SPNEGO Kerberos Authentication

Agiloft supports single sign on via the Kerberos authentication protocols, using SPNEGO to access the knowledgebase via HTTP.

What are SPNEGO and Kerberos?

- Kerberos is an a authentication protocol, which allows nodes communicating over a non-secure network to prove their identity to one another in a secure manner. It is designed to provide strong authentication for client /server applications by using secret-key cryptography.
- SPNEGO, pronounced *'spang-go* or *spe-'nay-go*, is a GSSAPI "pseudo mechanism" used by client-server software to negotiate the choice of security technology. SPNEGO is used when a client application wants to authenticate to a remote server, but neither end is sure what authentication protocols the other supports. Most notably used by browsers for HTTP negotiation.

Prerequisites

To complete SPNEGO/Kerberos setup you must have:

- A server environment configured with Kerberos/SPNEGO.
- Agiloft must be installed on a machine in the Active Directory domain.
- A known address for the domain key distribution center (KDC).
  Note: the KDC address is often the same as the domain controller address.
- An account name and password in the domain to be used for pre-authentication.
- A registered Service Principal Name (SPN) with the account mentioned above for all known names of a server where Agiloft is installed. To register an SPN, run `setspn.exe -A HTTP/<server> <account name>` for all known names of a server where Agiloft is installed. The command should be run on the domain controller.

Setup Kerberos/SPNEGO Access

To configure Kerberos/SPNEGO...

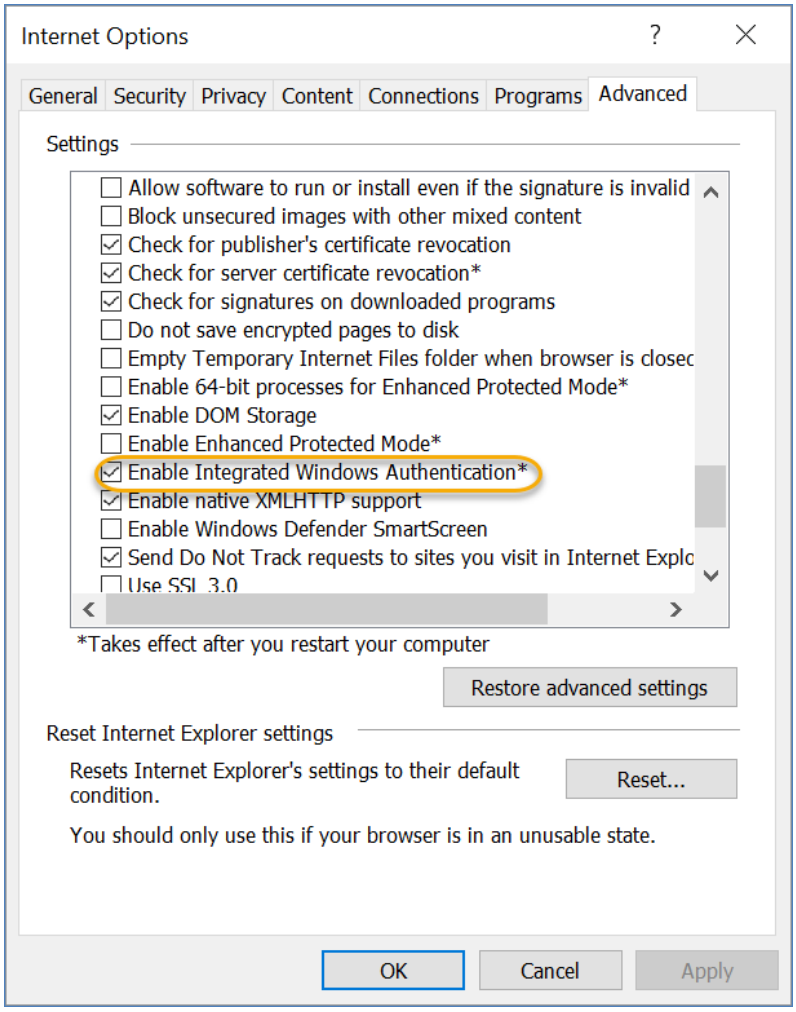
1. Go to **Setup > Access** and click the SPNEGO/Kerberos Setup button.
2. Select Yes under Enable SPNEGO Authentication.
3. Enter the User Name, Password, KDC Address and Domain, using the credentials and details listed above.
4. Click Test Connection to check the configuration details.

5. Click Finish.

Browser Settings

For Internet Explorer users, you must make the following modification to your browser settings:

1. In Internet Explorer (IE), go to **Internet Options > Advanced > Security**.
2. Check Enable Integrated Windows Authentication.



Access URL

The URL for SPNEGO authentication is:

`https://{server_name}/gui2/spnego.jsp?autoLogin=true&project={KBName}&State=Main`

Whenever possible, make sure to use the domain name for your server, such as `example.agiloft.com`, rather than the specific server hostname, such as `ps108.agiloft.com`.