Administrator Reference Guide for OU Campus v10

Long, Support Site Version
About OmniUpdate, Inc.
OmniUpdate® is the leading web content management system (CMS) provider for higher education. The company focuses on providing an exceptional product and customer experience to its OU Campus™ CMS users who manage more than 700 web and mobile sites in the U.S. and around the world. OU Campus is secure and scalable, server and platform independent, and seamlessly integrates with other enterprise campus systems. It provides college and university web developers, administrators, and marketers with the user-friendly tools and deployment flexibility they need to achieve excellence. For more information, visit.

About This Guide
The Administrators Reference Guide provides a list of the commonly used functionality for administrators of the OU Campus CMS. It includes overview topics and step-by-step procedures related to the configurations at the account and site level. The intended audience is administrators of OU Campus. End users of the system may find more detailed content regarding the basic use of OU Campus in the End-User Reference Guide and the Support site.

OU Campus Support
The Support site is available to everyone and users are encouraged to visit and browse the site for information. An institution's administrators are also available if the answer cannot be found on the Support site or further explanation and clarification is needed. Administrators may contact the OmniUpdate Support Team. Ways to access the OU Campus support documentation include:

• Support site: http://support.omniupdate.com/
• The help link in the main interface of OU Campus
• The WYSIWYG Help link
• Help links embedded in the system
• Text instructions are provide onscreen for specific fields and functionality
• OmniUpdate Community Network (OCN): http://ocn.omniupdate.com/

Conventions
Shorthand for navigation through the OU Campus CMS is indicated with a greater-than sign and bolded: > For example, Setup > Sites. Code snippets use Courier New and a shaded background.
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>With Binary Management</td>
<td>103</td>
</tr>
<tr>
<td>Example of a Dependency Tag in WYSIWYG</td>
<td>104</td>
</tr>
<tr>
<td>Examples of Dependency Tags in Source Editor</td>
<td>104</td>
</tr>
<tr>
<td>More About Links and Linking</td>
<td>104</td>
</tr>
<tr>
<td>Among Sites</td>
<td>105</td>
</tr>
<tr>
<td>When Publishing</td>
<td>105</td>
</tr>
<tr>
<td>Publish Threshold</td>
<td>105</td>
</tr>
<tr>
<td>About Unpublished Dependencies</td>
<td>105</td>
</tr>
<tr>
<td>S-Tag and Triggered Publish</td>
<td>105</td>
</tr>
<tr>
<td>Renaming or Moving a Directory or File</td>
<td>105</td>
</tr>
<tr>
<td>About HTTP Root</td>
<td>106</td>
</tr>
<tr>
<td>File Types</td>
<td>106</td>
</tr>
<tr>
<td>Dependencies Reporting</td>
<td>106</td>
</tr>
<tr>
<td>Broken Links</td>
<td>106</td>
</tr>
<tr>
<td>With Recycle</td>
<td>107</td>
</tr>
<tr>
<td>With Source Editor</td>
<td>107</td>
</tr>
<tr>
<td>Within the WYSIWYG Editor</td>
<td>107</td>
</tr>
<tr>
<td>Additional Scenarios and Considerations</td>
<td>108</td>
</tr>
<tr>
<td>Important Information and Reminders</td>
<td>108</td>
</tr>
<tr>
<td>Final Notes</td>
<td>110</td>
</tr>
<tr>
<td>Binary Management</td>
<td>111</td>
</tr>
<tr>
<td>Overview</td>
<td>111</td>
</tr>
<tr>
<td>About File Choosers and Binary Management</td>
<td>111</td>
</tr>
<tr>
<td>Sites</td>
<td>112</td>
</tr>
<tr>
<td>Overview</td>
<td>112</td>
</tr>
<tr>
<td>Sites List View</td>
<td>112</td>
</tr>
<tr>
<td>Creating a New Site</td>
<td>113</td>
</tr>
<tr>
<td>Options Menu and Site Actions</td>
<td>113</td>
</tr>
<tr>
<td>Edit Menu</td>
<td>113</td>
</tr>
<tr>
<td>Publish Menu</td>
<td>113</td>
</tr>
<tr>
<td>Scan Menu</td>
<td>113</td>
</tr>
<tr>
<td>Actions</td>
<td>113</td>
</tr>
<tr>
<td>Site Actions</td>
<td>115</td>
</tr>
<tr>
<td>Overview</td>
<td>115</td>
</tr>
<tr>
<td>Edit Menu</td>
<td>115</td>
</tr>
<tr>
<td>Scan Menu</td>
<td>117</td>
</tr>
<tr>
<td>Publish Menu</td>
<td>118</td>
</tr>
<tr>
<td>Actions Menu</td>
<td>119</td>
</tr>
<tr>
<td>Revert</td>
<td>122</td>
</tr>
<tr>
<td>Revert Scan</td>
<td>122</td>
</tr>
<tr>
<td>Publish Sitemap.xml</td>
<td>123</td>
</tr>
<tr>
<td>Overview</td>
<td>123</td>
</tr>
<tr>
<td>Generating a Site Map</td>
<td>123</td>
</tr>
<tr>
<td>Excluding Files, Directories, and Assets</td>
<td>123</td>
</tr>
<tr>
<td>Clone</td>
<td>125</td>
</tr>
<tr>
<td>Overview</td>
<td>125</td>
</tr>
<tr>
<td>Copy Staging Files</td>
<td>125</td>
</tr>
<tr>
<td>Cloning a Site Record and Files</td>
<td>128</td>
</tr>
<tr>
<td>Additional Steps to Go Live</td>
<td>129</td>
</tr>
<tr>
<td>More About Dependency Manager and Site Clone</td>
<td>130</td>
</tr>
<tr>
<td>Use Case Examples for Dependency Manager Settings</td>
<td>130</td>
</tr>
<tr>
<td>Use Case Examples for Site Settings</td>
<td>133</td>
</tr>
<tr>
<td>Example 1</td>
<td>133</td>
</tr>
<tr>
<td>Example 2</td>
<td>134</td>
</tr>
<tr>
<td>Best Practices</td>
<td>134</td>
</tr>
<tr>
<td>Site Information</td>
<td>135</td>
</tr>
<tr>
<td>Overview</td>
<td>135</td>
</tr>
<tr>
<td>Site Name</td>
<td>135</td>
</tr>
<tr>
<td>UUID</td>
<td>135</td>
</tr>
<tr>
<td>Public Key</td>
<td>135</td>
</tr>
<tr>
<td>Generate Button</td>
<td>136</td>
</tr>
<tr>
<td>Production Server FTP Settings</td>
<td>137</td>
</tr>
<tr>
<td>Production Server FTP Settings Overview</td>
<td>137</td>
</tr>
<tr>
<td>Settings Reference</td>
<td>138</td>
</tr>
<tr>
<td>Server</td>
<td>138</td>
</tr>
<tr>
<td>FTP Type</td>
<td>139</td>
</tr>
<tr>
<td>Username</td>
<td>139</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>139</td>
</tr>
<tr>
<td>Password</td>
<td>139</td>
</tr>
<tr>
<td>Show Password</td>
<td>139</td>
</tr>
<tr>
<td>Test Connection</td>
<td>139</td>
</tr>
<tr>
<td>UMask</td>
<td>139</td>
</tr>
<tr>
<td>FTP Root</td>
<td>140</td>
</tr>
<tr>
<td>FTP Home</td>
<td>141</td>
</tr>
<tr>
<td>HTTP Root</td>
<td>142</td>
</tr>
<tr>
<td>Image Directory</td>
<td>142</td>
</tr>
<tr>
<td>Template Location</td>
<td>142</td>
</tr>
<tr>
<td>Template Directory</td>
<td>142</td>
</tr>
<tr>
<td>Available To</td>
<td>143</td>
</tr>
<tr>
<td>More About Sites, Staging, and Production</td>
<td>143</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Preferences</td>
<td>205</td>
</tr>
<tr>
<td>Overview</td>
<td>205</td>
</tr>
<tr>
<td>LDAP Configuration</td>
<td>207</td>
</tr>
<tr>
<td>LDAP Configuration Overview</td>
<td>207</td>
</tr>
<tr>
<td>New User Options</td>
<td>209</td>
</tr>
<tr>
<td>New User Options Overview</td>
<td>209</td>
</tr>
<tr>
<td>Setup Toolbars</td>
<td>211</td>
</tr>
<tr>
<td>Overview</td>
<td>211</td>
</tr>
<tr>
<td>Creating a New Toolbar</td>
<td>212</td>
</tr>
<tr>
<td>Naming Convention for Group Creation and Editing</td>
<td>212</td>
</tr>
<tr>
<td>Paste Options</td>
<td>215</td>
</tr>
<tr>
<td>Editing a Toolbar</td>
<td>215</td>
</tr>
<tr>
<td>Deleting a Toolbar</td>
<td>215</td>
</tr>
<tr>
<td>Assigning a Toolbar</td>
<td>216</td>
</tr>
<tr>
<td>Assigning a Toolbar to a User</td>
<td>216</td>
</tr>
<tr>
<td>Assigning a Toolbar to a Site or Directory</td>
<td>216</td>
</tr>
<tr>
<td>Assigning a Toolbar to a Page</td>
<td>217</td>
</tr>
<tr>
<td>Assigning a Toolbar to an Editable Region</td>
<td>217</td>
</tr>
<tr>
<td>Font Size Sets</td>
<td>219</td>
</tr>
<tr>
<td>Overview</td>
<td>219</td>
</tr>
<tr>
<td>Adding a New Font Size Set</td>
<td>220</td>
</tr>
<tr>
<td>Assigning a Font Size Set to a Toolbar</td>
<td>221</td>
</tr>
<tr>
<td>Gadgets</td>
<td>223</td>
</tr>
<tr>
<td>Overview</td>
<td>223</td>
</tr>
<tr>
<td>System Gadgets Reference</td>
<td>224</td>
</tr>
<tr>
<td>Templates</td>
<td>229</td>
</tr>
<tr>
<td>Template Options Overview</td>
<td>230</td>
</tr>
<tr>
<td>Template Groups</td>
<td>230</td>
</tr>
<tr>
<td>Template Files</td>
<td>230</td>
</tr>
<tr>
<td>Template Options</td>
<td>231</td>
</tr>
<tr>
<td>Template Options Overview</td>
<td>231</td>
</tr>
<tr>
<td>Template Files Location</td>
<td>231</td>
</tr>
<tr>
<td>Templates Access Settings</td>
<td>232</td>
</tr>
<tr>
<td>Template Options Panel</td>
<td>232</td>
</tr>
<tr>
<td>Configuring the Title for a Template</td>
<td>233</td>
</tr>
<tr>
<td>Assigning Access to a Template</td>
<td>234</td>
</tr>
<tr>
<td>Defining a Thumbnail Image for a Template</td>
<td>234</td>
</tr>
<tr>
<td>Facebook</td>
<td>236</td>
</tr>
<tr>
<td>Overview</td>
<td>236</td>
</tr>
<tr>
<td>Facebook Account vs. Facebook Page</td>
<td>236</td>
</tr>
<tr>
<td>Creating a Facebook Page in Facebook</td>
<td>236</td>
</tr>
<tr>
<td>Setting up OU Social</td>
<td>244</td>
</tr>
<tr>
<td>OU Social Overview</td>
<td>244</td>
</tr>
<tr>
<td>Configuring XSL and PCF</td>
<td>244</td>
</tr>
<tr>
<td>Required Styling for Welcome URL Landing Page</td>
<td>244</td>
</tr>
<tr>
<td>Best Practices</td>
<td>245</td>
</tr>
<tr>
<td>Additional Resources</td>
<td>245</td>
</tr>
<tr>
<td>Setup Twitter</td>
<td>246</td>
</tr>
<tr>
<td>Overview</td>
<td>246</td>
</tr>
<tr>
<td>Setting up a Twitter Account</td>
<td>246</td>
</tr>
<tr>
<td>Modifying Twitter Account Options</td>
<td>249</td>
</tr>
<tr>
<td>Deleting a Twitter Account</td>
<td>250</td>
</tr>
<tr>
<td>Adding Default Text for Twitter</td>
<td>250</td>
</tr>
<tr>
<td>Default Text at the Account Level</td>
<td>250</td>
</tr>
<tr>
<td>Default Text at the Site Level</td>
<td>251</td>
</tr>
<tr>
<td>Best Practices</td>
<td>252</td>
</tr>
<tr>
<td>RSS</td>
<td>253</td>
</tr>
<tr>
<td>Overview</td>
<td>253</td>
</tr>
<tr>
<td>RSS With and Without a Feed Reader</td>
<td>253</td>
</tr>
<tr>
<td>RSS in OU Campus</td>
<td>255</td>
</tr>
<tr>
<td>Media RSS</td>
<td>255</td>
</tr>
<tr>
<td>RSS Feeds</td>
<td>257</td>
</tr>
<tr>
<td>Overview</td>
<td>257</td>
</tr>
<tr>
<td>Creating a New RSS Feed</td>
<td>258</td>
</tr>
<tr>
<td>Editing RSS Feeds</td>
<td>260</td>
</tr>
<tr>
<td>Publishing RSS Feeds</td>
<td>260</td>
</tr>
<tr>
<td>Deleting RSS Feeds</td>
<td>261</td>
</tr>
<tr>
<td>Apply an RSS Feed to a Page or Directory</td>
<td>261</td>
</tr>
<tr>
<td>Final Notes</td>
<td>262</td>
</tr>
<tr>
<td>RSS Feed Groups</td>
<td>263</td>
</tr>
<tr>
<td>Overview</td>
<td>263</td>
</tr>
<tr>
<td>Creating a New RSS Group</td>
<td>263</td>
</tr>
<tr>
<td>Adding Members to a Group</td>
<td>266</td>
</tr>
<tr>
<td>Editing an Aggregate Feed</td>
<td>266</td>
</tr>
<tr>
<td>Access Settings</td>
<td>267</td>
</tr>
<tr>
<td>Overview</td>
<td>267</td>
</tr>
</tbody>
</table>
Access Settings and Workflow .................................. 268
Inheritance and Precedence .................................... 268
   Inheritance ................................................... 268
   Precedence .................................................. 269
Permissions for Access Settings ............................. 270

Planning Access .............................................. 272
Planning Access Overview .................................. 272
Planning Groups .............................................. 272
Planning Access to Directories and Files ............... 272
Reassigning Access at the File Level .................... 272
Planning Editable Regions .................................. 272
Example .......................................................... 273

Workflow .......................................................... 274
Overview ......................................................... 274
Approvers ....................................................... 275
   Enforcing an Approver .................................... 275
   Bypassing the Approver ................................... 276
   Level 0 ......................................................... 276

Using Reports for Setting Up Workflow ............... 277
   Prior to Settings Assignment .......................... 277
   After Setting Access ..................................... 277

Page Access Settings ........................................ 278
Overview ......................................................... 278
Assigning Access to a Page ................................ 278
   Access From Preview/Edit Mode ....................... 279

Directory Access Settings .................................. 281
Overview ......................................................... 281
Assigning Access to a Directory .......................... 281

Site Access Settings ......................................... 283
Overview ......................................................... 283
Assigning Access at the Site Level ....................... 283
   Example of the Access Settings for the Site ..... 284

Directory Variables .......................................... 286
Overview ......................................................... 286
Creating New Directory Variables ....................... 287
   Creating Image or Media Directory Variables ...... 287
   Using a Directory Variable to Skip File Types on Publish .... 287
   Creating a User-Defined Directory Variable .. 288
   Overriding Directory Variables for a Subdirectory .... 288

Best Practices .................................................. 288

Editable Regions in a PCF .................................. 289
Overview ......................................................... 289
Administrator Introduction

The OU Campus administrators include Level 9 Assistant Administrators and Level 10 Administrators. While both levels have the ability to access all content areas within sites of an account, the extent of their ability to access the CMS differs.

A Level 9 administrator has the ability to navigate anywhere within sites. They have access to reports, as well as the ability to check back in pages and assets that users may have inadvertently left checked out to themselves. A Level 9 administrator can also set the access settings to any group defined in the system on directories, pages, and assets.

Level 10 Administrators are users without restrictions. Not only are they able to navigate to any page within any site, they can also publish pages and assets without any restrictions. Like Level 9, Level 10 has access to reports and the ability to check back in pages and assets checked out by other users (including other administrators). They also have the ability to set the access settings for directories, pages, and assets. They have the ability to set additional restrictions and customization, such as approvers, custom toolbars, file type restrictions, and directory variables. A Level 10 is also able to maintain account and site settings, add or delete users, create groups, custom toolbars, set up RSS feeds, make snippet assignments, manage template assignments, and create associations to Twitter, Facebook, and blogs.

This guide is a general reference for administrators. It is not an all-inclusive manual of the functionality included in the OU Campus system.

OU Campus Support

Online support is available through the OmniUpdate Support site at:

http://support.omniupdate.com/oucampus10/

The Support site, which is accessible by everyone in its entirety, includes user support on all the features in OU Campus, as well as video and text tutorials, archived Training Tuesdays, which are the free monthly webinars offered the last Tuesday of every month unless otherwise announced at 11:00 AM PST, and access to the Permissions Chart.

The Support site can be accessed through the Help link in the upper, right-hand corner of OU Campus. Additionally, support can be gained using the contextual help links found within OU Campus. Throughout the site the in-context help links are available and are specific to the area or task at hand. These links open the relevant page at the Support site.

Finally, contextual help may also be found within the CMS as instructions relating to particular fields.
The Support site is available to everyone. Users are encouraged to visit and search the Support site. The institution’s administrators are also available if the answer cannot be found on the Support site or further explanation and clarification is needed. Administrators may contact the OmniUpdate Support Team.

**Getting Started**

Below are links that will be helpful to those using OU Campus for the first time.

- Logging In
- Interface
- Global Navigation

From there one can navigate to any page on the support site detailing how to use the various features of OU Campus. The following links are for all the functions that administrator-level users can access from their global navigation bar.

- Dashboard
  - Workflow
  - Inbox
- Content
  - Assets
  - Snippets (levels 9 and 10 only)
  - RSS (level 10 only)
  - Find and Replace (level 10 only)
  - Recycle Bin
- Reports
  - Required Actions
  - Checked-Out Content
  - Pending Approvals
  - Scheduled Actions
  - Site Check (levels 9 and 10 only)
  - Custom Reports (levels 9 and 10 only)
  - Recent Saves
  - Recent Publishes
- Add-Ons
  - Marketplace
- Setup (level 10 only)
Filter

Overview

The filter tool is one of the most common utilities within OU Campus. It is available on many of the OU Campus screens that provide a view of content within the system.

For example, the Filter tool is available on the Pages and Assets list views, all reports, filechoosers, and many others. The Filter tool allows the content in a list view to be delimited by the string typed into the Filter field. The filter applies to specific columns available on the screen.

For example, the Pages list view includes a Name column, a Modified column, and others. In this case, the filter applies to the Name column. Typing `.inc` shows the files with the extension of `.inc` as well as any files with that have `.inc` within the file name.

Filtering in the Pages List View

The string that was entered can be quickly deleted by clicking the Delete icon on the right side of the Filter field.

Filtering and Selecting All

When the list view is filtered and the select all checkbox is used, then only the filtered results are selected. Manually filtered and individually selected results (by checkbox) are also persistent when navigating by pagination.

Filter Tool in Asset Manager

The Filter tool in the Assets list view allows users to delimit the Assets list view. Users can filter by asset type, the site in which the asset was originally created, and by commonly-occurring asset tags. Users can also simply type in a text string in the Filter bar. For more information about managing assets in the Asset Manager, visit the Asset Management page.
Assets (8)

Asset Types
- Web Content (1)
- Source Code (4)
- Image Gallery (3)

Sites
- GallenaUniversity (6)

Asset Tags
- Home - Image Slider (1)
- Blog - Featured Blog Post List (1)
- description (1)

University Description

{a:17642}
Quick Search

Overview

Quick Search is a tool that searches the content of pages within the Pages list view (found at Content > Pages). Quick Search does not search the source code of a page, but will search the text, metadata, and file names of files. Assets themselves are not searched, but the text of an asset that is included on a subscribing page is searched.

The Quick Search field in the Pages list view acts in a similar fashion as the Filter tool; when first entering text, the Pages list view will begin to be filtered. However, pressing enter after entering text in the Quick Search field will initiate a full-site content search. The full-site content search can also be initiated by entering text and then selecting Search Entire Site from the drop-down menu.

The entire site can be searched and advanced search options are also available. To perform a search, type a string into the search box and press Enter or click Search Entire Site. Additionally, Advanced Search allows users to further define search criteria based on page title, meta data, and limit search results based on access or current position in the folder structure.

If a user would like to make a global modification involving finding and replacing content, or would like to search source code, the global Find and Replace tool, available to Level 10 administrators, is a better option, as Quick Search is not suitable for code or regex searches. For more information on the Find and Replace tool, visit the Find and Replace page.

Administrators have the ability, through Access Settings, to choose which files or folders to exclude from Quick Search indexing.

Using Quick Search

1. From any directory within the Pages list view, enter the text to be searched for.
2. Press Enter to start the search.
3. To clear the search term, press the Delete icon.

Advanced Search

The Advanced Search option includes specific delimiters and Boolean options that may be used. These include Content, Path, Title, Description, Keywords, and Other Meta. The search parameters may also be used to limit access to the current folder level and below and to the current user.

By utilizing the Advanced Search option, it is possible to easily incorporate multiple criteria into the search without having to know the syntax, as well as to limit the search locations.
Advanced Search Fields

- **Content**: This searches the actual page content.
- **Path**: Define the path where the expected content is to be found. A wildcard can be used to search folders within the defined path.
- **Title**: This searches the meta tags for the page titles.
- **Keywords**: This searches the meta tags for pages’ keywords and phrases.
- **Description**: This searches the meta tags for the pages’ descriptions.
- **Metadata**: If other meta information is defined on pages being searched, this searches in those meta tags.

Scope

- **Limit Search To Current Folder and Subfolders**: This excludes any folders above the folder in which the user is currently located.
- **Only Pages I Can Access**: This limits the search to any pages that are accessible to the user.
Search Results

Search results in all cases are displayed when search is completed. The Search Results list view includes:

- The number search results found
- The content searched for
- The ability to export search results to a CSV file
- Filter search results
- Sortable columns

<table>
<thead>
<tr>
<th>Path</th>
<th>Last Saved</th>
<th>Relevancy</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>../resources/includes/emergency-notification.pcf</td>
<td>7/13/2015 12:15 PM</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>../resources/includes/footer/contact.inc</td>
<td>7/13/2015 12:15 PM</td>
<td>86%</td>
<td></td>
</tr>
<tr>
<td>../resources/includes/email/footer.pcf</td>
<td>7/13/2015 12:15 PM</td>
<td>71%</td>
<td></td>
</tr>
<tr>
<td>/faculty/education/arister.pcf</td>
<td>4/29/2015 10:49 AM</td>
<td>57%</td>
<td></td>
</tr>
<tr>
<td>/athletics/prospective-athletes.pcf</td>
<td>7/7/2015 7:02 PM</td>
<td>57%</td>
<td></td>
</tr>
<tr>
<td>/admissions/undergraduate.pcf</td>
<td>6/5/2015 2:19 PM</td>
<td>51%</td>
<td></td>
</tr>
<tr>
<td>/about/mission.pcf</td>
<td>4/29/2015 10:49 AM</td>
<td>43%</td>
<td></td>
</tr>
<tr>
<td>/academics/library.pcf</td>
<td>5/14/2015 5:32 PM</td>
<td>36%</td>
<td></td>
</tr>
</tbody>
</table>

Hovering over a search result will reveal the following menu items under the **Options** column:

- Go to Folder (takes the user to the parent directory where the file is located)
- Preview (takes the user to the Preview view of the page)

It is possible to type in the syntax utilized by the Advanced Search directly into the Quick Search. When using the Advanced Search, the syntax will appear in the Quick Search field once the Search button is clicked. Additionally, the Apache Lucene website includes details on the syntax and Boolean characters supported by the system.

**Indexing**

Indexing is the process by which content is added to the search. Once the Quick Search functionality is turned on at the account level, the sites can be indexed by Level 10 administrators.

In order to utilize the Quick Search functionality, the search functionality must be enabled at the site level, and the index must be built for the first time. The steps to do this are the same as the ones to be taken when a site index needs to be rebuilt.

When a site is indexed initially, it will also be indexed going forward automatically. Even if the search functionality is turned off, the indexing still occurs. The only time that indexing is not completed automatically is when the content is loaded via an FTP upload, which requires a Level 10 administrator to rebuild the index.
Building and Rebuilding the Index

1. Navigate to **Setup > Sites**.
2. Hover over the site row to index and select **Edit > Site**.
3. Navigate to the **Optional Features** panel.
4. To initially build or re-build the index, click **Build Index**. If the index has been built before, the date and time of the last build will be listed next to the button.
5. **Quick Search** can be enabled and disabled for the site by clicking on the checkbox next to the **Build Index** button.

It is possible to exclude specific folders and pages from being indexed. Select **Exclude From Search** in the Access menu of the folder or page to exclude it from the Quick Search index.

Keep in mind that this will not remove any content that has already been indexed from the search results, unless the option to apply recursively is available and selected, and it only excludes that folder or page, but not subfolders.

**Additional Information and Reminders**

Indexing will only index saved content. Any content that is currently being updated will not be indexed until it is saved. However, once the data is saved, it will be available for searching within approximately 10 seconds.

Quick Search will search through content and meta tags on the staging server. The search functionality will not search:

- Files on the production server
- Resources
- Assets
- Recycle Bin
- Source code

When a file or page is deleted or recycled, the content is automatically removed from the indexing.

The search results may include pages to which the user may not have access.
Servers

Overview

The OU Campus CMS by default includes a staging server and a production server. The staging server is not public-facing, while the production server is. The staging server can be used to preview content prior to publishing it to a public-facing web site. If Multi-Target Publish has been enabled for the account, alternative publish targets may be configured and if a user is a member of the assigned access group, they may select an alternative server to which to publish.

Staging

The staging server is used to store and serve web pages in the editing, workflow, and approval process prior to publishing on the target production server. Remember, when making updates to content within OU Campus and clicking the Save button, the file is only saved on the staging server. The updated content is not viewable on the web until the page is published.

Production

The production server is updated via the staging server. Published pages are transformed with the XSLT engine and the specific XSLs from an implementation and the resultant HTML and/or other page products (such as automatically-generated PDFs) are put on the production server.
Note: When a file is deleted from the staging server, it is also deleted from the production server and any publish targets. Anytime a file is deleted, it is deleted from all locations.

**Publish Targets**

When Multi-Target Publish in enabled, alternative publish targets may be defined. Access can be configured so that only a specific group of users have access to the server.

For more information, visit the Publish Targets page.

**Auxiliary Sites**

Auxiliary Sites can be configured at the account and site level. They allow for read-only repositories to be created and shared among sites so that a user may access content from an external source (such as images) across many pages.

For more information, visit the Auxiliary Site Selecting page.

**Binary Management**

With the addition of Binary Management, all content file types are under management of OU Campus on the staging server, unless the feature has been specifically disabled for the site or account by the administrator.

Differences when Binary Management is enabled or disabled:

- With Binary Management enabled, new files including images and video are uploaded to the staging server and must then be published to be available on the public-facing web site. Like pages, files are assigned a dependency tag and tracked. Links to those files are updated in a fashion similar to pages under the supervision of the Dependency Manager.
- With Binary Management disabled, files including images and videos are uploaded to the production server or default publish target. Binary files will not be tracked with Dependency Manager.

For more information, visit the Binary Management page.

**Server Choice**

When Binary Management is enabled, the default for the server drop-down is the production server or the default target. Note that Multi-Target Publish must be in use for an alternative publish target to be defined as
the default target. This is also the default for server drop-downs when Binary Management is not enabled. In either case, the server selector drop-down is available within various features:

- WYSIWYG image tool, media tool, and link tool
- Source Editor
- MultiEdit
- TCF
- Parameters file choosers

These settings can potentially be overridden by any default image and media paths defined in the site settings or with directory variables.

**Symlinks in Production Environments**

OU Campus supports the use of symlinks on a production server. When they are extant, the process that lists files and folders in the view of the production server will skip broken symlinks and continue with the listing. However, it is recommended that broken symlinks be updated.
Reports

Overview

Administrator functionality on the Reports menu is available for Level 9 or 10 administrators with the exception of the Recent Saves and Recent Publishes reports. Administrator functions for reports include the ability to check pages back in that have been inadvertently left checked-out, override the approval process when pages have been sent to unresponsive approvers, and run customized reports. Custom reports include the ability to run specific reports about content, users, and other system details, as well as export the results via a CSV file.

The following items are available from the Reports menu:

- Required Actions (All Levels)
  - Broken Pages (All Levels,
    Levels 0 through 8 only see broken pages to which they have access.
  )
- Out of Sync Pages (Available for Level 9 and 10 administrators)
- Checked Out Content (All Levels; Levels 0 through 8 only see their own checked out content)
- Pending Approvals (All Levels; Levels 0 through 8 only see their pending approvals)
- Scheduled Actions (All Levels; Levels 0 through 8 only see their scheduled actions)
- Site Check (Available for Level 9 and 10 administrators)
- Recent Saves (Available for levels 5 and above)
- Recent Publishes (Available for levels 5 and above)

Reports Menu for Different User Levels

<table>
<thead>
<tr>
<th>Levels 9 and 10</th>
<th>Levels 5 through 8</th>
<th>Levels 0 through 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="icon" alt="Reports" /> <img src="icon" alt="Add-Ons" /></td>
<td><img src="icon" alt="Reports" /> <img src="icon" alt="Add-Ons" /></td>
<td><img src="icon" alt="Reports" /> <img src="icon" alt="Add-Ons" /></td>
</tr>
<tr>
<td><img src="icon" alt="Required Actions" /></td>
<td><img src="icon" alt="Required Actions" /></td>
<td><img src="icon" alt="Required Actions" /></td>
</tr>
<tr>
<td><img src="icon" alt="Checked-Out Content" /></td>
<td><img src="icon" alt="Checked-Out Content" /></td>
<td><img src="icon" alt="Checked-Out Content" /></td>
</tr>
<tr>
<td><img src="icon" alt="Pending Approvals" /></td>
<td><img src="icon" alt="Pending Approvals" /></td>
<td><img src="icon" alt="Pending Approvals" /></td>
</tr>
<tr>
<td><img src="icon" alt="Scheduled Actions" /></td>
<td><img src="icon" alt="Scheduled Actions" /></td>
<td><img src="icon" alt="Scheduled Actions" /></td>
</tr>
<tr>
<td><img src="icon" alt="Site Check" /></td>
<td><img src="icon" alt="Site Check" /></td>
<td><img src="icon" alt="Site Check" /></td>
</tr>
<tr>
<td><img src="icon" alt="Custom Reports" /></td>
<td><img src="icon" alt="Custom Reports" /></td>
<td><img src="icon" alt="Custom Reports" /></td>
</tr>
<tr>
<td><img src="icon" alt="Recent Saves" /></td>
<td><img src="icon" alt="Recent Saves" /></td>
<td><img src="icon" alt="Recent Saves" /></td>
</tr>
<tr>
<td><img src="icon" alt="Recent Publishes" /></td>
<td><img src="icon" alt="Recent Publishes" /></td>
<td><img src="icon" alt="Recent Publishes" /></td>
</tr>
</tbody>
</table>
**Required Actions**

Required Actions has two list views: Broken Pages and Out of Sync Pages, which display any broken dependencies for the site on which the administrator is working and pages out of sync across all sites in order to allow an administrator to publish them.

For more information, visit the Required Actions page.

**Checked Out Content**

The Checked Out Content report is available for all user levels. Levels 0 through 8 only see their own checked out content. The Checked Out Content report provides a list of pages, files, and assets that are currently checked out. From the displayed list of files, it is possible to preview any page by clicking the preview button, or check-in any page by clicking the glowing light bulb next to the appropriate page.

For more information, visit the Checked Out Content page.

**Pending Approvals**

Available for all users. Level 9 and 10 administrators are able to view the pending approvals for all users, while user levels 8 and below are only able to view pages that have been sent to them for approval. The Pending Approvals report provides a list of pages that are currently awaiting approval. From the displayed list of files, it is possible to preview any page by clicking the preview button, or check-in any page by clicking the glowing light bulb next to the appropriate page. Checking in a page that is pending approval overrides the approval of that page, but does not publish it. This gives an administrator, or the original author, the ability to continue revising the page, or publish it using a different approval process.

For more information, visit the Pending Approvals page.

**Scheduled Actions**

Available for all users. Level 9 and 10 administrators are able to view the scheduled actions for all users, while user levels 8 and below are only able to view scheduled actions they have set.

The Scheduled Actions report provides a list of pages with a scheduled action. For example, items may be scheduled to automatically be published, expired, or set up to send an alert.

For more information, visit the Scheduled Actions page.

**Site Check**

The Site Check report allows a sitewide link check to be run in order to find all broken links or warnings related to links on the pages.

For more information, visit the Site Check page.

**Custom Reports**

Custom Reports allow level 9 and 10 administrators to create the kinds of specific reports that he or she needs to manage, monitor, report, and ultimately control or change settings within OU Campus. Custom Reports can be created with as little as two clicks for the following report types: Users, Groups, Pages, Directories, Sites, Page Products, Assets, Tweets, and Facebook Wall Posts. Reports run in real time and generate results in 2 seconds or less for sites with less than 1 million pages and 10,000 users.

For more information, visit the Custom Reports page.
Recent Saves
The Recent Saves report is available for levels 5 and above. It displays a list of content that has been recently saved and includes information about the type of save that was performed. The content listing includes linked file names to preview the content. The report is paginated so that a user might navigate through the list of pages in manageable chunks and may export the report to CSV.

For more information, visit the Recent Saves page.

Recent Publishes
The Recent Publishes is available for levels 5 and above. It displays a list of content that has been recently published, and includes information about the type of publish that was performed. The content listing includes linked file names to preview the content. The report is paginated so that a user might navigate through the list of pages in manageable chunks and may export the report to CSV.

For more information, visit the Recent Publishes page.
Required Actions

Overview

The Required Actions report consists of two reports: Broken Pages and Out-of-Sync Pages. The availability of these reports is based on user level and is different for each report. These reports can be found in Reports > Required Actions.

- For the **Broken Pages** report, Level 9 and Level 10 administrators will see all broken pages in the list. User levels 0 through 8 will only see broken pages listed to which they have access.
- The **Out-of-Sync Pages** report is only available to Level 9 and Level 10 administrators.

When the Required Actions menu item is clicked, the Broken Pages report is shown by default, and users with appropriate permissions can then navigate to the Out of Sync Pages report in the secondary navigation bar.
Broken Pages

Overview

Authority Level: All user levels. Level 9 and Level 10 administrators will see all broken pages in the report. User levels 0 through 8 will only see broken pages to which they have access.

To help solve the issue of broken links due to content being deleted, administrators can use the Broken Pages report. This report shows all content that has broken links to external content. This makes changing or fixing the links easier and can be used on a page-by-page basis. Administrators can click the linked content to preview the page or content in question. They can also hover over each item in the list view and click Edit to travel directly to the Edit or Source Editor screen of the selected page.

From the Broken Pages report, users can:

- View a list of all pages that have broken links
- Filter the results by name using the Filter tool
- Sort the results by column
- Export the results to a CSV file
- Click the hyperlinked page path to preview the pages
- View the status of the page (checked out, checked in, or locked to another user)
- Hover over the edit menu found in the Options column to travel directly to the WYSIWYG or Source Editor for the page

When a page uses an external source for content, such as an asset or a link to another page, it gains "dependency." It then "depends" on the external content to exist. Therefore, issues arise when that external asset, file, page, or directory is deleted. If Dependency Manager is active on the site, the system updates the links should a directory or page be renamed or moved, but any links to content that has been deleted still need to be repaired manually.

Dependency Manager has no effect on assets. For more information about Dependency Manager and Assets, please visit their respective pages.

Once the page has been edited, saved, and published to address the dependency issue, it is removed from the Broken Pages report.
Broken Links and Dependency Tags

When a dependency is lost (for example, a linked-to page or a subscribed-to asset is deleted) the dependency tag or asset tag, path, and file name are shown within asterisks when hovering over the status bar in a browser. For example:

```
gallena.edu/training/about/***Broken f:1234 http://gallena.edu/training/about/ filename.html***
```

or

```
*** Broken a:52 Gallena_University: Image Gallery Asset ***
```

Broken links are reported in the following locations depending upon the XSL for the implementation:

- Preview/Edit/Version Compare Modes
- WYSIWYG Editor: Insert/Edit Link Dialog
- WYSIWYG Editor: HTML Source
- Page-based Link Check
- Publish-based Link Check
- Site Check
- Custom Reports
- Broken Pages
- Source Editor

Additionally, depending upon the XSLs for the implemention, broken links or assets may appear differently in some of the above views.

Viewing Broken Link Tags

Clicking on the page hyperlink in the Broken Pages report will take users to the Preview view of the page in question. Alternatively, users can hover over the Options column and travel directly to the page’s Edit view or Source Editor.

Keep in mind that the below examples represent a sample implementation and may look different for each institution depending on how the XSLs are configured.

Preview View

For Assets, the broken link information is shown encapsulated in asterisks. Broken hyperlinks will not appear any different in the Preview view than functional hyperlinks; when clicked, the link will lead to a 404 error page.
Undergraduate Requirements

Admission to all majors at Gallena University is competitive. Freshmen applicants must meet minimum GU eligibility requirements below to be considered.

Current undergraduate enrollment is: *** Broken a:17691 GallenaUniversity: Undergrad Enrollment *** students.

Edit View

Assets and hyperlinks appear the same in the Edit view as they do in Preview view. Clicking an editable region's Edit link will allow users to view the content in the WYSIWYG Editor.

WYSIWYG Editor

Within the WYSIWYG Editor, a broken asset is shown in the editing area. It includes an a gray striped wrapper and text indicating that the asset is broken.

Broken hyperlinks are not shown as broken in the WYSIWYG editing area. The URL will appear as a normal link in the WYSIWYG as well as in the Insert/Edit Link modal. To effectively determine where broken hyperlinks are located, it is recommended to look in the Source Editor, where broken dependency tags for both assets and hyperlinks will be shown clearly.
Source Editor

In the Source Editor, any broken link will have its dependency tag highlighted in red. Both assets and files will be highlighted in this manner.

