Introductions

Permissions in evergreen control whether a staff account can log into the staff client and what functions that staff account can perform once logged into the client. There are 500+ permissions in Evergreen so this can be a topic of confusion when you first get started. Today's presentation is designed to break down the process of creating staff accounts and ensuring that staff are given the permission they need at the level they need it to do their day to day work.

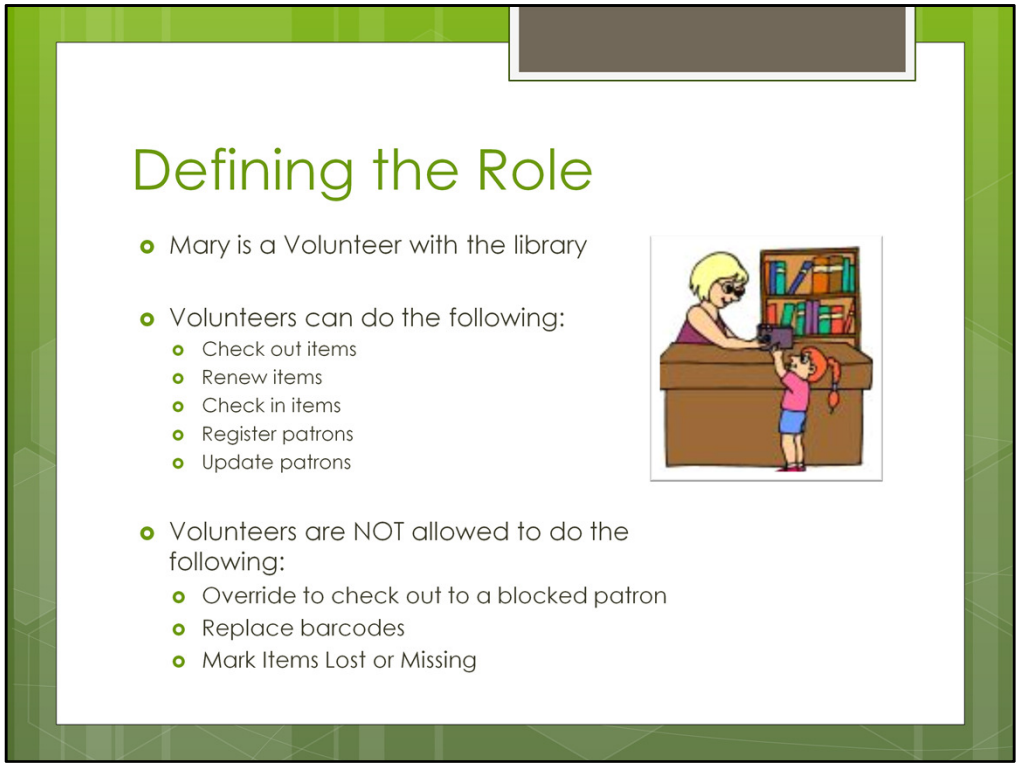
Questions to Answer

How can I ensure that staff have access to do their day to day functions?

How can I ensure they have permission to do things at the appropriate level?

The goal today is to walk away with answers to these two questions and to not feel like Charlie here ☺ So, let's get started!

The best place to start is outside of Evergreen and in your library. Look around. Who are your staff members and what do they do on a daily basis? If you have a small staff, you may only need a few logins and they may be tailored specifically for that staff member. In larger institutions, you may look at this in terms of the groups within your library such as public services staff versus technical services staff. No matter what your situation or institution, you need to document what each staff member (or group of staff members) need to be able to do in the client, what they shouldn't be doing in the client and at what level they should do things (such as only creating copies at their local branch). Once you have the roles defined, then you can go into Evergreen to start the process of entering the appropriate policies and staff accounts.



Here's an example of defining the role. This is Mary. She's a volunteer who works with the public checking out materials and doing a little bit of reference. She needs to be able to check out items, renew items, check items in, register patrons and update patrons. In addition, she should have the default permissions of logging into the staff client and searching the catalog. She SHOULD NOT be dealing with overrides that occur when she's checking items out or in. These are situational permissions. Perhaps only a circulation staff member or manager should be able to handle overrides. Mary should also not be performing cataloging related functions like replacing barcodes or marking items lost or missing. She should refer those to the circulation staff or to a cataloger. This is just one example of how to define the roles in your library. Think about what they need to do, what they definitely should not be doing and if there are situations that could arise (such as overrides) that they should or shouldn't be able to address.

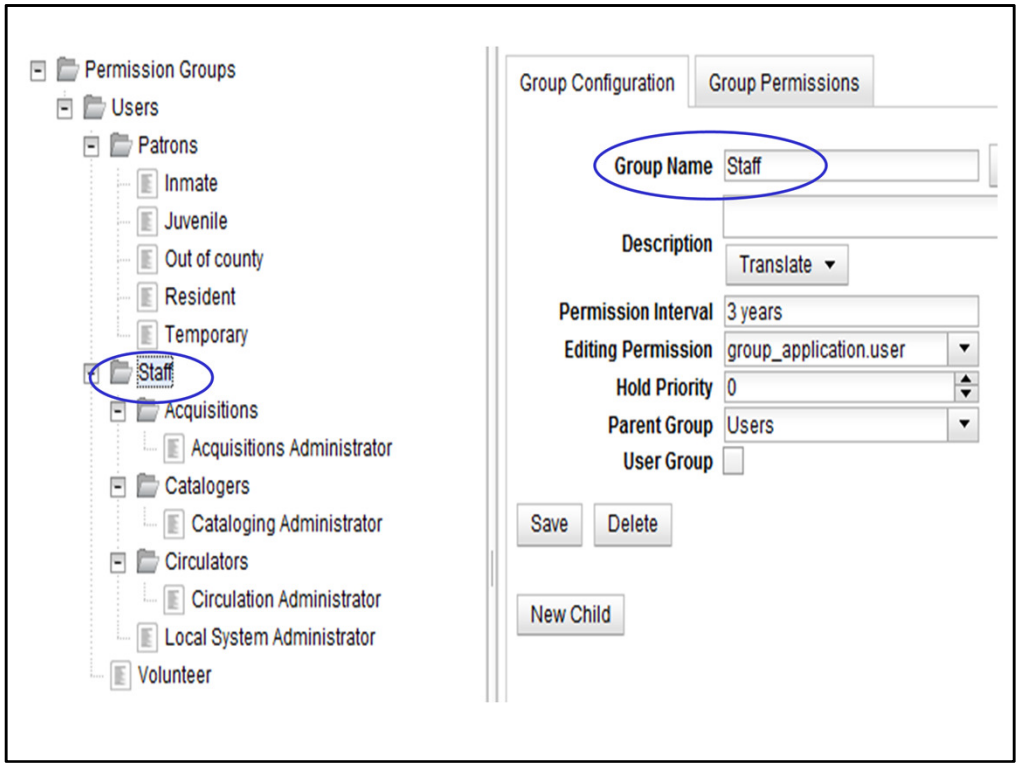
Here are the basic pieces: Permission Group (policy in Evergreen); Staff Account (which defines the username and password for the client and also ties the staff member to their appropriate permission group); Working Locations (often forgotten, you must define which libraries that staff member works out of such as the Main library and the Bookmobile).

