

HOW TO

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

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!



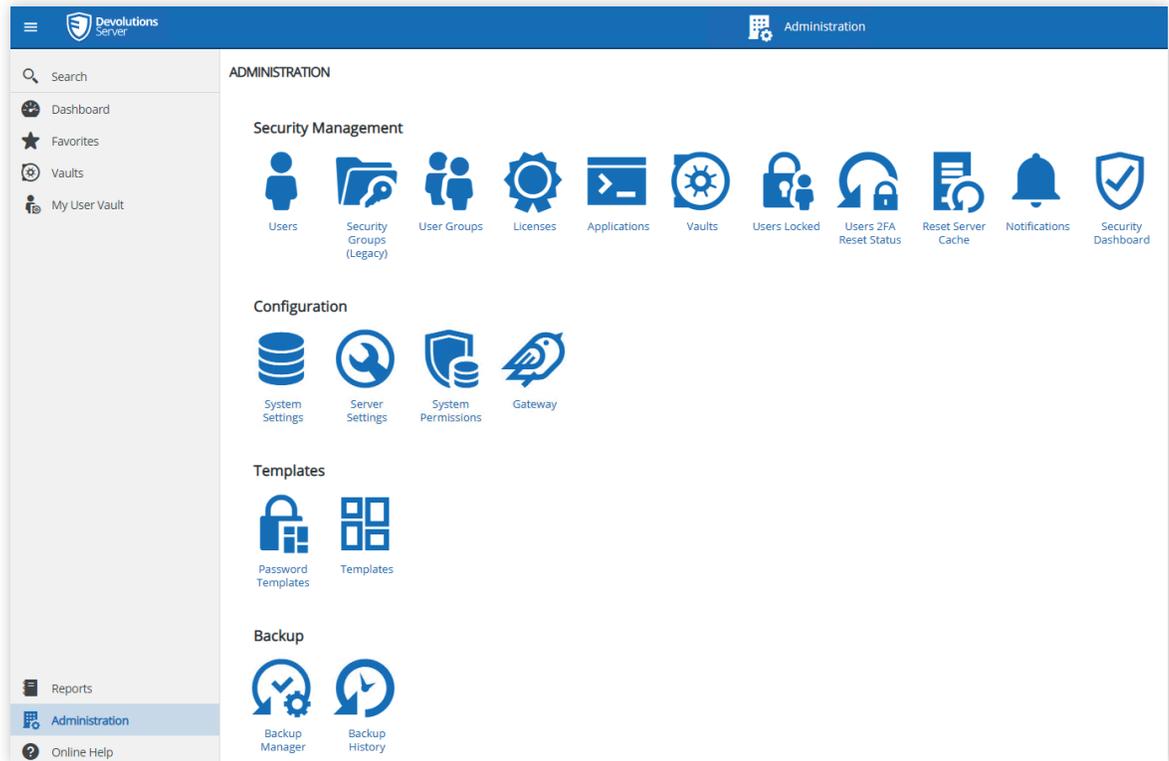
*As of version 2021.2.13.0, the Privileged Access Management (PAM) module is separately licensed. If you do not see the icon under **Administration** → **Server** settings, you will need to request or purchase the updated license.*

