HOW TO

Replace Remote Credential Guard with Devolutions Server PAM **to secure RDP credentials**

Devolutions

Traditionally, one of the only ways to avoid remote desktop protocol (RDP) credential memory leaks on a remote server was via the Remote Credential Guard (RCG) functionality. Although powerful, there are several limitations that make implementing and using RCG difficult for some organizations.

Devolutions Server with Privileged Access Management (PAM) functionality comes together to provide a powerful and flexible alternative. What if every RDP session utilized a one-time password that was reset upon timeout?

Even if credentials were extracted from memory, they would be useless quickly after!

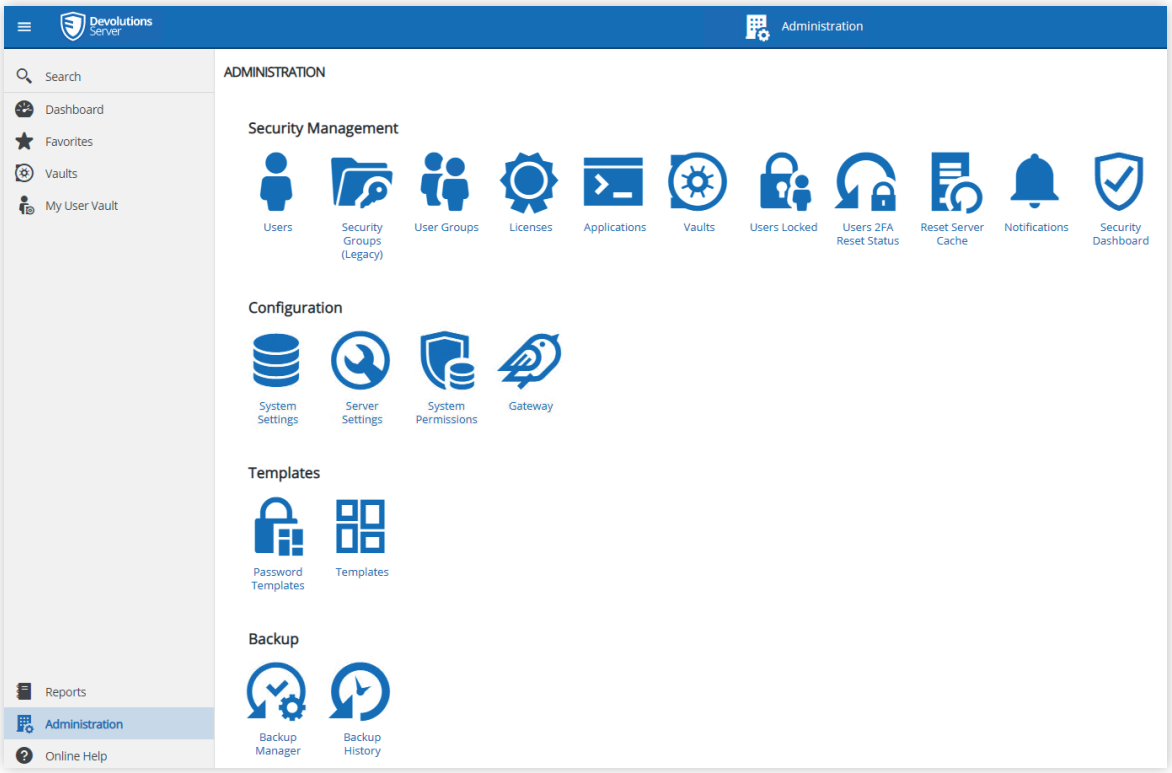
*As of version 2021.2.13.0, the Privileged Access Management (PAM) module is separately licensed. If you do not see the icon under **Administration → Server** settings, you will need to request or purchase the updated license.*

*In addition, once the license has been added under **Administration → Licenses**, you will need to refresh the browser page for the menu item to show up.*

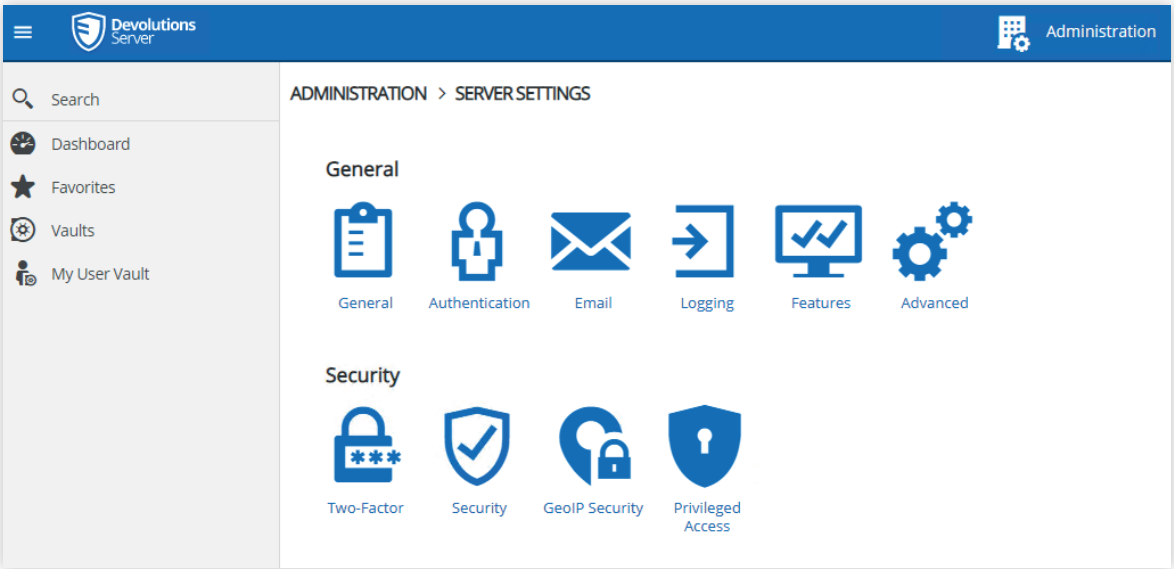
Enabling Devolutions Server PAM

Before using Devolutions Server PAM, the module must first be enabled and accounts imported and configured for use.

