How To synchronize users from an LDAP server to IDENTIKEY Authentication Server with ODBC database.

Creation date: 1/9/2010 Last Review: 12/12/2012 Revision number: 3

Document type: How To

Summary

The LDAP Synchronization Tool is a product that enables User information from any LDAP data store to be synchronized with an IDENTIKEY Authentication Server. This article describes the basic configuration of the tool to get you up and running quickly.

details

In the following example IDENTIKEY Authentication Server is installed with the embedded PostgreSQL database, but I want to use my existing Active Directory users in IDENTIKEY Authentication Server. I will configure a profile in the LDAP Synchronization tool that will create users in the IDENTIKEY Authentication Server Server based on their Active Directory samaccountname attribute.

In this example users exist in the standard AD users container. CN=Users,DC=vasco,DC=local

A domain of vasco.local was created in IDENTIKEY Authentication Server to store the users.

- Open the Synchronization Configuration GUI and select Profiles. Click the Add button to create a Profile if one does not already exist.
- From the Options tab select the desired settings.
change the Profile name to your desire
Set the Start time using the 24 hour format and set a Repeat interval if needed.

- Select the LDAP tab and enter the connection settings for your environment, then click the Test Login button to test the connection.

Click the Synchronization root button. Select the base DN location from the drop down list. Click the Get button to show the possible choices and select the location you wish to synchronize.
• Select the IDENTIKEY tab and enter the connection settings for the IDENTIKEY Authentication Server. Click the Test login button to test the connection.

Click the button in the Synchronization root section and you will see a Synchronization root window that will allow you to select the location to store the users in IDENTIKEY Authentication Server

• Select the Mappings and filtering tab. Depending on your LDAP back-end structure you may have Organizational Units that contain different objects for example users, computers, groups etc. To narrow down your search to only users you could create a filter based on LDAP attributes.
In this example the AD “objectcategory” attribute is used with a value of “person” to filter user objects.

To link the Active Directory user to the IDENTIKEY Authentication Server user we need to create a mapping. The AD Attribute “samaccountname” will be mapped to the IDENTIKEY Attribute “User ID”.

You could also filter based on group membership. If for example you created a group called “Digipass Users” you could setup a filter based on the LDAP attribute “memberof” and enter the distinguished name for the LDAP value. In my example CN=Digipass Users,CN=Users,DC=vasco,DC=local. Only users that are member of the group Digipass Users will be synchronized.
• Click the Test run button to validate your settings.

• After you validate your settings click the Apply and OK buttons. The LDAP Synchronization Tool service will restart and run the Synchronization job at the specified time and interval set.