*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.*

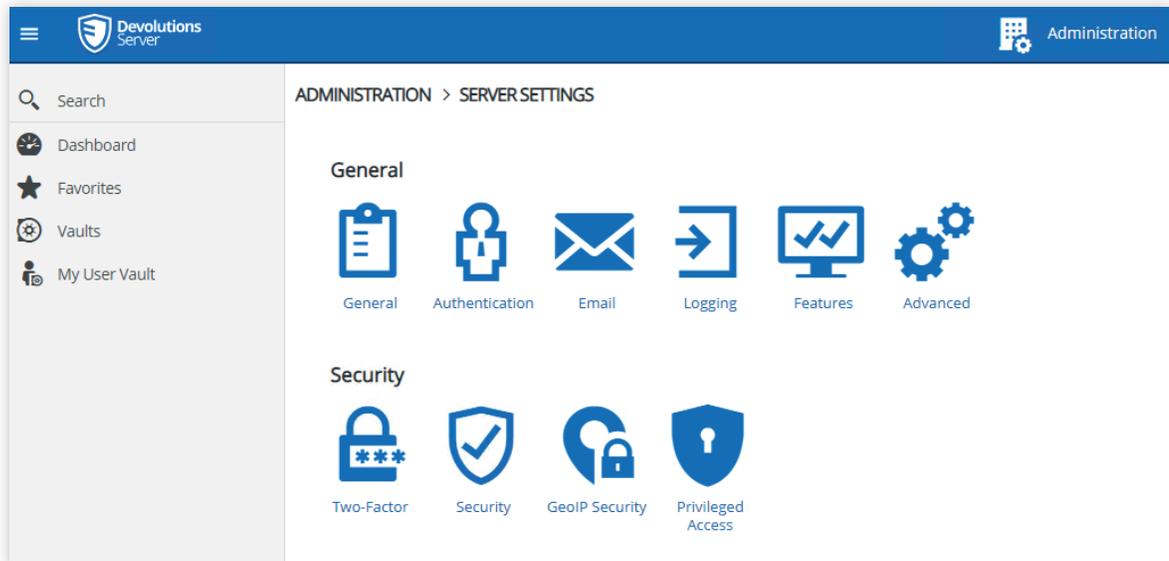
Enabling Devolutions Server PAM

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.

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](#)

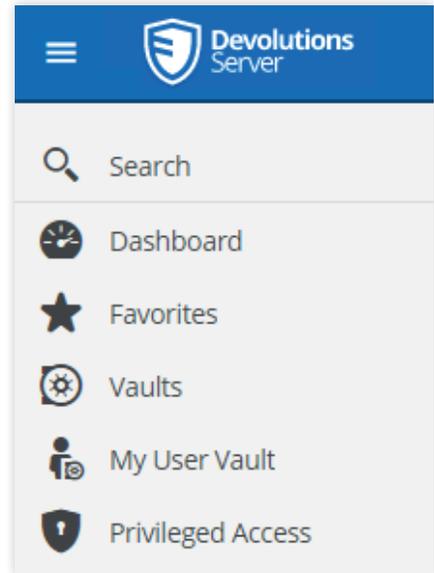
ADMINISTRATION > SERVER SET 

GENERAL

Enable PAM

Saved Successfully
The data has been successfully saved.

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



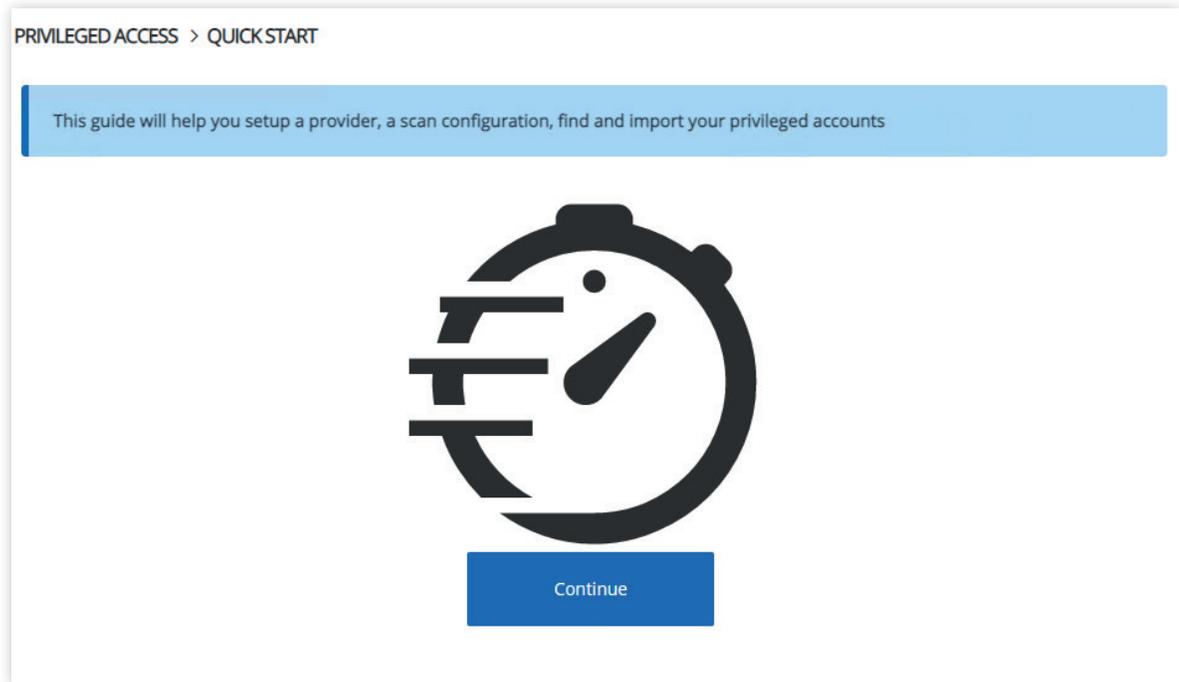
5. The first time that you access PAM you are presented with a welcome prompt. As you must import users to manage their passwords, go ahead and click the **Start Importing** button.