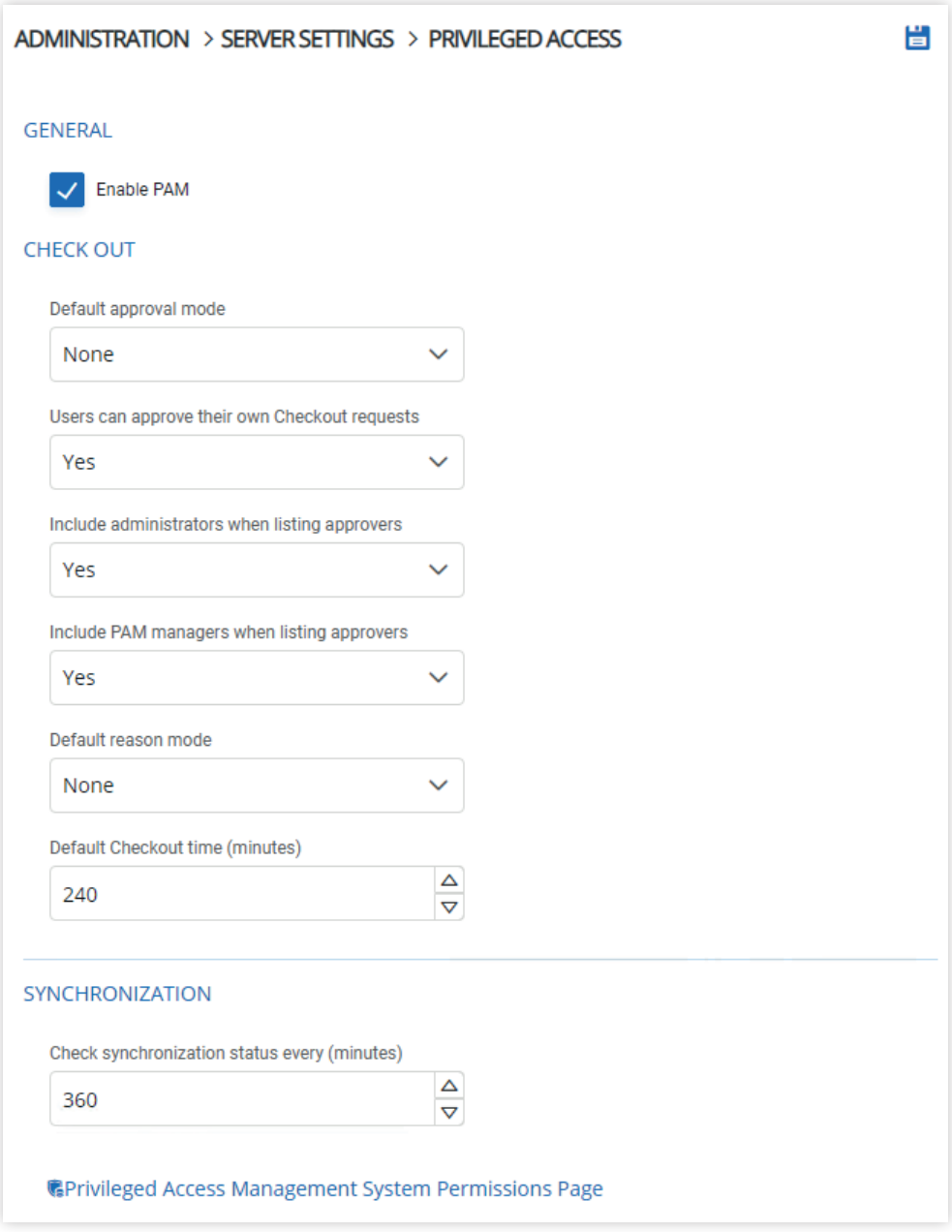
1. Log into the **Devolutions Server** web interface and navigate to **Administration → Server Settings.**

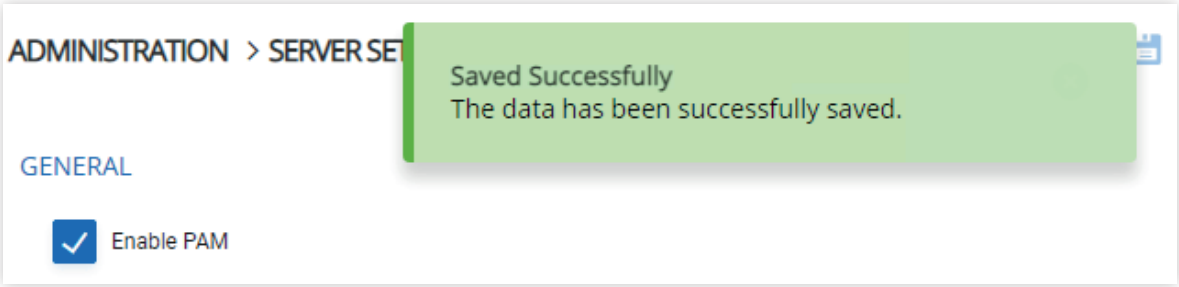


2. Once in **Server Settings** navigate to **Privileged Access**.

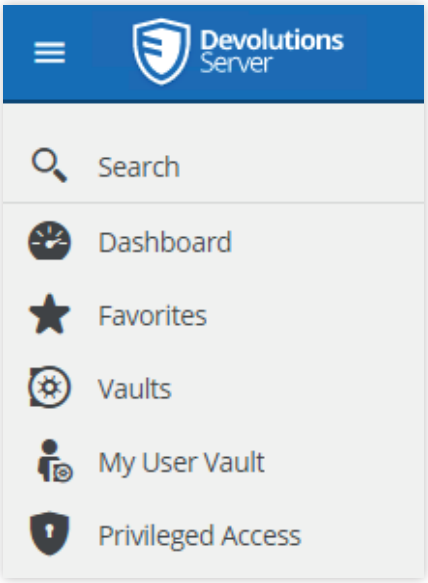


3. Once in the **Privileged Access** settings page, check the **Enable PAM** option, but leave all other values their defaults. Once configured, click the **Save** button (floppy disk icon) in the upper right corner.



