Windows security, Active Directory and Azure AD

TD16 – Module 4 – Section 2

June 2020

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The names of manufacturers, products, or URLs are provided for informational purposes only, and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links may be provided to third-party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

This training uses various tools and utilities downloaded from the Internet for the classroom environment.   
Downloading any tools, installing and using them should only be done at your own risk security checked the tools in a test environment.

© 2020 Microsoft Corporation. All rights reserved.

Microsoft and the trademarks listed at <https://www.microsoft.com/en-us/legal/intellectualproperty/Trademarks/Usage/General.aspx> are trademarks of the Microsoft group of companies. All other trademarks are the property of their respective owners.

Contents

[Hybrid Identity lab using Azure AD 1](#_Toc44074163)

[Abstract and learning objectives 1](#_Toc44074164)

[Overview 2](#_Toc44074165)

[Requirements 2](#_Toc44074166)

[Before the exercises 3](#_Toc44074167)

[List of VM to start 3](#_Toc44074168)

[How to start and connect to a VM 4](#_Toc44074169)

[Exercise 1: Setup a new Azure AD Directory 6](#_Toc44074170)

[Task 1: Register for a new Office 365 trial subscription 6](#_Toc44074171)

[Task 2: Basic Azure Active Directory User Management using the portal 9](#_Toc44074172)

[Task 3: Basic Azure Active Directory User Management using Powershell 10](#_Toc44074173)

[Task 4: Enable MFA for administrative accounts 12](#_Toc44074174)

[Exercise 2: Enable Hybrid Identity 13](#_Toc44074175)

[Task 1: Setup Azure AD Connect 13](#_Toc44074176)

[Task 2: Observe a synchronization round 16](#_Toc44074177)

[Task 3: Filter out objects from the synchronization process 17](#_Toc44074178)

[After the Lab 19](#_Toc44074179)

[Task 1: Stop and deallocated all the VMs 19](#_Toc44074180)

# Hybrid Identity lab using Azure AD

## Abstract and learning objectives

This lab walks the reader through the step-by-step process of building a hybrid identity lab (Hybrid AD) using Azure Active Directory and Windows Server Active Directory. It builds upon knowledge gained from other classes for Active Directory and Azure Active Directory, and once completed, will allow the reader to be familiar with fundamental Azure Active Directory concepts and operations.

## Overview

In this Lab, attendees will create a new Azure AD tenant, enable synchronization between this tenant and an existing Active Directory domain and perform common Azure AD administration tasks.

## Requirements

1. Attendee’s machine:
   1. Ideal resolution 1920 x 1080
   2. An Internet browser
   3. An RDP client
   4. Internet access without restriction on outbound connections.   
      The following outbound TCP port must be accessible :

* **TCP/80 and TCP/443** to reach Azure Portal
* **TCP/3389** to establish RDP remote connection to virtual machines exposed directly to Internet

or

* **TCP/(49152 to 65535)** to establish RDP remote connection to virtual machines exposed by a Load Balancer

## Before the exercises

Duration: 10 minutes

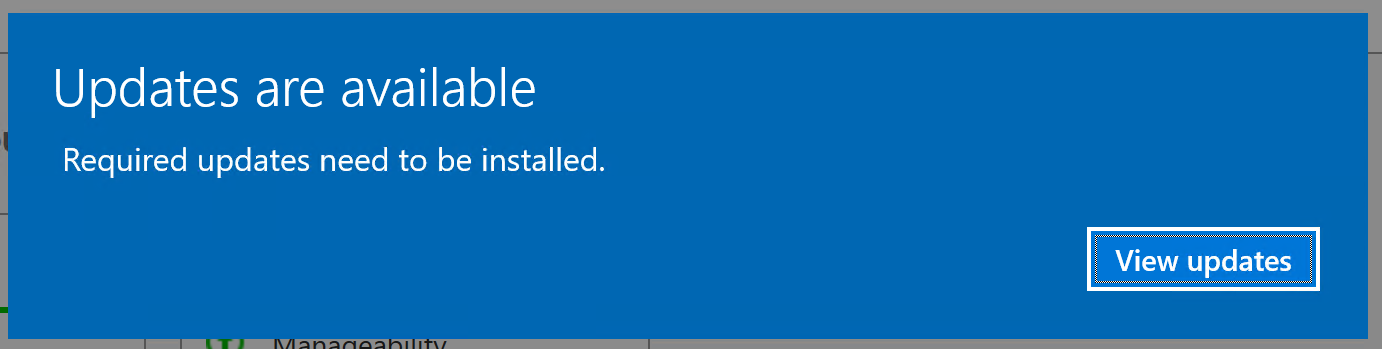
Synopsis: In this section, you will set up your environment for use in the rest of the Lab. You should have the following environment.

