

# COMMENT

les entreprises peuvent remplacer Remote Credential Guard avec la gestion des accès privilégiés de Devolutions Server afin de sécuriser les identifiants de RDP.

Autrefois, l'un des seuls moyens d'éviter les fuites de mémoire des identifiants dans le protocole remote desktop (RDP) sur un serveur distant était la fonctionnalité nommée Remote Credential Guard (RCG). Bien qu'elle soit puissante, il y a plusieurs limitations qui rendent l'implantation et l'utilisation de RCG difficile pour certaines organisations.

La combinaison de Devolutions Server et du module de gestion des accès privilégiés (PAM) représente une alternative puissante et polyvalente. Que se passerait-il si chaque session RDP utilisait un mot de passe à usage unique qui était réinitialisé au bout d'un certain temps?

Même si les identifiants étaient extraits de la mémoire, ils seraient rapidement inutilisables par la suite!



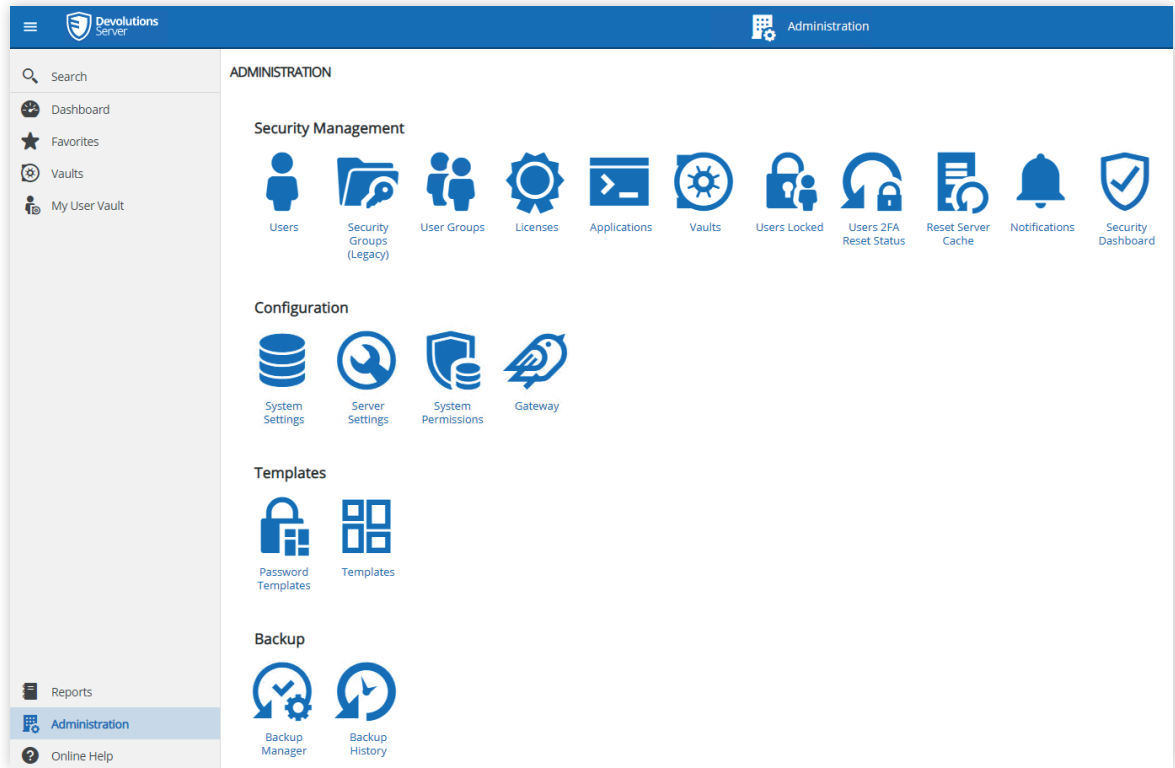
*Depuis la version 2021.2.13.0, le module de la gestion des accès privilégiés (PAM) a une licence distincte. Si vous ne voyez pas l'icône sous **Administration** → Paramètres du **serveur**, vous devrez demander ou acheter la licence.*

*De plus, une fois la licence ajoutée sous **Administration** → **Licences**, vous devrez actualiser la page du navigateur pour que l'élément du menu s'affiche.*

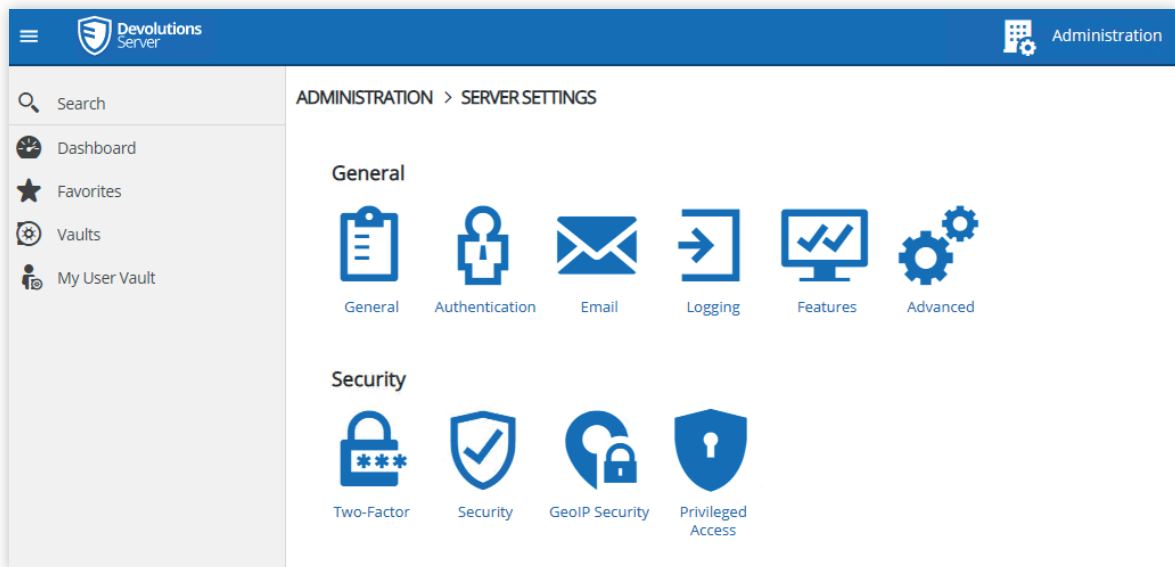
## Activation de la gestion des accès privilégiés (PAM) de Devolutions Server

Avant d'utiliser le PAM de Devolutions Server, le module doit d'abord être activé et les comptes importés et configurés.

