6.4.8 Windows User Management Facts

This lesson covers the following topics:

- Local user accounts
- Workgroup membership
- Microsoft account sign-in
- Domain account sign-in
- Azure Active Directory account sign-in

Local User Accounts

A local user account can be created and used to sign in and access your Windows 10 computer instead of using a Microsoft account. When you use a local account, some features offered to Microsoft accounts are not available. These include Microsoft's OneDrive and synced settings.

Local user account types include:

Account Type	Description
Administrator	Administrators have complete control of the system and can perform tasks such as: ▪ Change global settings ▪ Create/delete users ▪ Install applications ▪ Run applications in an elevated state ▪ Access all files on the system
Standard User	Standard users have limited permission. For example, standard users can: ▪ Use applications (but they cannot install them) ▪ Change some settings that apply only to them Standard users cannot run applications in an elevated state.

Local accounts can be created using various tools as follows:

Tool	Description
Windows Settings App	To create a local account on a computer not joined to a domain: 1. Right-click Start, select Settings, and then choose Accounts. 2. Select Family & other users (or Other users if the computer is joined to a domain). Then select Add someone else to this PC. 3. Follow the remaining steps to enter the name and password for the new user.
Computer Management	To create a local account: 1. Right-click Start and then select Computer Management. 2. From Computer Management, expand Local Users and Groups. 3. Right-click Users and then select New User.

	4. Complete the required options and click Create. With this tool you are not required to use security questions. This method also gives you the ability to: ▪ Force users to change the password at the next sign-in ▪ Restrict the user from changing the password ▪ Allow the password to never expire ▪ Disable/enable an account

Workgroup Membership

When working in an environment where multiple computers are connected on a network, one method of sharing resources between computers is to use a workgroup. A workgroup is Microsoft's implementation of peer-to-peer networking. Although using domains is the preferred method, workgroups can be useful in small environments of about two to eight computers. Anything larger than that begins to be an administrative challenge.

When using workgroups, consider the following:

- Workgroups provide only sign-in security.
- No username or password is required to join a workgroup.
- Computers that belong to the same workgroup can share resources only if they are on the same segment.
- Workgroups have no centralized authentication. This means that for a user to access a remote system, the same username and password must be created on the remote system. Otherwise, each user would need to know the username and password on the remote system.
- If a domain is not used, the computer is a member of the workgroup named Workgroup by default.

To make a computer a member of a workgroup:

1. Access the System Configuration app.
   - Right-click Start and then select System.
   - From the right pane, select System info under Related settings.
2. Under Computer name, Domain, and Workgroup settings, select Change settings.
3. From the Computer Name tab, click Change. Next, enter the name of the desired workgroup and click OK.

Microsoft Account Sign-In

With Windows 10, Microsoft's preferred method of signing onto a system is to use a Microsoft account. Microsoft accounts use a single sign-on system. This means that you can sign into different systems while maintaining the same user settings and password. You can even access your favorites websites. Microsoft accounts also provide synchronized access to other Microsoft services such as Office 365, Outlook, Skype, OneDrive, Xbox Live, Bing, and Microsoft Store.

Microsoft accounts can be created using an existing email address or by signing up for a Microsoft email address. You can also use a phone number instead of an email address. If your Windows system was originally configured to sign in using a local account, you can switch to a Microsoft account by doing the following:

1. Select the Start menu and go to Settings > Accounts > Your info.
2. Select Sign in with a Microsoft account instead. (Note: if you see Sign in with a local account instead, you're already using your Microsoft account.)
3. Follow the prompts to switch to your Microsoft account. If needed, you can create a Microsoft account at this time.

To switch from a Microsoft account back to a local account, right-click Start and go to Settings > Accounts > Your info. Then select Sign in with a local account instead and follow the prompts.

Domain Account Sign-In

In addition to local and Microsoft account sign-ins, you can also sign into a Windows system using a domain account. Domain accounts are created and stored in Active Directory on a domain controller server. This provides central management of users and group.

When using a domain user account to sign into your system, the username and password entered are sent to the domain controller. The domain controller then checks to see if the username and password submitted match the credentials it has for that particular user. If they do match, it sends a message back to the local system verifying the credentials, and the user is allowed to sign into the system. Before a user can sign in using a domain account, the domain user account must have already been created in Active Directory and the computer must have been joined to the desired domain.

To sign in using a domain account, you need to specify the domain to which you want to sign into. If this is the first time you are signing into the domain, or you want to make sure you are signing into the correct domain, select Other user from the sign-in screen. From this dialog, a known domain will be shown.

If the domain shown is the one you want to use, enter the username and password in the applicable fields. However, if the domain listed is not correct, you can change domains by specifying the correct domain in the username field using the syntax of domain\username. For example, to sign into the ACME domain using the Admin account, in the username field you would type **AMCE\Admin**. As soon as you type the backslash, the name of the domain is shown in the Sign in to area.

Azure Active Directory Account Sign-In

Azure Active Directory (Azure AD) is a cloud-based identity and access management service provided by Microsoft. It is similar to on-premises Active Directory except that Azure AD runs in Microsoft's Azure cloud. With Azure AD, users can sign in and access both internal and external resources. Internal resources include such things as the applications on a corporate network. External resources includes such things as Microsoft Office 365 and other Software as a Service (SaaS) applications.

As with on-premises Active Directory, to use Azure AD a user account must be created in Azure AD and the local computer must be joined to the Azure AD domain.

To join a device to Azure Active Directory:

- Right-click Start and then go to Settings > Accounts.
- Select Access work or school and select Connect.

- Select Join this device to Azure Active Directory.
- Follow the remaining prompts to complete the process.

After joining the computer to Azure AD, you sign in using the same steps as you would to sign into a local domain. The only difference is that you use the Azure AD domain.

Copyright © 2022 TestOut Corporation All rights reserved.