

AUB Enabled Desktop Environment

(AUBede)

User Manual 2.2

Prepared By: Samih Ajrouch
Approved By: Rim Kadi

*Published by the American University of Beirut
Computing and Networking Services
Beirut, Lebanon*

©AUB. All rights reserved. No part of this document may be reproduced or copied in any form or by any means (graphic electronic or mechanical, including photocopying) recording taping or information retrieval systems without express written permission from the American University of Beirut.

Furthermore, no part of this document may be distributed or shown to persons, or organizations other than those authorized by the American University of Beirut.

The information in this document pertains to the Enabled Desktop Environment plans for the American University of Beirut and is to be treated as confidential except where officially issued by the American University of Beirut for distribution.

Please direct questions or comments about this document to the assigned University representative.

Revision and Signoff Sheet

Change Record

Date	Author	Version	Change	Reference
01/08/2007	Samih Ajrouch	Prerelease 2.0	Updates and new additions to Rev. 1.0	AUBede Manual for sys admins ver 1 2.doc
07/08/2007	Rim Kadi	Prerelease 2.0r	Review and editing	AUBede Manual for sys admins ver 1 2R *.docx
13/08/2007	Samih Ajrouch	Prerelease 2.0	Review and editing	AUBede Manual for sys admins ver 2.2.doc

Document Reviewed and Approved by:

<i>Name</i>	<i>Date reviewed</i>
-------------	----------------------

Samih Ajrouch, CNS

Rim Kadi, CNS

TABLE OF CONTENTS

1	INTRODUCTION	6
2	COMPUTER ROLES	6
2.1	DEPARTMENT COMPUTERS:	6
2.2	LAB COMPUTERS:	7
2.3	KIOSK COMPUTERS:	7
3	JOINED, NOT JOINED AND MIGRATED COMPUTERS	7
3.1	NOT JOINED TO THE DOMAIN:	8
3.2	JOINED TO DOMAIN:	8
3.3	MIGRATED:.....	8
4	DEPARTMENTAL ORGANIZATIONAL UNITS	8
4.1	DEPARTMENT ORGANIZATIONAL UNIT.....	8
4.2	DELEGATING PERMISSIONS ON A DEPARTMENT OU	11
4.3	CREATING GROUP POLICIES ON THE NEWLY CREATED OR EXISTING OUS	15
4.4	CREATING THE DEPARTMENTAL “AUTOMATION” FOLDER.....	16
4.5	RUNNING THE PCCREATION/MIGRATION WEB FORM	16
4.6	MOVING ALREADY MIGRATED COMPUTERS	21
4.7	DISJOINING/DELETING DEPARTMENT COMPUTERS	21
5	LAB ORGANIZATIONAL UNITS.....	22
5.1	REQUESTING AN ORGANIZATIONAL UNIT	22
5.2	DELEGATING PERMISSIONS ON THE NEW REQUESTED OU	22
5.3	CREATING GROUP POLICIES ON THE NEWLY CREATED OUS	22
5.4	CREATING THE LAB “AUTOMATION” FOLDER	23
5.5	RUNNING THE PCCREATION/MIGRATION WEB FORM	24
5.6	FOR ALREADY JOINED COMPUTERS (WITHIN A DEPARTMENT)	25
5.7	FOR NEW COMPUTERS.....	25
5.8	RESULTS AND EFFECTS:.....	25
5.9	DISJOINING/DELETING LAB COMPUTERS.....	26
6	KIOSK ORGANIZATIONAL UNITS	26
6.1	RUNNING THE PCCREATION/MIGRATION WEB FORM	26
6.2	FOR NEW OR NON-MIGRATED COMPUTERS.....	27
6.3	IN ACTIVE DIRECTORY:	27
6.4	IN DFS:.....	28
6.5	AT COMPUTER STARTUP:.....	28
6.6	MOVING ALREADY MIGRATED COMPUTERS	29
6.7	DISJOINING/DELETING KIOSK COMPUTERS.....	29
6.8	COMMON SERVICES.....	29
6.9	SPECIAL MAPPED NETWORK DRIVES	32
6.10	START MENU REDIRECTION	33
7	DEPARTMENTAL SECURITY GROUPS	34
8	DEPARTMENTAL SERVERS.....	35
9	SETTINGS FOR PUBLIC LABS COMPUTERS	35
9.1	WINDOWS DISK PROTECTION:.....	35
9.2	PREPARING THE HARD DISK FOR THE WINDOWS DISK PARTITION:	37

9.3	PLACING EVENT LOGS ON A PERSISTENT PARTITION	38
9.4	DISABLING SYSTEM HIBERNATION	39
9.5	WDP AUB SETTINGS:	39
10	TEST ENVIRONMENT.....	40
11	RESTORING OBJECTS.....	40
APPENDIX A	41

1 Introduction

This document is intended to provide departmental system administrators with the operational guidelines to manage and maintain Active Directory objects and network resources in their department's Organizational Units¹ (OUs) under the AUBede framework.

Such system administrators are typically in charge of managing computing resources and personal computers used by a department staff, faculty and/ or students. This manual outlines the AUBede standard operation procedures of relevance. For further details and an overview of the AUBede design, the reader may refer to the AUBede Blueprint.

Applicable Policies

This AUBede Blueprint document is based on the following policies:

- [Policy on privileged Access](#) - pdf format
- [AUBnet accounts and email policies](#) - pdf format
- [AUBnet Code of Conduct](#)
- [AUBnet Minimal Data Backup Policy](#)
- [IT Management Principles, Policies and Guidelines](#) - pdf format
- [AUBede Baseline Configuration](#) (in progress)

2 Computer Roles

2.1 Department Computers:

The AUBede framework identifies a “Department Computer” role by a group of configuration settings. A “Department Computer” is a machine that is characterized by:

- A computer object name *<PCName>* that is determined according to the AUBede [\[Naming Convention\]](#)², by the department 3 letter abbreviation, the AUB barcode number followed by a “D”.

¹ For a definition of Organizational Unit (OU), please refer to the AUBede Blueprint or http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/deploy/dgbd_ads_dwv.msp?mfr=true

² The AUBede Naming Convention can be found in the AUBede Technical Configuration guide.

- 3 associated user groups with Administrator, “Power User” or Logon privileges
- One main user (usually either a staff or faculty member) at all times, typically granted Logon privileges and exceptionally “Power User” privileges.

2.2 Lab computers:

“Lab Computers” are defined as a collection of computers to be used by a group of users interchangeably and indiscriminately. A “Lab Computer” is a machine that is characterized by:

- An object name <PCName> that is determined according to the AUBede [[Naming Convention](#)]³, by the lab 3 letter abbreviation, the AUB barcode number followed by a “L”.

2.3 Kiosk computers:

“Kiosk Computers” are PCs located in public areas where an “Autologon” <Kiosk User> is the only user allowed to logon to the PC and only a restricted set of applications is accessible. These PCs only operate in kiosk mode. A “Kiosk Computer” is a machine that is characterized by:

- An object name <PCName> that is determined according to the AUBede [[Naming Convention](#)]⁴, by the department 3 letter abbreviation, the AUB barcode number followed by a “K”.
- 3 associated user groups with “Administrator”, “Power User” or “Logon” privileges
- One main user (usually either a staff or faculty member) at all times, typically granted “Logon” privileges and exceptionally “Power User” privileges.

3 Joined, Not Joined and Migrated Computers

A personal computer at AUB or AUBMC can be in any of the following states in relation to AUBede and its associated Active Directory “[win2k.aub.edu.lb](#)”:

³ The AUBede Naming Convention can be found in the AUBede Technical Configuration guide.

⁴ The AUBede Naming Convention can be found in the AUBede Technical Configuration guide.

3.1 Not joined to the Domain:

The computer is still member of a workgroup or of a domain other than the “*win2k.aub.edu.lb*” and will be joined to the domain.

3.2 Joined to Domain:

A “Departmental Administrator” or “Support Staff” has already joined the computer to the “*win2k.aub.edu.lb*” domain, but it is still not migrated to AUBede. Such computers are not yet migrated to their corresponding department “OU” and do not benefit from the AUBede automation and security policies and settings.

3.3 Migrated:

A migrated Computer is one that is joined to the “*win2k.aub.edu.lb*” domain and has gone through the PCMigration process using the [\[AUBede Administration Portal\]](#) as described below.

Such a computer is now placed in a specific destination “OU” based on its assigned department and role.

4 Departmental Organizational Units

An “OU” is created for every department to allow for an easier administration of the department’s resources under the AUBede framework⁵.

4.1 Department Organizational Unit

If the “Department OU” is not already created, a department’s system administrator has to request an “OU” from an administrator who is delegated the administration of a higher level OU. The higher level “OU Administrator” shall fill a [\[Privileged Access Agreement\]](#) form for the requested “OU” from the [\[AUBede Administration Portal\]](#) Guidelines for filling the form are in [\[Appendix A\]](#) and create the “OU” corresponding to the department’s name following the AUBede [\[Naming Convention\]](#) in addition to the three corresponding groups in Active Directory:

- <OUName>OUAdmins “Domain Local Group”

⁵ For AUBede Active Directory “OU” structure details, please refer to the AUBede Configuration Document.

- *<OName>Admins* (Global group)
- *<OName>Logon* “Domain Local Group”.

These groups will be placed outside the newly created “Department OU” so that the higher level “OU Administrator” can control their memberships.

Example:

To join department A to AUBede, department A’s system administrator requests from a member of *<Departments>OUadmins* to create department A “OU” with the corresponding groups. After the *<Departments>OUadmins* creates the OU, the structure will be as shown in Figure 1.

