

DMX: GETTING STARTED

IMPORTANT: DMX CONTENT ARCHITECTURE

At this point it's important you get familiar with the way DMX organizes its contents. In this part I'd like to discuss the consequences of the way DMX "works".

PORTAL-WIDE CONTENT

DMX modules act as 'windows' to an underlying 'Portal-Wide' tree of items. In other words: the data you enter in DMX is **shared across the portal**. And: there is only **one folder-document-tree per portal**. This means if you instantiate multiple DMX modules in your portal **they all display the same content** for a given user. This would not be very useful if it wasn't for the fact that we can set the 'root' folder to point to any folder of the underlying tree for every one of those DMX instances. This makes **DMX instances mimic 'virtual drives'** in a windows network. Now we can add DMX instances for particular purposes in our portal while preserving the ability to share content across the portal. You can find these settings under the module's settings. Below is an illustration of this design.

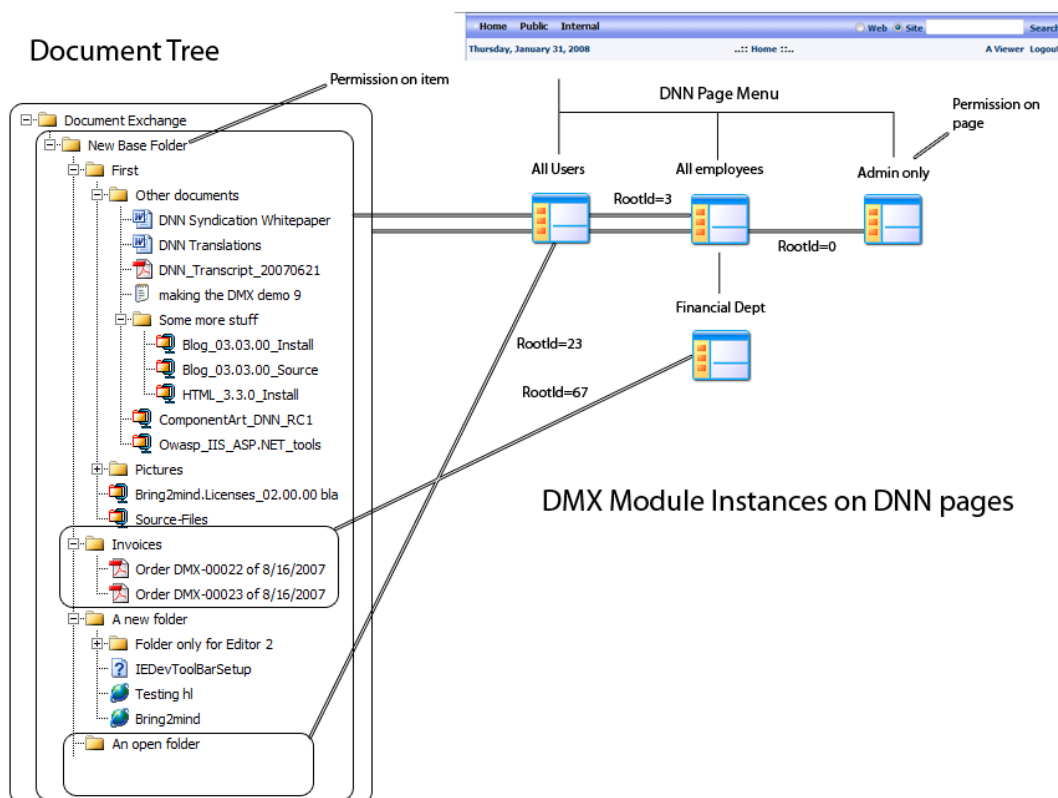


Figure 1. Overall DMX Content Architecture

You can see the DMX instance on the page that is visible to 'All Users' points to 'An open folder' and the

instance for the 'Financial Dept' starts at 'Invoices'. Note that there is an instance for Administrators that points to the very top of the tree.

Note that although DMX will show you the document tree starting at the node specified, it does not mean you cannot access other material through that DMX instance. DMX also shows 'categories' for example and documents available to the user will show up regardless of whether they are in the subtree of that DMX instance. In everyday use the permissions in DMX will follow the lines of the folders so this will not be too confusing (so content visible to 'All Users' will only be stored underneath 'An open folder' or below and content only for 'Financial Dept' will be kept under 'Invoices'). See more about this in the paragraph on 'permissions' below.

PERMISSIONS ARE SET IN THE CONTENT NOT IN MODULE SETTINGS

Each DMX module's permissions have no impact on the permissions on the content. The only permission that has any influence is "VIEW" here because it governs who can see the module. But it does not influence the VIEW permission on the root folder of that module for instance. The two are entirely separate.

