

Ignition 7.9 User Manual — Security

Generated 2026-10-12 from
<https://www.docs.inductiveautomation.com/docs/7.9/>

This is documentation for **Ignition 7.9**, which is no longer actively maintained.

For documentation on the latest stable release, see the [latest version](#) (8.3).

Security

Ignition and Security

Security in Ignition is simple to set up and allows many ways to control who can use it and what things they have access to. You can add as many user sources as you want, and even connect with Active Directory to add your existing users! You can even store other information like phone numbers, schedules, and more.

Ignition uses what's known as role-based security. Actions such as accessing the **Gateway**, logging in to a **project**, interacting with a client, or modifying **windows** in a project can require specific roles. Users are stored in a User Source, which is a list of users, roles, and other useful information such as the user's name or phone number. By default, Ignition creates User Source automatically for you to use. The User Source contains the "admin" user that initially grants access to the Gateway.

Features of Ignition Security

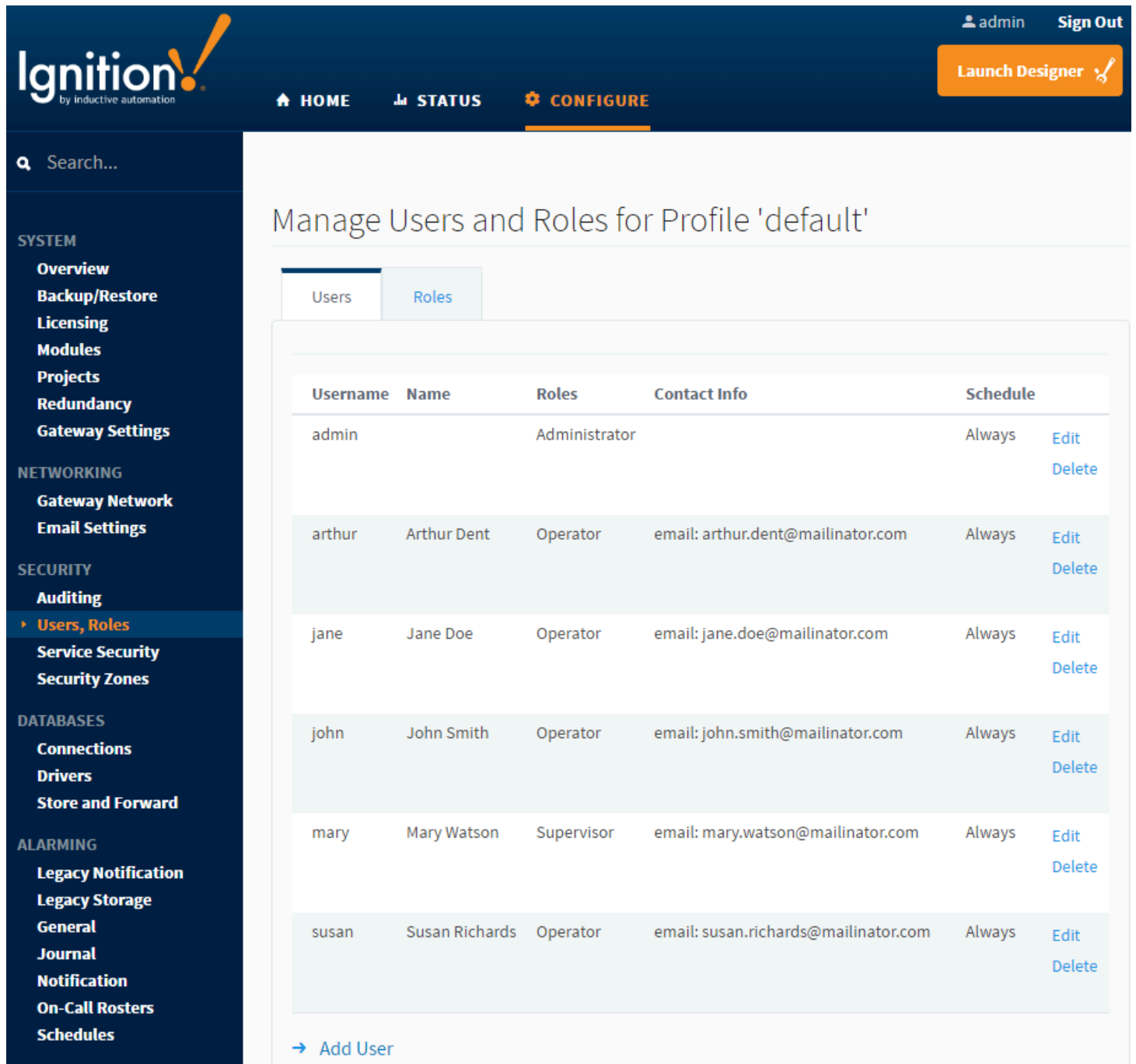
- Role-based security. Users can be assigned any number of roles, and roles can be checked at any time, in any project.
- **Adding new users** is simple. New users can be granted preexisting roles, and restrictions in Ignition will immediately be applied.
- **Database Authentication** Sources from external systems can be utilized in Ignition. Users will not need an additional password to log in to a client.
- **Authenticate against Active Directory (AD)**. **Roles can be created from AD groups**, or **custom roles can be assigned to users**. Additionally, Ignition clients support Single Sign ON (SSO).
- Multiple User Sources. Use the same User Source for all projects, or create a separate User Source for each project.

Users, Roles, and User Sources (Authentication)

Role-based security works under the concept that each user may be assigned to various roles. Security policies are then defined in terms of these roles, rather than defined for specific users. This

allows users to be reassigned, removed, and added without affecting the logic of the security policy.

The users and their roles are stored in **User Sources**. An Ignition Gateway may have many different User Sources defined, each governing the security of different aspects of the Gateway. For example, logging into the Gateway might be governed by one User Source, while the security in a project is governed by another.



The screenshot shows the Ignition Gateway web interface. The top navigation bar includes the Ignition logo, a search bar, and links for HOME, STATUS, and CONFIGURE. The CONFIGURE link is highlighted. The sidebar on the left contains a search bar and a list of system categories and their sub-items. The main content area is titled 'Manage Users and Roles for Profile 'default'' and features two tabs: 'Users' (selected) and 'Roles'. Below the tabs is a table listing users with columns for Username, Name, Roles, Contact Info, and Schedule. Each row has 'Edit' and 'Delete' links. At the bottom of the table is a link to 'Add User'.

Username	Name	Roles	Contact Info	Schedule
admin		Administrator		Always Edit Delete
arthur	Arthur Dent	Operator	email: arthur.dent@mailinator.com	Always Edit Delete
jane	Jane Doe	Operator	email: jane.doe@mailinator.com	Always Edit Delete
john	John Smith	Operator	email: john.smith@mailinator.com	Always Edit Delete
mary	Mary Watson	Supervisor	email: mary.watson@mailinator.com	Always Edit Delete
susan	Susan Richards	Operator	email: susan.richards@mailinator.com	Always Edit Delete

[→ Add User](#)

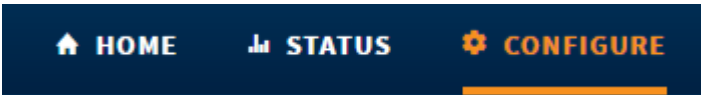
There are several types of User Sources that offer various features. For example, the **Internal User Source** offers the ultimate in ease-of-use: you simply define the users, their passwords, and the roles within the Ignition Gateway configuration web interface. In contrast, the **Active-Directory User Source** offers the power of integrating Ignition with a corporate security infrastructure. Users, passwords, and roles would be managed centrally by the IT department.

Contact Information and Schedules

User Sources are also used for other aspects of the system besides security. For example, the **alarm notification** system also takes user contact information to send alarm notification messages. A **schedule** can be defined for a user to control when they are able to log in, and when to receive alarm notification messages. Language preferences can be defined for each user to better support individual user's preferred language (**Localization**).

Gateway Security

The primary purpose of **Gateway security** is to protect access to the two most critical areas of Ignition: the Designer, and the Gateway. Many important resources are configured in these areas, so access to each Gateway section (**Home**, **Status**, and **Configure**), as well as the Designer, can be limited by role. Furthermore, the User Source authenticating Gateway access can be separate from those authenticating project access, allowing for compartmentalized authentication management.



SSL

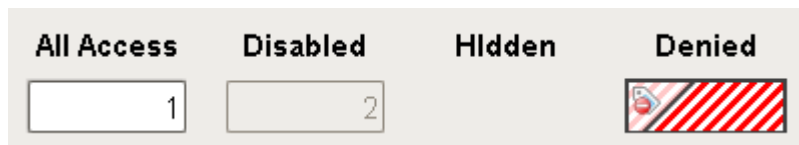
Ignition can use SSL with just one click by going to Configure > System > Gateway Settings! SSL (**Secure Sockets Layer**) is a widely adapted encryption protocol used all over the world. One of the main uses of SSL is to protect transferred data between a web-server and a web browser, but **Ignition clients can also benefit from this protocol** when communicating with the Gateway. Once enabled, data transferred between the Gateway and the client (such as recipe values, historical data, or customer accounts) will be encrypted. Thus the data will be unreadable by any malicious parties that may be eavesdropping in the network.

Use SSL	☐ Turns on SSL encryption when communicating with the Gateway. It is highly recommended that you purchase an SSL certificate from a certificate authority if you turn this feature on. (default: false)
---------	---

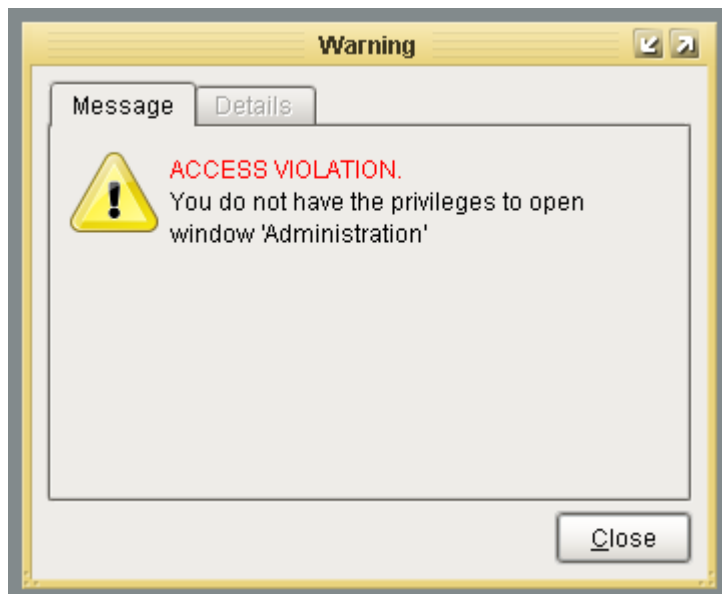
Project Security

Client Based Security

Easily control who can change values or even see your data. Security can be applied just about everywhere in a project. Individual components can check user roles from the client. Using Ignition's built-in **Security Settings**, the behavior of the component can change dynamically. This allows for a complex control scheme where components can be **hidden**, **disabled**, or **obscured** on a per-role basis. Project development becomes much easier! Develop once, and the Security Settings will control which components the user can interact with.



Security settings can also be applied to entire windows. Windows with administrator-level functionality can safely be added to a project without worry of unauthorized access.



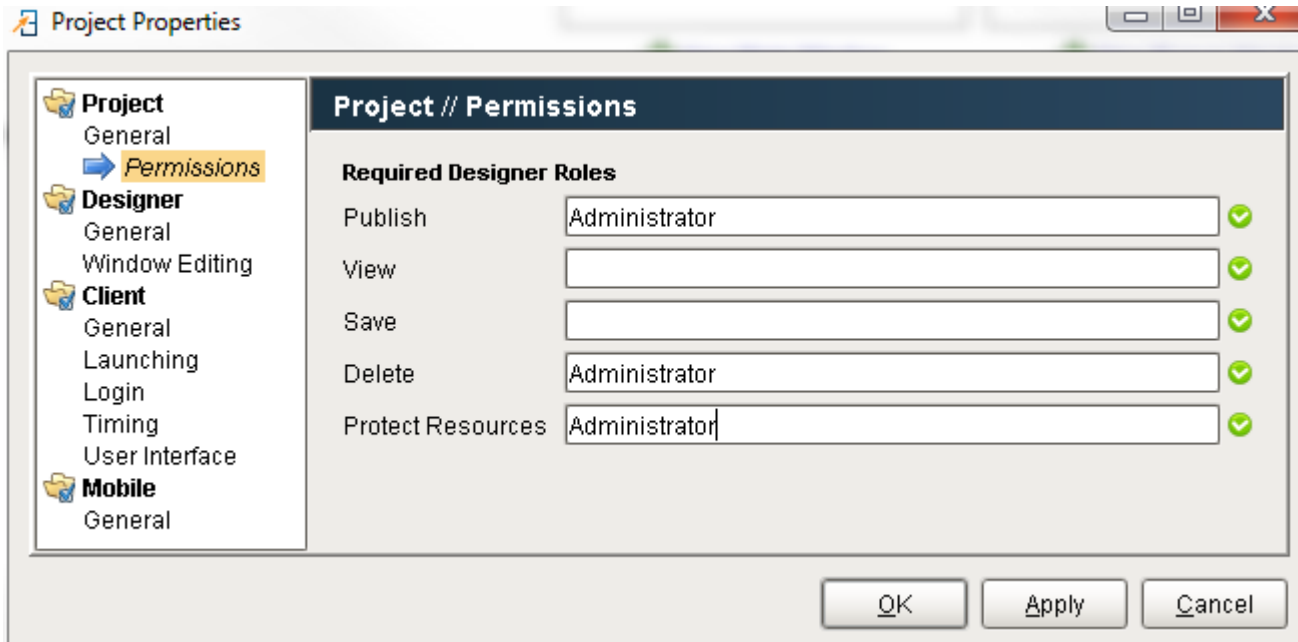
Furthermore, the **entire project** can be restricted to specific roles. This is commonly used when area-specific roles are given to users: i.e., operators in one location should not be able to view another site's project.

Looking for Multi-Conditional Security?

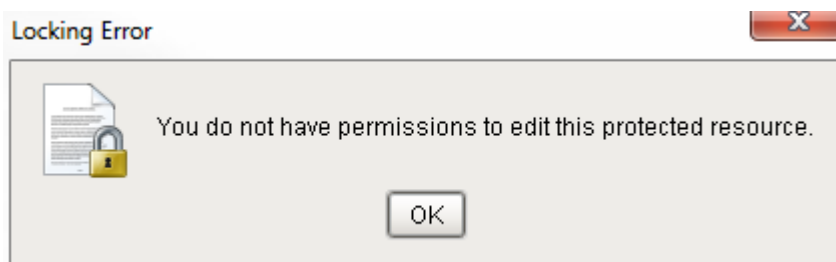
Roles can be checked from **any client-based scripting event**, so your security settings can go beyond just roles and account for specific times of the day, month, IP address, user names, lunar cycles, and anything else you can think of!

Project Based Access

Too many developers working on the same project could cause a number of problems: resource overlap, naming convention conflict, project creep, focus loss, and so on. To help with larger teams, Designer specific access levels can grant **project permissions** to certain roles. Actions such as **Publishing**, **Deleting**, or even **Viewing** the project in the designer can be restricted to certain roles.



Resources can also be **protected**, meaning that the window, template, or other resource should not be modified. This is a great way to flag an item as "complete" to the rest of the team, without having to manually document this information.



Auditing

Automatically record any changes that are made along with who did it, when it happened, and more. **Auditing** enables Ignition to record specific events to a SQL database. An Audit Profile can be used to record information for various systems in Ignition:

- **Project Auditing**: Record when users log in, log out, or write to any tags.
- **Notification Profile Auditing**: Record when a notification message would be sent. This reports who the notification was sent to, as well as if the attempt was successful or not.

Ignition provides a simple interface to view the Audit Log on the Gateway, and more.

Audit Log Viewer

Actor

Action

Target

Start Date

10/3/16

11

:

41

PM

End Date

10/4/16

11

:

59

PM

Search

Timestamp	Actor	Host	Action	Target	Value	Result	System	Context
10/4/16 7:40 AM	admin	WIN-VKBBHTNTPDV	tag write	New Tag[0]	6	AuditStatus[0x00000000, Severity=Good, Subcode=NotSpecified]	project=test	Designer
10/4/16 7:40 AM	admin	WIN-VKBBHTNTPDV	tag write	New Tag[4]	7	AuditStatus[0x00000000, Severity=Good, Subcode=NotSpecified]	project=test	Designer
10/4/16 7:40 AM	admin	WIN-VKBBHTNTPDV	tag write	New Tag[10]	8	AuditStatus[0x00000000, Severity=Good, Subcode=NotSpecified]	project=test	Designer
10/4/16 7:41 AM	admin	WIN-VKBBHTNTPDV	project save	test		AuditStatus[0x00000000, Severity=Good, Subcode=NotSpecified]	project=test	Designer
10/4/16 7:41 AM	admin	WIN-VKBBHTNTPDV	project publish	test		AuditStatus[0x00000000, Severity=Good, Subcode=NotSpecified]	project=test	Designer
10/4/16 7:41 AM	admin	WIN-VKBBHTNTPDV	project save	test		AuditStatus[0x00000000, Severity=Good, Subcode=NotSpecified]	project=test	Designer
10/4/16 7:41 AM	admin	WIN-VKBBHTNTPDV	project publish	test		AuditStatus[0x00000000, Severity=Good, Subcode=NotSpecified]	project=test	Designer

Since the activity is recorded into a SQL database, the data from the Audit Log can also be viewed by running a simple query. This way an "auditing" window can be added to any project, and allow any users (or users restricted to specific roles) the ability to view Activity recorded in the Audit Log. Even other systems can access the data in the Audit Log by querying the database!

File Edit View Project Component Alignment Shape Tools Help

Project Browser

Transaction Groups

Windows

Audit Events

Root Container

Label

Power Table

Rectangle

Tag Browser

Tag

Value

Data Type

Tags

Data Types

Audit Events

Timestamp	User	Action	Action Target	Action Value
Jun 28, 2016 11:53 AM	admin	tag write	B Tags/B3:0	1.0
Jun 28, 2016 11:49 AM	admin	logout		
Jun 28, 2016 11:49 AM	admin	login		

This is documentation for **Ignition 7.9**, which is no longer actively maintained.

For documentation on the latest stable release, see the [latest version](#) (8.3).

