**Sécurisation d’un domaine**

**Présenté par:**

**Mathis Douangpanya**

**Titre :** Sécurisation d'un domaine avec les GPO

**Date :** 31octobre 2024

**Le nom du responsable :** Mathis Douangpanya

**Objectif du laboratoire :**

* L’objectif de cet exercice est de sécuriser un domaine Active Directory en configurant des paramètres de sécurité via les Group Policy Object (GPO).
* Automatiser le déploiement d'applications sur un parc informatique via une GPO.
* Vérifier l’application correcte des politiques à l'aide de tests pratiques.

**Situation actuelle de l’ordinateur :** Toute configuration antérieure à ce laboratoire.

**Tâche à réaliser :**

* Longueur du mot de passe : Assurez-vous que le mot de passe des utilisateurs contient au moins 10 caractères
* Historique des mots de passe : Empêchez les utilisateurs de réutiliser les 3 derniers mots de passe.
* Complexité des mots de passe : Le mot de passe doit être une combinaison de lettres, de chiffres, et de caractères spéciaux.
* Expiration du mot de passe : Le mot de passe doit expirer après 60 jours
* Verrouillage de session : La session utilisateur doit se verrouiller automatiquement après 10 minutes d’inactivité et exiger un mot de passe pour se reconnecter.
* Restriction d'accès aux lecteurs : Empêchez l’accès au lecteur C: afin que les utilisateurs ne puissent pas explorer le disque local de leur machine.
* Restrictions sur les logiciels : Mettez en place des restrictions empêchant l'exécution de fichiers exécutables non autorisés, notamment ceux situés dans les répertoires de téléchargement. Seuls les logiciels des répertoires Program Files et Windows doivent être autorisés
* Déploiement d'une application : Déployez une application de votre choix sur les ordinateurs du domaine via une GPO. Choisissez une application, créez un package d'installation et configurez la GPO pour automatiser son déploiement sur les machines de l'OU "**SecureComputers**" seulement.

**Table de matière :**

Table des matières

[Partie 1 : 5](#_Toc188542332)

[1-Longueur du mot de passe : Assurez-vous que le mot de passe des utilisateurs contient au moins 10 caractères. /1 5](#_Toc188542333)

[2- Historique des mots de passe : Empêchez les utilisateurs de réutiliser les 3 derniers mots de passe. /1 6](#_Toc188542334)

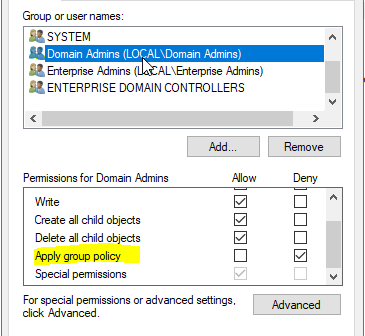
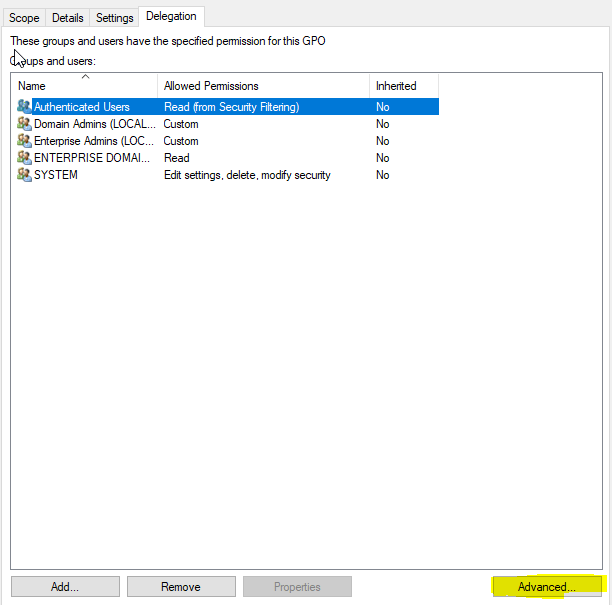
[3-Complexité des mots de passe : Le mot de passe doit être une combinaison de lettres, de chiffres, et de caractères spéciaux. /1 7](#_Toc188542335)

