CAS + Duo Security

SSO Upgrades

CAS 3.5.6 -> 4.2.6

- Hazelcast Ticket Registry replaced EhCache
- CAS Servers in both data centers
- Duo Security MFA
- New Impersonation feature
- Improved SLO support

Shibboleth 2.x -> 3.2.1

- New ShibCas Plugin for External AuthN
- Duo Security MFA through CAS
- IdP Servers in both data centers
- Improved SLO support

Duo Limitations

Needs to be linked to a Service in order to require use

Duo authentication result not stored in session

- Requires Duo MFA to be repeated for multiple services
- Improperly configured service will prompt for Duo on each request

Shibboleth SPs are all or nothing for using Duo

- Shibboleth does not currently allow mfa and non-mfa access

Service Registry

Will be required for all services that use CAS

Required now for any service wanting to use Duo

Service Now form to register service

- Link on CAS page in Service Catalog
- http://itcatalog.ucdavis.edu/service/central-authentication-service-cas

Renewed annually to keep registry up to date

Add Duo to CAS Service

Fill out Service Registry form in Service Now

Duo required for all logins to service

- Fill out Service Now form once with application URL
- Select Requires Duo in the form

Duo required only for certain paths

- Fill out Service Now form for paths that require Duo
- Fill out Service Now form for paths that do not require Duo
- Need to ensure you are using a CAS Client that can handle multiple paths

Inform users about registering for Duo and device options

- https://ucdavisit.service-now.com/ess/knowledge_detail.do?sysparm_article=KB0001225

Add Duo to SAML Client

Fill out the Service Registry form in Service Now

- Enter the EntityID of the SP in the URL
- Enter SAML Client in the CAS Clients box

Future Releases

CAS 5.0 and Shibboleth 3.3 will have full MFA support

- MFA AuthN valid for entire session
- New ways to require MFA
  - Global Principal Attribute
  - Principal Attribute by Service
  - Adaptive
    - IP Access rules
    - Geo Location
  - Opt-in Parameter
- Other MFA Providers
  - Yubikey
  - Google Authenticator
  - Radius

OAuth 2.0/OIDC

Available with the CAS 5 deployment

- Will enable CAS to be an OAuth/OIDC server
- Services will need to be registered in CAS
- Still deciding on which end points will be enabled
- Will have development server up soon for testing

Impersonation

Available only on ssodev.ucdavis.edu

Need to register user and service url

- Send E-mail to IET-Authentication or tsschmidt@ucdavis.edu
- Need username and exact URL to impersonate

Using the feature

- Type impersonate directly into address bar
  - https://ssodev.ucdavis.edu/cas/impersonate?service=https://my-server/myapp/index.html&renew=true
- Enter username to impersonate
- Enter login credentials