Managing Users and Roles



INDUCTIVE
UNIVERSITY

Role-based Access

[Watch the video](#)

Users and Roles

Security is based on the roles that are assigned to specific users. Roles do not have any structure or hierarchy by default, but can be created. You can create a hierarchy based on users with a greater role being assigned all matching lesser roles.

There isn't a built-in restriction to the number of roles a user can have, so each user can have access to many roles, or none at all.

ROLES AND SECURITY

It's important to think about the different roles in your project and how they affect the security of your project. For instance, what level of access a particular area of a project needs may determine the functional type roles that you create, and the different users assigned to each role.

You can manage users and roles using either the Gateway interface, or using the **User Management component** inside the Designer or Client. This section shows how to manage users and roles using the Gateway interface.

DANGER

When using role-based security in a project, the project stores the name of the role as a string. This means that if you were to modify the name of the role in the gateway, the role-based security in your project will not update to reflect the new name, and instead will try searching for a role with the original name. Be very careful when modifying the names of roles.

Creating a Role

1. On the Gateway webpage, go to the **Configure** section, and choose **Security > Users, Roles** from the menu on the left. The **User Sources** page is displayed.
2. Click on the **manage users** link for the **User Source** you want to manage.

User Sources

Name	Type	Description	
default	Internal	This is the default and always present internal authentication profile.	manage users edit
opcua-module	Internal	OPC-UA clients will authenticate against this profile by default.	More ▾ edit

3. Click the **Roles** tab, then look for the blue arrow at the bottom, and click the **Add Role** link.
4. Name the role by entering it in the **Role Name** field, and click on the **Add Role** button. The role is now available to be associated with specific users.

Users > Add Role[< back](#)[✓ Save](#)

Role name

Maintenance

✓

Assigning Roles to Users

1. On the Gateway webpage, go to the **Configure** section, and choose **Security > Users, Roles** from the menu on the left.
The User Sources page is displayed.
2. Click on the **manage users** link for the **User Source** you want to manage.
3. Click the **Edit** link for the User you want to edit, or click the blue **Add User** link to add a new user.
(When adding a new user, you can also add their roles at the same time).

Manage Users and Roles for Profile 'default'

Users

Roles

Username	Name	Roles	Contact Info	Schedule	
admin	Admin	Operator, Administrator	email: admin@inductiveautomation.com, phone: 800-266-7798	Always	Edit Delete
guest		guests		Always	Edit Delete

→

 Add User

4. If you're creating a new user, the Add User window will open. Enter the user's properties including the roles you want this user to have. If no roles have been created, then follow the instructions in the Creating a Role section from above. If your user already exists and you simply want to modify their roles, the Edit User window will open. (The Edit User window and the Add User window look identical).

To assign a role, there is a **Roles** property with a list of roles that have already been created. Select the role(s) that you want this user to have. (It's not required for a user to have a role, but be aware that they might not have access to an area of the project that requires them to have a role).

Roles

☒ Administrator
☐ guests

☐ Maintenance
☒ Operator

☐ Prod_Sups
☐ Test_Group



ADMINISTRATOR ROLE

When a project is first created, the **Administrator** role is the only role available, and no other roles will appear until they are created. When more roles are created, they appear as check boxes just like the Administrator option.

5. Click either **Add User** if you are adding a new user, or **Save Changes** if you are modifying a user's role(s). The user now has the privileges associated with the selected role(s).

Role Hierarchy

Often you might want one role that includes everything in the role below it. ie: Operator 1 can do everything that Operator 2 can, and more. This is possible to set up using the security roles for components in the designer, but is easier to give any Operator 1 both of the Operator 1 and Operator 2 roles.

Managing Users

User Sources support managing the users and roles from within Ignition to varying degrees. Some User Sources are fully manageable, meaning that you can administer the users, roles, contact info, and so on from within the Ignition Gateway, as well as inside a Vision Client. Other User Sources do not support this at all, while yet others only partially support it. Make sure you understand how and where the administration takes place before you choose a User Source type.

For User Sources that support it, you can manage the users and roles from within the Ignition Gateway's web configure interface under **Configure > Security > Users, Roles**. Click on the **manage** link next to the User Source you want to administer.

Often, it is desirable to let some management or administrative users of a Vision project manage other users without having to log into the Gateway's Configure section. To do this for a User Source that supports being managed, you can simply use the built-in **User Management Panel** that comes with the Vision Module.

User Management Component

Ignition has a special User Management component that allows you to add, modify, and delete users and roles (and more) inside the Designer and the Client. This is extremely simple to set up and use.

Using the User Management Component in the Designer and Client

1. In Designer, drag a **User Management** component to your window.
2. If you already have some users and roles setup using the Gateway interface, you will see those users and roles in the User Management component. If you don't have any users or roles setup, you can create them here. Use the icons on the right side to add, edit, or delete a user or role. The image below shows a header and some checkboxes because we are looking at the User Management page from one of the Project Templates.


User Management

Role Management Enabled: ☒ true
Show Username: ☒ true
Show Roles: ☒ true

Role Assigning Enabled: ☒ true
Show Name: ☒ true
Show Schedule: ☒ true

Contact Info Editing Enabled: ☒ true
Show Contact Info: ☒ true

Schedule Adjust Enabled: ☒ true

Users

Users

Username	Name	Roles	Contact Info	Schedule
admin	Maria	Operator, Adminis...	email: admin@in...	Always
guest		guests		Always
janedoe	Jane Doe	Operator	email: jane_doe...	Weekday Day Shift
operator	John Doe	Operator	email: iaoperator...	Always
jdoe	John Doe	Operator	email: john_doe...	Weekday Day Shift
Supervisor	Sal Supervisor	Prod_Sups	email: sup@maili...	Always
Sally	Sally	Operator	phone: 555-555-5...	Always

Roles

Role name	# of Members
Administrator	1
Operator	5
Prod_Sups	1
Test_Group	0
guests	1

- To add a new user, put the Designer in **Preview Mode**. Click the the **green plus icon** next to the user section.
- The Add User window will open. At a minimum, enter the **Username** and **Password**. All other properties are optional. When finished, click **Save**.
Click the **back** button to return to the Users section.

Users > Add User < back ✓ Save

User Properties

Username
 ✓

Password
 ✓
 ✓

First Name

Last Name

Schedule
 ↕

Language

Notes

Roles

- ☐ Administrator
- ☒ Operator
- ☐ Prod_Sups
- ☐ Test_Group
- ☐ guests

Contact Info

Type	Value
email	janderson@mailinator.com

✚ ✖ ⬆ ⬇

5. To add a new role, make sure the Designer is in **Preview Mode**, and click the the **green plus icon** next to the role.

The Add Role window will open. Enter the name of the new role. Click **Save**.

Click the **back** button to return to the Users window.

Users > Add Role < back ✓ Save

Role name

✓

6. Now you can see the user and role that were just added in the User Management window.

Users				
Users				
Username	Name	Roles	Contact Info	Schedule
admin	Maria	Operator, Admini...	email: admin@in...	Always
guest		guests		Always
janedoe	Jane Doe	Operator	email: jane_doe...	Weekday Day Shift
janderson	Jerry Anderson	Operator	email:	Always
operator	John Doe	Operator	email: iaoperator...	Always
jdoe	John Doe	Operator	email: john_doe...	Weekday Day Shift
Supervisor	Sal Supervisor	Prod_Sups	email: sup@mail...	Always
Sally	Sally	Operator	phone: 555-555-...	Always
Roles				
Role name		# of Members		
Administrator		1		
Maintenance		0		
Operator		6		

Save Failed. You are not authorized...

By default, changes to the system's user source may not be made from this component. This prevents users from locking themselves out of the gateway, or give themselves access to the gateway.

However, this behavior can be overridden from the Gateway: **Configure > System > Gateway Settings** page, and setting the checkbox for the '**Allow User Admin**' property. 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 selected user source and you will see an error at the bottom of the component if it is attempted.

Alternatively, you can simply have a separate User Source for the Gateway. This allows you to have a User Source containing all users that should have client access, and a Gateway-specific User Source that allows access to the Gateway and Designer. This would potentially entail changing the System's User Source: **Configure > System > Gateway Settings > System User Source** in the Gateway Webpage.

This is documentation for **Ignition 7.9**, which is no longer actively maintained.

For documentation on the latest stable release, see the [latest version](#) (8.3).

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

New in 7.9.1

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.

Name	Description
Name	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.
Description	An optional description of the user source. Useful for noting which database connection or AD server the User Source may be referencing.
Schedule Restricted	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 .
Failover Source	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 is initially set to None, meaning a failover User Source is not configured.
Failover Mode	When a Failover Source is configured, this property determines when the failover User Source should be consulted. The following options are available: Hard: The Failover User Source is only consulted when this User Source is unreachable. 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.
Cache Validation Timeout	The amount of time between cache updates of the User Source. New in 7.9.14 This property can be disabled if set to a number less than zero.

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.

Edit user "admin"

User Properties	
Username	admin
Change Password?	☐ Check this box to change the existing password.
Password	
Password	 Re-type password for verification.
First Name	Admin
Last Name	
Roles	☒ Administrator ☐ guests ☐ Maintenance ☒ Operator ☐ Prod_Sups ☐ Test_Group
Schedule	Always
Language	English
Notes	

Contact Info		
Type	Value	
E-Mail	admin@inductiveautomation.com	Up / Down Delete
phone	800-266-7798	Up / Down Delete
Add Contact Info		



TIP

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 > Sytem > 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.

This is documentation for **Ignition 7.9**, which is no longer actively maintained.

For documentation on the latest stable release, see the [latest version](#) (8.3).

Internal Authentication



INDUCTIVE
UNIVERSITY

Internal Authentication

[Watch the video](#)

Internal User Sources

An Internal type User Source stores user information internally in the Gateway's database. This means that Internal User Sources are included in Gateway Backup files, and don't require an external SQL database, or other external user management system.

When Ignition is first installed, the **"default" User Source** that initially grants access to the Gateway and Design is an Internal type User Source. You can, of course, continue to use this 'default' internal User Source for your project(s), or you may choose to use other User Sources instead.

The Internal User Source is fully **manageable** from within Ignition. You can access User Sources from the Gateway webpage under the **Configure** section, **Security > User, Roles**, and click the **edit** button.

User Sources

Name	Type	Description	
default	Internal	This is the default and always present internal authentication profile.	manage users edit
opcua-module	Internal	OPC-UA clients will authenticate against this profile by default.	More ▾ edit

Property Reference

This section details Internal User Source properties, organized by category.

Main Properties

Details on the Main Properties can be found on the [User Sources](#) page.

Password Policies Properties

The Internal User Source has password policies that are configurable from within the Gateway to provide an extra layer of security by ensuring that good password practices are used. You can change the default password policies by entering the appropriate password values to support your password policies. Below is a description of the Password Policy properties.

Name	Description
Password Maximum Age	The maximum age in days that the password will still be valid. After the number of days has past, when the user tries to login, it will prompt them to change their password. A value of 0 will disable this feature.
Password Minimum Length	The minimum amount of characters that a password must contain to be considered valid. If the user tries to make a shorter password, it will not allow it, and let them know that it does not meet the minimum length requirements.
Password Complexity	This determines how complex a password must be. There are four character types: lowercase letter, uppercase letter, digits, and special characters. The value here determines how many of those character types must be present at least once in the password for it to be considered valid.
Password History	Determines the number of previously used passwords to store. When users make a new password, old passwords can not be re-used. A value of zero disables this functionality. History is only stored while this setting is turned on, so any passwords used while this is off can be re-used when history is turned back on.

Password Policy

Password Max Age

The maximum age (in days) that a password is valid for. A value of zero disables password expiration.
(default: 0)

Password Min Length

Passwords must be at least this many characters long.
(default: 1)

Password Complexity

The number of character types (lowercase letters, uppercase letters, digits, punctuation) each password must contain. For example, a value of 3 means passwords must have 3 of the 4 character types to be considered valid.
(default: 1)

Password History

The number of previous passwords to store. Passwords in the history list may not be re-used. A value of zero disables this feature.
(default: 0)

This is documentation for **Ignition 7.9**, which is no longer actively maintained.

For documentation on the latest stable release, see the [latest version](#) (8.3).

Database Authentication



INDUCTIVE
UNIVERSITY

Database Authentication

[Watch the video](#)

Database User Source

The Database Authentication type uses an external database instead of storing data inside Ignition. Managing users is done via direct interaction with the database. This section addresses how to setup a database user source. The Database Authentication type requires you have a connection to an existing database, like SQL Server, Oracle, or MySQL. It stores all users, roles, schedules, and more in the database, and uses queries to check login credentials. When you create a database user source, you have the option of setting it up in Automatic or Manual mode.

Automatic Mode

In Automatic mode, Ignition will create and manage the database tables for you. You can specify a prefix for the tables that are created automatically for you, but their names after the prefix are chosen by the user source. In this mode, the user source will be fully **manageable** in Ignition.

Manual Mode

In Manual mode, you must provide SQL queries for various functions of the user source. In this mode, the user source will not be manageable from the Gateway or the Clients. You'll have to manage the users directly through the database. Examples for each of the queries are given on the user source setup page. Read each query description carefully to make sure you design your queries to return all the columns that are defined in the query's description as shown below.

Property Reference

Database User Sources have the following properties, organized by category

Main Properties

Details on the Main Properties can be found on the [User Sources](#) page. The Database User Source also has the following properties:

Name	Description
Database	The database connection this User Source will retrieve user information from.
Mode	How the gateway should manage the database tables. Has two settings Automatic: The gateway will automatically create the database tables necessary, and all interactions with the table will use the built-in queries. When this option is set, the Tablename Prefix property is utilized. Manual: The gateway will not automatically create any database tables, nor will it automatically modify users or roles. When set to manual, it is assumed that you want to manually write the queries that update the tables, or are utilizing another system. When Mode is set to this option, the Manual Mode properties are used to determine how the gateway should query user data.

Automatic Mode Properties

Name	Description
Tablename Prefix	When set to Automatic mode, this property determines the prefix that will be used on all automatically created tables. Useful when multiple database User Sources are connected to the same database scheme.

Manual Mode

Name	Description
Authentication Query	A query that must return a row if the given username and password combination provided is valid. The query will run as a prepared statement, so use the question mark character (?) to represent username first and then password. The returned row may contain the user's basic properties under the column names: • firstname • lastname • schedule • language • notes Note that the gateway will pass both the username and password the user typed in, so this query MUST utilize exactly two question marks, otherwise an exception will occur.
List Roles Query	A query that returns all possible roles that any user could be a member of. The role names must be returned in the first column of the query's results.
User's Roles Query	A query that returns all of the roles that the provided user belongs to. The roles must be strings and must be in the first column of the query's results. The query will be run as a prepared statement with one parameter: the username.

Name	Description
List Users Query	A query that returns a row containing each username. There must be at least one column: the username. Other columns are optional, supported columns are: • username • firstname • lastname • schedule • language • notes
Contact Info Query	A query that returns all of the contact info for the user. The first column must be the contact type, the second column the contact value. Optional, may be blank.
Schedule Adjustment Query	A query that returns the upcoming schedule adjustments for the user. This property is optional, and may be left blank. The results set expects the following columns: • Start(date) • End(date) • Available(boolean) • Note(string)
Extra Properties Query	A query that returns name, value pairs of extra properties for the user. Will be run with one parameter: the username. Optional, may be blank.

To Create a Database User Source

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

2. Choose the **Database** 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, but if you're using Automatic mode, enter the following properties as appropriate.

- **Name:** DBAuth - name of the user source.
- **Failover Source:** default - failover user source ('default' is the internal user source).
- **Failover Mode:** Hard - if the source is unreachable, then use the failover source. (Can choose the Hard or Soft option).
- **Database:** MySQL - external database.
- **Mode:** Automatic - tables in the external database will be automatically created when needed.
- **Tablename Prefix:** 'auth_' is the prefix for all the tables that get created. (You can leave this field blank, but if you use a prefix when the tables get created, they will contain the specified prefix in their name).

- When finished, click **Create New User Source**.

New User Source

Main	
Name	DBauth
Description	Database authentication
Schedule Restricted	☐ Users are only able to log in when their assigned schedule is active. (default: false)
Failover Source	default If this source is unreachable for authentication, this failover source will be used instead.
Failover Mode	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. (default: HARD)
Cache Validation Timeout	60000 The amount of time between cache updates of the user source. (default: 60,000)

Main Properties	
Database	MySQL Choose the database connection this user source will use.
Mode	Automatic In Automatic mode, tables will be created for you and all interaction with the database is handled automatically. In Manual mode, you write queries by hand against tables that you've created. Management of users (adding, removing etc) is not supported in manual mode. (default: Automatic)

Automatic Mode	
Tablename Prefix	auth_ When in automatic mode, tables will be created to store the users and roles. They will have this prefix. (default: scada_)

TABLE CREATION

The tables in the database will not be created in the database until they are needed. For example, as soon as a user or role is added, the associated tables will automatically get created.

- Now that your Authentication profile is created, add a user. On the right, click on the **More > Manage Users** link. Click on the **Add User** link and fill in the required fields.
- Now that your tables are created we can verify them. To view the tables, go into **Designer** and from the menu bar, select **Tools** in the menubar, then **Database Query Browser**. You will see all the tables that were created beginning with 'auth_' when the user and role get created.
- Double click on any of tables beginning with 'auth_', and click **Execute**. In this example, you will see the tables associated with 'roles' and 'users' displayed in the Schema area.

Database Query Browser

```
SELECT * FROM auth_users
```

☒ Limit SELECT to: 1000 rows

Resultset 1

id	username	passwd
1	User1	W6ph5Mm5Pz8GgiULbPgZG37mj... NUL

1 row fetched in 0.002s

Auto Refresh Edit Apply Discard

Schema History

- auth_roles
- auth_user_ci
- auth_user_ex
- auth_user_rl
- auth_user_sa
- auth_users**
 - id (INT) 🔑
 - fname (VARCHAR)
 - language (VARCHAR)
 - lname (VARCHAR)
 - notes (VARCHAR)
 - passwd (VARCHAR)
 - schedule (VARCHAR)
 - username (VARCHAR)

This is documentation for **Ignition 7.9**, which is no longer actively maintained.

For documentation on the latest stable release, see the [latest version](#) (8.3).

Active Directory Authentication

Active Directory User Source

The Active Directory Authentication profile uses Microsoft's Active Directory over **LDAP** (Lightweight 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

CAUTION

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.

