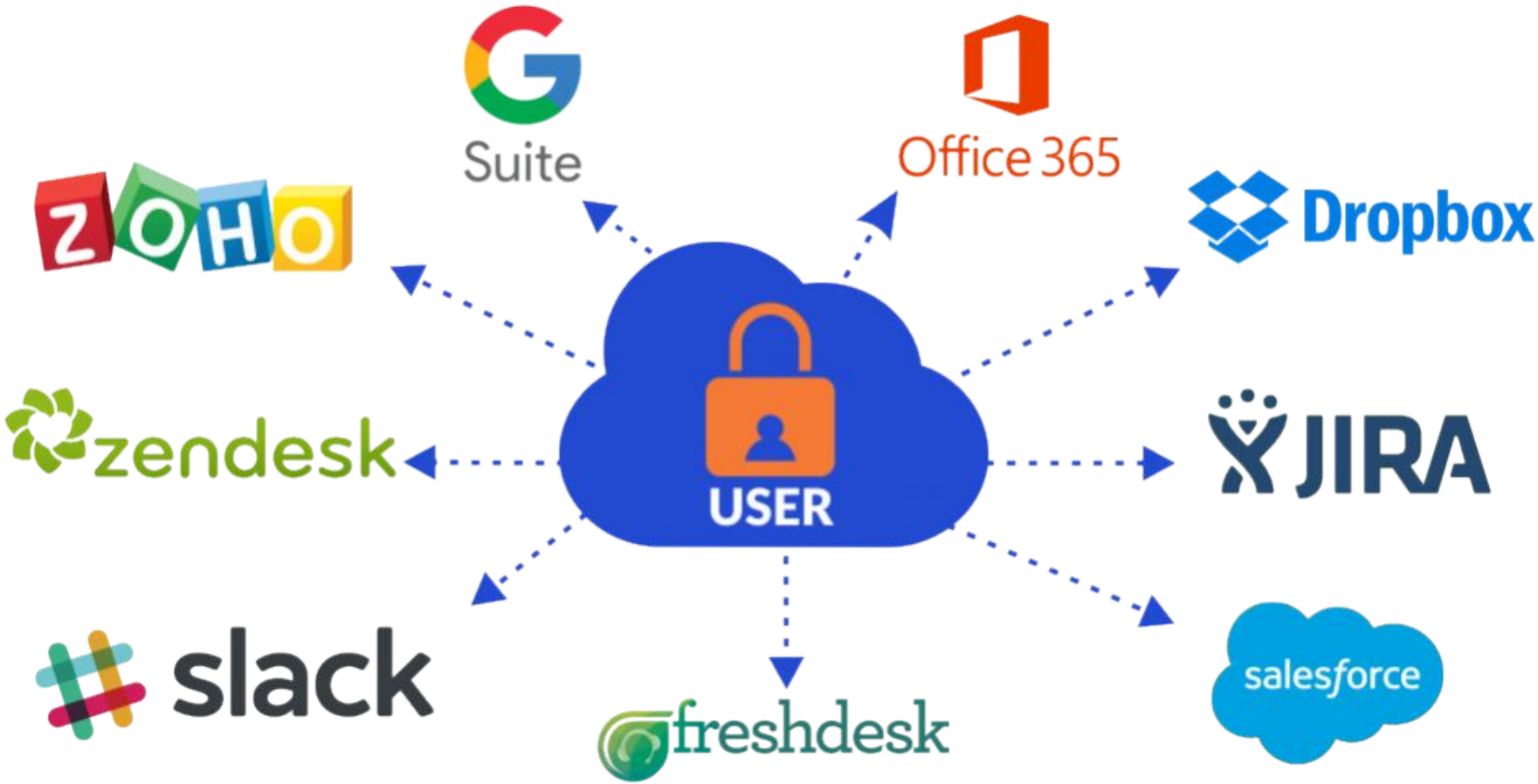
Single Sign On

SimpleSAMLphp

CivicActions | SSO | Dan Gurin | tweeter@dgurin | Drupal.org + GitHub + LinkedIn = DANGUR

Enterprise level user account costs

- Administration
  - Setup
  - Retire
- Support
  - Password resets
- Security
  - Policy
    - Password
    - Multi Factor authentication


Suite
Office 365
ZOHO
Dropbox
zendesk
USER
JIRA
slack
freshdesk
salesforce

Single Sign On (SSO)