[4-Expiration du mot de passe : Le mot de passe doit expirer après 60 jours. /1 8](#_Toc188542336)

[Partie 2 : 9](#_Toc188542337)

[5- Verrouillage de session : La session utilisateur doit se verrouiller automatiquement après 10 minutes d’inactivité et exiger un mot de passe pour se reconnecter. /2 9](#_Toc188542338)

[6- Question bonus : Restriction d'accès aux lecteurs : Empêchez l’accès au lecteur C: sauf à l’accès à C:\Users afin que les utilisateurs ne puissent pas explorer le disque local de leur machine. /1 10](#_Toc188542339)

[ 12](#_Toc188542340)

[7-Restrictions sur les logiciels : Mettez en place des restrictions empêchant l'exécution de fichiers exécutables non autorisés, notamment ceux situés dans les répertoires de téléchargement. Seuls les logiciels des répertoires Program Files et Windows doivent être autorisés. /5 12](#_Toc188542341)

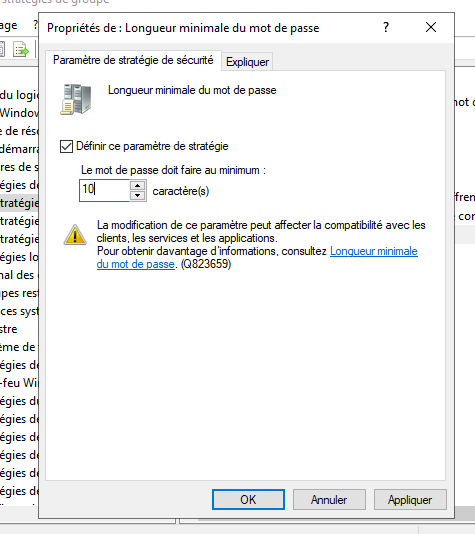
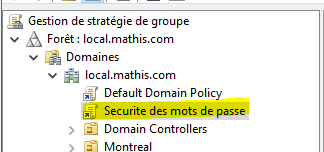
[8-Déploiement d'une application : Déployez une application de votre choix sur les ordinateurs du domaine via une GPO. Choisissez une application, créez un package d'installation et configurez la GPO pour automatiser son déploiement sur les machines de l'OU "**SecureComputers**" seulement. / 14](#_Toc188542342)

[Vérification: 17](#_Toc188542343)

# Partie 1 :

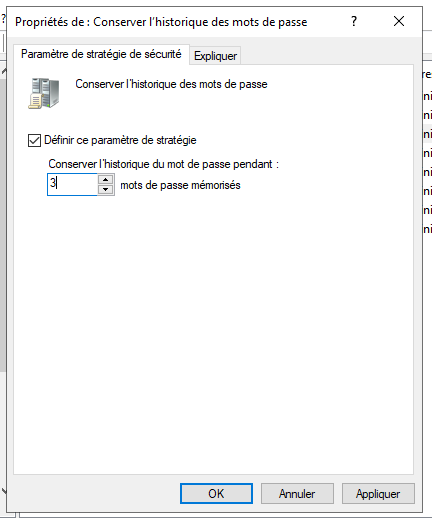
## 1-Longueur du mot de passe : Assurez-vous que le mot de passe des utilisateurs contient au moins 10 caractères. /1

* Créer GPO dans le domaine
* Été dans la modification de la GPO
* Déplacé dans paramètre Windows
* Déplacé dans paramètre de sécurité
* Déplacé vers Stratégie de compte
* Déplacé vers Stratégie de mot de passe
* Modifié la règle de sécurité longueur minimale du mot de passe
* Minimum 10 caractères.



