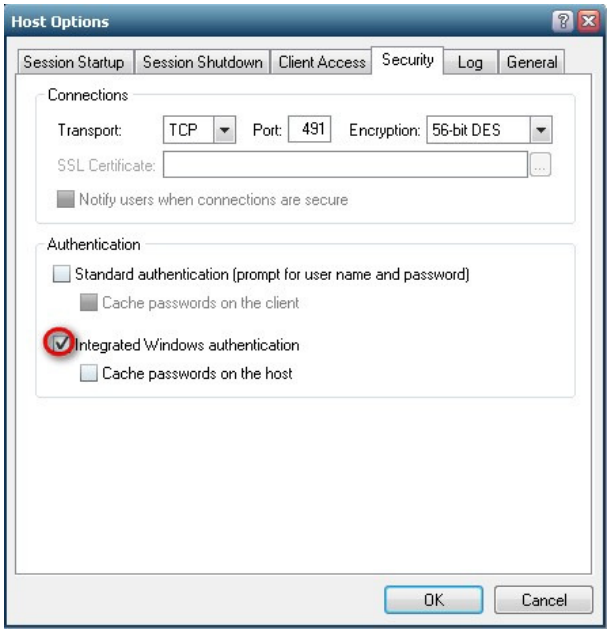
FH Web Edition - Integrated Windows Authentication

Integrated Windows Authentication

Integrated Windows authentication allows users to connect to an FH Web Edition Host and start a session without having to sign in to the host and re-enter their user name and password. When Integrated Windows authentication is the only option enabled, the user's user name and password are never transmitted over the network. Instead, FH Web Edition simply runs the user's session in the same security context as the FH Web Edition Client. Users are added to the host's NETWORK group instead of its INTERACTIVE group. As a result, they may be denied access to some resources.

When users connect to a FH Web Edition Host using Integrated Windows authentication, they are able to access most of the same resources on the host that they would be able to access if they signed in to the host interactively. However, depending on the authentication protocols supported by the client's and host's operating systems and the network, when users access resources that reside on other computers on the network they might be required to re-enter their user name and password. If network resources are unable to request a user name and password, access might be denied.

In order to access other computers on the network, the Active Directory must be configured to allow authentication credentials to be passed to other computers. Microsoft refers to the right to pass authentication credentials to a third or more computers as "delegation." Delegation is supported by Windows 2000 or later on Active Directory networks with the proper settings. Please refer to your Microsoft Windows operating system documentation for instructions on properly configuring an Active Directory Domain Controller. Windows NT Domains do not support delegation. When Integrated Windows authentication is enabled in this environment, users might not have access to resources that reside on other computers on the network.