- Many applications
- Same
  - Username / password
  - Two Factor Authentication
  - Password policies
    - No unnecessary passwords changes
- Centralized user management
  - Authentication
    - Disable
  - Authorization
    - Roles

Providers

- Identity Provider (idP)
  - Lightweight Directory Access Protocol (LDAP)
  - Centralized Authentication Service (CAS)
- Service Provider (SP)
  - SAML
  - Shibboleth
- Authentication
- Authorization
  - Drupal role(s)
  - Groups

SimpleSAMLphp Service Provider (SP)

- Scenario
  - External authentication system
  - Use Drupal for something other than just authentication
- Installation
  - SimpleSAMLphp Library
  - SimpleSAMLphp Auth Drupal Module

Let’s Get It Started

- PHP
  - php -m | grep 'date\|dom\|hash\|json\|mbstring\|openssl\|pcre\|SPL\|zlib'
- Download
  - https://simplesamlphp.org/download
  - https://simplesamlphp.org/docs/stable/simplesamlphp-install-repo
- Untar or clone to repo root
  - Not web root! ***REPO*** root
  - Untar
    - tar -zxvf simplesamlphp-1.16.2.tar.gz
  - Clone
    - git clone git@github.com:simplesamlphp/simplesamlphp.git repo_root/simplesamlphp

Service Provider/Point (SP)

- Common use case with Drupal
- Drupal does other things than manage users

Copy config and metadata templates

- Copy config from config-templates directory to config directory

```
mkdir config
```

```
cp config-templates/config.php config/config.php
```

```
cp config-templates/authsources.php config/authsources.php
```

- Copy metadata from metadata-templates directory to metadata directory

```
mkdir metadata
```

```
cp metadata-templates/saml20-idp-remote.php metadata/saml20-idp-remote.php
```

Session Store Options

- PHP
  - Default, Built in, Simplest :)
  - Usually does not work in load balanced environments :(
- SQL
  - Data Source Name (DSN) to access PHP Data Objects (PDO)s
  - Tables created automatically, prefix if many SimpleSAML installations using single DB
- Memcache
  - Can load balance and failover on different servers
- Redis
  - Default connection is localhost over port 6379
- Write your own plugin :O

Configure SQL Session Store

config/config.php $config array end under DATA STORE CONFIGURATION

```
‘store.type’ => 'sql',

'store.sql.dsn' => 'mysql:host=database;dbname=mysql',

'store.sql.username' => ‘username’,

'store.sql.password' => ‘password’,
```

Symbolic Links

- Access simplesaml from yoursite.com/simplesaml

```
ln -s web/simplesaml simplesaml/www
```

- Point key folders to composer managed directories
  - Definitely
    - config
    - metadata

```
ln -s simplesamlphp/config vendor/simplesamlphp/simplesamlphp/config
ln -s simplesamlphp/metadata vendor/simplesamlphp/simplesamlphp/metadata
```

  - Call Me Maybe
    - cert
    - log

Let’s Talk About Certs

- SP may sign requests & receive encrypted responses from idP
- Only one current authentication source
  - authX509userCert validate against LDAP userCertificate attribute
- Cert dir
  - simplesaml/cert
- Create cert
  - openssl req -newkey rsa:2048 -new -x509 -days 3652 -nodes -out saml.crt -keyout saml.pem
- Add to authsources.php

```
'default-sp' => array( 'saml:SP', 'privatekey' => 'saml.pem', 'certificate' => 'saml.crt')
```

