Remote Desktop Manager

Remote Connections & Passwords.
Everywhere!

User Manual

2022.2

Devolutions

Table of Contents

Overview

Part

I

1 Overview

1.1 Remote Desktop Manager

DESCRIPTION

Remote Desktop Manager is an application that integrates a comprehensive set of tools and managers to meet the needs of any IT team. It is designed to centralize remote connection technologies, credentials, and secure the access to these resources. Most connections are established using either an external library or third-party software.

Remote Desktop Manager is compatible with several relevant tools and technologies, including: **Apple Remote Desktop**, **Citrix**, **Dameware**, **FTP**, **Hyper-V**, **LogMeIn**, **Radmin**, **RDP (Microsoft Remote Desktop)**, **SSH Port Forward**, **SSH Shell**, **TeamViewer, Telnet**, **Remote Desktop Services**, **VMware**, **VNC**, **SCP**, **X Windows**, and more!

THE REMOTE DESKTOP MANAGER ECOSYSTEM

Remote Desktop Manager is available in two editions:

Free	For individuals only, no information can be shared with colleagues. The most popular remote access technologies are supported and passwords can be stored securely.
Enterprise	Used by teams, this edition offers user permissions, user groups, advanced logging, etc. RDM uses a Database Management System (DBMS) for storing the information and sharing it according to **your** security requirements. Devolutions also offers two specialized services for Cloud-Based storage or to get full Active Directory Integration.

Remote Desktop Manager is also offered on multiple platforms, as seen below.

Purchasing an Enterprise license grants the right to use ALL the various client applications.

You must use a desktop application to create a team data source. This explains why the mobile applications are free. They do allow for simple usage by an individual much like the Free Edition, but they can only **use**, not **manage**, a Team data source.

PLATFORM	FREE EDITION	ENTERPRISE EDITION
Windows	✓	✓
macOS	✓	✓
Linux	✓	✓
iOS		✓ (Free App)
Android		✓ (Free App)

1.2 Security

DESCRIPTION

All passwords stored in the data sources are encrypted using a strong encryption algorithm, to the extent that if a user attempts to access the data directly in the database, it will be considered unreadable.

If you choose to store passwords locally, Remote Desktop Manager will use the same mechanism used by mstsc.exe (Remote Desktop Manager client), which stores the passwords in the Windows Credential Manager. It must be noted that the password will not be able to be viewed due to being encrypted by Windows. For obvious reasons, this choice also means that credentials stored in this fashion are not shared.

U.S. FEDERAL GOVERNMENT APPROVED ENCRYPTION

Our application integrates an Advanced Encryption Standard (AES) algorithm to protect sensitive data in the database.

This cipher is proven to be very secure. AES/Rijndael became effective as a U.S. Federal government standard and is approved by the National Security Agency (NSA) for top secret information.

TIPS

Encryption of data while in transit is offered natively by our cloud services. Whenever you decide to use an on-premise solution, encryption of data in transit must be implemented by using the tools involving your chosen technologies. Most customers with security concerns choose Advanced Data Sources. Follow instructions specific to the chosen solution.

The encryption key is ***built-in*** the application and is therefore the same for ***all*** copies of the software in circulation. It is imperative that you follow our recommended steps and apply a Security Provider to encrypt not only the passwords, but also ***all connection data*** stored in the data source. This will provide protection over your data at rest, using a key under your exclusive control.

We recommend you follow these steps to ensure data security:

- Use an Advanced Data Source and grant user access by assigning permissions.

- Use encrypted communication with the database when available.
- Use the System Settings to control settings impacting security.
- Use the Security Provider to encrypt entries completely instead of just the password.
- If using the offline mode, add your own password for an additional layer of protection to the local cache. Go to ***File - Options - Security***.
- Require a password to launch the application and even require two-factor authentication. Go to ***File - Options - Security***.
- If your data source supports it, choose not to save password in the data source, which will prompt for the credentials on the first connection.
- Use our Group policies to set up the system.

1.3 System Requirements

DESCRIPTION

Remote Desktop Manager requires the following prior to installation:

MINIMUM REQUIREMENTS

Windows Desktop:

- Windows 11
  - Version 21H2
- Windows 10
  - Version 20H2, 21H1 and 21H2
- 8.1
- 7 SP1

Windows Server:

- Windows Server 2022
- Windows Server
  - Version 20H2
- Windows Server 2019
- 2016
  - Version 1607
- 2012 R2
- 2012

Microsoft .NET Framework 4.8

1 GHz or faster processor

4GB RAM

1024 x 768 screen resolution

500+ MB hard drive space

64-bit operating system

Microsoft Edge WebView2 Runtime

REMOTE DESKTOP SERVICES AND THIN CLIENT SUPPORT

Remote Desktop Manager can be installed on Remote Desktop Services and thin client.

MANUAL/PORTABLE DEPLOYMENT

Deploying manually using our zip file is documented as being a Portable (USB) deployment. In this case, the prerequisites will need to be handled manually as well. Please consult Prerequisite Software for details.

1.3.1 Prerequisite Software

DESCRIPTION

Specific prerequisite software need to be installed on your computer prior to running Remote Desktop Manager.

These installations are managed automatically by our installers. The only situations in which a manual installation of the prerequisite software should be performed are when the zip archive is used for deployment or when there is no Internet connection.

SETTINGS

The following package must be installed prior to proceeding with the Remote Desktop Manager installation:

- Microsoft .NET Framework 4.8

1.4 The Devolutions Platform

DESCRIPTION

Our platform offers multiple products to help managing all of the aspects of an IT infrastructure.

APPLICATIONS	DESCRIPTION	INSTALLATION
Remote Desktop Manager (RDM)	Application used to manage and centralize remote access technologies, privileged passwords, documents and shared information.	Windows, macOS, Linux, iOS, Android

APPLICATIONS	DESCRIPTION	INSTALLATION
Remote Desktop Manager Agent	The Remote Desktop Manager Agent can run commands on remote hosts, but what is really useful is that it can send commands to multiple hosts at the same time. Since Remote Desktop Manager uses a secure RDP channel to communicate with the Remote Desktop Manager Agent, it can only operate against Windows-based hosts.	Windows
Remote Desktop Manager Jump	Remote Desktop Manager Jump connects to a remote host, often called a Jump Box, Service Host, or a Bastion Server, which in turn connects to other hosts. Remote Desktop Manager Jump is actually an RDP in an RDP.	Windows
Devolutions Server (DVLS)	Devolutions Server is a full-featured shared account and password management solution with add-on privileged access components. It deploys rapidly, implements easily, and delivers the core features of a comprehensive PAM solution. Devolutions Server is designed to meet the ever-expanding security requirements of SMBs, while remaining very affordable.	Windows
Devolutions Password Hub Business	Devolutions Password Hub Business is a secure and cloud-based password manager for teams. It empowers your organization to easily and securely vault and manage business-user passwords, along with other sensitive information, through a user-friendly web interface that can be quickly, easily and securely accessed via any browser.	Windows, macOS
Devolutions Web Login (DWL)	Devolutions Web Login is a free browser plugin used in conjunction with Remote Desktop Manager, Devolutions Server and	Windows, macOS

APPLICATIONS	DESCRIPTION	INSTALLATION
	Devolutions Password Hub, which allows users to securely inject passwords into websites using credentials stored in their vaults.	

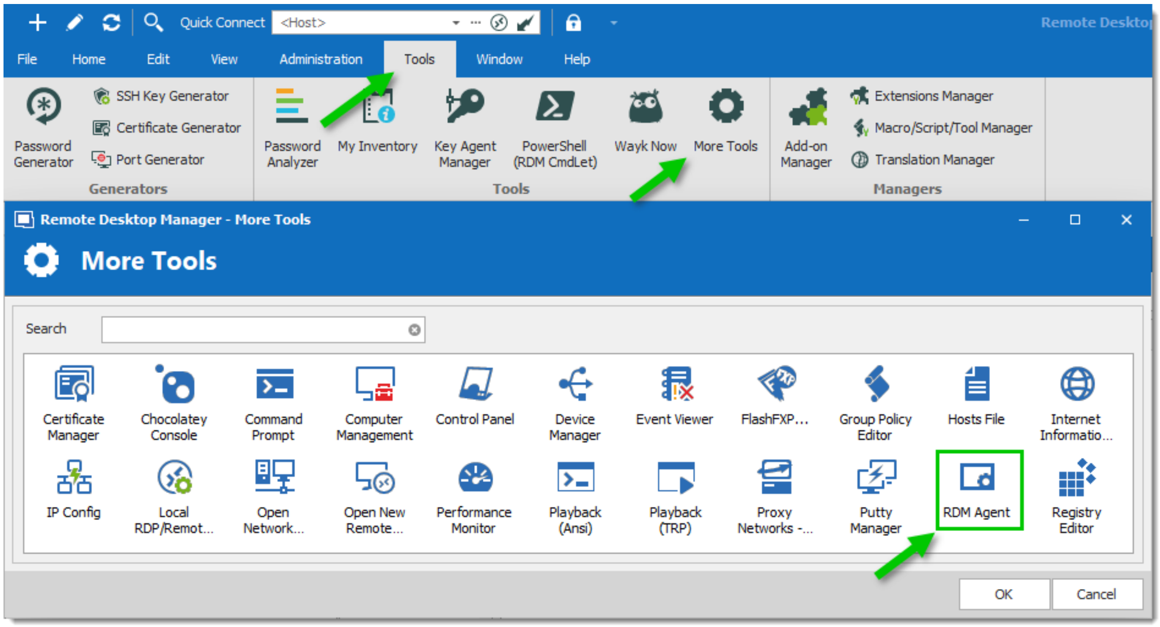
1.4.1 Remote Desktop Manager Agent

DESCRIPTION

Please note that if your Windows profile is corrupted, Remote Desktop Manager Agent and Remote Desktop Manager Jump might not work.

The Remote Desktop Manager Agent can run commands on remote hosts, but what is really useful is that it can send commands to multiple hosts at the same time. Since Remote Desktop Manager uses a secure RDP channel to communicate with the Remote Desktop Manager Agent, it can only operate against Windows-based hosts.

It supports both environment and Remote Desktop Manager variables. Remote Desktop Manager variables (i.e. $HOST$, basically all the ones surrounded by dollar signs) are resolved on the client against the running session, while environment variables (i.e. %windir%, basically all the ones surrounded by percent signs) will be resolved on the remote host at execution time. You can use Remote Desktop Manager variables while running file based scripts (.ps1) within the command. The file based script variables (.ps1) will be resolved prior to sending the script to the destination host.



RDM Agent

SCENARIOS

The Remote Desktop Manager Agent can be used to run scripts from another Remote Desktop Manager installation. Since it uses an RDP channel for communication, it saves you from remote management headaches such as opening various ports in your firewall. This requires the lightweight installation model of just the agent package (Methods 2-4 below).

It is also used by Remote Desktop Manager Jump for supporting many technologies. However, it does require a full Remote Desktop Manager installation on the remote host for those features.

INSTALLATION

Installing Remote Desktop Manager Agent on a remote host can be achieved in 4 different ways:

The Remote Desktop Manager Agent must be configured to automatically start when a Windows session is established. Method 1 below performs that automatically, but in other cases, you must configure this manually using Windows features (*startup* folder or *Run* registry key). Please consult the documentation of your operating system for details.

1. Install Remote Desktop Manager and select Tools – More Tools – RDM Agent. It will launch and auto-register the Agent to automatically start with Windows.

2. Download Remote Desktop Manager Agent from https://remotedesktopmanager.com/Home/Download, and install the agent on the remote computer.

3. Copy the files Devolutions.Utils.dll, Devolutions.Windows.Utils.dll and RDMAgent.exe from the installation folder of the Remote Desktop Manager version that is used by your team, or
download the zip file containing those files at https://remotedesktopmanager.com/Home/Download and deploy them on the remote host in the folder of your choice.

4. Via Chocolatey at https://chocolatey.org/packages/rdmagent.

```
C:\> choco install rdmagent
```

Chocolatey command line

Many new users using this technology wonder why a full installation of Remote Desktop Manager is required. There are three factors that make this a good solution:

- Remote Desktop Manager on the remote host does not require a data source, it's an empty shell.

- The logging of the activity is brought back to your data source.

- Every technology supported by Remote Desktop Manager can be used remotely.

1.4.2 Remote Desktop Manager Jump

DESCRIPTION

Remote Desktop Manager Jump connects to a remote host, often called a **Jump Box, Service Host, or a Bastion Server**, which in turn connects to other hosts. Remote Desktop Manager Jump is actually an RDP in an RDP.

This can be compared to RD Gateway from Microsoft and to some extent SSH port forwarding.

> The Jump is performed through Remote Desktop Manager Agent. The Agent needs to be **CURRENTLY EXECUTING** in a Windows Session on the remote host, or set to automatically start upon login. We have decided NOT to have this available through a service at this time.

> The Remote Desktop Manager Jump feature does not allow you to circumvent the need to properly license your remote host to allow more than two RDP connection at a time. There is no other way except for installing remote desktop session host role on the server and purchasing RDS CAL (per user) for the remote connection. For more information please consult this Microsoft link: Activate the Remote Desktop Services license server.

> Remote Desktop Manager must be installed on the Jump Host for the agent to be able to run commands. The application does not have to connect to any data source, as Remote Desktop Manager only serves as a shell for the agent to run commands.

Both instances of Remote Desktop Manager Jump or Remote Desktop Manager and RDM Agent running on the ***Jump Host*** communicate through an RDP channel. Commands are sent securely over the RDP channel and are then executed on the **Service Host**. Commands include running a script or opening a remote session of any type. It can even launch a VPN client on the **Service Host** prior to running the remote session.

- Usage Scenarios
- Configure a Jump Host
- Configure a session to use the Jump Host

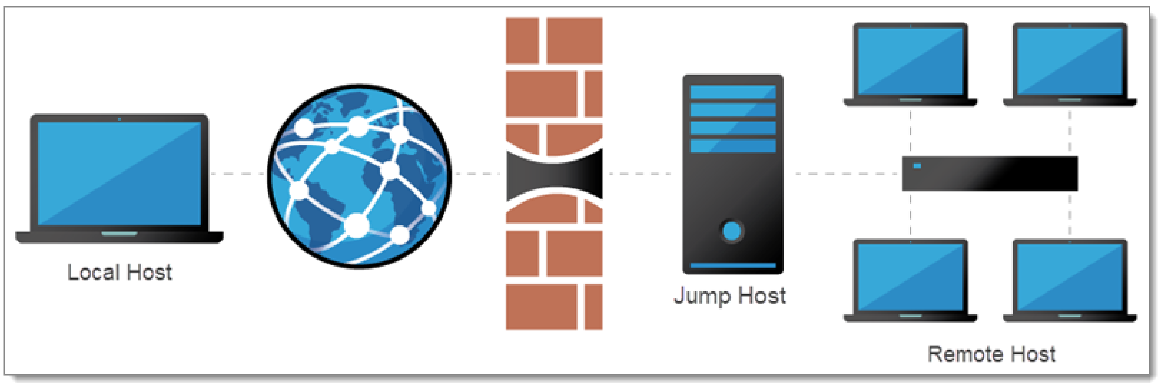
- Validate that the Jump Host works
- Pro Tips

USAGE SCENARIOS

There are two targeted scenarios:

1. Accessing a secure network through a single host

This allows you to have a strict firewall policy that allows connections only from a specific IP address. This configuration only grants you access to hosts that are accessible from the Jump Box. Let's imagine you have the following infrastructure:

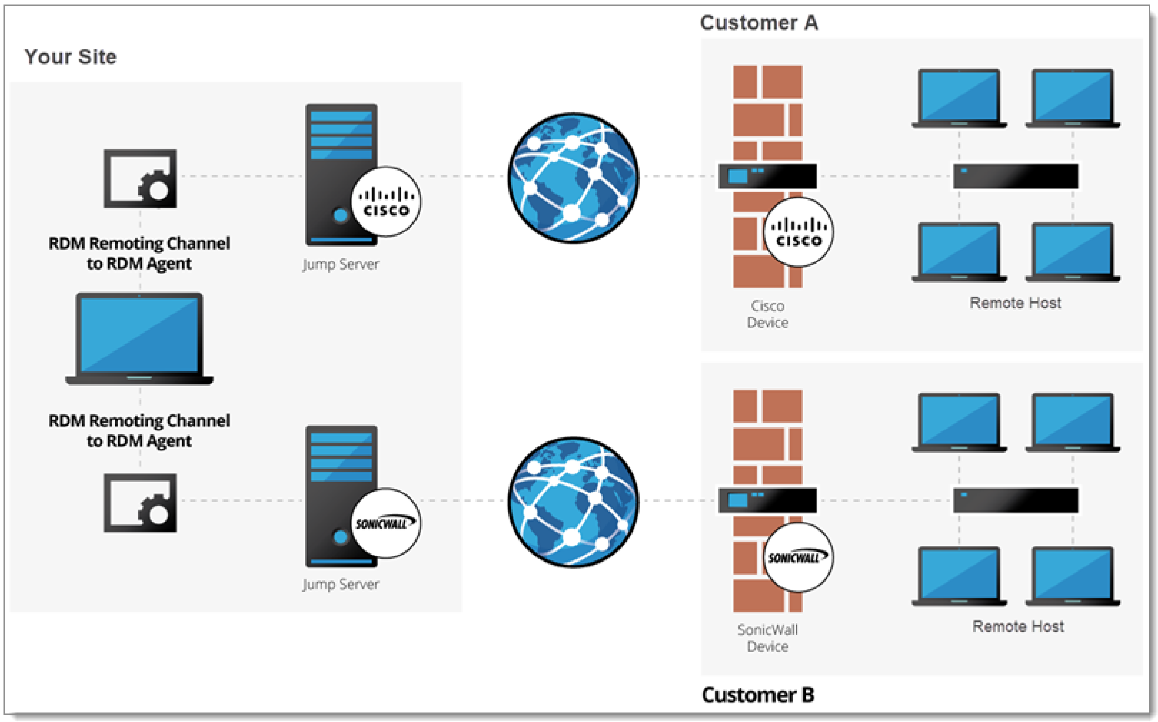


You need to access the remote hosts, but you want to limit risks and expose only the Jump Host to the internet traffic. This allows you to create strict firewall rules and to open only a single port. Therefore, it forces you to connect to the Jump Host before hopping to a remote host.

Remote Desktop Manager Jump helps achieve that goal simply and efficiently.

2. Workaround limitations of some VPN clients

These limitations make it impossible to use multiple VPN clients concurrently on the same workstation. In this case, you can have multiple virtual machines, each running a single VPN client. Using these virtual machines as jump boxes allows you to connect to the virtual machine, launch the VPN client, then launch the remote session.

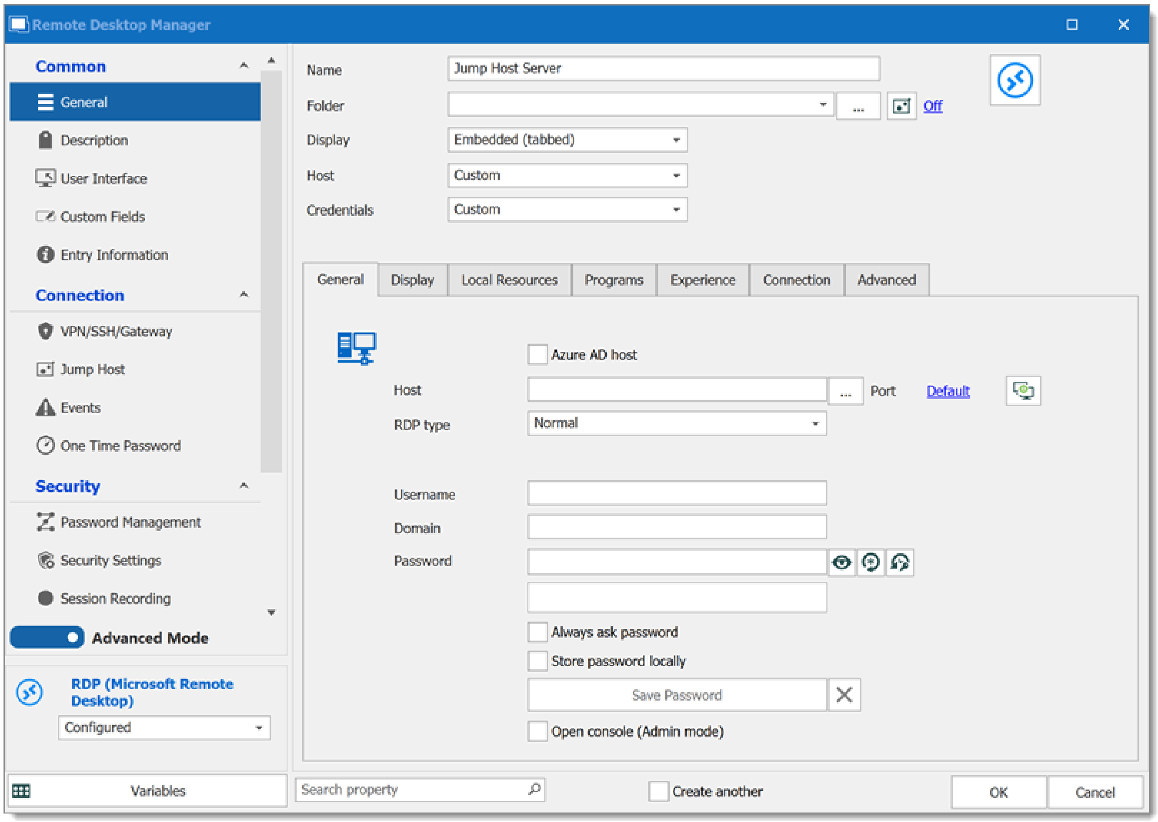


CONFIGURE A JUMP HOST

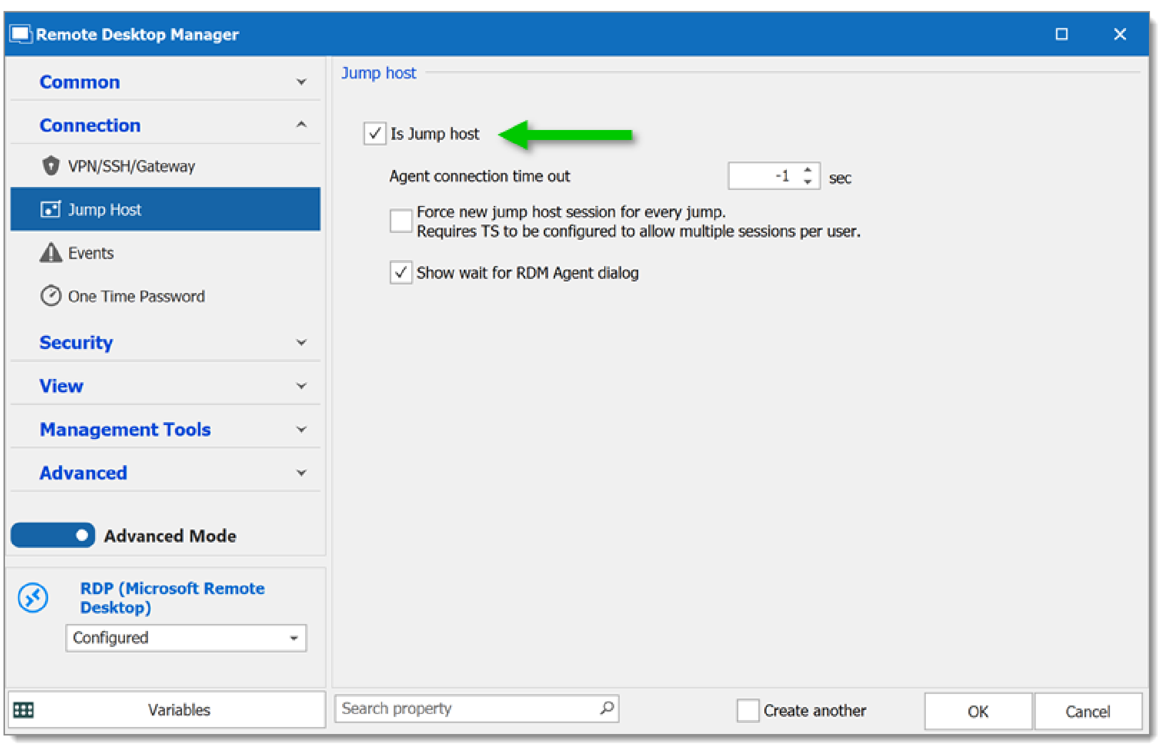
1. Create an ***RDP*** entry for the ***Jump Host***.

2. Fill the entry with a ***Name***, ***Host*** and the ***Credentials***.

For ***Jumps*** to work, you need to supply the credentials via the ***Jump Host*** session. If the RDP sessions prompt you for the credentials after the start, the ***Jump*** will fail.



3. In the ***Jump Host*** section, check ***Is Jump host***.



4. Click ***OK***.

5. Launch the ***Jump Host*** session.

6. Install Remote Desktop Manager on the ***Jump Host***.

> The ***Jump Host*** acts as a relay between the local and the remote systems, allowing to use the Remote Desktop Manager license that has been used on the local workstation to register the application on the ***Jump Host***.
>
> Install Remote Desktop Manager on the ***Jump Host***, perform your first jump and Remote Desktop Manager will be unlocked/licensed automatically via the jump communication/handshake.

> There is no need to create a data source on the ***Jump Host***. Remote Desktop Manager will open for the first time with a default ***SQLite Local Data Source***. This is sufficient because the application on the ***Jump Host*** only acts as an intermediate between the local and the remote hosts.

7. Confirm Remote Desktop Manager Agent is started and set to ***Auto Start***.

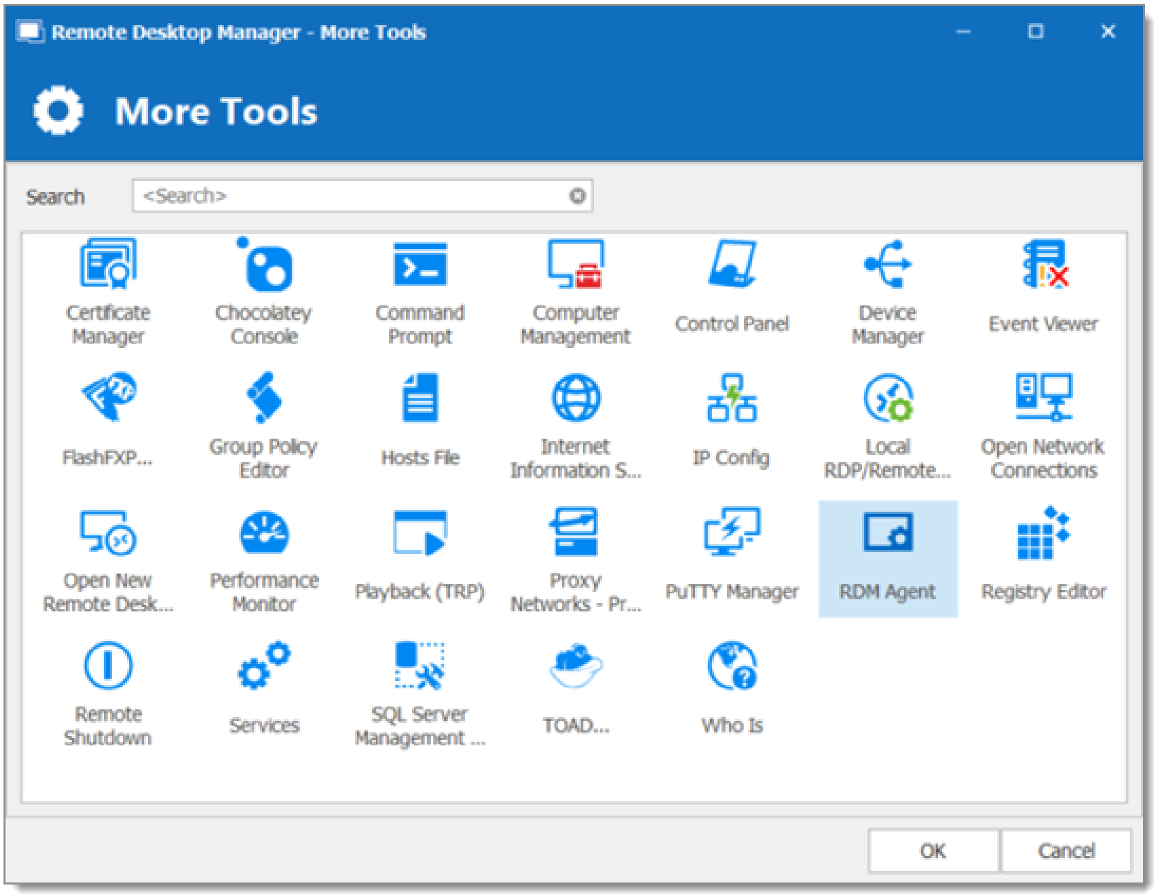
> ***Auto Start*** must only be activated for the Remote Desktop Manager Agent or Remote Desktop Manager but not for both. In the case where Remote Desktop Manager is set to ***Auto Start*** please make sure to delete the shortcuts form either/both the following locations:
>
> - Run: *shell:startup*
> - Run: *shell:common startup*

a. Go to ***Tools - More Tools***.

b. Select Remote Desktop Manager Agent.

c. Click ***OK***.

d. Click ***Yes***.



8. Right-click the Remote Desktop Manager Agent icon in the taskbar.

   a. Check ***Auto Start***.

9. Adjust the user interface of the ***Jump Host*** to maximize the area to display remote sessions.

- Make the application full screen.
- Hide the ***Navigation Pane*** in the ***View*** tab.
- Hide the ***Ribbon*** in the ***View*** tab.
  - To show the ***Ribbon*** again, click the Remote Desktop Manager icon at the top left corner.

> To reset the layout, in the ***Window*** tab, click ***Reset Layout***.

The ***Jump Host*** is ready to use.

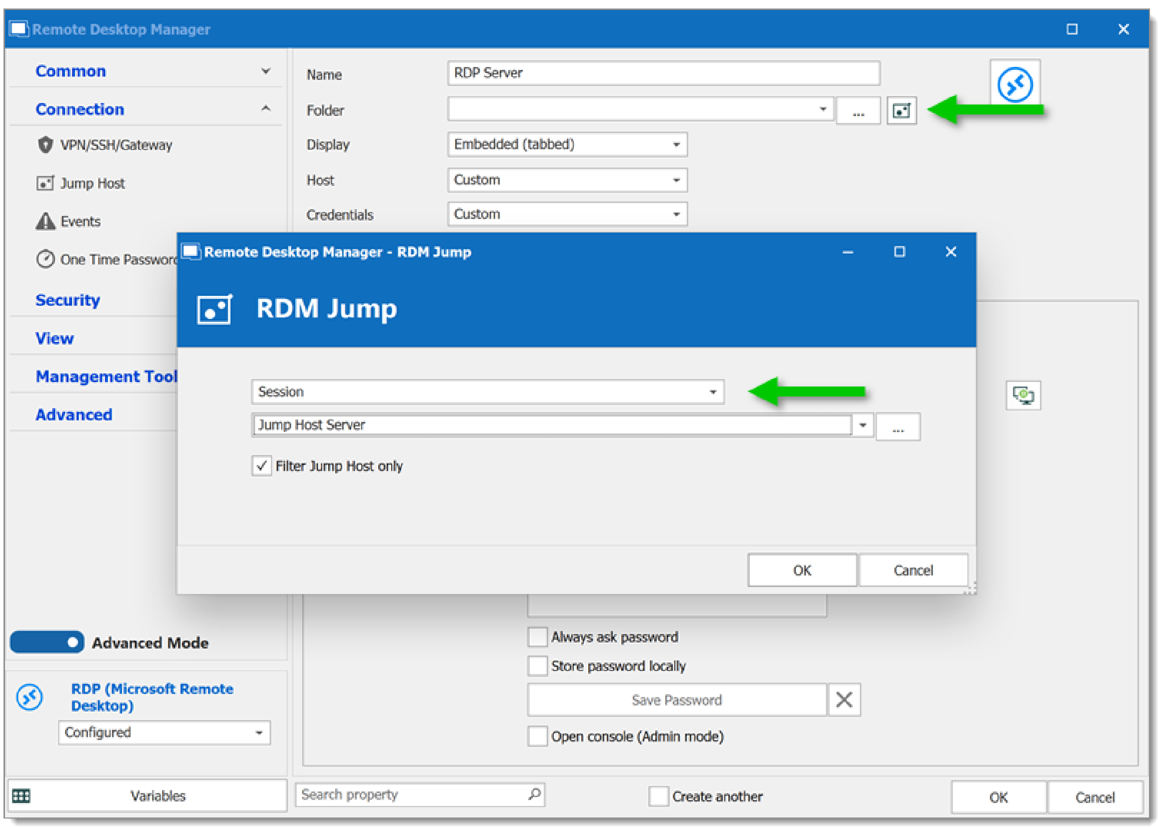
CONFIGURE A SESSION TO USE THE JUMP HOST

1. Create an ***RDP*** entry, on the local Remote Desktop Manager instance.
2. Set the ***Jump Host*** by clicking on the ***RDM Jump settings*** button.

- The ***Jump Host*** can be ***Inherited*** if it is defined in the parent folder.

Or

- Choose a specific ***Session*** to point directly to the ***Jump Host*** entry.



3. Click ***OK*** twice.
4. Launch the RDP session. The Remote Desktop Manager Jump opens automatically and it looks like a session in a session.

VALIDATE THAT THE JUMP HOST WORKS

1. Start the ***RDP*** session of the ***Jump Host Server***.
2. Wait for Remote Desktop Manager Agent to connect.
3. On the ***RDP*** tab, right click ***Agent Status***.
   a. Remote Desktop Manager Agent should be connected.
4. Keep the ***RDP*** tab open.
5. Start the ***Jump*** session.
   a. ***Jump*** session should start on the ***Jump Host Server***.
6. Close all sessions.
7. Start the ***Jump*** session directly.
   a. ***Jump Host Server*** & ***Jump*** session should both start.

All should be working correctly. If any of the steps fails, it is where you need to investigate.

PRO TIPS

- To gain more space for the dashboard, in the ***View*** tab, hide the ***Ribbon*** and ***Navigation Pane*** since the menus are not needed.
- Use the same Remote Desktop Manager license on the local and the remote instances. The Jump Host acts as a relay between the local and the remote systems, allowing to use the Remote Desktop Manager license that has been used on the local workstation to register the application on the Jump Host.
- There is no need to create a data source on the Jump Host. Remote Desktop Manager will open for the first time with a default ***SQLite Local Data Source***. This is sufficient because the application on the Jump Host only acts as an intermediate between the local and the remote hosts.

Getting Started

Part II

2 Getting Started

2.1 Using Remote Desktop Manager

DESCRIPTION

Remote Desktop Manager is highly flexible and can work for both individuals and teams. Please follow the checklist that applies to your environment:

- Checklist for Individuals: For individuals but also for teams of three users or less that do not want to implement security.
- Checklist for Teams: For a team environment that wishes to implement security.

2.2 Checklist for Individuals

DESCRIPTION

Here's a checklist to help you get started with Remote Desktop Manager for individuals.

CHECKLIST FOR INDIVIDUALS (ENTERPRISE EDITION)	DESCRIPTION
Step 1 - Register your license: • Enterprise Registration • Trial Registration	Remote Desktop Manager Enterprise Edition grants you a 30-day trial. If you decide not to register by the end of the trial, your data will not be altered or erased, and you will have full access to it once you provide a license key. Here is a video link to assist you: 

CHECKLIST FOR INDIVIDUALS (ENTERPRISE EDITION)	DESCRIPTION
Step 2 - Add your Data Source and set up your Devolutions account and a master key.	Warning: When choosing any data source type that is not **on-premises**, you need to think about the safety of the data at rest and during transport. We strongly recommend that you further encrypt your data by applying a master key for file-based solutions, or a Security Provider for Advanced Data Sources. This ensures **only you** can read the data. Upon first launch, Remote Desktop Manager uses a local SQLite data source. The different data sources are explained in the Data Sources section. For help selecting a data source tailored to your needs, please see Choosing your data source (Individuals). Here is a video link to assist you: Watch Video
Step 3 - Set up your Devolutions Online Backup.	Devolutions Online Backup allows you to securely back up your information for selected data sources. The backup is automatically executed 30 seconds after any modifications made to the data source content. It is best practice to always back up your data source. Here is a video link to assist you: Watch Video
Step 4 - Create your Default Settings.	In ***File - Options***, you can create, modify or reset default settings for your templates. Each entry type is supported and can have a default template defined to fit your requirements. Here is a video link to assist you: Watch Video
Step 5 - Create your folder structure.	Top level folders are at the foundation of a solid security structure. Your folder structure (folder entries) should represent your company structure.

	CHECKLIST FOR INDIVIDUALS (ENTERPRISE EDITION)	DESCRIPTION
		Here is a video link to assist you: Watch Video
	Step 6 - Import your Data.	The final step is to import all of your data into Remote Desktop Manager. You can import your sessions, logins and contacts in a few steps. Here is a video link to assist you: Watch Video

2.2.1 Select the Data Source type - Individuals

DESCRIPTION

This topic is primarily intended for individuals, but also for teams of three (3) users or less who do not wish to set up security.

To help you select a data source, here is a set of concerns and the list of data sources that can serve in such context. If you have multiple concerns, simply create the intersection of all sets to isolate a list of choices.

> When choosing any data source type that is not **on-premises**, you need to think about the safety of the data at rest and during transport. We strongly recommend that you further encrypt your data by applying a master key for file-based solutions, or a Security Provider for Advanced Data Sources. This ensures **only you** can read the data.

DATA SOURCE	LOCAL	SELF-HOSTED	CLOUD-BASED	SHARED BETWEEN YOUR COMPUTERS	WORKS OFFLINE	MULTI-USER
Devolutions Password Hub Personal			X			
SQLite	X				X	
XML	X				X	
Devolutions Online Drive			X	X	X	
Dropbox			X	X		Note 1

NOTES

NOTE 1

There is no protection against data contention issues. The data source is designed for one user to access the data from multiple computers. It is therefore impossible for several users to use the data simultaneously.

NOTE 2

The master XML is maintained by a single user and synchronized by Remote Desktop Manager to a web site that is hosted as per your requirements. Accessing the data through a URL ensures it is read-only for other users.

2.3 Checklist for Teams

DESCRIPTION

Here's a checklist to help you get started with Remote Desktop Manager when working in a team environment.

CHECKLIST FOR TEAMS	DESCRIPTION
Step 1 - Register your license: • Enterprise Registration • Trial Registration	Remote Desktop Manager Enterprise Edition grants you a 30-day trial. If you decide not to register by the end of the trial, your data will not be altered or erased, and you will have full access to it once you provide a license key.
Step 2 - Add your Data Source (for teams).	Warning: When choosing any data source type that is not **on-premises**, you need to think about the safety of the data at rest and during transport. We strongly recommend that you further encrypt your data by applying a master key for file-based solutions or a Security Provider for Advanced Data Sources. This ensures **only you** can read the data. Upon first launch, Remote Desktop Manager uses a local SQLite data source. The different data sources are explained in the Data Sources section. For help selecting a data source tailored to your needs, please see Choosing your data source (Teams).
Step 3 - Select your Security Provider.	Select your Security Provider before importing or creating any data in your database so nobody can read your entry configuration data, even when people have a direct access to your database.
Step 4 - Create your folder	Top level folders are at the foundation of a solid security structure. Your folder structure (folder entries) should

CHECKLIST FOR TEAMS	DESCRIPTION
structure.	represent your company structure. For example, you can create a folder for your Production team, one for your Staging team and one for your Testing team. Here is a video link to assist you: Watch Video
Step 5 - Create your Default Settings.	In ***File - Options*** you can set options for Remote Desktop Manager and create default settings Templates. Each entry type is supported and can have a default template defined to fit your requirements. After you configure the options, use the Custom Installer to share the pre-configured version with your team.
Step 6 - Create Users.	Remote Desktop Manager supports advanced User Management. User accounts must be created manually by an administrator of the database.
Step 7 - Create User Groups.	Create User Groups to manage your security system. You can then assign users to User Groups, making it easy to grant permissions to a set of users instead of having to manage permissions individually.
Step 8 - Create Entries.	An entry is how you save information about your sessions (e.g. RDP, SSH connections), credentials, websites, VPNs, synchronizers and documents.
Step 9 - Grant Permissions.	Once your users are created, you can then grant Permissions for user group-based access control. The permissions granted on the folder can be inherited by each entry set under that folder.
Step 10 - Import your Data.	The final step is to import all of your data into Remote Desktop Manager. You can import your sessions, logins and contacts in a few steps.

2.3.1 Select the Data Source type - Teams

DESCRIPTION

This topic is for teams that use the functionality offered by our Enterprise Edition.

When choosing any data source type that is not **on-premises**, you need to think about the safety of the data both at rest and during transport. We strongly recommend that you further encrypt your data by applying a master key for file-based solutions or a Security Provider for Advanced Data Sources. This ensures **only you** can read the data.

To help you select a data source, here is a set of concerns and the list of data sources that can serve in such context.

CONCERN	DEVOLUTIONS SERVER	SQL SERVER	SQL AZURE
Database not accessible to end users	X	Note 1 and 2	Note 1
AD accounts used for authentication	X	X	
AD group membership used to assign permissions	X		
Data stored on-premises	X	X	
Activity Logs	X	X	X
Data accessible globally	Note 3	Note 4	X

CONCERN	DEVOLUTIONS SERVER	SQL SERVER	SQL AZURE
Optional local cache of connections	X	X	X

NOTES

NOTE 1

Administrators can create accounts for end users without divulging the passwords. A locked data source definition is imported for each end user. This requires a lot of manual operations by the administrator.

NOTE 2

Integrated security is the name of a Microsoft technology that allows access to an instance of SQL Server without sending credentials, but rather by using the token provided by the authentication in your Windows computer. This therefore allows the users to connect directly to the database using other tools. It should not be used if you need to prevent direct access to the database.

Our SQL Server data source offers a third authentication option, namely the Custom (Devolutions) user type. It allows for the user to be impersonated and therefore not be made aware of the credentials used to connect to the database. Please consult User Management for details.

NOTE 3

You should not expose a Devolutions Server instance to the Internet without being able to protect it from DDoS attacks. Strong passwords must be used as well as obscure account names that are not easily inferred using social data mining.

NOTE 4

You can indeed expose a database to the Internet, but you must use SSL/TLS to encrypt traffic and also protect against DDoS attacks. Cloud services like Azure have that concern in the forefront. The default settings of the firewall should be to block everything and then add exceptions and rules. It is also necessary to open the minimum number of required ports, add the numbers of these ports to the exception list and filter all future requests based on their origin.

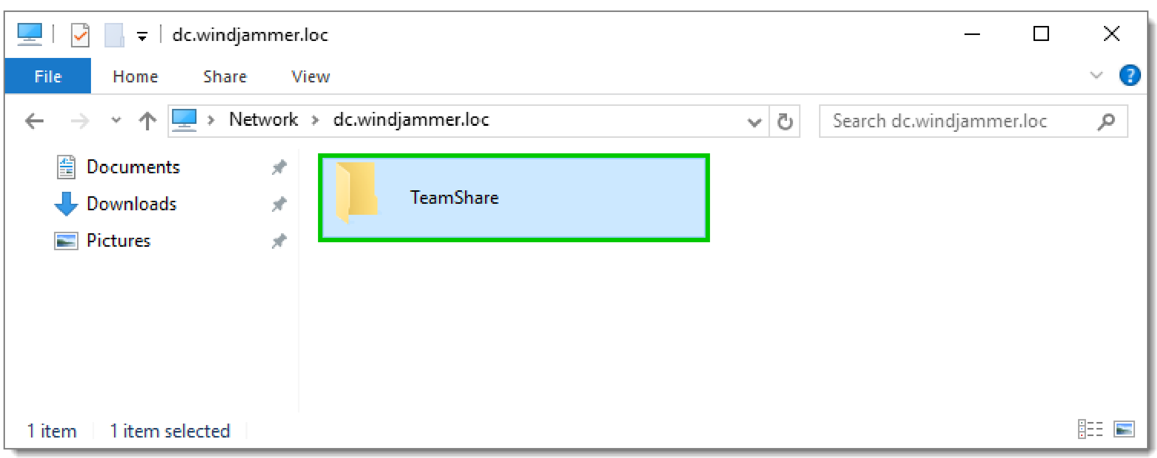
2.3.2 Set up a team folder for default settings

DESCRIPTION

You must create a team folder on a server drive to store your default settings templates in order to share them with your team.

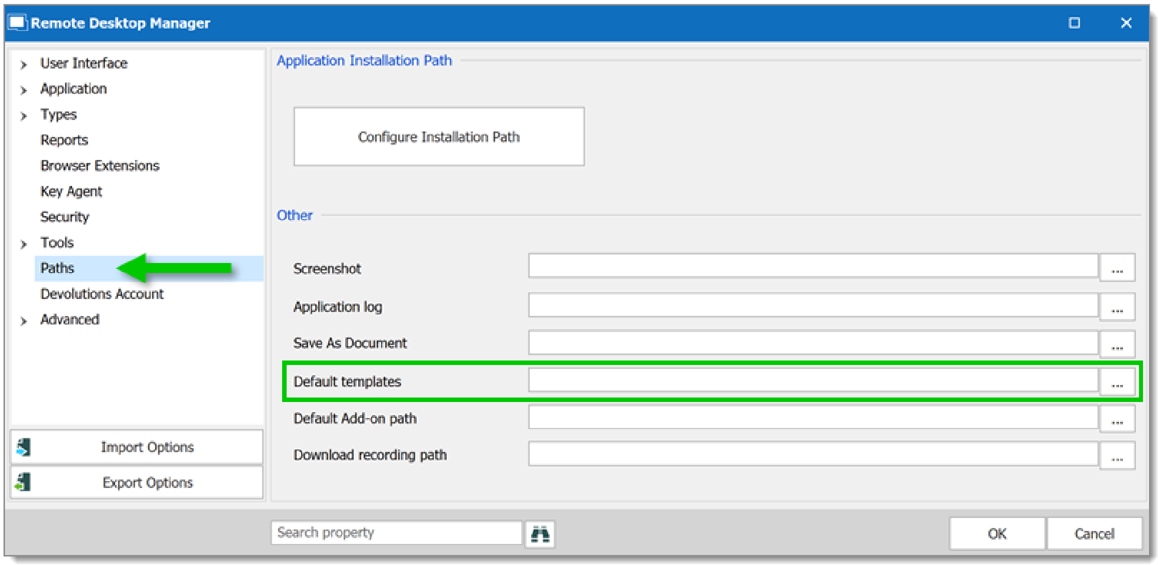
SETTINGS

1. Start by accessing your server drive (such as \\servercommon) and create a new team folder to hold all your team default settings templates.



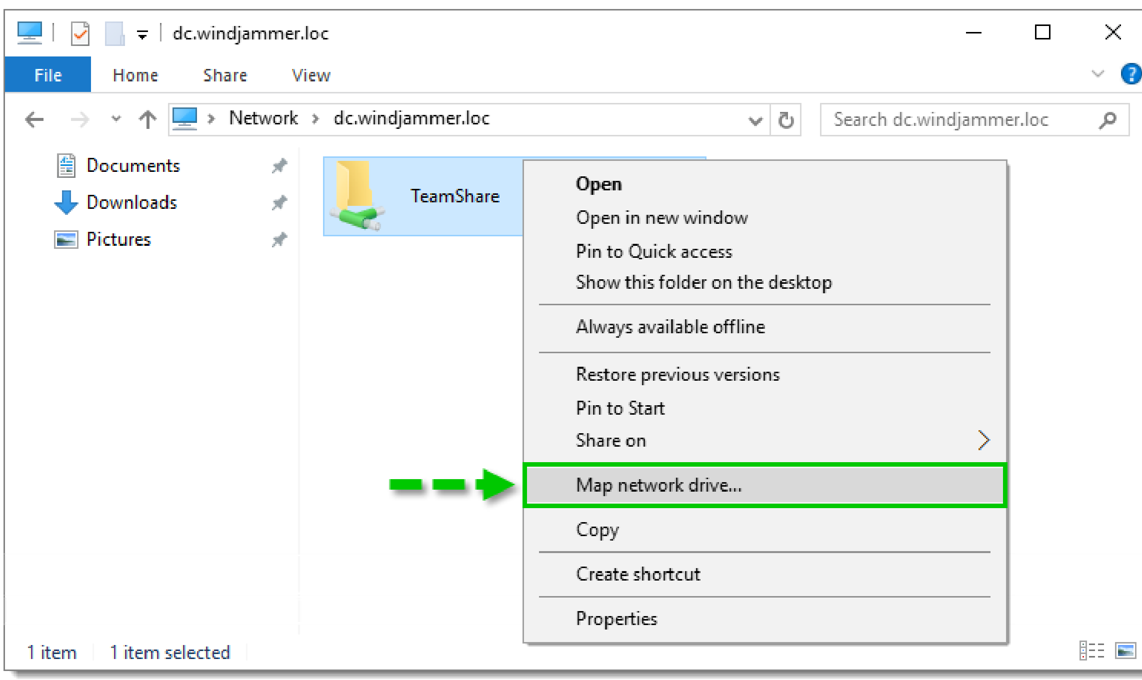
Server Drive - Team Folder

2. Go to ***File - Options - Path*** and enter the path of your newly created folder stored on your server drive. All your default templates will then automatically be saved in that folder.



File - Options - Path

3. If you have remote workers, ensure they have access to the shared server in offline mode. Map your network drive and then follow the instructions here for the offline mode access when using Windows 11/10.



Map Network Drive

2.4 Managing Credentials

DESCRIPTION

Depending on your organization's security policies, there are multiple ways of handling credentials. We can manage a wide range of scenarios; the most popular are listed below. It is critical to understand that these are the credentials used to connect to remote hosts, not the ones you use to launch Remote Desktop Manager.

> Most of these selections do not exist in the **Free** edition of Remote Desktop Manager as they depend on features offered by an Advanced Data Source.

Below are a few key points that the admin of the solution must be aware of:

Password visibility	You can store passwords in a **credentials** entry (username/password entry), which, by default, makes the password **usable** but **not visible** by the end user. We provide multiple credentials entry types. You should always consider carefully which type you are using based on your administrative and security needs.
Credentials set on folders	Our folders can have defined credentials. This is useful because, in most cases, the same credentials are reused for an entire branch of the network infrastructure. To use credentials defined in a folder, child sessions must be adjusted to use **inherited credentials**.
Entry location	When storing entries in the tree view, users with the **View** permissions on that entry (or folder by inheritance) will be able to use them. This is how you would share credentials with other members of your team. A User Vault exists for users to store personal information that should be seen by no one else. Credentials stored in this manner can still be accessed in the public area of the system by referencing them or through the **User Specific Settings** feature described below.
User Specific Settings	User Specific Settings are **partial overrides** for your entry settings, including credentials. When you apply such an override,

	you can choose the type of credentials **directly** in the override or you can choose to instead link to credentials stored elsewhere, such as the User Vault.

Here are the most common scenarios and ways to resolve them. In the majority of cases, we prefer sessions to use **inherited credentials**, which means they climb the tree until they have access to a set of credentials, whether defined, linked, or overridden in an entry.

SCENARIO	STRATEGY
One set of credentials is used by all of the staff, be it for the whole system or for a branch in your tree view (customer, department, etc.).	Set the credentials on the Vault Settings. All children use **inherited credentials**.
Each user has their own credentials for many different branches (often corresponding to customers/departments, etc.).	Make use of the User Specific Settings on each branch. All children use **inherited credentials**.
Each user has its own credentials managed by an administrator.	This solution involves a little more work. The administrator must create a folder for each user, then grant permissions only to that user. The user will then use User Specific Settings to specify that the credentials stored in that folder are used to override what is defined in the entries.
Each team uses the same credentials.	As above, but all team members have access to the folder. They all have to use the User Specific Settings.
Each user uses their domain account.	Configure sessions to use My Personal Credentials. Each user will be prompted to define them once per workstation that they use.

Installation

Part

III

3 Installation

3.1 Client

DESCRIPTION

Remote Desktop Manager can be downloaded as setup files, or as a binary compressed (zip) file.

INSTALLATION

Depending on the downloaded media, either run the setup, or extract the files from the archive in any folder and launch the executable. If you wish to use a portable device, or run multiple independent copies of the application, please consult Portable (USB).

LICENSE

Remote Desktop Manager Enterprise Edition comes with a 30 day-trial. If you possess a purchased license of the Enterprise Edition, please follow the instructions at Register Enterprise Edition. To register the Free Edition, please refer to the Register Free Edition.

DATA SOURCE

By default, a local data source is created using the SQLite format. You can add as many data sources as needed. Please consult Data Source Overview for more information.

> To use a SQL Server or Azure SQL data source, refer to the Configure SQL Server topic.

EXTERNAL APPLICATIONS

Configure your installation path for all external applications you intend to utilize such as RealVNC, Putty, Filezilla, etc. Set the paths in ***File – Options – Path.***

REMOTE DESKTOP SERVICES

Please consult the Remote Desktop Services topic.

3.1.1 Ancillary Files

DESCRIPTION

Remote Desktop Manager generates ancillary files on your workstation. The table below lists out an example of ancillary files and their locations.

As described in Configuration File Location, the default path for most of these files are customizable. For this reason, we use the ***[CONFIG]*** token in this documentation to denote when a file is stored in a configuration folder that can be relocated, or the ***[PROFILE]*** token to indicate that they are stored in the local profile. By default, these point to the **same exact folder**. The only method to separate them is by using a customized configuration.

Since you can also deploy on a portable device, sometimes known as using the XCOPY deployment model, we will use the ***[INSTALLDIR]*** token to indicate that the file is in the same location as Remote Desktop Manager.

The ***Override Source*** column indicates if an available mechanism can relocate the files of that category elsewhere.

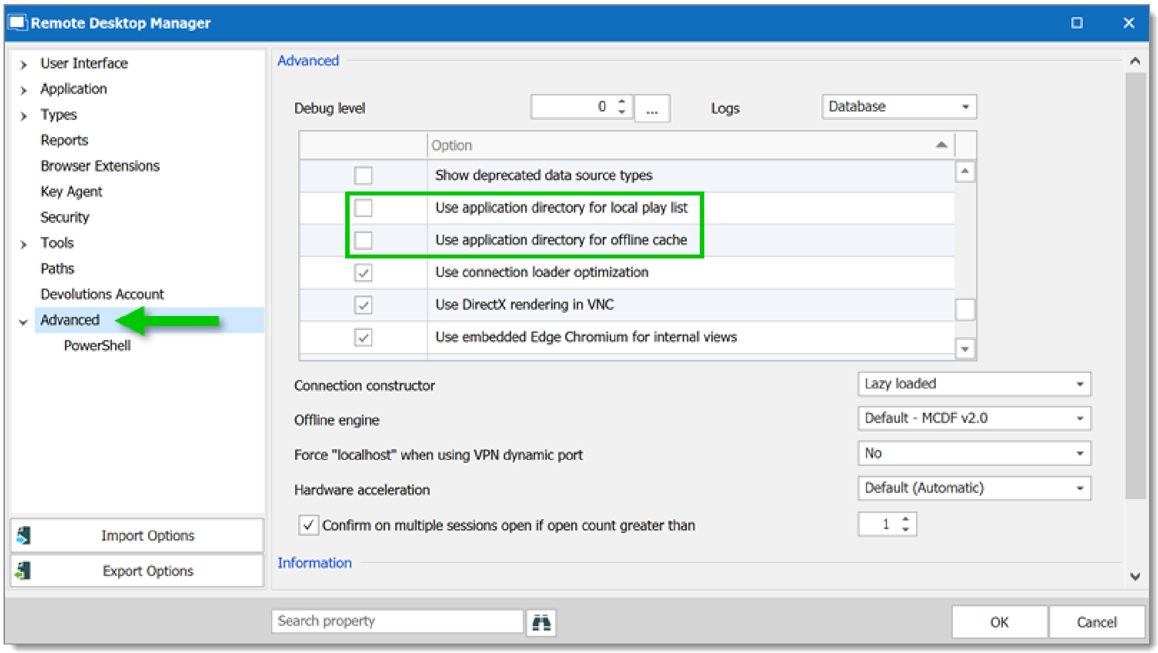
SUMMARY

FILE(S)	LOCATION	OVERRIDE SOURCE
Configuration File(s) (*.cfg, *.ext)	[CONFIG]	None
Data File(s) (*.xml, *.db)	[CONFIG] or custom path.	None

FILE(S)	LOCATION	OVERRIDE SOURCE
Default Settings	[CONFIG]	Data source settings (System Settings)
Encryption (*.enc, *.enb)	[CONFIG]	None
Layout Files (*.lyt)	[CONFIG]	None
Log Files (*.log, *.debug)	[CONFIG]	None
Local Play lists	[PROFILE] \[Datasource]\Playlists	***Use application directory for local playlist*** will use instead [INSTALLDIR]
Local Templates	They are serialized directly in the configuration file of the application.	None
Offline/Cache data (offline.db)	[PROFILE] \[Datasource]	***Use application directory for online cache*** will use instead [INSTALLDIR]
Sensitive (*.stv, *.stb)	[CONFIG]	None
Themes	[CONFIG]	None

OFFLINE AND LOCAL PLAY LIST OPTION

Offline and local play list options can be accessed by navigating to ***File - Options - Advanced***.



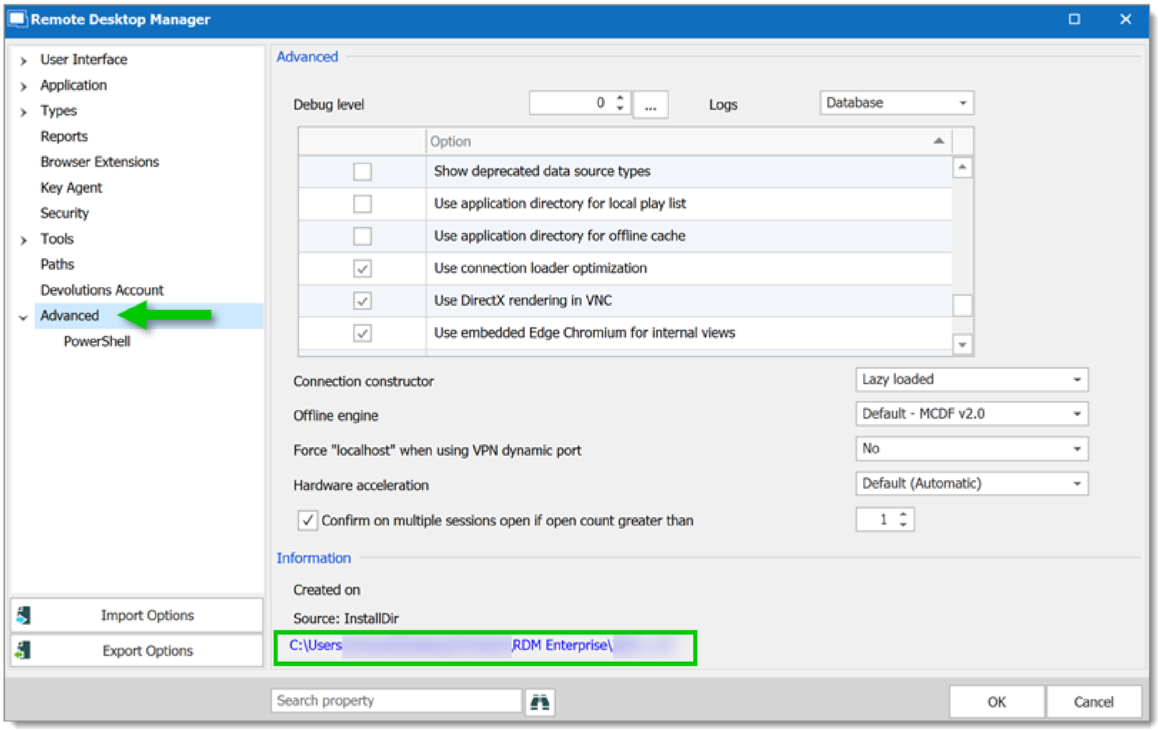
Options - Advanced

3.1.2 Configuration File Location

DEFAULT LOCATION

Remote Desktop Manager saves its configuration in a file named RemoteDesktopManager.cfg. This file contains most of the application settings.

> You can retrieve the installation folder of Remote Desktop Manager by clicking ***File – Options – Advanced***. A hyperlink displays the installation folder.



Options - Advanced

The configuration file can be located in different folders depending on certain conditions:

CASE	CONFIGURATION FILE LOCATION
Installed under "Program Files" or "Program Files (x86)"	`%LocalAppData%\Devolutions\RemoteDeskt`
Application running on Terminal Server	`%AppData%\Devolutions\RemoteDesktopManager`. This is the roaming profile and avoids multi-user conflicts.
Other	Installation folder

OVERRIDE THE DEFAULT PATH

There are two ways to change the folder where the configuration file is stored:

1. Create a file named **"Override.cfg"** in the application folder. Remote Desktop Manager opens this file and reads the first line. It should contain the desired installation folder (without the file name). If you wish to use the current installation path, put a period in the file. Here are a few examples:

EXAMPLES	
c:\RDM	The config file is saved in the designated folder.
.	The period is used to specify the Remote Desktop Manager installation folder.
%AppData%\Devolutions\RemoteDesktopManager	Specify the application roaming data folder.

2. By adding a key in the registry: **CurrentUser\SOFTWARE\RemoteDesktopManager, OptionPath**. Set the desired path in the key **OptionPath**. You must not include the file name in the value, just the path.

DEFAULT CONFIGURATION FOR REMOTE DESKTOP SERVICES ENVIRONMENT

Please refer to Remote Desktop Services for details.

3.1.3 Custom Installer Service

DESCRIPTION

- Generate and download custom installation packages for Remote Desktop Manager.
- Include preconfigured data sources in the package for quick enterprise wide deployment.
- Insert license serial in the installation package for easier management.
- Download the installer as a Windows Installer (.msi file).

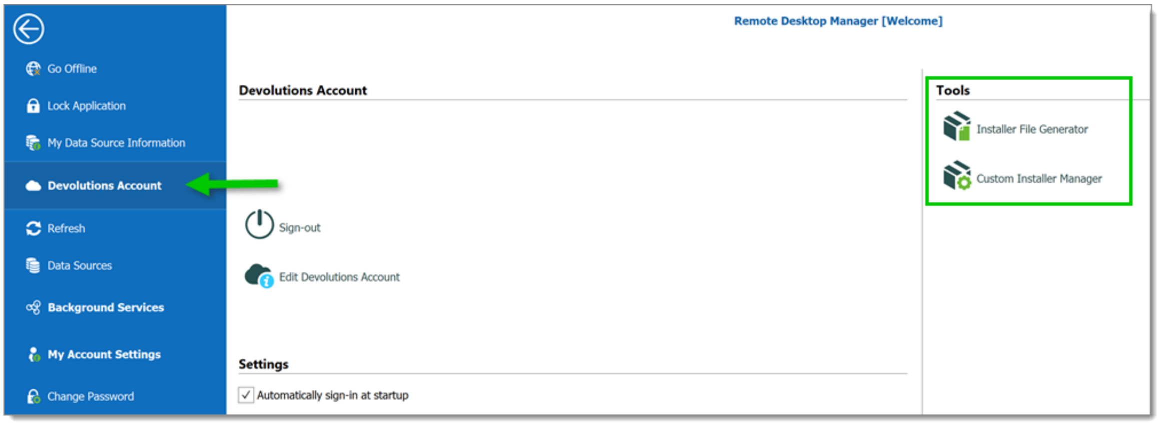
The Custom Installer Service, offered through our Devolutions Customer Portal services, replicates the configuration from a Remote Desktop Manager instance. This configuration is used to create an installer file (*.rdi), which will be used to create the installation package intended for distribution. The configuration can contain the license serial, data sources, credentials, database templates and more. It is best practice to have a Remote Desktop Manager installation used specifically to create the installation package.

> The Custom Installer Service uploads a configuration file to our online services. You should not use the service to redistribute passwords for data sources.

> Please note that you ***MUST*** create an installer file using Remote Desktop Manager before creating the installer on the Web portal. This is described here in the Installer File Generator topic.

> You can store and create up to 6 ***Custom Installer*** configuration file package in your Devolutions account.

The Custom Installer Service can be found in with the Devolutions Account tools, located in ***File - Devolutions Account - Tools***. You must be signed in to access it.



File - Devolutions Account - Tools

The following topics will help you get started to set up your customized installers with Remote Desktop Manager.

- Create an Installation Package
- Installer File Generator
- Option Selection Dialog

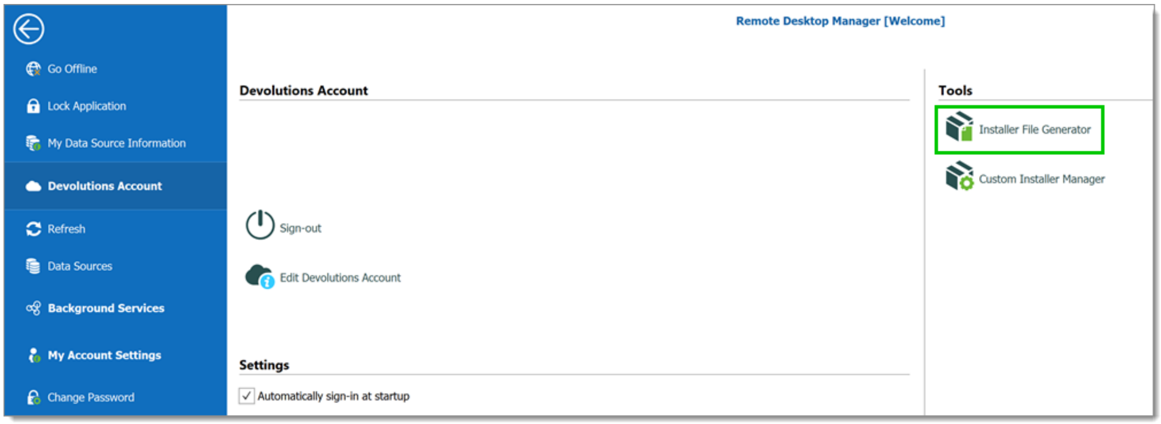
3.1.3.1 Installer File Generator

DESCRIPTION

When creating an installation package with the ***Custom Installer Manager***, an installer file is necessary to determine what to include in the installation configuration. It is risky to create an installer file for each new version since you have to repeat the process manually every time. Instead, it is possible to create the configuration once, save the resulting file (*.rdi), and reuse it as many times as needed.

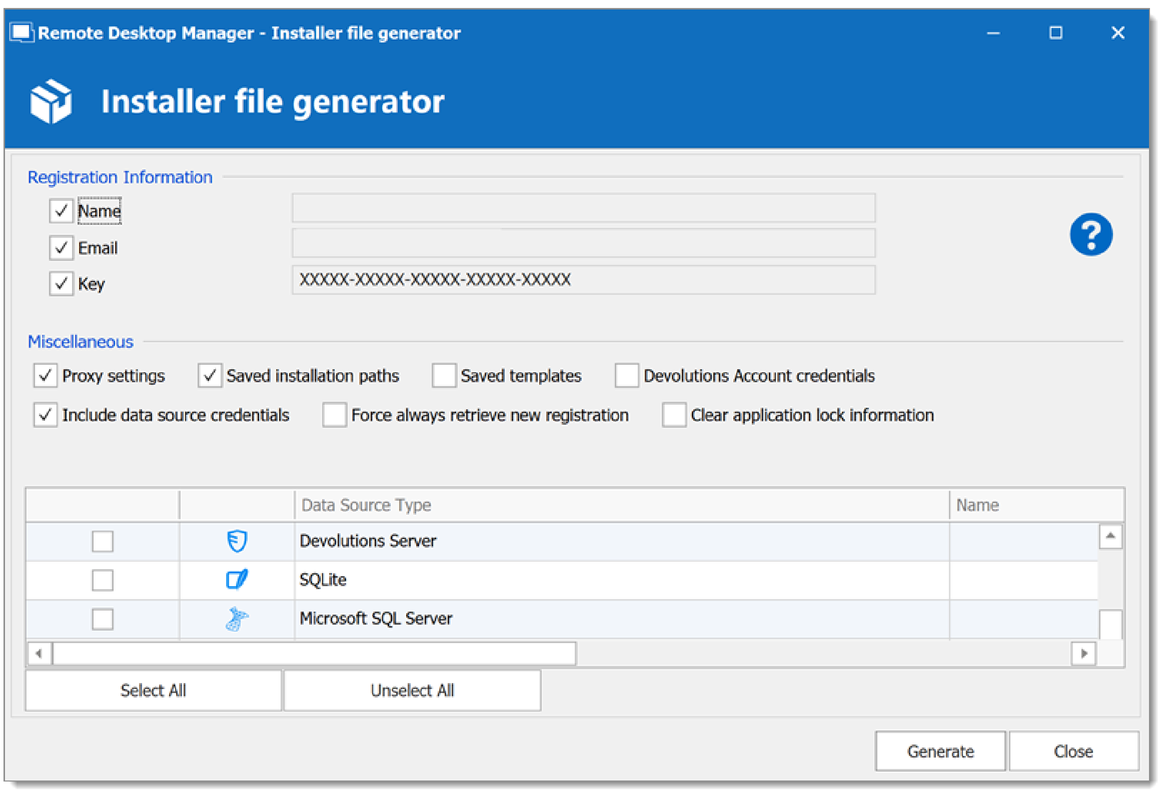
CREATING AN INSTALLER FILE

1. Click on ***File - Devolutions Account - Installer File Generator.***



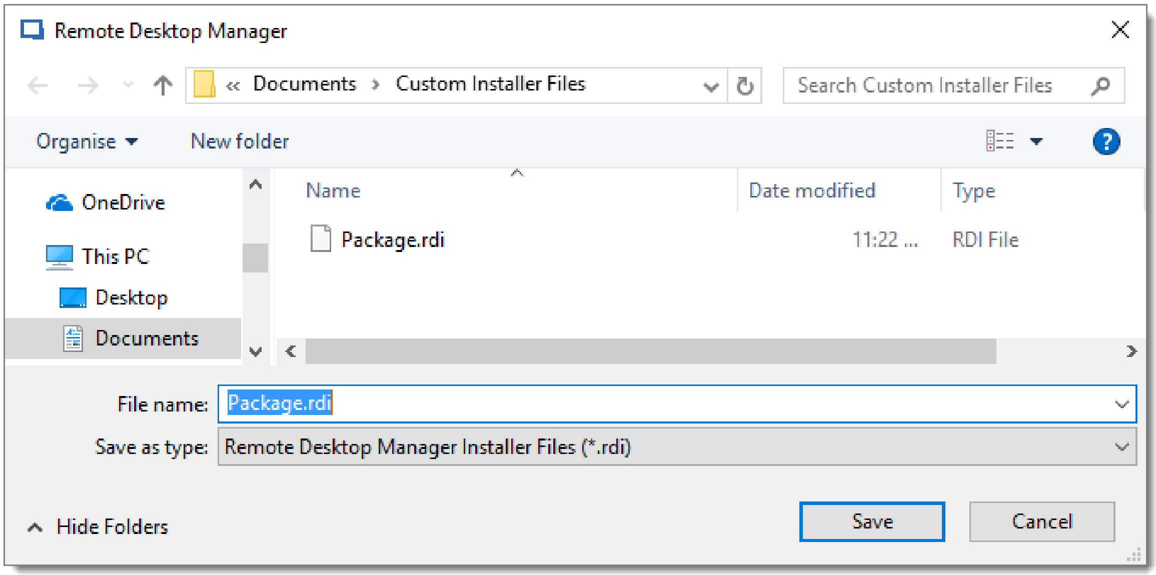
File - Devolutions Account - Installer File Generator

2. Select which data sources to include. You can also include the name and serial key for the registration.



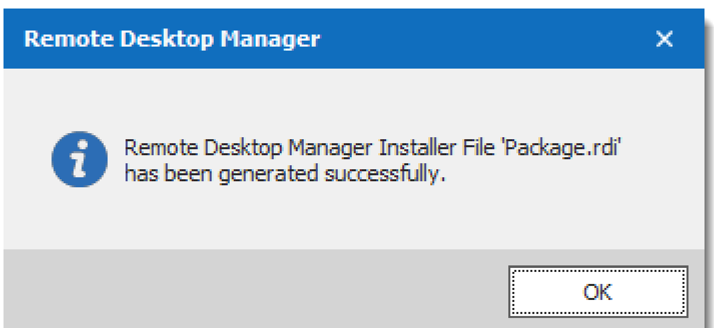
Installer File Generator

3. Click ***Generate*** and save the file.



Save the installer file

An information dialog is displayed when the file has been generated.



Package.rdi has been generated successfully

This file can be used in the ***Custom Installer Manager*** when creating an installation package.

For more information on how to create a custom installer package, please consult our Custom Installer Manager topic.

3.1.3.1.1 Option Selection Dialog

DESCRIPTION

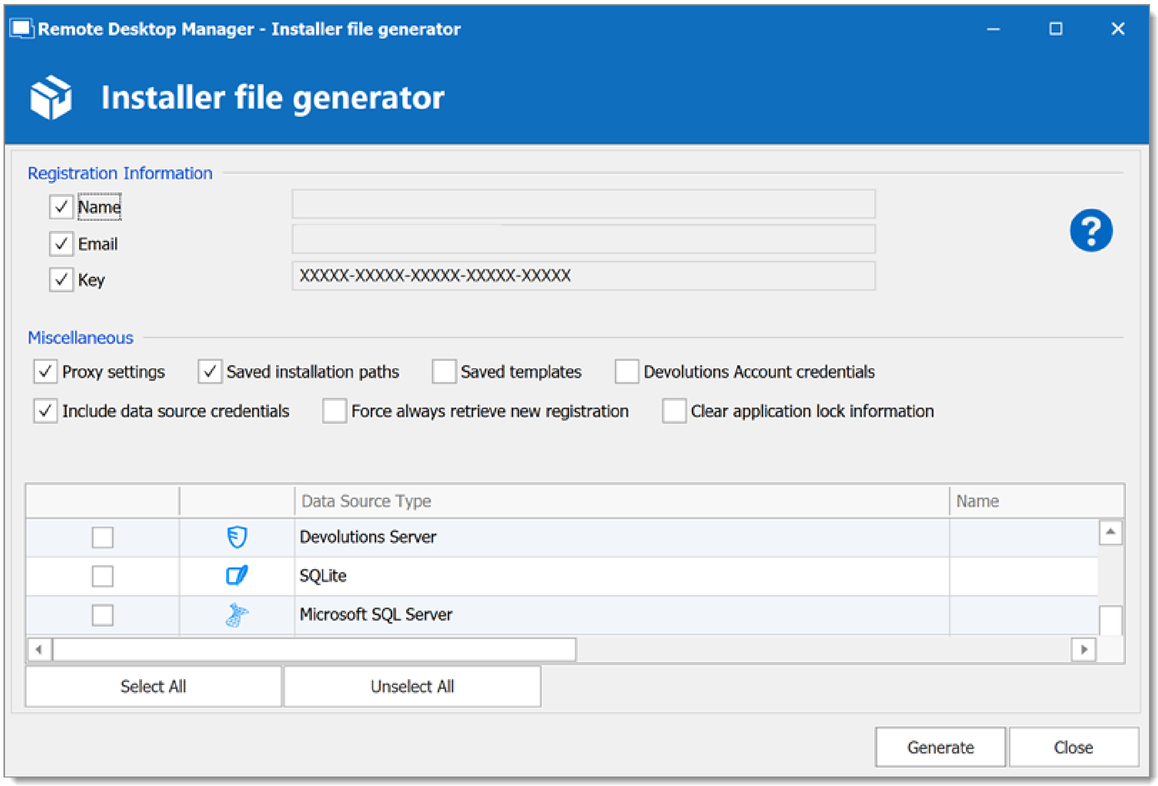
When generating the installer file, you must decide what to include in the configuration. This process will replicate the configuration of the Remote Desktop Manager instance currently used, and will generate an installer file (*.rdi). Once it has been generated, the installer file can be used as many times as needed to create custom installers. For security reasons, some settings that may contain credentials, such as ***Saved Templates***, are disabled by default. Enable these at your own risk.

> The same dialog is used for the Custom Installer Service and for exporting the Remote Desktop Manager configuration file. Some options must NOT be used for the Custom Installer Service to prevent sharing credentials that must stay confidential. Please read the documentation carefully.

> Remote Desktop Manager may install required add-ons automatically when it detects that they are needed (configured in ***File - Options - Paths***). If you need to customize the application's installation path of an Add-on, you must perform the modification, then create the installation package. This setting will be replicated in the installer file (*.rdi).

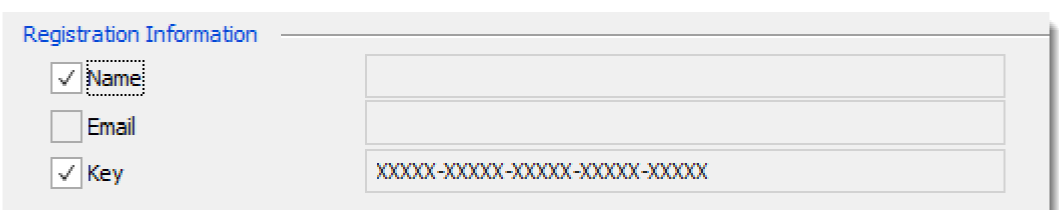
SETTINGS

You can open the ***Installer File Generator*** from ***File - Devolutions Account - Installer File Generator***.



Installer File Generator

REGISTRATION INFORMATION



Installer File Generator - Registration Information

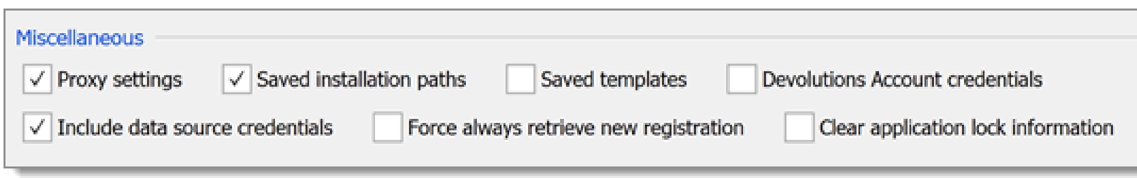
OPTION	DESCRIPTION
Name	Company registration name.
Email	Registration email if using a generic address.
Key	License serial.

MISCELLANEOUS

Do not redistribute the ***Devolutions Account credentials***. Doing so would share these to ALL users having access to the online account used to create the installer package.

All ***Local templates*** will be included. If any contain credentials, it may cause a security risk. Ensure you are sharing only what is needed.

The data sources you decide to redistribute should **NOT** contain identifiable credentials. Use of integrated security is highly recommended. You can also use environment variables for the username.



Installer File Generator - Miscellaneous

OPTION	DESCRIPTION
Proxy settings	Includes your Internet proxy settings
Saved installation paths	Preserves your installation paths configured for external third party applications. Use this only when all of the user's machines use the same paths.
Saved templates	Includes your local templates in the custom installer. Database templates are stored in the data source and may be a better option in you need to share them.

OPTION	DESCRIPTION
Devolutions Account credentials	Includes your Devolutions Account credentials used to create the custom installer. Please, consult security warning above.
Include data source credentials	Includes the credentials for all selected data sources below. Please, consult security warning above.
Force always retrieve new registration	Will allow the administrator to force the users to use this new configuration file.
Clear application lock information	Will clear the information from ***File - Options - Security - Lock application*** (local).

DATA SOURCES

Select the data sources that must be included in the configuration. In the description column, you will see details about each data sources. You should **ONLY** share data sources that are either using **Integrated Security**, or that are using an environment variable for the username. Passwords for accessing a data source should **NEVER** be shared.

3.1.3.2 Custom Installer Manager

DESCRIPTION

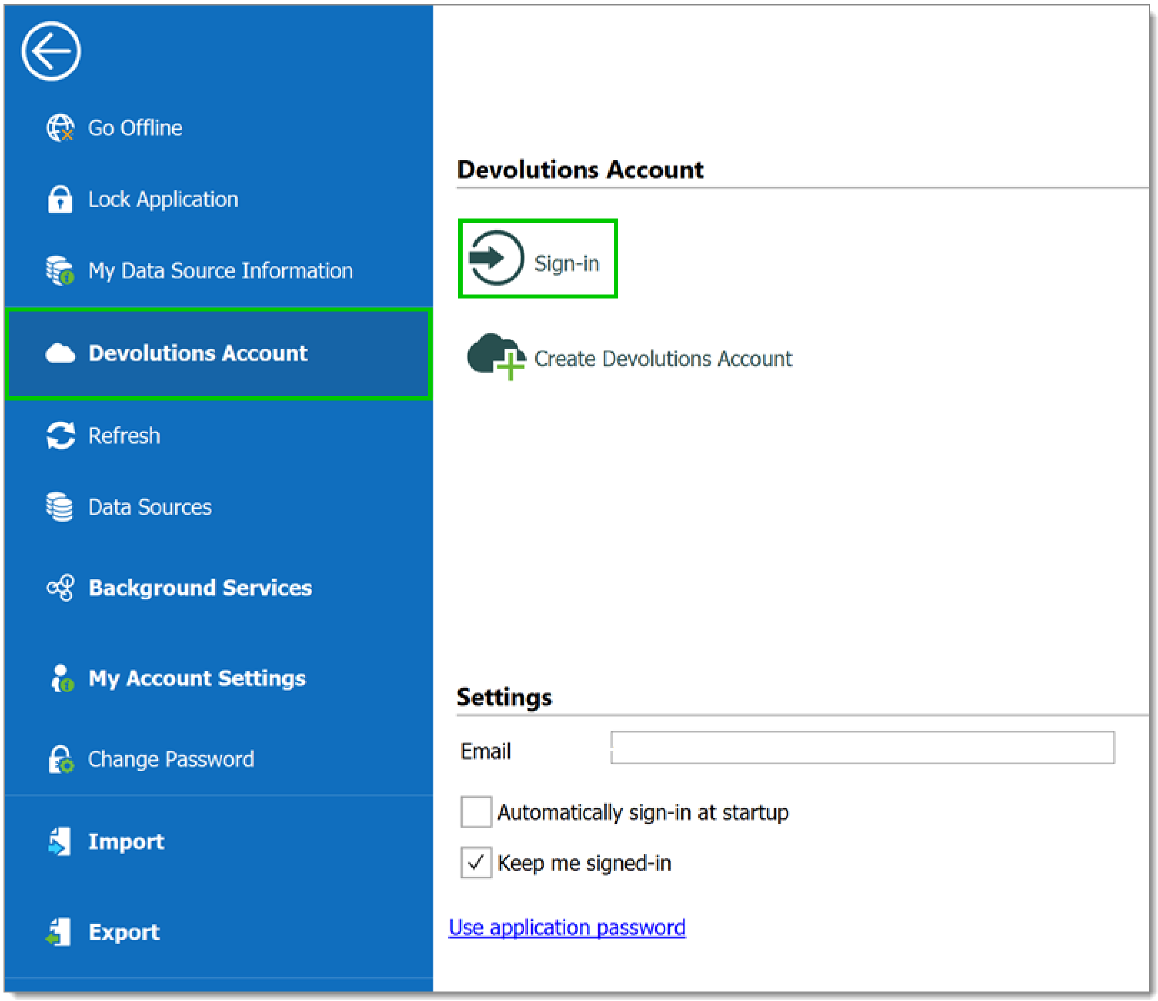
For stability reasons, in large installation bases, the latest official release is not available to the Custom Installer Service for an undetermined period while we ensure that no major issues are present. We recommend using this time with your organization to perform integration tests on a few workstations before upgrading your entire team.

Please ensure you have read and understood the content of Custom Installer Service Overview prior to subscribing to the service.

You can store and create up to 6 ***Custom Installer*** configuration file package in your Devolutions account.

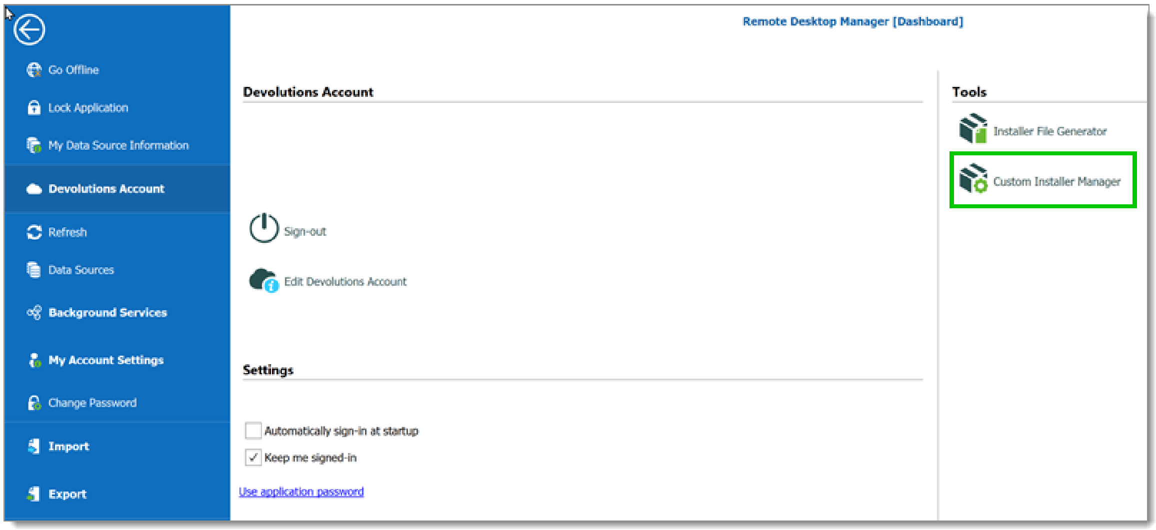
CREATE AN INSTALLATION PACKAGE

1. Click on ***File - Devolutions Account - Sign-in*** to connect to your ***Devolutions Account***.



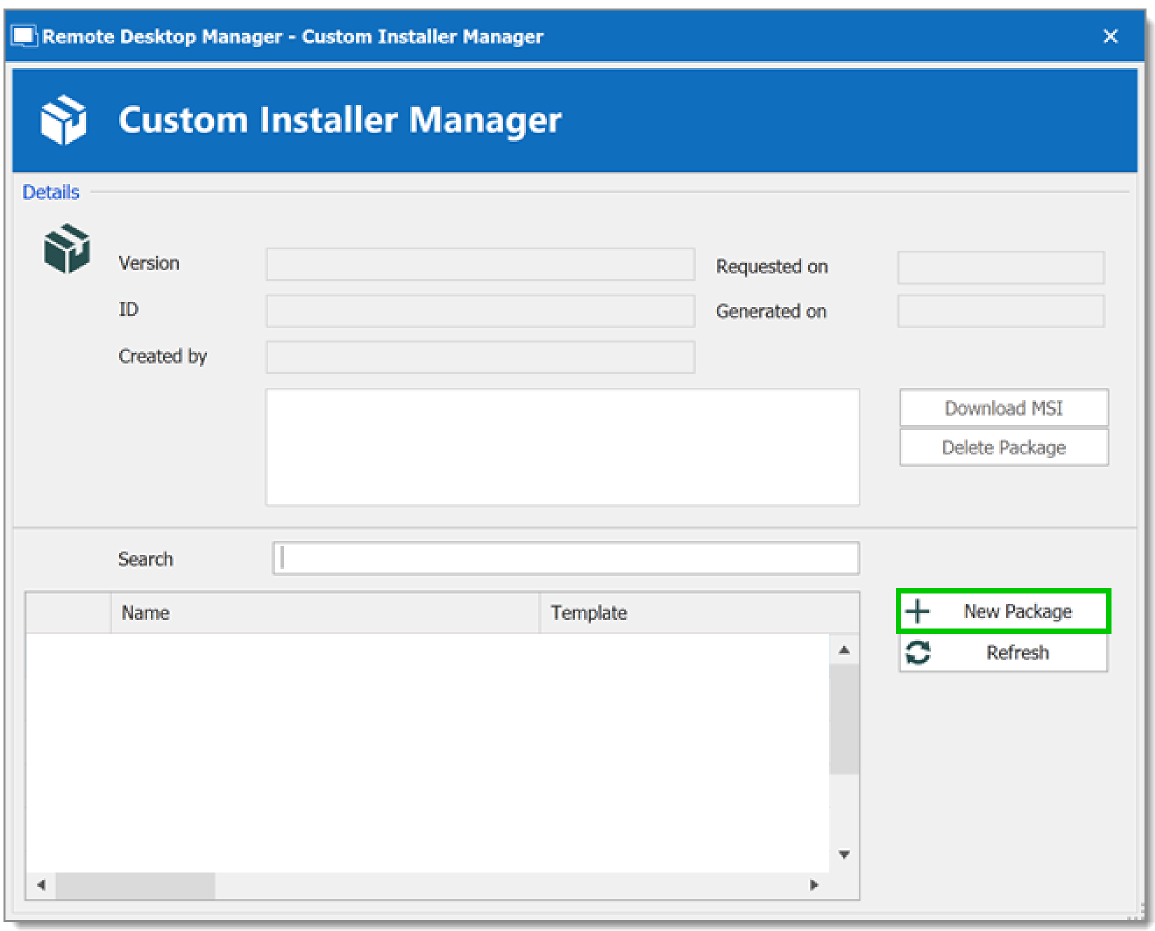
Devolutions Account Sign-in

2. Click on ***Custom Installer Manager*** to create a new custom installer with specific settings.



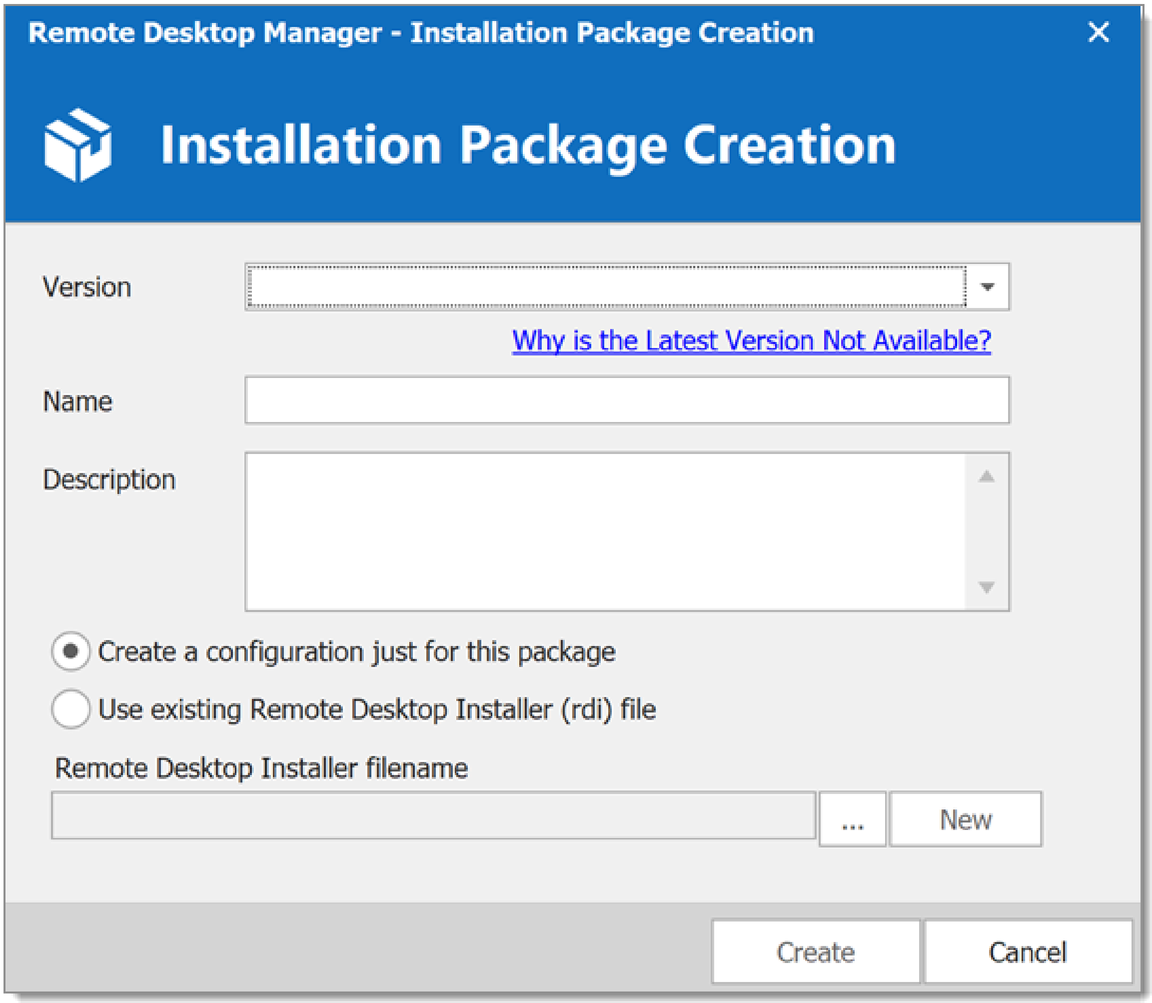
File - Devolutions Account - Custom Installer Manager

3. Click on ***New Package***.



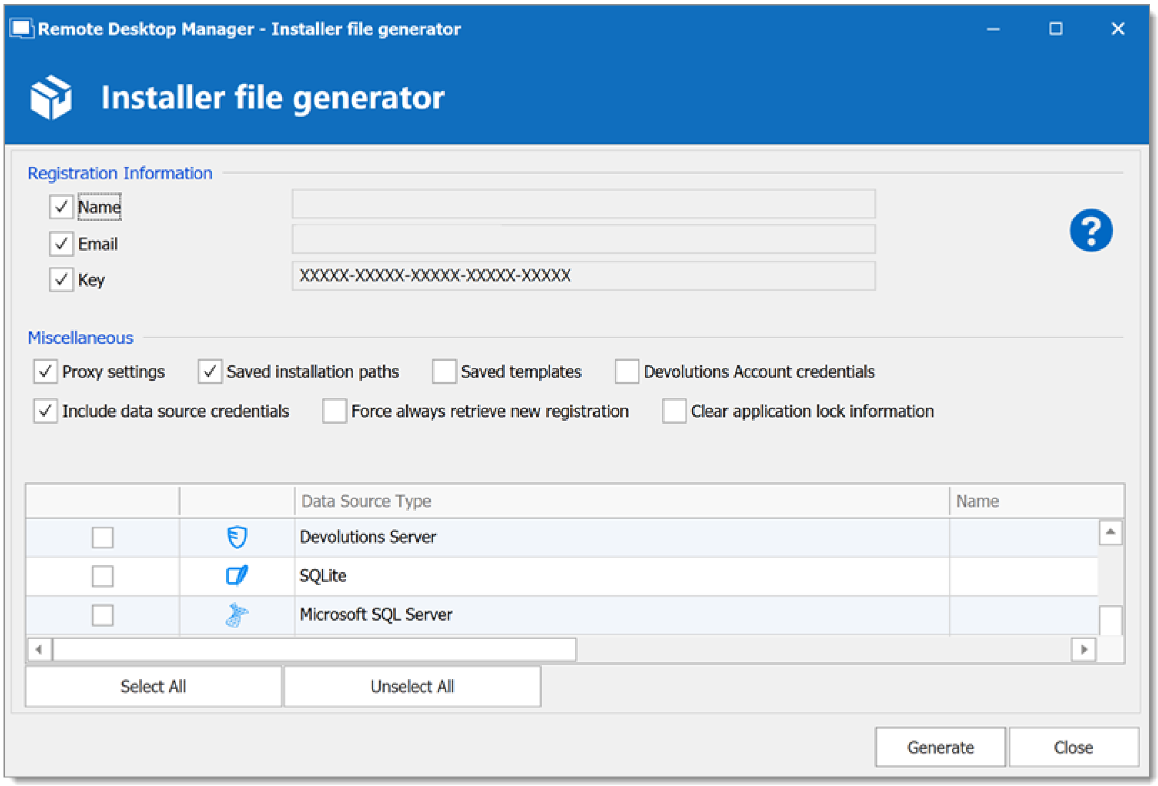
Custom Installer Manager - New Package

4. Select the application version, enter a name for your package and click on ***Create***. You can either create a new configuration or use an existing Remote Desktop Manager Installer (*.rdi) file. For more information, please consult our Installer File Generator topic.



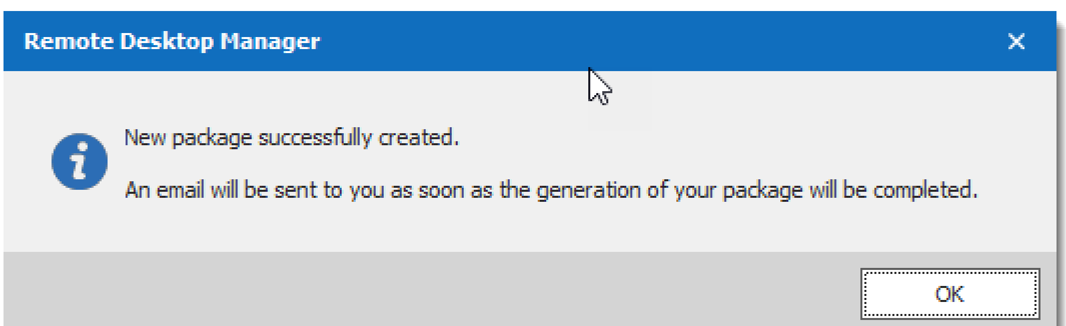
Installation Package Creation

When choosing to create a new configuration, select what to include in the custom installer, then click on ***Generate***.



Installer File Generator

5. Once the installation package has been created, the request is submitted to our online service. A confirmation dialog window appears if successful.

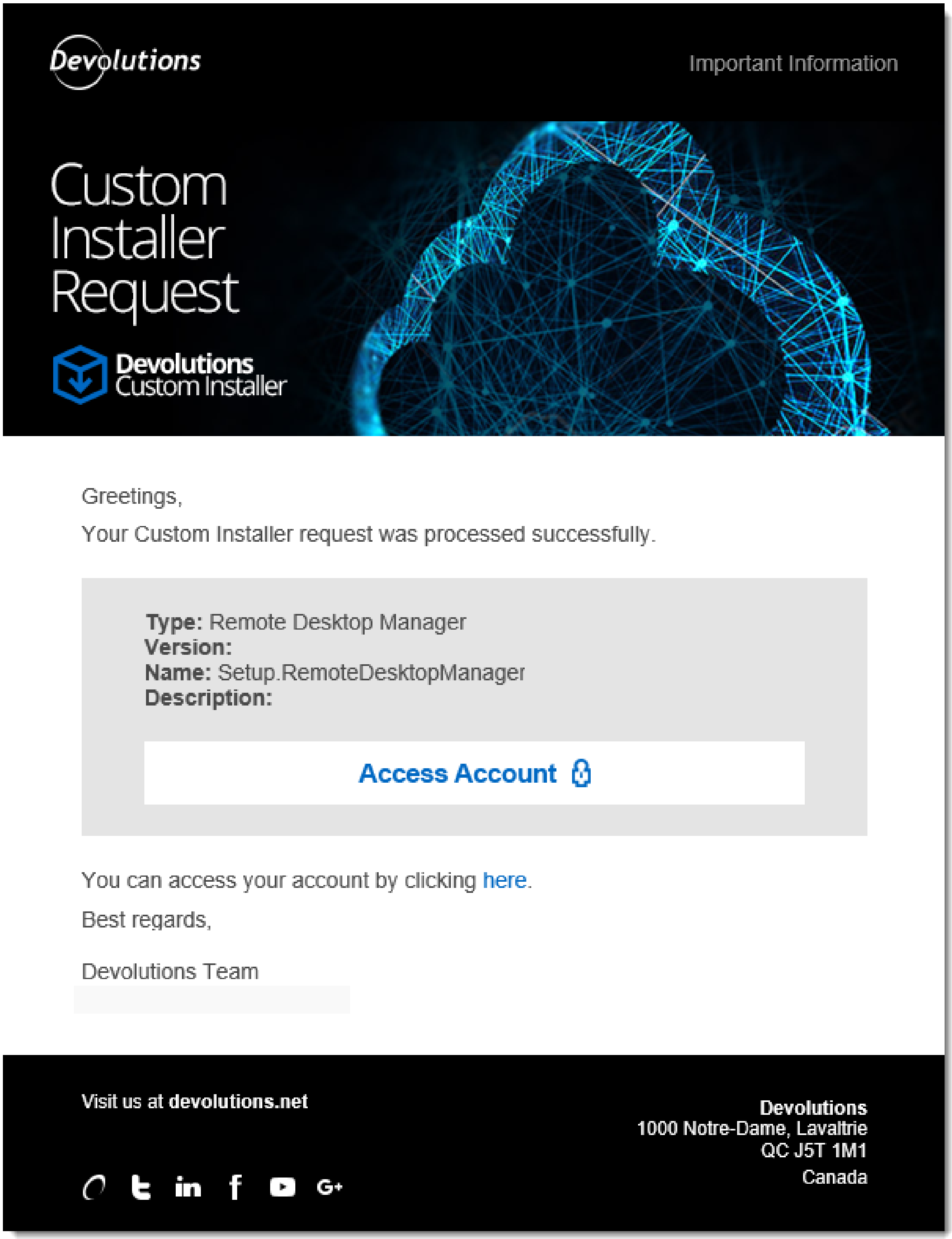


New package successfully created

6. The ***Custom Installer Manager*** will display an hourglass icon indicating that the package is being processed. When the package has been successfully generated, the ***Custom Installer Manager*** will display a green check mark. Note that this process can take a while.

DOWNLOADING AN INSTALLATION PACKAGE

Upon completion you will receive a confirmation email.

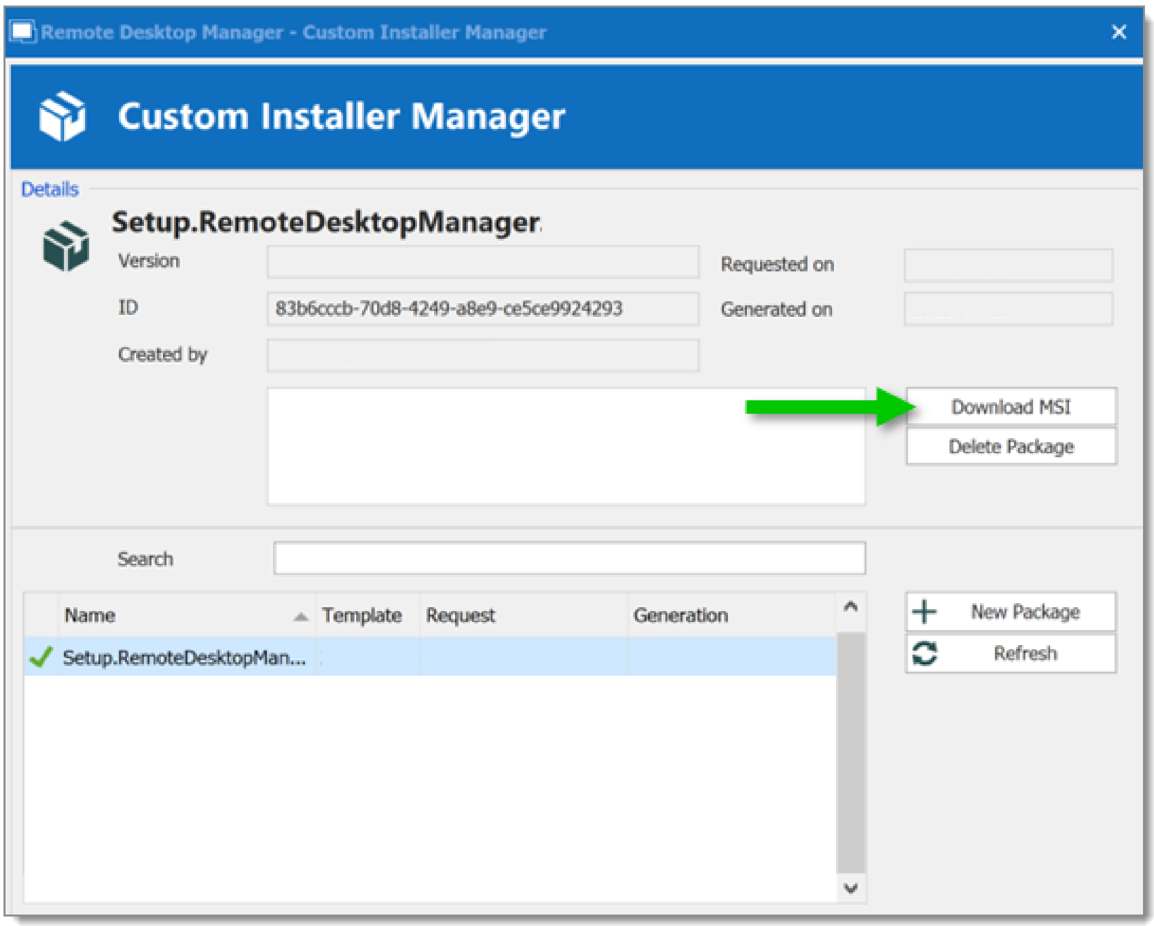


Email Confirmation - Custom Installer Processed

From here, there are two ways of downloading the package. You can download it directly from the ***Custom Installer Manager***, or you can log in to the ***Devolutions Account*** you created the installer with.

DOWNLOAD WITH THE CUSTOM INSTALLER MANAGER

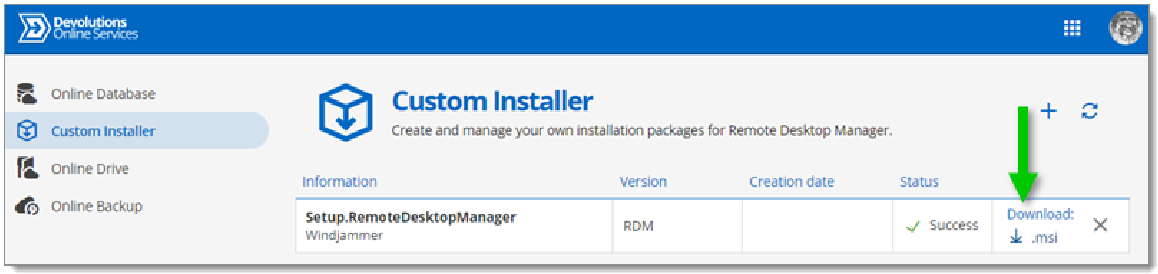
From the ***Custom Installer Manager***, click on ***Download MSI***.



Custom Installer Manager - Download Package

DOWNLOAD FROM THE DEVOLUTIONS CUSTOMER PORTAL

From the ***Devolutions Customer Portal*** you created the custom installer with, navigate to the ***Custom Installer*** section. Click on ***.msi*** to download the custom installer on your computer.



Devolutions Customer Portal - Download Custom Installer Package

3.1.4 For All Users

DESCRIPTION

Remote Desktop Manager's current installation package does require to install with elevated privileges, as well as making the application available to all users of the computer where you are installing. That being said, feedback has shown that it does complete successfully across a wide spectrum of our community's environments. Follow this procedure to reduce deployment issues in the future.

PROCEDURE

> This procedure registers all file types associations, this mean that rdp files will from now on be opened with Remote Desktop Manager. If you wish to avoid this, install manually using the Custom mode, and choose every option but that rdp association.

1. Copy the installer to a folder available for all users of the workstation. e.g. *c:\Deploy*.
2. Open an **Elevated Command** prompt (right click on the shortcut and select ***Run as administrator***).
3. Run the following command, adapted for the version that you are installing

```
msiexec /i Setup.{APPNAME}.{VERSION}.msi /Quiet /Passive INSTALLMODE=Complete
```

We also **recommend disabling the auto-update** check as all further installations or upgrades should be performed by an administrator **AND** using elevated privileges.

If you wish to proceed with upgrades from within Remote Desktop Manager, **it must** have been started using ***Run as administrator***.

NOTES

The Microsoft installer technology copies the installer package under a new randomized name as well as register it in a database. Our experience shows that this copy has a way of disappearing and that the database becomes corrupted. We often have to direct our community to use https://support.microsoft.com/en-us/mats/program_install_and_uninstall

The Quiet and Passive parameters are just to ensure that you do not have to make a choice during the installation. We found that this reduces the risk of errors.

3.1.5 Portable (USB)

DESCRIPTION

Remote Desktop Manager can be used as a portable application. Here are the steps required to ensure that it runs correctly:

> The portable installation mode allows you to run multiple versions of Remote Desktop Manager, using various license serials and configurations.

> To install a single portable Remote Desktop Manager application, follow this topic: Portable RDM Installation.

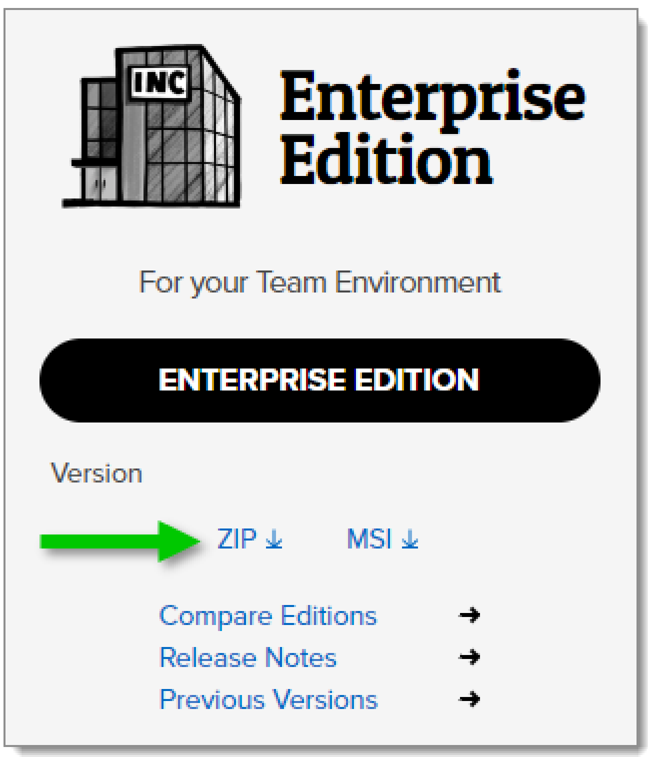
> This procedure is not recommended for running Remote Desktop Manager from a network shared by multiple users. This would prevent identifying individual users and there would be conflicts with user preferences.

Remote Desktop Manager stores the offline cache in your Windows profile by default. If you are using an Advanced Data Source and plan to use the offline mode, go to ***File - Options - Advanced*** and check ***Use application directory for offline cache*** to have the offline cached stored in the application folder instead.

The following steps ensure true portability and ease of maintenance. It can easily be adapted to your liking.

PROCEDURE

1. Download the ***ZIP*** package of Remote Desktop Manager Enterprise.



2. Create a RemoteDesktopManager folder on your portable device.
3. In the installation folder created in step 2, create two folders:

3.1. A ***config*** folder.

3.2. A ***data*** folder.

3.3. A ***tools*** folder (optional, only if you intend to use external tools like Filezilla).

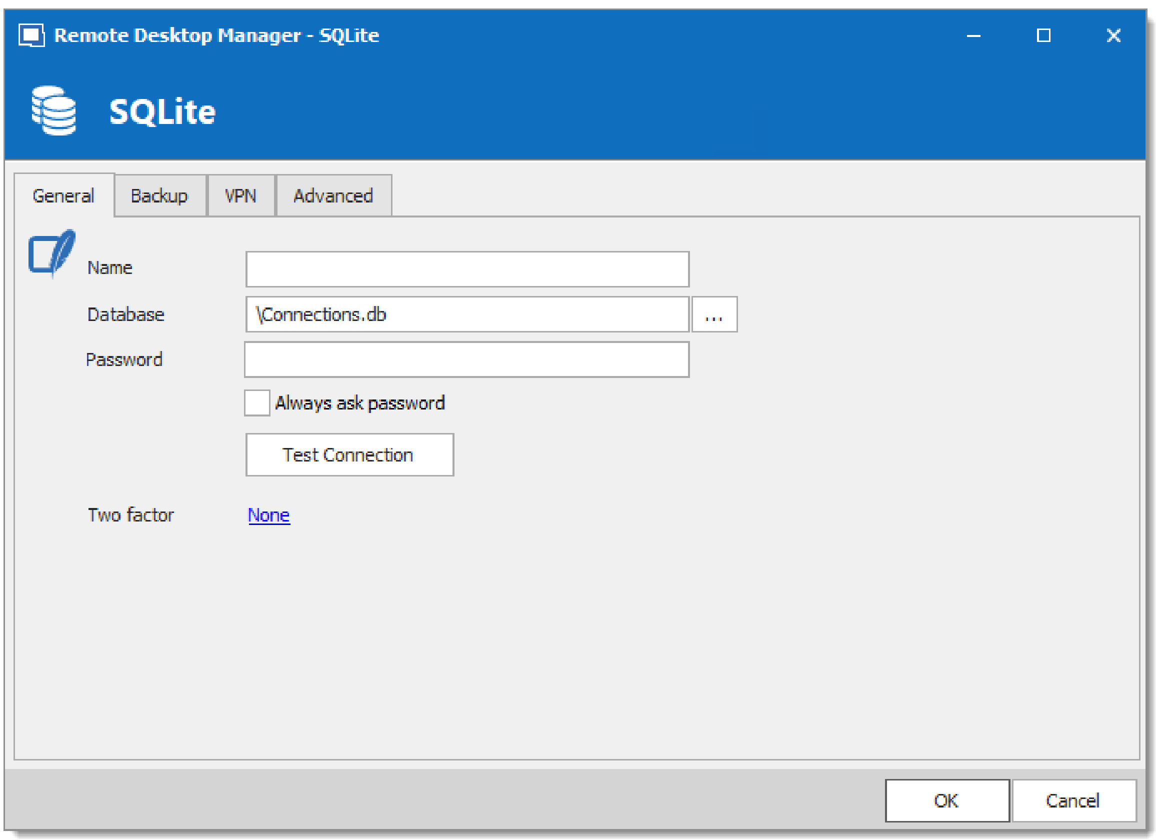
4. Unzip Remote Desktop Manager in the installation folder.

5. Create a text file named **override.cfg** in the installation folder. Set the content of the file to `.\config`

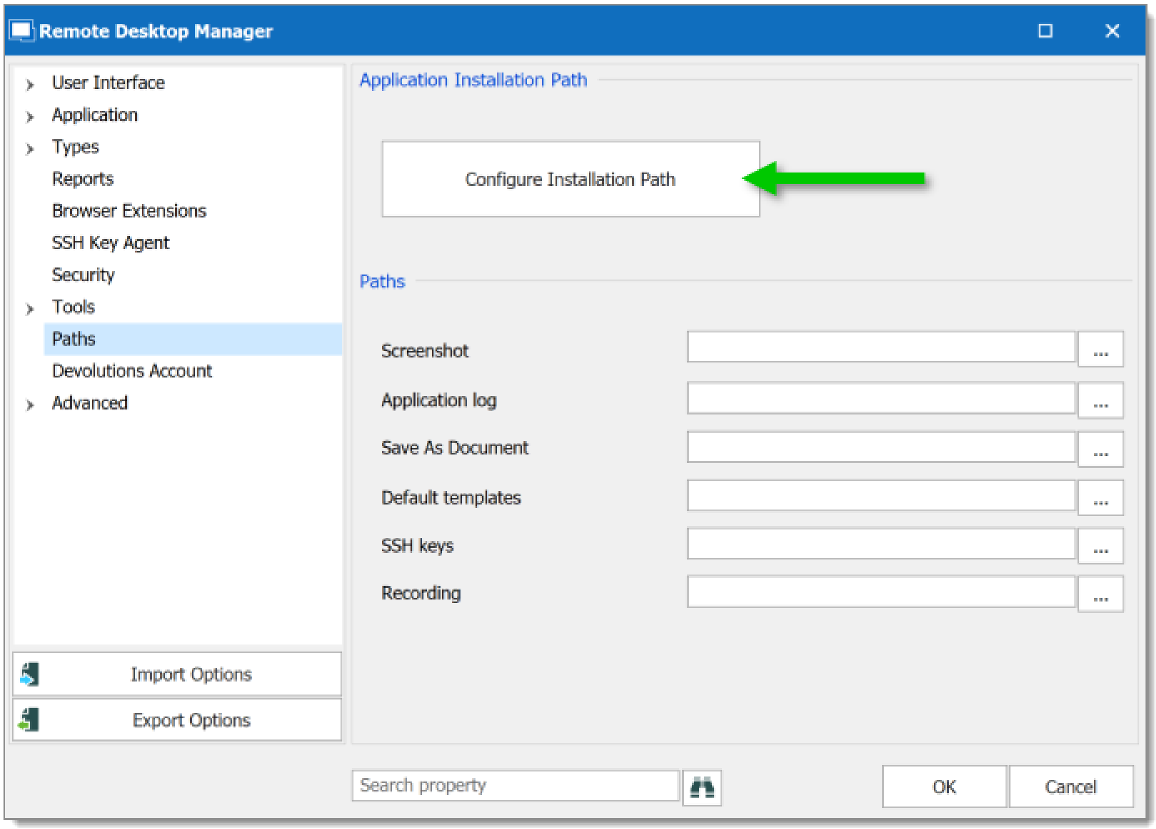
6. Open Remote Desktop Manager and display the data sources window using ***File - Data sources***.

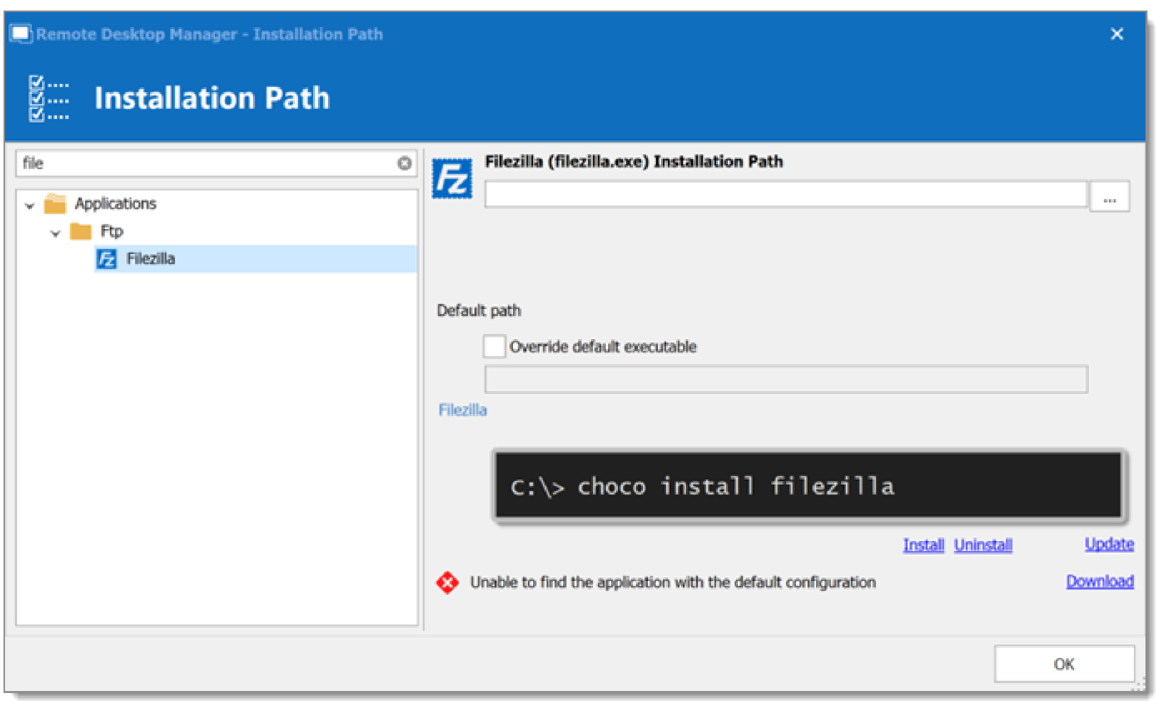
7. Create a new data source of a type that can be stored on your portable device. i.e. SQLite, XML, etc.

8. Configure the data source using a relative path so it is stored on the portable device: `.\Data\Connections.db`



9. Configure your portable applications (FileZilla, UltraVNC, etc.) in the same manner (relative to the installation folder). Click on ***Configure Installation Path*** to select your preferred portable application.





10. You can now delete the pre-existing ***Local data source*** that had been created automatically.

3.1.6 Registration

DESCRIPTION

REMOTE DESKTOP MANAGER ENTERPRISE EDITION

Please refer to the Enterprise Edition section to properly register your version. If you decide not to register at the end of the 30-day trial, your data will not be altered or erased and you will have full access to it once you provide a valid license serial.

REQUEST A TRIAL

It is possible to request a 30-day trial to try Remote Desktop Manager Enterprise Edition with all its features. For more information, please consult the Trial Request section.

REMOTE DESKTOP MANAGER FREE EDITION

Remote Desktop Manager Free Edition is similar to the Enterprise edition. It must be registered following the 30-day trial period to ensure continued use. Registration is free. Please refer to the Free Edition section to properly register your version.

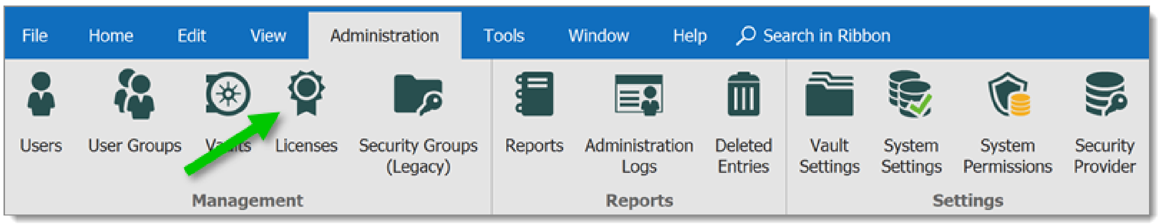
3.1.6.1 Enterprise Edition

DESCRIPTION

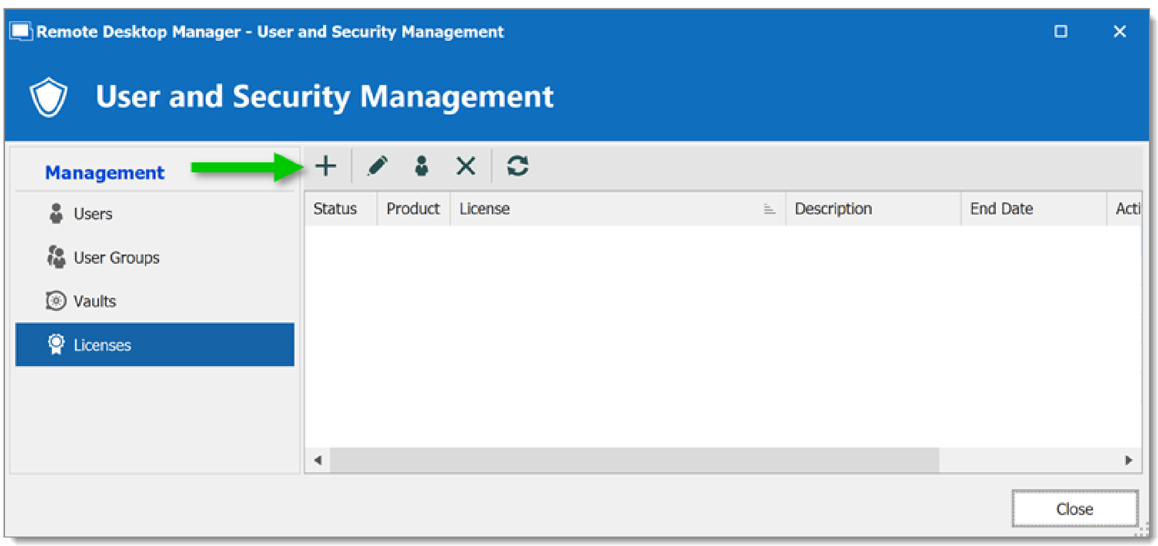
When the license serial is stored in an Advanced Data Source, there is no need to register Remote Desktop Manager as the license serial is retrieved directly from it. When launching the application for the first time, simply add the data source containing the serial.

It is possible to request a trial to try Remote Desktop Manager Enterprise for 30 days. If you decide not to register the application with an Enterprise Edition license serial at the end of the 30 day period, your data will not be altered or erased, and you will have full access to it once you provide a license serial.

1. To add a license serial to the data source, navigate to ***Administration - Licenses***.

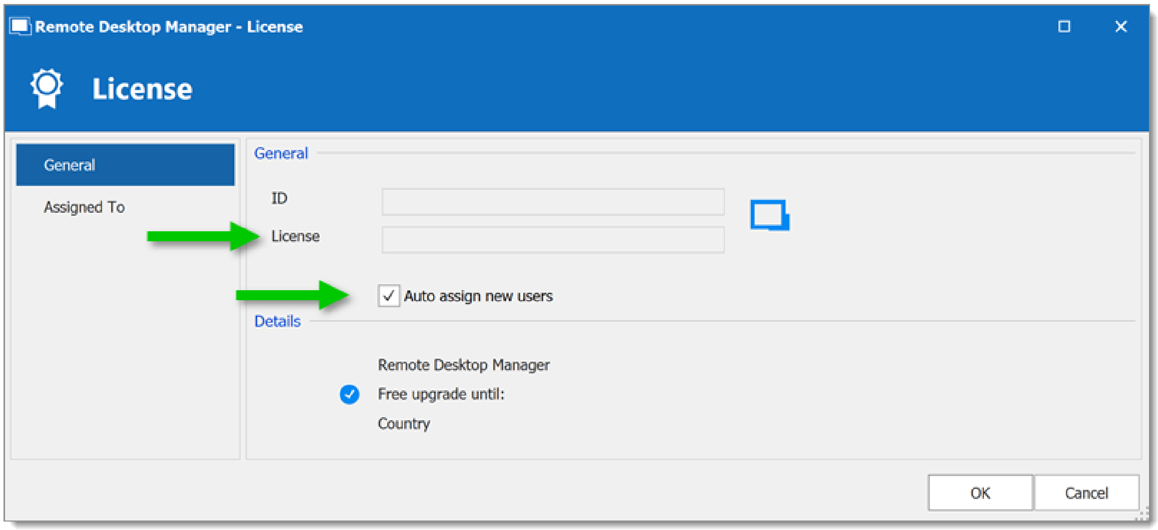


2. Click ***Add License***.



3. Enter the license serial.

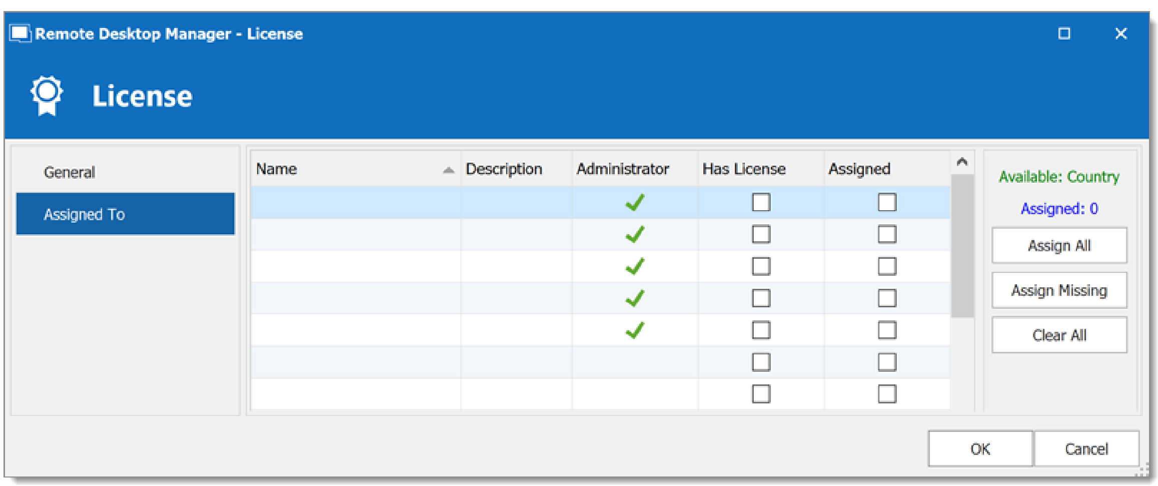
4. Optional: Check the ***Auto assign new users***, to automatically provide the RDM serial to all newly created users.



5. Click ***Assigned To***.

6. Click ***Assign All*** or select in the ***Assigned*** column who should have an RDM serial access.

This step will automatically assign the license to the selected users, removing the need to interact with each user.



7. Click ***OK*** and ***Close*** the window.

3.1.6.1.1 End of License

DESCRIPTION

Some of our Remote Desktop Manager Enterprise users could wonder, what will happen when my license expires. Here is a breakdown depending on your purchase model.

PERPETUAL

When you purchase a perpetual license, you always receive 1 or a 3 year maintenance with it. After that period, Remote Desktop Manager will continue to work indefinitely with the latest version available at the moment of the maintenance expiration.

If you discover a bug, a security issue or you want to have access to newest features and that you would like to upgrade, you would need to purchase a maintenance plan for your perpetual license.

SUBSCRIPTION

All Remote Desktop Manager Enterprise **Subscription** plans offer software maintenance (1 or 3 years), which includes all major/minor upgrades and technical support.

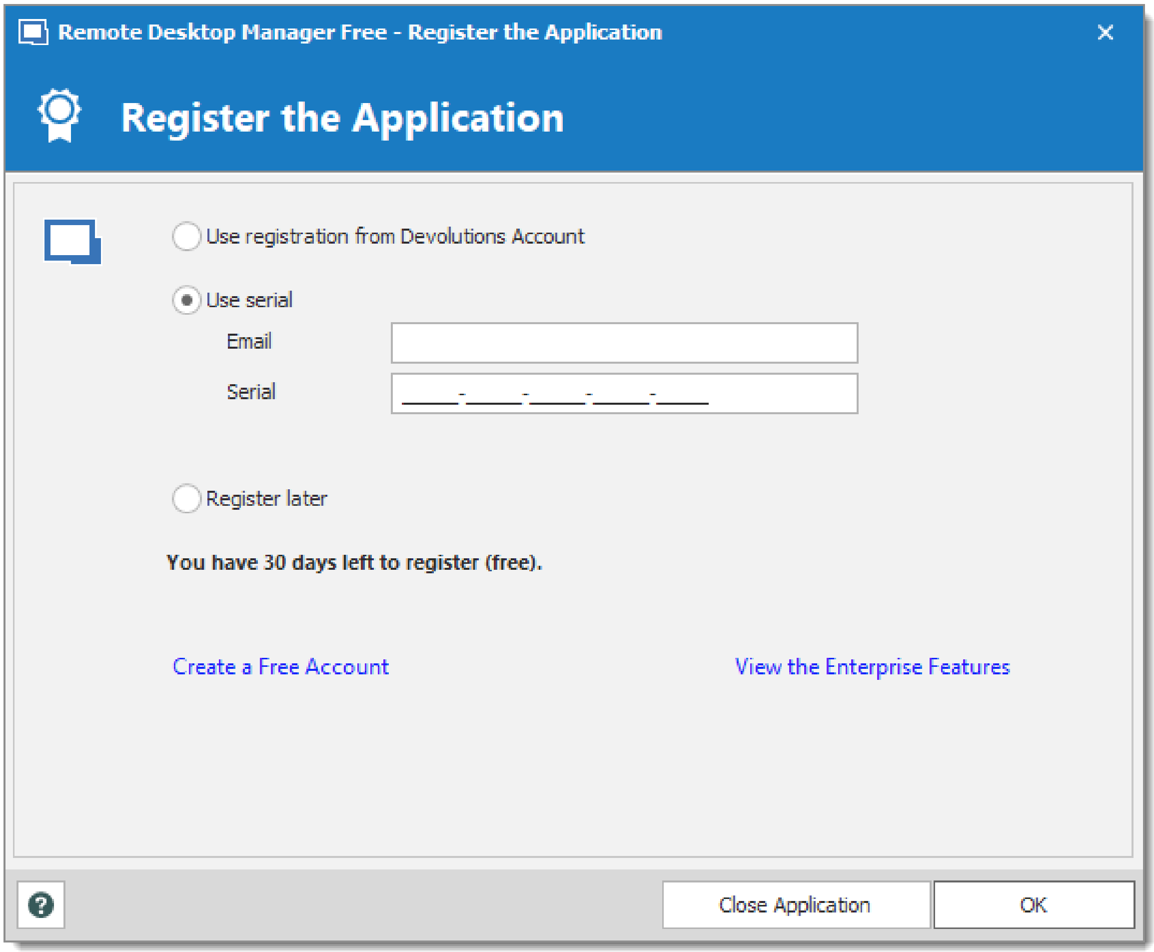
You need to renew your subscription agreement upon expiry. If you don’t renew your subscription, access to your data will be limited.

3.1.6.2 Free Edition

DESCRIPTION

Remote Desktop Manager Free Edition requires a free registration after 30 days to be able to continue the use of the application.

The **Register the Application** window will display at each Remote Desktop Manager launch until you have registered the product license. It shows the number of remaining days and your registration choice.



Register the Application

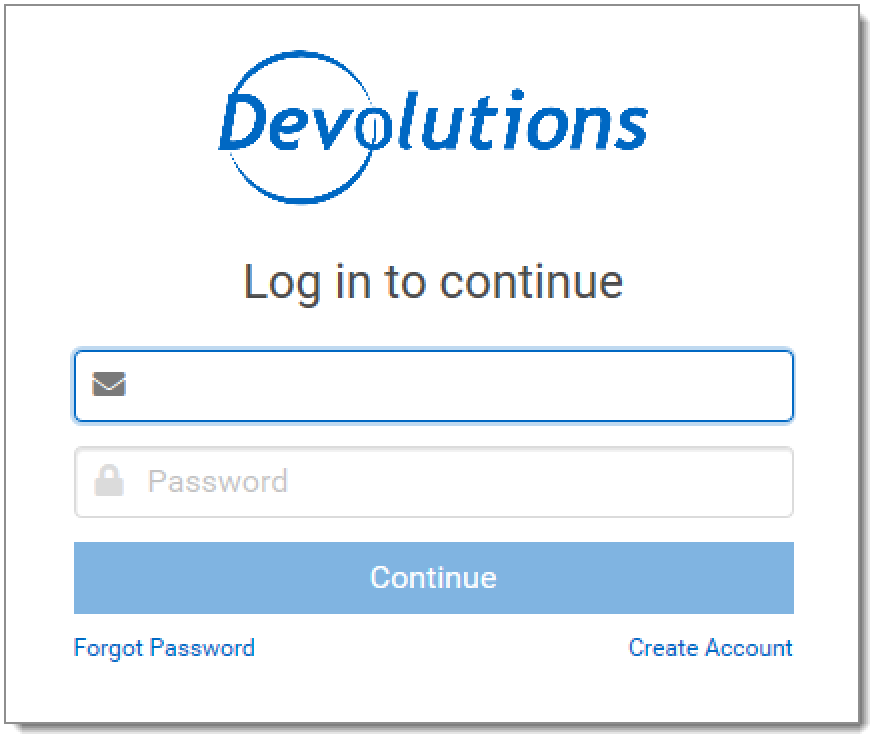
USE REGISTRATION FROM DEVOLUTIONS ACCOUNT

Every owner of a Devolutions Account is assigned a free license serial for Remote Desktop Manager in their Customer Portal.

To get a Devolutions Account, click on **Create a Free Account** in the register window**.**

To register your application follow these steps:

1. Select **Use registration from Devolutions Account**.
2. Click **Ok**.
3. Fill in your credentials and **Continue**.



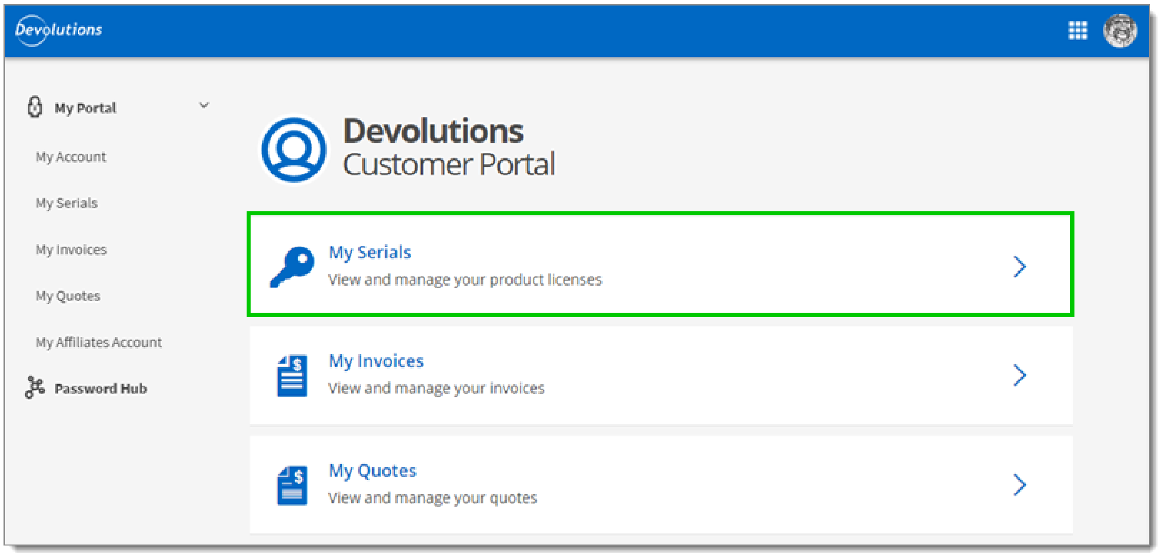
Devolutions Account Login

The license serial will be retrieved automatically.

REGISTER THE FREE EDITION WITHOUT AN INTERNET CONNECTION

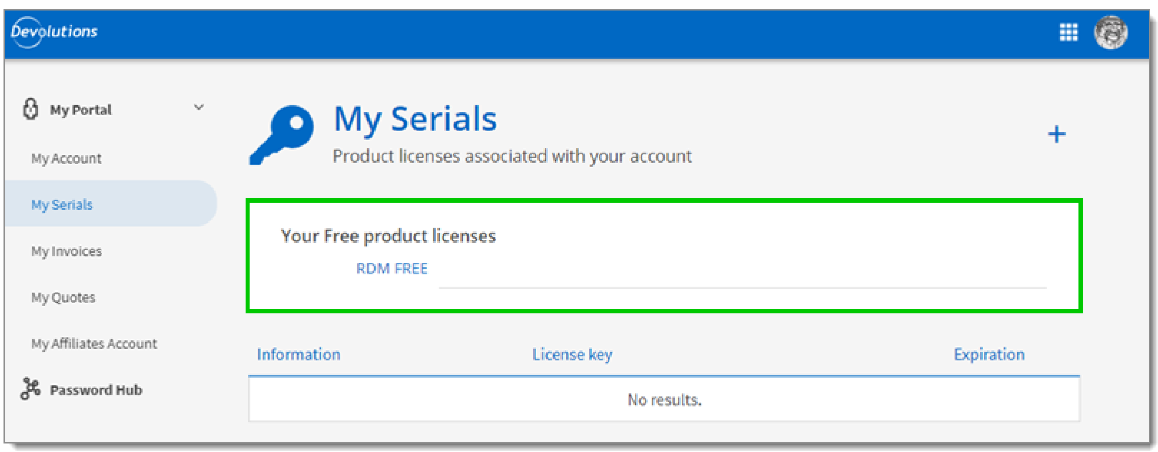
In the event that you need to register the application without an internet connection, the information must be entered manually. You will need the license serial from your Customer Portal.

Log in to Customer Portal and click on **My Serials**.



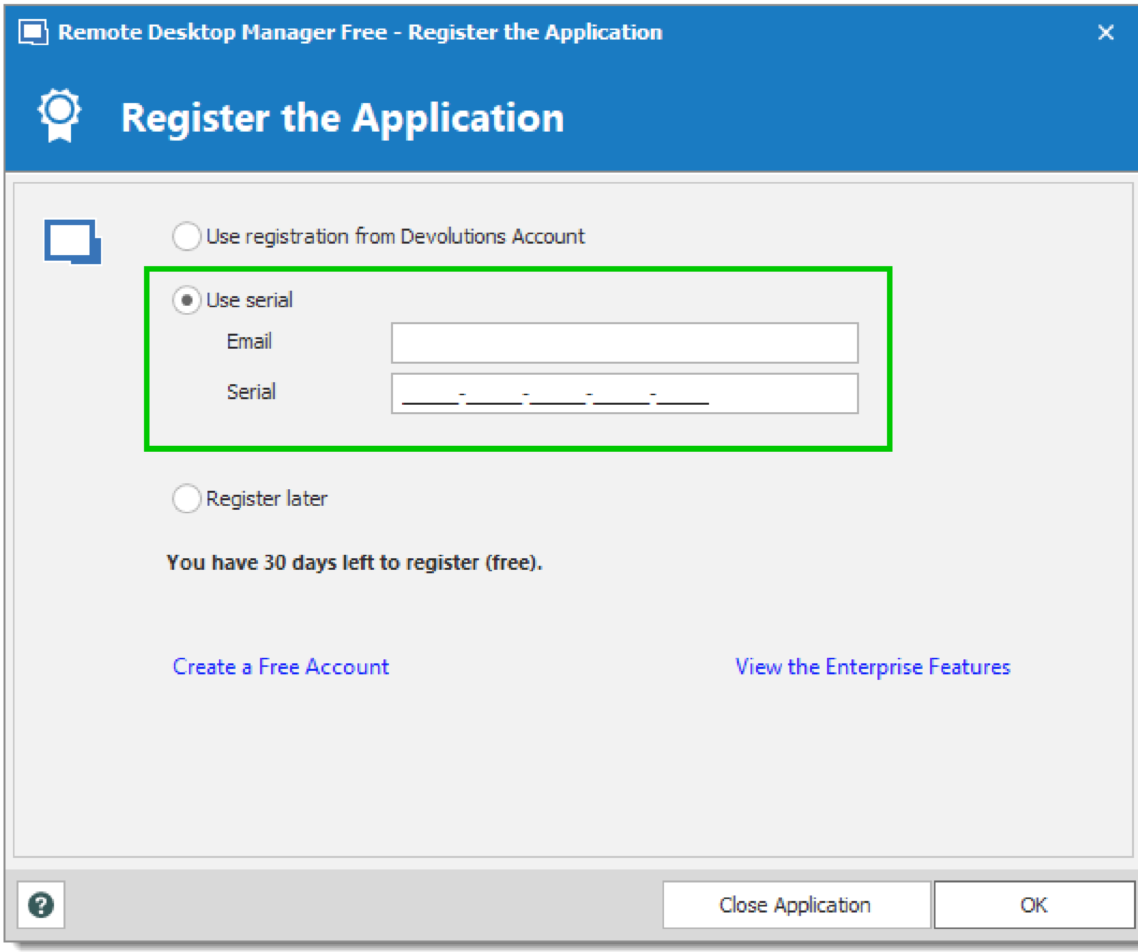
Customer Portal - My Serials

Copy the license serial for the **Free Remote Desktop Manager Edition**.



Free Product Licenses

Paste the license serial, enter an email address and press Ok.



Register Manually

3.1.6.3 Trial Request

DESCRIPTION

When launching Remote Desktop Manager for the first time, the application registration window is displayed. If you are not ready to buy Remote Desktop Manager, you must request a trial to use the application. The trial is valid for 30 day, after which the application cannot be used unless a valid Remote Desktop Manager Enterprise Edition license serial is provided.

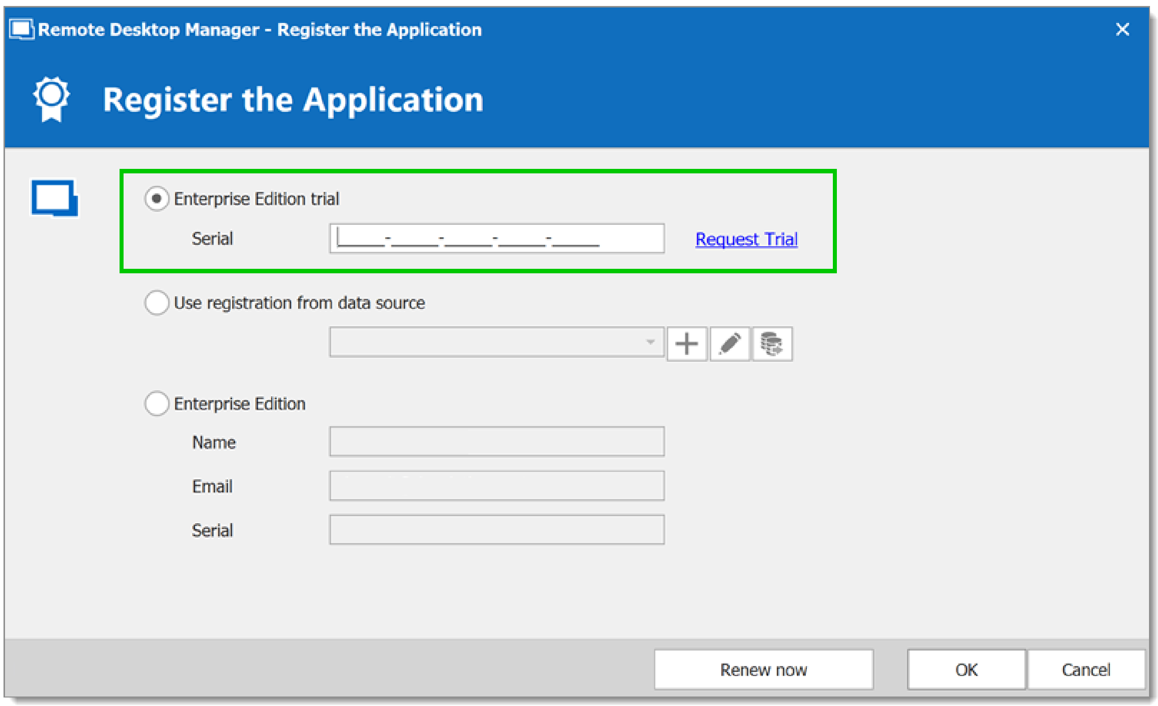
> Request your Remote Desktop Manager Enterprise 30 day trial from our website.

STEPS

1. Request from our website your Free 30 day trial or click in the ***Register the Application*** window the ***Request Trial*** link.

2. Paste the trial license serial that you will receive in a confirmation email from Devolutions.

3. Click ***OK***.



Register Enterprise Edition Trial

3.1.7 Remote Desktop Services

DESCRIPTION

Remote Desktop Manager has an excellent support for running under a Remote Desktop Services environment. A master configuration file can be created to distribute settings for all new users of the system or even to update existing user's configuration.

Please ensure that you have followed Microsoft's recommendation on how to set up an RDS environment. It will severally impact the performance if default Windows installations are performed.

https://docs.microsoft.com/en-us/windows-server/administration/performance-tuning/role/remote-desktop/session-hosts

Each user must have a unique application data folder (Roaming profiles or similar technologies). Remote Desktop Manager saves some user preferences to the local configuration file. The folder can be wiped out whenever the user logs out of the Windows Session, but it must be accessible for the duration of Remote Desktop Manager execution.

PROCEDURE

1. Install by following the procedure For All Users. This ensures that the Microsoft Installer Database does contain all of the needed information for all user profiles of the host.
2. After installing Remote Desktop Manager, configure your preferences. We recommend going through all the configuration options to find the set of options that you wish to distribute. The data sources deserve special interest since it is much better when they are configured by an administrator. You may even take the opportunity to lock the data sources to protect against any modification by the users. Please refer to Lock Data Source for more information.

When using Advanced Data Sources, for effective logging methods, proper session security and user-based features, it is **CRITICAL** that each user has their own account to authenticate against the data source.

Redistributing a data source registration should follow one of the patterns below:

- The data source is configured to always ask the username and password;
- You are using integrated security against SQL Server;
- You use environment variables for the username, and require the password. (we recommend `%USERDOMAIN%\%USERNAME%` or `%USERDNSDOMAIN%\%USERNAME%`)

Do not check the options to include ***Devolutions Account Credentials*** as well as any data source that contains saved credentials while also enabling ***Include data source credentials***.

3. When running Remote Desktop Manager under a Remote Desktop Services environment, we may have to tweak the parameters of the RDP entries to use less resources as possible and improve the startup performance of the application.

   a. To improve the Remote Desktop Manager startup performance, please see Solution #3 of the Startup Performance article.

   b. To limit the memory consumption of RDP entries, please see Memory Tuning of RDP Sessions.

4. When Remote Desktop Manager is configured to your liking, use ***File – Options – Export Options***. This will allow you to choose exactly the data sources to include, as well as the various categories of settings. Please refer to Export Options for further details. Save the file with the name ***default.cfg***.

5. Move the ***default.cfg*** file in the installation folder of Remote Desktop Manager, if you have used the default installation settings, it is under the %appdata%\Devolutions\RemoteDesktopManager directory.

WORKFLOW

NEW USERS

Whenever a new user creates a profile on the system, Remote Desktop Manager detects the presence of the *default.cfg* file and uses it as a template to create the user's configuration file.

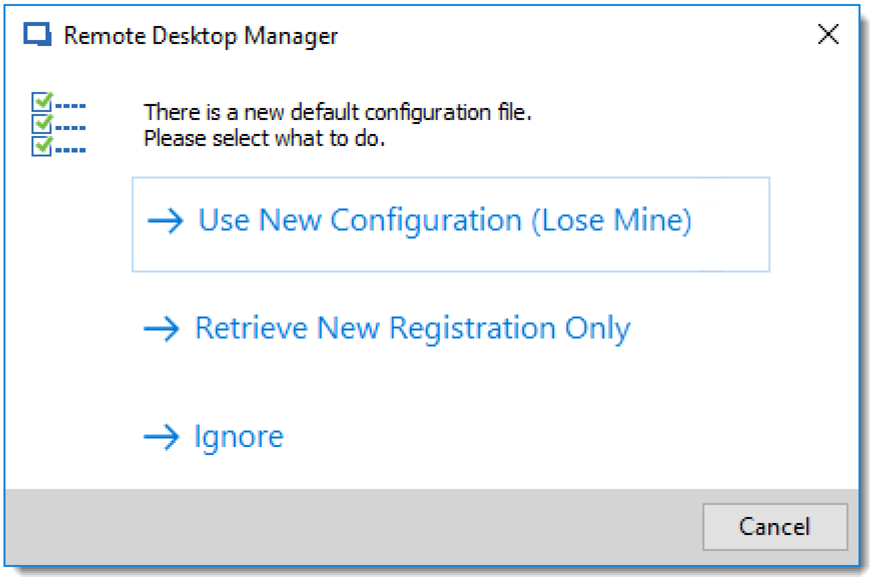
EXISTING USERS

A group policy exists to force the new configurations to be accepted automatically. Please see the How to Apply Policies article to know how to deploy the ***Force the loading of the default.cfg file*** parameter.

If the user chooses to ignore the new configuration file when presented with the dialog below, he will not be presented with the choice until the date/time of the *default.cfg* file has changed.

If the main concern is deploying a new license key, and you are using an Advanced Data Sources, you should rather use the feature to store it in ***Administration - Licenses***.

Whenever Remote Desktop Manager is started and it detects a new *default.cfg* file, the following dialog will appear:



New default.cfg detected

By selecting ***Use New Configuration (Lose Mine)***, the user's configuration is simply overwritten. If you only wish to update the Remote Desktop Manager license key after a renewal, choose ***Retrieve New Registration Only***.

3.2 Database Upgrade

DESCRIPTION

This topic applies to installations with data sources that are using a **database** as their data store.

Some Remote Desktop Manager releases must alter the database structure. These are performed automatically for you but it is best practice to perform a backup of your data source beforehand. Additionally, If you are in a team environment **you must be the sole user connected to the database** during the upgrade.

> The user performing the update must have administrative privileges on the underlying database. (**SYSDBA** or **DB_OWNER**).

✖	Perform a database backup and ensure that you can quickly perform a restore if required.

✖	If your organization allows for a read/write offline cache, ensure that all of your users have merged their offline edits.

STEPS

Follow these steps for a successful version update:

1. Ensure you are the sole user of the database during the upgrade process. If you environment allows for offline use, have your team switch to the offline mode; or have them switch to another data source.
2. Back up your database using the database tools.
3. Install the desired version of Remote Desktop Manager, using the Portable (USB) deployment model may be desirable if you are doing this on your personal workstation.
4. Open Remote Desktop Manager while logged on as a user with administrative rights. You must also be **SYSDBA** or **DB_OWNER**.
5. You may be prompted with an upgrade message when your data source is accessed. If so accept the upgrade.
   or
   Using ***File – Data sources***, locate your data source to upgrade and open its property window. Switch to the ***Upgrade*** tab, then click on ***Update Database***
6. Wait for a confirmation dialog.
7. Close the dialog.
8. Ensure your Remote Desktop Manager application is currently using that data source.
9. Press CTRL-F5 to force a full refresh.
10. Validate the content and perform a check of the technologies that are critical in your environment.

11. Update the client software on all workstations.

3.3 Uninstall

DESCRIPTION

INSTRUCTIONS

Remote Desktop Manager does not install anything in the Windows System directory. The only registry settings created are for the auto-run functionality and the installation path. As a result, which simplifies the uninstallation of Remote Desktop Manager.

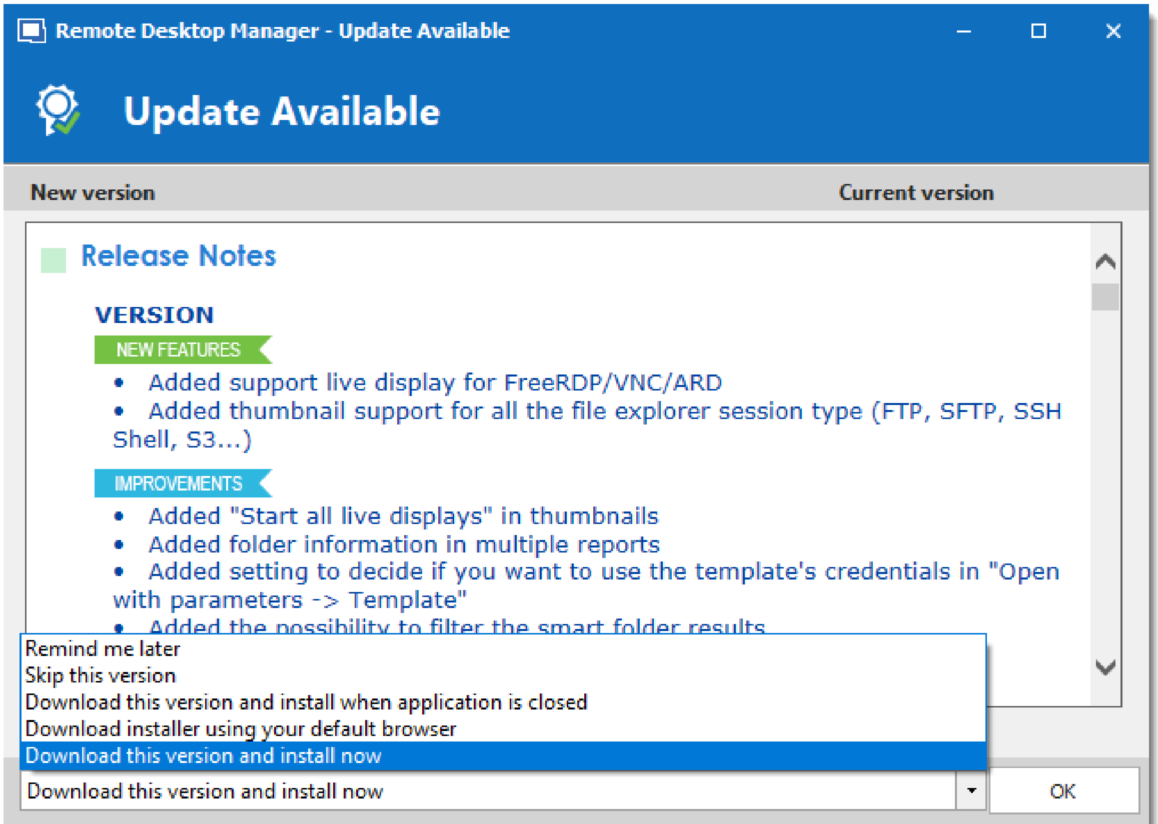
You can run the uninstaller if it was installed with the default setup file or delete the installation folder directly if it was installed from the binaries.

The application configuration files are saved in ***%LocalAppData%\Devolutions\RemoteDesktopManager*** or ***%AppData%\Devolutions\RemoteDesktopManager*** by default. If desired, it is possible to delete this folder for a complete uninstallation.

> Please note that if you are using a local data source like SQLite or XML, your data source may be saved in the configuration folder. Perform a backup of the data source prior to the deletion of the folder.

3.4 Update

The ***Update*** feature prompts the user to update to a newer version of the application and displays the release notes. The user's choice for the previous update is shown as selected.



Update

OPTION	DESCRIPTION
Remind me later	Remind to update the next time the application is opened.
Skip this version	Do not update the application with this version.
Download this version and install when the application is closed	Download the version and wait for the application to be closed before installing.
Download installer using your default browser	Download the installer externally using your default web browser.

OPTION	DESCRIPTION
Download this version and install now	Immediately download the new version and install it.

User Interface

Part

IV

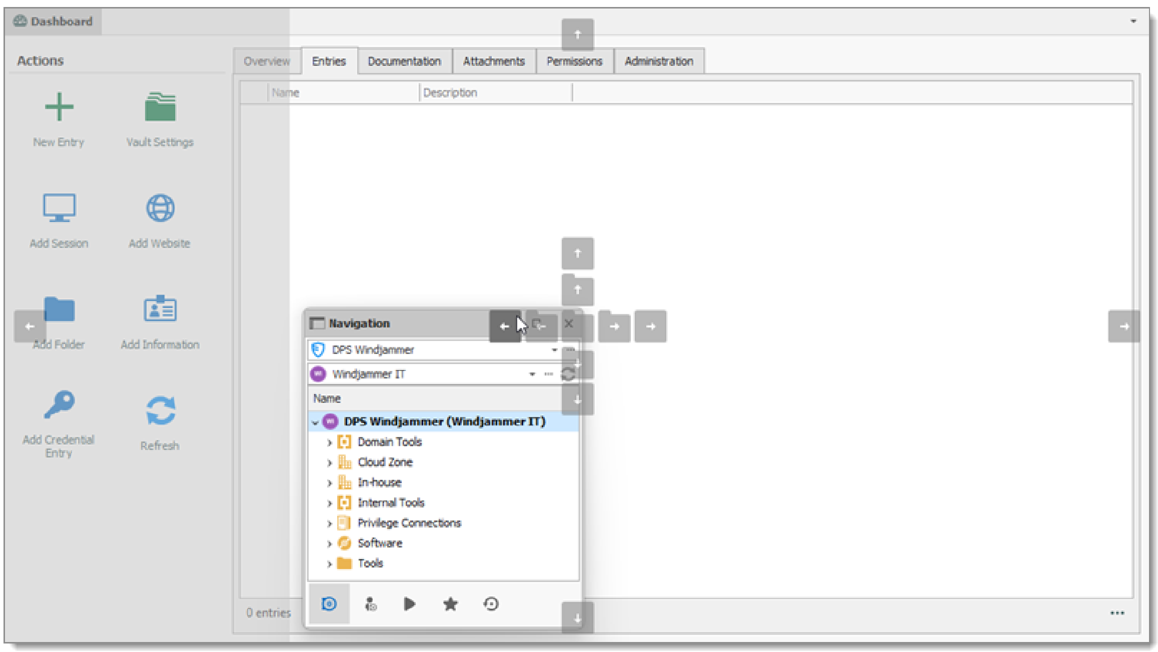
4 User Interface

4.1 UI Customization

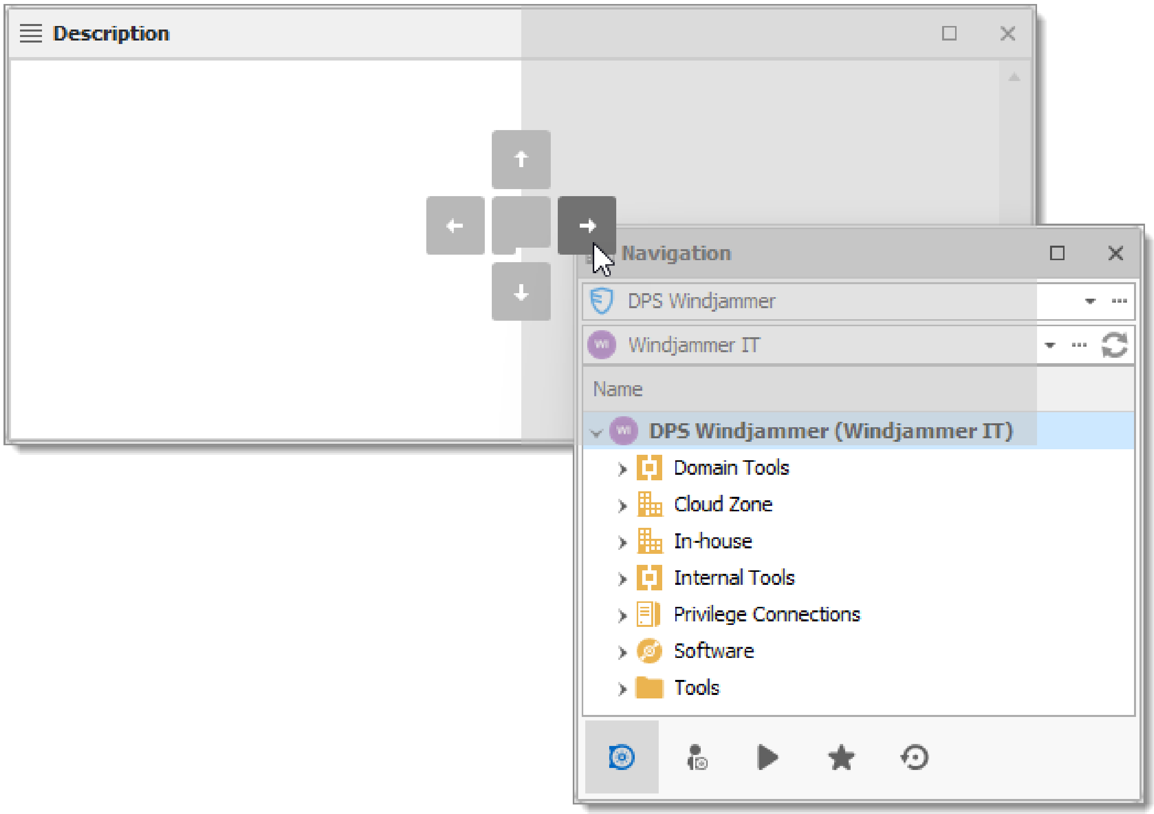
4.1.1 Docking

DESCRIPTION

Customizable styles (default ***Ribbon*** and default ***Menu***) have dockable panes that can be rearranged to your liking. Simply left-click then drag the sub-components to reveal drop zones. This allows you to drop the sub-component anywhere you want, even outside of the main form if you wish.



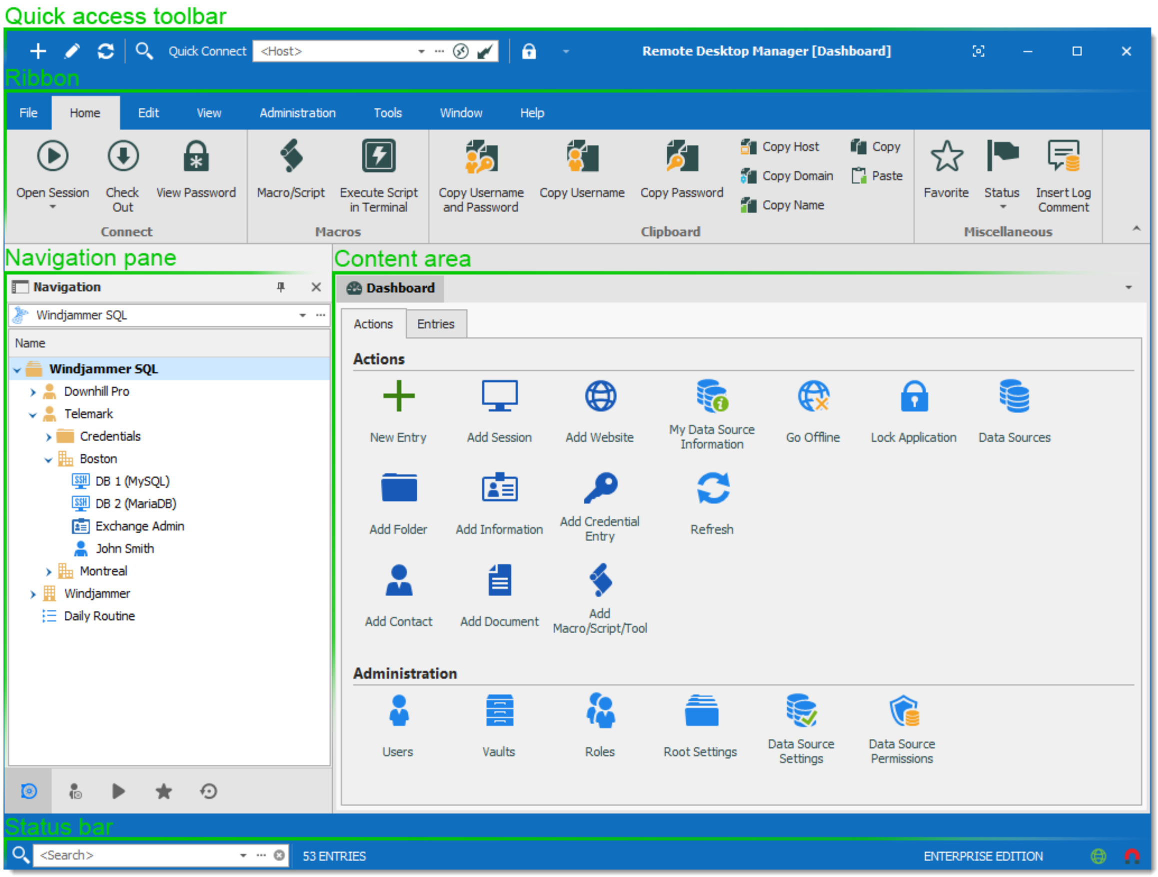
Panes can also be docked into another dockable pane using the same drag & drop method. In the following example, the ***Navigation Pane*** is dropped in the ***Description*** pane.



4.1.2 Main Screen

DESCRIPTION

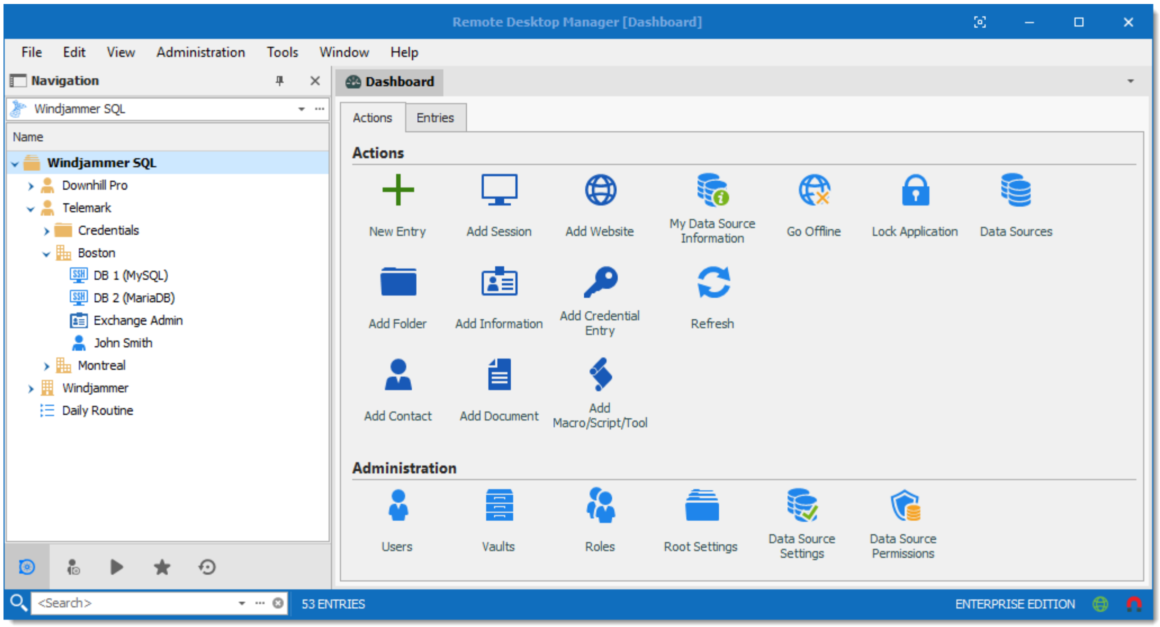
Illustrated below is the default Remote Desktop Manager main screen. Go to ***File – Options – User Interface*** to change the current style. We have various settings for you to customize your experience, such as different themes, shortcuts and more!



Overview of the default user interface

MENU USER INTERFACE STYLE

With the Menu user interface style, the ***Ribbon*** is been replaced by a standard menu, and the ***Quick Access toolbar*** is not present. This setting can be found in ***File – Options – User Interface – Ribbon Interface***.



Menu user interface style

4.1.3 Style

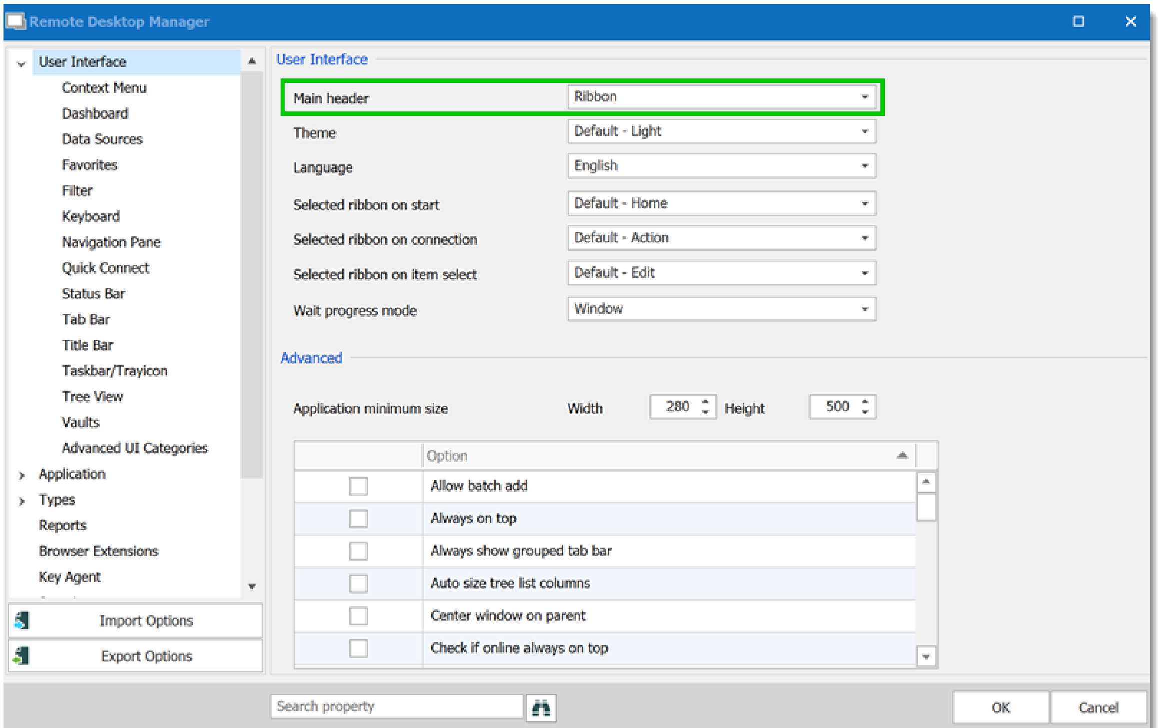
DESCRIPTION

Remote Desktop Manager supports different User Interface Styles (sometimes known as skins). These greatly influence the visual aspect of the User Interface as well as its mode of operation. Three styles currently exist:

- Ribbon
- Menu

CONFIGURATION

To select the User Interface style you must go in **File – Options – User Interface** and modify the **Main header**.

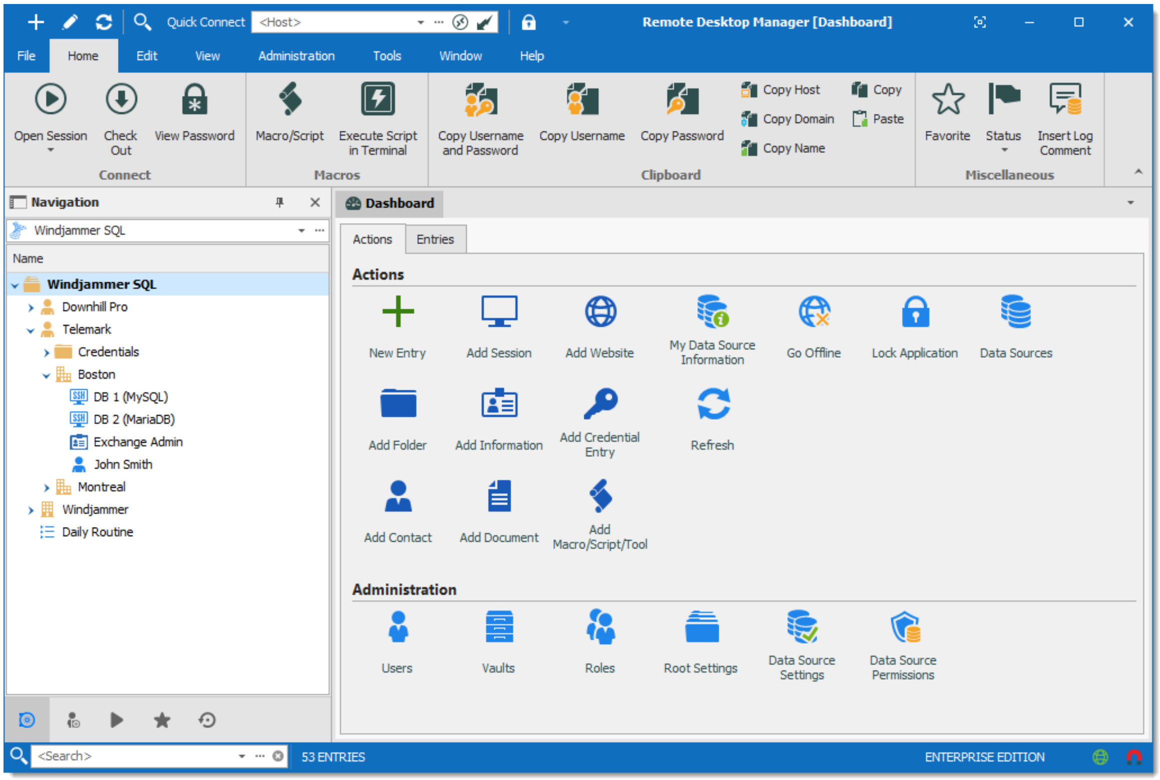


Options - User Interface

EXISTING STYLES

RIBBON

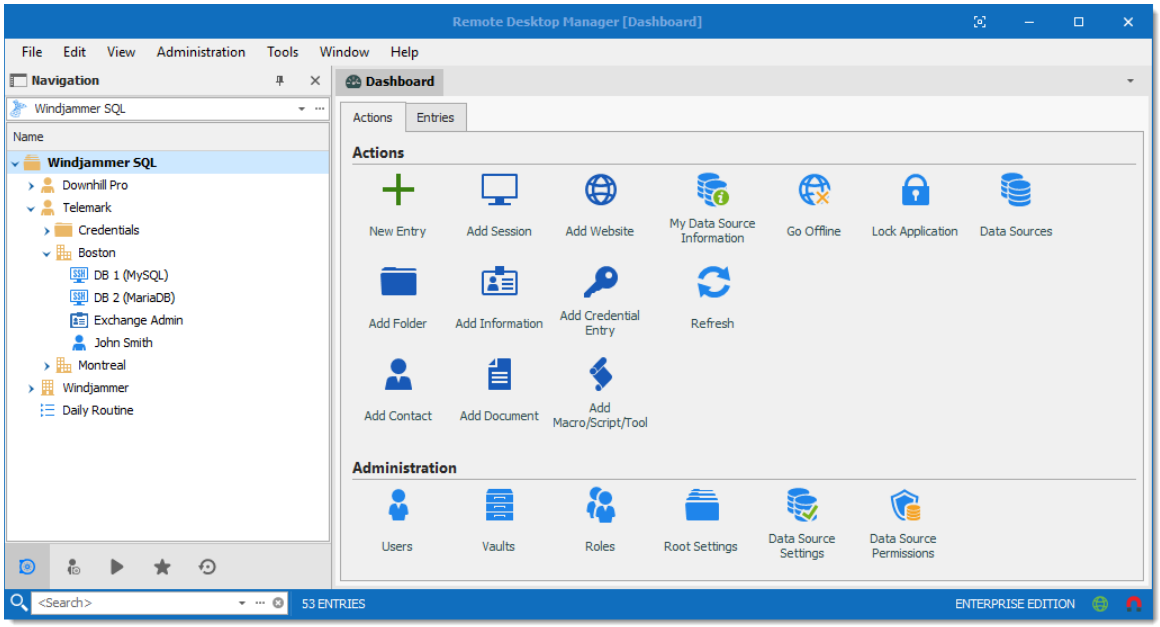
The latest style sports a ribbon. Icons and text makes it easy to explore features.



Ribbon User Interface

MENU

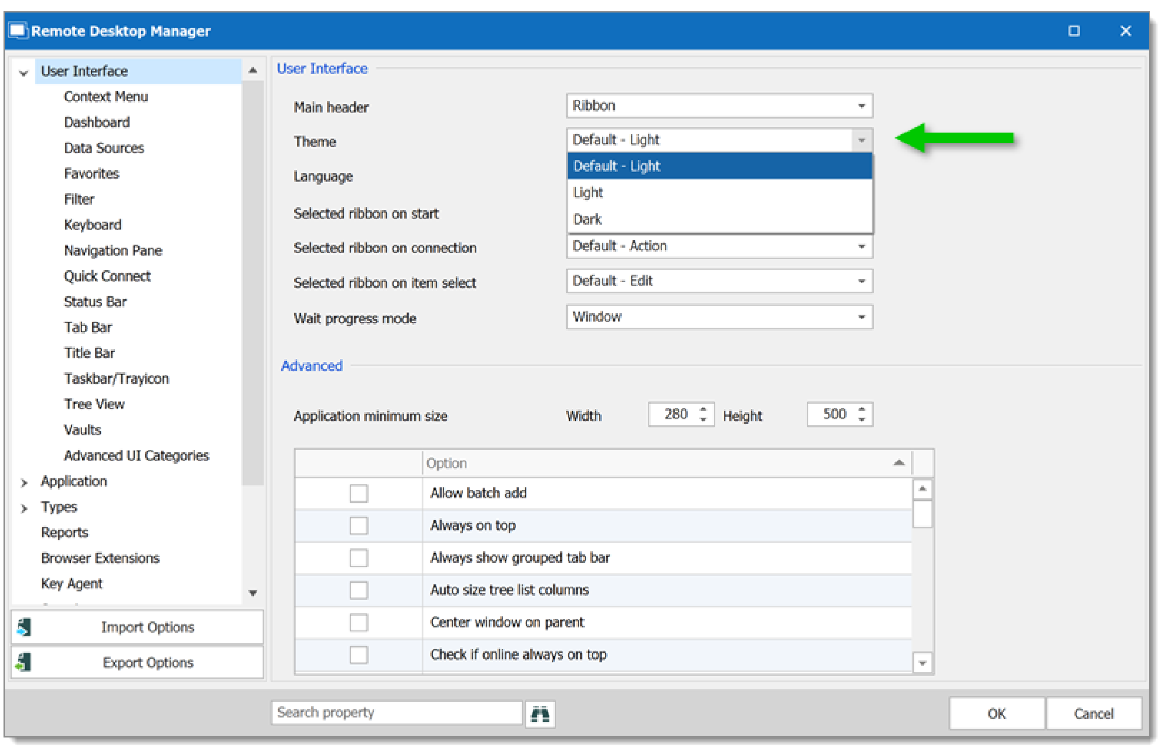
Previous generation style, it holds a standard menu to invoke commands.



Default User Interface

4.1.4 Theme

The themes will modify the color and shade of Remote Desktop Manager.

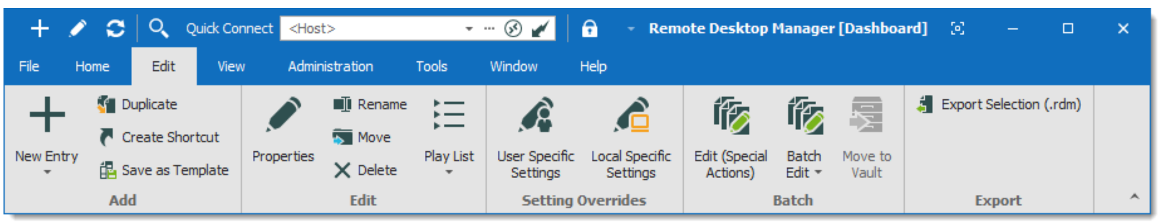


User Interface - Theme

OPTION	DESCRIPTION
Default - Light	Use the default theme, which is the Light theme.
Light	Use a clear theme with tones of white, gray, and blue.
Dark	Use a dark theme with tone of gray and black.

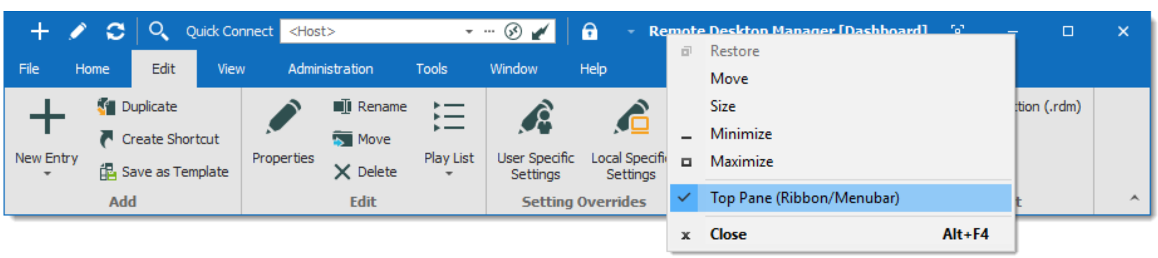
4.2 Top Pane

The ***Top Pane*** contains the [Quick Access Toolbar](#) and the Ribbon / Menu.

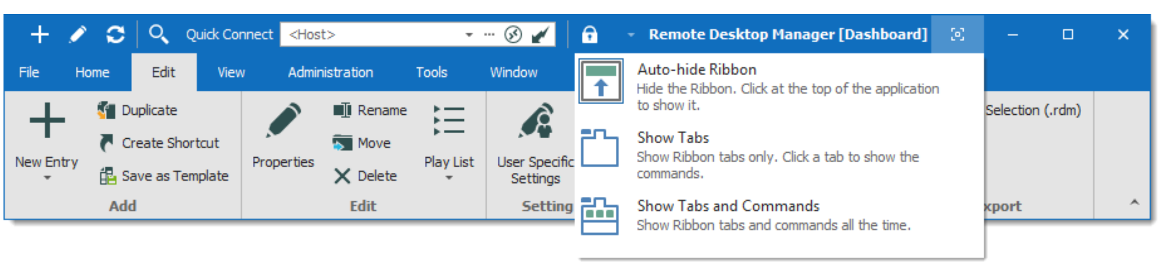


Remote Desktop Manager top pane

It can be hidden to maximize the work area.

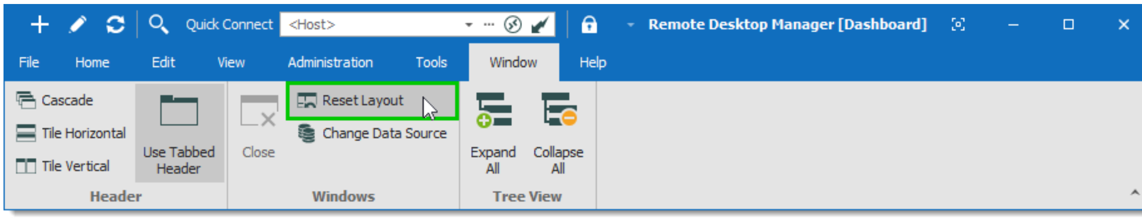


Hide the top pane completely



Hide the ribbon

If you end up confused by your modified settings and would like to reset it to its original layout, navigate to the ***Windows*** tab and select ***Reset Layout***.

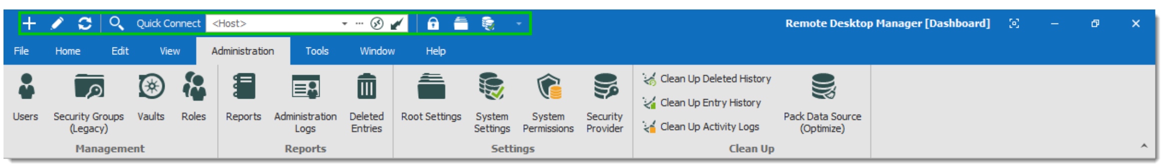


Windows – Reset layout

4.2.1 Quick Access Toolbar

The ***Quick Access Toolbar***, which is found at the top of the application, It is composed of multiple parts:

- System menu icon.
- Favorite commands.
- Quick Connect control.
- Lock command.

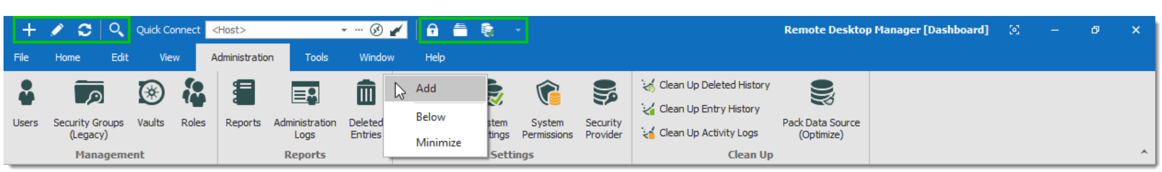


Quick Access Toolbar

> **Quick Access Toolbar buttons** are flagged locally on the current machine by the current user. These local buttons are saved in a file named **RemoteDesktopManager.qtb**. By default, this file is located in **%localappdata%\Devolutions\RemoteDesktopManager**.

FAVORITE COMMANDS

Commands contained in the ribbon can be added in the quick access toolbar. These are the favorite commands. To add a command to the quick access toolbar, right-click any icon in the ribbon the select **Add**.



Favorite Commands

COMMAND	DESCRIPTION
	Create a new entry in your current data source.
	Open the properties window of your selected entry.
	Refresh your data source.
	Open the filter dialog window to allow you to do a quick search.

Right-Click on any command to display the contextual menu. To remove an item from the quick access toolbar, right-click on the item and select **Remove**. To add an item to the quick access toolbar, right-click an item in the ribbon and select **Add**. Use this to customize your workspace with your preferences.

QUICK CONNECT CONTROL

Please refer to ***Quick Connect*** for a detailed description.

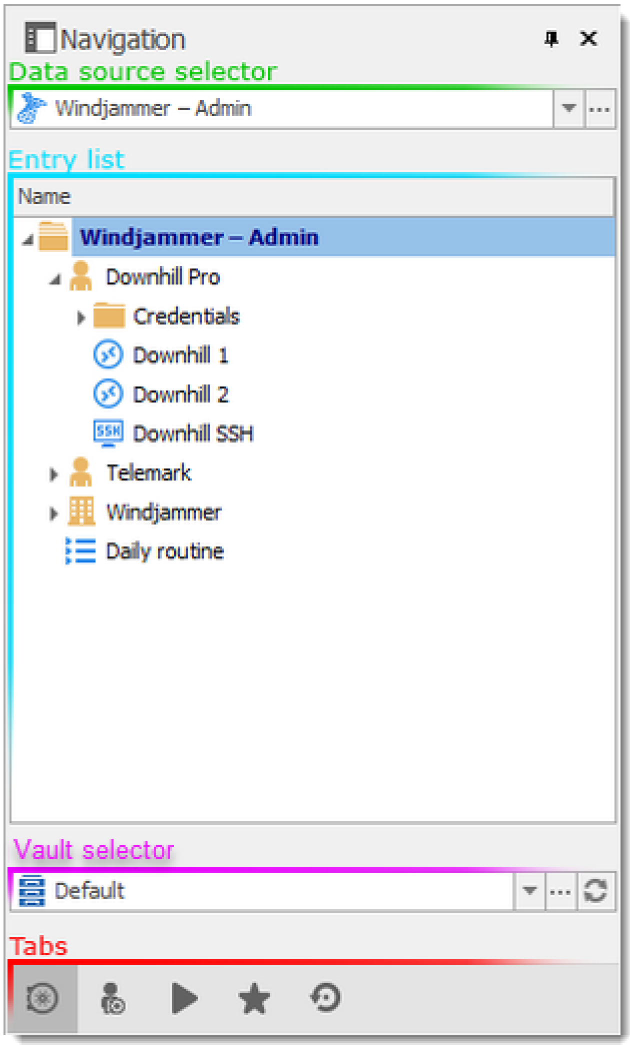
LOCK APPLICATION COMMAND

This command will minimize the application. When you attempt to restore it you will be prompted for the password. Applies only to data sources protected by a password.

4.3 Navigation Pane

DESCRIPTION

The ***Navigation Pane*** is one of the main components of the Remote Desktop Manager user interface. It lists all available entries in the current data source and allows to switch to another data source or Vault.



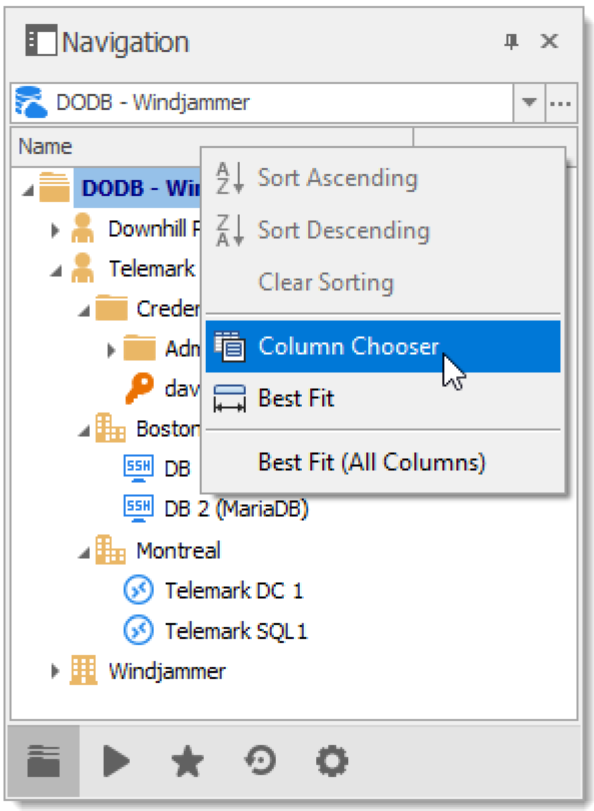
Navigation Pane

ELEMENT	DESCRIPTION
Data source selector	Allows to switch to another configured data source.
Entry list	Displays the content of the current data source, depending on the selected tab. It allows to select entries and perform action on them.
Vault selector	Allows to switch to another configured Vault in the data source.

ELEMENT	DESCRIPTION
Tabs	Allows to switch to different views of the entry list, such as the ***Favorite entries*** or the ***Opened sessions***.

COLUMN CHOOSER

Choose the columns to display in the tree view. Right-clicking on the column name in the ***Navigation Pane*** and select ***Column Chooser***.



Navigation Pane - Column Chooser

For more information on each tab, please consult the following topics:

- Vault
- User Vault
- Opened Sessions

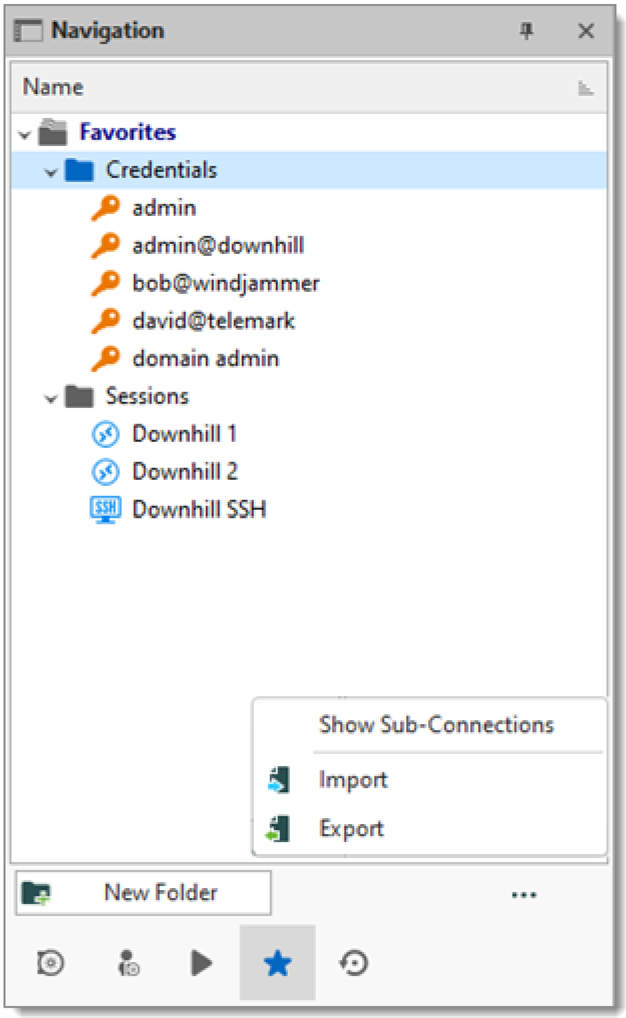
- Favorite Entries
- Most Recently Used Entries

4.3.1 Favorite Entries

DESCRIPTION

The **Favorites** tab contains entries flagged as favorite by the current user. Favorites are not shared and they roam with the user profile.