To further define this you will follow these steps:

1. Create the Permission Group by going to Admin – Server Admin – Permission Groups.
2. Refer to the Permissions list under Admin – Server Admin – Permissions to determine which permissions to assign to the group. Assign permissions and save.
3. Once the permission group is saved, you need to run a process on the application and utility servers called autogen. This is a server administration task and Equinox can do this for sites that are supported by us or the administrator at your library can do it on your server. This process re-populates the drop down menus that refer to the permission groups such as those on the patron registration screen and in the circulation/hold matrix. Very important!
4. If you've only made edits to an existing permission group, autogen is not needed but you will need to log out and back into the staff client.
5. Once you've logged back into the staff client, you will go to Patron Registration just as you would to register any patron. There is a field for OPAC login but this is also called Staff Client Username. Fill in the username and password you want this staff member to use. Keep in mind, you can have generic accounts that are shared by several staff members. Enter all the required information including the permission group you wish to assign, such as Circulators or Volunteer. SAVE the record.

6. Retrieve the account using Patron Search or by going to User Permission Editor from the Admin menu. If you retrieve the patron from a regular patron search, go to the Other tab to get to the User Permission Editor.
7. Once in User Permission Editor, assign the working locations at the top. For instance, if a staff member works at the main library and on the bookmobile and those are two separate organizational units on your system, you will check the box next to both. Be sure to scroll all the way to the bottom to save the changes.
8. Test the login. You can do this by logging all the way out and back into the staff client or by using the Operator Change function under the Admin menu. This is good if you need to test several logins you've created.

Let's go through all of this in more detail.



Permission Groups

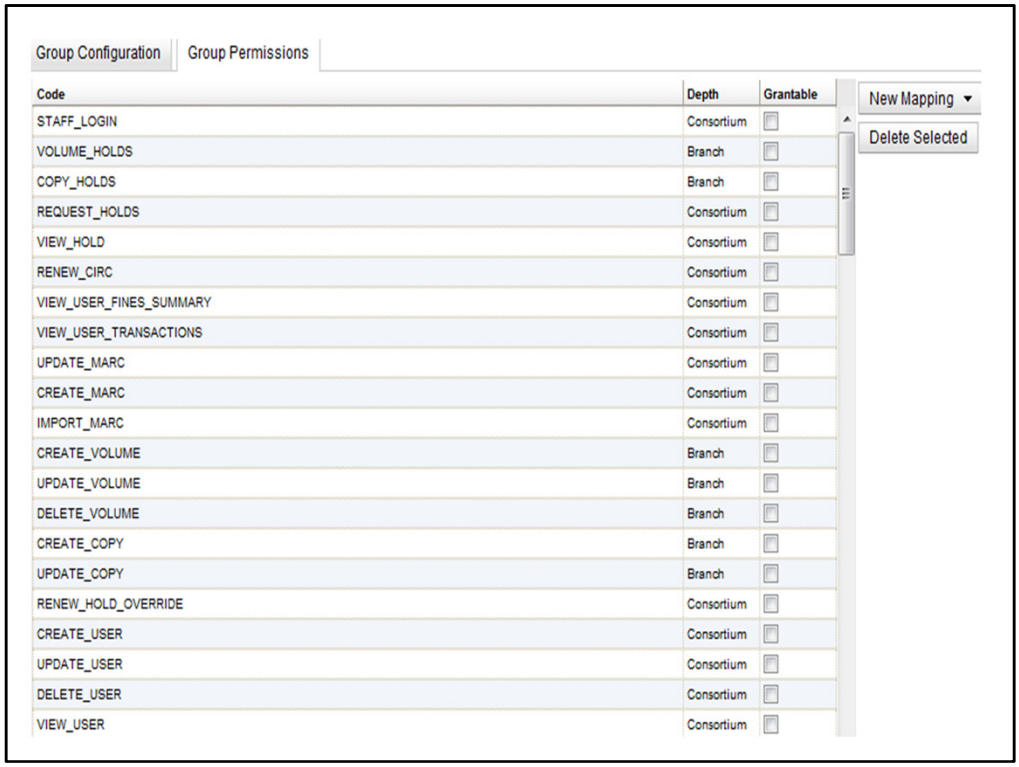
The Permission Group tree is much like the Org Unit tree where you define your libraries/branches. At the top, you have the Users group which is an umbrella over the other groups. There are generally two sub-divisions here of Patrons and Staff. All of the patron groups are associated with your users such as student, faculty, resident, non-resident, adult, juvenile, etc… The staff groups are there to define what staff members should and shouldn't do in the staff client. These are often organized into several folders. For instance, a Catalogers folder which might contain Cat1, Cat2 and Cat3 groups with varying degrees of permission. Or, as you see above, the Cataloging Administrator falling underneath the Catalogers group.

Permissions can be assigned at any level of the permission group tree. So, when putting together the list of permissions for each role within your library, you should also note which permissions EVERYONE should have. Those permissions can be added to the Staff group. There is something called "inheritance" happening here where all of the permissions at the Staff level get inherited by the groups below. Likewise, if you assign permissions to the Catalogers group, it gets inherited by the Cataloging Administrator group (based on the configuration here). So, start at the top with staff and assign all the permissions everyone needs. Then go to a specific group like Circulators and add any additional permissions they should have. Work your way down the tree this way.

