Lost in Authentication

CAS Clients and Best Practices

Parker Neff
Software Architect
Unicon, Inc.

Bill Thompson
Software Architect
Unicon, Inc.

Jasig 2011 – Spotlight on Open Source
Westin Westminster
Denver, Colorado, USA
May 23-25, 2011

UNICON

Introduction

- 6 days - Software Architect, Unicon, Inc.
  - CasOwa, CasAngelClient, Liferay 5.x/CAS Client & Proxy Ticket Support
- 2.5 years - Senior Associate Director, Information Technology, Development Office, Princeton University
  - .NET CAS Client
- 6 years - Associate Director for Architecture & Engineering – Enterprise Systems & Services – Rutgers University – The State University of New Jersey
  - myRutgers (uPortal), Jasig CAS 3.x
- Jasig – Board of Directors, uPortal Project Liaison (uP2/3), CAS Steering Committee

http://www.linkedin.com/in/wgthom

Introduction

Parker Neff

- 1 ½ Years - Software Architect, Unicon, Inc.
  - uPortal, Shibboleth, CAS, Liferay
- 9 years – Technical Director, Enterprise Architecture, Total Systems.
- 9 years – Senior Developer, Nintendo of America

Agenda

1. CAS Deployment Considerations
2. CAS Clients Survey
3. CAS Integration Stories

CAS Deployment Considerations

SSO Session vs Application Session

- CAS SSO - TGT is bound to browser session scoped cookie
- Default TGT policy is a 3-hour idle time-out, also have hard timeout, throttle-use,...
- Applications are responsible for session management once the user is authenticated
- CAS is not an application session manager

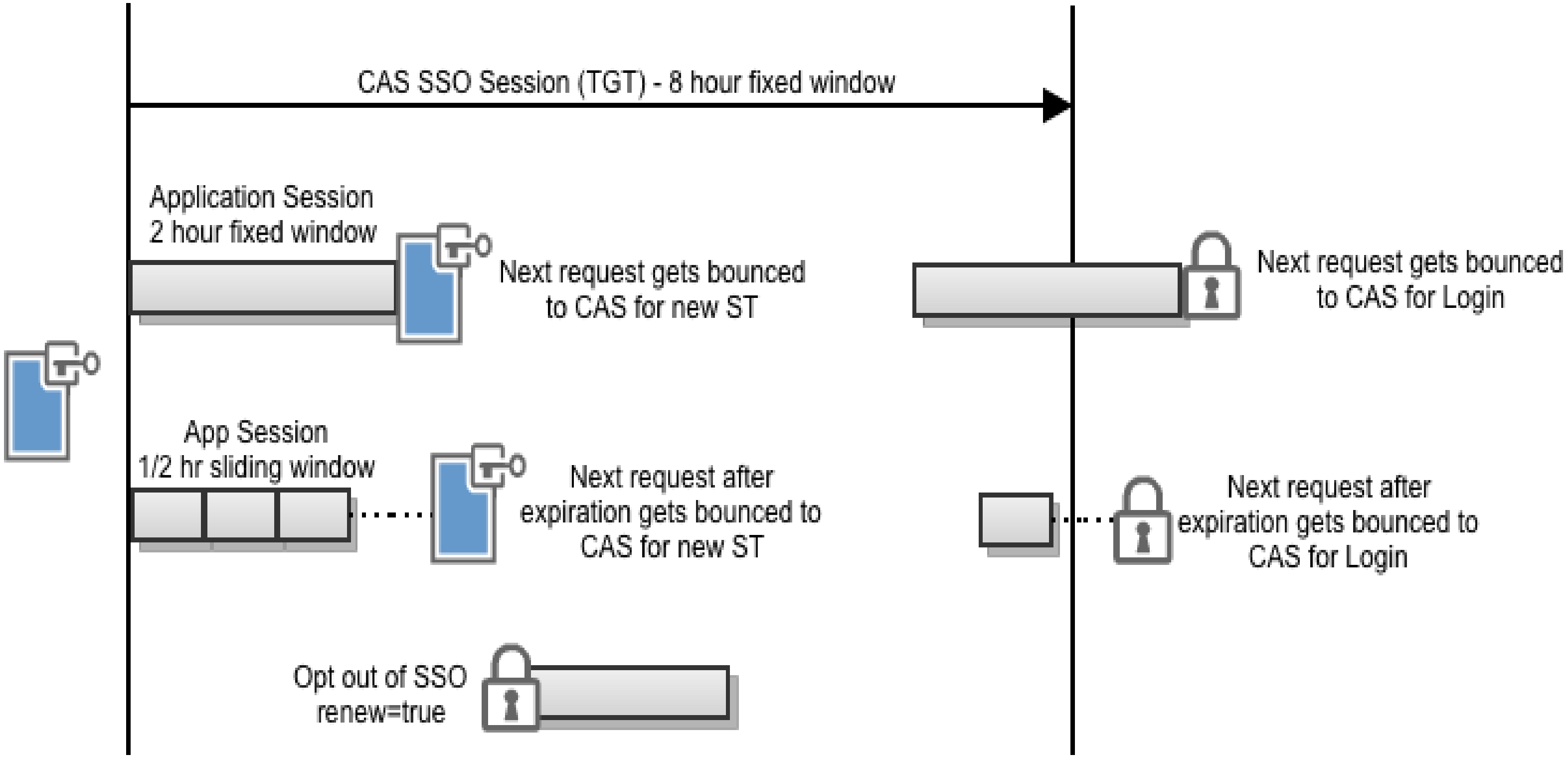
SSO vs App Session – Implications

- Security concerns about public terminals, kiosks - “keys to the kingdom”
  - Set TGT TTL to a smaller window
  - Group apps into different SSO domains
  - Reduce SSO domain via renew=true
  - Set TGT TTL automatically based on some request attributes – IP address
  - Ask the user – Public vs Private Workstation

SSO vs App Session – Expiration

- Application session is the responsibility of the application
  - Fixed window
  - Sliding window
  - Idle timeout
- If the app session expires, what is the UX on the next request? What should it be?

