LDAP

AID 097

ADITO Academy

Version 1.0 | 07.09.2021

Version	Changes
1.0	New Version for ADITO 2021

Index

1. What is LDAP?

The LDAP (Lightweight Directory Access Protocol) plugin is an interface to the Windows Active Directory (AD) which lets you compare and synchronize elements from the AD to ADITO like login- and userdata. Together with a functioning Kerberos or SSPI-Interface you are able to create users from your domain automaticly which can use the ADITO client without an extra login.

1.1. Structure

All attributes of an element can be called through the LDAP interface. This happens over the ADITO plugin that has to be added to the server.

A XML-structure defines which action to which instance of the directory will be executed. The credentials and the encryptiontype are set here.

The LDAP interface has the following functions available:

Action	Description
add	add an attribute to an existing LDAP entry
create	create an attribute/node to a LDAP entry
read	read an existing LDAP entry. This will return a specific attribute
remove	remove an existing attribute/node from an LDAP entry
replace	replace an existing LDAP entry
search	search an existing attribute/node from an LDAP entry. The attribute will be searched with the given filtercriteria

This interface is generic which means you are able to customize the ADITO system to your needs.

1.2. Included Files

1. LDAPIPluginXML.jar
   This plugin includes all necessary methods that are used to process the XML data.
   (<aditohome>/lib/server/plugin)

2. xStream-1.4.9.jar
   These external libraries are also used to process the XML data that come from the LDAP plugin. (<aditohome>/lib/server/ext)

Libraries and serverprocesses are described in their respective documentation properties.
(ActiveDirectoryXml_lib, ActiveDirectory_lib and activeDirectoryImport_serverProcess)

2. Leading Systems

2.1. Active Directory as a Leading System (Recommended)

The import process searches and reads all the existing user data of the AD. This search will find the "Distinguished Name". More options can be filtered through the parameter. The ADITO server will receive the resultsets of the found user data. These data sets will be compared to the ADITO system and inserted/updated if needed. The unique key for each user is the "objectGUID". This ID will be used to synchronize both systems.

2.2. ADITO as a Leading System

If ADITO is used as a leading system you have to create user-objects in order to transfer the information to the AD. Therefore you can use the entity "Employee" (Administration) to change the data of a user.

3. Handling

Normally a server process will sync the data on a nightly basis. The following descriptions are based on the Active Directory as a leading system.

3.1. Insert a new User (ldapImporterModule.onUserMissingInADITO)

Based on your filter criteria that you used in your configuration, the plugin will search for the given user in ADITO. If this user does not exist in ADITO, a process to insert the user will be triggered. The AD provides communication- and addressdata for ADITO to create a user and person in the system. The login credentials will sync to the given user.

3.2. Update an existing User (ldapImporterModule.onUserModified)

Based on your filtercriteria that you used in your configuration, the plugin will search for the given user in ADITO. If changes were made in the AD and the user exists in the ADITO system, the changes will be inserted/updated in the ADITO database.

