PINsafe®

Active Directory Integration Notes

Created July 2006
Revised October 2007

Table of Contents

Introduction

This configuration document outlines how to integrate PINsafe using Active Directory as a source of user data. During operation most of the administration work for users is carried out on the Active Directory Server. An existing AD infrastructure can be used or a new one created. This document assumes creation of new AD groups.

Overview

PINsafe carries out an LDAP lookup on an Active Directory Domain to populate its own database. PINsafe 3.3 onwards allows multiple AD servers to provide user information as well as an internal XML database.

The following steps are required:

1. On the AD server configure authentication groups and populate users with mobile phone numbers and email addresses where required.
2. Create an AD Repository Server
3. Configure the AD authentication Information
4. On the PINsafe Server select Repository/Groups and enter the Repository Group names
5. Configure a Transport for sending security strings
6. Auto PIN creation (optional but recommended)
7. Sync the AD database.

Hints: Ensure transports and alerts are working with XML users and test the configuration with a small number of users

Prerequisites

Active Directory with administrator rights
Active Directory login service account for PINsafe
Active directory populated fields for example mobile numbers and email addresses
PINsafe server
LDAP browser (optional but recommended)

Installation

Creating Active Directory Groups

Users are added to Active Directory (AD) groups to allow them access to differing authentication resources. By creating additional AD groups different configurations can be made to suit the required environment. The following documentation assumes the following configuration:

PINsafe Users - who have access to all authentication methods
PINsafe Administrators – who have access to all authentication methods and admin rights

Create a **Swivel** Organizational Unit (OU)
Right Click on the domain then select New and then OU, enter the name **Swivel**

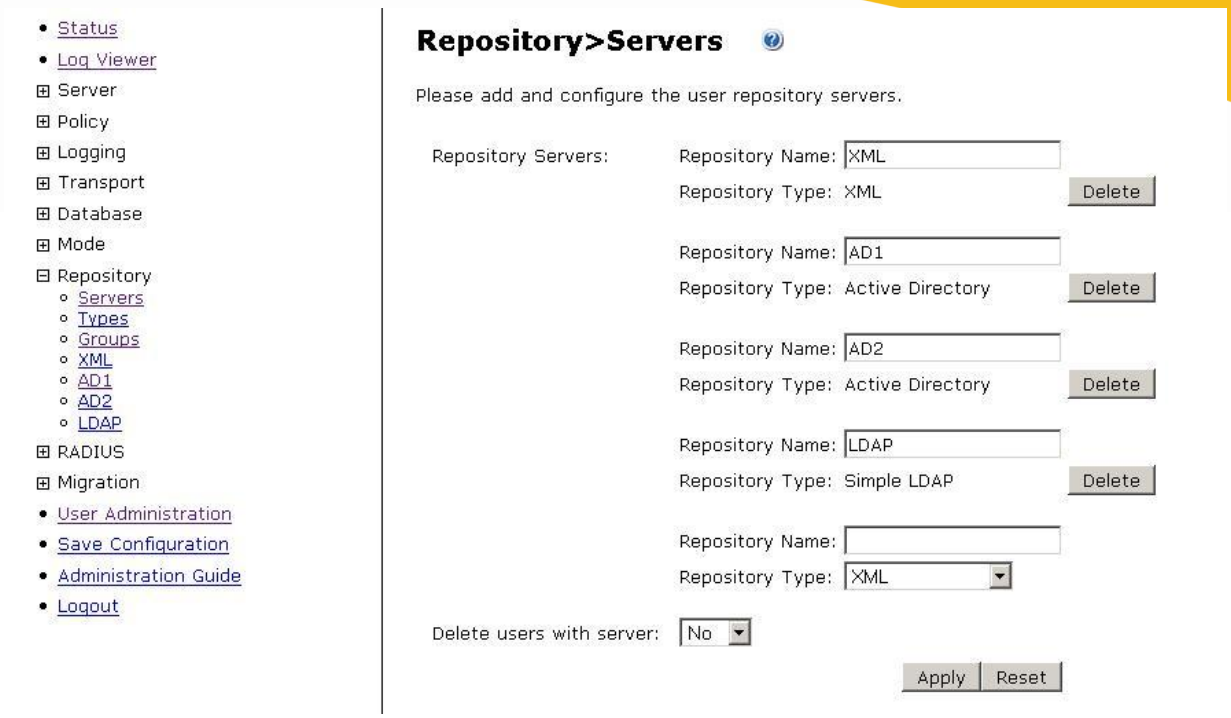
Within the **Swivel** OU create a **PINsafeAdmin** Container (CN)
Right click on the Swivel OU then select New Group, enter the name **PINsafeAdmin**

