Managing Non DCE Security for Infoprint Manager for AIX

Back to Administrator Procedures

Infoprint Manager Security, a feature that you administer through SMIT, allows you to protect your printing system by associating an Access Control List (ACL) with an Infoprint object or operation. An ACL is the list of users and groups who have permission to do something to or with an object, and what type of permission that is.

If you do not want to use Infoprint Manager Security, you can turn it off using the server properties notebook in the Infoprint Manager Administration GUI by setting the **Security level** for your server to **none**.

Types of permission

In Infoprint Manager, users can have three levels of permission: **read**, **write**, and **delete**. The levels provide the following types of access:

- **Read**

  For operations, the user can perform the operation. For servers and queues, the user can view the attributes. For destinations, the user can view attributes and submit jobs to that destination.
- **Write**

  For all objects, the user can view and modify attributes.
- **Delete**

  For all objects, the user can view and modify attributes and can delete the object.

Note: The levels of permission are not cumulative. If you give a user **delete** permission only, he will **not** automatically have **read** and **write** permissions. Be sure to mark all of the levels of permission that the user needs.

If you place userA on the ACL for the logical destination “print2ld” and give her **read** permission, she can send her print jobs to it and can open the “print2ld” object to see its properties. However, she cannot make changes to those properties. If she tried to change any of them or tried to delete the destination, she would receive an error message. If you decide that userA needs to be able to do more and give her **write** permission as well, she will be able to change the properties of “print2ld,” but still will not be able to delete it.

Important: If you protect a destination (logical or actual) so that only certain users can modify or delete its properties, you may inadvertantly prevent other users from submitting print jobs to it. To be sure that all of your users can still print to the destination, add the wildcard character (*) to the ACL as a user with read permission.

You can also attach ACLs to the operations that you can perform on Infoprint objects. Allowing you to protect both operations and objects means that Infoprint Manager Security provides different levels of security: you can protect all objects by using ACLs at the operation level or you can protect individual objects with

ACLs applied only to them. Or you can do both—protect all objects by using operation-level ACLs for some operations, and limit access to sub-sets of objects by using object-level ACLs.

Note: All Infoprint object names, including security groups and ACL members, are case sensitive.

For operations, there is only one level of permission: **read**. If a user has **read** permission, he can perform that action; if he does not, he cannot perform the action. For example, userB is a printer operator and must be able to move jobs to different positions in the print queue because some jobs need to be printed before others. You can give userB **read** permission for the operation **Reorder Job** to allow him to do his job. On the other hand, userC submits print jobs from his office workstation and doesn't like to wait for the jobs ahead of his in the queue to print. If you want to prevent him from moving jobs, don't put him on the ACL for the **Reorder Job** operation. When he tries to move his job to the top of the queue, the action will be denied.

When you install Infoprint Manager, many operations are already protected so that only members of the **admin** and **oper** groups can perform them. You can see the ACLs for operations using SMIT. Open an AIXterm window and type `smit`. With your mouse, open the Infoprint Printing System item and select **Security –> Access Control –> Operations –> Show Access Control List**. If you want users to be able to perform those operations, you must either add those users to the individual ACLs or to a group that has permission (either the existing **admin** and **oper** groups or a new group that you create).

Note: If an object is protected, a user can only perform an operation on that object if he has both **read** permission for the operation and the appropriate level of permission for the object.

- If the object is not protected, any user with **read** permission on an operation can perform that operation.
- If the object is protected, the permission needed depends on the operation. For example: **List** requires **read** permission on the object, **Set** requires **write** permission, and **Delete** requires **delete** permission.

By default, Infoprint objects (destinations, queues, servers) are not protected, members of the **admin** group have read permission on all operations, members of the **oper** group have read permission on most operations, and **all** users have read permission on five operations. Those five operations are:

- **List/Query** (all objects)
- **Print**
- **Modify job**
- **Query job**
- **Remove job** (delete job)

However, users who are not members of the **admin** and **oper** groups can only modify and remove jobs that they submitted. In addition, if the ACL for the **Reorder job** action is changed so that everyone can use it, users who are not members of the **admin** and **oper** groups will only be able to reorder jobs that they submitted. By default, members of the **admin** and **oper** groups can perform all six of those operations on all jobs.

Note: If you decide to protect your queues, all users will still be able to perform the tasks listed above on their own jobs. Users who are on the ACL for a queue will be able to perform those tasks on all jobs in that queue.

Security groups

No matter what size organization you work in, manually adding every user to every ACL can be a time-consuming process. To reduce some of the work, you can create *security groups*, groups of users who need to have the same levels of permission for the same objects. You use the name of the security group like a user ID; instead of adding each user ID to an ACL, you add the group name. For example, if you want all ten of your print operators to be able to perform the same operations, create a group and name it **operators**. Then, add **operators** to the appropriate ACLs.

When you install Infoprint Manager, three security groups are created by default:

- **acl_admin**

  Users who have authority to manage security by changing access control lists and groups. The default members are **root** and the user who was logged on when Infoprint Manager was installed.
- **admin**

  Users who have administrator authority. The default members are **root** and the user who was logged on when Infoprint Manager was installed.
- **oper**

  Users who have operator authority. The default member is **root**.

Note: You can modify these groups as needed. In the example above, you could have simply added your operators to the default **oper** group and modified any permissions that weren't set to the level that you wanted them.

You can add users to multiple groups, but you cannot make one group a member of another group. For example, if you hire five new print operators, you might create a group for them called **trainees**, since you only want them to have limited permissions until they are finished with their training. When they finish their training, you cannot add **trainees** as a member of the **operators** group. You will have to add their user IDs to the operators group one at a time. In addition, you will have to either delete the **trainees** group or delete the members from it—otherwise those users will have conflicting levels of permission.

When users are members of more than one group and each group has a different level of permission for a particular object, the most restrictive permission applies. In the example above, if you forgot to remove the new employees from the **trainees** group at the end of their training, they wouldn't be able to perform the tasks their job required- they would still be restricted.

Identifying users and groups: wildcarding

When you add users to ACLs or Security groups, you identify them by their user ID and the computer that they work on in this format: *username@computername*. The permissions you assign will only apply when that person accesses Infoprint Manager from that workstation.

If, however, you or any of your users want to be able to work with Infoprint Manager objects from various workstations, you may not want to add multiple user ID / computer name combinations for the same person—you can use wildcarding instead. When you use wildcarding, you replace the computer name or user ID with the wildcard character (*) when you add a member to an ACL or Security Group. The wildcard character stands for “any computer” or “any user ID.” So, if you create an ACL member called **administrator***, no matter what computer you log on to as **administrator**, you have the same permissions. If you use the wildcard character before the computer name, for example ***computer1**, any user who logs on to computer1 can perform the actions that the ACL member has permission for.

Working with ACLs and groups

Use the AIX SMIT utility to manage the security of your print system. Open an AIXterm window and enter `smit` on the command line. The line Infoprint Printing System will appear as an option. By following the menu item to the right with your cursor, you can navigate the following directory structure of menu choices:

Tab #1	**Tab #2**	**Tab #3**	**Choices**
Infoprint Printing Systems→	Security→	Groups→	Add Group Show Group Add User to Group Remove User from Group

Tab #1	**Tab #2**	**Tab #3**	**Tab #4**	**Choices**
Infoprint Printing Systems→	Security→	Access Control→	Operations→	Show Access Control List
			Servers→	Change Access Control List
			Destinations→	Remove Access Control List
			Queues→	

For specific information about a menu choice, press the F1 key for help.