Group Creation Conventions for Active Directory

Stephanie Obodda - 2016-01-25 - Comments (0) - Active Directory

This article is intended for IT staff at Brown who need to set up and configure aspects of the Active Directory Service. Faculty and staff who are general users of the service do not need to take action based on this document.

- - - -

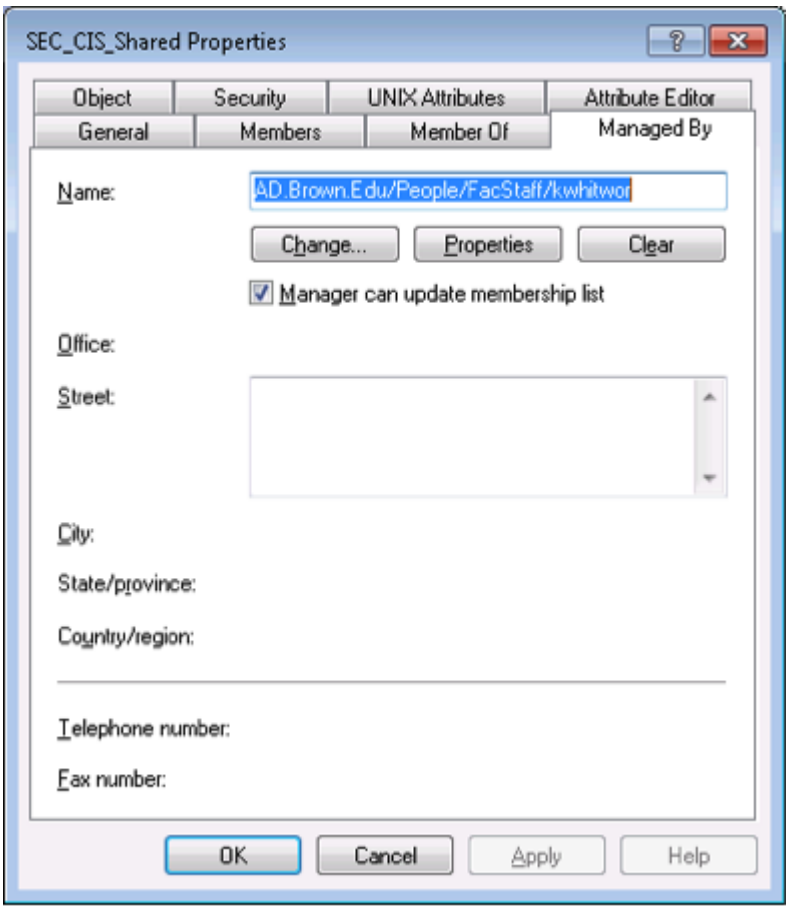
Quick Links

- Group Naming Conventions
- Userid Syntax

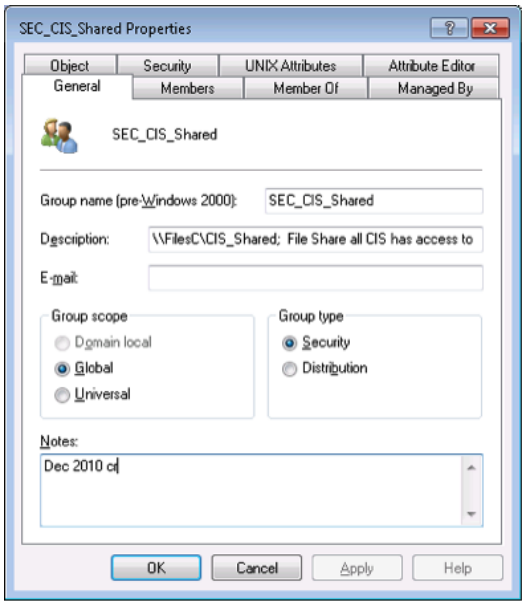
Overview

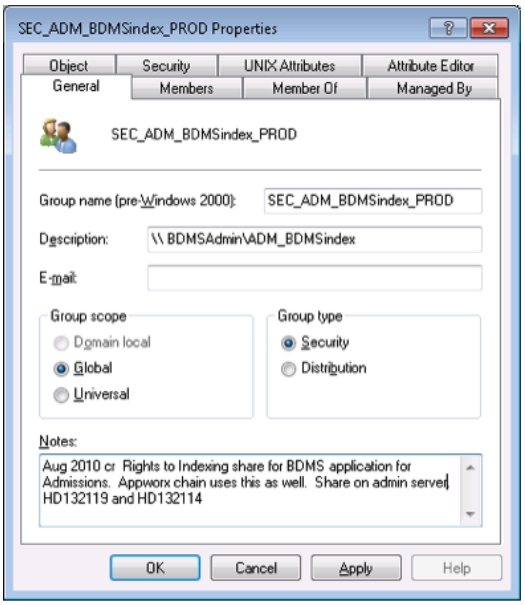
Each group must have the “Managed by” information filled in. This is the person that is responsible for verifying the group membership is correct.

Why is this important? Eventually we will be scripting a verification email to run 2 or 3 times a year on all of the AD groups. This email will be sent to the person in the manager’s field asking them to review their group membership.



When a new group is created in AD, information should be provided in the Notes section of the group object annotating the month/year of creation and the creator's name or initials. This should also be used for any additional information needed to explain what the group is used for.





The description field of the group object should reflect explicit information about the

group's use. If the group is used for granting access to a share, the server name and share should be given: e.g., \\FilesC\CIS_Shared.

To allow easy searches in Active Directory for specific types of groups, we are naming all objects with a standard prefix.