#### List of VM to start

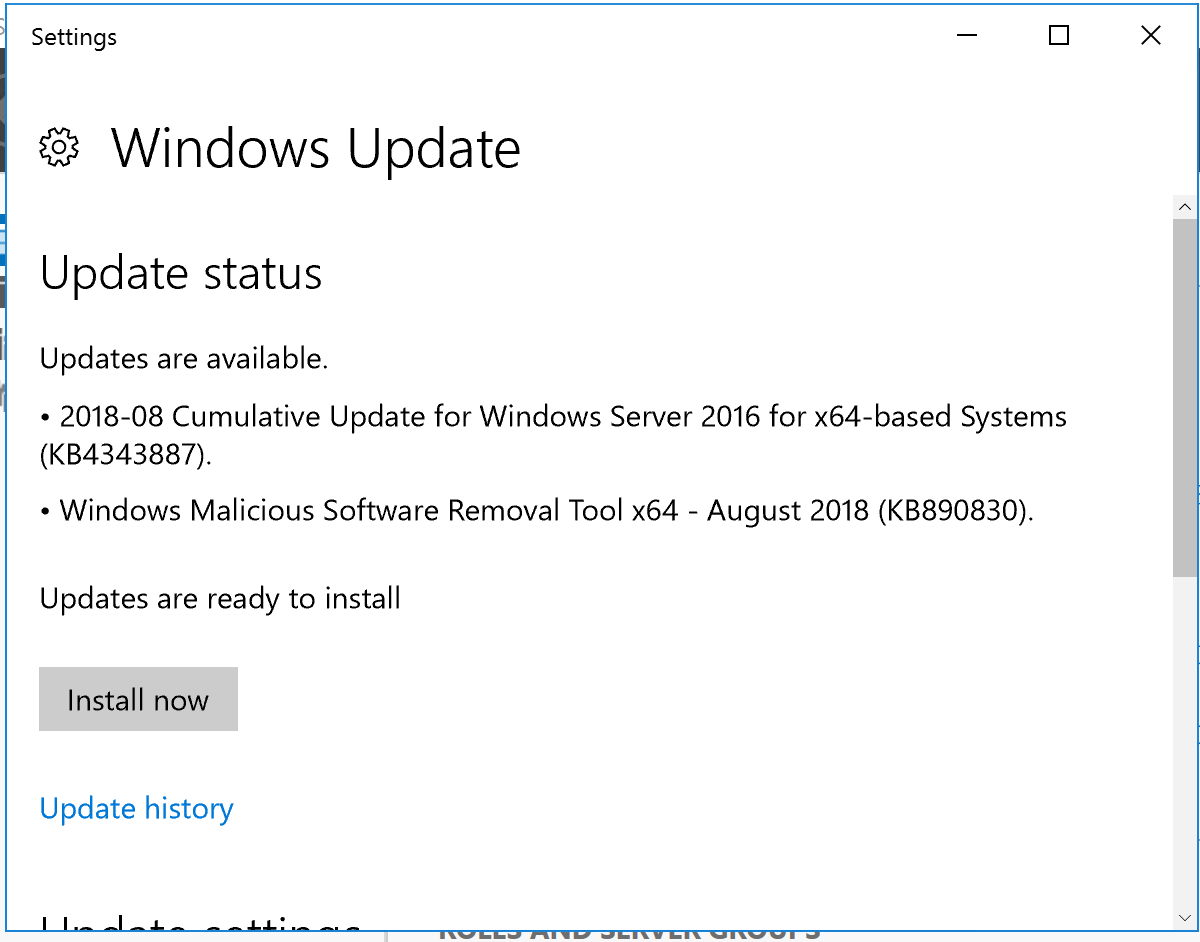
**Remember to start the in first and to wait 1 minute before starting the other VMs.**

|  |  |  |  |
| --- | --- | --- | --- |
| Name of VM | Hostname | OS Type | Role |
| ID-DC1 | CSI-TD-DC1 | Windows Server 2016 Standard | AD |
| ID-SRV1 | CSI-TD-SRV1 | Windows Server 2016 Standard | Server |

Note that the machines have been provisioned in March 2020.   
Therefore, it is possible to see the following message while connecting for the first time to the servers:



In this case, click on View updates.



We do not need the latest updates for these labs, so you can close this window.

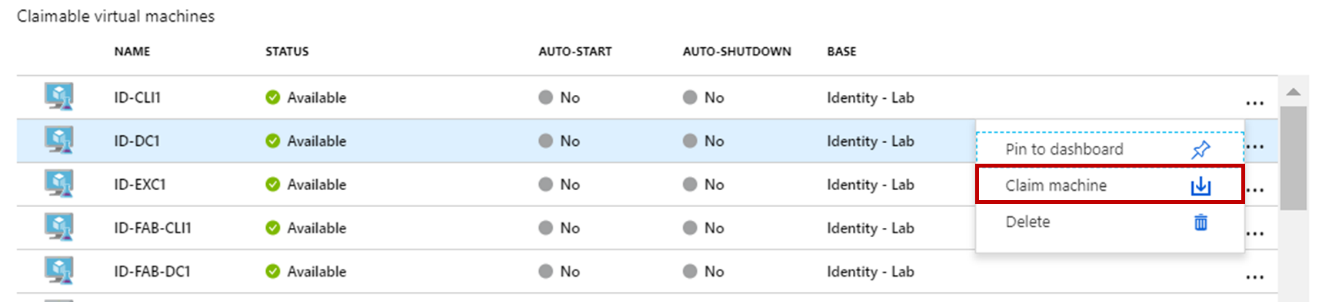
## 

#### How to start and connect to a VM

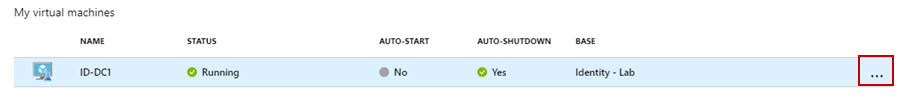
1. Go to Azure portal: <https://portal.azure.com>
2. Sign-in with your student or organizational account
3. Click on the Dev&Test Lab (Select the right subscription if the resource is not displayed)



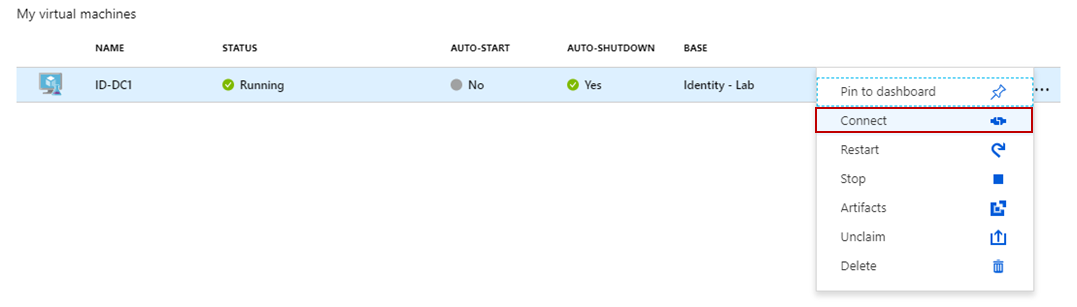
1. To start a VM, click on “Claim machine”



