

# NEW SSO FEATURES IN CYPRESS



OpenCraft -



**HOW IT WORKS**

# SAML 2.0 AND SHIBBOLETH



# STUDENT REGISTRATION FLOW



Caprica University

## CU Student Login

Login Name

Password

Continue

[Reset your password](#)

### Protect Your CU account!

- ✓ Watch out for sites or emails that [pretend to be legitimate](#) and ask for your CU login name and password.
- ✓ Please [report any suspicious requests](#) for your CU login name and password.
- ✓ [Learn more](#) about how to protect your computer.

[Learn about the CU Terms of Use »](#)

[Terms of Use](#) | [Copyright](#) | [Accessibility](#) | [Create CU Account](#) | [Need Help?](#)

The name that will identify you in your courses - **(cannot be changed later)**

Password \*

Country \*

# STUDENT REGISTRATION FLOW

**RelayState=testshib&SAMLResponse=PD94bWwgdm**  
Vyc2lrbj0iMS4wliBlbmNvZGluZz0iVVRGLTgiPz48c2FtbDjwO  
lJlc3BvbmlHhtbG5zOnNhbwycD0idXJuOm9hc2lzOm5hb  
WVzOnRjOINBTUw6Mi4wOnByb3RvY29sliBEZXN0aW5hdGl  
vbj0iaHR0cDovL2V4YW1wbGUubm9uZS9hdXRoL2NvbXBs  
ZXRIL3RwYS1zYW1sLylgSUQ9Il9hMDdmZDIhMDg0ODM3M  
2U1NTMyMGRjMzQyNDk0ZWY1ZCIgSW5SZXNwb25zZVRvP  
SJURVNUSUQiElzc3VISW5zdGFudD0iMjAxNS0wNi0xNVQw  
MDowNzoxNS4xODhaliBWZXJzaW9uPSlyLjAiPjxzYW1sMjpjC  
3N1ZXIgeG1sbnM6c2FtbDI9InVybJpvYXNpczpuYW1lczp0Yz  
pTQU1MOjluMDphc3NlcnRpb24iIEZvcmlhdD0idXJuOm9hc  
2lzOm5hbWVzOnRjOINBTUw6Mi4wOm5hbWVpZC1mb3JtY  
XQ6ZW50aXR5Ij5odHRwczovL2lkC50ZXN0c2hpYi5vcmcv  
aWRwL3NoaWJib2xldGg8L3NhbwycOkIzc3Vlcj48c2FtbDjw  
OIN0YXR1cz48c2FtbDjwOIN0YXR1c0NvZGUgVmFsdWU9In  
VybJpvYXNpczpuYW1lczp0YzpzTQU1MOjluMDpzdGF0dXM6U  
3VjY2VzcyIvPjwvc2FtbDJBkMk9RdTIRdmpnNlIPdFIQNIBOM2  
o3ZUs3CnBVY3hRldVdF...

# STUDENT REGISTRATION FLOW

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" Destination="http://example.none/auth/complete/tpa-saml/" ID="_a07fd9a0848373e55320dc342494ef5d" InResponseTo="TESTID" IssueInstant="2015-06-15T00:07:15.188Z" Version="2.0">
  <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://idp.testshib.org/idp/shibboleth</saml2:Issuer>
  <saml2p:Status>
    <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
  </saml2p:Status>
  <saml2:EncryptedAssertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="_dc77827bf5dc3b6f4d3693ee3156ba52" Type="http://www.w3.org/2001/04/xmlenc#Element">
      <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" />
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <xenc:EncryptedKey Id="_978a7b6419a318d86e3314cf9b1c913f" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
          <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
          </xenc:EncryptionMethod>
        </ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>MIIcsDCCAhmgAwIBAg....</ds:X509Certificate>
          <ds:X509Data></ds:X509Data>
        </ds:KeyInfo>
        <xenc:CipherData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
          <xenc:CipherValue>IXA/Hb6JR1imT3c5r+kA0mhubyV/9JjMCsvDIbPDrLUGX4iaU...</xenc:CipherValue>
        </xenc:CipherData>
      </xenc:EncryptedKey>
    </ds:KeyInfo>
    <xenc:CipherData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
      <xenc:CipherValue>
        TAGjvoJitsaPOHvaRPswXNhhxD2lvCKz1rsBkXnbayXe6bnpMB0x9ijE1Wj8UxbkIBhA110DxaN6ZnHQyK8jb7SoUSOc...
      </xenc:CipherValue>
    </xenc:CipherData>
  </xenc:EncryptedData>
</saml2:EncryptedAssertion>
</saml2p:Response>
```

# <SAML2:ATTRIBUTESTATEMENT T>

urn:oid:2.5.4.42:

**William**

urn:oid:2.5.4.4:

**Adama**

urn:oid:2.5.4.3:

**William Adama**

urn:oid:0.9.2342.19200300.100.1.3:

**adama@galactica.fleet.colonies.gov**

urn:oid:0.9.2342.19200300.100.1.1:

**Husker**



# <SAML2:ATTRIBUTESTATEMEN T>



urn:mace:dir:attribute-def:ubcMooEdX:  
**16874621837462**

urn:oid:1.3.6.1.4.1.5923.1.1.1.7:  
**urn:mace:ubc.ca:entl:mooc:edx:student**




# STUDENT REGISTRATION FLOW

The screenshot displays the edX edge user interface. At the top left is the edX edge logo, and at the top right is a user profile dropdown labeled "Husker". Below this is a section titled "CURRENT COURSES". The first course listed is "History of the Twelve Colonies", represented by a golden cornucopia icon. The course details include "CU - HIS101" and "Started - Aug 23, 2015". A gear icon for settings and a "View Course" button are also present. At the bottom, there is a navigation menu with links for "About", "Blog", "FAQs", "Contact", and "Donate". On the right side of the bottom section, it says "POWERED BY OPEN edX". The registration form includes three dropdown menus: "Country \*" (with "--" selected), "Gender" (with "--" selected), and "Year of birth" (with "--" selected). A fourth dropdown menu for "Highest level of education completed" is also present, with "--" selected.

edX edge Husker ▾

CURRENT COURSES

 History of the Twelve Colonies

CU - HIS101  
Started - Aug 23, 2015

⚙️ [View Course](#)

About Blog FAQs Contact Donate

POWERED BY OPEN edX

Country \*  
--

Gender -- Year of birth --


Highest level of education completed  
--

# STUDENT LOGIN FLOW

The screenshot displays the edX edge student login flow. At the top left is the edX edge logo, and at the top right is the user name 'Husker' with a dropdown arrow. Below the header is a section titled 'CURRENT COURSES'. The first course listed is 'History of the Twelve Colonies', represented by a golden cornucopia icon. The course details include 'CU - HIS101' and 'Started - Aug 23, 2015'. A gear icon for settings and a 'View Course' button are also present. At the bottom of the page, there is a navigation menu with links for 'About', 'Blog', 'FAQs', 'Contact', and 'Donate'. The footer contains links for 'Terms of Use', 'Copyright', 'Accessibility', 'Create CU Account', and 'Need Help?'. The login flow itself consists of two main options: 'Use my institution/campus credentials' (highlighted with a red bar and an orange arrow) and 'New to edX?' with a 'Create an account' button.

edX edge Husker ▾

CURRENT COURSES

 History of the Twelve Colonies

CU - HIS101  
Started - Aug 23, 2015

 [View Course](#)

About Blog FAQs Contact Donate

POWERED BY OPEN edX

Terms of Use | Copyright | Accessibility | [Create CU Account](#) | [Need Help?](#)

New to edX?

Part

2

**HOW WE IMPLEMENTED  
IT**

# TECHNICAL GOALS

1. Add Shibboleth Provider support to `third_party_auth`.
2. Support many Shibboleth institutional login options
3. Allow deep links to edX Edge that indicate a preferred institutional login
4. Be able to remove the legacy Shibboleth implementation

# FORMING A PLAN

Discovery

Technical Spec

Discussion

Revisions