Deleting Broken Dependency Tags

Deleting or Changing an Asset Tag from the WYSIWYG Editor

1. Navigate to the Edit mode of a page and select the appropriate editable region.
2. Find the broken asset wrapper. It will appear in gray.
3. Click anywhere on the asset wrapping, turning it green, and press the Delete key and click OK in the ensuing confirmation modal.
4. Alternatively, click the Insert/Edit Asset button in the JustEdit Toolbar and browse for a new Asset to replace the broken one.

Deleting a Broken Asset or Dependency Tag from the WYSIWYG Editor

Deleting a broken page dependency tag requires first identifying which links are broken on a page. Once that has been determined:

1. Position the cursor on the link in question.
2. Click the Insert/Edit Link icon on the WYSIWYG toolbar.
3. This displays the Insert/Edit Link modal. The broken link's path is displayed in grey below the Link URL box.
4. To remedy the broken dependency tag, perform one of the following actions:
   • Delete the tag from the Link URL field
   • Select another page by clicking the Browse icon
   • Enter the URL of a page to which to link

Deleting a Broken Asset or Dependency Tag in the Source Editor

If the page is viewed in the Source Editor, the broken dependency tag or asset tag is highlighted in red. Once the page has been edited to address the dependency issue, it will be removed from the Broken Pages report.

Assets that are broken appear in the Source Editor as a highlighted red \{\{a:###\}\} tag. Dependencies or pages that are broken appear in the Source Editor as a highlighted red \{\{f:###\}\}.
To delete a broken link from the Source Editor:

1. Select the entire broken \{{a:###}\} or \{{f:###}\} tag and press Delete. Simply clicking anywhere on the highlighted tag will select the entire tag.
2. Click Save in the Source Code Toolbar.

Once the broken link has been deleted, users are able to insert a new or correct link directly into the Source Editor by clicking Insert File Path or Insert Asset in the Source Code Toolbar.

NOTE: Changes do not take effect on the live page until the page is published. Publish out the page once the broken tag is removed and the change has been saved.
Out of Sync Pages

Overview

Authority Level
This report is available to level 9 and 10 administrators.

Pages are shown in the Out of Sync Pages report when an error occurs during a publish. An example of the type of error that would result in pages being included in this report is a loss of Internet connectivity during the publish process. It is anticipated that pages should rarely be marked as out of sync.

To remedy an out of sync page or pages, click the Publish All button and all publishing updates will be completed. The Out of Sync Pages report will display pages that are out of sync within any site within the account, regardless of which site the administrator is currently viewing.

In the Out of Sync Pages report, administrators can:

- View the number of out of sync pages listed in the report
- Filter results either by site name or path
- Click on the hyperlinked page name to travel to the page
- Use the Publish All button to publish all the out of sync pages listed in the report
- Use the Export CSV button to export the list of out of sync pages for the account in CSV format
- Sort by any file type, site name, or path

Publishing Dirty Pages

Whenever a page is moved or renamed, its subscribers (pages that link to it via a dependency manager tag) are marked as being "dirty" in the database. In this context, dirty means a page that has dependencies that will need to be republished in order to update the it with the new link.

In order to support Multi-Target Publish (MTP), it is necessary to keep track of which files were published where, in order to know which versions need to be updated on any particular server.

Illustrative Example

This example includes a site with a production server, a test server, and a development server. The test server is on revision #10 of the page, the development server is on revision #15, and the page has never been published to the production server.

Whenever the page is republished as a result of a file that it links to being moved or renamed, the appropriate server gets updated with the correct version. Afterward, the file's dirty flag is cleared. However,
if a page has never been published, as is the case in the example of the production server, it does not necessarily get automatically published, so the dirty flag remains.

This is the type of page that will be listed in the Out of Sync Page report until it is manually published by any publish action or with the use of the Publish All button on the Out of Sync Pages report.

After publishing out of sync pages, the pages are removed from the report. Any page checked out to a user remains checked out to the user.

**Exporting the Out of Sync Report**

1. Navigate to **Reports > Required Actions**.

2. From the Reports secondary navigation bar, select **Out of Sync Pages**.
3. Click **Export CSV**.

The report for the account is downloaded (dependent on browser settings) to the local computer in a CSV file. This includes the following information:

- **Path**: Shows the root relative path and file name
- **Name**: Shows the file name
- **Owner**: Includes the user name to whom the page is checked out, if any
- **Type**: Shows the file type as recognized by the CMS, for example, .pcf or .html
- **Site**: Shows the site to which the page belongs
Checked Out Content

Overview

Authority Level

Level 9 and Level 10 administrators will see all checked out content in the report. User levels 0 through 8 will only see content that is checked out to them.

The Checked Out Content report allows users to see what content (pages, assets, files, etc.) has been checked out. Checked out content includes files checked out to the current user, locked to other users, files scheduled for publish or expiration, and files pending approval in the workflow. In addition to being able to check in content, an administrator can preview pages and assets that are checked out to others. Lower user levels only see content checked out to them.

The Checked Out Content report includes:

- The number of items checked out
- The ability to filter results by the name of the file or who checked it out
- Sorting by file type, file path and asset name, status, checked out by, or checked out date
- Multi-selecting checkbox or individually selecting checkboxes to check-in en masse
- Clicking the status icon to check in content
- Administrators may check in files checked out to other users
Sorting Checked Out Content

The content can be organized according to different categories. By clicking on any of the following headers, content can be sorted in different ways.

**Type (Icon):** Provides an icon depicting the type of content that is checked out (e.g., page). Clicking on the Type column header will arrange the report by file type.

For an explanation of all different icons, visit the Icons reference page.

**Name:** Provides the path to the checked out page or the name of the asset. Clicking on the Name column header sorts the report by file name in ascending alphabetical order. Clicking the header again sorts the report by file name in descending alphabetical order.

**Status:** Gives the status of each item. Click the Status header sorts the report by file status, with pages checked in to the current user appearing first. Clicking the header again sorts the report in opposite order, with pages locked to another user appearing first.

For an explanation of all different icons, visit the Icons reference page.

**Checked Out By:** Provides the user name of the individual to whom the page is checked out. Clicking on the Checked Out By column header sorts the report by user name in ascending alphabetical order. Clicking the header again sorts the report by descending alphabetical order.

**Checked Out Date:** Provides the date the content was checked out by the named user. Clicking the Checked Out Date column header sorts the report by ascending date of check out. Clicking the header again sorts the report by descending date of check out.

**Last Saved Date:** Provides the date and time the content was last saved by the named user. Clicking the header sorts the report by ascending save date. Clicking the header again sorts the report by descending save date.
Checking In Content

If a content contributor has checked out a page and logged out of the system without checking that page back in, then no other user will be able to edit that page. A Level 9 or 10 administrator may check these pages back in.

Checking in a Single File

To view a record of all the checked out pages and assets in a site and check the content back in:

1. Navigate to Reports > Checked Out Content.
2. Hover over the status icon for the appropriate file and click.

3. This will open a confirmation modal. Note that any unsaved content will be lost and any scheduled publish or expiration will be canceled. To check the file back in to the system to make it available for other users to edit, click OK.

Checking in Multiple Files

Multiple files may also be checked in at a time.

1. Navigate to Reports > Checked Out Content.
2. Use the checkboxes to the left of the files to select the desired files.
3. Click Check In from the top row.
4. A success message is shown at the bottom of the screen confirming the check in of multiple files.

Note: Pages which are waiting for approval are also listed here as checked out. Pages in workflow cannot be checked back in here; administrators can do so in the Pending Approvals report.

Checking in Content with a Scheduled Publish or Expiration

If the checked out content is checked out due to a scheduled publish or expiration, it is possible to click the icon in order to change or cancel the publish.

After canceling the scheduled publish or expiration, the administrator can check in the page.
If the content is part of a multiple file check in, the scheduled publish or expire will be automatically canceled.
Pending Approvals

Overview

Authority Level

- All user levels.
- Level 9 and Level 10 administrators will see all pages pending approval by any user in the report. User levels 0 through 8 will only see pages pending their approval.

The Pending Approvals report lists all of content currently in the workflow awaiting approval. This report can be found by navigating to

Reports > Pending Approvals

For each report item, the report shows the file type with an icon, file path and name, the name of the user who sent the file for approval, the name of the approver, the date of the start of workflow, and the last date the file was modified. From the Actions menu, Users can reassign, check in content, and approve or decline the approval (if the file has been sent to them for approval).

In the Pending Approvals report, users can:

- See a list of the files pending approval
- Filter results by Path, who the approver is, or who submitted the file for approval
- Sort results by column: Type, Path, Approver, From, Workflow Started, and Modified Date
- Click the linked file name to view in Preview mode
- Hover and selecting a workflow-related action from the Actions menu
- Export report results to CSV
Actions Menu

Every file submitted for review has options that will appear upon hovering over the corresponding row. The options on the Actions menu include:

- **Reassign**
- **Check In**
- **Approve and Publish** (Shown when the file has been sent to the currently logged-in administrator for approval)
- **Decline** (Shown when the file has been sent to the currently logged-in administrator for approval)

**Reassign**
When a file is reassigned, it is removed from the approver’s workflow and placed in the workflow of another user. For more information on how workflow works in OU Campus, visit the Workflow page.

To reassign a file:

1. Hover over the page row and from the Actions menu, choose Reassign.
2. From the Reassign Approval modal, choose the new approver from the To drop-down menu. It is important to note here that only Level 9 and 10 administrators and users who have access to that page are shown in the drop-down menu.
3. Enter a Subject (required) and optionally, enter a Message.

4. If the Send Copy to Email checkbox is selected, an external email is sent to email address defined in the user’s settings. The content of the message includes several links and, optionally, a message from the submitting user. The included links are:
   • To the page submitted for review.
   • To the user's Dashboard inbox, where a copy of the message can be viewed.
   • To the original, unedited version of the page.
5. When finished filling out the required text fields, choose **Submit**.
6. After the page has been reassigned, the approver for the page is changed and this is reflected in the Workflow list view. An internal message is sent to the new approver notifying them that a new page is awaiting approval. The user who originally sent the page also receives a message in the system notifying them that the approver has been changed.

**Check In**

Choosing **Check In** removes the page from the workflow and checks it back in to the system.

The changes made to the file are saved, but it is not automatically published. The page must be published for the changes to be updated on the public-facing web site.

**Approve and Publish**

If the file selected is waiting for approval from the current user, then the option to **Approve and Publish** is available.

Choosing **Approve and Publish** displays the Publish modal for the page, which can include other publishing options depending upon the site configuration. For example, the Final Check, Schedule, and Social Media tabs may be available for those specific features and functionality.

For more information about the approvals workflow, visit the **Workflow** page.
Decline

If the file selected is waiting for approval from the current user, then the option to Decline is available.

Decline removes the file from the approver's workflow and sends the file back to the original sender for further editing and changes. Unlike Reassign, the ability to choose a user to send the page to becomes unavailable. This value is predefined as the original user who submitted the page for approval and cannot be changed.

To decline an approval:

1. Hover over the page row and from the Actions menu, choose Decline.
2. Enter a Subject (required) and optionally, enter a Message.
3. If the **Revert to Previous Version** checkbox is selected then the page submitted automatically reverts back to the last saved version of that page that is available on the production server. Selecting this function is optional.

4. When finished filling out the required text fields, click the **Decline** button.

Once an approval has been successfully declined, a system message appears at the bottom of the screen indicating that the page has been declined for approval and checked back into the database. Additionally, a message is sent to the recipient's inbox internal to OU Campus indicating that their request for approval was denied.
Scheduled Actions

Overview

Authority Level
All user levels. Level 9 and Level 10 administrators will see all scheduled actions in the report. User levels 0 through 8 will only see scheduled actions they have set themselves.

The Scheduled Actions report provides users with a view by which they can review, update, or cancel actions for pages that have had a scheduled action associated with them. This can include pages scheduled to be published, scheduled to expire, or that have a scheduled reminder for the content. Scheduled Actions are found in Reports > Scheduled Actions.

From the Scheduled Actions list view, users can:

- View the number of items with associated scheduled actions
- Filter results by File, Owner, or Recipient
- Export the list to a CSV file
- Sort results by any available column (File Type, File, Status, Owner, Recipient, or Scheduled Date)
- Click the file name to preview the content

Once a user has clicked on the file to preview the content, they can then cancel the reminder, remove the scheduled publish, or remove/reschedule the expiration.
Recent Saves

Overview

Authority Level: User levels 5-10 have access to this gadget.

The Recent Saves report displays a list of content that has been saved over the course of the last 90 days, and includes information about the type of save that was performed. This report can be viewed by navigating to Reports > Recent Saves.

From the Recent Saves report, users can:

- View the number of recently saved items
- Filter results by File and Publish Type
- Export the report to CSV
- Sort results by any available column (File Type, File, User, Save Type, and Last Saved Date)
- Preview the content by clicking the linked file name
- Browse paginated results through the pagination on the bottom of the list

When filtering or sorting the list the functionality applies to the entire list regardless of the current number of rows that are shown or what page is being viewed. For example, when viewing page 5 of the results and resorting by the Date column, the view is reset to page 1 and the list starts with the most recent or least recent date.
## Save Type Reference Table

<table>
<thead>
<tr>
<th>Save Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created from TCF</td>
<td>Indicates that a page was created using a template (TCF/TMPL).</td>
</tr>
<tr>
<td>New Copy</td>
<td>Indicates that the copy file operation was used from the Pages list view to create a copy of the content.</td>
</tr>
<tr>
<td>New Copy from WebDAV</td>
<td>Indicates while using WebDAV the file was copied.</td>
</tr>
<tr>
<td>Saved from Properties Editor</td>
<td>Indicates page parameters content was saved.</td>
</tr>
<tr>
<td>Saved by Asset Editor</td>
<td>Indicates any asset type was saved via the Edit Asset panel.</td>
</tr>
<tr>
<td>Saved from MultiEdit</td>
<td>Indicates the content was updated with a save from editing with the MultiEdit Content.</td>
</tr>
<tr>
<td>Saved from Source Editor</td>
<td>Indicates the content was updated with a save from editing with the Source Editor.</td>
</tr>
<tr>
<td>Saved from WebDAV</td>
<td>Indicates a file is uploaded new, overwritten, or moved/renamed via WebDAV.</td>
</tr>
<tr>
<td>Saved from WYSIWYG</td>
<td>Indicates the content was updated with a save from editing with the WYSIWYG Editor.</td>
</tr>
<tr>
<td>Updated by Find and Replace</td>
<td>Indicates that a find and replace action was performed that included replacing content in a file or asset.</td>
</tr>
<tr>
<td>Updated by Restore</td>
<td>Indicates the content item was restored from the recycle bin.</td>
</tr>
<tr>
<td>Updated by Revert</td>
<td>Indicates the content was updated by reverting to a previous version of the item.</td>
</tr>
<tr>
<td>Save Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Upload</td>
<td>Shows Upload when uploading from the Pages view, from the Pages list view with an overwrite, for Zip Import, and for Upload and Edit.</td>
</tr>
</tbody>
</table>
Recent Publishes

Overview

Authority Level
User levels 5-10 have access to this gadget.

The Recent Publishes report shows all content that has been published on a site over the last 90 days. From this screen, users can click the linked file to preview the content. Any version description or publish notes that were added at the time of publish can be viewed from the Versions screen. This report can be found in

Reports > Recent Publishes

From the Recent Publishes report, users can:

• View the number of recently published items
• Filter results by File, User, Publish Type, and Target
• Export the report to a CSV file
• Sort results by all available columns (File Type, File, User, Publish Type, Target, and Last Publish Date)
• Preview the page in question by clicking the file path/name
### Publish Type Reference Table

<table>
<thead>
<tr>
<th>Publish Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Deleted</td>
<td>As in permanently, from the recycle bin.</td>
</tr>
<tr>
<td>Content Expiration</td>
<td>Shown when a file has been expired with a replace or recycle.</td>
</tr>
<tr>
<td>Content Recycled</td>
<td>Shown when a file is sent to the recycle bin as any products are removed from the production server or publish targets. Also shown if content is restored from the recycle bin and then that is &quot;undone.&quot;</td>
</tr>
<tr>
<td>Content Republished</td>
<td>When an asset is published, subscribing pages are republished. There are exceptions to subscribing pages being republished. See <a href="#">Publishing Assets</a>.</td>
</tr>
<tr>
<td>Content Reverted</td>
<td>Shown when a file has been reverted on staging, but not yet published.</td>
</tr>
<tr>
<td>Directory Publish</td>
<td>Shown when content is published with the publishing of a directory.</td>
</tr>
<tr>
<td>File Publish</td>
<td>Shown when content has been published to the production server or a publish target. This can include a page, file, or asset, and includes when one or more files are selected and published, but does not include a directory or site publish. If content is published as a result of being included as an unpublished dependency, it is also shown here.</td>
</tr>
<tr>
<td>Find and Replace Publish</td>
<td>This indicates that a find and replace has been performed and the results were published.</td>
</tr>
<tr>
<td>Scheduled Publish</td>
<td>Content was published as the result of a scheduled publish.</td>
</tr>
<tr>
<td>Publish Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Site Publish</td>
<td>Shown when an administrator has performed a site publish.</td>
</tr>
</tbody>
</table>
Site Check

Overview

Authority Level: This report is available to level 9 and 10 administrators.

Site Check allows OU Campus administrators to check all links across the site, both internal and external. The resulting report provides a list of all broken links and all warnings, which can then be used to make global changes or individual changes as necessary. This tool works in conjunction with the individual link checking feature of Page Check.

The Site Check can be found at Reports > Site Check.

Site Check is a tool that can be used to identify and correct invalid links on pages under OU Campus management before or after they are published. Site Check does not test the links on pages on the production server, but it is checking that links to pages on the production server are valid. It is not parsing pages on the production server.

When running a new site check, users are able to navigate around OU Campus without interrupting the check. A notification will appear at the bottom of the screen when the check has completed. Users can click this link or navigate back to Reports > Site Check to view the results. The check that is currently running can also be canceled. A user will not be able to view the current or new site check results until the current Site Check has been completed.

Running a Site Check

When first clicking on the Site Check report, administrators will be taken to the Scope screen. Administrators can limit the site check in scope to specific directories and files, or can use the Select All checkbox to include content from the entire site.

Administrators can also choose to follow redirects and check the links within include files. A timeout setting can also be set after which if the link checker cannot validate the link, it will be reported as not found. While the site check

After the site check has been run, the results summary is shown in the Link Check screen. This shows the All Broken Links list view. The results can also be shown by page and a list of invalid pages is available. Additional options are available from the Broken Links by Page report.
To run a site check:

1. Navigate to Reports > Site Check. in the Scope options, use the Select All checkbox or pick and choose the directories and files to run the check on.

2. Scroll past the Scope panel and set the Link Check options. Alternatively, click Link Check in the secondary navigation bar.

There are three options in the Link Check panel:
- **Follow Redirects**: Checking this option will direct the system to follow all redirects to the final resulting page for the most accurate reporting.
- **With Includes**: Checking this option directs the system to check the links within any include files. If an include file of a page being checked can not be reached page check reports an error.
- **Timeout**: Select how long the system should attempt to check each link before reporting that the page could not be found. The default is 30 seconds.

3. Click Run.
This may take several minutes to complete. It is possible to continue with other work while this is running, or cancel the Site Check that is being run. If additional administrators attempt to run the check during this process, they will see the same "Site Check in progress" status indicator.

**Reviewing Site Check Results**

After the check has been completed, the results are shown in three reports. These are visible to all administrators. The available reports are:

- All Broken Links
- Broken Links by Page
- Invalid Pages

**All Broken Links**

This report lists all broken links. This report can be exported as a CSV file using the Export CSV button.

This list view includes:

- The number of pages with broken links listed in the view
- **Link Column**: Shows full URL for the broken link.
- **Path**: Shows the page that has the broken link. Click the link to preview the page.
- **Staging**: Indicates the result of the link check on the staging server.
- **Production**: Indicates the result of the link check on the production server.
- **Status Code**: Shows the HTTP response status code, if applicable.
There will not always be an icon in both the Staging and Production columns depending on the link, where it resides, and the result.

### Broken Links by Page

The Broken Links by Page report shows all pages on which there is one or more broken links or warnings. Once the links have been fixed, the report can be rerun by hovering over the row and selecting **Rerun**.

<table>
<thead>
<tr>
<th>Path</th>
<th>OK</th>
<th>Broken</th>
<th>Warning</th>
<th>Unchecked</th>
<th>Last Checked / Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>./leftnav.inc</td>
<td>4</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>12/8/2014 3:13 PM</td>
</tr>
<tr>
<td>./resources/includes/footer.inc</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>12/8/2014 3:13 PM</td>
</tr>
<tr>
<td>./resources/includes/footer_lang.inc</td>
<td>12</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>12/8/2014 3:13 PM</td>
</tr>
<tr>
<td>./resources/includes/social.inc</td>
<td>6</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>12/8/2014 3:13 PM</td>
</tr>
<tr>
<td>./resources/includes/topnav_lang.inc</td>
<td>17</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>12/8/2014 3:13 PM</td>
</tr>
</tbody>
</table>

This report includes:

- **Path**: Shows the root relative path and be clicked to preview the page
- **OK**: Number of links that were tested as okay or valid
- **Broken**: The number of broken links on the page
- **Warning**: The number of links with warnings
- **Unchecked**: The number of links that were not checked
- **Last Checked/Options**: The date that the links were last checked and when hovering over the row includes the options to View Results, Preview, and Rerun

Click **Results** while hovering over a row to view the **File Results** modal. This modal shows the file results and includes the following:

- The file name of the content that was checked
- The ability to load the modal in a new window
- **Link URL**: Shows the root relative path; when clicked, administrators will be taken to the page preview
- **Staging**: Indicates the result of the link check on the staging server
- **Production**: Indicates the result of the link check on the production server
- **Status Code**: Shows the HTTP response status code, if applicable
Click Close to dismiss the modal.

**Rerunning a Site Check**

From the Broken Links by Page view, all pages can be selected or individual pages can be selected and then the site check rerun.

1. From the Site Check menu, click Broken Links by Page.
2. Use the checkboxes to select all pages or individual pages.
3. Click Rerun on the header of the list view if multiple files are selected, or hover over the list item and click Rerun.
Invalid Pages

The Invalid Pages report will provide a list of pages that could not be checked and the error code indicating why that page could not be checked. These pages have a Preview option which will take the user to the page. However, if the PCF cannot be rendered, the issue causing the error must be fixed before the page can be checked.

About the Validator

The W3C Compliance Validator is a service that OmniUpdate offers to their clients which helps check the validity of Web documents.

Most Web documents are written using markup languages, such as HTML

or

XHTML

These languages are defined by technical specifications, which usually include a machine-readable formal grammar (and vocabulary). The act of checking a document against these constraints is called validation, and this is what the Markup Validator does.

Validating web documents is an important step which can dramatically help improving and ensuring their quality. Validation is, however, neither a full quality check, nor is it strictly equivalent to checking for conformance to the specification.

This Validator can process documents written in most markup languages. Supported document types include the
HTML

(through HTML 4.01) and XHTML

(1.0 and 1.1) family, MathML, SMIL and SVG

(1.0 and 1.1, including the mobile profiles). The Markup Validator can also validate Web documents written with an SGML

or XML

DTD

, provided they use a proper document type declaration.

This Validator is also a HTML validating system conforming to International Standard ISO/IEC 15445-HyperText Markup Language, and International Standard ISO 8879-Standard Generalized Markup Language (SGML),

which basically means that in addition to W3C recommendations, it can validate according to these ISO standards.
Setup

Overview

This section includes information about the Setup menu in OU Campus. The Setup menu is available to Level 10 administrators in the Global Navigation Bar and can be used to access the setup screens for much of the functionality found within OU Campus.

Account

The Account screen allows the administrator to set up and edit the account-specific settings and includes General Settings, Publish Settings, Login Page, Auxiliary Sites, and Optional Features. These settings apply to all users and sites within the account unless otherwise overridden.

For more information, visit the Account page.

Sites

The Sites screen is where the site configuration is completed. This is where administrators can configure the site’s access settings, scan when using Dependency Manager, publish the site, and even export a copy of the site.

For more information, visit the Sites page.
Users
The Users screen is where users can be added, modified and deleted. User settings apply to the entire account. User levels, approvers, and additional permissions can be configured in the Users screen.

For more information, visit the Users page.

Groups
The Groups screen is where groups can be created, modified, and deleted. Groups will be utilized within the entire account. Groups are used for assigning access and bypassing approver settings.

For more information, visit the Groups page.

Toolbars
The Toolbars screen is where custom toolbars can be created, modified, and deleted. Toolbars can be assigned to users, sites, directories, pages, and even editable regions.

For more information, visit the Toolbars page.

Font Size Sets
The Font Size Sets screen allows an administrator to define specific font sizes that will be made available to the users. The set is then assigned to a custom toolbar.

For more information, visit the Font Size Sets page.

Gadgets
Setup for Gadgets includes the functionality to add and configure gadgets in addition to those that are system provided. Users can configure their Dashboard to include or not include specific gadgets.

For more information, visit the Setup Gadgets page.

Custom Dictionaries
The Custom Dictionaries screen allows administrators to view, add, edit, and delete words in the site and account dictionaries in five different languages.

For more information, visit the Custom Dictionaries page.

Google Analytics
Setup for Google Analytics includes the functionality to add and configure one or more views associated with properties in a Google Analytics account. Once Google Analytics is configured for a site, analytics data is displayed with the Site Analytics Gadget and Page Analytics Gadget.

For more information, visit the Google Analytics Overview page.

Templates
The Templates screen allows each individual page template to be made available to specific groups in order to create both restrictions and flexibility.

For more information, visit the Templates page.
Facebook

The Facebook screen is where Facebook Pages can be added, managed, or deleted. Facebook allow users to send a wall post to the Facebook Page upon publication of a page. Additionally, OU Social can be used with the Facebook Pages, allowing a landing page to be made visible to visitors of the page and managed from within OU Campus. Multiple Facebook Pages can be added and made available to different groups, allowing the group members to see only the Facebook Pages to which they have been assigned.

For more information, visit the Setup Facebook page.

Twitter

The Twitter screen is where Twitter accounts can be added, managed, or deleted. Twitter accounts allow users to send a Tweet to Twitter upon publication of a page. Multiple Twitter accounts can be added and made available to different groups, allowing the group members to see only the Twitter accounts to which they have been assigned.

For more information, visit the Twitter page.

Resource Sharing

Many of these functions have varying levels of access depending on what level of OU campus the user is working at. The following chart details the levels at which these resources are able to be applied.

<table>
<thead>
<tr>
<th>Element</th>
<th>Skin</th>
<th>Account</th>
<th>Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Page Templates</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>In-Context Editing</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Users</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>User Groups</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Template Groups</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>XSLs</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Assets</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Dependency Tags</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Snippets</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>RSS Feeds</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Find &amp; Replace</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Toolbars</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Social Media Accounts</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Gadgets</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Google Analytics</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Add-Ons</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Auxiliary Sites</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Publish Targets</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Account

Overview

The account settings provide administrators the ability to modify all the global settings for the account. These settings affect all sites and users under an account unless a setting closer to the content (i.e., at the site, directory, or page level) overwrites it. Account settings in OU Campus are available on the Setup menu, which is only available to a Level 10 administrator.

From the OU Campus interface, to access the Account screen for account management features, navigate to Setup > Account.

The account settings in OU Campus match the account settings available within the Super Administration interface, which is available for Enterprise installations.

Editing Account Settings

Level 10 administrators can edit account settings by navigating to Setup > Accounts.
The **Account Settings** include the five specific panels. For more information about the specific functionality of each configuration option, see the following topics organized by panel:

- **General Settings**: Contains general information about the account and its main contact. JustEdit can also be configured from this panel.
- **Login Settings**: Contains the ability to set the number of failed login attempts available for a user before they are locked out of the system.
- **Publish Settings**: Contains settings relating to the publishing of pages; Page Check options can be set here.

<table>
<thead>
<tr>
<th>General Settings</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Name</td>
<td>Gallena_Training</td>
</tr>
<tr>
<td>First Name</td>
<td>Charity</td>
</tr>
<tr>
<td>Last Name</td>
<td>Katz</td>
</tr>
<tr>
<td>Organization</td>
<td>OmniUpdate</td>
</tr>
<tr>
<td>Street</td>
<td>1520 Flynn</td>
</tr>
<tr>
<td>City</td>
<td>Camarillo</td>
</tr>
<tr>
<td>State</td>
<td>California</td>
</tr>
<tr>
<td>Zip</td>
<td>93012</td>
</tr>
<tr>
<td>Country</td>
<td>United States</td>
</tr>
<tr>
<td>Phone</td>
<td>(805) 484-9400</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:ckatz@omniupdate.com">ckatz@omniupdate.com</a></td>
</tr>
<tr>
<td>Time Zone</td>
<td>(GMT-8:00) Pacific Time</td>
</tr>
<tr>
<td>Locale</td>
<td>English (United States)</td>
</tr>
<tr>
<td>Help URL</td>
<td></td>
</tr>
<tr>
<td>Logo URL</td>
<td></td>
</tr>
<tr>
<td>Failed Attempts</td>
<td>3</td>
</tr>
<tr>
<td>Lockdown</td>
<td></td>
</tr>
</tbody>
</table>

Messages sent by the system will come from this address, or OmniUpdate Support if left blank. Leave blank for standard OmniUpdate provided help. Replaces logo in top left of system.

The number of consecutive failed login attempts before a user is locked out.
• **Login Page:** Contains the fields where administrators can replace the OU Campus login page with a CAS or Shibboleth URL, add a custom announcement URL to the OU Campus login page, and configure a logout URL.
• **Auxiliary Sites:** Allows administrators to add auxiliary sites for the account.
• **Add-Ons:** Allows administrators to configure Add-Ons for the account.
• **Optional Features:** Contains a set of checkboxes to activate and deactivate optional features for the account, such as Binary Management, LDP, and Multi-Browser Preview.

When configuration is complete, remember to click **Save** to save any entered information, or if necessary to cancel the action click **Cancel**.

**Creating a New Account**

OU Campus can be provided as an Enterprise installation, which is a local server maintained by the institution, or provided as SaaS (software as a service). For Enterprise installations the Super Administration interface provides higher-level administrators access to add, modify, and remove accounts, sites, additional administrators, users, as well as view reports about those tasks. Administrators at the Super Administration level can create new accounts through the Super Administration interface.

For more information, see the **Super Administration** section of the support site.
General Settings

Overview

The fields and options available in the General Settings panel for editing an existing account are as follows:

Account Name: Name assigned to account. This cannot be edited.

General Settings includes several fields related to basic information about the account and the account's main contact:

• First Name
• Last Name
• Phone
• Institution
• Street
• City
• State
• ZIP
• Country
• Phone

Email Address: Messages sent by the system will come from this address. If this field is left empty, all system messages will come from donotreply@omniupdate.com.

Time Zone: Set the default time zone for the account by selecting the city or region from the drop-down menu that most closely matches the account's primary location. This will create the date and time stamps within the system, as well as keep the time accurate during Daylight Savings Time.

Leave blank for server default.

The default setting is

America/Los Angeles

for

SaaS clients and

the time zone where the staging server is housed for Enterprise licensing. When setting the time zone, please be aware of precedence as time zone can also be configured at the site level and user level. The setting configured for the user takes precedence, then site, and then account.

Locale: Sets the general locale and drives the default dictionary. Leave blank for server default. The default is English (United States), which will configure an English language dictionary. Precedence is user, site, account. The Locale setting does two things within OU Campus:

• Determines the format of the date and time stamps throughout the system.
• Changes the drop-down default for the custom dictionary selection available in the WYSIWYG Editor (and Page Check and Final Check).

For more information, visit the Locale page.
Help URL: Overrides the URL that users are taken to when they click Help > Support. Leave blank for the default link to the OU Campus support site or enter a URL for a separate help site that may have been created for the users.

JustEdit: Sets whether JustEdit is activated or deactivated for the account. Administrators may also choose Set by Administrator to give level 9 and 10 administrators the ability to activate JustEdit on a per-user basis, or Set by User to give each user in the account the ability to activate JustEdit for themselves.

For more information about JustEdit, visit the JustEdit page.
Login Settings

Failed Login Attempts: Sets the default number of consecutive failed attempts at logging in before a user is locked out. The number of login attempts can be set between 1 – 9.

<table>
<thead>
<tr>
<th>Login Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed Login Attempts</td>
</tr>
</tbody>
</table>

The number of consecutive failed login attempts before a user is locked out.
Locale

Overview

In general, the concept of locale includes more than just the date/time stamp, as it refers to a range of standards that vary by region. For example, it can specify the calendar used, how weeks are identified, month identification format, use of the 24-, 12-, or 6-hour clock, the notation for currency, character classification, paper size setting, and string collation.

In OU Campus, however, locale configures two things:

- The format for the date/time stamps throughout the system.
- The default language customization for spell check for the five available custom dictionaries. This includes the default for the drop-down list when there is an option for spell check. The ability to choose a custom dictionary for spell check is available during Page Check, Final Check, and within the WYSIWYG Editor.

The locale can be set at the account, site, or user level. When setting up a locale, the order of precedence is User, Site, Account. The system will use honor the setting at the user level first, then the site, then the account level.

Locale (v10)

The setting can be navigated to via many paths:

- Setup > Accounts > General Settings > Locale
- Setup > Sites > [edit site] > Site Preferences > Locale
- [Current user] > Settings > User Information > Locale
- Setup > Users > User Information > Locale

Locale provides a drop-down list of languages and corresponding countries for customizing and localizing the interface.
Example of Locale Drop-Down

The list often includes a general category as well as more specific ones, e.g. "Spanish" versus more localized variations such as "Spanish (Chile)" and "Spanish (Mexico)".

If left blank for all settings, the default is English (United States).

The custom language dictionaries are:

- English
- Spanish
- French
- Italian
- Portuguese

These can be used without configuring a locale, and can be selected from the drop-down list when necessary. When locale is configured, the drop-down for custom dictionary selection defaults to the appropriate dictionary in the WYSIWYG.
The configuration of a locale also determines the format of the date and time stamps throughout the system. For example, when selecting "French (France)" for the locale, the WYSIWYG selection for custom spelling dictionary defaults to French.

In the following example, when working in the WYSIWYG, the words on the page are spell checked against the default French dictionary. If configured by an administrator, users can add words to a custom dictionary file and those are then also included in spell check.
Timestamps

In the following example, when the locale setting for the United States uses the following format: month/day/year hour:minutes AM/PM (12-hour clock).

```
Modified
7/27/15 10:45 AM
```

The locale setting for the France uses the following format: day/month/year hour:minutes (24-hour clock).

```
Modified
27/07/15 10:45
```

The locale can be set for many regions, and the date and time format is converted accordingly. For example, choosing "Hindi (India)" converts to the following format:

```
Modified
27/07/15 10:45 पूर्वाहार
```

The above examples are from the folder structure. Locale is supported in custom reports also.

<table>
<thead>
<tr>
<th>#</th>
<th>Address</th>
<th>Date Created</th>
<th>Last Save</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>/_resources/css/ajax-loader.gif</td>
<td>29/08/15 पूर्वाहार</td>
<td>29/08/15 पूर्वाहार</td>
</tr>
<tr>
<td>2</td>
<td>/_resources/css/colorbox.css</td>
<td>29/08/15 पूर्वाहार</td>
<td>29/08/15 पूर्वाहार</td>
</tr>
<tr>
<td>3</td>
<td>/_resources/css/download.png</td>
<td>29/08/15 पूर्वाहार</td>
<td>29/08/15 पूर्वाहार</td>
</tr>
<tr>
<td>4</td>
<td>/_resources/css/email-base.css</td>
<td>29/08/15 पूर्वाहार</td>
<td>29/08/15 पूर्वाहार</td>
</tr>
</tbody>
</table>

For the complete list of available locales, see below.

<table>
<thead>
<tr>
<th>A-H</th>
<th>Arabic (Algeria)</th>
<th>Arabic (Bahrain)</th>
<th>Arabic (Egypt)</th>
<th>Arabic (Iraq)</th>
<th>Arabic (Jordan)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arabic (Kuwait)</td>
<td>Arabic (Lebanon)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Arabic (Libya)</td>
<td>Arabic (Morocco)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Arabic (Oman)</td>
<td>Arabic (Qatar)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Arabic (Saudi Arabia)</td>
<td>Arabic (Sudan)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Arabic (Syria)</td>
<td>Arabic (Tunisia)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Arabic</td>
<td>Belarussian (Belarus)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Belarussian</td>
<td>Bulgarian (Bulgaria)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bulgarian</td>
<td>Catalan (Spain)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalan</td>
<td>Chinese (China)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chinese</td>
<td>Chinese (Hong Kong)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chinese (Singapore)</td>
<td>Chinese (Taiwan)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chinese</td>
<td>Croatian (Croatia)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Croatian</td>
<td>Czech (Czech Republic)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Czech</td>
<td>Danish (Denmark)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Danish</td>
<td>Dutch (Belgium)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dutch</td>
<td>Dutch (Netherlands)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Language</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>English (Australia)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>English (Canada)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>English (India)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>English (Ireland)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>English (Malta)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>English (New Zealand)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>English (Philippines)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>English (Singapore)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>English (South Africa)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>English (United Kingdom)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>English</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Estonian (Estonia)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Estonian</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finnish</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finnish (Finland)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>French (Belgium)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>French (Canada)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>French (France)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>French (Luxembourg)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>French (Switzerland)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>French</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>German (Austria)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>German (Germany)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>German (Luxembourg)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>German (Switzerland)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>German</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Greek (Cyprus)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Greek (Greece)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Greek</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hebrew (Israel)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hebrew</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hindi (India)</td>
<td>Hindi (India)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>--------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hungarian (Hungary)</td>
<td>Hungarian (Hungary)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hungarian</td>
<td>Hungarian</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I-V</td>
<td>Icelandic (Iceland)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Icelandic</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indonesian (Indonesia)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indonesian</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Irish (Ireland)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Irish</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Italian (Italy)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Italian (Switzerland)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Italian</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Japanese (Japan)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Japanese (Japan, JP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Japanese</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Korean (South Korea)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Korean</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Latvian (Latvia)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Latvian</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lithuanian (Lithuania)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lithuanian</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Macedonian (Macedonia)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Macedonian</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Malay (Malaysia)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Malay</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maltese (Malta)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maltese</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Norwegian (Norway)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Norwegian (Norway, Nynorsk)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Norwegian</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Polish (Poland)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Language</td>
<td>Country</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spanish</td>
<td>Peru</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spanish</td>
<td>Puerto Rico</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spanish</td>
<td>Spain</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spanish</td>
<td>United States</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spanish</td>
<td>Uruguay</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spanish</td>
<td>Venezuela</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spanish</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Swedish</td>
<td>Sweden</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Swedish</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thai</td>
<td>Thailand</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thai</td>
<td>Thailand,TH</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thai</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Turkish</td>
<td>Turkey</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Turkish</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ukrainian</td>
<td>Ukraine</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ukrainian</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vietnamese</td>
<td>Vietnam</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vietnamese</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Locales List

### Overview

There are 152 locales available for use with the OU Campus CMS.