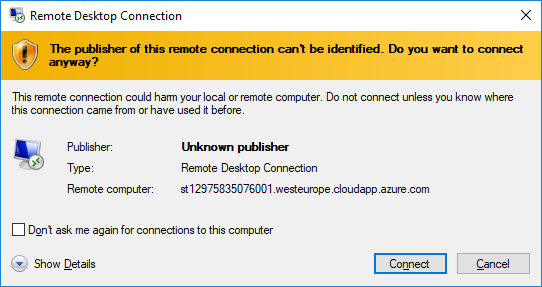
1. When the machine is started, it will be displayed in the “My Virtual Machines” pane.   
   After one minute, the status will be Running. You can wait 30 seconds more before trying to connect on it.



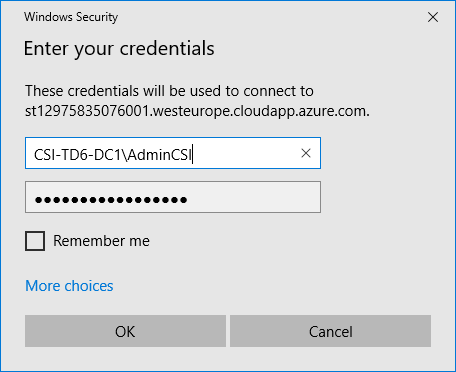
1. Select the running Virtual Machine and at the end of line, click on “…” then select Connect



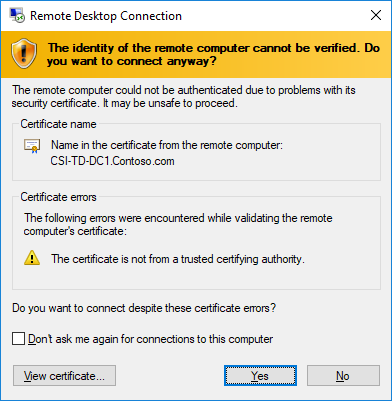
1. A warning is displayed about the publisher. You can ignore the warning and click on Connect.



1. Enter the user name and password to connect to the Virtual Machine detailed in each exercise below.   
   (Do not use your student or organizational account.)



1. A warning on the self-issued certificate is displayed. You can safely ignore this warning by clicking on Yes.



## Exercise 1: Setup a new Azure AD Directory

Duration: 15 minutes

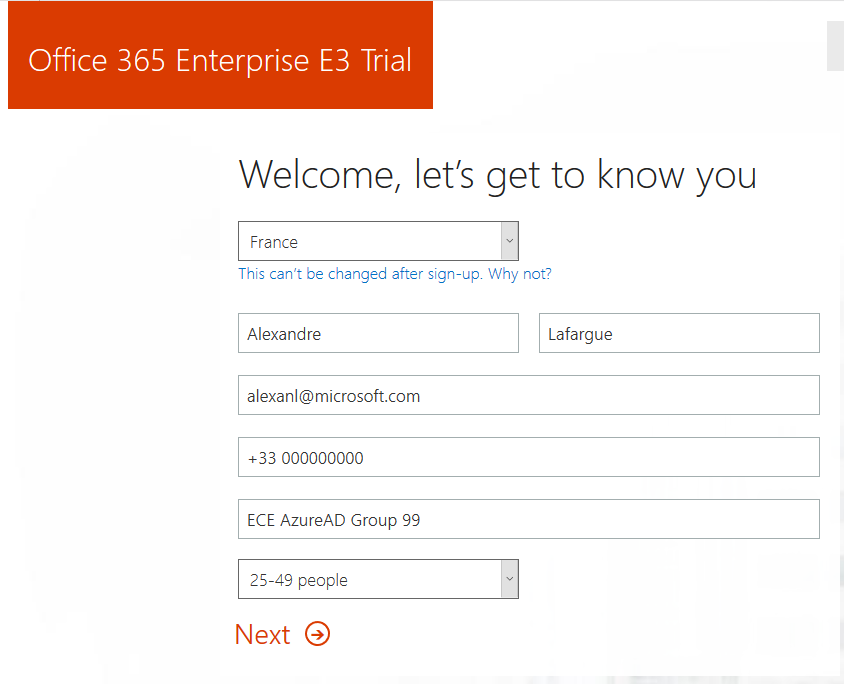
Synopsis: In this exercise, you will learn how to setup a basic Azure Active Directory tenant. You will use a trial Office 365 Enterprise subscription. Each Office 365 subscription has a shadow Azure AD tenant in order to support user’s authentication and identity management. In this lab, you will use only features from Azure AD.

#### Task 1: Register for a new Office 365 trial subscription

In this task, you will create your Office 365 subscription. This is purely configuration. There is no question to answer.

