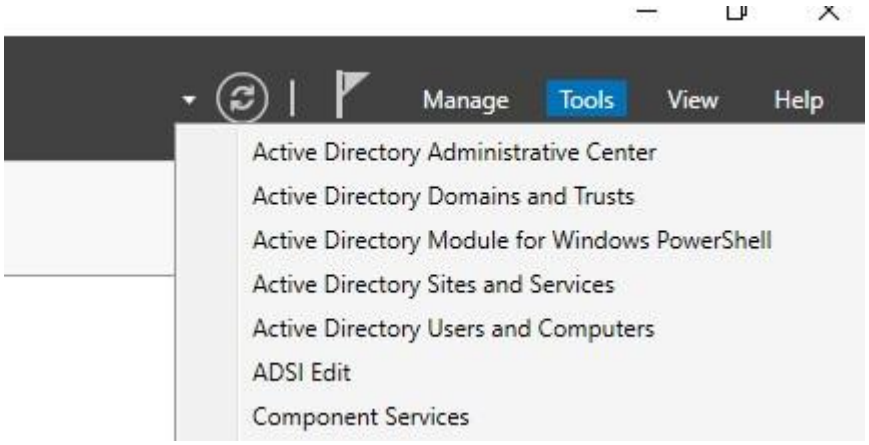
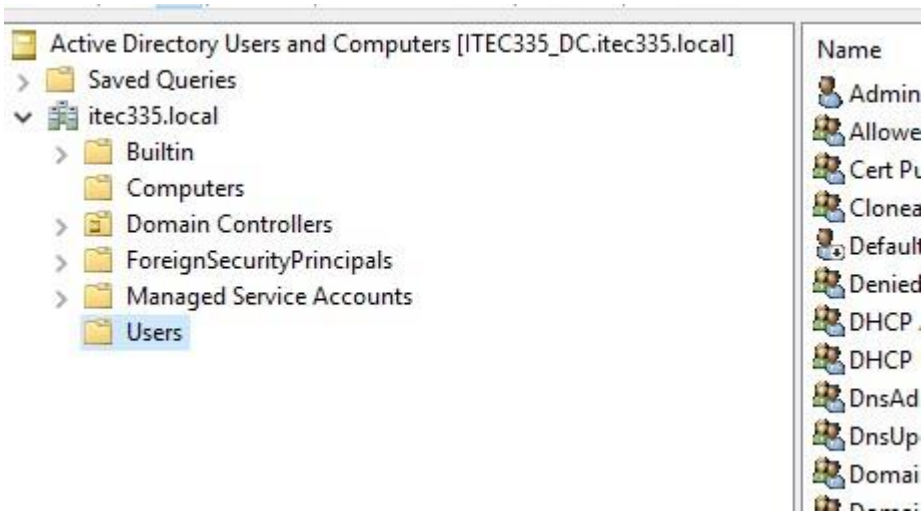
Windows Lab
Adding User Objects
ITEC 235