<table>
<thead>
<tr>
<th>Locale</th>
</tr>
</thead>
<tbody>
<tr>
<td>English (United States)</td>
</tr>
<tr>
<td>Albanian (Albania)</td>
</tr>
<tr>
<td>Albanian</td>
</tr>
<tr>
<td>Arabic (Algeria)</td>
</tr>
<tr>
<td>Arabic (Bahrain)</td>
</tr>
<tr>
<td>Arabic (Egypt)</td>
</tr>
<tr>
<td>Arabic (Iraq)</td>
</tr>
<tr>
<td>Arabic (Jordan)</td>
</tr>
<tr>
<td>Arabic (Kuwait)</td>
</tr>
<tr>
<td>Arabic (Lebanon)</td>
</tr>
<tr>
<td>Arabic (Libya)</td>
</tr>
<tr>
<td>Arabic (Morocco)</td>
</tr>
<tr>
<td>Arabic (Oman)</td>
</tr>
<tr>
<td>Arabic (Qatar)</td>
</tr>
<tr>
<td>Arabic (Saudi Arabia)</td>
</tr>
<tr>
<td>Arabic (Sudan)</td>
</tr>
<tr>
<td>Arabic (Syria)</td>
</tr>
<tr>
<td>Arabic (Tunisia)</td>
</tr>
<tr>
<td>Arabic (United Arab Emirates)</td>
</tr>
<tr>
<td>Arabic (Yemen)</td>
</tr>
<tr>
<td>Arabic</td>
</tr>
<tr>
<td>Belarussian (Belarus)</td>
</tr>
<tr>
<td>Belarussian</td>
</tr>
<tr>
<td>Bulgarian (Bulgaria)</td>
</tr>
<tr>
<td>Bulgarian</td>
</tr>
<tr>
<td>Catalan (Spain)</td>
</tr>
<tr>
<td>Catalan</td>
</tr>
<tr>
<td>Chinese (China)</td>
</tr>
<tr>
<td>Chinese (Hong Kong)</td>
</tr>
<tr>
<td>Locale</td>
</tr>
<tr>
<td>------------------------</td>
</tr>
<tr>
<td>Chinese (Singapore)</td>
</tr>
<tr>
<td>Chinese (Taiwan)</td>
</tr>
<tr>
<td>Chinese</td>
</tr>
<tr>
<td>Croatian (Croatia)</td>
</tr>
<tr>
<td>Croatian</td>
</tr>
<tr>
<td>Czech (Czech Republic)</td>
</tr>
<tr>
<td>Czech</td>
</tr>
<tr>
<td>Danish (Denmark)</td>
</tr>
<tr>
<td>Danish</td>
</tr>
<tr>
<td>Dutch (Belgium)</td>
</tr>
<tr>
<td>Dutch (Netherlands)</td>
</tr>
<tr>
<td>Dutch</td>
</tr>
<tr>
<td>English (Australia)</td>
</tr>
<tr>
<td>English (Canada)</td>
</tr>
<tr>
<td>English (India)</td>
</tr>
<tr>
<td>English (Ireland)</td>
</tr>
<tr>
<td>English (Malta)</td>
</tr>
<tr>
<td>English (New Zealand)</td>
</tr>
<tr>
<td>English (Philippines)</td>
</tr>
<tr>
<td>English (Singapore)</td>
</tr>
<tr>
<td>English (South Africa)</td>
</tr>
<tr>
<td>English (United Kingdom)</td>
</tr>
<tr>
<td>English</td>
</tr>
<tr>
<td>Estonian (Estonia)</td>
</tr>
<tr>
<td>Estonian</td>
</tr>
<tr>
<td>Finnish</td>
</tr>
<tr>
<td>Finnish (Finland)</td>
</tr>
<tr>
<td>French (Belgium)</td>
</tr>
<tr>
<td>French (Canada)</td>
</tr>
<tr>
<td>French (France)</td>
</tr>
<tr>
<td>French (Luxembourg)</td>
</tr>
<tr>
<td>French (Switzerland)</td>
</tr>
<tr>
<td>Language</td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td>French</td>
</tr>
<tr>
<td>German (Austria)</td>
</tr>
<tr>
<td>German (Germany)</td>
</tr>
<tr>
<td>German (Luxembourg)</td>
</tr>
<tr>
<td>German (Switzerland)</td>
</tr>
<tr>
<td>German</td>
</tr>
<tr>
<td>Greek (Cyprus)</td>
</tr>
<tr>
<td>Greek (Greece)</td>
</tr>
<tr>
<td>Greek</td>
</tr>
<tr>
<td>Hebrew (Israel)</td>
</tr>
<tr>
<td>Hebrew</td>
</tr>
<tr>
<td>Hindi (India)</td>
</tr>
<tr>
<td>Hungarian (Hungary)</td>
</tr>
<tr>
<td>Hungarian</td>
</tr>
<tr>
<td>Icelandic (Iceland)</td>
</tr>
<tr>
<td>Icelandic</td>
</tr>
<tr>
<td>Indonesian (Indonesia)</td>
</tr>
<tr>
<td>Indonesian</td>
</tr>
<tr>
<td>Irish (Ireland)</td>
</tr>
<tr>
<td>Irish</td>
</tr>
<tr>
<td>Italian (Italy)</td>
</tr>
<tr>
<td>Italian (Switzerland)</td>
</tr>
<tr>
<td>Italian</td>
</tr>
<tr>
<td>Japanese (Japan)</td>
</tr>
<tr>
<td>Japanese (Japan, JP)</td>
</tr>
<tr>
<td>Japanese</td>
</tr>
<tr>
<td>Korean (South Korea)</td>
</tr>
<tr>
<td>Korean</td>
</tr>
<tr>
<td>Latvian (Latvia)</td>
</tr>
<tr>
<td>Latvian</td>
</tr>
<tr>
<td>Lithuanian (Lithuania)</td>
</tr>
<tr>
<td>Lithuanian</td>
</tr>
<tr>
<td>Macedonian (Macedonia)</td>
</tr>
<tr>
<td>-------------------------</td>
</tr>
<tr>
<td>Macedonian</td>
</tr>
<tr>
<td>Malay (Malaysia)</td>
</tr>
<tr>
<td>Malay</td>
</tr>
<tr>
<td>Maltese (Malta)</td>
</tr>
<tr>
<td>Maltese</td>
</tr>
<tr>
<td>Norwegian (Norway)</td>
</tr>
<tr>
<td>Norwegian (Norway,Nynorsk)</td>
</tr>
<tr>
<td>Norwegian</td>
</tr>
<tr>
<td>Polish (Poland)</td>
</tr>
<tr>
<td>Polish</td>
</tr>
<tr>
<td>Portuguese (Brazil)</td>
</tr>
<tr>
<td>Portuguese (Portugal)</td>
</tr>
<tr>
<td>Portuguese</td>
</tr>
<tr>
<td>Romanian (Romania)</td>
</tr>
<tr>
<td>Romanian</td>
</tr>
<tr>
<td>Russian (Russia)</td>
</tr>
<tr>
<td>Russian</td>
</tr>
<tr>
<td>Serbian (Bosnia and Herzegovina)</td>
</tr>
<tr>
<td>Serbian (Montenegro)</td>
</tr>
<tr>
<td>Serbian (Serbia and Montenegro)</td>
</tr>
<tr>
<td>Serbian (Serbia)</td>
</tr>
<tr>
<td>Serbian</td>
</tr>
<tr>
<td>Slovak (Slovakia)</td>
</tr>
<tr>
<td>Slovak</td>
</tr>
<tr>
<td>Slovenian (Slovenia)</td>
</tr>
<tr>
<td>Slovenian</td>
</tr>
<tr>
<td>Spanish (Argentina)</td>
</tr>
<tr>
<td>Spanish (Bolivia)</td>
</tr>
<tr>
<td>Spanish (Chile)</td>
</tr>
<tr>
<td>Spanish (Colombia)</td>
</tr>
<tr>
<td>Spanish (Costa Rica)</td>
</tr>
<tr>
<td>Locale</td>
</tr>
<tr>
<td>-------------------------------</td>
</tr>
<tr>
<td>Spanish (Dominican Republic)</td>
</tr>
<tr>
<td>Spanish (Ecuador)</td>
</tr>
<tr>
<td>Spanish (El Salvador)</td>
</tr>
<tr>
<td>Spanish (Guatemala)</td>
</tr>
<tr>
<td>Spanish (Honduras)</td>
</tr>
<tr>
<td>Spanish (Mexico)</td>
</tr>
<tr>
<td>Spanish (Nicaragua)</td>
</tr>
<tr>
<td>Spanish (Panama)</td>
</tr>
<tr>
<td>Spanish (Paraguay)</td>
</tr>
<tr>
<td>Spanish (Peru)</td>
</tr>
<tr>
<td>Spanish (Puerto Rico)</td>
</tr>
<tr>
<td>Spanish (Spain)</td>
</tr>
<tr>
<td>Spanish (United States)</td>
</tr>
<tr>
<td>Spanish (Uruguay)</td>
</tr>
<tr>
<td>Spanish (Venezuela)</td>
</tr>
<tr>
<td>Swedish (Sweden)</td>
</tr>
<tr>
<td>Swedish</td>
</tr>
<tr>
<td>Thai (Thailand)</td>
</tr>
<tr>
<td>Thai (Thailand,TH)</td>
</tr>
<tr>
<td>Turkish (Turkey)</td>
</tr>
<tr>
<td>Turkish</td>
</tr>
<tr>
<td>Ukrainian (Ukraine)</td>
</tr>
<tr>
<td>Ukrainian</td>
</tr>
<tr>
<td>Vietnamese (Vietnam)</td>
</tr>
<tr>
<td>Vietnamese</td>
</tr>
</tbody>
</table>
Publish Settings

Overview

The Publish Settings include settings that are available or control the publishing of pages for an account. These settings work with other features throughout the system and in some cases can be overridden at the site level or by a user. Publish Settings include Page Check and Page Check Options that, when utilized, control the availability and type of quality controls that are required or made optional for users. Publish Threshold can be used to limit the number of pages that are published when an asset is re-published. Default text can defined for a Twitter tweet or Facebook wall post. This can also be defined in site settings and modified by a user during publish. The following Publish Settings are available:

- Page Check
  - Page Check Options (Only available when Page Check is enabled)
    - Spell Check
    - Link Check
    - W3C Validation
    - Accessibility Check
  - Accessibility Guidelines (Only available when Accessibility Check is enabled)
  - Accessibility Options (Only available when Accessibility Check is enabled)
- Publish Threshold
- Default Tweet/Wall Post
**Publish Settings**

- **Page Check**: On for Everyone
  
  Enable Page Check for everyone, by setting per user by an administrator, or by setting to let users enable for themselves.

- **Page Check Options**
  - Spell Check
  - Link Check
  - W3C Validation
  - Accessibility Check

- **Accessibility Guideline**: WCAG 2.0 (Level AA)

- **Accessibility Options**
  - Show Known Problems
  - Show Likely Problems
  - Show Potential Problems

- **Publish Threshold**
  
  The maximum number of files non-administrators can force to auto-publish when performing a change to a dependent file. A value of 0 will allow auto-publishing any number of pages. This applies to the Asset Manager and Dependency Manager features.

- **Default Tweet/Wall Post**
  
  The default text of the Twitter and/or Facebook message that is optionally posted when publishing a page.
Page Check

Overview

Page Check is an account-wide feature with several customization options that can be applied at the account, site, and even user level. This provides an administrator flexibility in the implementation of the various quality assurance checks that can be run on a page. Page Check can be run prior to final publish or as Final Check, either optionally or required at the time of publish. Alternatively, the decision to utilize any or all of the page checks can be left for each user to make. Once Page Check is enabled it can be initialized for a checked-out page:

- From Content > Pages > Review > Page Check
- From the page view of preview, edit, or while editing with the WYSIWYG Editor

Publish Settings

Enable Page Check for everyone, by setting per user by an administrator, or by setting to let users enable for themselves.

Page Check Options:
- Spell Check
- Link Check
- W3C Validation
- Accessibility Check

Accessibility Guideline:
- BITV 1.0 (Level 2)

Accessibility Options:
- Show Known Problems
- Show Likely Problems
- Show Potential Problems

Enabling Page Check

Prior to using Page Check, it must be enabled. Keep in mind that the options enabled in Page Check will be the available options that can be enabled in Final Check, if Final Check is to be enabled. Enabling Page Check activates it for all sites within the account.

1. From the Setup menu, choose Account.
2. Under **Publish Settings**, chose one of the enable options under **Page Check**:
   - **Disabled**: Disables Page Check for all users. The item does not appear as an option on the Review menu nor is it available when the page is checked out.
   - **On for Everyone**: Enables Page Check for everyone. This is the most common configuration of Page Check.
   - **Set by Administrator**: Administrators can activate Page Check on a per-user basis.
   - **Set by User**: Users can select Page Check for themselves from their user settings.

3. When any one of the enable options is chosen, the Page Check Options are shown. Any or all of the options can be chosen. Note: If Final Check is to be enabled for a site, it must be enabled for Page Check at the account level. If set to Set by Administrator or Set by User, the option to enable Page Check is available in the user settings.

4. When enabled, the Page Check Options include:
   - **Spell Check**: Enables the spell check functionality for Page Check/Final Check. Spell Check identifies any spelling errors on the page. The errors may be within editable regions to which the user does not have access, and may identify words that are not misspelled but need to be added to the custom dictionary. When using spell check, the choice of custom dictionary is available.
   - **Link Check**: Checks the validity of the links during Page Check/Final Check, including both links to other OU Campus managed pages and links to binary files and external websites.
- **W3C Validate**: Checks the markup for the page with W3C validator. For more information: [W3C Valid](#).
- **Accessibility Check**: Checks that published pages meet guidelines for accessibility for all users.

5. When **Accessibility Check** is selected, then the options for Accessibility Guideline and Accessibility Options are likewise enabled.

**Accessibility Guideline**:

- BITV 1.0 (Level 2): German accessibility standards.
- Section 508: USA federal requirements for accessibility standards.
- Stanca Act: Italian requirements for accessibility standards.
- WCAG: Web Content Accessibility Guidelines: Includes both 1.0 and 2.0 specifications as well as all three priority levels (A–AAA).

<table>
<thead>
<tr>
<th>Accessibility Guideline</th>
<th>BITV 1.0 (Level 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accessibility Options</strong></td>
<td>BITV 1.0 (Level 2)</td>
</tr>
<tr>
<td>Section 508</td>
<td></td>
</tr>
<tr>
<td>Stanca Act</td>
<td></td>
</tr>
<tr>
<td>WCAG 1.0 (Level A)</td>
<td></td>
</tr>
<tr>
<td>WCAG 1.0 (Level AA)</td>
<td></td>
</tr>
<tr>
<td>WCAG 1.0 (Level AAA)</td>
<td></td>
</tr>
<tr>
<td>WCAG 2.0 (Level A)</td>
<td></td>
</tr>
<tr>
<td>WCAG 2.0 (Level AA)</td>
<td></td>
</tr>
<tr>
<td>WCAG 2.0 (Level AAA)</td>
<td></td>
</tr>
</tbody>
</table>

**Accessibility Options**: Allows for selecting the specificity of the report based on the following:

- Show Known Problems
- Show Likely Problems
- Show Potential Problems

<table>
<thead>
<tr>
<th>Accessibility Options</th>
<th>Show Known Problems</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Show Likely Problems</td>
</tr>
<tr>
<td></td>
<td>Show Potential Problems</td>
</tr>
</tbody>
</table>

4. Click **Save** to save the changes.
Spell Check

Overview
The Spell Check can be enabled to run automatically with Page Check/Final Check each of which are enabled at the account/site level. To be available for Final Check, it must be enabled with Page Check. Spell Check by default is a tool available on the toolbar when editing with the WYSIWYG editor. Spell Check can be configured for the use of custom dictionaries to which users can add words and which support five different languages.

Variations of Enabling Spell Check
Spell Check can be separately enabled or disabled for Page Check, Final Check, and for the WYSIWYG Editor. Regardless, each has the option in the form of a drop-down for the user to choose to use one of the custom language dictionary. There are several combinations of configurations that can be utilized:

• If Page Check is enabled at the account level, Spell Check can be enabled as a Page Check Option.
• If Page Check and Spell Check are enabled at the account level, Final Check can be enabled for a site. Spell Check can be set in the site settings to be forced or optional at the time of publish.
• Spell Check within the WYSIWYG Editor can be enabled or disabled by editing or creating a custom toolbar, which can be applied to a content region or a user. The Spell Check is included with the default toolbar. Checking the spelling on a page can be toggled on and off within the WYSIWYG Editor by clicking the Spell Check icon.

In all of these scenarios, when there is a drop-down menu available to choose a custom dictionary, the default for the drop-down (and the language for the dictionary) is set with the locale setting in account settings.

Enabling Spell Check with Page Check
Spell Check identifies any spelling errors on the page. The errors may be within editable regions to which the user does not have access, and may identify words that are not misspelled but need to be added to the custom dictionary. When using spell check, the choice of custom dictionary is available.

1. From the Setup menu, choose Account.
2. Under **Publish Settings**, choose one of the options to enable Page Check from the **Page Check** dropdown.

3. Check the box next to **Spell Check**.

4. Click **Save**.

The Spell Check is now available from a Page Check.

**Enabling Spell Check with Final Check**

1. Enable **Spell Check** at the account level as described above.
2. From the **Setup** menu, choose **Sites**.

3. Hover over the desired site and select **Edit** from the site row.

4. Under **Publish Settings**, select **Final Check**.

5. Under **Final Check Options**, choose **Spell Check** to have the check run automatically before the final publish of a page. If left deselected, the option will be available at the time of publish for a user to manually run.
Customizing the Spell Check Dictionaries

The spell checker supports five languages, each with its own custom dictionary. The current languages supported are English, Spanish, French, Italian, and Portuguese. Words for a dictionary can be bulk-loaded with the addition of a text file for each language desired. It is not necessary to create a dictionary for foreign language words used in English. These can be added to the default English dictionary.

A customized dictionary can be added by an administrator at the site level. The dictionary is located in the OMNI_RESOURCES directory. Additionally, custom dictionaries can be added at the account and skin level by the OU Campus Support Team. The advantage of adding dictionary files at the account level is that it can be inherited for sites within that account. Contact OU Campus Support to have a custom dictionary added at the account or skin level.

If the OMNI_RESOURCES > dictionaries directory is not already created for a site, the path and file is created upon the first addition of a word to a dictionary. The files corresponding to the dictionaries are:

- English: OMNI-RESOURCES/dictionaries/custom_en
- Spanish: OMNI-RESOURCES/dictionaries/custom_es
- French: OMNI-RESOURCES/dictionaries/custom_fr
- Italian: OMNI-RESOURCES/dictionaries/custom_it
- Portuguese: OMNI-RESOURCES/dictionaries/custom_pt

New and custom words can be added to the spell check dictionary on a per site basis. Custom words that have been added to a site’s dictionary will be omitted by the spell checker tool in the WYSIWYG Editor for any page within that site. Keep in mind that it is possible that the spell checker in an individual’s browser may still mark the word as misspelled. If a word has been added to the dictionary, and it is still being marked as misspelled, check the browser’s spell check settings.
Users can override the default language and set the dictionary they want to use for an individual page from the spell checker tool in the WYSIWYG toolbar, or by choosing the locale in their user settings.

For information on setting locale, visit the Locale page.

**Granting Privileges to a User**

Adding custom words to the spell check dictionary is available dependent upon authority level. It is included automatically for Level 9 and 10 and it can be made available to Levels 1–8 by an administrator in user configuration.

1. Navigate to **Setup > Users**.

2. Hover over a user and select **Edit** from the user row.

3. Under **Preferences**, select the checkbox next to **Add to Dictionary** to allow a user to add words to the custom dictionary.
4. Click **Save**.

**Editing a Dictionary File**

An administrator can both add and delete words in the custom dictionaries. This is accessed through **OMNI_RESOURCES > dictionaries** and should be set up prior to starting to add words to the dictionaries. However, if a custom dictionary is not set up prior to adding a word, the system creates the custom dictionary when a word is added via WYSIWYG editing.

1. Open the file for editing by navigating to the custom dictionary file. For example:  
   OMNI-RESOURCES/dictionaries/custom_en
2. Add a new word on a new line.
3. To delete a word, remove the entire line and the word.
4. When finished editing, click **Save**. The page only needs to be saved to update the custom dictionary. It is not necessary to publish the dictionary file. The changes take effect immediately after clicking **Save**.

**Note**: Do not send to another for approval. Do not change the name of the file.
Publish Threshold

Overview

The Publish Threshold setting defines the maximum number of pages to be auto-published when an asset is republished or a page is moved or renamed when Dependency Manager is being utilized. If the threshold is set to 0, there is no limit on the number of pages that can be auto-published. If a different limit is set, and publishing the asset or renaming or moving a directory or page will require more pages to be published than allowed, an administrator will have to publish the asset or make the change to the directory or page.

When an asset is updated, it must be republished in order to update the subscribing pages and publish them to the production server. When the asset is published, all pages on which the asset resides are automatically republished with the updated asset. Only the content that is currently live will be republished, but the asset content will be updated. This means that if the page is in workflow or currently being edited, no changes that may be being made or have been made to the page will be lost or published by the auto-publish; only what was already approved and published.

Similarly, with Dependency Manager, when a page is renamed or moved, any pages linking to it must be republished on the production server so that the link paths are updated. This publish, like with assets, only publishes out the updated link, and all other content remains.

This means that if the number of pages on which the asset resides or a link exists to the page being updated exceeds the defined number in the Publish Threshold, the user is notified that an administrator needs to complete the action. The change will not be made or completed until the administrator either publishes the asset, or renames or moves the page.

If the change pertains to an asset, the user is presented with a message, and then directed to create a new message to the administrator.

The setting places a limit on the number of pages that a Level 8 or below user can republish at once. When they attempt to publish an asset, it is first determined how many pages will be affected. If this number is greater than the threshold, the asset will not publish, and the user will be notified and allowed to send the asset to an administrator for approval.

The maximum value for the Publish Threshold field is 99,999.

Configuring Threshold for Assets

Level 10 administrator privileges are necessary for configuring this setting.

1. Navigate to the Setup > Account.
2. Under Publish Settings > Publish Threshold enter the page threshold. If the number entered is 0, then no threshold is set and any number of pages are allowed to be republished.
3. After the desired threshold number was entered, click Save at the bottom of the page to save the changes. The threshold has now been set for the account.
Login Page

Overview

The Login Page panel is where administrators can configure various functionality with regards to the login page users see when they log into OU Campus.

OU Campus supports LDAP, CAS, and Shibboleth authentication which can be integrated into the existing single sign-on method. The fields available in the Login Page panel provide the ability to customize the authentication method.

The options in the Login Page panel are as follows:

**CAS or Shibboleth URL**: Enter a fully qualified URL to replace the standard OU Campus login page with a Central Authentication Service (CAS) or Shibboleth page for the entire account. CAS and Shibboleth provide single sign-on service and application authentication. Note that a Logout URL must be used if a page is defined for the CAS or Shibboleth URL.

For more information about using LDAP, CAS, and Shibboleth, see the topics at the Super Administration level via the Authentication page.

**Announcement URL**: If using the default OU Campus login page, this is used to customize the login page by specifying an HTML page that replaces the box shown on the right-hand side of the login page. Use a complete URL beginning with `https://`, as the OU Campus login page is also being served over https.

**Logout URL**: Determines the page that is shown upon logging out of the system.

![Login Page Panel](image)

Customizing the Announcement Page

System administrators can change the content of the announcements page that users see to the right of the login panel.
Creating the Announcement Page

A customized announcement page loads a web page inside of an iframe on the login page. Any web format, such as .html, .php, .aspx, or others can be used.

1. Create an HTML (or other web format) page in OU Campus and publish it.
2. Copy the full URL from the live website and paste it into the Announcement URL field in Setup > Account. Make sure the URL begins with https. For example: https://omniupdate.com/announcements/login_announcements.php
   
   If the page does not load, ensure that the production server (or wherever the page is hosted) is configured to serve https pages.
3. Click Save. If desired, log out of OU Campus and navigate to the OU Campus login page again to preview the announcement page.

The recommended size of the announcement URL window should be no larger than 720 x 600 for a screen resolution of 1024 x 768. A larger window will cause scroll bars on screen.

Configuring the Logout URL

Note that a logout URL must be used if a page is defined for the CAS or Shibboleth URL.

1. Navigate to Setup > Account.
2. From the Login Page panel, enter the URL in Logout URL field. The URL must be fully qualified (that is, contains http:// at the beginning of the URL).
3. Click Save. The user is directed to the URL upon logging out.
Auxiliary Sites

Overview

The Auxiliary Sites feature in OU Campus is a way by which users can navigate to other file locations other than the OU Campus staging server when they are inserting images, links, or media onto a page.

When users browse for files, they will first be directed to the directory in which they are currently editing a page, or the location configured in either the site settings or with a directory variable for images and media. However, when using the filechooser, users can select from a list of auxiliary sites in the drop-down menu found in the top right hand of the modal. After selecting an auxiliary site, users can browse for pages, media, or other files that reside on that server.

Auxiliary sites are typically used as repositories for media, such as images and video. Note that the auxiliary sites drop-down menu also lists the staging server and any publish targets, if Multi-Target Publish is in use.

Here is an example of how auxiliary sites can be used. A directory variable is in use for the alumni directory that automatically opens the filechooser to the default images directory, which is `/departments/alumni/images/`. Users frequently also need access to an image that is located in the main images folder for the institution, which is simply `/images/`. In this case, the auxiliary site can be configured for that `/images/` directory, so the user does not have to tediously navigate to it each time. It can be selected from the drop-down for easy access.
Auxiliary sites can either be on the same production server and identified as its own site location, or it can be a completely separate server, such as a media server where all current media is housed or a document repository. In order to configure an auxiliary site, the administrator must have the FTP account settings. It is not possible to link to a public-facing site, such as Flickr, as the connection is made via FTP. The connection is read-only, and media and files cannot be uploaded to another server via the file browser.

As many auxiliary sites can be added as necessary, and when configured in the account settings, apply to all sites within the account. If more fine-tuned control is required, auxiliary sites can also be created at the site level, which will limit access to that auxiliary site to the site in which it was created. Any auxiliary sites configured in an individual site’s settings are appended to any auxiliary sites set in the account settings.

**Setting Up an Auxiliary Site**

An auxiliary site can be configured in Account Settings or Site Settings, either inside the SuperAdmin interface or inside the normal OU Campus interface. Adding an auxiliary site at the account level specifies that it is available to all sites in the account. Adding an auxiliary site at the site level makes it available only for that site. The configuration options are identical at each level.

This functionality does not create the files or folder structure for the auxiliary site; it only allows OU Campus to retrieve files from an already existing FTP location. When these fields are populated, a back-end regex ensures the entries follow the expected syntax for each specific field. When viewing on-screen, note that the fields in bold are required. The setup fields for auxiliary sites are similar to those when configuring a site.

Auxiliary sites can be configured in the following locations:

- Setup > Account > Auxiliary Sites panel
- Setup > Sites > Edit > Auxiliary Sites panel
- Within the SuperAdmin interface, Accounts > Edit > Auxiliary Sites panel

Note that auxiliary sites cannot be configured when creating a new account or site; the feature can only be accessed by editing an account or site that has already been created.

1. From the Auxiliary Sites panel, click Add.

2. The **New Auxiliary Site** modal is displayed. The field names in bold indicate required items.
3. From the **New Auxiliary Site** modal, configure the fields as follows:

- **Site Name**: Required. Enter a user-friendly name for the auxiliary site that will appear in the insert link, image, and media modals, e.g. "Images of Buildings" or "Videos." Note that the drop-down menu in the filechooser may include auxiliary sites as well as publish targets, so it may be necessary on the part of the administrator to develop a taxonomy to help users distinguish among available sites and servers.
• **Server:** Required. Enter the host name or IP of the FTP server where the site is hosted. For example: \textit{training.oudemo.com}

• **FTP Type:** Required. Three options are available for FTP Type:
  • **SFTP:** Secure FTP
  • **FTP:** Active mode for FTP
  • **Passive FTP:** PASV mode for FTP

• **Username:** Required. Enter the user name for the FTP account.

• **Authentication Type:** Choose either **Password** or **Public Key**.

• **Password:** Required. Enter the password for the FTP account. If **Public Key** is selected for **Authentication Type**, this field will not appear.

• **UMask:** Choose either **User writable** or **User + group writable**.

• **FTP Root:** Required. Enter the FTP location for the auxiliary site. For example: \texttt{/public_html/_resources/videos}

• **FTP Home:** Optional. This should be a subdirectory of FTP Root.

• **FTP Directory:** Optional. This is where users are placed within the system by default when logging in. This should be a subdirectory of FTP Root.

• **HTTP Root:** Required. Enter the URL equivalent of the FTP Root. This is what is appended to the FTP path. It is required to specify the HTTP protocol prefix (\texttt{http://}) as well as include the trailing slash (/). For example: \texttt{http://videos.gallena.edu/_resources/videos/}

• **Available To:** Optional. Specify the group of users who will have access to this auxiliary site. The default value is Everyone.

4. Repeat the steps for any additional auxiliary sites to be created and click **Save**.

**Editing an Auxiliary Site**

The auxiliary site settings can be edited after the initial addition of the auxiliary site with the exception of the **Site Name** field. To edit an auxiliary site:

1. Click on the name of the auxiliary site in the **Auxiliary Sites** panel.
2. The **Edit Auxiliary Site** modal will appear.
3. Edit any information as necessary and click **Save**.

**Deleting an Auxiliary Site**

To delete an existing auxiliary site, click the grey \texttt{X} icon next to the auxiliary site name. This functionality does not delete files or folders from the auxiliary site, it only allows OU Campus to disconnect from the site so that it is no longer be available as an item on the drop-down menus.

**Best Practices**

There are some important things that an administrator should be aware of when creating an auxiliary site.

• The validation for the various fields in the **New/Edit Auxiliary Site** modals does not guarantee that the information is correct, merely that it follows proper syntax. It is the responsibility of the administrator to supply the correct FTP address, username, password, etc., in order for the site to function correctly.

• When entering the **HTTP Root** information, the \texttt{http://} requires a forward slash (/) at the end of the URL.

• Creating an auxiliary site in OU Campus does not create a new site or server; it simply allows OU Campus to retrieve files from an already existing site.
Optional Features

Overview
At the account level, additional features can be independently enabled and disabled. These are located within the Optional Features panel (Setup > Account > Optional Features). An optional feature can be enabled by selecting the adjacent checkbox or disabled by clearing the checkbox, and then clicking the Save button.

Asset Manager
Select the checkbox to allow access to the Assets screen, which gives users access to edit and create new assets as well as manage existing assets on the account. Clearing the checkbox disables all access to assets.

For a list of topics about LDP and assets configuration, visit the Assets & LDP Configuration page.

Binary Management
Select the checkbox to enable Binary Management for the account. Binary Management can then be enabled or disabled for each site under Setup > Sites > Site Settings. Before enabling Binary Management, it is recommended to review the documentation regarding the feature, starting with the Binary Management page.

Dependency Manager
Select the checkbox to enable Dependency Manager for the account, which manages internal links for sites. Before enabling Dependency Manager, it is recommended to review the documentation regarding the feature, located at the Dependency Manager page.

LDP
Select the checkbox to enable Live Delivery Platform (LDP) for an account. Further settings are available at the site level.

For more information, visit the Live Delivery Platform page.

Multi-Browser Preview
Use the Configure button to select the combination of platform, operating system, browser version, and browser that will be available for selection for Multi-Browser Preview for a page.

For more information, visit the Multi-Browser Preview Configuration page.
Reveal Site Password
Select the checkbox to allow the Production Server FTP password that was configured in the site settings to be revealed by clicking the **Show Password button**. Keep in mind that any Level 10 administrator will be able to reveal the password and view it from the system.
Configuring Add-Ons

Level 10 administrator privileges are required to edit account settings.

1. Navigate to Setup > Account > Add-Ons.
2. Click on the New button under Add-Ons.
3. Enter a user-friendly name (such as “This Is a Page” as opposed to “this-is-a-page”) which will display in the Add-Ons tab.
4. Enter the URL to page that should be displayed within the frame.
5. To make the add-on available to administrators only, select the check box next to Admin Only.
6. To open the application in a new window, select the check box next to Open in New Window.
7. Repeat the steps for any additional links to be created. The add-ons are saved when the Account settings are saved, and the tab is shown upon refreshing. Any links that are available to administrators only will appear bold to the administrator and are hidden from all other users.

Deleting Add-Ons

1. Navigate to Setup > Account > Add-Ons.
2. Click the Delete link for the add-on no longer desired.

Reordering Add-Ons

1. Navigate to Setup > Account > Add-Ons.
2. Reorder the add-ons by dragging and dropping the boxes under Add-Ons to the desired order.
Dependency Manager

Overview

The Dependency Manager is a feature that manages linking among internal files. It is used to help preserve the integrity of links leading to content maintained in OU Campus, including binary files if Binary Management is enabled. Dependency Manager maintains the correct link association when files or directories are moved or renamed. All the files that link to a moved or renamed file or directory are automatically republished to maintain the correct link. It also tracks the deletion of content and creates a notification in the Broken Pages list view.

Dependency Manager tracks links within a site and among sites within an account. This includes any file on any site within that account, but not sites that are contained with other accounts. The Dependency Manager automatically inserts dependency tags after it has been activated by an administrator and runs scans. For example, if Page A exists in OU Campus, and there are 100 other pages in OU Campus with links to Page A, these links are automatically updated if Page A is renamed or moved. If Page A is deleted, the 100 pages are also listed on the Broken Pages report found in Reports > Required Actions > Broken Pages. Level 9 and 10 administrators have complete access to the report. Users with an authority level of 8 or lower can view and perform actions only on the content to which they have access.

Dependency Manager is an optional feature which must be activated at the account level before it can be enabled for each individual site. A Level 10 administrator must also run an initial scan on each site in order to replace any paths in <a> and <link> tags for the href attribute. Going forward, when users insert new links, provided they use the browse functionality while inserting the link, the system automatically includes the dependency tag.

It is recommended that any Dependency Manager scan or revert be run during off-peak hours.

Prior to activating Dependency Manager and scanning the sites, it is advised that each site be exported. This will allow for a complete revert, using Zip Import, back to the site’s original state and URL configuration for links, should it be decided that utilizing Dependency Manager is not appropriate for the site. It is important to note that this will revert the site to the state it was at the time of export, and if any changes have been made since then, these will be lost.

Also note that upon initial scan (or rescan) of multiple sites within an account, two Dependency Manager scans are required of each site with the exception of the last site scanned, which only requires one scan. The first pass should scan each site one after another, and the second pass should start from the first site scanned and scan each one again with the exception of the last site. For example, if an account includes 10 sites, 19 total scans would need to be performed in order to ensure that all links among sites include the correct dependency tags. This ensures that any changes made after the first scan are correct and have not caused any new issues.

Dependency Manager and RFC2396

The Dependency Manager scan and revert scan is RFC 2396 compliant. In accordance with the specification, the Dependency Manager can convert URLs with very complex % encoded paths. URLs with unencoded spaces are not accepted.
Use Case
The Dependency Manager supports the use of %20 instead of a space in a file path works. A file can be uploaded via FTP that has spaces in the name. Insert the image on to the page and note that the inserted image has %20 in the file path. Enable both the Dependency Manager and Binary Management, and run a scan. The image path will be converted into a dependency tag. Run a revert scan and the link is converted back to %20. The %20 is the escaped encoding for the US-ASCII space character.

Unreserved/Encoded
The following are recommended characters, as using them in file names will translate into easy to read URLs. They are unreserved and never encoded.

- Uppercase letters
- Lowercase letters
- Numbers
- The following special characters: - _ . ! ~ * ' ( )

Reserved/Encoded
The following list of reserved characters are encoded by the Dependency Manager, but will result in URLs that are difficult to read. They are safe to use, but are not recommended:

- The space character
- The following special characters: " < > # % ; = > ? [ \ ] ^ ` { | }

Reserved/Unencoded
The following reserved characters are not encoded and are safe to use in paths as well:

- / : @ & + $ ,

All other UTF-8 characters may or may not be encoded depending on whether the file that contains the URL is UTF-8 or ASCII.

Dependency Links
When using Dependency Manager, links are inserted in a fashion similar to when Dependency Manager is disabled. Links can be added to the markup for a page in many ways, but only content that is browsed to with a file chooser has the tag automatically inserted; otherwise, an additional scan can be run. The ways of adding links are:

- Using Insert/Edit Link via the WYSIWYG
- Using the Source Editor
- Using the HTML Source Editor (not automatic)
- When Binary Management is enabled with Insert/Edit Image via the WYSIWYG
- Integrated into template design

When the link is inserted, the Link URL is shown as a dependency tag, which starts with a “d” or an “f”. These are similar in syntax to those tags used for designating assets.

When using a file chooser to select the file, once the appropriate page is selected, a dependency tag is shown in both the modal and the code view of a page. The page path is shown below the field in the Insert/Edit Link modal.
Links can also be added without browsing (for example, in the HTML Source Editor) and then a directory scan can be performed to convert the paths to dependency tags.

Example syntax for the tags are shown as follows:

- \{\{d:####\}\} — Directory tag
- \{\{f:####\}\} — File/Page tag
- \{\{a:####\}\} — Asset tag
- \{\{s:####\}\} — S-tag: Used with XML/XSL templating to pull content from a PCF file on staging

**Within Gadgets**

The Gadgets sidebar includes the Dependency Tag Info gadget, which provides the search functionality to find a dependency manager tag and also features the reporting information about the tag, such as the type of tag it is, the associated product name, the path to the product, the site under management, and a linked list of subscribers.

For more information, visit the Dependency Tag Info Gadget page.

**With Assets**

The Dependency Manager supports linking from within an asset; dependency tags can be added when creating and editing assets, and when the asset is inserted on the subscribing page the dependency tag is included in the content.