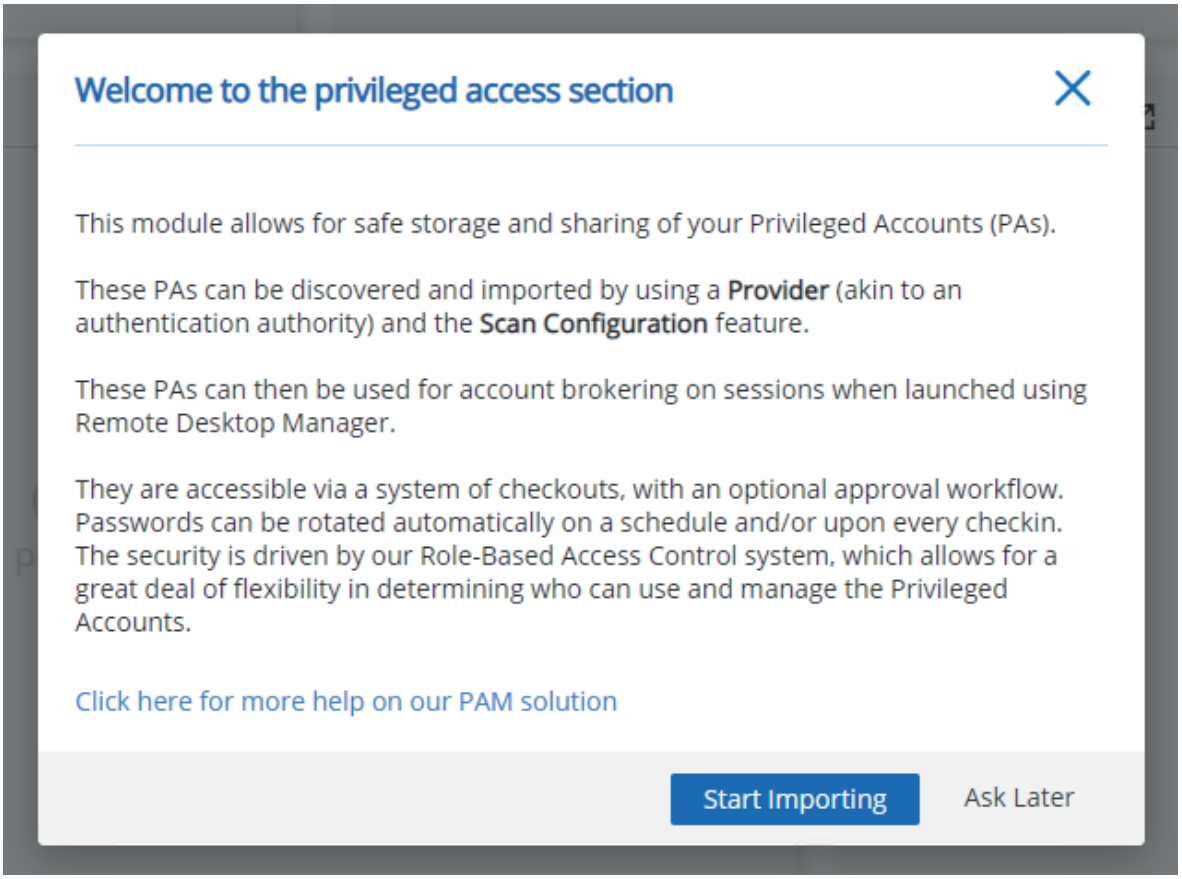


4. Upon saving, you will see a new menu item for **Privileged Access**. Click on the Privileged Access menu item link.

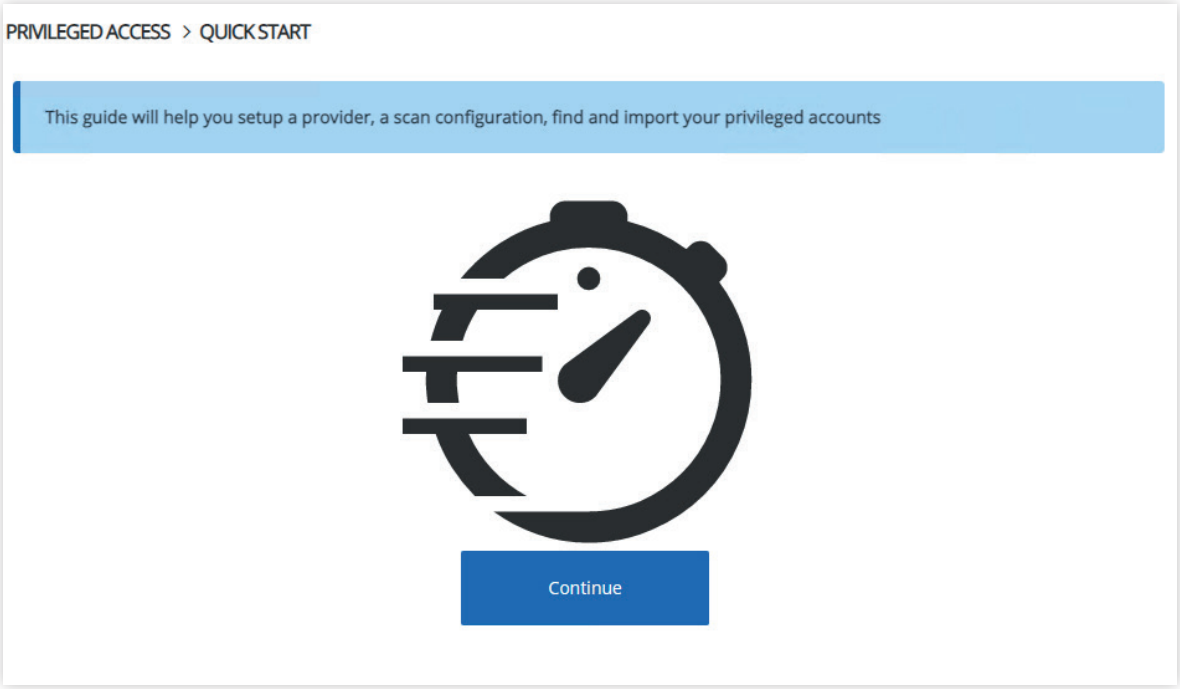


5. The first time that you access PAM you are presented with a welcome prompt. As you must import users to manage their passwords, go ahead and click the **Start Importing** button.

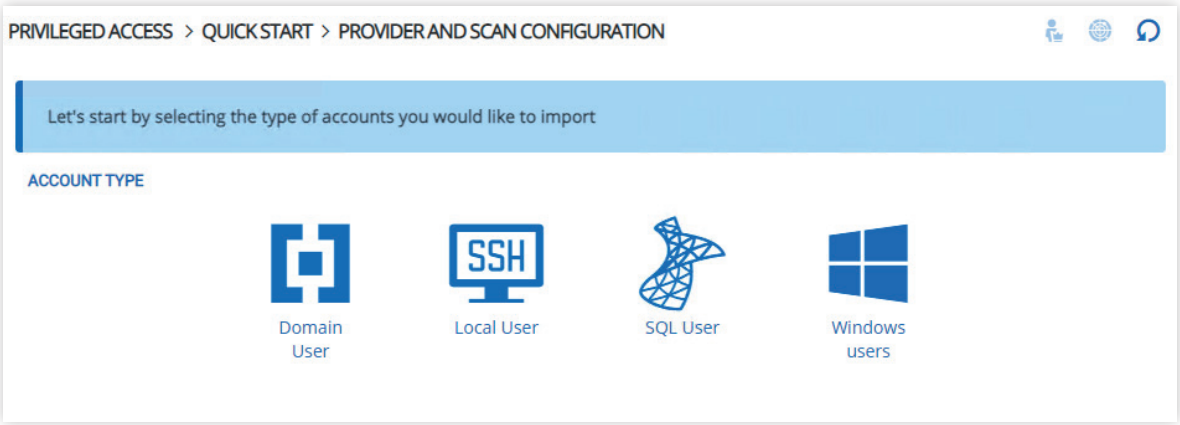
> *You can always restart this process by clicking on the start Quick Start menu link on the PAM homepage.*



6. Click **Continue** on the **Quick Start** guide.

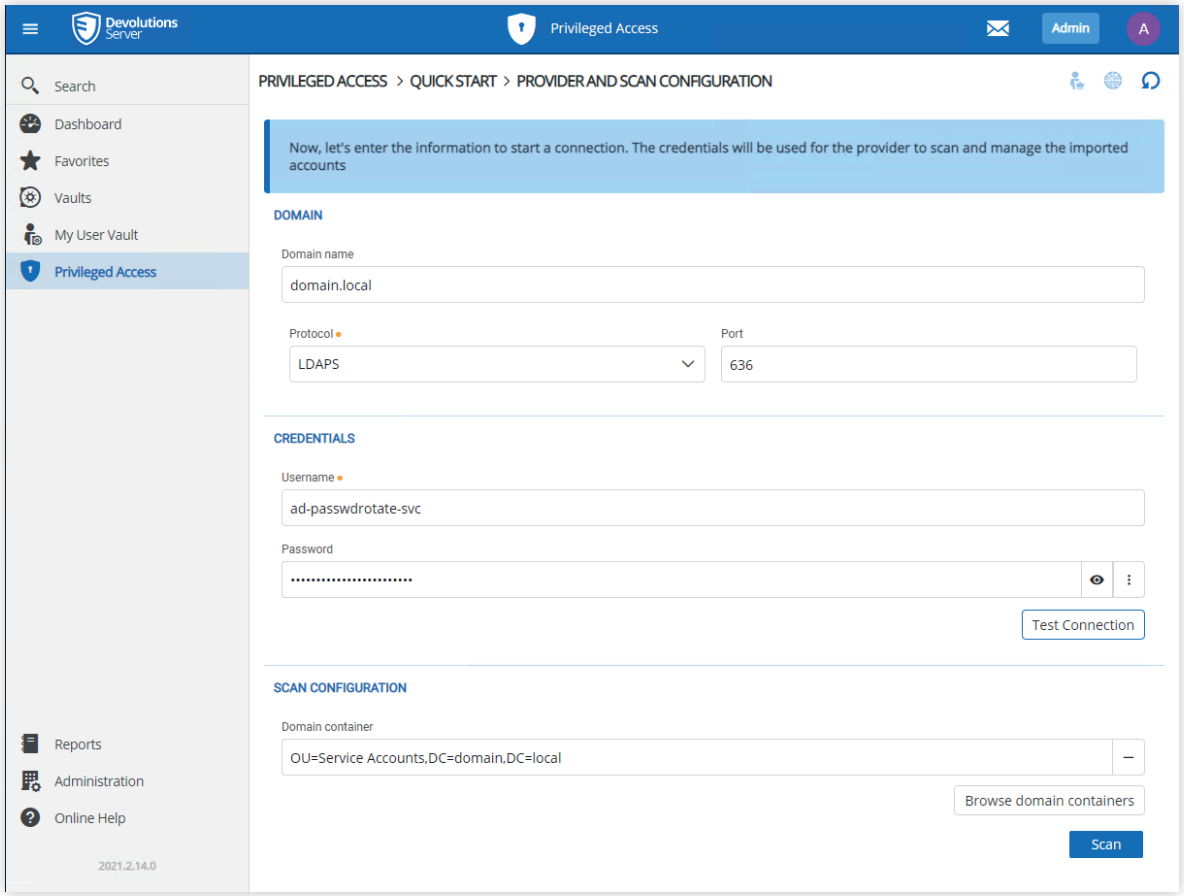


7. In this tutorial, you will be importing Active Directory (AD) Domain User accounts. Click on the **Domain User** button.

