DEPLOYMENT GUIDE

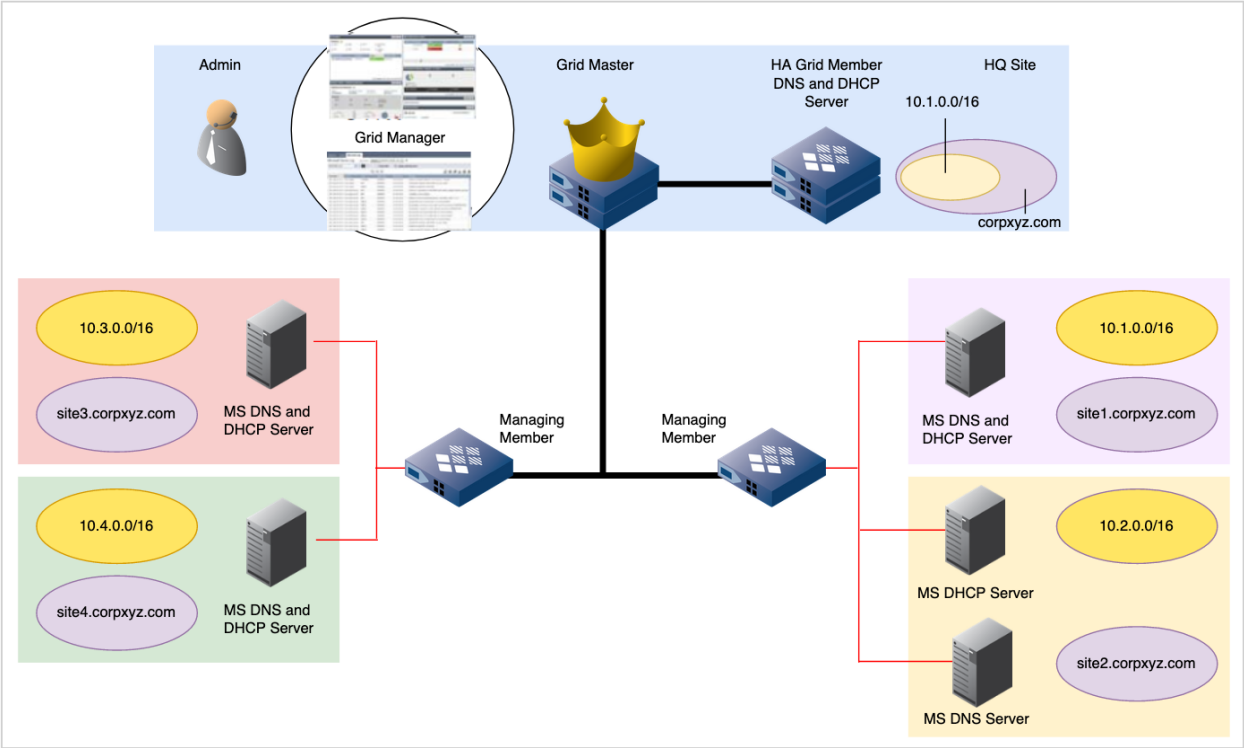
Integrating Microsoft Server 2019 into NIOS 8.6

Table of Contents

Introduction

NIOS 8.6 Grid members can be configured to manage Microsoft Windows DNS and DHCP servers, and synchronize their DNS and DHCP data to the Grid database, so you can view and/or manage the data from Grid Manager. After the data is synchronized, you can use the NIOS GUI to simplify DNS and DHCP configuration and troubleshooting. You can also use Smart Folders to organize your data, and monitor your networks and Microsoft servers from the Dashboard. In addition, you can control the DNS and DHCP services of the Microsoft servers from Grid Manager and configure server properties as well. You can use the Identity Mapping feature to get visibility of user interaction with their environments.

This deployment guide goes over the steps to add Microsoft Windows 2019 servers.



You do not have to configure or install any application on the Microsoft servers for the Grid members to communicate with the servers. Infoblox uses MS-RPC (Microsoft Remote Procedure Calls) to manage Microsoft servers.

