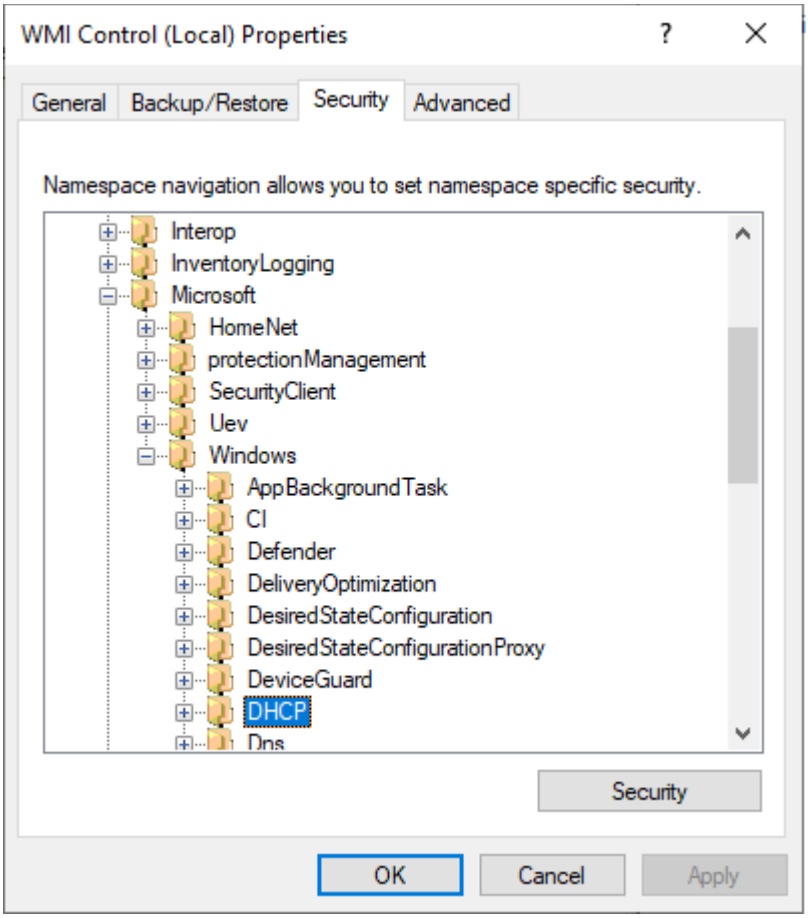
3. Right-click **WMI Control (Local)**, then click **Properties**.



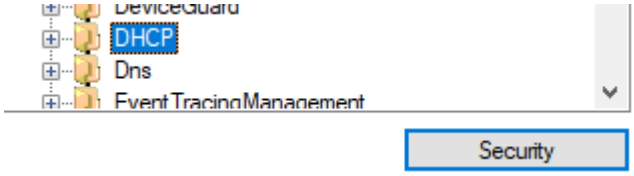
4. Click the **Security** tab in the **WMI Control (Local) Properties** panel.



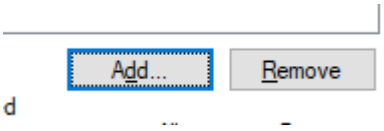
5. Expand **Root** → **Microsoft** → **Windows**, and then click **DHCP**.



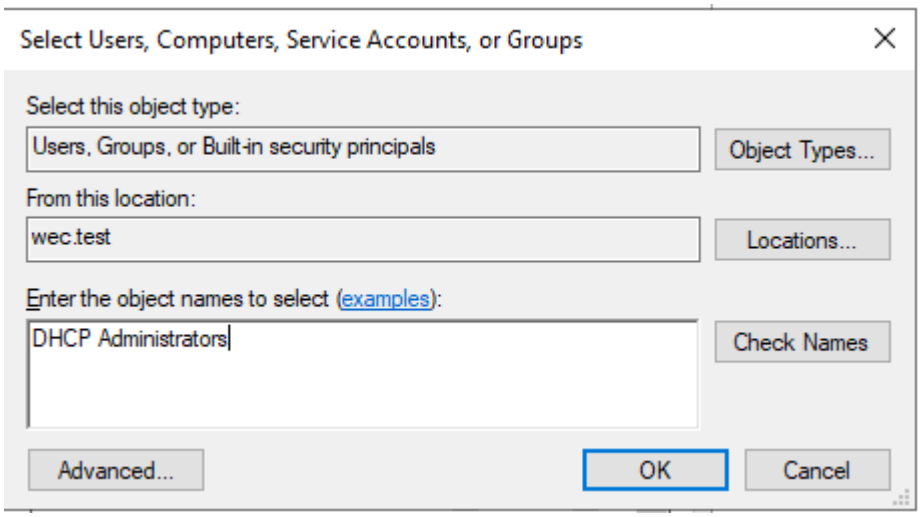
6. With DHCP highlighted, click **Security**.



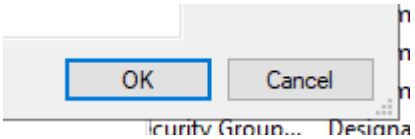
7. Click **Add** in the Security for ROOT\Microsoft\Windows\DHCP panel.



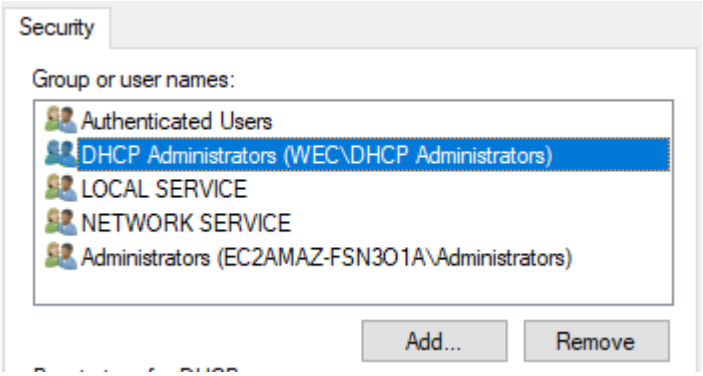
8. Type ***DHCP Administrators*** in the **Enter the object names to select** text field. Then, click **Check Names**.



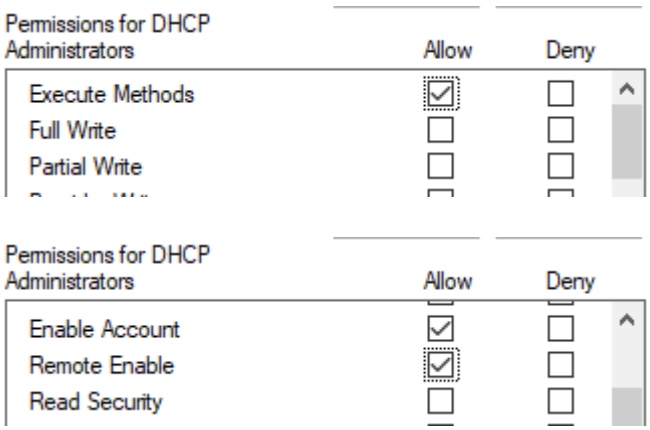
9. If DHCP Administrators is underlined, the appropriate group was located and selected. Click **OK**. ***Note:*** *If you are using a different user for the DHCP management use case, select that user instead of the DHCP Administrators group.*



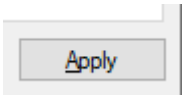
10. In the Security for ROOT\Microsoft\Windows\DHCP panel, select **DHCP Administrators** in the **Group or user names** field. ***Note:*** *If you selected a user instead of a user group, select that user instead.*



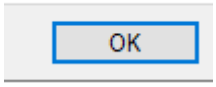
11. Click the **Allow** checkboxes associated with **Execute Methods** and **Remote Enable** in the **Permissions for DHCP Administrators** field.



12. Click **Apply**.



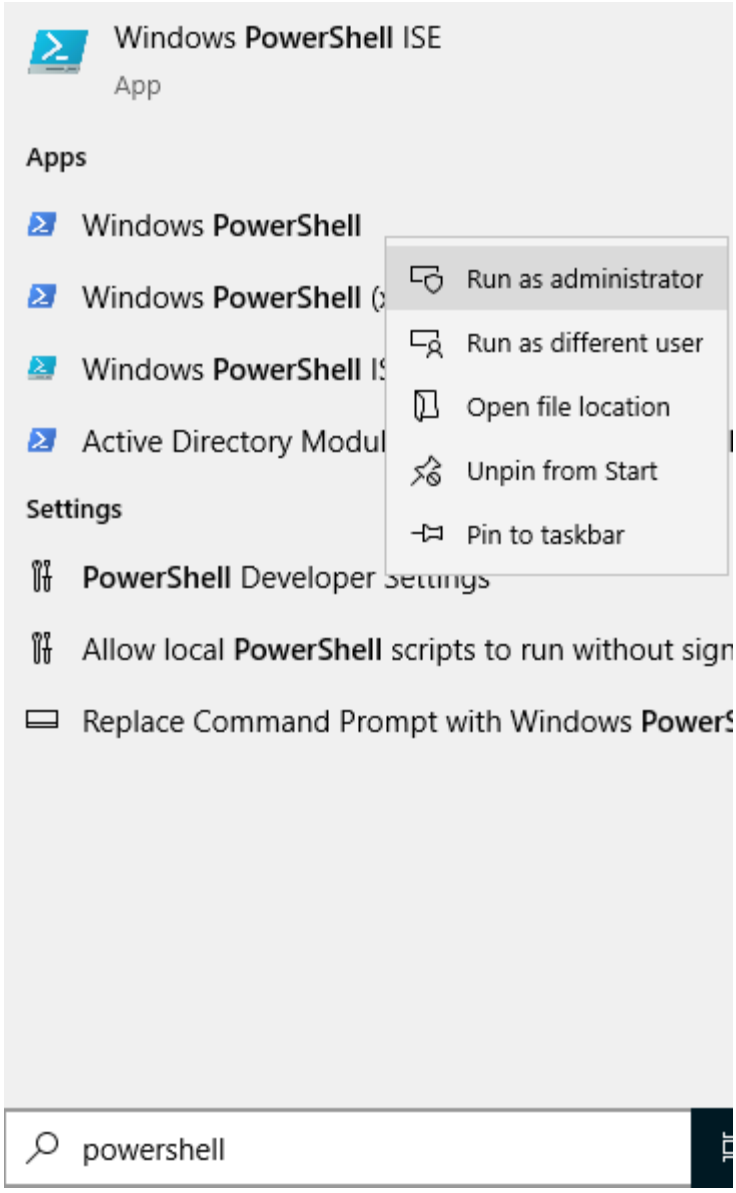
13. Click **OK**.



Enable WinRM and CredSSP on Each Domain Controller

Enable Windows Remote Management and Credential Security Support Provider Protocol on each Domain Controller and DHCP Server that will be managed by Infoblox via PowerShell commands.

1. To open an Elevated PowerShell console, search for ***PowerShell*** in the Windows search bar. Then, right-click **PowerShell** and click **Run as administrator.**



2. In the PowerShell window, input the following commands:

    a. Enable-PSRemoting -Force

```
PS C:\Windows\system32> Enable-PSRemoting -Force
```

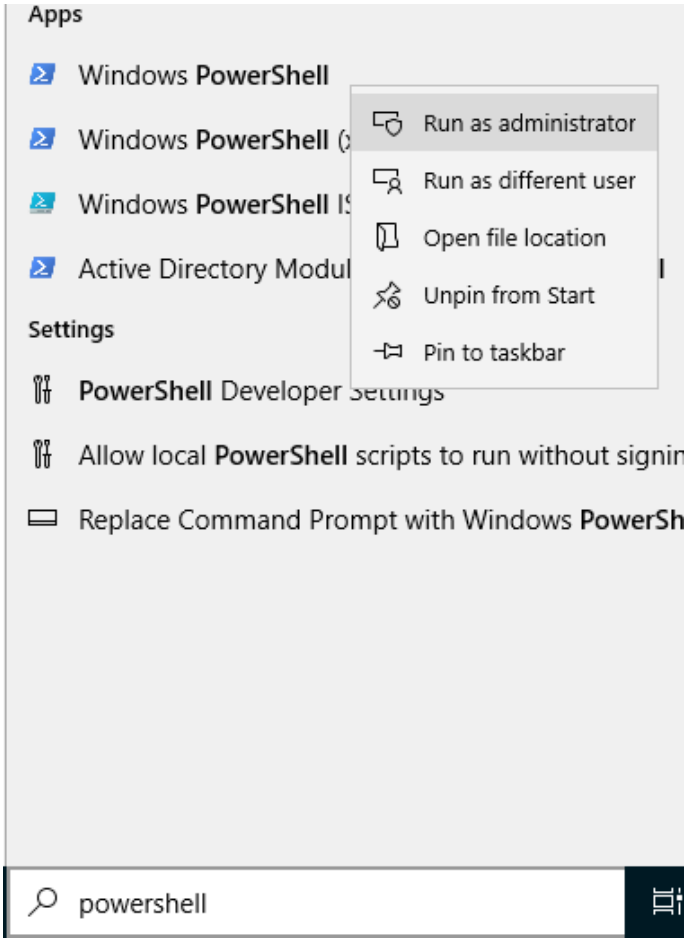
    b. Enable-WSManCredSSP -Role Server

```
PS C:\Windows\system32> Enable-WSManCredSSP -Role Server
```

Prepare the Windows Member Server for the DHCP Management Use Case

On the Windows Member server running the Universal DDI Agent for the DHCP management use case, PowerShell commands and Group Policy edits are required for the integration with Infoblox and Windows to work. To prepare the Windows Member server to manage Windows DHCP Servers, perform the following steps.

1. To open an Elevated PowerShell console, search for ***PowerShell*** in the Windows search bar. Then right-click **PowerShell** and click **Run as administrator.**



2. In the PowerShell Window, input the following commands (***Note:*** *As a reminder, these commands must be run on the Windows Member server running the Universal DDI Agent for the DHCP management use case. Replace the example IPs of "10.10.10.6,10.10.10.14" with the IPs of the DHCP servers you intend to manage with Infoblox. A single IP or multiple IPs delineated by commas may be used.):*

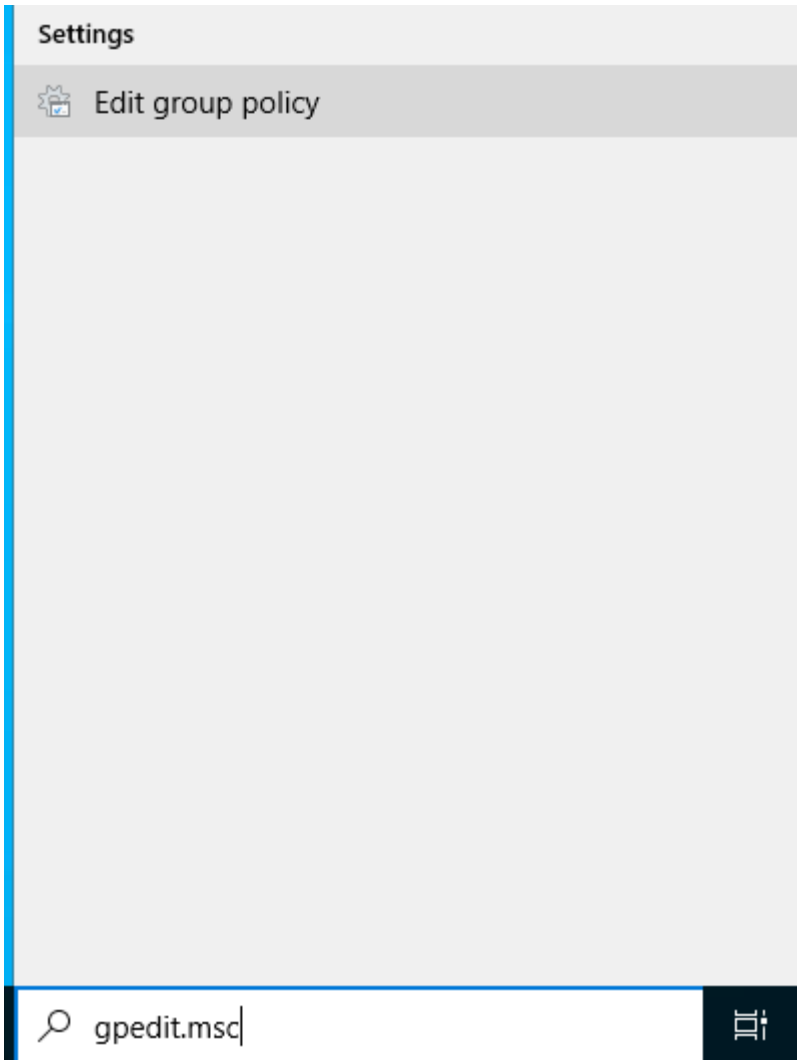
    a. Enable-WSManCredSSP -Role Client -DelegateComputer "10.10.10.6,10.10.10.14"

```
PS C:\Windows\system32> Enable-WSManCredSSP -Role Client -DelegateComputer "your-ip-here"
```

