Active Directory Authentication

Active Directory User Source

The Active Directory Authentication profile uses Microsoft's Active Directory over **LDAP** (Lightweigh t Directory Access Protocol) to store all the users, roles, and more that make up an Authentication profile. Active Directory **Groups** are used for Ignition's **roles** and user-role mappings.

While using an Active Directory User Source, administration of users and roles is through Active Directory itself, and not manageable within Ignition. Thus adding new users to an Active Directory User Source, or modifying pre existing users, requires the modifications be made from Active Directory, usually through an AD Administrator.

Property Reference

Active Directory User Sources have the following properties, organized by category

> ⚠ Certain properties in the Active Directory User Source allow you to filter users, such as the **User List Filter**. These filters only determine which users will be displayed on screen. They are not authentication filters, so even if a user does not show in the list they can still authenticate and may have access to unintended areas. Be sure to configure Project security appropriately to prevent this from happening!

Main Properties

Details on the Main Properties can be found on the User Sources page.

On this page

...

- Active Directory User Source
- Property Reference
  - Main Properties
  - Active Directory Properties
  - LDAP Search Properties
- To Create an Active Directory User Source

Active Directory Properties

Name	Description
Domain	The Windows Domain your active Active Directory server is running on. If you aren't sure of your domain, ask your network administrator. Leave blank to set advanced properties manually.
Gateway Username	The login name for the Gateway to use when querying Active Directory. Used for retrieving the list of users and roles via LDAP.
Password	The password for the above username.
Primary Domain Controller Host	The IP address or hostname of your primary domain controller. Example: "192.168.1.4" or "MainServer"
Primary Domain Controller Port	The port number for the primary domain controller's LDAP interface.
Secondary Domain Controller Host	The IP address or hostname of your secondary domain controller (optional). Example: "192.168.1.4" or "MainServer"
Secondary Domain Controller Port	The port number for the secondary domain controller's LDAP interface.

SSO Enabled	Whether or not to use Single-Sign-On (SSO) to authenticate AD users. This gives you the ability to log into the Client or Designer automatically with the password you logged into Windows with. For Client SSO login, each project must also have the **SSO Login** Project Property enabled. For Designer SSO login, **Allow Designer SSO** must be set in the Gateway Settings
SSO Domain	The domain that Windows users must match in order to use SSO. If blank, the main "Domain" property will be used.

LDAP Search Properties

Name	Description
Username Prefix	This prefix will be prepended to the username before an Active Directory bind is attempted for authentication.
Username Suffix	This suffix will be appended to the username before an Active Directory bind is attempted for authentication.
Automatic Suffix	If this option is checked, and the suffix is left blank, then the suffix will automatically be assigned a value of "@<domain>".
User Search Base	The base folder to search for users under, such as: **DC=MyCompany,DC=com** The entire subtree under this folder will be searched using the User Search Filter. Multiple subtrees can be specified by putting them in parenthesis, like so: **(OU=Administrators,DC=MyCompany,DC=com)(OU=Operators,DC=MyCompany,DC=com)**
User Search Filter	The LDAP search filter that will be used to find a specific user. Use the placeholder {0} as a standin for the login name.
User List Filter	The LDAP search filter used when querying for the list of all users. Should restrict the type to user.
User Name Attribute	The attribute on the User object to define the username.
User Role Attribute	Attributes of this name on the User object will define the user's roles.
Role Name Attribute	The attribute of this name on the Role object will define the role's name. Leave blank to use the raw value of the attribute defined by the **User Role Attribute** property.
Full Name Attribute	The attribute on the User object to define the full name of the user.
Phone Attribute	The attribute name on the user object that represents the user's phone number.
Email Attribute	The attribute name on the user object that represents the user's email address.
SMS Attribute	The attribute name on the user object that represents the phone number that this user receives text messages on.