Creating a User object using Active Directory Users and Computers

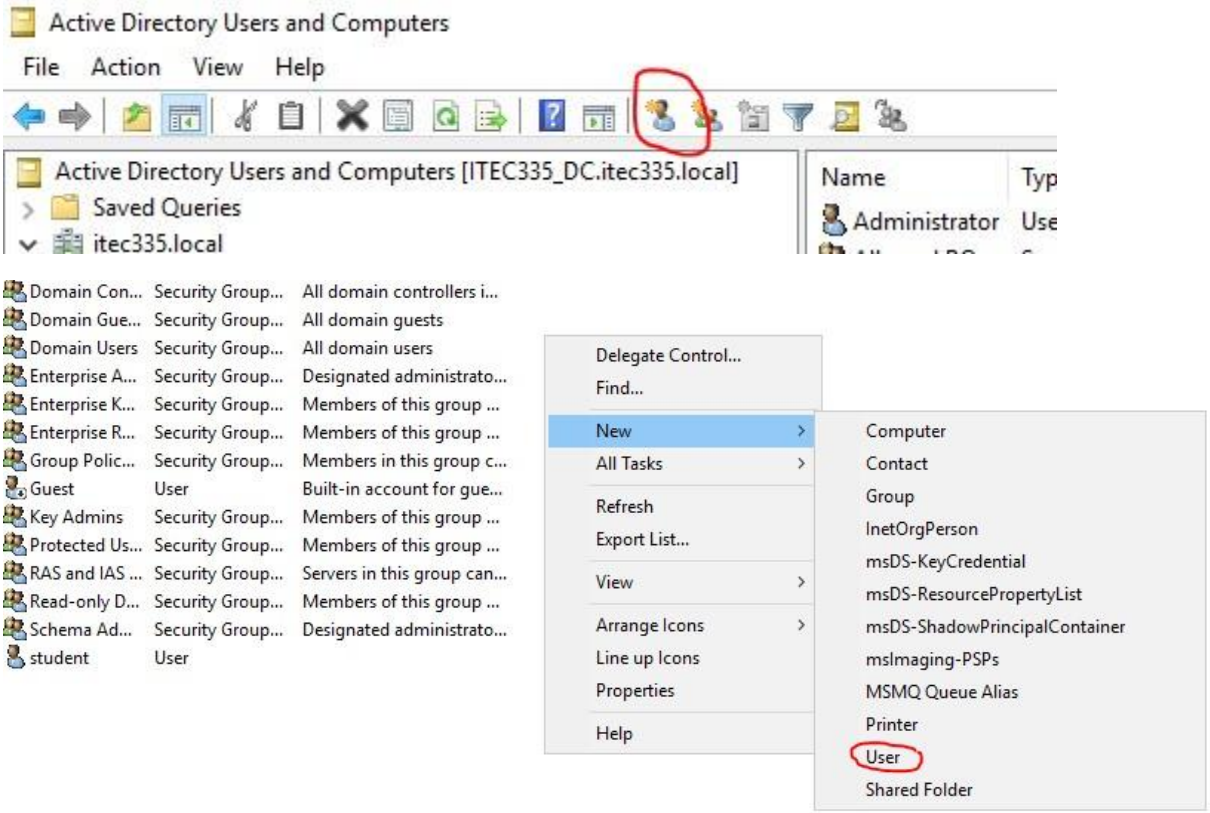
Like most things in Windows Land, there are multiple ways to add a user account. The most intuitive way to add a user is by using the *Active Directory Users and Computers Microsoft Management (MMC)* snap-in. You can access this from *Server Manager* by first clicking on *Tools* and then selecting *Active Directory Users and Computers*.



Once *Active Directory Users and Computers* opens, click the *Users* folder in the column on the left.



From here we can add a user using one of two methods. You can simply click on the *Create new user in the current container* link from the tool bar, or you can right click in the white space of the pane on the right and select *New* then *User*.



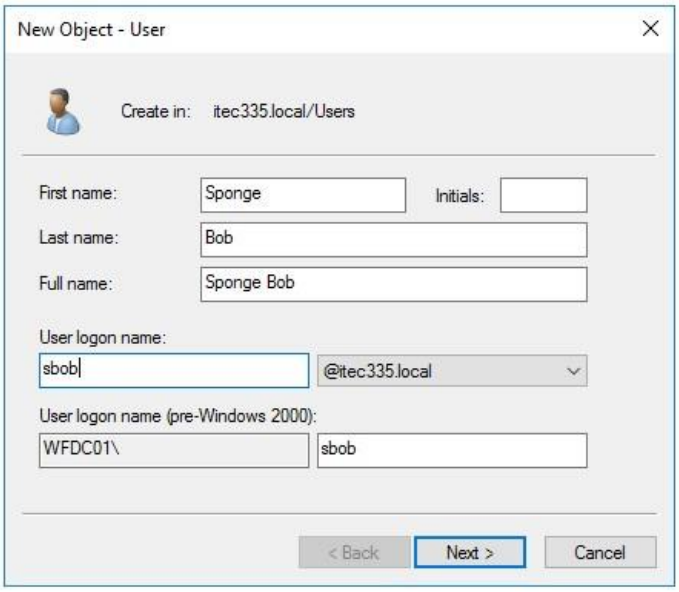
Using the method you prefer, create a new user using the following information:

First Name: *Sponge*
Last Name: *Bob*
User logon name: *sbob*

Click *Next*

Enter an easy to remember password. I recommend *Changeme2020*

Uncheck the box next to *User must change password at next logon*. This option prompts the user for a password change at logon. Click *Next* and *Finish*.