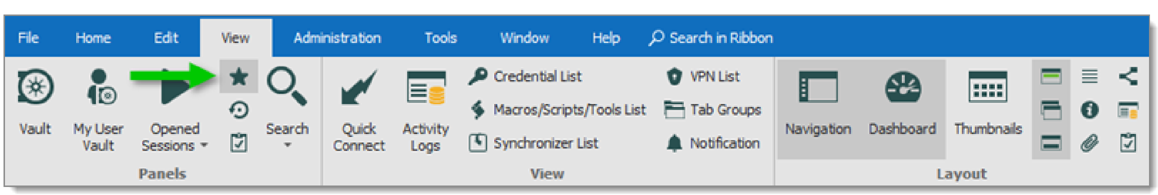
This is useful when the number of managed entries becomes too great or when a strict directory structure must be maintained.



Favorites UI

The favorites view can be personalized to show the sub-connections. Click on ••• and select ***Show Sub-Connections***. You can also ***Import*** and ***Export*** favorites by clicking on the corresponding option.

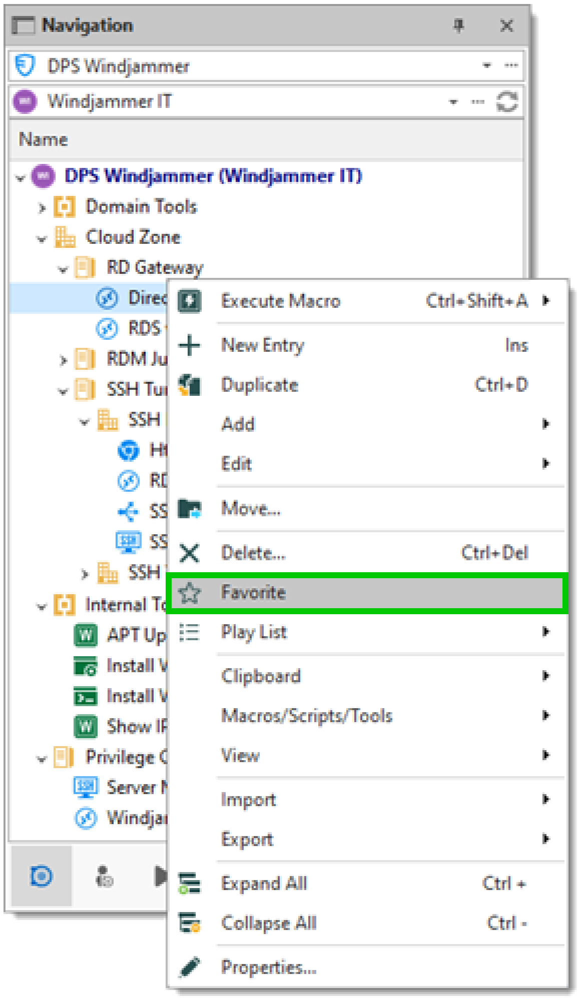
A shortcut to the ***Favorites*** tab of the ***Navigation Pane*** is located in the ***Panels*** section of the ***View*** tab.



View - Panels - Favorites

FLAG AN ENTRY AS FAVORITE

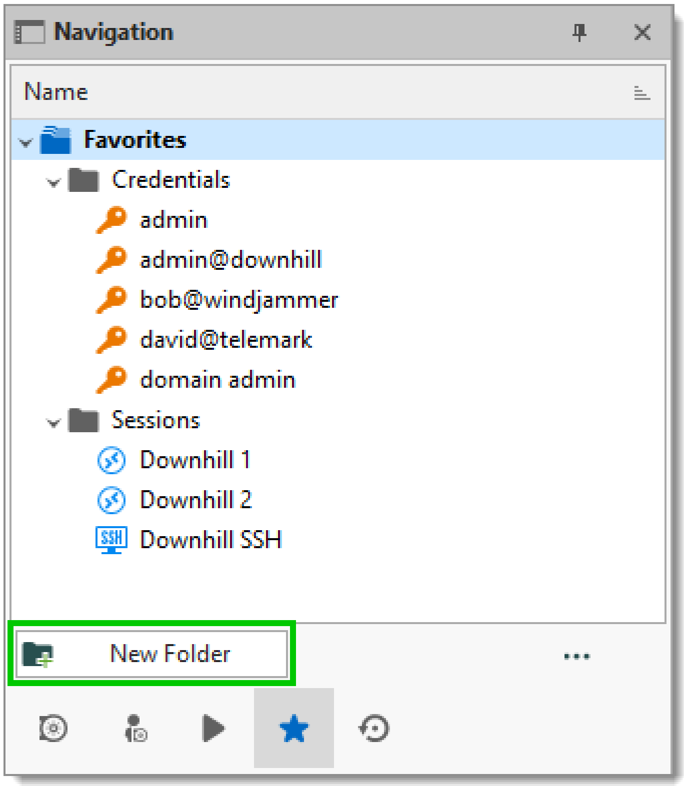
Right-click an entry in the Navigation Pane, then select **Favorite**.



Flag an entry as favorite

ORGANIZE THE FAVORITES

Favorites do not necessarily replicate the folder structure of the Vault. Add folders in the favorite view to organize your favorite entries.



Add folders to organize favorites

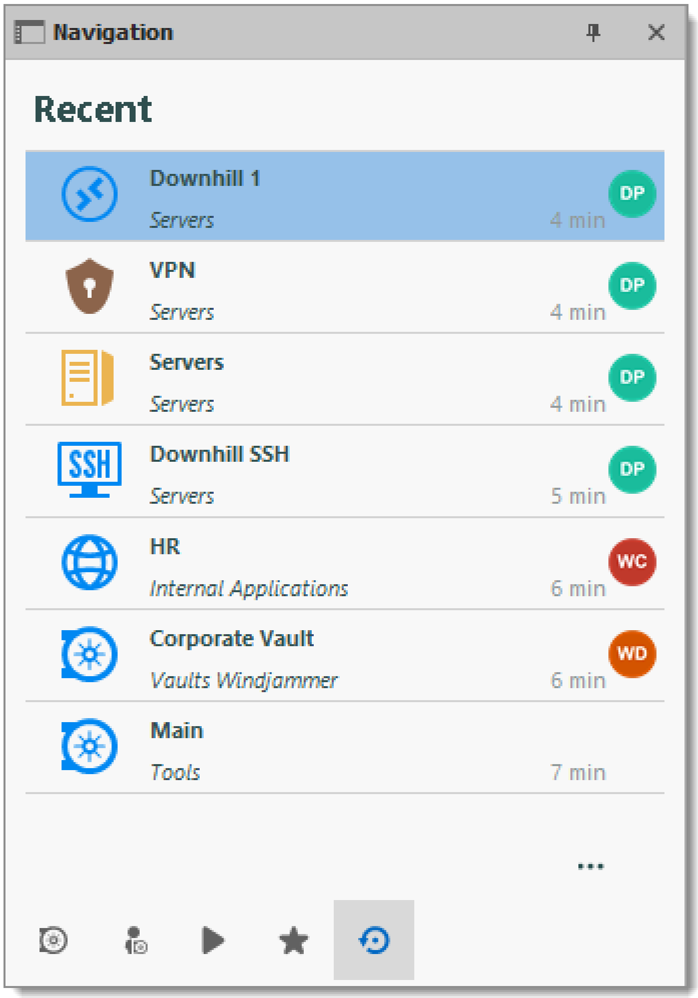
ICON OVERLAY

If desired, an icon overlay can be displayed in the Vault over favorite entries. To display the icon overlay, navigate to ***File - Options - User Interface - Favorites***, then enable the **Show favorite icon in navigation tree** option.

4.3.2 Most Recently Used Entries

DESCRIPTION

This tab shows the most recently used/modified items in the selected vault. It is accessible in the ***Navigation Pane***.



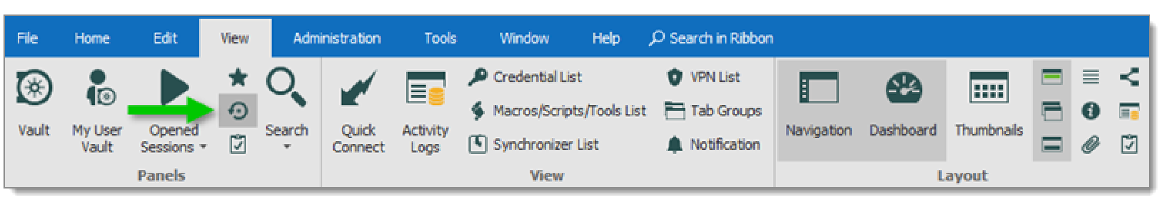
Most recently used entries

The ***Recent*** view can be customized in the same way as the tree view. Click on the ••• button to select your preferred view (***Tiles*** or ***Details***).

To delete the most recently used entries history, select ***Clear Recent Entries***.

By default, ten items will be kept in the ***Recent*** history. This setting can be changed in ***File - Options - Application - Recent***.

The ***Recent*** tab can also be accessed from the ***Ribbon*** in ***View - Panels - Recent***.



View - Panels - Recent

4.3.3 Navigation Pane Key Mapping

DESCRIPTION

Remote Desktop Manager, being a Windows application, supports key mapping in its navigation pane.

To expand a current folder: right arrow or + (plus) sign.

To collapse a current folder: left arrow or - (minus) sign.

To expand all from here: * (star) sign.

4.4 Content Area

DESCRIPTION

The content area contains the various dashboards to manage RDM, as well as embedded sessions. There is a single dashboard active at a time, depending on the currently selected node in the Navigation Pane.

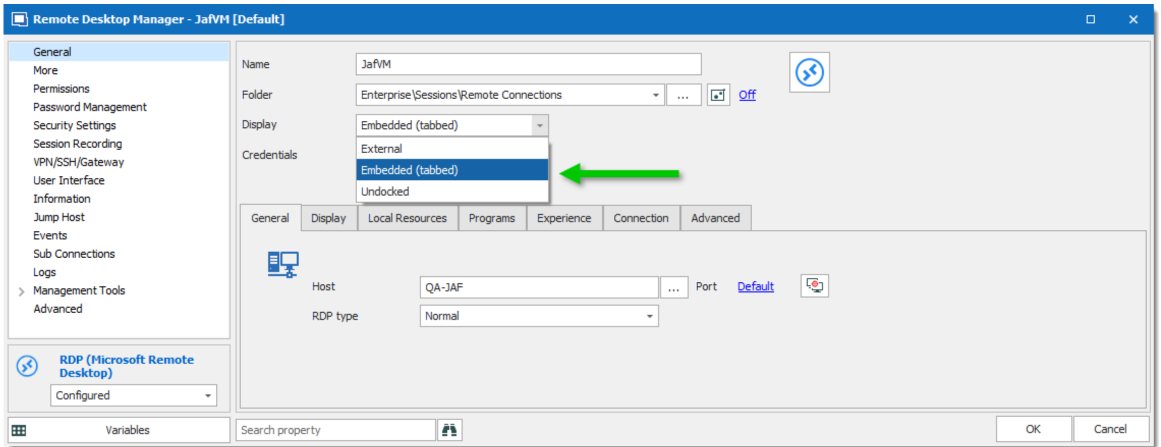
The options change depending on the entry:

- Sessions.
- Information Entries.
- Folders.
- Credentials.
- Macros/Scripts/Tools.

4.4.1 Embedded Sessions

DESCRIPTION

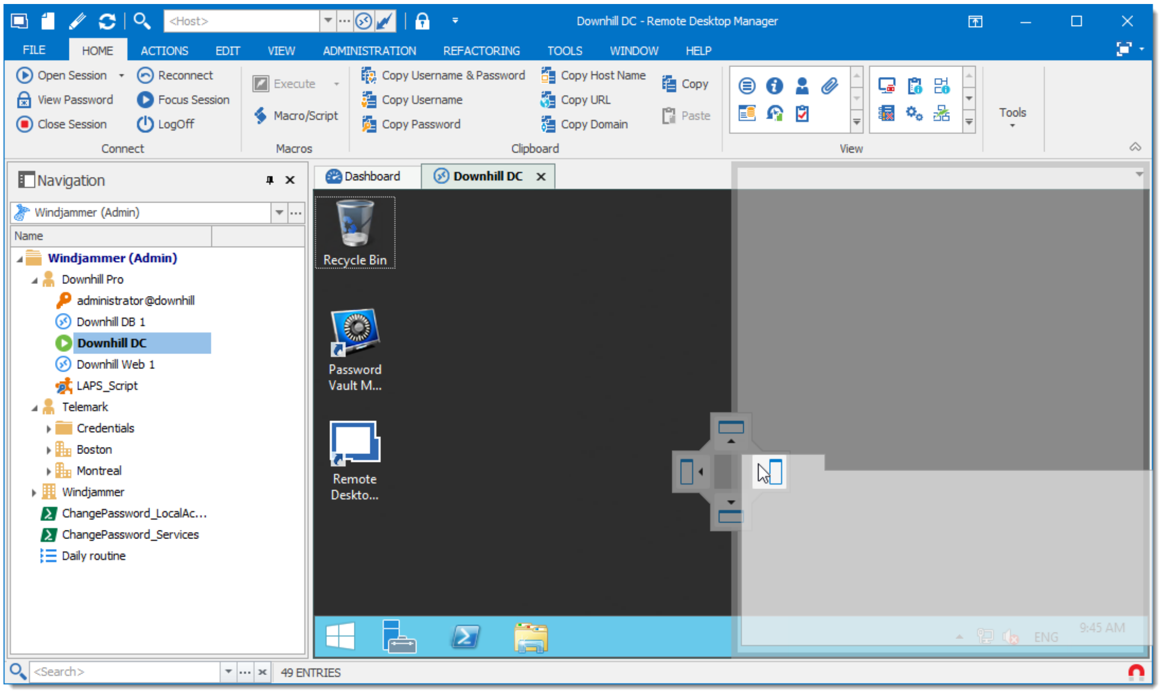
The **Embedded (tabbed)** display mode allows you to open multiple sessions as tabs withing Remote Desktop Manager, similar to the tabs in your standard web browser. Embedded sessions are one of the 3 available display modes, the other 2 being **External** and **Undocked**.



Display Mode Settings

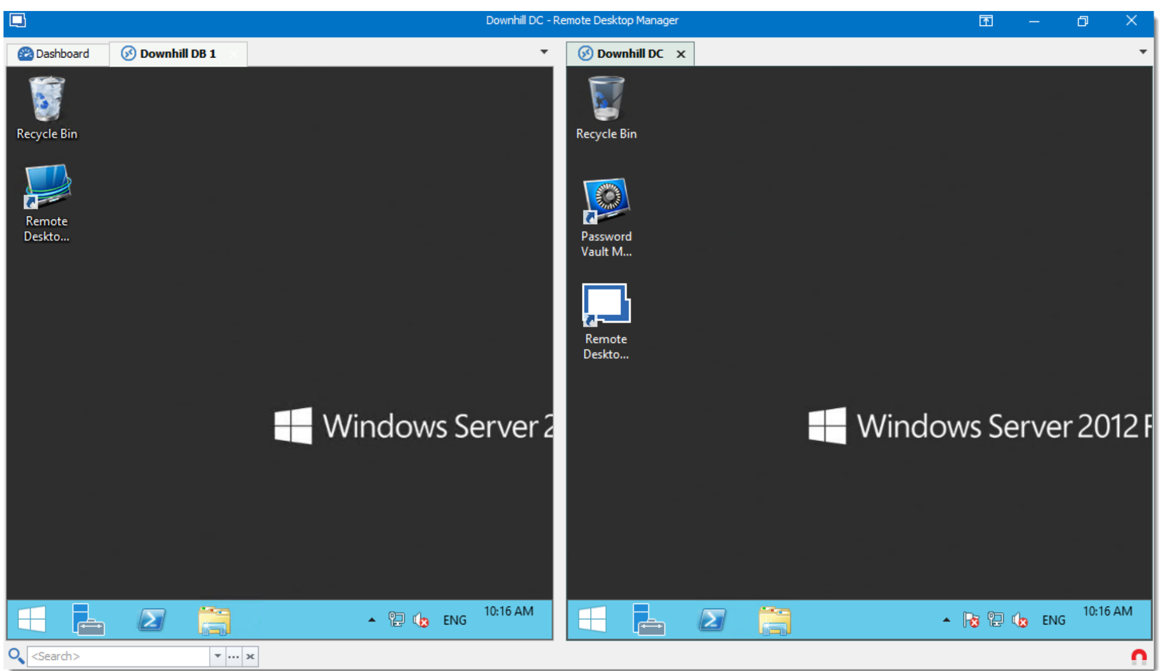
SPLIT WINDOWS

Within a Remote Desktop Manager embedded session is the option to display multiple tabbed windows simultaneously. As illustrated below, select and hold down on a tab and drag it towards the center of the screen to access the four-sided directional control. Aim the directional control to anchor the tab to the top, bottom, left or right of the adjacent tab.



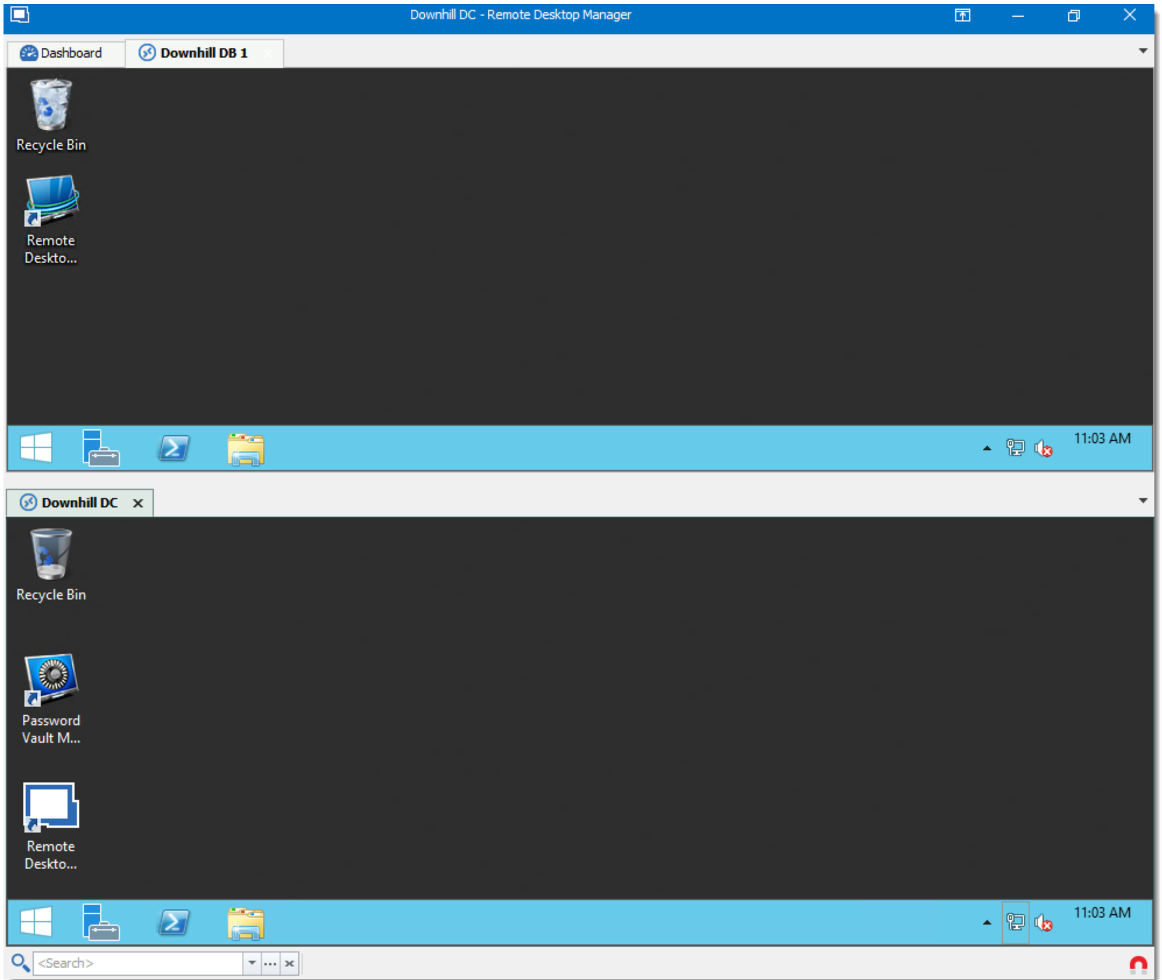
Split Window - Drag And Drop

Below is an example of a side-by-side split window.



Split Window - Side-By-Side

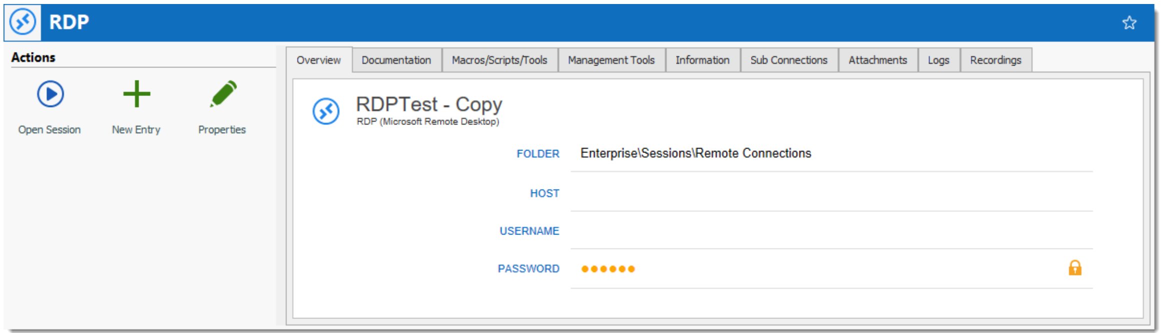
Below is an example of a top-down split window.



4.4.2 Dashboard

DESCRIPTION

The **Dashboard** displays commands and information related to the selected entry. The dashboard contents depend on the type of the selected entry.



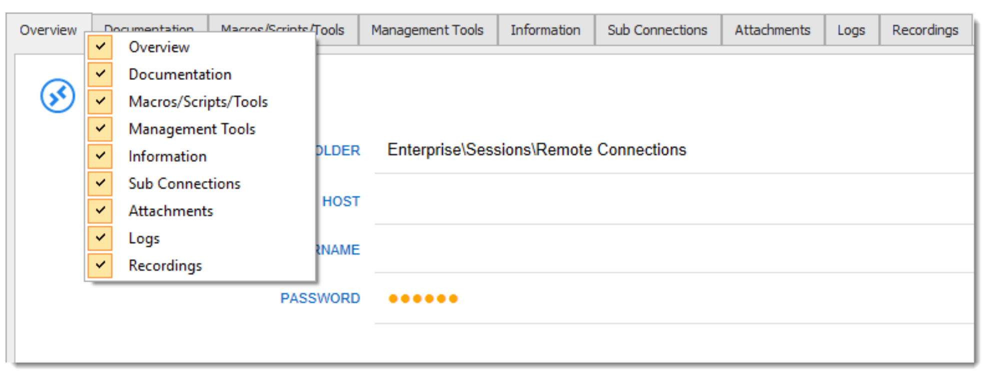
Dashboard for credential entry

The different tabs available in the dashboard:

- **Actions** - Add special Open actions to dashboard, similar to ***Open Session*** *or* ***Properties*** in the contextual menu. Configure in **File** – **Options** – **User Interface**
- **Overview**
- **Documentation**
- **Macros/Scripts/Tools**
- **Management Tools**: Configure the Hyper-V, VMware, XenServer Dashboard before using the dashboard.
- **Information**
- **Sub Connections**
- **Attachments**
- **Logs**
- **Recordings**

The tabs can be hidden if they are not necessary for a user.

Simply right-click any tab, then select an item to toggle the visibility of its relative tab.



4.5 Status Bar

The status bar rests at the bottom of the application. It is composed of multiple parts

- Search / Filter.
- Remote Desktop Manager version label.
- The Online / Offline toggle.
- Grab input toggle.

Status bar

SEARCH / FILTER

Please consult the Search/Filter for detailed explanations.

ONLINE / OFFLINE TOGGLE

This feature is indicated by the green globe between the version label and the Grab input toggle. Clicking it will change your connection between offline and online (for RDM only). You can tell which connection state you are currently using by the color of the globe. Green is online and orange is offline.

GRAB INPUT TOGGLE

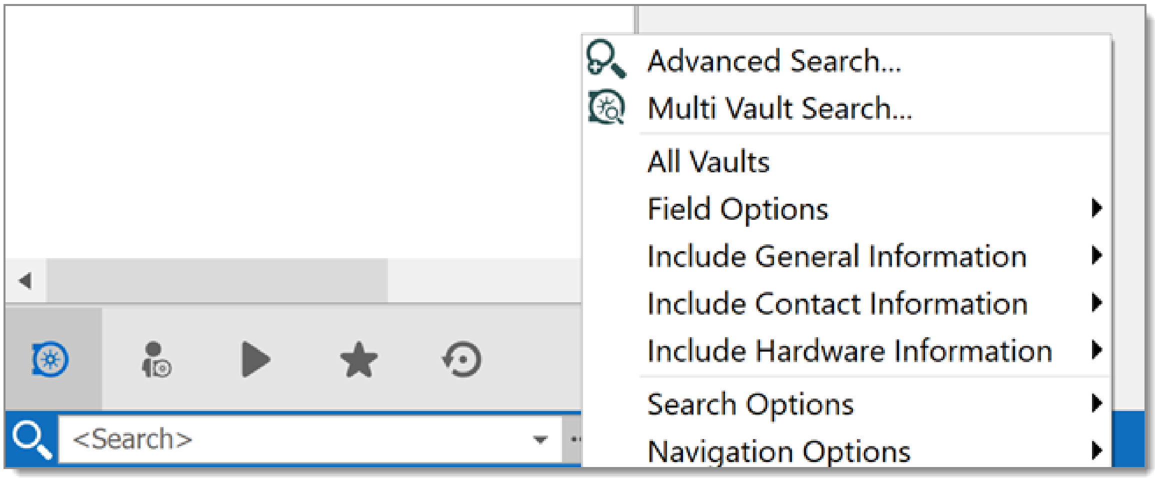
Please consult Grab Input for detailed explanations.

4.5.1 Search/Filter

It is possible to apply a filter in the Navigation Pane tree view by typing some characters in the filter box. The filter is applied using the specified settings in the application ***File – Options – User Interface – Filter***.

ELLIPSIS BUTTON

Select the ellipsis button to display the options.



Ellipsis button

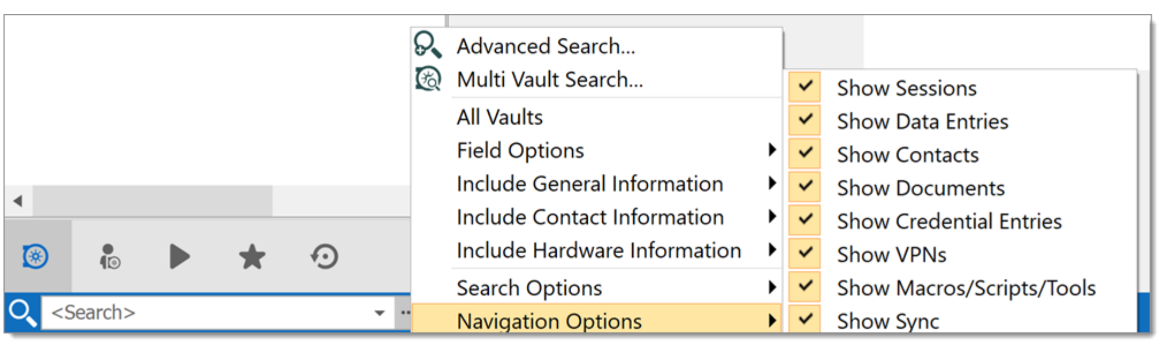
The filter expression is matched against fields as selected in the filter options such as:

- Search multiple or all Vaults at once.
- Field Options (Include Folder, Host, Username, etc.).
- General Information (Domain, IP, etc.).
- Contact Information (Name, Email, Phone number, etc.).
- Hardware Information (Serial number, Manufacturer, etc.).

It's possible to exclude results by choosing to display entries that match certain criteria:

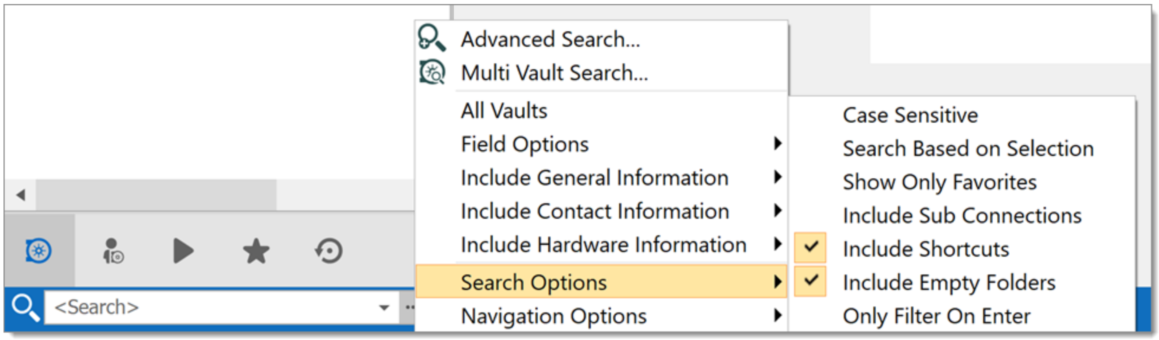
- Session types (credentials, script tools, VPN, etc.)
- If the session is marked as a Favorites

In Navigation options, you can limit the search parameters to specific entry types. Such as Sessions, Data Entries, etc.



Search Types

The Search Options offers the chance to customize your search, such as including shortcuts or favorites, making it case sensitive, and more!



Search Options

KEYBOARD SHORTCUT

Use the keyboard shortcut CTRL+F to quickly have access to the Search / Filter control. This can be disabled in ***File - Options - User Interface - Keyboard.***

You can set the focus back on the Navigation Pane by using the keyboard shortcut Ctrl+L, this also can be disabled in the options.

BOOLEAN FILTER

Here a few implementation notes for the Boolean filter:

- We use the C# nomenclature (&& for AND, || for OR)
- Evaluated left-to-right
- No parentheses matching
- Double-quotes (") are not required or removed, they are part of the text filter, do not use them unless you are looking for a double-quote.
- Leading/trailing white-spaces are trimmed

EXAMPLES (THIS WILL WORK)

- Boise && Laptop

- Boise&&Laptop
- Boise && Laptop
- Baton Rouge || Boise && Laptop
- Laptop && Baton Rouge

EXAMPLES (THIS WILL NOT WORK AS EXPECTED)

- Laptop && "Baton Rouge"

- Will work but filter for the string "Baton Rouge" and not the string Baton Rouge

- Laptop && (Baton Rouge || Boise)

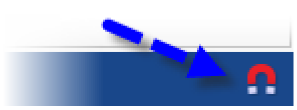
- Will work but filter for Laptop and the string (Baton Rouge || Boise)

4.5.2 Grab Input

DESCRIPTION

The **grab keyboard input** is used to capture the keyboard shortcuts when a session is running. It can be disabled momentarily to ensure that the shortcut is sent to the running session.

Ctrl+F is a shortcut that often interferes. It is used to focus Remote Desktop Manager's search/filter toolbar. However, it is almost always present in applications in the remote session and when you use the shortcut, Remote Desktop Manager sets the focus in the search/filter toolbar instead. This conflict can be avoided by disabling the feature.



Grab keyboard input

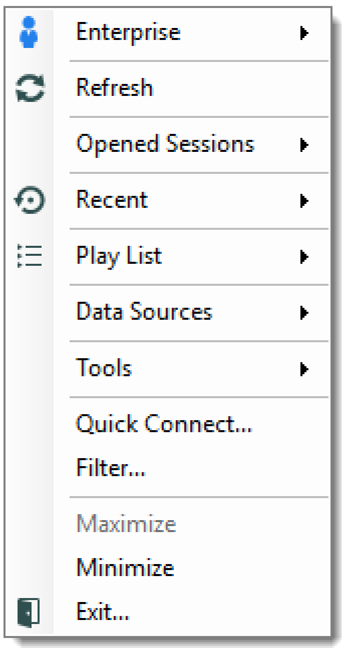
4.6 Tray Icon

DESCRIPTION

Remote Desktop Manager allows the user to control the application from the Windows system tray. You can also customize its content.

TRAY ICON CONTEXT MENU

Right-click on the Windows tray menu bar to access the context menu. You can launch sessions, change data source, use the Quick Connect feature, and more.



Tray Icon Context Menu

OPTION	DESCRIPTION
Sessions List	Displays the sessions from the current data source. Sessions are listed by default. It is possible to show only those marked as favorites.
Refresh	Refreshes the data source.
Opened Sessions	Lists all the currently open sessions.
Recent	Lists the Most Recently Used Entries.
Play List	Allows the user to launch a Play List from the tray icon.
Data Sources	Lists the available Data sources and allows the user to switch from one to another. This section appears only if enabled and more than one data source is

OPTION	DESCRIPTION
	configured.
Tools	Lists all the configured tools.
Quick Connect	Prompts for the Quick Connect dialog to open an add-hoc connection with a specific type, or a selected template.
Filter	Launches the Search/Filter feature.
Maximize	Restores the application to full screen.
Restore	Restores the application from minimize.
Minimize	Minimizes the application in the task bar.
Exit	Closes the application.

TRAY ICON PREFERENCES

The application options contain many settings that allows for customizing the system tray icon preferences. To change these, Navigate to ***File – Options – User Interface – Trayicon/Taskbar***.

Data Sources

Part V

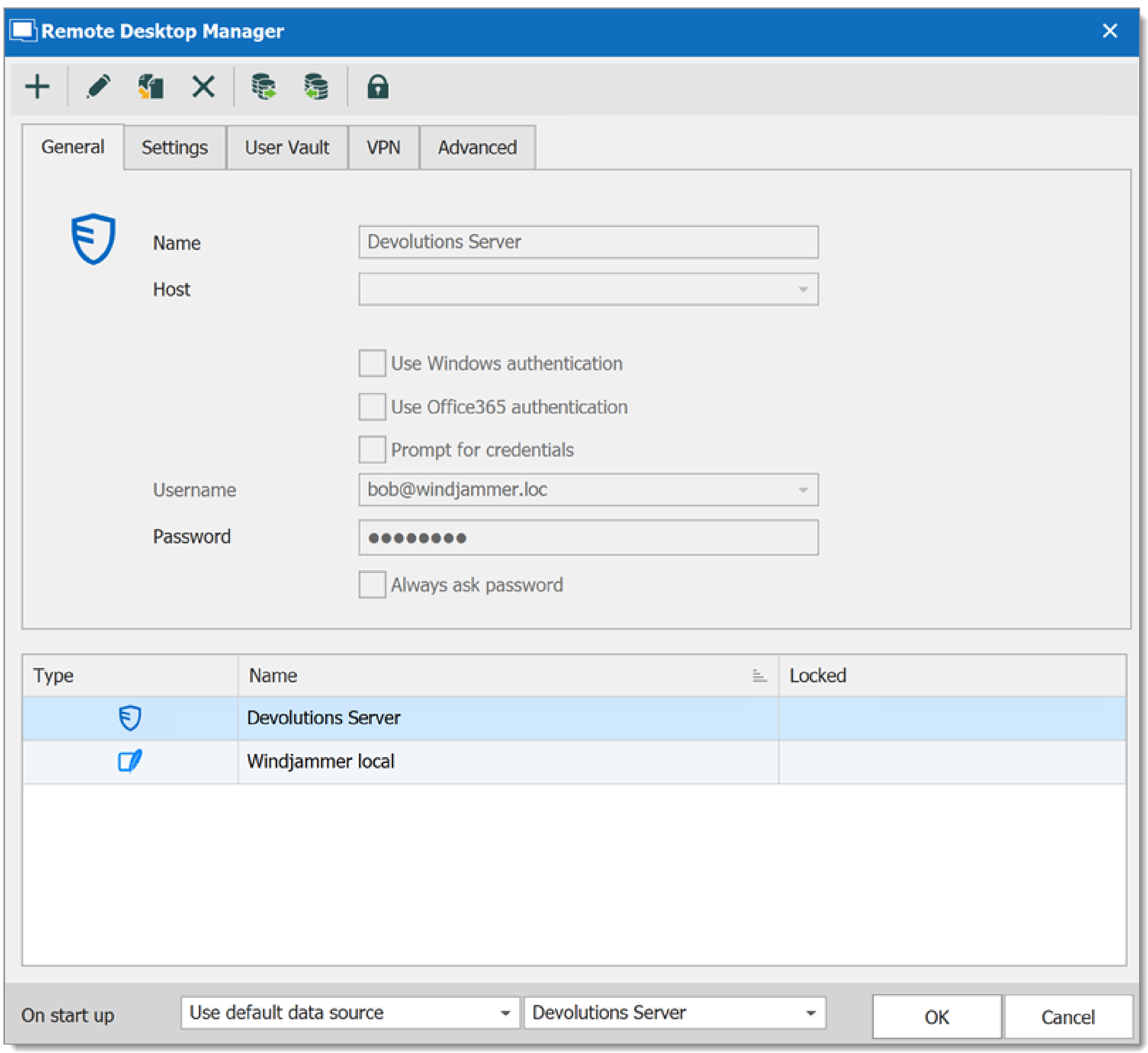
5 Data Sources

DESCRIPTION

The data sources are at the heart of Remote Desktop Manager, they are the container that holds entries.

SETTINGS

A data source can be a local file or a database (either local or shared). Multiple data sources can be managed at the same time as seen below.



Data Source

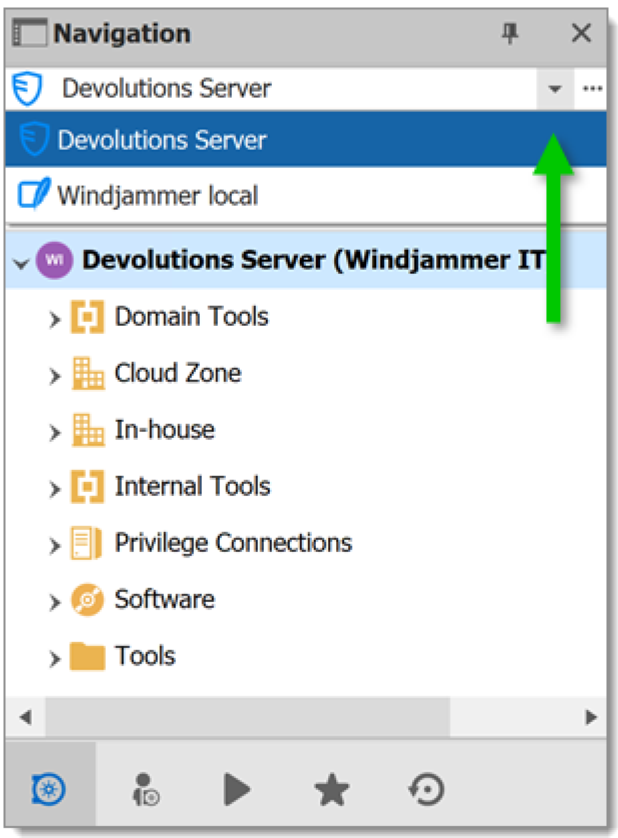
CREATE A DATA SOURCE

Please consult our Create a new data source topic for more information.

MULTIPLE DATA SOURCES

Multiple data sources can be configured, but there is only one active at a time.

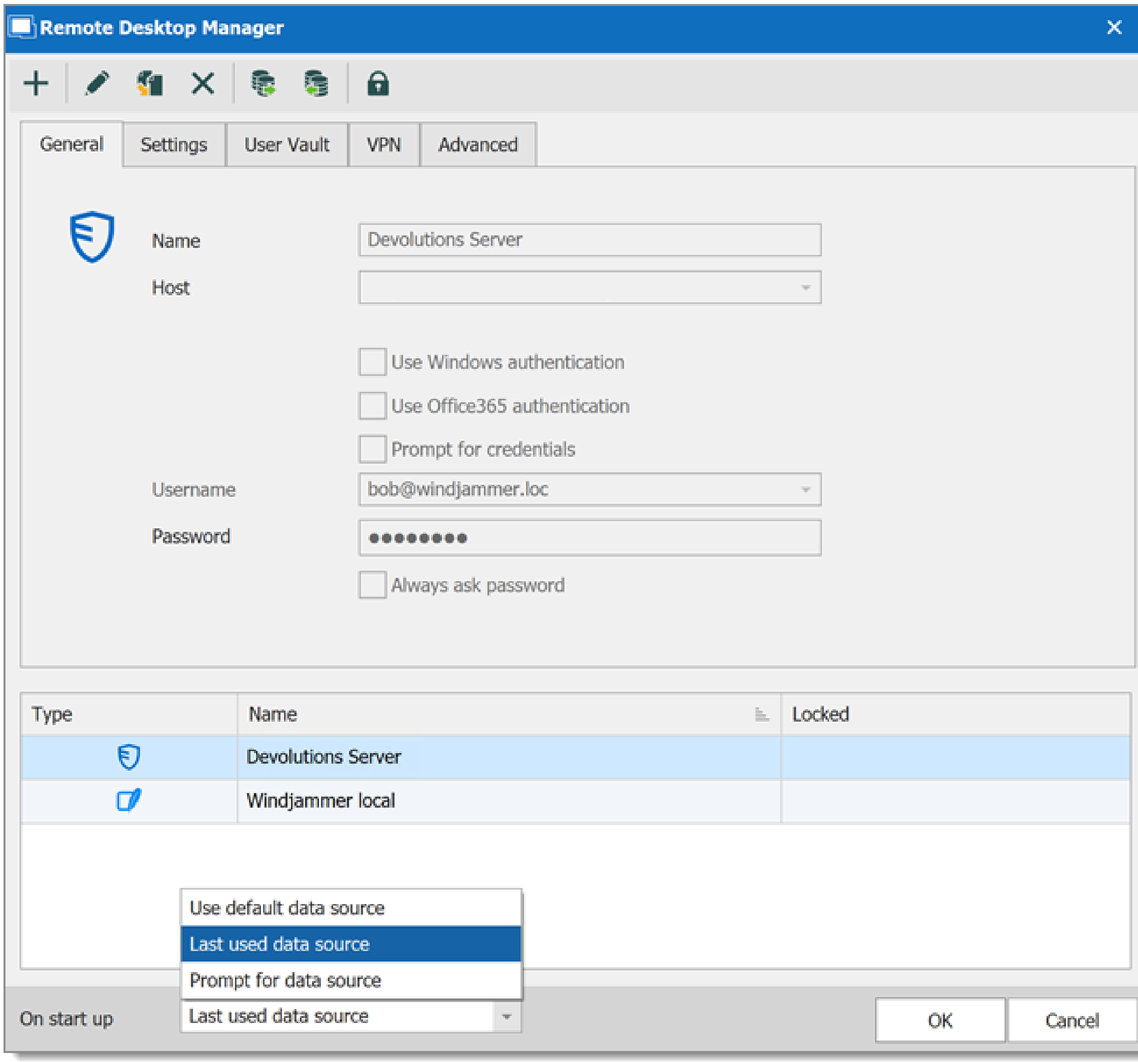
Switch from one data source to another by using the data source drop down list.



Select a Data Source

STARTUP DATA SOURCE

You may assign a data source to open automatically when Remote Desktop Manager starts.



Startup Data Source

OPTION	DESCRIPTION
Use default data source	Select the data source to connect to when the application starts.
Last used data source	Connect to the last used data source.
Prompt for data source	Prompt the user to for a data source to connect to.

DATA SOURCE SETTINGS (SYSTEM SETTINGS)

Advanced Data Sources can manage a lot more settings related to the database and security. Those settings are saved directly in the database. For more information, please consult the Data Source Settings (System Settings) topic.

5.1 2-Factor Authentication

DESCRIPTION

> This feature is only available for the following data sources: Devolutions Server, Microsoft Azure SQL, Microsoft SQL Server and SQLite.

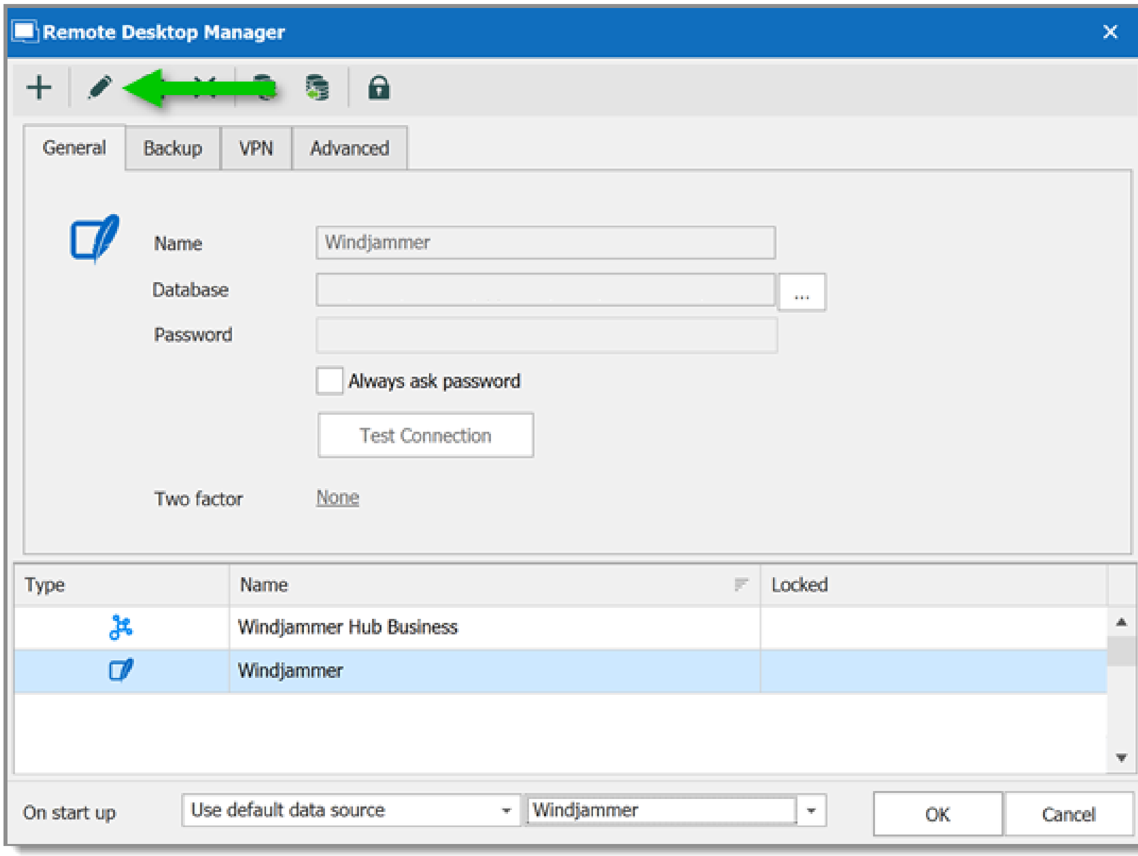
Two-factor authentication identifies users by two different components: something that the user knows (often a password) and something that the user possesses (e.g., a validation code sent to a mobile device).

If one of the components is missing or supplied incorrectly, the user's identity is not established with sufficient certainty and then access to the data source will remain blocked.

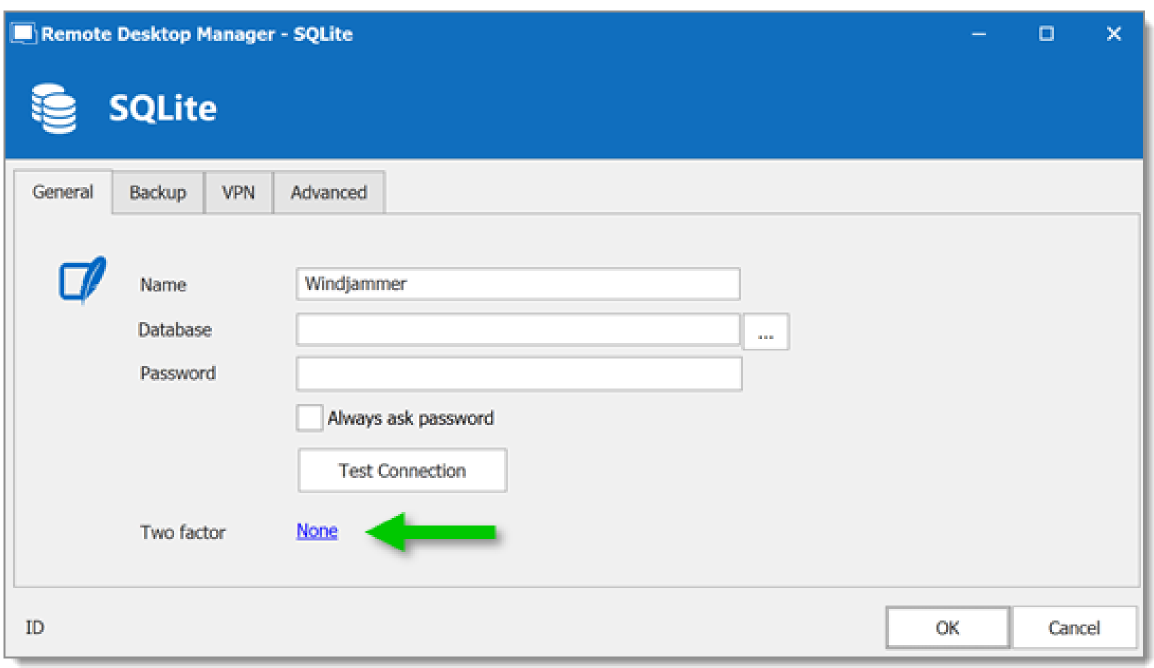
It is set at the Data Source level and Remote Desktop Manager supports Authenticator (TOTP), Yubikey, and Duo.

HOW TO CONFIGURE TWO-FACTOR AUTHENTICATION

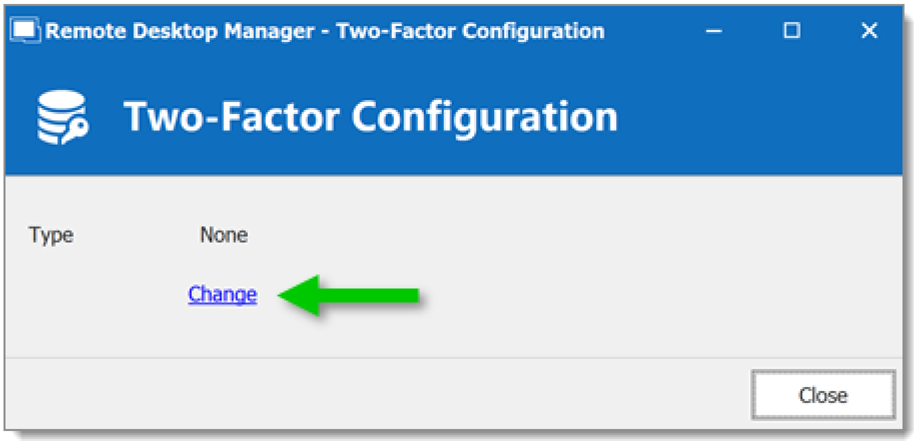
1. Click ***File - Data Sources***.
2. Select your ***Data source***.
3. Click the pencil to ***Edit Data Source***.



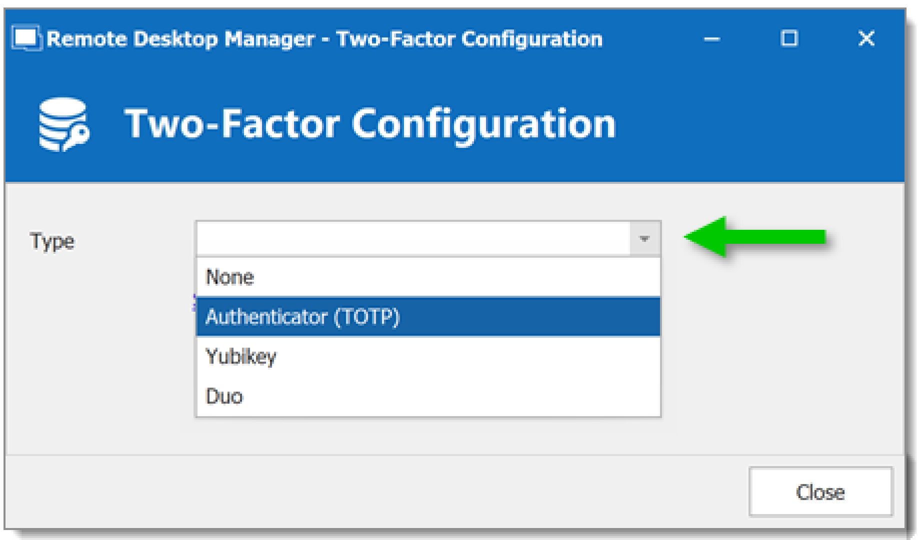
4. In the ***General*** tab click ***None***.



5. Click ***Change***.



6. Select your 2-Factor Authentication type.



7. Click ***Save*** to start the configuration.

To configure your specific 2FA, please select your type link:

- Authenticator (TOTP)
- Yubikey
- Duo

5.1.1 Authenticator (TOTP)

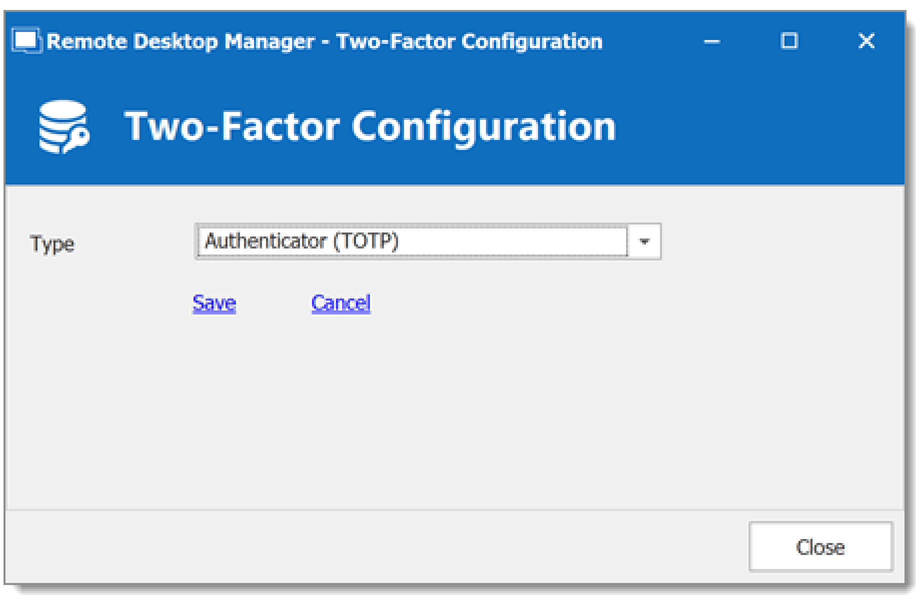
DESCRIPTION

Remote Desktop Manager allows you to use an ***Authenticator (TOTP)*** such as Devolutions Workspace or Google Authenticator to provide an additional security layer when opening a data source.

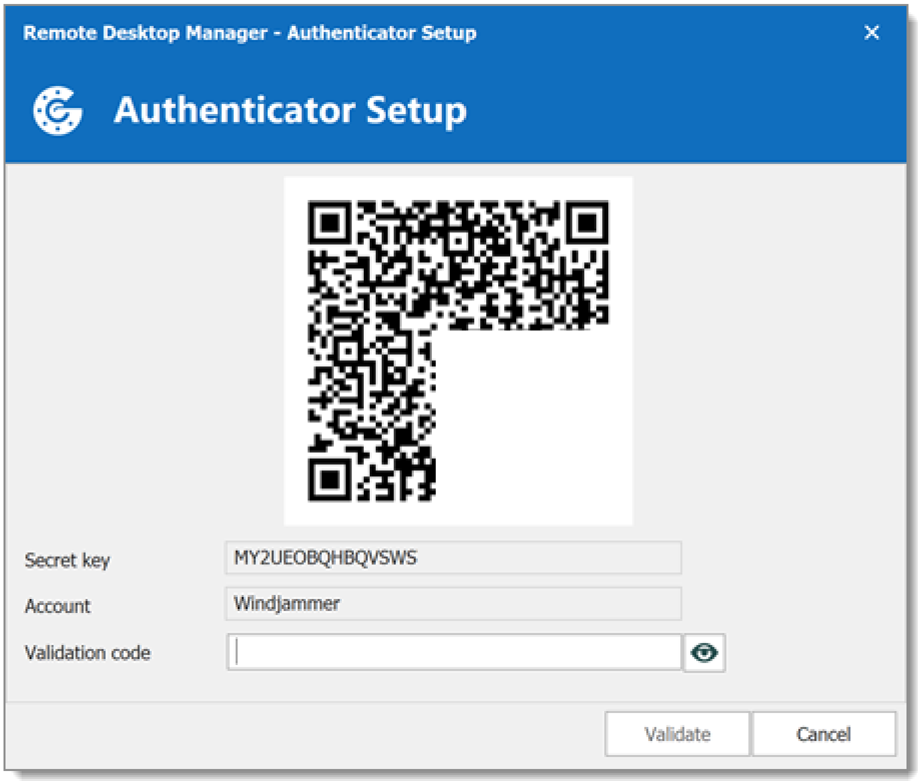
SETTINGS

Before you start the configuration, make sure you have installed the Devolutions Workspace or Google Authenticator application on a supported device.

1. Select ***Authenticator (TOTP)*** as your ***Type***.
2. Click ***Save***.



3. Scan the ***QR Code*** with your device application.
4. Enter the ***Validation code*** provided by the ***Authenticator (TOTP)*** in Remote Desktop Manager.
5. Click ***Validate***.



6. Relaunch Remote Desktop Manager to be prompted for the ***Authenticator (TOTP)*** code.

5.1.2 Yubikey

DESCRIPTION

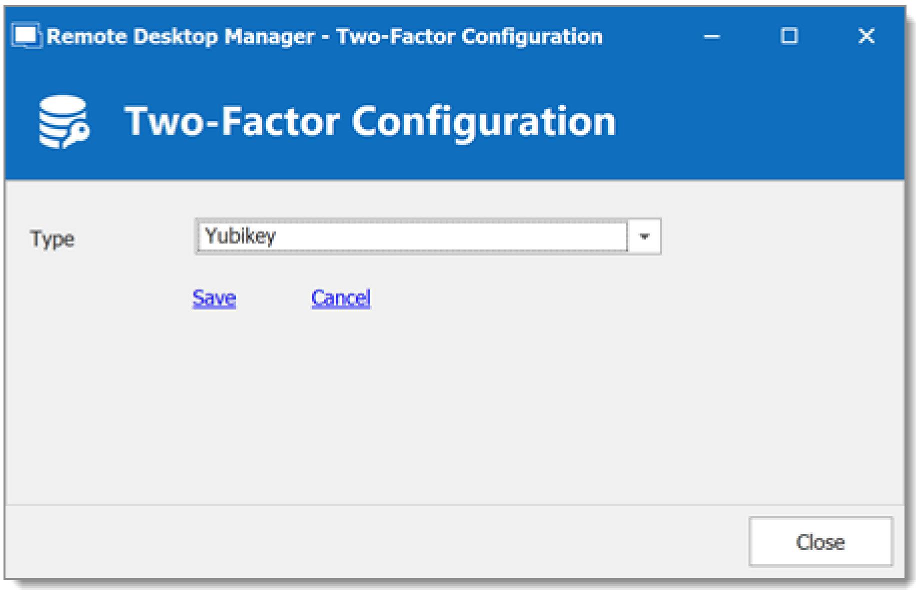
Remote Desktop Manager allows you to use a Yubikey to provide an additional security layer when opening a data source.

> Remote Desktop Manager only support the Yubico OTP at this time.

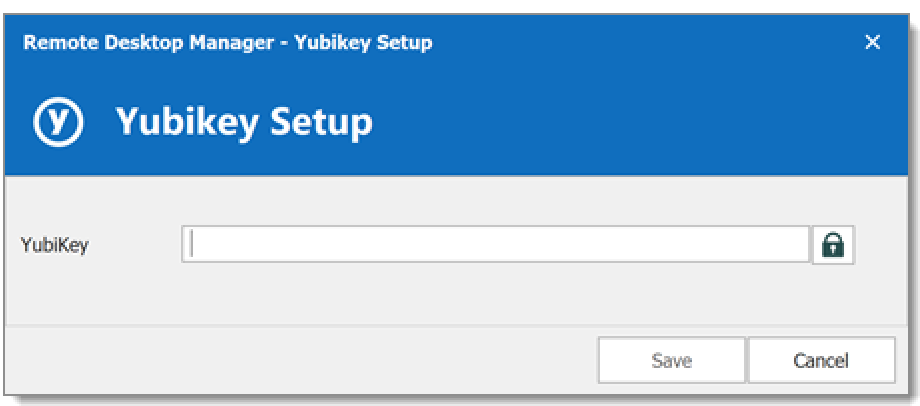
SETTINGS

> Before you start the configuration, make sure you have a Yubikey in your possession.

1. Select ***Yubikey*** as your ***Type***.
2. Click ***Save***.



3. Insert the Yubikey into a USB port of your computer
4. Hold the gold button on the Yubikey to have the code filled in the field
5. Click ***Save***.



6. Relaunch Remote Desktop Manager to be prompted for a Yubikey code.

5.1.3 Duo

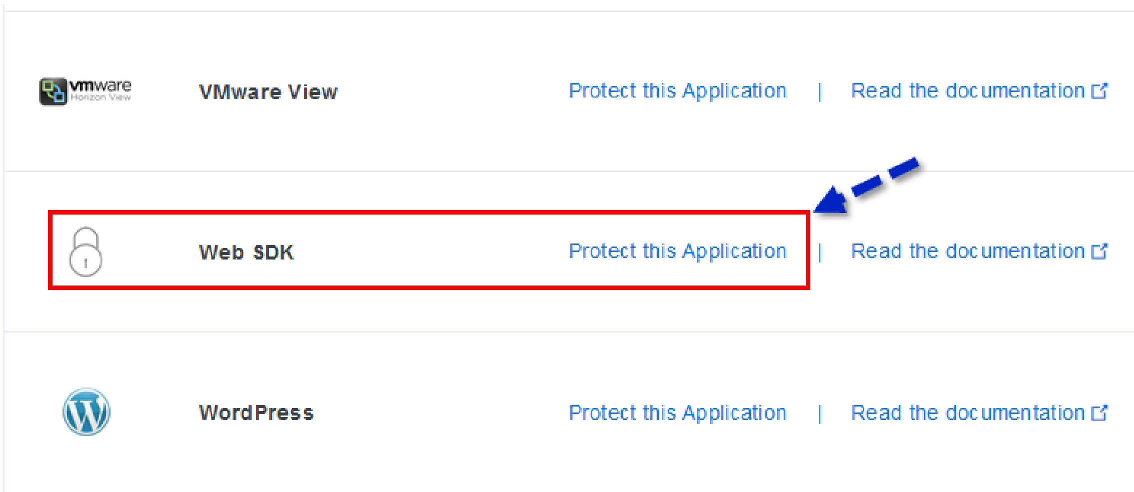
DESCRIPTION

Remote Desktop Manager allows you to configure a Duo Authentication to provide an additional security layer when opening a data source.

SETTINGS

> Before you start the configuration, make sure you have created yourself a Duo account and have also installed the Duo application on your compatible device.

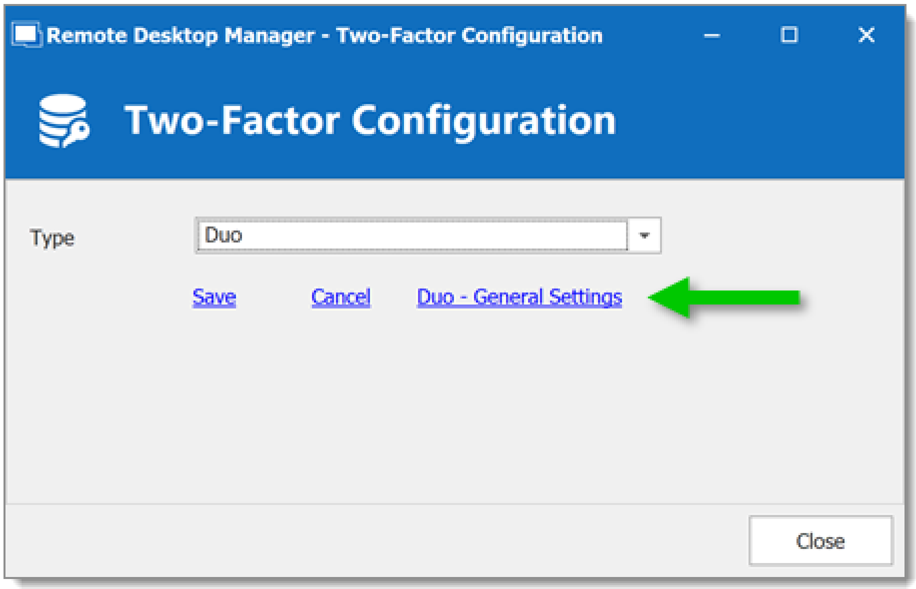
1. In your Duo account, you will need to protect the application **Web SDK**.



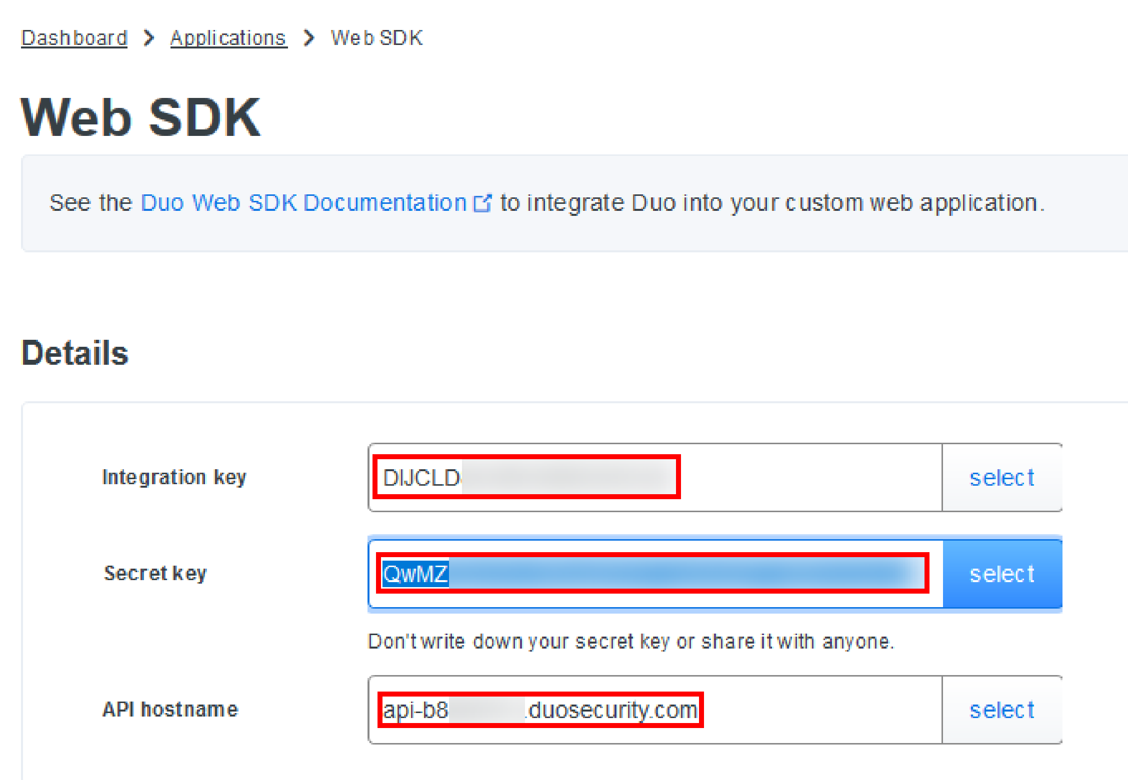
Web SDK application

2. In Remote Desktop Manager select the ***Type***.

3. Click ***Duo - General Settings***.



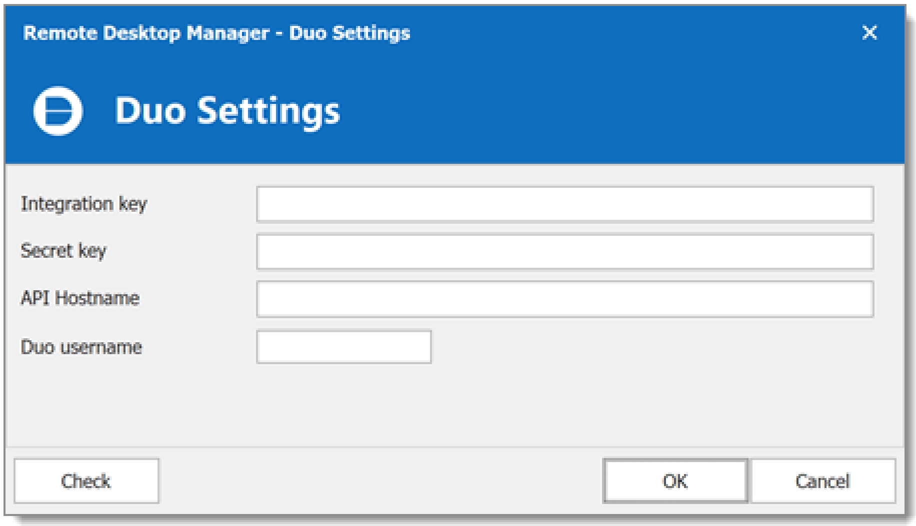
4. All the information necessary to fill in the ***Duo Settings*** fields will be generated by your Duo account.



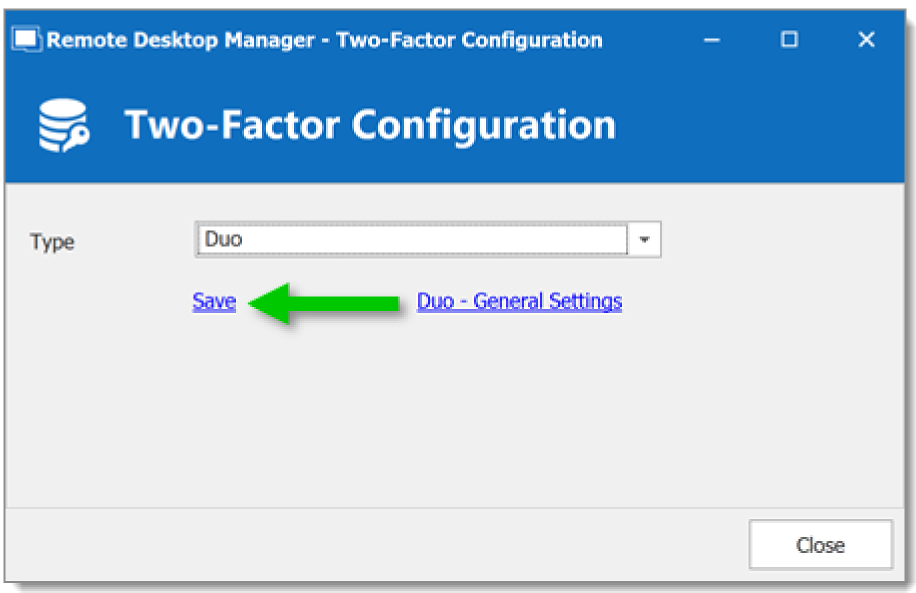
Duo Account - Web SDK

5. Copy and paste all the information.

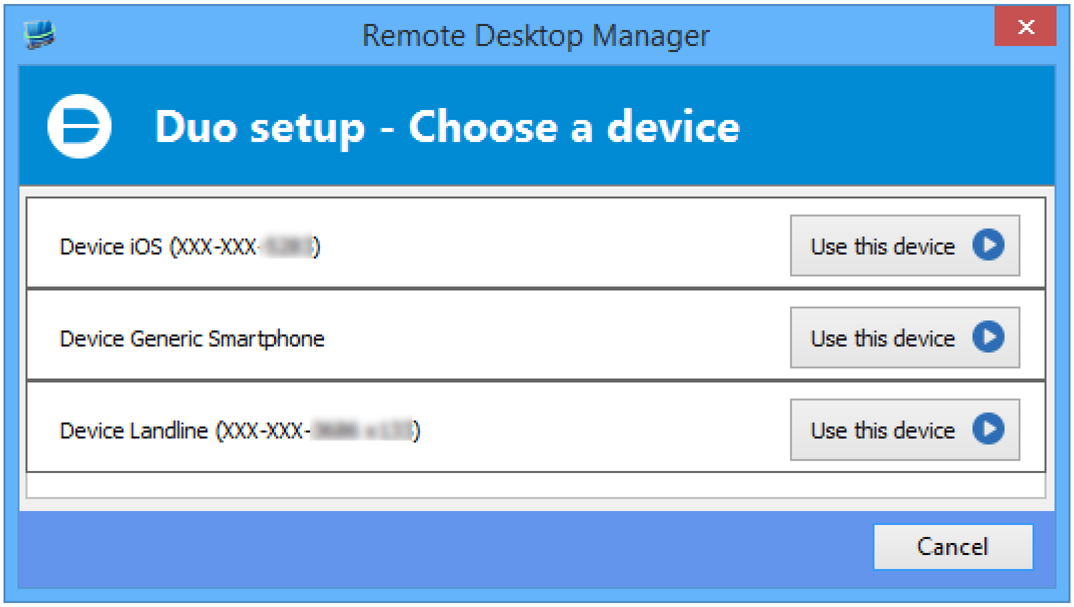
6. Click ***Check*** to validate the information and ***OK*** when done.



7. Click on ***Save*** to authenticate yourself.



8. If you have more than one device connected to your Duo account, select the device you wish to use for your 2-Factor authentication.



9. Select the method by which you would like to receive your Duo Passcode.

- ***Duo Push***: The code is "pushed" to your Duo application.
- ***Send SMS***: You will receive the code by SMS on your registered phone number.
- ***Phone***: You will receive a phone call and a computer generated voice will dictate the code to you.

Once you have completed all the steps, you will be prompted with the Duo Authentication every time you connect to your secured data source.

5.2 Caching

DESCRIPTION

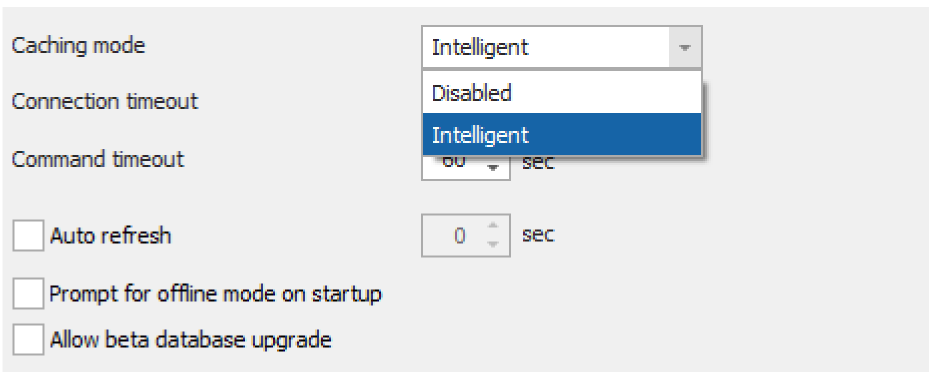
The caching mode will determine how the client will refresh the content of the data source when changes are detected. On large data sources caching is essential as it increases performance significantly.

> This feature is only available when using an Advanced Data Source.

If the cache is outdated, press **CTRL + Refresh** or **CTRL + F5** to refresh the local cache. This will force the application to retrieve the entire content of the data source to recreate the cache.

SETTINGS

The **Caching mode** option can be access via the ***File – Data Sources – Edit Data Source – Advanced tab*** of an Advanced Data Source.



Caching Mode

OPTION	DESCRIPTION
Disabled	No client caching.
Intelligent	Intelligent cache has the ability to handle many more sessions without experiencing performance degradation. In the case of intelligent cache each modification performs a token update on the server. When Remote Desktop Manager performs a refresh action it will query the data source for any changes (delta) of changes to be applied client side since it last checked the data source. The delta of the changes is then sent to the application and applied locally. When first opening the data source Remote Desktop Manager will loaded the session from the offline file then refresh to get the up-to date information.

LOCATION

The client cache is persisted to disk in ***%LocalAppData%\Devolutions\RemoteDesktopManager\[GUID:DataSourceID]***

There are three engines for the cache:
- SQLite (offline.db).
- MCDF (offline.mcdf).
- MCDF v2.0 (offline.mcdf2).

If using a version of Remote Desktop Manager prior to 11.2, the default engine will be the **SQLite**, in that case the database is encrypted using a non-portable computed key hash.

If using version 11.2 or newer of Remote Desktop Manager the default cache engine will be the **Microsoft Compound Document Format (MCDF)** files.

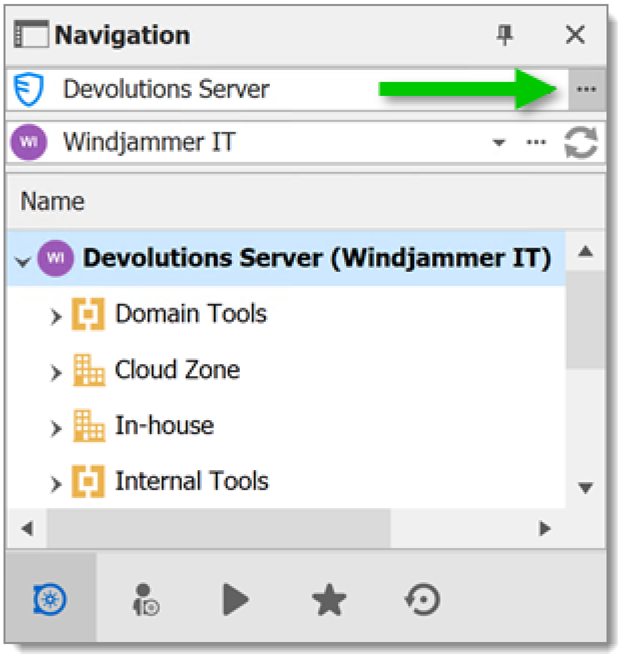
> You can enhance the security of the offline file by setting the Enhanced security in ***File – Options – Security – Offline Security.***

> Depending on the configuration of the Caching mode & the Offline mode the offline file may still exist since the file servers as a dual purpose caching & offline line support.

5.3 Create a data source

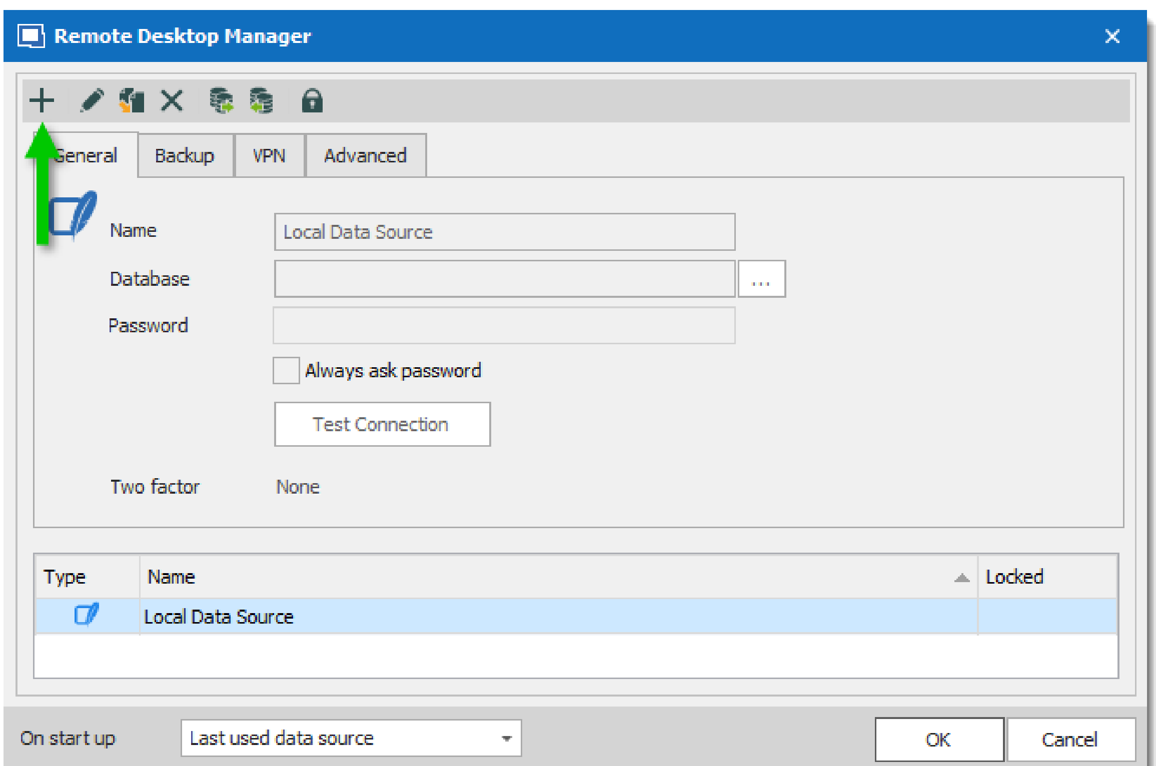
SETTINGS

1. Open the **Data Source Configuration** window in ***File - Data Sources*** or by clicking the **ellipsis** button (Will only show if you already have 2 existing data sources configured in Remote Desktop Manager) at the top of the Navigation Pane.



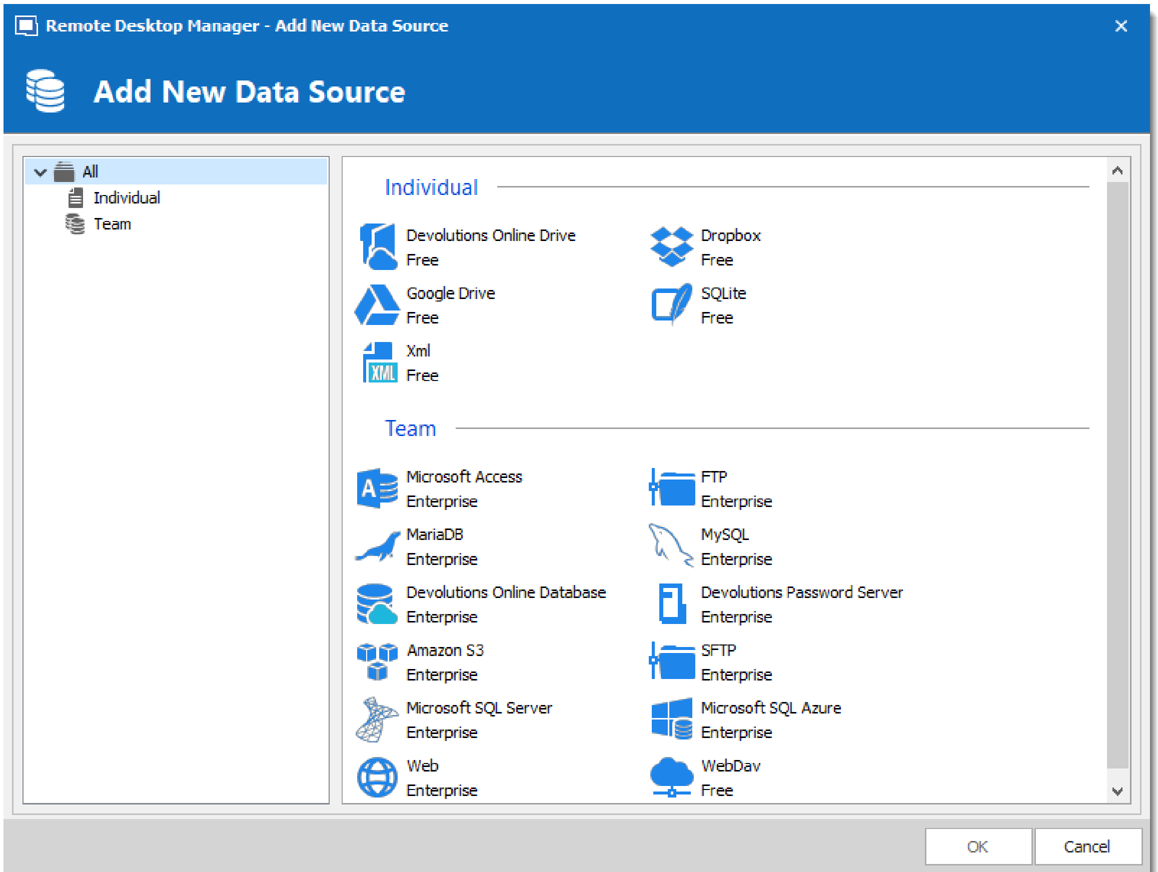
Open Data Source menu

2. Click the **Add a New data source** ➕ button.



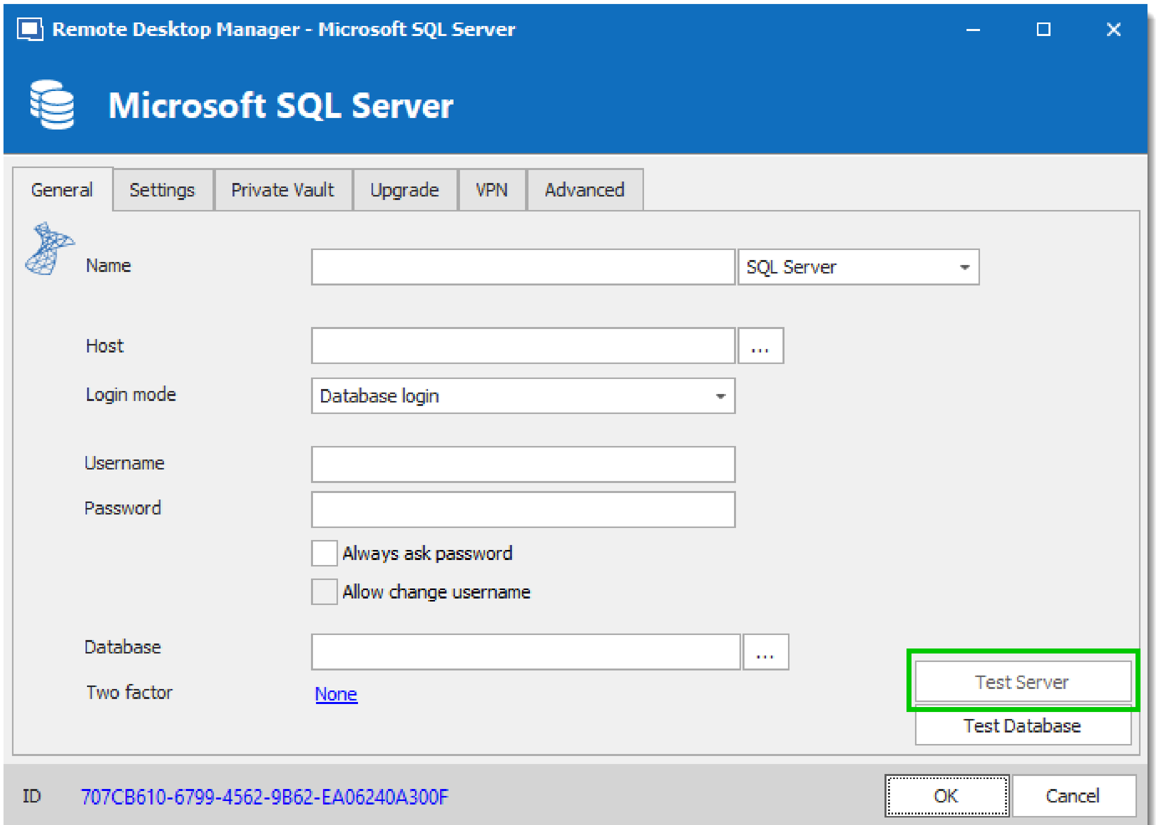
Add a new Data Source

3. Select the type of data source to create.



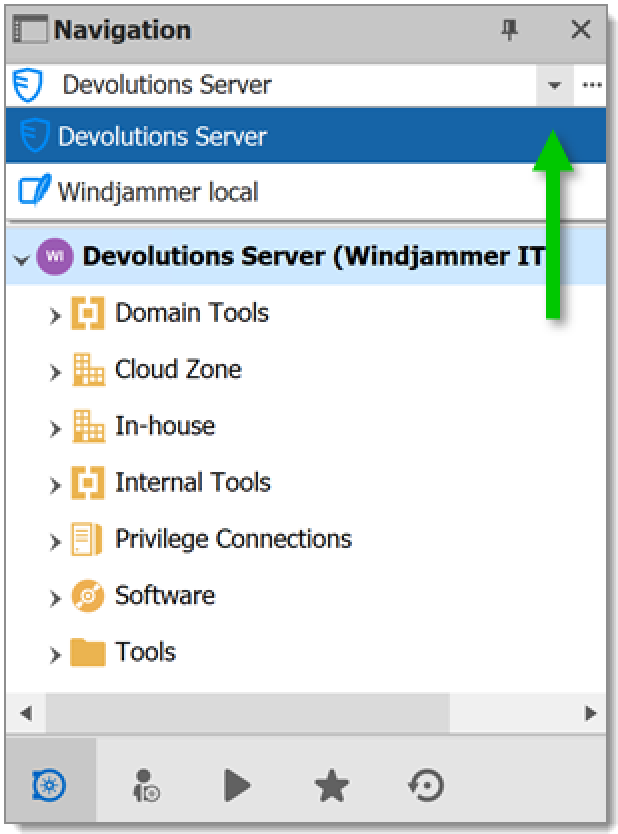
Select your Data Source type

4. Configure the connection settings. To validate the information, click the **Test Server** or **Test Connection** (depending on the type of data source being creating).



SQL Server - Connection Tab

5. Once created, select the new data source by selecting it from the data source drop down list at the top of the Navigation Pane.



Select your Data Source

5.4 Data Source Types

DESCRIPTION

Remote Desktop Manager supports multiple types of data source. First decide which data source you are going to use.

> Upon initial installation, you will be running from a local data source which is a SQLite database.

DATA SOURCE TYPES

NAME	DESCRIPTION	PROS AND CONS
Devolutions Online Drive	Remote Desktop Manager uses Devolutions Online Drive to store and synchronize your sessions. Access your sessions from anywhere using an Internet connection. For more information, please consult our Online Drive topic.	Pros: • Quick. • Reliable. • Free service. Cons: • No possibility of sharing. • No security management.
Devolutions Password Hub Business	Remote Desktop Manager connects to the Devolutions Password Hub Business vault. Note that there are different subscription levels for this product. For more information, please see the products features and highlights and consult our Password Hub Business topic.	Pros: • Quick. • Reliable. • Secure. • Shareable. Cons: • Cannot be hosted on premises. • No offline mode.
Devolutions Password Hub Personal	Remote Desktop Manager uses Devolutions Password Hub Personal to store and synchronize your sessions. Access your sessions from anywhere using an Internet connection.	Pros: • Quick. • Reliable. • Free service.

NAME	DESCRIPTION	PROS AND CONS
	For more information, please consult our Password Hub Personal topic.	Cons: • No possibility of sharing. • No offline mode.
Devolutions Server	Remote Desktop Manager uses Devolutions Server to store session information. For more information, please consult our Devolutions Server topic.	Pros: • Quick. • Reliable. • Secure. • Supports all features, such as attachments, Usage Logs, Offline Mode and User Management. • Active Directory integration. Cons: • Installation required.
Dropbox	Remote Desktop Manager uses the Dropbox API to retrieve the XML file from the configured repository. For more information, please consult our Dropbox topic.	Pros: • Can be shared in read-only mode. • Backups (by Dropbox) are automatic. • Storage infrastructure is free (if within your free storage quota).

NAME	DESCRIPTION	PROS AND CONS
		Cons: • No security management. • There is a possibility for conflict or data corruption to occur. • Does not support all features, such as Attachments, Usage Logs, Offline Mode and User Management. • Dropbox integration uses the Dropbox SDK, so features exclusive to the Business or Enterprise editions are NOT supported.
Microsoft Azure SQL	Remote Desktop Manager uses the Microsoft cloud platform to save and manage all sessions. For more information, please consult our Azure SQL topic.	Pros: • Quick. • Reliable. • Secure. • Supports all features, such as Attachments, Usage Logs, Offline Mode and User Management. Cons: • Microsoft Azure needs to be configured.
Microsoft SQL Server	Remote Desktop Manager uses SQLServer to save and manage all sessions. This is one of the	Pros: • Quick.

NAME	DESCRIPTION	PROS AND CONS
	available data source for a multi-user environment. For more information, please consult our SQL Server (MSSQL) topic.	• Reliable. • Secure. • Supports all features, such as Attachments, Usage Logs, Offline mode and User Management. • SQL Server Express is free. Cons: • SQL Server must be installed.
SQLite	Remote Desktop Manager uses a SQLite database to store session information. For more information, please consult our SQLite topic.	Pros: • Quick. • Reliable. • Free database. • Supports all features, such as Attachments, Usage Logs, Offline Mode and User Management. Cons: • No possibility of sharing. • No security management.
XML	Remote Desktop Manager saves the settings directly in a file with the XML format.	Pros: • Easy backup.

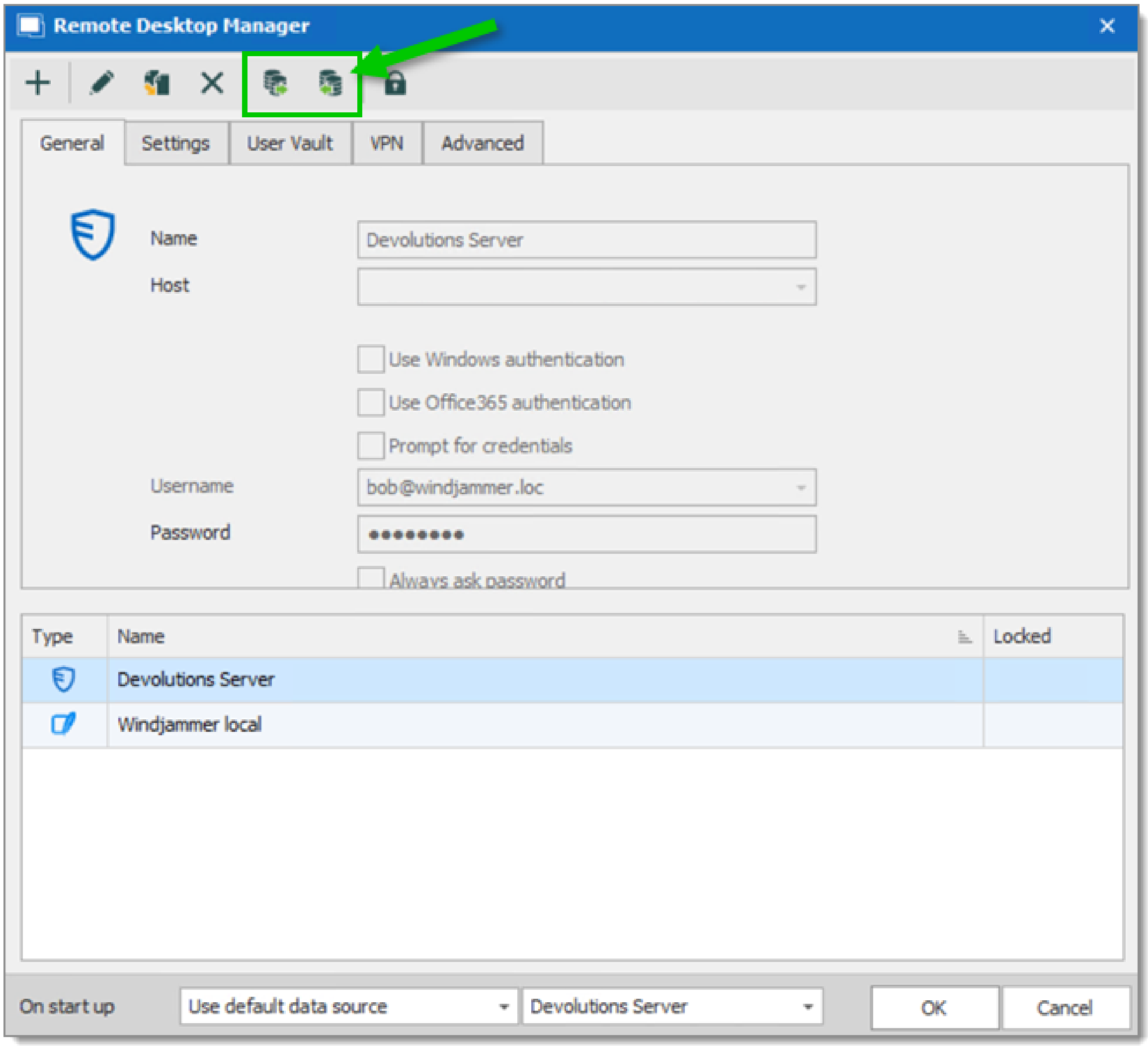
NAME	DESCRIPTION	PROS AND CONS
	For more information, please consult our XML topic.	• Can be edited manually or by an external system. • No installation. Cons: • No possibility of sharing. • No security management. • There is a possibility for conflict or data corruption to occur. • Does not support all features, such as Attachments, Usage Logs, Offline Mode and User Management.

5.4.1 Import and Export Data Source

DESCRIPTION

To simplify deployment for multiple users, it is possible to export and import data source configurations. The generated .rdd file contains all the information to recreate the configuration. Please note that the .rdd file does not include the database content. Only the configuration is exported. Use the entries's Export functionality to backup or copy the database's content.

Use ***File – Data Sources*** to access the import or export functionality.



Data Sources - Import and Export

Whether or not users can **Read/Write** in Offline mode is first decided at the data source's Caching mode level. **This cannot be changed remotely.** If you wish to prevent or allow remote users the Read/Write offline feature, you should do so before exporting your data source.

A locked data source can be exported and imported, but the content will be locked unless a password is entered when the data source is selected. See Lock Data Source for more information.

5.4.2 Advanced Data Sources

DESCRIPTION

Advanced Data Sources are highly configurable data sources, typically running on an advanced management system, such as a database management system or our own online services.

They greatly increase the set of managing features available to administrators, such as:

- Document uploads and entry attachments.
- Auditing and logging.
- Advanced security with User management.
- Offline mode.
- 2-Factor Authentication.

Currently, the ***Advanced Data Sources*** are:

- Devolutions Password Hub Business.
- Devolutions Server.
- Microsoft Azure SQL.
- Microsoft SQL Server (MSSQL).

5.4.2.1 Devolutions Server

DESCRIPTION

Devolutions Server (DVLS) allows to control access to privileged accounts and manage sessions through a secure solution. For more information, consult the product's web site here.

HIGHLIGHTS

- Highly secured server for your company.
- Shared connection and credentials with multiple users.
- Installed on-premises; can be deployed online.
- Support Windows authentication and Active Directory group integration.
- Optimized client and server side caching.

Devolutions Server supports **Microsoft SQL Server** and **Microsoft Azure SQL** as a data store.

For more information, please consult these topics:

- Devolutions Server installation instructions
- Devolutions Server Security Checklist

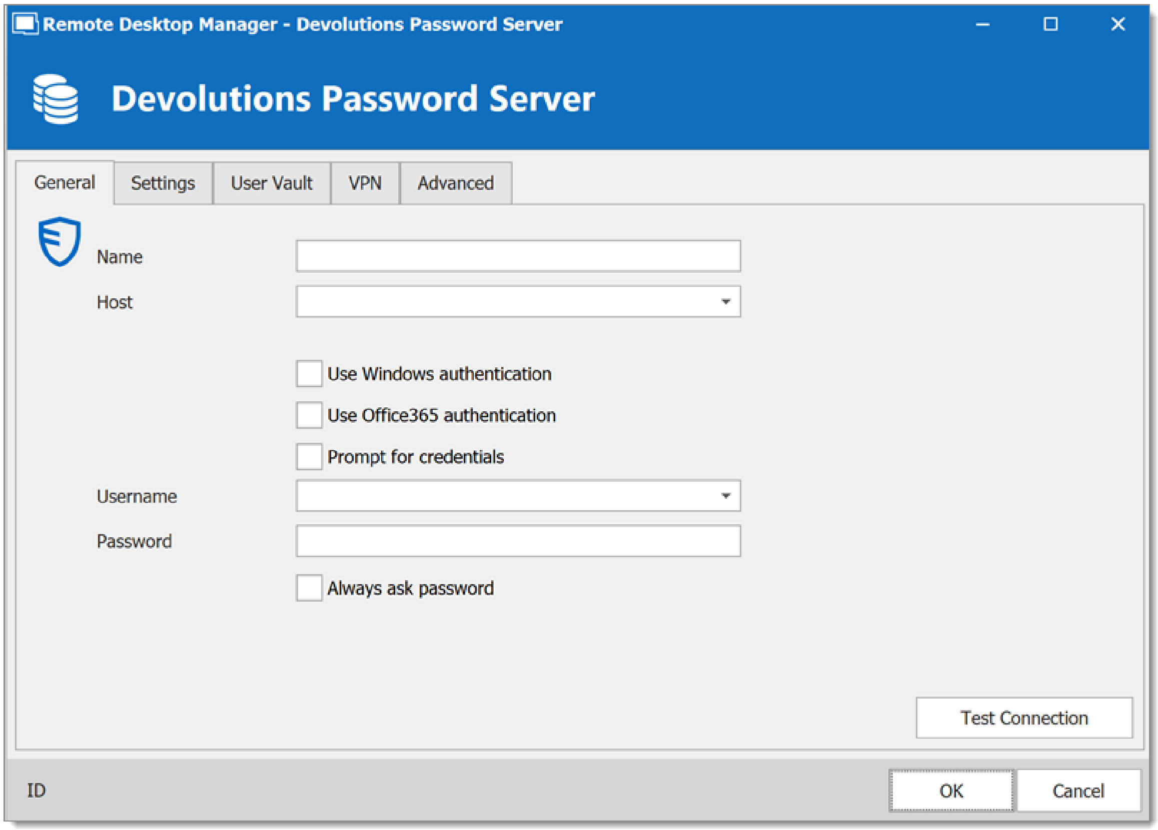
CONFIGURE THE SERVER DATA SOURCE ON ALL YOUR CLIENT MACHINES

Enter a name of the data source and the URL for the Host. Ensure you use the correct protocol if SSL is required by the server (https).

Export the data source, then import the file in your client workstations as described Import/Export Data Source.

SETTINGS

GENERAL

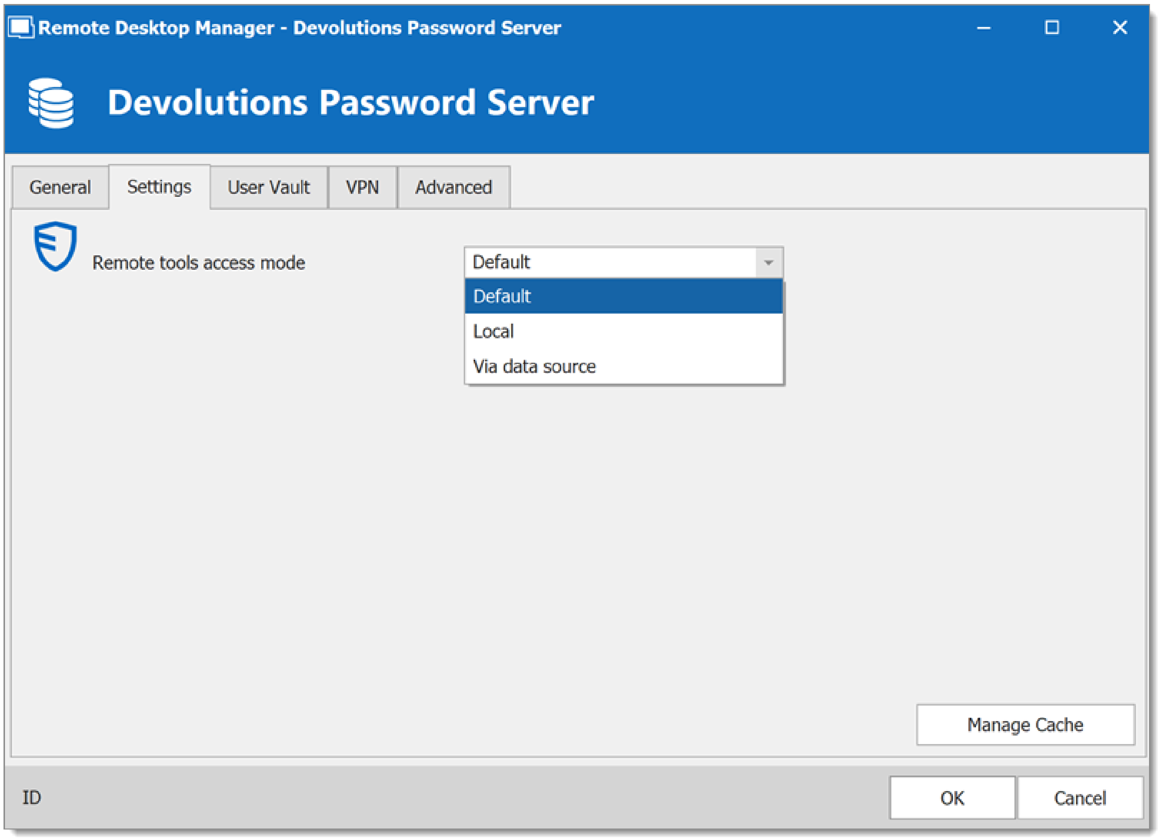


Devolutions Server - General

OPTION	DESCRIPTION
Name	Enter a name for the data source.
Host	Enter the URL of the DVLS instance. Example: http://<hostname or IP address>/<instance name>
Use Windows authentication	Use the same credentials are your current Windows user.
Use Office365 authentication	Use the same credentials as your current Office365 user. Choose an authentication option: • **Default**: Create a new authentication token each time and keeps it in the memory only.

OPTION	DESCRIPTION
	• **Persistent**: Takes the saved token, if it does not exist, will create a new one and save it. • **Linked account**: Takes a saved token from Windows (registry).
Always prompt for credentials	Always ask for the username and password when connecting to the data source.
Username	Enter the username to connect to the data source.
Password	Enter the password to connect to the data source.
Always ask password	Always ask for the password when connecting to the data source.
Test Connection	Test the connection with Devolutions Server to validate the credentials.

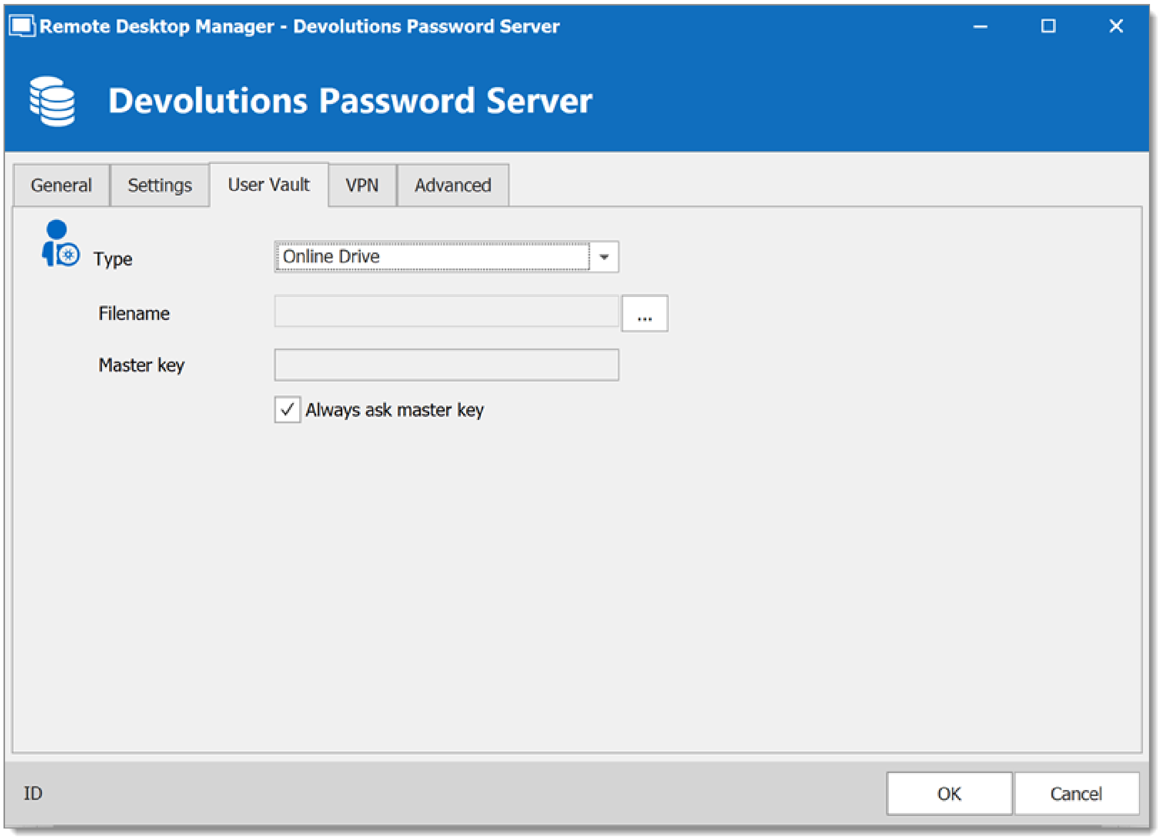
SETTINGS



Devolutions Server - Settings

OPTION	DESCRIPTION
Remote tools access mode	Select whether the Remote Tools will be accessed locally or through the host.
Manage Cache	Manage the data source cache. On large data sources caching is a must and will increase performance significantly. For more information, please consult the [Manage Cache](#) topic.

USER VAULT

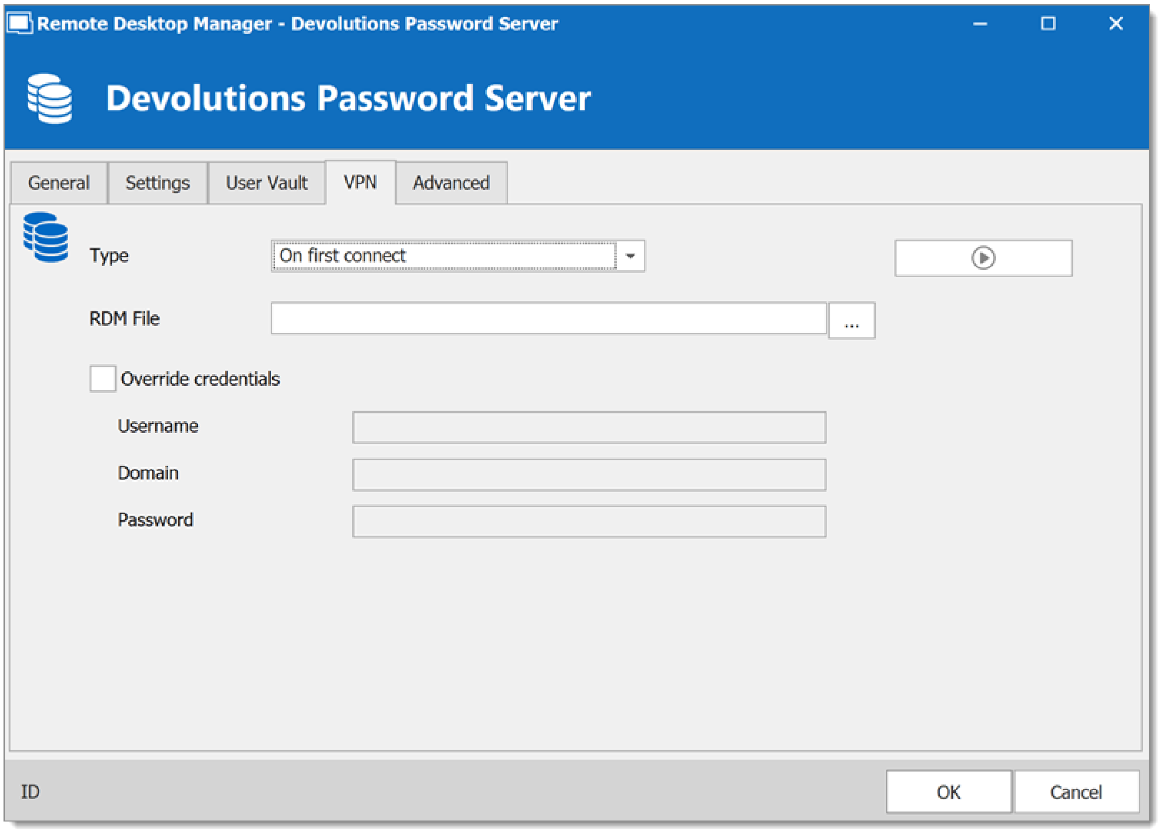


Devolutions Server – User Vault

OPTION	DESCRIPTION
Type	Select the type of User Vault to use. Select between: • **Default**: use the default User Vault, which is stored in the database. • **None**: disable the User Vault for all users. • **Online Drive**: use a Devolutions Online Drive file (*.dod) as a User Vault.

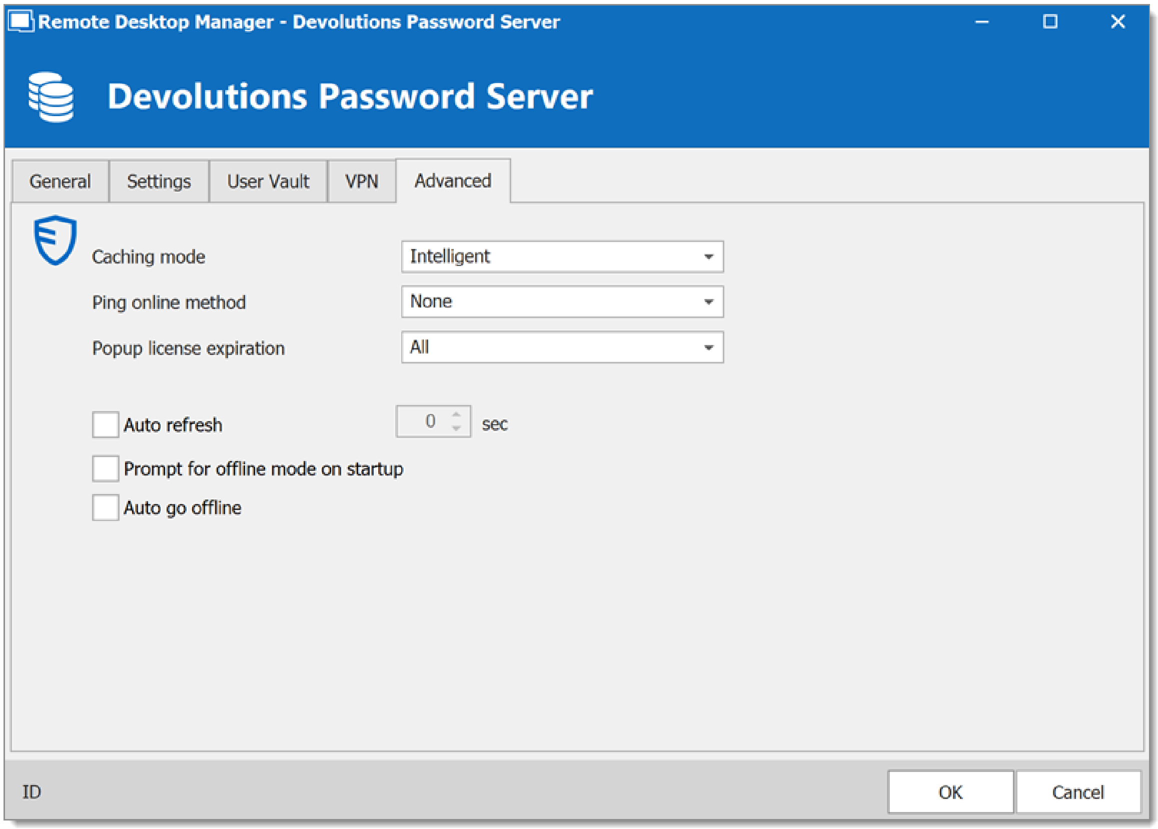
VPN

Open a VPN to access your data prior to connecting to your **Devolutions Server**.



Devolutions Server - VPN

ADVANCED



Devolutions Server - Avanced

OPTION	DESCRIPTION
Caching mode	Determines how the entries will be reloaded in the data source. For more information, please consult the Caching topic.
Ping online method	Indicate the preferred ping online method. Select between: • **None** • **Web request**
Popup license expiration	Determine how the application advises of the license expiration. Select between: • **All** • **Only Administrator(s)** • **Disabled**

OPTION	DESCRIPTION
Auto refresh	Set the interval for the automatic refresh.
Prompt for offline mode on startup	Ask to use the data source in offline mode when the user connects to the data source.
Auto go offline	Use the data source in offline mode when the ping method does not respond.
Disable lock	Disable the option to lock the data source directly. The application still can be locked but the user is not prompted for the data source password when unlocking the application.

5.4.2.2 Microsoft SQL Server

DESCRIPTION

With the Microsoft SQL Server data source, Remote Desktop Manager uses the power of Microsoft SQL Server to save and manage entries.

Supported Microsoft SQL Server:

- 2019 on Windows and Linux (all editions)
- 2017 on Windows and Linux (all editions)
- 2016 Service Pack 2
- 2014 Service Pack 3
- 2012 Service Pack 4

The following features are also supported:

- **Always on availability group**.
- **Clustering**.
- **Log Shipping**.
- **Database mirroring**.

HIGHLIGHTS

- Supports user management with a superior security model.
- Supports Offline mode for when the server or network is unavailable.
- Supports full entry logs and attachments.
- Supports Vaults to organize thousands of entries.

A proper database backup strategy should be implemented to prevent possible data loss. Please refer to the Backups topic.

Depending on the Recovery Model of the underlying database, some maintenance operations may have to be scheduled to run regularly in order to maintain the health of the database. Please consult Recovery Model.

Using either **Database Login** or **Integrated Security** is inherently less secure because it means that the end user can connect directly to the database using any tool available. We do have table and column level security, but security conscious organizations will consider this unacceptable. It is recommended to use our **Custom login** model.

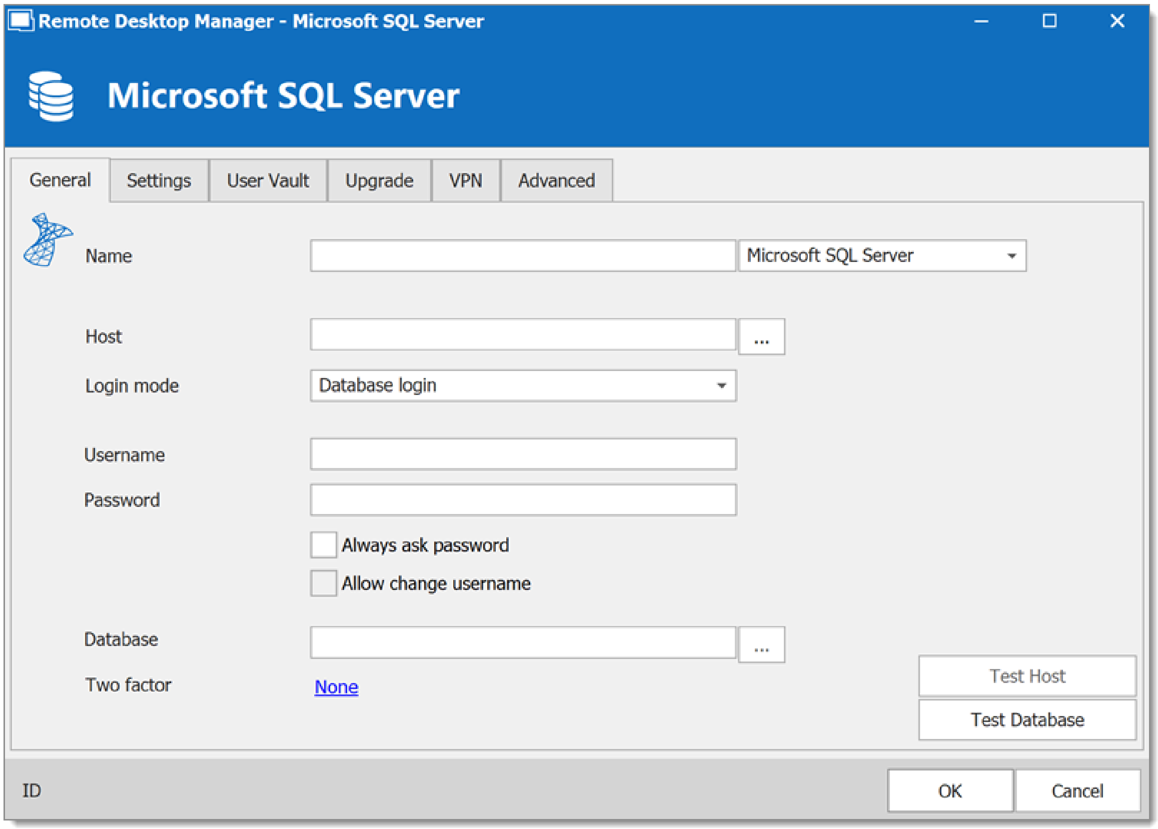
Creating Contained Database Users as mentioned in this article is the supported method with SQL Always On availability group.

CONFIGURATION

Consult the Configure SQL Server topic for more information on the configuration.

SETTINGS

GENERAL

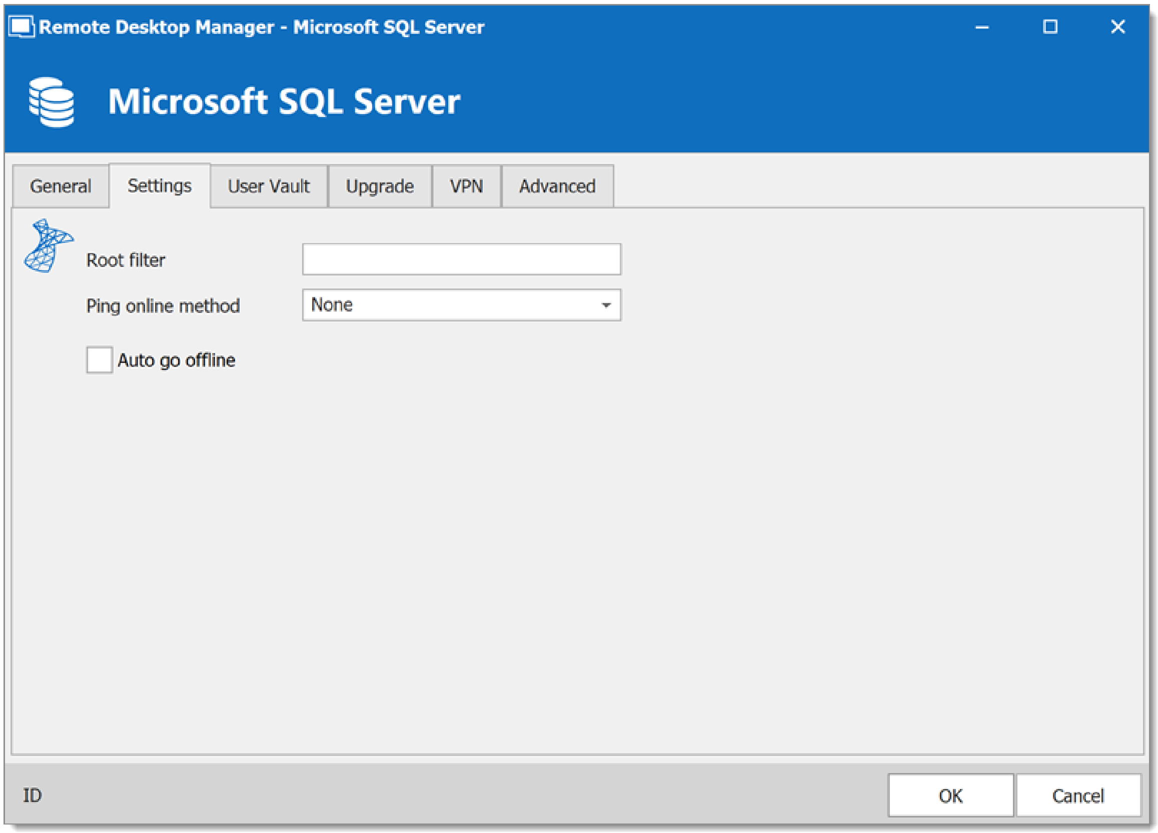


Microsoft SQL Server - General Tab

OPTION	DESCRIPTION
Name	Enter a name for the data source.
Host	Enter the server hostname or IP address.
Login mode	Specify the authentication mode to use. Select between: • **Database login** • **Integrated Security (Active directory)** • **Custom Login**
Username	Enter the username to access the Azure SQL database.
Password	Enter the password to access the Azure SQL database.

OPTION	DESCRIPTION
Always ask password	Prompt for the password when a user connects to the data source.
Allow change username	Allow the username to be edited when connecting to the data source. (Only with Always ask password enabled)
Database	Enter the name of the Azure SQL database.
Two factor	Enable the 2-Factor Authentication.
Test Server	Test the connection with the server to validate if the proper information has been provided.
Test Database	Test the connection with the database to validate if the proper information has been provided.

SETTINGS

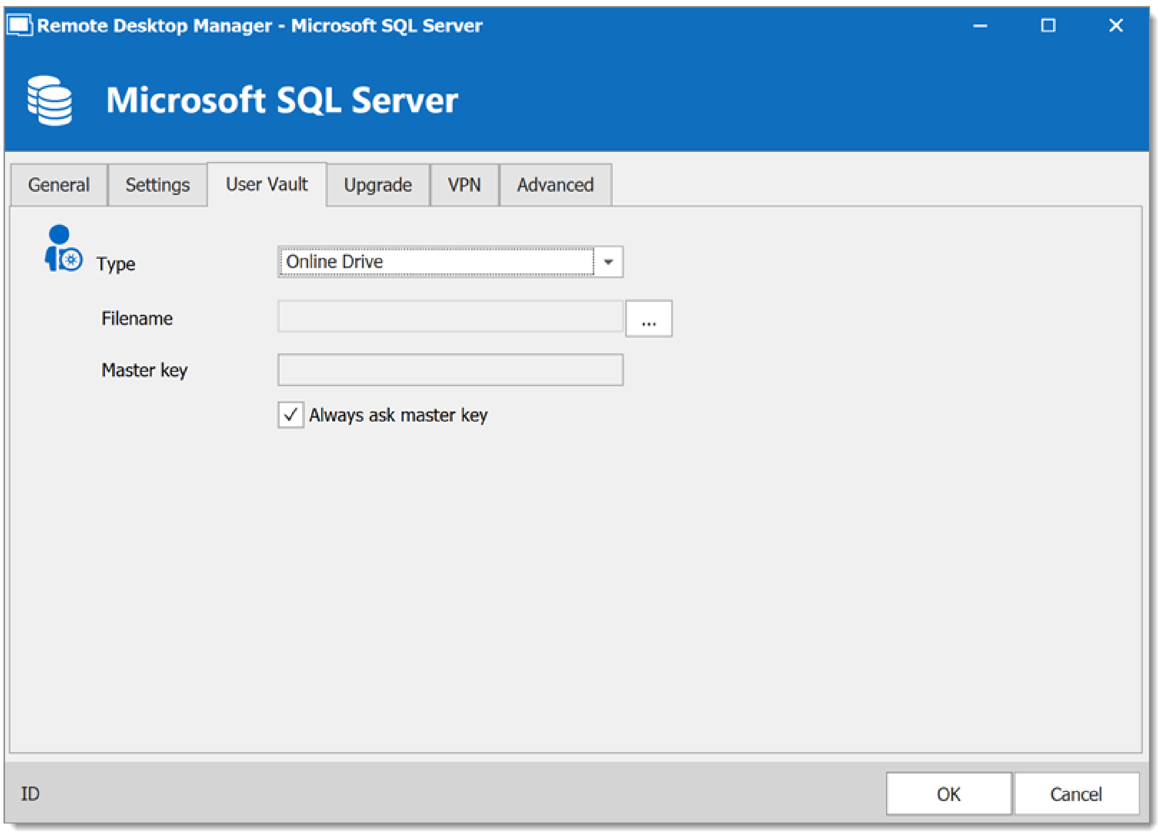


Microsoft SQL Server - Settings Tab

OPTION	DESCRIPTION
Root filter	Enter the name of a root level folder to display only the entries contained in that folder.
Ping online method	Indicate the preferred ping online method. Select between: • **None** • **Ping** • **Port Scan**
Auto go offline	Use the data source in offline mode when the ping method does not respond.

OPTION	DESCRIPTION
Disable lock	Disable the option to lock the data source directly. You can still lock the application but you won't be prompted for the data source password if this option is disabled.

USER VAULT

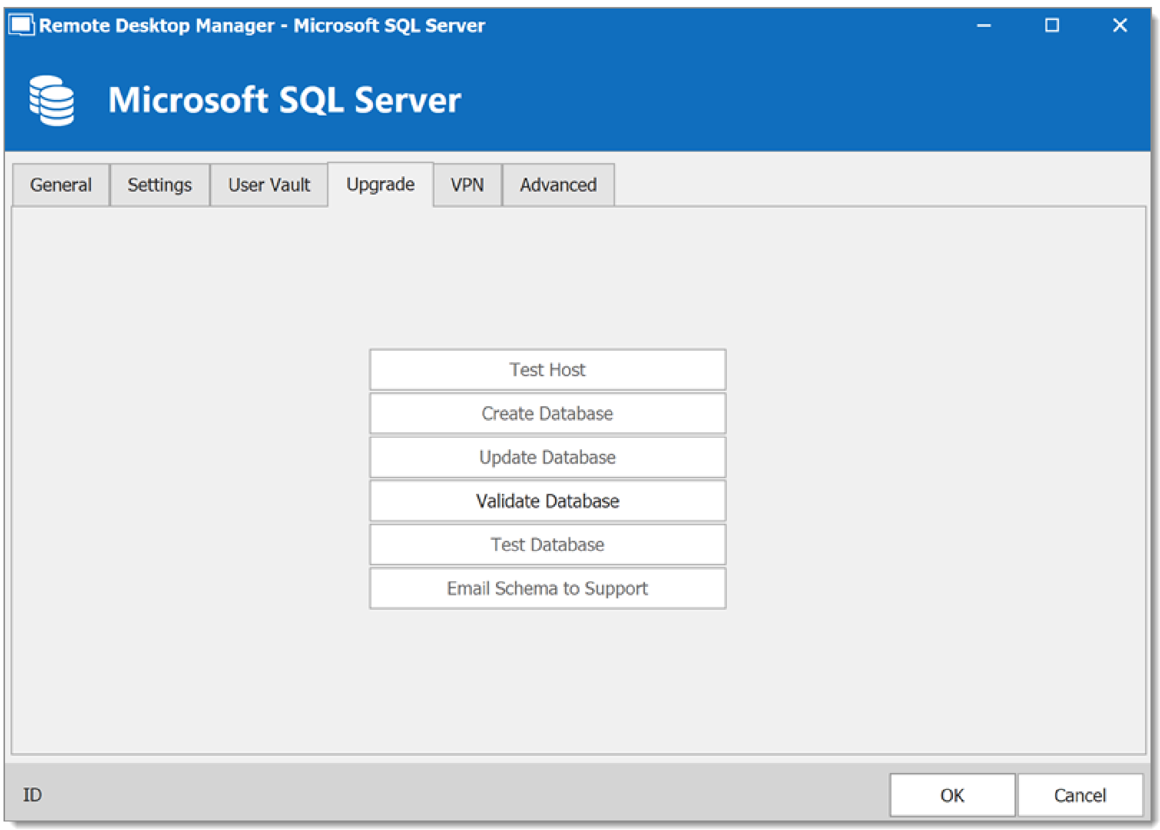


Microsoft SQL Server - User Vault Tab

OPTION	DESCRIPTION
Type	Select the type of User Vault to use. Select between: • **Default**: use the default User Vault, which is stored in the database.

OPTION	DESCRIPTION
	• **None**: disable the User Vault for all users. • **Online Drive**: use a Devolutions Online Drive file (*.dod) as a User Vault.

UPGRADE



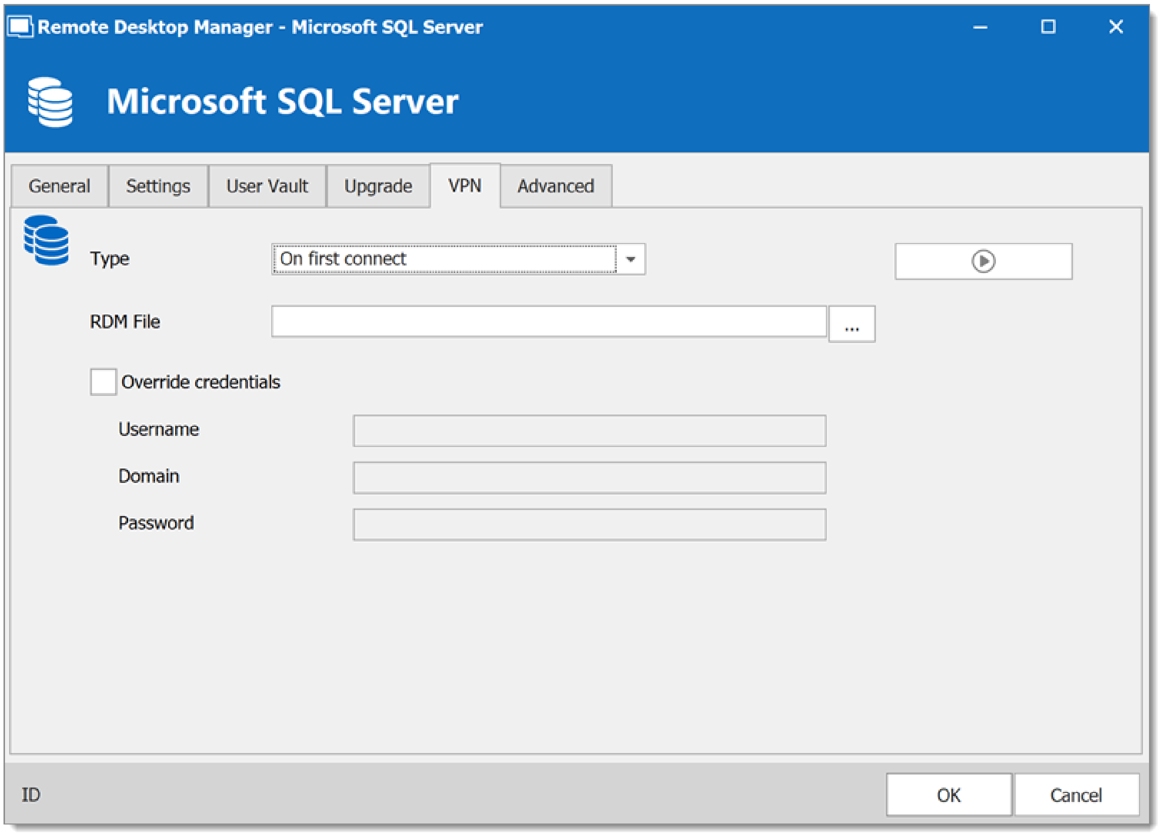
Microsoft SQL Server - Upgrade Tab

OPTION	DESCRIPTION
Test Server	Test the connection with the server to validate if the proper information has been provided.

OPTION	DESCRIPTION
Create Database	Create the database on the SQL server.
Update Database	Update the database on the SQL server.
Test Database	Test the connection with the database to validate if the proper information has been provided.
Email Schema to Support	Send your schema to the Devolutions support team.

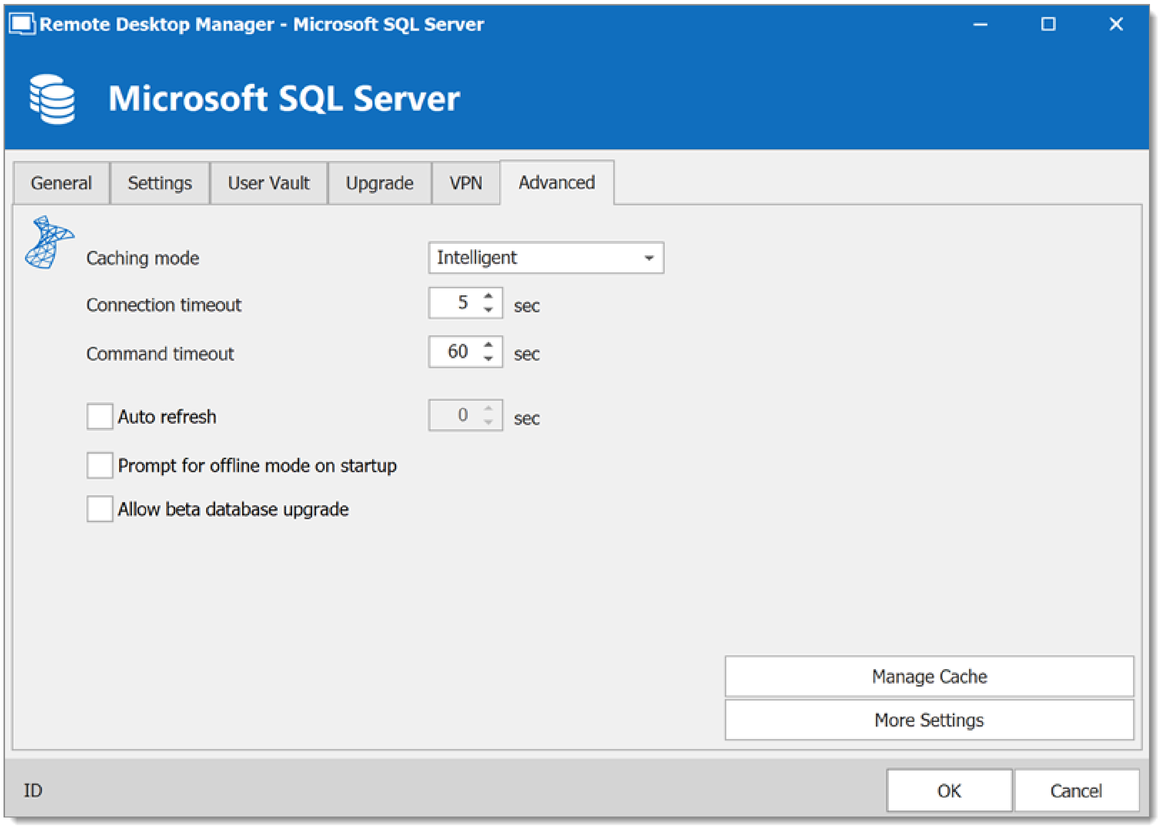
VPN

Open a VPN to access your data prior to connecting to your **Microsoft SQL Server**.



Microsoft SQL Server - VPN Tab

ADVANCED



Microsoft SQL Server - Advanced Tab

OPTION	DESCRIPTION
Caching mode	Determines how the entries will be reloaded in the data source. For more information, please consult the Caching topic.
Connection timeout	Set the delay of the connection timeout.
Command timeout	Set the delay of the command timeout.
Auto refresh	Set the interval for the automatic refresh.
Prompt for offline mode on startup	Ask to use the data source in offline mode when the user connects to the data source.

OPTION	DESCRIPTION
Allow beta database upgrade	Allow beta upgrade of the database (when using a beta version of Remote Desktop Manager).
Manage Cache	Manage the data source cache. On large data sources caching is a must and will increase performance significantly. For more information, please consult the Manage Cache topic.
More Settings	Edit the connection string values directly.

5.4.2.2.1 Configure SQL Server

DESCRIPTION

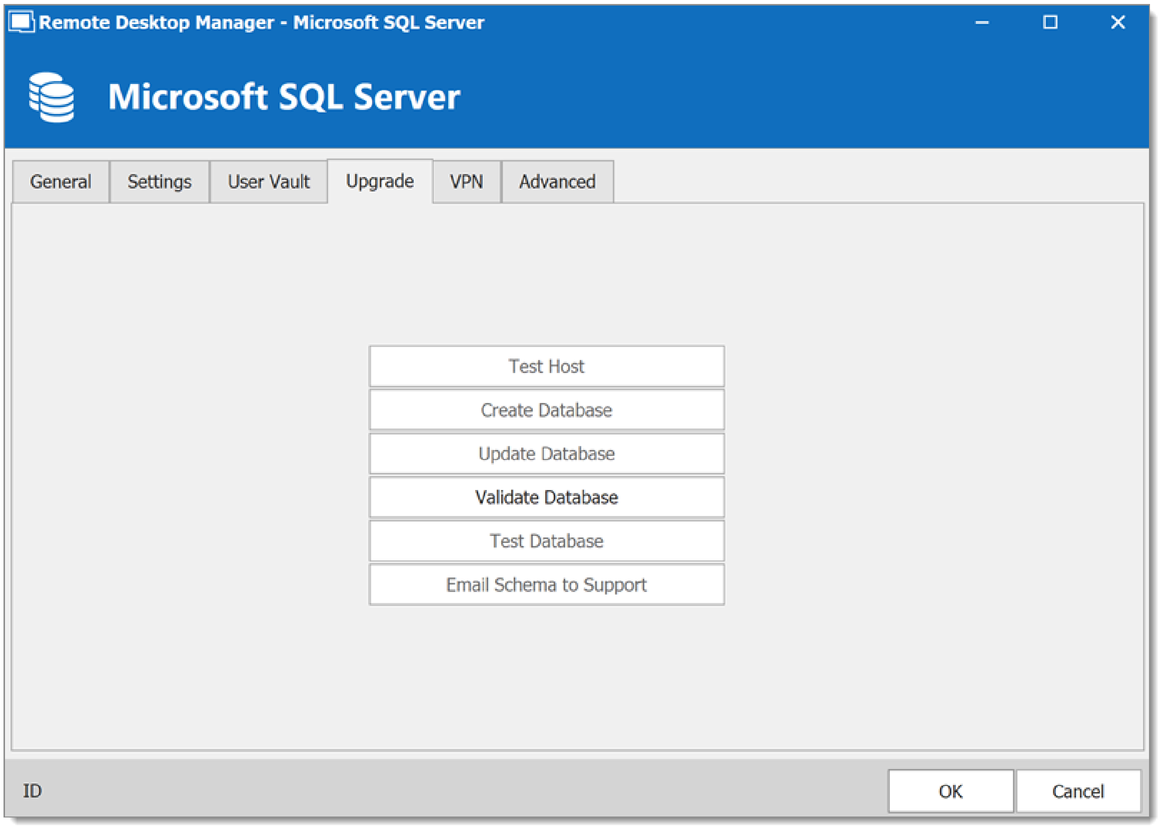
1. Install **Microsoft SQL Server** or **Microsoft SQL Server Express**.

> Newly installed Microsoft SQL Server instances do not allow remote connections. Please follow the directions in SQL Server.

> For added security, you can enable SSL Encryption to communicate with your instance of SQL Server. However, due to a framework limitation, this is not compatible with our iOS and Android versions of Remote Desktop Manager.
>
> Please follow directions on https://support.microsoft.com/en-us/kb/316898

2. Follow the steps in the Create a data source topic. On Step 4, before testing server or otherwise verifying the connection, continue with the steps below.

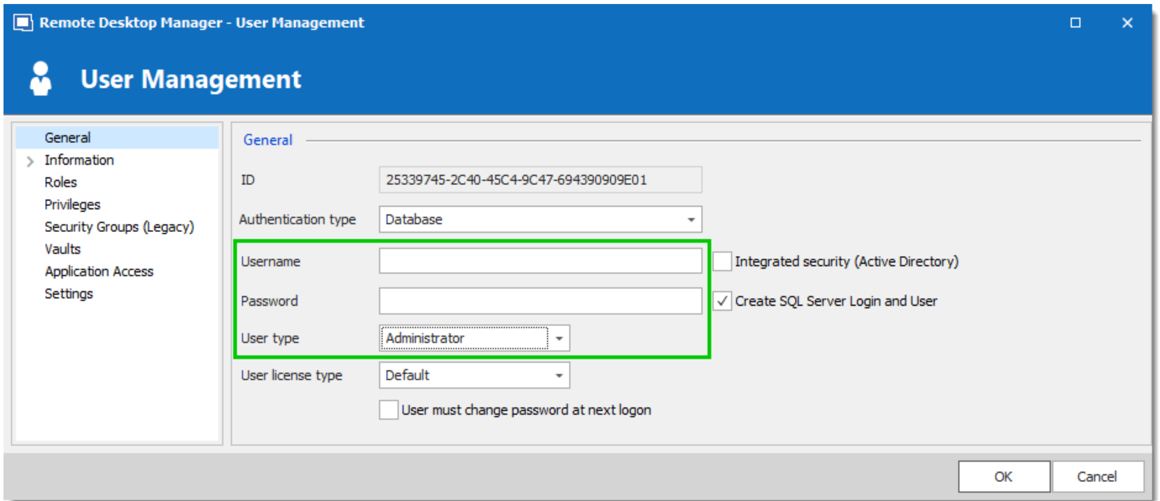
3. Select the **Upgrade** tab and click the **Create Database** button. If the database is already created on the Microsoft SQL Server, click the **Update Database** button to add the appropriate tables to the database.



Upgrade Tab

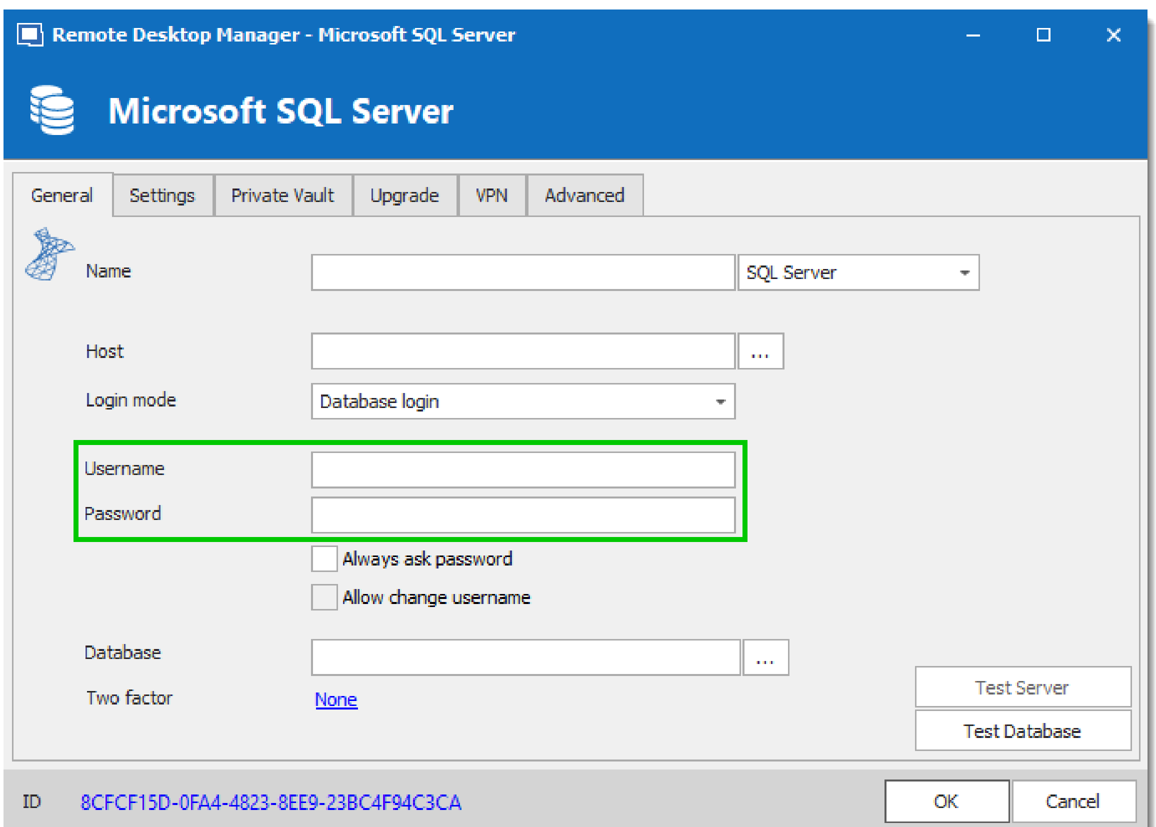
4. Once the database is created, create an administrator account for the database via the Administration - Users menu.

If the database is created using a system administrator (example: SA), we recommend to keep this user only for the database creation and the database upgrade. A Remote Desktop Manager administrator account must be created first. Then, regular users are created with this administrator account.



Create a Remote Desktop Manager Administrator Account

5. Connect to the Microsoft SQL Server database with the Remote Desktop Manager administrator account. To do so, edit the data source used to create the database and change the login information for the administrator account created with Remote Desktop Manager.



Connection to the Database with the RDM Administrator Account

The Microsoft SQL Server data source is now correctly configured.

5.4.2.2.2 Recovery Model

DESCRIPTION

Microsoft SQL Server backup and restore operations occur within the context of the recovery model of the database. Recovery models are designed to control transaction log maintenance. A recovery model is a database property that controls how transactions are logged, whether the transaction log requires (and allows) backing up, and what kinds of restore operations are available. Three recovery models exist: **simple**, **full**, and **bulk-logged**. Typically, a database uses the full recovery model or simple recovery model. A database can be switched to another recovery model at any time.

If the Recovery Model is set to Full, it is critical that regular backups of BOTH the database and the transaction log are performed. Not performing these backups will result in the database files to increase in size at an alarming rate. This will severely impact the performance in the long run.

For further information regarding SQL Recovery Models, refer to https://msdn.microsoft.com/en-CA/library/ms189275.aspx.

5.4.2.2.3 Encrypting Connections to SQL Server

DESCRIPTION

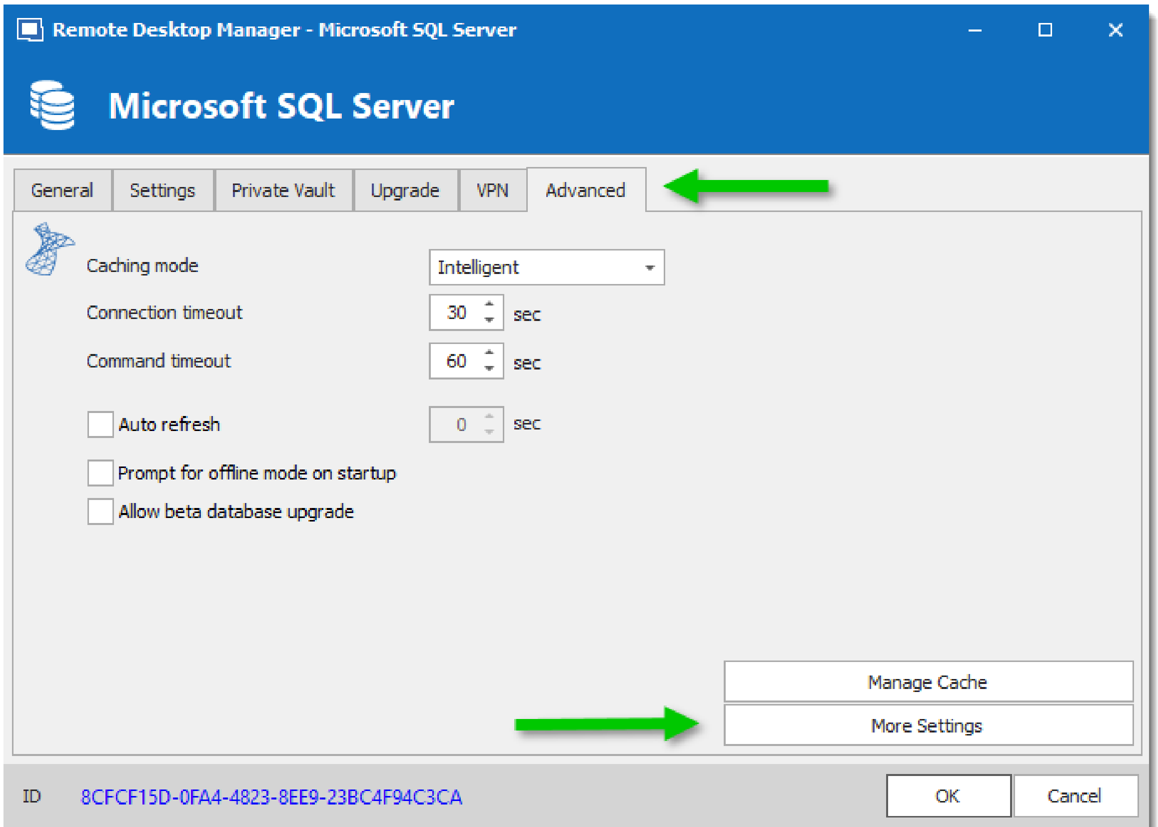
To ensure that the communication between Remote Desktop Manager and the Microsoft SQL Server database is encrypted, an extensive procedure must be followed on the Microsoft SQL Server instance.

Please consult this Microsoft technet article that provides detailed instructions: Encrypting Connections to SQL Server (technet).

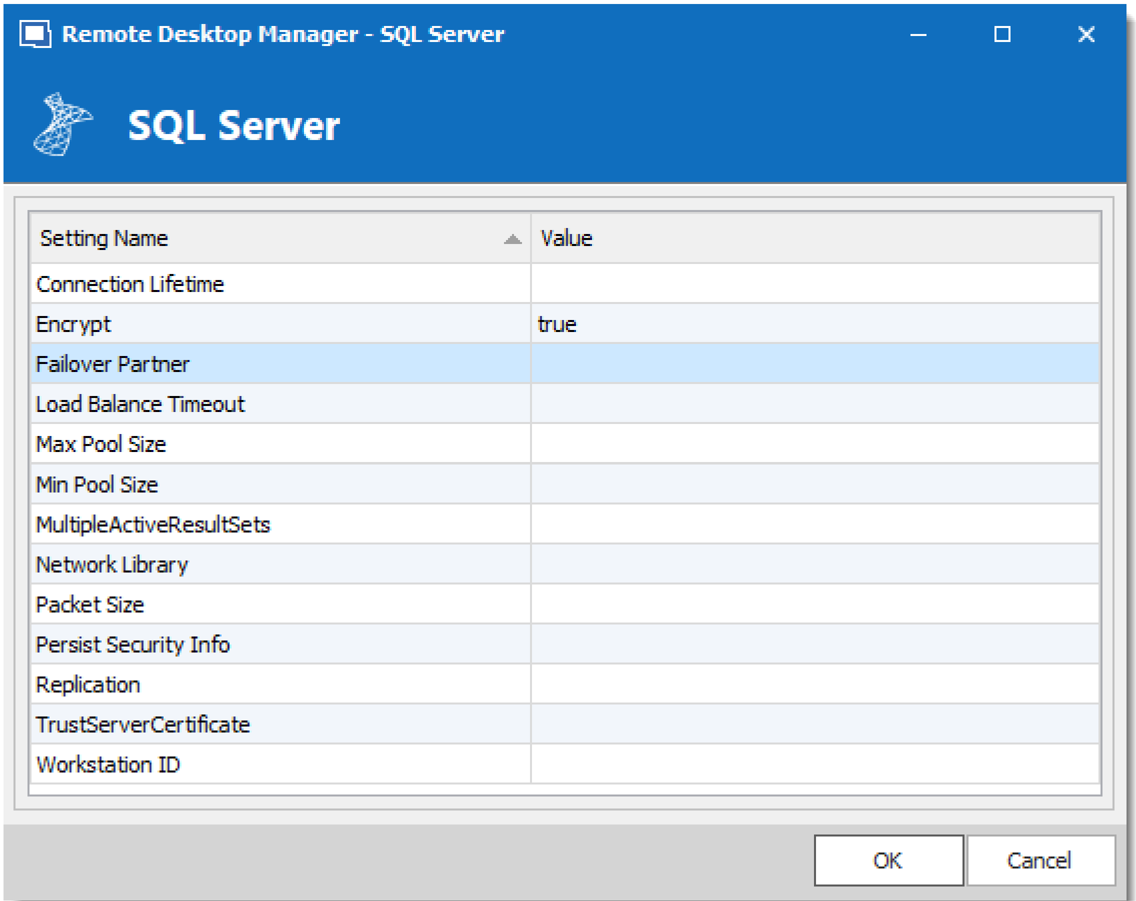
After it has been properly configured, the only modification to perform in Remote Desktop Manager is to set a property in the **More Settings** of the data source.

PROCEDURE

1. Create or edit an Microsoft SQL Server data source, access the **Advanced** tab and click the **More Settings** button.



2. Set the **Encrypt** property value to **true**. Click **OK** to validate.



5.4.2.3 Microsoft Azure SQL

DESCRIPTION

With the Microsoft Azure SQL data source, Remote Desktop Manager uses the Microsoft cloud platform to save and manage entries.

The following features are also supported:

- **Always on availability group**
- **Clustering**
- **Log shipping**
- **Database mirroring**

MINIMUM REQUIREMENT FOR AZURE SQL DATABASE FOR RDM

Microsoft Azure SQL offers different service tier in their purchase model for DTUS.

We recommend at minimum a Standard tier package S0 for 5 users and more.

Visit their website for more information.

HIGHLIGHTS

- Supports User Management with a superior security model.
- Supports Offline mode for when the server or network is unavailable.
- Supports entry logs and attachments.
- Get more information on Microsoft Azure SQL.

For Azure AD authentication, download and install the "Microsoft Active Directory Authentication Library for Microsoft SQL Server".

Please download it here : https://www.microsoft.com/en-us/download/details.aspx?id=48742.

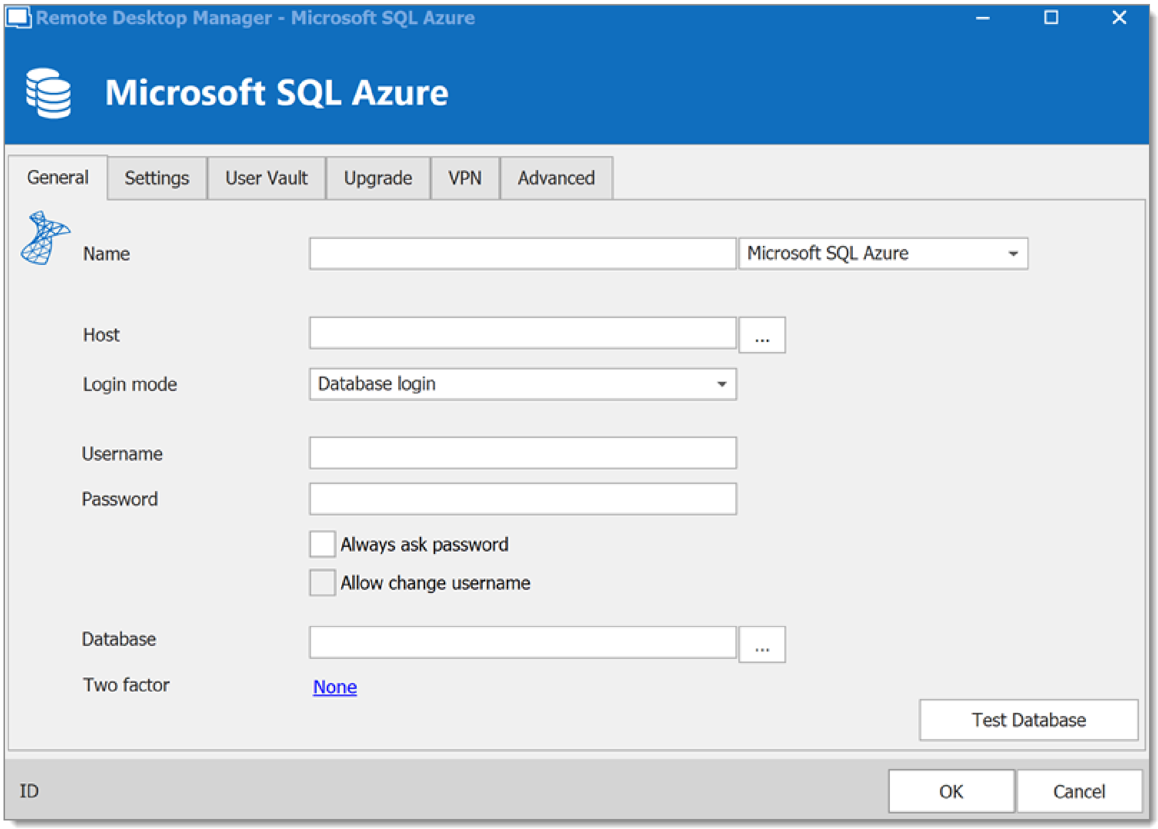
A proper database backup strategy should be implemented to prevent possible data loss. Please refer to the Backups topic.

CONFIGURATION

Consult the Configure Azure SQL topic for more information on the configuration.

SETTINGS

GENERAL

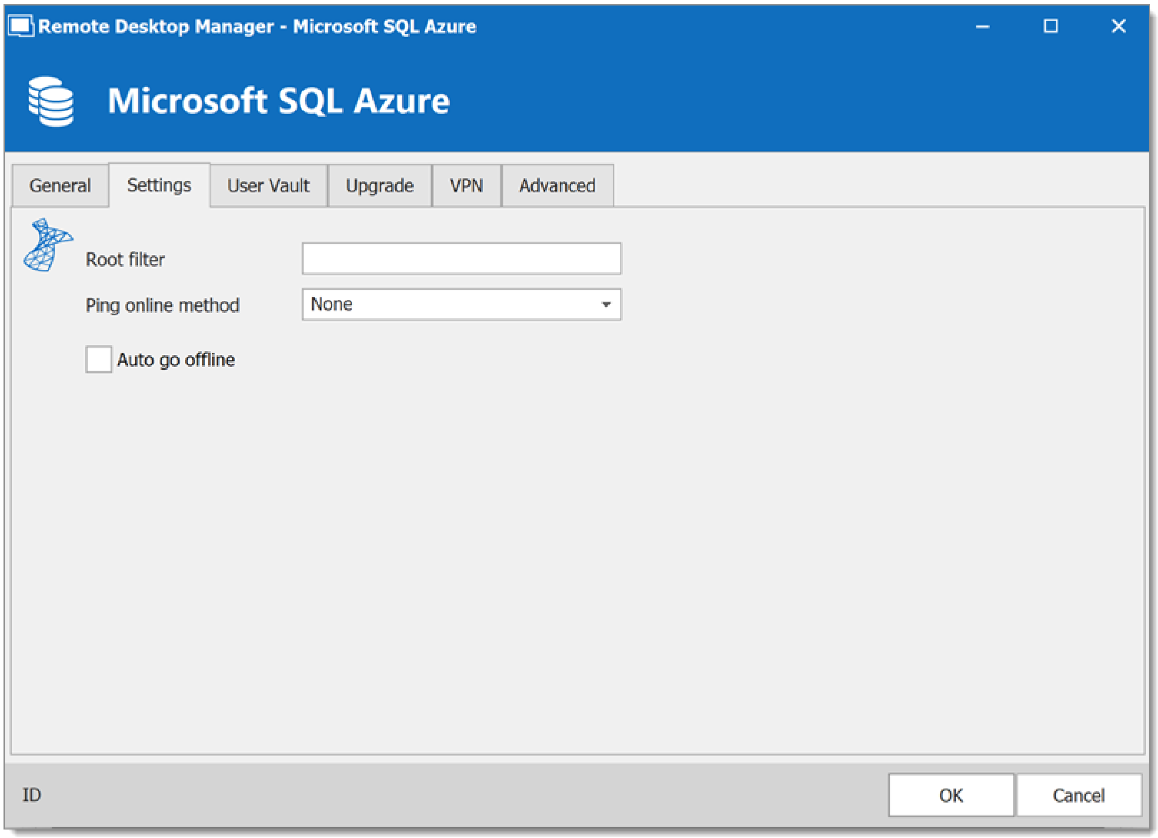


Microsoft Azure SQL - General

OPTION	DESCRIPTION
Name	Enter a name for the data source.
Host	Enter the server hostname or IP address.
Login mode	Specify the authentication mode to use. Select between: • **Database login** • **Custom login** • **Active Directory Password** • **Active Directory Integrated**

OPTION	DESCRIPTION
	• **Active Directory Interactive (with MFA support)**
Username	Enter the username to access the Azure SQL database.
Password	Enter the password to access the Azure SQL database.
Always ask password	Prompt for the password when a user connects to the data source.
Allow change username	Allow the username to be edited when connecting to the data source. (Only with Always ask password enabled)
Database	Enter the name of the Azure SQL database.
Two factor	Enable the 2-Factor Authentication.
Test Database	Test the connection with the database to validate if the proper information has been provided.

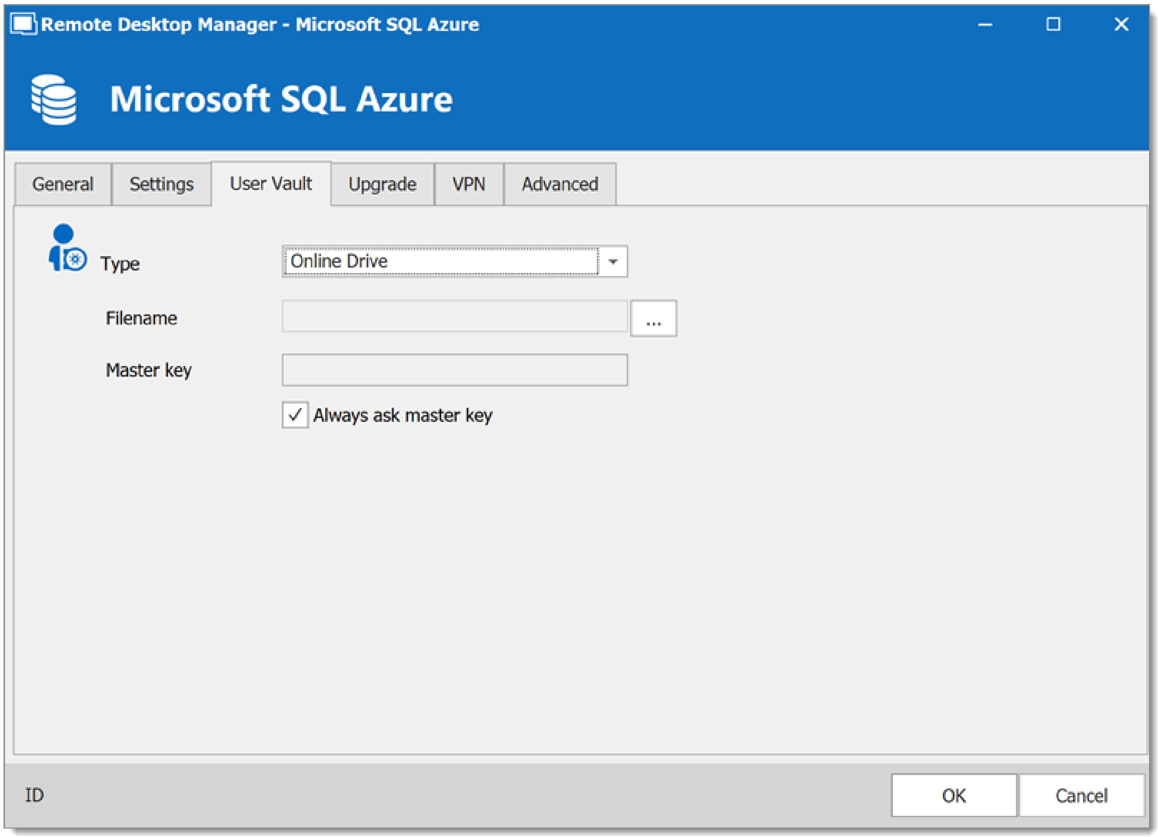
SETTINGS



Microsoft Azure SQL - Settings Tab

OPTION	DESCRIPTION
Root filter	Enter the name of a root level folder to display only the entries contained in that folder.
Ping online method	Indicate the preferred ping online method. Select between: • **None** • **Ping** • **Port Scan**
Auto go offline	Use the data source in offline mode when the ping method does not respond.
Disable lock	Disable the option to lock the data source directly. You can still lock the application but you won't be prompted for the data source password if this option is disabled.

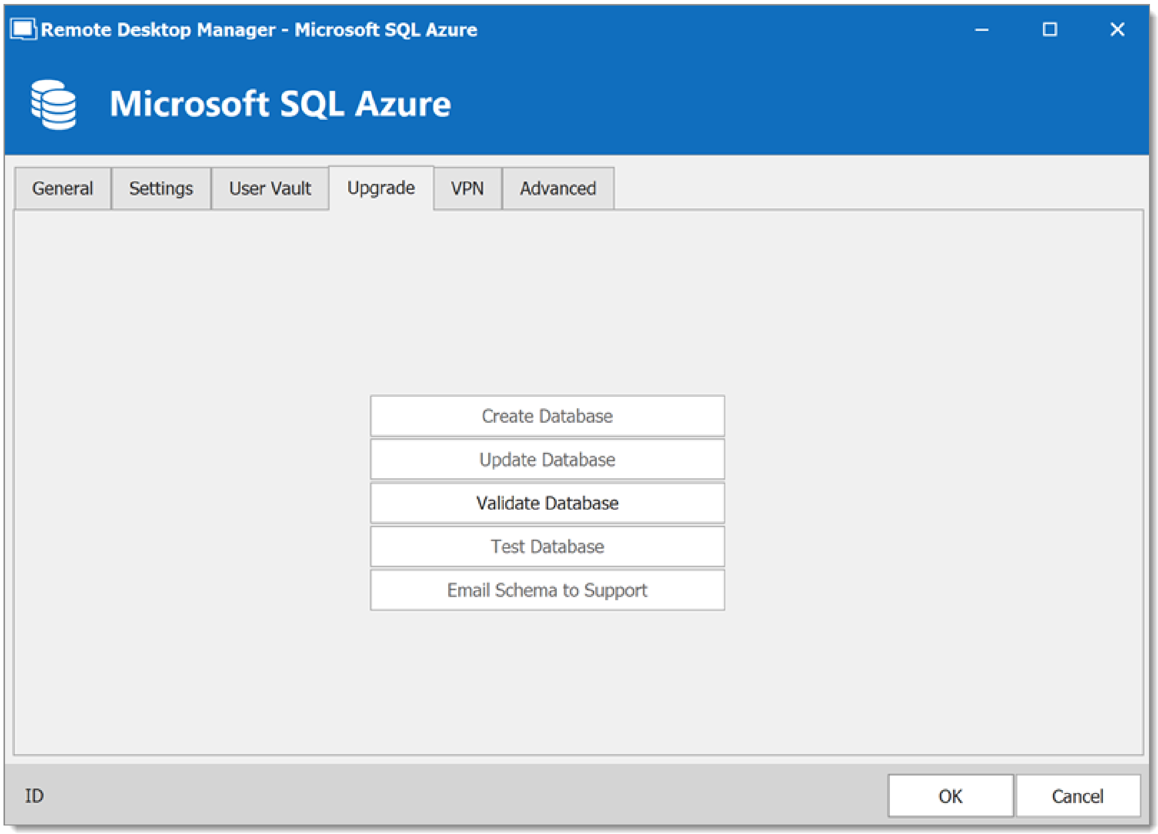
USER VAULT



Microsoft Azure SQL - User Vault Tab

OPTION	DESCRIPTION
Type	Select the type of User Vault to use. Select between: • **Default**: use the default User Vault, which is stored in the database. • **None**: disable the User Vault for all users. • **Online Drive**: use a Devolutions Online Drive file (*.dod) as a User Vault.

UPGRADE

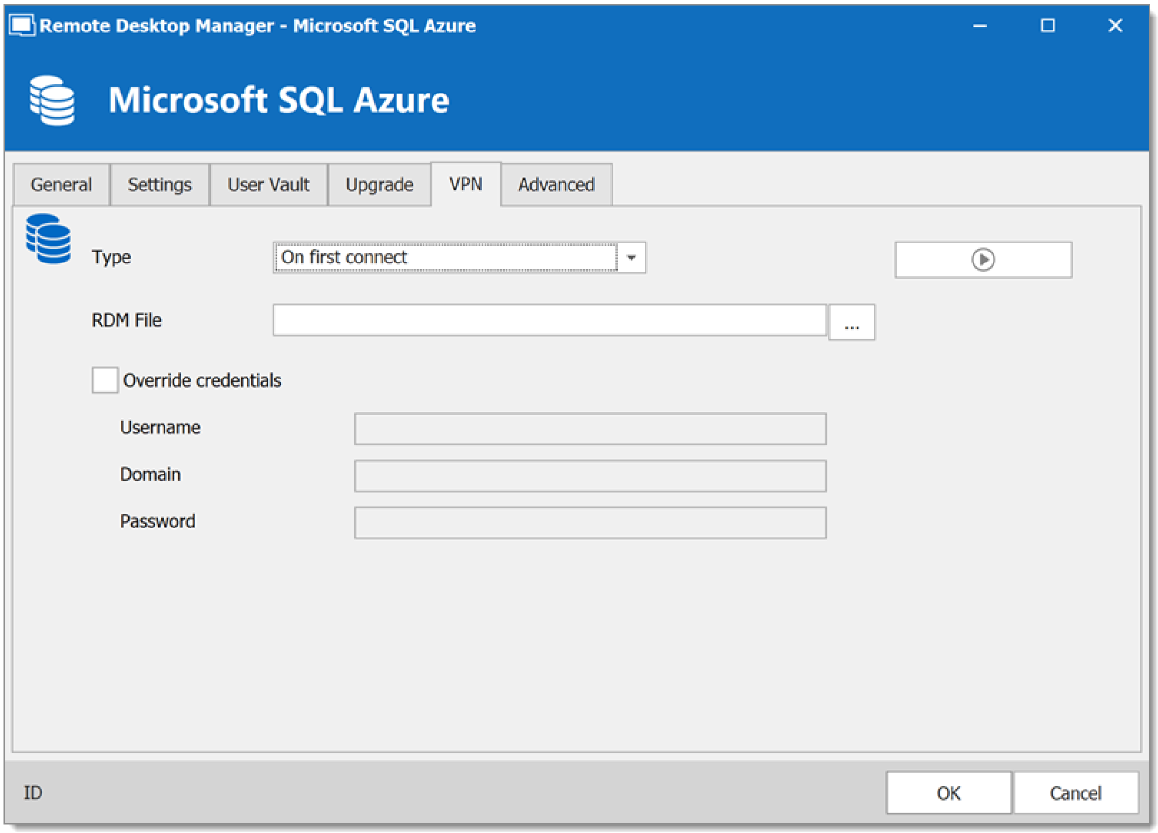


Microsoft Azure SQL - Upgrade Tab

OPTION	DESCRIPTION
Create Database	Create the database on the SQL server to use Remote Desktop Manager.
Update Database	Update the database on the SQL server, if required to use Remote Desktop Manager.
Test Database	Test the connection with the database to validate if the proper information has been provided.
Email Schema to Support	Send your schema to the Devolutions Support team.

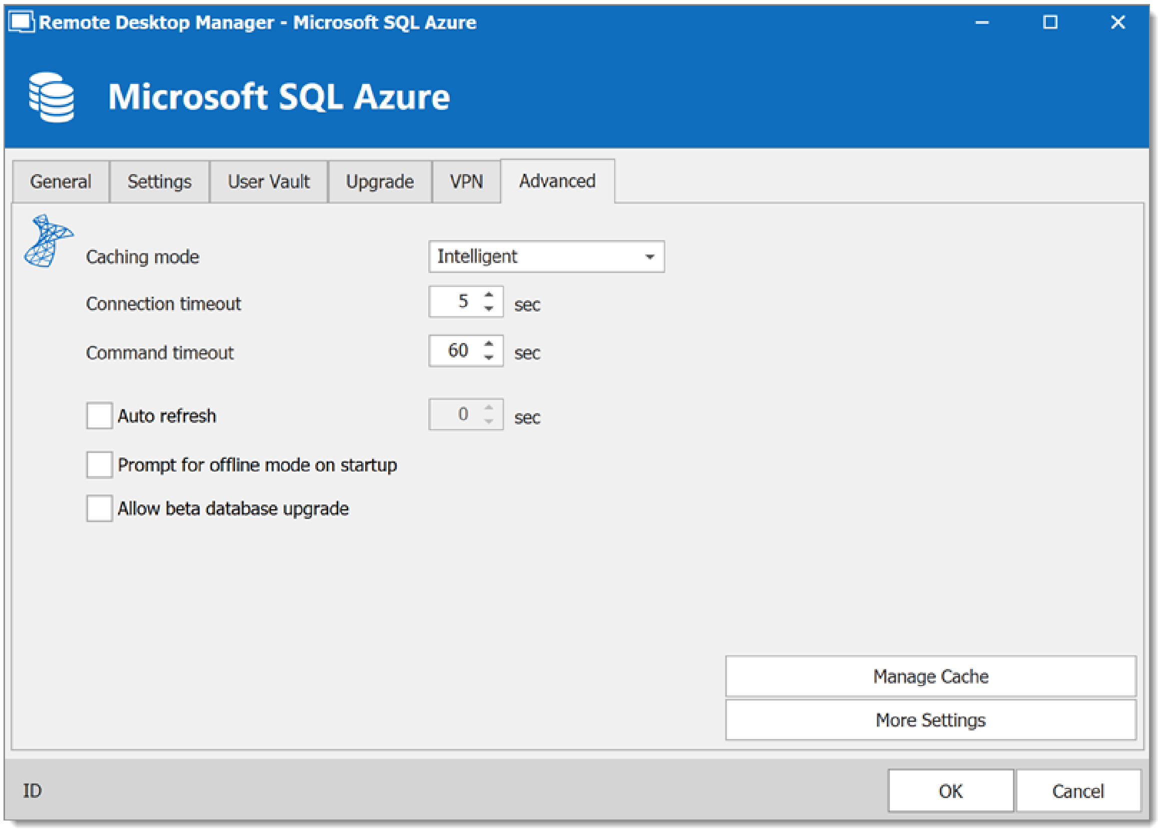
VPN

Open a VPN to access your data prior to connecting to your **Microsoft Azure SQL** database.



Microsoft Azure SQL - VPN

ADVANCED



Microsoft Azure SQL - Advanced Tab

OPTION	DESCRIPTION
Caching mode	Determines how the entries will be reloaded in the data source. For more information, please consult the Caching topic.
Connection timeout	Set the delay of the connection timeout.
Command timeout	Set the delay of the command timeout.
Auto refresh	Set the interval for the automatic refresh.
Prompt for offline mode on startup	Ask to use the data source in offline mode when a user connects to the data source.

OPTION	DESCRIPTION
Allow beta database upgrade	Allow beta upgrade of the database (when using a beta version of Remote Desktop Manager).
Manage Cache	Manage the data source cache. On large data sources caching is a must and will increase performance significantly. For more information, please consult the Manage Cache topic.
More Settings	Edit the connection string values directly.

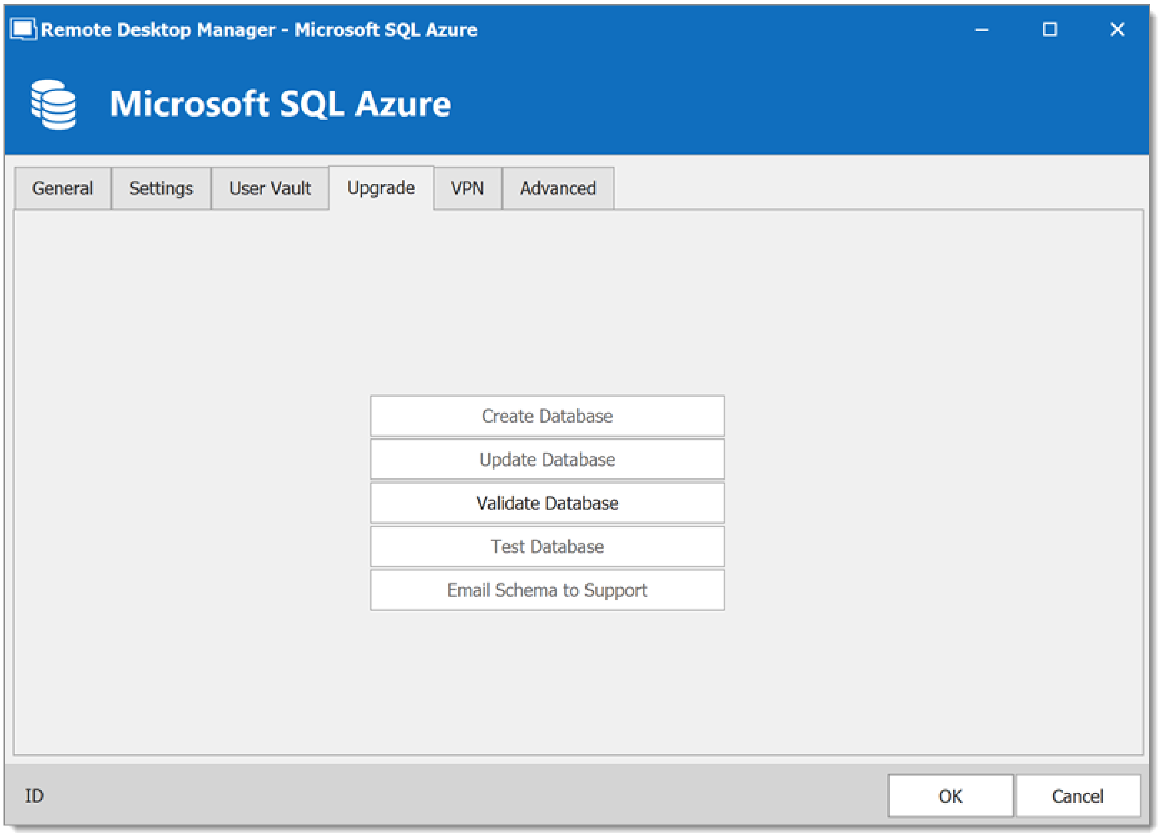
5.4.2.3.1 Configure Azure SQL

DESCRIPTION

1. Make sure that you have a valid **Microsoft Azure SQL** subscription to be able to create your database.

2. Follow the steps in the Create a data source topic. On Step 4, before testing server or otherwise verifying the connection, continue with the steps below.

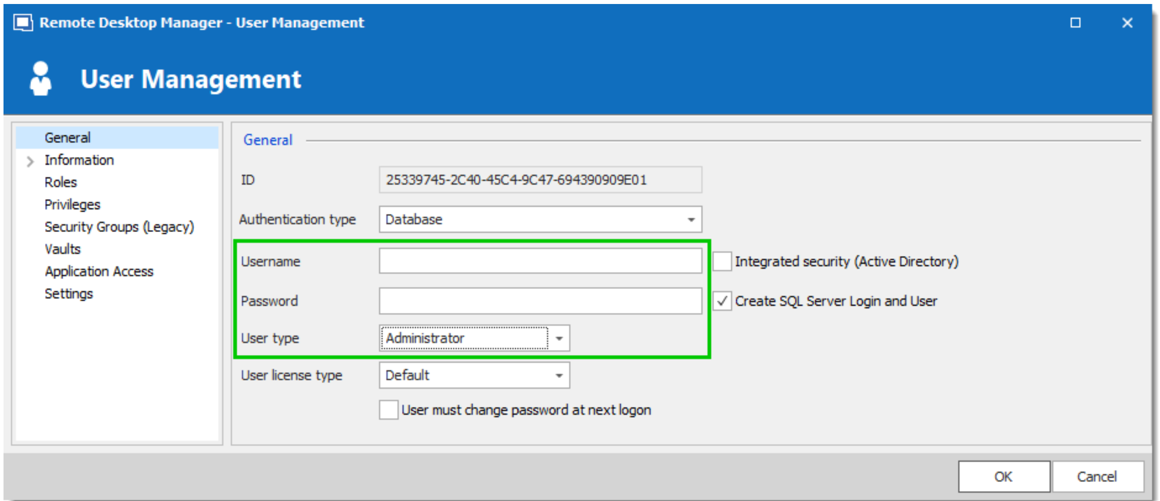
3. Select the **Upgrade** tab and click the **Create Database** button. If the database is already created on the Microsoft Azure SQL Server, click the **Update Database** button to add the appropriate tables to the database.



Upgrade Tab

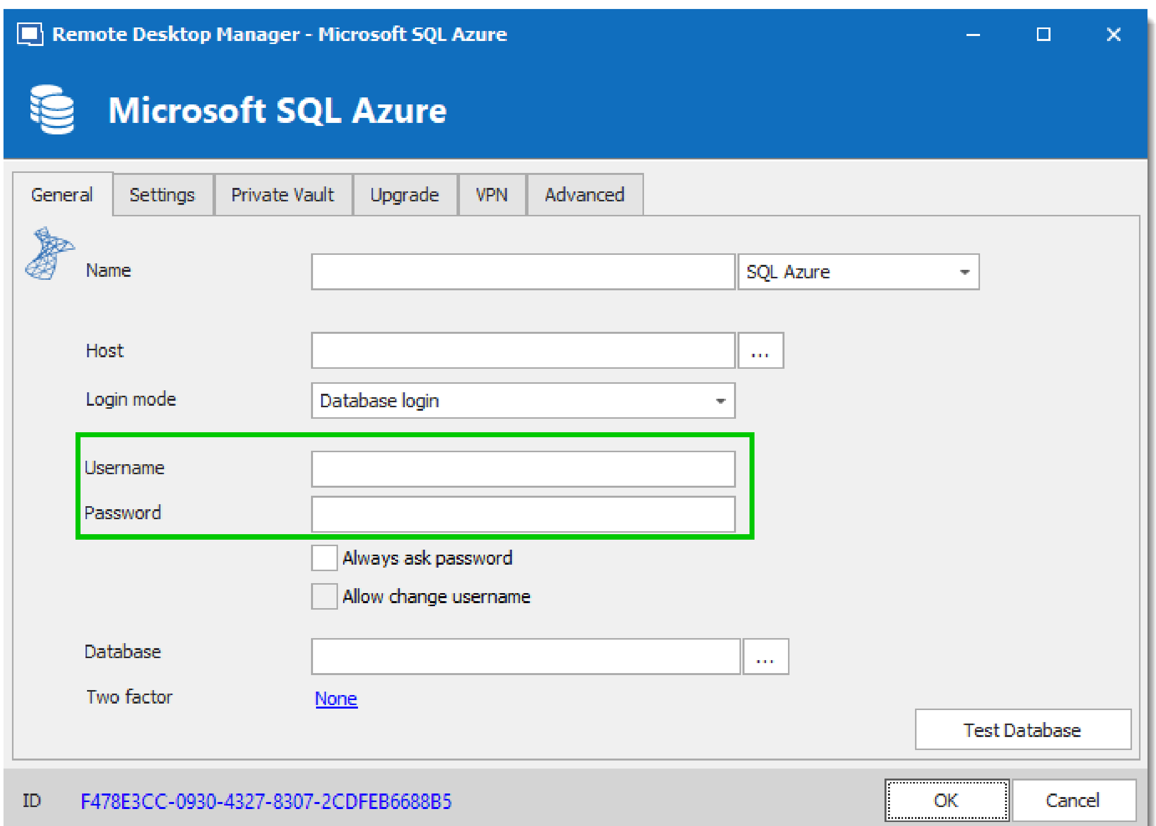
4. Once the database is created, create an administrator account for the database via the Administration - User Management menu.

> If the database is created using a system administrator (example: SA), we recommend to keep this user only for the database creation and the database upgrade. A Remote Desktop Manager administrator account must be created first. Then, regular users are created with this administrator account.



Create a Remote Desktop Manager Administrator Account

5. Connect on the Microsoft Azure SQL database with the Remote Desktop Manager administrator account. To do so, edit the data source used to create the database and change the login information for the administrator account that you have created.



Connection to the Database with the RDM Administrator Account

The Microsoft Azure SQL data source is now correctly configured.

5.4.2.3.2 Enable Azure Active Directory Authentication

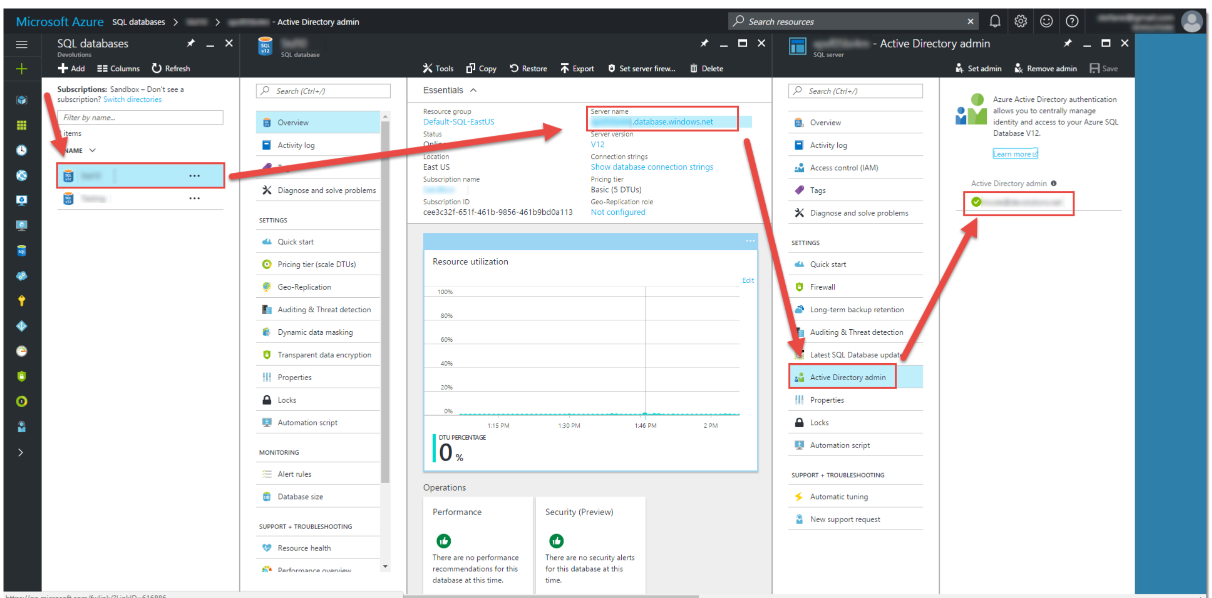
5.4.2.3.2.1 Configure the Active Directory Admin

DESCRIPTION

To enable SQL Server Azure Active Directory Authentication you must first configure the Azure Active Directory admin of the server.

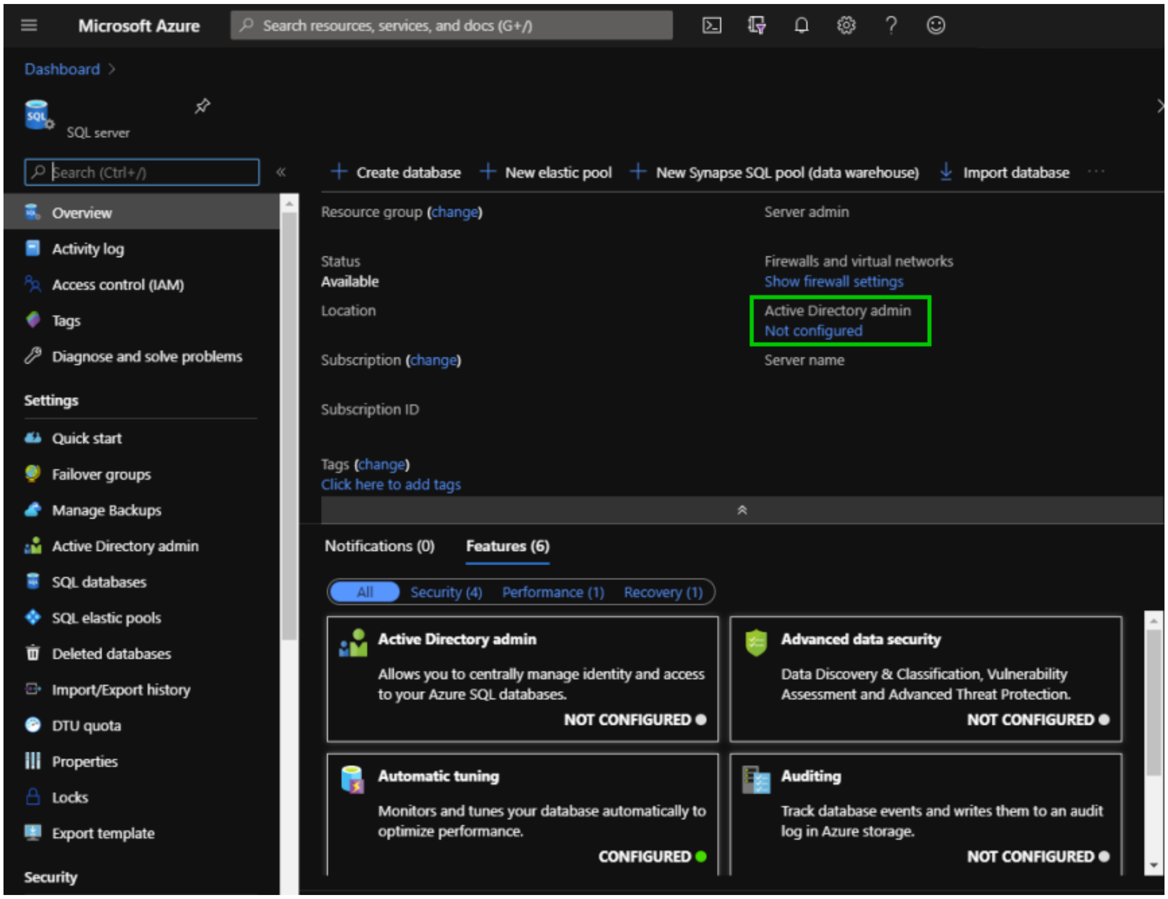
It may take a few minutes for this change to propagate. You might experience a time delay before being able to connect with this Active Directory account.

You can use an existing Microsoft Azure account if you already have one created. It is not necessary to create another to perform the following steps.