Read Timeout	The read timeout in milliseconds for LDAP operations.
Results Page Size	The number of entries returned per page of results in a query.
Role Search Base	The base folder to search for roles under, such as: **OU=Roles,DC=MyCompany,DC=com** The entire subtree under this folder will be searched using the Role Search Filter. If you specify the root of your tree structure, the search may take a very long time. Multiple subtrees can be specified by putting them in parenthesis, like so: **(OU=Builtin,DC=MyCompany,DC=com)(OU=Users,DC=MyCompany,DC=com)** If you leave this blank the whole subtree of the domain controller will be searched.
Role Search Filter	The LDAP search filter that will be used to locate roles.
Allow Anonymous	Determines whether the Gateway will accept blank usernames and passwords for authentication. Note that this check takes place on the Gateway, prior to handing off any credentials to the AD server. If **Security Authentication** is set to None, then this property should be enabled, otherwise, blank passwords will be rejected by the Gateway. If true, authentication attempts with blank passwords will be passed through to LDAP, which may choose to accept them.
Use SSL	Works in conjunctions with the **Domain Controller Host** and **Domain Controller Port** properties in the Active Directory Properties section. Disable to use "ldap://" protocol, enable to use "ldaps://"
Security Protocol	Specifies the security protocol between the Gateway and AD server. The following options are available: **AUTO:** No security protocol is explicitly used or requested by the Gateway. **SSL:** SSL should be used for the connection.
Security Authentication	This property specifies how usernames and passwords are used to bind to LDAP. The following options are available: **AUTO:** Unspecified from the Gateway side, meaning the LDAP implementation will choose. **NONE:** Anonymous access. **SIMPLE:** Plaintext username and passwords will be used. **STRONG:** Usernames and passwords will be encrypted.

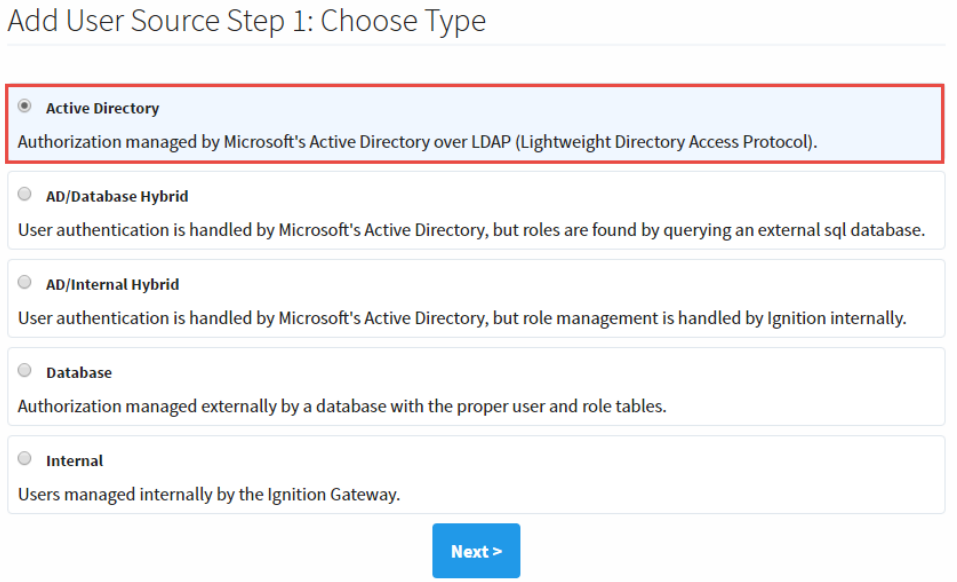
To Create an Active Directory User Source

To configure an Active Directory User Source, you must specify the host that is acting as your primary domain controller. You can also use a secondary domain controller in case the primary is unavailable. You'll also need to specify the name of the domain and credentials for the Gateway itself to use: the Gateway needs a user account to interact with the AD server, even when it's simply querying for a list of roles.

