SMS 2.0 SSO / LDAP Launch Kit

SMS 2.0 SSO/ LDAP Launch Kit

Table of Contents

What options are available in SMS 2.0 for Single Sign On?

LDAP (Lightweight Directory Access Protocol)

LDAP is an industry standard protocol that allows an application like Skyward to authenticate to a 3rd party LDAP directory like Microsoft's Active Directory or Novell's eDirectory.

In general terms you can think of an LDAP server as a phone book that has the usernames and passwords for the district users. Skyward can take advantage of this "phone book" by allowing it to be used to log into Skyward. The advantage is end users have one less password to remember.

In more technical terms the LDAP implementation allows users to use network credentials to log into SMS 2.0, including the web-based products like EA+ and Employee Access. User accounts can be in Windows Active Directory, Novell eDirectory, or any other third-party LDAP compliant directory. The LDAP Group Integration feature allows SMS 2.0 to read group memberships from your Network directory and then add them to linked Security Groups.

Single Sign On using SkySTS (Skyward Secure Token Service)

SkySTS allows SMS 2.0 users to authenticate to an **Id**entity **P**rovider (IdP) for 3rd party systems, and it allows SMS 2.0 to be an Identity Provider (IdP) for 3rd party systems.

SMS 2.0 to a remote IdP: This means the SMS 2.0 users can log in using credentials from a 3rd party IdP, such as Office 365 (Azure) or ClassLink, using SAML 2. For an overview video of the Single Sign-On process for your Skyward end-users and other recommended Skyward Security Best Practices, please visit our link to the Skyward Security Best Practices Blog.

SMS 2.0 as an IdP: This means that users of the 3rd party system can login into the 3rd party system using their SMS 2.0 user/password using SAML 1, 2, or wsFed. This has been popular for customers authenticating guardians (parents), SMS 2.0 is one of the few systems that has usernames & passwords for the parents, so when a school is looking to roll out a new 3rd party product to parents they can set it up to authenticate to SMS 2.0 using SkySTS. SMS 2.0 becomes the IdP, which means we provide the authentication for the 3rd party product. If LDAP is configured inside of SMS 2.0 for the user type, then the user would use the LDAP user/password.

Note: SkySTS is not compatible with the Business PaC Client (Point and Click) or Mobile App (Available in the iOS and Android app stores).

Frequently Asked Questions

How do I know if I already use LDAP?

Review the LDAP Tutorial: http://support.skyward.com/FAQ/View.aspx?ID=483059
(Support Center Login required)

What Features does LDAP Support?

- Supports encryption using LDAP w/TLS, LDAPS, or Kerberos
- Allows you to define up to three LDAP Servers for redundancy
- Allows you to specify the user types that will authenticate to each LDAP Server.
- Optional LDAP Group Membership Integration reads group memberships from your LDAP directory and manages Security Group memberships in Skyward.

Can Cloud Hosted (ISCorp) Customers use Single Sign On?

Yes, Cloud Hosted Customers can implement LDAP or SkySTS. When implementing these features across the internet a Secure protocol is used to encrypt the network traffic. To further secure access to your LDAP servers, lock down the traffic from the following source IP addresses.

ISCorp LDAP source address - Mequon, WI - 66.195.143.42

Note: IP Address 66.195.143.42 to be deprecated starting 8-16-2020.

New ISCorp LDAP source address - Mequon, WI – 192.222.0.56

ISCorp LDAP source address - Dallas, TX - 8.12.72.20

Note: Adding all ISCorp LDAP source address(es) is recommended, after 8-16-2020 please remove the deprecated IP Address.

Does LDAP support automatic sign-on?

The SMS 2.0 PaC client has the optional ability to automatically log on as the currently logged-on workstation user in Windows. This can be a security risk however, since any user could sit down at a logged-on user's workstation and gain access to the PaC software as the logged-on user. Because of this feature, we recommend districts take this risk into consideration before turning on that option.

The SMS 2.0 Web Applications do not support an automatic sign-on. To log into the Web Application the end user always enters their network username and password.

What tools are available for managing existing users in Skyward?

Skyward has several tools that assist you with implementing LDAP. **An important requirement of LDAP is that the skyward usernames match the LDAP usernames. Example: If the user's network login name is "jdoe" then the skyward login name must also be "jdoe".**

The following tutorials have the details on how to mass change or import the skyward logins to match the Active Directory or eDirectory login names. It is strongly recommended that you test your LDAP setup using a training database prior to running the utility (ies) on your live database.

Mass Changing Login names

How do I mass change Student Login names?

http://support.skyward.com/FAQ/View.aspx?ID=1062348
(Support Center Login required)

How do I mass change Employee Login names?

http://support.skyward.com/FAQ/View.aspx?ID=1112165
(Support Center Login required)

What tools are available for importing users in Skyward?

Student Import Tool (Student Suite) – automates the import of student users, passwords from a csv file. The Student import tool is found at the menu path of Web Student \ Students \ Student Access \ Setup \ Utilities \ Mass Generate Student Permissions and Passwords. The file format of the csv file can be viewed by clicking the "Preview Import File Format" hyperlink.

Staff Import Tool (Student Suite) – automate the import of staff users, passwords from a csv file. The Staff import tool is found at the menu path of Web Student \ Administration \ Skybuild \ Import \ Staff Import Utility. The file format of the csv file can be viewed by clicking the "Format" button.

Employee Import Tool (Business Suite) – automate the import of employee users. This Employee Import tool is known as the **Applicant Import Utility** and imports employees into a SMS 2.0 business database from an import file. The Applicant Import Utility is a licensed feature that was available starting in the June 2016 release. If you are interested, please contact your Account Representative.

Does SMS 2.0 work with 3rd party Account Automation / Identity Management products?

If your district wishes to do Identity Management beyond the capabilities of the user utilities provided by Skyward there are several ways to automate the creation of accounts, below are some examples

3rd Party solutions

Skyward has partnered with the Tools4ever UMRA solution to provide an Identity Management solution that provisions user accounts from Skyward Student or Business Suites to a variety of systems, including Active Directory. UMRA is our preferred IDM partner but Skyward can be used with any 3rd party IDM solution.

With the Skyward SIF agent and 3rd party ZIS and Active Directory Agents Active Directory accounts can be automatically provisioned when they are added to Skyward Student or Business Suites...

What are the PaC Client requirements?