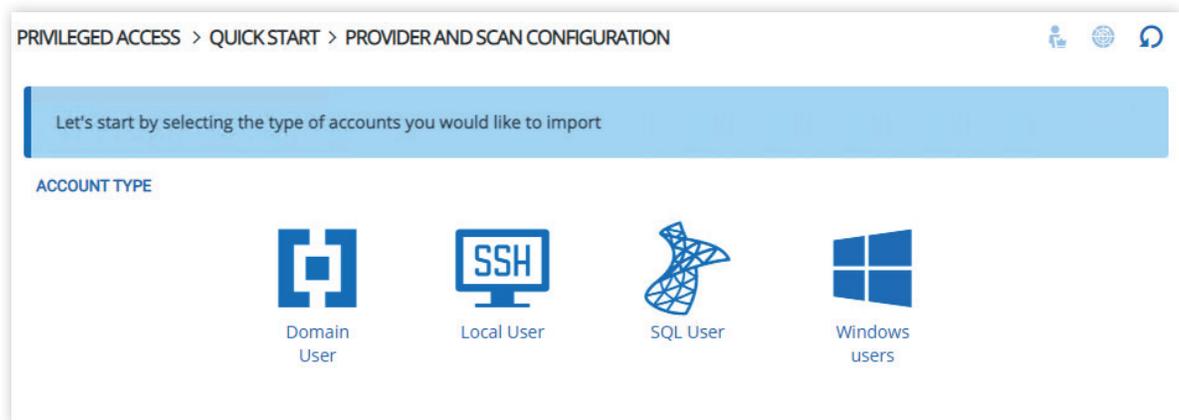
You can always restart this process by clicking on the start Quick Start menu link on the PAM homepage.

A screenshot of a dialog box titled 'Welcome to the privileged access section'. The dialog box has a close button (X) in the top right corner. The main text reads: 'This module allows for safe storage and sharing of your Privileged Accounts (PAs). These PAs can be discovered and imported by using a **Provider** (akin to an authentication authority) and the **Scan Configuration** feature. These PAs can then be used for account brokering on sessions when launched using Remote Desktop Manager. They are accessible via a system of checkouts, with an optional approval workflow. Passwords can be rotated automatically on a schedule and/or upon every checkin. The security is driven by our Role-Based Access Control system, which allows for a great deal of flexibility in determining who can use and manage the Privileged Accounts.' At the bottom of the dialog box, there is a link: 'Click here for more help on our PAM solution'. At the very bottom, there are two buttons: 'Start Importing' (a blue button) and 'Ask Later' (a gray button).

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](#).

Devolutions Server Privileged Access

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

2021.2.14.0

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

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

- Click **Scan** and on the resulting page, select the checkbox next to the accounts to import into 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. Click the **Import** icon in the upper-right (file icon with arrow) and enter a **Name**, here the provider is named **Active Directory Import**. 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.

