

I T H A K A

Enabling Access to Applications with Shibboleth:
Adding Shibboleth Logins to the Plone CMS

Alan Brenner

<http://tid.ithaka.org/shibplone.pdf>

Overview

- Zope and Plone
 - Zope as the Application Server
 - Plone as the Content Management System running in Zope
- End User Login Sequence Overview
- Apache Configuration
 - Apache as the Shibboleth Service Provider
 - Getting data from Apache to Zope
- AutoUserMakerPASPlugin
 - Overview and Installation
 - Configuration options
 - Python Source
- ShibbolethLogin
 - Installation, Configuration and Python Source
- ShibbolethPermissions
 - Installation and Configuration
 - Users grant permissions to their stuff
 - Python Source



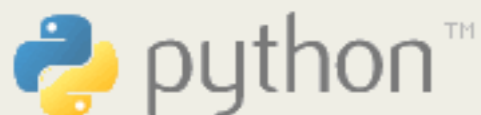
Who is Ithaka and Who am I?

- “Ithaka is an independent not-for-profit organization with a mission to accelerate the productive uses of information technologies for the benefit of higher education worldwide.”
 - Research, Strategic Services, Shared Services (IT, HR, etc.)
 - Affiliated with JSTOR and ARTstor
 - “Incubating” Aluka, NITLE and Portico
 - <http://www.ithaka.org/>
- I am a Senior Engineer in the Technology Innovation and Development group. I develop software, run web sites, databases, and email and VoIP systems, and administer several servers. I have developed these Plone ‘Products’ under the direction of the Research in Information Technology program of the Andrew W. Mellon Foundation.
 - <http://tid.ithaka.org/>
 - <http://rit.mellon.org/>

