

King Fahd University of Petroleum and Minerals
Information Technology Center (ITC)
Academic Technologies (ATS)



Smart Classroom Tutorial Series

**KFUPM User ID's and
Windows Accounts**

28th May, 2005

Contents

1. Introduction to User Accounts
2. Creating Windows Accounts
3. Changing or Resetting Password's for Windows Accounts
4. KFUPM User ID's
5. LDAP @ KFUPM

1. Introduction to User Accounts

User Accounts are the mechanism that we use to give people access to resources on the network. These resources can include things such as files and folders, printers, applications, and so on. When logging on, a user is authenticated (proves their identity) to the computer or network, by providing the correct combination of User Account Name and a Password.

1.1 What is Domain?

A *domain* is a logical grouping of networked computers that share a central directory database that contains user account and security information for resources within the domain.

In a domain, the directory database is stored on computers that are configured as domain controllers. A domain controller manages all security-related aspects of interactions between users and domains. Security and administration are centralized.

1.2 What is the difference between Authentication and Authorization?

Authentication

An *authentication* system is how you identify yourself to the computer. The goal behind an authentication system is to verify that the user is actually who they say they are.

Authorization

Once the system knows **who** the user is through authentication, *authorization* is how the system decides **what** the user can do.

1.3 User Accounts

There are mainly three types of user accounts. They are

1. Built-in User Account
2. Local User Account
3. Domain User Account

1.3.1. Built-in User Account

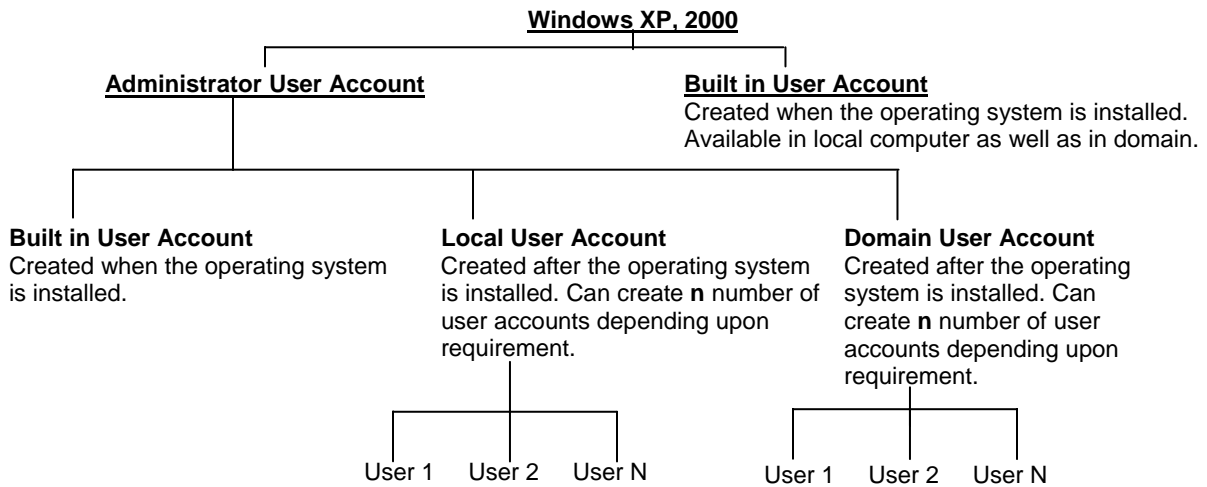
Built-in User Accounts are accounts that are created at the time of installation. Two built-in local user accounts are created in Windows 2000: **Administrator**, and **Guest**. There are two similar built-in accounts in (Domain) Active Directory: Administrator and Guest. In both cases the Guest account is disabled by default. Windows 2000 servers and Windows XP Professional may also have additional built-in accounts for Internet Information Server, such as **IUSR_servername** and **IWAM_servername**. The administrator and guest accounts cannot be deleted.

1.3.2. Local User Account

Local User Accounts enable users to log on to a single, specific computer. The Local User Account can be given access to resources on that specific computer alone. For a user to access resources on more than one computer using a Local user account, the user must have a Local account created on each computer. Naturally, with more than a handful of computers on a network, administering Local accounts can quickly become an administrative nightmare. However, when using Local accounts, no Domain Controller (a specific type of Windows 2000/NT server) is required.