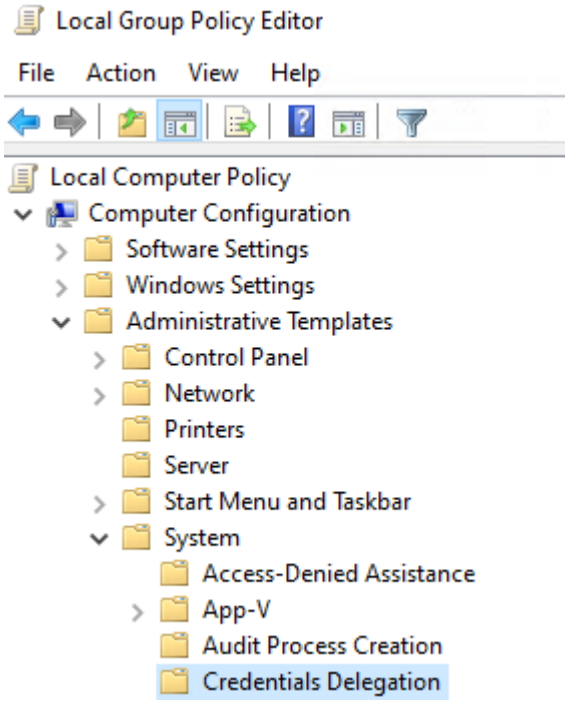
    b. Set-Item WSMan:\localhost\Client\TrustedHosts -Value "10.10.10.6,10.10.10.14"

```
PS C:\Windows\system32> Set-Item WSMan:\localhost\Client\TrustedHosts -Value "your-ip-here"
```

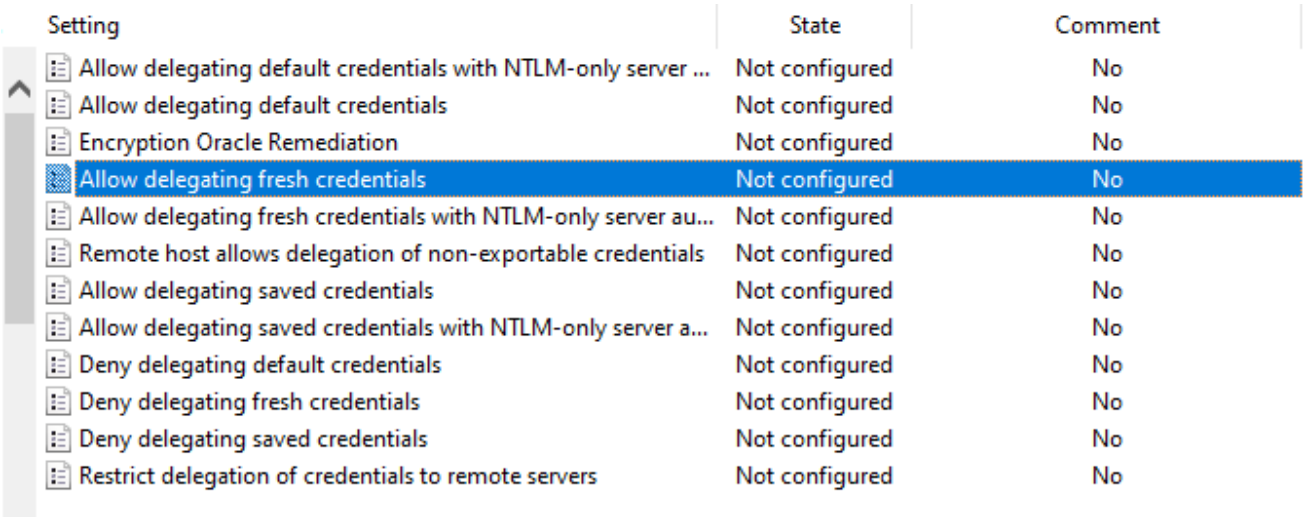
3. Open the **Local Group Policy Editor** by typing ***gpedit.msc*** in the Windows search bar and clicking **Edit group policy** in the search results.



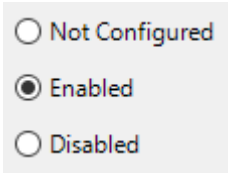
4. In the **Local Group Policy Editor**, navigate to **Computer Configuration → Administrative Templates → System → Credentials Delegation**.



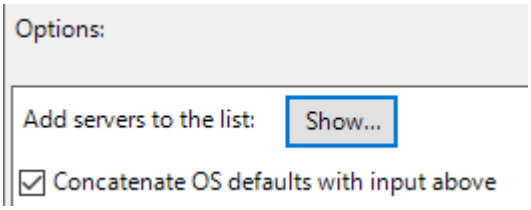
5. In the list of Credentials Delegation policies, double-click **Allow delegating fresh credentials**.



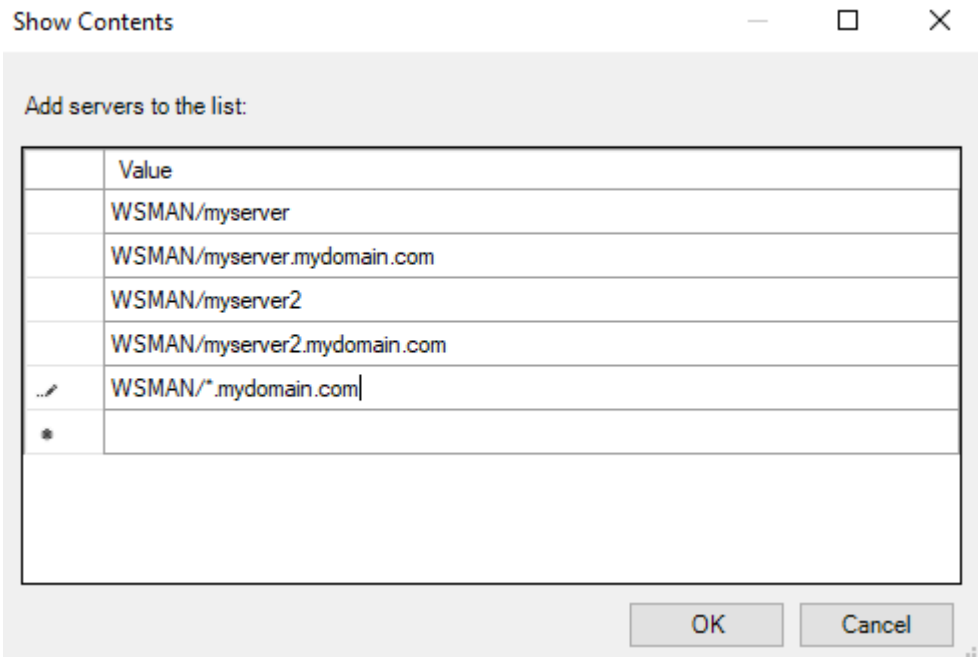
6. **Enable** the policy by clicking the **Enabled** bubble.



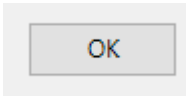
7. Click the **Show...** button in the **Options** table.



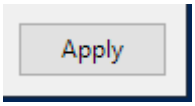
8. Input the following entries into the table of servers (***Note:*** *Replace the example text in the following entries with the appropriate information associated with your environment. The following text: <your-server-name> and <your-server-name>.<your-domain-name>.<tld>, and *.<your-domain-name>.<tld> must be replaced with the name of your DHCP server, proper domain of the DHCP server, and the top-level-domain that your domain is associated with. Additionally, include all DHCP servers you intend to manage with Infoblox.*):
    - WSMAN/<your-server-name>
    - WSMAN/<your-server-name>.<your-domain-name>.<tld>
    - WSMAN/*.<your-domain-name>.<tld>



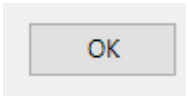
    - Click **OK** to confirm the addition of the servers.



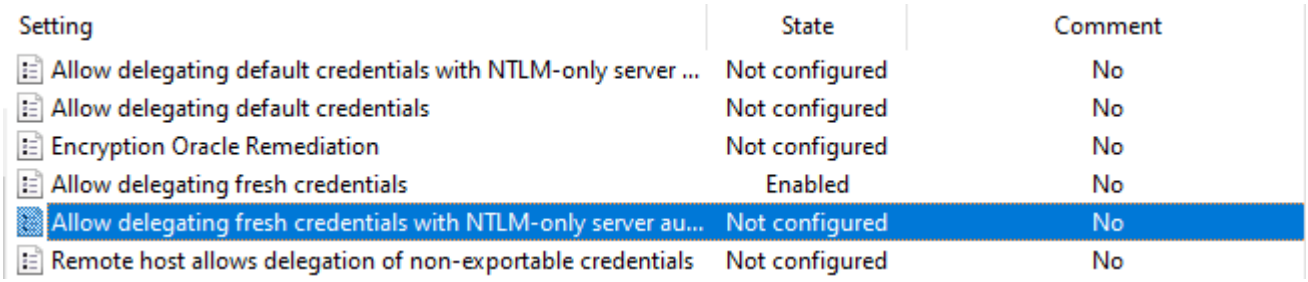
9. Click **Apply** to confirm the changes to the policy.



10. Click **OK**.

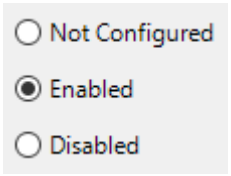


11. Double-click **Allow delegating fresh credentials with NTLM-only server authentication**.

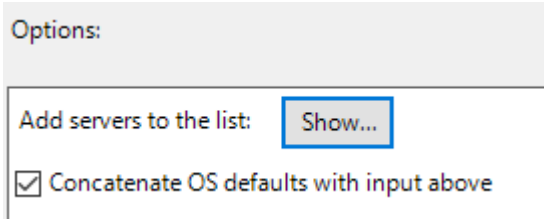


Setting	State	Comment
Allow delegating default credentials with NTLM-only server ...	Not configured	No
Allow delegating default credentials	Not configured	No
Encryption Oracle Remediation	Not configured	No
Allow delegating fresh credentials	Enabled	No
Allow delegating fresh credentials with NTLM-only server au...	Not configured	No
Remote host allows delegation of non-exportable credentials	Not configured	No

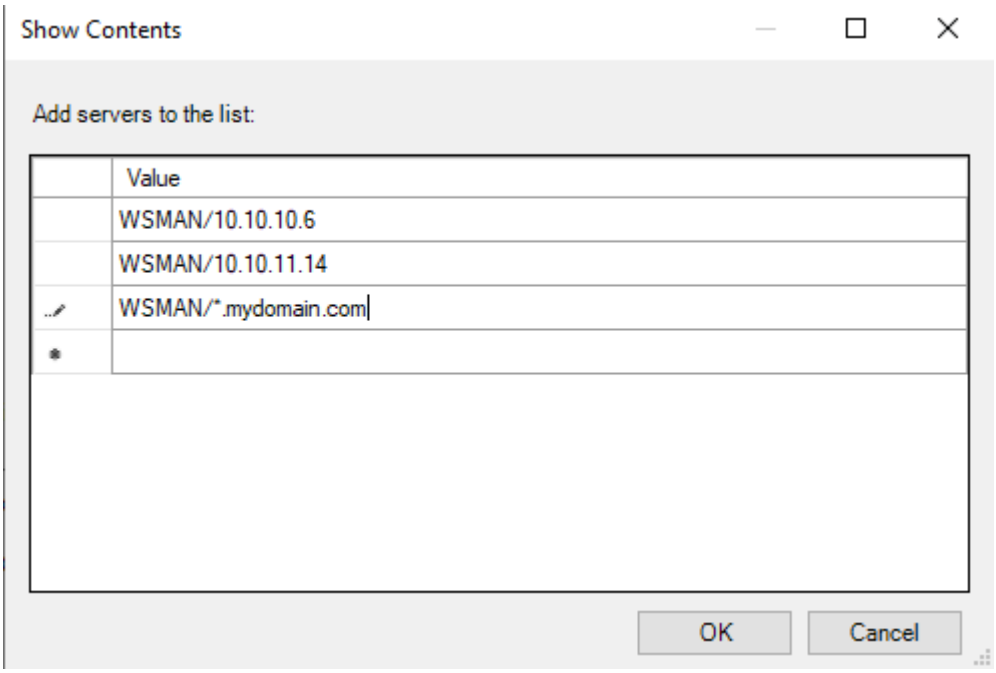
12. Enable the policy by clicking the **Enabled** bubble.



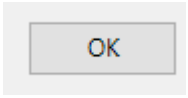
13. Click the **Show...** button in the **Options** table.



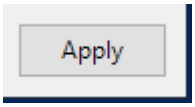
14. Input the following entries into the table of servers (***Note:*** *replace the example text in the following entries with the appropriate information associated with your environment. The following text: <IP-of-your-server> and *.<your-domain-name>.<tld> must be replaced with the IP of your DNS server, proper domain of the DNS server, and the top-level-domain that your domain is associated with. Additionally, include all DNS servers you intend to manage with Infoblox using the same format of WSMAN/<IP-of-your-server>. This step is only required if Kerberos is disabled in your environment, or if NTLM is preferred*):
    - WSMAN/<IP-of-your-server>
    - WSMAN/*.<your-domain-name>.<tld>



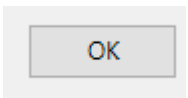
15. Click **OK** to confirm the addition of the servers.



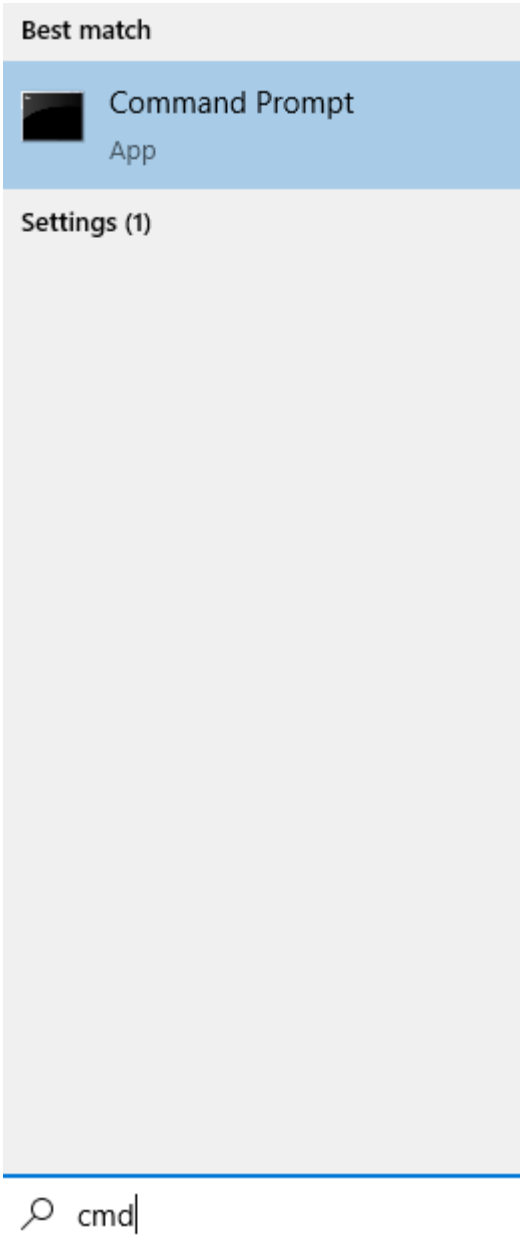
16. Click **Apply** to confirm the changes to the policy



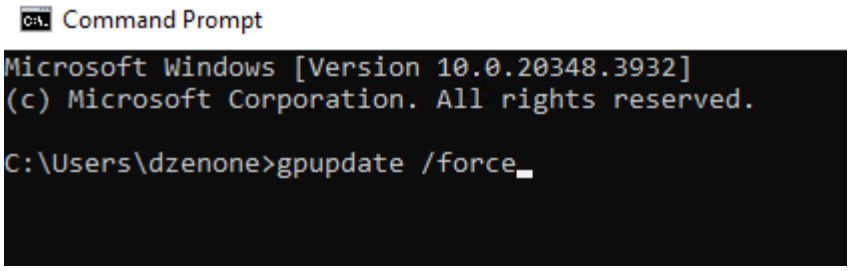
17. Click **OK**.