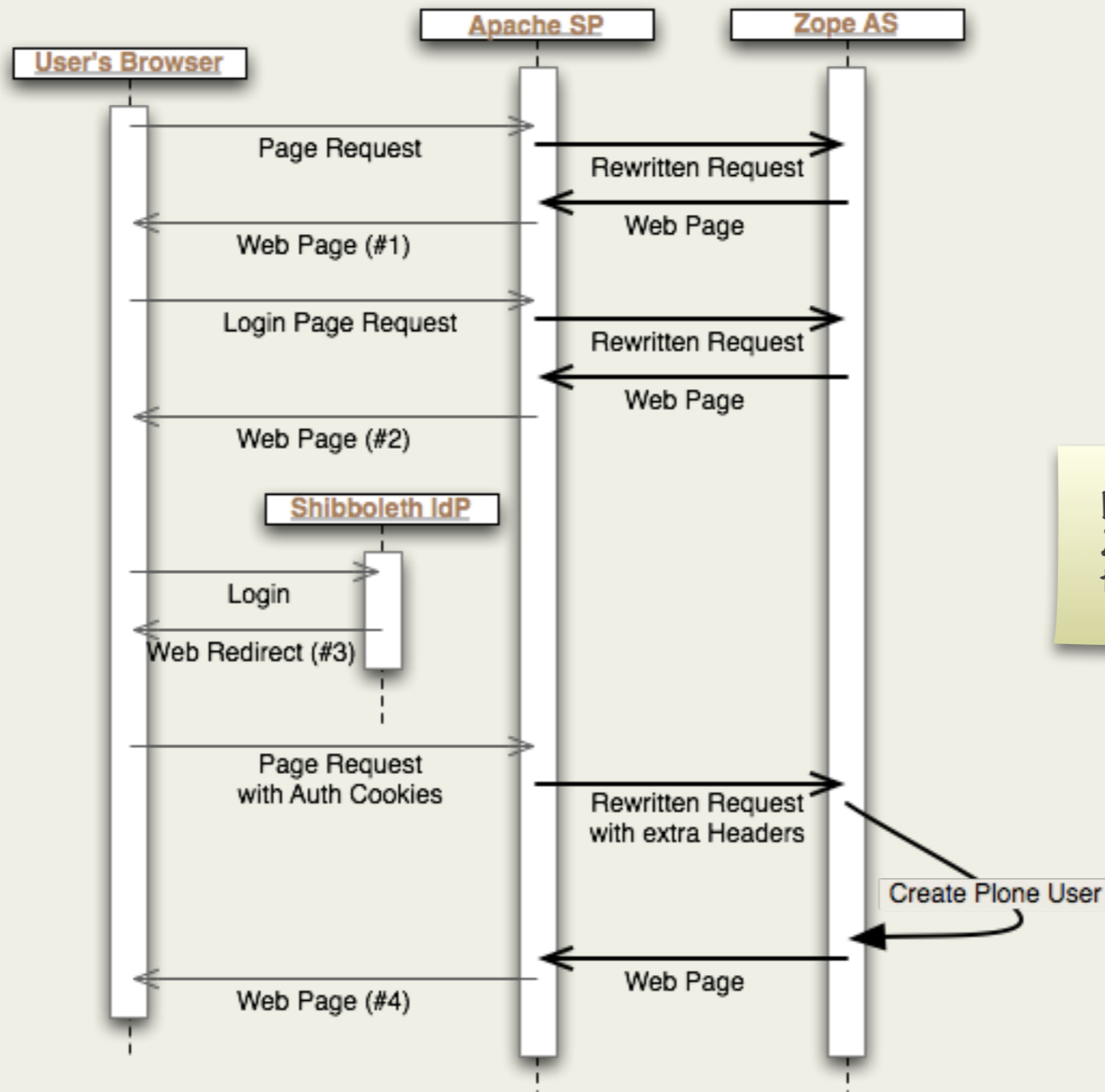


Zope and Plone

- Python
 - Both Zope and Plone are (mostly) written in Python, with a bit of C in Zope for performance in it's built-in database
 - <http://www.python.org/>
- Zope
 - "An open source application server for building content management systems, intranets, portals and custom applications"
 - <http://www.zope.org/>
- Plone
 - "A ready-to-run content management system"
 - Like Zope, it is extensible with 'Products' and Python modules
 - <http://plone.org/>
 - Currently at 3.0. The Shibboleth integration code is still for Plone 2.5.



Initial Login Sequence



I focus on the Apache to Zope communication in this presentation.

Plone: Login Sequence #1

site map accessibility contact

Plone™

home members news events test

log in join

you are here: home

navigation

- Home
- Members
- News
- Events
- test

log in

Login Name

Password

log in

Forgot your password?

New user?

Welcome to Plone

by Alan Brenner — last modified 2007-03-08 15:20

Congratulations! You have successfully installed Plone.

If you're seeing this instead of the web site you were expecting, the owner of this web site has just installed Plone. Do not contact the Plone Team or the Plone mailing lists about this.

The first thing you should do is to set up your site by visiting the [Site Setup](#) area. Become familiar with Plone by getting one of the [Plone books](#), and make sure you look at the available [add-on products](#) and [online documentation](#).

Quick Start

Some useful hints if you are new to Plone:

- Access key + 4 focuses the LiveSearch field – you can start writing your search terms straight away, and have all your information at your fingertips without leaving the keyboard. For information about how to use access keys in your particular browser, see the [Accessibility page](#).
- Plone will automatically be displayed in the language your browser asks for. If you need more control over languages in Plone, install Plone Language Tool from the [Site Setup](#). If you need to maintain your content in multiple languages, download [LinguaPlone](#).

September 2007

Su	Mo	Tu	We	Th	Fr	Sa
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

This is the default initial page. ShibbolethLogin modifies the page at the "log in" link in the upper right. You can easily remove the "log in" box ('portlet') on the left.

Plone: Login Sequence #2

The screenshot shows the Plone website's login page. At the top left is the Plone logo. To the right are links for 'site map', 'accessibility', and 'contact', along with a search box. Below the logo is a navigation menu with 'home', 'members', 'news', 'events', and 'test'. A secondary navigation bar contains 'log in' and 'join'. A breadcrumb trail reads 'you are here: home'. The main heading is 'Please log in', followed by the instruction: 'To access this part of the site, you need to log in with your user name and password.' Two login options are listed: 'Log in with a Local System user id.' and 'Log in with a Protect Networks user id.', both enclosed in a red box. Below these are links for 'registration form' and 'click here to retrieve it'. A box titled 'Account details' contains 'Login Name' and 'Password' fields, each with a note about case sensitivity, and a 'log in' button. A note at the bottom says 'Please log out or exit your browser when you're done.' A yellow callout box on the right explains that ShibbolethLogin adds 'Where are you from' links to Shibboleth Identity Providers and that the 'Account details' box encloses the login for local Plone accounts. A small illustration of a ship is in the bottom right corner.

site map accessibility contact

Plone™

home members news events test

log in join

you are here: home

Please log in

To access this part of the site, you need to log in with your user name and password.

Log in with a [Local System](#) user id.

Log in with a [Protect Networks](#) user id.

If you do not have an account here, head over to the [registration form](#).

If you have forgotten your password, [click here to retrieve it](#).

Account details

Login Name
Login names are case sensitive, make sure the caps lock key is not enabled.

Password
Case sensitive, make sure caps lock is not enabled.

Please log out or exit your browser when you're done.

ShibbolethLogin adds these 'Where are you from' links to Shibboleth Identity Providers. You specify the link titles and targets in the Zope Management Interface.

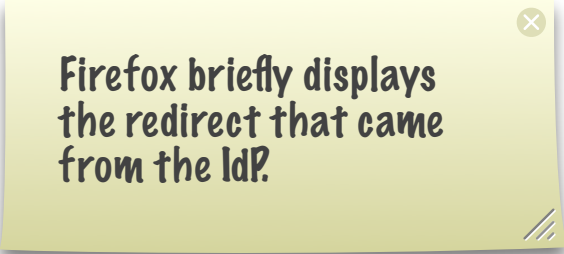
The "Account details" box encloses the login for local to Plone accounts.

Login Sequence #3

Shibboleth Authentication Request Processed

You are automatically being redirected to the requested site. If the browser appears to be hung up after 15-20 seconds, try reloading the page before contacting the technical support staff in charge of the desired resource or service you are trying to access.

Redirecting to requested site...



Firefox briefly displays
the redirect that came
from the IdP.