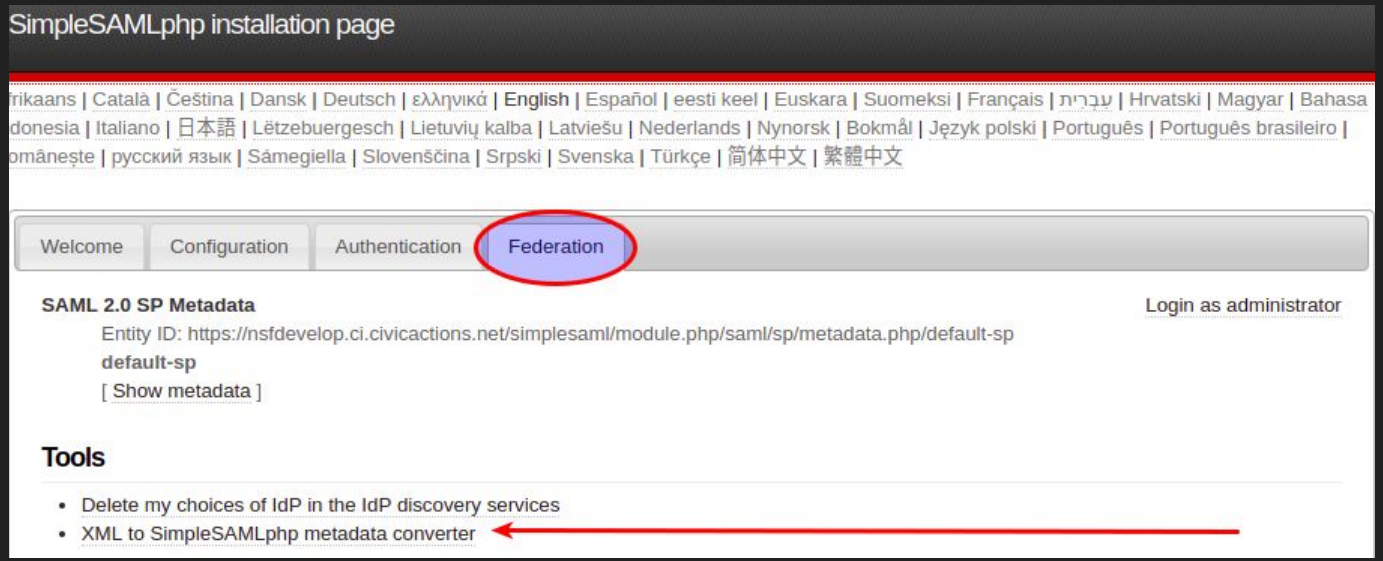
HTTPS

- SSL required
- Free certificates https://letsencrypt.org/
- Base URL Path in $config array
  - simplesaml/config/config.php

```
'baseurlpath' => 'https://your.drupal.site/simplesaml/'
```

Identity Provider (idP) Metadata

- Get metadata XML file from Identity Provider
- Parse XML to SimpleSAMLphp metadata
- Add metadata file to /simplesaml/metadata/saml20-idp-remote.php



Set Default idP

- Prevents from asking each time
- Super annoying if there is only one!

In /simplesaml/config/authsources.php file

Add to $config array:

```
'entityid' => 'https://adfs.your-idp.gov/adfs/services/trust',
```

Logging

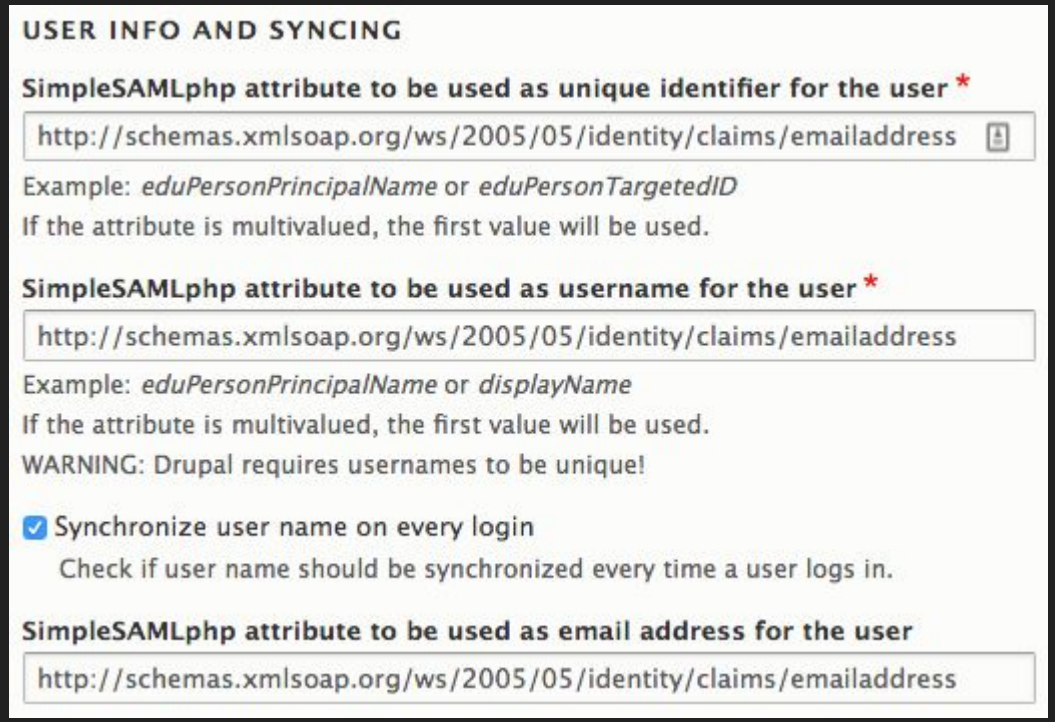
- Levels
  - DEBUG, INFO, NOTICE, WARNING, ERR
- Handlers
  - syslog, file, or errorlog
- /simplesaml/config/config.php $config array

```
'logging.level' => SimpleSAML\Logger::DEBUG,

'logging.handler' => 'file',

'logging.logfile' => 'simplesamlphp.log',
```

