GS2 LDAP Setup

 This document will guide you through the process of configuring your GS2 for LDAP authentication using either an open LDAP Server or Microsoft’s Active Directory. The last section includes steps specific to implementing an open LDAP server with a Synology NAS, but the concepts are applicable to other LDAP implementations as well. Contact GRIDSMART Support for assistance.

# What is LDAP and AD?

Open Lightweight Directory Access Protocol (Open LDAP) is an open and cross-platform protocol used for directory services authentication. LDAP provides the communication language that applications use to communicate with other directory services servers. Directory services store the usernames, passwords, and computer accounts, and share that information with other entities on the network.

Active Directory (AD) is a directory services implementation that provides all sorts of functionality like authentication, group and user management, policy administration and more. AD uses the LDAP protocol, so in practice the behavior on the GS2 will be the same.

Please consult your IT or Networking team for additional guidance.

## LDAP Prerequisites

* Server for hosting LDAP (This document will assume the user is configuring a Synology NAS, but the same concepts should carry over for most implementations).
* LDAP user groups appropriate for each permissions group on the GS2 (admin, publish, readonly).
* DNS Server (Can be hosted on same server as LDAP)
* Domain name entries for your GS2’s
* Domain name entry for your LDAP server

## Additional Prerequisites for Secure LDAP (recommended)

* Trusted CA certificate for your local domain
* Certificate for your local domain on your LDAP server

**NOTE:** *Regardless of implementation, we recommend your LDAP or AD server be assigned a static IP address or have a DHCP reservation. Consult with your IT or Networking department as needed.*

Table of Contents

[What is LDAP and AD? 1](#_Toc47619152)

[What you will need to use LDAP 1](#_Toc47619153)

[For Secure LDAP (recommended) 1](#_Toc47619154)

[1.0 Configuring GS2 for LDAP 3](#_Toc47619155)

[1.1 Enable Synology LDAP on GS2 3](#_Toc47619156)

[1.2 Active Directory Roles for GS2 4](#_Toc47619157)

[1.3 Configuring DNS on the GS2 4](#_Toc47619158)

[2.0 Configuring GS2 for AD 5](#_Toc47619159)

[2.1 Enable Microsoft Active Directory on GS2 5](#_Toc47619160)

[2.2 Active Directory Roles for GS2 7](#_Toc47619161)

[2.3 Configuring DNS on the GS2 7](#_Toc47619162)

[3.0 GS2 LDAP Debugging and Security 9](#_Toc47619163)

[3.1 Troubleshooting LDAP on GS2 9](#_Toc47619164)

[3.2 Troubleshooting LDAP with JXplorer 9](#_Toc47619165)

[4.0 GS2 Secure LDAP 11](#_Toc47619166)

[4.1 Enabling Secure LDAP / LDAPS on GS2 (Recommended) 11](#_Toc47619167)

[4.2 Troubleshooting Secure LDAP / LDAPS with JXplorer 12](#_Toc47619168)

[5.0 GS2 LDAP Import/Export 14](#_Toc47619169)

[5.1 Export/Import LDAP/AD settings 14](#_Toc47619170)

[6.0 Using Synology NAS 15](#_Toc47619171)

[6.1 Installing DNS Server and LDAP Server on Synology NAS 15](#_Toc47619172)

[6.2 Configuring DNS Server on Synology NAS 16](#_Toc47619173)

[6.3 Creating LDAP DNS Entry on Synology NAS 18](#_Toc47619174)

[6.4 Creating GS2 DNS Entry on Synology NAS 20](#_Toc47619175)

[6.5 Configuring LDAP Server on Synology NAS 21](#_Toc47619176)

[6.6 Adding LDAP Group on Synology NAS 23](#_Toc47619177)

[6.7 Adding LDAP User on Synology NAS 24](#_Toc47619178)

# 1.0 Configuring GS2 for LDAP

## 1.1 Enable Synology LDAP on GS2

 This section will guide you through the process of enabling Synology’s LDAP on the GS2.

1. Login to the GS2 Device Manager with an administrator account.
2. In the left-hand menu, click **Settings**.



1. Under the **Users** section, click the **LDAP** tile.



1. The **Enable LDAP** option should be unchecked.



1. Check the checkbox next to **Enable LDAP**.



1. For **Which directory type are you using**, select **LDAP**.



1. For **Fully Qualified Domain Name**, provide the FQDN for your LDAP Server.



1. For **Bind DN** and **Bind Password**, provide the **Bind** credentials for your LDAP Server.



1. The **LDAP URL** should resemble the following:



1. For **User Role to LDAP Group Assignments**, provide the corresponding groups in your LDAP Server.



1. Click the **Apply Changes** button.



## 1.2 Active Directory Roles for GS2

 The following three **Security Groups** are required for GS2 authentication. These will be used for **User Role to LDAP Group Assignments** in the previous section. **Security Groups** must be created in the LDAP server (see section 6.6 and 6.7 for an example).