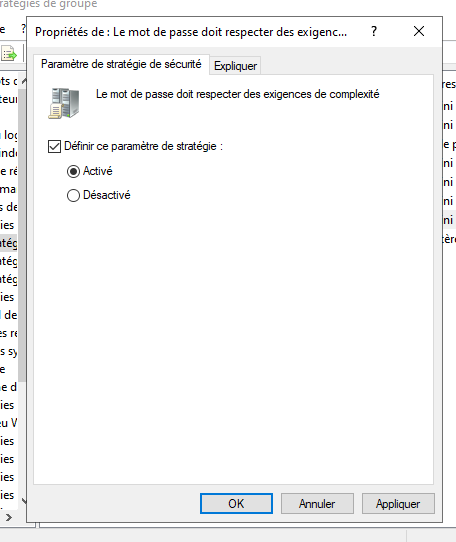
## 2- Historique des mots de passe : Empêchez les utilisateurs de réutiliser les 3 derniers mots de passe. /1

* Aller dans la modification de la GPO
* Déplacé dans paramètre Windows
* Déplacé dans paramètre de sécurité
* Déplacé vers Stratégie de compte
* Déplacé vers Stratégie de mot de passe
* Modifié la règle Conserver l’historique des mots de passe.
* 3 mots de passe mémorisés



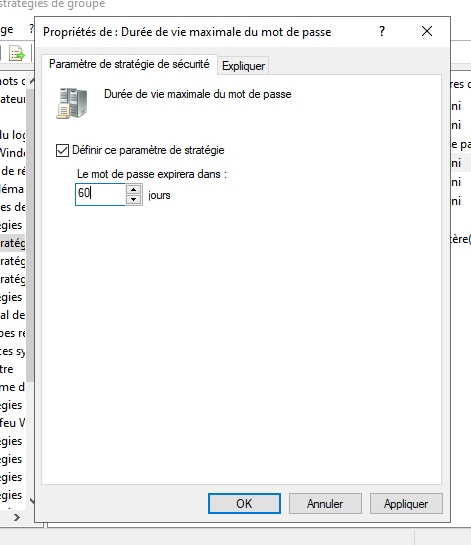
## 3-Complexité des mots de passe : Le mot de passe doit être une combinaison de lettres, de chiffres, et de caractères spéciaux. /1

* Aller dans la modification de la GPO
* Déplacé dans paramètre Windows
* Déplacé dans paramètre de sécurité
* Déplacé vers Stratégie de compte
* Déplacé vers Stratégie de mot de passe
* Modifié la règle Le mot de passe doit respecter des exigences de complexité
* Activé la règle



## 4-Expiration du mot de passe : Le mot de passe doit expirer après 60 jours. /1

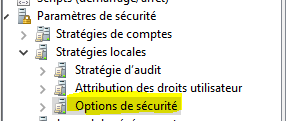
* Aller dans la modification de la GPO Sécurité de mots de passe
* Déplacé dans paramètre Windows
* Déplacé dans paramètre de sécurité
* Déplacé vers Stratégie de compte
* Déplacé vers Stratégie de mot de passe
* Modifié la règle Durée de vie maximale du mot de passe
* 60 jours.

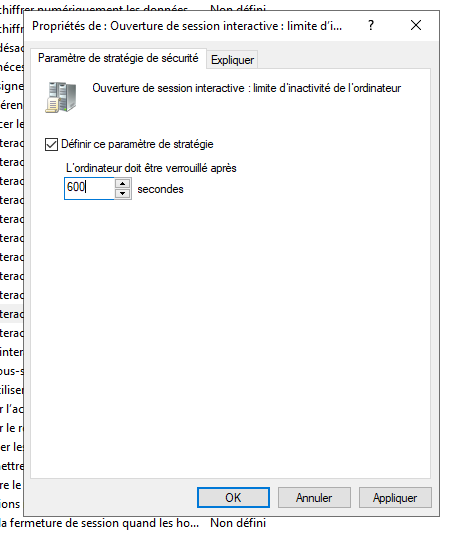


# Partie 2 :

## 5- Verrouillage de session : La session utilisateur doit se verrouiller automatiquement après 10 minutes d’inactivité et exiger un mot de passe pour se reconnecter. /2

* Aller dans la modification de la GPO Sécurité de mots de passe
* Déplacé dans paramètre Windows
* Déplacé dans paramètre de sécurité
* Déplacer vers Stratégie locale
* Déplacer vers Options de sécurité
* Modifié la stratégie limite d’inactivité de l’ordinateur.