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 Changed in 7.9.20 This setting was disabled and deprecated in 7.9.20 to protect against a potential security vulnerability. While the property is still visible, it cannot be enabled without setting a special system property. This is not recommended. Check out the Active Directory SSO Disabled for 8.1.17 & 7.9.20 article for more information.
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 <code>@<domain></code> .
User Search Base	The base folder to search for users under, such as: <code>DC=MyCompany,DC=com</code> 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: <code>(OU=Administrators,DC=MyCompany,DC=com)</code> <code>(OU=Operators,DC=MyCompany,DC=com)</code>
User Search Filter	The LDAP search filter that will be used to find a specific user. Use the placeholder <code>0</code> as a standing 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.

Name	Description
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: <code>OU=Roles,DC=MyCompany,DC=com</code> 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: <code>(OU=BuiltIn,DC=MyCompany,DC=com)(OU=Users,DC=MyCompany,DC=com)</code> 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 <code>ldap://</code> protocol, enable to use <code>ldaps://</code>
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.

Name	Description
	• 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**.

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. 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.

Project Properties

Project
General
Permissions

Designer
General
Window Editing

Client
General
Launching
Login
Timing
User Interface

Mobile
General

Client // Login

Login Screen

Welcome Message

Welcome Image 

Username Text

Password Text

Login Button Text

Show Locale Selector 

Auto Login

Enable Auto-Login ☐

Username

Password

Password (repeat)

SSO Login

Enable SSO Login ☒

OK Apply Cancel

This is documentation for **Ignition 7.9**, which is no longer actively maintained.

For documentation on the latest stable release, see the [latest version](#) (8.3).

AD Internal Hybrid



INDUCTIVE
UNIVERSITY

AD Internal Hybrid

[Watch the video](#)

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.

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	ADInternalHybrid
Description	
Schedule Restricted	☐ Users are only able to log in when their assigned schedule is active. (default: false)
Failover Source	default If this source is unreachable for authentication, this failover source will be used instead.
Failover Mode	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. (default: HARD)
Cache Validation Timeout	60000 The amount of time between cache updates of the user source. (default: 60,000)

Active Directory Properties	
Domain	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	The IP address or hostname of your primary domain controller. Example: "192.168.1.4" or "MainServer"
Primary Domain Controller Port	389 The port number for the primary domain controller's LDAP interface. (default: 389)
List Users from Active Directory	☒ If true, Active Directory will be queried for the list of all users. If false, users must be added manually. (default: true)
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. (default:)
Password	The password for the above username.
Password	Re-type password for verification.
SSO Enabled	☐ 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. (default: false)
SSO Domain	The domain that Windows users must match in order to use SSO. If blank, the main "Domain" property will be used. (default:)

☐ Show advanced properties

Create New User Source

This is documentation for **Ignition 7.9**, which is no longer actively maintained.

For documentation on the latest stable release, see the [latest version](#) (8.3).

AD Database Hybrid



INDUCTIVE
UNIVERSITY

AD Database Hybrid

[Watch the video](#)

AD/Database User Source

This AD/Database Hybrid User Source is not **manageable** from within Ignition. Users/passwords must be administered through **Active Directory**, and roles, contact info, and so on, must be administered directly through the database. The way AD/Database Hybrid works, is it has all the same information requirements as the other authentication profiles, but it also has a number of Database properties. You need to specify a database (i.e., MySQL) to store information, and setup queries that you want to use. You must also specify the host that is acting as your primary domain controller, and 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 when it queries the list of roles.

Property Reference

This User Source shares many properties with both the AD User Source and Database User Source.

- See the [Active Directory Authentication](#) page for a list of Active Directory User Source related properties.
- See the [Database Authentication](#) page for a list of Database User Source related properties.

Creating an AD/Database Hybrid User Source

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/Database 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 >

i MAY NEED TO CONTACT YOUR INTERNAL IT DEPARTMENT FOR..

When using AD/Database 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. The New User Source window will open. Some properties are optional depending on how you setup your profile.

New User Source

Main	
Name	ADDBHybrid
Description	
Schedule Restricted	☐ Users are only able to log in when their assigned schedule is active. (default: false)
Failover Source	default If this source is unreachable for authentication, this failover source will be used instead.
Failover Mode	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. (default: HARD)
Cache Validation Timeout	60000 The amount of time between cache updates of the user source. (default: 60,000)

Active Directory Properties	
Domain	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	The IP address or hostname of your primary domain controller. Example: "192.168.1.4" or "MainServer"
Primary Domain Controller Port	389 The port number for the primary domain controller's LDAP interface. (default: 389)
List Users from Active Directory	☒ If true, Active Directory will be queried for the list of all users. If false, the database will be queried instead. (default: true)
Gateway Username	The login name for the gateway to use when querying Active Directory. Used for retrieving the list of users via LDAP. (default:)
Password	The password for the above username.
Password	Re-type password for verification.
SSO Enabled	☐ 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. (default: false)
SSO Domain	The domain that Windows users must match in order to use SSO. If blank, the main "Domain" property will be used. (default:)

Database Properties	
Database	MySQL ▾ Choose the database connection this authentication profile will use.
User Properties Query	A query that returns the basic properties for a single user. Supported return columns are [firstname, lastname, schedule, language, notes]. The username will be inserted into this query as a parameter. Example: <code>SELECT firstname, lastname, schedule, language, notes FROM user_table WHERE username = ?</code>
Role List Query	A query that returns all possible roles that any user could have. The role names must be returned in the first column of the query's results. Example: <code>SELECT rolename FROM roles</code>
User's Roles Query	A query that returns all of the roles that the provided user belongs to. The roles must be strings (i.e. the role names), and must be in the first column of the query's results. The username will be inserted into this query as a parameter. Example: <code>SELECT rolename FROM user_role_mapping WHERE username = ?</code>
Contact Info Query	A query that returns all of the contact info for the user. The first column must be the contact type, the second column the contact value, and the third column the name of a schedule. Optional, may be blank. Example: <code>SELECT contact_type, contact_value, schedule FROM user_contact WHERE username=?</code>
Schedule Adjustment Query	A query that returns the upcoming schedule adjustments for the user. Columns must be Start(date), End(date), Available(boolean), Note(string). Optional, may be blank. Example: <code>SELECT start_date, end_date, is_available, note FROM user_schedule_adj WHERE username=?</code>
Extra Properties Query	A query that returns name, value pairs of extra properties for the user. Will be run with one parameter: the username. Optional, may be blank. Example: <code>SELECT prop_name, prop_value FROM user_props WHERE username=?</code>
List Users Query	A query that returns a row containing each username. Only used if "List Users from Active Directory" is false. There must be at least one column: the username. Other columns are optional, supported columns are: [username, firstname, lastname, schedule, language, notes]. Example: <code>SELECT username, firstname, lastname, schedule, language, notes FROM user_table</code>

This is documentation for **Ignition 7.9**, which is no longer actively maintained.

For documentation on the latest stable release, see the [latest version](#) (8.3).

Fallback Cache Authentication

New in 7.9.1

Overview

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.

Creating the Fallback Cache User Source

The Fallback Cache User Source is created in a similar fashion to any other User Source:

1. **Gateway Webpage > Configure > Security > User, Roles** > Click on the **Create new User Source...** link.
2. Select the Fallback Cache option and click the **Next** button.
3. Type in a name for the new User Source and click **Create New User Source**.

User Source Properties

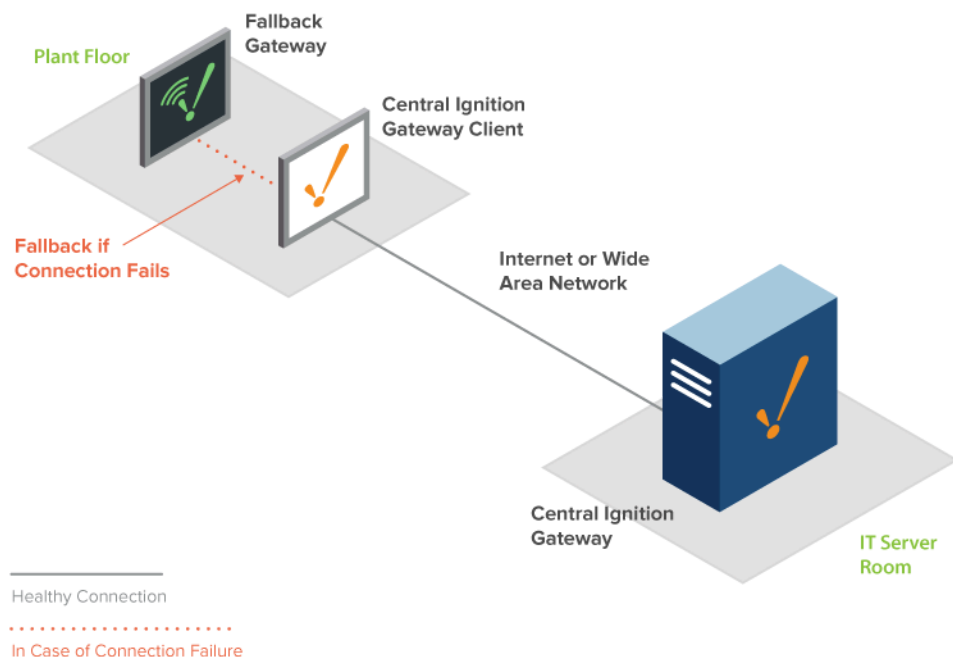
The Fallback Cache User Source has many of the same common or **Main** properties as other User Sources, but it does have one unique property:

Cache Retention: This property determines the number of days credentials will be stored in the cache. Once exceeded, the credentials will be removed from the cache.

Populating the Cache

Users and Roles can not be manually added to the Fallback Cache. Instead, they are automatically copied from remote Gateways. This type of User Source is normally configured on an **Edge Gateway**, but can be utilized on an Ignition Gateway.

1. Before the Fallback Cache will populate, both the **Central Ignition Gateway** and **Fallback Gateway** must be connected over the **Gateway Network**. The credentials are passed from a User Source on the **Central Ignition Gateway** to the Fallback Cache over the Gateway Network.
2. A Fallback Cache User Source must exist on the **Fallback Gateway**.
3. A client must be launched on the **Fallback Gateway** from the **Central Ignition Gateway**. If the user successfully authenticates against the **Central Ignition Gateway's** User Source, then the credentials are cached into the Fallback Cache.



This is documentation for **Ignition 7.9**, which is no longer actively maintained.

For documentation on the latest stable release, see the [latest version](#) (8.3).

Verifying a User Source



INDUCTIVE
UNIVERSITY

Verifying an Authentication Profile

[Watch the video](#)

You can verify that a user exists in a given User Source, if the password is correct, what roles a user has, and any other information added about the user.

To Verify a User

1. Go to the **Configure** section of the Gateway.
2. Choose **Security > Users**, Roles from the menu on the left. The **User Sources** page is displayed.
3. Select the **Verify an Authentication Profile** link.

User Sources

Name	Type	Description	
default	Internal	This is the default and always present internal authentication profile.	manage users edit
opcua-module	Internal	OPC-UA clients will authenticate against this profile by default.	More ▾ edit

[→ Create new User Source...](#)
[→ Verify an Authentication Profile...](#)

4. The Verify Authentication Profile window will appear. Choose a **Profile** from the dropdown list. Enter a **Username** and **Password**. Click **Test Login**. Ignition will test the credentials then display the results of the validity test.

Verify Authentication Profile

 Use this page to test your Authentication Profile's settings.

Test Login	
Profile	default ▼
Username	admin
Password	*****

Test Login

If the Login is incorrect, an error message will appear stating that the Login failed for a specified user. If the Login is correct, a successful message will appear for a specified user along with their information.

Login Successful

 Login succeeded for user "admin"

User's roles:

Username	admin
First Name	Admin
Last Name	
Schedule	Always
Roles	• Operator • Administrator
Contact Info	• email / admin@inductiveautomation.com • phone / 800-266-7798

Extended Properties

[Test again...](#)

This is documentation for **Ignition 7.9**, which is no longer actively maintained.

For documentation on the latest stable release, see the [latest version](#) (8.3).

Gateway Security



INDUCTIVE
UNIVERSITY

Changing admin Password

[Watch the video](#)

By default, the **Configure** section of the Gateway is password protected, and this cannot be removed. You can also optionally protect the **Status** and the **Home** sections of the Gateway webpage. The roles that are required to access any of these sections can be changed in the **Configure** section of the Gateway webpage under **System > Gateway Settings**.

The default username and password for the Configure and Status sections of the Gateway is:

username: **admin** password: **password**

Changing the 'admin' Password

When Ignition is first installed, a default "admin" user automatically gets created. Once you're logged into Ignition, you have access to everything in the system as the 'admin' user. You can modify projects, add users and roles, add database connections, setup the Gateway, and literally do everything.

The first step in securing your Ignition installation is to change the default username/password for the 'admin' user.

1. On the Gateway webpage under the **Configure** section, go to **Security > Users, Roles**. The default user source contains the 'admin/password' combination to access the Configure section.
2. Click on **manage users** and you will see the admin user.
3. On the right side, click **edit** to change the password for the admin user.

Manage Users and Roles for Profile 'default'

Users

Roles

Username	Name	Roles	Contact Info	Schedule	
admin	Admin	Operator, Administrator	email: admin@inductiveautomation.com, phone: 800-266-7798	Always	Edit Delete

4. Click the **checkbox** to change the existing password.
Enter the new password, then re-type the new password to confirm it.

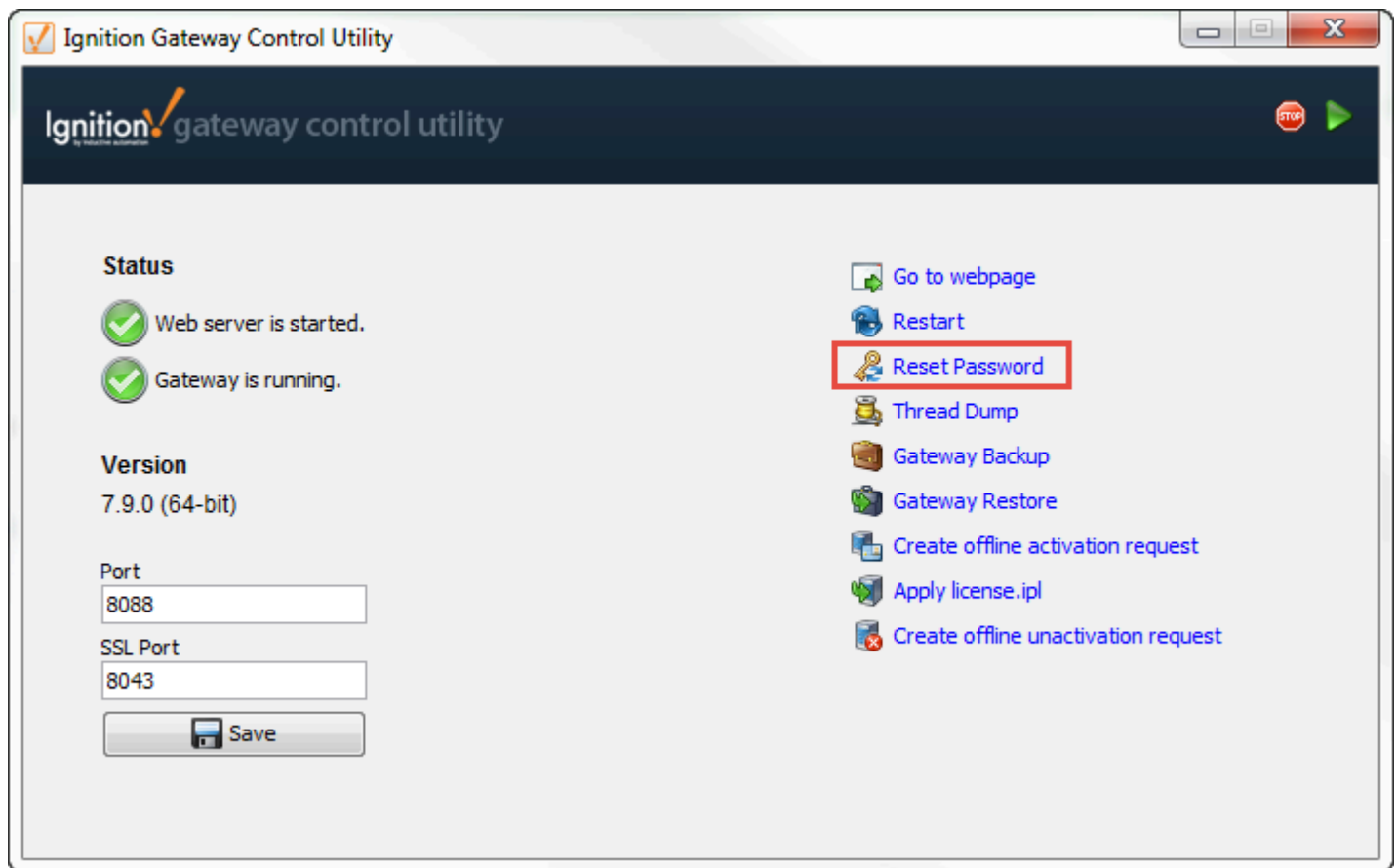
User Properties

Username	admin
Change Password?	☒ Check this box to change the existing password.
Password	*****
Password	***** Re-type password for verification.

5. When you're finished, click Save Changes.
6. To test the new password, logout and log back in as the admin with the new password.

Password Reset

Ignition provides you with the capability to reset the admin password from the Gateway Control Utility (GCU). The default is user/password combination is '**admin/password,**' and will grant access to the Gateway webpage. Normally, this is not considered a security risk because the GCU can only be used from the machine the software is installed on, which should be secure. However, it is important to know about this feature so that the GCU can be removed if the machine can't be properly secured, for example, when the server is also used as a client.



Locking the Gateway



INDUCTIVE
UNIVERSITY

Locking the Gateway

[Watch the video](#)

You can set up security for the Gateway webpage sections and the Designer. The Gateway can use any existing authentication profile independent of any projects. Each of the Status, Home, and Configure pages can be restricted by role. Outside of logging into a Client, the Designer as well can require a special role.

Here is where you should start thinking about your security policy. Roles play an important part. Roles allow you to provide access to different areas of the Gateway (and project). We recommend that you create separate roles for the Gateway Configure Page, Status Page, Home Page, and Designer so that individual users only have access to specified areas where they will be working.

To Setup Security for the Gateway

1. Go to the **Configure** section of the Gateway.

2. Choose **System > Gateway Settings** from the menu on the left.

The **Gateway Settings** page is displayed.

3. Enter the roles the user must have in order to access the **Gateway Config Roles**, **Status Page Roles**, **Home Page Roles**, and **Designer Roles**.