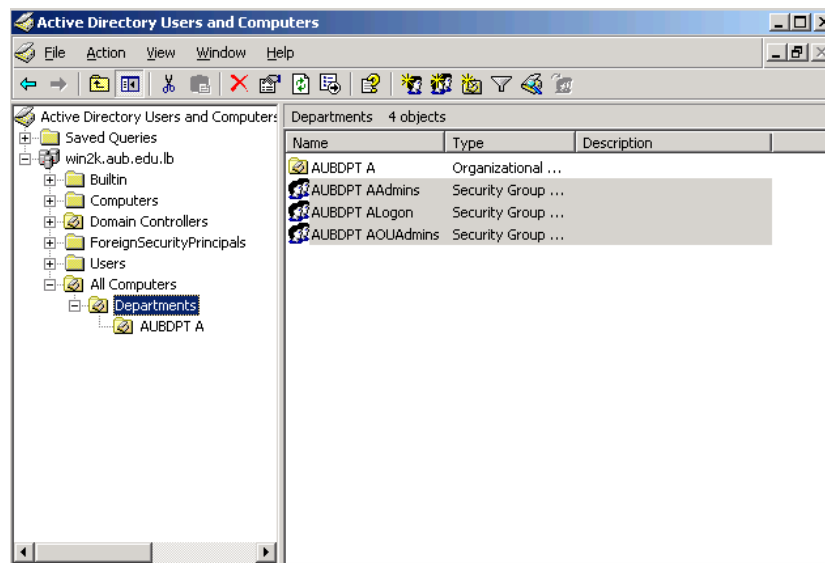


Figure 1: “win2k.aub.edu.lb” departments “OU” structure

After the “OU” and the three corresponding groups are created, the higher level “OU Administrator” will have to fill in the membership of these groups.

- The *<OName>Admins* group SHOULD contain as members higher-level *<OName>admins* group.
- The *<OName>OUAdmins* group SHOULD contain as members higher-level *<ONames>OUadmins* group.
- The *<OName>Logon* group SHOULD contain as members higher-level *<OName>Logon* group.

- Members of **<OUname>OUAdmins** will be the users who will manage the OU, i.e. the system administrator who originally requested the “OU” in addition to other system administrators (if applicable). **<OUname>OUAdmins** will have the right to create/delete/manage computer and group objects, create/delete/manage sub OUs, create/delete group policy objects, and delegate permissions for other users on the sub OUs.
- Members of **<OUname>Admins** will be the users who will have administrative privileges on all computers inside the department OU. Members of this group will be indirectly members of the local “**Administrators**” group of each computer in the department. Members of **<OUname>OUAdmins** may also be members of this group.
- Members of **<OUname>Logon** will be the users and groups who will have the right to logon to all computers in the department.

4.2 Delegating permissions on a department OU

The required delegation permissions need to be set by the higher level “OU Administrator” for the *<OUName>OUAdmins* on their department OU. The higher level “OU Administrator” can run the “Delegation of Control” wizard on a “Department OU” that he/she created (for the previous example, a member of *<Departments>OUAdmins* will run the delegation of control wizard on the *<AUBDPT>OU* to grant permissions to *<AUBDPT>OUAdmins*). At the prompt, the user running the wizard should choose the *<OUName>OUAdmins* group for which he/she will delegate control on the “Department OU” as shown in the **Figure 2**.

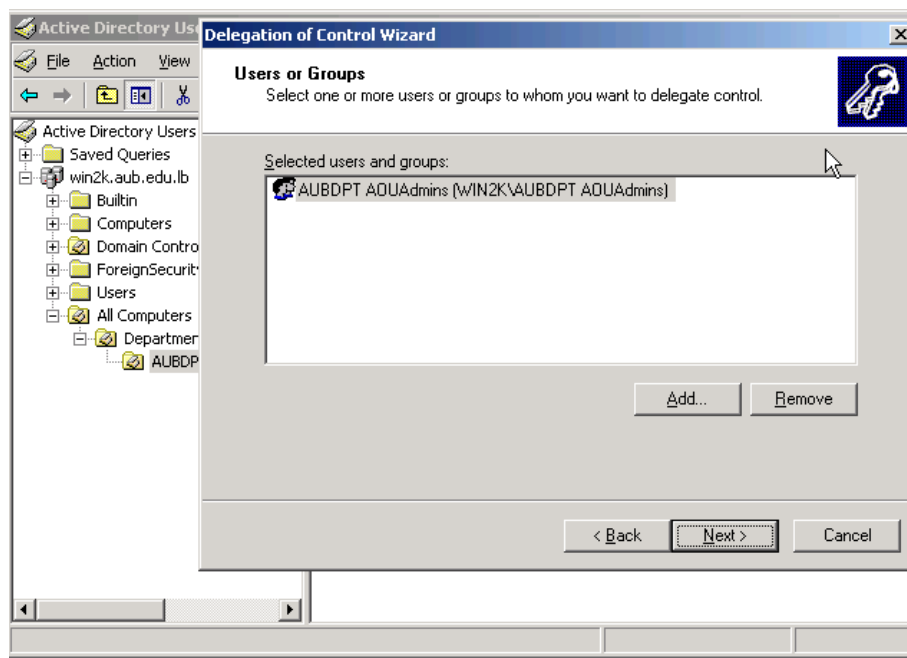


Figure 2: Delegation of Control Wizard (select group)

The next window will prompt the higher level “OU Administrator” to select a delegation task. The custom task option should be selected at this stage as shown in **Figure 3**.

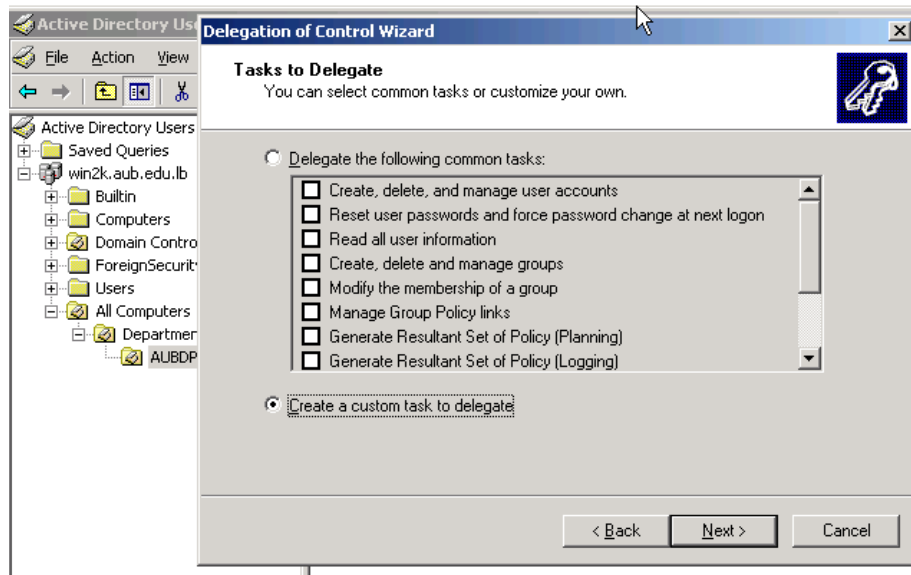


Figure 3: Delegation of Control Wizard (custom task)

In answer to the 'Delegate Control of' option, ***“This folder, existing objects in this folder, and creation of new objects in this folder”*** should be selected as shown in Figure 4.

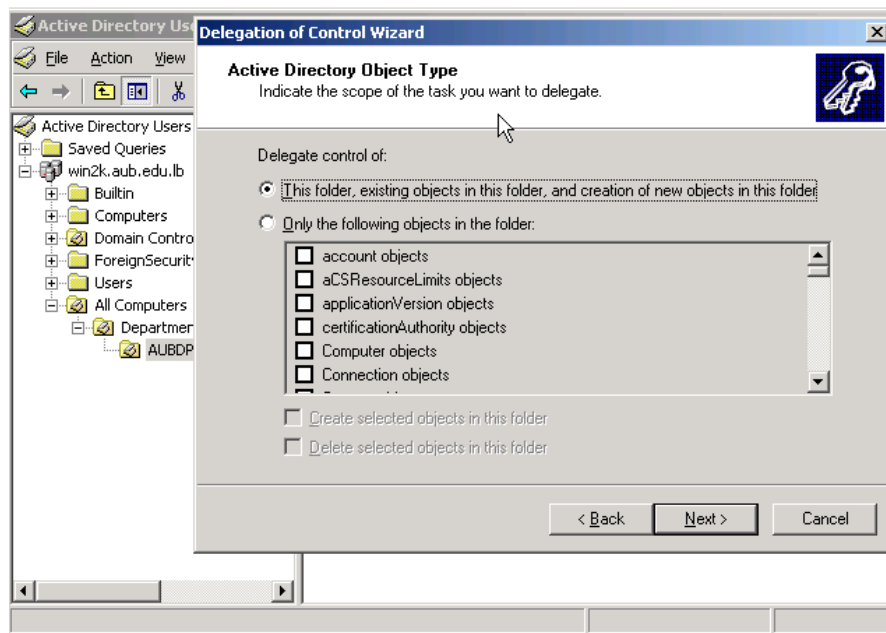


Figure 4: Delegation of Control Wizard (Active directory object type)

Then, the following permissions must be selected:

- Read
- Write
- Read all properties
- Write all properties
- Create computer objects
- Delete computer objects
- Create group objects
- Delete group objects
- Create GroupPolicyContainer objects
- Delete GroupPolicyContainer objects
- Create Organizational Unit objects
- Delete Organizational Unit objects

After completing the above steps, the administrator running the delegation task must run the wizard again to give <OUName>OUAdmins full control on computer objects. On the first page of the delegation of control wizard, the same group is selected as in **Figure 2**. On the next page, also “Create a custom task to delegate” is chosen as in **Figure 3**. On the following page, “Only the following objects in the folder” radio button is selected and then “*computer objects*” and “*group objects*” checkbox is selected as shown in **Figure 5**.