* Admin
	+ gsadmin
* Publish
	+ gspublish
* View Only
	+ gsviewonly

## 1.3 Configuring DNS on the GS2

This section will guide you through adjusting your GS2 network settings to use your DNS server. **If you did not create a new DNS server and are instead using your existing DNS server, you can ignore this section.**

1. Login to the GRIDSMART Device Manager with an admin account.
2. In the left-hand menu, click **Settings.**



1. Under the **Users** section, click the **Network** tile.



1. Ensure the **Use DHCP** checkbox is unchecked (You will need to set a static IP address for your GS2 to assign a new DNS IP address).
2. Set the DNS field to your DNS server’s IP address.

**Note:** *If you have configured your new DNS server to forward traffic to your network’s existing DNS server, ensure you are still able to connect to GRIDSMART Cloud.*

# 2.0 Configuring GS2 for AD

## 2.1 Enable Microsoft Active Directory on GS2

This section will guide you through configuring Active Directory on the GS2.

1. Login to the GRIDSMART Device Manager with an admin account.
2. In the left-hand menu, click **Settings**.



1. Under the **Users** section, click the **LDAP** tile.



1. Check the checkbox next to **Enable LDAP**.



1. For **Which directory type are you using**, select the radio button next to **Active Directory**.



1. For **Fully Qualified Domain Name**, provide the FQDN for your Active Directory Server. Consult with your IT or Networking department as needed.

 

1. For **Bind DN** and **Bind Password**, provide the **Bind** credentials for your Active Directory Server. Consult with your IT department or Active Directory Administrator as needed.



1. The **LDAP URL** should resemble the following.



1. For **User Role to LDAP Group Assignments**, provide the corresponding groups in your Active Directory Server. Consult with your IT department or Active Directory Administrator as needed.



1. Click the **Apply Changes** button.



## 2.2 Active Directory Roles for GS2

The following three **Security Groups** are required for GS2 authentication. These will be used for **User Role to LDAP Group Assignments**. **Security Groups** must be created in Active Directory by your Active Directory Administrator.

* Admin
	+ gsadmin
* Publish
	+ gspublish
* View Only
	+ gsviewonly

## 2.3 Configuring DNS on the GS2

This section will guide you through adjusting your GS2 network settings to use your new DNS server. If you did not create a new DNS server and are instead using your existing DNS server, you can ignore this section.

1. Login to the GS2 Device Manager with an administrator account.
2. In the left-hand menu, click **Settings.**



1. Under the **Users** section, click the **Network** tile.



1. Ensure the **Use DHCP** checkbox is unchecked. You will need to set a static IP address for your GS2 to assign a new DNS. Consult with your IT or Networking department as needed.
2. Set the **DNS** to your DNS server’s IP address.

**Note:** *If you have configured your new DNS server to forward traffic to your network’s existing DNS server, ensure you are still able to connect to GRIDSMART Cloud.*

# 3.0 GS2 LDAP Debugging and Security

## 3.1 Troubleshooting LDAP on GS2

This section will guide you through enabling the LDAP debug logs on the GS2. The last 75 lines of debug logs can be viewed under *Diagnostics 🡪 Logs 🡪 Advanced 🡪 Request Errors*. Contact GRIDSMART support for assistance with interpreting logs.

1. Login to the GRIDSMART Device Manager with an admin account.
2. In the left-hand menu, click **Settings**.



1. Under the **Users** section, click the **LDAP** tile.



1. At the bottom of the page, check **Enable debug logs**.
2. Click **Apply Changes**.



## 3.2 Troubleshooting LDAP with JXplorer

This section will guide you through troubleshooting your LDAP server using JXplorer client. This is an alternative way to test LDAP on your network from your own machine. You can find and download JXplorer from <http://jxplorer.org/>

1. Under **File**, click on **Connect**
2. Within the **Host** field, enter the hostname for your LDAP server.
3. Adjust the **Security** level to **User + Password** 
4. For **User DN,** enter the full domain name for the **Bind** account created on the LDAP server (**example:** uid=ldapbind,cn=users,dc=ldap,dc=mycompany,dc=com).
5. Enter the **Bind Password** that you created when you made your **Bind** account.
6. Once all settings are correct, click **OK**.