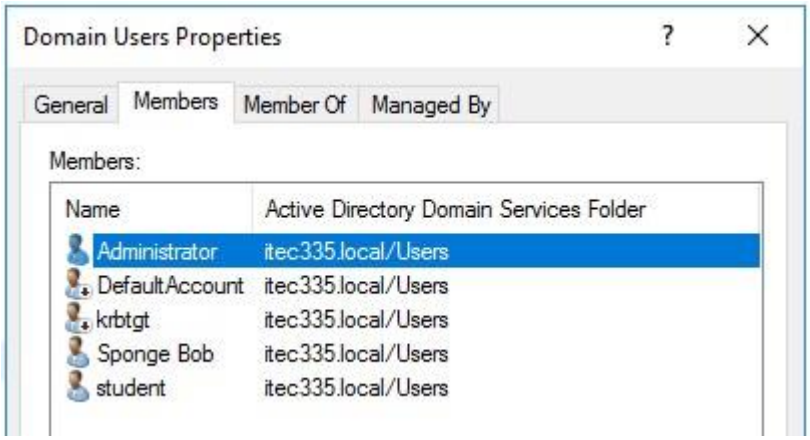
You should now see the new user object you just created. If you do not, click the refresh button found in the tool bar.

Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group...	Members of this group ...
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...
Read-only D...	Security Group...	Members of this group ...
Schema Ad...	Security Group...	Designated administrato...
Sponge Bob	User	
student	User	

Double click on the *Sponge Bob* user object. You will notice that you now have several more tabs than you did when you were initially creating the user account. Spend some time exploring the various tabs. Note the *Unlock account* check box found on the *Account* tab.

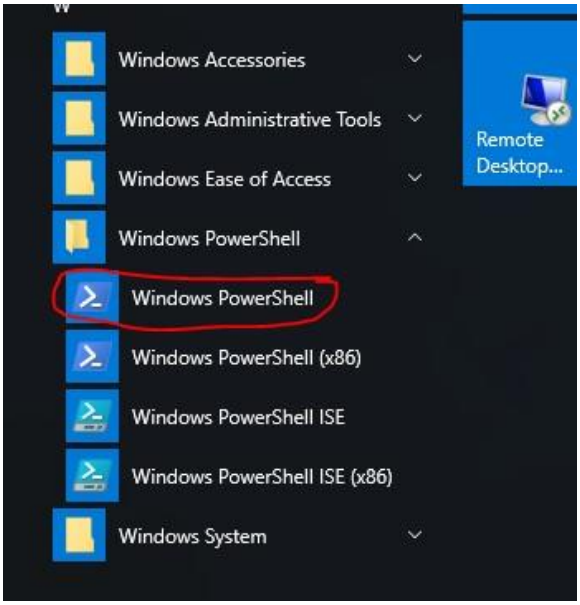
Now click the *Member Of* tab. You will notice that Sponge Bob belongs to the *Domain Users* group. This means that *Sponge Bob* is authorized to access and modify anything assigned to the *Domain Users* group object. Click *Cancel* to close the Sponge Bob Properties dialog box.

Double click the *Domain Users* group, which *Sponge Bob* belongs too. Click the *Members* tab to display the objects that are members of the *Domain Users* group. You will notice that *Sponge Bob* is listed as a member. We can use this tab to quickly determine the users that belong to a specific group. Click cancel to close the Domain Users Properties dialog box.



Creating a User object using PowerShell

Another way that we can add users is by using PowerShell. To open PowerShell you can either use *Windows Search*, or you can select it from the *Start Menu*. You will find *Windows PowerShell* in the *Windows PowerShell group* on the *Start Menu*. Both methods are illustrated below.