1.3.3. Domain User Account

Domain User Accounts allow users to log on, just like Local User Accounts, except that their identity or authentication is recognized by all of the computers in the Domain. This is because Domain User Accounts physically reside within Active Directory, rather than in a local computer. This is much more convenient for both users and administrators, since the user only has to remember one User Account Name and Password, and administrators can grant permission to the resources (files, printers, etc.) of any computer in the domain to the one single User Accounts. In order to utilize Active Directory, however, there must be at least one Domain Controller server on the network (in large networks there could be hundreds of Domain Controllers).



1.4 Difference between Administrator and Guest User account

1.4.1 Administrator User Account

The Administrator account has full control of the local computer or domain and can assign user rights and access control permissions to local computer or domain users as necessary. It is recommended that you set up this account with a strong password.

The Administrator account is a default member of the Administrators (Local Computer) , Domain Admins, Enterprise Admins, Group Policy Creator Owners, and Schema Admins groups in (Domain) Active Directory. The Administrator account can never be deleted or removed from the Administrators group, but it can be renamed or disabled. Because the Administrator account is known to exist on many versions of Windows, renaming or disabling this account will make it more difficult for malicious users to try and gain access to it.

Important

When the Administrator account is disabled, it can still be used to gain access to a domain controller using Safe Mode.

1.4.2 Guest User Account

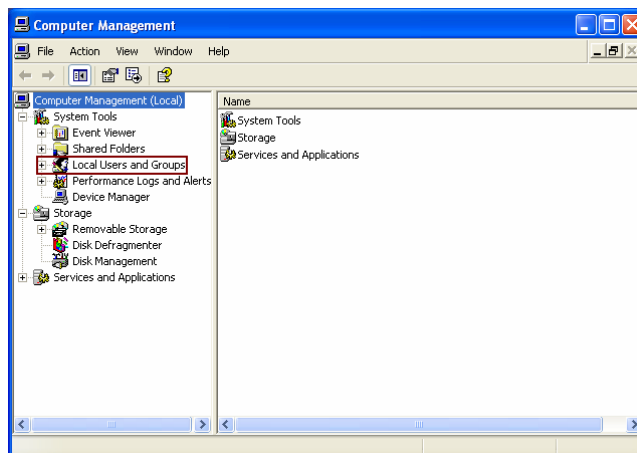
The Guest account is used by people who do not have an actual account in the domain. A user whose account is disabled (but not deleted) can also use the Guest account. The Guest account does not require a password.

You can set rights and permissions for the Guest account just like any user account. By default, the Guest account is a member of the built-in Guests group (Local Computer) and the Domain Guests global group (Domain), which allows a user to log on to a domain. The Guest account is disabled by default, and it is recommended that it stay disabled.

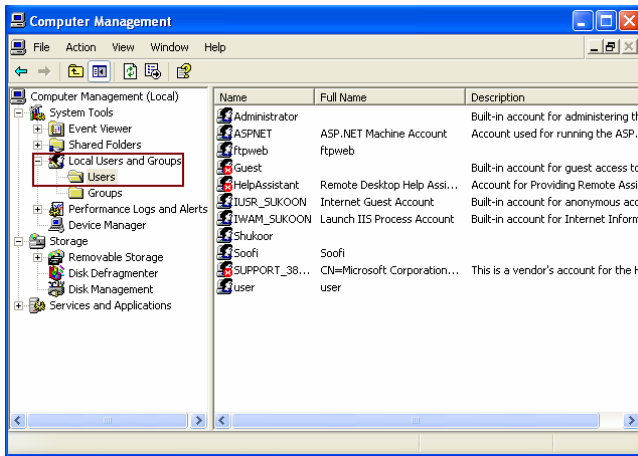
1.5 Why Guest account is disabled?

To avoid hackers and hacker utilities to access the Guest account, the guest account is disabled as a security reason. It is recommended not to leave a blank password for guest account because of hackers, they can enable the guest account, get in to the computer to do damage. It is wise to assign a password to the Guest account, but leave the Guest account disabled.

