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

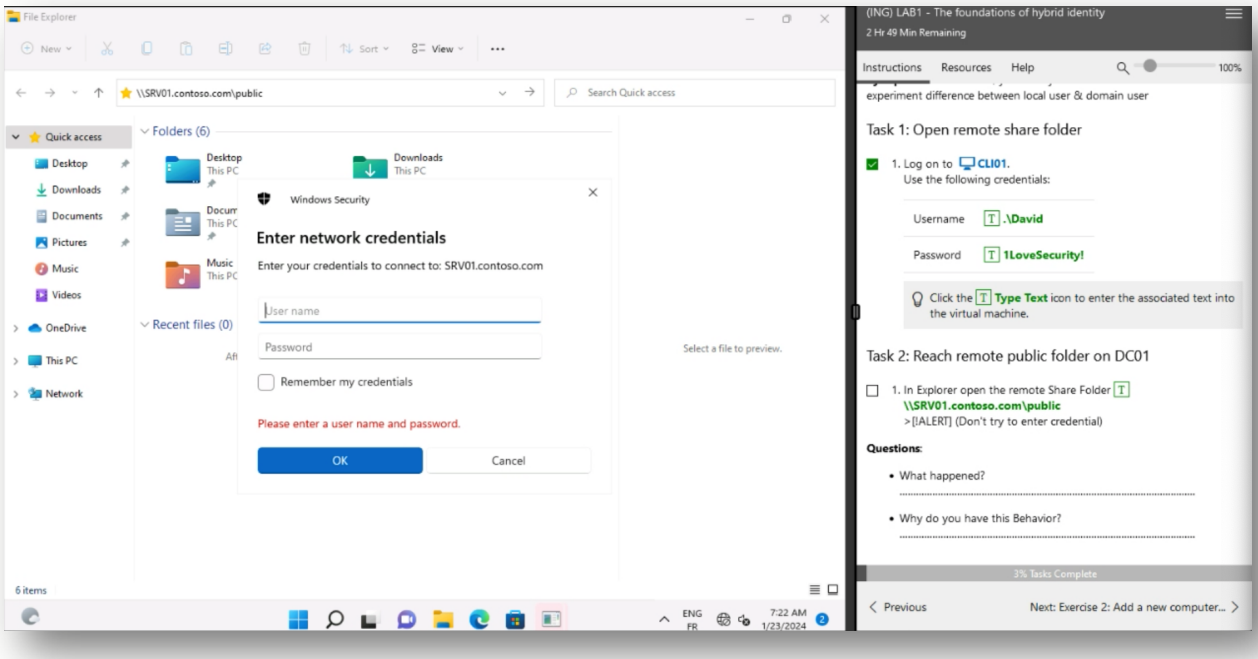
Exercise 1: Manage access without Active Directory

Task 1: Open remote share folder

Task 2: Reach remote public folder on DC01

Questions

- What happened?
    - 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?
    - 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.



Exercise 2: Add a new computer to the domain

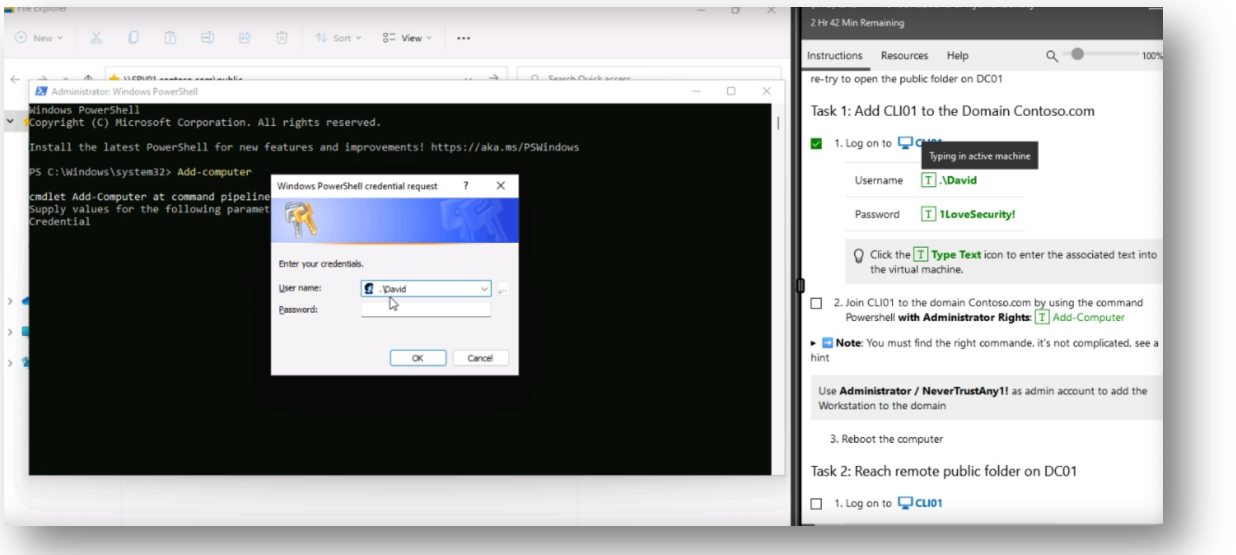
Task 1: Add CLI01 to the Domain Contoso.com

Task 2: Reach remote public folder on DC01

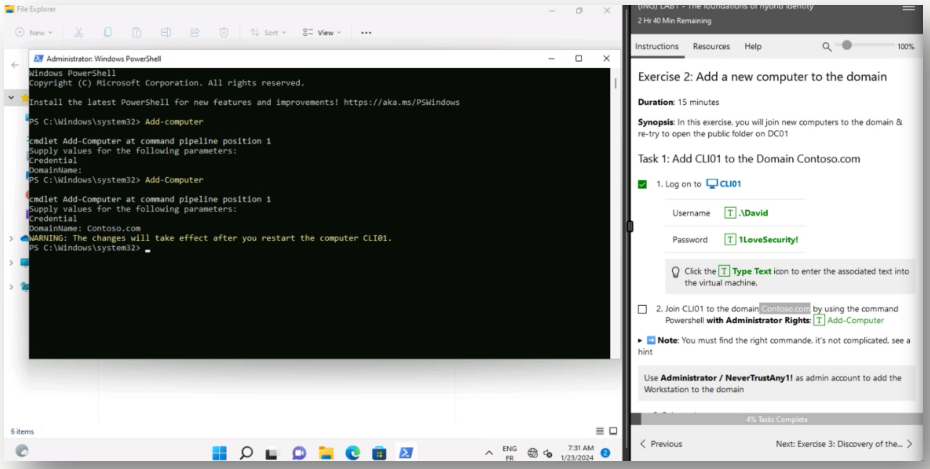
Questions:

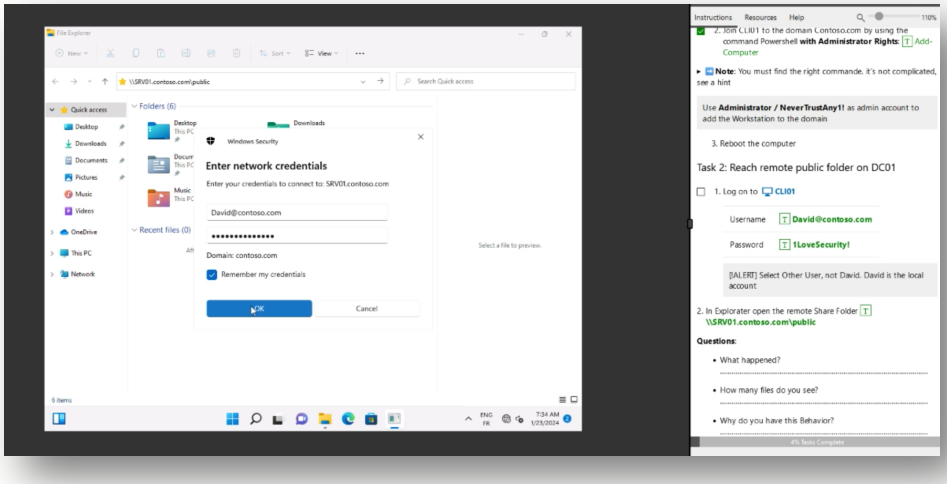
- What happened?
    - En entrant la commande Add-Computer, on obtient une fenêtre qui nous demande de nous authentifier pour avoir des droits administrateurs sur le PowerShell. Par la suite, on nous demande d'ajouter un DomainName Contoso.com.

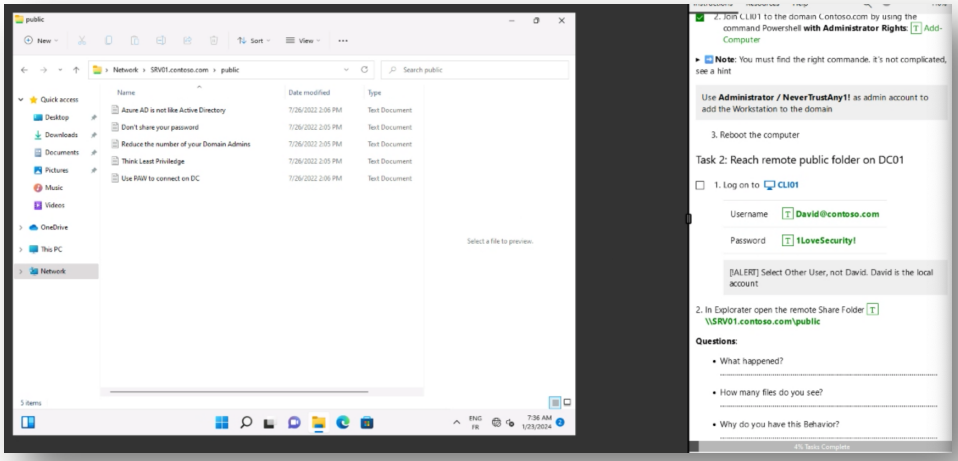
- How many files do you see?
    - Nous voyons actuellement 5 fichiers (comme visible sur la dernière capture d'écran)
- Why do you have this Behavior?
    - Le PC a été ajouté au domaine Contoso.com, lui permettant donc d'accéder à ces fichiers. L'utilisateur David peut maintenant se connecter avec ses identifiants David@Contoso.com .



Module 1 – Lab 1 – The foundations of hybrid identity







Exercise 3: Discovery of the environment

Task 1: Create a new OU

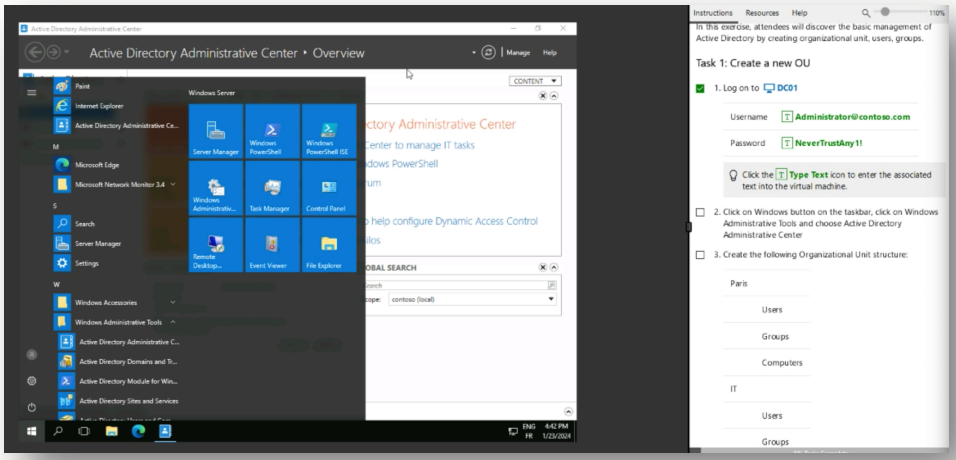
Task 2: Create new users

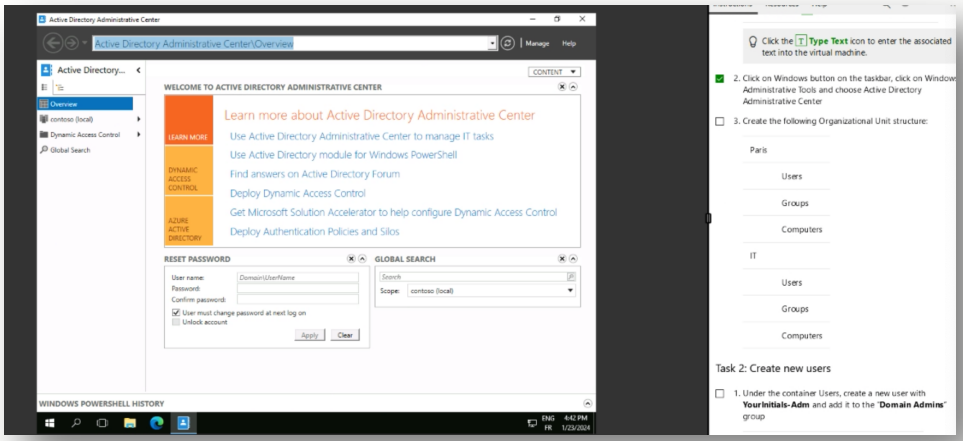
Task 3: Create a new group

Task 4: Enumerate & find objects in ADDS

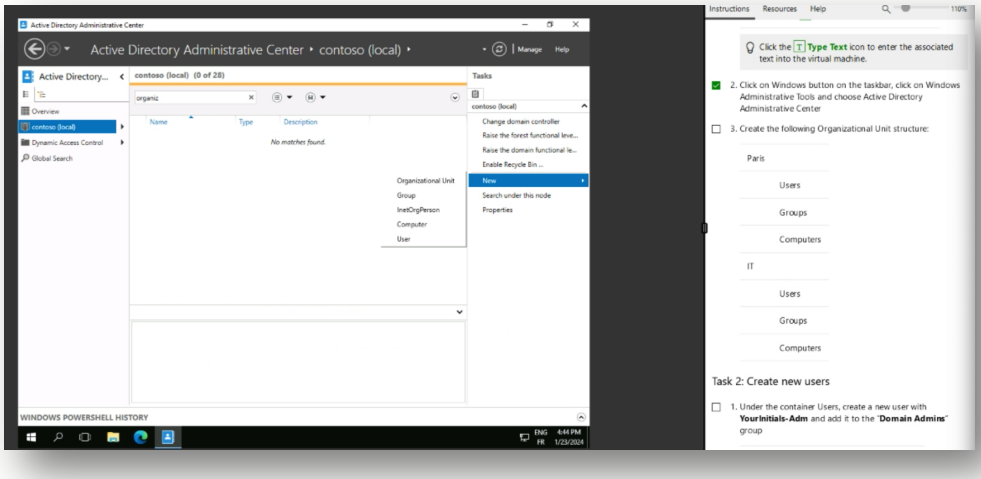
Questions:

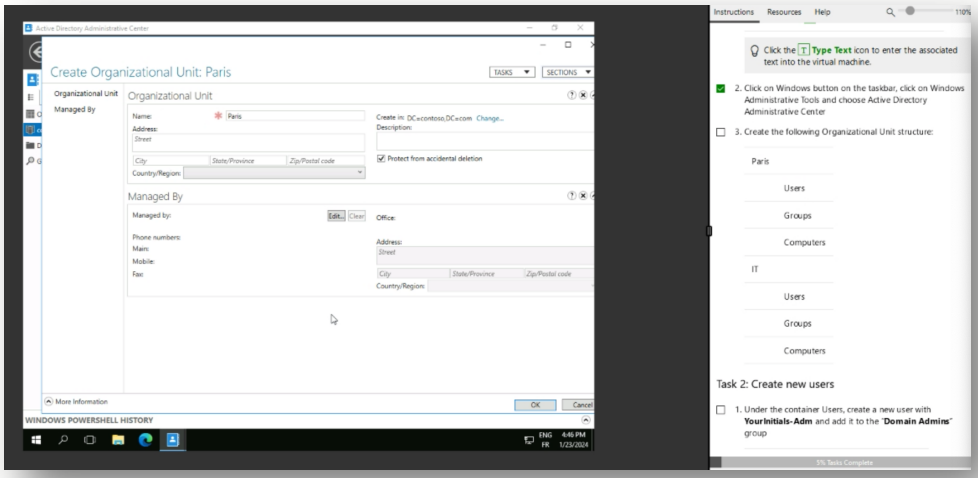
- How many users you have?
    - 81
- How many computer(s) you have?
    - 13

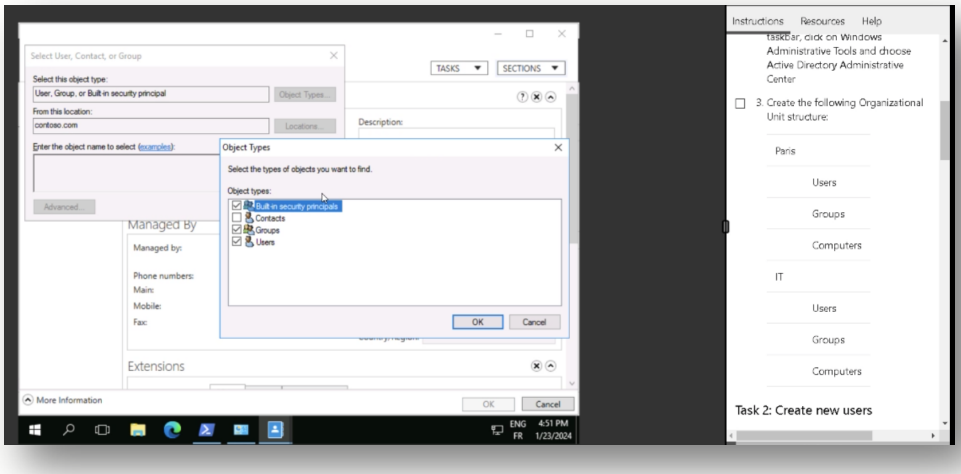




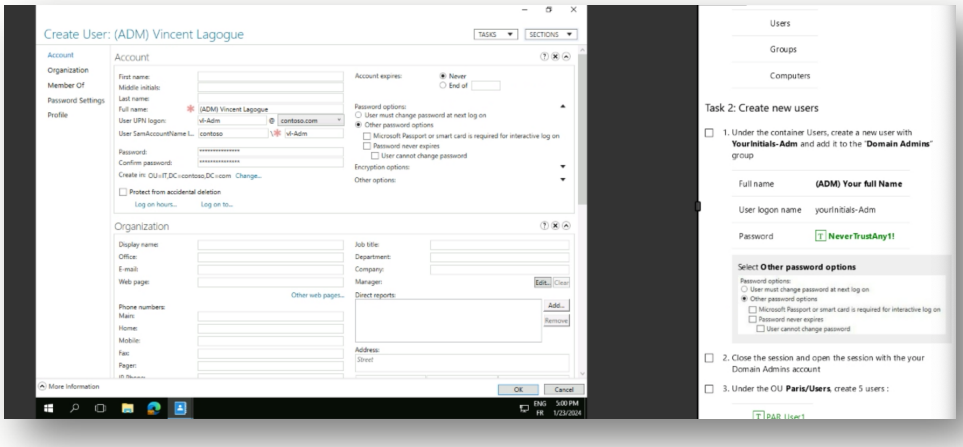
Module 1 – Lab 1 – The foundations of hybrid identity

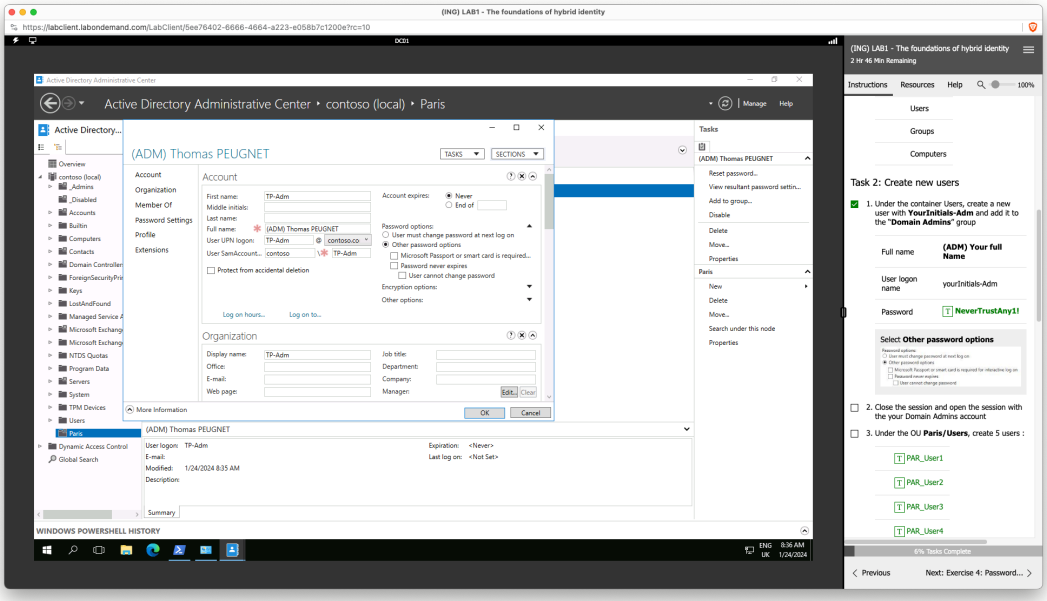




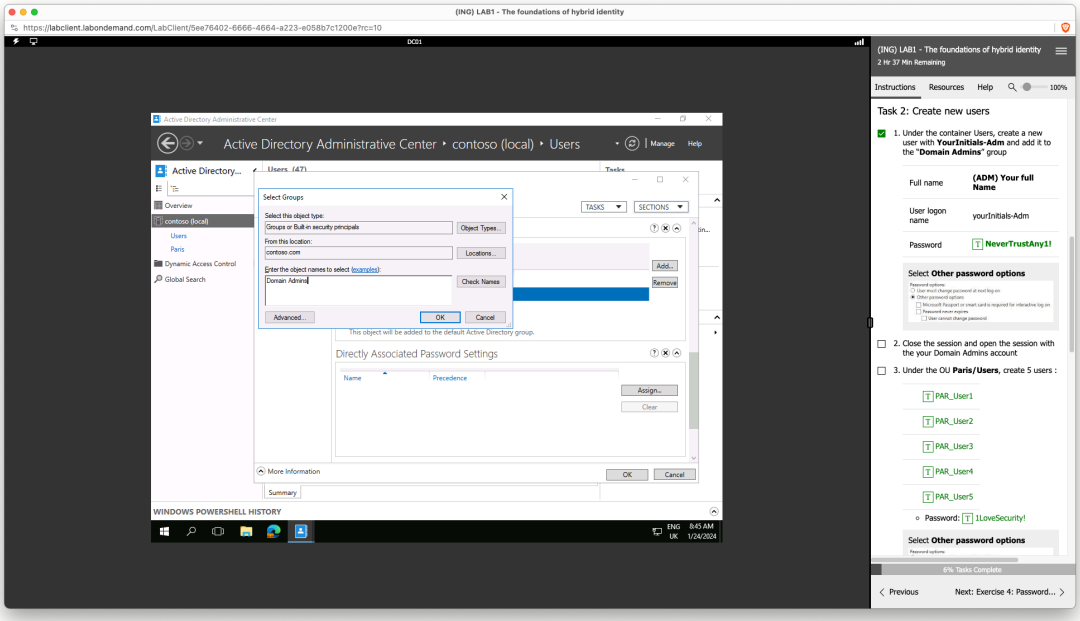


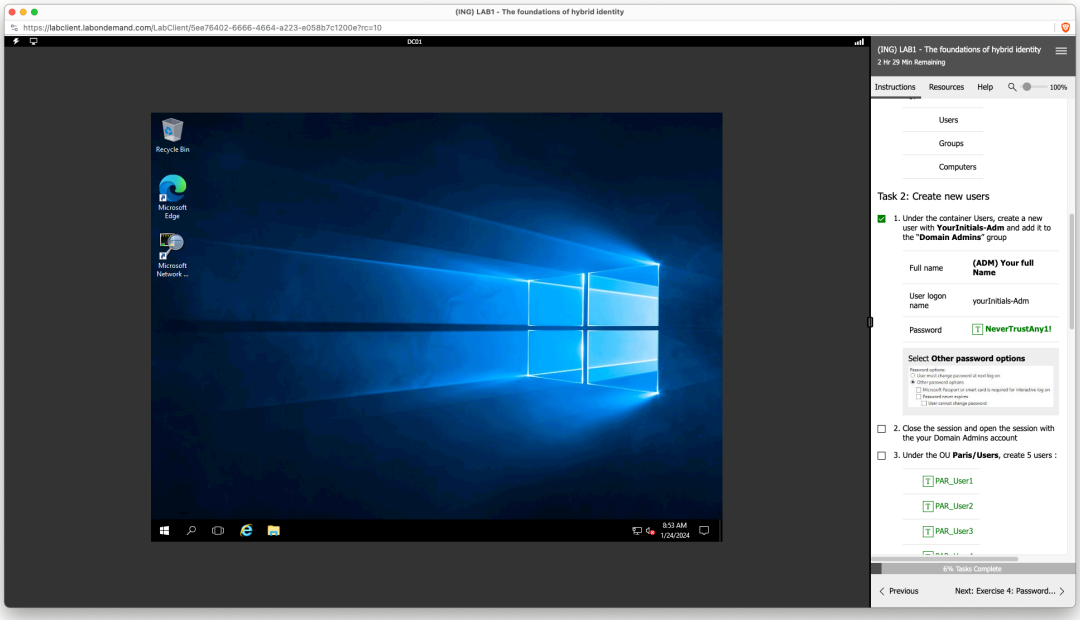
Module 1 – Lab 1 – The foundations of hybrid identity