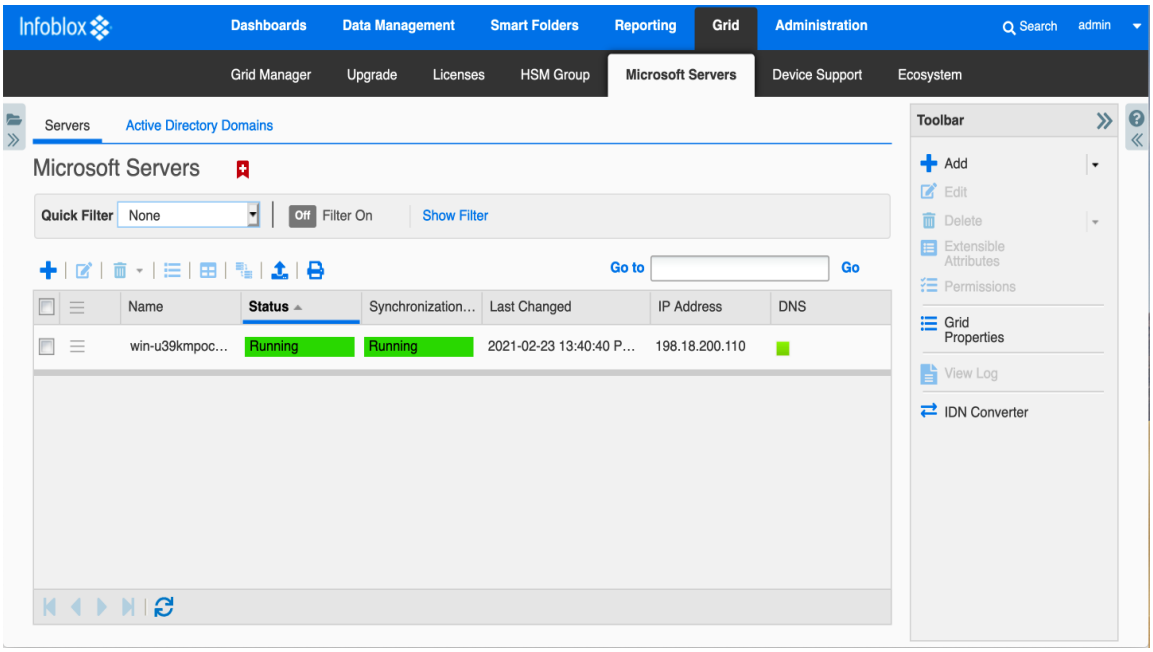
A Grid member can manage a Microsoft server in either of two modes, Read-Only or Read-Write. In Read-Only mode, the Grid member synchronizes data from the Microsoft server to the Grid so admins can use Grid Manager to view the synchronized data, but not update it. Read/Write mode allows admins to update the synchronized data as well.

Updates from Grid Manager are then synchronized to the Microsoft server, and updates from the Microsoft server are synchronized to the Grid.

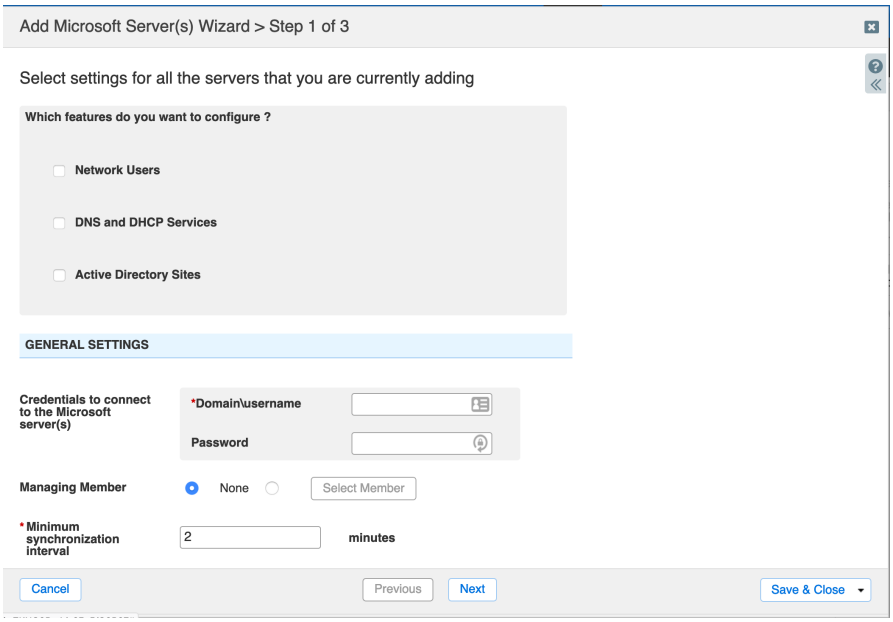
Assigning Grid Members to Microsoft Servers

To configure a Grid member to manage one or more Microsoft servers:

1. Navigate to **Grid** tab → **Microsoft Servers** tab → **Servers** tab.



2. Click on the '**+**' to bring up the '**Add**' wizard.

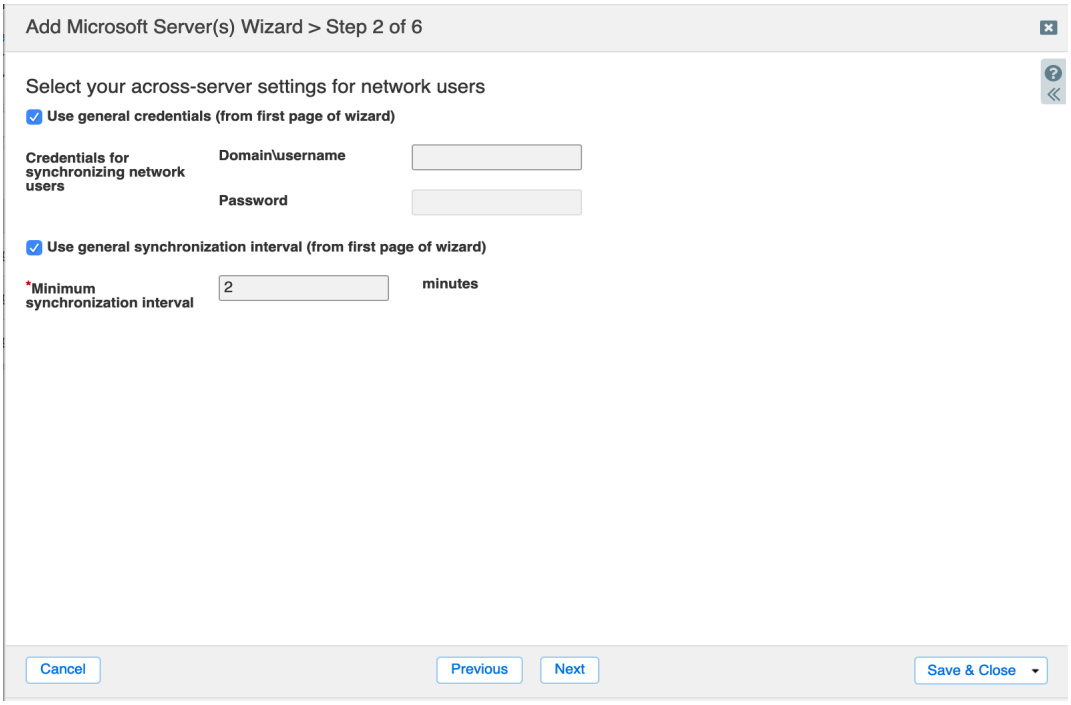


- Which features do you want to configure?: This section appears only when you have selected the Enable MS AD feature check box for mapping network users. You can select multiple options in this section:
  - **Network Users**: Select this check box to enable the Grid member to synchronize user information with the managed Microsoft servers.
  - **DNS and DHCP Services**: Select this check box to enable the Grid member to synchronize DNS and DHCP services with the Microsoft servers.
  - **Active Directory Sites**: Select this check box to enable the Grid member to synchronize Active Directory sites.
- In the **General Settings** section, complete the following:
  - **Credentials to Connect to the Microsoft Server(s):** Enter the login name and password that the appliance uses to connect to the Microsoft servers. These must be the same as those you specified when you created the user account for the Grid member on the Microsoft servers. *Note that you must specify the domain name and the user name in the following format:* ***domain_name\user_name****.*
  - **Managing Member**: Click Select Member and select the Grid member that manages Microsoft servers.
    Select None if you do not want to associate a Microsoft server with a Grid member.
  - **Minimum Synchronization Interval** (min): The default synchronization interval is two minutes. This is the time between the completion of one synchronization and the start of a new one. Synchronizing large data sets could take longer than the synchronization interval, causing a delay in the start of the next synchronization. For example, if the synchronization interval is two minutes but a synchronization takes five minutes, the time between the start of the first synchronization and the start of the next one is approximately seven minutes.
- **Logging Level**: Select a logging level for the Microsoft server log from the drop-down list: Low, Normal, High, and Debug. NIOS logs the messages based on the logging level you set.
  - Low: Logs only error messages.
  - Normal: Logs warning and error messages.
  - High: Logs warning, error and information messages.
  - Debug: Logs messages about all events associated with synchronization.
- **Logging output destination**: From the drop-down list, select an output destination to which the appliance saves log messages for Microsoft servers. When you select Microsoft Log, the

appliance logs the messages that are generated for the respective Microsoft server in the existing Microsoft log. This is selected by default. When you select Syslog, NIOS logs the messages that are generated for the respective Microsoft server in the syslog. Comment: You can enter additional information about the servers.

- **Synchronize Data into Network View**: This field appears only when there is more than one network view in the grid. When there are multiple network views, you must specify to which network view the data from the Microsoft server is synchronized.
- **Synchronize DNS Data into DNS View**: This field appears only when there is more than one DNS view in the selected network view. You can select a different network view for the Microsoft server.
- **Disable Synchronization**: Select this to disable the Microsoft servers. This allows you to provision the Microsoft servers and then enable them at a later time.