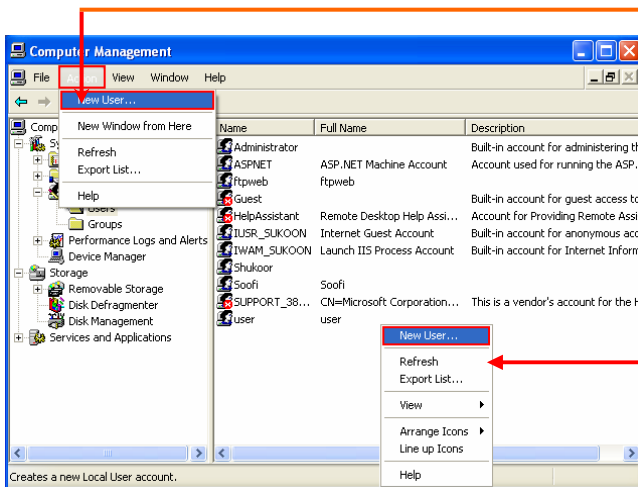
2 Creating Local User Accounts



Creating a local user is simple. You must have enough permissions (E.G.: Administrator) to create users on the local machine, in order to be successful. After logging in, right click on **My Computer** icon from desktop → Click on **Manage**.



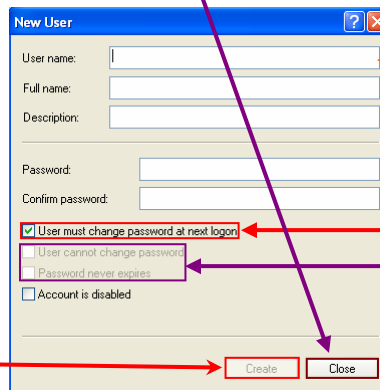
In the window that appears, you should see a folder called "Local Users and Groups" on left panel. This folder will contain two subfolders: "Users," and "Groups," click the "Users" folder in the left pane of the window, and you should see at built-in user accounts and available user accounts in the right pane.



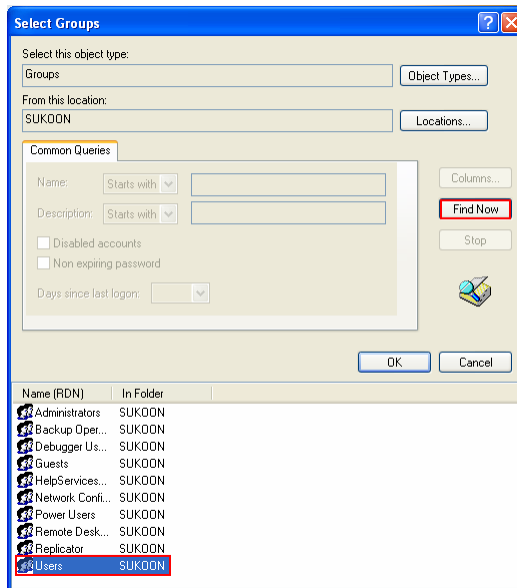
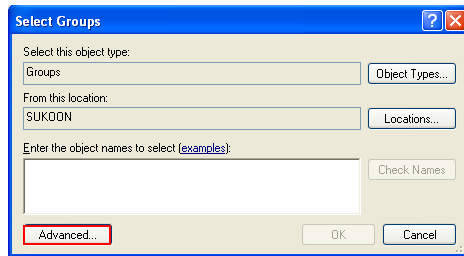
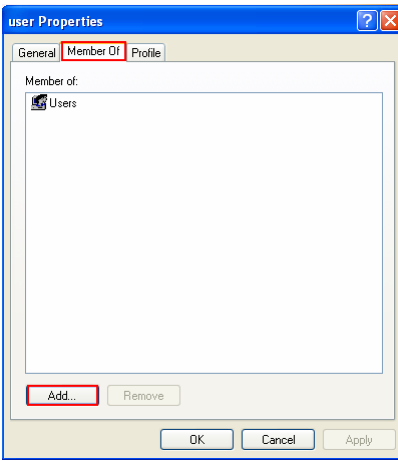
OR

To create the new user, choose "New User..." from the Action menu, or by right-clicking in an open area of the right-hand pane.

This will bring up a dialogue box to fill out. The only required field is the "Username" field, but you should also enter in (and confirm) a password in the appropriate fields, and you may also wish to fill in the Full Name and Description fields. By default, the "User must change password at next logon" box is checked, but if you clear it, you can choose to select "User cannot change password" and/or "Password never expires". If you want the account to start out disabled, you can also check that box. After making all of the desired selections, click "Create" to create the new user. The user will be created, and the form will then be cleared so that you can create another user. Click "close" if you are done.