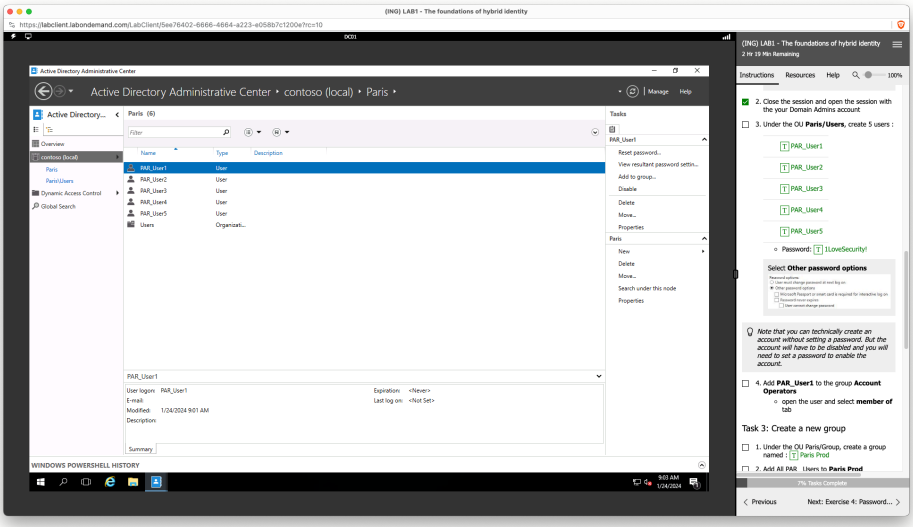


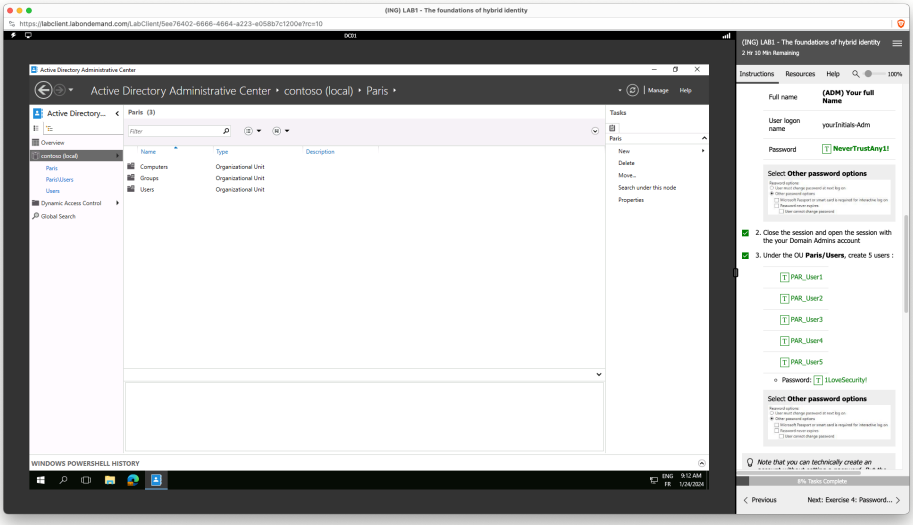
Module 1 – Lab 1 – The foundations of hybrid identity

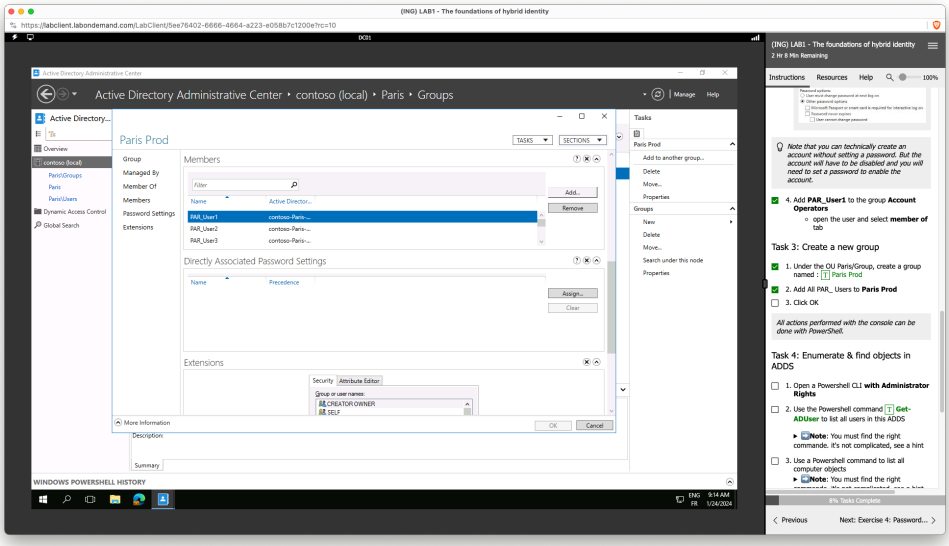




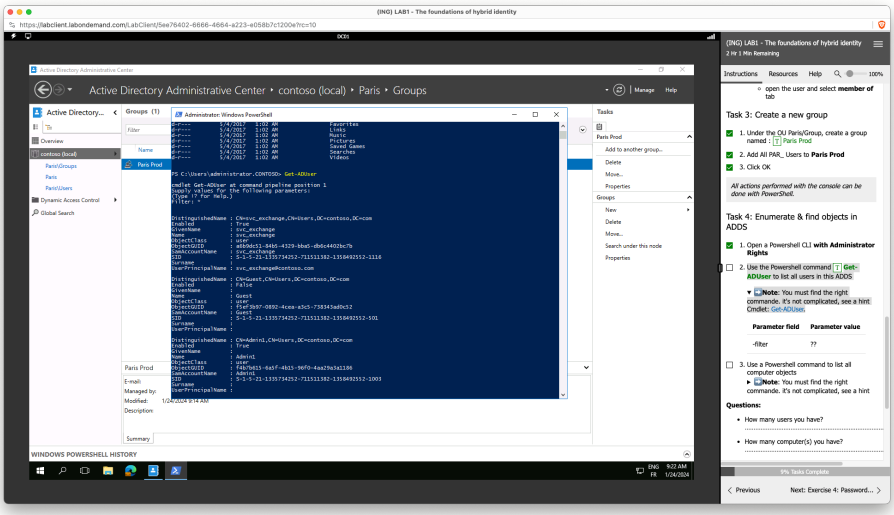
Module 1 – Lab 1 – The foundations of hybrid identity

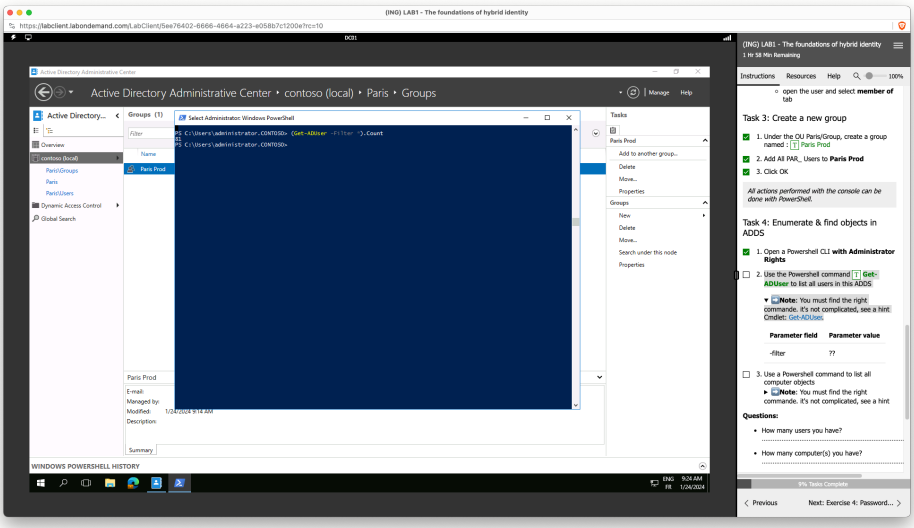


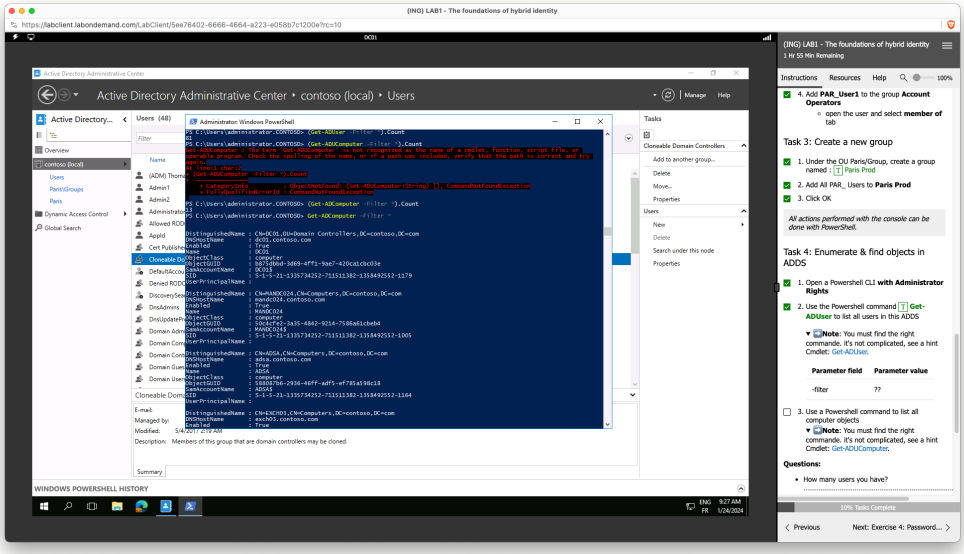


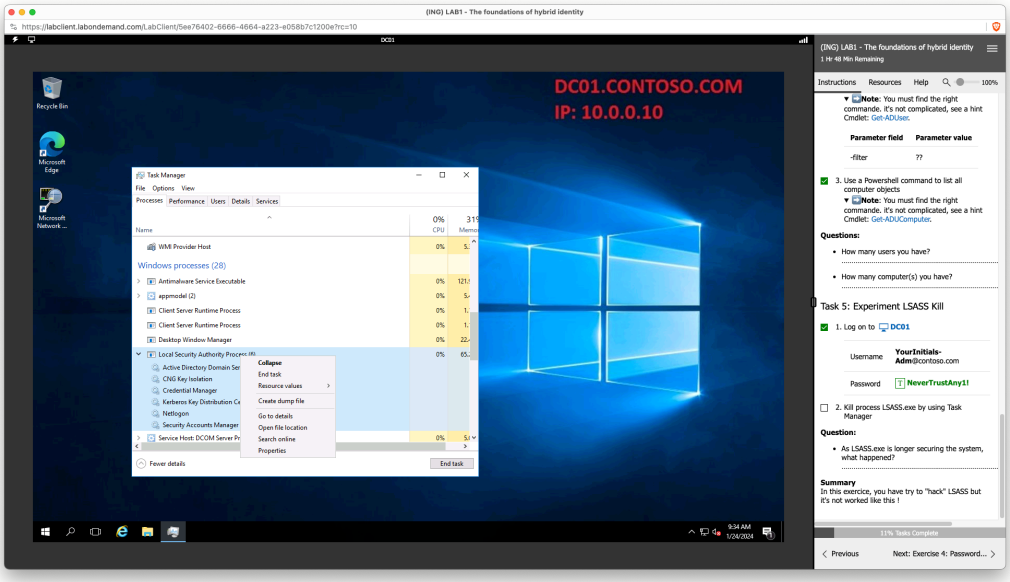


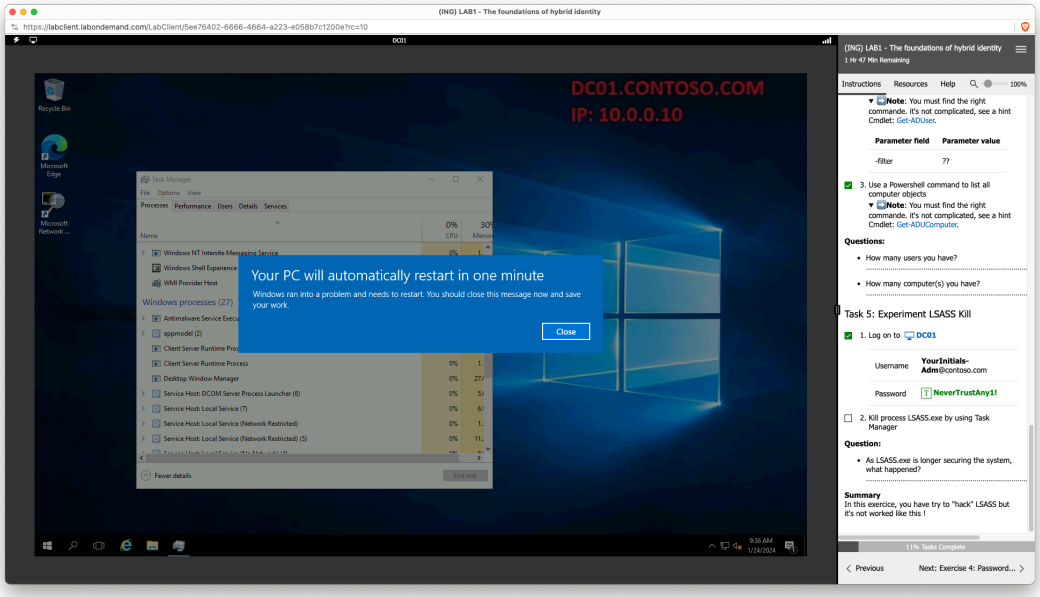
Module 1 – Lab 1 – The foundations of hybrid identity











Task 5: Experiment LSASS Kill

Question:

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

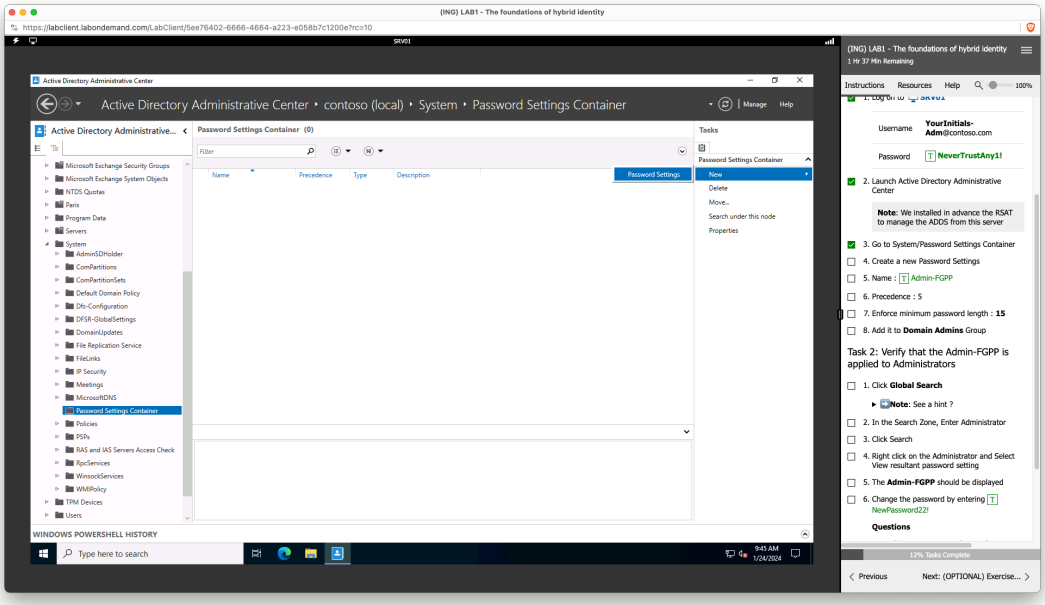
Exercise 4: Password Policy vs FGPP

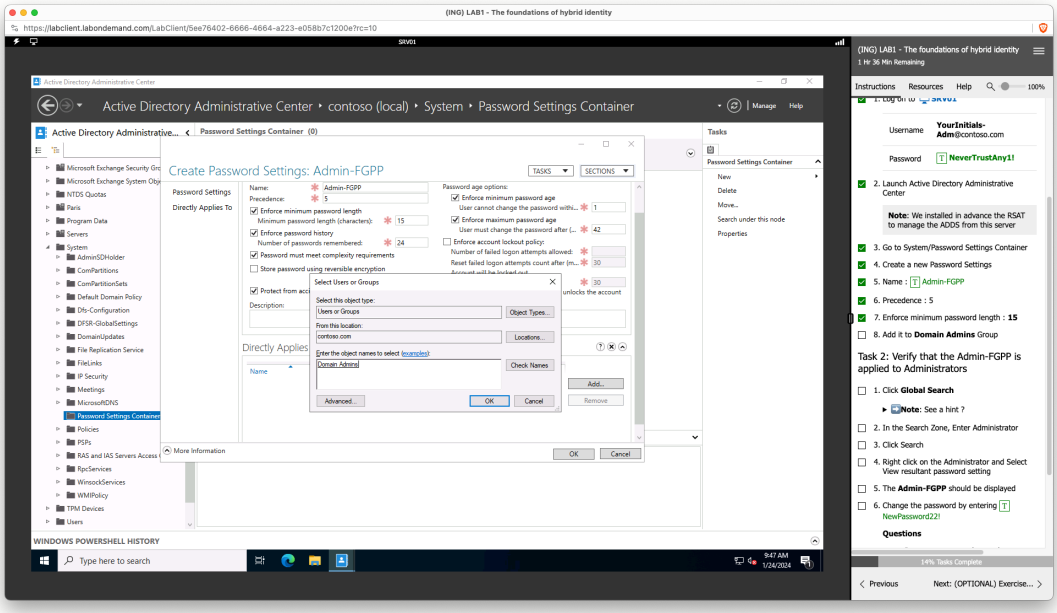
Task 1: Configure FGPP

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

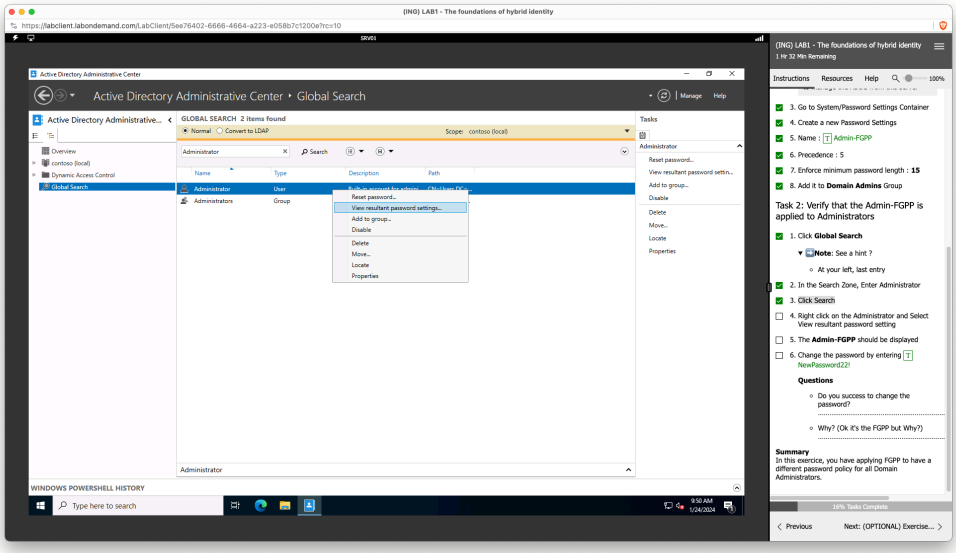
Questions

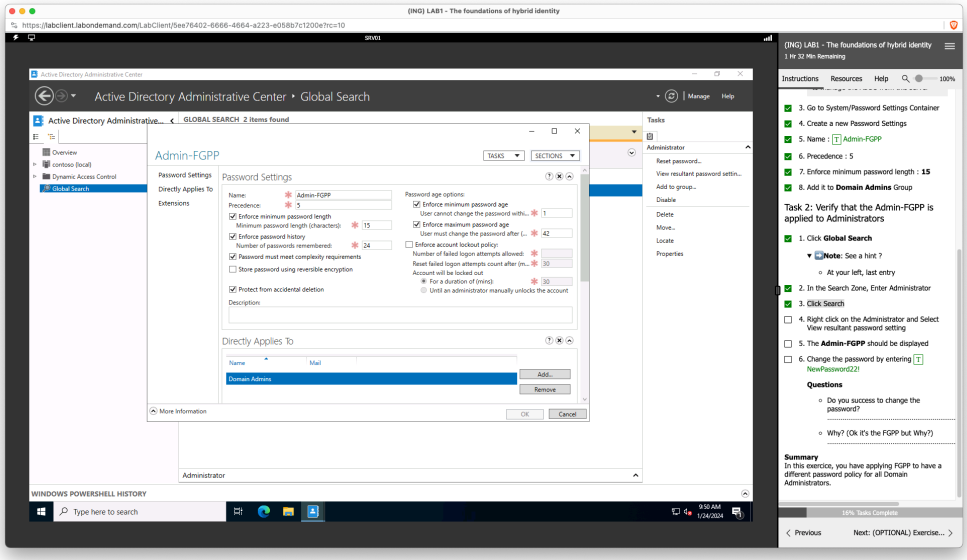
- Do you success to change the password?
    - Non.
- Why? Ok it's the FGPP but Why?
    - Le mot de passe qu'on tente de changer n'est pas raccord avec la password policy qu'on a créé avant.



