LDAP How to Guide

Contents

Overview

This document covers the use of LDAP with Swivel to read information from Active Directory and LDAP servers.

Swivel has a specific class for Active Directory imports, for further information see AD data source configuration

Prerequisites

Swivel 3.x

LDAP 3 compatible server

Creating the LDAP Repository

Add the LDAP Repository Servers

On the Swivel Server:

Select Repository/General and create an LDAP Repository, the name is descriptive and must be unique and up to 32 characters in length, and when created it should appear on the left hand side below Repository. Create additional Swivel servers for each LDAP server.

Click Apply to save settings

For information on creating custom synchronisation schedules see Schedule.

LDAP Repository Configuration

The following LDAP options can be configured.

Administrator: Administrative account username

Password: Administrative account password

Server: LDAP server Hostname/IP

Port: 389 LDAP, 636 LDAP SSL, 3268 Global Catalog, 3269 Global Catalog SSL

Base DN: If you set a base DN, user DNs will be relative to that. (specifying the base DN as part of the admin user name will result in the base DN being used twice). Whether Base DN needs to be specified varies on the implementation. Typically, you don't need to specify a base DN at all - Swivel will work it out for itself, sometimes the base DN needs to be specified.

Use SSL: The Swivel server or appliance can be configured to accept self signed certs by selecting the Accept self-signed certificates, located under the Repository/Name of LDAP server entry

Synchronization schedule: How often to synchronise with the LDAP server. A typical value is once per hour

Username attribute: The LDAP attribute to use as the primary key for user

Mark missing users as deleted: If set to Yes, when a user is removed from the LDAP group, then mark the user for deletion requiring a Purge. If set to No then the user will be deleted from Swivel.

Initial PIN attribute: An LDAP attribute that can containa PIN value to be read from the LDAP source.

Initial password attribute: An LDAP attribute that can containa password value to be read from the LDAP source. Be aware that this is a Swivel password, not a repository password. Setting a Swivel password is an additional security feature, but not all of our integrations support it: many assume the Swivel password is empty, and rely on the target system having its own password.

Import disabled users: If set to Yes then the disabled users will be imported. If set to No then disabled users will not be imported. It will not affect existing users but only applies to initial user import.

Import disabled state: Enable/disable the importing of users' disabled state from the user repository. When enabled the user repository will be consulted as to whether or not an account is disabled. Currently, Active Directory supports this functionality. Simple LDAP will support it if the name of the disabled attribute is entered in the appropriate settings. When enabled, it will no longer be possible to manually set the disabled state of the user within the Swivel administration interface. If Import disabled users is set to No, then this option has no effect, as disabled users will not be imported at

all.

Base Search Context: The base DN used when searching the repository. This can normally be left blank unless you have difficulty synchronizing the repository.

Group ObjectClass Name: The objectClass attribute value to be used for groups. Only groups with this object class will be searched when synchronizing. For writeable LDAP repository, this is the objectClass that will be used when creating new groups. It must therefore be a valid LDAP objectClass. Required parent classes will automatically be added.

User ObjectClass Name: The objectClass attribute value to be used for users. The same comments apply as for Group ObjectClass

Member attribute name: The attribute used when locating or setting group membership for a user.

Member group attribute name: The attribute used when locating group membership for a sub-group. Typically, this need not be set, as it is the same as for users, but some LDAP implementations use a different attribute.

Ignore FQ name changes: Ignore changes in the FQ name for the users

User disabled flag name: The attribute used to indicate that a user account is disabled. This is an optional attribute: if empty, all users are treated as enabled. Values must be of boolean type.

User enabled flag name: The attribute used to indicate that a user account is enabled. This has the same use as the User disabled flag name, but with opposite logic: true indicates that the account is enabled, rather than disabled.

Reformat Phone Number: If this option is set to Yes, then any phone number imported from the repository is reformatted by removing all non-digits (including spaces), and removing or adding a prefix, according to the following two options.

Prefix to remove: If Reformat Phone Number is enabled and this option is not empty, then the first occurrence of the specified prefix is removed.

Prefix to add: If Reformat Phone Number is enabled and this option is not empty, then the value of this option is added to the beginning of the number. A typical example of usage for phone number reformatting, in the UK, would be to set Prefix to remove to "0" and Prefix to add to "+44". This will ensure that phone numbers imported as, for example, "01937 582 020" will be stored in Swivel as "+441937582020"

Add domain qualifier: This option and the next allow you to add a fixed prefix or suffix to all usernames in this repository. This option specifies whether it should be a prefix, a suffix or neither. The prefix or suffix can be used to ensure uniqueness where there is a danger of having the same username in multiple repositories. It can also be used to ensure that the format of the username is correct for the target authentication platform. Be aware that if a prefix or suffix is used, users must always use them when authenticating to Swivel.

Repository Domain Qualifier: This option allows you to specify what prefix or suffix should be added to users in this repository, as described in the previous option. If you use this option, make sure that any separator characters are included. For example, if usernames should be in the form domain\username, the prefix should be domain\.

Installing trusted CA certificates for LDAPS

Certificates for LDAPS can be added to the Swivel appliance or server using the keytool command to import the cert as a trusted CA cert.

Appliance:

/usr/java/jre1.6.0_18/lib/security/cacerts

Check Password With Repository

Agents and RADIUS NAS entries have the options to Check password with Repository. This requires that the LDAP servers supports an LDAP **simple bind authentication**.

Testing

Known Issues

User Sync Issues

Swivel 3.8 release 2 onwards, any error retrieving user details will skip over that user, but mark it as deleted (or actually delete the user, if mark as deleted is disabled).

Swivel 3.5 to 3.8 first release, if an error occurs trying to read a specific user?s details, it will only skip that particular user if the error is ?Not found?. Any other LDAP error will cause it to abort.

Group Sync Issues

Swivel 3.5 and later, Errors attempting to access LDAP or to read the group details will cause the user sync to abort. In earlier versions of PINsafe, such errors could cause all users to be deleted.

User Import Issues

Swivel version 3.8 (release 1) and earlier, usernames must be EXACTLY the same on both servers, including case. If the username is changed on the source, it may invalidate user credentials. Do not change the username case on the LDAP server (such as changing the uid attribute to or from upper case and lower case, as it will try to import the user as a new user, but fails as the user already exists.

There are two ways to fix this: either change the LDAP repository to have upper case (or lower case) usernames, or modify the PINsafe database to change usernames to lower case. The SQL statement to do this is as follows: UPDATE PINSAFEJ SET H = LOWER(H);

Moving LDAP servers Issues

The usernames must be exactly the same on each server. With PINsafe 3.8 release 1 and earlier the base DN on the two servers must be the same. The PINsafe user sync can handle situations where a user has been moved within the same LDAP directory (basically, the repository returns a "not found" error). However, if the base DN is different, an "authentication failed" error is produced which causes PINsafe to abort the user sync.

If the base DN is the same and usernames are the same, moving to a different repository with the same users is possible. Delete the current data source repository definition, making sure that "Delete users with repository" is set to "No", and then create a new repository with EXACTLY the same name (including case and spacing).

Base DN cannot be deleted

If the Base DN cannot be deleted it may be necessary to delete the LDAP repository and recreate it. This is resolved in Swivel 3.9.4.

Troubleshooting

Try with the base DN blank and try that first.

Usually you will require the username attribute, member attribute, user objectclass and group objectclass.