3. Click **Next**.
4. If you have selected the Network Users check box, complete the following in the Select your across-server settings for Network Users page:



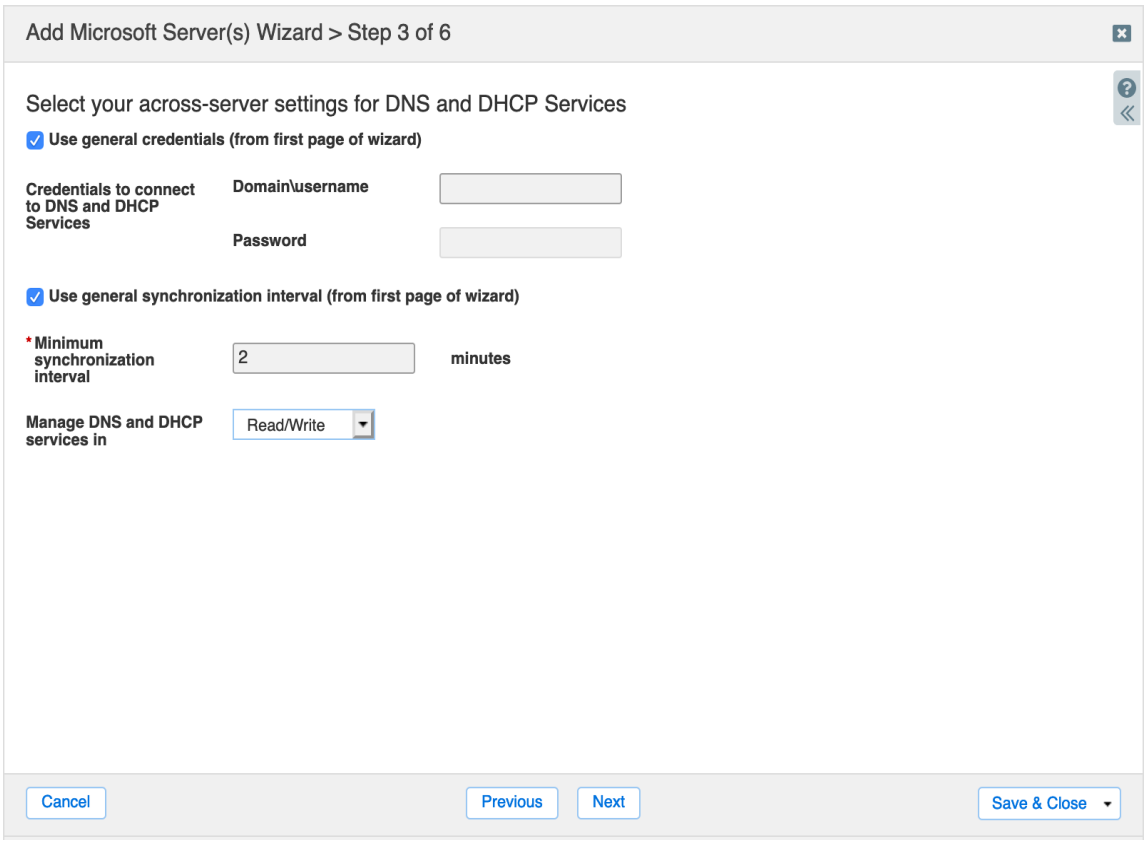
- Use **General credentials** (from the first page of wizard): Select this **check box** if you want to use the same credentials that you specified for connecting the Microsoft servers.
- **Credentials for synchronizing Network User service information**: Specify a username and password to synchronize user information from Active Directory domain controllers. The

username you specify here must belong to the Domain User group and Event Log Reader group in Microsoft.

- **Use General synchronization interval** (from first page of wizard): Select this check box to use the same synchronization interval that you specified in the Minimum Synchronization Interval for synchronizing the user and device mapping information from the Microsoft Active Directory authentication logs.

- **Minimum synchronization interval**: The default synchronization interval is two minutes. This is the time between the completion of one synchronization and the start of a new one. Specify an interval to synchronize user information from the Microsoft Active Directory authentication logs.

5. If you have selected the DNS and DHCP Services check box, complete the following in the Select your across-server settings for DNS and DHCP Services page:

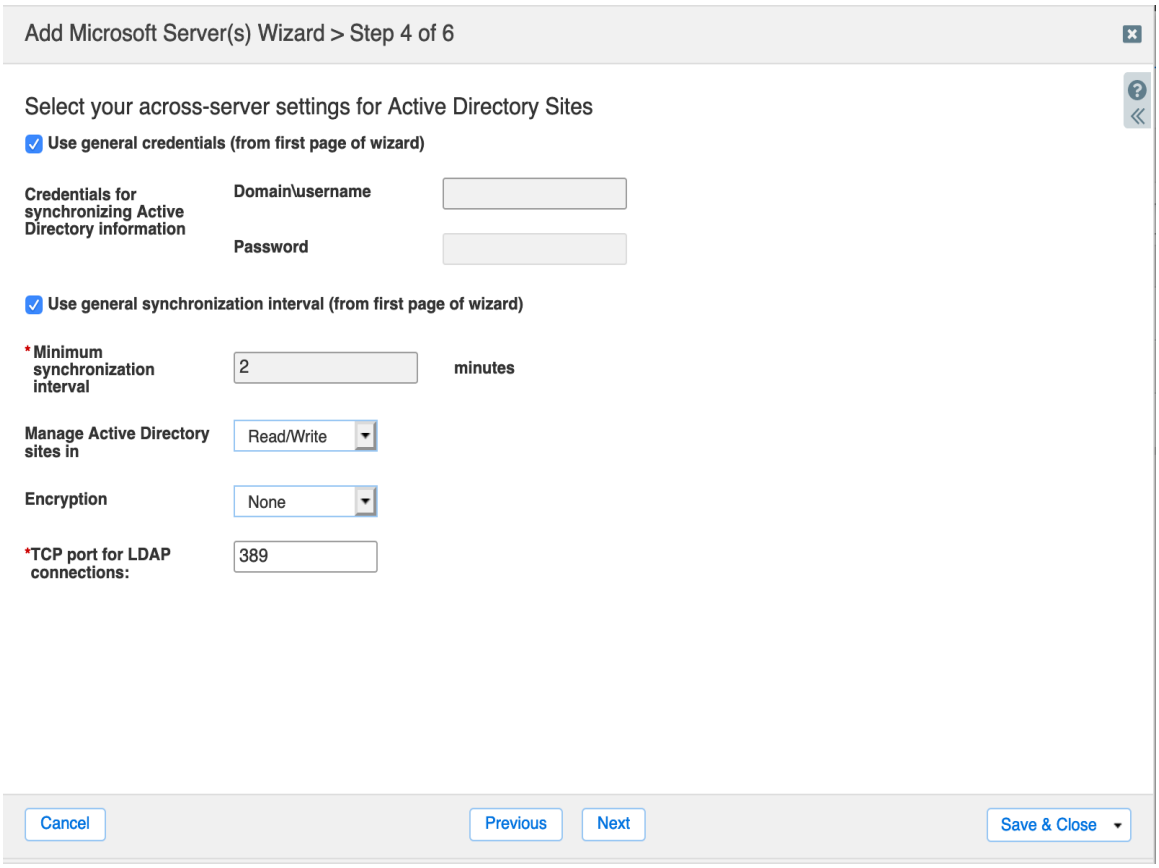


- **Use General credentials** (from the first page of wizard): Select this check box if you want to use the same credentials that you specified for connecting the Microsoft servers.

- **Credentials to connect to DNS and DHCP Services**: Specify a username and password to synchronize DNS and DHCP services. You must use the same username and password that you specify here when the appliance prompts for credentials during DNS or DHCP synchronization.

- **Use General synchronization interval** (from first page of wizard): Select this check box to use the same synchronization interval that you specified in the Minimum Synchronization Interval for synchronizing the DNS and DHCP services as well.
- **Minimum Synchronization interval**: The default synchronization interval is two minutes. This is the time between the completion of one synchronization and the start of a new one. Specify an interval to synchronize the DNS and DHCP data from the Microsoft server.
- **Manage DNS and DHCP services in**: Select a value from the drop-down list. You can choose to manage the DNS and DHCP synchronization services in either Read-only or Read/Write mode.

6. If you have selected the Active Directory Sites check box, complete the following in the Select your across-server settings for Active Directory Sites page:



- **Use General credentials** (from the first page of wizard): Select this check box if you want to use the same credentials that you specified for connecting the Microsoft servers. Clear the check box to specify a new username and password for managing Active Directory sites.
- **Credentials for synchronizing Active Directory information**: Specify a username and password to synchronize Active Directory sites. You must specify the same username and password that

you specify here when the appliance prompts for credentials while synchronizing Active Directory sites.

- **Use General synchronization interval** (from first page of wizard): Select this check box to use the same synchronization interval that you specified in the Minimum Synchronization Interval for synchronizing Active Directory sites.