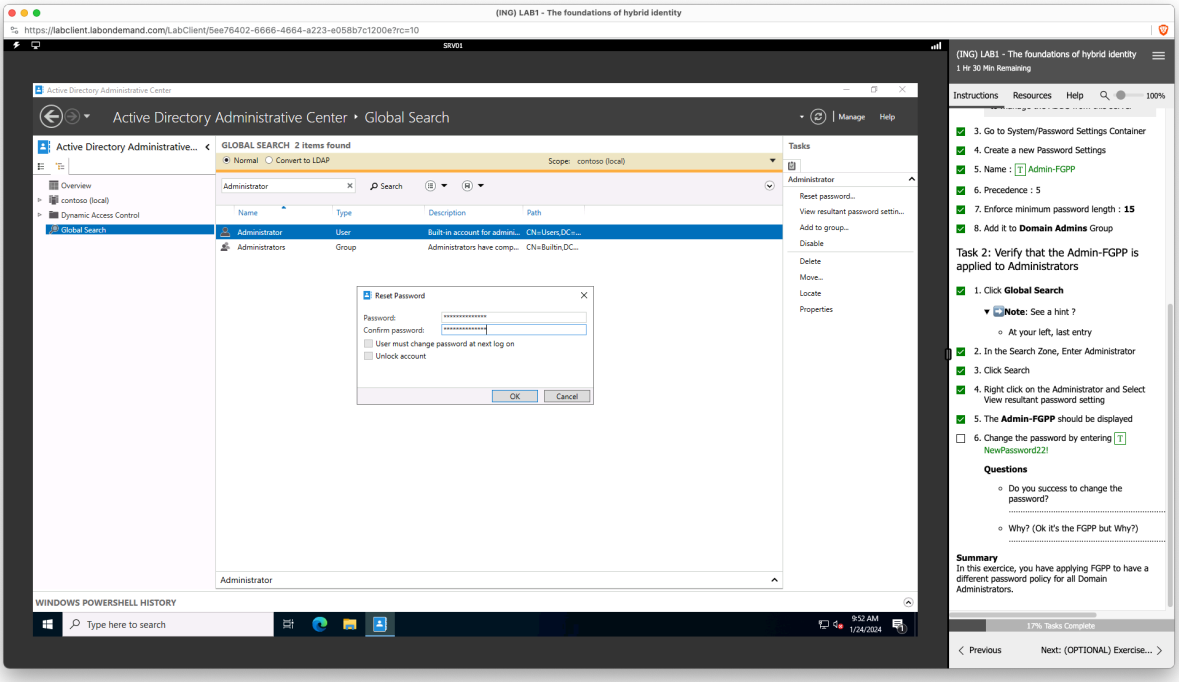


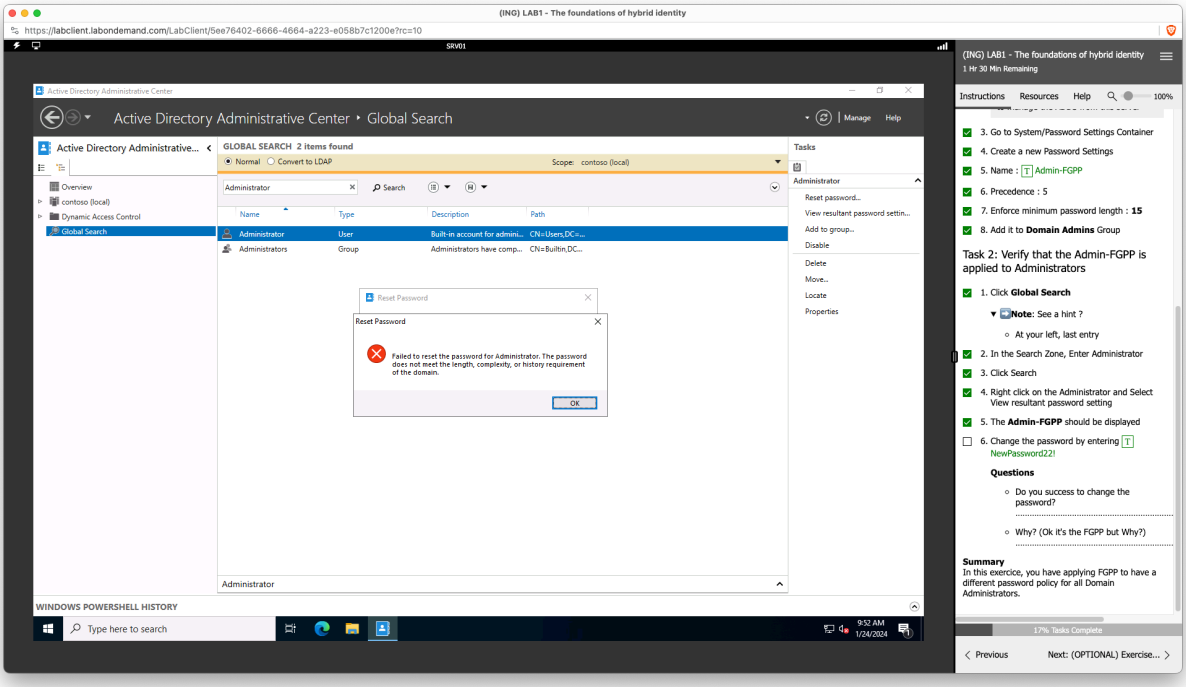
Module 1 – Lab 1 – The foundations of hybrid identity



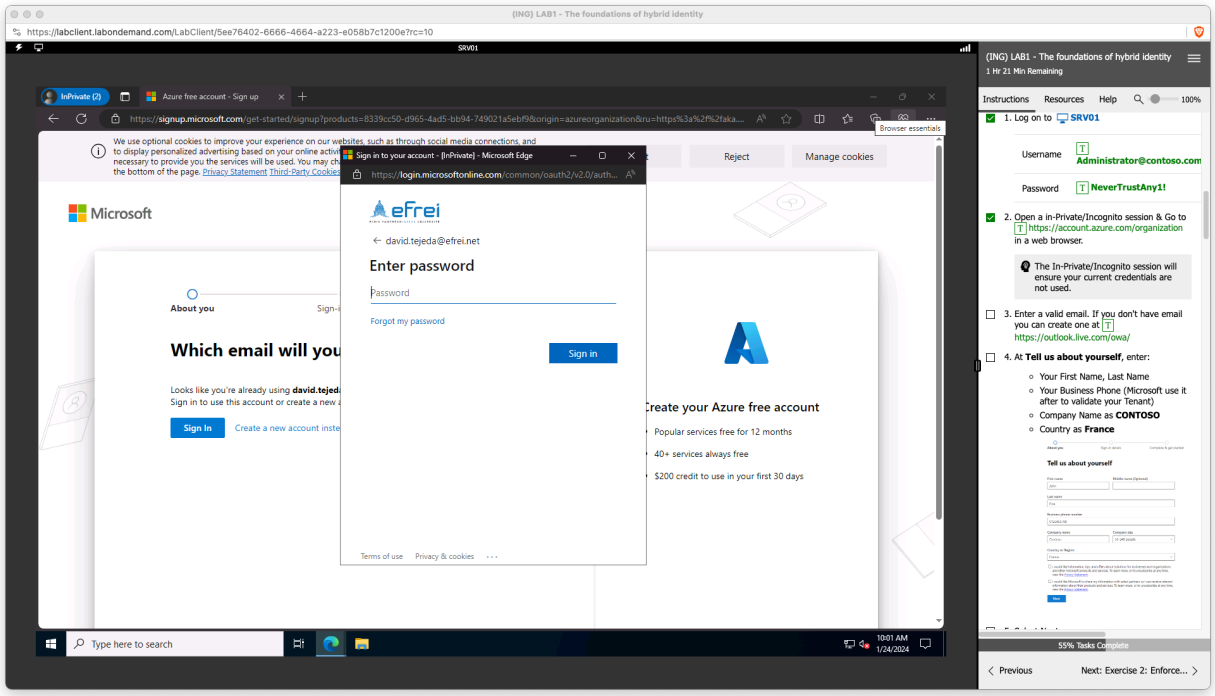


Module 1 – Lab 1 – The foundations of hybrid identity





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?
    - 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.

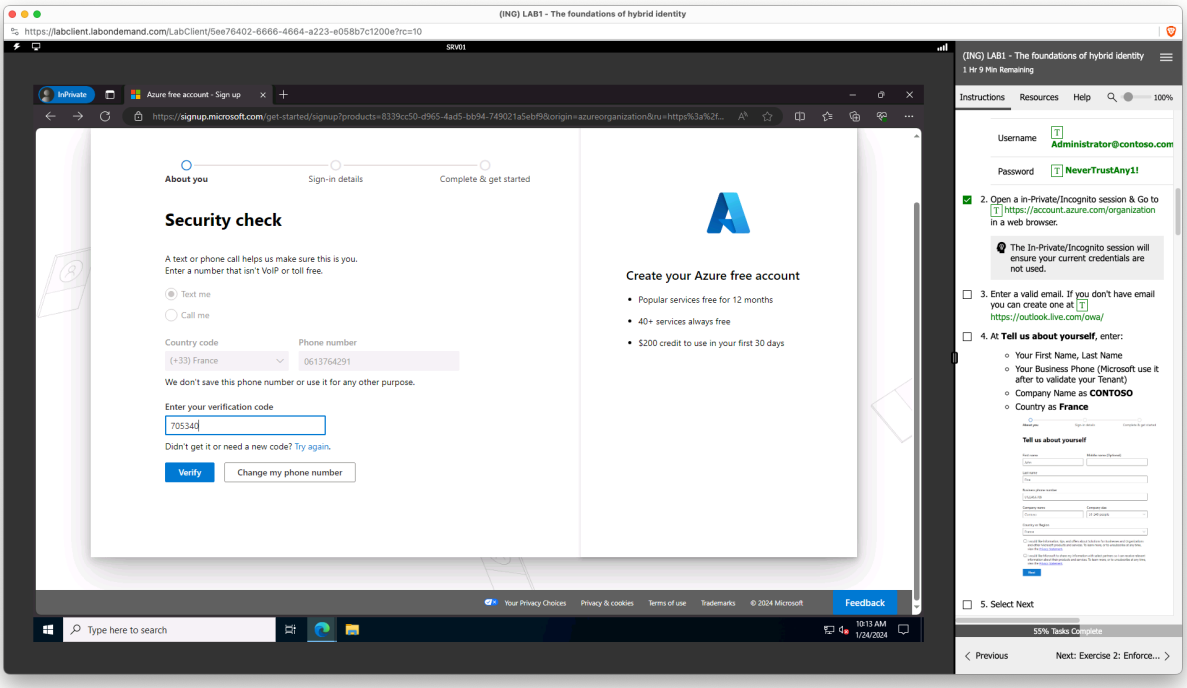
Questions:

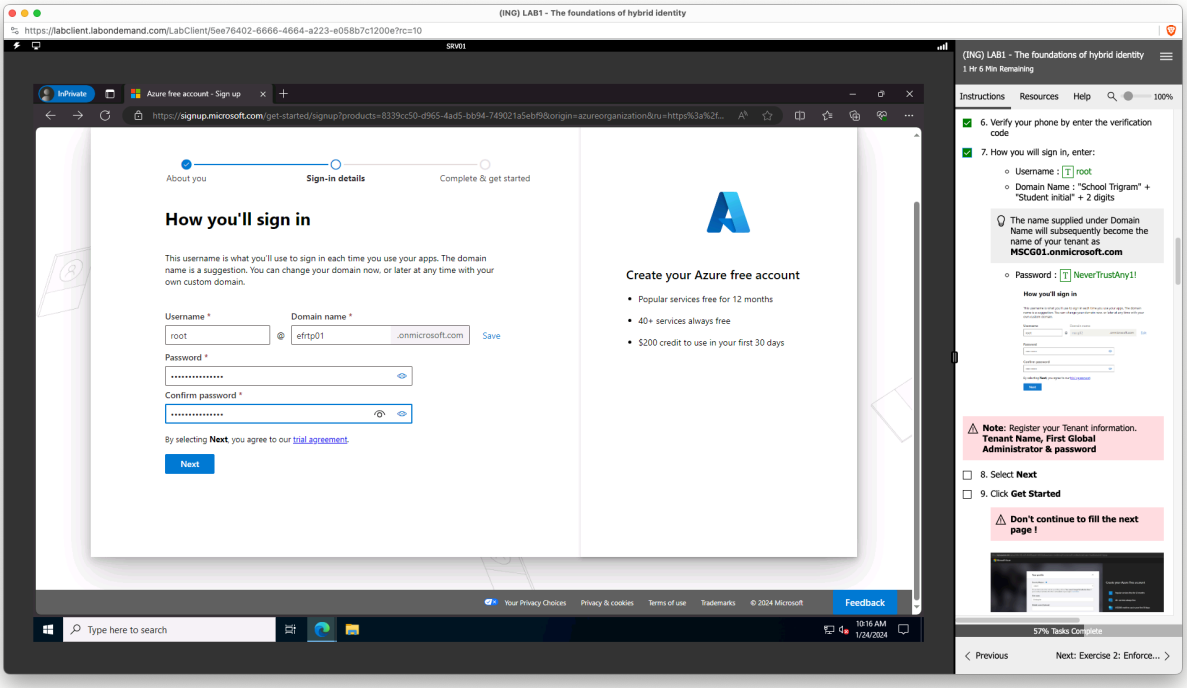
- What is the goal of SSO?
    - Le but du Single Sign-On (SSO) est de permettre aux utilisateurs d'accéder à plusieurs applications et services en utilisant une seule fois leurs identifiants de connexion.
- Why is it Seamless?
    - Il fournit une transition entre différents services et applications 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

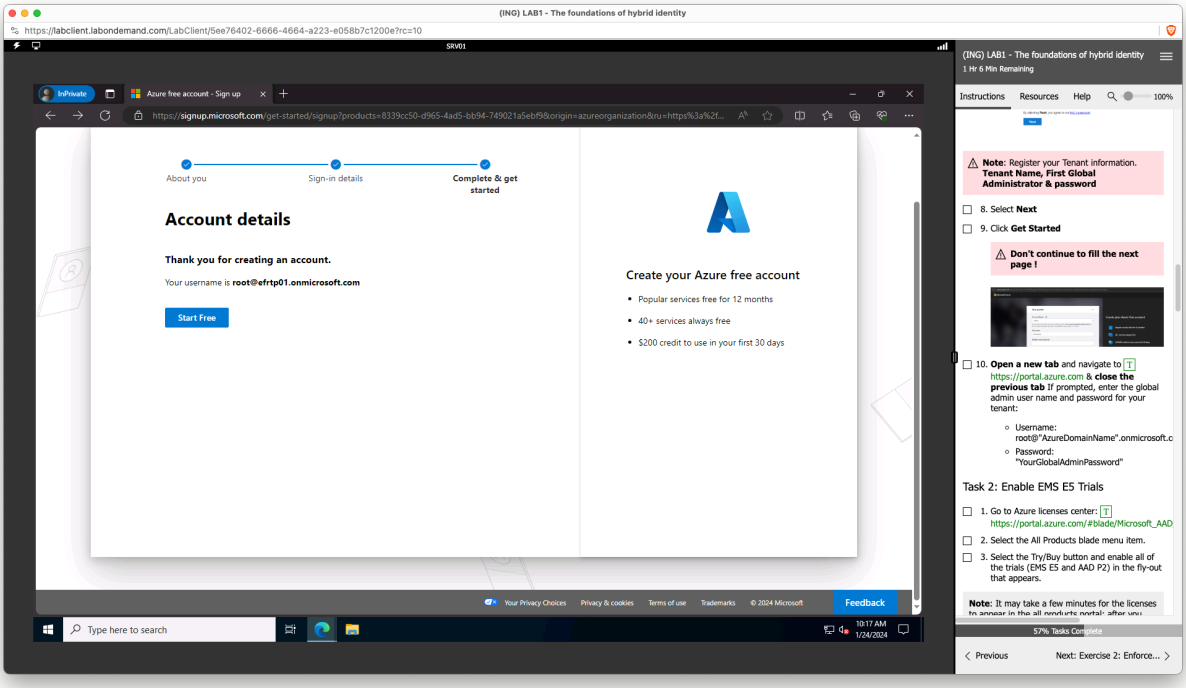
Task 5: Check directory synchronization

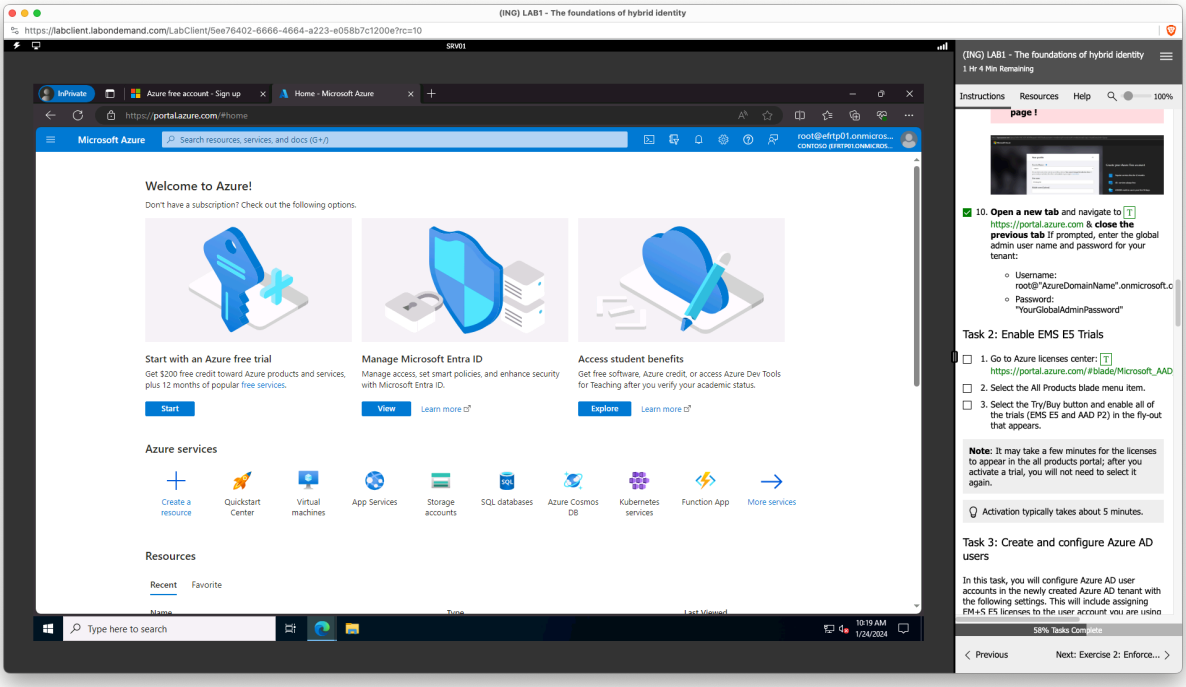
Task 6: Disable security defaults



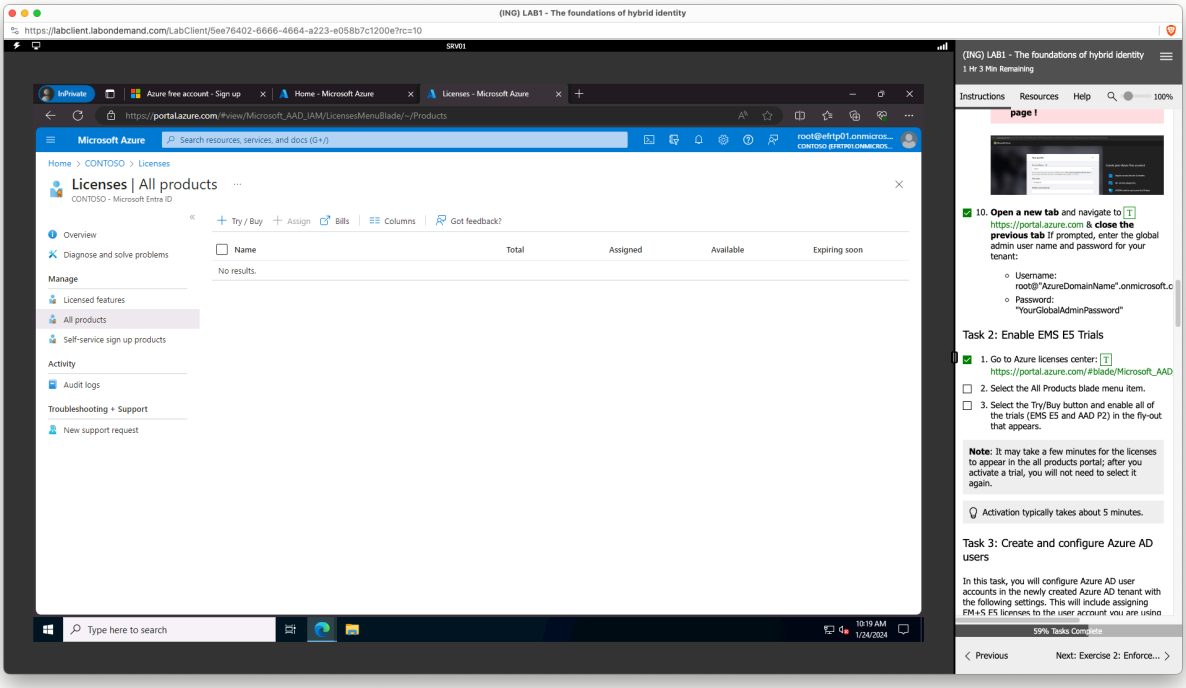


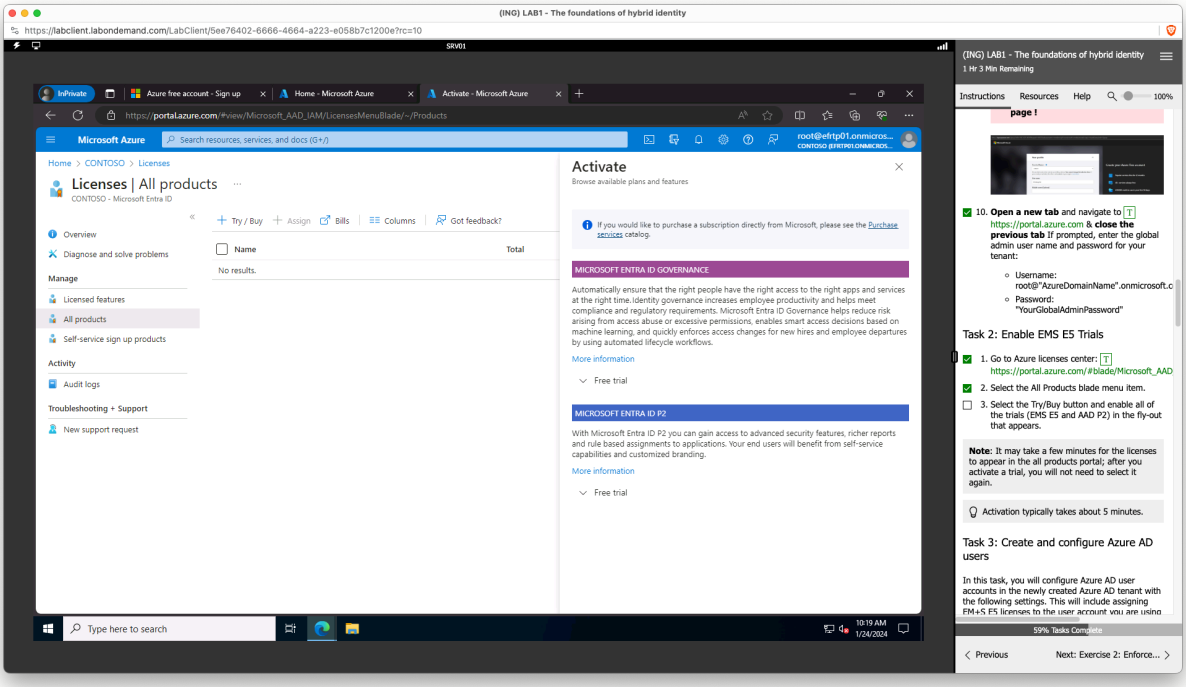
Module 1 – Lab 1 – The foundations of hybrid identity



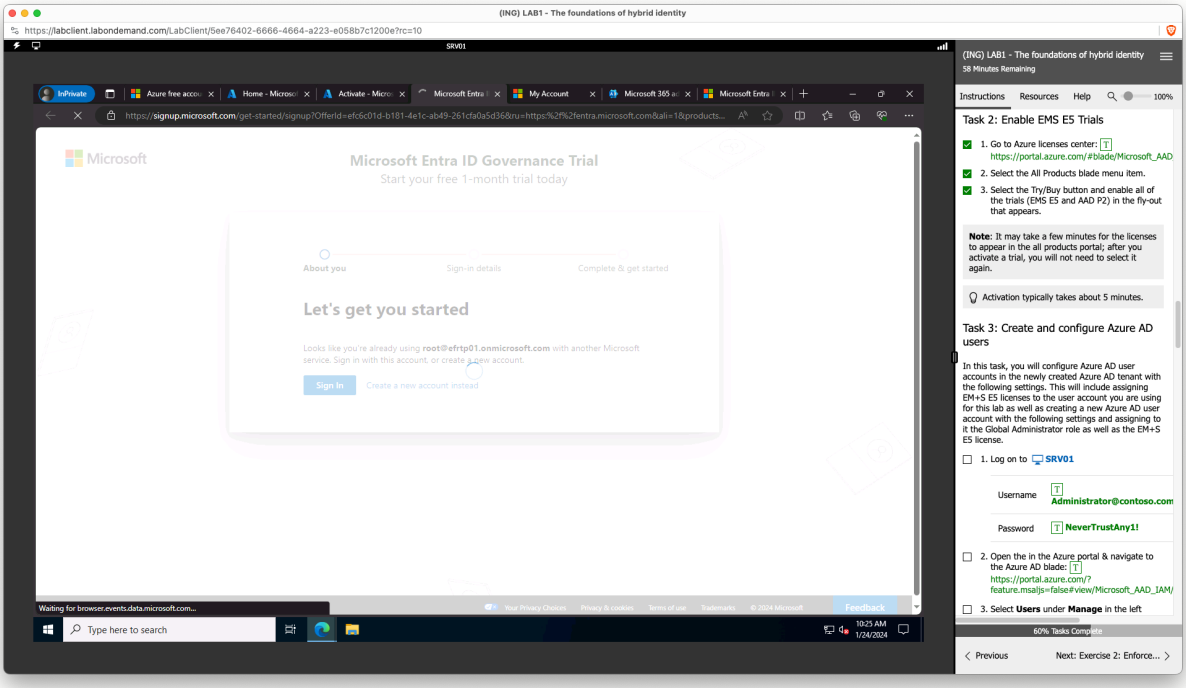


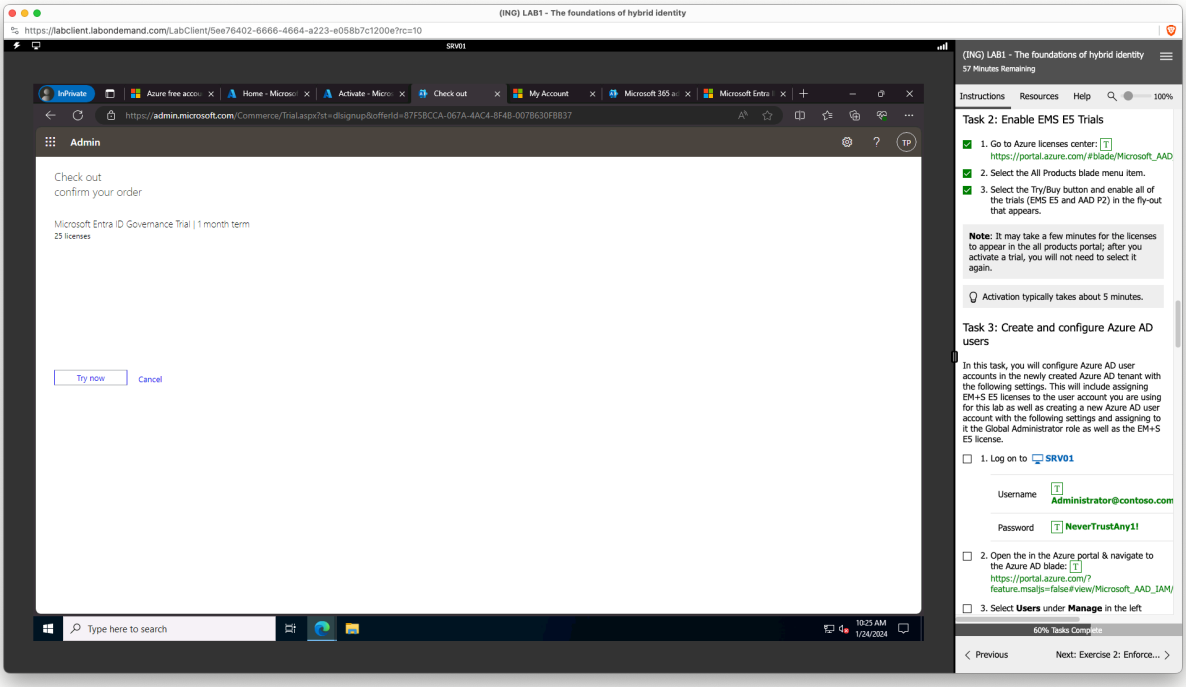
Module 1 – Lab 1 – The foundations of hybrid identity