There are no special requirements to use LDAP with the full PaC client. In Active Directory environments with single sign-on enabled, users can be automatically logged into the PaC client or with single sign-on disabled, users can be required to enter a network username and password. In Novell eDirectory environments the user will need to enter the network username and password to log into the full PaC Client.

When Logging into the PaC Client in a Terminal Server Environment and the automatic logon option is enabled and PaC is running in a terminal server environment, the network credentials that will be used to log on to PaC will be the ones used to log onto the terminal server, not the ones used to log onto the local client workstation.

PaC does not support SkySTS.

How LDAP work in the SMS 2.0 Web Applications?

The actual authentication happens on the SMS 2.0 Web server in a Web speed environment. The webserver(s) must be able to communicate to the LDAP server so the LDAP traffic must be allowed on the firewall, most notably when the web server is in a DMZ or outside the firewall (Cloud Hosted). If the LDAP requests are being made across a public network then you must use Kerberos, SSL/TLS, or LDAPS to encrypt the usernames and passwords.

Implementing Single Sign On using SkySTS

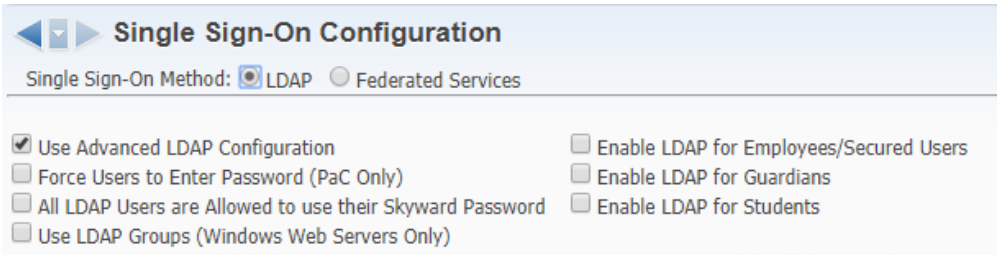
SMS 2.0 supports Single Sign On to a 3rd party Identity Provider like Google or Microsoft Azure / Office 365, ClassLink, or others that support SAML 2. Implementation details are found in the SMS 2.0 SkySTS Launch Kit. If you have questions please contact IT Services by creating an IT Services Service call at https://support.skward.com (Support Center Login Required)

Configuring LDAP

Step 1: Configure LDAP Global Options

1. Navigate to Product Setup -> Skyward Contact Access -> District Setup -> **Single Sign-On Configuration**.

2. Set the **Single Sign-On Method to LDAP** and enable the **Use Advanced LDAP Configuration** checkbox.



3. **Configure: All LDAP Users are allowed to use their Skyward Password**

   Enabling this feature is recommended for the initial testing phase of the LDAP configuration. This option allows all users to continue to login using both the SMS 2.0 and LDAP username and password. Once LDAP is tested and working as expected Skyward recommends that this feature be disabled. Allowing users to use the SMS 2.0 passwords is a security risk; it leaves a back door using the skyward login and password that may not be maintained.

4. **Configure: Force User to Enter Password (PaC Only)**

   This option is only available if the Server Type is set to Windows. If this option is not checked, and 'Password Authentication' is set to either 'LDAP' or 'Both', the system will automatically log you in with your network user name and password, if the user name exists in the SMS 2.0 product (the passwords do not need to be the same). This setting has no effect with Novell eDirectory or SMS 2.0 web applications.

5. **Configure: Use LDAP Groups (Windows Web Servers Only)**
   Enabling this feature allows you to integrate the LDAP directory groups for SMS 2.0 user security. Users' group memberships are read transparently from the LDAP directory during the user's login process allowing you to manage group memberships exclusively from your LDAP Directory.

   See also: Configure the LDAP Group Membership Integration

6. **Choose the Types of Users that will use LDAP**

   Enable LDAP for Employees/Secured Users: Controls the ability for Employees and Secured users to authenticate using their LDAP username and password. Employees and Secured users include teachers as they are Secured Users.

   Enable LDAP for Guardians: Controls the ability for Guardians to authenticate using their LDAP username and password.

   Enable LDAP for Students: Controls the ability for Students to authenticate using their LDAP username and password.

   Tech Note: LDAP Security Group or User Override
   You can override the LDAP setting on the security of an individual user or group of users that allows those users to use their Skyward password.

   The Allow Use of Skyward Password setting is also available on Security Groups found under Product Setup → Skyward Contact Access → Security Groups.

   The tutorial below shows you how to setup the security of individual users, so they can login using their Skyward password. This is an individual user setting that allows these users to override the LDAP only configuration. We recommend this only be set for a small group of high-level skyward users.

   Individual User LDAP Override Tutorial:
   http://www.skyward.com/DeptDocs/Corporate/Documentation/Public%20Website/Tutorials/Software/PS_CA_SE_US_991530_100_T.htm
   (Support Center Login required)

Step 2: Configure LDAP: Server(s)

1. Choose the LDAP Method

Specifies the protocol used to communicate to the LDAP server.

- **Simple*** - LDAP with no encryption (port 389 clear text)

Simple should only be used for testing. When Simple LDAP is used usernames and passwords are transmitted in clear text, it might allow an attacker to intercept your usernames and passwords.

- **Simple with Kerberos –** Secure LDAP using Kerberos encryption (port 389 encrypted)
- **SSL/TLS –** Secure LDAP using TLS Encryption (port 389 encrypted)
- **LDAPS** -Secure LDAP using LDAPS (port 636 encrypted)

Kerberos (Windows to AD Only)

Check this checkbox if using Windows Skyward Web servers and an Active Directory Domain for authentication. This option overrides the Simple Method and always uses secure communication by enabling Kerberos for encryption (port 389 encrypted). If you are using Kerberos and are not using the Group Membership Integration, then the only required configuration fields are Server Name and Name Types.

LDAPS/TLS Requirements

LDAPS or LDAP w/TLS are the recommended encryption options. Both require an SSL certificate to be installed on the Web / PaC servers which is detailed here. Cloud Hosted Customers must send the exported certificate to their hosting provider to be installed on their SMS 2.0 Web / PaC Servers.

- Both Reverse and Forward DNS entries must exist for the LDAP Host
- The Server Name must be entered as the FQDN (Fully Qualified Domain Name) of the LDAP Host
- The LDAP SSL Certificate must match the LDAP Host FQDN
- The LDAP Host Certificate Authority must be installed on the Skyward Web Servers and PaC Client Server/Workstations (PaC is only used for Business).