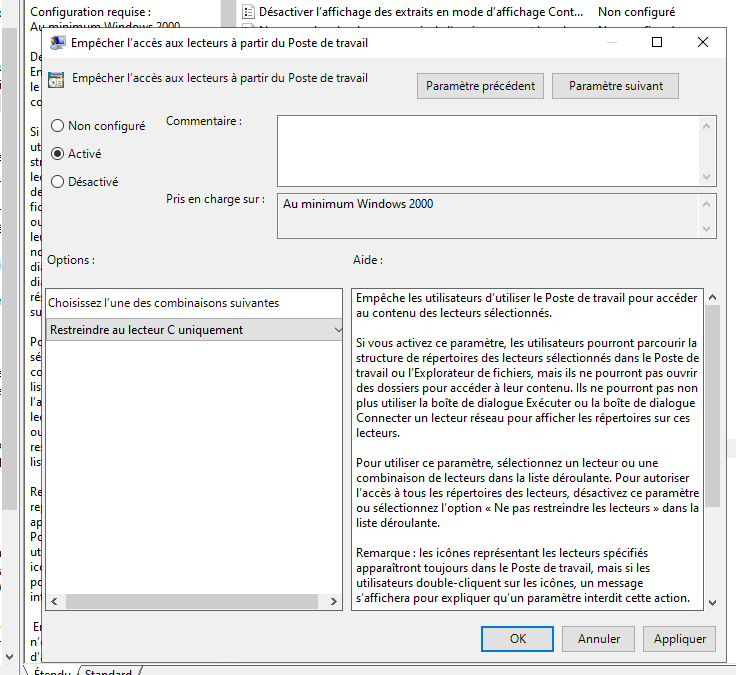


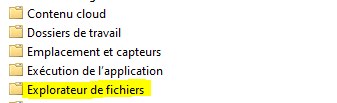


# 6- Question bonus : Restriction d'accès aux lecteurs : Empêchez l’accès au lecteur C: sauf à l’accès à C:\Users afin que les utilisateurs ne puissent pas explorer le disque local de leur machine. /1

**Partie 1:**

* Création d’une nouvelle GPO
* Aller dans la modification de la GPO
* Déplacer vers configuration utilisateur
* Déplacer vers Stratégie
* Déplacer vers modèle d’administration
* Déplacer vers composant Windows
* Déplacer vers explorateur de fichier
* Modifier le paramètre Empêcher l’accès aux lecteurs à partir du poste de travail.
* Activer et choisir Restreindre au lecteur C uniquement.



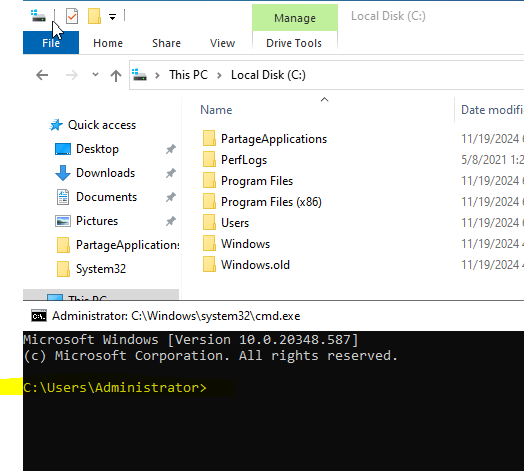
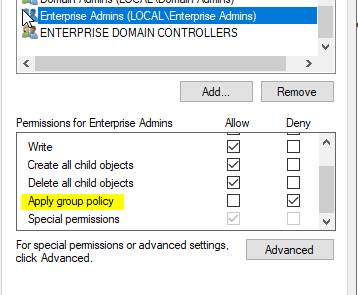