Each option can accept any number of roles as long as they are separated by commas. Also, if the option is blank, any user can log in. The **Global Resource Protection** will shelter the Global Resources (like Alarm Pipelines or SFCs) from edits by users without a matching role.

Gateway Settings	
System Name	Controller The name of this Ignition system, used to differentiate this system from others in a larger architecture. (default:)
System User Source	default This user source controls access to the Gateway's web configuration interface and the Designer.
Gateway Config Role(s)	Administrator,super_admin Users must belong to one of these roles in order to log into the configuration section. Multiple roles can be specified by separating them with commas. (default: Administrator)
Status Page Role(s)	Administrator Users must belong to one of these roles in order to log into the status section. Multiple roles can be specified by separating them with commas. If blank, the status page will not be password-protected. (default: Administrator)
Home Page Role(s)	 Users must belong to one of these roles in order to log into the home section. Multiple roles can be specified by separating them with commas. If blank, the home page will not be password-protected. (default:)
Designer Role(s)	Administrator,super_admin Users must belong to one of these roles in order to log into the Designer. Multiple roles can be specified by separating them with commas. (default: Administrator)
Create Project Role(s)	Administrator Users must belong to one of these roles in order to create a new Designer project. Multiple roles can be specified by separating them with commas. (default:)
Global Resource Protection	Administrator,super_admin The roles required to protect or modify a protected global resource such as an alarm pipeline. If blank, anyone that can log into the Designer can protect global resources. (default:)

Enabling SSL



INDUCTIVE
UNIVERSITY

Requiring SSL

[Watch the video](#)

To enhance security in Ignition, you may opt to enable SSL encryption. This will affect all communication to and from the Gateway that is done over the HTTP protocol. This includes not only browsers interacting with the Gateway's web interface, but all Vision Client communication as well. Turning on SSL will encrypt all data sent over HTTP. This protects your installation from anyone "snooping" the data as it passes over the network. This may be important if data transferred between the Gateway and Clients is sensitive in nature. This also helps to thwart a security vulnerability known as "session hijacking".

To Turn On SSL

1. Go to the **Configure** section of the Gateway.
2. Choose **System > Gateway Settings** from the menus on the left.
3. Select the checkbox for **Use SSL**, and click on **Save Changes** at the very bottom of the page.

Use SSL	☒ Turns on SSL encryption when communicating with the Gateway. It is highly recommended that you purchase an SSL certificate from a certificate authority if you turn this feature on. (default: false)
---------	--

After SSL is enabled, all Clients, Designers, and web browsers are redirected to the SSL port if they try to use the standard HTTP port. By default, the SSL port is 8043. You can change it to the standard SSL port of 443. To do this, follow the directions in [Setting the Port](#).

**SSL PORTS - FIREWALL RULES

If you are using a firewall, both SSL and HTTP ports must be open for a client to launch (i.e., 8088 and 8043). Following the initial connection, all traffic will happen over the SSL port.

New in 7.9.8 You can now setup Ignition to use HTTP Strict Transport Security (HSTS) policy. To do this, there needs to be a change made to the ignition.conf file and the Gateway needs to be setup to use SSL.

```
-Dignition.https.sts.maxAge="47474747"  
-Dignition.https.sts.includeSubDomains="true/false"
```

Each of those lines need to be added as a Java Additional Parameter to the ignition.conf file. Each parameter needs to be added as the next available uncommented parameter in the list of parameters. So if the last uncommented parameter is 4, then these lines should be added like the following:

```
wrapper.java.additional.5=-Dignition.https.sts.maxAge="47474747"  
wrapper.java.additional.6=-Dignition.https.sts.includeSubDomains="true/false"
```

Once these have been added and Use SSL turned on, the Gateway can be restarted, at which point it will be using HSTS properly.

DANGER

Do not place those parameters in the ignition.conf file without turning on Use SSL. If Use SSL is not turned on, those parameters may prevent your Gateway from starting.

When Using SSL

Ignition supports using SSL communications to the Gateway webpage as well as Client/Designer communication with the Gateway. It is highly recommended that you purchase an SSL certificate from a certificate authority if you turn this feature on. The procedures for **How to Install a Genuine SSL Certificate** are below.

Installing a Genuine SSL Certificate

When you turn on SSL in Ignition, the web browser uses what is called a "self-signed" certificate. This gives you the encryption benefits of SSL, but not the identity validation, and it isn't a "real" certificate. This is why a web browser will display nasty warnings to users that they shouldn't trust the website.

We are not able to ship a real certificate with Ignition because SSL certificates have to be purchased individually from a certificate authority, such as Verisign, GoDaddy, or Comodo.

This guide shows you how to purchase and install a real SSL certificate from a certificate authority and install it in Ignition. You'll need to be comfortable executing command-line programs to complete this guide. The examples in this guide assume a Windows environment, but the general procedure would be identical in Linux.

1. Install the Java Development Kit (JDK).

There are some command-line tools you'll need to use to create a certificate request and to install your certificate. These tools come with the Java Development Kit (JDK). It is likely that you only have the Java Runtime Environment (JRE) installed. Go to <http://java.oracle.com> and click on Java SE. Download the Java SE 6 JDK and install it.

2. Open a command prompt.

Open a command prompt from **Start > Run > cmd** and change directory into your JDK tools directory.

```
cd C:\Program Files\Java\jdk1.6.0_24\bin
```

3. Create your KeyStore.

SSL certificates for Ignition are stored in a file called a `KeyStore`. You'll need to create your own `KeyStore` file with a certificate in it before you can purchase the SSL certificate.

i. Enter the following command:

```
keytool -genkey -alias tomcat -keyalg RSA -keysize 2048 -keystore C:\ssl.key
```

you can put the file wherever you want for now, but you should call it `ssl.key`

ii. At the prompt, enter a password. Use the password: `ignition`

iii. At the prompt, you are asked for your `first and last name`. Do not use your first and last name. This value must be one of the following for your Ignition Gateway:

a. Fully Qualified Domain Name, for example `secure.yourdomain.com`

b. Public IP address, for example `202.144.8.10`

c. Full Server Name of your internal server, for example `scadaserver`

d. Private IP address, for example `192.168.0.1`

iv. At the prompt, you are asked for information about your company. Input all data accurately, as the certificate authority needs to verify this information.

v. Lastly, at the prompt, you are asked for the password for `alias <tomcat>`. Press RETURN to use the same password as the `KeyStore` file.

4. Generate a Certificate Signing Request.

You have a `KeyStore` file named `ssl.key` at the root of your `C:\` drive (or wherever you specified it to be in step 3a).

In your command prompt window, enter this command:

```
keytool -certreq -alias tomcat -file C:\csr.txt -keystore C:\ssl.key
```

It will prompt you for the `KeyStore` password (`ignition`). You now have a certificate request file at `C:\csr.txt`

5. Buy the SSL certificate.

Now you need to get your SSL certificate signed by a certificate authority. When you go to a certificate authority (Verisign, GoDaddy, Comodo, and so on), they'll ask for your CSR, which is the `csr.txt` file that you created in step 4. Typically they'll ask you to paste your CSR into their web form. Open `csr.txt` in notepad, and copy-and-paste it into the certificate authority's form. If prompted what software generated the CSR, choose Tomcat or Java. After the certificate authority has processed your payment and reviewed your CSR, they will send you your certificate via email.

6. Install the SSL certificate.

After your SSL certificate has been emailed to you, follow the instructions provided for installing

the certificate into a Java KeyStore. Your certificate authority provides these instructions. The following is the procedure for installing a Comodo SSL certificate, provided as an example:

- i. Extract the certificate files that were emailed to you, in this example they were extracted to

`C:\cert`

- ii. Install the root certificate with the following command:

```
keytool -import -trustcacerts -alias root -file
```

```
C:\cert\AddTrustExternalCARoot.crt -keystore C:\ssl.key
```

- iii. Install the COMODO intermediate certificate:

```
keytool -import -trustcacerts -alias INTER -file C:\cert\COMODOHigh-
```

```
AssuranceSecureServerCA.crt -keystore C:\ssl.key
```

- iv. Install your server's certificate:

```
keytool -import -trustcacerts -alias tomcat -file C:\cert\192_168_1_7.crt -
```

```
keystore C:\ssl.key
```

7. Replace Ignition's default KeyStore.

You now have a KeyStore file at `C:\ssl.key` that holds your SSL certificate. The certificate alias is `tomcat` and the password is `ignition`. You can now replace the `KeyStore` file that ships with Ignition with your file. Make a backup of the file at `C:\Program Files\Inductive Automation\Ignition\tomcat\ssl.key` and replace it with your `KeyStore` file. You need to restart the Ignition service after replacing this file.

Make sure your SSL port is allowed through your server's firewall. The default SSL port is 8043, and can be changed to the standard SSL port (443) through the Gateway Control Utility (GCU). If you have a redundant installation, you'll need to repeat this procedure on your backup server and buy a second certificate for it.

Metro KeyStore System Properties

New in 7.9.13 Aliases, passwords, and private key passwords can now be set on both the webserver's KeyStore, as well as the Metro KeyStore via modifications to the `ignition.conf` file. Making these changes is similar to the process described under the To Turn SSL On header above. Thus:

```
wrapper.java.additional.5=-Dmetro.keystore.alias="New Alias"  
wrapper.java.additional.6=-Dignition.ssl.keystore.alias="Another Alias"
```

Once these have been added, the Gateway must be restarted for the change to take effect. A listing of possible properties are shown below.

KeyStore File Path: `$IGNITION/webserver/metro-keystore`

System Property	Default Value	Description
metro.keystore.password	metro	The SSL KeyStore password.
metro.keystore.password	metro-key	The alias of the target SSL KeyStore entry.
metro.keystore.password	The value of system property metro.keystore.password	The encrypted private key password.

SSL KeyStore System Properties

KeyStore File Path: `$IGNITION/webserver/ssl.key`

System Property	Default Value	Description
ignition.ssl.keystore.alias	tomcat	The alias of the target SSL KeyStore entry.
ignition.ssl.keystore.password	ignition	The SSL KeyStore password.
ignition.ssl.privatekey.password	The value of system property ignition.ssl.keystore.password	The encrypted private key password.

This is documentation for **Ignition 7.9**, which is no longer actively maintained.

For documentation on the latest stable release, see the [latest version](#) (8.3).

Using Audit Profiles

Audit Profiles cause Ignition to record details about specific events that occurred. Audit Profiles are simple to set-up, and immediately start to record events. By default, only Tag writes, SQL UPDATE, SQL INSERT, and SQL DELETE statements are recorded. This allows you to keep track of which user wrote to which Tag, or modified which table. Furthermore, a time-stamp is recorded, so you can easily track the changes and outline an order of events.

New in 7.9.13 Ignition Gateways can now create an **Internal Audit Profile**, allowing an Ignition Gateway to store audit records without an external SQL database. The only way to interact with the Internal Audit Profile is via the **Status** page of the **Gateway webpage**. There are only two settings for the Internal Audit Profile type: **Name** and **Description** (which are identical to those same properties on the Database type).

Audit Profile Types

There are two different types of audit profiles: Database and Internal. Database type stores audit events in an external database. Internal type stores audit events in a local SQLite database file.

To Create an Audit Profile for a Database Profile Type

1. Go to the **Configure** section of the Gateway.
2. Choose **Security > Auditing** from the menu on the left.
3. The **Audit Profiles** page is displayed, and click **Create** new **Audit Profile** link.
4. Select **Database** or **Internal** audit profile type. This example uses the **Database** type, then click **Next**.

Add Audit Profile Step 1: Choose Type

☒ **Database**

Audit events stored in an external database using a flexible table schema.

☐ **Internal**

Audit events stored in a local SQLite database file.

Next >

5. Enter the **Name** of the audit log and **Description** (optional).
6. Under the **Database Settings**, select the **Database** where the table will be stored, select the **Auto Create** check box, and enter the desired **Table Name**.
7. Click **Create New Audit Profile**.

Main	
Name	Audit
Description	New audit profile for the project

Database Settings	
Database	MySQL The database connection to use to store audit events.
Auto Create	☒ If true, the table schema specified here will be automatically verified and created if necessary. (default: true)
Table Name	AUDIT_EVENTS The name of the table to store audit events. (default: AUDIT_EVENTS)

☐ Show advanced properties

Create New Audit Profile

Once some changes have been made to a Tag or a Database table, Ignition will begin recording.

AUDIT_EVENTS_ID	EVENT_TIMESTAMP	ACTOR	ACTOR_HOST	ACTION	ACTION_TARGET	ACTION_VALUE
1	2016-07-25 17:50:09	admin	IU-WorkStation	tag write	B Tags/B3: 1	1.0
2	2016-07-25 17:50:51	admin	IU-WorkStation	tag write	B Tags/B3: 1	100.0
3	2016-07-25 17:50:53	admin	IU-WorkStation	tag write	B Tags/B3: 1	2.0
4	2016-07-25 17:50:56	admin	IU-WorkStation	tag write	B Tags/B3: 1	8.0
5	2016-07-25 17:51:20	admin	IU-WorkStation	query	update audit_events set acto...	4
6	2016-07-25 17:51:51	admin	IU-WorkStation	query	UPDATE audit_events SET `A...	1

Auditing Project Events



INDUCTIVE
UNIVERSITY

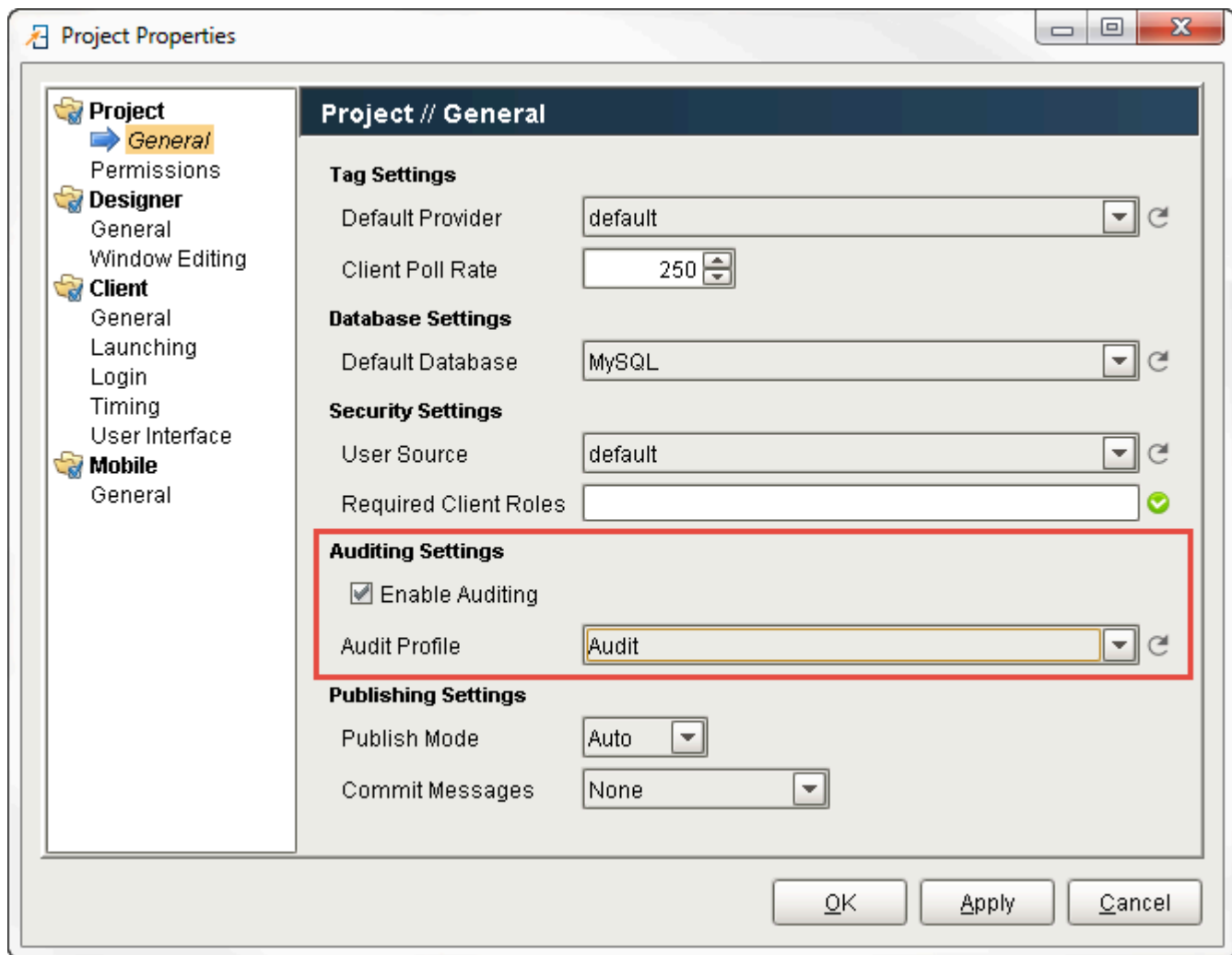
Project Auditing

[Watch the video](#)

A project can be assigned to an Audit Profile. Once configured, Ignition will track changes made to the Designer, as well as keep track of when users logged in or logged out of a client. Additionally, the hostname of the computer used will be recorded.

To Assign an Audit Profile to a Project

1. Go to the **Designer**, open the project that you want to enable auditing on, and go to **Project > Properties**.
2. Go to the **General** section, select the **Enable Auditing** check box, and select your **Audit Profile** from the drop-down menu. The audit profile is used to record audit actions for your project. If the new audit profile does not show up, click **Refresh**.
3. Click **OK**.
4. **Save** your Project.



To View Information in an Audit Log

There are a few ways to [view audit information](#): using a Table component, interface on the Gateway, or the Database Query Browser. Here is one example of viewing an Audit Log using the Database Query Browser.

1. Go to **Tools > Database Query Browser**.
2. Under the **Schema** area, double click on a **table**, and it will expand the query in the Database Query Browser area.
3. Click **Execute**, and all the audit log data will be displayed in the Resultset1 area.

Database Query Browser

```
SELECT * FROM audit_events
```

☒ Limit SELECT to: 1000 rows

Resultset 1

A...	EVENT_TIMESTAMP	ACTOR	ACTOR_HOST	ACTION	ACTION_TARGET
1	2016-07-06 17:46:39	admin	IU-WorkStation	login	
2	2016-07-07 11:22:39	admin	IU-WorkStation	login	
3	2016-07-07 11:23:32	admin	IU-WorkStation	project save	Documentation
4	2016-07-07 11:23:32	admin	IU-WorkStation	project publish	Documentation
5	2016-07-07 11:23:34	admin	IU-WorkStation	project save	Documentation
6	2016-07-07 11:23:34	admin	IU-WorkStation	project publish	Documentation

10 rows fetched in 0.002s

Auto Refresh Edit Apply Discard

Test

Schema

audit_events

- AUDIT_EVENTS_I
- ACTION (VARCHA
- ACTION_TARGET
- ACTION_VALUE (
- ACTOR (VARCHA
- ACTOR_HOST (V

Refer to the [Database Query Browser](#) to learn more about how it works.

