For Your Eyes Only

A guide to secure your YaleSites content

Presenter
Mike Brooks, Project Manager

snp technologies inc.

"*Your friendly, neighborhood Drupal Partner*"

What we'll cover

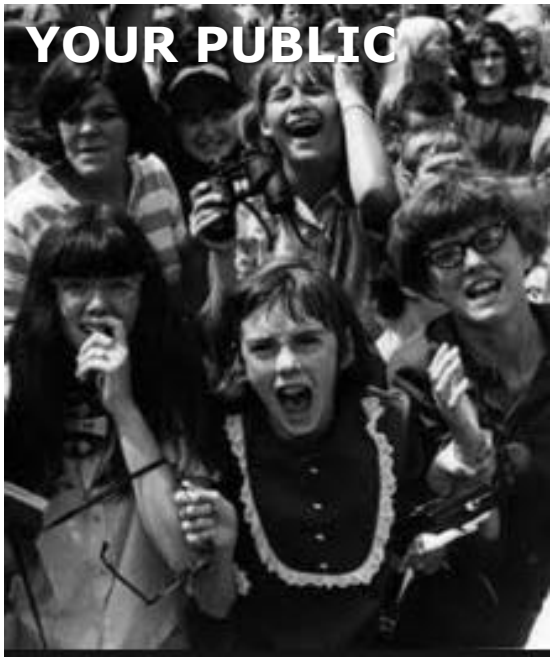
- What is Access Control
- Access Control planning
- Putting it to work in your YaleSite
- Resources

What is Access Control

- Barriers
- Instructions to your visitors
- Underlying Architecture
- Tools

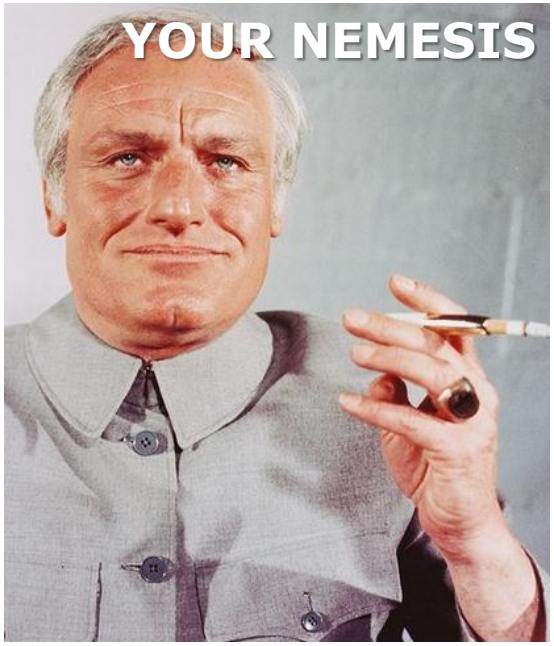

YOUR STAFF


YOUR BOSS


YOUR PUBLIC


YOUR ADMIN


YOUR IT GUY


YOUR NEMESIS

What is Access Control

Concern #1

- My website is public facing, but I also have private content that should be visible **only** to people I approve.

What is Access Control

Concern #2

- I want to give people in my department the ability to manage website content.
- Furthermore, they should be able to manage their content, but not that of others.

What is Access Control

Concern #3

- My contributors should have no administrative rights and not be able compromise the look and feel or security of the site.

What is Access Control

Concern #4

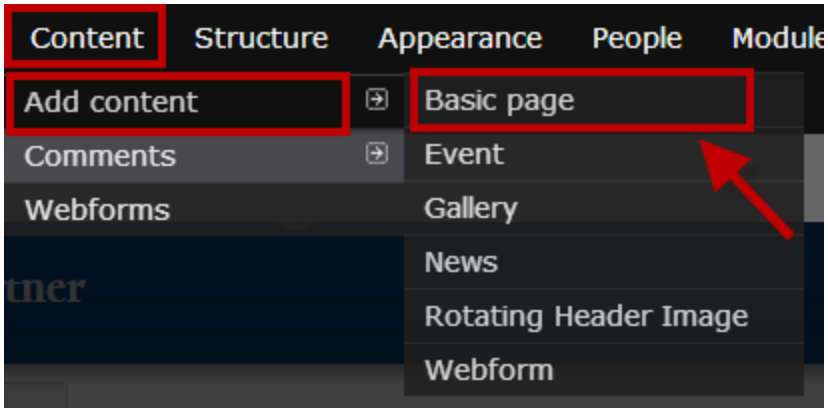
- I want to give people in my department the ability to add and edit content, but not publish. As department head, I want to review and approve content. I need an editorial workflow.