2. Disable Follow Referrals

- **Disabled** (Unchecked) **Recommended** setting for the best LDAP query performance, when enabled LDAP queries will not follow referrals.
- **Enabled** (Checked) LDAP queries will follow referrals. Referrals may be required if the LDAP server being queried does not hold a copy of the entire Network Directory, but this LDAP Server configuration is rare.

3. Configure: Server Name

Identifies the Host Name and port of the LDAP server. You can enter the ip address or DNS hostname of the LDAP server, if using TLS or LDAPS the hostname entered must match the common name of the SSL certificate. If no port is entered the system will use port 389 or 636 (LDAPS). To use custom LDAP ports, enter the server information using this format: **HOSTNAME:PORT**

4. Configure: Domain Name

Identifies the name of the Active Directory domain, not required for Kerberos.

Tech Note: Important for Active Directory Environments:
Check your Active Directory configuration to ensure that the guest account is not enabled. Microsoft and Skyward strongly recommends against enabling the Active Directory guest account for security purposes.

How do I disable the Guest Account for LDAP?
https://support.skyward.com/FAQ/View.aspx?ID=1110789
(Support Center Login required)

5. Configure: Name Types (Use Control Click to select multiple Name Types)

Choose the name types that will be used by the LDAP Server

- **EMPLOYEE** – Employee Users (Employee Access)
- **GUARDIAN –** Guardians (Family Access)
- **SECURITY USER –** Security Users (All Systems; non-EA, EA+, SA, FA only users)
- **STAFF –** Staff Users (Educator Access + / Teacher Access)
- **STUDENT –** Student Users (Student Access)

6. Configure: LDAP Search (optional)

Search Base DN

The Search Base DN is required if you are using the LDAP Group Integration. It can be used to improve the lookup performance for large directories. By default, the system will search the entire directory to find the DN of the user. If you would like to limit the search to a specific part of the directory, specify the DN of the location where the search should start.

If you are using LDAP/LDAPS the Search Base DN must be entered using LDAP notation (example: ou=users. Sites that use Kerberos would enter the container name without LDAP notation (example: users)

Tech Note: After entering the Search Base DN, tab through the Filter field to automatically populate the default filter.

Filter (%s-login):

The Default search filter is displayed below and should only be modified if familiar with LDAP searches. The Filter field will populate automatically after you enter the Search Base DN.
DN(&(objectclass=person)(|(cn=%s)(uid=%s)(sAMAccountName=%s)))

Search User DN

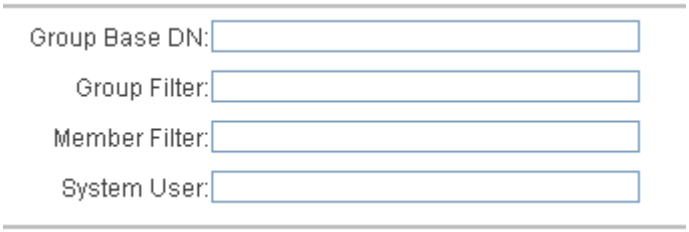
The Search User DN is optional. Enter the DN (distinguished name) of the Search User to use. If this field is not filled in, the system will attempt an anonymous connection to search for the DN of the user.

1. A service account should be created as a logon account for searching the LDAP tree.
2. Use the service account information for the **Search User DN** and **Search User Password**.

Search User Password

If a Search User DN field is used, enter the password for that user.

7. Configure LDAP Groups Search (required if using LDAP Groups)



Group Base DN

The Group Base DN is required if you are using the LDAP Group Integration... By default, the system will search the entire directory to find the DN of the group. If you would like to limit the search to a specific part of your directory, specify the DN of the location where the search should start using LDAP notation.

If you are using LDAP/LDAPS the Group Base DN must be entered using LDAP notation (example: ou=users. Sites that use Kerberos would enter the container name without LDAP notation (example: users)

Note: After entering the Group Base DN, tab through the Group Filter and Member Filter fields to automatically populate the default filters.

Group Filter

The Default search filter is displayed below and should only be modified if familiar with LDAP searches. The Group Filter field will populate automatically after the Group Base DN is entered.
(&(objectclass=group)(member=%s))

Member Filter

The Default search filter is displayed below and should only be modified if familiar with LDAP searches. The Member Filter field will populate automatically after the Group Base DN is entered.
(&(objectClass=user)(MemberOf=%s))

Active Directory Nested Groups (Optional)

Active Directory Nested Groups are supported. Group nesting is when you add a group as a member of another group.

Nested Groups requires a special member filter documented in this Microsoft Article: https://msdn.microsoft.com/en-us/library/aa746475(v=vs.85).aspx
In our experience it will take longer to query the members of groups when utilizing the Nested Group member filter. The longer LDAP queries means that users will experience slower logins to SMS 2.0; this is a downside of using Active Directory nested groups... If using Nested Groups, change the member filter to:
(&(objectClass=user)member:1.2.840.113556.1.4.1941:MemberOf=%s))

System User

The system user value is used to get the group's members and is optional. Common values for the system are CN (eDirectory), UID, Principal Name (AD/eDir), or sAMAccountName (AD).

Step 3: Adding self-signed certificates to the SMS 2.0 Web Server(s)

If you are using LDAP w/TLS or LDAPS to connect to the LDAP Server(s), the SSL certificate used by the LDAP Server(s) must be trusted by the SMS 2.0 Web Server(s). The certificate must be added to the Web Server(s) certificate store or sent to the hosting provider to be installed on the Web Server(s).

Install the Certificate on all SMS 2.0 Web Server(s)

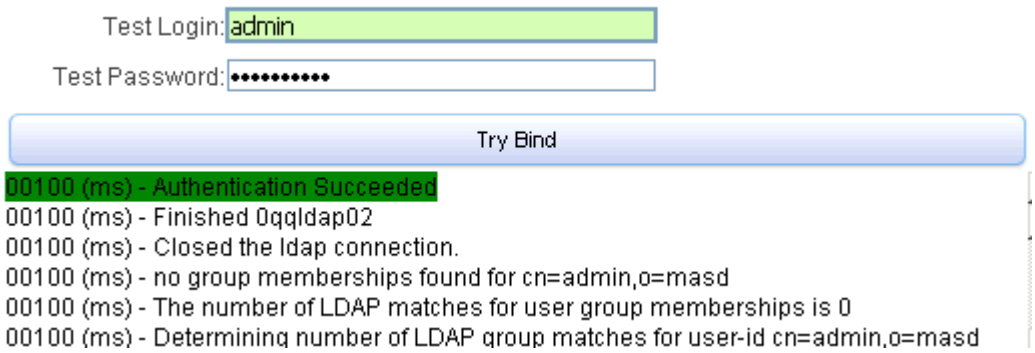
1. From the web server run line type MMC and hit enter
2. File | Add/Remove Snap-in
3. From the list choose Certificates and then the add button
4. Choose Computer account and select Next |Finish | Ok
5. Click the plus sign to the right of Certificates (Local Computer) and expand Trusted Root Certification Authorities and then Certificates
6. Right click Certificates | All Tasks | Import | Next
7. Browse to the certificate file that was exported and select Next |Next |Finish

Configure the PaC client to work with the Self signed certificate.