As for the Group Configuration fields that get defined when you add or edit a permission

group:

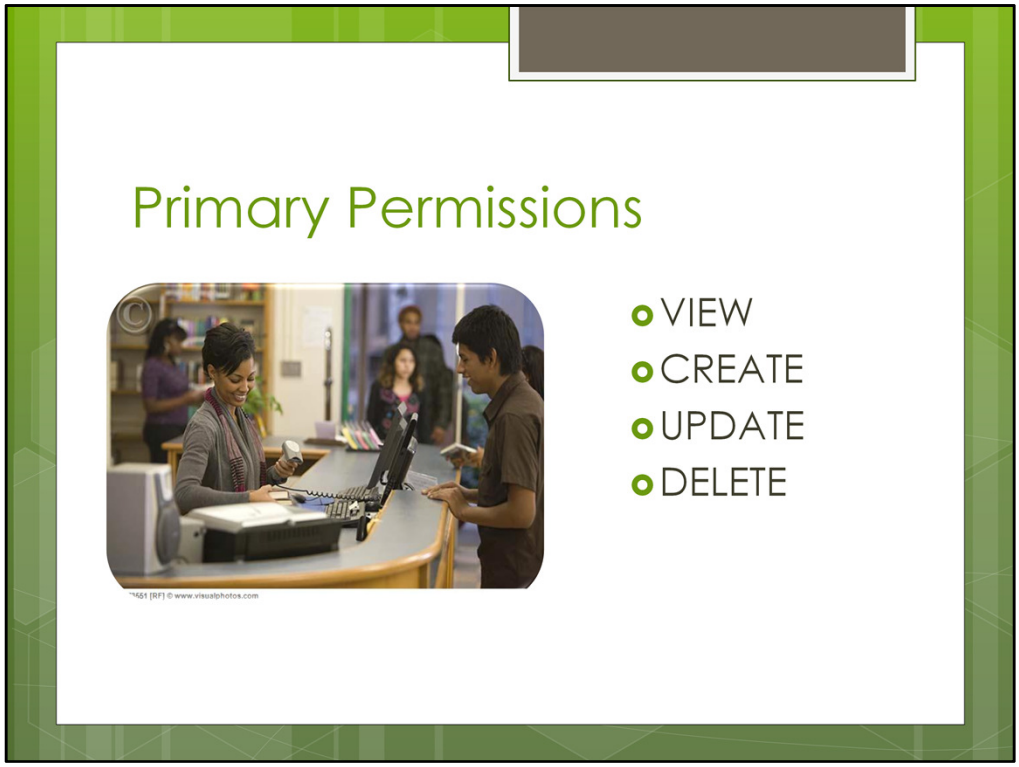
- Enter a name and description (optional) for the group.
- Enter the permission interval. For patrons, such as Residents, this might be something like 3 years. You may want this higher for staff.
- Editing permission refers to the level at which they can edit patrons and we will refer back to this later when talking about the group.application permissions.
- Hold priority, if set above 0 would be assigning a priority to a group. For instance, setting it to 1 while all other groups are 0 would give that group a higher priority in the holds queue, putting them at the top of the queue every time they request an item. This works for groups like Catalogers who need to get a hold of books to process them.
- Parent group defines the umbrella which this group falls under. In the case of Staff, the parent group is Users. In the case of Circulators or Catalogers, the parent group is Staff. This also determines which permissions will be inherited. This is why Circulators inherit the Staff permissions.
- User Group is checked or unchecked to determine whether this group is actually going to be assigned to staff accounts or if it's just there for organizational purposes. In this case, it looks like Staff is used for organization only. For small libraries, it's likely that Staff might be the only group and it is used for all staff members except for maybe the administrator or director.
- Be sure to always hit Save here if making edits. If changes are made to the name field, you will need to run the autogen script mentioned on the last slide.



Once a group is in place, go to Admin – Server Admin – Permission Groups, highlight your group and click on the second tab labeled Group Permissions. This is where all the action takes place… where you add all the individual permissions for staff. Remember you can always refer back to the Permissions list under Server Admin.

Click on New Mapping to add a new permissions and to assign the depth of the permission (to be discussed later). Also indicate whether this staff member should be able to grant the permission to someone else. Permissions can also be edited here (be sure to click save) or deleted.

Let's break down the different types of permissions to help you further determine what should be assigned to certain groups here. REMEMBER: If you assign a permission at a higher level, such as at the Staff group level, you do not have to add it again to the lower groups. Permissions are inherited from the top down.



The primary permissions will be organized into four groups: VIEW, CREATE, UPDATE and DELETE. Note that the VIEW permission is sometimes implied. If you can create and update, you can view. In other cases, it is there for everyone like the ability to see MARC records (to search the catalog). Examples below:

CREATE_CIRC_MOD
DELETE_CIRC_MOD
UPDATE_CIRC_MOD

CREATE_COPY
DELETE_COPY
UPDATE_COPY

CREATE_COPY_LOCATION
DELETE_COPY_LOCATION
UPDATE_COPY_LOCATION

CREATE_COPY_NOTE
DELETE_COPY_NOTE
UPDATE_COPY_NOTE
VIEW_COPY_NOTE

CREATE_FUND

DELETE_FUND
UPDATE_FUND
VIEW_FUND

CREATE_MARC
DELETE_RECORD (slight variation in the naming here)
UPDATE_MARC

CREATE_MFHD_RECORD
DELETE_MFHD_RECORD
UPDATE_MFHD_RECORD

CREATE_ORG_UNIT
DELETE_ORG_UNIT
UPDATE_ORG_UNIT

CREATE_USER
DELETE_USER
UPDATE_USER
VIEW_USER

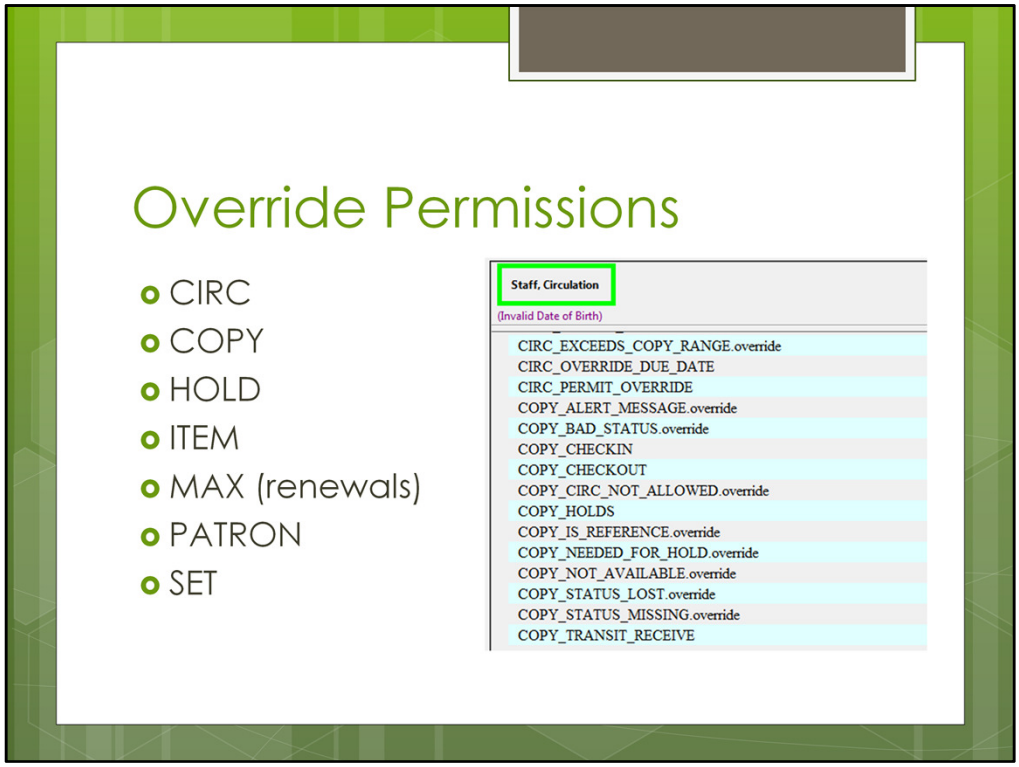
CREATE_VOLUME
DELETE_VOLUME
UPDATE_VOLUME

