
halFILE 4.0

Active Directory Integration

This document describes halFILE and e.halFILE Active Directory Integration

Contents

Overview.....	2
Why use Active Directory Integration?	2
Before you start.....	2
halFILE Active Directory Integration Set Up Procedure	3
halFILE Active Directory Integration.....	3
e.halFILE Active Directory Integration.....	4
Windows Authentication.....	4
Digest Authentication.....	4
Behind the Scenes	4

Overview

Windows Active Directory is a powerful tool for maintaining network users across multiple servers and domains. halFILE and e.halFILE can be configured to integrate with Windows Active Directory. This lets you set up Windows Active Directory Groups containing users that have similar security properties in halFILE. Then in halFILE you do not need to set up each individual user, only the groups that match the Windows Active Directory Groups. When you add a user to a Windows Active Directory group, that user automatically inherits the privileges of that group when going into halFILE. Furthermore, no login to halFILE is required. The user is automatically logged in under the network user id.

Why use Active Directory Integration?

- Administer users from one place, Windows Active Directory.
- No halFILE security setup is required when a new employee is hired that needs to use halFILE. Set up the person's network user id, put him in the appropriate Active Directory Groups and he should be able to get into halFILE with the correct security.
- Easy to remove users when employee turnover occurs. If an employee leaves, you delete him from Windows Active Directory and he/she no longer has access to halFILE.
- Quickly change halFILE roles for users. If a user is promoted to a new job requiring different halFILE privileges, then move the user from one Active Directory Group to another and those privileges automatically flow over to halFILE security.

Before you start

Before you enable the Active Directory Integration feature in halFILE, you should spend some time planning your groups. These groups will be used to assign User Privileges (Configure-Security-User Profiles), Custom Search Settings (File-Database Custom Search button) and User Features (Extended Settings behind the database privileges in Configure-Security-User Profiles).

If you are enabling this feature on an existing site, you should define your Windows Active Directory groups and assign users to these groups.

halFILE Active Directory Integration Set Up Procedure

Set up a Windows Active Directory Group for each type of User that you would have in halFILE. For example, if I have Search only users, Search and Index users and Admin users, I would set up 3 Active Directory Groups as follows:

- HFAD_User_Search – for users with Search only privileges.
- HFAD_User_Index – for users with Search and Index privileges.
- HFAD_User_Admin – for users with Admin privileges.
- Add the Network users into the appropriate HFAD_User group(s).
- Set up a Windows Active Directory Group for each type of Custom Search you require. For example, if you have a Custom Search for Public users and a second Custom Search profile for Employees, then you would set up the Active Directory Groups as follows:
 - HFAD_Search_Public
 - HFAD_Search_Employee
- Add the Network users into the appropriate HFAD_Search group(s).
- Change halFILE to use Active Directory Integration. In the Administrator, this is under Tools-Options / Security/Versions tab. Check the “Use Active Directory Integration” box. Note: You must check the “Use halFILE Integrated Security” box to enable this check box.
- Set up a single User and Custom Search in halFILE for each Windows Active Directory Group, using the same name as the Windows Active Directory Group. So using the above examples, set up users named HFAD_User_Search, HFAD_User_Index and HFAD_User_Admin. Set up all the features as needed including Extended Settings and Group/Document Level Security. Then, set up Custom Search Profiles named HFAD_Search_Public and HFAD_Search_Employee.
- Now, when a user goes into halFILE, they are automatically assigned their Network user id. halFILE looks up the user id in the Windows Active Directory Groups to determine which groups the user belongs to. Then, the user’s profile for halFILE security is created for the user.

halFILE Active Directory Integration

Active Directory integration is now part of halFILE.exe in 4.0 so there is no need to launch HFWAD32.exe. If active directory integration is enabled then halFILE will automatically access halSystems.ActiveDirectory.dll and login the user if they have rights. So once configured there is no change necessary at the client workstations for users to access the system.

e.halFILE Active Directory Integration

e.halFILE uses the same security setup as halFILE. However, there are some special set up requirements in Microsoft Internet Information Services (IIS) that need to be configured as follows:

- Create a hfLogin folder under c:\websites\- Create an application inside IIS called hfLogin under your website and point to c:\websites\- Do not set a Connect As User leave as pass-through authentication
- Click on the newly created hfLogin application in IIS
- Double click authentication
- Enable Windows Authentication (intranet) or Digest Authentication (Internet) (see explanation below) and disable all others.

Note: If these authentication methods are not in the list you will need to install them in add features/roles of server administrator.

- Copy halweb.ini from scripts to hfLogin folder and add a DomainName=<yourdomain> (i.e. Austin.local) as ASP.NET cannot obtain a domain context without this information as a security precaution.
- Change the login button or link on your website to go to <http://sitename/hflogin/hflogin.aspx>

Windows Authentication

Select Windows Authentication for intranet sites where you do not want the users to be prompted for a password. This only works if they are using Internet Explorer browser and are connected locally. If access from a public Internet site or using any other browser than you will want to use Digest authentication

Note: If Windows Authentication is enabled and users are still prompted by IE for a username/password then you might make sure the sitename does not include any periods as windows may conclude that is part of the Intranet zone rather than the Internet zone. Use something like <http://servername> to access the site not <http://servername.domain.local> or a public domain name

Digest Authentication

Select Digest Authentication when you want to support a wide variety of browsers and/or the site is available as a public domain on the Internet. This will prompt the user for their active directory username/password each time but will not transmit that information to the server. It will use an encrypted hash to communicate with Active Directory.

Behind the Scenes

New tables in the HFWParams database are used to store the above information including:

ADUsers
ADUserFeatures
ADCustomSearch

When a user logs in, halFILE queries Windows Active Directory to determine which Active Directory Groups he/she belongs and dynamically builds the security system for that user in halFILE according to the settings for matching group names set up in halFILE.