1. Connectez-vous à l'interface Web de **Devolutions Server** et naviguez jusqu'à **Administration** → **Paramètres du serveur**.




2. Une fois dans les **Paramètres du serveur**, naviguez jusqu'à **Accès privilégiés**.



3 - Comment les entreprises peuvent remplacer Remote Credential Guard avec la gestion des accès privilégiés de Devolutions Server afin de sécuriser les identifiants de RDP.


3. Une fois dans la page des paramètres **d'accès privilégiés**, cochez l'option **Activer PAM**, mais laissez toutes les autres valeurs par défaut. Une fois configuré, cliquez sur le bouton **Enregistrer** (icône de disquette) dans le coin supérieur droit.


ADMINISTRATION > SERVER SETTINGS > PRIVILEGED ACCESS 


GENERAL


Enable PAM


CHECK OUT



Default approval mode  
None 

Users can approve their own Checkout requests  
Yes 

Include administrators when listing approvers  
Yes 



Include PAM managers when listing approvers  
Yes 

Default reason mode  
None 


Default Checkout time (minutes)  
240  

---

SYNCHRONIZATION

Check synchronization status every (minutes)  
360  

[Privileged Access Management System Permissions Page](#)

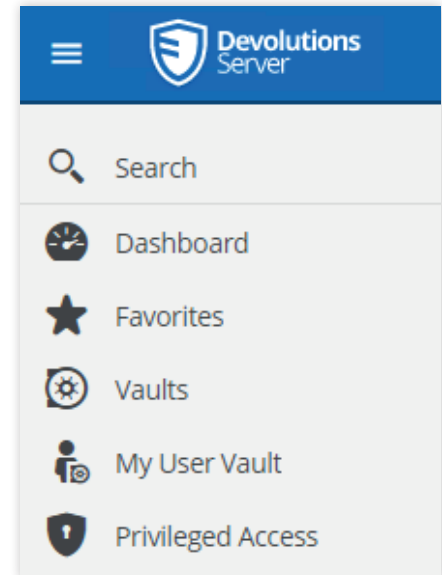
ADMINISTRATION > SERVER SET 

Saved Successfully  
The data has been successfully saved.

GENERAL

Enable PAM

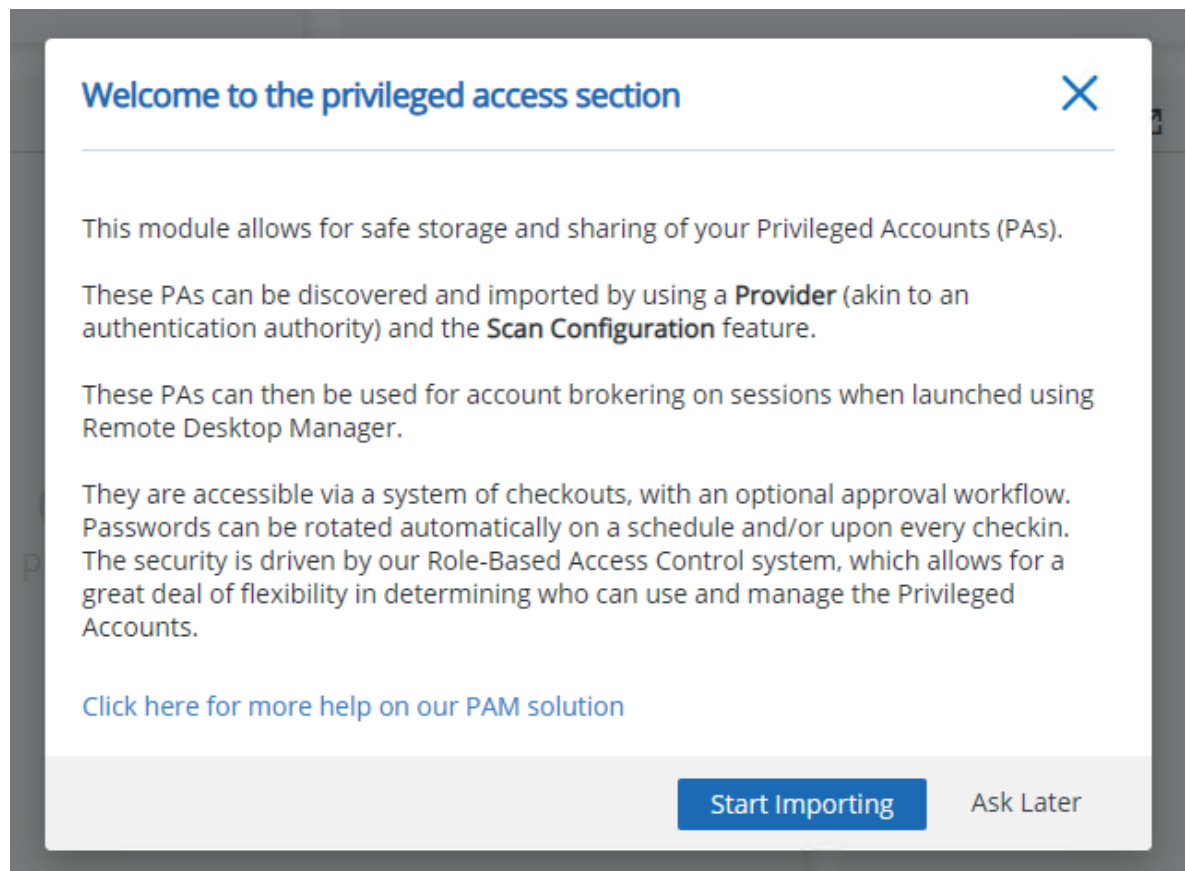
4. Après l'enregistrement, vous verrez un nouvel élément de menu pour **les accès privilégiés**. Cliquez sur le lien de l'élément du menu **Accès Privilégiés**.



