Central Authentication Service (CAS)


Configuration

To enable Central Authentication Service (CAS), edit user.txt and add lines similar to:

```
::CAS
LoginURL http://www.yourlib.org/cas/login
ServiceValidateURL http://www.yourlib.org/cas/serviceValidate
/CAS
```

By default, the use of CAS disables EZproxy's normal login methods, including the presentation of the login menu.

This form also supports the general directives Admin, Allow, Authenticated, Banner, Debug, Deny, Group, Invalid, NoGroups, Refused, Stop, Unknown, User, and UsrVar, plus a specialized version of Test to check tag values using an XPath to specify the tag to check. For example:

```
::CAS
Debug
LoginURL http://www.yourlib.org/cas/login
ServiceValidateURL http://www.yourlib.org/cas/serviceValidate
Group NULL
Test -RE cas:group (Undergrad|Grad); Group +Student
Test //*/cas:group Employees; Group +Employee
Test /cas:authenticationSuccess/cas:groups/cas:group Staff; Group +Staff
NoGroups; Deny unaffiliated.html
/CAS
```

For this example to work, config.txt would need to default the Student, Employee, and Staff groups as well.

The Debug directive tells EZproxy to record additional diagnostic messages to messages.txt. This includes recording the entire XML response from the Service Validation URL, which can help in sorting out which attributes are available to use for making authentication decisions.

In all three tests, the tag cas:group is being tested. The first and second tests use an identical search to locate tags, as EZproxy assumes a search from the root across all nodes if no path information is included. The third test uses an absolute path to the tag.

Support additional attribute release by EZproxy CAS server

EZproxy has the ability to act as a CAS Identity Provider to a CAS Service Provider (CAS SP). This functionality has been greatly enhanced. It is enabled in config.txt by adding an entry such as:

```
CASServiceURL [-anonymous] [-Scope=scope] WildURL
```
where *WildURL* is a case-insensitive simple wildcard match (supports * and ?) for a CAS SP to authorize. Although not recommended, the value * can be used to allow any CAS Service Provider to gain access.

**Original CAS syntax**

The original CAS syntax can still be used and is entered in user.txt similar to this:

```
::CASLogin=http://www.yourlib.org/cas/login,CASServiceValidate=http://www.yourlib.org/cas/serviceValidate
```

changing the URLs to point to your institution's CAS login and service validate URLs.