**Partie 2: Enlever les admins de cette GPO**

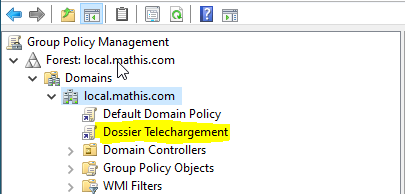
* Aller dans l’onglet délégation de la GPO
* Déplacer dans advanced
* Cocher deny apply group policy pour Domain Admins et Entreprise Admins

## 

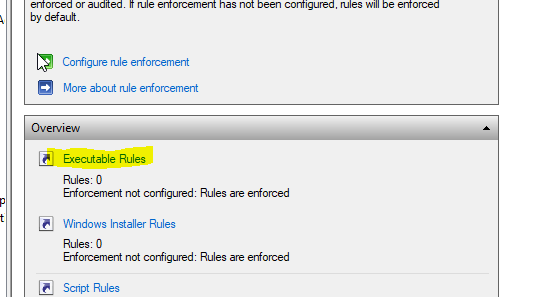


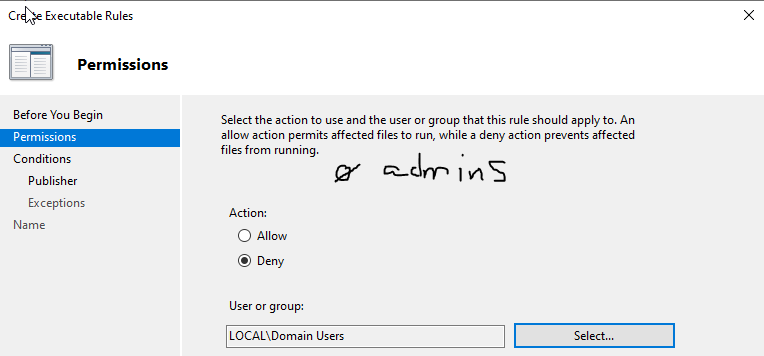
## 7-Restrictions sur les logiciels : Mettez en place des restrictions empêchant l'exécution de fichiers exécutables non autorisés, notamment ceux situés dans les répertoires de téléchargement. Seuls les logiciels des répertoires Program Files et Windows doivent être autorisés. /5

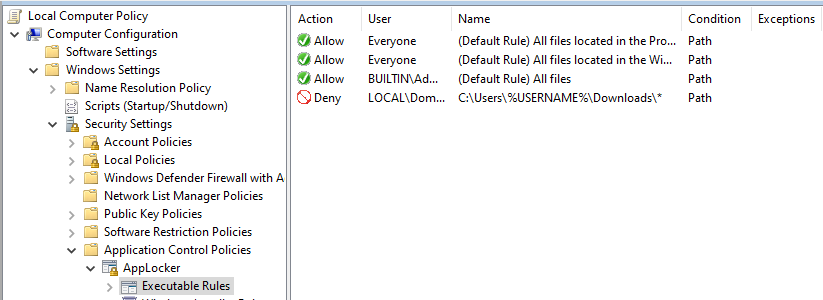
* Crée une nouvelle GPO
* Aller dans gpedit.msc.
* Naviguer vers Configuration de l’ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies de contrôle des applications > AppLocker.
* Activer le service Application Identity via services.msc.
* Dans Executable Rules, cliquer sur Create Default Rules.
* Ajouter une règle Deny pour le chemin C:\Users\%USERNAME%\Downloads\\*.
* Appliquer la règle au groupe Domain Users.
* Activer l’enforcement des règles via Configure Rule Enforcement.
* Tester en exécutant des fichiers dans Téléchargements (bloqué) et dans Program Files/Windows (autorisé).
* Vérifier les résultats dans l’Observateur d’événements (AppLocker).





