**USER ACCOUNT**

A **user account** is a location on a network server used to store a computer username, password, and other information. A **user account** allows or does not allow a **user** to connect to a network, another computer, or other share. Any network that has multiple users requires **user accounts**

A user's account allows a user to [authenticate](https://en.wikipedia.org/wiki/Authentication) to a system and potentially to receive [authorization](https://en.wikipedia.org/wiki/Authorization_(computer_access_control)) to [access](https://en.wikipedia.org/wiki/Access_control) resources provided by or connected to that system In Active Directory, a user account is an object that consists of all the information that defines a domain user, which includes user name, password, and groups in which the user account has membership. User accounts can be stored in either Active Directory or on your local computer.

Understanding user accounts

A **user account**allows you to **sign in** to your computer. By default, your computer already has one user account, which you were required to create when you set up your computer. If you plan to share your computer with others, you can create a**separate user account** for each person.

Why use separate user accounts?

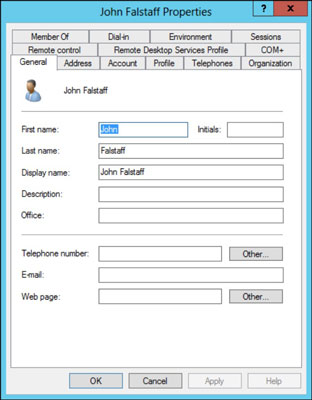
At this point, you may be wondering why you would even need to use separate user accounts. But if you're sharing a computer with multiple people—for example, with your family or at the office—user accounts allow everyone to save their own files, preferences, and settings without affecting other computer users. When you start your computer, you'll be able to choose which account you want to use.

Before you create new user accounts, it's important to understand the different types.

* **Administrator**: Administrator accounts are special accounts that are used for making changes to system settings or managing other people's accounts. They have full access to every setting on the computer. Every computer will have at least one Administrator account, and if you're the owner you should already have a password to this account.
* **Standard**: Standard accounts are the basic accounts you use for normal everyday tasks. As a Standard user, you can do just about anything you would need to do, such as running software or personalizing your desktop.

For each user account you create on your network, you can set additional properties for the user by right-clicking the new user and choosing Properties from the contextual menu. This command brings up the User Properties dialog box, which has about a million tabs that you can use to set various properties for the user.

The figure shows the General tab, which lists basic information about the user, such as the user’s name, office location, and phone number.



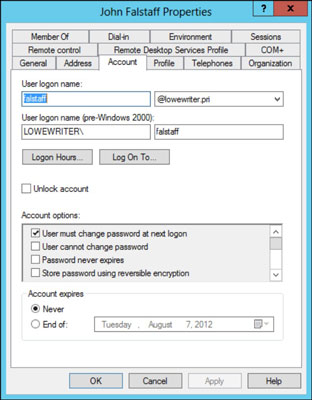
CHANGE THE USER’S CONTACT INFORMATION

Several tabs of the User Properties dialog box contain contact information for the user, such as

* **Address:** Change the user’s street address, post office box, city, state, zip code, and so on.
* **Telephones:** Specify the user’s phone numbers.
* **Organization:** Record the user’s job title and the name of his boss.

SET ACCOUNT OPTIONS

The Account tab of the User Properties dialog box features a variety of interesting options that you can set for the user. You can change the user’s logon name, change the password options that you set when you created the account, and set an expiration date for the account.

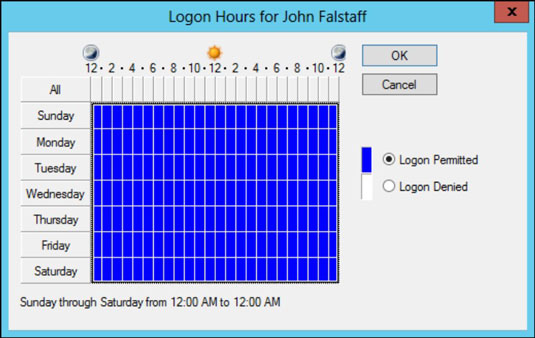


The following account options are available in the Account Options list box:

* **User Must Change Password at Next Logon:** This default option allows you to create a one-time-only password that can get the user started with the network. The first time the user logs on to the network, he is asked to change the password.
* **User Cannot Change Password:** Use this option if you don’t want to allow users to change their passwords. (Obviously, you can’t use this option and the preceding one at the same time.)
* **Password Never Expires:** Use this option to bypass the password-expiration policy for this user so that the user will never have to change her password.
* **Store Password Using Reversible Encryption:** This option stores passwords by using an encryption scheme that hackers can easily break, so you should avoid it like the plague.
* **Account Is Disabled:** This option allows you to create an account that you don’t yet need. As long as the account remains disabled, the user won’t be able to log on.
* **Smart Card Is Required for Interactive Logon:** If the user’s computer has a smart card reader to read security cards automatically, select this option to require the user to use it.
* **Account Is Trusted for Delegation:** This option indicates that the account is trustworthy and can set up delegations. This advanced feature usually is reserved for Administrator accounts.
* **Account Is Sensitive and Cannot Be Delegated:** This option prevents other users from impersonating this account.
* **Use DES Encryption Types for This Account:** This option beefs up the encryption for applications that require extra security.
* **Do Not Require Kerberos Preauthentication:** *Kerberos* refers to a common security protocol used to authenticate users. Select this option only if you are using a different type of security.

