# PHP CAS Setup - Simple

This article is a reference guide for setting up PHP applications running CAS for UGA. This content is provided for informational purposes for UGA authorized personnel. This will help you get started.

- 1. EITS reference guide
- 2. CAS Reference Guide
- 3. Request CAS Access
- 4. Download the PHP CAS library from Jasig.org. The file will be a Gzipped Tar File (TGZ). If you are running windows, you may need to use a program like WinRAR.
  - After unzipping the file, find the CAS folder. Copy it along with the CAS.php file to a folder in your project called phpcas.

The file stucture is like this:

phpcas
 CAS

- Languages
  - PGTStorage
  - ProxiedService
  - ProxyChain
  - Request
- AuthenticationException.php
- Autoload.php
- Client.php
- CookieJar.php
- Exception.php
- GracefullTerminationException.php
- InvalidArgumentException.php
- OutOfSequenceBeforeAuthenticationCallException.php
- OutOfSequenceBeforeClientException.php
- OutOfSequenceBeforeProxyException.php
- OutOfSequenceException.php
- ProxiedService.php
- ProxyChain.php
- ProxyTicketException.php
- TypeMismatchException.php
- CAS.php
- 5. Upload the files to root /phpcas (outside your public\_html folder). This should be your site's root folder where your etc and cgi-bin folders are located.
- 6. You need to upload the config files, log files and key files for dev and prod to your etc directory. prodcas.pem and devcas.pem are located in the etc folder in this project.

# **Simple Cas**

1. Upload etc/config.php to your etc directory. This is an example of the areas of the config.php file that you will need to modify.

```
// Basic Config of the phpCAS client //
// source folder
define('__ROOT__', dirname($_SERVER["DOCUMENT_ROOT"]));
$phpcas_path = __ROOT__.'/phpcas/source';
// Full Hostname of your CAS Server
# prod = 'cas.uga.edu', dev = cas.dev.uga.edu, stage = cas.stage.uga.edu
$cas_host = 'cas.uga.edu';
// Context of the CAS Server
$cas_context = '/cas';
// Port of your CAS server. Normally for a https server it's 443
$cas_port = 443;
// Path to the ca chain that issued the cas server certificate
# Either /etc/prodcas.pem or /etc/devcas.pem
$cas_server_ca_cert_path = __ROOT__.'/etc/prodcas.pem';
```

 Upload index.php to your website where you want CAS protection. You can choose the CAS or the CAS\_SAML implementation. CAS\_SAML provides access to user information from Active Directory. When you set up the CAS client in index.php, you will choose one or the other. The two options are below: phpCAS::client(CAS\_VERSION\_2\_0, \$cas\_host, \$cas\_port, \$cas\_context);

### CAS\_SAML

phpCAS::client(SAML\_VERSION\_1\_1, \$cas\_host, \$cas\_port, \$cas\_context);

- 3. Change the paths according to the environment that you are wanting to test against. (dev, stage or prod).
- 4. You need to wait for your application to be added to CAS Dev and then wait for someone on the security team to contact you about testing your application in Dev. If your application is approved in Dev you will be able to move to Staging. If it is approved in Staging, you will be able to move to CAS Prod. You will coordinate this with the team that contacts you regarding your CAS request. You will need to modify the code each time to accomodate Dev, Stage or Prod.
- 5. Errors will probably happen. Please refer to the /etc/log file.

#### Maintenance

- From time to time, the CAS SSL cert will have to be renewed. In this case, you must get the new public key cert file and update it in your application. There is a cert for dev and prod. Whichever one is being updated is the one that you will have to request from someone in Networking. Your CAS application may quit working if you do not update the CAS SSL certificate in the /etc folder.
- If the CAS SSL cert has been renewed already, you can manually update it by opening https://cas.uga.edu (or https://cas.dev.uga.edu) in Mozilla Firefox. Click the green lock to open the more information box.



Click the right-pointing arrow and then click the More Information button and you will see a screen similar to this:

•		Page Inf	o - https:	//cas.uga.edu/	cas/login	
		General	Media	Permissions	Security	
Website Ident	iity					
Website: Owner: Verified by:	cas.uga.edu University Of ( GeoTrust Inc.	Georgia				Man Castificate
Privacy & Hist	tory	r to today?		Vec. 18	times	
Have I visited this website prior to today? Is this website storing information (cookies) on my computer?			Yes	umes	View Cookies	
Have I saved	any passwords f	or this websit	e?	No		View Saved Passwords
Technical Det	ails					
Connection	Encrypted (TLS_	RSA_WITH_	AES_128_0	BC_SHA, 128 bit	keys, TLS 1.2)	)
The page you	are viewing was	encrypted be	efore being	transmitted over th	ne Internet.	
Encryption m unlikely that a	akes it difficult fo anyone read this p	r unauthorize bage as it trav	d people to veled acros	view information t s the network.	raveling betwe	en computers. It is therefore

· Under the Security tab click View Certificate. Click the Details tab

Certificate Hiera	rchy	
GeoTrust Print	mary Certification Authority	
GeoTrust	EV SSL CA - G4	
cas.ug	a.edu	
Certificate Fields	S	
cas.uga.edu		
Certificate	3	
Version	n	
Serial N	Number	
Certific	cate Signature Algorithm	
Issuer		
<ul> <li>Validity</li> </ul>		
Not	L Betore	
Field Value	Alter	
Export		
		Olean

• Under the Details tab you will see a button called Export... Click it.

	Save Certificate To File	
Save As:	cas.uga.edu	~
Tags:		
Where:	🛅 Desktop ᅌ	
	Format: X.509 Certificate with 🗘	
	Cancel	Save

- You will see a Format select box at the bottom of the new window. Select X.590 Certificate with chain (PEM). Then click Save.
  You can use the saved certificate to update the one on your server.

# CAS\_PHP\_Simple.zip

## **Related articles**

- EITS reference guide
   CAS Reference Guide
   Request CAS Access
   Download the PHP CAS library from Jasig.org.
- PHP CAS Setup Simple