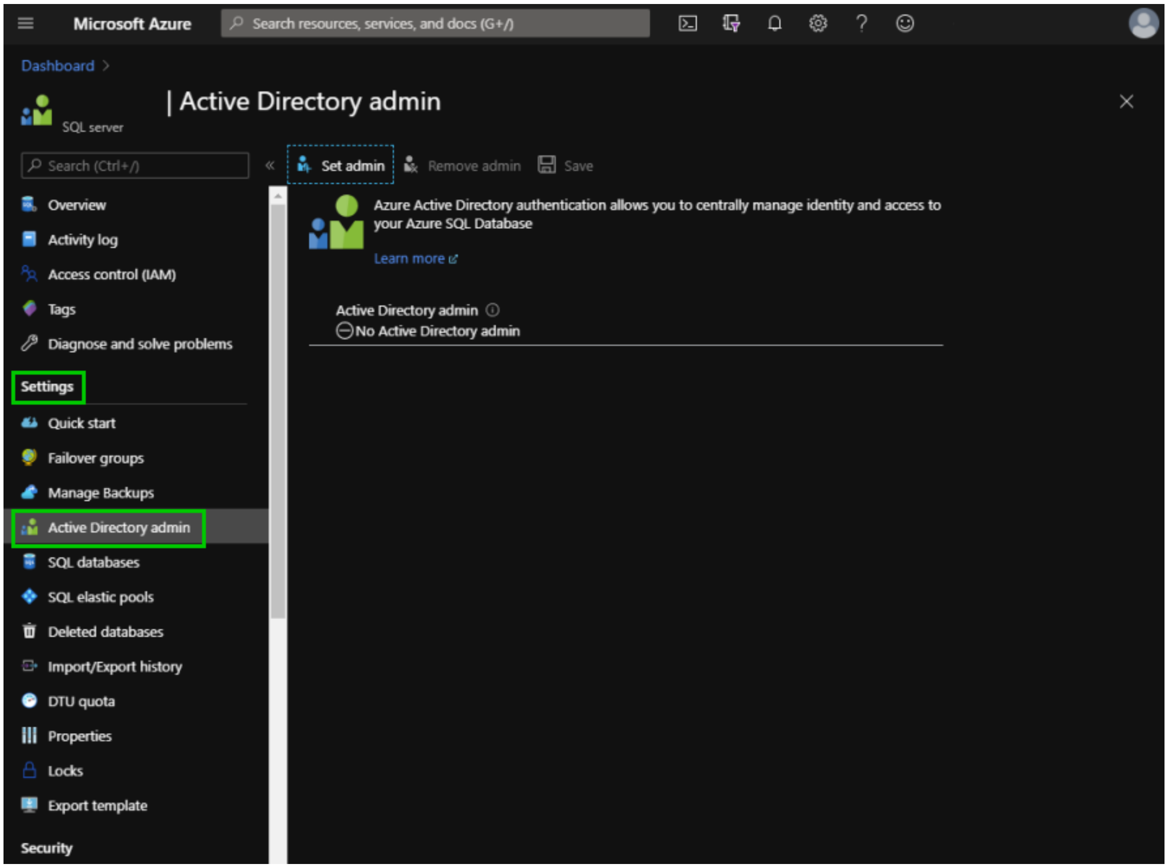


Azure AD Portal

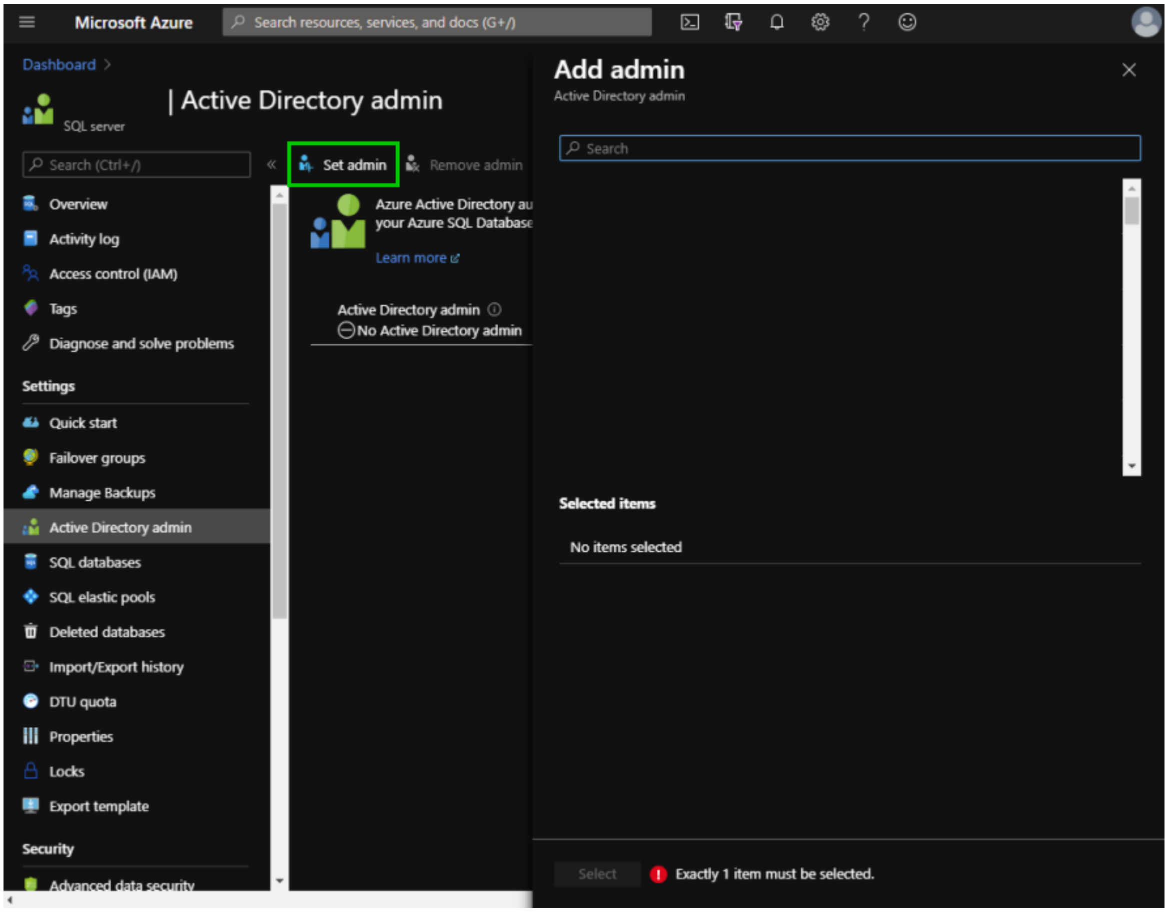
1. Has show in the ***Overview*** tab the ***Active Directory admin*** is set to ***Not configured***.



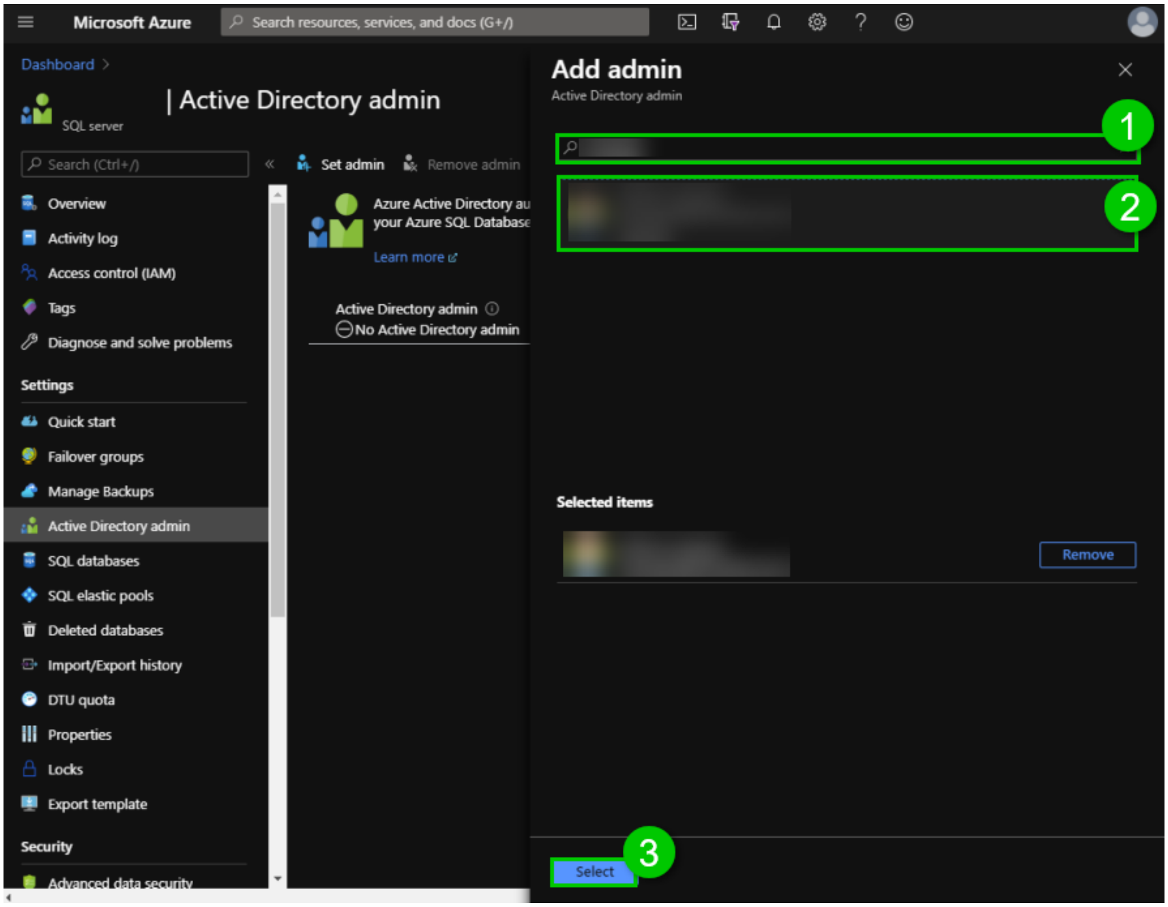
2. Click on ***Active Directory admin*** under ***Settings*** in the left menu.



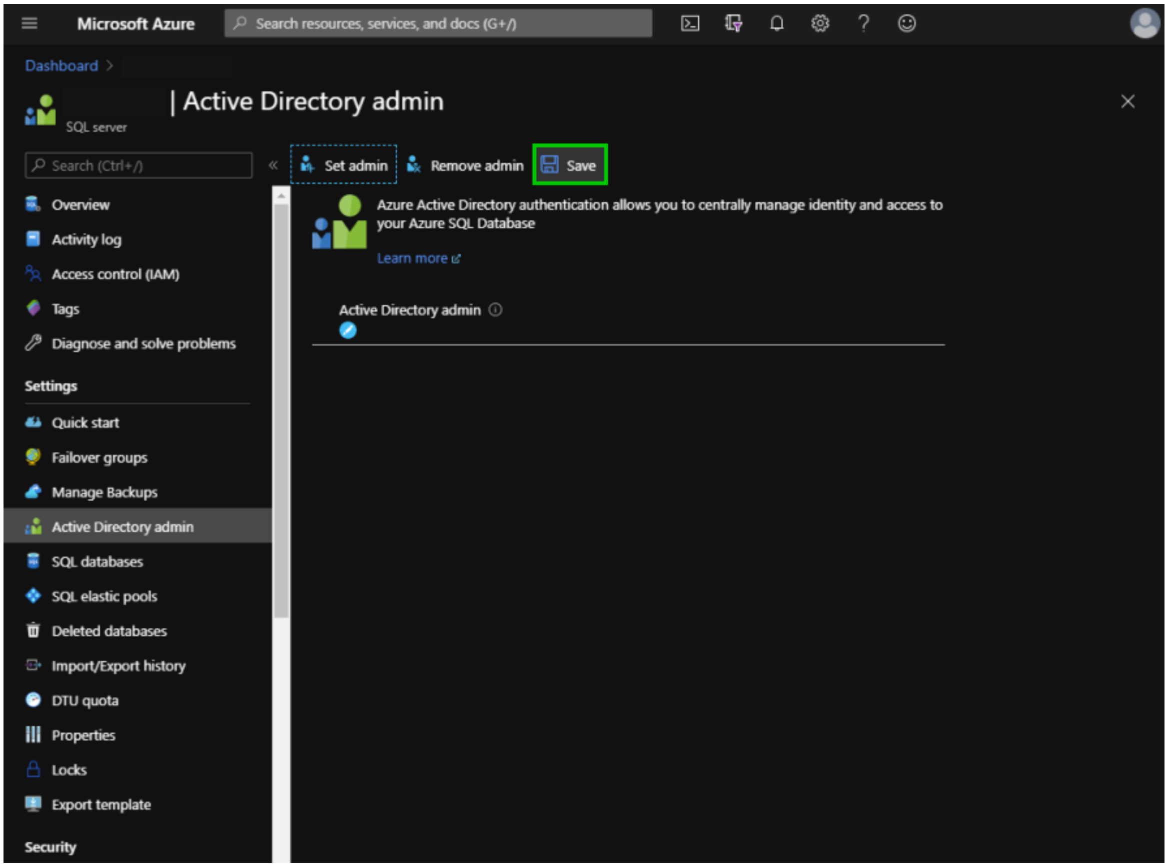
3. Click on ***Set admin*** to search for the admin.



4. Type the admin name in the ***Search*** field, click on the admin in the list provided and then ***Select***.



5. To finish the process click on ***Save***.



6. Copy the ***Active Directory admin*** email, it is essential for the next steps.

5.4.2.3.2.2 Create an Azure Active Directory App Registration

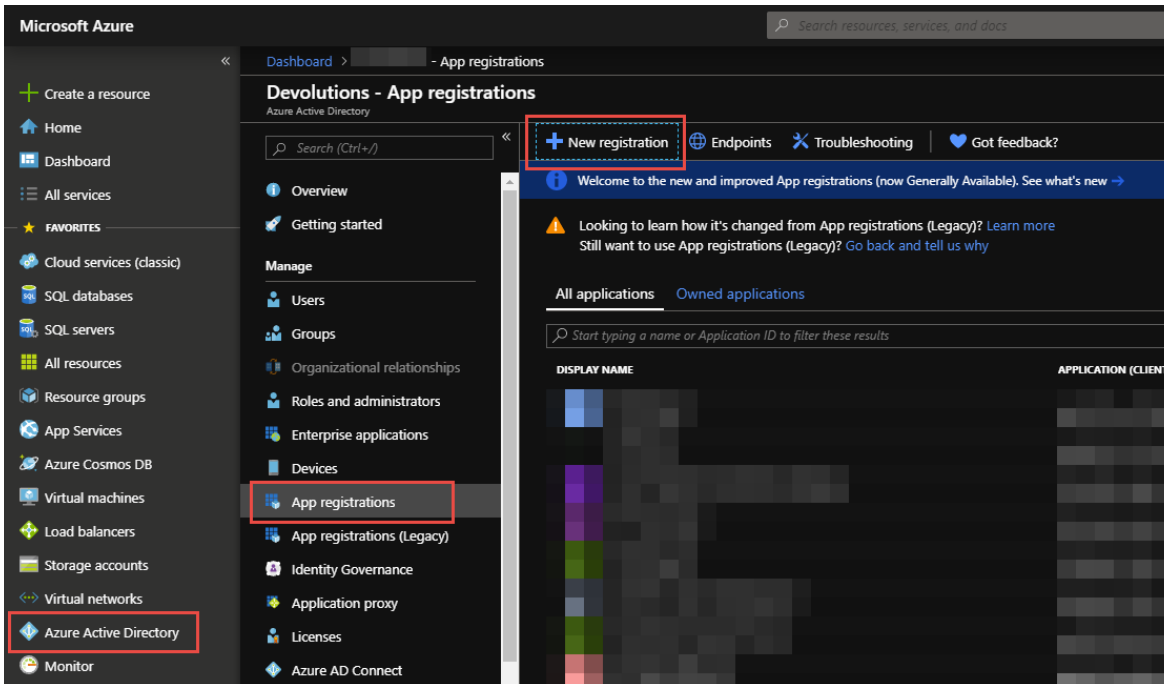
DESCRIPTION

> This step is optional and not required if your Remote Desktop Manager version is 2022.1 and higher.

To be able to use the **Active Directory Interactive (with MFA Support)** authentication method in Remote Desktop Manager, a new app registration needs to be registered in the Microsoft Azure SQL console (Azure Active Directory) with the appropriate API permissions.

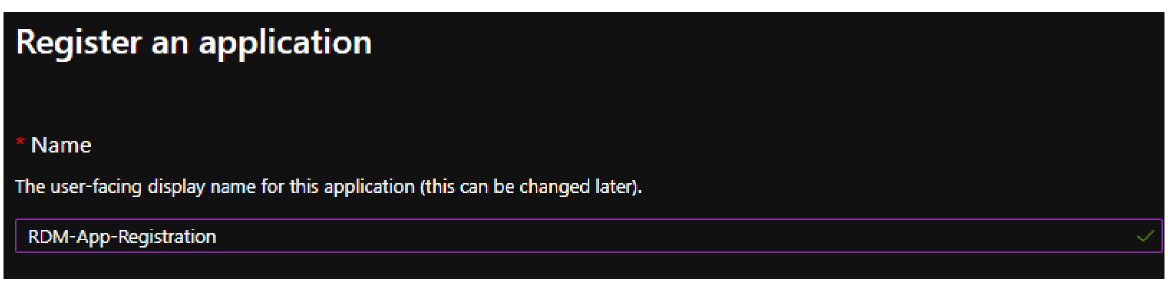
SETTINGS

1. Login on [Azure Portal](#).
2. In the **Azure Active Directory** section, select ***App registrations*** and then, ***New registration***.



App Registration

3. Configure the ***Name***.

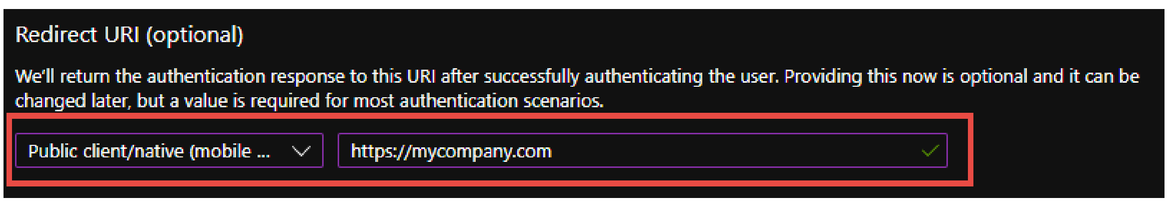


4. Select the ***Supported account types***.

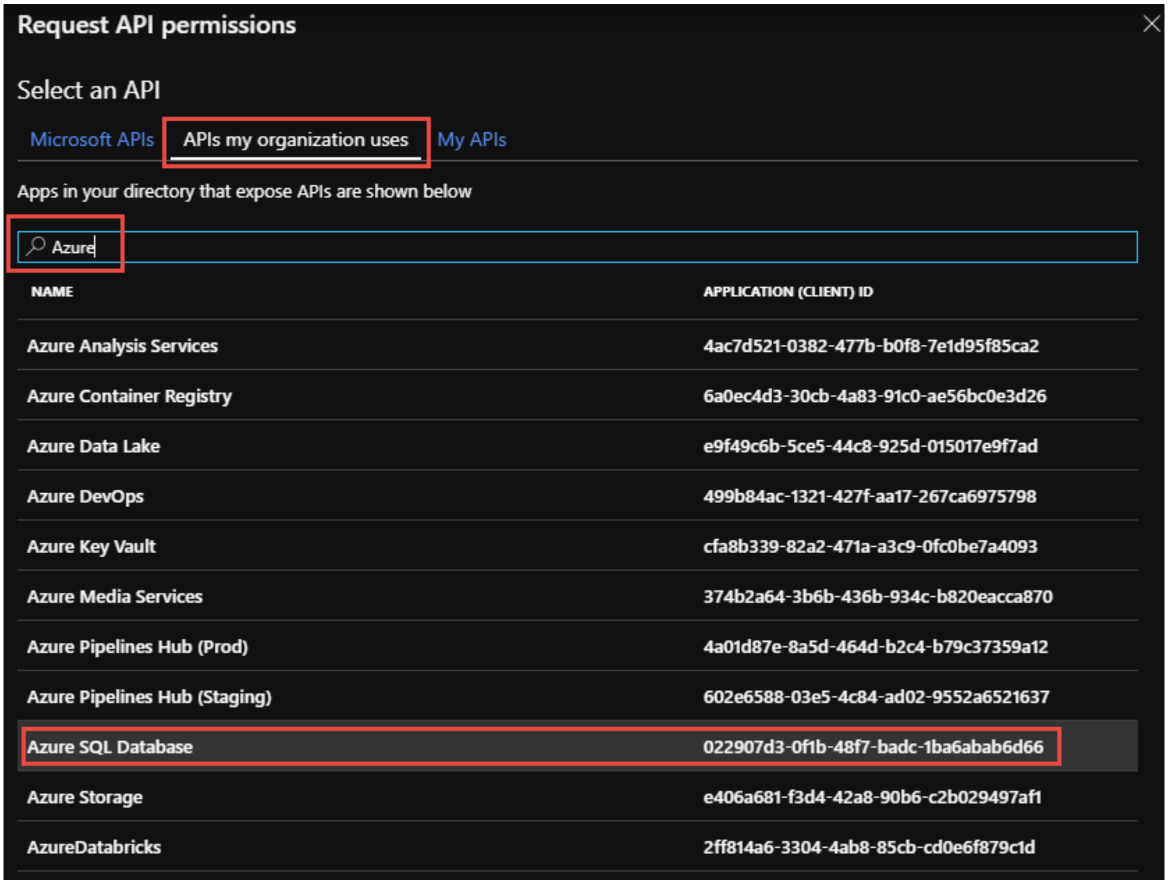
5. Configure the ***Redirect URI*** as indicated below and click ***Register***.

The ***Redirect URI*** setting MUST be configured ***Public client/native (mobile & desktop)***.

In our example the ***Redirect URI*** is set to https://mycompany.com, but we suggest you personalize it to the domain of your company home page. This will be necessary in the authentication step of the topic Configure RDM Active Directory Interactive (with MFA).

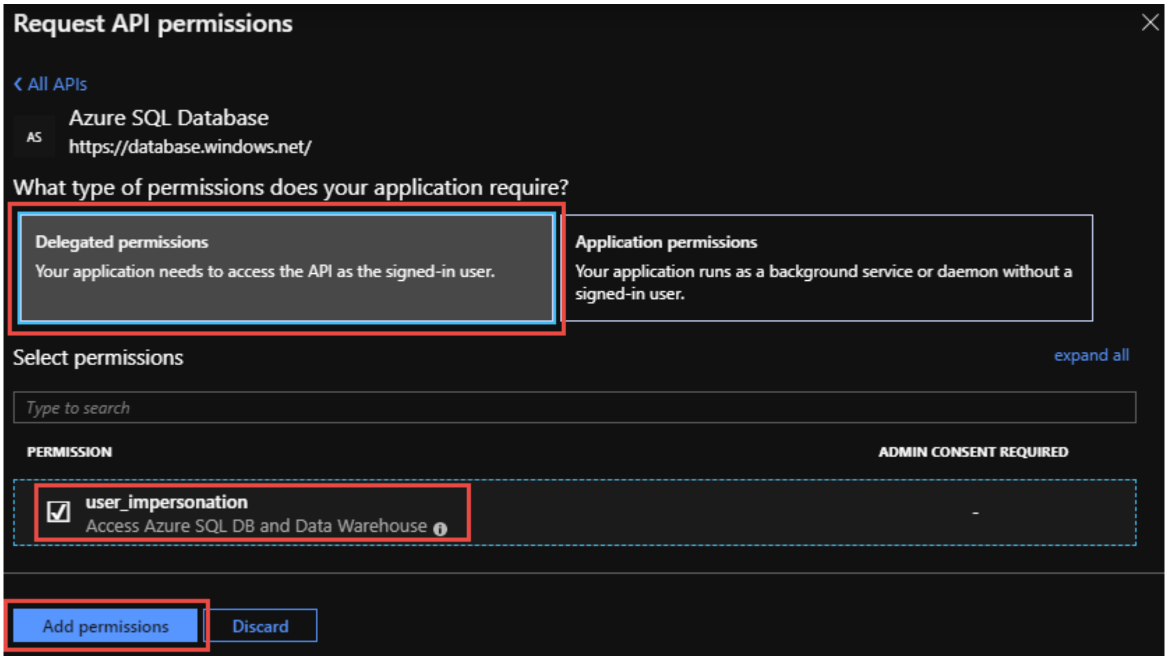


6. Select ***APIs my organization uses***, then type **Azure** and select ***Azure SQL Database***.



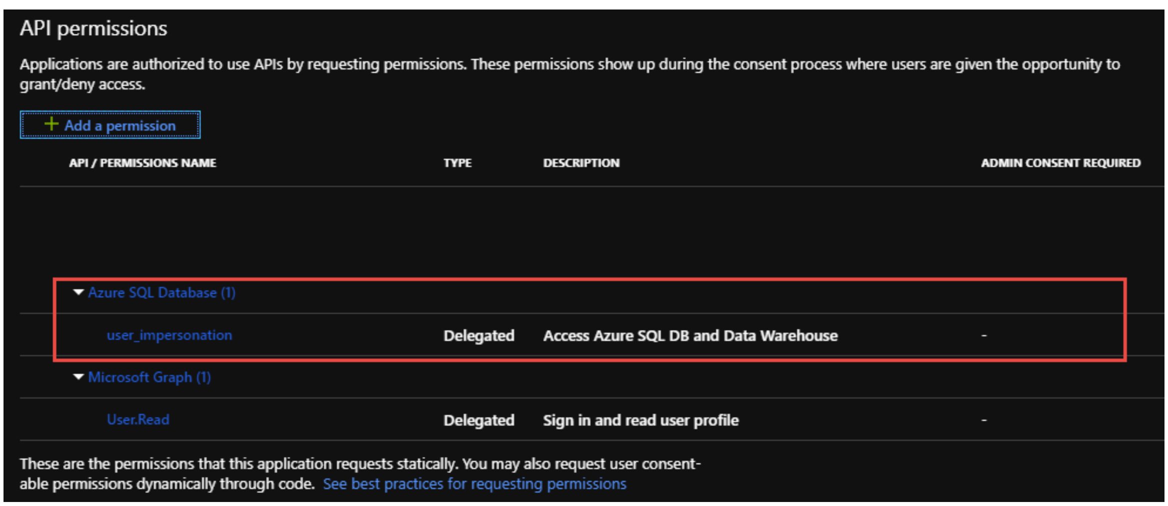
APIs my organization uses

7. Select ***Delegated permissions – user_impersonation*** and click ***Add permissions***.



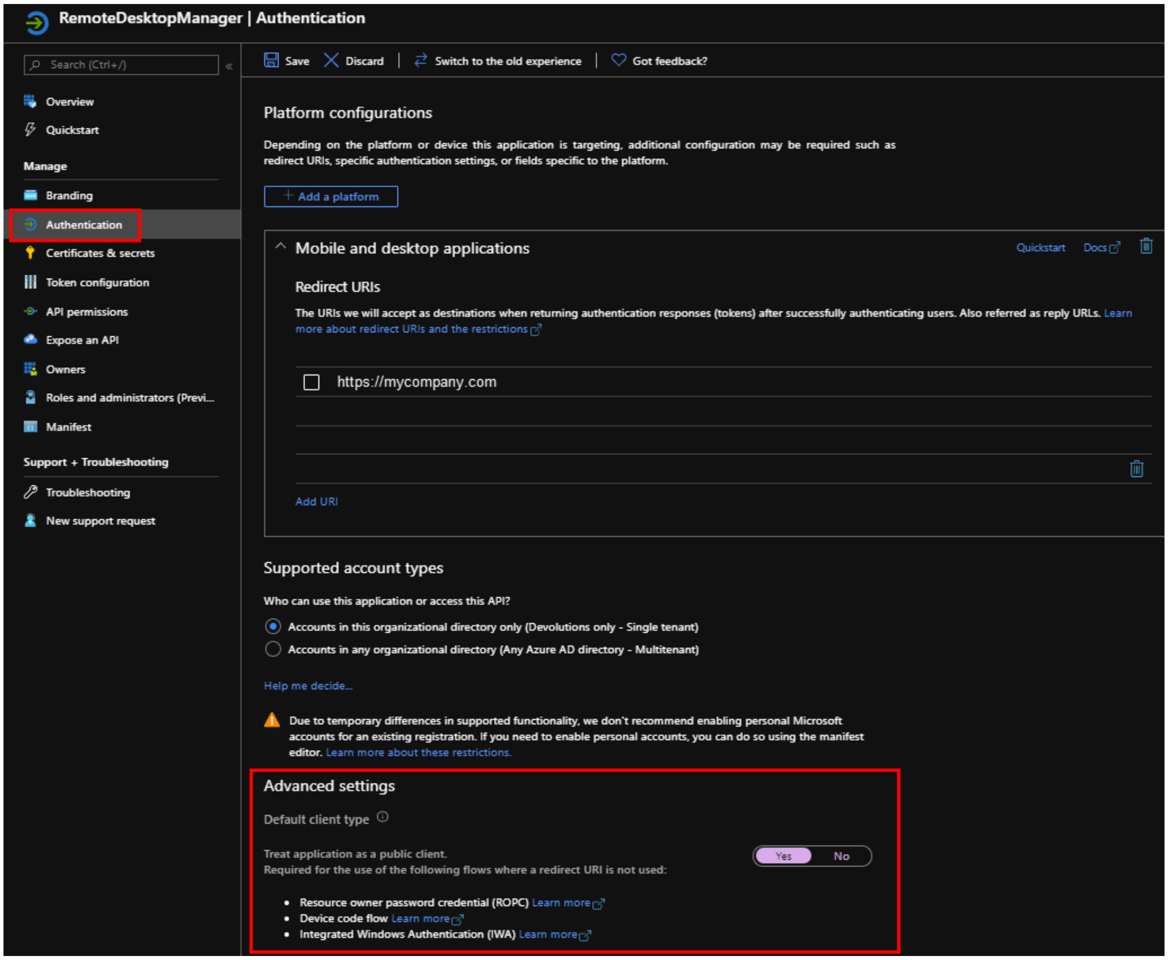
user_impersonation

8. The ***API permissions*** should look like this. You will see the new permission we just added and the preexisting Microsoft Graph.



API / Permissions Name

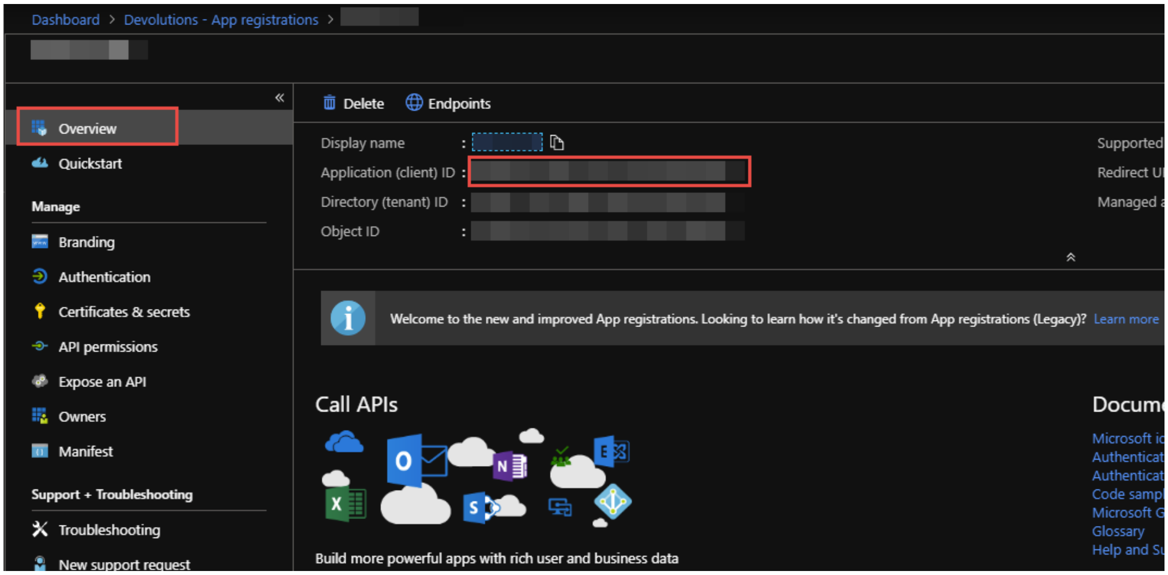
9. **Optional step**: Click on the ***Authentication*** section and switch to ***Yes***, if you desire the ***Integrated Windows Authentification (IWA)*** option



Authentication

10. Your **Azure Active Directory App Registration** is now completed.

11. Copy the ***App Registration's Application (client) ID*** needed in Remote Desktop Manager in the next step.



Application (client) ID

5.4.2.3.2.3 Configure RDM Active Directory Interactive (with MFA)

DESCRIPTION

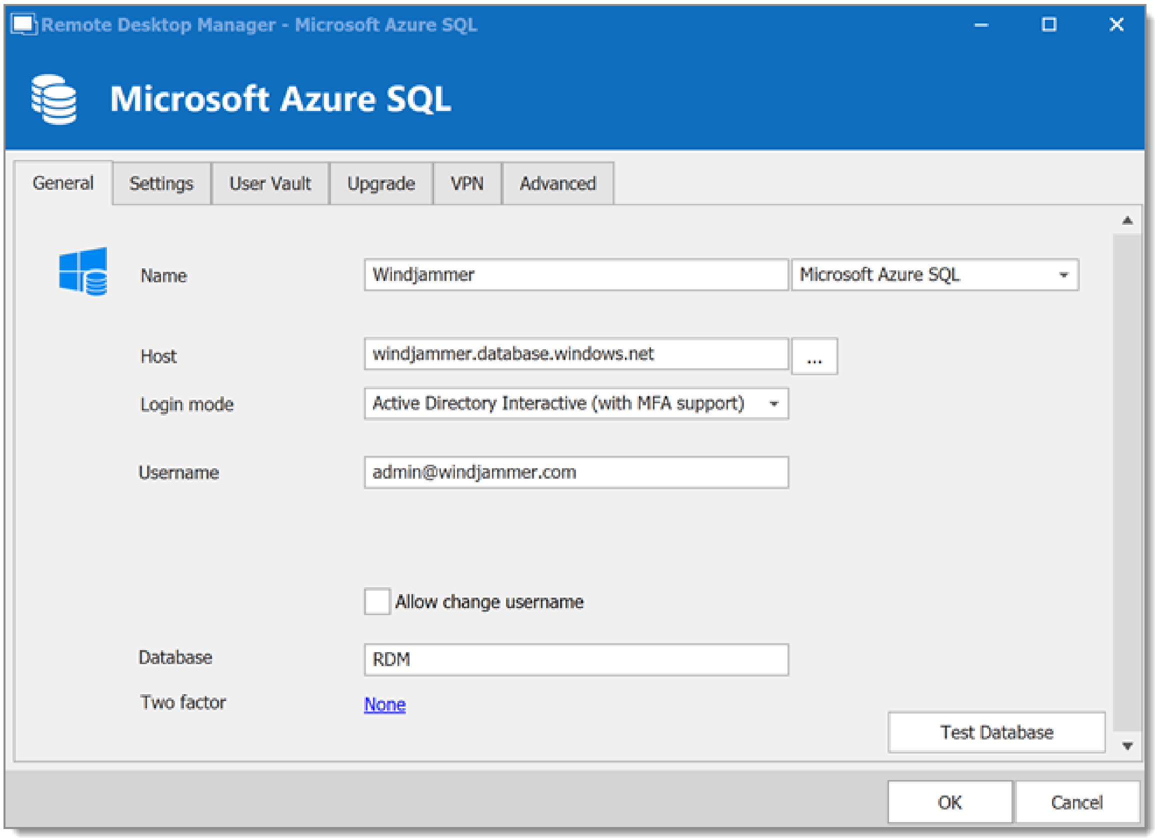
This topic is for Remote Desktop Manager version 2022.1 and higher. If you are using an older version please follow this topic instead.

Active Directory Interactive (with MFA Support) allows you to authenticate on your Microsoft Azure SQL data source using your Office365 account + MFA.

When creating SQL Active Directory users, you must be logged in with an Azure Active Directory user. Otherwise it will fail and you will be notified of the error.

Use the servers defined Azure Active Directory Admin to create your first RDM admin users. Once you've created, you can use this new account to create other users.

SETTINGS

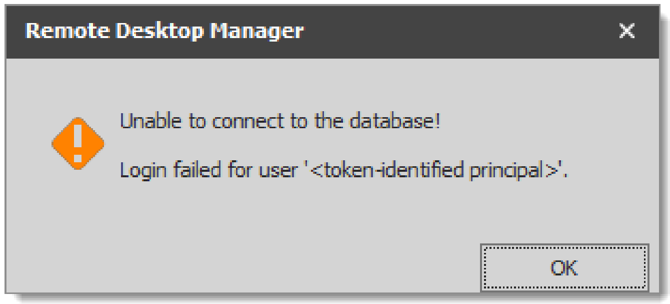


Azure with MFA

1. Select ***Active Directory Interactive (with MFA Support)*** from the ***Login mode*** dropdown menu.

2. In the ***Username*** field, paste the ***Active Directory admin*** email you created in the Microsoft Azure SQL databases.

On first connect, the username must be the Active Directory Admin as defined in the Configure the Active Directory Admin. Once you add other AD user in RDM they will be able to connect.



If you get this message error: Unable to connect to the database! Login failed for user '<token-identified principal>' double check the username for spelling errors.

3. Configure the database to authenticate in the ***Database*** field.

5.4.2.3.2.4 Configure RDM Older Version AD Interactive (with MFA)

DESCRIPTION

This topic is for Remote Desktop Manager versions lower than 2022.1. If you are using 2022.1 and higher please follow this topic instead.

Active Directory Interactive (with MFA Support) allows you to authenticate on your Microsoft Azure SQL data source using your Office365 account + MFA.

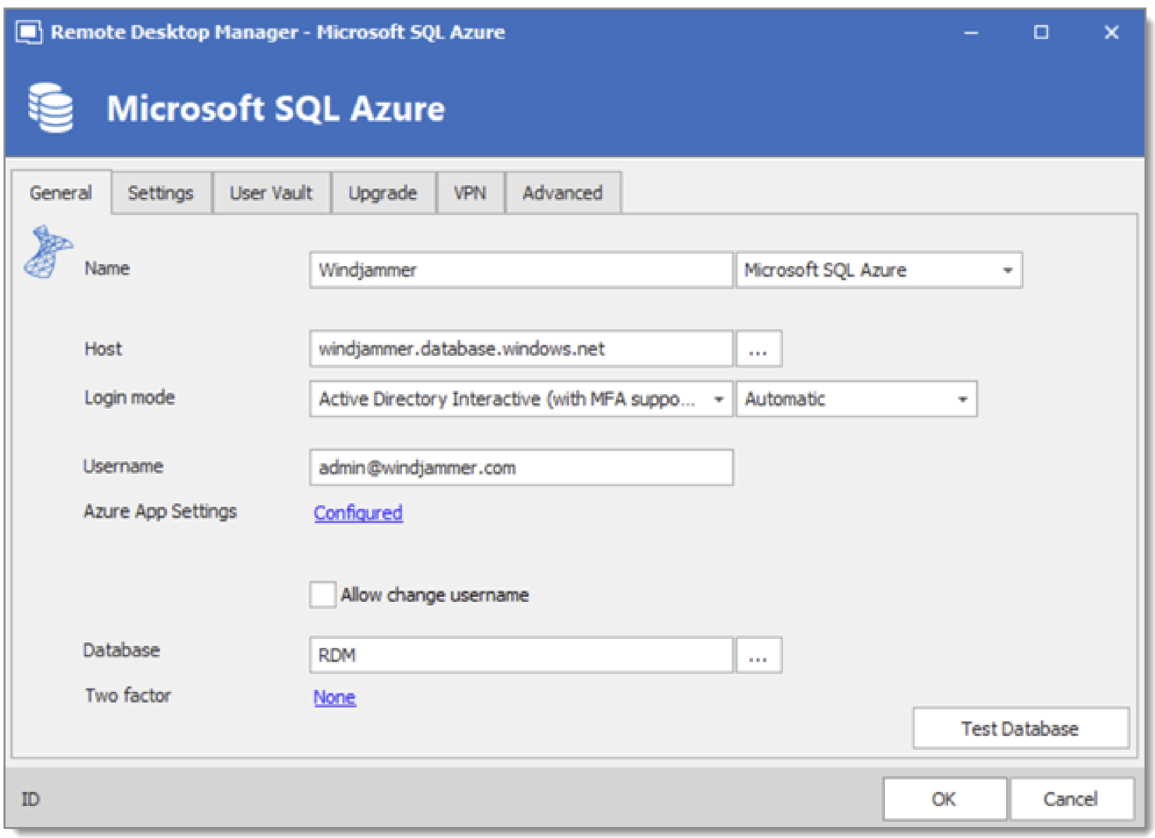
For Azure AD authentication, download and install the Microsoft **Active Directory Authentication Library for Microsoft SQL Server** on every client computer.

This install the required Microsoft libraries that will enable Azure AD authentication. Please download it here : https://www.microsoft.com/en-us/download/details.aspx?id=48742.

When creating SQL Active Directory users, you must be logged in with an Azure Active Directory user. Otherwise it will fail and you will be notified of the error.

Use the servers defined Azure Active Directory Admin to create your first RDM admin users. Once you've created, you can use this new account to create other users.

SETTINGS



1. Select ***Active Directory Interactive (with MFA Support)*** from the ***Login mode*** dropdown menu.

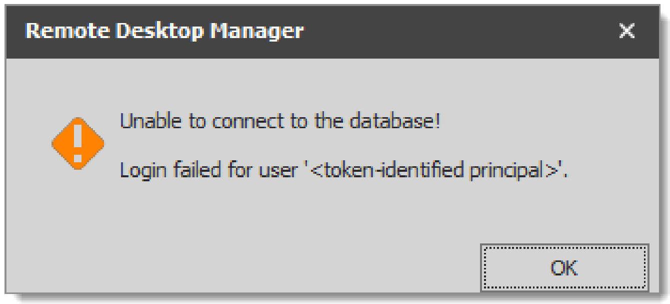
2. You can specify how you want RDM to interact with Azure AD during the authentication.

OPTION	DESCRIPTION
Default	This is the default mode. The user will be prompted for credentials even if there is a token that meets the requirements already in the cache.
Automatic **(Shared in older versions)**	Azure AD will prompt the user for credentials only when necessary. If a token that meets the requirements is already cached then the user will not be prompted.

When it comes to Azure AD joined devices (registered devices). Azure AD may or may not prompt for MFA. **This is entirely controlled by Azure AD**, there is nothing we can do in RDM to force or bypass the MFA other than the ***Default*** or ***Automatic*** options mentioned above.

3. In the ***Username*** field, paste the ***Active Directory admin*** email you created in the Microsoft Azure SQL databases.

On first connect, the username must be the Active Directory Admin as defined in the Configure the Active Directory Admin. Once you add other AD user in RDM they will be able to connect.

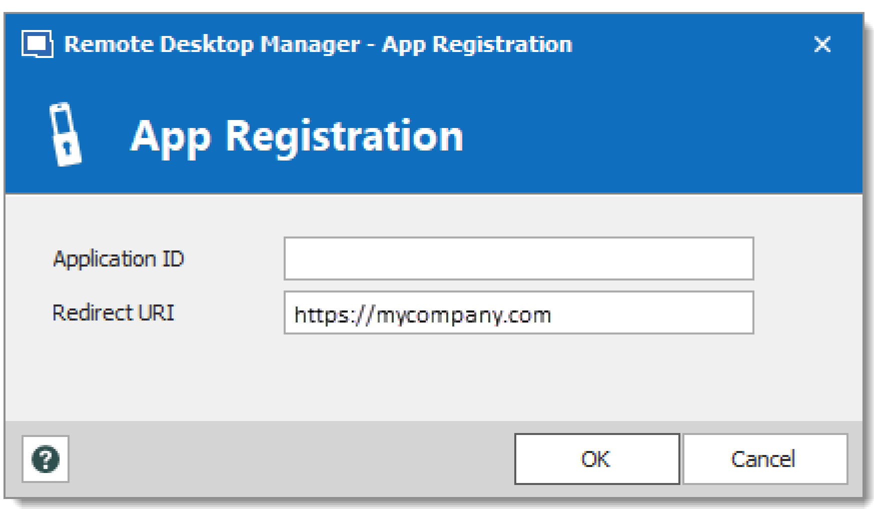


If you get this message error: Unable to connect to the database! Login failed for user '<token-identified principal>' it is because you are not using the ***Active Directory admin*** email you created in the Microsoft Azure SQL databases.

4. Click on ***Configure*** to set the Azure App Settings and enter the application ID from the Azure Active Directory App Registration and the corresponding Redirect URI.

When you receive this error: ***AADSTS70001 - Application with Identifier was not found in the directory…***

Validate that your ***Application ID*** in RDM is identical to the ***App Registration's Application (client) ID*** (step 11 of Create an Azure Active Directory App Registration)



App Registration

5. Configure the database to authenticate in the ***Database*** field.

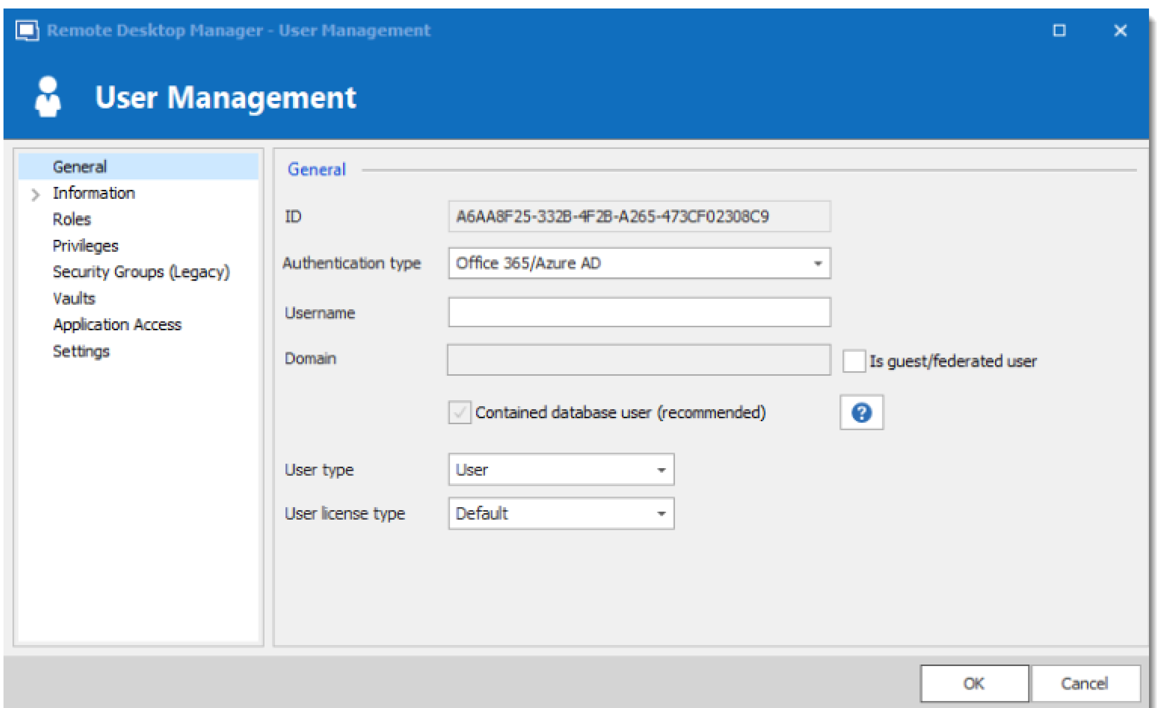
5.4.2.3.2.5 Configure Azure Active Directory user in RDM

DESCRIPTION

From Remote Desktop Manager navigate to ***Administration – Users***, and add a new user.

In the ***Authentification type*** select ***Office365/Azure AD*** and enter in the ***Username*** field the email of the user, click ***Ok***.

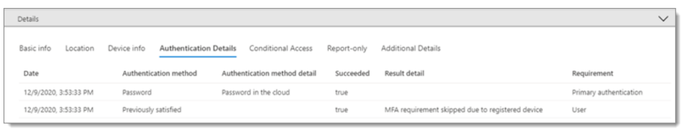
> If ***Office365/Azure AD*** is not available in the drop down menu of ***Authentification type***, please validate that all the steps have been done as per this topic.



Set the Authentication type to Office365/Azure AD

The option ***Is guest/federated user*** should only be check in rare and special case where the account is guest or federated. If that is the case, you will be required to enter a full domain that should resemble this: azuresubscriptionprefix.onmicrosoft.com

If you do not receive the MFA prompt. Please validate your Azure logs in ***Authentications Details - Result detail***. If this message appears: ***MFA requirement was skipped due to registered device***, we currently have no way to force and MFA prompt on registered devices and that’s why you are not getting the MFA prompt in that case.



5.4.2.4 Password Hub Business

DESCRIPTION

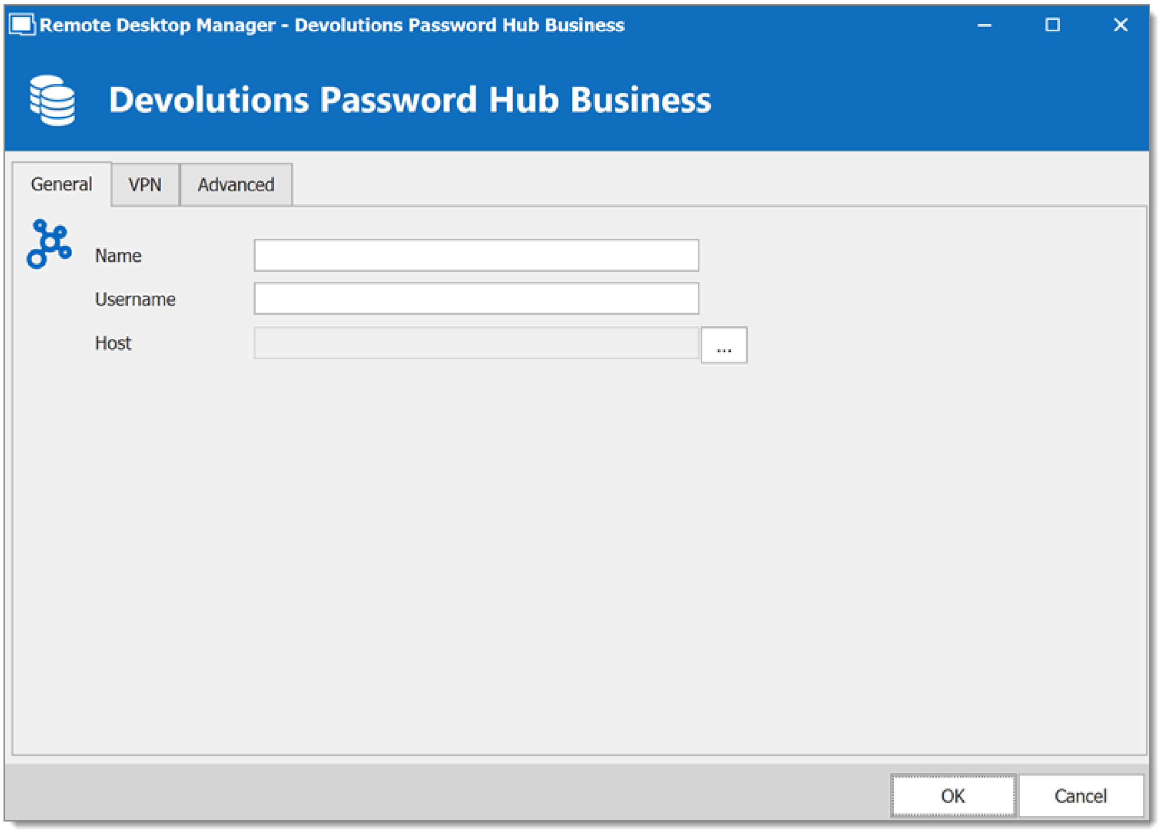
Devolutions Password Hub Business, for businesses who need to share passwords and credentials within their organization.

Please consult our website for more information on this service.

To start your free Devolutions Password Hub Business trial today click here.

SETTINGS

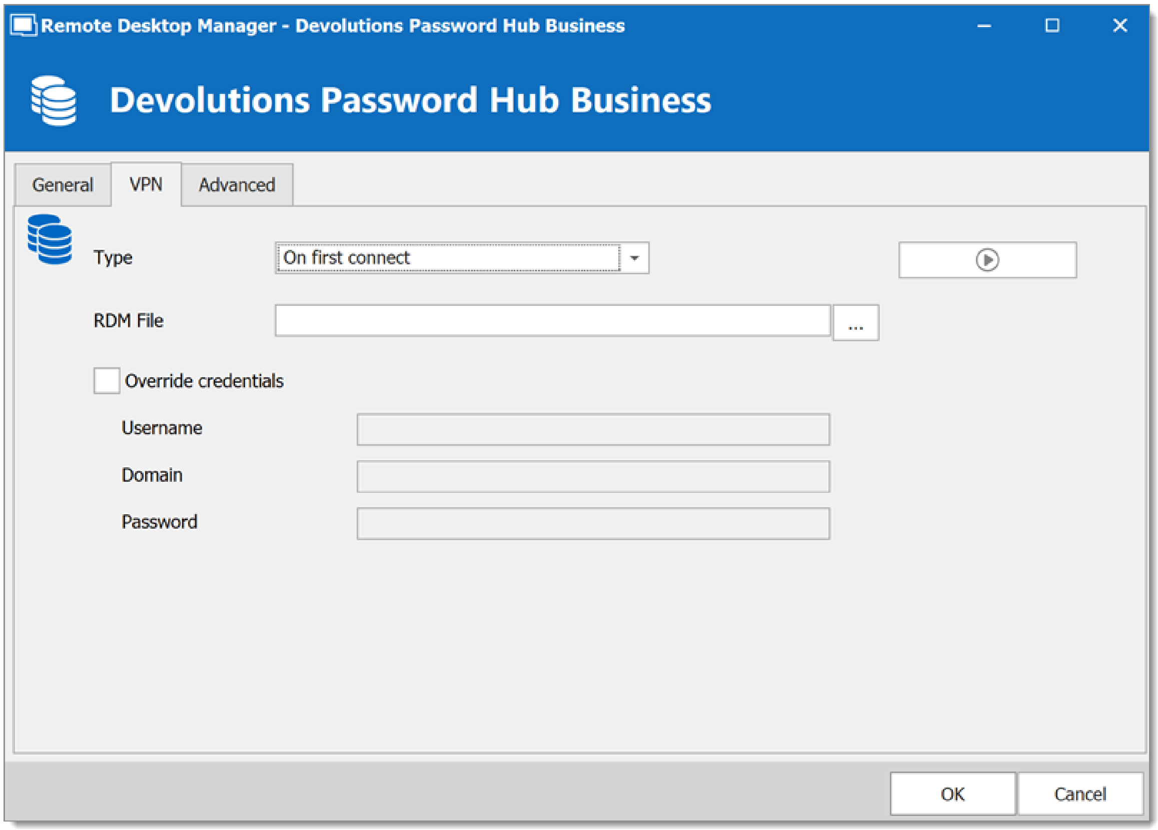
GENERAL



OPTION	DESCRIPTION
Name	Name of the data source.
Username	Your Devolutions Account email address.
Host	Copy in the ***Host*** your Devolutions Password Hub Business URL (ex: https://windjammer.devolutions.app/) or click on the 3 dots to get a drop down list to select from.

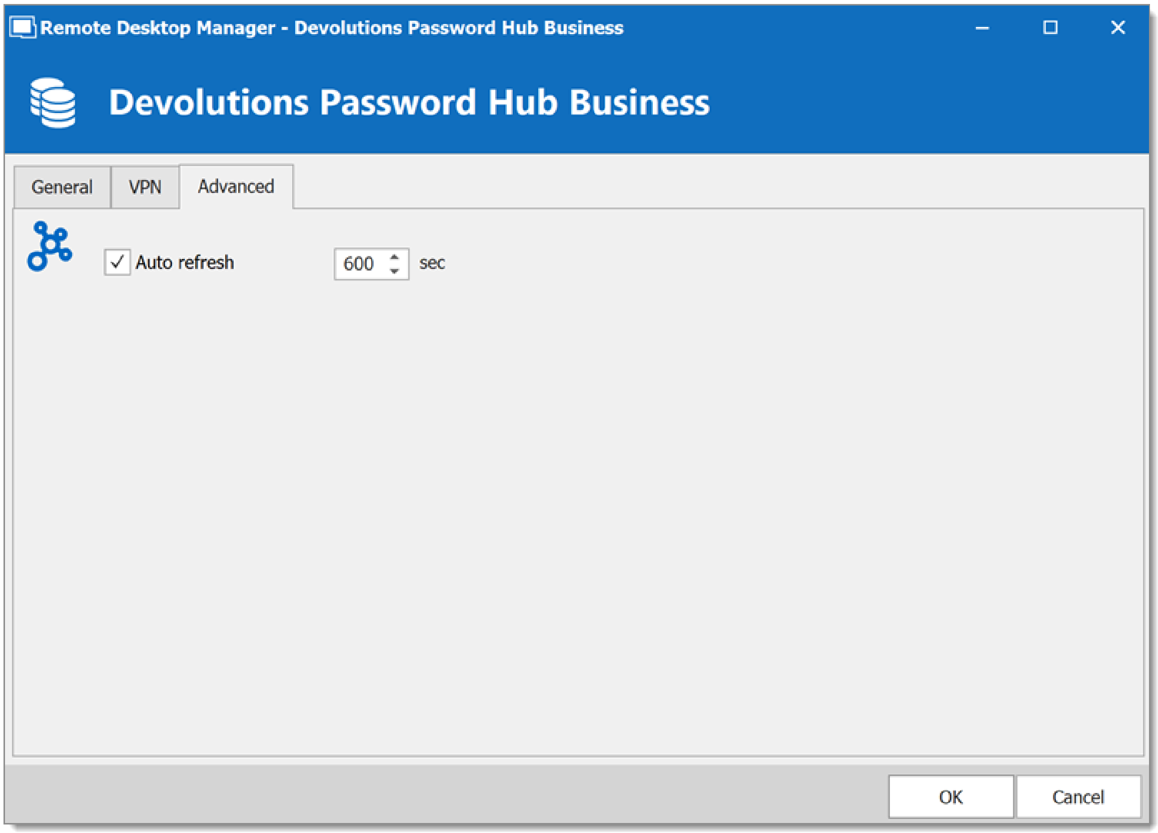
VPN

Open a VPN to access your data prior to connecting to your Devolutions Password Hub.



ADVANCED

Set the interval for the automatic refresh.



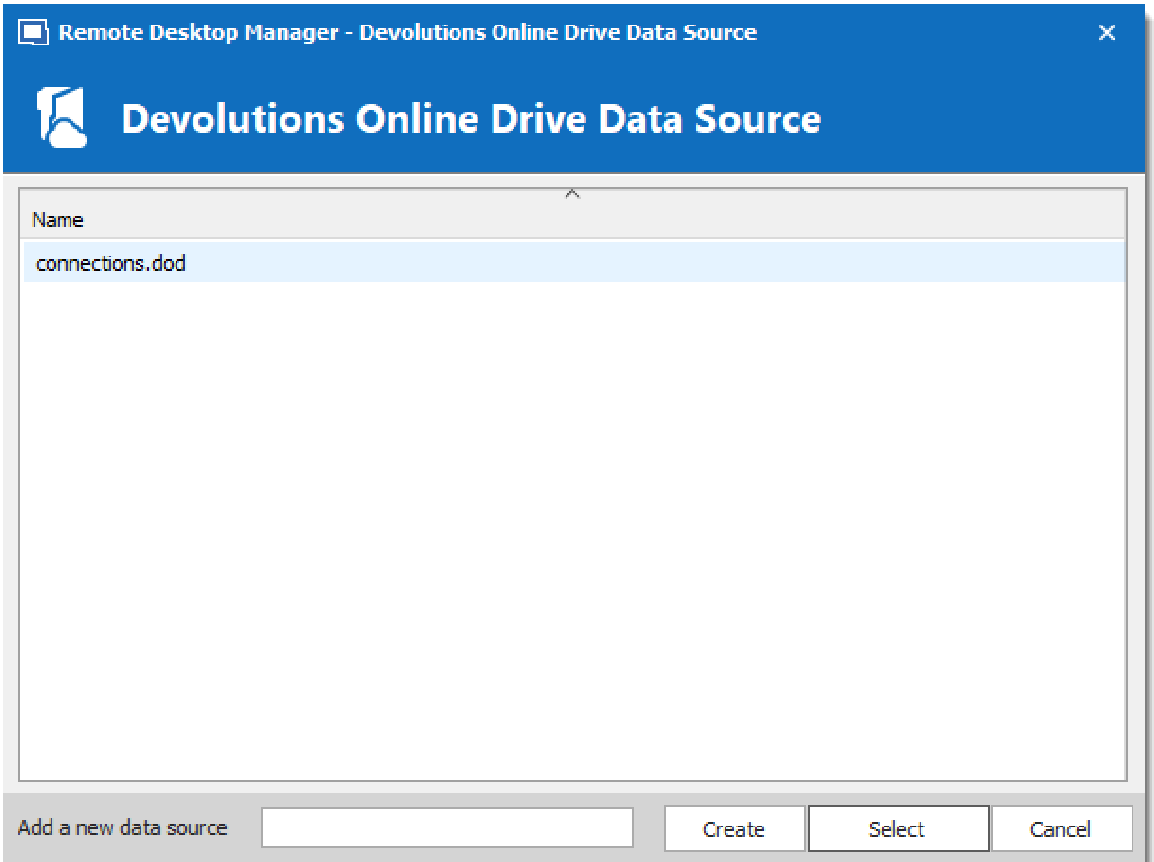
5.4.2.5 User Vault

DESCRIPTION

The **User Vault** allows you to connect a personal Vault stored in a **Devolutions Online Drive** file directly to your **Advanced Data Source**, thus allowing you to store information that only you can have access to. For more information about the User Vault please follow this link.

1. In the **User Vault** tab of your Advanced Data Source, select **Online Drive** in the **Type**.

2. Click on the **ellipsis** next to the **Filename** field. A list containing your pre-existing Devolutions Online Drive files will prompt. You may choose to use an existing file (.dod) or if you wish you can enter a name in the **New data source field** and click on **Create** to automatically create a new Devolutions Online Drive file.



Devolutions Online Drive Data Source

5.4.3 DropBox

DESCRIPTION

Remote Desktop Manager uses the Dropbox API to retrieve a XML file from the configured repository. There is no need to install the Dropbox client on the machine to open the data source. It is also possible to configure more than one Dropbox account on the same machine.

> The Dropbox integration uses the Dropbox SDK, so any features that are exclusive to the Business or Enterprise editions are NOT supported.

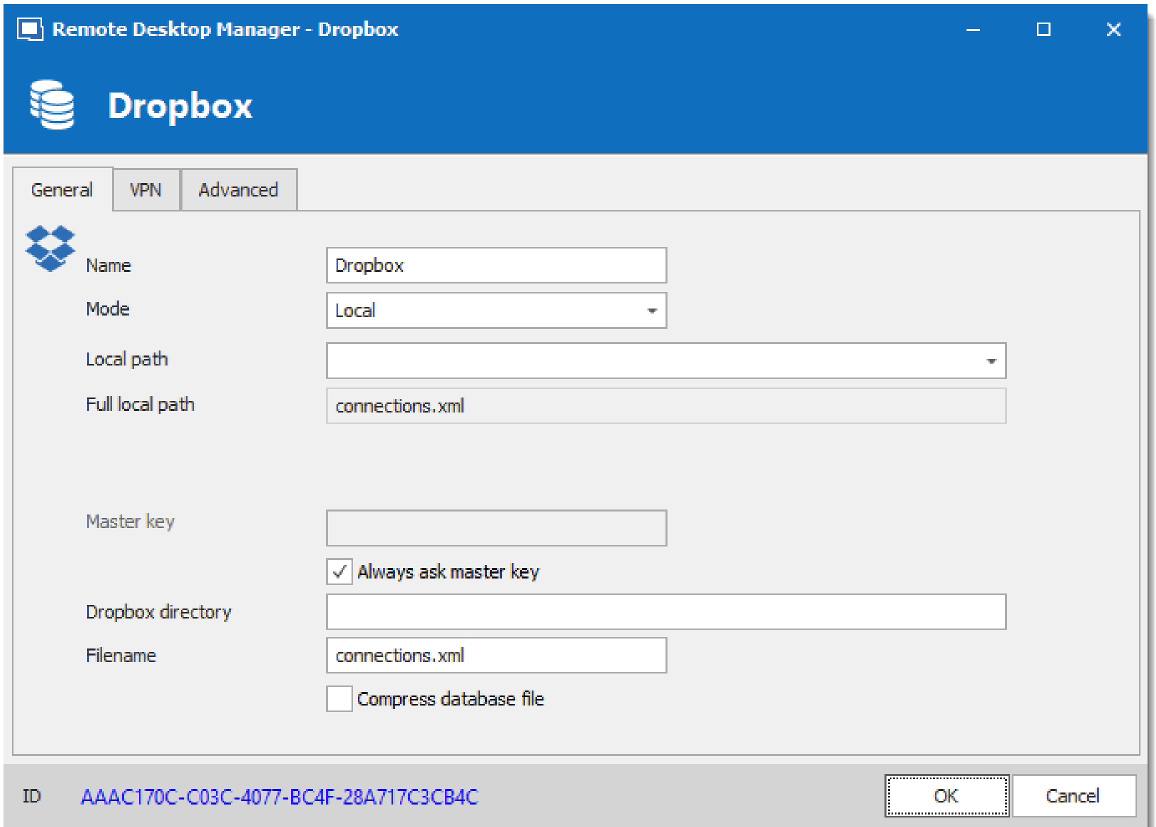
HIGHLIGHTS

- This data source can be shared over the Internet between multiple locations.
- The data source supports auto refresh.
- This is a file-based data source, based on the XML data source.
- To avoid data corruption, the session list should be modified in one location at a time.
- No need to have the Dropbox client installed to use the Dropbox data source.
- Each Dropbox data source can use a different Dropbox account.

> Although it can be shared between multiple locations, there is no conflict management for the configuration. If you share with other users you may get update conflicts and run into issues. This data source type is meant for **a single user using multiple computers, not multiple users**.

SETTINGS

GENERAL



Dropbox - General Tab

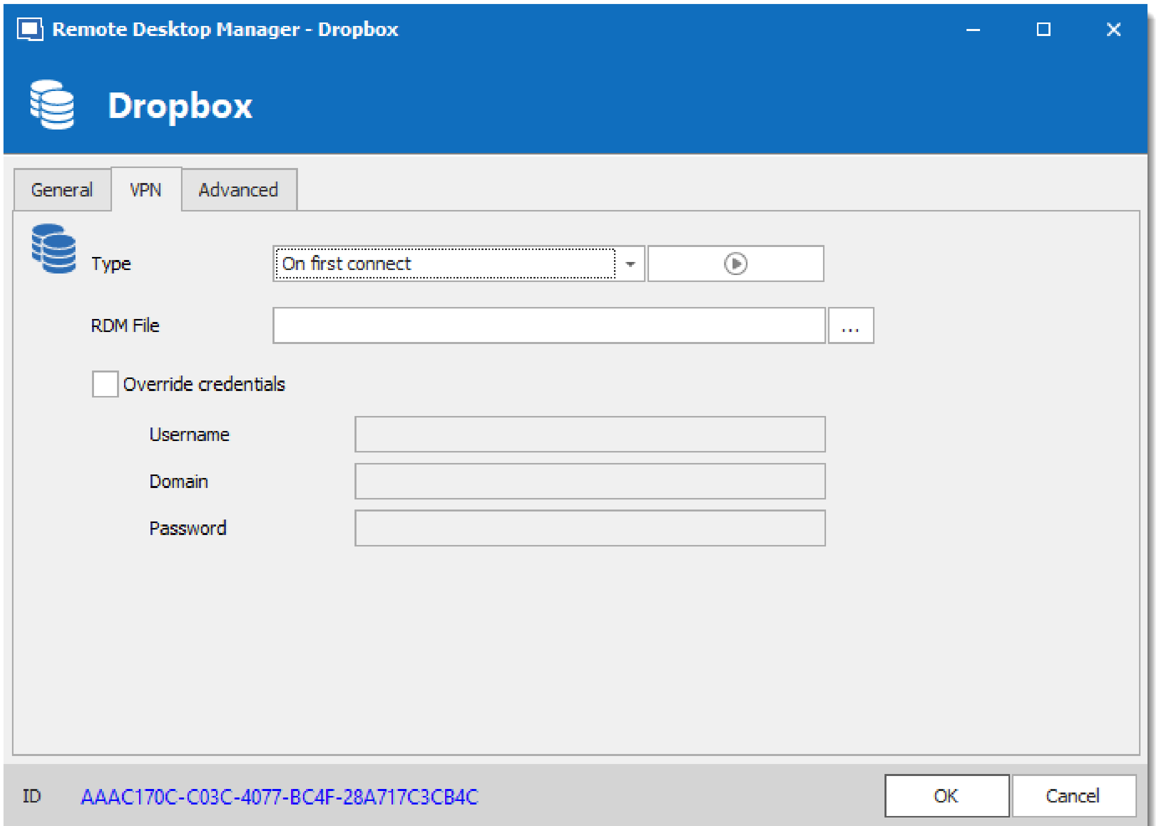
Remote Desktop Manager supports the 2-Factor Authentication of Dropbox. When the button **Validate with Dropbox** is pressed and the 2-Factor Authentication is enabled in Dropbox, a window prompt will open and ask for the Dropbox account password, then a second prompt will open for the security code. The security code can be received by SMS or generated by Google Authenticator.

OPTION	DESCRIPTION
Name	Name of the data source.
Mode	Select the mode that is preferred to configure the data source. Select between: • **Account**

OPTION	DESCRIPTION
	• **Local**
Local path (Local Mode)	Contains the local path where the Dropbox files are accessible.
Email (Accout Mode)	Contains the email address associated with the Dropbox account.
Validate with Dropbox (Account Mode)	Button to validate the email address with the Dropbox account.
Master key	Add an additional layer of security to your data source by using master key.
Always ask master key	Connecting to the data source will always prompt for the master key.
Dropbox directory	Indicate the folder in Dropbox. It should not contains any drive since it's stored online. Leave it empty to use the default Dropbox root.
Filename	Indicate the filename used to store the data on the data source.
Compress database file	Activate this option if you wish to compress your database file.

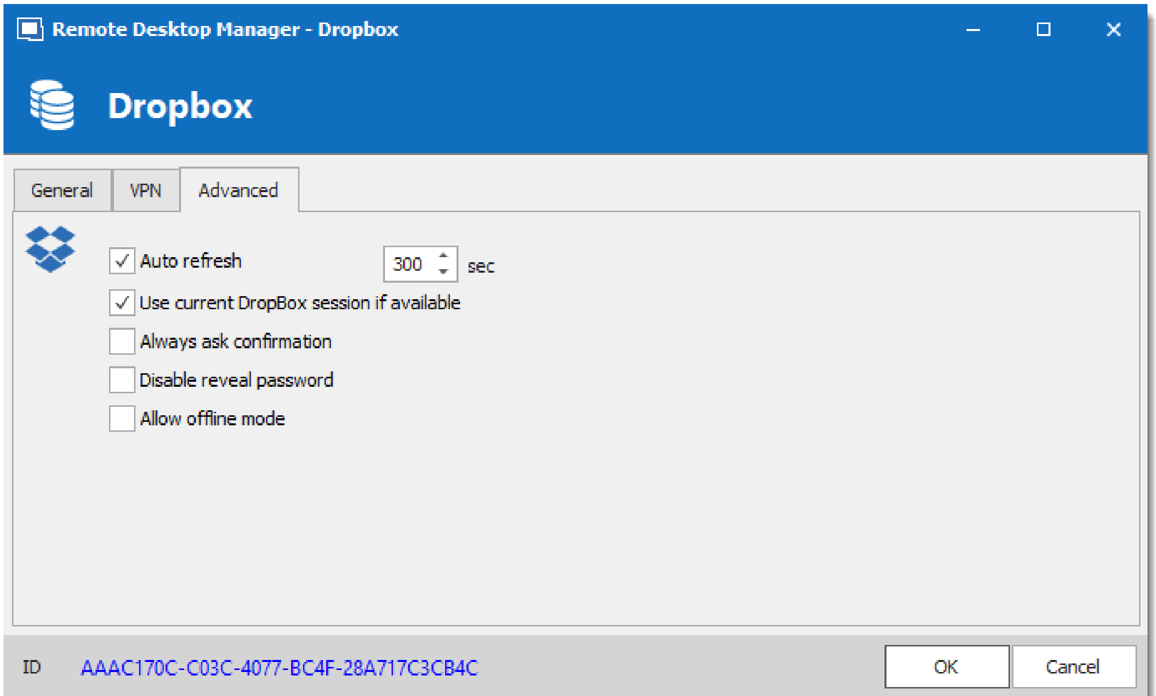
VPN

Open a VPN to access your data prior to connecting to your **Dropbox**.



Dropbox - VPN Tab

ADVANCED



Dropbox - Advanced Tab

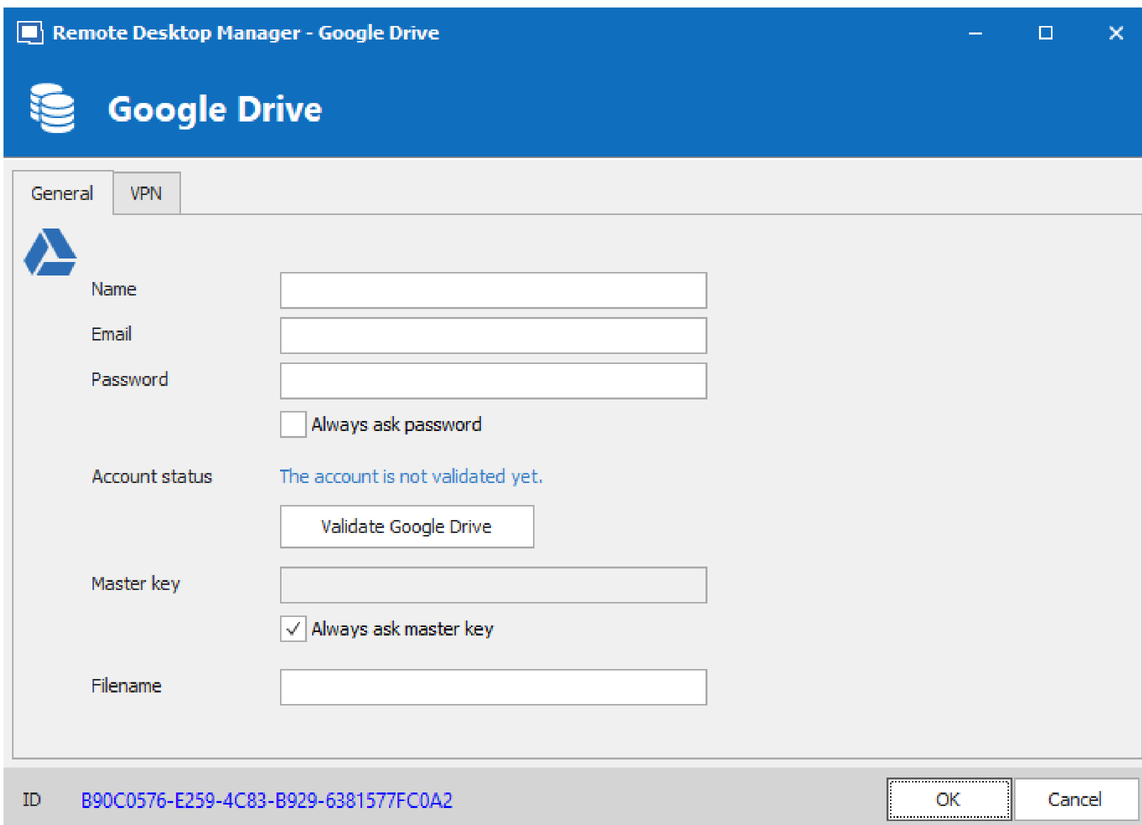
OPTION	DESCRIPTION
Auto refresh	Set the interval to use between each automatic refresh.
Use current Dropbox session if available	This option will use the Dropbox account who has been already validated without any other validation.
Always ask for confirmation	Always ask for confirmation when connecting to the data source.
Disable reveal password	Disable the reveal password feature when a user access this data source.
Allow offline mode	Allow the data source to be used in Offline mode.

5.4.4 Google Drive

DESCRIPTION

Remote Desktop Manager downloads and uploads the session settings directly from file located on an FTP site.

GENERAL



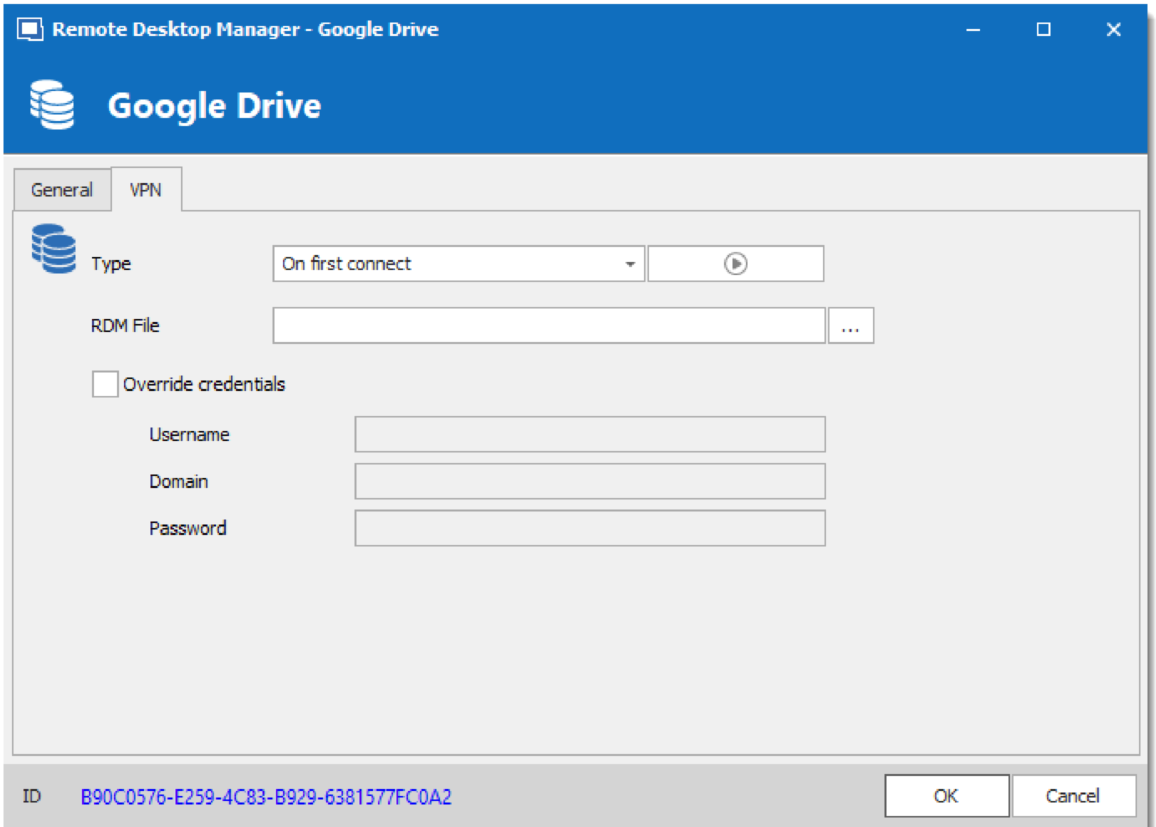
Google Drive - General Tab

OPTION	DESCRIPTION
Name	Enter the name of the data source.
Email	Enter the Google email to access Google Drive.

OPTION	DESCRIPTION
Password	Enter the password of the Google account.
Always ask password	Always ask for the password when connecting to the data source.
Account status	Indicated if the account has been validated with Google Drive. Credentials must be validated before using the data source.
Validate Google Drive	This contextual button attempts validates the credentials currently in use (or removes currently validated credentials).
Master key	Enter the master key of the data source (If enabled).
Always ask master key	Enabling this option will prompt for a master key whenever you are connecting to the data source.
Filename	Enter the Google Drive path of the data source's file.

VPN

Open a VPN to access your data prior to connecting to your **Google Drive**.



Google Drive - VPN Tab

5.4.5 Devolutions Online Drive

DESCRIPTION

The Devolutions Online Drive stores and synchronizes your remote connections and credentials data in our Cloud services. You can access your sessions from anywhere via an Internet connection.

It is an online file storage service dedicated to a single file type, Remote Desktop Manager's connection list. Devolutions Online Drive is completely free and has no limitations as to how many sessions you might have, it is for **single users** as it cannot share files.

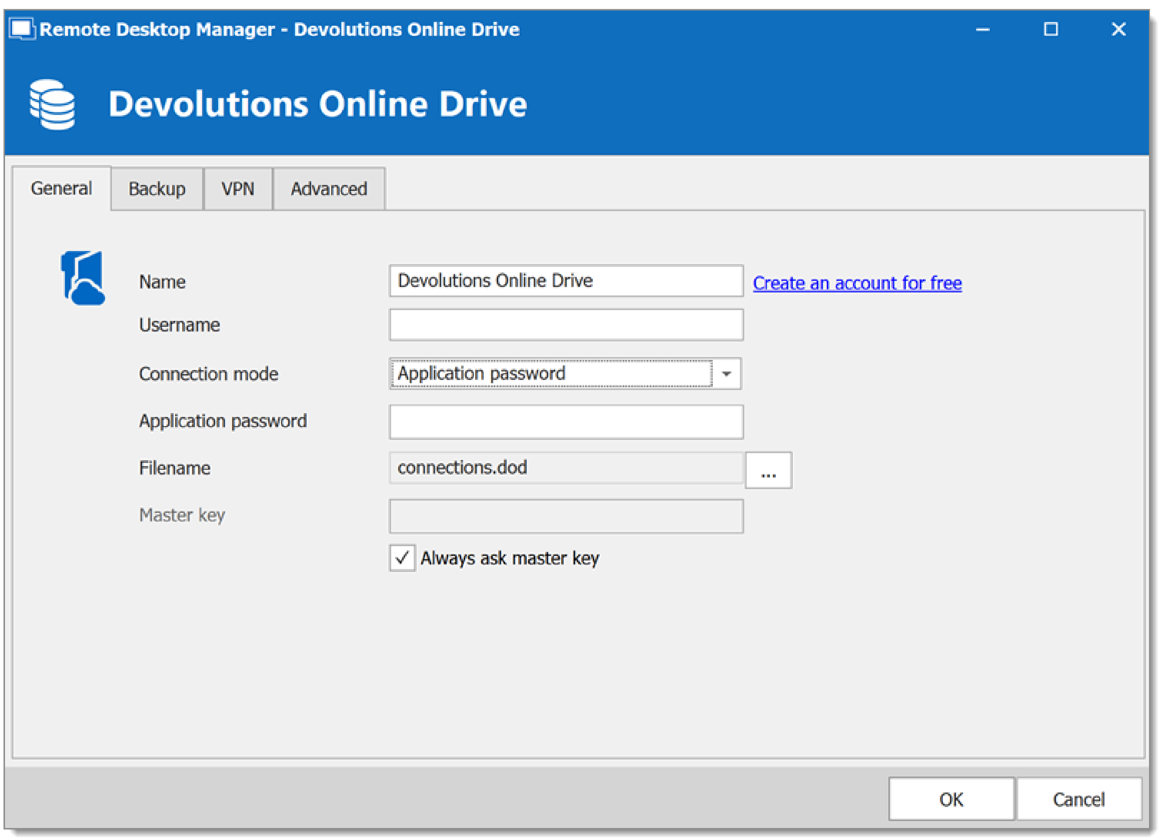
Please consult the Online Drive topic for information on this service.

Since this service is hosted in the cloud, we strongly recommend that you further encrypt your data by applying a Master key. This will ensure that the file will be unreadable by no one but you.

Even though this is a cloud service, you **MUST** use our Online Backup service to keep history of your data. Devolutions offers a free backup service, and we do not maintain multiple versions of the Online Drive content. This makes it critical that you enable the backup feature. This service will keep multiple versions of your file and is the best option.

SETTINGS

GENERAL

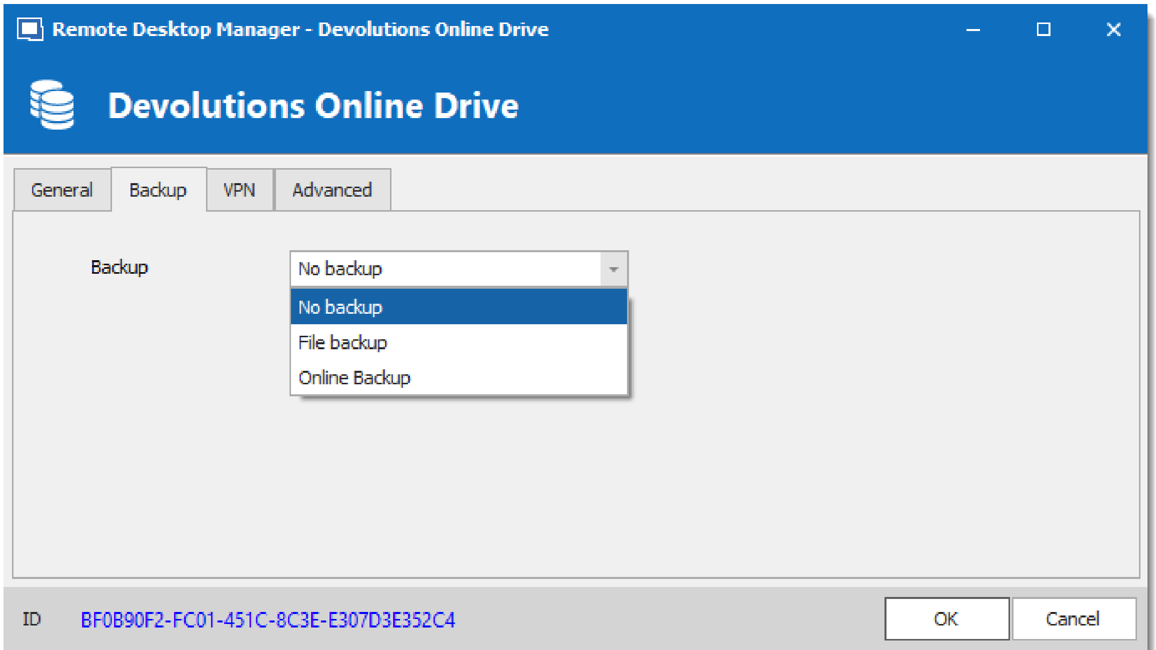


Devolutions Online Drive - General Tab

OPTION	DESCRIPTION
Name	Enter the name of the data source.
Create an account for free	Create a new Devolutions Account.
Username	Enter your Devolutions Account username.
Connection mode	Choose the Default or Application password method.
Application password	Enter your Application password.
Always ask password (default only)	Prompts for the password every time a connection to the Devolutions Online Drive is attempted.
Filename	Indicate the filename used to store the data on the Devolutions Online Drive.
Master key	Contains a master key to access the data source.
Always ask master key	Ask for the master key every time a connection to the Devolutions Online Drive is attempted.

BACKUP

Please consult the Online Backup topic for information on this service.

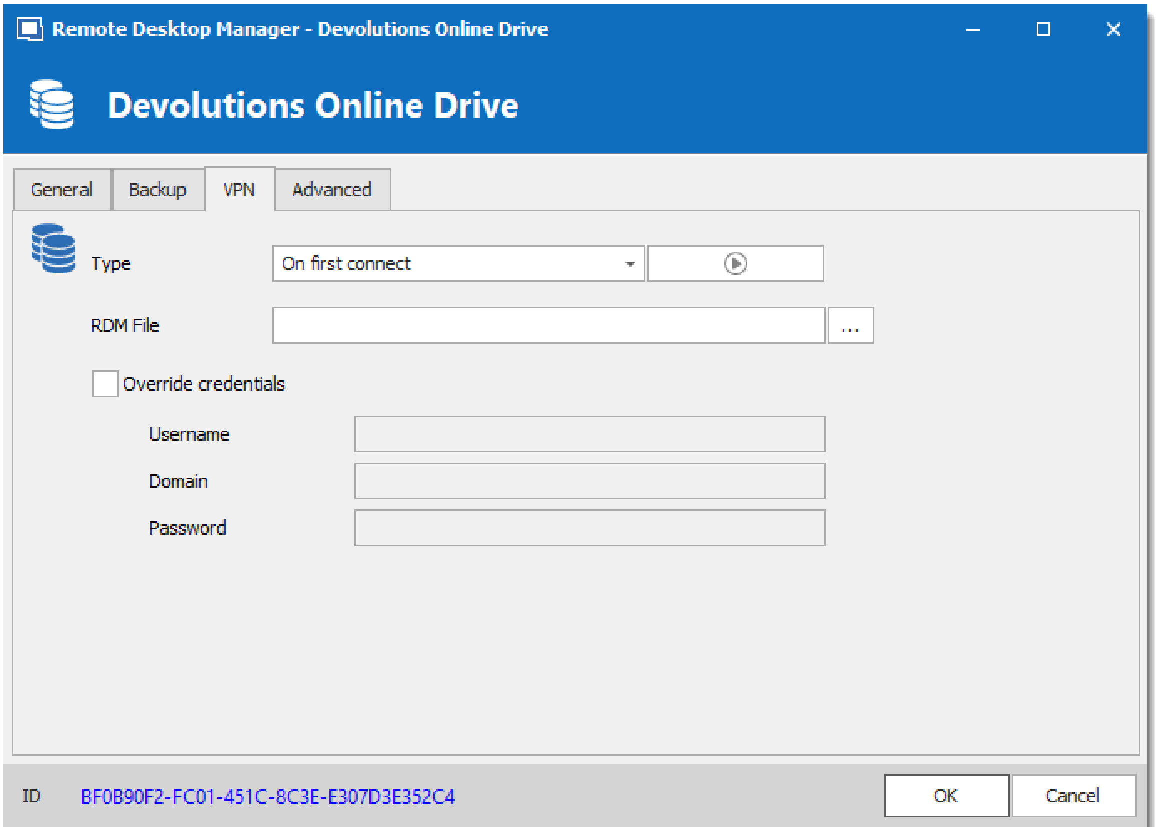


Devolutions Online Drive - Backup Tab

OPTION	DESCRIPTION
Backup	Choose the backup mode. Select between: • **None**: No backup of the data source will be created. • **File backup**: The backup will be saved to a local file when a modification occurs in the data source. • **Online Backup**: An Online Backup (using the Online Backup) will automatically be created when a modification occurs in the data source.

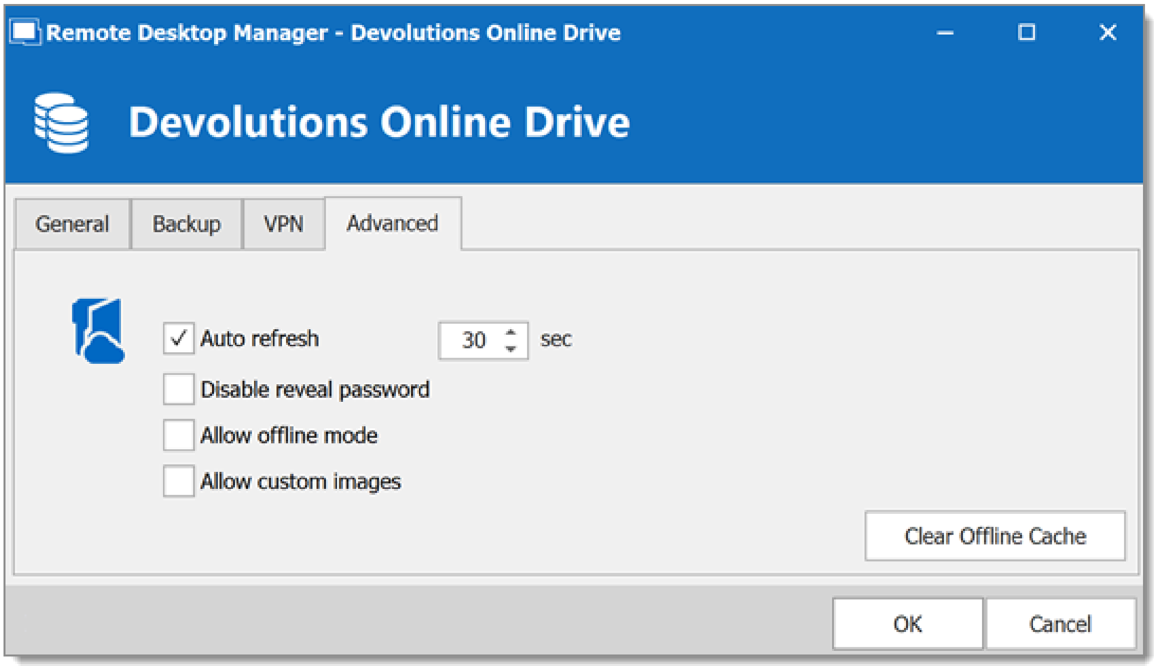
VPN

Open a VPN to access your data prior to connecting to your **Devolutions Online Drive**.



Devolutions Online Drive - VPN Tab

ADVANCED



Devolutions Online Drive - Advanced Tab

OPTION	DESCRIPTION
Auto refresh	Set the interval to use between each automatic refresh.
Disable reveal password	Disable the reveal password feature when a user access the data source.
Allow offline mode	Allows the data source to be used in Offline mode.
Allow custom images	Allows the use of custom images.
Clear Offline Cache	Clear the offline cache on the local computer. This can be very helpful when encountering offline issues.

5.4.6 Password Hub Personal

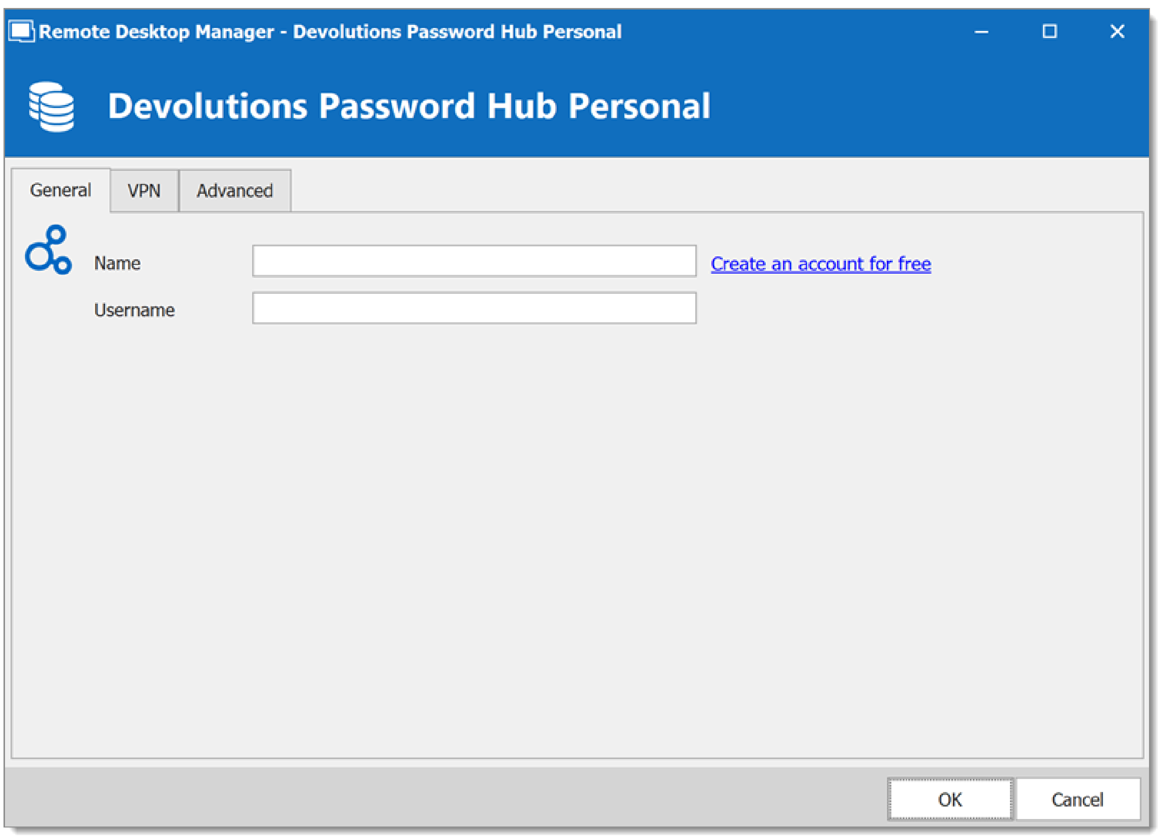
DESCRIPTION

Devolutions Password Hub Personal, for individual users who want to secure personal passwords in a secure vault for free.

Please consult our website for more information on this service.

SETTINGS

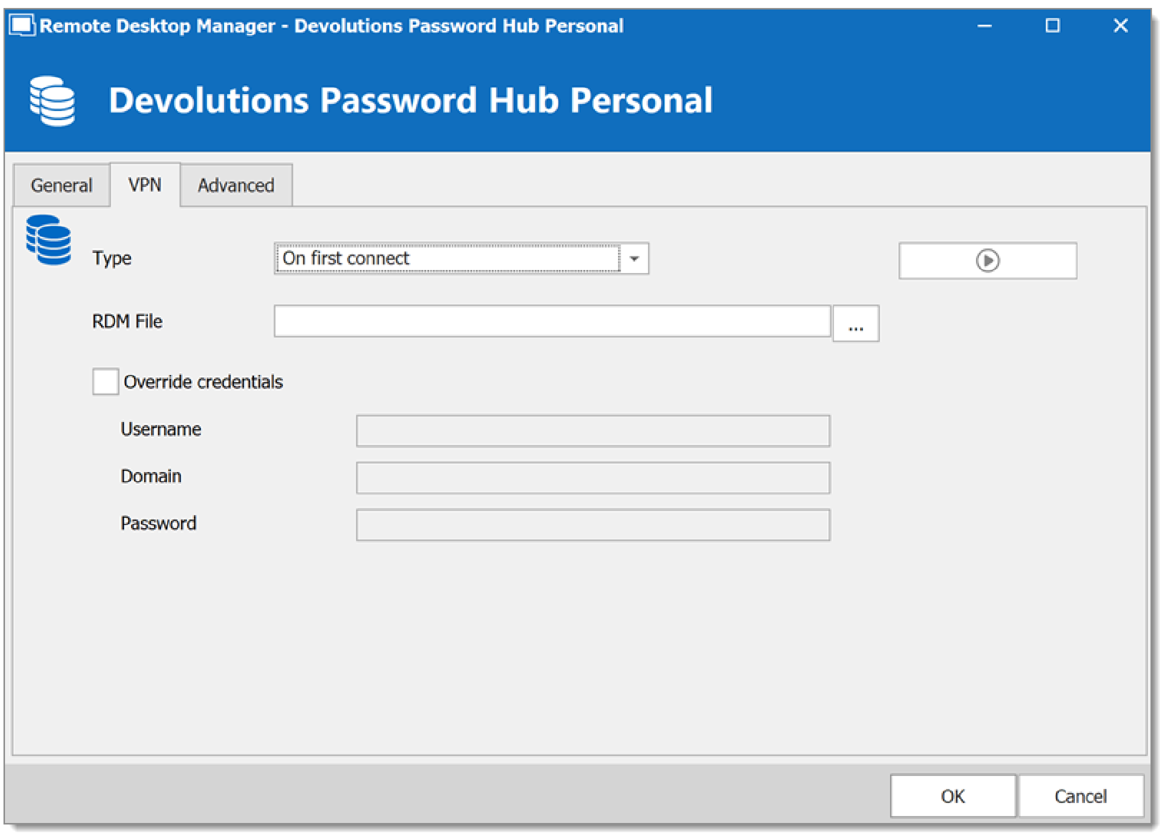
GENERAL



OPTION	DESCRIPTION
Name	Name of the data source.
Username	Your Devolutions Account email address. You can create one for free, just follow the link provided.

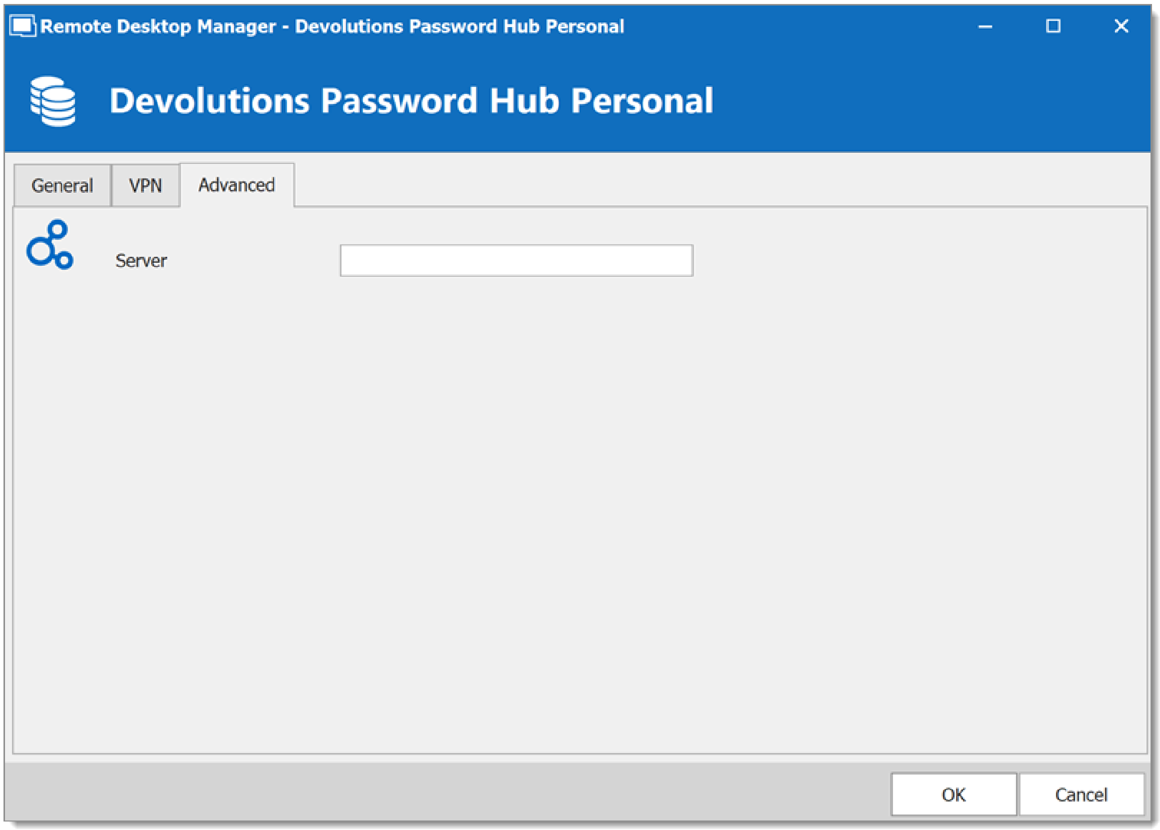
VPN

Open a ***VPN*** to access your data prior to connecting to your Devolutions Password Hub.



ADVANCED

This is the ***Server*** address.



5.4.7 SQLite

DESCRIPTION

Remote Desktop Manager's SQLite data source is ideal for single user and stand-alone situations. More powerful and more flexible than the XML file format, it also supports a few of the Advanced Data Source options like Logs and Attachments.

HIGHLIGHTS

- Full connection log and attachments support
- The Online Backup Service is available for this data source

All passwords are encrypted by default by Remote Desktop Manager. You can specify a custom password to fully encrypt the content of the SQLite database.

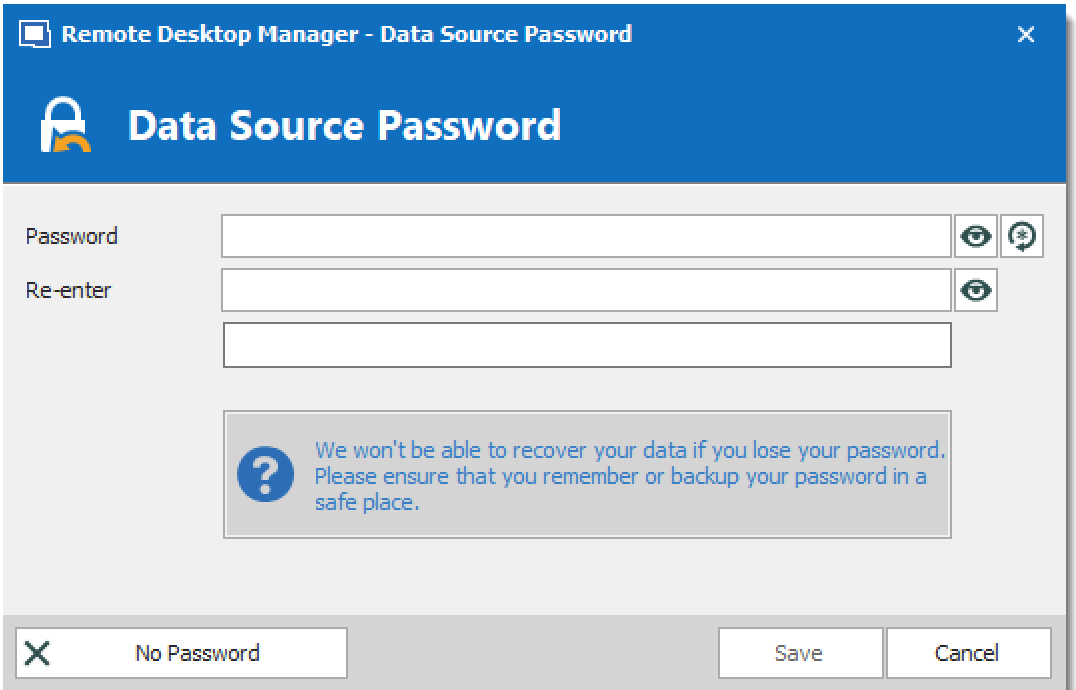
Password recovery is not possible, the data will be unrecoverable if you cannot authenticate. Please ensure you backup the password in a safe place.

SQLite supports an unlimited number of simultaneous readers, but will only allow one writer at any instant in time. For this reason Remote Desktop Manager does not support sharing a SQLite data source between several users by storing it on a network drive. If you want to share your data and work in a team environment with your colleagues, please use one of the Advanced Data Sources. Please consult SQLite.org for more information.

PASSWORD MANAGEMENT

You can specify a password to further encrypt your data. Specify it at creation time. If the data source already exists you can modify the password by using the ***File – Manage Password*** dialog.

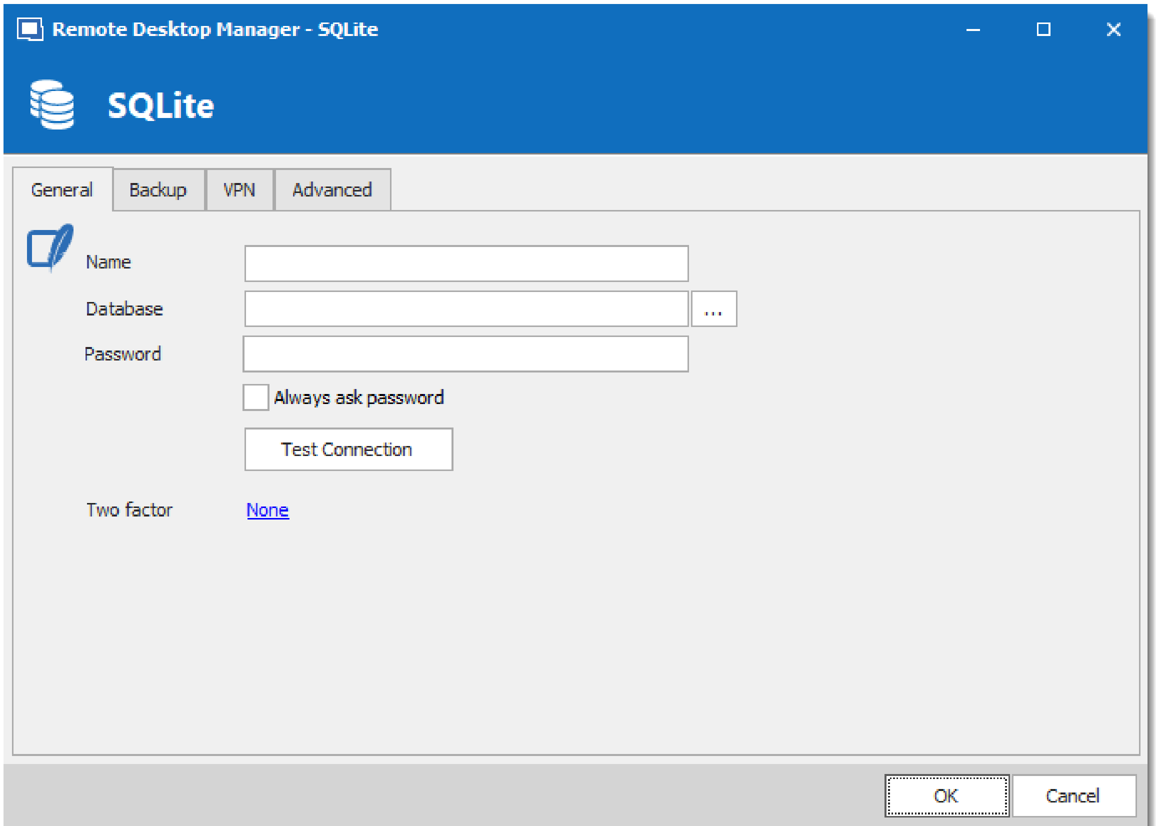
Change or clear the password of a SQLite data source.



Manage password dialog

SETTINGS

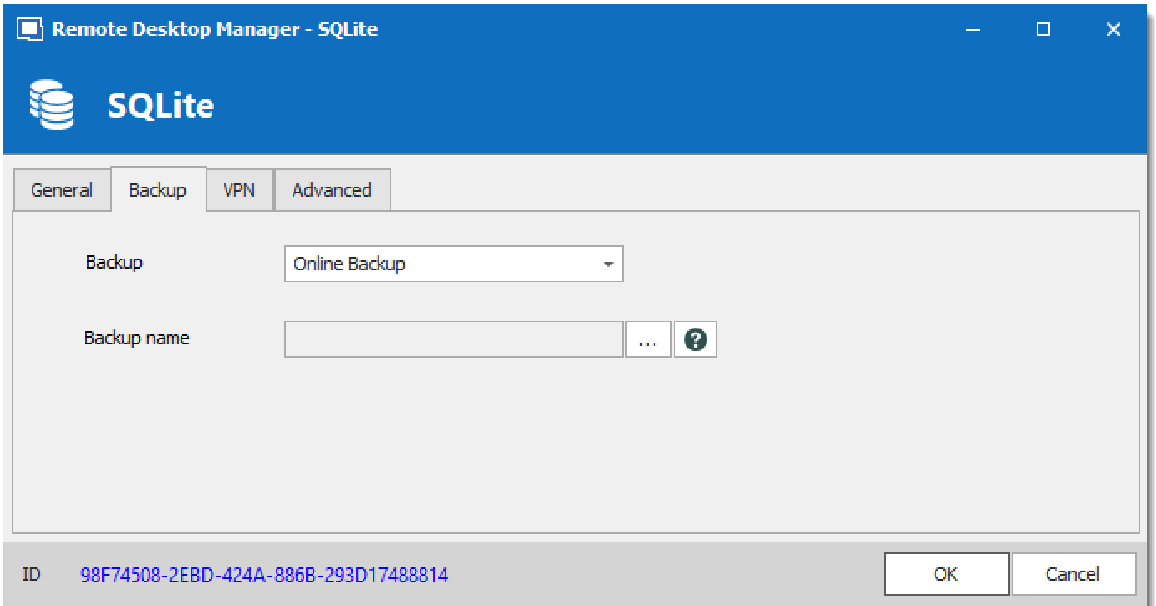
GENERAL



SQLite - General Tab

OPTION	DESCRIPTION
Name	Name of the data source.
Database	Indicates the filename of the SQLite database (.db).
Password	Specify a password to further encrypt your data source.
Always ask password	Always ask for the password when connecting to the data source.
Test Connection	Test the current database path and password for conneciton.
Two factor	Enable the 2-Factor Authentication to access your data source.

BACKUP

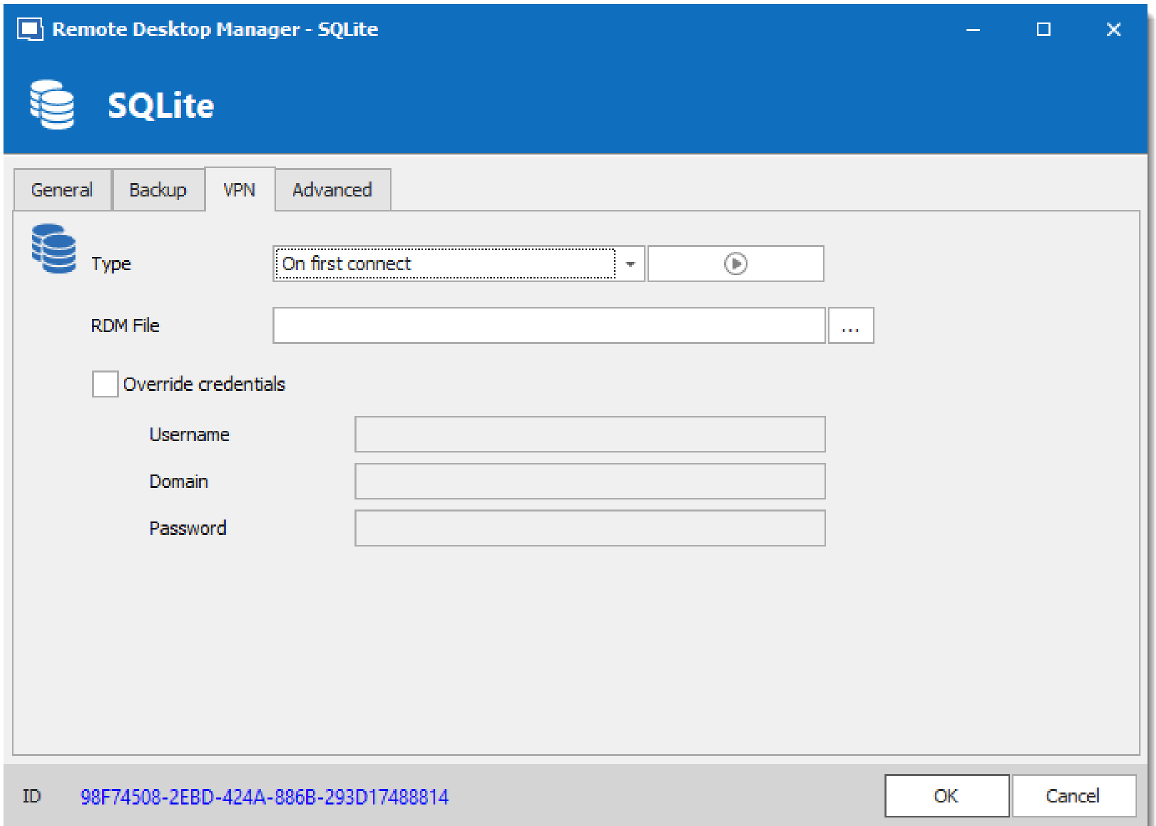


SQLite - Backup Tab

OPTION	DESCRIPTION
Backup	Select between: • **None**: No backup of your data source will be created. • **File backup**: Your backup will be saved to a chosen file but will not automatically do backup every 30 seconds. • **Online Backup**: An Online Backup (using Online Backup) will automatically be created.

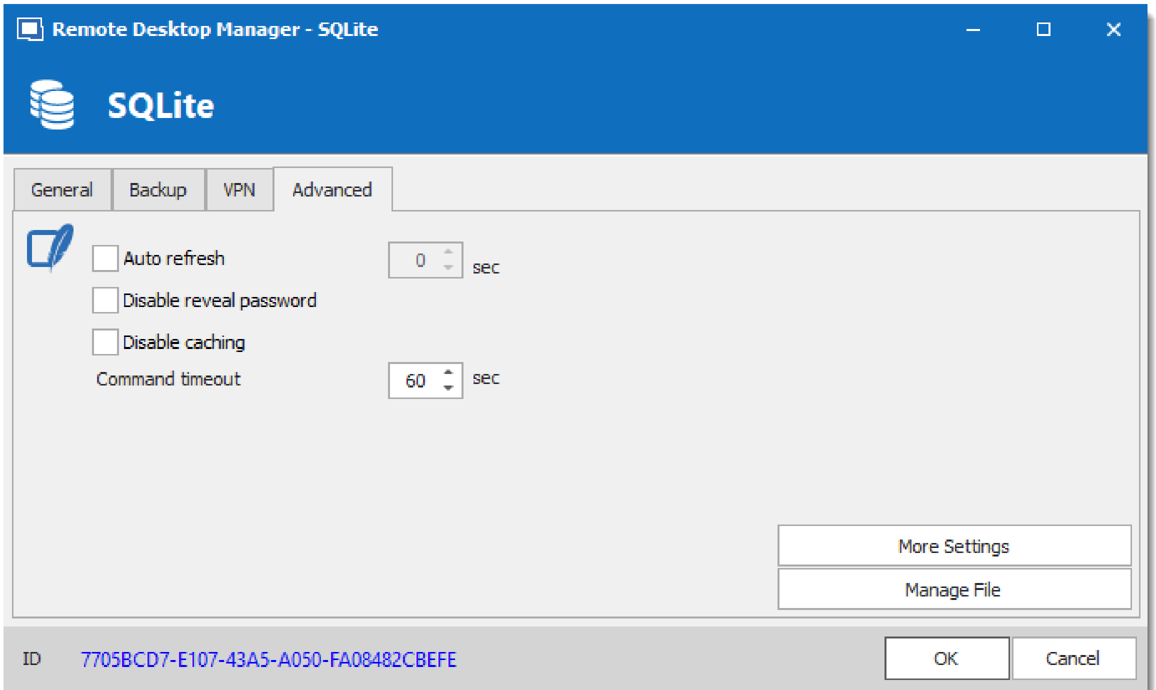
VPN

Open a VPN to access your data prior to connecting to your **SQLite**.



SQLite - VPN Tab

ADVANCED



SQLite - Advanced Tab

OPTION	DESCRIPTION
Auto refresh	Set the interval for the automatic refresh.
Disable reveal password	Disable the reveal password feature when a user access this data source.
Disable caching	Entries will be reloaded in Simple mode in the data source. See Caching topic for more information.
Command timeout	Waiting time before a command timeout.
More Settings	Use to directly modify the connection string value.
Manage File	Contains multiple SQLite commands to facilitate managing. You should usually only access these when our support teams demands it.

5.4.8 XML

DESCRIPTION

Remote Desktop Manager saves the settings directly in an XML file format.

HIGHLIGHTS

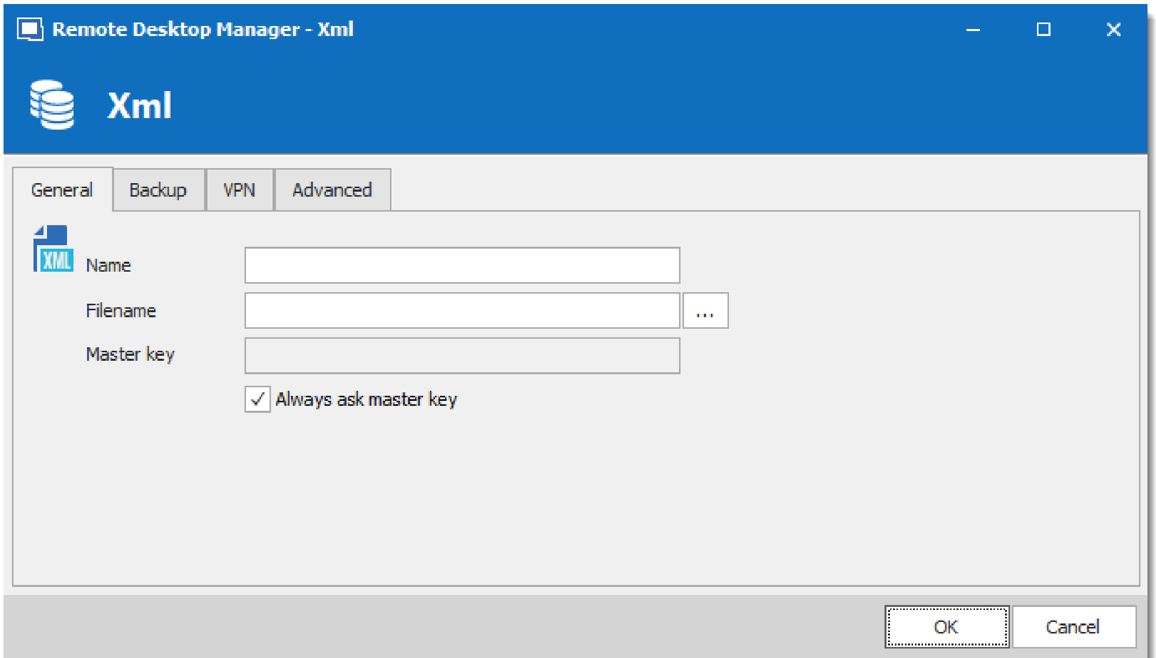
- It is possible to configure an auto refresh interval.
- The Online Backup is available for this data source.

Although it can be shared between multiple locations, there is no conflict management for the configuration. If you share with other users you may get update conflicts or otherwise run into issues. This data source type is meant for a single user using multiple computers, not multiple users.

All passwords are encrypted by default. You can specify a custom password (master key) to fully encrypt the content of the file. It is impossible to recover the data if the master key is lost. Please make sure to remember or backup the master key in a safe place.

SETTINGS

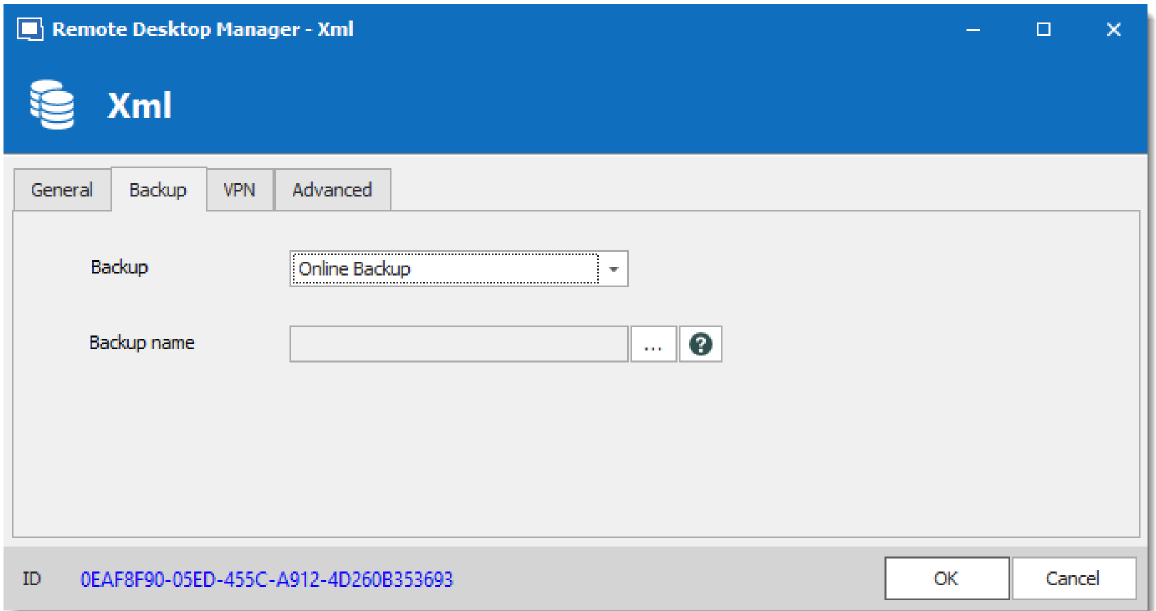
GENERAL



XML - General Tab

OPTION	DESCRIPTION
Name	Name of the data source.
Filename	Specify the full path of the XML file used to save the data. Relative paths and environment variables can be used as well.
Master key	Add an additional layer of security by encrypting your data source with a master key.
Always ask master key	Always prompts for the master key when connecting to the data source.

BACKUP

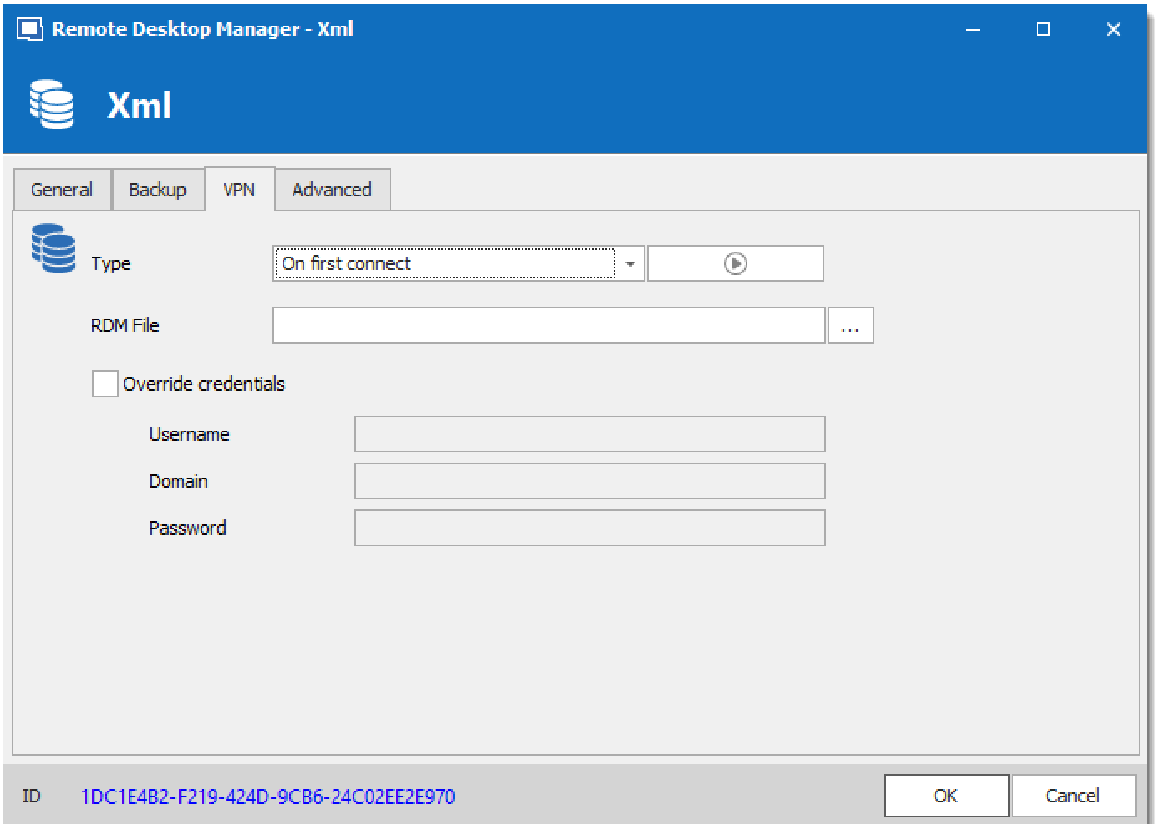


XML - Backup Tab

OPTION	DESCRIPTION
Backup	Select between: • **None**: No backup of your data source will be created. • **File backup**: Your backup will be saved to a chosen file but will not automatically do backup every 30 seconds. • **Online Backup**: An Online Backup (using Online Backup) will automatically be created.
Backup name	Specify the backup name that will allow you to automatically save your sessions in a safe online storage space and restore them in the event of problems.

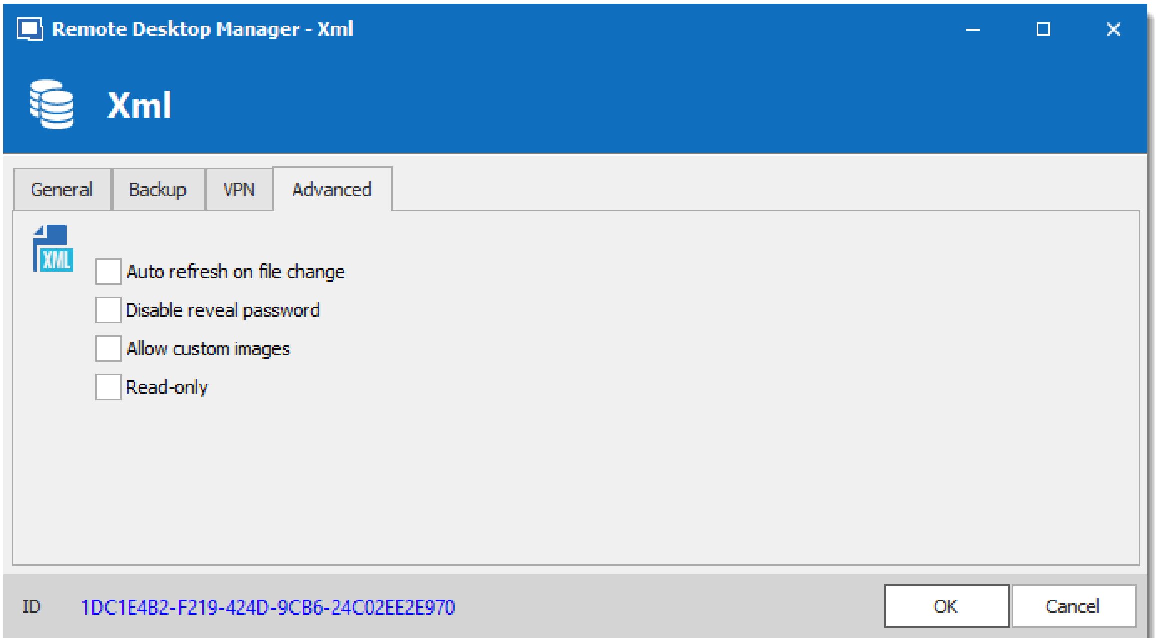
VPN

Open a VPN to access your data prior to connecting to your **XML**.



XML - VPN Tab

ADVANCED



XML - Advanced Tab

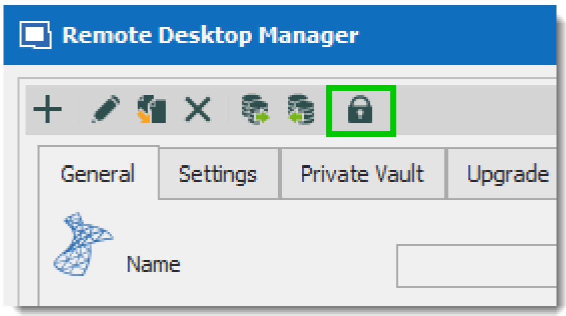
OPTION	DESCRIPTION
Auto refresh on file change	Indicate if the application monitor the file changes to automatically refresh the data source.
Disable reveal password	Disable the reveal password feature when a user accesses this data source.
Allow custom images	This will enable the loading of any custom images in the tree view.
Read-only	Set the data source in read only. No new entry can be created and the existing data cannot be edit.

5.5 Lock Data Source

LOCK DATA SOURCE

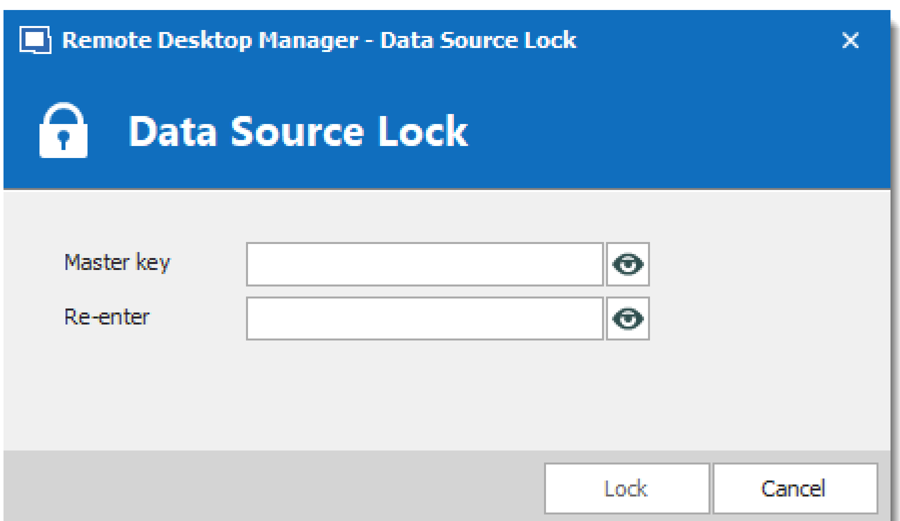
To protect sensitive data in your data source configuration (e.g. server URL or credentials), you may wish to lock the data source configuration before you deploy it to your users. You can do it by using the Lock/Unlock button from the toolbar.

SETTINGS



Lock Data Source toolbar

The locked data source will require a password. The password must be specify when the lock is applied. Use the same password to unlock it or to modify the data source configuration.



Lock Data Source dialog

There is **NO way** of unlocking the data source if the password is lost or forgotten. In such an event, you will need to configure a new data source. However the content of the database will not be lost.

5.6 Offline mode

DESCRIPTION

The offline mode connects to a local copy of the data source when you are not connected to the data source. This is useful when working from a remote location and the network is unreachable or if there is any kind of connectivity issue.

The read/write offline mode adds to users the possibility to manipulate entries while disconnected from the data source. This is useful for off-site personnel or when working in environments that have sporadic network availability.

> This feature is not available for all data sources, please consult the help topic of the respective data source to know if it supports offline mode.

> The offline cache is first encrypted using our own private key mixed with some information taken from the local computer. This makes it impossible for a copy on another machine to be readable. By default it is also encrypted with Windows NTFS encryption, in which case there is no key saved anywhere.

For added security, offline files are set to expire after a delay. The default expiry is set to 7 days but can be modified via the System Settings.

Remote Desktop Manager will prompt for offline mode when the application is unable to reach the data source but the offline mode can be toggled manually with ***File – Go Offline***.

Several features are not available in offline mode, such as:

- Attachments and logs.
- User management (Add/Edit/Delete users).

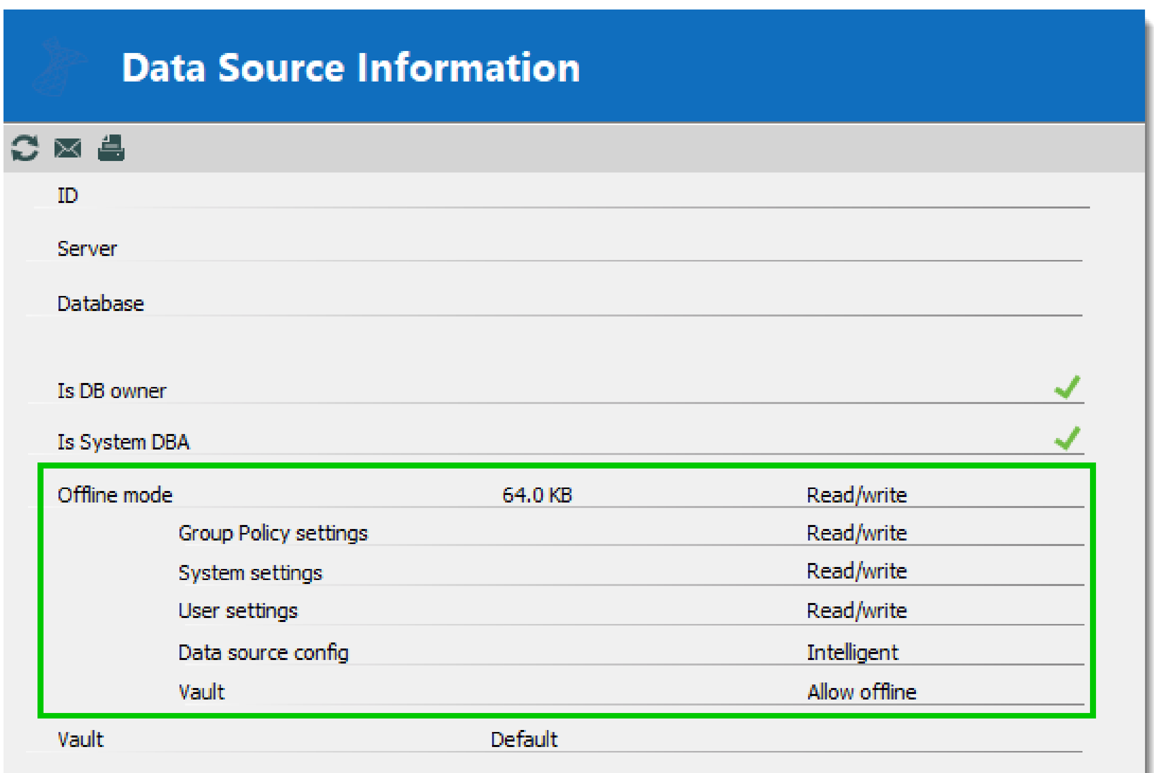
AVAILABILITY

The offline mode availability relies on several settings:

- The data source offline cache must be enabled in ***File - Data Sources - Advanced - Caching Mode - Intelligent***. (This step needs to be done before you export your data source to other computers)
- The user's account must be enabled in ***Administration - Users - Edit - Settings - Offline mode***.
- The user groups policies (only for the DVLS data source) in ***Administration - User groups - Edit - Settings - Offline mode***.
- The data source System Settings in ***Administration - System Settings - Offline - Offline mode*** and ***Expiration***.
- For each Vault ***Administration - Vault Settings - Security Settings - Allow offline***.

The lowest setting (in terms of security) prevails over the others, which may prevent you from using the offline mode. If the **Go Offline** button is not available, please consult your administrator.

The Data Source Information displays the size of the offline cache file along with the effective modes (disabled, read-only or read/write).

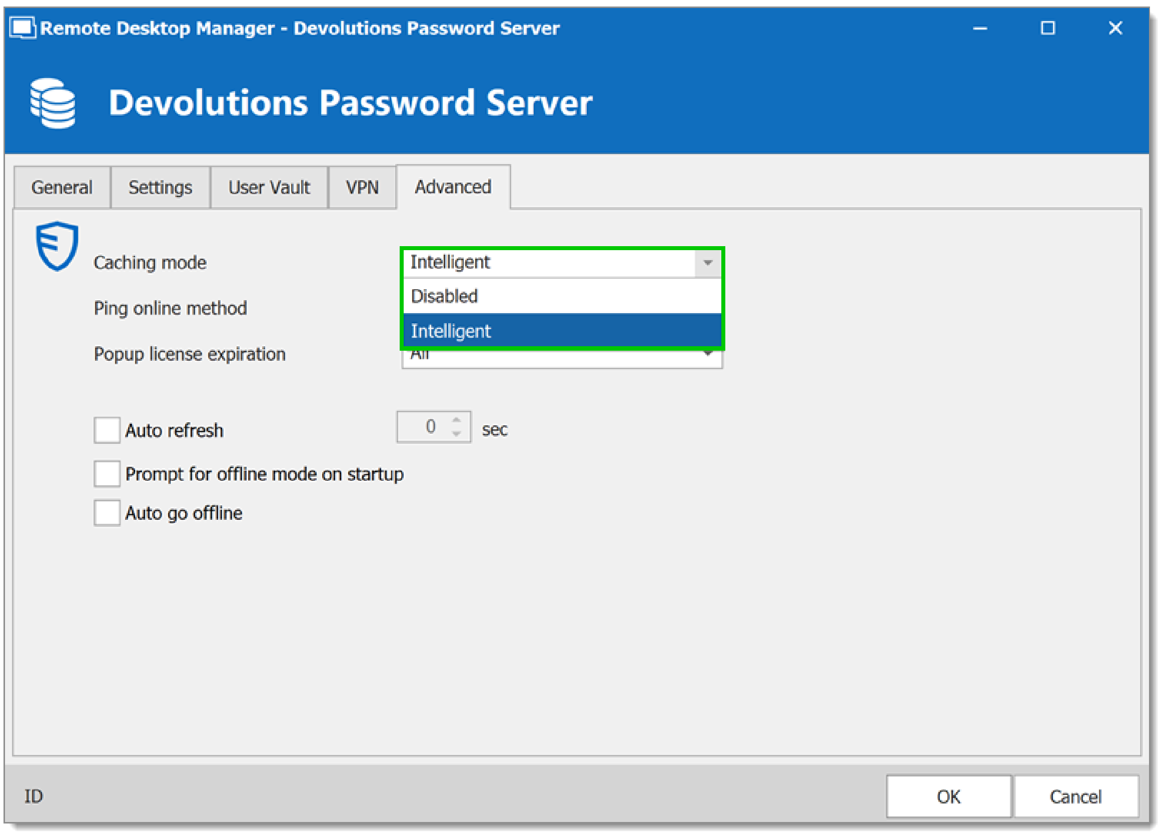


My Data Source Information - Offline mode

CACHING MODE

The caching mode must be set to **Intelligent** to enable the offline mode.

> This step cannot be modified remotely once you have exported your data source settings. You should take a moment and think about the needs of your data source and select what is appropriate before moving on to exporting.



Data Source configuration – Advanced – Caching mode

OPTION	DESCRIPTION
Disabled	Prevent an offline cache from being used.
Intelligent	Use the offline cache only for recent changes.

Some features of Remote Desktop Manager are unavailable while offline. Even with read/write access mode, you may not be able to perform all actions, such as adding attachments or managing users since these features are not cached locally. On the other hand, note that the User Vault is still available in offline mode.

GRANT/DENY OFFLINE

OPTION	DESCRIPTION
Disabled	Prevents an offline cache from being used.
Read-only	Allow to view and use entries only. The content of the data source cannot be modified.
Read/Write	Allow to view, use, and edit entries. Conflicts caused by offline modifications are managed when back online.

Beyond the group policies, the Offline mode is controlled on multiple levels:

- User permissions.
- System Settings.
- In a Vault's setting.

A user must be granted Read/Write at all levels to allow read/write privileges.

USER PERMISSIONS	SYSTEM SETTINGS	Vault SETTINGS	EFFECTIVE ACCESS
Disabled or Read-only or Read/write	Disabled or Read-only or Read/write	**Allow offline disabled**	**Disabled**

USER PERMISSIONS	SYSTEM SETTINGS	Vault SETTINGS	EFFECTIVE ACCESS
Disabled or Read-only or Read/write	Disabled or Read-only or Read/write	Allow offline enabled	**Disabled**
Disabled or Read-only or Read/write	**Disabled**	Allow offline enabled	**Disabled**
Disabled	Disabled or Read-only or Read/write	Allow offline enabled	**Disabled**
Read-only or Read/write	Read-only or Read/write	**Allow offline disabled**	**Disabled**
Read-only or Read/write	Read-only or Read/write	Allow offline enabled	**Read-only**
Read-only or Read/write	**Read-only**	Allow offline enabled	**Read-only**
Read-only	Read-only or Read/write	Allow offline enabled	**Read-only**
Read/write	**Read/write**	**Allow offline enabled**	**Read/write**

You want to know the current effective Offline mode while connected? See My Data Source Information.

5.6.1 Offline Read/Write

DESCRIPTION

The **Read/Write** offline mode allows the user to add, edit and delete entries while the data source is offline. Those changes are saved locally and synchronized with the data source once it is back online.

Some functionalities are not available while offline and you may not be able to perform all actions. Note that the User Vault is still available in offline mode.

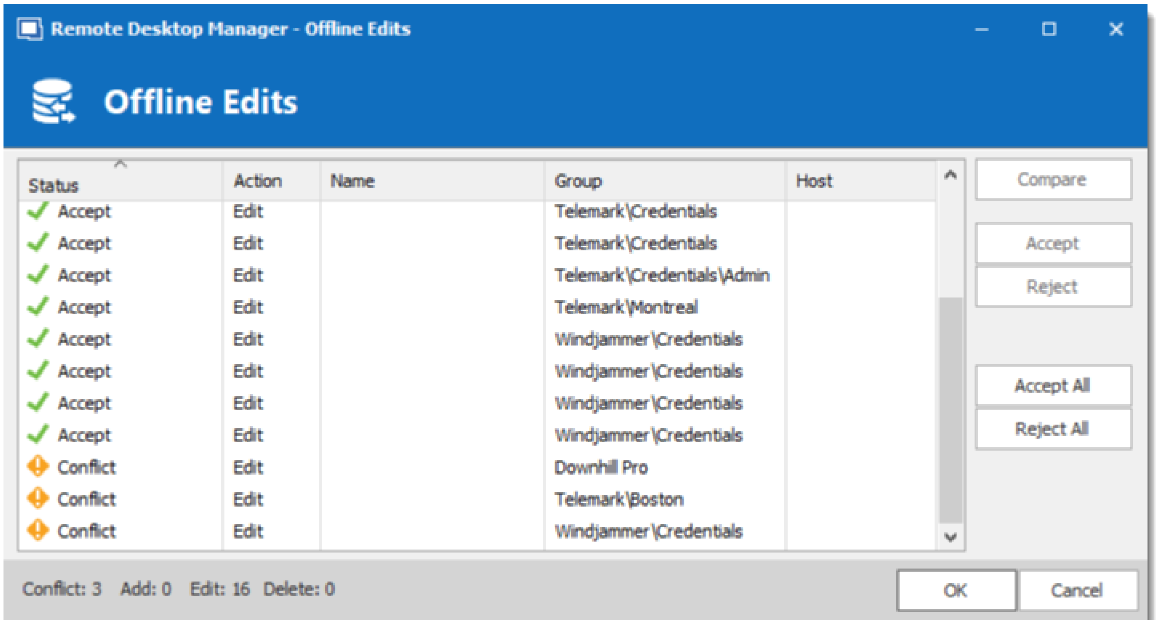
Once offline, the users security settings still applies. Add/Edit/Delete privileges granted by the administrator are still in effect. See User Management.

When an entry is edited by an online user while another user is offline, the local version of the entry stored in the offline cache becomes different from the online version. This causes a conflict when the offline user gets back online.

OFFLINE EDITS WORKFLOW

- Connect to the data source.
- Go offline with File – Go Offline.
- Edit any entry.
- Go back online with File – Go Online.

The **Offline Edits** window is displayed:



Offline Edits

Use this dialog to accept/reject your offline changes.

You can use the **Compare** action to have a side by side comparison of your changes with the current live entry.

Entries will be marked:

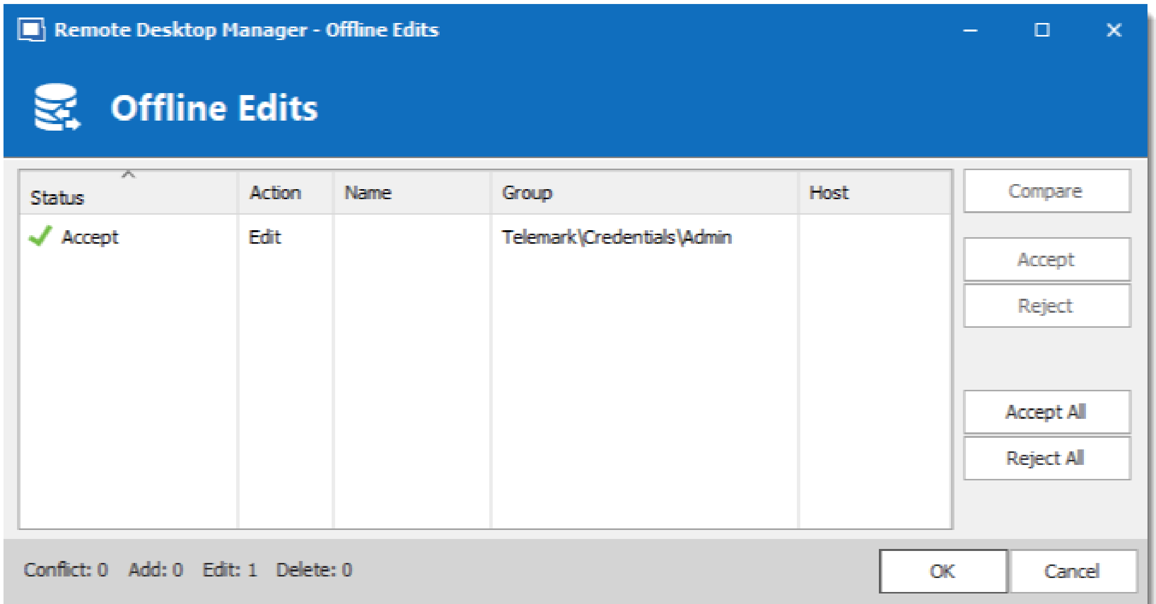
- Accept - when no outside changes have been detected.
- Conflict - when outside changes have been detected since you were last connected.

MULTIPLE OFFLINE EDITS

When multiple users edit the same entry offline simultaneously, a conflict occurs when the second user is back online.

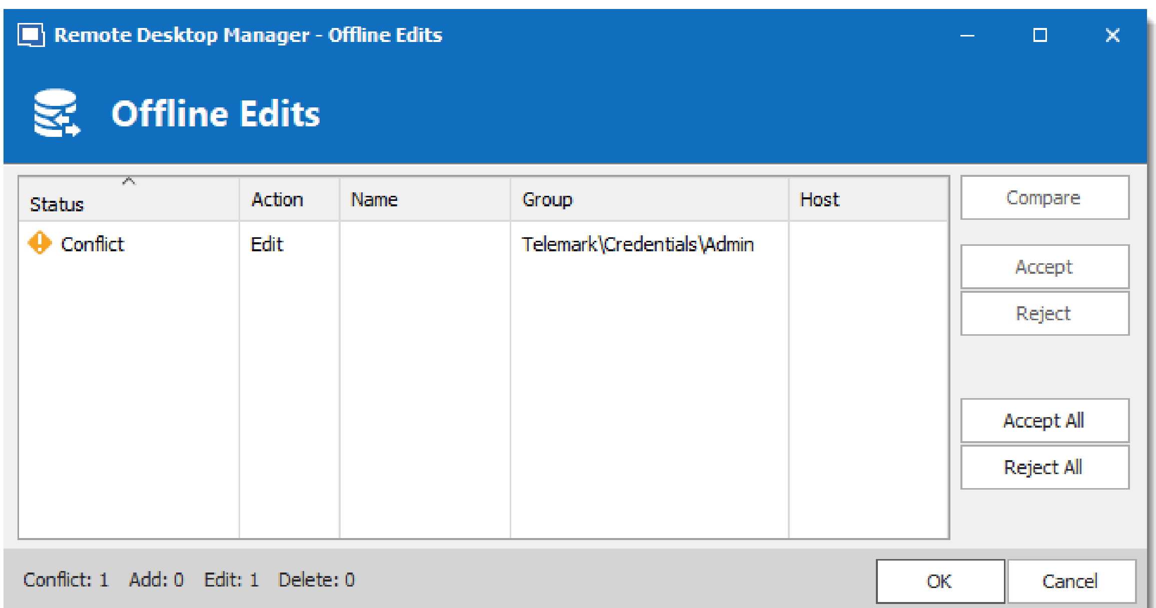
Here is an example of such a case to help resolving conflicts properly:

When the first user returns online, the **Offline Edits** window is displayed. Changes are accepted by default.



Offline Edits For The First User Back Online

When a second user returns online, a conflict occurs and the **Offline Edits** window is displayed.



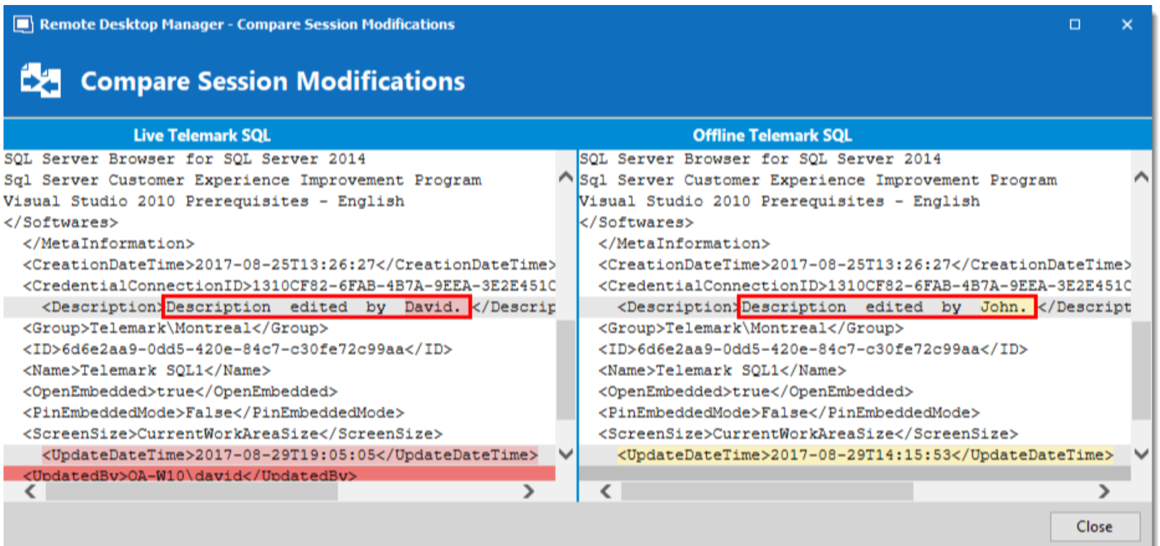
Offline Edits For The Second User Back Online

When the conflict occurs, the user must decide to accept or reject the changes. The different versions of the entry can be compared to view which changes has been made.

COMPARE VERSIONS OF AN ENTRY

Click the **Compare** button to compare the versions of a conflicted entry. Analyze the XML structure of the entry to decide to **Accept** or **Reject** the changes.

The content on the left represents the entry retrieved online, and the content on the right represents the local version of the entry, edited in Offline mode.



Compare Session Modification

5.7 Manage Cache

DESCRIPTION

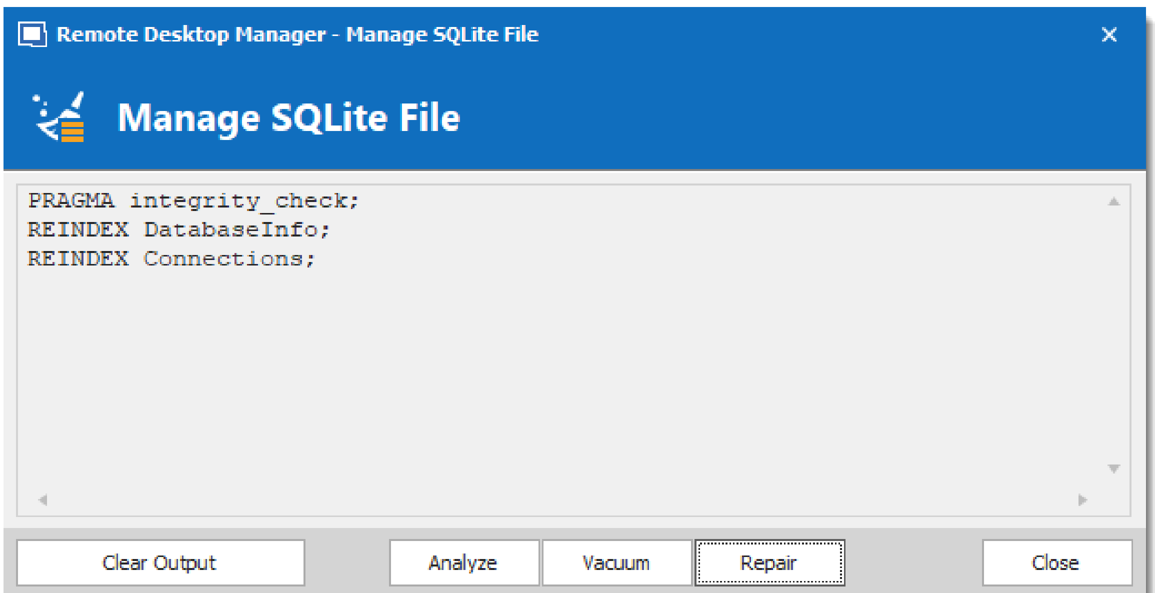
This option allows you to manage your cache which decides how the client will re-load entries when changes are detected. On large data sources caching is a must and will increase performance significantly.

> This feature is only available when the offline engine is set to use SQLite. We are phasing out this engine because of multiple issues reported by customers. We recommend you use **MCDFv2**.

The Manage Cache options should usually only be used **upon request from our Support Team** when experiencing cache issue.

SETTINGS

The Manage Cache options will only be available when using an SQLite cache.



Manage Cache

OPTION	DESCRIPTION
Clear output	Clear the output window.
Analyze	Analyze will generate a report of everything that is contained in the cache. It will read the offline data and perform a read/write test to verify if the offline file is valid.

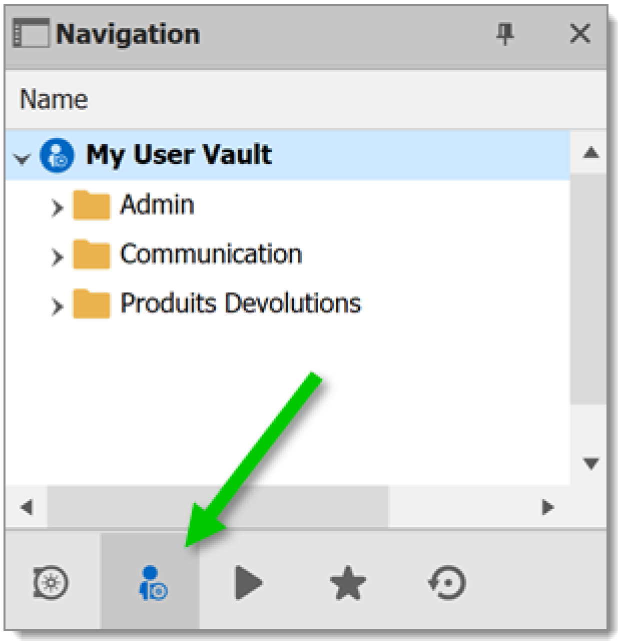
OPTION	DESCRIPTION
Vacuum	This will run an SQLite command to reduce your cache size. The Vacuum should only be used **after trying to execute a Repair** of your cache. If the repair hasn't solved your issue running a Vacuum will usually solve issues when dealing with a corrupted cache.
Repair	The repair will run four different SQLite commands to repair a corrupted cache: ▪ PRAGMA integrigy_check ▪ REINDEX DatabaseInfo ▪ REINDEX Connections ▪ REINDEX Properties

5.8 User Vault

DESCRIPTION

The **User Vault** is a user centric Vault for entries of any type. It allows each user to create entries that only them can access.

The User Vault is available for all Advanced Data Sources.



Navigation Pane – User Vault

A NOTE ON CREDENTIALS

Credentials in the User Vault can be used in two ways:

1. From a session using the **User Vault search**.
2. When using the **User Specific Settings** feature.

These restrictions can easily be understood when you keep in mind that the User Vault is in fact contained in the user area of the database. It must be used from within the User Vault, or by using our extension mechanism that is user specific.

Commands

Part

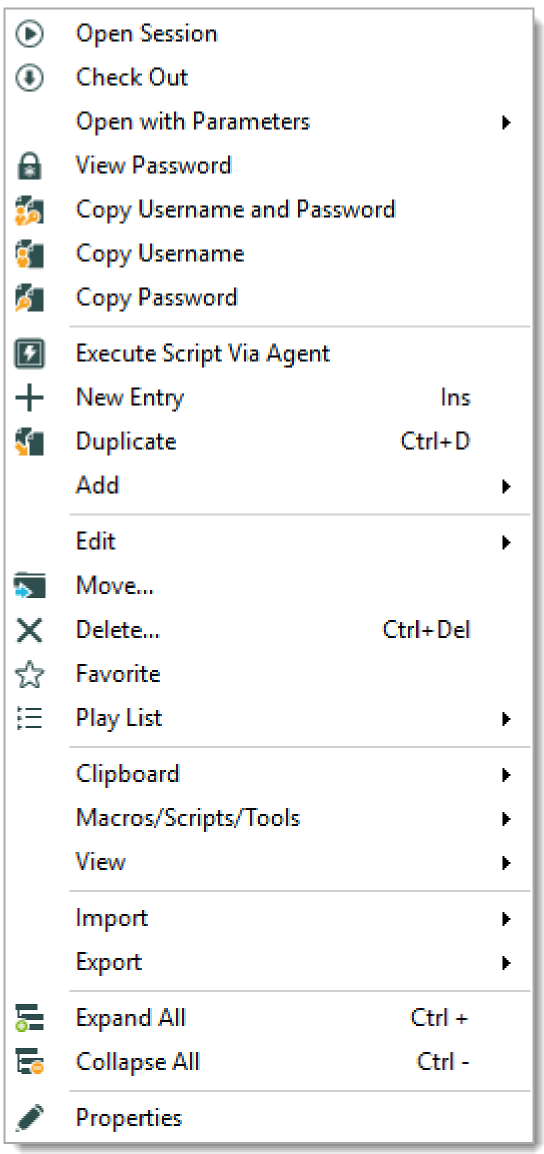
VI

6 Commands

6.1 Context Menu

DESCRIPTION

The **Context Menu** contains several entry-specific actions. The available actions depend on which type of entry is selected. Right click on an entry to display the context menu.

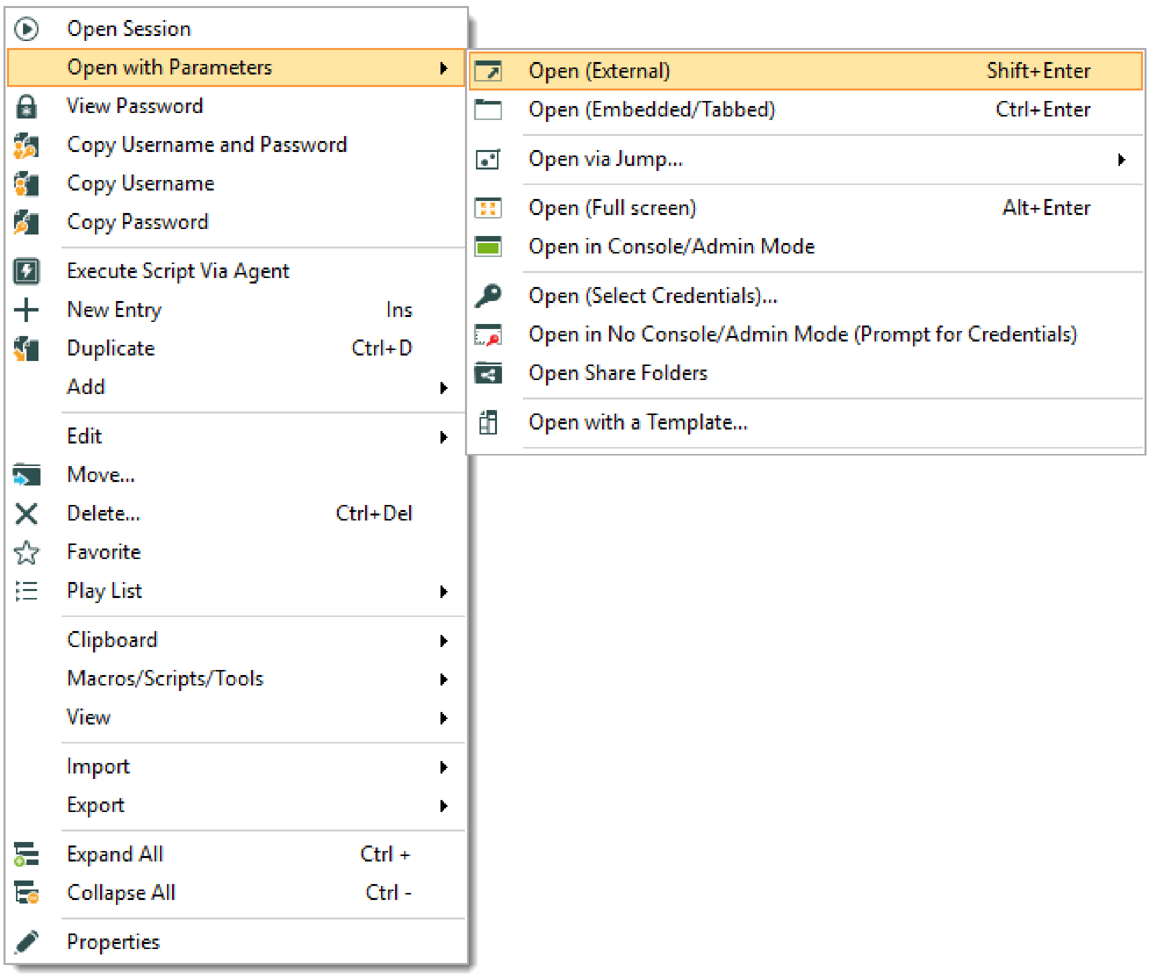


Context Menu

6.1.1 Open with Parameters

DESCRIPTION

The **Open with Parameters** menu all options available to open a session.



Open with Parameters

OPTION	DESCRIPTION
Open (External)	Open a session as an external process, with no direct link to Remote Desktop Manager.

OPTION	DESCRIPTION
Open (Embedded/Tabbed)	Open the session within the confines of the Remote Desktop Manager dashboard and display tabs at the top of the window.
Open via Jump...	Open the session through a Jump host.
Open (Full Screen)	Open the session with the full screen display mode.
Open in Console/Admin Mode	Connect to the console session of a server using Remote Desktop for Administration.
Open (Select Credentials)...	Prompts you with the list of the credentials link to your Data Source to allow you to chose the one needed to open your session.
Open in No Console/Admin Mode **(Prompt for Credentials)**	Open your session normally and prompt your for your credentials to connect.
Open Share Folders	Open the shared folders of the remote computer.
Open with a Template...	Open from a template that you have already created.
VPN	Select between: • **Open (Without VPN).** • **Open VPN Only.** • **Close VPN Only.**

6.1.2 Documentation

DESCRIPTION

The ***Documentation*** feature allows for storing information about resources in the data source. To access an entry's documentation, select an entry in the Navigation Pane, then select the ***Documentation*** tab in the dashboard. Alternatively, right-click an entry in the Navigation Pane, then select ***View – Documentation***.

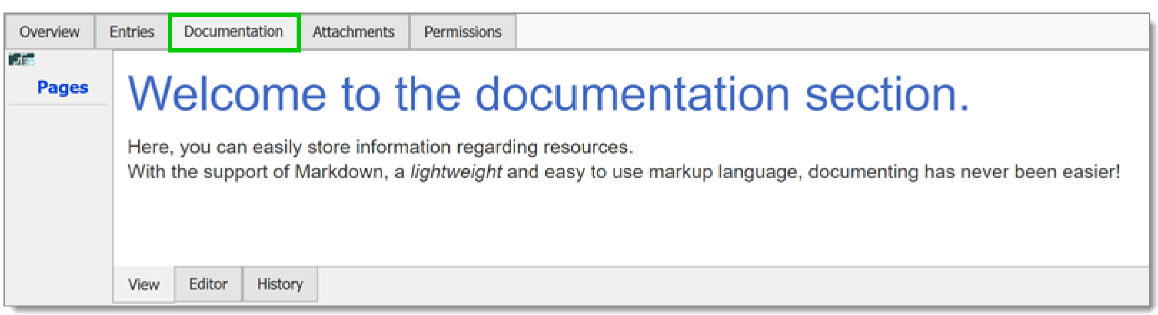
The documentation is written using Markdown, a plain text formatting syntax.

This feature is available with Devolutions Server and SQL Server data sources.

The ***Documentation*** feature is encrypted **only** for the data source Devolutions Server. If you are using data sources like SQL Server or Azure SQL, the ***Documentation*** feature is **not** encrypted.

The feature for using ***Documentation*** in offline mode is available for documents that are stored in the database.

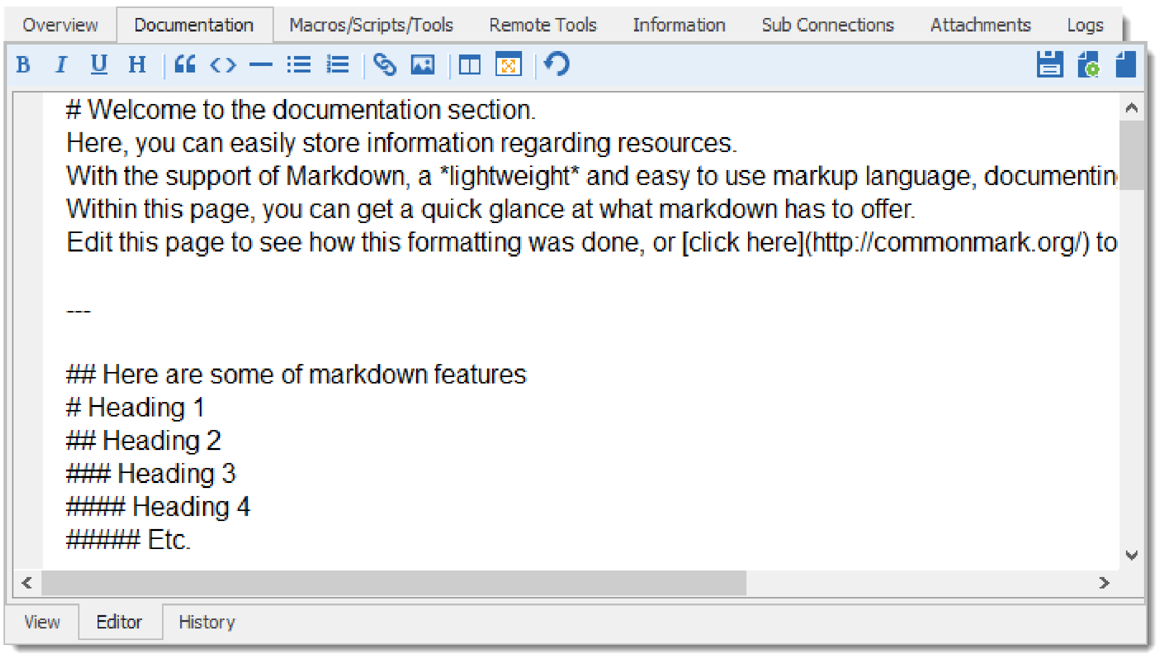
Enable the ***Synchronize document to offline*** in the ***Security Settings***. This property is set to be inherited by default.



6.1.2.1 Editor

DESCRIPTION

The documentation editor is a simple plain text editor. The text is formatted using the Markdown text formatting syntax. Markdown is a markup language designed to be as easy-to-read and easy-to-write as possible.



Documentation editor

MARKDOWN FORMATTING TAGS

- Paragraphs
- Emphasis
- Headers
- Lists
- Horizontal rulers
- Links
- Images

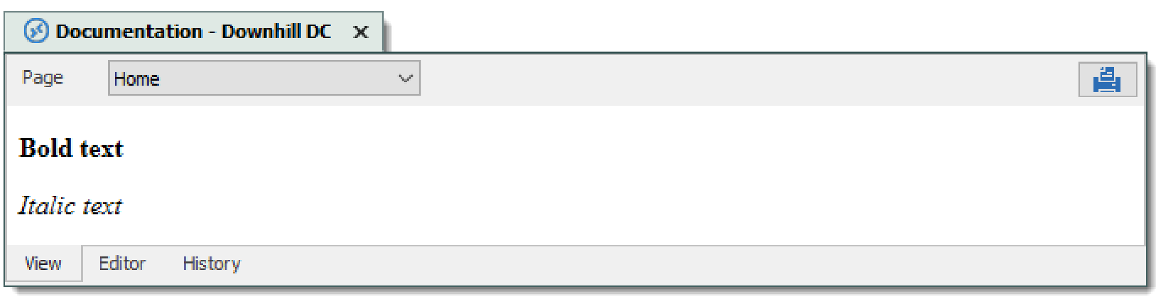
- [Blockquotes]
- [Code examples]

PARAGRAPHS

A paragraph is one or more consecutive lines. Normal paragraphs should not be indented with spaces or tabs.

EMPHASIS

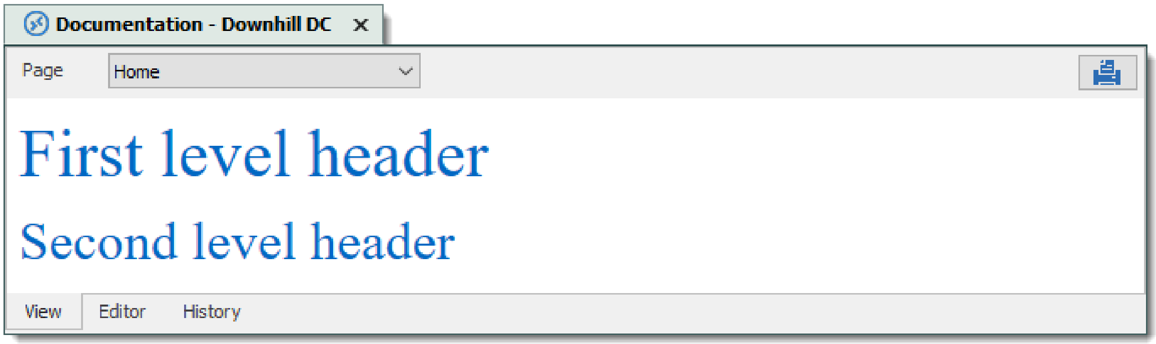
Two methods of text emphasis are available:
```
**Bold text**

*Italic text*
```
Output:



HEADERS

There are two ways of creating headers with Markdown.

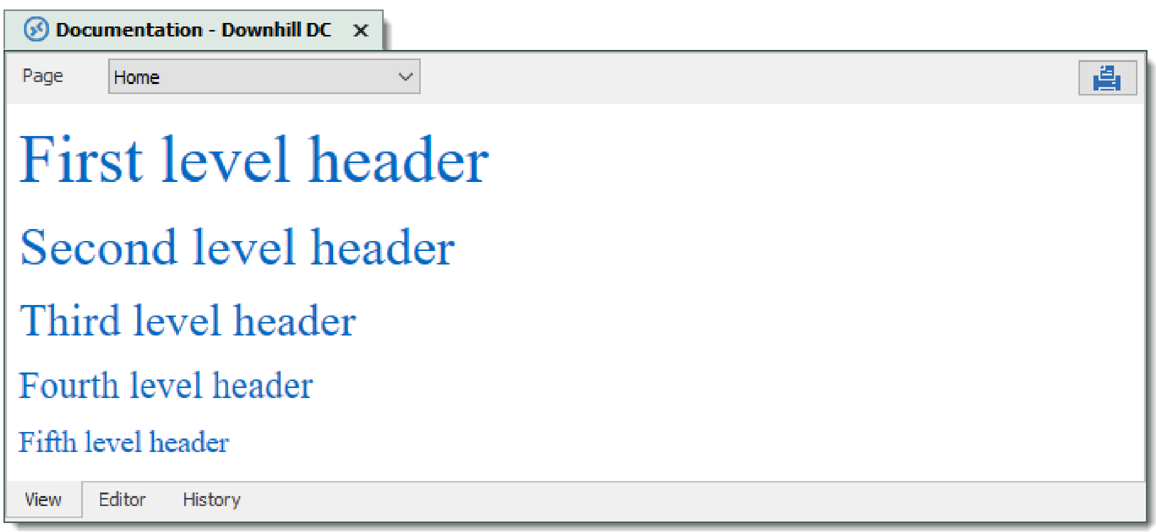
First and second level can be created by "underlining" the text with equal signs (=) and hyhens (-).
```
First level header
==================

Second level header
-------------------
```
Output:



More levels of headers can be created by using one to five hash symbol (#) at the beginning of the line.

```
# First level header

## Second level header

### Third level header

#### Fourth level header

##### Fifth level header
```

Output:



LISTS

Use asterisks, pluses, and hyphens to create an unordered bulleted list. These three markers are interchangable.

```
* Item 1
* Item 2
* Item 3
```

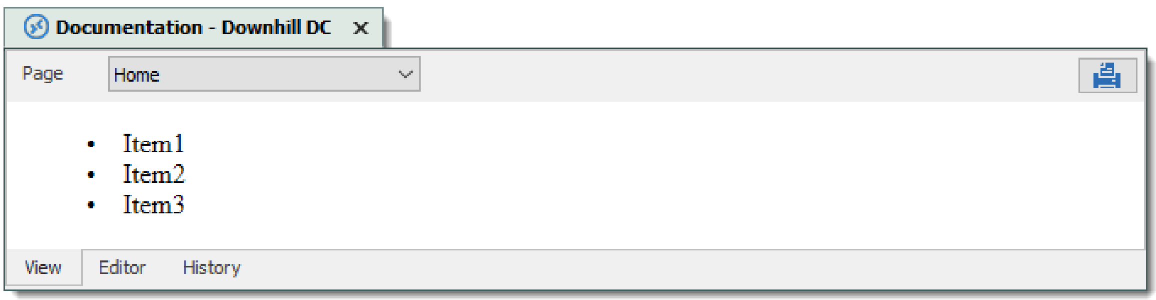
or

```
+ Item 1
+ Item 2
+ Item 3
```

or

```
- Item 1
- Item 2
- Item 3
```

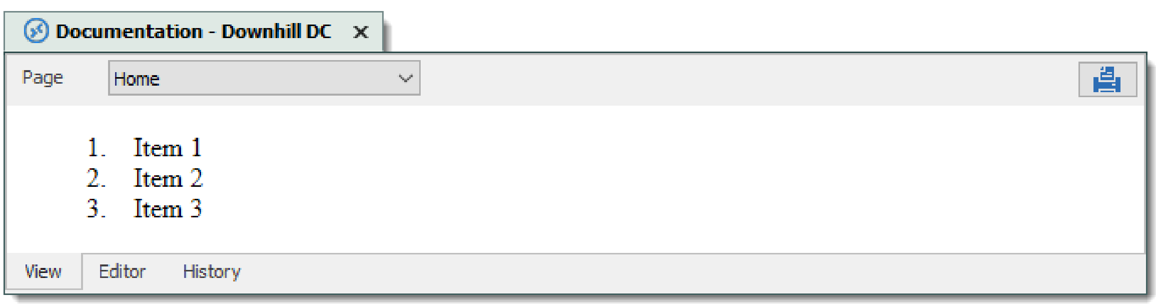
Output:



Use regular numbers, followed by periods, to create an ordered bulleted list.

```
1. Item 1
2. Item 2
3. Item 3
```

Output:



HORIZONTAL RULERS

Use three undersocres, asterisks, or hyphens to create a horizontal ruler.

```
___
```

or

```
***
```

or

```
---
```

Output:

LINKS

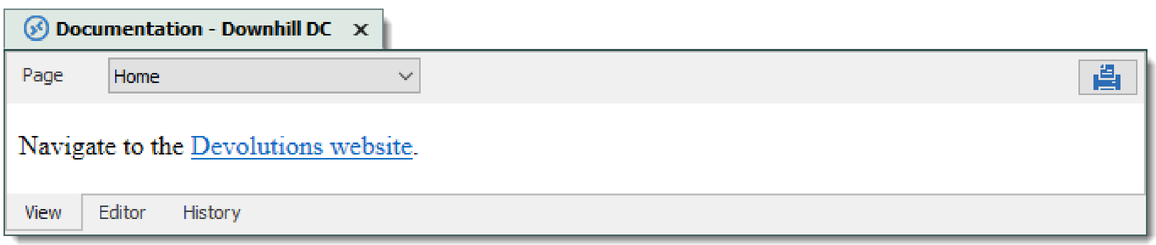
Use square brackets to delimit the text you want to turn into a link.

There are two ways of creating links: inline and reference.

Use parentheses immediately after the link text for inline-style links:

```
Navigate to the [Devolutions website](https://devolutions.net).
```

Output:



Optionally a title attribute may be included in the parentheses.

```
Navigate to the [Devolutions website](https://devolutions.net "Website of Devolutions'
```

Output:

For reference-style links, define the links elsewhere in the document, then refer to a link by its name in another set of square brackets.

```
Navigate to the [Devolutions website][mainwebsite] or the [Devolutions forum][forumwel

[mainwebsite]: https://devolutions.net/ "Website of Devolutions"
[forumwebsite]: https://forum.devolutions.net/ "Forum of Devolutions"
```

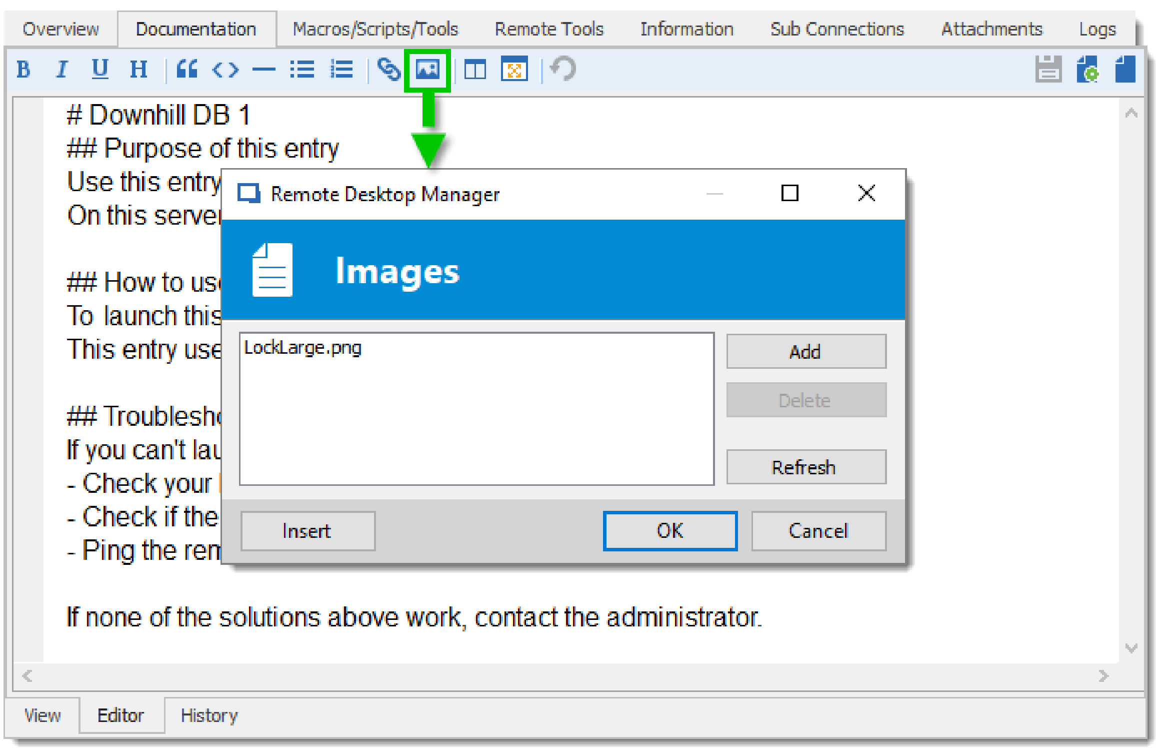
Output:

The title attribute is optional again. Link names may contain letters, numbers and spaces, but are not case sensitive.

IMAGES

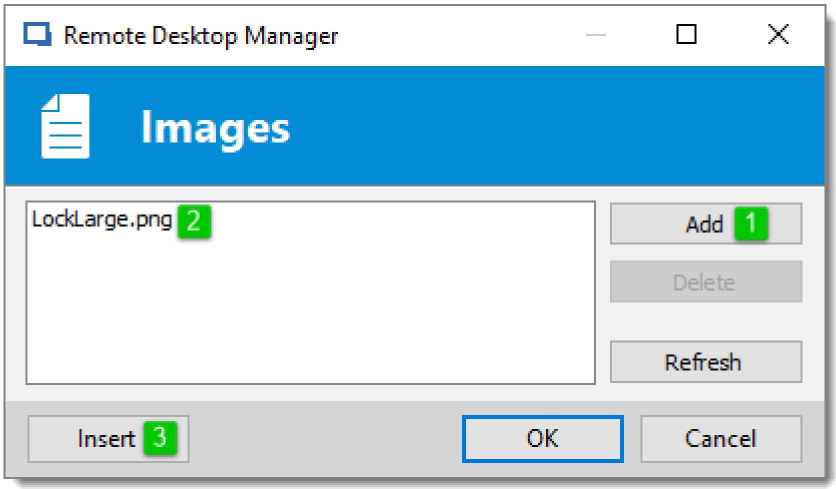
Image syntax is very similar to link syntax. Images must be added in the image manager before referencing them.

To add images in the image manager, click the ***Manage images*** button.



Documentation editor – Image manager

Click ***Add*** to select an image from the computer. Select the image in the list, and click ***Insert*** to place the image in the text.



Documentation editor - Add an image

BLOCKQUOTES

Quote a passage of text by inputting a greater-than (>) symbol at the beginning of the line of text.

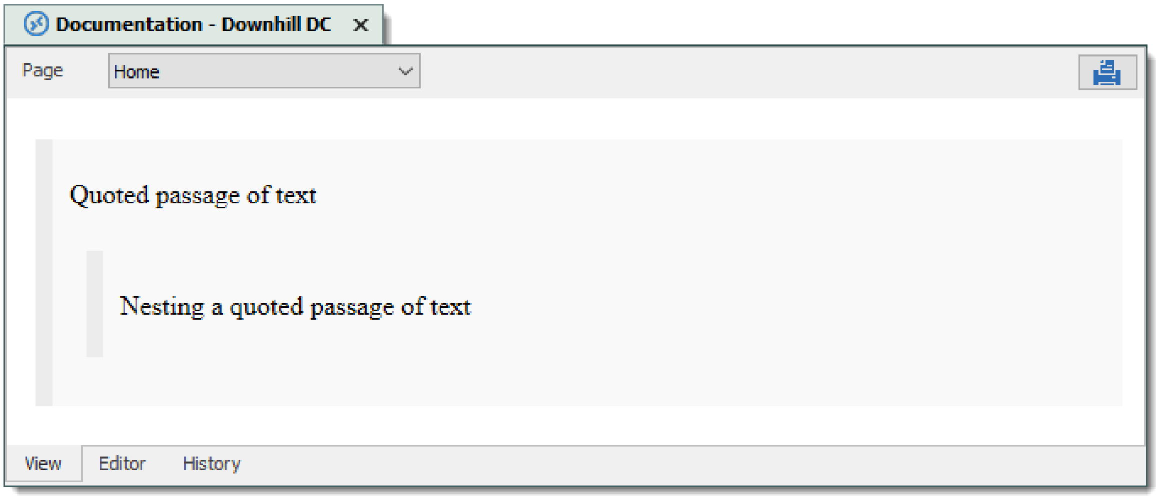
```
> Quoted passage of text
```

Output:

Blockquotes can easily be nested.

```
> Quoted passage of text
>> Nesting a quoted passage of text
```

Output:

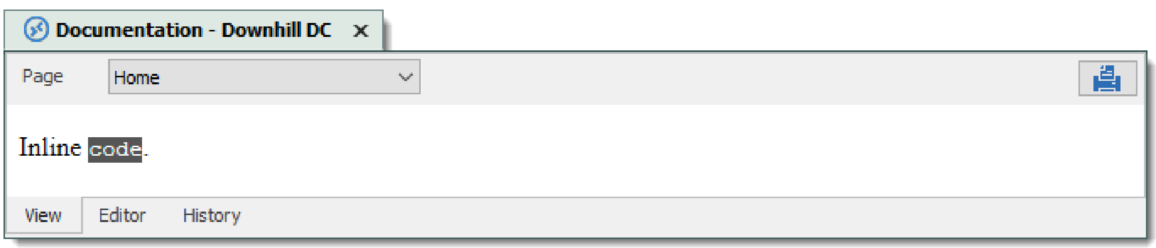


CODE EXAMPLES

Inline code is created by enclosing the text in backthicks (`).

```
Inline `code`.
```

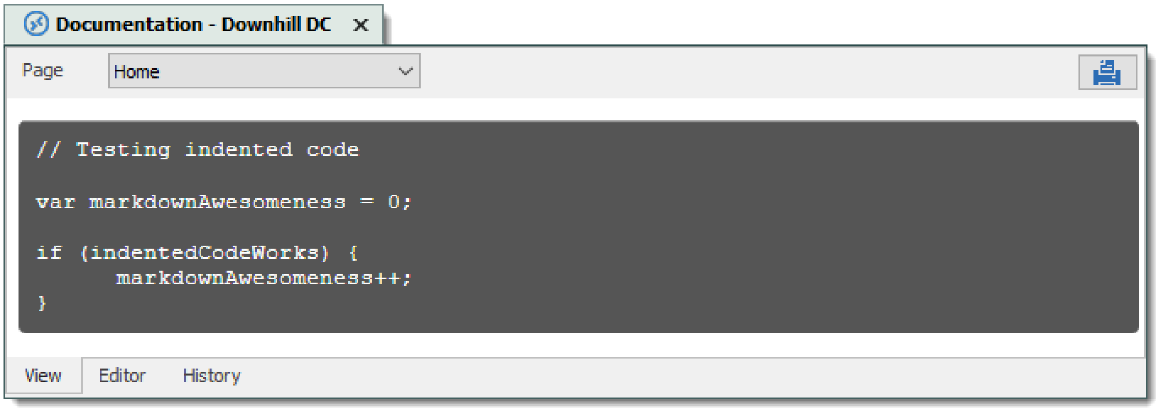
Output:



Code blocks are created be indenting the text with four spaces at the beginning of each lines There must have an empty line before.

```
    // Testing indented code

    var markdownAwesomeness = 0;

    if (indentedCodeWorks) {
          markdownAwesomeness++;
    }
```

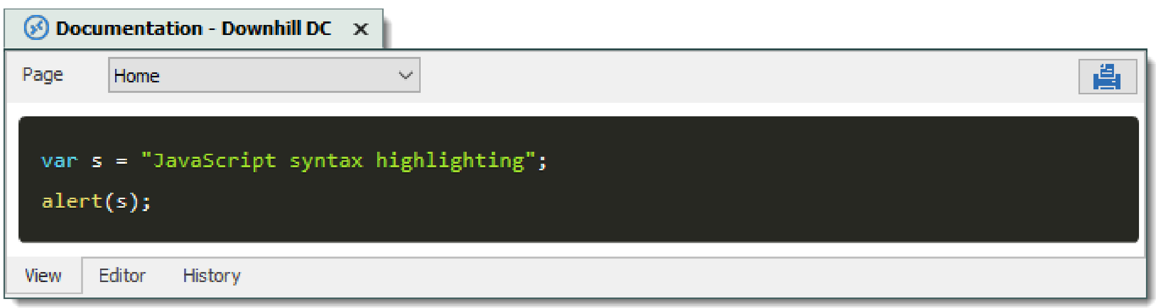
Output:



A specific syntax highlighting can be specified as well.

````
```javascript
var s = "JavaScript syntax highlighting";
alert(s);
```
````

Output:



6.1.3 Entry History

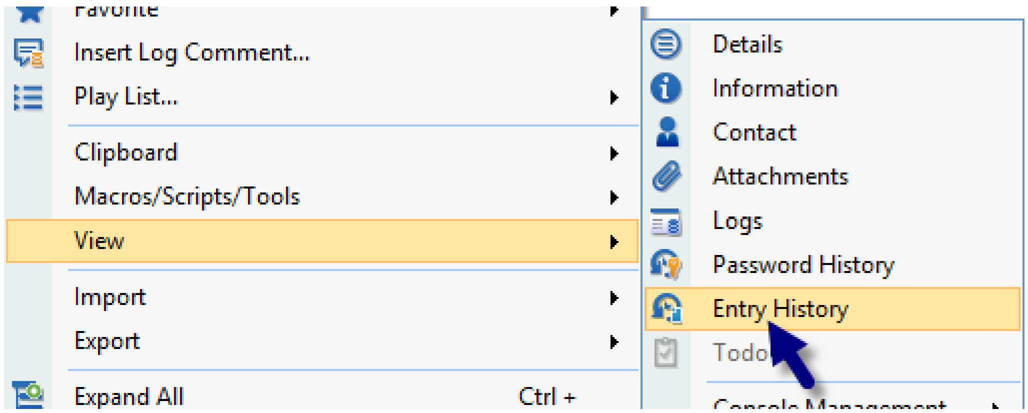
DESCRIPTION

Entry History feature allows you to view details regarding different version of your sessions and also gives you the option of performing compares between different versions.

> This feature requires an Advanced Data Source.

You must be an administrator of the data source to perform this action.