Group Naming Conventions

- SEC_
- DLG_
- PRT_
- XFER_
- FTP_
- GADM_
- APL_
- RDP_
- VM_
- QAD_

SEC_

- SEC stands for Security
- Used to grant access to shares and directories on a server.
- Syntax = SEC_dept_share_xx
  i. The department acronym is placed in the "dept." space, e.g., SEC_CIS or SEC_ADM
  ii. The share or directory name follows the department acronym: e.g., SEC_CIS_shared
  iii. Additional information to define the location or usage follows the directory name: e.g., SEC_CIS_DR_CoreTeam; SEC_ADM_BDMSindex_PROD. Explicit information on the group's use should also be reflected in the Description and Notes field of the group object in Active Directory (AD).
  iv. Suffix used for group naming to annotate rights given via group membership
    1. If there is not a suffix on the group name then Read Write is assumed.
    2. RO - Read ONLY access is followed by "_RO", e.g., SEC_CIS_DR_Files_RO
    3. RW - Read Write access is followed by "_RW". This is generally used when there is both a Read ONLY and a Read Write group for access to the share, e.g., SEC_CIS_DR_Files_RW
    4. ViewSubfolders - Rights for traversing a directory, the group name will be followed by "_ViewSubfolders": e.g., SEC_CIS_EAS_ViewSubfolders
- Groups are located in the department OU under deptGroups: e.g., AD.Brown.Edu/Departments/Public Safety/PublicSafetyGroups
    i. Some groups that require additional security are located in the Infrastructure OU and access is limited to the Windows team, CAP, and the ITSupport group.

ii. There are also a few groups used for Security where access is limited to only the Windows team. These are located in the InfrastructureSystems OU.

- Groups will always be used to grant access to shares even if they only contain 1 member. This allows us to audit what a user has rights to by reading their group membership in their user object. If an individual user account is used to grant access it cannot be audited.
- * Full rights to the departmental Windows shares for the department's SysAdmin are granted with the group SEC_dept_Delegates. The SysAdmin's personal userid is added to this group since most users have persistent mappings to the shares via a login script using their personal id. The SysAdmin would be unable to make a second connection to the share using their adm account with the persistent mapping using their personal userid.

DLG_

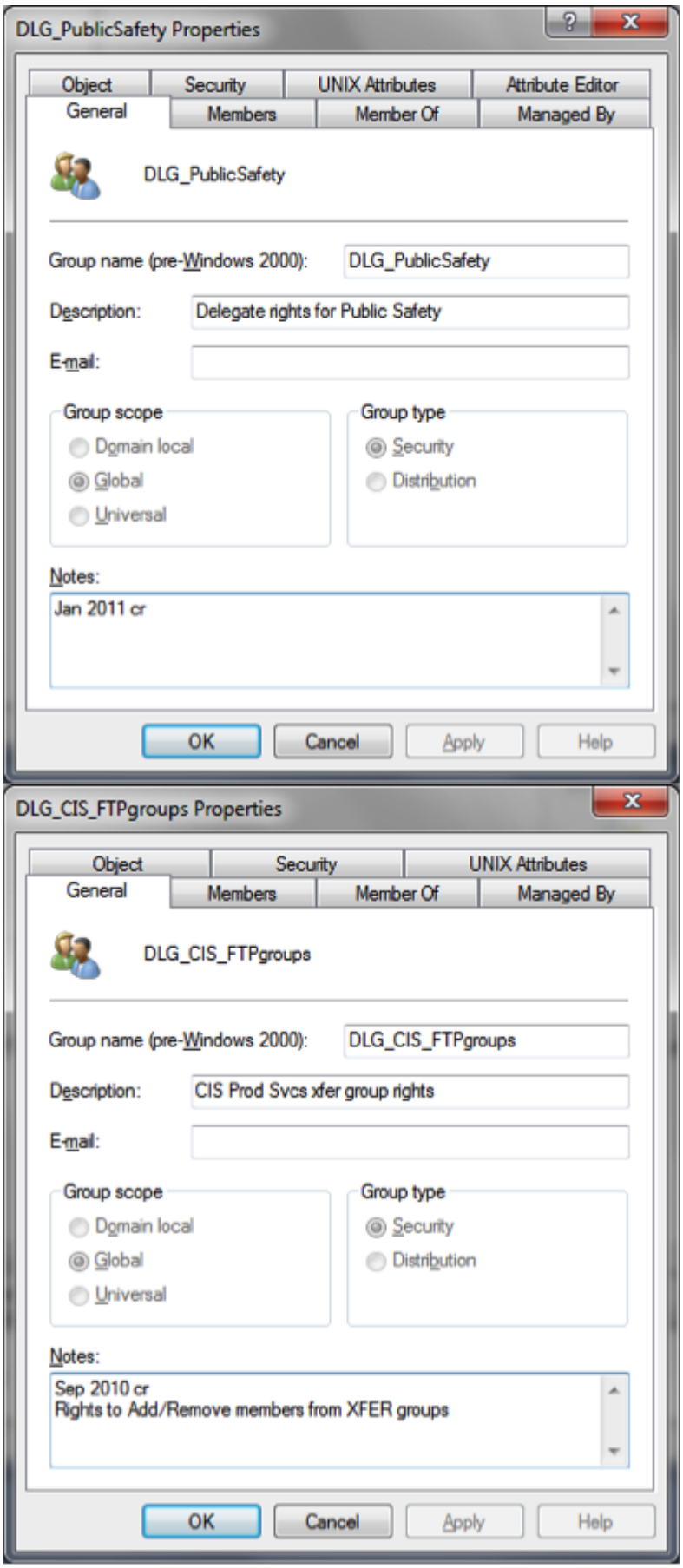
a. DLG stands for Delegate

b. Used for granting rights on the department OU in AD. The local SysAdmin's adm_userid account is used for the group membership. (The group SEC_dept_Delegates is used to grant access to the files in the department share – see above *). The DLG groups are also used for granting rights to perform specific administrative tasks in AD, e.g., rights to add and remove members from groups for applications for CAP.

c. Syntax = DLG_dept_function (function added for groups with limited rights)

i. The department acronym is placed in the "dept." space, e.g., DLG_CIS_ITSupport or DLG_English

ii. The function of the group is added after the department acronym to annotate groups with limited rights to specific objects or OUs.



iii. Additional information to define the rights granted follows the directory name: e.g., DLG_CIS_FTPgroups. Explicit information on the group's use should also be reflected in the

Description and Notes field of the group object in Active Directory (AD).

d. Groups are located in the InfrastructureSystems OU: AD.Brown.Edu/InfrastructureSystems/Infrastructure_Groups/DelegateGroups/DLG_Admissions. Both HD2 and CAP have been given rights to this OU to add and remove members for the groups.

e. If the delegated administrator is a local department administrator with AD access they should have an adm_userid account created to use rather than using their personal userid: e.g., DLG_PublicSafety – group member is adm_hpedward. This insures that the person is aware of the elevated privileges they are using while working in AD.

