

Module 1 – Lab 1 – The foundations of hybrid identity

 **Student name:** TEJEDA David, PEUGNET Thomas

 **Student class:** EFREI RS3 2025

 **Date:** 23/01/2024

Active Directory Services hands-on lab step-by-step

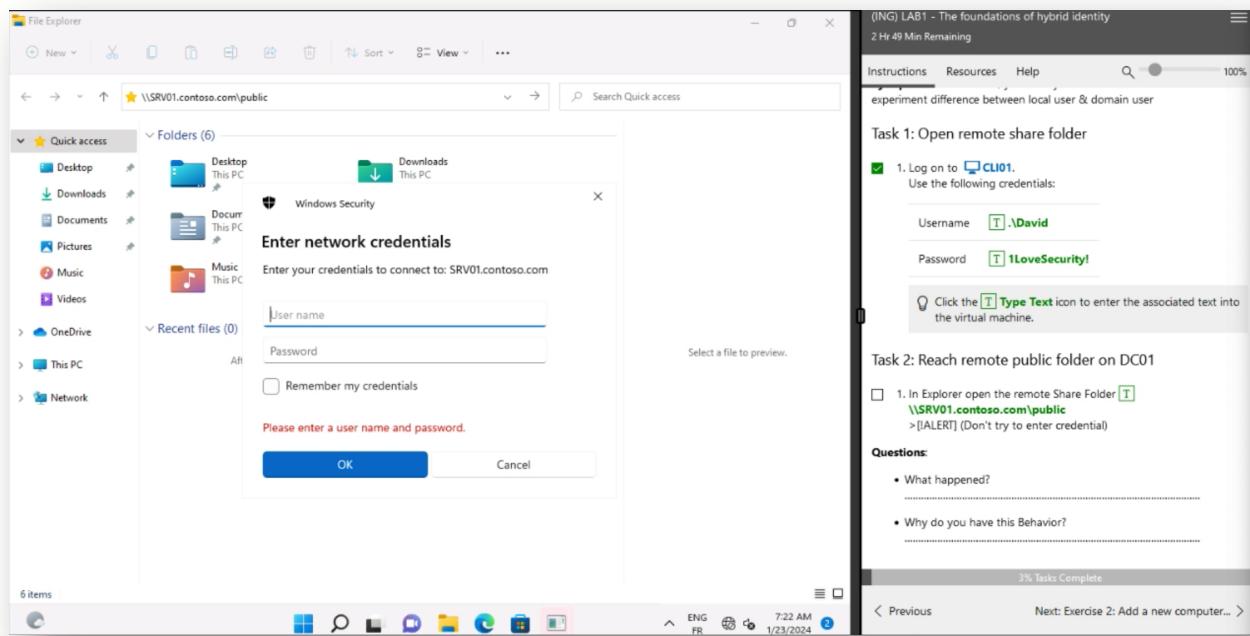
Exercise 1: Manage access without Active Directory

Task 1: Open remote share folder

Task 2: Reach remote public folder on DC01

Questions

- What happened?
 - o Un message est apparu pour nous informer qu'un nom d'utilisateur était nécessaire pour accéder à cette localisation.
- Why do you have this Behavior?
 - o Cette localisation est soumise à une politique de droits. Il est donc nécessaire que l'utilisateur soit authentifié pour qu'il soit possible de vérifier que ce dernier possède bel et bien les droits/groupes suffisants pour accéder à cette ressource.



Module 1 – Lab 1 – The foundations of hybrid identity

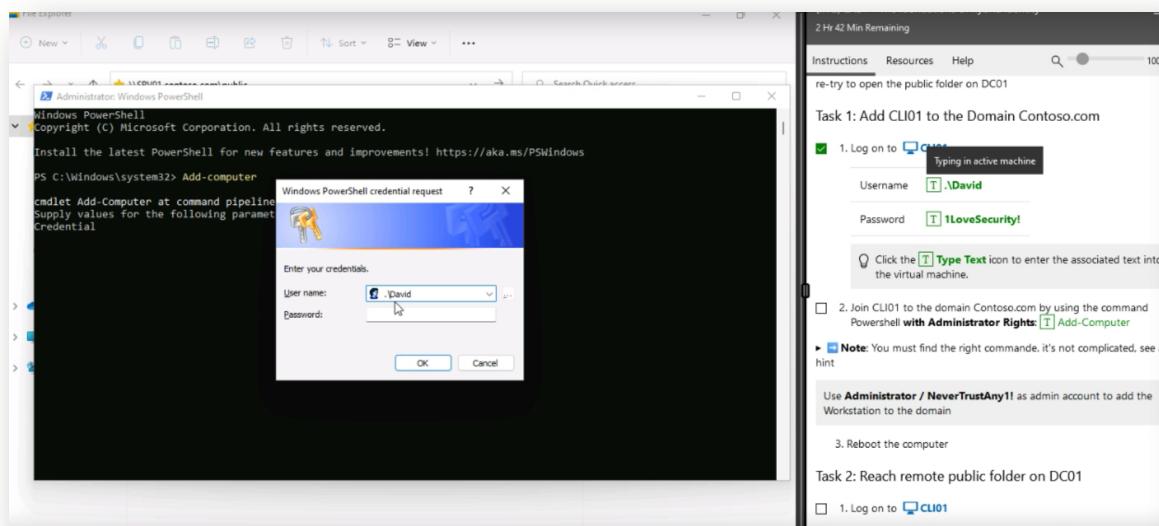
Exercise 2: Add a new computer to the domain

Task 1: Add CLI01 to the Domain Contoso.com

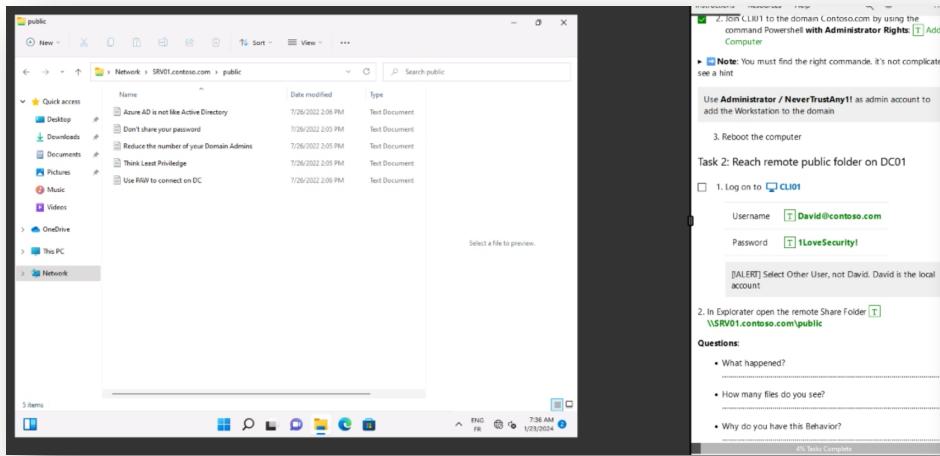
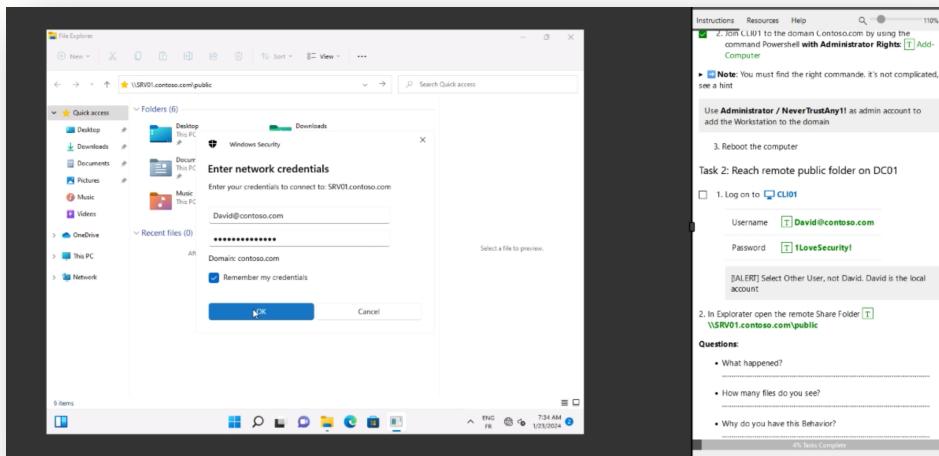
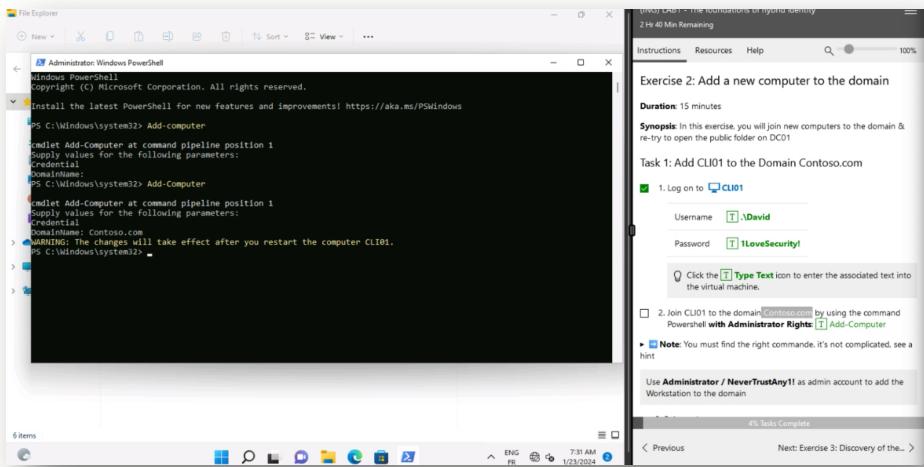
Task 2: Reach remote public folder on DC01

Questions:

- What happened?
 - En entrant la commande Add-Computer, on obtient une fenêtre qui nous demande de nous authentifier pour avoir des droits administrateurs sur le PowerShell. Par la suite, on nous demande d'ajouter un DomainName Contoso.com.
- How many files do you see?
 - Nous voyons actuellement 5 fichiers (comme visible sur la dernière capture d'écran)
- Why do you have this Behavior?
 - Le PC a été ajouté au domaine Contoso.com, lui permettant donc d'accéder à ces fichiers. L'utilisateur David peut maintenant se connecter avec ses identifiants David@Contoso.com .



Module 1 – Lab 1 – The foundations of hybrid identity



Module 1 – Lab 1 – The foundations of hybrid identity

Exercise 3: Discovery of the environment

Task 1: Create a new OU

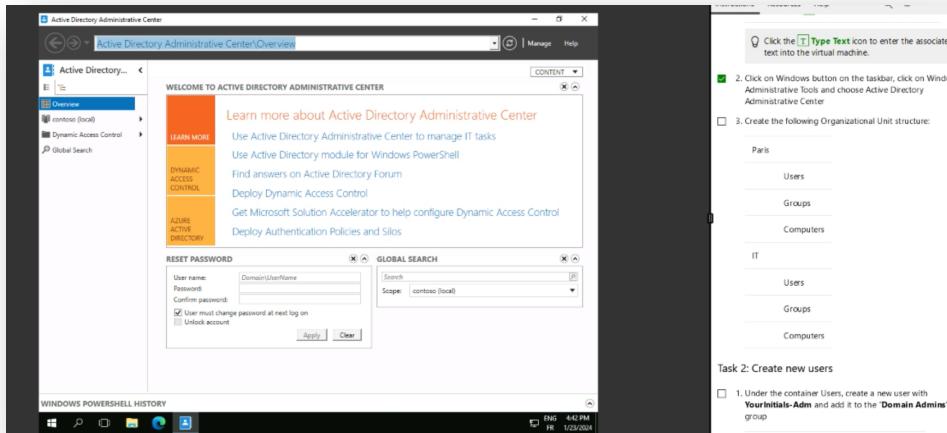
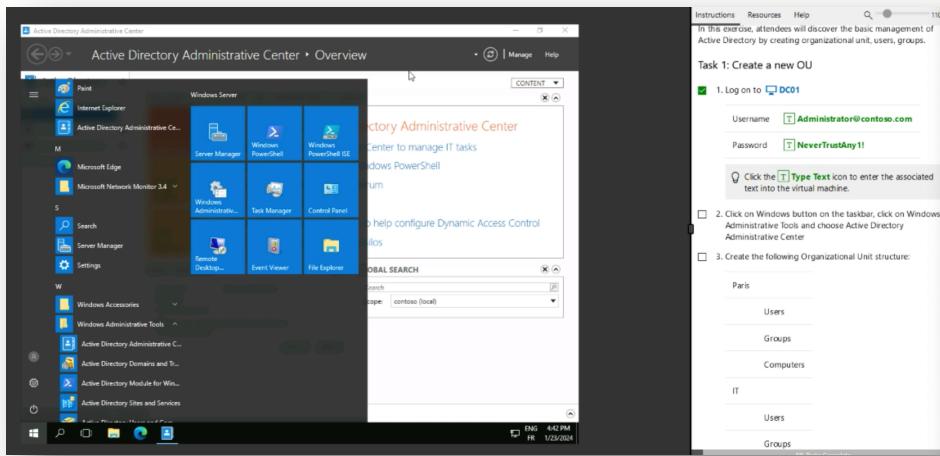
Task 2: Create new users