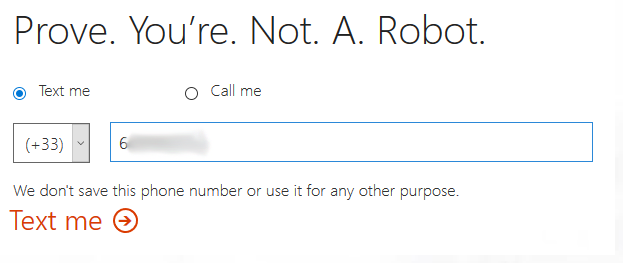
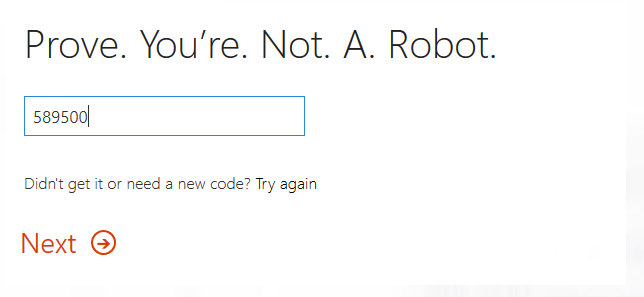
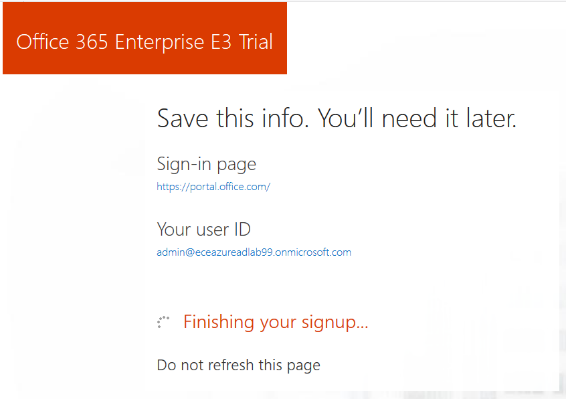
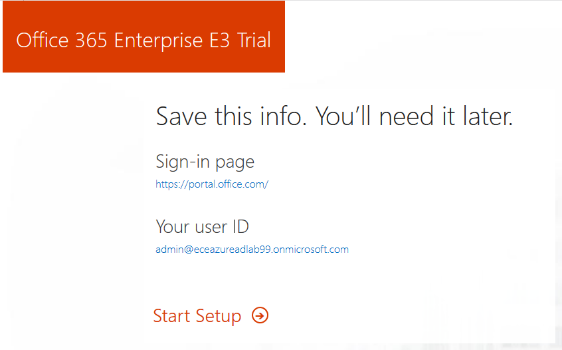
**Important:** Unless you are currently signed in with your Office 365 trial subscription, ensure you sign out from any other Microsoft service you are currently signed in and clear your browser’s cookies. Otherwise, the portals will try to use your organizational credential which will fail.

1. Go to <https://go.microsoft.com/fwlink/p/?LinkID=403802&culture=en-US&country=US>
2. Fill in the registration form, all fields are mandatory
   1. For the Country or Region drop list, ensure you select the country you are living in. This cannot be changed after subscription is created
   2. Ensure you put a valid email address

You should end up with a screen like:  


1. Click **Next**. On the **Create your User ID** page, fill in the form in order to create the first account of the subscription. This account will be an administrator account. Ensure you choose a complex password.

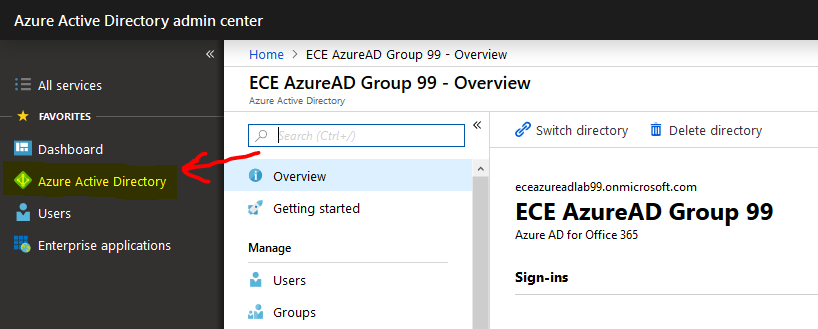
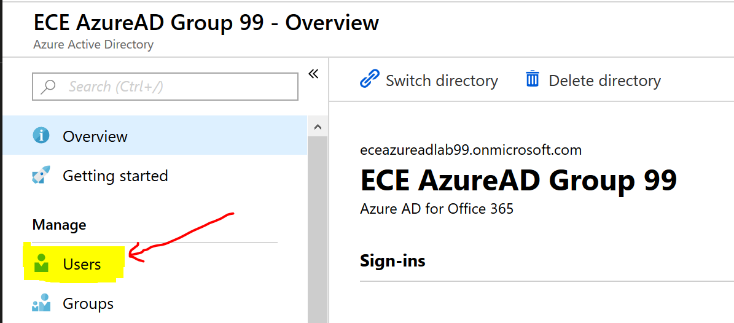
|  |  |
| --- | --- |
|  | Note1: As you are running a lab and not a commercial evaluation, ensure you unselect contact options so that you are not called back by pre-sales staff.  Note 2: Ensure you select **admin** as the user name to stay coherent with the rest of this document  Note 3: Even if you are free to choose any name for the *.onmicrosoft.com* domain, it is highly recommended to avoid short or common names which could prevent commercial users to register their company or trademarks. We do recommend you name your domain as:  *org\_name*azureadlab*group*.onmicrosoft.com  org\_name being few letters matching your organization’s name  group being your group number on 2 digits. Eg: eceazureadlab99.onmicrosoft.com |

1. In the next page, enter a valid mobile phone number and click **Text Me**. A text message will be sent to you for verification purpose  
   
2. Enter the code you received on your mobile phone and click **Next**  
   
3. Your subscription is going to be created. This can take some time.  
   
4. When, the subscription creation process is terminated, you should end with a similar screen. There is no need to click on **Start Setup**.  
   

#### Task 2: Basic Azure Active Directory User Management using the portal

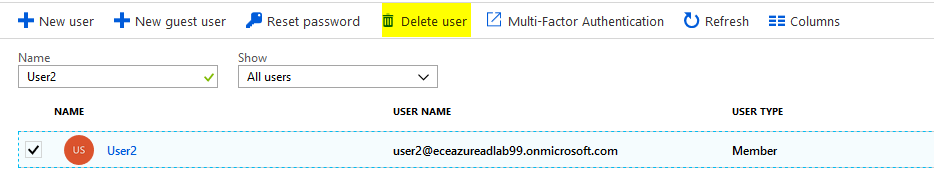
In this task, you will train yourself in basic account management tasks like user and group creation using the Azure AD portal. There are some questions at the end of the task.