Audit Table Definition

The following table describes the audit table as it exist in the database:

Column Name	Description
AUDIT_EVENTS_ID	The id of the row.
ACTION	Brief description of the action.
ACTION_TARGET	The target of the action.
ACTION_VALUE	The value acted upon the action target.
ACTOR	The logged in user when the action occurred or a description of the system that generated the action.
ACTOR_HOST	The host computer where the action occurred.
EVENT_TIMESTAMP	The time when the action occurred.
ORIGINATING_CONTEXT	A numerical description of the origin of the originating system. gateway = 1, designer = 2, client = 4
ORIGINATING_SYSTEM	The name of the project or system where this action occurred.
STATUS_CODE	A 32 bit integer that represents a bitmask of severity (good, bad, uncertain). The bitmask represents the status of the action recorded. For example, a tag write failing would result in a "bad".

ORIGINATING_CONTEXT

Scope	Value
Gateway	1
Designer	2
Client	4

Custom Auditing

The Audit Table is simply a database table, so custom events can be logged to the table. This is commonly done through scripting events. In most cases, users will log certain button presses and event values by adding just several lines of code.

This is documentation for **Ignition 7.9**, which is no longer actively maintained.

For documentation on the latest stable release, see the [latest version](#) (8.3).

Alarm Notification Auditing



INDUCTIVE
UNIVERSITY

Alarm Notification Auditing

[Watch the video](#)

Alarm Notification profiles can be set to store information in an Audit Profile.

How to Store Alarm Notifications in an Audit Profile

Once you have an [audit profile](#) created in Ignition, you can configure your Alarm Notification Profile to start using it.

1. Go to the **Configure** section of the Gateway.
2. Choose **Alarming** > **Notification** from the menu on the left. The Alarm Notification Profiles page is displayed.
3. Edit the appropriate notification profile by clicking the **edit** link.

Alarm Notification Profiles

Name	Description	Enabled	Type	Status	
Email		true	Email Notification	Running	delete edit
Email 1		true	Email Notification	Running	delete edit
SMS		true	SMS Notification	Running	delete edit

4. The Edit Alarm Notification Profile page is displayed. Scroll down to the **Auditing** section, and select an **Audit Profile** from the drop-down menu. Click **Save Changes**, and Ignition will

automatically begin storing information.

Auditing	
Audit Profile	Audit If an audit profile is selected, events such as emails and acknowledgements will be stored to the audit system. Note that alarm acknowledgements are also stored to the alarm journal.
☐ Show advanced properties Save Changes	

Now that the alarm notification profile is storing data into the Audit system, you have a complete log of all alarm emails and acknowledgements that you can review.

See [View Audit Information](#) for more info on how to retrieve information from the Audit Log.

This is documentation for **Ignition 7.9**, which is no longer actively maintained.

For documentation on the latest stable release, see the [latest version](#) (8.3).

View Audit Information



INDUCTIVE
UNIVERSITY

View Audit Information

[Watch the video](#)

Audit profiles store information into a database, you can then display that information in an Audit Log to see what information is stored. Here is a complete list of what information is captured in the Audit Log.

Information Captured in the Audit Log

Ignition Platform

Category	Actions
Projects	Designer saves, project property changes, project setting changes, and deleting a project
Gateway Network	Saving changes, creating/deleting an outgoing connection, and approving an incoming connection
Gateway - Email Settings	Creating/deleting a SMTP Profile, and editing/saving changes to an SMTP Profile
Gateway - Audit Profile	Creating/deleting an Audit Profile, and editing/saving changes to an Audit Profile
Gateway - User Sources	Creating/deleting, and editing/saving changes to a user source
Gateway - Managing Users in User Source (Hybrid Only)	Creating/deleting, and Editing a Role.
Gateway - Security Zones	Adding/deleting, and editing/saving to a Security Zone
Gateway - Database Drivers - JDBC Drivers	Creating/deleting, and editing/saving changes to a JDBC Driver
Gateway - Database Drivers - Translators	Creating/deleting, and editing/saving changes to a Translator.
Gateway - Store and Forward	Ediing/saving changes to a Store and Forward engine
Gateway - Alarming General	Saving changes to Alarming General settings
Gateway - Alarm Journal	Creating/deleting, and editing/saving changes to an Alarm Journal. Create/edit/delete notifications (email, remote Gateway, simple one-way SMS, Voip.
Gateway - Schedules	Creating a new schedule

Category	Actions
Gateway - Realtime Tags	Creating/deleting, and editing/saving a Realtime Tag provider
Gateway - OPC Client Connections	Creating/deleting, and editing/saving an OPC Connection

Enterprise Administration

Category	Actions
Gateway - EAM Setup	Setting the Gateway as either an Agent or Controller
Gateway - EAM Event Thresholds	Editing/saving changes to Event Thresholds
Gateway - EAM Controller Settings	Uninstalling, and editing/saving changes to the Controller Settings
Gateway - EAM Agent Management	Creating/deleting, and editing/saving changes to an Agent Group
Gateway - EAM License Management	Adding/removing a license
Gateway - EAM Agent Tasks	Creating a Gateway task, and when a task runs (automatic, scheduled, or on demand)
Gateway - EAM Agent Settings	Editing/saving the Agent Settings

OPC UA and Devices

Category	Actions
Gateway - Device Connections	Creating/deleting, and editing/saving a device connection. Editing/saving changes to Modbus Address Mapping (Modbus Driver), Aliased Points (DNP3 Driver), and Tag Import (Omron Driver)
Scripting - Device Connections	Creating/deleting a device connection. Disabling a device with <code>system.device.setDeviceEnabled</code>
Gateway - OPC UA Server Settings	Editing/saving OPC UA server settings

Tag History

Category	Actions
Gateway - Historical Tags	Creating/deleting, and editing/saving a Historical Tag Provider (Edge Historian, OPC-HAD Provider, Remote History Provider, Tag History Splitter)

Alarm Notifications

Category	Actions
Gateway - Alarm Notifications	Creating/deleting, and editing/saving changes to an Alarm Notification Profile. Changes made to the Notification Profile Scripts (Voice Notification).
Gateway - Alarming On-Call Rosters	Creating/deleting, and editing/saving changes to an On-Call Roster.

System Functions

Category	Actions
system.db	system.db.addDatasource system.db.removeDatasource system.db.runNamedQuery system.db.runPrepUpdate

Designer

Category	Actions
Login Attempts	Login attempts

Vision

Category	Actions
Managing Users in User Source	Adding/deleting, and editing/saving changes to a User. Creating/deleting, and editing/saving a Role.
On-Call Rosters	Creating/deleting an On-Call Roster.

There are a few ways to view audit log information: using a Table component, Database Query Browser, or the interface on the Gateway.

To Access the Audit Log with Table Functions

Since Ignition makes accessing data from databases seamless, it is possible to bind a data property of a table directly to database table. Alternatively, it is possible to access the contents of the audit log with table functions.

Once you have an **Audit Log setup and attached to a project**, you can go back to that project and see what information is in that audit log. This example uses the Table Functions to extract data from the Audit Log.

1. In **Designer**, drag a **Table** component on to a window.

2. In the **Property Editor**, click on the binding icon from the table's **Data** property.
The Property Binding window is displayed.
3. Select the **Functions** Binding Type.
4. Select **Functions** from the various binding options.
 - i. **Binding Function**, select the **Audit Log** from the drop-down menu.
 - ii. **Audit Profile Name**, select **Audit** or the name of your Audit Profile.
 - iii. **Start Date**, enter the appropriate start date.
 - iv. **End Date**, enter the appropriate end date.
 - v. **Polling Mode**, select **Relative**.
 - vi. Select any other appropriate function options from the menu.
5. Click **OK**.

The screenshot shows the 'Property Binding: Root Container.Table' dialog box. The left sidebar has four sections: 'Binding Types' (with 'Functions' selected), 'Tag' (with 'Tag History', 'Tag', and 'Indirect Tag'), 'Property' (with 'Property' and 'Expression'), and 'Database' (with 'DB Browse' and 'SQL Query'). Below these is an 'Other' section with 'Cell Update' and 'Functions' (which is highlighted with a red box). At the bottom left is a 'No Binding' button with a red X icon. The main area is titled 'Binding Function' and contains a dropdown menu set to 'Audit Log'. Below this is the 'Audit Profile Name' dropdown set to 'Audit'. The 'Start Date' and 'End Date' fields are set to '2017-02-01 00:00:00' and '2017-02-28 00:00:00' respectively. There are six filter fields: 'Actor Filter', 'Action Filter', 'Target Filter', 'Value Filter', 'System Filter', and 'Context Filter'. The 'Context Filter' is set to '0'. At the bottom, the 'Polling Mode' is set to 'Relative' (with 'Off' and 'Absolute' also available), the 'Polling Rate' is '0' seconds, and the 'Retain Rows' checkbox is unchecked. 'OK' and 'Cancel' buttons are at the bottom right.

6. Once you click OK, the table will populate with all the information stored in the audit log based on the Table Functions you selected. You can use the [Table Customizer](#) to configure how you want

the table to look by reorganizing and hiding columns, making columns sortable, assigning meaningful headers, and much more.

Timestamp	Actor	Action	Action Target	Action Value	Result C...	Result	System	Contex...	Context
Feb 13, 201...	Scheduled Report	report executed	Test Report	Failed Action - ...	-2,147,483,...	AuditStatus...	project=Para...		1 Gateway
Feb 14, 201...	Scheduled Report	report executed	Test Report	Failed Action - ...	-2,147,483,...	AuditStatus...	project=Para...		1 Gateway
Feb 14, 201...	admin	login			0	AuditStatus...	project=Para...		2 Designer
Feb 14, 201...	admin	login			0	AuditStatus...	project=Para...		4 Client
Feb 14, 201...	admin	project save	Parameters		0	AuditStatus...	project=Para...		2 Designer
Feb 14, 201...	admin	project publish	Parameters		0	AuditStatus...	project=Para...		2 Designer
Feb 14, 201...	admin	tag edit	[default]Tanks/T...	ComplexTagD...	0	AuditStatus...	project=Para...		2 Designer
Feb 14, 201...	admin	tag edit	[default]Tanks/T...	ComplexTagD...	0	AuditStatus...	project=Para...		2 Designer
Feb 14, 201...	admin	tag edit	[default]Tanks/T...	ComplexTagD...	0	AuditStatus...	project=Para...		2 Designer
Feb 14, 201...	admin	tag edit	[default]Tanks/T...	ComplexTagD...	0	AuditStatus...	project=Para...		2 Designer
Feb 15, 201...	Scheduled Report	report executed	Test Report	Failed Action - ...	-2,147,483,...	AuditStatus...	project=Para...		1 Gateway
Feb 15, 201...	admin	project save	Parameters		0	AuditStatus...	project=Para...		2 Designer
Feb 15, 201...	admin	project publish	Parameters		0	AuditStatus...	project=Para...		2 Designer

To Access the Audit Log Using the Database Query Browser

The Database Query Browser makes it easy to search your database tables to view audit information.

1. In the **Designer** under the **Tools** menubar, select **Database Query Browser**.

The Database Query Browser will open.

2. On the right side of Browser window under **Schema**, will be a list of tables from the currently selected database. Double click on the **audit_events** table, and click **Execute**. The data from the **audit_events** table will appear in the Resultset 1 tab.

The screenshot shows the Database Query Browser window. At the top, the query `SELECT * FROM audit_events` is entered. Below the query, there is a checkbox for "Limit SELECT to:" with a value of "1000" rows. The main area displays "Resultset 1" with a table of audit events. The table has columns: AUDIT_EVENTS..., EVENT_TIMESTAMP, ACTOR, ACTOR_HOST, and ACTION. The data shows various events including Scheduled Reports, logins, and project saves. On the right side, the "Schema" pane shows a list of tables, with "audit_events" selected. At the bottom, there are buttons for "Auto Refresh", "Edit", "Apply", and "Discard".

AUDIT_EVENTS...	EVENT_TIMESTAMP	ACTOR	ACTOR_HOST	ACTION
933	2017-02-13 12:00:11	Scheduled Report	Controller	report executed
934	2017-02-14 00:00:11	Scheduled Report	Controller	report executed
935	2017-02-14 16:58:13	admin	mipsaro-ws2	login
936	2017-02-14 16:59:42	admin	mipsaro-ws2	login
937	2017-02-14 17:01:45	admin	mipsaro-ws2	project save
938	2017-02-14 17:01:45	admin	mipsaro-ws2	project publish
939	2017-02-14 17:19:13	admin	mipsaro-ws2	tag edit
940	2017-02-14 17:20:25	admin	mipsaro-ws2	tag edit
941	2017-02-14 17:21:22	admin	mipsaro-ws2	tag edit
942	2017-02-14 17:23:14	admin	mipsaro-ws2	tag edit
943	2017-02-15 00:00:11	Scheduled Report	Controller	report executed
944	2017-02-15 10:40:29	admin	mipsaro-ws2	project save

Refer to the [Database Query Browser](#) to learn more about how it works.

To Access the Audit Log on the Gateway

Ignition provides a simple interface to view Audit Logs on the Gateway.

1. On the Gateway webpage in the **Configure** section, scroll down to **Security > Auditing**.
2. The Audit Profile page will be displayed. Select the Audit Profile where your information is stored, and click **More > view log**.

Audit Profiles

Name	Type	Description		
Audit	Database		view log	More ▾ edit
Audit1	Database		delete	More ▾ edit

3. Choose the parameter settings if your looking for something specific, otherwise, enter a **Start Date** and **End Date**, and click **Search**.

Audit Log Viewer

Actor

Action

Target

Start Date

2/15/17

17

4

:

12

AM ▾

End Date

2/17/17

17

11

:

59

PM ▾

Search

This is documentation for **Ignition 7.9**, which is no longer actively maintained.

For documentation on the latest stable release, see the [latest version](#) (8.3).

Security Zones



INDUCTIVE
UNIVERSITY

**Security Zones and Service
Security**

[Watch the video](#)

What are Security Zones?

A Security Zone is a list of Gateways, Computers, or IP addresses that are defined and grouped together. This group now becomes a zone on the **Gateway Network**, which can have additional policies and restrictions placed on it. While Users and Roles restrict access to specific functions within the Gateway like making certain controls read-only for certain users and read/write for others, Security Zones provide this functionality to the Gateway Network, limiting locations instead of people to be read-only for specific actions. This allows for greater control over the type of information that is passing over the network, improving security and helping to keep different areas of the business separate, while still allowing them to interconnect.

Using Security Zones

Sometimes, in addition to knowing who the user is, it is important to know where they are sending a command from. An operator may have permissions to turn on a machine from an HMI, but if the operator were to login to a project on a different Gateway in the network that had remote access to those Tags, it might not be a good idea to let the operator write to those Tags. From the remote location, the operator can't see if the physical machine is clear to run.

This is where Security Zones come in. While Security Zones themselves don't define the security, they instead define an area of the Gateway Network, breaking up Gateways and network locations into manageable zones that can then have a security policy set on them. Once there are zones defined, a security policy can be assigned to each zone, and a priority of zones can be set in the event that more than one zone applies in a given situation.

DANGER

When using zone-based security in a project, the project stores the name of the security zone as a string. This means that if you were to modify the name of the zone in the gateway, the zone-based security in your project will not update to reflect the new name, and instead will try searching for a zone with the original name. Be very careful when modifying the names of security zones.

Defining a Security Zone

When setting up a new Security Zone, it might be a good idea to setup a **Gateway Network** first if you haven't already. While Security Zones can be defined and used without a connected Gateway, they work best when used in conjunction with other Gateways on a Gateway Network, so it is a good idea to setup a Gateway Network first.

Security Zones are defined in the **Configure** section of the Gateway webpage by going to **Security > Security Zones**.

NOTE

There is a special zone called Default. It is always present and can't be modified, and will be used if an incoming connection does not match any of the other defined zones.

Selecting the **Create new Security Zone** link brings up a new page where the Security Zone can be defined.

Security Zones

Name	Description
Default	This zone cannot be edited, and will be used for zone-based settings when no other zone is matched.

[→ Create new Security Zone...](#)

Besides the name and description, there are two major sections here: Identifiers and Qualifiers. These are two forms of checks that need to happen before an incoming connection gets placed in a Security Zone.

General	
Name	New Zone
Description	(default:)

Identifiers

The identifiers are how incoming connections are distinguished between different zones. While there are a few different ways to define the incoming connection, it only needs to match one of them to match this zone.

- **IP Addresses** - This defines an IP address that the connection is coming from. This can be a list of IP addresses by using commas to separate them. It can also make use of the *() wildcard like '192.168.100.'*, or use a range such as '100.100.1-100.0-255'. With IP addresses, virtually all connections can be listed. Use 127.0.0.1 for the local connection.
- **Host Names** - The host name refers to the system name of the machine generating the request such as Joe_Workstation. This can be a list of names separated by commas, and it can also use the *() wildcard like '_Workstation'*.
- **Gateway Names** - The Gateway name is the name of the Ignition instance. This is set in the **Configure** section by going to **System > Gateway Settings**, and changing the System Name. This can be a comma separated list and can use the wildcard such as '* Ignition Gateway'.

Many incoming connections can be defined using any of the three identifiers, or even multiple at once. As mentioned before, an incoming connection only needs to match one of the identifiers for it to be accepted.



CAUTION

When identifying a Gateway through a proxy Gateway, the IP Address should be using the ip of the proxy, but the Gateway Name should use the name of the Gateway we are trying to identify.

Identifiers	
IP Addresses	May be a comma separated list of addresses, and the addresses may use wildcards or ranges. For example, '192.168.*.*' or '192.168.1-5.0-255'.
Host Names	A comma separated list of allowed host names. May use the wildcard '*', such as 'Manufacturing_*'. Host names are the system names of the machines generating the requests. For example, the computer name of the machine running a client.
Gateway Names	A comma separated list of gateway names. May use the wildcard '*'. Gateway names are the names of the Ignition instance.

Qualifiers

After first being identified as part of a particular Security Zone, the connection then must check the Qualifiers. With the Qualifiers, the incoming connection needs to fit in with all of the properties before it is fully placed into the Security Zone.