This may be the first time you have used PowerShell. Therefore, we will begin this section of the lab by exploring a few of the features of PowerShell. To get help with help, simply type **`help`** and press *Enter*. Entering this command displays a help file that describes the various ways of accessing help. To access the help file for displaying a list of AD users, enter the following command: **`help get-aduser`** and press *Enter*. To scroll through the text, you can use the *Enter* key to scroll one line at a time or you can use the *Space Bar* to scroll an entire page.

To display a list of all users in Active Directory, we can use the following command: **`get-aduser -filter *`** after typing the command, press *Enter*. In this command, the * is a wild card character that means “all”.

```
Administrator: Windows PowerShell

PS C:\Users\Administrator>  get-aduser -filter *

DistinguishedName : CN=Administrator,CN=Users,DC=itec335,DC=local
Enabled           : True
GivenName         :
Name              : Administrator
ObjectClass       : user
ObjectGUID        : a0ecf21f-4f99-4da1-bde3-e3aeee1b3d70
SamAccountName    : Administrator
SID               : S-1-5-21-3581384273-2017186728-3935983078-500
Surname           :
UserPrincipalName :

DistinguishedName : CN=Guest,CN=Users,DC=itec335,DC=local
Enabled           : False
GivenName         :
Name              : Guest
ObjectClass       : user
ObjectGUID        : 7dcc9d49-be60-4dcd-97cb-c4f4a1c32ced
SamAccountName    : Guest
SID               : S-1-5-21-3581384273-2017186728-3935983078-501
Surname           :
UserPrincipalName :

DistinguishedName : CN=DefaultAccount,CN=Users,DC=itec335,DC=local
Enabled           : False
GivenName         :
Name              : DefaultAccount
ObjectClass       : user
ObjectGUID        : fd36ff20-ed36-408a-8572-c4cf9cb4d044
SamAccountName    : DefaultAccount
SID               : S-1-5-21-3581384273-2017186728-3935983078-503
Surname           :
UserPrincipalName :

DistinguishedName : CN=student,CN=Users,DC=itec335,DC=local
Enabled           : True
GivenName         :
Name              : student
ObjectClass       : user
ObjectGUID        : e99b2e51-8218-4acd-8ef3-0c9f904881ad
SamAccountName    : student
SID               : S-1-5-21-3581384273-2017186728-3935983078-1000
Surname           :
UserPrincipalName :

DistinguishedName : CN=krbtgt,CN=Users,DC=itec335,DC=local
```

If you want to display a single user in Active Directory, replace the ***** with search criteria (Remember: Active Directory is a database). For example, to display the Sponge Bob user we created earlier, enter the following command: **`get-aduser -filter 'Name -like "Sponge Bob"'`** and press *Enter*.

```
PS C:\Users\Administrator> get-aduser -filter 'Name -like "Sponge Bob"'


DistinguishedName : CN=Sponge Bob,CN=Users,DC=itec335,DC=local
Enabled           : True
GivenName         : Sponge
Name              : Sponge Bob
ObjectClass       : user
ObjectGUID        : 11583a2c-6905-42b1-a697-d5f2ffcef7a2
SamAccountName    : sbob
SID               : S-1-5-21-3581384273-2017186728-3935983078-1108
Surname           : Bob
UserPrincipalName : sbob@itec335.local


PS C:\Users\Administrator> _
```

Use the following command to create a user account for Patrick Star:

`new-aduser` and press *Enter*. After you press Enter, you will be prompted for the name of the new user. Type **`Patrick Star`** and press *Enter*. You can view the user object you just created by using the following command: **`get-aduser -filter 'Name -like "Patrick Star"'`**

```
PS C:\Users\Administrator> new-aduser

cmdlet New-ADUser at command pipeline position 1
Supply values for the following parameters:
Name: Patrick Star
PS C:\Users\Administrator> get-aduser -filter 'Name -like "Patrick Star"'


DistinguishedName : CN=Patrick Star,CN=Users,DC=itec335,DC=local
Enabled           : False
GivenName         :
Name              : Patrick Star
ObjectClass       : user
ObjectGUID        : dc2ee049-4030-48d0-93ad-6806d1465c2e
SamAccountName    : Patrick Star
SID               : S-1-5-21-3581384273-2017186728-3935983078-1110
Surname           :
UserPrincipalName :
```