The image displays two screenshots of the 'Import 2 account(s)' dialog box. The left screenshot shows the main configuration screen with the following fields and options:

- PROVIDER**
 - Name: Active Directory Import
- DESTINATION**
 - Folder: \
- OPTIONS**
 - Reset Password On Import
 - Reset Password On Check In
- SCAN CONFIGURATION**
 - Save scan configuration
 - Name: Active Directory Import Scan Configuration
 - Recurring scan

The right screenshot shows a 'Select folder' sub-dialog with the following elements:

- Buttons: Expand All, Collapse All
- Folder list: root
- Buttons: OK, Cancel

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.

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. 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.

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

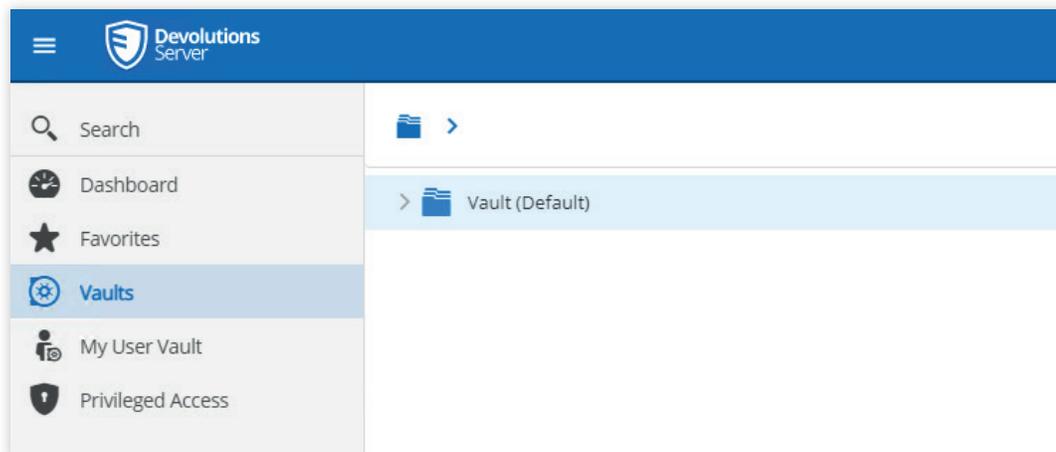


service-acct-2
Domain User

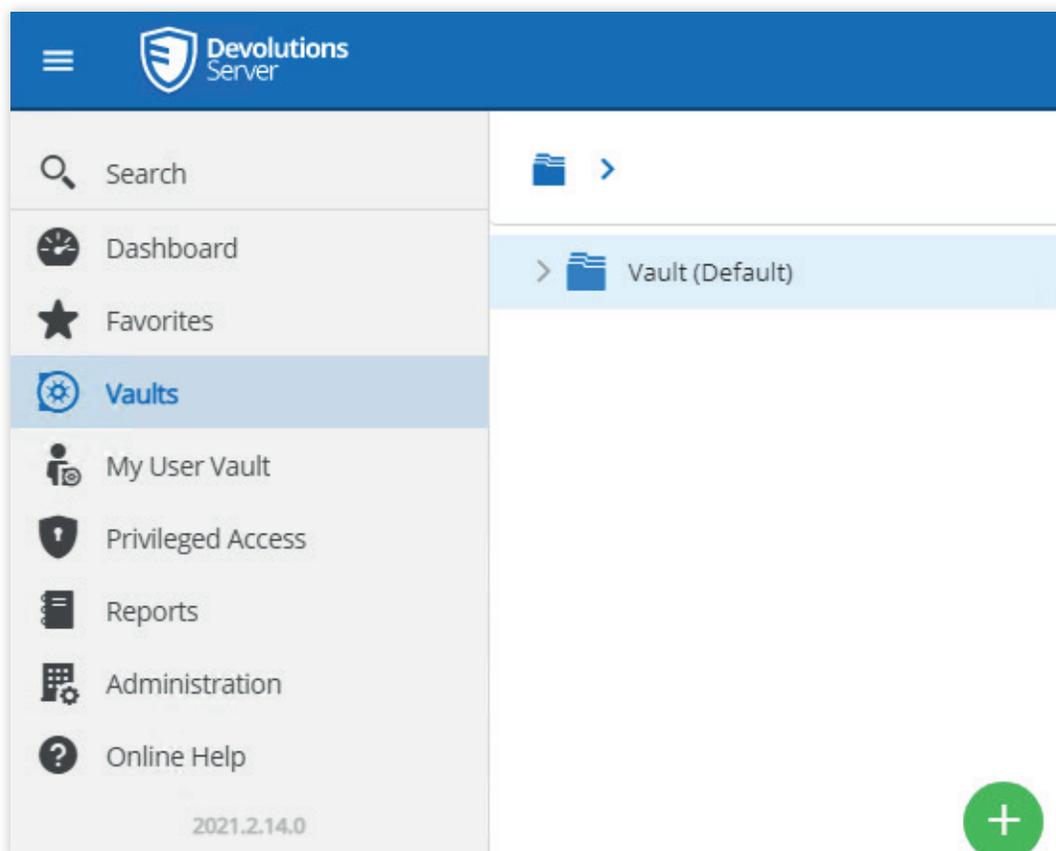
Adding a Privileged Account as a Vault Entry