**Important:** Unless you are currently signed in with your Office 365 trial subscription, ensure you sign out from any other Microsoft service you are currently signed in and clear your browser’s cookies. Otherwise, the portals will try to use your organizational credential which will fail.

1. Sign in to Azure AD by browsing <https://aad.portal.azure.com> and by using the credential you created in previous task.
2. When in the Azure portal, select the Azure Active Directory blade  
   
3. Select the **Users** section from the **Manage** group  
   
4. Using the documentation located at <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/>, perform the following:
   1. Create a new user with the following data:
      1. Name: Admin2
      2. User name: admin2@*your\_subscription\_domain*
      3. Directory role: Global administrator
   2. Create a new user with the following data:
      1. Name: User1
      2. User name: user1@*your\_subscription\_domain*
      3. Directory role: User
   3. Create a new user with the following data:
      1. Name: User2
      2. User name: user2@*your\_subscription\_domain*
      3. Directory role: User

**Notes:**

* **Ensure you display and save the generated password before creating the account. Otherwise, you won’t be able to sign in with the account.**

1. Now, clear all the cookies and session state in your browser or, open a new inPrivate session and go to <https://portal.office.com>  
   Note: If you fail to properly clear existing cookies, you will be automatically signed in with your current account.
2. Try signing in with **Admin2** accounts
3. Now, you will simulate an accidental deletion of account **user2**. Select **User2** from the user list and select **Delete user**  
   
4. Using the same documentation, try to restore **User2**.

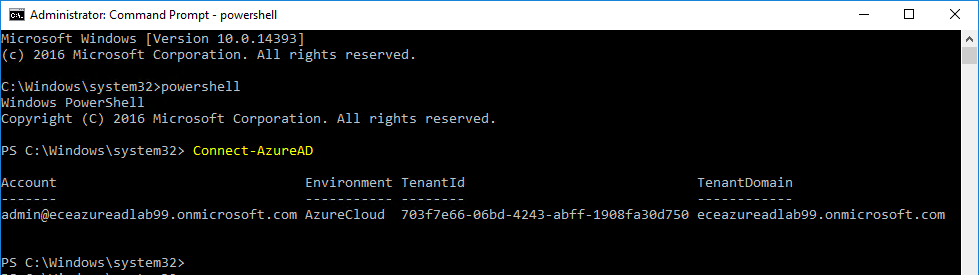
Additional Questions:

1. When you first signed in with **Admin2** account, what did you have to do before accessing the portal?
2. Suppose a user forgets its password,
   1. What can you do to help him/her?
   2. Describe what would be the necessary steps.
3. How much time does a deleted account remains in the suspended state?
4. Can you restore a permanently deleted user?

#### Task 3: Basic Azure Active Directory User Management using Powershell

In this task, you will use Powershell and the Azure AD module to perform common administrative task in your Azure AD subscription.

Reference documentation is located at : <https://docs.microsoft.com/en-us/powershell/module/azuread/?view=azureadps-2.0>

1. Sign in **CSI-TD-SRV1** with following credentials  
    Username: **AdminCSI@Contoso.com**  
    Password: **PiKarAlR@AlBenMo1**
2. In order to ease browsing the web from a server SKU, you will disable Internet Explorer Enhanced Security Configuration
   1. From the start menu, launch **Server Manager**
   2. In the right pane, select **Local Server**
   3. In **IE Enhanced Security Configuration**, click on **On**
   4. Select **Off** for both Administrators and Users
   5. Click **OK** and close **Server Manager**
3. Start a new powershell prompt as Administrator and run the following command  
   Install-Module AzureAD
4. If prompted to install a NuGet provider, answer **Yes**.
5. If you receive a warning about installing from un untrusted repository, answer **Yes**.
6. After installation completes, the Azure AD powershell module will be automatically loaded. No need to run Import-Module cmdlet.
7. In the powershell prompt, run the following command:  
   Connect-AzureAD
8. This will trigger an authentication prompt. Use the credentials you created in the first task.
9. When authentication is complete, you should have a screen like:  
   
10. Using the reference documentation, find the commands to create a new Azure AD user with these specifications:
    1. Display name : User3
    2. User Principal Name : user3@...
    3. Password : P@ssw0rd1
    4. Password should not expire
11. Using the reference documentation, find the command to create a new Azure AD group with these specifications:
    1. Display name: Group1
    2. This group is a security group
    3. This group is not mail enabled
12. Using the reference documentation, find the command to add **user3** in the **Group1** group
13. Using the reference documentation, find the command to disable (not delete!!) **user3**.

Additional Questions:

1. Copy-Paste here the command(s) you ran to create user **user3**.
2. Copy-Paste here the command(s) you ran to create group **Group1**
3. Copy-Paste here the command(s) you ran to put **user3** in group **Group1**
4. Copy-Paste here the command(s) you ran to disable **user3**

#### Task 4: Enable MFA for administrative accounts

Due to inherent risks of passwords, it is highly recommended that any Azure or Office 365 account with administrative privileges be required to use MFA *– Multi-Factor Authentication* to sign in.

The first account of any Azure AD subscription is always a Global Administrator (which is basically the most powerful role). Also, in the previous task, you created a second administrator. Your environment now has 2 very sensitive accounts you must protect. In this task, you will enable MFA for these 2 accounts. For simplicity reason, you will require MFA on a per user basis.

For the purpose of the lab, you will need your mobile phone and connectivity to your mobile services provider. During the lab, Azure MFA will initiate a call to you. The call is only from Azure to you and won’t cause any cost to you.

**Important:** Unless you are currently signed in with your Office 365 trial subscription, ensure you sign out from any other Microsoft service you are currently signed in and clear your browser’s cookies. Otherwise, the portals will try to use your organizational credential which will fail.