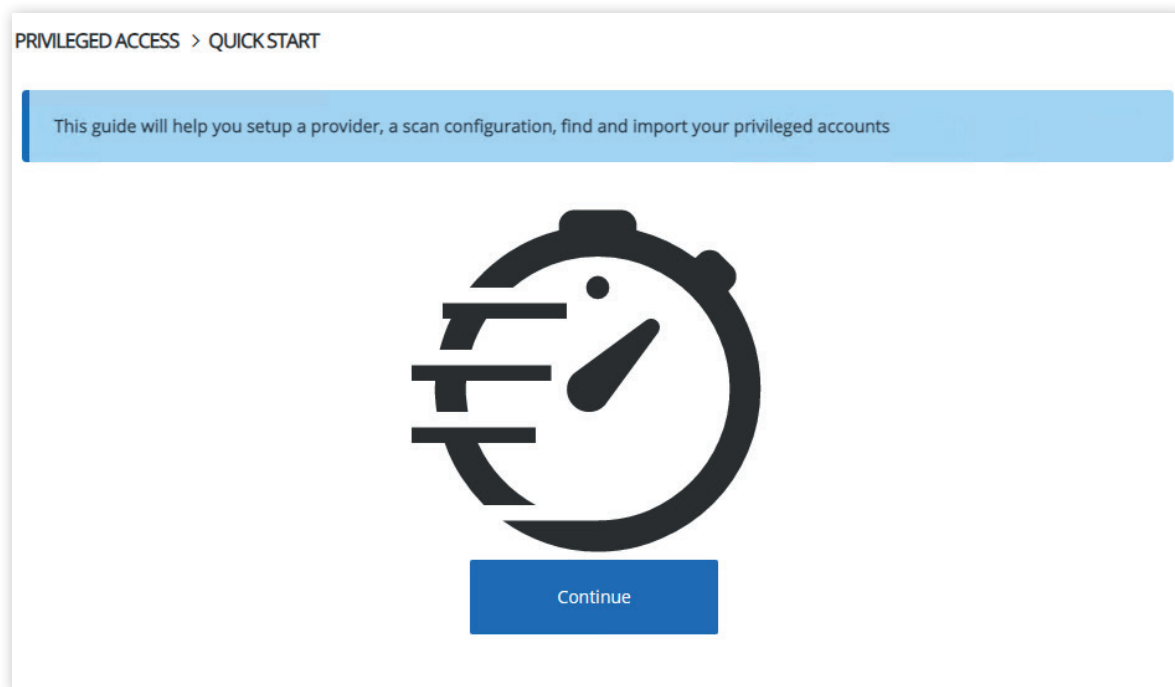
5. La première fois que vous accédez au PAM, une fenêtre de bienvenue apparaît. Comme vous devez importer des utilisateurs pour gérer leurs mots de passe, allez-y et cliquez sur le bouton **Commencer l'importation**.



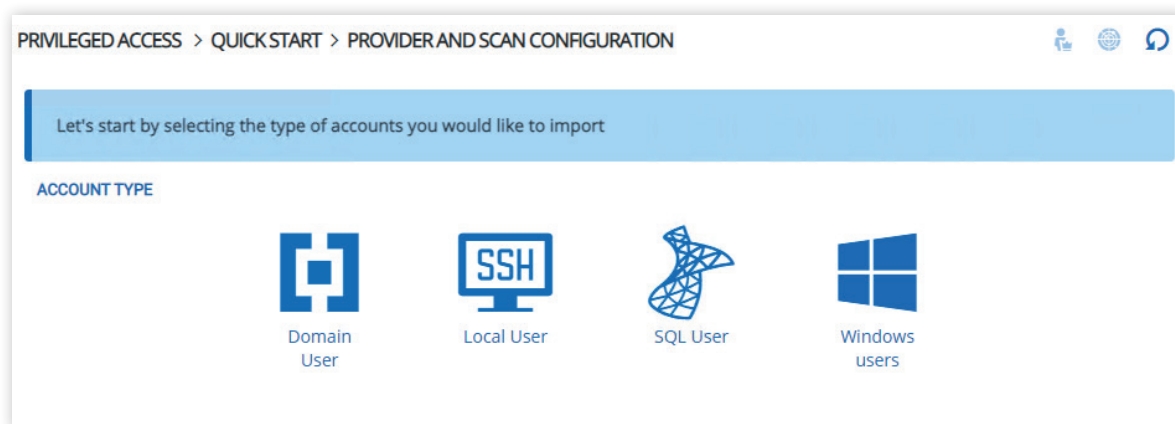
*Vous pouvez toujours redémarrer ce processus en cliquant sur le lien du menu Démarrage rapide de la page d'accueil du PAM.*



6. Cliquez sur **Continuer** dans le **Guide de démarrage rapide**



7. Dans ce tutoriel, vous allez importer des comptes d'utilisateurs de domaine Active Directory (AD). Cliquez sur le bouton **Utilisateur du domaine**.



8. Ensuite, vous devez entrer la **configuration du répertoire** et du **scan**. Il est préférable d'utiliser LDAPS et un compte de service AD avec les droits adéquats, comme indiqué ci-dessous. Cliquez sur **Parcourir les conteneurs du domaine** et choisissez le conteneur (unité organisationnelle ou OU) avec les comptes à importer. Ici, l'OU sélectionnée est OU=Service Accounts,DC=domain,DC=local.



*Pour limiter les autorisations du compte de service, définissez-le de manière qu'il ait juste assez de droits pour [accéder aux objets AD et réinitialiser les mots de passe](#).*

PRIVILEGED ACCESS > QUICK START > PROVIDER AND SCAN CONFIGURATION

Now, let's enter the information to start a connection. The credentials will be used for the provider to scan and manage the imported accounts

**DOMAIN**

Domain name  
domain.local

Protocol  
LDAPS

Port  
636

**CREDENTIALS**

Username  
ad-passwdrotate-svc

Password  
.....