Task 3: Create a new group

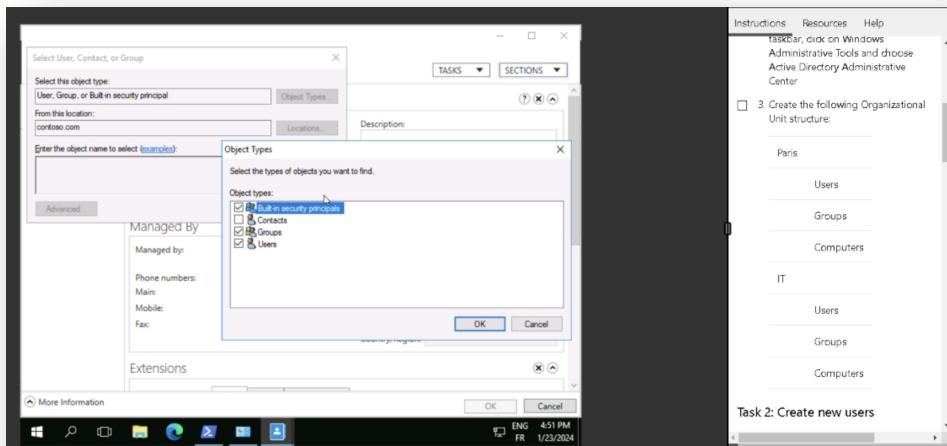
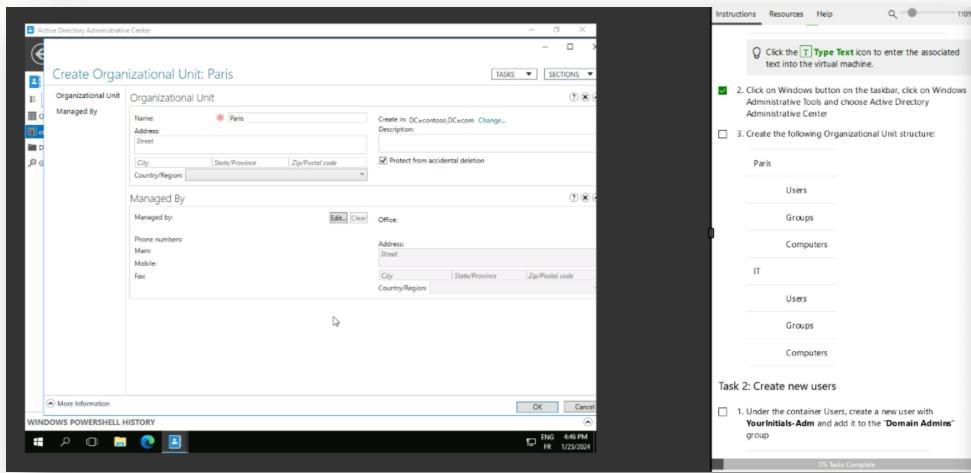
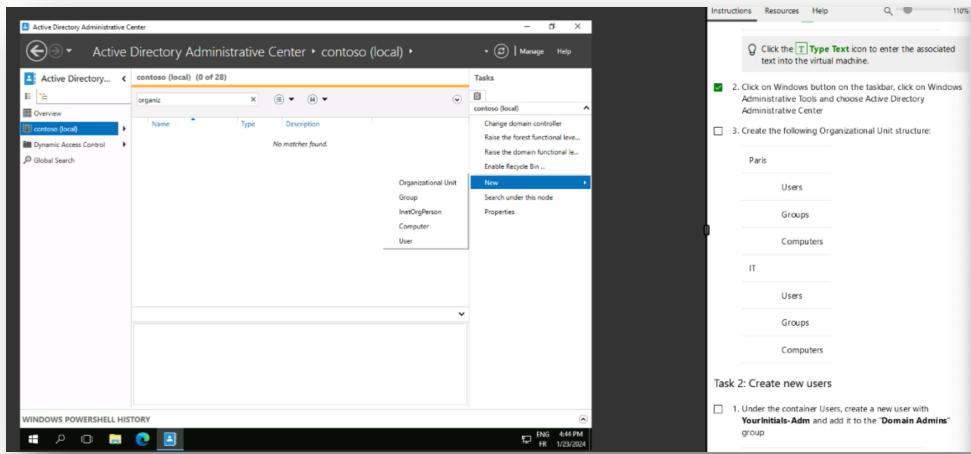
Task 4: Enumerate & find objects in ADDS

Questions:

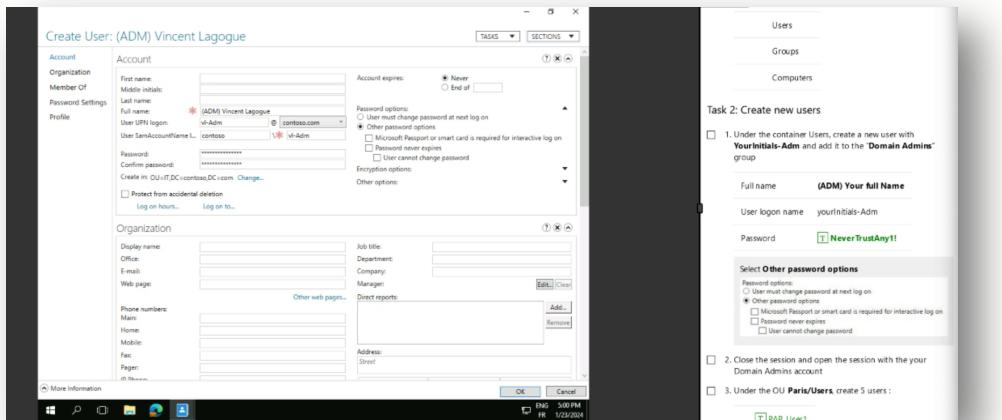
- How many users you have?
 - o 81
- How many computer(s) you have?
 - o 13



Module 1 – Lab 1 – The foundations of hybrid identity



Module 1 – Lab 1 – The foundations of hybrid identity



(ADM) LAB1 - The foundations of hybrid identity

Active Directory Administrative Center > contoso (local) > Paris

Tasks

(ADM) Thomas PEUGNET

Reset password...

View resultant password settings...

Add to group...

Disable

Delete

Move...

Properties

Paris

New

Delete

Move...

Search under this node

Properties

Instructions Resources Help

Task 2: Create new users

1. Under the container Users, create a new user with YourInitials-Admin and add it to the "Domain Admins" group

Full name: (ADM) Your full Name

User logon name: yourinitials-Admin

Password: NeverTrustAny1!

Select Other password options

Other password options

User must change password at next log on

Other password options

Microsoft Passport or smart card is required for interactive log on

Never expires

User cannot change password

Encryption options

Other options

2. Close the session and open the session with your Domain Admins account

3. Under the OU Paris/Users, create 5 users:

PAR_User1

PAR_User2

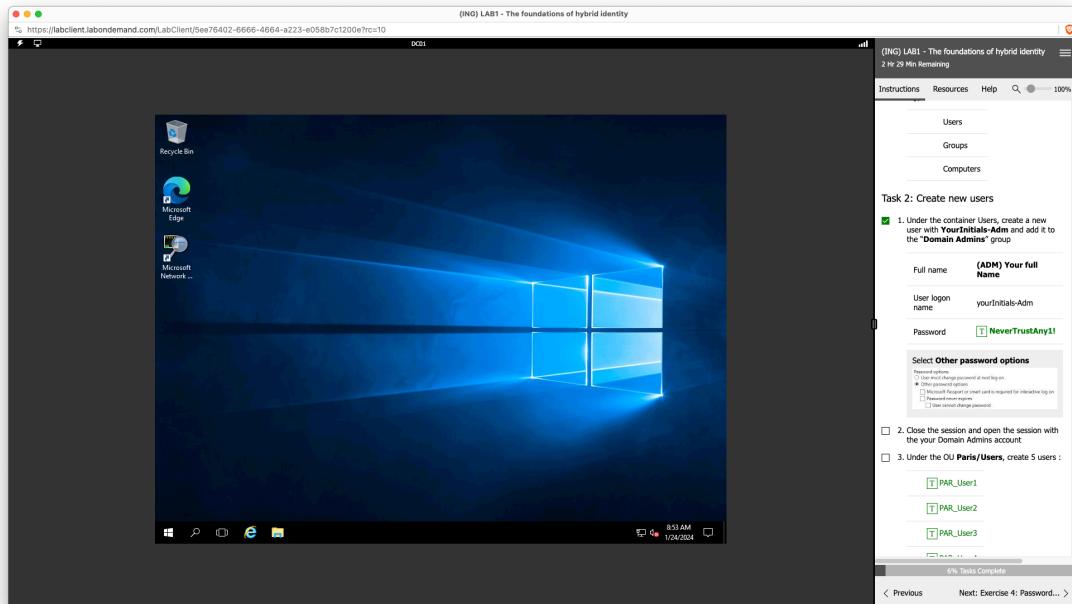
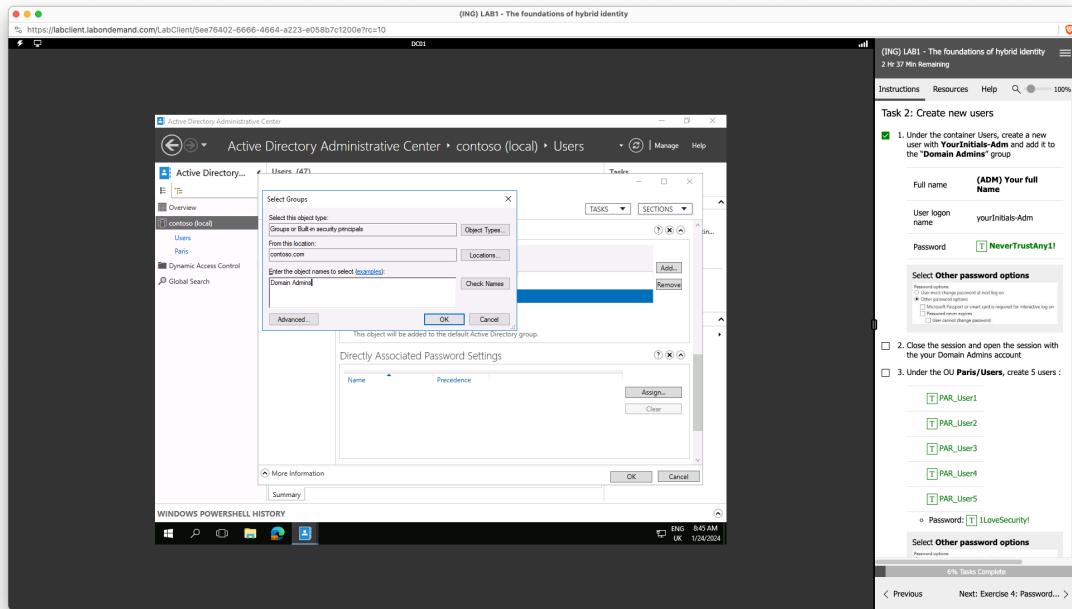
PAR_User3

PAR_User4

PAR_User5

6% Tasks Complete

Module 1 – Lab 1 – The foundations of hybrid identity



Module 1 – Lab 1 – The foundations of hybrid identity

The screenshot shows the Active Directory Administrative Center interface. The left pane displays the Paris organizational unit (OU) containing five user accounts: PAR_User1 through PAR_User5. The right pane shows a detailed view of PAR_User1, including its properties like User logon, Last log on, and Last password change. A context menu is open over PAR_User1, and a password reset dialog box is displayed on the right side of the screen.

This screenshot is identical to the one above, showing the Paris OU in the Active Directory Administrative Center. It displays the same five user accounts and the same password reset dialog box.

The screenshot shows the Active Directory Administrative Center interface. The left pane displays the Paris Prod group under the Paris OU, which contains three members: PAR_User1, PAR_User2, and PAR_User3. The right pane shows a detailed view of PAR_User1, including its properties and a context menu. A password reset dialog box is also present on the right.

Module 1 – Lab 1 – The foundations of hybrid identity

(ING) LAB1 - The foundations of hybrid identity

Active Directory Administrative Center

Groups (1)

Paris Prod

Instructions Resources Help

Task 3: Create a new group

1 Under the OU ParisProd, create a group named: Paris Prod

2 Add All PAR_... Users to Paris Prod

3 Click OK

All actions performed with the console can be done with PowerShell.

Task 4: Enumerate & find objects in ADDS

1 Open a PowerShell CLI with Administrator Rights

2 Use the PowerShell command `Get-ADUser` to list all users in this ADDS

3 Use a PowerShell command to list all computer objects

4 Use a PowerShell command to list all computer objects

Parameter field Parameter value

-filter ??

Questions

- How many users do you have?
- How many computer(s) you have?

10% Tasks Complete

(ING) LAB1 - The foundations of hybrid identity

Active Directory Administrative Center

Groups (1)

Paris Prod

Instructions Resources Help

Task 3: Create a new group

1 Under the OU ParisProd, create a group named: Paris Prod

2 Add All PAR_... Users to Paris Prod

3 Click OK

All actions performed with the console can be done with PowerShell.

Task 4: Enumerate & finds objects in ADDS

1 Open a PowerShell CLI with Administrator Rights

2 Use the PowerShell command `Get-ADUser` to list all users in this ADDS

3 Use a PowerShell command to list all computer objects

4 Use a PowerShell command to list all computer objects

Parameter field Parameter value

-filter ??

Questions

- How many users do you have?
- How many computer(s) you have?

10% Tasks Complete

(ING) LAB1 - The foundations of hybrid identity

Active Directory Administrative Center

Users (48)

Instructions Resources Help

Task 3: Create a new group

1 Under the OU ParisProd, create a group named: Paris Prod

2 Add All PAR_... Users to Paris Prod

3 Click OK

All actions performed with the console can be done with PowerShell.