Did you happen to notice that *Enabled* contains the value *False*? This user account is not yet enabled. Since we have not entered a password for this user, the account defaults to disabled. To change (set) the password for this user, enter the following command (all one line):

`Set-adaccountpassword -identity 'Patrick Star' -reset -newpassword (convertto-securestring -asplaintext "ChangeMe2020" -Force)`

Once you have set a password, you can enable the Patrick Star account by entering the following command: **`enable-adaccount -identity "Patrick Star"`**

Verify that Patrick Star is enabled by typing the following:

`get-aduser -filter 'Name -like "Sponge Bob"'` and press *Enter*. *Hint: You can press the up arrow to cycle through previously entered commands.*

```
PS C:\Users\Administrator> enable-adaccount "Patrick Star"
PS C:\Users\Administrator> get-aduser -filter 'Name -like "Patrick Star"'


DistinguishedName : CN=Patrick Star,CN=Users,DC=itec335,DC=local
Enabled           : True
GivenName         :
Name              : Patrick Star
ObjectClass       : user
ObjectGUID        : dc2ee049-4030-48d0-93ad-6806d1465c2e
SamAccountName    : Patrick Star
SID               : S-1-5-21-3581384273-2017186728-3935983078-1110
Surname           :
UserPrincipalName :
```

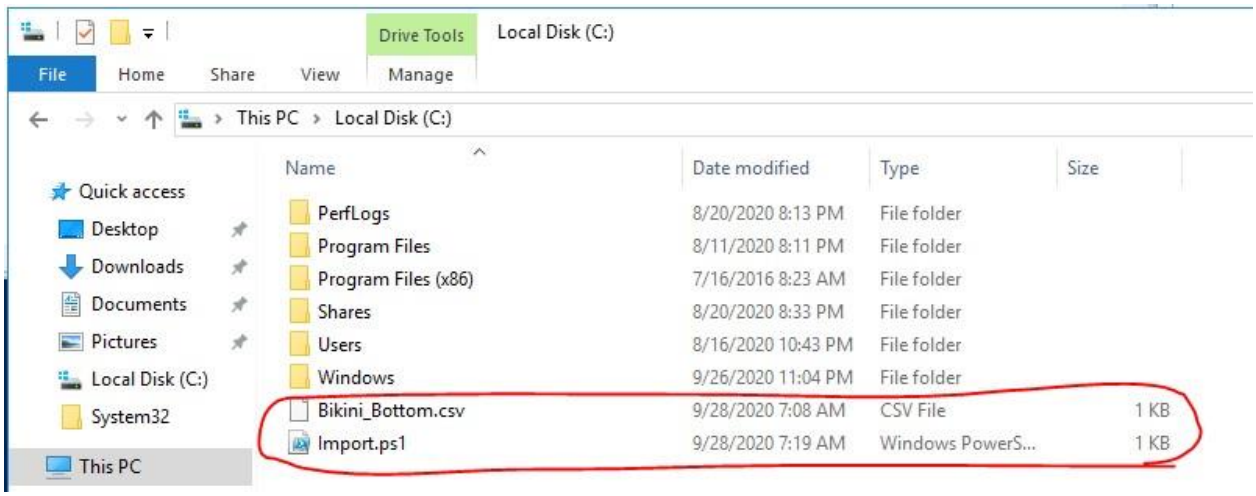
You may be wondering if this is the way that most network administrators use to create user accounts. The answer to that is yes and no. It depends if you are creating a few users or several users. If you are simply creating a small number of users (1-10), then using the graphical AD Users and Groups method is the more efficient method. However, if you are creating several user accounts, then a PowerShell script is the more efficient method.

In the next session, you will create a script that will add users listed in a comma separated values (CSV) file.