PRT_

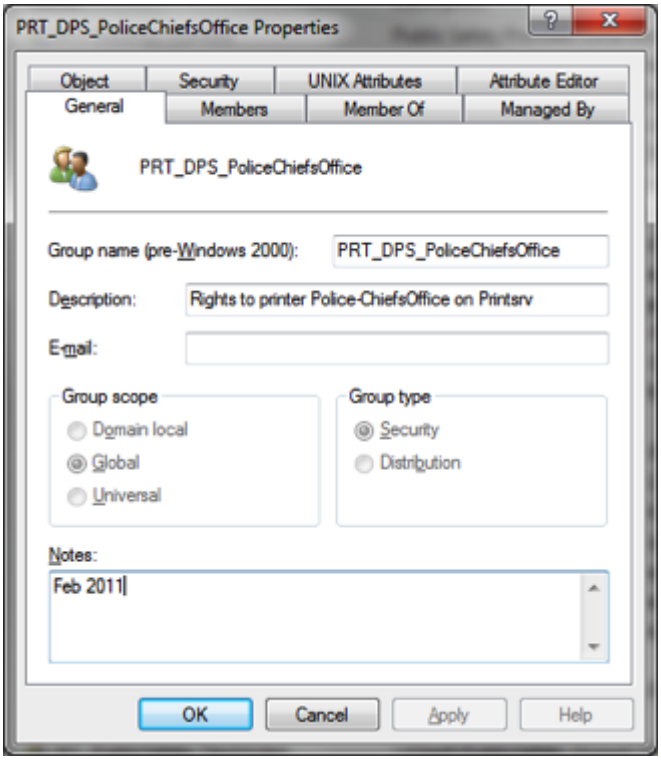
a. PRT stands for Printer

b. Used to lock down access to a printer located on the CIS print servers

c. Syntax = PRT_dept_PrinterName

i. The department acronym is placed in the “dept.” space

ii. The printer name the group is used to lock down follows the dept. acronym.



d. Groups are located in the department OU under deptGroups: e.g., AD.Brown.Edu/Departments/Public Safety/PublicSafetyGroups

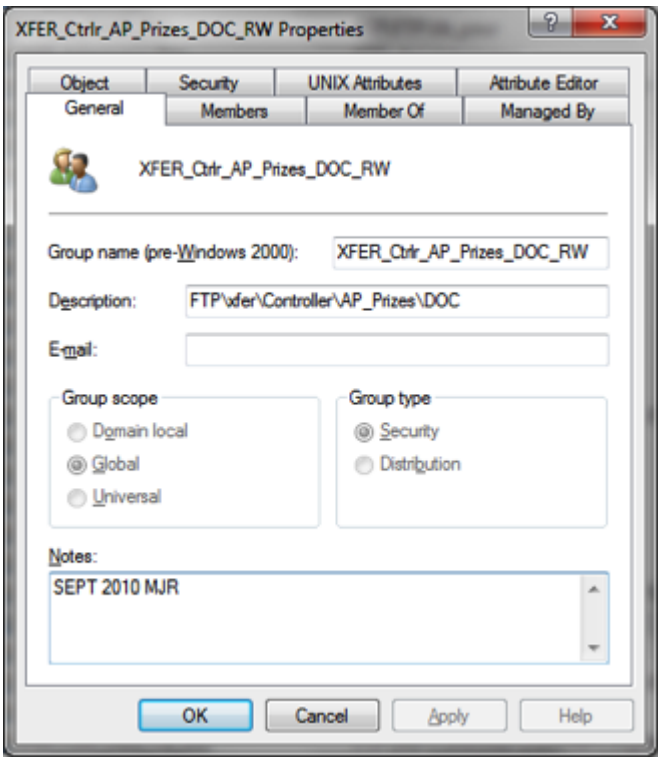
XFER_

a. XFER stands for Transfer

b. Used to grant rights to directories in the Production Services XFER directory and rights to the FTP server.