Within the **Swivel** OU create a **PINsafeUsers** Container (CN)
Right click on the Swivel OU then select New Group, enter the name **PINsafeUsers**

Add users to the PINsafeUsers and PINsafeAdmin group as appropriate

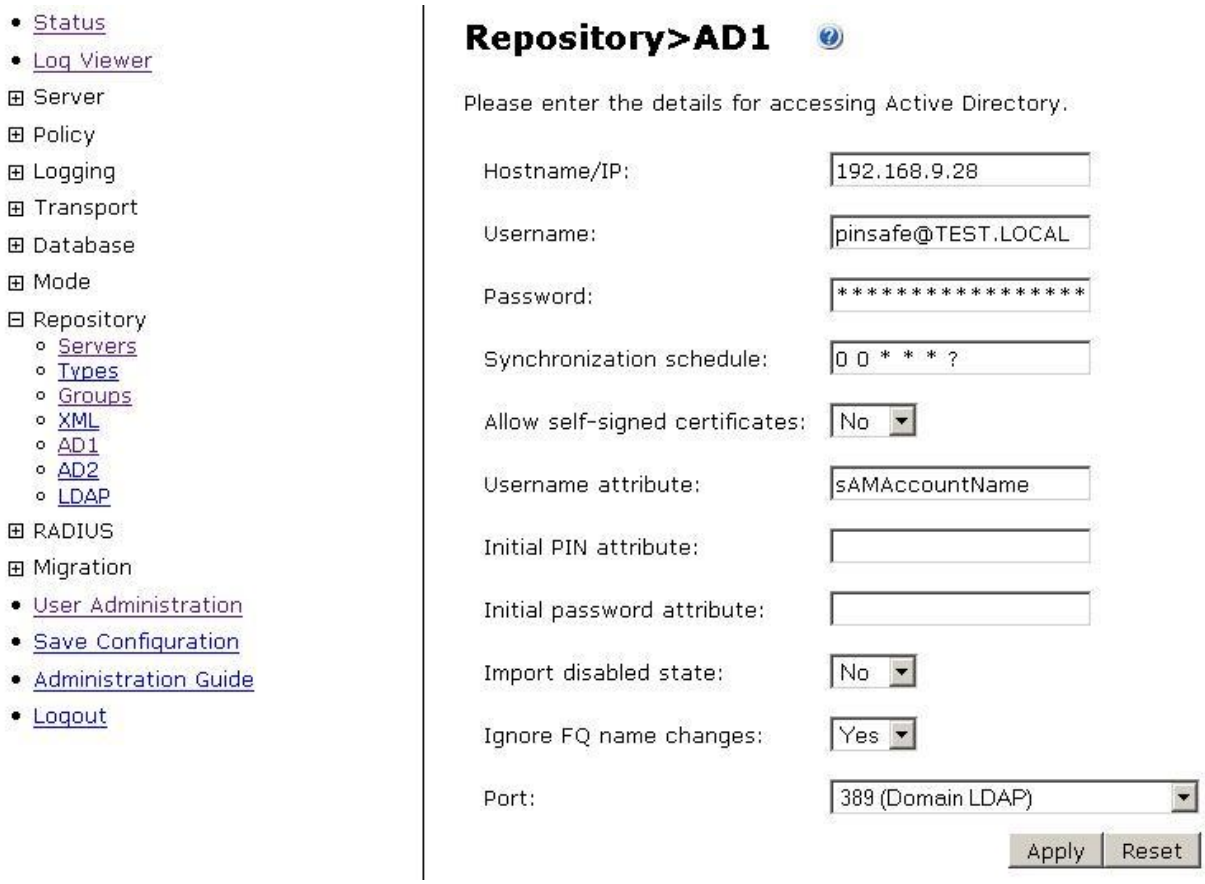
Configure the AD Repository Servers

On the PINsafe Server select Repository/General and create an Active Directory Repository, the name should appear on the left hand side below Repository.