SSO vs App Session – Expiration


CAS SSO Session (TGT) - 8 hour fixed window
Application Session
2 hour fixed window
Next request gets bounced to CAS for new ST
Next request gets bounced to CAS for Login
App Session
1/2 hr sliding window
Next request after expiration gets bounced to CAS for new ST
Next request after expiration gets bounced to CAS for Login
Opt out of SSO
renew=true

Gateway & Landing Pages

- Gateway – check for SSO, otherwise just send them back unauthenticated
  - Portal home pages
  - Web application home pages
  - Resource with both protected and non-protected content
- Good replacement for old login screens, system status, scheduled downtime, etc.

Logout Pages

- What does logout mean in the context of SSO? What is the context of SSO?
  - Portal
    - SSO started and ended with the portal
    - Other apps participated in CAS but could not initiate a SSO session (new patch by Drew Mazurek: CAS-967)
  - Any App
    - How does the user know they have SSO?
    - When does it end? Logging out of any app?
    - Need logout pages to avoid logging back in

Single Sign Out

- Non-browser mediated mechanism to help clean up server-side resources of visited applications in the event of a CAS SSO logout.
  - Smells a little like session management
  - Inherently best effort, CAS simply does a back channel http requests to the service URLs associated with the issued Service Tickets
  - Still up to the individual applications to do the right thing

CAS Server Config

- Service Manager
- Ticket Registry Cleaner
- HA setup
- Primary authentication handlers
- Ticket Expiration Policy
- Remember Me authentication
- Throttling Logins
- Much more at: https://wiki.jasig.org/display/CASUM/Home

CAS Clients

Official – Legacy – Incubating – Unofficial
CASifying Apps – Integration Patterns

CAS Clients – Official

- Acegi (Spring Security)
- CAS Client for Java 3.0/3.1
- mod_auth_cas (Apache)
- PhpCAS
- .NET CAS Client

Official Clients

Generally being actively developed and maintained. Likely to get support on the cas-user list.

CAS Clients – Unofficial

.Net Http module   ASP.NET Forms Authentication   AuthCAS   CAS + Seam Web Applications

CASP Adds CAS   Authentication

CherryPy C   usion client script

Google Web To   th module

Perl Client   Seraph as CAS Client

Unofficial Clients

Essentially all of the clients people have let us know about, that may or may not be in active development anymore, and may solve a niche need. You should use these at your own risk. Many are excellent clients, but may no longer be supported any more. Others are purely theoretical examples of of how a client would function.

Soulwing CAS Client   Soulwing Java CAS Client   Symfony CAS Client

VBScript   Virginia Tech CAS Clients   WebObjects Client

https://wiki.jasig.org/display/CASC/Unofficial+CAS+Clients

CAS Clients – Incubating

- CASBar – Toolbar for Firefox 2

Official Clients

Incubating Clients are new clients that are under development, and which may become official clients. They're up-and-coming clients that we're paying attention to, have petitioned the Steering Committee to become official clients, and often have active members on cas-user.

CAS Clients – Legacy

- Yale CAS Client
- Apache Module
- PAM
- PL/SQL

Legacy Clients

In many cases, no longer actively developed, but still function quite well (i.e. the PAM module). In other cases, they've been superseded by newer clients (i.e. The Jasig CAS Client for Java). You will still find many people on cas-user who are familiar with these modules, but many have migrated to the newer code.

CAS Clients – CASifying Apps

Apache OFBiz Joomla 1.5 OpenCms OpenReports

SharePoint & ASP.NET Web Sites WebAdvisor Confluence as CAS Client

EZPublish Fisheye and Crucible Oracle Calendar web client with mod_cas

Oracle P +webmail

Pe re

CASifying Apps

Describes some unofficial instructions, many contributed by users, on how to CASify particular applications.

Sakai Sun Identity Manager Tomcat Manager

Roller weblogger Tomcat uPortal Client

WordPress Client Zimbra Zope client

https://wiki.jasig.org/display/CASC/CASifying+Applications

CAS Clients – CASified Apps

uPortal Mantis pNews Sympa

TikiWiki Mule Claroline Moodle

CASified Apps

Project / Vendor maintained CAS integration.
Works out-out-of-the-box!

Liferay Portal ILIAS Learning Management

Chamilo Simply Voting BlueSocket

https://wiki.jasig.org/display/CASC/CASifying+Applications

CAS Clients – Integration Type

- **Language / Platform Level Clients**
  - CAS Client for Java 3.x, phpCAS, .NET CAS Client
  - ASP, ColdFusion, Perl,...,Ruby of Rails, PL/SQL, Zope

- **Container Level Clients**
  - mod_auth_cas (Apache 2.x) – REMOTE_USER
  - Soulwing CAS Client (Tomcat)
  - IBM WebSphere (Trust Association Interceptor)

- **Application Specific Clients**
  - Apache OFBiz, Bonita BPM, Joomla, Oracle 11i Apps, PeopleSoft, SCT Banner, OpenCms,...,MediaWiki, WebSphere, WordPress...

CAS Clients – Integration Patterns

- **Custom Applications**
  - Official Clients (Java, .NET, PHP, Apache)
  - Incubating or Unofficial...or create your own. (ASP to Zope)
- **Application Specific Clients**
  - Usually 3rd party, integrate with app specific APIs for security, identity,...
  - Usually built in conjunction with Official Clients
- **Applications with out-of-the-box Support**
  - Sweet! Just turn it on!
- **Authentication Shims (the Hard Cases)**
  - Trust Mode, ClearPass, Application Session APIs, SSO Bridge

CAS Clients – AuthN Shims

- **Trust Mode**
  - App specific configuration to rely on REMOTE_USER or some other Request variable to trust the user was authenticated
- **ClearPass**
  - Enable ClearPass extension to get a hold of user credential in the clear...replay them to app login screen
- **Application Session APIs**
  - Authenticate first with CAS then call back channel API or web service to initiate application session
- **SSO Bridges**
  - Rely on native application support for a specific SSO provider. CASifying Oracle Access Manager.
  - Rely on 3rd party Identity Provider for authentication and user attributes - casshib

Case Study: Workforce Retraining Initiative

workforce
Retraining

http://portal.workforceretrainingus.com

WRI Overview

- Pilot program involving Cisco and the state of Michigan.
- Provides workforce retraining in the areas of broadband infrastructure and heath IT.
- Leverages training materials in the Cisco Networking academy.