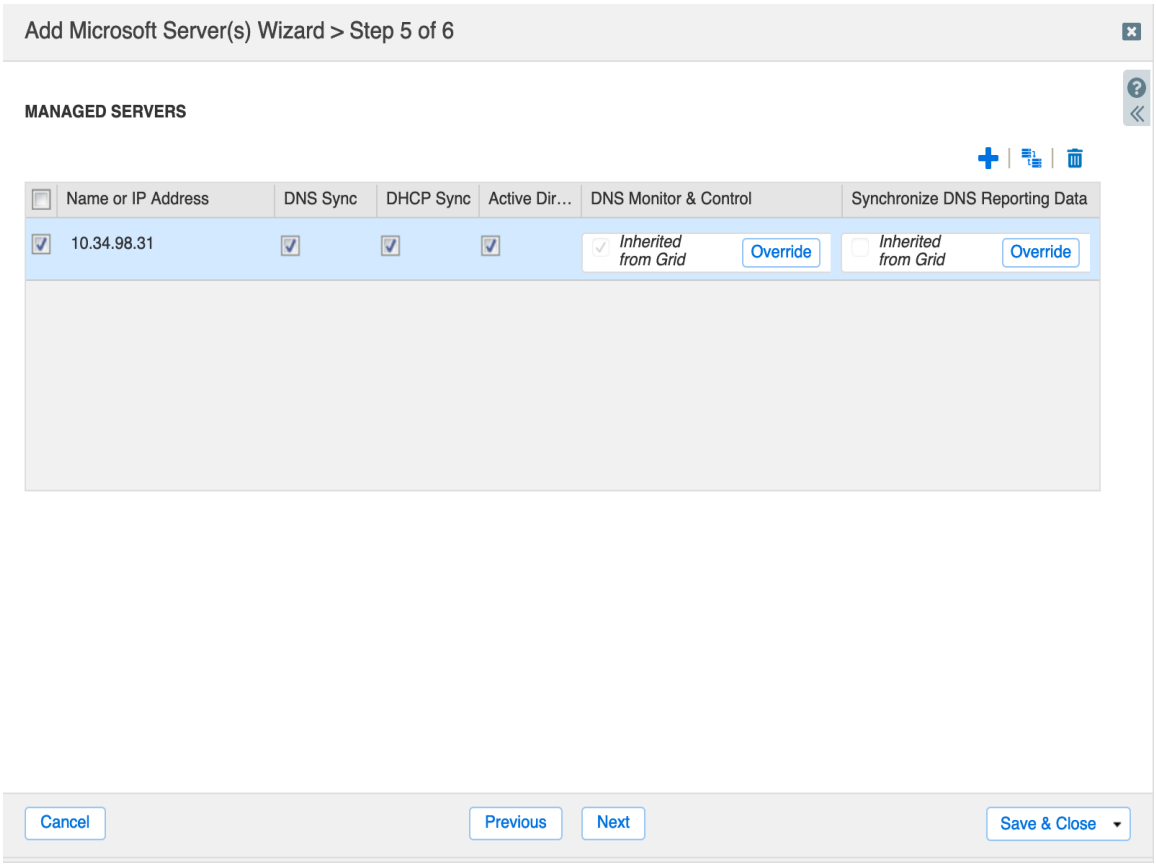
- **Minimum Synchronization interval**: The default synchronization interval is two minutes. This is the time between the completion of one synchronization and the start of a new one. Specify an interval to synchronize the Active Directory sites.

- **Manage Active Directory sites in**: Select a value from the drop-down list. You can choose to manage the Active Directory Site in either Read-only or Read/Write mode.

- **Encryption**: You can encrypt the network traffic between the Grid member and the managed Microsoft server using SSL. Select a value, None or SSL, from the drop-down list. Infoblox strongly recommends that you select SSL from the drop-down list to ensure the security of all communications between the NIOS appliance and the Active Directory server. When you select SSL, the appliance automatically updates the TCP port to 636. When you select this option, you must specify the FQDN of the Microsoft server instead of the IP address and you must upload a CA certificate from the Active Directory server. Click CA Certificates to upload the certificate. In the CA Certificates dialog box, click the **Add** icon, and then navigate to the certificate to upload it.

- **TCP port for LDAP connections**: The appliance displays the port number by default based on the encryption type that you select. When you select None, the appliance automatically updates the TCP port to 389.

7. Click **Next** and do the following in the **Managed Servers** table:



- **Name or IP Address**: Enter either the FQDN or IP address of the Microsoft server. In order for the member to resolve the FQDN of a Microsoft server, you must define a DNS resolver for the Grid member in the DNS Resolver tab of the Member Properties editor. *Note that if the IP address of the Microsoft server is specified, then the DNS resolver must resolve it when the member and Microsoft server synchronize DHCP data only.*

- **DNS Sync**: Select this option to enable the Grid member to manage the DNS service and synchronize DNS data with this server. Clearing this check box disables DNS service management and data synchronization. This allows you to pre-provision specific Microsoft servers and then enable them at a later time.

- **DHCP Sync**: Select this option to manage the DHCP service of the Microsoft server and synchronize DHCP data with this server. Clearing this check box disables DHCP service management and data synchronization. This allows you to pre-provision specific Microsoft servers and then enable them at a later time.

- **Active Directory Sites**: Select this option to manage Active Directory sites and synchronize Active Directory Sites and networks with the Grid.