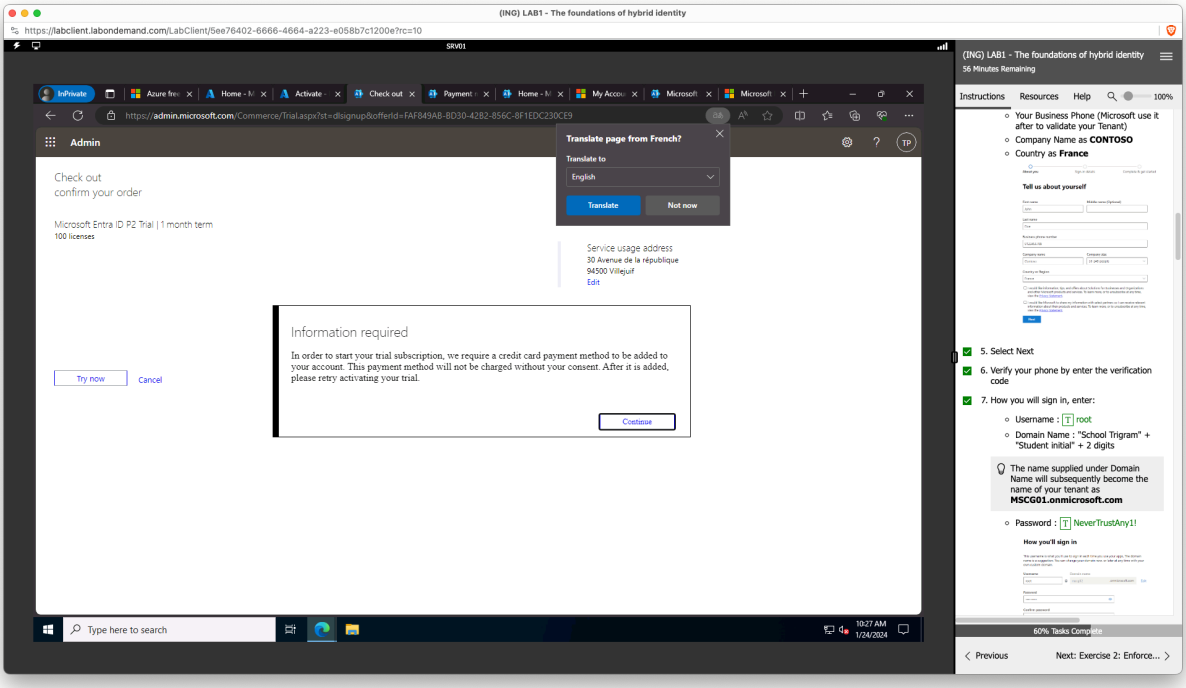


Module 1 – Lab 1 – The foundations of hybrid identity

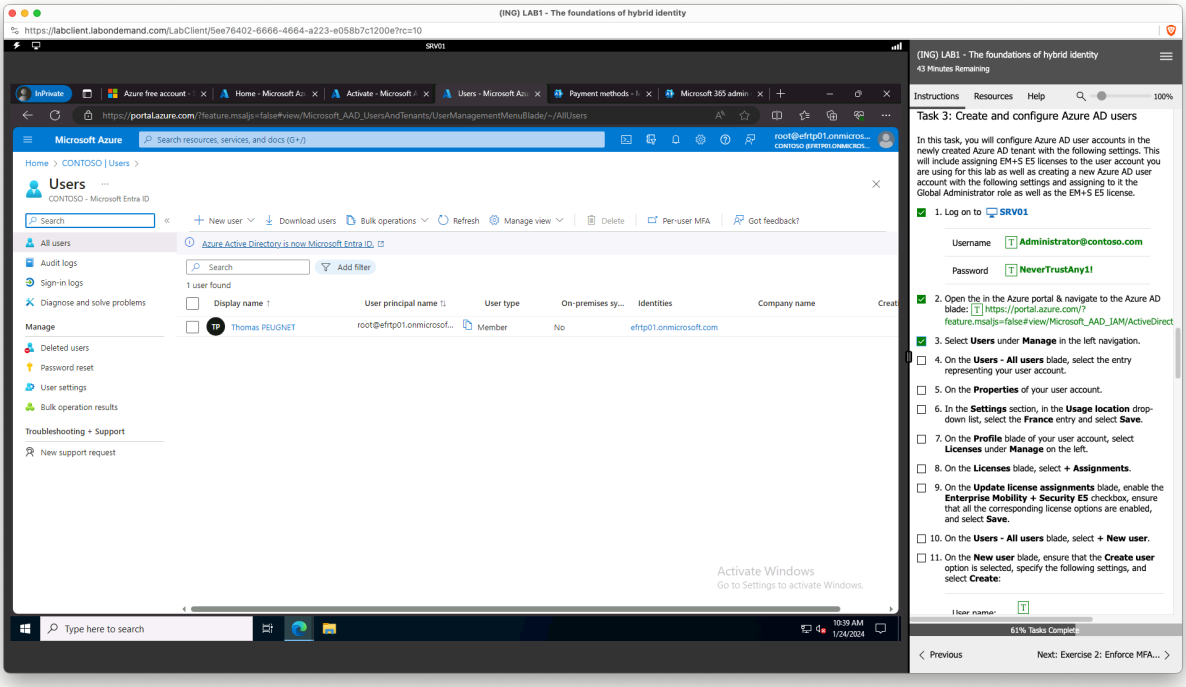




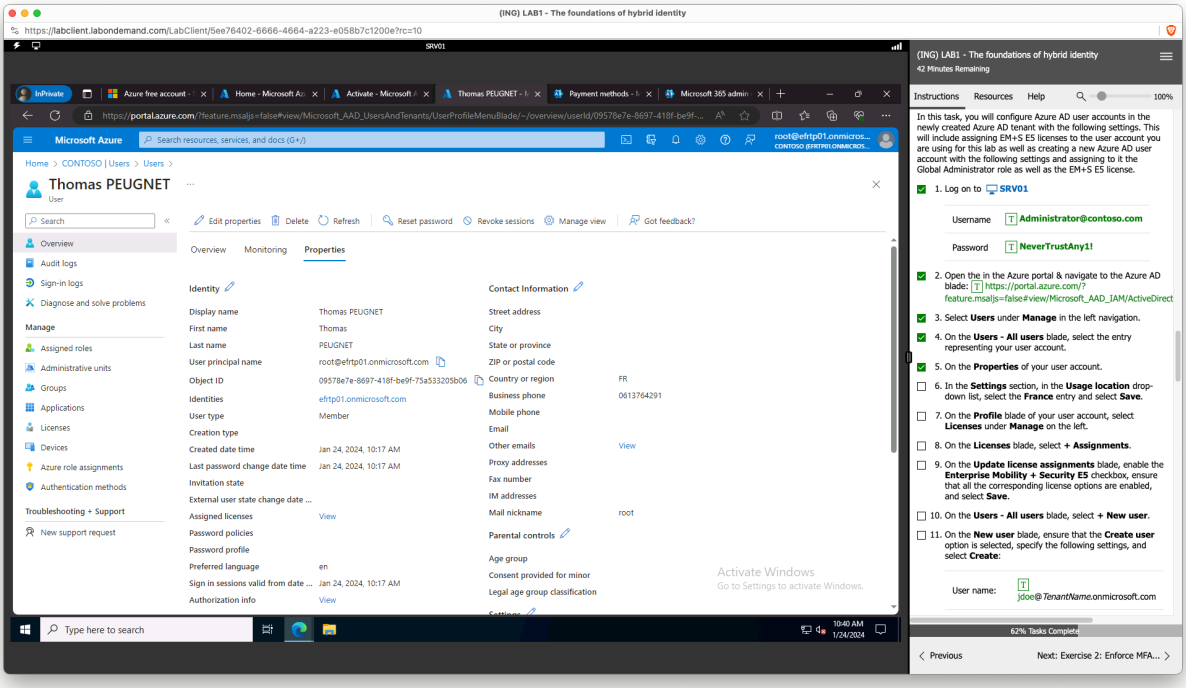
Module 1 – Lab 1 – The foundations of hybrid identity

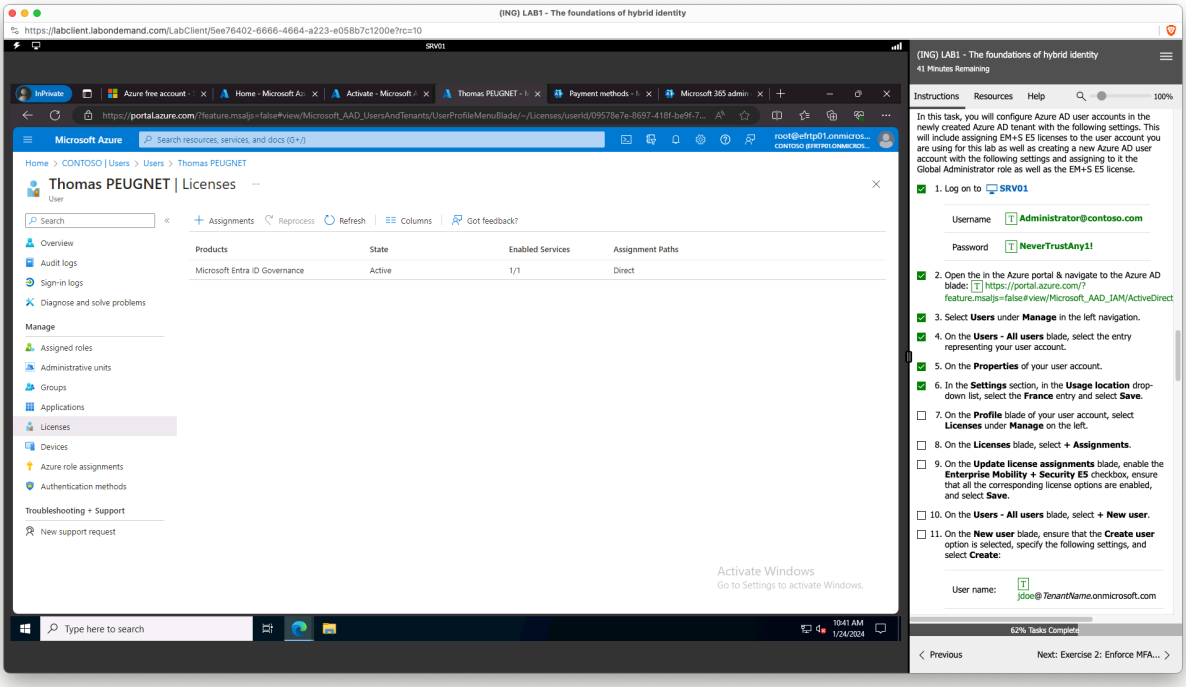


Credit card required – Step Skipped

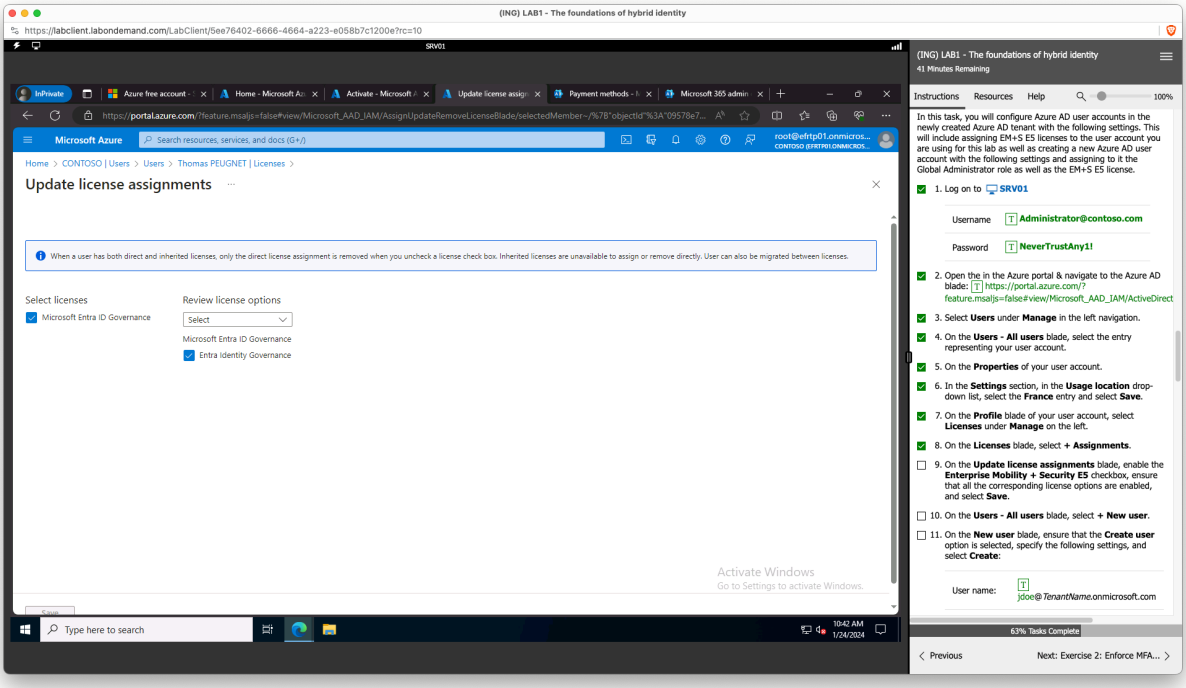


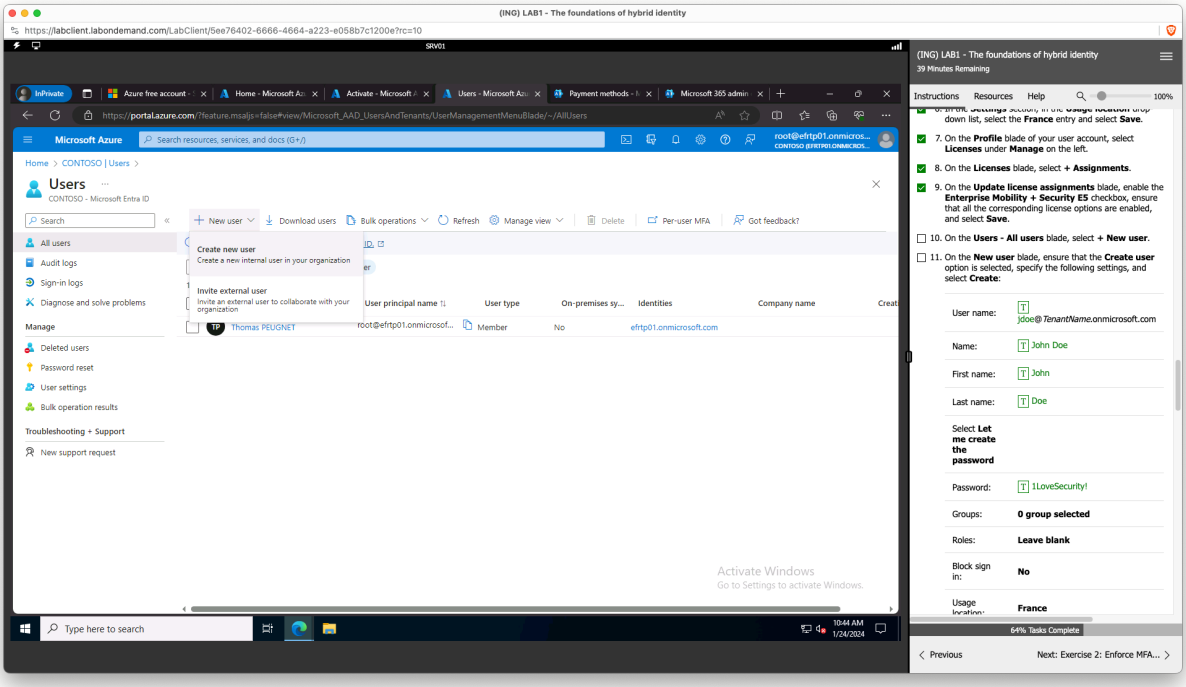
Module 1 – Lab 1 – The foundations of hybrid identity



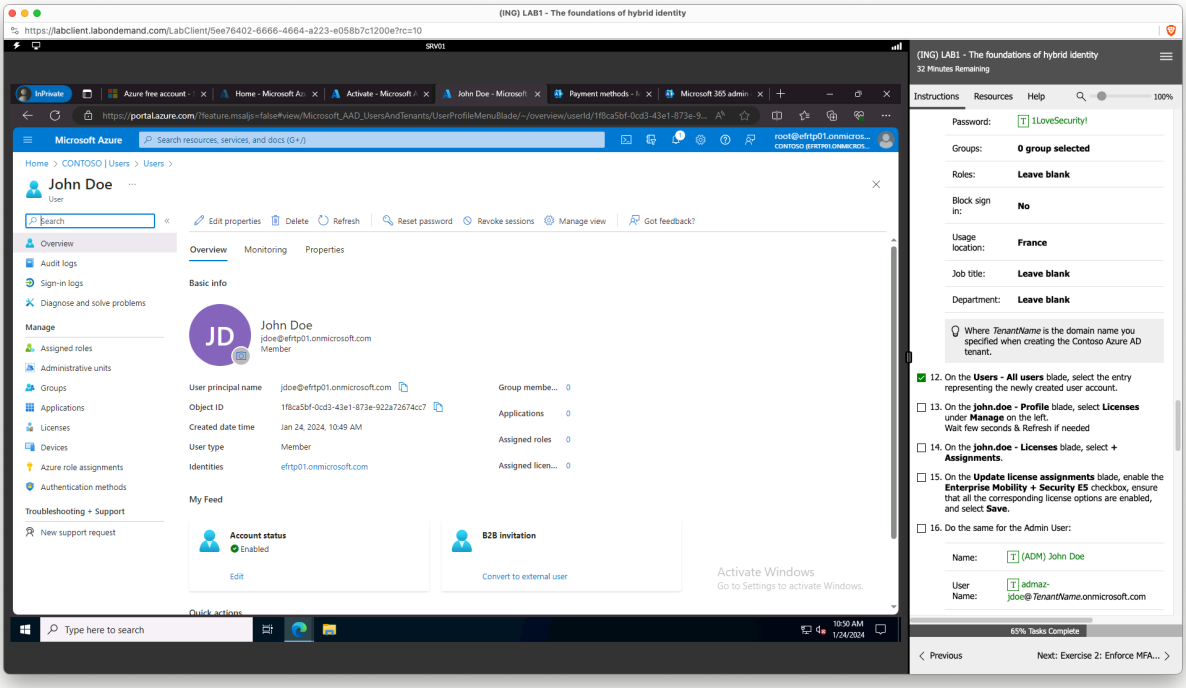


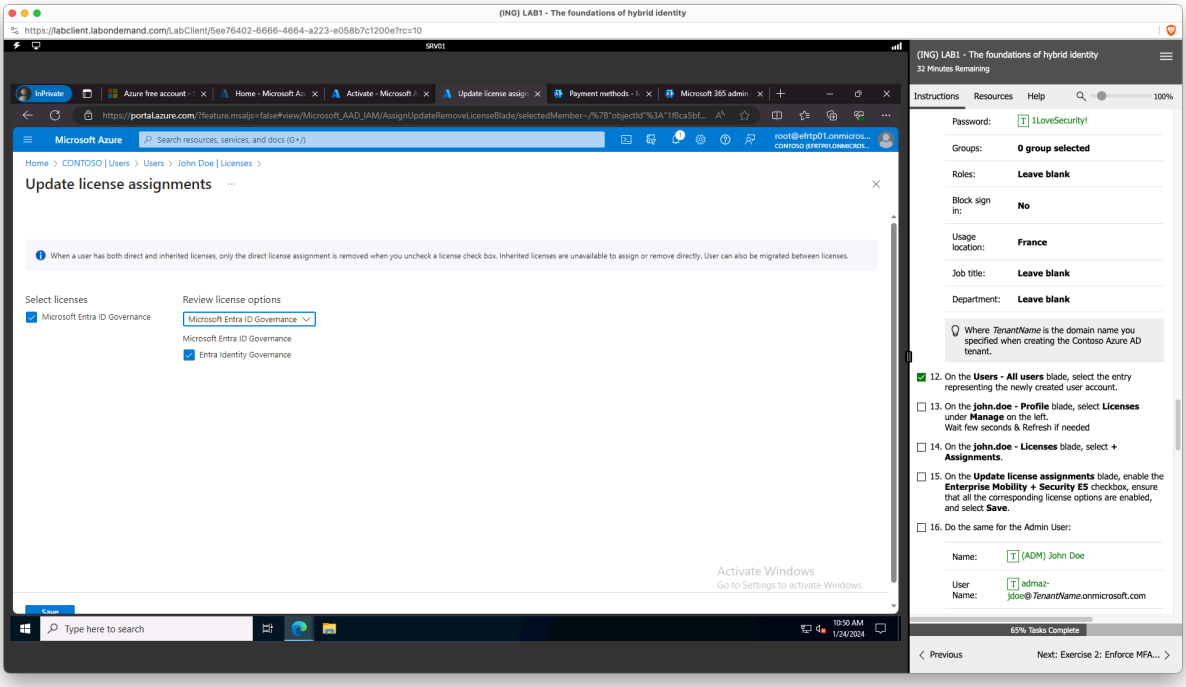
Module 1 – Lab 1 – The foundations of hybrid identity



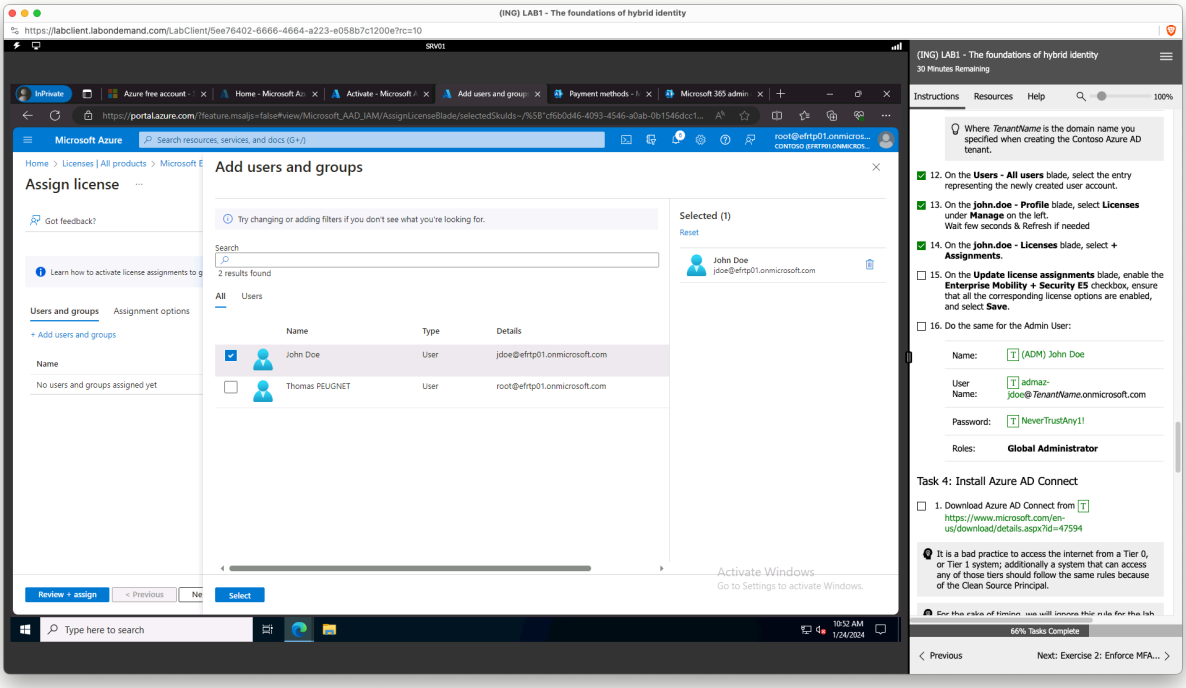


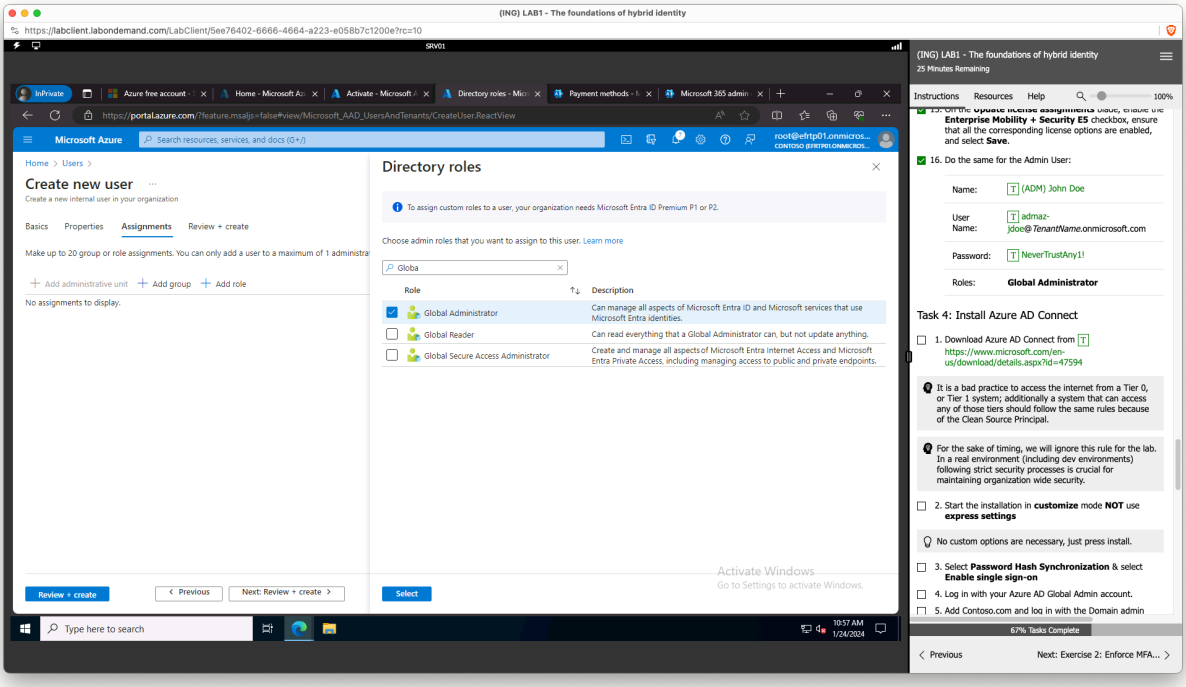
Module 1 – Lab 1 – The foundations of hybrid identity