What's interesting about this?

- Single sign on
- OpenLDAP
- Multiple sources of identities, CAS and Shibboleth.
- Uses casshib extension.

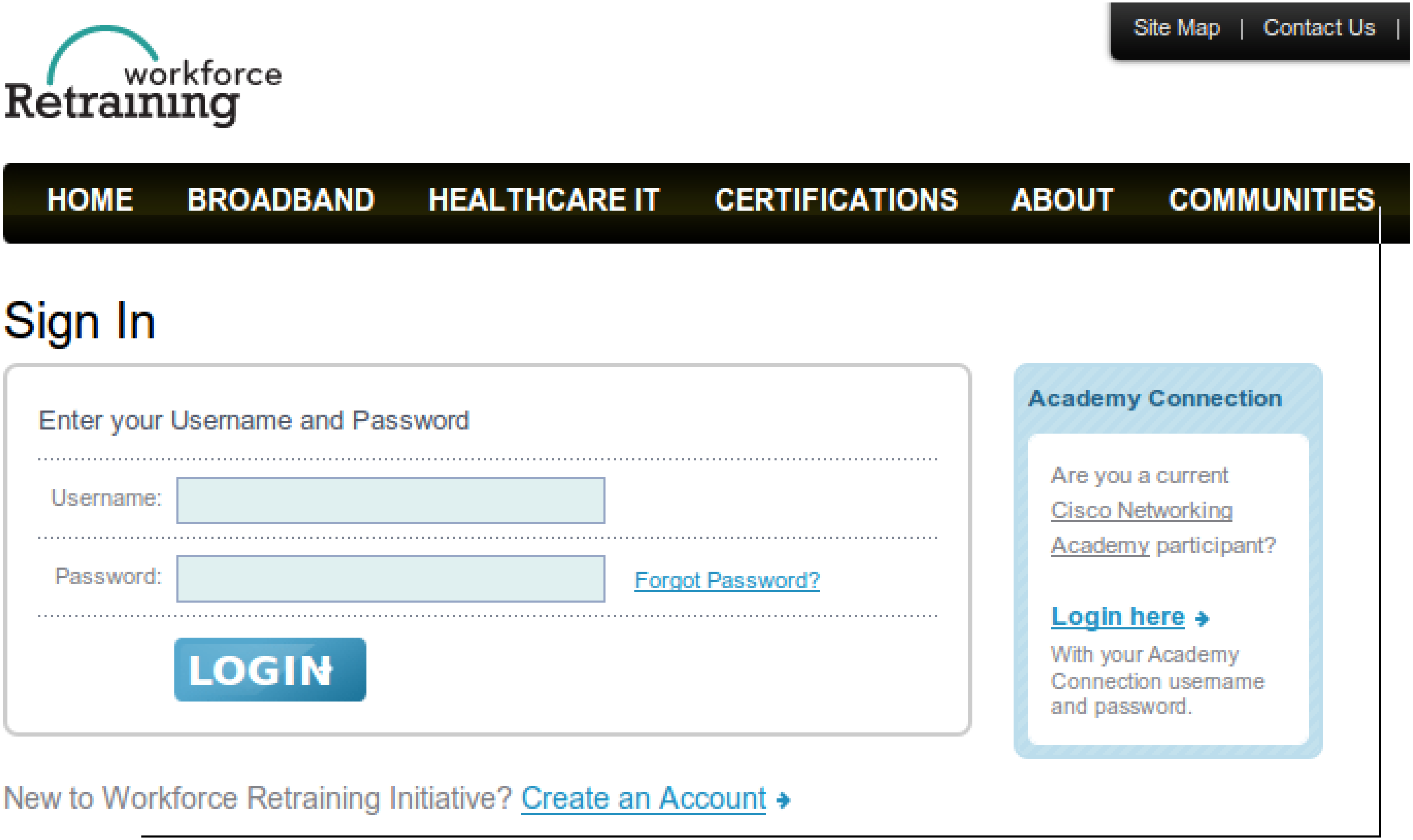
Shibboleth

- Open source
- Federated Web single sign on
- SAML
- Just-in-time release of attributes
- Identity Provider
- Service Provider

What's is casshib?

- Acts as a proxy between CAS and shibboleth
- Application is protected by CAS but delegates the login page to a Shibboleth IDP.
- Multiple sources of identities, CAS and Shibboleth.
- Shibboleth passes user attributes back to CAS.
- Shibboleth Service provider not required.
- JA-SIG license.

Federated Authentication



Sign In

Enter your Username and Password

Username:

Password:

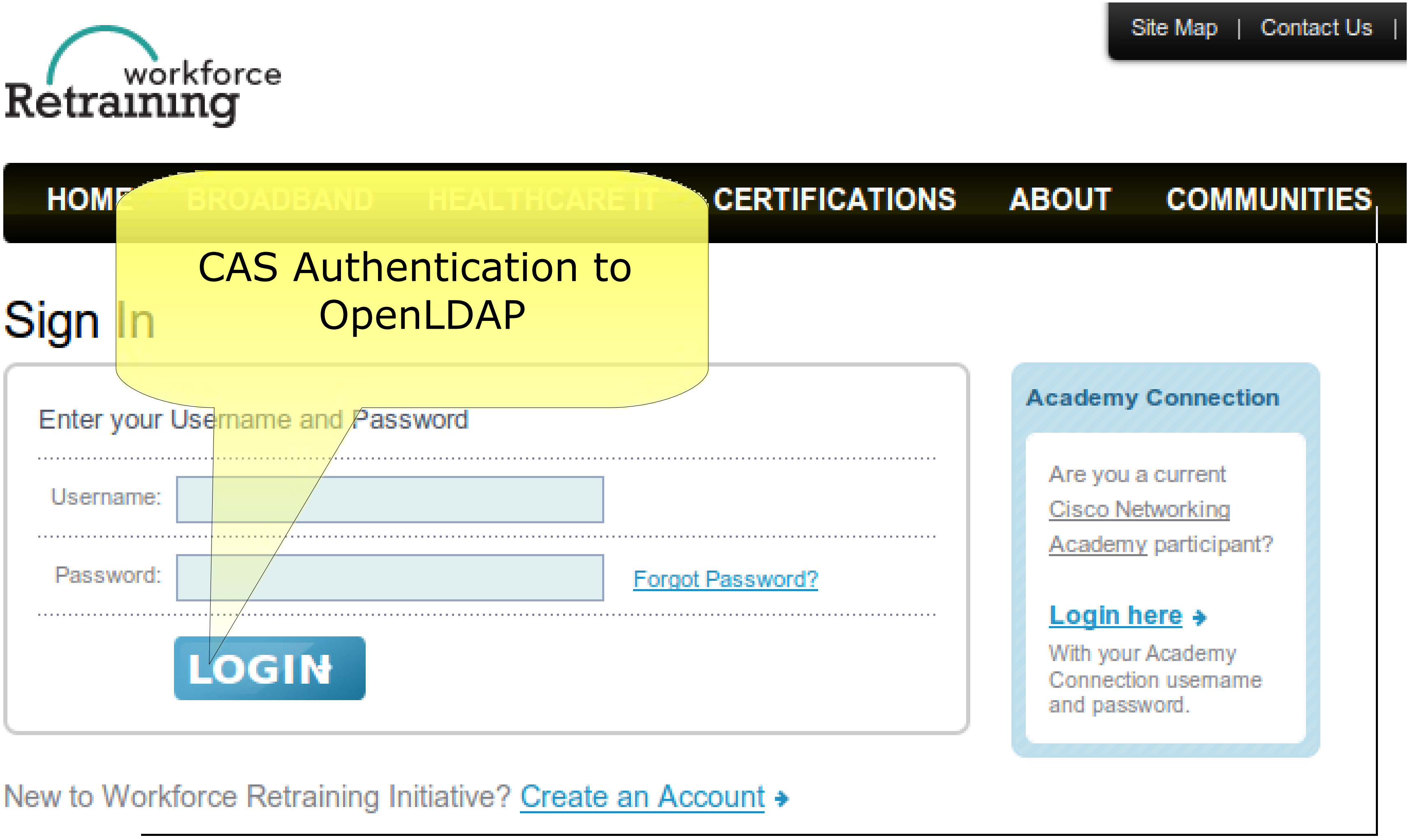
Academy Connection

Are you a current Cisco Networking Academy participant?

With your Academy Connection username and password.

New to Workforce Retraining Initiative? Create an Account

Federated Authentication



Sign In

Enter your Username and Password

Username:

Password:

Forgot Password?

Academy Connection

Are you a current Cisco Networking Academy participant?

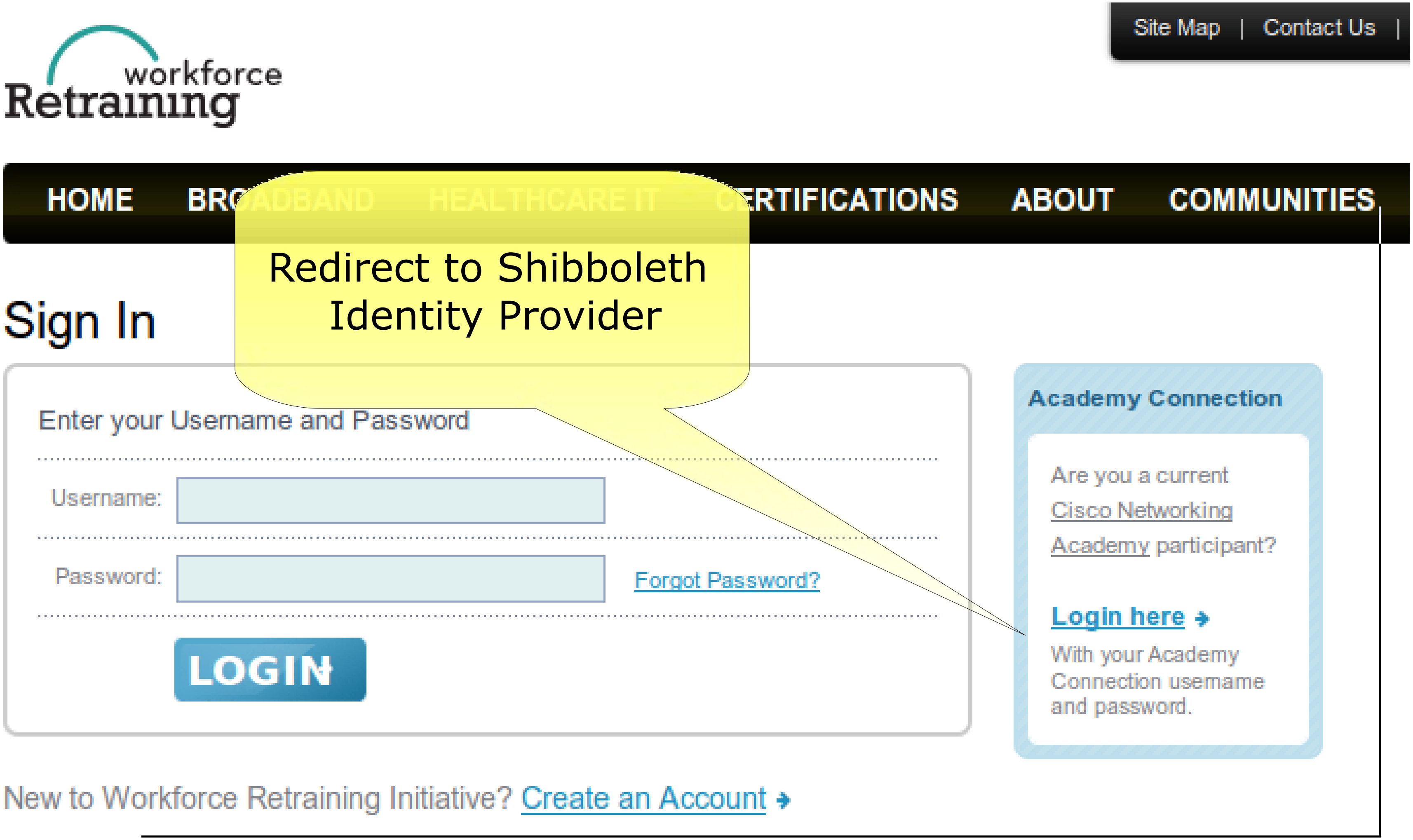
Login here

With your Academy Connection username and password.