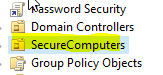


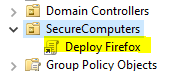


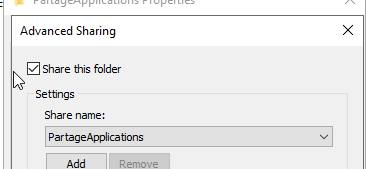


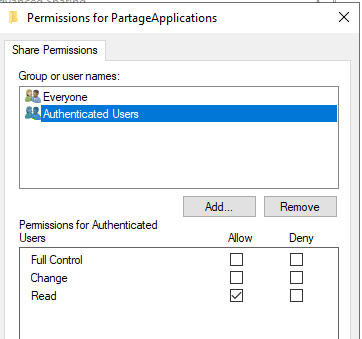
## 8-Déploiement d'une application : Déployez une application de votre choix sur les ordinateurs du domaine via une GPO. Choisissez une application, créez un package d'installation et configurez la GPO pour automatiser son déploiement sur les machines de l'OU "**SecureComputers**" seulement. /

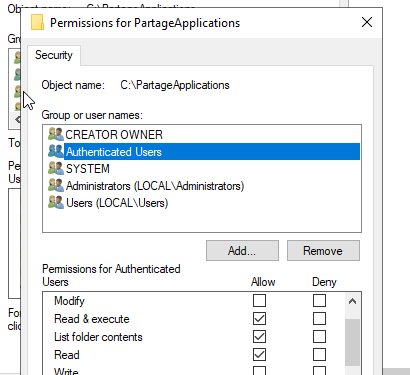
* Création d’une nouvelle OU
* Création d’une nouvelle GPO dans la nouvelle OU
* Télécharger un fichier MSI
* Créer un nouveau fichier de partage dans C:
* Aller dans propriété de ce fichier
* Déplacer dans Sharing
* Aller dans Advanced Sharing
* Cocher Share this folder
* Aller dans permissions et ajouter Authentificated users et cocher allow read
* Déplacer dans l’onglet Security du fichier
* Ajouter Authentificated users et cocher allow read & execute
* Ajouter le fichier MSI dans ce fichier
* Déplacer dans Computer Configuration
* Déplacer dans Policies
* Déplacer dans Software Settings
* Déplacer dans Software installation
* Crée un nouveau Package et mettre le fichier MSI qui est dans le fichier de partage.