1. From the workstation run line type MMC and hit enter
2. File | Add/Remove Snap-in
3. From the list choose Certificates and then the add button
4. Choose Computer account and select Next |Finish | Ok
5. Click the plus sign to the right of Certificates (Local Computer) and expand Trusted Root Certification Authorities and then Certificates
6. Right click Certificates | All Tasks | Import | Next
7. Browse to the certificate file that was exported and select Next |Next |Finish
8. Now PaC will be able to authenticate using LDAP.

Tech Note: Cloud Hosted Customers must send the exported certificate to their hosting provider to be installed on their SMS 2.0 Web / PaC Servers.

Step 4: Test LDAP Settings



1. **Test Login**

   Enter a valid login name for your LDAP or Active Directory Domain

2. **Test Password**

   Enter the password for the Test Login account

3. **Try Bind**

   After entering the Test Login information, click the Try Bind button to test the configuration. A green Authentication Succeeded message should display if successful. If the Test Authentication is not successful scroll through the log and review it for errors.

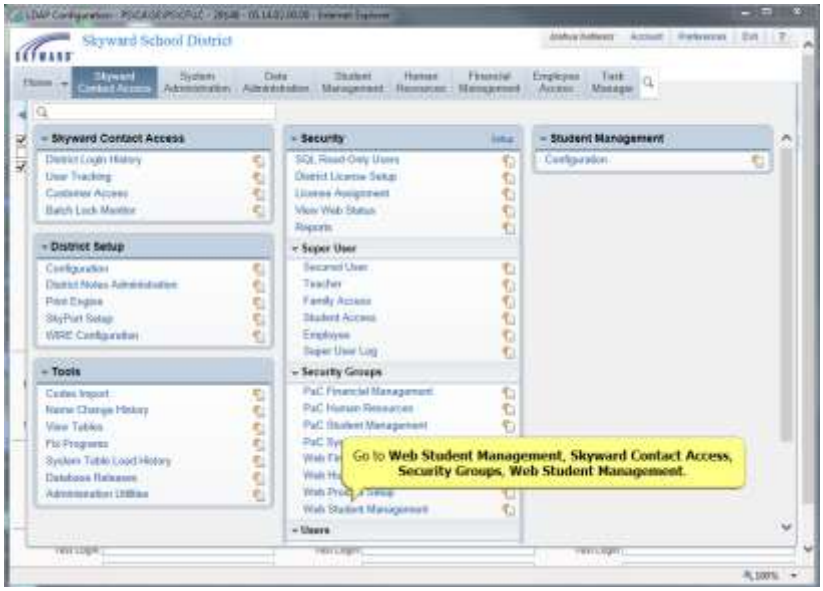
Common LDAP Issues:

- The SMS 2.0 Web Server must be able to communicate with the LDAP Server using the host name or IP Address specified, and the LDAP port used must be open between the SMS 2.0 Web server and the LDAP Server.
- If using LDAP w/TLS or LDAPS the SSL certificate must be trusted by the SMS 2.0 Web Server(s). If using self-signed certificates, the certificate must be added to the Web Server(s) certificate store or sent to the hosting provider to be installed on the Web Server(s).
- If using LDAPS the LDAP Server name must match the LDAP SSL Security Certificate.
- You can troubleshoot LDAP connectivity by installing a free LDAP Browser like the Softerra LDAP Browser on the SMS 2.0 Web Server.

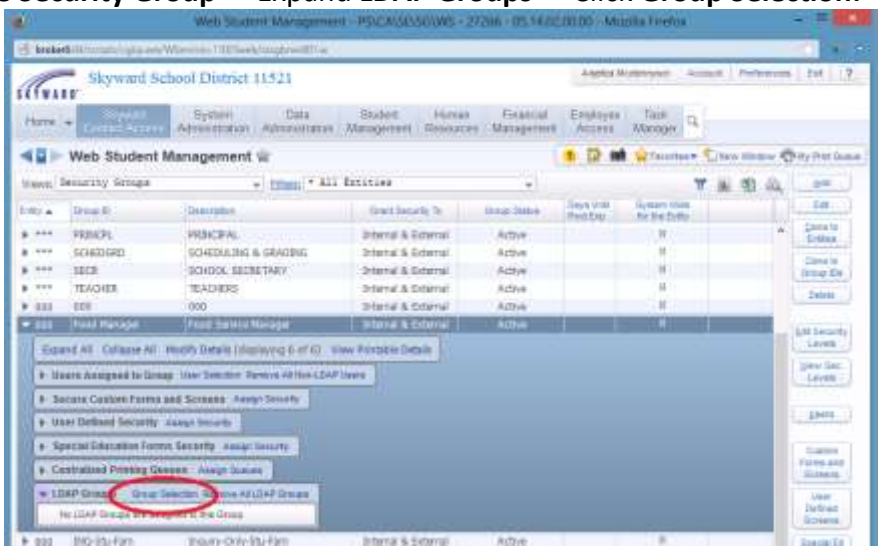
Configure the LDAP Group Membership Integration