New to Workforce Retraining Initiative? Create an Account

CAS Authentication to OpenLDAP

Federated Authentication



Site Map | Contact Us |

workforce Retraining

HOME BROADBAND HEALTHCARE IT CERTIFICATIONS ABOUT COMMUNITIES

Redirect to Shibboleth Identity Provider

Sign In

Enter your Username and Password

Username:

Password: Forgot Password?

LOGIN

Academy Connection

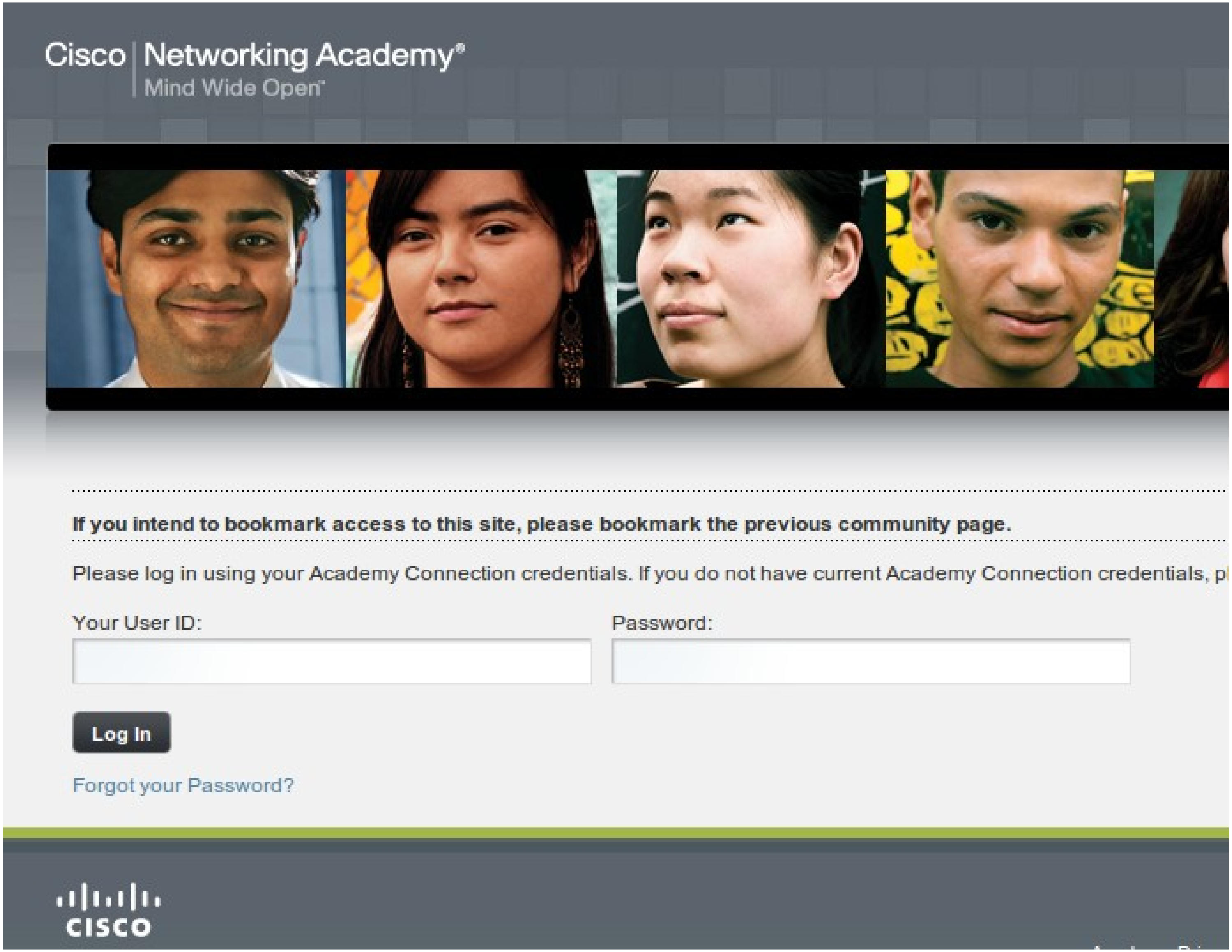
Are you a current Cisco Networking Academy participant?

Login here ➜

With your Academy Connection username and password.

