**System Logging**

In general computer usage, logon is the procedure used to get access to an operating system or application, usually in a remote computer. Almost always a logon requires that the user have (1) a user ID and (2) a password. Often, the user ID must conform to a limited length such as eight [character](http://searchcio-midmarket.techtarget.com/definition/character)s and the password must contain at least one digit and not match a natural language word. The user ID can be freely known and is visible when entered at a keyboard or other input device. The password must be kept secret (and is not displayed as it is entered).

Modern networked operating systems, such as Microsoft Windows, Mac OS X, and the UNIX family of operating systems, allow users to log on to their machines locally by using them directly, or by connecting to a file server remotely through a network logon. Because both logons tend to happen simultaneously after users enter their usernames and passwords, they do not usually perceive much of a difference between the two logons. Network logons can be disabled by administrators, thus preventing individuals from robbing passwords and remotely taking over the machine.

**Network login**

Domain account is when you login using a domain account on a network. You would need a domain controller to be able to setup accounts to login. You would then join the computer to the domain and use a login from the central database. The point of having a domain account is to control what can be done on the computer and if you are able to login.

**Local account**

Local account is an account setup on the machine. By default there are some accounts. You can have both. You can have a domain user and then have that user as a local admin so they can perform admin stuff on the computer itself.

User profile is just the profile they use. If you are on the domain or login on locally it will store the profile on the computer itself. You can have roaming profiles though and store them on a server.

Domain account = centrally managed.

Local account = locally managed on the computer itself.

When you login to the machine you can choose to login to the domain or the machine. In vista you have to type .\username to login to the machine with a local account.

**Welcome screen**

The Welcome screen provides a list of accounts on the computer. To log on with one of these accounts, you click the account and type a password (if one is required). Note that the Welcome screen does not display all the accounts that have been created on the computer. Some accounts, such as Administrator, are hidden from view. The Welcome screen is convenient because it displays a list of available accounts. But to enhance security in a homegroup or workgroup, you can use the Logon screen instead of the Welcome screen—therefore not displaying a list of accounts.

**Logon screen**

The Logon screen requires users to type a logon name rather than selecting an account from a list of available accounts. The Logon screen has several features that you can control. By default, the name of the last user to log on is displayed in the User Name field of the Log On To Windows dialog box. You can improve security by hiding the user name of the last user to log on. Instead, users will need to know a valid account name for the computer. To do this, start the Local Security Policy tool from the Administrative Tools menu or type secpol.msc at an elevated command prompt. Then, under Local Policies\Security Options, double-click Interactive Logon: Do Not Display Last User Name. Click Enabled, and then click OK.

You can configure whether the Welcome screen is used through the Always Use Classic Logon setting in Group Policy. For this, you have the following options:

Enable the policy to use the Logon screen rather than the Welcome screen.

Disable the policy to use the Welcome screen.

Use Not Configured to use the default configuration (the Welcome screen).