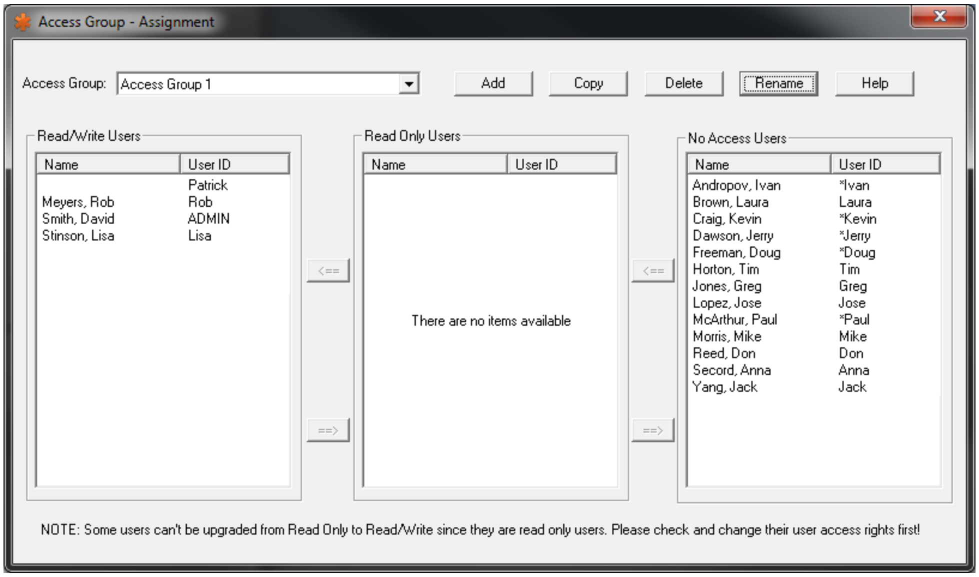
OBTAIN How-To: Access Groups

<u>What is an Access Group?</u>

Often times, in any datacenter, there are multiple different groups of assets that are owned by different groups of people. Our users asked for a way to assign specific assets to specific groups/users and prevent users from other groups from making modifications to those assets. As a solution to this request the Access Groups feature was added into OBTAIN. Access Groups allows a user to define different user groups to represent the various different groups of people/assets that exist in their datacenter. After a user group has been defined, assets can be assigned to those groups making it so only users in those groups can make modifications to those assets, in OBTAIN.

<u>How to Use Access Groups:</u>

1) Define a new Access Group:
    a. On the Device window, while looking at any Device, click on the Nexus tab and then click the Access Groups button.
    b. On the Restrict Assets window click the List button.
    c. On the Asset Group window click the Add button.
    d. Input an Access Group name and click Create.



Access Group: Access Group 1

Read/Write Users

Name	User ID
	Patrick
Meyers, Rob	Rob
Smith, David	ADMIN
Stinson, Lisa	Lisa

Read Only Users

Name	User ID

There are no items available

No Access Users

Name	User ID
Andropov, Ivan	*Ivan
Brown, Laura	Laura
Craig, Kevin	*Kevin
Dawson, Jerry	*Jerry
Freeman, Doug	*Doug
Horton, Tim	Tim
Jones, Greg	Greg
Lopez, Jose	Jose
McArthur, Paul	*Paul
Morris, Mike	Mike
Reed, Don	Don
Secord, Anna	Anna
Yang, Jack	Jack

NOTE: Some users can't be upgraded from Read Only to Read/Write since they are read only users. Please check and change their user access rights first!

(Figure 1)

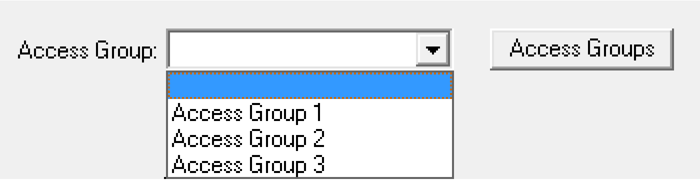
2) **<u>Assign users to an Access Group:</u>**

Once an Access Group has been defined users need to be assigned to it to determine who is and isn't able to modify the information on specific Assets. All of the users in OBTAIN are listed within the three boxes on the Access Group window. By default, when you make a new Access Group, all ADMIN level users are set in the Read/Write column and all Advanced and Normal users are set in No Access. To change which users have which permissions, click on a user's name and use the <= and => buttons to move them between the Read/Write, Read Only and No Access columns. Users set as Read/Write will be able to modify any Asset that is part of that Access Group. Read Only users will be able to bring up an Asset to view its information but will be unable to make any updates to it.