Plone: Login Sequence #4

site map accessibility contact site setup

Plone™

home members news events test

Alan Brenner my folder preferences undo log out

you are here: home

navigation

- Home
- Members
- News
- Events
- test

recent changes

- test 2007-07-20
- permtest 2007-07-13
- abrenner 2007-07-09
- me 2007-05-29

contents view edit properties **sharing**

display add to folder state: public draft

Welcome to Plone

by Alan Brenner — last modified 2007-03-08 15:20

Congratulations! You have successfully installed Plone.

If you're seeing this instead of the web site you were expecting, the owner of this web site has just installed Plone. Do not contact the Plone Team or the Plone mailing lists about this.

The first thing you should do is to set up your site by visiting the [Site Setup area](#). Become familiar with Plone by getting one of the [Plone books](#), and make sure you look at the available [add-on products](#) and [online documentation](#).

Quick Start

Some useful hints if you are new to Plone:

- Access key + 4 focuses the LiveSearch field – you can start writing your search terms straight away, and have all your information at your fingertips without leaving the keyboard. For information about how to use access keys in your particular browser, see the [Accessibility page](#).
- Plone will automatically be displayed in the language your browser asks for. If you need more control over languages in Plone, install Plone Language Tool from the [Site Setup](#). If you need

September 2007

Su	Mo	Tu	We	Th	Fr	Sa
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

And now I'm logged in.

Note my full name, and the sharing tab. My name is there because Shibboleth provided a header that got saved as my name. ShibbolethPermissions uses sharing tab.



Apache Configuration

- Install mod_shib
- mod_php is helpful during setup.
 - Create an index.php like:

```
<html><head><title>env</title></head><body><?php phpinfo(); ?></body></html>
```
 - This shows all of the values that are (or are not) getting set by mod_shib
- Configure Apache to proxy HTTP connections for Zope
- Configure Apache to rewrite HTTPS connections for Zope



Apache: httpd.conf and modules

- This can go in the httpd.conf:

```
# Load the SHIBBOLETH module
LoadModule mod_shib /usr/local/shibboleth-sp-1.3/libexec/mod_shib_22.so
# This is the XML file that contains all the global, non-apache-specific
# configuration. Look at this file for most of your configuration parameters.
ShibSchemaDir /usr/local/shibboleth-sp-1.3/share/xml/shibboleth
ShibConfig /usr/local/shibboleth-sp-1.3/etc/shibboleth/shibboleth.xml
```

- These modules also get loaded in the httpd.conf:

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule rewrite_module modules/mod_rewrite.so
```



Apache: HTTP Proxy

- (Almost) Minimal configuration:

```
<VirtualHost 192.168.191.1:80>  
    ServerName alan.ithaka.org  
    ServerAdmin alan.brenner@ithaka.org  
    DocumentRoot /usr/local/apache-httpd-2.2.4/htdocs  
    ProxyRequests Off  
    ProxyPass /index.php !  
    ProxyPass / http://127.0.0.1:8253/VirtualHostBase/http/alan.ithaka.org:  
80/test/VirtualHostRoot/  
</VirtualHost>
```

- This configures Apache to get pages from localhost port 8253.
- This tells Zope that pages it returns have <http://alan.ithaka.org/> as the base URL.
- It also tells Zope to fetch all pages from its /test folder (my Plone install).
- You might want to add Apache caching, other non-proxied URLs, etc.
- This is standard Apache in front of Zope, as documented at Plone's web site.



Apache: HTTPS Rewriting 1

- Apache listens on 443

```
<VirtualHost 192.168.191.1:443>
```

- Tell Apache to Proxy everything

- Sort of, since we don't tell Apache to proxy
- This gets most of the HTTP Headers passed through to Zope

```
<Proxy *>
```

```
    Order deny,allow
```

```
    Allow from all
```

```
</Proxy>
```

- Tell Apache to rewrite the header to set X_REMOTE_USER

- The REMOTE_USER value is looked up
- The value is stored temporarily
- The value is saved in the X_REMOTE_USER header

```
RewriteEngine On
```

```
RewriteCond %{LA-U:REMOTE_USER} (.+)
```

```
RewriteRule .* - [E=RW_RU:%1]
```

```
RequestHeader set X_REMOTE_USER %{RW_RU}e
```



Apache: HTTPS Rewriting 2

- Tell Apache not to rewrite these (my IdP is on the same Apache)

```
RewriteCond %{REQUEST_URI} !^(shibboleth-(sp|idp)|Shibboleth.sso|SAML)
```

- Tell Apache to rewrite everything else to Zope

- Mostly like the HTTP proxy.

- Add \$1 to the end of the Zope URL to pass the rest of the URL.