Some other categories to understand:

- RENEW generally refers to the RENEW_CIRC permission to renew checkouts. There's also a RENEW_HOLD_OVERRIDE to allow staff to override renewals where the item is needed for a hold.
- MARK refers to several permissions linked to copy status. For instance: MARK_ITEM_AVAILABLE; MARK_ITEM_BINDERY; MARK_ITEM_DAMAGED; MARK_ITEM_IN_PROCESS; MARK_ITEM_IN_TRANSIT; MARK_ITEM_LOST; MARK_ITEM_MISSING, etc…
- MERGE refers to the merging of patron records or bibliographic records. The three permissions are listed here: MERGE_AUTH_RECORDS; MERGE_BIB_RECORDS and MERGE_USERS.
- ADMIN is fairly obvious. Many admin functions start with the word ADMIN although this does not encompass all of the administrative permissions. Remember that there are many permissions that start with CREATE, UPDATE and DELETE that could be administrative tasks such as creating and updating circulation modifier policies. Likewise, there may be some ADMIN permissions that you would give to some staff. Here are some examples of the ADMIN permissions: ADMIN_BOOKING_RESERVATION; ADMIN_BOOKING_RESOURCE; ADMIN_CIRC_MATRIX_MATCHPOINT; ADMIN_COPY_LOCATION_ORDER; ADMIN_FUND; ADMIN_FUNDING_SOURCE; ADMIN_HOLD_MATRIX_MATCHPOINT, etc…
- MANAGE and RECEIVE relate to the acquisitions and serials modules primarily. Examples: MANAGE_CLAIM; MANAGE_FUNDING_SOURCE; MANAGE_FUND;

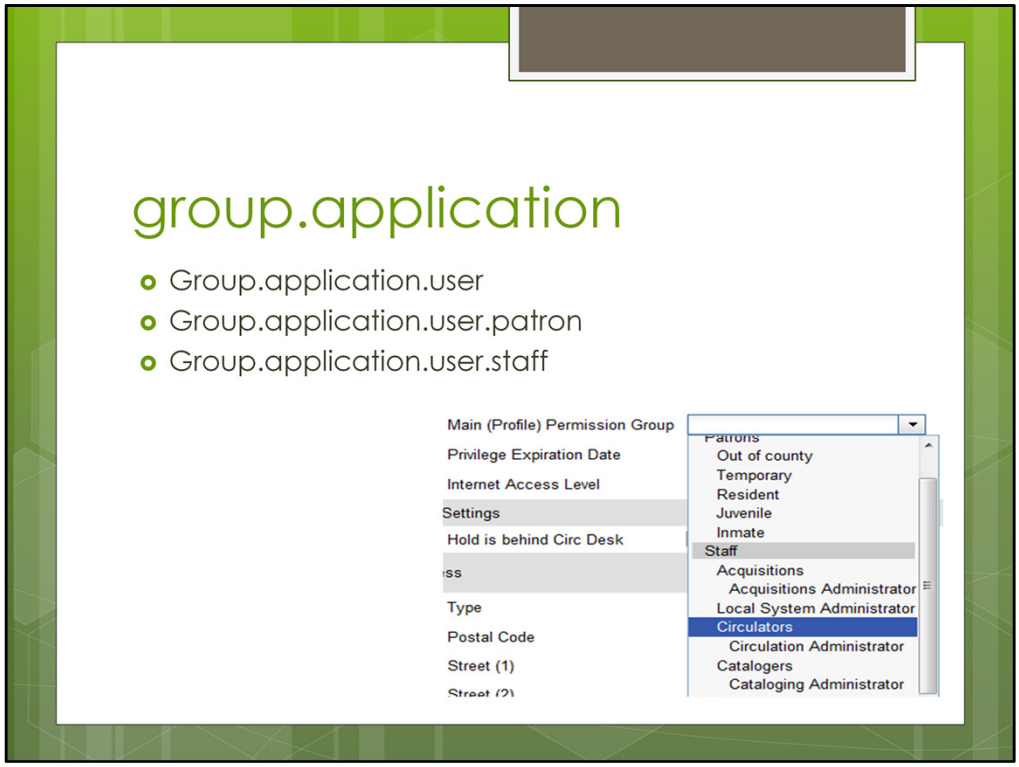
MANAGE_PROVIDER; RECEIVE_PURCHASE_ORDER; RECEIVE_SERIAL.

- There are three OFFLINE permissions that relate to the offline module in Evergreen: OFFLINE_EXECUTE; OFFLINE_UPLOAD and OFFLINE_VIEW.
- IMPORT functions relate to importing bib and authority records such as IMPORT_ACQ_LINEITEM_BIB_RECORD; IMPORT_MARC… Some of the other IMPORT permissions exist under the CREATE, UPDATE, VIEW functions such as CREATE_IMPORT_ITEM.