**With Multi-Target Publish**

Dependency links can be selected across publish targets if Multi-Target Publish is configured and in use for the account. Dependency Manager and dependency tags only pertain to pages maintained within OU Campus.

**With Binary Management**

With the advent of Binary Management, binary files, such as images, PDFs, and other documents, are managed by Dependency Manager when Binary Management is enabled for a site and binary files are uploaded to the staging server in OU Campus v10. Dependency tags are used to track and manage binary files on staging and production in a fashion similar to other linked-to files. For example, when file linking is managed by the Dependency Manager, if a binary file is renamed, moved, or published, then pages with links to that dependency are updated. Unpublished dependencies included images can be included with a page publish by selecting to include unpublished dependencies.

When Dependency Manager is used with Binary Management, binary files are treated like all other files managed by OU Campus, offering many advantages to both users and administrators, including reporting.
**Example of a Dependency Tag in WYSIWYG**

![Insert Link](image)

**Examples of Dependency Tags in Source Editor**

![Source Editor Example](image)

**More About Links and Linking**

If a site has Dependency Manager turned on, then a Dependency Manager tag is created when linking to any file on any site within that account, as long as the target file is under management of OU Campus. This is irrespective of the target site’s Dependency Manager setting. The only exception to this is if the file on the target site has never been recorded by the Dependency Manager in the database. Two common causes of this are:

1. The target file existed on the site before Dependency Manager came into being and that file has not been edited in a way that would cause this tag to be properly updated.
2. The target file was uploaded to staging via SFTP or WebDAV and also has not been touched in a way to cause the database to assign a Dependency Manager tag to the file.

In these cases, when linking, the appropriate text-type URL to the file is returned.

The other class of selectable files that only return text URLs are files on a target production server that are not under OU Campus management.
Among Sites

If one site has Dependency Manager enabled and another does not, the linking behavior is determined by the site record of the site doing the linking. So, for example, if Dependency Manager is on for Site A within an account, the link to Site B with the Dependency Manager off is still tracked with a dependency tag. However, if Site B links to Site A, there is not the ability to add a dependency tag in Site B.

When Publishing

When pages are published that contain dependency tag links, the dependency tag is replaced with the URL to the target page. The Dependency Manager supports both root relative URL links (e.g., /folder/folder/file.ext) as well as absolute URL links (e.g., http://www.college.edu/folder/folder/file.ext). The Dependency Manager does not create page relative links (although it can read and convert them into dependency tags when the site is scanned). The Dependency Manager will create either root relative or absolute URL links when pages are published based upon what the current access setting for URLs is for each page.

Publish Threshold

The Publish Threshold setting defines the maximum number of pages to be auto-published when an asset is republished or a page is moved or renamed when Dependency Manager is being utilized. If the threshold is set to 0, there is no limit on the number of pages that can be auto-published. If a different limit is set, and publishing the asset, or renaming or moving a directory or page will require more pages to be published than allowed, an administrator will have to publish the asset or make the change to the directory or page.

About Unpublished Dependencies

The unpublished dependencies publish option is available with a site, directory, or page publish, and lets a user choose whether or not to include in the publish any additional files that the page is dependent upon for content. This applies if the additional content has not yet been published to the target server. For example, if Page A has been created but not yet published, and Page B, which is being published, links to it, selecting to publish the unpublished dependencies will ensure that Page A is also published. This also extends to any binary files that have been inserted on a page, but not yet published to the production server.

This action prevents broken links from existing on the current page being published. This checkbox at publish time is only shown if the Dependency Manager is being used on the site, dependency tags are used in the page being published, and one or more of those dependency tags refer to content that has not yet been published to the target server.

S-Tag and Triggered Publish

The S-tag uses the dependency tag syntax, is preceded with s: instead of d: or f:, and is accessible through file choosers, which are commonly used in the parameters of a page. When using the tag on a page, that page executes a triggered publish when the source file is republished. The XSL can use the path generated by the tag to display content being maintained on a different page. This is similar in concept to an include file or an asset. When the original file is updated, the page containing the content is also published automatically. One example of how this is utilized is when a mobile page uses content from the main web site. When the content on the main web site is updated and published, the mobile page is also published with the updated content.

Renaming or Moving a Directory or File

Dependency Manager maintains the correct link association when files or directories are moved or renamed. All the files that link to a moved or renamed file or directory are automatically republished to maintain the correct link.
When a file or directory is either moved or renamed, a prompt that all dependent pages will be republished will appear. This will republish the page based on the current version of the page on the live production server with the new dependency links. If changes have been made but not published to the live site, those changes will not be published to the live production server, but will be available in OU Campus and still saved on the staging server. This includes backed-up versions.

**About HTTP Root**

If HTTP Root is changed in the site settings, the entire site should be republished to ensure the links are updated. The HTTP Root setting is used to indicate the location of the site on the web server as accessed through HTTP and should usually correlate to FTP Home or FTP Root.

**File Types**

Before a file is scanned, OU Campus determines if a file contains HTML according to file extension. The Dependency Manager scanner utilizes this information to determine if a file contains HTML. The list of extensions that determine if a file contains HTML is as follows:

- .html
- .htm
- .xhtml
- .shtml
- .shtm
- .jspx
- .php
- .php3
- .phtml
- .asp
- .chtml
- .cshtml
- .dna
- .cfm
- .inc
- .aspx
- .mht
- .ssi

**Dependencies Reporting**

When utilizing Custom Reports to produce a Products or Assets report, the report lists the dependency tag for the content. The reports also include a list of subscribers to the dependency.

**Broken Links**

If content is deleted, a broken link is created. The system has various indications for broken links. Dependency Manager provides informative reporting for broken links and broken assets. When a dependency is lost, such as a linked-to page or a subscribed-to asset is deleted, the dependency tag, path, and file name are shown within asterisks, e.g. *** Broken f:1234 /training/about/filename.html***.

Broken links are reported in the following locations:

- WYSIWYG Editor
- Page-based Link Check
- Publish-based Link Check
• Site Check
• Custom Reports
• Broken Pages

With Recycle

If a recycle bin has been set up for the site, when recycling a file, a prompt indicates how many links will be broken if the page is recycled. Keep in mind that the warning will not appear prior to deleting a directory or file if the recycle bin has not been configured. After the file is recycled, the system displays the pages have broken links as a result.

With Source Editor

Source Editor reports any broken links within the source code by highlighting the relevant dependency tag red.

Within the WYSIWYG Editor

OU Campus provides a visual indication that a link is broken within the WYSIWYG Editor as well. It includes the note that the link is broken, the actual tag, and the file name with path that is being linked to. To view this, position the cursor on the link or select the link, and click Insert/Edit Link. The notification is displayed below the Link URL field.
Additional Scenarios and Considerations

When a directory with dependency tags pointing to files within the same directory is copied, the links in the files of the copied directory either have to be manually updated or OmniUpdate Customer Support can be contacted to help with this scenario.

This may include:

1. Copying a directory to create a new directory within the same site with the same starting content.
2. Copying a directory’s files to convert it into a new site.

To take a directory from an existing site that is using dependency tags and make it into a new site of its own (e.g., http://www.college.edu/athletics/ is to become http://athletics.college.edu/), specific steps must be taken to obtain the desired outcome. It is important to note that most of the following steps are necessary for this process with sites that do not use dependency tags. The instructions below add the steps needed when Dependency Manager is used on the source site.

1. Perform the process during a downtime (evening or weekend).
2. In the Setup > Sites view, select the Revert tool to remove all dependency tags from the source site.
3. Use the Zip Export tool to download a copy of the site from OU Campus.
4. Create the new site record the same way sites are normally created in OU Campus.
5. On the workstation being used, open the exported zip file and extract the folder desired to be the source of the new site.
6. Create a new zip file of just the directory that is the origin of the new site.
7. In the new site in OU Campus, from the top Content > Pages view, use the Upload tool to import the zip file just created (select the Ignore containing folder check box of the Zip Import, if there is one).
8. Once the files are uploaded, on the new site use the Find and Replace from the Content menu to search for the paths that have the containing folder, which was ignored upon import, and remove the now incorrect folder name (e.g., Find: /athletics; Replace with: /).
9. Use the Find and Replace to correct the links from the new site to the source site, usually found in header and footer navigation and links (e.g., any paths that are not on the new site, such as /admissions... would become http://www.college.edu/admissions...).
10. On the source site, use the Find and Replace from the Content menu to search for the paths that have the now removed folder and change them to the new site URL (e.g., Find: /athletics...; Replace with: http://athletics.college.edu/...).
11. Use the scan tool from Setup > Sites view to scan the new and old sites to create new dependency tags for each site.
12. On the source site, delete the now obsolete /athletics... directory.
13. If any URL paths were missed in step 10, any pages on the source site with links to the now deleted directory are shown via Reports > Required Actions > Broken Pages list view.
14. Fix the pages listed in the Broken Pages report; the two sites will now have correct dependency tags for each site and for sites within the account.
15. Populate the new site’s Production Server with any needed binaries to support the new site.
16. Continue to setup and configure the new site as would be done for any other site.

For questions regarding this process, or to have only the individual directory being copied reverse scanned (Revert), contact Support.

Important Information and Reminders

1. Dependency Manager tracks and updates links within the following file types and extensions:
   - PCF: .pcf
   - XML: .xml
2. Dependency Manager does not track binary files, such as images (with the exception of those that are products of a PCF), unless Binary Management is enabled. Without Binary Manager, any changes such as file moves or renaming to binary files, with the exception of those that are products of a PCF, will require that any links be updated manually. Otherwise, Dependency Manager works with anything editable from within OU Campus or generated by an editable file from within OU Campus.

3. Dependency Manager does not track links to pages or sites not under management by OU Campus. This also applies to sites that are not in the same account as the current site under OU Campus management.

4. The Dependency Manager is account-bound and can only track and manage URL changes to pages or directories that are within sites in the same OU Campus account.

5. To utilize dependency tags when using the file choosers, "dependency=yes" needs to be entered into the filechooser parameter or variable tag.

Example:

```
<variable name="leftnav_include" prompt="Left Nav" alt="Choose your left nav" type="filechooser" path="/includes/navs" dependency="yes">/includes/navs/default.html</variable>
```

6. As a best practice, it is suggested that a complete site export be completed on each site prior to activating Dependency Manager to allow for an immediate and complete reversal via Zip Import if the end result is not desired.

7. If a directory or file is uploaded or deleted via FTP, run the scanner on the affected directories or entire site to avoid publishing issues.

8. The following regex can be used to see which links have been replaced with Dependency tags: `\{\{\[fd\]: \d+\}\}`

9. The Dependency Manager supports linking from within assets; dependency tags can be added when creating and editing assets, and when inserted on a page the tag is honored.

10. Dependency Manager links are case sensitive. As such, it is advised that paths for links to pages managed in OU Campus are always inserted using the browse functionality.

11. Dependency Manager inserts dependency tags into `<a>` and `<link>` tags for the href attribute automatically, both when the Dependency Manager scanner is run and when new links are created. However, tags can be manually included elsewhere as desired.

12. Dependency Manager will not automatically add dependency tags to any other types of tags, including PHP, ASP, and JavaScript.

    Important Exception: Dependency tags cannot be placed within processing instructions or the prologue, the instructions prior to the opening XML comment. Entering in dependency tags within these will cause an error as the page will not be able to be rendered.

13. Dependency Manager renders root relative links (i.e., `/directory/page`) and absolute links (i.e., `http://www.college.edu/directory/page`), depending on the site settings. The rendered URL to the production site cannot and will not be page relative (i.e., `../page`).

14. If there is production side processing that requires certain formatting of paths, be aware of how the paths will render and either avoid using Dependency Manager where it might be adversely affected or change the production side processing.

    If page relative URLs currently exist on any of the pages and it is required that they remain page relative, the Dependency Manager scanner should be run on a per directory basis, not a site-wide basis.

    If page relative URLs are required going forward, these will need to be added manually without using the WYSIWYG Editor and Source Editor browse functions or the file chooser.
If the HTTP Root setting is changed in the site settings, the entire site should be republished.

15. Run the Dependency Manager scanner if a page to which others are dependent is restored from the Recycle Bin, or if a directory or file is uploaded or deleted via FTP/SFTP/WebDAV.

The scan can be run on only the affected directory or directories.

16. The Revert scan is not reverting the site to its state prior to Dependency Manager being utilized. It is replacing the dependency tag with the root relative or absolute URL, dependent on the site settings.

17. Dependency Manager will not scan or update files within the following folders:
   - OMNI_RESOURCES at root
   - OMNI_ASSETS at root
   - Recycle Bin (if defined) at root
   - OMNI_INF at all levels

18. OU Campus does not contain any tracking of which sites have been scanned. If this is desired, it is recommended that it be completed internally.

19. Reporting is available with details on which dependency tags refer to which pages, and which pages are currently subscribing to those pages.

20. Dependency tags will not be referenced in the Custom Reports if the page or directory was deleted.

21. Dependency tags are supported across publish targets, if Multi-Target Publish is being utilized.

**Final Notes**

Please be sure to read the Dependency Manager White Paper prior to contacting Support. It contains information on the benefits, limitations, and considerations.
Binary Management

Overview

Binary Management expands web content management to binary files including photos, videos, and PDFs. One can manage binary files directly from the OU Campus staging server by scheduling future publishing times, setting binaries to expire, versioning, and setting up approval systems. In addition, Dependency Manager handles the renaming of binaries across the entire website, making it easy to apply site-wide changes from a single location.

Prior to the introduction of Binary Management, binary files were uploaded directly to the production server, offering no direct control over when they were made available for public viewing. Binaries were not managed by Dependency Manager, which meant that if a file was renamed, moved, or deleted, all links pointing to it were broken until a site check was run or someone identified that the link was broken. This had to be performed on a page-by-page basis. With the introduction of Binary Management, binary files are treated like all other files managed by OU Campus, offering many advantages to both users and administrators.

About File Choosers and Binary Management

In previous versions of OU Campus, including version 9, the default behavior was to access the production server when using a utility to choose a page or file.

OU Campus version 10 now has Binary Management enabled for an account, and it can be turned on for each site. The default for Binary Management to use the staging server, so that files, pages, and images will always default to staging, and the location that is linked to is the staging instance for all file choosers.

It is possible to override the default and switch to the production server, auxiliary site, or publish target, and choose from any of those locations.

When linking to an instance on staging, upon transformation, the Dependency Manager works behind the scenes to provide the appropriate link to the corresponding instance of the item on the production server or publish target.

Note for version 10.1.0: Pass-through ability is slated to be added for users that are not members of the group whose members have access to edit an item. This will provide the ability to link to it or include it on a page. Currently, a user can navigate to production and select it, but that will become seamless and available via staging.
Sites

Overview

From the Setup menu, Level 10 administrators can view and edit the configured sites in the account. The Setup menu can be viewed as the main configuration area for many of the features within the OU Campus CMS. By navigating to **Setup > Sites**, an administrator can create a new site or modify an existing site, as well as view and utilize site actions on the Sites screen.

Sites List View

The Sites list view shows all of the sites for an account. From this view, an administrator can:

- View the number of sites in an account
- Filter the list of sites by site name or URL
- Create a new site
- Edit site settings for an existing site
- Sort the existing sites by site name, URL, or date/time that content within the site was saved
- Hover to access the Options menus
Creating a New Site

A new site record can be created by clicking the **New** button. This creates the site record and allows the administrator to configure the appropriate settings. Two settings for LDP and Auxiliary Sites become available and may be edited after the site record is saved.

Once created within the system, files can be uploaded via the interface singularly or with a zip file that keeps the file structure intact, if so desired. Another method to create a new site is to use site clone, which allows for the site record to be copied with or without also copying the files from the cloned site.

For more information, visit the Site Settings page.

Options Menu and Site Actions

Hovering over the site row will reveal menu options under the Options column heading. The options include:

**Edit Menu**

- **Site**: Edit site settings.
- **Site Access**: Edit access settings at the site level (similar to the Access Settings modal for pages or directories)
- **Asset Access**: Configure access settings for assets on the site.

**Publish Menu**

- **Publish Site**: Publishes the entire site and all files currently inside it. By default, only checked-in files are included in site publish, though this option may be changed.
- **Publish Sitemap.xml**: Publishes a sitemap XML document.

**Scan Menu**

- **Dependency Scan**: Scans entire site for links and dependencies, and syncs the staging server with the database. If Dependency Manager is turned on, it will replace links to dependencies with dependency tags. For more information, please visit the Dependency Manager page.
- **Revert Site**: Reverts all dependency tags on the site to their root-relative links.

**Actions**

- **Clone**: Clones the site.
- **Save Version**: Saves a version of every page and file on the site.
- **Initialize**: Adds a DirectEdit button on every page in the site.
• **Purge Staging Binaries**: Only available if Binary Management has been activated in the past and is currently disabled. Removes all binary files from the staging server. Does not delete files from the production server.

• **Export as Zip File**: Exports the entire site as a ZIP file.

• **Delete**: Deletes the site.

For more information about the site actions available under the Options table heading, visit the Sites Actions page.
Site Actions

Overview

While on the Sites screen, administrators can perform various functions on sites that have already been configured in the account. These functions become visible under the Last Save/Options table heading when a user hovers over the site row.

The available options are as follows:

- **Edit**
  - Site
  - Site Access
  - Asset Access
- **Publish**
  - Publish Site
  - Publish Sitemap.xml
- **Scan**
  - Dependency Scan
  - Revert Site
- **Actions**
  - Clone
  - Save Version
  - Initialize
  - Purge Staging Binaries
  - Export as Zip File
  - Delete
<table>
<thead>
<tr>
<th>Icon</th>
<th>Text</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![Map Marker Icon](image) | **Site** | Brings the administrator to Site Settings, where site information can be edited. Site Settings includes the following panels:  
- Site Information  
- Production Server FTP Settings  
- DirectEdit Button  
- Site Preferences  
- Publish Settings  
- WYSIWYG Editor  
- File Naming  
- Binary File Naming  
- LDP Settings  
- Auxiliary Sites  
- Optional Features  
Users can also reach the Site Settings screen by clicking on the linked site name in the Sites list view. |
| ![Key Icon](image) | **Site Access** | Brings up the Site Access Settings modal, where administrators can modify access settings at the site level. Options include:  
- Recursive Modification  
- Access Group  
- Approver  
- Enforce Approver  
- Bypass Approval  
- Template Group  
- Extensions (allowed/disallowed)  
- Toolbar  
- RSS Feed  
- URL Type  
- Exclude from Search  
- Exclude from Sitemap.xml  
- Directory Variables  
Changes may be made independently and recursively. Recursive modifications are made to all items even if checked-out by another user or in workflow, and retain their |
Asset Access

Used to modify the asset access settings at the site level, which include:

- Recursive Modification
- Access Group
- Available To
- Approver
- Enforce Approver
- Bypass Approval
- Asset Creation Access

With the exception of creation groups, settings can be applied recursively. Recursive modifications are made to all existing assets, even ones checked out by another user or in workflow. Modifications made to these assets will not alter their status.

Scan Menu

- Dependency Scan
- Revert Site

Runs a scan to synchronize the database with the files on the staging server. If Dependency Manager is enabled, the scan will also identify the valid paths the Dependency Manager scanner can convert within the
<table>
<thead>
<tr>
<th>Icon</th>
<th>Text</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td><strong>Revert Site</strong></td>
<td>Revert is only available if Dependency Manager is enabled for the account. Performing a reverse scan converts all dependency tags to root relative links or absolute links, depending on the site settings. If necessary, this should only be done during off-peak times, such as evenings or weekends. This scan can take up to 1 or 2 hours for a large site.</td>
</tr>
</tbody>
</table>

**Publish Menu**

<table>
<thead>
<tr>
<th>Site</th>
<th>URL</th>
<th>Last Save/Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>gallea-sandbox</td>
<td><a href="http://bscheirman.oudemo.com/">http://bscheirman.oudemo.com/</a></td>
<td><img src="image" alt="Publish Site" /></td>
</tr>
</tbody>
</table>

Display 100 rows per page
<table>
<thead>
<tr>
<th>Icon</th>
<th>Text</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![Publish Site](image) | Publish Site | Publishes all files currently saved on the staging server and pushes them to the production server, which by default includes checked out files. Options for a site publish include:  
- Checked-in Files Only  
- Use Last Published Version  
- Changed Files Only  
- Exclude Binary Files  
- Also Include Unpublished Dependencies  
- Publish Target (if Multi-Target Publish is in use, an alternative publish target may be chosen)  
- Version Description is added to all pages |
| ![Publish Sitemap.xml](image) | Publish Sitemap.xml | Generates an XML file with the paths to the pages that are within the site. It is possible to exclude pages and directories by using access settings. |

**Actions Menu**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Text</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Clone" /></td>
<td>Clone</td>
<td>Clone creates a copy of the site settings to help in the creation</td>
</tr>
<tr>
<td>Icon</td>
<td>Text</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td><img src="image" alt="Copy Icon" /></td>
<td>of a new site. By default, only the site settings are copied; the files within the site are not copied. Selecting the Include Staging Files checkbox copies files from the source to destination site. Items that do not get copied include assets, trash folder, archives, access settings, directory variables, etc. If the destination site has Dependency Manager turned on, the dependency links are updated to point to links on the cloned site. If there are links that point to a separate site, those are left the same. Asset linking is unchanged and continue to point to the original asset.</td>
<td></td>
</tr>
<tr>
<td><img src="image" alt="Save Version Icon" /></td>
<td>Save Version</td>
<td>Creates a backup of the entire site to the versioning system. A new version of each page is added to the version list of each page. When performing a commit at the site level, the account name is notated as the user in the version list.</td>
</tr>
<tr>
<td><img src="image" alt="Initialize Icon" /></td>
<td>Initialize</td>
<td>Initialize adds a DirectEdit button or updates the last modified date within the DirectEdit button to all pages on the staging server. If using the last modified date link for the DirectEdit button, doing this sets all pages on the staging server to have the current date. Using this does not affect the files on the production server unless the site is published.</td>
</tr>
<tr>
<td><img src="image" alt="Purge Staging Binaries Icon" /></td>
<td>Purge Staging Binaries</td>
<td>Removes binary files (images, etc.) from the staging server. When Binary Management is enabled, files that are not maintained in OU Campus, such as images, media, PDFs, and documents are uploaded directly to the production server.</td>
</tr>
<tr>
<td>Icon</td>
<td>Text</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td><img src="image1.png" alt="Icon" /></td>
<td>This feature removes files that are considered of a binary file type from the staging server. This function does NOT affect or delete any files on the production server. If Binary Management was enabled at one time and then disabled, Purge can be used to remove any binary files still extant on staging. This command is only available when Binary Management is disabled for a site.</td>
<td></td>
</tr>
<tr>
<td><img src="image2.png" alt="Icon" /></td>
<td>Export as Zip File</td>
<td>Exports the entire site as a .zip file to the local workstation being used. This export does not contain the past versions of pages or any access settings for directories or files. The export does not include binary files that are on the production server. The export only contains files on the staging server. It is advisable and can be useful to perform a Dependency Manager revert on the site prior to export. After exporting, re-scan the site to have the dependency tags re-added.</td>
</tr>
<tr>
<td><img src="image3.png" alt="Icon" /></td>
<td>Delete</td>
<td>Deletes the site from the site list, deletes the site record, and the database records. The site can be restored if the same site name is used (as all the files still reside on the staging server), but the database information, permissions, dependencies, etc., will no longer exist. Files are not deleted from the production server or any publish targets.</td>
</tr>
</tbody>
</table>
Revert

Revert Scan

It is possible to conduct a Revert scan on any site that has been previously scanned. It is important to note that a Revert scan is not a revert process. It does not restore the pages, nor the links, to their states prior to the initial scan. Instead it replaces the dependency tags with root relative URLs (e.g., `/folder/file.html`) or absolute URLs (e.g., `http://www.college.edu(folder/file.html)`), depending on the site settings.

To conduct the Revert scan:

1. Navigate to **Setup > Sites**.
2. Hover over **Scan** on the site row and choose **Revert** from the drop-down menu.
3. A prompt will appear confirming that the intended action is to have the dependent tags removed and all dependent links converted to root relative or absolute URLs, depending on the site settings. Click **OK**.
4. At the start of the revert, a notification is shown indicating that the site is being reverted. This notification can be closed, and the **Sites** screen can be navigated away from. A new notification displays wherever the administrator is in the CMS once the scan has been completed.

5. Once completed, a notification is displayed indicating that the site has been successfully reverted.
Publish Sitemap.xml

Overview

Location: Setup > Sites > hover > Publish menu > Publish Sitemap.xml

Authority: Level 10 administrator

A site map can be generated for use with Google’s indexing and other web services that use an XML source file for a sitemap. The Publish Sitemap.xml generates an XML file, which can then be reused to create a site index, submitted to Google, or used in another fashion as determined by the site's designers and administrators.

Regenerating a site map overwrites the existing sitemap. The administrator should ensure that any pages that should not be included in indexing, such as references to template and navigation files, be excluded from the site map generation prior to using the Publish Sitemap.xml command.

Generating a Site Map

A Level 10 administrator can generate a sitemap.xml.

1. Navigate to Setup > Sites.
2. Hover and from the Publish menu on the site row and select Publish Sitemap.xml.

3. Click OK. The XML file called sitemap.xml is created at the site root /sitemap.xml on the production server.
4. When the action has completed, the notification includes a link, which can be used to view the generated sitemap XML file.

The provided URL can then be submitted to Google, or otherwise used.

Excluding Files, Directories, and Assets

It is possible for a Level 10 administrator to choose specific files, entire directories, and assets that should be excluded from the sitemap creation. The Exclude From Sitemap options are available in the corresponding access settings.

If all files within a directory or site should be excluded, use the recursive option Apply Selected Settings to This Folder and All Enclosed Files and Folders. Make sure to select the checkbox for this option to be applied recursively as well as the radio button for Yes to indicate to exclude files and directories.

This example uses the recursive option for a directory.
1. From a Pages list view, hover over Edit for a directory and select Access.

2. Under Recursive Modifications, select Apply Selected Settings to This Folder and All Enclosed Files and Folders.

   Access Settings - faculty

   Recursive Modification
   - Apply All Settings to This Folder Only
   - Apply Selected Settings to This Folder and All Enclosed Files and Folders

   Recursive modification does not apply to directory variables, directory variables are always inherited.

3. Select the checkbox for Exclude From Sitemap.

4. Select the Yes option.
5. Click Save.

Note: Exclusions should be made before generating a sitemap.
Clone

Overview

One of the available site actions is the Clone feature. The Clone feature can be used to help create a new site. When using Clone, just the site record can be cloned, or the site record and the site staging files can be cloned. Level 10 administrator privileges are required to use the Clone feature as it is available in Setup > Sites.

Once the clone action has been started and the site record is cloned to start with, but not yet saved, all of the panels that are available when creating a new site are available. However, the LDP Settings and Auxiliary Sites panels, as well as the UUID and public key information, are not available until the record is saved, which is similar to new site creation. When cloning a site, it is necessary to change the Production Server FTP Settings in order to not overwrite existing information that has already been published to the web server. The combination of HTTP Root, FTP Root, and FTP Home must be unique within the account.

For more information, visit the Site Settings page.

Copy Staging Files

When cloning, staging server files can also be copied to the newly cloned site by selecting the Copy Staging Files checkbox. All the files seen in a Content > Pages list view get copied.

<table>
<thead>
<tr>
<th>Feature/Functionality</th>
<th>Clone Site Record</th>
<th>Copy Staging Files</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staging Server Files</td>
<td>No</td>
<td>Yes</td>
<td>Everything from Content &gt; Pages</td>
</tr>
<tr>
<td>Production Server Files</td>
<td>No</td>
<td>No</td>
<td>The site-level OMNI-INF is not copied.</td>
</tr>
<tr>
<td>OMNI-INF</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Binaries</td>
<td>No</td>
<td>Yes, if Binary Management is enabled on the original site.</td>
<td>If the original site has Binary Management on and the target clone does not, binary files are still copied to staging. The Purge tool can be used to delete binary files from staging if Binary Management will not be used on the cloned site.</td>
</tr>
<tr>
<td>Dependency Tags</td>
<td>No</td>
<td>No</td>
<td>The site files are cloned, the dependency tags for the site are reverted, and then the site is rescanned, producing new dependency tags.</td>
</tr>
<tr>
<td>Recycle Bin Location</td>
<td>Yes</td>
<td>Yes</td>
<td>This is a site setting.</td>
</tr>
<tr>
<td>Feature/Functionality</td>
<td>Clone Site Record</td>
<td>Copy Staging Files</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------</td>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Recycle Bin Contents</td>
<td>No</td>
<td>No</td>
<td>Must register site if using LDP Forms</td>
</tr>
<tr>
<td>LDP Registration</td>
<td>No</td>
<td>No</td>
<td>Any feeds defined via Content &gt; RSS are not cloned.</td>
</tr>
<tr>
<td>RSS Feeds</td>
<td>No</td>
<td>No</td>
<td>Access settings are not cloned.</td>
</tr>
<tr>
<td>RSS feed assignments</td>
<td>No</td>
<td>No</td>
<td>The XML feed files are not on staging and no files are copied from production. Note: if the directory that contains the rss feed was created with the creation of the rss feed on the originating site, the cloned site will not necessarily have that directory on staging.</td>
</tr>
<tr>
<td>RSS Feed XMLs</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>RSS Groups</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>RSS Items</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Snippets and Snippet Categories</td>
<td>No</td>
<td>No</td>
<td>Any source files in the file structure is cloned, but the snippet configuration is not.</td>
</tr>
<tr>
<td>Reports such as the Checked Out Content Report</td>
<td>No</td>
<td>No</td>
<td>Report information is not cloned, but the Recent Saves report will immediately display the cloned files as saved.</td>
</tr>
<tr>
<td>Assets</td>
<td>No</td>
<td>No</td>
<td>Assets are not cloned. Assets are created within a site, but available for an account, unless the Lock to Site checkbox is selected. A page subscribed to an asset remains subscribed to the original asset on the original site. Asset linking is unchanged.</td>
</tr>
<tr>
<td>Feature/Functionality</td>
<td>Clone Site Record</td>
<td>Copy Staging Files</td>
<td>Notes</td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>-------------------</td>
<td>-------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>and continues to point to the original asset with a dependency tag reference; however, asset linking is supported across sites within an account.</td>
<td></td>
<td></td>
<td>No database settings are cloned. (For example: access settings, directory variables, snippets)</td>
</tr>
<tr>
<td>Database Settings</td>
<td>No</td>
<td>No</td>
<td>No database settings are cloned. (For example: access settings, directory variables, snippets)</td>
</tr>
<tr>
<td>Access Settings (all)</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Snippets</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Directory variables not cloned</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Find and Replace Last Replace Results</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>File Locks (including checked out files, scheduled actions and workflow)</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Versioning</td>
<td>No</td>
<td>No</td>
<td>Previously published versions and committed backups are not included in the cloning.</td>
</tr>
<tr>
<td>Account-bound items are available for all sites: Users, Groups, Toolbars, Font Size Sets, Gadgets/Custom Gadgets, Google Analytics, Add-Ons</td>
<td>No</td>
<td>No</td>
<td>Are not cloned, but are still available within the new site as they are account-bound items. Gadgets with site-specific information will not include old site’s history such as for My Checked-Out Content or Activity. Images may include default paths.</td>
</tr>
<tr>
<td>Templates</td>
<td>Yes</td>
<td>Yes</td>
<td>Location setting, and template files at the site level are cloned if they are stored in a local</td>
</tr>
<tr>
<td>Feature/Functionality</td>
<td>Clone Site Record</td>
<td>Copy Staging Files</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------</td>
<td>--------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>staging folder (which is used by default).</td>
</tr>
<tr>
<td>Template Groups</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Facebook Pages Setup</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Twitter Account Setup</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Default Tweet/Wall Post</td>
<td>Yes</td>
<td>Yes</td>
<td>Part of the site record.</td>
</tr>
</tbody>
</table>

**Cloning a Site Record and Files**

The length of time required to clone site files is dependent upon the size of the site in terms of number of files and file sizes. A particularly large number of media files large in size could possibly take a considerable amount of time to clone.

It should be noted that any use of the Site Clone tool (with file copy) should only be done when all users are logged out. The source site and its files, folders, and access settings are not affected by the use of the Site Clone tool.

Once the clone action is initiated successfully, a notification is provided that transmits the message that the file copy was initiated. By and by, when the clone action has completed, another notification is displayed with a message of success.

1. Navigate to **Setup > Sites**.
2. Hover over **Actions** on the site row and click **Clone**.

3. Create a unique **Site Name**. This identifies the site being edited. It is also the file name of the folder that contains the sites files on the staging server. A Site Name cannot include spaces, but can include uppercase and lowercase letters, numeric values, hyphens, and underscores. It also should not include duplicated names even if the letter case is different. In other words, www and WWW would be an example of a duplicated name. **Note**: Keep in mind that when a site is set up within a subfolder (e.g., http://www.college.edu/admissions) and there will also be a site at the domain (e.g., http://www.college.edu/), it may happen that users create folders within the main domain site that overwrite the contents of the other sites contained within the subfolder. Use caution when setting up this type of site structure.

4. In the **Site Information** panel, select the **Copy Staging Files** checkbox in order to also copy the site files and directories. Otherwise, leave cleared to just copy a site record.
5. The following three fields must form a unique combination. Together they are combined to build the URL:

- **FTP Root**: Where the files are served from. For example, /public_html. A trailing slash should **not** be used.
- **HTTP Root**: The URL root of the website. A trailing slash should be included, eg. http://www.college.edu/. If a path exists in the **FTP Root**, that path must match the **HTTP Root**. For example, if the **FTP Root** is /site then the **HTTP Root** would be http://www.college.edu/site/. If the **HTTP Root** changes, the entire site will need to be republished.
- **FTP Home**: The **FTP Home** and the **HTTP Root** form the URL for the Dependency Manager links. **FTP Home** should be configured as a subdirectory of **FTP Root**. For example, if the **FTP Root** is /public_html, **FTP Home** could be /public_html/art.

6. The Dependency Manager honors both the source and the clone settings. When cloning, it is not necessary to manually revert/rescan for dependency tags. The Dependency Manager will manage the creation of new dependency tags for the cloned site by reverting and rescanning. Links among sites within an account are maintained. The Dependency Manager settings can also be used to take absolute links from the source site and have them scanned into Dependency Manager links on the clone site.

7. Click **Save**. The **Clone** feature does not clone the following items in the site record, but are available after save.
   - Public Key
   - LDP Settings
   - Auxiliary Sites/Publish Target

These settings are always unique to the site and are not duplicated between sites.

**Additional Steps to Go Live**

The following steps will need to be performed similarly to new site creation:

- **Quick Search**: After cloning, it is necessary to build the index for the Quick Search in the site record for the new site (Setup > Sites > Edit for the site > Options > Quick Search).
- **Site Publish**: When using Copy Staging Files to clone files, it is necessary to publish the entire site to the production server. All files can be published from Setup > Sites > Publish > Publish Site.
- **Initialize**: Initialize adds a DirectEdit button to each page that is missing one. **Site Access** settings and any directory variables for the site may need to be reconfigured. Administrators Only is set as the **Access Group** by default.
- Any internal absolute paths pointing to the old domain name would need to be fixed. For example, if dependency tagging wasn’t in place for an URL and http://www.exampleSchool.edu/about/index.html was used in a link, it would need to be updated. If the cloned site is at: http://artcollege.exampleSchool.edu/about/index.html, then the hard-coded link would now be incorrect.
• If the clone was created by adding an appending an additional directory to the domain and site-root relative paths were used in include files (or other pages) rather than dependency tags, then the paths need to be updated. For example, `/about/index.html` would need to be `/clone/about/index.html`.

The Find and Replace feature can be used to selectively fix changed paths.

**More About Dependency Manager and Site Clone**

The use of absolute or relative links should be considered when cloning a site. The functionality of the site clone when using the file copy option honors both the source site’s and the clone site’s Dependency Manager settings. The Clone feature can smartly revert scan and rescan Dependency Manager links to update the Dependency Manager tags. The Dependency Manager settings can also be used to take absolute links from the source site and have them scanned into Dependency Manager links on the clone site.

**Use Case Examples for Dependency Manager Settings**

The scenarios below illustrate the result of a clone with the various options of Dependency Manager settings and for whether the site setting for URLs is absolute or root relative.

*Source Site Dependency Manager On, Clone Site Dependency Manager On*

![Diagram](image)

When Dependency Manager is enabled for both source site and clone site, the following occurs:

1. The source files are copied to the new site.
2. Dependency Manager performs a Revert scan of the tags.
3. Dependency Manager re-scans the cloned site using the settings for URLs, absolute or root relative. The end result is a cloned site with Dependency Manager tags that are all local to the clone and not pointing to the source site.

**Source Site Dependency Manager On, Clone Site Dependency Manager Off**

![Diagram showing source site dependency manager enabled, clone site dependency manager disabled, resulting in no dependency tags.]

When Dependency Manager is enabled for the source site and off for the clone, the following occurs:

1. The source files are copied to the new site.
2. Dependency Manager performs a Revert scan of the tags. The scan uses link formats based on the cloned site’s settings for URLs (absolute or root relative).

The end result is a cloned site with no Dependency Manager tags. All URLs are absolute or root relative to itself and not pointing to the source site.
Source Site Dependency Manager Off, Clone Site Dependency Manager On

When Dependency Manager is disabled for the source site and enabled for the clone, the following occurs:

1. The source files are copied to the new site.
2. The Dependency Manager scanner creates links on the cloned site as specified by the cloned site's settings for URLs (absolute or root relative).

The end result is a cloned site with Dependency Manager tags that may or may not all be local to itself. Any pre-existing local Dependency Manager tags will remain pointing to the source site (see Edge Case #2 below).

Source Site Dependency Manager Off, Clone Site Dependency Manager Off

When Dependency Manager is disabled for both source site and clone site, the following occurs:

1. This only copies site files.
2. No Dependency Manager scanning of any kind occurs.
3. A true copy of the source site is made.

The end result is a cloned site without any action being taken for Dependency Manager tags. Any existing Dependency Manager tags are copied as is and will continue to point to where they pointed before they were cloned.
All URLs in whatever form (absolute or root relative) point to itself and not to the source site. Any pre-existing absolute URLs that pointed to the source site will remain pointing to the source site (see Edge Case #1 below).

**Note for all use cases:** Any Dependency Manager tags that exist in the source site that point to web sites other than the source will continue to point to those other sites from the clone no matter what combination is used. The same is true for Asset tags, the asset tags will continue to point to the proper asset.