```
RewriteRule ^/(.*) http://127.0.0.1:8253/VirtualHostBase/https/  
alan.ithaka.org:443/test/VirtualHostRoot/$1 [L,P]
```

- Setup Shibboleth Authentication

```
<Location />
```

```
AuthType shibboleth
```

```
ShibRequireSession Off
```

```
require shibboleth
```

```
</Location>
```

```
</VirtualHost>
```



AutoUserMakerPASPlugin Overview

- Overview
 - PAS is the “Pluggable Authentication System” added to Plone 2.5
 - AutoUserMakerPASPlugin allows Zope to delegate authentication
 - Works with any authentication system available to Apache, not just Shibboleth
 - Can use values from Apache for authorization (to set Plone roles) as well
 - Origin
 - Originally a Zope/Plone Product called apachePAS by Rocky Burt on behalf of Zest Software (<http://zestsoftware.nl/>)
 - Updated and turned in to AutoMemberMakerPASPlugin by Erik Rose of the WebLion project at Penn State (<http://weblion.psu.edu/>)
- Installation
 - Standard Plone Product install (same for ShibbolethLogin and ShibbolethPermissions)
 - Unzip in the Plone \$INSTANCE_HOME/Products directory
 - Restart Zope
 - Go to the Add/Remove Products page, click the checkbox by the product name and the install button



Plone: Installing the Products

site map accessibility contact site setup

Plone™

home members news events test

alanbbr preferences undo log out

you are here: home

site setup

Plone Configuration

- Add/Remove Products
- Error Log
- Language Settings
- Mail Settings
- Navigation Settings
- Placeful Workflow
- Portal Settings
- Search Settings
- Skins
- Smart Folder Settings
- Users and Groups Administration
- Zope Management

Add/Remove Products

▲ Up to Site Setup

This is the Add-on Products install section, you can add and remove products in the lists below.

To make new products show up here, put them in the directory `/usr/local/test-2.9.7-2.5.3/Products` on the file system, and restart the server process.

Products available for install

- AutoUserMakerPASPlugin 0.6**
Product Description
- ShibbolethLogin 0.6**
Product Description
- ShibbolethPermissions 0.6**
Product Description

install

Installed products

- Archetypes 1.4.4-final**
Product Description Install log
- CMFPlacefulWorkflow 1.0.5**
Product Description Install log
- CMFSquidTool**
Install log
- CacheSetup**
Install log
- Marshall**
Install log
- MimetypesRegistry 1.5.0-final**



Plone: After Installing the Products

The screenshot shows the Plone site setup interface. At the top, there is a navigation bar with links for 'site map', 'accessibility', 'contact', and 'site setup'. The Plone logo is on the left, and a search box is on the right. Below the navigation bar, there are tabs for 'home', 'members', 'news', 'events', and 'test'. A user profile for 'alanbbr' is visible with links for 'preferences', 'undo', and 'log out'. The main content area is titled 'Add/Remove Products' and includes a breadcrumb 'Up to Site Setup'. A text block explains that this is the Add-on Products install section and provides instructions on where to place new products. The interface is divided into two columns: 'Products available for install' and 'Installed products'. The 'Products available for install' column contains an 'install' button. The 'Installed products' column lists several products, with 'AutoUserMakerPASPlugin 0.6' highlighted in a yellow box. A sidebar on the left contains various site setup options like 'Plone Configuration', 'Error Log', 'Language Settings', etc. A small illustration of a ship is in the bottom right corner.

site map accessibility contact site setup

Plone™

home members news events test

alanbbr preferences undo log out

you are here: home

site setup

Plone Configuration

- Add/Remove Products
- Error Log
- Language Settings
- Mail Settings
- Navigation Settings
- Placeful Workflow
- Portal Settings
- Search Settings
- Skins
- Smart Folder Settings
- Users and Groups Administration
- Zope Management

Add/Remove Products

▲ Up to Site Setup

This is the Add-on Products install section, you can add and remove products in the lists below.

To make new products show up here, put them in the directory `/usr/local/test-2.9.7-2.5.3/Products` on the file system, and restart the server process.

Products available for install

install

Installed products

- Archetypes 1.4.4-final
 - Product Description
 - Install log
- AutoUserMakerPASPlugin 0.6
 - Product Description
 - Install log
- CMFPlacefulWorkflow 1.0.5
 - Product Description
 - Install log
- CMFSquidTool
 - Install log
- CacheSetup
 - Install log
- Marshall

17

AutoUserMakerPASPlugin Configuration

- Configured through the “Zope Management Interface”, [ZMI](#)
- Configure domain name removal (if needed--probably should change)
 - The default is to remove all domain names from user ID's
 - This can map multiple people to the same Plone account
(abrenner@ithaka.org and abrenner@internet2.edu both are abrenner to Plone)
- Configure the HTTP headers to look for (if needed)
- Configure the headers to user for authorization (if needed)
 - If you add headers to the the User Mappings field, the AuthZ tab will allow you to assign Plone roles and groups, and to map existing Plone users, to header values.
 - If you add headers to the User Sharing fields, users can grant permissions to people *who have not ever logged in* (limited to what they have permissions on). AutoUserMakerPASPlugin will assign the granted permissions to a new user, immediately after it creates the user.



ZMI: acl_users

ZOPE Logged in as **alanbbr** Zope Quick Start Go

Root Folder

- + Control_Panel
- + acl_users
- temp_folder
- + test

© Zope Corporation
Refresh

Contents Search Properties Security Undo Ownership Interfaces Find Cache Doc

Pluggable Auth Service at /test/acl_users Help!

Apache Authentication Add

Type	Name	Size	Last Modified
<input type="checkbox"/>	AutoUserMakerPASPlugin (AutoUserMakerPAS Plugin)		2007-09-12 17:22
<input type="checkbox"/>	ShibbolethLogin (ShibbolethLogin Plugin)		2007-09-12 17:22
<input type="checkbox"/>	ShibbolethPermissions (ShibbolethPermissions Plugin)		2007-09-12 17:22
<input type="checkbox"/>	chooser		2007-03-08 14:20
<input type="checkbox"/>	credentials_basic_auth (HTTP Basic Auth)		2007-03-08 14:20
<input type="checkbox"/>	credentials_cookie_auth		2007-03-08 14:20
<input type="checkbox"/>	local_roles		2007-03-08 14:20
<input type="checkbox"/>	mutable_properties		2007-03-08 14:20
<input type="checkbox"/>	plugins		2007-03-08 14:20
<input type="checkbox"/>	portal_role_manager		2007-03-08 14:20
<input type="checkbox"/>	sniffer		2007-03-08 14:20
<input type="checkbox"/>	source_groups		2007-03-08 14:20
<input type="checkbox"/>	source_users		2007-03-08 14:20
<input type="checkbox"/>	user_factory (Plone User Factory)		2007-03-08 14:20

Rename Cut Copy Delete Import/Export Select All

/test is the Plone install in the Zope environment.

acl_users is the user and group repository.

The AutoUserMakerPASPlugin and other entries are links to the configuration pages.

ZMI: AutoUserMakerPASPlugin 1

Options AuthZ Activate Undo Ownership Interfaces Security Properties Doc

Apache Authentication at [/test/acl_users/AutoUserMakerPASPlugin](#)

Domain Name Stripping

- Do not strip domain names from usernames.
- Strip domain names from all usernames.
- Strip domain names from all usernames in the domain(s) below. **Enter one per line.**

User Setup Headers

HTTP Headers as made available by Apache/Shibboleth. See your Shibboleth's AAP.xml. Enter one per line. User setup will use the first available value.

HTTP_X_REMOTE_USER

User ID (for example, HTTP_X_REMOTE_USER)

HTTP_SHIB_PERSON_COMMONNAME

Only use the strip all option when you know there will not be ID duplication.

Use the strip from list option when you already have users in Plone and want to migrate to external authentication.

ZMI: AutoUserMakerPASPlugin 1 Example

Options AuthZ Activate Undo Ownership Interfaces Security Properties Doc

Apache Authentication at [/test/acl_users/AutoUserMakerPASPlugin](#)

Domain Name Stripping

- Do not strip domain names from usernames.
- Strip domain names from all usernames.
- Strip domain names from all usernames in the domain(s) below. **Enter one per line.**