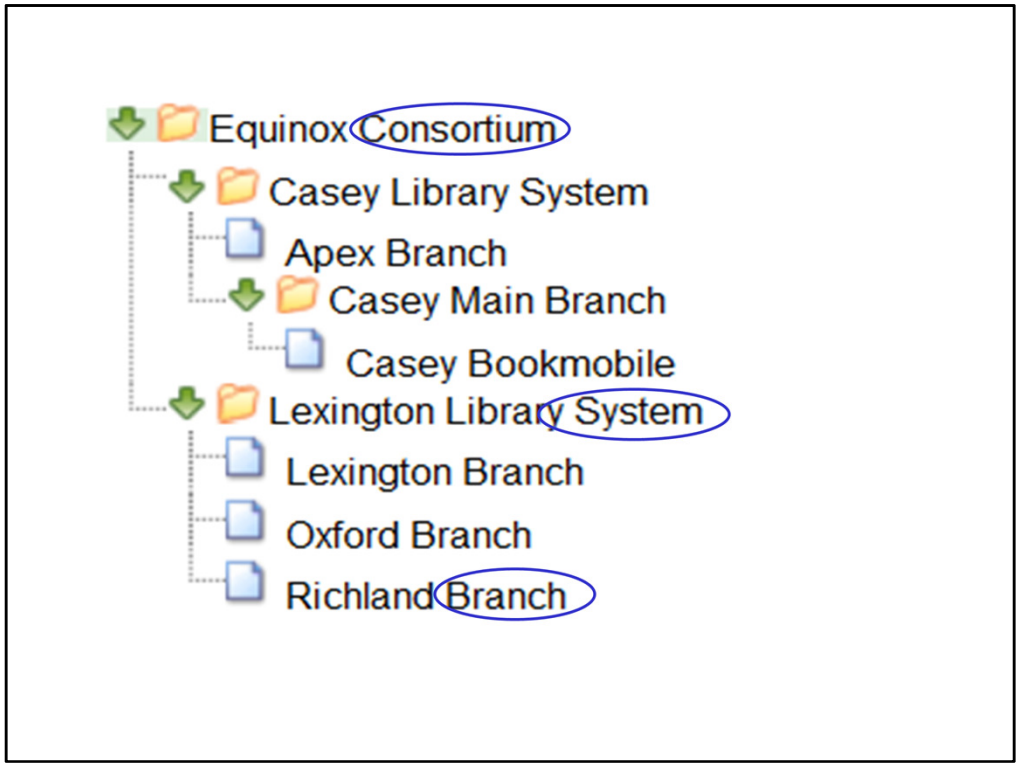
Some permissions relate to situations that might arrange if the circumstances are just right. For instance, a staff member tries to check out a book and the system says the patron is blocked. Also, what if a patron brings up a book to check out that needed to be pulled from the shelf to fill a hold? Many situations can occur and many of them happen in the circulation functions. Many of these permissions will end with ".override" so they are easy to find on the list. Therefore, many of the overrides start with words like CIRC, COPY, HOLD, etc… Here are some examples:

CIRC_PERMIT_OVERRIDE
COPY_ALERT_MESSAGE.override
COPY_CIRC_NOT_ALLOWED.override
COPY_IS_REFERENCE.override
COPY_NEEDED_FOR_HOLD.override
HOLD_EXISTS.override
HOLD_ITEM_CHECKED_OUT.override
ITEM_AGE_PROTECTED.override
ITEM_ON_HOLDS_SHELF.override
MAX_RENEWALS_REACHED.override
PATRON_EXCEEDS_CHECKOUT_COUNT.override
PATRON_EXCEEDS_FINES.override
PATRON_EXCEEDS_OVERDUE_COUNT.override
SET_CIRC_CLAIMS_RETURNED.override

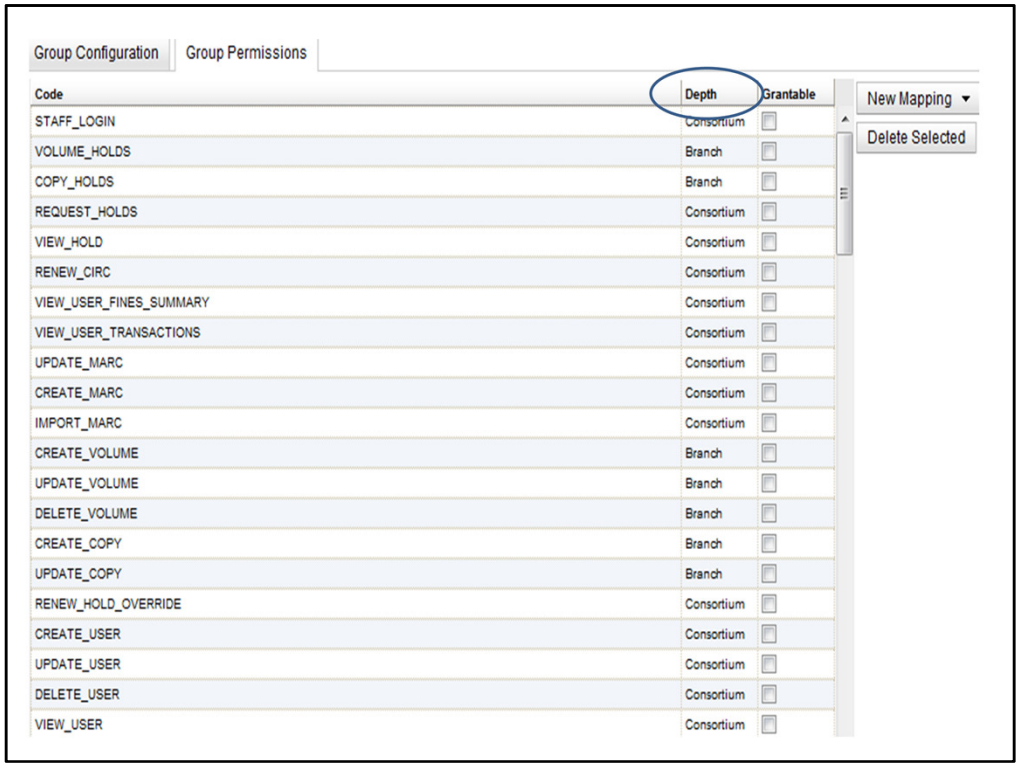


Probably the hardest concept to understand with permissions is the group.application permissions. For each permission group or sub-group that is created, there is a group.application permission. So, referring back to the list of Users/Permission Groups in our example system (slide 6) you will see the tree starts with Users then is followed by two sub-groups of Patron and Staff. Underneath we have very specific groups such as Circulators and Catalogers. So, each one has a group.application permission in the list (Users = group.application.user; Patrons = group.application.user.patron; Staff = group.application.user.staff; Circulators = group.application.user.staff.circ). When you add a group.application permission to a staff account you are saying that staff member can create and update accounts with that group.

Let's use a concrete example. You have a circulator and you want them to create and edit patron records but not staff records. You would assign them the group.application.user and group.application.user.patron permissions. You would not give them the user.application.staff (or anything below this) permission. You would also go to the Group Configuration tab referenced on slide 6 and make sure the editing permission is set to group.application.user.patron to make sure they are only editing at the patron group and below. This should ensure that only the patron groups are showing up when you log in with this account and go to register or update a patron account.