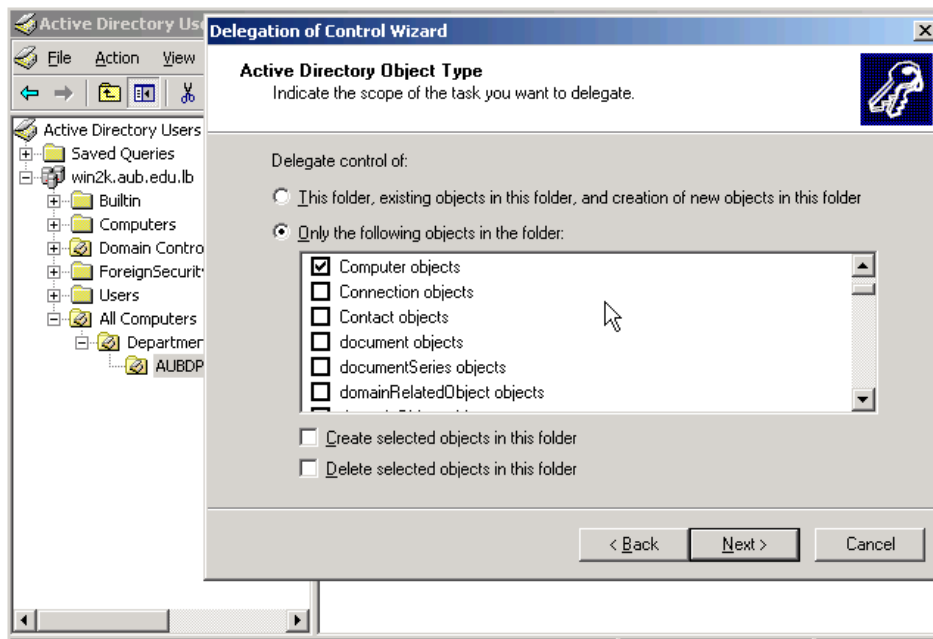


Figure 5: Delegation of Control Wizard (select computer objects)

On the permissions page, select “Full Control” to grant the group `<OUName>OUAdmins` full control on computer and group objects in their “Department OU” as shown in **Figure 6**.

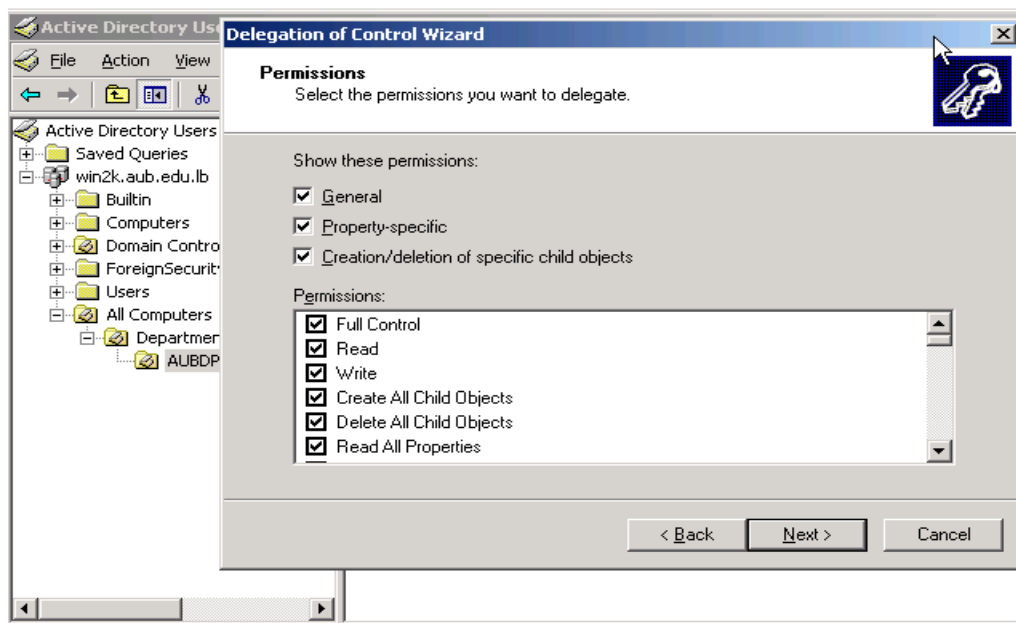


Figure 6: Delegation of Control Wizard (full control on computer objects)

In order for the new *<OUName>OUAdmins* to be able to create group policies on their departments, they must be added to the “Group Policy Creator Owners” group in addition to all previously granted permissions. The higher level “OU Administrator” might not have the permission to add members to “Group Policy Creator Owners” group and the AUBede CNS coordinator shall be contacted for this purpose.

Note:

The permissions delegation process validation is automated by a script that runs **weekly** against all “Departmental OU”s to reset the permission and correct any miss-configured OUs.

4.3 Creating Group Policies on the newly created or existing OUs

Now as the *<OUName>OUAdmins* can create group policies on their OUs, there is one mandatory group policy that shall be created before any computer is migrated to the OU. This group policy defines who will have the right to logon to computers in this department. Thus the department administrator will create this group policy on the new “OU” (for the previous example, a member of the *<Departments>AOUAdmins*” will create the policy on the *<DepartmentOU> OU*).

The configuration of this group policy will be as follows:

Computer Configuration

 Windows Settings

 Security Settings

 Local Policies

 User Rights Assignment

 Allow Logon locally

 Add: win2k\”*Domain Admins*”,
win2k*<OUName>Logon*, win2k*<OUName>Admins*, administrators, “*logonlocally*”.

The *<OUName>OUAdmins* can later create additional group policies.

Notes:

1. Any member of *<OUName>OUAdmins* who creates a Group Policy on the department’s “OU” shall grant the *<OUName>OUAdmins* Full Control permission on this Group Policy.
2. [\[Naming Convention\]](#) should be strictly followed when creating new group policies. Group policies not complying with the standard naming convention will be automatically deleted as part of the regular AUBede maintenance. For further details on the [\[Naming Convention\]](#), please refer to the AUBede Technical Configuration document.

4.4 Creating the Departmental “Automation” folder

For every department joining AUBede, the “OU Administrator” can optionally request a folder under the [\\win2k.aub.edu.lb/files/automation](http://win2k.aub.edu.lb/files/automation) directory. This folder will be named by the department’s name (ex: AUBDPT A) and will be used by the department’s administrator to:

- Create and store automation scripts (such as the printers’ scripts)
- Store automation utilities that should be deployed on the “OU” computers
- Store start menu shortcuts to which users’ start menus shall be redirected
- Other automation procedures

The administrator of the new “OU” should request the automation folder if and when needed from the higher level “OU Administrator”. This “Administrator” will:

- Create the folder holding the new *<OUName>*. This folder will be created inside [\\win2k.aub.edu.lb/files/automation/<higherlevelOUfolder>](http://win2k.aub.edu.lb/files/automation/<higherlevelOUfolder>).
- Grant the lower level *<OUName>OUAdmins* administrator the “Modify” permission on this folder.

4.5 Running the PCCreation/Migration Web form

To move or join new computers to a department OU, a web form has been developed for system administrators to use. This web form will move already joined computers to the correct department, or create computer objects for computers that will be joined. It will also create groups and scripts required to migrate the computer. The system administrator must contact AUBede CNS coordinator in order to be added to a special group, “PCCreators”, allowed to use this web form.

Note:

The PCCreation/Migration web form **SHOULD BE USED** at all times to join a PC and place it in the department “OU” without missing any of the required tasks associated with the creation of a new PC object (such as the creation of the 3 associated groups and initial migration scripts).

The web form is located at the following address: <http://aubede.aub.edu.lb> in the “**PCCreation**” section and it will require user authentication. The user will have to enter [win2k\<username>](#) and the corresponding password to be authenticated. After the user is authenticated the procedure shown in

Figure 7 takes place:

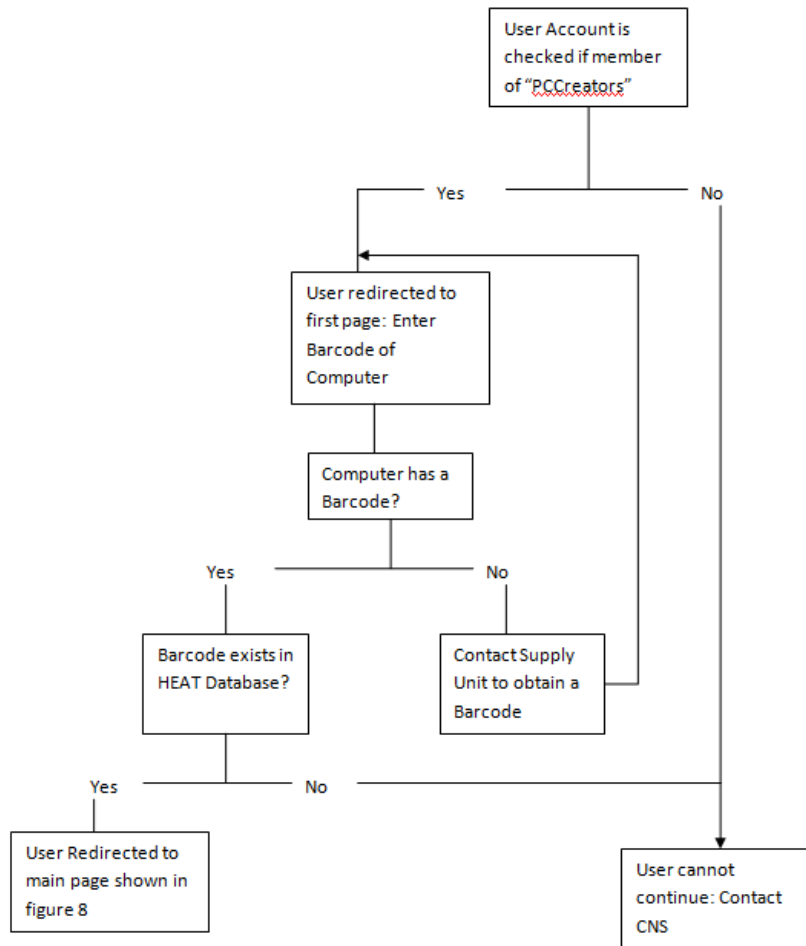


Figure 7: Procedure after authenticating to PCCreation/migration web form

AUBede Enhanced Desktop Environment
American University of Beirut

Authenticated User: RIM KADI

[Back To Menu](#) [Help](#) [Log out](#)