Task 4: Enumerate & finds objects in ADDS

1 Open a PowerShell CLI with Administrator Rights

2 Use the PowerShell command `Get-ADUser` to list all users in this ADDS

3 Use a PowerShell command to list all computer objects

4 Use a PowerShell command to list all computer objects

Parameter field Parameter value

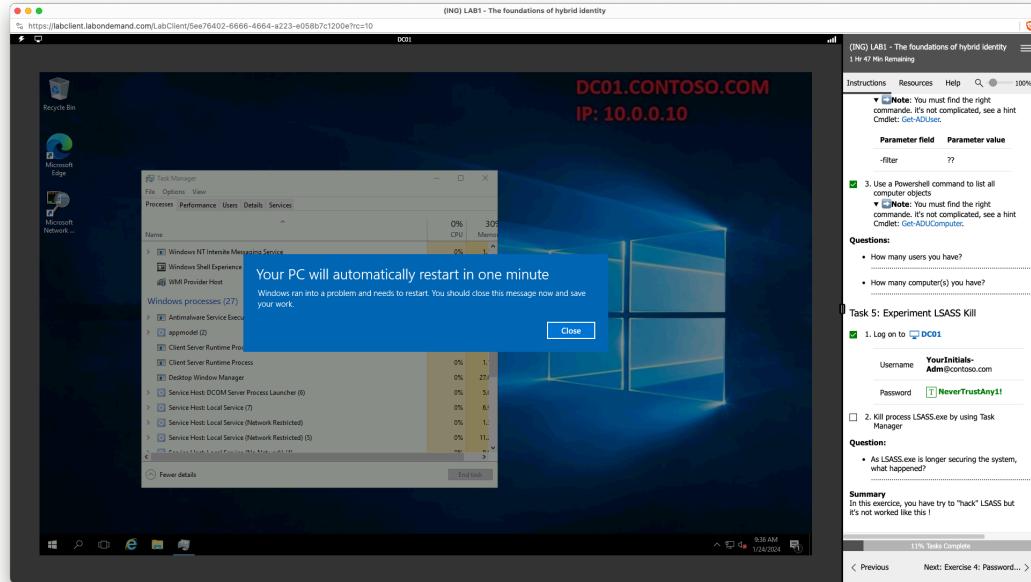
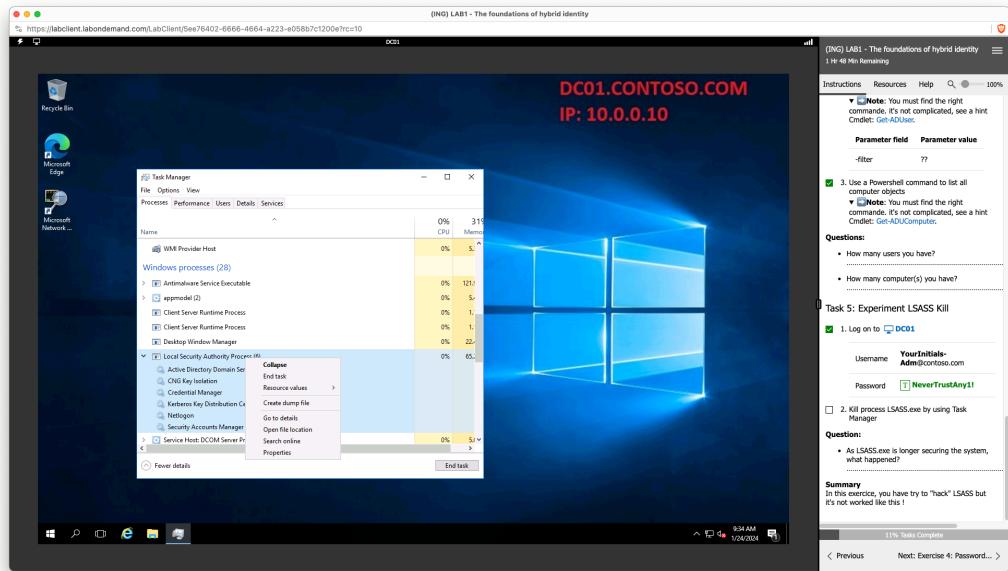
-filter ??

Questions

- How many users do you have?

10% Tasks Complete

Module 1 – Lab 1 – The foundations of hybrid identity



Task 5: Experiment LSASS Kill

Question:

- As LSASS.exe is longer securing the system, what happened?
 - o Le kill de LSASS.exe va entraîner une perte de contrôle sur l'authentification des utilisateurs, des problèmes de sécurité.
 - o Après le kill, la session a été déconnectée et le PC a redémarré.

Module 1 – Lab 1 – The foundations of hybrid identity

Exercise 4: Password Policy vs FGPP

Task 1: Configure FGPP

Task 2: Verify that the Admin-FGPP is applied to Administrators

Questions

- Do you success to change the password?
 - o Non.
- Why? Ok it's the FGPP but Why?
 - o Le mot de passe qu'on tente de changer n'est pas raccord avec la password policy qu'on a créé avant.

The screenshot shows the Active Directory Administrative Center interface. On the left, the navigation pane includes 'System', 'Administrative Center', 'Groups', 'Users', and 'Computers'. Under 'System', 'Password Settings Container' is selected. In the center, a table lists 'Password Settings Container (0)' with columns for Name, Precedence, Type, and Description. A context menu is open over the container, with 'New' selected under the 'Password Settings' option. The right pane displays task steps for creating an Admin-FGPP, including steps like '3. Go to System/Password Settings Container', '4. Create a new Password Settings', and '5. Name : Admin-FGPP'. A note states: 'Note: We installed in advance the RSAT to manage the ADDS from this server'.

The screenshot shows the 'Create Password Settings: Admin-FGPP' dialog box. It contains fields for 'Name' (Admin-FGPP), 'Precedence' (5), and 'Password age options'. Under 'Password Settings', there are several checkboxes: 'Enforce minimum password length' (set to 15), 'Enforce minimum password history' (set to 24), 'Enforce password complexity requirements' (set to 24), and 'Store password using reversible encryption'. Under 'Protect from password reuse', there are checkboxes for 'User lockout' (set to 10) and 'Reset failed logon attempts count after' (set to 30). The 'Directly Applies To' section shows 'Domain Admins' selected. The right pane displays task steps for verifying the Admin-FGPP application, including steps like '1. Click Global Search' and '2. In the Search Zone, Enter Administrator'. A note states: 'Note: We installed in advance the RSAT to manage the ADDS from this server'.

Module 1 – Lab 1 – The foundations of hybrid identity

(ING) LAB1 - The foundations of hybrid identity

Active Directory Administrative Center • Global Search

GLOBAL SEARCH 2 Items Found

Administrator

Administrator User

Administrators Group

Tasks

Administrator

Reset password... View resultant password settings... Add to group... Delete Move... Locate Properties

3. Go to System/Password Settings Container

4. Create a new Password Settings

5. Name : Admin-FGPP

6. Precedence : 5

7. Enforce minimum password length : 15

8. Add it to Domain Admins Group

Task 2: Verify that the Admin-FGPP is applied to Administrators

1. Click Global Search

2. In the Search Zone, Enter Administrator

3. Click Search

4. Right click on the Administrator and Select View resultant password setting

5. The Admin-FGPP should be displayed

6. Change the password by entering NewPassword22!

Questions

Do you success to change the password?

Why? (Ok it's the FGPP but Why?)

Summary

In this exercise, you have applying FGPP to have a different password policy for all Domain Administrators.

10% Tasks Complete

(ING) LAB1 - The foundations of hybrid identity

Active Directory Administrative Center • Global Search

GLOBAL SEARCH 2 Items found

Administrator

Administrator User

Administrators Group

Tasks

Administrator

Reset password... View resultant password settings... Add to group... Delete Move... Locate Properties

Admin-FGPP

Directly Applies To

Extensions

Admin-FGPP

Precedence : 5

Enforce minimum password length : 15

Enforce password history : 24

Enforce password complexity required : 24

Password must meet complexity requirements

Store password using reversible encryption

Protect from accidental deletion

Enforce minimum password age : 1

Minimum password length (characters) : 15

Enforce maximum password age : 42

Enforce account lockout policy : 30

Number of failed logon attempts allowed : 30

For a duration of (mins) : 30

Until an administrator manually unlocks the account

Enforce minimum password age : 1

User cannot change the password within : 1

Enforce maximum password age : 42

Lockout duration after (mins) : 30

Lockout count after (mins) : 30

Account will be locked out

For a duration of (mins) : 30

Until an administrator manually unlocks the account

Directly Applies To

Name : Domain Admins

Add... Remove

Administrator

More Information

OK Cancel

3. Go to System/Password Settings Container

4. Create a new Password Settings

5. Name : Admin-FGPP

6. Precedence : 5

7. Enforce minimum password length : 15

8. Add it to Domain Admins Group

Task 2: Verify that the Admin-FGPP is applied to Administrators

1. Click Global Search

2. In the Search Zone, Enter Administrator

3. Click Search

4. Right click on the Administrator and Select View resultant password setting

5. The Admin-FGPP should be displayed

6. Change the password by entering NewPassword22!

Questions

Do you success to change the password?

Why? (Ok it's the FGPP but Why?)

Summary

In this exercise, you have applying FGPP to have a different password policy for all Domain Administrators.

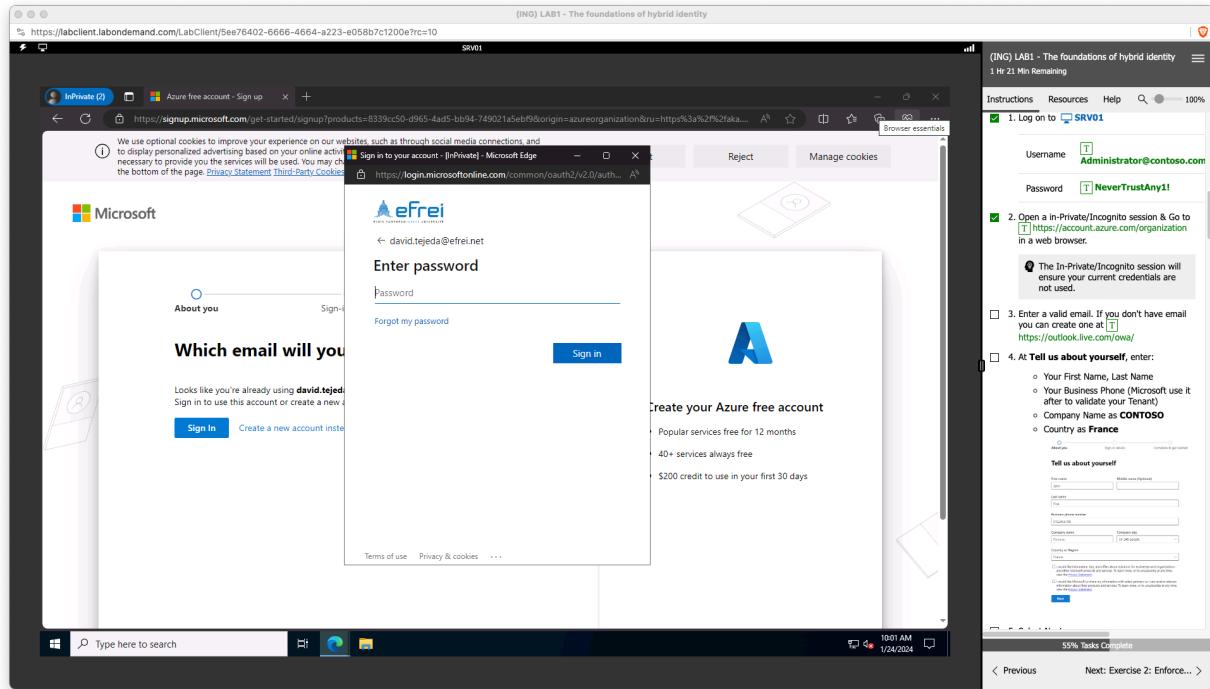
15% Tasks Complete

Module 1 – Lab 1 – The foundations of hybrid identity

The screenshot shows the Active Directory Administrative Center interface. In the center pane, a global search for 'Administrator' is performed, resulting in two items found: 'Administrator' (User) and 'Administrators' (Group). The 'Administrator' user is selected, and a 'Reset Password' dialog box is open. The password 'NewPassword2!' is entered twice. The right pane displays a task list for 'Task 2: Verify that the Admin-FGPP is applied to Administrators'. Step 6, '6. Precedence : 5', is checked. Step 7, '7. Enforce minimum password length : 15', is also checked. Step 8, '8. Add it to Domain Admins Group', is listed but not checked. A note indicates that the Admin-FGPP should be displayed. The Windows PowerShell History window at the bottom shows the command 'Set-LocalUser -Name Administrator -Password (ConvertTo-SecureString -String "NewPassword2!" -AsPlainText -Force)'.

This screenshot is nearly identical to the one above, showing the Active Directory Administrative Center interface. However, the 'Reset Password' dialog box now displays an error message: 'Failed to reset the password for Administrator. The password does not meet the length, complexity, or history requirement of the domain.' The right pane's task list for Task 2 remains the same, with step 7 (minimum password length) failing. The Windows PowerShell History window shows the same command as before.

Module 1 – Lab 1 – The foundations of hybrid identity



Extending identities to the cloud with Azure AD

Exercise 1: Integrate an Active Directory Forest with an Azure Active Directory tenant

Task 1: Create an Azure Active Directory tenant and activate an EMS E5 trial

Task 2: Enable EMS E5 Trials

Task 3: Create and configure Azure AD users

Task 4: Install Azure AD Connect

Questions:

- What is the goal of the filtering?
 - o C'est de sélectionner les objets (utilisateurs, groupes, contacts) qui seront synchronisés depuis l'Active Directory local vers Azure AD, en fonction de critères spécifiques.

Questions:

- What is the goal of SSO?
 - o Le but du Single Sign-On (SSO) est de permettre aux utilisateurs d'accéder à plusieurs applications et services en utilisant une seule fois leurs identifiants de connexion.
- Why is it Seamless?
 - o Il fournit une transition entre différents services et applications sans que l'utilisateur ait à saisir ses identifiants de connexion à chaque fois. Donc c'est assez fluide.

Module 1 – Lab 1 – The foundations of hybrid identity

Task 5: Check directory synchronization

Task 6: Disable security defaults

The screenshot shows a Microsoft Edge browser window with the title bar '(ING) LAB1 - The foundations of hybrid identity'. The main content area is titled 'Azure free account - Sign up' and shows a 'Security check' step. It asks for a verification code, which has been entered as '70534d'. Below this, there are options to 'Verify' or 'Change my phone number'. To the right of the main window, a sidebar titled 'Instructions' lists several tasks:

- 2. Open a In-Private/Incognito session & Go to <https://account.azure.com/organization> in a web browser.
 - The In-Private/Incognito session will ensure your current credentials are not used.
- 3. Enter a valid email. If you don't have email you can create one at <https://outlook.live.com/owa/>
- 4. At Tell us about yourself, enter:
 - Your First Name, Last Name
 - Your Business Phone (Microsoft use it after to validate your Tenant)
 - Company Name as **CONTOSO**
 - Country as France
- 5. Select Next

At the bottom of the sidebar, it says '55% Tasks Complete'.

The screenshot shows a Microsoft Edge browser window with the title bar '(ING) LAB1 - The foundations of hybrid identity'. The main content area is titled 'Azure free account - Sign up' and shows the 'How you'll sign in' step. The user has entered 'root' for the 'Username' and 'efrtp01.onmicrosoft.com' for the 'Domain name'. Below these fields are 'Password' and 'Confirm password' fields, both containing 'root'. A note at the bottom says 'By selecting Next, you agree to our [trial agreement](#)'. A 'Next' button is visible at the bottom of the form.

To the right, the sidebar continues the task list:

- 6. Verify your phone by enter the verification code
- 7. How you will sign in, enter:
 - Username : **root**
 - Domain Name : "School Trigram" + "Student Intel" + 2 digits
 - The name supplied under Domain Name will subsequently become the name of your tenant as **MSCG01.onmicrosoft.com**
 - Password : **NeverTrustAny1!**
- Note: Register your Tenant information. Tenant Name, First Global Administrator & password
- 8. Select Next
- 9. Click Get Started

At the bottom of the sidebar, it says '57% Tasks Complete'.