Test Connection

**SCAN CONFIGURATION**

Domain container  
OU=Service Accounts,DC=domain,DC=local

Browse domain containers

Scan



9. Cliquez sur le bouton **Tester la connexion** pour vérifier que votre connexion est valide avec les identifiants fournis.

PRIVILEGED ACCESS > QUICK START > PROVIDER AND SCAN CONFIGURATION

Connection successful

Now, let's enter the information to start a connection. The credentials will be used for the provider to scan and manage the imported accounts

**DOMAIN**

Domain name

Protocol •  Port

**CREDENTIALS**

Username •

Password

10. Cliquez sur **Scan** et sur la page suivante, cochez la case à côté des comptes à importer dans le PAM.

PRIVILEGED ACCESS > QUICK START > PROVIDER AND SCAN CONFIGURATION > IMPORT ACCOUNTS

5 account(s) were found. 0 account(s) are already imported.

Container  Filter

	↑↓ User Principal Name	NetBios Name	↑↓ SAM Account Name	First Name	↑↓ Last Name	↑↓ Email	↑↓ Container
<input checked="" type="checkbox"/>	service-acct-1...	DOMAIN\serv...	service-acct-1				OU=Service A...
<input checked="" type="checkbox"/>	service-acct-2...	DOMAIN\serv...	service-acct-2				OU=Service A...
<input type="checkbox"/>	ad-fullaccess-...	DOMAIN\ad-f...	ad-fullaccess-...				OU=Service A...
<input type="checkbox"/>	ad-passwdrot...	DOMAIN\ad-p...	ad-passwdrot...				OU=Service A...
<input type="checkbox"/>	ad-readonly-s...	DOMAIN\ad-r...	ad-readonly-svc	Read-Only	AD Service Ac...		OU=Service A...

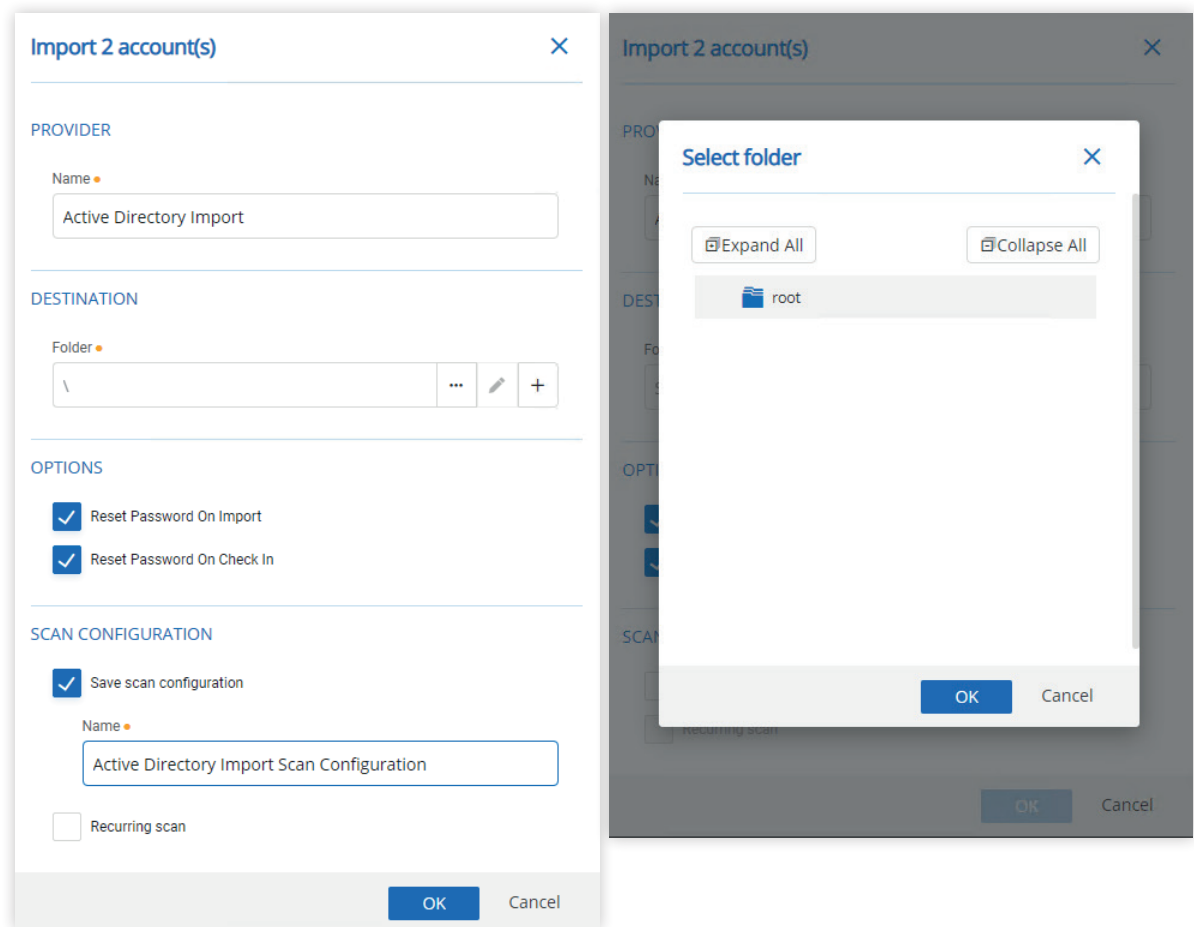
<< 1 >>



11. Cliquez sur l'icône **d'importation** en haut à droite (icône de fichier avec la flèche) et entrez un **Nom**. Ici, le répertoire est **Active Directory Import**. Ensuite, choisissez le dossier dans lequel importer les comptes, ici le dossier racine (/). Enfin, cliquez sur **Enregistrer** la configuration de scan et entrez un nom, ici **Active Directory Import Scan Configuration**, et cliquez sur **OK**.



*Ne laissez l'option Réinitialiser le mot de passe à l'importation cochée que si ces comptes de service ne seront pas touchés par le changement de mot de passe.*



12. Une fois que les ressources sont importées, vous verrez que l'importation a réussi : le guide de **démarrage rapide** est terminé.

PRIVILEGED ACCESS > QUICK START > PROVIDER AND SCAN CONFIGURATION

All users have been imported successfully

5 account(s) were found. 2 account(s) are already imported.