18. Open a **Command Prompt** window on the Windows Member server. Search for ***cmd*** in the Windows search bar and click **Command Prompt** in the search results.



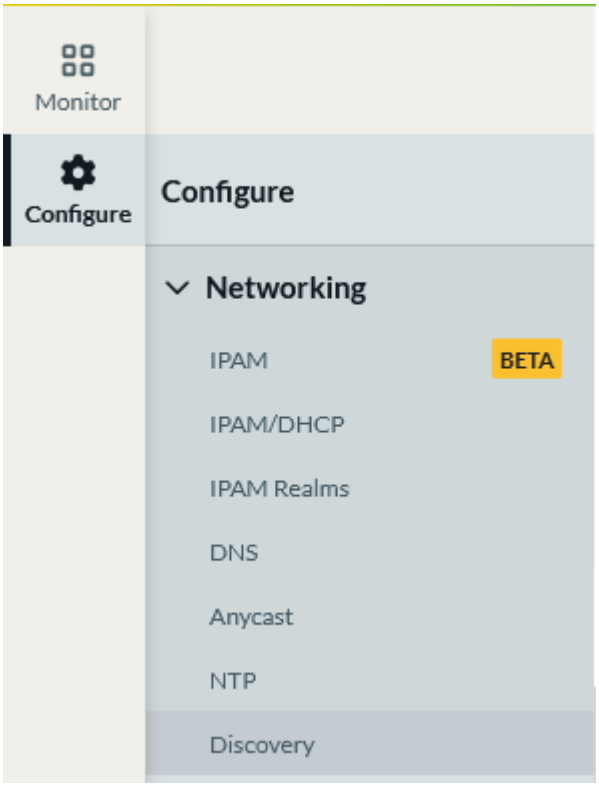
19. In the **Command Prompt** window, input the command **gpupdate /force**.



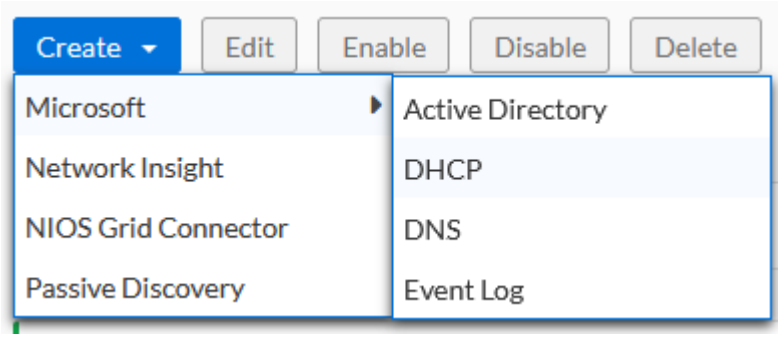
Create a DHCP Discovery Job

Once you have installed the Universal DDI Agent and created a Domain User for DHCP management, a Discovery Job can be created. To create a Discovery Job for DHCP management, perform the following steps:

1. Navigate to the **Discovery** page by highlighting **Configure**. Expand **Networking**, then click **Discovery** in the dropdown list.



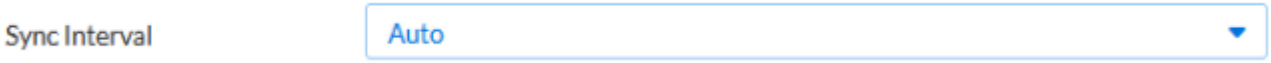
2. On the Discovery page, ensure that you are on the **On-Prem** tab. Click **Create**, highlight **Microsoft**, then click **DHCP** in the list.



3. In the **Create Discovery Job Configuration – Microsoft: DHCP panel**, ensure that the **State** toggle switch for the new Discovery Job is set to **Enabled**.

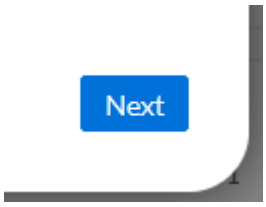
4. Input a name in the **Name** text field.

5. (Optional) Change the sync interval via the **Sync Interval** dropdown list. ***Note:*** *It is considered a best practice to keep the Sync Interval as* ***Auto****, which is 15 minutes.*

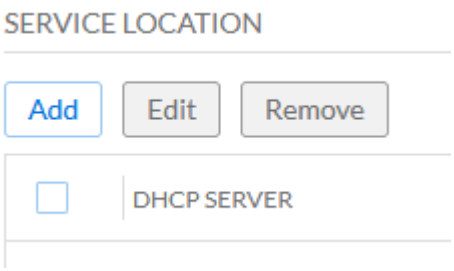


6. Select Read Only or Read/Write based on the desired state of the integration.

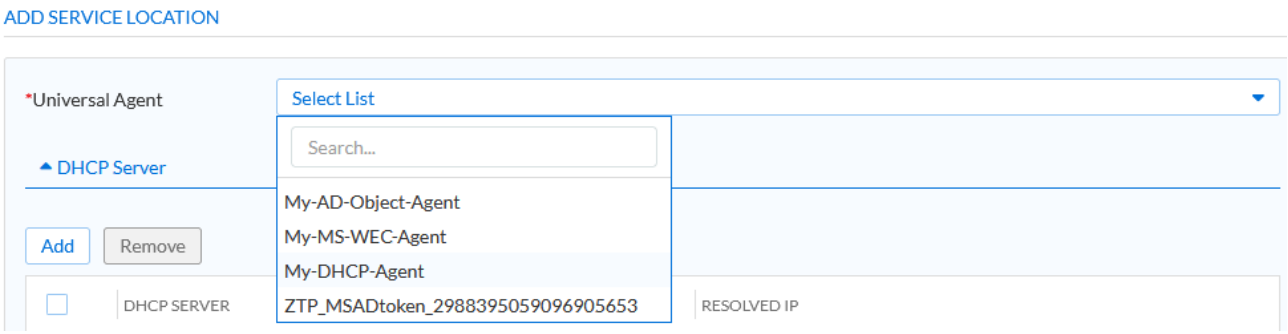
7. Click **Next**.



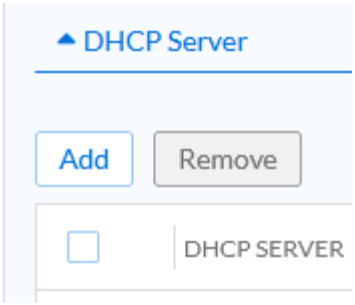
8. On the **SERVICE LOCATION** page, click **Add** to begin adding a Windows Server-based DHCP server to manage.



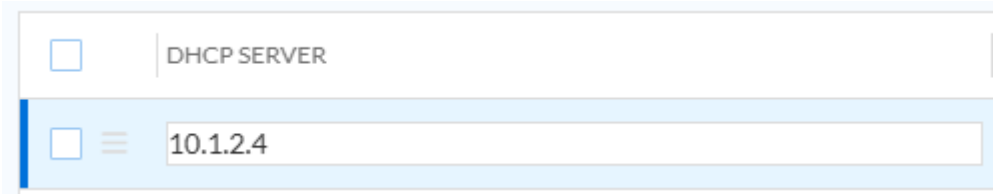
9. Select the appropriate Universal DDI Agent in the **Universal Agent** dropdown list.



10. Under the **DHCP Server** header, click **Add**.

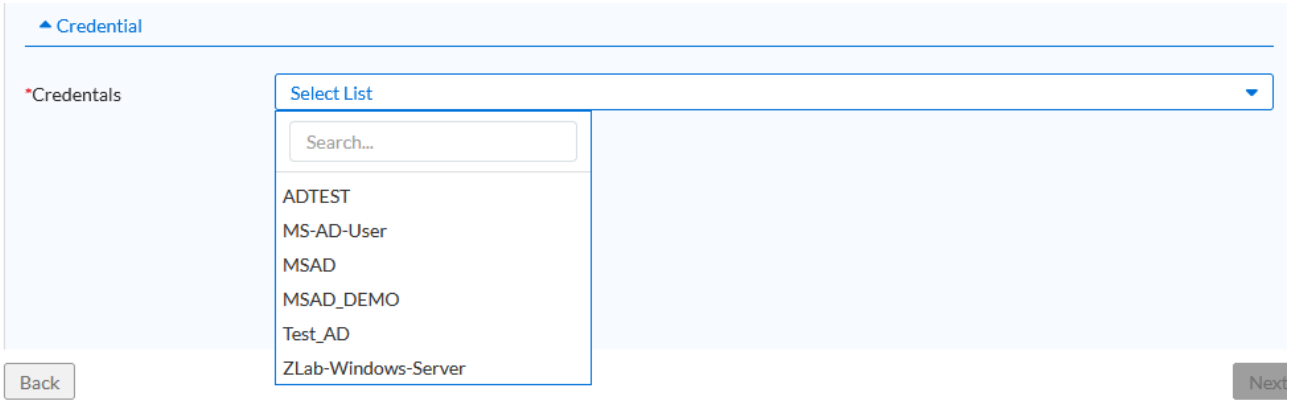


11. Input the IP of a Windows DHCP server.

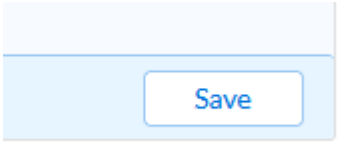


12. (Optional) Repeat steps 10-11 to add any additional DHCP servers you would like Infoblox to manage to the Discovery Job.

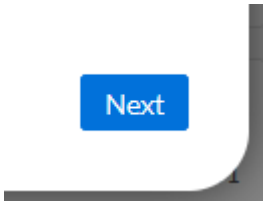
13. Under the **Credential** header, select the appropriate credentials via the **Credentials** dropdown list.



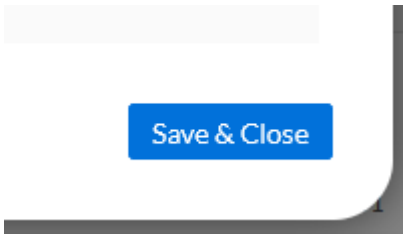
14. Click **Save.**



15. Click **Next**.



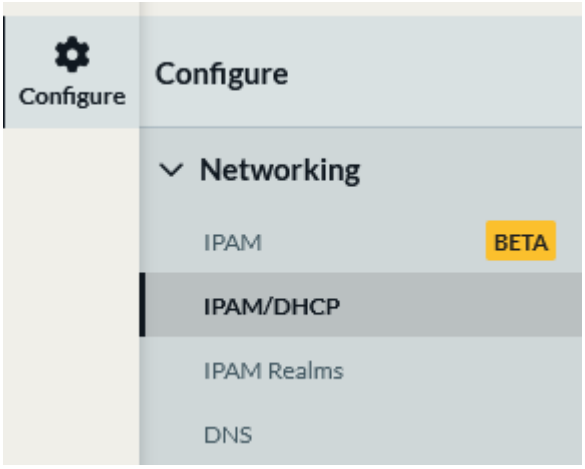
16. Click **Save & Close** to confirm the creation of the new Discovery Job.



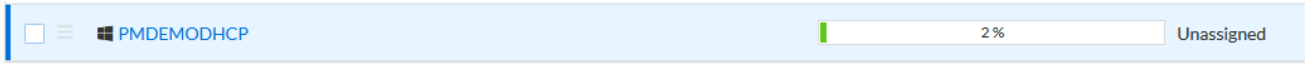
Managing Windows Server DHCP from the Infoblox Portal

To manage Windows Server-based DHCP objects from the Infoblox Portal, perform the following steps (***Note:*** *These steps are intended for a portal environment with a Read/Write DHCP Discovery Job configured*):

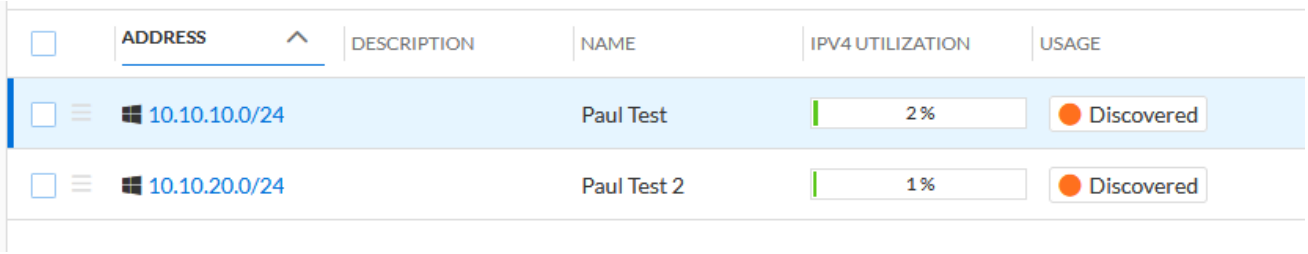
1. Navigate to the **IPAM/DHCP** page by highlighting **Configure**. Click **Networking**. Then, click **IPAM/DHCP** in the dropdown list.



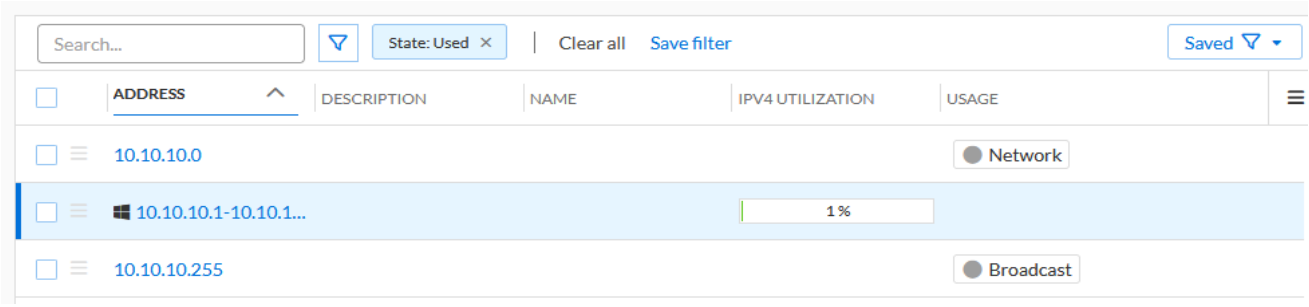
2. In the list of IP spaces, locate and **click** an IP space with the Windows icon associated with it.



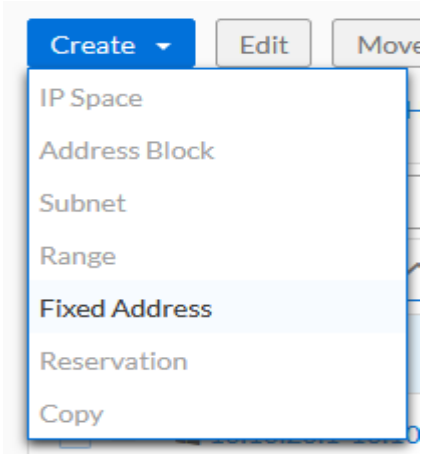
3. Inside will be networks that were synced via the agent. **Click** on a discovered network.