SETTINGS

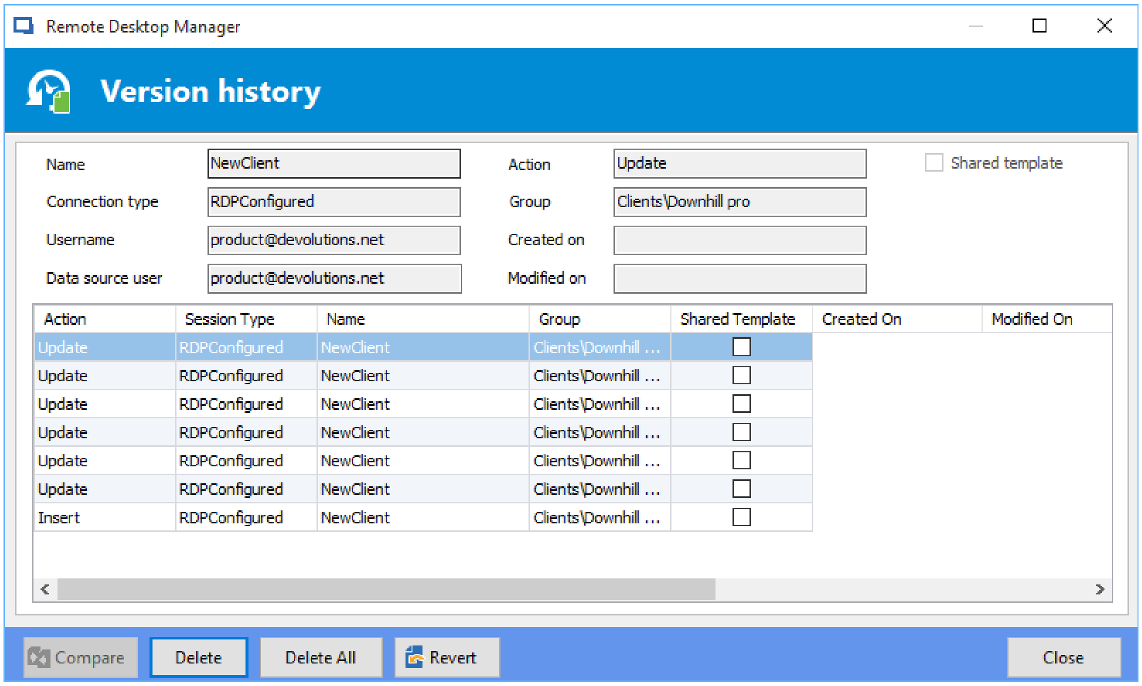


Home - Entry History

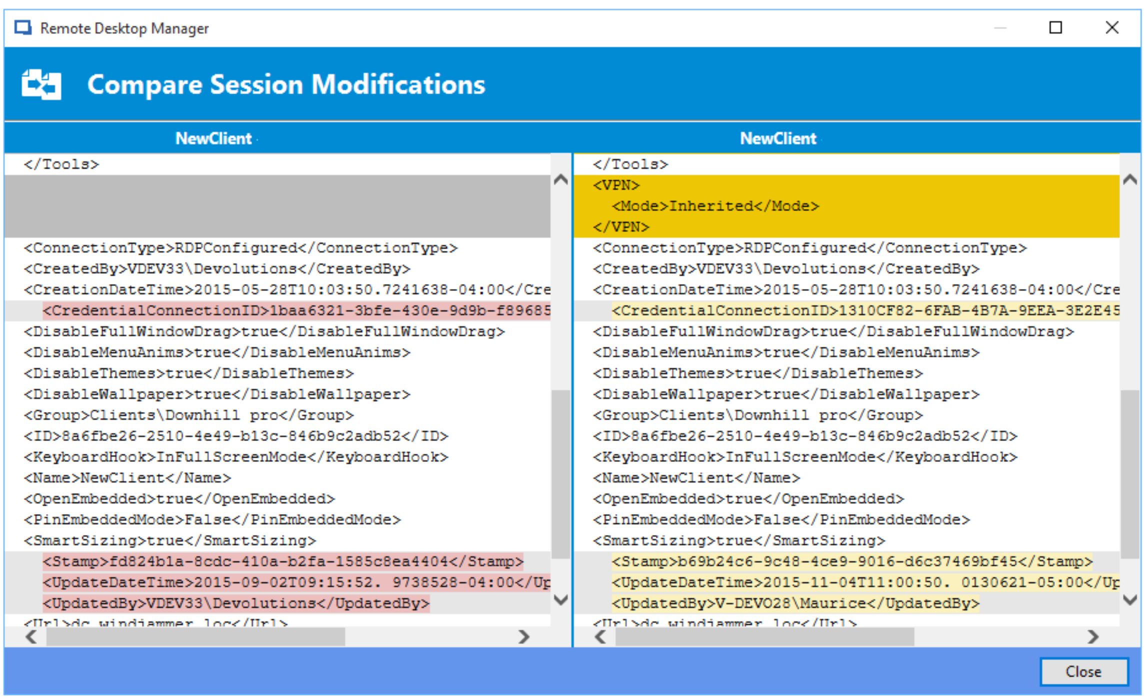
To display the entry history, ***right-click*** on an entry and select ***View - Entry History***.

ENTRY HISTORY VIEW

The entry history view dialog allows you to compare two entries and manage history revisions. To compare simply select any two entries then use the ***Compare*** button. You can delete any history revision or the entire history using the ***Delete*** and ***Delete All*** buttons.



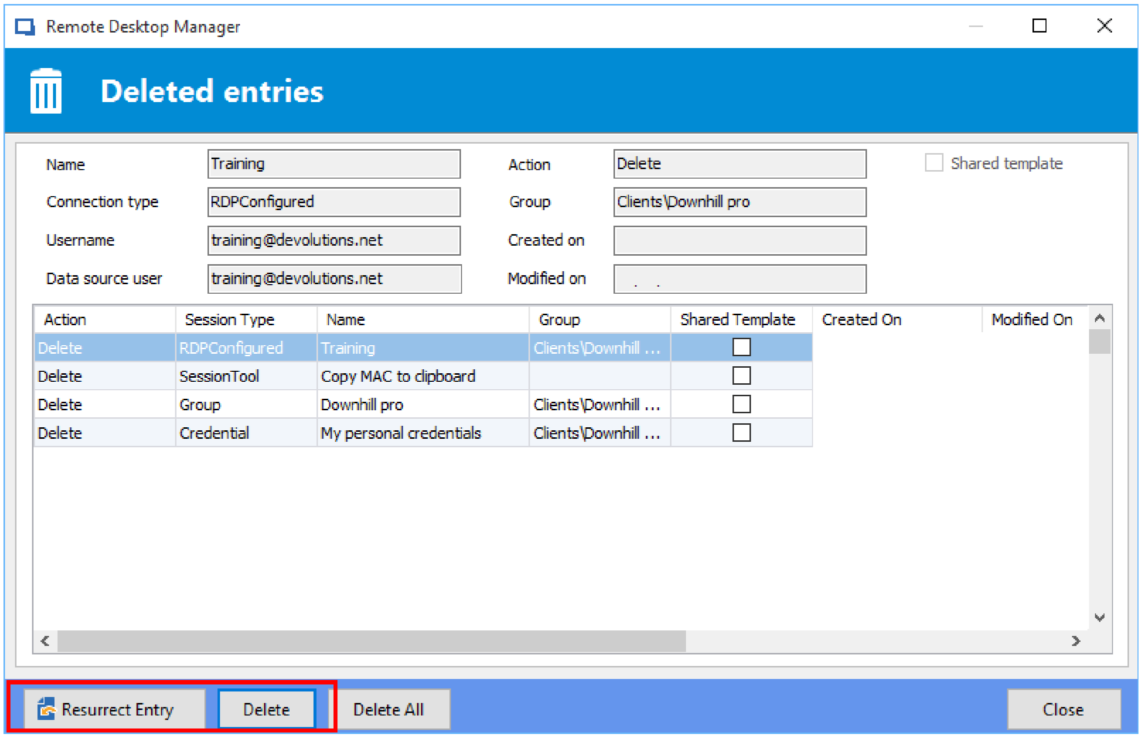
Entry history view



Compare session modifications

VIEW DELETED ENTRIES

Use the ***Administration - [View Deleted](#)*** to manage and resurrect deleted entries.

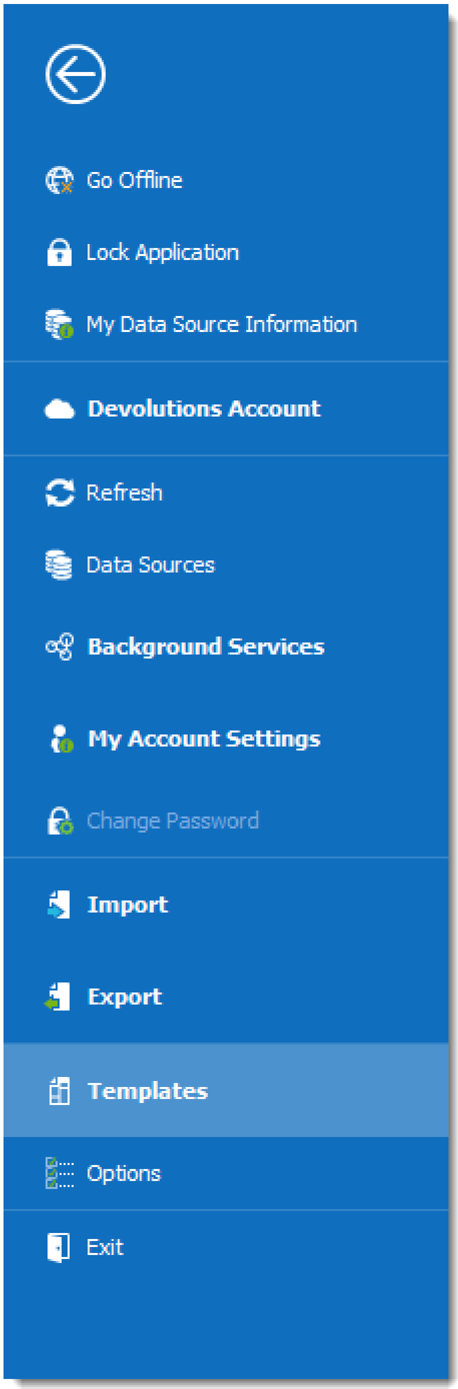


Deleted Entries

6.2 File

DESCRIPTION

The **File** menu contains many actions regarding the application and the data source. This menu is contextual and depends on the connected data source.



File

GO OFFLINE/ONLINE

Toggle the data source offline mode.

For more information, please consult the Offline mode topic.

LOCK APPLICATION

Lock and minimize the application.

The user is prompted for the data source password when the application is restored (if required by the configuration).

MY DATA SOURCE INFORMATION

Display configuration information relative to the current data source.

For more information, please consult the My Data Source Information topic.

DEVOLUTIONS ACCOUNT

Connect to a Devolutions Account, create custom installer for Remote Desktop Manager, manage license serials, and more.

For more information, please consult the Devolutions Account topic.

REFRESH

Refresh the data source and retrieve the most recent data.

For more information, please consult the Refresh topic.

DATA SOURCES

Open the data source configuration screen.

For more information, please consult the Data Sources topic.

BACKGROUND SERVICES

View and execute synchronizers.

For more information, please consult the Background Services topics.

MY ACCOUNT SETTINGS

View information about the current user and edit personal credentials.

For more information, please consult the My Account Settings topic.

CHANGE MASTER KEY

Prompts to change the current Master Key

For more information, please consult the Change Master Key topic.

IMPORT

Import entries in the data source.

For more information, please consult the Import topic.

EXPORT

Export entries from the data source.

For more information, please consult the Export topic.

OPTIONS

Edit the application options.

For more information, please consult the Options topic.

TEMPLATES

Edit templates and default settings for entries.

For more information, please consult the Templates topic.

6.2.1 Go Offline/Online

DESCRIPTION

Toggle the data source Offline Mode.

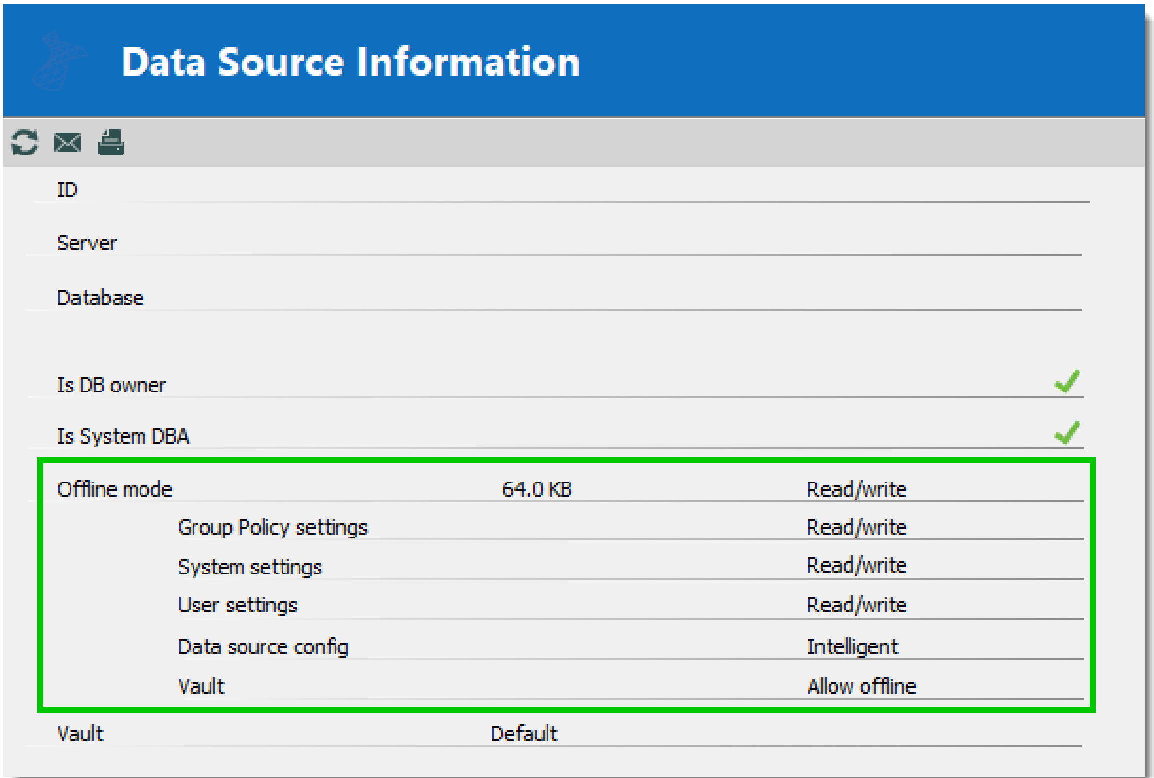
Use the offline mode to connect to a local copy of the data source when the remote database is unavailable. This is useful when working from a remote location and the network is unreachable or if there is any kind of connectivity issue.

> There are security considerations to take into account when enabling the offline mode.

The offline mode availability relies on several settings, refer to the Offline Mode topic.

The lowest setting (in terms of security) prevails over the others, which may prevent you from using the offline mode. If the **Go Offline** button is not available, please consult your administrator.

The **Data Source Information** displays the size of the offline cache file along with the effective modes (disabled, read-only or read/write).



Data Source Information - Offline mode

Several features are not available in offline mode, such as:

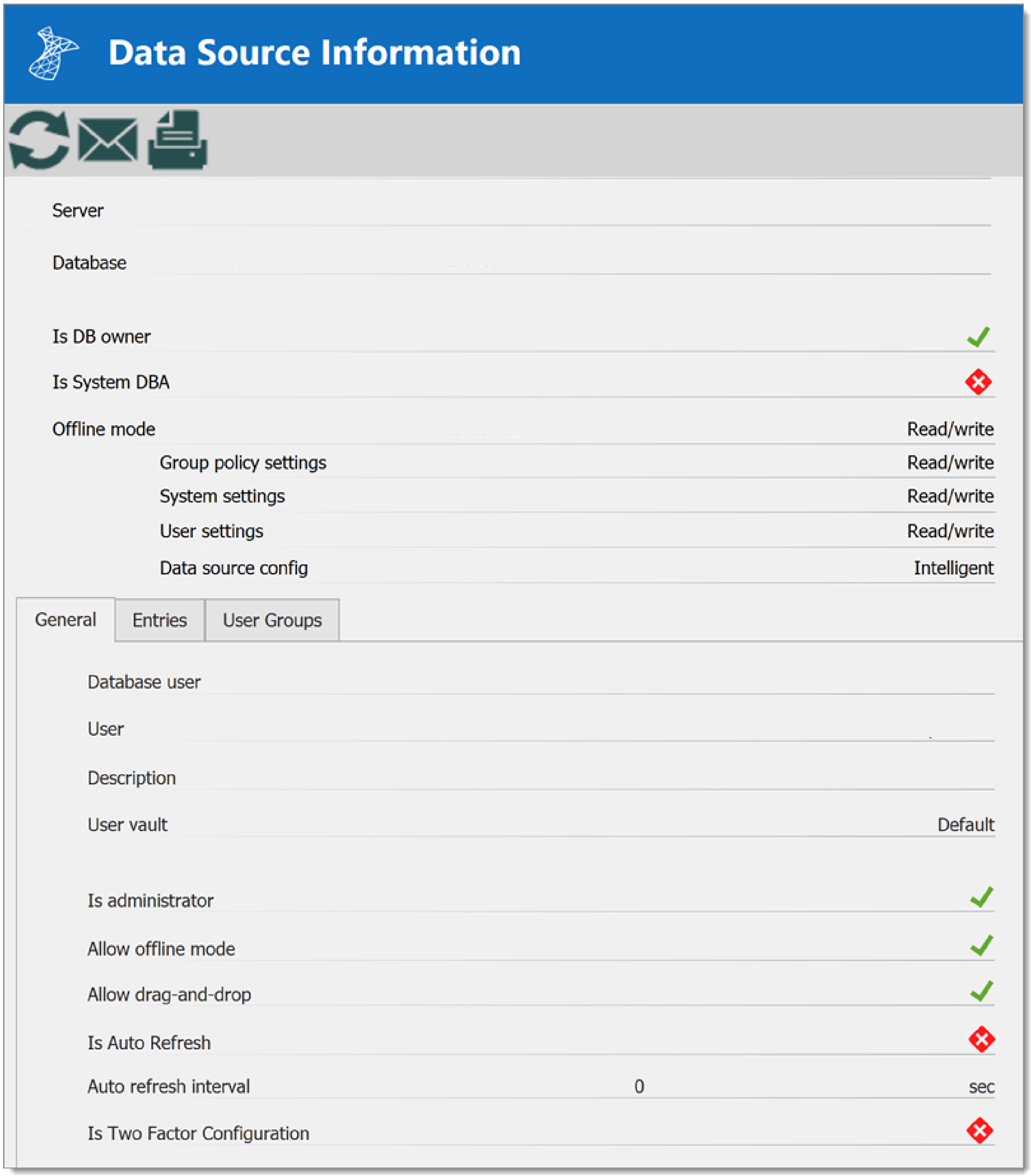
- Attachments and logs.
- User management (Add/Edit/Delete users).

6.2.2 My Data Source Information

DESCRIPTION

The **Data Source Information** displays various information related to the current data source, such as the current user and security access.

> The **My Data Source Information** view can be different depending on the Data Source Type. This topic uses an SQL Server data source.

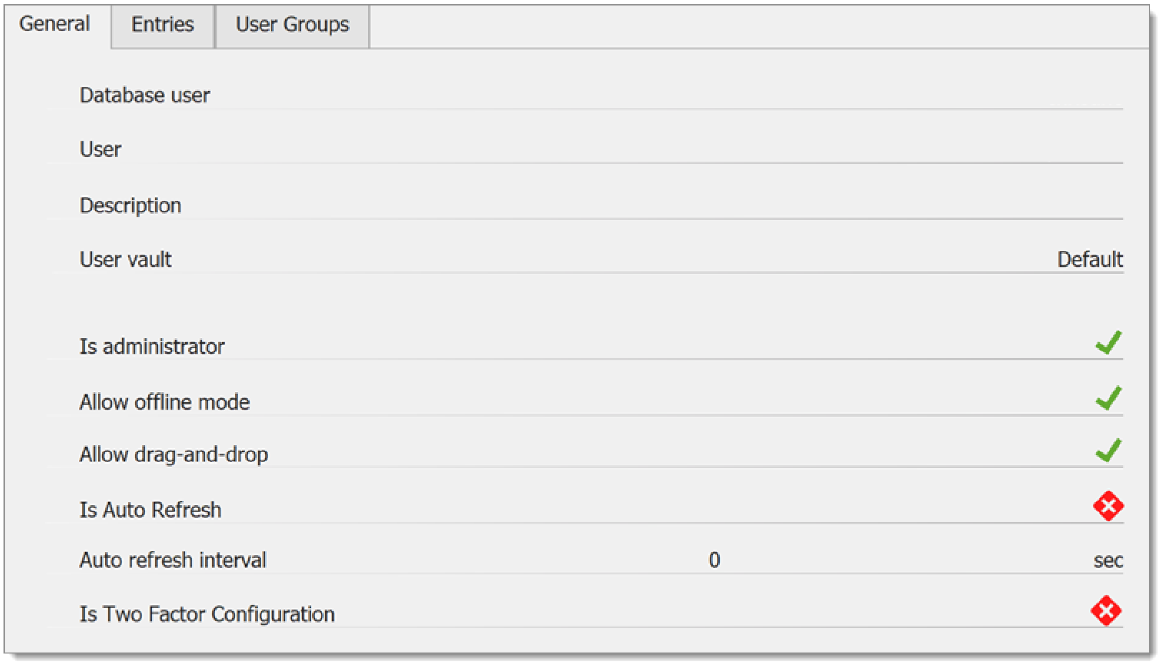


File – My Data Source Information

USER AND SECURITY

GENERAL

The General tab displays information about the current user and data source configuration.

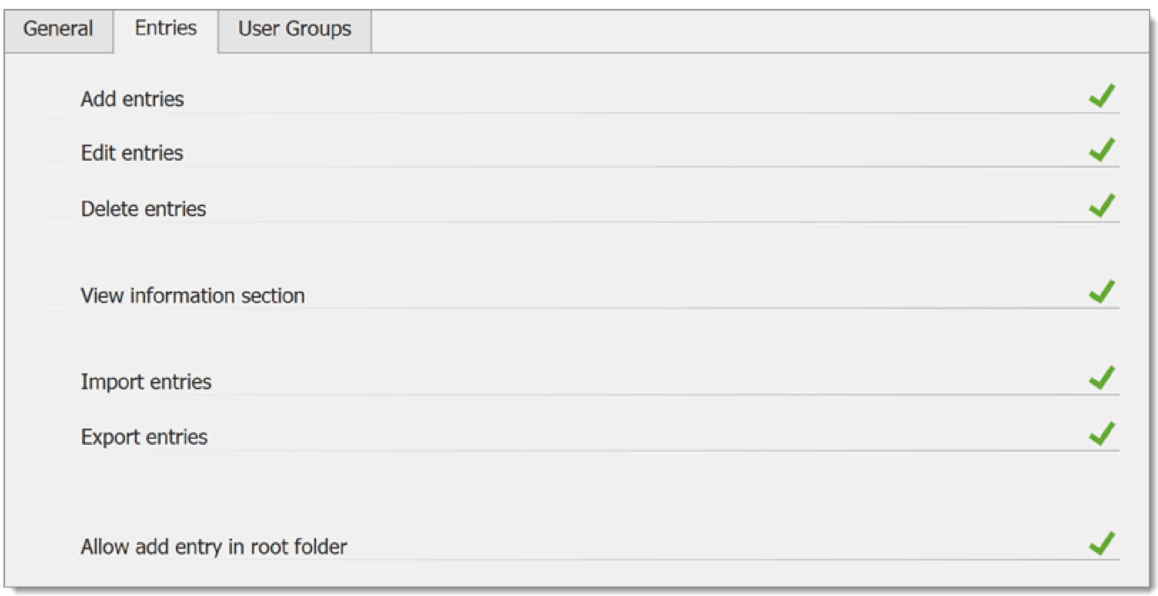


My Data Source Information - General

OPTION	DESCRIPTION
Database user	The name of the user currently logged to the database.
User	The actual windows user.
Description	Display the description of the user connected to the data source.
Is administrator	Indicates if the user is an administrator.
Allow offline mode	Indicates if the user can use the data source in offline mode.
Allow drag-and-drop	Indicates if the user can drag-and-drop entries in the data source.

OPTION	DESCRIPTION
Is Auto Refresh	Indicates if the data source auto refreshes.
Auto refresh interval	Indicates the delay for the auto refresh to occur.
Is Two Factor Configuration	Indicates if the data source is configured with a second factor of authentication.

ENTRIES



My Data Source Information – Entries

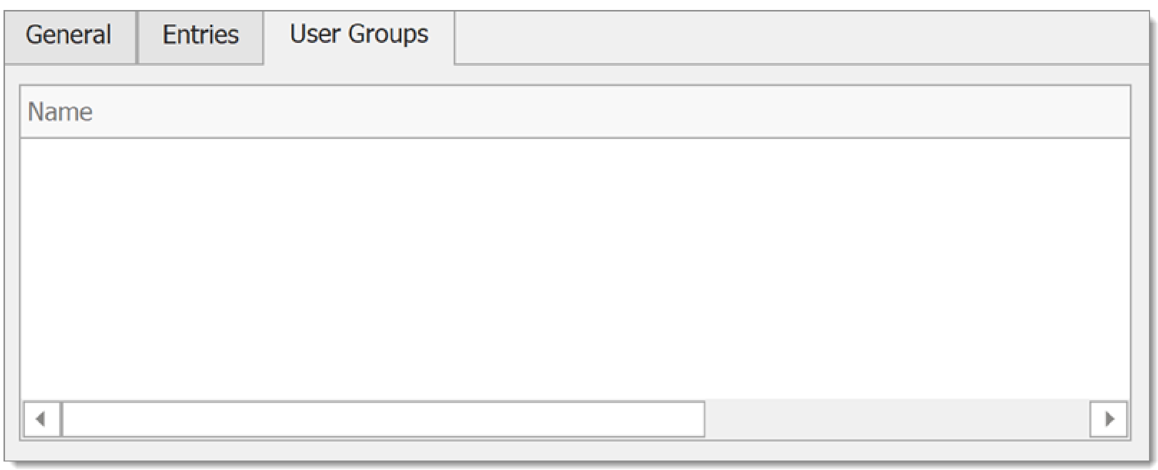
OPTION	DESCRIPTION
Add, Edit and Delete entries	Indicates if the user has the right to add, edit, or delete entries.
View information section	Indicates if the user can view the information section of entries.

OPTION	DESCRIPTION
Import and Export entries	Indicates if the user has the privilege to import or export entries.
Allow add entry in Vault folder	Indicates if the user can add entries in the Vault of the data source.

USER GROUPS

The **User Groups** tab displays the user groups that the user is a member of and the rights related to those user groups.

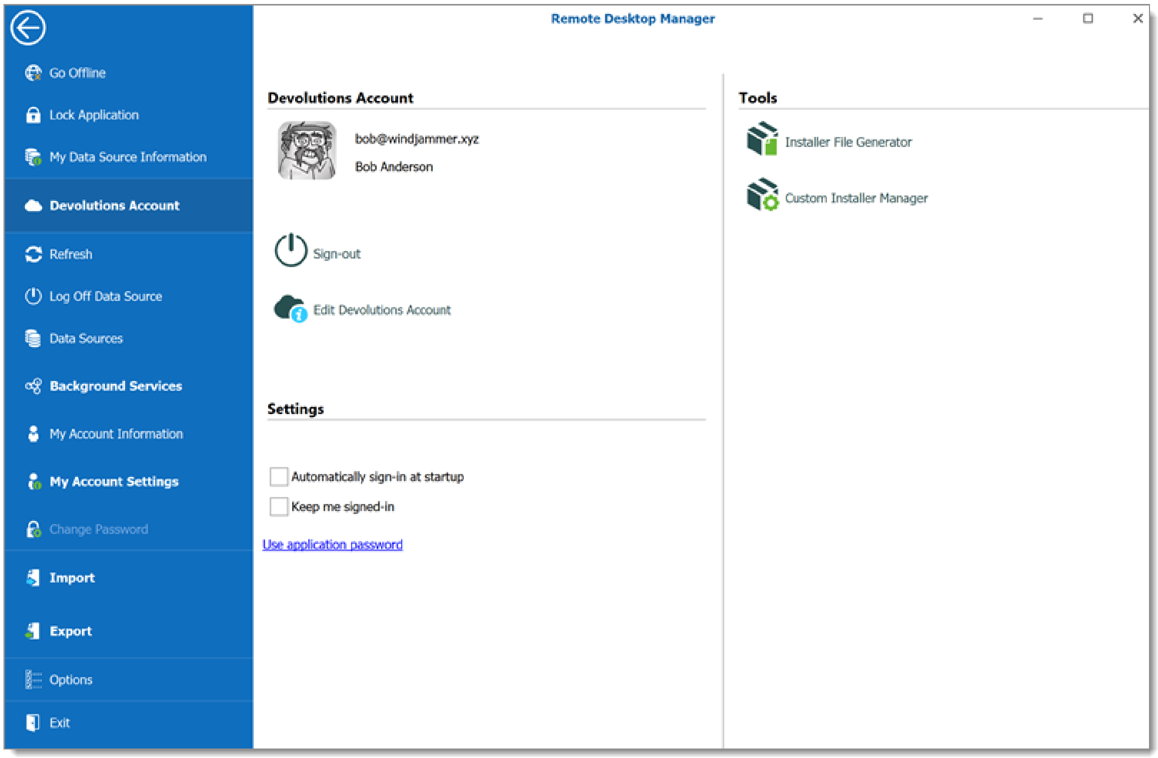
> This feature is only available with an [SQL Server/Azure SQL]() and a [Devolutions Server (DVLS)]() data source.



6.2.3 Devolutions Account

DESCRIPTION

In ***File - Devolutions Account*** create and connect your Remote Desktop Manager to your Devolutions Account. The Devolutions Account is free for customers and includes access to the ***Custom Installer Manager***.



Devolutions Account

DEVOLUTIONS ACCOUNT

OPTION	DESCRIPTION
Sign-in or Sign-out	Sign-in or out with your Devolutions Account.
Create a New Devolutions Account	Create a new Devolutions Account.
Edit Devolutions Account	Edit your Devolutions Account.

SETTINGS

OPTION	DESCRIPTION
Automatically sign-in at startup	Automatically sign-in to your Devolutions Account at the startup of the application.
Keep me signed-in	Keep a token in memory to remain signed into your Devolutions Account.
Use application password	Use the Application password to connect to your Devolutions Account.

TOOLS

OPTION	DESCRIPTION
Installer File Generator	Create a Remote Desktop Manager Installer File (.rdi). Consult topic Installer File Generator.
Custom Installer Manager	Consult topic Custom Installer Manager.

6.2.4 Backup

DESCRIPTION

Please consult topic Online Backup for information on this service.

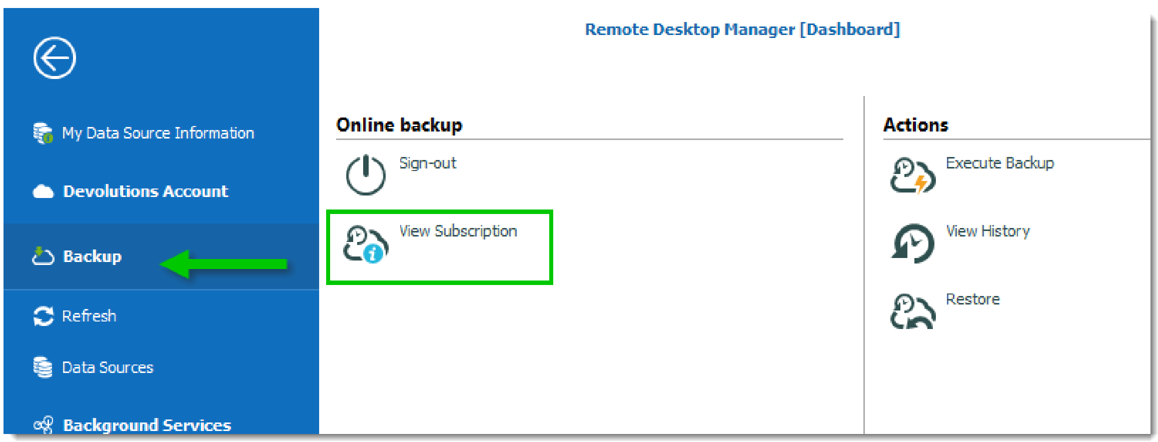
6.2.4.1 Settings

DESCRIPTION

The Online Backup allows you to backup your Devolutions Online Drive, SQLite or XML data sources in a safe online storage. The backup option is available through ***File – Backup*** menu.

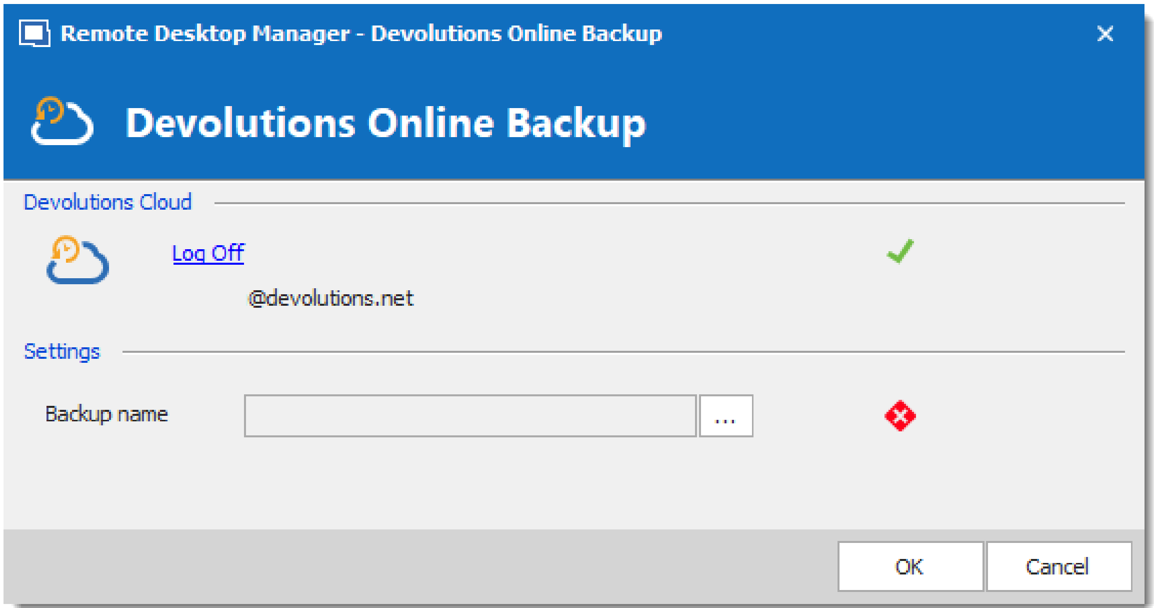
SETTINGS

1. Click on ***File – Backup*** to Sign-in with your Devolutions Account.
2. Click on **View Subscription**.



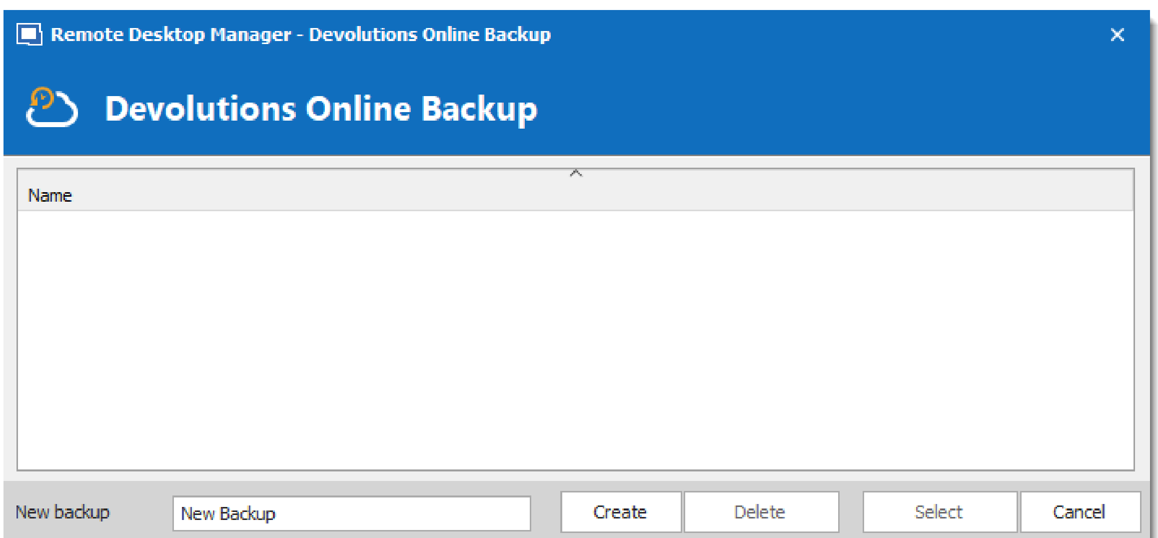
Online Backup - View Subscription

3. Click on the ellipsis to enter your **Backup name**.



Backup Name

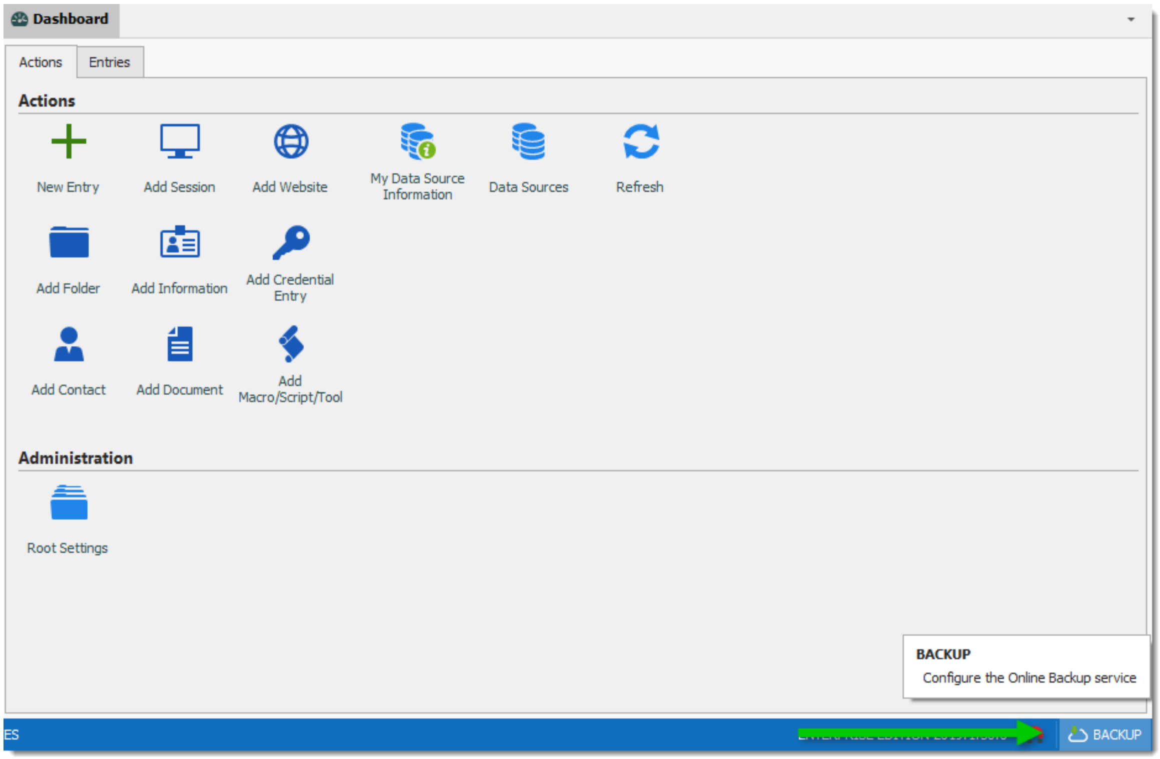
4. You will need to specify a unique backup name in the field **New backup** for each of your data source which will then be used to backup and restore the data source. Click on **Create** to automatically create your Online Backup.



Create Backup

5. Once you've completed all the steps, perform a change in the data source to properly activate the Online Backup.

6.The backup logo will display a green arrow meaning your backup is now enabled.



Online Backup Activated

You must perform this for all your Devolutions Online Drive, SQLite or XML data sources in order to be fully protected!

The automatic backup is executed in the background 30 seconds after any modification is made to the data source content.

6.2.4.2 Restore

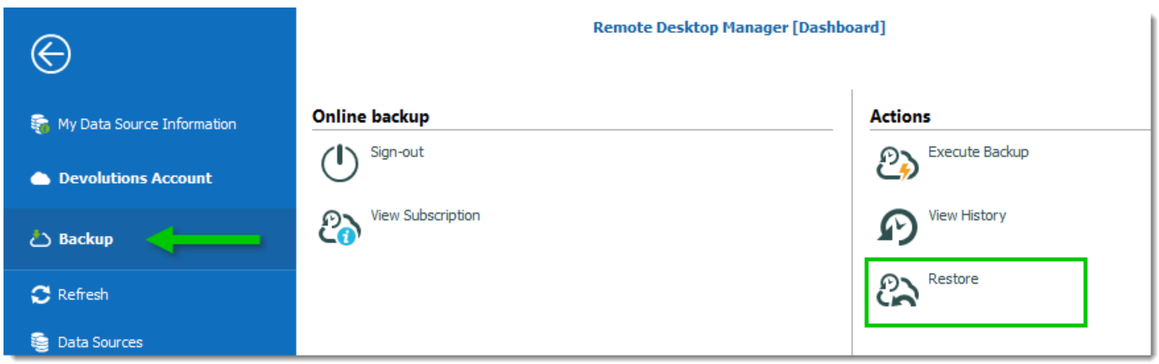
DESCRIPTION

Before being able to restore a backup, you **MUST** create an empty data source and define the backup name before being able to use it. You need to create a new SQLite, XML or Online Drive data source in ***File – Data Sources***.

At some point, you may need to restore a backup of your Devolutions Online Drive, SQLite or XML data sources. The restore option is accessible from the menu ***File – Backup – Restore***.

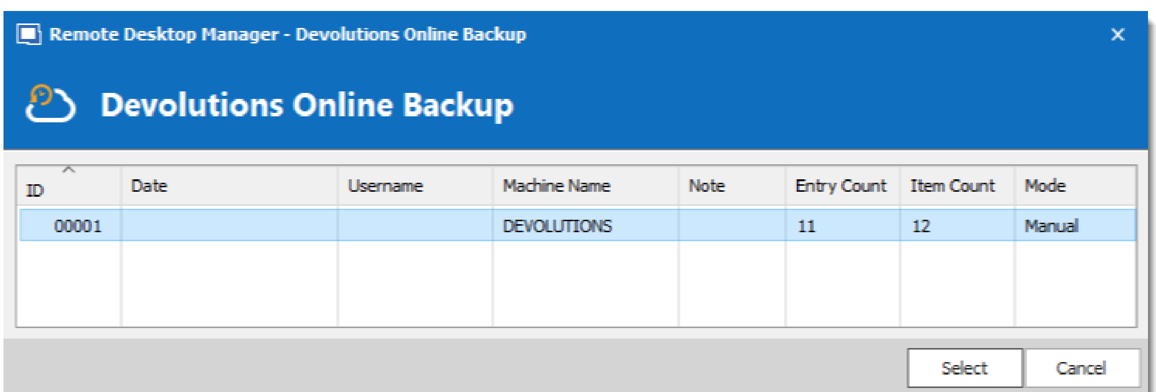
SETTINGS

1. To restore a data source from a backup, select it as the current data source.
2. Click on ***File – Backup – Restore.***



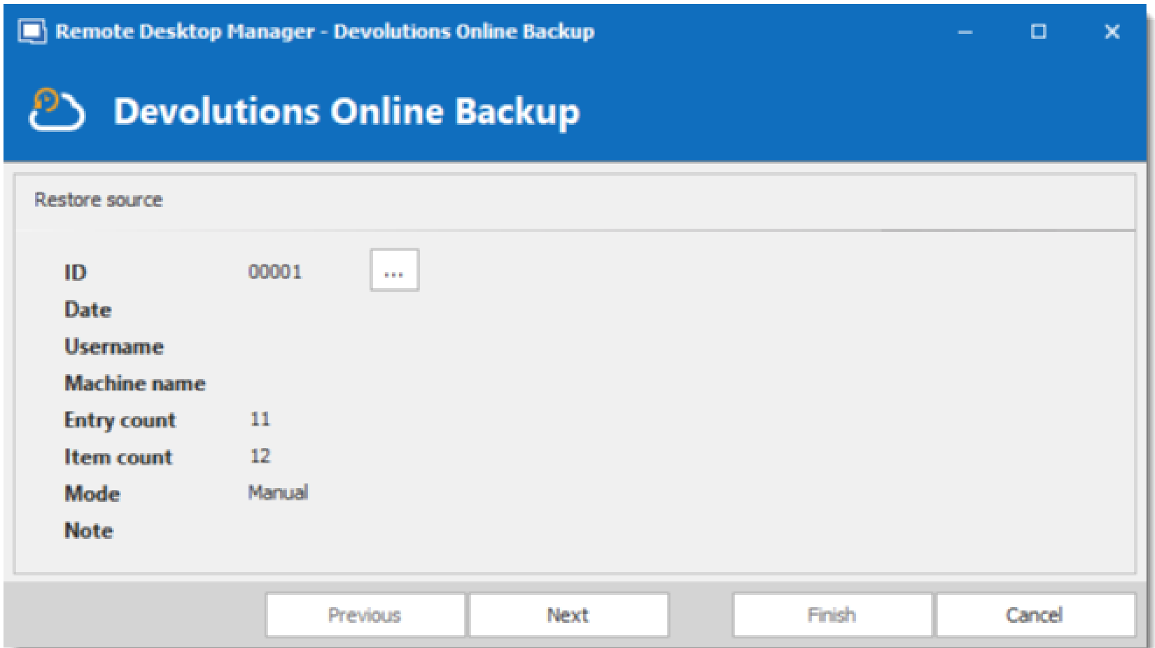
Backup Restore

3. Select the backup that you wish to restore from the list and click on **Select.**



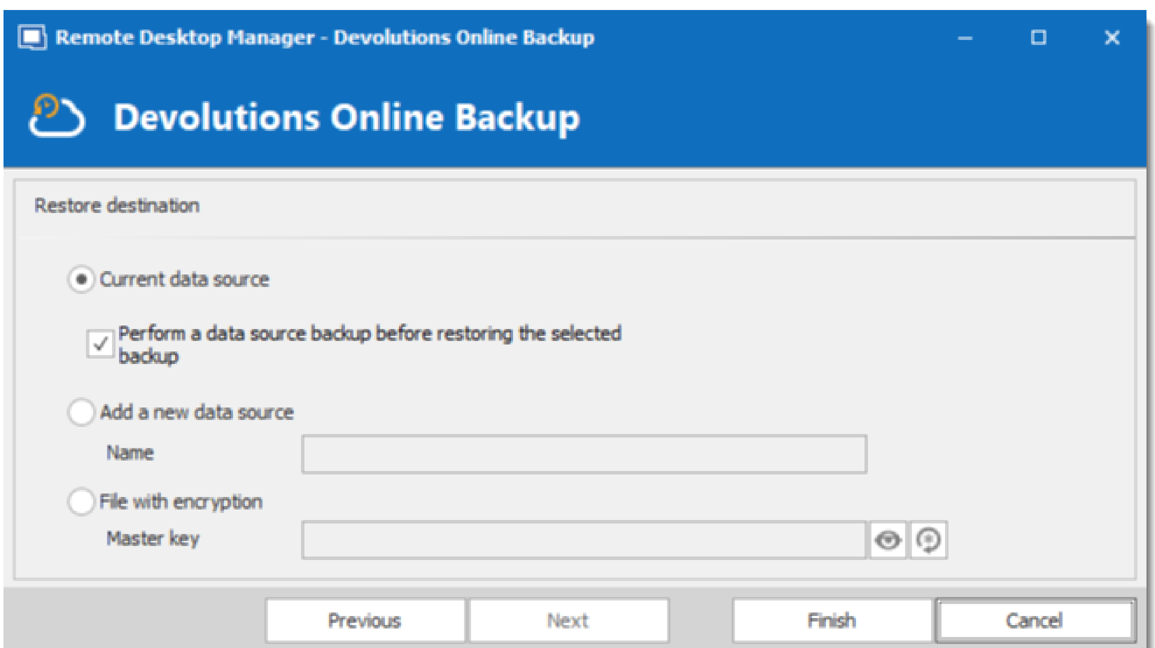
Select your Backup

4. The Online Backup wizard will display a brief description of the backup. Click on **Next.**



Backup Wizard

5. Select the restore destination. It is not necessary to select the option **Perform a backup data source before restoring the selected backup** since it is empty.



Restore Destination

6. Click on **Finish** to perform your backup restore.

6.2.5 Refresh

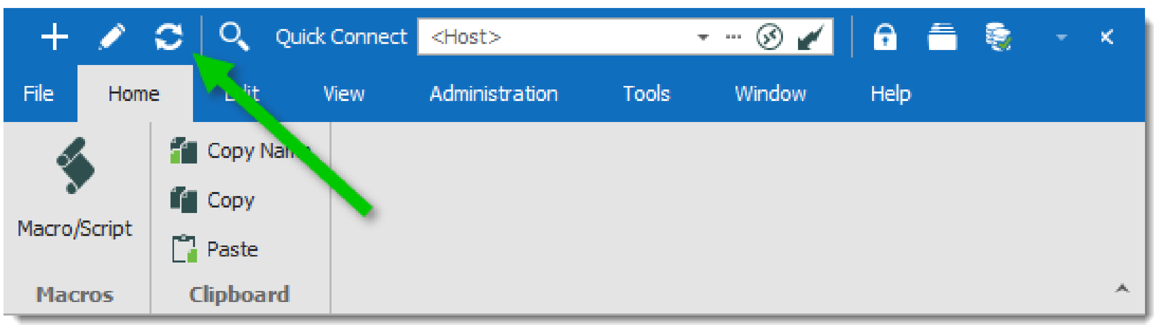
DESCRIPTION

Refreshing the data source allows for updating its content. Data sources are usually refreshed automatically after a set period of time.

To refresh the data source, use ***File – Refresh***. Do a refresh to make sure that the data source is up to date.

SIMPLE REFRESH

A simple refresh updates the data source to retrieve only the modified content. Use the above-mentioned ***File – Refresh*** or the refresh button in the Quick Access Toolbar.



Refresh the Data Source

LOCAL CACHE REFRESH

A refresh of the local cache resets the local cache of the data source. All the content is retrieved from the database and the local cache file is recreated. Click the refresh button while holding the **Ctrl key** or use the **Ctrl+F5** key combination. A local cache refresh may also help when experiencing Cache issues.

6.2.6 Change Master Key

DESCRIPTION

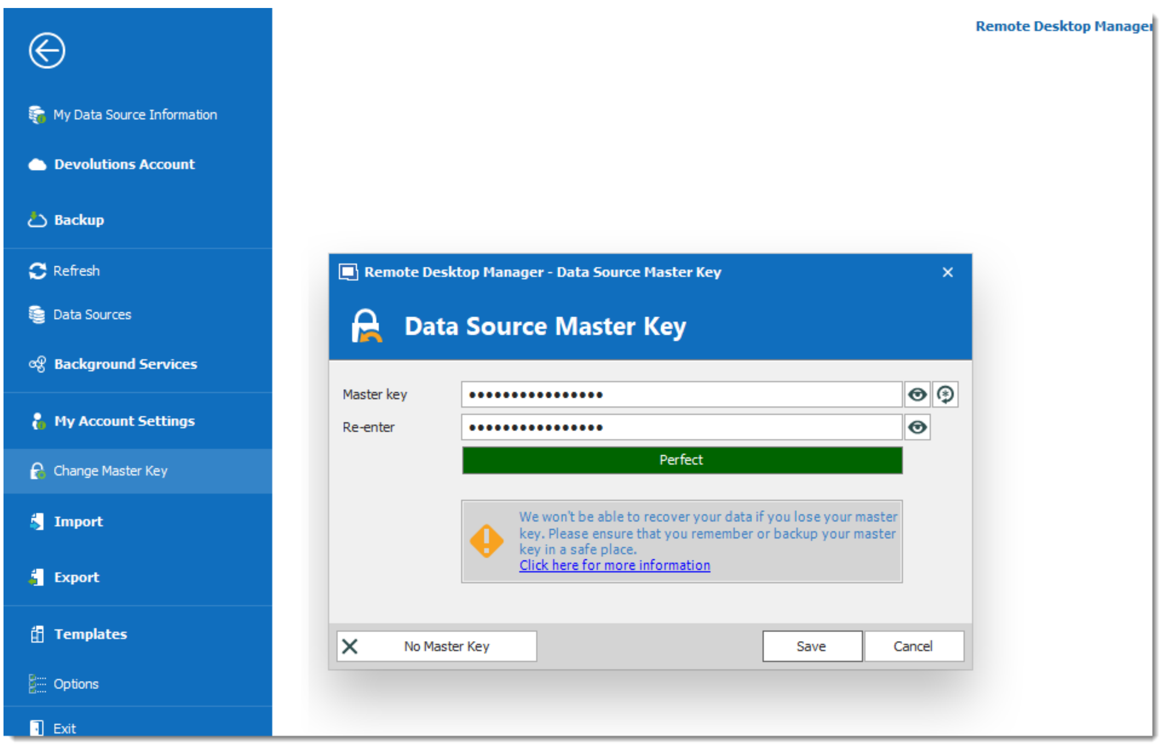
Use ***File – Change Master Key*** to encrypt the data source.

The master key prevents unauthorized users to access the data source without knowing the master key. It is highly recommended to apply a master key to the data source if you're using Remote Desktop Manager in a portable environment (i.e. USB Flash Drive, USB Hard Drive).

A master key can be used with the following data sources:

- Devolutions Online Drive
- Dropbox
- Google Drive
- XML

Since version 14.0.4.0, the user is automatically prompted to add a master key when connecting to one of the above mentioned data sources for the first time. The master key is completely optional (yet highly recommended).



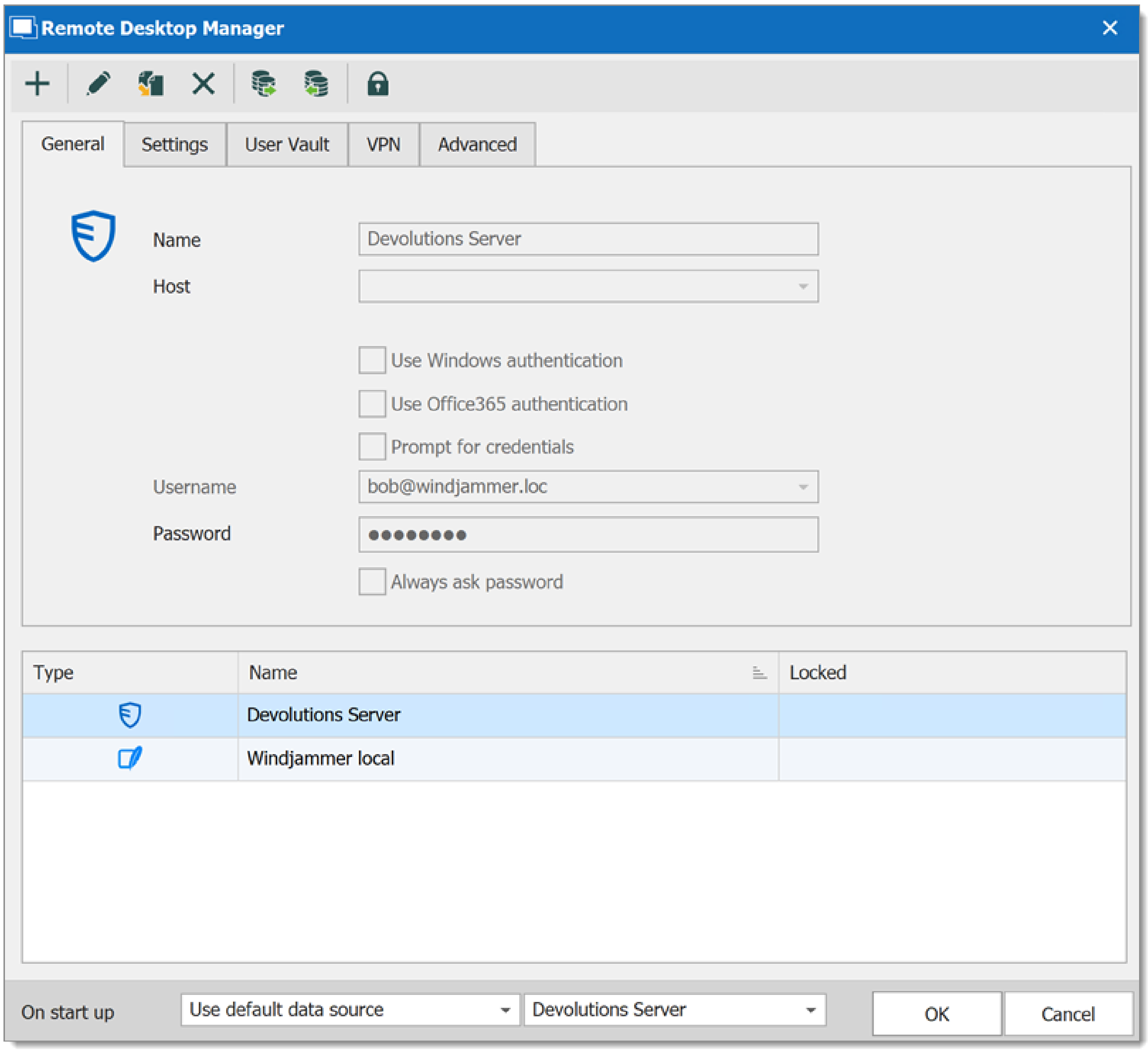
Change Master Key

6.2.7 Data Sources

DESCRIPTION

Use ***File – Data Sources*** to manage data sources. Remote Desktop Manager supports multiple types of data source. Most are available only with an Enterprise Edition of Remote Desktop Manager.

Please refer to the Data Source Types topic for more information on all supported types of data sources.



Data Source

SETTINGS

ADD A NEW DATA SOURCE

Use the **Add** button to create a data source configuration.

EDIT/DUPLICATE/DELETE DATA SOURCE

Use the – – buttons to respectively edit, duplicate or delete the selected data source configuration.

> Only the configuration will be deleted but the actual file or database will still be available.

IMPORT/EXPORT DATA SOURCE CONFIGURATION

Use the – buttons to respectively import or export the selected data source configuration. The configuration is exported as a **.RDD** file.

LOCK DATA SOURCE

Use the **lock** button to lock the data source with a password to prevent any modification to a data source configuration. This is useful when having sensitive credentials that you wish to protect from other users.

UNLOCK DATA SOURCE

Use the **unlock** button to unlock a data source locked with a password.

ON START UP

Choose which data source to connect to when the application starts.

OPTION	DESCRIPTION
Use default data source	Set the data source that you always want to open at start up.

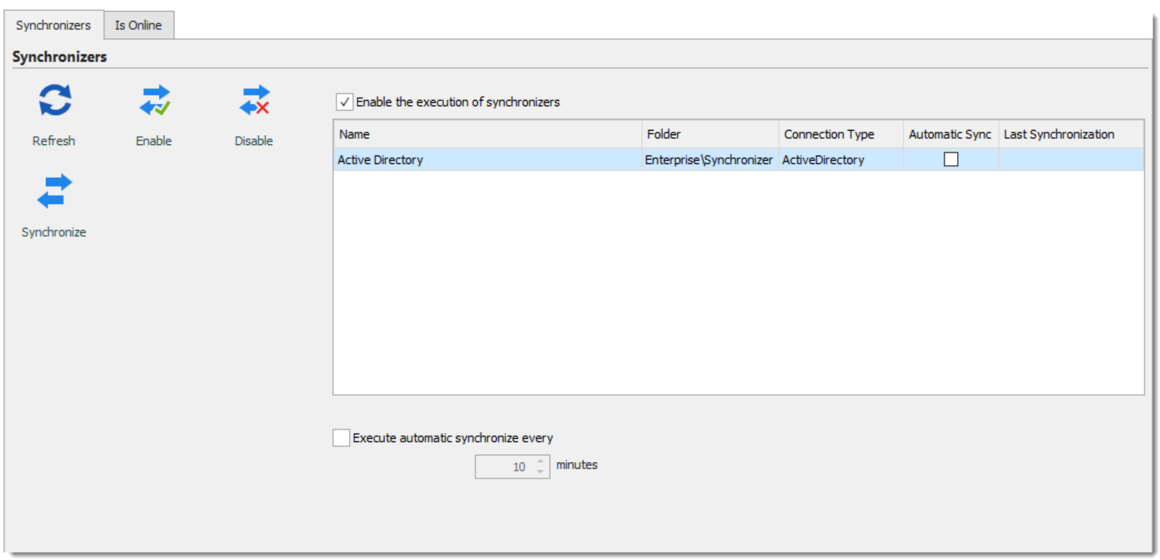
OPTION	DESCRIPTION
Last used data source	Open with the last used data source.
Prompt for data source	A message box will open on startup for the data source selection.

6.2.8 Background Services

SYNCHRONIZERS

Synchronizers centralizes all your synchronizers entry in one place.

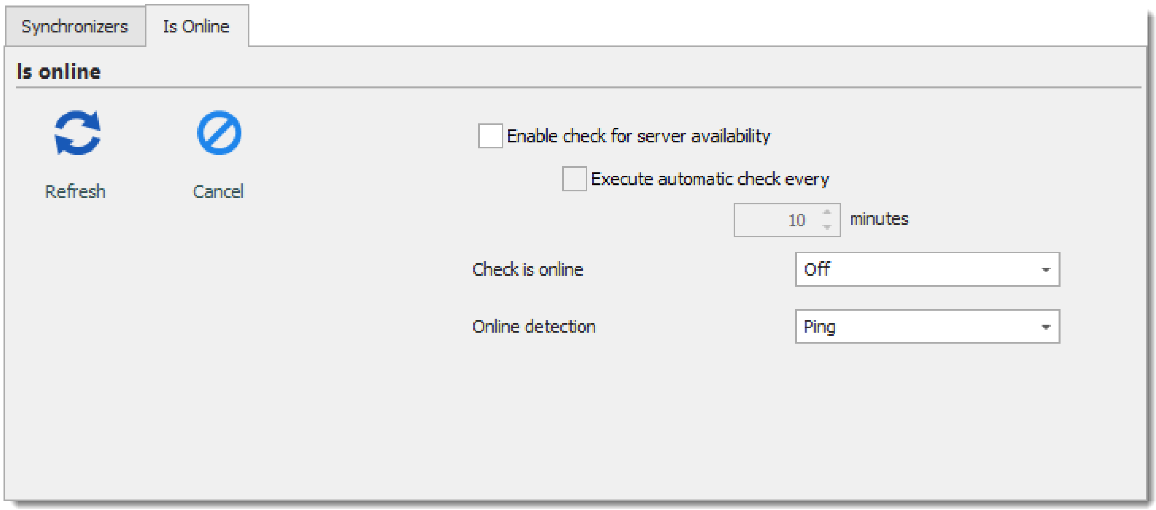
When experiencing a performance degradation with Remote Desktop Manager you will be able to verify if a synchronizer is running in the background causing the system to slow down.



Synchronizers

IS ONLINE

Is Online allows you to verify and change the settings of your server's online availability.



Is Online

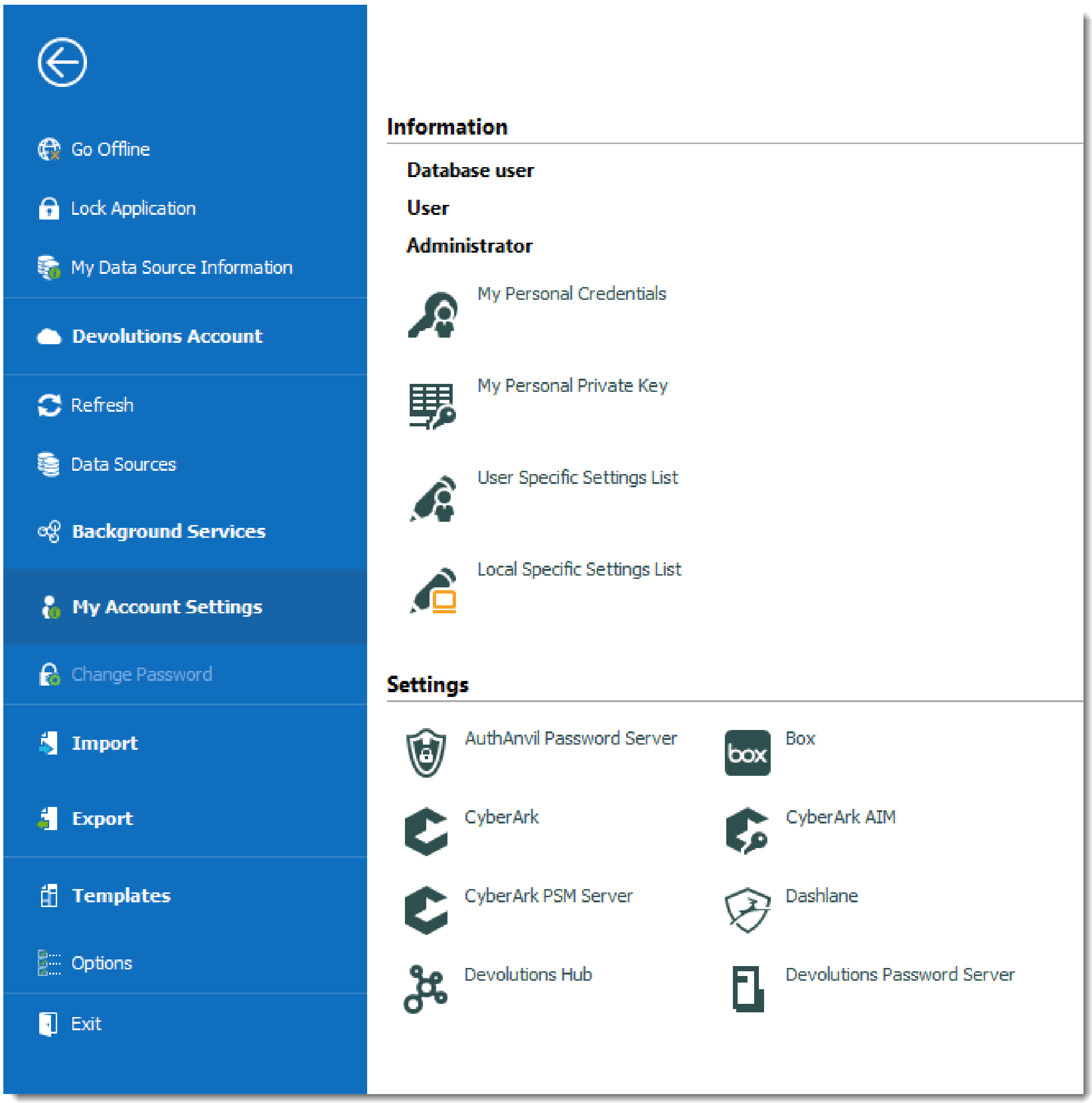
OPTION	DESCRIPTION
Enable check for server availability	Server is ping to determine if they are available. Server will be displayed in "red" in the tree view if not available.
Execute automatic check every	Execute the online check automatically each determined amount of minutes.
Check is online	If the option is **On** the application will verify if the server is online.
Online detection	If **Check is online** option is enable, select the detection method between: • **Ping** • **Port scan**

6.2.9 My Account Settings

DESCRIPTION

Use ***File – My Account Settings*** to configure accounts that connect to different web platforms. Set up account settings one time and use it in entries as many time as required. This section also allows to manage **Personal Credentials**, **Personal Private Key** and **Specific Settings** lists.

SETTINGS



My Account Settings

INFORMATION

OPTION	DESCRIPTION
Database user	Indicates the current user connected to the application.
User	Indicates the user of the current Windows session.
Administrator	Indicates if the current user is administrator or not.
My Personal Credentials	Please consult My Personal Credentials topic for more information.
My Personal Private Key	Configure a personal private key for further use in sessions.
User Specific Settings List	Provide a list of all the User Specific Settings configured in Remote Desktop Manager.
Local Specific Settings list	Provide a list of all the Local Specific Settings configured in Remote Desktop Manager.

SETTINGS

We support a specifics settings for a variety of Credentials, explore to your heart's content!

6.2.9.1 My Personal Credentials

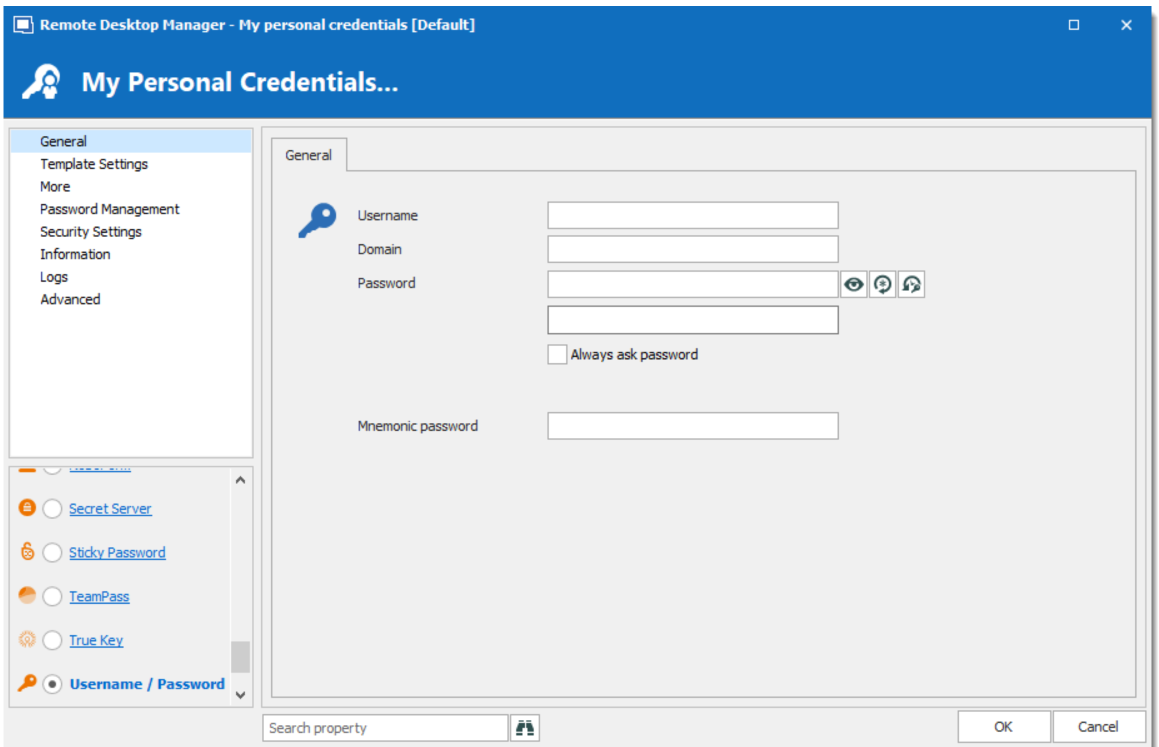
DESCRIPTION

The **My Personal Credentials** feature is a single credential entry which is locally stored on your computer in your Windows profile.

It is typically used to hold the Windows credentials for your running sessions because Remote Desktop Manager can't access them. If you can't use integrated security then you must store your credentials in **My Personal Credentials**.

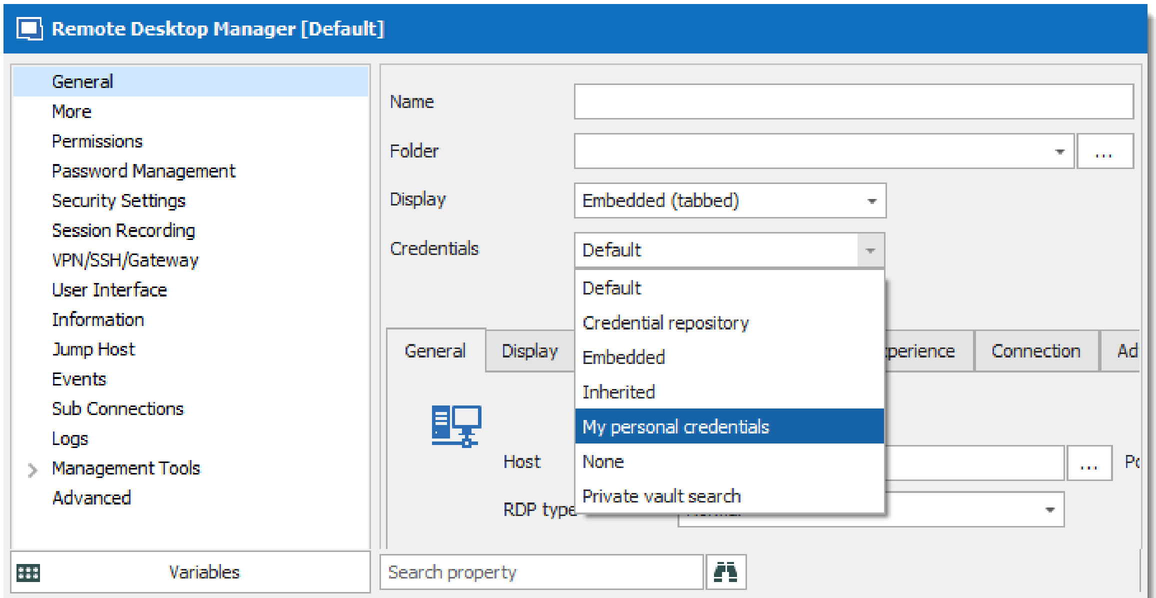
This allows you to centralize one special credential to replace or emulate the ones for your Windows session. When a password change is needed you simply need to change it once in **My Personal Credentials**.

> If you want to change the credential type, go in ***%LOCALAPPDATA% (Default) or %APPDATA% (Remote Desktop Services)\Devolutions\RemoteDesktopManager*** and delete the **Credentials.rdt** file to reset it.



My Personal Credentials

My Personal Credentials can be selected in your entries under **Credentials**.

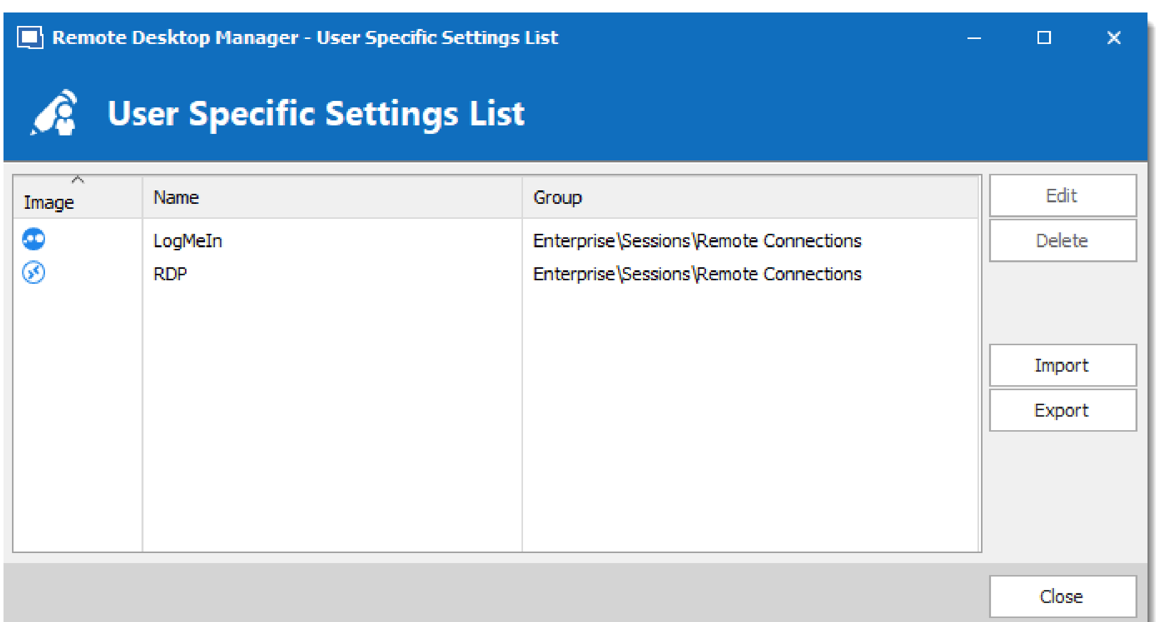


Credentials - My personal credentials

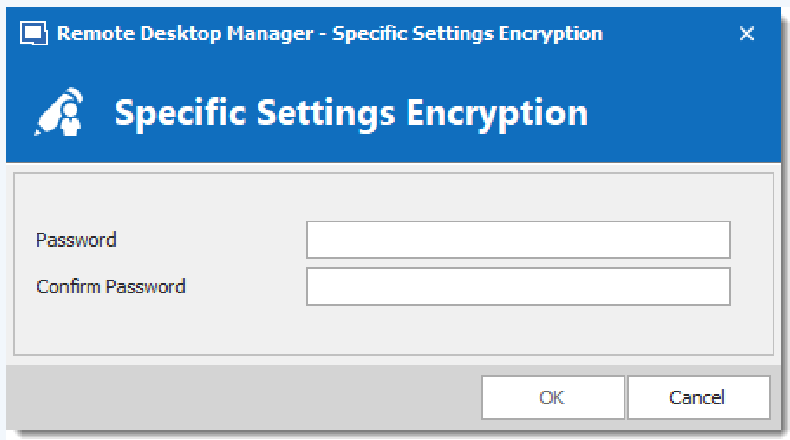
6.2.9.2 User Specific Settings List

DESCRIPTION

The **User Specific Settings List** feature will provide all entries that are overridden with user Specific Settings.



User Specific Settings List dialog

OPTION	DESCRIPTION
Edit	Edit the selected User Specific Settings.
Delete	Delete the selected User Specific Settings.
Import	Import a list of user Specific Settings from a .rds file. As this file is encrypted using a mandatory password, you will have to provide the password to successfully import the content of the .rds file.
Export	Export a list of user Specific Settings into a .rds file. A password is required to encrypt the .rds file. 

6.2.10 Import

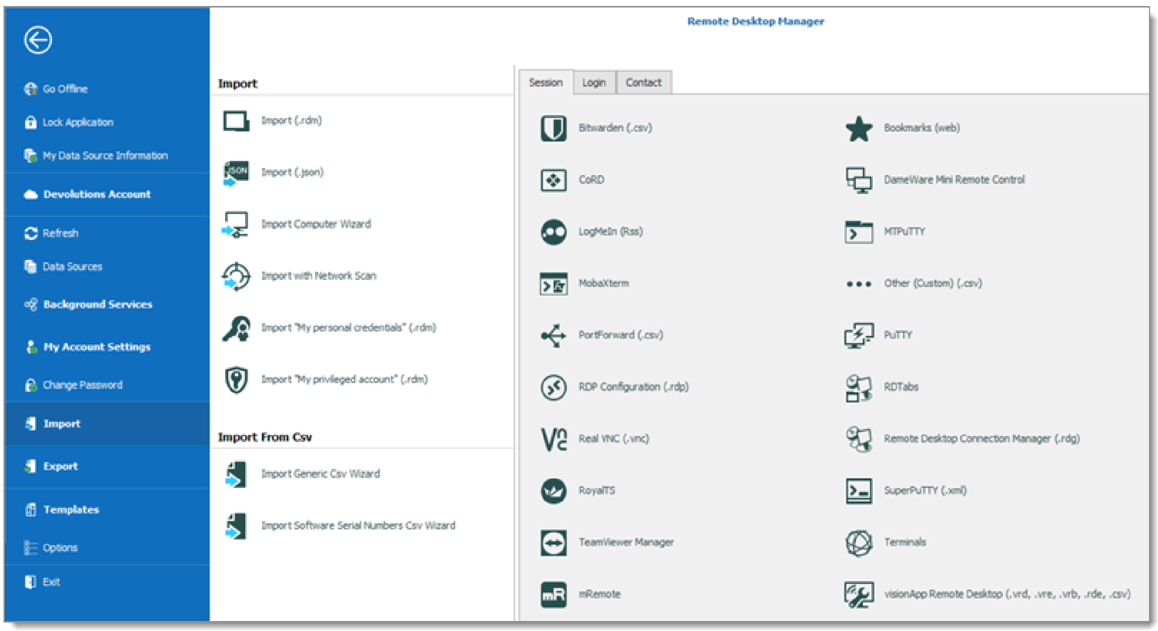
DESCRIPTION

Use the ***File - Import*** to import entries in Remote Desktop Manager. You can import entry types from multiple sources.

We support native import formats from many popular tools on the market. In case we don't support the native format, or don't support the third party, we have wizards to import from a csv file.

The import feature is only active if the import ***Privileges*** has been enabled inside the user account.

SETTINGS



IMPORT (.RDM)

Import is used to import sessions stored in .rdm files who is Remote Desktop Manager native export format.

IMPORT (.JSON)

Import sessions from a .json file format.

IMPORT COMPUTER WIZARD

You can import session from computers from different sources. These sources include:

- Network neighborhood

* Active Directory
* Host list

Please refer to Import Computer Wizard for more information.

IMPORT WITH NETWORK SCAN

The ***Import with Network Scan*** allows you to perform a network scan based on a predefine range of IP address to find sessions to import. Consult the topic Import with Network Scan to learn more about this option.

IMPORT "MY PERSONAL CREDENTIALS" (.RDM)

Import your ***My Personal Credentials*** from a .rdm file.

IMPORT FROM CSV

Import entries from a .csv file. Please refer to Import Generic CSV Wizard for more information and strategies.

IMPORT SESSIONS, LOGINS AND CONTACTS

* Import Sessions
* Import Logins
* Import Contacts

6.2.10.1 Import Computer Wizard

DESCRIPTION

This feature is only available when using an Advanced Data Source.

The ***Import Computer Wizard*** allows you to create sessions for computers using one of the following sources:

- Network neighborhood.
- Active directory: Your current domain or another domain on your network.
- Host list: List of computers from a file.

OVERVIEW

The wizard has a few major-steps:

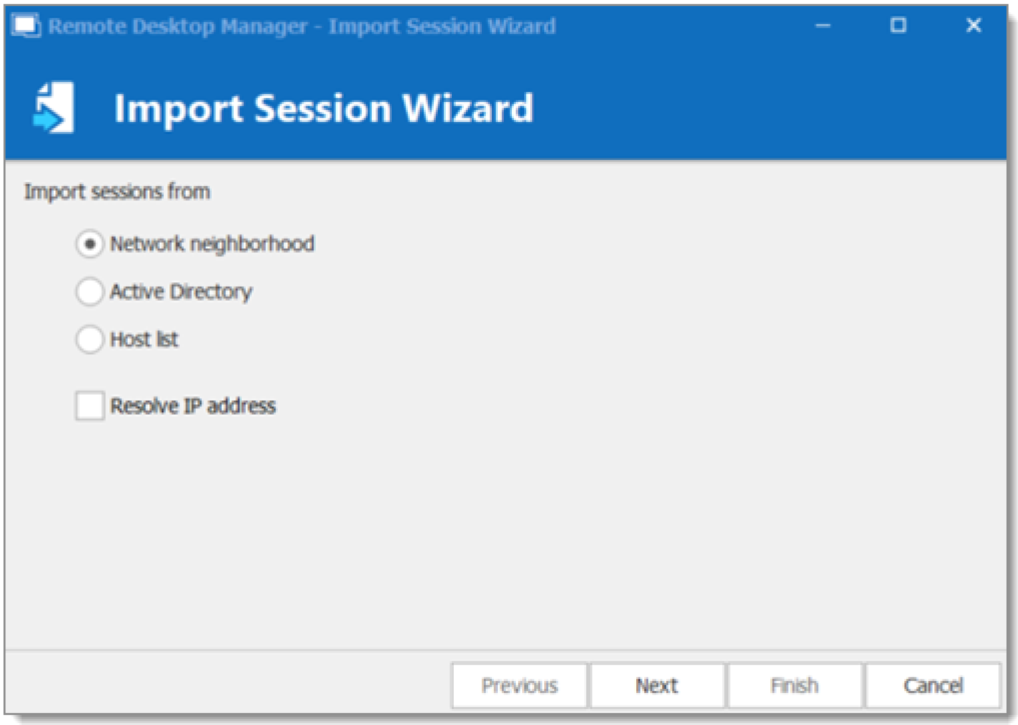
1. Select computers by using one of the three sources;
2. Optionally apply a template from which to base new sessions on; and
3. Optionally edit each newly created session prior to them being saved.

The template selection should not be overlooked, in fact, it is probably the most important step to ensure your newly created sessions are usable right after being created. You should divide the sessions in batches based on which template you need to apply and import one batch at a time.

WORKFLOW

Upon launching the wizard, you are prompted for the source to use.

The ***Resolve IP address*** option must be checked if you want to use the IP address in the host field of your sessions instead of the host name.

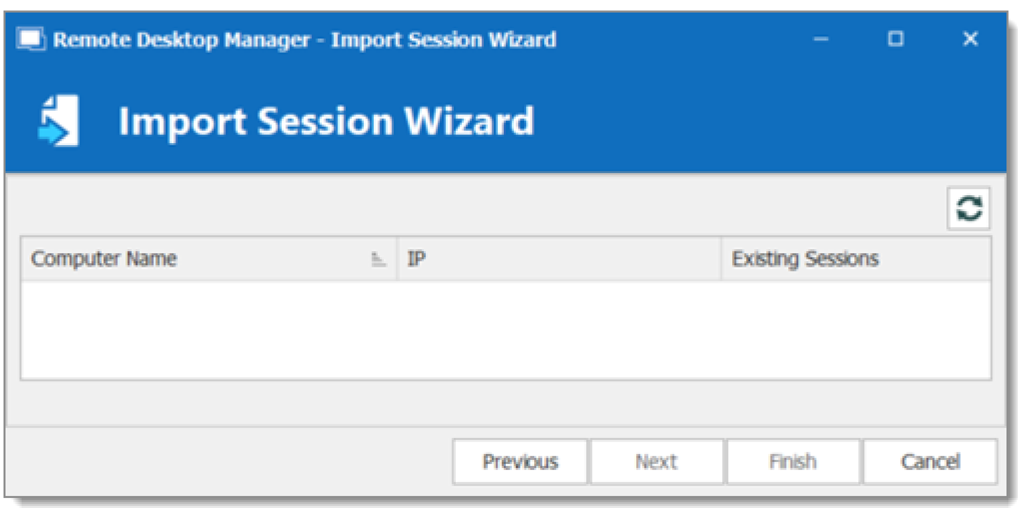


Import Session Wizard

Refer to the sections below depending on the chosen source.

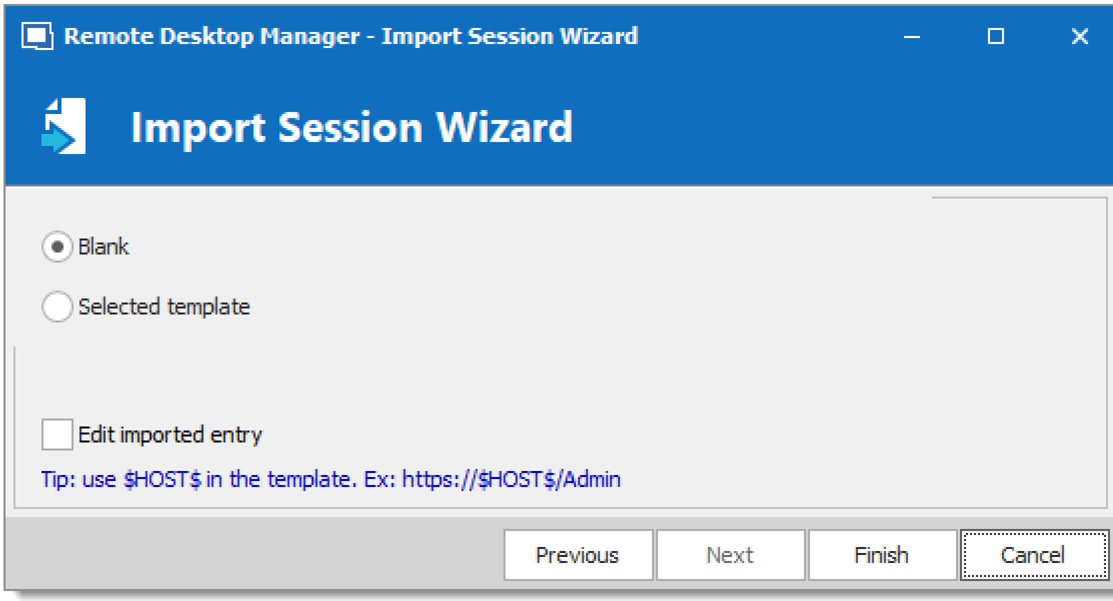
NETWORK NEIGHBORHOOD

The next screen will immediately be populated with the result of the network discovery.



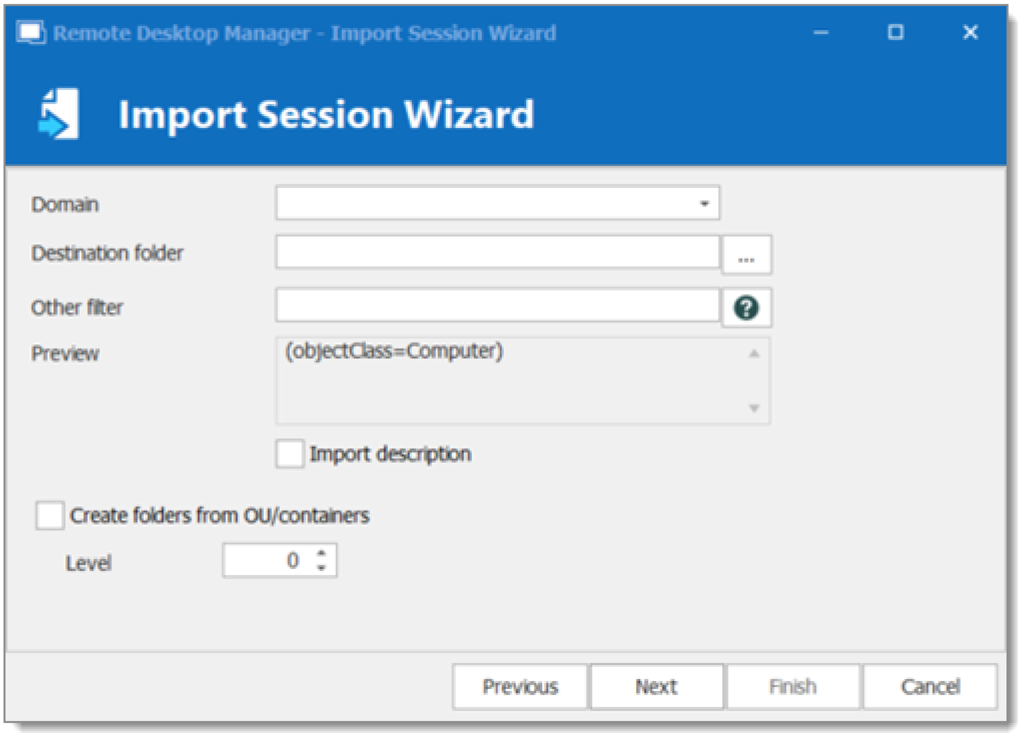
If you prefer your sessions to use the IP address instead of the Host name to connect to the devices, check the ***Select by IP address*** option. This requires that the ***Resolve***

by IP address was selected in the first screen of the wizard. Select the computers for which you want to create session and proceed to Template Selection below. Multi-select is allowed by using CTRL-click and SHIFT-click.

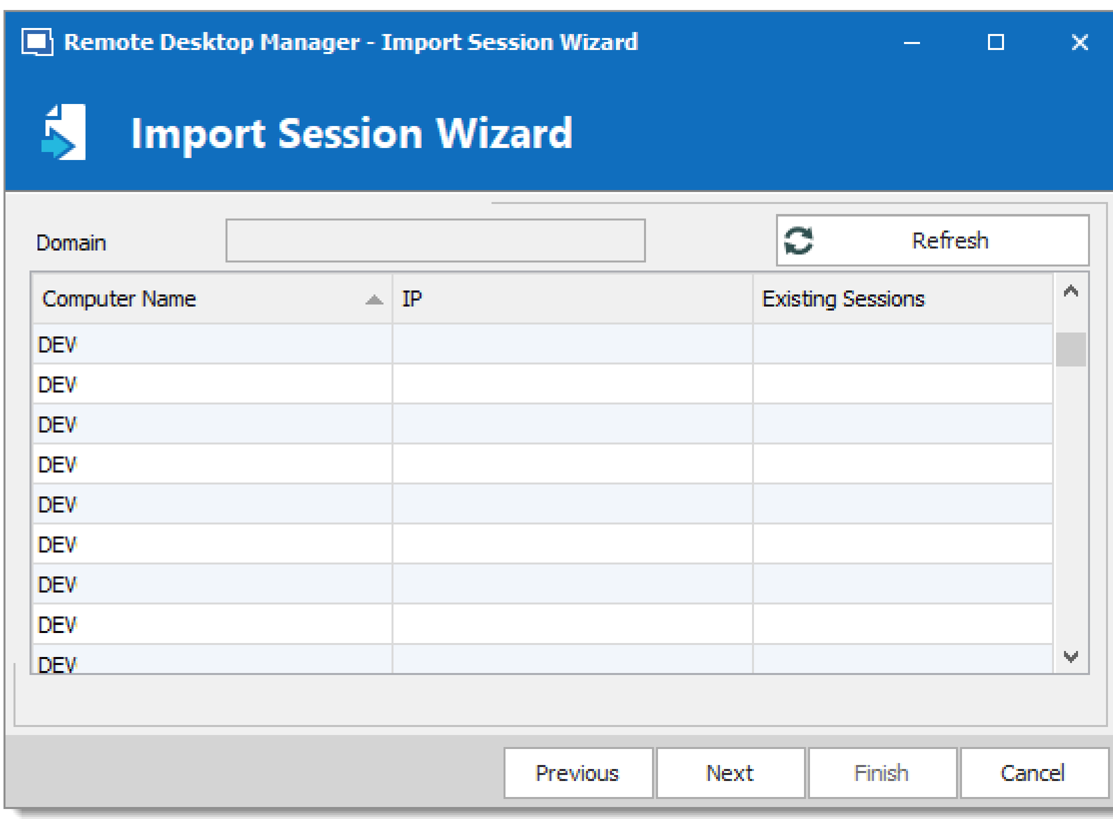


ACTIVE DIRECTORY

The following screen allows you to select the domain to interrogate after which you must press refresh to load the list of computers that are available.



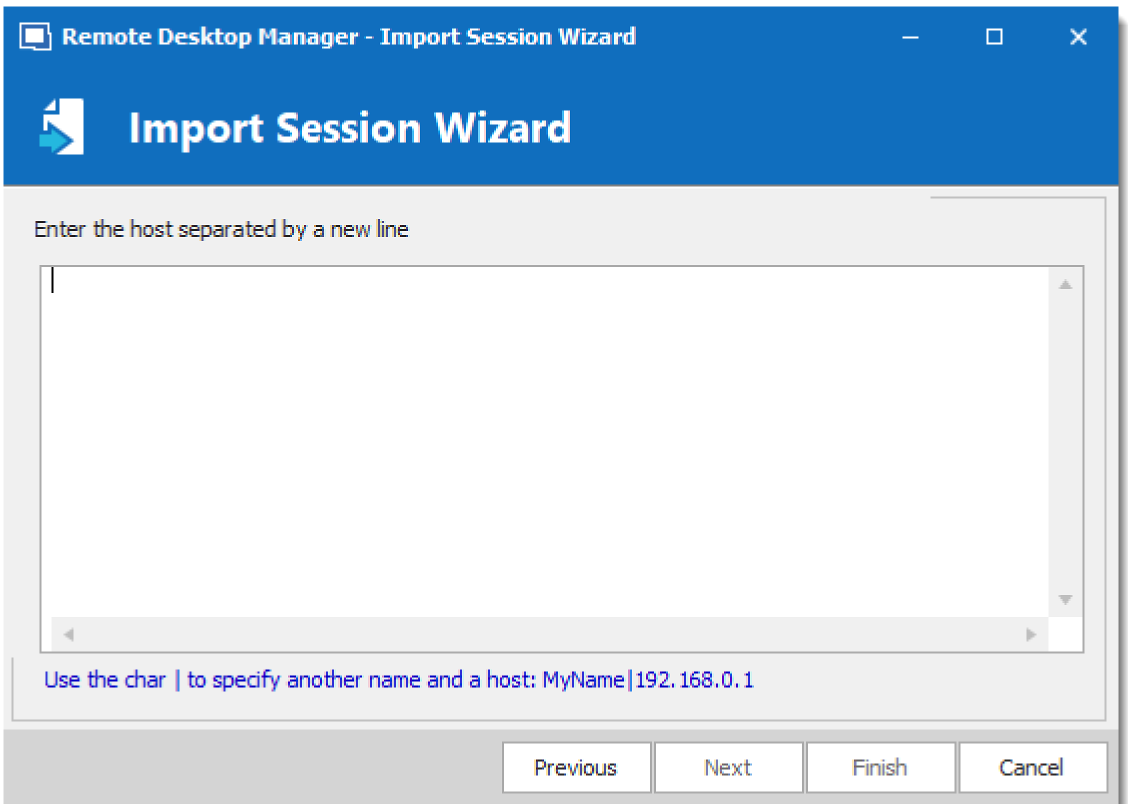
After the query is executed, the results are displayed in the grid.



If you prefer your sessions to use the IP address instead of the Host name to connect to the devices, check the ***Select by IP address*** option. This requires that the ***Resolve by IP address*** was selected in the first screen of the wizard. Select the computers for which you want to create session and proceed to Template Selection below. Multi-select is allowed by using CTRL-click and SHIFT-click.

HOST LIST

The following screen allows you to enter a list of hosts in an Edit control. If you prefer that your sessions use the IP address to connect to the hosts, you must enter the host name, a pipe, then the IP address.



Proceed to Template Selection below.

TEMPLATE SELECTION

The template selection is an optional step, but it's the only way that you have to choose a protocol type other than RDP. It also allows you to set your preferences and have them used by all the created sessions. In fact, we recommend you to import in batches for each of the session type that you need to import.

If you intend to modify each of your imported sessions as they are created, check the ***Edit*** imported entry option. Note that each session will be displayed sequentially so you can perform your modification and save. A Batch Edit is probably preferable if you have more then a few sessions to import.

6.2.10.2 Import Generic CSV Wizard

DESCRIPTION

The ***Generic CSV Wizard*** has been greatly enhanced to support not only all entries general fields but also subfields. This gives you access to all properties, even for types provided by add-ons, therefore unknown by Remote Desktop Manager.

> For a review on the CSV file format, and the impact of decisions made in this entry, please consult Import Strategies and File Format

SETTINGS

1. In your ***Navigation pane***, select the ***Vault*** you want to import the sessions in.
2. Go to ***File - Import - Import Generic Csv Wizard***.
3. Select the CSV file to import and click ***Next***.
4. Validate and click ***Finish***.

The import will proceed using your chosen settings.

6.2.10.2.1 Import Strategies and File Format

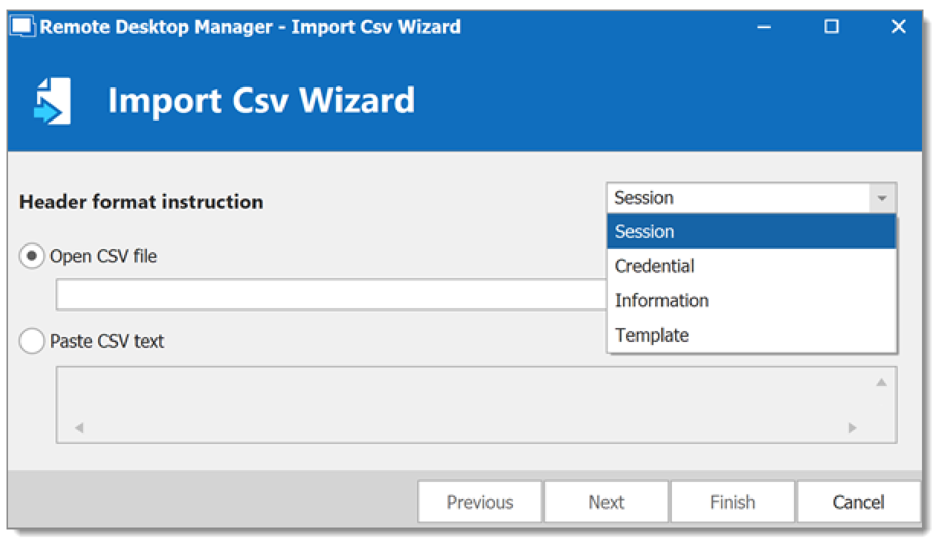
DESCRIPTION

The most important decision is about **if** and **how** to apply a template as part of the process.

Both methods of importing from CSV allows you to choose a template for newly created entries. If you do choose a template as part of the process, it will be apply to **ALL** entries created from that batch. Sometimes, it may be a good strategy to split the entries in different CSV files by grouping them by type of entries you wish to create.

If you need finer control, you can specify the template to use in a **Template** column of the CSV file. But since you're able to specify the entry type from within the CSV file it may not be necessary.

In ***File - Import***, we recommend you use the ***Import Generic Csv Wizard*** option first. You can modify, if needed, the ***Header format instruction***.



COLUMNS

Some validations on entry settings are not in the business layer but rather in the property dialogs. This means that using the import process can result in invalid entries that trigger errors. Please validate the resulting entries carefully.

In the CSV file, the ***Host*** and the ***Name*** field are mandatory. If no template is specified, the RDP type will be used as a fallback type.

We cannot provide the list of all supported fields for all entry types because Remote Desktop Manager uses an open architecture and therefore is not even aware of all the fields of entry types that are provided by our Add-On system. A good method of finding out the field structure is to create an entry of the desired type and to use ***Clipboard – Copy***, then paste the content in your favorite editor. You will see the structure and the field names.

Default values for fields are **NOT** serialized. This means that they are simply left out of the serialized structure.

Implementing support for all fields comes at a cost. The import process is time consuming because of all the dynamic field access that takes place. A massive initial import of entries should be separated in batches of manageable size. Please perform trials and tune the number of entries to achieve acceptable performance.

All of our entries share a basic set of fields, the rest are tied to the specific technology being interfaced with (RDP, SSH, etc). Some fields are grouped in structures like the Information Tab for instance. This means that those fields are accessible only when providing the structure name as a prefix, for example: "**MetaInformation\OS**" or "**MetaInformation\PurchaseDate**"

Note that the content of the CSV file can contain our variables and they will be resolved upon saving. For instance you could use the **$HOST$** variable in fields like **Description**, **URL**, **Putty\CustomSessionName**, etc. It will be replaced by the corresponding value.

Here is a list of some relevant fields.

OPTION	DESCRIPTION
Host	Host name of the device, **this is a mandatory field**.
Name	Name of the entry, **this is a mandatory field**.

OPTION	DESCRIPTION
ConnectionType	Token representing the connection type. It is best to use the ***Clipboard-Copy*** method to obtain the acceptable values.
Group	Destination folder. Note that if the import process itself had a Destination Folder defined as well, the folder listed here would be created below the one from the process.
Description	Description of the entry.
Open (Embedded)	Boolean value (**true** or **false**) that indicates to open the session embedded. The default value is false, meaning that the native client will be used depending on the technology. MSTSC.EXE for instance.
Username	Username used to open a session to the device.
Domain	Domain used to open a session to the device.
Password	Password used to open a session to the device. Please note that this field is encrypted and stored into another field upon being imported.
MetaInformation\SerialNumber	Serial Number of the device.
MetaInformation\ServiceTag	Service Tag of the device
MetaInformation\PurchaseDate	Purchase date in a ISO8601 format, i.e. yyyy-mm-dd

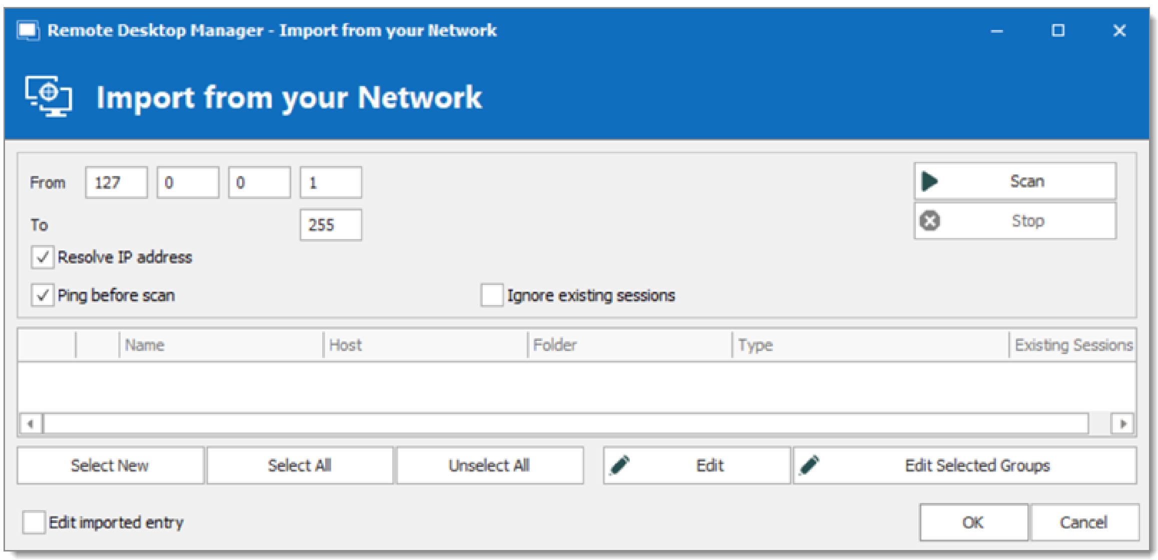
6.2.10.3 Import with Network Scan

DESCRIPTION

The ***Import with Network Scan*** allows you to perform a network scan based on a predefine range of IP address to find sessions to import.

Once the scan is completed select the sessions, you wish to import (by default every session will be selected) and click on ***OK*** to import those sessions in your data source.

If you wish to review each and every session as they are imported you can check the ***Edit imported entry***. However we do not recommend this for large number of sessions.



6.2.10.4 Import Sessions

DESCRIPTION

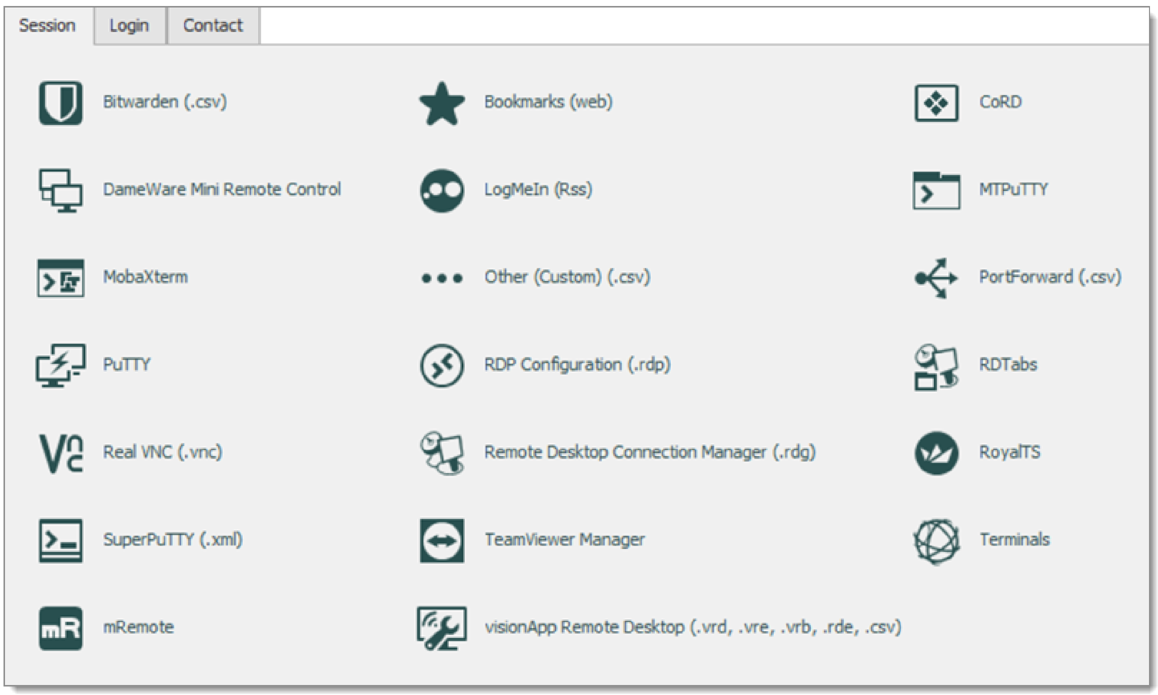
Use ***File - Import - Session*** to import sessions from other software into Remote Desktop Manager.

The import feature is only active if the import ***Privileges*** has been enabled inside the user account.

You can import your sessions from an existing application or an existing file format. Some application encrypt the data but it must be in plain text to allow the application to parse the content.

All entries will be imported in the current folder.

For some applications it's not possible to extract the password.



6.2.10.5 Import Logins

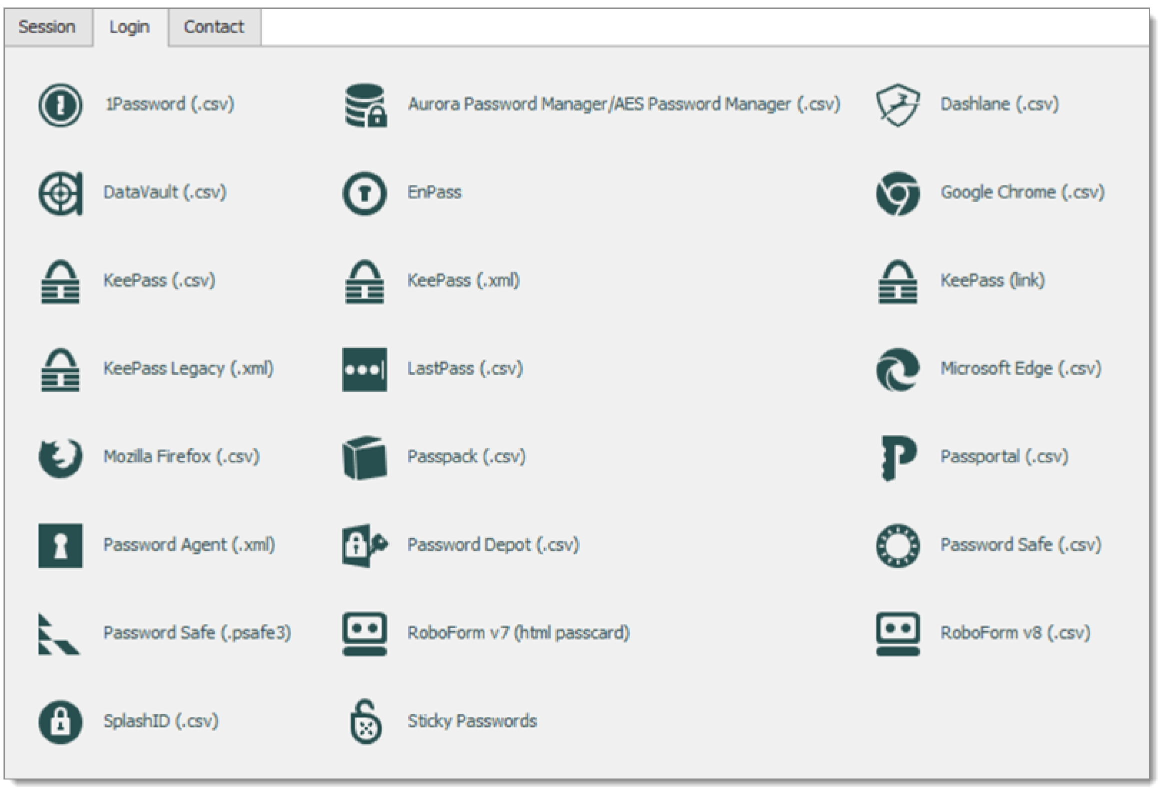
DESCRIPTION

Use ***File - Import - Login*** to import different logins or credentials from other software into Remote Desktop Manager.

The import feature is only active if the import ***Privileges*** has been enabled inside the user account.

You can import the credentials from a wide array of formats exported by various password management solutions. The export content must not be encrypted in order to parse the content.

All the entries will be imported in the current folder.

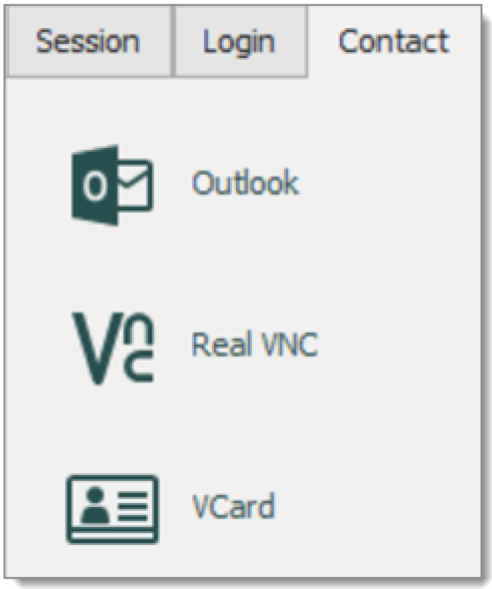


6.2.10.6 Import Contacts

DESCRIPTION

Use ***File - Import - Contact*** to import contacts from other software into Remote Desktop Manager.

The import feature is only active if the import ***Privileges*** has been enabled inside the user account.



IMPORT FROM CONTACT

It's possible to import the contact from different sources:

- Outlook
- Real VNC
- VCard

All the entries will be imported in the current folder.

Outlook contacts subfolders are also supported.

6.2.11 Export

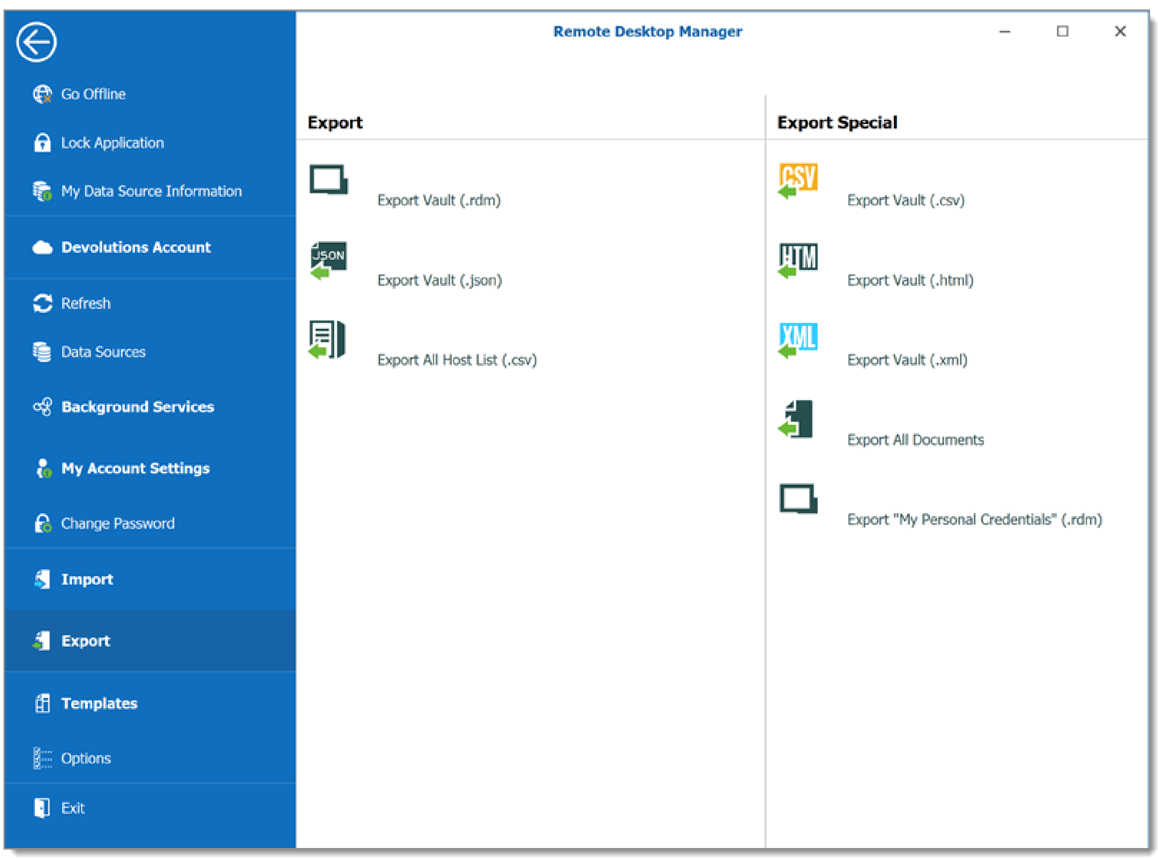
DESCRIPTION

Use ***File - Export*** to export vaults from Remote Desktop Manager.

The export feature is only active if the ***Import*** and ***Export Privileges*** has been enabled inside the ***User Management*** account.

The only appropriate formats to import vaults back into Remote Desktop Manager are the .rdm and .rdx format.

SETTINGS



File - Export

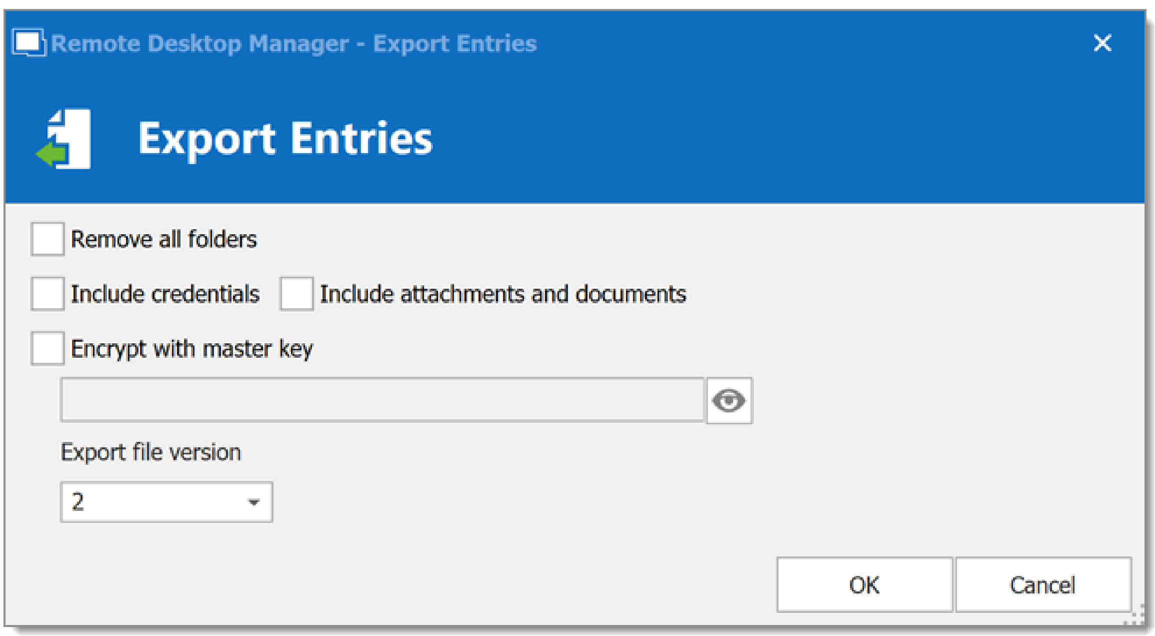
When using an Advanced Data Source, export capabilities can be disabled via security policies at the data source level (no one can export) or at a user level (particular users can't export).

EXPORT VAULT (.RDM)

Export a vault in a .rdm file that can be imported into any Remote Desktop Manager data source. You can also include credentials in this export format and secure your file with a master key.

By default the credentials are NOT included. It's critical to check the ***Credentials*** option in order for the exported data to include the credentials.

Specifying a ***Master key*** will encrypt the whole content of the .rdm file to protect its content. It is highly recommended as a backup measure, but the key is absolutely necessary for decryption. Preserve this as well in a separate storage device for safekeeping.



EXPORT VAULT (.JSON)

Export a vault in a .json file format. You can also include credentials in this export format and secure your file with a master key.

EXPORT ALL HOST LIST (.CSV)

Export a simple host list in .csv format. You will be prompted to see if you wish the export to be slightly more detailed and include the following information: Host, Description, Display Name, Group, Security Group.

EXPORT VAULT (.CSV)

Export the vault using the .csv format file. For security reasons the .csv file will be contained within a password encrypted zip file. This type of security can be hacked using brute force attacks, it should be used only when the zip file is under your exclusive control.

> Please note that the csv columns will vary depending on entry types being exported. This makes it the wrong format if ever you want to import the data back in Remote Desktop Manager. Use this only to migrate to another system.

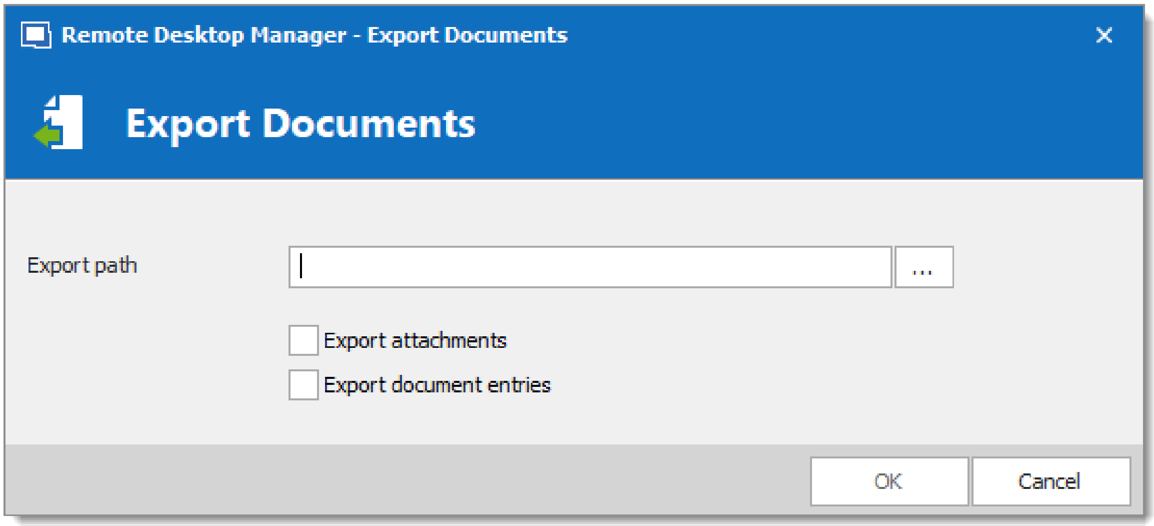
EXPORT VAULT (.HTML)

Export the vault with an AES-256 to encrypt self contained html file. See Export Html Encrypted topic for more information.

EXPORT VAULT (.XML)

Because it brought confusion to our user base, this export format has been converted to perform the exact same export as the ***Export Vault*** but sets the file extension to .xml instead.

EXPORT ALL DOCUMENTS



Export Documents

Export all attachments or all document entries that are linked to your data source.

EXPORT "MY PERSONAL CREDENTIALS" (.RDM)

Export your ***My Personal Credentials*** in a .rdm file and encrypt with a ***Master key***.

> A ***Master key*** will encrypt the .rdm file to protect its content. The key is absolutely necessary for decryption.

6.2.11.1 Encrypted Html

DESCRIPTION

The Html Encrypted export format was designed for simple and secure exports of entries. It allows for an html export of the entry information while using symmetric encryption (AES-256) to encrypt sensitive information such as passwords. The file is an ultra portable self contained html file that requires no external script files or installs. As long as you have a web browser with JavaScript enabled, you can get to your encrypted data.

With a secure encrypted document, you can freely send the information via email or any other protocol without compromising the sensitive data. Use the export as means of sharing or as a backup for sensitive information.

SETTINGS

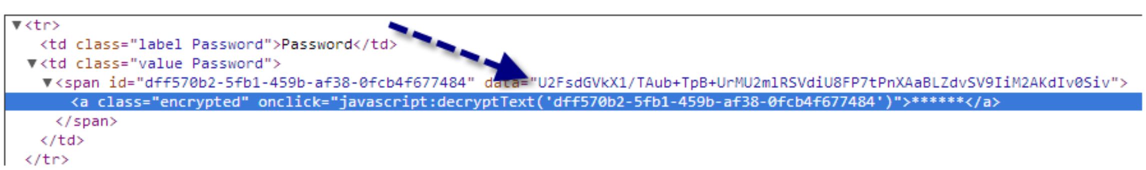
Select the entries to export or export the vault. ***Right-click*** and select ***Export - Export Special - Export Selection (.html)*** or use ***File - Export - Export Vault (.html)***. You will be prompted for a password for the symmetric encryption key. Select the file name for the new document. Once the export is completed, the file will open in your default browser.

Ensure you do not forget the password as you will not be able to decrypt the data without it.

When exporting multiple entries that are all contained within the same file, at decrypt time, each encrypted value must be decrypted individually for security reasons. Once you're done with the sensitive data simply hit **F5** to refresh the file or simply close it. Your data is now safe from prying eyes.

AES-256

We use AES-256 to encrypt/decrypt your sensitive data. Since the decryption is done entirely in the browser, there’s no need for external tools, downloads or installs.



Encrypted Value

SAFE & SMART VIRTUAL BACKUP

In addition, HTML Export using symmetric encryption is a great way to securely backup your passwords and other sensitive information. It allows you to share information via email or simply send the file to your personal email account as a backup.

6.2.12 Templates

DESCRIPTION

Templates are useful to have predefined values when creating an entry. Use templates to:

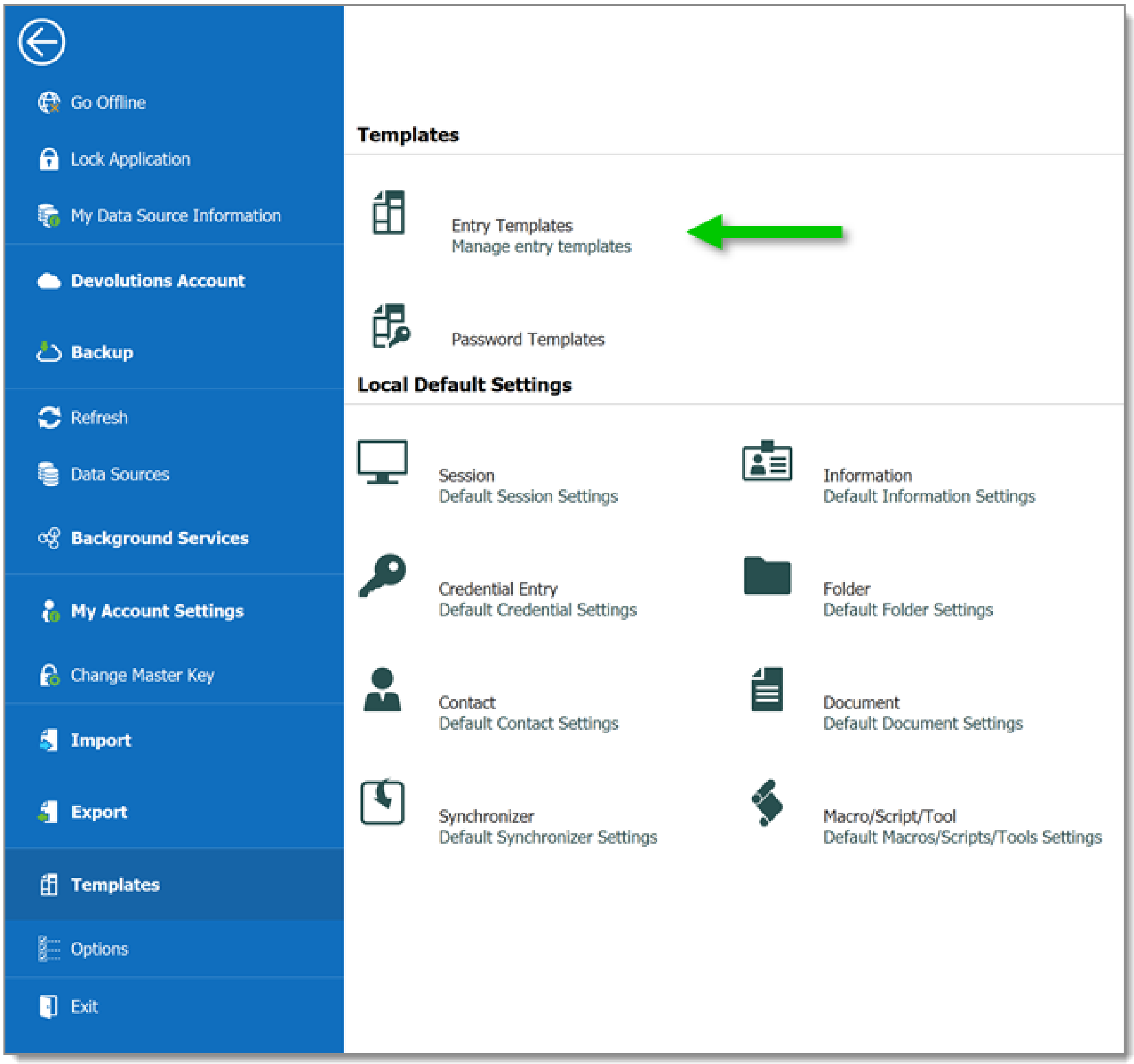
- Add preconfigured entries
- Use with the Quick connect feature
- Open entries as a template
- Create password templates

To access and manage templates, navigate to ***File - Templates***.

It's possible to create local and database templates.

- Local templates are saved in the Remote Desktop Manager configuration file. They are available only to the current user of the machine.
- Database templates are saved in the database. They are available to all users of the data source.

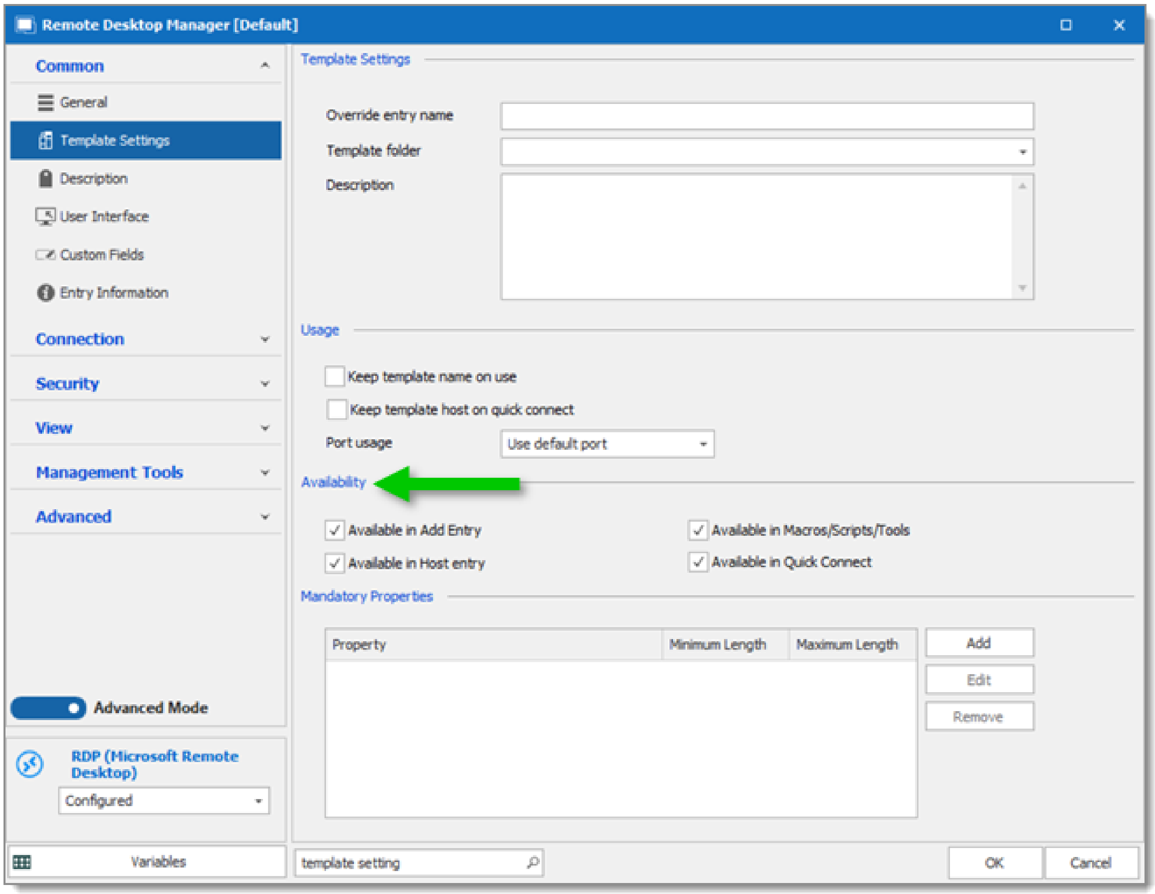
> By default, standard users cannot create or manage templates. To allow users to create or manage templates, the permission must be granted to users using the ***Administration - Templates*** section of the System Permissions.



File – Templates

AVAILABILITY

When creating a template, its availability can be specified in the ***Template Settings***.

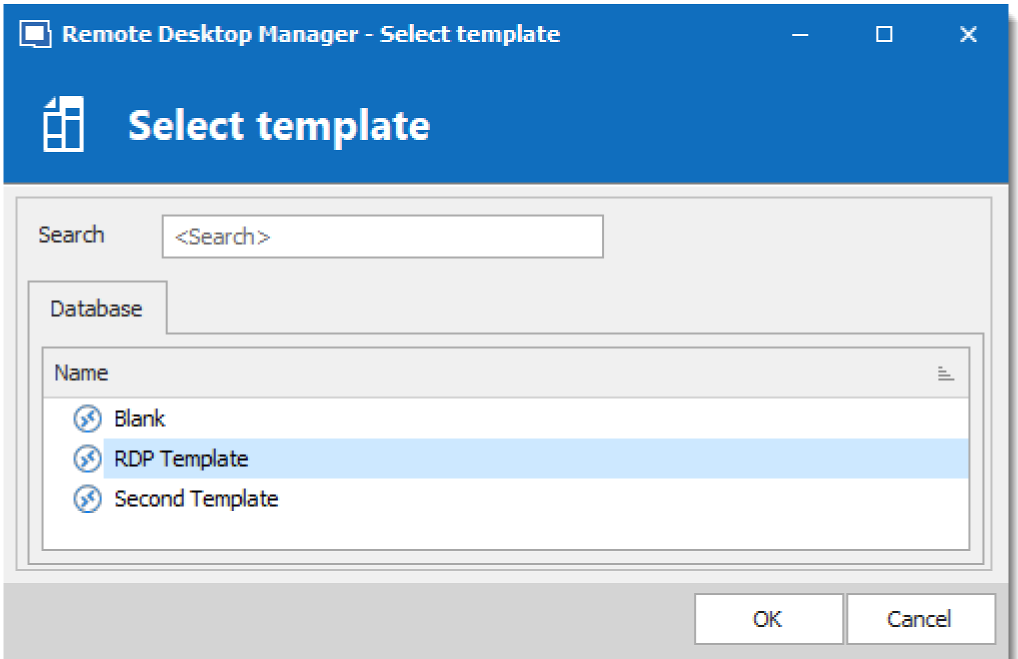


USAGE

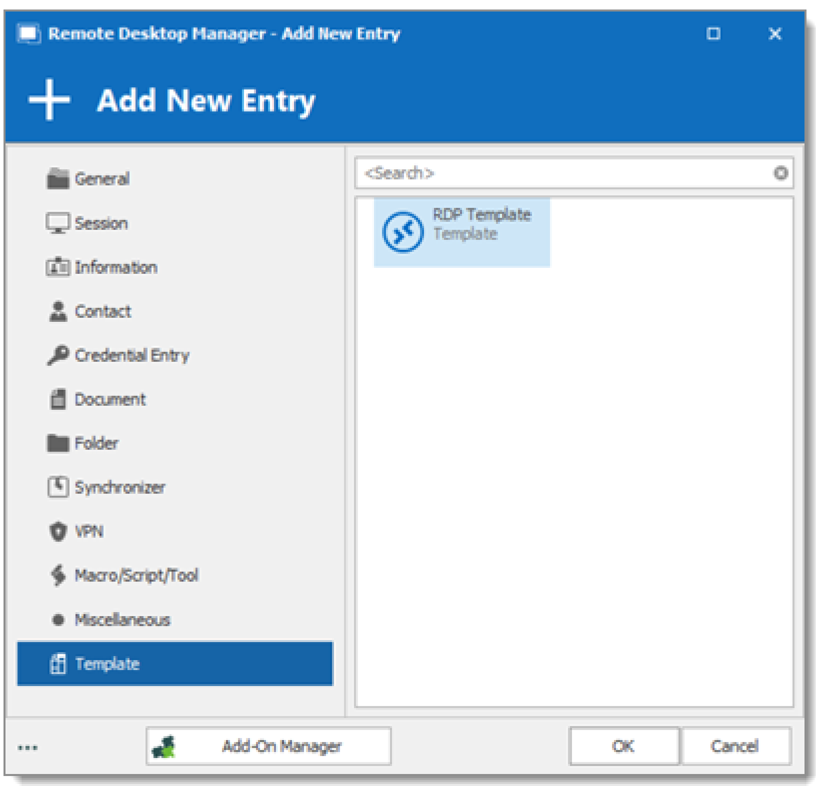
Templates can be used in the following cases:

CREATE A NEW ENTRY

By default, when creating an entry of a type that has templates configured for, the user is prompted for a template to use. This behavior can be modified in the System Settings.

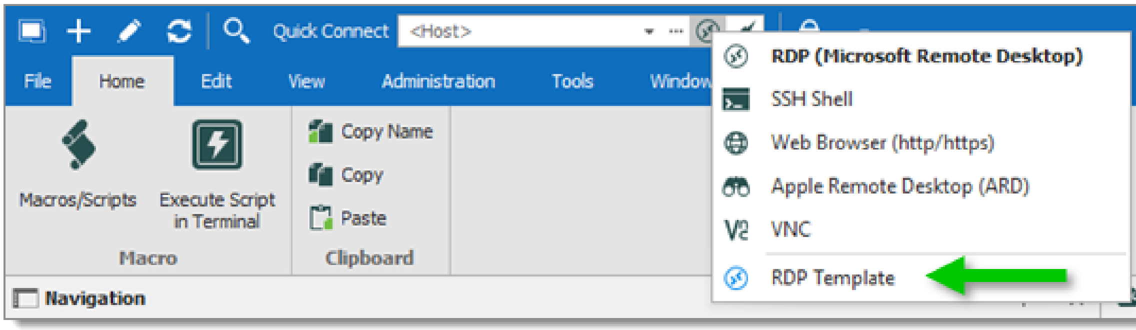


The template can be selected before creating the entry as well. Use the ***Template*** section of the ***Add New Entry*** window.



RUN A QUICK CONNECT SESSION

Templates can be used with the ***Quick Connect*** feature. For example, the same template can be used to connect to different hosts.



6.2.12.1 Creating Templates

DESCRIPTION

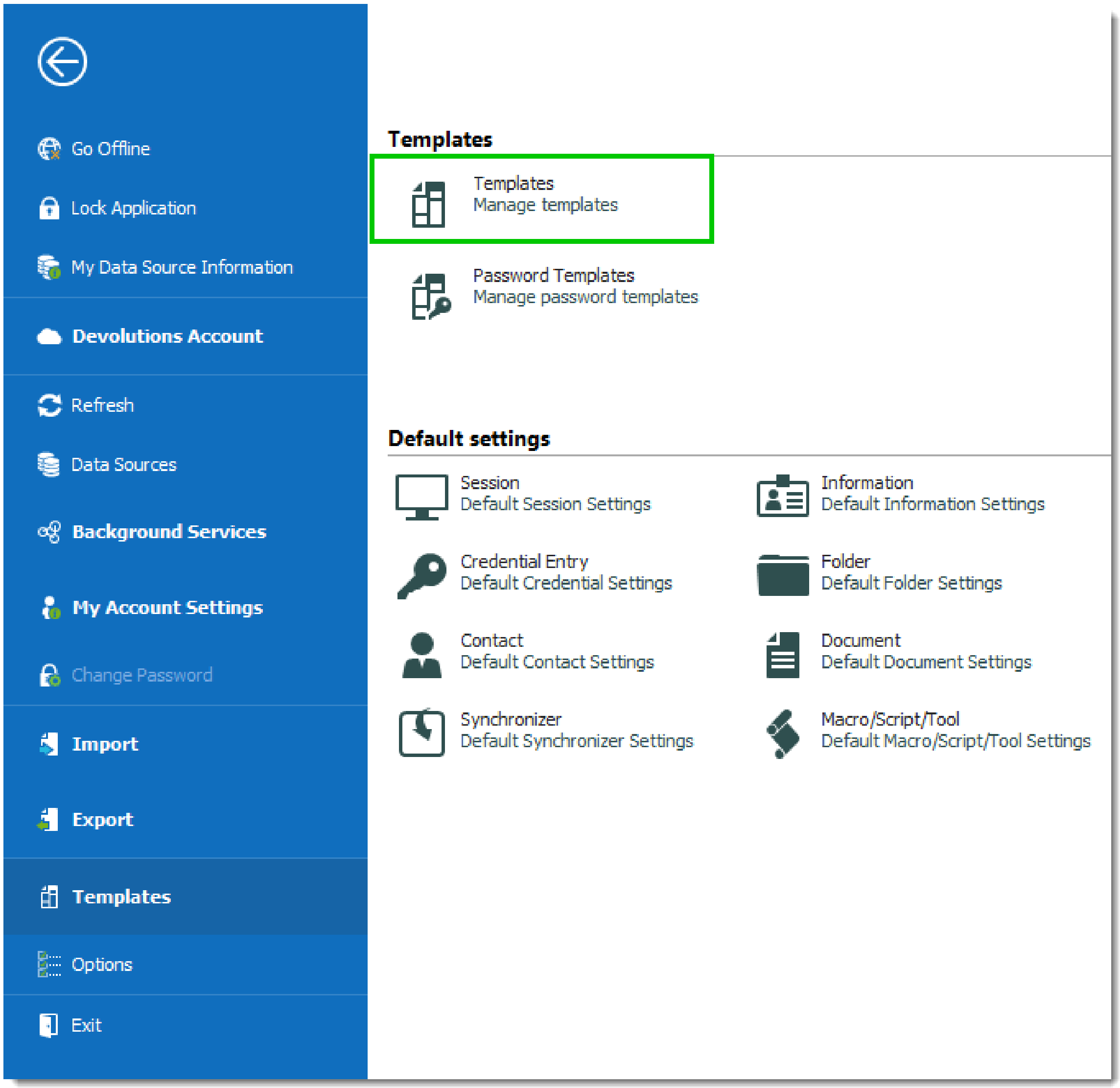
There are many ways to create template for entries. You can create a new template, save an entry as a template, import entries as templates, and duplicate a existing template. It is also possible to create group templates.

In this topic:

- New Template
- Save as Template
- Import Template
- Duplicate Template
- Template Groups

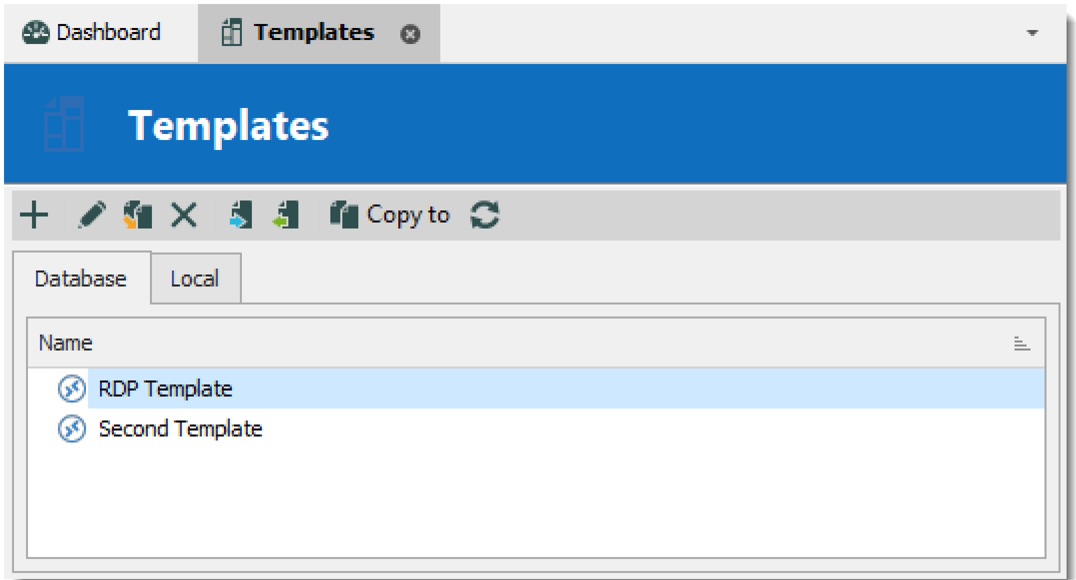
CREATE A NEW TEMPLATE

1. Navigate to ***File – Templates*** and select **Templates**.



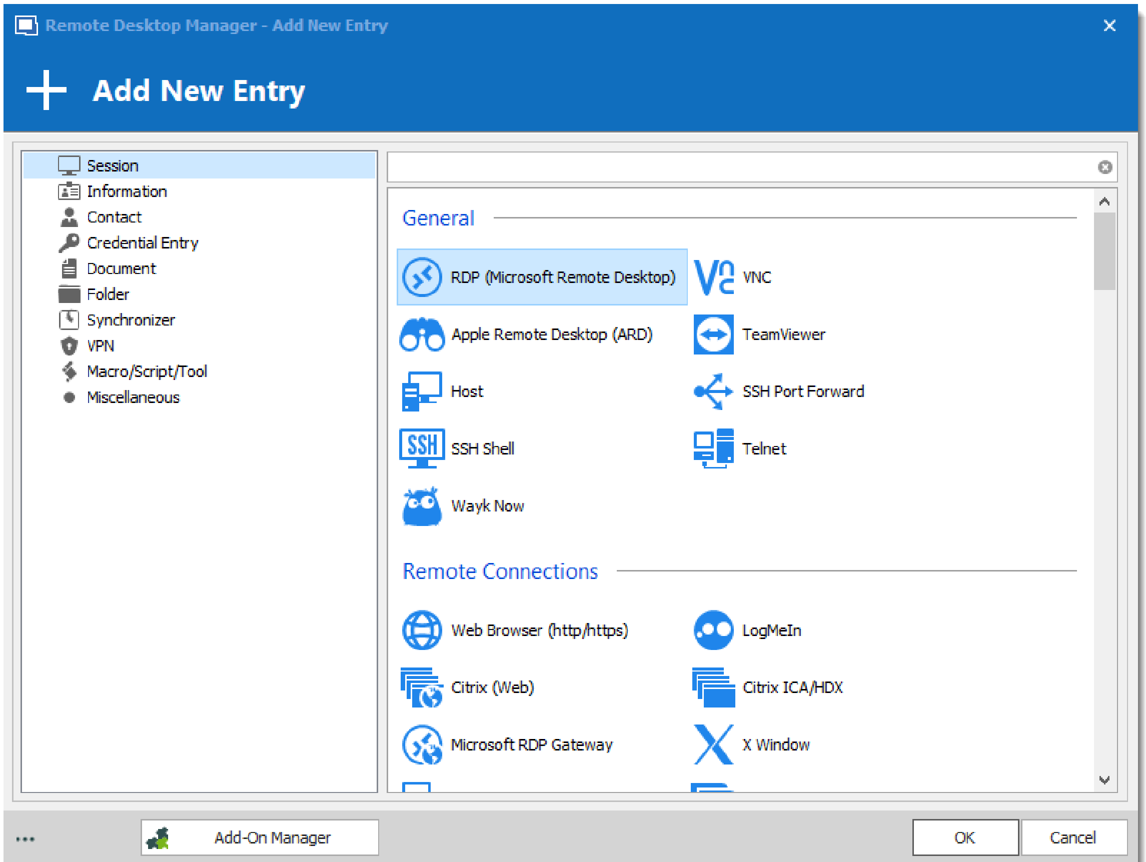
File – Templates

2. In the **Templates** window, click the **Add template** ✚ button.



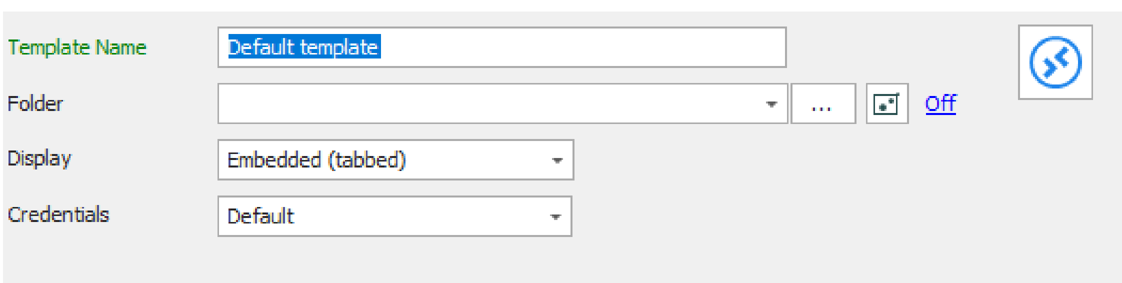
Add a new template

3. Select an entry to create the template for.



Select an entry to create the template for

4. Enter a name for the template, and configure the properties as necessary.

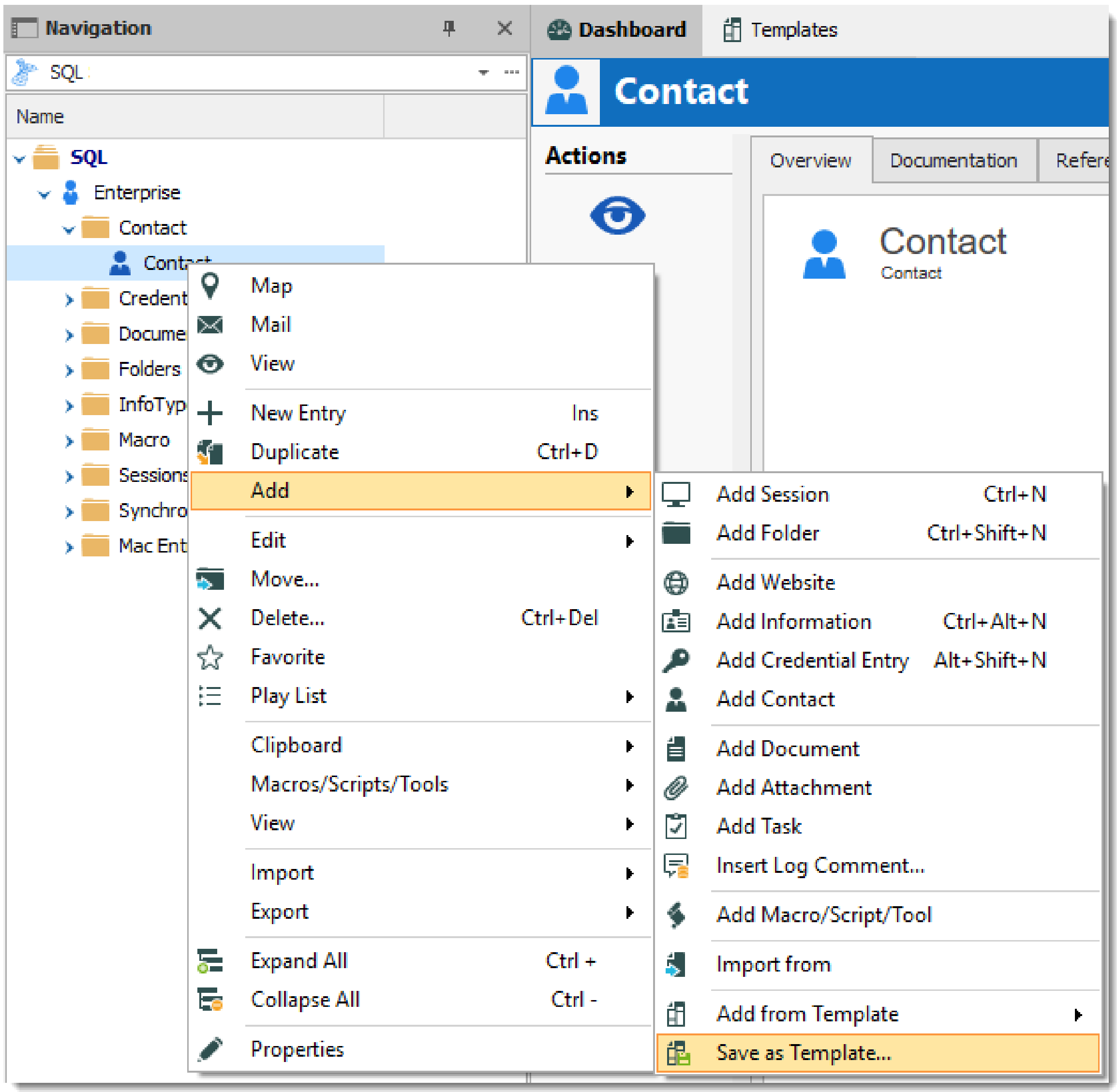


Template Properties

SAVE ENTRY AS TEMPLATE

It is possible to save entries as templates to use their properties in other entries. Furthermore, this can be achieve on folders to include all their child items in the template.

From the Navigation Pane, **right-click** an entry and select ***Add – Save as Template...***



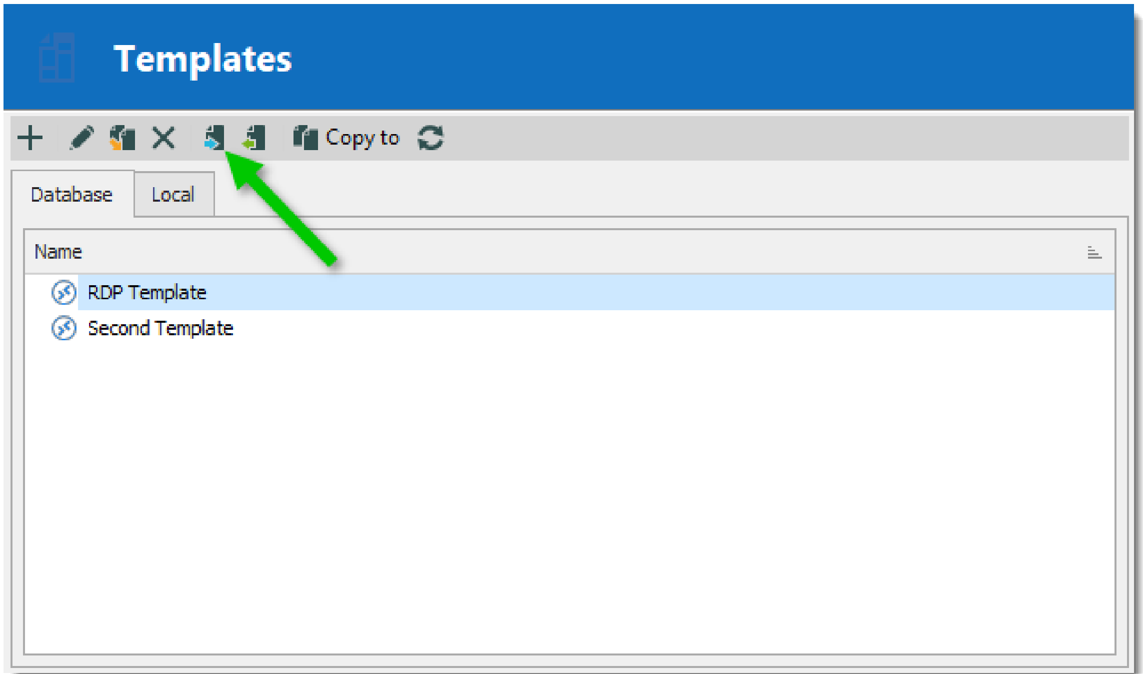
Save as Template...

IMPORT TEMPLATE

It is possible to import previously exported entries as templates.

1. Navigate to ***File – Templates***, and select **Templates**.

1.1. From the **Templates** window, click on the **Import template** button.



Import Template

2. Select the ***.rdm** file to import to create a template for each entry in the file.

DUPLICATE TEMPLATE

It is possible to duplicate a template to edit a copy of the properties.

Navigate to ***File – Templates***, and select **Templates**. From the **Templates** window, click on the **Duplicate template** button.

Change the template name to distinguish the copy from the original, and edit the properties to meet your requirements.

TEMPLATE GROUPS

It is possible to save a set of selected entries or a folder and all its child items to a unique template.

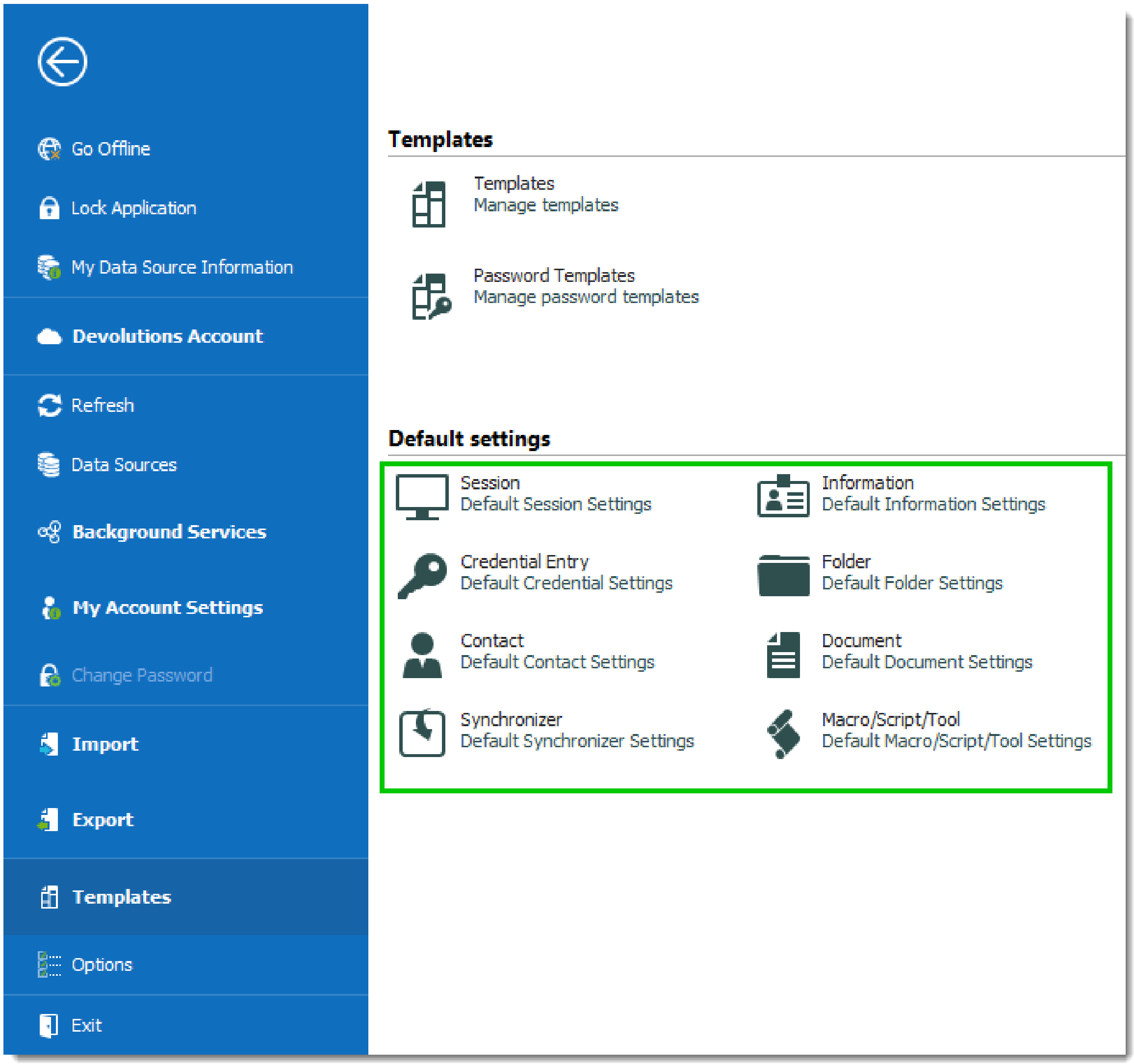
Right-click a selection of entries or a folder, select **Add**, then **Save as Template...**

6.2.12.2 Default Settings

DESCRIPTION

Default Templates create default settings for new entries. Every entry type is supported and can have a default settings template defined.

- **Session**
- **Information**
- **Credential Entry**
- **Folder**
- **Contact**
- **Document**
- **Synchronizer**
- **Macros/Scripts/Tools**



File - Templates - Default settings

SETTINGS

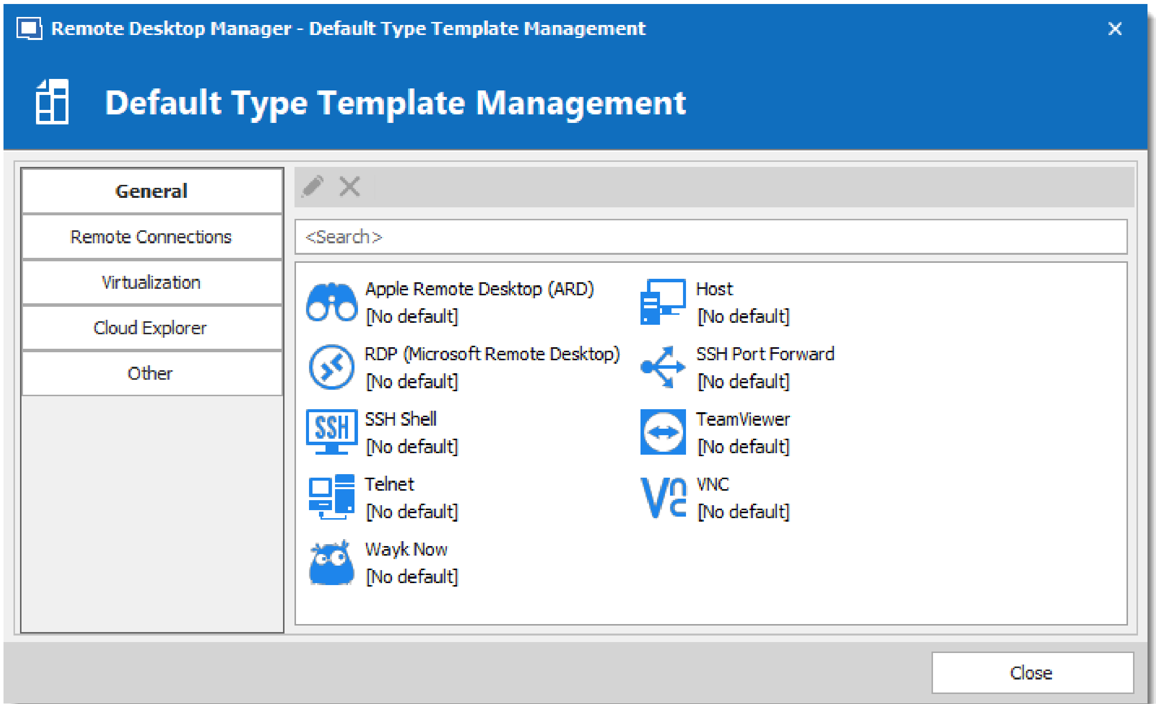
To help you locate the entry type you want to customize, all entry types are organized by category.

Select a category of entry from the ***File – Templates*** menu, then select the specific entry type to be edited.

Please note that a **[No default]** notice is displayed below each type that does not have a default template defined.

All entry types without the **[No default]** notice have a default template. You can double-click on the type to edit the template or press the edit  button.

If you want to remove the default settings template, press the delete button.



Default Type Template Management

6.2.12.3 Password Templates

DESCRIPTION

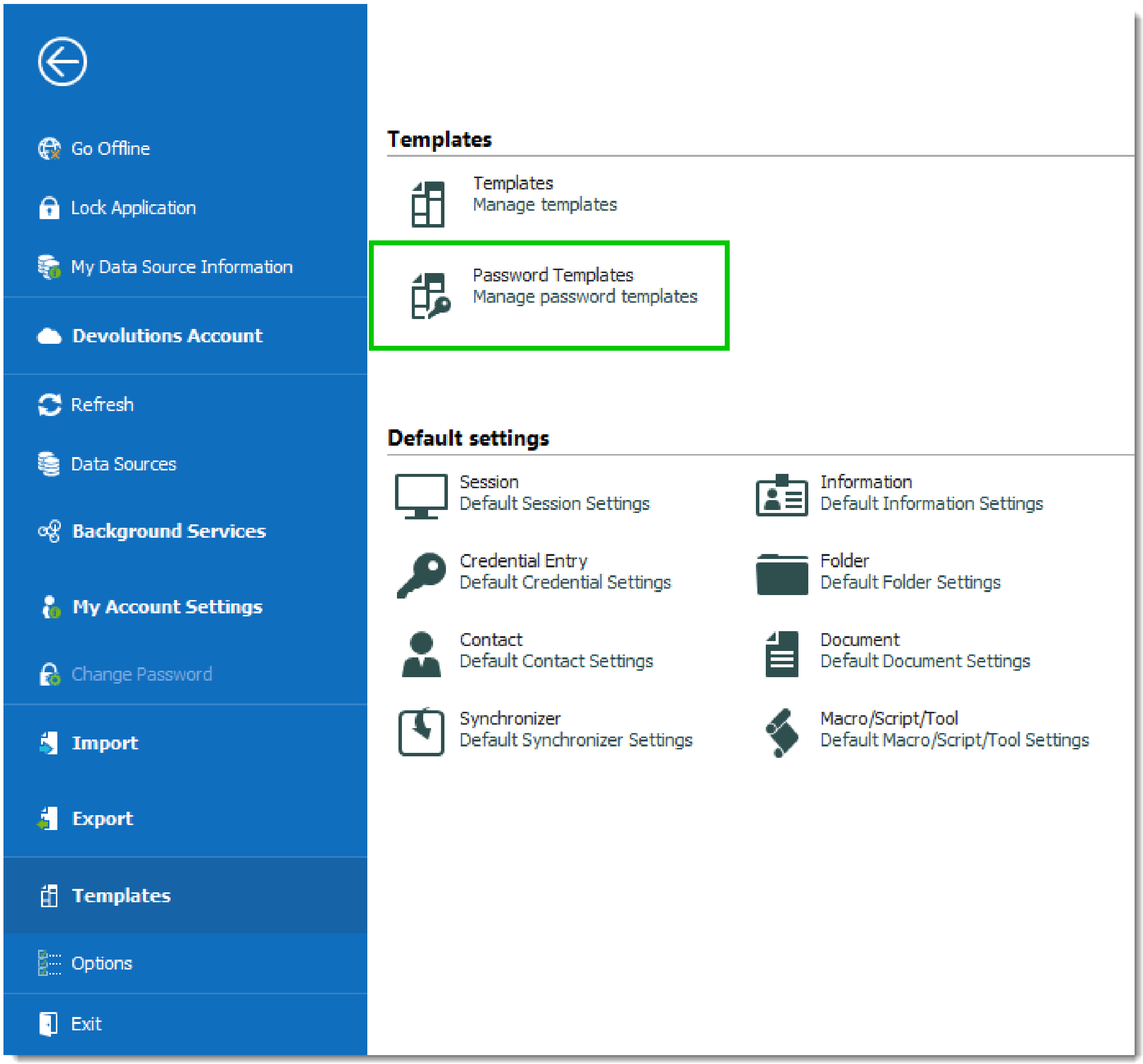
Password templates set requirements for the password format: characters usage, patterns, readability.

Password templates are available in the password generator. Password templates can be optional or required.

SETTINGS

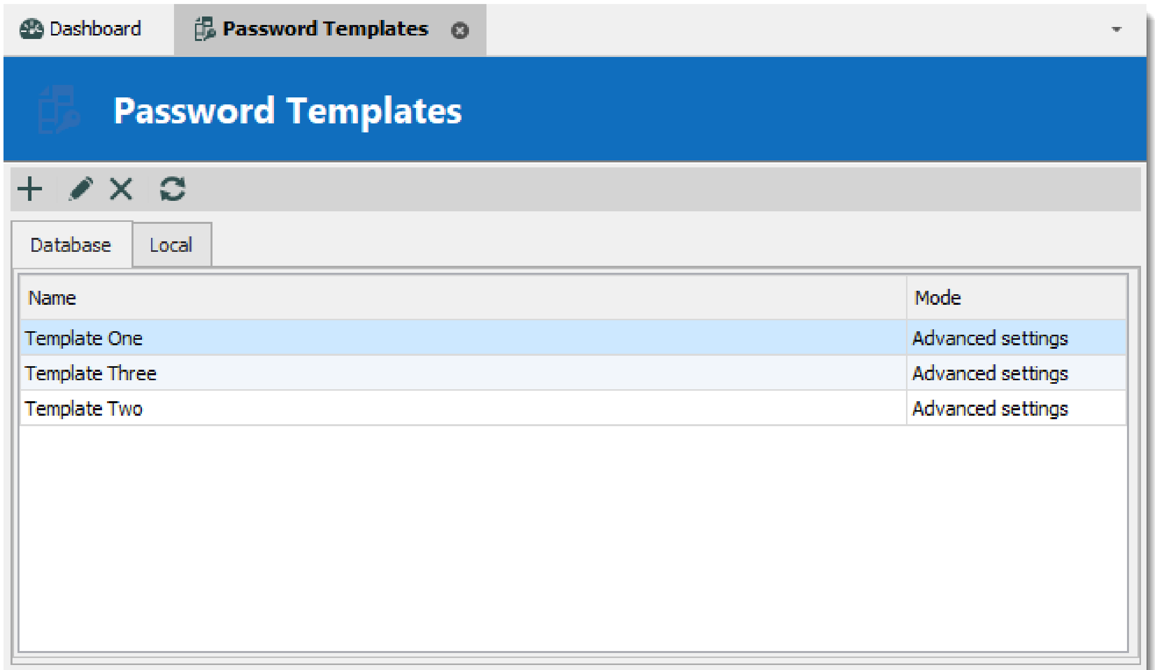
CREATE A PASSWORD TEMPLATE

1. Go to ***File – Templates,*** and click **Password Templates**.



File – Templates – Password Templates

2. The **Password Templates** window provides an overview of current templates, as well as add, edit and delete commands.



Password Template Window

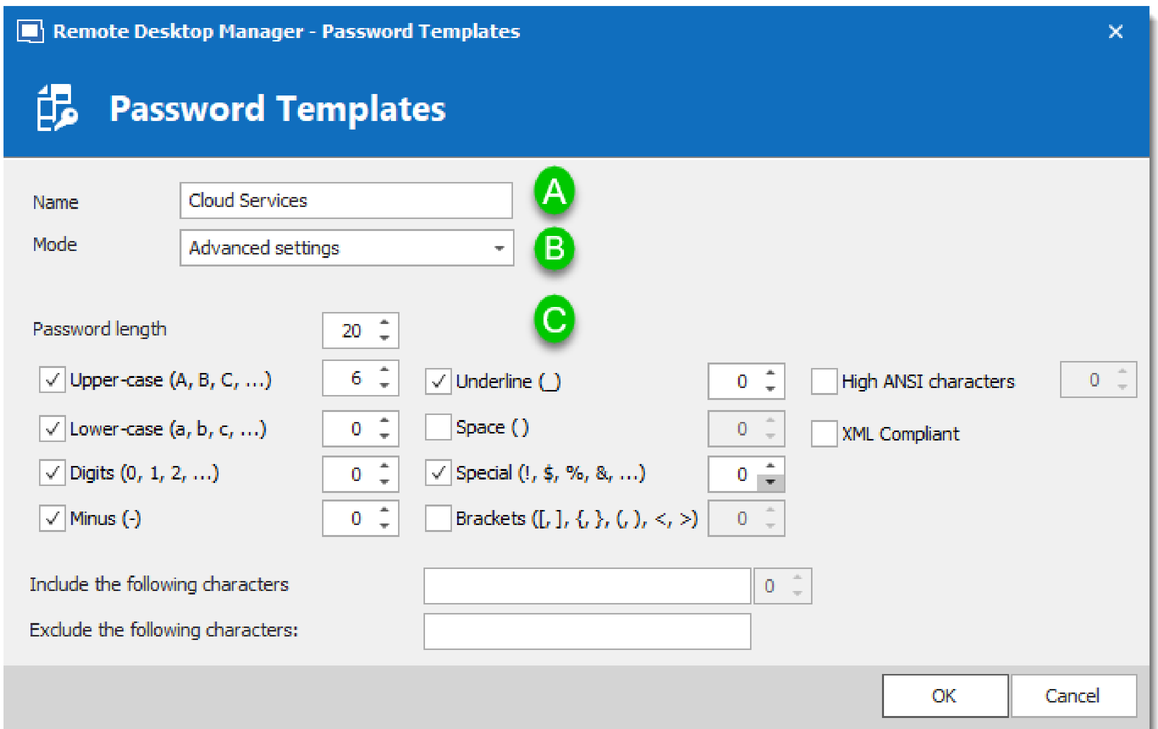
3. To add a new template click **Add** (plus sign).

4. a) Enter a template name.

   b) Choose a **Mode** and configure the settings.

OPTION	DESCRIPTION
Default	General settings about length and minimum amounts for characters and symbols.
Advanced settings	Granular character settings (e.g. special characters and symbols, inclusions, exclusions).
Readable password	Settings for syllables, numbers and symbols.
Use a pattern	Set a pattern for the passwords using the key.
Pronounceable password	Settings for length, case, digits and characters.

c) Choose specific settings



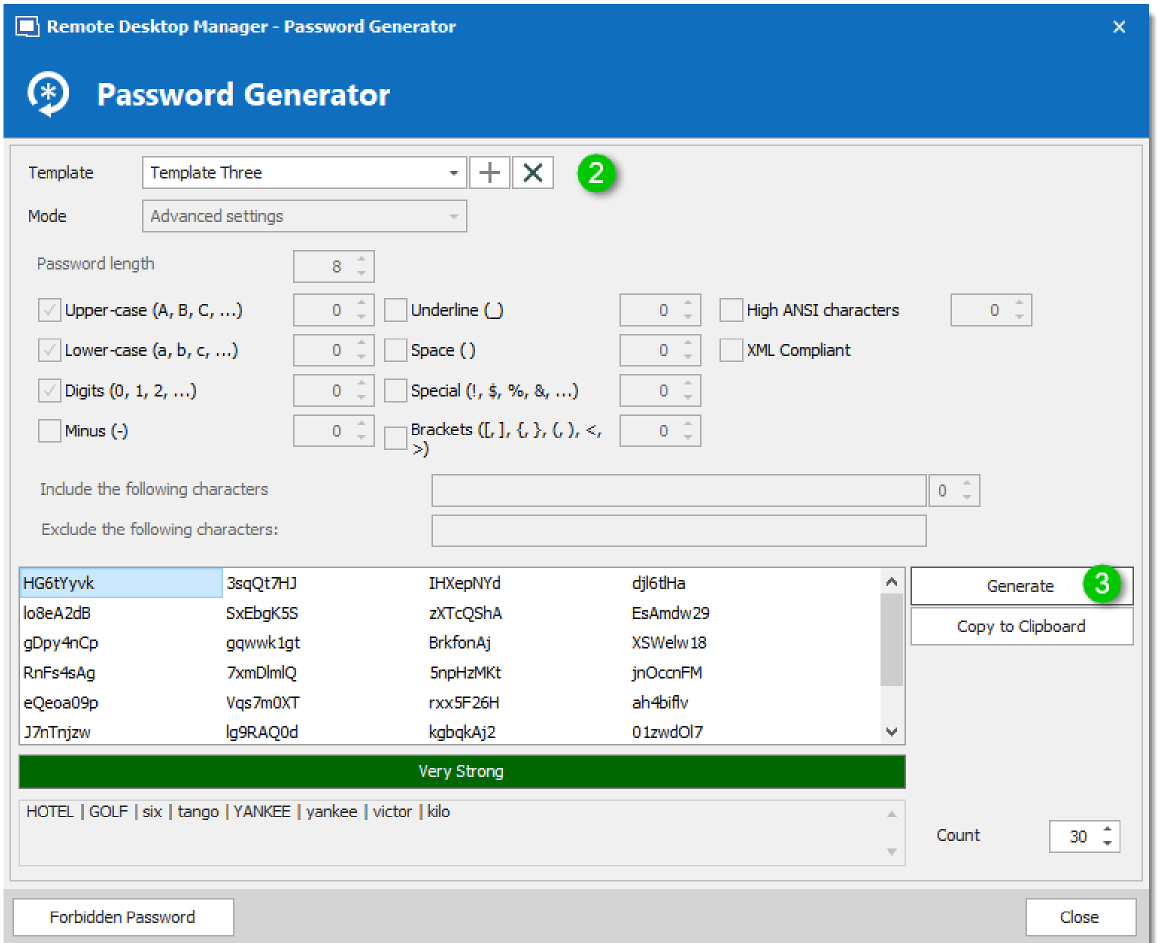
5. The password is now available in the **Password Generator** (**Tools** menu).

USE A PASSWORD TEMPLATE WITH PASSWORD GENERATOR

1. On the **Tools** tab, click **Password Generator**. Or open the password generator from an entry .

2. To choose a password template, select the title from the list. **Default** is equivalent to no template, until it is configured by an administrator. When you select a template the options are unavailable because they were saved in the template.

3. Click **Generate** to list possible passwords.



Password Generator using a password template

SET A DEFAULT PASSWORD TEMPLATE

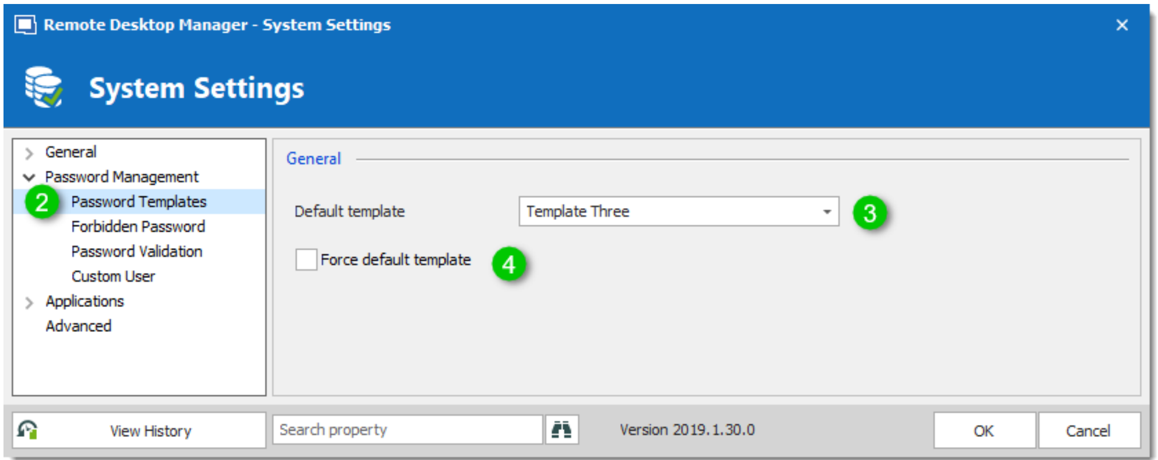
The default template in the **Password Generator** is set to "no template" until an administrator configures the template.

1. On **Administration**, click **Data Source Settings (System Settings)**.

2. Click **Password Templates**.

3. Choose the template. The chosen template will now be the **Default** in Password Generator.

4. If you want to force one template, check **Force default template**. No other choices will be available in the password generator.



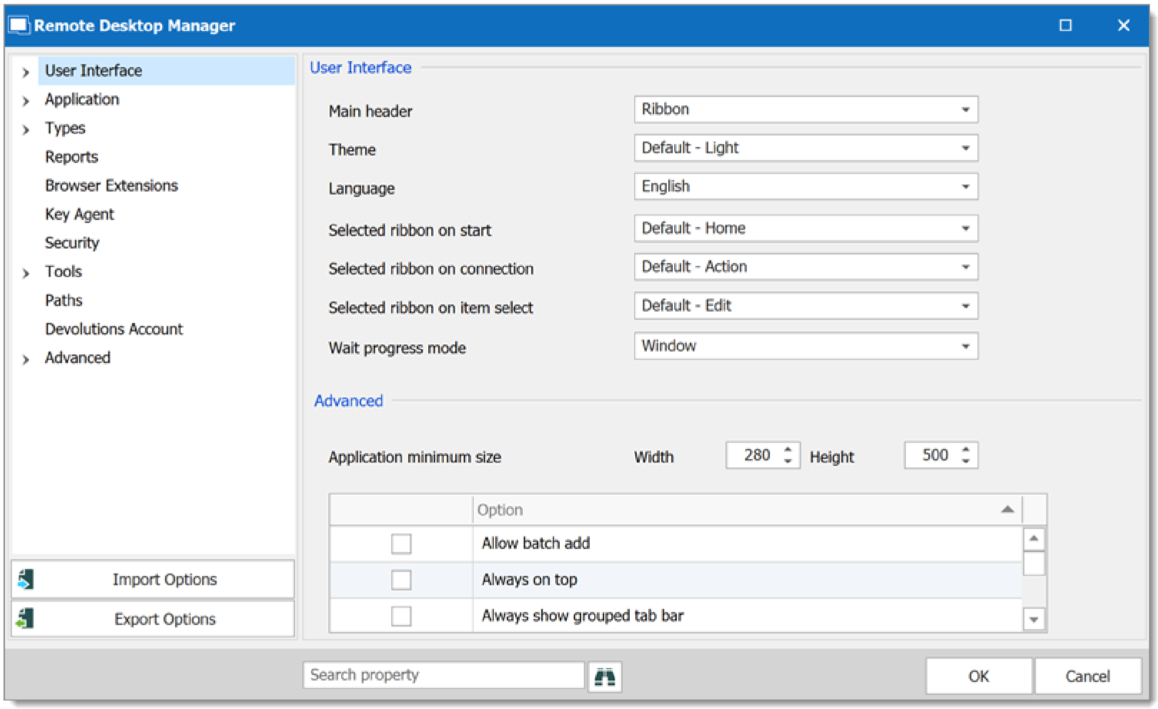
System Settings – Password Templates

6.2.13 Options

DESCRIPTION

There are multiple options available to manage and customize your Remote Desktop Manager in the menu ***File – Options***. Most of these options are related to changes to the local instance.

Use the **Search property** to find a specific option.

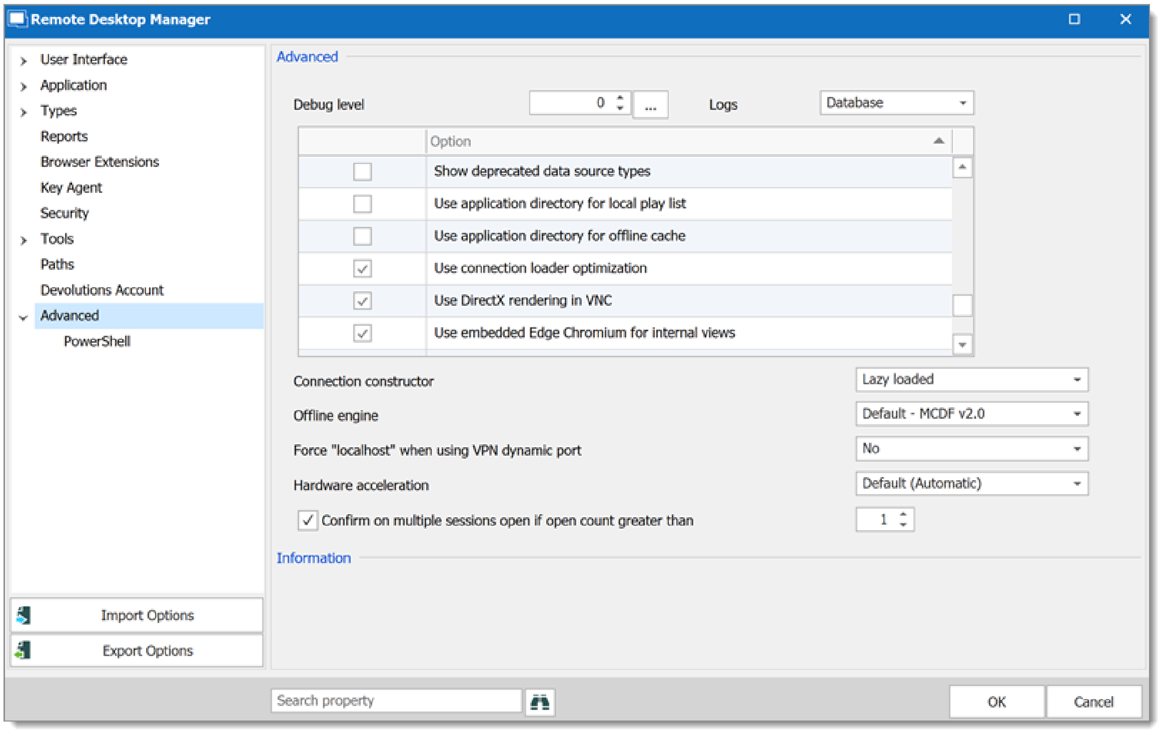


File - Options

6.2.13.1 Advanced

DESCRIPTION

Use the ***File - Options - Advanced*** tab to control the application behavior as it pertains to low level settings.



Options - Advanced

SETTINGS

ADVANCED

OPTION	DESCRIPTION
Debug level	Set the level of debugging information that Remote Desktop Manager will capture. This should only be modified upon request from a Devolutions support technician as it might cause your system to slow down .
Logs	The logs can be saved in a file or in a database file. Select between: • **Both:** Logs will be saved in a text file and in a database file.

OPTION	DESCRIPTION
	• **Database:** Logs will be saved in a file named RemoteDesktopManager.log.db. The file is located in the installation folder of the application. • **File:** Logs will be saved in a file named RemoteDesktopManager.log. The file is located in the installation folder of the application.
Connection constructor	The connection constructor is used for memory optimization when using legacy. We strongly recommend to leave this option at Default. **Only change this option upon request from a Devolutions support technician.**
Offline engine	You can choose your Offline engine between the SQLite or OpenMCDF. **Only change this option upon request from a Devolutions support technician.**
Force "localhost" when using VPN dynamic port	Forces the use of "localhost" when using the VPN dynamic port.
Confirm on multiple session open if open count greater than	Select a target number where mass opening sessions will demand confirmation.

OTHER OPTIONS - CONNECTIONS

OPTION	DESCRIPTION
Allow embedded credential source mode (Legacy)	Allow Embedded Credential mode in entries. This mode is deprecated and not recommended. Please review the Credentials Options available.

OPTION	DESCRIPTION
Automatically open file location after session recording	After a session recording, it will open the destination folder where the file is saved.
Disable close all confirmation message	Disables the Close all confirmation message when closing/disconnecting multiple entries at the same time.
Disable compromised password pwned check	Disables the pwned check feature if it isn't forced by the administrator in the System Settings - Password Validation option.
Disable DPAPI on offline cache	Disable the DPAPI encryption on the offline cache. This encryption is provided by Windows and used to make the offline cache more secure.
Disable form editor cache	Disables the form editor cache and force RDM to always fetch the information. It is not recommended to disable this feature for performance reasons.
Disable log off confirmation message	When pressing the logoff button in an embedded RDP session, Remote Desktop Manager, will disconnect the session without the logoff confirmation message.
Disable multi-thread loading	This setting allows Remote Desktop Manager to use multiple threads to load the data. Disabling this option will decrease the performance.
Disable multi-thread offline file	This setting allows Remote Desktop Manager to use multiple threads in offline file. Disabling this option will decrease the performance.
Disable resilient database connection handling	Resilient Database connection handling is a mechanism we put in place to retry certain database connections in RDM to avoid certain errors. Some slowness can be expected when enabled.

OPTION	DESCRIPTION
Disable system event handlers	Only used for diagnostic purposes, do not set unless recommended by the Devolutions Support team.
Disable thumbnail view for Google Chrome	Disable the thumbnail view for Google Chrome in ***View - Thumbnails*** to improve the application performance.
Enable global event logging for Telnet and SSH (DevolutionsTerminal.log)	Enables global event logging for Telnet and SSH entries. It will create the file DevolutionsTerminal.log at the same place where the configuration file is located.
Enable offline read/write locks	Activate locks for the Offline read/write rights.
Ensure that KeePass is running	Validate that KeePass is running on your computer before accessing any KeePass data.
Force refresh before edit entry	Perform a refresh of the entry before entering in edit mode. This is useful in a multi-user environment with a shared data sources. This ensure that you are editing the most recent version of the entry.
Force restore application with desktop shortcut	When double-clicking on the desktop shortcut it will restore the application that is already open. If the option is unchecked a second Remote Desktop Manager window will open.
Open shortcut session silent	Disable the command line warning message when using a shortcut.
Show deprecated data source types	We don’t support some data sources anymore, enabling this option will show them again.

OPTION	DESCRIPTION
Use connection loader optimization	Only enable this option upon request from our Support team.

OTHER OPTIONS - GENERAL

OPTION	DESCRIPTION
Add folder in hierarchy during batch add	When doing a batch add of folders, depending on the option chosen, it will either create them all on the same level or make them a child of the previous folder.
Allow multiple instances	Allows more than one instance of Remote Desktop Manager to run concurrently. This is not a recommended practice.
Allow non upgraded data source	Allow Remote Desktop Manager to work on an older data source that has not been upgraded.
Check focus content on RDP activation	If an RDP session requests the focus, it will pull RDM to the foreground, focusing it.
Confirm on drag and drop move	When session(s) are moved by drag and drop, a confirmation message will appear to confirm the move.
Disable favicon cache	Disables the favicon cache and force RDM to always fetch the favicon from the web. It is not recommended to disable this feature for performance reasons.
Disable stack trace	Disable the stack trace details when an error occurs in Remote Desktop Manager. This is a security feature.
Disable telemetry	Disable the analysis of data or statistics. Telemetry is the equivalent of Google Analytics. Note that the statistics are anonymous.

OPTION	DESCRIPTION
Disable user gravatar	Disable the fetching of the gravatar in the Administration - Users window to improve the application performance.
Focus content on application activation	Set focus on the last embedded session when the application is activated.
Include Active Directory computers in select computer dialog	Enable to view the list of all Active Directory.
Include network neighborhood computers in select computer dialog	Enable to view the list of all neighboring computers. It is not recommended to enable this feature for performance reasons.
Lock integrated security: validate only against domain context	The integrated security lock validates by default against the local machine and the domain context. You have the option to validate only against the domain.
No Internet connection	Disable the application to access the internet.
Use application directory for local play list	Use the installation folder to save the local play list that has been created.
Use application directory for offline cache	Use the installation folder to save the offline cache file.
Use Devolutions updater	Only modify this option upon request from our Support team.

OPTION	DESCRIPTION
Use Microsoft Office instead of editors	When adding a new document by selecting a file supported by a Microsoft Office application (Word, Excel), it will make a Word/Excel document instead of a Rich Text Editor/Spreadsheet Editor entry.
Use ZipCrypto compression (not recommended)	Enable this option to allow the ZipCrypto compression in RDM. We do not recommend enabling this option. Here is a blog written by our security team about the subject: Why you should never use the native .Zip Crypto in Windows.

OTHER OPTIONS - MICROSOFT EDGE

OPTION	DESCRIPTION
Use embedded Microsoft Edge for documentation and markdown	Enabling this option will allow to use the browser Microsoft Edge instead of Internet Explorer for the documentation and markdown.
Use embedded Microsoft Edge for overview panel	Enabling this option will allow to use the browser Microsoft Edge instead of Internet Explorer for the overview panel.
Use embedded Microsoft Edge for release notes	Enabling this option will allow to use the browser Microsoft Edge instead of Internet Explorer to display release notes.
Use embedded Microsoft Edge for reports	Enabling this option will allow to use the browser Microsoft Edge instead of Internet Explorer to display the reports.

OTHER OPTIONS - UI OPTIONS

OPTION	DESCRIPTION
Always show "Go Offline" button	Always display the "Go Offline" button in the status bar when Offline Mode is active.
Disable custom images	Disable the loading of any custom images in the tree view. Too many custom images could dramatically increase the size of the data source and increase the load time at the same time.
Disable document selector (CTRL + Tab)	When left enabled, it will allow to switch from multiple open tab connections.
Disable layout restoration	Disable manually configured tab layout and restore the layout settings on a RDM restart.
Enable tags textbox in properties	By default, the Tags field, in the Properties of an entry, can only be filled through the tag selector. With this option, it lifts that restriction and you can write in the Tags text box directly.
Hide last opened play list in play list management	Hide the last opened play list at startup in the play list dialog.
Hide loading data sources progress bar	Will hide the loading data sources progress bar when loading.
Keep View Password window on top	Force the View Password window to display on top of all the RDM windows.
Use old entry sort	Use the old entry sort from previous version of Remote Desktop Manager.

INFORMATION

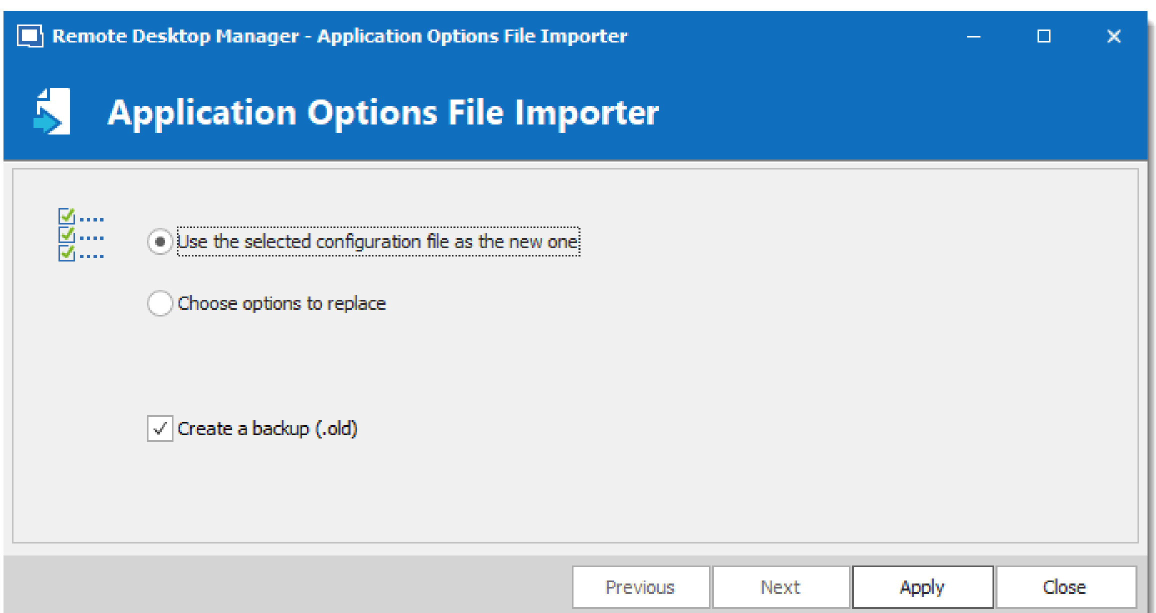
OPTION	DESCRIPTION
Created on	Creation date of Remote Desktop Manager configuration folder.
Source	Source of Remote Desktop Manager configuration settings.
Path	Shortcut to access the configuration folder directly.