> **May need to contact your internal IT Department**
>
> When using Active Directory User Source, you may need to consult with your internal IT Department to get the required information to complete your user source setup. These settings are common to AD (not specific to Ignition), and your IT department will know what values to supply to each property.

1. On the Gateway Webpage, under the **Configure** section, go to **Security > Users, Roles**.
   The User Sources page will be displayed. Click the blue arrow, **Create new User Source**.

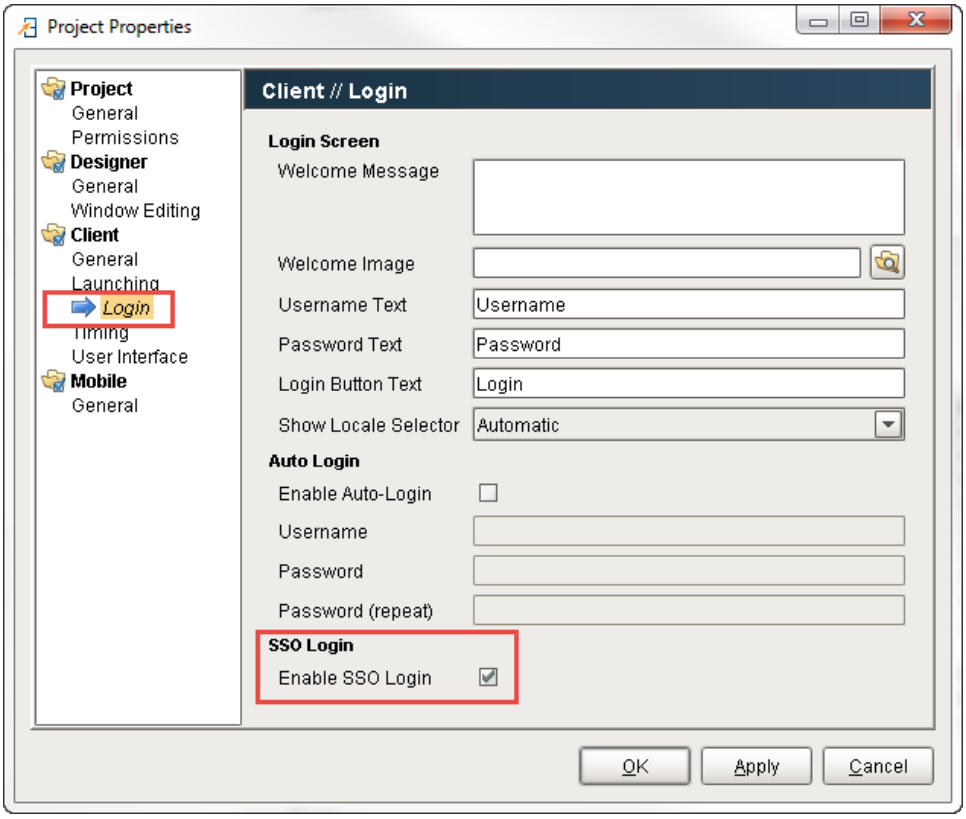
2. Choose the **Active Directory** authentication type, and click **Next**.



3. The New User Source window will open. Note that some properties are optional. In the very least, you must specify the following: **Domain**, **Gateway Username**, **Password**, **Primary Domain Controller Host**.

4. If you plan on using Single-Sign-On, then you will need to enable the **SSO Enabled** property, and continue on to the next step. In either case, click the **Create New User Source** button to create the User Source.
5. If you plan on using **Single-Sign-On**, you need to enable it per project by modifying the project's settings: in the **Designer** under **Project > Properties**.
   Under **Client > Login**, mark the checkbox for **Enable SSO Login**. Click **OK**.

> **Enable Single-Sign-On (SSO)**
>
> SSO is enabled on a per project basis. You have to configure it in the Active Directory authentication profile, and enable it for each project you want to use SSO with.



Related Topics ...

- AD Internal Hybrid
- Internal Authentication
- User Sources
- Project Security in Designer and Gateway