New to Workforce Retraining Initiative? Create an Account ➜

Federated Authentication



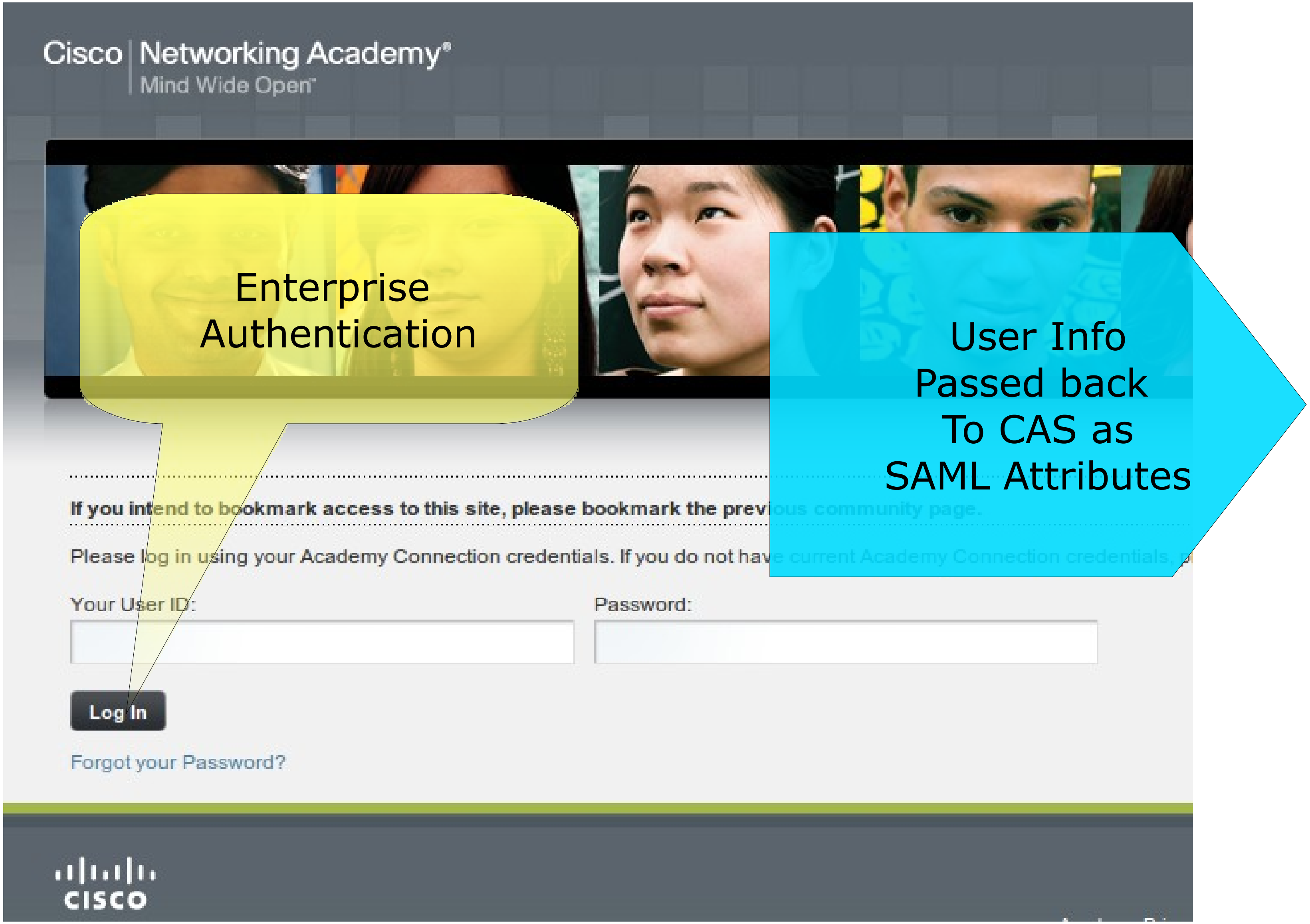
If you intend to bookmark access to this site, please bookmark the previous community page.

Please log in using your Academy Connection credentials. If you do not have current Academy Connection credentials, pl

Your User ID:

Password:

Federated Authentication



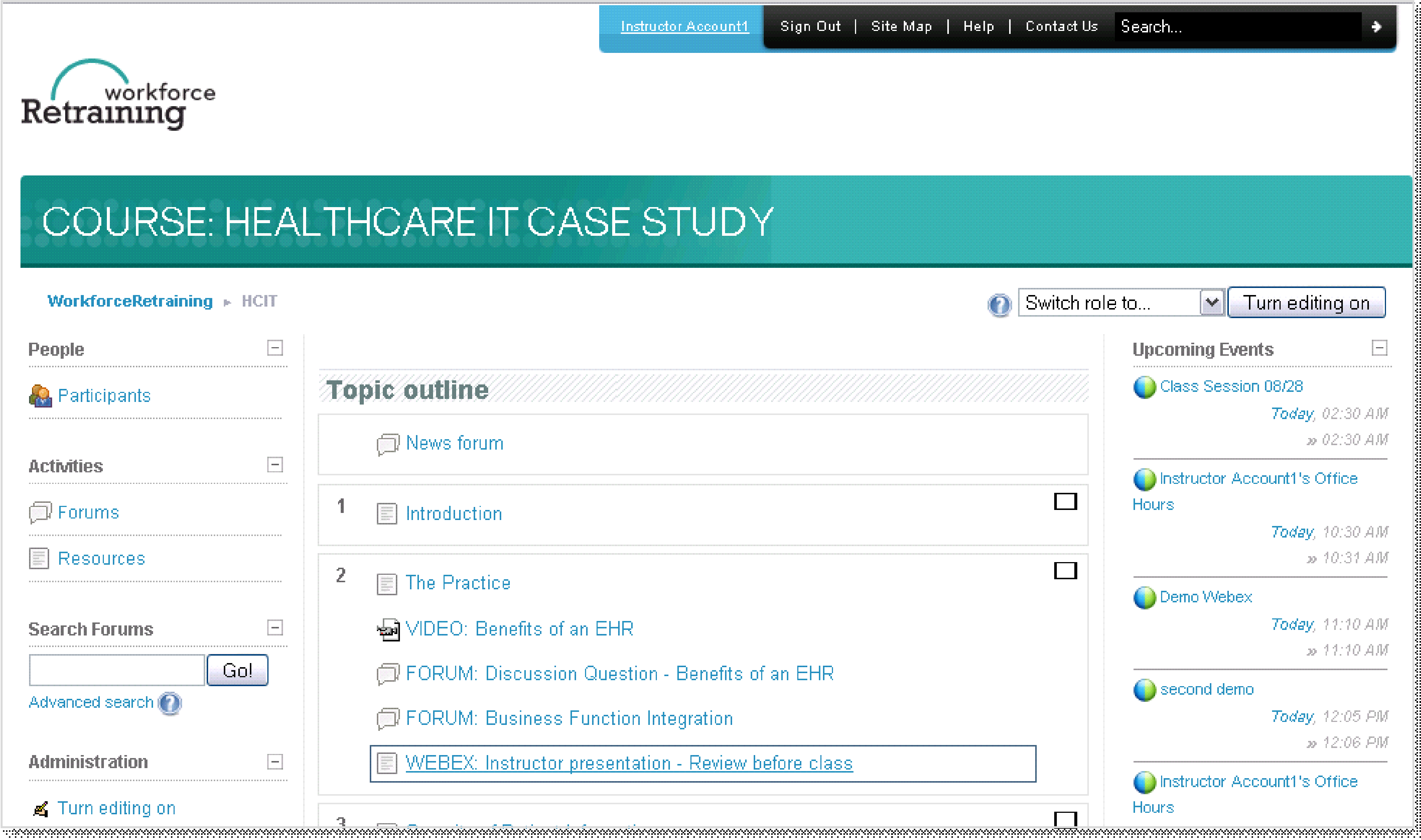
If you intend to bookmark access to this site, please bookmark the previous community page.