Once the user is created, you can double-click it to view or change its properties and can also assign it group membership, a home directory, or a logon script.



In this example the user is being added to “Users” group, if you want to add the user to Administrator group or any other group you have to select the group respectively. Click OK three times. Remember, local users only exist on a single machine, so if you have several machines that you want a local user to log into, you will have to create a user account on each machine. That can get tedious if you have more than a handful of machines. That's why we have Active Directory. In AD, you can create a user once, and a user can login once and have access to all of the machines that it has been assigned permissions to. So how do you create an Active Directory user?

By now you have successfully created the user account and change its properties.

Note: Some images do not belong to windows 2000. The procedure is same only images differ.

3 Changing or Resetting the Password in Windows XP/2000

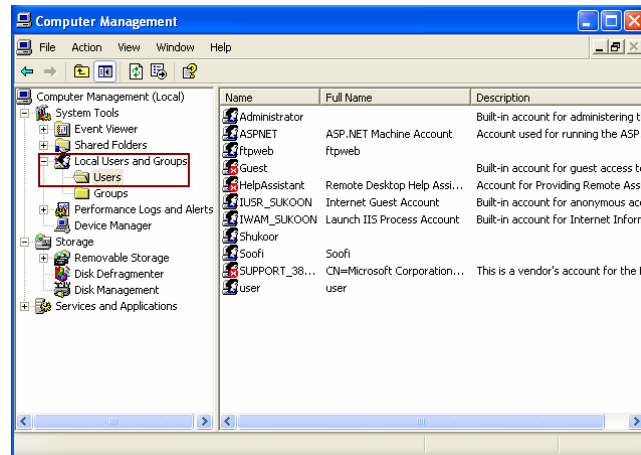
3.1 Why change password

It is very importance to change the passwords of your computer accounts, E-mail and Internet, frequently. Unfortunately, our experience during the last few months showed that most of us do not change their passwords that frequent. Even worse, some of us uses very simple easy to guess passwords, allowing others to guess them and utilizes these accounts. Remember that any problems that are created from your computer accounts will be your sole responsibility. Recently, we were faced with many security problems

that were caused by users using other accounts. Therefore, we kindly request you to change your passwords now, if you did not do in the last two weeks, and keep doing this process every two-three weeks.

3.1.1 To change the password for local computer user account

Right click on **My Computer** → Click on **Manage**. From left pane double click (or click the + sign besides) **Local Users and Groups**.



Select the user and right click → Set Password → click on Proceed to reset the password. Enter the new password and confirm it and click OK. You have successfully changed (reset) the password.

4 KFUPM User ID's

There are mainly two user accounts @ ITC, KFUPM. They are

1. E-mail user account (UNIX based) and
2. ITC user account (ITC domain and Internet account) Windows 2000 based.

4.1 Passwords for E-mail and ITC (Internet account)

1. E-mail user account

The password for E-mail must be alphanumeric (according to KFUPM ITC policies email password must be alphanumeric with at least 2 numerals).

2. Where as ITC domain account (Internet account) can be numeric or alphabets or alphanumeric.

4.1.2 Why change password

It is very importance to change the passwords of your computer accounts, E-mail and Internet, frequently. Unfortunately, our experience during the last few months showed that most of us do not change their passwords that frequent. Even worse, some of us uses very simple easy to guess passwords, allowing others to guess them and utilizes these accounts. Remember that any problems that are created from your computer accounts will be your sole responsibility. Recently, we were faced with many security problems that were caused by users using other accounts. Therefore, we kindly request you to change your passwords, if you did not do in the last three months, and keep doing this process every three months. To change the ITC/STU domain password visit the URL

<http://www.kfupm.edu.sa/itc/?c=howto/changepassword> for faculty and staff (ITC Domain) click FACULTY/STAFF, for students (STU domain) click STUDENTS.

It's necessary for users to use good passwords to protect their data and their computers, as well as the KFUPM network.