4. Inside will be a list of discovered DHCP objects, and other discovered network objects if they exist.



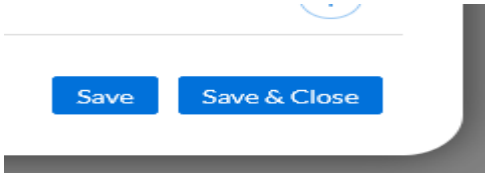
5. Click **Create**, then select **Fixed Address** in the dropdown list.



6. Input an appropriate IP address for this fixed address in the **IP Address** text field.

7. Input the MAC address of the device that will be using this address in the **MAC Address** text field.

8. Click **Save & Close** to confirm the creation of the fixed address.



Discovery Job for DNS Management

This section is intended to guide administrators through the creation of a Discovery Job for DNS management of Windows-based DNS. Discovery Jobs for DNS management can be configured as Read Only or Read/Write.

Create Credentials for DNS Management

To configure a Discovery Job to manage Windows-based DNS from the Infoblox Portal, credentials for an AD User must be added to the Infoblox Portal. The user(s) must be added to the appropriate AD groups and have the following permissions as listed below:

DNS Management:

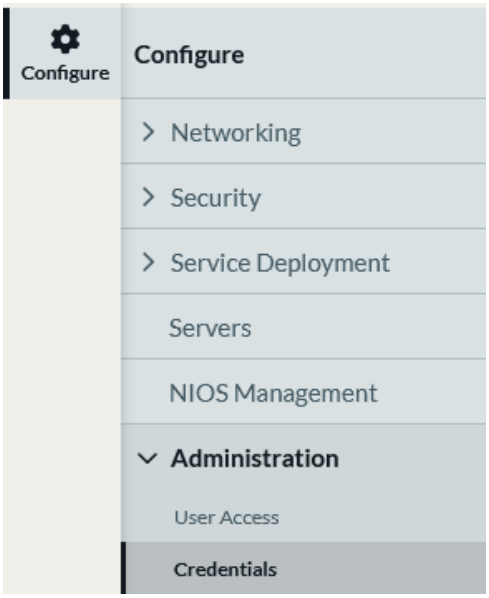
- DNS Admins
- Domain Users
- Remote Management Users

The following permissions must also be added in each instance where the DNS service is hosted on a Windows Member server:

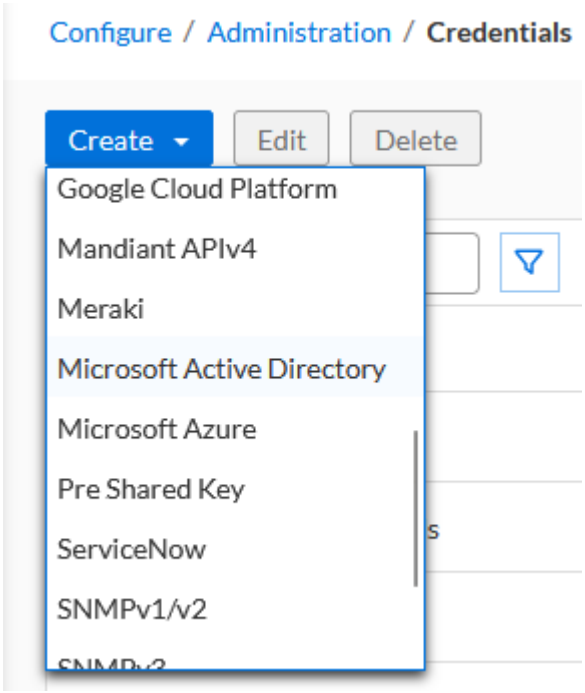
- Local Administrator (on the Windows Member server)
- Full control for the following registry entry: KEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\DNS Server

To add the user to the Infoblox Portal, perform the following steps:

1. Log in to the Infoblox Portal. Highlight **Configure**, expand **Administration**, and then click **Credentials** in the dropdown list.

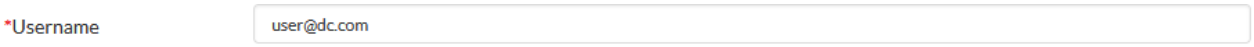


2. Click **Create** and then click **Microsoft Active Directory** in the dropdown list.



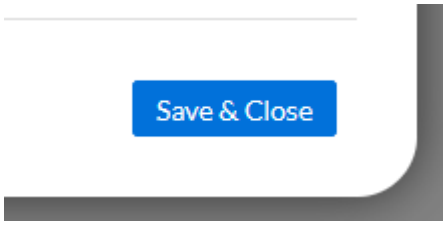
3. Input a **Name** for the Microsoft AD credentials.

4. Input a Microsoft AD User in the **Username** text field. ***Note:*** *This user must be in the DNS Admins built-in groups.*



5. Input the password associated with the AD User in the **Password** text field.

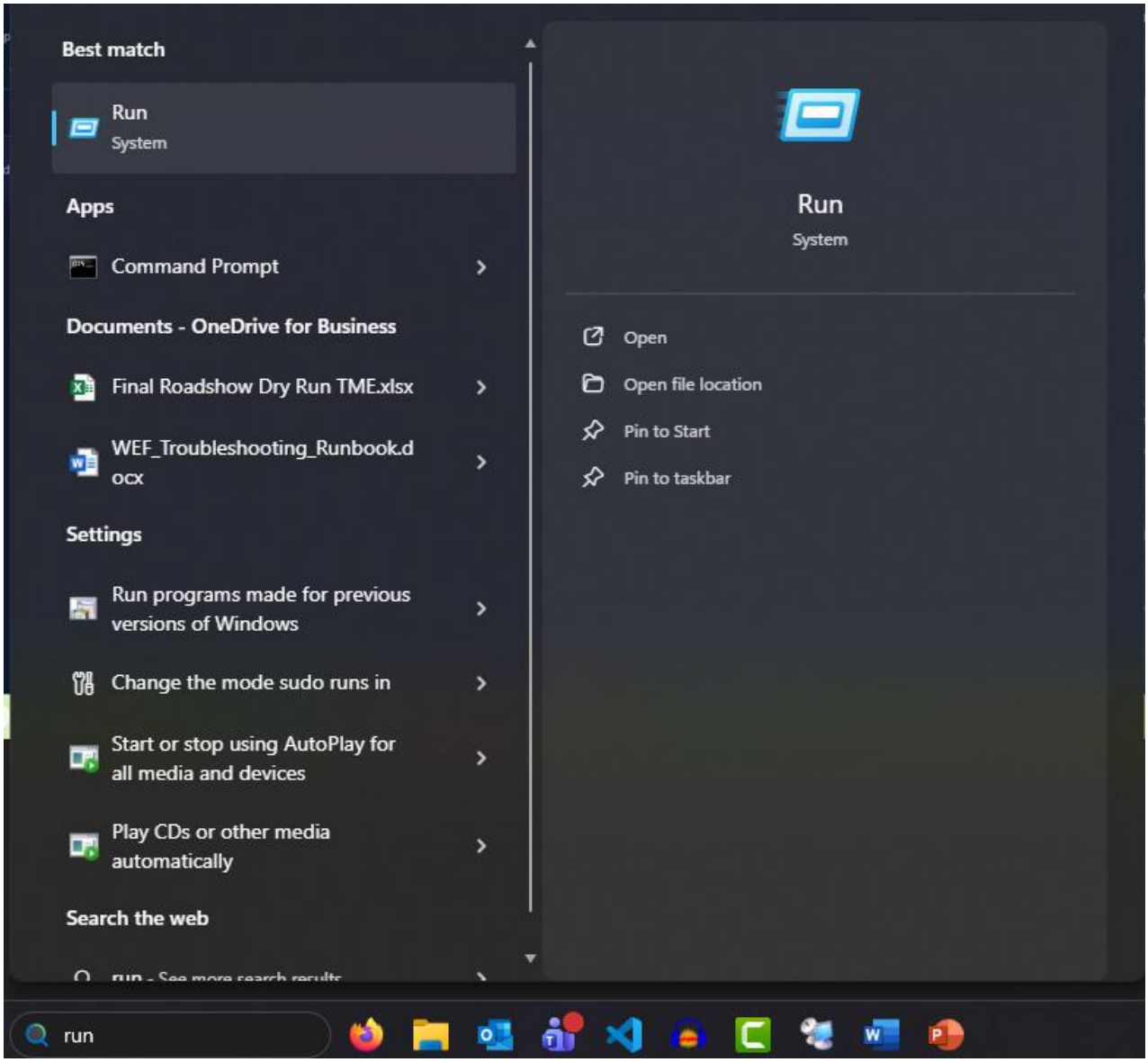
6. Click **Save & Close**.



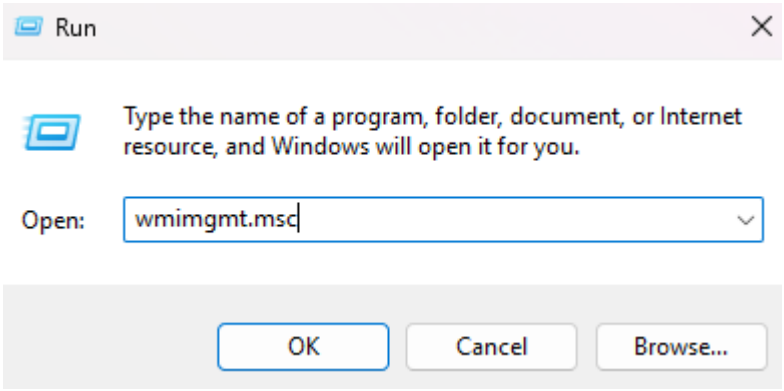
Configure WMI Permissions for DNS Namespace

On each Windows DNS server that will be managed by Infoblox, perform the following steps:

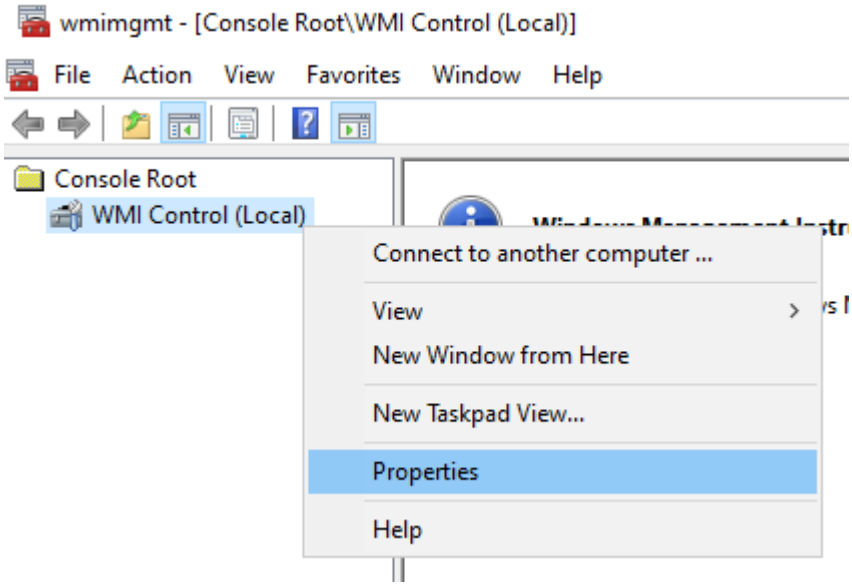
1. Access **Run** by searching for **Run** in the Windows search bar and clicking **Run**.



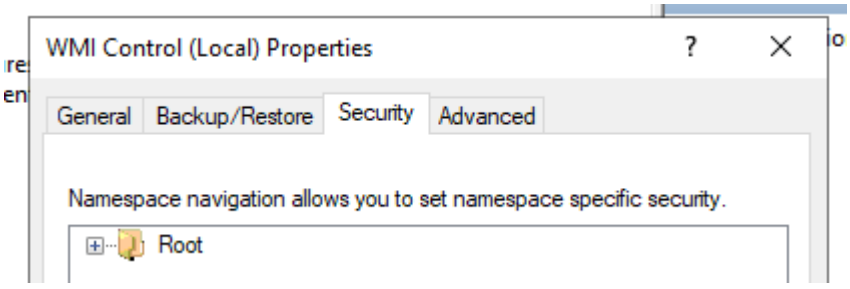
2. Run **wmimgmt.msc** by inputting **wimimgmt.msc** in the **Open** text field and clicking **OK**.



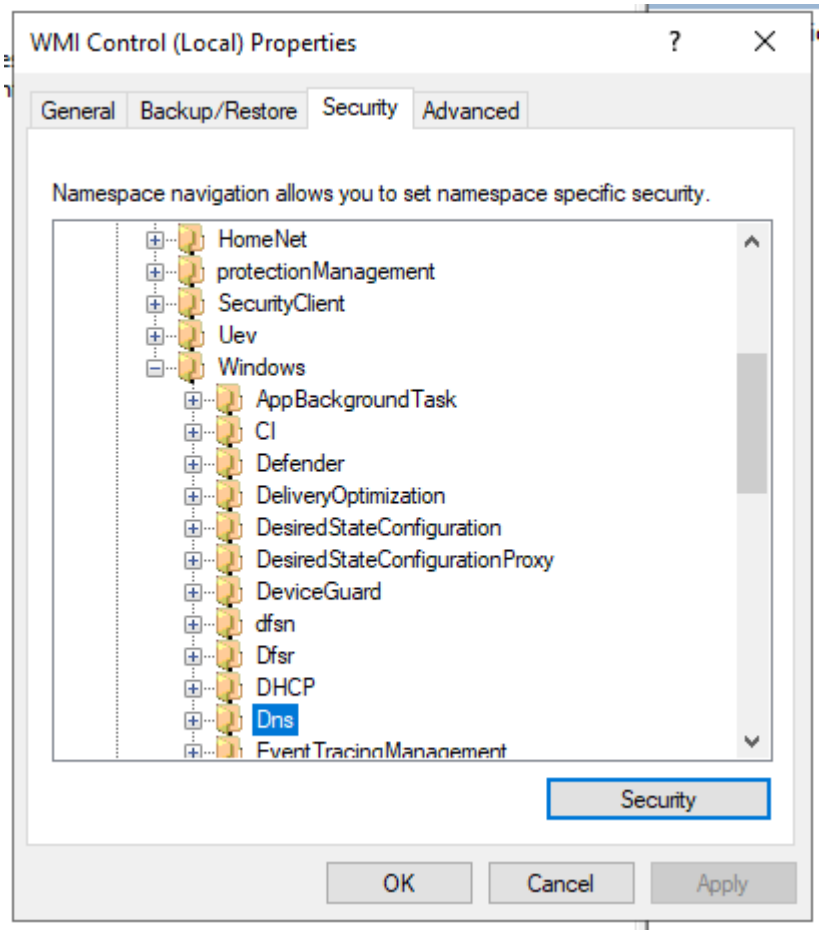
3. Right click **WMI Control (Local)**, then click **Properties**.



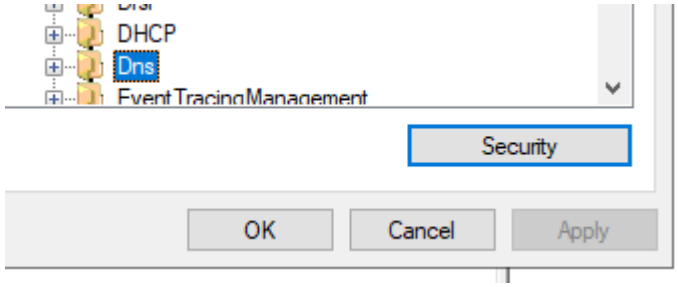
4. Click the **Security** tab in the **WMI Control (Local) Properties** panel.