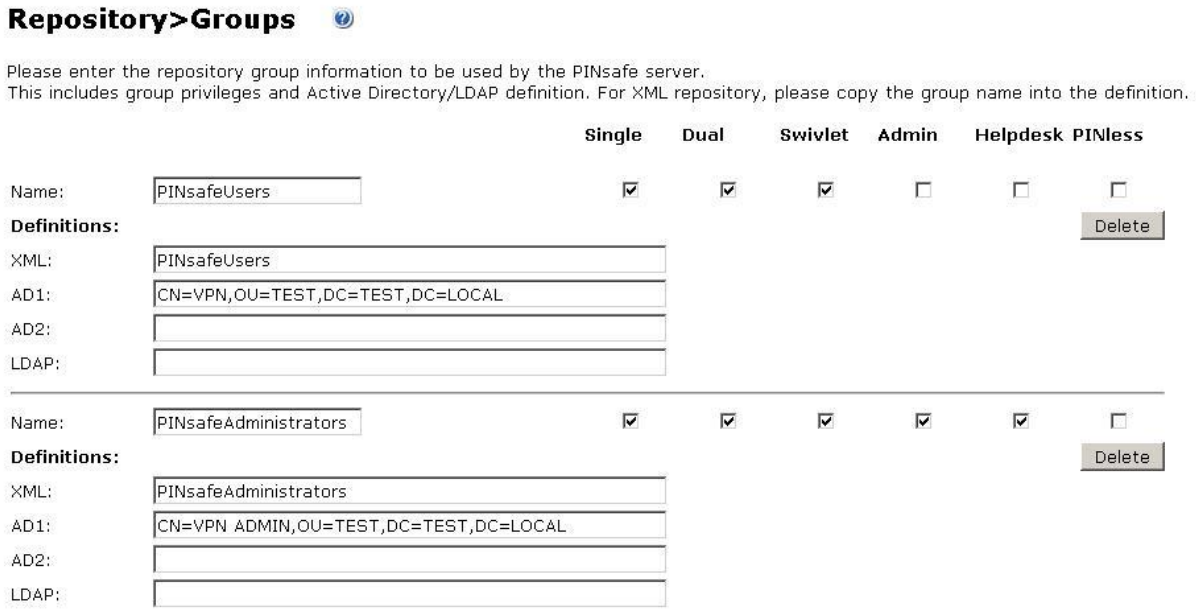
Configure the AD Authentication Information

Select the Repository/<AD Name> you have created and enter the username and password and Active Directory Server IP address. (Note this should be an account without a regular password expiry). The user must be an account with rights to the system and the UPN (User Principle Name) must be specified, (e.g. user@mydomain.com).