```
ithaka.org  
mellon.org
```

User Setup Headers

HTTP Headers as made available by Apache/Shibboleth. See your Shibboleth's AAP.xml. Enter one per line. User setup will use the first available value.

```
HTTP_X_REMOTE_USER
```

User ID (for example, HTTP_X_REMOTE_USER)

```
HTTP_SHIB_PERSON_COMMONNAME
```

I recommend a configuration like this, unless you absolutely know you will not have user ID conflicts.

ZMI: AutoUserMakerPASPlugin 2

User Setup Headers

HTTP Headers as made available by Apache/Shibboleth. See your Shibboleth's AAP.xml. Enter one per line. User setup will use the first available value.

HTTP_X_REMOTE_USER

User ID (for example, HTTP_X_REMOTE_USER)

HTTP_SHIB_PERSON_COMMONNAME

User's full name (HTTP_SHIB_PERSON_COMMONNAME)

HTTP_SHIB_ORGPERSON_TITLE

User's description (HTTP_SHIB_ORGPERSON_TITLE)

HTTP_SHIB_INETORGPERSO_MAIL

User's email (HTTP_SHIB_INETORGPERSO_MAIL)

HTTP_SHIB_ORGPERSON_LOCALITY

User's locality (HTTP_SHIB_ORGPERSON_LOCALITY)

HTTP_SHIB_ORGPERSON_STATE

User's state (HTTP_SHIB_ORGPERSON_STATE)

HTTP_SHIB_ORGPERSON_C

User's country (HTTP_SHIB_ORGPERSON_C)

User Mapping Headers

The defaults might be all you need.

You can list sources for each field. AUMPP will use the first non-empty entry in the list.



Plone: Display of the User Setup Headers

The screenshot shows the 'Personal Preferences' page in Plone. On the left is a navigation sidebar with categories like 'Plone Configuration' and 'Add-on Product Configuration'. The main content area is titled 'Personal Preferences' and contains a section for 'Personal Details'. A blue rounded rectangle highlights the 'Full Name' field, which contains the text 'Alan Brenner'. Other fields include 'E-mail' (Alan.Brenner@lthaka.org), 'Location' (Princeton, NJ, US), 'Language' (Language neutral (site default)), and 'Biography' (Senior Engineer). A yellow callout box on the right contains the text: 'AutoUserMakerPASPlugin fills these values in, when the User Setup Headers have data. As mentioned in the login sequence, Plone shows the "Full Name" instead of the userid when this has data.'

Plone Configuration

- Add/Remove Products
- Error Log
- Language Settings
- Mail Settings
- Navigation Settings
- Placeful Workflow
- Portal Settings
- Search Settings
- Skins
- Smart Folder Settings
- Users and Groups Administration
- Zope Management Interface

Add-on Product Configuration

- Cache Configuration Tool
- Kupu visual editor
- qPloneSkinDump

Personal Preferences

▲ Up to My Preferences

Your personal settings.

Personal Details

Full Name
Alan Brenner

E-mail ■
Alan.Brenner@lthaka.org

Location
Your location – either city and country – or in a company setting, where your office is located.
Princeton, NJ, US

Language
Your preferred language.
Language neutral (site default) ▼

Biography
A short overview of who you are and what you do. Will be displayed on the your author page, linked from the items you create.
Senior Engineer

AutoUserMakerPASPlugin fills these values in, when the User Setup Headers have data. As mentioned in the login sequence, Plone shows the "Full Name" instead of the userid when this has data.



ZMI: AutoUserMakerPASPlugin 3

User Mapping Headers

Use the items below for global authorization/account mapping. **Enter one per line.** Examples include HTTP_X_REMOTE_USER, HTTP_SHIB_EP_PRINCIPALNAME, HTTP_SHIB_EP_ORGDN, and HTTP_SHIB_EP_ENTITLEMENT. If this maps to more than one user id, then this effectively declares a group.

You only need to fill these in when you, or your users, want to grant permissions to users authenticated via AutoUserMakerPASPlugin.

User Sharing Headers

Make the items below available for user sharing, *when ShibbolethPermissions is installed*. **Enter one per line.** Use the item in the second box as the label users see. Labels must be in the same order as the sources. Non-existent labels will use the source name. Examples are the same as the global authorization values, above.

Save



ZMI: AutoUserMakerPASPlugin 3 Example

User Mapping Headers

Use the items below for global authorization/account mapping. **Enter one per line.** Examles include HTTP_X_REMOTE_USER, HTTP_SHIB_EP_PRINCIPALNAME, HTTP_SHIB_EP_ORGDN, and HTTP_SHIB_EP_ENTITLEMENT. If this maps to more than one user id, then this effectively declares a group.

HTTP_X_REMOTE_USER

When you add lines to the User Mapping Headers, AutoUserMakerPASPlugin enables assigning global Plone roles.

Adding User Sharing Headers allows users to grant permissions to users who don't exist yet.

User Sharing Headers