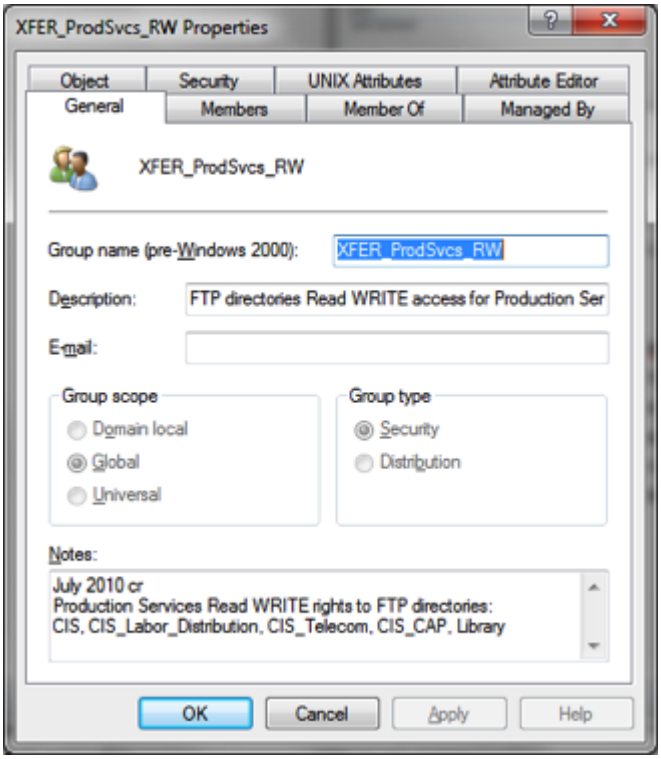
c. Syntax = XFER_DirectoryStructure

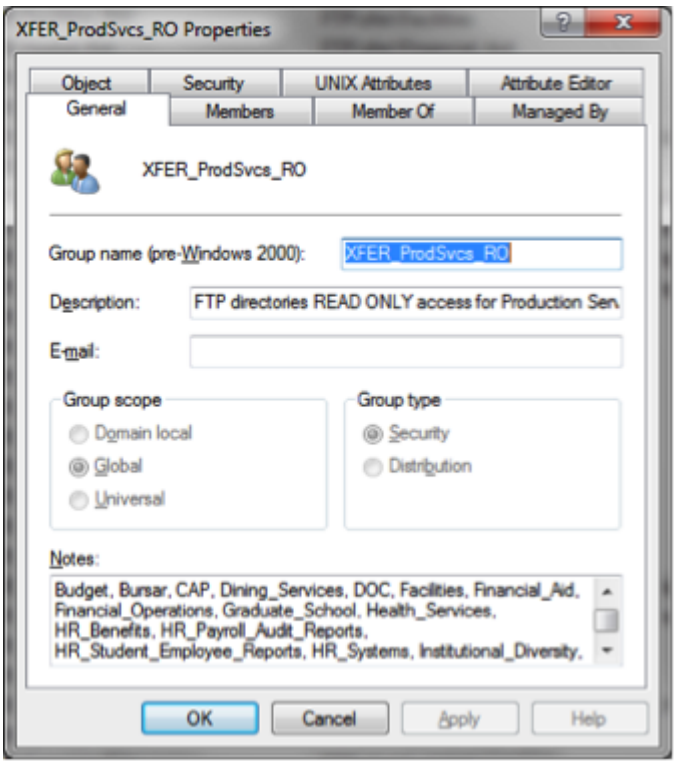
i. The group Description contains the full path of the directory it gives access to.



ii. There are some directories having Read ONLY and Read Write groups. These are annotated by the suffix _RO or _RW.

iii. There are Team XFER groups for the DBAs, EAS, and Production Services. These groups have the directories they are granted access to in the Notes field of the group object.





d. Groups are located in the InfrastructureSystems OU inside the Helpdesk_Groups OU under the FTP OU. AD.Brown.Edu/InfrastructureSystems/HelpDesk_Groups/FTP. Production Services, CAP, and ITSC groups have been given the rights to add and remove members from the XFER groups.

e. For rights to the FTP server the XFER (and FTP groups) have all been nested in the group XFER_FTP_AllUsers. It is the XFER_FTP_AllUsers group that gives access to the FTP server. This nesting is done by the Windows group at the time a new directory is created in the XFER and FTP structures.

FTP_

a. FTP stands for File Transfer Protocol (FTP)

b. Used to grant rights to directories in the Departmental FTP directory (NON-Production Services) and rights to the FTP server. This directory structure is separate from the XFER directory structure in use by Production Services for the file transfers. It is strictly used for FTP.

c. Syntax = FTP_DirectoryStructure. The group Description contains the full path of the directory it gives access to.

d. Groups are located in the InfrastructureSystems OU inside the Helpdesk_Groups OU under the FTP OU. AD.Brown.Edu/InfrastructureSystems/HelpDesk_Groups/FTP. Production Services, CAP, and ITSC groups have been given the rights to add and remove members from the XFER groups.

e. For rights to the FTP server the XFER (and FTP groups) have all been nested in the group XFER_FTP_AllUsers. It is the XFER_FTP_AllUsers group that gives access to the FTP server. This nesting is done by the Windows group at the time a new directory is created in the XFER and FTP structures.

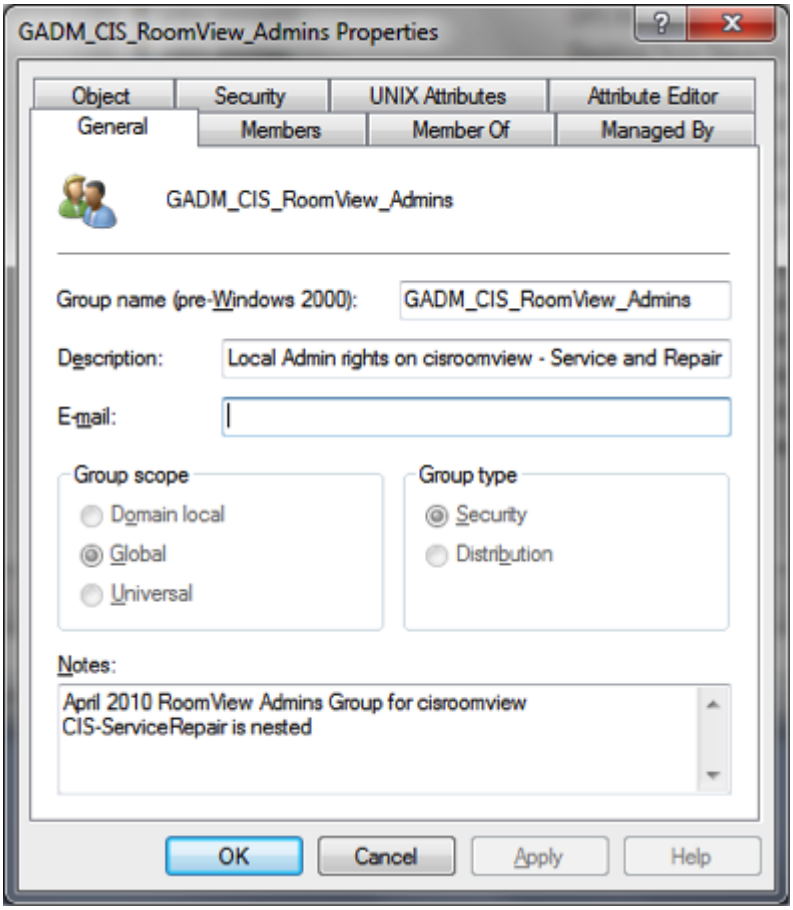
f. The FTP groups are NOT used for the XFER share or directories. They are completely

separate from the production services directory structure.