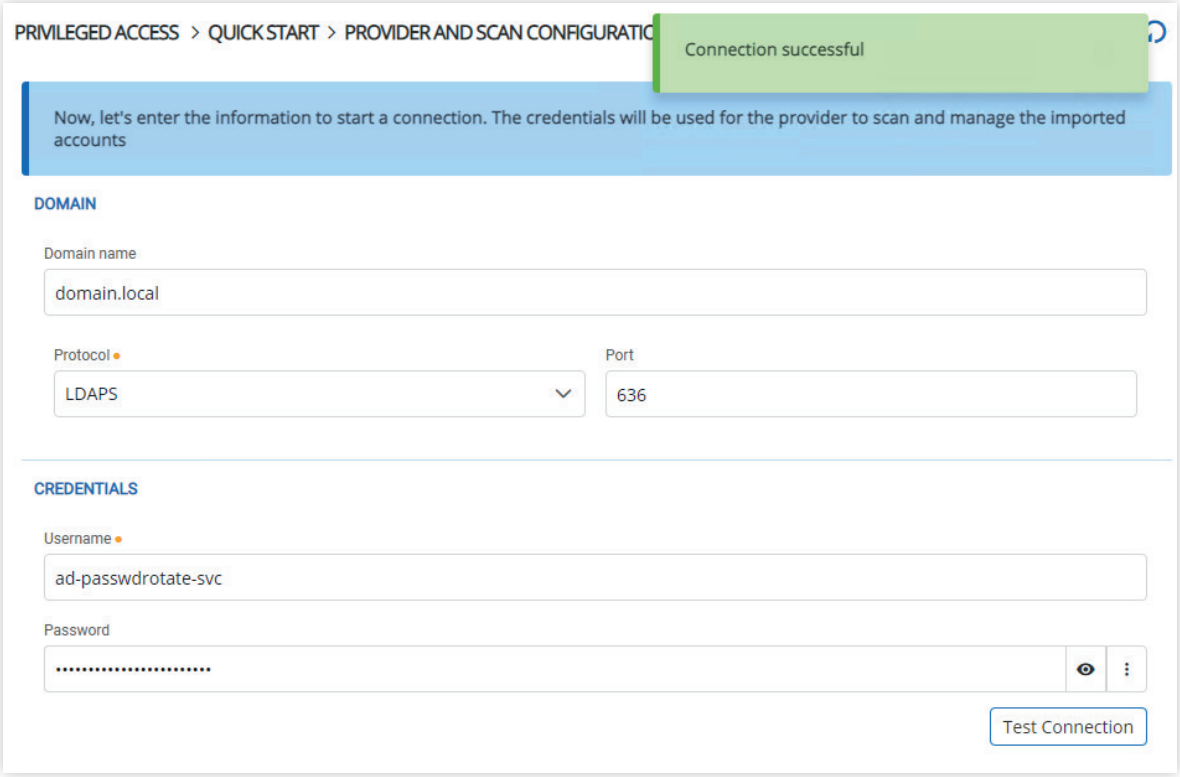


8. Next, you must enter the **Provider** and **Scan Configuration**. It is recommended to use LDAPS and an AD service account with the appropriate rights as shown below. Click **Browse domain containers** and choose the container (Organizational Unit or OU) with accounts to import. Here, the OU chosen is OU=Service Accounts,DC=domain,DC=local.

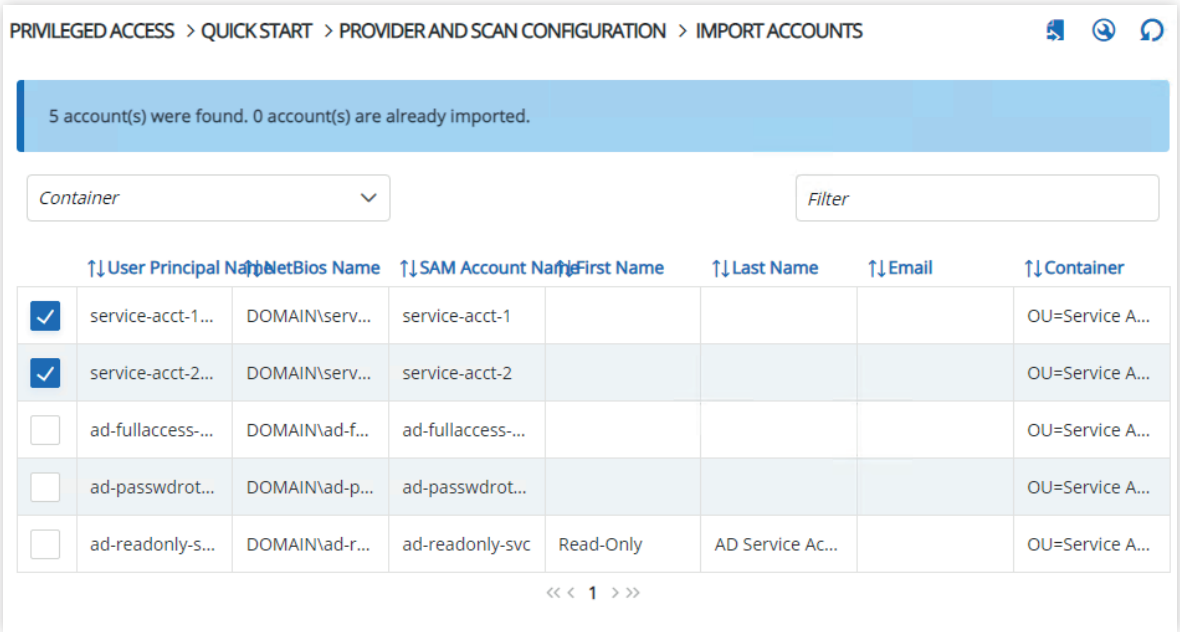
> *To limit permissions of the service account, set the service account to have just enough to access the AD objects and reset passwords.*