Module 1 – Lab 1 – The foundations of hybrid identity

(ING) LAB1 - The foundations of hybrid identity

Instructions Resources Help 100% 1 Hr 6 Min Remaining

Note: Register your Tenant information.
Tenant Name, First Global Administrator & password

8. Select Next
9. Click Get Started
Don't continue to fill the next page!

10. Open a new tab and navigate to <https://portal.azure.com> & close the previous tab If prompted, enter the global admin user name and password for your tenant:
Username: root@AzureDomainName.onmicrosoft.com
Password: "YourGlobalAdminPassword"

Task 2: Enable EMS E5 Trials

1. Go to Azure licenses center: https://portal.azure.com/#blade/Microsoft_AAD
2. Select the All Products blade menu item.
3. Select the Try/Buy button and enable all of the trials (EMS E5 and AAD P2) in the fly-out that appears.

Note: It may take a few minutes for the licenses to appear in the all products portal after you activate a trial, you will not need to select it again.

57% Tasks Complete

< Previous Next: Exercise 2: Enforce... >

(ING) LAB1 - The foundations of hybrid identity

Instructions Resources Help 100% 1 Hr 4 Min Remaining

page !

10. Open a new tab and navigate to <https://portal.azure.com> & close the previous tab If prompted, enter the global admin user name and password for your tenant:
Username: root@AzureDomainName.onmicrosoft.com
Password: "YourGlobalAdminPassword"

Task 2: Enable EMS E5 Trials

1. Go to Azure licenses center: https://portal.azure.com/#blade/Microsoft_AAD
2. Select the All Products blade menu item.
3. Select the Try/Buy button and enable all of the trials (EMS E5 and AAD P2) in the fly-out that appears.

Note: It may take a few minutes for the licenses to appear in the all products portal after you activate a trial, you will not need to select it again.

Activation typically takes about 5 minutes.

Task 3: Create and configure Azure AD users

In this task, you will configure Azure AD user accounts in the newly created Azure AD tenant with the following settings. This will include assigning EMS E5 licenses to the user account you are using.

58% Tasks Complete

< Previous Next: Exercise 2: Enforce... >

Module 1 – Lab 1 – The foundations of hybrid identity

The screenshot shows the Microsoft Azure portal interface. On the left, the 'Licenses' blade is open under 'CONTOSO - Microsoft Entra ID'. It displays a table with columns: Name, Total, Assigned, Available, and Expiring soon. A note says 'No results.' On the right, a task pane titled '(ING) LAB1 - The foundations of hybrid identity' is visible. It shows a progress bar at 59% complete. Task 1: Open a new tab and navigate to https://portal.azure.com & close the previous tab. If prompted, enter the global admin user name and password for your tenant. Step 1: Go to Azure licenses center: https://portal.azure.com/#blade/Microsoft_AAD_LicensingBlade/Products. Step 2: Select the All Products blade menu item. Step 3: Select the Try/Buy button and enable all of the trials (EMS E5 and AAD P2) in the fly-out that appears. Note: It may take a few minutes for the licenses to appear in the all products portal; after you activate a trial, you will not need to select it again. Activation typically takes about 5 minutes. Task 2: Enable EMS E5 Trials Step 1: Go to Azure licenses center: https://portal.azure.com/#blade/Microsoft_AAD_LicensingBlade/Products Step 2: Select the All Products blade menu item. Step 3: Select the Try/Buy button and enable all of the trials (EMS E5 and AAD P2) in the fly-out that appears. Note: It may take a few minutes for the licenses to appear in the all products portal; after you activate a trial, you will not need to select it again. Activation typically takes about 5 minutes. Task 3: Create and configure Azure AD users In this task, you will configure Azure AD user accounts in the newly created Azure AD tenant with the following settings. This will include assigning FMS+E5 licenses to the user account you are using. 59% Tasks Complete.

The screenshot shows the Microsoft Azure portal interface. On the left, the 'Licenses' blade is open under 'CONTOSO - Microsoft Entra ID'. It displays a table with columns: Name, Total, Assigned, Available, and Expiring soon. A note says 'No results.' On the right, a task pane titled '(ING) LAB1 - The foundations of hybrid identity' is visible. It shows a progress bar at 59% complete. Task 1: Open a new tab and navigate to https://portal.azure.com & close the previous tab. If prompted, enter the global admin user name and password for your tenant. Step 1: Go to Azure licenses center: https://portal.azure.com/#blade/Microsoft_AAD_LicensingBlade/Products. Step 2: Select the All Products blade menu item. Step 3: Select the Try/Buy button and enable all of the trials (EMS E5 and AAD P2) in the fly-out that appears. Note: It may take a few minutes for the licenses to appear in the all products portal; after you activate a trial, you will not need to select it again. Activation typically takes about 5 minutes. Task 2: Enable EMS E5 Trials Step 1: Go to Azure licenses center: https://portal.azure.com/#blade/Microsoft_AAD_LicensingBlade/Products Step 2: Select the All Products blade menu item. Step 3: Select the Try/Buy button and enable all of the trials (EMS E5 and AAD P2) in the fly-out that appears. Note: It may take a few minutes for the licenses to appear in the all products portal; after you activate a trial, you will not need to select it again. Activation typically takes about 5 minutes. Task 3: Create and configure Azure AD users In this task, you will configure Azure AD user accounts in the newly created Azure AD tenant with the following settings. This will include assigning FMS+E5 licenses to the user account you are using. 59% Tasks Complete.

Module 1 – Lab 1 – The foundations of hybrid identity

The screenshot shows a Microsoft Edge browser window with two tabs open. The left tab displays the Microsoft Entra ID Governance Trial sign-up page, which includes fields for 'About you', 'Sign-in details', and 'Complete & get started'. The right tab shows a task list titled 'Task 2: Enable EMS E5 Trials' with three completed steps:

1. Go to Azure licenses center: https://portal.azure.com/#blade/Microsoft_AAD
2. Select the All Products blade menu item.
3. Select the Try/Buy button and enable all of the trials (EMS E5 and AAD P2) in the fly-out that appears.

Notes and tips are provided: 'Note: It may take a few minutes for the licenses to appear in the all products portal; after you activate a trial, you will not need to select it again.' and 'Activation typically takes about 5 minutes.'

The task bar at the bottom indicates '60% Tasks Complete'.

The screenshot shows a Microsoft Edge browser window with two tabs open. The left tab displays the Microsoft Entra ID Governance Trial sign-up page, which includes fields for 'About you', 'Sign-in details', and 'Complete & get started'. The right tab shows a task list titled 'Task 2: Enable EMS E5 Trials' with three completed steps:

1. Go to Azure licenses center: https://portal.azure.com/#blade/Microsoft_AAD
2. Select the All Products blade menu item.
3. Select the Try/Buy button and enable all of the trials (EMS E5 and AAD P2) in the fly-out that appears.

Notes and tips are provided: 'Note: It may take a few minutes for the licenses to appear in the all products portal; after you activate a trial, you will not need to select it again.' and 'Activation typically takes about 5 minutes.'

The task bar at the bottom indicates '60% Tasks Complete'.

Module 1 – Lab 1 – The foundations of hybrid identity

(ING) LAB1 - The foundations of hybrid identity

SRV01

InPrivate https://labclient.labondemand.com/LabClient/Searc... 56 Minutes Remaining

Instructions Resources Help Search 100%

Your Business Phone (Microsoft use it after to validate your Tenant)

Company Name as **CONTOSO**

Country as **France**

Tell us about yourself!

First name: Middle name:
Last name: Suffix:
Business phone number: Extension:
Address: Zip code:
City: State:
Country: Postcode:
Fax: Email:

5. Select Next

6. Verify your phone by enter the verification code

7. How you will sign in, enter:

- Username: root
- Domain Name: "School Trigram" + "Student initia" + 2 digits

The name supplied under Domain Name will subsequently become the name of your tenant as **MSGO1.onmicrosoft.com**

>Password: NeverTrustAny1!

How you'll sign in

60% Tasks Complete

< Previous Next: Exercise 2: Enforce MFA... >

Credit card required – Step Skipped

(ING) LAB1 - The foundations of hybrid identity

SRV01

InPrivate https://labclient.labondemand.com/LabClient/Searc... 43 Minutes Remaining

Instructions Resources Help Search 100%

Task 3: Create and configure Azure AD users

In this task, you will configure Azure AD user accounts in the newly created Azure AD tenant with the following settings. This will include assigning EM+S ES licenses to the user account you are using for this lab as well as creating a new Azure AD user account with the same settings and assigning to it the Global Administrator role as well as the EM+S ES license.

1. Log on to SRV01

Username: Administrator@contoso.com

Password: NeverTrustAny1!

2. Open the Azure portal & navigate to the Azure AD blade: https://portal.azure.com/?feature.msajis=false&view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade/#/AllUsers

3. Select **Users** under **Manage** in the left navigation.

4. On the **Users - All users** blade, select the entry representing your user account.

5. On the **Properties** of your user account.

6. In the **Settings** section, in the **Usage location** dropdown list, select the **France** entry and select **Save**.

7. On the **Profile** blade of your user account, select **Licenses** under **Manage** on the left.

8. On the **Licenses** blade, select **+ Assignments**.

9. On the **Update license assignments** blade, enable the **Enterprise Mobility + Security ES** checkbox, ensure that all the corresponding license options are enabled, and select **Save**.

10. On the **Users - All users** blade, select **+ New user**.

11. On the **New user** blade, ensure that the **Create user** option is selected, specify the following settings, and select **Create**:

User name:

61% Tasks Complete

< Previous Next: Exercise 2: Enforce MFA... >

Module 1 – Lab 1 – The foundations of hybrid identity

The screenshot shows the Microsoft Azure portal interface. On the left, a navigation sidebar lists options like Overview, Audit logs, Sign-in logs, Diagnose and solve problems, Manage (Assigned roles, Administrative units, Groups, Applications, Licenses, Devices), Troubleshooting + Support, and New support request. The main content area displays user details for 'Thomas PEUGNET'. Under the 'Properties' tab, it shows basic information such as Display name (Thomas PEUGNET), First name (Thomas), Last name (PEUGNET), User principal name (root@eftp01.onmicrosoft.com), Object ID (09578e7e-6697-41bf-be9f-75a53320b00), Identities (eftp01.onmicrosoft.com), User type (Member), Creation type (Created), Creation date (Jan 24, 2024, 10:17 AM), Last password change date (Jan 24, 2024, 10:17 AM), and various contact details like Street address, City, State or province, ZIP or postal code, Country or region (FR), Business phone (0613764291), Mobile phone, Email, Other emails, Proxy addresses, Fax number, IM addresses, Mail nickname (root), and Parental controls. Below this, there are sections for Preferred language (en), Consent provided for minor, Legal age group classification, and a note about activating Windows. On the right, a task pane titled '(ING) LAB1 - The foundations of hybrid identity' provides step-by-step instructions for configuring Azure AD user accounts, including logging on to SRV01, navigating to the Azure portal, selecting users under Manage, and assigning licenses. It also includes a note about enabling Enterprise Mobility + Security (EMS) licenses.

This screenshot shows the Microsoft Azure portal interface, similar to the previous one but focusing on licenses. The left sidebar shows the same navigation options. The main content area displays the 'Licenses' section for 'Thomas PEUGNET'. It shows a table with columns: Products, State, Enabled Services, and Assignment Paths. There is one entry: Microsoft Entra ID Governance, Active, 1/1, Direct. Below the table, there is a note about activating Windows. On the right, the task pane '(ING) LAB1 - The foundations of hybrid identity' continues the configuration steps, specifically detailing how to assign EMS licenses to the user account.

Module 1 – Lab 1 – The foundations of hybrid identity

(ING) LAB1 - The foundations of hybrid identity

In this task, you will configure Azure AD user accounts in the newly created Azure AD tenant with the following settings. This will include assigning EM+S E5 licenses to the user account you are using for this lab as well as creating a new Azure AD user account with the following settings and assigning to it the Global Administrator role as well as the EM+S E5 license.

Instructions Resources Help

41 Minutes Remaining

1. Log on to SRV01

Username: Administrator@contoso.com
Password: NeverTrustAny1!

2. Open the in the Azure portal & navigate to the Azure AD blade: https://portal.azure.com/?feature.msajs=false&view/Microsoft_AAD_IAM/ActiveDirect...

3. Select Users under Manage in the left navigation.

4. On the Users - All users blade, select the entry representing your user account.

5. On the Properties of your user account.

6. In the Settings section, in the Usage location dropdown list, select the France entry and select Save.

7. On the Profile blade of your user account, select Licenses under Manage on the left.

8. On the Licenses blade, select + Assignments.

9. On the Update license assignments blade, enable the Enterprise Mobility + Security E5 checkbox, ensure that all the corresponding license options are enabled, and select Save.

10. On the Users - All users blade, select + New user.

11. On the New user blade, ensure that the Create user option is selected, specify the following settings, and select Create:

User name: jdoe@TenantName.onmicrosoft.com

63% Tasks Complete

< Previous Next: Exercise 2: Enforce MFA... >

When a user has both direct and inherited licenses, only the direct license assignment is removed when you uncheck a license check box. Inherited licenses are unavailable to assign or remove directly. User can also be migrated between licenses.

Select Licenses

Review license options

Microsoft Entra ID Governance

Microsoft Entra ID Governance

Entra Identity Governance

Activate Windows
Go to Settings to activate Windows.

(ING) LAB1 - The foundations of hybrid identity

In this task, you will manage user accounts in the newly created Azure AD tenant with the following settings. This will include creating a new user account with the following settings and assigning to it the Global Administrator role as well as the EM+S E5 license.

Instructions Resources Help

39 Minutes Remaining

1. Open the in the Azure portal & navigate to the Azure AD blade: https://portal.azure.com/?feature.msajs=false&view/Microsoft_AAD_UsersAndTenants/UserManagementBlade#/AllUsers

2. On the Users - All users blade, select + New user.

3. Create new user

Create a new internal user in your organization

Invite external user

Invite an external user to collaborate with your organization

User principal name: jdoe

User type: Member

On-premises sync: No

Identities: efrt01.onmicrosoft.com

Company name:

Activate Windows
Go to Settings to activate Windows.

New user

Name: John Doe

First name: John

Last name: Doe

Select Let me create the password

Password: 1LoveSecurity!

Groups: 0 group selected

Roles: Leave blank

Block sign in: No

Usage location: France

64% Tasks Complete

< Previous Next: Exercise 2: Enforce MFA... >

Module 1 – Lab 1 – The foundations of hybrid identity

The screenshot shows the Microsoft Azure portal interface. On the left, the 'Overview' tab is selected under the 'John Doe' user card. The 'Basic info' section displays the user's principal name (jdoe@efrtp01.onmicrosoft.com), object ID (1f8ca5bf-0cd3-43e1-873e-92aa72674c7), creation date (Jan 24, 2024, 10:49 AM), user type (Member), and identities (efrtp01.onmicrosoft.com). To the right, a sidebar titled '(ING) LAB1 - The foundations of hybrid identity' provides instructions for configuring hybrid identity. Step 12 is checked, indicating the user has been successfully created in Azure AD.