6.2.13.2 Import Options

SETTINGS

Select the Configuration File to import in Remote Desktop Manager and click on ***Open.***

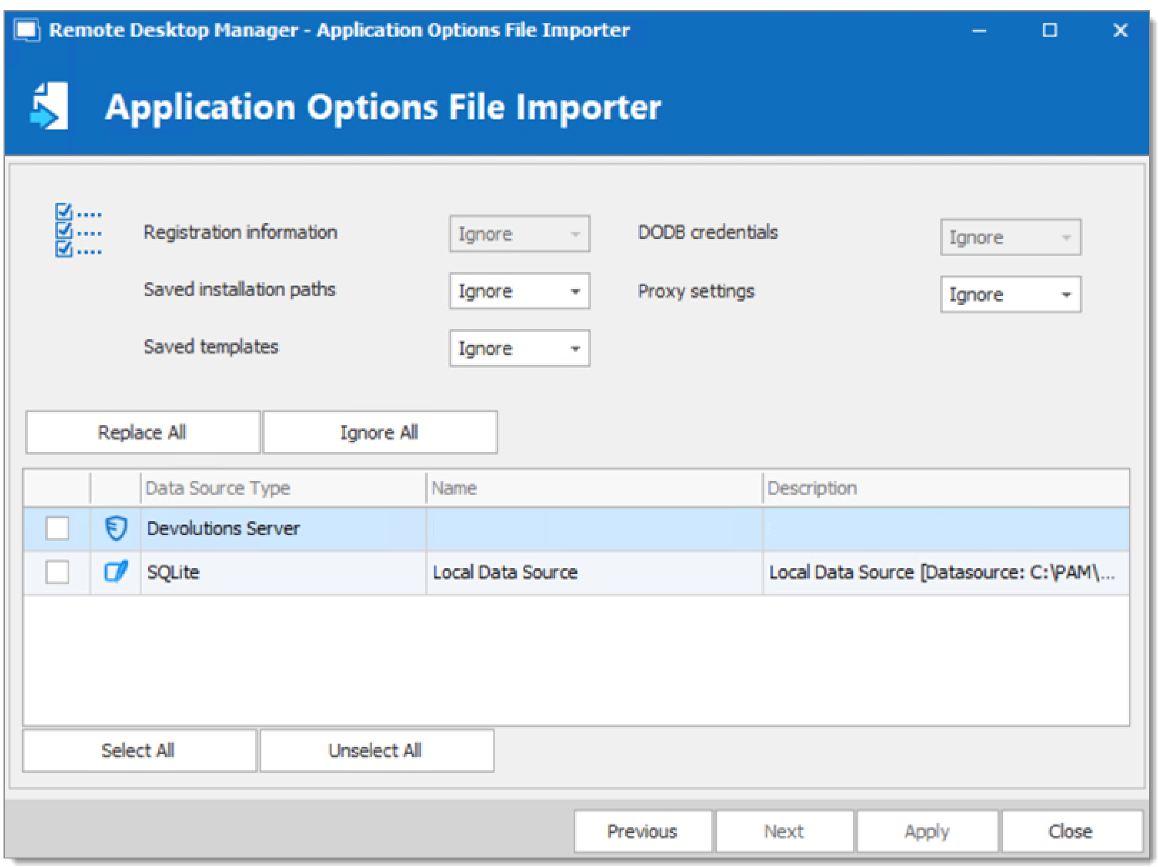
REMOTE DESKTOP MANAGER OPTIONS FILE IMPORTER



Application Options File Importer

OPTION	DESCRIPTION
Use the selected configuration file as the new one	Use the RemoteDesktopManager.cfg file as a new configuration file for your application.
Choose options to replace	Select which options to replace in your actual RemoteDesktopManager.cfg file. See below for more information.
Create a backup (.old)	Create a backup of your old RemoteDesktopManager.cfg

CHOOSE OPTIONS TO REPLACE



Application Options File Importer

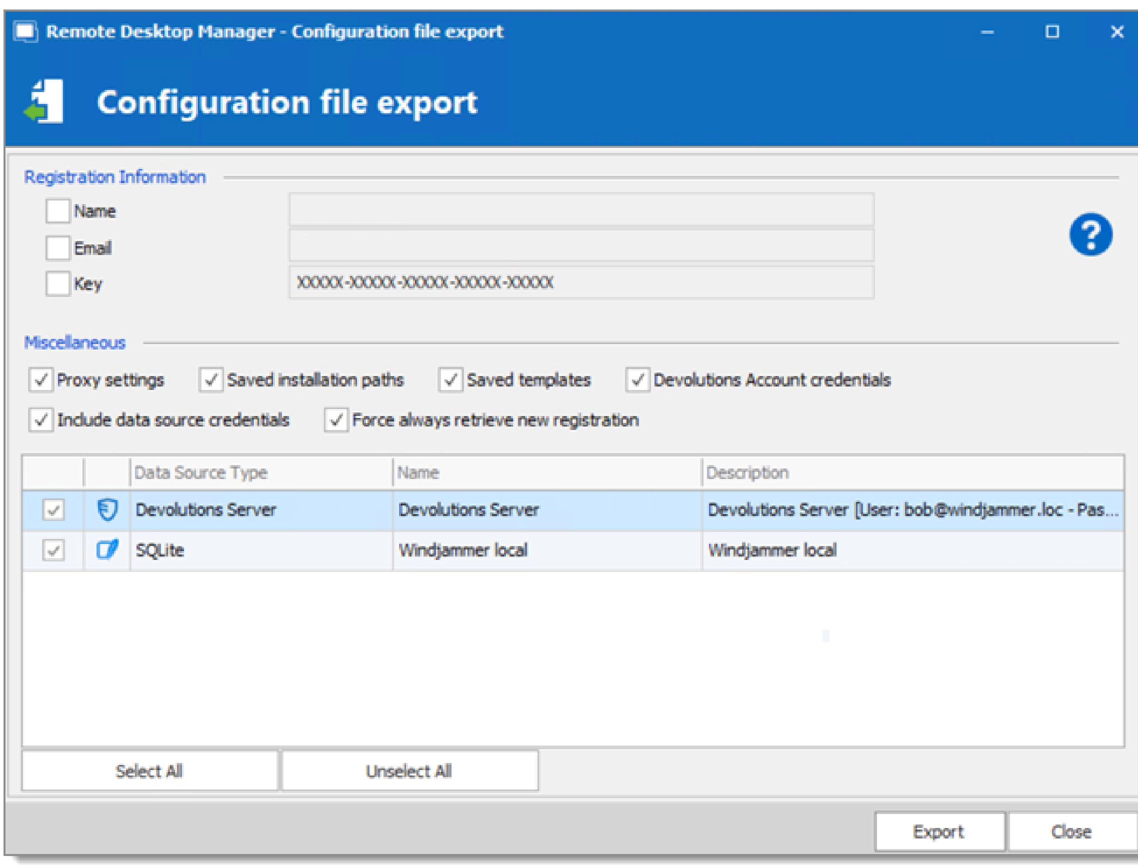
Decide which options to replace with the one from RemoteDesktopManager.cfg that you wish to import. Select **Replace** to replace an existing setting with a new one or select **Ignore** if you want to keep the setting that you already have.

6.2.13.3 Export Options

DESCRIPTION

Use ***File – Options – Export Options*** to control the options to export from your application configuration. Use this to easily transfer settings to another machine.

> Sharing the exported file with a colleague would effectively give that person whatever credentials you have set in your data source definitions.
>
> Devolutions does not recommend sharing any credential to a team data source.



Configuration file export dialog

SETTINGS

REGISTRATION INFORMATION

OPTION	DESCRIPTION
Name	Company registration name.
Email	Registration email.
Key	Serial key.

MISCELLANEOUS

The local templates may contain credentials, ensure you do not share the exported file.

OPTION	DESCRIPTION
Proxy settings	Includes your proxy settings.
Saved installation paths	Preserve your installation paths configured for the external application.
Saved templates	Include your local templates in the export.
Include data source credentials	Include your data source credentials.

DATA SOURCES

> The data source configurations you select will be exported with the username/password as they are currently configured. If you are creating a file to quickly set up new employees, you must be careful not to give away your credentials. Using the [Custom Installer Service]() is recommended for this case.

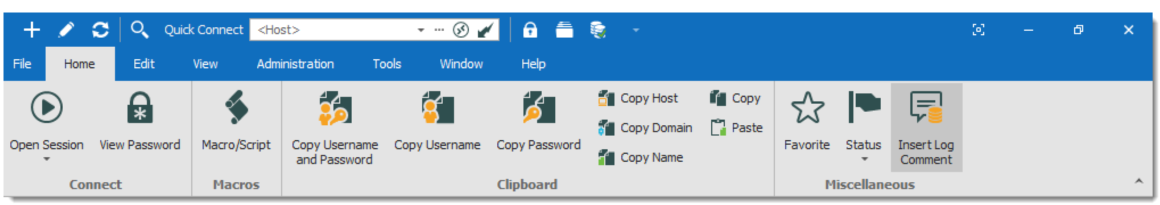
All your configured data sources will be displayed in this section. Select the one(s) that you want to include in the export. Please note that the content of the data source is not exported.

When your settings are customized to your liking, click on **Export**. You will be prompted to save your settings in a RemoteDesktopManager.cfg file.

6.3 Home

DESCRIPTION

The **Home** ribbon tab allows you to apply an action on the currently selected session. The ribbon will display the following tab when the session is embedded.



Ribbon - Home

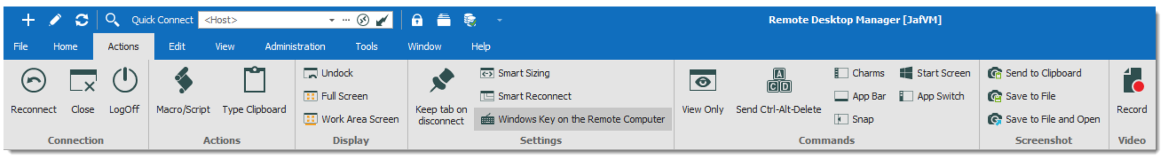
- Connect.
- Macros.
- Clipboard: Configure clipboard in File – Options.
- Miscellaneous.

6.4 Actions

DESCRIPTION

The **Actions** tab is only available when a session is open. Available actions differ depending on the action.

For our example we are running an RDP session. The ribbon will display the following tab when the session runs with the Embedded (tabbed) display mode.



Ribbon - Actions

CONNECTION

OPTION	DESCRIPTION
Reconnect	Quickly close the session and then re-open it automatically. Use it to update the resolution of your embedded RDP connections when you resize the window.
Close	Close the active session.
LogOff	Logoff the RDP session. See Logoff topic for more information.

ACTIONS

Option	Description
Execute	Execute the selected macro or script in the previous window or in the current tab. This is only available when there is something to

Option	Description
	Execute.
Macro/Script	Displays a window where you can select a macro or script, as well as the execution options.
Type Clipboard	Send the content of the clipboard over to the opened session.

DISPLAY

OPTION	DESCRIPTION
Undock	Undock your embedded session and move it anywhere outside Remote Desktop Manager or even on another monitor.
Embedded	Re-embed your session when your session is undocked. This option will only appear if your session is not already in an embedded mode.
Full Screen	Display your session in full screen outside Remote Desktop Manager.
Work Area Screen	This mode allows you to open the connection in full screen but to also have access to your local taskbar.

SETTINGS

OPTION	DESCRIPTION
Keep tab on disconnect	Your session tab will stay after a session disconnect. For more information, see Keep Tab Opened topic.
Smart Sizing	Enable or disable the RDP smart sizing. This setting will determine whether or not the client computer can scale the content on the remote computer to fit the window size of the client computer.
Smart Reconnect	Automatically reconnect your session with the most appropriate band.
Windows Key on the Remote Computer	When enabling **Windows key**, it will send the function to your host instead of running it on your computer.

COMMANDS

This tab contains multiple type of commands and keystrokes combinations to affect the current session in a variety of instances. As such, these commands depend on the currently selected (and opened) entry. For a few example scenarios, refer to the following topics:

- RDP
- VNC
- Telnet

Session add-ons may add custom command in this section, they will not be documented in these topics but rather in the add-on documentation.

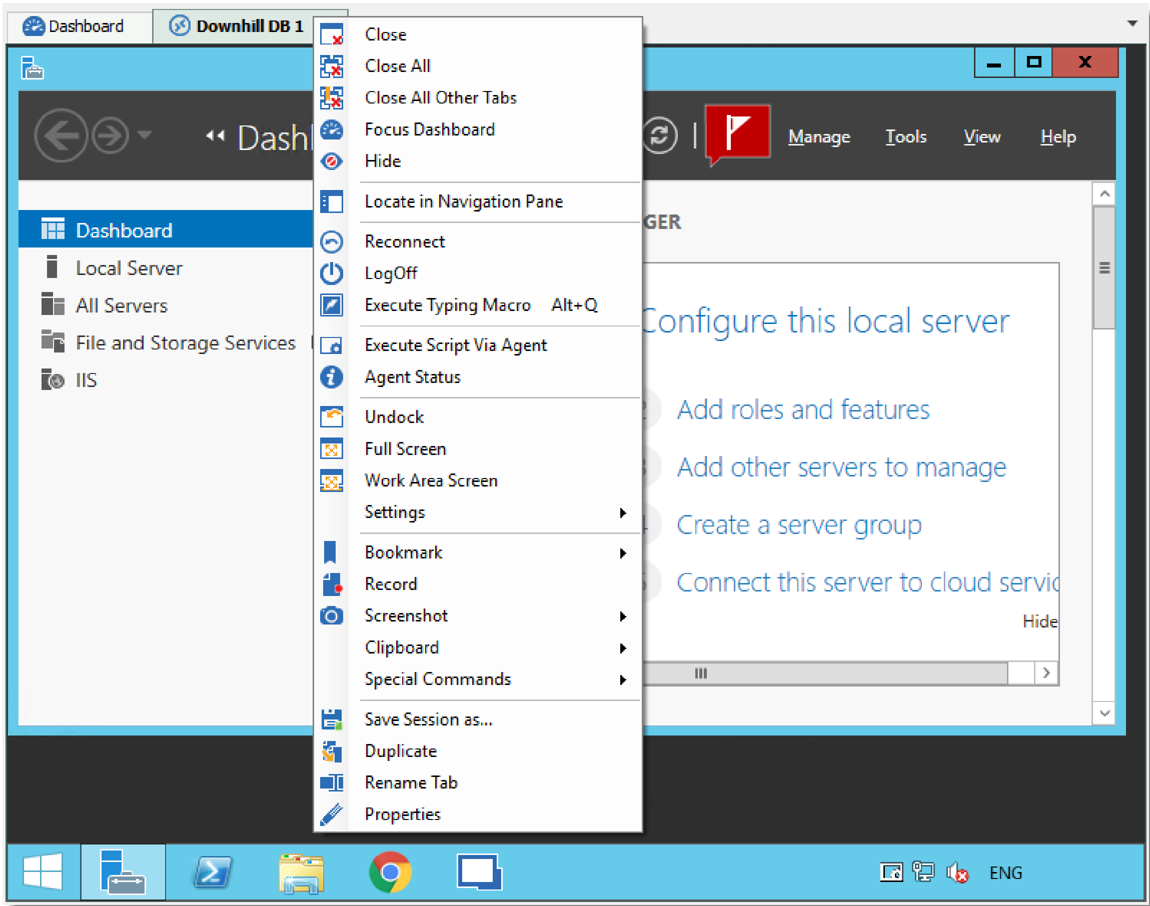
SCREENSHOT

OPTION	DESCRIPTION
Send to Clipboard	Performs a typical capture to the clipboard.
Save to File	Prompts for a file name and saves the capture to that file.
Save to File and Open	Prompts for a file name and saves the capture to that file, then automatically open the file using your default editor.

VIDEO

OPTION	DESCRIPTION
Record	Record your screen in an MP4 format. We recommend the use of a VLC player to view the recorded video.

Alternatively, these actions are also available by **right-clicking** on the tab of an embedded session.



Actions Context Menu of an Embedded Session

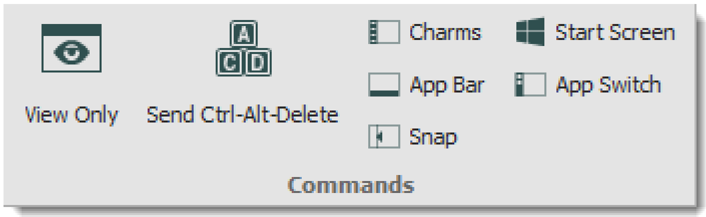
6.4.1 Commands

6.4.1.1 RDP

DESCRIPTION

The commands for an RDP session allows you to send remote commands to your host.

SETTINGS



RDP Commands

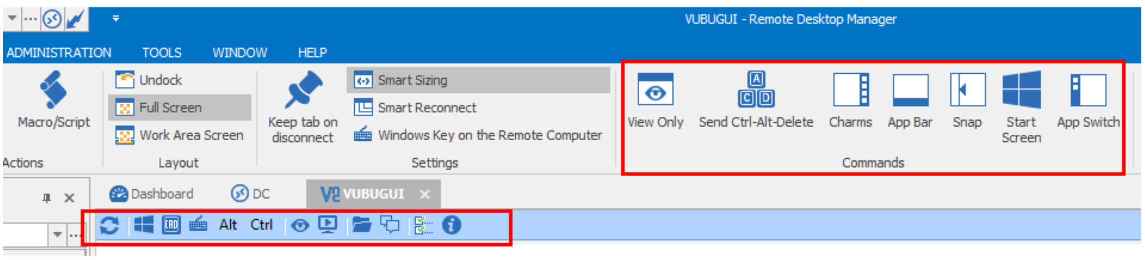
OPTION	DESCRIPTION
View Only	Prevent the session from receiving any input from the keyboard or the mouse. This feature was requested to allow monitoring while preventing manipulation errors. Use it to have a read only access to the remote server.
Send Ctrl+Alt+Delete	Send the key combination CTRL+ALT+DELETE to the host.
Charms	On Windows 8 or Windows 2012 server, displays the Charms bar (Search, Share, Start, Devices, and Settings bar).
App Bar	On Windows 8 or Windows 2012 server, displays the App bar to show navigation, commands, and tools.
Snap	On Windows 8 or Windows 2012 server, allows you to run two applications side-by-side.
Start Screen	Open the Start menu on the host computer.
App Switch	On Windows 8 or Windows 2012 server, switches from an application to another.

6.4.1.2 VNC

DESCRIPTION

The VNC Commands allows you to send remote commands to your host. You will also notice another toolbar holding more defined commands for a VNC session.

SETTINGS



VNC Commands

OPTION	DESCRIPTION
Refresh Screen	Refresh the host screen.
Window Start Menu	Open the Start menu on the host computer.
Send Ctrl-Alt-Delete	Send the key combination CTRL+ALT+DELETE to the host.
Send Custom Keys	Send custom keys combination to the host.
Alt	Send ALT to the host.
Ctrl	Send CTRL to the host.
View only mode	This will prevent the session from receiving any input from the keyboard or the mouse. This feature was requested to allow monitoring while preventing manipulation errors. Use it to have a read only access to the remote server.
Remote input	Keyboard and pointer events will be sent to the server and the local and remote clipboard will be synchronized.
Open file transfer	Open the file transfer with the host computer.

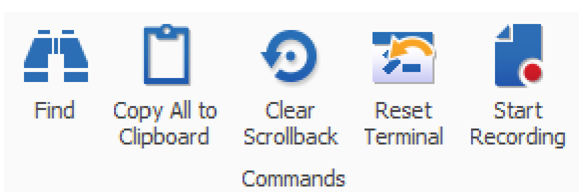
OPTION	DESCRIPTION
Open chat dialog	Open a chat dialog with the host computer.
Options	Open the Connection Options window.
Information	Open the window containing information regarding your VNC connection status and traffic.

6.4.1.3 Telnet

DESCRIPTION

The actions for a Telnet session allows you to send remote commands to your host.

SETTINGS

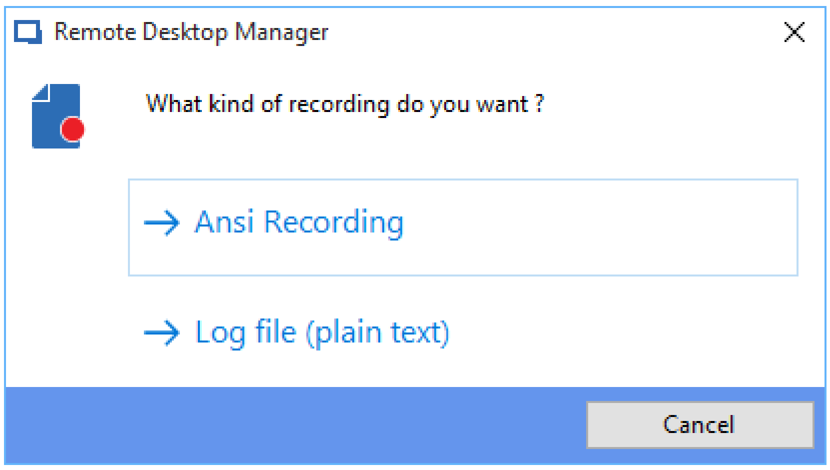


Telnet Commands Actions

OPTION	DESCRIPTION
Find	Open a find window to search for specific words.
Copy All to Clipboard	Copy all selected text to the Clipboard.
Clear Scrollback	Clear the scrolling display that precedes the current line.

OPTION	DESCRIPTION
Reset Terminal	Reset host terminal connection.

START RECORDING

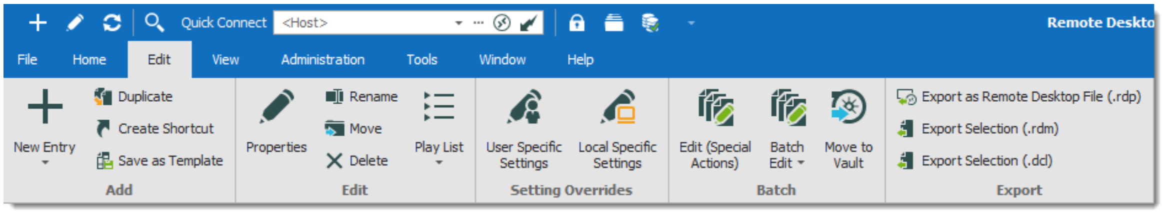


OPTION	DESCRIPTION
Ansi Recording	Will record all of the activity in the SSH session using the Ansi format. This can be replayed like a video using ***Tools - Tools - Terminal playback (Ansi)***.
Log file (plain text)	Will record all of the activity in the SSH session using a text format.

6.5 Edit

DESCRIPTION

The **Edit** tab contains operations to quickly Add, Edit, Overrides, Batch Edit or Export entries.



Ribbon - Edit

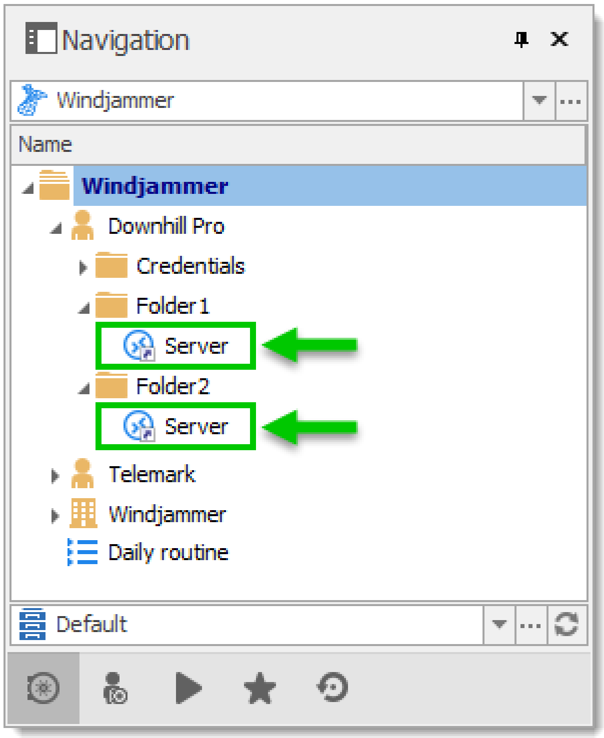
ADD

OPTION	DESCRIPTION
New Entry	Create a new entry (session, folder, information entry, credentials, etc.).
Duplicate	Create a duplicate of your entry.
Create Shortcut	Link your entry to more than one group. For more information, consult the text below.
Save as Template	Save the selected entry as a local or database template.

A shortcut is the reiteration of an existing entry. In contrast to a duplicated entry, which has its own ID and properties, a shortcut is a link to an entry and its properties. You can create shortcuts easily by right-clicking the entry ***Edit – Create Shortcut*** or by using the aforementioned button in the **Edit** tab. There are a few scenarios where a user would want to use the same entry differently, such as connecting to two different hosts with a single RDP session.

For example, it is possible to:

- Assign different access to the same entry.
- Create a favorite folder with everything centralized.
- Reuse a document for different scenarios.



These two entries are the exactly the same

Entries reiterated this way also have both folder paths indicated in their Folder field in their properties, the paths are separated by a semi-colon.

> There is no visual differences between the shortcut and the original entry. Therefore, you'll need to delete all entries to completely remove said entry. You will be asked for confirmation when attempting to delete said shortcut.

EDIT

OPTION	DESCRIPTION
Properties	Edit the properties of the selected entry.
Rename	Rename the selected entry.

OPTION	DESCRIPTION
Move	Move the selected entry to another folder.
Delete	Delete the selected entry. A confirmation dialog is displayed to confirm the action.
Play List	Use the various play list features.

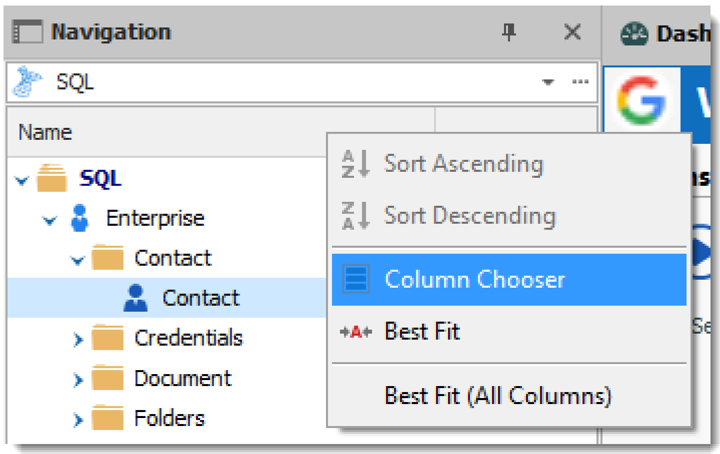
The **Play List** feature in Remote Desktop Manager is a lot like a music play list. It opens a list of entries, in a specific order, automatically.The Play List can be used to create groups of sessions for a specific task or for security reasons. You can build your own Play List and start all entries from a Play List at the same time.

- Create and Edit a Play List
- Using a Play List

SETTING OVERRIDES

OPTION	DESCRIPTION
User Specific Settings	Override properties of the selected entry with settings with settings specific to the current user. For more information, please consult the Specific Settings topic.
Local Specific Settings	Override properties of the selected entry with settings specific to the local machine. For more information, please consult the Specific Settings topic.

A Specific Settings column can be added in the Navigation Pane. **Right-click** on the column **Name** in the Navigation Pane and select **Column Chooser**. **Double-Click** on **Specific Settings** to add the column. Now, if there is a specific setting applied to an entry, it is displayed next to the entry's name.



Navigation Pane - Column Chooser

BATCH

OPTION	DESCRIPTION
Edit (Special Actions)	Perform special actions on the selected entries, such as change the type, run a script, and more. For more information, please consult the Batch Actions Samples.
Batch Edit	Perform an action on multiple entries at once. This is particularly useful for doing mass modifications of entries (such as changing the display mode after modifying the workspace or their credential entries when changing your passwords). Multiple entries must be selected for this feature to be visible. For more information, please consult the Batch Edit topic.

OPTION	DESCRIPTION
Move to Vault	Transfer the selected entries to another Vault in the database.

EXPORT

OPTION	DESCRIPTION
Export Entry as Remote Desktop File (.rdp)	Export the selected entries in a Remote Desktop File (.rdp) format.
Export Selection (.rdm)	Export the selected entries in a .rdm file that can then be imported into any Remote Desktop Manager data source. You could choose to include the credentials of your entry in your export format and secure your file with a master key.

6.5.1 Entries

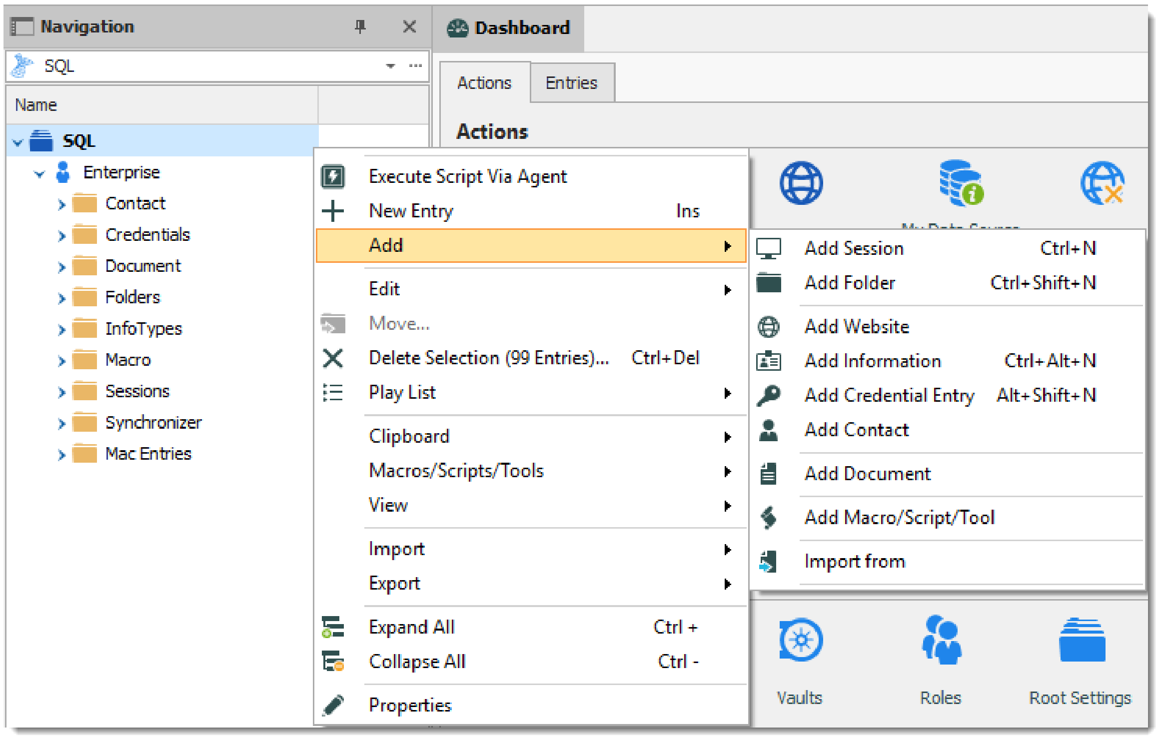
6.5.1.1 Creating an Entry

DESCRIPTION

When getting started with Remote Desktop Manager, you must configure your entries. There are many types of entries; you should know what third party or technology you will use in order to choose the appropriate entry type(s) that you plan on configuring.

CREATING AN ENTRY FROM THE CONTEXT MENU

On the main application window, simply right-click on **the name of the data source** and select **Add** from the menu. To initialize a new session, you can specify either the type of session, or a template. You will be prompted to customize your settings in the entry properties window.



Adding a new entry

CREATING AN ENTRY WITH DRAG & DROP

You can also create a session by dragging and dropping an .rdp file in the main application window. By doing so, Remote Desktop Manager will ask you whether to import the content and create a new session, or create a session linked to the .rdp file. It is also possible to drag and drop the **LogMeIn** desktop shortcut to create a **LogMeIn** session.

> It is possible that drag and drop will not work because of your security settings. They may prevent applications running in different contexts from interacting. For example, if Remote Desktop Manager is running in an elevated context (administrator mode) and Internet Explorer is running in default mode, Windows will not allow you to drag a URL link in the application.

CREATING AN ENTRY BY IMPORTING ITS CONFIGURATION

You can also import entries by using the Import Computer Wizard, or by importing its configuration directly from any compatible applications supported by our import tools. You can learn more in the Import section.

6.5.1.2 Checkout system

DESCRIPTION

The ***Checkout system*** locks an entry while it is being used or modified. It prevents users from using or editing an entry at the same time.

The checkout system can be enabled for ***Sessions***, ***Documents***, ***Credentials*** and ***Information*** entries.

You can set the check out mode at the Vault, folder or entry level.

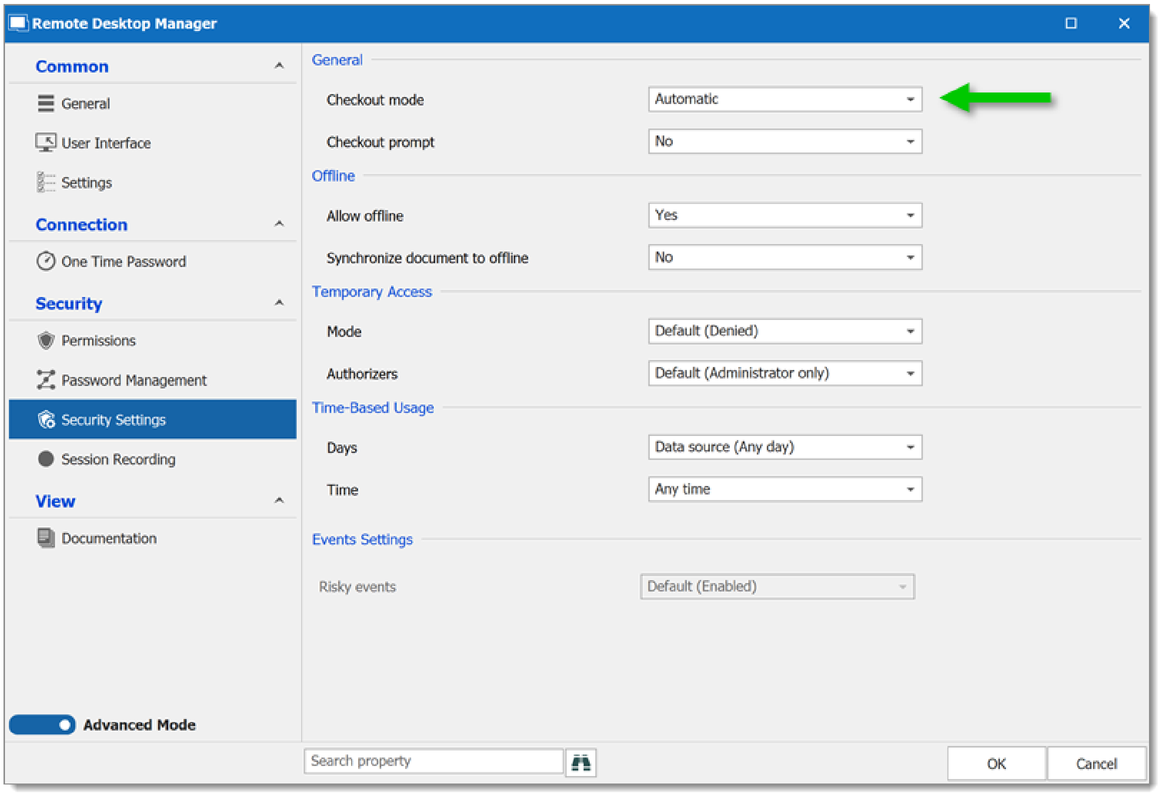
This feature is only available when using SQL Server or Devolutions Server data sources.

Administrators can set ***Automatic check in after*** a number of minutes in ***Administration - System Settings - Vault***.

Administrators can force ***Check In*** entries that are ***Check Out*** by other users. Right-click the entry that is check out, click ***Check In***.

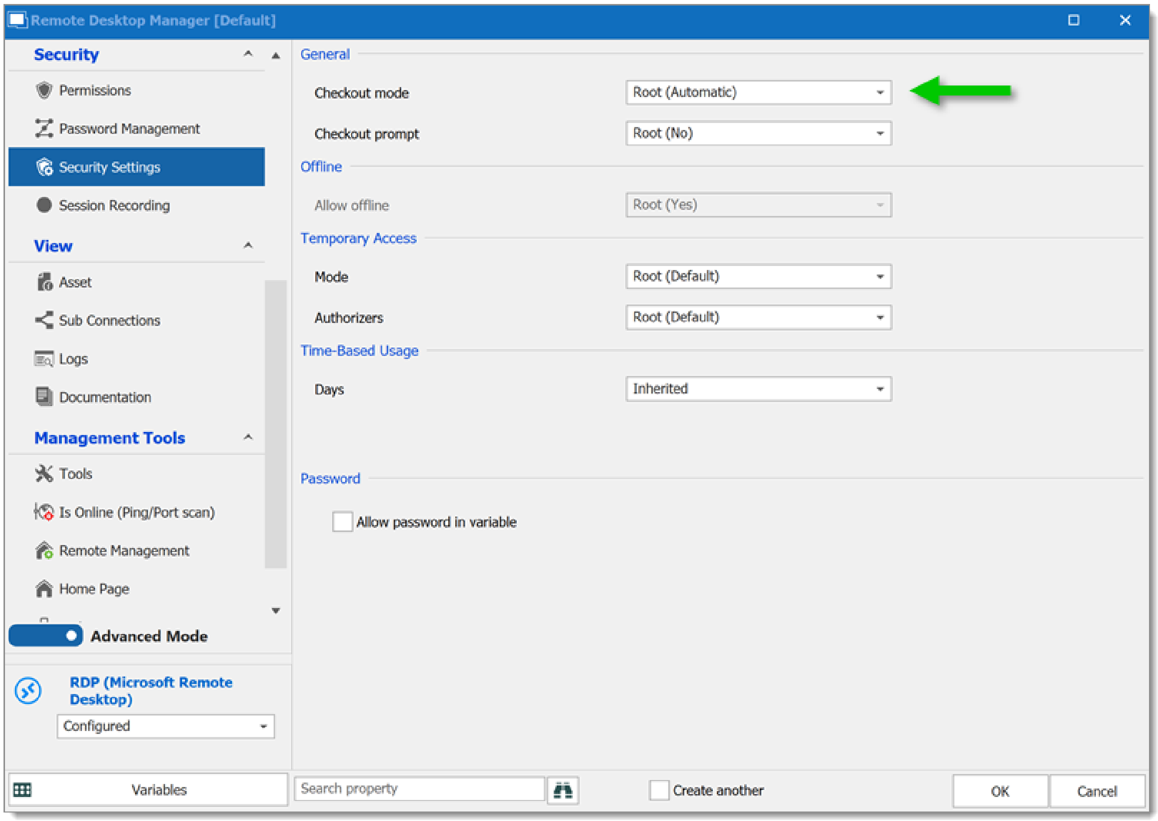
SECURITY SETTINGS

To access the check out settings, go into the ***Properties*** of an entry, folder or of the root folder. Navigate to the ***Security Settings*** section.



CHECKOUT MODE

Checkout mode enables or disables the checkout system. It also decides how the checkout mode functions.

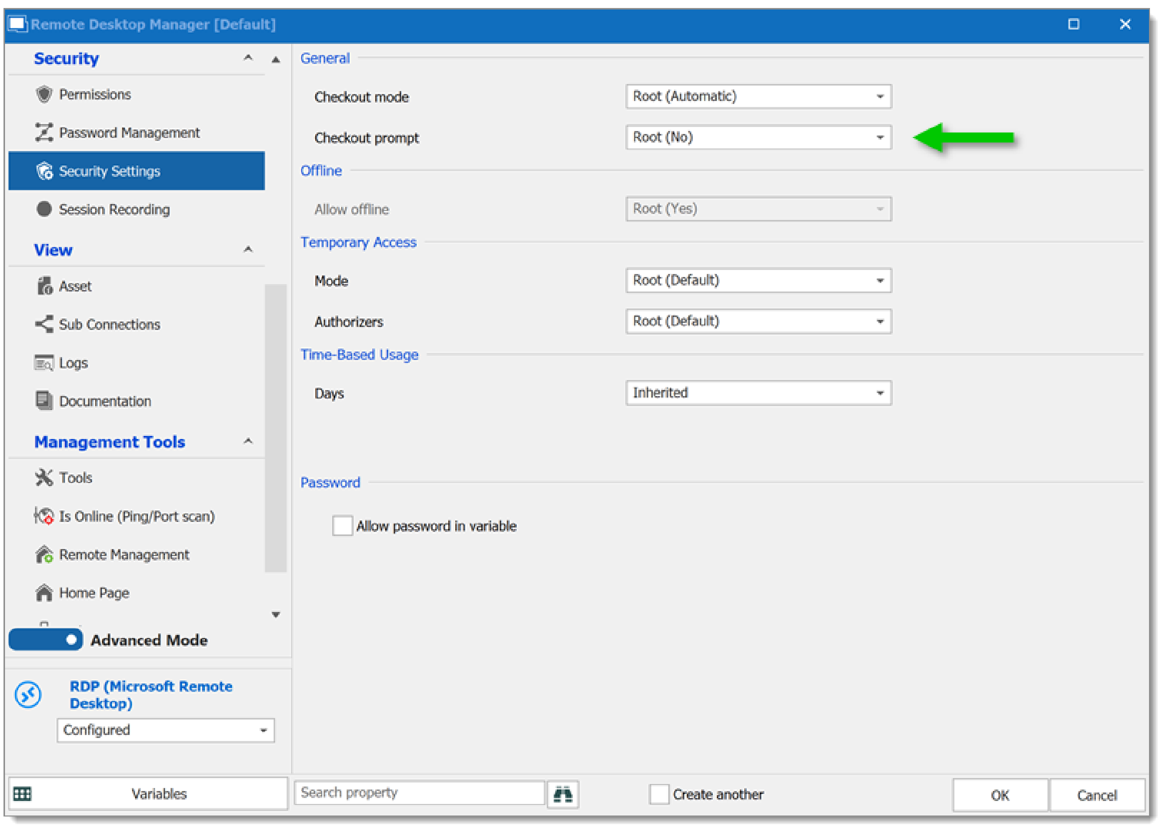


OPTION	DESCRIPTION
Root	Inherits the checkout mode setting from the root folder.
Not available	Disables the checkout system.
Automatic	Checks out an entry automatically when the entry is opened and automatically checks the entry in when the entry is closed. Users can edit properties without checking out the entry.
Manual	Users need to check out the entry manually prior to opening or editing the entry. No action can be performed without checking out the entry.
Inherited	Inherits the check out mode from the parent folder.

OPTION	DESCRIPTION
Optional	Offers the option to check out an entry manually or use (open and edit) the entry without checking it out.

CHECKOUT PROMPT

Checkout prompt sets if a user must enter a comment when they check out the entry. Administrators can monitor the comments through the logs available on the entry or the ***Activity Logs***.



OPTION	DESCRIPTION
Root	Uses the checkout prompt setting from the root folder.
Yes	Prompts the user for comment when they check out an entry.

OPTION	DESCRIPTION
No	Removes the prompt for comment.
Inherited	Inherits the setting from a parent folder.

6.5.1.3 Dynamic Credential Linking

DESCRIPTION

Dynamic credential linking creates a single credential entry for a supported credential manager and use this credential with any entry type that supports the Credential repository.

SUPPORTED CREDENTIAL MANAGERS

Here is the list of all implemented credential managers that support dynamic credential linking:

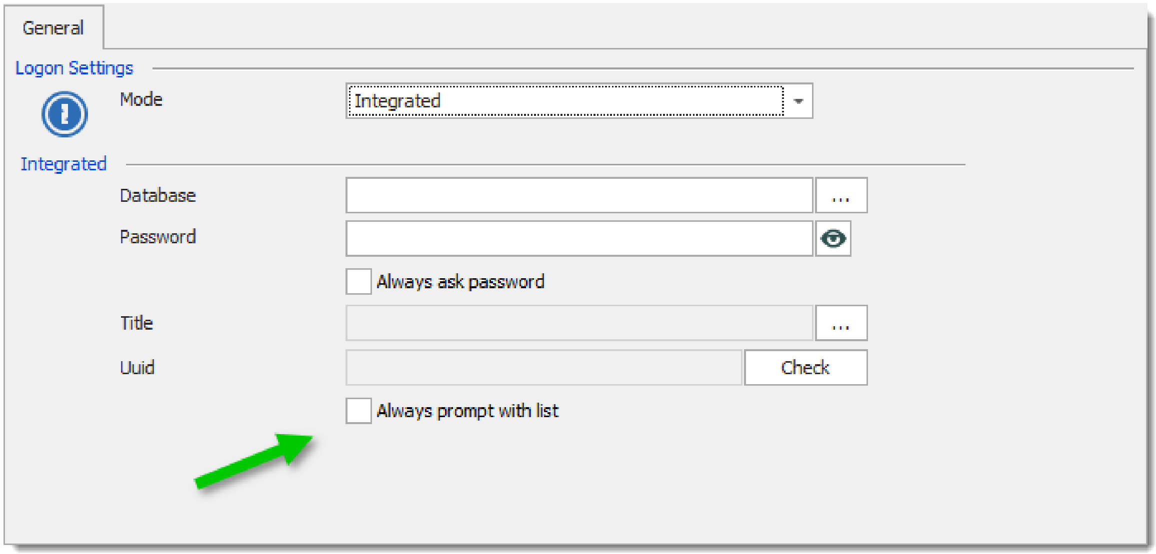
- **1Password**
- **Bitwarden**
- **Dashlane**
- **Devolutions Password Hub**
- **Devolutions Server**
- **KeePass**
- **Keeper**
- **LastPass**
- **Mateso Password Safe**
- **PassPortal**

- **Password List**
- **Password Manager Pro**
- **Password Safe**
- **PasswordState**
- **Password Vault Manager**
- **Pleasant Password Server**
- **RoboForm**
- **Secret Server**
- **Sticky Password**
- **TeamPass**
- **True Key**
- **Zoho Vault**

> A dynamic credential link can also be applied to a Folder or a VPN entry type if desired.

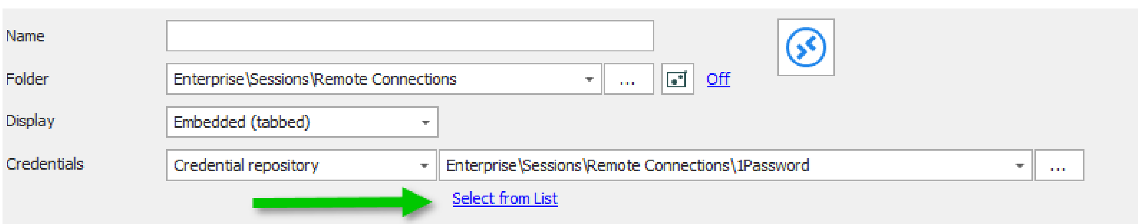
SETTINGS

1. Create a credential entry and check **Always prompt with list**.



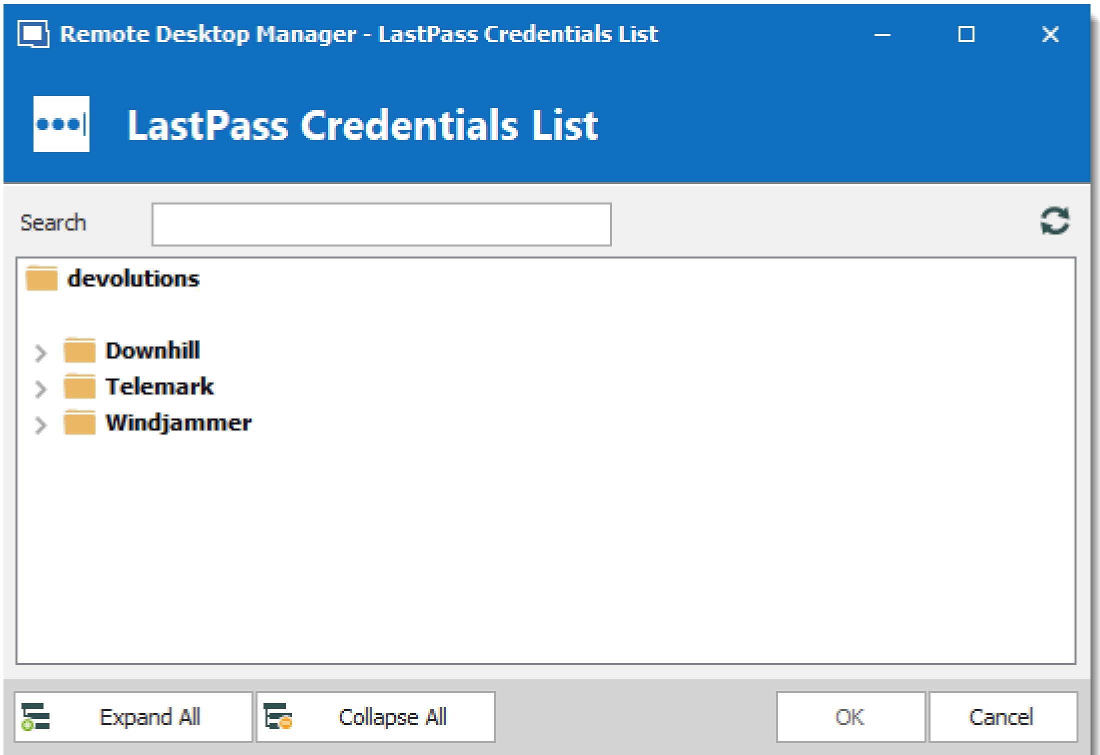
1Password Settings

2. When creating a entry, select **Credential repository** from the **Credentials** drop down list, then select the credential entry created in the previous step. Notice that a new action appears just below the credential selection drop down list.



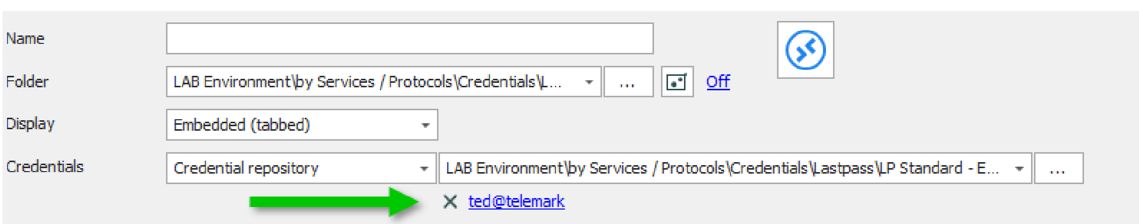
Select from List

3. Select a credential from the list.



LastPass Credentials list

4. The link changes to the name of the credential. To remove linked credential and bring back automatic list prompt, simply click on the "X".

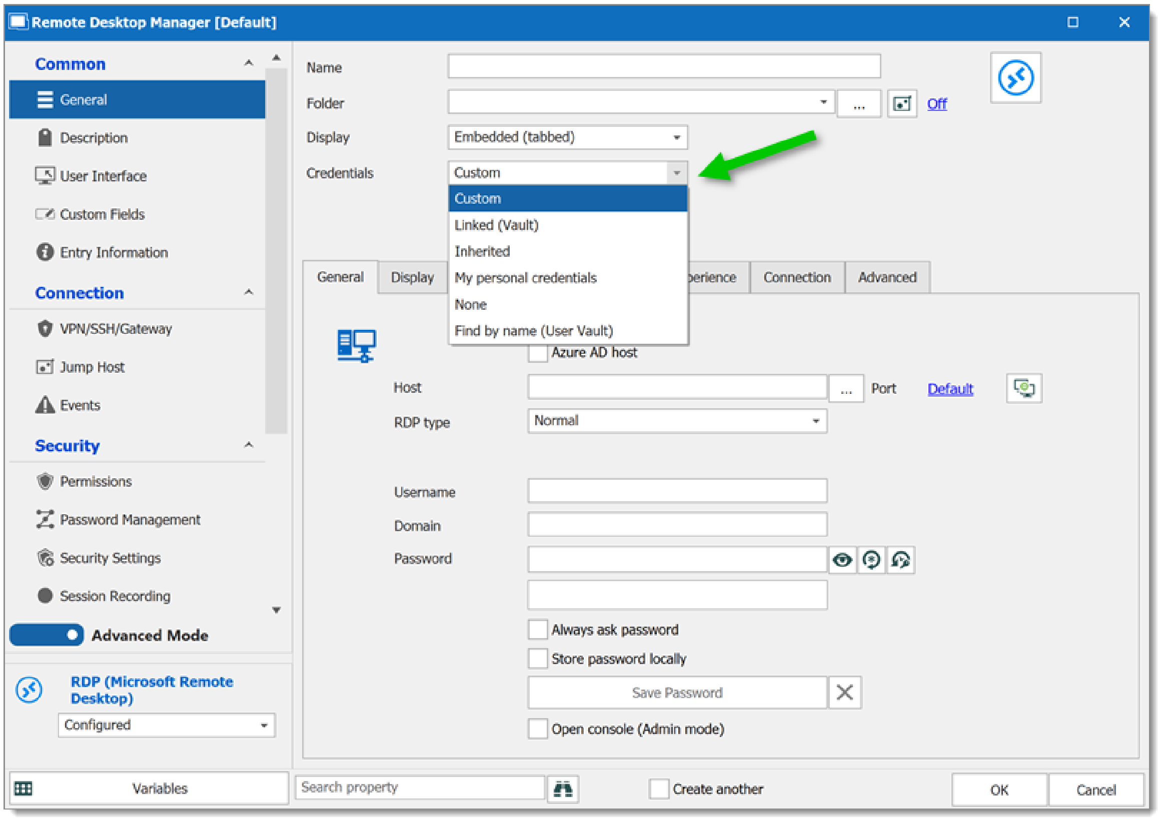


Name of the credential

6.5.1.4 Entry Credentials Options

DESCRIPTION

Multiple options are available to use for ***Credentials*** in your Remote Desktop Manager entries.



OPTION	DESCRIPTION
Custom	This option allows to enter custom credentials in the ***General*** section of the entry.
Linked (Vault)	Link your entry to use an existing ***Credential*** entry in the same vault.
Embedded (Legacy)	Embed a ***Credential*** entry in the entry itself. This mode is deprecated and not recommended. Please review other options available.
Inherited	The credentials used by this entry will be inherited and defined by climbing up the navigation tree until it has access to a set of credentials in a parent folder.
My personal credentials	Will use the credentials set in My personal credentials feature. This allows you to centralize one credential to

OPTION	DESCRIPTION
	replace or emulate the ones for your Windows session.
None	No credentials will be allowed to be saved or linked to this entry.
Find by name (User Vault)	Will search your ***User Vault*** for the name specified. If the box is left empty, when launch, a ***Credential list*** will open with all available ***Credentials*** entry from your ***User Vault***.

6.5.2 Edit

6.5.2.1 Play List

6.5.2.1.1 Create and Edit a Play List

DESCRIPTION

You can create Local or Shared play List in Remote Desktop Manager. There's several methods to create or edit a Play List:

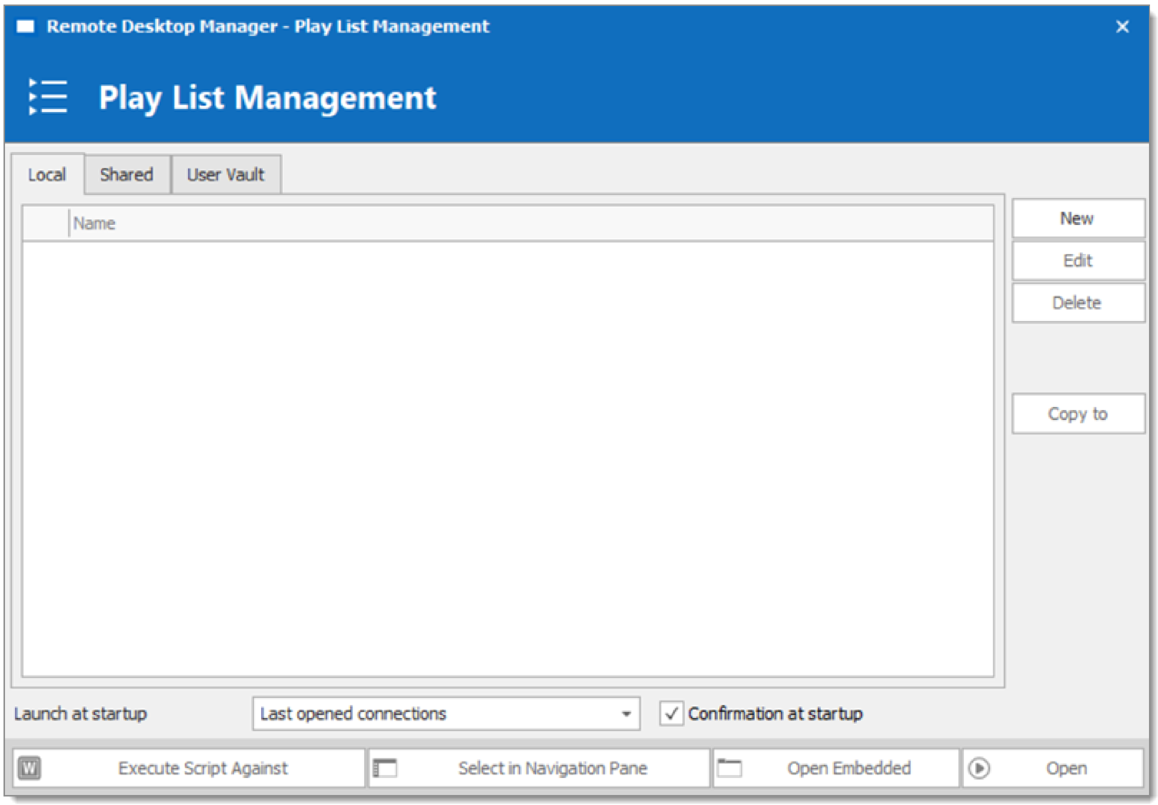
- Using the Play List Management.
- Create Play List depending on entries state and selection.
- Edit an existing Play List.

You can also use the context menu to create and edit your **Play List**. When your entries are selected, right-click in the Navigation Pane and select ***Play List - Add Selection to Existing Play List***.

SETTINGS

USE THE PLAY LIST MANAGEMENT

From the ribbon in ***Edit - Play List - Play List Management***.



Local Play List

Play lists can be saved three different ways:

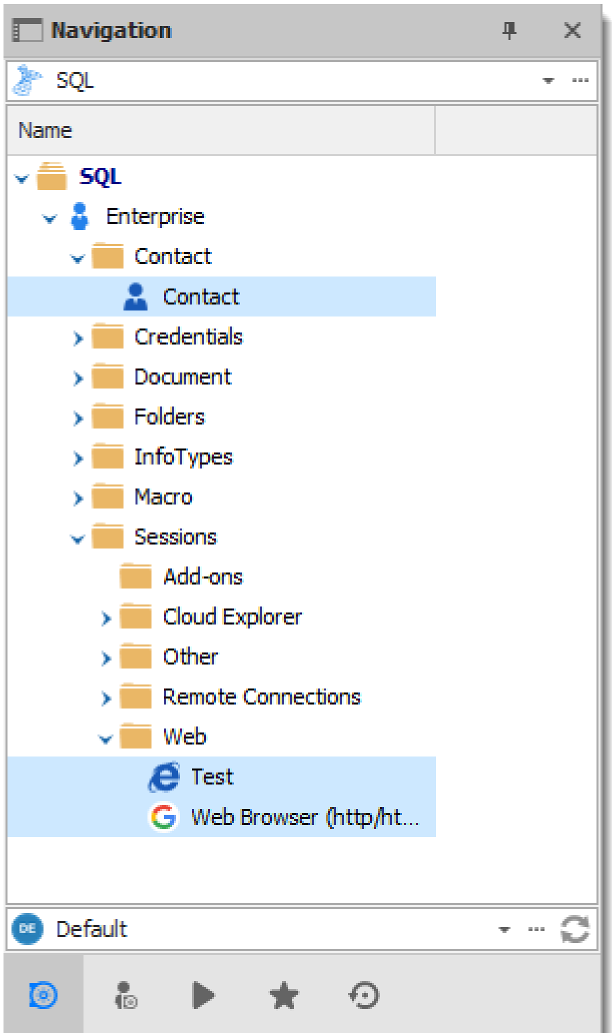
OPTION	DESCRIPTION
Local	The Play List is saved locally and can only be accessed as such. These can only be launched through the Play List Management.
Shared	The Play List is saved in the database. It can be accessed by anyone on the data source. These can be launched through the Play List Management or by using the entry itself.

OPTION	DESCRIPTION
User Vault	The Play List is saved in your User Vault and can only be accessed by the user. These can be launched through the Play List Management or by using the entry itself.

ACTIONS

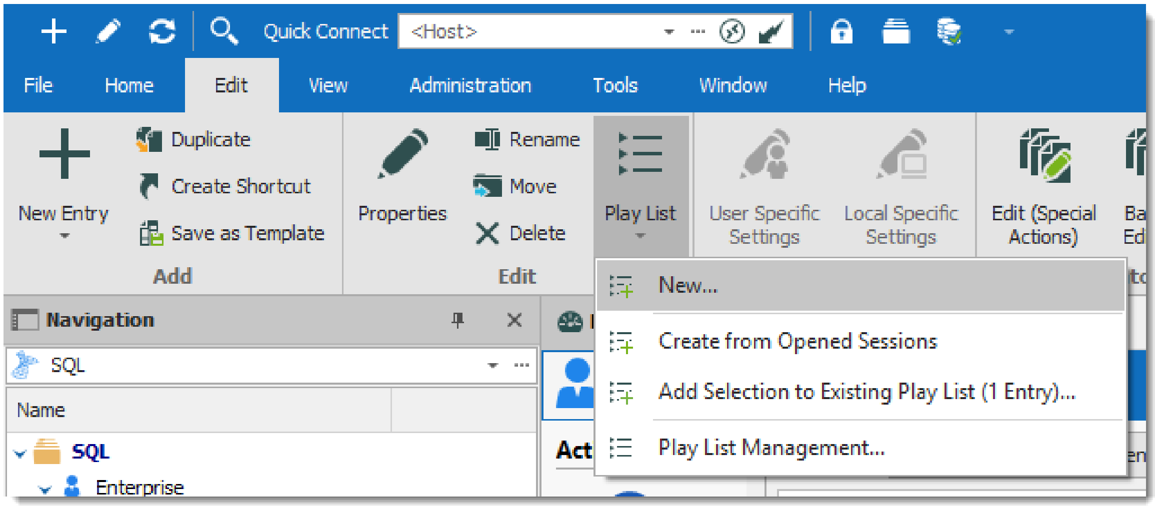
CREATE PLAY LIST DEPENDING ON ENTRIES STATE AND SELECTION

1. If you wish to pre-determine a list of entries, select them for your Play List in the Navigation Pane.



Selected Entries in the Navigation Pane

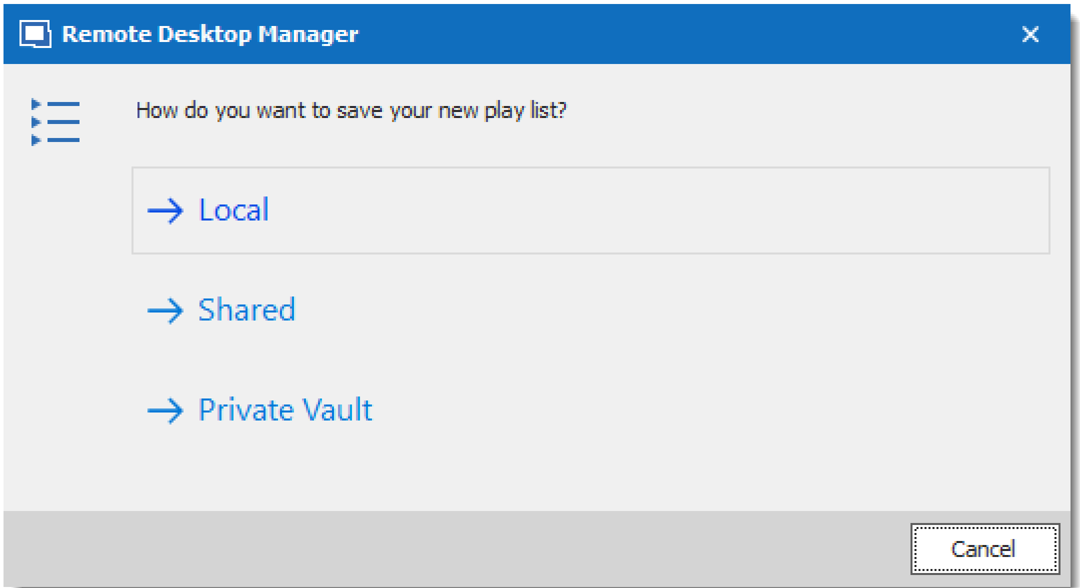
2. On the **Edit** ribbon menu, click **Play List,** then select whichever setting you prefer.



Edit - Play List - New

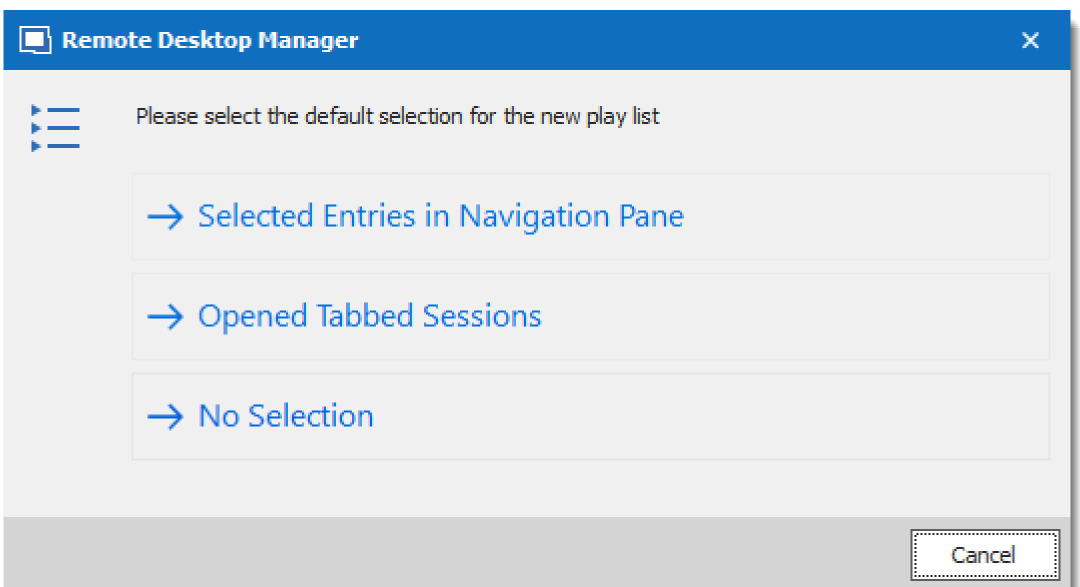
OPTION	DESCRIPTION
New	Creates a new Play List directly, a window prompt will ask you where you wish to save it and which selection you would like to highlight.
Create from Opened Sessions	Brings up the window for creating a new Play List with all currently opened session already selected for the Play List. You can select and remove additional entries if desired.
Add Selection to Existing Play List (X Entry)	Prompts a window where you can select currently accessible Play Lists and adds the selection in the Navigation Pane to the Play List.

3. Choose if you wish to save your Play List locally, in a shared Vault or in your User Vault. Saving it locally will prompt a different window. This window will contain everything needed for a local Play List.



Save New Play List

4. The next window lets you choose how you want your current selection or opened sessions to affect your playlist.



Selected Entries in Navigation Pane

OPTION	DESCRIPTION
Selected Entries in Navigation	All currently selected entries in the Navigation Pane will already be selected for your Play List. You can still add and

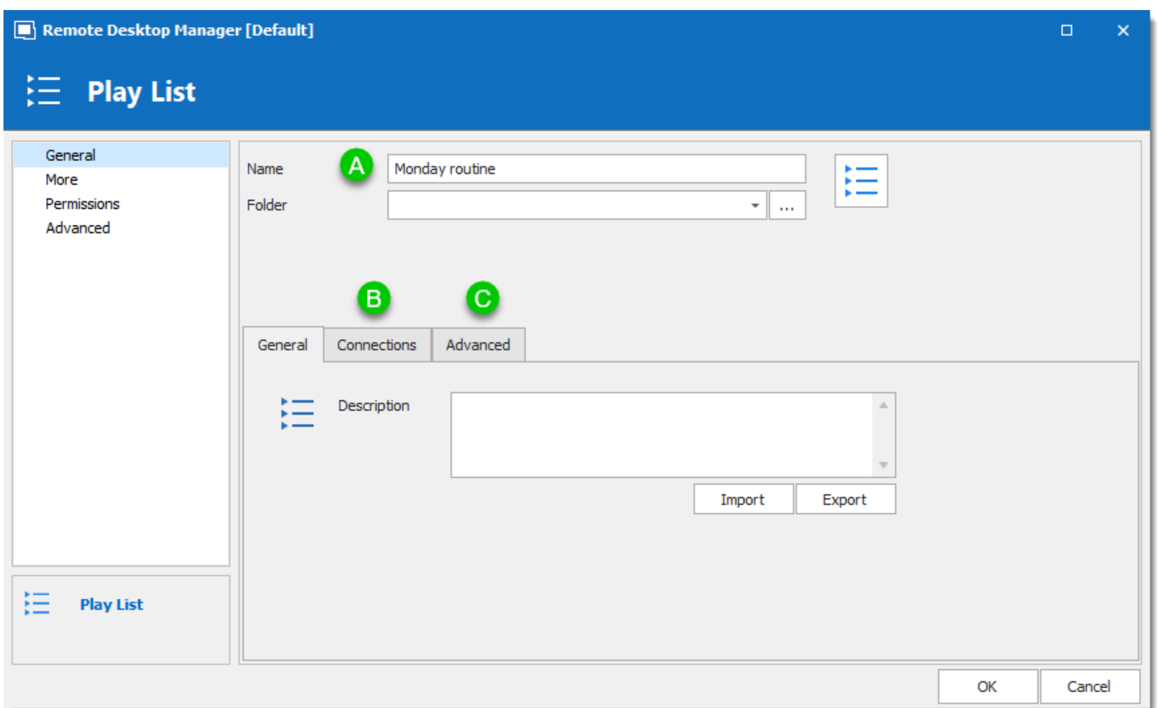
OPTION	DESCRIPTION
Pane	remove entries to the Play List if you desire.
Opened Tabbed Sessions	All currently opened sessions (Embedded only) will already be selected for your Play List. You can still add and remove entries to the Play List if you desire.
No Selection	No pre-determined selection will be taken into account, create your Play List from a fresh start.

5. Follow this sequence:

a) Enter a name for your Play List.

b) You can review, add or remove entries from the play list on the ***Connections*** tab.

c) In ***Advanced*** you can set how the entries open.

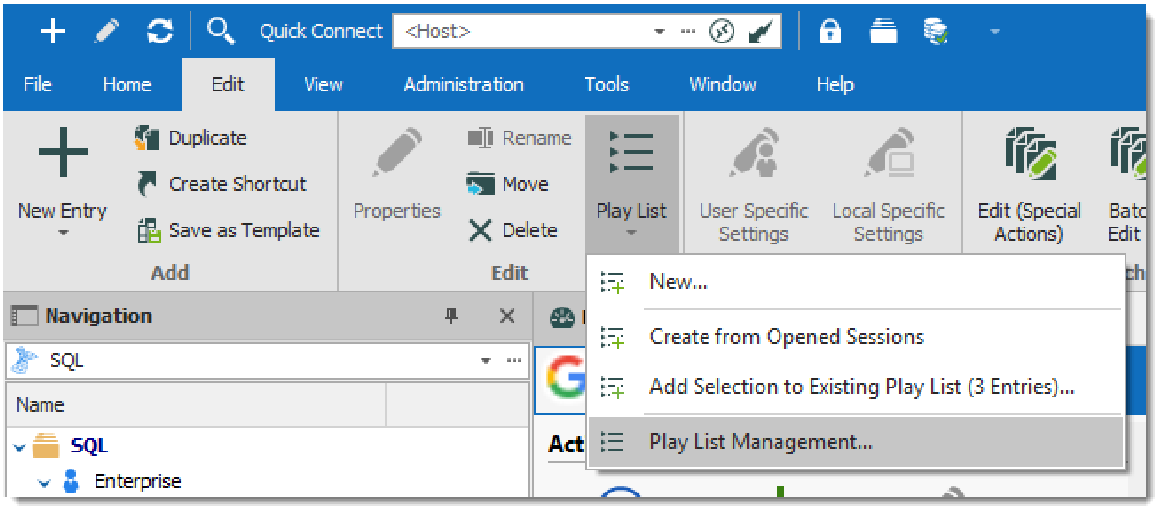


Play List Editor

And there you have it, your Play List is ready for use.

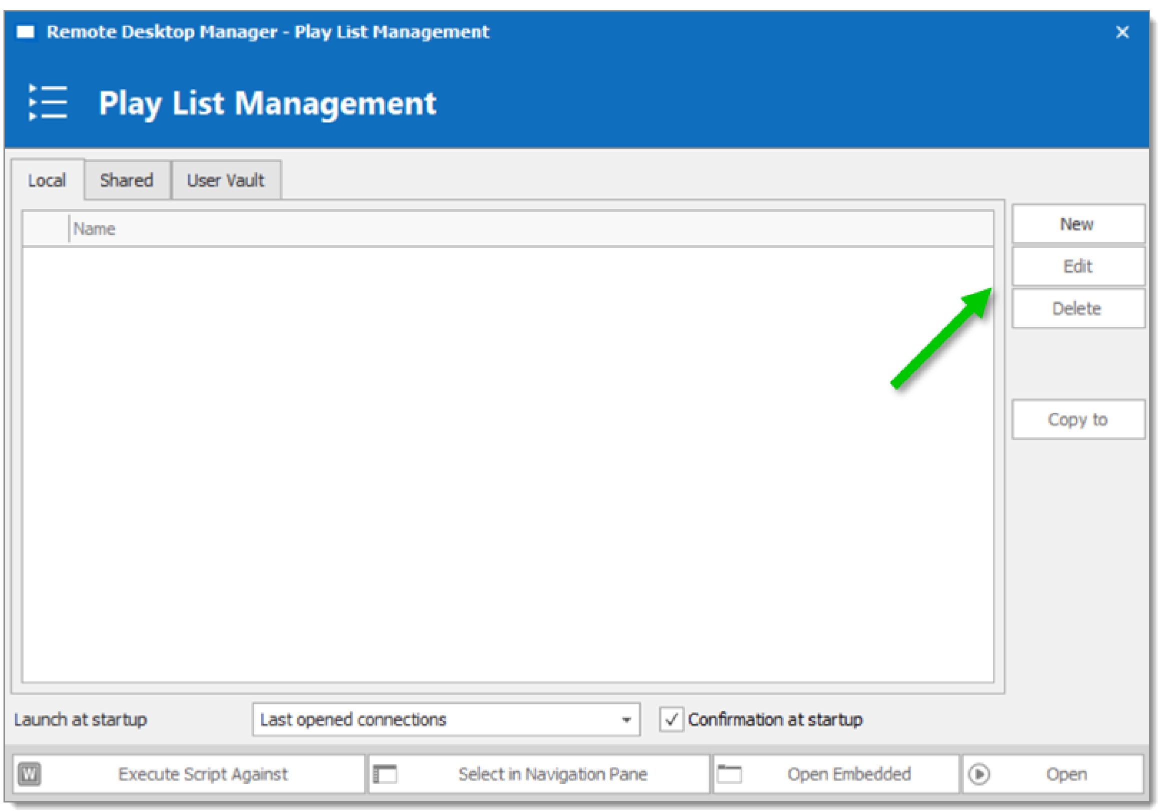
EDIT EXISTING PLAY LIST

1. On Edit, click **Play List Management.**



View - Play List Management

2. Select the Play List you wish to modify and click **Edit**.



Play List Management

If the Play List is shared or saved in your User Vault, you can also right-click the entry and click ***Properties*** to access it.

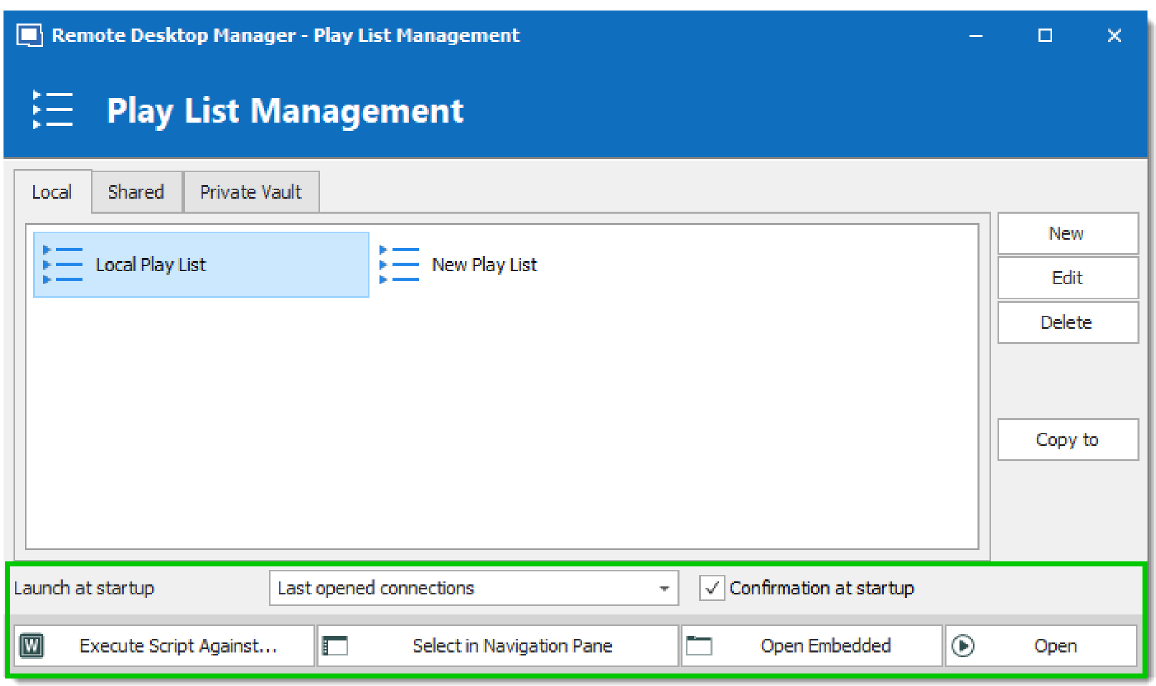
6.5.2.1.2 Play List Management

SETTINGS

USING A PLAY LIST

First, open your Play List Management ***Edit – Play List – Play List Management***.

There are five methods to using your Play List.



Default Mode

OPTION	DESCRIPTION
Open	Launch the selected Play List.

OPTION	DESCRIPTION
Open Embedded	Overrides the display selection of entries inside the Play Lists and launches them as Embedded (some entries might not support this).
Select in Navigation Pane	Selects all entries the Play List contains in the Navigation Pane.
Execute Script Against...	This will prompt for you to select the **Typing Macro** (exclusively) you wish to execute against your Play list.
Launch at startup	Here you can select a specific Play List you would like launched whenever the application starts. You can also default back to **None** or **Last opened Connections**.

6.5.3 Setting Overrides

6.5.3.1 Specific Settings

DESCRIPTION

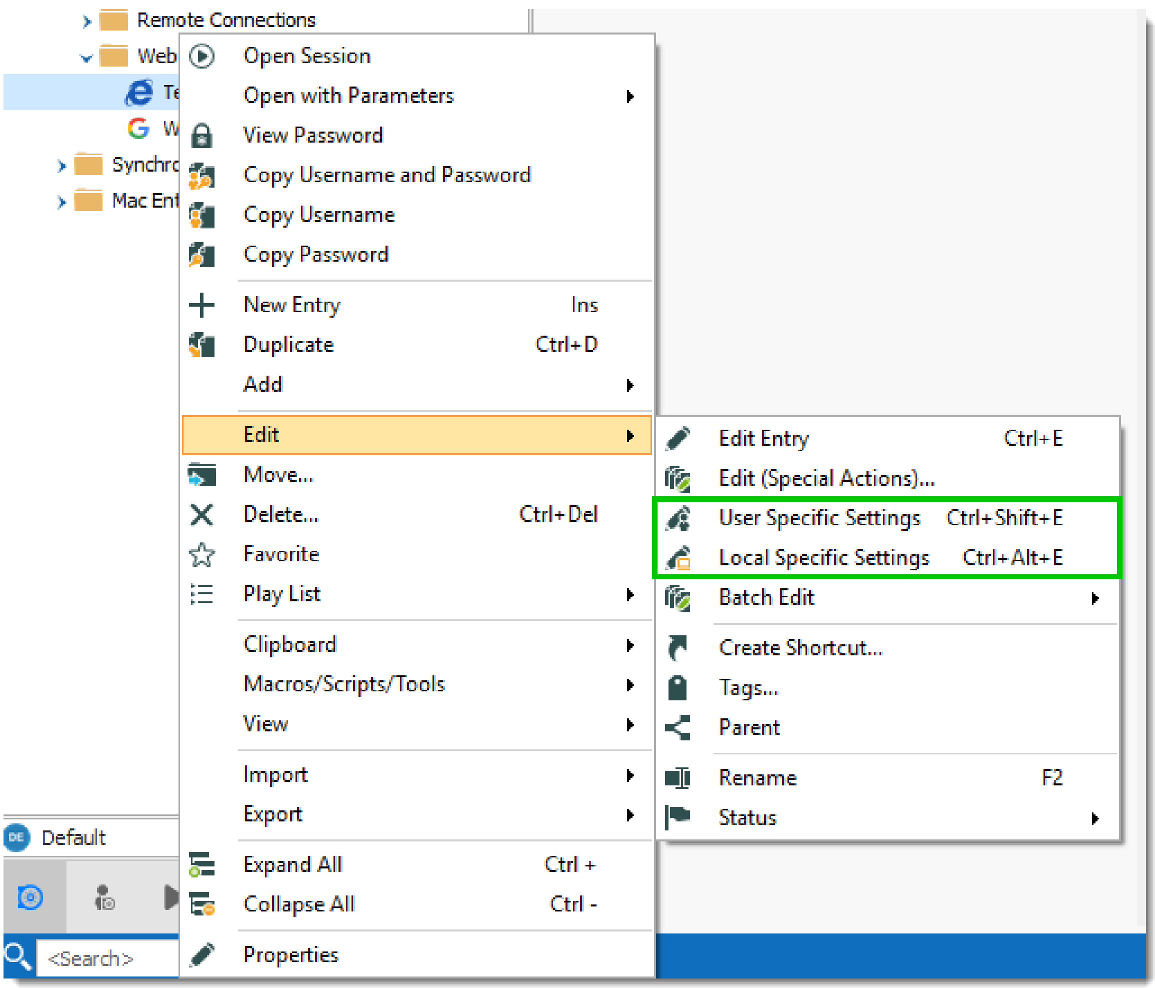
Specific Settings are used to override the properties of an entry. Several settings can be overridden, such as the credentials or the display mode. There are two types of Specific Settings: user Specific Settings and local machine Specific Settings.

- **User Specific Settings** override an entry's properties for a single user.
- **Local Specific Settings** override an entry's properties for all users of a specific device.

> This feature is only available when using an Advanced Data Source. A setting on the data source allows usage of Specific Settings. Contact your administrator if the menu is grayed out.

If both User Specific Settings and Local Specific Settings are defined on the same entry, Local Specific Settings have the priority.

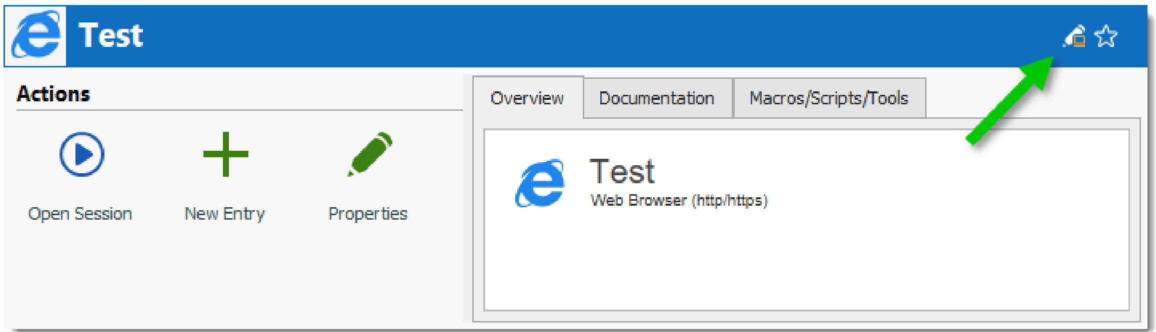
These can also be accessed by using the right-click on an entry and going to ***Edit – User/Local Specific Settings***.



Context menu – Edit – User and Local Specific Settings

SPECIFIC SETTINGS INDICATOR

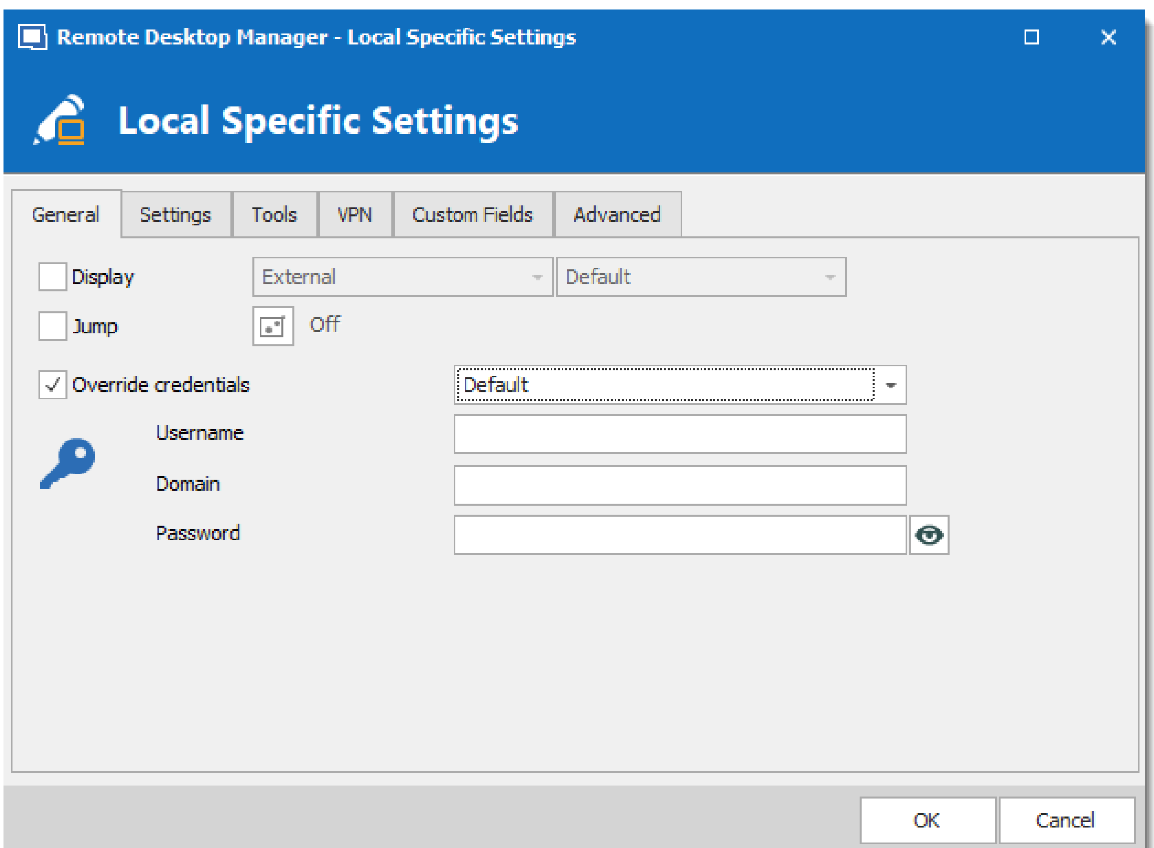
An indicator icon is displayed in the dashboard when an entry with **Specific Settings** is selected. Click on the icon to open the **Specific Settings** dialog.



Specific Settings indicator

WORKFLOW

In the majority of cases, editing the **Specific Settings** displays the following dialog:



User Specific Settings

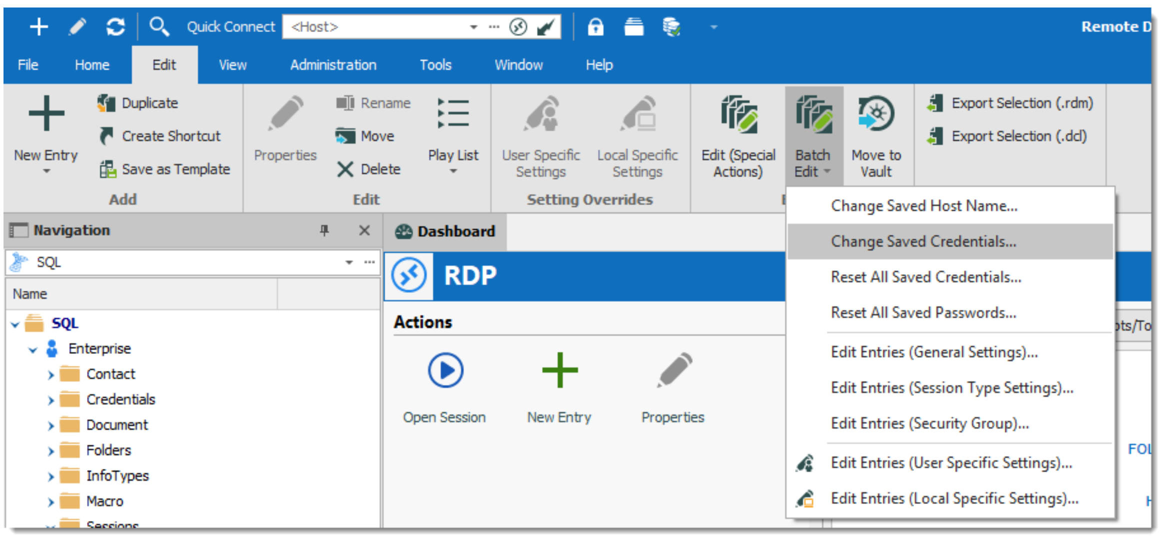
Specific settings are context sensitive, and several settings might not be available for some entry types.

6.5.4 Batch

6.5.4.1 Batch Edit

DESCRIPTION

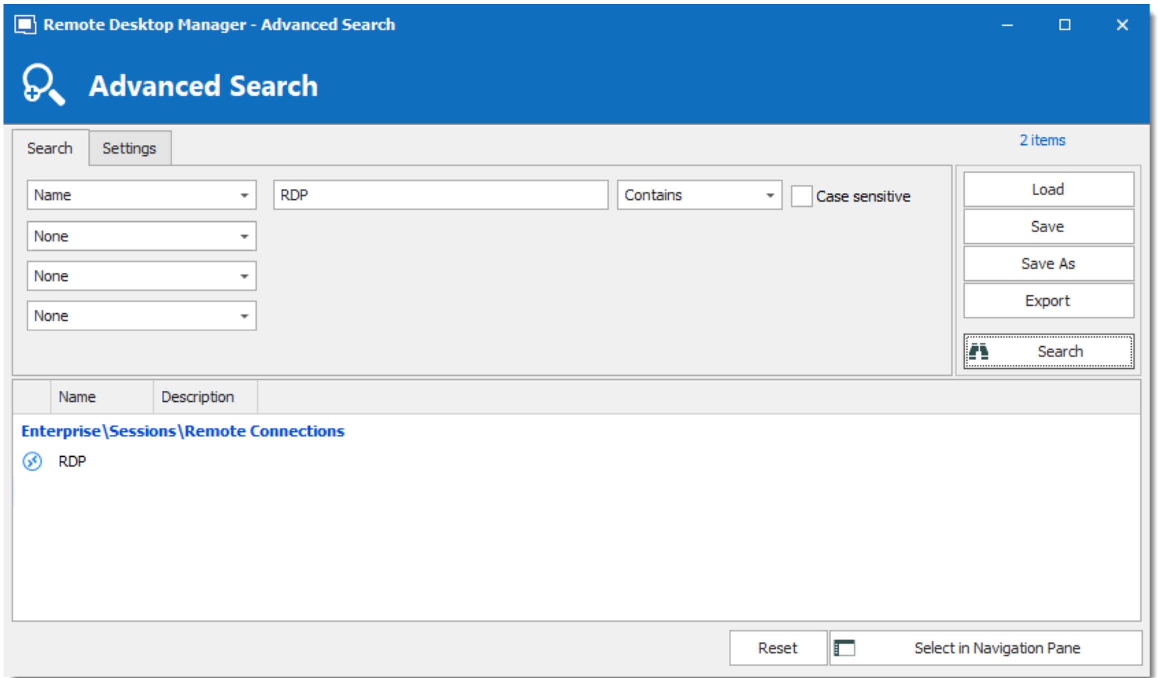
The **Batch Edit** feature changes the settings of multiple entries in one operation. For example, it can be used to remove or update the credentials of a group of sessions.



Edit - Batch Edit

ADVANCED SELECTION

Select multiple entries by using the usual **Ctrl/Shift + Left-click**, etc. For a method with a little more power, use the Advanced Search feature, which allows to select multiple entries at once, based on the defined criteria. The advanced search is available in ***View – Advanced Search***. If required, you can achieve similar result with the **Multi Vault Advanced Search**.



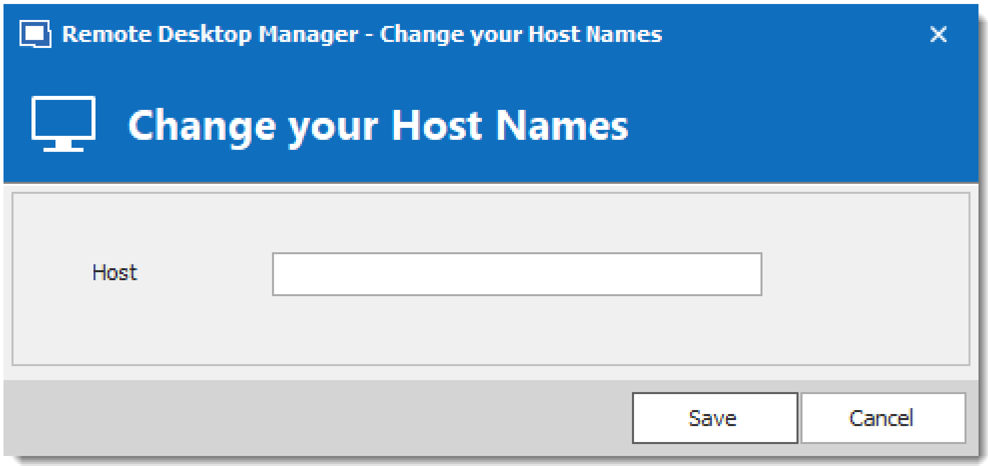
Advanced Search

Press on **Select in Navigation Pane** to select the same entries as in the **Advanced Search** dialog. Then use ***Edit – Batch Edit*** to edit all the selected entries.

SETTINGS

CHANGE SPECIFIC SETTING

You can choose to change a specific setting, for instance, the Host name.



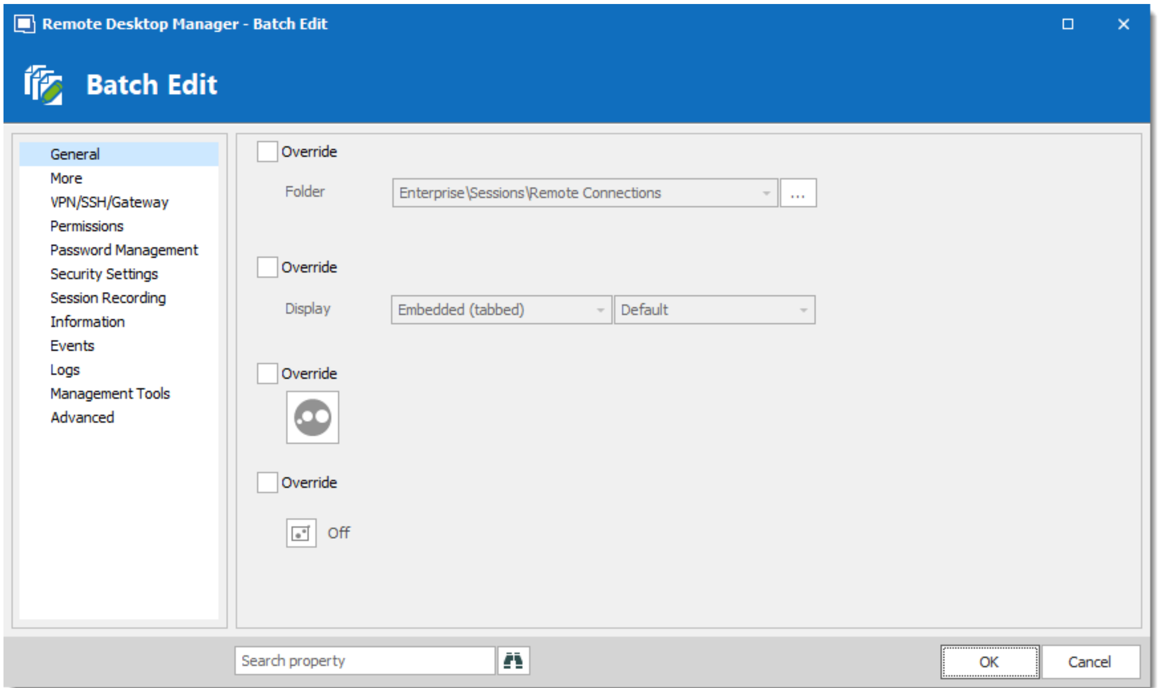
Change Host Name

RESET ALL SAVED CREDENTIALS OR PASSWORD

Clear all the existing credentials of all the selected sessions or specifically the password if desired.

EDIT SESSIONS (GENERAL SETTINGS)

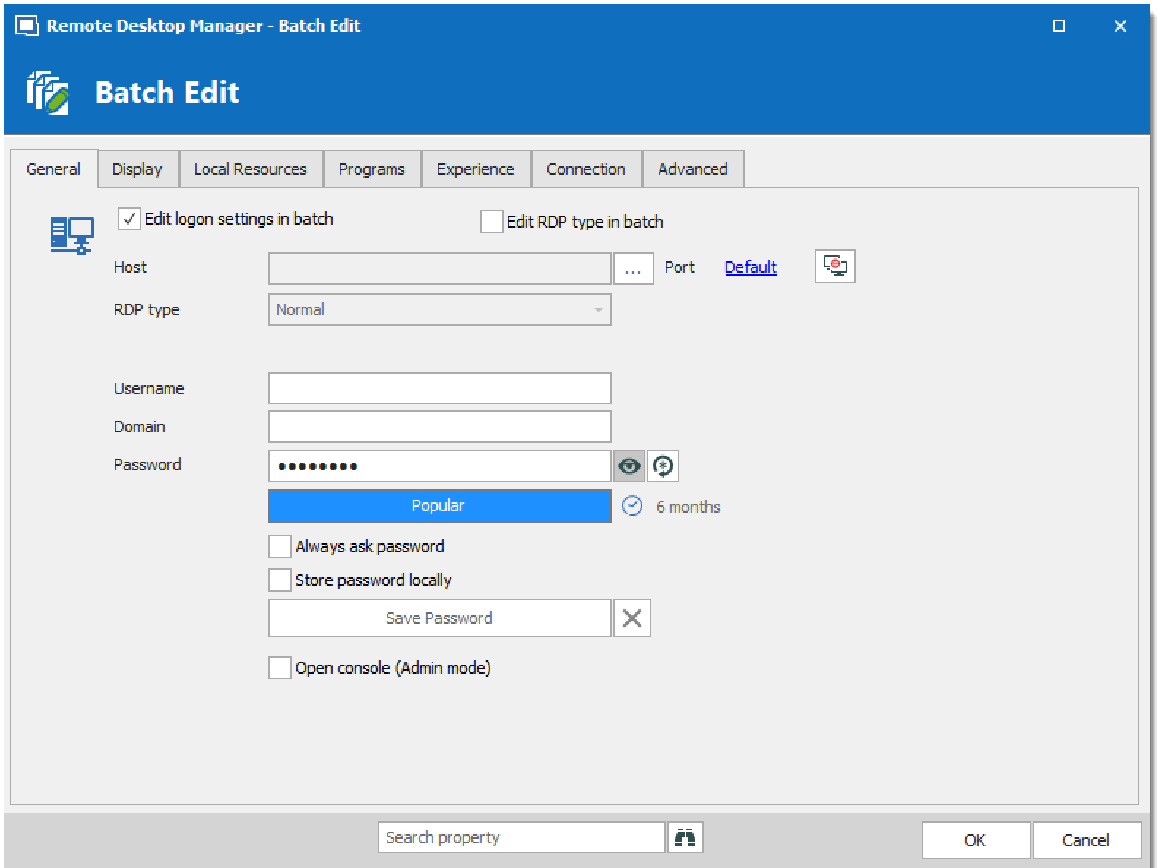
Edit Sessions (General Settings) allows you to change the common settings of all the selected entries.



Batch Edit – Common settings

EDIT SESSIONS (SESSION TYPE SETTINGS)

Change settings that are is available only for specific session types, such as Microsoft RDP.



Sessin Type Settings

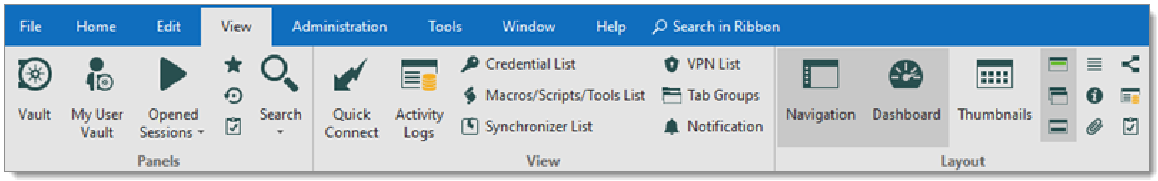
EDIT SESSIONS (USER/LOCAL SPECIFIC SETTINGS)

Specific Settings can be modified in a batch if supported by the type of the edited entries.

6.6 View

DESCRIPTION

The ***View*** tab is used to control different features regarding the panels, views, logs, and layout of Remote Desktop Manager.



View

Refer to the following topics for more information:

- ***Panels***
- ***View***
- ***Logs***
- ***Layout***

PANELS

OPTION	DESCRIPTION
Vault	Access the view mode of the ***Navigation Pane*** for the current vault.
User Vault	Display your ***User Vault*** in the ***Navigation Pane***.
Opened Sessions	Display the currently opened sessions in the ***Navigation Pane***.
PAM Dashboard	Connect to a privileged account, copy its password, and manage its checkout/check-in process through a privileged access management dashboard.
Favorites	Display your favorite entries and folders in the ***Navigation Pane***.
Recent	Display your most recently used entries in the ***Navigation Pane***.

OPTION	DESCRIPTION
Task List	Display a list of your current tasks.
Search	Search items through your database/data source using specific criteria.

VIEW

OPTION	DESCRIPTION
Quick Connect	Launch a ***Quick Connect*** session.
Activity Logs	Open the ***Activity Logs***.
Credential List	Open a window to view the credential entries in the database.
Macros/Scripts/ Tools List	Open a window to search for macros, scripts, or tools in the database.
Synchronizer List	Open a window to search for synchronizer entries in the database.
VPN List	Open a window to search for VPN entries in the database.
Tab Groups	Open a docked window to browse through the various tab groups.
Notification	Open a window to browse through the various notifications (such as entries expired or about to be, or tasks).
Message	Open a window to access your messages.

LOGS

This section only appears when using an individual type data source.

OPTION	DESCRIPTION
Local Connection Logs	Open a window to access your local logs.

LAYOUT

OPTION	DESCRIPTION
Navigation	Toggle the ***Navigation Pane***.
Dashboard	Toggle the ***Dashboard***.
Thumbnails	Toggle the ***Thumbnails***.
Top Pane (Ribbon/Menubar)	Toggle the ***Ribbon*** (right-click the application header to bring it back or use **Alt+F11**).
Grouped Tab Bar	Toggle the ***Grouped Tab Bar*** (must have group tabs to work).
Status Bar	Toggle the ***Status bar***.
Description	Toggle the ***Description*** pane.
Asset	Toggle the ***Asset*** pane.

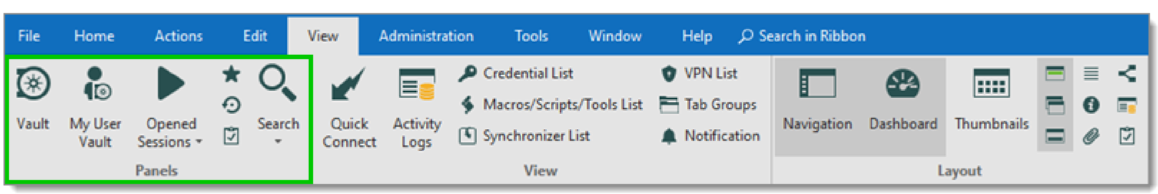
OPTION	DESCRIPTION
Attachments	Toggle the ***Attachments*** pane.
Sub Connections	Toggle the ***Sub Connections*** pane.
Logs	Toggle the ***Logs*** pane.
Task	Toggle the ***Task*** pane.

> Although they are windowed by default, all those panes can be dragged and docked anywhere within Remote Desktop Manager.

6.6.1 Panels

DESCRIPTION

In Remote Desktop Manager, the ***Panels*** section of the ***View*** tab allows you to browse and search the vaults, sessions, and entries in the ***Navigation Pane***.



Below are the different features available in this section:

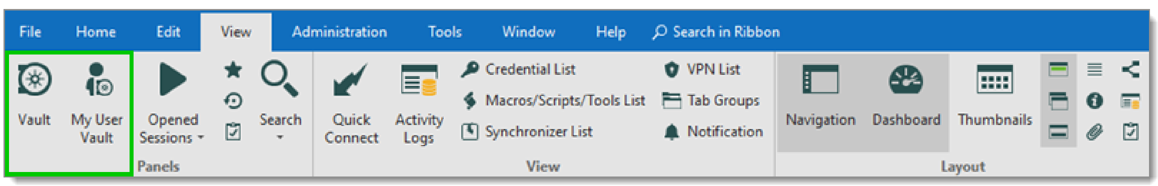
- ***Vault*** and ***User Vault***
- ***Opened Sessions***
- ***PAM Dashboard***
- ***Favorites***

- ***Recent***
- ***Task List***
- ***Search***

6.6.1.1 Vaults

DESCRIPTION

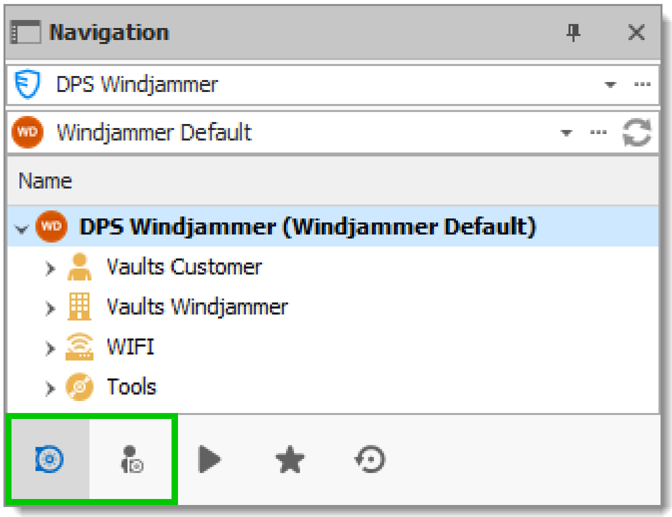
Vault are containers for your entries, your credentials, sensitive information, sessions, and more.



You will start with two vaults:

- One main default ***Vault*** created for sharing entries to team members that you grant access to. You can add and share more vaults in ***Administration - Vaults***.
- One ***User Vault***, which is user-centric and is used to store information such as personal account credentials. The ***User Vault*** prevents users from using a non-secured tool to manage their personal passwords at work. The ***User Vault*** can be disabled in ***Administration - System Settings - User Vault***.

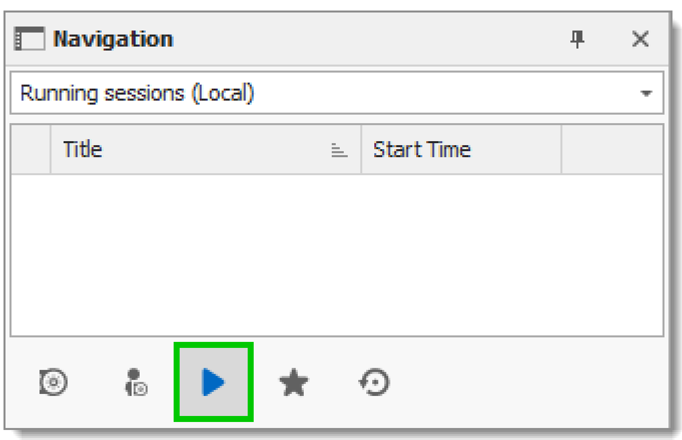
The two vault types can also be found in the ***Navigation Pane*** menu.



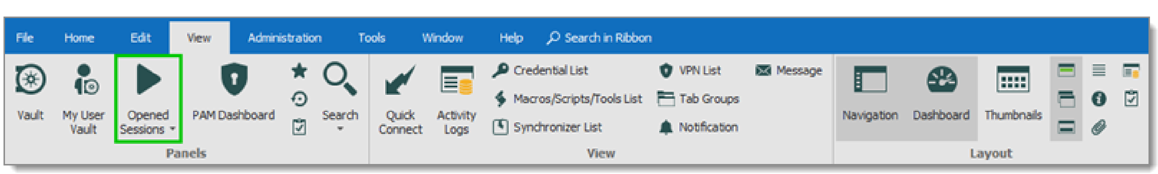
6.6.1.2 Opened Sessions

DESCRIPTION

The ***Opened Sessions*** tab shows currently running sessions by type and for the local machine only. The ***Opened Sessions*** can be accessed from the ***Navigation Pane*** menu.



It is also located in the [***Panels***]() section of the [***View***]() tab in the ***Ribbon***.

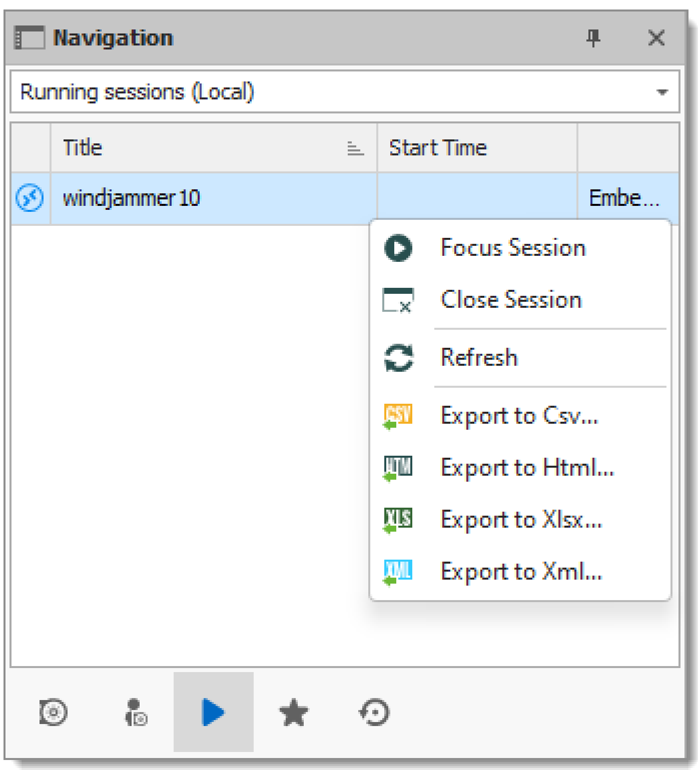


You can give the focus to an opened session by double-clicking it from the list. All of the embedded sessions are listed and the external sessions will appear if Remote Desktop Manager is able to discover the specific type of session.

Opened sessions can be sorted by types:

- ***Running sessions (Local)***
- ***Running sessions (Global)***
- ***Hidden session tabs***
- ***VPN groups (Opened)***
- ***Entry states***

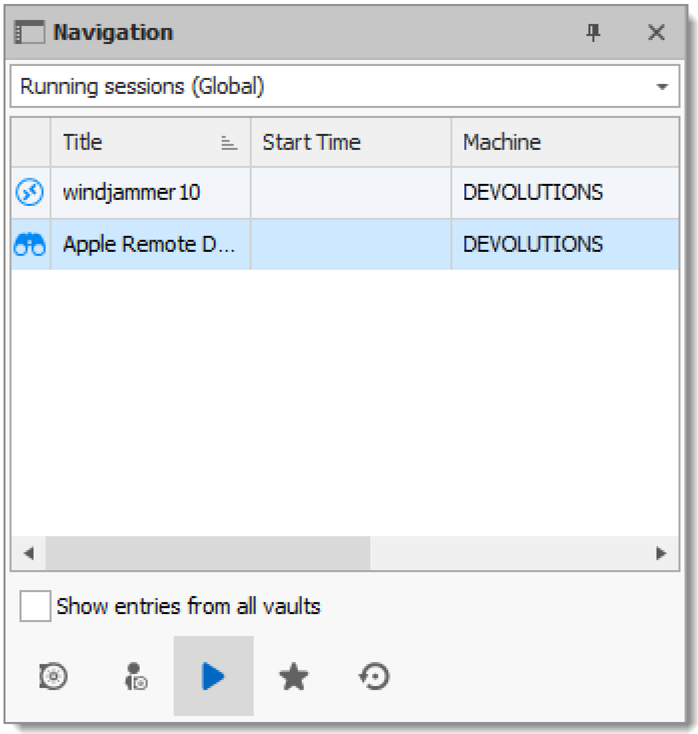
RUNNING SESSIONS (LOCAL)



Local Opened Sessions

RUNNING SESSIONS (GLOBAL)

With the SQL Server data sources, you can monitor currently running sessions, provided they have been opened within Remote Desktop Manager.



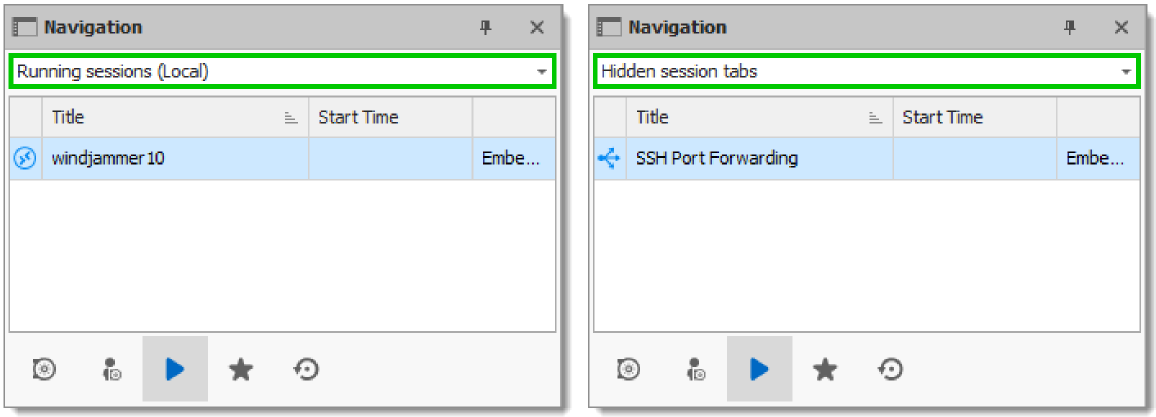
Global Opened Sessions

For many reasons beyond our control, it is possible for a session to be terminated without Remote Desktop Manager being aware that this has occurred. This can happen, for example, if Remote Desktop Manager is not running when another application ends. Therefore, any terminated session will remain listed in the log. You may manually mark it as closed via the contextual menu by selecting ***Flag as Closed***.

To review a detailed log, double click on a session entry.

HIDDEN SESSION TABS

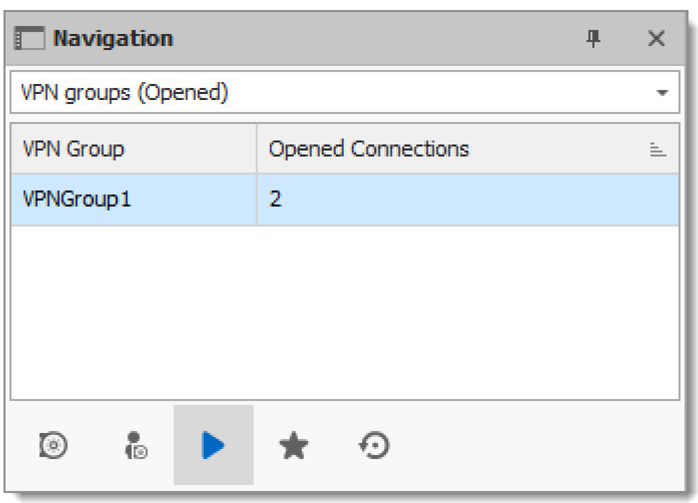
Some sessions, like SSH Port Forward, can be hidden from the dashboard when the connection is established. When these sessions are hidden, they are not displayed in the ***Local Sessions***. Select ***Hidden Sessions*** from the combo box above the entry list to display hidden sessions only.



Local Sessions / Hidden Sessions

VPN GROUPS (OPENED)

Sessions can be configured to use a VPN Group. When multiple sessions are using the same VPN group, it will appear in this section with the number of opened connections using that same group.

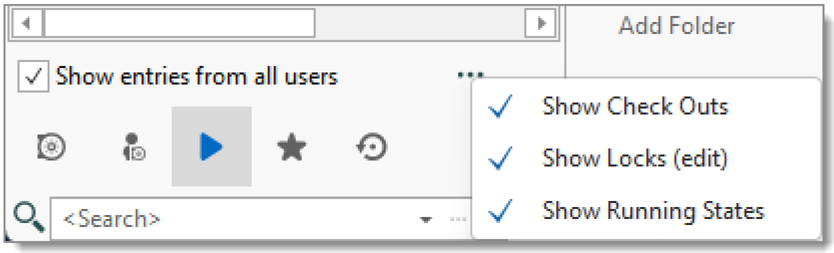


VPN Groups

ENTRY STATES

You can see the status of the entries in the selected database.

There are different viewing options. You can choose to show entries from all users and checked out, locked, or running entries.



Different Viewing Options

NOTES

- Remote Desktop Manager tries to detect opened sessions even if they were not launched from the application. It uses the name of the process to accomplish this task.
- VPN sessions do not appear in the list.

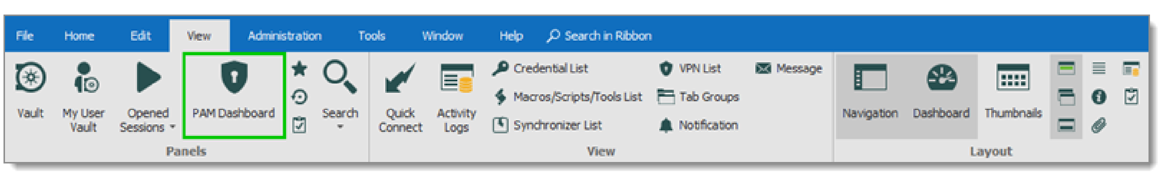
6.6.1.3 PAM Dashboard

DESCRIPTION

A license is now required to enable the Privileged Access Management (PAM) module. Please contact our sales department for more information about the license.

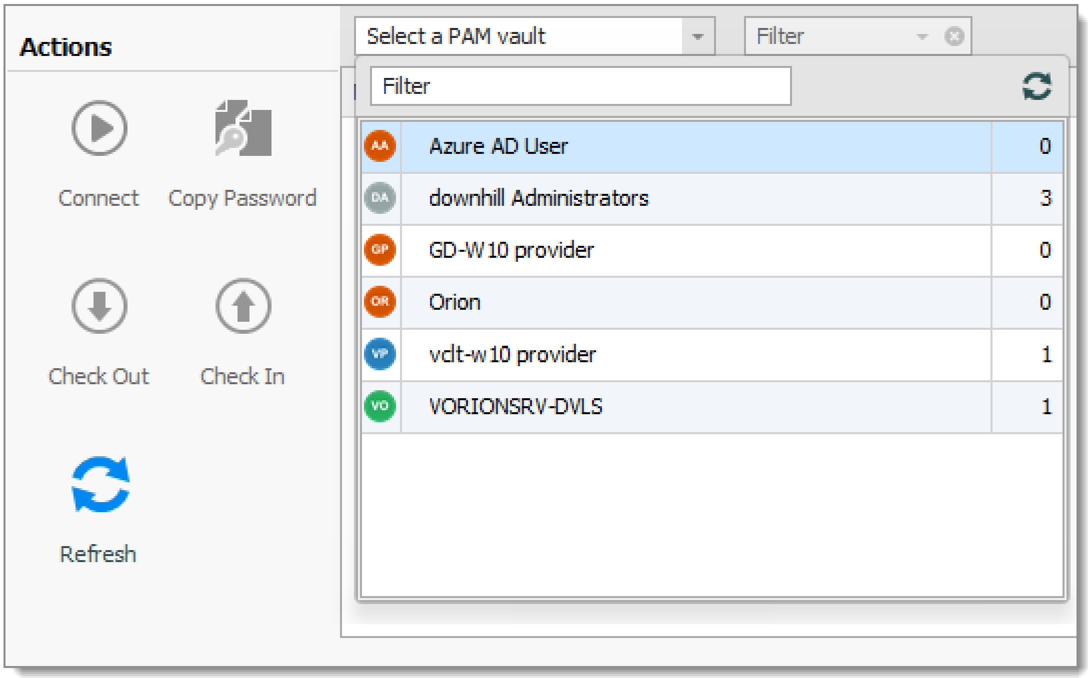
The ***PAM Dashboard*** is only available with our Devolutions Server.

The ***PAM Dashboard*** feature can be found in ***View - Panels - PAM Dashboard***.

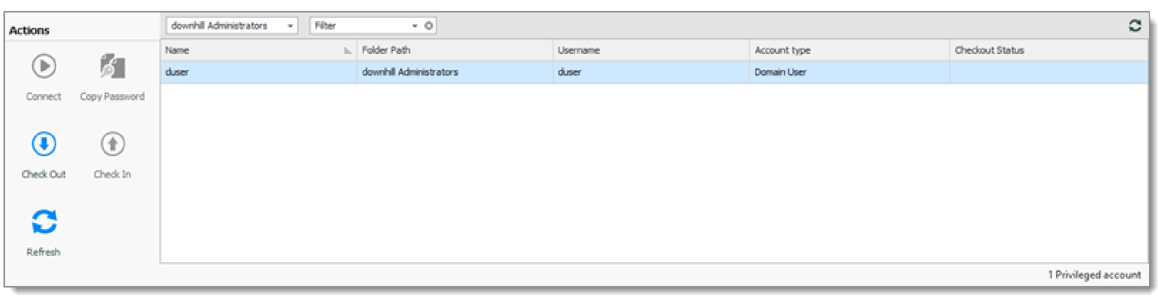


In the ***PAM Dashboard***, for every privileged account, it is possible to connect to the account, copy the password, and manage the checkout/check-in process.

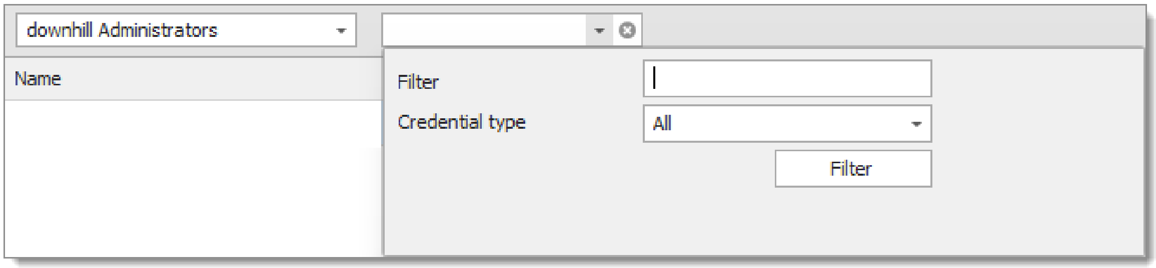
To access the user accounts, a PAM folder must first be selected. If you have multiple folders, it might be helpful to use the filter bar to find the one you are looking for. Note that these are the same folders as in your Devolutions Server console. You can go to our Privileged Account Management in Devolutions Server topic to learn more about it.



When the folder is selected, all the accounts in that folder will appear. It is possible to sort them by ***Name***, ***Folder Path***, ***Username***, ***Account Type***, or ***Checkout Status***.



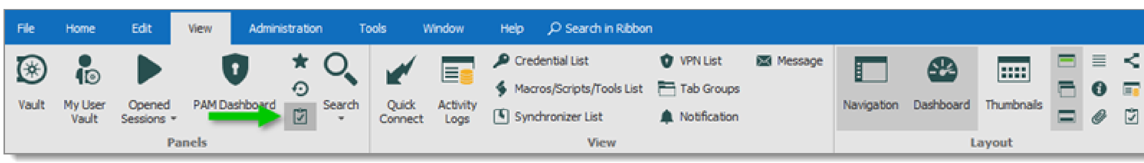
If there are multiple accounts in the folder, you can use the filter bar to display only the accounts containing what you typed. You can push your search even further by filtering the accounts by credential type.



6.6.1.4 Task List

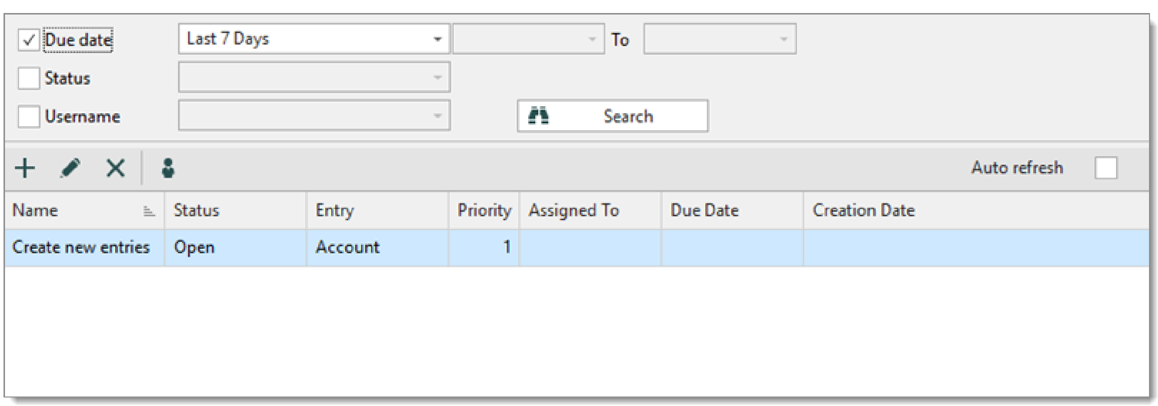
DESCRIPTION

Create a ***Task List*** to keep track of work that needs to be done by the team. Toggle the ***Task List*** pane in ***View - Panels - Task List***.



You can perform a search to filter out the list of displayed tasks. You can search by ***Due Date***, ***Status***, or ***Username***.

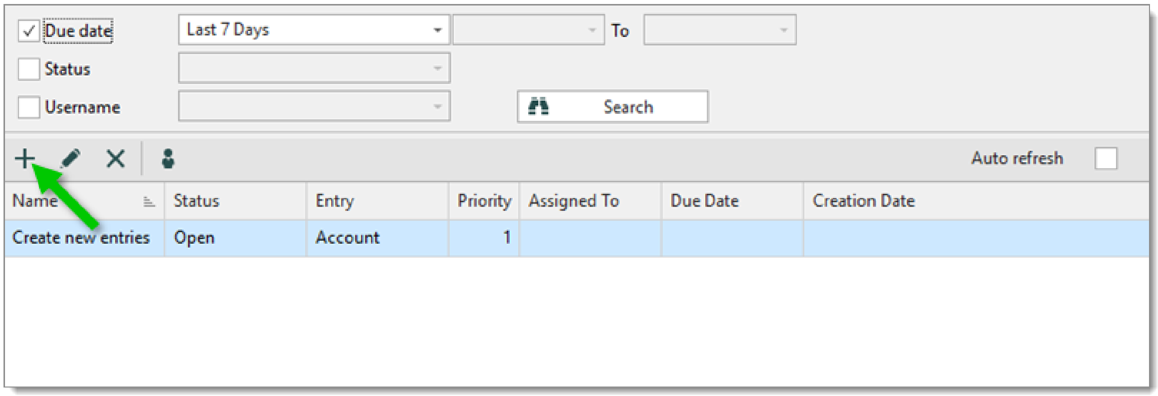
This feature is only available for the following data sources: Devolutions Server, Azure SQL, SQL Server, and SQLite.



Task List

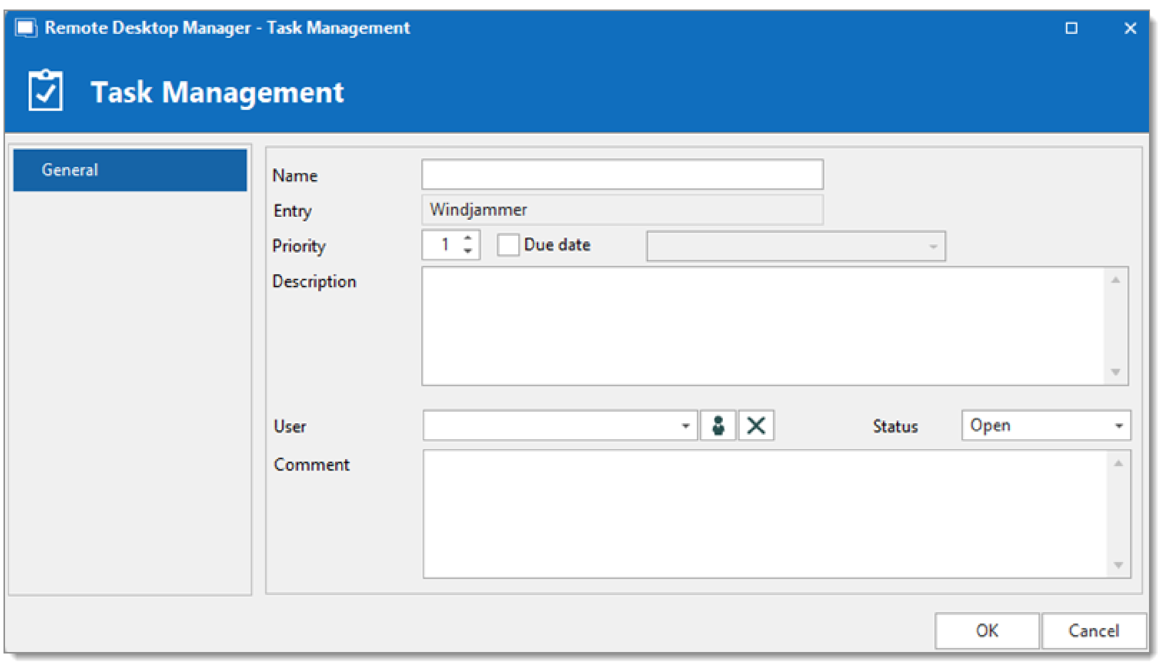
CREATING A TASK

1. Click on **Add** to open the ***Task Management*** window.



Add a task

2. Enter your task information, like the name of the task, the priority, the due date, the description, etc.



Task Management

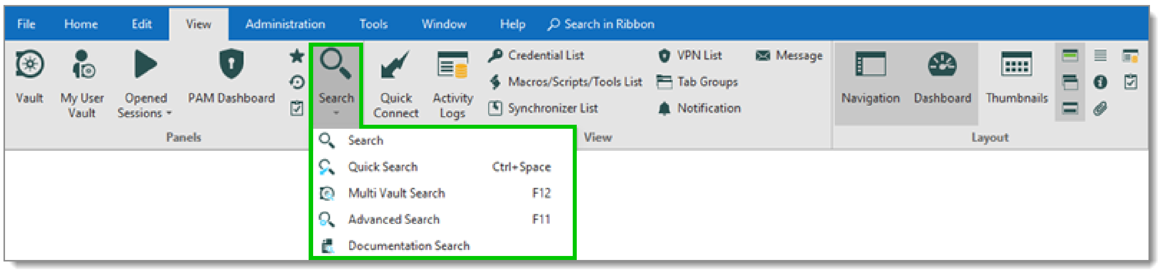
OPTION	DESCRIPTION
Name	Enter a custom name for the task.

OPTION	DESCRIPTION
Entry	Displays the entry currently selected in the Navigation Pane. The task is assigned to this entry. It is a read-only field.
Priority	Set the priority of the task (from 0 to 100).
Due date	Set a deadline for the task.
Description	Enter a description of the task for the assigned user.
User	Assign a user to the task.
Assign me to this task	Click this button to assign the task to yourself.
Delete	Clear the assigned user.
Status	Set a status for the task. Select between the following: • **Open** • **Assigned** • **In progress** • **Closed** • **Done** • **Cancelled** • **Postponed**
Comment	Enter a comment for the task.

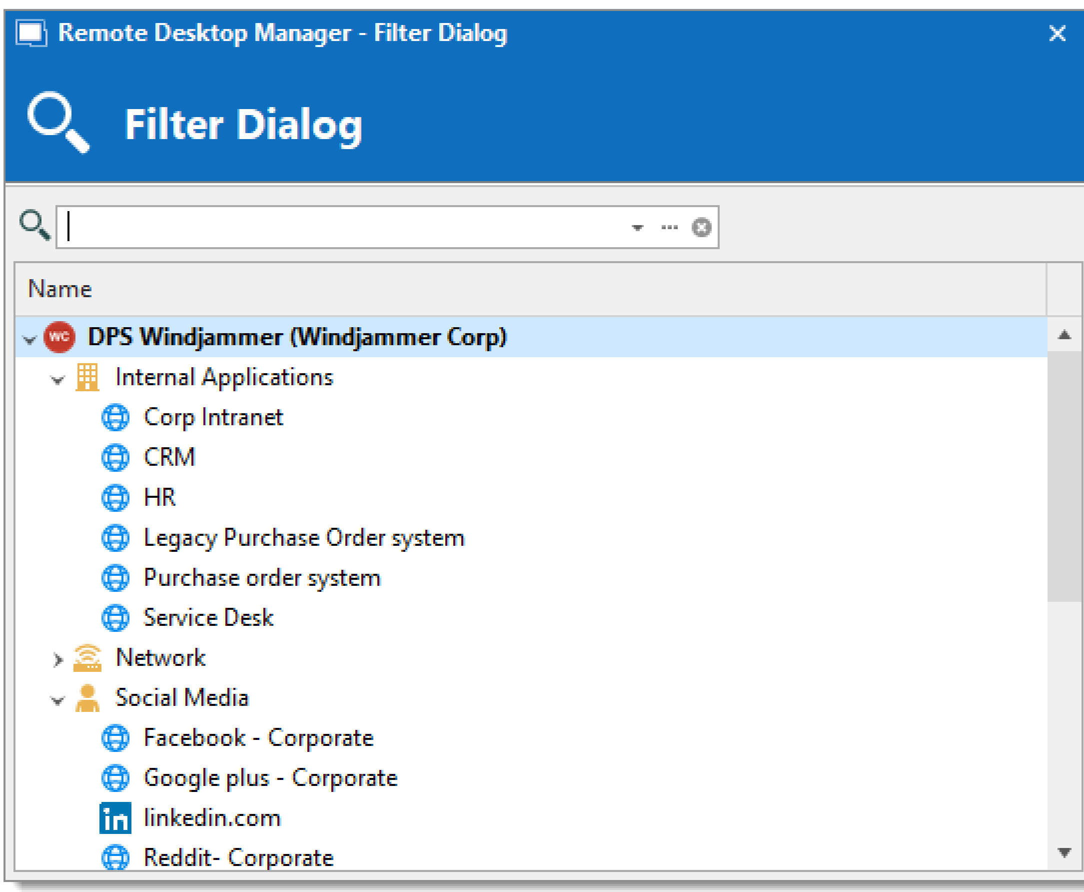
6.6.1.5 Search

DESCRIPTION

The ***Search*** function in the ***Panels*** section of the ***View*** tab allows you to search folders and entries in the database you are currently in.



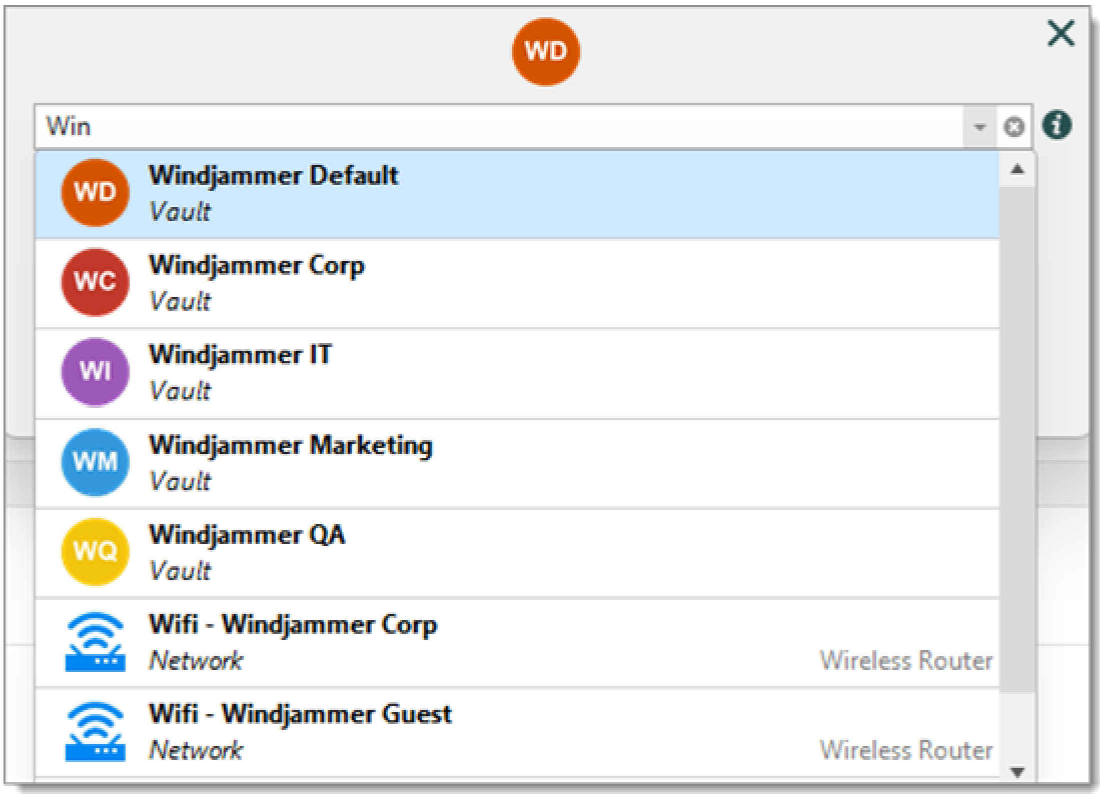
When using the ***Search*** function, a tree view is also displayed, showing exactly where the results of your search are located in the database. Filter options are also available when clicking on the ellipses button. Learn more about them in our Search/Filter topic.



It is also possible to do a ***Quick Search***, which allows you to search through the database without displaying the tree view. The results are therefore more concise.

Pro tip: Use the following shortcuts while selecting an entry for an even quicker search.

- Press **Enter** to navigate to the entry.
- Press **Ctrl+Enter** to open the entry.
- Press **Ctrl+R** to navigate to the root folder of the entry.



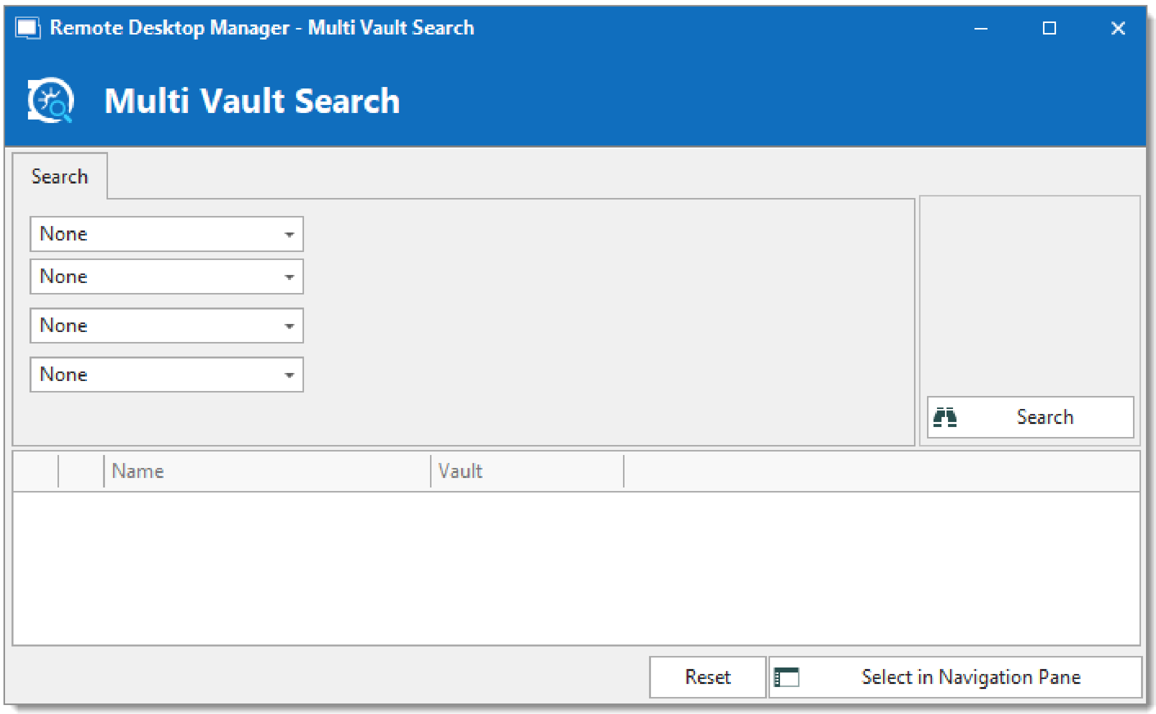
For information about other search methods, see our related topics:

- [***Multi Vault Search***]
- [***Advanced Search***]
- [***Documentation Search***]

6.6.1.5.1 Multi Vault Search

DESCRIPTION

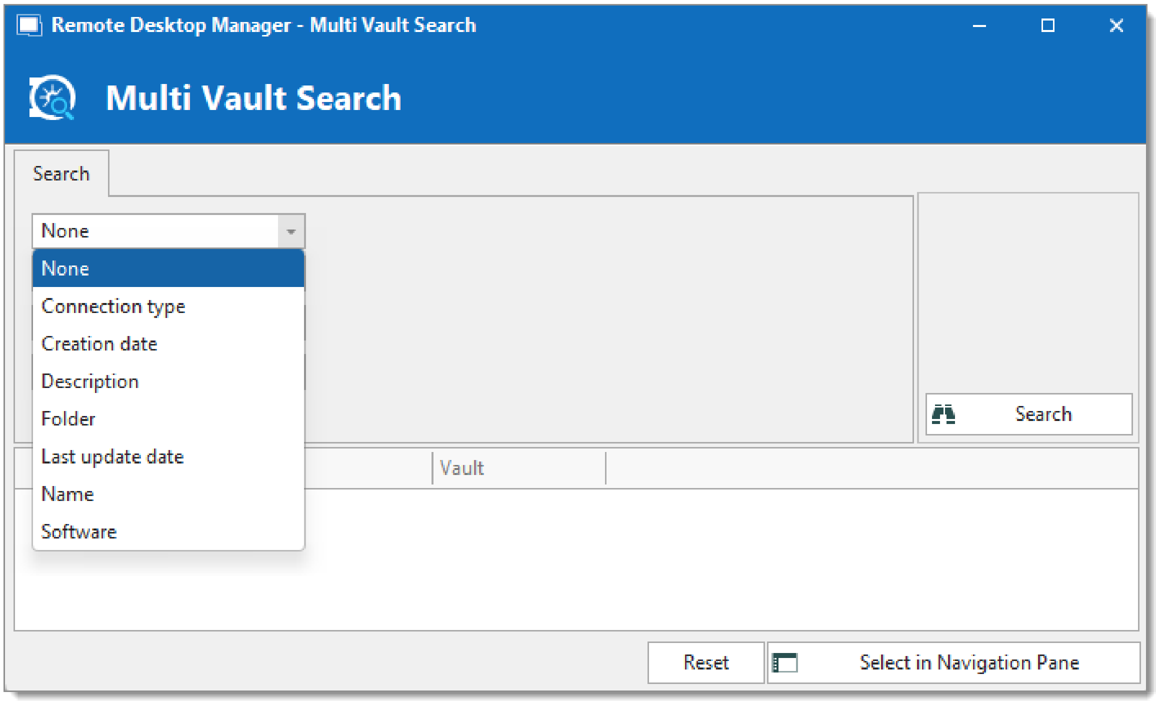
The ***Multi Vault Search*** feature of Remote Desktop Manager allows you to search for folders and entries in all the vaults of the selected data source at once.



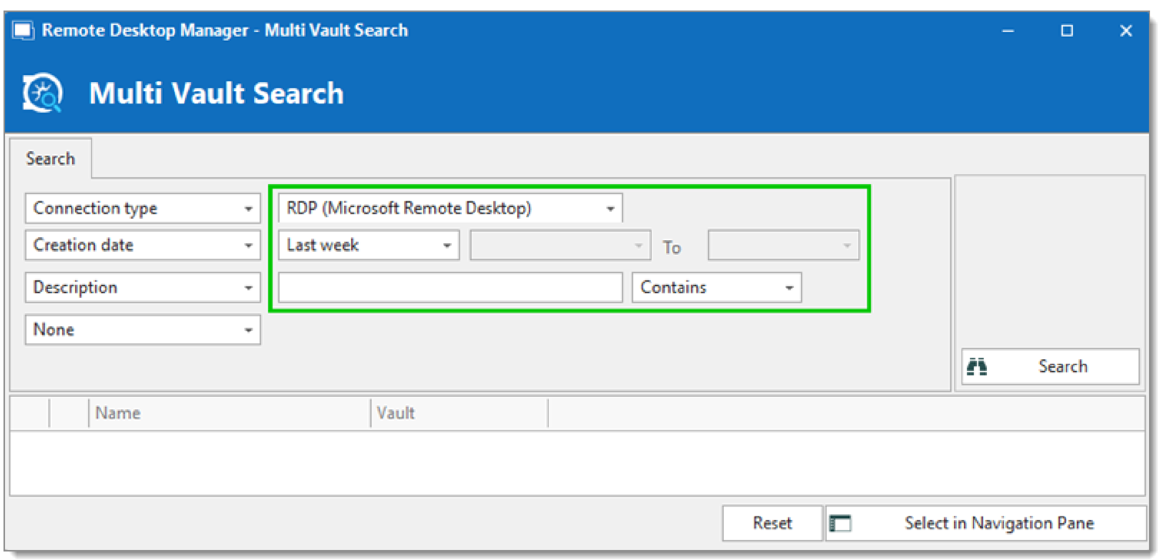
CRITERIA TYPES

The following criteria are available to refine your search: ***Connection type***, ***Creation date***, ***Description***, ***Folder***, ***Last update date***, ***Name***, and ***Software***.

At least one criterion must be used to filter your results, and a maximum of four criteria can be applied at once.



Drop-down lists will appear when selecting certain criteria to give you more search options.

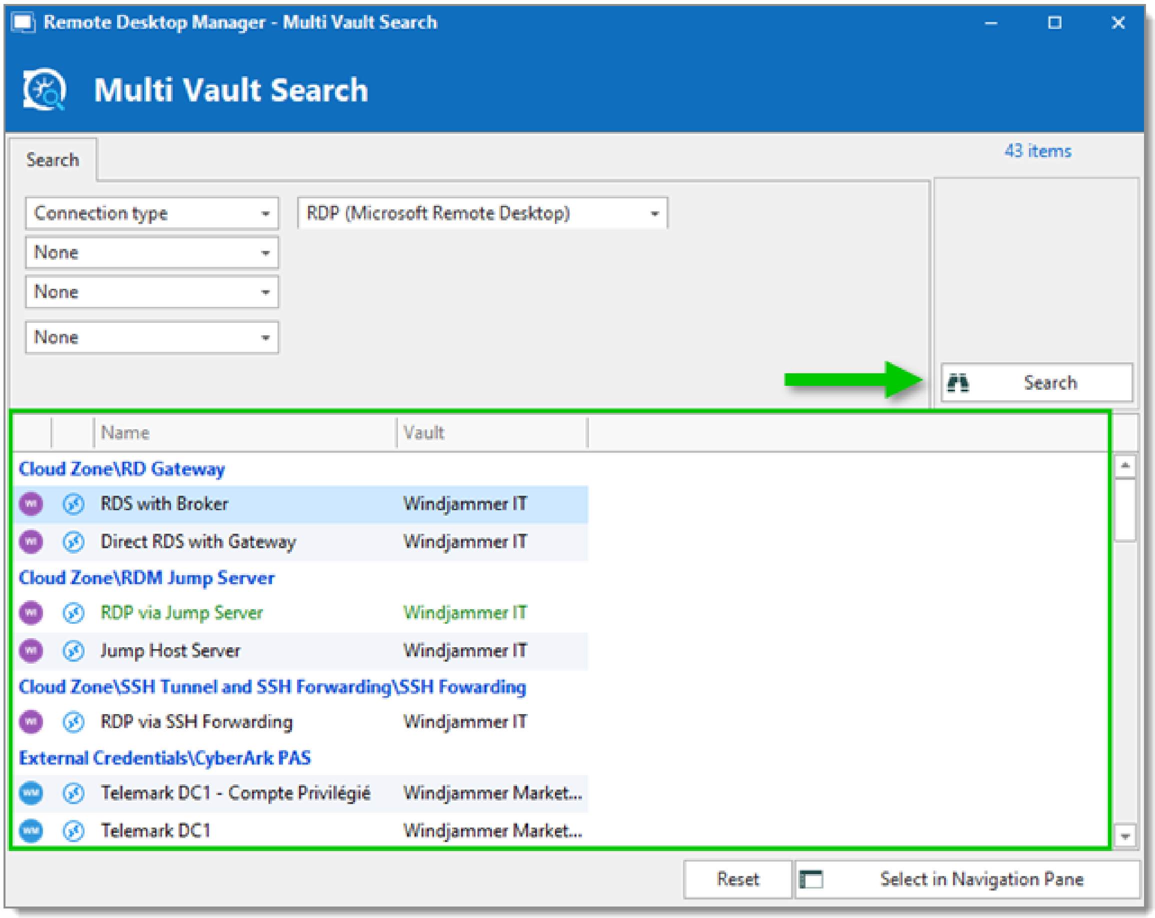


Below is a description of what each of these drop-down lists type is used for.

CRITERIA	DROP-DOWN LIST DESCRIPTION
Connection type	Select from the list the connection type of the entries you are looking for.
Creation date **Last update date**	Select from the list the period of time, up to 90 days ago, when the entries/folders were created or last updated. There also is a custom option in the list that allows you to specify dates to delimit your time period. This can be useful if you want to search between specific dates or if the entries or folders were created / last updated more than 90 days ago.
Description **Folder** **Name**	Search by typing part or all of a word in the name of the entries or folders or in their description. From the list, select the option that applies: • ***Contains*** - any name that includes the characters you have entered, anywhere in the field name. • ***Starts with*** - any name beginning with the characters you have entered. • ***Ends with*** - any name ending with the characters you have entered. • ***Exact expression*** - will find names that match every character you have entered, exactly as entered.

RESULTS DISPLAY

The results are displayed when the ***Search*** button is pressed. Once done, the name of all entries and folders and the vault in which they are located are shown in the results field. The paths to entries or folders are also displayed above each result or result group.



It is possible to select multiple entries at once by shift-clicking or all of them with the **Ctrl+A** shortcut. Right-clicking one or more entries shows the same menu and options as the ***Navigation Pane***.

OTHER FUNCTIONS

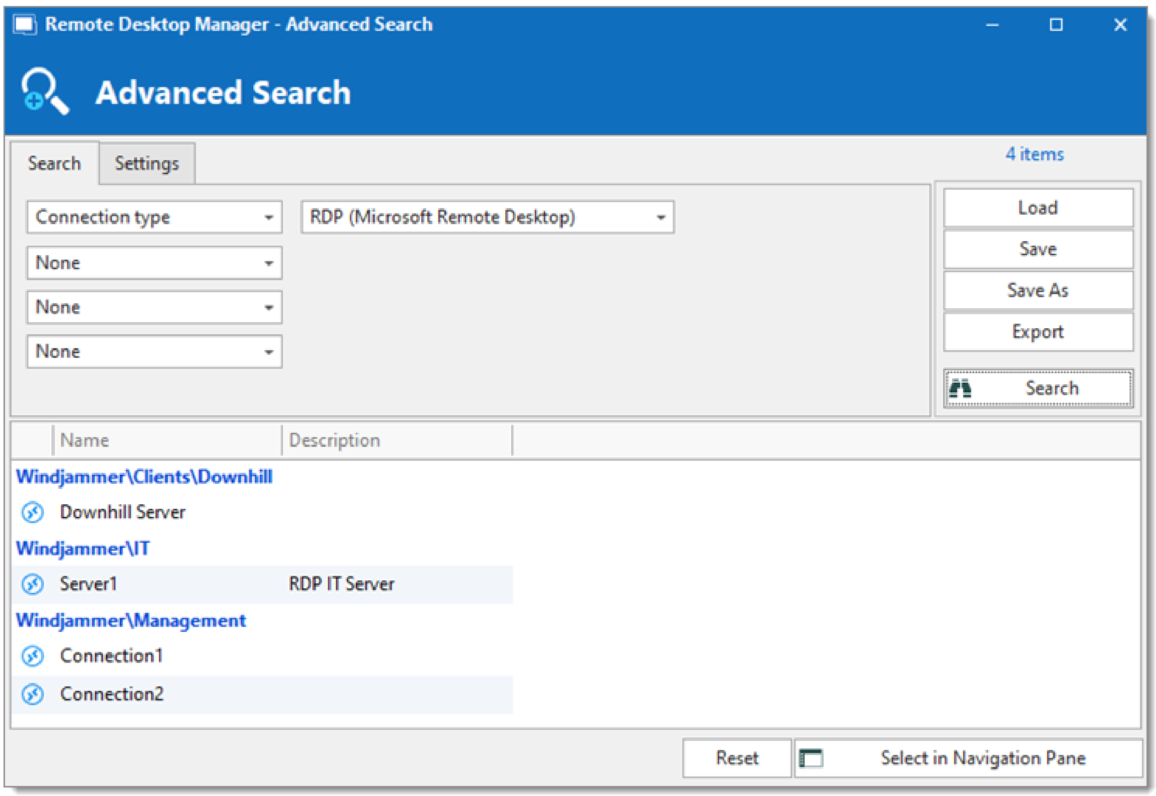
The ***Select in Navigation Pane*** button, when pressed, takes you directly to the selected entry or folder in the corresponding vault's ***Navigation Pane***.

The ***Reset*** button clears all your search results and options, giving you a clean slate for a new search.

6.6.1.5.2 Advanced Search

DESCRIPTION

The ***Advanced Search*** allows you to search for entries and folders based on multiple criteria in one vault at a time. To search multiple vaults simultaneously, please refer to the ***Multi Vault Search*** topic.



Advanced Search Window

It is possible to select multiple entries at once by shift-clicking or all of them with the **Ctrl+A** shortcut. Right-clicking one or more entries shows the same menu and options as the ***Navigation Pane***.

SEARCH TAB

OPTION	DESCRIPTION
Criteria	You can select multiple different criteria at once to tweak

OPTION	DESCRIPTION
	your search: • ***Connection type*** • ***Contact reference*** • ***Creation date*** • ***Custom field*** • ***Description*** • ***Domain*** • ***Folder*** • ***Host*** • ***Is favorite*** • ***Tags*** • ***Last update date*** • ***Name*** • ***OS*** • ***Password strength*** • ***Security group (legacy)*** • ***Serial Number*** • ***Server role*** • ***Status*** • ***Username*** • ***URL***

OPTION	DESCRIPTION
	• ***Version*** • ***IP*** • ***MAC*** • ***Software***
Load	Load searches that have been previously saved.
Save	Save your search locally and reuse it.
Save As	Save a previously saved search but under a different name.
Export	Export the entries of your search result as a CSV, HTML, XLS or XML file. Sensitive information will be encrypted using AES.
Search	Once you have selected your search criteria, click on ***Search*** to display the search results.
Reset	Reset all your fields to proceed with a new search.
Select in Navigation Pane	Select your search result in your ***Navigation Pane***. This option can be used in combination with a Batch Edit.

There will be a drop-down list next to certain criteria fields (ex: Name) to give you more search options:

- ***Contains*** - any name including the characters you have entered.
- ***Starts with*** - any name beginning with the characters you have entered.
- ***Ends with*** - any name ending with the characters you have entered.
- ***Exact expression*** - any name exactly matching every character you have entered.
- ***Does not contain*** - any name that does not include the characters you have entered.

- ***Regular expression*** (regex) - any sequence of characters specifying a search pattern.

6.6.1.5.3 Documentation Search

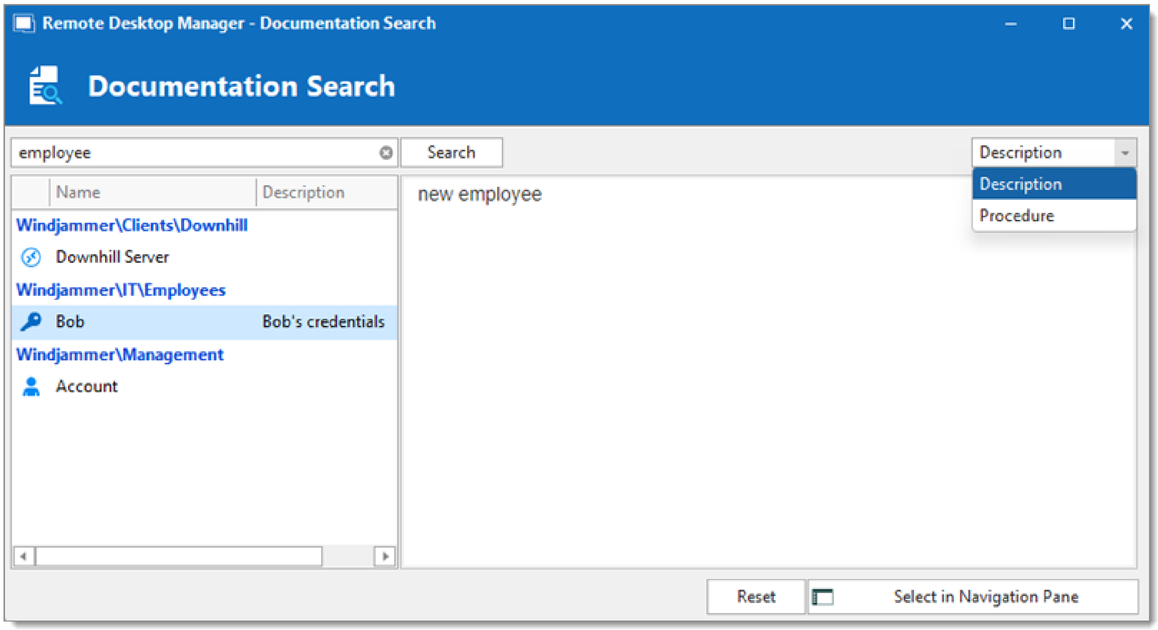
DESCRIPTION

We can search documentation pages linked to entries. ***Documentation Search*** provides a preview of the documentation pages, page title, and related entry details. The tool searches the current repository.

> ***Documentation Search*** is available with Devolutions Server and SQL Server data sources.

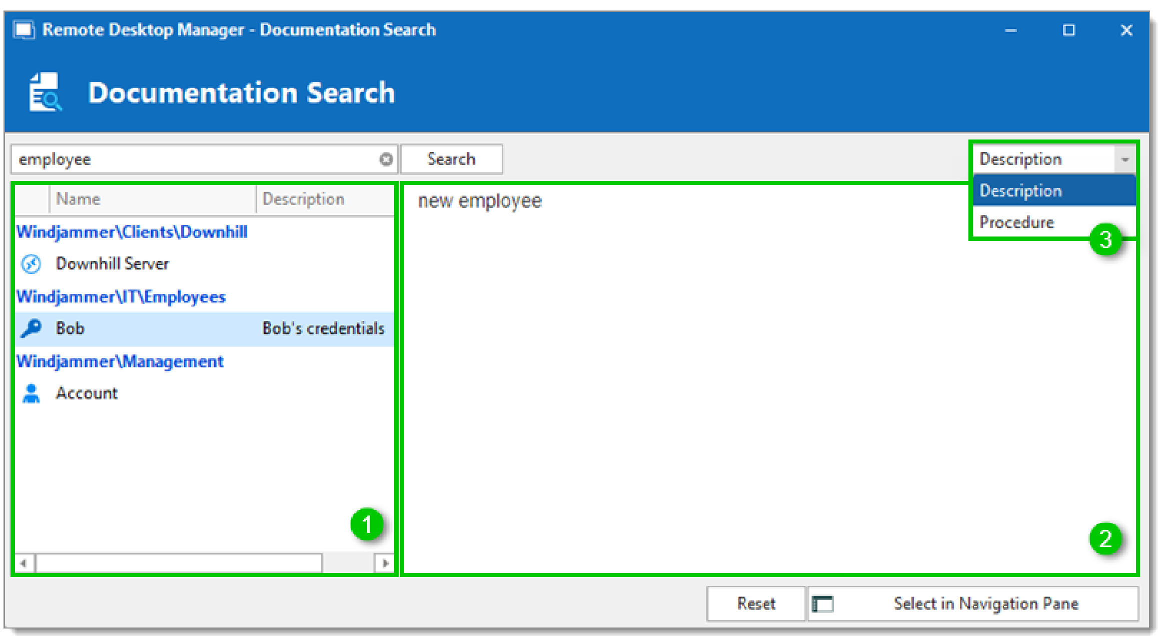
> The ***Documentation*** feature is encrypted only for the Devolutions Server data source. If you are using data sources such as SQL Server or Azure SQL, the feature is not encrypted.

> The ***Documentation*** feature is not available offline.



Documentation search dialog window

USER INTERFACE



Documentation search elements

ELEMENTS	DESCRIPTION
1. **Navigation Pane**	Lists search results by location and entry.
2. **Content area**	Displays a preview of the documentation page.
3. **Drop-down menu**	Lists the different page titles. When an entry contains multiple documentation pages with the searched term, a list of the page titles is available.

It is possible to select multiple entries at once by shift-clicking or all of them with the **Ctrl+A** shortcut. Right-clicking one or more entries shows the same menu and options as the ***Navigation Pane***.

OTHER FUNCTIONS

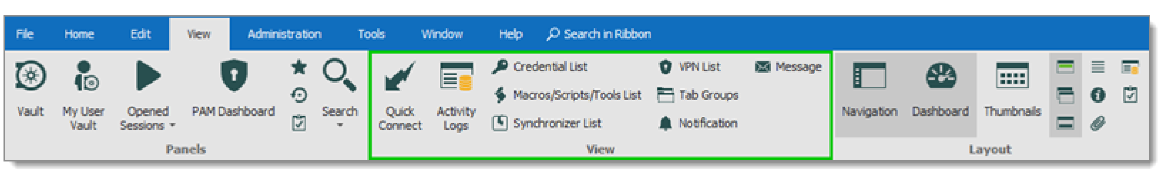
The ***Select in Navigation Pane*** button, when pressed, takes you directly to the selected entry or folder in the corresponding vault's ***Navigation Pane***.

The ***Reset*** button clears all your search results and options, giving you a clean slate for a new search.

6.6.2 View

DESCRIPTION

The ***View*** section in the ***View*** tab allows you to access different lists and information as well as to quickly connect to a host.



QUICK CONNECT

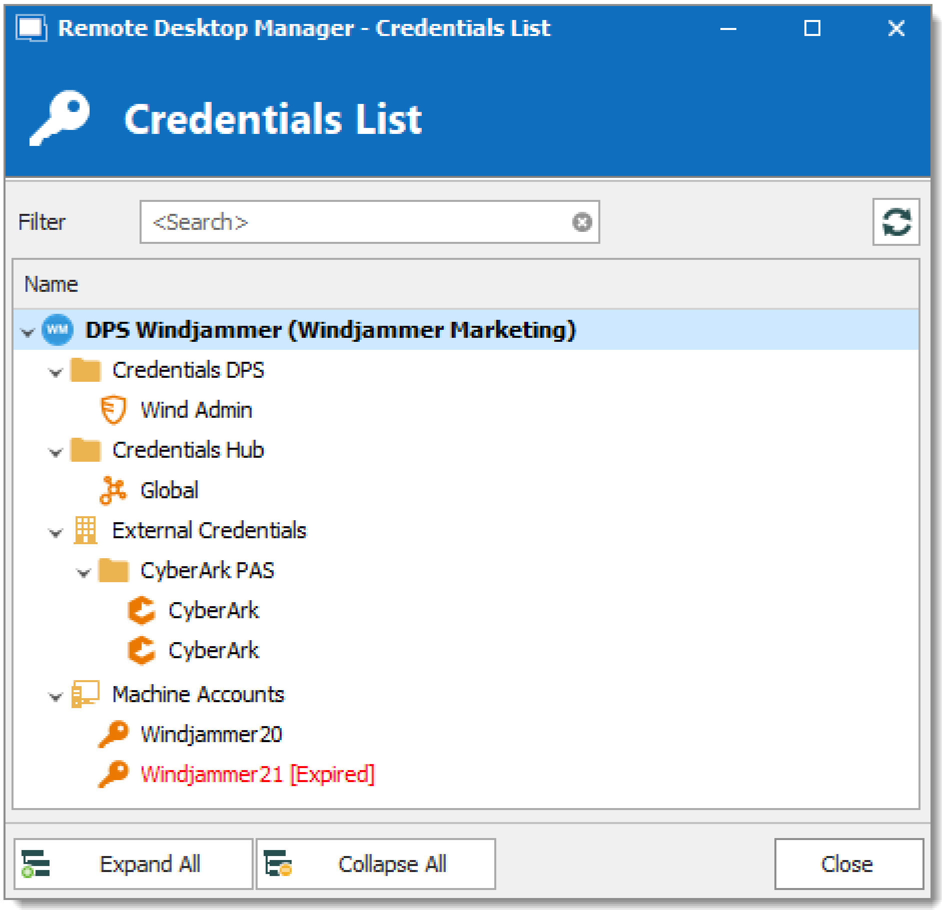
The ***Quick Connect*** feature allows you to open an **ad-hoc** session by specifying the host and session type. For more information, visit our ***Quick Connect*** topic.

ACTIVITY LOGS

The ***Activity Logs*** feature opens a tab containing information about user activity in the selected data source. For more information, visit our ***Activity Logs*** topic.

LISTS

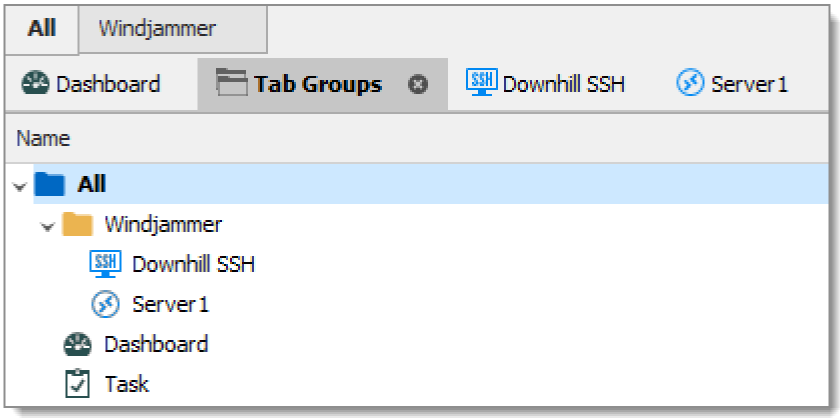
Multiple list types are available in the ***View*** section: ***Credential List***, ***Macros/Scripts/Tools List***, ***Synchronizer List***, and ***VPN List***. These options open a window showing a tree view of all entries of the specific entry type in the database. The lists can be filtered using the search bar. Right-clicking on an item shows the same menu and options as in the ***Navigation Pane***.



TAB GROUPS

The ***Tab Groups*** feature opens a docked window showing a tree view of the various tab groups. It is possible to select multiple tabs at once by shift-clicking or all of them with the **Ctrl+A** shortcut. Right-clicking on one or more tabs shows more options.

The other ***Tab groups*** will only appear if a session that is part of a tab group (other than the ***All*** tab) is active.

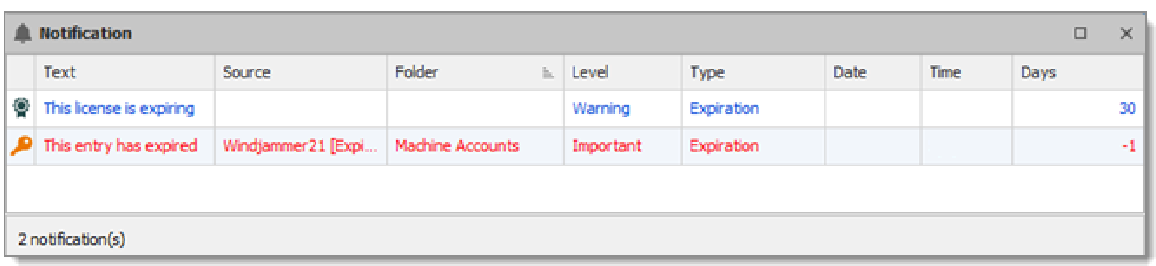


Although it is docked by default, the ***Tab Groups*** pane can be windowed, dragged, and docked anywhere within Remote Desktop Manager.

To learn how to create a tab group, refer to our ***Grouped Tab Bar*** topic.

NOTIFICATION

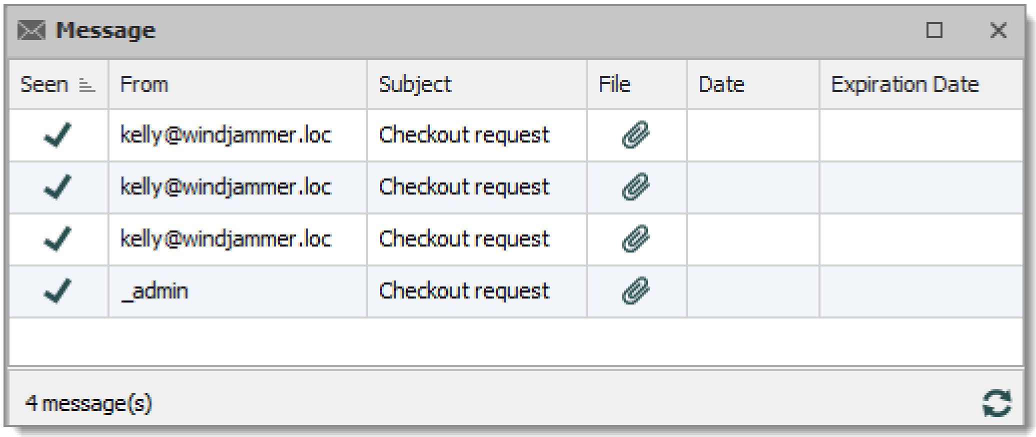
The ***Notification*** feature opens a window showing the various notifications (such as expired or about to be expired entries or tasks). Right-clicking on a notification shows more options. If you double-click on an "expired license" notification, a browser page opens to take you to your Devolutions Server account. Notifications can be sorted or searched by ***Text***, ***Source***, ***Folder***, ***Level***, ***Type***, ***Date***, ***Time***, or ***Days***.



Although it is windowed by default, the ***Notification*** pane can be dragged and docked anywhere within Remote Desktop Manager.

MESSAGE

The ***Message*** feature opens a window to let you access your messages. You can double-click on a message to open it. Messages can be sorted or searched by ***Seen***, ***From***, ***Subject***, ***File***, ***Date***, or ***Expiration Date***.

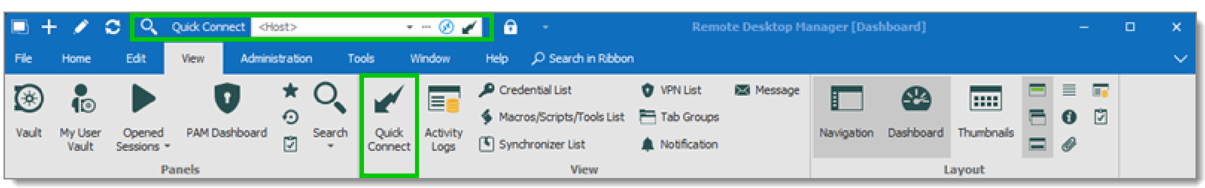


Although it is windowed by default, the ***Message*** pane can be dragged and docked anywhere within Remote Desktop Manager.

6.6.2.1 Quick Connect

DESCRIPTION

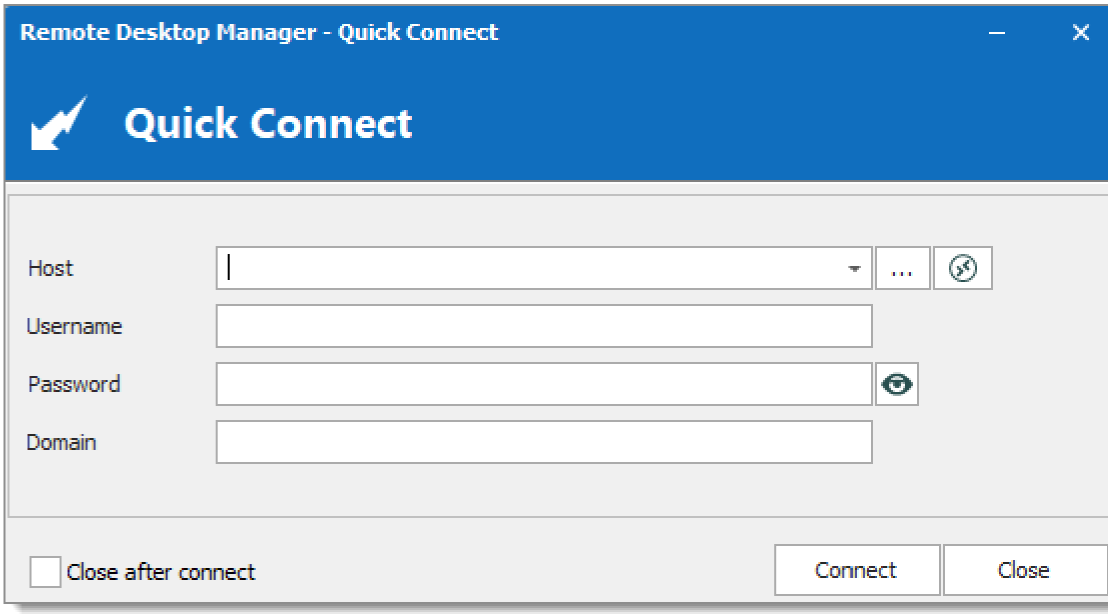
Quick Connect allows you to open an **ad hoc** session by specifying the host and session type. This feature is accessible via the ***Quick Connect*** toolbar or in the ***View*** section of the ***View*** tab in Remote Desktop Manager.



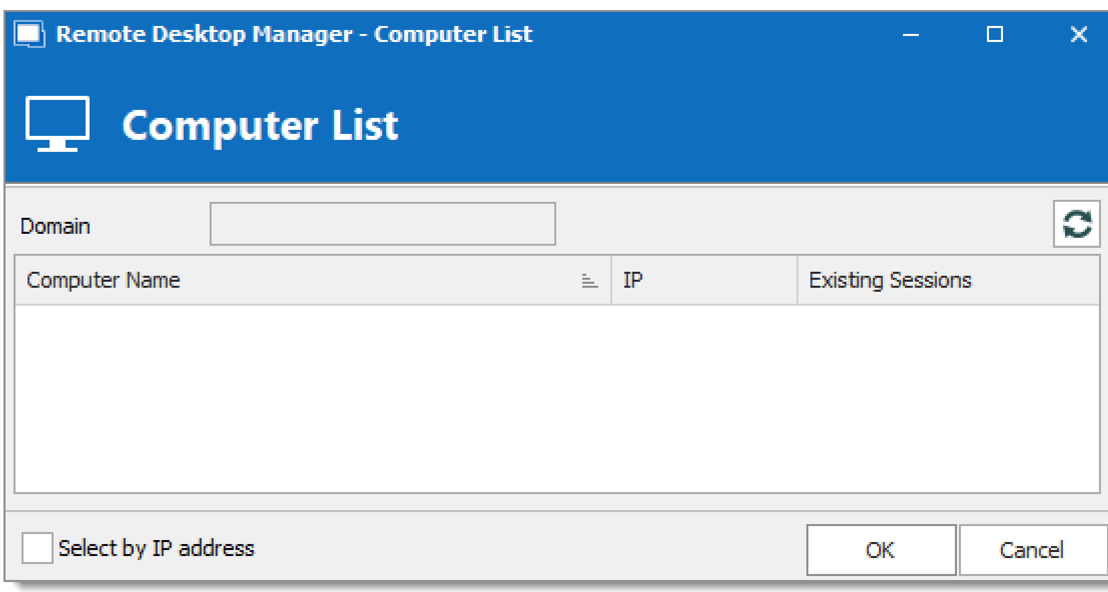
SETTINGS

Note that the ***Quick Connect*** toolbar only lets you specify a host, a computer, and a session type.To have access to the other options available in the windowed version, you have to use the ***Quick Connect*** icon in the ***View*** section of the ***View*** tab.

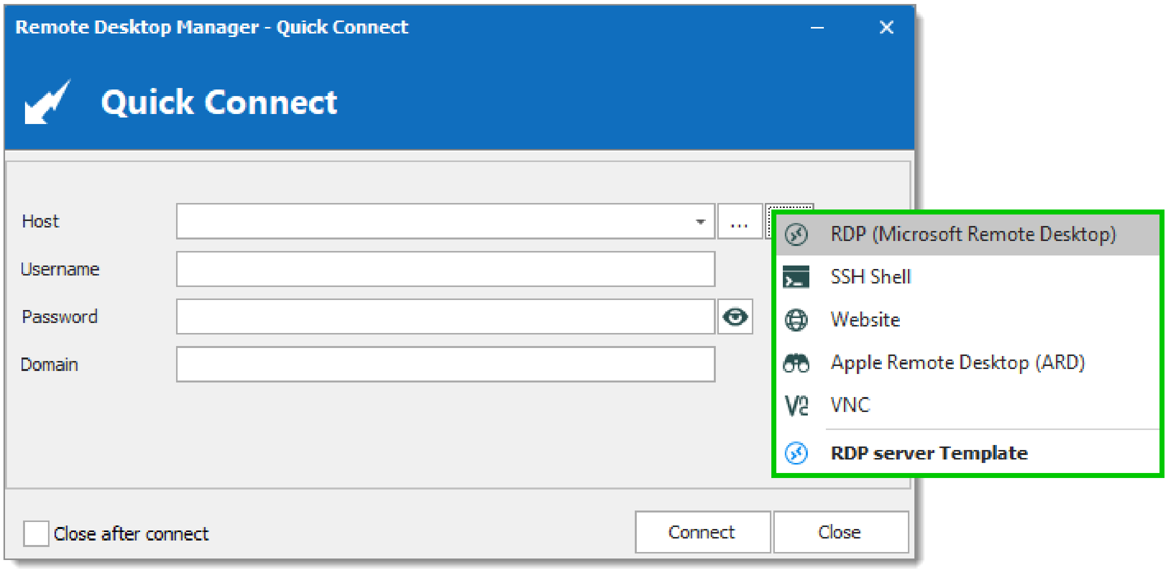
When opening ***Quick Connect*** via the ***View*** tab, a window appears where you can specify your session ***Host***, ***Username***, ***Password***, and ***Domain***.



Clicking on the **first** button next to the ***Host*** field opens yet another window where you will be able to select a computer to connect to in a list.



Clicking on the **second** button next to the ***Host*** field shows a menu where you can select your session type. It is also possible to create a ***Template*** and establish connection with it. Visit this page to learn more about this option and consult this topic on how to create a template.



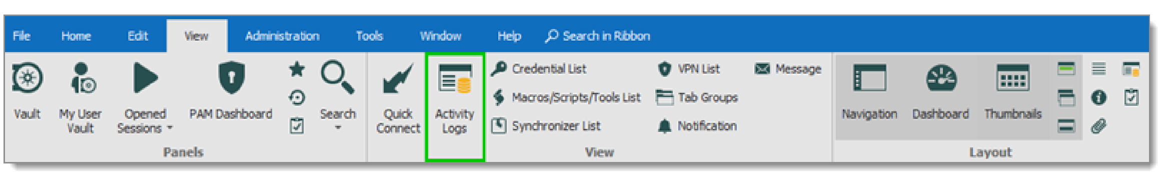
OTHER FUNCTIONS

You can choose to check the ***Close after connect*** box at the bottom left of the ***Quick Connect*** window if you want the window to close itself after you press the ***Connect*** button and you are connected to the session.

6.6.2.2 Activity Logs

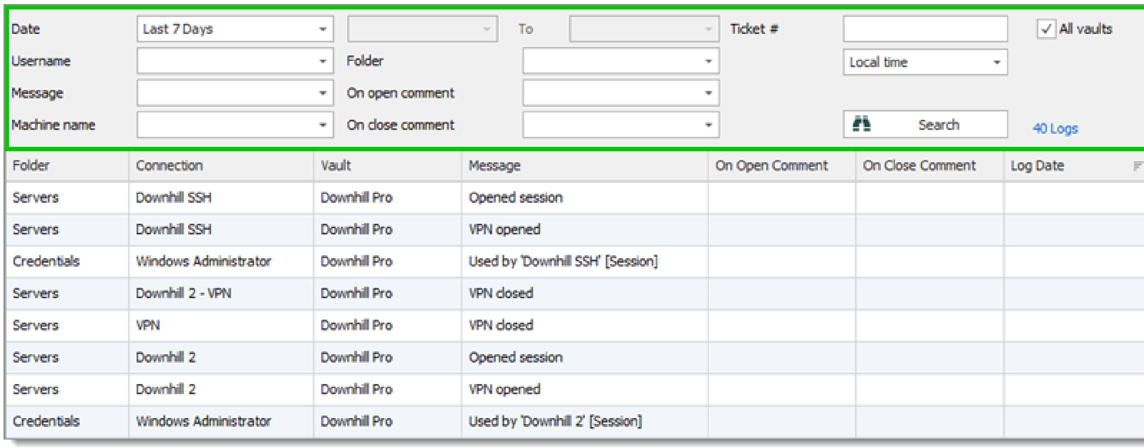
DESCRIPTION

Activity Logs provide a robust logging solution. With this feature, it is possible to monitor an open session for all users using Advanced Data Sources. The log is available for specific sessions in the ***View - Activity Logs*** context menu, in the session properties (***Activity Logs*** pane), and in the ***Dashboard***.



SEARCH

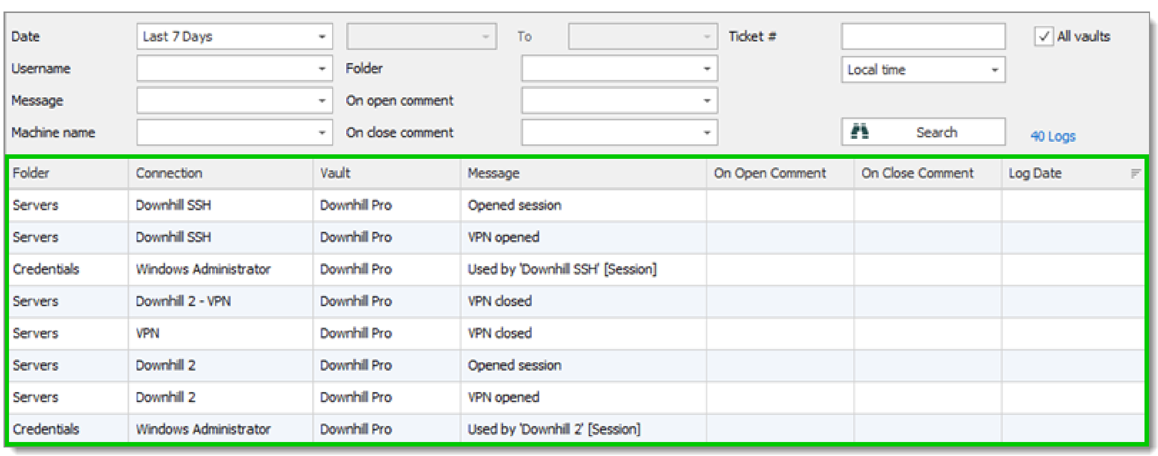
All activities in the data source are automatically displayed when opening the ***Activity Logs*** without having to apply any settings. However, search fields are available and can be useful when there are many activity entries. The results can be refined by specifying the ***Date*** or a custom period, the ***Username***, the ***Message***, the ***Machine name***, the ***Folder***, the ***On open comment***, the ***On close comment***, and the ***Ticket #***. It is also possible to choose between ***Local Time*** and UTC Time and to search in all vaults or in the current vault only. When all the criteria have been chosen, the ***Search*** button will apply them to the results.



Search fields

LOGS

The log contains all the CRUD operations (add, edit, and delete), passwords being viewed, credentials being used by other sessions, etc. It is possible to right-click an entry to access more options.



Logs

The information available for each activity line is presented in the following table.

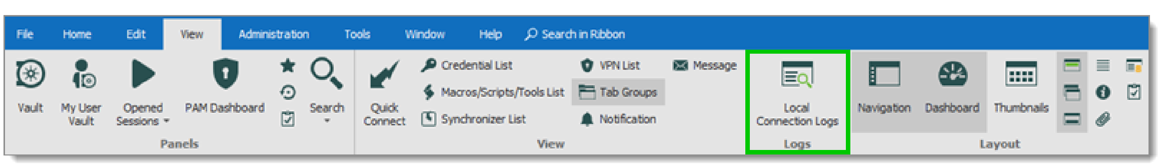
OPTION	DESCRIPTION
Folder	Indicates the folder where your entry is located.
Connection	Indicates the connection being used to open your entry.
Vault	Indicates the vault in which the action was executed.
Message	Indicates the action that has been executed on your entry or session.
On Open Comment	The ***On Open Comment*** is defined in the ***Log*** tab of your session.
On Close Comment	The ***On Close Comment*** is defined in the ***Log*** tab of your session.
Log Date	Indicates the date and time your session was opened or your entry was edited.
End Date/Time	Indicates the date and time your session or entry was closed.
Active Time	This information is only available for embedded mode sessions. The active time of your session, meaning the time at which your session was open in embedded mode and the time you were active on your session, will be recorded. If your session is open, but you are on the ***Dashboard*** tab, for example, and not on you session tab, no active time will be recorded.
Duration	This information is only available for embedded mode sessions. When sessions are open in embedded mode, the duration of the session will be recorded. This means that even if you are on the ***Dashboard*** tab, for example, and not actively working in your session, but your session tab is open, the session duration will be recorded.

OPTION	DESCRIPTION
Machine User	Indicates the name of the machine user.
User	Indicates the connected user's name.
Connection user	Indicates the connection user.
Ticket #	Indicates the ticket number.
Machine	Indicates the machine name.
Connection Type	Indicates the connection type that was used.
Connection Logs ID	Indicates the unique identifier of the connection log.

6.6.3 Logs

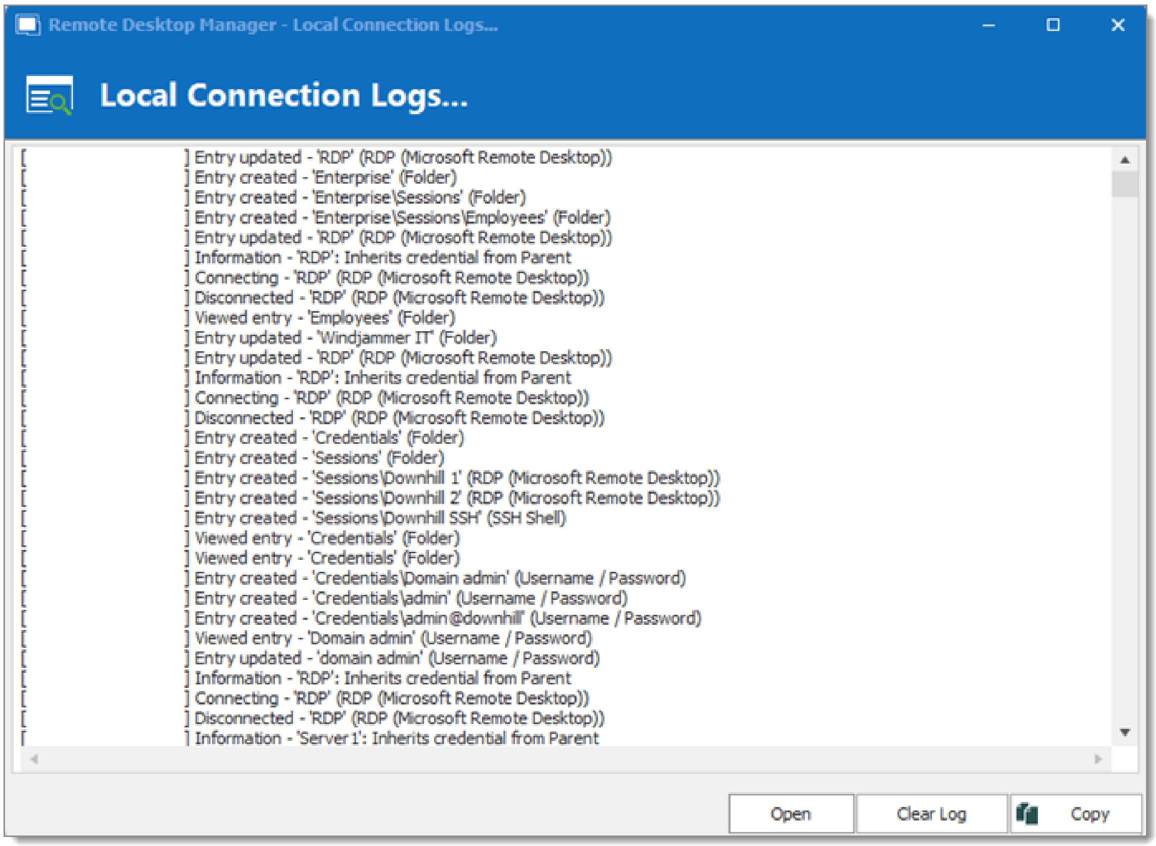
DESCRIPTION

When using Remote Desktop Manager locally with an individual type data source, the ***Activity Logs***, normally found in the ***View*** section of the ***View*** tab, are not available. In this situation, the ***Logs*** section appears in the ***View*** tab.



LOCAL CONNECTION LOGS

In the ***Logs*** section, you will find the ***Local Connection Logs*** feature, which is useful if you still want to access your local logs. Clicking on it opens a window containing all your local logs in chronological order (oldest to newest). You can scroll through the list to find the logs you are looking for.



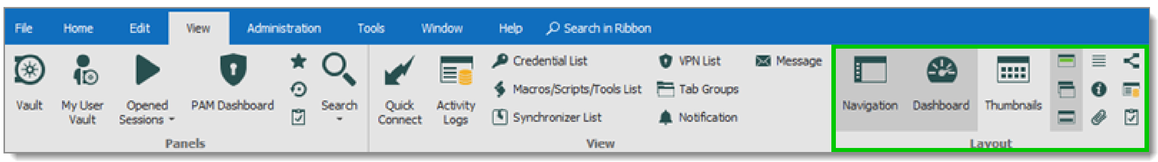
The buttons at the bottom of the window give you more options.

OPTION	DESCRIPTION
Open	Open the local folder on your computer where the logs are stored.
Clear Log	Clear the logs from the ***Local Connection Logs*** window. The logs are not erased from the folder.
Copy	Copy the logs to your clipboard as they appear in the ***Local Connection Logs*** window.

6.6.4 Layout

DESCRIPTION

The ***Layout*** section located in the ***View*** tab includes several options for changing the display of Remote Desktop Manager. It is possible to enable/disable certain windows and tabs to customize your experience.



Most tabbed windows can be moved and docked as you wish. This applies to the default styles (***Ribbon*** or ***Menu***). To learn more about this feature, see our Docking topic.

The table below lists each option available in this section and provides a brief description of each.

OPTION	DESCRIPTION
Navigation	Enable/disable the ***Navigation Pane***. The keyboard shortcut **Alt+F8** can also be used to perform these actions. See the ***Navigation Pane*** topic for more information.
Dashboard	Enable/disable the ***Dashboard***. The keyboard shortcut **Alt+F6** can also be used to perform these actions. See the ***Dashboard*** topic for more information.
Thumbnails	Enable/disable the ***Thumbnails*** pane. This option displays all active sessions in the data source. From this window, it is possible to start or stop all live views.
Top Pane (Ribbon/Menubar)	Enable/disable the ***Top Pane***. To make it reappear, simply right click on the Remote Desktop Manager title bar (the top bar), then select the ***Top Pane (Ribbon/Menubar)*** from the menu. The keyboard shortcut **Alt+F11** can also be used to perform these actions. See the ***Top Pane*** topic for more information.

OPTION	DESCRIPTION
Grouped Tab Bar	Enable/disable the ***Grouped Tab Bar***. See the ***Grouped Tab Bar*** topic for more information.
Status Bar	Enable/disable the ***Status Bar***. The keyboard shortcut **Alt+F7** can also be used to perform these actions. See the ***Status Bar*** topic for more information.
Description	Enable/disable the ***Description*** pane. This option allows you to add a description to an entry.
Asset	Enable/disable the ***Asset*** pane. This option allows you to view ***Asset***, ***Software***, ***Hardware***, ***Contact***, and ***Purchase*** information as well as ***Notes*** related to the entry. It is not possible to edit information from this view.
Attachments	Enable/disable the ***Attachments*** pane. See the ***Attachments*** topic for more information.
Sub Connections	Enable/disable the ***Sub Connections*** pane. This option displays the sub connections of the selected entry.
Logs	Enable/disable the ***Logs*** pane. See the ***Logs*** topic for more information.
Task	Enable/disable the ***Task*** pane. See the ***Task*** topic for more information.