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.

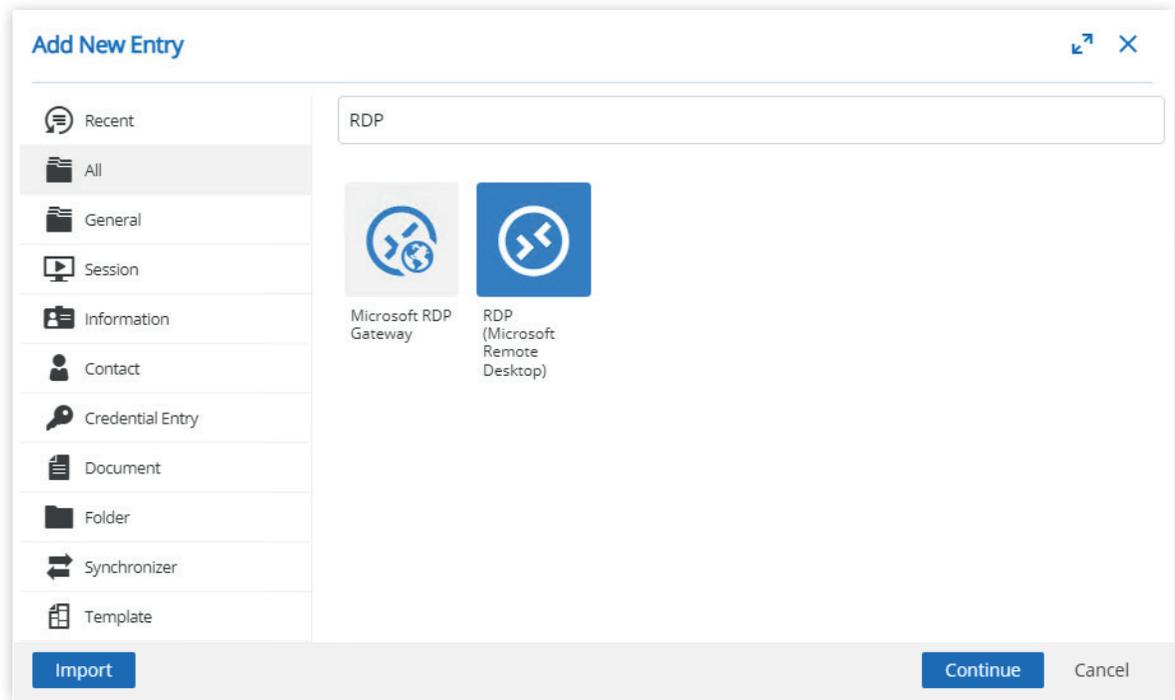
1. Navigate to the **Vaults** menu item and then to a vault, here the **Vault (Default)** is used.