This is a consequence of having "per item" permissions and sharing the content throughout the portal. It was necessary to separate the module's permission mechanism from the internal permission mechanism.

THE DOCUMENTS ARE STORED IN A "VAT"

This vat is called the repository. DMX separates the display and management of documents from the storage through what is known as a "storage provider". This enables us to offer you a choice of location to store documents. The most basic (and default) is storing them on the server's hard disk. Alternatives are in SQL or on Amazon S3.

A consequence of this is that DMX does not expose the stored documents in a way that allows you to access them with other software "behind the scenes". I.e. even if you chose to store documents on the server's hard disk, they're not stored in a way that reflects the DMX folder structure. The files are renamed in a way that will make them unrecognizable to anyone looking at the hard disk and will block IIS from serving them directly over the web. Instead, DMX is the only program that knows what the contents are and how to transmit this.

FLEXIBLE UI

Because DMX can be used multiple times to access the same data we envisioned you'd use it in various places in the portal for different audiences. So with DMX 5 we introduced the "flexible UI" meaning that we offer multiple ways of rendering DMX. That way you can use a simplified rendering for visitors that just need to browse and download and a more powerful UI for those that need to manage content. Out of the box DMX 6 comes with 3 UIs: a (default) 2 panel view using Ajax which shows a folder tree on the left and the folder's content on the right (this view resembles the Windows Explorer as much as it can), a 3-panel view similar to the previous but with a details panel showing the details of a selected item, and finally a so-called "template view". The template view takes HTML templates and pumps out DMX content using that. This creates almost limitless possibilities in rendering content on screen.

THE ABSOLUTE ROOT

There is such a thing as the absolute root collection which is the root of the underlying document tree. It has

an EntryId (the unique identifier of content in DMX) of 0. It is a special case as, contrary to all other items in the document tree, this one has no record in the database. In DMX's interface you'll see this folder show up as "Document Exchange". It is just a placeholder to let DMX know: start here. As a consequence it does not have the same metadata as other items like permissions. Instead this folder has fixed permissions where All Users can view it and only Administrators/Document Managers can add contents to it.

PERMISSIONS: WHO CAN SEE WHAT?

This brings us to permissions. It is important to keep in mind that every item in DMX has its own permission set. This means that regardless of which DMX instance you're watching, you'll still only see what you're allowed to see. The various DMX instances are just to help you organize content, they don't influence permissions. Well, almost. The VIEW permissions on a module are laid over the DMX permissions if you like. If you have the permission to see DMX content but you don't have permission to see the DMX module, you still won't be able to access the content because you actually can't see the module.

This needs a little more thorough examination. You can have access to item X in the document exchange but you need to see the module somewhere in order for you to access this. Let's take the illustration above and imagine there was no 'All Users' instance. Now let's assume you are a regular employee (i.e. not 'Financial Dept'). If Joe at Finance was to send you a link to 'Order DMX-00022 of 8/16/2007' you would never be able to see or download it because the permissions on this document are such that DMX will prevent you at all times to access it. If he sent you a link to 'Source-Files' however, you are permitted by DMX to see it. But the link includes the url to the page where Joe was viewing this, e.g.

<http://ourhost/Internal/Financial/Tabid/234/Default.aspx?EntryId=56>

This url would take you to the page in DNN with TabID 234 which is not viewable to you. Ah, now DNN will override the permissions and deny you to see this document. Instead you'd need to go to your own page and find it there.

For this reason DMX has a concept called the "default DMX instance" that is visible to the largest group (i.e. 'All Users' or 'Registered Users' if you have no public content). It's good practice to have one of these in your portal. On the 'main options' admin screen you select this module and every link that is produced in DMX will point to that instance. That way you are assured you can send someone a link to content that he/she will always be able to click and see.

HOST PERMISSIONS: A NOTE OF CAUTION

DMX does its best to avoid unauthorized access. Many aspects of its functioning are bound to users and roles. There is an anomaly in DNN that is not widely known: the host does not belong to any portal role by default. This means the host is not known as an 'Administrator'. Instead, DNN relies upon developers to make workarounds for this. Unfortunately in the case of DMX this would lead to a good deal of extra code that introduces new vulnerabilities. Because this is risky, a host/superuser **impersonates** the portal's Administrator (the Portal's administrator is set on the Site Settings page). Note: if you are having trouble adding stuff to the absolute root of your installation, verify that the Admin account you're using actually belongs to the 'Administrators' role that you set in the portal settings as being the administrator's role. There have been support calls where this was not the case.