GADM_

a. GADM stands for Group administrators

b. Used for granting local administrative rights on a server where a server's application is managed by one group and the Windows group is only responsible for the standard maintenance (backups, windows updates).



c. Syntax = GADM_ServerName_Admins

i. ServerName is the name of the server this group has been added to. This group gets nested in the Local Administrators group on the server.

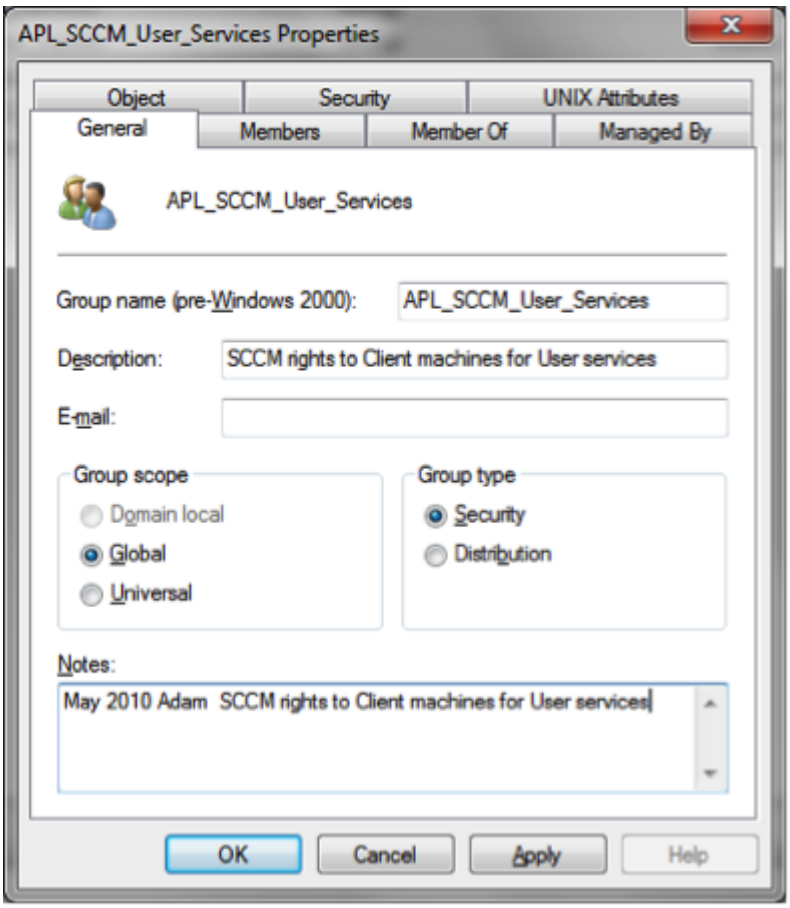
ii. The name of the team and information on the application should be added to the Notes section of the object.

d. Groups are located in the InfrastructureSystems OU. The only team with rights to this OU is the Windows Team.
AD.Brown.Edu/InfrastructureSystems/Infrastructure_Groups/LocalServerGroups

APL_

a. APL stands for Application

b. Used to grant application rights on a server where the Windows group is responsible for the server, including the application installation and configuration, but another group is responsible for the application administration.



c. Syntax = APL_application_AdditionalInfo

i. Application name should follow the APL

ii. Any further information necessary to define the group use should follow the application name; e.g., Names of groups the rights are for, limited rights granted

d. Groups are located in the InfrastructureSystems OU. The only team with rights to this OU is the Windows Team.

RDP_

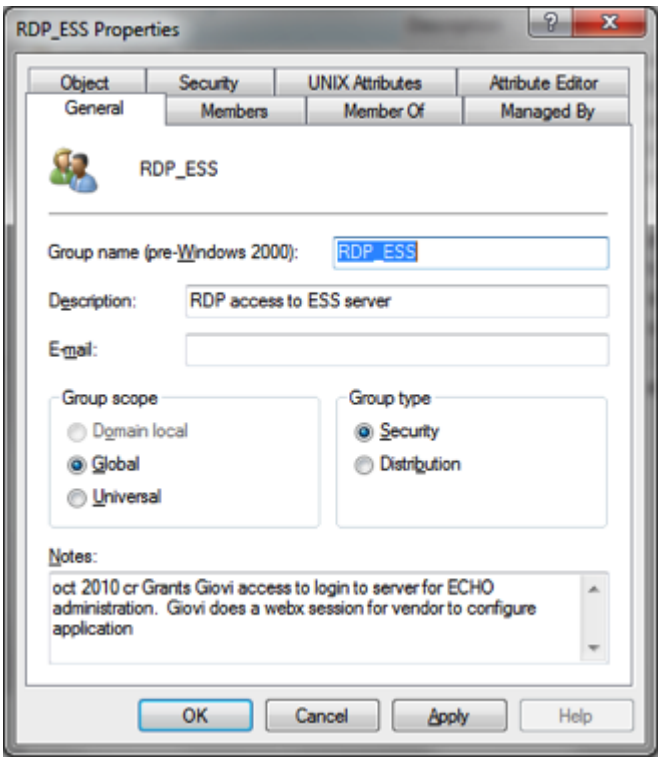
a. Stands for Remote Desktop Protocol (RDP).

b. Used to grant RDP rights to allow logon to a server for application administration on a server. This is used on a server where the Windows group is responsible for the server, but another group is responsible for the application administration (without the need for Local administration rights).

c. Syntax = RDP_ServerName

i. ServerName is the name of the server this group has been added to. This group gets nested in the local Remote Desktop Users group on the server.

ii. The name of the team and information on the application should be added to the Notes section of the object.



d. Groups are located in the InfrastructureSystems OU. The only team with rights to this OU is the Windows Team.