5. Expand **Root** → **Microsoft** → **Windows**. Then, click **Dns** in the dropdown list.

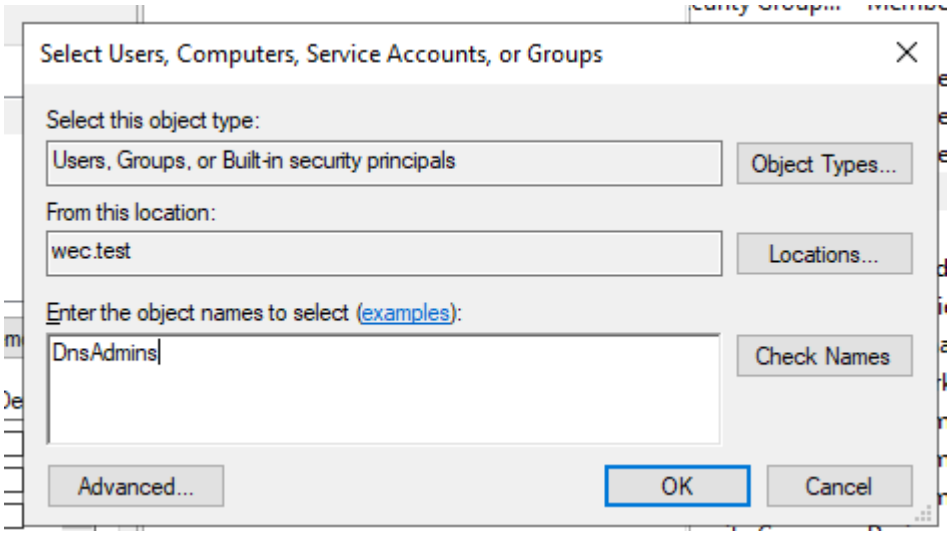


6. With Dns highlighted, click **Security**.

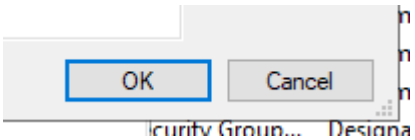


7. Click **Add** in the Security for ROOT\Microsoft\Windows\Dns panel.

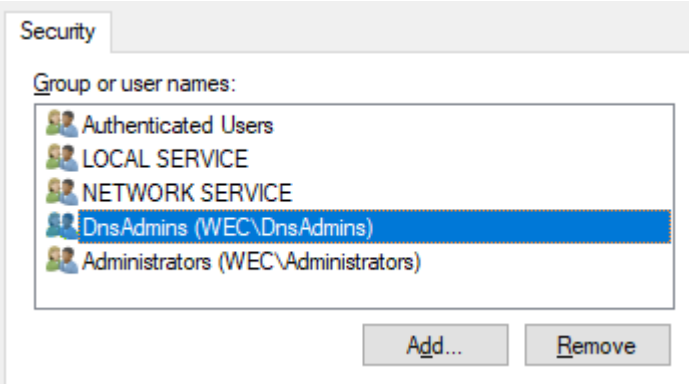
8. Type ***DnsAdmins*** in the **Enter the object names to select** text field. Then, click **Check Names**.



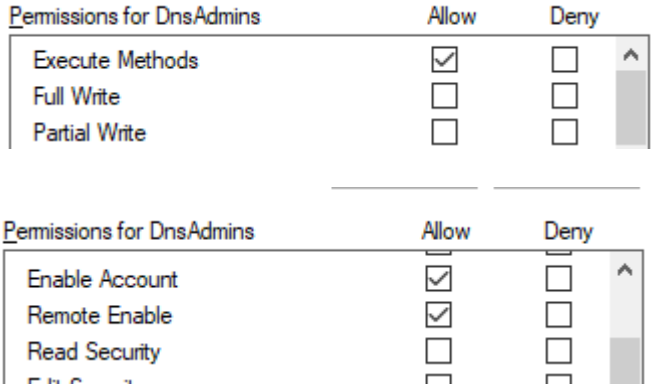
9. If DnsAdmins is underlined, the appropriate group was located and selected. Click **OK**. ***Note:*** *If you are using a different user for the DNS management use case, select that user instead of the DnsAdmins group.*



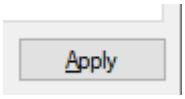
10. In the **Security for ROOT\Microsoft\Windows\Dns** panel, select **DNSAdmins** in the **Group or user names** field. ***Note:*** *If you selected a user instead of a user group, select that user instead.*



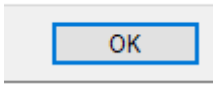
11. Click the **Allow** checkboxes associated with **Execute Methods** and **Remote Enable** in the **Permissions for DnsAdmins** field.



12. Click **Apply**.



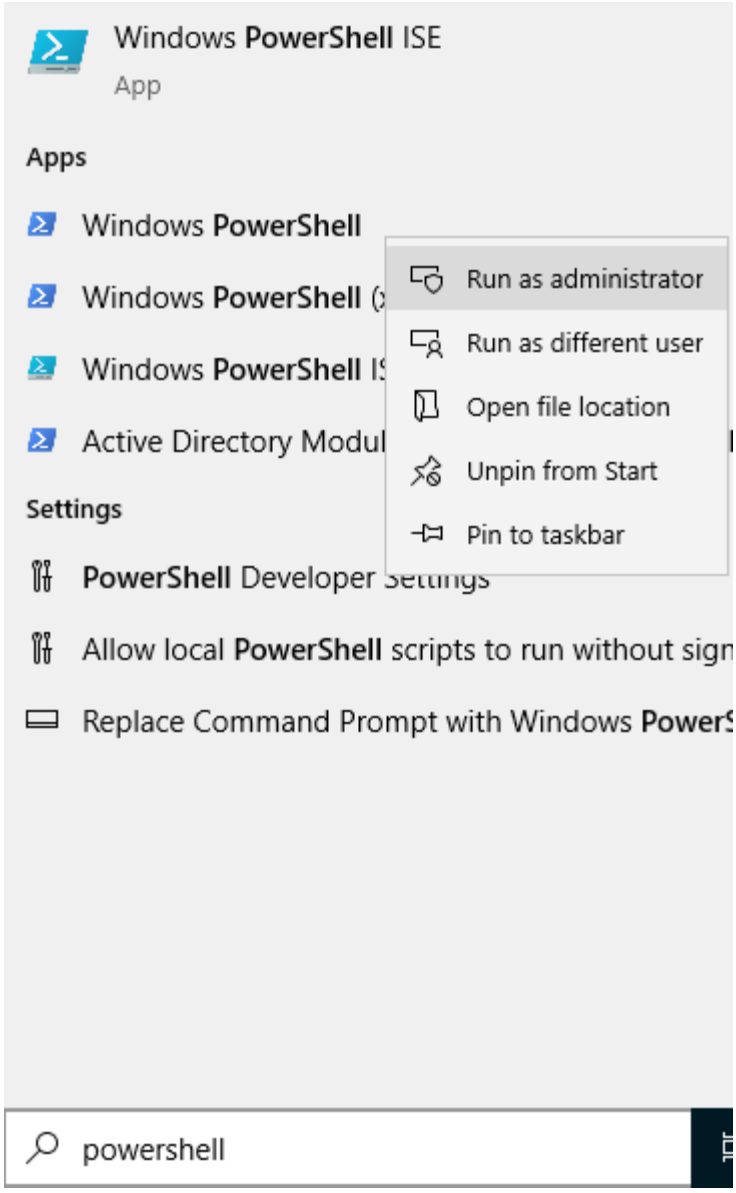
13. Click **OK**.



Enable WinRM and CredSSP on Each Domain Controller

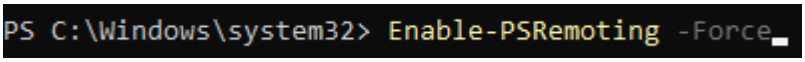
Enable Windows Remote Management and Credential Security Support Provider Protocol on each Domain Controller and DNS Server that will be managed by Infoblox via PowerShell commands.

1. To open an Elevated PowerShell console, search for ***PowerShell*** in the Windows search bar. Then, right-click **PowerShell** and click **Run as administrator.**

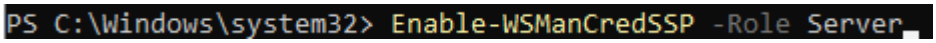


2. In the PowerShell window, input the following commands:

    c. Enable-PSRemoting -Force



    d. Enable-WSManCredSSP -Role Server



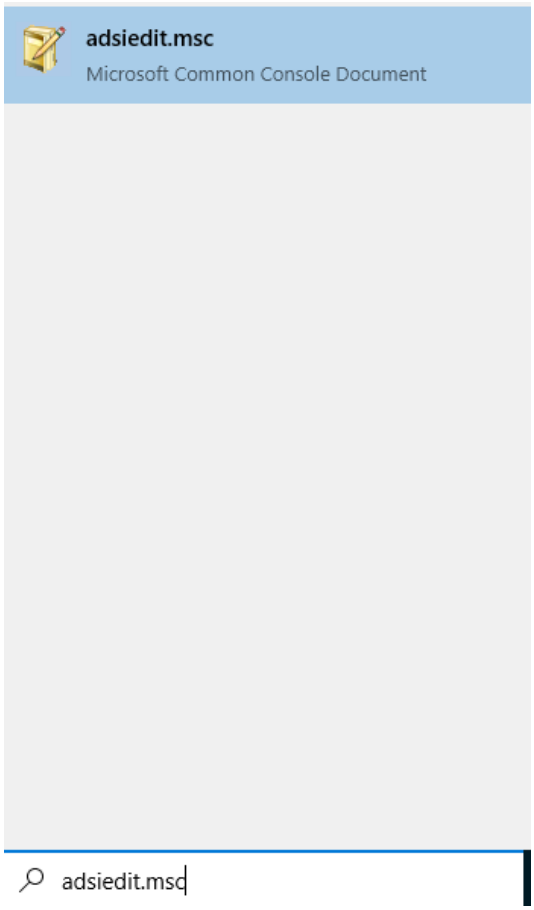
Assign Permissions for DNS Zone Management

The following section is only required if you intend to manage zones directly from the Infoblox Portal. If the intended configuration is read-only, skip to the following subheader.

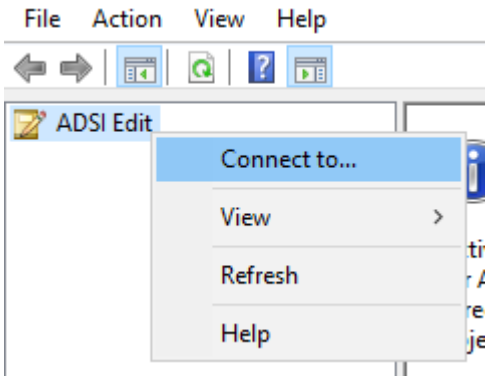
Please note this section utilizes ADSIEdit which directly modifies AD objects. Misconfiguration can affect DNS or AD replication. Proceed only if you are experienced with ADSIEdit and have a verified backup of your AD. Always make changes on a test or staging system before applying them in production.

To configure the permissions required for DNS zone management via the Infoblox Portal, perform the following steps on using a Windows account with Enterprise Admin rights on a Domain Controller.

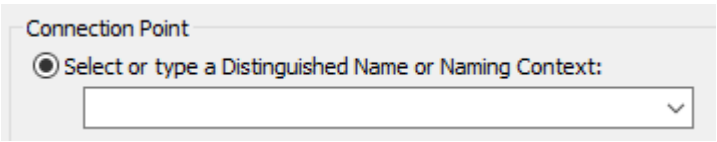
1. Open ADSIedit.msc by searching for **adsiedit.msc** in the Windows Search bar and clicking **adsiedit.msc** in the results.



2. In the ADSI Edit window, right-click **ADSI Edit**, then click **Connect to...**

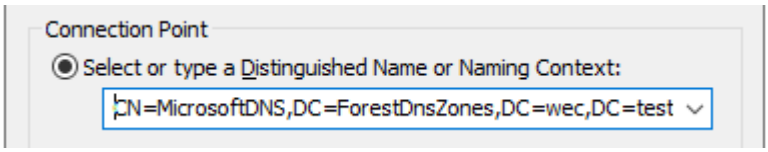


3. Click the **Select or type a Distinguished Name or Naming Context** bubble under the **Connection Point** header. Change DC, could have multiple DCs and TLD to appropriate info.

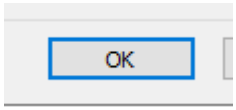


4. Input the following distinguished name. ***Note:*** *Change the text yourdomain and com to the appropriate domain and top-level domain that matches your environment. If your domain has multiple subdomains add those into the distinguished name using the same format of DC=<your-subdomain-here> with no whitespace and delineate with a comma.*

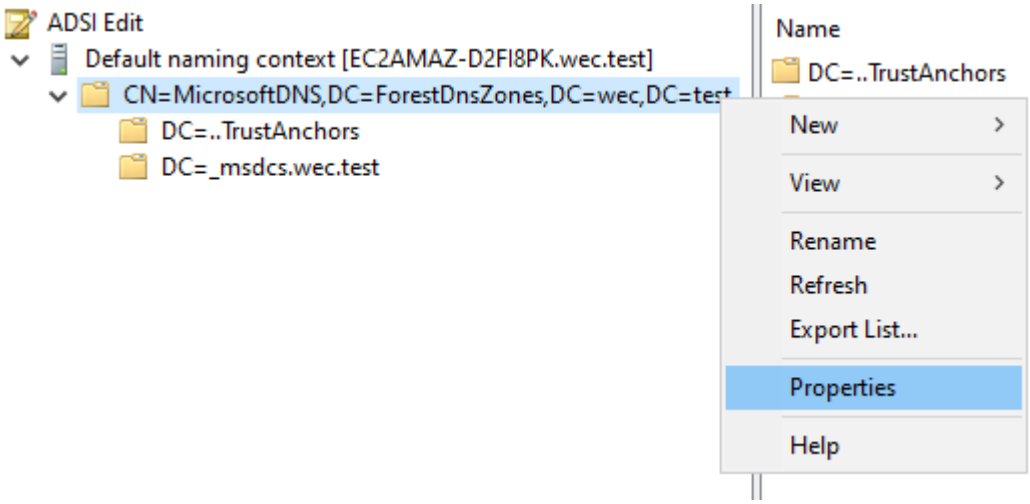
    a. CN=MicrosoftDNS,DC=ForestDnsZones,DC=yourdomain,DC=com



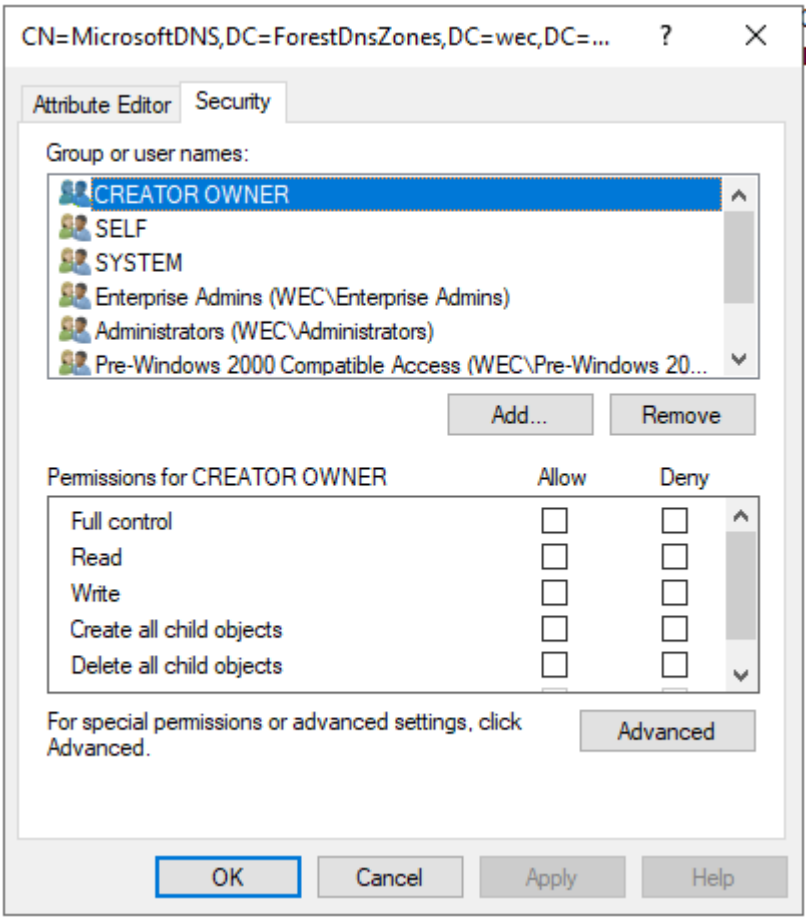
    b. Click **OK**.