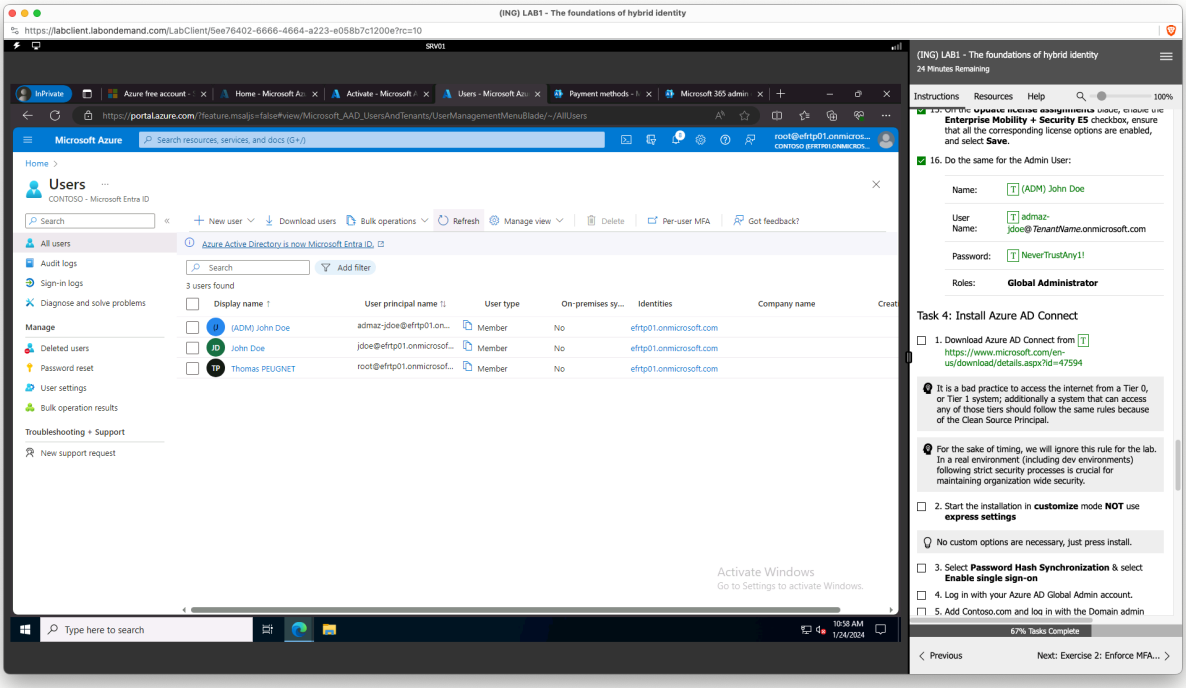


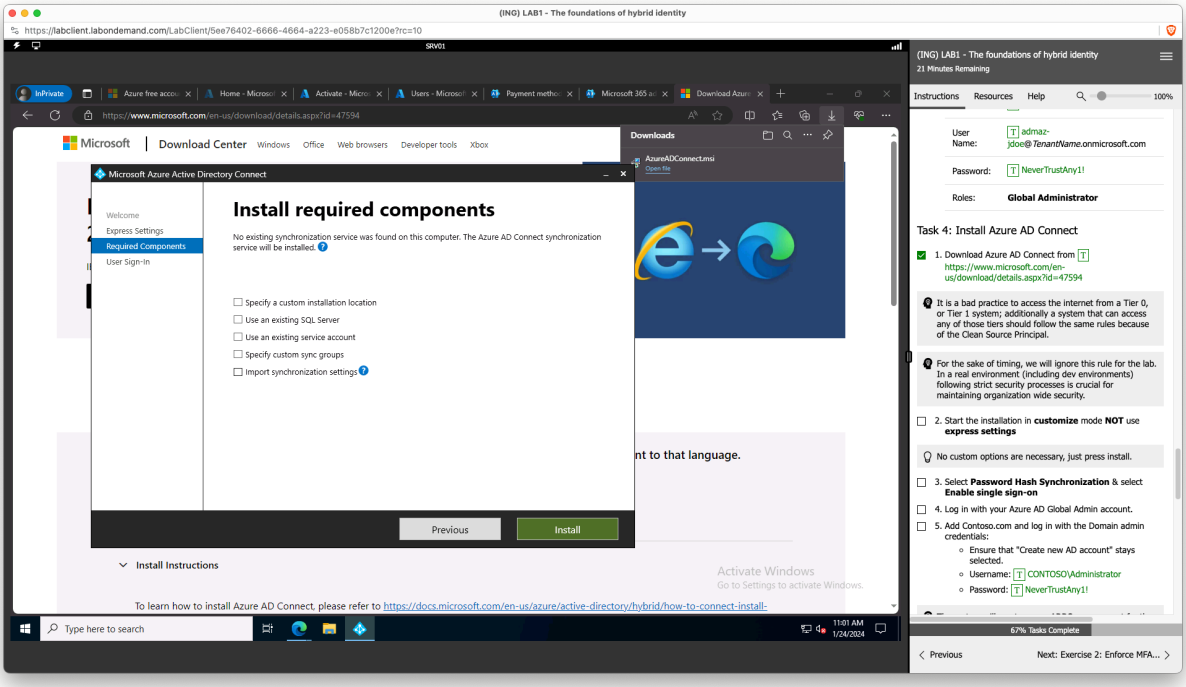
Module 1 – Lab 1 – The foundations of hybrid identity



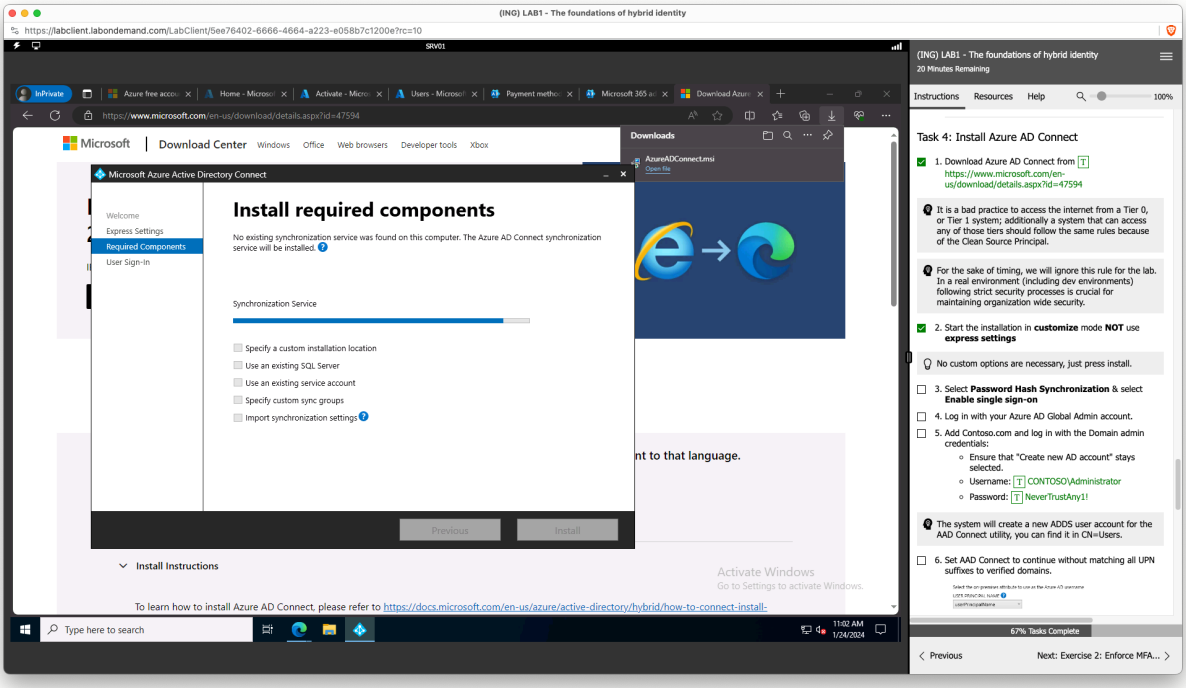


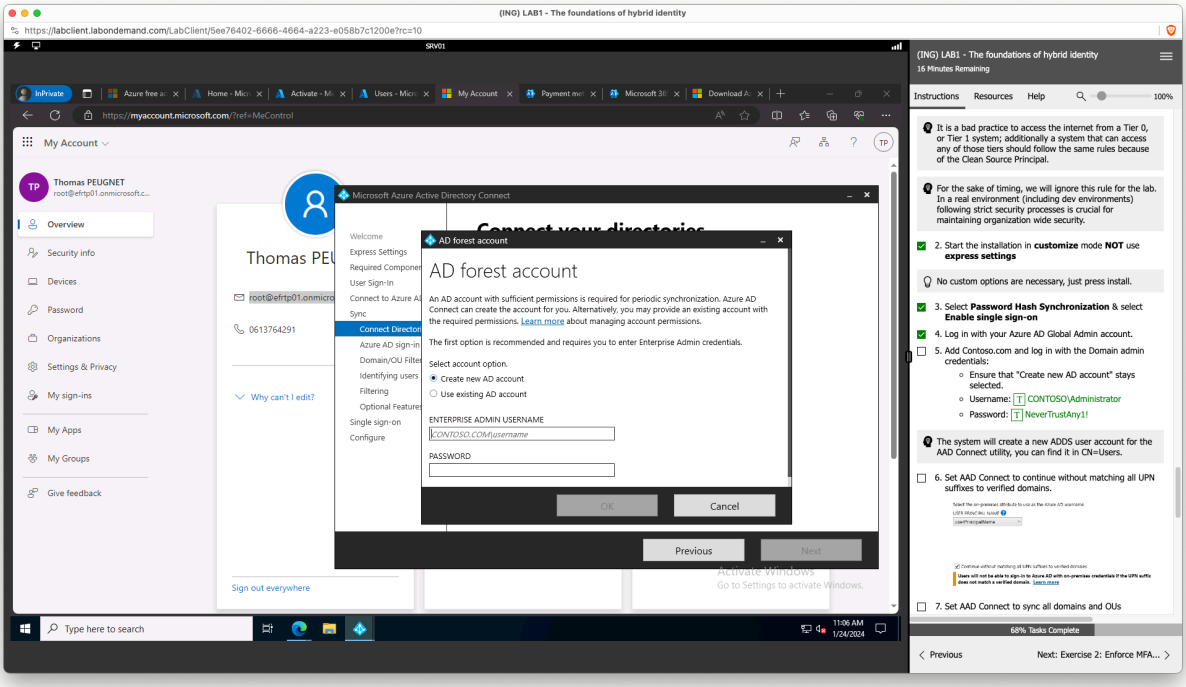
Module 1 – Lab 1 – The foundations of hybrid identity



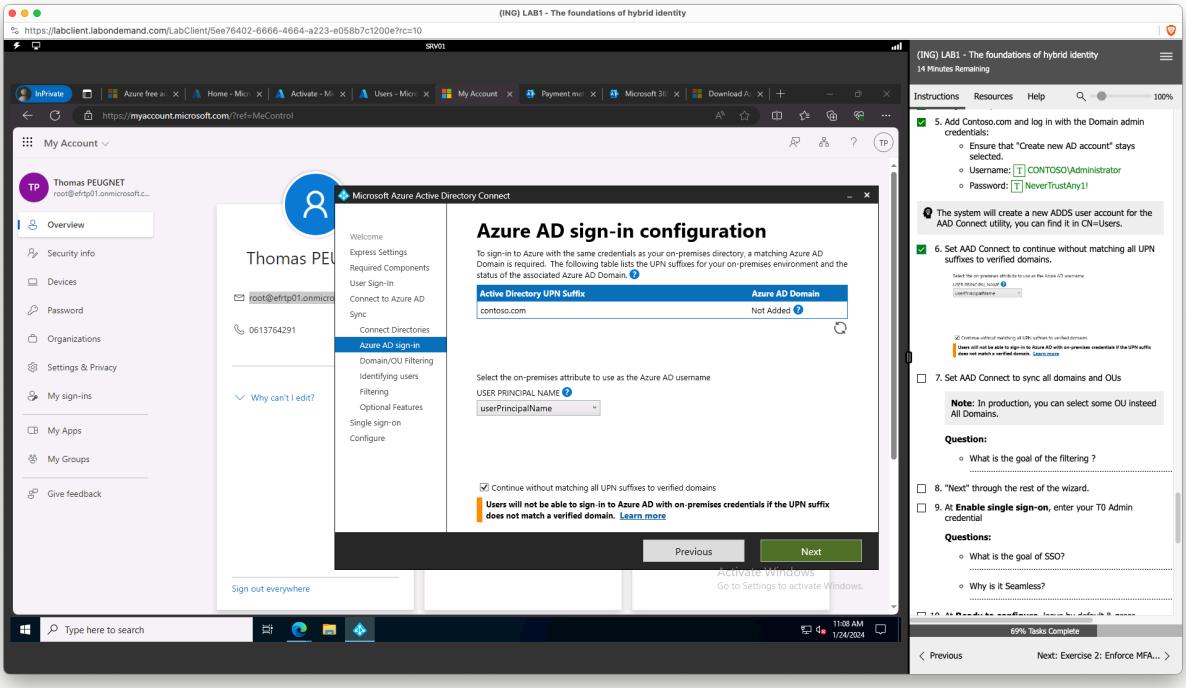


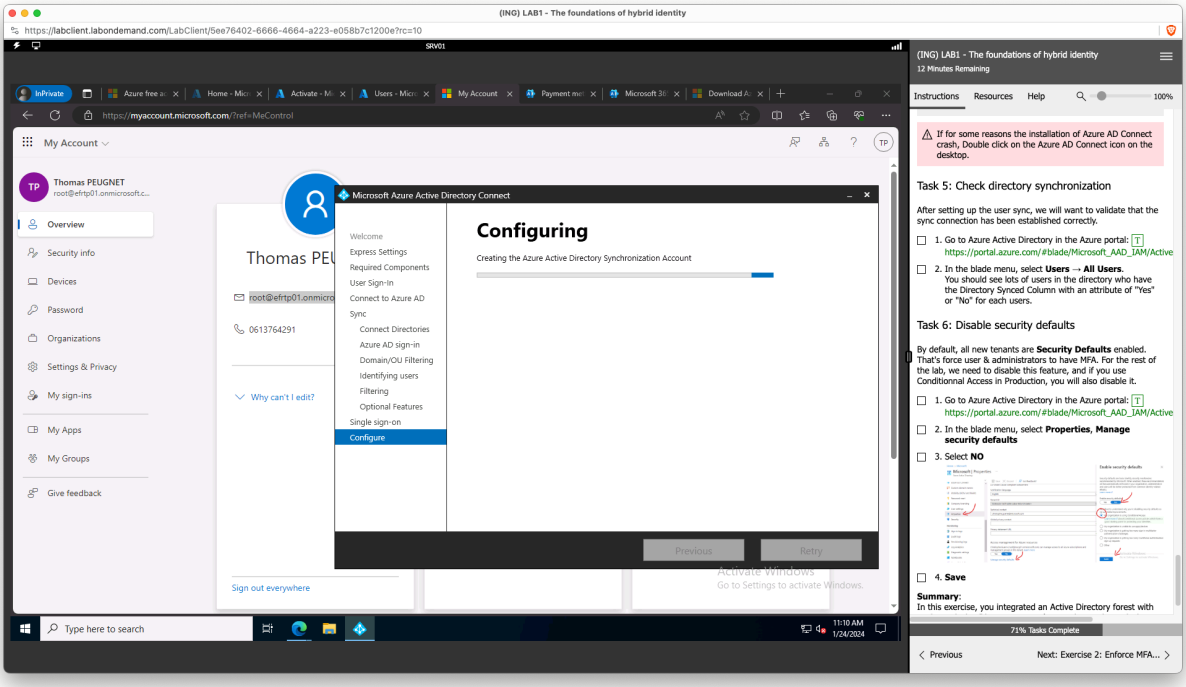
Module 1 – Lab 1 – The foundations of hybrid identity



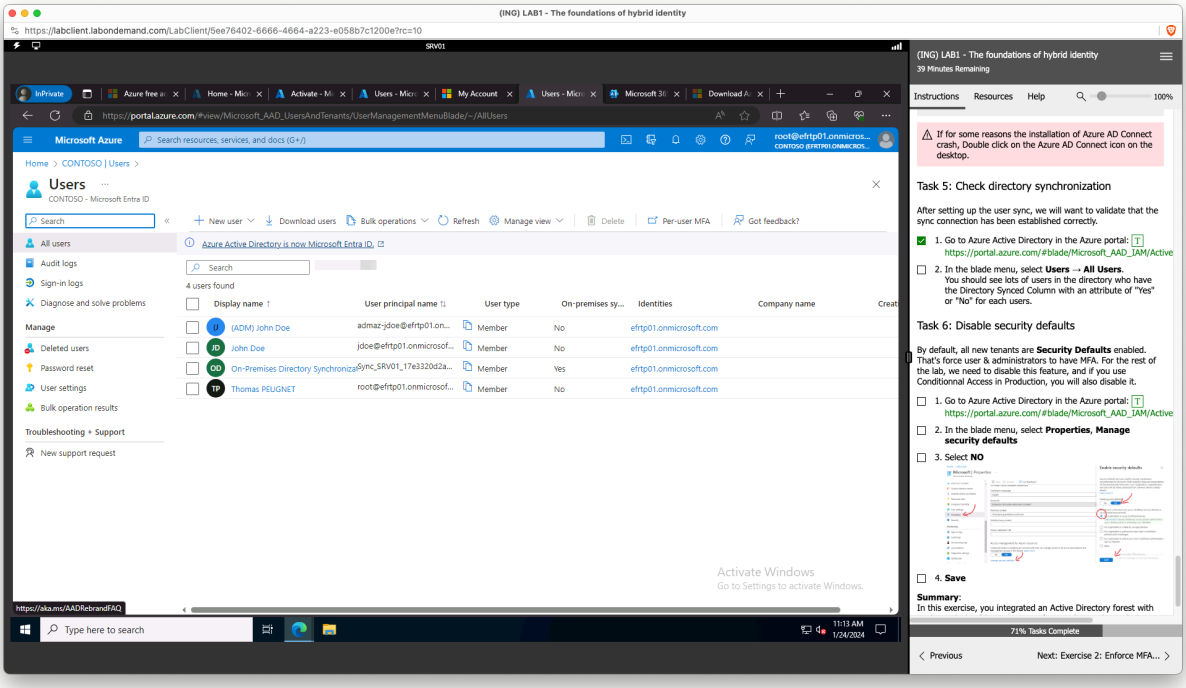


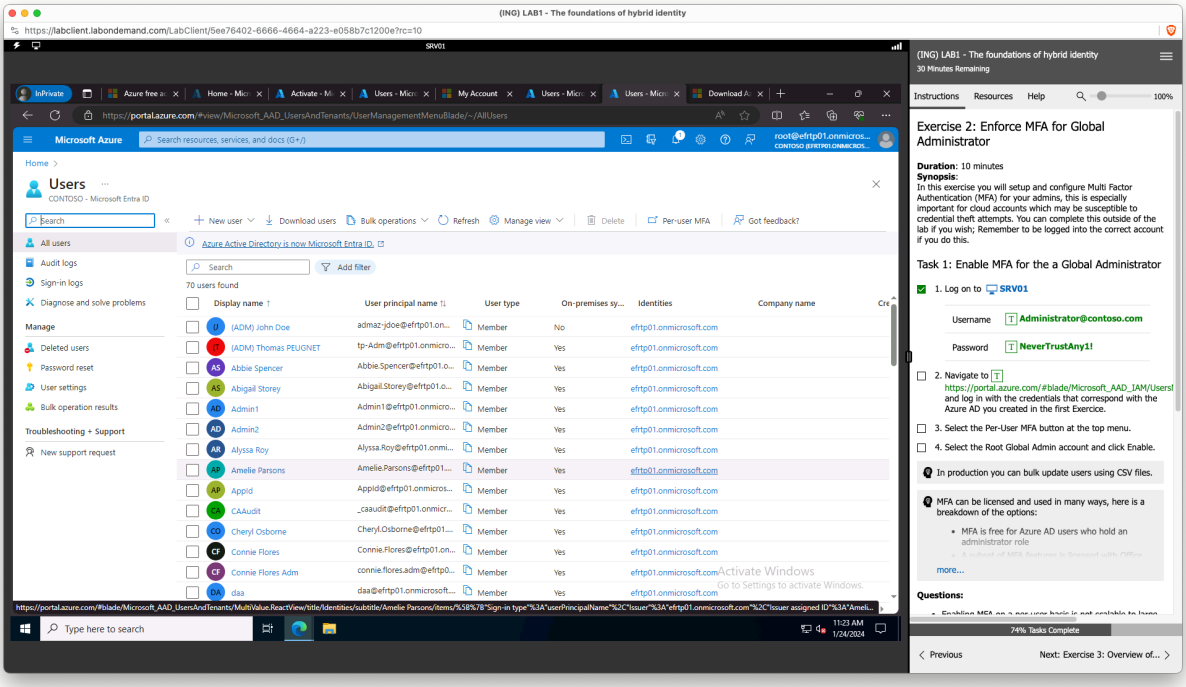
Module 1 – Lab 1 – The foundations of hybrid identity