**Note:**

If everything is working, you should see a directory tree with users and user groups, appropriate for the various permissions groups.

The top three levels should be the domain for your LDAP server in reverse order. For example, the three levels from top to bottom would be **com**, **mycompany**, and **ldap** for a domain called **ldap.mycompany.com**.



# 4.0 GS2 Secure LDAP

## 4.1 Enabling Secure LDAP / LDAPS on GS2 (Recommended)

This section will guide you through enabling LDAPS on the GS2. Using LDAPS is recommended to encrypt network traffic between the GS2 and your LDAP server.

**NOTE:** You will need a Trusted CA Certificate on your GS2’s and a certificate on the same domain for the LDAP server. Consult your IT team or reach out to GRIDSMART Support for help with this.

1. Login to the GS2 Device Manager with an administrator account.
2. In the left-hand menu, click **Settings**.

****

1. Under the **Users** section, click the **LDAP** tile.



1. Change the **LDAP URL** to begin with “ldaps” without quotes.



1. Click the **Apply Changes** button.



1. At the top, click the **Trusted CA Certificate** tab.



1. Click the **Browser** button.



1. Select your certificate file and click **Open**.



1. Click the **Apply Certificate** button.

## 4.2 Troubleshooting Secure LDAP / LDAPS with JXplorer

This section will guide you through troubleshooting your LDAPS server using JXplorer client. This is an alternative way to verify LDAPS on your network from your own machine. You can find and download JXplorer from <http://jxplorer.org/>

1. Under **Security**, click on **Trusted Servers and CAs.** You should see the following window:
2. Select **Add Certificate.**
3. Find and select your Trusted CA Certificate for your network’s domain.
4. Confirm the details of your Trusted CA Certificate, then click **OK.**
5. Enter a unique name for the Trusted CA Certificate in JXplorer.
6. When prompted for **Key Store Password**, if you have not updated from the default password for JXplorer, the password is **changeit**.
7. If the Trusted CA Certificate is successfully imported, you should now see the entry with the unique name you chose.
8. Under **File**, click on **Connect.**
9. Enter the hostname for your LDAP server in the **Host** field.
10. Change the **Port** from 389 to 636, this is the LDAP SSL port.
11. Adjust the **Security** level to **SSL + User + Password** 
12. For **User DN,** you should enter the full domain name for the **Bind** account created on the LDAP server (**example:** uid=ldapbind,cn=users,dc=ldap,dc=mycompany,dc=com).
13. Enter the **Bind Password** that you created when you created your **Bind** account.
14. Once all settings are correct, click **OK**.

**Note:**

If everything is working, you should see a directory tree with users and user groups, appropriate for the various permissions groups.

The top three levels should be the domain for your LDAP server in reverse order. For example, the three levels from top to bottom would be **com**, **mycompany**, and **ldap** for a domain called **ldap.mycompany.com**.



# 5.0 GS2 LDAP Import/Export

## 5.1 Export/Import LDAP/AD settings

In order to make sharing an LDAP/AD configuration across multiple Processors easier, the GS2 allows users to export an existing LDAP configuration.

To export LDAP settings, navigate to **Settings** 🡪 **LDAP** 🡪 **Export** and click **Export LDAP Config**, and save the zip file that will contain the LDAP settings and certificate.



To import LDAP settings, navigate to **Settings** 🡪 **LDAP** and click **Import settings…**

You will be prompted to upload the .zip file exported in the previous section, which will apply LDAP settings and certificates to your processor.

****

# 6.0 Using Synology NAS

Synology offers an LDAP server add-on package. The following instructions will guide you through installing the LDAP server add-on package, configuring the package, and configuring the GS2 for LDAP authentication. While these steps are specific to implementing an LDAP server with a Synology NAS, the concepts are applicable to other LDAP implementations as well.

## 6.1 Installing DNS Server and LDAP Server on Synology NAS

1. From the DiskStation Manager Desktop, click the **Package Center** icon.



1. Search for **DNS**.



1. Click the **Install** button on the **DNS Server** tile.



1. Search for **LDAP**.



1. Click the **Install** button on the **LDAP Server** tile.



1. Close the **Package Center** window.

## 6.2 Configuring DNS Server on Synology NAS

1. From the DiskStation Manager Desktop, click the **Main Menu** button located in the top left screen corner.



1. Click the **DNS Server** icon to open the **DNS Server** window.



1. In the left divider column, click the **Resolution** tab.



1. Check the checkboxes for the following:
* **Enable resolution services**
* **Enable forwarders**
1. For **Forwarder 1**, provide your network’s current DNS IP address (This will route any domains not registered in this DNS server to the Forwarder DNS server. Consult with your IT or Networking department as needed).