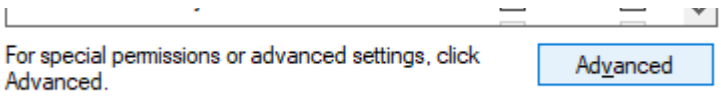
5. In the left panel, right-click the distinguished name that was input. Then, click **Properties**.



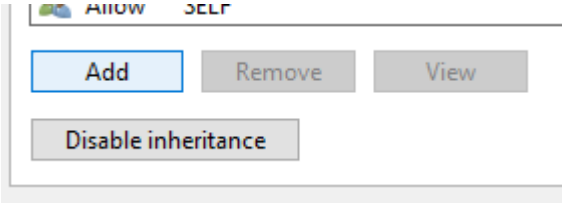
6. In the window that is revealed, click the **Security** tab.



7. Near the bottom of the panel, click **Advanced**.

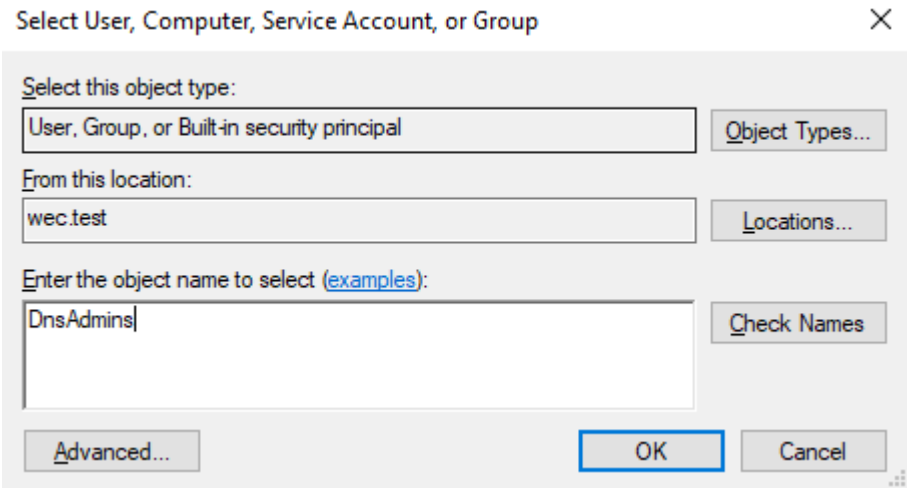


8. Under the table of permission entries click **Add**.

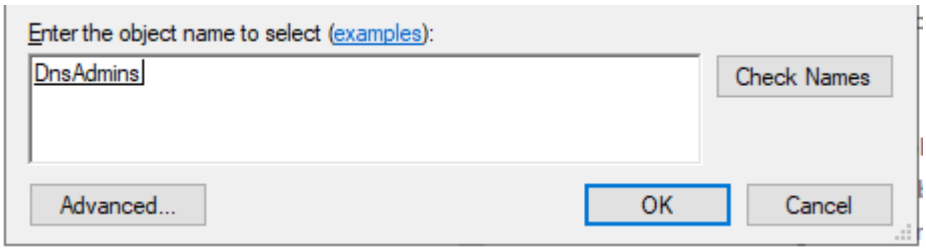


9. In the **Permission Entry for MicrosoftDNS** window click **Select a principal**.

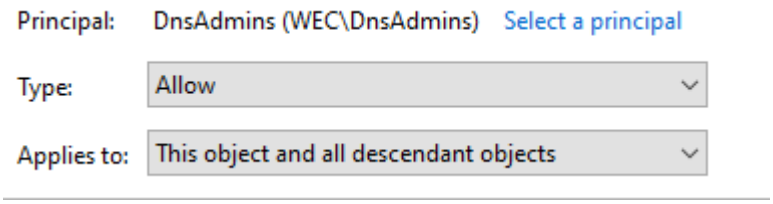
10. Search for the DnsAdmins built-in group, or a service user within the DnsAdmins group. Input the correct username or group in the **Enter the object name to select** field. Then click **Check Names** via the **Select User, Computer, Service Account, or Group** panel.



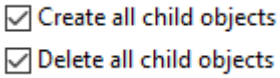
11. If the name becomes underlined the user or user group has been found. Click **OK**.



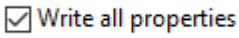
12. Validate that the principal is correct, the type is **Allow**, and the **Applies to** field shows **This object and all descendant objects**.



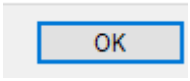
13. In the list of Permissions, click the checkboxes associated with **Create all child objects** and **Delete all child objects**.



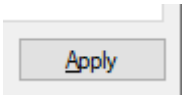
14. Additionally, in the list of permissions validate that **Write all properties** has been checked.



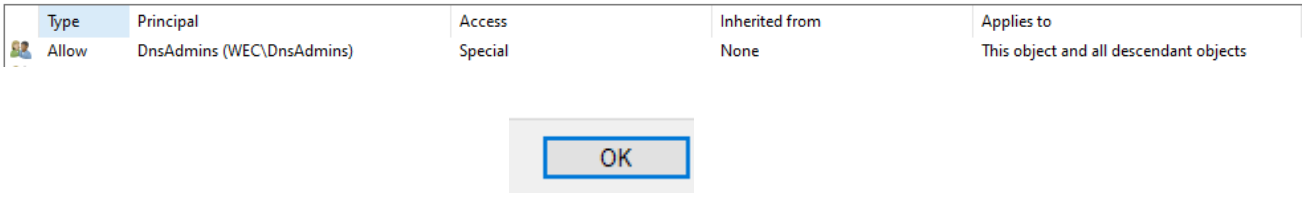
15. Click **OK**.



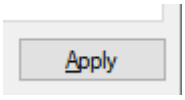
16. Click **Apply**.



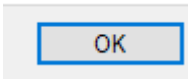
17. Wait for the new Permission entry to populate. ***Note:*** *This process may take a while if your environment contains a large quantity of records and zones*. Once the new Permission entry has populated, click **OK**.



18. Click **Apply**.



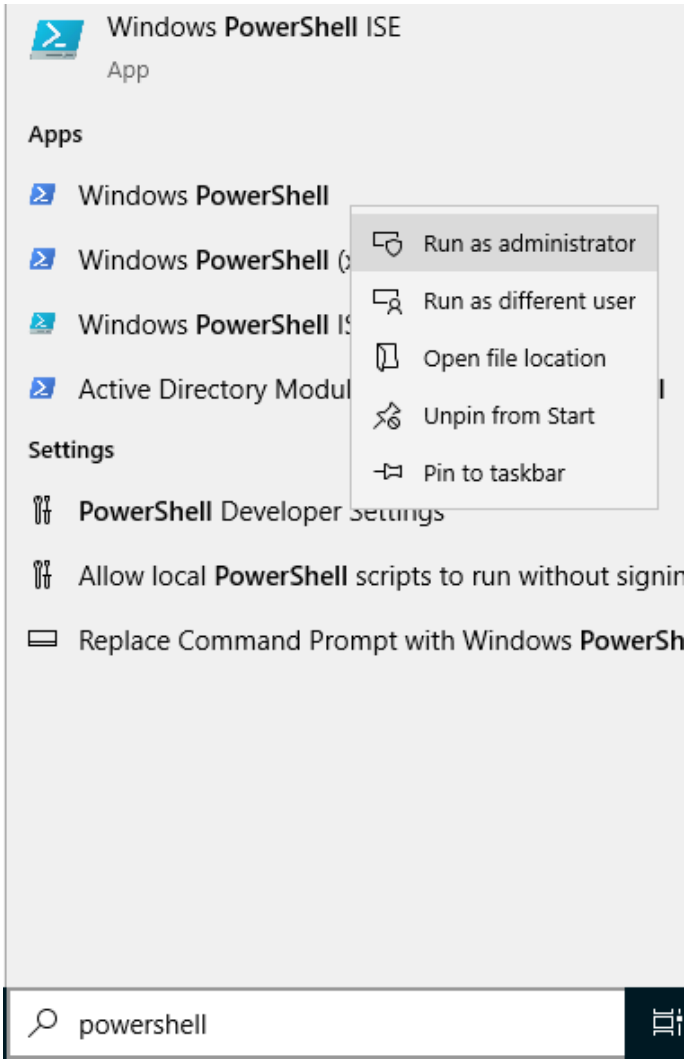
19. Click **OK**.



Prepare the Windows Member Server for the DNS Management Use Case

On the Windows Member server running the Universal DDI Agent for the DNS management use case, PowerShell commands and Group Policy edits are required for the integration with Infoblox and Windows to work. To prepare the Windows Member server to manage Windows DNS Servers, perform the following steps.

1. To open an Elevated PowerShell console, search for ***PowerShell*** in the Windows search bar. Then, right-click **PowerShell** and click **Run as administrator.**



2. In the PowerShell Window, input the following commands (***Note:*** *As a reminder, these commands must be run on the Windows Member server running the Universal DDI Agent for the DNS management use case. Replace the example IPs of "10.10.10.6,10.10.10.14" with the IPs of the DNS servers you intend to manage with Infoblox. A Single IP or multiple IPs delineated by commas may be used.):*

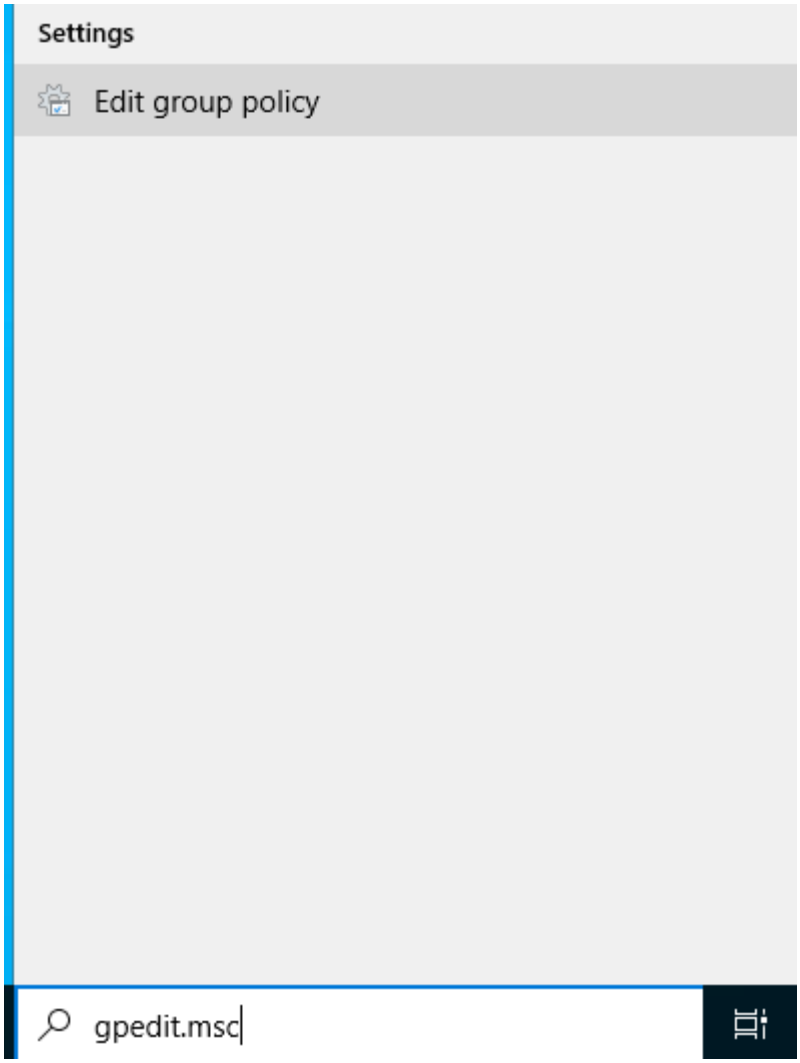
   - Enable-WSManCredSSP -Role Client -DelegateComputer "10.10.10.6,10.10.10.14"

```
PS C:\Windows\system32> Enable-WSManCredSSP -Role Client -DelegateComputer "your-ip-here"
```

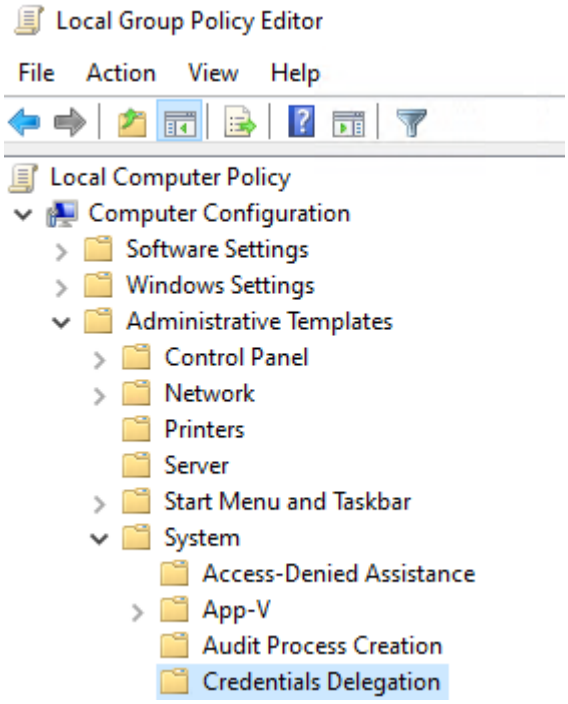
   - Set-Item WSMan:\localhost\Client\TrustedHosts -Value "10.10.10.6,10.10.10.14"

```
PS C:\Windows\system32> Set-Item WSMan:\localhost\Client\TrustedHosts -Value "your-ip-here"
```

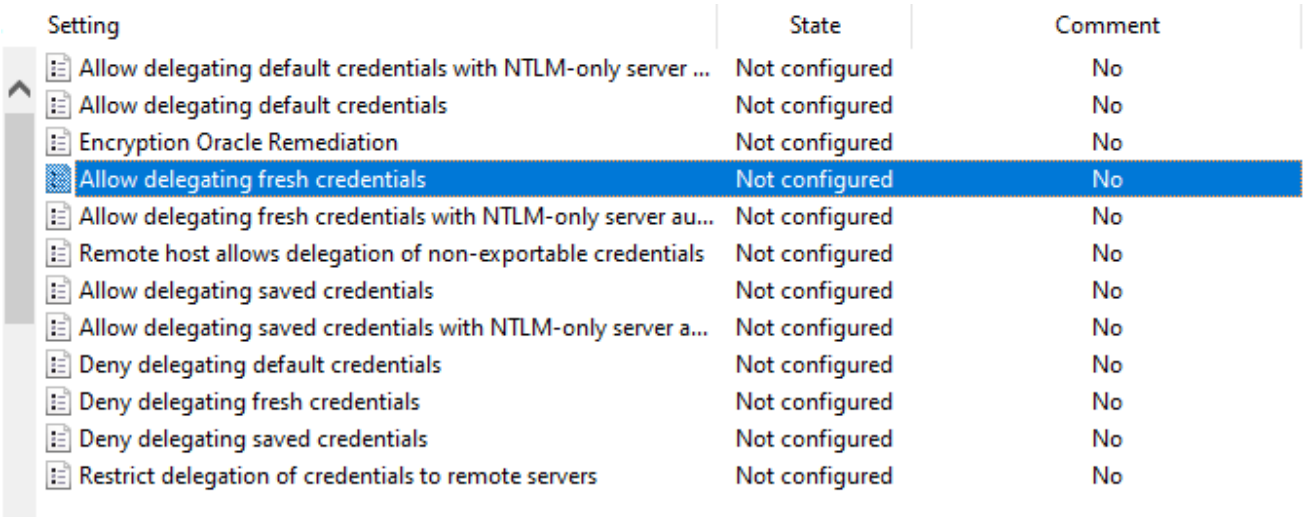
3. Open the **Local Group Policy Editor** by typing ***gpedit.msc*** in the Windows search bar. Then, click **Edit group policy** in the search results.