Access Fundamentals

- Content
- Roles
- Users
- Permissions

Access Fundamentals

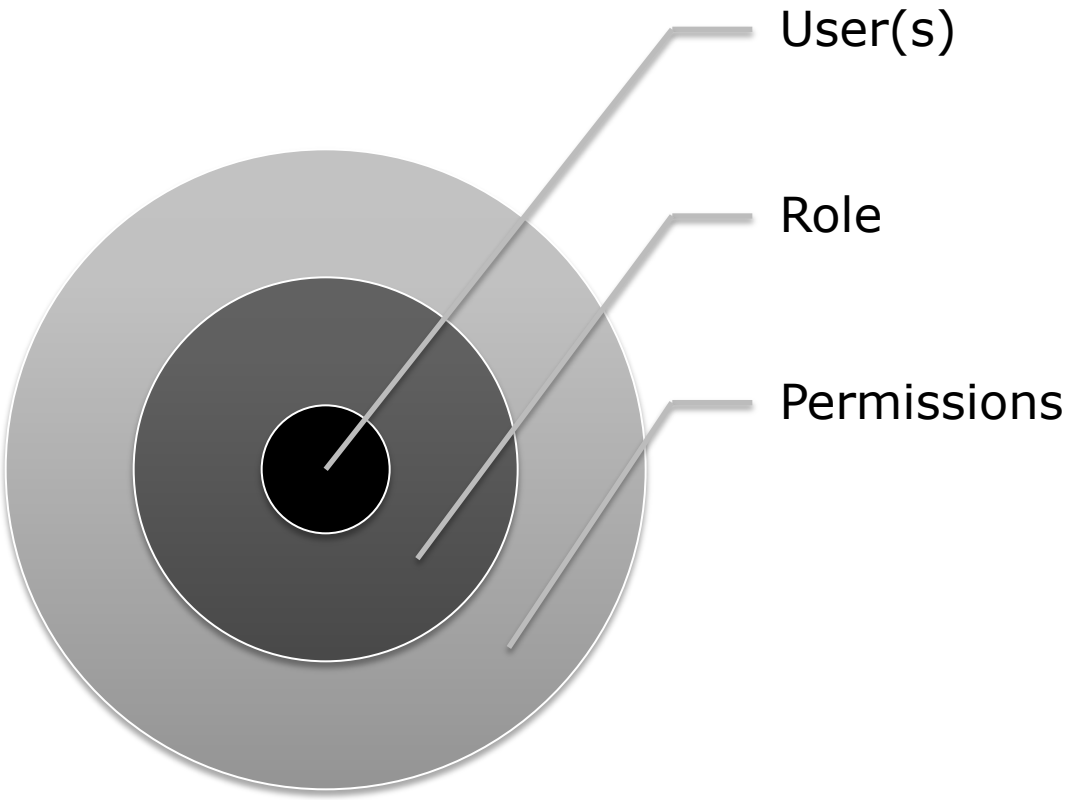
Content



YaleSites: Add pages and content
http://yalesites.yale.edu/book/add-pages-and-content

Lynda.com: Drupal 7 Essential Training
http://www.lynda.com/Drupal-7-tutorials/essential-training/73655-2.html