COMPUTER DETAILS	
Bar Code:	<input type="text" value="adm27035"/> <input type="button" value="Get Info"/>
Computer Name:	<input type="text" value="vdklabd12-vdk"/>
Parent Department:	<input type="text" value="PC SUPPORT UNIT"/>
Location:	<input type="radio"/> Medical Center <input type="radio"/> Campus
Computer Type:	<input type="radio"/> Lab Computer <input checked="" type="radio"/> Department Computer <input type="radio"/> Kiosk
Computer Organization Unit:	<input type="text"/> ...
Joined to Domain?:	<input type="radio"/> Yes <input checked="" type="radio"/> No
UserName	<input type="text"/> <input type="button" value="Check"/> <input type="radio"/> Power User <input checked="" type="radio"/> Normal User
Site:	<input type="text" value="Site-ARH"/> ▼
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

Last updated on July 14, 2004
 AUBede Enhanced Desktop Environment - American University of Beirut
 Website created by: Computing and Networking Services

Figure 8: PCCreation/Migration Web Form for Department computers

4.5.1 For new or non-migrated department computers

Fill in the following information

- *Computer name:* As it will be created in Active Directory
- *Location:* Medical Center or Campus
- *Computer Type:* In this case it is a “Department Computer”. Department computers are usually used by a specific and known staff or faculty member. Two other options are also available and will be discussed in later sections: Lab computer and kiosk.
- *Computer Organizational OU:* This is the “Department OU” in which the computer object should be placed

- *Joined to Domain*: If the computer is already joined choose Yes otherwise choose No.
- *Username*: Enter the username of the user who will use this computer.
- *User Type*: Choose whether this user will be a “Power User” on the computer or a normal user.
- *Site*: Select the site (domain controller) where changes will first take effect before being replicated to other sites (domain controllers).

After the system administrator submits the form the following process takes place:

- In HEAT Database:
 - The computer barcode is used to locate the computer in the database
 - For every barcode the following fields are retrieved and updated:
 - Computer name
 - Computer user
 - Department
 - Type of computer user (**Normal User** or “**Power User**”)
- In Active Directory:
 - If the computer is not already joined, the computer object will be created in the “Department OU” chosen from the web form. If the computer was already joined to the domain, the computer object will be moved to the “Department OU” specified in the web form.
 - Three global groups are created in the same “Department OU” where the computer object is created. These groups are: *<Computername>Administrators*, *<Computername>Powerusers*, and *<Computername>Logon*.
 - *<OUName>Admins* will be added to the group *<Computername>Administrators*.
 - The user account of the user who will use the computer (filled in the web form) will be added to the *<Computername>Logon* and to the *<Computername>Powerusers* groups (if requested).
 - The *<Computername>Administrators* and *<Computername>Powerusers* groups will be added to the *<Computername>Logon* group.
- In DFS:

In `\\win2k.aub.edu.lb\files\automation\addstaffpc`, a folder holding the computer name will be created. Inside this folder a file named `runonce.bat` is created. This file contains the configuration commands that should be executed the first time the computer starts up after the web form has been filled and submitted.

- At Computer Startup:

When the computer starts up for the first time after the web form has been filled and submitted, the following steps take place automatically:

- All members of the local administrators group of the computer are removed except the “Administrator” account and the “*Domain Admins*” group.
- A local group named “*logonlocally*” will be created on the computer.
- The domain group `<Computername>Logon` will be added to the local group “logonlocally”
- The domain group `<Computername>Administrators` will be added to the local computer group “*Administrators*”.
- The domain group `<Computername>Powerusers` will be added to the local group “power user”.
- A local group “*denynetwork*” will be created and the domain group `<Computername>Administrators` will be added to this group
- `Runonce.bat` inside “`\\win2k.aub.edu.lb\files\automation\addstaffpc`” file is deleted

4.5.2 Results and Effects:

- Allowing users to logon to a “Department Computer”: The group policy “Logon rights to `<Department>OUnam`” on each “Department OU” grants the logon right to the local group “logonlocally” group of each computer. At the first computer startup, the domain group `<Computername>Logon` is added to the “*logonlocally*” group. Thus, to grant any user the logon right to a specific “Department Computer”, his/her user account must be added to the `<Computername>Logon` domain group from Active Directory.
- Giving users administrative rights on a “Department Computer”: The domain group `<Computername>Administrators` is put member of the local “Administrators” group of the computer. Thus, members of the domain group `<Computername>Administrators` have administrative privileges on the “Department Computer”. Every user who needs such privileges must be added to this domain group. The same process applies for the domain group `<Computername>Administrators`

- Denied network access: Members of the domain group <Computername>Administrators are put members of the local group “Denynetwork”. There is a group policy on all “Department Computers” that denies this group the access to the computer from the network.

4.6 Moving Already Migrated Computers

To move already migrated computers from one department to another or from one user to another within the same department, the computer must be disjoined from the domain by using the “PCDeletion” web form as detailed in the Disjoining/Deleting Department Computers section below. The same computer must be joined again using the “PCCreation” web form.

4.7 Disjoining/Deleting Department Computers

Whenever a computer is to be renamed, moved to another department, moved to another user within the same department, or disjoined from the domain, the “PCDeletion” web form must be used.

Using the “PCDeletion” webform guarantees the proper and complete AD object deprovisioning process.

This web form is part of AUBede administration portal: “<http://aubede.aub.edu.lb>” under the “PCDeletion” section.

Only members of the “PCDeletors” domain group are allowed to use this web form. Thus after a user is authenticated, his/her account is checked against the “PCDeletors” membership. If the user is not member of this group, he/she cannot continue and must contact CNS AUBede coordinator; otherwise he/she is redirected to the next page. The System administrator will have to enter the computer barcode and/or computer name. Then upon submission of the web form, the following procedure takes place:

Since this is a “Department Computer”:

- The computer account will be deleted from Active Directory
- The corresponding groups will be deleted from Active Directory
- The automation folder will be deleted from [\\win2k.aub.edu.lb/files/automation/addstaffpc](http://win2k.aub.edu.lb/files/automation/addstaffpc)
- The corresponding fields are updated in HEAT database

Because the information in HEAT database must be updated whenever the computer’s attributes are changed, using the “PCDeletion” is mandatory in the case of:

- Renaming a computer

- Moving a computer between departments
- Changing computer primary owners
- Disjoining a computer

5 Lab Organizational Units

5.1 Requesting an organizational unit

The process for requesting an organizational unit for “Lab Computers” is the same as that for department computers. The higher level “OU Administrator” shall create the “OU” with the three groups:

- *<OUname>OUAdmins* “Domain Local Group”: Members should contain groups/users who will administer the lab “OU”
- *<OUname>Admins* “Domain Local Group” – unlike for departments where it was global group): Members should include groups/users who will be members of the local administrators group on each computer in the lab.
- *<OUname>Logon* “Domain Local Group”: Members should include all groups/users who are allowed to logon to these “Lab Computers”

5.2 Delegating permissions on the new requested OU

This is also the same procedure as for department OUs (Please refer to section Delegating permissions on a department OU above).

5.3 Creating Group Policies on the newly created OUs

For lab organizational units, there are **two mandatory group policies** that should be created before any computer is migrated to this “OU”. These two group policies define:

- The users (or groups) that have the right to logon locally to “Lab Computers”.
- The users (or groups) that will be members of the administrators group on “Lab Computers”.

The first group will have the following configuration:

Computer Configuration

Windows Settings

Security Settings

Local Policies

User Rights Assignment

Allow Logon locally

Add: win2k\Domain admins, win2k\<OUname>Logon, win2k\<OUname>Admins, Administrators

The second group policy will define and restrict groups/users who will be members of the local administrators group on each computer in the <OUname> OU. The configuration of this policy is as follows:

Computer configuration

Windows Settings

Security Settings

Restricted Groups

Add group

Write Administrators (without choosing the Browse option)

Members of this group:

Add: Administrator (without choosing the Browse option), Win2k\administrators, and win2k\<OUname>Admins.

The lab administrator can later on create additional Group policies as needed.

Notes:

1. Each member of the <OUname>OUAdmins who creates any group policy shall grant the <OUname>OUAdmins the Full control permission on this Group Policy.
2. [\[Naming convention\]](#) should be strictly followed when creating new group policies. Group policies not complying with the standard naming convention will be automatically deleted as part of the regular AUBede maintenance.
3. For better performance we are disabling the user portion from all GPO's linked to computers object

5.4 Creating the Lab "Automation" folder

This is the same procedure as for department OUs (Please refer to section Creating the Departmental "Automation" folder above).


5.5 Running the PCCreation/Migration Web form

For adding or migrating “Lab Computers”, the PCCreation/Migration web form from the AUBede portal “<http://www.aubede.edu.lb/>” should be used. The user has to be authenticated and should be member of the “PCCreators” group. The barcode of the computer to be created should then be entered. The barcode should already exist in the HEAT database; if the barcode does not exist in the HEAT database, the user cannot continue. If the barcode is found, the system administrator will see the main page as shown in Figure 9 where the following fields have to be entered:

- **<Computer name>**: As it will be created in Active Directory
- **Location**: Medical Center or Campus
- **Computer Type**: In this case it is a lab computer. For a description of Department and Kiosk computers, please refer to the corresponding sections in this document.
- **<Computer Organizational Unit>**: *i.e. the lab “OU” in which the computer object should be created.*
- **Joined to Domain**: If the computer is already joined choose Yes otherwise choose No.
- **Site**: Select the site (domain controller) where changes will first take effect before being replicated to other sites (domain controllers)



AUBede

Enhanced Desktop Environment
American University of Beirut



AUB
American University of Beirut
الجامعة الأمريكية في بيروت

Authenticated User: RIM KADI

 [Back To Menu](#)
 [Help](#)
 [Log out](#)

COMPUTER DETAILS

Bar Code:	<input type="text" value="adm27035"/>	<input type="button" value="Get Info"/>
Computer Name:	<input type="text" value="vdklabd12-vdk"/>	
Parent Department:	<input type="text" value="PC SUPPORT UNIT"/>	
Location:	<input type="radio"/> Medical Center <input type="radio"/> Campus	
Computer Type:	<input checked="" type="radio"/> Lab Computer <input type="radio"/> Department Computer <input type="radio"/> Kiosk	
Computer Organization Unit:	<input type="text"/> ...	
Joined to Domain?:	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Site:	<input type="text" value="Site-ARH"/> ▼	

Last updated on July 14, 2004

[AUBede Enhanced Desktop Environment](#) - [American University of Beirut](#)

Website created by: [Computing and Networking Services](#)

Comments/suggestions/help: aubede@aub.edu.lb

Figure 9: PCCreation/Migration form for Lab Computers

5.6 [For already joined computers \(Within a department\)](#)

For already joined computers, upon web form submission the computer object will be moved to the destination lab “OU” specified in the web form.