4.2 KFUPM E-mail Accounts

4.2.1 Using E-mail account @ KFUPM

To check E-mails using KFUPM E-mail service, there are few possible ways

1. Configure MS E-mail client MS Outlook, MS Outlook Express or any other E-mail clients to KFUPM mail server. How to configure MS Outlook or MS Outlook Express, visit URL <http://www.kfupm.edu.sa/itc/?c=howto/configmail>.
2. You can also use internet browser e.g. Internet Explorer for checking your E-mails. To access web based mail service visit <https://webmail.kfupm.edu.sa/>.
3. You can also use telnet or telnet client (PUTTY) telnet to 196.15.32.8 to access your E-mail through UNIX. For more information on PUTTY, visit URL <http://www.kfupm.edu.sa/itc/sos/putty/>.

4.3 **KFUPM Password Policies**

4.3.1 **Password Maintenance Policy**

In an effort to provide secured and reliable computing environment to all the members of the KFUPM Community, and based on the approval of H. E. The Rector on the recommendations of the Computer Utilization Committee, the ITC has developed an enhanced password maintenance policy for both the Internet and UNIX accounts. We kindly request all our community to adherence to the following policy statements:

1. All users are advised to change their passwords for both the Internet and UNIX accounts once before May 15, 2001 for the first time, and must change them every three months thereafter. The Unix and NT systems will enforce the users to change the password in the due time. An earlier e-mail warning will be sent to users to remind them about the due date for the password change.
2. The new password has to fit in the following simple criteria:
 - o Password must have at least 8 characters and the new password must be different from your previous password.
 - o Password must consist of at least 2 Non-Alphabetic characters [Non-Alphabetic characters include: Numbers 0 to 9 and special characters such as !@#\$\$%^&*()_+].

4.3.2 **Password Selection Guidelines**

The object when choosing a password is to make it as difficult as possible for a hacker/cracker to make educated guesses about what you've chosen. This leaves hackers/crackers no alternative but a brute-force search, trying every possible combination of letters, numbers, and punctuation. A search of this sort, even conducted on a machine that could try one million passwords per second (most machines can try less than one hundred per second), would require, on the average, over one hundred years to complete. The following guidelines for a password selection may be useful (from APS Online Journal password selection):

4.3.2.1 **Some Do's**

- Do use a password with mixed-case alphabetic.
- Do use a password with non-alphabetic characters, e.g., digits or punctuation.
- Do use a password that is easy to remember, so you don't have to write it down.
- Do use a password that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.

4.3.2.2 **Some Dont's**

- Don't use your login name (username) in any form (as-is, reversed, capitalized, doubled, etc.).
- Don't use your first or last name in any form.
- Don't use your spouse or child's name.
- Don't use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, member society number, the brand of your automobile, the name of the street you live on, etc.
- Don't use a password of all digits, or all the same letter. This significantly decreases the search time for a hacker/cracker.
- Don't use a word contained in (English or foreign language) dictionaries, spelling lists, or other lists of words.
- Don't use a password shorter than six characters.

Although this list may seem to restrict passwords to an extreme, there are several methods for choosing secure, easy-to-remember passwords that obey the above guidelines. Some of these include the following:

- Choose a line or two from a song or poem, and use the first letter of each word. For example, "Let me take you down, 'cause I'm going to Strawberry Fields" becomes "LmtydclgtSF". (Of course, only the first eight characters count.)
- Alternate between one consonant and one or two vowels, up to eight characters. This provides nonsense words that usually make excellent passwords. Examples include "bababuoy," "seeplip," and so on.
- Choose two short words and concatenate them together with a punctuation entity between them. For example: "cat;snow," "trip+car," "pill?dog."

The importance of obeying these password selection guidelines cannot be over emphasized. The infamous "Internet Worm," as part of its strategy for breaking into new machines, attempted to crack user passwords. First, the "Worm" tried simple choices such as the login name, user's first and last names, and so on. Next, the "Worm" tried each word present in an internal dictionary of 432 words (presumably the "Worm's" creator considered these words to be "good" words to try). If all else failed, the "Worm" tried going through the host system dictionary, /usr/dict/words, trying

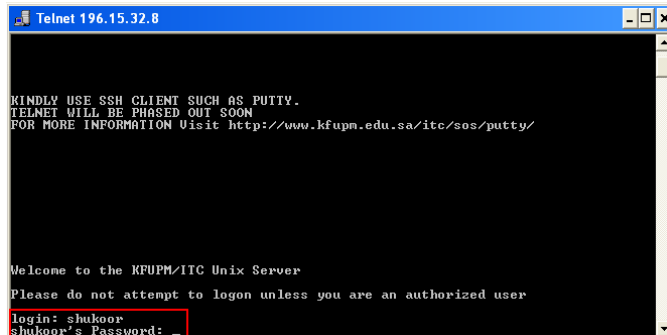
each word. The password selection guidelines above successfully guard against all three of these strategies, according to popular security handbooks.