9. Click the **Test Connection** button to verify that your connection is valid with the provided credentials.

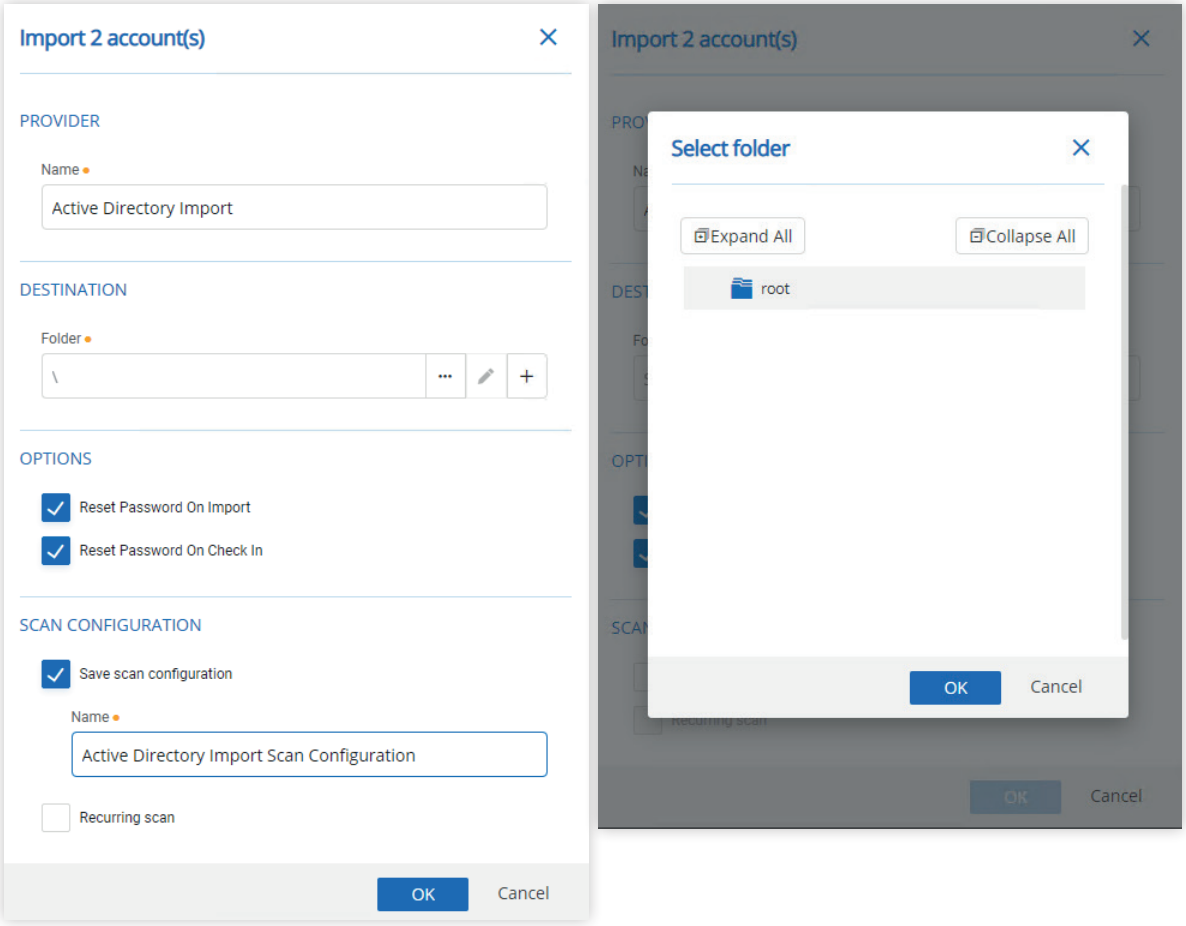


10. Click **Scan** and on the resulting page, select the checkbox next to the accounts to import into PAM.

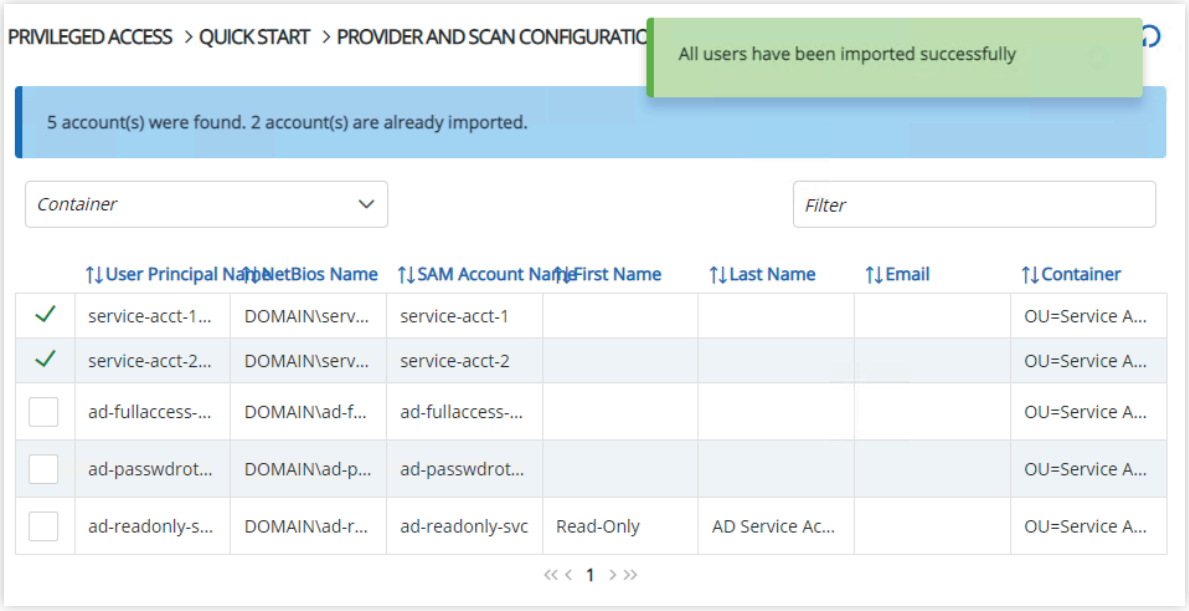


11. Click the **Import** icon in the upper-right (file icon with arrow) and enter a **Name**, here the provider is named **Active Directory Impor**t. Next, choose the folder to import the accounts into, here the root folder (/) is used. Finally, click on Save scan configuration and enter a name, here named **Active Directory Import Scan Configuration**, and click **OK**.

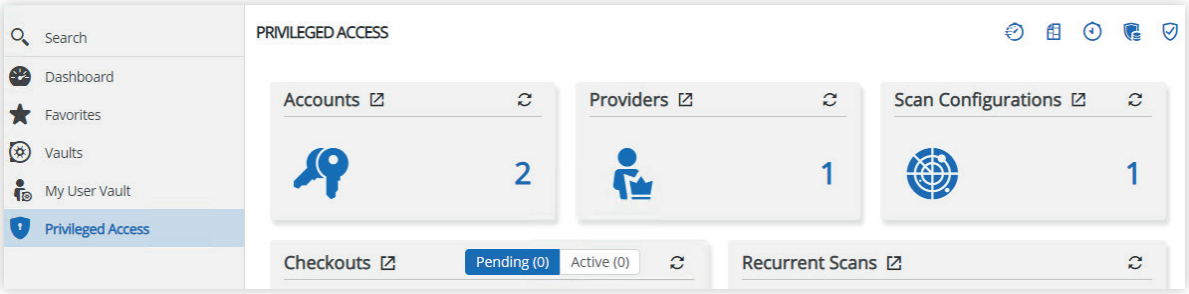
> *Only keep the Reset Password on Import option checked if these service accounts will not be affected by the password change.*