Let's go back now and talk about the depth at which you can assign a permission. For instance, if you assign the permission of CREATE_COPY, do you want that staff member to create copies for their branch only, for the system or for the entire consortium? Here's an example hierarchy of organizational units. It starts with the Consortium level for the Equinox Consortium. It is followed by the two library Systems of Casey and Lexington. Each System has Branches such as the Apex Branch or the Oxford Branch. It is also possible to go deeper in your organizational hierarchy and have sub-libraries or sub-groups. In the case here, you can see the Casey Bookmobile is a sub-library of the Casey Main Branch. Each of these represent a depth at which you can assign each permission. Let's look at the Group Permissions screen again…

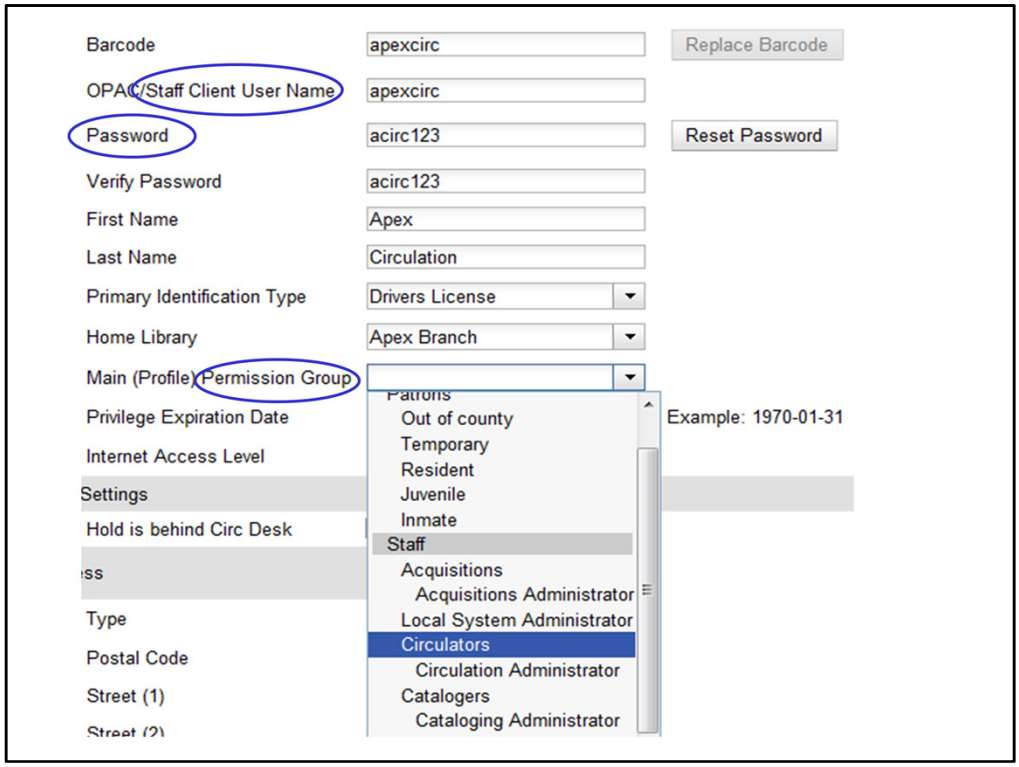


So, as each permission is added to the Group Permissions, be sure to assign the appropriate depth. There are some occasions where the depth MUST be at the Consortium level.

Here are the reasons why a permission would be at the Consortium level always:

- Bibliographic and Authority records are not owned by one branch or system. They are shared across of a consortium. Therefore, anything related to the import, creation, updating or deleting of these records should be set to the Consortium depth.
- Global policies such as adding circulation modifiers or add organizational units should also be set to the consortium level. They are generally only being managed by global administrators of the system. This is not true for local policies such as creating or editing a new copy location. Those may be assigned at the branch or system level and the person logging in should not see the option to add or edit copy locations for another branch or system.
- Administrators in general will assign all of their permissions at the Consortium level unless they are a Local Administrator or Branch Manager.
- If centralized processing of materials (for cataloging, acquisitions or serials) is handled centrally for the consortium then those permissions for creating copies, creating volumes, etc… should be set to the Consortium.

- One more situation. There are some situations where a permission is in use and you may not realize it. For instance, when updating a bibliographic record, it will pull up the record summary which includes the user who first created the title or last edited the title. The VIEW_USER permissions is in use here to allow staff to see those two fields. Because of this, catalogers should really have their VIEW_USER permission set to the Consortium level.

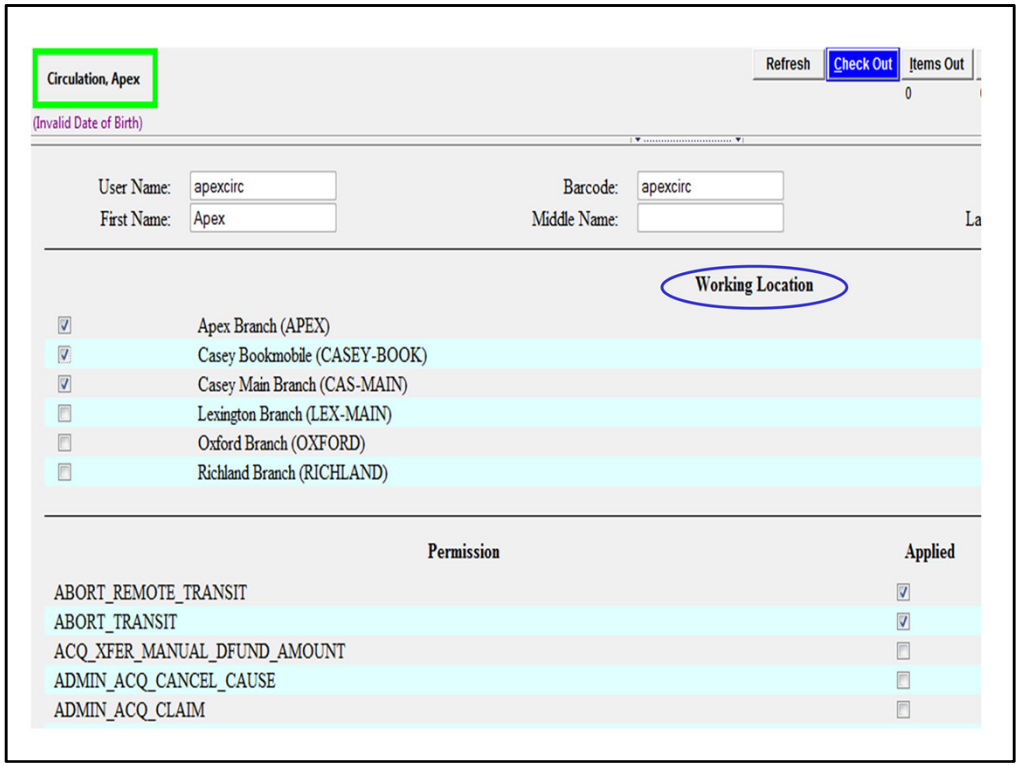


Now that the permission groups are set up and permissions have been assigned, you can register the staff account. REMEMBER: If you set up a brand new permission group, the autogen process needs to run on the application and utility servers before this step will work. In addition, if you edited an existing group, be sure to log out and back in before creating the staff account to load all the changes.

To register a staff account, you will use the Patron Registration screen. Fill in the Staff Client User Name, Password and Permission Group as well as all other required fields. This is what ties the permission group together with the staff's login.

Something else to discuss is whether you want to create staff accounts for each individual staff member or if you want to have shared accounts such as the example above where the staff member is described simply as apexstaff and their name is Apex Circulation. This may depend on the size of your library and the turnover rate of staff members. Student workers, for instance, turn over often so it's best to have a generic log in for them unless you are trying to track what each person is doing.