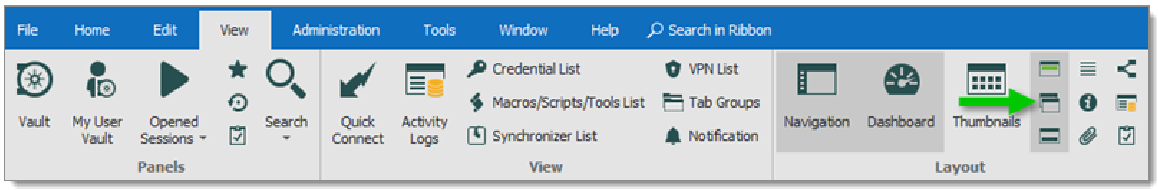
6.6.4.1 Grouped Tab Bar

DESCRIPTION

Remote Desktop Manager is great for running many sessions at once by using its embedded/tabbed display mode. It's especially true when using multiple remote control technologies at the same time. No longer will you have to dig in your task bar to locate the session of interest, you have them all running in tabs within the same tool used to launch them.

But when you reach a certain number of running sessions, it may become difficult to identify them using only their name. To improve user experience, the ***Grouped Tab Bar*** feature was created to filter the tab pages.

To enable the ***Grouped Tab Bar***, navigate to ***View - Layout*** in the ribbon, then select ***Grouped Tab Bar***.

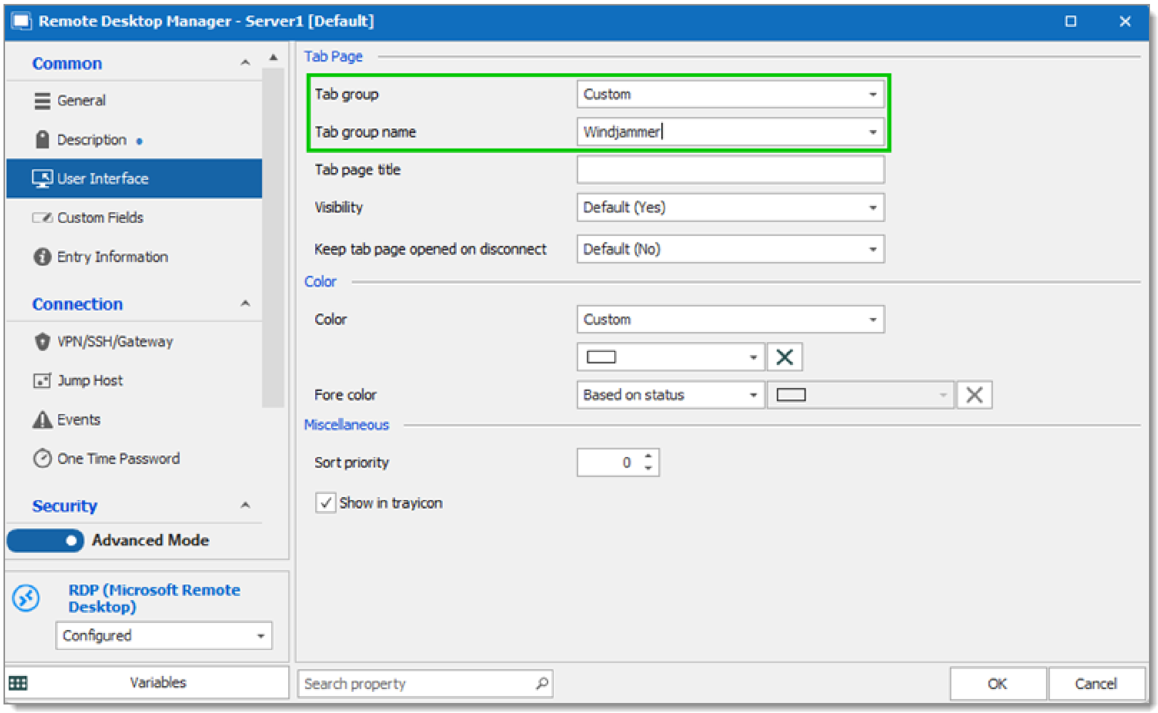


The ***Grouped Tab Bar*** will only appear if a session that is part of a ***Tab group*** (other than the ***All*** tab) is active. To make it show at all times, check the ***Always show grouped tab bar*** box in ***File - Options - User Interface - Advanced***.

The ***Tab Groups*** feature in ***View - View*** lets you see a tree view of the various tab groups. For more information, visit the ***View*** topic.

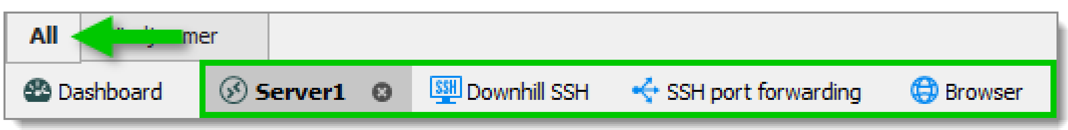
SETTING UP A TAB GROUP

The ***Tab group*** settings are found in the ***User Interface*** side menu of your session properties. The ***Properties...*** option can be found when right-clicking on an entry.

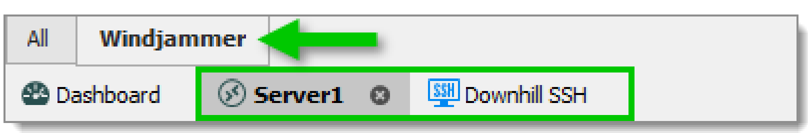


The ***Tab group*** field lets you choose between a custom or inherited tab group. If you want to specify a custom name, you can simply type a name or choose an already existing one in the ***Tab group name*** field to create a tab group when launching an instance, then click on ***OK***.

When the ***All*** group tab is selected, it performs no filtering. All running sessions are visible in this tab.



When a different group tab is selected, it hides all the sessions that do not match with the filter. In the example below, only two sessions appear in the custom **Windjammer** group tab.

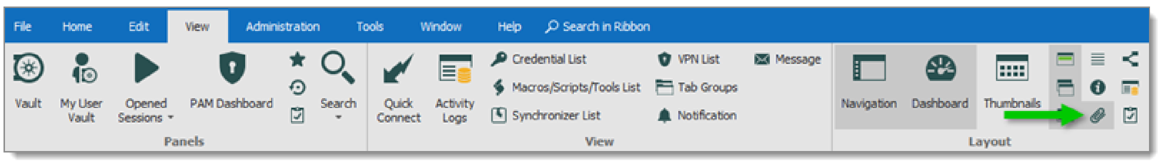


6.6.4.2 Attachments

DESCRIPTION

Files are attached to an entry and are stored directly in the database.

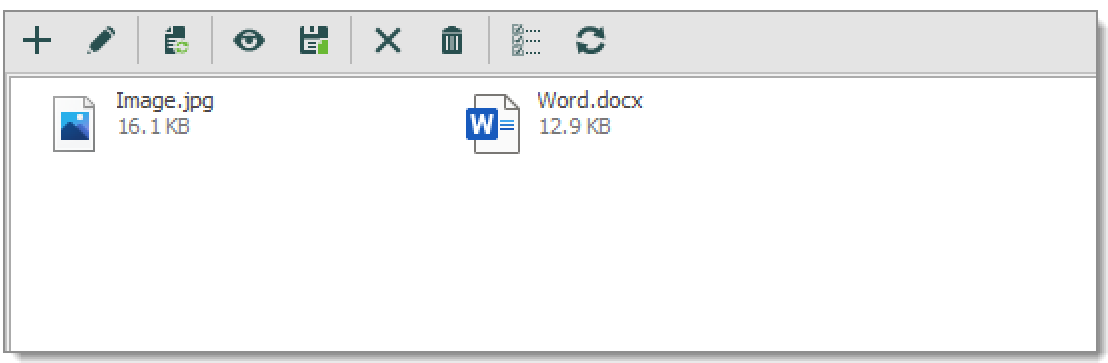
To enable the attachment pane, navigate to ***View - Layout*** in the ribbon, then select ***Attachments***.



View – Layout – Attachments

This feature is only available when using an [Advanced Data Source](#).

The files in attachments are not available in offline mode.



Attachments

The attachment type and size are limited only by your bandwidth and the data source. You can also view a saved attachment:

- from the session context menu;
- from the session properties; or
- directly on the ***Dashboard***.

The refresh button allows you to update directly the selected document. Use it to save your local modifications.

ACTIONS

Use the toolbar above the attachments list to manage the selected attachment.

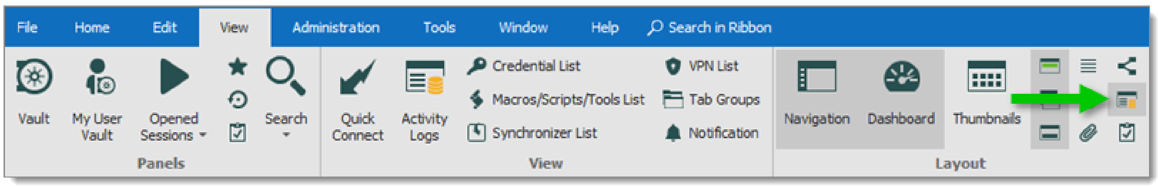
Attachments toolbar

OPTION	DESCRIPTION
Add Attachment	Select a local file to add.
Edit Attachment	Edit the selected attachment.
Update Document	Update the selected attachment.
View Attachment	Open the selected attachment.
Save Attachment As	Save the attachment on a local drive.
Delete Attachment	Delete the selected attachment.
Deleted Attachment List	Display deleted attachments in a new window. It is possible to search in the list and permanently delete er restore one or more attachments.
Details	Display details about the selected attachment, above the attachment list.
Refresh	Refresh the attachments list.

6.6.4.3 Logs

DESCRIPTION

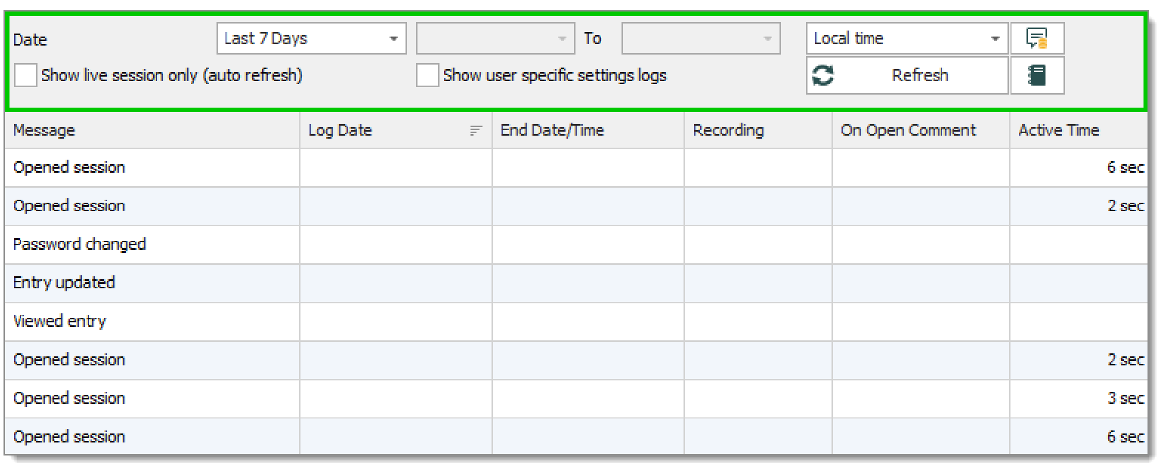
The ***Logs*** feature is similar to ***Activity Logs***, but it only provides information about the selected entry. Logs are available from the context menu ***View - Layout - Logs***.



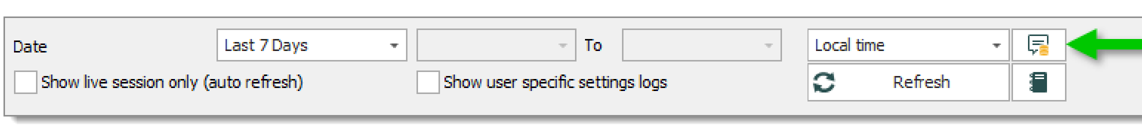
FUNCTIONS

The log entries can be filtered by ***Date*** or by using a custom time period, specifying whether it is ***Local Time*** or ***UTC Time***.

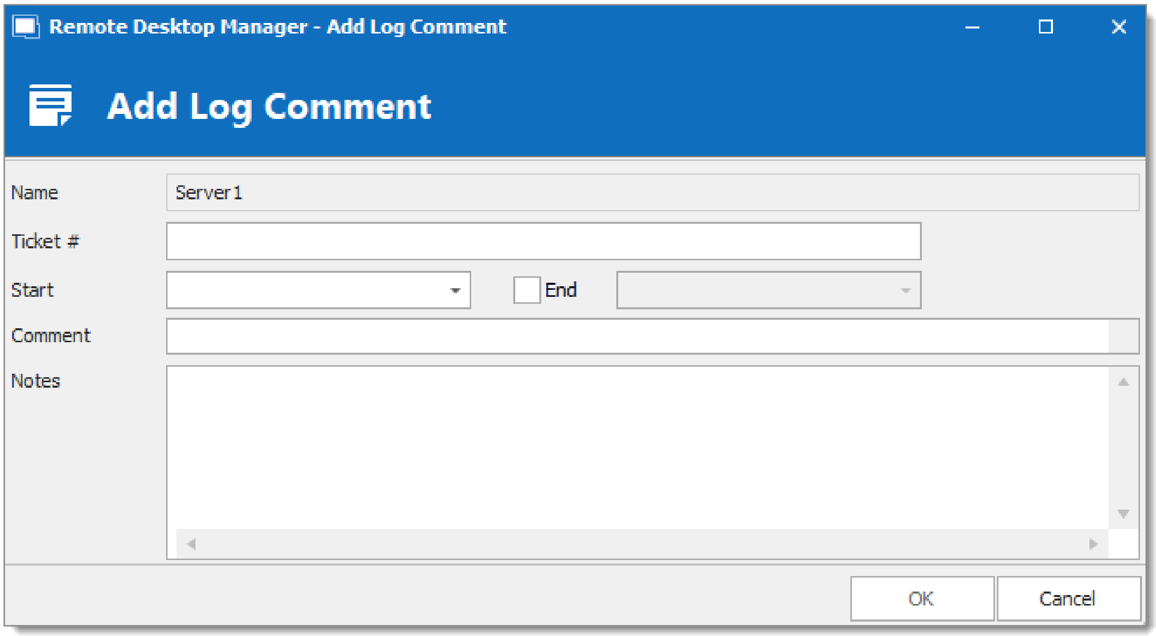
It is also possible to enable the ***Show live sesison only (auto refresh)*** and ***Show user specific settings logs*** options by checking the appropriate box.



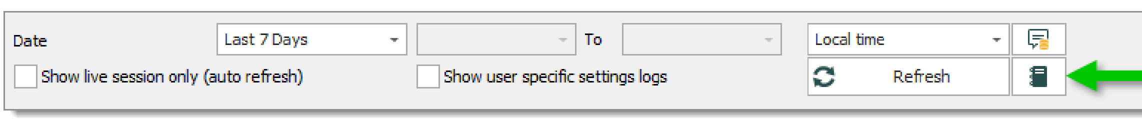
LOG COMMENT



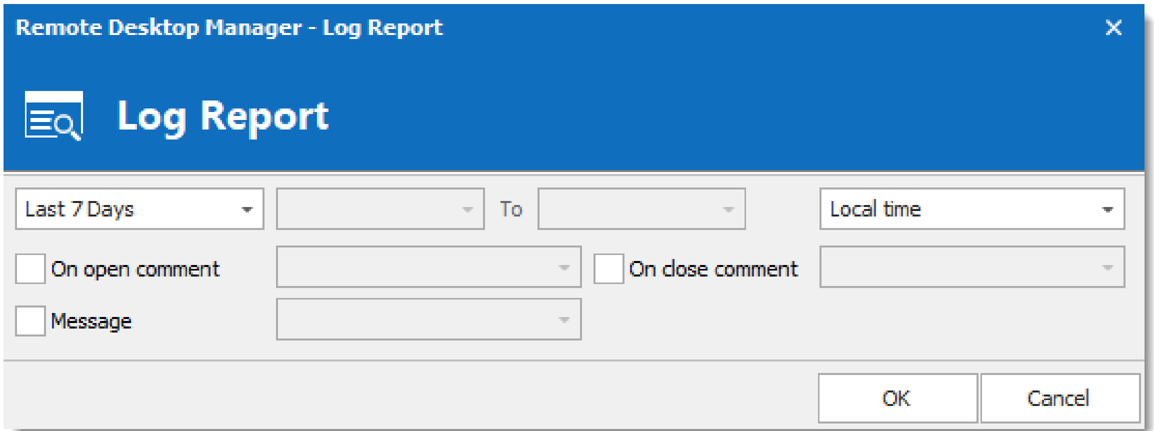
Clicking on the ***Insert Log Comment*** button opens a window that allows you to add a comment to the log while specifying a ticket number, a start date (and an end date, if desired), and notes.



GENERATE A REPORT

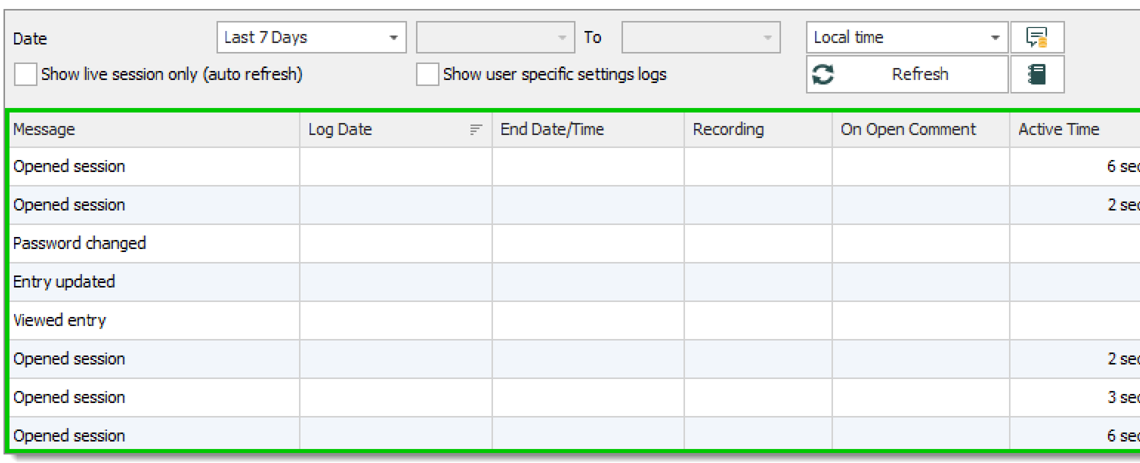


Clicking on the ***Generate report*** button opens a window that allows you to generate a report of the logs while specifying the time period, the type of time (***Local Time*** or ***UTC Time***), and, optionally, an ***On open comment***, an ***On close comment***, and a ***Message***. When finished, clicking the ***OK*** button generates a report that can be saved, exported (in CSV, HTML, Xlsx, or XML format), or printed.



LOGS

Le journal contient toutes les opérations CRUD (ajout, modification et suppression), les mots de passe affichés, les identifiants utilisés, etc. Il est possible de cliquer sur une entrée avec le bouton de droite pour accéder à plus d'options.



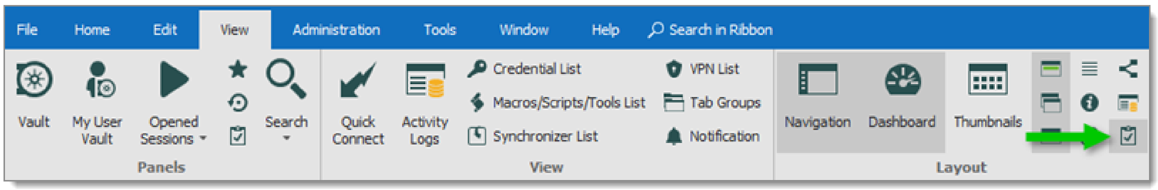
The information about entries is the same as in ***Activity Logs***, except that ***Folder***, ***Connection***, ***Vault***, and ***Connection Log ID*** are not available in ***Logs*** since the information is specific to an entry only. For a description of the available information, see the ***Activity Logs*** topic.

6.6.4.4 Task

DESCRIPTION

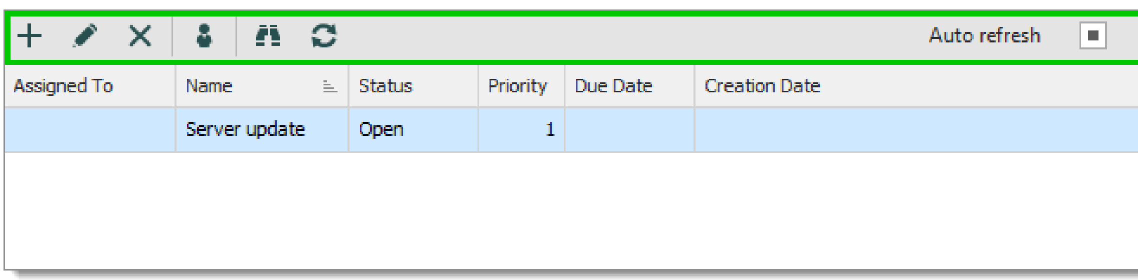
The ***Task*** feature is similar to ***Task List***, but it applies only to the selected entry. Tasks are available from the context menu ***View - Layout - Task***.

This feature is only available for the following data sources: Devolutions Server, Azure SQL, SQL Server, and SQLite.

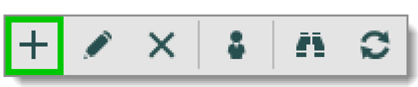


FUNCTIONS

Create tasks to keep track of the work that needs to be done per entry. You can ***Add***, ***Edit***, and ***Delete*** a task using the corresponding icons. It is also possible to ***Assign a User to a task***, apply a ***Filter*** and ***Refresh*** the page. The refresh can be done automatically by checking the ***Auto refresh*** box.

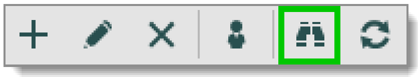


CREATION OF TASKS

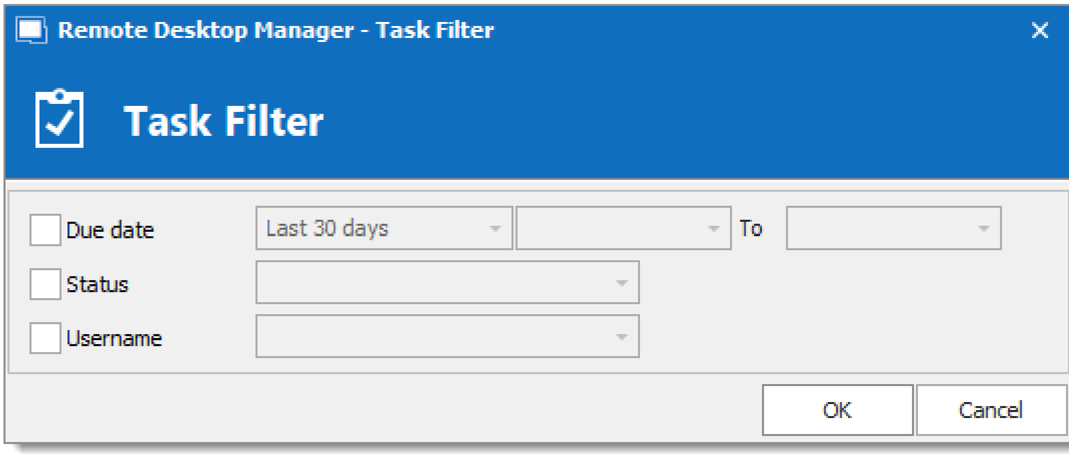


For more information on how to create a task, see the **Creating a Task** section of the ***Task List*** topic.

TASK FILTER

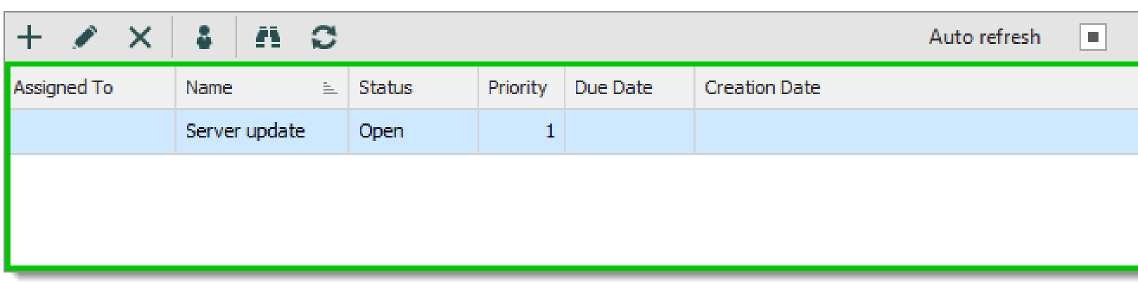


Clicking on the ***Filter*** icon opens a window that allows you to filter the tasks in the entry by ***Due Date***, ***Status*** or ***Username***.



TASKS

The information available is as follows: ***Assigned To***, ***Name***, ***Status***, ***Priority***, ***Due Date***, and ***Creation Date***. For more details about this information, please refer to the ***Task List*** topic.

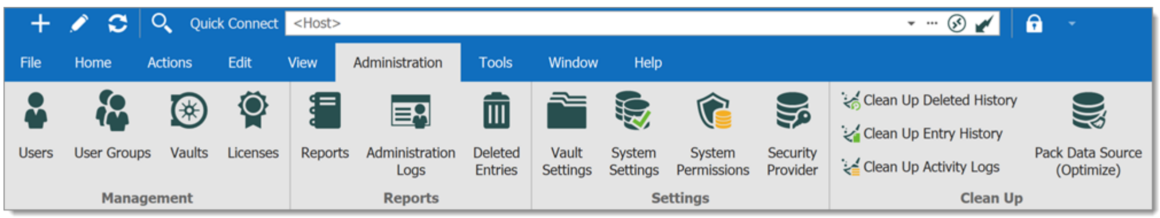


6.7 Administration

DESCRIPTION

The **Administration** tab allows to manage settings and users of a data source, view reports such as the activity logs, and much more. This tab is only available to administrators of the data source.

Most features contained in the Administration tab are only available when using an Advanced Data Source.



Ribbon - Administration

MANAGEMENT

These feature requires an Advanced Data Source.

OPTION	DESCRIPTION
Users	Opens the User Management.
Security Groups (Legacy)	Security Groups are now a Legacy option, and although we have left documentation in the online help to help users identify it, we strongly recommend switching to User Groups instead.
Vaults	Opens the Vault Management tab of User Management.
User Groups	Opens the User Groups Management tab of User Management.

REPORTS

The logs feature requires an Advanced Data Source.

OPTION	DESCRIPTION
Reports	Open the Reports section to select which type of report best suit your current needs.
Administration Logs	Opens the Administration Logs.
Deleted Entries	Open a log of all Deleted Entries (since last clean up).

SETTINGS

These feature requires an Advanced Data Source.

OPTION	DESCRIPTION
Vault Settings	Opens the Vault Settings. The Vault Folder is the one at the top of the navigation pane (in Tree View). It is the one from which all entries and folder stem. By default, lower level folders inherit settings and security from parent folder until reaching the Vault. Therefore, using permissions on the Vault folder allows to secure all entries below the Vault level. Refer to Default security for entries for more information.
System Settings (Data Source Settings)	Opens the System Settings. There are many features here, all meant to help you customize your data source and security needs. Remember that these settings applies to all users that have access to the data source.

OPTION	DESCRIPTION
System Permissions	Modify System Permissions.
Security Provider	Set up a Security Provider for an additional layer of security.

CLEAN UP

This feature requires an Advanced Data Source.

OPTION	DESCRIPTION
Clean Up Deleted History	Perform a partial or full clean up of the Deleted History.
Clean Up Entry History	Perform a partial or full clean up of the Entry History.
Clean Up Activity Logs	Perform a partial or full clean up of the Activity Logs. You also have the option to clean up the **Administration Logs** if desired.
Pack Data Source (Optimize)	The Pack Data Source (Optimize) feature analyzes all entries, compress and save them, thus saving space in your data source.

6.7.1 Management

6.7.1.1 User Management

DESCRIPTION

The **Users Management** allows to create and manage users and their privileges. You can set the default privileges on the user type in **Data Source Settings (System Settings)**. Remote Desktop Manager offers advanced user rights management that allows for restricting access to entries. Please note that availability of some features depends on the active data source.

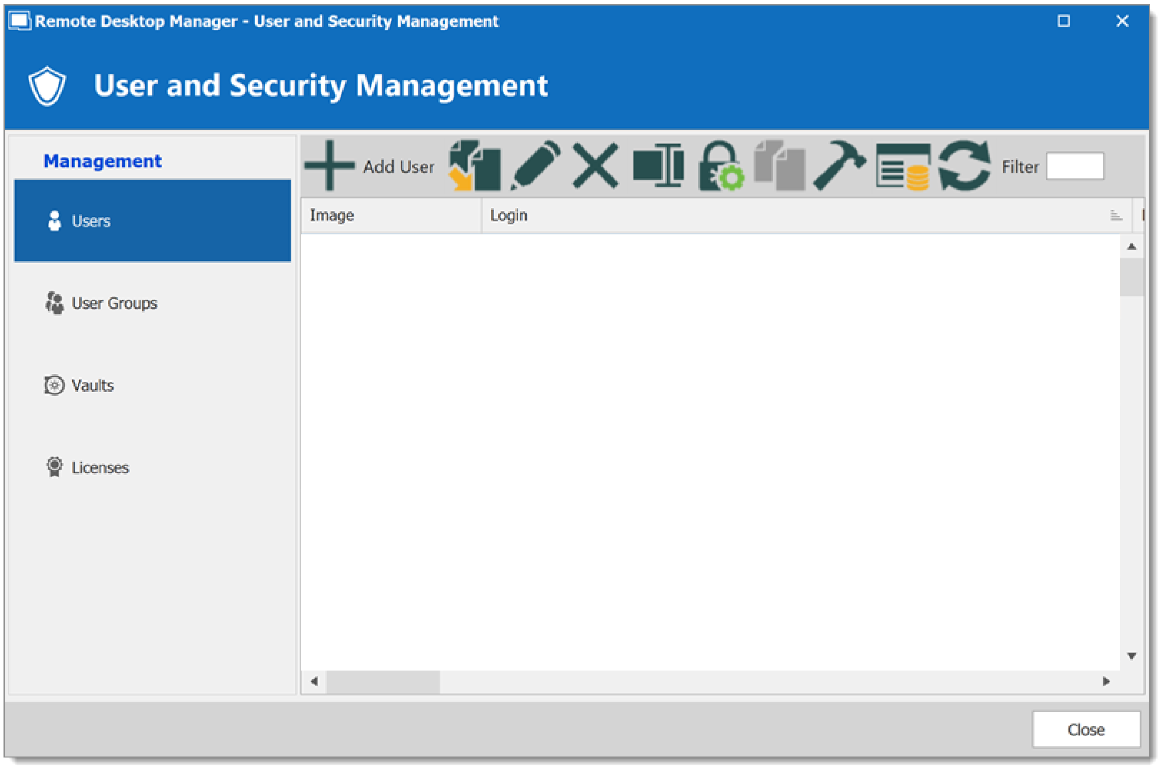
> This feature requires an Advanced Data Source.

> A user can be created using default security (specify the password) or Integrated Security. Not all Advanced Data Sources support the use of Integrated Security.

> In order to create users and assign rights, you must be administrator of not only Remote Desktop Manager, but also of the underlying database.

MANAGE USERS

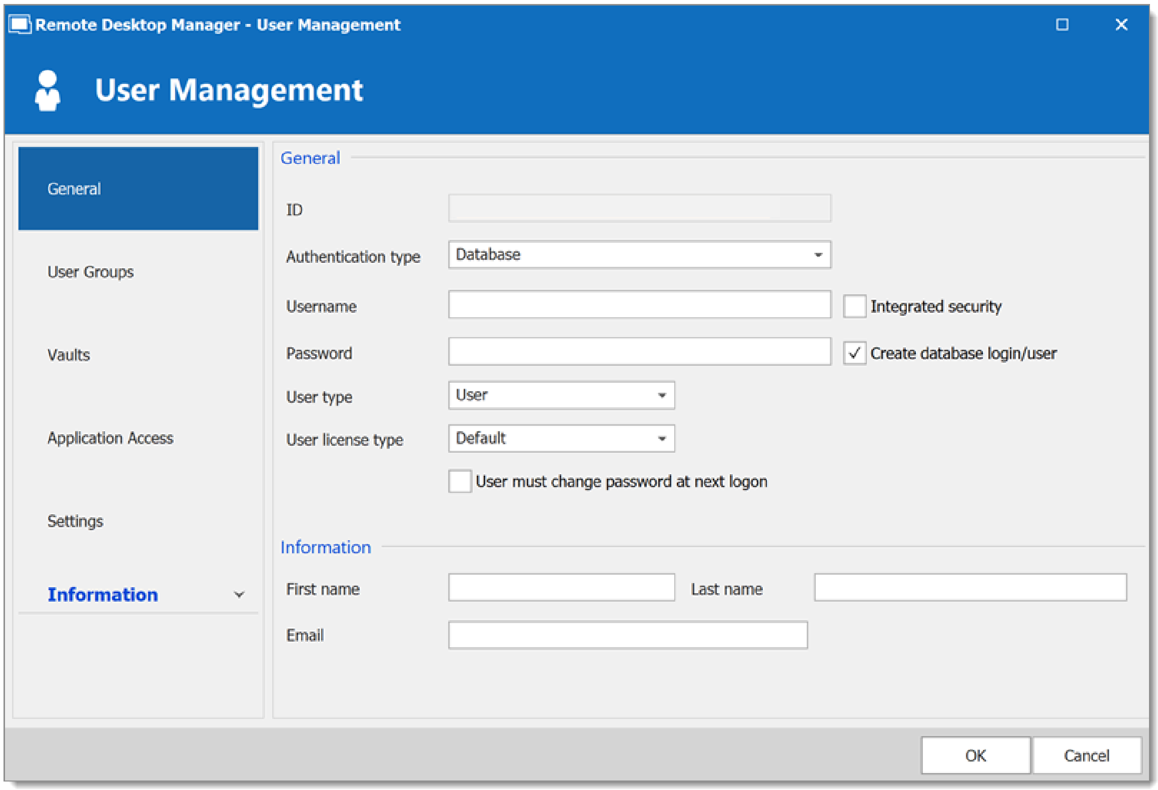
To create, edit, delete, rename or otherwise manage users as a whole, simply use the buttons in the toolbar.



User and Security Management - Toolbar

USER MANAGEMENT SETTINGS

GENERAL



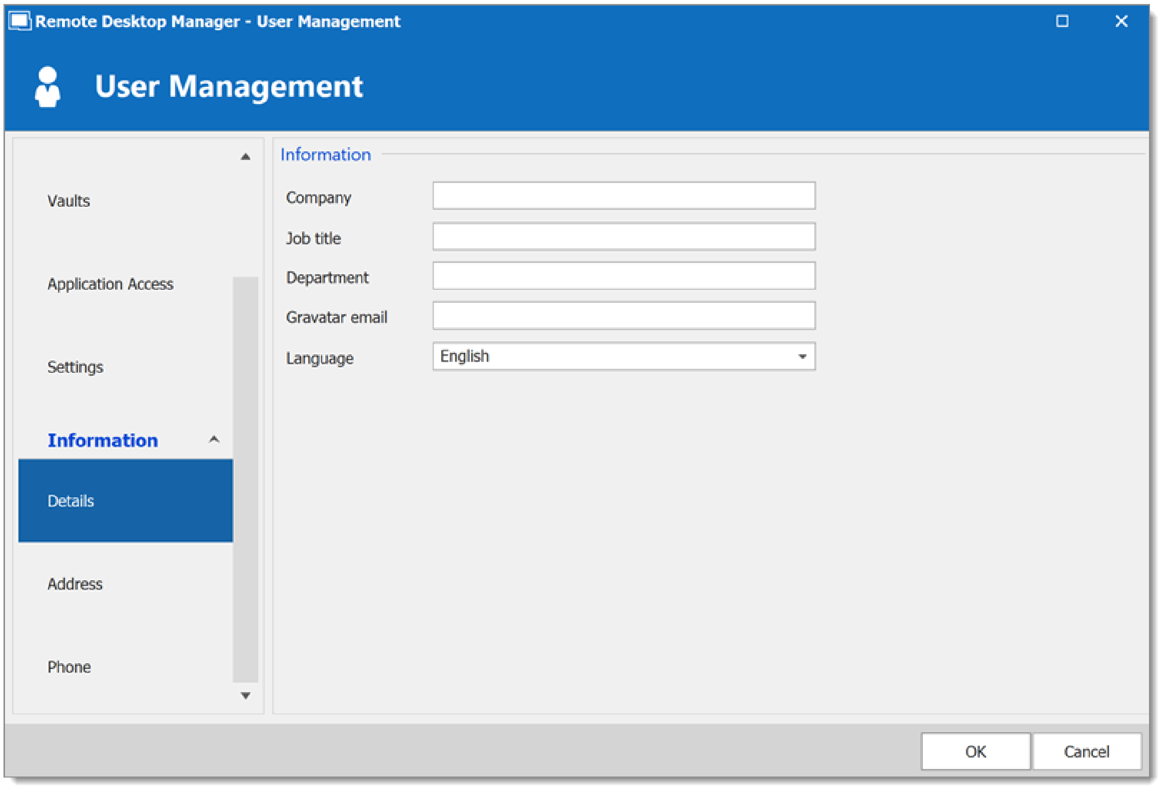
User Management - General

OPTION	DESCRIPTION
Authentication type	Select the user's authentication type: • **Custom (Devolutions)**: create a user specific to Remote Desktop Manager without creating an SQL login. • **Database (SQL Server)**: authenticate using the SQL login from your SQL Server.
Username	Enter the username for the user. When using Integrated Security the user must be selected from the directory.
Integrated security (Active Directory)	Specifie to use Active Directory to authenticate to the data source. Applies only to SQL Server and Devolutions Server, depending on their configuration. For more information, please consult the Integrated Security topic.

OPTION	DESCRIPTION
Password	Enter the user's Password. This field is disabled when using Integrated Security.
User type	Select the type of user to create, select between: • **Administrator:** Grant full administrative rights to the user. • **Read only user:** Grant only the view access to the user. • **Restricted user:** Select which rights to grant to the user. • **User:** Grant all basic rights to the user (Add, Edit, Delete). For more information, please consult the User Types topic.
User license type	Select the license type of the user. Select between: • **Default** • **Connection Management** • **Password Management**
Full name	Enter the First name and Last name of the user.
Email	Insert the user's email address.

INFORMATION

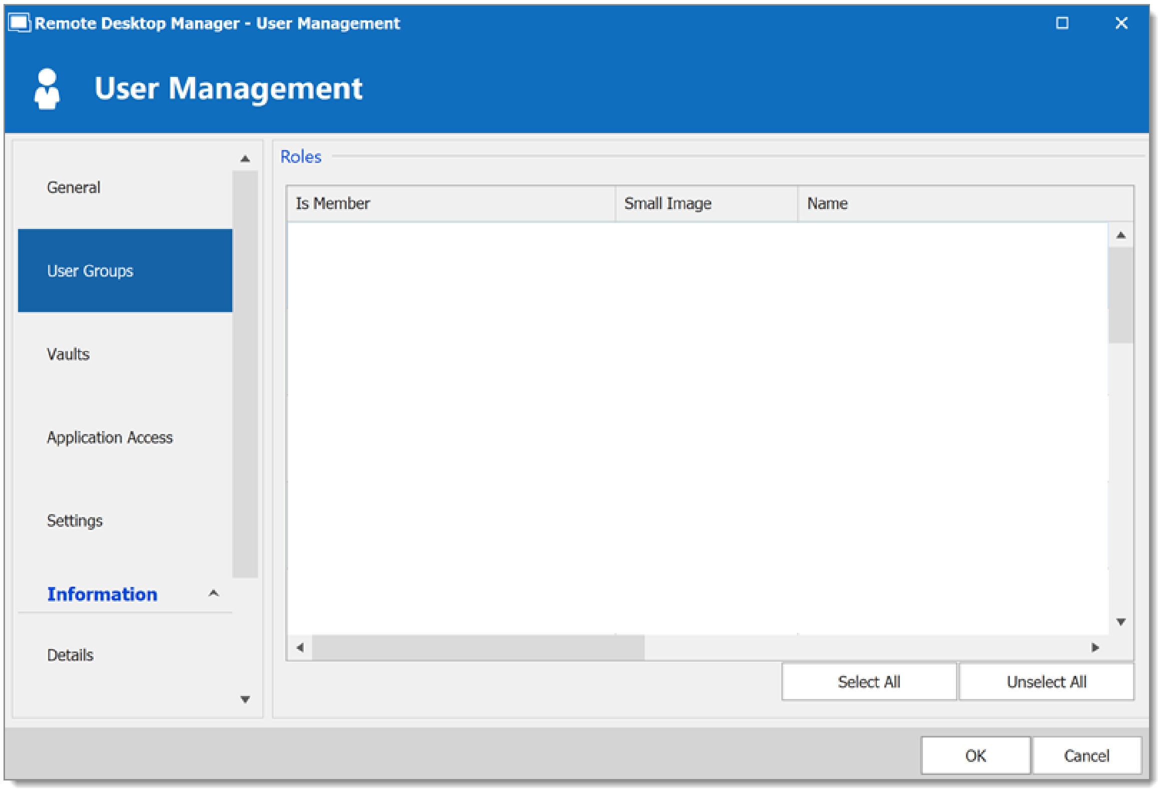
The **Information** section allows to store information regarding the users, such as their name, address, and more. The Information section is divided in three sub-sections: **Details, Address, Phone**.



User Management - Information - Details

USER GROUPS

Select user groups to assign to the user.

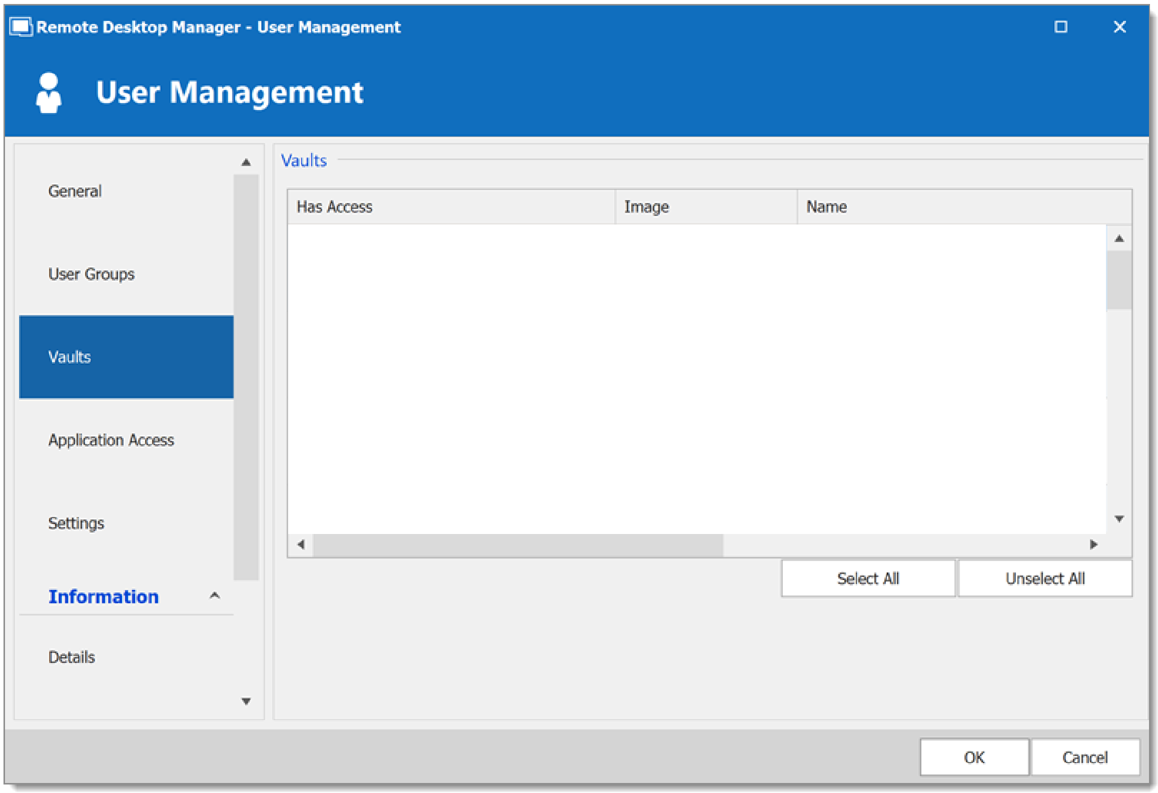


User Management - User Groups

OPTION	DESCRIPTION
User Groups	Check the **Is Member** box to assign the user groups to the user. Consult User Groups Management topic for more information.

VAULTS

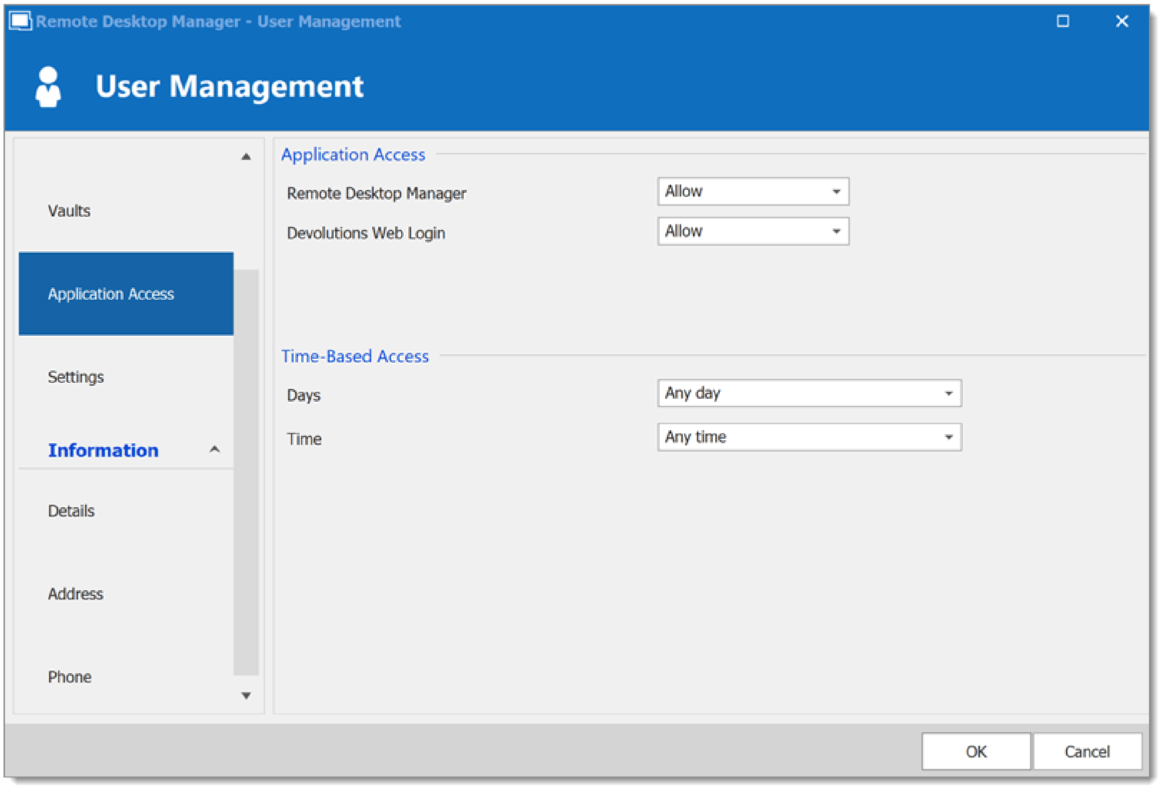
Select which repositories the user has access to. For more information, please consult the Vaults topic.



User Management - Vaults

APPLICATION ACCESS

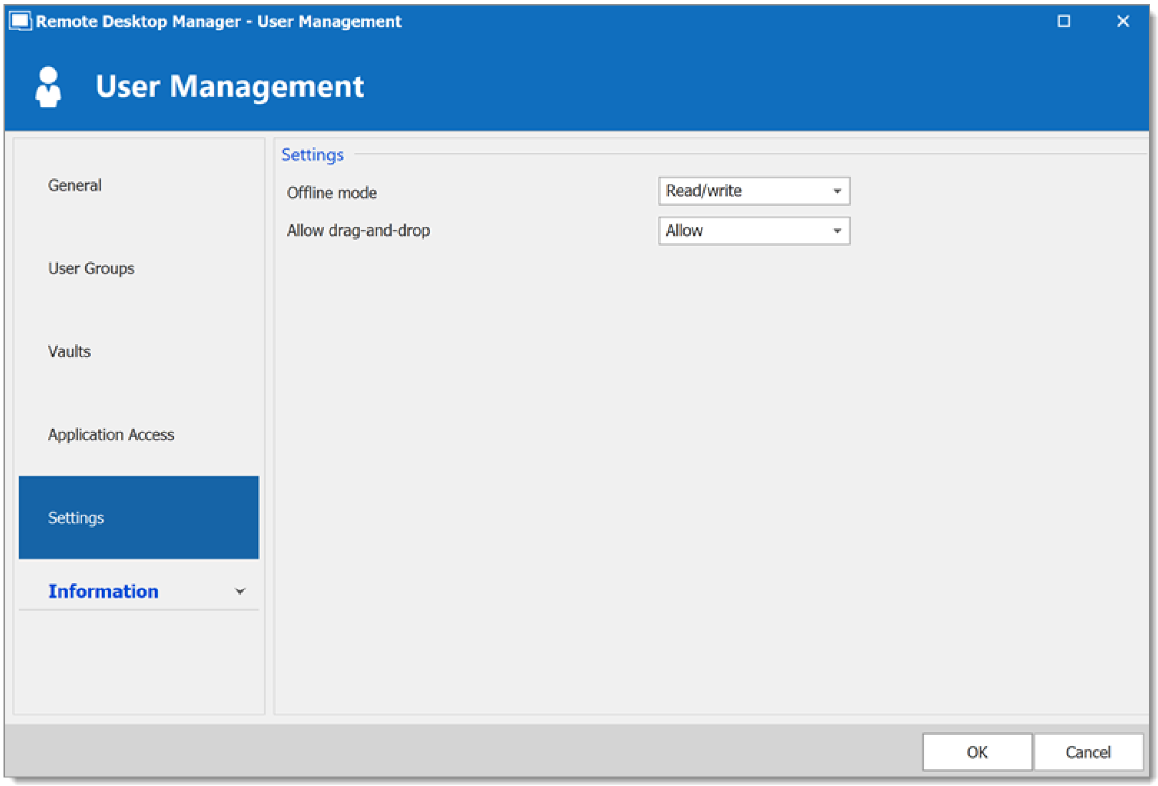
The application access section allows to restrain access to Remote Desktop Manager or Devolutions Web Login.



User Management - Application Access

OPTION	DESCRIPTION
Remote Desktop Manager	Select if the user can access to the data source from Remote Desktop Manager.
Devolutions Web Login	Select if the user can access to the data source form Devolutions Web Login.

SETTINGS



User Management - Settings

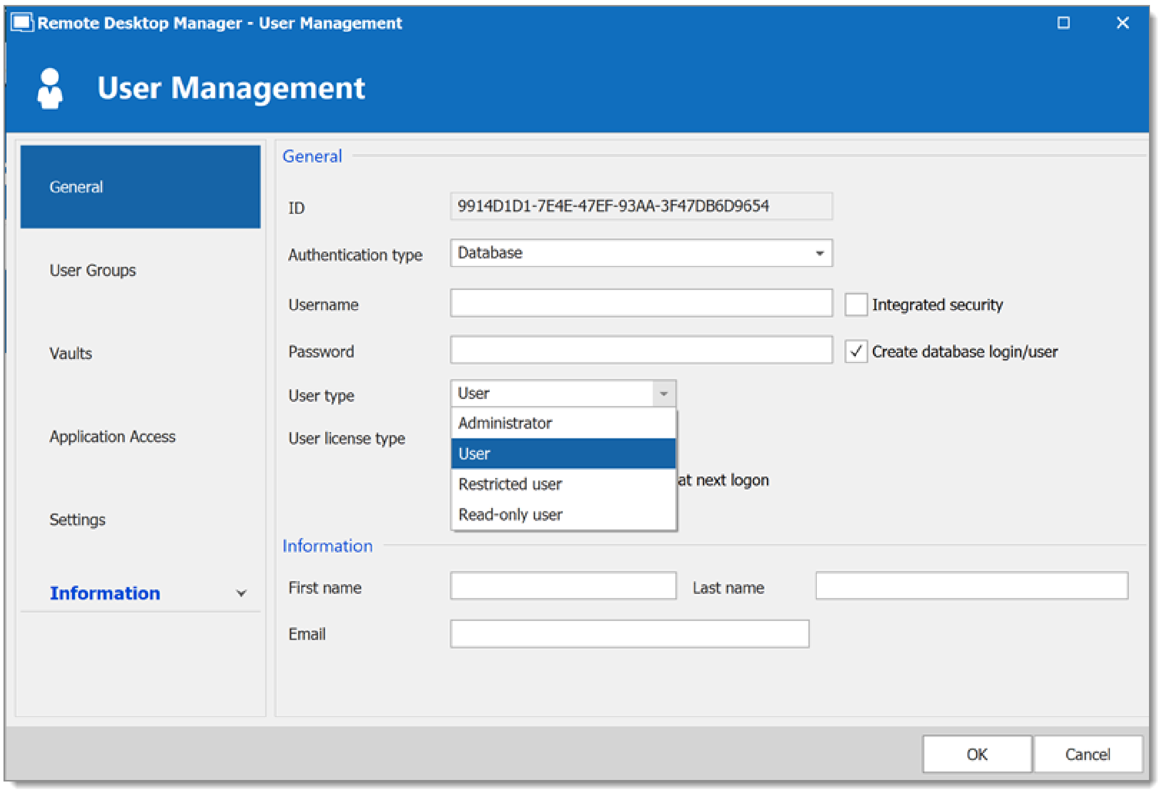
Allow the user to enable the Offline Mode on the data sources. This also depends on the data source being configured to allow it. There are 4 modes available:

OPTION	DESCRIPTION
Disabled	No offline cache allowed for the user.
Cache only	Allow to save a cache of the data source but not the offline mode.
Read-only	A read-only cache. The user will not be able to edit data in the data source. This mode is allowed for Advanced Data Sources only.
Read/Write	An advanced cache, with change synchronization. This mode is allowed for Advanced Data Sources only.

6.7.1.1.1 User Types

DESCRIPTION

When creating users in Remote Desktop Manager, four types of user are available. Basic rights are granted to the created users depending on their type.



User Management - User Type

TYPE	DESCRIPTION
Administrator	Grant all rights and permissions to the user.
User	Grant all the basic rights to the user (Add, Edit, Delete). For more information, please consult the Rights section below in this topic.
Restricted user	Personalize the rights to grant to the user.

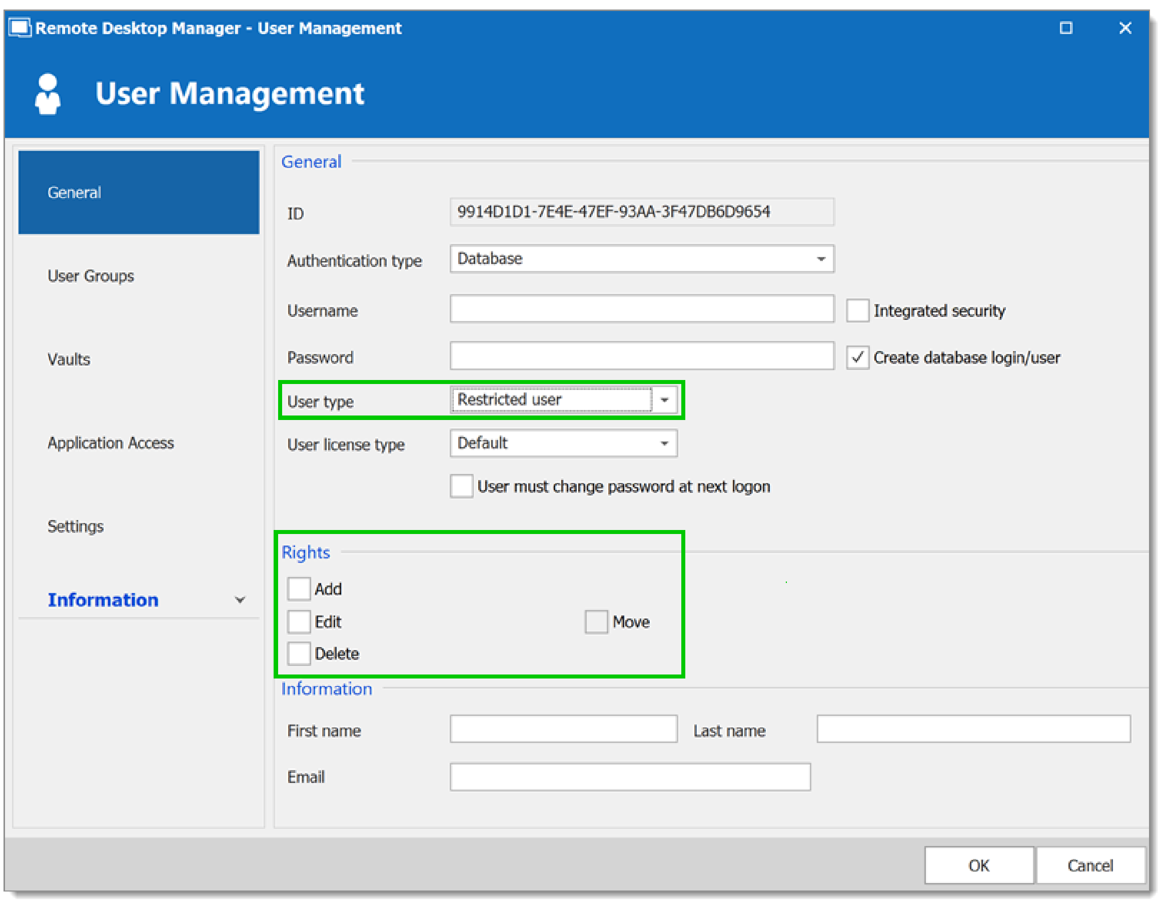
TYPE	DESCRIPTION
Read only user	Grant only the view access to the user.

RIGHTS

When setting a user to the **Restricted User** type, rights must be granted manually. These rights have an immediate influence on which actions the user can perform on unsecured entries. Therefore, rights must be granted for users to be able to perform actions on entries, as permissions cannot override the absence of right.

Once rights are granted, they can be restricted with the User Groups Based Security or Security Groups.

The **Add** right also displays the **Add in Vault** option. This must be enable for users to be able to add entries into the Vault folder of the data source.



User Management - Rights

6.7.1.1.2 Integrated Security

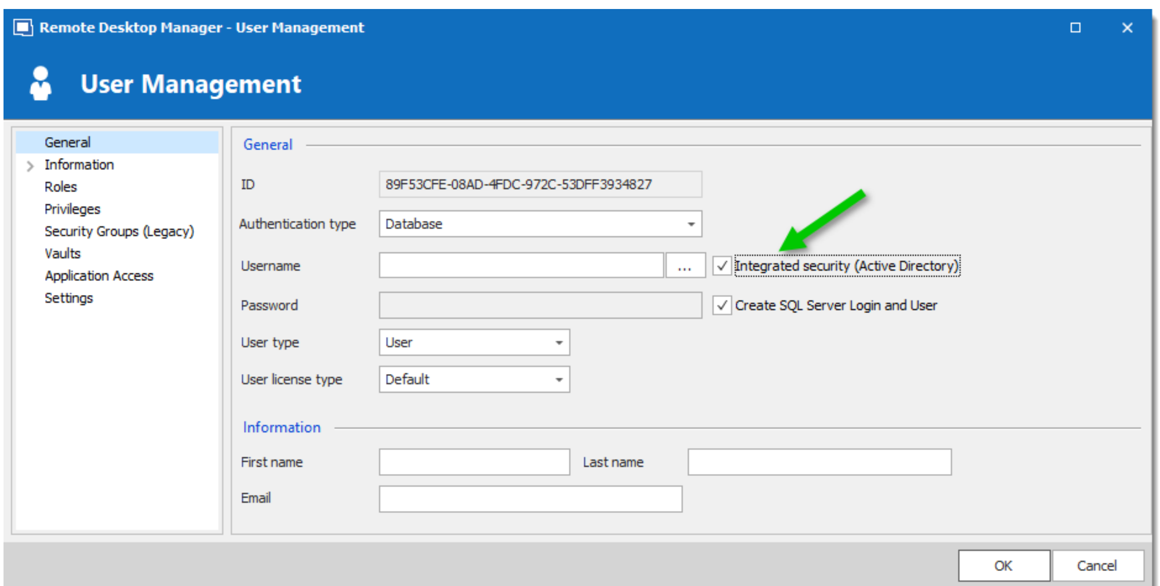
DESCRIPTION

Integrated Security is a Microsoft technology, which uses the credentials of the current Windows session and send them automatically to the remote resources for authentication.

> This feature is available with the SQL Server or Devolutions Server data sources.

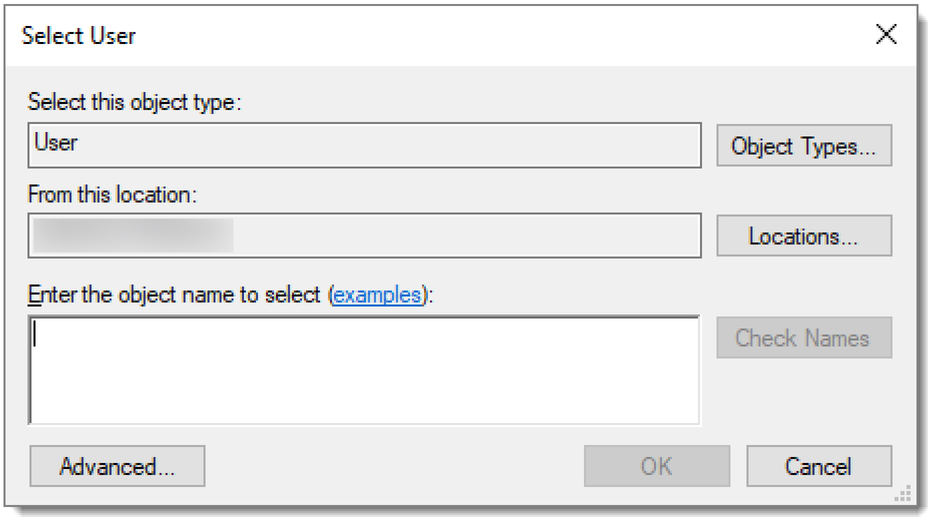
SETTINGS

To use the Integrated Security, enable the **Integrated Security** box in the **User Management** window. The **Password** field is disabled because the operating system will provide a cached copy automatically.



Integrated Security

When the option is activated, an ellipsis button either appears or is enabled. Click this button to display the **Select User** dialog.



Select User

Ensure the appropriate domain is displayed in the **From this location** field. Sometime the location defaults to the local computer. Click the **Locations** button to browse for the domain instead.

When using Integrated Security, the currently running windows session must be from a user of the domain. If you need to use other credentials, Remote Desktop Manager must be started using the RUNAS command as described in Running Remote Desktop Manager as Another User.

6.7.1.2 User Groups Management

DESCRIPTION

User Groups in Remote Desktop Manager manages multiple users at the same time by grouping them. The management of permissions granted to user groups are quite similar to the corresponding notions for users, but instead of a single user, they apply to all users to which you've assigned the user groups.

This feature is only available with an Advanced Data Source.

USER GROUPS IN DEVOLUTIONS SERVER

User Groups in Devolutions Server are in fact links to Active Directory groups. By leveraging Active Directory integration you can easily define access rights for all domain users in your organization. Once a domain user log in the Devolutions Server data source, their user account will be created if needed and users rights will be controlled by the defined groups.

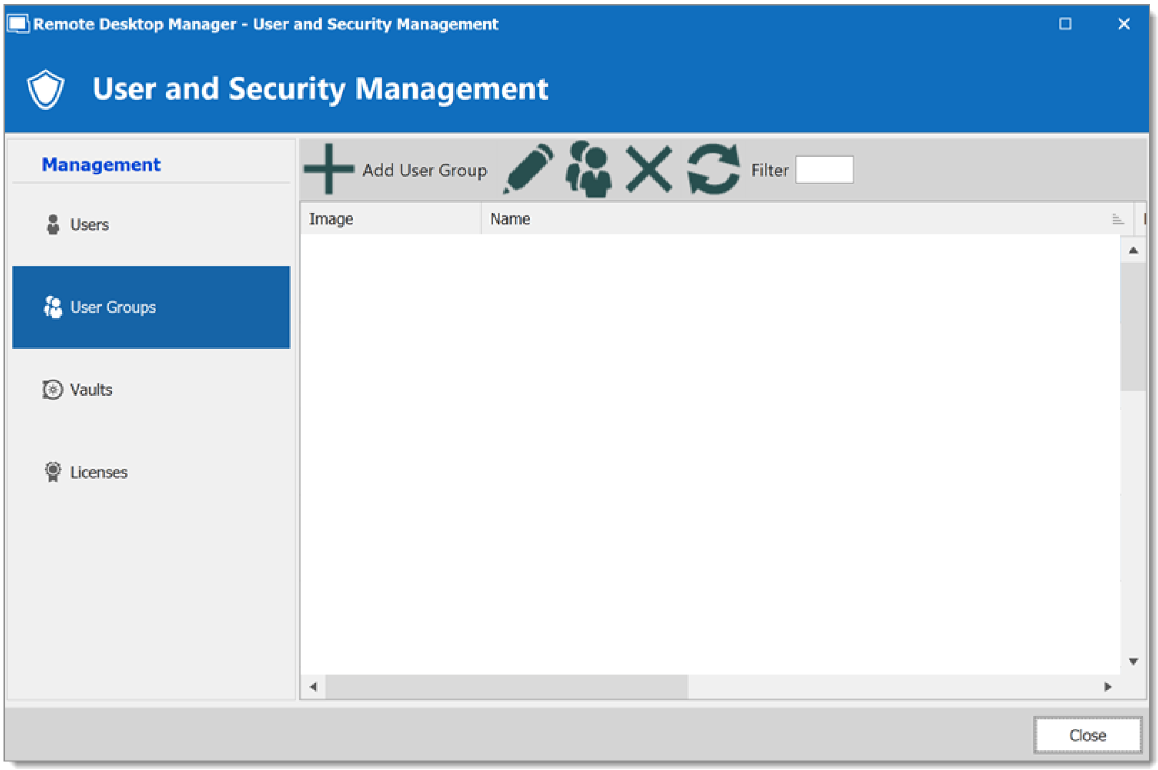
Please note that the Unsecured group permissions (the ones above the grid) are ignored. You must set them on each user individually.

For more information please see Devolutions Server User Groups Management.

CREATE USER GROUPS

User Groups in Remote Desktop Manager are mainly used to group users. You can assign multiple user groups to each user. The end result is the union of all permissions given to the user groups.

To create a user groups, in the **User and Security Management** window, click the **Add User Group** button in the **User Groups** section. From the same menu, you can also edit, assign users, delete or refresh.



User Groups - Add User Group

6.7.1.3 Vaults Overview

DESCRIPTION

Vaults are containers that divide the data source into multiple compartments.

We recommend using vaults for improved organization and security.Vaults also help performance as they limit the amount of entries that load at once.

Vaults are available with Advanced Data Sources: Devolutions Server, Azure SQL and SQL server.

This feature underwent a change of name, as **Vaults** were called **Repositories** before **Remote Desktop Manager 2019**.

This article covers:

- Create vault

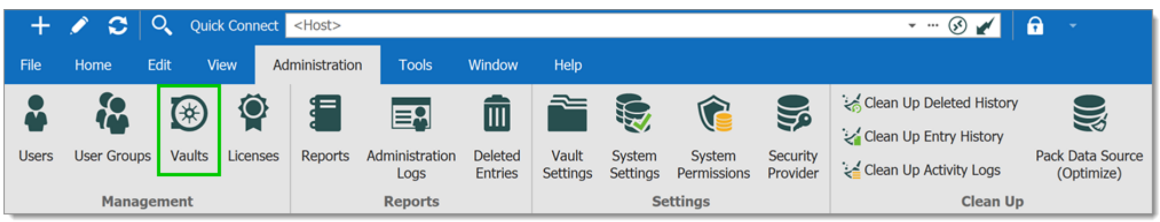
- [Move entries to different vaults]
- [Navigate between vaults]
- [Role-based security with vaults]
- [Vaults shortcuts]

SETUP AND USE VAULTS IN REMOTE DESKTOP MANAGER

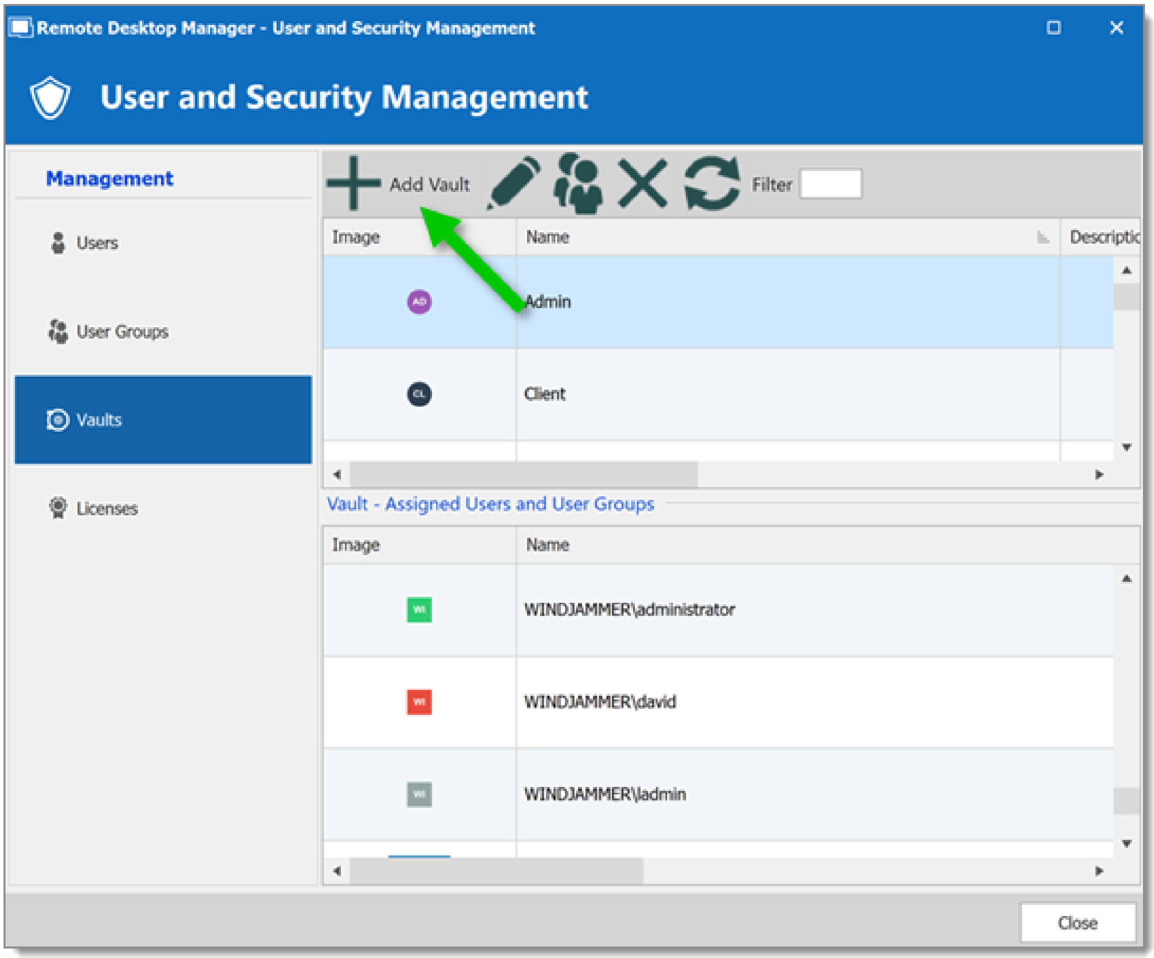
CREATE A VAULT

We recommend creating a different vault for each customer or department.

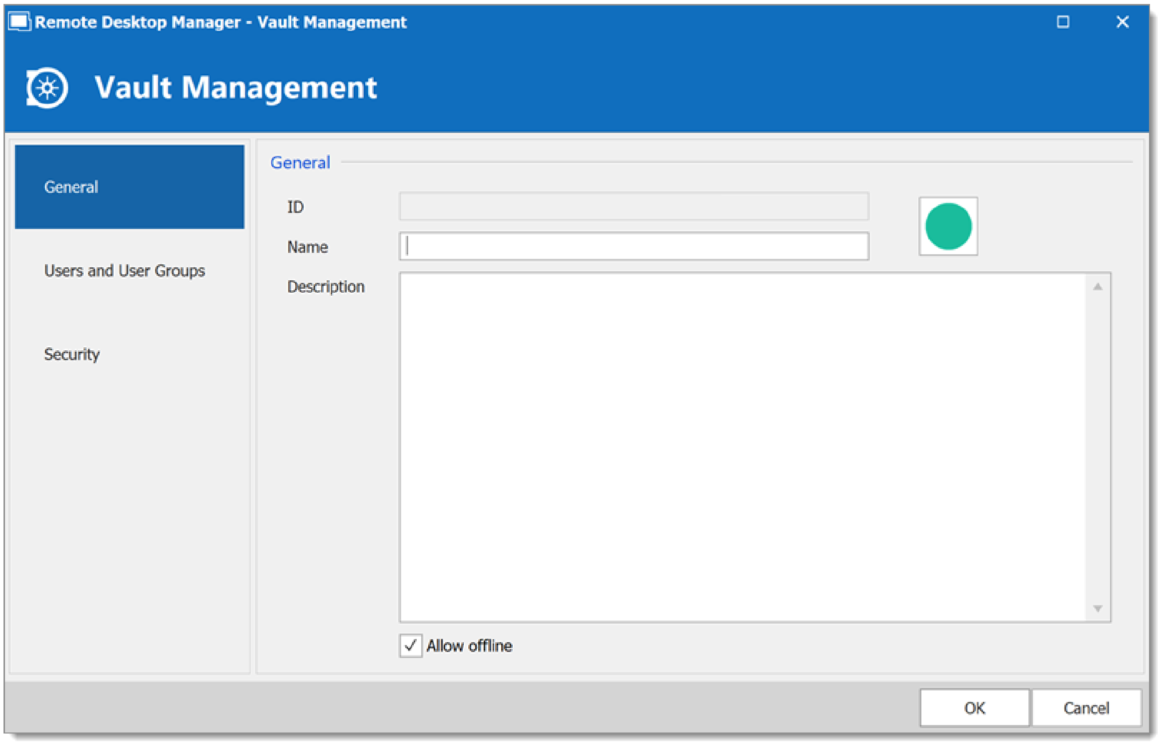
1. On the ***Administration*** tab, click ***Vaults***.



2. Click ***Add Vault***.

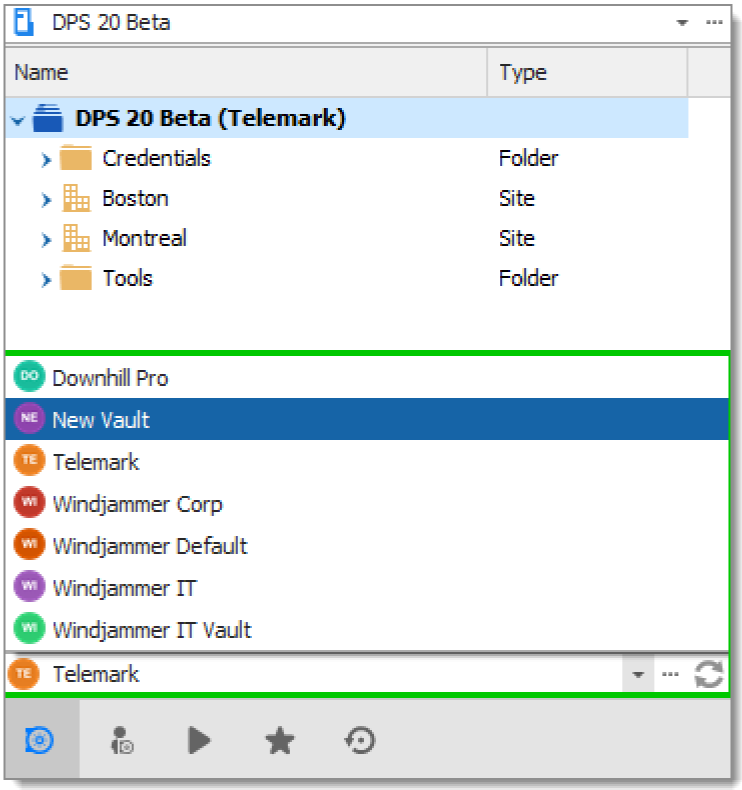


3. Enter a ***Name*** and ***Description*** (optional). The ID is generated automatically.



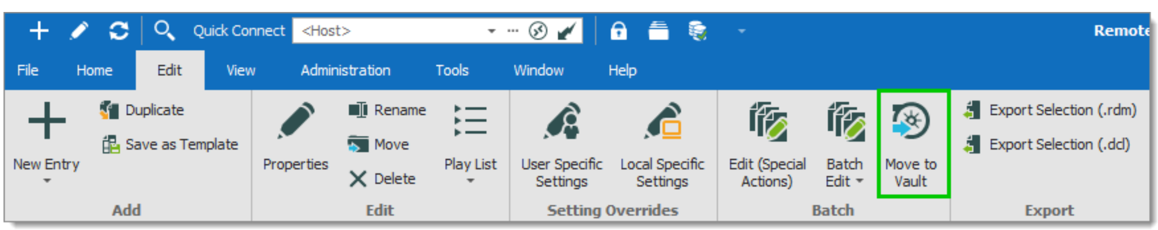
MOVE BETWEEN VAULTS

In the navigation pane, use the vault list to move between vaults. Change the location of the vault list in ***File – Options – User Interface – Vault Location***.

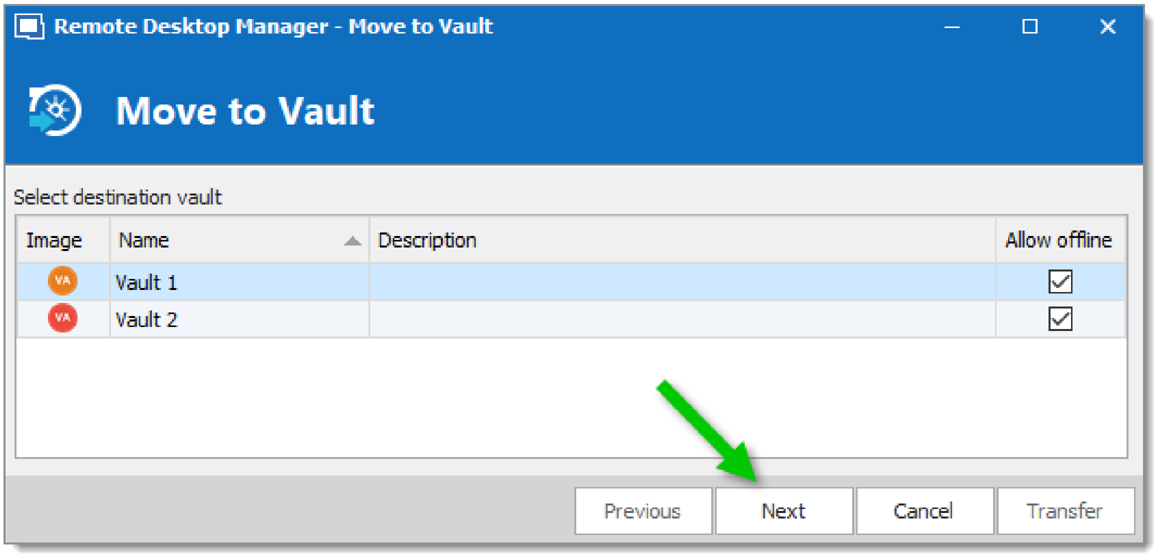


MOVE ENTRIES TO A DIFFERENT VAULT

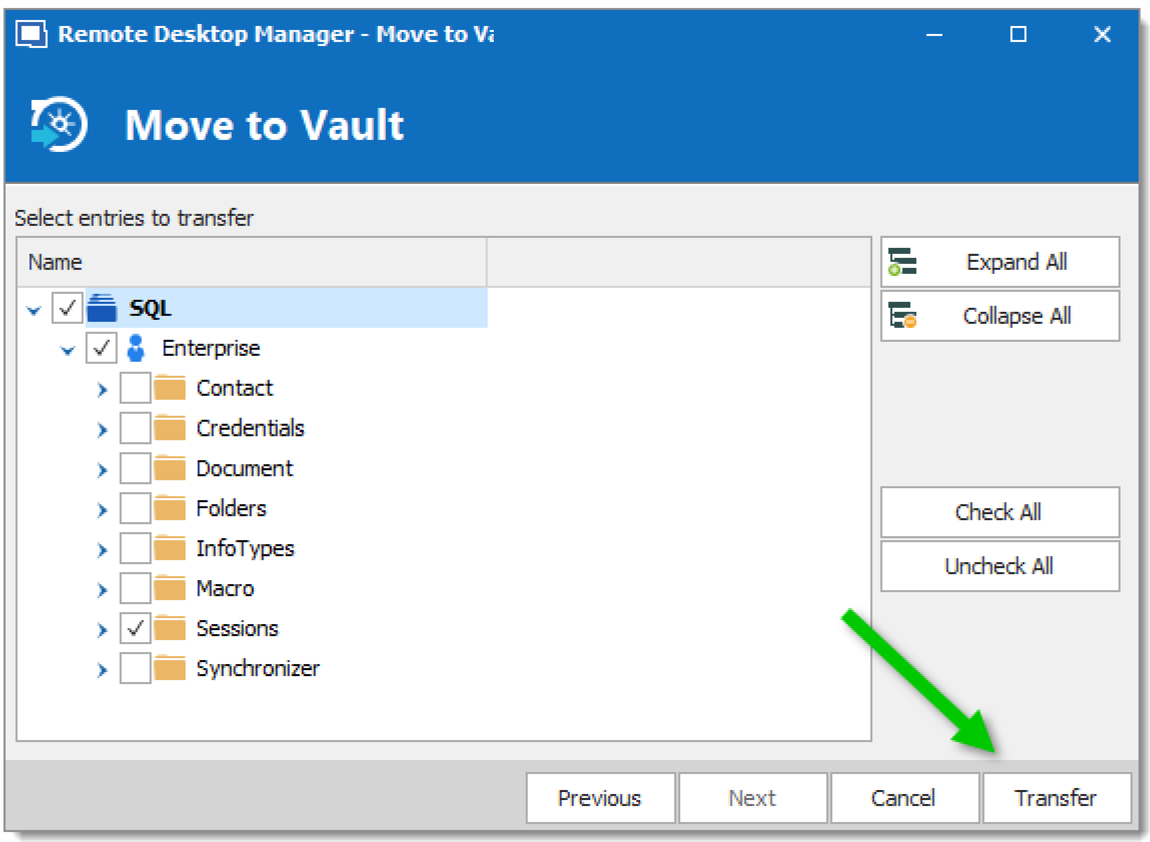
1. Start in the vault you want to transfer entries out of.
2. On the ***Edit*** tab, click ***Move to vault***.



3. Select the vault you want to move the entries to, and click ***Next***.



4. Choose the entries you want to transfer to the new vault, and click ***Transfer***.



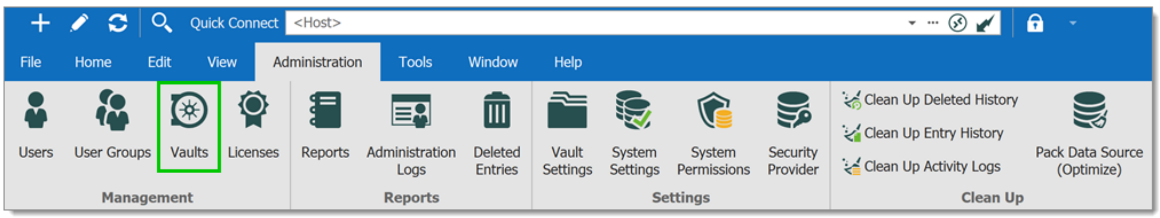
MANAGE ROLE-BASED SECURITY BY VAULT

Vaults simplify user management because Active Directory groups define who has access to a vault. These Active Directory groups are known as ***User groups*** in

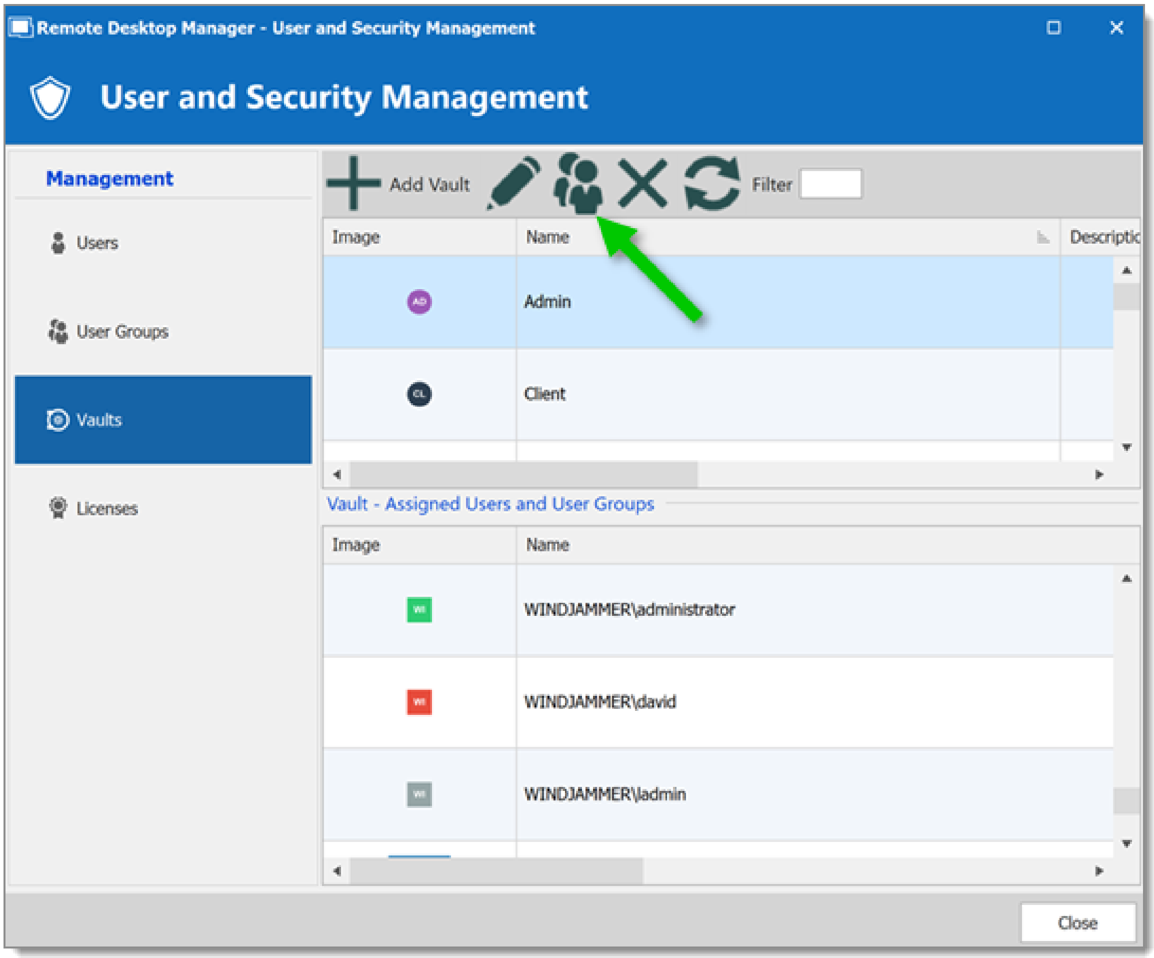
Remote Desktop Manager. In general, most user groups have access to a couple of vaults, while some groups will only have access to one vault. Limiting access to vaults minimizes the need to set permissions on lower-level folders.

GIVING ROLES ACCESS TO A VAULT

1. On the ***Administration tab***, then click ***Vaults***.

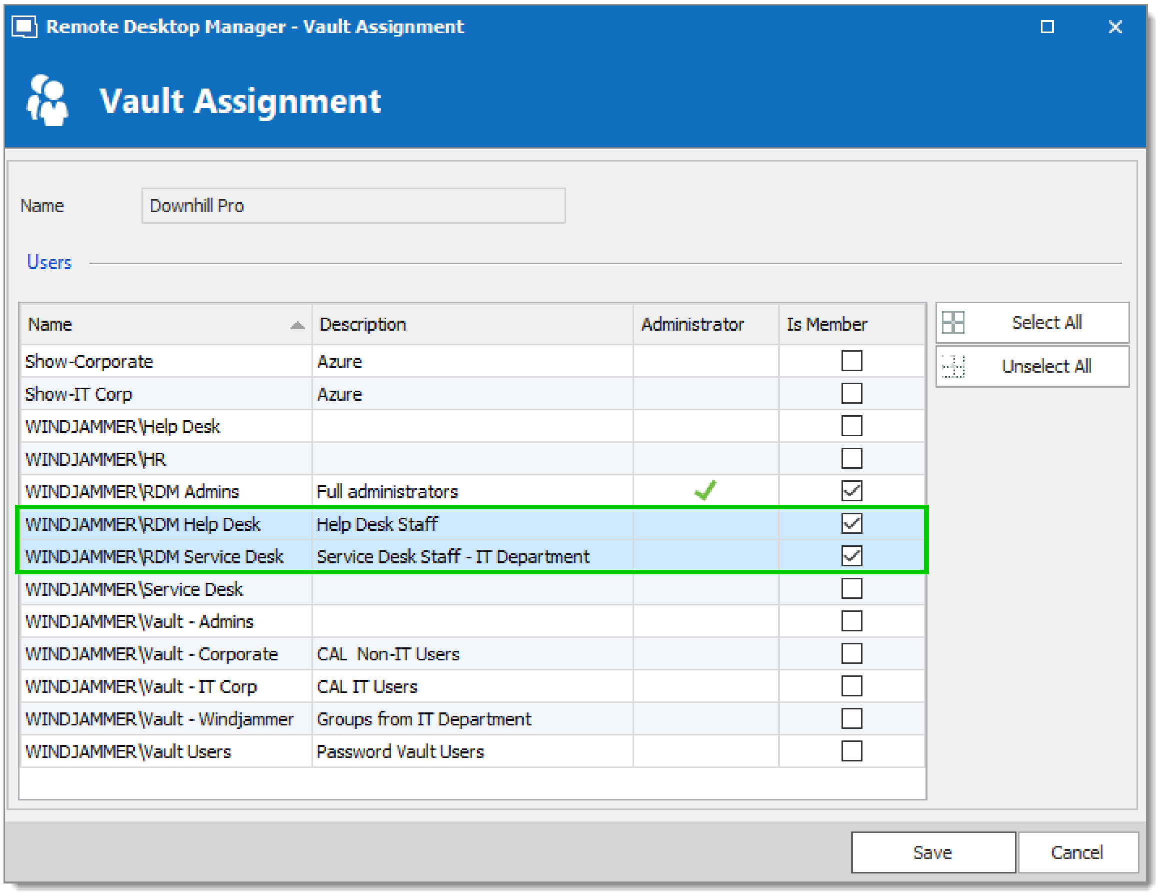


2. On the ***User and Security Management*** window, choose the vaults, then click ***Assign User groups***.



User and Security Management - Vaults - Assign Roles

3. Choose which user groups have access to the vaults: select the ***Is Member*** box.



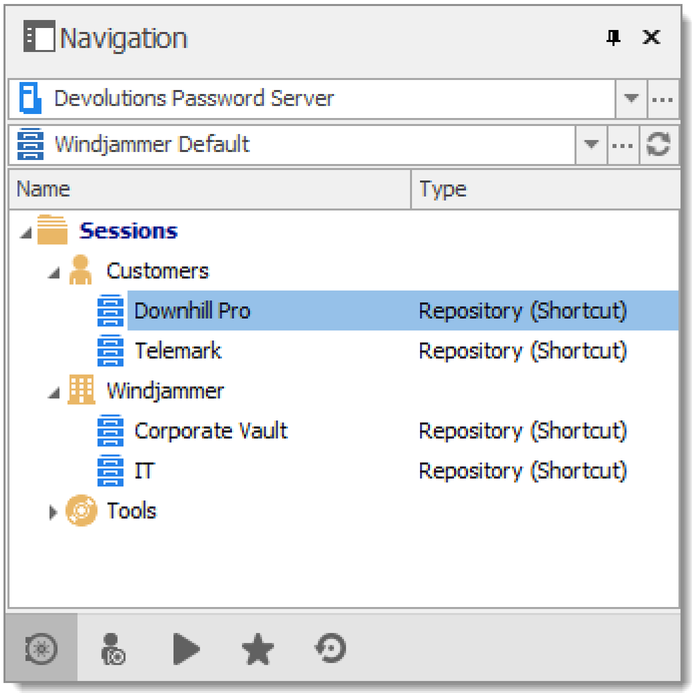
VAULTS SHORTCUTS

Navigate between vaults with the Vault List or vaults shortcuts.

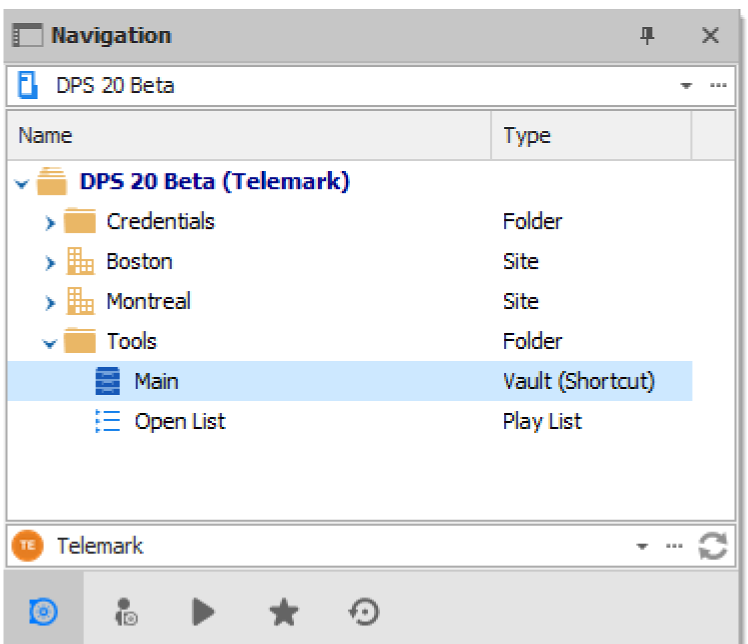
We recommend administrators and users who have access to multiple vaults create vaults shortcuts to navigate between vaults.

If you use vaults shortcuts, the vault should only contain folders. Do not save entries at the vault root.

The main (default) vault contains shortcuts to other vaults.



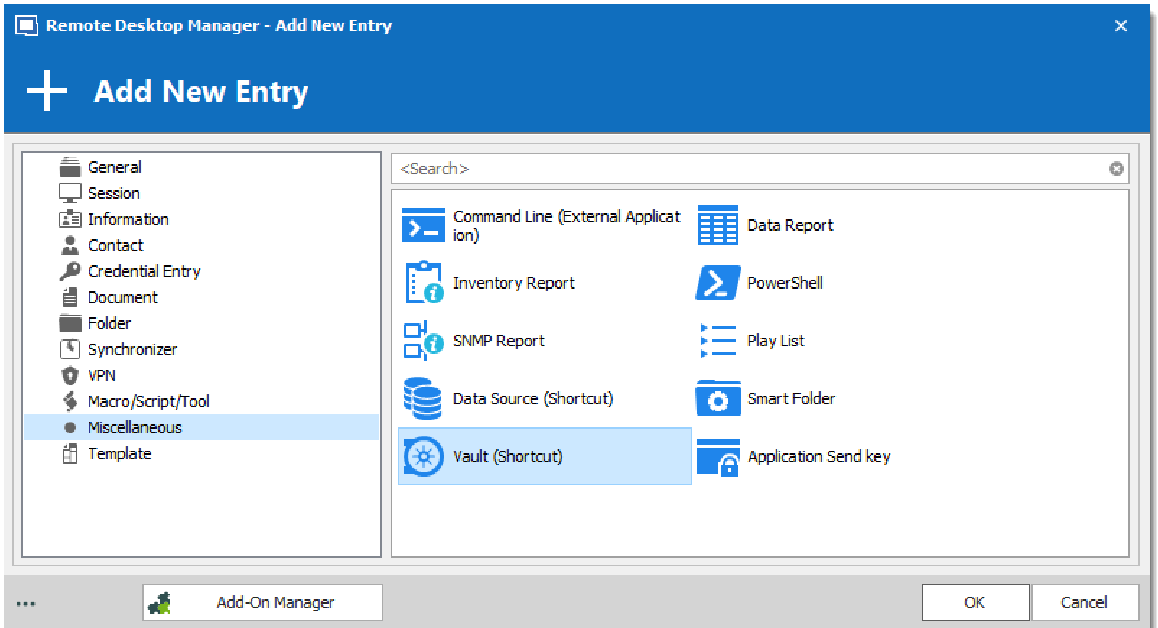
Each vault contains a shortcut that returns the user to the main vault.



CREATE A VAULT SHORTCUT

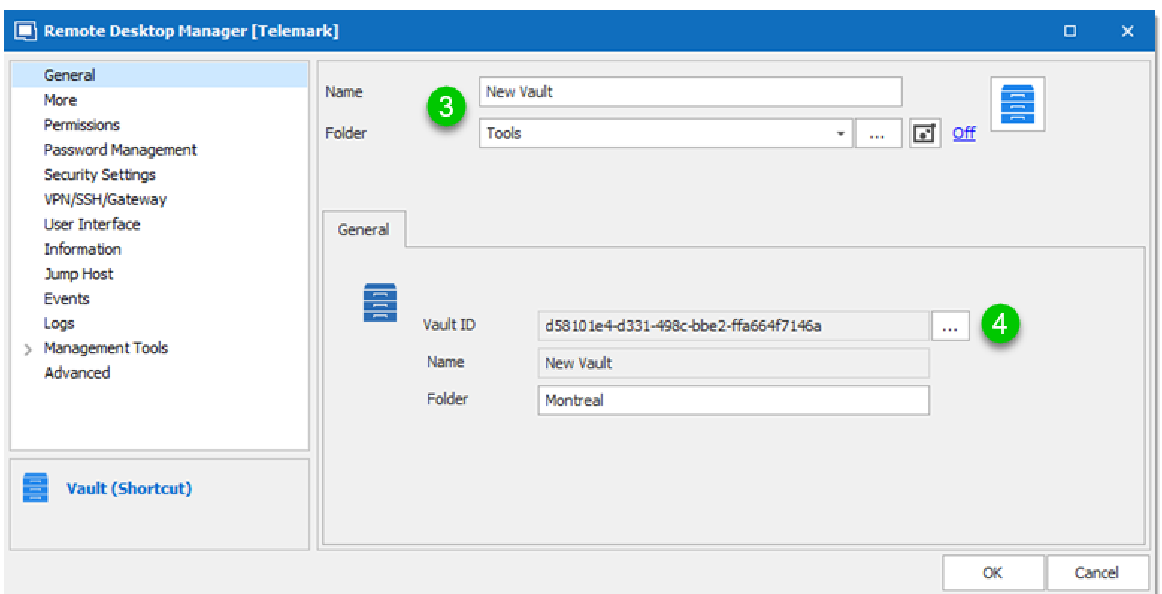
1. On the ***Edit*** tab, click ***New Entry***.

2. Click ***Miscellaneous*** and then select ***Vault (Shortcut)***.

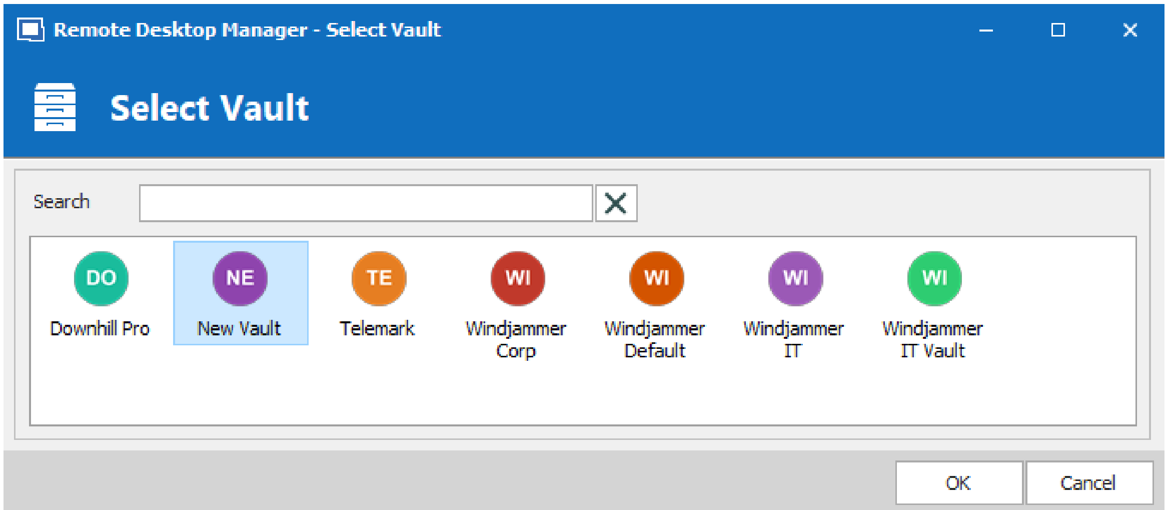


3. In the ***Name*** box, enter the name of the vault you are creating a shortcut to. Save the shortcut in a folder.

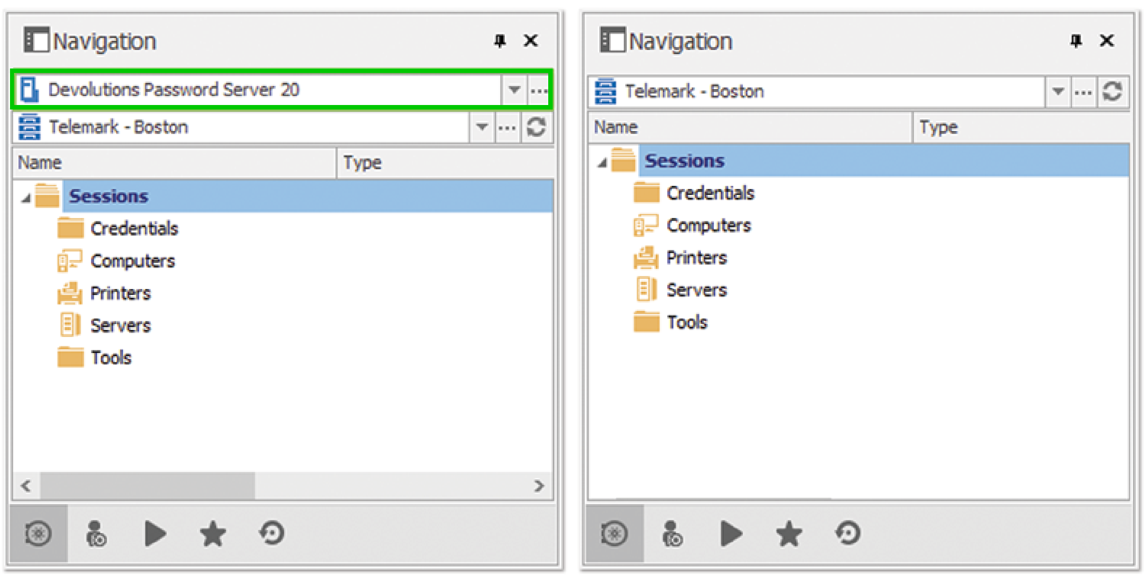
4. To find the ***Vaults ID***, click the ellipses button. Enter a folder name (case sensitive) to create a shortcut to a specific folder.



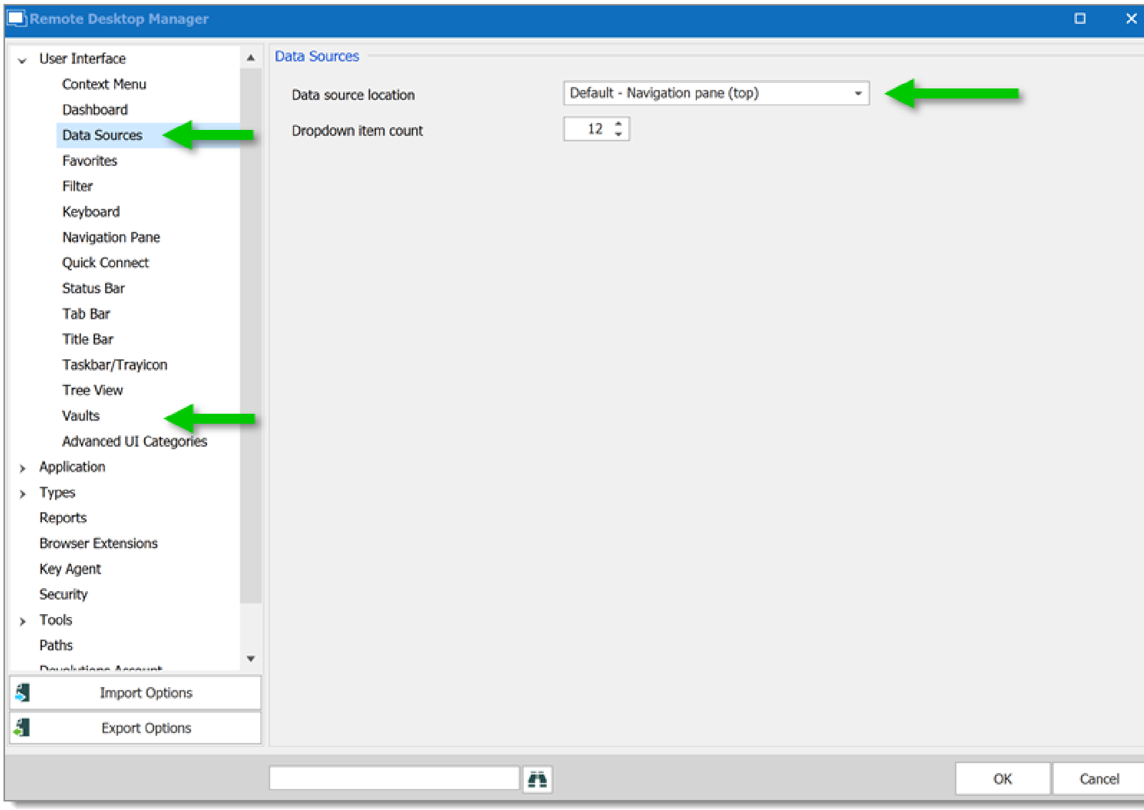
5. Select the destination vault.



We recommend removing the data source drop-down list when using vault shortcuts. Then the vaults list can be moved above the Navigation Pane.



You can find the options in ***File - Options - User Interface - Data Sources*** and ***Vaults***.



6.7.1.4 Licenses

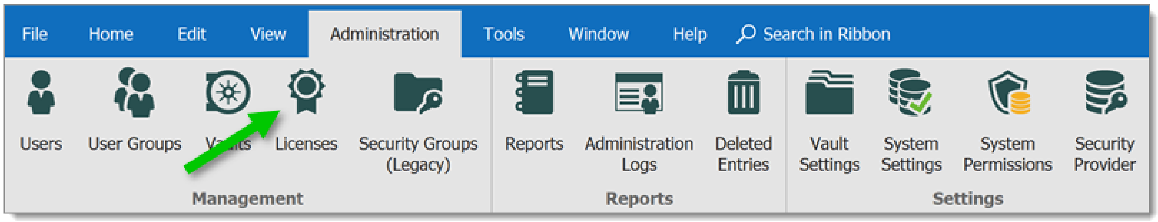
DESCRIPTION

Managing Remote Desktop Manager registration globally for all your users can be done with a license serial stored in an advanced data source such as Devolutions Server, Microsoft SQL Server or Azure SQL.

> It is possible to request a trial to try Remote Desktop Manager for 30 days. If you decide not to register the application at the end of the 30 days period, your data will not be altered or erased, and you will have full access to it once you provide a valid license serial.

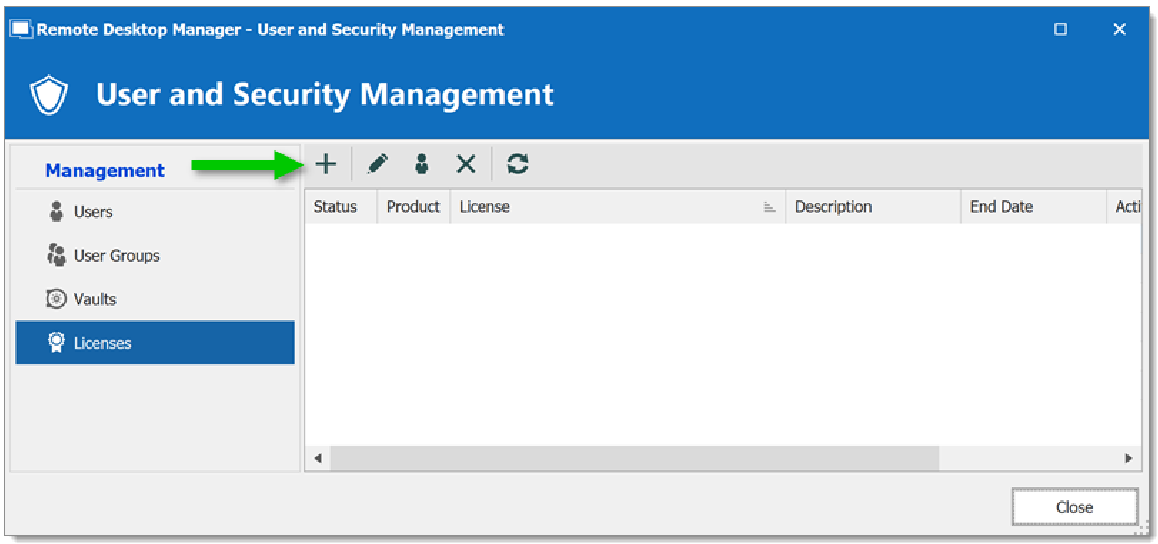
With license stored in an Advanced Data Source, there is no need to register Remote Desktop Manager as the license serial is retrieved directly from it. When launching the application for the first time, add the data source containing the serial.

1. To add a license serial, navigate to ***Administration - Licenses***.



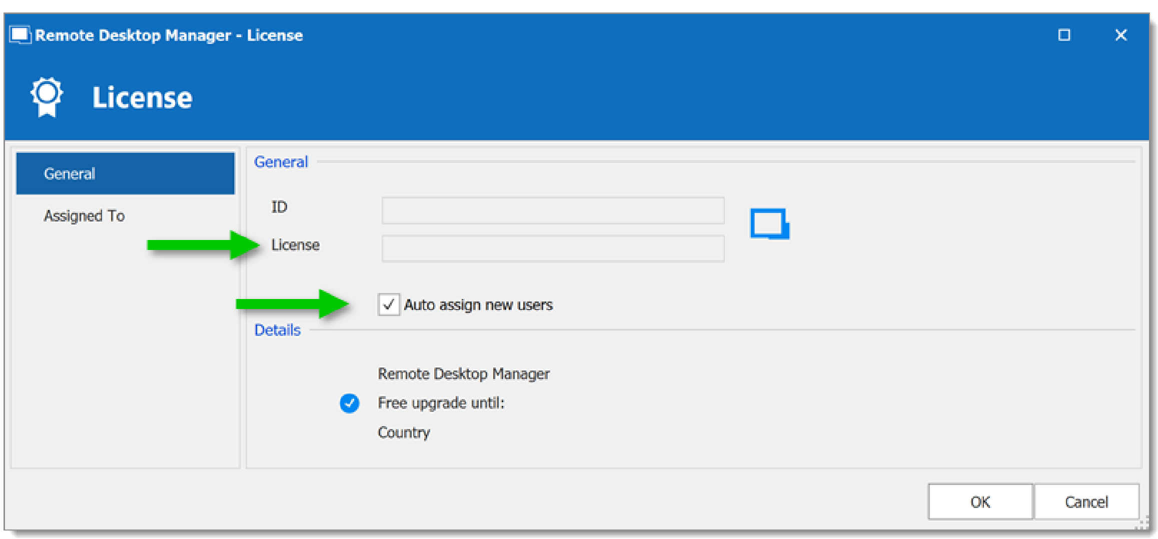
Administration - Licenses

2. Click ***Add License***.



3. Enter the license serial.

4. Optional: Check the ***Auto assign new users***, to automatically provide the RDM serial to all newly created users.



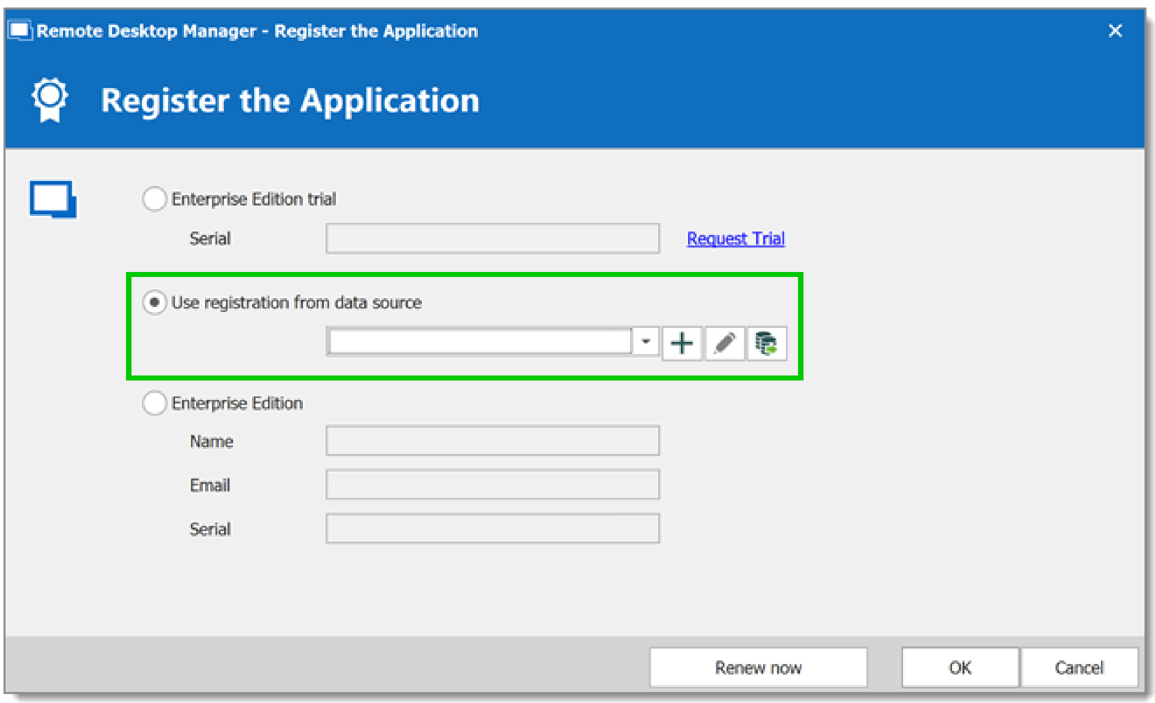
5. Click ***OK*** to save.

Your license is now saved in the advanced data source. Follow this next topic to automatically Assign Licenses to selected users, removing the need to interact locally with their Remote Desktop Manager.

6.7.1.4.1 Assign Licenses

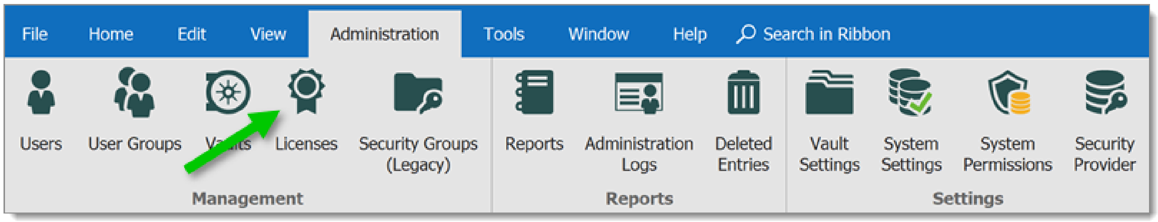
DESCRIPTION

When the license is stored in an Advanced Data Source in ***Administration - Licenses***, there is no need to register Remote Desktop Manager locally as the license serial is retrieved directly from it. When launching the application for the first time, add the data source containing the serial.



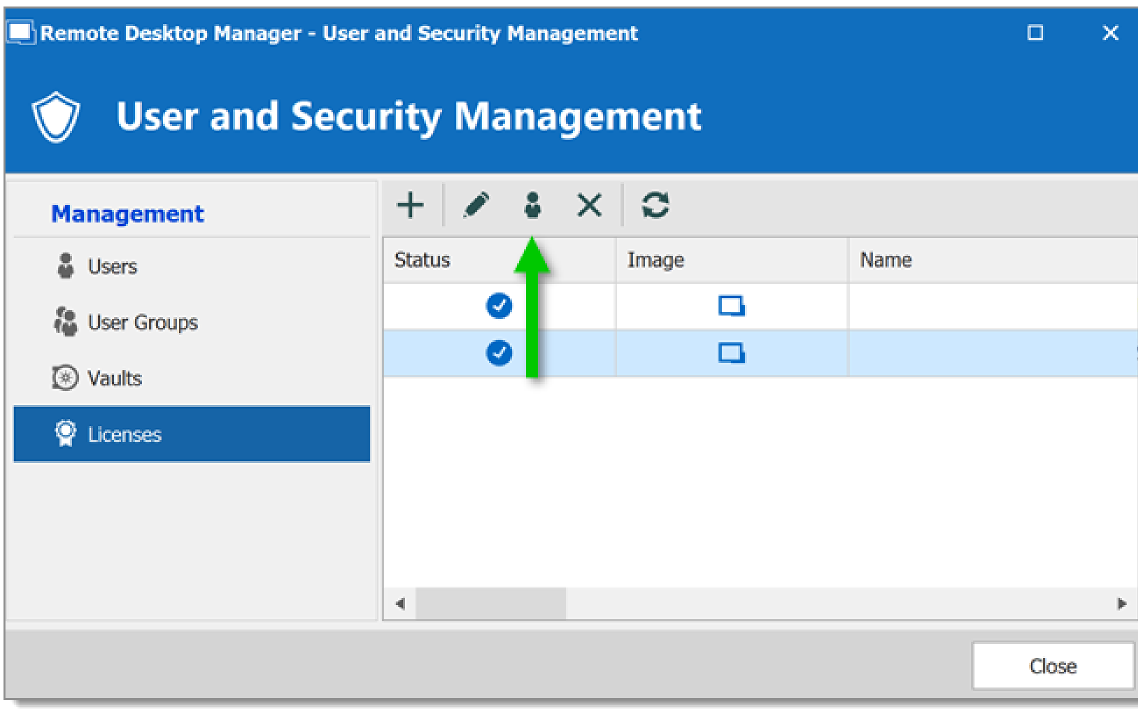
As an administrator, manage your users license in Remote Desktop Manager.

1. Go to ***Administration - Licenses***.



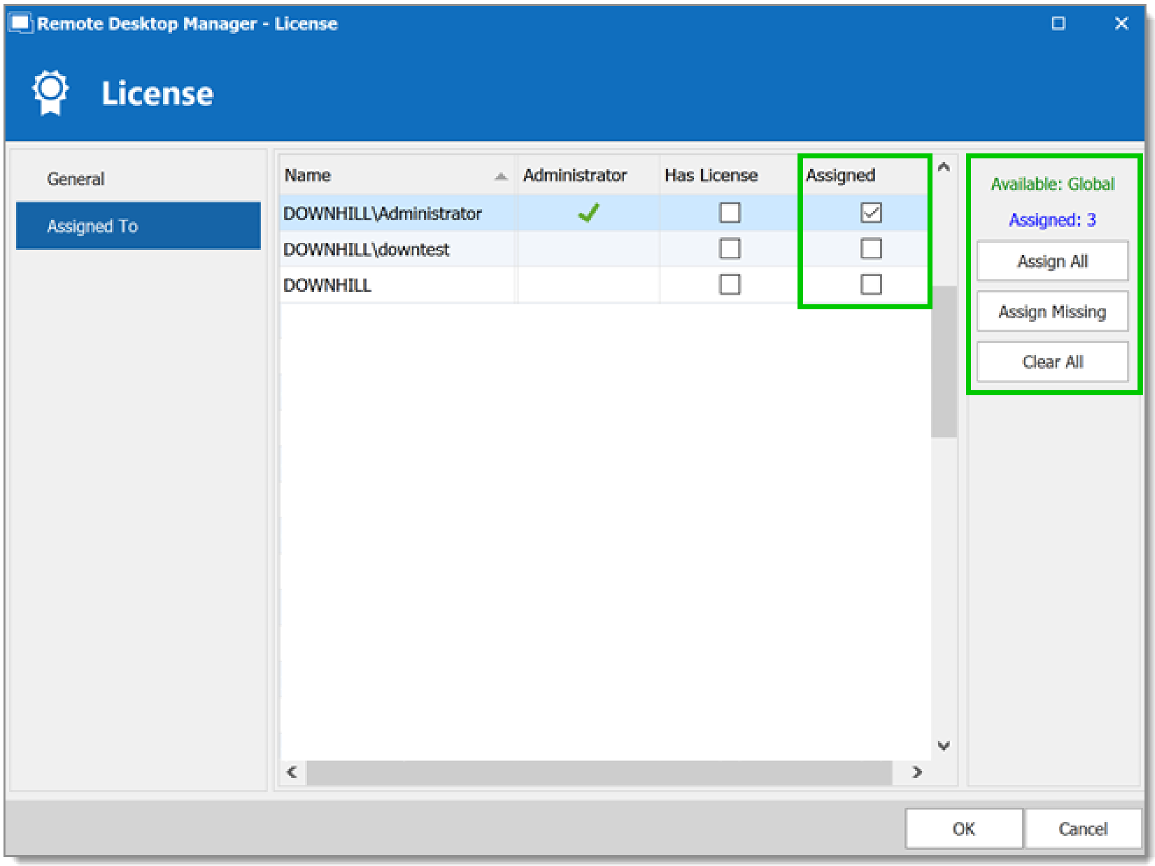
2. Select the license and click the ***Assign Licenses*** icon.

> If you have more than one license, our [Sales team](#) can provide a co-terminated renewal to facilitate your license management.



3. In the ***Assigned*** column, check next to each user you need to grant a license or use the global action buttons.

> This step will automatically assign the license to the selected users, removing the need to interact with each user.



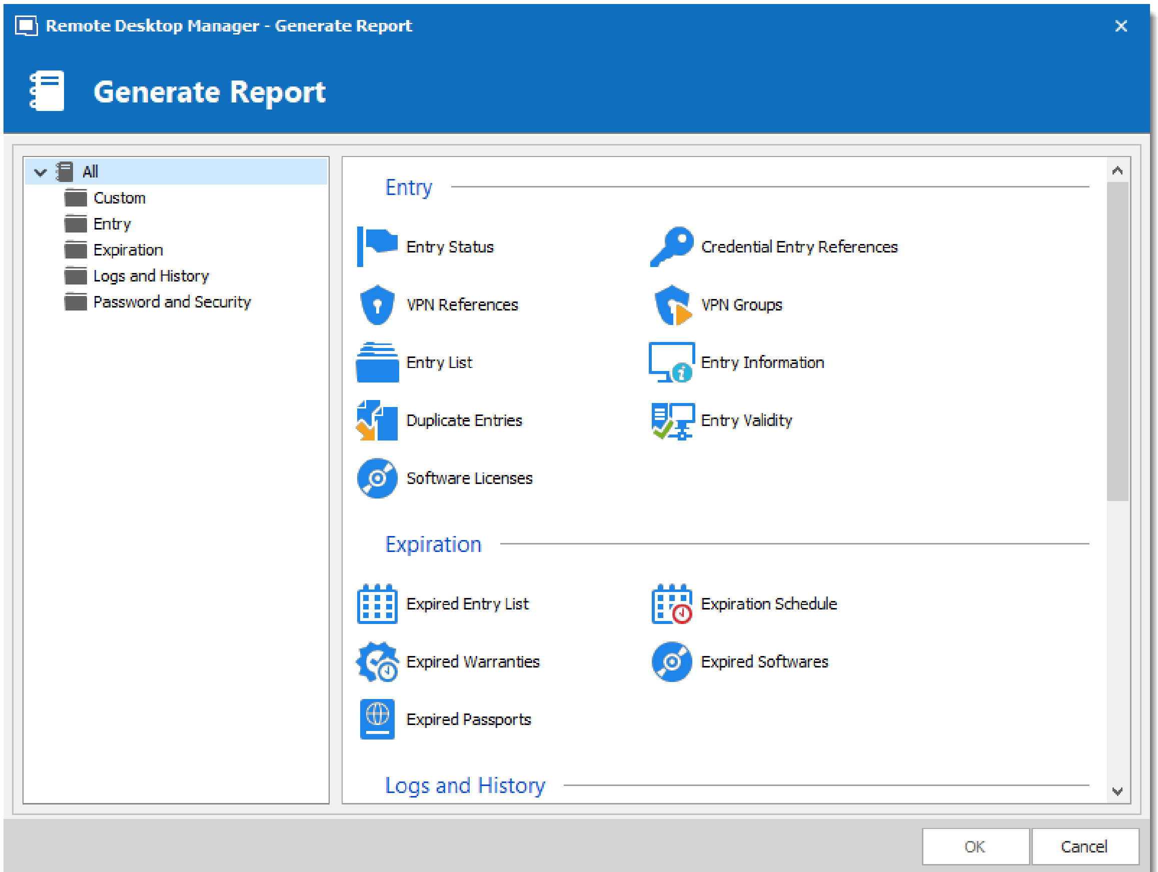
4. Click ***OK*** to save.

6.7.2 Reports

6.7.2.1 Reports

DESCRIPTION

The **Reports** section automatically generates reports detailing Remote Desktop Manager usage related to: Entries, Expired Assets, Passwords, Security and Users. You have the option to export your generated report, as well as executing and exporting reports through a command line.



Generate Report

From this window, you can browse and select a wide variety of Report Types. Explore to your heart's content.

Once Generated, a report will provide you with all the information you selected during this step. These final results can take various shapes and have different features (such as editing a specific entry or printing the result) depending on what the report actually is.

> These logs are still restricted by user rights. A user with restricted access wouldn't be able to select Password and Security for example.

6.7.2.1.1 Export Reports

DESCRIPTION

The Export Reports is a way to execute and export reports through a command line. You can use this feature in a shortcut or in a batch file and use the Windows task scheduler to execute it.

You will be able to export Data Report, Inventory report as well as most of the reports found in our Generate Report list except for the Password Usage and Security Group.

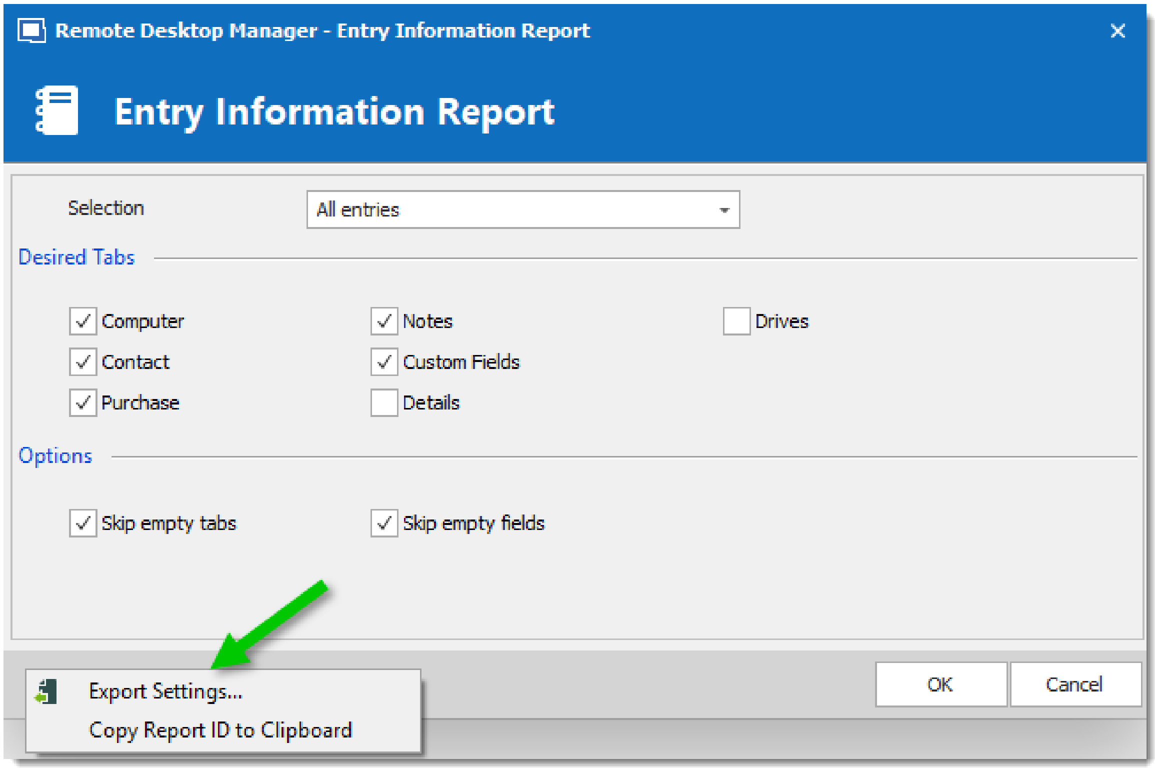
> You must have the rights to run report in Remote Desktop Manager to use this feature.

SETTINGS

Watch Video

For Reports containing settings, you will have to start with exporting your report settings to create the ***.rdr** file that the command line use to generate the reports. Here is a list of reports containing settings:

1. Select your Report in ***Administrations – Report*** and then select the option ***Export Settings*** in the ***More*** text button. It will create an ***.rdr** file containing all your report settings. This is also where you Report ID is located (this will be useful later on).



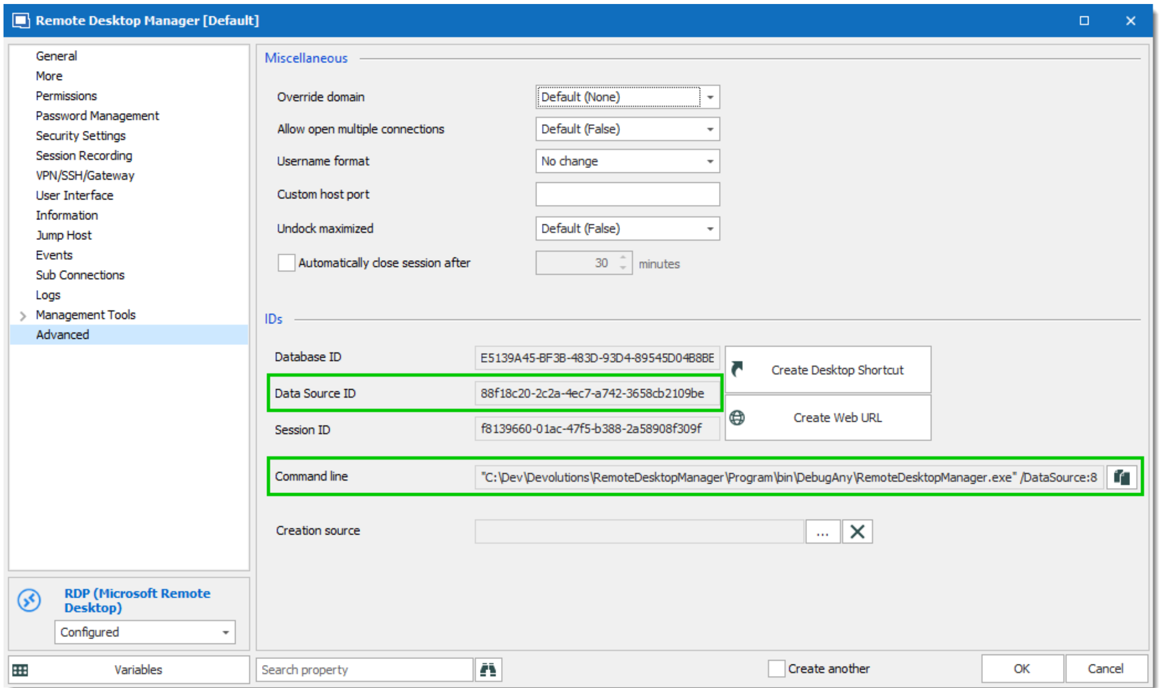
Export Settings

2. In your Windows Command Prompt enter the following command line:

```
C:\*** /DataSource:*** /report:***/reportoutput:"***" /reportsettings:"***.rdr"
```

PARAMETERS	DESCRIPTION
C:	Enter the path used to start your Remote Desktop Manager application (path of the RemoteDesktopManager.exe file)
/DataSource	Specify the data source ID.
/report	Specify the type of report to generate or the report ID.
/reportoutput	Specify the path to save your report and the name for the newly generated report.
/reportsettings	Specify the path of your report settings file (.rdr).

To find your Data Source ID and the Command Line use to start Remote Desktop Manager edit one of your session from your data source and select the Advanced section.



RDP Session - Advanced Section

Here is a list of types of ***Reports*** you can find in Remote Desktop Manager and the name to enter in the command line to generate the report:

REPORT TYPE	REPORT NAME (TYPE) TO INSERT IN THE COMMAND LINE
Activity Logs Report	SharedConnectionLog
Duplicate Entry	DuplicateEntry
Entry Information	ConnectionInformation
Entry Status	ConnectionStatus
Expired Entry List	ConnectionExpiredEntry

REPORT TYPE	REPORT NAME (TYPE) TO INSERT IN THE COMMAND LINE
Expired Passports	ConnectionExpiredPassport
Expired Softwares	ConnectionExpiredSoftware
Expired Warranties	ConnectionExpiredWarranty
Password Complexity	PasswordComplexity
VPN Groups	VPNGroup

Here is an example of a command line for an Entry Information Report:

```
C:\Program Files (x86)\Devolutions\Remote Desktop Manager\RemoteDesktopManager.exe /Da
/reportoutput:C:\dev\devolutions\Rapport\rapportEntry.csv /reportsettings:C:\dev\devol
```

6.7.2.2 Deleted Entries

DESCRIPTION

The ***Administration – View deleted*** option allows you to view the deleted entries as well as restoring them.

> This feature requires an Advanced Data Source.

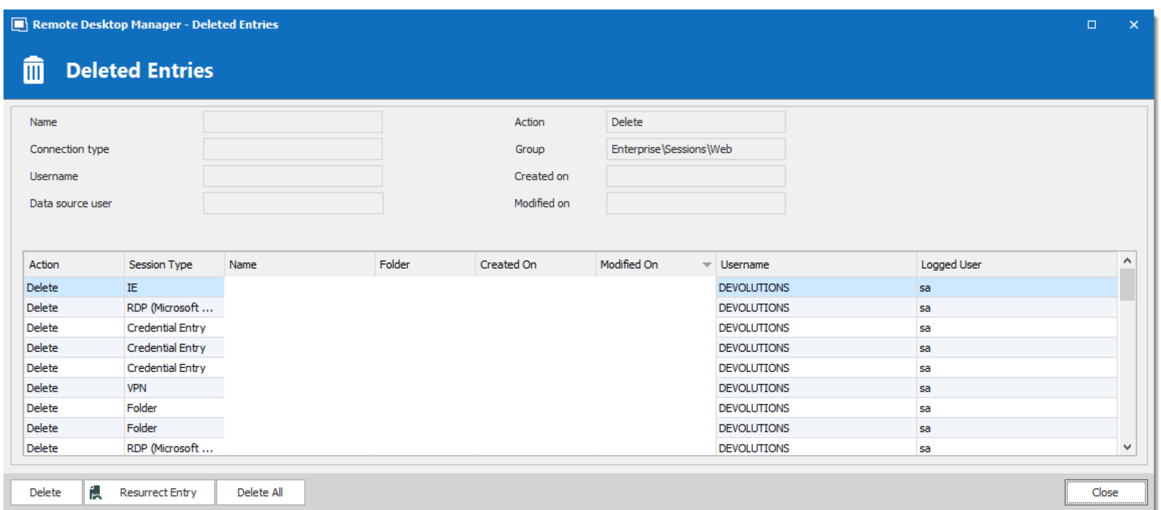
> Administrators can permanently delete some or all deleted entries.

Sub-connections are not retained in the View Deleted window. To restore a sub-connection, please have a look at Entry History.

SETTINGS

MANAGE DELETED ENTRIES

The **Deleted Entries** will generate a list containing all the entries previously deleted from your data source. You may resurrect an entry, meaning it will become an active entry again and will be shown in your data source. You may also chose to permanently delete your entries, once you have permanently deleted your entries you won't be able to resurrect them afterward.



Deleted Entries

OPTION	DESCRIPTION
Delete	Permanently delete the selected entry.
Resurrect Entry	Use this button to restore an entry.
Delete All	Permanently delete all the deleted entries.

Deleted entries can be resurrected as long as the Security Provider has not been changed since the deleted action.

EXPORT DELETED ENTRIES LIST

You can use the **Right-click** button on one or several lines to export them in CSV, HTML or XML format.

6.7.3 Settings

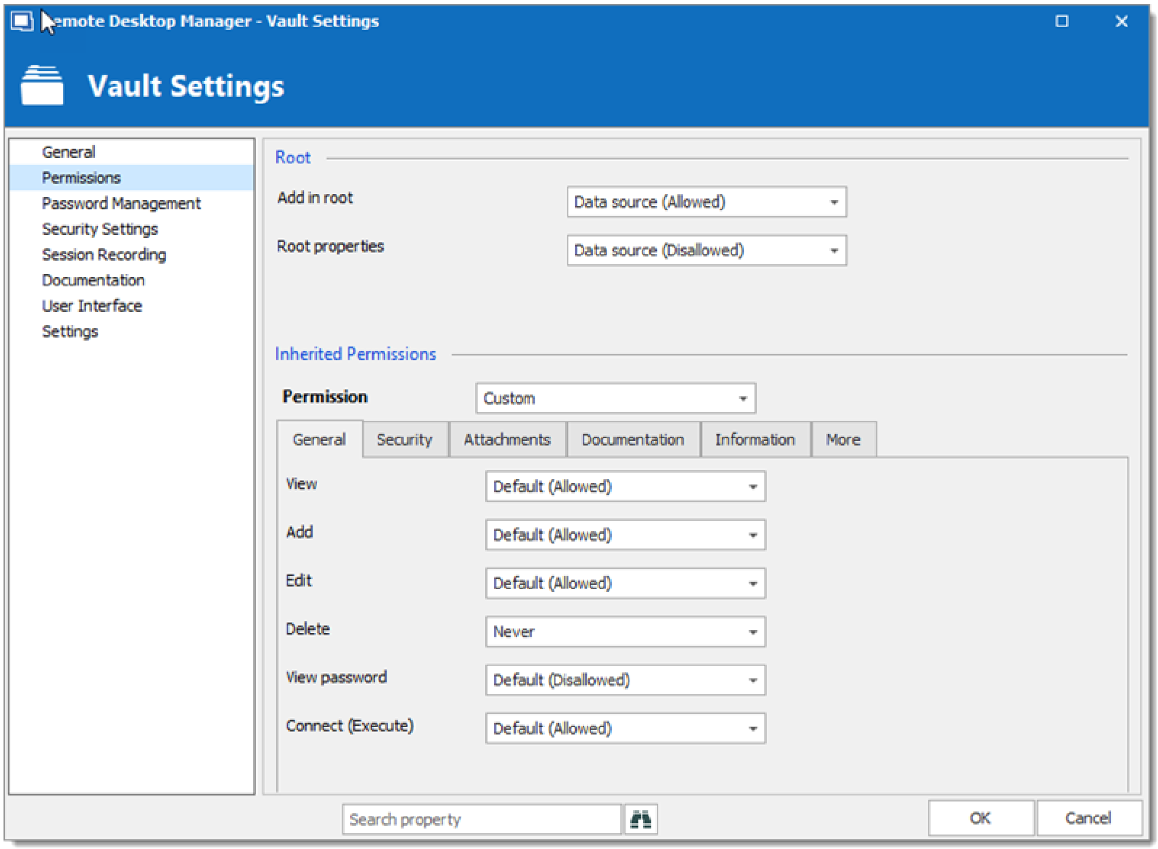
6.7.3.1 Vault Settings

6.7.3.1.1 Default security for entries

DESCRIPTION

In the Vault settings, navigate to the **Permissions** section. Under **Inherited Permissions**, change the **Permission** drop down list to the desired settings.

- **Custom** allows to select specific user groups/users for each permission below.
- **Never** denies any access to all users.



Vault – Permissions

To confirm the change, edit an entry below the Vault and navigate to the ***Security – Permissions*** section. All permissions set to ***Default*** inherit the value from Data Source Permissions (System Permissions) or the user. Inherited values are displayed next to the permissions.

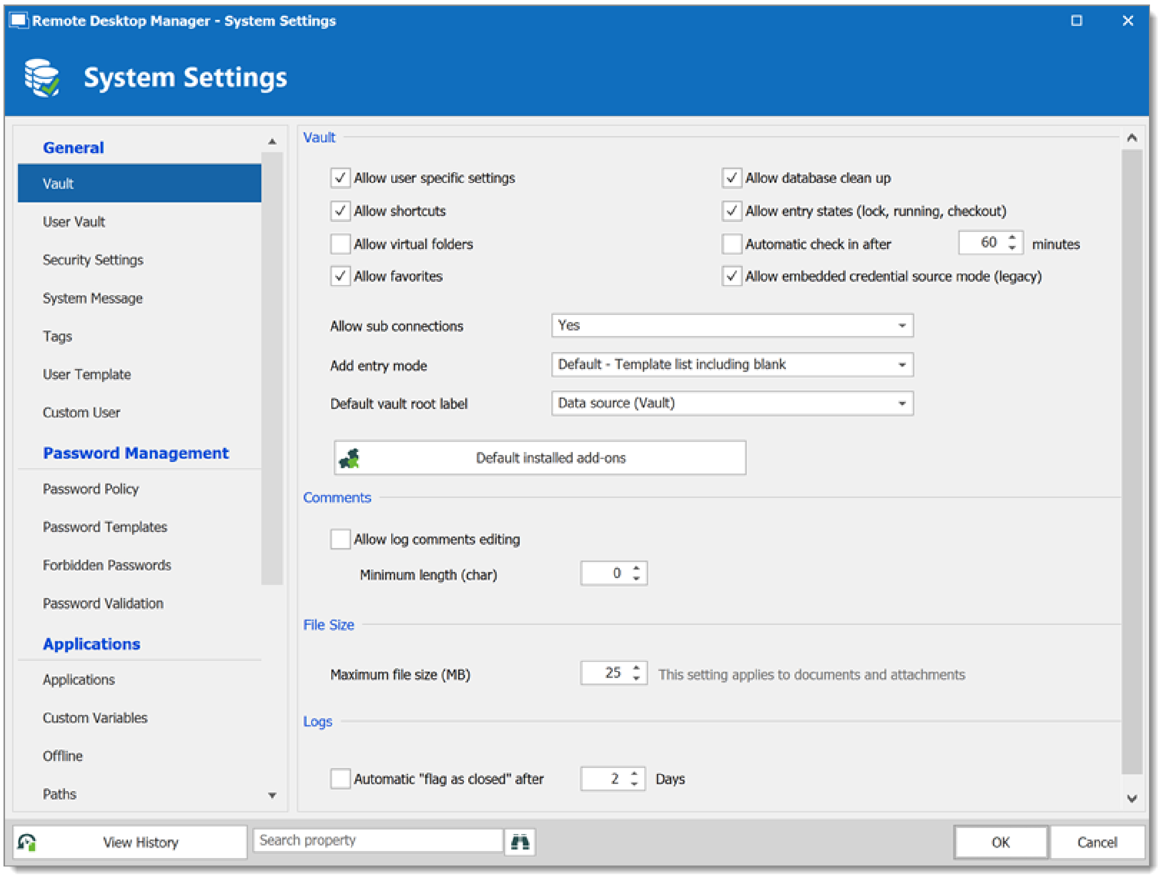
6.7.3.2 System Settings

6.7.3.2.1 General

GENERAL

The **General** section allows to manage the availability of different features related to the database.

These settings applies to all users that have access to the data source.



System Settings - General

GENERAL	DESCRIPTION
Allow user Specific Settings	Allow users to save User Specific Settings.
Allow database clean up	Allows logs and deleted history to be cleaned up. For more information, please consult the Clean up topic.
Allow shortcuts	Allow the reiteration of entries through the shortcut feature.

GENERAL	DESCRIPTION
Allow entry states (Lock, Running, Checkout)	Allow entries to be locked when used or edited.
Allow virtual folders	Allow to store entries in virtual folders. (Not supported with Devolutions Server.)
Automatic check in after	Forces checked out entries to check in automatically after a set delay.
Allow sub connections	Allow users to create sub connections.
Allow favorites	Allow users to favorite connections.
Allow embedded credential source mode (legacy)	Allow embedded Credential entry in the entry itself. This mode is deprecated and not recommended. Please review other Credentials options available.
Add entry mode	Select if users are prompted to choose a template when creating a new entry. Select between: • **Default** • **Template list (include default)** • **Template list only** • **No template selection**

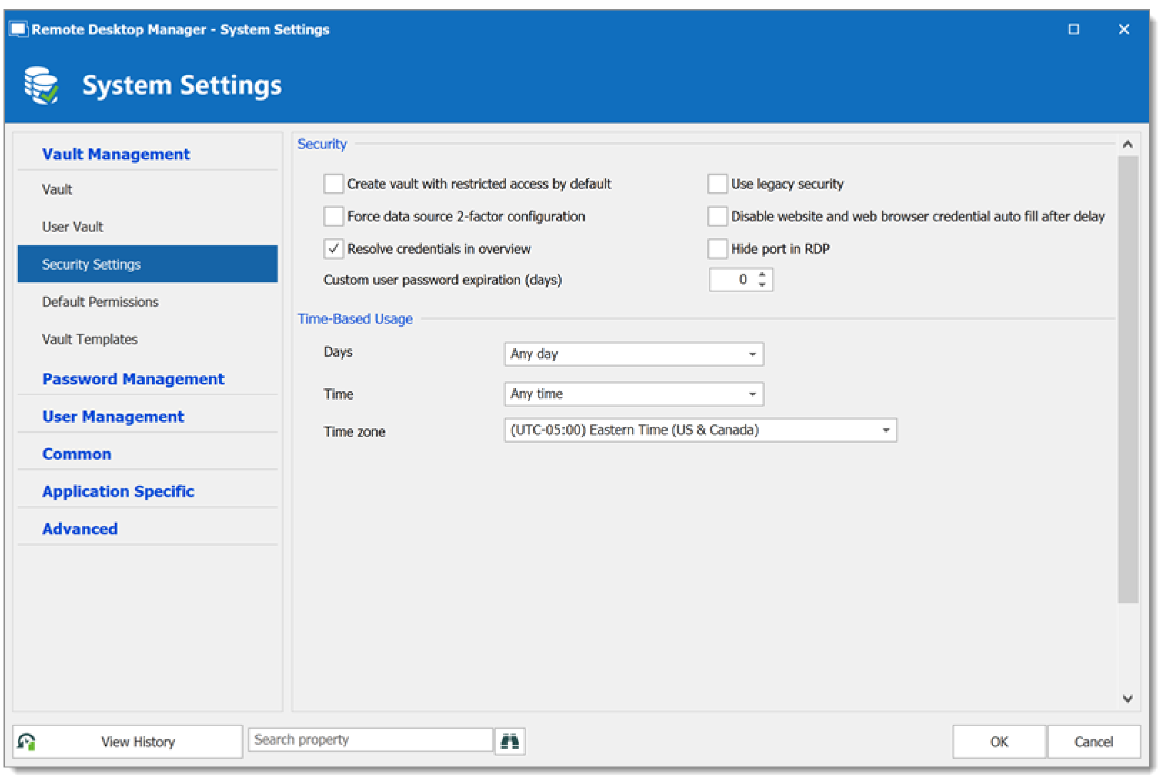
COMMENTS	DESCRIPTION
Allow log comments editing	Enable the log comment editing for all users.

COMMENTS	DESCRIPTION
Minimum length (char)	Set the minimum length (in characters) allowed for comments.

FILE SIZE	DESCRIPTION
Maximum file size (MB)	Limit the size of attachments and document entries to avoid to over load the data source.

6.7.3.2.1.1 Security

SETTINGS



DATA SOURCE SECURITY	DESCRIPTION
Create Vault with restricted access by default	Automatically secure the Vault settings when creating a repository. Therefore, the permissions settings are set to **Never**.
Force data source 2-factor configuration	Require the users to have a 2-factor configuration applied on the data source. Not shown with Devolutions Server as 2FA set elsewhere.
Resolve credentials in overview	Displays username and password fetched from a Credential repository in the entry overview in the dashboard. Uncheck this option if it takes too long to resolve.
Use legacy security	Use the old system of managing privileges: Security groups (deprecated). • To manage your users permissions, we recommend you switch from Security groups (deprecated) to ***Permissions***. Once the migration done, disable the legacy security, by unchecking ***Use legacy security***.

TIME-BASED USAGE	DESCRIPTION
Time of day	Select the hours which the data source is limited to. Select between: • **Any time**: the session can be used at any hour. • **Custom**: manually select the time frame the session is available for.
Time of week	Select which days the data source is available for. Select between:

TIME-BASED USAGE	DESCRIPTION
	• **Any day**: the session can be used any day of the week or week-end. • **Week days**: the session can be used only the week days. • **Week ends**: the session can be used only the week ends. • **Custom**: manually select each day the session is available for.
Time Zone	Select the time zone you are currently in.

6.7.3.2.1.2 Allow Password Access From External System

DESCRIPTION

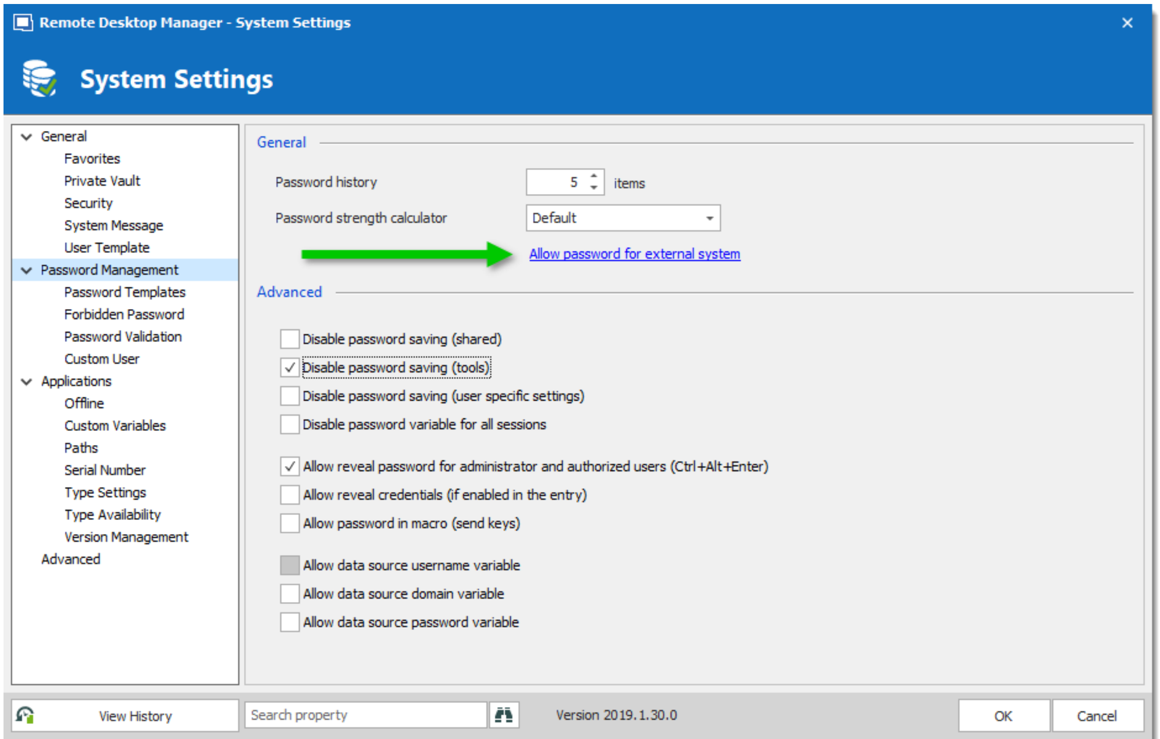
This feature is only available when using an Advanced Data Source.

Accessing passwords stored in your data source by querying the underlying database is not possible because of the encryption we apply on the passwords. For those of you that need to access passwords directly in the database, for example by a CRM system, we have created a way to achieve this.

SETTINGS

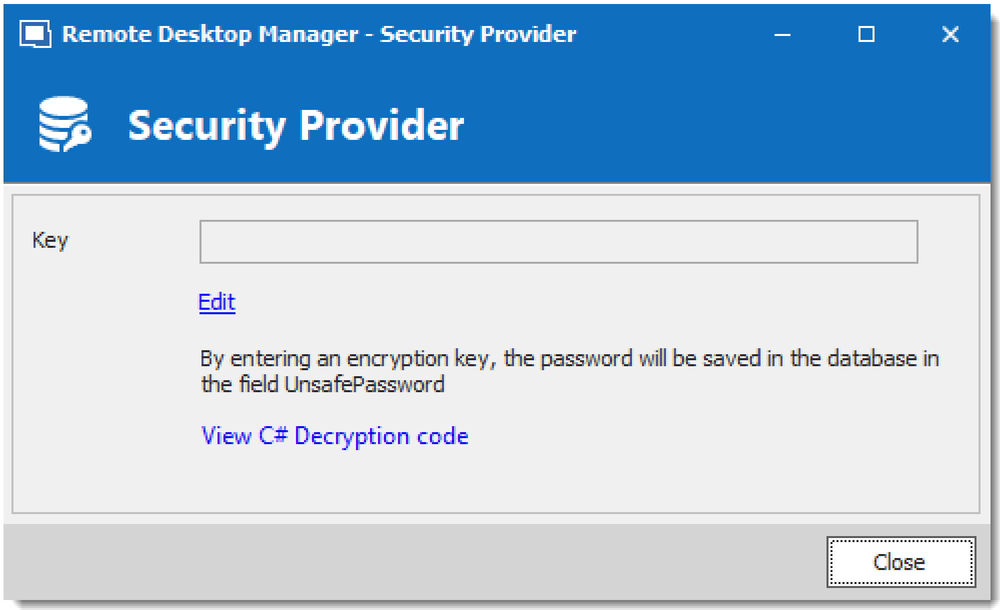
The session information, which is an XML structure, is stored in the **Data** field of the **Connections** table in the underlying database.

However, getting the encrypted password from the database requires the **Allow password for external system** to be configured.



Password Policy - Allow Password For External System

Enter an encryption key in the **Key** field. Once a key is provided it will cause the system to extract a copy of the password from our XML structure, this will then be re-encrypted using the **key** you have provided and stored back into the **UnsafePassword** field of the **Connections** table.



Security Provider

DECRYPTION CODE

Use the following .net code to decrypt your passwords.

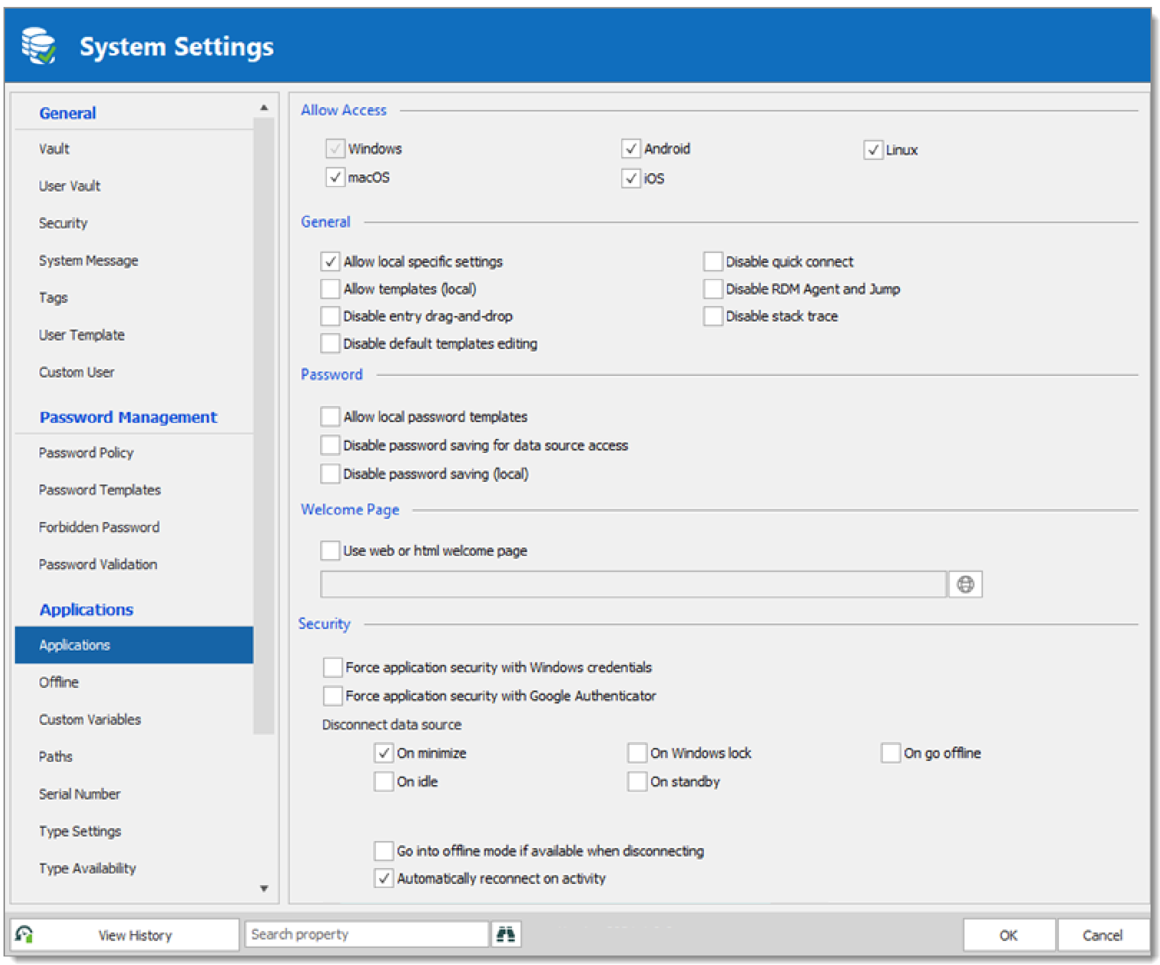
```
public static string Decrypt(string encryptedString, string key)
{
  if (string.IsNullOrEmpty(encryptedString))
  {
    return encryptedString;
  }

  try
  {
    TripleDESCryptoServiceProvider tripleDesCryptoServiceProvider = new TripleDESC
    MD5CryptoServiceProvider cryptoServiceProvider = new MD5CryptoServiceProvider(

    string strTempKey = key;

    byte[] byteHash = cryptoServiceProvider.ComputeHash(Encoding.ASCII.GetBytes(st

    tripleDesCryptoServiceProvider.Key = byteHash;

    tripleDesCryptoServiceProvider.Mode = CipherMode.ECB;

    byte[] byteBuff = Convert.FromBase64String(encryptedString);

    string strDecrypted =
      Encoding.UTF8.GetString(
        tripleDesCryptoServiceProvider.CreateDecryptor().TransformFinalBlock(
          byteBuff, 0, byteBuff.Length));

    return strDecrypted;
```

```
        }
        catch (Exception)
        {
            return null;
        }
    }
```

6.7.3.2.2 Application

DESCRIPTION

The **Applications** section manages the availability of different features related to Remote Desktop Manager application.



ALLOW ACCESS	DESCRIPTION
Operating systems	Enable access to the data source from the selected operating systems.

GENERAL	DESCRIPTION
Allow local Specific Settings	Allow users to save Local Specific Settings.
Allow templates (local)	Allows to locally save entry's templates.
Disable entry drag-and-drop	Disable entries drag and drop from one folder to another. This setting is useful for avoiding accidental drag and drop.
Disable quick connect	Disable the Quick Connect feature for all users of the data source.
Disable RDM Agent and Jump	Disable the option to activate a session as an RDM Agent or Jump.
Disable stack trace	Disable the stack trace details when an error occurs in Remote Desktop Manager. This is a security feature.

PASSWORD	DESCRIPTION
Allow local password templates	Allows password templates to be saved locally.
Disable password saving for data source access	Prevent users to save or change the passwords stored in the data source configurations.

PASSWORD	DESCRIPTION
Disable password saving (local)	Prevent users from saving passwords in the properties of entries.

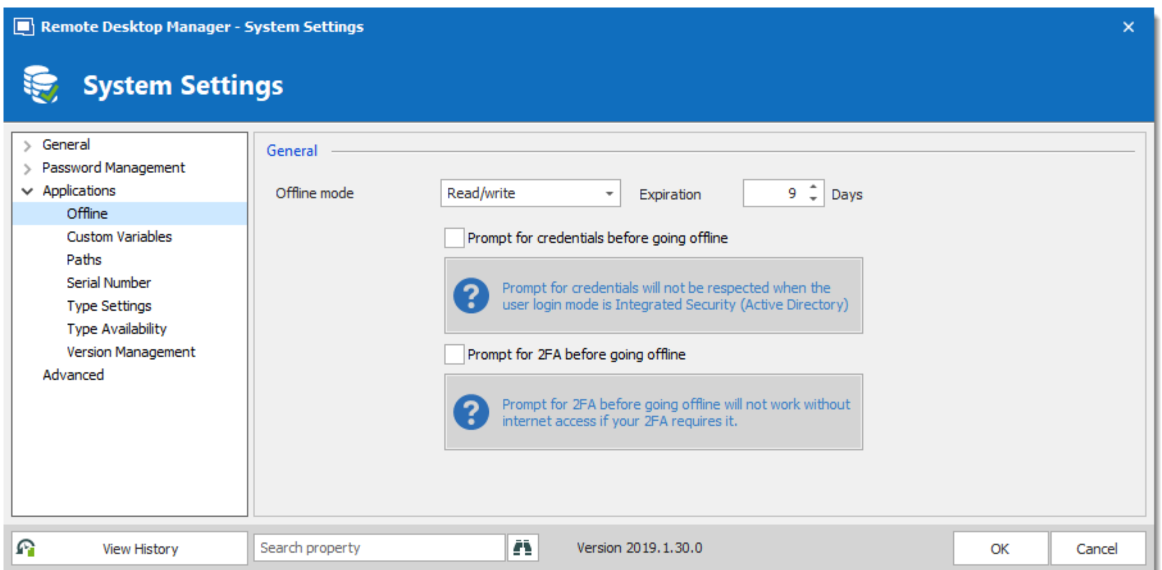
WELCOME PAGE	DESCRIPTION
Use web or html welcome page	Enter an URL to use as the application's welcome page.

SECURITY	DESCRIPTION
Force application security with Windows credentials	Require the users to authenticate with their Windows credentials at application startup.
Force application security with Google Authenticator	Require the users to authenticate with Google Authenticator at application startup.
Disconnect data source	Set the application to lock: • **On Minimize:** lock application when minimized in the taskbar for all users of the data source. • **On Idle:** automatically lock the application when it is not used after a determined amount of time. • **On Windows lock:** lock the application on Windows lock. • **On standby:** lock the application when on standby.
Go into offline mode if available when disconnecting	Will switch RDM from online to offline mode if available when disconnecting.

SECURITY	DESCRIPTION
Automatically reconnect on activity	Instead of using the manual refresh button, after an idle time, activate the option to reconnect automatically.

6.7.3.2.2.1 Offline

DESCRIPTION



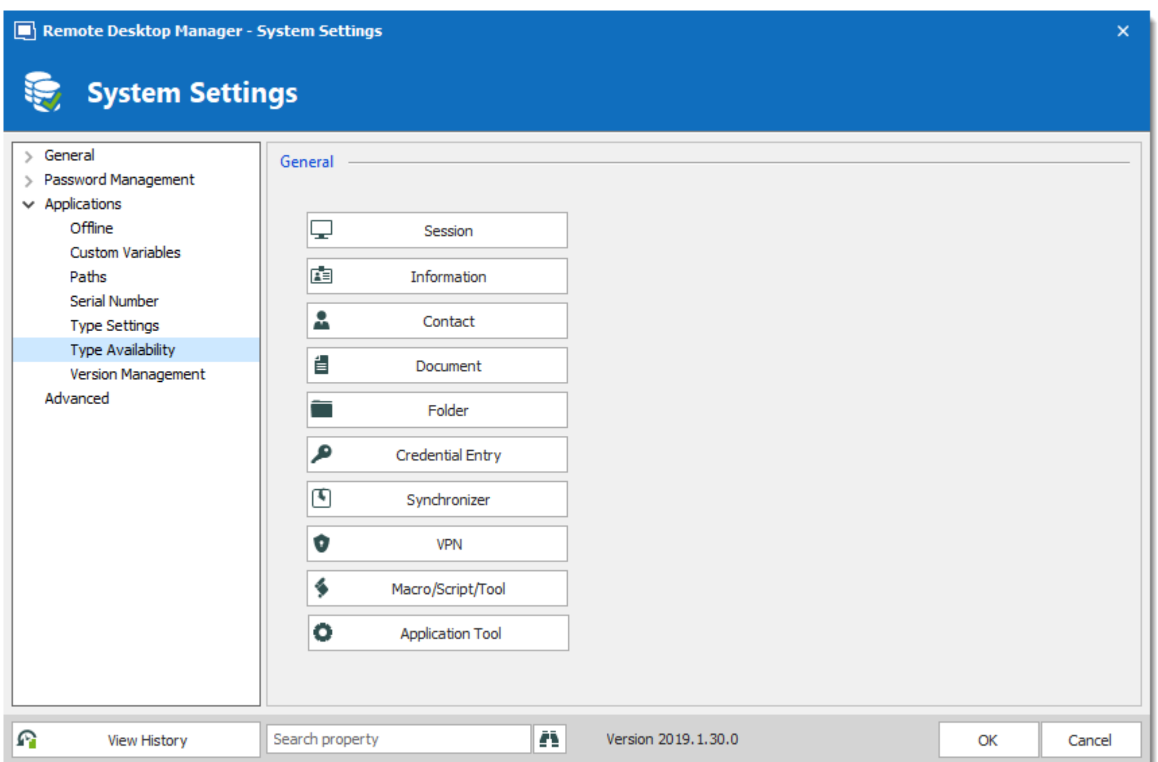
OPTION	DESCRIPTION
Offline mode	Set the global data source Offline Mode availability. The offline mode is useful when using a VPN connection that makes using local network impossible.
Expiration	Number of days before the offline cache expires. You must go online prior to the end of that period to re-validate the data.

OPTION	DESCRIPTION
Prompt for credentials before going offline	Force the user to provide their credentials before going offline.
Prompt for 2FA before going offline	Force the user to provide their 2FA before going offline.

It is not recommended to set the **Expiration** to 0, as this will disable the expiration of the offline cache.

6.7.3.2.2.2 Type availability

SETTINGS



System Settings - Types - Availability

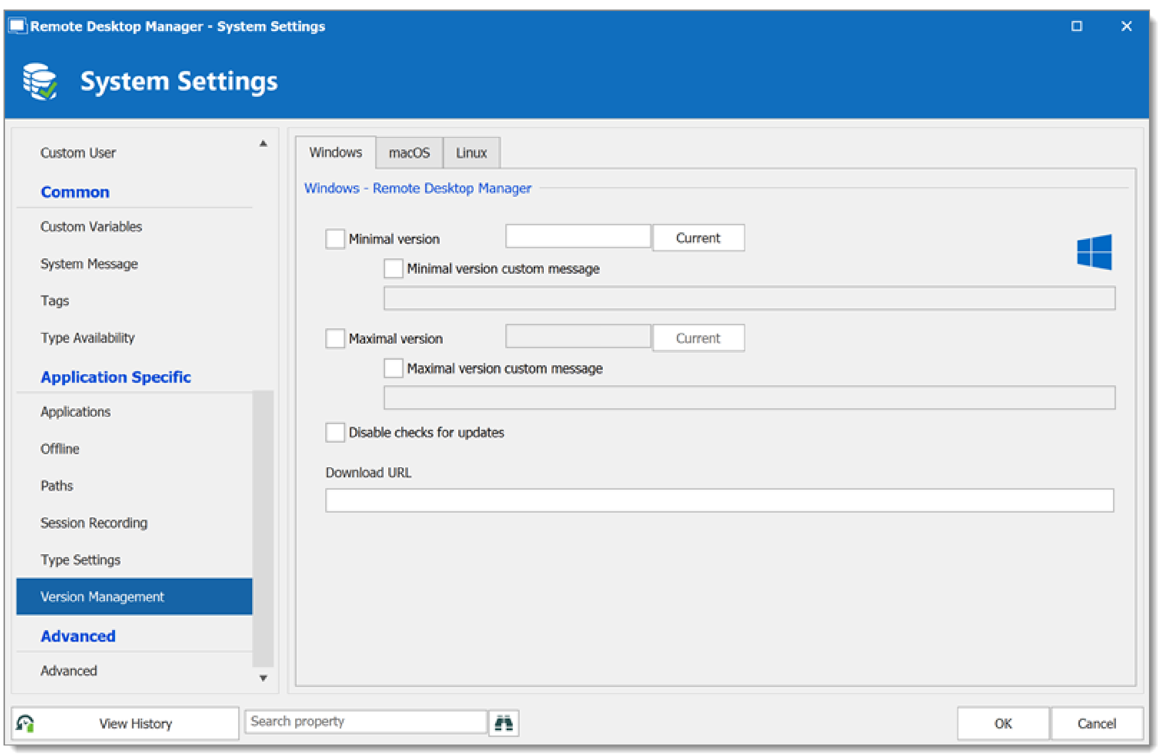
OPTION	DESCRIPTION
Type Availability	Select entry types to exclude. Excluded entries will not be in the **Add New Entry** window.

6.7.3.2.2.3 Version Management

DESCRIPTION

The **Version Management** allows the administrators to manage the data source availability in other versions of Remote Desktop Manager.

WINDOWS AND MACOS



Version Management

OPTION	DESCRIPTION
Minimal version	Forces users of the data source to use a minimal version of Remote Desktop Manager. Enter the entire version number (2019.1.0.0) to force a specific version. Use this to disable connecting to the data source with an older version.
Minimal version custom message	Enter a custom message for the minimal version notification.
Maximal version	Forces users of the data source to use a maximal version. Enter the entire version number (2019.1.0.0) to force a specific version. Use this to disable connecting to the data source with a newer version.
Maximal version custom message	Enter a custom message for the maximal version notification.
Disable checks for updates	Disable the auto update notification message. Use this to manually update the application and prevent from getting notified when new versions are available.
Download URL	Use in conjunction with the minimal or maximal version, once a minimal or maximal version requirement is not met the system will prompt the user that the version is no longer valid and it will open the link (path/URL) to download the newer or older version.

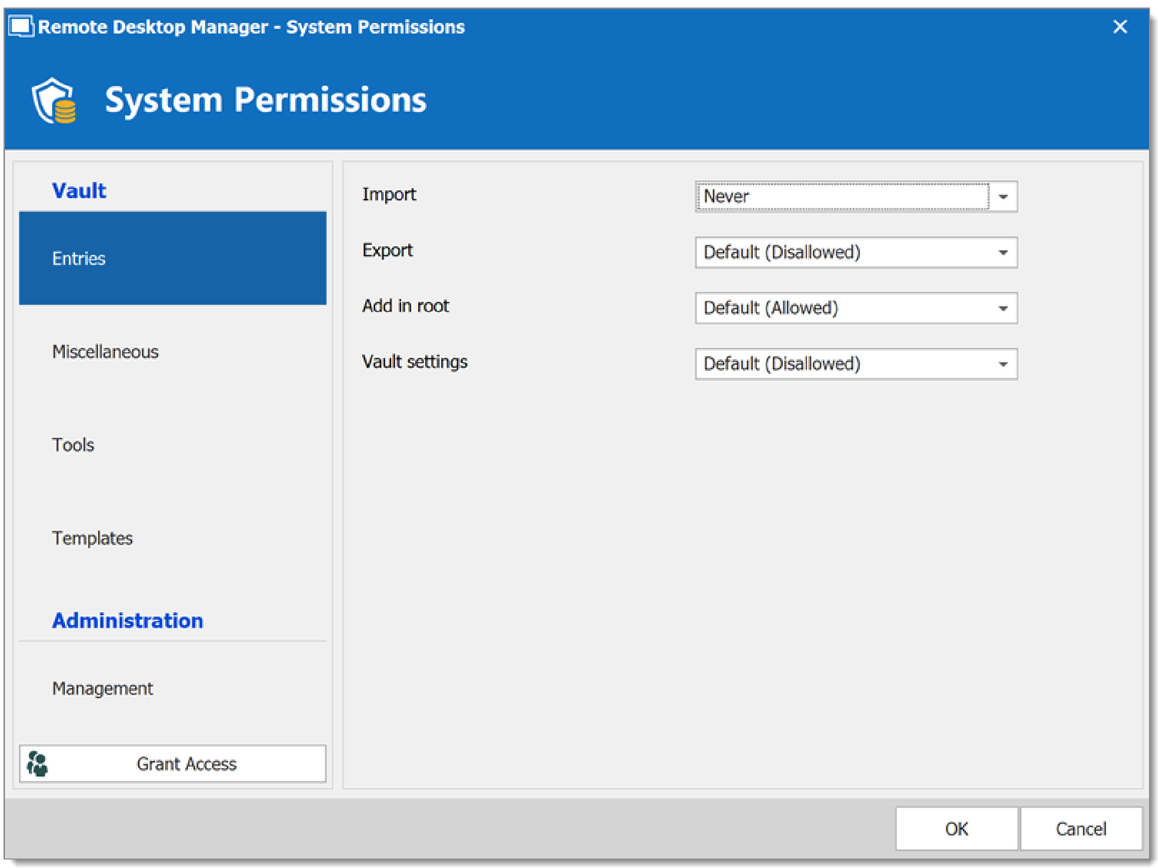
6.7.3.3 System Permissions

DESCRIPTION

The **System Permissions** allows to grant some administrative permissions to standard users without making them administrators. The **Default** setting inherits the permission set on the user or user groups. For more information about permissions, consult General Security.

This feature is only available when using an Advanced Data Source.

ENTRIES

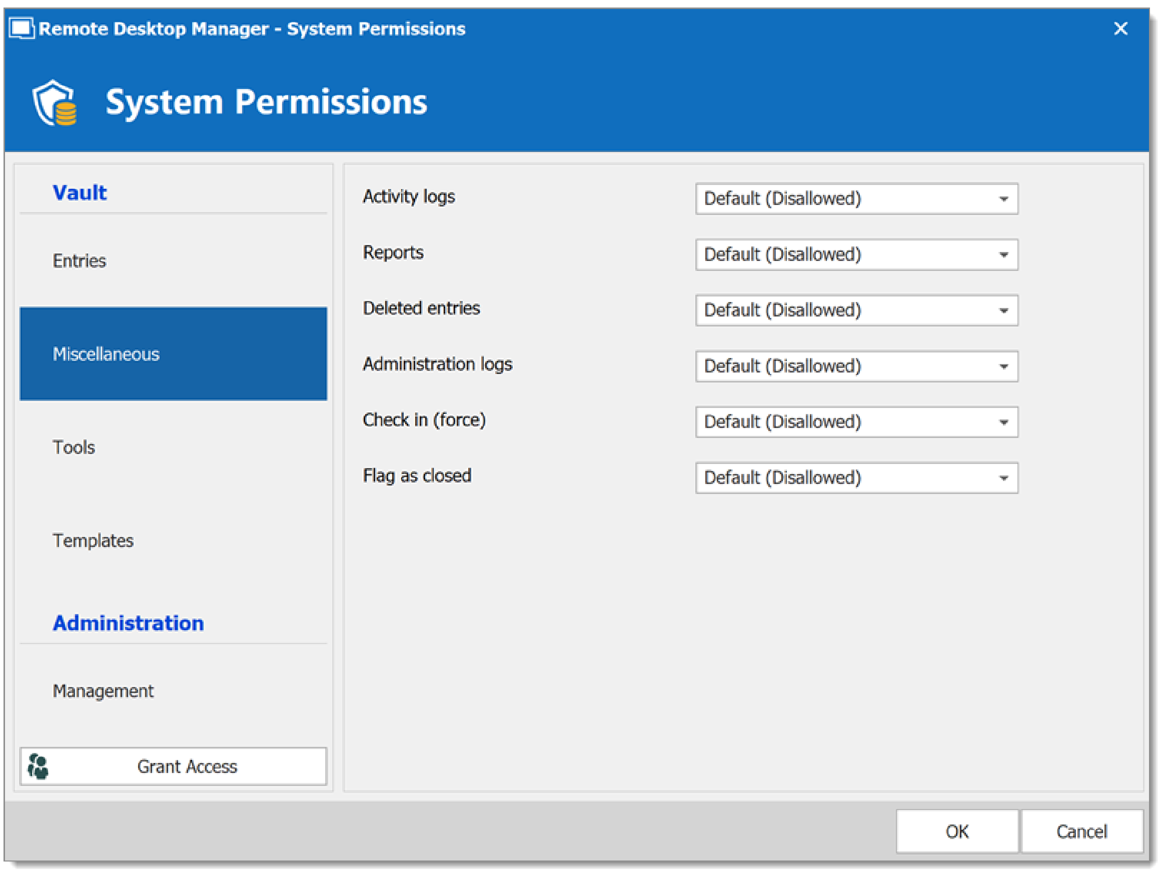


System Permissions - Entries

OPTION	DESCRIPTION
Import	Allow users/user groups to import entries in the data source.

OPTION	DESCRIPTION
Export	Allow users/user groups to export from the data source.
Add in root	Allow users/user groups to create entries in the root folder.
Vault settings	Allow users/user groups to access the Vault properties.

MISCELLANEOUS

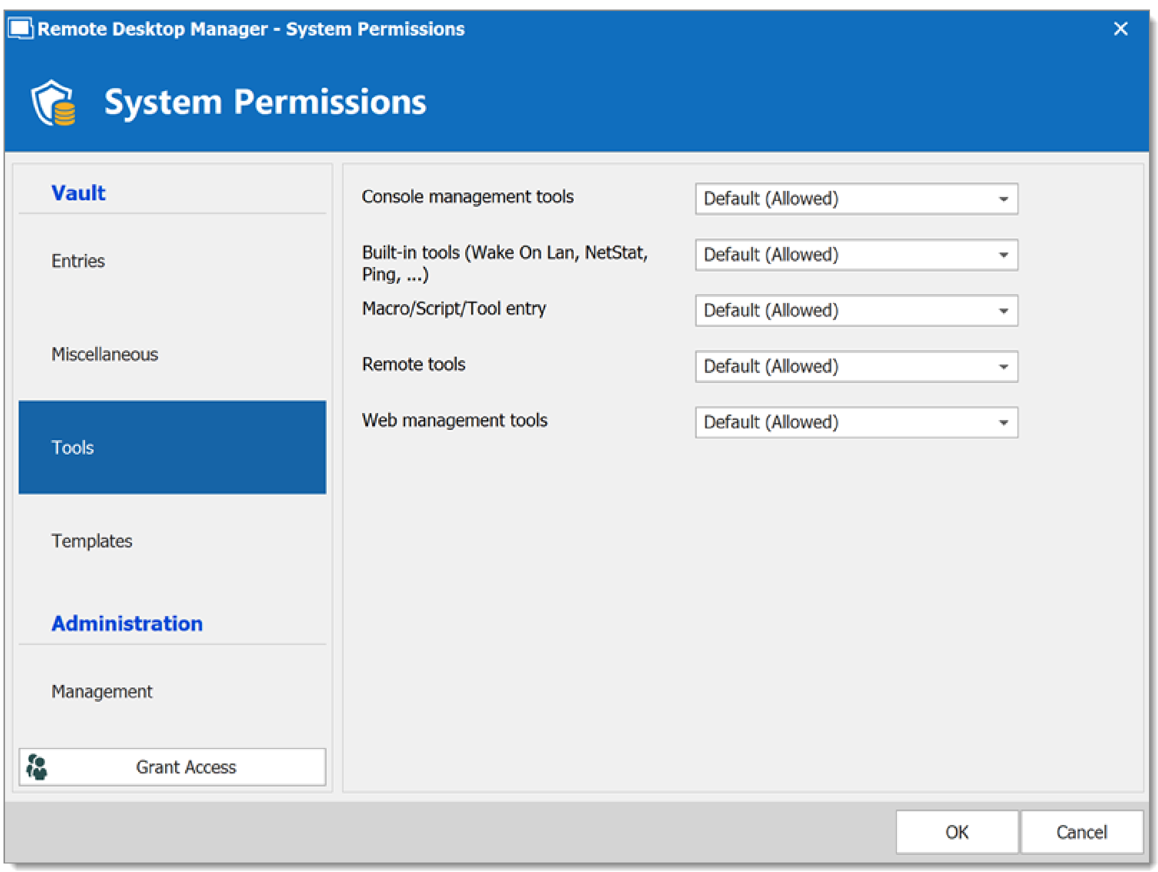


System Permissions - Miscellaneous

OPTION	DESCRIPTION
Activity logs	Allow users/user groups to view the activity logs.

OPTION	DESCRIPTION
Reports	Allow users/user groups to generate and view reports.
View deleted entries	Allow users/user groups to view and restore deleted entries.
View administration logs	Allow users/user groups to view the administration logs.
Check in (force)	Allow users/user groups to check in entries with the checked out state.

TOOLS

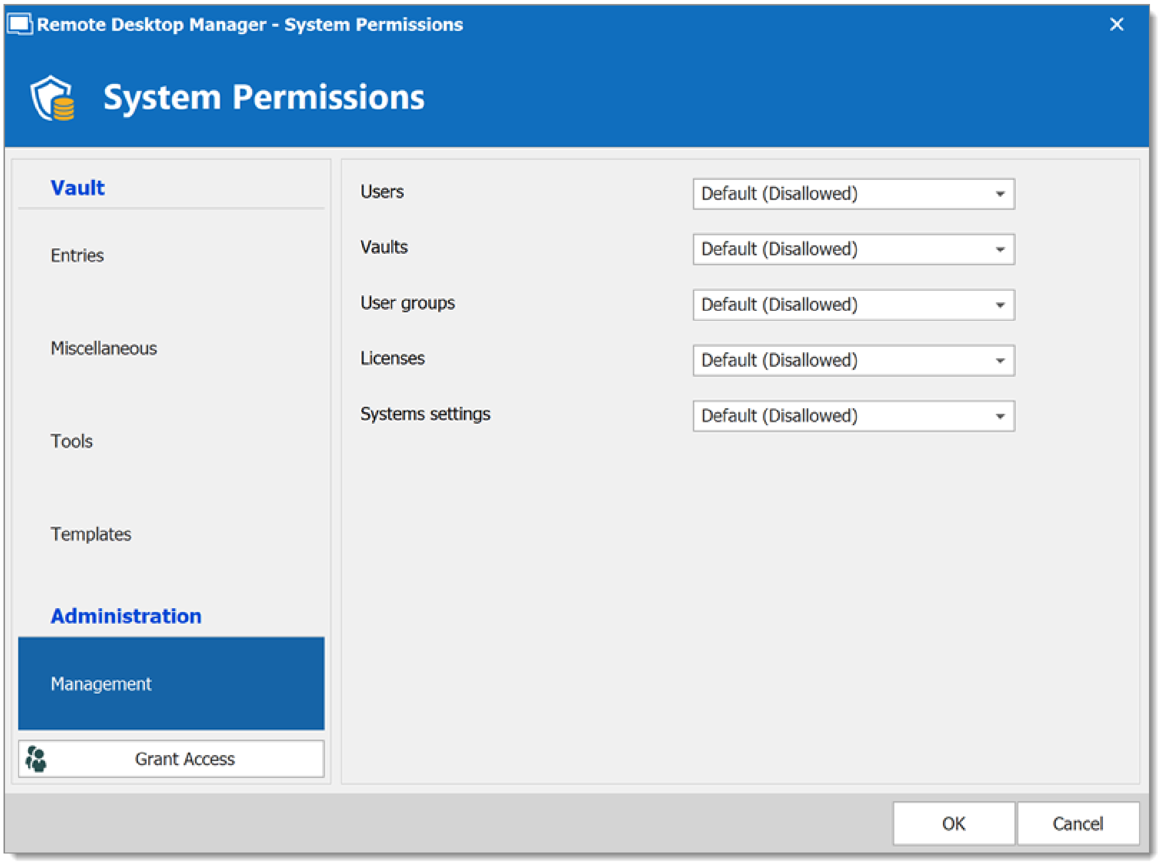


System Permissions - Tools

OPTION	DESCRIPTION
Console management tools	Allow users/user groups to use console management tools.
Buit-in tools (Wake-on-LAN, NetStat, Ping, ...)	Allow users/user groups to use session related tools.
Macros/Scripts/Tools entry	Allow users/user groups to use Macros/Scripts/Tools entries.
Management Tools	Allow users/user groups to use Management Tools.
Web management tools	Allow users/user groups to use web management tools.

MANAGEMENT

The **Default** value in **Tools** is equivalent to **Never**.



System Permissions - Management

OPTION	DESCRIPTION
User	Allow users/user groups to access the user management.
Security Group	Allow users/user groups to access the security groups management.
User Groups	Allow users/user groups to access the user groups management.
Vault	Allow users/user groups to manage Vaults.
Data source settings (System Settings)	Allow users/user groups to access data source settings.

OPTION	DESCRIPTION
Template	Allow users/user groups to create and manage templates.
Password template	Allow users/user groups to create and manage password templates.

6.7.3.4 Security Providers

DESCRIPTION

The **Security Provider** allows for encrypting the data source content. To access the security provider, navigate to ***Administration – Security Provider***.

This feature requires an Advanced Data Source.

Regardless of the selected security provider, passwords stored in data sources are **ALWAYS** encrypted using AES 256 bit encryption.

When configuring a Certificate Security Provider in a published app environment (Citrix, RemoteApp, XenApp) as a Security Provider, the user who will run Remote Desktop Manager in the RemoteApp environment (Citrix) will require a ***Read permission*** on the certificate.

If the ***Read permission*** isn't correctly set, Remote Desktop Manager will generate the CryptographicException - Keyset does not exist error dialog. Follow the Certificate Security Provider in a Published app Environment topic to resolve the issue.

By using a security provider, you ensure that nobody can read entries configuration data, even when people have a direct access to the database(s) or a backup. Shared data sources should always be secured with a security provider.

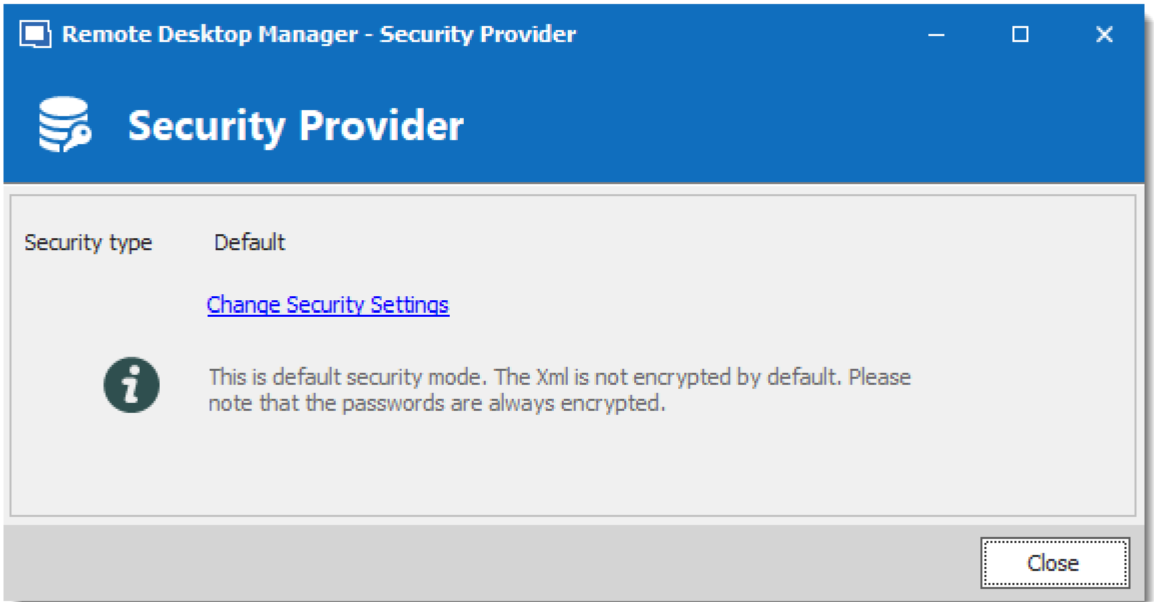
Prior to applying a new or changing an existing security provider, make sure that every users are disconnected from the data source. If you are changing an existing Shared Passphrase or Certificate, please note that users will get back access to the data source when they the new Shared Passphrase or Certificate on their computer.

SETTINGS

Please note that changing a security provider on a data source with a great number of entries is a lengthy operation.

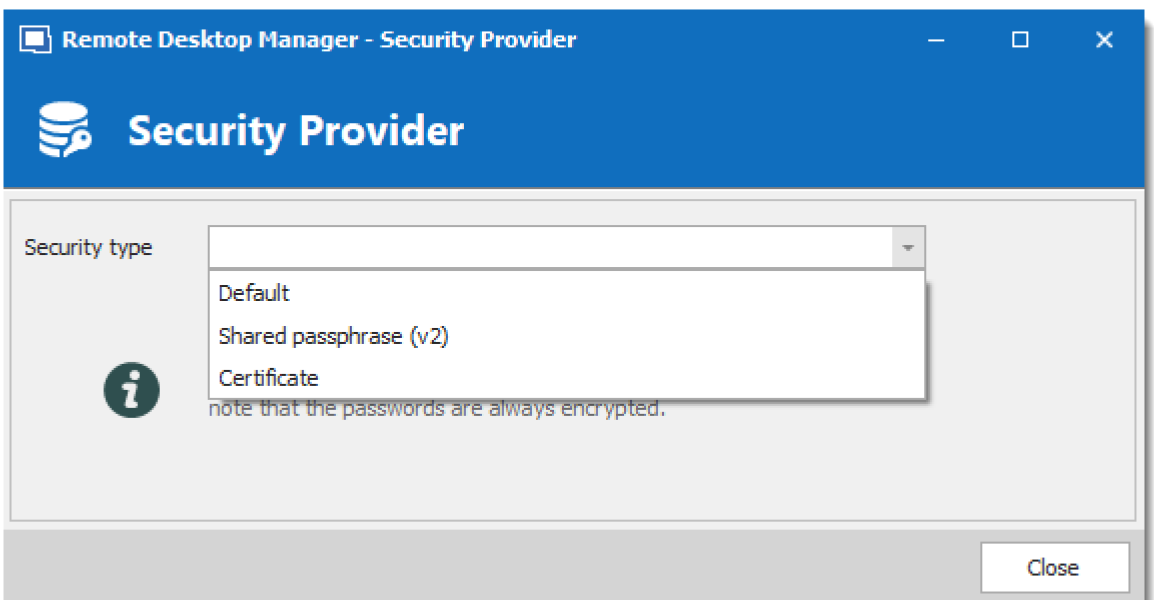
Applying a new security provider does process the whole database, therefore we advise you to create a backup prior to this operation.

1. Click on **Change Security Settings** to change the security provider.



Security Provider

2. Select a security type from the drop down list.



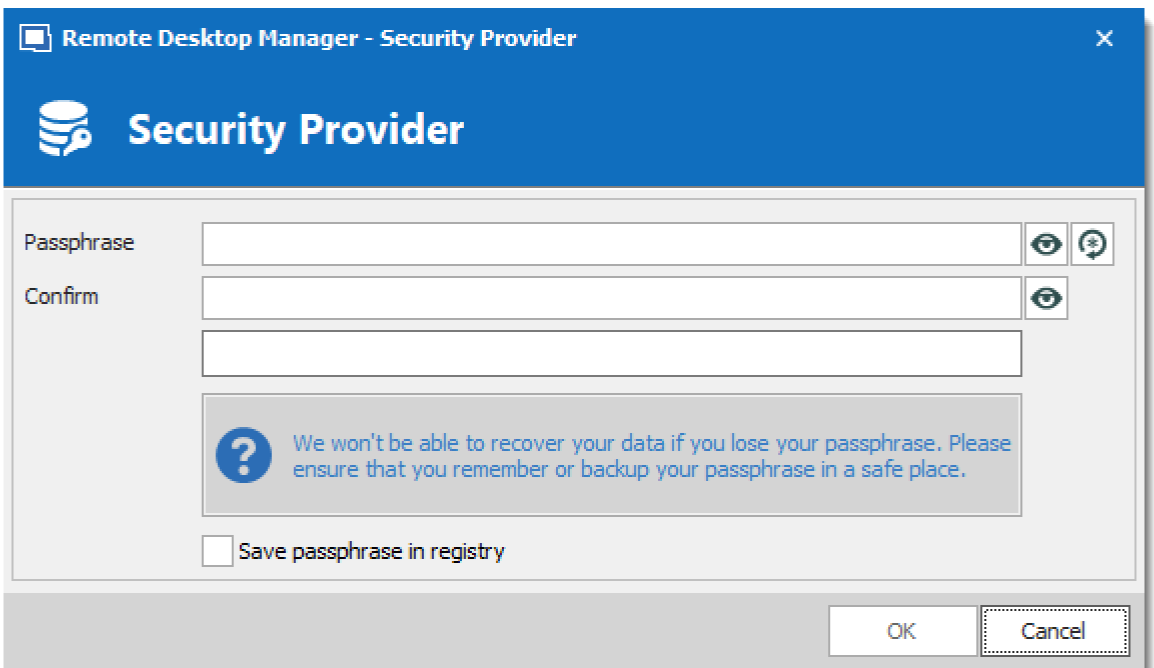
Security Type

OPTION	DESCRIPTION
Default	This is the legacy security provider. The data is encrypted if the entry configuration is set accordingly in the advanced settings of the entries.