Using a PowerShell Script to Create Multiple User Accounts

For this section of the lab, we will use PowerShell ISE instead of PowerShell. PowerShell ISE is the PowerShell Integrated Scripting Engine. This tool provides a convenient way to create and debug scripts. You can find *PowerShell ISE* in the *Windows PowerShell group* on the *Start Menu*. Once you have PowerShell ISE open, click the *New* icon in the tool bar.

Your display should now include a text editor in the upper pane. Using the *Save* icon (Floppy Disk) in the tool bar, save the new text file to the C: partition of your server. You should also save the provided "Bikini_Bottom.csv" file to the C: partion of your server.



With both files save to the C: partition of your server, we are now ready to proceed. We will begin by displaying the properties of the Sponge Bob user we created earlier. We do this by entering the following command: **`Get-ADUser sbob -Properties *`**

This command displays the fields and attributes for the Sponge Bob user. Scroll through the list until to the PrimaryGroup field. Record the attribute for your users. We will use this in future steps.

```
PasswordNotRequired                  : False
POBox                                :
PostalCode                           :
PrimaryGroup                         : CN=Domain Users,CN=Users,DC=itec335,DC=local
primaryGroupID                       : 513
PrincipalsAllowedToDelegateToAccount : {}
ProfilePath                          :
ProtectedFromAccidentalDeletion      : False
```

In the example above, the domain name is itec335.local. Yours will most likely be different. We need to edit the Bikini_Bottom.csv file to include the domain name used by your server. The next paragraph provides instructions to complete this task. Feel free to use any method you prefer.

> Right click on the *Bikini_Bottom.csv* that you copied to the root of C: on your Server 2016 installation and click *Edit.* Click in the white space of the opened *Bikini_Bottom.csv* file. Hold *CTRL* and press the *h* key. This will open the *Replace* dialog box. Type itec335.local in the *Find what:* field and type the name of your DC in the *Replace with:* field. Press the *Replace All* button. Click *File* and *Save*.

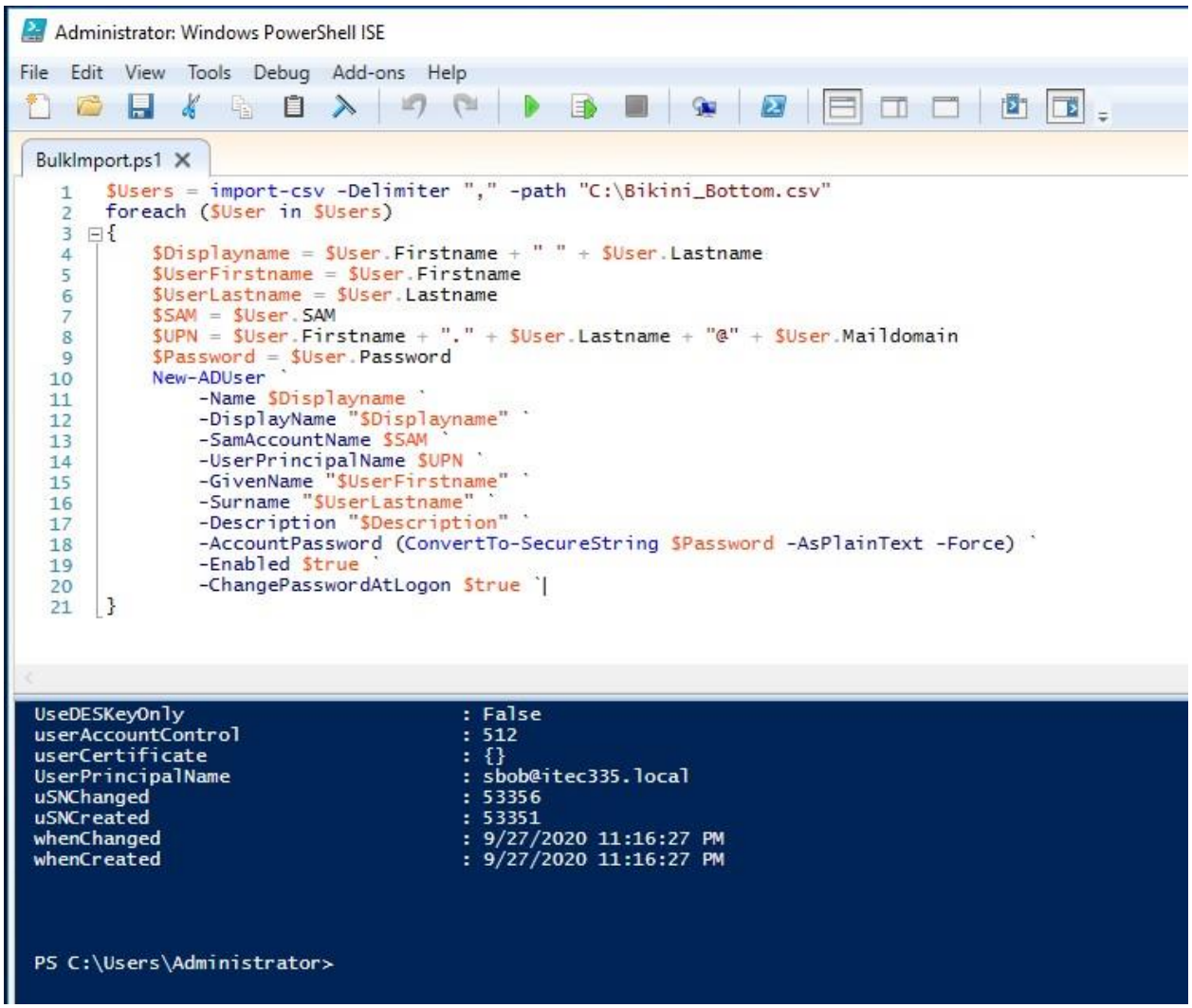
After you have modified the provided CSV file to include your domain, copy or type the script below into the text editor space of Windows PowerShellISE. Notice the back quotes used after each line starting with "New-ADUser". This is the mark below the tilde next to the number 1 key. See the blue key in the illustration to the right.