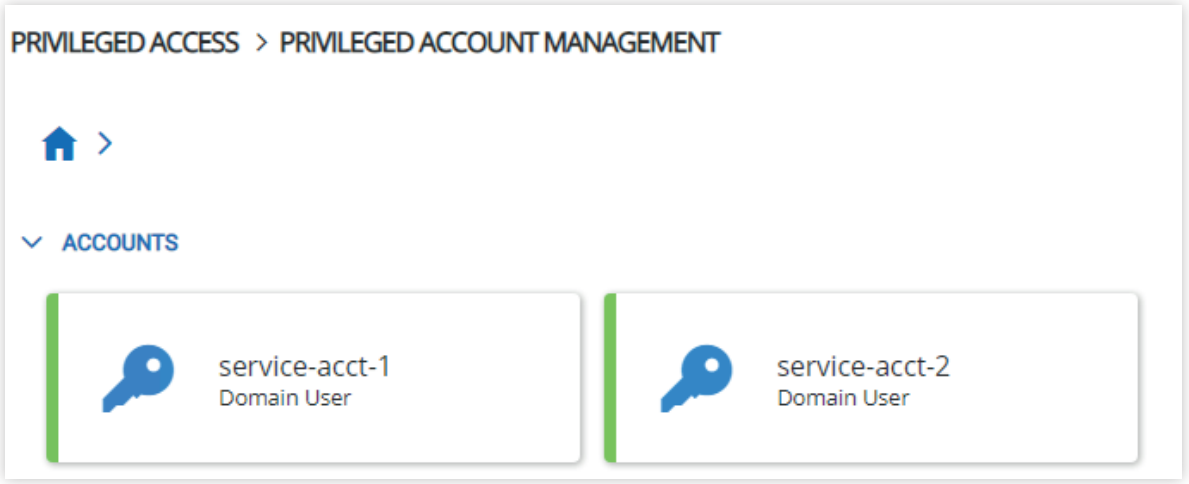


12. Once the resources are imported you will be presented with a successful import and at this point, the **Quick Start** guide has been completed.



13. Finally, click on the **Privileged Access** left-hand menu link and note that there are two **Accounts**, one **Provider**, and one **Scan Configuration** available. Click on **Accounts** to verify that the accounts are usable. Here, two accounts are shown, and if successfully imported with a password reset, will show a green left-hand border.

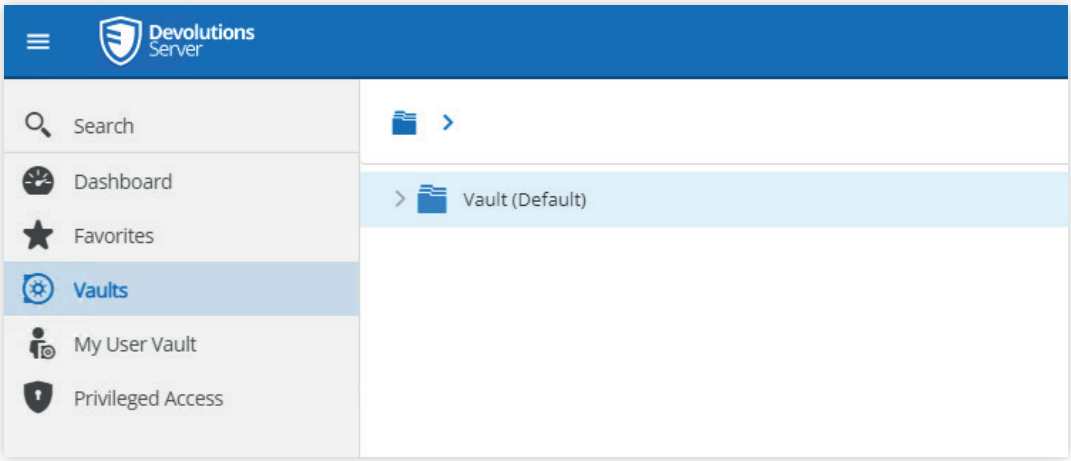




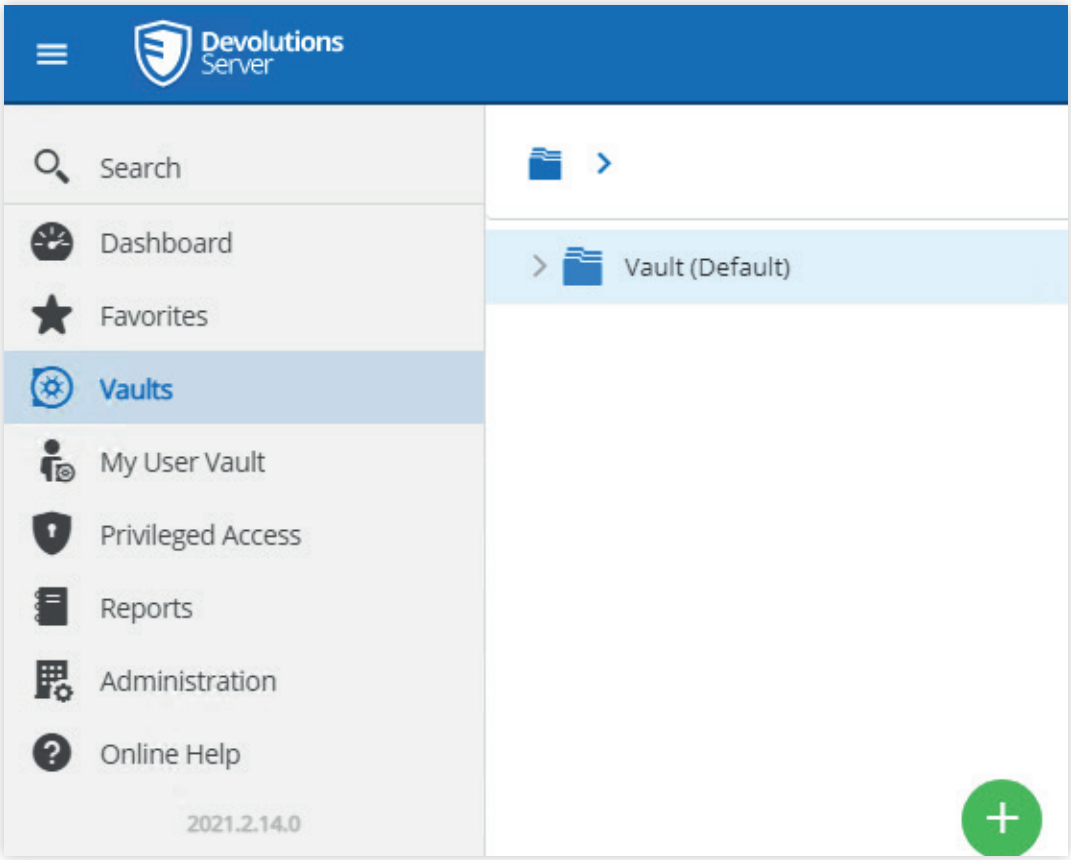
Adding a Privileged Account as a Vault Entry

To integrate the usage of PAM with the Remote Desktop Manager, a new entry must be added to a vault which the entry is then configured for use with PAM.