3) **Assign Assets to an Access Group:**

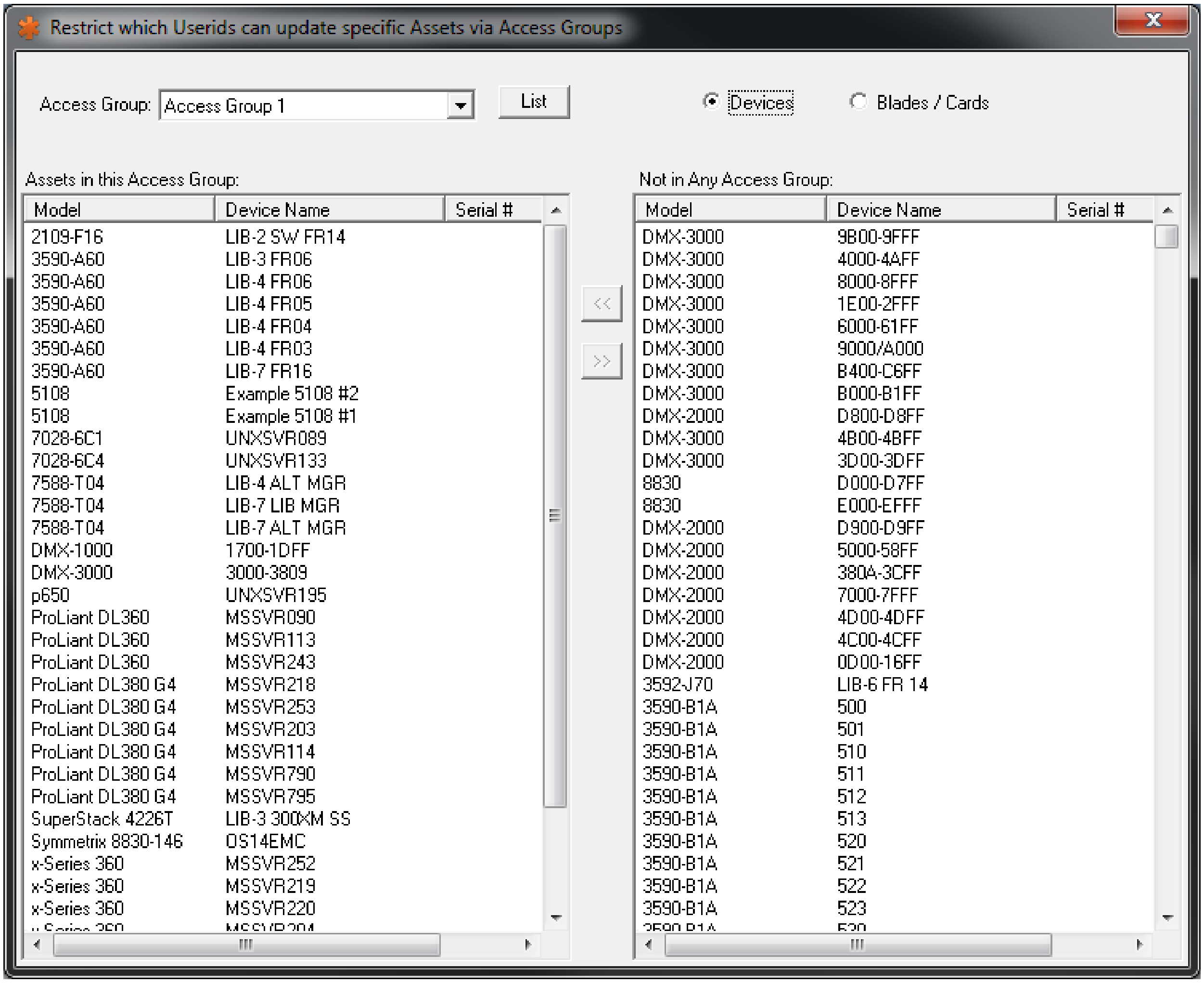
There are two ways to assign an Asset to an Access Group:

a. On the Nexus tab of a Device there is an Access Group drop-down list. By clicking on the drop-down list and selecting an Access Group the Device you are currently viewing is then assigned to that Access Group.