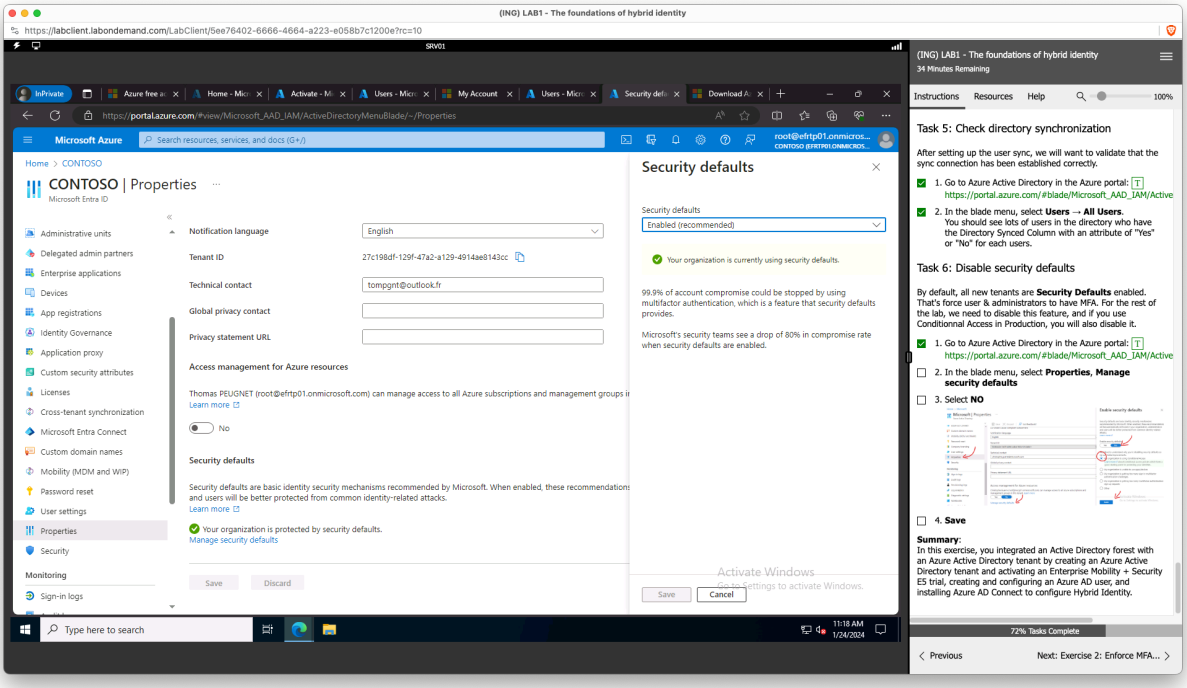


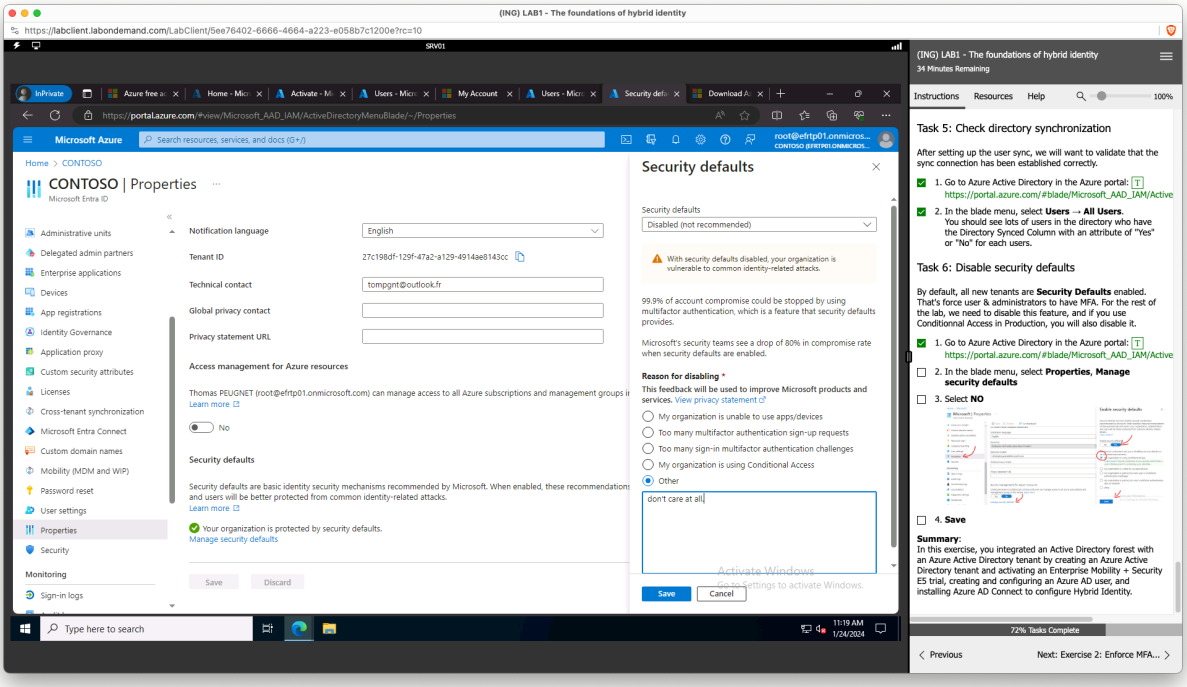
Module 1 – Lab 1 – The foundations of hybrid identity





Module 1 – Lab 1 – The foundations of hybrid identity



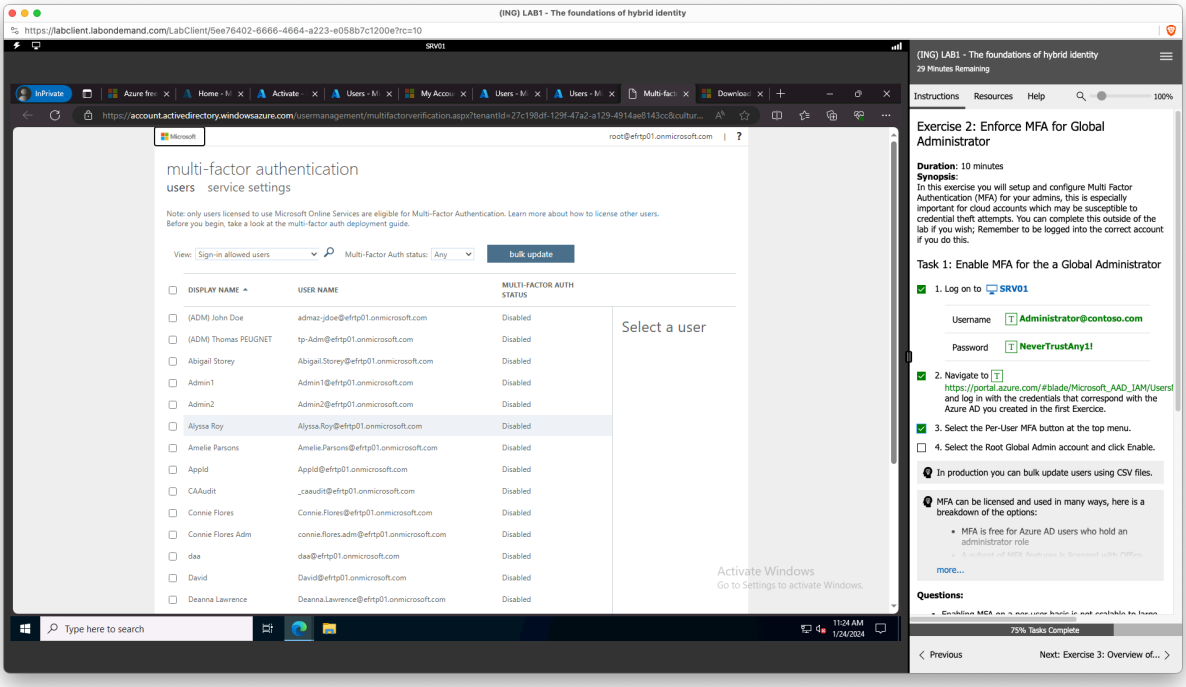


Exercise 2: Enforce MFA for Global Administrator

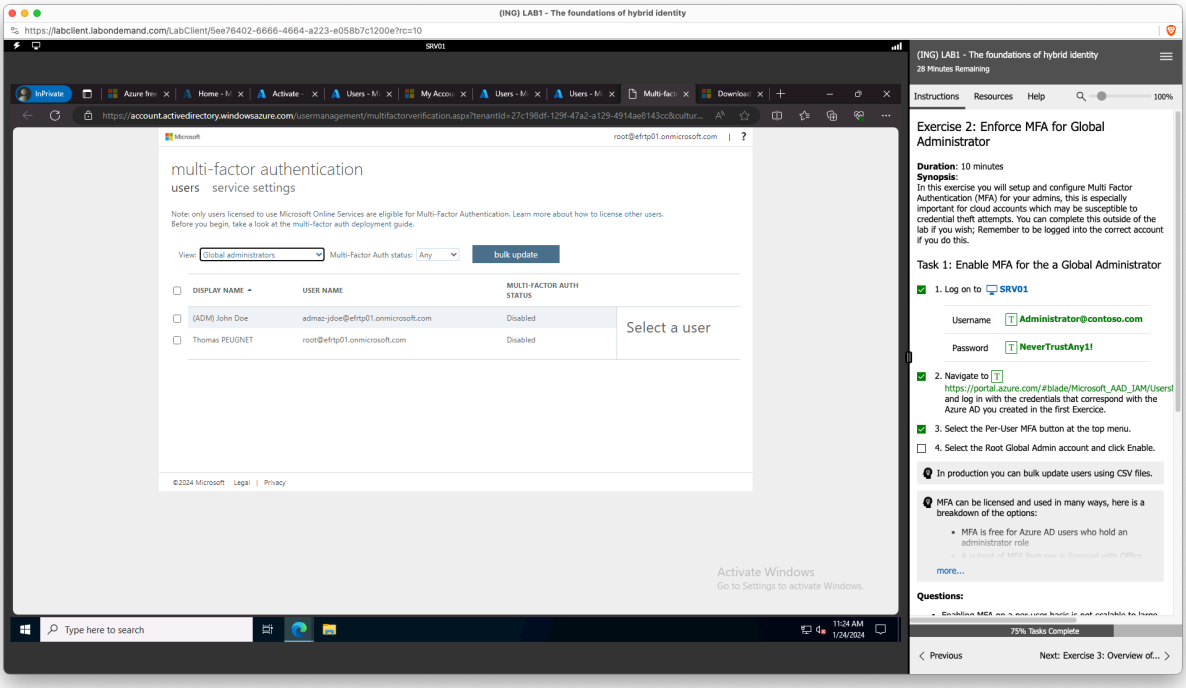
Task 1: Enable MFA for Global Administrators

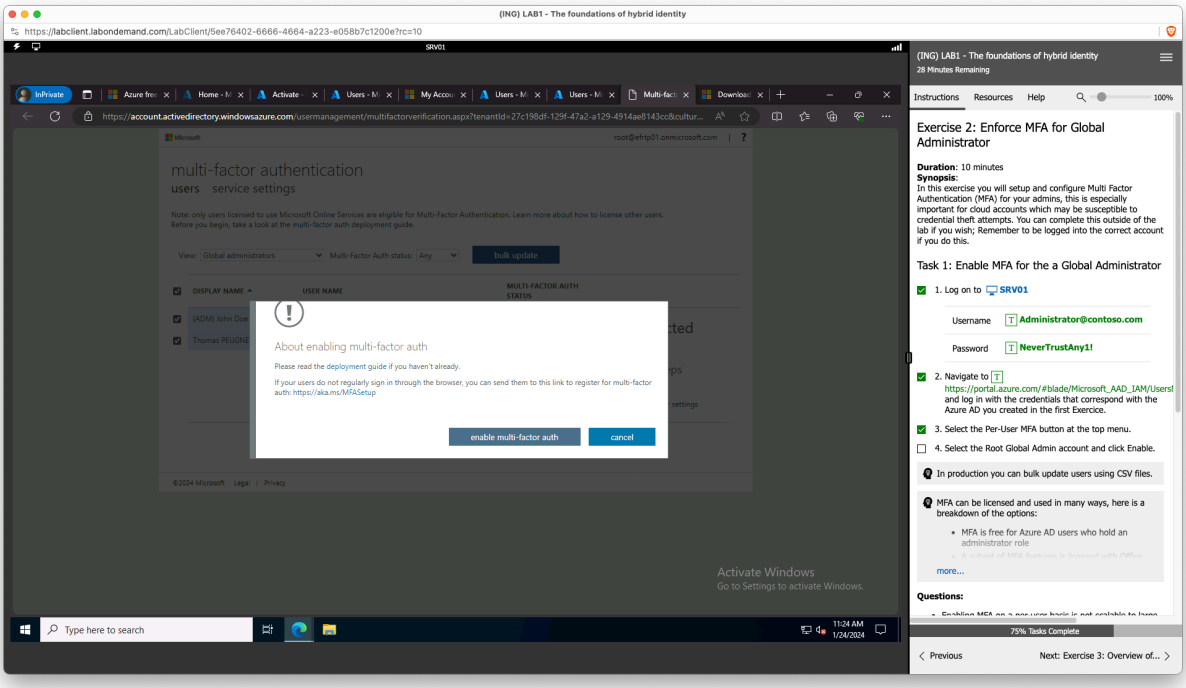
Questions:

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

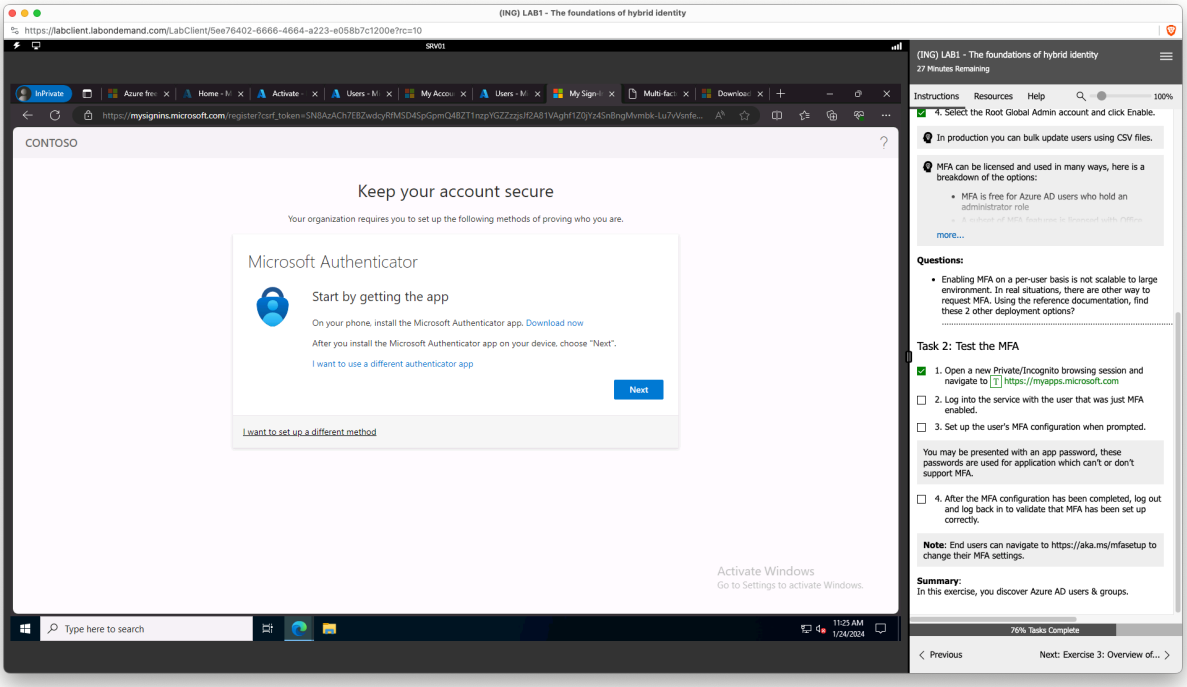


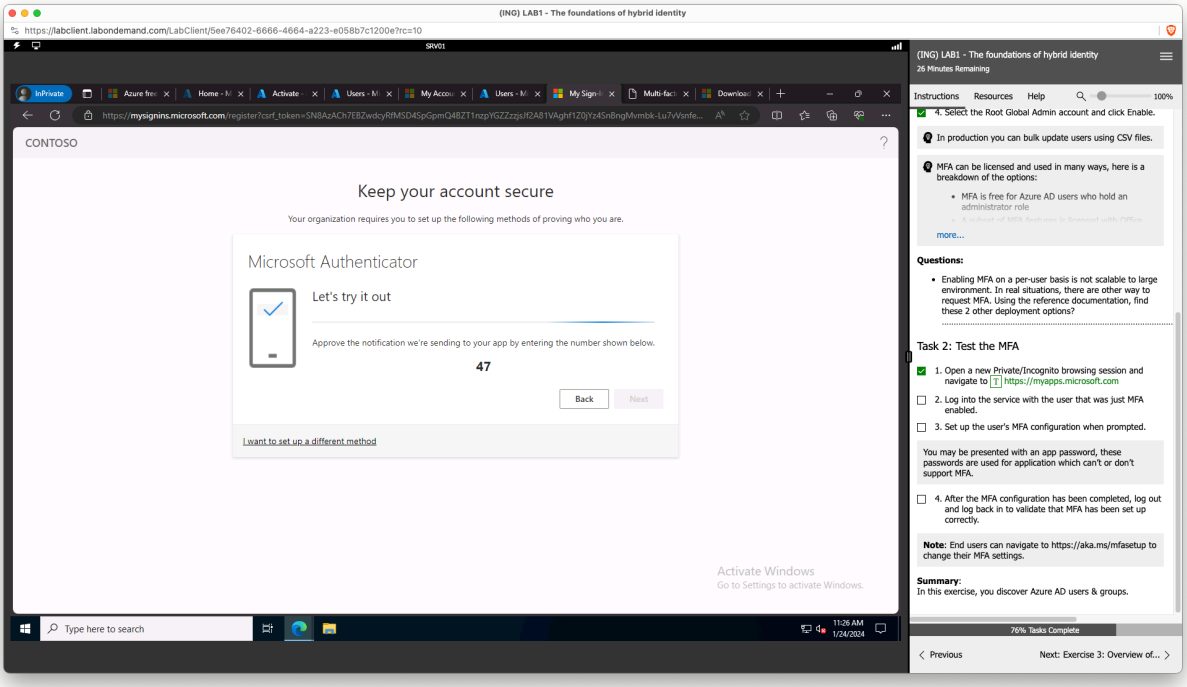
Module 1 – Lab 1 – The foundations of hybrid identity



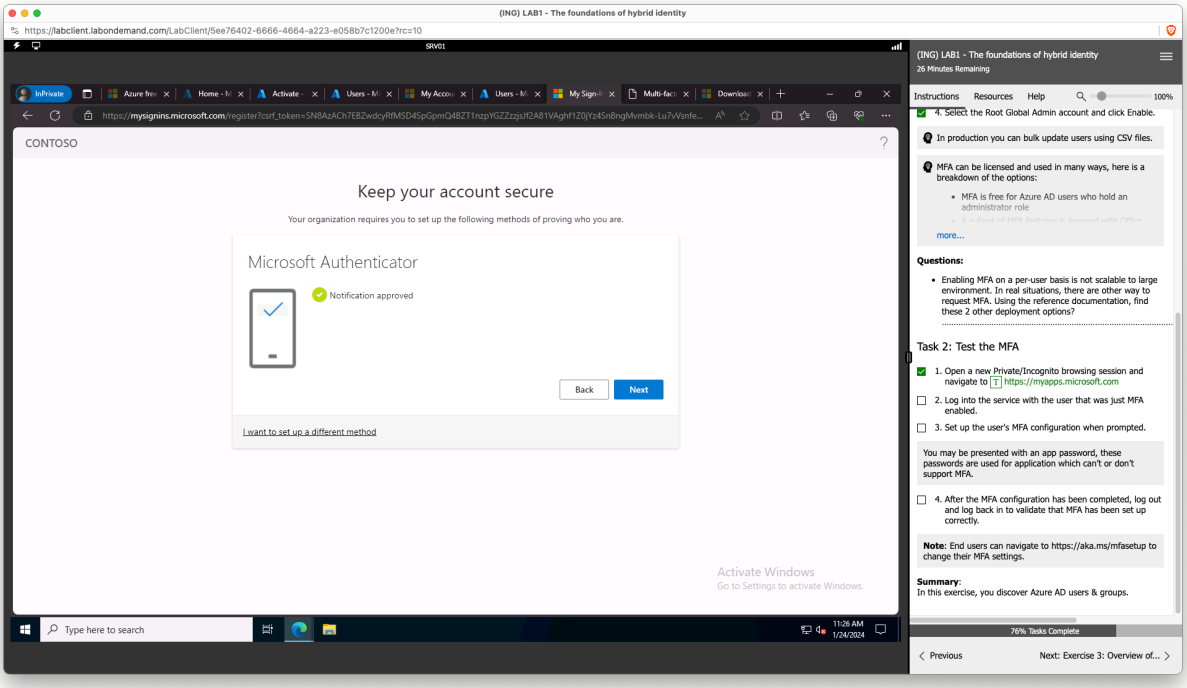


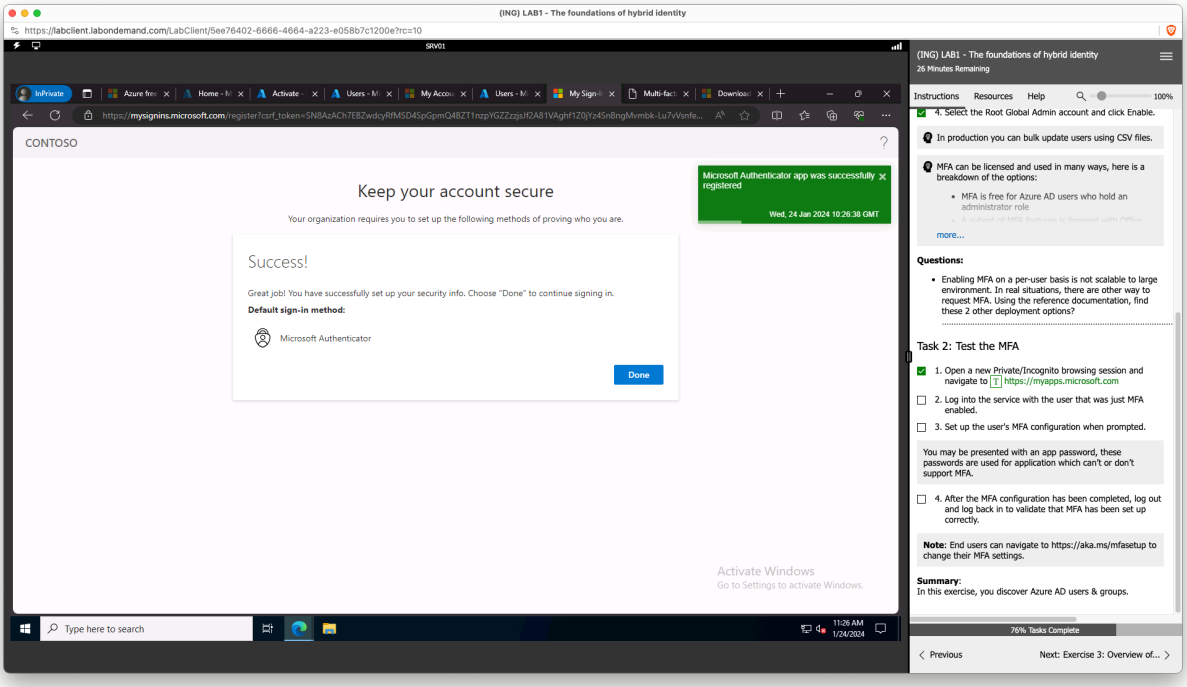
Task 2: Test the MFA

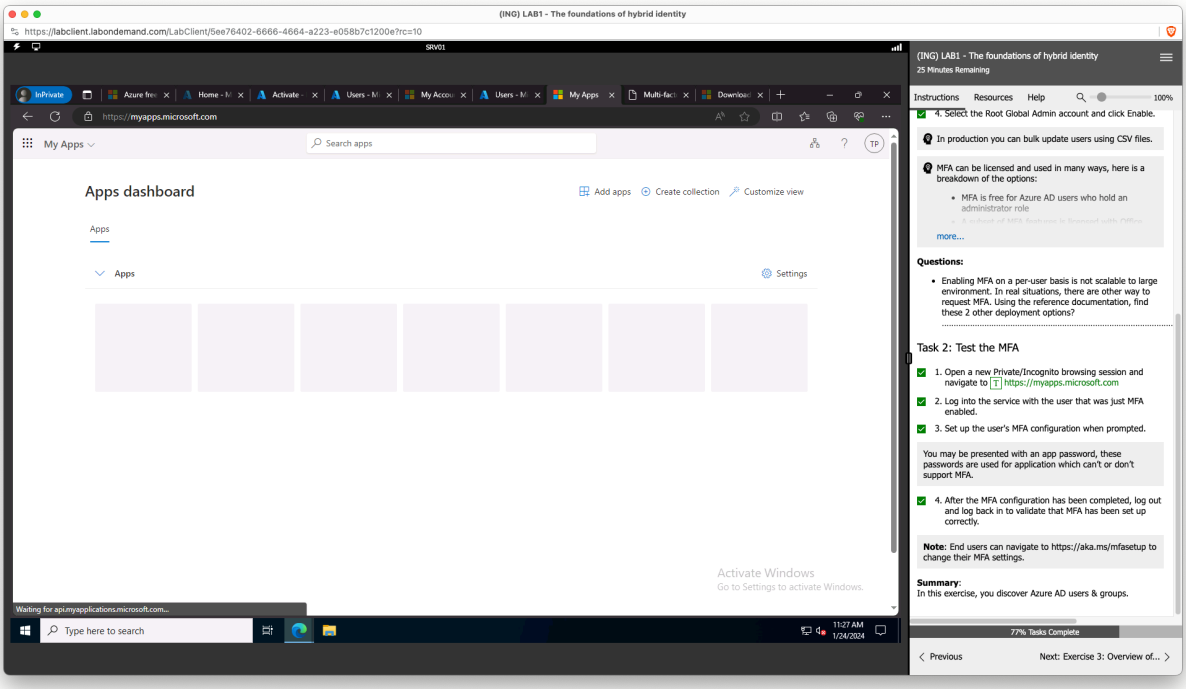




Module 1 – Lab 1 – The foundations of hybrid identity







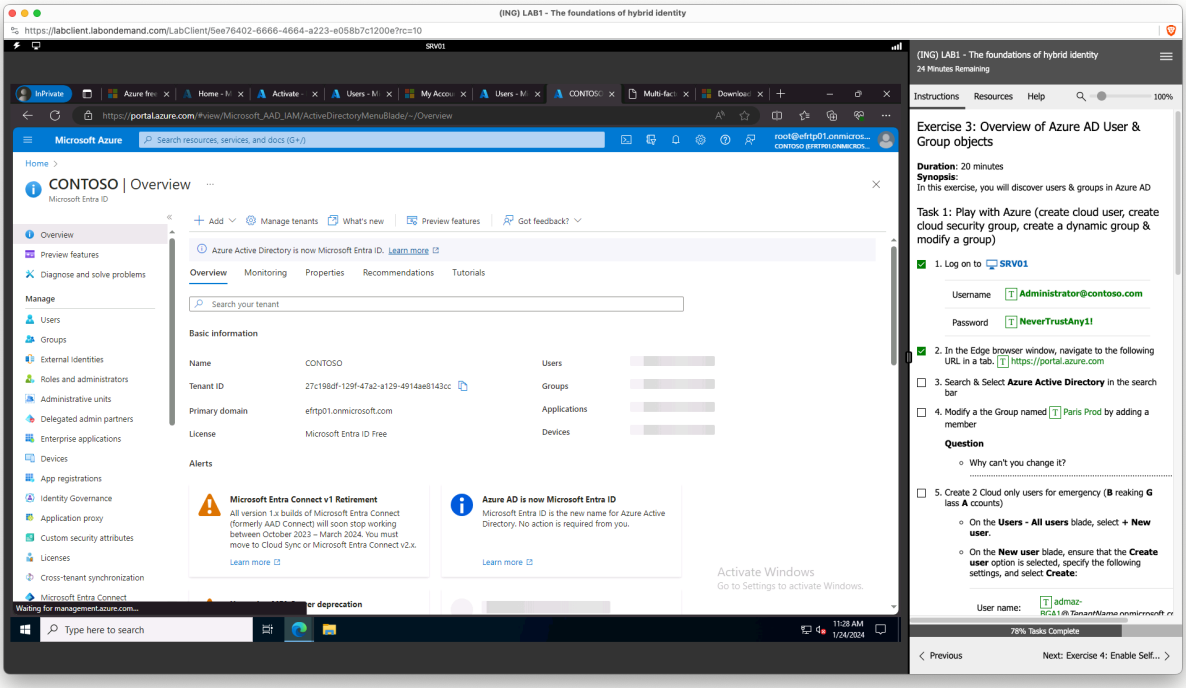
Exercise 3: Overview of Azure AD User & Group objects