No matter what combination of setting mentioned above is used, there is one common scenario that will require the admin to do some post processing after the site is cloned. If the source site contains absolute URLs pointing to any binaries on the source site’s production server, the admin will need to use the Global Find and Replace feature on the cloned site. This is to take into account the different HTTP Root to correct all the binary absolute URLs (if they need to be pointing to the cloned site’s HTTP Root). This is because URLs pointing to binaries are not under Dependency Manager control and are not changed as part of the Site Clone’s file copy function.

For more information about Find and Replace, visit the Find and Replace page.

There are also two edge cases that could require the administrator to do some pre- or post-processing depending on the state of the source site and the expected result for the cloned site.

**Edge Case #1**
In this scenario, the source site has absolute URLs and Dependency Manager is off, and the admin wants Dependency Manager to remain off for the cloned site and still use absolute URLs.

The cloned site would have absolute URLs that point to the source site.

An administrator would need to either use the Global Find and Replace to correct for the cloned site’s HTTP Root to correct for all the link URLs incorrectly pointing to the source site.

Alternatively, the admin should set the Dependency Manager setting for the clone to be turned on before clicking Submit to start the clone procedure. When it is complete the admin can use the Revert feature to un-scan the Dependency Manager tags back into absolute URLs.

**Edge Case #2**
In this scenario, a site clone is made when the source site’s Dependency Manager setting is off, but the source site contains Dependency Manager tags that point to pages on the source site.

These Dependency Manager tags will be preserved in the cloned site, and they will continue to point to the source site’s page URLs. This is on purpose, as there are cases where this is the intended or required result of a site clone procedure. If this is not the intended result, the administrator needs to be sure to turn the source site’s Dependency Manager setting on before the site clone tool is used. Once the site clone process is complete the admin can reset the source site’s Dependency Manager setting to off.

**Use Case Examples for Site Settings**

**Example 1**
A university with a domain of gallena.edu would like to create a site at a subdomain for the art department, art.gallena.edu.

The OU Campus level 10 administrator could use the following settings:

**Site Name:** art
Server: art.gallena.edu

FTP Root: /public_html

HTTP Root: http://art.gallena.edu/

FTP Home:

The URL is http://art.gallena.edu/ and the FTP Home can be left blank. Logging in via FTP, the user would be putting files to the FTP Root.

Example 2

In another example, the Art Department at Gallena University would like to create a site for the ceramics course of study.

The administrator could use the following settings:

Site Name: ceramics

Server: art.gallena.edu

FTP Root: /public_html/ceramics

HTTP Root: http://art.gallena.edu/ceramics/

Best Practices

• The combination of HTTP Root and FTP Home creates the URL (the public_html directory is not shown in the URL).
• The FTP Home should be a subdirectory of FTP Root.
• If FTP Root is different from the default of what the cloned site was using (i.e., public_html) and not using local templates, then the path for templates needs to match also. For example, if FTP Root was changed to /public_html/art then the path to the template directory would be /public_html/art/_resources/ou/templates.
• The cloned files on staging need to be published.
• Users should not be active in the site during cloning.
Site Information

Overview

The Site Information panel provides read-only access to the site name, UUID, and public key, and includes the ability to re-generate the site’s public SSH key. The UUID and public key are automatically generated during the creation of the site record and are viewable after the site settings have been saved.

Site Name

This is the name given to identify the site being edited. It is also the filename of the directory that contains the files for the site on the staging server. This cannot be changed once defined during site creation and should be unique to the account.

A site name cannot include spaces, but can include uppercase and lowercase letters, numeric values, hyphens, and underscores. It also should not include duplicated names even if the letter case is different. In other words, www and WWW would be an example of a duplicated name.

Note: When setting up the site structure (the sites that are created within the account), if it is desired that a site be set up with a subfolder, such as http://www.institution.edu/admissions, and that there will also be a site at just the domain root (e.g., http://www.institution.edu/), it is possible that users may create folders within the domain that essentially overwrites the contents of the other sites. Use caution when setting up this site structure.

An alternative site structure is to use a subdomain for each site. For example, the admissions department would be http://admissions.institution.edu/ and where the DNS is managed separately for each subdomain.

UUID

The read-only UUID is used with Live Delivery Platform.

Public Key

The public key field displays the site’s SSH public key. This key can be used to create a secure connection from OU Campus to the production server without using a username and password combination. This is automatically generated after saving the site record when creating a site.
In order for Public Key Authentication to function properly, the OU Campus public key needs to be copied to the `.ssh/authorized_keys` file on the institution's production server.

More information regarding public keys can be found at this page on Ubuntu's documentation site.

**Generate Button**

The Generate button can be used to regenerate the public key for a site.

**Warning:** Be aware that if the server has already been configured to authenticate with a public key, re-generating a new key will break that existing connection and it will need to be re-configured on the server to authenticate with the new public key.

Additionally, if a site has been registered with an installation of an SSM on the production server, the site will need to be re-registered, as each site needs to be registered with the SSM in order to function properly. Registering a site adds the following to the SSM database:

- Name
- Site’s UUID
- Public Key

To regenerate the public key, click **Generate** and confirm.
Production Server FTP Settings

Production Server FTP Settings Overview

The Production Server FTP Settings panel includes several configuration items that determine the proper communication with the production server, as well as directory and access configurations. This is important for not only publishing, but it also sets up the main images folder, identifies the images directory, and the location of the templates. An access group can be assigned to the production server.

In order to update the website using OU Campus, the production server credentials must be correct. If on new site setup errors are experienced when publishing or when uploading to the production server, incorrect FTP settings could be the cause.

The settings include:

- Server
- FTP Type
- Username
- Authentication Type
- Password
- Show Password
- Test Connection
- Umask
- FTP Root
- FTP Home
- HTTP Root
- Image Directory
- Template Location
- Available To

Field names in bold on-screen indicate that the setting is required.

**NOTE**: Image Directory, Template Directory, FTP Home, and FTP Directory require that the defined FTP Root be included in the entered path, but the FTP Root should *not* be included with the LDP Gallery Directory (under the LDP Settings). Include only preceding slash / and the directory name for that setting.
Production Server FTP Settings Example

Settings Reference

Server
The FTP address for where the web site is hosted. Required. For example:
This can also be specified with an IP address.

**FTP Type**
The available options for FTP Type are:

- SFTP: Secure FTP
- FTP: Active mode for FTP
- Passive FTP: PASV mode for FTP

When secure FTP connection is chosen, additional options are available for Authentication Type and UMask.

**Username**
The username for the FTP account. For example:

humanities.gallena.edu

or

ksmith

**Authentication Type**
When utilizing Secure FTP (SFTP), the Authentication Type may also be chosen.

Authentication can be performed with Password or Public Key as the selection depends on how the production server is configured. A public key is generated after the site settings are saved and displayed in the Site Information panel.

**Password**
The password for the FTP account. An optional feature at the account level, when enabled, provides the ability to reveal the password.

**Show Password**
Once enabled at the account level, the Show Password button allows the password to be revealed. Note that when allowing a password to be shown that any level 10 administrator has access to the site settings and will be able to view the password for the server.

**Test Connection**
Additionally, the Test Connection button is available, which tests that the required credentials as entered are correct.

**UMask**
The UMask options are available for Secure FTP. UMask settings set the UNIX based file permissions for files within the site. Changing this setting does not change existing files, it only applies to new files. By default OU Campus sets all file permissions to 644, user writable. The following image illustrates the UMask setting of User Writeable, which includes read/write for the user, but only read for the group.
Example of Read/Write for User Only

<table>
<thead>
<tr>
<th>Name</th>
<th>Ext</th>
<th>Size</th>
<th>Changed</th>
<th>Rights</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>..</td>
<td></td>
<td></td>
<td>9/4/2013 10:07:31 AM</td>
<td>rwxr-xr-x</td>
<td>1732</td>
</tr>
</tbody>
</table>

Choosing **User + Group Writable** sets the permissions to 664, user and group writable. Switching this setting in the site record requires that the modified files be republished either via a site publish or other type of publish to make the file settings change on the server.

Example of Read/Write for User and Group

<table>
<thead>
<tr>
<th>Name</th>
<th>Ext</th>
<th>Size</th>
<th>Changed</th>
<th>Rights</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>..</td>
<td></td>
<td></td>
<td>9/4/2013 10:07:31 AM</td>
<td>rwxr-xr-x</td>
<td>1732</td>
</tr>
<tr>
<td>center-1.html</td>
<td></td>
<td>638</td>
<td>9/4/2013 4:05:24 PM</td>
<td>rw-r--r--</td>
<td>1732</td>
</tr>
<tr>
<td>index.html</td>
<td></td>
<td>655</td>
<td>9/4/2013 4:05:24 PM</td>
<td>rw-r--r--</td>
<td>1732</td>
</tr>
<tr>
<td>.leftnav.inc</td>
<td></td>
<td>216</td>
<td>9/4/2013 4:05:19 PM</td>
<td>rw-r--r--</td>
<td>1732</td>
</tr>
<tr>
<td>.properties.inc</td>
<td></td>
<td>94</td>
<td>9/4/2013 4:05:19 PM</td>
<td>rw-r--r--</td>
<td>1732</td>
</tr>
</tbody>
</table>

**NOTE:** The addition of group writable applies to the UNIX files system and does not have a direct relationship to the groups setup in the OU Campus system.

**FTP Root**

The FTP Root setting determines the root of what is accessible in OU Campus in Production view. Basically, it is a view of the production server. Anything below the FTP Root path can be accessed, anything above it is off limits. Being accessible as a view within OU Campus is also a reflection of the server settings as if write permissions are not available at the FTP Root on the server, OU Campus cannot write to that location either.

The FTP Root field requires a preceding slash, but not a trailing slash.

FTP Root is required, but can be left as slash to indicate root: /. However, the root of the FTP server account does not always have the correct permissions to be the FTP Root or website root. If this is the case, this setting allows the FTP root path to be defined. For example, if the permissions are configured to allow only the FTP user only read/execute FTP access to the account root while the directory with the appropriate web server permissions is /public_html (user: read/write/execute), then the FTP Root should be /public_html. If left as root / then OU Campus will not be able to upload to /. If set up this way, OU Campus users with proper access, would be able to see any files and directories typically at the FTP server account root, such as the logs directory, but not publish pages to those directories without proper server write permissions.
Example of FTP Root as /

If the production server uses /public_html as the web server root similar to the above example, the FTP Root in OU Campus should reflect this. For example:

/public_html

If setting up multiple sites within OU Campus that will share the server, the FTP Root can be used to delineate sites as explained later on this page: Sites, Staging, and Production.

For example, if the Art Department requires a separate site then the FTP Root can be set as:

/public_html/art/

and the HTTP Root is set correspondingly:

http://humanities.gallena.edu/art/

What is seen when navigating between the staging and production in OU Campus is the same, as is what is viewed on the web server in the /art directory when logging in via FTP. When editing these settings a site publish may be necessary to re-set the view. If not already created on the FTP server, the path specified in FTP Root is created when the site record is saved.

**FTP Home**

FTP Home is an optional setting and must be a subdirectory of FTP Root. It is the highest directory to which files can be written on production for a site and the default location for production navigation when defined. For example, if FTP Home is defined in the settings as /public_html/art, then the /art directory becomes the root of the files published to production. In other words, if the index.pcf exists at the root of the staging files and the FTP Home is defined as above (/art), the index.html is published to exampledomain.com/art/index.html. Whereas, without the FTP Home defined, it would be published to, the domain root, exampledomain.com/index.html

The FTP Home field requires a preceding slash, but not a trailing slash.

- If FTP Home isn't defined, it is (internally) set to FTP Root
- If FTP Home is defined, it must equal or be within FTP Root (i.e., a subdirectory)
- If the Template Directory is defined, it must be within FTP Home

**Usage**

FTP Home was originally designed as a way to share image resources across sites. It was not intended to be used to support sharing templates across sites, as that is the job of the OMNI-INF/templates directory at the account level.
While all templates placed in the account’s OMNI-INF/templates directory are available to all sites in the account, this too can be controlled by the Template Groups function of OU Campus. This would allow only a subset of templates be available to a specific subset of sites in an account.

In current OU Campus implementations, it would be very rare to set the FTP Home to path other than the FTP Root. With the advent of the Asset Manager and Binary Management it should never be used as a way to share files across sites. While FTP Home is still supported, it functionality has been deprecated.

**HTTP Root**

The HTTP Root corresponds to the FTP Root, but as accessed through HTTP. The URL root of the website; for example:

http://humanities.gallena.edu/

If a path exists in the FTP Root, that path must follow the HTTP Root. For example if the FTP Root is `/public_html/art`, the HTTP Root would be:

http://humanities.gallena.edu/art/

The HTTP Root must include the `http://` and the trailing slash `/`.

**Note:** If the HTTP Root changes, the entire site must be republished.

The HTTP Root field accepts top-level domains consisting of two characters or more.

**Image Directory**

This is an optional path where users are placed when inserting an image from within the WYSIWYG. The Images Directory setting must be a subdirectory of FTP Root and should include a preceding slash, but not a trailing slash. For example:

/public_html/images

The Image Directory field can be used in conjunction with the FTP Home setting to create sites that can access a shared images location.

**Template Location**

Two options are available for template location as they can be housed either on the staging or production server. Choosing either option allows a path to be defined for the location of the templates with the use of Template Directory. Templates that have been added to the hidden OMNI-INF folders are inherited, allowing both global templates and local templates to be used. OMNI-INF templates can be inherited from the skin, account, or site level. The options are:

- Local (Staging Server)
- Remote (Production Server)

**Template Directory**

This allows a path to be defined on either the staging or production server for site-specific templates. These templates are used in addition to the templates found in the OMNI-INF folders. When identifying a remote path for templates, include the defined FTP Root. For example:

/public_html/_resources/ou/templates

Do not include the FTP Root when defining the path to the local staging server. For example:
Available To

The Available To setting assigns a group in order to limit the ability to see the production server view at the site root level. Only members of the assigned group have the ability to access the production list view of the server. The default group of Everyone indicates that everyone can access the production server unless otherwise restricted at the directory or page level, or other access setting. This allows for preview and for publish to the server unless otherwise restricted with an approver in workflow. The Administrators Only group indicates that no access group has been specified; this allows Level 9 and Level 10 administrators to publish, but not other users.

More About Sites, Staging, and Production

A site can be created without the use of FTP Home, but FTP Home can be used in conjunction with FTP Root to help change the way files are accessible via staging and this also effects how a site is pushed to production. For example, without the use of FTP Home, the FTP Root refers to the site root as it will be uploaded via FTP. For example, humanities.gallena.edu. One method of setting up sites is to use a unique subdomain for every site. This allows for the DNS for the subdomain to be managed separately than the main domain. Since the subdomain is configured as the “server” in OU Campus, there is little risk of overwriting content on the production server. If several sites are added under a domain or subdomain, and they all share the FTP production server, then FTP Root can be used to help delineate sites. Say that the College of Humanities has several departments that all require their own sites; such as the Art Department and the Ethnology Department, but that do not use a separate subdomain. For example, http://humanities.gallena.edu/art. Creating a unique site allows for the Art Department to see only their site as the site root in OU Campus. Even though the site root is unique, multiple sites within the account can be accessed through a file browser by clicking Sites in the breadcrumb, so pages and images can be linked to across multiple sites within an account. With the FTP Root set to humanities.gallena.edu/art/, the content is pushed to that location on the web server.

If viewing the contents on the web server upon logging in via FTP, it would include directories for the sites:

/public_html
>/art
>/ethnology/
>/linguistics/
…and so on.
The HTTP root for the main humanities site would be: http://humanities.gallena.edu/ and the FTP Root would be /public_html. Take care when creating sites in the manner as both the College of Humanities and the Art Department could create unique /art directories on the staging server that would push content to the same location on the web server, which could overwrite one another.

In the two views shown below of staging and production are for the FTP Root of the Art site. To edit another site, the user can choose from the sites drop-down.

FTP Root via Staging View
FTP Root via Production View

One way to help prevent overwriting folders designated sites is to limit access to the production server. This can be done with the use of the Available To setting in the site settings. Only members of the group assigned by the Available To setting have access to production. What this means is that users that are not members of the group, cannot view the Production list view at all and likewise cannot publish since no publish targets are available.

Another way to help circumvent overwriting content on the production server is to limit the users who can create directories by creating template groups and assigning specific templates to them. At the site root for the College of Humanities, create a template group that does not include the template that creates a new section. This would also require that a specific template group or groups be created with the template for creating new sections, so that subdirectories could be created as necessary at subordinate areas.
DirectEdit Button

DirectEdit Button Overview

The DirectEdit button is the button or link on each page of the live site on which users can click in order to access OU Campus and begin editing pages. When a user clicks this link and logs in, the user is provided direct access to editing the page in OU Campus on the staging server. The DirectEdit link is determined by template design and included with a new implementation. The DirectEdit configuration requires that JavaScript be in place, additional code in the XSL, and an identifier where the link should be included.

Example of DirectEdit Link

Keep in mind that the system allows for as much or as little flexibility as desired. In some cases, it may be desired to force users to always use the DirectEdit link to access a page to be edited. This would minimize the need for assigning permissions at a very granular level to the directories housing the pages. Granting access to only the directories containing the pages they should be editing limits the number of groups that may need to be created, but it also limits a user's ability to navigate through the folder structure to pages to edit.

Relation to Account Settings

At the account level, the Login Page fields work in conjunction with the DirectEdit login to control the authentication method used when logging in to OU Campus. If an institution uses CAS or Shibboleth for authentication users are first directed to the URL defined in the account settings when they initially click the DirectEdit link. If this setting is not defined for an account, the standard OU Campus Login page is used. The Announcement URL field of the account settings can be used to customize the Login page.

Setting up DirectEdit

In addition to the account level settings, DirectEdit for a site can be configured, which provides a selection of the type to use and also allows for code to be used to style the link, which overrides the standard button.

1. Navigate to Setup > Sites.
2. Locate the desired site, if multiple sites are available.
3. Hover over the site row and click Edit.
4. Scroll to the panel or select DirectEdit Button from the left panel.
5. Choose a Button Type, and if necessary provide custom CSS for the Button Code.
6. Click Save.
Example of DirectEdit Panel Settings

<table>
<thead>
<tr>
<th>Gallena_University</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Information</td>
</tr>
<tr>
<td>Production Server FTP Settings</td>
</tr>
<tr>
<td>DirectEdit Button</td>
</tr>
<tr>
<td>Site Preferences</td>
</tr>
<tr>
<td>Publish Settings</td>
</tr>
<tr>
<td>WYSIWYG Editor</td>
</tr>
<tr>
<td>File Naming</td>
</tr>
<tr>
<td>Binary File Naming</td>
</tr>
<tr>
<td>LDP Settings</td>
</tr>
<tr>
<td>Auxiliary Sites</td>
</tr>
<tr>
<td>Optional Features</td>
</tr>
</tbody>
</table>

**DirectEdit Button**

**Button Type**
Determines if a button is used and where the button is located. The options are as follows:

- **None**: The None button type will not add a DirectEdit button to the bottom of each page. All DirectEdit buttons/links (including the button code) are disabled. Only used if there should not be any DirectEdit links for the site.
- **Standard**: The Standard button type without an additional definition in the Button Code field uses the OU icon as the DirectEdit log in link. Can be used in conjunction with the **Button Code** field to override the OU icon with styling, an image, and text.

**Standard Button Example:**

- **Transparent**: Adds a predefined transparent GIF as the DirectEdit button. The following image shows the result of a cursor hovering over a DirectEdit button that has been defined as a transparent GIF.

![Transparent GIF Example](www.omniupdate.com/testdrives/de.jsp?user=kgreen&site=Gallena_Sandbox&path=%2Fabout%2Fhistory.pcf)

**Button Code**
The button code can be an image or other text. For example, here is an example of a text link that includes the last updated date:

![Last Updated 5/7/12](Last Updated 5/7/12)

The standard last updated date link can be configured with the following code:
This can be interpreted as identifies what on the screen is the DirectEdit link (e.g., Last Updated [DATE]). It is configured as a link and includes an href of ^0, which is what takes the user to the current page for editing within OU Campus.

### Button Code Reference

<table>
<thead>
<tr>
<th>Button Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>^0</td>
<td>This part of the href indicates that this is the DirectEdit link and will take the user to the login page.</td>
</tr>
<tr>
<td>^1</td>
<td>The use of this indicates the complete URL path. This is generally used in back-end code only.</td>
</tr>
<tr>
<td>^2</td>
<td>This formats the date that appears on the page as month/day/year format (e.g., 1/1/11).</td>
</tr>
<tr>
<td>^3</td>
<td>This formats the date as a three character month, day, and year (e.g., Jan 1, 2011).</td>
</tr>
</tbody>
</table>

Another example of a the button code used to style the DirectEdit link:

```html
<a id="direct-edit" style="color: #9C9C9C; text-decoration: none;" href="^0">&nbsp;Last Updated ^2</a>
```
Site Preferences

Overview

Site Preferences is where certain site-specific alternatives can be configured. Most of the features are exclusive to each site with the exception of time zone and locale, which can also be configured at the account level. The settings include:

- Recycle Bin
- Time Zone
- Locale
- Local Assets Group

Recycle Bin

The Recycle Bin field allows a directory to be input that will be used to hold files that have been recycled. Administrators can then restore or permanently delete files from the Recycle Bin. If no Recycle Bin is configured, pages and files are permanently deleted without any ability to recover them.

A Level 10 administrator can set up the Recycle Bin from Setup > Sites. A Recycle Bin is configured for each site by default during the implementation process. For more information about the use of the recycle, delete, and restore functions, see the Move to Recycle Bin page.

For a tutorial regarding setting up the Recycle Bin, refer to the Configuring the Recycle Bin section on the Recycle Bin page.

Directories themselves cannot be recycled, but the files within them can be recycled and the directory deleted afterwards. For more information, visit the Delete page.

Time Zone

Sets the default time zone for the site by selecting a city or region that most closely matches the site’s location. This will automatically set the time zone for that location, as well as keep the time accurate during Daylight Savings Time. The default setting is America/Los Angeles for SaaS clients. This can be changed to the time zone where the updates are actually occurring providing a more accurate time in the reporting.
This is especially useful for SaaS customers. If this is left blank, it will inherit the value for the setting from the account. When evaluating time zone and the setting is configured at all levels, the precedence is in this order: user, site, account.

**Locale**

Configures a locale for the site. The default is English (United States). This setting also identifies which dictionary should be used by default. If this is left blank, it will inherit the settings from the account settings. When evaluating locale and the setting is configured at all levels, the precedence is in this order: user, site, account.

For more information, visit the [Locale](#) page.

**Local Assets Group**

The Assets list view can be used to restrict the use of assets to the current site only for the specified group. For the **Restrict users to locally-created assets only** drop-down, the group that is selected will only be able to access assets that were created in the same site.
Publish Settings

Overview

The Publish Settings panel provides default settings pertinent to a page or pages within a site being published, which currently includes Final Check configuration options, default text for tweets and Facebook wall posts, and whether OU Tags are removed at from the source of a page upon page publish.

These publish settings can be altered from the Setup > Sites > Site Settings menu in the regular OU Campus interface, or from the SuperAdmin interface (if the institution is on its own skin of OU Campus and has access to SuperAdmin).

Final Check/Final Check Options

Final Check gives a Level 10 administrator the ability to enforce quality assurance tests to be performed on a page before publishing. These include spell check, link checking, W3C validation, and accessibility compliance.

When enabled in this panel, the selected checks will run automatically when a user clicks the Publish button on a page. The page cannot be published until the enforced checks have been completed. Users are able to view the results of each check upon their completion. Users can publish the page/file even if the checks return with errors, though it is strongly encouraged to fix any errors before publishing the page.

Once Final Check is selected, the Final Check Options are shown.

For Final Check and the Final Check options to be available for a site, Page Check and the corresponding Page Check Options must be enabled at the account level as only the options that were made available at the account level are available for Final Check at the site level.

For more information about Page Check and the available checks, visit the following pages:

- Page Check
- Spell Check
- Link Check
• W3C Validation
• Accessibility Check

Default Tweet/Wall Post
Social media integration within OU Campus allows for the configuration for the use of Twitter accounts and Facebook posts. After setup of these options, when a page is published the user may, at the time of publish, send a tweet to one or more Twitter accounts and post to one or more Facebook pages. This field allows for default text to be defined, which is populated for the user. The user can edit the text at the time of page publish. This default text can also be defined at the account level, but any value entered here at the site level will overwrite the account-level value for the current site.

Remove OU Tags
When activated, removes all forms of the OU Campus tags from the source code of pages when publishing. That includes the OmniUpdate comment tags, transitional tags, and ouc: node formats. For example:

```xml
<!-- com.omniupdate.div>
<!-- ouc:div-->
<ouc:div>
```

```xml
</ouc:div>
```
WYSIWYG Editor

WYSIWYG Editor Overview

The WYSIWYG Editor panel in Site Settings allows behaviors to be set for the WYSIWYG Editor on a site-by-site basis. In addition to the settings found here, custom toolbars can be created and assigned to editable regions, users, directories, and sites. A custom toolbar can be created with limited editing functionality in order to restrict editing of specific areas. Toolbar assignments can also be defined in a template.

WYSIWYG Editor Site Settings Example

Use HTML5 Schema

By default HTML5 Schema is not selected. Select the checkbox to enable the HTML5 schema for the WYSIWYG Editor for a site. When selected, the WYSIWYG Editor expects to utilize HTML5-type HTML, which includes the addition of HTML5 elements and the removal of invalid elements. An XHTML schema is utilized when this checkbox is not selected. This also affects page validation during Page Check and Final Check. When selected, page validation is for HTML5. If non-HTML5 elements are included in the XSL, this does not change WYSIWYG editing, but can be possibly listed as an error or warning during validation with Page Check or Final Check.

With the XHTML schema, the WYSIWYG Editor does not remove HTML5 elements, such as section and article, but to add these elements to the page would require utilizing source code or using a snippet. The XHTML schema also allows for attributes that have been identified as invalid in HTML5 but not in XHTML. When the HTML5 schema is enabled, invalid attributes are removed. Additionally, the HTML5 block-level elements, such as section and article, are available in the Format drop-down, making them easy to add to the content without having to use a snippet or access the source code. The Show/Hide Block Elements was added to the WYSIWYG Editor in both XHTML and HTML5 states that provides a visual indicator of the occurrence of block level elements, allowing editors to see where they are within the content.
Because pages that are edited using the WYSIWYG Editor must conform to the HTML5 schema once it is enabled, invalid attributes are removed and it is possible that the entire tag may be removed. For instance, the name attribute in an anchor tag is invalid in HTML5. As such, anchor tags that contain only a name attribute without any other attributes are removed. This may, essentially remove any anchors within a given page. These particular tags can be fixed by changing the name attribute to an id attribute.

It is strongly advised to review page content prior to enabling HTML5 schema. A complete backup of the site should be created. The W3C validation tool can be used to help check the page’s HTML5 validation. This requires that the templates, specifically the declaration in the XSL, be set to HTML5. Global Find and Replace can be used to search for any invalid attributes, but that may not be the best option for fixing or replacing any potential issues. For more information on invalid and obsolete attributes in HTML5, see the W3 documentation:
http://www.w3.org/TR/html5/obsolete.html

See also:
HTML5

Format Drop-Down

Note: When enabling HTML5 Schema for a site, IE 8 will not create a line of text by pressing return after an HTML5 tag (e.g., article, section) has been created.

URL Type

URL Type defines format of link and image URLs:

- **Absolute**: Renders a complete URL (e.g., http://www.college.edu/folder/file.html).
- **Root Relative**: Renders the URL from after the “/” of the configured root.
- **Page Relative**: Renders the URL from after the “/” relating to the page that the user is on and on which the user is entering the link or uploading the image.

NOTE: If Dependency Manager is being used, links referencing other pages and directories within the account are rendered as root relative or absolute based in the settings defined, but they cannot be rendered as page relative.

Decorative Images

This allows users to insert an image without having to include a description, for instance if the image is a decorative image (e.g., a horizontal rule that is an image instead of the standard code). Users are able to select Decorative Image when inserting a new image in order to bypass the description requirement. Keep in mind that enabling this option may affect the site’s Section 508 compliance. The options are:

- **Disabled**: Recommended as this forces users to add a description when adding images.
- **Admin Only**: Allows administrators the option of adding a description for an image, but does not require it.
- **All Users**: Provides all user the option of adding a description for an image, but does not require it.

Disable Image Resizing

When using Insert/Edit Images to add images there is a setting that allows for resizing the image. This is found on the Appearance tab > Dimensions. Selecting this checkbox in the site settings disables the ability for users to input custom size dimensions for images. This also disables the ability to drag a grab-handle and resize the image with a drag.
Note: Image resizing is still available with the Image Editor and width and height can be modified in code view. When enabled the feature is made unavailable. This is not supported by Internet Explorer.

Disable Image Alignment Menu
Disallows the ability to align images (left, center, right, justify). The feature is found in the WYSIWYG Editor > Insert/Edit Images > Appearance tab > Alignment. When enabled in the site settings the feature is unavailable.

Toolbar
Determines the default toolbar for the WYSIWYG Editor, if none other is defined. Toolbar is an access setting; rules of precedence and inheritance apply. As an access setting, a toolbar can be assigned to a user, and at the site, directory, page, and editable region levels. By default, the "Default" toolbar is used for new sites, which is an all-inclusive toolbar. If it is necessary to assign a different toolbar (than what is assigned here) for the site-root directory (and not other directories) use a non-recursive action for the Toolbar setting from Setup > Sites > Edit > Site Access.
File Naming

File Naming Overview

Location: Setup > Sites > Edit > Site > File Naming

The File Naming panel helps control the file naming convention of new files and when uploading non-binary files. This does not apply to the naming of binary files. The Binary File Naming panel is specifically for controlling the file naming convention of binary file types.

File naming uses regular expressions, often referred to as regex, to control the characters allowed in the naming of a file. A commonly used regular expression in file naming is:

```
[a-z0-9\-_\.]*
```

This particular regular expression allows for the file name to include lowercase letters, numerals 0–9, hyphens, underscores, and periods. All other characters are disallowed and present the user with a warning message.

Note that the interface is case-insensitive meaning that it is not allowed to have filenames that differ only in case. Both filename.pcf and FILENAME.pcf are considered the same. The user interface and WebDAV both enforce this. Even in the event that the SaaS staging server or another server-type on an Enterprise system is using a Linux-type file system that allows for distinct files based on case sensitivity, they are not honored in OU Campus.

During site creation, the Text Regex field becomes available after entering text in the File Name Regex field.

File Naming Options

- **Default Extension**: The value defined in the site settings is used if a tcf does not specify an extension. **Note**: It is not necessary to enter the period for a file extension. The correct format for making a PCF-type file the default extension to be used when creating pages is:
  
  pcf

- **File Name Regex**: A regular expression can be input into this field to limit the names of files. Regular expressions (regex) allow specification of whether or not letters, numbers, capitalization, etc., are allowed for page naming. A commonly used regex allows for lowercase letters, numbers, hyphens, underscores, and periods. It is formatted like this:
  
  `[a-z0-9\-_\.]*`

- **File Name Must NOT Match Regex**: Select this checkbox to specify that the regex input that was not specified in **File Name Regex** should not be allowed.

- **Regex Description**: The description is shown in addition to the standard error message. This is displayed during file upload via the WYSIWYG Editor, Source Editor, and the folder structure if the uploaded content does not conform to the defined regex.

- **Test Regex**: When the **File Name Regex** field is used, this allows the administrator to test the configured regex to make sure that it is preventing the correct characters. The name of a file can be entered here and on-screen a green checkmark or red circle indicates the pass or fail status for the on-screen test.

- **Allow Uppercase in Folder Names**: Allows that folders can be created with uppercase letters. If this is not selected, then the regex for the system allows for lowercase letters, numbers, underscores, tildes, and dashes to be used. If this setting is selected, then the CMS regex additionally allows for uppercase letters to be used. **NOTE**: If the TCF contains the force-lowercase="yes" attribute, this setting is overridden. Additionally, if force-lowercase is being used in the TCF with destination="{directory/} {dirname}" in the template tag, all the force-lowercase values (yes or no) must match.
**File Naming Tutorial**

The following provides an example for the use of file naming to restrict file names to use only lowercase letters, numbers, hyphens, underscores, or periods.

1. Navigate to **Setup > Sites**, hover and from the Edit menu for the site, click **Site**.
2. In the **File Naming** panel, enter the following regex described in the **File Name Regex** field: 
   ```plaintext
   [a-z0-9\-_]*
   ```
3. Ensure that the checkbox for **File Name Must Not Match** is not selected.
4. In **Regex Description**, enter a user message. For example, “Use lowercase letters, numbers, hyphens, underscores, and periods only.”

In **Test Regex** field, enter a phrase to test the regex syntax. In this example, a file name using lowercase letters, numbers, hyphens, underscores, and periods receives the green checkmark. Enter a file name with uppercase letters to receive an error.
Binary File Naming

Overview

Location: Setup > Sites > Edit > Site > Binary File Naming

Available To: Level 10 administrators

Binary file naming controls the rules that are applied to the naming convention for binary files such as pictures, movies, and PDF files. This limits the ability to upload binary files to those that comply with a specific file naming convention, such as using a rule that all letters must be lower case. This also allows administrators to ensure that the file naming convention is enforced when binary files are renamed, which can be accomplished with the Image Editor for image binaries and through the folder structure. The Binary File Naming feature is enforced whether Binary Management is enabled or disabled. If Binary Management is disabled, the regex is still used even though the files are published immediately to the production server.

Note: The Text Regex field becomes available after entering text in the Binary File Name Regex field during site creation.

About Regular Expressions

Binary File Naming uses regular expressions, often referred to as regex, to control the characters allowed in the naming of a file. A commonly used regular expression in file naming is: `[a-z0-9\-_]*`

This particular regular expression allows for the file name to include lowercase letters, numbers 0–9, hyphens, underscores, and periods. All other characters are disallowed and present the user with a warning message.

Binary File Naming Reference

Binary File Name Regex: A regular expression (regex) can be input into this field to have binary files conform to a file naming convention. Regular expressions allow specification of whether or not letters, numbers, capitalization, etc., are allowed for binary file naming. A commonly used regex allows for lowercase letters, numbers, hyphens, underscores, and periods. The syntax is: `[a-z0-9\-_]*`
Binary File Name Must NOT Match: When this is selected, the regex placed in the Binary File Name Regex field indicates that the characters are not allowed in the naming of a file.

**Binary Regex Description:**
The description is shown in addition to the standard error message. This is displayed during file upload via the WYSIWYG Editor, Source Editor, and the folder structure if the uploaded content does not conform to the defined regex.

**Test Regex:** The Binary File Name Regex field allows the administrator to test the configured regex to make sure that it is preventing the correct characters. The name of a file can be entered here and on-screen a green checkmark or red highlighting indicates the pass or fail status for the test.

**Binary File Naming Tutorial**
The following provides an example for the use of Binary File Naming to restrict file names to use only lowercase letters, numbers, hyphens, underscores, or periods.

To set up the Binary File Naming regular expression:

1. Navigate to Setup > Sites, hover and from the Edit menu for the site, click Site.
2. In the Binary File Naming panel, enter the following regex described in the Binary File Name Regex field: `\[a-z0-9\-_\]`.
3. Complete the fields for the Binary File Naming panel as follows:
   - In the Binary File Name Regex field enter: `[a-z0-9\-_\].*`
   - Ensure that the checkbox for Binary File Name Must NOT Match is not selected.
   - In Binary Regex Description, enter a user message. This example uses the text: “Use lowercase letters, numbers, hyphens, underscores, and periods only.”
4. In Test Regex field, enter an example file name to test the regex syntax. In this example, a file name using lowercase letters, numbers, hyphens, underscores, and periods receives the green checkmark.

5. Test by enter a name using uppercase letters and a red X indicates the error.
6. After completing the necessary fields, click Create or Save.

Error Examples

Below are some commonly experienced messages when trying to upload a file with an incorrect naming convention. Keep in mind that the message may be slightly different depending on the site’s settings. These examples utilize the regex that was used for the tutorial that is intended to restrict file names to use only lowercase letters, numbers, hyphens, underscores, or periods: $[a-z0-9\._-]*$

With Upload

There are three types of available upload options when uploading from the file structure: Standard, Upload and Edit, and Zip Import.

Standard Upload

When performing a standard Upload, if the file name contains illegal characters, the upload is disallowed and the error is shown in red. The description configured with the Binary Regex Description field is also shown.

To replicate the error:

1. Navigate to the Pages list view where the binary is to be uploaded.
2. Click the Upload icon.
3. Drag a file with uppercase characters in the file name to upload it.
4. Click Start Upload.
5. Note the error message.

6. Click Rename & Retry, remove the file from the modal by hovering over the file name and clicking Rename, renaming the file in your computer file browser, and upload it again.
7. Click **Start Upload** to upload the file.

### Upload to \_resources\_images

<table>
<thead>
<tr>
<th>Filename</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>cloud.png</td>
<td>Upload Successful</td>
</tr>
</tbody>
</table>

**Zip Import**

The second type of upload is Zip Import.

If illegal characters exist in the file name of a file or files, the warning message is shown in the Zip Selection section area.

Users can navigate to any file containing illegal characters, and correct the errors by clicking on the file name and updating it to meet the necessary criteria.

The **Extract** button is dimmed until all file naming issues are resolved.

**Upload WYSIWYG Editor**

When a regex has been defined for binary file naming to restrict file names to a specific file naming convention, this functionality is also used by the Insert/Edit Image feature of the WYSIWYG Editor.

**During Rename**

If attempting to rename a file from the Pages list view, any attempted rename that does not match the regex will trigger an error message like the one below.

⚠️ The name “favicon$$.png” contains illegal characters.
LDP Settings

LDP Settings Overview

The LDP Settings are available for configuring the Live Delivery Platform (LDP) settings when the Forms module is being used. Each site on which forms are to be placed must be registered with the Server-Side Module (SSM).

Note:

Live Delivery Platform is an optional set of features in OU Campus. Please contact the university's designated OmniUpdate Sales Director for details.