idP sets attributes

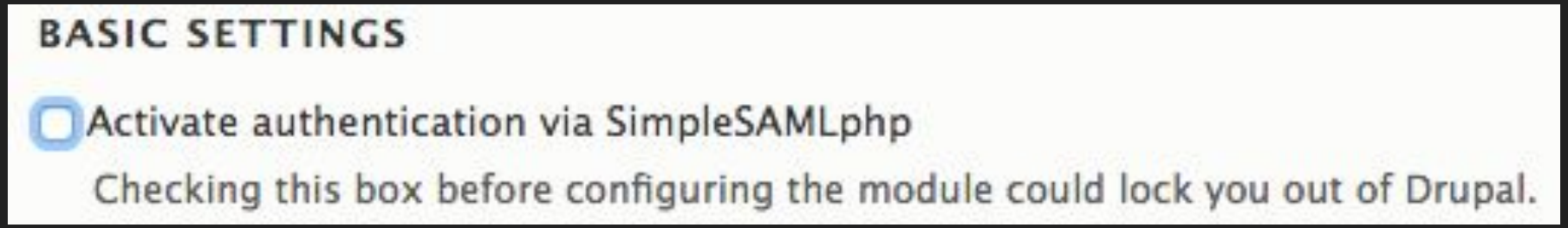
- Unique ID
  - UserPrincipalName
- User
  - Email without the @domain.gov
- Email

Use the full exact name of the attribute



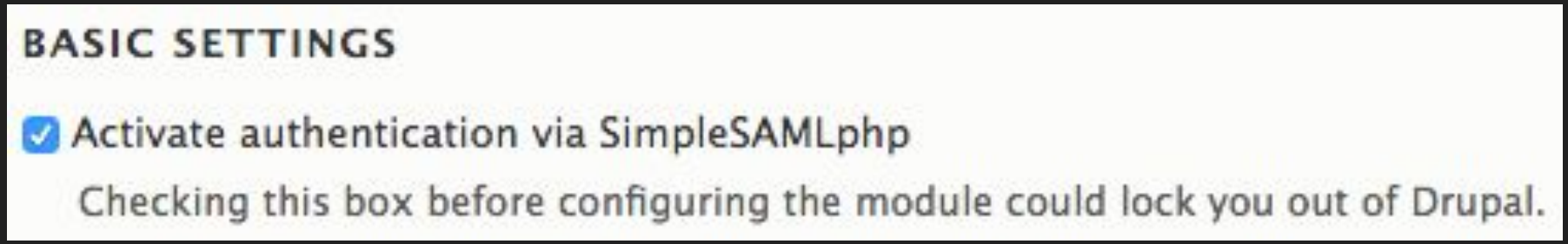
Local dev

- Config Split
- Drush / Drupal Console
- Deactivate
- Disable SimpleSAMLphp Auth module



Activation

- Delete test entities in metadata files
- Install a new certificate if your cert has been exposed
- config.php 'logging.level' => SimpleSAML\Logger::NOTICE,
- simplesamlphp_auth.settings.yml activate: true



Resources

- SimpleSAMLphp homepage
- List of all available SimpleSAMLphp documentation
- Join the SimpleSAMLphp user's mailing list

Free Open Source Symposium

Q & A

CivicActions | SSO | Dan Gurin | tweeter@dgurin | Drupal.org + GitHub + LinkedIn = DANGUR

Thank you!

CivicActions | SSO | Dan Gurin | tweeter@dgurin | Drupal.org + GitHub + LinkedIn = DANGUR