The screenshot shows the 'Update license assignments' blade for user 'John Doe'. Under the 'Select licenses' section, 'Microsoft Entra ID Governance' is selected. In the 'Review license options' dropdown, 'Microsoft Entra ID Governance' is also selected. A note at the top states: 'When a user has both direct and inherited licenses, only the direct license assignment is removed when you uncheck a license check box. Inherited licenses are unavailable to assign or remove directly. User can also be migrated between licenses.' To the right, the same hybrid identity configuration sidebar is visible, showing step 12 is completed.

Module 1 – Lab 1 – The foundations of hybrid identity

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with 'InPrivate' and 'Azure free account'. The main area is titled 'Add users and groups' under 'Assign license'. It shows a search bar with 'John Doe' and two results found. Below is a table with columns 'Name', 'Type', and 'Details'. Two users are listed: 'John Doe' (User, jdoe@eftp01.onmicrosoft.com) and 'Thomas PEUGNET' (User, root@eftp01.onmicrosoft.com). On the right, a task pane titled '(ING) LAB1 - The foundations of hybrid identity' provides step-by-step instructions for license assignment, including selecting users and managing assignments.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with 'InPrivate' and 'Azure free account'. The main area is titled 'Create new user' under 'Users'. It shows tabs for 'Basics', 'Properties', 'Assignments' (which is selected), and 'Review + create'. Below is a section for 'Choose admin roles' with a dropdown menu set to 'Global'. It lists three roles: 'Global Administrator', 'Global Reader', and 'Global Secure Access Administrator'. Each role has a description. On the right, a task pane titled '(ING) LAB1 - The foundations of hybrid identity' provides step-by-step instructions for creating a new user, including selecting roles and managing assignments.

Module 1 – Lab 1 – The foundations of hybrid identity

The screenshot shows the Microsoft Azure portal interface. On the left, the 'Users' blade is open, displaying a list of users including 'John Doe' and 'Thomas PEUGNET'. On the right, a task list titled 'Task 4: Install Azure AD Connect' is visible, with several steps listed:

- 1. Download Azure AD Connect from <https://www.microsoft.com/en-us/download/details.aspx?id=47594>
- 2. Start the installation in **customize mode** **NOT use express settings**
- 3. Select **Password Hash Synchronization** & select **Enable single sign-on**
- 4. Log in with your Azure AD Global Admin account.
- 5. Add Contoso.com and log in with the Domain admin credentials:

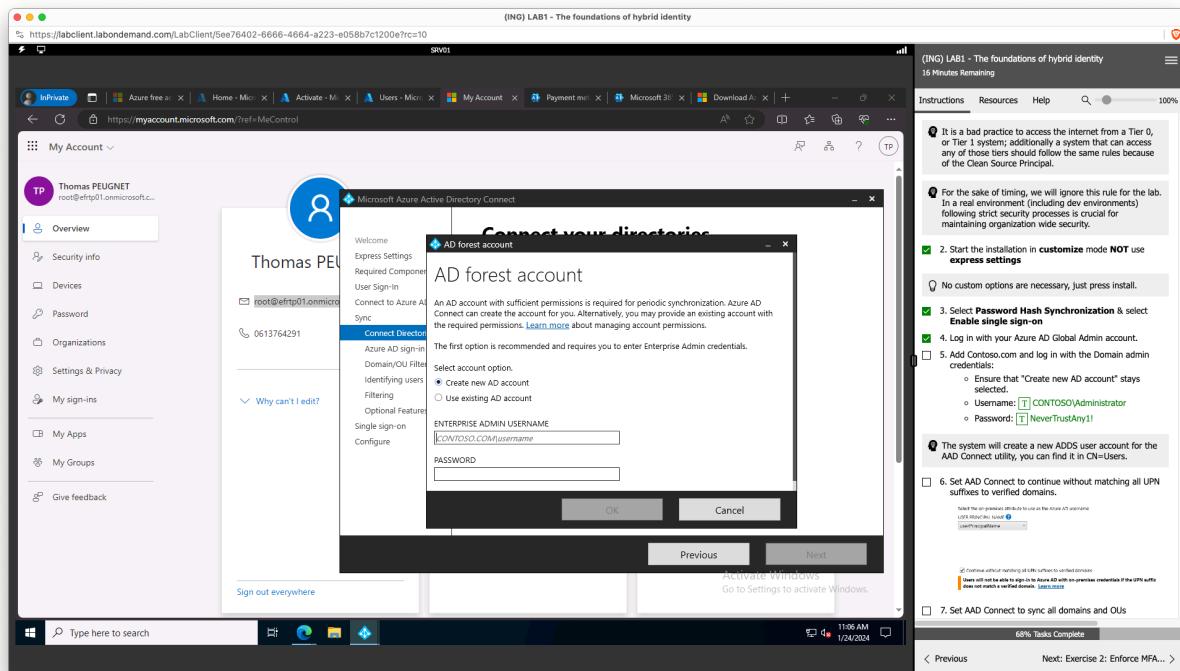
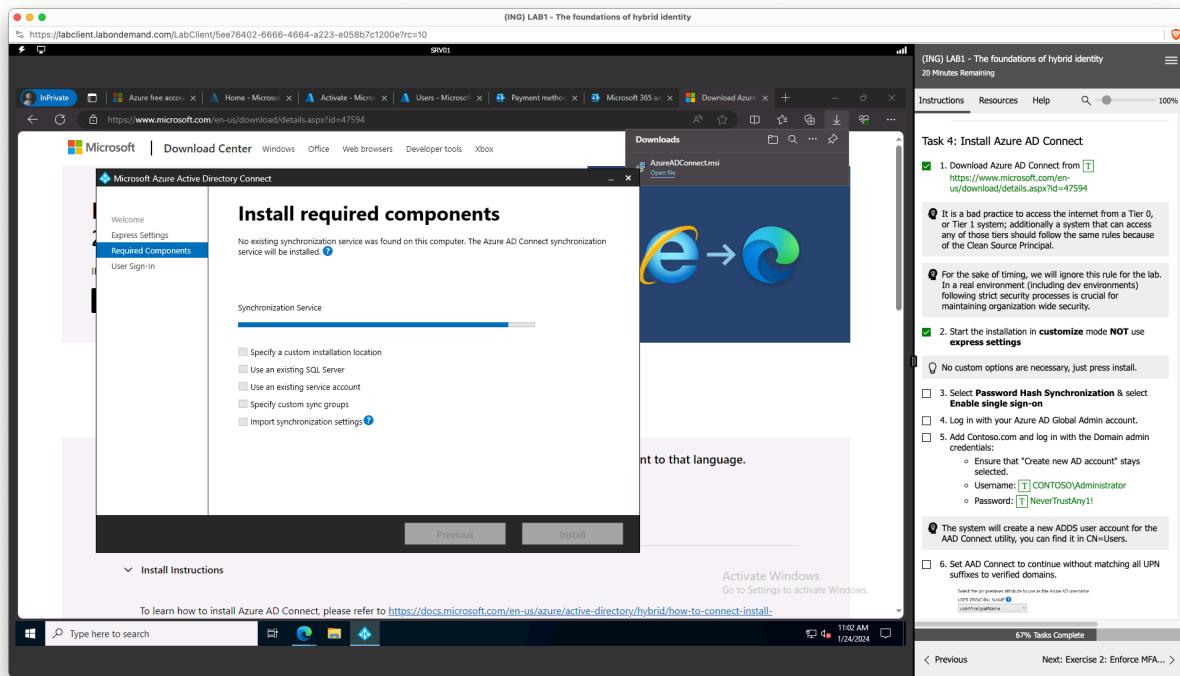
The task list indicates 67% completion. The Windows taskbar at the bottom shows the date as 1/24/2024.

The screenshot shows the 'Install required components' step of the Microsoft Azure Active Directory Connect setup wizard. The wizard interface includes tabs for 'Welcome', 'Express Settings', 'Required Components' (which is selected), and 'User Sign-in'. The 'Required Components' tab lists several options:

- Specify a custom installation location
- Use an existing SQL Server
- Use an existing service account
- Specify custom sync groups
- Import synchronization settings

A large blue button labeled 'Install' is prominent at the bottom. To the right, there is a preview window showing the synchronization process between an 'e' icon and a 'cloud' icon. The task list on the right side of the screen remains the same as in the previous screenshot.

Module 1 – Lab 1 – The foundations of hybrid identity



Module 1 – Lab 1 – The foundations of hybrid identity

Microsoft Azure Active Directory Connect

Azure AD sign-in configuration

To sign-in to Azure with the same credentials as your on-premises directory, a matching Azure AD Domain is required. The following table lists the UPN suffixes for your on-premises environment and the status of the associated Azure AD Domain.

Active Directory UPN Suffix	Azure AD Domain
contoso.com	Not Added

Select the on-premises attribute to use as the Azure AD username

USER PRINCIPAL NAME

checkbox: Continue without matching all UPN suffixes to verified domains
Users will not be able to sign-in to Azure AD with on-premises credentials if the UPN suffix does not match a verified domain. [Learn more](#)

Previous Next

Sign out everywhere

Activate Windows Go to Settings to activate Windows.

11:08 AM 1/24/2024

Instructions Resources Help

5. Add Contoso.com and log in with the Domain admin credentials:
a. Ensure that "Create new AD account" stays selected.
b. Username: CONTOSO\Administrator
c. Password: NeverTrustAny1!
The system will create a new AD DS user account for the AAD Connect utility, you can find it in CN=Users.

6. Set AAD Connect to continue without matching all UPN suffixes to verified domains.
Select the on-premises attribute to use as the Azure AD username
CONTOSO\LocalUser
checkbox: Create additional bindings at UPN suffixes to verified domains
Users will not be able to sign-in to Azure AD with on-premises credentials if the UPN suffix does not match a verified domain. [Learn more](#)

7. Set AAD Connect to sync all domains and OUs
Note: In production, you can select some OU instead All Domains.

Question:
o What is the goal of the filtering ?
o "Next" through the rest of the wizard.

8. At Enable single sign-on, enter your TO Admin credential
Question:
o What is the goal of SSO?
o Why is it Seamless?

10. At Ready to configure, click Start configuration
69% Tasks Complete

< Previous Next: Exercise 2: Enforce MFA... >

Microsoft Azure Active Directory Connect

Configuring

Creating the Azure Active Directory Synchronization Account

After setting up the user sync, we will want to validate that the sync connection has been established correctly.

Previous Retry

Activate Windows Go to Settings to activate Windows.

11:08 AM 1/24/2024

Instructions Resources Help

12 Minutes Remaining

Task 5: Check directory synchronization
If for some reasons the installation of Azure AD Connect crash, Double click on the Azure AD Connect icon on the desktop.

1. Go to Azure Active Directory in the Azure portal: https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade
2. In the blade menu, select **Users - All Users**. You should see lots of users in the list who have the **DirectWrite Enabled** column with an attribute of "Yes" or "No" for each user.

Task 6: Disable security defaults
By default, all new tenants are **Security Defaults** enabled. That's force users & administrators to have MFA. For the rest of the lab, we need to disable this feature, and if you use Conditional Access in Production, you will also disable it.

1. Go to Azure Active Directory in the Azure portal: https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade
2. In the blade menu, select **Properties, Manage security defaults**
3. Select **NO**
4. Save

Summary:
In this exercise, you integrated an Active Directory forest with

74% Tasks Complete

< Previous Next: Exercise 2: Enforce MFA... >

Module 1 – Lab 1 – The foundations of hybrid identity

(ING) LAB1 - The foundations of hybrid identity

SRV01

https://labclient.labondemand.com/LabClient/Sessions/6402-6666-4664-a223-e058b7c1200e?rc=10

Microsoft Azure | Search resources, services and docs (G+)

Home > CONTOSO | Users >

Users ...

CONTOSO - Microsoft Entra ID

All users Audit logs Sign-in logs Diagnose and solve problems Manage Deleted users Password reset User settings Bulk operation results Troubleshooting + Support New support request

Search

Azure Active Directory is now Microsoft Entra ID.

4 users found

Display name	User principal name	User type	On-premises sync	Identities	Company name
John Doe	admaz-jdoe@efrtp01.onmicrosoft.com	Member	No	efrtp01.onmicrosoft.com	
John Doe	jdoe@efrtp01.onmicrosoft.com	Member	No	efrtp01.onmicrosoft.com	
On-Premises Directory Sync	Sync_SRV01_17e3220d2a...	Member	Yes	efrtp01.onmicrosoft.com	

Thomas PEUGNET

root@efrtp01.onmicrosoft.com

Member

No

efrtp01.onmicrosoft.com

Activate Windows
Go to Settings to activate Windows.

https://aka.ms/AADRebrandRQ

Type here to search

11:13 AM 1/24/2024

ING LAB1 - The foundations of hybrid identity

39 Minutes Remaining

Instructions Resources Help

If for some reasons the installation of Azure AD Connect crash, Double click on the Azure AD Connect icon on the desktop.

Task 5: Check directory synchronization

After setting up the user sync, we will want to validate that the sync connection has been established correctly.

1. Go to Azure Active Directory in the Azure portal. https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade

2. In the blade menu, select **Users** → **All users**. You should see lots of users in the directory who have the **Directory Synced** column with an attribute of "Yes" or "No" for each users.

Task 6: Disable security defaults

By default, all new tenants are **Security Defaults** enabled. That's force user & administrators to have MFA. For the rest of the lab, we need to disable this feature, and if you use Conditional Access in Production, you will also disable it.

1. Go to Azure Active Directory in the Azure portal. https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade

2. In the blade menu, select **Properties**, **Manage security defaults**

3. Select **NO**

4. Save

Summary:
In this exercise, you integrated an Active Directory forest with

71% Tasks Complete

< Previous Next: Exercise 2: Enforce MFA... >

(ING) LAB1 - The foundations of hybrid identity

SRV01

https://labclient.labondemand.com/LabClient/Sessions/6402-6666-4664-a223-e058b7c1200e?rc=10

Microsoft Azure | Search resources, services and docs (G+)

Home > CONTOSO - Microsoft Entra ID

All users Audit logs Sign-in logs Diagnose and solve problems Manage Deleted users Password reset User settings Bulk operation results Troubleshooting + Support New support request

Search

Azure Active Directory is now Microsoft Entra ID.