- **Require Secure Connection** - If this is true, only connections that are made over a secure channel will be accepted.
-  **DANGER**
A Security Zone is only able to check connections made to the gateway the zone is defined on. This means that connections through a proxy Gateway may not be secure.
- **Direct Connection Required** - If this is true, only connections that come from a direct connection will be accepted. The Gateway Network allows you to connect three Gateways in a 1-2-3 configuration, where Gateway 1 can see Gateway 3 through the proxy Gateway 2.
 - **Allow Client Scope** - If this is false, Clients will not be placed in the zone.
 - **Allow Designer Scope** - If this is false, Designers will not be placed in the zone.
 - **Allow Gateway Scope** - If this is false, any Gateway scoped requests will not be placed in the zone.

As mentioned above, a connection must pass all of the qualifier checks before being accepted into a Security Zone. So if Require Secure Connection was checked, and Allow Client Scope was not, any requests coming from Clients would be rejected even if they are secure, and the same goes for any non-secure connections coming from sources other than a Client.

Requests can be a part of more than one zone, depending on how the zones are setup. This can be useful for making a whole section of IP addresses read only, but a specific Gateway in that IP address range may be listed specifically in another zone, which can be given read/write access. Any connection which does not fall into one of the zones will be placed in the Default zone.

Qualifiers	
Require Secure Connection	☐ If true, only connections made over a secure channel will be accepted into the zone. (default: false)
Direct Connection Required	☐ If true, only requests that come from a direct connection will be accepted. This is used in the context of the gateway network, where request may be routed through an intermediate proxy gateway. (default: false)
Allow Client Scope	☒ If false, requests from clients will not be accepted in this zone. (default: true)
Allow Designer Scope	☒ If false, requests from designers will not be accepted in this zone. (default: true)
Allow Gateway Scope	☒ If false, requests from the gateway scope will not be accepted in this zone. (default: true)

Service Security

After creating some Security Zones, a Security Policy can then be defined for each zone. This can be found by going to the **Configure** section and navigating to **Security > Service Security**. At first, none of the zones will have a policy defined, and the Default zone will be at the top. Editing any of them will bring up the Security Policy definition page for that zone. The Security Policy has four sections: Alarm Notification, Alarm Status, History Provider Access, and Tag Access. They work together to define how the local Gateway gives access to incoming Gateway connections. All four sections also have the ability to completely block access to specific services with the Service Access setting in each section. Setting that to deny will deny the zone access to that particular information, regardless of what the rest of the options are set to.

CAUTION

It is important to realize that if you have a single Gateway, limiting access of certain clients to certain Tags is still done in the [individual Tags](#).

- **Alarm Notification** - The Accessible Pipeline Filter setting is a list of Pipelines in the current Gateway that other connections can use for alarm notification. Note that this setting is an inclusionary list not an exclusionary list, meaning that if there are no pipelines listed there, then all of them will be available. The list is a comma separated list, and it can make use of the (*) wildcard.
- **Alarm Status** - The Allow Acknowledge setting will allow the Gateways that fall within the zone to acknowledge alarms on the local Gateway.

New in 7.9.7 The Allow Shelving setting will allow the Gateways that fall within the zone to Shelf alarms on the local Gateway. IE: Other Gateways can shelve alarms on this Gateway. For this Gateway to shelve alarms on others, this must be set on the remote Gateway.

- **History Provider Access** - The History Provider Access has two different settings. First, it has a Default Access Profile. This is the default access rights for Tag History. Second, there will be a setting for each History Provider setup on the local Gateway. In the picture below, there is an "Access Level: 'New Connection'" that can be set that corresponds to the History Provider that was created when a database was connected. It can be set to Query and Storage, which will allow connections in the current zone to both run queries and store Tag History against the Tag History provider, Query Only, which will only allow the zone to query out history data, but not store it, and No Access, which will completely block access to that History Provider. The final setting is Inherited, which will inherit the Default Profile Access rights. Any new history providers will automatically get added to the security policy set at inherited so it may be beneficial to set the Default Profile Access to be either Read Only or No Access so that a recently added history provider does not accidentally get storage rights when it should not.

CAUTION

The Default Access Profile should not be set to Inherited. This also goes for the Default Provider Access Level in the Tag Access section.

- **Tag Access** - The Tag Access also has a few different settings. The Default Provider Access Level, which works the same as the History Provider Default Access Profile. It sets the default access rights for realtime providers. It will then have a setting for each provider configured in the local Gateway, as well as an additional one for system Tags. These can be set to **ReadWriteEdit**, which will allow connections in the current zone to read, write to, and edit the Tags in that provider, **ReadWrite**, which allows the zone to read and write to Tags, and **ReadOnly**, which only allows the zone to read the Tags. It also can be set to None, which will prevent the zone from interacting with the Tag Provider altogether, and Inherited, which will again inherit the access rights set in the Default Provider Access Level. Any new Tag Providers will automatically get added to the security policy with Inherited access rights.

New in 7.9.1 The Trust Remote Roles setting will allow similarly named roles on other Gateways to access Tags with role specific security on them.

Alarm Notification	
Service Access	Allow
Accessible Pipeline Filter	 A comma separated list of alarm pipeline names on this gateway (which can include the wildcard '*') that will be made available for use in the alarm notifications of other gateways in this security zone.
Alarm Status	
Service Access	Allow
Allow Acknowledge	☒
Allow Shelving	☐
History Provider Access	
Service Access	Allow
Default Profile Access	Query Only
Access Level: 'DB'	Inherited

Tag Access	
Service Access	Allow
Trust Remote Roles	☐
Default Provider Access Level	ReadOnly
Access Level: 'default'	Inherited
Access Level: 'System'	Inherited

Default Security Zone

While the Default zone may not have a custom security policy defined, it does default to not include any notification pipelines, allow alarm acknowledgment, query only history access, and read only Tag access. This means that if a remote Tag Provider is setup on a remote Gateway, and the local Gateway has not changed the default security settings, the remote Gateway will have read only access to the Tag History Provider. This can be changed by editing the Default zone's security policy to fit a different preference, or creating new Security Zones with custom security policies. Once a security policy has been defined on a zone, it will automatically jump to the top of the list. A new option will also become available that will clear the policy from the zone.

Setting Zone Priority

Once a security policy has been defined for two or more zones, a new option appears on the Service Security page to move the zones up and down the list. This allows a priority to be set on the Security Zones, since a connection can apply to multiple zones. For example, say Zone 2 dictates that all requests coming from a range of IP addresses have query only history access, and read write access to Tags. Zone 1 includes specific Gateways, one of which is also contained in Zone 2, that will have query and storage history access and read write edit access to Tags. When a request comes in from a connection, it first determines which Security Zones it belongs to. The request then starts at the top of the Service Security list and goes down until it finds the first zone that it is in, and uses the access rights of that zone. In our example, we want to make sure Zone 1 is above Zone 2, so that the Gateway that is in both Zone 1 and Zone 2 gets the full access rights afforded to it by the security policy of Zone 1 instead of getting the limited access rights from Zone 2.

Service Security



Security policies are defined based on Security Zones. The highest ranking policy (from the top down) for a connection's zones will be used. If no other policies match, the "Default" policy will be used.

Security Zone	Policy Defined?			
Zone 1	true	Edit	Clear Policy	Move Down
Zone 2	true	Edit	Clear Policy	Move Up
Default	false	Edit		

This is documentation for **Ignition 7.9**, which is no longer actively maintained.

For documentation on the latest stable release, see the [latest version](#) (8.3).

Tag Security



INDUCTIVE
UNIVERSITY

Tag Security

[Watch the video](#)

Tag Access Rights

Tag security is often the best way to configure security for data access. By defining security on a Tag, you affect the Tag across all windows in all projects, as opposed to configuring component security on each component that displays or controls that Tag.

If a user opens a window in the Client that has components that are bound to a Tag that the user doesn't have clearance to read or write to, the component will get a forbidden overlay.

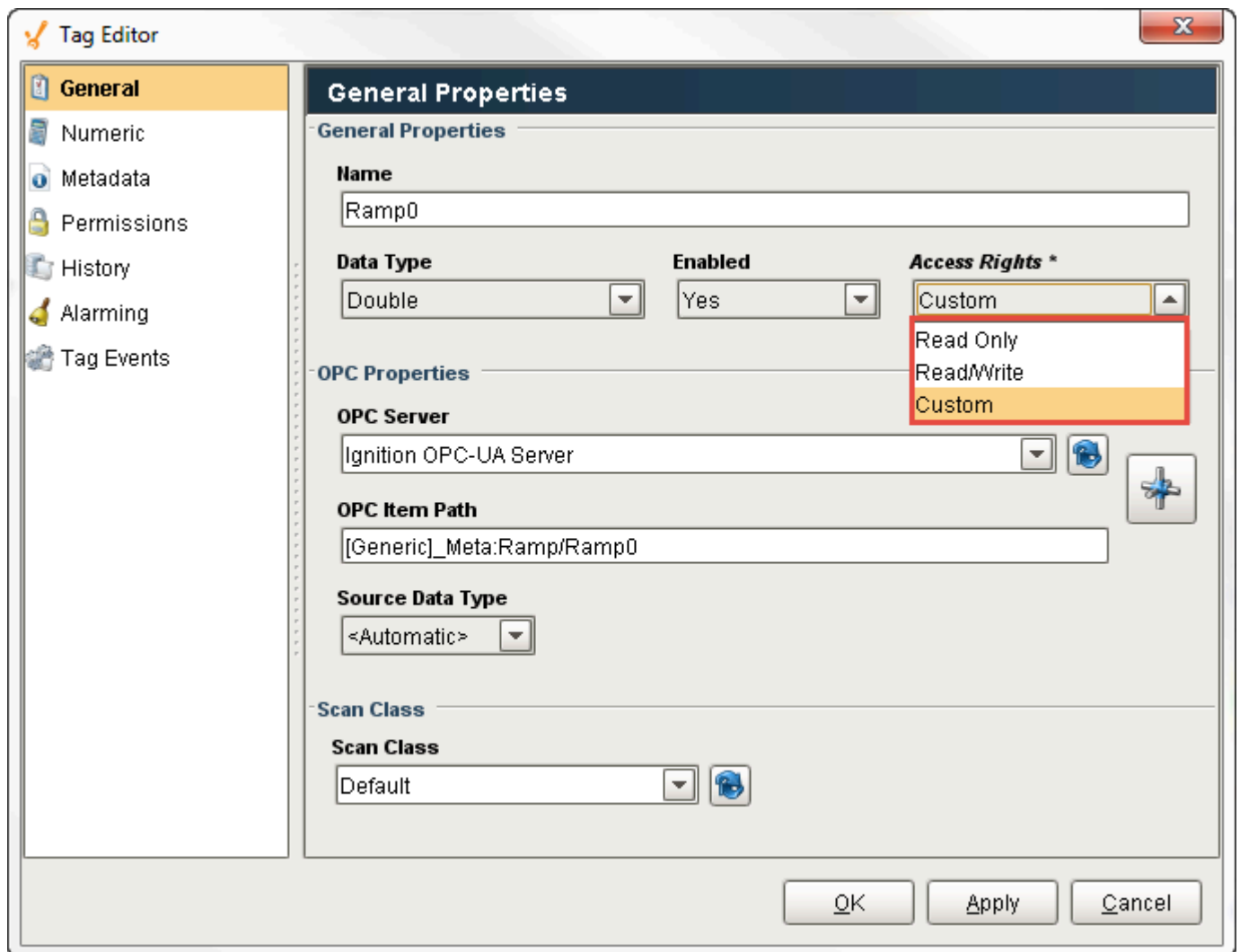


See also: [Quality Overlays](#), [Permission Properties](#).

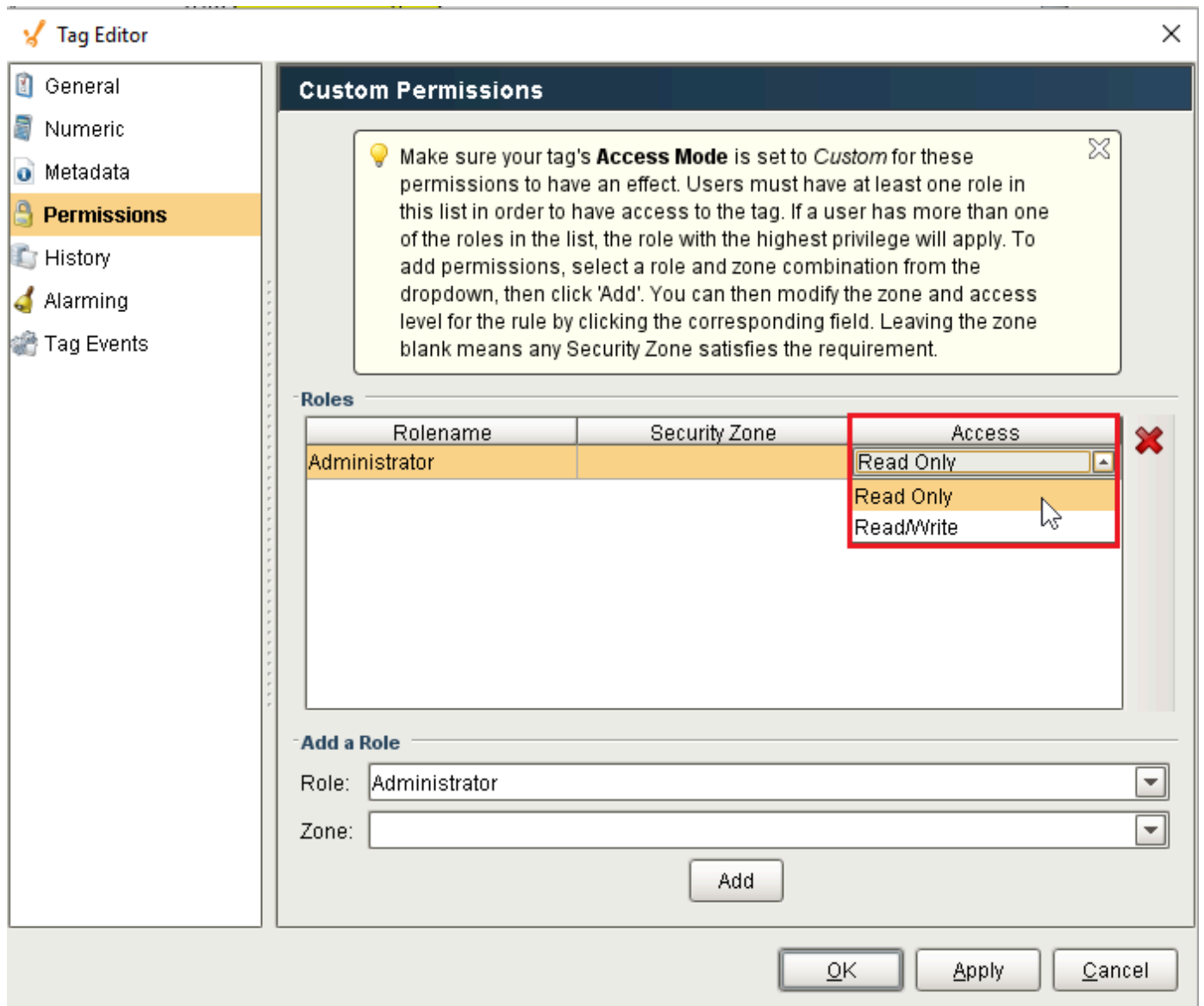
To Set the Access Rights to a Tag

You can add read/write security to individual Tags or multiple Tags in the Designer. In order to change permissions on a Tag, you have to make changes in two places. 1) Set the **Access Rights** property to Custom. 2) Add Role(s) to the **Permissions** page.

1. In the **Tag Browser**, edit a Tag by double-clicking on the Tag.
2. In the **General** tab, from the **Access Rights** drop-down, select **Custom**.



3. Select the **Permissions** tab on the left side, and from the **Add a Role** drop-down select a role. Click the **Add** button.
4. Change each role's **Access** rights by selecting the **Read Only** or **Read/Write** option. If a user does not have any of the listed roles, they will be denied both read and write permissions.



5. Click **OK**. Now the user has the Read/Write permission to interact with the Tag.

Tag Access Rights with Security Zones

Tag permissions can also include **Security Zones**. Security Zones allow you to not only limit Tags by a user's role, but also by area. They are setup in the same way as setting the Access Rights just for a user, except a zone must also be specified. It does require that Security Zones be configured, and a few Gateways connected in a Gateway Network. Leaving the Security Zone empty will assume the access permission is for all zones.

- General
- Numeric
- Metadata
- Permissions**
- History
- Alarming
- Tag Events

Custom Permissions

💡 Make sure your tag's **Access Mode** is set to *Custom* for these permissions to have an effect. Users must have at least one role in this list in order to have access to the tag. If a user has more than one of the roles in the list, the role with the highest privilege will apply. To add permissions, select a role and zone combination from the dropdown, then click 'Add'. You can then modify the zone and access level for the rule by clicking the corresponding field. Leaving the zone blank means any Security Zone satisfies the requirement.

Roles

Rolename	Security Zone	Access
Administrator		Read Only
Operator	Zone 1	Read Only
Operator	Zone 2	Read/Write
Supervisor		Read/Write

Add a Role

Role:

Zone:

This is documentation for **Ignition 7.9**, which is no longer actively maintained.

For documentation on the latest stable release, see the [latest version](#) (8.3).

Tag Provider Security



INDUCTIVE
UNIVERSITY

Tag Provider Security

[Watch the video](#)

In addition to setting up security on [individual Tags](#), **Tag Provider Security** allows you to limit the ability to modify Tags to only those users with specified roles. This can be extremely useful if you want to let many people use Tags in their projects, but not allow them to edit your Tag structure or Delete Tags. Tag Provider security is Role-based, and each Tag Provider has it's own role requirements. When using this security, we recommend you create a role specifically for Tag edits (ie: TagEditor or defaultTagEditor).

To Configure Tag Provider Security

Typically, the Administrator will identify what role(s) are required to modify Tags in Designer.

1. Go to the **Configure** section of the Gateway webpage.
2. Choose **Tags > Realtime** from the menu on the left. The **Realtime Tag Providers** page is displayed.
3. Click **edit** to modify the realtime Tag Provider that you want to apply the roles to.

Realtime Tag Providers

Name	Type	Description	Enabled	
default	Standard Tag Provider	Default tag provider	true	delete edit

4. In the **Tag Editing Roles** property, enter the roles that you want to grant permission to edit Tags. By entering roles, you block users without one of these roles from editing Tags in the Designer.