SETTINGS

You can configure many aspects of the module. As any other module in DotNetNuke you access the configuration through the module's menu. In DNN 5 that is the little triangle to the left of a module's title, in DNN 6 it is underneath the Manage floating button over the module:

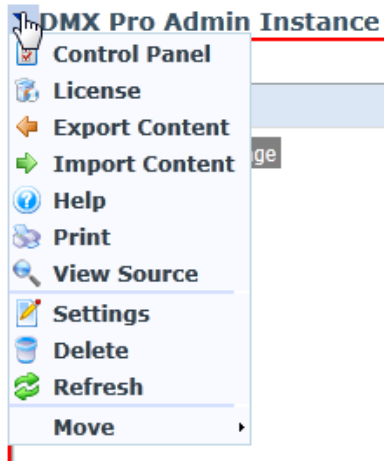


Figure 2. DotNetNuke 5 Module Menu

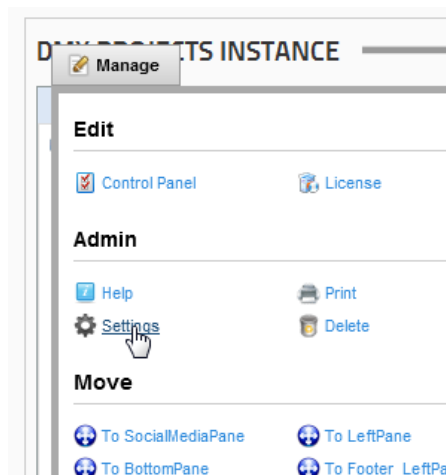


Figure 3. DotNetNuke 6 Module Menu

You'll see both give access to **"Control Panel"** and to **"Settings"**. The Control panel takes you to settings that span all instances of the module in the portal. This is where, for instance, you set up where the module stores its documents. The **"Settings"** (also referred to as the **"Module's Settings"**) are settings specific to the module. These include which UI to render for the module for instance. Please keep this distinction in mind when reading through other documentation. The **"global"** settings are handled through the control panel and the **"local"** settings through the Module Settings.

CACHING

A word about caching. Caching is the mechanism by which data is temporarily stored on the server and retrieved on subsequent web requests to speed up the performance of the site. DMX leverages DotNetNuke's inbuilt system of caching. Caching makes sense when the data you are storing is **"difficult"** to compile (i.e.

takes up valuable processing time on the server). In DMX there are many places where caching is useful. One such area is the user and his/her abilities in the system (Doc Admin, etc). Another is various system settings in DMX. These items are cached on the server to keep DMX running snappy. But keep in mind that DMX is unaware of what you do in the rest of the application. So if for example you change a user's authority in DNN, this is not pushed through to DMX. What you need to be aware of is that if the system somehow behaves unexpectedly you need to be aware that caching may be the issue. You can flush the cache by logging in as host and on the host settings page go to "performance" and clicking the "empty cache" link.

BEST PRACTICE SETTING UP DMX

If you've read the above and it has sunk in the following should seem logical. But just for completeness what follows is what we consider 'best practice' in using DMX.

1. Create a page visible for the administrators only and add DMX to it. Leave the root collection of this instance untouched. This instance is meant to manage the whole document tree.
2. Make a plan for the various instances since you can set up DMX instances as windows to the underlying document tree. For example, if you have a software company like me, you want a 'downloads' section, and maybe an instance on a page for customers only.
3. For each application add collections to the absolute root in your installation. Make sure you set permissions correctly on these first collections. In my example I'll give the 'downloads' collection the permission of View for registered users for instance, and edit and add by administrators and employees.
4. Add the DMX instances on the pages where you need them. Make sure the right roles have View access to the page or else they won't see anything.
5. Set the root collection in the DMX instance to the relevant collection under the module's settings.

This should give you a document management system with a maximum of control and flexibility. Note that in a particular DMX instance you cannot edit the root collection, whether it is the absolute root or not. Permissions are by default inherited from parent to child so when someone adds a file the permissions are inherited from the folder in which it is placed. If there is a role selected for approval then the items will first need to be approved before it is visible to others.