SPECIFY LOGON HOURS

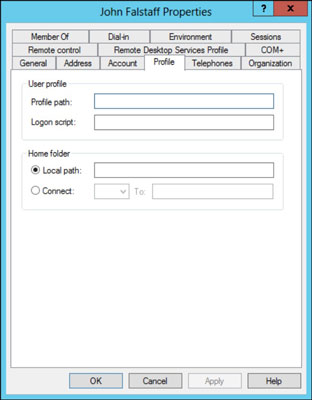
You can restrict the hours during which the user is allowed to log on to the system. Click the Logon Hours button on the Account tab of the User Properties dialog box to open the Logon Hours for [User] dialog box.



Initially, the Logon Hours dialog box is set to allow the user to log on at any time of day or night. To change the hours that you want the user to have access, click a day and time or a range of days and times, select Logon Permitted or Logon Denied, and then click OK.

SET THE USER’S PROFILE INFORMATION

From the Profile tab, you can configure three bits of information about the user’s profile information:



* Profile Path: This field specifies the location of the user’s roaming profile..
* Logon Script: This field is the name of the user’s logon script. A logon script is a batch file that’s run whenever the user logs on. The main purpose of the logon script is to map the network shares that the user requires access to.

Logon scripts are carryovers from early versions of Windows NT Server. In Windows Server 2012, profiles are the preferred way to configure the user’s computer when the user logs on, including setting up network shares. Many administrators still like the simplicity of logon scripts, however.

* Home Folder: This section is where you specify the default storage location for the user.

**Group Management**

Groups are Active Directory or local computer objects that can contain users, contacts, computers and other groups. You can use groups to carry out the following tasks:

* Manage user and computer access to shared resources such as Active Directory objects and their properties, network shares, files, directories, and printer queues.
* Filter Group Policy settings.
* Create e-mail distribution lists.

The default groups that are put in the **Built incontainer** of Active Directory Users and Computers are: Account Operators, Administrators, Backup Operators, Guests, Incoming Forest Trust Builders (only appears in the forest root domain), Network Configuration Operators, Performance Monitor Users, Performance Log Users, Pre-Windows 2000 Compatible Access Print Operators, Remote Desktop Users, Replicator Server Operators Users.

**Group Scope**

Each group has a specific role, or scope which defines how it can be used and where it is valid within Active Directory. Each group is assigned one of the following scopes:

* **Domain local:** can only specify permissions on resources within a single domain.
* **Built-in local:** created automatically whenever an Active Directory domain is created. Built-in local groups have the same scope as domain local groups. You cannot create them or delete them, but you can modify their members and their membership of other groups.
* **Global:** can contain users, groups, and computers from its own domain as members. Global groups are available under any domain functional level.
* **Universal:** can contain users, groups, and computers from any domain in its forest. Only available when the domain functional level is set at Windows 2000 native or Windows Server 2003.

**Windows Domain Administrator Groups**

On a Windows network, there are several Security Groups that have high levels of access to various parts of the network. These groups should be audited regularly to ensure that there are no normal users as members, only Administrators. The default groups are:

* Administrators
* Domain Admins
* Schema Admins
* Enterprise Admins

There may be other groups with high levels of access that have been manually created. These should be documented and added to the auditing process.

**Domain Service Accounts**

There is another type of user account that has special access to parts of your network – the Service Account. Service Accounts are user accounts that are used by software (normally on a server) to carry out automated tasks such as running backups, or managing your anti-virus administration. These services should never be set up to use Administrator account credentials – there should be at least one dedicated Service Account on your network.

**Domain Guest Accounts**

Windows has a default guest account called Guest. These guest accounts are the first port of call for criminal hackers and should be immediately and permanently disabled. If a guest account is required, it should not have an obvious name such as Guest.

**Domain User Accounts**

These are the normal user accounts that are used by staff in their day-to-day work to log onto a computer and do their normal work. They should not have any special permissions that could potentially lead to damage or data loss. These user accounts are normally members of a Security Group called Domain Users.

In some cases, it is necessary to grant special or administrative permissions to users. This should be restricted to Local Admin access (they are Administrators only on their own computers, and not on the Domain).

**Local Accounts**

These are similar to Domain accounts, but are limited to local access only. Local access can be to a computer or a server. Local accounts can be Administrator accounts, normal user accounts, and Guest accounts. The built-in Administrator and Guest user accounts should always be disabled on workstations, and the built-in Guest user accounts should always be disabled on servers.

**Local Groups**

On computers and servers, there is a default Security Group called Administrators. Membership of this group should be limited to a domain group called Domain Admins