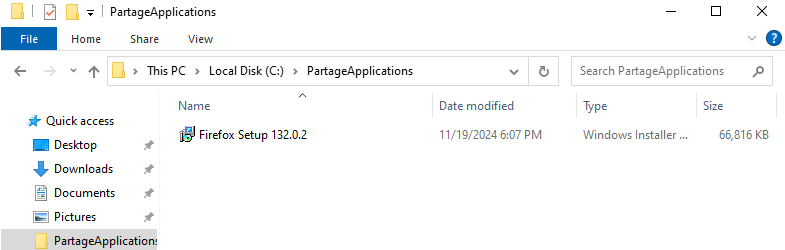


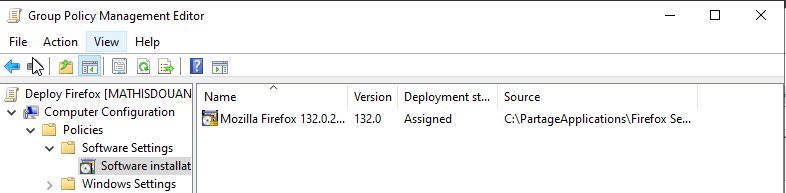






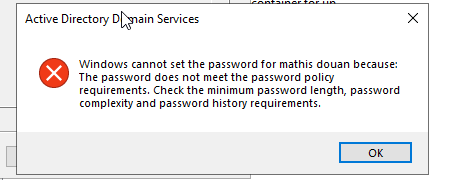




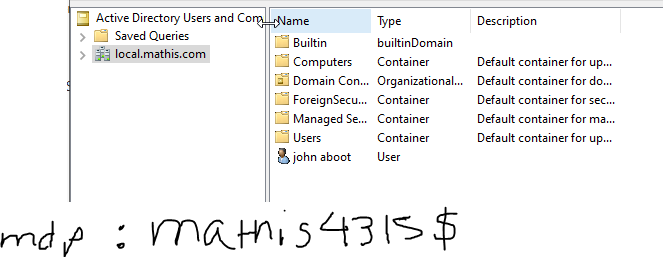


# Vérification:

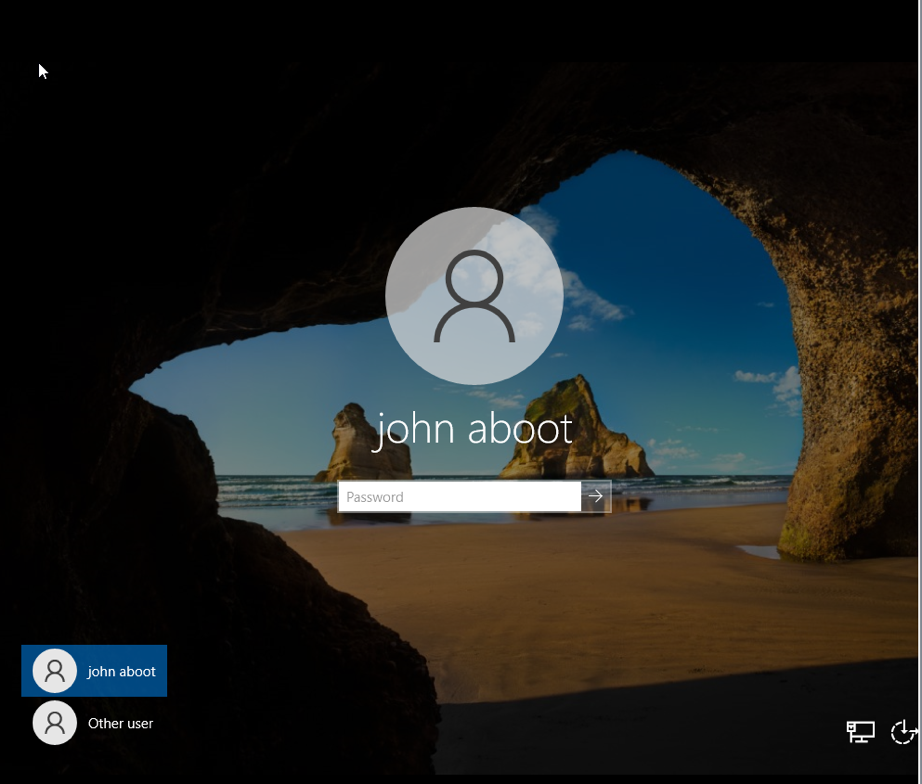
1. Vérification de la longueur du mot de passe et des politiques de complexité :
   1. Créez un nouvel utilisateur dans Active Directory et essayez de définir un mot de passe ne répondant pas aux exigences (par exemple, moins de 10 caractères ou sans caractères spéciaux). /2



* + Essayez ensuite de définir un mot de passe qui respecte les règles et vérifiez si cela fonctionne. /2



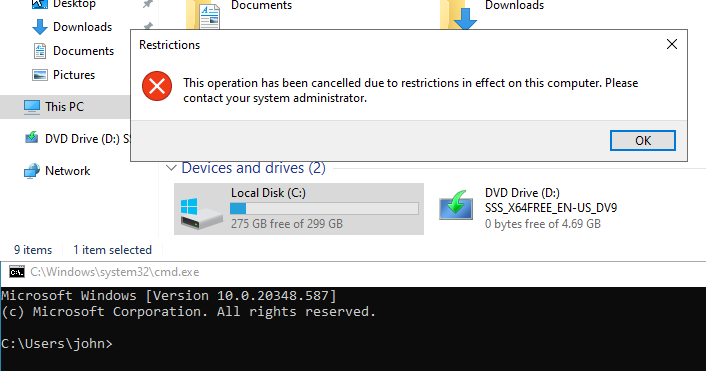
1. Vérification de la politique de verrouillage de session :
   * Sur un poste de travail, connectez-vous en tant qu'utilisateur du domaine et laissez la session inactive pendant 10 minutes. /2