Make the items below available for user sharing, when *ShibbolethPermissions* is installed. **Enter one per line.** Use the item in the second box as the label users see. Labels must be in the same order as the sources. Non-existent labels will use the source name. Examples are the same as the global authorization values, above.

HTTP_X_REMOTE_USER
HTTP_SHIB_ORGPERSON_ORG

User ID
Organization

Save

ZMI: AutoUserMakerPASPlugin AuthZ 1

Options AuthZ Activate Undo Ownership Interfaces Security Properties Doc

Apache Authentication at /test/acl_users/AutoUserMakerPASPlugin

Add Role Mapping

Source Values	Roles			User	Group(s)
	Manager	Owner	Reviewer		
HTTP_X_REMOTE_USER abrenner	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		Administrators Reviewers

These values are python regular expressions that will be compiled as raw strings. See [the python re module documentation](#) and [Dive Into Python's Regular Expressions chapter](#). The member role is always given. To map an existing user to a Shibboleth user, select the existing user id from the drop down list. In this case, roles given here are ignored (the Shibboleth user gets the already existing Plone user's roles).

Add

The initial role mapping shows anyone with 'abrenner' in the HTTP_X_REMOTE_USER getting assigned to the Administrators group at first log in.



ZMI: AutoUserMakerPASPlugin AuthZ 2

Options AuthZ Activate Undo Ownership Interfaces Security Properties Doc

Apache Authentication at /test/acl_users/AutoUserMakerPASPlugin

Add Role Mapping


Source Values	Roles			User	Group(s)
	Manager	Owner	Reviewer		
HTTP_X_REMOTE_USER <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	Administrators Reviewers

These values are python regular expressions that will be compiled as raw strings. See [the python re module documentation](#) and [Dive Into Python's Regular Expressions chapter](#). The member role is always given. To map an existing user to a Shibboleth user, select the existing user id from the drop down list. In this case, roles given here are ignored (the Shibboleth user gets the already existing Plone user's roles).

Edit Role Mappings

Source Values	Roles			User	Group(s)	Delete
	Manager	Owner	Reviewer			
HTTP_X_REMOTE_USER <input type="text" value="abrenner"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	Administrators Reviewers	<input type="checkbox"/>

After clicking the Add button, AutoUserMakerPASPlugin has a mapping, so it shows it with some edit/delete options.



ZMI: AutoUserMakerPASPlugin AuthZ 3

Options AuthZ Activate Undo Ownership Interfaces Security Properties Doc

Apache Authentication at /test/acl_users/AutoUserMakerPASPlugin

Add Role Mapping


Source Values	Roles			User	Group(s)
	Manager	Owner	Reviewer		
HTTP_X_REMOTE_USER <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value=""/>	Administrators Reviewers

These values are python regular expressions that will be compiled as raw strings. See [the python re module documentation](#) and [Dive Into Python's Regular Expressions chapter](#). The member role is always given. To map an existing user to a Shibboleth user, select the existing user id from the drop down list. In this case, roles given here are ignored (the Shibboleth user gets the already existing Plone user's roles).

Edit Role Mappings

Source Values	Roles			User	Group(s)	Delete
	Manager	Owner	Reviewer			
HTTP_X_REMOTE_USER <input type="text" value="abrenner"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="me"/>	Administrators Reviewers	<input type="checkbox"/>

This shows that the external user 'abrenner' will be the Plone user 'me'. Handy for migrating existing Plone sites, so users have one less password to deal with.



AutoUserMakerPASPlugin Source

- AutoUserMakerPASPlugin/Extensions/Install.py
 - Instantiates and activates as the Authentication and Extraction interfaces
- AutoUserMakerPASPlugin/auth.py
 - Defines the ExtractionPlugin class
 - Implements the IExtractionPlugin interface
 - The extractCredentials method gets the HTTP request values configured by the Plone administrator and stores them for use by a class that implements the IAuthenticationPlugin interface.
 - Defines the AutoUserMakerPASPlugin class
 - Implements the IAuthenticationPlugin interface
 - The authenticateCredentials method creates Plone users from Shibboleth authenticated users, and assigns roles and permissions to those users.
 - Defines the ApacheAuthPluginHandler class
 - handles the ZMI configuration forms




ShibbolethLogin

- Installing this modifies the default login_form, adding a section that show the configured Identity Providers.
 - This only works when you haven't modified the default login_form.
 - You can use the tal:block in a customized form:


```
<tal:block tal:define="wayf here/acl_users/ShibbolethLogin">
  <p i18n:translate="description_external_login"
    tal:repeat="idp python:wayf.getWayf(came_from)">
    Log in with a <a href="" tal:attributes="href python:idp[1]"><span
tal:content="python: idp[0]">PROVIDER</span></a> user id.
  </p>
</tal:block>
```
- Configuration is all on one page in the ZMI (acl_users/ShibbolethLogin).
 - The configuration page has 2 defaults as examples.
 - The first example should have all of the 'localhost's replaced with your configuration.
 - The second example works as-is: ProtectNetwork's identity provider.
 - The Plone administrator needs to configure this right after installation.
 - At least remove the "localhost" entries.

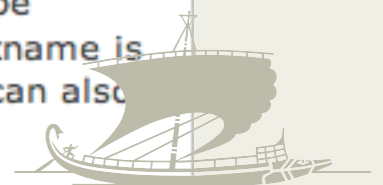


ZMI: ShibbolethLogin Configuration

Options	Activate	Undo	Ownership	Interfaces	Security	Properties	Doc
 Shibboleth Login at /test/acl_users/ShibbolethLogin							
<h2>Shibboleth Login URL</h2>							
<input type="text" value="https://localhost/shibboleth"/> <p>The Shibboleth provider ID (see your shibboleth.xml).</p>							
<input type="text" value="https://localhost/Shibboleth.sso/SAML/POST"/> <p>The URL to use by the Identity Provider. Probably something like https://hostname/Shibboleth.sso/SAML/POST.</p>							
<input type="text" value="Local System"/> <input type="text" value="Protect Networks"/> <p>Labels for the URLs, below. One per line in the same order as the URLs.</p>							
<input type="text" value="https://localhost/Shibboleth.sso/WAYF/localhost?target=https://idp.protectnetwork.org/protectnetwork-idp/SSO"/> <p>URLs to redirect to for initiating a session. The URL to return to will be appended to this value. This could be something like https://hostname/Shibboleth.sso/SessionInitiatorLocation?target= where the hostname is the system running the service provider and SessionInitiatorLocation is as defined in shibboleth.xml. This can also be something like https://idp.protectnetwork.org/protectnetwork-idp/SSO.</p>							
<input type="text" value="https://localhost/Shibboleth.sso/Logout?return="/> <p>The URL to redirect to for terminating a session. The URL to return to will be appended to this value. This should be something like https://hostname/Shibboleth.sso/Logout?return= where the hostname is the system running</p>							

Replace at least all of the 'localhost's with your server.

The big fields are a (meta-) WAYF.



ShibbolethLogin Python

- ShibbolethLogin/Extensions/Install.py
 - Instantiates an instance in the acl_users folder
 - Gets the default login_form, modifies it to add the TAL block, and saves the updated form in portal_skins/custom
 - Installs a custom logout_form that redirects users back to the HTTP site.
- ShibbolethLogin/redirector.py
 - Defines a ShibbolethLogin class
 - retrieves configuration values for the login and logout forms
 - Defines a ShibbolethLoginHandler class
 - handles the ZMI configuration forms



ShibbolethPermissions

- Installing this modifies the default Plone sharing page, adding a section for granting permissions to new users based on incoming attributes.
 - Already existing Plone users, regardless of how they authenticate, are handled by the existing Plone sharing mechanism.
- Site administrators configure the fields available to users in the AutoUserMakerPASPlugin ZMI page.
- The ShibbolethPermissions ZMI page shows all existing grants.
 - The administrator can delete them on this page.
 - This page has links to each page that has user sharing; edit them there.
- Users grant permissions by clicking on the “sharing” tab of any page that they have permissions on.
 - This will probably require some user education.
 - Fields are regular expressions, which includes simple strings.
 - Some fields can have complex values like LDAP distinguishing names.
 - Fields that don't have values match everybody.
 - There is no simple *match everybody except* syntax.



Plone: User Sharing 1

Alan Brenner my folder preferences undo log out

you are here: home

navigation

- Home
- Members
- News
- Events
- test

recent changes

- test 2007-07-20
- permtest 2007-07-13
- abrenner 2007-07-09
- me 2007-05-29
- Past Events 2007-03-08
- All recent changes...

contents view edit properties **sharing**

display add to folder state: public draft