Step 1: LDAP Group Maintenance: Link Security Groups to LDAP Groups

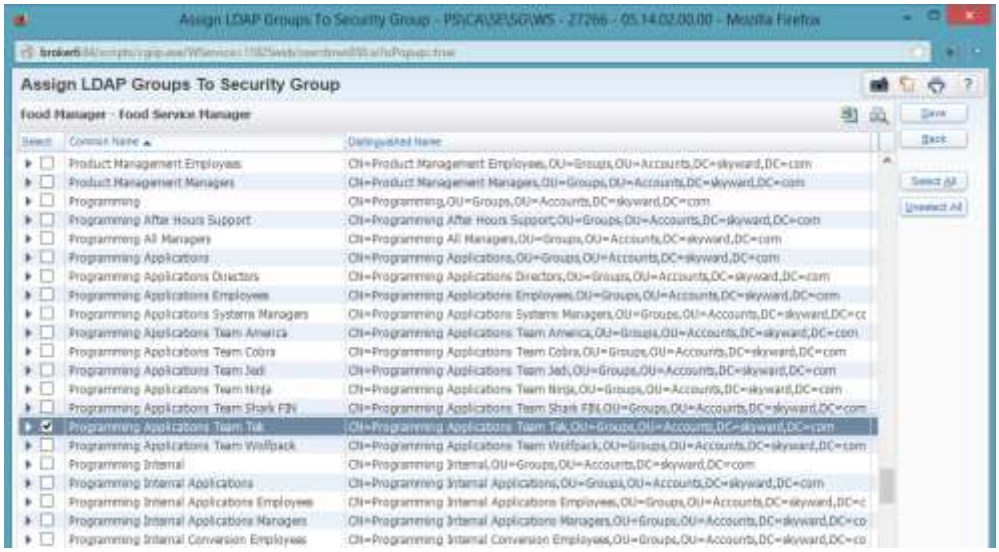
After the **LDAP group** feature has been enabled and configured, **LDAP Groups** can be linked to **Skyward Security groups**. To link a Security Group, browse to Product Setup -> Skyward Contact Access -> Security Groups -> and choose the Product area that you wish to manage.



Expand the **Security Group** -> Expand **LDAP Groups** -> Click **Group Selection.**

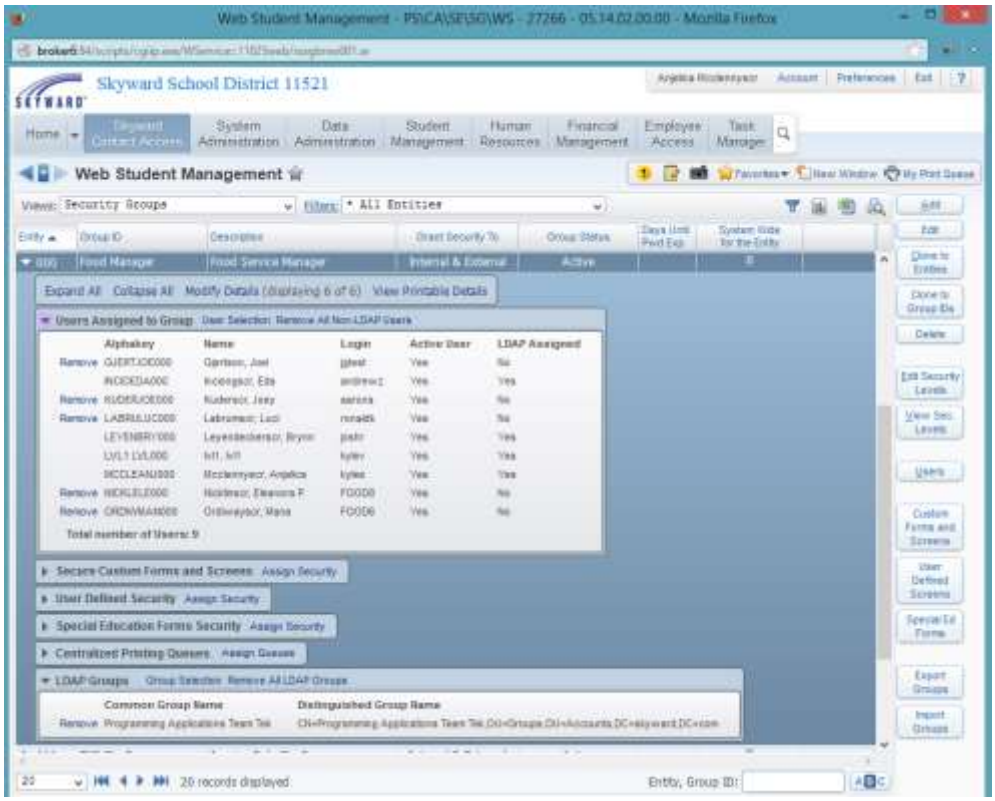


Choose the **LDAP Groups** that should be associated to the **Skyward Security Group** -> The members of the LDAP Group will inherit the skyward application security setup in the Security Group. LDAP Group Membership is verified and updated on every successful user login



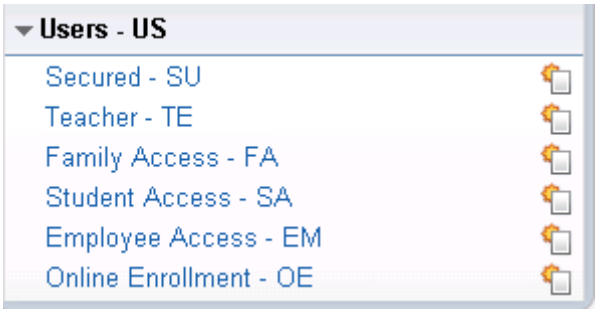
Step 2: LDAP Group Maintenance: Security Group Membership

To view the Security Group memberships, expand the **Users Assigned to Group**. Users that have been assigned to security groups by LDAP are indicated in the column labeled **LDAP Assigned**. The LDAP groups attached to the security group are displayed under the **LDAP Groups** detail area.