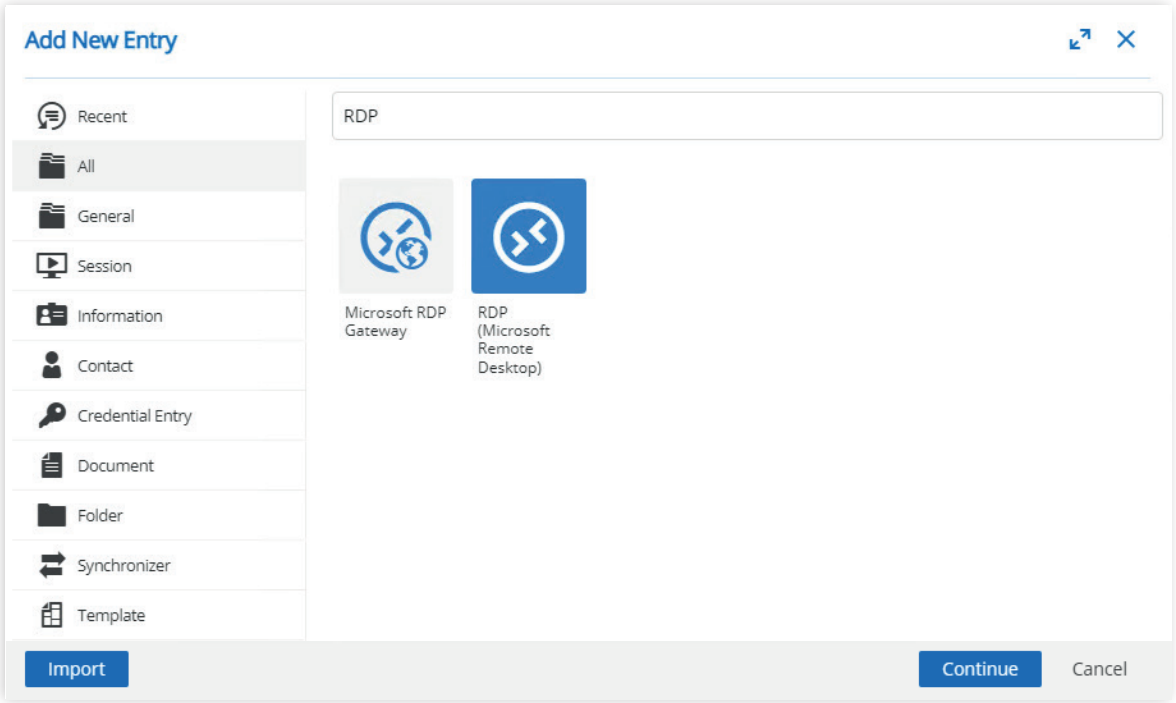
1. Navigate to the **Vaults** menu item and then to a vault, here the **Vault (Default)** is used.



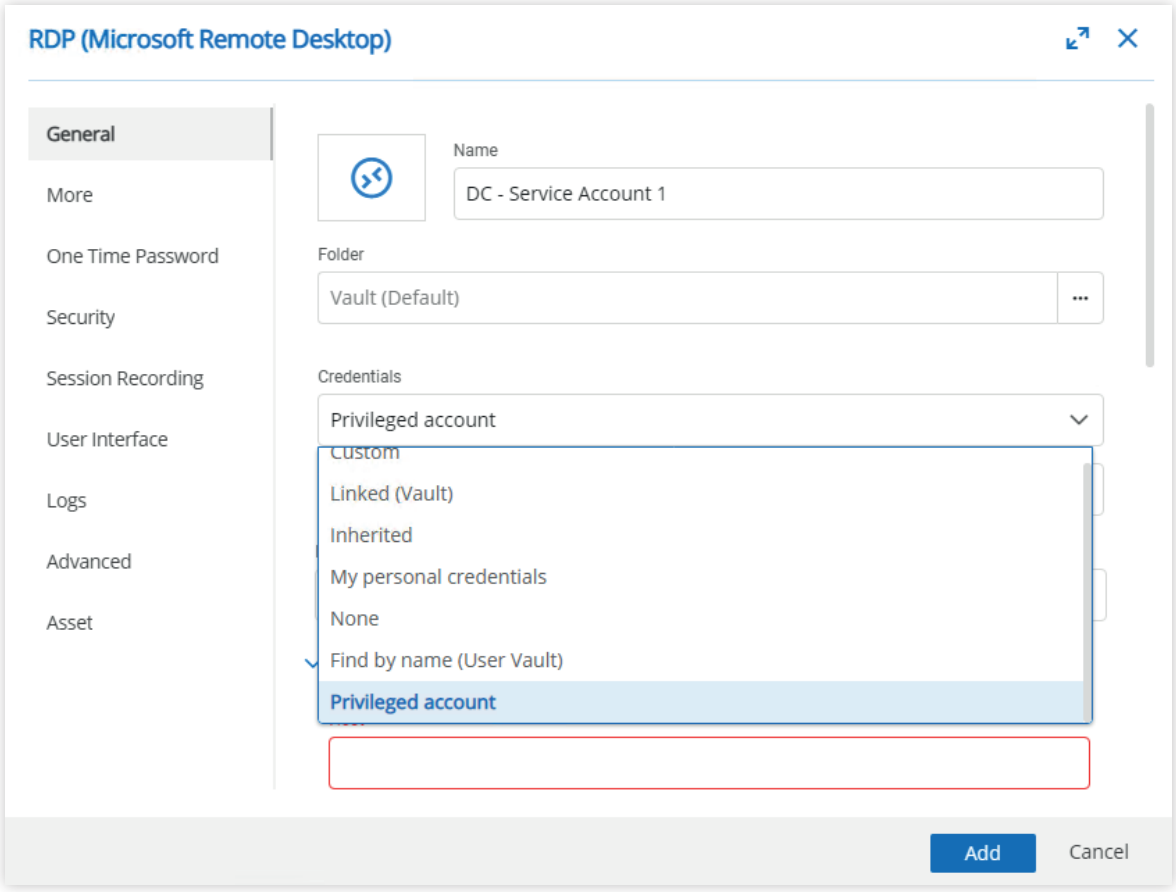
2. Click the green plus-circle icon to add a new entry to the selected vault.

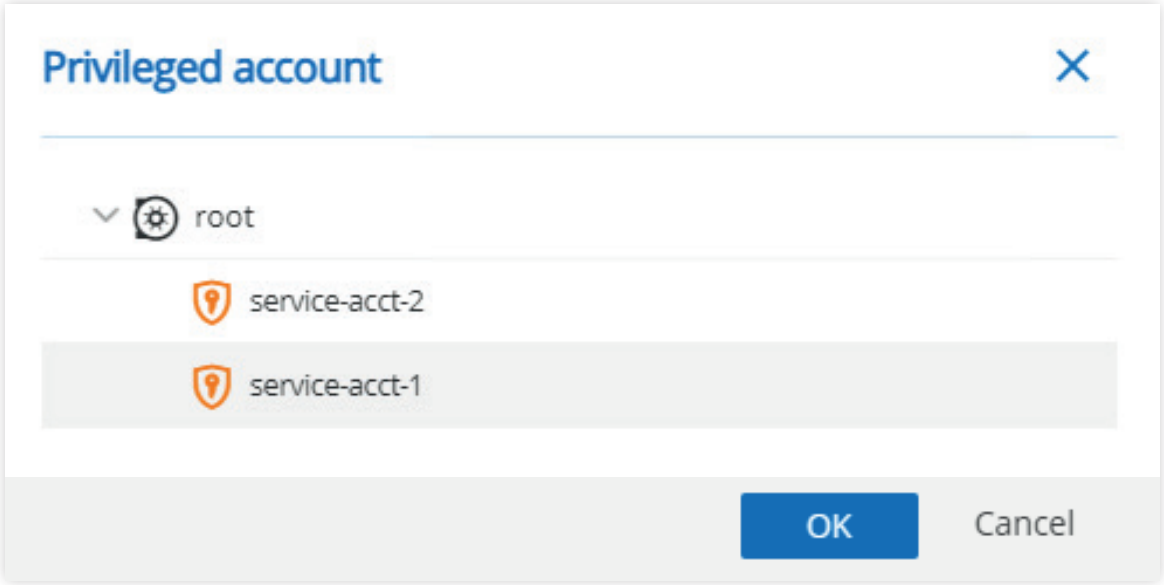


3. On the **Add New Entry** page, enter “RDP” in the search bar to filter the results to **RDP (Microsoft Remote Desktop)**, select the icon, and click **Continue**.