Current sharing permissions for Welcome to Plone

Attention! You are setting the sharing permissions for a Page. If you want to set the permissions for its container, click [here](#).

You can share the rights for both entire folders and single items. These users have privileges here:

Assigned Roles for Welcome to Plone

	name	type	inherited role(s)	local role(s)
<p>Roles to assign to selected user(s)/group(s)</p> <input type="checkbox"/> Manager <input type="checkbox"/> Member <input type="checkbox"/> Reviewer				
<input type="checkbox"/> assign selected role(s) to selected user(s)/group(s)				
<input type="checkbox"/> delete selected role(s) and user(s)/group(s)				


Add sharing permissions to users

Sharing is an easy way to allow others access to collaborate with you on your content. To share this item, search for the person's name or email address in the form below, and assign them an appropriate role. The most common use is to give people Manager permissions, which means they have full control of this item and its contents (if any).

September 2007

Su	Mo	Tu	We	Th	Fr	Sa
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

This is the top of the sharing tab. Scroll down to get to the ShibbolethPermissions section.



Plone: User Sharing 2

Add sharing permissions to groups

Groups are a convenient way to share items to a common set of users. Select one or more groups, and a role to assign.

Search Terms

Search Term

perform search

Shibboleth Permissions

Manage permissions from Shibboleth attributes.

Assign Permissions based on Shibboleth Attributes

User ID abrenner

Organization

dc=internet2,dc=edu

Role to assign

- Manager
- Member
- Owner
- Reviewer

apply settings

Advanced settings

Advanced Settings

Inherit roles from higher levels

Determines if the roles given to users and groups from higher levels are in effect in this context. Use this to block people who have local roles in

The titles come from the AutoUserMakerPASPlugin configuration.

Adding a grant to a specific abrenner. A User ID of just abrenner would match abrenner@ithaka.org too.



Plone: User Sharing 3

Shibboleth Permissions

Manage permissions from Shibboleth attributes.

Manage existing Shibboleth rules.

<input type="checkbox"/>	source/values	local role(s)
<input type="checkbox"/>	HTTP_SHIB_ORGPERSON_ORG = 'dc=internet2,dc=edu' HTTP_X_REMOTE_USER = 'abrenner'	Owner

Roles to assign to selected attribute sets.

Manager ▲
Member ▼
Owner ▲
Reviewer ▼

assign selected role(s) to selected shibboleth patterns(s)

delete selected shibboleth pattern(s)

Assign Permissions based on Shibboleth Attributes

User ID

Organization

Role to assign
 Manager ▲
 Member ▼
 Owner ▲
 Reviewer ▼

apply settings

Since we've set up a permission, we've now got an edit area.



ZMI: ShibbolethPermissions

Path	Shibboleth Attribute(s)	Plone Role(s)
<input type="checkbox"/> /test/front-page	HTTP_SHIB_ORGPERSON_ORG = 'dc=internet2,dc=edu' HTTP_X_REMOTE_USER = 'abrenner'	Owner

Delete Selected Shibboleth Pattern(s)

The path is a link to the page that the user has shared.

The attribute list shows those items the user filled in, with the actual HTTP header names.

ShibbolethPermissions Python

- ShibbolethPermissions/Extensions/Install.py
 - Instantiates an instance in the acl_users folder
 - Gets the default folder_localrole_form, inserts the TAL based Shibboleth forms, and saves the updated form in portal_skins/custom
 - Installs several small functions that get called by the forms to get and set the configuration
- ShibbolethPermissions/permissions.py
 - Defines the ShibbolethPermissions class
 - Handles the storage of the user's permission sharing (CRUD)
 - Defines the ShibbolethPermissionsHandler class
 - Handles the ZMI forms



Summary

- The software is available at:
 - <http://www.python.org/>
 - <http://www.zope.org/>
 - <http://plone.org/>
 - The Plone site has complete python/zope/plone installers for Windows, OS X and SuSE Linux, with a “Unified Installer” for other Linuxes, BSDs and Solaris.
 - Installing by hand is just the common `./configure; make; make install` process for Zope, running `mkzopeinstance` to create a directory tree and unzipping Plone in it.
 - <http://tid.ithaka.org/software/>
 - AutoUserMakerPASPlugin
 - ShibbolethLogin
 - ShibbolethPermissions