70 users found

Display name	User principal name	User type	On-premises sync	Identities	Company name
John Doe	admaz-jdoe@efrtp01.onmicrosoft.com	Member	No	efrtp01.onmicrosoft.com	
Thomas PEUGNET	tp-Adm@efrtp01.onmicrosoft.com	Member	Yes	efrtp01.onmicrosoft.com	
Abbie Spencer	Abbie.Spencer@efrtp01.onmicrosoft.com	Member	Yes	efrtp01.onmicrosoft.com	
Abigail Storey	Abigail.Storey@efrtp01.onmicrosoft.com	Member	Yes	efrtp01.onmicrosoft.com	
Admin1	Admin1@efrtp01.onmicrosoft.com	Member	Yes	efrtp01.onmicrosoft.com	
Admin2	Admin2@efrtp01.onmicrosoft.com	Member	Yes	efrtp01.onmicrosoft.com	
Alyssa Roy	Alyssa.Roy@efrtp01.onmicrosoft.com	Member	Yes	efrtp01.onmicrosoft.com	
Amelie Parsons	Amelie.Parsons@efrtp01.onmicrosoft.com	Member	Yes	efrtp01.onmicrosoft.com	
AppId	AppId@efrtp01.onmicrosoft.com	Member	Yes	efrtp01.onmicrosoft.com	
CAudit	_caudit@efrtp01.onmicrosoft.com	Member	Yes	efrtp01.onmicrosoft.com	
Cheryl Osborne	Cheryl.Osborne@efrtp01.onmicrosoft.com	Member	Yes	efrtp01.onmicrosoft.com	
Connie Flores	Connie.Flores@efrtp01.onmicrosoft.com	Member	Yes	efrtp01.onmicrosoft.com	
Connie Flores Admin	connie.flor.es.adm@efrtp01.onmicrosoft.com	Member	Yes	efrtp01.onmicrosoft.com	
das	das@efrtp01.onmicrosoft.com	Member	Yes	efrtp01.onmicrosoft.com	

Activate Windows
Go to Settings to activate Windows.

https://portal.azure.com/#blade/Microsoft_AAD_UsersAndTenants/MultiValueReactView/title/identities/subtitle/Amelie.Parsons/items/%3A%2FSign-in-type%3A%2FUserPrincipalName%2C%2FIssuer%3A%2FIssuerAssignedID%3A%2Fmore...%2F

Type here to search

11:23 AM 1/24/2024

ING LAB1 - The foundations of hybrid identity

30 Minutes Remaining

Instructions Resources Help

Exercise 2: Enforce MFA for Global Administrator

Duration: 10 minutes

Synopsis: In this exercise, you will setup and configure Multi Factor Authentication (MFA) for your admins, this is especially important for cloud accounts which may be susceptible to credential theft attempts. You can complete this outside of the lab if you wish. Remember to be logged into the correct account if you do this.

Task 1: Enable MFA for a Global Administrator

1. Log on to SRV01

Username: [Administrator@contoso.com](https://SRV01)
Password: [NeverTrustAny1!](https://SRV01)

2. Navigate to https://portal.azure.com/#blade/Microsoft_AAD_IAM/Users and log in with the credentials that correspond with the Azure AD you created in the first exercise.

3. Select the Per-User MFA button at the top menu.

4. Select the Root Global Admin account and click Enable.

In production you can bulk update users using CSV files.

MFA can be licensed and used in many ways, here is a breakdown of the options:

- MFA is free for Azure AD users who hold an administrator role
- A subset of MFA features is licensed with Office 365

Questions:

- Enabling MFA on a user can break inauthentic logins.

74% Tasks Complete

< Previous Next: Exercise 3: Overview of... >

Module 1 – Lab 1 – The foundations of hybrid identity

Microsoft Azure > CONTOSO

CONTOSO | Properties

Security defaults

Security defaults: Enabled (recommended)

Your organization is currently using security defaults.

Task 5: Check directory synchronization

After setting up the user sync, we will want to validate that the sync connection has been established correctly.

1. Go to Azure Active Directory in the Azure portal: https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/
2. In the blade menu, select **Users** → **All Users**. You should see lots of users in the directory who have the Directory Synced Column with an attribute of "Yes" or "No" for each user.

Task 6: Disable security defaults

By default, all new tenants are **Security Defaults** enabled. That's force user & administrators to have MFA. For the rest of the lab, we need to disable this feature, and if you use Conditional Access in Production, you will also disable it.

1. Go to Azure Active Directory in the Azure portal: https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/
2. In the blade menu, select **Properties**, **Manage security defaults**
3. Select **NO**

4. Save

Summary:

In this exercise, you integrated an Active Directory forest with an Azure Active Directory tenant by creating an Azure Active Directory tenant and activating an Enterprise Mobility + Security ES trial, creating and configuring an Azure AD user, and installing Azure AD Connect to configure Hybrid Identity.

72% Tasks Complete

Microsoft Azure > CONTOSO

CONTOSO | Properties

Security defaults

Security defaults: Disabled (not recommended)

⚠️ With security defaults disabled, your organization is vulnerable to common identity-related attacks.

Reason for disabling *

This feedback will be used to improve Microsoft products and services. View privacy statement.

My organization is unable to use apps/devices

Too many multifactor authentication sign-up requests

Too many sign-in multifactor authentication challenges

My organization is using Conditional Access

Other

don't care at all

Activate Windows

Save Cancel

Task 5: Check directory synchronization

After setting up the user sync, we will want to validate that the sync connection has been established correctly.

1. Go to Azure Active Directory in the Azure portal: https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/
2. In the blade menu, select **Users** → **All Users**. You should see lots of users in the directory who have the Directory Synced Column with an attribute of "Yes" or "No" for each user.

Task 6: Disable security defaults

By default, all new tenants are **Security Defaults** enabled. That's force user & administrators to have MFA. For the rest of the lab, we need to disable this feature, and if you use Conditional Access in Production, you will also disable it.

1. Go to Azure Active Directory in the Azure portal: https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/
2. In the blade menu, select **Properties**, **Manage security defaults**
3. Select **NO**

4. Save

Summary:

In this exercise, you integrated an Active Directory forest with an Azure Active Directory tenant by creating an Azure Active Directory tenant and activating an Enterprise Mobility + Security ES trial, creating and configuring an Azure AD user, and installing Azure AD Connect to configure Hybrid Identity.

72% Tasks Complete

Module 1 – Lab 1 – The foundations of hybrid identity

Exercise 2: Enforce MFA for Global Administrator

Task 1: Enable MFA for Global Administrators

Questions:

- 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?
 - o Déploiement basé sur les stratégies d'accès conditionnel
 - o Activation de MFA par le biais de groupes de sécurité

The screenshot shows a dual-monitor setup. The left monitor displays the Microsoft Azure Active Directory Multi-factor Authentication configuration page, specifically the 'multi-factor authentication' section under 'users'. It lists various users with their email addresses and current MFA status (all set to 'Disabled'). A 'bulk update' button is visible at the top right of the list. The right monitor displays a task list titled 'Exercise 2: Enforce MFA for Global Administrator' with the following steps:

1. Log on to SRV01
2. Navigate to https://portal.azure.com/#blade/Microsoft_AAD_IAM/Users
3. Select the Per-User MFA button at the top menu.
4. Select the Root Global Admin account and click Enable.

Below the tasks, there is a note: 'In production you can bulk update users using CSV files.' and a breakdown of MFA licensing: 'MFA can be licensed and used in many ways, here is a breakdown of the options:

- MFA is free for Azure AD users who hold an administrator role
- A subset of MFA features is licensed with Premium

' followed by a 'more...' link. At the bottom of the task list, it says '75% Tasks Complete'.

Module 1 – Lab 1 – The foundations of hybrid identity

multi-factor authentication

users service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users. Before you begin, take a look at the multi-factor auth deployment guide.

View: Global administrators Multi-Factor Auth status: Any bulk update

DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
(ADM) John Doe	admaz-jdoe@efrtp01.onmicrosoft.com	Disabled
Thomas PEUGNET	root@efrtp01.onmicrosoft.com	Disabled

Select a user

©2024 Microsoft Legal | Privacy

Activate Windows Go to Settings to activate Windows.

SRV01

(ING) LAB1 - The foundations of hybrid identity

Instructions Resources Help

Exercise 2: Enforce MFA for Global Administrator

Duration: 10 minutes

Synopsis: In this exercise you will setup and configure Multi Factor Authentication (MFA) for your admins, this is especially important for cloud accounts which may be susceptible to credential theft attempts. You can complete this outside of the lab if you wish; Remember to be logged into the correct account if you do this.

Task 1: Enable MFA for the a Global Administrator

1. Log on to SRV01

Username: Administrator@contoso.com
Password: NeverTrustAny1!

2. Navigate to https://portal.azure.com/#blade/Microsoft_AAD_IAM/Users and log in with the credentials that correspond with the Azure AD you created in the first Exercise.

3. Select the Per-User MFA button at the top menu.

4. Select the Root Global Admin account and click Enable.

In production you can bulk update users using CSV files.

MFA can be licensed and used in many ways, here is a breakdown of the options:

- MFA is free for Azure AD users who hold an administrator role
- A subset of MFA features is licensed with Office 365

more...

Questions:

- Enabling MFA on a new user hasn't yet been made available in Azure Active Directory.

75% Tasks Complete

< Previous Next: Exercise 3: Overview of... >

multi-factor authentication

users service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users. Before you begin, take a look at the multi-factor auth deployment guide.

View: Global administrators Multi-Factor Auth status: Any bulk update

DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
(ADM) John Doe	admaz-jdoe@efrtp01.onmicrosoft.com	Disabled
Thomas PEUGNET	root@efrtp01.onmicrosoft.com	Disabled

About enabling multi-factor auth

Please read the deployment guide if you haven't already.
If your users do not regularly sign in through the browser, you can send them to this link to register for multi-factor auth: https://aka.ms/MFASetup

enable multi-factor auth cancel

©2024 Microsoft Legal | Privacy

Activate Windows Go to Settings to activate Windows.

SRV01

(ING) LAB1 - The foundations of hybrid identity

Instructions Resources Help

Exercise 2: Enforce MFA for Global Administrator

Duration: 10 minutes

Synopsis: In this exercise you will setup and configure Multi Factor Authentication (MFA) for your admins, this is especially important for cloud accounts which may be susceptible to credential theft attempts. You can complete this outside of the lab if you wish; Remember to be logged into the correct account if you do this.

Task 1: Enable MFA for the a Global Administrator

1. Log on to SRV01

Username: Administrator@contoso.com
Password: NeverTrustAny1!

2. Navigate to https://portal.azure.com/#blade/Microsoft_AAD_IAM/Users and log in with the credentials that correspond with the Azure AD you created in the first Exercise.

3. Select the Per-User MFA button at the top menu.

4. Select the Root Global Admin account and click Enable.

In production you can bulk update users using CSV files.

MFA can be licensed and used in many ways, here is a breakdown of the options:

- MFA is free for Azure AD users who hold an administrator role
- A subset of MFA features is licensed with Office 365

more...

Questions:

- Enabling MFA on a new user hasn't yet been made available in Azure Active Directory.

75% Tasks Complete

< Previous Next: Exercise 3: Overview of... >

Module 1 – Lab 1 – The foundations of hybrid identity

Task 2: Test the MFA

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Microsoft Authenticator

Start by getting the app

On your phone, install the Microsoft Authenticator app. [Download now](#)

After you install the Microsoft Authenticator app on your device, choose "Next".

I want to use a different authenticator app

[Next](#)

I want to set up a different method

Activate Windows
Go to Settings to activate Windows.

INQ LAB1 - The foundations of hybrid identity
27 Minutes Remaining

Instructions Resources Help

4. Select the Root Global Admin account and click Enable.

In production you can bulk update users using CSV files.

MFA can be licensed and used in many ways, here is a breakdown of the options:

- MFA is free for Azure AD users who hold an administrator role.

more...

Questions:

- 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?

Task 2: Test the MFA

- Open a new Private/Incognito browsing session and navigate to <https://myapps.microsoft.com>
- Log into the service with the user that was just MFA enabled.
- Set up the user's MFA configuration when prompted.

You may be presented with an app password, these passwords are used for application which can't or don't support MFA.

- After the MFA configuration has been completed, log out and log back in to validate that MFA has been set up correctly.

Note: End users can navigate to <https://aka.ms/mfasetup> to change their MFA settings.

Summary:
In this exercise, you discover Azure AD users & groups.

76% Tasks Complete

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Microsoft Authenticator

Let's try it out

Approve the notification we're sending to your app by entering the number shown below.

47

[Back](#) [Next](#)

I want to set up a different method

Activate Windows
Go to Settings to activate Windows.

INQ LAB1 - The foundations of hybrid identity
26 Minutes Remaining

Instructions Resources Help

4. Select the Root Global Admin account and click Enable.

In production you can bulk update users using CSV files.

MFA can be licensed and used in many ways, here is a breakdown of the options:

- MFA is free for Azure AD users who hold an administrator role.

more...

Questions:

- 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?

Task 2: Test the MFA

- Open a new Private/Incognito browsing session and navigate to <https://myapps.microsoft.com>
- Log into the service with the user that was just MFA enabled.
- Set up the user's MFA configuration when prompted.

You may be presented with an app password, these passwords are used for application which can't or don't support MFA.

- After the MFA configuration has been completed, log out and log back in to validate that MFA has been set up correctly.

Note: End users can navigate to <https://aka.ms/mfasetup> to change their MFA settings.

Summary:
In this exercise, you discover Azure AD users & groups.

76% Tasks Complete

Module 1 – Lab 1 – The foundations of hybrid identity

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Microsoft Authenticator

Notification approved

Back Next

I want to set up a different method

Activate Windows
Go to Settings to activate Windows.

(ING) LAB1 - The foundations of hybrid identity

26 Minutes Remaining

Instructions Resources Help

4. Select the Root Global Admin account and click Enable.

In production you can bulk update users using CSV files.

MFA can be licensed and used in many ways, here is a breakdown of the options:

- MFA is free for Azure AD users who hold an administrator role
- A license for MFA is required to download with O365...

more...

Questions:

- 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?

Task 2: Test the MFA

1. Open a new Private/Incognito browsing session and navigate to <https://myapps.microsoft.com>

2. Log into the service with the user that was just MFA enabled.

3. Set up the user's MFA configuration when prompted.

You may be presented with an app password, these passwords are used for application which can't or don't support MFA.