1. Review the documentation of Azure MFA located at <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates>
2. Using the instructions from the documentation, enable MFA for the 2 administrative accounts present in your Azure AD environment (admin and admin2)
3. Sign in with admin2 on <https://portal.office.com> to see the changes.
4. Do the same for the admin account.

Additional Questions:

1. What happened when you signed in with either admin or admin2 account?
2. Enabling MFA on a per-user basis is not scalable to large environment. In real situations, there are other way to request MFA. Using the reference documentation, find these 2 other deployment options.

## Exercise 2: Enable Hybrid Identity

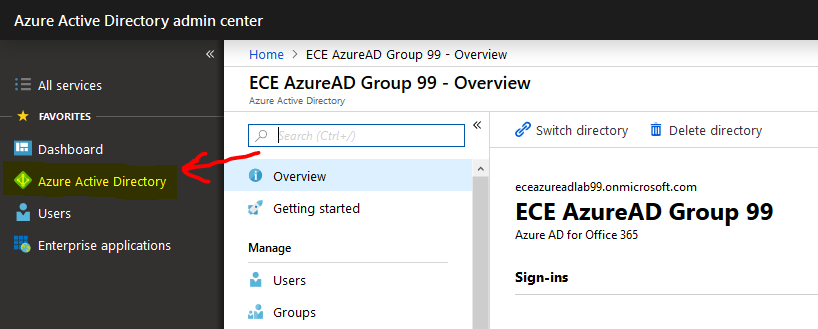
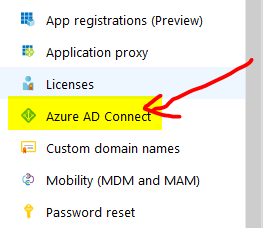
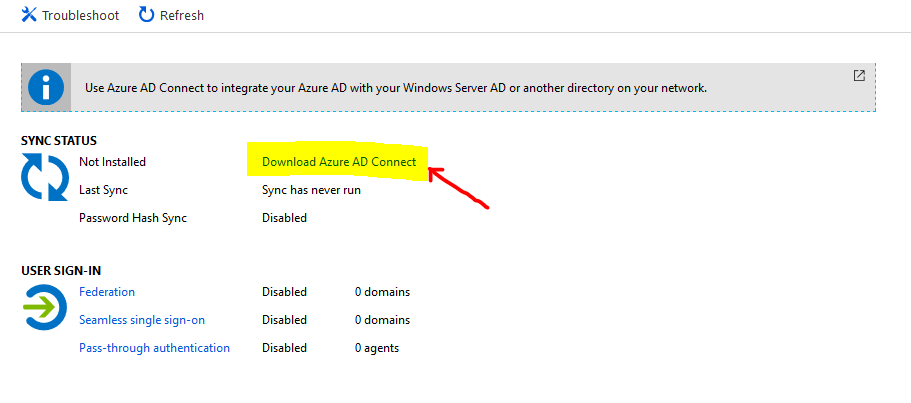
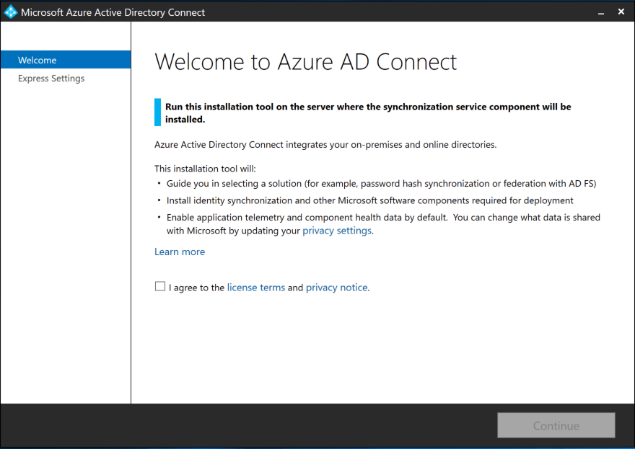
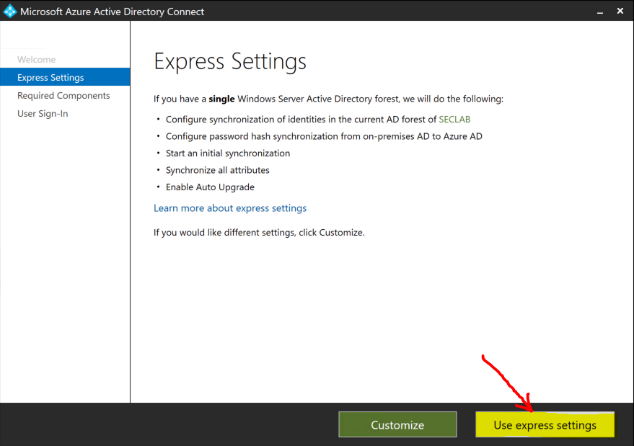
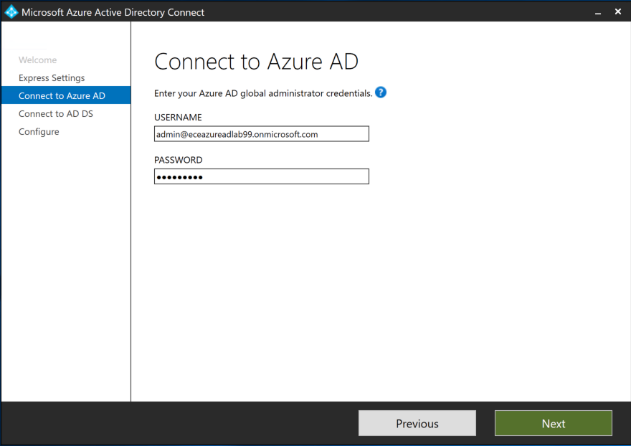
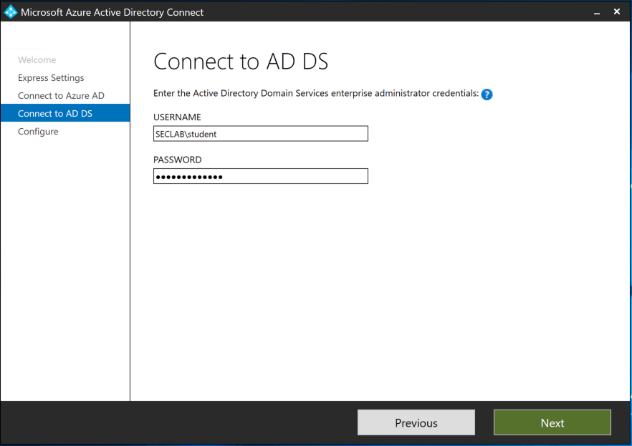
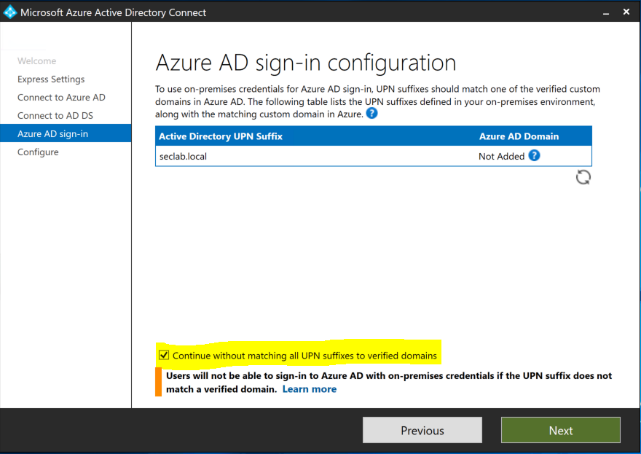
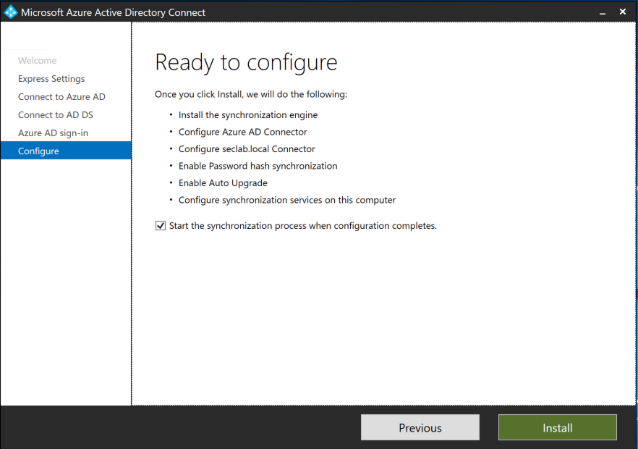
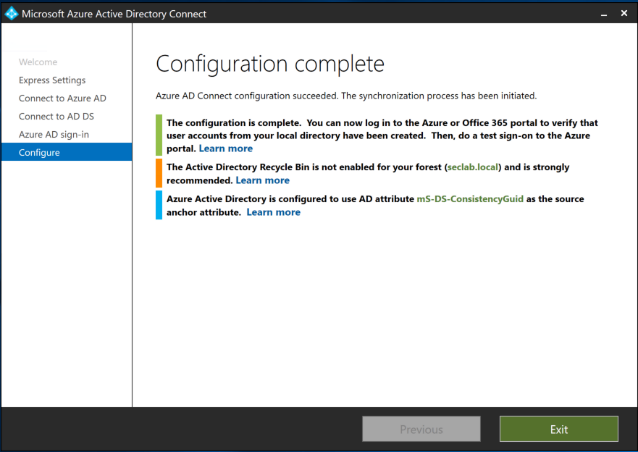
Duration: 1 hour