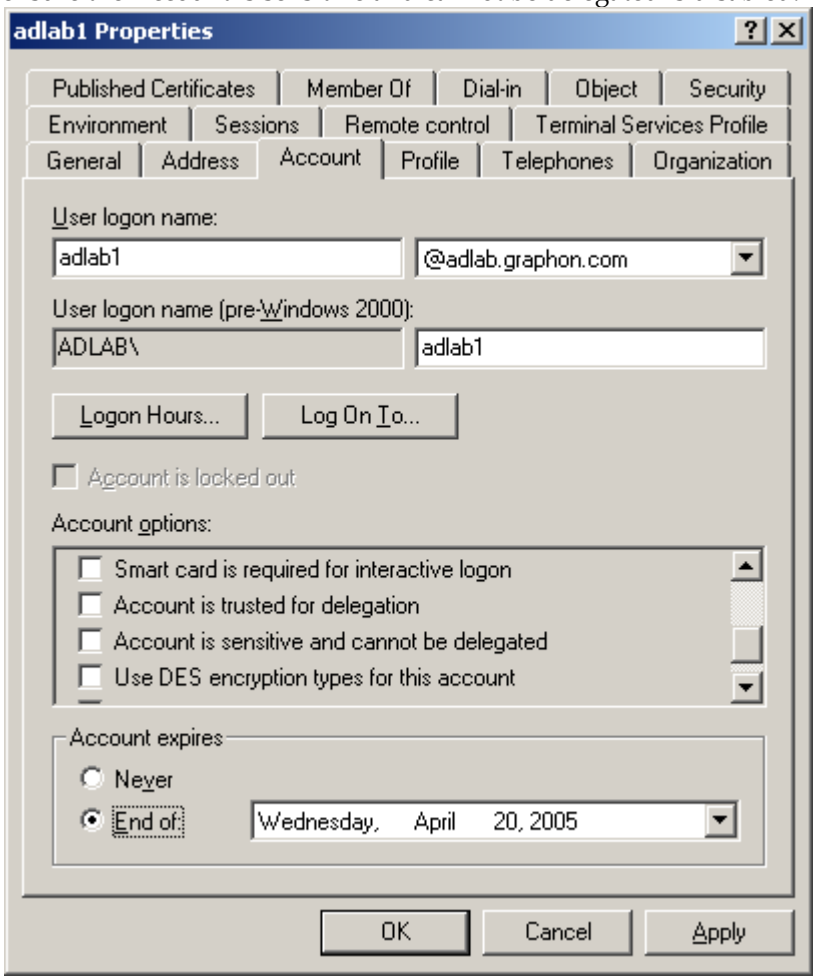


To Enable Integrated Windows Authentication

- From the FH Web Edition 4 Connection Manager, Click Tools | Host Options
- Click the Security Tab
- Check Integrated Windows Authentication
- Click OK

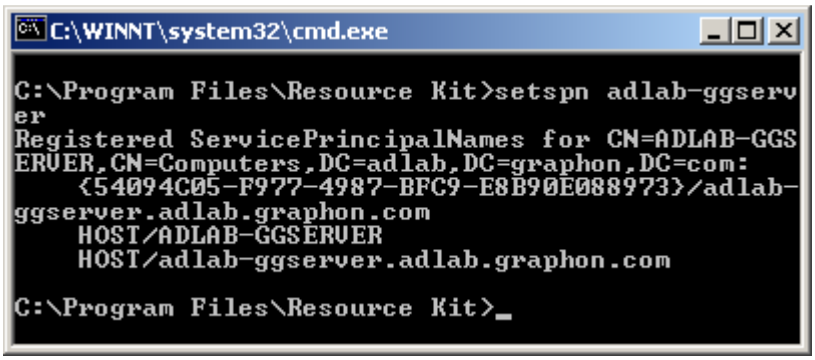
Configuration Requirements for Integrated Windows Authentication

- The Primary Domain Controller (PDC) and any Backup Domain Controllers (BDC) must be running Windows 2000 or later. Delegation requires the Kerberos authentication protocol, which was introduced with Windows 2000.
- The Domain Name System (DNS) servers must support Service Location (SRV) resource records. It is also recommended that DNS servers provide support for DNS dynamic updates. Without the DNS dynamic update protocol, administrators must manually configure the records created by domain controllers and stored by DNS servers. The DNS service provided with Windows 2000 or later supports both of these requirements.
- The computers hosting the FH Web client, the FH Web Server, and any backend services, such as email or a database, must be running Windows 2000 or later in a Windows 2000 or later domain.
- The client's user account must support being delegated by the FH Web Application Publishing Service. In the Active Directory Users and Computers Management Console, select the user and click Action | Properties. Click the Account tab. In the Account options list box, scroll down and ensure the Account is sensitive and cannot be delegated is disabled.



- The FH Web Server must have the right to delegate the user's account to other computers. In the Active Directory Users and Computers Management Console, select the computer and click Action | Properties. Enable Trust computer for delegation. The FH Web Application Publishing Service must be configured to run in the Local System account for these delegation rights to apply.

- The FH Web Application Publishing Service must be able to register its Service Principle Name (SPN) with the Active Directory. It attempts to do this during installation and upon every restart of the service. The setspn.exe utility (available in the Microsoft Resource Kit and as a separate download from Microsoft) can be used to verify the SPN is properly set. The following Command Window shows output obtained from setspn.exe when run on the FH Web Server.



- Replace adlab-ggserver with the computer name of your FH Web Server. The {54094C05-F977-4987-BFC9-E8B90E088973} Globally Unique Identifier (GUID) is specifically used by the FH Web Application Publishing Service to create the {54094C05-F977-4987-BFC9-E8B90E088973}/adlab-ggserver.adlab.graphon.com SPN.
- The following Command Window shows output obtained by running setspn.exe on the FH Web Server and indicates a network configuration error. If all the above requirements are met this should not occur.

Product Headquarters
FIREHOUSE Software
ACS, A Xerox Company
2900 100th Street, Suite 309
Urbandale, IA 50322

Toll Free: 1-800-921-5300
Phone: 515-288-5717
Fax: 515-288-4825
www.firehousesoftware.com
support@firehousesoftware.com

ACS
A xerox Company