4. After the MFA configuration has been completed, log out and log back in to validate that MFA has been set up correctly.

Note: End users can navigate to <https://aka.ms/mfasetup> to change their MFA settings.

Summary:
In this exercise, you discover Azure AD users & groups.

76% Tasks Complete

< Previous Next: Exercise 3: Overview of... >

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method:

Microsoft Authenticator

Done

Activate Windows
Go to Settings to activate Windows.

(ING) LAB1 - The foundations of hybrid identity

26 Minutes Remaining

Instructions Resources Help

4. Select the Root Global Admin account and click Enable.

In production you can bulk update users using CSV files.

MFA can be licensed and used in many ways, here is a breakdown of the options:

- MFA is free for Azure AD users who hold an administrator role
- A license for MFA is required to download with O365...

more...

Questions:

- 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?

Task 2: Test the MFA

1. Open a new Private/Incognito browsing session and navigate to <https://myapps.microsoft.com>

2. Log into the service with the user that was just MFA enabled.

3. Set up the user's MFA configuration when prompted.

You may be presented with an app password, these passwords are used for application which can't or don't support MFA.

4. After the MFA configuration has been completed, log out and log back in to validate that MFA has been set up correctly.

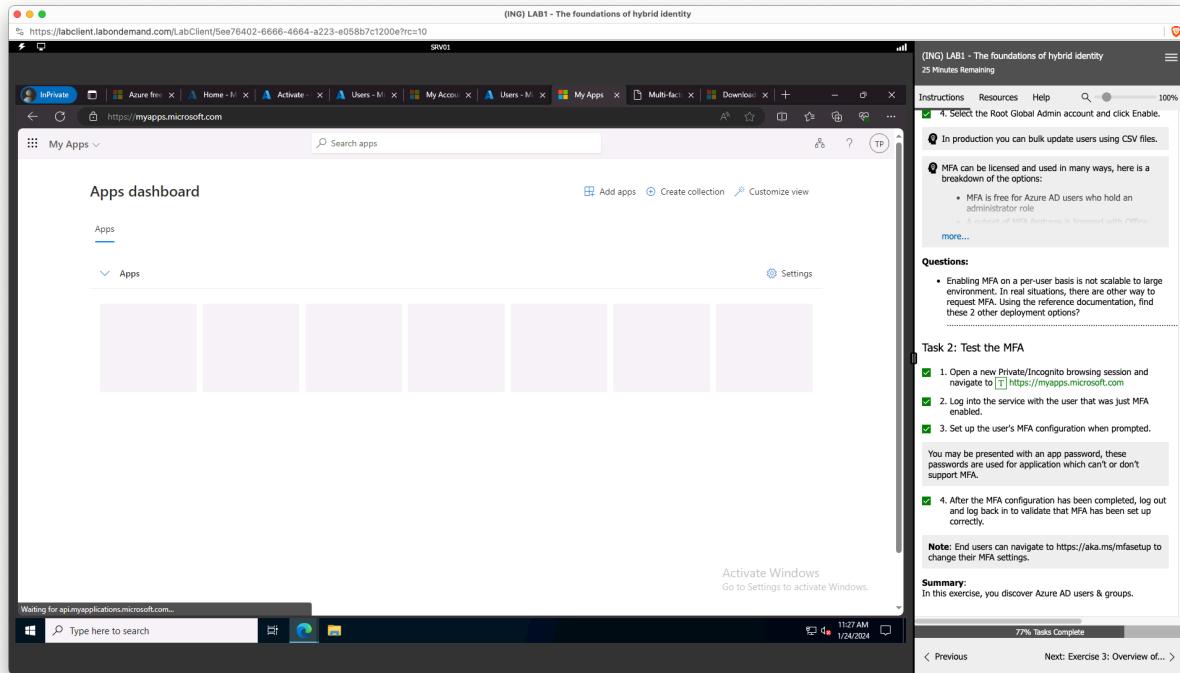
Note: End users can navigate to <https://aka.ms/mfasetup> to change their MFA settings.

Summary:
In this exercise, you discover Azure AD users & groups.

76% Tasks Complete

< Previous Next: Exercise 3: Overview of... >

Module 1 – Lab 1 – The foundations of hybrid identity



Exercise 3: Overview of Azure AD User & Group objects

Task 1: Play with Azure (create cloud user, create cloud security group, create a dynamic group & modify a group)

Question

- Why can't you change it?
 - o Je n'ai pas les droits suffisants. Mon Azure AD ne peut pas modifier un on Premise.

Module 1 – Lab 1 – The foundations of hybrid identity

The screenshot shows the Microsoft Azure portal's Overview page for the CONTOSO tenant. The left sidebar includes sections for Overview, Preview features, Diagnose and solve problems, Manage (Users, Groups, External identities, Roles and administrators, Administrative units, Delegated admin partners, Enterprise applications, Devices, App registrations, Identity Governance, Application proxy, Custom security attributes, Licenses, Cross-tenant synchronization, and Microsoft Entra Connect), and a note about waiting for management.azure.com. The main area displays basic information like Name (CONTOSO), Tenant ID (27c198df-129f-47a2-a129-4914ae8143cc), Primary domain (eftp01.onmicrosoft.com), License (Microsoft Entra ID Free), and a warning about Microsoft Entra Connect v1 Retirement. A banner at the bottom left mentions 'Waiting for management.azure.com...'. On the right, there's a task bar for Exercise 3: Overview of Azure AD User & Group objects, which includes tasks like logging on to SRV01, navigating to https://portal.azure.com, and modifying a group named Paris Prod.

The screenshot shows the Microsoft Azure portal's Groups blade for the Paris Prod group. The left sidebar lists Members, Owners, Roles and administrators, Administrative units, Group memberships, Applications, Licenses, Azure role assignments, Activity (Access reviews, Audit logs, Bulk operation results), and Troubleshooting + Support. The main area shows the Paris Prod group details, including Membership type (Assigned), Source (Windows Server AD), Type (Security), Object ID (b9d38fed-cc53-44fb-b4c8-c97debc14e73), and Created at (1/24/2024, 11:13:46 AM). It also shows Direct members (5 total, 5 user(s), 0 group(s), 0 device(s), 0 other(s)), Group memberships (0), Owners (0), and Total members (5). A banner at the bottom left mentions 'Waiting for management.azure.com...'. On the right, there's a task bar for Exercise 3: Overview of Azure AD User & Group objects, which includes tasks like logging on to SRV01, navigating to https://portal.azure.com, and modifying a group named Paris Prod.

Module 1 – Lab 1 – The foundations of hybrid identity

(ING) LAB1 - The foundations of hybrid identity

SRV01

Microsoft Azure | Search resources, services and docs (G+)

Home > CONTOSO | Groups > Groups | All groups > Paris Prod

Paris Prod | Properties

Overview | Save | Discard | Got feedback?

General settings

Some groups can't be managed in the Azure portal. Learn where to manage these groups.

Group name: Paris Prod

Group description: Enter a description for the group

Group type: Security

Membership type: Assigned

Object ID: b9d38fed-cc53-44fb-b4c8-c97debc14e73

Microsoft Entra roles can be assigned to the group: Yes

Group writeback state: No writeback

Activate Windows. Go to Settings to activate Windows.

Instructions | Resources | Help | 23 Minutes Remaining

Exercise 3: Overview of Azure AD User & Group objects

Duration: 20 minutes

Synopsis: In this exercise, you will discover users & groups in Azure AD

Task 1: Play with Azure (create cloud user, create cloud security group, create a dynamic group & modify a group)

1. Log on to SRV01

Username: administrator@contoso.com
Password: NeverTrustAny1!

2. In the Edge browser window, navigate to the following URL in a tab. <https://portal.azure.com>

3. Search & Select **Azure Active Directory** in the search bar

4. Modify a the Group named **Paris Prod** by adding a member

Question

Why can't you change it?

5. Create 2 Cloud only users for emergency (Breaking Glass Accounts)

On the **Users - All users** blade, select + New user.

On the **New user** blade, ensure that the **Create user** option is selected, specify the following settings, and select **Create**:

User name: admz-BGAI@TenantName.onmicrosoft.com
Name: Breaking Glass Accounts 1
Password: NeverTrustAny1!
Groups: 0 group selected
Roles: Global Administrator
Block sign-in: No
Usage: Personal

79% Tasks Complete

< Previous | Next: Exercise 4: Enable Self... >

(ING) LAB1 - The foundations of hybrid identity

SRV01

Microsoft Azure | Search resources, services and docs (G+)

Home > CONTOSO | Users > Users

Create new user

Create a new internal user in your organization

Basics | Properties | Assignments | Review + create

Create a new user in your organization. This user will have a user name like alice@contoso.com. Learn more

Identity

User principal name: eftp01.onmicrosoft.com
Domain not listed

Mail nickname: alice
Derive from user principal name

Display name: Alice

Password: *****, Auto-generate password

Account enabled: Yes

Review + create | < Previous | Next: Properties >

Activate Windows. Go to Settings to activate Windows. Give feedback

Instructions | Resources | Help | 22 Minutes Remaining

Exercise 3: Overview of Azure AD User & Group objects

Duration: 20 minutes

Synopsis: In this exercise, you will discover users & groups in Azure AD

Task 1: Play with Azure (create cloud user, create cloud security group, create a dynamic group & modify a group)

2. In the Edge browser window, navigate to the following URL in a tab. <https://portal.azure.com>

3. Search & Select **Azure Active Directory** in the search bar

4. Modify a the Group named **Paris Prod** by adding a member

Question

Why can't you change it?

5. Create 2 Cloud only users for emergency (Breaking Glass Accounts)

On the **Users - All users** blade, select + New user.

On the **New user** blade, ensure that the **Create user** option is selected, specify the following settings, and select **Create**:

User name: admz-BGAI@TenantName.onmicrosoft.com
Name: Breaking Glass Accounts 1
Password: NeverTrustAny1!
Groups: 0 group selected
Roles: Global Administrator
Block sign-in: No
Usage: Personal

79% Tasks Complete

< Previous | Next: Exercise 4: Enable Self... >

Module 1 – Lab 1 – The foundations of hybrid identity

The screenshot shows the Microsoft Azure portal interface. On the left, the 'Users' blade is open for the 'CONTOSO - Microsoft Entra ID' tenant. It displays a list of 70 users, including columns for Display name, User principal name, User type, On-premises sync status, Identities, and Company name. A message box indicates 'Successfully created user' for a new user named 'Breaking Glass Accounts 1'. On the right, a separate window titled '(ING) LAB1 - The foundations of hybrid identity' is displayed, showing a step-by-step lab exercise. Step 5 asks to 'Create 2 Cloud only users for emergency (Breaking Glass Accounts)'. Step 6 asks to 'Create with the same procedure to create Breaking Glass Accounts 2'. Step 7 asks to 'Find him in AD DS'. The lab progress is at 79% tasks complete.

This screenshot is similar to the one above, showing the Microsoft Azure portal and the lab exercise window. The user list in the Azure blade has been updated to include two new users: 'Breaking Glass Accounts 1' and 'Breaking Glass Accounts 2'. The lab exercise window shows steps 6 and 7 completed, and step 8 partially completed, asking to 'Create a security Group Named SG_Privileged_Accounts'. The lab progress is now at 100% tasks complete.

Module 1 – Lab 1 – The foundations of hybrid identity

(ING) LAB1 - The foundations of hybrid identity

Instructions Resources Help 19 Minutes Remaining

Groups: 0 group selected

Roles: Global Administrator

Block sign-in: No

Usage location: France

Job title: Leave blank

Department: Leave blank

6. Create with the same procedure to create Breaking Glass Accounts 2

7. Find him in ADDS

- Open DSA.msc
- Right click and select Find. Search your user creation

Questions:

- Do you find it?
- Why?

8. In Azure AD, Create a security Group Named SG_Privileged_Accounts

- Select Azure AD roles can be assigned to the group (at Yes)
- Add all Global Administrators as members
 - Your first account creating during Tenant creation, 2 BGA & Jdoe admin account

Don't forget to specify the owner ('You')

9. Create a Dynamic Group Named SG_d_Privileged_Accounts

80% Tasks Complete

< Previous Next: Exercise 4: Enable Self.. >

(ING) LAB1 - The foundations of hybrid identity

Instructions Resources Help 19 Minutes Remaining

Groups: 0 group selected

Roles: Global Administrator

Block sign-in: No

Usage location: France

Job title: Leave blank

Department: Leave blank

6. Create with the same procedure to create Breaking Glass Accounts 2

7. Find him in ADDS

- Open DSA.msc
- Right click and select Find. Search your user creation

Questions:

- Do you find it?
- Why?

8. In Azure AD, Create a security Group Named SG_Privileged_Accounts

- Select Azure AD roles can be assigned to the group (at Yes)
- Add all Global Administrators as members
 - Your first account creating during Tenant creation, 2 BGA & Jdoe admin account

Don't forget to specify the owner ('You')

9. Create a Dynamic Group Named SG_d_Privileged_Accounts

80% Tasks Complete

< Previous Next: Exercise 4: Enable Self.. >

Module 1 – Lab 1 – The foundations of hybrid identity

The screenshot shows a Windows desktop environment with a taskbar at the bottom. On the desktop, there is a Microsoft Edge browser window titled '(ING) LAB1 - The foundations of hybrid identity' displaying a lab exercise. The browser URL is <https://labclient.labondemand.com/LabClient/See76402-6666-4664-a223-e058b7c1200?rc=10>. The browser tabs include 'Azure free', 'Home - M...', 'Activate - M...', 'Users - M...', 'My Account - M...', 'Users - M...', 'Multi-factor - M...', 'Download - M...', and 'Multi-factor - M...'. The main content area of the browser shows the 'Active Directory Users and Computers' console with a list of users under the 'contoso.com' domain. To the right of the browser, there is a 'Questions' section with several numbered tasks and questions, some of which are checked off. A progress bar at the bottom right indicates '80% Tasks Complete'. Below the browser, the Windows taskbar has icons for Start, File Explorer, Task View, and other system applications.

This screenshot is nearly identical to the one above, showing the same Windows desktop environment, Microsoft Edge browser, and 'Active Directory Users and Computers' console. The difference is in the 'Active Directory Users and Computers' interface itself. In the previous screenshot, the 'contoso.com' tree was expanded. In this screenshot, the 'contoso.com' node is collapsed, and a context menu is open over it, showing options like 'Find...', 'New...', 'Refresh', 'Export List...', 'Properties', and 'Help'. The rest of the interface, including the browser-based lab exercise and the 'Questions' section, remains the same.

