User Sources

User Sources

User sources (previously known as Authentication Profiles), are a collection of users, roles, and other user data, such as contact information or schedule. When a new user or role is created, it is applied and stored in the user source. Projects and the Gateway are assigned a User Source to authenticate against. This determines which users have access to which project(s).

There are several types of user sources: single-storage types with varying storage mediums, "hybrids" that combine features of the previous three types, and a cache type used in Local Client Fallback systems.

Single-Storage

Users and roles are stored in a single location. The single-storage users sources are:

- **Internal Authentication** - Users and roles are stored internally to Ignition.
- **Database Authentication** - Users and roles are stored in a SQL database. Managing users is done via direct interaction with the database.
- **Active Directory Authentication** - Users and roles are managed by Active Directory. Users are authenticated through the LDAP protocol.

Hybrid

Users in hybrid user sources authenticate against Active Directory, meaning that user names and passwords are checked against those stored in Active Directory. However, roles are stored either internally in Ignition or in a SQL database, so it is possible to make a role change without have to contact your Active Directory administrator. This way, Active Directory can be consulted to see if a user is valid, but the management of roles does not require coordination with the IT department, who typically control the Active Directory system. This "best of both worlds" approach is popular for many users of Active Directory.

- **Active Directory-Internal Hybrid** - Users managed by Active Directory and roles stored to Ignition internally.
- **Active Directory-Database Hybrid** - Users managed by Active Directory and roles stored in an SQL database.

Fallback Cache

This feature is new in Ignition version 7.9.1

Click here to check out the other new features

This User Source was developed specifically for a system that is using Local Client Fallback, and allows you to cache the login credentials from a remote user source. This means your users can still log in with their normal username/password on a Local Client Fallback project, even when the network connection is unavailable.

More information can be found on the Fallback Cache Authentication page.

Shared Functionality

Regardless of type, all User Sources have the following functionality:

- **Failover Source**: If the User Source is unavailable for authentication, then a backup User Source can be specified. The type of the fail-over User Source can differ from the primary, so configurations where an internal-type fails over to a database-type are possible.
- **Schedule Restrictions**: The User Source can prevent users from logging in when they are off schedule, meaning that the schedule assigned to the user determines when the user may login.

Main Properties

All User Sources have a section of properties that are categorized as "Main". Below is a description of these properties.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the User Source. This is how other systems in Ignition reference the user source. Note that every User Source must have a unique name.</td>
</tr>
<tr>
<td>Description</td>
<td>An optional description of the user source. Useful for noting which database connection or AD server the User Source may be referencing.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Restricted</td>
</tr>
<tr>
<td></td>
<td>Forces schedule restrictions on users. Specifically, if a user attempts to log into a client while they are off schedule, the login will fail. Utilizes User Schedules.</td>
</tr>
<tr>
<td>Failover</td>
<td>Source</td>
</tr>
<tr>
<td></td>
<td>Allows authentication attempts against this User Source to failover to another User Source in the event of a network outage, or some other connection issue. Useful with database or Active Directory user sources, as connection failures to the database /AD server will prevent users from logging in. This property in initially set to None, meaning a failover User Source is not configured.</td>
</tr>
<tr>
<td>Failover Mode</td>
<td>When a Failover Source is configured, this property determines when the failover User Source should be consulted. The following options are available:</td>
</tr>
<tr>
<td></td>
<td>Hard: The Failover User Source is only consulted when this User Source is unreachable.</td>
</tr>
<tr>
<td></td>
<td>Soft: The Failover User Source will be consulted if the user's credentials fail authentication, meaning that the user typed in credentials that are unrecognized or incorrect.</td>
</tr>
<tr>
<td>Cache</td>
<td>Validation Timeout</td>
</tr>
<tr>
<td></td>
<td>The amount of time between cache updates of the User Source.</td>
</tr>
</tbody>
</table>

The 'default' User Source

When Ignition is installed for the first time, an internal User Source named 'default' is created. This User Source contains the 'admin' user, and the Gateway uses this User Source as the system user source, so that users can initially log into the Gateway. You can manage the default User Source by navigating to the Configure > Security > Users, Roles section of the Gateway. The manage users link will allow you to add new users, modify roles and passwords for existing users, remove users, and add/remove roles from the user source. Choosing to edit a user will bring you to the following page allowing you to make any necessary changes to that user.
With potentially multiple User Sources defined, you need to understand which User Sources are controlling which aspects of Ignition. To determine what kind of User Source is governing what, do the following:

**The ‘admin’ user**

After installing Ignition, it is highly recommended to change the password for the admin user. The default user credentials to access the Gateway are public knowledge, and not fit for a production environment.

Alternatively, the admin user could be deleted, but a new user with the ‘Administrator’ role should be created first so that you will not be locked out of the Gateway. Should this occur, the Gateway Control Utility can be used to recreate the admin user.

**Which User Source Controls What?**

With potentially multiple User Sources defined, you need to understand which User Sources are controlling which aspects of Ignition. To determine what kind of User Source is governing what, do the following:
1. To manage users and passwords for logging into the Gateway Configuration section, you'll need to see what User Source is currently set as the Gateway's User Source. You can check this under **Configure > System > Gateway Settings** by looking at the System User Source field and the Gateway Config Role(s) field.

2. To manage users and passwords for logging into the Designer, you follow the same steps as in #1, except that you need to look at the Designer Role(s) field to see what roles are allowed to log into the Designer.

3. To manage users and passwords for logging into a Vision Client, you go to the **Configure > System > Projects** section. Look at the project in question and you can find its User Source listed there.

4. Now that you know what User Source you need to manage, you can find out what kind it is under the **Security > Users, Roles** section.

*In This Section ...*