(Figure 2)

b. Alternately, by clicking the Access Groups button, also on the Nexus tab, the Restrict Access via Access Groups dialogue will open. From here, an Access Group can be selected from the top left drop-down list. Devices, Blades and Cards can then be assigned to that Access Group, in mass, by using the << and >> buttons to move the Assets between the "Assets in this Access Group" and the "Not in Any Access Group" columns (See Figure 3).


Restrict which Userids can update specific Assets via Access Groups
List
<<
>>

Access Group: Access Group 1

● Devices ○ Blades / Cards

Assets in this Access Group:

Model	Device Name	Serial #
2109-F16	LIB-2 SW FR14	
3590-A60	LIB-3 FR06	
3590-A60	LIB-4 FR06	
3590-A60	LIB-4 FR05	
3590-A60	LIB-4 FR04	
3590-A60	LIB-4 FR03	
3590-A60	LIB-7 FR16	
5108	Example 5108 #2	
5108	Example 5108 #1	
7028-6C1	UNXSVR089	
7028-6C4	UNXSVR133	
7588-T04	LIB-4 ALT MGR	
7588-T04	LIB-7 LIB MGR	
7588-T04	LIB-7 ALT MGR	
DMX-1000	1700-1DFF	
DMX-3000	3000-3809	
p650	UNXSVR195	
ProLiant DL360	MSSVR090	
ProLiant DL360	MSSVR113	
ProLiant DL360	MSSVR243	
ProLiant DL380 G4	MSSVR218	
ProLiant DL380 G4	MSSVR253	
ProLiant DL380 G4	MSSVR203	
ProLiant DL380 G4	MSSVR114	
ProLiant DL380 G4	MSSVR790	
ProLiant DL380 G4	MSSVR795	
SuperStack 4226T	LIB-3 3000XM SS	
Symmetrix 8830-146	0S14EMC	
x-Series 360	MSSVR252	
x-Series 360	MSSVR219	
x-Series 360	MSSVR220	
x-Series 360	MSSVR204	

Not in Any Access Group:

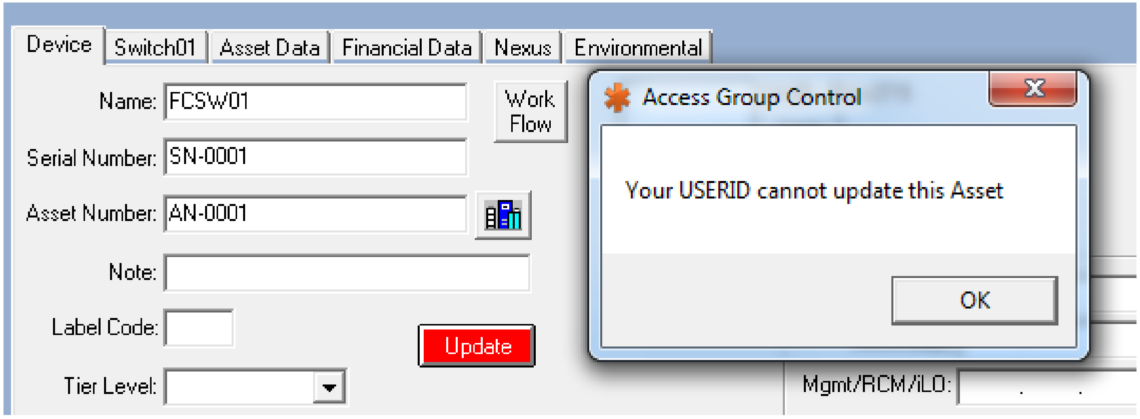
Model	Device Name	Serial #
DMX-3000	9B00-9FFF	
DMX-3000	4000-4AFF	
DMX-3000	8000-8FFF	
DMX-3000	1E00-2FFF	
DMX-3000	6000-61FF	
DMX-3000	9000/A000	
DMX-3000	B400-C6FF	
DMX-3000	B000-B1FF	
DMX-2000	D800-D8FF	
DMX-3000	4B00-4BFF	
DMX-3000	3D00-3DFF	
8830	D000-D7FF	
8830	E000-EFFF	
DMX-2000	D900-D9FF	
DMX-2000	5000-58FF	
DMX-2000	380A-3CFF	
DMX-2000	7000-7FFF	
DMX-2000	4D00-4DFF	
DMX-2000	4C00-4CFF	
DMX-2000	0D00-16FF	
3592-J70	LIB-6 FR 14	
3590-B1A	500	
3590-B1A	501	
3590-B1A	510	
3590-B1A	511	
3590-B1A	512	
3590-B1A	513	
3590-B1A	520	
3590-B1A	521	
3590-B1A	522	
3590-B1A	523	
3590-B1A	530	