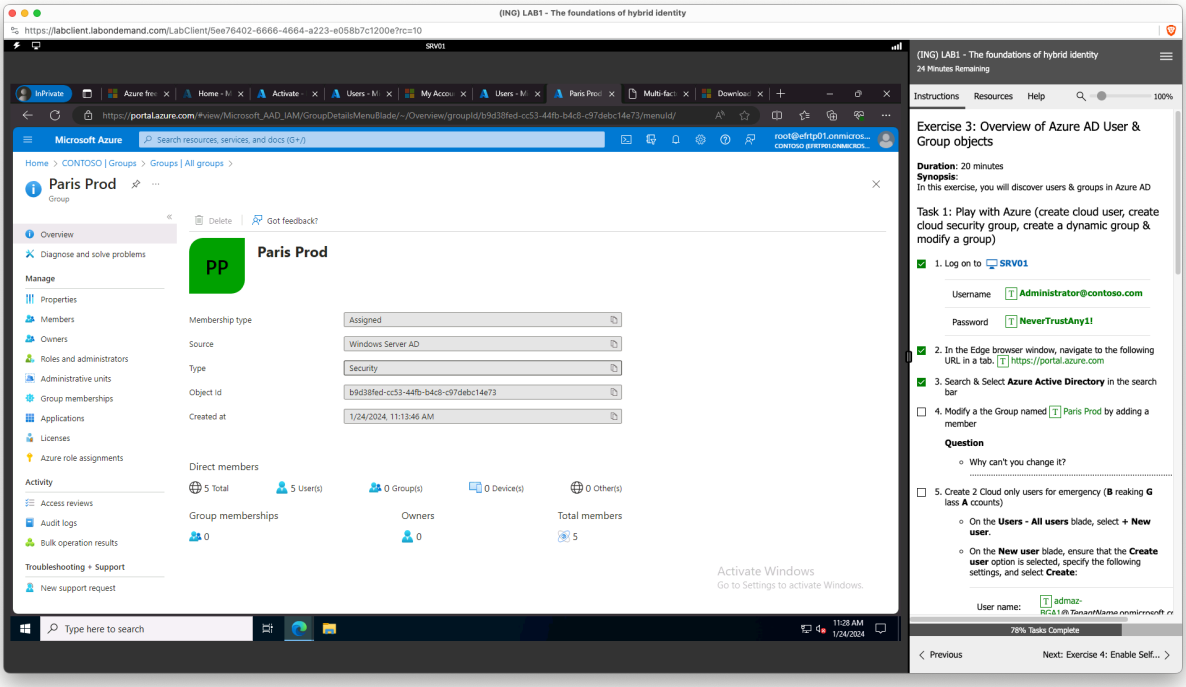
Task 1: Play with Azure (create cloud user, create cloud security group, create a dynamic group & modify a group)

Question

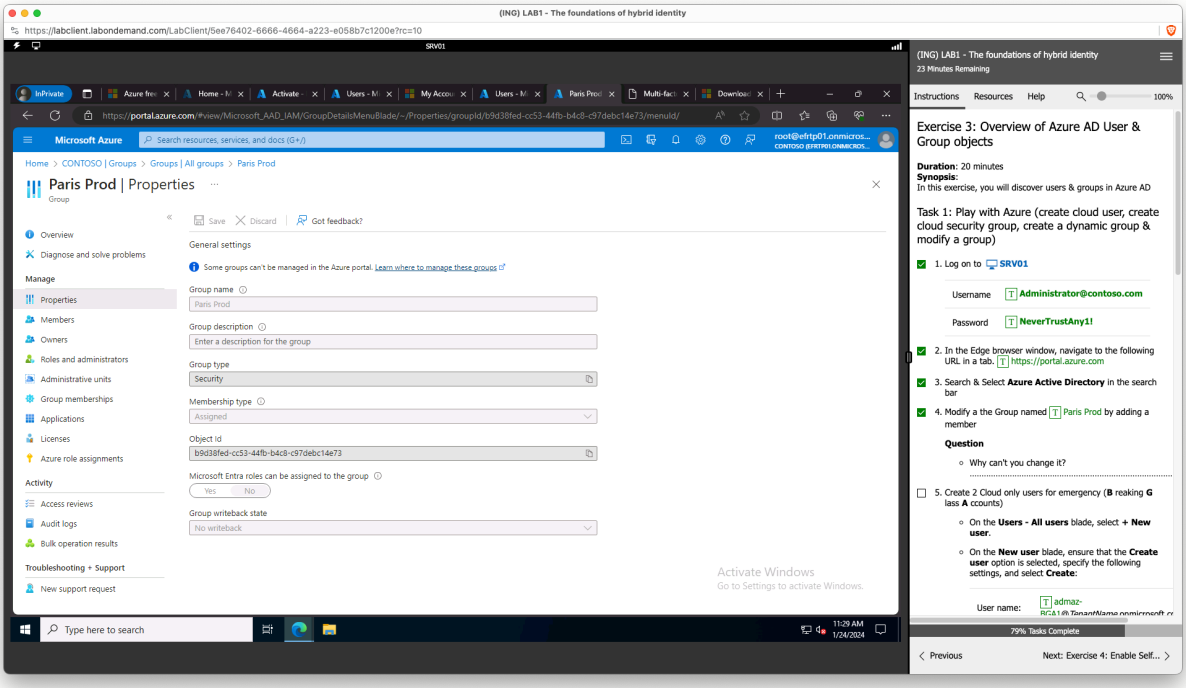
- Why can't you change it?
    - Je n’ai pas les droits suffisants. Mon Azure AD ne peut pas modifier un on Premise.

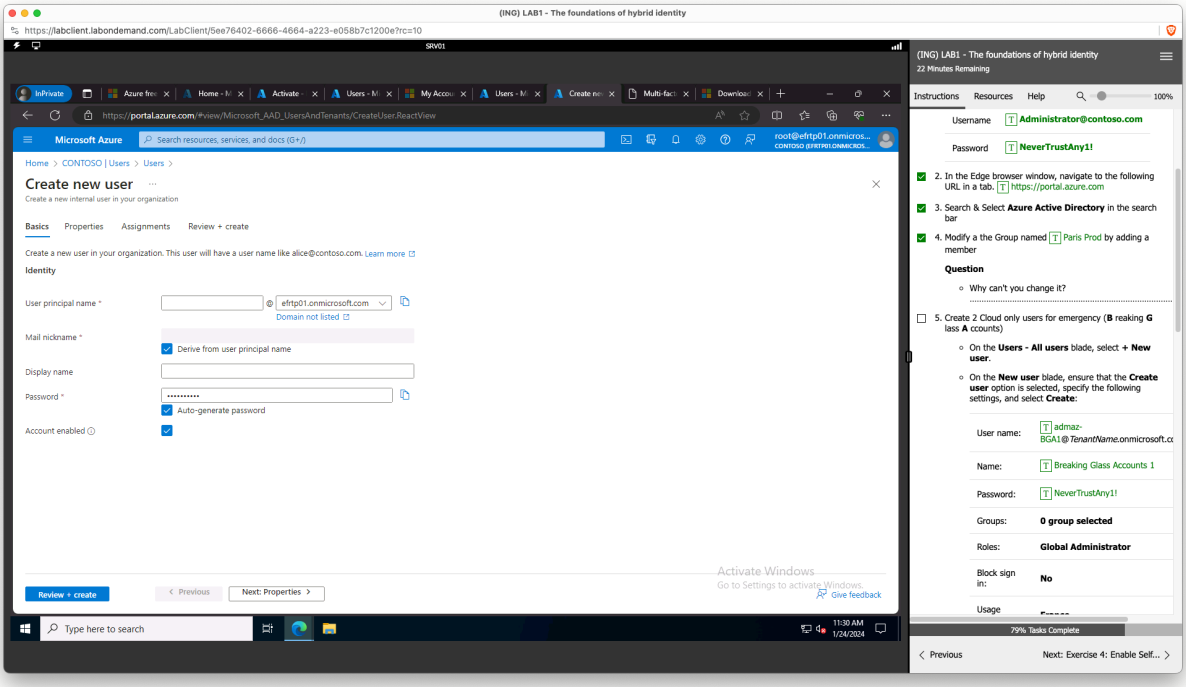
Module 1 – Lab 1 – The foundations of hybrid identity



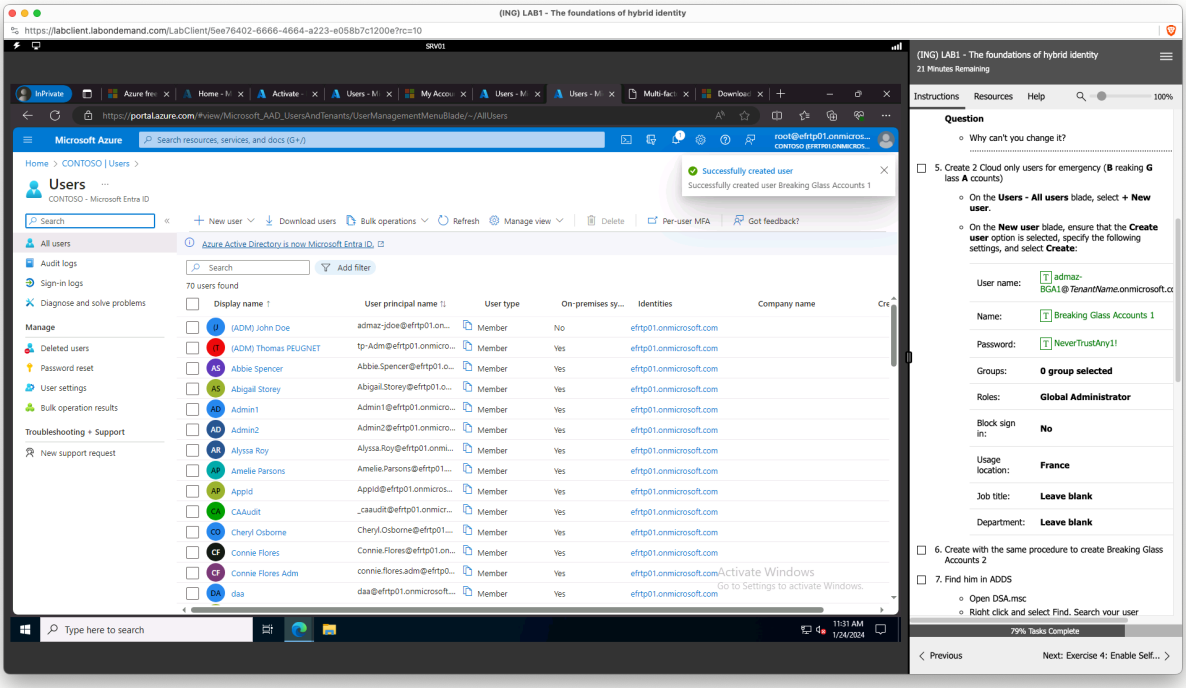


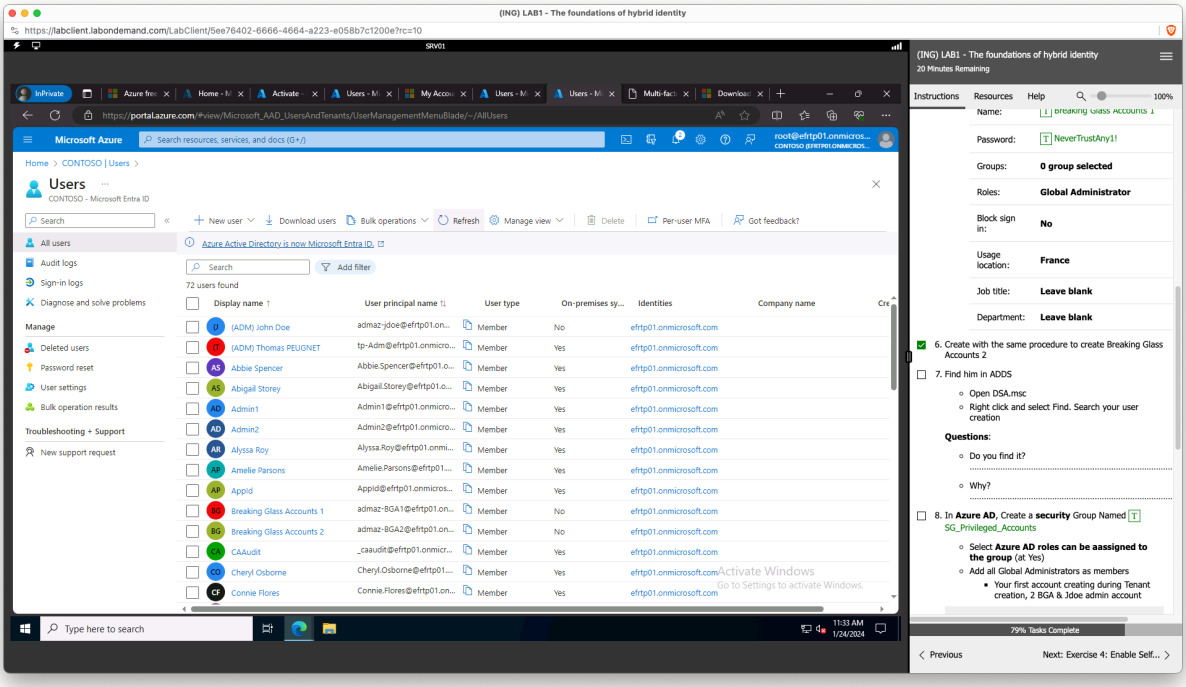
Module 1 – Lab 1 – The foundations of hybrid identity



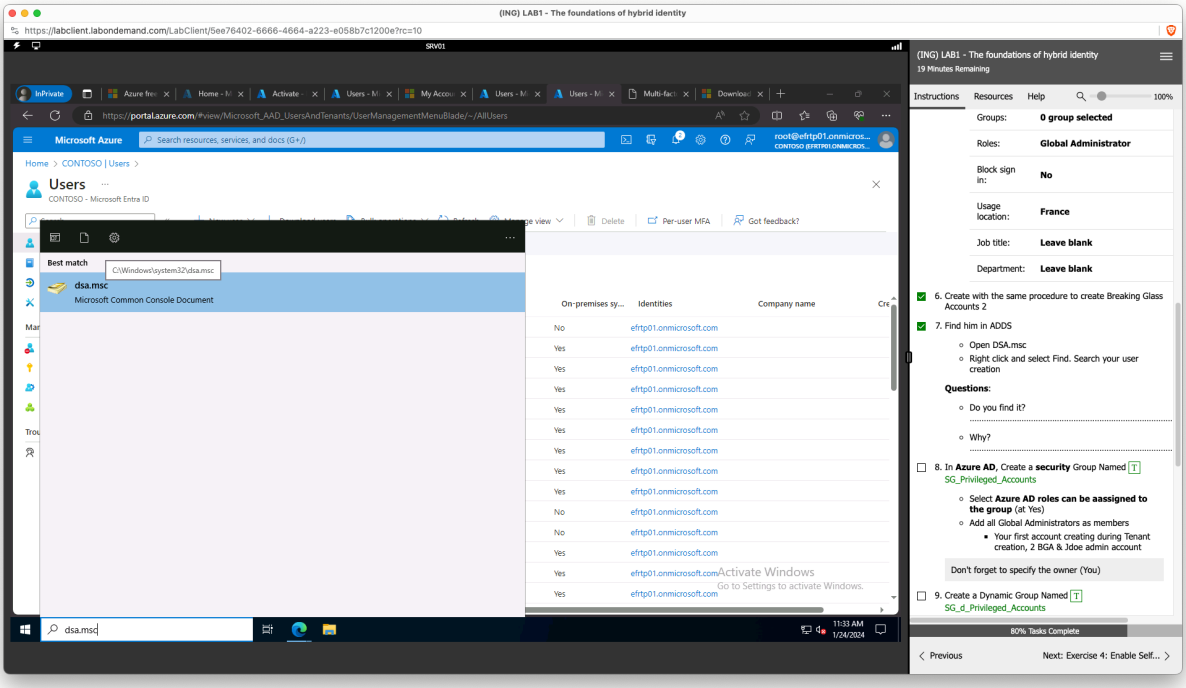


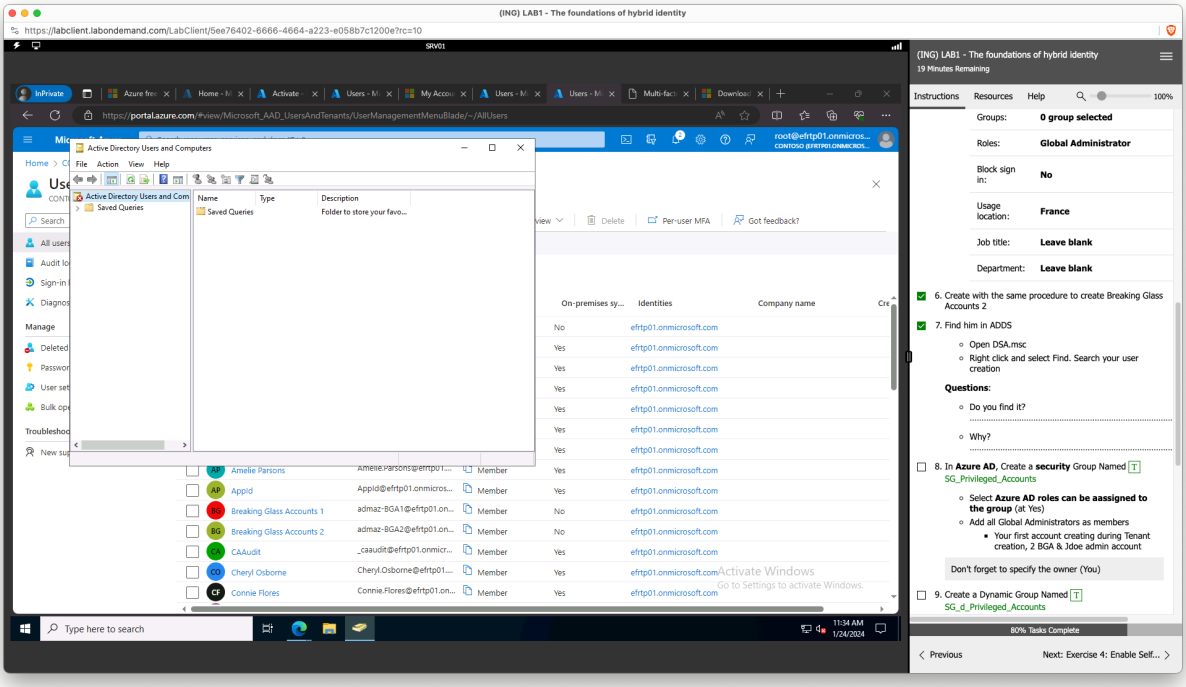
Module 1 – Lab 1 – The foundations of hybrid identity



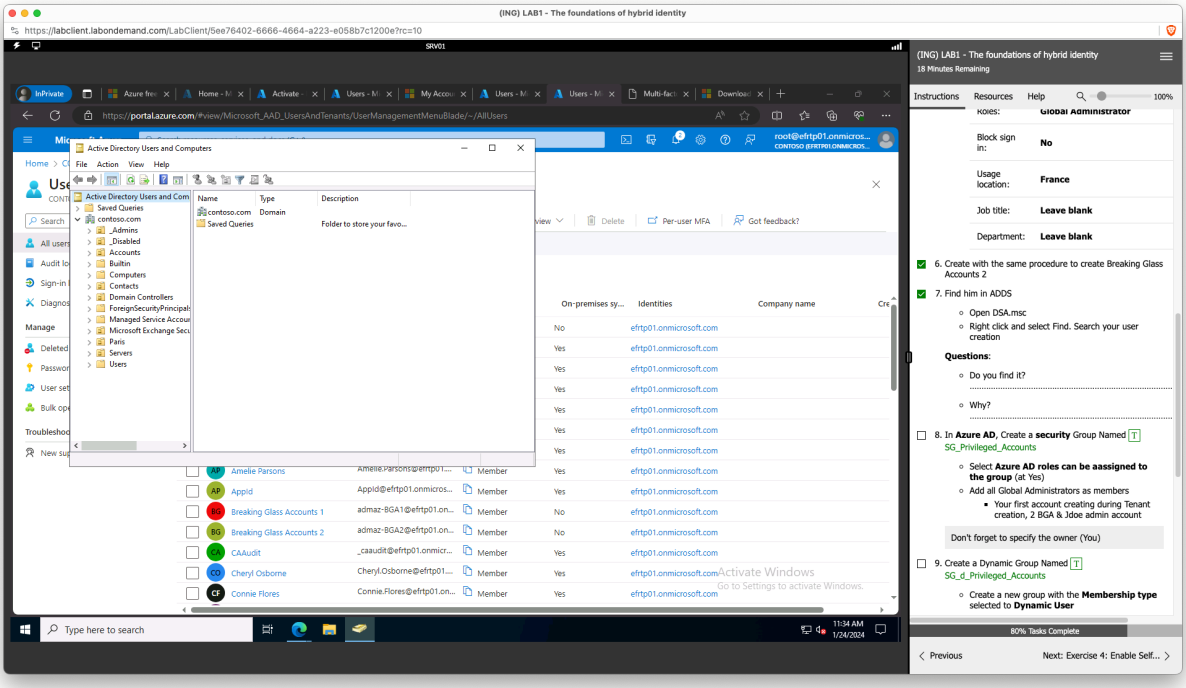


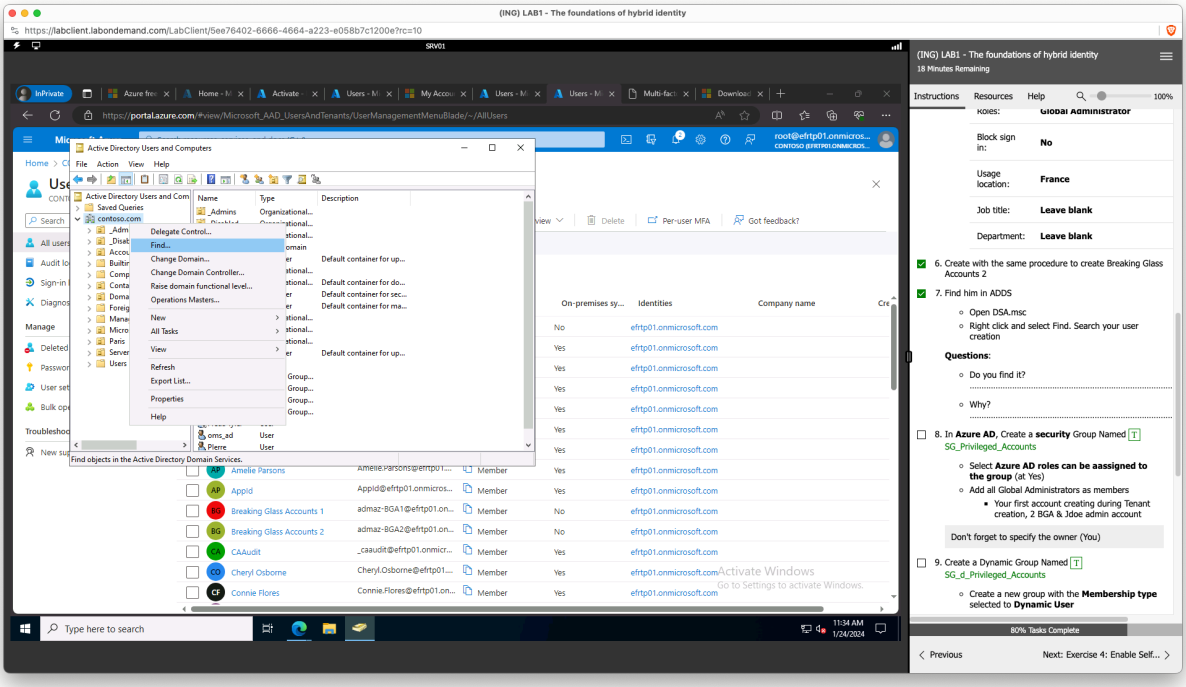
Module 1 – Lab 1 – The foundations of hybrid identity