Container  Filter

	↑↓ User Principal Name	NetBios Name	↑↓ SAM Account Name	First Name	↑↓ Last Name	↑↓ Email	↑↓ Container
<input checked="" type="checkbox"/>	service-acct-1...	DOMAIN\serv...	service-acct-1				OU=Service A...
<input checked="" type="checkbox"/>	service-acct-2...	DOMAIN\serv...	service-acct-2				OU=Service A...
<input type="checkbox"/>	ad-fullaccess-...	DOMAIN\ad-f...	ad-fullaccess-...				OU=Service A...
<input type="checkbox"/>	ad-passwdrot...	DOMAIN\ad-p...	ad-passwdrot...				OU=Service A...
<input type="checkbox"/>	ad-readonly-s...	DOMAIN\ad-r...	ad-readonly-svc	Read-Only	AD Service Ac...		OU=Service A...

<< 1 >>

13. Pour conclure, cliquez sur le lien **Accès privilégiés** du menu de gauche et notez qu'il y a deux **Comptes**, un **Répertoire**, et une configuration de **Scan** disponibles. Cliquez sur **Comptes** pour vous assurer que les comptes sont utilisables. Deux comptes sont visibles, et s'ils ont été importés avec une réinitialisation du mot de passe, ils afficheront une bordure verte à gauche.


PRIVILEGED ACCESS

Accounts 2 Providers 1 Scan Configurations 1


Checkouts Pending (0) Active (0) Recurrent Scans

PRIVILEGED ACCESS > PRIVILEGED ACCOUNT MANAGEMENT

ACCOUNTS



service-acct-1  
Domain User



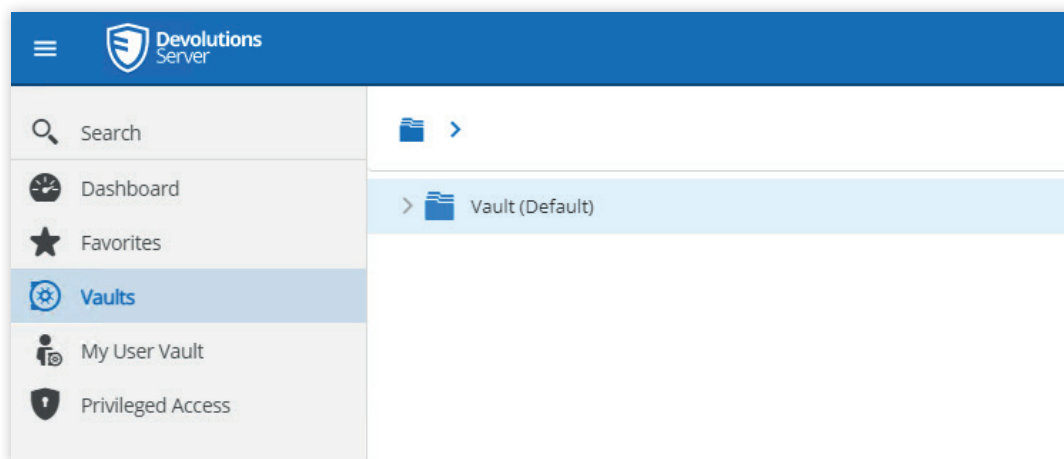
service-acct-2  
Domain User

10 - Comment les entreprises peuvent remplacer Remote Credential Guard avec la gestion des accès privilégiés de Devolutions Server afin de sécuriser les identifiants de RDP.

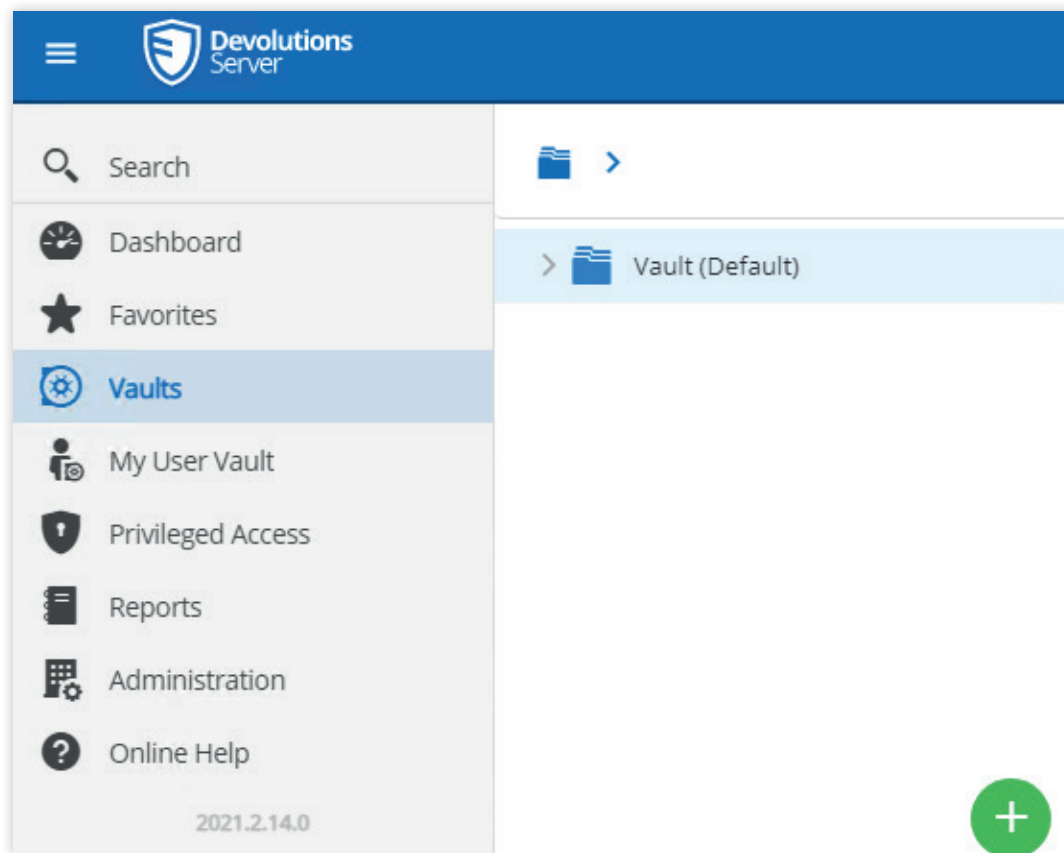
## Ajout d'un compte privilégié en tant qu'entrée dans un coffre

Afin d'intégrer le PAM à Remote Desktop Manager, une nouvelle entrée doit être ajoutée à un coffre, qui sera ensuite configurée pour être utilisée avec le PAM.