The following functionality is available from the LDP Settings panel:

• **LDP Admin Host**: The host on which the SSM resides. This is the hostname or IP address of the server used by the application to access LDP administrator functionality.
• **Download Reg File**: When downloaded, the registration file contains the necessary components, which must then be run on the server with the SSM.
• **Test Connection**: After registering the file on the SSM, test the connectivity to ensure that the file has been registered properly.
• **LDP Gallery Directory**: Each site for which an LDP Image Gallery is to be used requires a directory to be configured in which the images are stored. This is a staging location, so unlike the production server settings, FTP Root should *not* be included with the LDP Gallery Directory. Include only preceding slash / and the directory name to specify the directory to contain the images.

Site Settings for LDP Settings

![LDP Settings Panel]

One SSM installation can work with as many sites as necessary. Each site includes its own unique identifier. When working with a Form Asset, which is one of the Live Delivery Platform modules, forms to be submitted also require a unique identifier. The SSM that is required for forms to function properly is installed as part of the implementation of LDP as it contains the databases necessary to house the form submissions. During
the initial installation of the SSM, the current sites are registered with the SSM. When adding sites after the initial implementation registration is accomplished by using the registration file found in the site settings.

The SSM is installed on the institution’s production server. It can be installed on the same server or a different server than that of the website. It is written in Python and the installation includes a MySQL database, which is where the form data are stored. As part of the configuration of the SSM, a server-side connector script is installed on the same server as the website. The connector script’s language is determined based on the needs of the institution. The purpose of the connector script is to act as a bridge between the website where the data is being submitted and the SSM.

Registering a Site

Each site needs to be registered with the SSM in order to function properly. This adds the following to the SSM database:

- Name
- Site’s UUID
- Public Key

The values for a site’s UUID and public key are automatically generated when a site is created and are shown in the Site Information panel of the site settings. The UUID is used for LDP forms; the public key for authentication purposes. If a the public key is regenerated, the site must be re-registered.

To register the site:

1. Navigate in OU Campus to Setup > Sites > Edit.
2. Click on Download Reg File.
3. Save the file and upload it to the server.
4. Run the following command for each registration file and replace /root/registration-site.ldp with the path to the registration file.

   oussm -c /opt/oussm/ssmconfig.ini register /root/registration-site.ldp

The site is now registered. An example of successful registration messaging is:

```
2013-04-01 12:00:25-0700 [-] Log opened.
2013-04-01 12:00:25-0700 [-] Registering admin method: ldp.test.ping
2013-04-01 12:00:25-0700 [-] Database is version 2, application is version 2
```

After the site is registered, the registration file can be deleted.

Also, the OmniUpdate Support Team can register additional sites:

Support Help Desk

SSM Test Connection Messages

After the Server-Side Module

(SSM) has been installed or during troubleshooting of the SSM, the use Test Connectivity tool may be used to help troubleshoot.
<table>
<thead>
<tr>
<th>Stage</th>
<th>Test Connection Message</th>
<th>Steps to Take Toward Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Connection</td>
<td>Connection Timed Out</td>
<td>Has the SSM been installed? If not install it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Has the firewall on the server on which the SSM has been installed been opened to port 7516? If not, open the port. It must remain open.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Is the SSM running? If not, restart the server. If the startup file has not been included, it should be.</td>
</tr>
<tr>
<td>During Authentication</td>
<td>Authentication Failed. Has the site been registered with the SSM?</td>
<td>Has the site been registered with the SSM? If not, register it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Has the public key been regenerated? If not, download the registration file again and re-register the site.</td>
</tr>
<tr>
<td>Success</td>
<td>Test complete: meets overall minimum version.</td>
<td></td>
</tr>
</tbody>
</table>


Auxiliary Sites

Overview

In Site Settings, administrators have the ability to create, edit, and delete publish targets and auxiliary sites in the Auxiliary Sites panel.

Auxiliary Sites at the Site Level

Auxiliary sites can be added to OU Campus at the site level and at the account level. When adding an auxiliary site at the account level, the site is available on all sites within the account. If an auxiliary site is added at the site level, it is only available within the site in which it was created.

When auxiliary sites are configured at both the account and at the site level, then each individual site is able to access the auxiliary sites at both the account level and those added to the current site. The available auxiliary sites will be visible in the auxiliary sites drop-down menu in a filechooser.
Keep in mind that the auxiliary site, utilized as an additional media or document repository option, requires that the files be displayed in a folder structure, which is generally obtained via FTP access. This is not meant to be a method by which images on a public website, such as Flickr, are retrieved for use on the site.

Setting up an auxiliary site at the site level follows the same steps as setting one up at the account level. For more information about setting up auxiliary sites, please visit the Auxiliary Sites page under Account Settings.

**Publish Targets**

Administrators can add additional publish targets to a site, which allows users to choose the server they would like to send a page or file when it is published.

For more information about setting up additional publish targets for Multi-Target Publish, visit the Publish Targets page.
Optional Features

Overview

The Optional Features panel at the site level includes five optional site-specific features. Dependency Manager and Binary Management must first be enabled at the account level to be available for a specific site.

Find and Replace

Select the checkbox to enable the global Find and Replace for Level 10 administrators. When enabled, this is shown in Content > Find and Replace. When enabled, Find and Replace provides the functionality to search content and code within the site and replace it with new values.

For more information, visit the Find and Replace page.

Quick Search

Select the checkbox to enable quick search for the site.

For more information, see the Quick Search page.

Dependency Manager

Select the checkbox to enable Dependency Manager, which governs the automated use of links and linking when files are moved or renamed. Dependency Manager must be enabled in the account settings before it can be enabled for a particular site.

For more information, visit the Dependency Manager page for the account level.

Binary Management

Select the checkbox to enable Binary Management, which allows for binary files such as images to be managed on the staging server in a fashion similar to managing file linking with Dependency Manager.

For more information, visit the Binary Management page.

For more information about enabling the feature at the account level, visit the Binary Management page at the account level.

WebDAV

Select the checkbox to allow WebDAV to be enabled for specific Level 9 and Level 10 administrators. For more information, visit the WebDAV page.
WebDAV

Overview

WebDAV integration provides access to the file system on the staging server similar to FTP/SFTP and can be used in lieu of FTP/SFTP. WebDAV (Web Distributed Authoring and Versioning) is a communications protocol that honors settings in OU Campus. Unlike FTP/SFTP, when file management is performed using WebDAV, OU Campus treats the files as if they were being managed via the OU Campus interface.

Advantages of WebDAV over FTP is that FTP does not connect to the OU Campus database. File management is not integrated with OU Campus when using FTP. WebDAV implementation allows the files to be tied into OU Campus functionality. This includes permissions/access control, checking files in and out, renaming, adding, deleting, etc. WebDAV functionality (aka verbs) such as rename, delete, get, and put work seamlessly with OU Campus.

WebDAV capability provided by default for an account and must be enabled on a per-site basis and for each level 9 or level 10 administrator that should be provided access. Once enabled in OU Campus, a WebDAV client can be used to connect to the staging server. This view of the system provides restricted access to both the OMNI-RESOURCES and the OMNI-INF folders for a site.

File Permissions and Management

When using WebDAV, access settings for files inherit the access settings from their parent directories when uploading. When a nested folder structure is used in the upload, each directory maintains the correct directory access settings and the files being uploaded have the appropriate settings inherited from the parent.

When using WebDAV with OU Campus the following file management actions honored include (but are not limited to):

- Permissions/access control
- Checking in and out files
- Updating files
- Editing and saving changes to files
- Uploading files and directories
- Moving files and directories
- Downloading files and directories
- Deleting files and directories
- Creating files and directories
- Renaming files and directories
- Dependency tag management

Note: Asset files are not accessible for editing via WebDAV.

Authentication Methods

The various current methods of authenticating log in credentials are supported. This includes LDAP, CAS, Shibboleth, and OU Campus login. Once the administrator has set up LDAP and/or OU Campus users, WebDAV can be used.

Enabling WebDAV

WebDAV can be enabled at the site level, and then Level 10 administrators can then configure access for users with authority levels 9 and 10.
Enable WebDAV for Each Site

1. Navigate to Setup > Sites and click Edit > Site for the site.
2. From Optional Features, select the WebDAV checkbox.
3. Select Save.

Allowing WebDAV Access for a User

Level 10 administrators can give users access to WebDAV through the Setup > Users screen.

1. Navigate to Setup > Users, Edit for the user > Restrictions. If adding a new user, the WebDAV URL will be visible after saving the user setup.
2. Select the Allow WebDAV Access checkbox. This allows for file access to the staging server. If using OU Campus authentication, the password is the same as what is used to login to OU Campus. If LDAP is used, the LDAP password is used with the WebDAV client.
3. Note the WebDAV URL. This is used when configuring settings for the WebDAV client. The WebDAV URL listed in this section is the path to the site. A specific folder can be appended to it and used for the WebDAV client configuration.

Supported Clients

The integration of WebDAV into OU Campus supports a number of WebDAV clients. The following clients have been tested:

- <oXygen/> XML Editor 14.2 (both Windows and Mac)
• Cyberduck 4.3 (FTP/SFTP/WebDAV client, both Windows and Mac) (Note: older versions of CyberDuck may also be supported depending on version and encryption settings)
• Dreamweaver C6 (Web development, both Windows and Mac)
• BitKinex 3.2 (FTP/SFTP/WebDAV client, Windows)
• Transmit 4 (FTP/SFTP/WebDAV client, Mac)
• Coda 2 (FTP/SFTP/WebDAV client, Mac)
• Interarchy 10 (FTP/SFTP/WebDAV client, Mac)
• Mac OS X 10.8 Finder (Mac)

Clients with File Locking Support
The following clients have been tested and are known to support file locking (check in/check out):

• <oXygen/> XML Editor (both Windows and Mac)
• Dreamweaver (both Windows and Mac)
• BitKinex (Windows)

Clients without File Locking Support
The following clients have been tested and are known to not support file locking (check in/check out):

• Cyberduck (both Windows and Mac)
• Transmit 4 (Mac)
• Coda 2 (Mac)
• Interarchy 10 (Mac)
• Mac OS X 10.8 Finder (Mac)

Example Setup (Cyberduck)
1. Click Open Connection.
2. Select WebDAV (Web-based Distributed Authoring and Versioning) from the drop-down.
3. For the Server field, enter the WebDAV URL noted previously. That is, the path specified from Setup > Users > WebDAV section > WebDAV URL.
4. Clear the Anonymous Login checkbox.
5. Enter Username and Password.
6. Click Connect.
Notes

- When troubleshooting connection errors, note that WebDAV must be enabled for each site, as well as for the administrator. If not enabled at one of these levels, the WebDAV client will not be able to connect.
- Use extreme caution when granting staging server access as an administrator is able to delete the site files from the staging server.
- Users may need to refresh their browser windows in both OU Campus and the WebDAV client to see changes made by one or the other, if both are active at the same time.

Moving Files and Folders

- Files and folders are able to be moved only within the WebDAV enabled site.
- Moving files across sites is not supported. (One alternative to be considered is copying files to a local computer and then to the desired site.)

Naming and Renaming

- Naming and renaming a file will not conform to the site's pre-defined regex settings.
- Special characters are permitted upon upload and renaming file or folders. Users need to be careful as some special characters can cause OU Campus to stop responding to the file. Error behavior in this case can include preview and rename not functioning. If a problem character is present in a file that was uploaded or renamed via a WebDAV client into OU Campus, the user needs to use the WebDAV client to rename the file.

Upload

- Uploading non-binary files (text) via WebDAV is permitted.
- Uploading binary files via WebDAV to the OU Campus staging server is permitted as long as Binary Management is enabled.
Locking

- The WebDAV client (that supports locking) checks out the file to the user in OU Campus.
- If a file is checked out to another user in OU Campus, then the file is locked to the WebDAV client, the client will not be able to edit it but can view a read-only copy of the file.
- OU Campus can override locks that are initiated by a WebDAV client. When this occurs, the corresponding WebDAV client still holds the lock even though it is now invalid. However, OU Campus correctly denies access if the WebDAV client tries to act on the (now invalidly locked) file. An exception to this is that Dreamweaver allows a lock override.
Users

Overview

Users and groups are account-wide settings; that is, the same user can access all sites within an account. Users and user groups can be created and modified by a level 10 administrator.

Setting up a user gives the individual the ability to access OU Campus and defines the user’s authority level, which provides inherent permission for specific functionality within the CMS. There are 11 user levels within OU Campus (0–10). The most commonly used user levels are 4 and 6 (general content contributors), and 8 (approvers, developers, etc.) . Level 9 and 10 users are considered administrators in OU Campus, with Level 10 administrators being the only users who can access to the Setup menu. For more information about the inherent permissions available to each user level, see the Permission Chart.

In addition to the inherent abilities provided with the authority level, additional permissions can be assigned. These permissions can range from the ability to add words to the site’s custom dictionary to the assignment of an approver. All users inherently have an ability to publish content unless otherwise revoked through the assignment of an approver, which is accomplished through the access settings in the interface or at a code level for site developers.

Users are added as members to groups, and groups, in turn, are assigned to specific areas or functionality in order to limit the functionality to members of the group. Users, as individuals, can only be assigned to the approver settings.

Before group assignment can be designated, users must be added to the system. It is valuable to understand the various fields found in the user configuration prior to doing an initial import of users since the
fields found in the user settings can be included in the user import file in order to make the creation of initial users easier. User settings can be updated at any time.

An administrator can create new users and modify existing user settings from Setup > Users. A few settings can be user controlled from current user menu on the global navigation bar.

**Users List View**
The Users list view includes the following features and functionality:

- Shows the number of users in the account
- Filtering by user, name, and level
- Creating a new user
- Sorting the list by username, by name (the combination of first and last name), level, or the date and time of each user's login
- Selecting multiple users to create a group
- Selecting multiple users to delete users
- Modifying a user's settings
- Deleting a user

**Creating a New User**
Level 10 administrators may create new users of any level 0 through 10 and configure the settings available specific to that user level. To create a new user, click the New button in the upper, right-hand corner of the Setup > Users screen. When setting up a new user the required information is indicated on-screen in bold. For new users, this includes the Username and User Level fields, and if not using LDAP, the Password field.

The User Information, Restrictions, Preferences, and LDAP Configuration panels are available during new user creation as well as being available for editing after. The New User Options are only available during the initial creation.

**Basic Steps**
1. Navigate to Setup > Users.
2. Click New.
3. Add User Information and Preference settings as necessary.
4. Under **Restrictions**, select the **User Level** and configure the level-specific settings.
5. If necessary to send a welcome message and password, select the appropriate checkboxes.

6. Click **Create**.

**More Details for Creating Users**

The following panels are available when creating a new user:

- User Information
- Restrictions
- Preferences
- LDAP Configuration
- New User Options

Note that both the Restrictions and Preferences panels include settings specific to the selected user level. Users can view selected settings from Settings in the current user menu on the global navigation bar and change the User Information items (with the exception of the Username), and can enable and disable Page Check, if so configured for user enablement at the account level.

**Modifying Existing Users**

Administrators may edit an existing user’s settings with the exception of Username. From **Setup > Users**, user settings can be modified by clicking on a user name, or hovering and clicking Edit, or selecting the checkbox next to the user name and clicking Edit. Remember to click Save when done making changes.
Deleting a User or Users

Created users can be deleted by hovering over a user and clicking Delete.

Multiple users can be deleted from the system with one action by selecting the checkboxes and clicking Delete.

Deleting a user removes the user from any access settings in which they were a part and checks in content that they had checked out either in workflow or otherwise.

Unlocking a User

An Level 10 administrator can reset a user if the user has become locked out of the account by attempting to log in with too many incorrect log in attempts. The number of failed attempts allowed is configured in Setup > Account.

1. Navigate to Setup > Users. The locked out user is shown in red and with a lock.

2. Hover and click Reset. The user’s password remains the same as it was prior to the user being locked out.

It is also possible, if CAS, Shibboleth, and LDAP are not being used, to change the user’s password by editing the user record. Keep in mind that the new password needs to be communicated to the user.

A user can reset his or her own password with the Reset Password feature. For more information: Log In

Creating a Group

In addition to being able to create groups from Setup > Groups, a group can be created from within the Users screen. Users must already be added to the system to be available for selection to be added to a group.

1. Do one of the following:
   • Select the checkbox adjacent to each user to add as a member
   • Click the checkbox in the header row to select all users
2. Click **Create Group**. This shows the **New Group** dialog.

3. Define the **Name** for the group.

4. To add additional members to a group, select a user or users from the **Available Users** list and use the single arrow to move the selection to the other list.

   To remove members from the group, select a user or users from the **Members** list use the single arrow to move the selection to the other list.

   The **Control** (PC) or **Command** (Mac) key can be used to select multiple users.

   The double-arrows can be used to move the entire list from side to the other.

5. Click **Save**.
Permission Chart

Overview

Authority levels are set by administrators by assigning a user level to a user. The functions available to each authority level are detailed in the table below. A checkmark indicates that the feature is inherent to that authority level. A diamond indicates that it can be assigned by an administrator. Level 10 administrators can also modify access settings based on content, which includes for a page, binary file, directory, site, publish target, or asset. Access settings are modified by assigning a group. The system group Administrators Only provides rights to Level 10 administrators. The system group Inherit from Parent indicates that the value is dependent upon the setting of the parent item. For example, if a file has Inherit from Parent as the value, then the directory setting is used. The system group Everyone includes all user and administrator levels. Site level settings are available to Level 10 administrators.

Legend

◊

Assigned by an administrator

√

Inherent for the authority level

<table>
<thead>
<tr>
<th></th>
<th>Review</th>
<th>Contributor</th>
<th>Editor</th>
<th>Design</th>
<th>Asst. Admin</th>
<th>Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>WYSIWYG</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
</tr>
<tr>
<td>EDITOR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add entries to</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
</tr>
<tr>
<td>Spellcheck</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dictionary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom Dictionary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Ability to</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>manage and edit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>words in the</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom Dictionary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>from Site</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>&gt; Custom Dictionary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GADGETS ACCESS TO DASHBOARD AND SIDEBAR GADGETS</td>
<td>LEVEL 0</td>
<td>LEVEL 1</td>
<td>LEVEL 2</td>
<td>LEVEL 3</td>
<td>LEVEL 4</td>
<td>LEVEL 5</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td>LEVEL 0 do not have access to edit pages and therefore do not have access to the Images Gadget and Snippets Gadget</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

| GADGET SETUP A LEVEL 10 administrator can add new gadget and set access settings for gadget availability | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| HTML EDITOR ACCESS TO EDITABLE REGION HTML | ◊ | ◊ | ◊ | ◊ | ◊ | ◊ | ◊ | ◊ | ◊ |
| Via the WYSIWYG Editor, click the HTML button in the WYSIWYG Toolbar to use the HTML Source Editor. Provide access to the editable region's HTML. A custom toolbar that does not include the HTML button can be created and assigned to a user. |
|---|---|---|---|---|---|---|---|---|---|
| Edit Page Source | Level 9 user can be | ◊ | ◊ | ◊ | ◊ | ◊ | ◊ | ◊ | √ | √ |
restrictions from using the Source Editor by selecting the Disable Full HTML checkbox in the User Information screen by a Level 10 administrator. If given access to the Source Editor, user levels 1-8 can only see the source of pages to which they have access.

<table>
<thead>
<tr>
<th>CONTENT</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show All Files Content is visible within</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
</tbody>
</table>
the current directory, but navigation cannot be accomplished if there is no access to the directory or page. Access Group can allow for or restrict access to content. Administrators can restrict access to the production server in Site Settings, which prevents users in that group from publishing or viewing files on production.
<table>
<thead>
<tr>
<th>Modify Page Parameters</th>
<th></th>
<th></th>
<th></th>
<th>√</th>
<th>√</th>
<th>√</th>
<th>√</th>
<th>√</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upload File</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>If assigned, levels 1-5 can only upload files in areas to which they belong</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zip Import</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Assign with Allow Upload for Level 6-8. If assigned, can only import ZIP files in areas to which they belong</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Move to Recycle Bin</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>----------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Assign permission and level 8 users can only recycle files to which they are assigned access rights. Level 9 and Level 10 can recycle any content. Directories cannot be recycled. If the Recycle Bin is not configured, files are permanently deleted, not recycled.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recycle Bin</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>If a user has</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>√</td>
<td>√</td>
</tr>
</tbody>
</table>
been given permission to recycle files, they can also enter the Recycle Bin to permanently delete or restore files.

<table>
<thead>
<tr>
<th>Delete Directory</th>
<th>Level 9</th>
<th>Level 10</th>
<th>Level 11</th>
<th>Level 12</th>
<th>Level 13</th>
<th>Level 14</th>
<th>Level 15</th>
<th>Level 16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete Binary File</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>√</td>
</tr>
<tr>
<td>Level 1–8 users can only delete binary files to which they are assigned access rights; including images, PDFs, Word documents, Excel spreadsheets, and so on.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create New Page Available templates may vary depending on the template group assigned to the directory by an administrator. If the template group is not assigned at the directory,</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
level, then it inherits the group from parent directory or the site level. If not assigned at the site level, then all templates for the site are available for use.

<table>
<thead>
<tr>
<th>Overwrite Files</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>◇</td>
<td>◇</td>
<td>◇</td>
<td>◇</td>
<td>◇</td>
<td>◇</td>
<td>◇</td>
<td>◇</td>
<td>◇</td>
<td>√</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Create New Section</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
</tr>
</tbody>
</table>
New Folders
Available templates may vary depending on the template group assigned to the directory by an administrator. If the template group is not assigned at the directory level, then it inherits the group from the parent directory or the site level. If not assigned at the site level, then all templates for the site are available.
for use. The New Folder option may or may not be available for use, depending on the template group used.

<p>| Moving a File, Moving a Directory | Ability to move files and directories | Level 8 users can only move files and directories to which they have access |  ✓  |  ✓  |  ✓  |
| Renaming a File, Renaming a Directory | Ability to move files and directories | Level 8 users can only move files and directories to which they have access |  ✓  |  ✓  |  ✓  |</p>
<table>
<thead>
<tr>
<th>Directory</th>
<th>Ability to rename files and directories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 8</td>
<td>users can only rename files and directories to which they have access</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Copying a File, Copying a Directory</th>
<th>Ability to copy files and directories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 8</td>
<td>users can only copy files and directories to which they have access</td>
</tr>
</tbody>
</table>

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Other Pages Feature</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>If access to area is available, then Preview, Versions/Save Version, Quick Search, Publish, Scheduled Publish, and Submit for Approval are all available. Publish and Scheduled Publish are revoked with the Approver setting.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Assets List View Can be overridden at site level with Asset Access &gt;</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Access Group. Default is the Everyone group. When list view access is disallowed, non-members can only utilize assets.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create Assets Administrators can restrict asset creation at the site level, and each asset type can have a unique group who can create that asset type. These options are available at Setup.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Site &gt; Asset Access</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Edit Assets &amp; Asset Properties</strong></td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Can be overridden on a per asset basis with assignment of Access Group.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>View Asset Log</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Copy Assets Level 8 users can only copy assets to which they have access</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Rename Assets Level 8 users can only rename assets</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use Assets (e.g., insert onto page): Assign with Available To access setting; default is Everyone group.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>View LDP Form Asset Submissions</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Delete Assets Level 1-8 users can only delete assets to which they are assigned access rights.</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
</tr>
<tr>
<td>Other Features If access to</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Asset List View is available, then Preview, Version, Save Version, Publish, Scheduled Publish, and Submit for Approval are all available. Publish and Scheduled Publish are revoked with the Approver setting.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Access to assets regardless of groups assigned.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create Snippets</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign RSS Feeds</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rebuild RSS Feeds If an RSS</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Action</td>
<td>Level 1</td>
<td>Level 2</td>
<td>Level 3</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>Feed item update from within the Content view, the feed can be rebuilt, published update</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Can be revoked by assigning an approver (except for Level 9 and Level 10)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit RSS Items if feed is assigned</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Find and Replace</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SOCIAL MEDIA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Setup Facebook Pages &amp; Twitter Accounts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GROU &amp; USERS</td>
<td>Ignore Groups &amp; Tagging</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Create &amp; Modify Users</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create &amp; Modify User Groups</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign Editing Rights</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign of group with access to content including page, directory or asset; Limited to content to which they belong and can only assign to groups to which they belong</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlimited Assign</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Editing Rights Assignment of group with access to page, directory or asset; No limit by page or group association.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>WORKFLOW &amp; PUBLISHING</strong> My Checked-Out Content Gadget Shows pages checked out to current user.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Log</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Publish Content Can be revoked by assigning an approver.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Publish Directory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Publish Entire Site</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>REPORT MENU</td>
<td>Ability to see data for all pages/users site-wide</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>√</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Requisition Actions, Checked Out Content, Pending Approvals, and Scheduled Actions Reports** (if not administrator, only able to see content to which they have access)

- √
- √
- √
- √
- √
- √
- √
- √
- √

**Recent Saves and Recent Publish Reports** (if not administrator, only able to see content to which they have access)

- √
- √
- √
- √
- √
- √
- √

OU Campus  Permission Chart  Page 200 of 289
<table>
<thead>
<tr>
<th></th>
<th>have access</th>
<th>Site Check and Custom Report</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Access to Site and Account Info (Setup Menu)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACCOUNT INFO</td>
<td></td>
<td>Configure site-wide Access Settings</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configure Asset Access Settings</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Activate Dependency Manager and run scanner on site and/or directory</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
User Information

Overview

The User Information Panel is where the personal information for the user is found. Keep in mind that the settings in this panel, with the exception of the user name, can be modified by the user.

The User Information Panel contains the following fields:

- **Username**: The username for the user, which will be used to log in to OU Campus. Must be 4-32 characters, containing only letters, numbers, or underscores. If using LDAP, CAS, or Shibboleth, the username must match the user’s current username in that authentication system.
- **Password**: The password for the user, which will be used to log in to OU Campus. It may be up to 32 characters long and is case-sensitive. If using LDAP or to keep the current password (if editing a user that already exists in the system), leave this field blank. This field will be hidden for CAS and Shibboleth users, unless WebDAV is enabled for the user.
- **First Name**: First name for the user.
- **Last Name**: Last name for the user.
- **Phone**: Contact phone number for the user.
- **Email**: External email address for the user. This allows for internal OU Campus messages to be sent to the user’s external email address as well.
- **Time Zone**: Select the city or region that is closest to the user’s location. This will automatically set the time zone for that user, which overrides any time zone settings set at the account or site level. Setting the time zone populates the date and time stamps throughout the system.
- **Locale**: Locale configures the formatting for the time and date stamps throughout the system. Choose a locale from the drop-down menu to override the locale settings set at the account or site level.
Restrictions

Overview

The Restrictions panel includes the configuration options for user settings as the authority level for the user can be configured and options are made available based on the user level assigned. For example, selecting a user level of 6-Editor enables several additional options. On-screen items in bold are required. For the Restrictions panel, this includes the User Level setting.

For more information about authority levels and screenshots for the various Restrictions panels:

Authority Levels

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Level</td>
<td>Required. Sets the abilities of the user according to the permission chart. Available levels are 0–10.</td>
</tr>
<tr>
<td>Appraover</td>
<td>The user in the system who is the default approver for this user. If the Enforce Approver option is not selected, then the user can still choose another user to whom to submit the content, but will not have publishing rights. This setting can be overridden by an approver setting closer to the content. Those in a Bypass Approval group that is assigned to a content region can override the approval process.</td>
</tr>
<tr>
<td>Enforce Approver</td>
<td>If selected, this prevents this user from being able to change the recipient the content being sent for approval. When not enabled and an approver is specified, the user will still have the ability to choose to whom to send the content for approval.</td>
</tr>
<tr>
<td>Disable Full HTML</td>
<td>Disallows access to editing with the Source Editor, which would otherwise allow source editing of all content regions for a page. This can usually be accessed with the Edit Full Page button at the bottom of a page in edit mode or, for a checked out page, via the Pages list view &gt; Edit &gt; Source or via the Source button. Only available for level 9.</td>
</tr>
<tr>
<td>Allow Source</td>
<td>If selected this gives user levels 1–8 the ability to edit with the Source Editor, which allows source editing of all content regions for a page. This can usually be accessed with the Edit Full Page button at the bottom of a page in edit mode or, for a checked out page, via the Page list view &gt; Edit &gt; Source or via the Source button. Only available for areas to which the user has access.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow Upload</td>
<td>If selected this gives user levels 1–5 the ability to upload files and images to areas to which they have access.</td>
</tr>
<tr>
<td>Allow Zip Import</td>
<td>If selected this provides Zip Import access to users level 6–8.</td>
</tr>
<tr>
<td>Allow Overwrite</td>
<td>If selected this gives user levels 1–8 the ability to overwrite files in areas to which they have access.</td>
</tr>
<tr>
<td>Allow Delete</td>
<td>Grants users level 1–7 the ability to delete/recycle files and pages, and delete assets.</td>
</tr>
<tr>
<td>Toolbar</td>
<td>By selecting a toolbar in the drop-down menu, the administrator assigns a customized version of the toolbar. Toolbar selection can be overridden per site, directory, individual page, or region on a page, or configured to be assigned by a TCF including as a selection with parameters. Available for all levels. A custom toolbar must be previously configured to be available. The default setting of (Default - All Buttons) provides this user with the default toolbar.</td>
</tr>
<tr>
<td>Allow WebDAV Access</td>
<td>Once enabled in OU Campus, a WebDAV client can be used to connect to the staging server. Level 10 administrators can allow access for users with authority levels 9 and 10.</td>
</tr>
<tr>
<td>WebDAV URL</td>
<td>Autopopulated when the Allow WebDAV Access checkbox is selected. Note the WebDAV URL. This is used when configuring settings for the WebDAV client. The WebDAV URL listed in this section is the path to the account, not the site. A specific site or folder can be appended to it and used for the WebDAV client configuration.</td>
</tr>
</tbody>
</table>
Preferences

Overview
The Preferences panel provides additional permissions and access for a user. The availability of these settings is dependent upon user level and/or how the account has been configured. The four features and affected functionality include Add to Dictionary, JustEdit, Page Check, and Failed Login Notification.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add to Dictionary</td>
<td>Indicates whether or not this user can add words to the spell check dictionary. Select the checkbox to allow users to add words to the custom dictionaries via the WYSIWYG Editor. By default, user levels 0–8 do not have the checkbox selected.</td>
</tr>
<tr>
<td>JustEdit</td>
<td>Enables and disables JustEdit for this user. This option only appears if JustEdit has been set to Set by User or Set by Administrator at the account level. If JustEdit has been set to Disabled or On for Everyone at the account level, this option will not appear in the Preferences panel. For more information about JustEdit, visit the JustEdit page.</td>
</tr>
<tr>
<td>Page Check</td>
<td>Enable and disables Page Check for this user, dependent upon the account settings. If set to On for Everyone at the account level, this is dimmed and preselected. If set to Set by User at the account level, the user may configure this option from Settings. If Set by Administrator is set, then an Level 10 administrator may enable and disable Page Check on a user-by-user basis. If</td>
</tr>
<tr>
<td>Failed Login Notification</td>
<td>Receive a notification when the user has made too many failed login attempts.</td>
</tr>
</tbody>
</table>

Field

Add to Dictionary

JustEdit

Page Check

Failed Login Notification
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Page Check is not enabled at the account level this is not available.</td>
</tr>
<tr>
<td>Failed Login Notification</td>
<td>Allows a Level 10 administrator to be notified when any other users are locked out of their account. This is only available for users assigned as Level 10. Select the checkbox for any Level 10 administrators that should be notified when any user has too many failed login attempts. The Failed Login Attempts field can be configured at the account level; entering a number sets the standard.</td>
</tr>
</tbody>
</table>
LDAP Configuration

LDAP Configuration Overview

The LDAP Configuration panel only applies if an LDAP system is in use for the institution. It specifies the user's LDAP information in order for OU Campus to communicate with the LDAP server. This provides authentication and allows users to use the single sign-on service provided with the LDAP credentials used for the institution. For more information about authentication:

Authentication Methods

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Type</td>
<td>Specifies the authentication type for the LDAP system.</td>
</tr>
<tr>
<td></td>
<td>• Simple specifies plain text authentication via port 389.</td>
</tr>
<tr>
<td></td>
<td>• Simple (SSL) uses SSL to authenticate via port 636.</td>
</tr>
<tr>
<td></td>
<td>• Simple (StartTLS) uses TLS (aka SSL 3.0) to authenticate via port 636.</td>
</tr>
<tr>
<td></td>
<td>Please be aware that when using SSL or StartTLS, the SSL certificate for the LDAP server needs to be submitted to the OmniUpdate Support team for installation prior to using LDAP authentication. Should the certificate or hostname need to be changed at any point following the initial installation please be sure to send notice at least 24 hours in advance so the changes can be made and the server can be restarted. Note: LDAP users will not be able to log into OU Campus if the certificate or hostname that is installed does not match the current configuration of the LDAP server.</td>
</tr>
<tr>
<td>Hostname</td>
<td>The name of LDAP server.</td>
</tr>
<tr>
<td>DN</td>
<td>The unique LDAP identifier for this user; the full and complete distinguished name (DN). For example: &quot;cn=myusername,cn=Users,dc=example,dc=com&quot;.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>Please make sure the password is longer than four characters.</td>
</tr>
</tbody>
</table>
New User Options

The New User Options are only available during the initial creation. When creating a new user the following items are available in addition to the other panels of information:

- Creating a group of one with just the new user as a member.
- Sending a welcome message. Select this checkbox to enable the other related options.
- Sending a password with the welcome message is only available when creating a new user and an email address is defined for the user.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Group</td>
<td>create a group with this name and put this user in it</td>
</tr>
<tr>
<td>Send Welcome Message</td>
<td>send a welcome message to the user’s email address</td>
</tr>
<tr>
<td>Send password in welcome message</td>
<td>send a password in welcome message (does not apply to LDAP, CAS, or Shibboleth)</td>
</tr>
</tbody>
</table>

**Creating a Group of One**

Create Group creates a group of one that can be used if only one individual should be provided access to a particular directory, page, or editable region. This is not selected by default when creating a new user. A group of one may be necessary if only one person should be given publishing rights in order to override an approver.

If a group of just the one user is not desired (the group name will be the user name), make sure that the checkbox is not selected. It is advised that groups of one should not be created unnecessarily as having too many groups can make assignment of the access settings more difficult.

**Sending a Welcome Message**

When creating a new user, it is helpful to send the user a welcome message notifying the user that access to OU Campus has been granted. This can include a personalized message, but it can only include the password for an OU Campus user; that is, if CAS, Shibboleth, or LDAP are not being used for purposes of authentication.

1. Click **Send Welcome Message**.
2. Click **Send Password in Message** if CAS, Shibboleth, or LDAP are not being used. This sends the password to the user.
3. Optionally, in the **Additional Message to User** field, include a personalized message.
4. The message is sent once **Create** is clicked.
NOTE: Unless an email address is defined, a welcome message cannot be sent. If no email is defined for the new user, the Send Welcome Message checkbox will be unavailable.
Setup Toolbars

Overview

Setup Toolbars gives the administrator the ability to create custom WYSIWYG toolbars or edit existing toolbar configurations. Having custom toolbars allows an administrator to make specific functionality available on a certain toolbar and in turn assign the toolbar to a user or region. This helps restrict the type of changes a user can make to content.

For example, if users should not be able to change the font family or font sizes of text, a toolbar can be created that does not include the Font Family and Font Size drop-downs. It can then be assigned to a directory, user, page, or even an editable region. Likewise, if an editable region is used in which a user should only be allowed to insert a video, then a toolbar can be created that only includes the Insert/Edit Embedded Media. The toolbar is then assigned to that editable region. One common use of a customized toolbar is to limit the editing options of an include file, such as that which is used for a navigation file.

The Toolbars screen can be accessed from the global navigation menu by selecting Setup > Toolbars.

Customized toolbars are created and edited from the Toolbars screen. Assigning them can be accomplished via access settings or can be part of a template.
The Toolbars screen includes the following features and functionality:

- Indicates the number of toolbars
- Toolbars can be filtered
- New toolbars can be created
- Toolbars can be sorted by name
- Multiple toolbars can be selected and deleted en masse
- A toolbar can be edited by clicking the linked toolbar name, selecting the adjacent checkbox, or hovering over the toolbar row and clicking Edit
- A toolbar can be created by copying an existing toolbar
- A singular toolbar can be deleted by hovering over the row and clicking Delete

Creating a New Toolbar

The WSIWYG toolbars are organized into three rows, each with unique tool groups. These tool groups are displayed in the toolbar, separated by a vertical line. Certain tools included in the toolbar may appear dimmed or unavailable. These tools require prior on-screen actions to be performed before the tool becomes available. For instance, when creating a hyperlink a user must first highlight the text from which they wish to link. For more information about available toolbar tools and their functionality:

Toolbar Reference

Any number of new toolbars can be created as necessary, and after creation they are available for assignment to a user or specific region. On the New Toolbar screen, a preview is displayed at the top of the screen. Under the Settings panel, the Buttons section shows all of the available tools that can be added to the toolbar. Each tool can be enabled or disabled by selecting the checkbox under the corresponding tool icon. The Options section is designated for additional functionality, such as how information is pasted into the WYSIWYG Editor.

Naming Convention for Group Creation and Editing

Names can contain:

- Lowercase letters
- Uppercase letters
- Numerals 0 through 9 (inclusive)
- Underscores _
- Hyphens -
- Spaces
- Periods .

Names must:

- Be a minimum of two characters in length
Names must not:

- Be an empty string
- Be named Everyone as that is a system group and reserved
- Be greater than 32 characters in length

1. To create a new toolbar, navigate to the Toolbars screen and click the **New** button. The Preview panel shows the preview of how the toolbar with the selected tools will appear.

![Preview panel showing toolbar settings](image)

2. From the **Settings** panel, enter the name in the **Toolbar Name** field.

![Settings panel](image)

3. Under the **Buttons** section, select the checkbox for each tool to include on the toolbar. Clear a checkbox to remove it from the toolbar. Note that **Select All** adds every tool to the toolbar, whilst **Deselect All** removes every tool from the toolbar.
4. Select any **Options** that are necessary. The two additional options that are available are:

- **Font Size Set**: Any configured **Font Size Sets** are available to add to the toolbar.
- **Paste**: The paste option determines how a user can paste information into the WYSIWYG Editor.

5. Click **Create** to finalize the creation. The system displays a message at the bottom of the screen indicating the successful creation of the toolbar. The toolbar is now shown in the Toolbars list view.
Paste Options

Paste options control which buttons for pasting content are available on the toolbar for use within the WYSIWYG Editor.

The first option creates two paste buttons. The first button performs two types of pastes in that it removes the MSO formatting from content pasted from Microsoft Office. When pasting from content copied from a web page, the paste retains valid content, code, and styling for HTML. The second button with this option, when activated in the WYSIWYG, removes formatting and pastes plain text only.