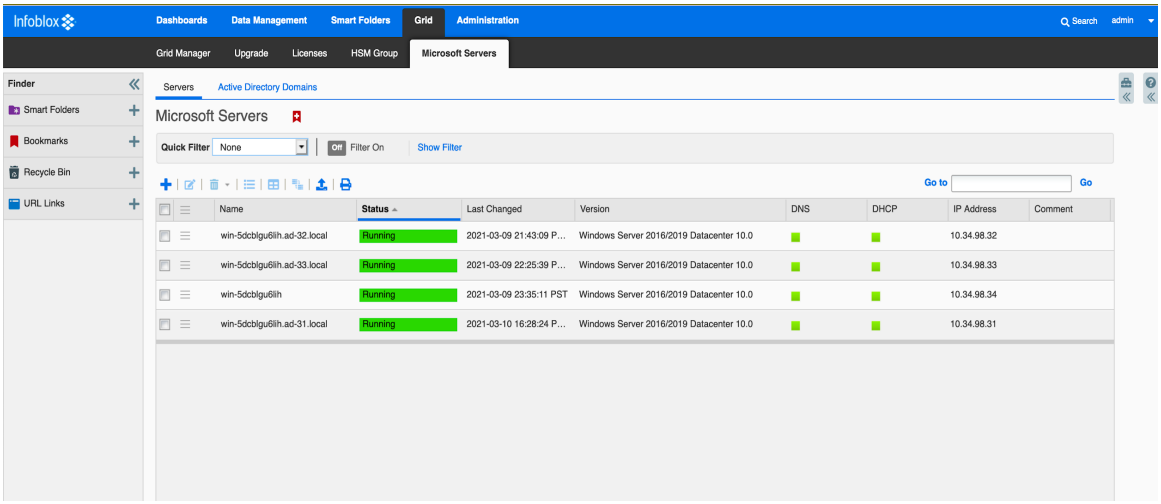
- **DNS Monitor & Control**: Click **Override** to override the setting inherited from the Grid. To inherit the same settings as the Grid, click Inherit. Select this to enable monitoring and the ability to control DNS service for the Microsoft server.

- **Synchronize DNS Reporting Data**: Click **Override** to override the settings that are inherited from the Grid. To retain the same settings as the Grid, click Inherit. Select this to synchronize DNS reporting data from the Microsoft server. *Note that synchronization of DNS reporting data is effective only when the DNS Sync option is enabled for the Microsoft server.*

- **DHCP Monitor & Control**: Click **Override** to override the setting inherited from the Grid. To inherit the same settings as the Grid, click Inherit. Select this to monitor and control DHCP service for the Microsoft server.

- **Synchronize Network Users**: Click **Override** to override the settings inherited from the Grid. To inherit the same settings as the Grid, click **Inherit**. Select this to enable the identity mapping for the Microsoft server. Click **Save and Close**.

8. After about 5 minutes, you should see the following:



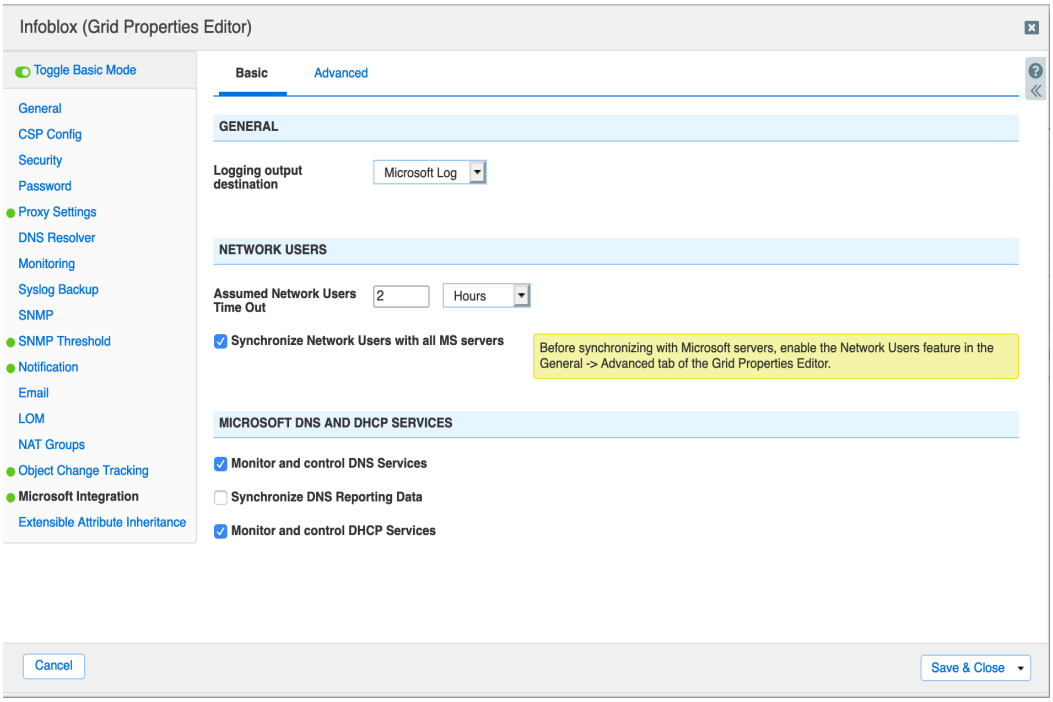
Note the bottom entry.