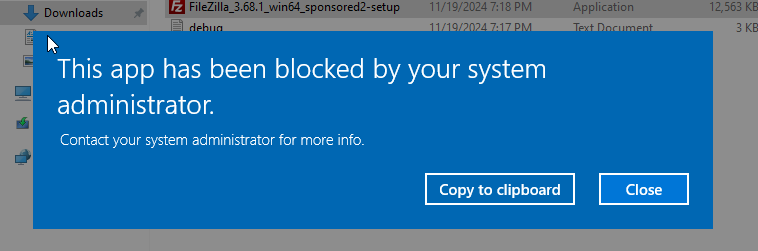
* + Vérifiez si la session se verrouille automatiquement et si un mot de passe est requis pour se reconnecter. /2

Après 10 minutes (600 secondes) sa me ramène à l’écran du début en me demandant mon mot de passe

1. Bonus : Vérification de la restriction d'accès au lecteur C: /1
   * Sur un poste de travail, essayez d'accéder au disque local (C:) via l'Explorateur de fichiers.



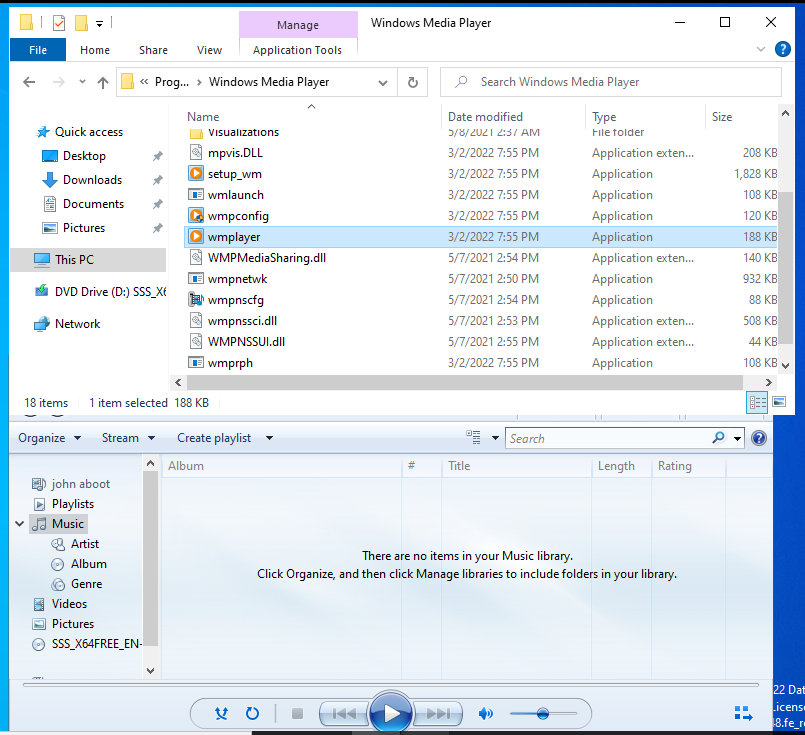
1. Vérification des restrictions sur les logiciels :
   * Téléchargez un fichier exécutable dans le répertoire de téléchargement d’un poste de travail et tentez de l’exécuter. /2



* + Vérifiez que le fichier ne peut pas être exécuté. /2

Comme démontré dans la photo, le fichier FileZilla ne peut pas être exécuté

* + Essayez d’exécuter une application dans le répertoire Program Files et assurez-vous que cela fonctionne. /2



1. Vérification du déploiement de l'application :
   * Connectez-vous à une machine dans l’OU "SecureComputers" et vérifiez que l'application déployée via la GPO est bien installée automatiquement. /2

Comme démontré dans la photo ci-dessous, l’applicaton Firefox est bien installé et s’exécute bien sur l’utilisateur John comme démontré dans CMD

* + Lancez l'application pour vérifier son bon fonctionnement. /2