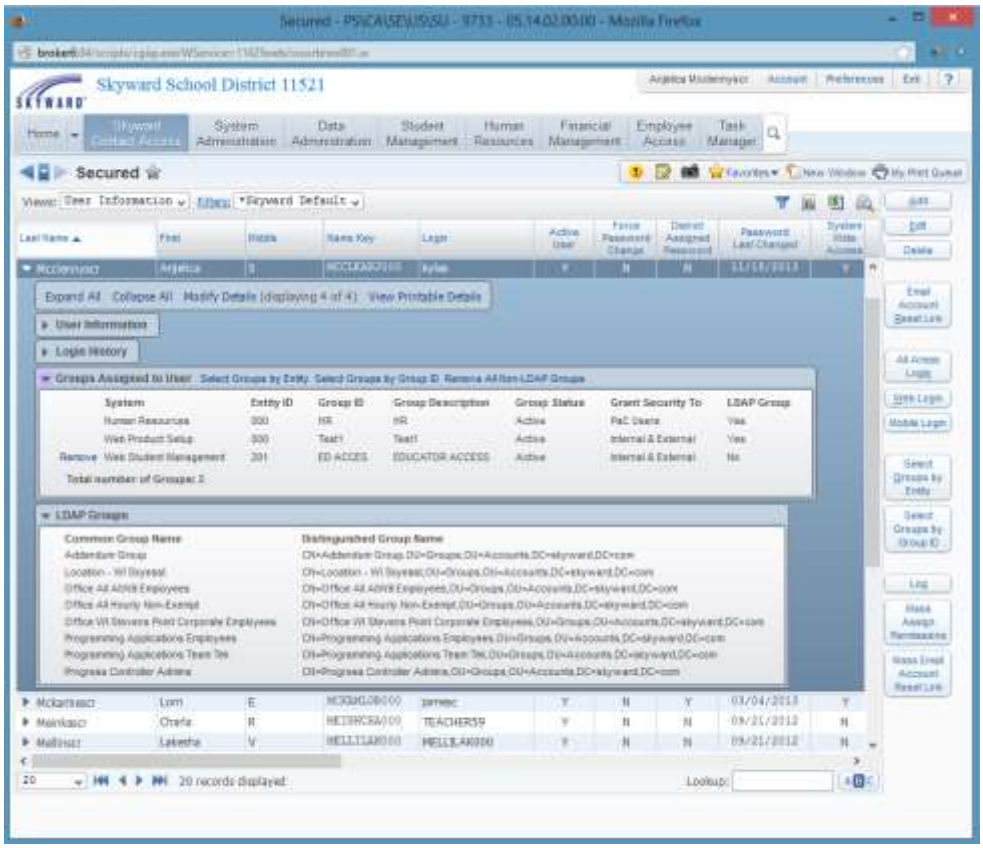


Step 3: LDAP Group Maintenance: Groups assigned to Users

To view **LDAP Group** information for individual users, browse to Product Setup -> Skyward Contact Access -> Users -> and select a browse from the Users menu.

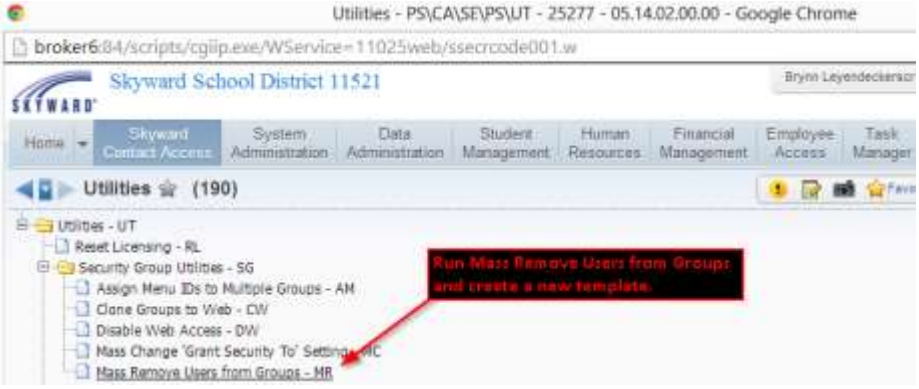


Expand a username, the **Groups Assigned to User** will indicate if the group was assigned by LDAP. There is also a **LDAP Groups** detail section that displays all the LDAP groups the user is in.

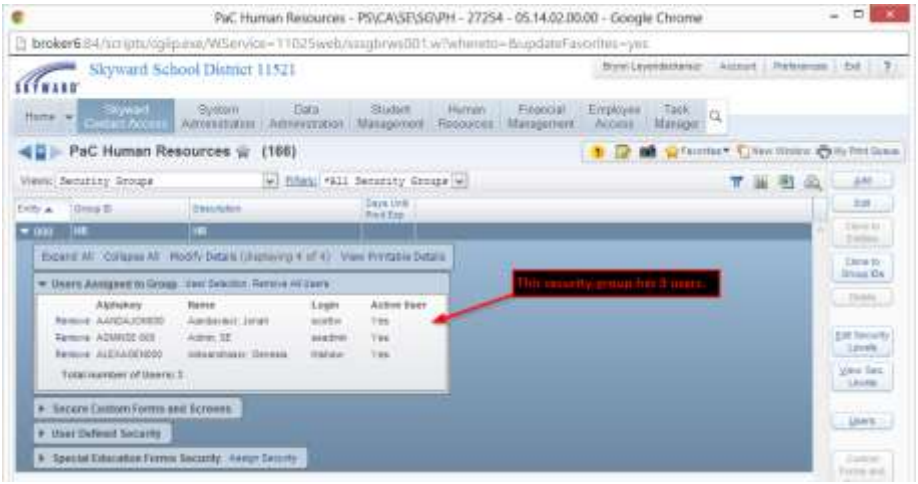


Step 4: LDAP Group Maintenance: Mass Remove Users from Groups (optional)

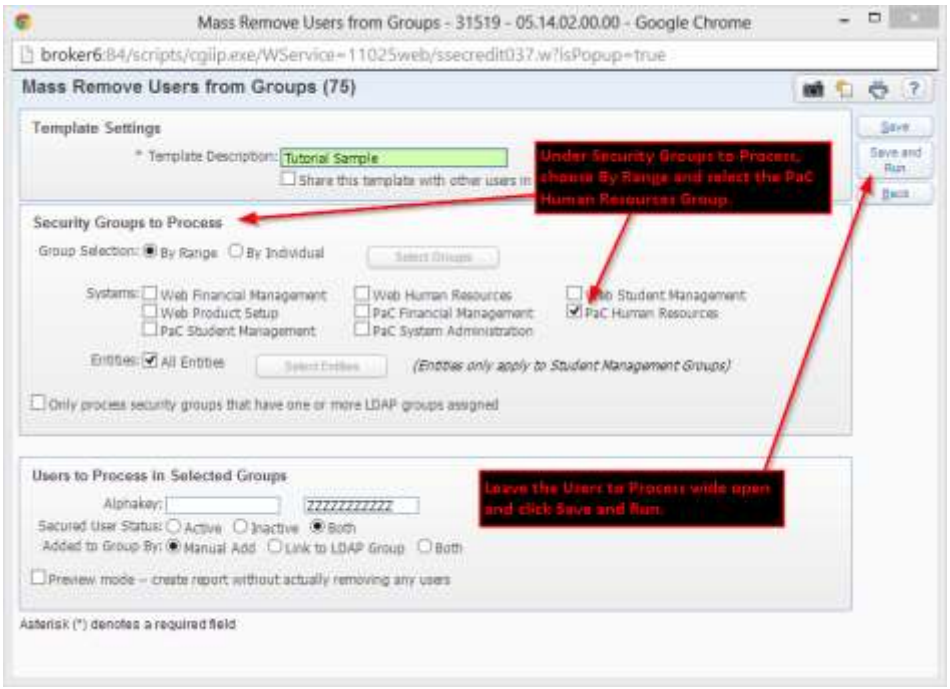
Skyward created a utility for districts who want to move from the traditional Security Group membership to an all **LDAP Group** membership or vice versa. Browse to Product Setup -> Skyward Contact Access -> Security -> Setup -> Utilities -> **Mass Remove User from Groups.**



The screenshot below shows a Group named HR that has three (3) traditional active Security Group members. The **Mass Remove Users from Groups** will remove the Security Group members.