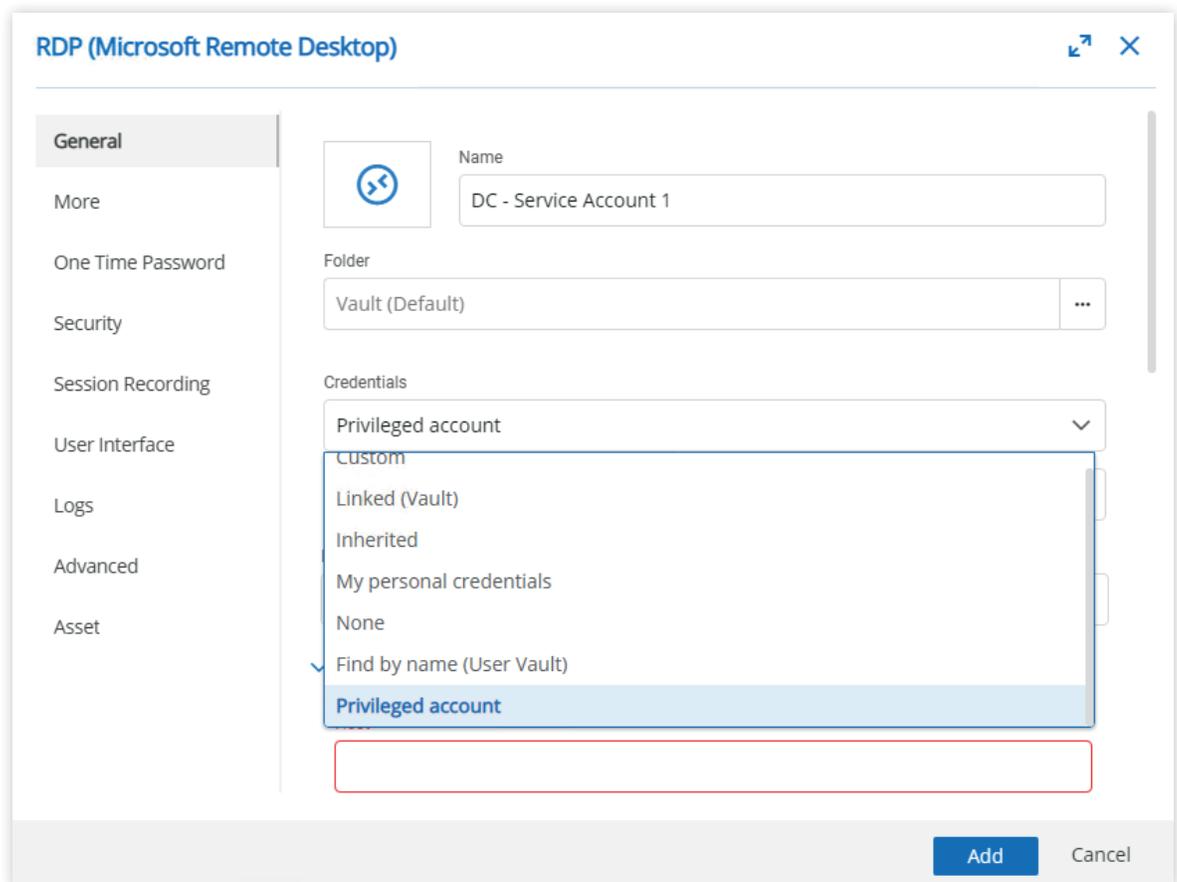
2. Click the green plus-circle icon to add a new entry to the selected vault.

