ADAM How to guide

Contents

- 1 Overview
- 2 Prerequisites
- 3 CSV Import to ADAM
- 4 Testing
- 5 Known Issues
- 6 Troubleshooting
    - 6.1 Error Messages

Overview

PINsafe can use ADAM as a data source, this document covers the integration with ADAM.

This document is in the process of being written

Prerequisites

PINsafe 3.8 ADAM release

CSV Import to ADAM

PINsafe will only import those attributes that it requires to ADAM: those attributes are:

- username
- given name
- surname
- disabled flag
- transport attributes (e.g. mail)

Any other attributes given in the imported file will be ignored.

Therefore, if you need to import userPrincipalName, you will need to set that as the username attribute before importing. This will mean that uid will not be populated, but uid is not a required attribute, so that is not a problem. If both uid and userPrincipalName exist, PINsafe will ignore any value set for uid if the username attribute is set to be userPrincipalName.

In short, it doesn't matter whether you use uid or userPrincipalName as far as PINsafe is concerned, but it will only take notice of the one you have set as username attribute.

Testing

Known Issues

Troubleshooting

Error Messages

Error creating LDAP user "Username": [LDAP: error code 20 - 0000217B: AtrErr: DSID-03050758, #1: 0: 0000217B: DSID-03050758, problem 1006 (ATT_OR_VALUE_EXISTS), data 0, Att 90290 (userPrincipalName)]

User already exists

"Error creating LDAP user "Username": [LDAP: error code 19 - 0000052D: AtrErr: DSID-033807A4, #1: 0: 0000052D: DSID-033807A4, problem 1005 (CONSTRAINT_ATT_TYPE), data 2245, Att 9005a (unicodePwd)]"

When a user is created in ADAM it gets created and is reflected in PINsafe Console. If the user is created in PINsafe it is not reflected in ADAM.

This is due to policy settings in ADAM. When you create a user directly in ADAM without a password, it is created but marked as disabled.

When you create a user through the PINsafe console, you have to choose the repository option either to generate a random password or to enter one manually. If you choose not to enter a password, you need to change the policy settings in ADAM to allow empty passwords. If they are entering a manual password, it might not meet the requirements.

admin:Exception occurred during repository attribute query, object: , attribute: rootDomainNamingContext, exception: [LDAP: error code 49 - 8009030C: LdapErr: DSID-0C0903CF, comment: AcceptSecurityContext error, data 533, v2580]

First of all, ensure that the password has been set and is correct for your bind user.

If you find that you are unable to use the Distinguished Name and password of the bind user you have created, it could be one of two problems:

- The ADAM or AD LDS instance (service) you created may not be running as a Domain user. This can be the cause if you are attempting to bind with a domain user from an existing Windows Domain.
- The ADAM or AD LDS user you created within the directory is disabled by default. Try changing the msDS-UserAccountDisabled attribute from TRUE to FALSE. Also note that if a password is not set then this can cause this attribute to be set to TRUE. If the user account is disabled by this attribute then you will not be able to bind with it.