4.4 Changing or Resetting the Password

4.4.1 For E-mail (UNIX Account)

4.4.1.1 Using Telnet 196.15.32.8

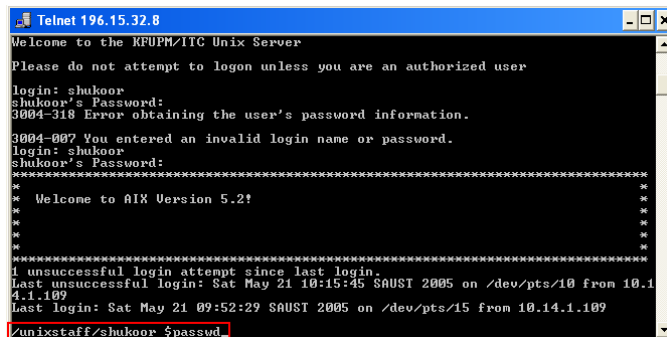
Point to **START**→ **Run**→ in the **Open** bar type **TELNET 196.15.32.8**→ and click **Run**



```
Telnet 196.15.32.8
KINDLY USE SSH CLIENT SUCH AS PUTTY.
TELNET WILL BE PHASED OUT SOON
FOR MORE INFORMATION Visit http://www.kfupm.edu.sa/itc/sos/putty/

Welcome to the KFUPM/ITC Unix Server
Please do not attempt to logon unless you are an authorized user
login: shukoor
shukoor's Password: _
```

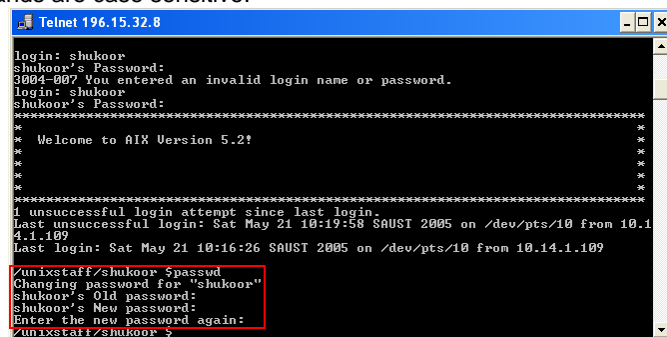
After entering the **Username** press **Enter** (Do not Use **Tab**), enter the **Password** (The cursor will not move, you will not see ********* astrix because of UNIX Security).



```
Telnet 196.15.32.8
Welcome to the KFUPM/ITC Unix Server
Please do not attempt to logon unless you are an authorized user
login: shukoor
shukoor's Password:
3004-318 Error obtaining the user's password information.
3004-007 You entered an invalid login name or password.
login: shukoor
shukoor's Password:
*****
* Welcome to AIX Version 5.2!
*****
1 unsuccessful login attempt since last login.
Last unsuccessful login: Sat May 21 10:15:45 SAUSTI 2005 on /dev/pts/10 from 10.1
4.1.109
Last login: Sat May 21 09:52:29 SAUSTI 2005 on /dev/pts/15 from 10.14.1.109
/unixstaff/shukoor $passwd
```

Enter the **passwd** command to reset or change the password and press **Enter**

Note: All UNIX commands are case sensitive.



```
Telnet 196.15.32.8
login: shukoor
shukoor's Password:
3004-007 You entered an invalid login name or password.
login: shukoor
shukoor's Password:
*****
* Welcome to AIX Version 5.2!
*****
1 unsuccessful login attempt since last login.
Last unsuccessful login: Sat May 21 10:19:58 SAUSTI 2005 on /dev/pts/10 from 10.1
4.1.109
Last login: Sat May 21 10:16:26 SAUSTI 2005 on /dev/pts/10 from 10.14.1.109
/unixstaff/shukoor $passwd
Changing password for "shukoor"
shukoor's Old password:
shukoor's New password:
Enter the new password again:
/unixstaff/shukoor $
```

In order to change or reset the old password, first enter the **Old Password** and press **Enter**, then enter the **New Password** according to **KFUPM Password Maintenance Policy** and press **Enter** again enter the **New Password** for **Confirmation** and press enter. You have successfully changed or reset your E-mail password.