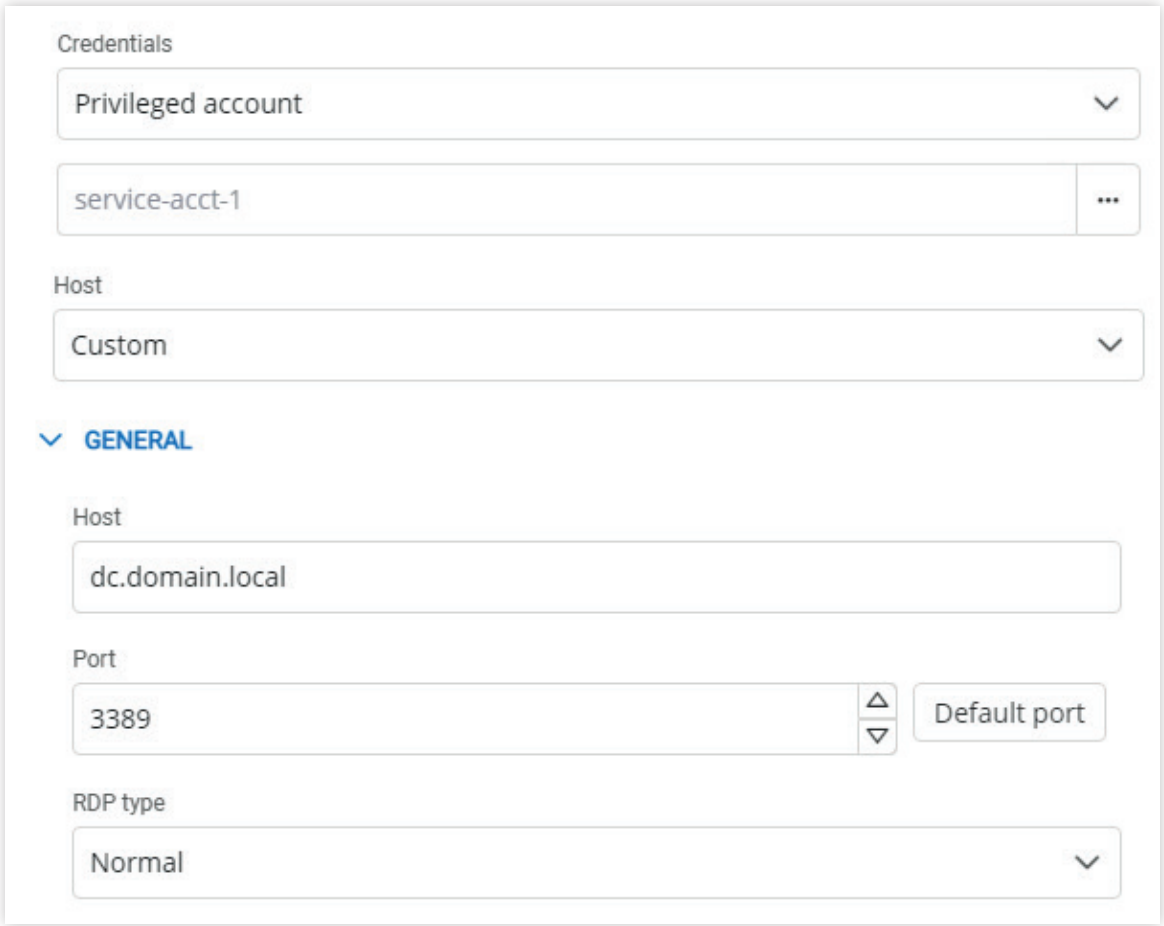


4. Enter a name, here the entry is named “DC - Service Account 1” and then select **Credentials → Privileged Account**. Select the account to add, here service-acct-1 is used.





5. Add the host information, here dc.domain.local is used with all default values and no **Username** and **Password** specified which is taken at the time of the connection from the specified PAM credential.

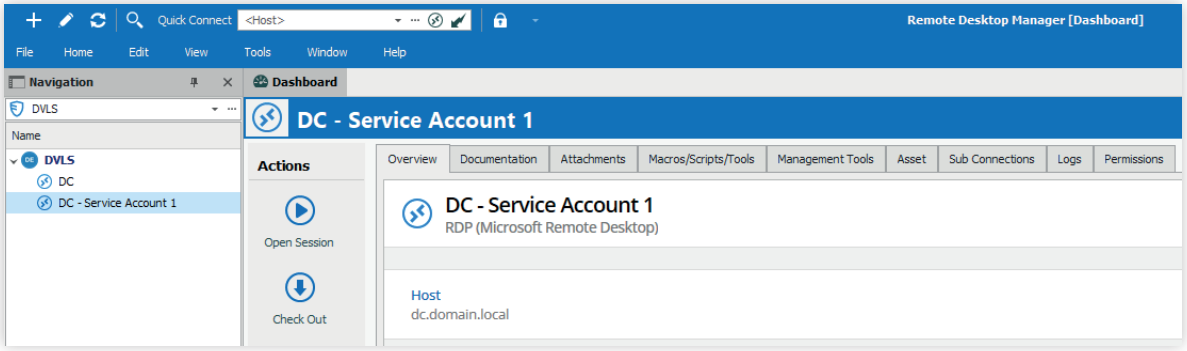


Remoting via RDP with a PAM Managed Service Account

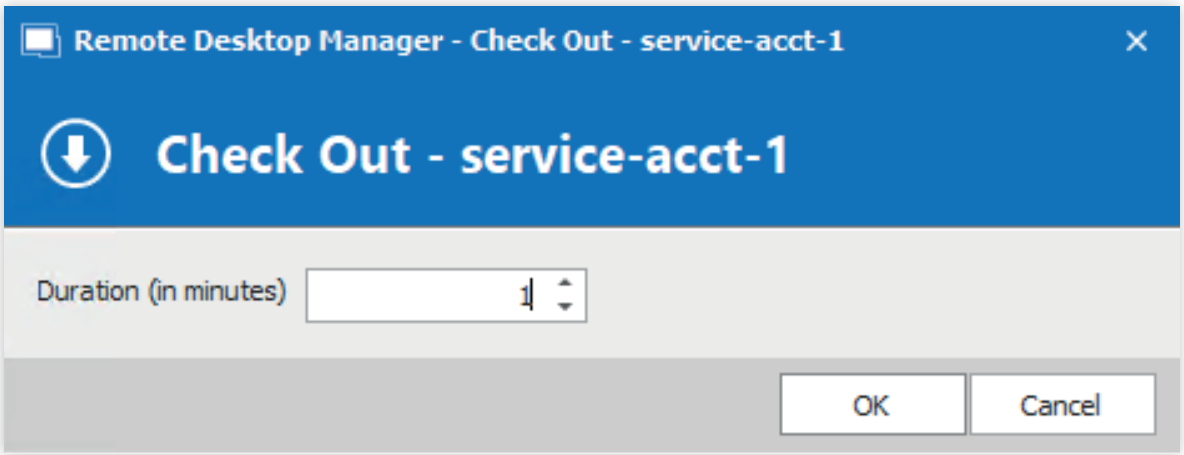
Now that an entry has been configured, you are ready to remote a host with a PAM-configured RDP entry.

1. Launch **Remote Desktop Manager** and navigate to the entry previously created, here named “DC - Service Account 1”. Select the entry and click **Open Session**.

> *If you receive a permission denied message for the Privileged Account, verify that the accessing account has Reader permissions to the Privileged Account itself.*



2. You are then prompted for a check-out duration, here shown with a time of 1 minute (default is 240 minutes) for demonstration. Click **OK** to continue and a Remote Desktop session will open.



3. After the session has concluded, the credential's current password will remain active for the duration previously specified (1 minute in this tutorial).

After that time, the password will be rotated, and opening a new session will require checking the credential out again. Shown below are the Devolutions Server PAM module logs demonstrating the rotation of the password and the Remote Desktop Manager behavior.