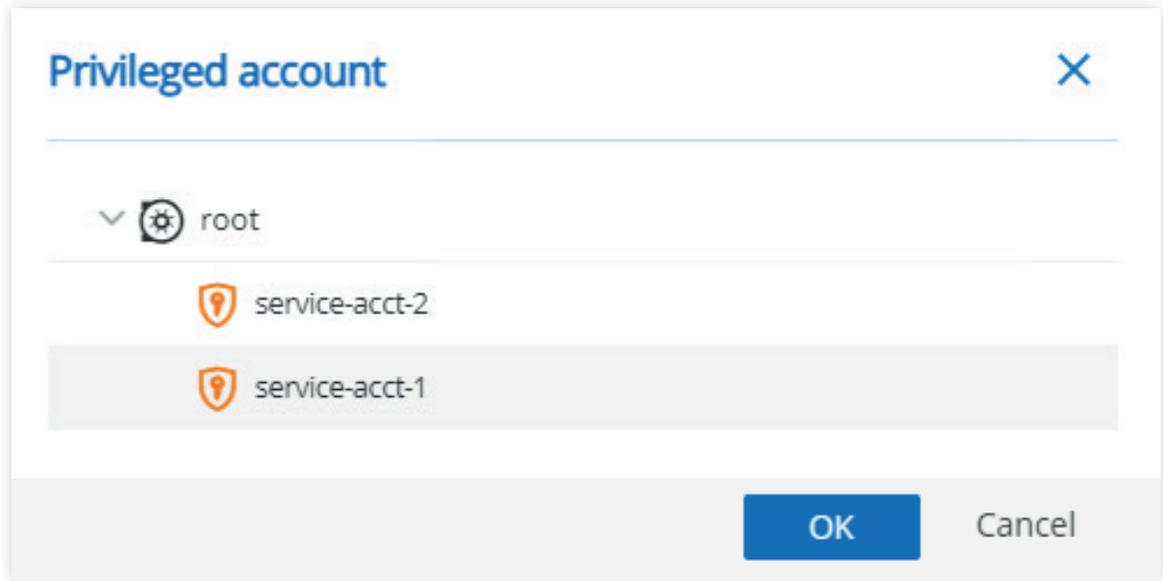


3. On the **Add New Entry** page, enter “RDP” in the search bar to filter the results to **RDP (Microsoft Remote Desktop)**, select the icon, and click **Continue**.