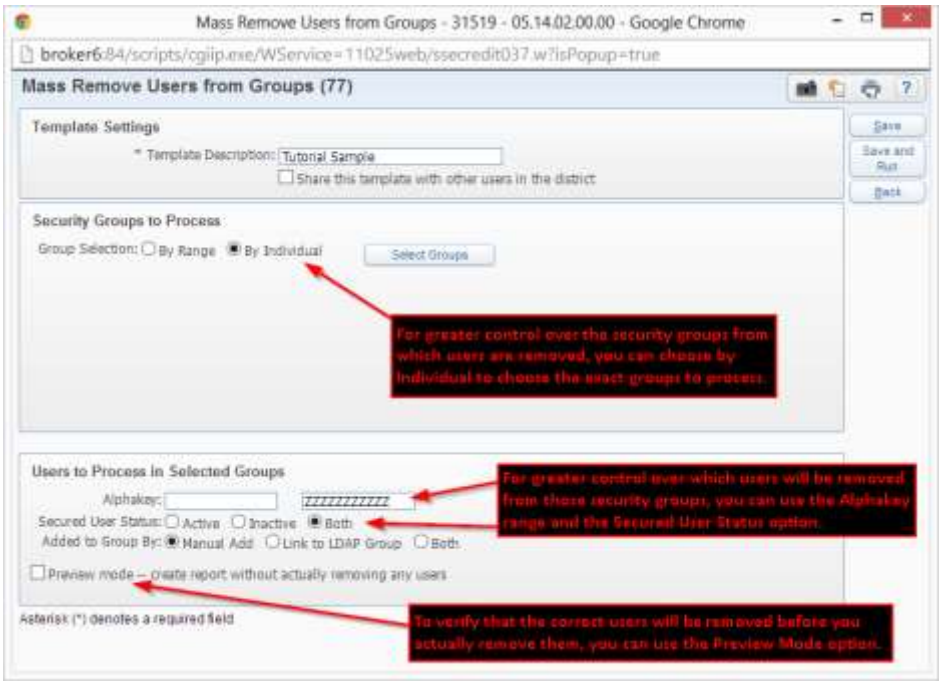
The **Mass Remove Users from Groups** utility allows you mass change group membership based on the criteria chosen.



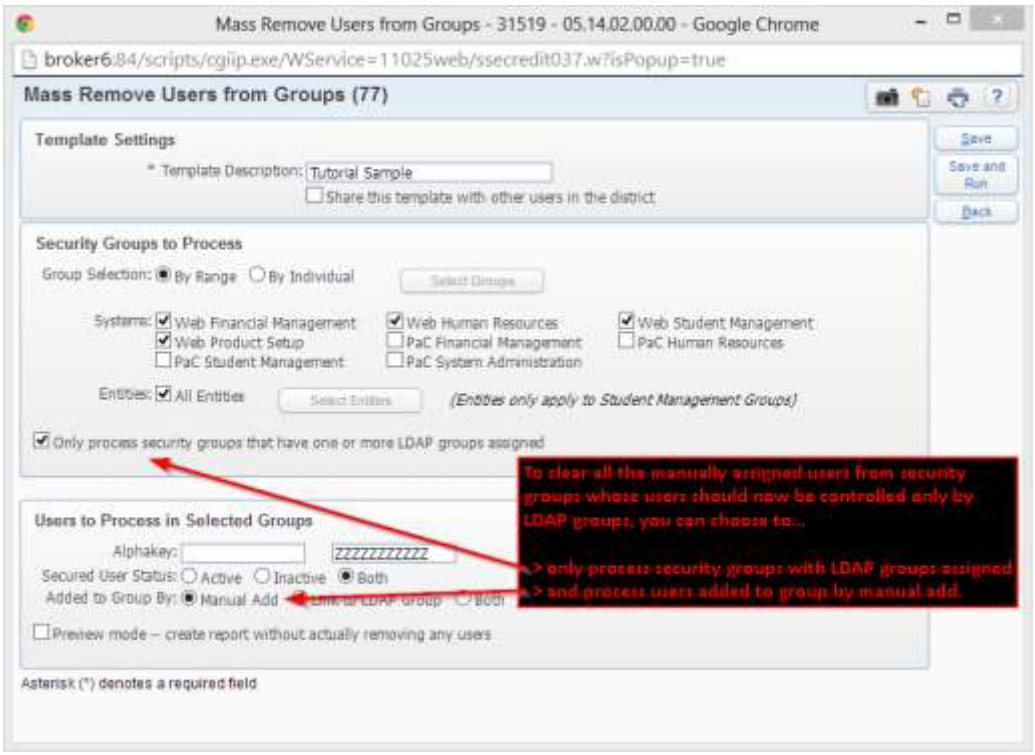
Mass Remove Users from Groups sample report showing the users that were removed from the HR group.

The **Mass Remove Users from Groups** utility has successfully removed the three (3) members.

The **Mass Remove Users from Groups** utility has many options that gives control over what groups to modify.



The **Mass Remove Users from Groups** utility allows modification of Skyward Security groups that have LDAP groups assigned to them.