AD.Brown.Edu/InfrastructureSystems/Infrastructure_Groups/LocalServerGroups

VM_

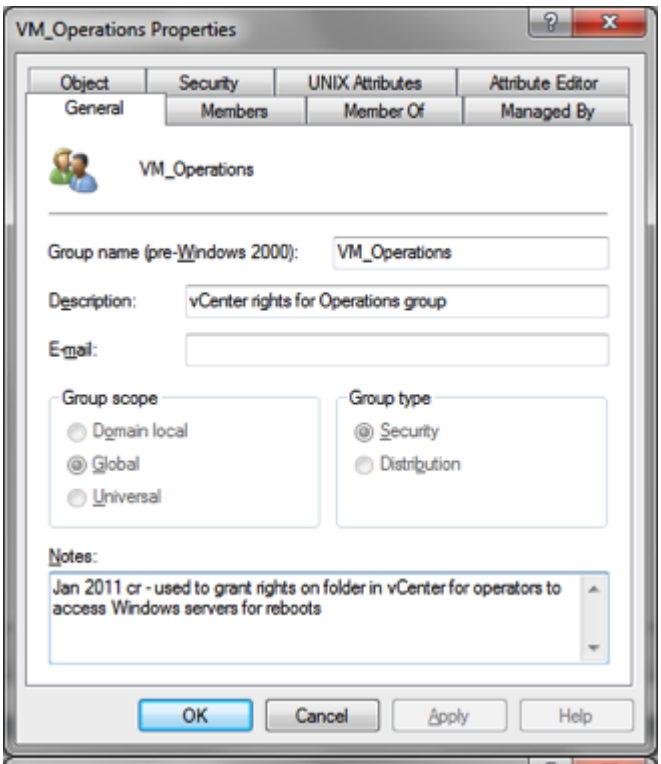
a. VM stands for VMWare

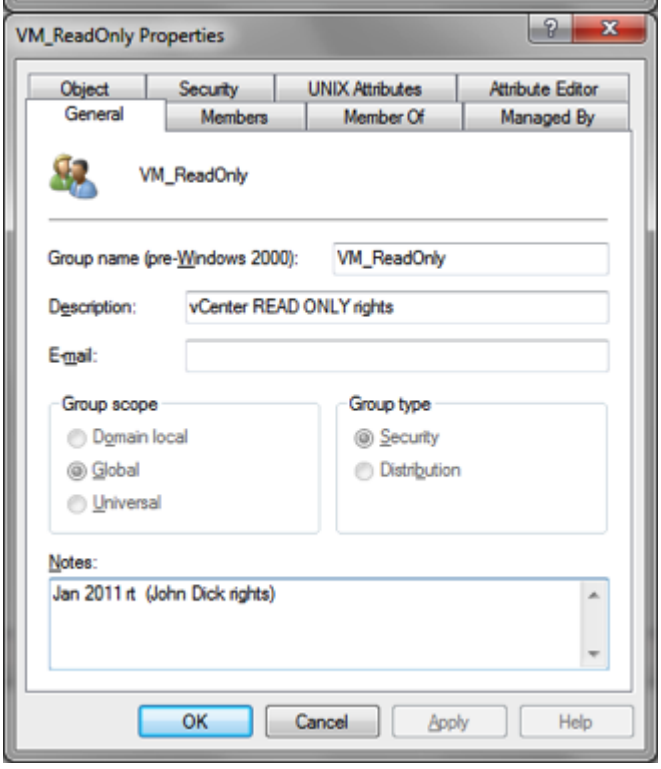
b. Used to grant rights to the vCenter console

c. Syntax = VM_rights_group.

i. Rights are added to the group name to further clarify the group usage

ii. Group is the name of the team the rights have been given to.





d. Groups are located in the InfrastructureSystems OU.
AD.Brown.Edu/InfrastructureSystems/Infrastructure_Groups/VMwareGroups

QAD_

a. QAD is the Active Directory Test domain

b. Used to grant rights on the QAD domain for testing

c. Syntax = QAD_StandardConvention. The standard conventions in use on the AD domain are followed for the QAD groups. The QAD is simply placed in the beginning of the group name to annotate the group is used in the test domain.

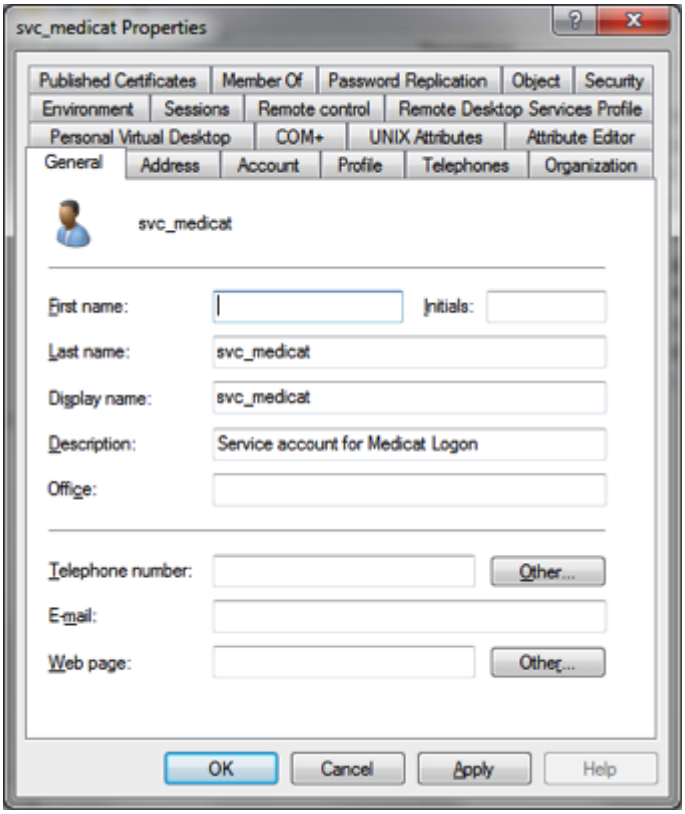
d. Groups are located in the InfrastructureSystems OU.
AD.Brown.Edu/InfrastructureSystems/Infrastructure_Groups/QADtesting
e. The QAD groups are AD domain groups that are used to grant rights in the QAD domain. The groups are located in ad.brown.edu so users can access files in the QAD domain using their AD accounts. There is a one-way trust from QAD to AD.