Edit Realtime Tag Provider

Main	
Name	default
Description	Default tag provider
Tag Editing Role(s)	Administrator,super_admin Users must belong to one of these roles in order to edit this provider's tags in the Designer. Multiple roles can be specified by separating them with commas. If blank, tag editing for this provider will not be restricted in the Designer. (default:)
Enabled	☒ (default: true)

5. Click on **Save Changes**.

This is documentation for **Ignition 7.9**, which is no longer actively maintained.

For documentation on the latest stable release, see the [latest version](#) (8.3).

Client Security

Client Permissions

New in 7.9.4

Every project's clients are governed by a set of permissions to control what is allowed to originate from the client. For example: access to construct queries against the database, or the ability to edit Users and Roles in your authentication profile. To maintain a secure system, these are all set to OFF by default but you can enable them for everyone, for specific users, or even for specific users that are logged into certain zones. See descriptions of these categories and how to change them on the [Project Permissions](#) page.

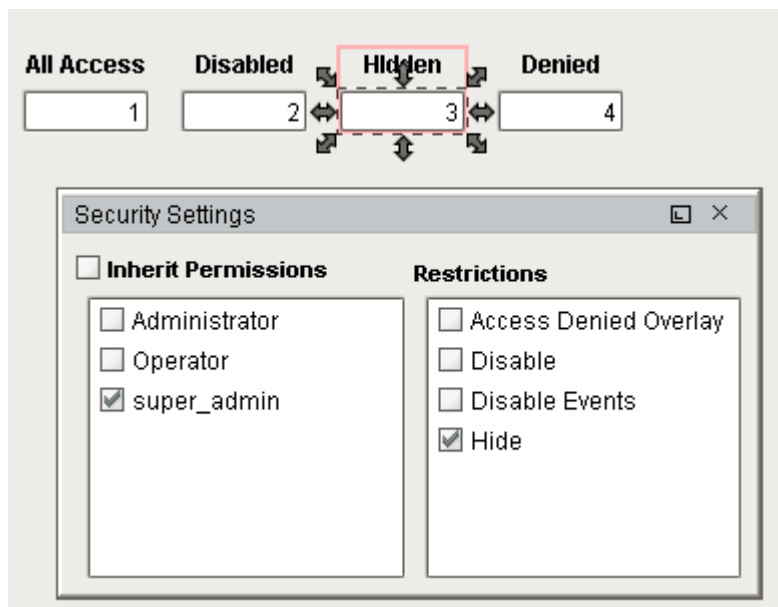
CAUTION

Unlike new Ignition projects, any projects that were created before 7.9.4 and then updated beyond 7.9.4 will have these permissions set to true.

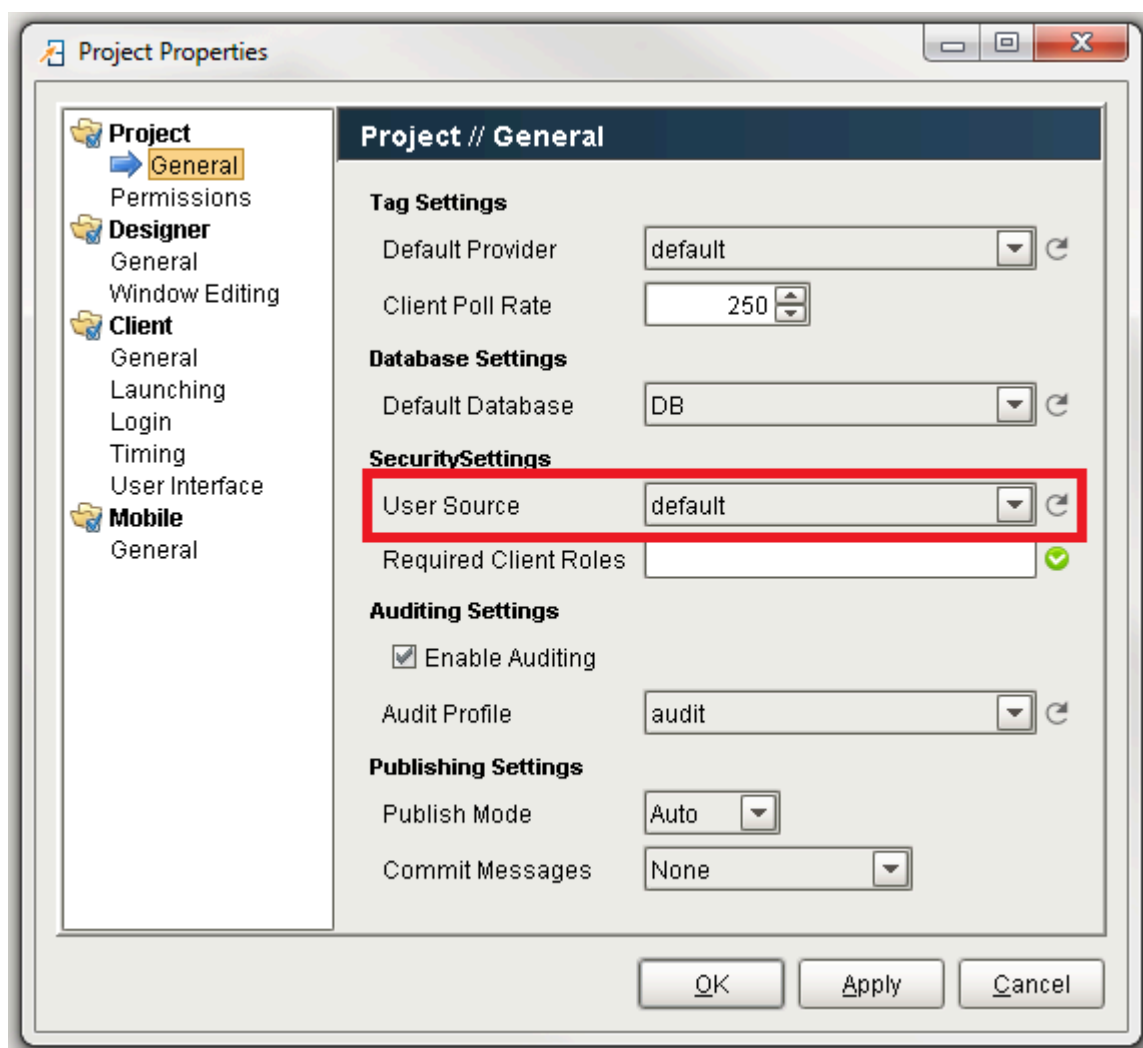
Role-Driven Client Security

On the simplest level, security settings can be applied to individual windows or components. Users with different roles can all view the same project from the client, but the functionality and readability can change based on the roles assigned to each user. Generally, higher level access provides full functionality to all contents of a project, and lower level access is restricted to generalized read-only privileges. However, client security settings are flexible enough to accommodate any security requirements.

Below we see the Security Settings panel in action. This panel is the interface that applies Ignition's built-in security settings. Security settings can be applied to a single component, multiple components simultaneously, or even a whole window. Users who should be allowed full access can be selected, and restrictions can be applied for users that should not have full access.



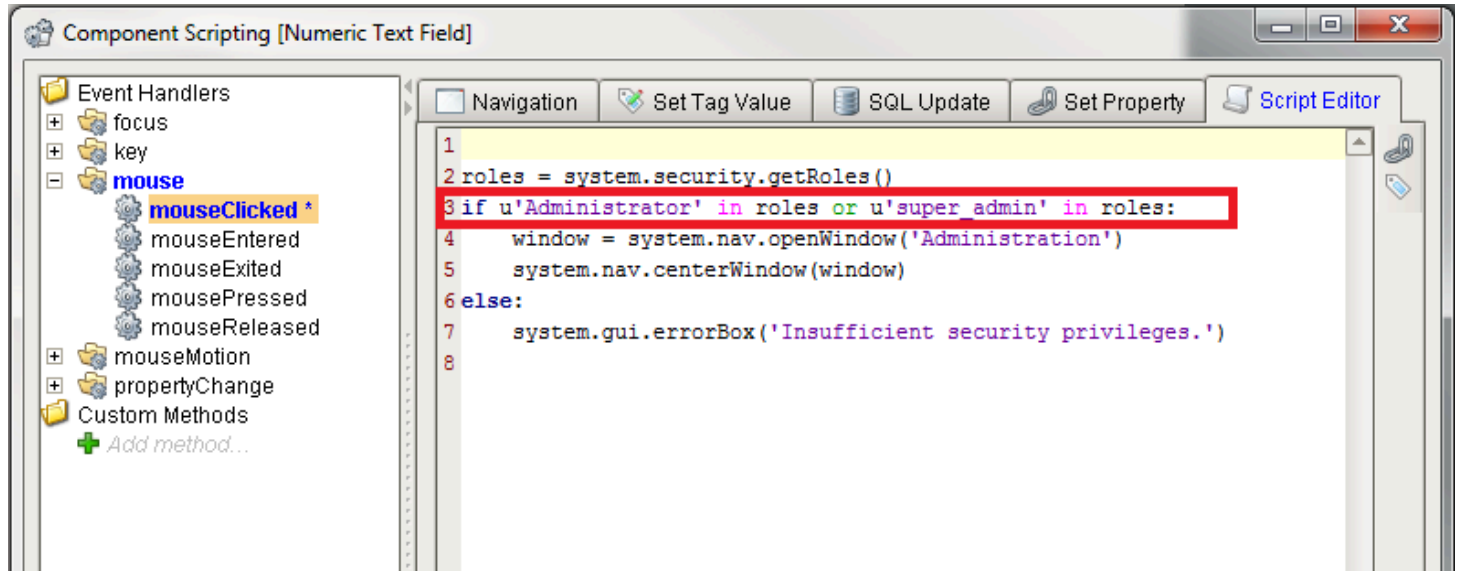
Projects are assigned a User Source to authenticate against. All roles that have been defined in the User Source can be referenced in the client to block or allow access. Once roles have been created, you can easily start assigning component-specific security settings in the Designer.



More information can be found on the [Component and Window Security](#) page.

Incorporating Scripting into Security

The component-based security settings are fairly simplistic: the user either has the required roles, or a restriction applied. In situations where consideration for access should go beyond a simple role check, security-based scripting can provide a larger degree of granularity. Information about the logged-in user, such as user-name or roles, can be detected by scripting, allowing for the creation of a robust security system.



More information can be found on the [Security in Scripting](#) page.

This is documentation for **Ignition 7.9**, which is no longer actively maintained.

For documentation on the latest stable release, see the [latest version](#) (8.3).

Login Security



INDUCTIVE
UNIVERSITY

Project Security

[Watch the video](#)

In Gateways with multiple projects, sometimes client access should be limited on a per-user-basis. The most common use-case is when users from one area of a facility should be able to launch clients that are specific to their area, but should not be able to launch clients from other areas. While there are several different ways to approach this, the easiest is to require different roles to log into each project.

Every project in Ignition is going to have authentication associated with it. You can change the **User Source** (Authentication profile) for a project as well as assign **Required Client Roles**. A user must provide a username and password from this User Source, and that username must have at least one of the Required Client Roles to log in.

To Add a Required Role to a Client

1. From the Designer, go to **Project > Properties** and go to the **General** section.
2. In the **Project Properties** window, under **Security Settings**, select the **User Source** from the drop-down menu.
3. Enter the **Required Client Roles** that the Client needs in order to access the Client. This field will show all matching roles as you start typing. Multiple roles may be specified by separating them with a comma.
4. Click **OK** to commit the settings.
5. **Save** your project.

CAUTION

Changing your security settings will not log users out of an open client, but it will stop them from logging in again.

Project Properties

Project
General
Permissions

Designer
General
Window Editing

Client
General
Launching
Login
Timing
User Interface

Mobile
General

Project // General

Tag Settings

Default Provider: default

Client Poll Rate: 250

Database Settings

Default Database: MySQL

Security Settings

User Source: default

Required Client Roles: Administrator, Operators

Auditing Settings

☒ Enable Auditing

Audit Profile: Audit

Publishing Settings

Publish Mode: Auto

Commit Messages: None

OK Apply Cancel

This is documentation for **Ignition 7.9**, which is no longer actively maintained.

For documentation on the latest stable release, see the [latest version](#) (8.3).

Component and Window Security



INDUCTIVE
UNIVERSITY

**Component and Window
Security**

[Watch the video](#)

Role-based security inside of Ignition works on multiple levels: component, group, container, and window levels. Each of these levels also have special categories of security that help with tuning security to various design considerations.

Each window and component can define its own security settings. These settings determine who can see and/or use the component. It's good business practice to have a well thought out security policy for your project.

Changing Security Settings on a Component

To define a security for a component that is different from that of the parent, use the following steps.

1. Right-click on a component and select **Security**. The Security Settings panel is displayed in the bottom section of the Property Editor.
2. Deselect the **Inherit Permissions** check box to override the permission settings so no permissions are inherited from a group, container, or window. (By default, Inherit Permissions uses permissions from whatever container a component is in).
3. Select the role that the user must have from the list of roles displayed under the **Inherit Permissions** section. If the roles you created do not appear, it's probably because the Designer was open before those roles were created, so right-click in the Inherit Permissions section and select **Refresh**.
4. In the **Restrictions** section, choose the option that will enact if the user does not have the selected role.

i. Disable - sets the Enabled property to false when the window opens up.

CAUTION

If you choose to disable the security on a component, make sure that it is a component that actually does something different when it is disabled. For example, buttons and input boxes can't be used when they are disabled, but disabling a Label component has no effect.

i. Disable Events - prevents event scripts from running when the user doesn't have security clearance.

ii. Hide - acts the same way the Disable restriction does, but it sets the Visible property to false on the component.

iii. Access Denied Overlay - shows an opaque overlay on top of the component when the user doesn't have security clearance.

5. You can keep the panel open or close it. The security settings take effect immediately.

Here are several examples of what different security permissions and restrictions would look like on a Multi-State Button component in a Client.

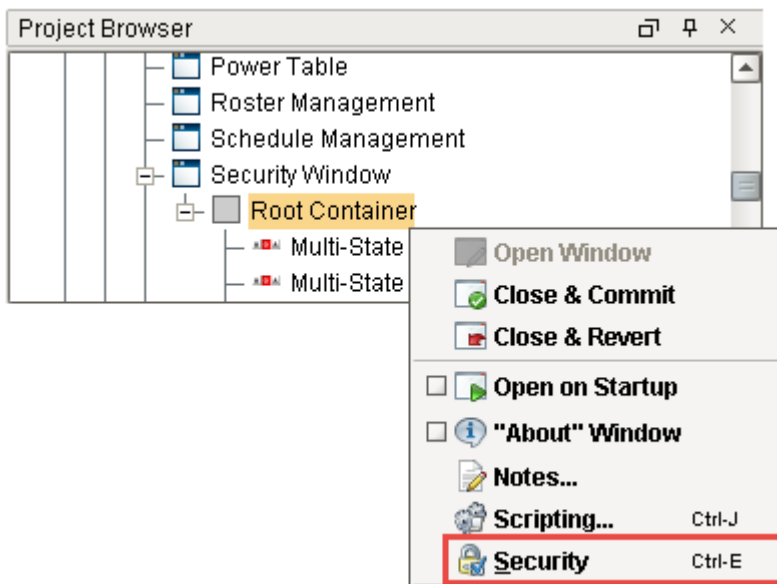


IN THE CLIENT

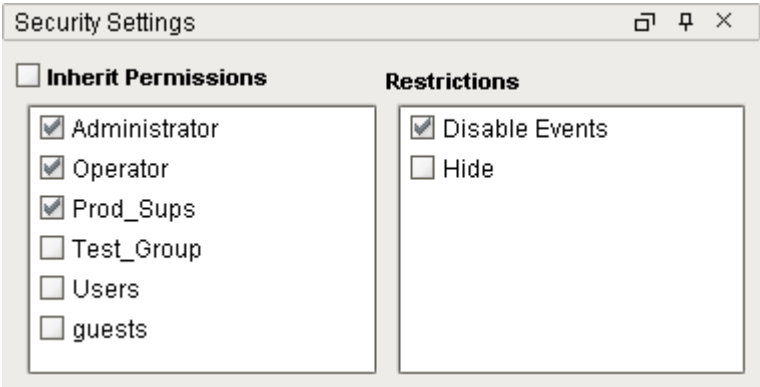
In the Client, if the user does not match the role filter that you define, the component will be disabled or hidden and disabled. When a user with higher permission logs in, the component will be usable again.

Setting Security on a Window

You can configure security settings that control who can and who can't open a window. While in the Designer, right-click on a window in the **Project Browser** and select **Security**. Window Security is configured the same way that Component Security is configured.



Select the permissions based on your business requirements. Windows only have one Restriction option: **Do Not Open**. This means unless the user has one of the selected roles, they cannot open the window. They will see a warning message instead.



This is documentation for **Ignition 7.9**, which is no longer actively maintained.

For documentation on the latest stable release, see the [latest version](#) (8.3).

Security in Scripting

Securing Event Handlers



INDUCTIVE
UNIVERSITY

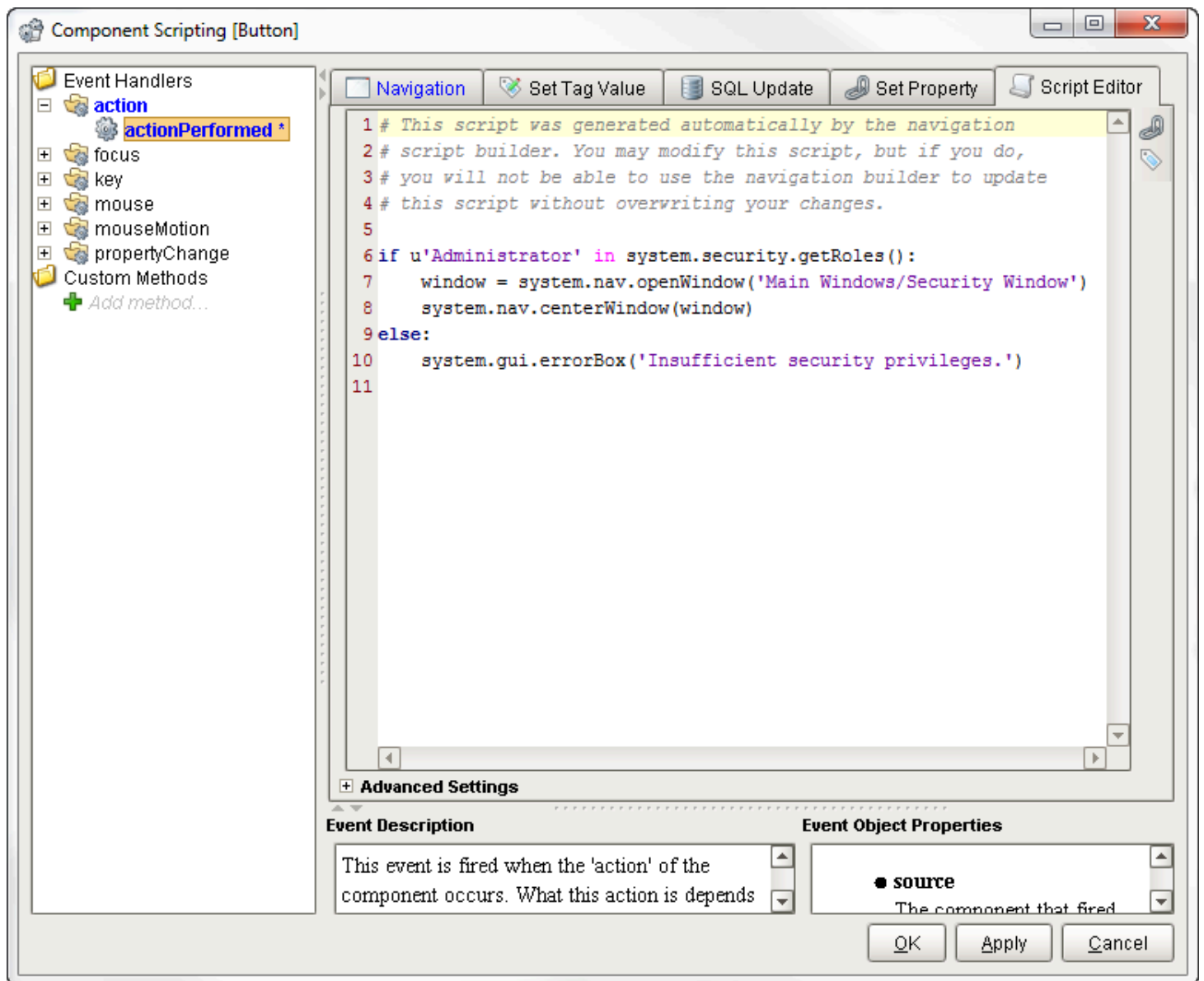
Securing Event Handlers

[Watch the video](#)

Security can be added to any of the event handlers in Ignition. You can set up security in an event script for a component using the `system.security.getRoles()` function, and use this function in any script in Ignition that runs in a Client. This example uses an event handler to build a navigation and security script.

1. In **Designer**, right click on your component and select **Scripting**. The Component Scripting window will open.
2. Select the **action** > **actionPerformed** Event Handler. Under the **Navigation** tab, select **Open** and **Center** to set the location and position of the component on the Client window.
3. Under **Action Qualifiers**, click on the **Security** button, and start to build your security script.
4. Check the **Required Roles** checkbox, and select from the list of role(s) that you want to have access to your button. When you close the list of Required Roles, Ignition will build the script for you based on the role(s) you selected.
5. Click on the **Script Editor** tab, and you'll notice that the code is well documented, it contains the roles you specified, and includes an error message. The error message will popup when a user in a role, other than the role(s) specified, accesses the button.

Here is what the script looks like in Ignition.



Here is the code you can copy to ensure the user invoking the script has sufficient privileges. This script identifies the "Administrator" role.

```
if u'Administrator' in system.security.getRoles():
    #This part of the script will run if the user has the correct privileges. For
    example:"
    print "this script will run if the user has a the administrator role."
else:
    system.gui.errorBox('Insufficient security privileges.')
```

Special Security Qualifiers

Event handlers often execute logic that must be secured. The various script builders all have special security qualifiers that can be enabled. These qualifiers get translated into the generated script by accessing the user's current roles via scripting.

Example

```
if 'Administrator' in system.security.getRoles():
    productCode = event.source.productCode
    qty = event.source.parent.getComponent("QuantityBox").intValue
    query = "UPDATE my_secure_table SET quantity=? WHERE product=?"
    system.db.runPrepUpdate(query, [qty, productCode])
else:
    system.gui.errorBox('Insufficient security privileges.')
```

See also: [Script Builders](#), `system.security.getRoles`

Setting the Client to Read-Only



INDUCTIVE
UNIVERSITY

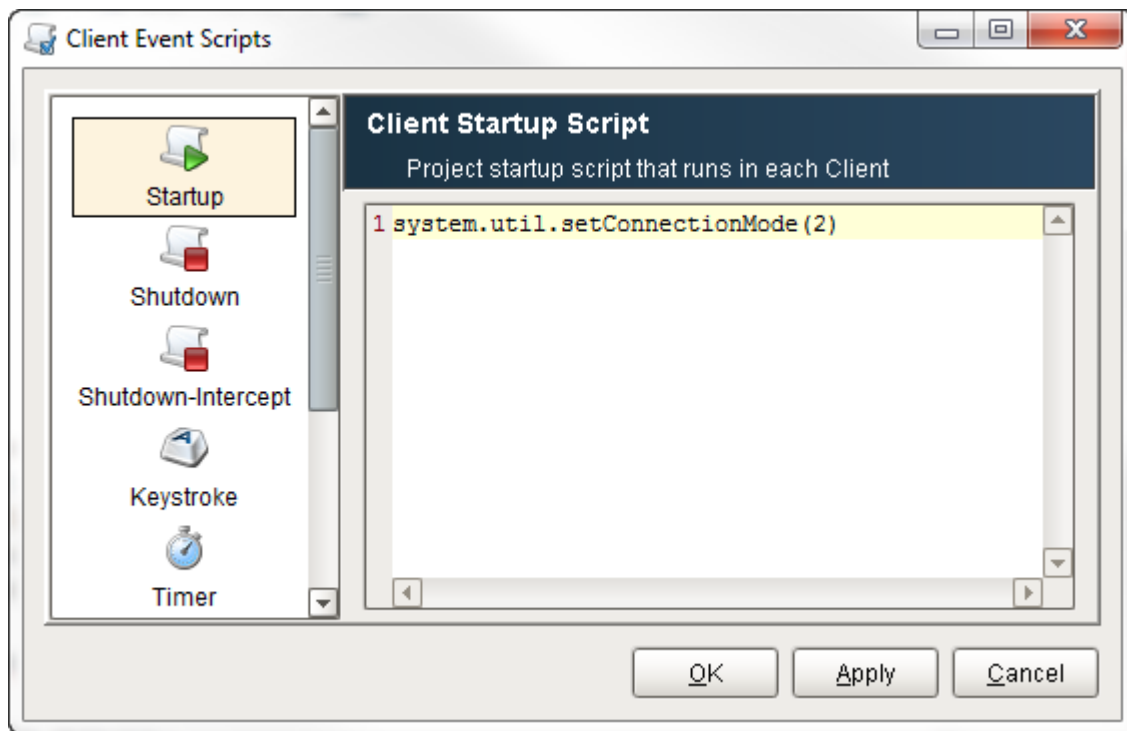
Setting Client Read Only

[Watch the video](#)

There are times when it is best to open a Client in a Read-Only mode to eliminate the possibility that a Client will affect a device or database. The Client event startup script that sets the Client mode to Read-Only is an easy way to accomplish this. Similar to the buttons in the Designer, this function can be used to set Disconnected, Read-Only, and Read/Write modes in any script in Ignition that runs in a Client. This function can be called in any Client scoped script, but is most commonly used in the Startup script.

Setting up the Client Event Startup Script

1. From the Designer, go to **Project Browser > Client Event Scripts**. The Client Event Scripts window is displayed.
2. In the **Startup** script, enter this code: `system.util.setConnectionMode(2)` where 2 means Read-Only.
3. Click **OK**. The startup script will run the next time a user logs into the Client, resulting in the Client being Read-Only.



You can prevent a Client from logging in with the following script:

```
system.security.logout()
```

This is documentation for **Ignition 7.9**, which is no longer actively maintained.

For documentation on the latest stable release, see the [latest version](#) (8.3).

Project Security in Designer and Gateway

When several users are all working on the same project, managing changes to the project can become cumbersome. By default, all users with Designer access can modify, delete, save, and publish all resources available in the Designer. In some situations, it is desirable to limit what each user can do in the Designer. Ignition has several built-in Designer restriction methods to help in these scenarios.

Designer Project Permissions



INDUCTIVE
UNIVERSITY

Project Permissions

[Watch the video](#)

Actions such as publishing, viewing, saving, deleting, and editing of project resources are restricted to users who have sufficient roles to do so. Editing of these required roles is done in the permissions section of the Project Properties dialog in the Designer. If required roles are not set for an action, then all users with Designer access can perform the action.

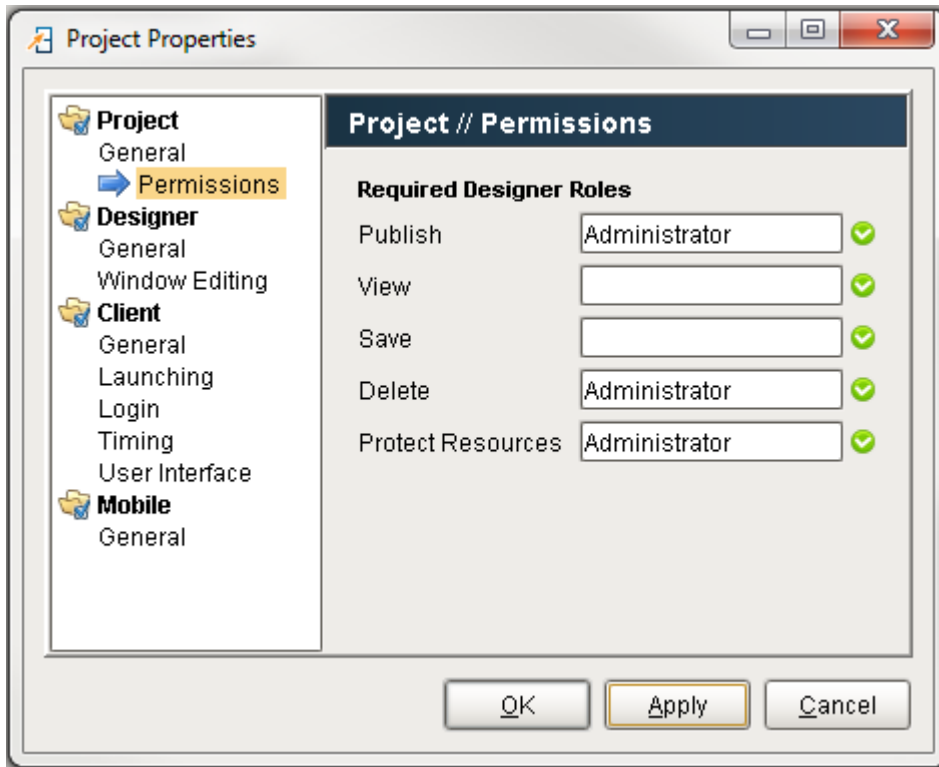
ROLE CHANGES

The Designer does not poll for role changes, so if a user who is currently logged into the Designer has their roles changed, they will need to re-launch the Designer for the new role(s) to take effect.

Controlling Project Edits by Role

You can control who gets to login to a project by assigning roles and giving permissions to those roles in the Required Designer Roles property which you set up in the Designer.

1. In the Designer, from the menubar, choose **Project > Properties**.
2. Go to the **Project > Permissions** area, and under the Required Designer Roles, enter the appropriate roles next to each project level restriction, as required. In the text boxes on this page, enter a comma-separated list of role names that are required to access the project. As you start typing, matching role names will pop up.



The following table describes each of these five options

Option	Result
Publish	User must have at least one of these roles to publish the project.
View	User must have at least one of these roles to view the project in the Designer.
Save	User must have at least one of these roles to save the project.
Delete	User must have at least one of these roles to delete the project.
Protect Resources	User must have at least one of these roles to access protected resources.

To Lock Global Resources on the Gateway

Before assigning any roles in the Global Resource Protection property, you need to keep in mind all the different roles in your project, what level of access they need in each area of the project, and that it agrees with your security policy. Typically, the Administrator, identifies what role is required, and the user(s) who have that role so the proper protection is placed on global resource objects.

1. To block certain users, a role requirement must be added on the Gateway Webpage under the **Configure** section **Configuration > Gateway Settings**, otherwise, other users who have Designer access, can edit a protected resource. Scroll down to the **Global Resource Protection** option.

Add or modify the roles in the Global Resource Protection field to protect the global resources. In this example, you can enter multiple role names separated by commas.

Once you enter the required roles, anyone without one of these roles will not be able to modify protected objects. Click **Save Changes**.

Global Resource Protection	Administrator,super_admin The roles required to protect or modify a protected global resource such as an alarm pipeline. If blank, anyone that can log into the Designer can protect global resources. (default:)
-----------------------------------	---

! GLOBAL RESOURCE PROTECTION SUPERSEDES THE INDIVIDUAL LOCKS APPLIED IN THE DESIGNER

The roles you identify in the Global Resource Protection property to protect or modify any of the protected global resources (i.e., alarm pipeline, scripts, etc.), will supersede all of the individual locks that were applied in the Designer.

Restrict Project Creation

The ability to create new projects can also be restricted by role. In cases where multiple users have Designer access, this property can prevent each user from creating a large amount of 'test' or 'sandbox' projects. This is ideal for production systems where you don't want other users creating new projects.

Granting Permission for Project Creation

The **Create Project Role(s)** property can allow users with one of the specified roles to create new projects on the Gateway. To grant permission to create new projects in Designer, you must assign a role in the Create Project Roles(s) property of Gateway Settings. On the **Configure** section of the

Gateway, go to **Configure > Gateway Settings**, and scroll down to Create Project Role(s) property. Enter a role that users should have to create a new project, and click **Save Changes**.

Create Project Role(s)	Administrator Users must belong to one of these roles in order to create a new Designer project. Multiple roles can be specified by separating them with commas. (default:)
------------------------	--

Protecting Project Resources

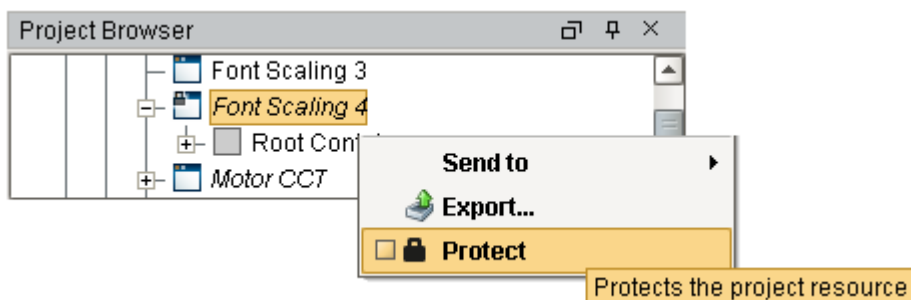


INDUCTIVE
UNIVERSITY

Locking Project Resources

[Watch the video](#)

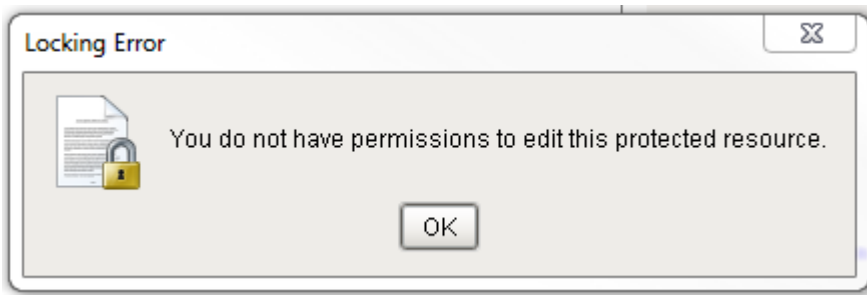
You can lock individual project resources from inside Designer by opening the Project Browser, and right clicking on any of the objects that you want to lock in. Select the **Protect** option to protect it. Once it's protected, it cannot be changed except by someone that has the permission to unprotect it, and modify it.



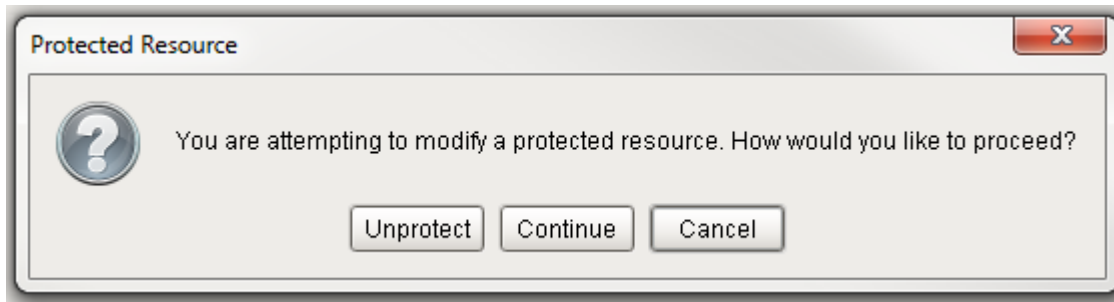
Protected Resources

Protected resources are global or project resources that can only be edited by select users with the required roles. These roles are required to protect resources from being edited in the Designer, and do not apply to the clients. This means you can prevent a resource from being edited by other users who have Designer access. It is often used in scenarios where development work is finished on a window or object, and no further changes should be made to it. Other objects like **Templates** or **Alarm Pipelines** are often protected so they may be used, but not modified.

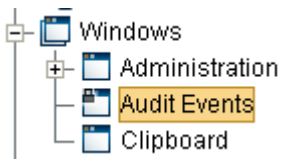
Users without a required role will see the following message in the Designer when attempting to open a protected resource:



Users with a required role are allowed to modify the resource, but a message will appear informing them that the resource is protected, and will be asked how to proceed:



Additionally, a lock  icon will appear on the resource informing users that it is protected. An example can be seen on the 'Audit Events' window below:



To remove the protection, simply right click the object and select the **Protect** option to unprotect it.

Protecting Global Resources



INDUCTIVE
UNIVERSITY

Locking Global Resources

[Watch the video](#)

Just like protecting project resources, you can protect individual global resources using the Protect option. Global Resources can be locked in two different locations: in the Designer and on the Gateway webpage using the Global Resource Protection property as described earlier on this page.

To Lock Global Resources in Designer

1. Go to the Global section of your Project Browser.

2. Right click on one of your Alarm Notification Pipelines, and select **Protect**. This example uses the Basic Email pipeline object, but any object can be protected. To remove the protection, simply right click the object and select the **Protect** option again to unprotect it. Once an object is protected, you will see that you can still modify it.