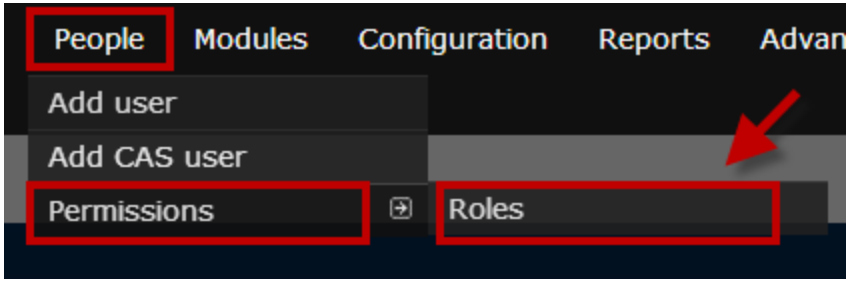
Access Fundamentals



Drupal 7 Essential Training – #10 Managing Users
http://www.lynda.com/Drupal-7-tutorials/essential-training/73655-2.html

Access Fundamentals

Roles

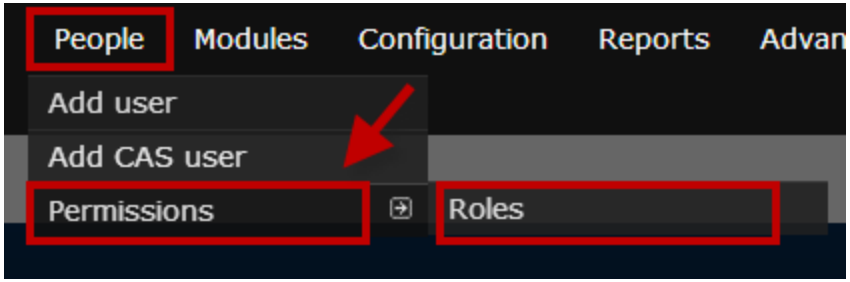


YaleSites: Roles
http://yalesites.yale.edu/book/roles

Drupal 7 Essential Training – #10 Managing Users
http://www.lynda.com/Drupal-7-tutorials/essential-training/73655-2.html

Access Fundamentals

Permissions



YaleSites: Permissions
http://yalesites.yale.edu/book/permissions

Drupal 7 Essential Training – #10 Managing Users
http://www.lynda.com/Drupal-7-tutorials/essential-training/73655-2.html

Access Fundamentals

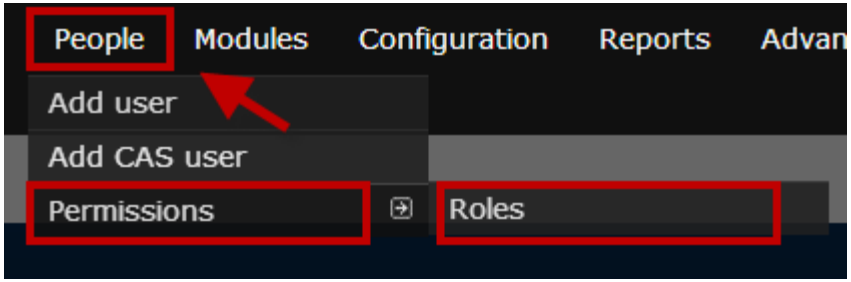
Content Access Matrix - OOTB

		Roles / Permissions				
		Anonymous User	**Authenticated User**	**Admin**	**Editor**	**Site Builder**
Content	**Basic Page**	R	R	CRUD	CRU	CRU
	Event	R	R	CRUD	CRU	CRU
	Gallery	R	R	CRUD	CRU	CRU
	News	R	R	CRUD	CRU	CRU
	Rotation Header Image	R	R	CRUD	CRU	CRU
	Webform	R	R	CRUD	CRU	CRU