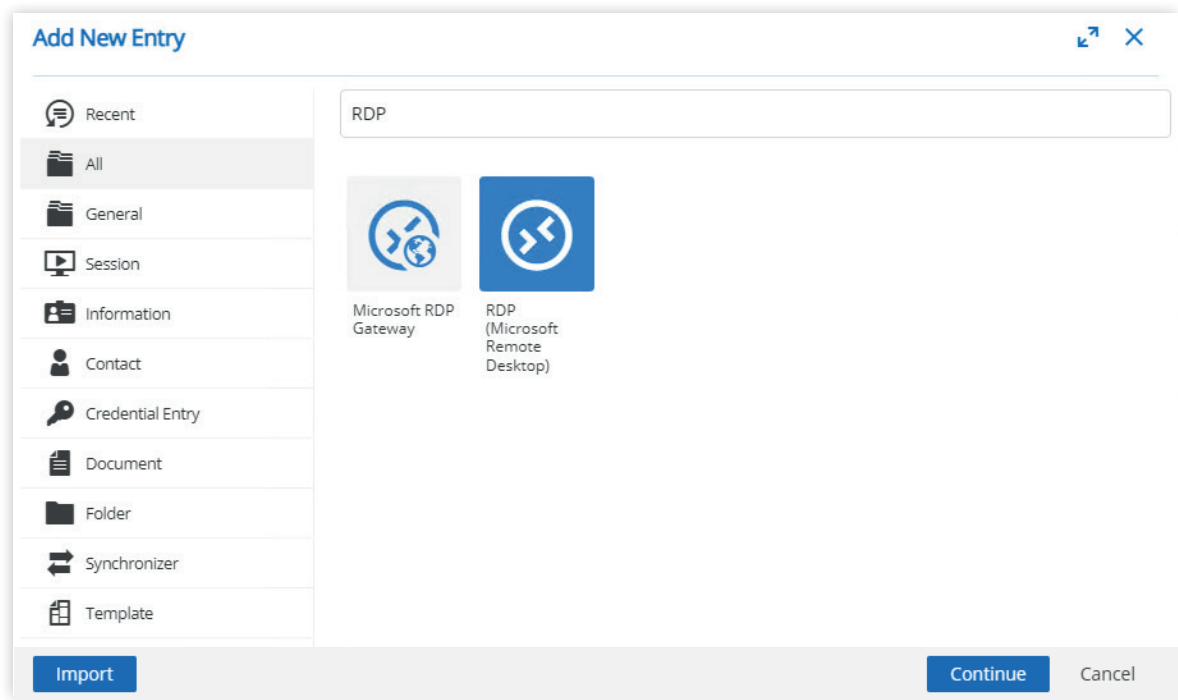
1. Allez dans l'élément de menu **Coffres** et ensuite dans un coffre. Ici, le **Coffre (par défaut)** est utilisé.



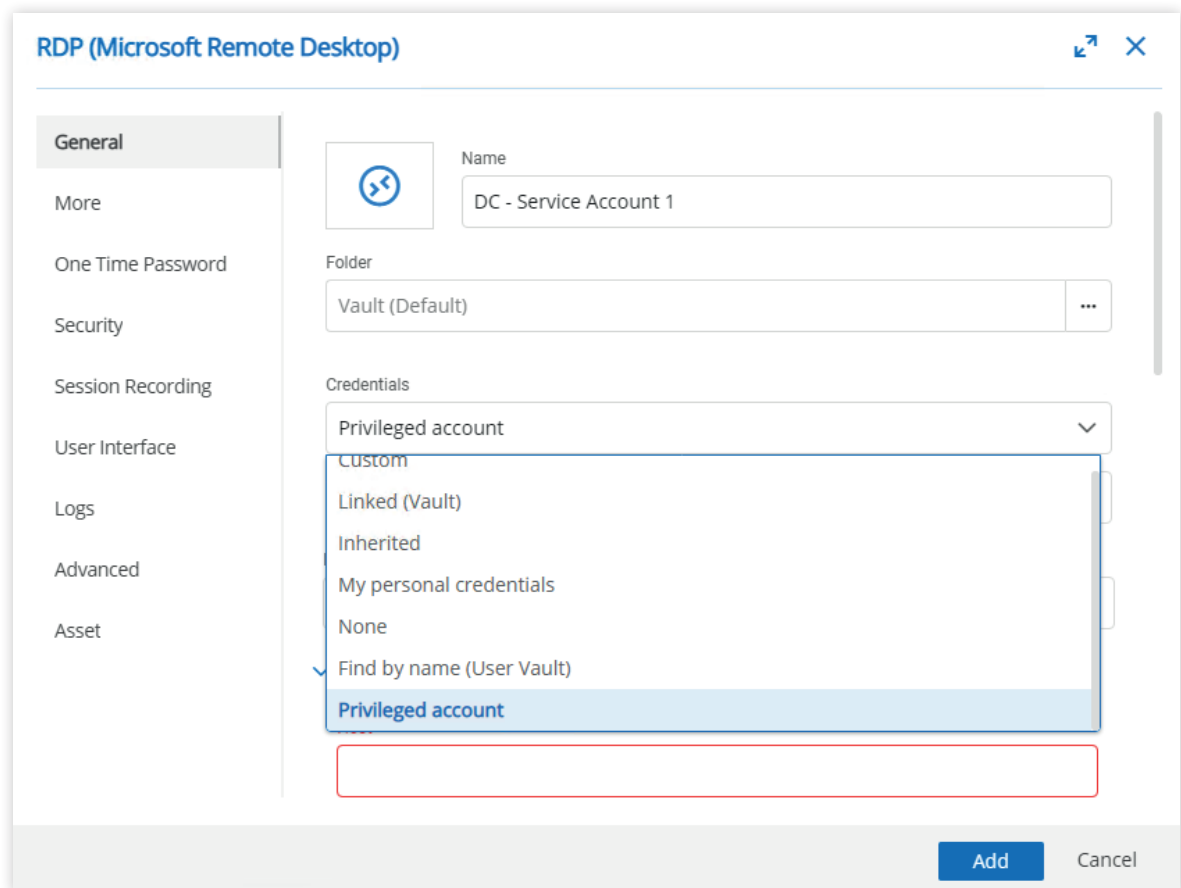
2. Cliquez sur l'icône verte en forme de cercle pour ajouter une nouvelle entrée au coffre sélectionné.

