

Central Authentication Service (CAS)

What is CAS

The central authentication system provides a means for authenticating users against a central repository. Instead of asking a user for their username (netId) and password at every application, the CAS server provides a mechanism for users to login once and not have to login to every application every time they are used. The CAS server stores a cookie in the users browser when they successfully authenticate and looks for the cookie before requesting a user to present their credentials.

Integrating your application with CAS will vary slightly based on your application environment.

For more information please visit the links at the right. They contain the full documentation that should help you with any type of CAS integration that you are planning to do.

The web endpoints that you will need to configure into your application are:

- <https://idp.rice.edu/idp/profile/cas/login>
- <https://idp.rice.edu/idp/profile/cas/serviceValidate>
- <https://idp.rice.edu/idp/profile/cas/logout>



Other Resources

- [JA-SIG CAS Home](#)
- [Client Integration](#)
 - [Java](#)
 - [Spring](#)
 - [PHP](#)
 - [Perl](#)
 - [.NET](#)
 - [All Others](#)