C	Create
R	Read
U	Update
D	Delete

Access Fundamentals

Users

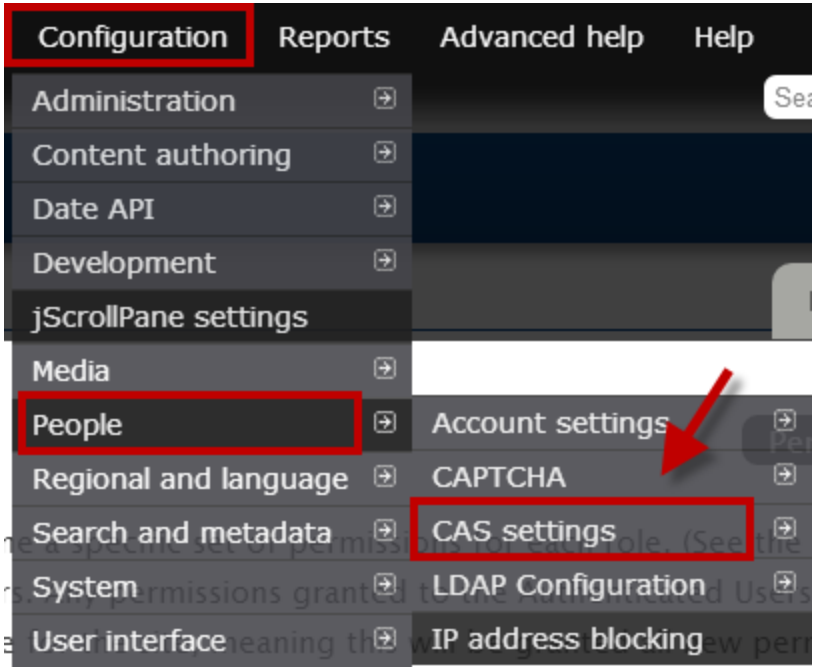


YaleSites: Adding People
http://yalesites.yale.edu/book/adding-people

Drupal 7 Essential Training – #10 Managing Users
http://www.lynda.com/Drupal-7-tutorials/essential-training/73655-2.html

Access Fundamentals

CAS Settings



YaleSites: Adding People
http://yalesites.yale.edu/book/adding-people

Access Fundamentals

Login

- Out of the box…
  - No login form or link
  - Login via [your domain]/cas
  - Anyone that logs in with a NetID is assigned the authenticated user role.
  - When you log in for the first time, contact OPAC to be granted admin rights, if not already an admin.

Access Fundamentals

Login Customizations

- Add Login Block
- Add Login Link, i.e. /user
- Configure CAS Redirection
- Configure CAS Role Mapping
- Configure CAS login & logout Destinations

Access Fundamentals

Drupal File System

- Configuration » Media » File System
- Public Files vs. Private Files

Files in the public directory can be accessed directly through the web server; when public files are listed, direct links to the files are used and anyone who knows a file's URL can download the file.

Files in the private directory are not accessible directly through the web server; when private files are listed, the links are Drupal path requests.

http://drupal.org/documentation/modules/file

http://yalesites.yale.edu/book/restrict-access-uploaded-files

Access Control Planning

Our YaleSite Example

- Crews Lab research group http://crewslab.yale.edu/

Access Control Planning

Content Access Matrix - Crews Lab

		Roles			
		Anonymous	**Admin**	**Editor**	**Members**
Content	**Home page**	R	CRUD	CRUD	R
	Research	R	CRUD	CRUD	R
	Projects	R	CRUD	CRUD	R
	People	R	CRUD	CRUD	R
	Publications	R	CRUD	CRUD	R
	Group News	R	CRUD	CRUD	R
	Links	R	CRUD	CRUD	R
	Intranet		CRUD	CRUD	R
	Progress Report		CRUD	CRUD	R
	Contact Us	R	CRUD	CRUD	R

C	Create
R	Read
U	Update
D	Delete

Access Control Planning

Concern #1 (remember me?)

- My website is public facing, but I also have private content that should be visible **only** to people I approve.

  *Intranet and Progress Report should be visible to Member, Admin and Editor roles **only**.*

Concern #1 Solved

Step 1 – Create a new Role for users that need read (view) access to the private content.

Follow the admin menu path:
People » Permissions » Roles

Below the lists of roles, enter the name of your new role (“Member” in our example) and click the Add role button.

Concern #1 Solved

Step 2 – Edit permissions for the new role

Click the edit permissions link to the right of the new role.

In the Permissions list, locate View published content and verify that it is checked.

