

Cascading Authentication

What is Cascading Authentication?

Cascading Authentication is the method ProQuest uses to determine that a user is authorized to access a ProQuest link.

How Does It Work?

When a user clicks on a ProQuest link, the server attempts to validate the user and connect them to the ProQuest article they want to view.

First, ProQuest checks to see if the user has a currently active ProQuest session running. If the user is currently logged in to ProQuest, they are taken immediately to the page.

If they are not, ProQuest then checks for a cookie—a piece of information stored on the user's computer by ProQuest—to see how to proceed next.

If the cookie indicates that the link is from an Athens account, the user is redirected to the Athens Login page.

ProQuest checks to see how the user last connected to ProQuest.

- If the connection was via a referring URL, an IP, or Client ID:

It checks for the following connection types in the following order:

1 **IP** If the current IP address matches the last used IP, the user is redirected to the ProQuest login page.

2 **Referring URL** If the current URL matches the last used URL, the user is redirected to the ProQuest login page.

3 **Client ID** If the current Client ID matches the last used ID, the user is redirected to the client login page.

If the current connection uses one of these methods, but the current information doesn't match the information used last time, the authorization fails and the user sees an error message.

- If the connection was via Local Authorization:

The user is redirected to the local authorization login page.

- If the connection was via User ID and password:

The user is redirected to the User login page.

If all of these methods fail, the authorization fails and the user sees an error message.

Troubleshooting

If you cannot access a link, and should be able to, log in to your ProQuest account and try to connect to the link again.

Flowchart

Here is a flowchart to demonstrate the order and process of the cascading authentication process:

