

Deploying Contribute to Departments or Enterprises

Contribute is a powerful desktop tool which enables users across an organization to connect to and edit web page content. This article provides a set of best practices for deploying Contribute to multiple users within an organization. The article is intended for website administrators and IT professionals. It covers required network and server permission settings, the role of Contribute permission groups, and provides tips for defining appropriate Contribute connection paths.

The article also provides suggestions for setting up Contribute to meet the needs of various website structures-from sites as simple as a root folder with multiple user-specific folders to multiple group folders with specific access groups.

This article also describes some strategies to employ when using cascading style sheets and Dreamweaver Templates in a site and for using Dreamweaver and Contribute collaboratively to edit web pages.

Table of Contents

| | |
|---|----|
| Administrator's Checklist for Deploying Contribute | 3 |
| Step 1: Set Up Network and Web Server Permissions | 4 |
| Disable browsing of Contribute generated folders | 6 |
| Step 2: Determine Site Administration Requirements | 7 |
| Shared settings | 8 |
| Permission groups | 8 |
| Define shared setting and permission requirements | 9 |
| Deploy Contribute for a flat website structure using file system controls | 10 |
| Deploy Contribute to a deep website structure | 11 |
| Deploy Contribute to sites consisting of multiple separate websites | 12 |
| Step 3: Create an Administrator Connection | 13 |
| Use Contribute with a local network | 14 |
| Use Contribute with FTP | 14 |
| Step 4: Define Permission Groups | 15 |
| Step 5: Distribute Contribute | 15 |
| Step 6: Send User a Connection Key | 16 |
| Connection Keys | 16 |
| Send connection keys | 16 |
| Step 7: Use CSS Style Sheets and Dreamweaver Templates | 17 |
| Cascading Style Sheets (CSS) | 17 |
| Dreamweaver Templates | 18 |
| Step 8: Configure Dreamweaver Users | 19 |

Administrator's Checklist for Deploying Contribute

Use the checklist below to guide you through the key tasks of setting up Contribute users to edit a website. The checklist also includes tips for using Dreamweaver and Contribute together on websites.

1. **Set up network and web server permissions** to allow read/write/and modify access as needed so that users can update the website files.
2. **Determine Contribute site administration requirements** appropriate for your website.
3. **Create a connection** to the website using the Contribute Connection Wizard.
4. **Define Contribute permission groups** as needed based on the controls you want to place on a user's ability to edit pages on the site.
5. **Distribute Contribute** to your users.
6. **Send connection keys** to your users so they can access their website files and folders.
7. **Create CSS and Dreamweaver Templates** so Contribute users can more effectively use the product and you can maintain control of the site's layout and style elements.
8. **Configure Dreamweaver users** so they work safely with Contribute sites.

Step 1: Set Up Network and Web Server Permissions

Contribute users in your organization will access the web pages they'll edit either through a local area network connection, or by using File Transfer Protocol (FTP). To ensure their connections work and that they're able to edit the pages, check to make sure they have the correct permissions to connect to and modify pages in the appropriate folders.

Network and file server permissions determine whether users can access another computer over the network, read or open files or folders, and delete or modify files. As a website administrator, you should check that network and file server permissions are set correctly so that users can read, write, and modify pages they'll need to update.

For example, if the files the user will update are on a server named *HRAdmin*, in a folder named *HRSite*, you must make sure they are able to access *HRAdmin* and have with read, write, and modify permissions to the *HRSite* folder.

Additionally, Contribute users must have proper permissions to update files on their local machines. When a Contribute user publishes a page to the web server, a copy of the page is stored locally on their computer. If they don't have the ability to update files locally, they will not be able to edit pages.

Set folder permissions

In Windows, to set user permissions for a network folder, you use the Properties dialog box. Right-click the folder you want to set properties for, then select Properties. In the Security tab, set the permissions to allow or deny access to folders as appropriate.

Note: You can set folder permissions to allow a user or group of users to modify a folder and later define more restrictive folder or file editing options when you set Contribute permission group options

If the Contribute users will use File Transfer Protocol (FTP) to access the web server, make sure that the website folder has delete, overwrite, and rename privileges enabled. When using anonymous FTP, these file protection options are typically disabled by default. This prevents users from connecting to the website, publishing updates to pages, and adding new pages to the website.

To test that FTP is set up correctly for an end user, you can FTP a test web page to the server, then using the login you will provide to the user, attempt to view the page in a browser.

Whenever you provide access to a web server, proper security measures should be taken to ensure that both the operating system of the server hosting the site, the web server software itself, and if using FTP, the FTP server are secure. Refer to the documentation provided with your server's operating system, FTP, and web server software for the best practices related to securing your website from both accidental and malicious tampering.

Storage considerations

If the server hosting your organization's website has disk quotas enabled, carefully consider if the quotas are too restrictive for the users responsible for updating the website, or if those users shouldn't be restricted by quotas. This is especially important if users will be adding new pages, Microsoft Word documents, or large, rich media files to the website.

Disable browsing of Contribute generated folders

When you create a site connection, Contribute creates special files that are stored in folders whose names begin with an underscore (such as `_mm`, `_baks`, and `_notes`). The underscore naming convention is used for these folders to allow Dreamweaver and Contribute to distinguish between them and the other folders in your site.

Contribute and Dreamweaver use this naming convention to filter these special files and prevent them from displaying in the Dreamweaver Site window and in the Contribute Remote File Browser. This serves to hide them from being browsed, overwritten, or inadvertently altered by users. Additionally, most search engines and bots are designed not to return pages found in underscore folders.

Apache web servers

If your website uses Apache, you can explicitly disable the browsing of folders and files that begin with an underscore. If you know how to modify the Apache web server's `httpd.conf` file and have permission to do so, you can use the `DirectoryMatch` directive to prevent visitors from viewing any file in a folder beginning with an underscore.

If you're not sure how to edit the Apache `httpd.conf` file, or you don't have permission to do so, ask your system administrator or ISP to do it for you. To learn more about limiting access to files and folders, and other security issues relevant to the Apache web server, see the documentation supplied with your Apache distribution.

Microsoft IIS web servers

Microsoft IIS does not provide the same high level filtering of specific folders in the same way as Apache. To achieve some level of filtering, you can use the file system's hidden flag to hide individual folders from general access. This will cause IIS to return a 404 File Not Found page for a URL pointing to the specific underscore folder. If you want to filter the folders, you will have to set the hidden flag individually for each folder you wish to hide. If directory listings are not enabled for the folder, this setting isn't necessary, since without directory listings users automatically get a 403 forbidden error when browsing to a folder path web address.

Note: It is very important that this hidden flag is only set on folders and not the files inside them. By hiding files contained in an underscore folder you may cause Contribute and Dreamweaver to cease functioning correctly.

Shared settings

Contribute creates a special folder (`_mm`) and a shared settings file (`contribute.xml`) in each website to which you create a connection. The shared settings file contains information about each permission group you define, including the administrator permission group. If you are creating multiple site connections for different sets of users, make sure the connection paths you define do not overlap. As the administrator, you should create your connection at the highest level of pertinent access to the website; you can define user permission groups to define user access at lower levels of the site depending on their specific access requirements.

The shared settings can only be altered by entering the site administrator's password. You should store the shared settings on the website's server so you can easily update the user permissions when necessary. By controlling the site from the server, you will not need to resend a connection key. The changes will automatically apply when the user connects to the site.

Permission groups

You can set sitewide settings which apply to all users in a site as well as permission group settings which apply to user groups you define. A permission group is a set of permissions that define what files and folders a user can edit, as well as the types of edits they are permitted to make. For example, you can allow or deny users the ability to create or delete pages, set whether they use font tags or inline style when writing code, and define which pages or template(s) upon which they will base new pages.

An administrator can define any number of Contribute permission groups, and define different options for different groups. Contribute permissions are not assigned on a per user basis and no record is kept to track which users are using a particular permission group.

Based on your users' needs you should create user group names which make it easier for you to manage the permissions assigned to a particular group. For example, if one group will have access to the Sales site and have full editing permissions, and another group will have text-only editing permissions, you might name the first group Sales-Full, and the second Sales-Text, and so on.

Define shared setting and permission requirements

Now that you know how shared settings work and how an administrator can set up specific permission groups to limit user access, we will discuss the different scenarios for setting up Contribute for large or multi-team organizations.

This section describes three primary configurations for Contribute administrators to consider as they determine how to set up Contribute sites.

Keep in mind, the main drivers in successfully setting up multiple users are: (1) defining where the shared settings file is stored and (2) preventing connection paths from overlapping. Depending on how your website is structured, you will need to use different strategies for setting up access for various groups of users.

Use information in this section to help you determine where to create the shared settings file for the following common website structures:

Flat website centrally administered Typically, this is a website where users have read access to the root of the site and read/write access to specific folders in the site as controlled by the file server or network permissions. There is a single root folder and all users are part of the same Contribute permission group. See [Deploy Contribute for a flat website structure using file system controls](#) in the section below.

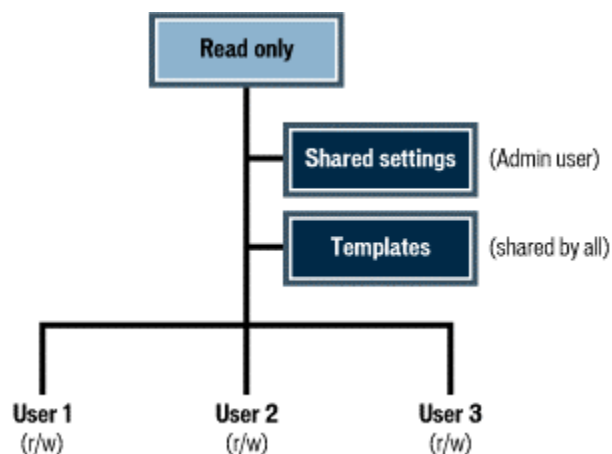
Deep website centrally administered In this structure there is a single root folder. The root folder contains folders for each section or organizational function within the website. Contribute permission groups are used to control user access to particular folders on the site, and to assign a sub-set of the common templates used in the site. While not required, file server permissions are usually used in addition to Contribute permission groups to restrict user access to appropriate sections of a site. See [Deploy Contribute to a deep website structure](#) in the section below.

Deep website with distributed administration In this type of site, separate groups take responsibility for their own sections of a sectionalized site. Access may be further divided so that users within a particular group have permission to edit only specific folders within their section of the site. With this type of structure, there may be multiple administrators for the site. This is effectively like setting up each department or group with a separate Contribute-enabled website. See [Deploy Contribute to sites consisting of multiple separate websites](#) in the section below.

Deploy Contribute for a flat website structure using file system controls

This set-up is useful for creating faculty or employee homepages, a series of collaborative team websites, small business websites, and departmental websites that have independent web servers and/or web administrators. The key aspect of this arrangement is that all users have the same set of Contribute permissions. In other words, there is a single permission group within the shared settings file that controls the behavior of Contribute when editing the website. There is also a single set of Dreamweaver templates (if the site uses Dreamweaver templates) shared by all users. For such sites, the administrator defines and restricts different users to different parts of the site using file system permissions.

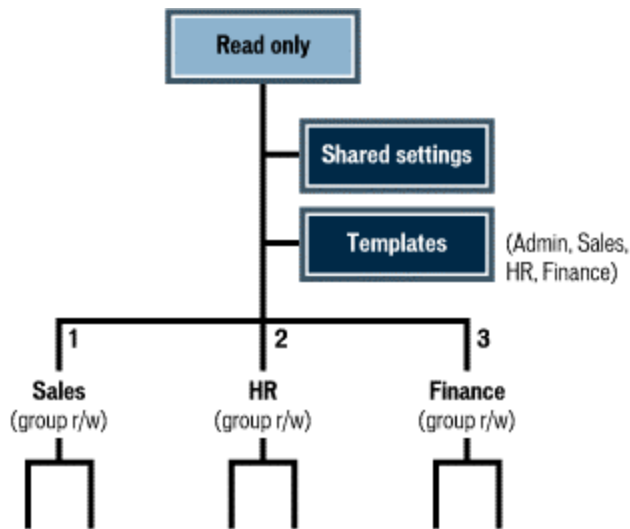
In addition to the shared settings and templates, you can also store CSS style sheets (CSS), Server Side Includes (SSIs), images, and other sitewide, "Read-only" assets used in the site off of the site root.



In this scenario, the administrator uses the Connection Wizard to create a site connection to the root folder, for example, /myIntranet. In the Administer Website dialog box (Edit > Administer Website), the administrator defines a Permission group which provides all users with access to the folders in /myIntranet. Any user connecting to the site with this connection key has access to all the folders in this directory.

Deploy Contribute to a deep website structure

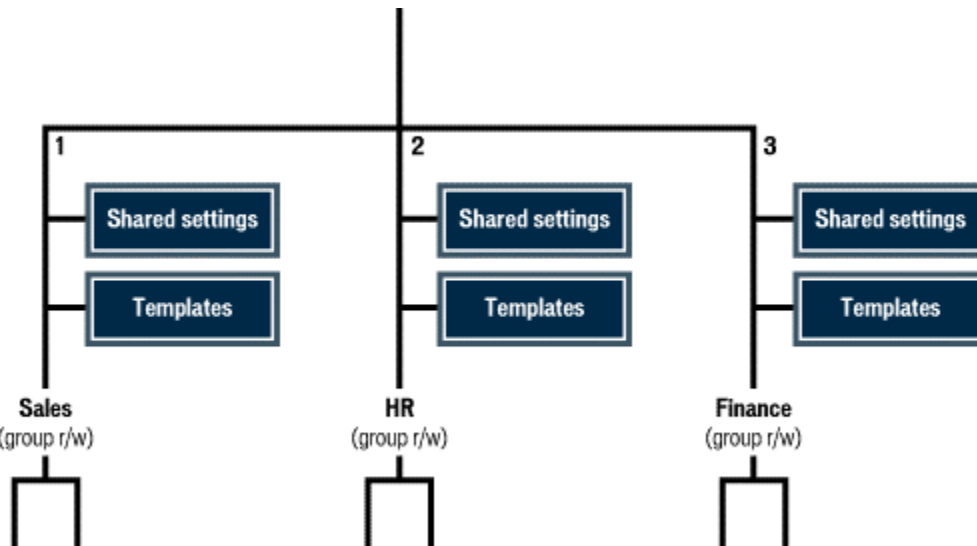
The following set up works best with larger, centrally controlled websites, such as a corporate intranet, public government website, or university website. In this set up there is, typically, a single administrator who uses site and possibly department templates to control the site, but the separate site sections are maintained by different contributors. The site administrator sets up a single shared settings file for the entire site, and then defines a permission group for each section of the site. Each Contribute permission group is restricted to the appropriate section of a site and is given access to the subset of templates used in their section of the site. At the file server level, individual users are given read access to all sections of the site, and read, write, and modify access to the section of the site they are allowed to edit.



In this scenario, the administrator creates a site connection to the root folder, for example, /myIntranet. In the Administer Website dialog box (Edit > Administer Website), the administrator creates three Permission groups for users, and sets user access to a specific folder: For example, for a Sales site Contribute user, the administrator selects the Folder/File Access option, then only allows members of this user group to edit content in the folder at /myIntranet/Sales.

Deploy Contribute to sites consisting of multiple separate websites

In the scenario below, there are multiple administrators for the site, one for each section. Each administrator can set up their site for Contribute users. The specific templates for each section of the site are kept in template subfolders for each section. As in the previous example, the other users can browse the full site, but will be restricted to editing only their folder. This provides a different level of flexibility while keeping Contribute files out of the root of the site. This set-up also allows each group to act more independently.



In this scenario, three administrator connections are created. The administrator for each site creates a connection to their departments section of the website, for example, /myIntranet/Finance. Additional Permission groups can be created to define any restrictions for users in the site, for example, to specific subfolders in the Finance folder or to set editing options.

Step 3: Create an Administrator Connection

Because Contribute does not allow you to create overlapped connection paths, before you create website connections carefully consider the folder structure of your website, and create a connection to the highest required access level in the site's structure. If you need to limit users to folders below this level, use Contribute Permissions settings to specify specific folder access and editing options. For information about setting up Permission groups, see [Step 4: Define Permission Groups](#).

You use the Contribute Connection Wizard to set up a website connection. To become a site administrator when you are setting up a site connection, choose the "Yes, make me the administrator" option in the Connection Wizard. If you are becoming the administrator of an already established site connection, choose Edit > Administer Website, then select "Yes" when prompted.

About matching network paths and web address (URLs)

When creating a connection to the website, Contribute prompts you to provide the web address (URL) of the website, and the network or FTP information of the server and folder storing the website. Both the web address and network path must point to the same folder within the website.

For example, if your website is located at the directory path \\MyServer\wwwroot\sites\MySite, and the corresponding web address for this site is http://www.myserver.com/sites/MySite, then you must correctly enter these values in the Contribute Connection Wizard when creating the connection.

To ensure the website and network folder (or in the case of FTP, the FTP folder) are the same, Contribute uploads a temporary file using the path information you provide. Contribute then attempts to read the temporary file via HTTP using the web address you provided. If Contribute succeeds in locating the temporary file, the paths match, and Contribute creates the connection. If the paths don't match, Contribute prompts you again for the correct path.

If your users will use FTP to connect to a website folder beneath the FTP Host folder, you must provide an absolute folder path to the folder.

Use Contribute with a local network

When using Contribute to connect to a web server using a local network connection, the web server must be visible to the local network. Contribute can also be used with VPN servers to ensure all file transmissions occur behind your firewall. If the web server is not visible to the local network, you can create an FTP connection with Contribute to work with the website.

To ensure that you are entering the correct network path, use the Connection Wizard's Browse button to locate and select the network folder. If the path to the folder is correct, but Contribute is still unable to create a connection, verify that the folder has proper read/write permissions.

To learn how to check your server's network and folder permissions, refer to the documentation supplied with your server operating system.

Use Contribute with FTP

As you create an FTP connection with Contribute, Contribute attempts to auto-detect the FTP path, checking that the FTP folder is the same folder that contains your website's files. If the folder paths don't match, Contribute isn't able to write to the page displayed by your browser and prompts you to enter the correct path.

To ensure that you are entering the correct FTP path, use the Connection Wizard's Browse button to locate and select the FTP folder. If the path to the folder is correct, but Contribute is still unable to create a connection, verify that the folder has proper read/write permissions for the user. If you are creating an anonymous FTP account, the server must be configured to support delete, rename, and overwrite privileges for the anonymous user. In some cases, file permissions on Unix servers may be configured in a way that prevents Contribute from operating, especially if the server doubles as a file server. For more information on this topic see ["Setting up a site connection in Contribute"](#) on the Macromedia Contribute Support Center.

Step 4: Define Permission Groups

Once you have determined your site administration requirements, setting up Contribute permission groups is a very straightforward process. You use the Administer Website dialog box (Edit > Administer Website) to create permission groups and define sitewide settings as needed.

Note: It is best to limit your sites to no more than 25 permission groups. In some cases you may encounter performance problems if you create more than 50 permission groups.

For additional information about Permission group settings, see Macromedia Technote ID 16611, [“Options for Contribute website administrators”](#).

Step 5: Distribute Contribute

Contribute is a desktop program. Each Contribute user must install and use it on their local machine. Most administrators who will install Contribute to multiple users already have a system in place for deploying desktop programs in their organizations. Remember that restricted users may not be able to install programs and some folders and files may be off limits, and thus may need to have Contribute installed on their machine by a desktop administrator.

You can post Contribute on an intranet site or local network for download. You can also distribute Contribute on a CD. In all cases, you must accept and comply with the terms and conditions of the volume licensing agreement. For additional information about the agreement, see [Macromedia's volume licensing agreement](#).

Step 6: Send User a Connection Key

To set up a Contribute user, you need to provide them with the basic site connection information for the web server. This is done by sending them a connection key.

Connection Keys

A connection key is a file generated by Contribute that contains all the information that Contribute requires to connect to a site. The information in the connection key is encrypted with a 128-bit algorithm for security purposes, and end users cannot read or change the connection or permission group information contained in the connection key. Administrators create these password protected connection keys using the Send Connection Key feature of the Administer Website dialog box. The keys can be sent to end users via email, or saved to the network.

Connection keys do not automatically expire. To invalidate a connection key, an administrator must delete the permission group from the shared settings files. This can be done in Contribute through the Administer Websites dialog box (Edit > Administer Websites). If a user uses a connection key that points to a deleted group, the message box updates alerting him or her to contact the site administrator.

Send connection keys

The easiest way to get end users connected is to send them a connection key via email. You can use the Send Connection Key option in the Administer Website dialog box to automatically generate an email with a connection key attachment and simple instructions for getting started. You must then notify the end user of the connection key password so they can access the site. Typically, you would send the password information in a separate e-mail or contact the users by phone with the information.

When a Contribute user receives a connection key, they simply double-click it to start the connection process. The file is encrypted, so the user must know the password that the administrator defined for the key. Connection keys also specify what permission group settings to apply. When the correct password is supplied, Contribute automatically makes a connection to the site and allows page edits as defined for the associated permission group.

Step 7: Use CSS Style Sheets and Dreamweaver Templates

Both cascading style sheets and Dreamweaver templates provide you with ways to control consistency in the look and feel, and the layout of pages in your sites.

Style sheets help you ensure consistent text formatting and provide a way for you to define additional styles Contribute users can apply in the pages they edit. Dreamweaver templates let you define the areas of a page a Contribute user can edit.

By using templates, you can lock regions of a page you do not want a user to edit. You can use the full range of Dreamweaver templates options in a Contribute site. For example, you can create templates that include optional regions, repeating regions, template properties, and so on. You can also use nested templates to design department or site specific page layouts which are based on other templates. For additional strategies for preparing sites for Contribute users, see [Optimizing Web Development for Contribute Users: A Strategy Guide for Site Administrators](#).

Cascading Style Sheets (CSS)

You cannot use Contribute to attach a CSS style sheet to a page. You can use Dreamweaver to define CSS styles for an individual document or to create a style sheet you can attach to multiple documents. Contribute does, however, recognize CSS styles which are attached to a page, and allow the user to use these styles. Contribute users can use the Style popup menu to apply styles which have been defined in the page or in an attached style sheet.

Tip: You can make it easier for Contribute users to work with CSS styles:

Name the styles so they make sense to Contribute users. For example, you can provide a more descriptive name like MainHeading, Title, or Headline instead of Heading, depending on how your user is likely to use the style.

Each style you define in the attached style sheet will appear in the Styles pop-up menu. If you want to hide certain styles from appearing in the menu, add “_mmhide” before the style name. For example, _mmhideNavTable.

For more information about using CSS, see these resources on the Macromedia website:

- [Using Cascading Style Sheets in Contribute](#)
- [Best Practices with CSS in Dreamweaver MX](#)

Dreamweaver Templates

Dreamweaver templates are powerful design tools, which help you control how and where a site contributor can add or edit content. By using Dreamweaver templates, you can help Contribute users reuse design and layout elements and maintain consistency across multiple site pages. Contribute lets you take advantage of the many template options available in Dreamweaver MX, such as editable regions, repeating regions or tables, template properties, and optional regions. Although Contribute works with templates built in Dreamweaver 4, it works best with templates built in Dreamweaver MX.

Templates let you easily manage updates to a website. When you update a Dreamweaver template, you can automatically apply the updates to all pages based on that template.

Contribute users can create new pages based on the templates you define for a site in the Administer Website dialog box. You can also use options in this dialog box to hide any site templates you don't want users to see.

Templates can be very restrictive or allow for great flexibility depending on how you design them. Keep in mind the needs of the Contribute user when you design templates. In most cases, more flexibility (few locked regions) will allow them greater success.

Other template options you can use to provide structure are optional and repeating regions. Using these template options can help you provide structure in areas where you want to control the design. For example, you can set up a repeating region or repeating table to make it easy for a user to create additional table rows with worrying about the design being altered.

Step 8: Configure Dreamweaver Users

When using Dreamweaver and Contribute together, the site administrator needs to make sure Dreamweaver Design Notes are enabled and are uploaded to the web server.

Dreamweaver MX users should update to the Dreamweaver MX 6.1 Updater to take advantage of the new site options available for integrating with Contribute. This also ensures that features like Check In/Check Out and Rollback work seamlessly between Dreamweaver and Contribute users.

Users of older versions of Dreamweaver should ensure that Check In/Check Out are enabled, and that Design Notes are always uploaded to the web server. These options are part of the site settings. All Dreamweaver users should ensure that any existing pages they are editing have been properly checked out to prevent inadvertent overwriting of pages. They should ensure that their sites are connected to the same site root folder as the Contribute users.

Summary

Understanding how Contribute interacts with the server is important for a smooth implementation of the program within a large organization. Understanding the server/permissions requirements will ensure not only that Contribute is working smoothly, but will reassure webmasters that the site is secure and stable and will allow them to keep an eye on the big picture. Allowing Contribute users to update their own content will enable everyone to work more efficiently. A good understanding of the Contribute workflow will ensure that updates, synchronizing, and site wide changes can be implemented smoothly. Properly implemented, Contribute will allow users to easily update their content and reduce the hassle for webmasters.