Please log in using your Academy Connection credentials. If you do not have current Academy Connection credentials, p

Enterprise Authentication

User Info Passed back To CAS as SAML Attributes

WRI Authenticated User



COURSE: HEALTHCARE IT CASE STUDY

People

- Participants

Activities

- Forums
- Resources

Search Forums

Administration

- Turn editing on

Topic outline

News forum

1 Introduction □

2 The Practice □

VIDEO: Benefits of an EHR

FORUM: Discussion Question - Benefits of an EHR

FORUM: Business Function Integration

WEBEX: Instructor presentation - Review before class

Upcoming Events

Class Session 08/28
Today, 02:30 AM
» 02:30 AM

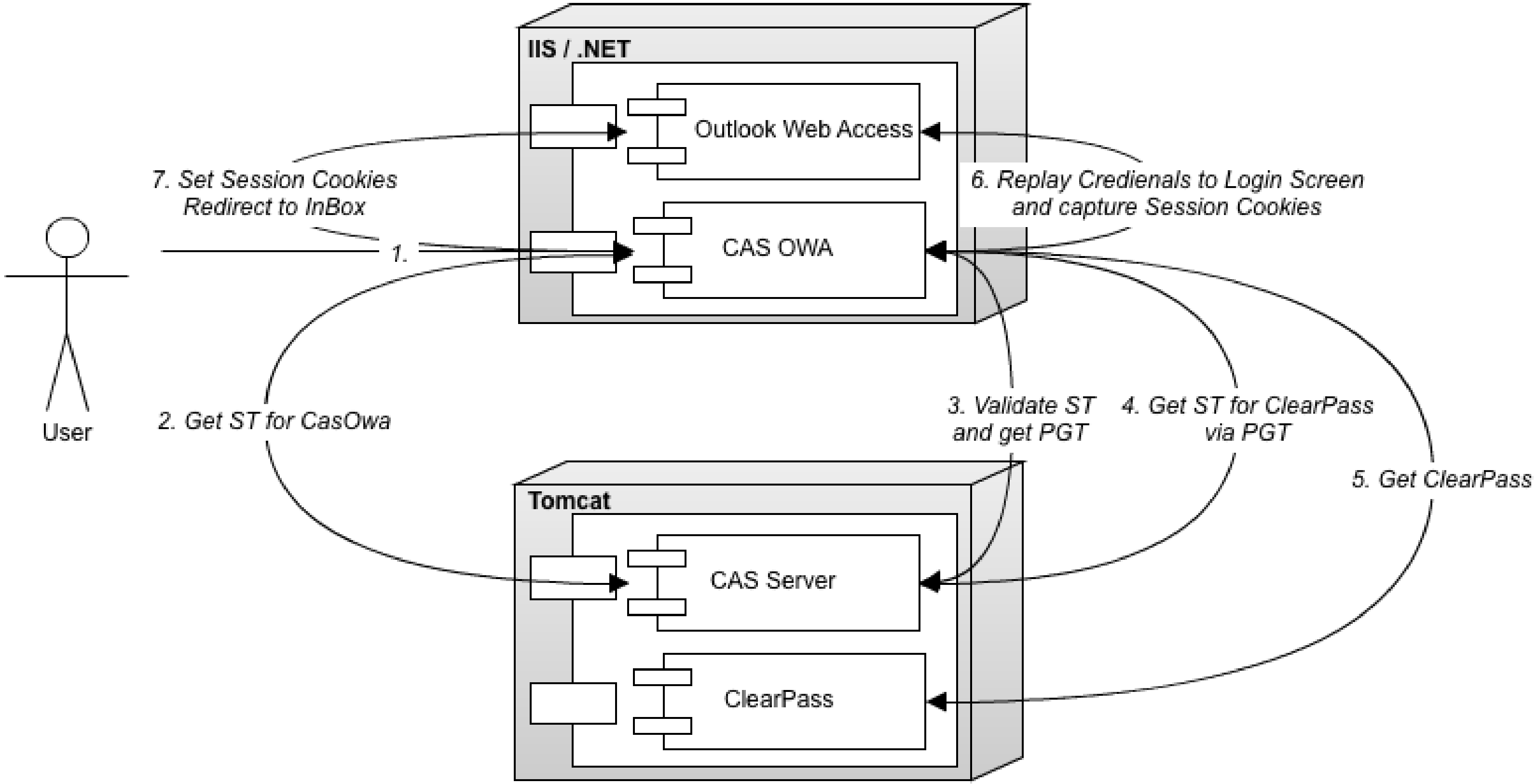
Instructor Account1's Office Hours
Today, 10:30 AM
» 10:31 AM