OPTION	DESCRIPTION
Shared passphrase	Set up a shared passphrase for the Security Provider.
Certificate	Set up a Certificate for the Security Provider.

SHARED PASSPHRASE

If the passphrase is lost, **nothing** that can be done to recover the data. When using a passphrase, always copy it to a secure location.



Security Provider - Shared Passphrase

Entries configuration data is encrypted using a mix of a key stored in Remote Desktop Manager and the passphrase you've entered.

The passphrase is required only when configuring the data source. A policy can be enabled to always prompt for the passphrase when connecting to the data source.

When configuring a security provider with a shared passphrase, you have the choice of whether or not you wish to save it in the registry. Remote Desktop Manager will try first to save it on the LOCAL_MACHINE, if unable it will save it in the CURRENT_USER instead.

- HKEY_CURRENT_USER\SOFTWARE\RemoteDesktopManager<Datasource ID>.shk
- HKEY_LOCAL_MACHINE\SOFTWARE\RemoteDesktopManager<Datasource ID>.shk

If the option is not enabled, then the passphrase is saved locally at the following location:

- %LOCALAPPDATA%\Devolutions\RemoteDesktopManager<Datasource ID>.shk

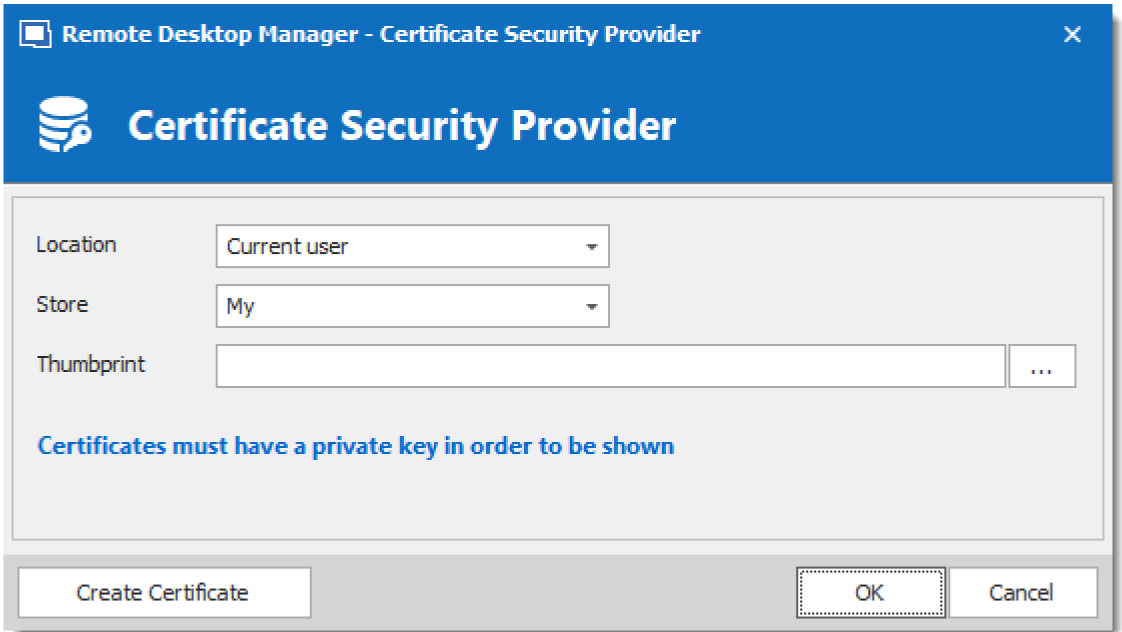
In a Terminal Services environment, it should be saved at this location:

- %APPDATA%\Devolutions\RemoteDesktopManager<Datasource ID>.shk

In a portable installation of RDM, the passphrase will be saved at the same location as the portable Remote Desktop Manager instance.

CERTIFICATE

When choosing **Certificate** as Security Provider, entries configuration data is encrypted using a mix of a key stored in Remote Desktop Manager and the private key contained in the certificate.



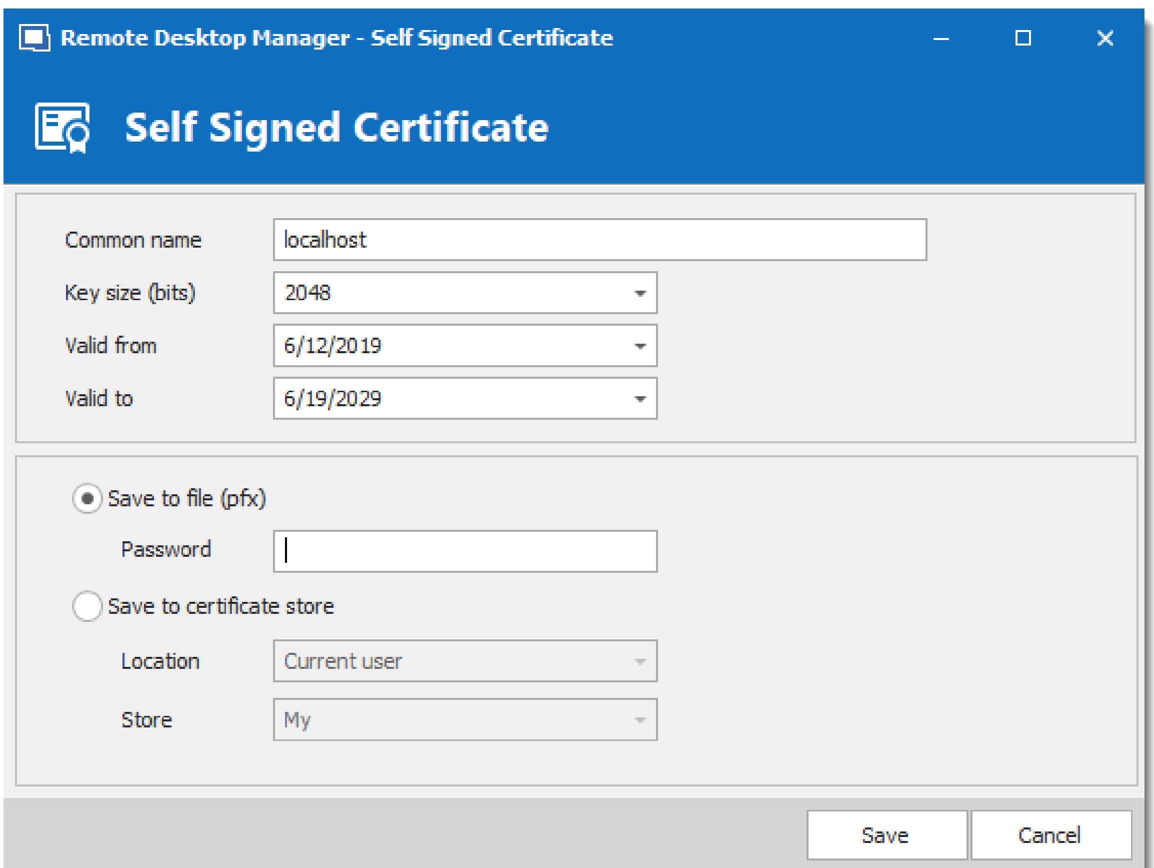
Security Provider - Certificate

OPTION	DESCRIPTION
Location	Indicate the certificate location. Select between: • **Current user** • **Local machine**
Store	Indicate the store location of the certificate. Select between: • **Address book** • **Authorization root** • **Certificate authority** • **Disallowed** • **My** • **Root** • **Trusted people**

OPTION	DESCRIPTION
	• **Trusted publisher**
Thumbprint	Select an existing RSA certificate.

CREATE CERTIFICATE

It is possible to create a Self Signed certificate by clicking on **Create Certificate**.



Self Signed Certificate

OPTION	DESCRIPTION
Common	Name of the certificate.

OPTION	DESCRIPTION
name	
Key size (bits)	Indicate the key size (bits) of the certificate. Select between: • **384** • **512** • **1024** • **2048** • **4096** • **8192** • **16384**
Valid from	Start date of the certificate.
Valid to	End date of the certificate.
Save to file (pfx)	Save the certificate as a pfx file and secure this certificate with a password.
Save to certificate store	Indicate the location and the store to save the certificate.

6.7.4 Clean up

6.7.4.1 Clean Up Deleted History

DESCRIPTION

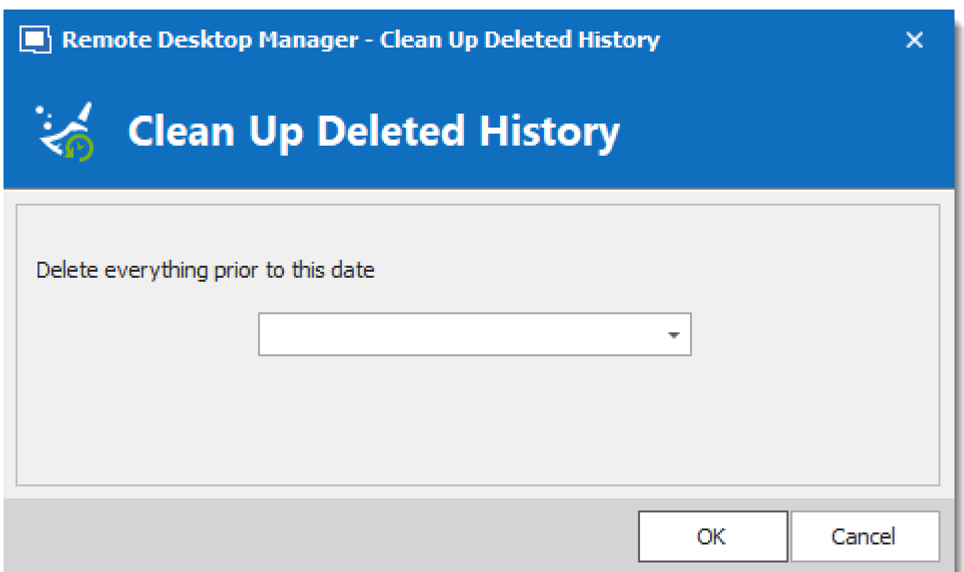
The **Deleted History** permanently delete entries that had been previously deleted. Full history is always preserved because every entry "version" is kept in historical tables.

This feature requires an Advanced Data Source.

You must be an administrator of the data source to perform this action.

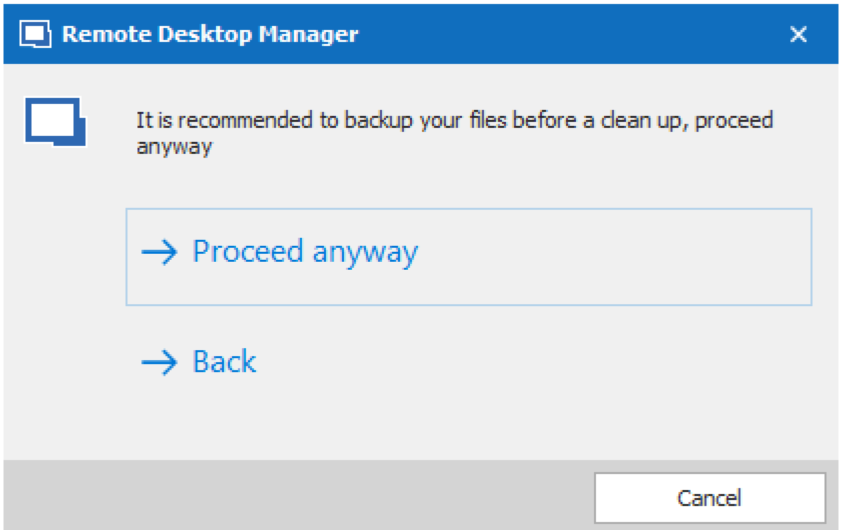
SETTINGS

1. Select prior to which date you wish to permanently delete your deleted entries.



Clean up Deleted History

2. Confirm your choice prior to permanently delete your deleted entries.



Confirmation window

There will be no backup of your History. We strongly recommend to do a Backup before proceeding.

6.7.4.2 Clean Up Entry History

DESCRIPTION

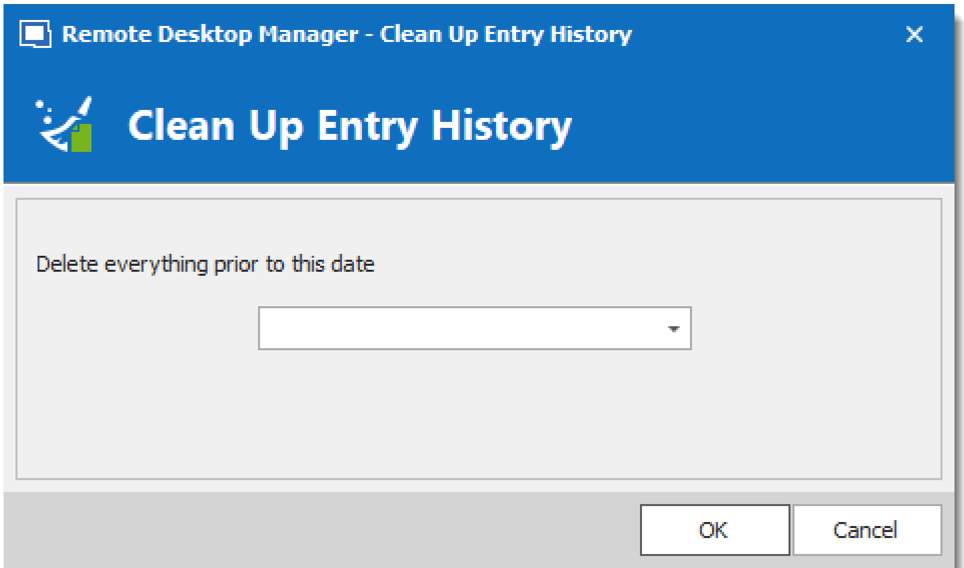
The **Entry History** deletes the history attached to your entry, you can find the history by right clicking on your entry and selecting ***View – Entry history***.

This feature requires an Advanced Data Source.

You must be an administrator of the data source to perform this action.

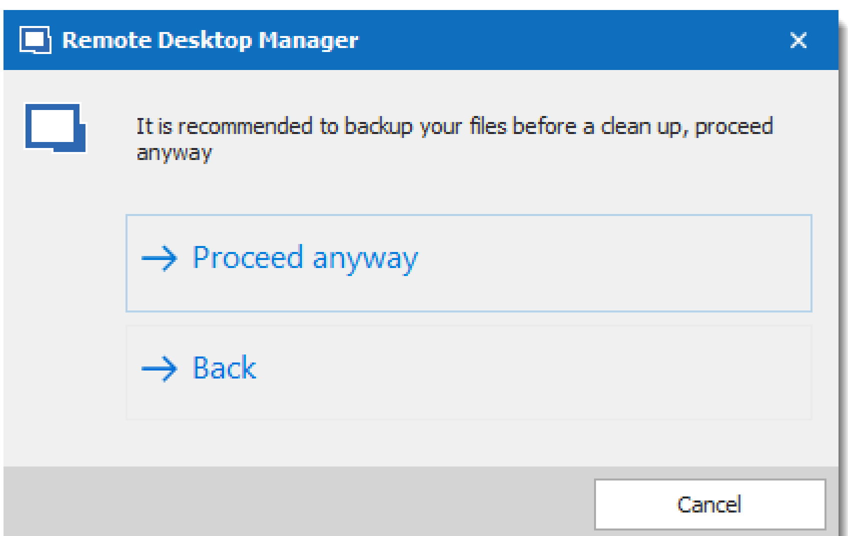
SETTINGS

1. Select prior to which date you wish to permanently delete your Clean up entry history.



Clean up Entry History

2. Another window will appear to confirm your choice of deleting all the history prior to the chosen date.



Confirmation window

No History backup is created. We strongly recommend to do a Backup before proceeding.

6.7.4.3 Clean Up Activity Logs

DESCRIPTION

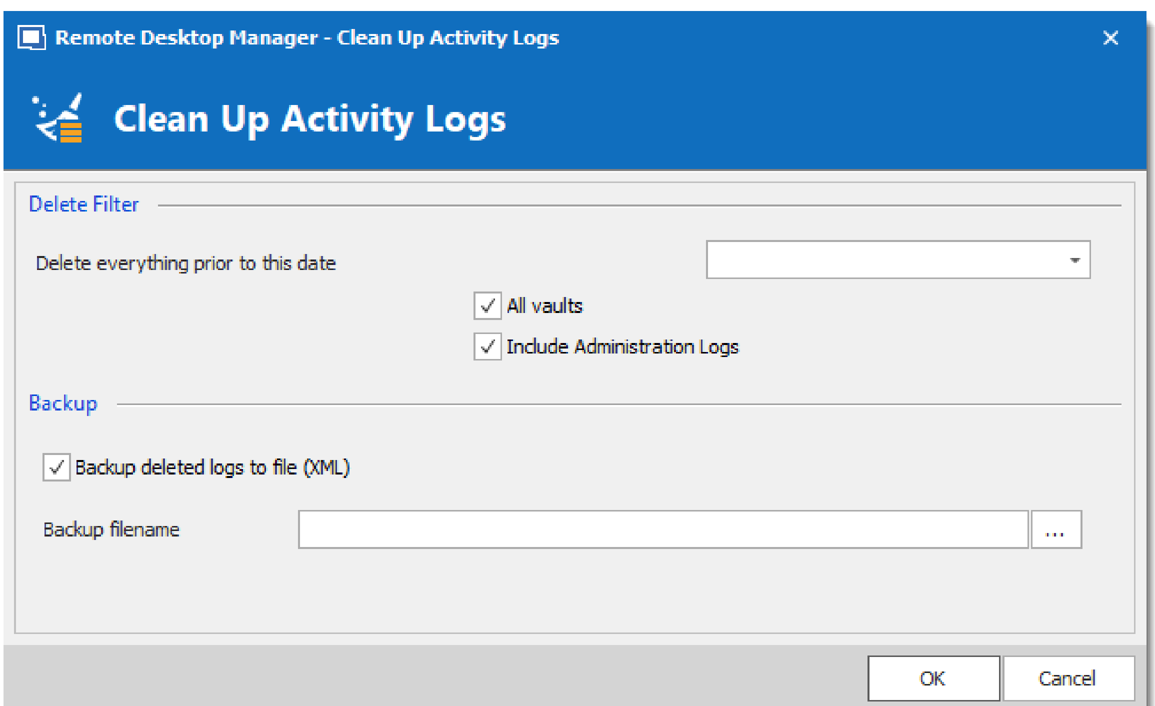
The **Clean Up Activity Logs** will delete your data source's Activity Logs, you also have the option to clean up the **Administration logs** and set up a back up if desired..

This feature requires an Advanced Data Source.

You must be an administrator of the data source to perform this action.

SETTINGS

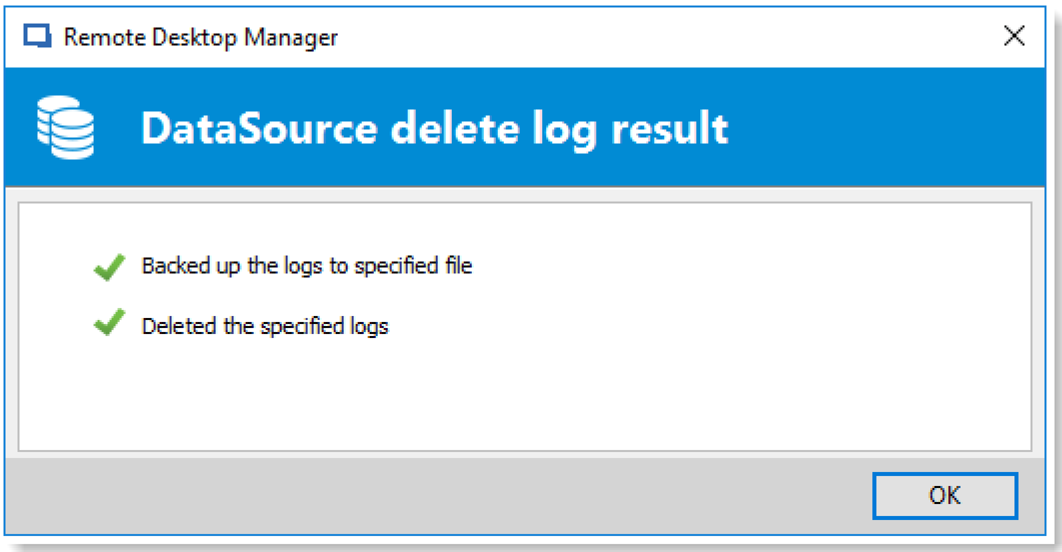
1. You must confirm your choice prior to permanently deleting your data source logs.



Clean up Data Source logs

A backup of your log will be created as an XML file although it will then be impossible to import this file in Remote Desktop Manager.

2. Once you have entered your Backup file name and proceeded with the clean up a delete log result window will appear.



Data Source Delete log result

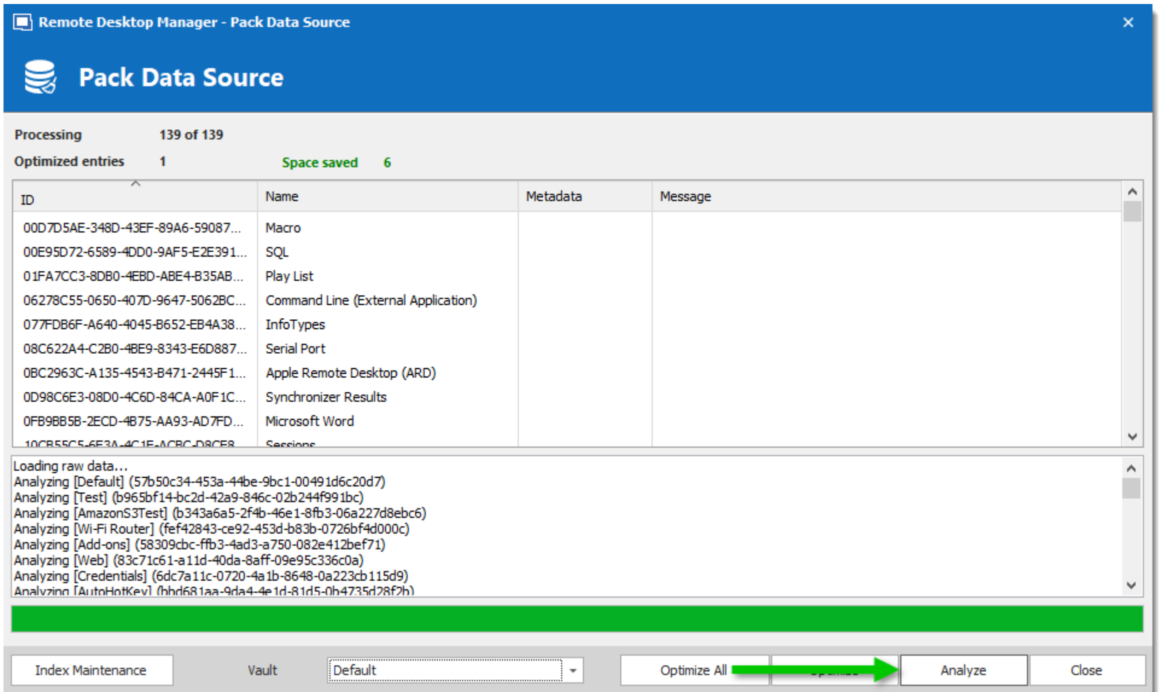
6.7.4.4 Pack Data Source (Optimize)

DESCRIPTION

When holding a great number of entries in your data source it is a best practice to compress them to avoid slowness issues when using your data source. The **Data Source (Optimize)** will analyze all your entries, compress them and then re-saves them, thus saving space in your data source.

SETTINGS

1. Open the data source you wish to optimize. In **Administration** click on **Pack Data Source (Optimize)** and then click on **Analyze**.



Pack Data Source (Optimize) - Analyze

2. Once the Analyze is completed click on **Optimize** to proceed with the optimization of your data source. You can select which **Vault** you wish to **Analyze** and **Optimize**, or use the **Optimize All** feature to perform the **Optimize** action on all available **Vaults**.

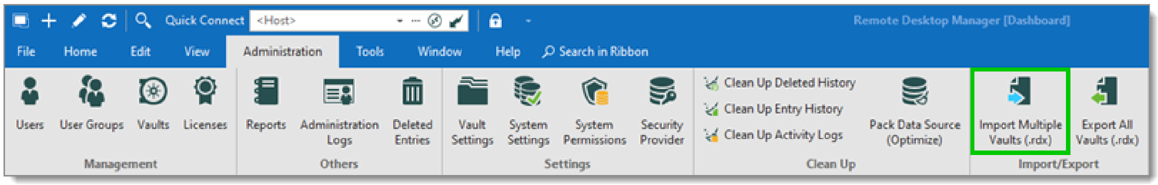
6.7.5 Import/Export

6.7.5.1 Import Multiple Vaults

DESCRIPTION

The ***Import Multiple Vaults (.rdx)*** function lets you import one or more vaults at a time. Learn how in this topic.

> The vaults you want to import must have been previously exported using the ***Export All Vaults (.rdx)***, because they need to be in the .rdx format.

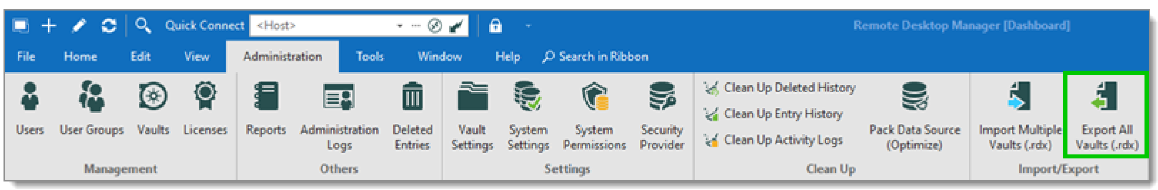


To learn more about other import functions, see our Import topic.

6.7.5.2 Export All Vaults

DESCRIPTION

The ***Export All Vaults (.rdx)*** function lets you export one or more vaults at a time. Learn how in this topic.

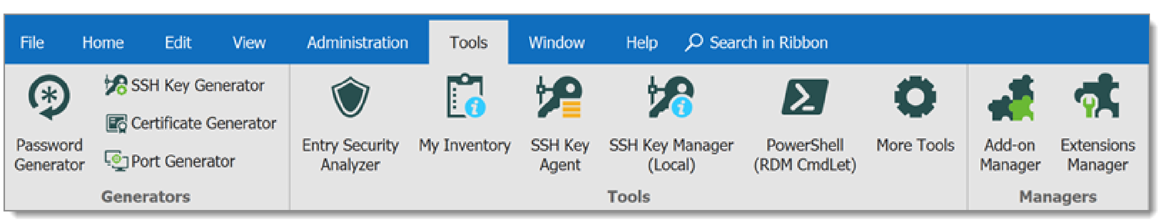


To learn more about other export functions, see our Export topic.

6.8 Tools

DESCRIPTION

The ***Tools*** tab contains your Add-on and Extensions manager as well as your Devolutions Server Console, Generators and multiple useful tools.



GENERATORS

OPTION	DESCRIPTION
Password Generator	Opens the Password Generator window. You can use this to generate password according to pre-determined criteria for better security.
SSH Key Generator	Launches the SSH Key Generator. SSH keys provide a secure way of logging into a virtual private server with SSH than using a password alone.
Certificate Generator	Launches the Certificate Generator. With this you can create a self-signed certificate, which is an identity certificate that is signed by the same entity whose identity is certified.
Port Generator	Launches the Port Generator. With this you can generate ports for your connections.

TOOLS

OPTION	DESCRIPTION
Entry Security Analyzer	Opens the Entry Security Analyzer. This is used to evaluate the strength of passwords stored in the data source.
My Inventory	Set up a My Inventory report.
SSH Key Agent and Manager	Opens the Key Agent Manager. This is used to hold all your SSH Keys in memory, already decoded and ready for them to be used.
PowerShell (RDM CmdLet)	Opens the PowerShell (RDM CmdLet).

OPTION	DESCRIPTION
More Tools	The **More Tools** window contains a variety of application tools such as: Chocolatey Console, Local RDP/RemoteApp Manager, Playback (Ansi), RDM Agent and more.

MANAGERS

OPTION	DESCRIPTION
Add-on Manager	Opens the Add-on Manager. It is used to simplify the management of different add-ons.
Extensions Manager	Opens the Extensions Manager. This is used to simplify the management and installation of Web Browser extensions and other miscellaneous extensions.

6.8.1 Generators

6.8.1.1 Password Generator

DESCRIPTION

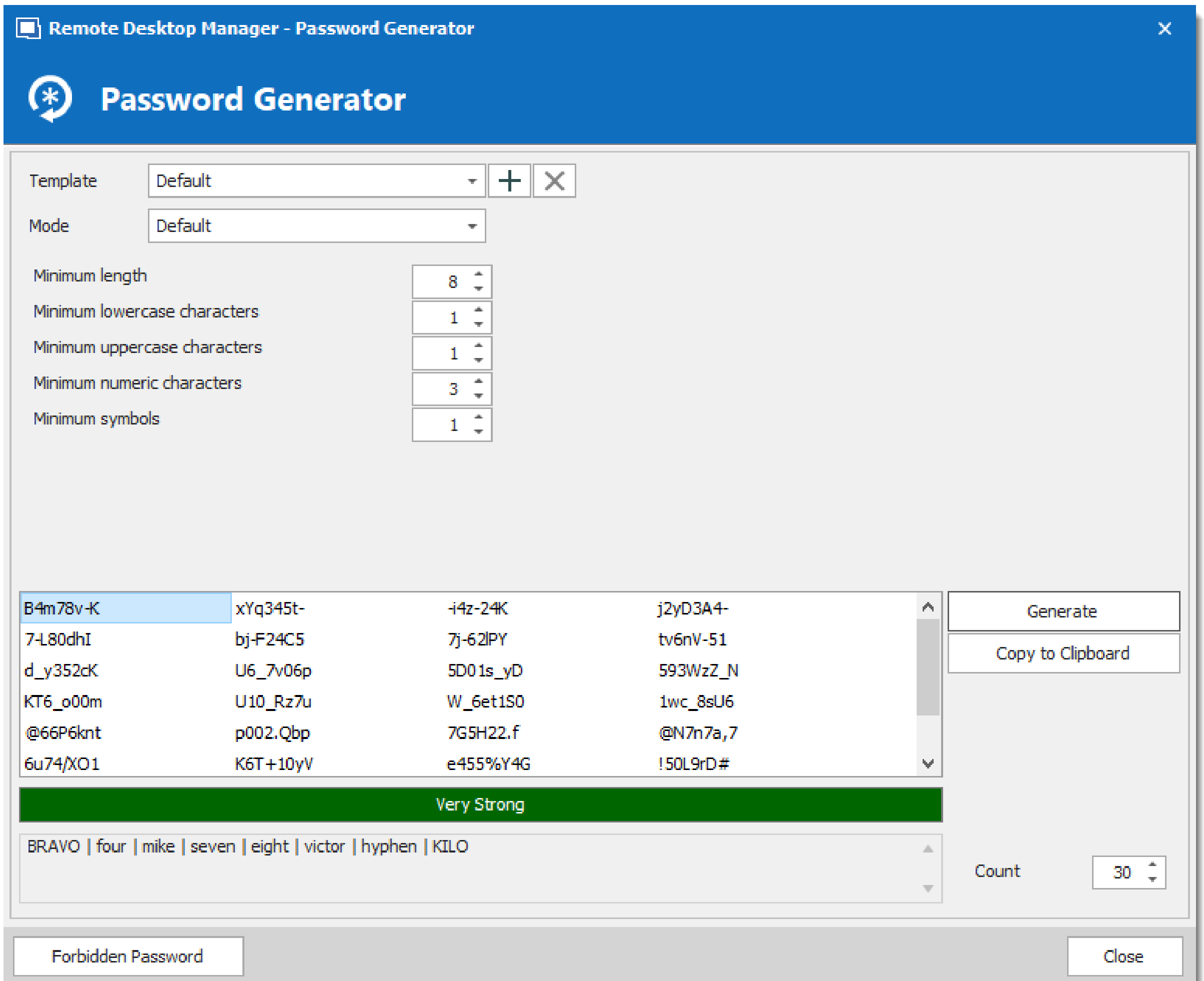
The **Password Generator** is available in the ***Tools – Password Generator*** menu. It allows to create random passwords that are and difficult to interpret or predict, due to a mix of uppercase and lowercase letters, numbers and punctuation symbols.

You can also create password generator templates to generate passwords. After you have selected your mode and settings, you can then create your template.

MODE

DEFAULT

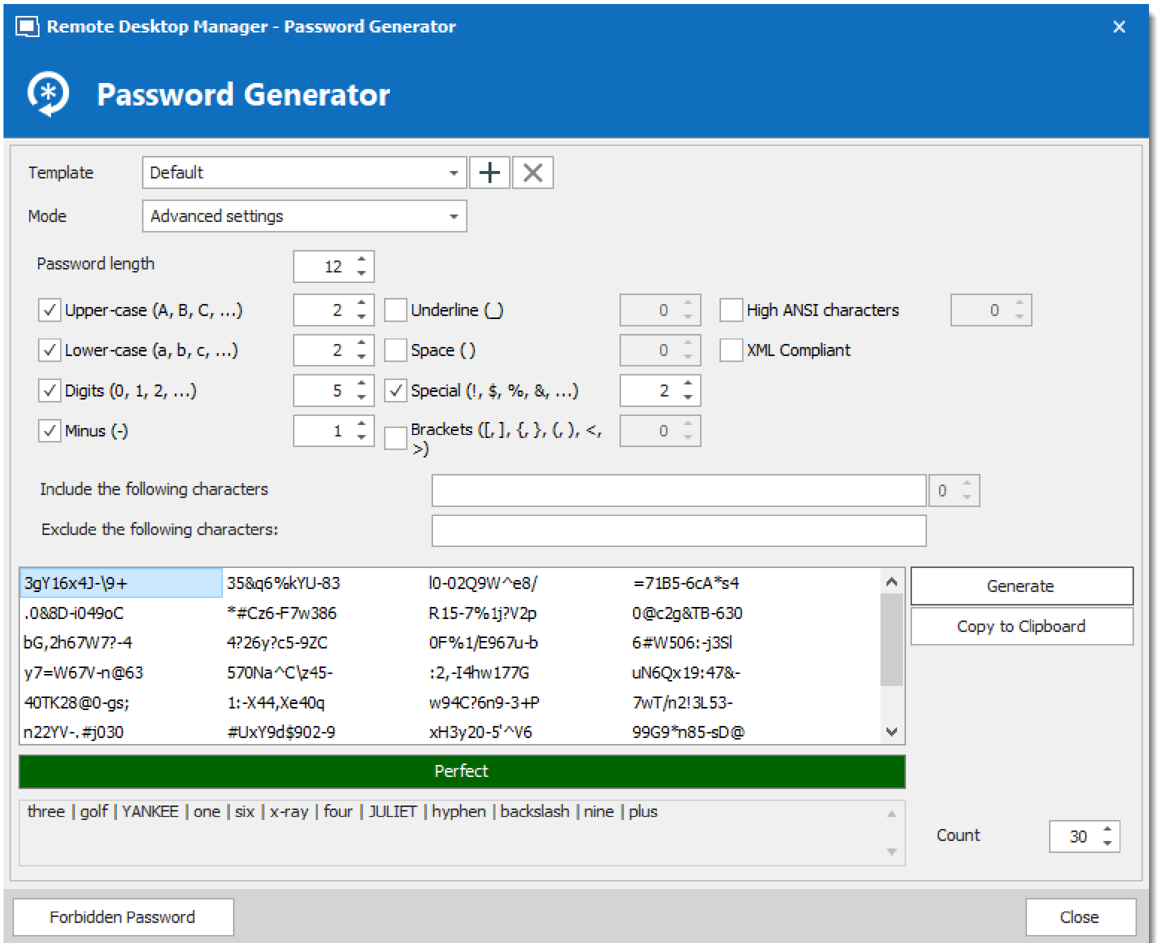
Customize all criteria you would want your password to have.



Password Generator - Default

ADVANCED SETTINGS

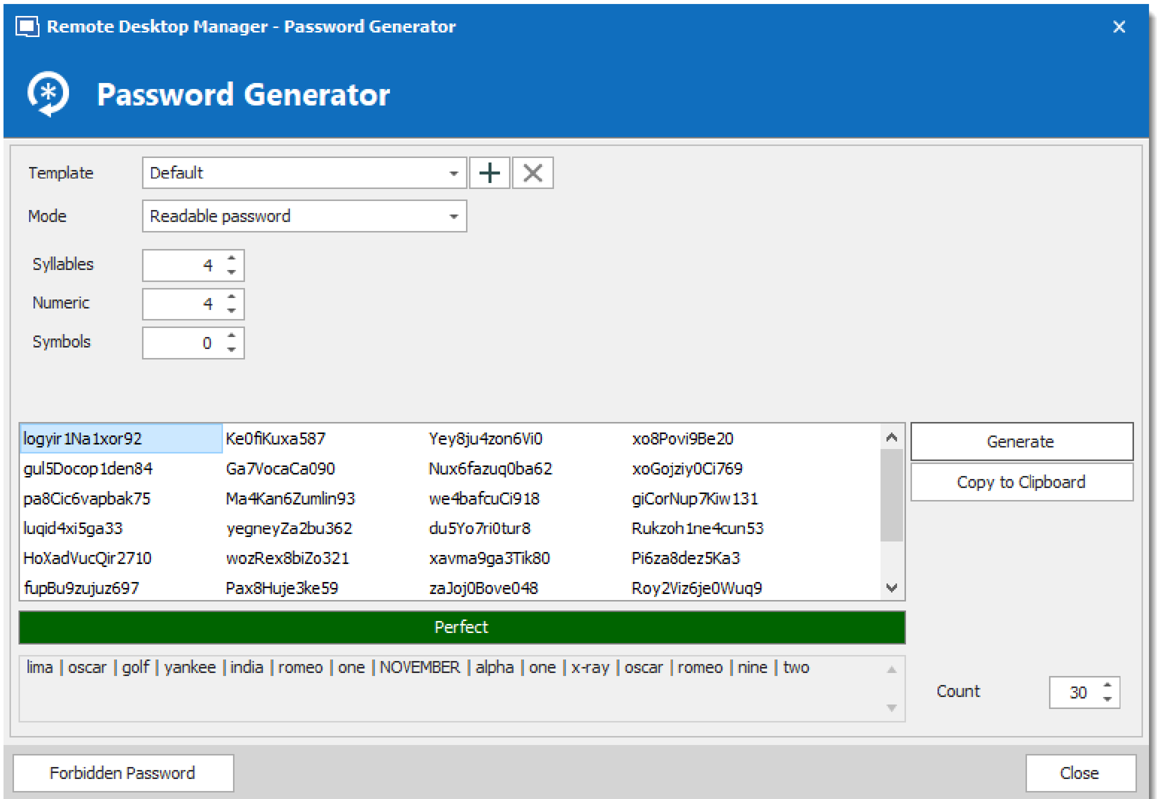
Select the type and amount of characters to include in the password.



Password Generator - Advanced Settings

READABLE PASSWORD

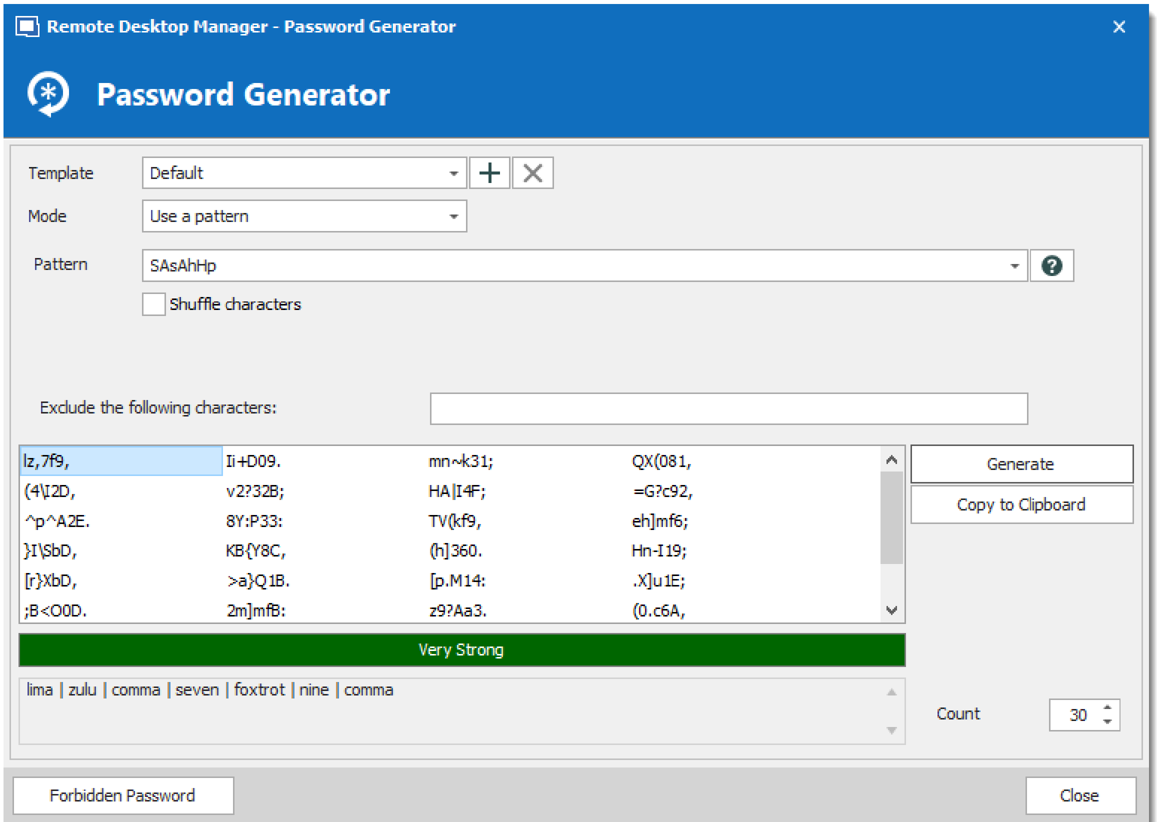
Generate passwords that are readable but are not actual words.



Password Generator - Readable password

USE A PATTERN

Press the button and select any pattern you need to create the passwords, you can also exclude certain characters if desired. A list of the most recent used pattern will also be created.



Password Generator - Use a pattern

The following are supported patterns:

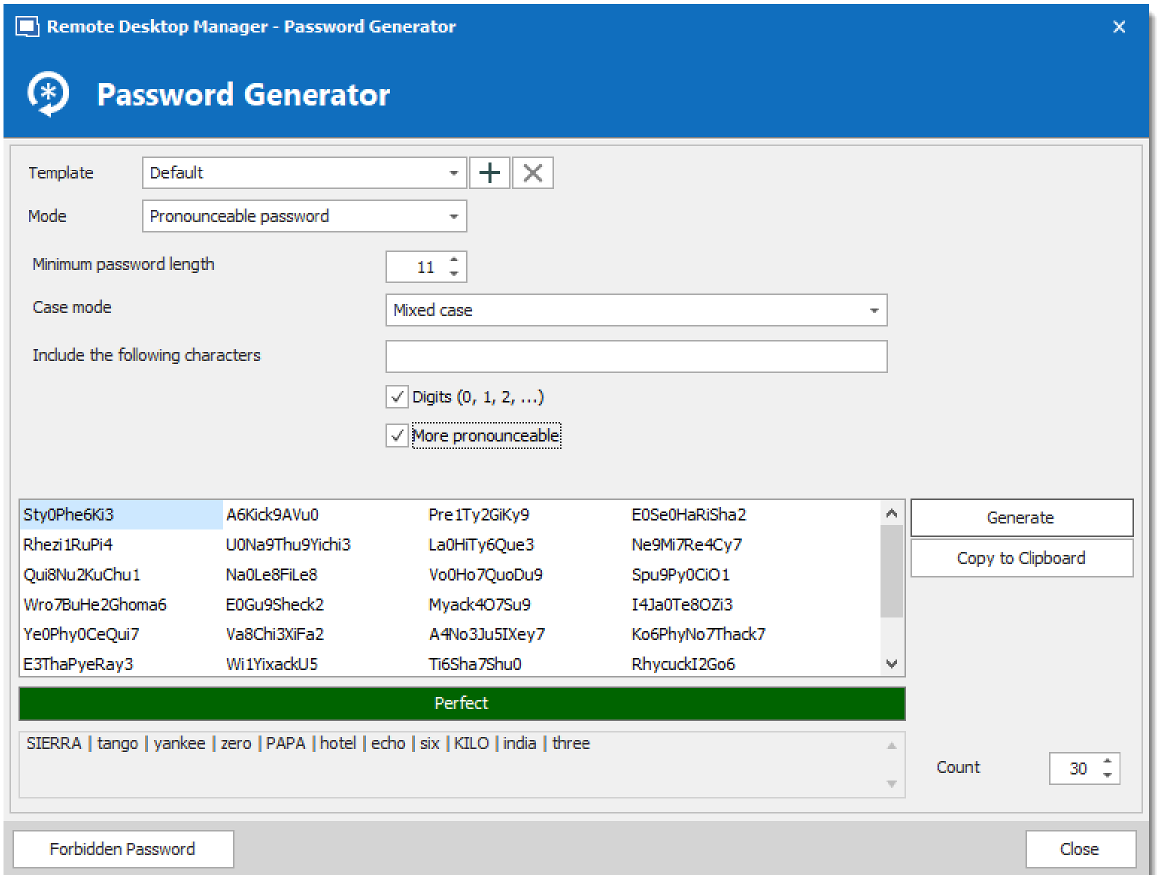
DESCRIPTION	KEY	SAMPLE
Lower-Case Alphanumeric	a	abcdefghijklmnopqrstuvwxyz 0123456789
Mixed-Case Alphanumeric	A	ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789
Bracket	b	()[]{}<>
Lower-Case Consonant	c	bcdfghjklmnpqrstvwxyz
Mixed-Case Consonant	C	BCDFGHJKLMNPQRSTVWXYZ bcdfghjklmnpqrstvwxyz

DESCRIPTION	KEY	SAMPLE
Digit	d	123456789
Lower-Case Hex Character	h	0123456789 abcdef
Upper-Case Hex Character	H	0123456789 ABCDEF
Lower-Case Letter	l	abcdefghijklmnopqrstuvwxyz
Mixed-Case Letter	L	ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefgh ijklmnopqrstuvwxyz
Punctuation	p	,.;:
Printable 7-Bit Special Character	s	!"#$%&'()*+,-./:;<=>?[\]^_{|}~
Printable 7-Bit ASCII	S	A-Z, a-z, 0-9, !"#$%&'()*+,-./:;<=>?[\]^_{|}~
Upper-Case Letter	u	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Upper-Case Alphanumeric	U	ABCDEFGHIJKLMNOPQRSTUVWXYZ 0123456789
Lower-Case Vowel	v	aeiou
Mixed-Case Vowel	V	AEIOU aeiou
High ANSI	x	From '~' to U255 (excluding U255)

DESCRIPTION	KEY	SAMPLE
Upper-Case Consonant	z	BCDFGHJKLMNPQRSTVWXYZ
Upper-Case Vowel	Z	AEIOU
Escape (Fixed Char)	\	Use following character as is
Escape (Repeat)	{n}	Repeats the previous character n times
Custom character	[x]	Define a custom character sequence

PRONOUNCEABLE PASSWORD

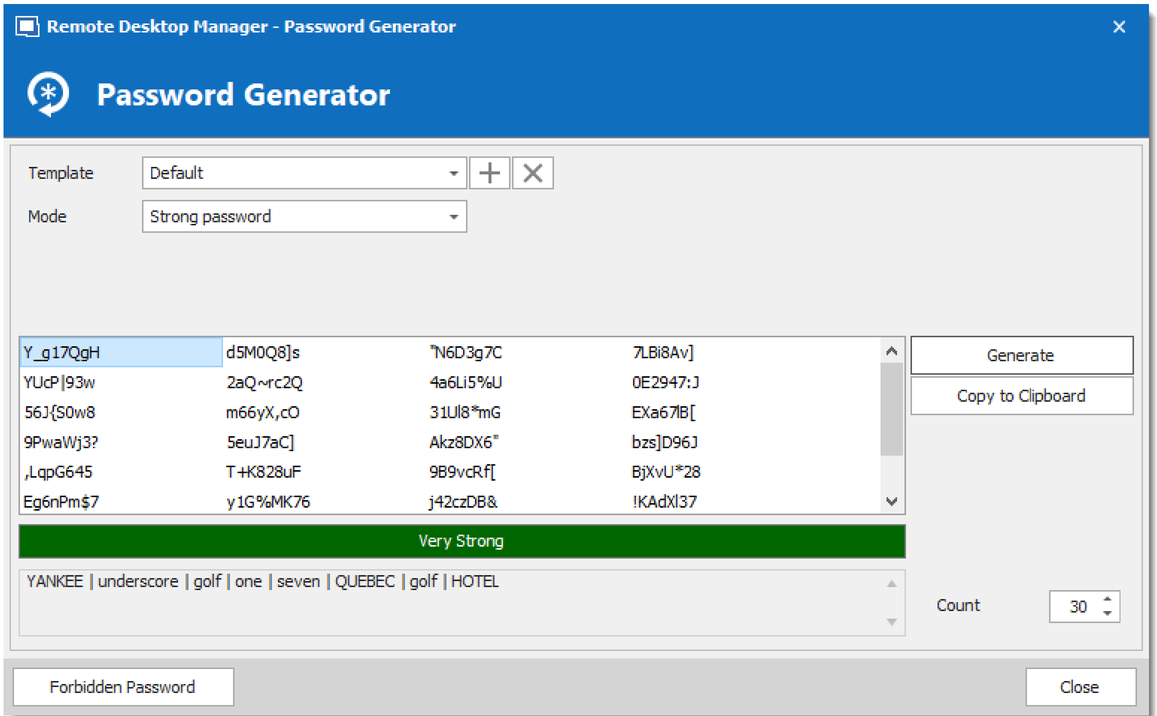
Generate passwords that are pronounceable, but are not actual words.



Password Generator - Pronounceable password

STRONG PASSWORD

Generate an 8 character passwords with alphanumeric and special characters.



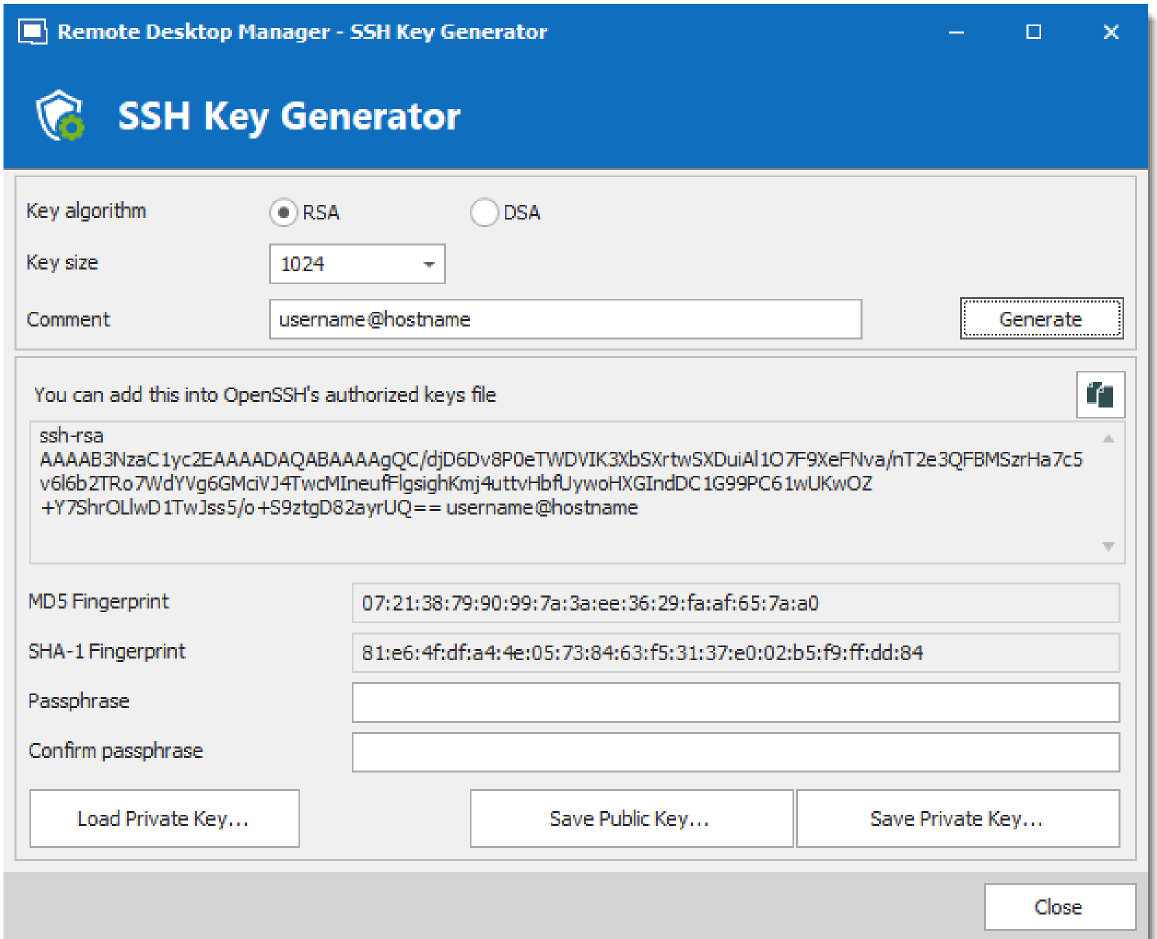
Password Generator - Strong password

6.8.1.2 SSH Key Generator

DESCRIPTION

SSH keys provide a secure way of logging into a virtual private server with SSH than using a password alone. While a password can eventually be cracked with a brute force attack, SSH keys are nearly impossible to decipher by brute force alone.

SETTINGS



SSH Key Generator

OPTION	DESCRIPTION
Key algorithm	You can choose between: **RSA**: RSA can be used for signing/verification and also for encryption/decryption. When using RSA it is recommended to use a 2048 bits key size. **DSA**: It is faster in signing but slower in verifying. It can only be used for signing/verification it **does not encrypt/decrypt**. When using DSA it is a recommended to use a 1024 bits key size.
Key size	You can choose your SSH Key size between:

OPTION	DESCRIPTION
	1024 bits: Minimum key size **2048 bits**: Default and recommended key size **4096 bits**: Maximum key size
Comment	Enter your username and the name of the computer you're transferring your key to.
Load Private Key	This feature will allow you to import a previously saved SSH Key.
Save Public Key	Saving the public key will generate a *.pub file. Simply enter a file name when prompted.
Save Private Key	You will have the option of saving your Private Key in different format, choose between: • PKCS #8 Private Key (*.pri) • PuTTY Private Key (*.ppk) • OpenSSH Private Key (*.pri)

If you did not specify a passphrase you will have to confirm that you do not wish to use a passphrase.

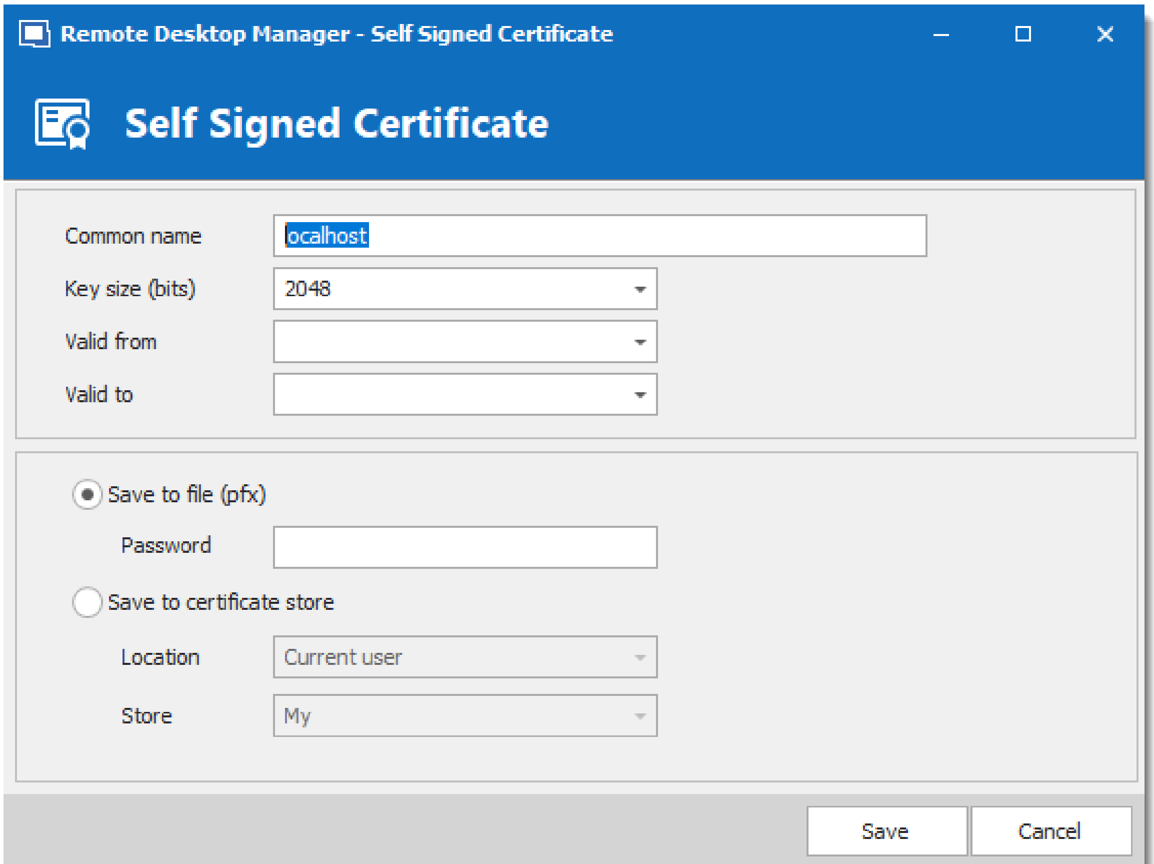
> If using the Key Agent Manager you must chose the PuTTY Private Key (.ppk) file format or the OpenSSH Private Key (.pri) file format. The PKCS Private Key is not a supported file format for the Key Agent Manager.

6.8.1.3 Certificate Generator

DESCRIPTION

The **Certificate Generator** allows you to create a self signed certificate which is an identity certificate that is signed by the same entity whose identity is certified.

SETTINGS

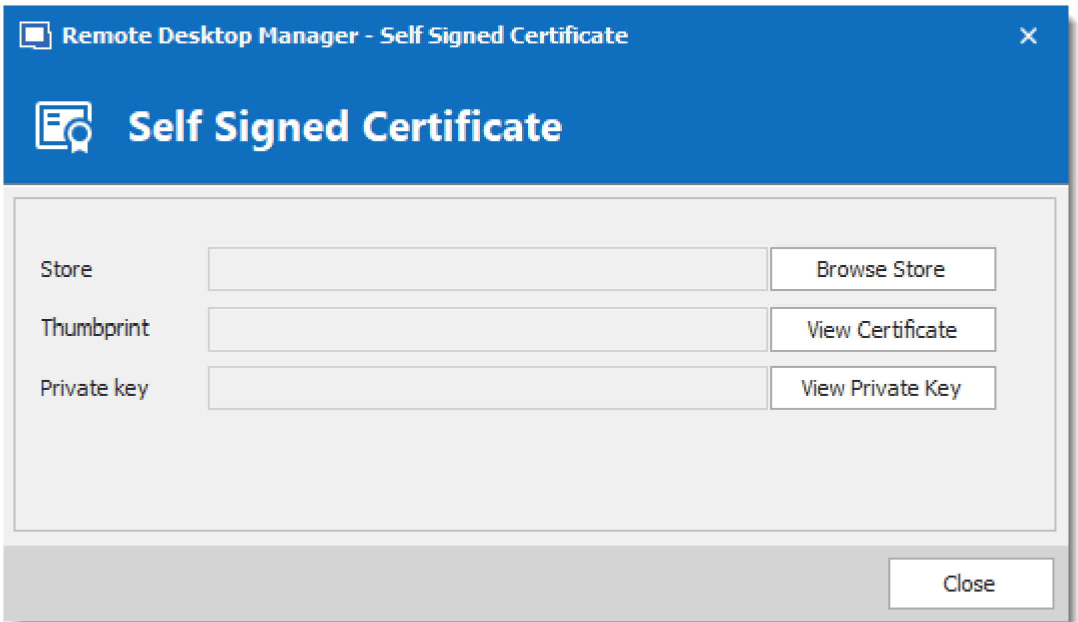


Certificate Generator - Self Signed Certificate

OPTION	DESCRIPTION
Common name	Name of the certificate.
Key size (bits)	Indicates the key size (bits) of the certificate. Select between: • **1024** • **2048**

OPTION	DESCRIPTION
	• **4096** • **8192** • **16384**
Valid from	Starting date of the certificate.
Valid to	Expiration date of the certificate.
Save to file (pfx)	Save the certificate into a ***.pfx** file and secure this certificate with a password.
Save to certificate store	Indicate the location and the store to save the certificate.
Location	Indicate the location of the certificate. Select between: • **Current user** • **Local machine**
Store	Indicate the store location of the certificate. Select between: • **Address book** • **Authorization root** • **Certificate authority** • **Disallowed** • **My** • **Root** • **Trusted people**

OPTION	DESCRIPTION
	• **Trusted publisher**



Self Signed Certificate

OPTION	DESCRIPTION
Store	Indicate the store where the certificate will be located.
Browse Store	Browse the store that is indicated in the store field.
Thumbprint	Display the certificate thumbprint.
View Certificate	Display the certificate that you have created.
Private Key	Display the certificate private key

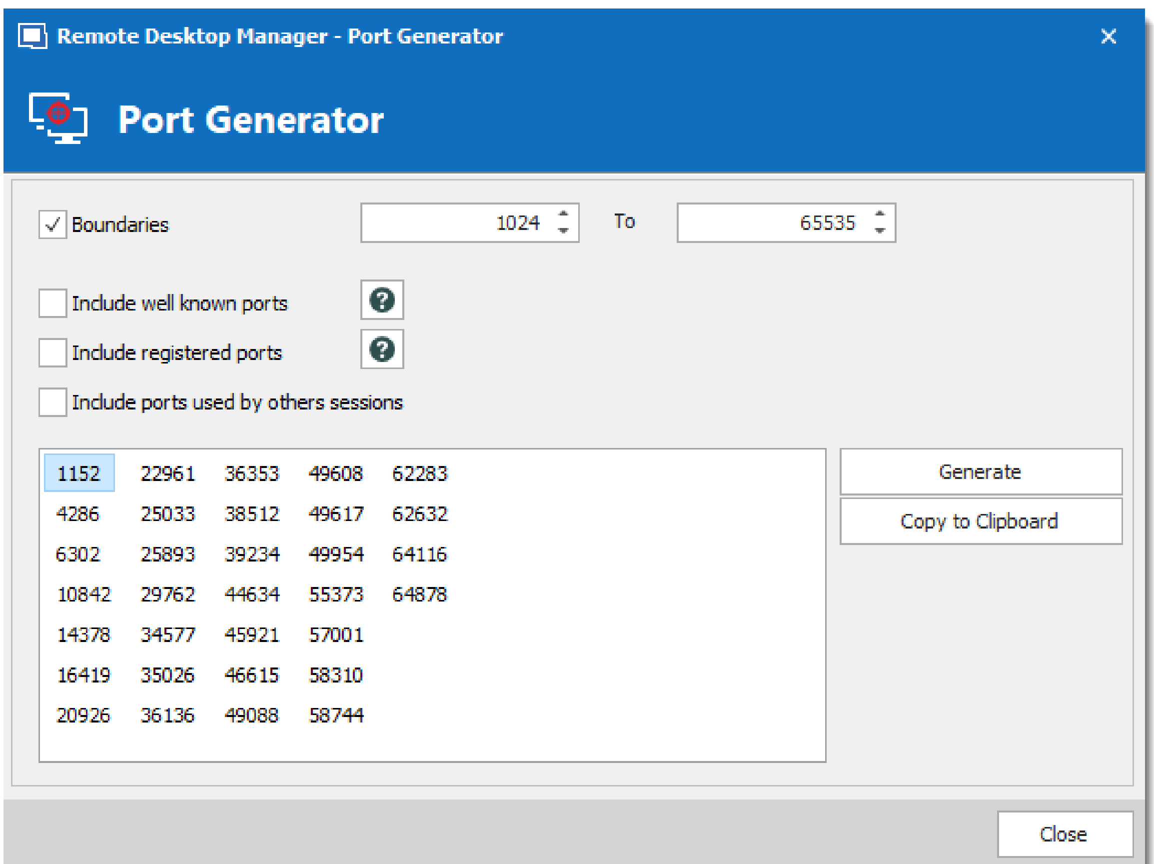
OPTION	DESCRIPTION
View Private Key	View the private key file on your computer.

6.8.1.4 Port Generator

DESCRIPTION

The Port Generator allows you to generate ports for your connections.

SETTINGS



Port Generator

OPTION	DESCRIPTION
Boundaries	Determinate the port range to generate the ports between those 2 numbers.
Include well known ports	Include ports from range 0 to 1023. They are the well-known ports or system ports. They are used by system processes that provide widely used types of network services
Include registered ports	Include ports from range 1024 to 49151. They are assigned by IANA for specific service upon application by a requesting entity. On most systems, registered ports can be used by ordinary users.
Include ports used by others sessions	Include the ports that are already used by other sessions.

6.8.2 Tools

6.8.2.1 Devolutions Localizer

DESCRIPTION

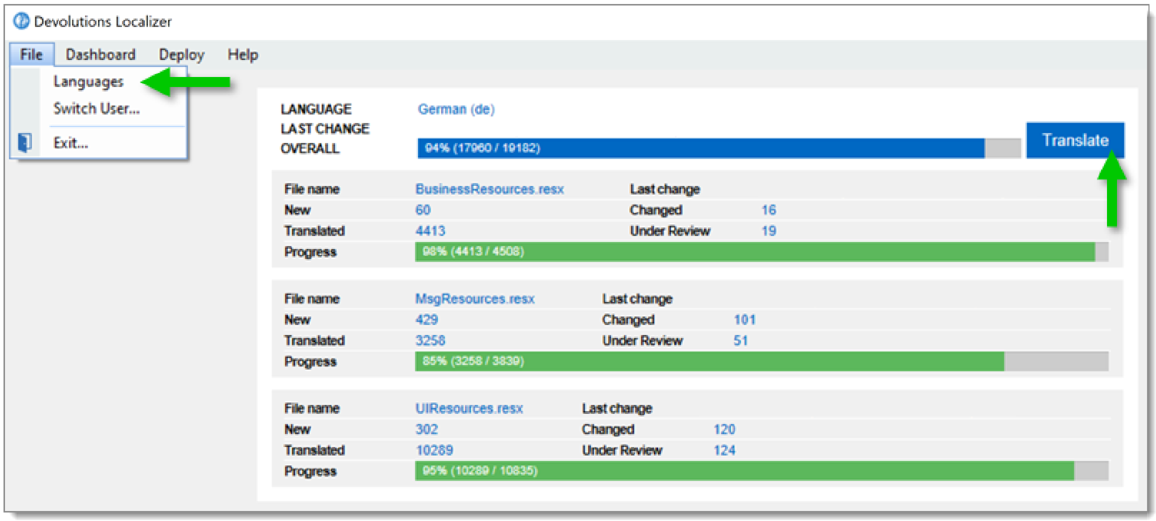
Devolutions Localizer is our custom translation tool for our applications. We welcome you to contribute to the Devolutions community by translating our tools for the benefit of other users just like you around the world.

Download the Devolutions Localizer translation tool to get started!

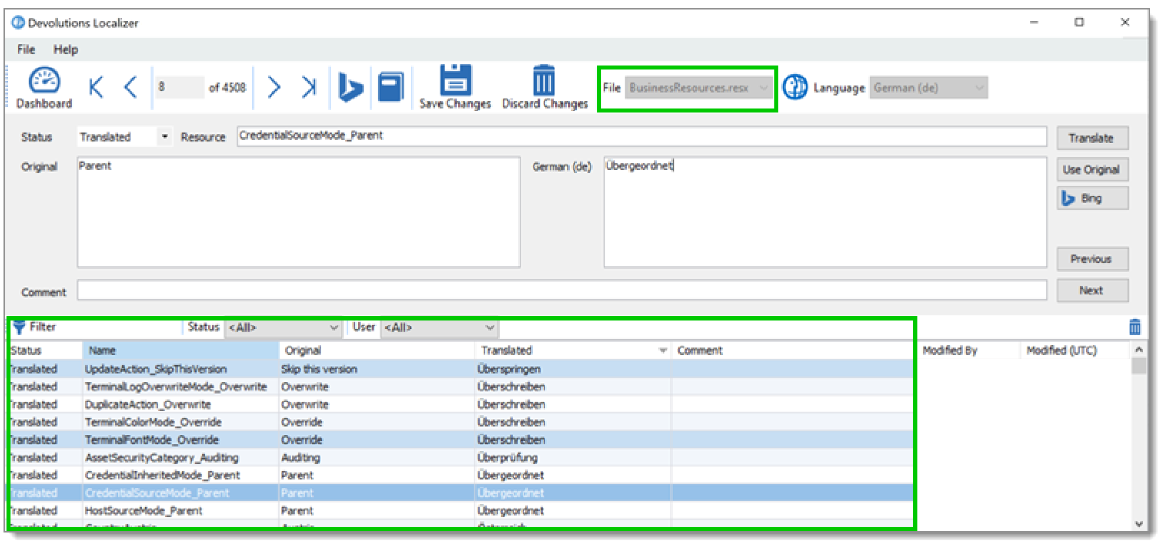
> A free Devolutions Account is required to log in to the Devolutions Localizer tool.

TRANSLATE

1. In ***File - Languages*** select the language to translate, then click on the ***Translate*** button.

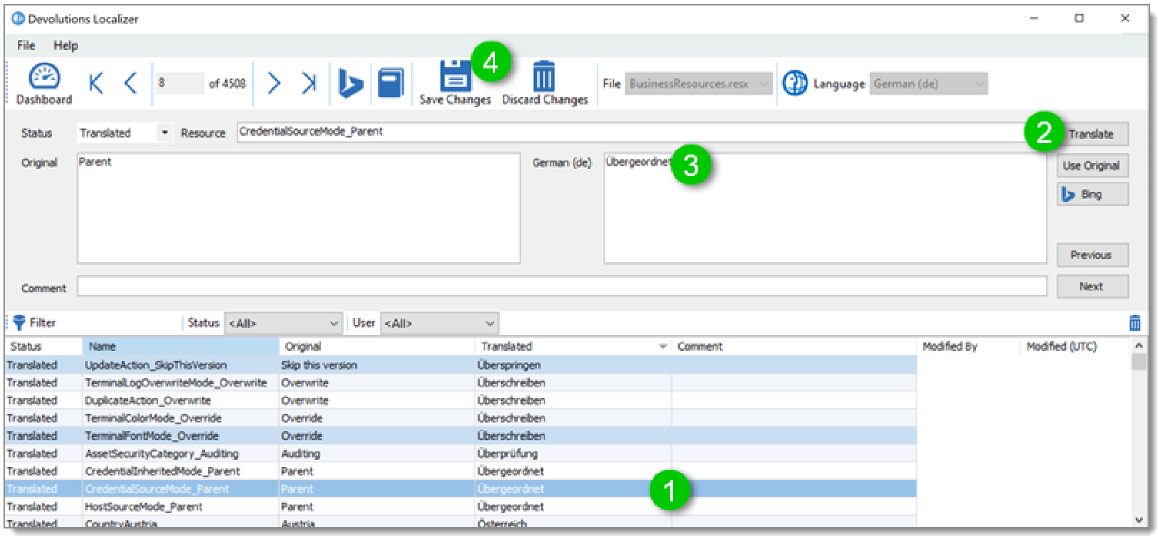


2. Choose from which file to translate, then in the lower part, you will be able to filter and review the content already translated or in need of translation.



3. To start select a ***Resource*** line in the bottom list and click ***Translate***. The original text will appear in the left window, type the translated text in the right window.

A ***Bing*** button is available to assist you translating your text.



4. When done, change the status to ***Translated*** for this resource and click ***Save Changes***. This will send your translation to our server and it will be deployed with the next release version of our applications.

PREVIEW

You can preview your changes in Remote Desktop Manager prior to the release or view the ones already in place but not yet released.

1. Close your Remote Desktop Manager.

2. In the Devolutions Localizer ***Dashboard*** click ***Deploy - Generate & Start*** to view your changes, or ***Start (use existing)*** to view unreleased changes.

To change the language of your Remote Desktop Manager application to reflect the one you were translating go to ***File - Options - User Interface - Language***. Select the language and click ***OK***. You will need to restart the application for this to take effect.

KEYBOARD SHORTCUTS

Devolutions Localizer also features several keyboard shortcuts to speed up the translation process:

- **CTRL+D**: Mark current resource as ***Translated***.

- **CTRL+E**: Mark current resource as ***Use original***, this ignores any translation text and will display the original value as is.

- **CTRL+DOWN**: Jump to the next resource.
- **CTRL+UP**: Jump back to the previous resource.
- **CTRL+B**: Request a Bing translation for the current resource.
- **CTRL+S**: Save all pending changes.
- **CTRL+F**: Enable/disable filtering.

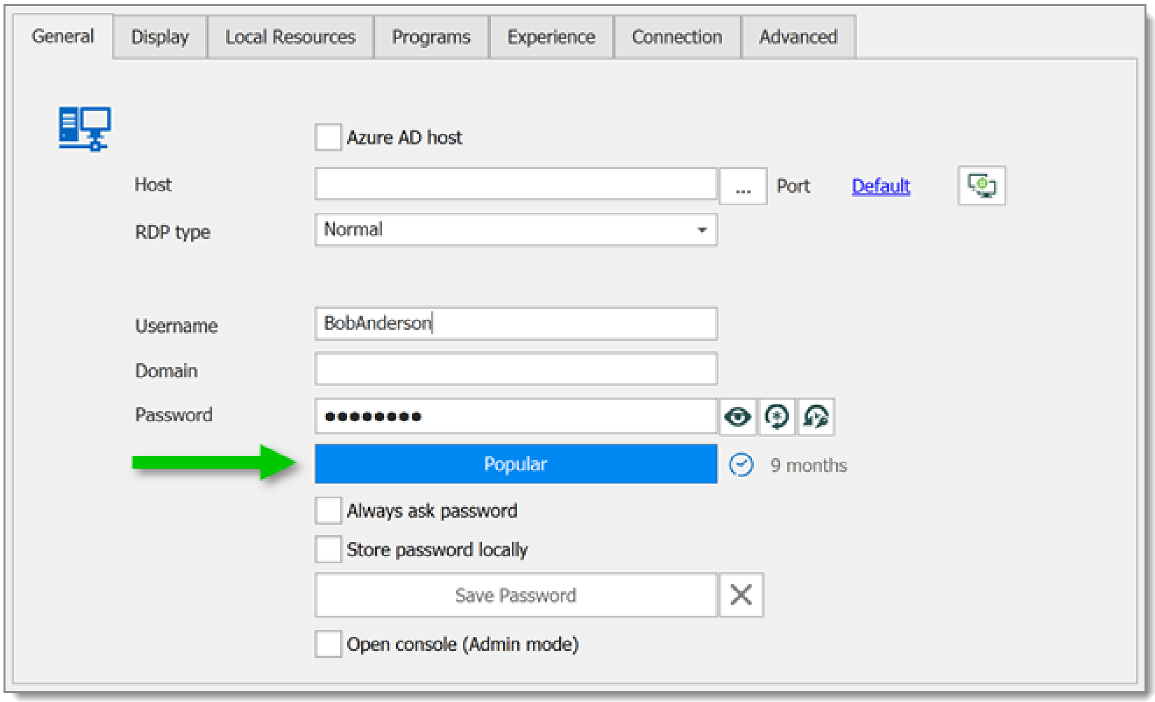
6.8.2.2 Entry Security Analyzer

DESCRIPTION

> The information in this topic is how the "Legacy" mode of password analysis works. The mode can be changed in the System Settings for ZXCVBN . The "Legacy" mode is not the default mode.

The ***Entry Security Analyzer*** evaluates the strength of passwords stored in the data source. To access the password analyzer, navigate the ***Tools*** tab.

A strenght password control is also displayed under most password fields of entries.



The ***Entry Security Analyzer*** follows a set of rules to determine the strength of the password with a score from 0 to 100. There are two categories of rules.

REINFORCE

These are the rules which make the passwords stronger:

- The password length
- The number of uppercase letters (A-Z)
- The number of lowercase letters (a-z)
- The number of digits (0-9)
- The number of symbols (!, @, #, $, etc.)
- The number of digits or symbols in the middle of the password
- Three or more of the rules above are met

The minimum requirements for a Strong password are:

- The password is at least 5 characters long

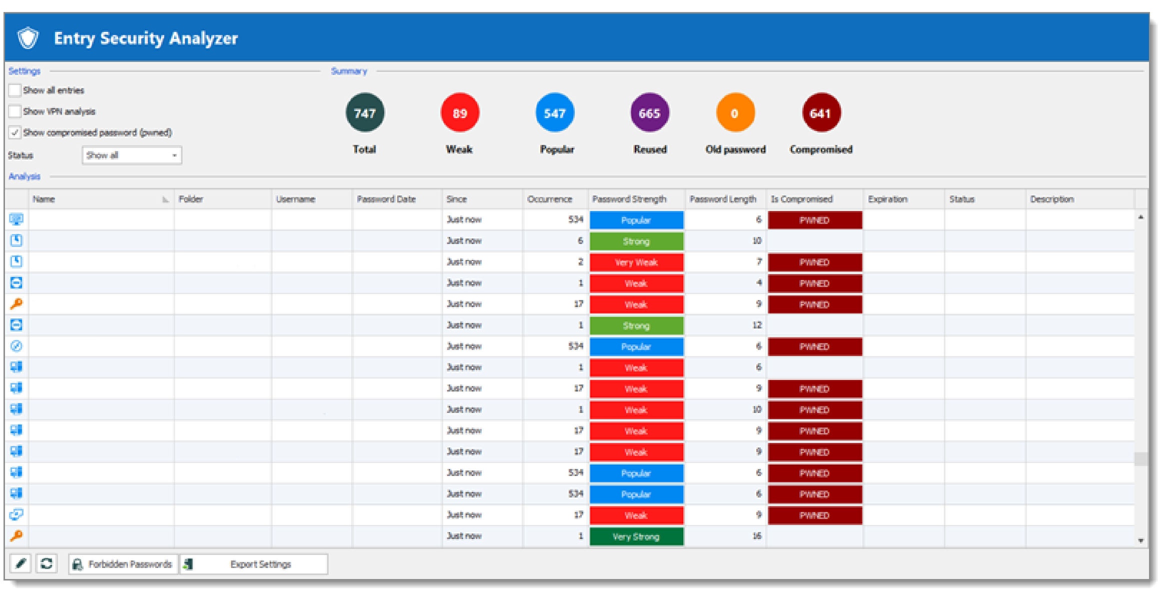
- The password contains uppercase and lowercase characters
- The password contains digits

WEAKENING

These are the rules which make the passwords weaker:

- The password contains only letters
- The password contains only digits
- The password has repeated characters
- The password has consecutive uppercase letters (two or more)
- The password has consecutive lowercase letters (two or more)
- The password has consecutive digits (two or more)
- The password has sequential letters (ABCD, DCBA)
- The password has sequential digits (1234, 4321)

SETTINGS



OPTION	DESCRIPTION
Show all entries	Shows you all the entries in your session, including those without password.
Show VPN analysis	Add the VPN Host column.
Show compromised password (pwned)	Show if the password has been pwned. A pwned password is a password that has been exposed in data breaches (i.e., they are owned/pwned by hackers).
Edit	Open the current entry to edit it.
Forbidden Passwords	Create a list of prohibited passwords.
Export Settings	Export the password analyzer settings.

6.8.2.3 Key Agent Manager

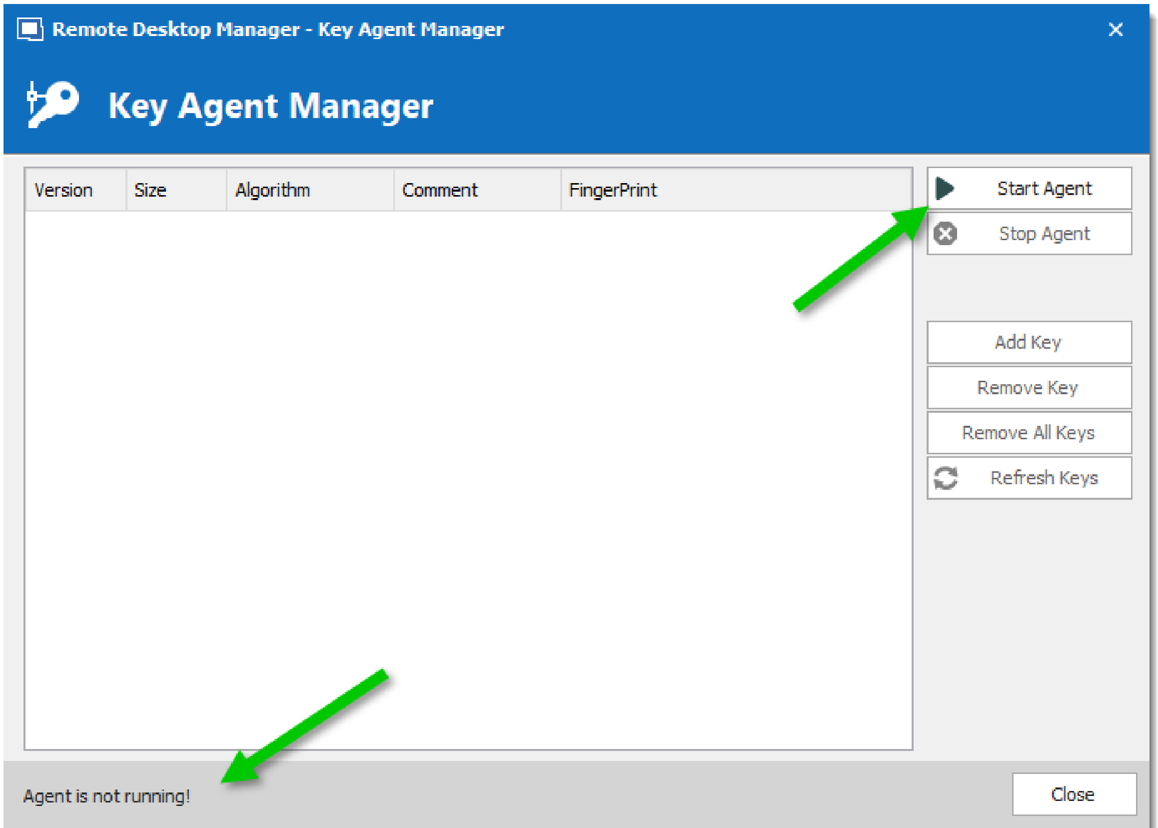
DESCRIPTION

The **Key Agent Manager** is used to hold all your SSH Keys in memory, already decoded and ready for them to be used. It has the same use as Pageant (SSH Key Manager) has for Putty except that the Key Agent Manager is used with Remote Desktop Manager.

SETTINGS

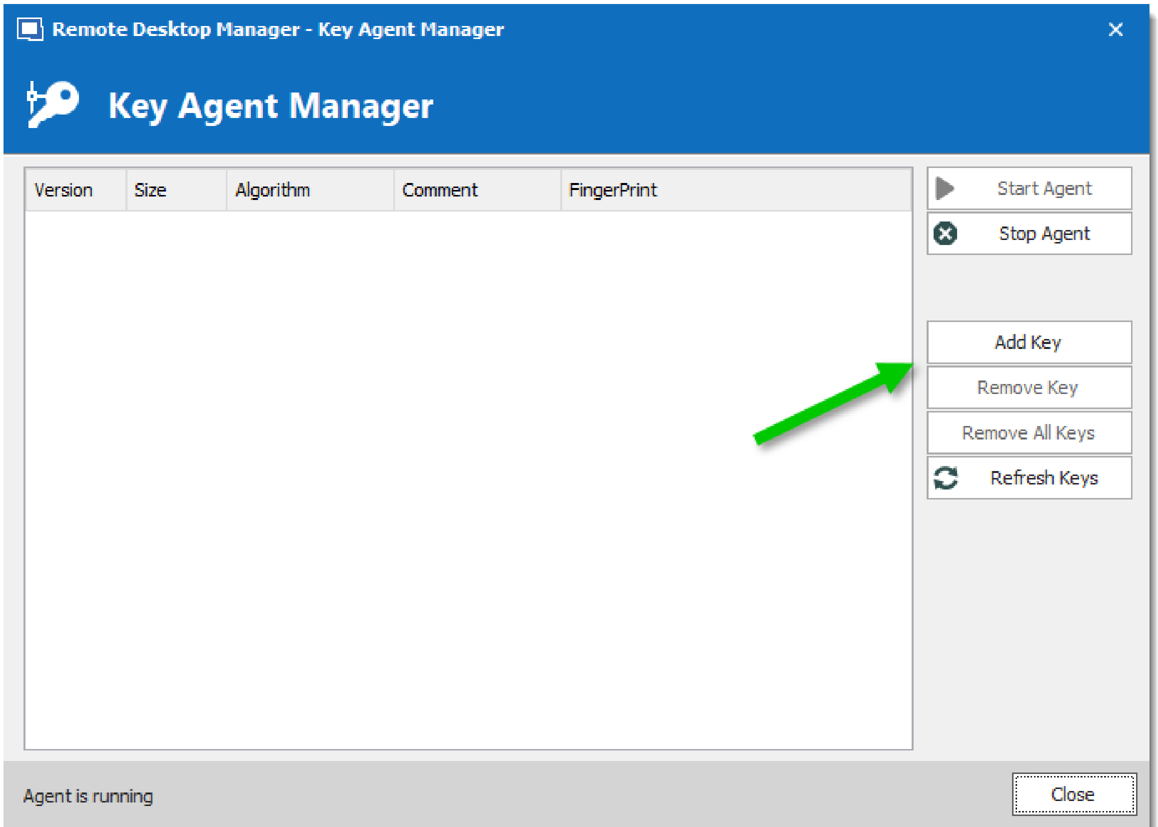
1. When opening the Key Agent Manager you will notice at the bottom right that the **agent is not running** you will need to click on **Start Agent**. If you wish to always have

your Key Agent running you can activate the option in ***File – Option – Key Agent – Start agent on application start***.



Key Agent Manager - Start Agent

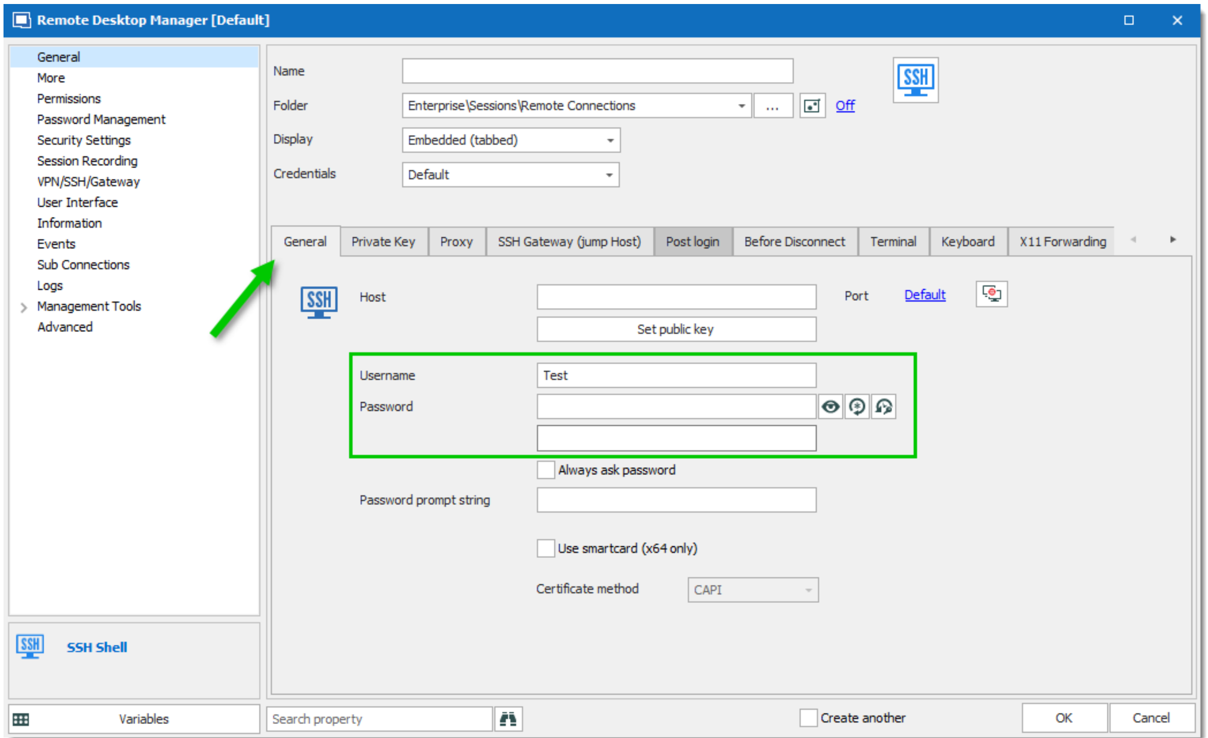
2. Click on **Add key** and select the file to open your SSH key.



Key Agent Manager - Add Key

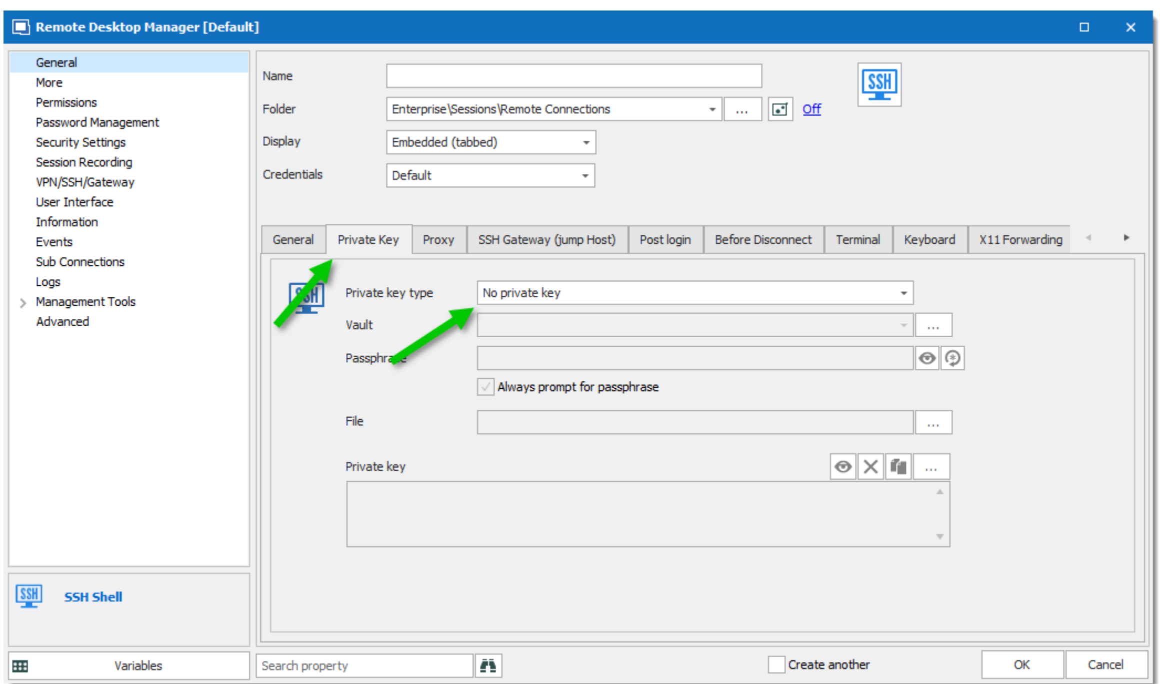
3. All your added SSH Key will appear in your Key Agent Manager.

4. In your SSH Shell Session in the **General** tab enter a Username and leave the Password field blank.



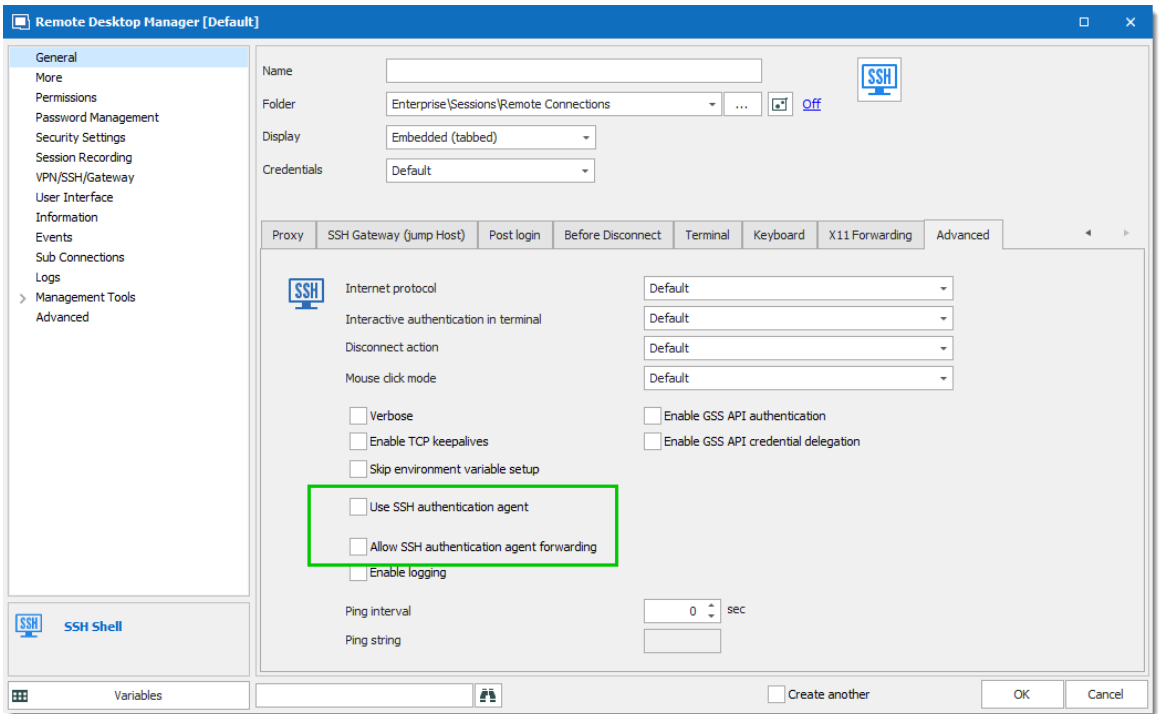
SSH Shell session - General Tab

5. In the **Private Key** tab of your SSH Shell session leave the option for the Private Key to **No Private Key**.



SSH Shell session - Private Key Tab

6. In the **Advanced** tab of your SSH Shell session activate the option **Use Agent**. The Use Agent automatically take the information of the SSH Key kept in your Key Agent Manager.

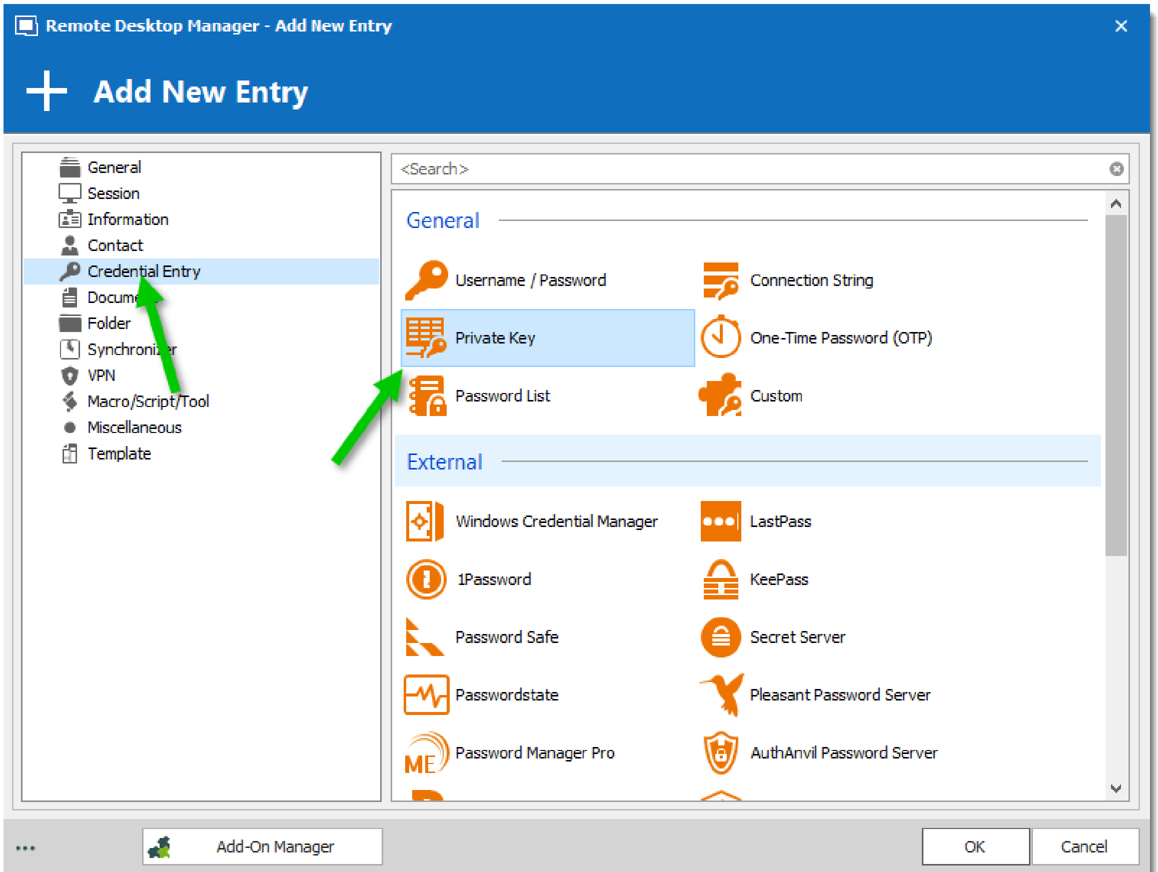


SSH Shell session - Advanced

PRIVATE KEY CREDENTIAL

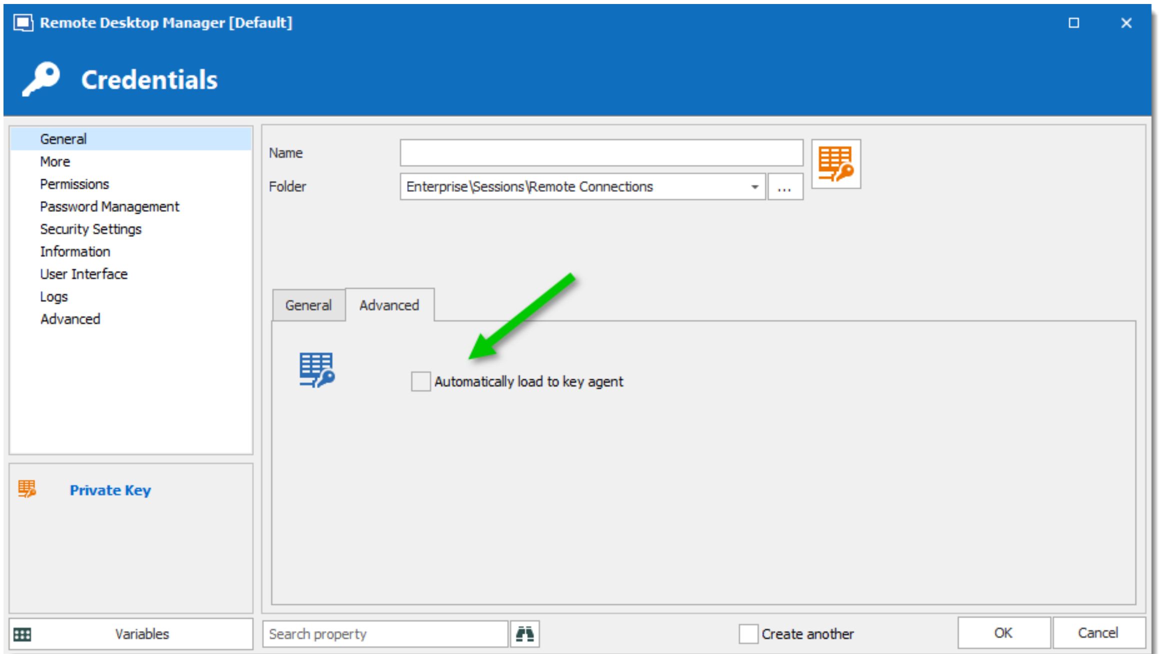
When creating new Private Key credential entry in Remote Desktop Manager you have the option of loading them automatically in your Key Agent Manager.

1. Create your new Private Key credential.



New Credential Entry - Private Key

2. In the **Advanced** tab of your Private Key entry activate the option **Automatically load to key agent.**



Private Key - Advanced Tab

6.8.2.4 PowerShell (RDM CmdLet)

DESCRIPTION

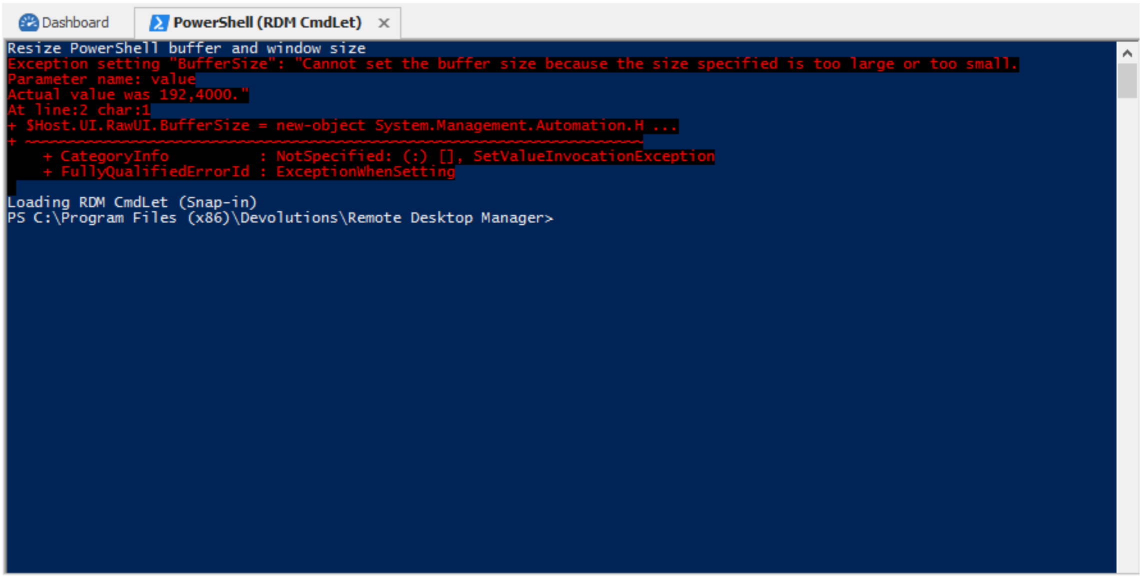
The **PowerShell (RDM CmLet)** automatically opens an embedded PowerShell window. RDM snap-in allows for quick and robust automation of actions such as add/edit/open of sessions, the possibilities are endless.

Since its release, this highly-requested feature has become very useful in solving user requests. A quick search through our forum reveals many usages of the cmdlets, such as automating the creation of Windows Start Menu shortcuts for every RDM session.

To learn more, you can find full RDM cmdlet documentation available via the PowerShell Scripting topic or directly in PowerShell using the Get-Help cmdlet.

SETTINGS

You will find on the Forum multiple PowerShell script to import edit or interact with the Remote Desktop Manager data.



PowerShell

6.8.2.5 More Tools

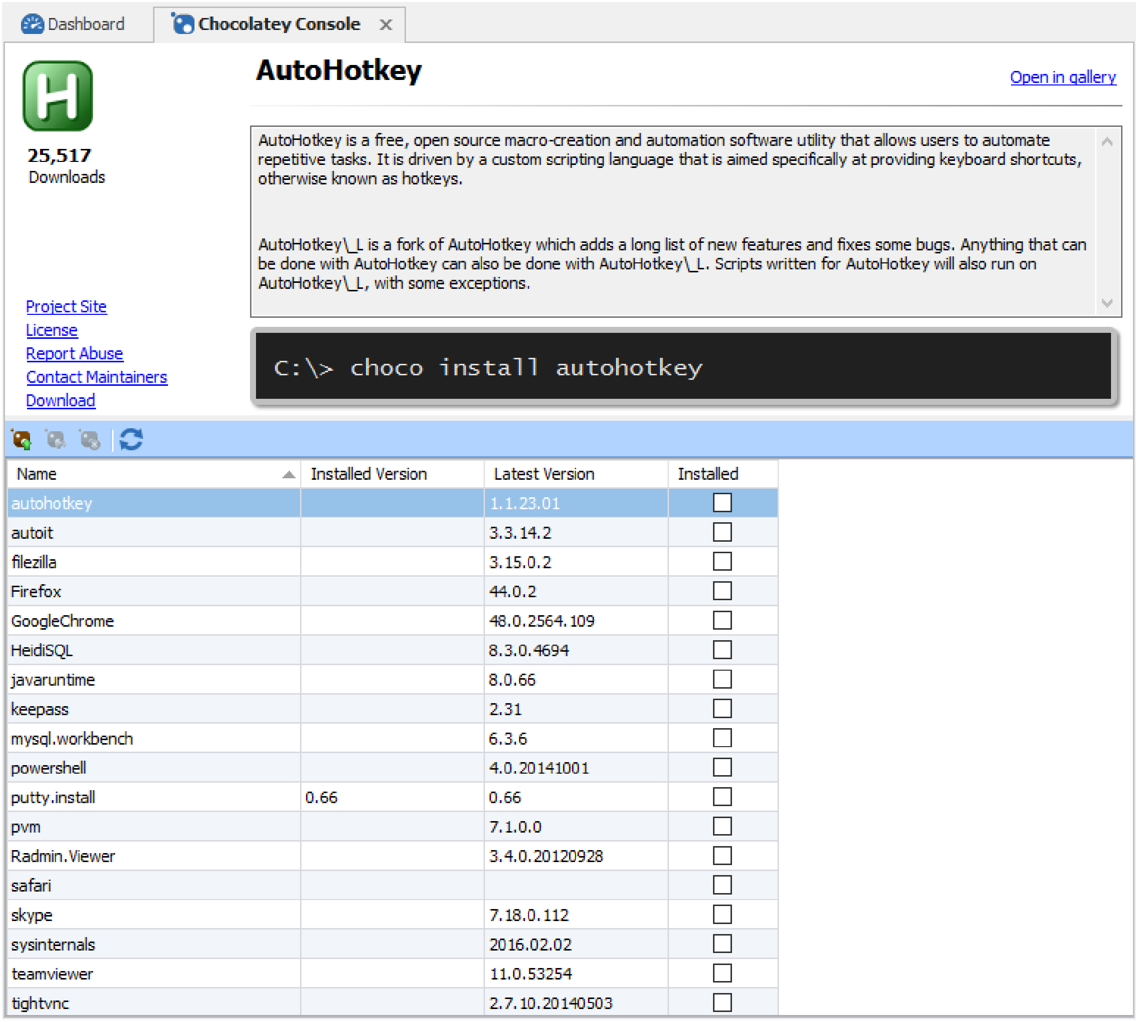
6.8.2.5.1 Chocolatey Console

DESCRIPTION

> Chocolatey need to be installed on your computer to use the Chocolatey Console.

The Chocolatey Console is available in the ***Tools – More Tools - Chocolatey Console*** menu. It allows you to install all the supported applications from Chocolatey directly from Remote Desktop Manager.

SETTINGS

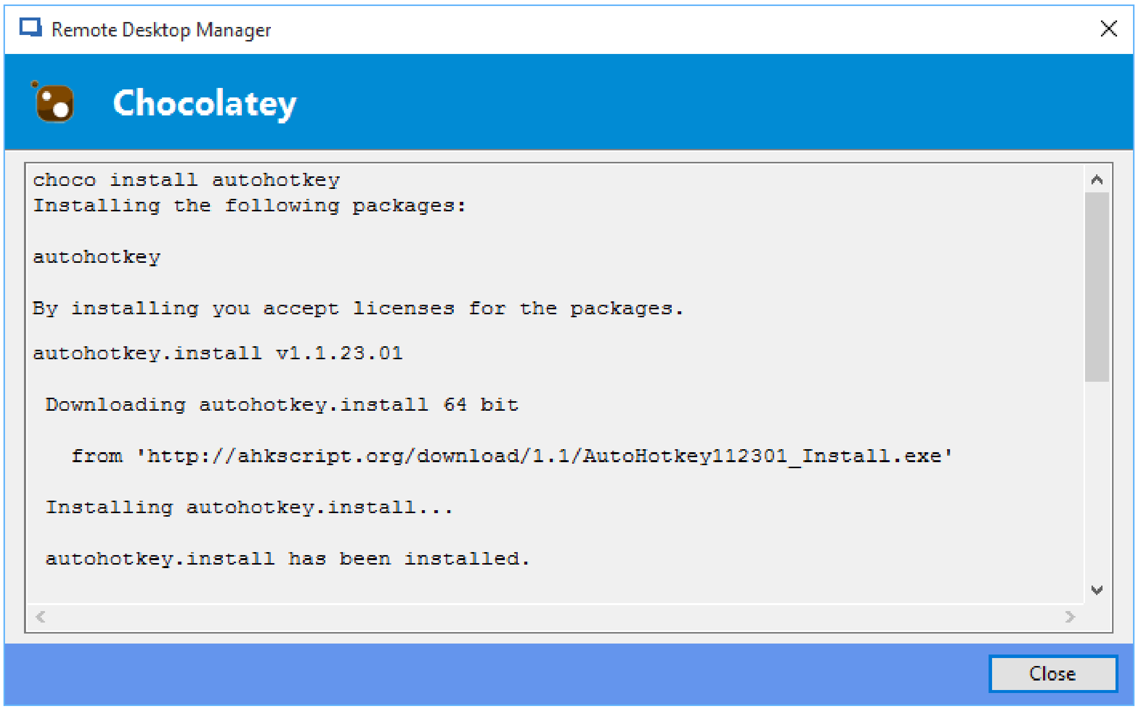


Chocolatey Console

OPTION	DESCRIPTION
	Install the selected application.
	Update the selected application.
	Uninstall the selected application.
	Refresh the Chocolatey details list.

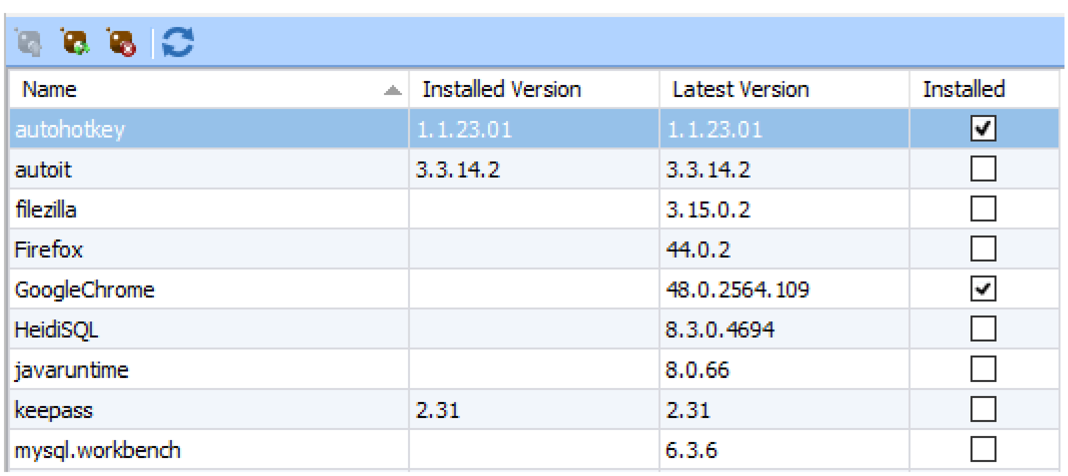
USAGE

During the installation, you will see the following window.



Installation window

When the installation is completed you will see a check mark in the **Installed** column.



Installation Complete

6.8.2.5.2 Local RDP/RemoteApp Manager

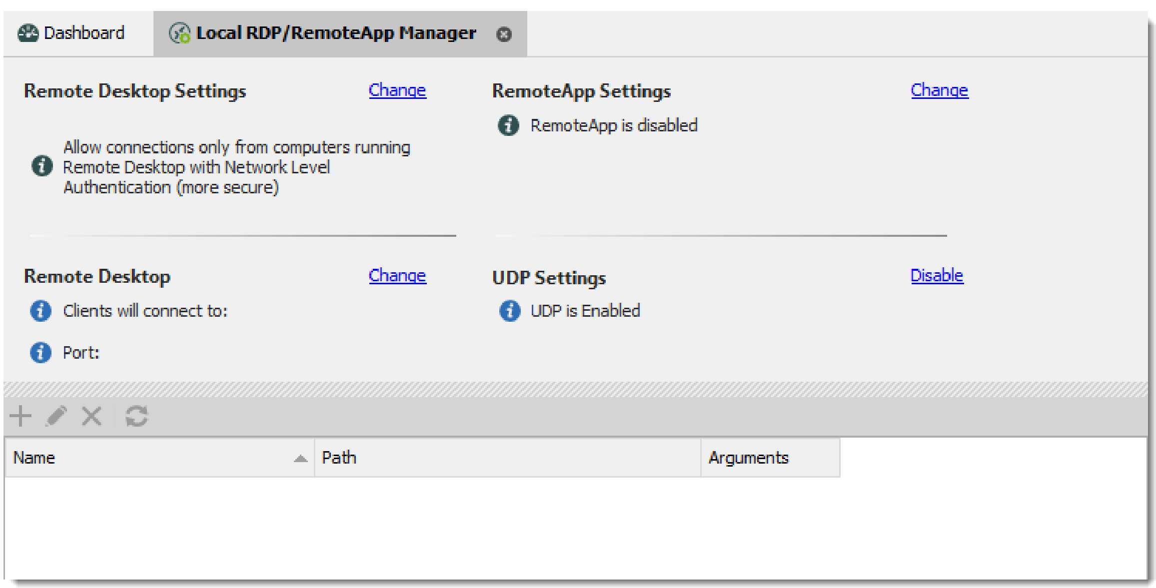
DESCRIPTION

The local RDP settings and the RemoteApp settings are available from ***Tools – More Tools - Local RDP/RemoteApp Manager***.

If you run Remote Desktop Manager on a Windows Server 2008 machine the TS RemoteApp MMC console will be launched.

If you are running on Windows Vista, the RemoteApp console built into Remote Desktop Manager will be launched because RemoteApp functionality is available in Windows 7 but not the MMC console. Therefore instead of having to modify the required registry entries you can use the Remote Desktop Manager RemoteApp Manager.

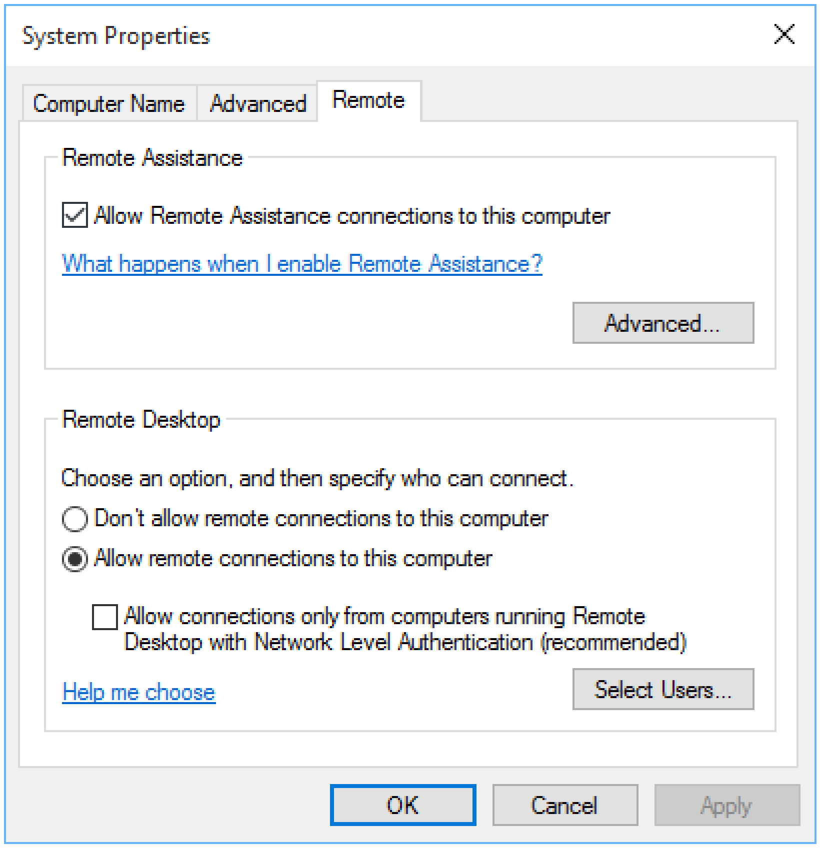
SETTINGS



More Tools - Local RDP/RemoteApp Manager

REMOTE DESKTOP SETTINGS

Allow or disallow the remote connections to your computer.

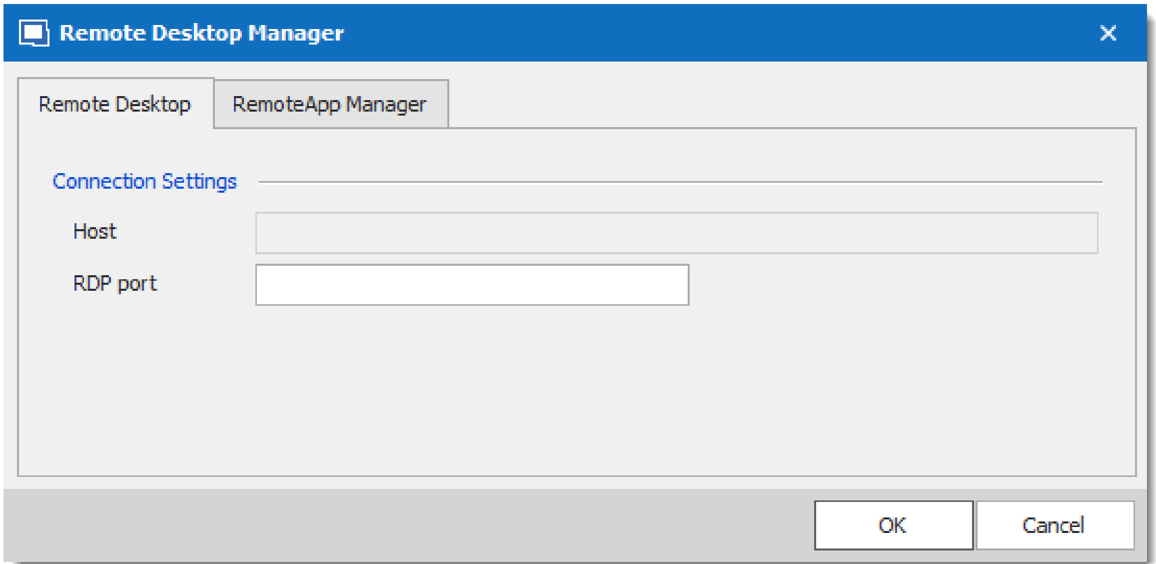


Remote Desktop Settings

REMOTE DESKTOP

Allows you to modify the local RDP port.

Remote Desktop Manager must be run as an administrator to modify the Remote Desktop settings.

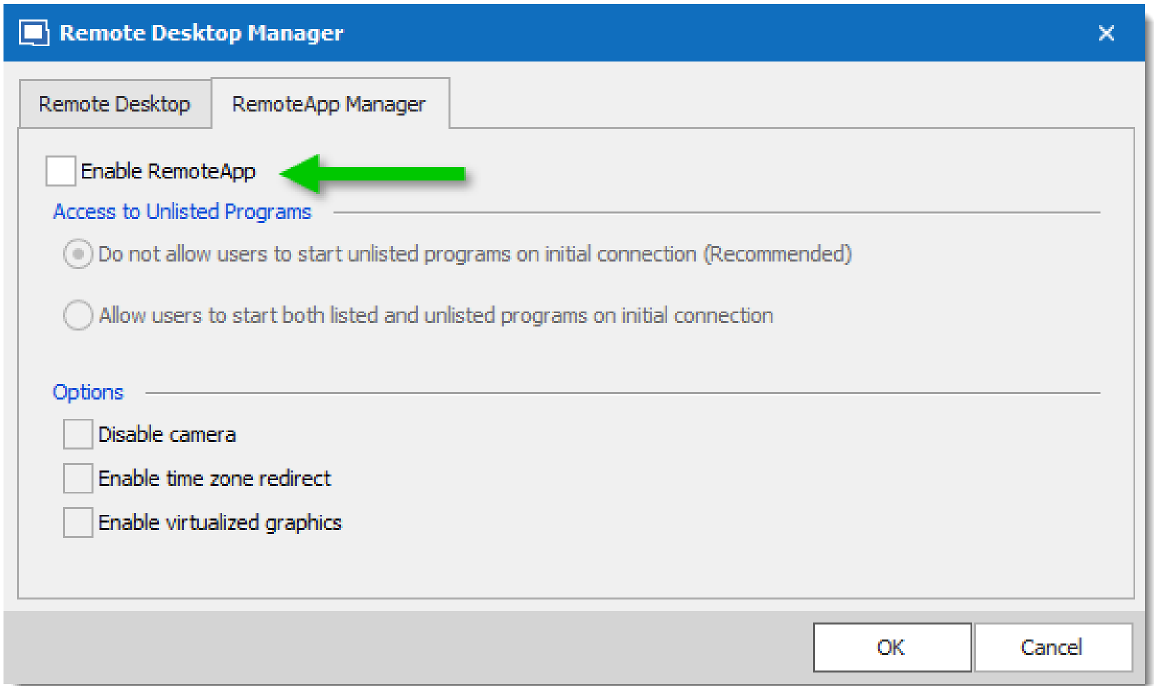


Remote Desktop Connection Settings

REMOTEAPP SETTINGS

You must Enable RemoteApp to be able to create a New RemoteApp Setting.

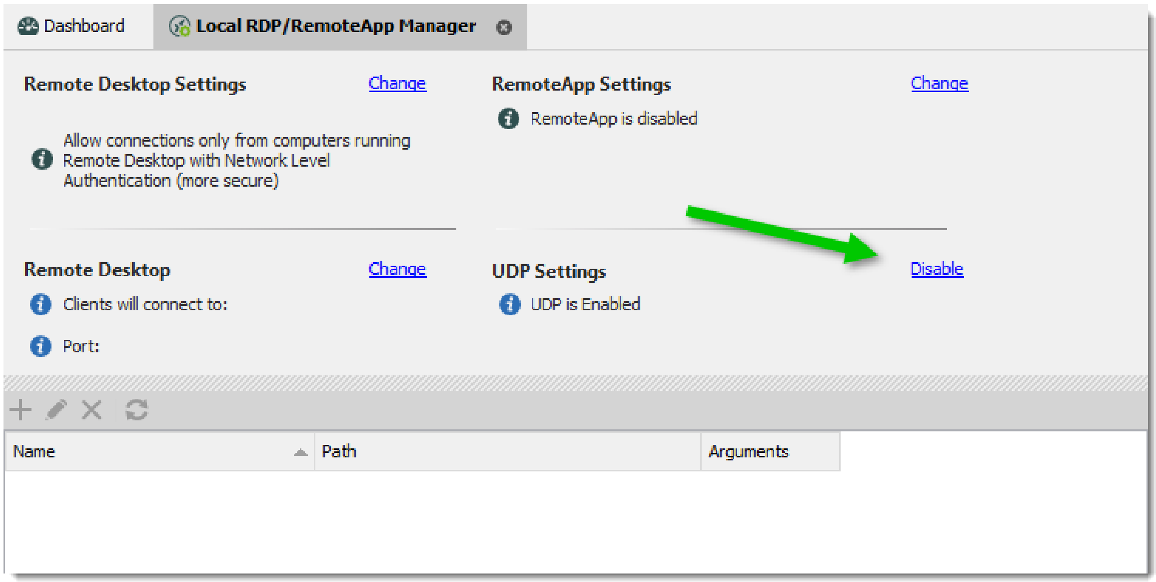
> Remote Desktop Manager must be run as an administrator to modify the RemoteApp settings.



RemoteApp Settings

UDP SETTINGS

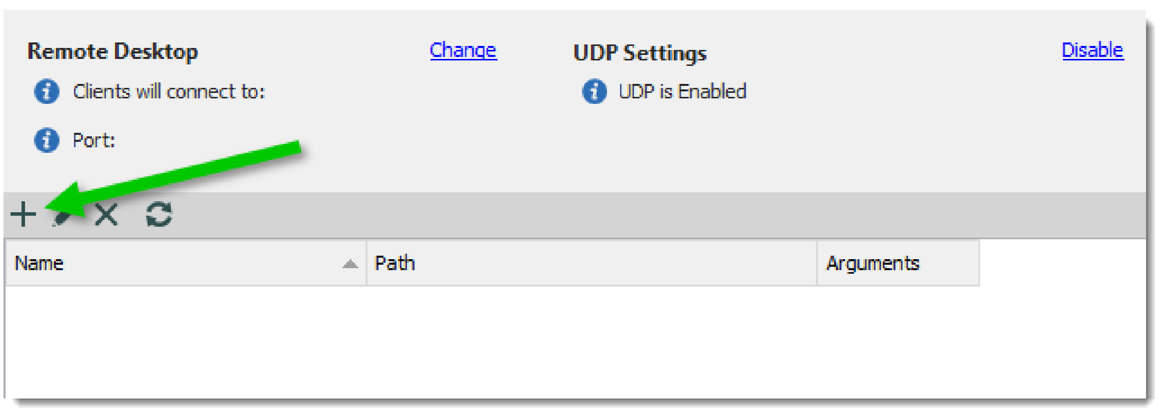
Enable or disable UDP (User Datagram Protocol) locally on your computer. UDP is a communication protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP).



Local RDP/RemoteApp Manager - UDP is Enabled

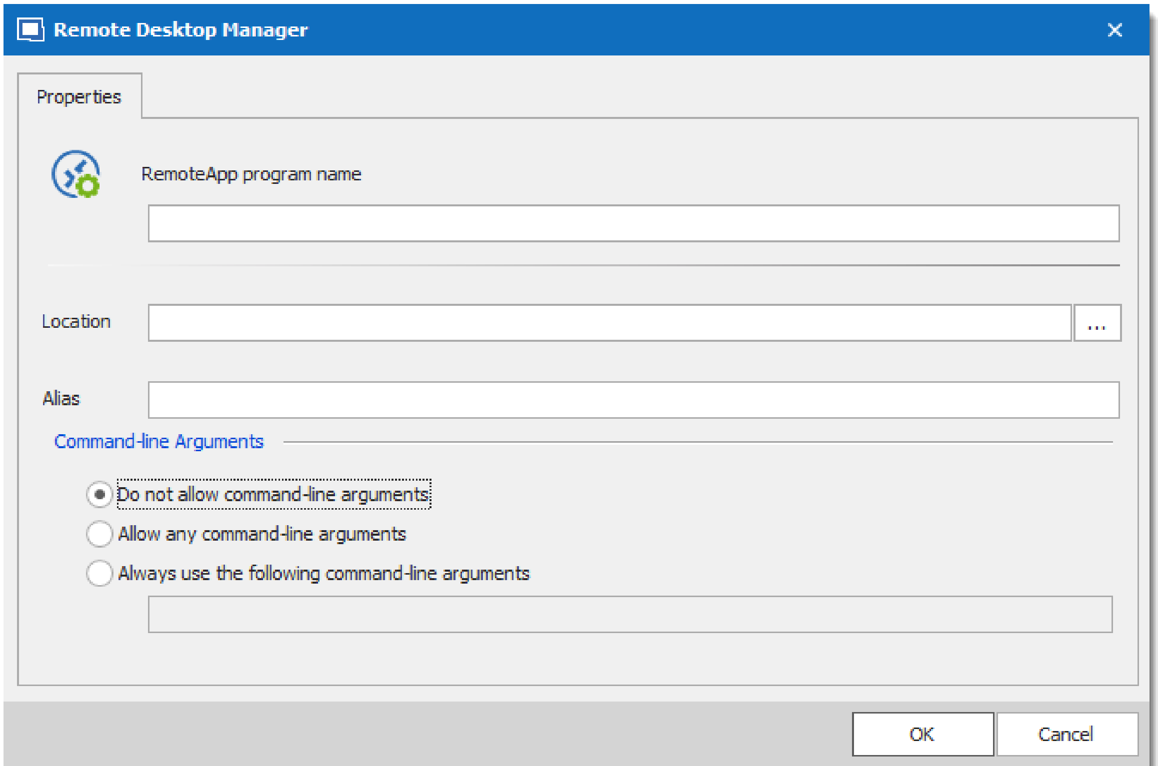
USAGE

1. Click on **New RemoteApp Settings.**

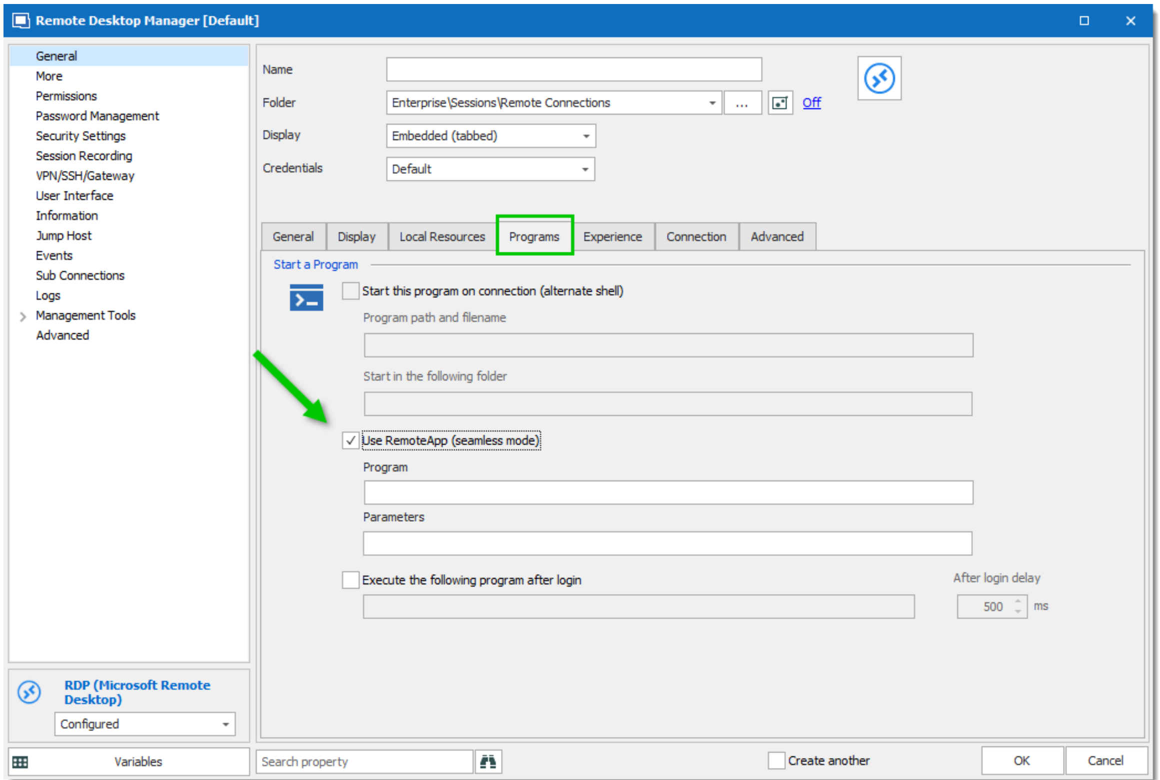


New RemoteApp Settings

2. Configure the RemoteApp



3. Create a new RDP session and select the **Programs** tab. Enable the **Use RemoteApp** option and then enter the name of the RemoteApp program and save the session. When the session is launched you will have the RemoteApp running locally.



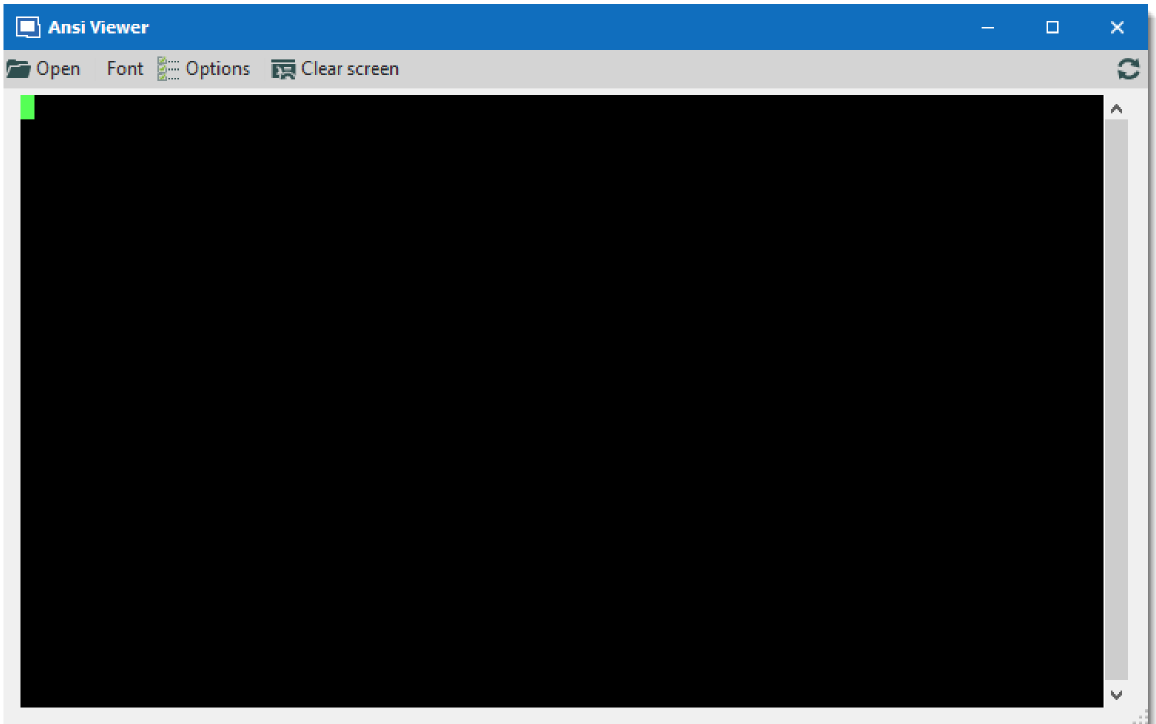
RDP session - Programs Tab

6.8.2.5.3 Playback (Ansi)

DESCRIPTION

The **Playback (Ansi)** is available in ***Tools – More Tools – Playback (Ansi)***.

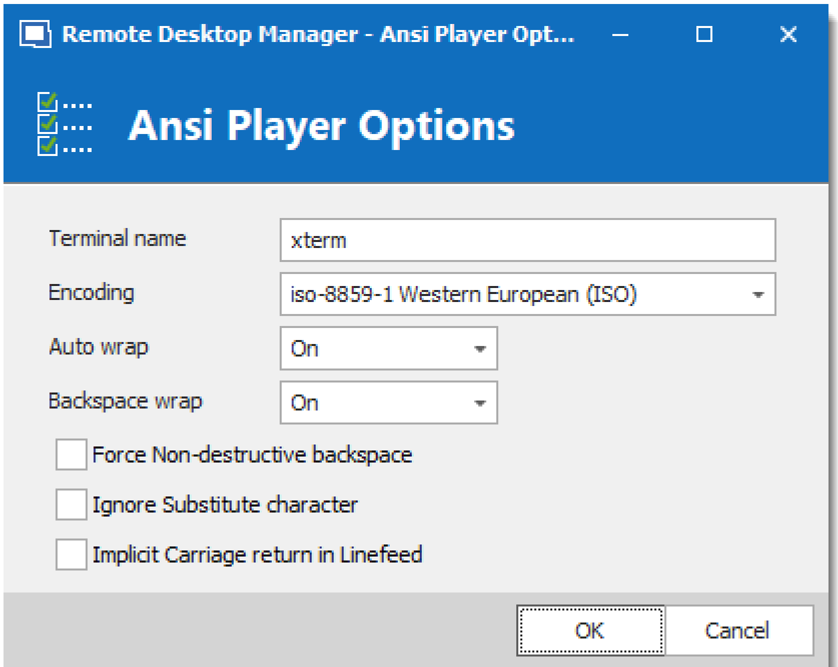
SETTINGS



More Tools - Playback (Ansi)

OPTION	DESCRIPTION
Open	Select the ansi file you wish to open in the Terminal Playback.
Font	Select the font for the Terminal Playback.
Options	See **Options** section.
Clear screen	Clear the screen to play another ansi file.

OPTIONS



Playback (Ansi) - Ansi Player Options

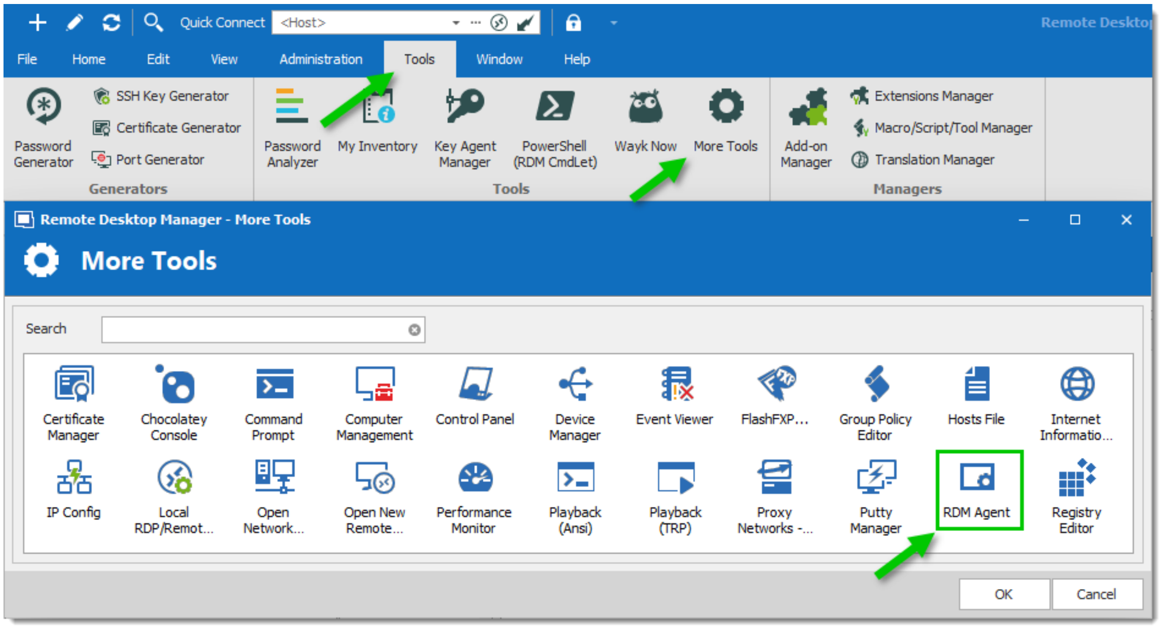
OPTION	DESCRIPTION
Terminal name	Indicate the terminal name.
Encoding	Indicate the encoding you wish to use.
Auto wrap	Indicate what happen when text reaches the right-hand edge of the window. Select between: • **On** • **Off** • **Dos**
Backspace wrap	This option allows you to choose what you want to do when you press backspace. Some terminals believe that the backspace key should send the same thing to the server as Control-H (ASCII code 8). Other terminals believe that the backspace key should send ASCII code 127 (usually known as Control-?) so that it can be distinguished from Control-H. Select between:

OPTION	DESCRIPTION
	• **On** • **Off** • **Dos**
Force Non-destructive backspace	Allow to perform a normal backspace without deleting a character.
Ignore Substitute character	Ignore the substitute character that can be use in Putty.
Implicit Carriage return in Linefeed	Most servers send two control characters, CR and LF, to start a new line on the screen. The CR character makes the cursor return to the left-hand side of the screen. The LF character makes the cursor move one line down (and might make the screen scroll). Some servers only send LF, and expect the terminal to move the cursor over to the left automatically. If you come across a server that does this, you will see a stepped effect on the screen. If this happens to you, try enabling the option and things might go back to normal.

6.8.2.5.4 RDM Agent

DESCRIPTION

The **Remote Desktop Manager Agent** is a very powerful tool that allows commands to be run on multiple machines.

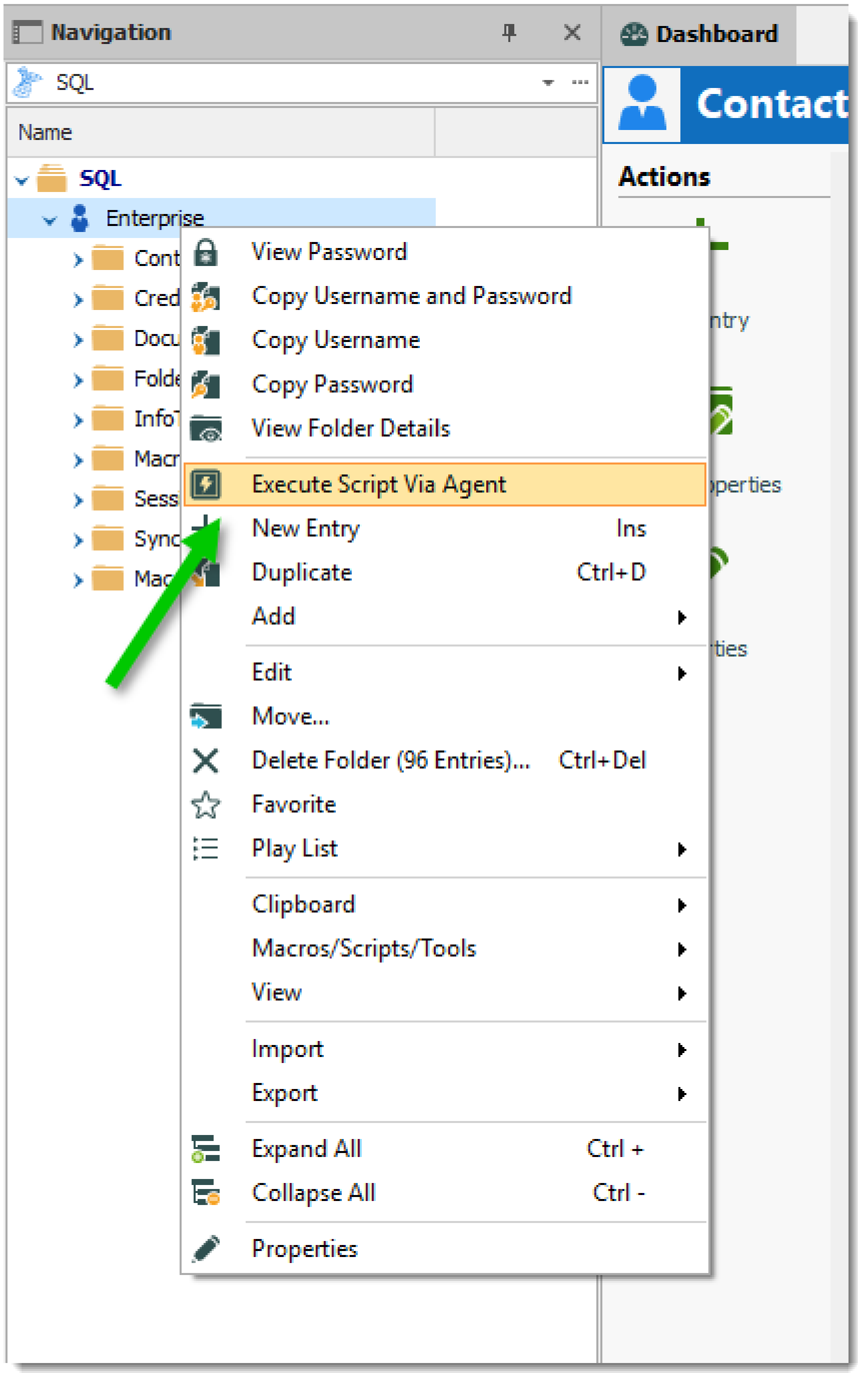


More Tools - RDM Agent

SETTINGS

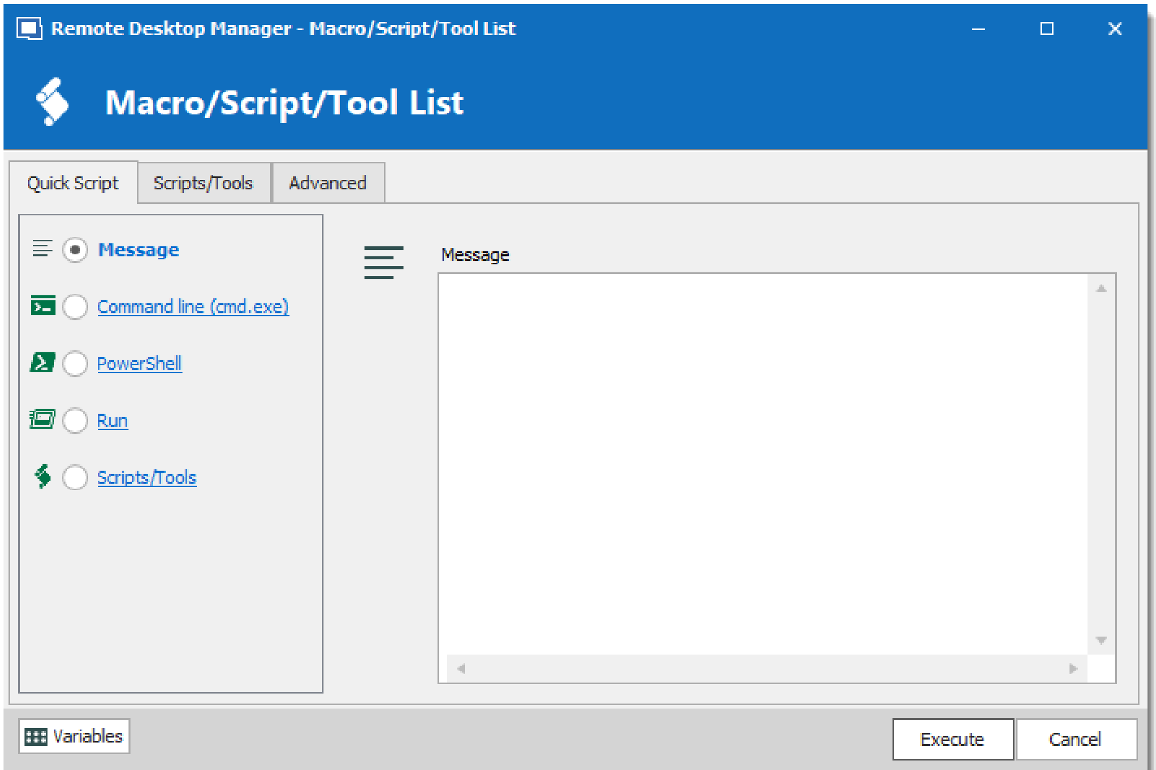
To launch a script through the **RDM Agent**, you first need to open an RDP connection to all the machines you wish to execute the script on. Once opened, select all the opened sessions in the Navigation Pane, right-click them and select Execute Script via Agent.

> Execute script via Agent only needs the RDM Agent when the script is executed from the Quick Script tab. RDM needs to be fully installed on the remote computer when the script is executed from the Scripts/Tools tab.



Execute Script Via Agent

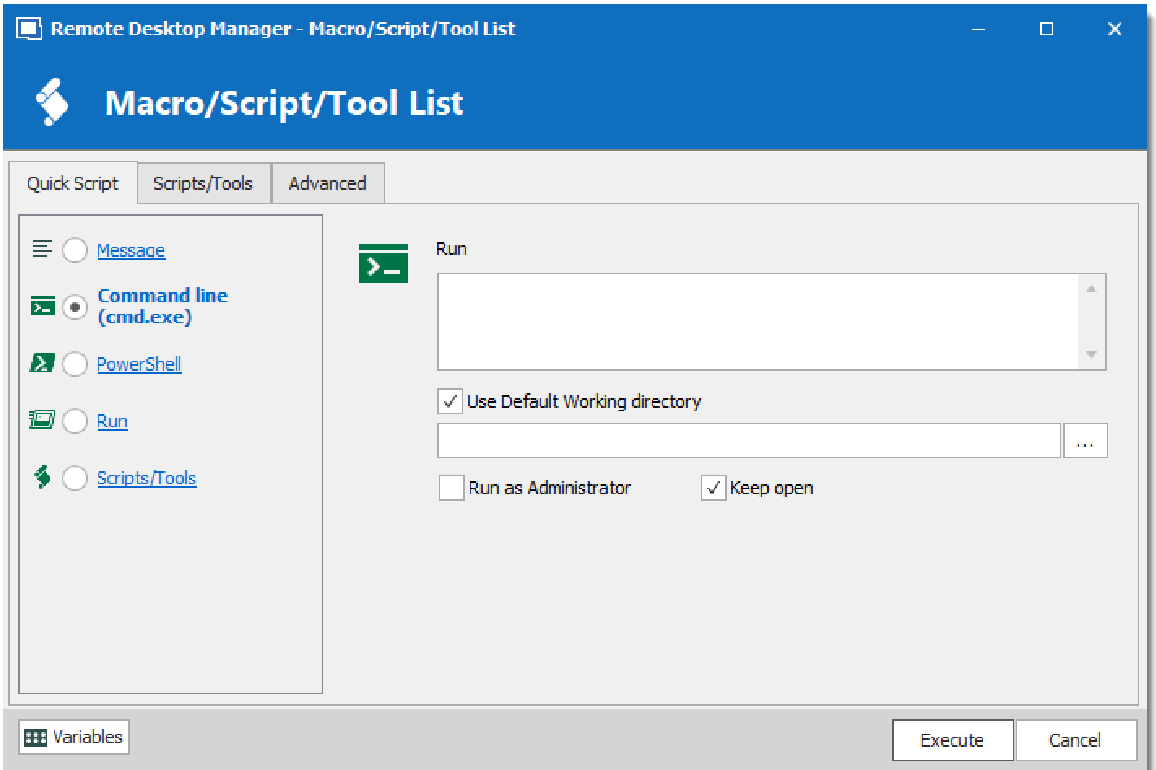
QUICK SCRIPT - MESSAGE



Quick Script - Message

OPTION	DESCRIPTION
Message	Send a message to all targets.

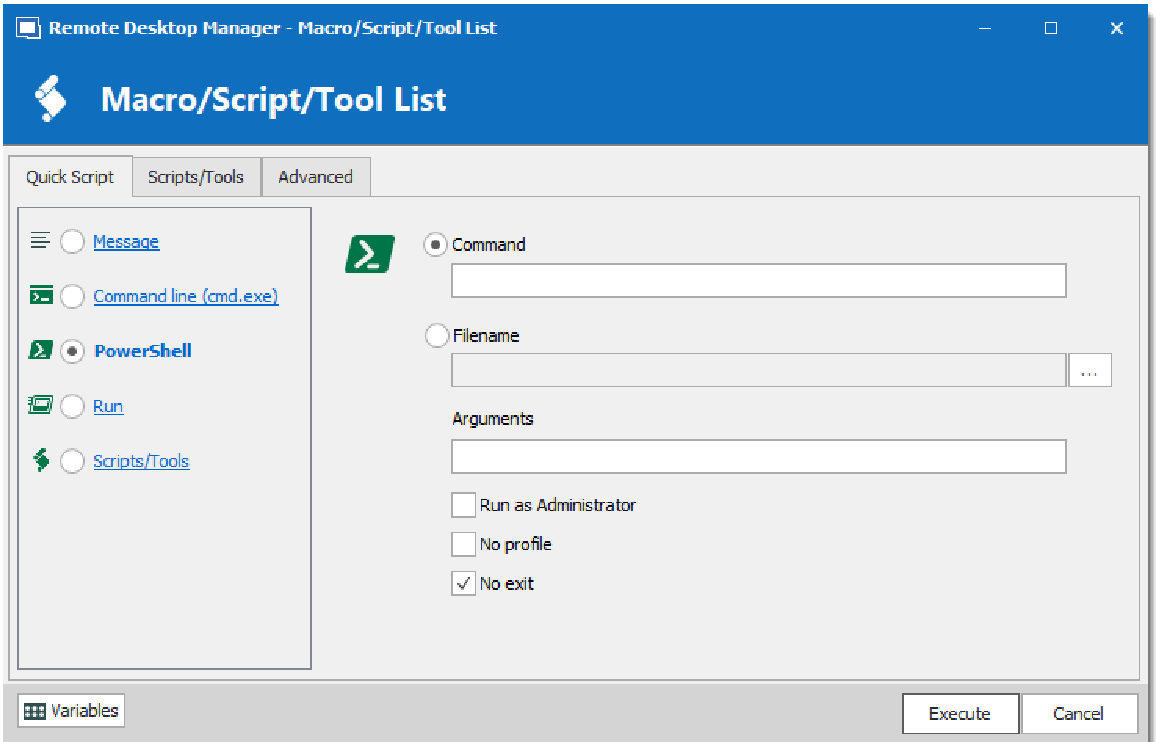
QUICK SCRIPT - COMMAND LINE (CMD.EXE)



Quick Script - Command Line

OPTION	DESCRIPTION
Run	Indicate the command line that you want to execute.
Use Default Working directory	Use the default working directory when connect to the session.
Run as Administrator	Elevates the process to run as an administrator.
Keep open	Keep the window open after the execution of the command line.

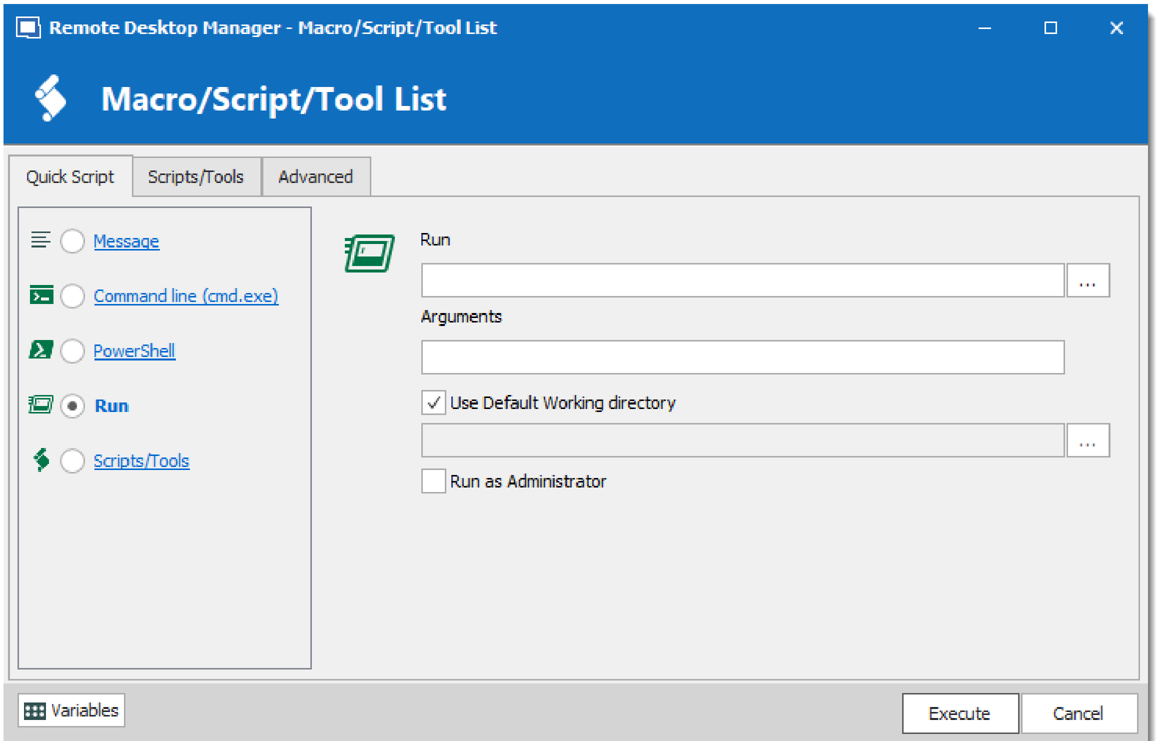
QUICK SCRIPT - POWERSHELL



Quick Script - PowerShell

OPTION	DESCRIPTION
Command	Indicate the PowerShell command that you want to execute.
Filename	Select a PowerShell file on the network or on the computer.
Arguments	Arguments that are appended to the Command.
Run as Administrator	Elevates the process to run as an administrator.
No Profile	Does not load the Windows PowerShell profile.
No exit	Does not exit after running startup commands.

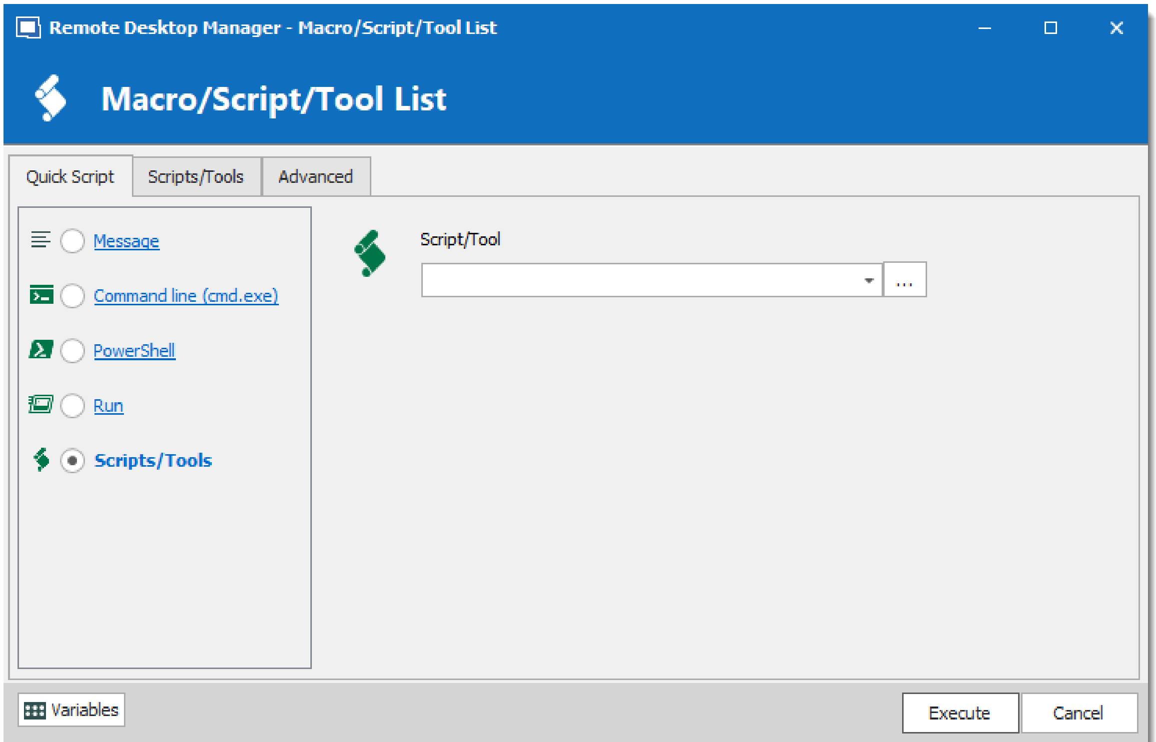
QUICK SCRIPT - RUN



Quick Script - Run

OPTION	DESCRIPTION
Run	Select the program or file that you want to execute.
Arguments	Arguments that are appended to the Command.
Use Default Working directory	Use the default working directory when connect to the session.
Run as Administrator	Elevates the process to run as an administrator.

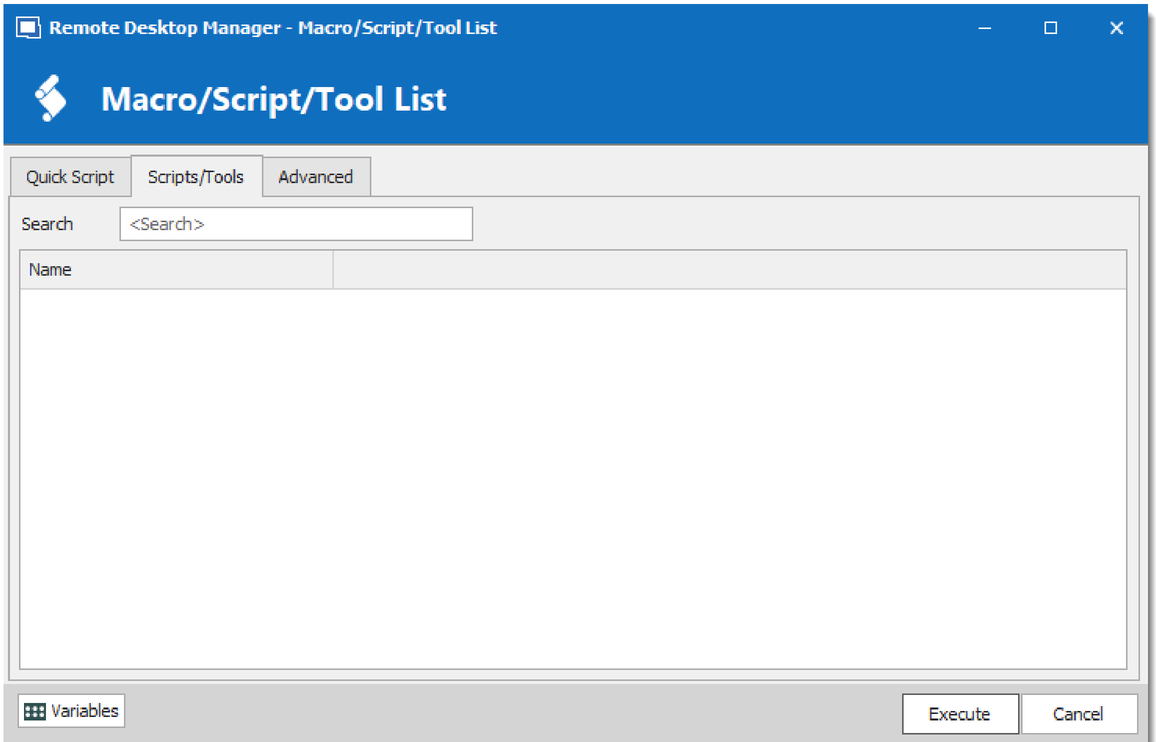
QUICK SCRIPT - SCRIPTS/TOOLS



Quick Script - Scripts/Tools

OPTION	DESCRIPTION
Scripts/Tools	Select a script or a tool session that you have already created in Remote Desktop Manager.

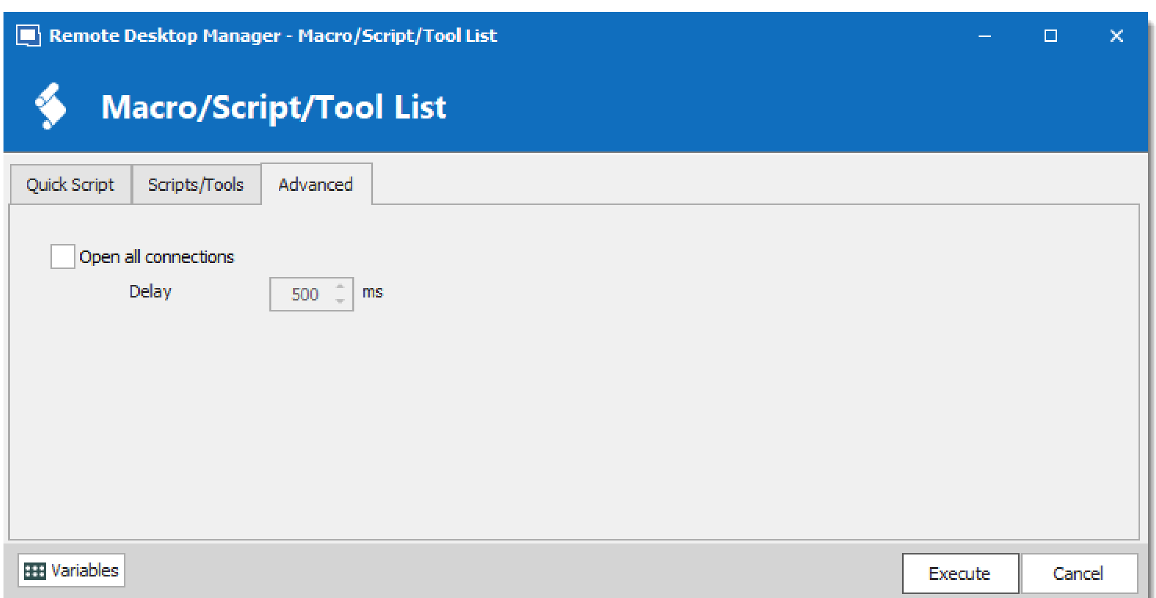
SCRIPT/TOOLS



Scripts/Tools

Search for a script or a tool you wish to execute through the RDM Agent.

SETTINGS

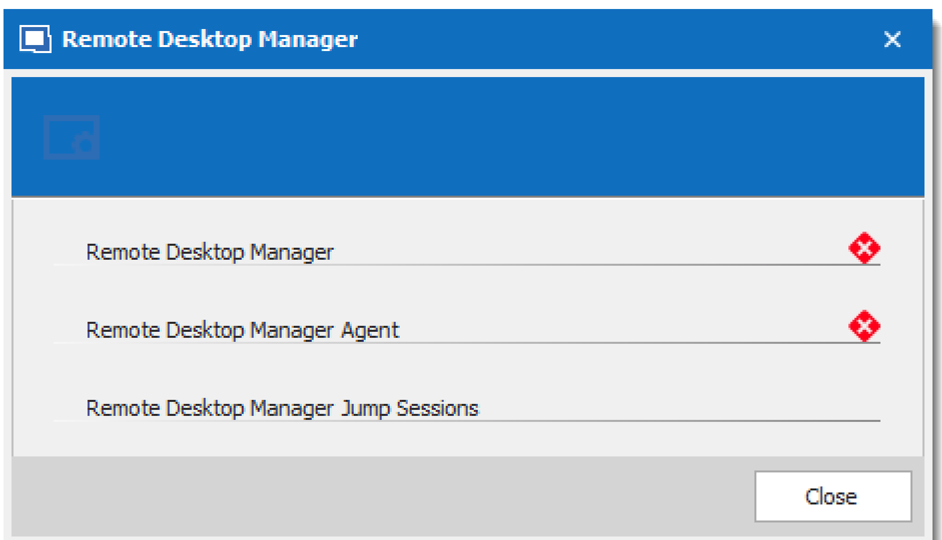


Advanced

OPTION	DESCRIPTION
Open all connections	When multiple sessions are selected to **Execute Script Via Agent**, it will open all the selected connections.
Delay	Enter the time delay between opening each selected session.

AGENT STATUS

Open a RDP session, right-click on this single session and select Agent Status. The Agent Status will show you that Remote Desktop Manager is installed on the remote computer or not, that the Remote Desktop Manager Agent is active or not and how many Remote Desktop Manager Jump sessions are opened.

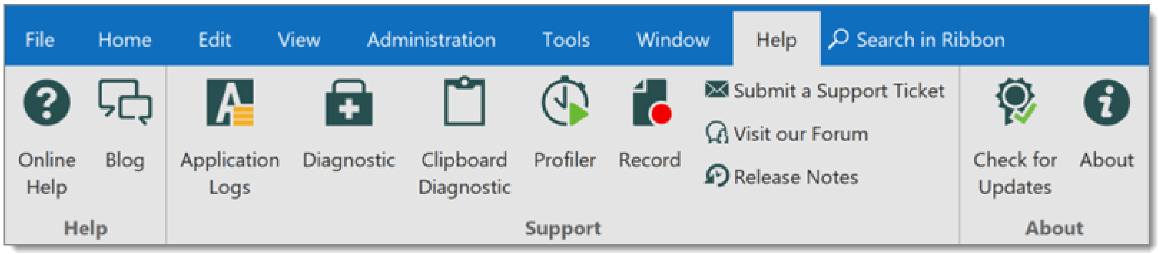


Agent Status

6.9 Help

DESCRIPTION

In the ***Help*** tab section you will find links to the ***Devolutions forum***, ***Blog***, ***Online Help*** and much more. Diagnostics tools for Remote Desktop Manager are all located in the ***Support*** section. many supported related features, such as the ***Application Logs***, the ***Profiler***, and the ***Recorder***.



Ribbon - Help

HELP

OPTION	DESCRIPTION
Online Help	Launches the Online Help documentation for Remote Desktop Manager.
Blog	Visit our Blog and learn about the Devolutions team, as well as our goals, products and more.

SUPPORT

OPTION	DESCRIPTION
Applications Logs	Opens the Application Logs to view encountered errors.
Diagnostic	Launches the Diagnostic feature.
Clipboard Diagnostic	The Clipboard Diagnostic tool helps to view all requests in real time and identify which application is involved with copy paste errors.
Profiler	Use the Profiler to acquire specific information. Used to diagnose connectivity issues with a data source.

OPTION	DESCRIPTION
Record	Use the Recorder to help our Devolutions Support team troubleshoot the problem.
Submit a Support Ticket	Submit a Support Ticket to help us make your experience better by reporting experience issues or by asking for new features.
Visit our Forum	Visit our Forum for help and exchange with the Devolutions community.
Release Notes	Send you directly to our Remote Desktop Manager web page to view the new features and enhancements when a new version is released.

ABOUT

OPTION	DESCRIPTION
Check for Updates	Validate if a Remote Desktop Manager update is available.
About	Learn about Remote Desktop Manager.

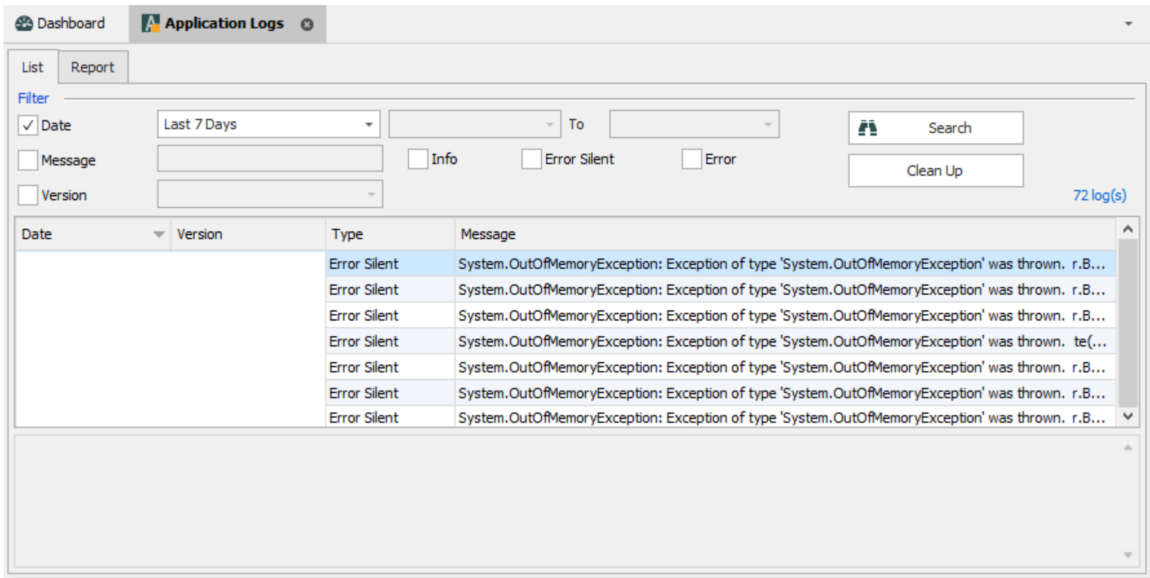
6.9.1 Support

6.9.1.1 Application Log

DESCRIPTION

When encountering errors, you can verify the local application log, which is available in ***Help – Application Logs***.

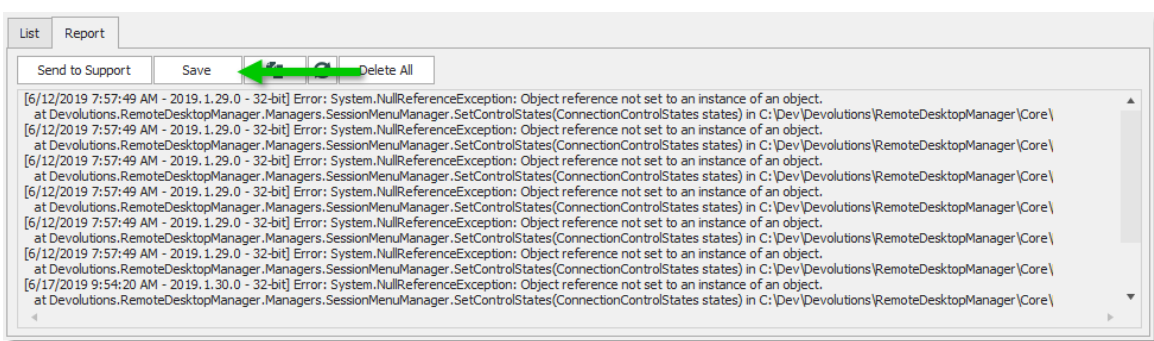
These logs are saved in ***%LocalAppData%\Devolutions\RemoteDesktopManager\RemoteDesktopManager.log.db***. Logs are displayed as a list which can be filtered by date, message, version,or type of log.



View Application Log dialog

REPORT

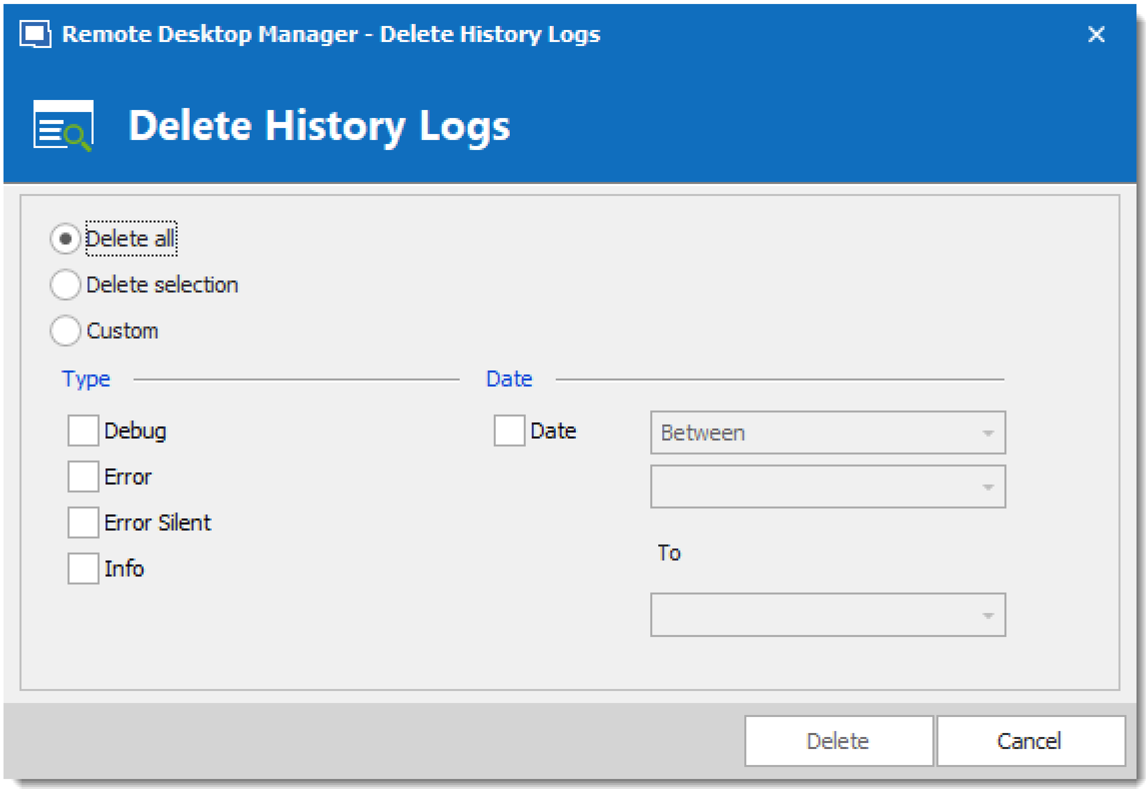
A report of the logs can be saved in a text file as well. Simply navigate to the **Report** tab of the application log, then click on the **Save** button to select a location to save the file.



CLEAN UP

For security reason, it is a best practice is to clean up the application log once every month. To do so, in the application log, use the **Clean Up** feature.

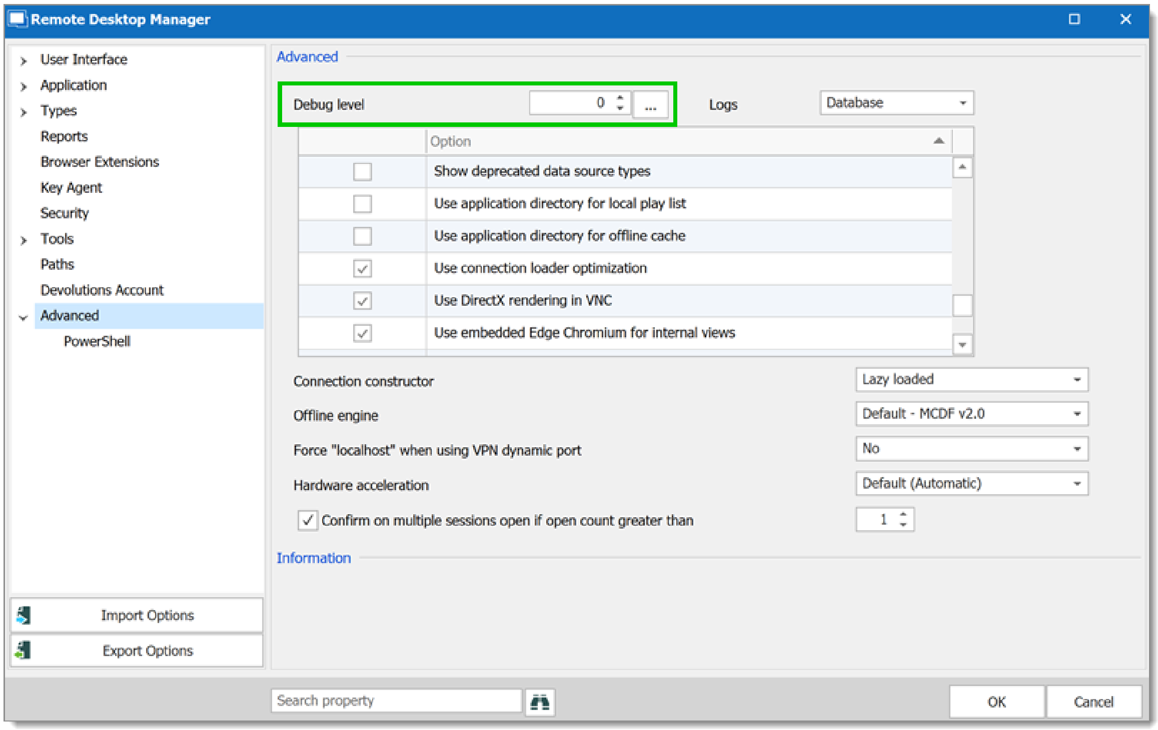
We strongly recommend to do a **Delete all**, but this can be customized to delete specific logs by type, date or selection.



INCREASING THE DEBUG LEVEL

When experiencing issues with Remote Desktop Manager our support team might ask you to increase the debug level of the application during the support process. We strongly suggest to only increase the debug level when requested by our support team.

Increase the debug level in File - Options - Advanced.



File – Options – Advanced – Debug level

6.9.1.2 Diagnostic

DESCRIPTION

If you encounter a problem with Remote Desktop Manager, you can run a system diagnostic, which is available in ***Help – Diagnostic.*** This could help diagnose or give a pointer to what kind of issues you might be experiencing.

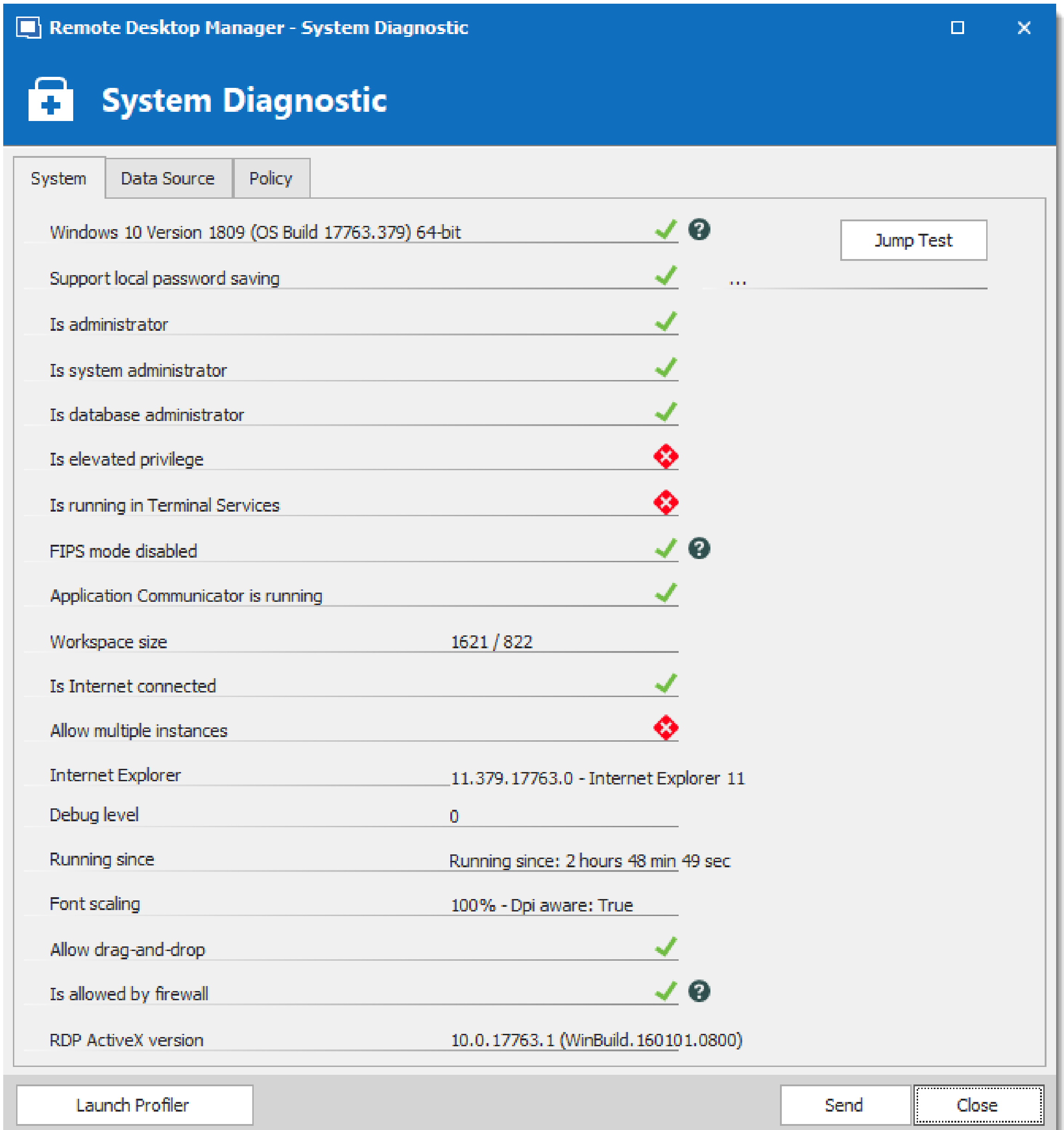
SYSTEM

The administrator item could be the possible source for security problem. This happen often when a user has the SYSDBA or is DB_OWNER of the SQL Server database.

Some other issues could be related to the fact that the application is running in Remote Desktop Services. However Remote Desktop Manager is fully compatible with Remote Desktop Services.

FIPS related issues and solutions can be found in the specific FIPS (Encryption) troubleshooting section.

If you have a Remote Desktop Manager Jump configured you can run a test of your Jump host by clicking on Jump Test.



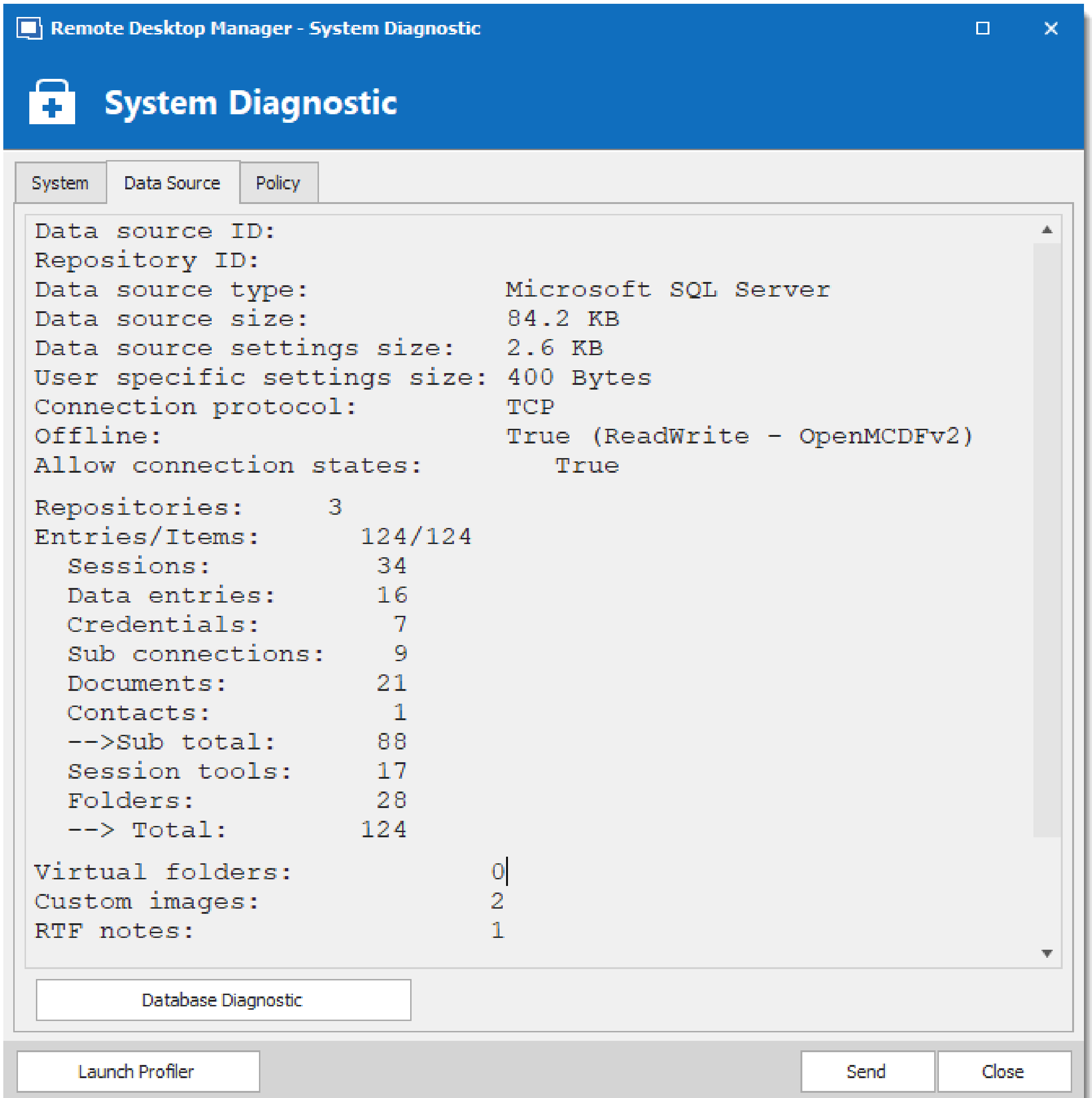
System Diagnostic – System

Please read the Troubleshooting topic if experiencing issues with Remote Desktop Manager, it lists error messages and could contain the fix/workaround for your problem.

DATA SOURCE

The **Data Source** tab contains information regarding the current data source, such as the number of entries it contains, the size of your data source, the number of custom images and the offline state.

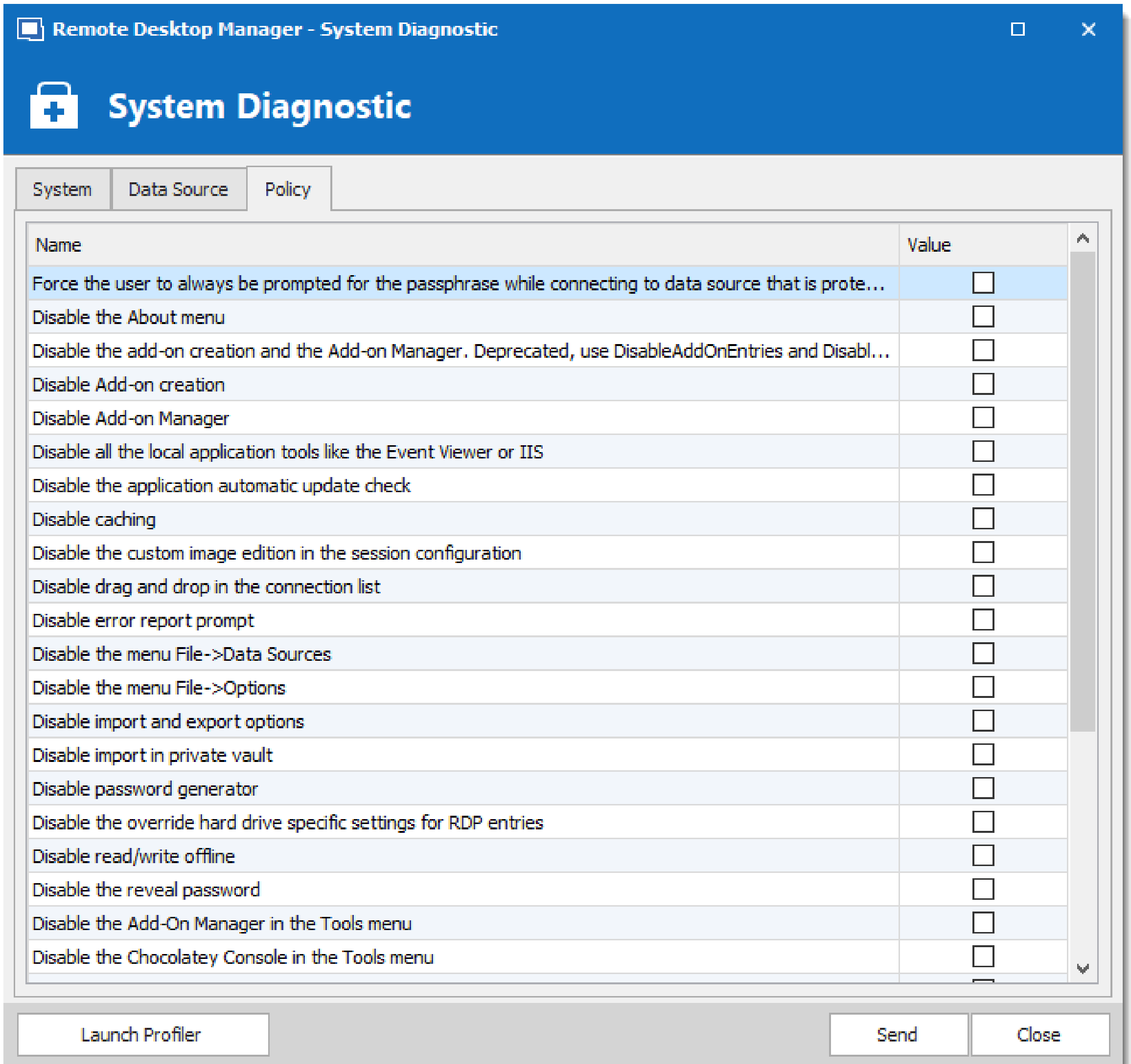
Too many custom images could dramatically increase the size of the data source and cause load time issue.



System Diagnostic - Data Source

POLICY

The Policy tab display the list of Group Policy Templates to see if any of them has been applied.



System Diagnostic - Policy

6.9.1.3 Profiler

DESCRIPTION

Remote Desktop Manager has a built-in profiler to diagnose connectivity issues with a data source.