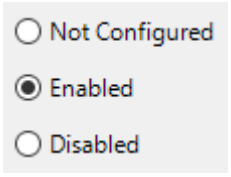
4. In the Local Group Policy Editor, navigate to **Computer Configuration** → **Administrative Templates** → **System** → **Credentials Delegation**.



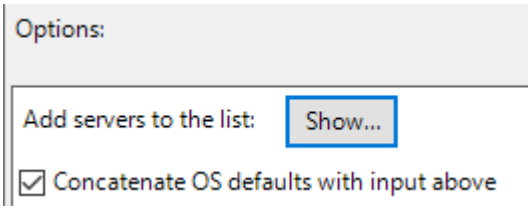
5. In the list of Credentials Delegation policies, double-click **Allow delegating fresh credentials**.



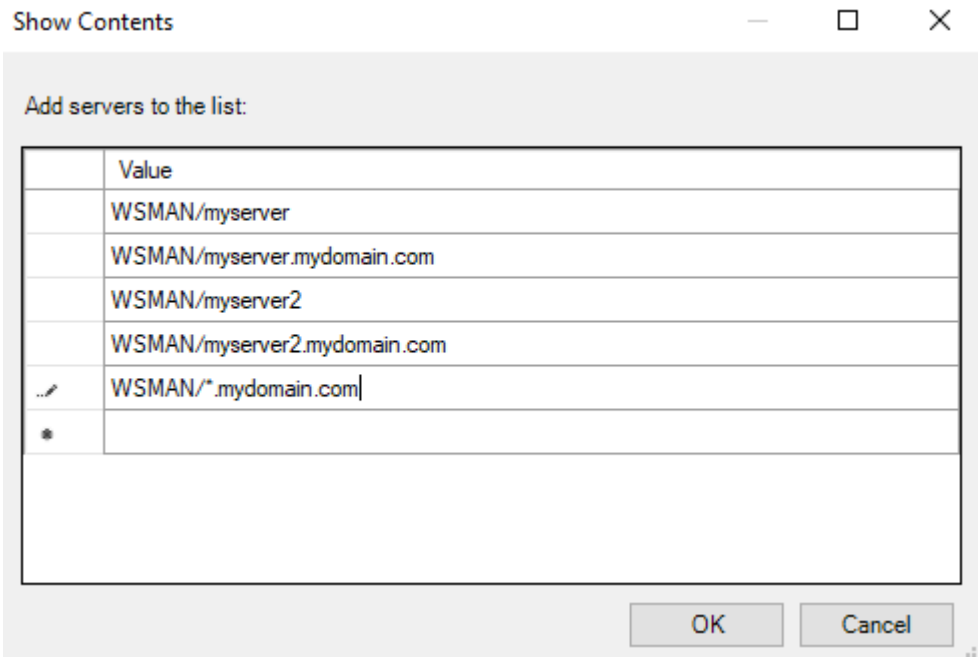
6. Enable the policy by clicking the **Enabled** bubble.



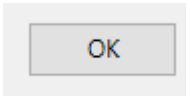
7. Click the **Show...** button in the **Options** table.



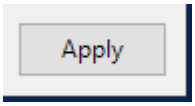
8. Input the following entries into the table of servers (***Note:*** *Replace the example text in the following entries with the appropriate information associated with your environment. The following text: <your-server-name> and <your-server-name>.<your-domain-name>.<tld>, and *.<your-domain-name>.<tld> must be replaced with the name of your DNS server, proper domain of the DNS server, and the top-level-domain that your domain is associated with. Additionally, include all DNS servers you intend to manage with Infoblox.*):
    - WSMAN/<your-server-name>
    - WSMAN/<your-server-name>.<your-domain-name>.<tld>
    - WSMAN/*.<your-domain-name>.<tld>



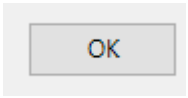
    - Click **OK** to confirm the addition of the servers.



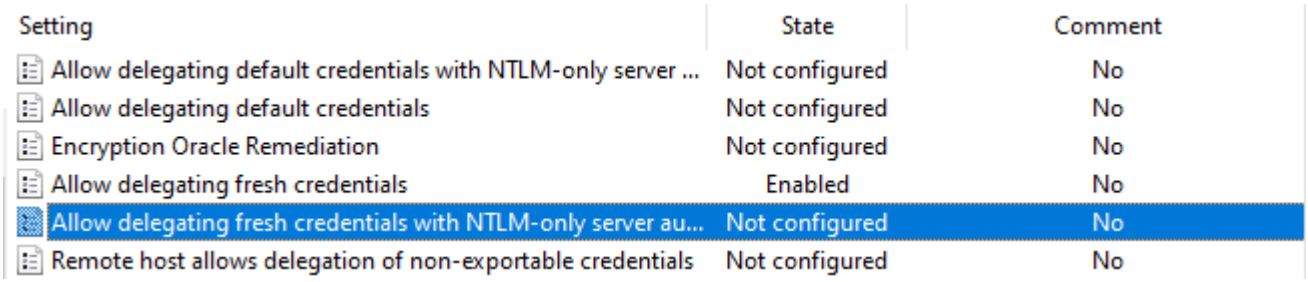
9. Click **Apply** to confirm the changes to the policy.



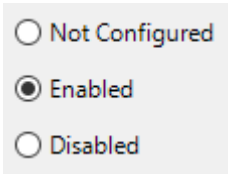
10. Click **OK**.



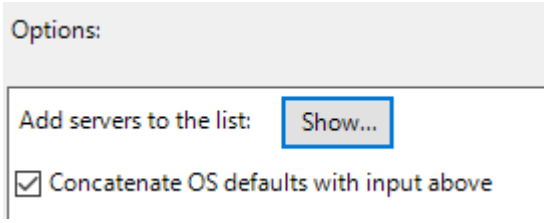
11. Double-click **Allow delegating fresh credentials with NTLM-only server authentication**.



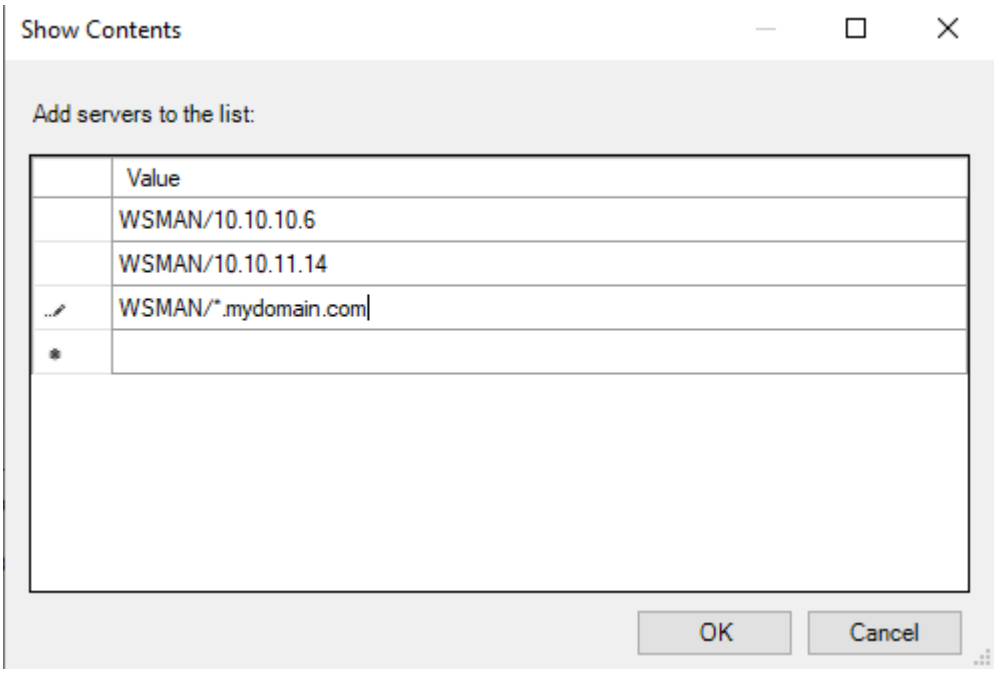
12. Enable the policy by clicking the **Enabled** bubble.



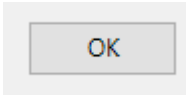
13. Click the **Show...** button in the **Options** table.



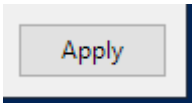
14. Input the following entries into the table of servers (***Note:*** *Replace the example text in the following entries with the appropriate information associated with your environment. The following text: <IP-of-your-server> and *.<your-domain-name>.<tld> must be replaced with the IP of your DNS server, proper domain of the DNS server, and the top-level-domain that your domain is associated with. Additionally, include all DNS servers you intend to manage with Infoblox using the same format of WSMAN/<IP-of-your-server>. This step is only required if Kerberos is disabled in your environment, or if NTLM is preferred*):
    - WSMAN/<IP-of-your-server>
    - WSMAN/*.<your-domain-name>.<tld>



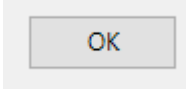
15. Click **OK** to confirm the addition of the servers.



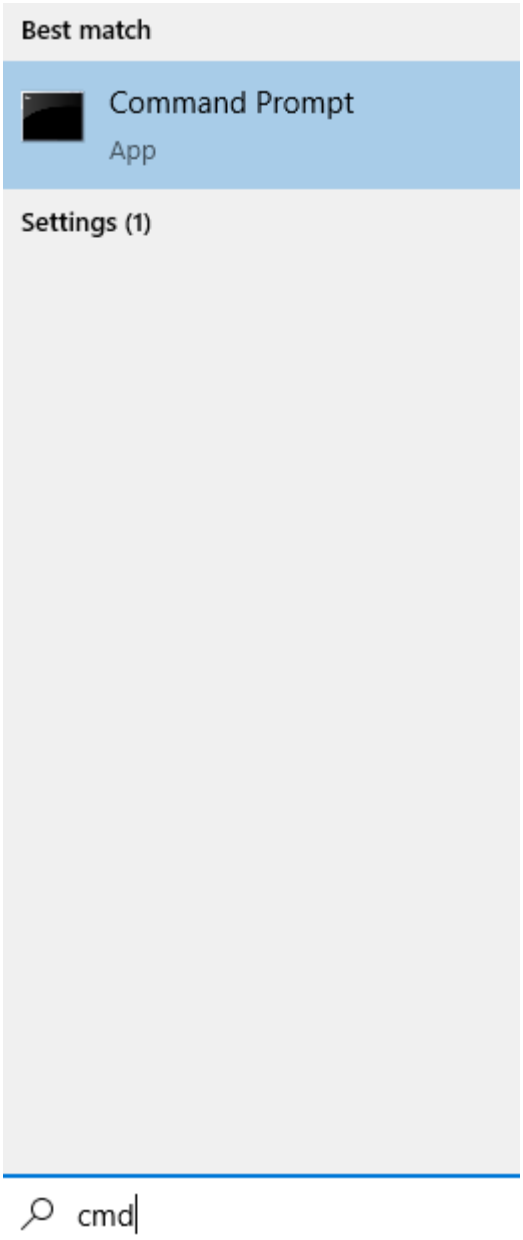
16. Click **Apply** to confirm the changes to the Policy



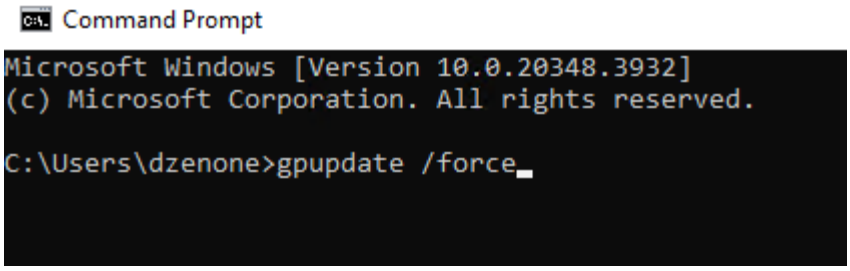
17. Click **OK**.



18. Open a Command Prompt window on the Windows Member server. Search for ***cmd*** in the Windows search bar and click **Command Prompt** in the results.



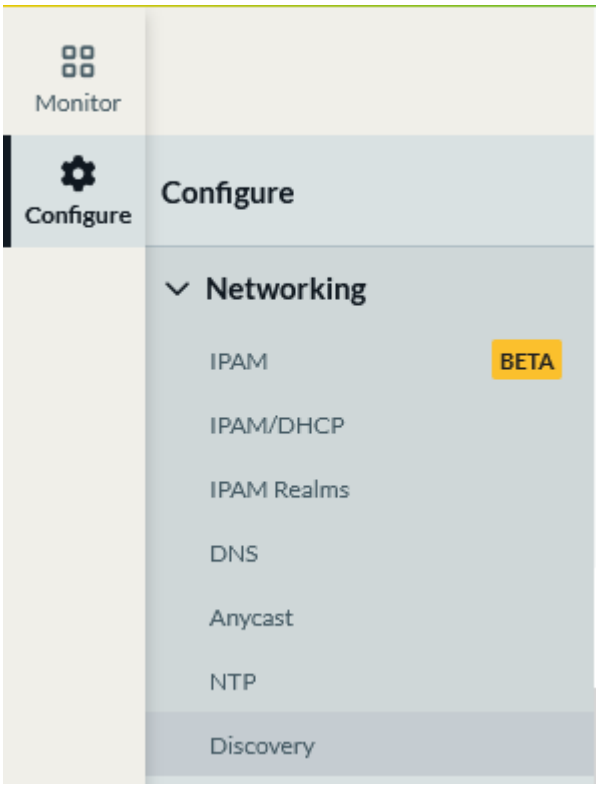
19. In the **Command Prompt** window, input the command **gpupdate /force**.



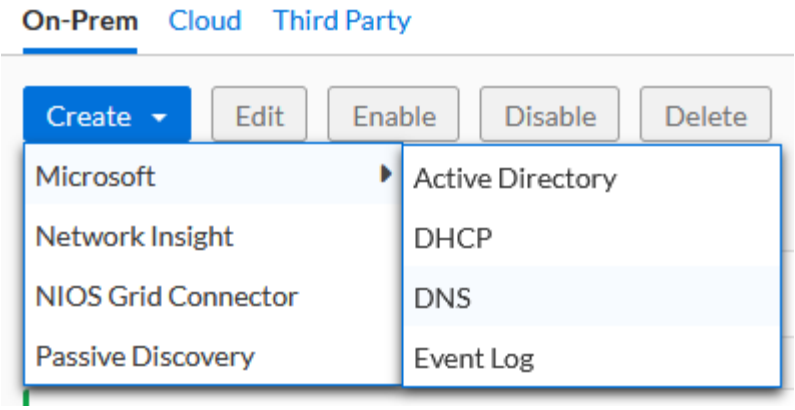
Create a Microsoft DNS Discovery Job

Once you have installed the Universal DDI Agent and have created a Domain User for DNS management, a Discovery Job can be created. To create a Discovery Job for DNS management, perform the following steps:

1. Navigate to the **Discovery** page by highlighting **Configure**. Expand **Networking**, then click **Discovery** in the dropdown list.



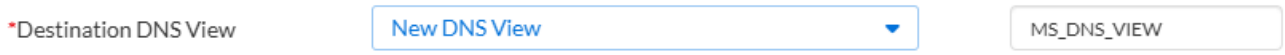
2. On the Discovery page, ensure that you are on the **On-Prem** tab. Click **Create**, highlight **Microsoft**, then click **DNS** in the list that is revealed.