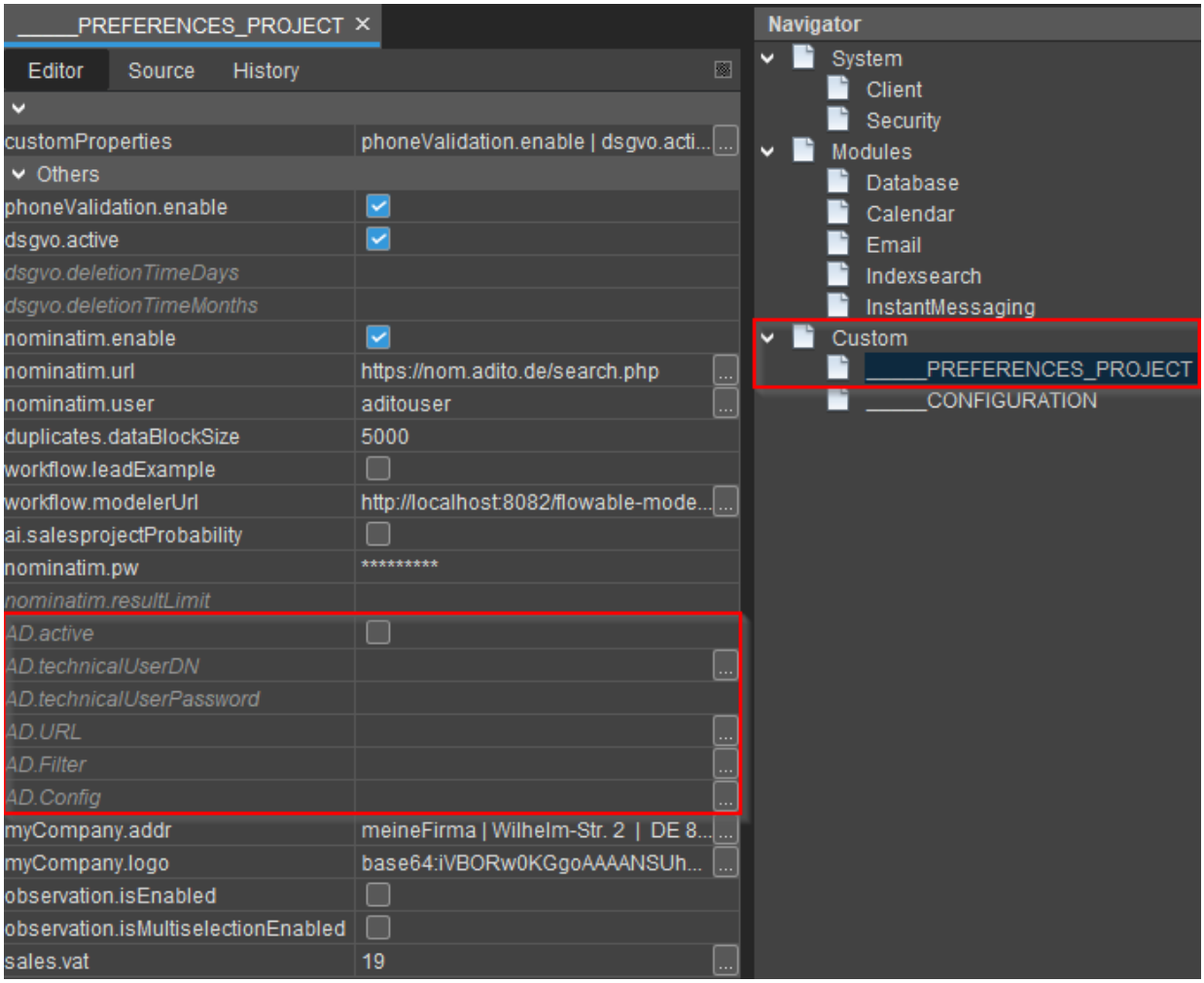
3.3. Delete an existing User (ldapImporterModule.onUserMissingInLdap)

If the LDAP importer does not find the user in the AD but that is already in ADITO, the process will set the state of this user to "inactive".

Because ADITO sets the nonexistent user to inactive you are able to set it back to active if it was a problem with the AD. ADITO does not delete the datasets!

4. Preferences

In order to configure your LDAP in ADITO you need to enter the information in the preferences of your project.



Preference	Description	Example
AD.active (bool)	make the Process general executable	
AD.technicalUserDN (string)	Complete distinguishedName of the technical user	CN=AD_User,OU=tec_users,OU=intern,DC=adito,DC=de
AD.technicalUserPassword (password)	Password of the technical User	
AD.URL (string)	URL to the Active Directory Server (withe ldap:// prefix and port), separate more values with semicolon	ldap://ad.adito.de:389
AD.Filter (string)	Filter in LDAP Filter Syntax	(&(objectClass=*)(memberOf=CN=adito_user,U=groups,DC=adito,DC=de))
AD.Config (string)	Start point of the search in tree, separate more values with semicolon	OU=users,OU=intern,DC=adito,DC=de

The general default LDAP ports are 389, 3268, 3269, 636. ADITOs default LDAP port should be 636.
Additionally, the connection to the insecure ports 389 and 3268 should be disabled.

5. Tools

You can use the tool LDAP Browser (from Softerra) to view the structure of the LDAP directory. This tool is free and helps you to find the right configuration for your AD.

6. Next steps

In order to use your LDAP-Plugin in your system you have to go to your system and configure it to your need. Open your ADITO Designer and go to the documentation property of the "activeDirectoryImport_serverProcess".