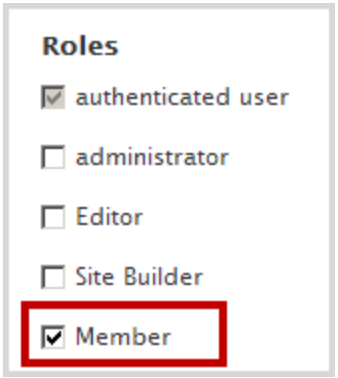
Concern #1 Solved

Step 3 - Add users to the new role

Click People in the admin menu to open the People overlay.

In the OPERATIONS column, click edit for each user.

On the Roles section, check the new role (Member in our example).



Concern #1 Solved

Step 4 - Enable the Content Access Module

Click Modules in the admin menu to open the Modules overlay.

Scroll down to the ACCESS CONTROL section and enable the Content Access module.

You will be prompted to Rebuild Permissions. Proceed with this step.

Concern #1 Solved

Step 5 – Configure Private Files

Follow the admin menu path:
Configuration » Media » File system

In the Private files system path text box, enter: sites/default/files/private

Concern #1 Solved

Step 6 – Edit your Content type

Follow the admin menu path to the Access Control tab of the Content type you want to be private:

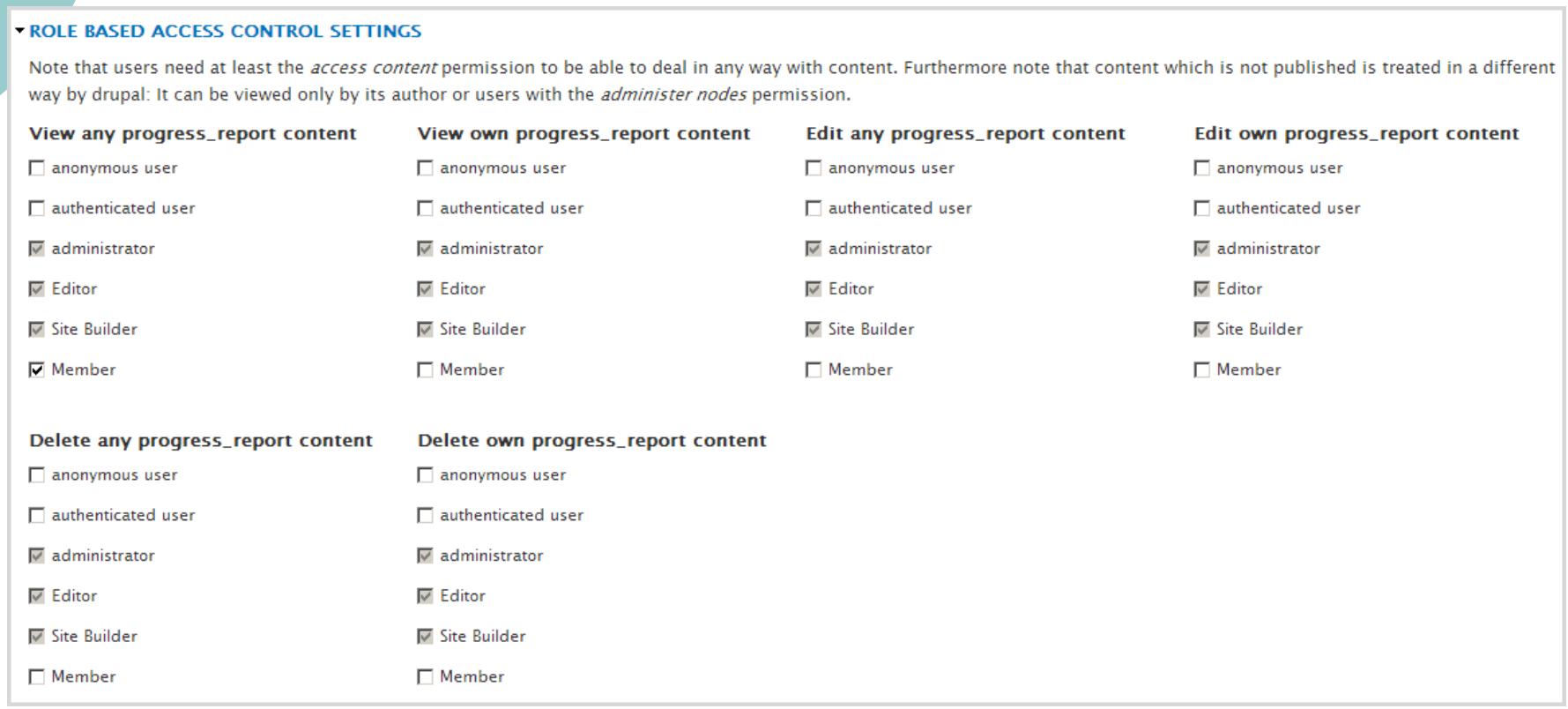
Structure » Content types » [My Content type] » Access control