3. In the **Create Discovery Job Configuration – Microsoft: DNS** panel, ensure that the **State** toggle switch for the new Discovery Job is set to **Enabled**.

4. Input a name in the **Name** text field.

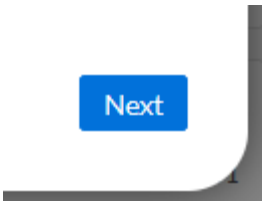
5. Select an existing DNS view or create a new one in the **Destination DNS View** dropdown list. ***Note:*** *A DNS view acts as a bucket for DNS data synced from Windows. If you select* ***New DNS View****, you must provide a name in the text field that is revealed.*



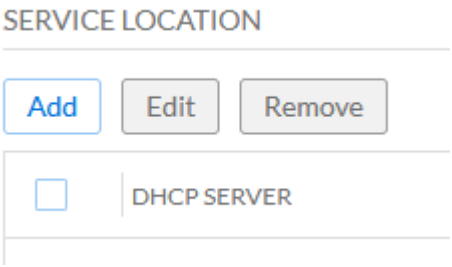
6. (Optional) Change the sync interval via the **Sync Interval** dropdown list. ***Note:*** *It is considered a best practice to keep the Sync Interval as* ***Auto****, which is 15 minutes.*

7. Select Read or Read/Write based on the desired state of the integration.

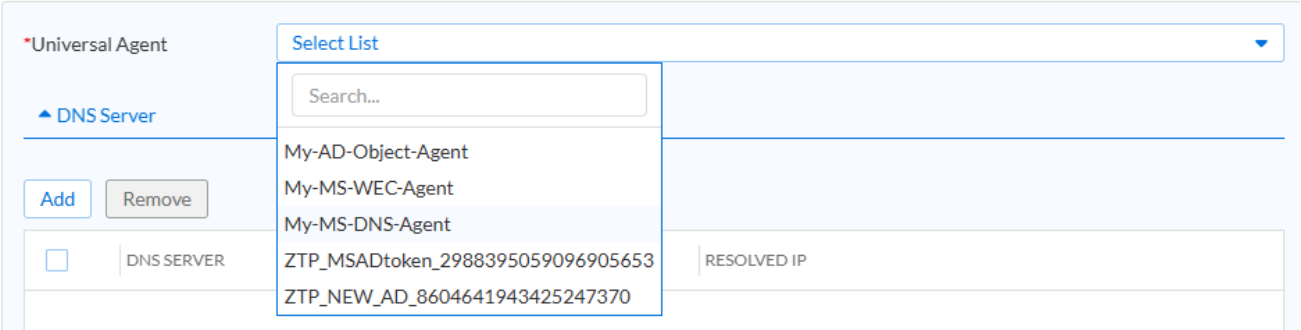
8. Click **Next**.



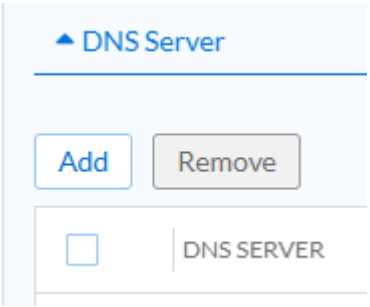
9. On the **SERVICE LOCATION** page, click **Add** to begin adding a Windows Server-based DNS server to manage.



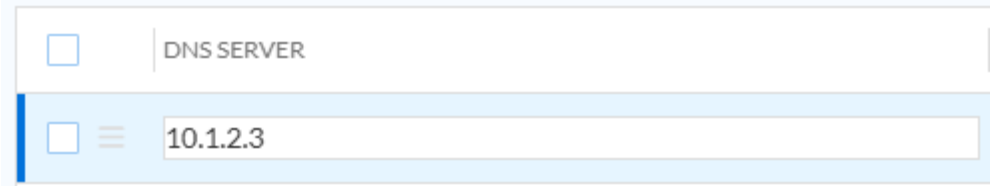
10. Select the appropriate Universal DDI Agent in the **Universal Agent** dropdown list.



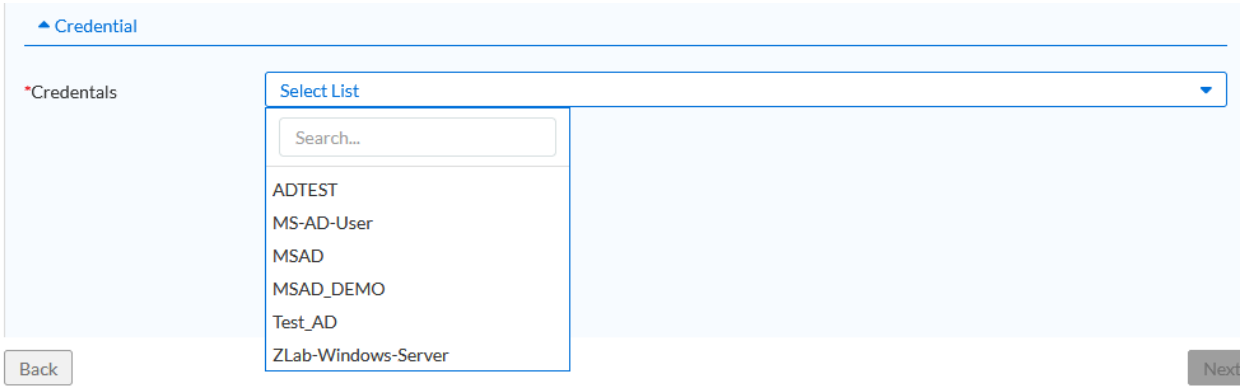
11. Under the **DNS Server** header, click **Add**.



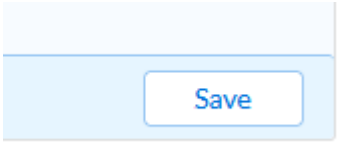
12. Input the IP of a Microsoft DNS Server.



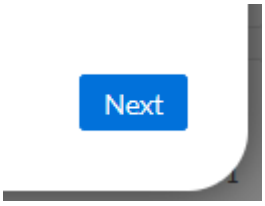
13. (Optional) Repeat steps 11-12 to add any additional DNS servers you would like Infoblox to manage to the Discovery Job.
14. Under the **Credential** header select the appropriate credentials in the **Credentials** dropdown list.



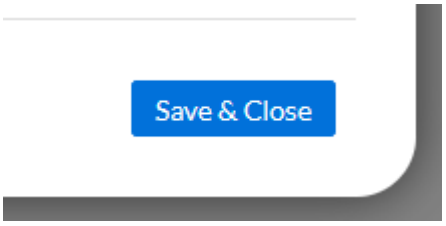
15. Click **Save.**



16. Click **Next**.



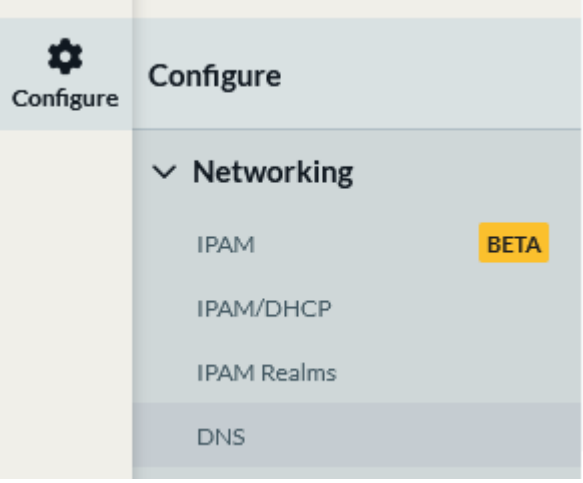
17. Click **Save & Close** to confirm the creation of the new Discovery Job.



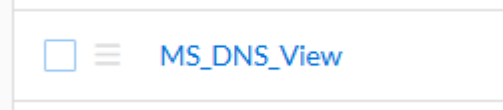
Managing Windows Server DNS from the Infoblox Portal

To manage Windows Server-based DNS objects from the Infoblox Portal, perform the following steps (***Note:*** *These steps are intended for a portal environment with a Read/Write DNS Discovery Job configured*):

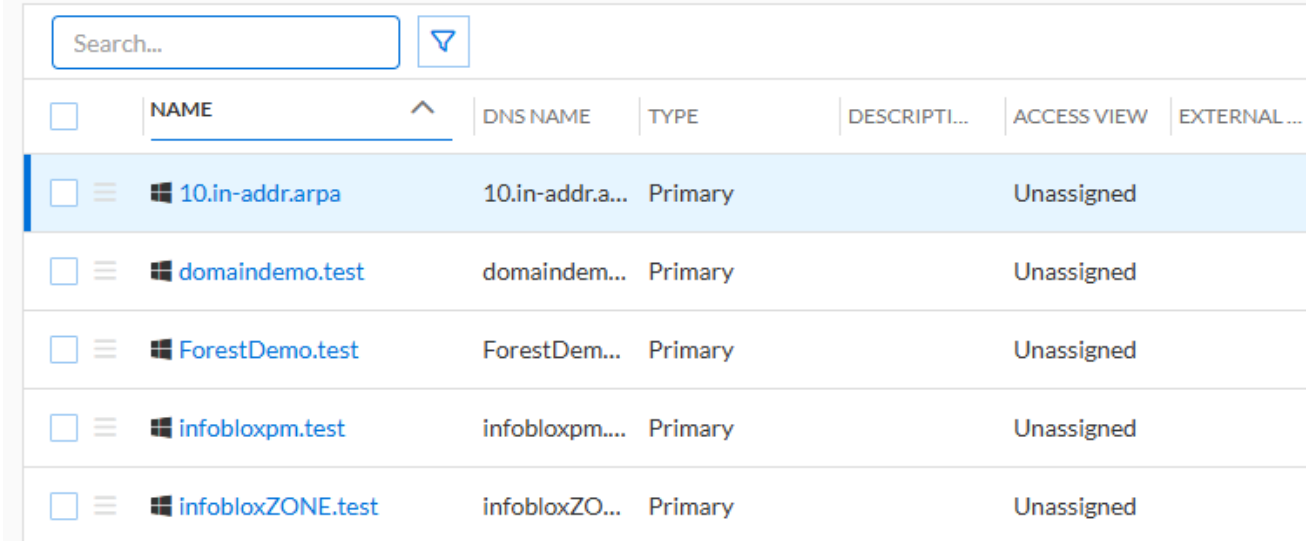
1. Navigate to the DNS page by highlighting **Configure** and clicking **Networking**. Then, click **DNS** in the dropdown list.



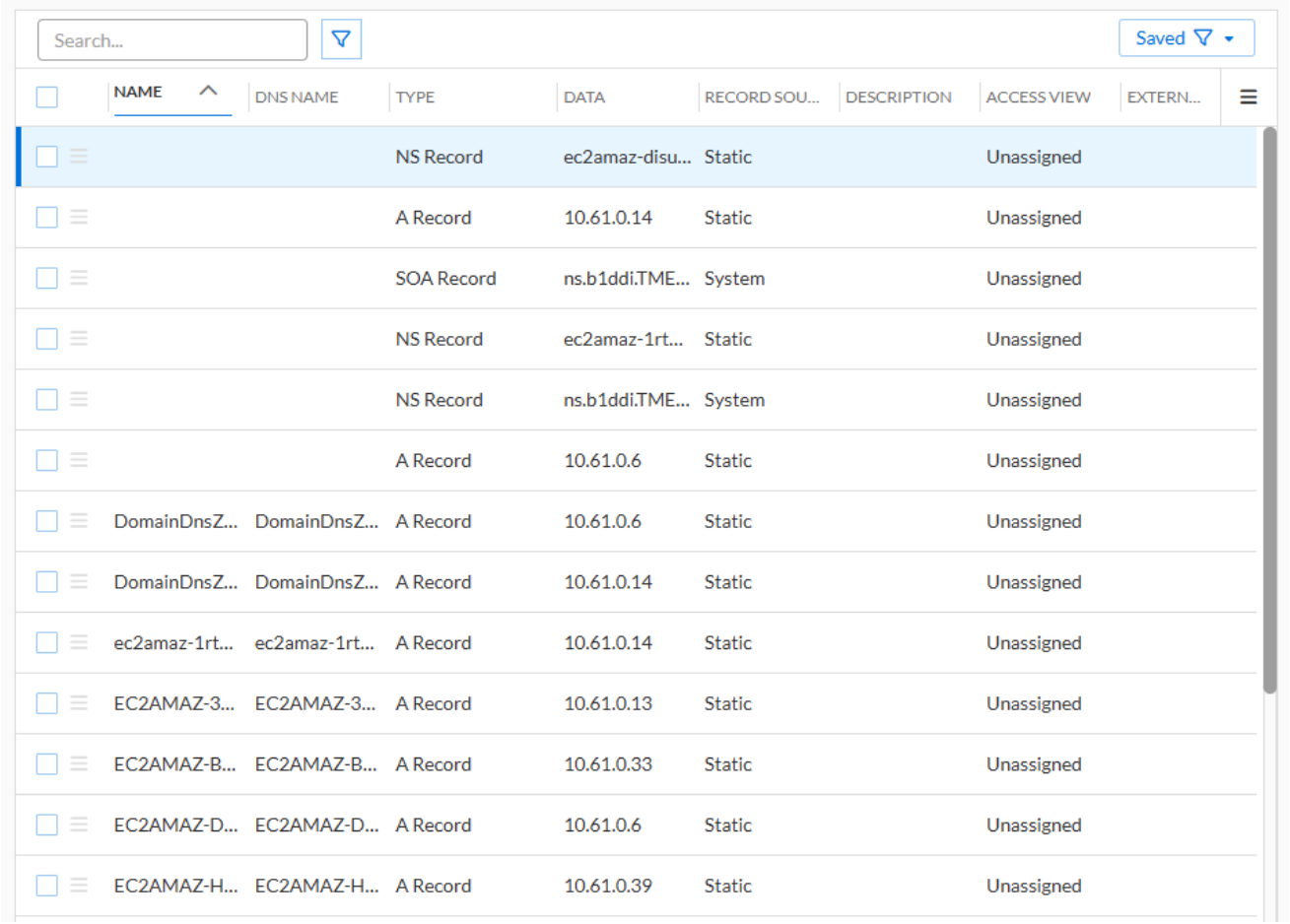
2. Locate and click the **DNS View** that was selected or created in the previous section.



3. Inside the view will be multiple synced zones from Microsoft. Click any **DNS zone** to view the records inside.



4. Inside will be records synced from Microsoft. From here, test the integration by creating a new record or editing an existing record and viewing the results in Windows Server.


Search...
Saved
NAME
DNS NAME
TYPE
DATA
RECORD SOU...
DESCRIPTION
ACCESS VIEW
EXTERN...
NS Record ec2amaz-disu... Static Unassigned
A Record 10.61.0.14 Static Unassigned
SOA Record ns.b1ddi.TME... System Unassigned
NS Record ec2amaz-1rt... Static Unassigned
NS Record ns.b1ddi.TME... System Unassigned
A Record 10.61.0.6 Static Unassigned
DomainDnsZ... DomainDnsZ... A Record 10.61.0.6 Static Unassigned
DomainDnsZ... DomainDnsZ... A Record 10.61.0.14 Static Unassigned
ec2amaz-1rt... ec2amaz-1rt... A Record 10.61.0.14 Static Unassigned
EC2AMAZ-3... EC2AMAZ-3... A Record 10.61.0.13 Static Unassigned
EC2AMAZ-B... EC2AMAZ-B... A Record 10.61.0.33 Static Unassigned
EC2AMAZ-D... EC2AMAZ-D... A Record 10.61.0.6 Static Unassigned
EC2AMAZ-H... EC2AMAZ-H... A Record 10.61.0.39 Static Unassigned

infoblox.

Infoblox unites networking, security and cloud with a protective DDI platform that delivers enterprise resilience and agility. We integrate across hybrid and multi-cloud environments, automate critical network services and preemptively secure the business—providing the visibility and context needed to move fast without compromise.

Corporate Headquarters
2390 Mission College Blvd, Ste.
501 Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com