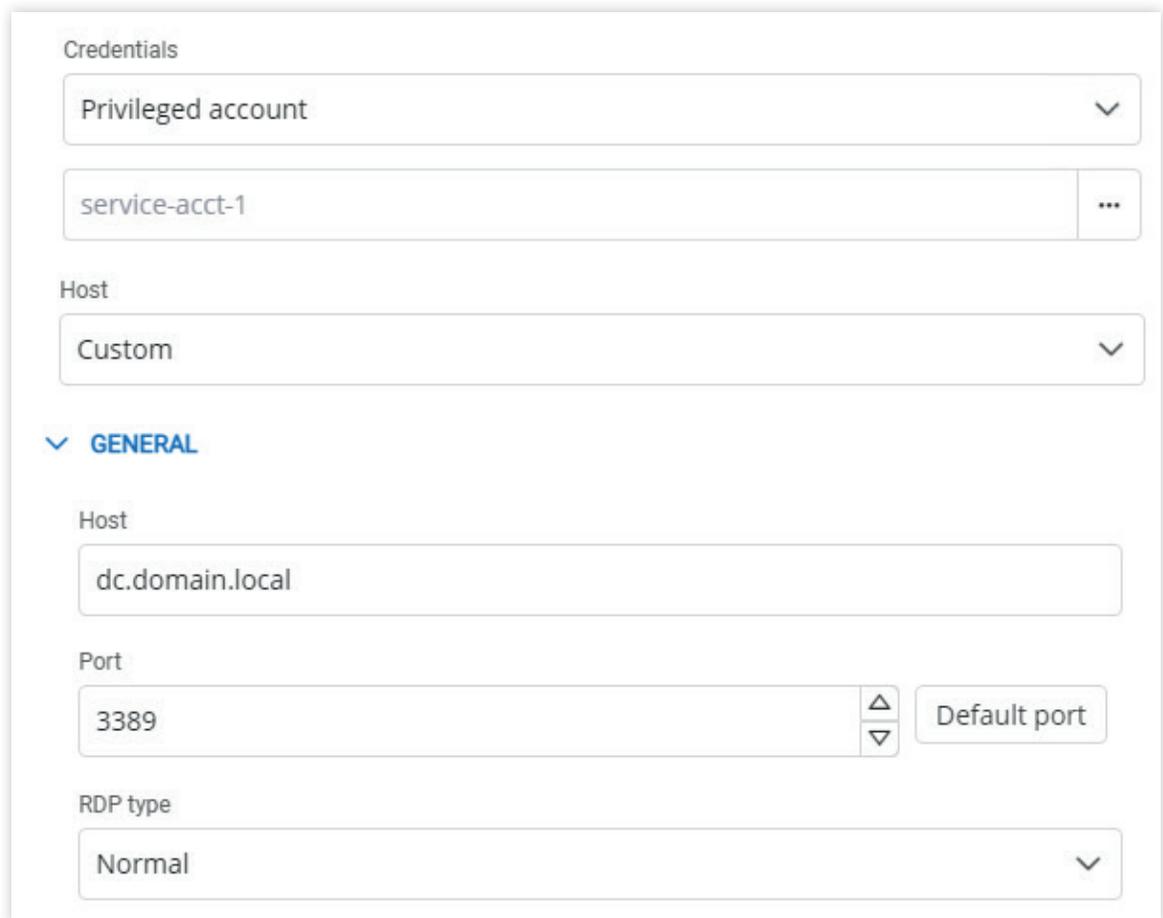


4. Enter a name, here the entry is named “DC - Service Account 1” and then select **Credentials** → **Privileged Account**. Select the account to add, here service-acct-1 is used.





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.



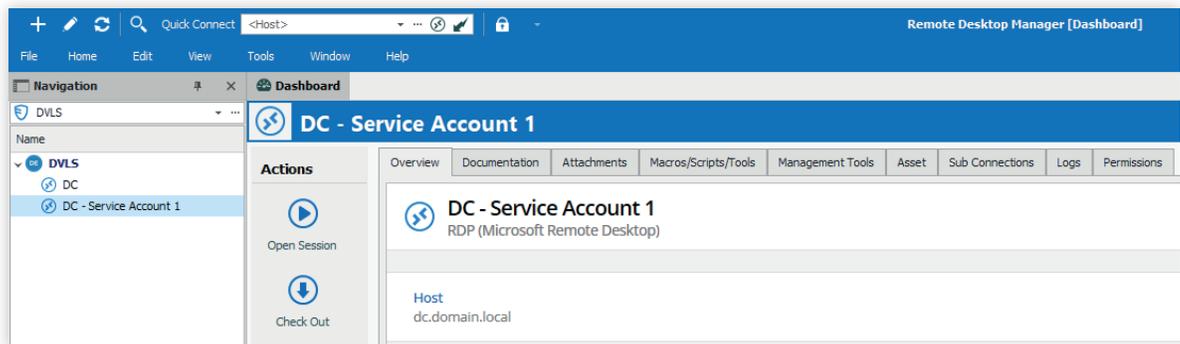
Remoting via RDP with a PAM Managed Service Account

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

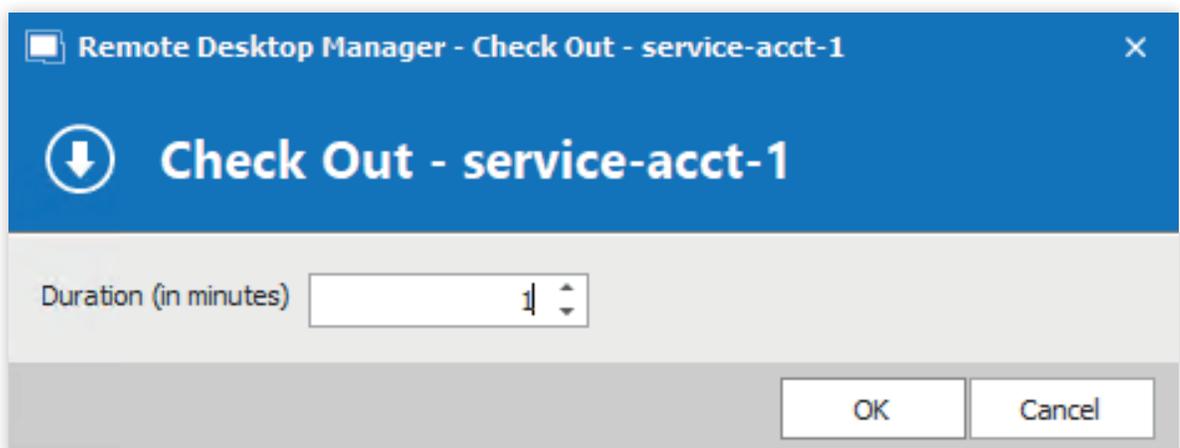
1. Launch **Remote Desktop Manager** and navigate to the entry previously created, here named “DC - Service Account 1”. Select the entry and click **Open Session**.



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.

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	●●●●●●