```
class SAMLAuthBackend(SAMLAuth): # pylint: disable=abstract-method
    """
    Customized version of SAMLAuth that gets the list of IdPs from third_party_auth's list of
    enabled providers.
    """
    name = "tpa-saml"

    def get_idp(self, idp_name):
        """ Given the name of an IdP, get a SAMLIdentityProvider instance """
        from .models import SAMLProviderConfig
        return SAMLProviderConfig.current(idp_name).get_config()

    def setting(self, name, default=None):
        """ Get a setting, from SAMLConfiguration """
        if not hasattr(self, '_config'):
            from .models import SAMLConfiguration
            self._config = SAMLConfiguration.current() # pylint: disable=attribute-defined-outside-init
        if not self._config.enabled:
            from django.core.exceptions import ImproperlyConfigured
            raise ImproperlyConfigured("SAML Authentication is not enabled.")
        try:
            return self._config.get_setting(name)
        except KeyError:
            return self.strategy.setting(name, default)

    def _check_entitlements(self, idp, attributes):
        """
        Check if we require the presence of any specific eduPersonEntitlement.

        raise AuthForbidden if the user should not be authenticated, or do nothing
        to allow the login pipeline to continue.
        """
        if "requiredEntitlements" in idp.conf:
            entitlements = attributes.get(OID_EDU_PERSON_ENTITLEMENT, [])
            for expected in idp.conf['requiredEntitlements']:
                if expected not in entitlements:
                    log.warning(
                        "SAML user from IdP %s rejected due to missing eduPersonEntitlement %s", idp.name, expected)
                    raise AuthForbidden(self)
```

Fork me on GitHub

# COURSE 1: OPEN SOURCE COLLABORATION

**python-auth** Google / John Cox

**python-social-auth** Matías Aguirre

**python-social-auth**  
"Social auth made simple"

**python-saml** OneLogin / Sixto Martin  
"Forget those complicated libraries and use the open source library provided and supported by OneLogin Inc."

**TestShib** Internet2  
"All SAML 2.0 implementations are welcome and may be tested against Shibboleth here."

# STORY 2: CRI-9 - BUG OR FEATURE?

“There has been a lot of student confusion and frustration over the social auth sign in and the new sign in page. Over the last 48 hours we have received over 70 questions from student asking what the dashboard is and how to link it to Google/Facebook.”



# STORY 3: TESTING WITH UNIVERSITY PARTNERS

- University of British Columbia
- UC Berkeley
- Georgetown University



# STORY 4: MISTAKES I MADE

- Scheduling reviews
- Celery Beat
- Storing secrets in the DB
- Twitter backend
- CRI-9 email validation



# HOW TO SET IT UP

**[bit.ly/cypress-sso-setup](https://bit.ly/cypress-sso-setup)**

(+ edx-code)

# PART 3: QUESTIONS

*Consider asking...*

- How did these changes affect the existing third\_party\_auth providers (Google/Facebook/LinkedIn)?
- How can my school be added to edge.edx.org / edx.org ?
- Can I put my school's login button where the Google/Facebook buttons are, instead of the "institution" list?
- What is the "Dummy Provider" ?
- What sort of community contributions could improve this feature?
- Have any more features been added recently?
- Are there any advanced features not mentioned in the docs?