Demo Webex
Today, 11:10 AM
» 11:10 AM

second demo
Today, 12:05 PM
» 12:06 PM

Instructor Account1's Office Hours

AuthN Shims – Outlook Web Access

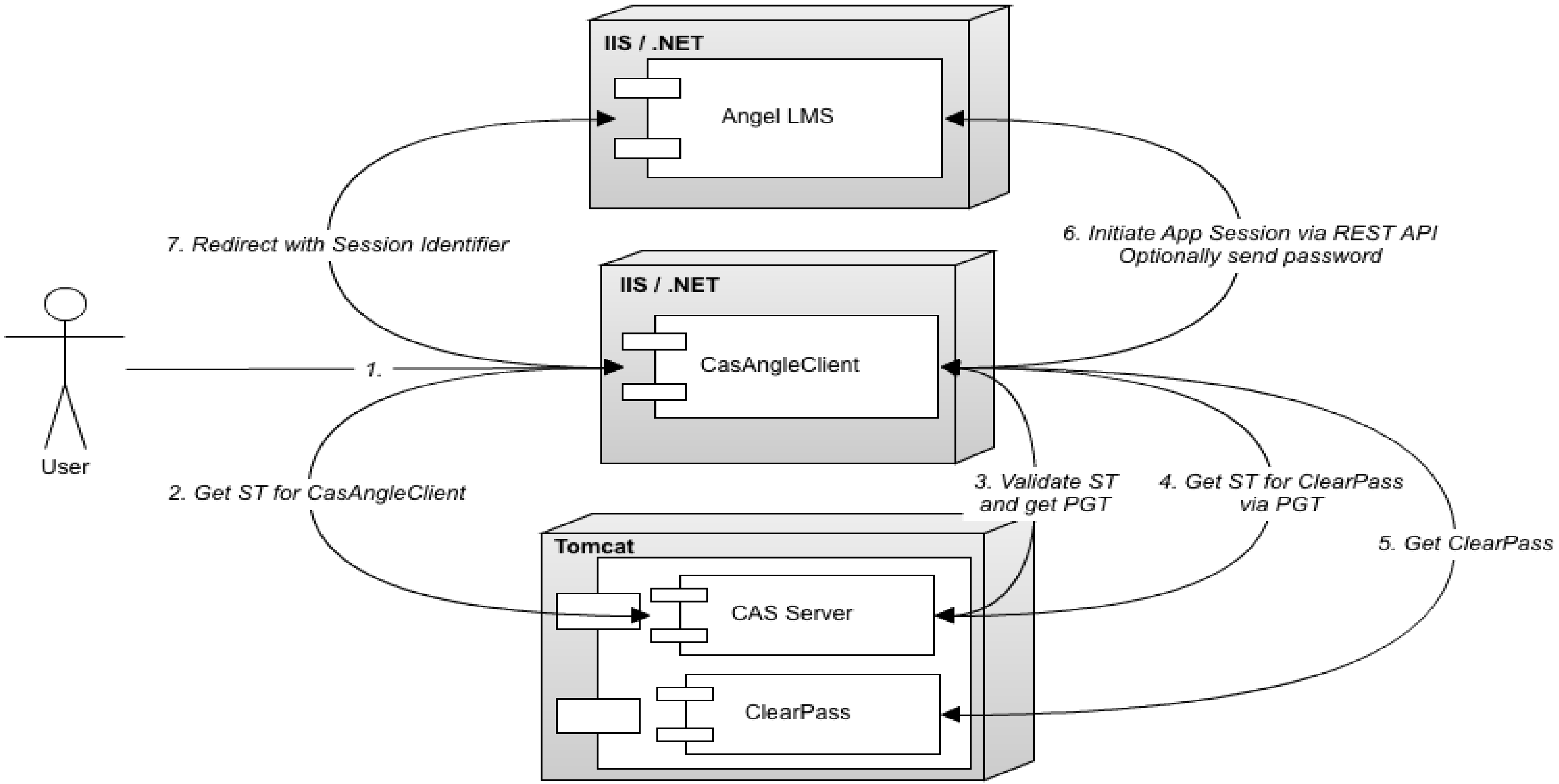


AuthN Shims – CasOwa

```
// .NET CAS Client does all the CAS protocol work
user = context.User as IcasPrincipal;
proxyTicket = user.GetProxyTicketFor(ClearPassUri);

// Leverage ClearPass extension to get the password
clearPass = GetTextForElement(response, "cas:credentials");

// Replay Credentials to OWA Login Form
request = WebRequest.Create(OwaUrl + OwaAuthPath);

// Capture Session cookies
Cookies.Add(new HttpCookie(cookie.Name, cookie.Value));

// Redirect to Inbox with Session Cookies set
context.Response.Redirect(redirectUrl);
```

https://github.com/wgthom/CasOwa

AuthN Shims – CasAngelClient



AuthN Shims – CasAngelClient

```
// .NET CAS Client does all the CAS protocol work
context.User.Identity.IsAuthenticated
CasAuthentication.GetProxyTicketIdFor(ClearPassUrl);

// Leverage ClearPass extension to get the password
GetTextForElement(clearPassResponse, "cas:credentials");

// Authenticate against Angel and retrieve redirect URL
strPost = "APIACTION=AUTHENTICATION_PASS&APIUSER="
       + AngelApiUser
       + "&APIPWD=" + AngelApiPassword
       + "&USER=" + context.User.Identity.Name
       + "&PASSWORD=" + clearPass
       + "&VALIDATE=" + (AngelApiValidate ? "1" : "0");
angelApiResponse = PerformHttpPost(AngelApiUrl, strPost, false);

redirectUrl = GetTextForElement(angelApiResponse, "success");
FormsAuthentication.SignOut();
context.Response.Redirect(redirectUrl);
```

STATE UNIVERSITY OF NEW YORK
EMPIRE STATE COLLEGE

https://github.com/wgthom/CasAngelClient

References

Adding "Public Workstation" vs. "Private Workstation" Timeouts - https://wiki.jasig.org/x/nBDP

Jasig CAS Gateway Feature - http://www.jasig.org/cas/client-integration/gateway

CAS Clients - https://wiki.jasig.org/display/CASC/Home

CAS Client for Outlook Web Access - https://github.com/wgthom/CasOwa

CAS Client for Angel LMS - https://github.com/wgthom/CasOwa

So Long, and Thanks for All the Fish

Bill Thompson
Software Architect
Unicon, Inc.

wgthom@unicon.net
www.unicon.net

Parker Neff
Software Architect
Unicon, Inc.

pneff@unicon.net
www.unicon.net