The backquote allows you to continue a command on the next line.

```
$Users = import-csv -Delimiter "," -path "C:\Bikini_Bottom.csv"
foreach ($User in $Users)
```

```
{
    $Displayname = $User.Firstname + " " + $User.Lastname
    $UserFirstname = $User.Firstname
    $UserLastname = $User.Lastname
    $SAM = $User.SAM
    $UPN = $User.Firstname + "." + $User.Lastname + "@" + $User.Maildomain
    $Password = $User.Password
    New-ADUser `
        -Name $Displayname `
        -DisplayName "$Displayname" `
        -SamAccountName $SAM `
        -UserPrincipalName $UPN `
        -GivenName "$UserFirstname" `
        -Surname "$UserLastname" `
        -Description "$Description" `
        -AccountPassword (ConvertTo-SecureString $Password -AsPlainText -Force) `
        -Enabled $true `
        -ChangePasswordAtLogon $true ` }
```

You should now have the following:



Once you are satisfied with your script, press the green Run Script button in the PowerShell ISE toolbar <u>or</u> press F5.

If you entered everything correctly, the script will run add the new users to Active Directory. If not, you may have to read through the red text to determine what has been typed incorrectly.

Success looks like this:

```
PS C:\Users\Administrator> C:\Users\Administrator\Desktop\BulkImport.ps1

PS C:\Users\Administrator>
```

It may be necessary to refresh the Active Directory window to display the new users.

Enterprise Read-only Domain Controllers	Security Group...	Members of this group ...
Eugene Krabs	User	
Gary Snail	User	
Group Policy Creator Owners	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Karen Plankton	User	
Key Admins	Security Group...	Members of this group ...
Misses Puff	User	
Patrick Star	User	
Pearl Krabs	User	
Protected Users	Security Group...	Members of this group ...
RAS and IAS Servers	Security Group...	Servers in this group can...
Read-only Domain Controllers	Security Group...	Members of this group ...
Sandy Cheeks	User	
Schema Admins	Security Group...	Designated administrato...
Sheldon Plankton	User	
Sponge Bob	User	
Squidward Tentacles	User	
student	User	

To complete this project, submit a screen capture like the one above that shows the users you added.