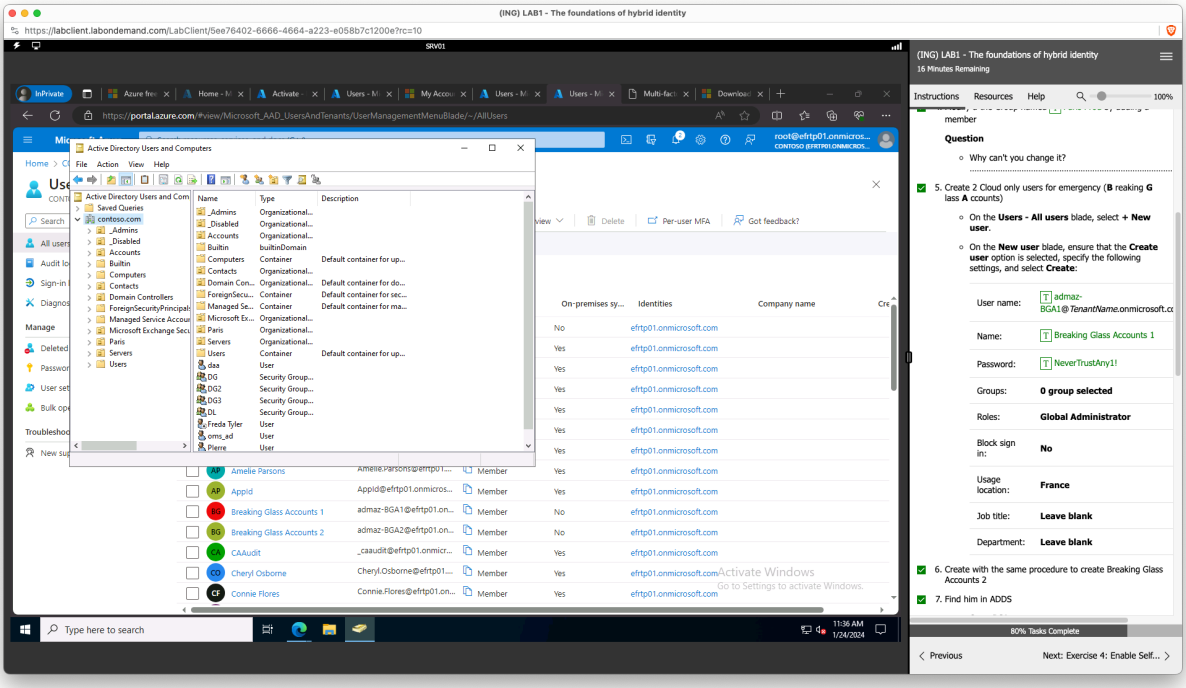


Module 1 – Lab 1 – The foundations of hybrid identity





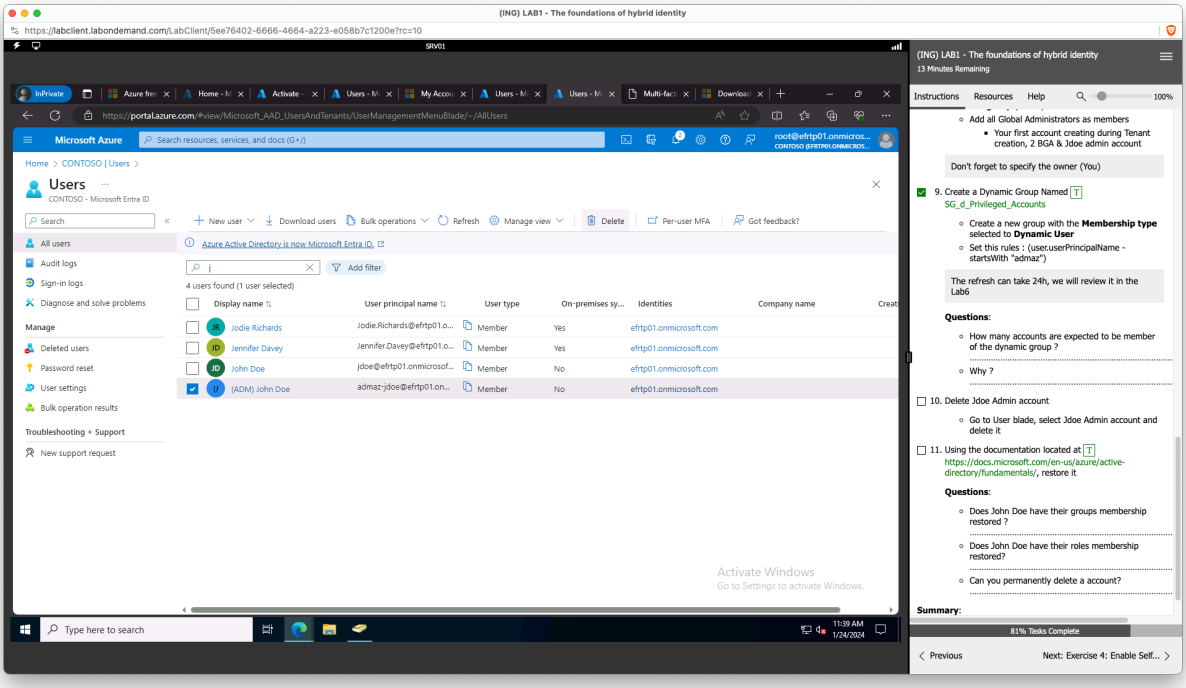
Module 1 – Lab 1 – The foundations of hybrid identity

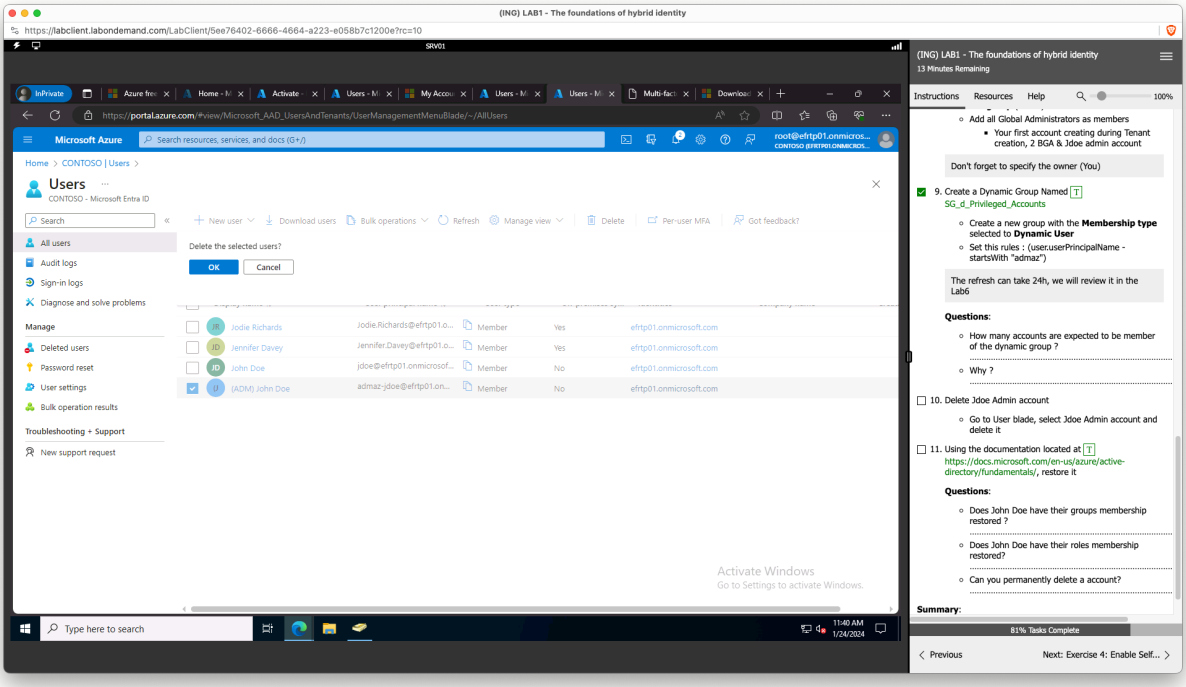


Questions:

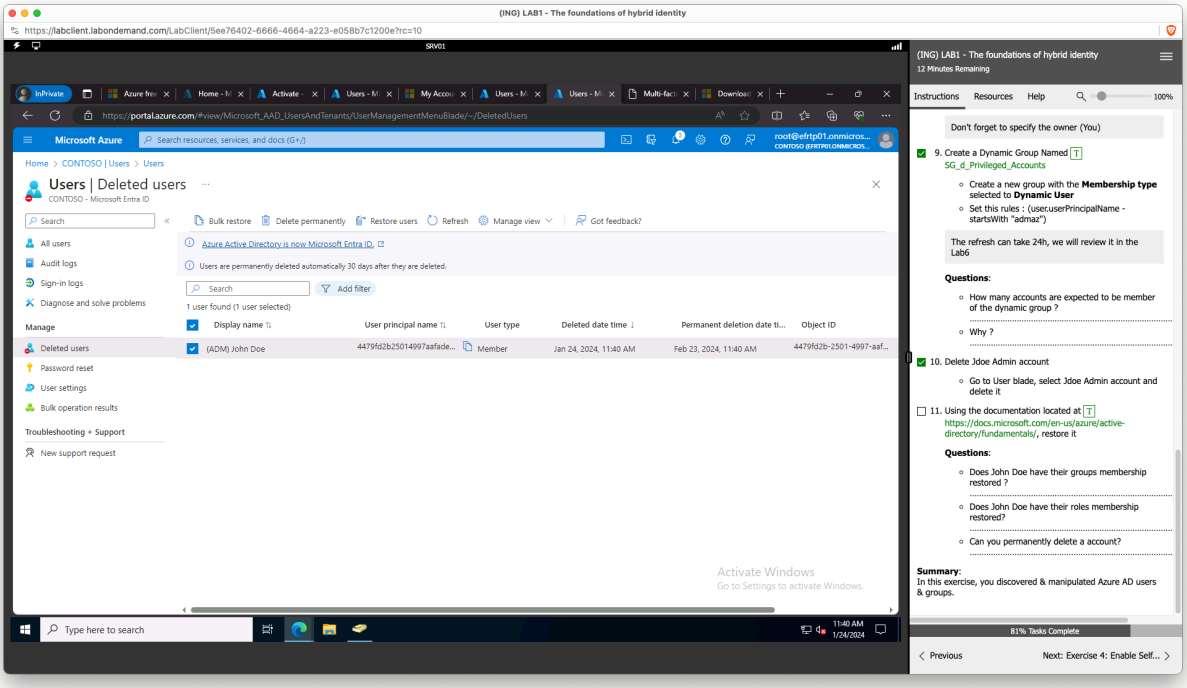
- Do you find it?
    - Non
- Why?
    - La synchronization est unilatérale, pour cette raison qu'il n'apparqît pas.

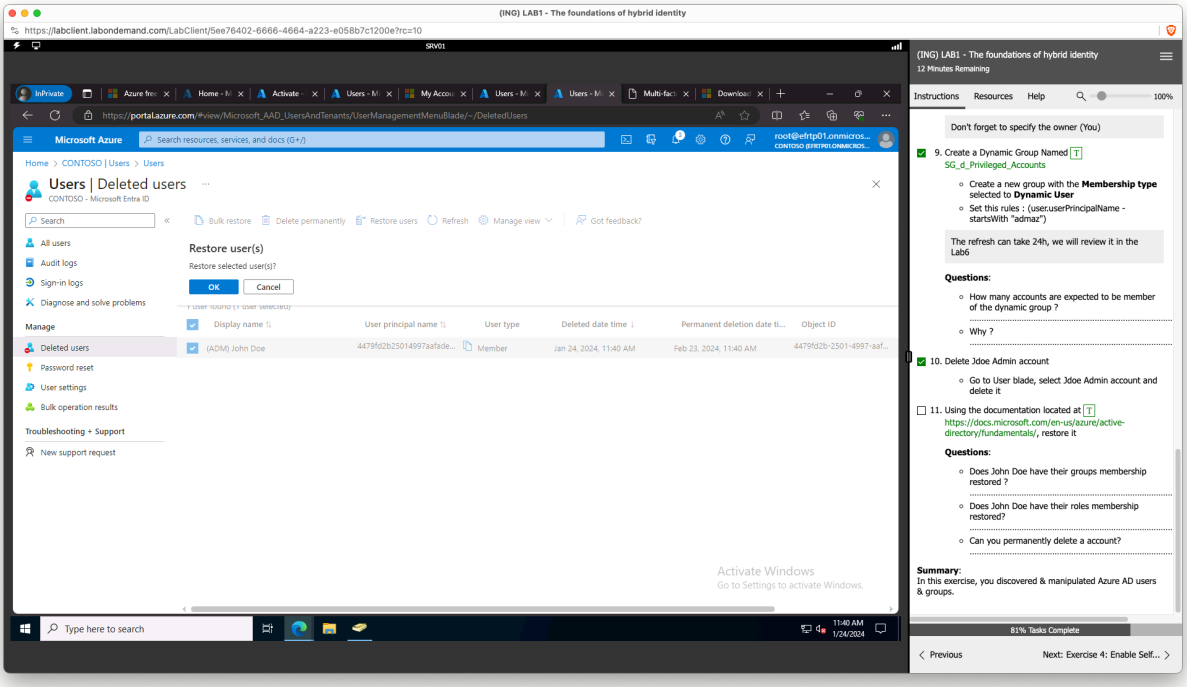
Module 1 – Lab 1 – The foundations of hybrid identity

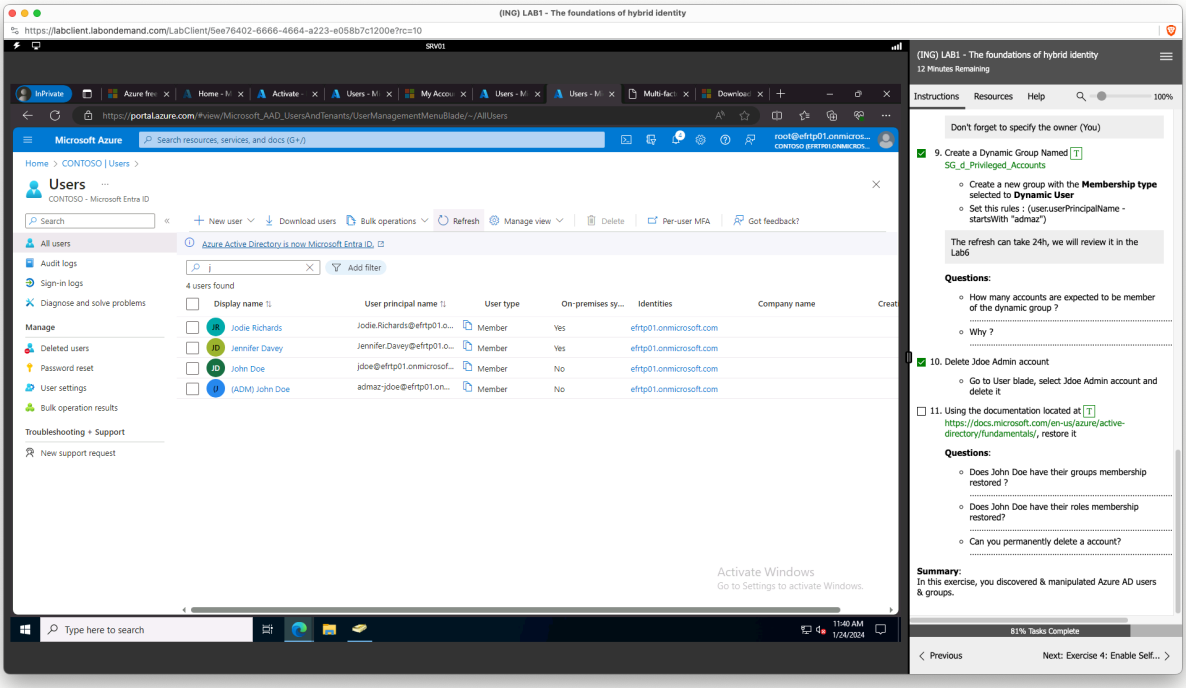




Module 1 – Lab 1 – The foundations of hybrid identity







Questions:

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

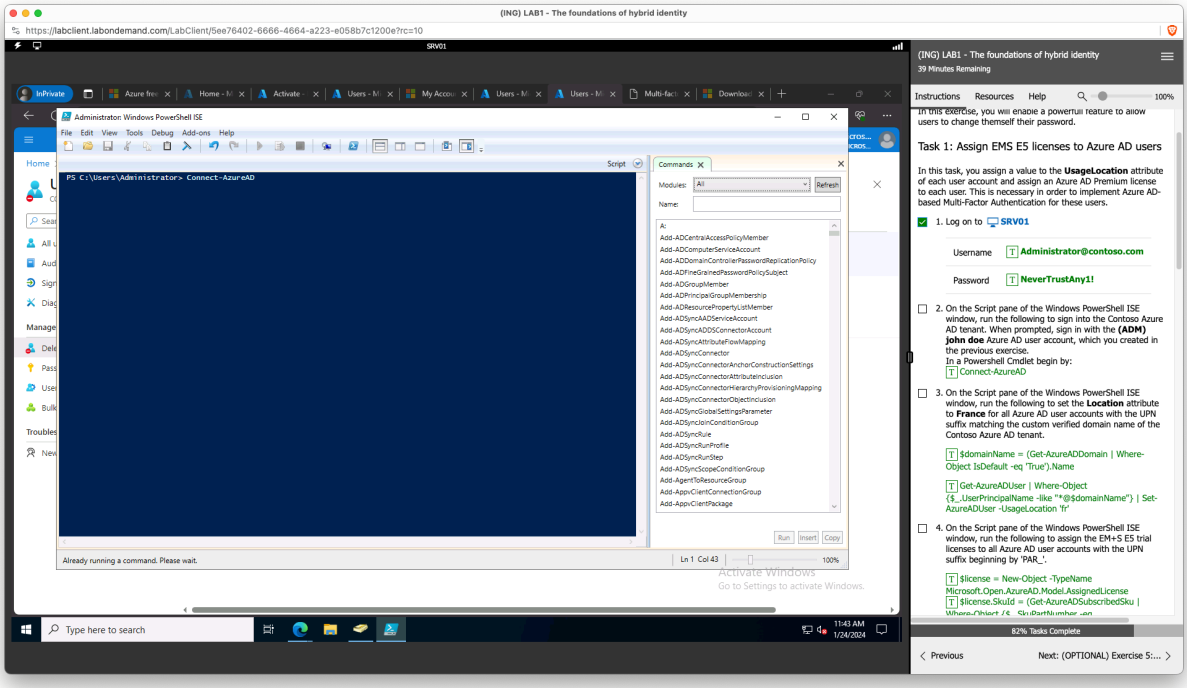
Exercise 4: Enable Self Service Password Reset

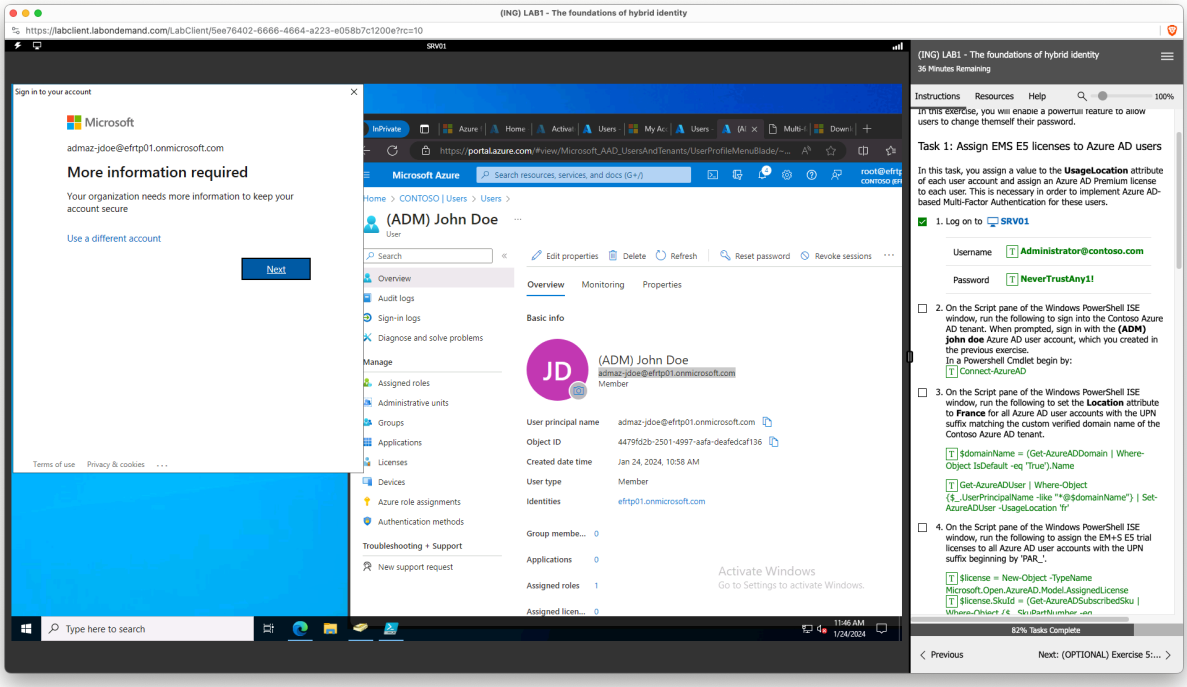
Task 1: Assign EMS E5 licenses to Azure AD users

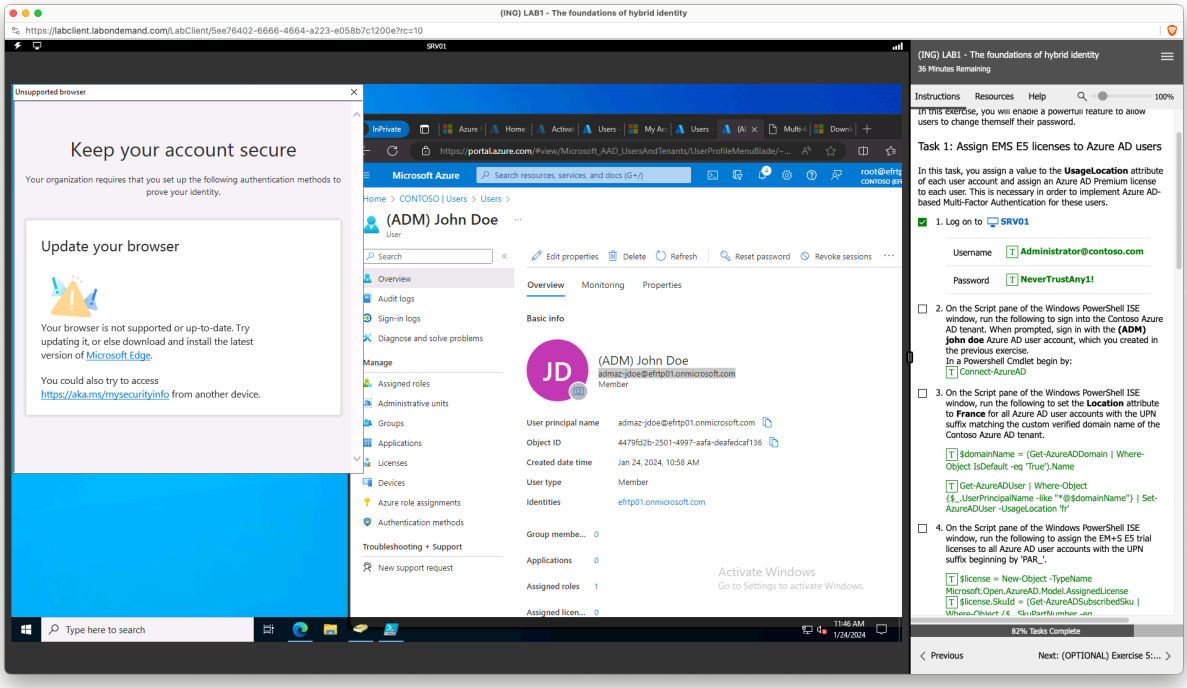
Questions:

- 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







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