5.7 [For New Computers](#)

For computers not yet joined to the domain, upon submission a computer object is created in the destination lab “OU” specified in the web form.

5.8 [Results and Effects:](#)

- Allowing users to logon to “Lab Computers”: Any user who must logon to any of the “Lab Computers” should be put member of the domain group **<OUname>Logon**

- Granting administrative privileges on all “Lab Computers”: Any user who must have administrative privilege on any computer in the lab “OU” should be put member of the domain group <OUname>Admins
- Granting “OU” administrative privileges: Any user who should manage an “OU” should be put member of the <OUname>OUAdmins.

5.9 Disjoining/Deleting Lab Computers

As for department computers, for every lab computer that will be **renamed, moved to another department, disjoined from domain, the “PCDeletion” web form must be used.** The process will delete the computer object from active directory and update all necessary fields.

The user running this form must be member of the “PCDeletors” domain group.

6 Kiosk Organizational Units

“Kiosk Computers” are public computers used in different departments where only one user is always logged on to the machine. This user is called the “Kiosk user”. The windows interface on “Kiosk Computers” is customized to restrict users’ access to a limited set of applications.

6.1 Running the PCcreation/Migration Web form


NOTE: The kiosk user must be created in the proper OU, before the web form is used. A system administrator can request the right to create kiosk users for his/her department in certain specific cases (AUBede recommends against the creation of users that are not synchronized with the main HR and students databases). The Organizational Unit that will contain kiosk users is called “*Kiosk Users*” and is located inside the “*AllUsers*” Organizational Unit. The administrator will be notified of what password to choose for kiosk users.

In order to add or migrate a machine to a kiosk machine, the PCCreation/Migration web form must be used by going to <http://aubede.aub.edu.lb>.

After the administrator enters the barcode of the computer, the following fields need to be filled as shown in Figure 10.

- *Computer name:* As it will be created in Active Directory
- *Location:* Medical Center or Campus
- *Computer Type:* In this case it is a kiosk computer. For details about lab and department computers, please check the corresponding sections in this document.

- **“Kiosk User”**: Choose the user account which will always be logged on to the machine. This user will logon automatically (autologon) to the computer when the machine is started.
- **Computer Organizational Unit**: i.e. the “OU” in which the computer object should be created.
- **Joined to Domain**: If the computer is already joined choose Yes otherwise choose No.
- **Site**: Select the site (domain controller) where changes will first take effect before being replicated to other sites (domain controllers)



AUBede Enhanced Desktop Environment
 American University of Beirut

Authenticated User: RIM KADI

[Back To Menu](#) [Help](#) [Log out](#)

COMPUTER DETAILS

Bar Code:

Computer Name:

Parent Department:

Location: Medical Center Campus

Computer Type: Lab Computer Department Computer Kiosk

Kiosk User: ...

Computer Organization Unit: ...

Joined to Domain?: Yes No

Site:

Last updated on July 14, 2004
[AUBede Enhanced Desktop Environment - American University of Beirut](#)
 Website created by: [Computing and Networking Services](#)
 Comments/suggestions/help: aubede@aub.edu.lb

Figure 10: PCCreation/Migration form for Kiosk Computers

6.2 For new or Non-Migrated computers

After submitting the web form for “Kiosk Computers” the following procedure takes place:

6.3 In Active Directory:

- If the computer is not already joined, the computer object will be created in the “OU” chosen from the web form. If the computer was already joined to the domain, the computer object will be moved to the “OU” specified in the web form.

- Three global groups are created in the same “OU” where the computer object is created. These groups are: <Computername>*Administrators*, <Computername>*Powerusers*, and <Computername>*Logon*.
- <OName>*Admins* will be added to the group <Computername>*Administrators*.
- The kiosk user account chosen in the web form will be added to the <Computername>*Logon* domain group.
- The <Computername>*Administrators* and <Computername>*Powerusers* groups will be added to the <Computername>*Logon* group.

6.4 In DFS:

In \\win2k.aub.edu.lb\files\automation\addstaffpc, a folder holding the computer name will be created. Inside this folder a file named runonce.bat will be created. This file contains the configuration commands that should be executed the first time the computer starts up after the web form has been filled and submitted.

6.5 At Computer Startup:

When the computer starts up for the first time after the web form has been filled and submitted, the following steps take place automatically:

- All members of the local administrators group of the computer are removed except the “Administrator” account and the “*Domain Admins*” group.
- A local group named “*logonlocally*” will be created on the computer.
- The domain group <Computername>*Logon* will be added to the local group “*logonlocally*”
- The domain group <Computername>*Administrators* will be added to the local computer group “Administrators”.
- The domain group <Computername>*Powerusers* will be added to the local group “Power User”.
- A local group “*denyntwork*” will be created and the domain group <Computername>*Administrators* will be added to this group
- The kiosk user account is configured for autologon; that is, every time the computer starts up the kiosk user account is automatically logged on.
- Runonce.bat inside \\win2k.aub.edu.lb\files\automation\addstaffpc file is deleted

6.6 Moving Already Migrated Computers

To move already migrated “Kiosk Computers” from one department to another or for changing the kiosk user, the computer must be disjoined from the domain by using the “*PCDeletion*” web form. The computer must be rejoined using the “*PCCreation*” web form.

6.7 Disjoining/Deleting Kiosk Computers

For every kiosk computer to be renamed, moved to another department, or disjoined from the domain, the “*PCDeletion*” web form must be used. The process will delete:

- The computer object and all related groups from active directory,
- The computer folder from DFS
- Updates all necessary fields.

6.8 Common Services

6.8.1 Printing Services

Some departments may install a printer server where different printers are shared. Each printer would be accessible to only a department or a lab. Thus, depending on the lab or department (in other words depending on the OU), the user must have the proper printer added to his profile.

For example, if a user logged on in *<labA>*, *<printerA>* located in *<labA>* should be added. If the same user logged on in *<lab>*, *<printerB>* located in lab should be added and *<printerA>* should be removed, and so on so forth....

With the release of Windows Server 2003 R2, printers are now a lot easier to manage in an enterprise environment. A new tool in R2 that lets you easily manage printers and print servers from a single, central point of management. The Print Management console, once installed on an R2 machine, can then be used to manage print servers running Windows 2000 Server, Windows Server 2003, and Windows Server 2003 R2—and also, to a limited extent, print servers running Windows NT 4.0. To learn more about configuring the windows 2003 R2 print server [[click here](#)]

To automate this process, a procedure has been developed. The procedure is as follows:

- a. Using group policy management console create and link a blank Add printer to *<OUName>PO* to the OU

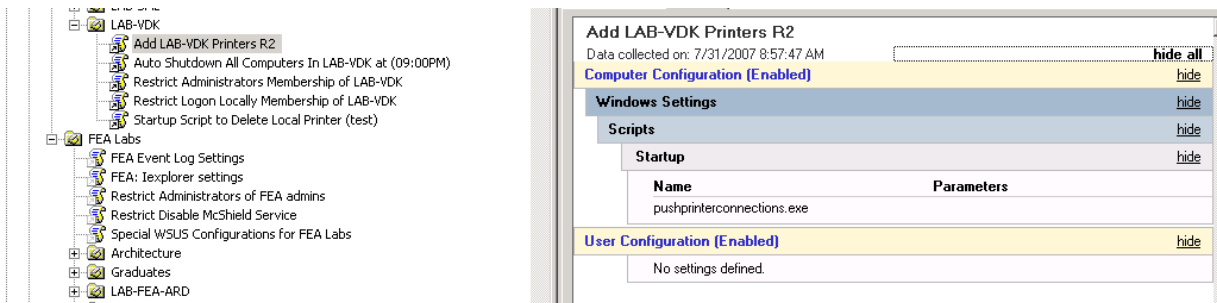


Figure 11: Create GPO to add printer

- b. Open up the Print Management console from the print server and select the printer you wish to deploy
- c. Right-click on *<Printer Name>* and select Deploy with Group Policy from the shortcut menu. This opens the Deploy with *Group Policy* dialog box

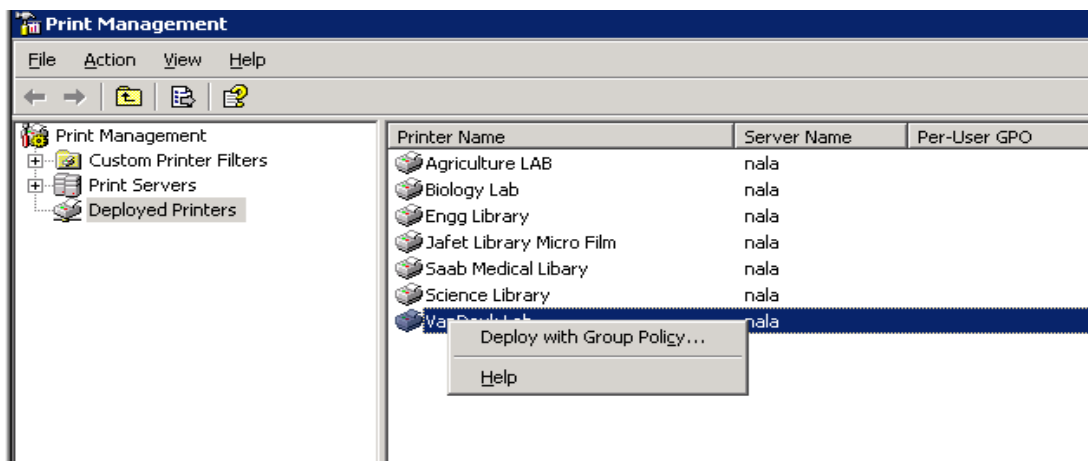


Figure 12: Deploy printer using PM MMC console

- d. Click the Browse button and select the GPO you plan on using to deploy the printer