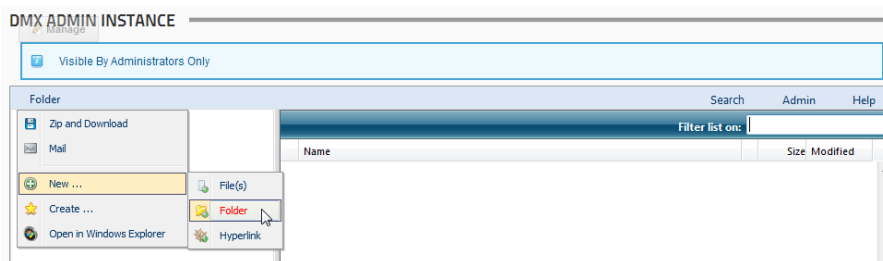


Figure 4. Add a new item to the root

DMX ADMIN INSTANCE

Visible By Administrators Only

Editing: New Item (Unknown Type)
Folder: Document Exchange

COREMETADATA

Type: Folder
 Description: Finance Documents
 Author: Peter Donker (Host)
 Keywords:

Remarks:

Thumbnail: Use Thumbnail

CUSTOMATTRIBUTES

PERMISSIONS

	View	Edit	Add	Approve
Administrators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
All Users	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Customers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
External Consultants	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Registered Users	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sales and marketing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Secretariat	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Subscribers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 5. Give it a meaningful name

PERMISSIONS

	View	Edit	Add	Approve
Administrators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
All Users	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Customers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
External Consultants	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Registered Users	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sales and marketing	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Secretariat	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Subscribers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Support	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Unauthenticated Users	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Username:

Permissions Only By Admin

Figure 6. Important: set permissions correctly

Now you can add a copy of DMX to the page for this group of users and set the root folder in the module settings (see above how to reach the module settings):

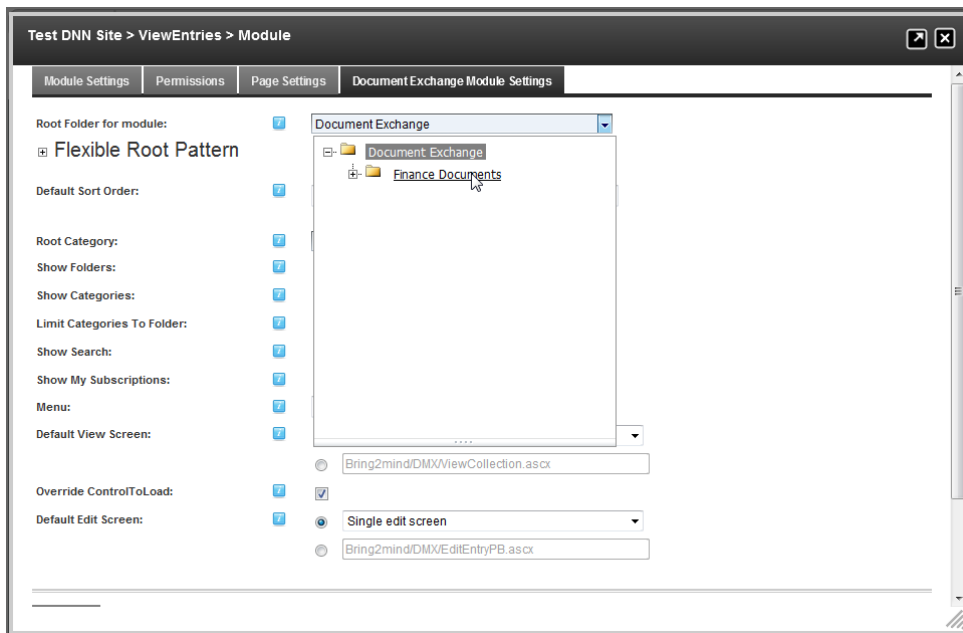


Figure 7. Selecting the root folder for a module

HELP FOR CONTINUING YOUR SETUP

You can now continue to set up categories and any subfolders that you may need. Refer to other documentation for explanation about other aspects of DMX. We've broken down the manual in constituent parts and made it available in the default UI under the help menu:

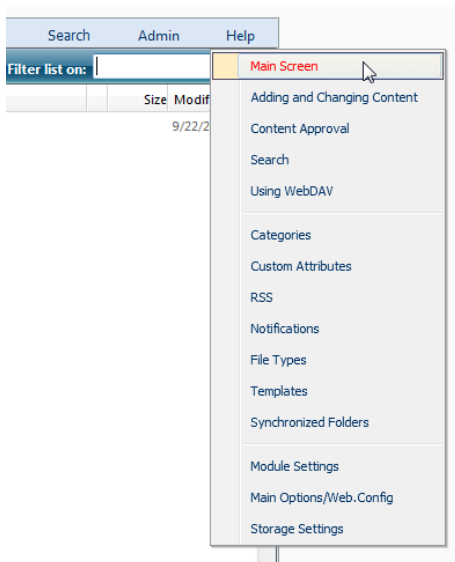


Figure 8. DMX Help menu

This helps us keep the manual more manageable as well. If you still have questions don't hesitate to contact us. There is a forum on the Bring2mind site with ample content on this product:

<http://www.bring2mind.net/Support/Forums/tabid/143/Default.aspx>

Alternatively you can contact us at support@bring2mind.net