The second option will show only a single paste button on the toolbar, the Paste as Plain Text Only tool. When used in the WYSIWYG Editor removes all formatting and pastes as plain text only.

Editing a Toolbar

To modify an existing toolbar:

1. Navigate to Setup > Toolbars.
2. Hover over the page row and select Edit.
3. Make any necessary changes and click Save. The system displays a success message at the bottom of the screen.

Deleting a Toolbar

Deleting a toolbar removes it from the database and removes the toolbar from any access settings to which it was assigned. For example, deleting a toolbar that had been assigned to a specific page removes it as being the toolbar used for editing that page. Any access setting that has a deleted toolbar automatically uses the default setting, which is to inherit from parent. To delete a toolbar:

1. Navigate to Setup > Toolbars.
2. Hover over a toolbar row and select Delete.
3. A dialog box will appear asking the user to confirm or cancel deletion. Select **Delete**. The system displays a success message at the bottom of the screen.

**Assigning a Toolbar**

Normally, it can be helpful to assign toolbars to users based upon skill level and permissions. However, there are occasions when a toolbar is more appropriate for a page, or in many cases solely for an editable region such as a sidebar or navigation element.

When a toolbar is being assigned via the access settings, it is important to understand that the setting closest to the content takes precedence. The order of precedence is:

- **User** (least precedence)
- **Site**
- **Directory**
- **Page**
- **Editable Region** (greatest precedence)

**Assigning a Toolbar to a User**

After a toolbar has been created, it can be assigned to one or more users. When a toolbar is assigned to a user, and a different toolbar is assigned to a page, the page setting takes precedence over the user setting. A Level 10 administrator can assign a toolbar to an individual user. Assignments to a user are account-wide.

To assign a toolbar to a user:

1. Navigate to **Setup > Users**.
2. From the users list, hover over the user row and select **Edit**. Additionally, clicking on the username in the row item will allow the administrator to edit the toolbar settings.
3. From the **Restrictions** panel > **Toolbar** drop-down, select the toolbar to assign to the user.
4. Select **Save**.

**Assigning a Toolbar to a Site or Directory**

A toolbar assigned from the access settings for a site overrides any specified at the user level, but are overridden by any toolbar specified for a specific folder, page, or editable region. Content created within a directory with a toolbar defined by the access setting will inherit the directory setting unless overridden by a setting closer to the content. When assigning a toolbar at the site or directory level, the changes can also be made recursively. If not assigned, the default is to inherit the parent setting.

1. Navigate to **Setup > Sites** or to the directory.
2. Hover over the site row and from the **Edit** menu, select **Site Access**. For a directory, from the **Edit** menu, select **Access**.
3. The change in toolbar assignment may be made recursive by choosing: **Apply Selected Settings to All Existing Files and Folders in the Site** (or Directory). Applying a setting recursively applies the change to all existing files and subdirectories as well as to those that will be created new. Otherwise, changes are only applied to content created going forward. This does not override a toolbar assignment made with an attribute on an editable region.

4. From the **Toolbar** drop-down, choose the toolbar.

5. Click **Save**.

### Assigning a Toolbar to a Page

To assign a toolbar to a specific page or directory:

1. Navigate to the Pages list view in **Content > Pages**.
2. Hover over the page row and from the **Edit** menu, select **Access**.
3. From the **Page Access Settings** dialog, select the toolbar from the **Toolbar** drop-down.
4. Click **Save**.

### Assigning a Toolbar to an Editable Region

The process for assigning a toolbar to editable regions differs slightly. An editable region can be viewed in the code view of a PCF. But because editable regions are defined by an OU Campus template, the toolbar assignments of this type should be defined in the corresponding TMPL file, so that the changes for a page template can use the assigned setting. A user must be a Level 10 administrator in order to assign editable regions a specific toolbar.

1. Navigate to the local template directory that was defined under **Setup > Sites**. In this example, `/_resources/ou/templates` is the template directory.
2. Check out the TMPL file. Hover over the template row and select **Edit**. From the menu, select **Source**.
3. In the Source Editor, locate the editable region to be assigned a toolbar. An editable region using the comment style of OU tagging is surrounded by `<!-com.omniupdate.div>` tags as shown in this example:
4. To define a specific toolbar, the attribute and corresponding value -- `toolbar="filename"` -- is included in the `<!--com.omniupdate.editor>` tag, where "filename" is the name of the toolbar that the administrator wishes to assign. The resulting code should look like:

```html
<!-- com.omniupdate.div label="twocolumn_content" group="Everyone" button="700" break="break" --><!-- com.omniupdate.editor toolbar="filename" csspath="/resources/ou/editor/onecolumn.css" cssmenu="/resources/ou/editor/styles.txt" width="1050" -->
<h2 class="h-color-link"><!--%echo var="title" --></h2>
<!-- /com.omniupdate.div -->
```

5. Click **Save**.

6. Test the changes by creating a new page with the edited template.
Font Size Sets

Overview

The Font Size Sets option allows administrators to create custom sets of font sizes that will appear in the Font Size drop-down in the WYSIWYG Editor toolbar. Each set of sizes may be composed of up to seven sizes for a unit of measurement: e.g., px; pt; em; and x-small, x-large, et cetera. These sets may then be applied to different custom toolbars to allow them to appear in the drop-down list in the editor.

From the Font Size Sets list view, administrators can:

- Filter the list of font size sets
- Create new sets using the New button
- Sort list view columns by Name and Sizes
- Click an existing set to edit it
- Select font size sets using checkboxes
- Hover over each row to display Edit and Delete options.
Adding a New Font Size Set

1. While logged in as a Level 10 administrator, choose **Font Size Sets** from the **Setup** menu.
2. Click **New**.
3. Add a **Name** for the set. When assigning a font size set to a toolbar, the choice is available by name.
4. In the **Sizes** field specify the first font size and unit of measurement; e.g., 6px. It is recommended to define the smallest size first as that will appear at the top of the list. Click **Add Size** to add another field for another font size. Enter one font size per field. Font sizes can be three digits long with up to four decimal places available.
5. Repeat step 4 as necessary to add each additional size.
6. When finished, click **Save**.

To remove a font size, click the delete icon by the field.

After the initial creation, a font size set may be edited, deleted, or assigned to a toolbar.

**Assigning a Font Size Set to a Toolbar**

1. Select **Toolbars** from the **Setup** menu.
2. Select a toolbar to edit or create a new one if necessary.
3. In the **Options** area, from the **Font Size Set** drop-down menu, choose the new font size set.
4. When finished, click **Save** or **Create**.

The font size is assigned as inline CSS with a span; for example,

```html
<p>
<span style="font-size: 2px;">This is text assigned a smaller font.
</span>
</p>
```
Gadgets

Overview

Administrators can add new gadgets and edit existing gadgets from Setup > Gadgets. From this screen, administrators can configure access settings for each gadget in the system, choose which gadgets appear in the Gadgets sidebar and Dashboard by default, and other settings unique to each gadget.

Gadgets are found in either the Gadgets sidebar, a global element that can be expanded and collapsed from the right side of the OU Campus interface, or on the Dashboard. Currently there are a total of 15 system gadgets included with OU Campus, but custom gadgets can be created by administrators and added into the system at any time.

The Gadgets screen includes the following features and functionality:

- Number of gadgets in the list
- Filtering by the Name or Type column
- Drop-down menu where administrators can choose to display All Gadgets, System Gadgets, or Custom Gadgets.
- The New button for adding additional gadgets to the system
- Sortable columns for Name, Type, Access Group, and Location/Options.

Clicking a gadget name will bring up the Edit Gadget modal, where access settings, display options, and other settings can be changed.
Gadgets are available account-wide and can be either a system gadget or custom gadget. System gadgets are included with the CMS, designated with OU icon, and cannot be deleted. Administrators can add custom gadgets, and these are available for each user to customize their dashboard and/or Gadgets sidebar.

### System Gadgets Reference

<table>
<thead>
<tr>
<th>Gadget</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity Gadget</td>
<td>Dashboard, Sidebar</td>
<td>The Activity Gadget shows all types of content with recently performed actions by any and all users, such as a scheduled publish, expire, or upload. It is an administrator-only, system gadget that cannot be assigned an access group and is shown</td>
</tr>
<tr>
<td>Gadget</td>
<td>Location</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>by default on the Dashboard and Gadgets sidebar.</td>
</tr>
<tr>
<td><strong>Dependency Tag Info Gadget</strong></td>
<td>Sidebar</td>
<td>Search functionality for dependency tags that reports information about the tag. Valid search syntax is shown below the field. It is a system gadget that is shown by default on the Gadgets sidebar and does not have any configurable properties.</td>
</tr>
<tr>
<td><strong>Images Gadget</strong></td>
<td>Sidebar</td>
<td>Drag and drop images from any folder into edit views. It is a system gadget that is shown by default on the Gadgets sidebar when editing with the WYSIWYG Editor or Source Editor and does not have any configurable properties.</td>
</tr>
<tr>
<td><strong>Inbox Gadget</strong></td>
<td>Dashboard</td>
<td>Provides a scrollable list of recently received messages. It is a system gadget that is shown by default on the Dashboard and does not have any configurable properties.</td>
</tr>
<tr>
<td><strong>Link Check Gadget</strong></td>
<td>Sidebar</td>
<td>Checks all links on a page for broken links and allows users to send a report to any user in the system. It is a system gadget that is available on the sidebar and does not have any configurable properties.</td>
</tr>
<tr>
<td><strong>My Checked-Out Content Gadget</strong></td>
<td>Dashboard, Sidebar</td>
<td>Shows the content checked out by the current user and the date/time stamp that the content, which can be a page, asset, or file, was checked out. Within this gadget, the pages are linked and can be clicked to for editing or approving. The light bulb icon indicates the page is checked out. It is shown by default on the Dashboard and Gadgets sidebar and does not have any configurable properties.</td>
</tr>
<tr>
<td>Gadget</td>
<td>Location</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Page Analytics</td>
<td>Sidebar</td>
<td>With the Page Analytics Gadget, data tracked for analysis with Google Analytics is available within OU Campus for each in the form of a sidebar gadget. The Page Analytics Gadget can be configured to be shown or hidden by each user for their Gadgets sidebar. Administrators can assign an access group to each view and configure the availability of the gadget itself. Any views from the Google Analytics account that have been added to OU Campus, and not otherwise restricted, can be selected.</td>
</tr>
<tr>
<td>Page Info Gadget</td>
<td>Sidebar</td>
<td>Displays information about the file currently being viewed or edited. It is a system gadget that is hidden by default on the Gadgets sidebar when editing with the WYSIWYG Editor or Source Editor and does not have any configurable properties.</td>
</tr>
<tr>
<td>Page Parameters Gadget</td>
<td>Sidebar</td>
<td>Edit page parameters directly from the gadget without having to navigate away from the Preview or Edit view. This is a system gadget that only appears when a user is viewing a page. Administrators can choose whether meta tags are shown in the gadget.</td>
</tr>
<tr>
<td>Request Help Gadget</td>
<td>Sidebar</td>
<td>Sends page and user information along with a custom message to a pre-defined group in OU Campus who can help users in need. This is a system gadget that is shown in the sidebar. Administrators configure the group to which a message is sent.</td>
</tr>
<tr>
<td>Site Analytics</td>
<td>Dashboard</td>
<td>With the Site Analytics Gadget, data tracked for analysis with</td>
</tr>
<tr>
<td>Gadget</td>
<td>Location</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Google Analytics</td>
<td></td>
<td>Google Analytics is available within OU Campus in a handy, colorful, intuitive, and flexible Dashboard gadget. The Site Analytics Gadget can be configured to be shown or hidden by each user for their Dashboard. Administrators can assign an access group to each view and configure the availability of the gadget itself. Users of the Google Analytics account can configure views as necessary to provide a bird's eye view of the analytics reporting for the entire site, or alternatively by applying filtering, can provide a more granular view.</td>
</tr>
<tr>
<td>Snippets Gadget</td>
<td>Sidebar</td>
<td>Drag and drop any snippet into an edit view. It is a system gadget that is shown by default on the Gadgets sidebar when editing with the WYSIWYG Editor or Source Editor. It can be configured to with an access group whose members have access to the source code of the snippet in the gadget.</td>
</tr>
<tr>
<td>URL Shortener Gadget</td>
<td>Sidebar</td>
<td>Enter a long URL to have it shortened. It can dragged onto the editing field. It is a system gadget that is shown by default on the Gadgets sidebar and does not have any configurable properties.</td>
</tr>
<tr>
<td>Workflow Gadget</td>
<td>Dashboard, Sidebar</td>
<td>Gives users the ability to track all workflow items they are involved in from one gadget. Users involved in a particular workflow item can message each other directly inside the gadget. This is a system gadget that appears in both the dashboard and the sidebar and has no configurable properties.</td>
</tr>
<tr>
<td>Gadget</td>
<td>Location</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>YouTube Gadget</td>
<td>Sidebar</td>
<td>Drag and drop YouTube videos from linked YouTube channels or by searching all of YouTube. This is a system gadget that appears in the sidebar when a user is inside the WYSIWYG or Source Editor of a page. From the Gadgets Setup screen, administrators can give users the ability to search all of YouTube from the gadget.</td>
</tr>
</tbody>
</table>
Templates

Templates Overview

Authority Level: Available to Level 10 and Site-Specific

Managing templates allows an administrator to control what the end users have access to create as well as which end user have access to a specific template. This includes the creation of new pages, new sections, and new empty folders. Here are two important concepts to distinguish between when managing templates:

- Assigning a group of users to a template determines which users (as members of that group) can utilize that template
- Assigning a template group to a directory determines which templates can be used in that directory

New Folder v. New Section

The difference between creating a new folder and creating a new section is that when creating a new section the template can be configured to create new pages as well. The basic New folder tool generally should not be used to create new directories that will contain web pages, as the support files are not created when selecting the New Folder checkbox. This will lead to error message as the supporting pages needed by the XSLs will not be available. The most common use of the New Folder checkbox is when users need a directory to contain images, PDFs, Word docs, or other non-web page files. For this reason, it is generally recommended to use template groups to allow administrators to repress the ability to have empty folders created in directories, as often times users can become confused between the basic (built-in) New Folder tool and new section templates (which create folders and files).

Assigning a User Group to a Template

It is the assigning of a group (that consists of users) to a template that determines who can use that particular template to create new pages (or sections). The Everyone group is a system group that includes all users and cannot be edited at the administrator level. The None group indicates that no user group assignment has been made and that only Level 9 and Level 10 administrators have access. Any other group assignment allows for the members of said group to use that template. If for the Faculty template, the assigned group is the Academics group, which includes the members of the administration that are allowed to create new faculty profiles, those are the only individuals who will have access to that template. This is one way to limit access to template usage for page creation. To make sure that only that template can be used, in the access settings for the Faculty directory, the assigned Template Group is “Faculty.” And in that template group, only the Faculty template is included.

Some templates have a specific purpose and should only be used in a specific directory. This prevents new sections and pages from being created in areas in which they should not and also helps by disallowing access to users who should not have the ability to use templates to create certain types of content.

For example, the Faculty Profile template has a specific design for the content that is presented, which includes the same bits of information that should be provided for each faculty member. The site developer may choose to make this template the only one available for new page creation within the Faculty directory. This can limit access to who can create new profiles, as well as ensure that when creating a new faculty profile only this one template can be chosen and that all the appropriate information is included.
Template Options

Templates and template groups can be managed from Setup > Templates. This includes configuring the settings for specific templates and for access to configuring templates groups. For getting started with template options:

Template Options

Template Groups

Template groups can be created and then used to restrict the use of templates to a specific directory or directories by assigning the template group in the access settings. For more information:

Template Groups

Template Files

When an account and the sites within it are initially configured, by default in the site settings, template files are configured to be stored locally. While template files may also be stored remotely (on the production server), it is not usually configured in a such a manner. For more information:

Template Files
Template Options

Template Options Overview

The Template Options screen shows all available templates, including those being inherited from the hidden OMNI-INF folders. The three basic settings available for template management:

- Defining the title of the template as seen by end users
- Assigning an access group whose members will be able to use the template
- Defining the thumbnail URL that provides the image that is seen by end users

Template Files Location

The template directory is configured in the site record (Setup > Site) and the location for templates can be configured to be local or remote; although, it is a best practice to use local templates. The directory location is often set to the following location: `/resources/ou/templates`. Thumbnail images used for templates are commonly included in this directory and with Binary Management enabled should be published to the production server.

Templates, in this context, refer to a set of files by which users can create new content. The templating framework used within OU Campus utilizes XSL and the term "templates" is also used by web developers to informally refer to the `<xsl:template>` element in XSL stylesheets. These are two separate concepts, and while they can be intertwined within the context of OU Campus templating, they should not be confused.

The CMS is flexible as it allows for the integration of various web-related protocols, styling elements, markup and scripting languages, and this includes the process of using OU Campus templates from which users can create new content.
Templates Access Settings

Templates are made available to specific user groups for creating new content. Creating new content from a user perspective most frequently includes creating new pages and sometimes new sections, but templates can be more specifically designed to create a new RSS article, new RSS archive, a new folder, and so on.

The ability to limit the use of a template to a specific group helps an administrator manage the creation of new content based on users. When used in conjunction with template groups, it allows different groups of users to see different templates that are assigned to the directories. This provides a very granular control over new page and section, as well as other new content creation.

Templates can be used without using template groups as well. For instance, if it is necessary to allow only administrators to create new sections, but all other templates should be readily available to all users in all directories, assigning a group with just administrators as members to the new section templates can be sufficient. However, remember that using template groups is the only way to prevent the basic built-in “New Folder” tool from being made available, and it can also be used to create empty groups if new pages and sections should not be available for creation in a particular directory.

Template Options Panel

The Template Options panel shows the number of templates available, lists the templates and settings, and the templates can be filtered by the value of the Title field.

Three settings for individual templates can be configured here:

- **Title**: Defines the friendly name that is shown on the drop-down for the New button and when clicking the New button. The friendly name for a template is also shown when hovering over the list view for template groups and when editing template groups.
- **Group**: Allows assignment of a group whose members are able to use the template. Unless otherwise restricted, the template is visible from the Pages list view with the drop-down on the New button and when clicking the New button.
- **Thumbnail URL**: Determines the thumbnail image that a user sees for the template. If left blank, the http root, template path, and file name corresponding to template with the .gif appended is automatically populated. For example, if the file name of the TCF is interior.tcf, the file name populated for the image is interior.gif. An image file location can be specified by URL for a location on the production server or other publish target, and other image file formats (e.g., PNG, JPG) are acceptable.
Configuring the Title for a Template

1. Navigate to Setup > Templates.
2. In the Title field, provide a friendly name for the template. The title for the image is displayed when using the New button. This is also used for screen readers and helps fulfill Section 508 compliance requirements. The default Title text is the name of the TCF.
Assigning Access to a Template

Assigning access to a template involves creating a group of users whose member will be allowed to utilize the template. Prior to assigning a group to a template, the group itself should be created in Groups and members assigned to it.

1. Navigate to Setup > Templates.
2. For the template, select the group from the Access drop-down.
   - Selecting Everyone makes the template available to all users, who can then create new content using the template. This is the default setting.
   - Selecting a specific group will make the template available only to members of that group.

Defining a Thumbnail Image for a Template

1. Navigate to Setup > Templates.
2. The Thumbnail URL should be configured with the complete URL (including http://) for the location of the image on the production server or publish target and is used to represent the template when a user selects new content. If left blank, the http root, template path, and file name corresponding to template with .gif appended is automatically populated. For example, if the file name of the TCF is interior.tcf, the file name populated for the image is interior.gif. An image file location can be specified by URL for a location on the production server or other publish target, and other image file formats (e.g., PNG, JPG) are acceptable. A standard size for the thumbnail is 150px by 150px.

3. Click Save. The screen appears the same whether or not Save has been clicked, but if Save is not clicked, all changes are lost when navigating away from the page.
Facebook

Overview

This section details how to setup Facebook Pages in OU Campus and in Facebook, and utilize the OU Social App. OU Social requires an app be added to the Facebook Page through Facebook and a page designated through OU Campus that will provide the content for the Facebook Page. The OU Campus page contains the content and styling. The OU Social app is used to integrate both accounts and add a Facebook Page Tab using the OU Campus page. Advantages include that the content need only be maintained in one place and that the styling can be consistent with the main web sites style. The tab at Facebook can be used as a welcome, landing, or informational section.

Facebook Pages can be added by a Level 10 administrator from Setup > Facebook. The Facebook Page must be created at Facebook prior to integration with OU Campus. To read more about actually sending to Facebook, and to find out how to use Facebook within OU Social, see Send to Facebook. After the pages are added in both systems, the OU Social app manages the integration between OU Campus and Facebook.

Be sure to read the warning at the end of this page regarding changing Facebook passwords.

Facebook Account vs. Facebook Page

It is important to understand the difference between a Facebook account and a Facebook page. A Facebook account, or timeline, is for personal, non-commercial use only. They represent individuals and must be held under an individual name. Pages are for professional or official use, and allow an organization, business, celebrity, or band to maintain a presence on Facebook. Facebook pages are only allowed to represent real organizations and should be created by an authorized representative.

In addition, pages are managed by administrators who have personal Facebook timelines. Pages are not separate Facebook accounts and do not have separate log in information from your timeline. They are merely different entities on the site, similar to how groups and events in Facebook function. Once a page is set up within the timeline, other administrators can be added to help manage the page. Administrators are other individuals with a personal Facebook timeline. People who choose to connect to the Facebook page will not be able to see identify the page administrator or have access to the personal account.

Creating a Facebook Page in Facebook

To use Facebook within OU Campus and OU Social, a Facebook page needs to be configured. The following steps for creating a Facebook page can be completed from a Facebook account.

1. From the Timeline view, click Create a Page at the bottom of the screen.
2. Select the type of organization the page represents.
3. Read and Agree to the terms.
4. Fill out the rest of the information about the page.
5. This creates the URL for the Facebook page. Several Facebook wizards at the Admin Panel run to help with set up.

**Adding a Facebook Page in OU Campus**

1. Navigate to **Setup > Facebook**.
2. To add a new Facebook page, click **New**.

![Facebook Pages Table]

3. A dialog will appear prompting the user to **Authorize** OU Campus to access the Facebook account.

![Authorize Dialog]

4. Click **Authorize**. Authorize attempts to login to an existing Facebook account/personal timeline and discover any pages that exist for it. There are various results:
   - If already logged into Facebook and pages exist, the system shows the pages linked to that account.
   - If logged into Facebook and no pages exist, a message to the affect that there are no pages is displayed. Use **Create a Page** at Facebook before attempting to add again, or if necessary to access a different account, log out of Facebook with the current user and attempt to **Authorize** again.
   - If not logged into a Facebook account, a dialog is displayed. Enter the login credentials: email address and password.
   - If all pages within the account have already been added, a message is displayed to that affect.
5. If prompted, click **Allow** to allow OU Social to access the pages that need to be added to OU Campus.
6. Click **Login**.
7. A dialog will appear prompting that the authorization process is completed, and the available Facebook pages for that account are listed. Only pages that have not already been listed are shown.
8. Use the checkboxes next to the pages to enable the page. In order for the page to be available for users at the time of publish, it must be enabled.
9. If desired, select an **Available To** group and provide a **Description** to help users in OU Campus choose the appropriate page to which to post.
10. Click **Save**.

The page or pages are now shown on the Facebook Pages screen. Pages may be enabled or disabled by editing the record from the list view and selecting or clearing the checkbox. A page must be enabled for it to be offered as a choice to a user at the time of page or file publish.

**Editing Facebook Pages in OU Campus**

Select a page by either using the left checkbox and clicking the blue Edit button that appears in the top row, or by hovering over the desired page and choosing the Edit option that appears there. This is also where the path for the content that will populate on the Facebook Page when visitors click the OU Social app added to the page. For more details on how to use this feature, see:

**OU Social**

<table>
<thead>
<tr>
<th>Page</th>
<th>Enabled</th>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OU Campus Training</td>
<td>✔️</td>
<td>Everyone</td>
<td>Training Department Page</td>
</tr>
<tr>
<td>Training OU Campus</td>
<td>✔️</td>
<td>Everyone</td>
<td>Training page for OU Campus</td>
</tr>
</tbody>
</table>

The Edit Facebook Page dialog includes:

- **Name**: This cannot be changed on OU Campus and can only be changed by the page’s administrator within Facebook.
- **Description**: A brief description that helps OU Campus users know which page to choose.
- **Available To**: Assigns an access group whose members have the permission post to the page. In other words, if a user is not in the assigned group, the Facebook page is not available to them at the time of content publish.
- **Welcome Page**: Path to the HTML page that populates on the Facebook Tab when using the OU Social app with a page. Click **Choose** to navigate the folder structure of the site. A frequently used location to contain the OU Social page is: `/_resources/ousocial/index.html`
  Click **Clear** to remove the populated page.
- **Enabled**: The ability to enable or disable the Facebook page from being available at all during time of page publish.
The Welcome URL is utilized with OU Social and is a path within OU Campus. The content and styling on the page is shown when clicking the Tab on the Page. Click Choose to navigate to and select the file. It can be changed at any time. The content can be edited through the OU Campus page as any page can be and the styling can be defined in an XSL.

Adding Default Text for Facebook

Once a Facebook page has been authorized and connected to the appropriate Account or Site, Default Text can be configured so that it is available to users at the time of page publish or with a scheduled publish. To utilize Send to Facebook during page publish, Facebook account settings must be configured from Setup > Account.

At the Account Level

1. Navigate to Setup > Account.
2. Under the Publish Settings options, there is a field called Default Tweet/Wall Post.
3. Enter a **Default Tweet/Wall Post**. This sets the default text for tweets and wall posts for the sites within an account, which can be used or edited at the time of page publish by navigating to the **Social Media** tab in the **Publish** dialog. This allows standardized text to be defined; for example, the hashtag or name for the institution might be included to help minimize typographical errors, or reinforce branding or trending topics. A maximum of 140 characters are allowed for Twitter, and 420 for Facebook. The maximum number of characters for Facebook can only be reached when using the **Social Media** tab in the **Publish** dialog. The text for **Default Tweet/Wall Post** defaults to the character count of 140.

4. Click **Save Settings** to save changes.

**Note:** Keep in mind that the default text can be overridden at the site level and during page publish.

### At the Site Level

1. Navigate to **Setup > Sites** and click the **Edit** for the appropriate site. A site’s edit options can be found by hovering over the desired site and choosing **Edit**, or selecting the appropriate site via the checkbox and using the blue **Edit** button that appears in the top row.

2. Enter a **Default Tweet/Wall Post**. This sets the default text for tweets and wall posts for the sites within an account, which can be used or edited at the time of page publish by navigating to the **Social Media** tab in the **Publish** dialog. This allows standardized text to be defined; for example, the hashtag or name for the institution might be included to help minimize typographical errors, or reinforce branding or trending topics. A maximum of 140 characters are allowed for Twitter, and 420 for Facebook. The maximum number of characters for Facebook can only be reached when using the **Social Media** tab in the **Publish** dialog. The text for **Default Tweet/Wall Post** defaults to the character count of 140.

3. Click **Save** to save the changes.

**Note:** Keep in mind that the default text submitted here overrides any default text set at the account level, and all default text can be overridden during page publish.
Warning
If communication with Facebook fails during a publish request for either the Facebook function in the Social Media tab or OU Social, OU Campus will automatically turn off the Facebook functionality. Additionally, a message will be sent to the publisher's Workflow titled, "Facebook Status Update Failed."

When the Facebook Account password is changed, Facebook revokes all associated keys, which includes the connection or key to OU Campus. Since this key has been revoked by Facebook, all publishes to Facebook then fail for the Facebook Pages associated by that Account. To fix this issue, delete the Facebook Pages from within Setup > Facebook, and follow the initial setup steps to re-add a Facebook Page.

Should a publish request fail, a message is sent to the users OU Campus inbox that details the status of the Facebook post attempt and includes the name of the Facebook page.

When a fail occurs, the Facebook Page is still shown in the list of available pages. However, it does not appear within the publish options until it is reactivated. From within Setup > Facebook, it is possible to verify that the page has been disabled. Click the Edit button and verify that the checkbox next to Enabled is cleared, or clear the Enabled checkbox in the Setup > Facebook screen. Be sure to click Save in both instances when done.

Note: Simply clicking on Enabled does NOT reactivate the page. The Facebook Page must be completely deleted and re-added using the updated or new password. This action will delete all associated reports with regard to the Facebook Page.

Best Practices
Facebook Groups: It is recommended that you create a user group for each Facebook page, and set the access to that group.

Multiple Groups: If a user is a member of two groups; for example, Group A and Group B, and if Group A has permission to post and Group B doesn't, Group A will take precedence and allow the user to post to Facebook when publishing a page that has an access setting of Group B. This does not give access to Group A to edit the page. Only one group can be assigned access to a Facebook page.

Deleting a Facebook Page: When a Facebook page is deleted, all wall posts to that page are removed from the database and cannot be retrieved. Thus, those posts will not show up in the Custom Reports. To disable the account and still keep the information, clear the Enabled checkbox.
Setting up OU Social

OU Social Overview

The OU Social app is a means by which the landing page content on a Facebook Page can be managed using OU Campus. Utilizing OU Social involves an integration between OU Campus and Facebook.

The OU Campus Facebook pages can be added by a Level 10 administrator from Setup > Facebook. For more information:

Facebook

The OU Social app is setup for a Facebook Page by the administrator of the Facebook account.

Configuring XSL and PCF

1. After adding and configuring the app in Facebook, download the sample XSL file, or configure an XSL file in OU Campus.
2. If using the sample XSL file, update the included CSS as necessary, and make sure that the XPath is correct for the page to be used. For instance, is the XPath document/content/node() or document/maincontent/node()?
3. Upload the XSL file to the XSL folder in OU Campus.
4. Create the page to be used with Facebook using the New Page Wizard, or identify the page that should be published to both the website and Facebook.
5. Update the existing PCF stylesheet declaration (if using a page exclusively for Facebook) or add a new PCF stylesheet declaration (if using a page for both the website and Facebook).

Example Update Existing:

```xml
<?pcf-stylesheet path="/resources/xsl/fb.xsl" extension=".fb.html" title="Facebook" ?>
```

Example Add Another Instruction:

```xml
<?pcf-stylesheet path="/resources/xsl/default.xsl" extension="html" title="Web Page" ?>
<?pcf-stylesheet path="/resources/xsl/fb.xsl" extension=".fb.html" title="Facebook" alternate="yes" ?>
```

6. Save the changes.
7. Publish the page.
8. Navigate Setup > Facebook. (See the Setting up a Facebook Page page for complete details.)
9. Edit the added Facebook page.
10. Select Choose under the "Welcome URL."
11. Find and select the desired page.
12. Save the changes.

Note: An HTML template/page can be used as well. XSL is not required for use with OU Social.

Required Styling for Welcome URL Landing Page

When creating or modifying the landing page in OU Campus that will be the landing page on the linked Facebook Page, there are some styling requirements that must be noted.

1. The landing page code cannot contain any header or body tags.
2. The landing page cannot reference any external CSS.
3. All URLs within the page must be absolute.
If the site is set up to use root relative or page relative URLs with directories and pages inheriting the settings from the site, it is advisable that the settings are changed for the OU Social page(s). This can be done within the access settings. If this setting is not changed, the URL may be converted on publish to the inherited type.
Do not use root relative or page relative URLs.

For more details on configuring the landing page, visit Facebook’s Apps page.

**Best Practices**

In addition to the required styling, there are a couple of best practices that should be included in the design of the landing page.

1. The width of the page should not exceed 760px when styling for the OU Social Welcome URL landing page.
2. Styling should be achieved using in-line coding when styling for the OU Social Welcome URL landing page.
3. Assets and Snippets can also be used within the content area on the OU Social Welcome URL landing page as it is with the main website.

A basic template for OU Social’s Welcome URL landing page is available here.
This template attached is configured to work with Facebook. In order to utilize this template with both Facebook and the main website, an additional XSL page will need to be created containing the header, body and footer tags, as well as the content for the header and footer. The PCF will need to be updated with an additional processing instructions to call in that XSL stylesheet when the page is being published to the main website.

**Additional Resources**

Facebook offers information for developers and Page administrators.

Read more information on Facebook Pages.

Read more information on Apps on Facebook.

Learn about adding Facebook Pages in OU Campus on the Setting up a Facebook Page documentation page.
Setup Twitter

Overview
This section details how to set up a Twitter account for integration with OU Campus. To read more about sending to Twitter at the time of publish, please see:

Twitter

Setting up a Twitter Account
The administration of Twitter with OU Campus involves adding one or more Twitter accounts, and authorizing the accounts and the app. Once an account addition is completed, various management actions can be performed for the account as necessary, such as modifying the access group and disabling the account.

To set up a new Twitter account:

1. Navigate to Setup > Twitter.
2. Click the New button in the top right of the Twitter screen.
3. A dialog will appear prompting the administrator to Authorize OU Campus to access the Twitter account. Click Authorize.
4. Enter the username and password for the desired Twitter account and click **Authorize App**.
5. The Twitter account will automatically authorize OU Campus to access it, and a new dialog will appear confirming the authorization of the account and a prompt to save the new account.
6. Enter a **Description** to help users select the correct Twitter account when sending updates on publish. Select the **Access Group** for the Twitter account. It is recommended to create an access group for each Twitter account.

7. Click **Save**.

The Twitter account will now be available to be modified from the Twitter screen and for users to send updates to on publish.

**Modifying Twitter Account Options**

The next step is to determine who can publish to the account. After the Twitter account has been added, the account settings can be modified. To access the settings:

1. Select **Edit** by either:
   - Hovering over the appropriate Twitter account and selecting the **Edit** icon that appears on hover over.
   - Selecting the appropriate Twitter account via the checkbox to the left of the account name and click the blue **Edit** button that appears in the top row.
Clicking on the hyperlinked name of the account.

2. Using the **Edit** button will allow the administrator to update the following options:

   - **Account**: This shows the Twitter handle that is attached to the account. The Twitter handle can be seen in the Edit settings for the Twitter account however, the name of the account can only be changed through Twitter.
   - **Description**: This can help users decide to which Twitter account they want to send the tweet. As a best practice, provide a description of the account during setup.
   - **Access Group**: This allows the administrator to identify the group that has access to send tweets to the identified Twitter account. The **None** group indicates that no group has been assigned and only Level 9 and Level 10 have access to publish with Twitter. The system group, **Everyone**, grants access to all users. As a best practice, user groups should be created for each Twitter account to set access.
   - **Enabled**: This allows the administrator the ability to enable or disable the Twitter account. Clearing the checkbox disables the Twitter account but keeps it linked in OU Campus, which also allows any reporting associated with the account to still be available. Enabling the account allows users to publish to the account.

3. Commit all changes using the **Save** button.

**Deleting a Twitter Account**

If a Twitter account needs to be deleted, an administrator may either:

   - Hover over the appropriate account and click the **Delete** icon.
   - Select the account via the checkbox to the left of the account name and click the blue **Delete** button that appears in the top row.

**Note**: Deleting a Twitter account deletes any reporting associated with the Twitter account. To keep any associated reporting but disable the account, clear **Enabled** from the Twitter account's settings.

**Adding Default Text for Twitter**

At the account level and for each site, default text can be added so that it will be available to users at the time of page publish or with a scheduled publish. To utilize Send to Twitter and Send to Facebook during page publish, Twitter and Facebook account settings must be configured from **Setup > Twitter** and **Setup > Facebook**.

**Note**: Any default text added at the account level can be overridden by adding default text at the site level. Any default text added at either the site or account level can be overridden at the time of publish.

**Default Text at the Account Level**

1. Navigate to **Setup >Account**.
2. Under the **Publish Settings** options, locate the field called **Default Tweet/Wall Post**.
3. Enter a Default Tweet/Wall Post. This sets the default text for tweets and wall posts for the sites within an account, which can be used or edited at the time of page publish when the Send to Twitter or Send to Facebook feature is used in the Social Media tab of the Publish dialog. This allows standardized text elements to be defined; for example, the hashtag or name for the institution might be included to help minimize typographical errors, or reinforce branding or trending topics. A maximum of 140 characters are allowed for Twitter, and 420 for Facebook.

4. Click Save Settings and save changes.

**Default Text at the Site Level**

The configuration of default text for sending to Facebook or Twitter at the site level is similar to that of configuration at the account level.

1. Navigate to Setup > Sites.

2. Click the Edit icon for the appropriate site. Edit can be selected by either:
   - Hovering over the desired site and selecting the Edit icon.
   - Selecting the appropriate site via the checkbox to the left of the site name and clicking the blue Edit button that appears in the top row.
3. Under the **Publish Settings** options, define the **Default Tweet/Wall Post**. This sets the default text for tweets and wall posts for the site, which can be used or edited at the time of page publish in the Social Media tab in the Publish dialog. This allows standardized text elements to be defined; for example, the hashtag or name for the institution might be included to help minimize typographical errors, or reinforce branding or trending topics. A maximum of 140 characters are allowed for Twitter, and 420 for Facebook.

4. Click **Save** to save changes.

**Best Practices**

**Twitter Groups**: It is recommended to create a user group for each Twitter account and set the access to that group.

**Multiple Groups**: If a user is a member of group A that has permission to tweet and a member of group B that does not, the user will be allowed to tweet when publishing a page that is accessed through group B.

**Deleting a Twitter Account**: When a Twitter account is deleted, all tweets to that account are removed from the database and cannot be retrieved. Thus, those tweets will not show up in the Custom Reports. To disable the account and still keep the information, clear the Enabled check box found under the Twitter account's settings.
RSS Overview

RSS stands for Really Simple Syndication or Rich Site Summary. It allows visitors to subscribe to feeds on topics of interest. In a college or university setting, RSS can be used to easily deliver content such as breaking news, emergencies, and events on campus. This can save time for both content contributors and site visitors.

When new items are added to a feed, the visitor will be able to view them through a feed reader. Feed readers turn the RSS XML file into something that's easy to read. Feed readers can operate through an email client, a web browser, or as a stand-alone news reader.

RSS With and Without a Feed Reader

This XML file does not appear to have any style information associated with it. The document tree is shown below.
Feeds are often thought of as news tickers. They are often limited to a title and short description, with the title generally linking to the full article or page. Media, dates or other elements may also be included in the feed. What is displayed depends on the feed reader being used and what it is configured to display. The feeds can also be parsed to be displayed on a page within the campus website.