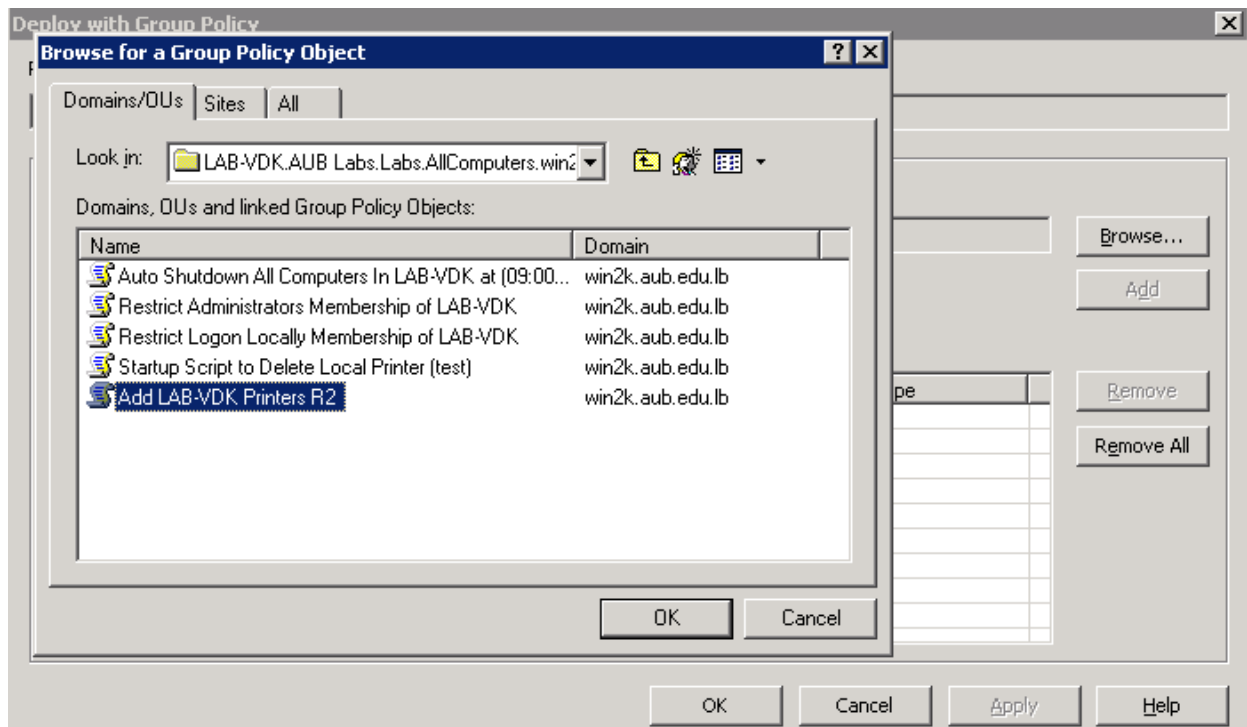


Figure 13: Browse and select GPO

- e. Click OK to return to the Deploy with Group Policy dialog box.
- f. Now click the Add button to add the connection settings

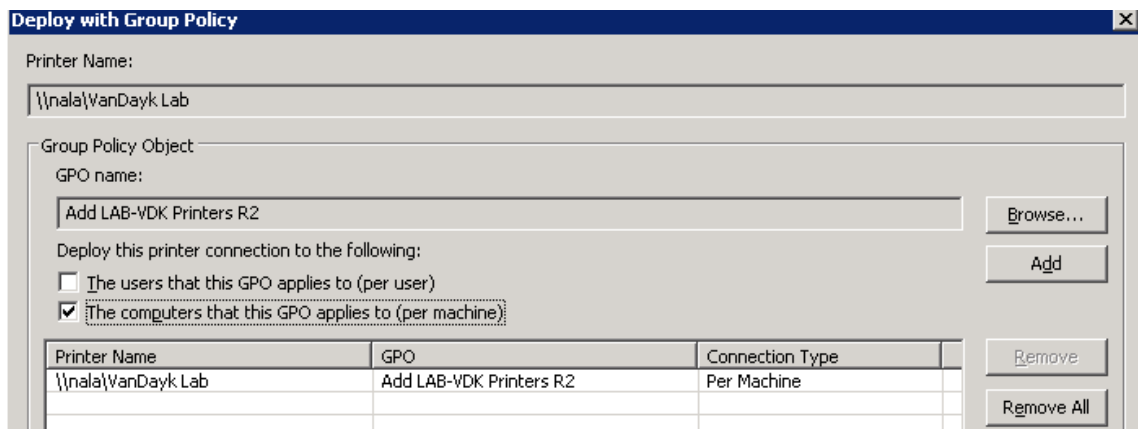


Figure 14: Select type of deployment

- g. Click OK a few times and you'll now see the printer under the list of deployed printers:

The second step is to add PushPrinterConnections.exe to the computers

- h. Open the *Add printer to <OUName>* in the Group Policy Object Editor and navigate to User Configuration, Windows Settings, Scripts (Logon/Logoff)
- i. Right-click on the Logon policy in the right-hand pane and select Properties
- j. Click the Show Files button and copy the file “*PushPrinterConnections.exe*” from the “%Windir%\PMCSnap” folder into the open policy folder
- k. Close the policy folder and click the Add button on Logon Properties, and type PushPrinterConnections.exe into the Script Name field
- l. Click OK a couple of times. The logon script will be displayed in the policy when it has been successfully added

6.9 Special Mapped Network Drives

Each department may require that departmental shared folders be mapped as special network drives to users logging on to department computers. The procedure to be followed for this requirement is as follows:

- Share the necessary folders with proper NTFS and share permissions.
- On the “OU” that contains the computers where the users who will see the mapped drives shall logon, configure the following group policy:

1. **Name:** <Departmentname>: Map folderdescription to network drive

2. **Configuration:**

Computer Configuration

Administrative Templates

System

Group Policy

User group policy loopback processing mode (Enabled: Merge)

User Configuration

Windows Settings

Scripts

Logon

Add logon script named: mapfolderdescription.bat. Use the “net use” command to map the folder to a chose network drive.

Note:

NEVER use the X: or P: drive letters. The X drive points to home or institutional folders of all users at AUB. The P drive is used for the automation process of automatic updates on all computers at AUB.

6.10 Start Menu Redirection

Some administrators require that users in the lab/department share the same start menu. The “Administrator” may choose to personalize the start menu on lab/department computers by hiding some shortcuts and adding others. This is possible using start menu redirection.

The procedure to be followed for start menu redirection is:

- a. In the automation folder corresponding to the department/lab in [\\win2k.aub.edu.lb/files/automation/department/labname](http://win2k.aub.edu.lb/files/automation/department/labname), create a folder named “start menu”.
- b. Grant authenticated users the Read and Execute permission on this folder.
- c. Copy the start menu shortcuts that should appear to users in this lab/department and place them in this folder.
- d. On the department/lab “OU” in Active Directory create the necessary group policy to redirect users’ start menus to this folder.

The configuration of the group policy is:

Computer Configuration

Administrative Templates

System

Group policy

User group policy loopback processing mode (Enabled: Merge)

User Configuration

Windows Settings

Folder Redirection

Start Menu

Redirect to the following location:
<\\win2k.aub.edu.lb\files\automation\...\department\labname\start> menu

7 Departmental Security Groups

Every department will require creating domain security groups in order to set permissions on folders, printers, or other resources. For every department, there will be a special “OU” where the department system “Administrator” will be delegated the right to create groups and modify their memberships.

Notes:

Access to resources should always be granted to domain groups rather than individual users

The location of this “OU” will be as shown in Figure 1.