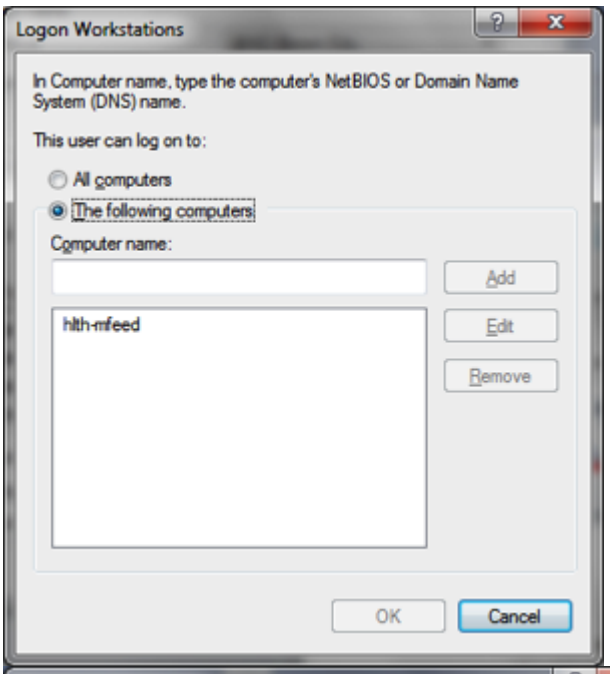
Userid Syntax

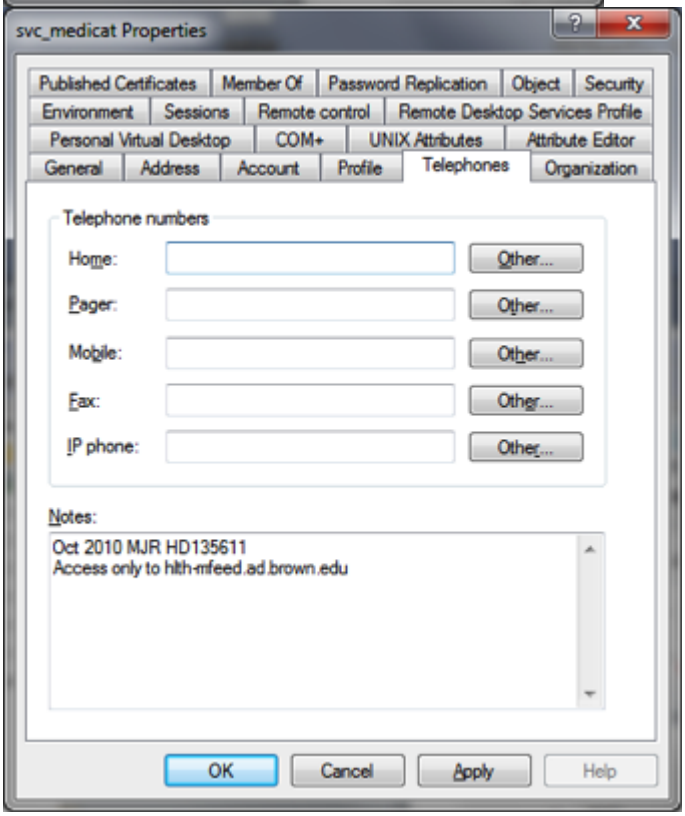
- SVC_
- ADM_
- VEN_

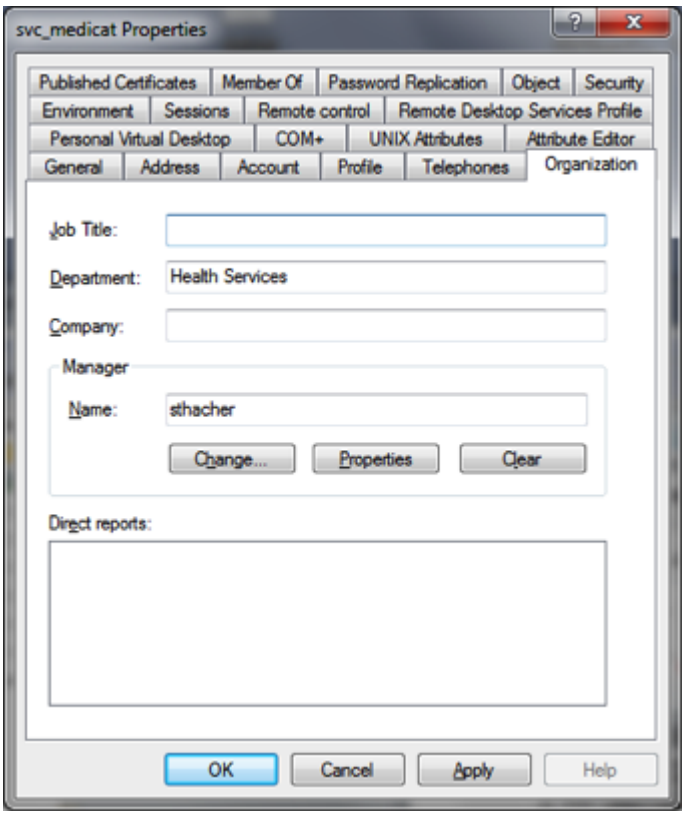
SVC_

a. SVC stands for Service.
b. Used to create user objects for applications and/or services on a server that needs to run as a user.
c. Syntax = SVC_ApplicationName or function.
i. Object name = userid
ii. Description field annotates the application the account is used for
iii. The user object is locked down so it can only logon to the machines it needs (when possible)
iv. If possible, the logon hours are set to reflect when the user object is used (as in the case of a batch job running)
v. The Notes field under Telephones gives additional information about the user object.
vi. The organization tab in the user object should have the department and manager fields filled in.