Don't forget to hit SAVE!



Before you test the login, you must do the final step in the process which is assigning working locations. This is often forgotten and when you go to login, you'll find you can't do much in the staff client until these are assigned. The idea of a working location is simply where does the staff member work out of? If they work at multiple locations, check all the boxes you need to represent where they work over the course of the week.

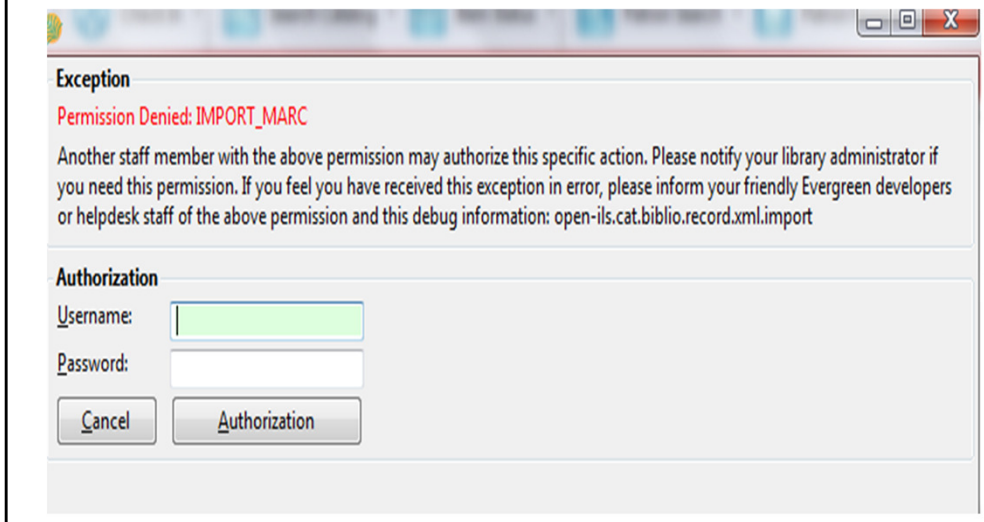
To find the working locations, retrieve the user using a patron search OR click on Admin – User Permission Editor and search for them by barcode/username. If you retrieve them via the standard Patron Search screen, be sure to go to the Other tab and then User Permission Editor. The working locations are at the top. Check the box(s) and scroll ALL THE WAY DOWN to find the Save button. You should see how many working locations were updated when you click Save.

Also, while we're here, the User Permission Editor can also be a great place to add a few additional permissions to one staff account. It is not advised that you try to change all the permissions currently there because it won't save them. The group permissions already in place will supercede changes you try to make. You can only use this screen to add additional permissions not currently a part of their group.

An example: You may have one Circulation Supervisor and you assign them to the Circulators group like everyone else in Public Services. You can go to the User Permission Editor to give that Circulation Supervisor account a few more permissions in addition to the ones already assigned from the Circulators group. This prevents the need to add another

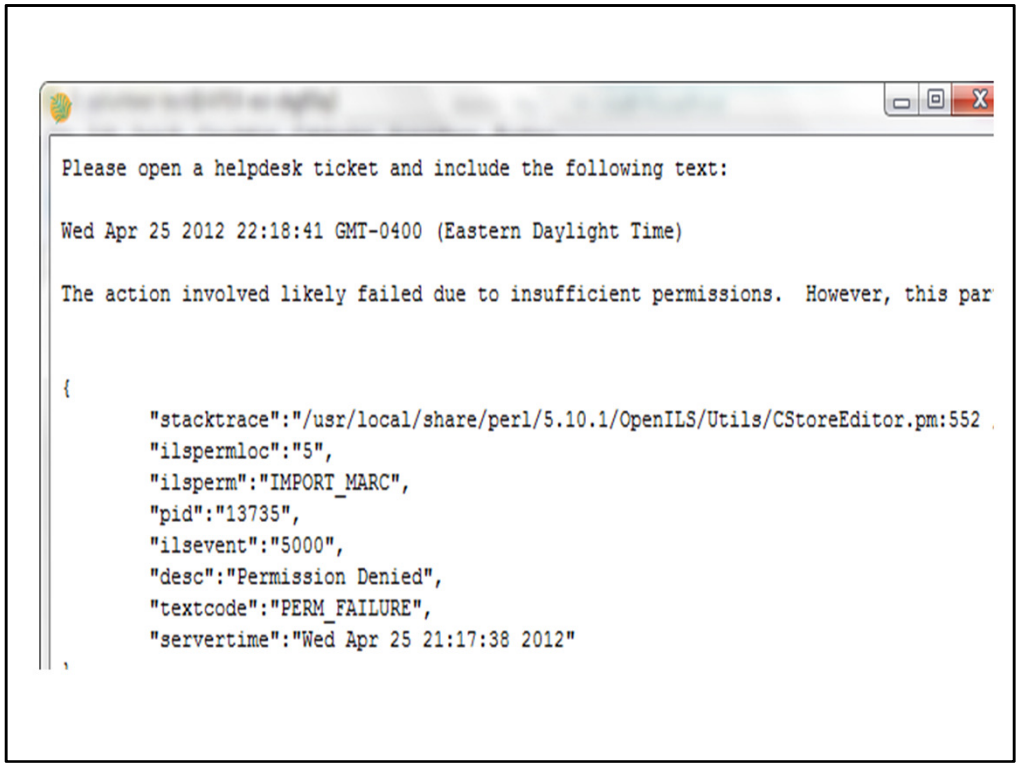
Permission Group under Server Admin.

ALWAYS remember to scroll all the way down the screen past all the permissions to click the Save button. It will not alert you that you are leaving the screen with unsaved changes.