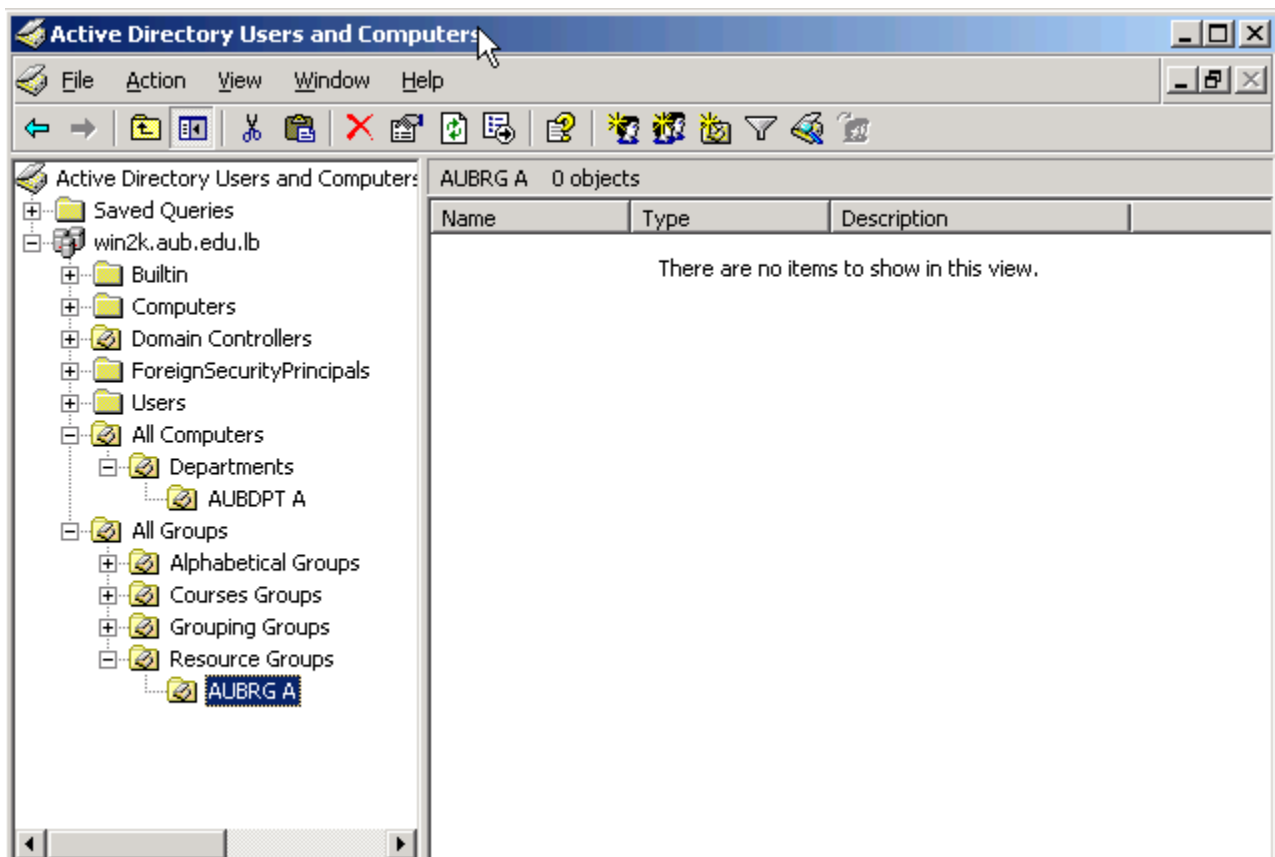


Figure 15: “OU” structure for security groups

8 Departmental Servers

Every “Administrator” will be delegated permissions on an “OU” inside the “All Servers” OU. This “OU” will hold the department name. The department system “Administrator” will place all department server computer objects inside this OU. The department system administrator will have the permission to manage these servers.

It should be noted that like computer OUs, each server “OU” should also have three corresponding groups:

- *<ServerOUname>OUAdmins*: Members can manage the OU
- *<ServerOUname>Admins*: Members will have administrative privileges on servers in the OU
- *<ServerOUname>Logon*: Members will have the right to logon to servers in the OU

The Delegation is done at the “OU” level using the delegation of control wizard. The permissions required are the same as delegating control on a department or lab computer OU. (Refer to section Delegating permissions on a department OU above)

Two group policies are required on each OU:

- The first policy defines who has the right to logon to the servers
- The second policy restricts the membership of the local administrators group on the servers. Refer to section Printing Services Printing Services

9 Settings for Public Labs Computers

To maintain the systems stable and reliable in AUB public labs, the CNS introduces the Microsoft Shared Computer Toolkit. This tool provides a simple and effective way to defend shared computers from viruses, Spywares and malicious software by clearing changes to the hard disk, or effectively resetting the disk, every time the computer restarts.

This toolkit includes several tools designed especially to help manage individual computers that are members of windows workgroups. One of these tools is the Windows Disk Protection WDP that can be used in domain environments to protect computers from unwanted changes.

9.1 Windows Disk Protection:

Unauthorized changes to a hard disk can make shared computers less reliable.

Windows Disk Protection clears all changes that are made to the Windows partition each time the computer restarts. WDP ensures that computers start from a clean and trusted copy of

Windows each time, removing viruses, spyware, temporary files and personal data from the computer with each restart.

Because certain changes, such as critical updates and antivirus signatures, need to be permanently saved, Windows Disk Protection allows you to schedule such changes to occur automatically at whatever time you choose.

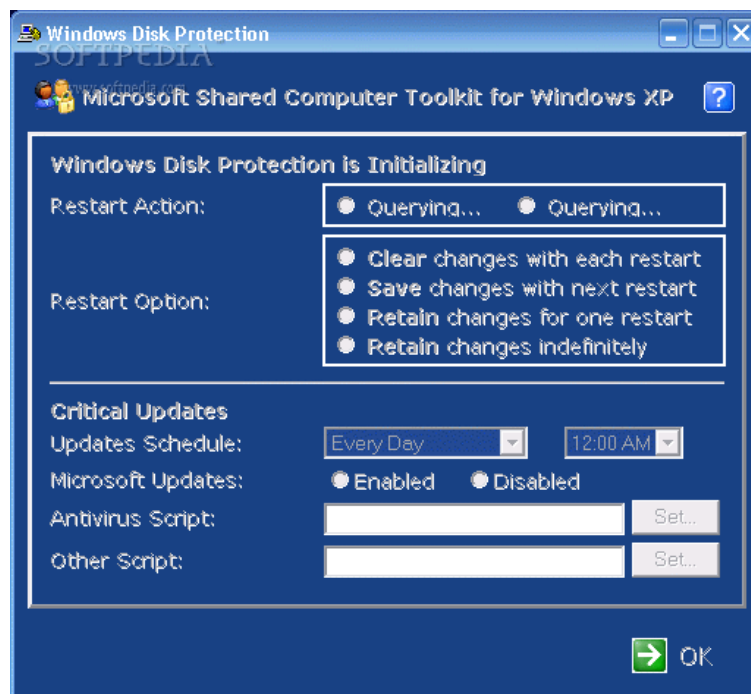


Figure 16: WDP main Window

When an “Administrator” needs to install software or update system settings, she/he must follow the following procedure:

1. Restart the system (To ensure that recent disk changes are cleared)
2. Install software or update the system
3. Access the WDP graphical tool (Shortcut available in the start menu)
4. Enable the option: Saves changes with next restart
5. Restart the system, the WDP filter works before the windows startup to save the changes made by the “Administrator”

Windows starts with the option clear changes with next restart enabled, therefore no need to adjust any WDP settings after the restart.

As a Summary, the WDP:

- Helps protect operating system files
- Clears changes when the computer restarts
- Automates critical and antivirus updates
- Lets you choose to save changes to disk

9.2 Preparing the Hard Disk for the Windows Disk Partition:

The WDP requires a minimum of 1 GB of unallocated disk space. This unallocated disk space will become the protection partition for storing disk changes temporarily when WDP is turned on.

To turn on the WDP, we must fulfill the following requirements:

1. At least 1GB or approximately 10% of the windows partition (whichever is greater) is available as unallocated disk space
2. The unallocated disk space must follow a primary partition; it cannot be at the beginning of the disk.
3. The disk that contains unallocated disk space may have no more than three primary partitions.
4. The position of the unallocated disk space is not significant (but normally for AUB public PCs, it 's located between C and D partitions)

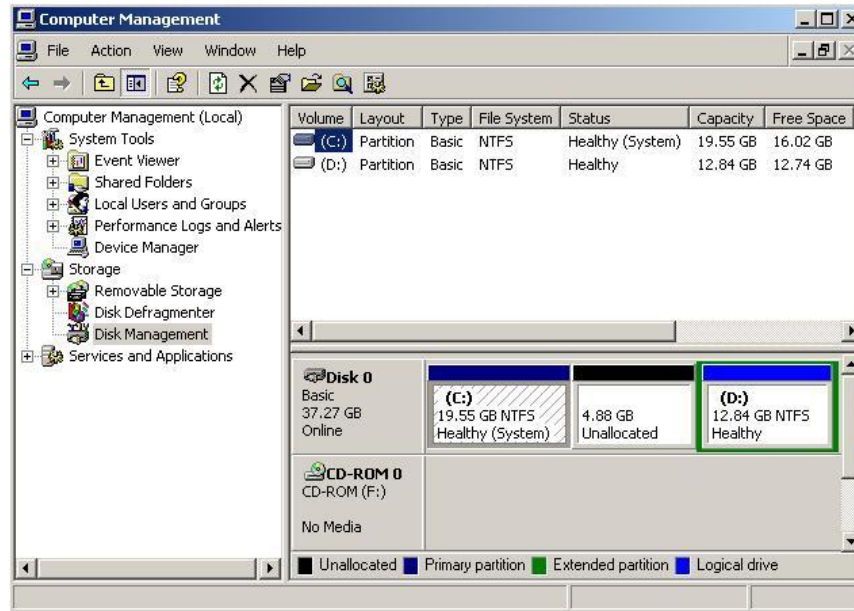


Figure 17: Disk management windows

Note:

If we are preparing an image for a public PC, and it has to be deployed by using the Norton Ghost, it's always recommended to create and format a partition for this unallocated space (F: for example, to be deleted after the deployment)

9.3 Placing Event Logs on a Persistent Partition

Entries made to system and application event logs stored on the Windows partition will be lost each time the system restarts when Windows Disk Protection is on. For this reason, it may be worthwhile to move the event logs to a persistent partition. We can accomplish this by modifying the paths saved in the following registry keys:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security\
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\System\
- The new path is D:\CNS\Events Logs*.evt

CNS is a hidden folder created on D drive, the administrators only can access the contents of this folder (the users permissions are removed from NTFS Security of this folder)

Note:

To automate the events redirection process (described in section 4), you can run the vbs script "Events Redirection.vbs" located in the following location:

\\pumbaa\Softwares\Public labs\toolkit\Events Redirection

9.4 Disabling System Hibernation

When a system hibernates, it writes the contents of the system RAM to a file on the disk. Because modifications to the Windows partition are cleared when Windows Disk Protection is on and set to Clear changes with each restart, hibernation will fail.

Thus, the system hibernation must be disabled before turning on the WDP.