Synopsis: In this exercise, you will learn how to enable Hybrid Identity between your existing Active Directory environment and your new Azure AD tenant. You will go through the steps of installing the synchronization tool, observe the basic of its operations and have an overview of its customization capabilities.

#### Task 1: Setup Azure AD Connect

In this Task, you will setup the synchronization process between your existing Active Directory environment and your new Azure AD subscription. These are purely configuration steps. There is no question to answer.

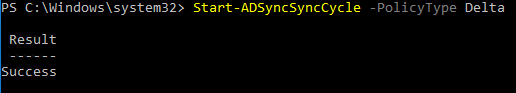
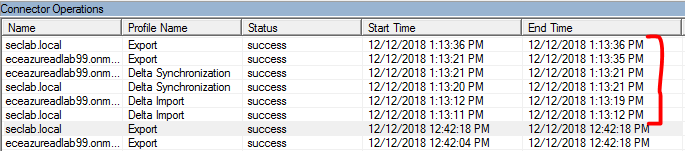
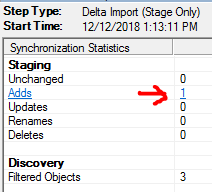
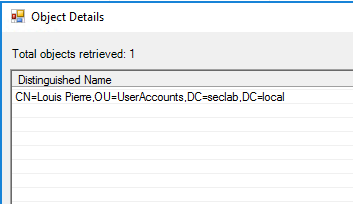
**Important:** Unless you are currently signed in with your Office 365 trial subscription, ensure you sign out from any other Microsoft service you are currently signed in and clear your browser’s cookies. Otherwise, the portals will try to use your organizational credential which will fail.

1. Sign in to Azure AD by browsing <https://aad.portal.azure.com> and by using the credential you created in previous exercise.
2. in the Azure portal, select the **Azure Active Directory** blade from the left pane.  
   