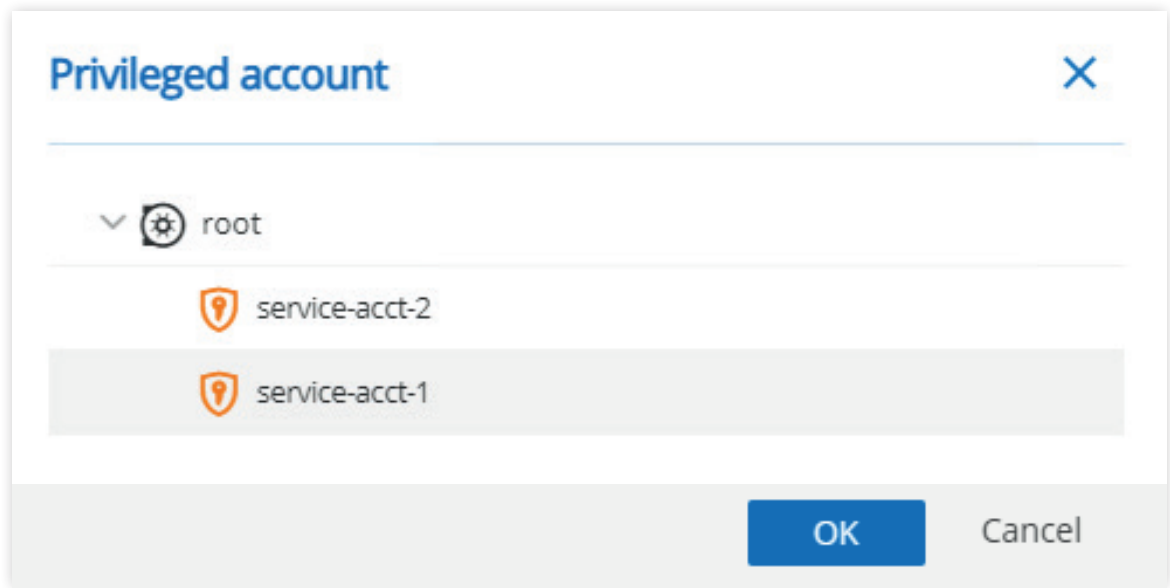


3. Sur la page **Ajouter une nouvelle entrée**, entrez RDP dans la barre de recherche pour filtrer les résultats sur **RDP (Microsoft Remote Desktop)**, sélectionnez l'icône, puis cliquez sur **Continuer**.

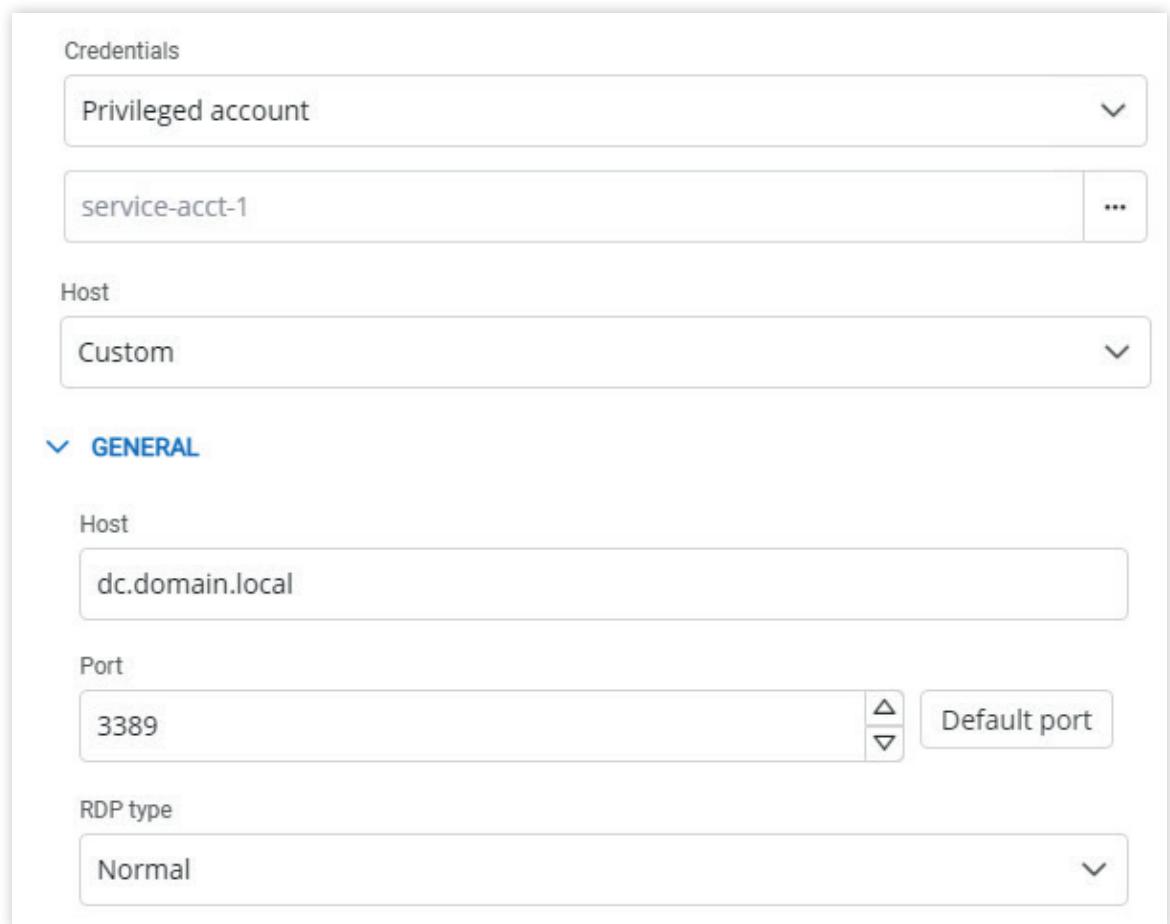


4. Saisissez un nom, ici l'entrée est nommée DC - Service Account 1, puis sélectionnez **Identifiants** → **Compte privilégié**. Sélectionnez le compte à ajouter, ici service-acct-1 est utilisé.