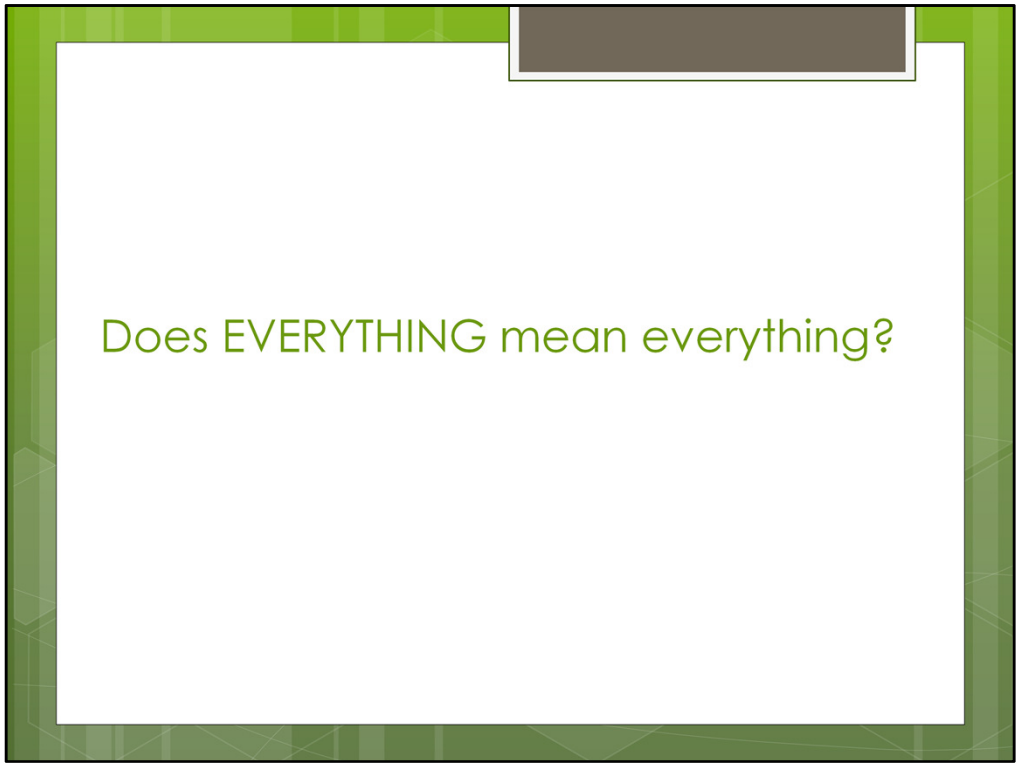


If you go to log in to test an account, you may run into errors when trying to access something you don't have permission to use. Here's an example of trying to go to the Import MARC screen. So, you can see the system is fairly obvious when you've missed assigning a permission or when someone is trying to access something they shouldn't.

You can also see that you can enter authorization to give someone permission to do something they wouldn't normally do. In this case above, if a Circulator was going to import a batch of MARC records and they hit up against this message, a manager or admin user could enter their credentials here to give them access temporarily. It doesn't grant them access forever to this screen, just this one time.



Other errors related to permissions may not be so obvious but if you ever have a “debug output” button on the screen, you can click on it and you may see something like this that makes it pretty obvious that the error was a result of a permission not being assigned.



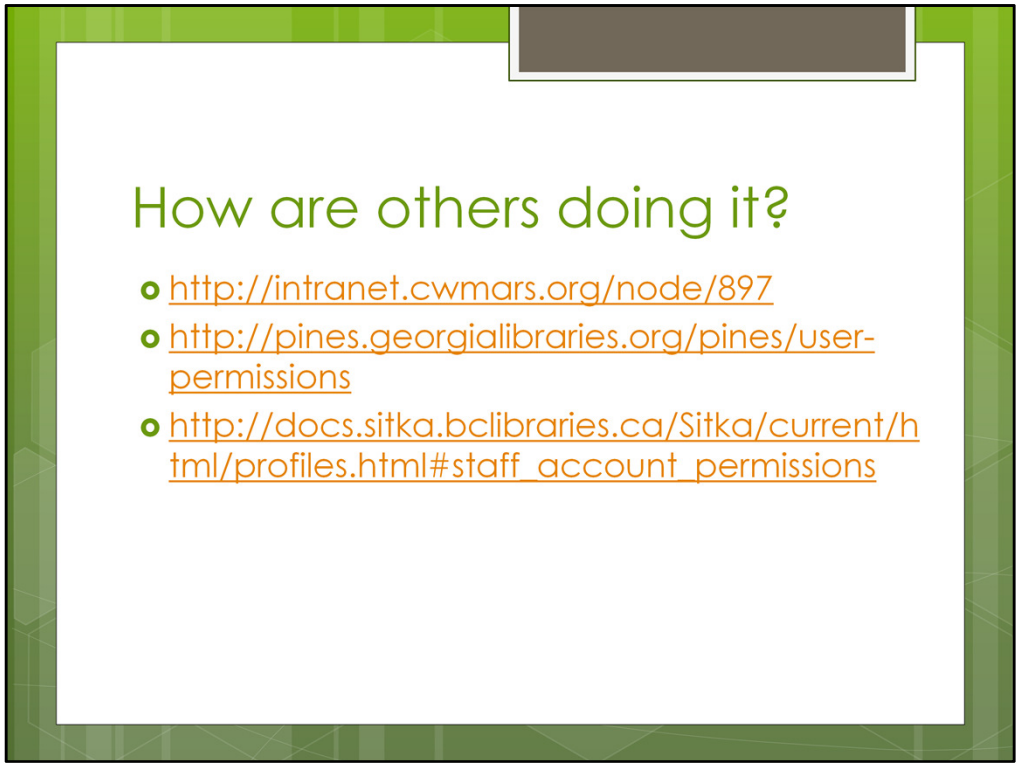
A big question I get all the time is does the EVERYTHING permission really encompass EVERYTHING. The short answer is NO. It includes A LOT but not EVERYTHING. So, it's a good permission to add to an administrators group to get you started but there are a few things missing. For instance, many of the newer permissions will not be encompassed in EVERYTHING so if you've upgraded recently and are looking at the new permissions, know that they generally aren't getting rolled into EVERYTHING. In addition, things like IMPORT_MARC are not included here. This permission may eventually go away or get changes to include all permissions. The fate of the EVERYTHING permission is unclear at this time.

Here is a list of some of the new permissions at version 2.2. This may not be exhaustive but I tried to find all the new permissions I could. Always remember after an upgrade to check documentation for the list of new permissions or go to Admin – Server Admin – Permissions to review the list again for new items.

New at version 2.2

- CREATE_AUTHORITY_CONTROL_SET
- UPDATE_AUTHORITY_CONTROL_SET
- DELETE_AUTHORITY_CONTROL_SET

- CREATE_MONOGRAPH_PART
- UPDATE_MONOGRAPH_PART
- DELETE_MONOGRAPH_PART
- MAP_MONOGRAPH_PART.



You do not have to do this from scratch. Equinox delivers some permission groups to get you started and there are also other consortia who have documented their permission groups well. Check these out.

So, in summary, be sure to think very specifically about what each staff member should or shouldn't do in the system before you start creating groups and staff accounts. Document the permission groups well so when you make changes, you can update the document. Permission groups are global so they are shared across a consortia. Therefore, when talking about other global policies during the implementation phase, permission groups should also be discussed and some consensus is needed. You do not have to reinvent the wheel – borrow from others who have put a lot of time and research into their permission groups (see previous slide). Finally, remember as you upgrade you will need to check for new permissions.

Please let me know if you have questions about anything documented here. I can be reached at shae@esilibrary.com. Thank you for your time today!