(Figure 3)

How are Device Updates Restricted?

There are two main areas where Device updates are restricted. The first is on the Devices window and the second is on the Racks window.

1) **Devices Window:**
   If a user has the Devices window open and they are currently viewing a Device which they have Read-Only access to, then they will not be able to modify any of the information on the Device. If the user attempts to modify any information on the Device they will receive an informational pop-up box which will inform them that they do not have permission to modify the current Device (see Figure 4).



Name: FCSW01

Serial Number: SN-0001

Asset Number: AN-0001

Note:

Label Code:

Tier Level:

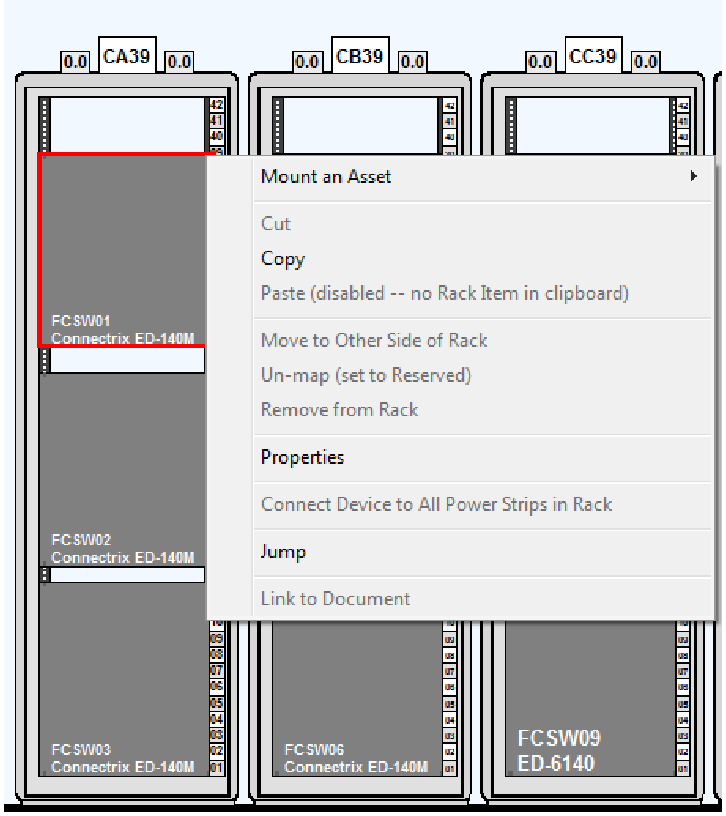
Mgmt/RCM/iLO:

Your USERID cannot update this Asset

(Figure 4)

2) **Racks Window:**
   Aside from modifying the information on a Device, there are also restrictions which prevent a user from making changes to a Device in the Racks window. First, if a user tries to mount a Device into a Rack, any Devices that the user is restricted from modifying will not be displayed in the list of mountable Devices. Second, if a restricted Device is already mounted in a Rack the user will not be able to do any of the following; cut and paste the Device, remove the Device from the Rack or move the Device using the arrow keys (see Figure 5).

   (In Figure 5, note that all of the options that would modify the Device in the Rack are greyed out, signifying that they are disabled and unusable).



(Figure 5)