**NOTE:** *You may use a Public DNS Provider, such as Google’s DNS IP address* ***8.8.8.8****.*

1. For **Forward policy**, select **Forward First**.



1. In the left divider column, click the **Zones** tab.



1. Click the **Create** button, then click the **Master zone** submenu item.



1. For **Domain type**, select **Forward Zone**.



1. For **Domain name**, use the desired domain name for your local network.
2. For **Master DNS server**, use the IP address of the NAS. It is recommended to assign a static IP address or have a DHCP reservation.



1. Uncheck all checkboxes.



1. Click the **OK** button.



## 6.3 Creating LDAP DNS Entry on Synology NAS

To reach your LDAP server by name, an entry must exist in DNS to resolve requests. This entry will establish your ***Fully Qualified Domain Name*** *(FQDN)* for future LDAP client configurations.

NOTE: In our example, the *Fully Qualified Domain Name* *(FQDN)* is **ldap.mycompany.com**.

1. In the **DNS Server** window, double-click the entry you previously created when configuring DNS.



1. The **Edit Resource Record** window will pop-up.



1. Click the **Create** button, then click the **A Type** submenu item.



1. The **Add Resource Record A** window will pop-up.



1. For **Name**, provide a unique name for your LDAP server.



1. For **IP address**, use the static or DHCP IP address of the NAS.



1. Click the **OK** button.



1. In our example, the **Fully Qualified Domain Name** is **ldap.mycompany.com**.



1. On the **Edit Resource Record** window, click the **Finish** button.

## 6.4 Creating GS2 DNS Entry on Synology NAS

In order to reach your GS2 by name, an entry must exist in DNS to resolve requests.

1. In the **DNS Server** window, double-click the entry you previously created when configuring DNS.



1. The **Edit Resource Record** window will be displayed.



1. Click the **Create** button, then click the **A Type** submenu item.



1. The **Add Resource Record A** window will pop-up.



1. For **Name**, provide a unique name for your GS2, such as GS1234.



1. For **IP address**, use the static IP address of the GS2.



1. Click the **OK** button.



1. On the **Edit Resource Record** window, click the **Finish** button.



## 6.5 Configuring LDAP Server on Synology NAS

1. From the DiskStation Manager Desktop, click the **Main Menu** button located in the top left screen corner.



1. Click the **LDAP Server** icon to open the **LDAP Server** window.



1. Select **Enable LDAP Server**.



1. Select **As the Provider server**.



1. Provide the Fully Qualified Domain Name of the LDAP Server and a strong password.



1. Select **Apply**.



1. After changes are applied, the **Authentication Information** will provide the **Base DN** and **Bind DN** for configuring client connections.



## 6.6 Adding LDAP Group on Synology NAS

This section will guide you through the process of adding a group to Synology’s LDAP Server. A group is associated to a user account, granting a specific permission.

The GS2 has three permission levels corresponding to three unique LDAP groups.

|  |  |
| --- | --- |
| **Permission** | **Example** |
| Admin | gsadmin |
| Publish | gspublish |
| View Only | gsviewonly |

1. In the **LDAP Server** window, click the **Manage Groups** tab in the left divider column.



1. Click the **Create** button.



1. For **Group name**, provide a unique name for the group.



1. For **Group description**, provide the permission level this group will grant.



1. Click the **Next** button.



1. Review your settings.



1. Click the **Apply** button.



## 6.7 Adding LDAP User on Synology NAS

This section will show you how to configure a user on Synology’s LDAP Server. A user can authenticate and be granted permissions based on associated groups. Our example entry will establish the **Bind** user to configure future LDAP clients. This **Bind** user will be used later for configuration on the GS2.

1. In the **LDAP Server** window, click the **Manage Users** tab in the left divider column.



1. Click the **Create** button.



1. For N**ame**, provide a unique name for the user.



1. For **Password**, choose a strong password to secure your LDAP Server and then repeat for **Confirm password**. You will use this password later for configuration on the GS2.



1. Click the **Next** button.



1. Select the groups to associate with this user account. Our example is for the **Bind** account and should only have the **users** group associated.



1. Click the **Next** button.



1. Click the **Next** button.



1. Review your settings.



1. Click the **Apply** button.