Module 1 – Lab 1 – The foundations of hybrid identity

The screenshot shows a Windows desktop with two windows open. The background window is 'Active Directory Users and Computers' showing a list of users in the 'contoso.com' domain. The foreground window is 'Microsoft Azure Active Directory - All users' showing a 'Create New User' form. The user is creating a new user named 'Breaking Glass Accounts 1' with the password 'NeverTrustAny1' and selecting 'Global Administrator' as the role. The 'Groups' field is set to '0 group selected'. The 'Instructions' tab is selected in the Azure window.

Questions:

- Do you find it?
 - o Non
- Why?
 - o La synchronisation est unilatérale, pour cette raison qu'il n'apparaît pas.

Module 1 – Lab 1 – The foundations of hybrid identity

(ING) LAB1 - The foundations of hybrid identity

13 Minutes Remaining

Instructions Resources Help

9. Create a Dynamic Group Named ✓

o Create a new group with the **Membership type** selected to **Dynamic User**

o Set this rules : `(userPrincipalName - startsWith "admaz")`

The refresh can take 24h, we will review it in the Lab6

Questions:

- o How many accounts are expected to be member of the dynamic group ?
- o Why ?

10. Delete Jdoe Admin account

- o Go to User blade, select Jdoe Admin account and delete it

11. Using the documentation located at <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/>, restore it

Questions:

- o Does John Doe have their groups membership restored ?
- o Does John Doe have their roles membership restored ?
- o Can you permanently delete a account ?

Summary: 81% Tasks Complete

< Previous Next: Exercise 4: Enable Self.. >

Activate Windows
Go to Settings to activate Windows.

SRV01

https://labclient.labondemand.com/LabClient/See76402-6666-4664-a223-e058b7c1200e?rc=10

Microsoft Azure | Search resources, services and docs (G+)

Home > CONTOSO | Users > Users

CONTOSO - Microsoft Entra ID

All users Audit logs Sign-in logs Diagnose and solve problems Manage Deleted users Password reset User settings Bulk operation results Troubleshooting + Support New support request

New user Download users Bulk operations Refresh Manage view Delete Per-user MFA Got feedback?

Display name User principal name User type On-premises sync Identities Company name Created

Jodie Richards Jodie.Richards@efrtp01.onmicrosoft.com Member Yes efrtp01.onmicrosoft.com

Jennifer Davey Jennifer.Davey@efrtp01.onmicrosoft.com Member Yes efrtp01.onmicrosoft.com

John Doe jdoe@efrtp01.onmicrosoft.com Member No efrtp01.onmicrosoft.com

(ADM) John Doe admaz:jdoe@efrtp01.onmicrosoft.com Member No efrtp01.onmicrosoft.com

(ING) LAB1 - The foundations of hybrid identity

13 Minutes Remaining

Instructions Resources Help

9. Create a Dynamic Group Named ✓

o Create a new group with the **Membership type** selected to **Dynamic User**

o Set this rules : `(userPrincipalName - startsWith "admaz")`

The refresh can take 24h, we will review it in the Lab6

Questions:

- o How many accounts are expected to be member of the dynamic group ?
- o Why ?

10. Delete Jdoe Admin account

- o Go to User blade, select Jdoe Admin account and delete it

11. Using the documentation located at <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/>, restore it

Questions:

- o Does John Doe have their groups membership restored ?
- o Does John Doe have their roles membership restored ?
- o Can you permanently delete a account ?

Summary: 81% Tasks Complete

< Previous Next: Exercise 4: Enable Self.. >

Activate Windows
Go to Settings to activate Windows.

SRV01

https://labclient.labondemand.com/LabClient/See76402-6666-4664-a223-e058b7c1200e?rc=10

Microsoft Azure | Search resources, services and docs (G+)

Home > CONTOSO | Users > Users

CONTOSO - Microsoft Entra ID

All users Audit logs Sign-in logs Diagnose and solve problems Manage Deleted users Password reset User settings Bulk operation results Troubleshooting + Support New support request

New user Download users Bulk operations Refresh Manage view Delete Per-user MFA Got feedback?

Delete the selected users?

OK Cancel

Jodie Richards Jodie.Richards@efrtp01.onmicrosoft.com Member Yes efrtp01.onmicrosoft.com

Jennifer Davey Jennifer.Davey@efrtp01.onmicrosoft.com Member Yes efrtp01.onmicrosoft.com

John Doe jdoe@efrtp01.onmicrosoft.com Member No efrtp01.onmicrosoft.com

(ADM) John Doe admaz:jdoe@efrtp01.onmicrosoft.com Member No efrtp01.onmicrosoft.com

Module 1 – Lab 1 – The foundations of hybrid identity

The screenshot shows the Microsoft Azure portal interface. On the left, the 'Deleted users' section of the 'Users' blade is visible, displaying a single user named '(AD) John Doe' who was deleted on Jan 24, 2024, at 11:40 AM. On the right, a 'LabClient' window titled '(ING) LAB1 - The foundations of hybrid identity' is open. It contains instructions for creating a dynamic group named 'SG_d_Privileged_Accounts' and deleting the 'Jdoe Admin' account. The 'Questions' and 'Summary' sections provide additional context and links to documentation.

The screenshot shows the Microsoft Azure portal interface. The 'Deleted users' section now shows '(AD) John Doe' with a status of 'Restored'. A 'Restore user(s)' dialog box is open, with 'OK' selected. On the right, the 'LabClient' window titled '(ING) LAB1 - The foundations of hybrid identity' is still open, showing the completed task of restoring the user. The 'Questions' and 'Summary' sections provide feedback and links to documentation.

Module 1 – Lab 1 – The foundations of hybrid identity

The screenshot shows a dual-pane interface. The left pane is the Microsoft Azure portal's 'Users' blade for the 'CONTOSO' tenant, displaying a list of users including Jodie Richards, Jennifer Davey, John Doe, and (ADM) John Doe. The right pane is a 'LabClient' window titled '(ING) LAB1 - The foundations of hybrid identity' with a '12 Minutes Remaining' timer. It contains a 'Questions' section with numbered tasks:

- 9. Create a Dynamic Group Named **SG_d_Privileged_Accounts**
 - Create a new group with the **Membership type** selected to **Dynamic User**
 - Set this rule : (**userPrincipalName** - **startsWith "admaz"**)
- 10. Delete Jdoe Admin account
 - Go to User blade, select Jdoe Admin account and delete it
- 11. Using the documentation located at <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/>, restore it.

The 'Summary' section notes: 'In this exercise, you discovered & manipulated Azure AD users & groups.' A progress bar shows '81% Tasks Complete'. Navigation buttons include '< Previous' and 'Next: Exercise 4: Enable Self.. >'.

Questions:

- Does John Doe have their groups membership restored?
 - o Non
- Does John Doe have their roles membership restored?
 - o Oui
- Can you permanently delete an account?
 - o Oui. Delete Permanently

Exercise 4: Enable Self Service Password Reset

Task 1: Assign EMS E5 licenses to Azure AD users

Questions:

- Does John Doe admin account has a license assigned?
- Does PAR_User3 account has a license assigned?
- Why?

Module 1 – Lab 1 – The foundations of hybrid identity

The screenshot shows a Windows PowerShell ISE window titled "Administrator: Windows PowerShell ISE". The command entered is:

```
PS C:\Users\Administrator> Connect-AzureAD
```

The right pane displays a task list for "Task 1: Assign EMS E5 licenses to Azure AD users". Step 1 is checked and shows:

- 1. Log on to **SRV01**

Step 2 is uncheckable and shows:

- 2. On the Script pane of the Windows PowerShell ISE window, run the following to sign into the Contoso Azure AD tenant. When prompted, sign in with the **(ADM) John Doe** user account, which you created in the previous exercise.
In a PowerShell Cmdlet begin by:
`Connect-AzureAD`

Step 3 is uncheckable and shows:

- 3. On the Script pane of the Windows PowerShell ISE window, running the following to set the **Location** attribute to **France** for all Azure AD user accounts with the UPN suffix matching the custom verified domain name of the Contoso Azure AD tenant.
`$domainName = (Get-AzureADDomain | Where-Object IsDefault -eq 'True').Name
Get-AzureADUser | Where-Object {$_._UserPrincipalName -like "*$domainName"} | Set-AzureADUser -UsageLocation 'fr'`

Step 4 is uncheckable and shows:

- 4. On the Script pane of the Windows PowerShell ISE window, run the following to assign the EM+S E5 trial license to all Azure AD user accounts with the UPN suffix beginning by **PAR**.
`$license = New-Object -TypeName Microsoft.Open.AzureAD.Model.AssignedLicense
$license.SkuId = (Get-AzureADSubscribedSku | Where-Object {$_.OfferType -eq 'Enterprise'}).SkuId
Set-AzureADUser -UsageLocation 'fr' -License $license`

The status bar at the bottom right indicates "82% Tasks Complete".

The screenshot shows the Microsoft Azure portal with the URL https://portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade/. The user profile is displayed for **(ADM) John Doe**.

The user details include:

- User principal name: `admaz-jdoe@efrtp01.onmicrosoft.com`
- Object ID: `44795f2b-2301-4997-aafa-deafedc136`
- Created date time: `Jan 24, 2024, 10:58 AM`
- User type: `Member`
- Identities: `efrtp01.onmicrosoft.com`

The right pane displays a task list for "Task 1: Assign EMS E5 licenses to Azure AD users". Step 1 is checked and shows:

- 1. Log on to **SRV01**

Step 2 is uncheckable and shows:

- 2. On the Script pane of the Windows PowerShell ISE window, run the following to sign into the Contoso Azure AD tenant. When prompted, sign in with the **(ADM) John Doe** user account, which you created in the previous exercise.
In a PowerShell Cmdlet begin by:
`Connect-AzureAD`

Step 3 is uncheckable and shows:

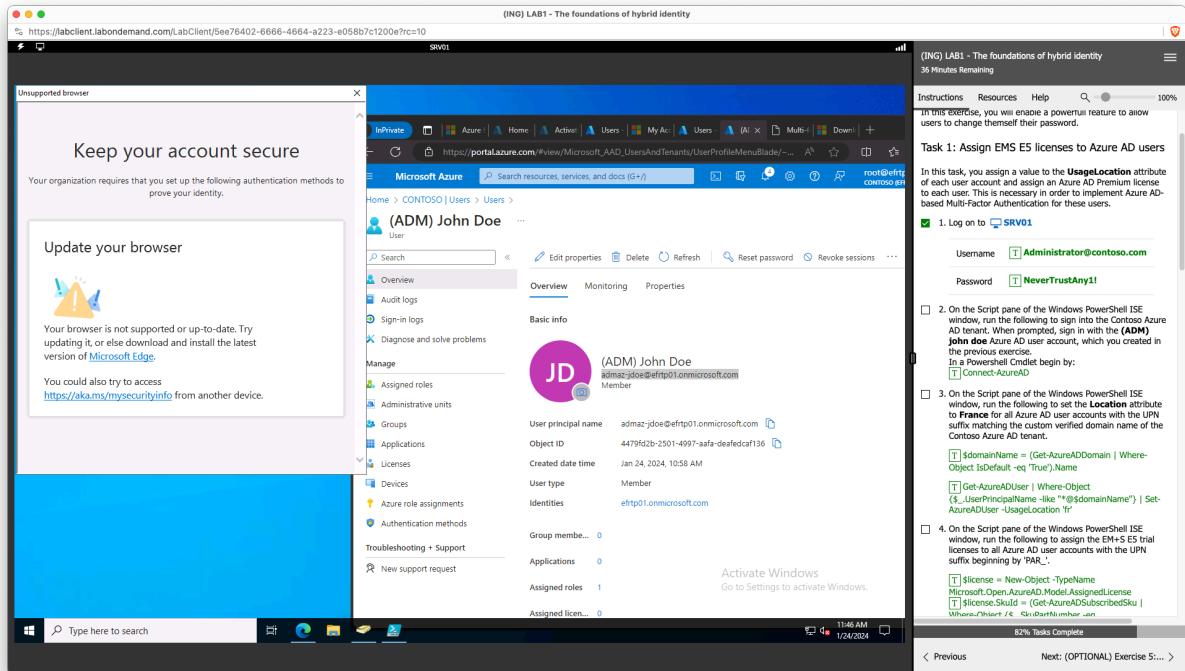
- 3. On the Script pane of the Windows PowerShell ISE window, running the following to set the **Location** attribute to **France** for all Azure AD user accounts with the UPN suffix matching the custom verified domain name of the Contoso Azure AD tenant.
`$domainName = (Get-AzureADDomain | Where-Object IsDefault -eq 'True').Name
Get-AzureADUser | Where-Object {$_._UserPrincipalName -like "*$domainName"} | Set-AzureADUser -UsageLocation 'fr'`

Step 4 is uncheckable and shows:

- 4. On the Script pane of the Windows PowerShell ISE window, run the following to assign the EM+S E5 trial license to all Azure AD user accounts with the UPN suffix beginning by **PAR**.
`$license = New-Object -TypeName Microsoft.Open.AzureAD.Model.AssignedLicense
$license.SkuId = (Get-AzureADSubscribedSku | Where-Object {$_.OfferType -eq 'Enterprise'}).SkuId
Set-AzureADUser -UsageLocation 'fr' -License $license`

The status bar at the bottom right indicates "82% Tasks Complete".

Module 1 – Lab 1 – The foundations of hybrid identity



On ne peut pas aller au-delà de cette étape. En effet, il semblerait que la version de Microsoft Edge ne soit pas suffisamment récente pour effectuer la vérification. Le LAB ne peut être continué faute d'avoir la possibilité de mettre à jour la webview de MS Edge.

Task 2: Enable password writeback and Self-Service Password Reset

Questions:

- What is the goal of the Password Write Back?
 - Permettre aux utilisateurs de modifier ou de réinitialiser leurs mots de passe dans le cloud (comme avec Azure AD) et de répliquer ces changements dans l'environnement Active Directory local.
- Is it the same functionality of the Password Hash Sync?
 - Non.
Ce n'est pas la même fonctionnalité. Le Password Hash Sync (PHS) permet de synchroniser les hash de mots de passe de l'Active Directory local vers Azure AD, permettant ainsi aux utilisateurs de se connecter avec les mêmes identifiants sur site et dans le cloud.

Module 1 – Lab 1 – The foundations of hybrid identity

- What is the goal of the SSPR?
 - Permet aux utilisateurs de réinitialiser leurs mots de passe de manière autonome sans avoir besoin de contacter le support informatique.
- What is the number of days before users are asked to re-confirm their authentication information by default?
 - 180 jours