5. Ajouter les informations sur l'hôte. Ici, dc.domain.local est utilisé avec l'ensemble des valeurs par défaut et sans aucun nom **d'utilisateur** et **mot de passe** spécifiés. Ils seront obtenus au moment de la connexion à partir des identifiants du PAM.



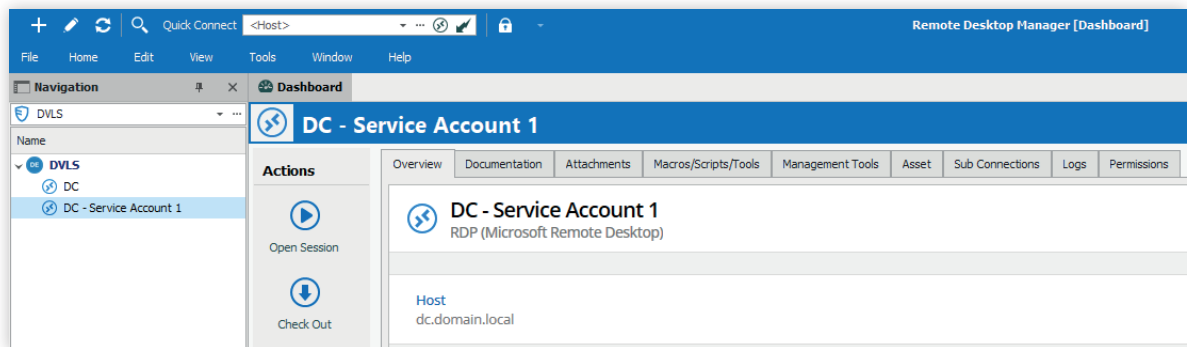
## Connexion à distance à partir de RDP avec un compte de compte de service géré par le PAM

Maintenant qu'une entrée a été configurée, vous êtes prêt à contrôler à distance un hôte avec une entrée RDP configurée par le PAM.

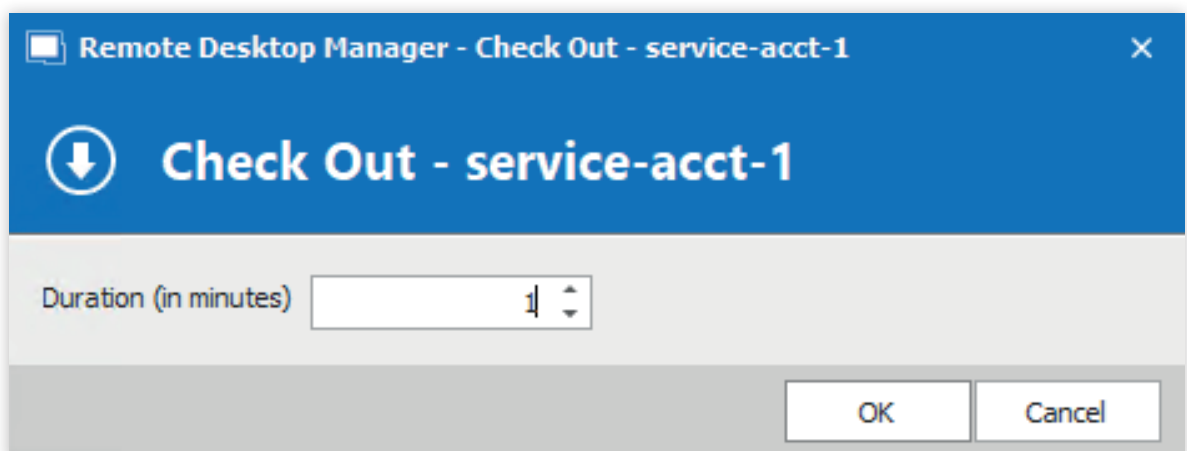
1. Lancez **Remote Desktop Manager** et accédez à l'entrée précédemment créée, ici nommée « DC - Service Account 1 ». Sélectionnez l'entrée et cliquez sur **Ouvrir la session**.



*Si un message d'autorisation refusée est affiché pour le compte privilégié, vérifiez que le compte accédant dispose des autorisations de lecture du compte privilégié lui-même.*



2. Vous êtes ensuite invité à indiquer une durée de réservation. Dans cet exemple, il s'agit d'une durée de 1 minute (par défaut 240 minutes). Cliquez sur **OK** pour continuer et une session de Bureau à distance s'ouvrira.



**3.** Une fois la session terminée, le mot de passe de l'identifiant restera actif pendant la durée spécifiée précédemment (1 minute dans ce tutoriel).

Après cette période, le mot de passe sera réinitialisé et l'ouverture d'une nouvelle session nécessitera une nouvelle réservation des identifiants. Vous trouverez ci-dessous les journaux du module PAM de Devolutions Server illustrant la rotation du mot de passe et les actions de Remote Desktop Manager.

service-acct-1 - Logs

User:  Action:  Date:   Include PamSystem

Folder	Action	User	Date
root	Password reset	PamSystem	12/17/2021 22:16
root	Checkout expired	PamSystem	12/17/2021 22:16
root	Password brokering	testaccount1@domain.local	12/17/2021 22:15
root	Checkout active	testaccount1@domain.local	12/17/2021 22:15
root	Checkout requested	testaccount1@domain.local	12/17/2021 22:15

Password History

Modified By	Modified on	Password
PamSystem	12/17/2021 22:16	●●●●●