

AD Internal Hybrid

AD/Internal User Source

The Active Directory/Internal Hybrid authentication profile type combines the Internal User Source type with the Active Directory User Source type. Active Directory is used to find all of the users, and to check their credentials when they attempt to log in. However, it allows assigning of roles, contact info, and other meta-information about a user through Ignition, then stores all this information as if it were an Internal User Source. This way, Active Directory can be consulted to see if a username/password is valid, but the management of roles does not require coordination with your IT Department, who typically controls the Active Directory system. This "best of both worlds" approach is popular for many users of Active Directory.

The AD/Internal Hybrid User Source is partially manageable in Ignition. Users cannot be added or removed, and their usernames and passwords cannot be changed. This is because this information resides in Active Directory, not within Ignition. Other information, such as user roles, contact info, schedules, are [manageable](#) in Ignition.

Gateway Settings

Before you can use the User Management component to manage roles, contact info, etc., you first have to go into Gateway Settings, and mark the checkbox to '**Allow User Admin.**' This allows for the administration of the Gateway's system user source from the Designer and the Client. Unless this is enabled, the Vision Module's User Management component is prevented from modifying the Gateway system's user source.

On this page

...

- [AD/Internal User Source](#)
- [Property Reference](#)
- [Creating an AD/Internal Hybrid User Source](#)



AD Internal Hybrid

[Watch the Video](#)

Property Reference

This User Source shares many properties with the AD User Source. Please see the [Active Directory Authentication](#) page for a list of properties.

Creating an AD/Internal Hybrid User Source

To set up an AD/Internal Hybrid 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 for authentication for when it queries the list of roles.

May need to contact your internal IT Department for...

When using AD/Internal Hybrid User Source, you may need to consult with your internal IT Department to get the required information to complete your user source setup.

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 **AD/Internal Hybrid** authentication type, and click **Next**.

Add User Source Step 1: Choose Type

Active Directory
Authorization managed by Microsoft's Active Directory over LDAP (Lightweight Directory Access Protocol).

AD/Database Hybrid
User authentication is handled by Microsoft's Active Directory, but roles are found by querying an external sql database.

AD/Internal Hybrid
User authentication is handled by Microsoft's Active Directory, but role management is handled by Ignition internally.

Database
Authorization managed externally by a database with the proper user and role tables.

Internal
Users managed internally by the Ignition Gateway.

[Next >](#)

3. The New User Source window will open. Some properties are optional depending on how you setup your profile.

New User Source

Main	
Name	<input type="text" value="ADInternalHybrid"/>
Description	<input type="text"/>
Schedule Restricted	<input type="checkbox"/> Users are only able to log in when their assigned schedule is active. <small>(default: false)</small>
Failover Source	<input type="text" value="default"/> If this source is unreachable for authentication, this failover source will be used instead.
Failover Mode	<input type="text" value="Hard"/> The failover mode to use if a failover source is set. Hard: Failover only if this source is un-reachable. Soft: Try the failover source when a user fails to authenticate with this source. <small>(default: HARD)</small>
Cache Validation Timeout	<input type="text" value="60000"/> The amount of time between cache updates of the user source. <small>(default: 60,000)</small>

Active Directory Properties	
Domain	<input type="text"/> The Windows domain for this Active Directory server. Examples: "MyCompany.com" or "SuperCorp.local". If you aren't sure of your domain, ask your network administrator. Leave blank to set advanced properties manually.
Primary Domain Controller Host	<input type="text"/> The IP address or hostname of your primary domain controller. Example: "192.168.1.4" or "MainServer"
Primary Domain Controller Port	<input type="text" value="389"/> The port number for the primary domain controller's LDAP interface. <small>(default: 389)</small>
List Users from Active Directory	<input checked="" type="checkbox"/> If true, Active Directory will be queried for the list of all users. If false, users must be added manually. <small>(default: true)</small>
Gateway Username	<input type="text"/> The login name for the gateway to use when querying Active Directory. Used for retrieving the list of users and roles via LDAP. <small>(default:)</small>
Password	<input type="password"/> The password for the above username.
Password	<input type="password"/> Re-type password for verification.
SSO Enabled	<input type="checkbox"/> Whether or not to use Single-Sign-On (SSO) to authenticate AD users. Note that projects must also have this option enabled for SSO to work. <small>(default: false)</small>
SSO Domain	<input type="text"/> The domain that Windows users must match in order to use SSO. If blank, the main "Domain" property will be used. <small>(default:)</small>

Show advanced properties

Create New User Source

Related Topics ...

- AD Database Hybrid
- Internal Authentication
- User Management Component