Logon Workstations
In Computer name, type the computer's NetBIOS or Domain Name System (DNS) name.
This user can log on to:
All computers
The following computers
Computer name:
Add
Edit
Remove
hlth-mfeed
OK
Cancel


svc_medicat Properties
Published Certificates
Member Of
Password Replication
Object
Security
Environment
Sessions
Remote control
Remote Desktop Services Profile
Personal Virtual Desktop
COM+
UNIX Attributes
Attribute Editor
General
Address
Account
Profile
Telephones
Organization
Telephone numbers
Home:
Pager:
Mobile:
Fax:
IP phone:
Other...
Notes:
Oct 2010 MJR HD135611
Access only to hlth-mfeed.ad.brown.edu
OK
Cancel
Apply
Help



d. Groups are located in the InfrastructureSystems OU.

e. If the service account is being used to run an FTP job the account should begin SVC_FTP and be followed by the directory it is used in. This account must be a member of the group XFER_ServiceAccounts for access to the FTP server and share.

ADM_

a. ADM stands for Administrator

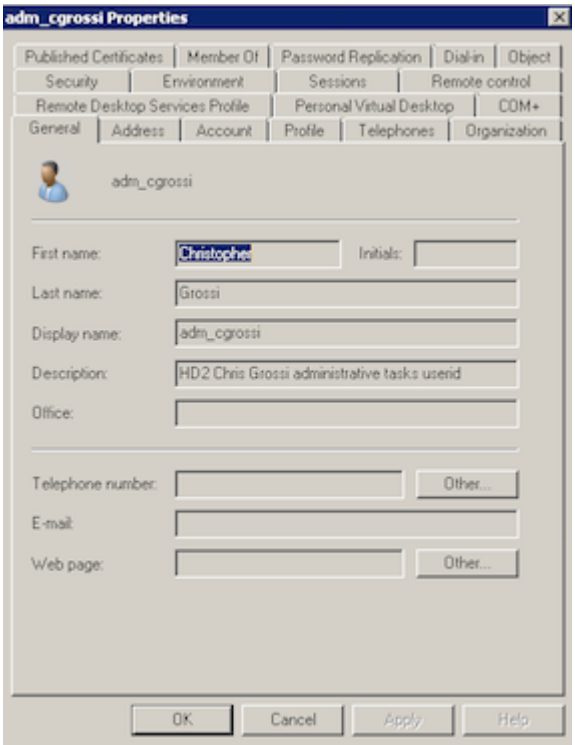
b. Used to give elevated permissions to IT personnel on servers, in AD, etc. This account is used rather than the user's personal userid to perform administrative tasks.

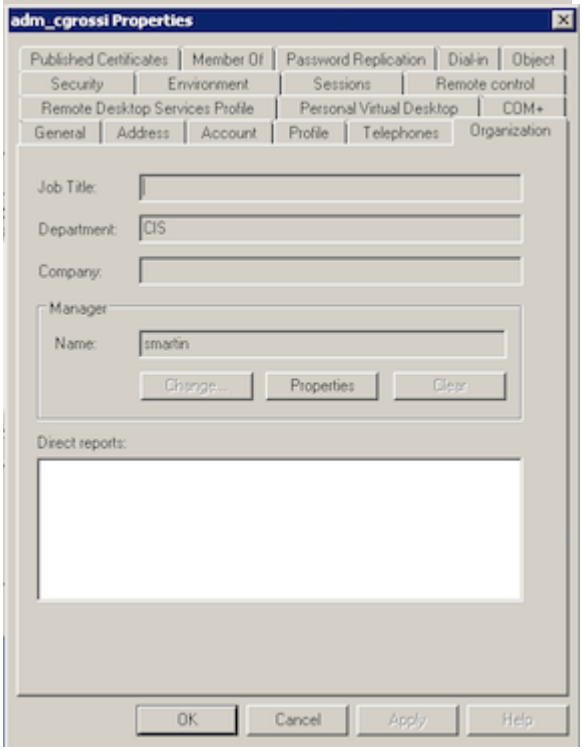
c. Syntax = ADM_PersonalUserid,

i. The user's personal userid follows the adm, e.g., Kristen Soule's personal userid is "ksoule", so her administrative account is "adm_ksoule".

ii. The Description field of the user object should contain the user's department and their name

iii. The organization field of the user object should also reflect the user's department. Any additional information needed should be placed in the Notes field on the Telephone tab.





d. The ADM accounts are located in the InfrastructureSystems OU. The SELF has been granted rights to Change password for their object.

VEN_

a. VEN stands for vendor

b. This account is used to grant vendor support access to a server. This account could be a local account on a server or in AD. If the account is located in AD it is placed into either the GADM or RDP group for the server(s) it supports.

c. Syntax = VEN_CompanyName

i. The Description field of the user object should reflect information about the object use

ii. The vendor’s contact information should be placed in the Telephone number, E-mail, and Web page fields on the General Tab.

iii. The vendor’s address should be placed on the Address Tab.

iv. The account should be locked down so it only has access to the machines it needs to logon to.

v. This account should be disabled when not in use. When the account is enabled a note should be placed with the date in the Notes area.

vi. The department information should be filled in on the Organization Tab

vii. A manager should be assigned and the Department information should be filled in on the Organization Tab.

d. The VEN accounts are located in the InfrastructureSystems OU.