9.5 WDP AUB Settings:

WDP is configured for all AUB public PCs as following:

- *Microsoft Updates: enabled*
- *Updates Schedule: weekly* (time is set in accordance with the closing hour of the lab)
- *Antivirus Script: mcupdate.exe*
- (*Location=C: \Program Files\Network Associates\Virus Scan*)

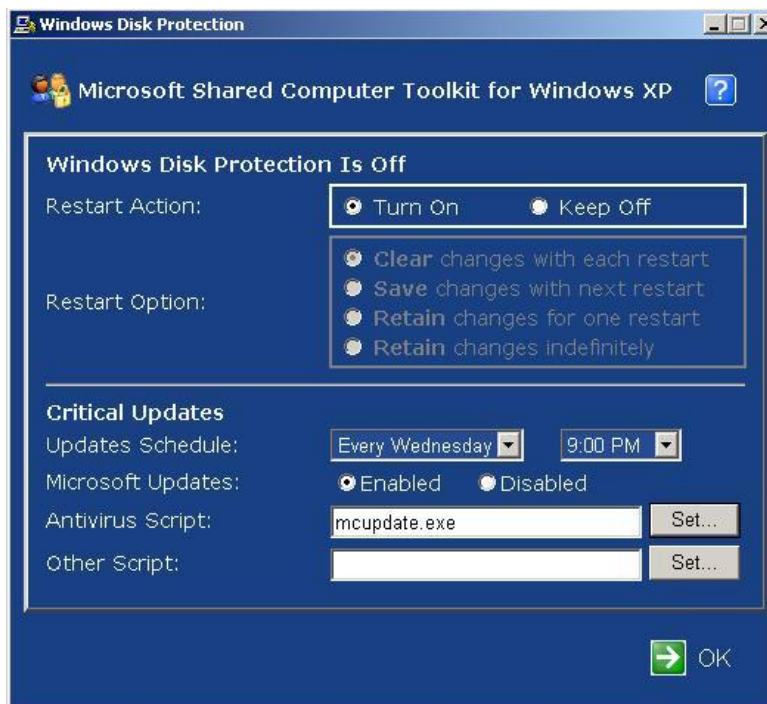


Figure 18: auto update/virus scan schedule

Note:

WDP creates 3 scheduled tasks on the system (At1, At2, and At3) for its maintenance period (period of updates); it's always recommended to delete any At scheduled task before turning on the WDP tool

10 Test Environment

A test Environment, "Cloned copy of win2k real environment", is available for system administrators wishing to test automated scripts, policies, or other Active Directory-related technologies. Administrators should contact the AUBede team (aubede@aub.edu.lb) for testing appointment.

11 Restoring objects

OU Administrators may request to have one or more deleted objects restored by contacting the AUBede Support Team (aubede@aub.edu.lb). Please provide the original LDAP path of the deleted object(s). CNS will make every effort to restore the objects to their original state; however, there are no guarantees as some attributes may not be restored or recoverable.

Individual units/departments are encouraged to properly document their OUs for easier recovery. Those wishing to implement their own backup/restore mechanism are encouraged to do so. CNS will be using command line tools "Adrestore.exe ver. 1.1" provided by Sysinternal/Microsoft to restore the deleted object

Appendix A

Guidelines for Requesting, Granting and Revoking

Privileged Access on AUBede Active Directory Objects

Applicable Policies

11.1.1 Policy on Privileged Access

11.1.2 (<http://cns.aub.edu.lb/cns/policy/2003/CNS-P-GEN-PRIV-ACCESS-B.pdf>)

11.1.3 Information Technology Management Principles, Policies and Guidelines

11.1.4 (<http://cns.aub.edu.lb/cns/policy/2003/CNS-P-ADM-APPS-A.pdf>)

Privileged Access Granting and Revoking Authority

Deans	Highest Privileged Access Granting/ Revoking Authority over <i>their respective faculty</i> Organizational Unit (OU) and corresponding resources under “ <i>AllComputers</i> ” and “ <i>Departments</i> ”, executed by proxy by the director of CNS or delegated as required.
Directors of Administrative and Academic Units	Highest Privileged Access Granting/ Revoking Authority over <i>their respective department</i> “OU” and corresponding resources under “ <i>AllComputers</i> ” under their OU, executed by proxy by CNS-AD-Administrator.
PC Custodian	Privileged Access Granting/ Revoking Authority over <i>the specific user’s PC</i> .
CNS-AD-Administrator	The Computing and Networking Services department is entrusted with the CNS-AD- Administrator role. As such CNS implements actions based on technical considerations

that guarantee best AUBede practices in terms of safety, functionality and security.

Access Rights, Access Group Membership and Audit Mechanism for a Domain PC

Access rights and permissions on resources depend on a user’s group membership as well as the “OU” where the PC hosting the resources is located. A detailed description of the Privileged Access rights, roles and permissions is provided in the “Access Rights Matrix”.

Table 1 below provides a brief description of the main Organizational Units (OUs) and groups used in the AUBede design and in granting Privileged Access.

Table 1

Object Type	Naming Covention	Description
Security Groups	“Domain Admins”	Built in group. Highest privileges on the domain resources. Membership of this group is highly restricted. Any and all transactions performed by users in this group will be audited.
	“Built-inADAdministrators”	Users in this group (mostly used in scripts) have the permission to modify Active Directory. Such modifications are audited.
	“DataAdmin”	Has Administrator privileges on specific data folders.
	“AllComputersAdmins”	Administrators of the “AllComputers” OU.
	“DepartmentsAdmins”	Administrators of the “Departments” OU.
	“AllLabsAdmins”	Administrators of the “AllLabs” OU.
	“AllServersAdmin”	Administrators of the “AllServers” OU.
	“MCAdmins”	Administrators of the “MedicalCenter” OU.
	“AllHomeAdmins”, “AllProfilesAdmins”, “InstitutionalDataAdmins”	Administrators of the data in the Homes, profiles and institutional data directories respectively.
	<DepartmentName>Admin	Administrators of the <DepartmentName> OU.
	<DepartmentName1>Admin	Administrators of the <DepartmentName1> OU.
	<PCName>Logon	Contains users who can logon to <PCName> .
	<PCName>PowerUser	Contains users with “Power User” privilege on <PCName> .
<PCName>Admin (Domain Group)	Contains users with administrator user privilege on <PCName> .	

Organizational Unit	"AllComputers"	The main "OU" under which are created OUs to hold computer objects not acting as servers.
	"Departments"	Under "AllComputersAdmins" , this "OU" contains all the departments' OUs outside the medical center.
	"AllLabsAdmins"	Under "AllComputersAdmins" , this "OU" contains all the labs' OUs.
	"AllServersAdmin"	The main "OU" under which are created OUs to hold computer objects acting as servers.
	"MedicalCenter"	Under "AllComputersAdmins" , this "OU" contains all the departments' OUs within the medical center.

AUBede Privileged Access Authority Type

Table details the Privileged Access Rights and the corresponding Granting/Revoking Authority and the final Execution entity to implement the requested change.

Table

Privileged Access Role	Granting Authority	Executed by
"Domain Admin"	CNS Director	<i>Domain Admin, Built-inADAdministrators</i>
"Built-inADAdministrators"	CNS Director	<i>Domain Admin, Built-inADAdministrators</i>
"AllComputersAdmins"	CNS Director	<i>Domain Admin, Built-inADAdministrators</i>
"DepartmentsAdmins"	CNS Director	<i>Domain Admin, Built-inADAdministrators</i>
"AllLabsAdmins"	CNS Director	<i>Domain Admin, Built-inADAdministrators</i>
"AllServersAdmin"	CNS Director	<i>Domain Admin, Built-inADAdministrators</i>
"MCAdmins"	CNS Director + AUBMC Director	<i>Domain Admin, Built-inADAdministrators</i>
"AllHomeAdmins", "AllProfilesAdmins", "InstitutionalDataAdmins"	CNS Director	<i>Domain Admin, Built-inADAdministrators</i>
<DepartmentName>Admin	Director, Dean, Chairperson or Manager of <DepartmentName>	"AllDepartmentsAdmins" or "MCAdmins"
<DepartmentName1>Admin	Manager or Supervisor of <DepartmentName1>	<DepartmentName>OUAdmin
Win2kUser	Registrar, Personnel	"ADSync"
<PCName>Logon	<PCName> Custodian	<DepartmentName>OUAdmin
<PCName>PowerUser	<PCName> Custodian	<DepartmentName>OUAdmin
<PCName>Admin (Domain Group)	Head of Department where <PCName> is located + <PCName> Custodian	<DepartmentName>OUAdmin

<PCName> Local Administrator (Local)	Head of Department where <PCName> is located + CNS	Password Escrow Custodian
---	---	---------------------------

Requesting Privileged Access Workflow

To request privileged access, the requester (Privileged Access User or PAU) should:

1. Read and accept receipt of the [Policy on Privileged Access](#) (if first time PAU)
2. Complete and sign a [\[AD Privileged Access Agreement Form\]](#) (PAAF) and secure his/her supervisor approval
3. Forward the request to the parent “OU” administrator to assess and validate the requirements
4. Secure the approval of the appropriate granting authority for that OU
5. The parent “OU Administrator” would then execute the request and file the supporting documents.

Instructions on How to Fill the Privileged Access Agreement Form

The first section of the form should be filled with the details of the system administrator requesting the privileged access. The system administrator could be part of CNS system administrators’ team or a departmental system administrator who will be entrusted with the administration of the “Departmental OU”.

The form offers the following selection fields:

Scope: select one of three different available scopes representing the level at which the Privileged Access will take effect:

Institution: widest scope whereby the granted Privileged Access would affect users and/or PCs on the whole of AUBede.

OU: whereby the granted Privileged Access would affect users and/or PCs under the specified OU.

PC: whereby the granted Privileged Access would take effect only on the specified PC name (as it appears in the win2k Active Directory).

Role: depending on the chosen Scope one of a number of roles can be selected. A detailed description of each role can be read from the “Access Rights Matrix” and the accompanying “Authorized Security Document”.

Access Audited by: select out of the available options the type of audit/alert if any applied to the Privileged Access to be granted.

OU / PC name: enter the name of the “OU” or PC the on which the Privileged Access would apply.

–The PAAF should be signed and approved as follows:

1. The requester (PAU) requesting the privileged access should first sign the submitted form.
2. The form is then forwarded to the parent “OU Administrator” for assessment, comments and approval.
3. The form has then to be approved by the prime custodian of the subject system/data the "Granting Authority".