IMPORTANT: Do not forget to logout at the prompt type **logout** or **exit** (not for putty) and press **Enter**.

4.4.1.2 Using PUTTY (TELNET CLIENT)

Please visit the following URL to download the TELNET and FTP client PUTTY and PSFTP and to get the detailed information on Putty <http://www.kfupm.edu.sa/itc/sos/putty/>.

For more details please feel free to contact ITC-Help Desk at X 1900, or visit ITC online Help Desk URL <https://help.kfupm.edu.sa/>.

4.4.2 ForINTERNET ACCOUNT (ITC DOMAIN)

Internet user account is the ITC domain user account, this means if a user wants to access the internet he has to give internet user account and password which is same as ITC domain user account. If a user wants

to logon to ITC domain same user account and password will be used. If a user is having ITC domain user account he can able to access all the available resources for his ITC domain user account e.g. internet, KFUPM-filer system etc.

4.4.2.1 How To Change The ITC Domain User Account (Internet User Account) Password

There are ways to change or reset the ITC domain user account password. The easiest and simple way to call ITC help desk X 3991, 1900 or visit KFUPM home page from right side click **change password**, you will get two options

1. Faculty and Staff
2. Student

Click on the appropriate link to change or reset the password. A security dialog box is displayed, click **yes** to proceed. You will be prompted to enter ITC user name, followed by Current Password which is again followed by **New Password**, this is again followed by **New Password Again** (for confirmation). After you change or reset the password click on **Change Password Now**, if you make any mistake while entering the new password, don't worry you can still reset it on just clicking **Start Over**. If you forget your new password don't worry again just call ITC help desk. ITC is pleased to server the KFUPM community at its best.

ITC Username:
Current Password:
New Password:
New Password Again:

Note: Passwords are case-sensitive on this system. Password, PASSWORD, and password are three different passwords.

If your computer is a member of ITC domain (i.e. if your computer is joined to ITC domain) at the time of logon to ITC domain, it will prompt to change the password if your password is getting expired. According to KFUPM Password Maintenance policy ITC domain and E-mail passwords expire every three months.

5 LDAP @ KFUPM

What is LDAP?

Short for *Lightweight Directory Access Protocol*, a set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. And unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access. Because it's a simpler version of X.500, LDAP is sometimes called *X.500-lite*.

Although not yet widely implemented, LDAP should eventually make it possible for almost any application running on virtually any computer platform to obtain directory information, such as email addresses and public keys. Because LDAP is an open protocol, applications need not worry about the type of server hosting the directory.

LDAP lets you "locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate intranet," and whether or not you know the domain name, IP address, or geographic whereabouts. An LDAP directory can be distributed among many servers on a network, then replicated and synchronized regularly. An LDAP server is also known as a Directory System Agent (DSA).

LDAP was developed at the University of Michigan; it's "lightweight" in contrast to DAP, a part of the older X.500 directory protocol for networks. It is both simpler and less secure, hence lighter. It can be used to route email in large organizations as well as look up people and machines across public or private networks.

KFUPM LDAP Implementation

- **UNIX System Integration With KFUPM LDAP Directory**
- **Application Integration With KFUPM LDAP Directory**
- **Directory Admin Tool & KFUPM LDAP Data Model**
- **UNIX Logon to Access User Home Directory**
- **KFUPM E-Mail Service**
- **User Password and Help-Desk Password Reset Web Tools**
- **WebCT User Authentication via KFUPM LDAP Directory**
- **HRS Application User Authentication via KFUPM LDAP Directory Services**
- **Prototype Graduate Studies System Application User Authentication via KFUPM LDAP Directory Services**



KFUPM User ID's and Windows Accounts

Feedback Form

To improve this document and our services please feel free to write us your comments and suggestions, we will be glad to hear your comments and suggestion to improve our services.

Name: _____
Department: _____
Email: _____
Telephone: _____
Fax: _____

Comments:

Suggestions:

Abdul Shukoor

Network Engineer

Telephone Office 3941

Fax 2326

Email: shukoor@kfupm.edu.sa

P.O Box 5037

ATS Manager

Information Technology Center

Telephone Office 3909

Fax 2326

Email: itc.mats@kfupm.edu.sa

P.O. Box 5037