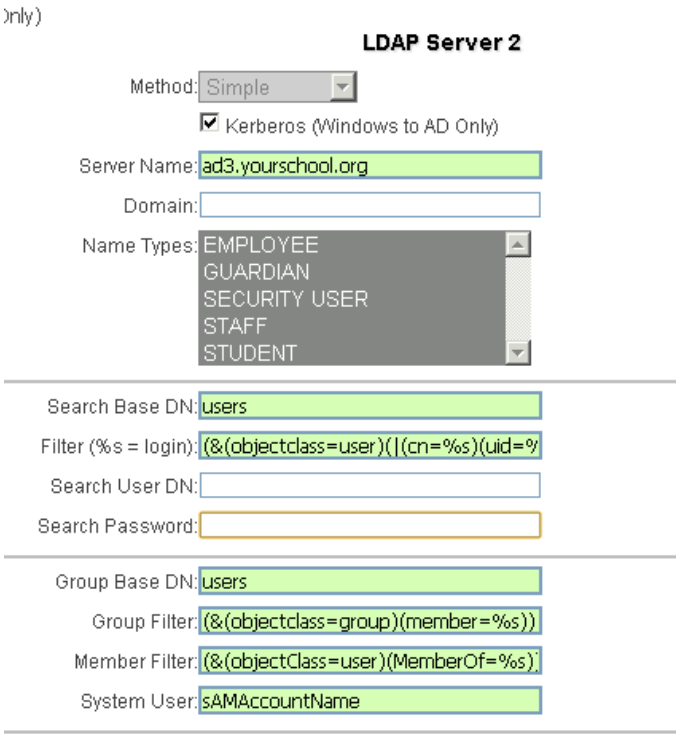
LDAP Server Configuration Examples

Configure LDAP: Windows Active Directory LDAP Kerberos Example

1. Select Kerberos (Windows to AD Only)
2. Enter (3) Windows Domain Controllers Server Names. The servers in the example are accessible using the hostnames one.yourschool.org, two.yourschool.org, and three.yourschool.org.
3. Enter the Domain for the Active Directory Domain named yourschool.org
4. Select all Name Types Selected for all three LDAP Servers

Configure LDAP: Windows Active Directory LDAP Kerberos Group Example

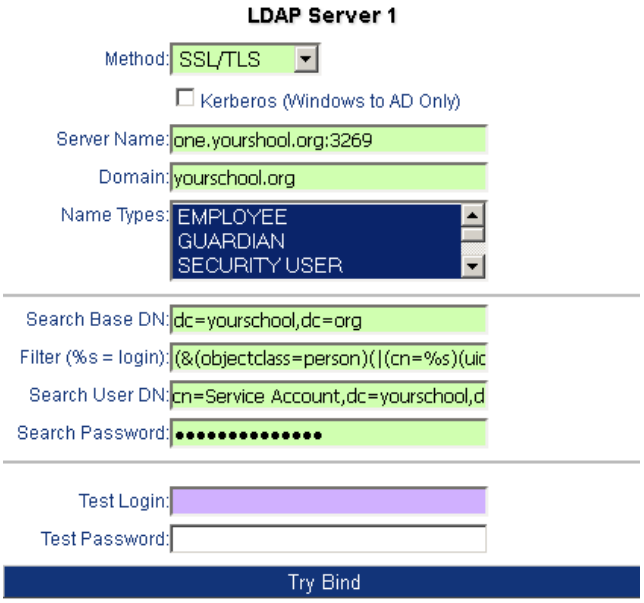
1. Enable the Use Groups Configuration option.
2. Select Kerberos (Windows to AD Only)
3. Enter the Server Name, Domain Name, and select name types.
4. Enter Search Base DN, tab to the Group Base DN
5. Enter Group Base DN, tab to the Test Login.
6. Enter Test Login / Password and click Try Bind.



Configure LDAP: Active Directory Global Catalog LDAP SSL/TLS Example

If your school district has multiple Active Directory (AD) domains in the same forest, then you can setup Skyward to use the AD global catalog that runs on port the secure LDAP port 3269. Before implementing the Global Catalog, settings make certain the AD server is a global catalog because not all domain controllers are also global catalogs. The global catalog role can be viewed from Active Directory Sites and Services by looking at the Properties of the Domain Controllers NTDS Properties.

1. Select SSL/TLS to use TLS encryption option.
2. Enter Global Catalog Server Name and port.
3. Enter the Domain Name.
4. Select the Name Types desired for the LDAP Server.
5. Enter the Search Base DN, in our example we are searches will start from the domain named **"dc=yourschool.dc-org".** Any part of the domain name will be '**dc='**. For example, the domain yourschool.org becomes **'dc=yourschool,dc=org'**. In an AD environment The Computers, Users, Built-in, and ForeignSecurityPrincipals folders are not OU's, even though they look similar.
6. Enter the Search User DN. In this example we created an account name "Service Account" and it would have a DN of **'cn=Service Account,dc=yourschool,dc=org'**. The **CN** property is going to be the **Display Name** of the user, not the login name. The **sAMAccountName** property is going to be the **Pre-Windows 2000 login name** for the user.
7. Enter the Search password of the Search User account.



Configure LDAP: Secure LDAP SSL/TLS Example (Novell eDirectory)

Using iManager to export a Self-Signed Certificate

1. Go to Novell Certificate Access | Server Certificates
2. Check the box next to the SSL CertificateDNS and click Export on the top menu
3. Under the Certificates: drop down select the certificate that has Organizational CA in the name
4. Select the DER format and select Next
5. Click on Save Exported Certificate.
6. Save the certificate to the local disk with an extension of .crt ext orgca.crt
7. Exit out of iManager

Configure LDAP w/TLS LDAP Server(s)

1. Select SSL/TLS to use the standard 389 port with TLS encryption.
2. Enter (3) Novell eDirectory Server Names. The servers in the example are accessible using the hostnames one.yourschool.org, two.yourschool.org, and three.yourschool.org.
3. Select the Name Types desired for all three LDAP Servers.
4. Enter the Search Base DN, in our example we are searches will start from the organization named **"sd".**
5. Enter the Search User DN for all three LDAP Servers. In this example the LDAP Service Account "ldapproxy" has been created in an organization unit named users in the "sd" organization. The Service Account would have a DN of **'cn=ldapproxy,ou=users,o=sd'**.
6. Enter the Search password of the Search User account for all three servers.

Configure LDAP: Secure LDAPS Group Example (Novell eDirectory)

1. Enable the Use Groups Configuration option.
2. Select LDAP/LDAPS.
3. Enter the Server Name and select name types.
4. Enter Search Base DN in LDAP Notation, tab to the Group Base DN
5. Enter Group Base DN in LDAP Notation, tab to the System User and enter an appropriate value. If unsure of the value, try a leaving the system user blank.
6. Enter Test Login / Password and click Try Bind.