9. **Save** the configuration and click Restart if it appears at the top of the screen.

Setting Grid Properties for Managing Microsoft Servers

To configure Grid properties for managing Microsoft servers, complete the following:

1. Grid: From the **Grid** tab → **Grid Manager** tab, expand the Toolbar and click **Grid Properties** → **Edit**. Select **Microsoft Integration** tab in the Grid Properties Editor wizard.



Complete the following in the Basic tab:

- **Logging output destination**: From the drop-down list, select an output destination to which the appliance saves log messages for Microsoft servers. When you select Microsoft Log, the appliance logs the messages that are generated for the respective Microsoft server in the existing Microsoft log. This is selected by default. When you select Syslog, NIOS logs the messages that are generated for the respective Microsoft server in the syslog.

- **Network Users:** You can control the network users tab in the **Data Management → Network Users** screen. You can set the time from minutes to hours to days. Enable **Synchronize Network Users** with all MS Servers to ensure the Network Users screen is populated

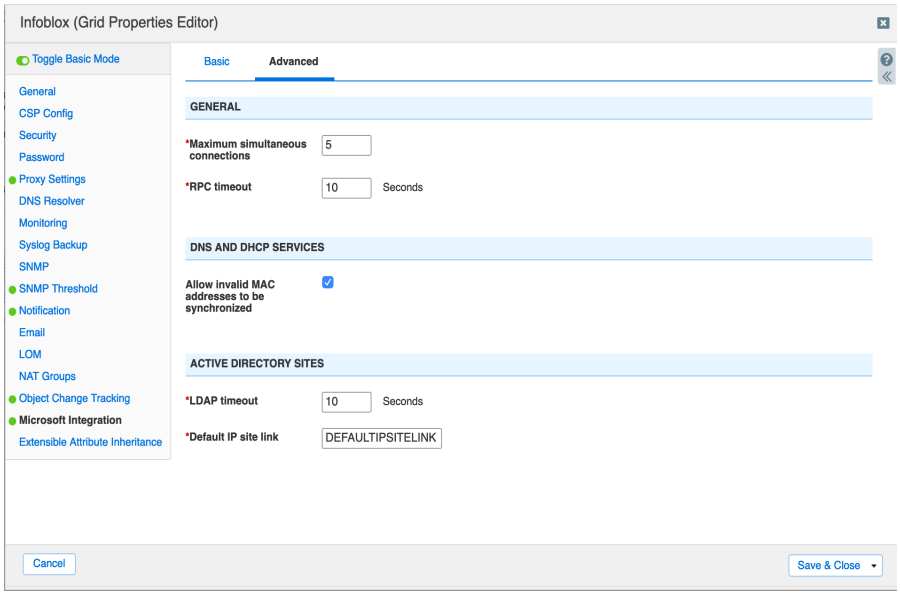
- **Monitor DNS and DHCP Services**: You can enable monitoring and control services for DNS and DHCP services at the Grid level and override the settings for each service at the Microsoft server level. This is enabled, by default. Each monitoring and control setting applies only to the corresponding service and is applicable to the respective Microsoft server only.

    - **Monitor and control DNS Services**: Select this to enable monitoring and the ability to control DNS service for the Microsoft server.

    - **Synchronize DNS Reporting Data**: Select this to synchronize DNS reporting data from the Microsoft server. Clearing this check box disables DNS reporting data synchronization.

    - **Monitor and control DHCP Services**: Select this to enable monitoring and the ability to control a DHCP service for the Microsoft server.

2. Optionally, select the **Microsoft Server Settings** tab in the Grid Properties Editor wizard and complete the following in the **Advanced** tab or click the **Advanced** tab in a Microsoft server editor:



   - **Maximum simultaneous connections**: Specify a maximum number of simultaneous RPC connections that can be configured for the respective Microsoft server, which are managed by the Grid. The default is five. You can specify a value between two and 40.

   - **RPC timeout**: Specify the RPC timeout value in seconds to control the network communication timeout. The default is ten seconds. You can specify a value between one and 60.

   - **Allow Invalid MAC Address to be synchronized**: This is enabled, by default. Select this to enable synchronization for invalid MAC addresses.

   - **LDAP timeout**: Specify the LDAP connection timeout value. The default is 10 seconds. You can specify a value between one and 60 seconds.

   - **Default IP site link**: Specify the default IP site link in the form of a string. The appliance does not validate it against the Windows server during configuration. The appliance displays an error message during synchronization, if the site link for IP does not match the configured name on the Windows server.

3. **Save** the configuration.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

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