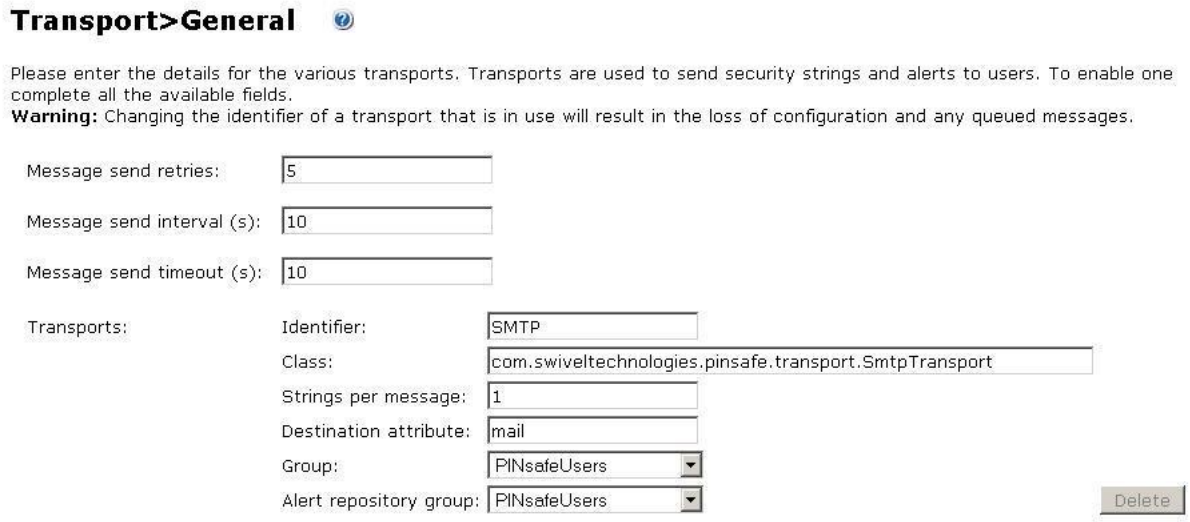
Create PINsafe Groups

On the PINsafe Server select Repository/Groups and enter the Repository Group names corresponding to those created in Active Directory. Leave the fields blank that are not required. The input fields are case sensitive. Use an LDAP browser if unsure of the path.
The format must be:
CN=<AD Container>,OU=<Organizational Unit>,DC=<mydomain>,DC=<com>
Example: CN=PINsafeAdmin,OU=Swivel,DC=swivelsecure,DC=com



Configuring Transport Groups

Configure Transport for sending security strings (Repository Group) and alerts (Alert Repository Group). For SMS use 'destination attribute': **mobile**, for SMTP use 'destination attribute' **mail**. Note: If using the Telephone Number field in AD instead of the mobile field, then the 'destination attribute' **telephoneNumber** needs to be specified. Hint: Test that all Transports are working. Note if using AD users and XML users you will have to use separate Transports to specify the different destination attributes.

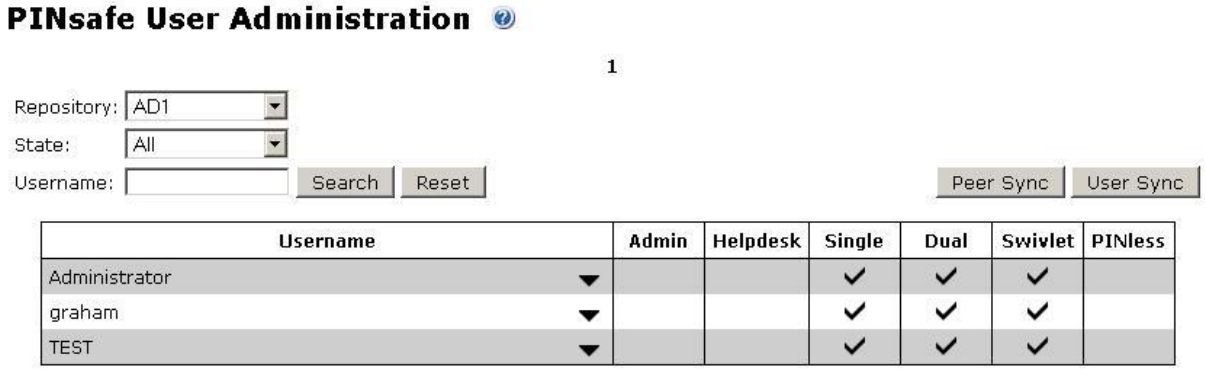


Auto Create PIN credentials (optional)

On the PINsafe Server select Server/Authentication Policy and set 'Create Pin Credentials' to Yes. This is recommended for large numbers of AD users.

Sync the AD Database

On the PINsafe Server select User Admin and from the repository the AD server name then click on sync now. Users should appear.



Troubleshooting

Check the PINsafe server logs and system event logs for any errors or lack of communication.

> SEVERE Exception occurred: javax.naming.**AuthenticationException**: [LDAP: error code 49 - 80090308: LdapErr: DSID-0C090334, comment: AcceptSecurityContext error, data 525, vece]

AuthenticationException: This can be seen when an incorrect authentication is made against an AD domain. Check the username and password.

> ERROR Exception occurred: during repository attribute query, object:<name>, attribute: sAMAccountName, exception:java.naming.**InvalidNameException**:<name>: [LDAP: error code 34 – 000208F: NameErr: DSID-031001B3, problem 2006 (BAD_NAME), data 8350, best match of:'<name>']; remaining name <name>

InvalidNameException: Names have failed to be found and existing names are not found. Check the AD paths and names. Use an LDAP browser (such as Softerra which produce a freeware LDAP browser) to find the correct authentication information to the PINsafe server.

> admin:Exception occured during repository group member query, group: CN=VPN,OU=TEST,DC=TEST,DC=LOCAL, exception javax.naming.**CommunicationException**: 192.168.0.1:389 [Root exception is java.net.ConnectException: Connection timed out: connect]

CommunicationException: There is a connectivity problem between the PINsafe server and the AD server

Additional Information

For assistance in the PINsafe installation and configuration please contact support at support@nappliance.com