While feeds can be set with a plethora of extensions, they are generally XML-type files, and that is what OU Campus uses. An RSS feed is a single XML document that follows the RSS format and is hosted alongside other website resource files.
RSS in OU Campus

OU Campus can be used to manage the use of RSS as a content delivery medium for syndicated content. Template options, such as XML variables and built-in support for custom scripts in many scripting languages allow for flexible implementations in the presentation of news and media feeds.

RSS feeds and RSS feed groups can be set up by level 10 administrators and feed items can be added by users. For more information on setting up feeds, feed groups, and adding items, visit the following three pages:

- **RSS Feeds**: Traditional and Media RSS feeds are available to be created by a level 10 administrator and are assigned to a page or directory using access settings.
- **RSS Feed Groups**: RSS feeds can be easily combined into aggregate groups in OU Campus for syndication on the website or newsreader subscription. Individual feeds can be added to multiple feed groups that are updated automatically.
- **RSS Feed Items**: RSS items in OU Campus can be automatically created when a page is created, and published to a feed or feeds when the page is published.
  It is also possible for a page to be associated with a particular feed after the feed has been created.

OU Campus provides for easy creation and management of any number of RSS feeds.

The granularity of the information can also be controlled by determining if just headlines and short summaries are to be displayed or entire articles automatically downloaded. RSS feeds can be read in web browsers, email clients or stand-alone RSS software.

RSS feeds can be published to different/multiple targets. When rebuilding the feed the default publish target can be overridden.

In addition, RSS can be automatically converted into an SMS message and delivered to all subscribing cell phone users.

**Media RSS**

Media RSS extends the capabilities of RSS feeds by allowing the inclusion of media content, including videos, pictures, podcasts, and files. The easy-to-use Media RSS interface allows users to add media content to a feed without the need for any special programming or technical knowledge.

Media RSS complements the RSS 2.0 specification, allowing the attachment of media items to a feed without the need to place these items inside the RSS description. An advantage to using Media RSS, as opposed to using regular RSS 2.0, is the separation of content; the RSS description remains clean, and users are directed to visit the website in order to view media content. Some feed readers even have the ability to view information about the media content within the reader itself; however, support for this functionality is not universal and should not be relied upon.

Media RSS is compatible with any media content, so long as that content may be reached from a valid URL. This includes the following media types:

- Flash
- DIVX
- QuickTime
- Windows Media
- Real Player
- WAV
- MP3
- Podcasts

Other file types may also be added as media content. For example image files, PDF files, MS Word documents, and web pages.

Note: For true streaming, podcasts can be uploaded via OU Campus, and streaming software installed on the production server.
RSS Feeds

Overview

RSS feeds are containers for individual RSS items. In and of itself, a feed is simply an XML document that follows the RSS standards; the items within a feed are the articles that a user reads. Depending on the university's implementation, RSS feed files are usually found in the /_resources folder or in a separate /rss directory.

Feeds can be set up in OU Campus by a Level 10 administrator and then assigned to a directory or page using access settings. A list of feeds can be found by clicking

Content > RSS

in the Global Navigation Bar.

If applied to a directory, created pages will inherit the access settings for RSS. An RSS feed can also be configured to be built into a template control file (TCF) and the template can be chosen as a new page. New pages are then created within the designated directory using a news template, which is setup to look for the RSS feed and often includes fields to pre-populate the item's details.

It is possible for a page to be designated as an item for a particular feed after is has been created by a Level 10 administrator. It is also possible to have a variable in the template that allows an RSS feed to be selected for the page on page creation. To learn more about RSS items, refer to the RSS Feed Items page.

Aggregate feeds can also be created. The creation of the feed is the same as that of an individual feed, but instead of items being assigned to it, the individual feeds are assigned to it, and their items appear in it. For more information about these aggregate feeds, refer to the RSS Feed Groups page.

RSS Feeds View
Here is a breakdown of the RSS Feeds screen:

- **Local Navigation**: Allows users to navigate quickly between the RSS Feeds view and the RSS Groups view.
- **Filter**: Allows users to filter the RSS Feeds list based on the feed’s file path or title.
- **New Button**: Allows users to create new RSS feeds.
- **RSS Feeds List View**: Navigate among all existing RSS feeds for the site. The same functionalities (multi-select, hover options, sort by path or title, etc.) present in other list views in OU Campus are also available here.
- The options available on hover include Edit, Items, Publish, and Delete.

### Creating a New RSS Feed

By default, an implementation may already include RSS feeds that are within the `/_resources/rss/` or `/rss/` directory. Prior to creating a new feed, an RSS directory where the XML file for the feed will reside should be created.

To create a new RSS Feed:

1. Select **Content > RSS** from the global navigation bar. The **RSS Feeds** view is shown.
2. Click **New**.
3. Configure the **File Properties**.
4. Configure the **Feed Properties**.
5. Click **Save**.
The **File Properties** panel includes:

- **Path**: Determines where the RSS XML file will be created and feed items stored. It must be absolute to the staging root (e.g., /rss/weather.xml). It must begin with a slash and must not end with a slash. The directories within the path must be configured for the feed to be created, but the XML file itself will be created by the addition of a feed item. RSS feed paths are not modifiable after creation. Take note of the file structure before creating the feed.

- **Template**: Provides a choice of pre-defined XML structures to use. Provided are /generic-2_0.xml or /generic-mrss-2_0.xml type templates. The XML template for media is the mrss template. It should be used when adding media files (images and video) to the feed items. If the generic non-media template is used and users add media content to the feed, it will not be published. Please contact support for assistance if there are not any templates listed in the drop-down.

The **Feed Properties** panel includes:

- **Title**: Provide a title for the feed. This will be visible to subscribers.
- **Description**: Give the feed a description, which subscribers will be able to see.
- **Link**: The **Link** field should contain an absolute URL to the website (e.g.: http://www.omniupdate.com). Include the link to which the **Path** defined above will be appended. This is often the **HTTP Root** from the site settings.
- **Publish Date**: The date is auto-populated with a variable that provides the date the page is published. It can also be manually entered here, but it is recommended that it be left set to [auto] so that the OU Campus system can automatically fill it in with the feed’s publish date. If manually entered, the format for this field must conform with RFC 822 (e.g.: Sat, 07 Sep 2012 02:00:00 GMT).
- **Publish Time**: The time is auto-populated with a variable that provides the time the page is published.
• **Item Count**: Define the number of items to be displayed by the feed. For RSS feeds, the item count can be anywhere between 1–9999. Once the number of items in an RSS feed reaches this number, any older RSS items are removed from the feed.

After creating the feed, items can be added to it. A page template can be configured to not only create a page, but to prepopulate and create the RSS item details during the page creation process. If a template is used that does not have RSS items configured to be created automatically, this will have to be done manually for that page after the fact. More information on how to create RSS items can be found on the RSS Feed Items page.

### Editing RSS Feeds

Users are able to edit the properties of existing RSS feeds within OU Campus from the RSS Feeds view. The Edit RSS Feed view is very similar to the New Feed view in both interface and functionality.

<table>
<thead>
<tr>
<th>/rss/events.xml</th>
<th>GU Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>/rss/news.xml</td>
<td>GU News</td>
</tr>
<tr>
<td>/rss/weather.xml</td>
<td>Weather Alerts</td>
</tr>
</tbody>
</table>

To edit an existing RSS feed:

1. Select **Content > RSS** from the global navigation bar. The RSS Feeds view is shown.
2. Click the linked path or hover over the row to display the options and select **Edit**.
3. Make any necessary changes in the **File Properties** or **Feed Properties** panels and click **Save**.

Publish the feed for the changes to take effect.

### Publishing RSS Feeds

RSS feeds can make use of publishing to different targets. When feeds and aggregate feeds are rebuilt, they are rebuilt onto production server and publish targets alike. When Multi-Target Publish is configured and in use, a publish target can be selected to rebuild a feed to, which overrides rebuilding the feed to the default production server. When pages are scheduled to publish or expire, RSS feeds assigned to that page are rebuilt. To publish an RSS Feed:

1. Select **Content > RSS** from the global navigation bar. The RSS Feeds view is shown.
2. Hover over the RSS feed to be published and select **Publish**.
3. In the Publish Feed modal, select a target server from the drop-down to publish the feed to and click **Publish**.
Dealing with RSS Feeds

If the action was successful, a system message will appear at the bottom of the browser indicating success.

**Deleting RSS Feeds**

1. Select Content > RSS from the global navigation bar. The RSS Feeds view is shown.
2. Hover over the RSS feed to be deleted and select Delete.
3. In the Delete RSS Feed dialog, click Delete.

If the feed has been successfully deleted, a system message will appear at the bottom of the browser indicating success.

**Apply an RSS Feed to a Page or Directory**

Once the RSS feed is created, the feed can be associated with a page in two ways. The level 10 administrator can either assign RSS feed access to a page or it can be built into a template. A user selecting the RSS template during new page creation will be able to select the feed from a drop-down and then be able to add an RSS item to the page.

An RSS feed can be assigned to a directory using the access settings. If the feed is assigned to a directory, then any pages created in that directory will have the option to be associated with that particular feed.

To assign an RSS feed to a page:

1. Navigate to the Pages list view by selecting Content or Content > Pages from the global navigation bar.
2. Hover onto the page in question and from the Edit menu, select Access.
3. In the RSS Feed field, select the feed with which the items should be associated.
4. Click Save.

Assigning the feed to a directory or site requires involves the same process; simply navigate to the site or directory in question and edit the access settings as described above.

Once a feed has been associated, RSS can be selected from the Edit menu.
Final Notes

- Feeds must be set up prior to them being available to be assigned to an aggregate feed group.
- The page that the feed is associated with must be published.
RSS Feed Groups

Overview

After creating RSS feeds, it is possible to aggregate them into a group. This combines several feeds into one single RSS XML file. Subscribers can then subscribe to the individual feeds or the aggregate feed if interested in all topics within that general category. Items that appear in a feed will also appear in the group to which their feed is assigned.

An example of creating an RSS group to aggregate feeds is taking the individual Football, Soccer, and Baseball feeds and combining them into one RSS group: Athletics. The three feeds can each be viewed individually, or viewed together in the Athletics aggregate feed.

Creating a New RSS Group

Creating an RSS group is similar to creating an RSS feed, because the same fields are available for both. For additional details regarding the field settings, refer to the RSS Feeds page.

1. Navigate to Content > RSS.
2. From the RSS menu, click Groups.
3. Click the New button.
4. Fill in the Path and Template fields for the File Properties panel.
   . Identify the Path from the root of the site to where the XML file for the aggregate feed group should be created. The folders leading to the file must already exist, but the file does not have to exist. Generally, this is an XML file. For
Template
both the generic template and a media template are available.

5. Fill in the fields for the Feed Properties:
   Enter a Title for the feed. This is what will be shown in the feed readers.

   Enter a Description for the feed.

   Enter the HTTP root in the Link field. This is the path to the feed that is prepended to the feed file and should be a fully qualified URL. The trailing slash is required and the path to file should already be created.

   Leave the Publish Date blank.

   Item Count: Enter the number of items that will be displayed in feed readers before they start to "fall off" the feed. While they will still exist in the file, they will no longer be part of the public feed. This can be a number between 1 and 9,999.
6. From the **Feed Group Members** panel, from the Available Feeds list select the individual feeds to be added to the Selected Feeds list. Feeds can be moved between lists with the single arrows, or all feeds can be moved between lists with the double arrows.
7. Click **Save**. The **RSS Groups** list view is shown with the newly added group and any other previously added group.

8. Publish the aggregate feed by hovering or selecting the checkbox and clicking **Publish**. Note: A new group, like a new RSS feed, must be published to create the XML file on the production server that is the feed.

**Adding Members to a Group**

After an RSS group has been created, additional members can be created at any time. Note that an RSS feed must already be created before it can be added as a member to an aggregate feed.

1. Navigate to Content > RSS.
2. From the
   
   **RSS**
   
   menu, click

   **Groups**
   
   . The

   **RSS Groups**
   
   list view is shown.
3. Select the group to edit.
4. Under
   
   **Feed Group Members**
   
   , click in the

   **Members**
   
   field and choose the additional feed from the drop-down.
5. Click **Save** when done.

**Editing an Aggregate Feed**

An RSS Group can be modified from the RSS Groups screen in the following manner:

- Click the linked path or **Edit** to modify the group.
- Click **Publish** to rebuild the aggregate feed (useful when new members have been added to a group, for example).
- Click **Delete** to delete the feed group. This only deletes the group, but not the original feeds or items.
Access Settings

Overview

The access settings in OU Campus provide control for functionality found throughout the system. Examples of access settings include defining which users can edit a specific page, binary file, directory, or asset. Access settings can also be assigned to users; for example, a toolbar or an approver can be assigned to a user. When access settings overlap, the order of precedence determines the access setting that is used; a setting that is closer to the content overrides others. Understanding the access settings and how settings closer to the content take precedence can be very helpful in configuring a site in order to provide the appropriate access to content for specific groups of users.

Access settings can be assigned to:

- Editable regions
- Pages
- Binary files
- Directories
- Sites
- Publish targets
- Users
- Templates
- RSS feeds
- Assets
- Facebook Pages (as used within OU Campus)
- Twitter Accounts (as used within OU Campus)

Generally, access settings that can be modified include:

- Access Group
- Approver
- Enforce Approver
- Bypass Approval
- Template Group
- Extensions
- Toolbar
- RSS Feed
- URL Type
- Exclude from Search
- Exclude from Sitemap
- Directory Variables

Additional settings that involve access to content are:

- Available To (available in various locations, including the production server for a site, Facebook page, Twitter account, etc.)
- Local Assets Group (Specifies a group that can access assets only on the site on which the setting is configured)
- Lock to Site (available for assets)
- Admin Access Only (Add-Ons)

For more information, visit the Access Settings Reference Table page.
Access Settings and Workflow

Access settings can be configured to determine and implement an approval workflow. Users may have approvers set to them, which will revoke their right to publish and require them to submit pages to another user for approval instead. This applies even to user levels who would normally be able to publish on their own, the only exception being Level 10 Administrators. Approvers may be enforced, which means that the user can no longer choose to whom to send the content for approval, but are instead required to send it to enforced approver only. On the other hand, a Bypass Approval group may be set, allowing members of the group to override the approval process.

In the example above, Anna is a user editing content. Normally, her enforced approver is Bob, meaning any changes she makes need to be approved by him. However, the approver for the alumni directory is Christine, so if Anna makes changes within that director Christine must approve them not Bob. On the other hand, Anna is in the Bypass Approval group for the Faculty Page, so she may publish directly any changes she makes to that page.

Inheritance and Precedence

Two important concepts to keep in mind during the creation of workflows in OU Campus are the ideas of inheritance and precedence.

Inheritance explains how the system functions in terms of access settings being determined by the settings above them. Precedence explains that the settings closer to the content override any settings that may have been set above it.

Inheritance

Access settings are inherited by default from the parent. For example, if a site has a specific access setting, any directories created within the site will automatically have that same access setting as well unless specified otherwise. Likewise, pages and binary files inherit their parent directory setting unless otherwise restricted. New assets inherit access settings from the Site Asset Access settings. One exception to the rule of inheritance is for URL Type, as this takes the URL Type as specified with the site record if not specifically set.
One way to override inheritance is by assigning the access setting within a TCF. When a user creates new content with the template using that TCF, then the desired value for the access group can be assigned automatically. Likewise, the TCF can also be designed to allow a user to choose an access group at the time of new content creation.

When configuring the access settings and other permissions, it is generally best to start at the top and work down, as it is common for the permissions to become more restrictive and less generalized as the settings get closer to the content. For example, a site might allow access to twenty users, a directory within the site might allow access to ten, a page within the directory five, and so forth.

If the content has already been migrated into the system or configured, the recursive option within the site and directory settings may be useful. Using the Recursive Modification setting can selectively change access settings for the current item and all subordinate items, even if they have already been created; Non-Recursive Modification applies only to files created after the settings have been modified. When first assigning permissions, using the recursive setting is relatively safe, but as the permissions are changed throughout the site, the use of the recursive option should be used sparingly.

**Precedence**

Precedence takes place by giving settings closer to the content higher importance. For example, when a user has an approver assigned to their user settings, and the user is working on a page with a different approver assigned, the approver for the page takes precedence. This provides a solid workflow structure, while at the same time allowing for a flexible alternative that can be set up and used quickly and easily as a group can be assigned at various levels in the system to circumvent the approvals process, for example, to a page or directory.

In conjunction with inheritance, precedence defines the order in which settings will be used. The closer a setting is to the content, the greater precedence it takes. This is especially important to understand with regard to user settings.

Users are considered to have the least amount of precedence as they are furthest from the content. Therefore, if it is important to have settings based on the user, be sure that the setting is not different anywhere else within the site.

The order of precedence is as follows (in order of lowest to highest):
Additionally, access settings can be assigned to the servers, assets, templates, blogs, and other social media.

**Permissions for Access Settings**

**Level 8:** Can change who has access to the directory, page, binary file, or asset to any group to which he or she belongs. Level 8 users can only change settings for areas to which he or she belongs.
Level 9: Can change who can access the directory, page, binary file, or asset to any currently defined group. Level 9 does not have access to change the access settings for the site.

Level 10: Can change who can access the directory, page, binary file, or asset, as well as modify the other site access settings and directory variables, including those belonging to the site.
Planning Access

Planning Access Overview

Pre-planning access to sites, directories, pages, and specific editing regions on pages is very important for management over the long haul.

Planning Groups

When managing access, consider what content groups of users should be able to edit. First create groups of users, then build access (or editing rights) around these groups. Doing so will make it easier to manage access to sites, directories, files, and sections of files by adding and deleting users to those groups.

Remember that only Level 10 administrators can create users and groups, and that all Level 9 and Level 10 users ignore group access settings, giving these users access to everything on the site.

Planning Access to Directories and Files

Two important values for access settings are Everyone and (Administrators Only). The Everyone group is a system group that cannot be edited but includes everyone within the account. The (Administrators Only) group includes only only Level 9 and Level 10 administrators. There is also the (Inherit from Parent) group, which is the default for most of the settings if no other group has been selected.

This can be capitalized upon in an organizational sense by assigning access from the top down. Find a directory tree structure and assign it the broadest possible access in a recursive manner, using the checkbox that assigns permission to "This folder and all existing items within." Continue moving deeper through the directory tree, modifying access settings to narrow and refine access using this same manner. Note that several access values can be modified simultaneously (while leaving some values untouched) by using the checkboxes next to each property.

Reassigning Access at the File Level

As needed, override access at the file level to ensure that only the smallest possible group has access to that file.

Planning Editable Regions

Finally, editable regions of a page should tagged with the appropriate group name. There are two best practice strategies to keep in mind at this level of access.

1. Regions of a page that should be editable by everyone who has access to the file should be assigned to the special group "Everyone." Since only those who have access to the file can access the page in the first place, it is redundant to restrict access for those specific regions to the same group.
2. Regions of a page that need to be restricted to specific users should be set to specific functional groups such as "header," "footer," "left_navigation," etc., rather than the specific users themselves, and the appropriate users placed in each group. This provides the most flexibility over time, while at the same time giving users the correct access to the correct pages.

In order to tag editable regions and change their access settings, it is necessary to go into the source code of that page and change it from there.

For more information, visit the Editable Regions page.
Example

Consider the following path to a page:

/admissions/2009/fall/index.html

Following our recommended settings, the /admissions/ directory would be set to the group "admissions," making sure that the change is applied recursively.

That assigns all files and folders within the directory to the "admissions" group, including the index.html file.

The page now allows access to the following users who comprise the "admissions" group: Anna, Bob, Christine, Diego, Erika, Fred, and Grace.

The editable regions then allow access to specific user groups as follows:

- main body (Anna, Bob, Christine)
- header (Diego, Erika)
- footer (Diego, Erika)
- left_navigation (Anna, Christine, Diego, Erika)
- news (Anna, Fred, Grace)

In this example, the file index.html has five tagged editable regions: main body, header, footer, left_navigation, and news. Each of these regions is tagged in the source code with the group by the same name, with the exception of the main body regions that are tagged with the group "Everyone." With that, and the page tagging as described above, the results are as follows:

- The main body of the page will be editable by Anna, Bob, and Christine (but no one else).
- The header will be editable by Diego and Erika (but no one else).
- The footer will be editable by Diego and Erika (but no one else).
- The left_navigation of the page will be editable by Anna, Christine, Diego, and Erika (but no one else).
- The news will be editable by Anna, Fred, and Grace, but no one else. Furthermore, the only region of the page that Fred and Grace can edit is the news.

This way, if Bob someday leaves the main body group, and Henry takes his place, no changes will have to be made to the access settings themselves. All that will need to be changed is the members of the group, i.e. taking Bob out and putting Henry in.
Workflow

Overview

Workflow is used to control what users can publish with the establishment of an approval process. Workflow helps control where people can edit, who can publish, who needs to review content before it is published, and who can bypass the approval process. In the context of OU Campus, workflow is both a process and an area of the interface as the Workflow view within the Dashboard, shows the content that is pending approval.

The configuration of the system determines the roles of various users within workflow. Any level user can be deemed as an approver, or be assigned as a member of the group that can bypass the approvals process. An approver can also be assigned to specific content types within a site, or at the site level. Assigning an approver to a user in essence revokes all publishing rights for that user.

Users have different levels of access to functions within the system, inherently, based on user level, as well as by the assignation of access settings, and therefore, see different options, buttons, menus, and content. Some areas of the interface or production targets may not be viewable. For example, users that have access to a page and no other restrictions (such as an approver), have the ability to publish the page and will see the Publish button in addition to Schedule, Submit for Approval, and Expire options in a dropdown list. A user with an approver assigned is not able to publish and does not see the Publish Now or Schedule buttons, but instead only sees Submit. Users who are able to publish can choose to send content to another user, but are not required to.

When implementing a new site or several new sites, it is advisable to plan out the expected functionality in terms of workflow within the system prior to creating groups and assigning permissions. The basic steps include:

1. Define the workflow architecture.
2. Create users in the system.
3. Set approvers for users who need them.
4. Add users to groups to control access.
5. Set site, publish targets, folder, page, asset, and user access settings. Groups can be assigned to settings at multiple levels and enforced according to precedence.
6. Set groups on editable regions in page templates, page properties, and template control files.
7. Train end-users on the workflow process.
The system allows for as much or as little flexibility as desired. In some cases, it may be desired to force users to always use the DirectEdit link to access the pages to be edited. The alternative is to assign permissions at various levels of specificity, ranging from the site level to the directories housing the pages to the editable regions. Enforcing access through a DirectEdit link limits the number of groups that may need to be created, but it also limits the users’ abilities to navigate through the folder structure to get to pages to edit.

**Approvers**

There several things to keep in mind when playing the role of an approver. Once a page is sent to an approver, it is automatically checked out to that user. Other users in workflow might be completely dependent upon the approver to review and publish the page. To this end, the approver has the standard reviewing tools available such as compare, backup, and review, as well as the standard functionality found for publishing, unless another layer of review has been put into place.

As an approver, it is prudent to review a page and approve it or decline it in a timely fashion, as there may be a delay in the review cycle or with the publication of pertinent information if the page is left sitting in workflow. Publish options for a page in workflow include Schedule, Reassign, Decline, and Expire.

**Enforcing an Approver**

Flexibility is introduced into workflow with the ability to enforce an approver or not. If an approver is enforced for a user, then that user must submit any content to that approver specifically, instead of choosing to whom they submit the content. This may also be used when a peer-to-peer review is desired before the page goes to the final approver for review and publication. Then the person to whom the page is sent for review can publish it, rights permitting, or send it back to the original user or the designated approver.
There can be multiple levels of review. This situation allows for additional flexibility within the system and is defined by an approver having an approver. This implements a workflow process whereby more than one user can review a page.

Most access settings within OU Campus are configured with the use of groups. The assigning of an approver, while it can be accomplished at several levels within the system, only assigns a singular user.

**Bypassing the Approver**

In addition to choosing not to enforce an approver, there are two types of overrides that can circumvent the approval process. One is at the administrator level, as an administrator has the capability to reassign a page that has been sent for approval.

The second override is the use of the Bypass Approval access setting. A group can be assigned to the Bypass Approval setting and members of that group have the ability to publish without respecting the restrictions of any assigned approvers.

**Level 0**

Any level user in the system can be assigned as an approver and a frequently used scenario is to create Level 0 for the role of approver. The Level 0 is unique among user levels as it includes very few permissions other than publishing. This level is also known as the reviewer or executive level as the user can review, and choose to decline or publish, but cannot perform any of the editing functions. If changes need to take place, the Level 0 user needs to send the page back to the original user to have the edits completed.
Using Reports for Setting Up Workflow

The use of reporting can also be helpful when setting up workflow. Custom Reports can be used prior to setting up the access settings in order to identify the directories and pages within the site. They can also be used after configuration of the access settings is complete to verify that everything is configured as expected.

Prior to Settings Assignment

It can be helpful to run two reports prior to setting up the groups and assigning access: Directories and Pages. These reports can then be exported and conflated into one file, such as an Excel spreadsheet. Additional information can be added, such as that for access settings, an approver, and a group whose members can bypass the approval process. If other information is desired, that can be added too, but this section will focus on determining the appropriate groups needed for proper navigation.

The data can be populated once the file is configured to include the columns needed to create the access and other settings. It is helpful to add user names alphabetically under each. This allows for easier sorting so that the groups needed can be identified and created in OU Campus.

After defining which users should have access to the pages and directories, sort by the Access column in order to see how many groupings of users there are. This helps determine how many groups are needed and which users need to be in those groups. Following the same steps for publishers helps identify any additional groups that may be needed.

Keep in mind that the purpose of this is to create a site structure that allows users to navigate from the top of the site to the destination folder, but as discussed earlier, it is also possible to create fewer groups and force users through DirectEdit.

When users are assigned to a directory, they have the ability to create new pages and upload files to that directory, user level permitting. So forcing users through the DirectEdit link may be desired in order to prevent undesired pages from being created or files from being uploaded.

<table>
<thead>
<tr>
<th>Path to Page or Directory</th>
<th>Access</th>
<th>Approver</th>
<th>Publishers</th>
</tr>
</thead>
<tbody>
<tr>
<td>/index.pcf</td>
<td>ckatz</td>
<td>ckatz</td>
<td>None</td>
</tr>
<tr>
<td>/about</td>
<td>aharrison, ckatz</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>/about/index.pcf</td>
<td>aharrison, ckatz</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>/admissions</td>
<td>aharrison, ckatz, jzimmerman</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>/admissions/index.pcf</td>
<td>aharrison, ckatz, jzimmerman</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

After Setting Access

Run the reports again after the groups needed have been created and assigned. Be sure to select the checkboxes for Access, Publishers, and Approvers to make certain the output includes the appropriate data. This allows comparison and confirmation of proper group and individual assignment to the directories and pages so that the appropriate users can navigate to the pages they need to access and edit. This is also helpful in identifying areas to which users should not be allowed access.

In addition, either a Groups report or a Users report can be run in order to ensure that users are assigned to the proper groups, after confirming that directory and page assignment is as desired.
Page Access Settings

Overview

Page access settings are a subset of those available at the directory level, as there are more options for control at the directory level than at the page level. The access settings for a page can be navigated from the Pages list view or from preview/edit mode for a page:

- From Pages list view: **Edit > Access**
- From preview/edit mode: **Properties > Access**

Example of Access Settings from Properties

Assigning Access to a Page

Access settings at the page level override settings for a site, directory, or user. Those set on an editable region take precedence over those set at a page level. A page’s access settings can be edited regardless of whether it is checked in or out.

1. Navigate to the file in the **Pages** list view.
2. Hover over **Edit** on the file row and choose **Access**. Alternatively, from preview/edit mode, click **Properties** and select **Access**.
3. This displays a dialog where the access settings can be modified. Settings include:
   • Access Group
   • Approver
   • Enforce Approver
   • Bypass Approval
   • Toolbar
   • RSS Feed
   • URL Type
   • Exclude Search
   • Exclude from Sitemap

4. Click **Save**.

**Access From Preview/Edit Mode**

If the user is previewing or editing the page, the access settings can be modified from the page's Properties.

1. On the **Page Actions Toolbar**, click **Properties**.

2. Choose **Access** from the menu.

3. The **Access Settings** panel is shown. Make changes to the settings for the page.

4. Click **Save**.

For more information, visit the **Access Settings** page.
Directory Access Settings

Overview

Access settings at the directory level override settings for a site. A new directory, page, or file inherits its parent directory's access settings if directory access settings have not been explicitly set. An existing directory's access settings can be overridden with a site level recursive modification. Existing directories can have access settings that override settings from the site level with the use of templates. This is useful when controlling which groups can access pages in the directory, as well as who has permission to publish and approve specific content.

Example of Access Settings (Directory)

Assigning Access to a Directory

Access settings for a directory can be changed both non-recursively or recursively. Non-recursive modification changes only the directory and new content created within, while recursive modification affects all extant pages within the directory. The following instructions are for non-recursive modifications.

1. Navigate to the Pages list view for the directory.
2. Hover over the directory row, and from the Edit menu, choose Access.
3. For **Recursive Modification**, leave at the default, which is **Apply All Settings to This Folder Only**.
4. Change the setting as needed. The following access settings are available:
   - Access Group
   - Approver
   - Enforce Approver
   - Bypass Approval
   - Template Group
   - Extensions
   - Toolbar
   - RSS Feed
   - URL Type
   - Exclude Search
   - Exclude from Sitemap
5. Click **Save**.

Additionally, see the following topics for more complicated scenarios and additional functionality regarding access settings:

- **Recursive Modification**
- **Access Settings** (Includes information about each available setting.)
- **Directory Variables**
Site Access Settings

Overview

The access settings for a site in OU Campus provide control for much of the functionality found throughout the system, but can still be overridden by access settings that are closer to the content. Examples of the settings include defining which users can access the content, publish the content, and even override the approval process. Understanding the access settings and how settings closer to the content take precedence and inheritance can be very helpful in configuring a site in order to provide the appropriate access to content to specific groups of users.

Settings applied here can be applied recursively to existing items throughout the site and those created in the future, or non-recursively, which will apply the changes to the root folder only for items going forward. The access settings for a site are located through Setup > Sites > Edit > Site Access, and are available to Level 10 administrators only.

Assigning Access at the Site Level

1. Navigate to the

   Pages

   list view for the directory.

2. Hover over the directory row, and from the Edit menu, choose Access.

3. For Recursive Modification, leave at the default, which is Apply All Settings to This Folder Only.

4. Change the setting as needed. The following access settings are available:
   - Access Group
   - Approver
   - Enforce Approver
   - Bypass Approval
   - Template Group
   - Extensions
   - Toolbar
   - RSS Feed
   - URL Type
   - Exclude Search
   - Exclude from Sitemap

5. Click Save.
Example of the Access Settings for the Site

Additionally, see the following topics for more complicated scenarios and additional functionality, and information regarding access settings:

- **Recursive Modification**
- **Access Settings** *(Includes information about each available setting)*
• Directory Variables
Directory Variables

Overview

Directory variables are located at the site level and directory level, and can be an important asset to a site developer or administrator. Directory variables allow administrators the flexibility to define different variables, which may be applied to either the page in an <!--%echo var="[VARIABLE]" --> statement or to the XSLs. As an example, if different areas of the school (academics, athletics, etc.) have different theme colors, but the rest of the templates are the same, the theme color can be defined as a directory variable and changed as needed.

Directory variables can also be used to define a new image or media directory that users are placed in by default when browsing for an image or media file. This overrides the site setting for the image and media directory values. Directory variables are defined in name/value pairs. The syntax for the variable name is as follows:

- Image Directory: ox_ftp_image_root
- Media Directory: ox_ftp_media_root
- To skip files to publish: publish
- User-defined directory variables are created in key/value pairs with the user creating the text for both

The value to define an image or media directory is the path to the folder in which they will be placed, i.e. "/academics/images." The value to exclude files from being published is, for example, "skip: [EXTENSIONS,COMPOUND EXTENSIONS]," replacing EXTENSIONS and/or COMPOUND EXTENSIONS with any file extensions or specific files that should be excluded. Note that they are separated with a comma and should not include spaces.

These variables have context — applying a directory variable to the "/academics" folder sets the value for that directory and all of the directories subordinate to it. Therefore, "/academics/biology" has this value defined, but a sibling directory such as the "/athletics" directory does not. However, this value is not set permanently, and the value can be overridden further down in the directory structure by reusing the same name.

Since they are snippets of text, these directory variables can hold anything that a standard variable defined in a TCF can. Directory variables allow them to be stored in a contextual manner, where the value may change based on the current location. Some possibilities include:

- Path to a CSS file which may change a color scheme or background image based on the section of the site.
- Contact information for the maintainer of that portion of the website.

Both contextual configuration information and pre-populated variables are accessible in TMPL files when creating a new file, though it is not as likely that contextual configuration information will be echoed into a file.

Directory variables are defined per-directory from the access settings for a site or directory.
Examples of Directory Variables on Access Settings Modal

The Directory Variables section includes the following functionality:

- Viewing the inherited properties for folder
- Viewing the properties for the folder
- Adding properties (click Add)
- Deleting properties (click the Delete icon)

Creating New Directory Variables

Creating Image or Media Directory Variables

Two pre-populated variables that can be used during the new page creation process (along with TCFs) are Image and Media Directory Variables. When setting these variables on a descendent directory, and the parent makes use of an access group, a user can still access a child folder when inserting an image or media item when the ox directory variables are assigned.

1. Click New Directory Variable and define one of the following for the Property Name:
   - ox_ftp_image_root: Redefines the default image directory in the WYSIWYG Editor, the default value of which is found in the site setup.
   - ox_ftp_media_root: Redefines the default media directory in the WYSIWYG Editor, the default value of which is found in the site setup.

2. Define the Property Value as the path from the site root to the target image directory. For example:

```
/admissions/images  or  /athletics/baseball/images
```

Additionally, a relative path from current directory can be used, such as "./" or "./images." This places the user into the target directory relative to the current directory they are in. Please note that all directory variables are inherited as new subdirectories are created. These are in effect until new settings for those variables are created in the sub-folders.

When the ox_ftp_image_root or ox_ftp_media_root are set for a given directory, a user is placed into that set location when they use the Insert Image or Insert Media tools of the WYSIWYG editor. However, they are still able to navigate out of that location if they so choose.

Using a Directory Variable to Skip File Types on Publish

The publish directory variable can be used to skip the publish of files with a specific extension or with a compound extension. The system-level directory variable allows for skipping certain file extensions or compound extension names (including the extension) on publish. For example, publish can be used to ensure that XSL files do not get published except with the manual publish of the individual page. In this case, it skips files with the defined extension on publish. The syntax is as follows:

Directory Variable Name: publish
Directory Variable Value: skip:[EXTENSIONS,COMPOUND EXTENSION]

1. Click **New Directory Variable** and for the **Property Name** add: publish
2. Define the **Property Value** with the extensions to be skipped on publish. The list should be comma delimited and not contain spaces. For example: skip:xsl,xslt,xml,skp.pcf

In this example, any files ending in the extension of .xsl, .xslt, or .xml are not published. The compound extension of skp.pcf functions so that any files ending in .skp.pcf are skipped upon publish. This allows for specific files to be skipped. In this case, the specific file or files need to be renamed to include the compound extension.

**Creating a User-Defined Directory Variable**

1. From the **Content > Pages** view, click the **Access** icon for the directory. This shows the Assign Directory Access screen. For Directory Variables two sections are displayed: Non-editable inherited values, and an editable list of entries for the current directory.
2. Directory variables are entered in name/value pairs. Enter a variable name on the left (for example, what would be used in an echo var statement `<!-%echo var="NAME" -->` ), and a value on the right (what that `<!-- --->$ tag would be replaced with upon creation). Please refrain from naming variables with names that begin with “ox_” as these are reserved for future development purposes. To override a variable with a new value, reuse the variable name in the editable portion of the screen. The new value will replace the old when the variable’s contents are accessed.
3. Define a **Property Name** for the variable. This can be anything, but it must be referenced exactly in either the XSL or a TMPL.
4. Define the **Property Value** to replace the variable in the templates for the directory.
5. Click the **New Property** link to add another directory variable or **Save**.

After saving the access preferences, the directory variables are immediately accessible in the current directory and all directories below it, including contextual configuration information and pre-populated variables.

**Overriding Directory Variables for a Subdirectory**

For example, a directory variable of department is defined for the artdept directory as “artdept”.

After the directory variable was defined, a subdirectory called ceramics was created. Since the department directory variable is inherited with the creation of the subdirectory, it may be the case that the directory variable for the ceramics folder needs to be defined. When overriding inherited variables at the directory level, keep in mind that the Property Name must match exactly.

**Best Practices**

Define a variable's default value using the access button for the top of the site (found under the Setup tab), and redefine it to have intended values further down in the directory structure. This eliminates the possibility of having an empty string (“”) used during the variable substitution in TMPL files.
Editable Regions in a PCF

Overview

After page creation, the PCF can be edited with the Source Editor to modify access settings for an editable region of a page. The OmniUpdate div tag includes the access group assignment. Changing the value of the attribute changes access to the editable region. For example, this editable region is accessible by everyone:

```html
<!-- com.omniupdate.div label="twocolumn_content" group="Everyone" button="700" break="break" -->
<!-- ouc:editor csspath="/_resources/ou/editor/twocolumn_content.css" cssmenu="/_resources/ou/editor/styles.txt" width="1050" -->
<h2 class="h-color-link">Approval Workflow</h2>
<p>&nbsp;</p>
<p>Thanks!</p>
<!-- /com.omniupdate.div -->
```

If the value found in `group="Everyone"` was changed, the access to the editable region would change as well. So if, for example, one wanted to restrict access to that page to the “Admissions” group, then it would be changed to `group="Admissions"`. Each editable region will have its own section of source code that may be edited independently of the others.

To make permanent changes to the template, the value can be modified in the TMPL, and all new pages created with the modified TMPL have the new access setting instead of changing it page-by-page via the PCF.

For example, the code in the TMPL is similar to that of the PCF illustrated above:

```html
<content>
<!-- com.omniupdate.div label="twocolumn_content" group="Everyone" button="700" break="break" -->
<!-- com.omniupdate.editor csspath="/_resources/ou/editor/twocolumn_content.css" cssmenu="/_resources/ou/editor/styles.txt" width="1050" -->
<h2 class="h-color-link">Approval Workflow</h2>
</content>
```

To change the group access, edit the value in exactly the same manner as illustrated previously.