3. In the Azure Active Directory blade, select the **Azure AD Connect** section  
   
4. In the right pane, click the **Download Azure AD Connect** link to download the synchronization tool.  
   
5. Sign in **CSI-TD-SRV1** with following credentials  
    Username: **AdminCSI@Contoso.com**  
    Password: **PiKarAlR@AlBenMo1**
6. Copy the Azure AD Connect setup file to the machine
7. Launch the setup file. The installation program will install the tool and launch the configuration wizard. You should end up with a screen like  
     
   Check the license agreement box and click **Continue**
8. For the purpose of the lab, you will stick with the **Express Settings** which are suited to simple environment. In the next page of the setup assistant, click **Use express settings**
9. On the **Connect to Azure AD** page, enter the Azure AD credentials you created in Task #1 and click **Next**.  
   
10. On the Connect to AD DS page, enter domain credentials and click Next  
    
11. Check the box **Continue without matching all UPN suffixes to verified domains** and click **Next**  
    
12. Click **Install**  
    
13. Now, the setup application will configure Azure AD Connect. This process can take some minutes.  
    

#### Task 2: Observe a synchronization round

In this task, you will force a synchronization round and observe how data is handled by AAD Connect.

The documentation to use for this task is located at <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-whatis>

1. Sign in **CSI-TD-SRV1** with following credentials  
    Username: **AdminCSI@Contoso.com**  
    Password: **PiKarAlR@AlBenMo1**
2. Create a new user in your Active Directory environment. Username and passwords choice are left to you.
3. Open the start menu and launch **Synchronization Service**  
   
4. Focus on the **Connector Operations** list. Every sync operation adds an entry to the list. By default, operations are sorted in chronological order with the most recent on top.  
   If no sync operation has been started since you created the user (probability is low), force a sync round by running this Powershell command (launch Powershell as Administrator) :  
   Start-ADSyncSyncCycle -PolicyType Delta
5. The command output should be similar to:  
     
   And 6 additional lines should have appeared in the **Synchronization Service Manager** as shown in the picture:  
   
6. Refer to the documentation to understand the role of each of the 6 steps in the synchronization round.  
   Reading the article named *Azure AD Connect sync: Understanding the architecture* is highly recommended.
7. Select the the **Delta Import** operation related to you Active Directory domain. In the **Synchronization Statistics**, the **Add** row should be a clickable link and display **1** as its value.  
   
8. By clicking the **Add** link, a window will appear containing the list of new objects imported from Active Directory  
   
9. Double clicking on one of the objects will open a new window displaying attributes details.
10. Try to analyze the six steps and understand their meaning. Then, answer the additional questions.

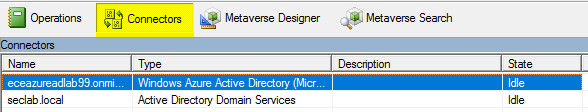
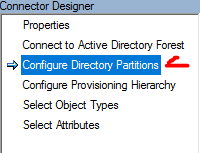
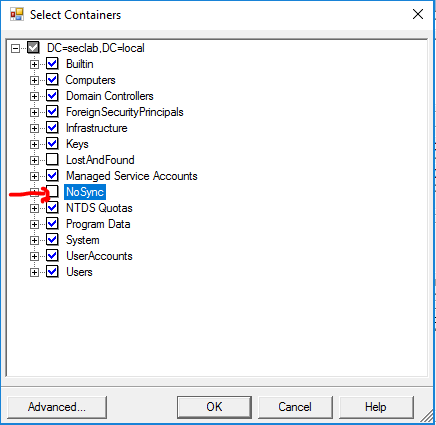
Additional Questions:

1. How often does AAD Connect synchronizes your Azure AD tenant and Active Directory domain?
2. Is it possible to manually force a synchronization? If yes, how can this be achieved?
3. Which synchronization step creates entry in the metaverse for new Active Directory objects?
4. Which synchronization step creates new Azure AD objects from data contained in the metaverse?

#### Task 3: Filter out objects from the synchronization process

In this task, you will train yourself in configuring Azure AD Connect and exclude some objects from the synchronization process. For the purpose of the lab, we will create a new OU – *Organizational Unit* and configure AAD Connect not to sync objects in this OU.

The reference documentation to use is located at <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-whatis>

1. Sign in **CSI-TD-SRV1** with following credentials  
    Username: **AdminCSI@Contoso.com**  
    Password: **PiKarAlR@AlBenMo1**
2. Create a new organizational unit in your Active Directory domain. OU’s name choice is left to you.
3. Start a new Powershell command prompt as Administrator  
   In order to modify the connectors’ configuration, the synchronization must be disabled first by running:  
   Set-ADSyncScheduler -SyncCycleEnabled $false
4. Open the start menu and launch **Synchronization Service**  
   
5. Click on **Connectors** located on the top tool bar  
   
6. Double click on the connector related to your Active Directory domain
7. Select **Configure Directory Partitions** from the left outer panel  
   
8. Click on **Containers**  
   
9. When you're prompted, provide any credentials with read access to your on-premises Active Directory. It doesn't have to be the user that is prepopulated in the dialog box.
10. In the **Select Containers** dialog box, clear the OU that you don’t want to synchronize with the cloud directory, and then click **OK**.  
    
11. Create a new user account in that OU and run the steps you’ve learn in previous task to initiate a synchronization run and check that the user account is not provisioned in Azure Active Directory.

Additional Questions:

1. Using the reference documentation, what are the other kind of filtering you can use?
2. In the default configuration, there are filtering already in place for user accounts based on attribute values. Using the reference documentation, list 2 existing attribute-based filters that apply **only** on user objects.

## After the Lab

Duration: 10 minutes

In this exercise, attendees will deallocate any Azure resources that were started in support of the lab.

#### Task 1: Stop and deallocated all the VMs

1. Properly shutdown all the VMs
2. Deallocate the VM in the Azure Portal
3. To Stop a VM, simply click on Unclaim.