Under ROLE BASED ACCESS CONTROL SETTINGS Uncheck the anonymous user and authenticated user for all permission levels. Put a check in the View any [type] content for the role that should have access.

Concern #1 Solved

Step 6 – Edit your Content type

In our example, the setting are:



ROLE BASED ACCESS CONTROL SETTINGS

Note that users need at least the *access content* permission to be able to deal in any way with content. Furthermore note that content which is not published is treated in a different way by drupal: It can be viewed only by its author or users with the *administer nodes* permission.

View any progress_report content	View own progress_report content	Edit any progress_report content	Edit own progress_report content
☐ anonymous user	☐ anonymous user	☐ anonymous user	☐ anonymous user
☐ authenticated user	☐ authenticated user	☐ authenticated user	☐ authenticated user
☑ administrator	☑ administrator	☑ administrator	☑ administrator
☑ Editor	☑ Editor	☑ Editor	☑ Editor
☑ Site Builder	☑ Site Builder	☑ Site Builder	☑ Site Builder
☑ Member	☐ Member	☐ Member	☐ Member

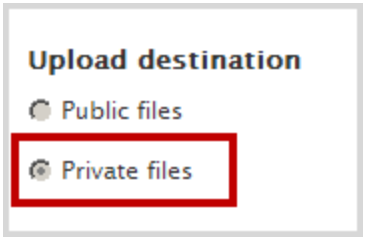
Delete any progress_report content	Delete own progress_report content
☐ anonymous user	☐ anonymous user
☐ authenticated user	☐ authenticated user
☑ administrator	☑ administrator
☑ Editor	☑ Editor
☑ Site Builder	☑ Site Builder
☐ Member	☐ Member

Concern #1 Solved

Step 7 – Set Upload destination to Private files

This step is only necessary if your content type has File fields.

Edit each File field in your content type. Scroll to the Upload destination section at the bottom of the Field overlay and select Private files.



Concern #1 Solved

Add content and Test!

Other Access Control Tools

- CAS Redirection
  - Configuration » People » CAS Settings
- Custom Access Denied Page
  - Configuration » System » Site information
- Field Permissions Module
  - Modules - FIELDS - Field Permissions
    - When enabled, you see Field visibility and permissions in the bottom of the Field Settings page of the content type.

Other Access Control Tools

- Text formats
  - Configuration » Content authoring » Text formats
  - Out-of-the-box:

NAME	ROLES
Filtered HTML	administrator, Editor, Site Builder
Full HTML	administrator, Editor, Site Builder
Plain text	*All roles may use this format*
PHP code	administrator
Display Suite code	administrator, Site Builder

Other Access Control Tools

- Comment settings
- Workbench
  - For editorial workflow
  - Can be used for access control with respect to edit rights.
    - Restricts access to a section by Taxonomy **OR** Menus site wide.
  - Does not control view access

http://yalesites.yale.edu/module-tutorials/workbench

Discussion

Contact

Mike Brooks, Project Manager
(203) 287-9114 x114
mike@snp.com
www.linkedin.com/in/mikesnp
mikesnp on drupal.org

snp technologies inc.

2321 Whitney Avenue, Suite 401A
Hamden, CT 06518
www.snp.com
www.facebook.com/SNPtechnologies