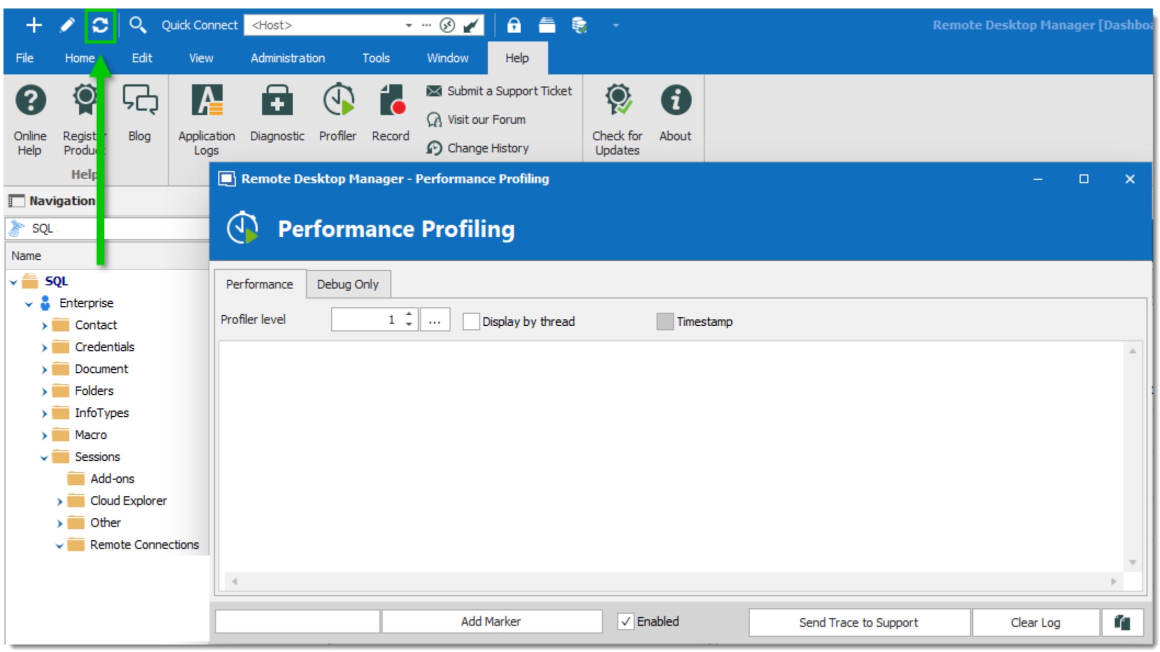
> Displaying the Profiler window might slow down the operations on the data source. Proceed with care.

To diagnose startup issues, you can enable the profiler from the command line as described in Command Line Arguments

PROCEDURE

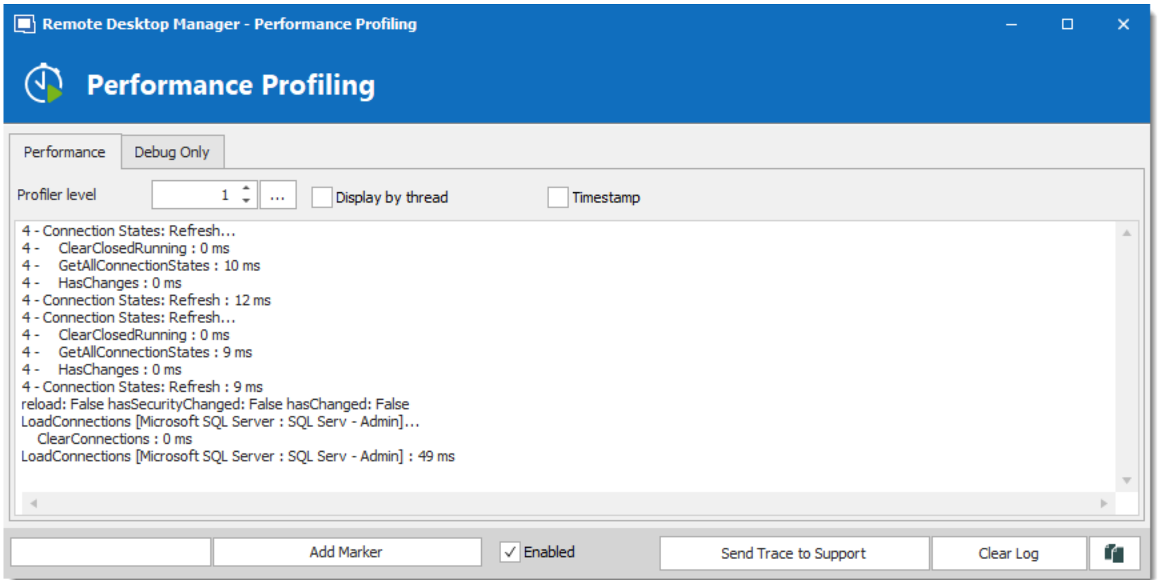
1. Once the Profiler is opened, refresh the data source.

Holding the **Ctrl** key while performing the refresh should force a full reload of the data source, recreating the offline cache.



Refresh Data Source

2. The Profiler data will appear in the **Performance Profiling** window.

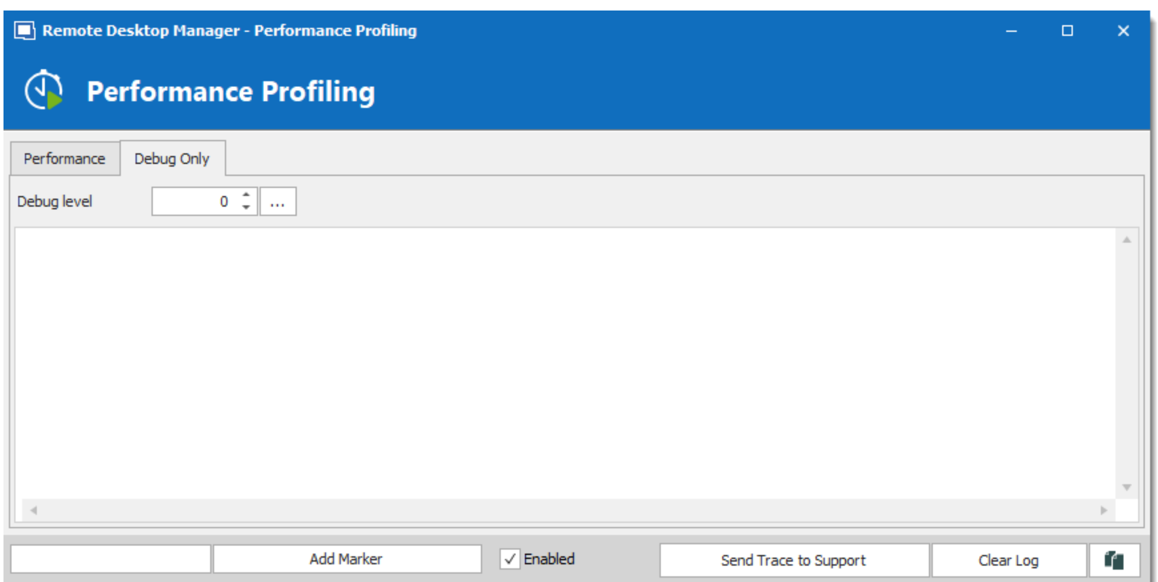


Performance Profiling

3. Click on **Send Trace to Support** in order to send the Profiler data logs to our Devolutions support team. You can add a Marker when running multiple tests to separate them.

DEBUG ONLY

To learn more about the **Debug only** tab please see the Debugging topic.



Debug only

6.9.1.4 Record

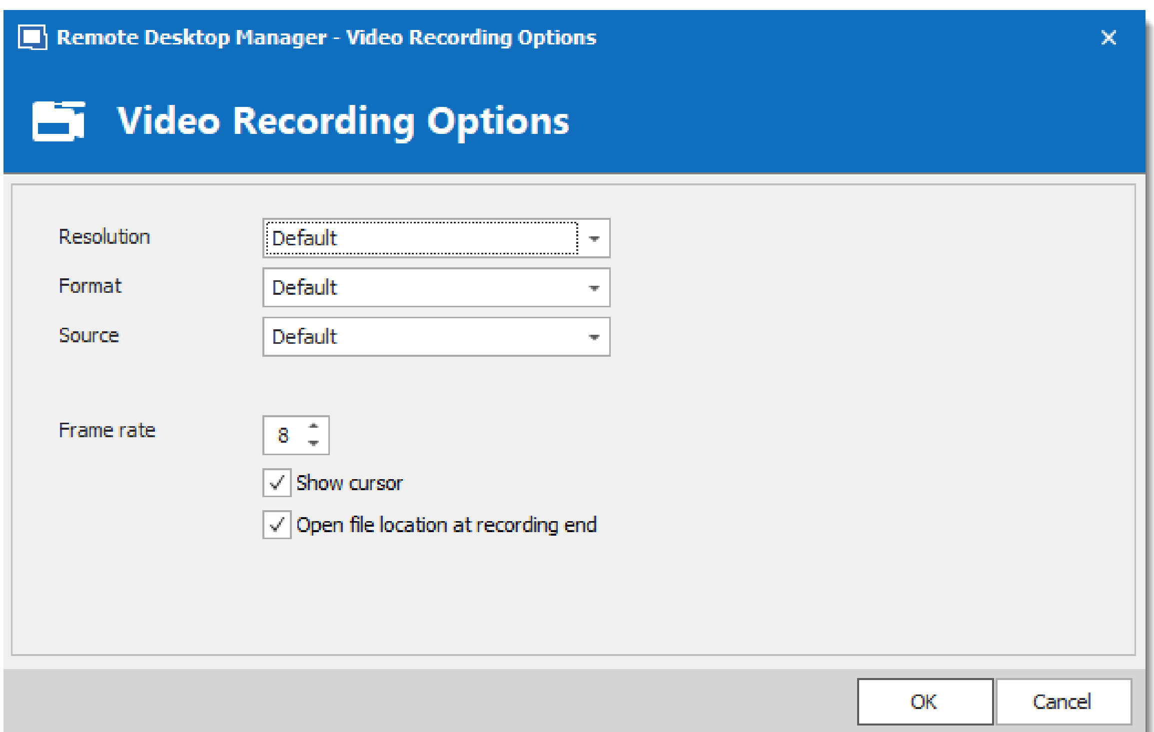
DESCRIPTION

If you are experiencing issues with Remote Desktop Manager, you can help our Devolutions Support team troubleshoot the problem by sending them a short video of your issue. Launch this by using the **Record** feature located in the menu ***Help – Record.***

The **Record** is an easy-to-use built-in screen recorder that could even be a useful for your in-house training as it is not limited to Remote Desktop Manager.

SETTINGS

The Video Recording Options uses the MP4 format, which on Vanilla installs of Windows is not supported. If you encounter any difficulty viewing the video we strongly suggest the use of a VLC player.



Video Recording Options

Devolutions Web Login

Part

VII

7 Devolutions Web Login

7.1 Overview

DESCRIPTION

Devolutions Web Login is a web browser password plugin used in conjunction with Remote Desktop Manager, Devolutions Server and Password Hub, which allows users to securely inject passwords into websites using credentials stored in their vaults.

It gives system administrators full control over the management of passwords, without affecting the user's productivity.

Remote Desktop Manager Centralize, Manage and Secure Remote Connections	**Devolutions Server** Secure, Manage and Monitor Access to Privileged Accounts	**Password Hub** Vault and Manage Business-User Passwords
Remote Desktop Manager centralizes all remote connections on a single platform that is securely shared between users and across the entire team.	Devolutions Server lets you control access to privileged accounts and manage remote sessions through a secure solution that can be deployed on-premises.	Password Hub is a secure and cloud-based password manager for teams.

Advanced users, other browser extensions, or even JavaScript injection can all result in the password being read from the password edit control, even if it displays dots instead of the password. Any use of an external browser must be carefully weighed against your security requirements.

7.2 Installation

DESCRIPTION

Devolutions Web Login is a free browser extension companion tools. It does require one of our products to function at this time.

Click on the browser link below to start the installation of Devolutions Web Login plugin:

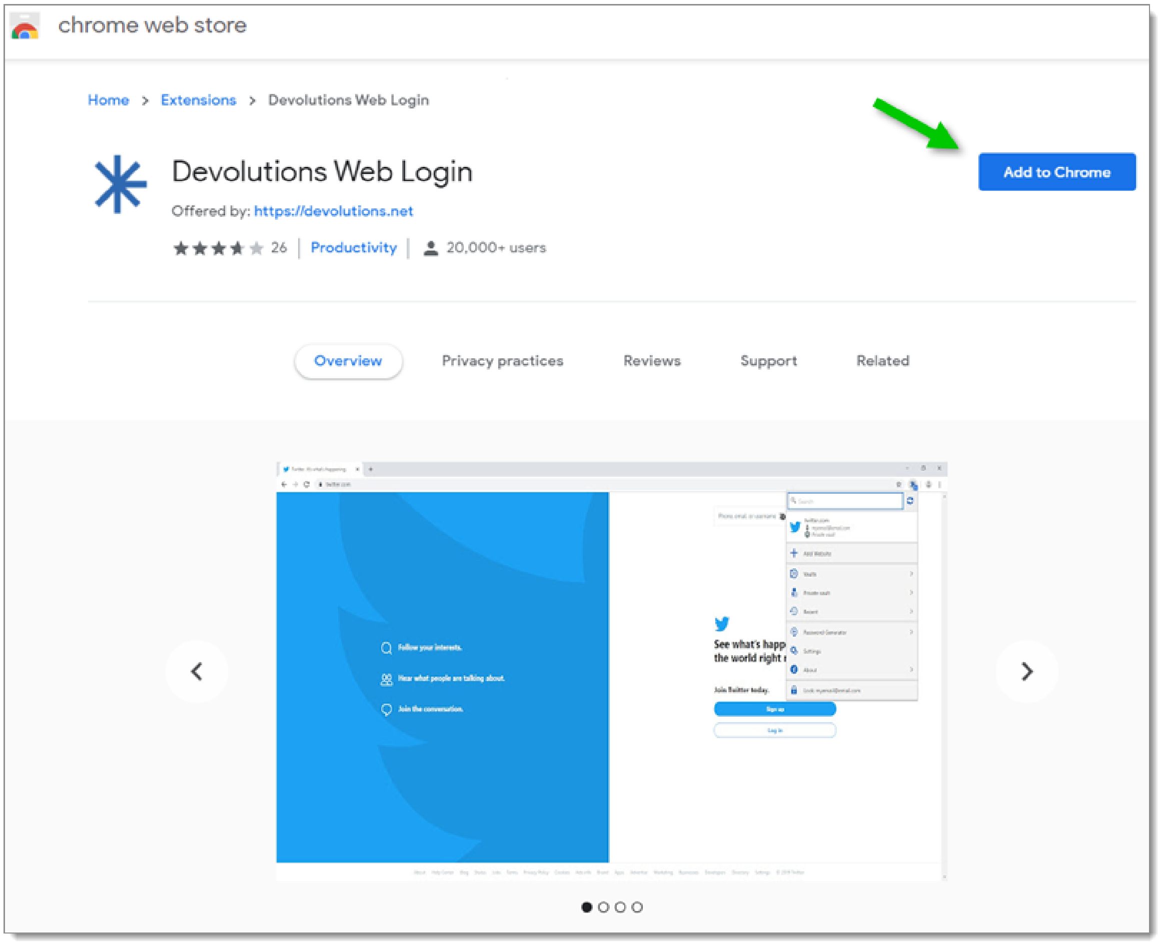
- Chrome
- Firefox
- Edge
- Opera

7.2.1 Chrome

DESCRIPTION

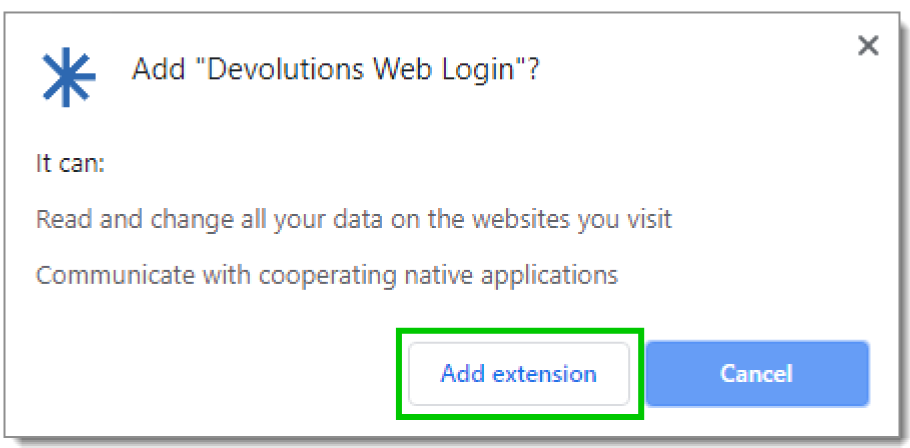
Follow the steps below to complete the installation of Devolutions Web Login in the Chrome web browser.

1. Open Chrome.
2. Navigate to Devolutions Web Login extension or use the link from our Website.
3. Click the ***Add To Chrome*** button.



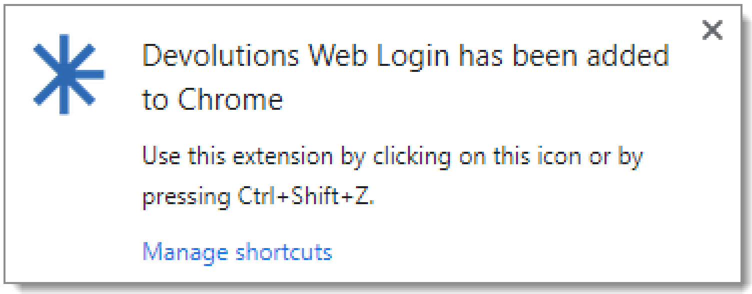
Devolutions Web Login Chrome Web Store

4. Click ***Add extension*** in the confirmation dialog.

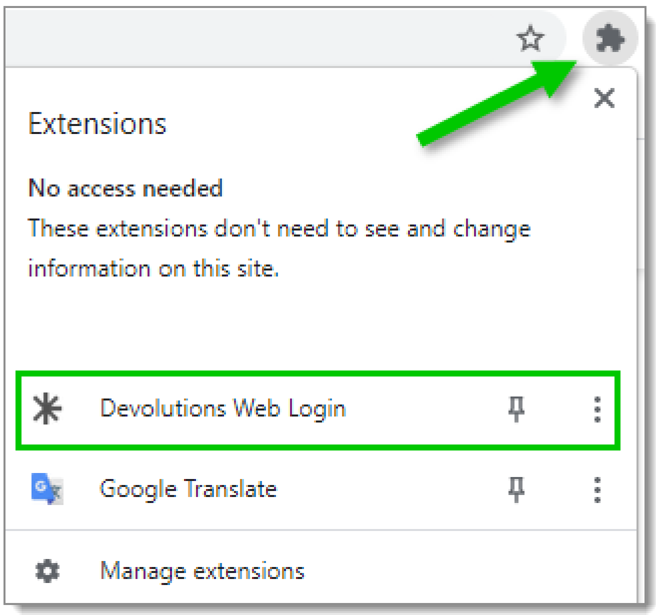


Extension Installation Confirmation

Once installed a confirmation box will appear.



5. Click the Chrome extension button and ***Pin*** Devolutions Web Login to finish the installation.



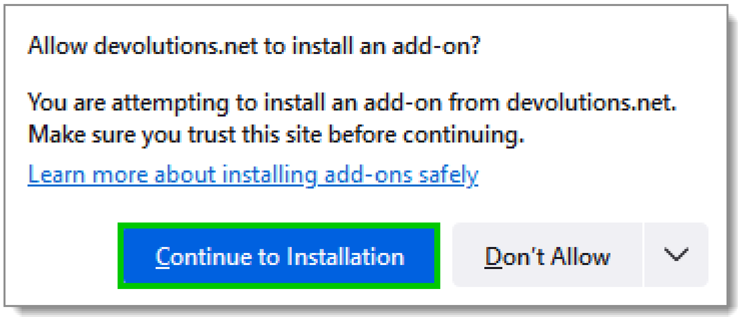
Devolutions Web Login Extension Button

7.2.2 Firefox

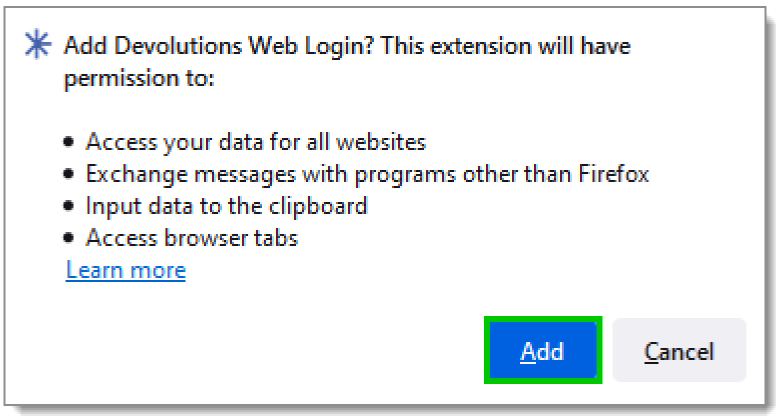
DESCRIPTION

Follow the steps below to complete the installation of Devolutions Web Login in the Firefox web browser.

1. Open a Firefox window.
2. Download the extension from our [Devolutions Web Login] website page.
3. Click ***Continue to Installation*** in the confirmation dialog.

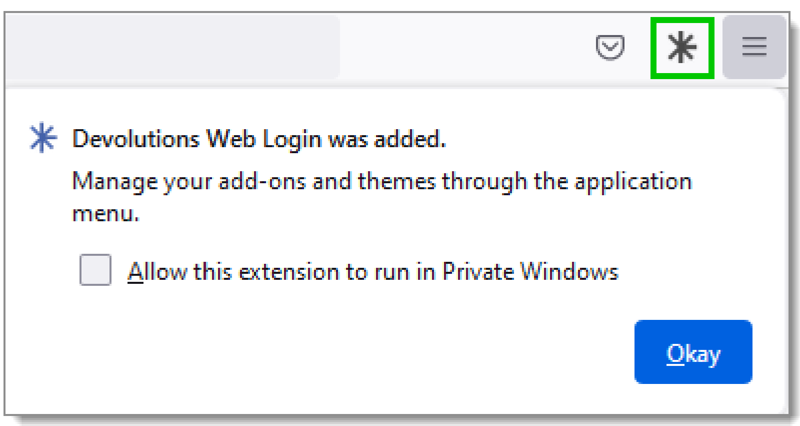


4. Click ***Add***, when prompted to add Devolutions Web Login to the extension.



Add the Extension

5. Once installed, access the extension by clicking in the top-right corner of Firefox.



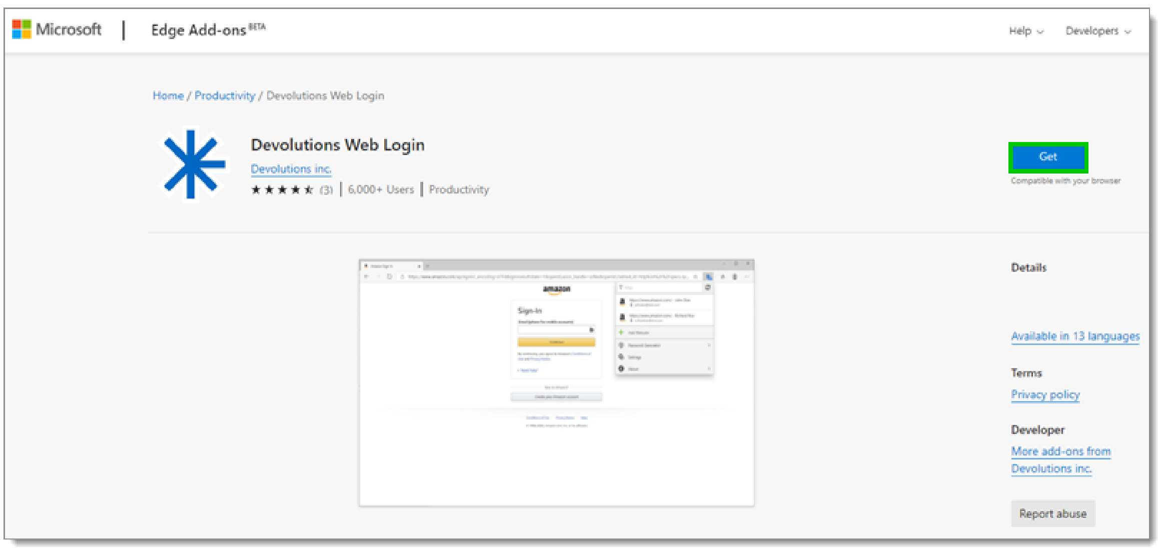
Devolutions Web Login Extension Button

7.2.3 Edge

DESCRIPTION

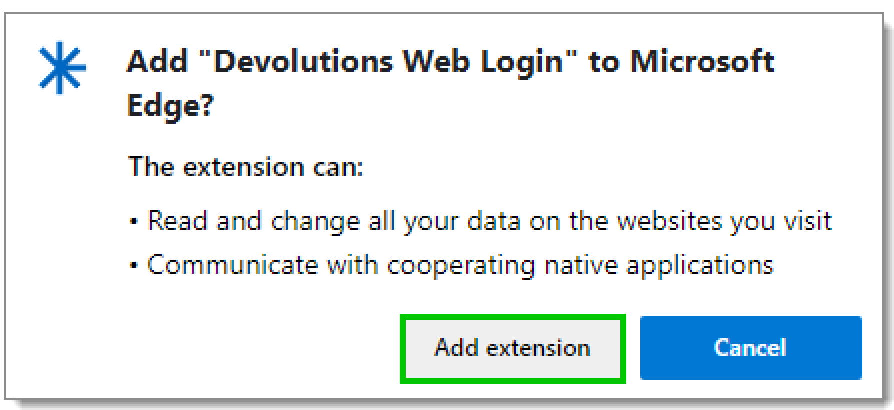
Here are the steps to install Devolutions Web Login on Microsoft Edge.

1. Open a Microsoft Edge window.
2. Download the extension from Devolutions Web Login website page.
3. Click ***Get***.



Chrome Web Store

4. Add the extension to Microsoft Edge.



Add Devolutions Web Login to Microsoft Edge Beta

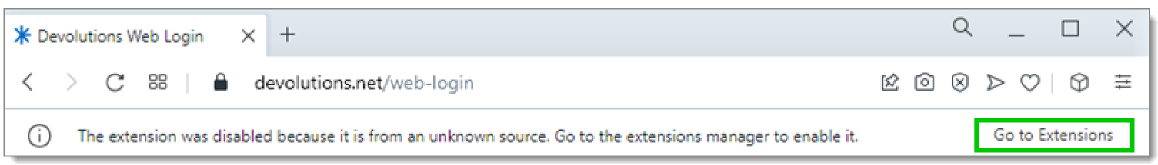
The extension is installed. Access it by clicking in the top-right corner of the Microsoft Edge web browser.

7.2.4 Opera

DESCRIPTION

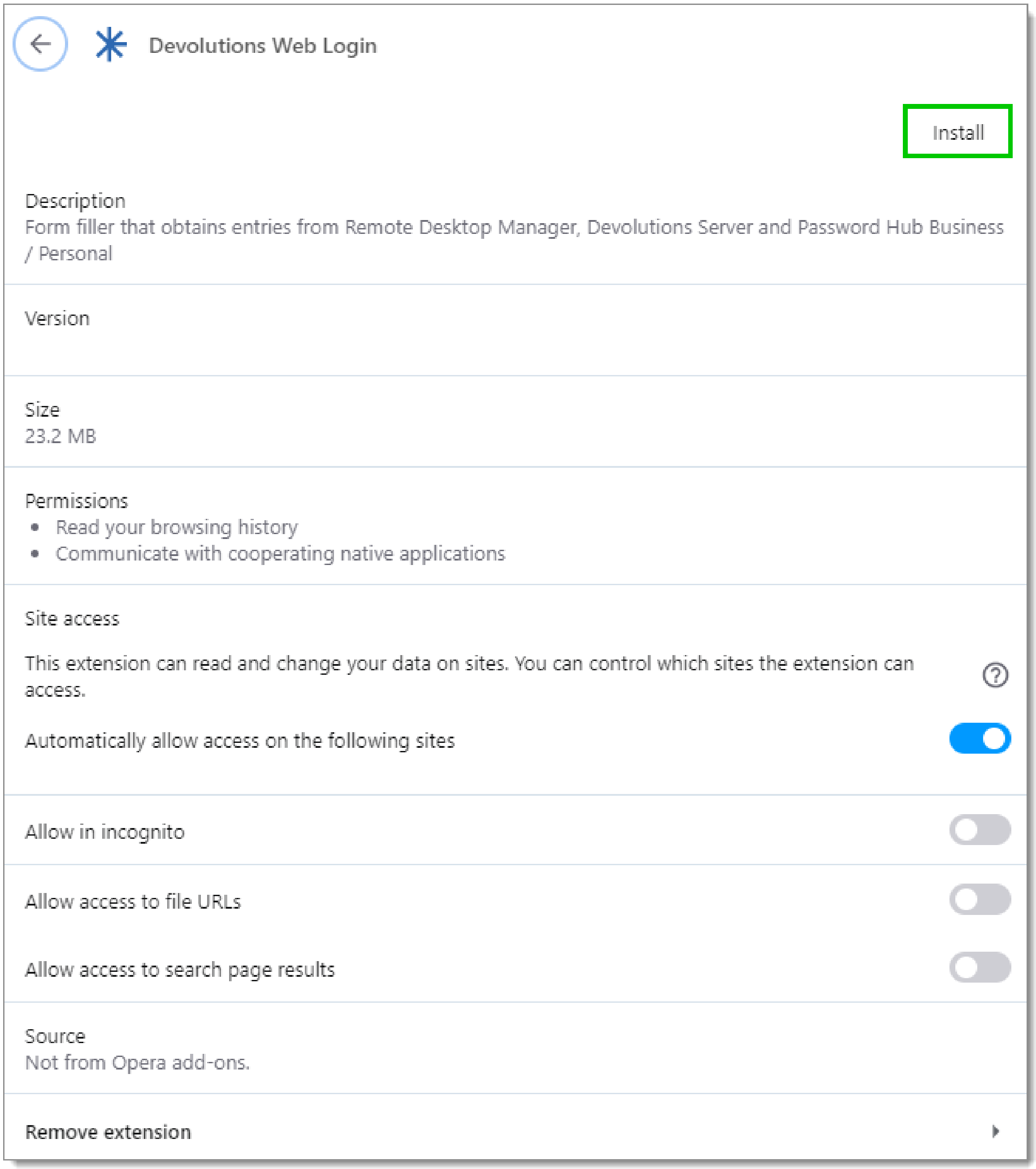
Follow the steps below to complete the installation of Devolutions Web Login in the Opera web browser.

1. Open Opera.
2. Download the extension of Devolutions Web Login from our website page.
3. Click on ***Go to Extension*** from the information panel at the top or click on the Extension button



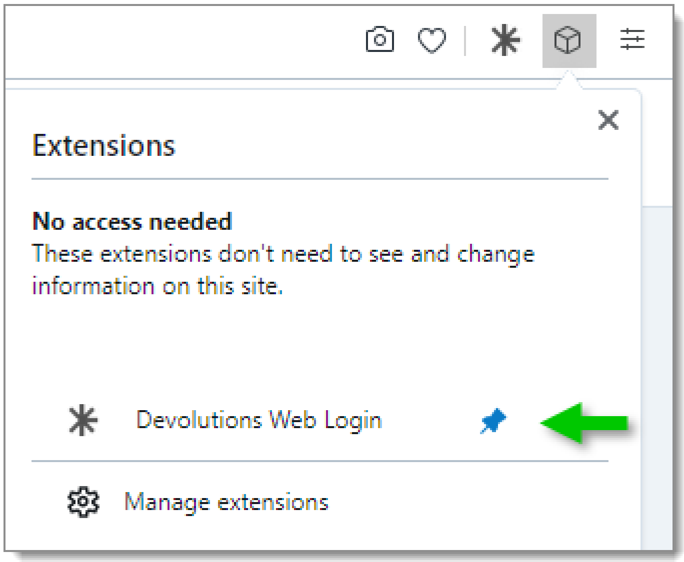
Opera Extensions Enabling

4. Click ***Install*** and the ***Yes, install*** pop up.



Opera Install Window

5. Click on the ***Extensions*** button of the browser and ***Pin*** the Devolutions Web Login extension.



Access the extension by clicking in the top-right corner of Opera.

7.3 First Login

7.3.1 Password Hub Business Login

DESCRIPTION

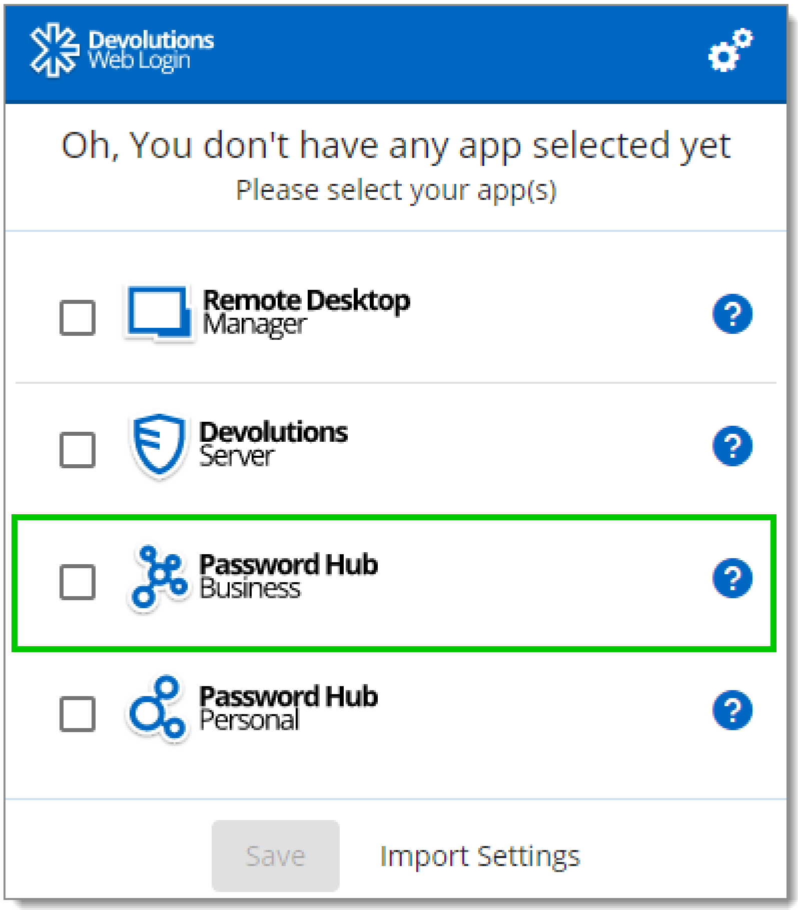
FIRST LOGIN WITH DEVOLUTIONS WEB LOGIN

Follow these steps to connect Password Hub Business to Devolutions Web Login extension:

1. Click on ***Devolutions Web Login*** extension at the top right corner of your browser.

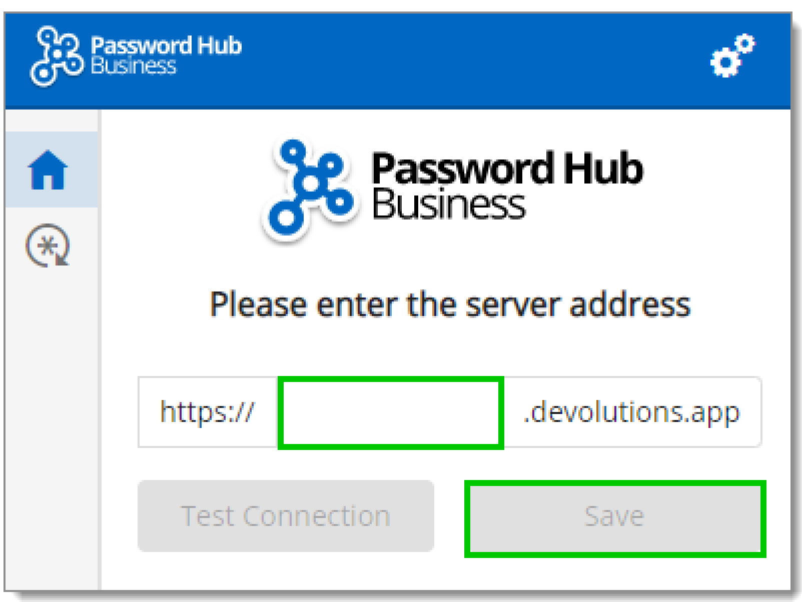
> A Password Hub Business access is required to continue.

2. Choose ***Password Hub Business*** in the list and ***Save***.



First Login

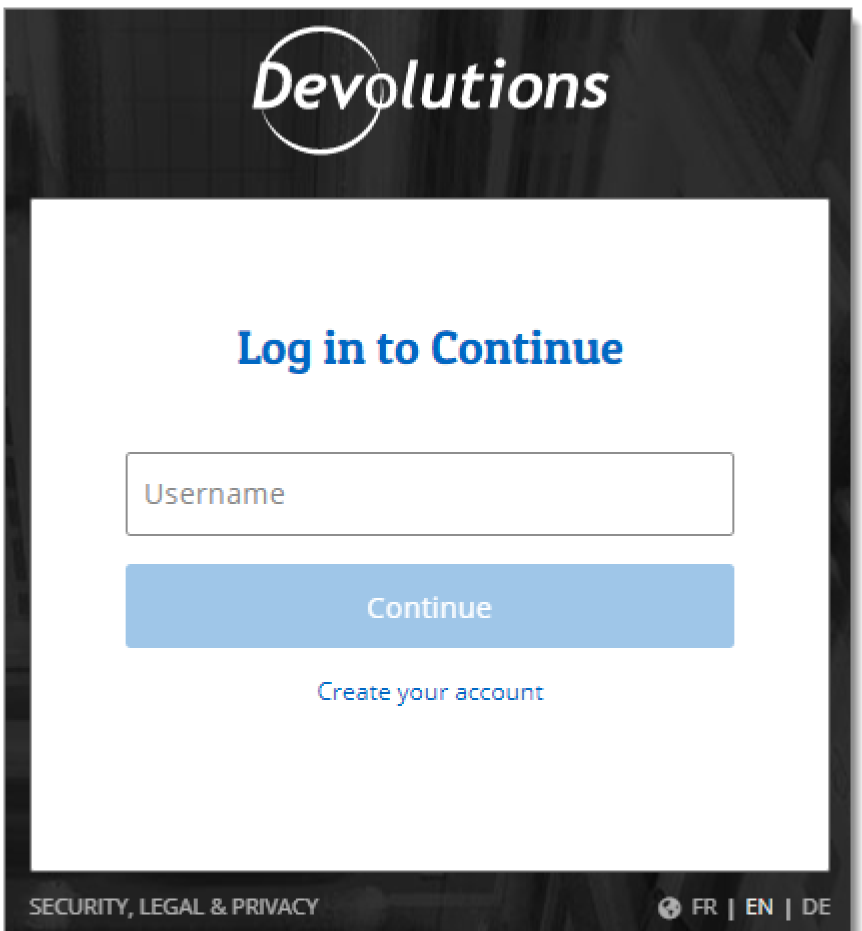
3. Enter your Password Hub Business server address and ***Save***.



4. ***Log in*** to your Devolutions Account.

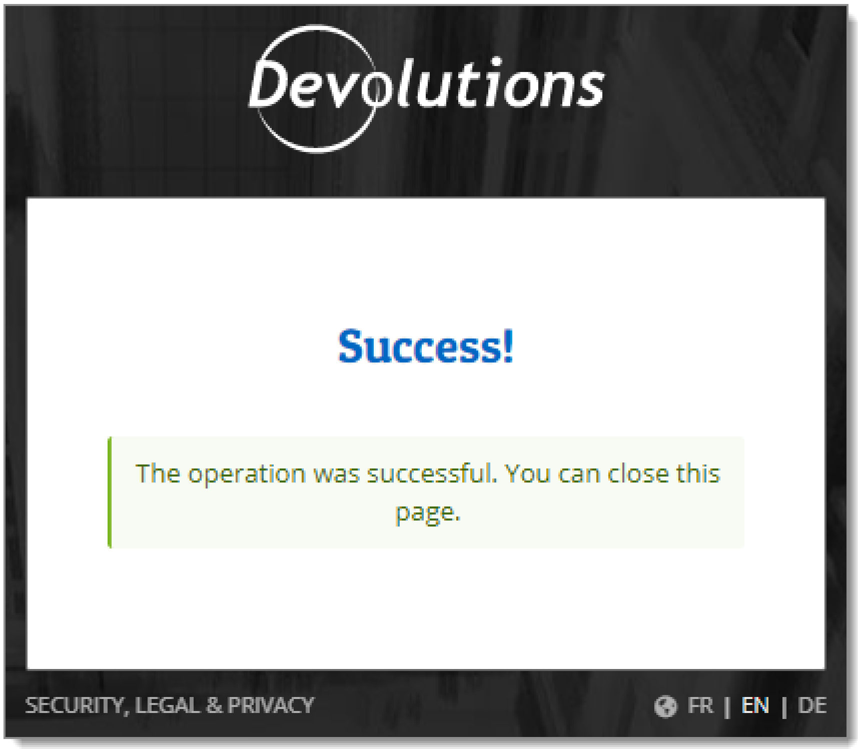
Log In

5. Enter the credentials from your Devolutions Account to continue.

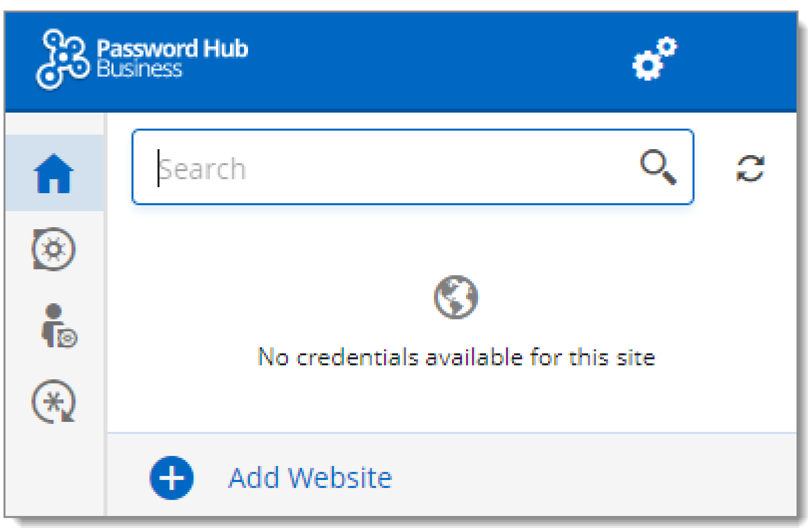


Devolutions Account Login

6. When complete, a log in confirmation message will appear.

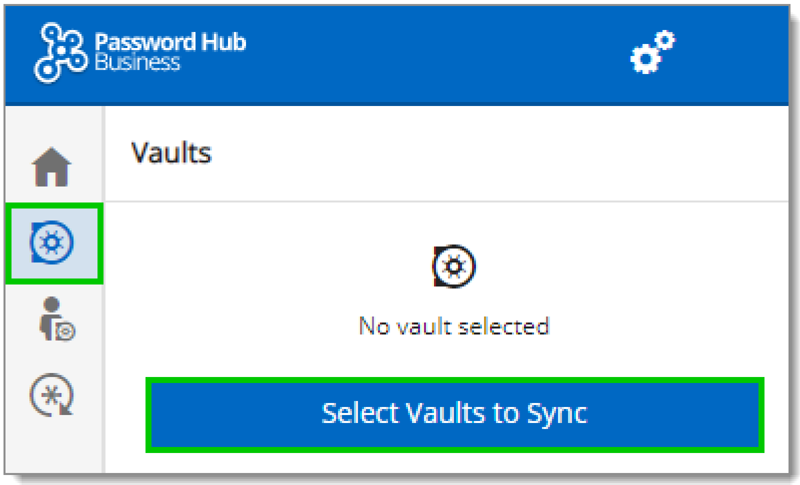


7. If you click on the ✱ icon, you can validate that Devolutions Web Login is now connected to your Password Hub Business.

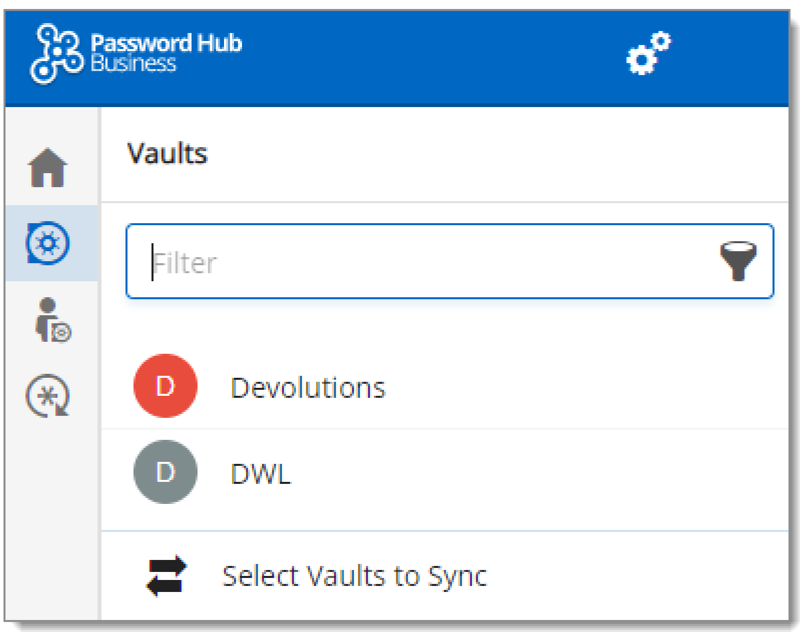


Devolutions Web Login Connected to Password Hub Business

8. To select the vaults to be synchronized, click on the ***Vaults*** icon and the ***Select Vaults to Sync*** button. Afterward, you click on the ***Select all*** button, or refine your view by adding a check mark next to the specific vaults to synchronize.



9. When done selecting your vaults, click on the ***Select Vaults to Sync*** at the top of the panel, to get the following view.



7.3.2 Password Hub Personal Login

DESCRIPTION

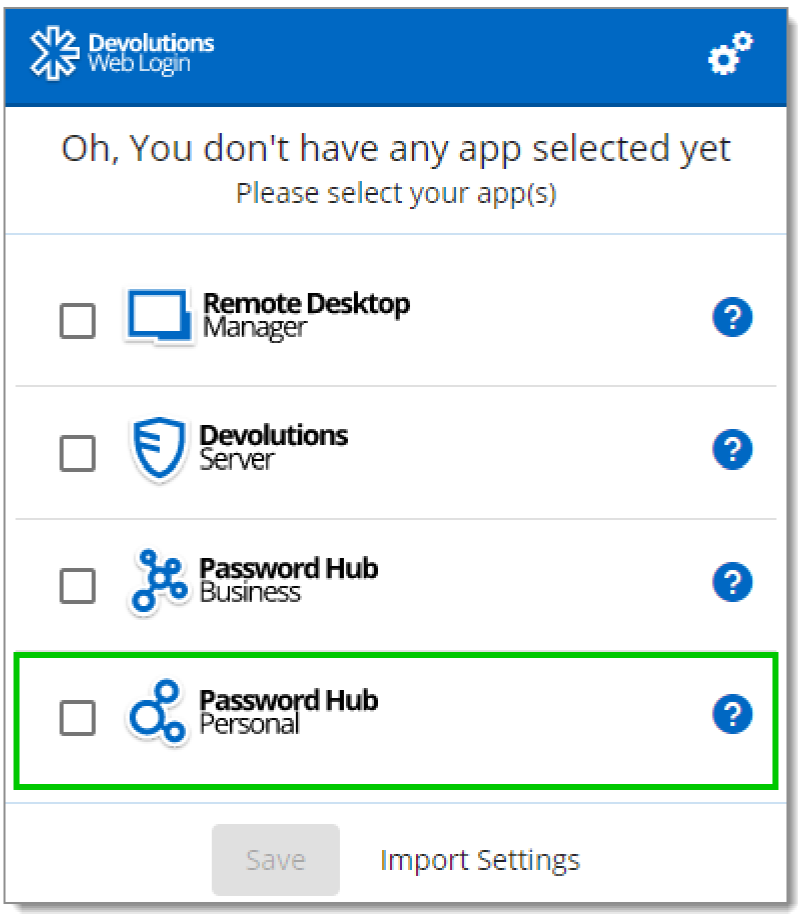
FIRST LOGIN WITH DEVOLUTIONS WEB LOGIN

Follow these steps to connect Password Hub Personal to Devolutions Web Login extension:

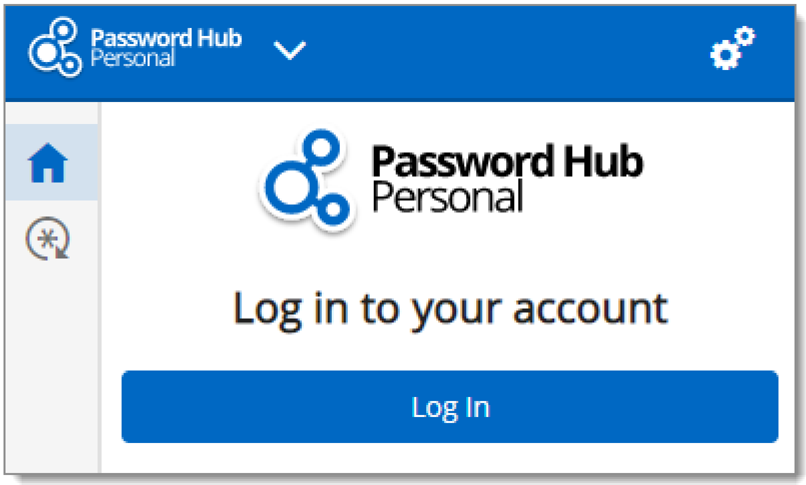
1. Click on ***Devolutions Web Login*** extension at the top right corner of your browser.

> A Password Hub Personal access is required to continue.

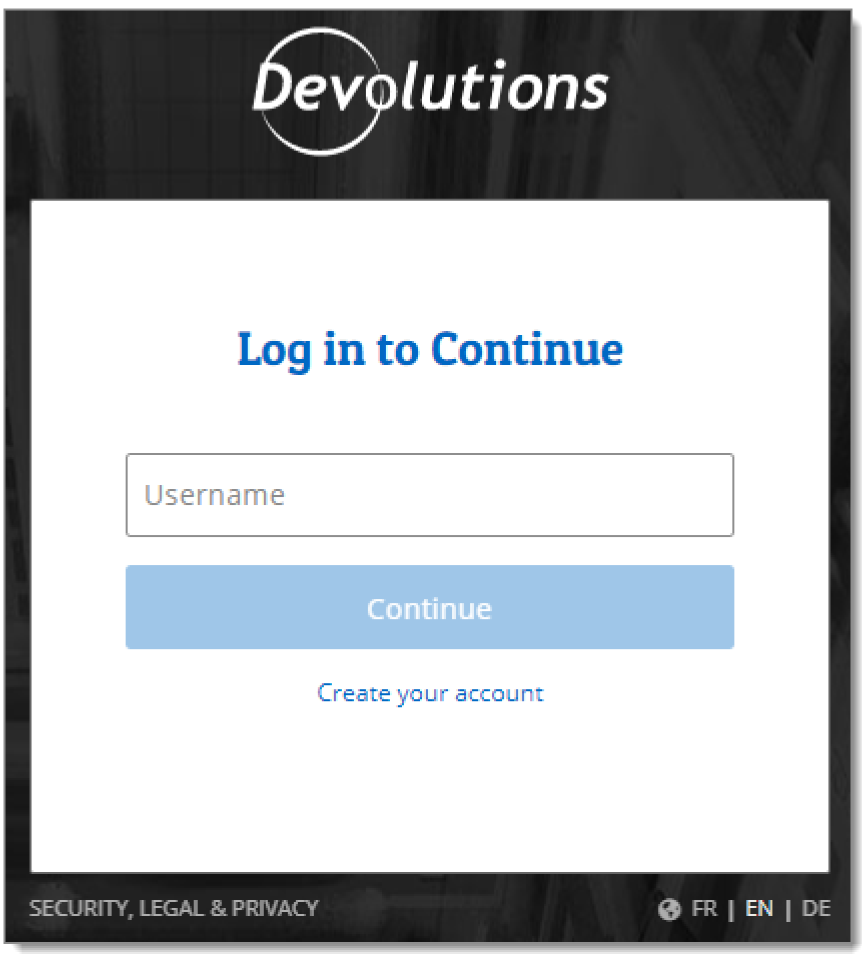
2. Choose ***Password Hub Personal*** in the list and ***Save***.



3. ***Log in*** to your account.

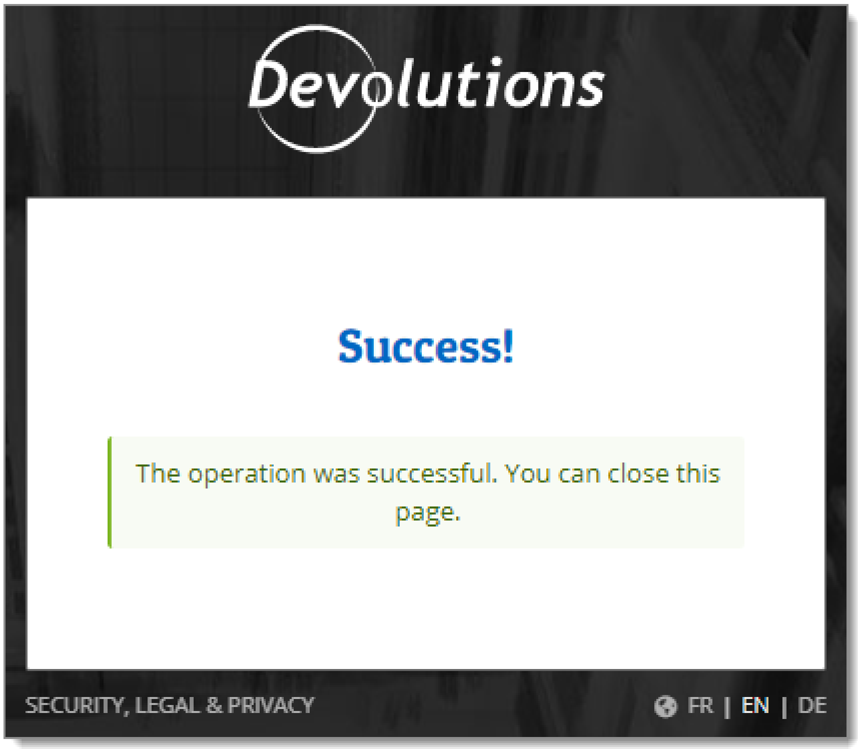


4. Enter the credentials from your Devolutions Account to continue.

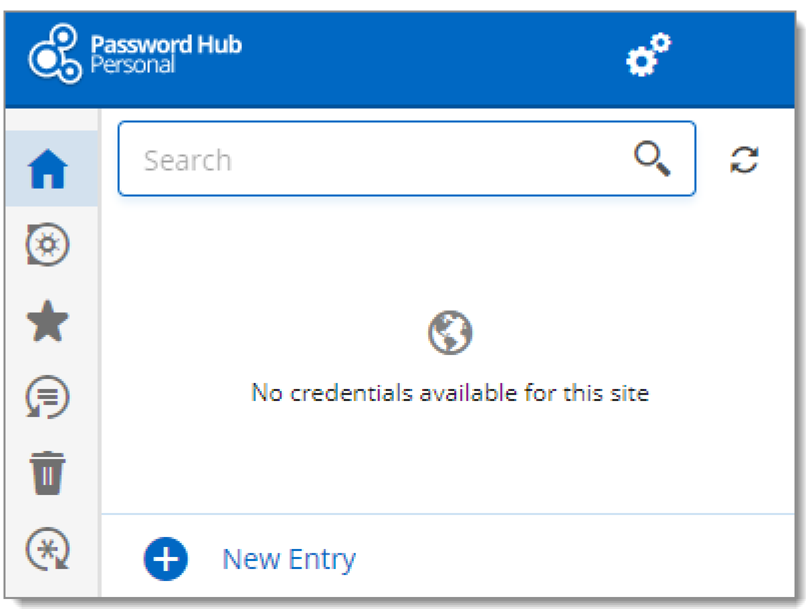


Devolutions Account Login

5. When complete, a log in confirmation message will appear.



6. If you click on the ✳ icon, you can validate that Devolutions Web Login is now connected to your Password Hub Personal.



7.3.3 Devolutions Server Login

DESCRIPTION

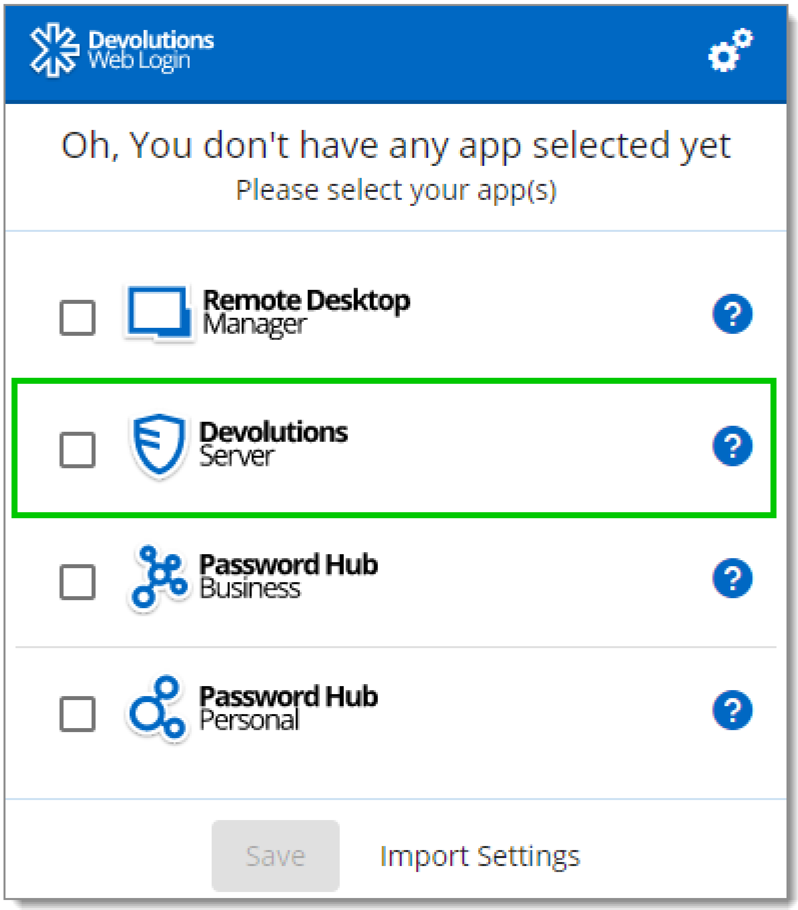
FIRST LOGIN WITH DEVOLUTIONS WEB LOGIN

Follow these steps to connect Devolutions Server to Devolutions Web Login extension:

1. Click on ***Devolutions Web Login*** extension at the top right corner of your browser.

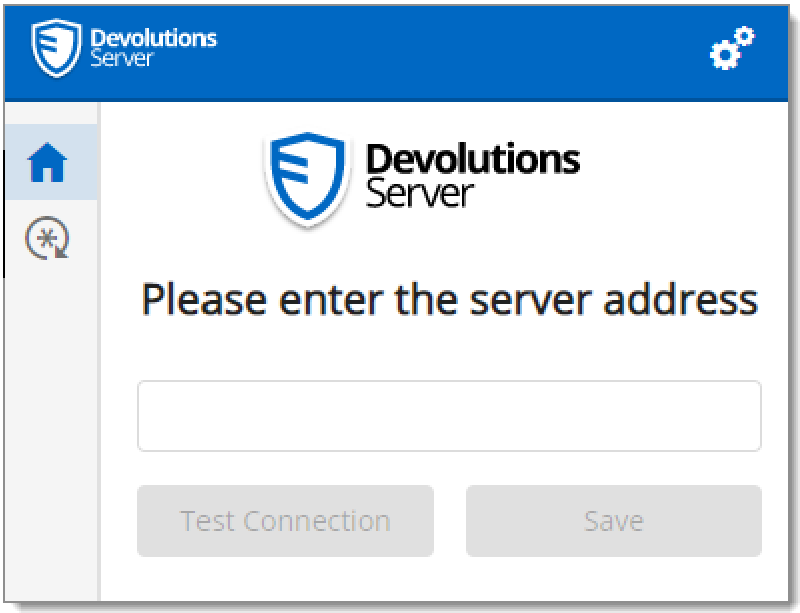
> A Devolutions Server access is required to continue.

2. Choose ***Devolutions Server*** in the list and ***Save***.



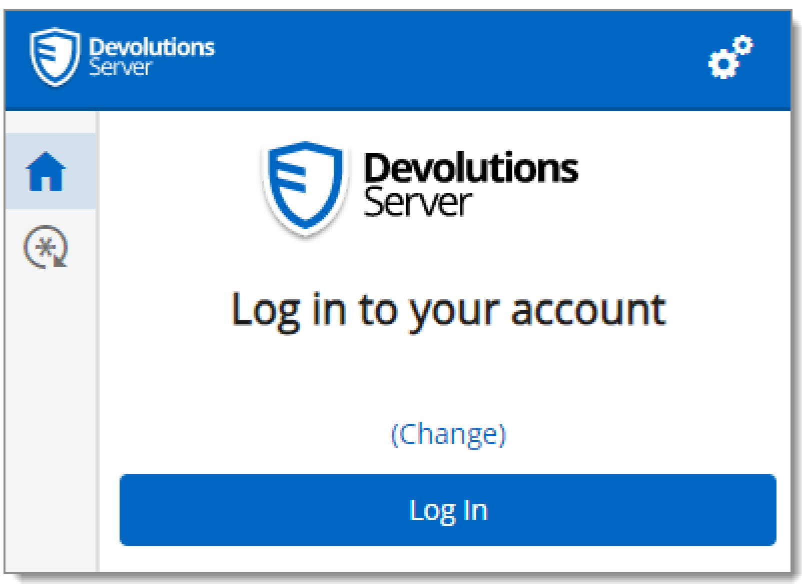
First Login

3. Enter the address of your server. You will need to input the same information that you would use to connect to the web interface of your Devolutions Server. Test the connection to validate it, then ***Save***.



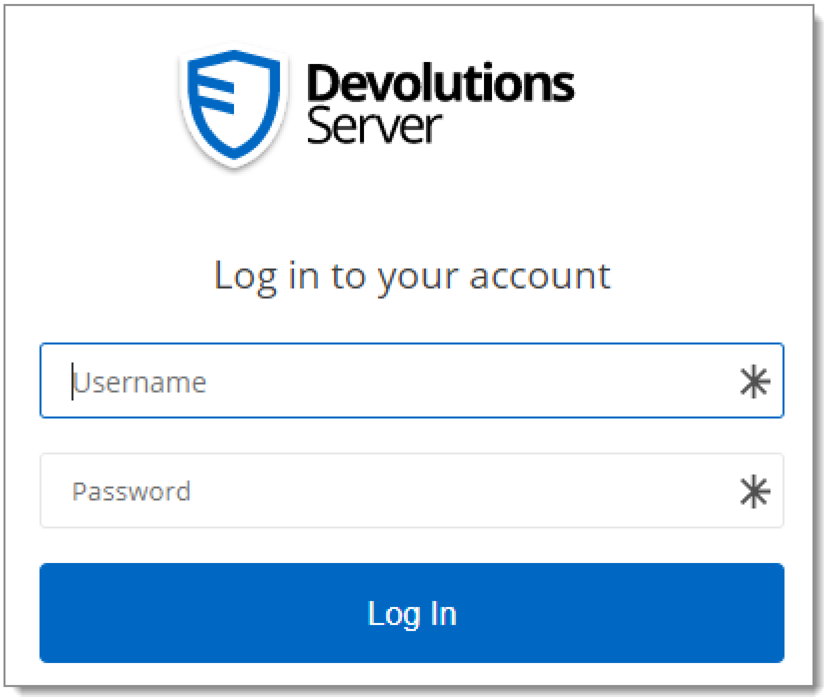
Server Address

4. Click ***Log In***.



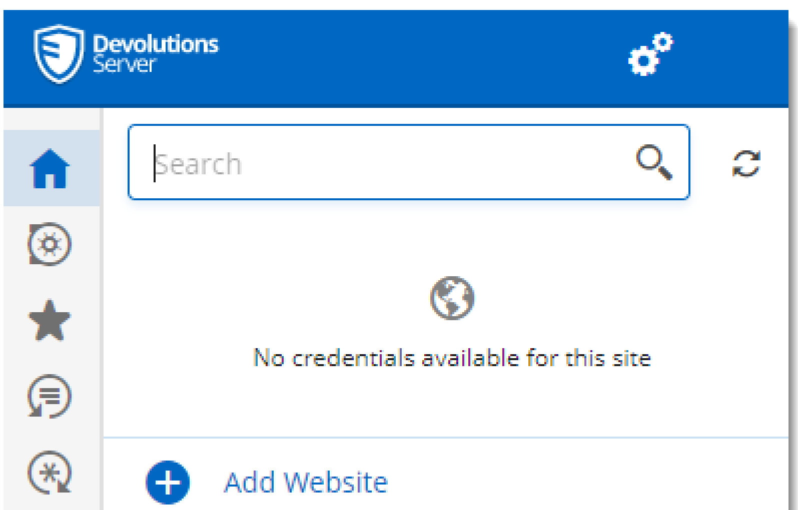
Devolutions Web Login Login

5. Enter your Devolutions Server credentials and click ***Log in***.



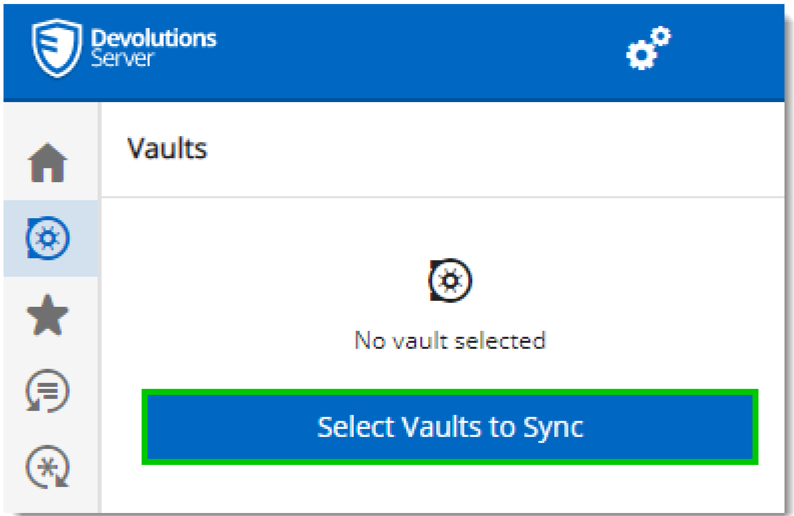
Devolutions Server Login

6. If you click on the ✳ icon, you can validate that Devolutions Web Login is now connected to your Devolutions Server.

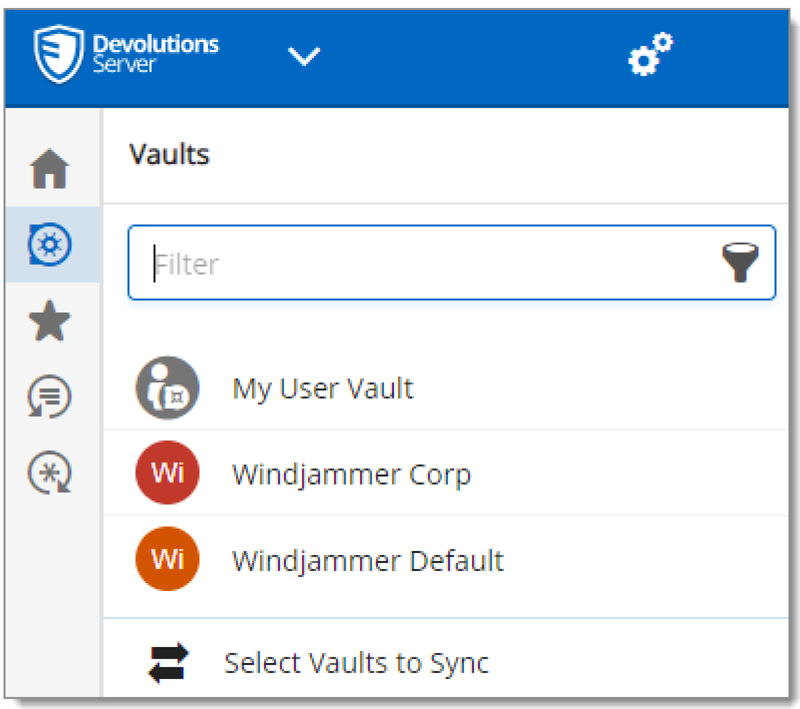


Devolutions Web Login Connected

7. To select the vaults to be synchronized, click on the ***Vaults*** icon and the ***Select Vaults to Sync*** button. Afterward, you click on the ***Select all*** button, or refine your view by adding a check mark next to the specific vaults to synchronize.



8. When done selecting your vaults, click on the ***Select Vaults to Sync*** at the top of the panel, to get the following view.



7.3.4 Remote Desktop Manager Login

DESCRIPTION

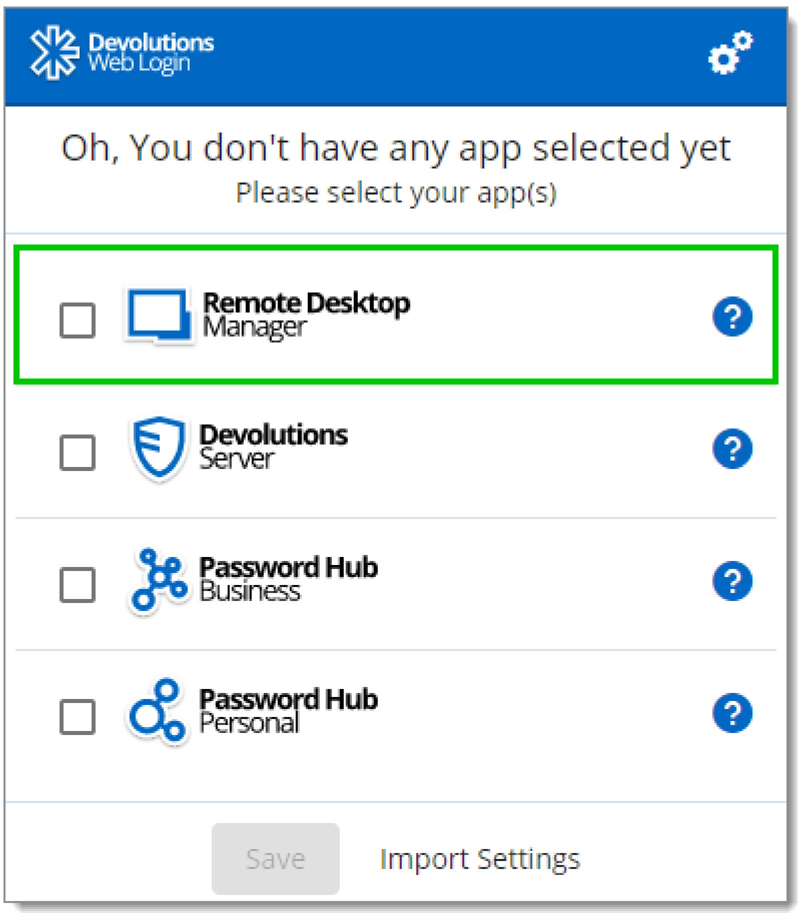
FIRST LOGIN WITH DEVOLUTIONS WEB LOGIN

Follow these steps to connect your Remote Desktop Manager to Devolutions Web Login extension, you will be prompted to pair the two applications.

1. Click on Devolutions Web Login extension at the top right corner of your browser.

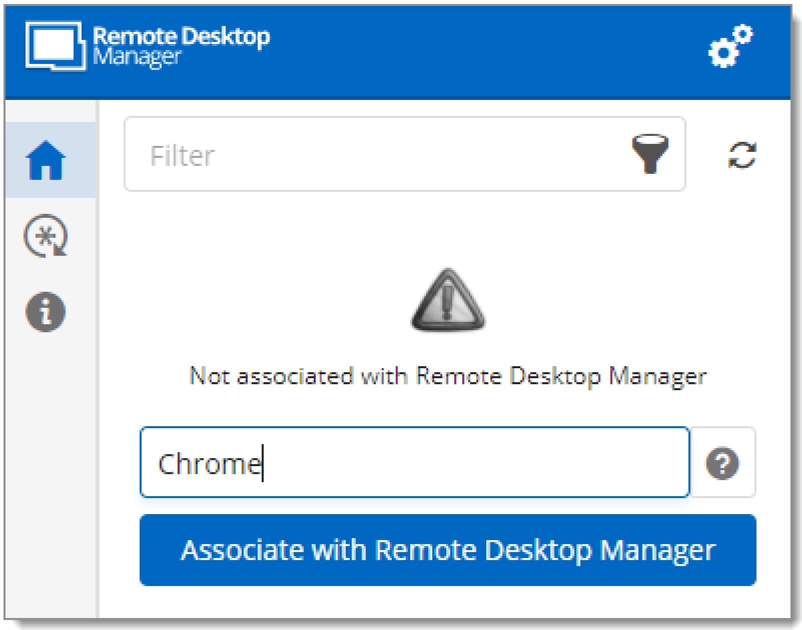
> Remote Desktop Manager must be installed and running to continue.

2. Choose ***Remote Desktop Manager*** in the list and ***Save***.



3. Enter a name, for this association, in the text box.

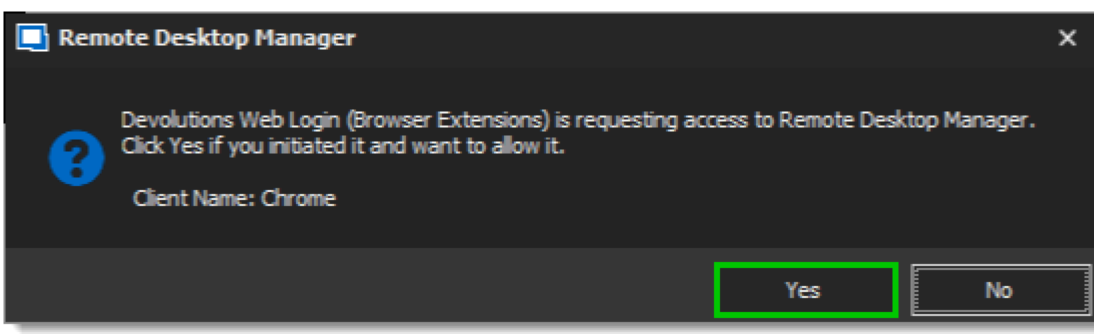
This name can be used to identify a particular association and to deny access to it from Remote Desktop Manager. The default name is the name of the web browser running Devolutions Web Login.



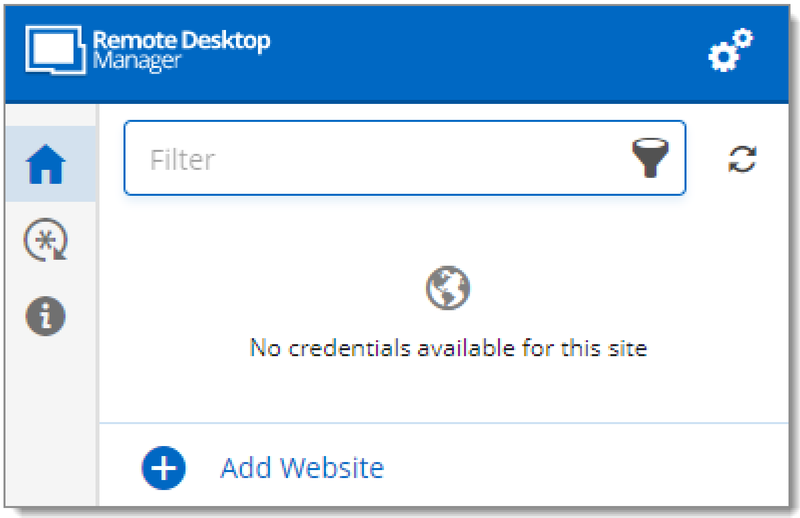
4. Click on ***Associate with Remote Desktop Manager***.

A popup window should appear on Remote Desktop Manager asking if the request was actually sent by you.

5. Click ***Yes*** in Remote Desktop Manager to accept the association request.



6. If you click on the icon, you can validate that Devolutions Web Login is now paired to your Remote Desktop Manager.

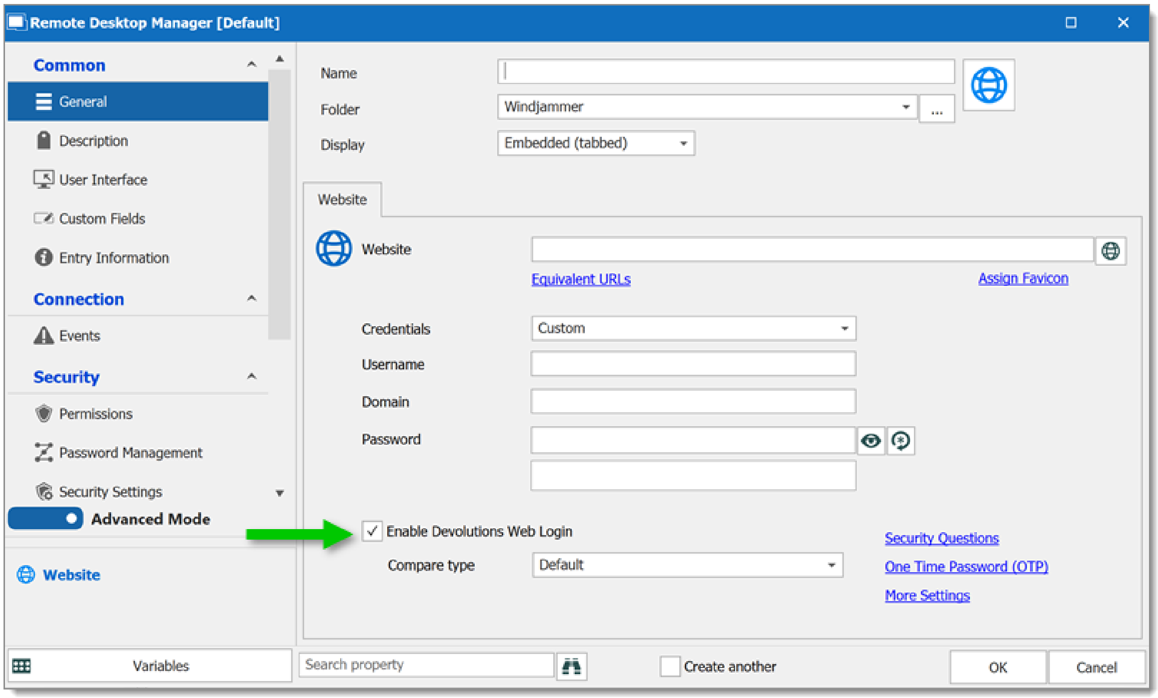


Note that, while Remote Desktop Manager can handle multiple associations (e.g., multiple browsers), Devolutions Web Login can only be paired to a single instance of RDM at any time.

7.3.4.1 Enable Devolutions Web Login

DESCRIPTION

Checkmark ***Enable Devolutions Web Login*** in Remote Desktop Manager entries to allow Devolutions Web Login extension to retrieve the credentials when connecting to its respective website.



Enable Devolutions Web Login

7.4 Exploring Devolutions Web Login

7.4.1 Menu

DESCRIPTION

The user interface **Devolutions Web Login** is slightly different in appearance when connected to Remote Desktop Manager, Devolutions Server or Password Hub Business and Personal.

See below a list of the menu and information available from the Devolutions Web Login extension:

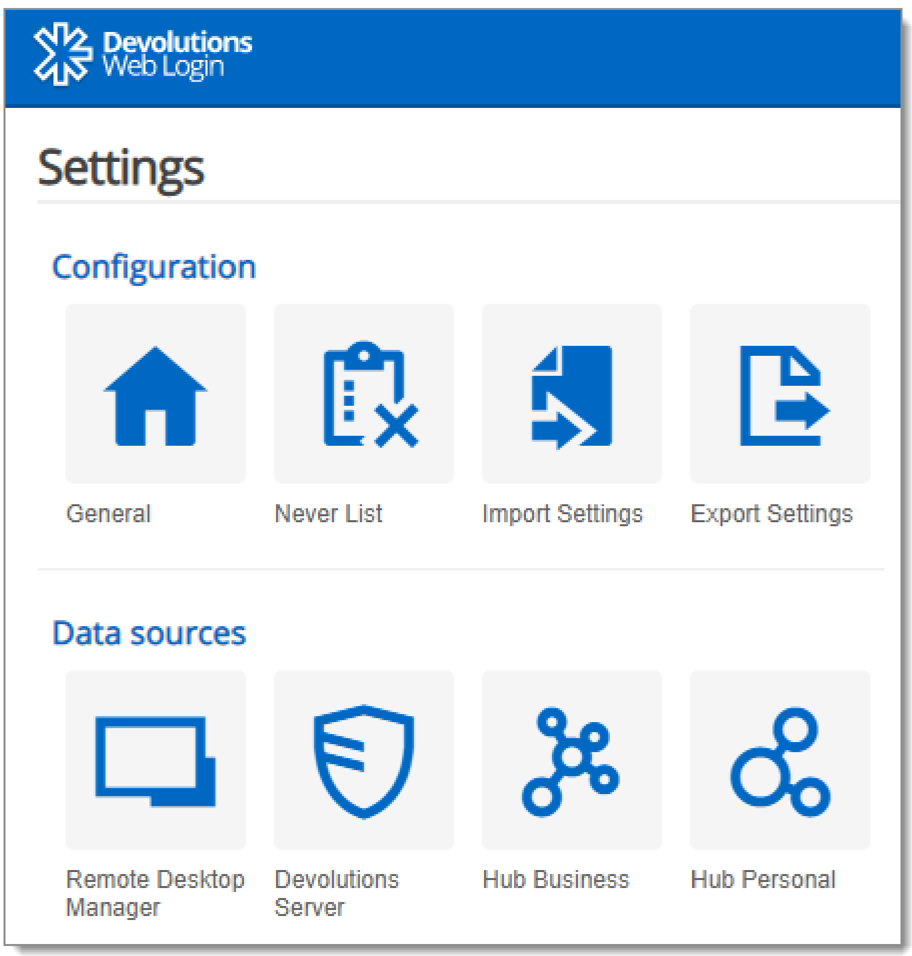
- Refine the credential list available with the ***Filter*** search bar.
- ***Add Website*** from Devolutions Web Login in a specific folder located in a vault or your User Vault.
- **Visualize the credential** stored in the vaults if you are connected with Devolutions Server or Password Hub.

- Browse ***Recent*** entry or ***Favorites***.
- Use the ***Password generator*** to create custom and more secure credentials.
- Set Devolutions Web Login ***Settings***.

7.4.1.1 Settings

DESCRIPTION

Devolutions Web Login settings are separated in two categories, ***Configuration*** and ***Data sources***.



Devolutions Web Login Settings

CONFIGURATION

The ***General*** settings are about the user interface and interaction.

- Show Devolutions Web Login extension icon in the credentials fields.
- Show the prompt when saving credentials on new login.
- Show the context menu options.
- Color the fields that are filled with Devolutions Web Login
- Set the color ***Theme*** of the application.
- Disable the analytics telemetry in the ***Advanced*** setting.

The ***Never list*** displays the list of websites, added locally, to which the user will never be prompted to save credentials.

- Type can range from: ***Never add site, Never autofill, Never do anything*** to ***Never show icons in fields***.
- Matching options are: ***Base domains, Host, Starts with, RegEx*** and ***Exact***.

The ***Import / Export Settings*** allows to save and transfer your currently set preferred settings.

- Import setting from other browsers or users.
- Choose to export Devolutions Web Login ***Settings, Password Generator*** template and the ***Never List***.

DATA SOURCES

The data sources settings are used to customize Devolutions Web Login interactions with Remote Desktop Manager, Devolutions Server and Password Hub Business or Personal.

REMOTE DESKTOP MANAGER

GENERAL OPTIONS	DESCRIPTION
Enable Remote Desktop Manager app	Retrieve entries from Remote Desktop Manager when the application is open.

GENERAL OPTIONS	DESCRIPTION
Use default port (19443)	Communicate with the default port 19443 between the application.
Add entry in User Vault by default	Save new entries in the User Vault.
Destination folder	Choose the folder where the credentials are stored in the vault.

ACTION OPTIONS	DESCRIPTION
Automatically retrieve credentials on page load	Devolutions Web Login automatically search for credentials in the data source when connecting to a website. If disabled, click on the Devolutions Web Login extension icon to manually retrieve credentials.
Automatically fill in credentials on load	Fill automatically the credentials when loading a web page.
Automatically submit the form after filling	Submit the credentials automatically when the fields are filled.

ADVANCED OPTIONS	DESCRIPTION
Application key	Secure the port with an application key by using the same code in Remote Desktop Manager and Devolutions Web Login. Navigate to ***File - Options - Browser Extensions*** in Remote Desktop Manager to set the application key.

ADVANCED OPTIONS	DESCRIPTION
Enable native messaging	Exchange messages with a native application installed on the user's computer.
Use legacy API	Use the old browser extension API for compatibility with older versions of Remote Desktop Manager.

DEVOLUTIONS SERVER

GENERAL OPTIONS	DESCRIPTION
Enable Devolutions Server	Retrieve entries from Devolutions Server.
Destination folder	Choose the folder where the credentials are stored in the vault.
Server URL	Enter the URL of the Devolutions Server instance to connect to.

ACTION OPTIONS	DESCRIPTION
Automatically retrieve credentials on page load	Devolutions Web Login automatically search for credentials in the data source when connecting to a website. If disabled, click on the Devolutions Web Login extension icon to manually retrieve credentials.
Automatically fill in credentials on load	Fill automatically the credentials when loading a web page.
Automatically submit the form after filling	Submit the credentials automatically when the fields are filled.

ADVANCED OPTIONS	DESCRIPTION
Default compare type	Set a default comparing option type.
Sync all available vaults	Enable to synchronize all the available vaults from Devolutions Server.

PASSWORD HUB BUSINESS AND PERSONAL

GENERAL OPTIONS	DESCRIPTION
Enable Password Hub	Retrieve entries from Password Hub.
Server URL (Business only)	Enter the URL of the Password Hub instance to connect to.

ACTION OPTIONS	DESCRIPTION
Automatically fill in credentials on load	Fill automatically the credentials when loading a web page.
Automatically submit the form after filling	Submit the credentials automatically when the fields are filled

ADVANCED OPTIONS	DESCRIPTION
Devolutions Account login	Set your Devolutions Account login URL.
Show favicon	Display the Devolutions Web Login favicon.
Default compare type	Set a default comparing option type.
Sync all available vaults (Business only)	Enable to synchronize all the available vaults from Devolutions Server.

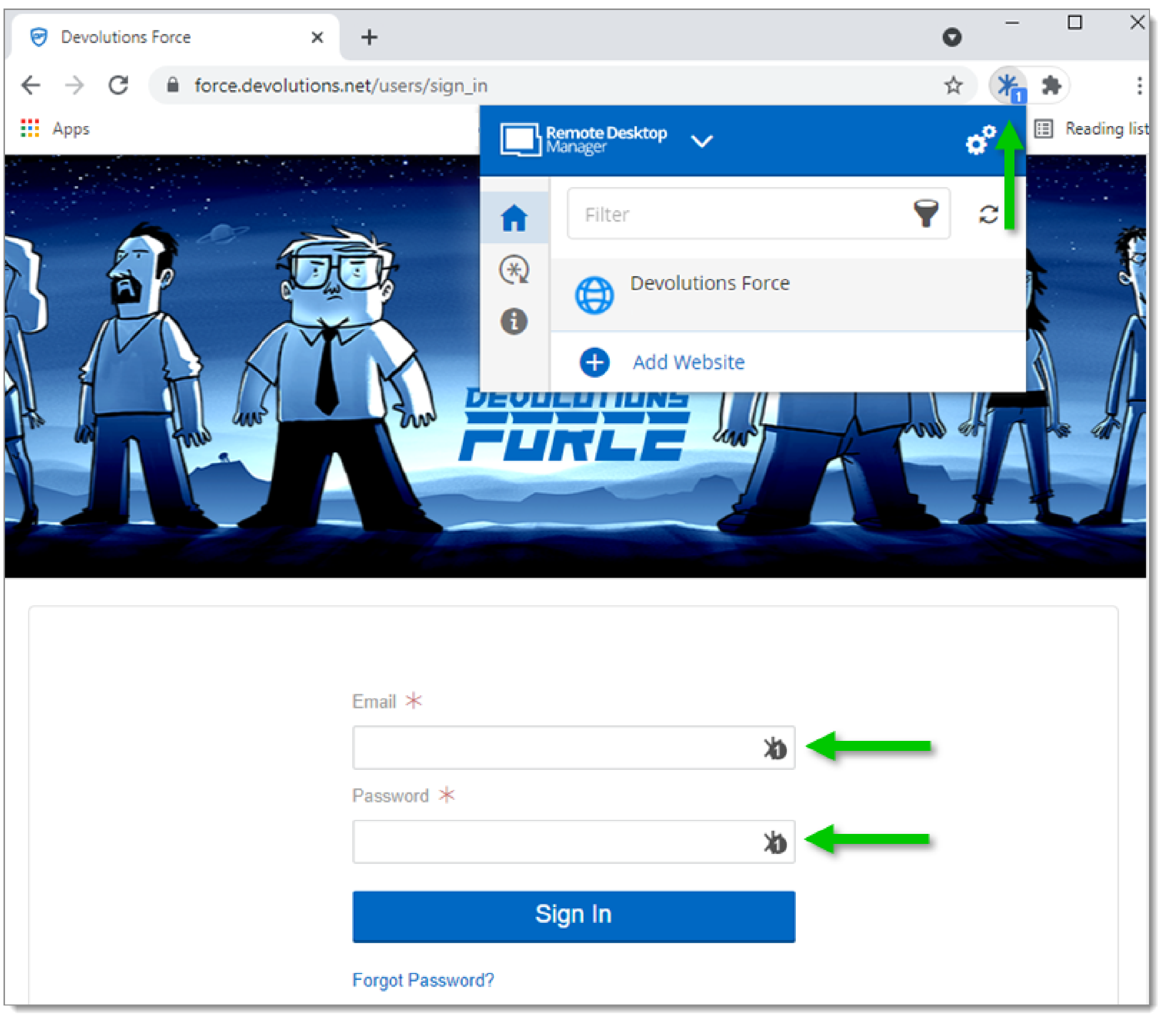
7.4.2 Retrieve Credentials

DESCRIPTION

Once configured in your Devolutions product, credentials are automatically detected by **Devolutions Web Login** when connected to their respective applications.

LOG IN TO A WEBSITE

Select an entry from the list in Devolutions Web Login or click on the icon in the credential field of the browser to fill in the login information and connect to the website.



Automatic Log In

7.4.3 Secure Devolutions Web Login

DESCRIPTION

In Remote Desktop Manager version 2021.1 and higher, we changed how our browser extension, Devolutions Web Login, communicates with Remote Desktop Manager to fill in credentials inside web pages. We did these changes to increase the security of this feature. Follow this link for the steps.

If you are using a version prior to 2021.1 and as mentioned in the Devolutions Web Login Overview topic, installing the extension in a Terminal Services environment can introduce security risks. In such environments, each user must have a distinct port assigned, as well as an application key to prevent any other Devolutions Web Login from listening in.

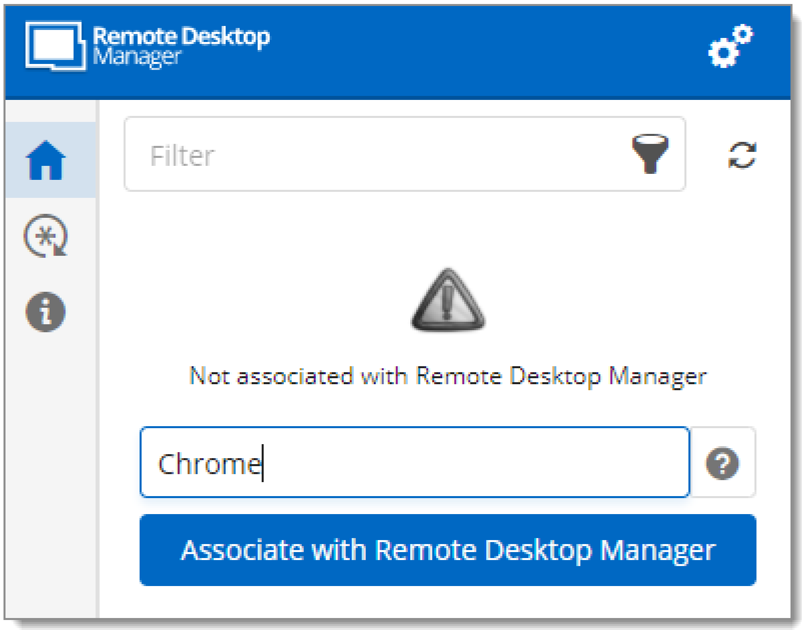
If you insist on using it, it is critical that each user is assigned a distinct port. An application key must be set as well. The first client application that starts will be able to use the port exclusively. ALL Devolutions Web Login calling on that port will get the responses unless an application key is set. Follow this link for the steps.

HOW TO SET UP DEVOLUTIONS WEB LOGIN FOR VERSION 2021.1 AND HIGHER

An application key is mandatory if you are using Devolutions Web Login on a Terminal server. Please follow the steps describe here.

When you will first open Devolutions Web Login and choose to use it with Remote Desktop Manager, you will be prompted to pair the two applications.

1. Enter a name, for this association, in the text box.

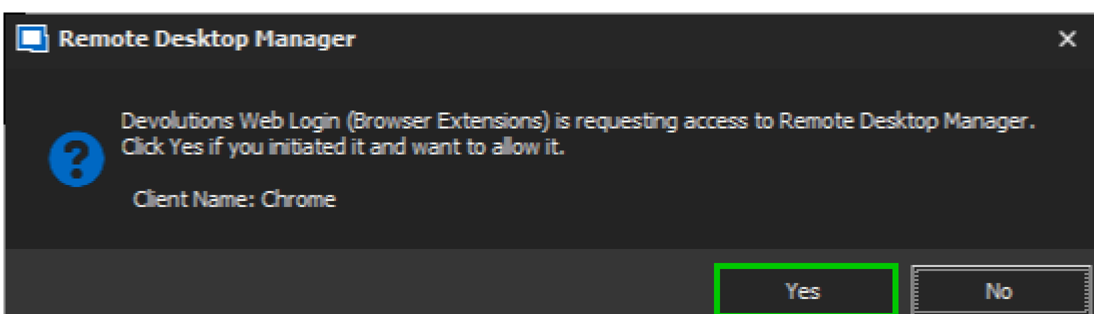


This can be used to identify a particular association and to deny access to it from Remote Desktop Manager. The default name is the name of the web browser running Devolutions Web Login.

2. Click on ***Associate with Remote Desktop Manager***.

A popup window should appear on Remote Desktop Manager asking if the request was actually sent by you.

3. Click ***Yes*** to accept the association request.



You are now paired.

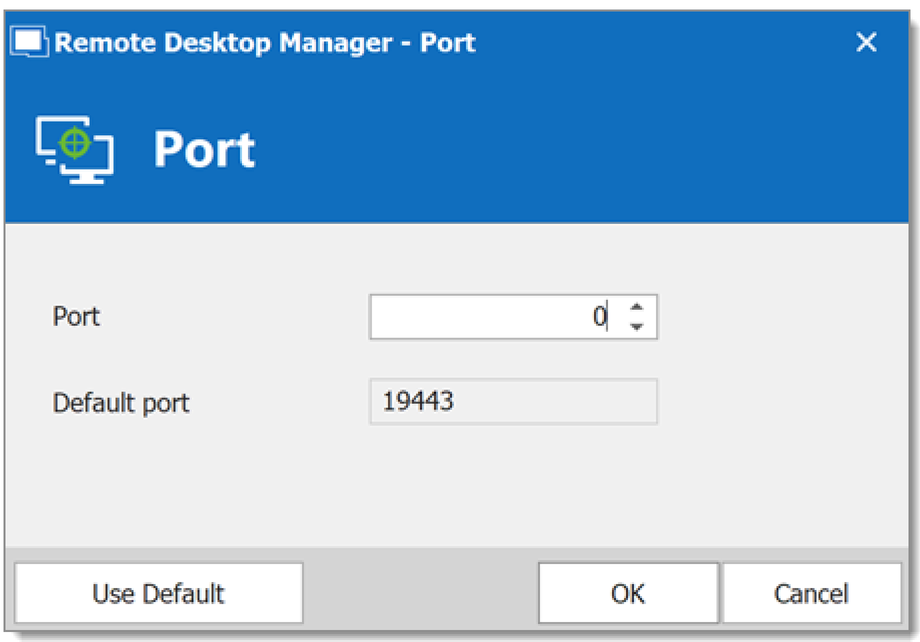
Note that, while Remote Desktop Manager can handle multiple associations (e.g., multiple browsers), Devolutions Web Login can only be paired to a single instance of RDM at any time.

HOW TO SET UP DEVOLUTIONS WEB LOGIN FOR VERSION LOWER THAN 2021.1 AND FOR TERMINAL SERVER

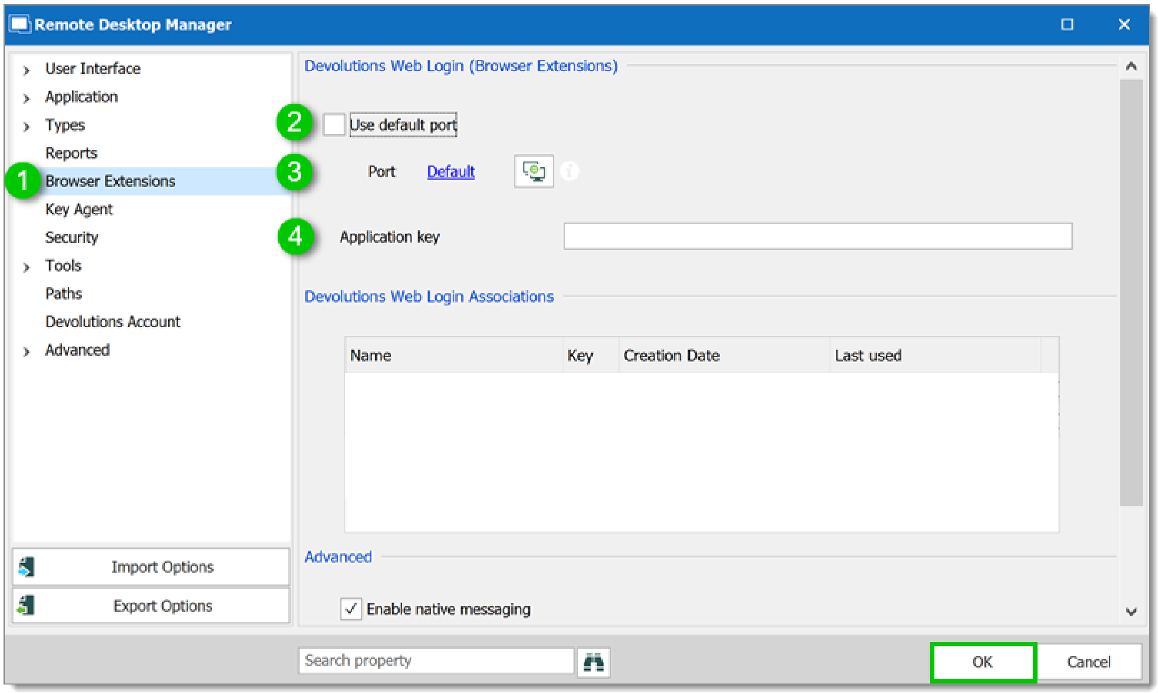
The application key is displayed in clear text, it must be kept secret by the user.

To enable the security layer in Remote Desktop Manager, follow these steps:

1. Navigate to ***File - Options - Browser Extensions***.
2. Uncheck ***Use default port***.
3. Click ***Default*** to enter a custom port and ***OK*** when done.

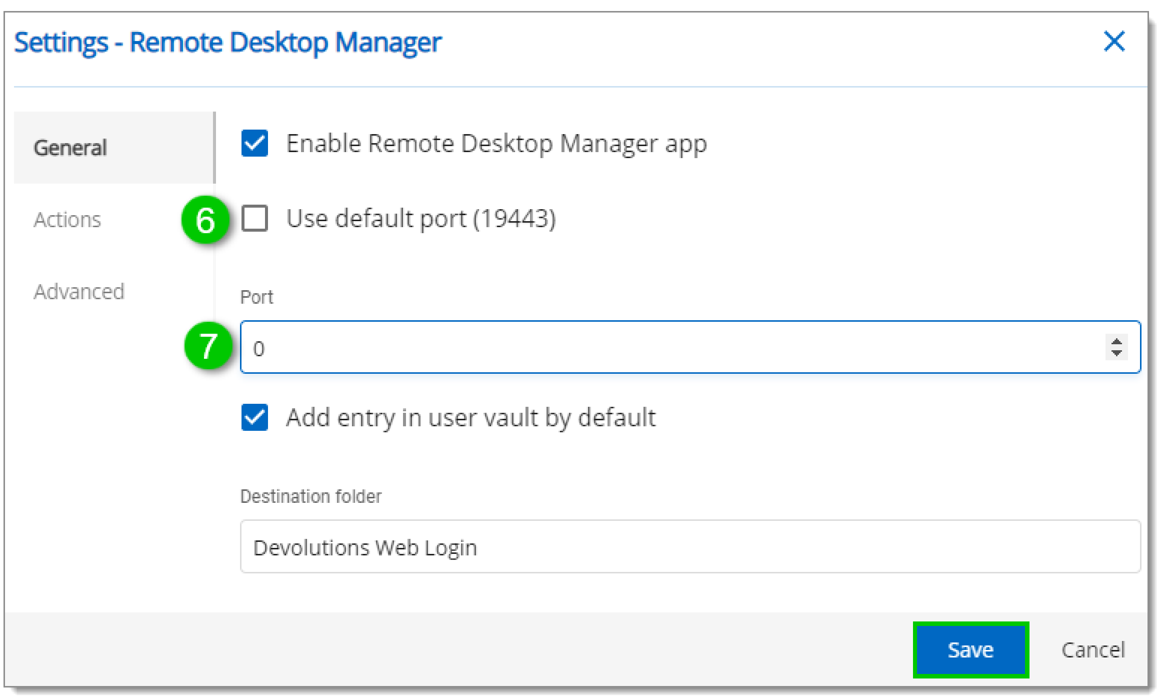


4. Type an ***Application key*** then click ***OK*** to save.

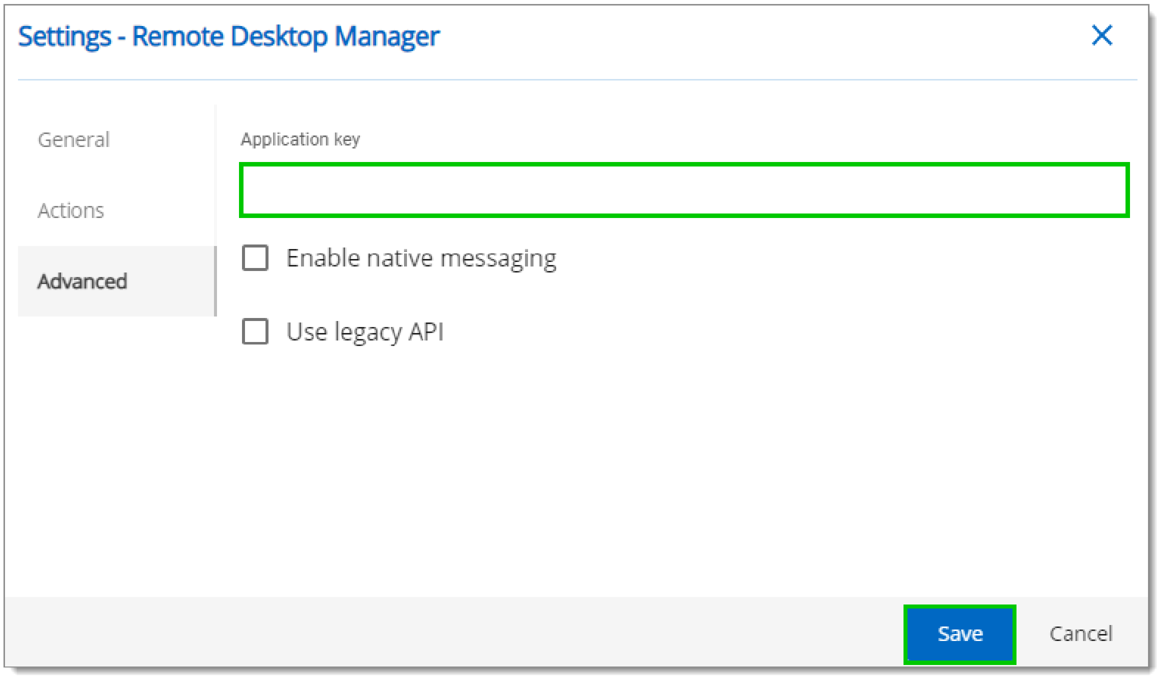


Remote Desktop Manager Browser Extensions Options

5. In your browser, click the Devolutions Web Login icon and go to ***Settings - Data sources - Remote Desktop Manager***.
6. Disable ***Use default port***.
7. Enter the custom port created earlier in Remote Desktop Manager and ***Save***.



8. Click ***Advanced*** and enter the same ***Application key*** as Remote Desktop Manager, ***Save***.



Devolutions Web Login Settings for Remote Desktop Manager

7.4.3.1 Unpair a Browser Extension

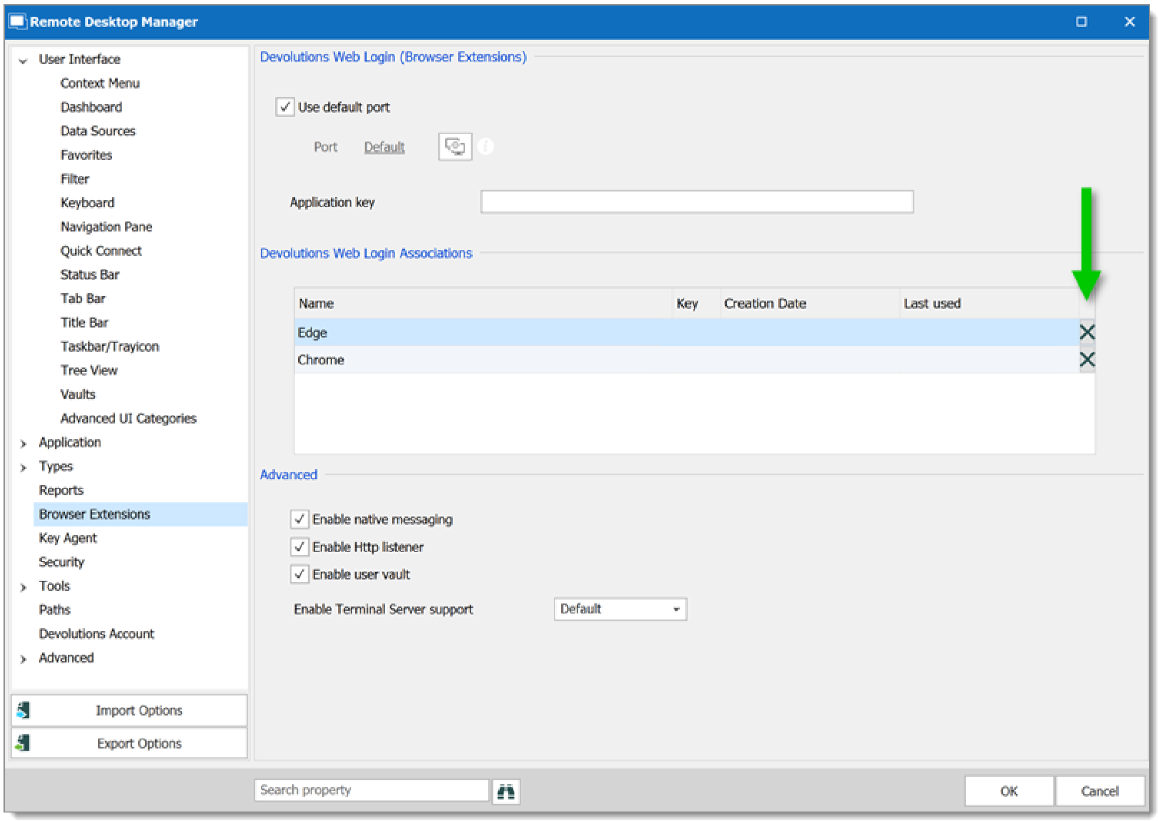
DESCRIPTION

In the event you want to deny access to Remote Desktop Manager from a previously paired browser extension, you need to delete it from Remote Desktop Manager.

1. In RDM go to ***File - Options - Browser Extensions***.

2. In the ***Devolutions Web Login Associations*** section click the ***X*** button of the entry in the list and click ***OK*** to save the modifications.

> In the ***Devolutions Web Login Associations*** section, you will find a list of each association made to Remote Desktop Manager including some information to identify them. This includes the name specified at the time of association (which defaults to the web browser's name), a part of the encryption key used between the two, it's creation date and the date when it was last used.



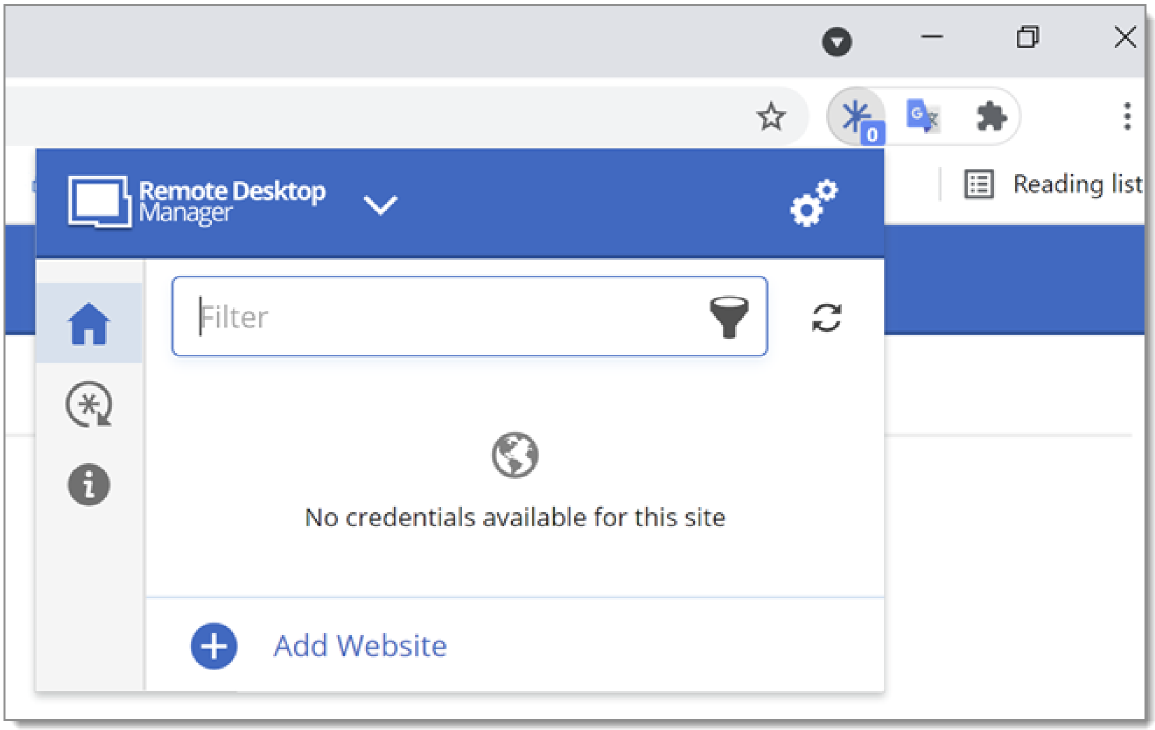
7.4.4 Keyboard Shortcuts

DESCRIPTION

Here is the list of keyboard shortcuts available for Devolutions Web Login:

CTRL+SHIFT+Z

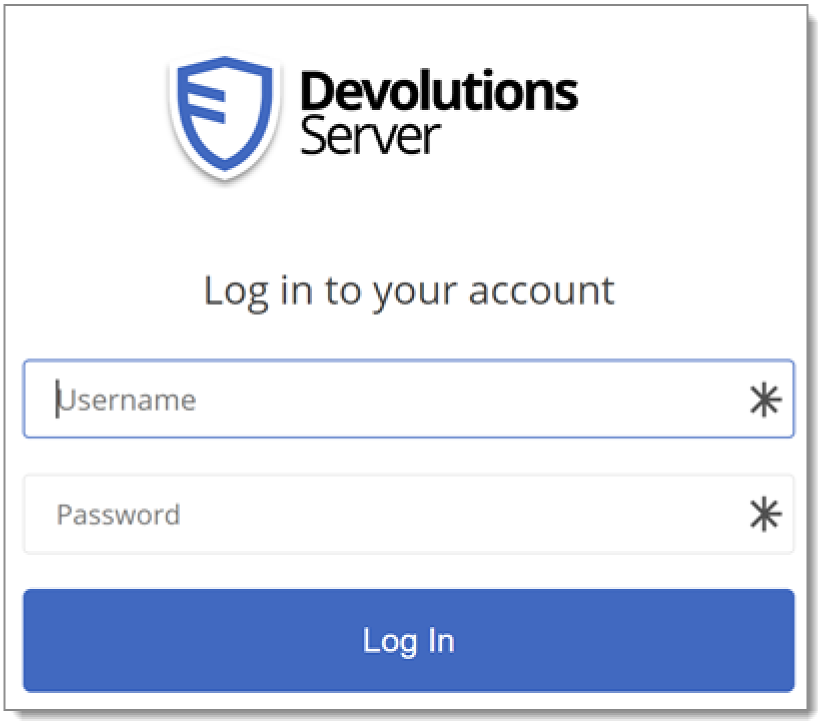
Use this key shortcut to open Devolutions Web Login window in your active browser.



Devolutions Web Login in Chrome

CTRL+SHIFT+Y

Use it to autofill your credential when only one is available for an entry.



One Credential Login with Devolutions Web Login

User Groups Based Access Control

Part

VIII

8 User Groups Based Access Control

DESCRIPTION

Remote Desktop Manager user group based access control allows to create a granular protection system that is quite flexible. However, flexibility comes at a price and sometimes making the wrong choices could increase the time involved in managing the system.

The following recommendations are based on our experience with the system and the ideas shared by our community. Follow these guidelines, as they will help you to use the user group based access control efficiently.

Here are the main key points of the user group based access system:

- Security is inherited: child items and folders are covered by a parent folder's security.
- Permissions can be overridden: a permission set on a sub folder will override the parent item's permission.
- Permissions are granular: Multiple permissions can be set on entries at once.

ENHANCE THE SECURITY

While the user group based access control is a great feature to secure access to entries, many other features can be used to add more security layers. For more information, please consult the following topics:

- Security Provider
- Credential repository
- Password Templates
- Two-factor authentication
- One-time password

SCENARIOS

Because of the great flexibility of our system, it becomes difficult to describe how to achieve the exact security system that matches your needs. For this reason, we have elected to describe the most popular systems that we have seen in use in our current community of users. We hope that one of them will closely match your needs. You can obviously mix and match the various strategies used in our scenarios to achieve your requirements.

Please consult the following:

- Simplified security
- Advanced security

USER GROUPS CONFIGURATION

When using the user group based access control, user groups are mostly used to control user access for multiple users at once.

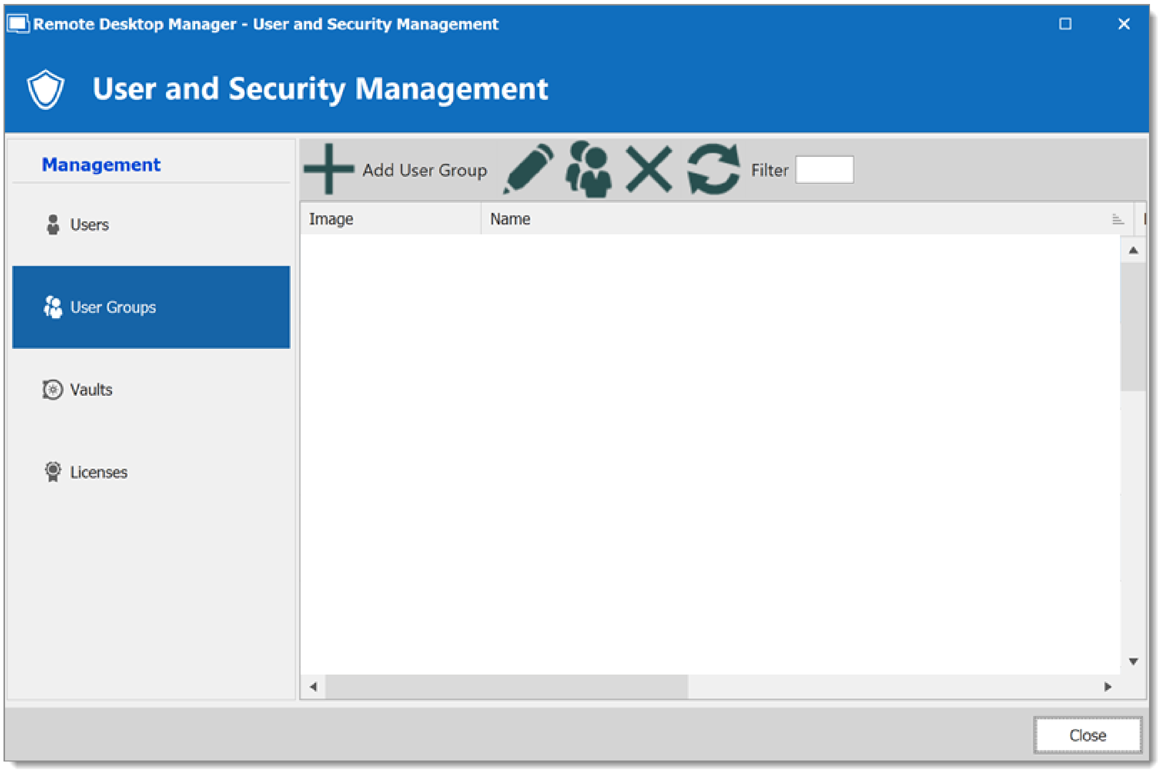
Common user groups can be:

- Service Desk: a single point of contact to handle incidents, problems and questions from staff and customers. Provide an interface for activities such as change requests, software licences, configuration management, and more.
- Help Desk: manage, co-ordinate and resolve support requests.
- Consultants: employed externally on a temporary basis, they usually are read-only users and can use only a subset of entries.

To be more specific, we will use these team names in our scenarios.

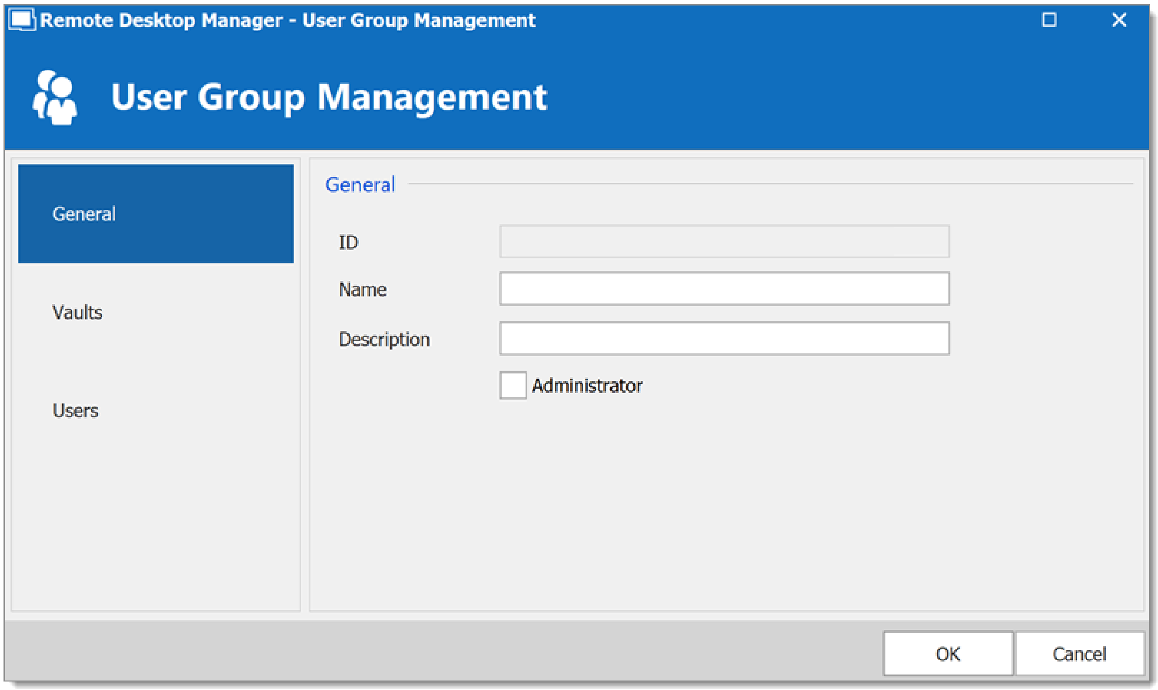
CREATE THE USER GROUPS

To create user groups, navigate to ***Administration – User Groups***, then click **+ Add User Groups**.



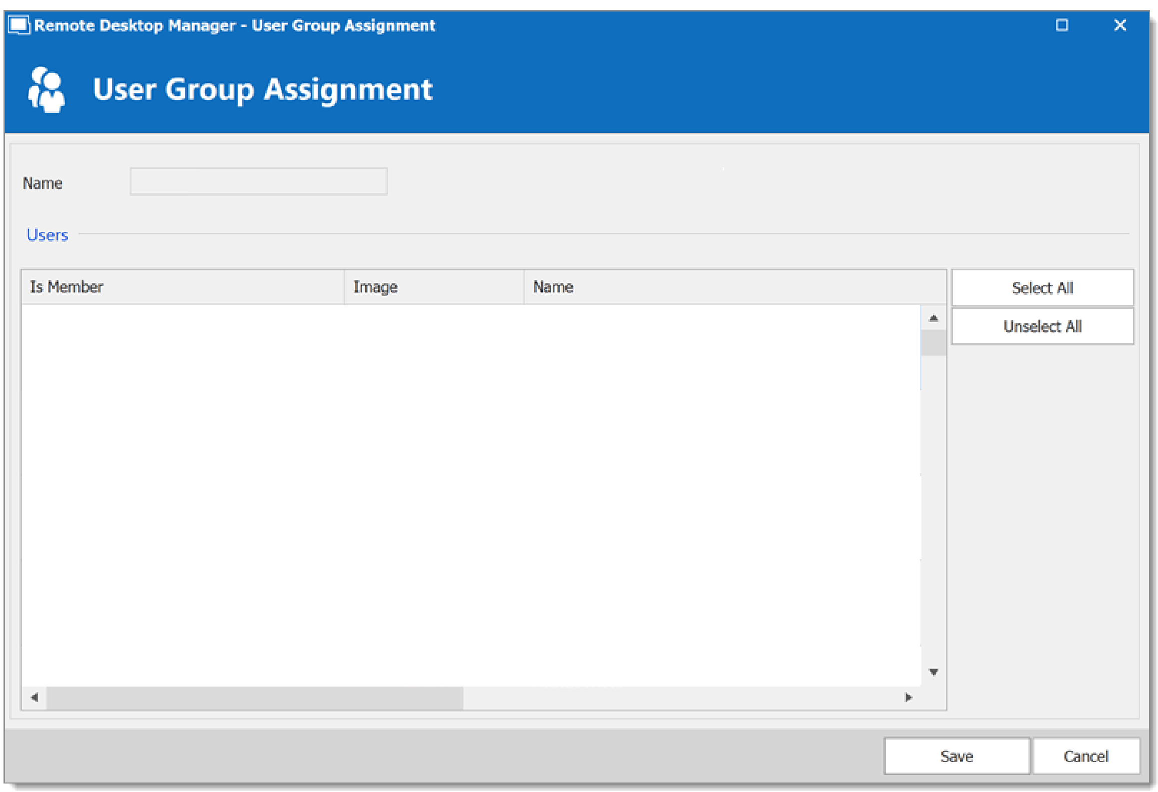
Create a User Group

All settings can be left to default unless the user group contains only administrators. In this case, check the **Administrator** box when configuring the user group. Enter a **Name** for the user group, then click **Ok**.



Configure a User Group

To assign users to the user group, click , then check the **Is Member** box of the respective user.



Assign a user to the User Groups

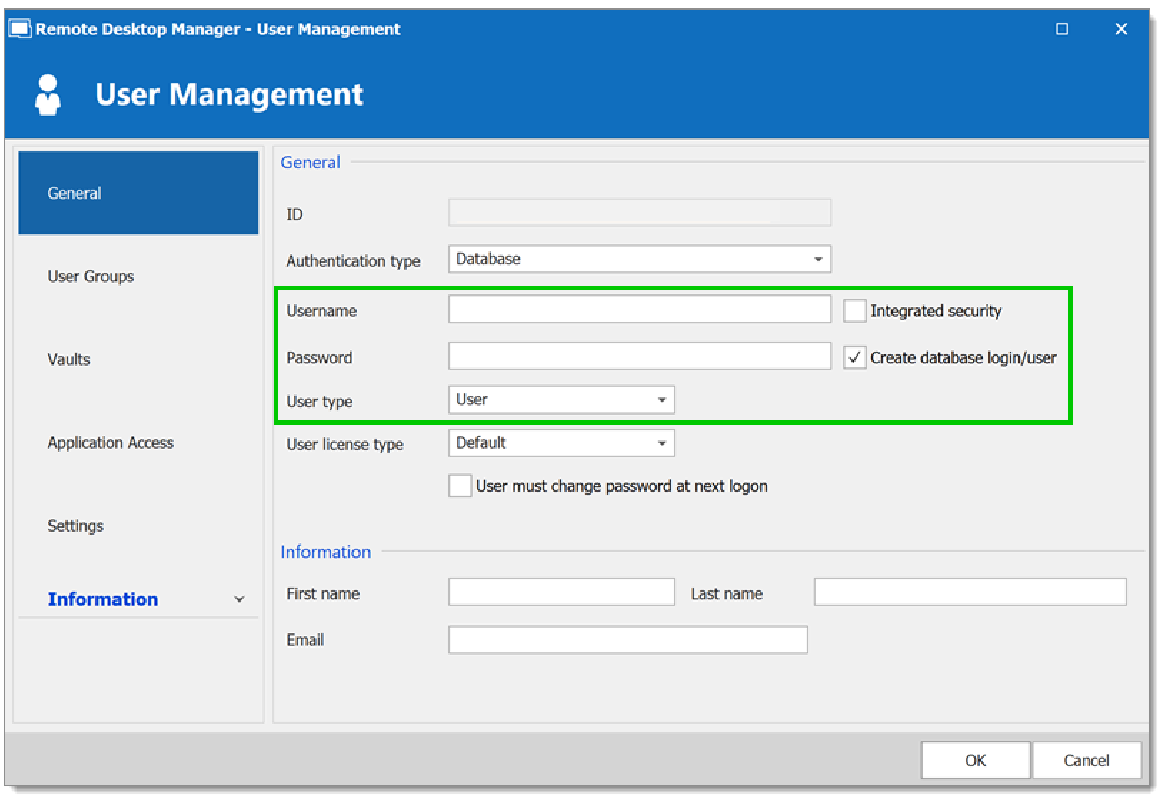
USER CONFIGURATION

USER TEMPLATE

It is possible to change the default user template. To do so, navigate to ***File – Options – Security – User Template***. These settings control the default settings of a new user. The best practice is to disable all privileges.

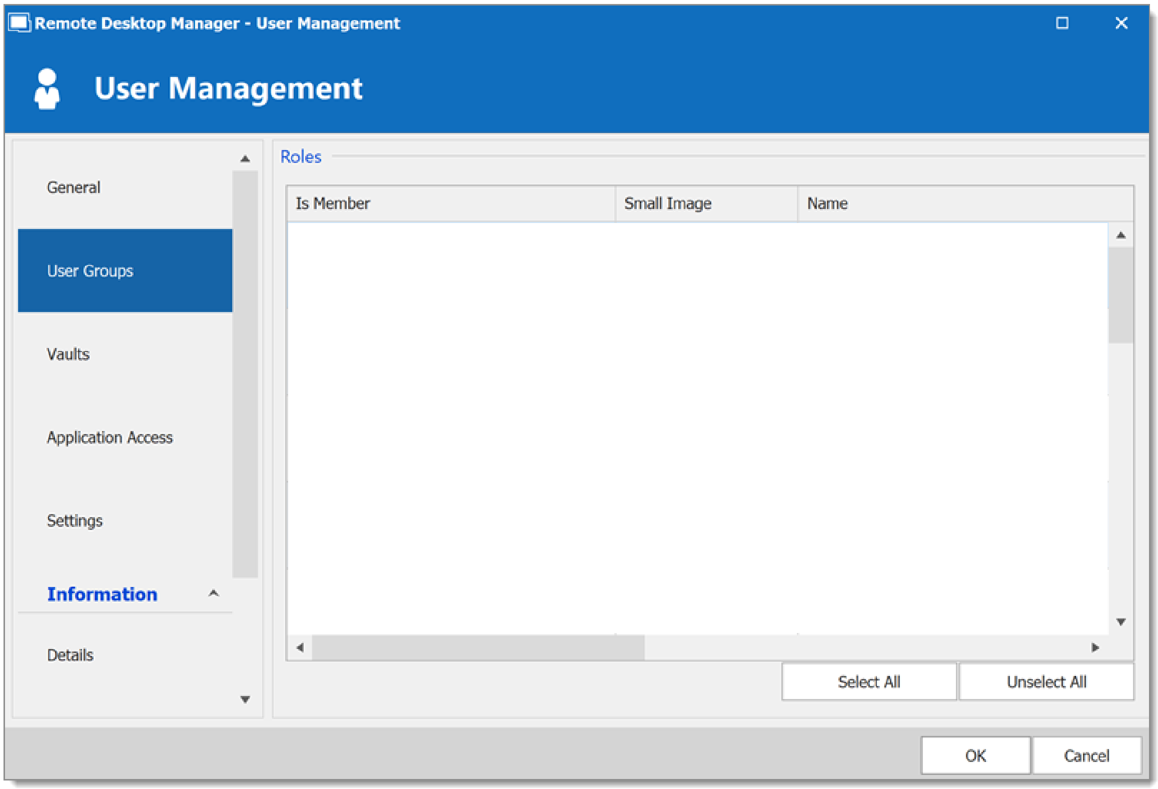
CREATE THE USER

To create users, navigate to ***Administration – Users***, then click **Add User**. Enter a **Login** and **Password** for the user and select the **User type**.



Create a user

A user can be assigned to multiple user groups at once by checking the **Is Member** box of the respective user groups in the **User Groups** section of the **User Management**.



Assign a user to a User Groups

ADMINISTRATORS

Administrators can do everything, regardless of the security. These users are usually the chief officers and senior management.

RESTRICTED USERS

Restricted users have limited access to resources. They usually have the **Add** and **Edit** rights only. These users can be mid or first level executives, such as service desk and help desk.

USERS

Users also have limited access to resources much like Restricted users. However, Users have by default the **Add**, **Edit** and **Delete** rights and can perform these actions on all unsecured entries.

READ ONLY USERS

Read only users can only view and use resources, but cannot edit them. These users are usually external consultants.

SELECT THE APPROPRIATE USER TYPE

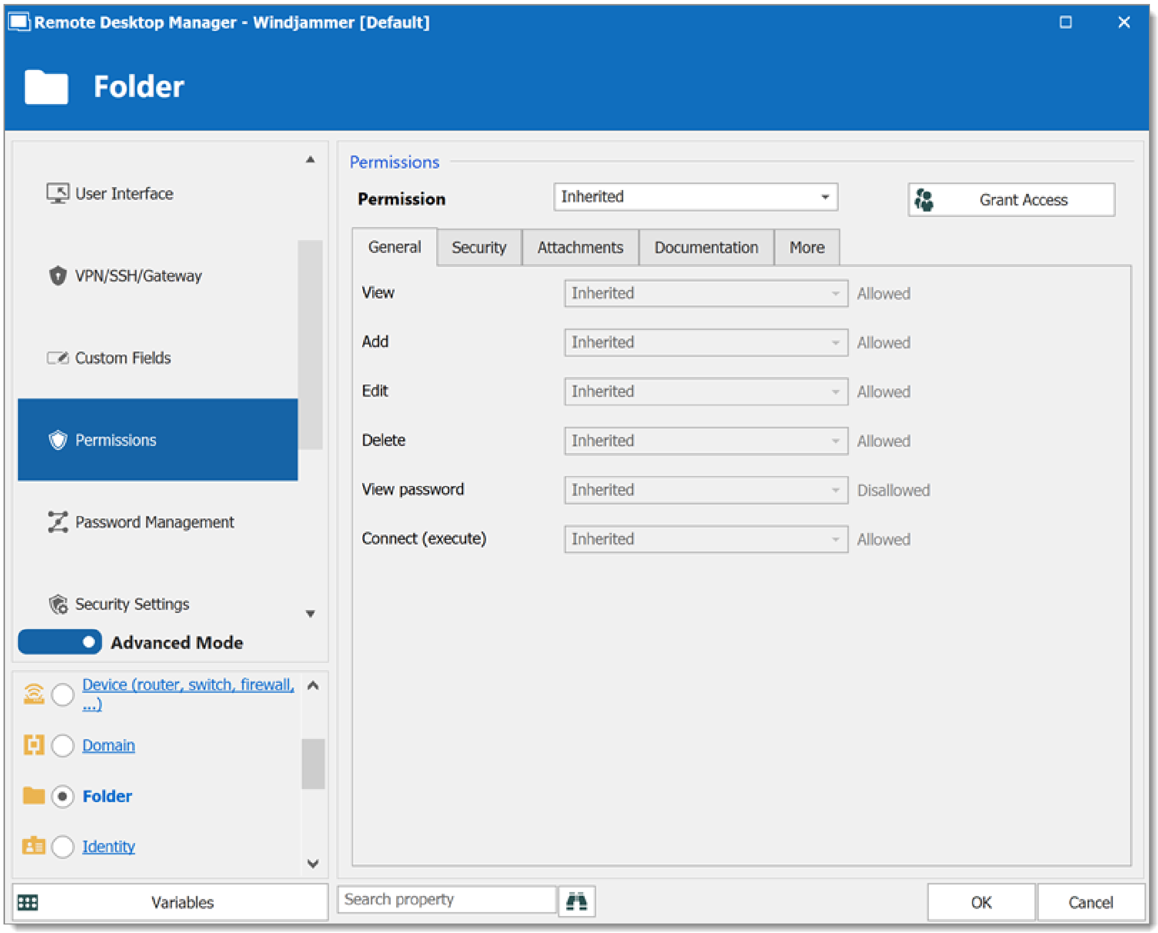
When creating users, some key points must be taken into consideration. Ask yourself the following questions while configuring a new user:

- Should they be able to access any resource without restriction? These are your **Administrators**.
- Should they be able to add, edit, or delete entries? A **User** would have all of these. Alternatively, you can select specific rights with **Restricted User**.
- Should they be able to see sensitive information, or import and export entries? **Read-Only** users are best used for those who should very limited access.

ENTRY CONFIGURATION

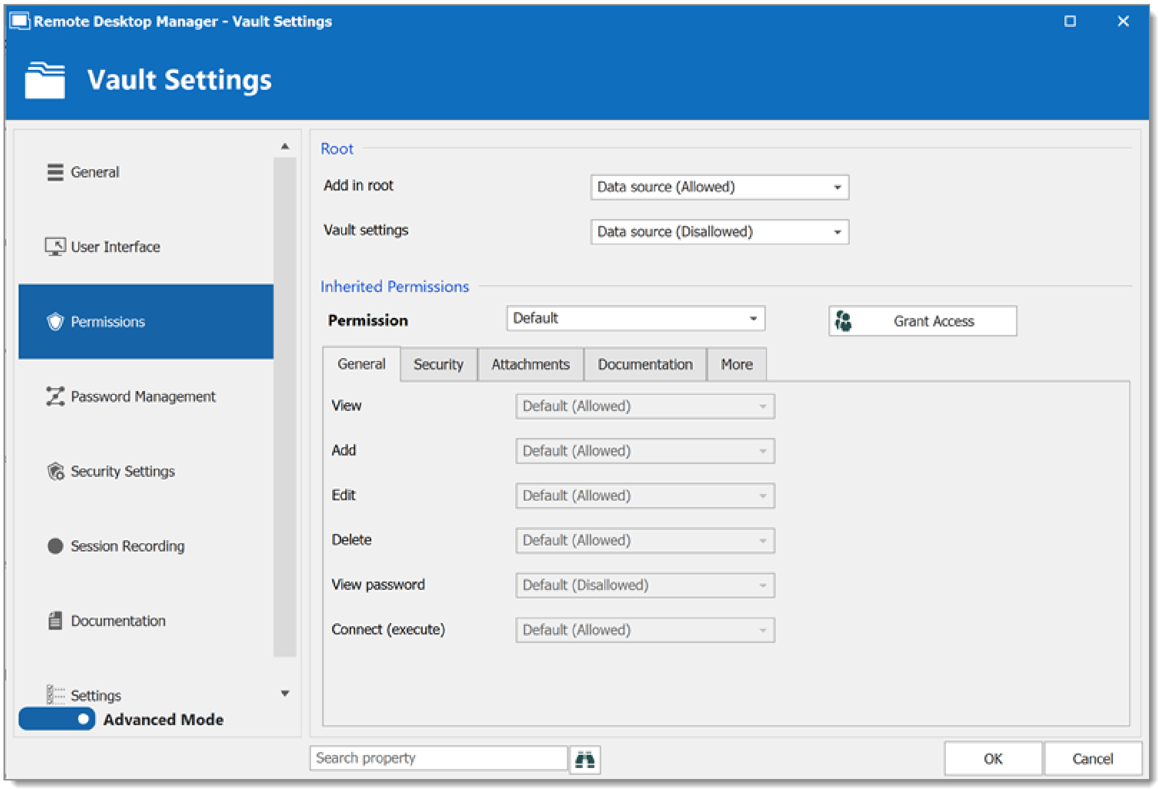
Access is granted or denied to users by setting permission on entries. Permissions can be set to users or user groups. The best practice is to grant permissions to user groups to control access for multiple users at once.

To set permissions on an entry, edit any entry, then navigate to the **Permissions** section.



Entry's Permissions

Permissions are usually set on folders, and apply to all child entries. A best practice is to set all the permissions of the Vault folder to **Never**. As a result, all permissions of all entries are denied by default.

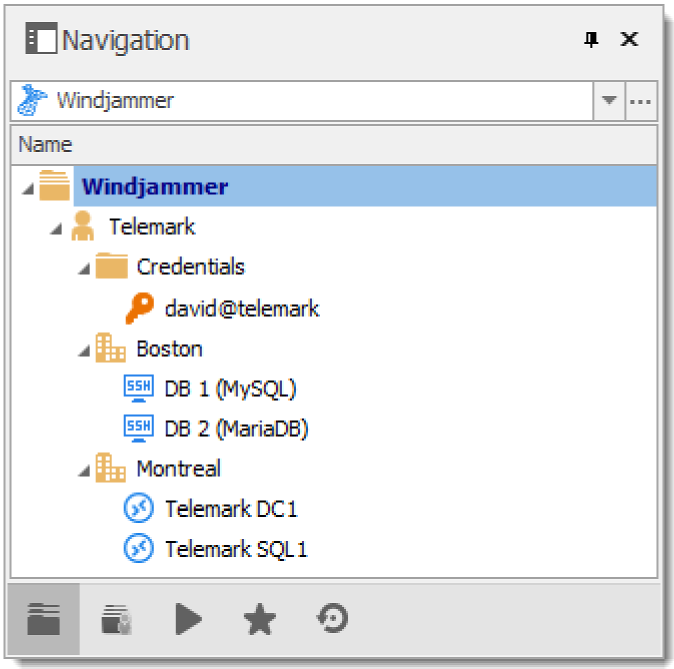


Vault Settings Permissions

Access is denied to users by expressly granting the access to other users. In other words, all users that are not on the list of a permission have the access denied.

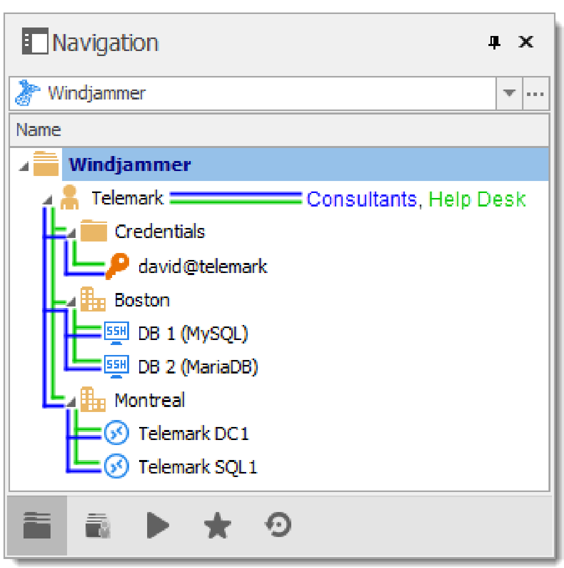
For a user to have access to a sub folder, the user must have at least the view permission on all parent folders.

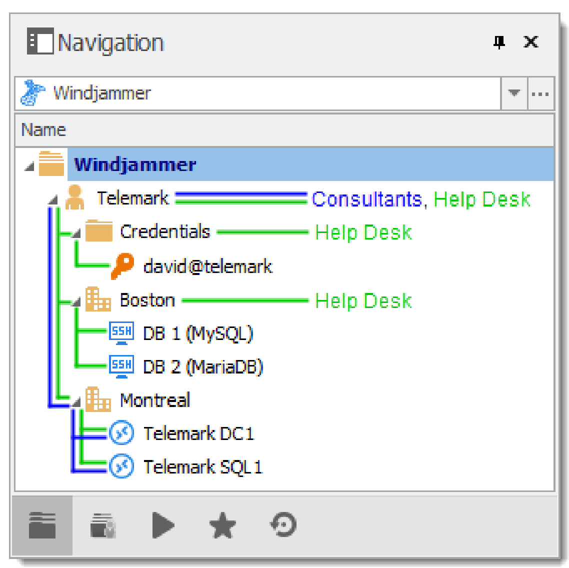
Consider the following structure:



There are three levels of folders: the Vault, Telemark, and child items of Telemark.

Suppose that a user, such as a consultant, must have access to the Montreal folder only. The consultant must be granted the view permission on the Telemark folder as well. However, granting the view access to the Telemark folder gives to the consultant the permissions to view all child items of Telemark. To deny the view permissions for the consultant on specific child items, the view permissions of these items must be expressly set for other users.



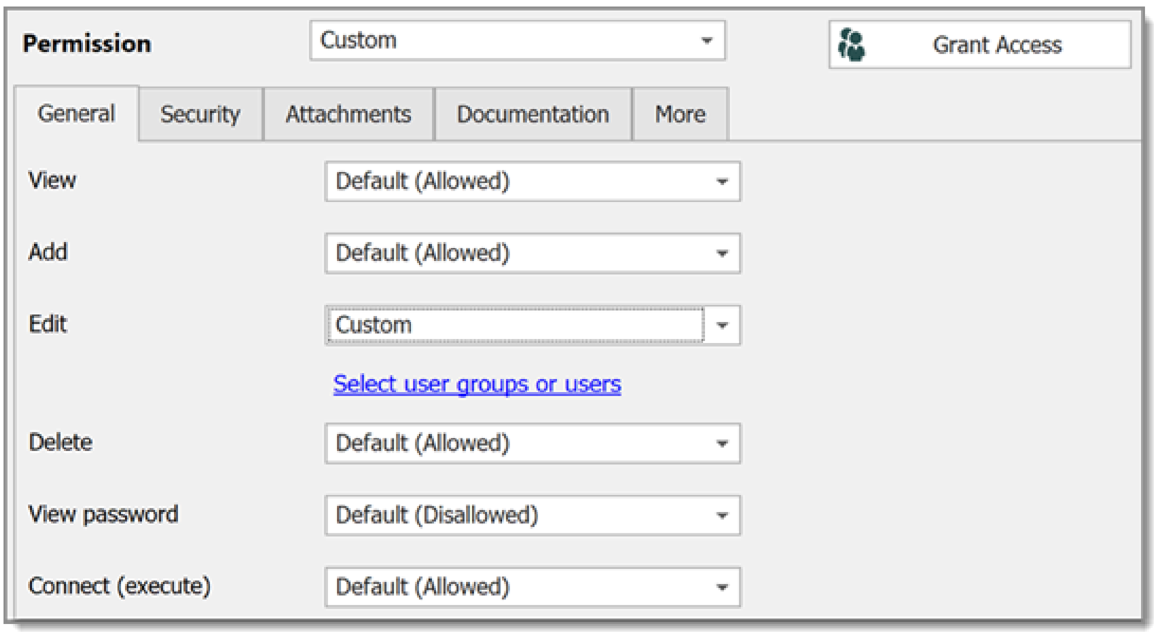


8.1 Permission

DESCRIPTION

The Permission window which is only available in an Advanced Data Source, can be found in every entry properties in the **Permission** section.

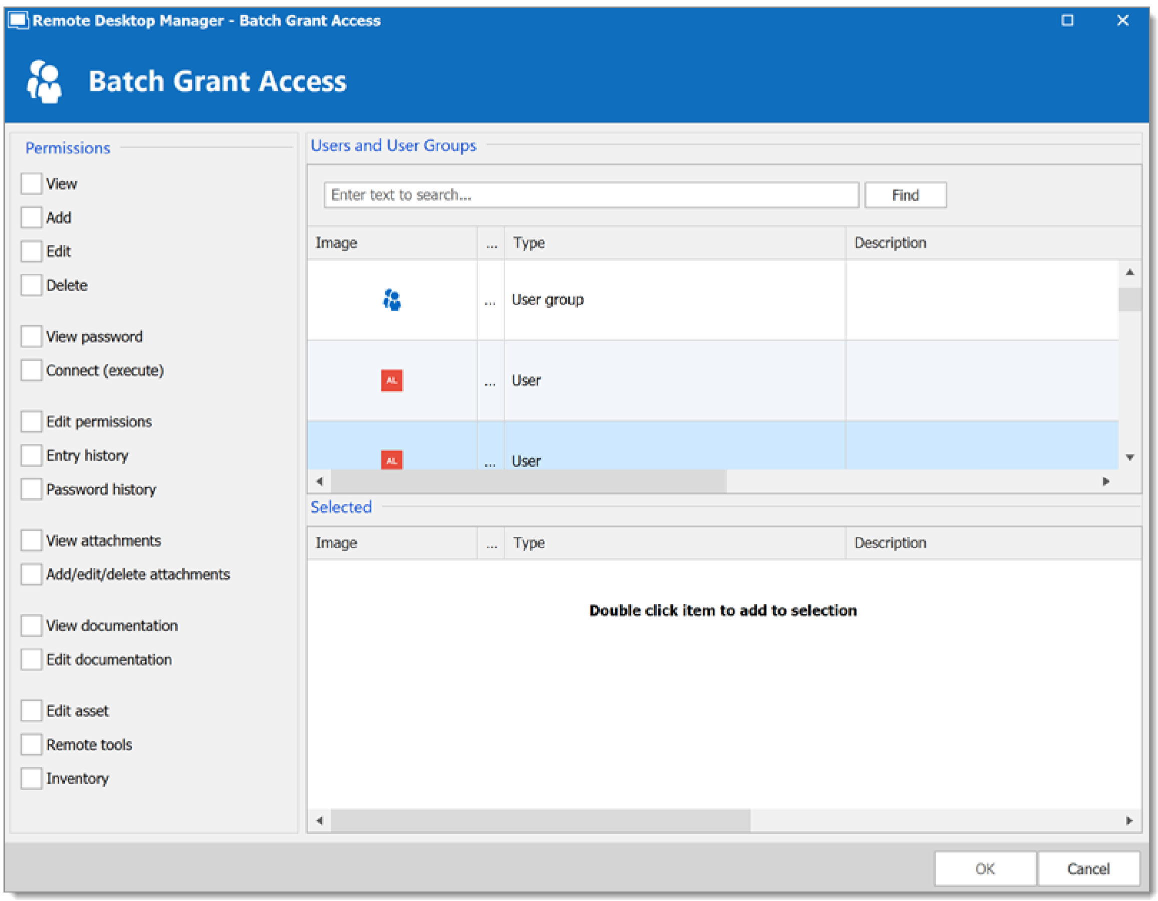
The user group based permission system can give a very accurate control of the security. Here is an overview of the permission window:



Permission panel

OPTION	DESCRIPTION
Permission	Sets the permission mode. Select between: • **Inherited (Default)**: will inherit the permissions from the parent groups. • **Custom**: lets you specify a custom value for each of the permission. • **Everyone**: everyone will be granted all the permissions below. • **Never**: no one but the administrators will be granted the permission.

OPTION	DESCRIPTION
Grant Access	Allows batch granting access to a specific entry or entries.
Inherited values	Indicates what is inherited from parent groups.
Select user groups or users	Lets you select Users / User groups to be granted the permission. Available only if the permission is set to **Custom**.



Batch Grant Access

8.2 Scenarios

8.2.1 Simplified Security

DESCRIPTION

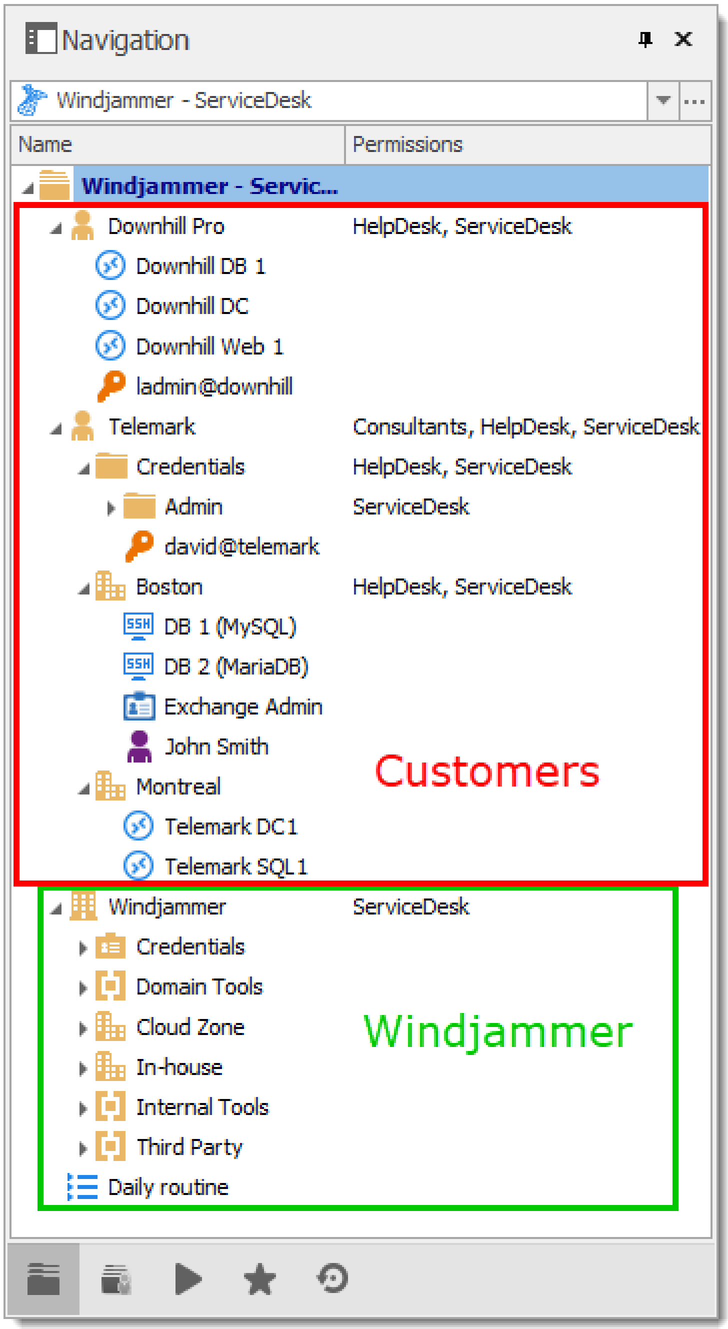
This feature is only available when using an Advanced Data Source.

While the following scenario is relevant for small to medium enterprises, it is not recommended for a larger business. For a scenario more suited for large enterprises, please consult the Advanced Security scenario.

Watch Video

Our fictional company, Windjammer, has four User Groups: HelpDesk, ServiceDesk, Administrations, and Consultants. There are two client companies: Downhill Pro and Telemark.

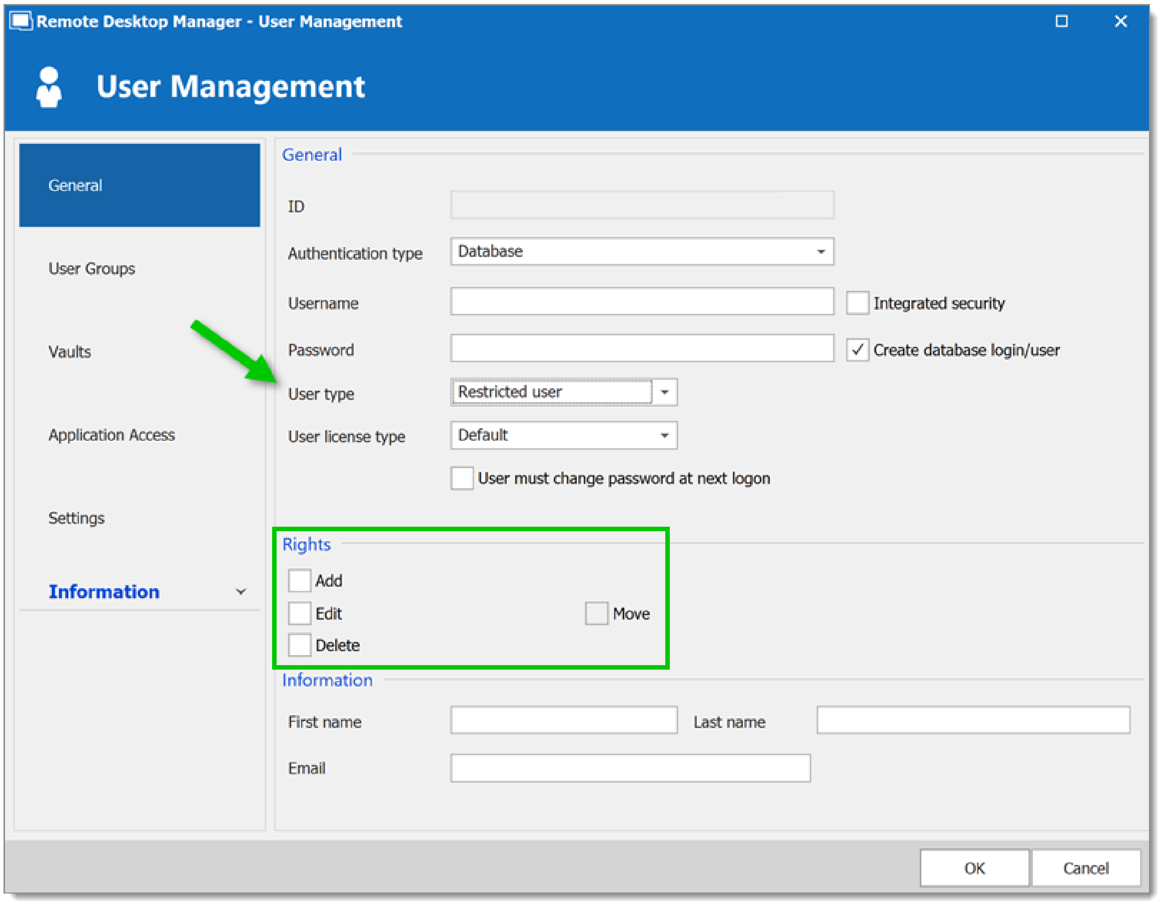
The following tree structure represents entries which users have access to once all permissions are set:



USER CONFIGURATION

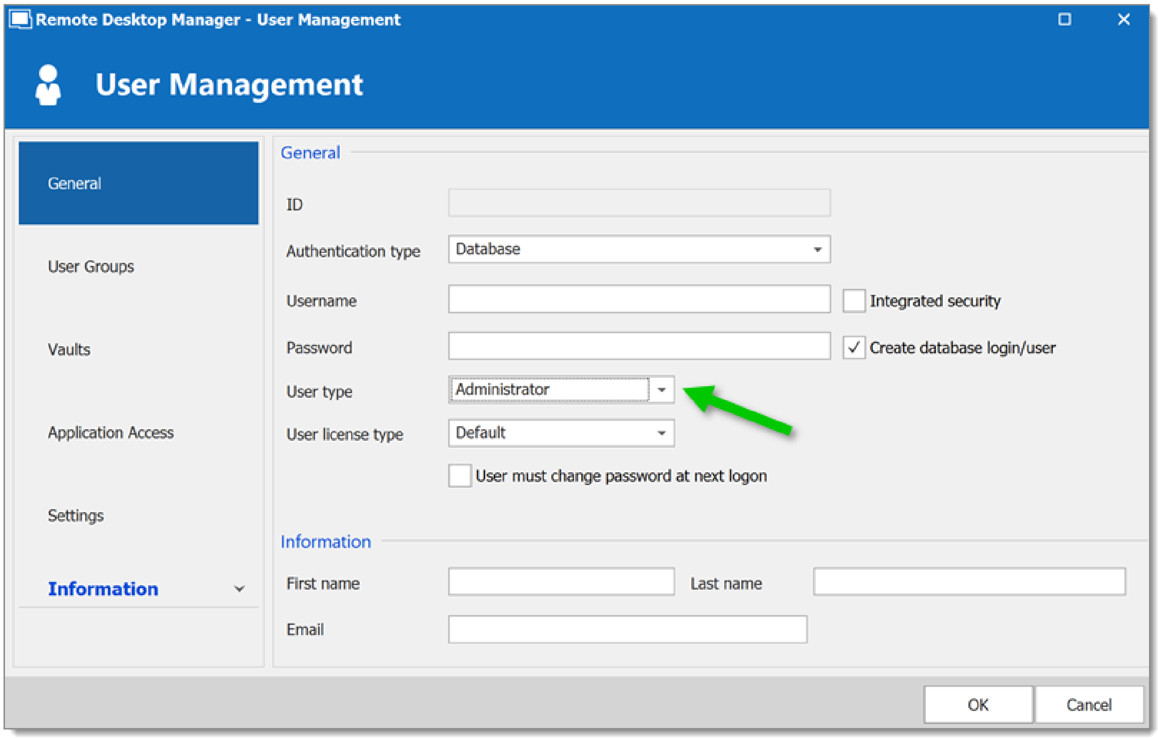
Here is an example for user configuration. To create users, navigate to ***Administration – Users – Add User***.

The following rights selection is available when setting a user to **Restricted user**.



User Management - Rights Section

Administrators: administrators have a lot more access than regular users. When creating these users, set the User type to **Administrator** to give them access to everything. The administrator can access all entries, regardless of permissions.



User Management - Administrator

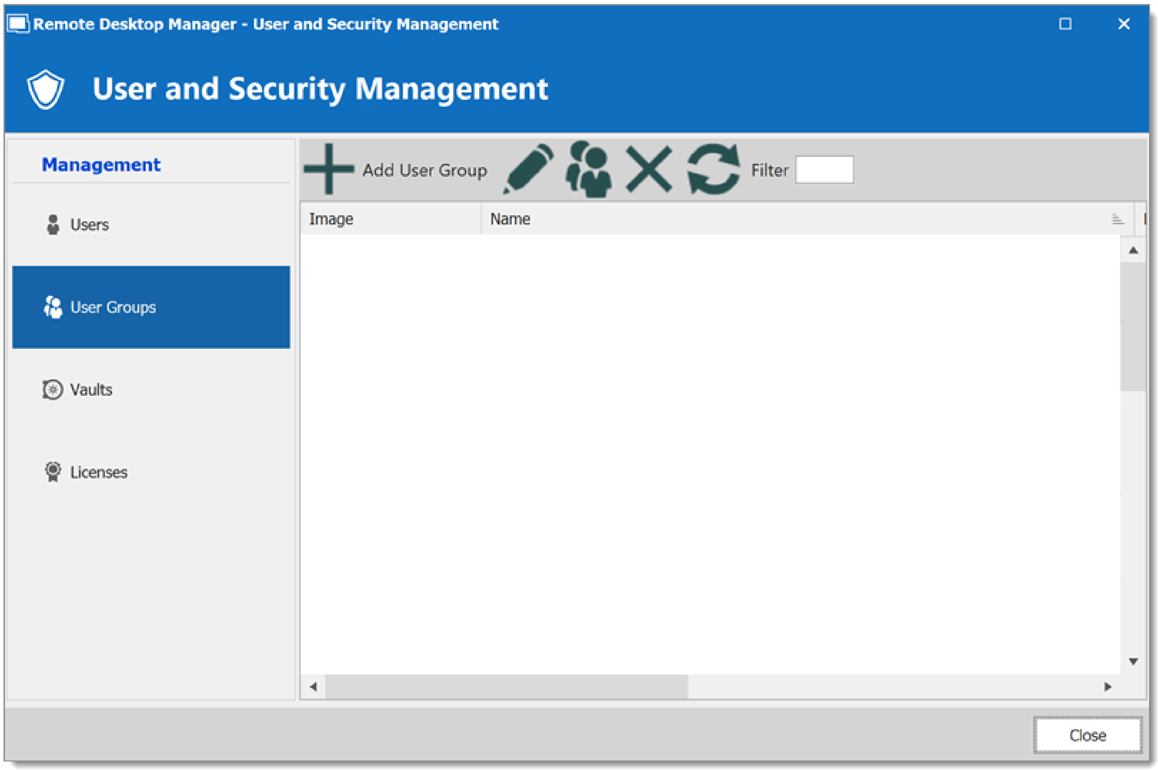
Regular users (User): these users have fewer rights than administrators. They essentially have all the basic rights (except for **View Password**) but are susceptible to all denied permissions. Later, we will deny these rights by specifying which users can actually perform these actions.

Consultants: consultants can only view a subset of entries, we will set those as **Read-Only**. They cannot add, edit or otherwise affect the information in any way.

USER GROUPS CONFIGURATION

Now that the users are created, we will add the user groups which we will later grant the permissions to. We need to create the user groups to assign users to them. There is no need to grant any privileges to these user groups.

- ServiceDesk
- HelpDesk
- Consultants



User and Security Management - User Groups

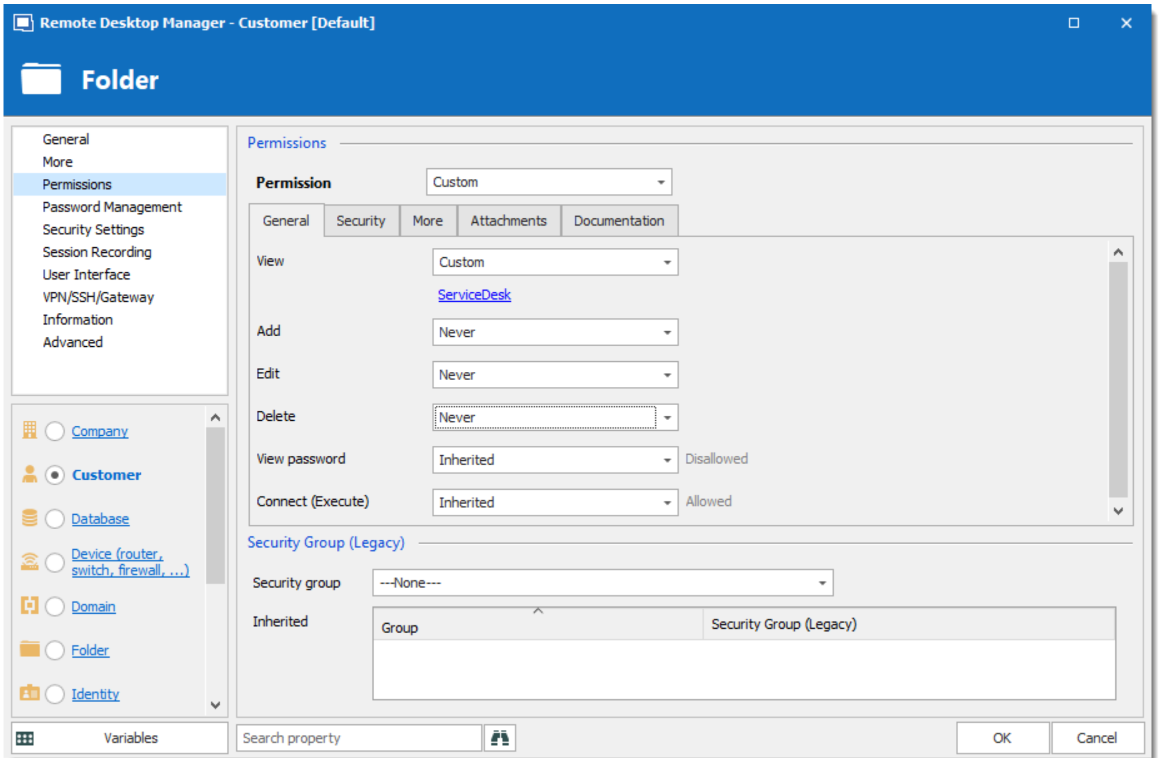
ENTRIES CONFIGURATION

Now, everything is ready to grant or deny access to the user groups.

- The ServiceDesk will have the permission to view and open all entries but will be able to edit only the entries in the customer groups/folders.
- The HelpDesk will have the permission to view and open entries in the customer groups/folders only and will not be able to edit them.
- The Consultants will have the permission to view and open entries in the Montreal folder only but will not be able to edit it nor its child items.

We will begin with the Vault level folders: Downhill Pro, Telemark and Windjammer.

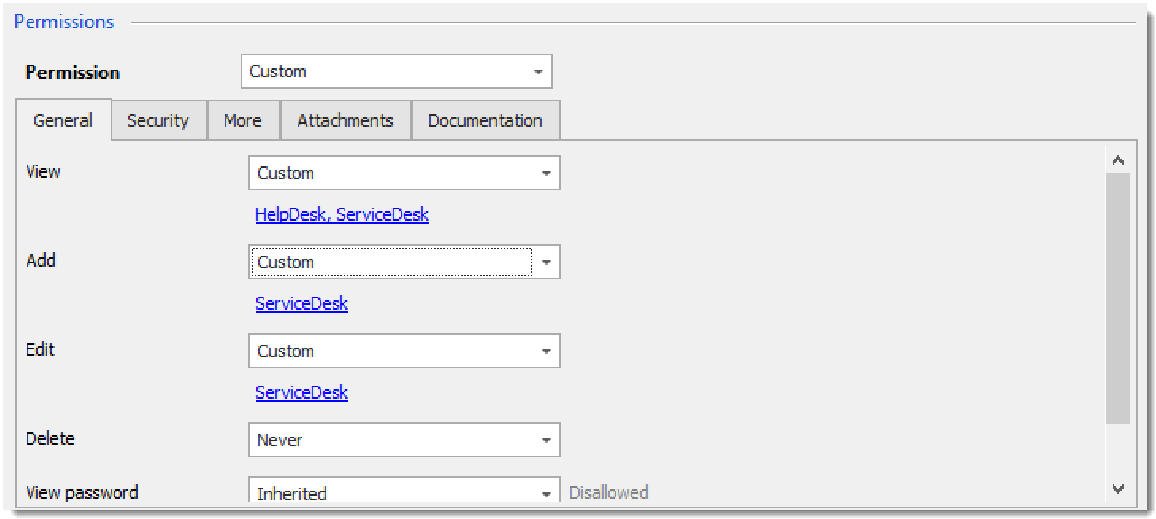
The permission to view the Windjammer folder will be set for the ServiceDesk only since we want them to be able to use its child entries. We don't want the ServiceDesk to add or edit anything. We will set the **Add**, **Edit** and **Delete** permissions to **Never**. Only the administrator will be able to add or edit entries in the Windjammer folder.



Windjammer - Permissions

- **View**: **Custom**; ServiceDesk.
- **Add**: **Never**; Only the administrator can add entries.
- **Edit**: **Never**; Only the administrator can edit entries.
- **Delete**: **Never**; Only the administrator can delete entries.

For Downhill Pro, we will grant permissions to the ServiceDesk and the HelpDesk.

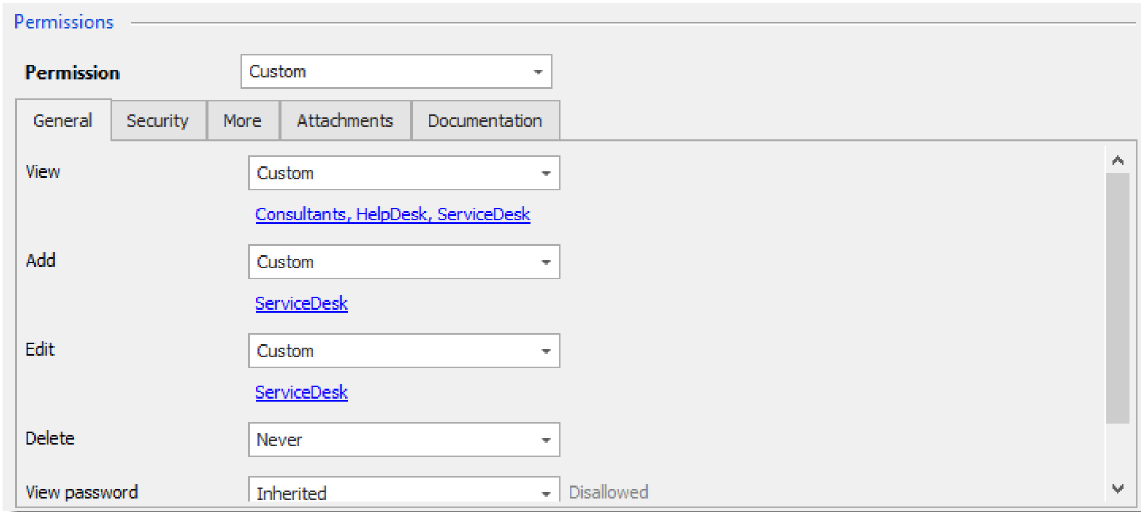


Downhill Pro - Permissions

- **View**: **Custom**; HelpDesk, ServiceDesk.
- **Add**: **Custom**; ServiceDesk.
- **Edit**: **Custom**; ServiceDesk.
- **Delete**: **Never**; Only the administrator can delete entries.

We already have a good example of the flexibility of Remote Desktop Manager's Security. A ServiceDesk user can view and use all the entries in the Downhill Pro folder, even the credential entries, but it will never be able to see any password since View Password is Disallowed (from the Vault folder).

Next, for the Telemark folder, we will grant permissions to the ServiceDesk, the HelpDesk and the Consultants. This is where things get complex. If we want the Consultants to be able to view only the Montreal folder which is a child item of Telemark, we must grant to consultants the permission to view the entire Telemark content. Then we will grant permissions on child items only to the user group that should have access to these items. This last step will deny the view permission for the consultants on the child items.

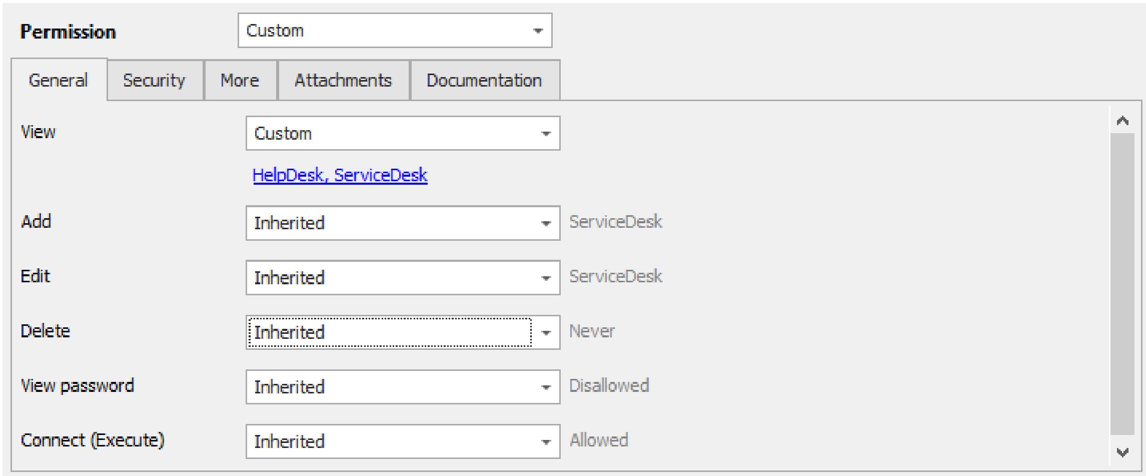


Telemark - Permissions

- **View**: **Custom**; Consultants, HelpDesk, ServiceDesk.
- **Add**: **Custom**; ServiceDesk.
- **Edit**: **Custom**; ServiceDesk.
- **Delete**: **Never**; Only the administrator can delete entries.

Since we want the users to be able to use the credential entries, we will grant the ServiceDesk and the HelpDesk the permission to view the Credentials folder. This way, the ServiceDesk and HelpDesk will be able to use the entries in the folder without revealing the passwords. Therefore, by specifying that only the HelpDesk and ServiceDesk have the **View** permission, we deny the view access to any user group or user that is not in the list of the permission.

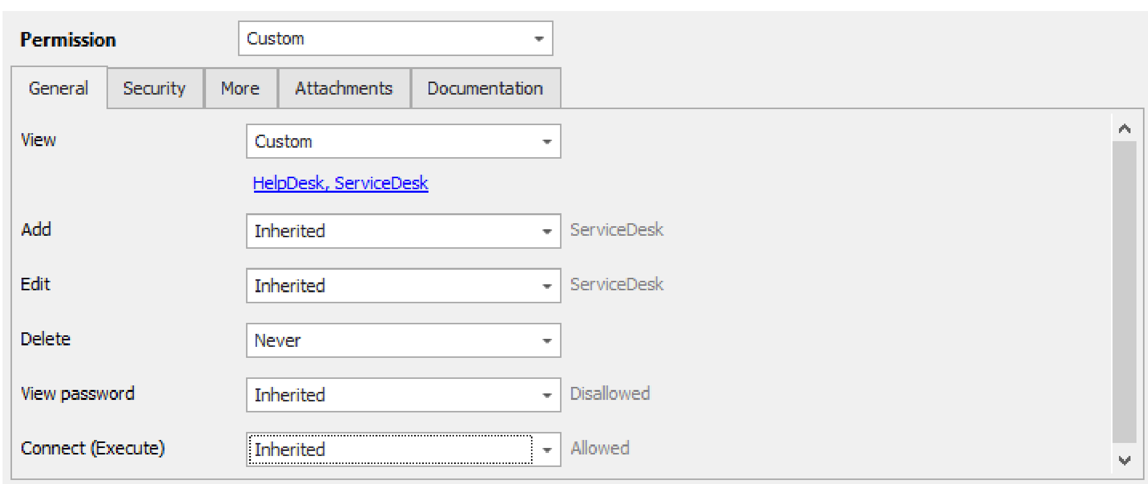
The **Add**, **Edit** and **Delete** permissions can be left to **Inherited** since they inherit the settings from the Telemark parent folder. The ServiceDesk is the only user group that has been granted the **Add** and **Edit** permission in the parent folder and the **Delete** permission inherits the Never setting.



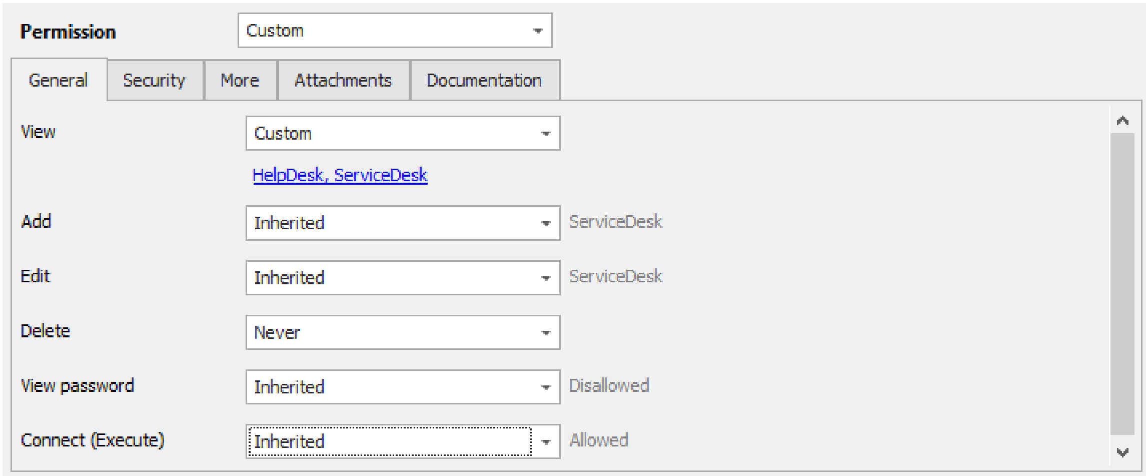
Telemark\Credentials - Permissions

- **View**: **Custom**; HelpDesk, ServiceDesk.
- **Add**: **Inherited**; ServiceDesk inherited from Telemark folder.
- **Edit**: **Inherited**; ServiceDesk inherited from Telemark folder.
- **Delete**: **Inherited**; Never inherited from Telemark folder.

We want the ServiceDesk to be able to use the Domain Admin credential entry as well but not the HelpDesk. For this we must grant the **View** permission to the ServiceDesk. The ServiceDesk will still be able to edit the credential entry but will never see the password. The delete permission is set to **Never**.



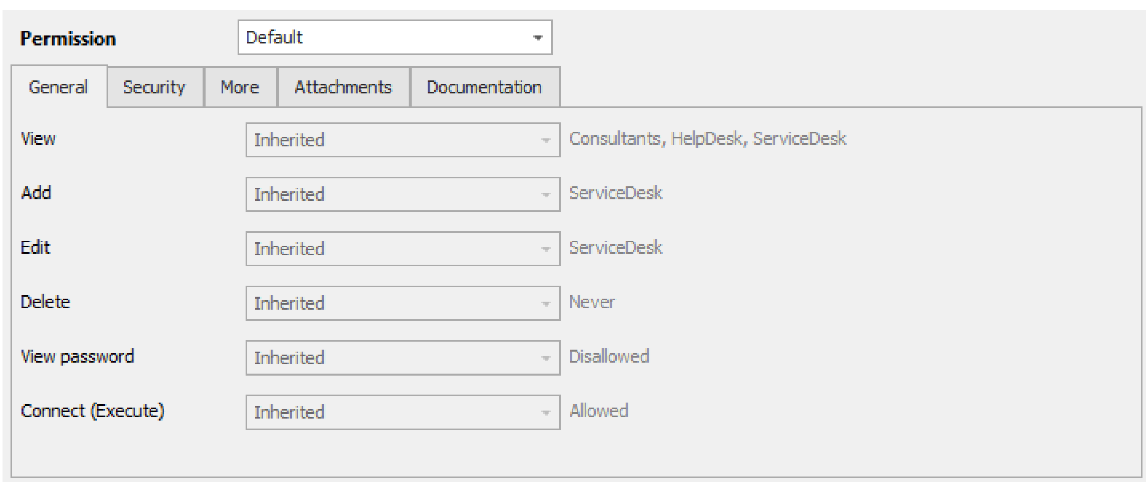
The last step for the Telemark child items is to set the **View** permission to the ServiceDesk and the HelpDesk on the Boston folder and leave every other permission of this folder to **Default**. This denies the Consultants to view the Boston folder. Now, the Consultants will be able to view and open entries only in the Montreal folder.



Telemark\Boston - Permissions

Every time a new folder is added, the **View** permission must be set for ServiceDesk and HelpDesk to hide the new folder and its content from the Consultants.

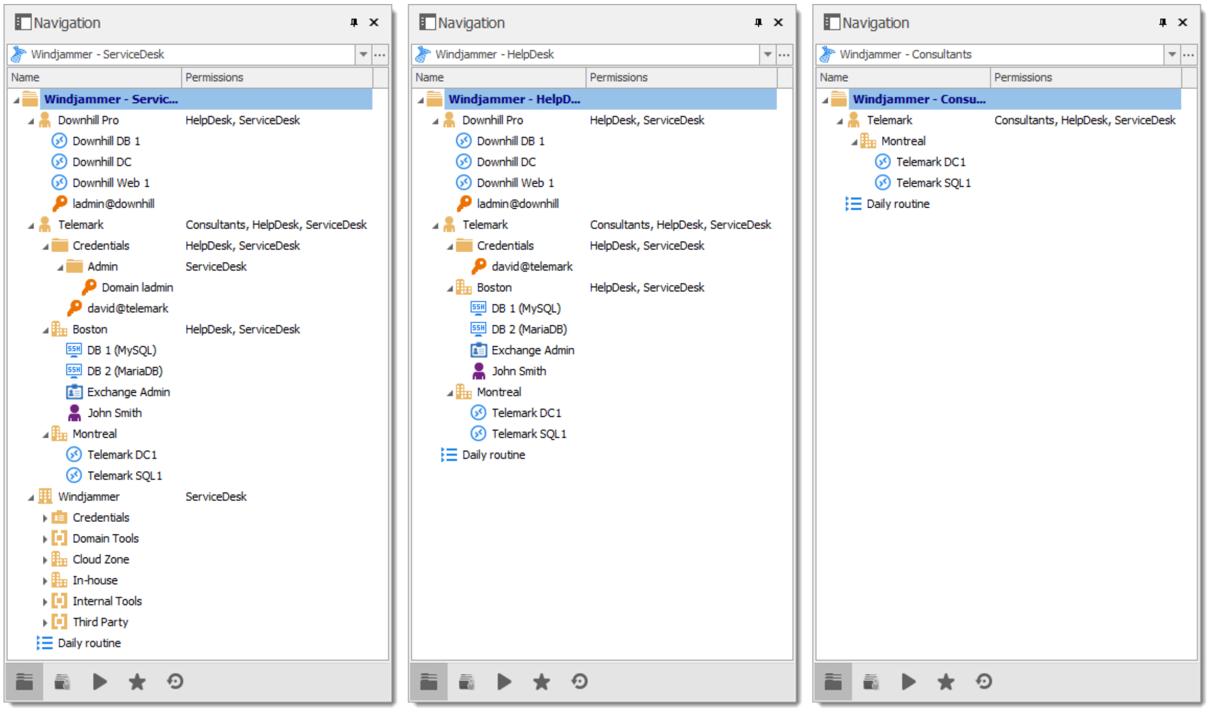
No need to set any permissions on the Montreal folder, since they are inherited from the parent folders.



Telemark\Montreal - Permissions

IN CONCLUSION

The permissions are now correctly set. Note that every entry added at Vault level will have no security by default. This means they would be available for anyone, even the consultants. This can be confirmed by looking at the screenshot below in which the entry **Daily routine** is available for everyone. Here is what each user should see in the tree view:



Side by Side Tree View

You can further customize your permissions by using the **Security Settings** tab when editing entries, or the **Logs** tab to add more traces of coming and goings. As always, great care must be taken when granting permissions.

If you need more details on each permission, please consult our Common Settings – Permissions topic.

8.2.2 Advanced Security

DESCRIPTION

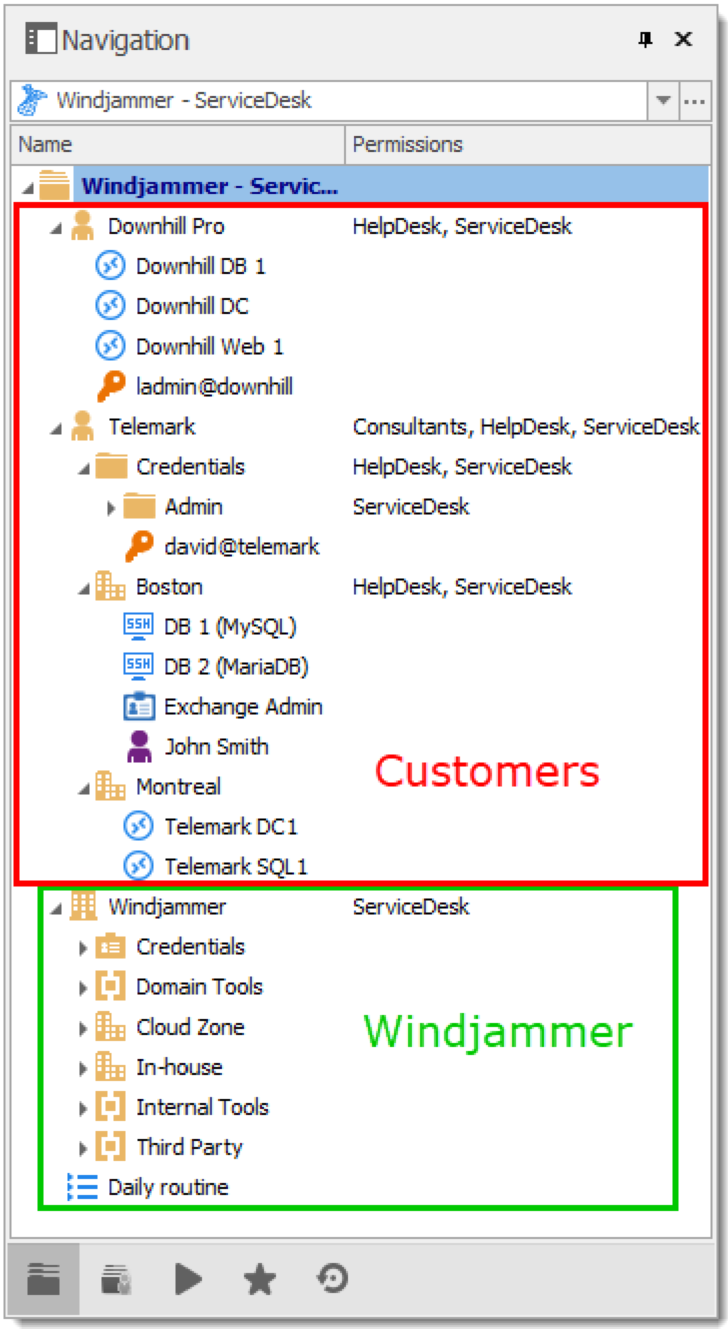
> This feature is only available when using an Advanced Data Source.

> The following scenario is designed for large enterprises. For a scenario more suited for small enterprises, please consult our Simplified Security scenario.

While this example fits for large enterprises, please keep in mind that any privilege should be granted only as necessary. Be careful when granting permissions to a user or a user group.

Our fictional company, Windjammer, has three user groups: HelpDesk, ServiceDesk, and Consultants. There are two client companies: Downhill Pro and Telemark.

The following tree view structure represents entries which users have access to once all permissions are set:



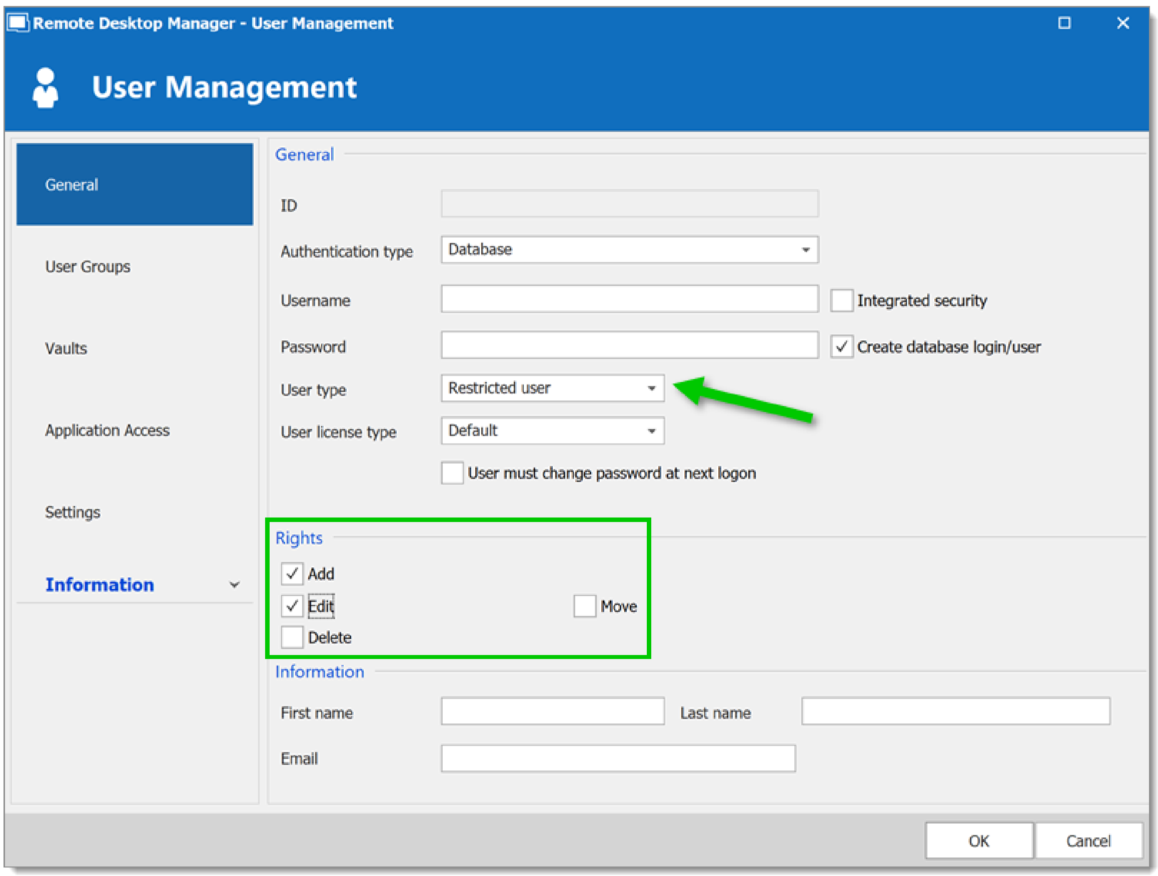
USER CONFIGURATION

Here is an example of user configuration. To create users, navigate to ***Administration – Users – Add User.***

In this scenario, all the options in the **Privileges** section of the **User Management** are set to **None**.

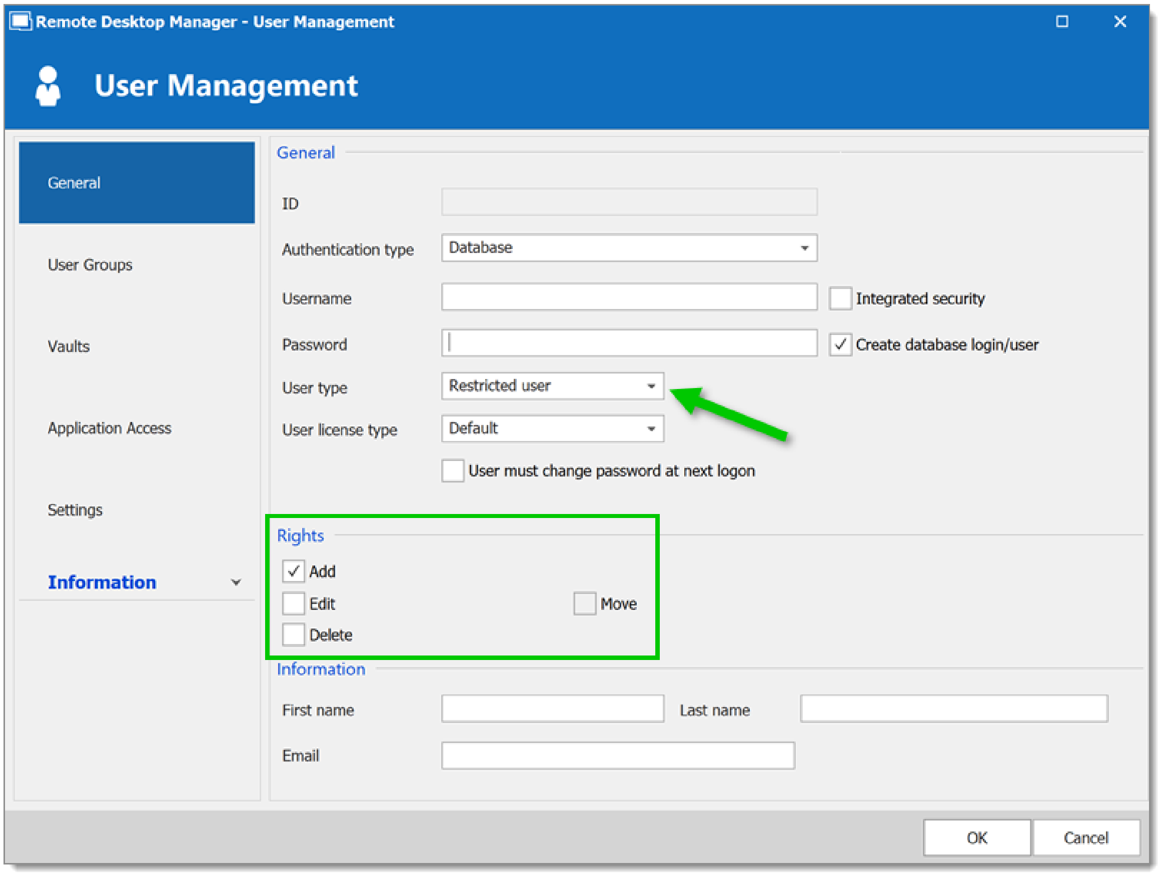
Here we select the user type to give them the most basic rights (**Add**, **Edit**, and **Delete**).

ServiceDesk users are **Restricted users**. They have the **Add** and **Edit** rights. However, they cannot add entries into the Vault folder.



User Management - ServiceDesk - Restricted User

HelpDesk users are **Restricted Users** as well. They only have the **Add** right. However, they cannot add entries into the Vault folder.



User Management - HelpDesk - Restricted User

Consultants are **Read Only Users** and can only view a subset of entries. They cannot add or edit anything.

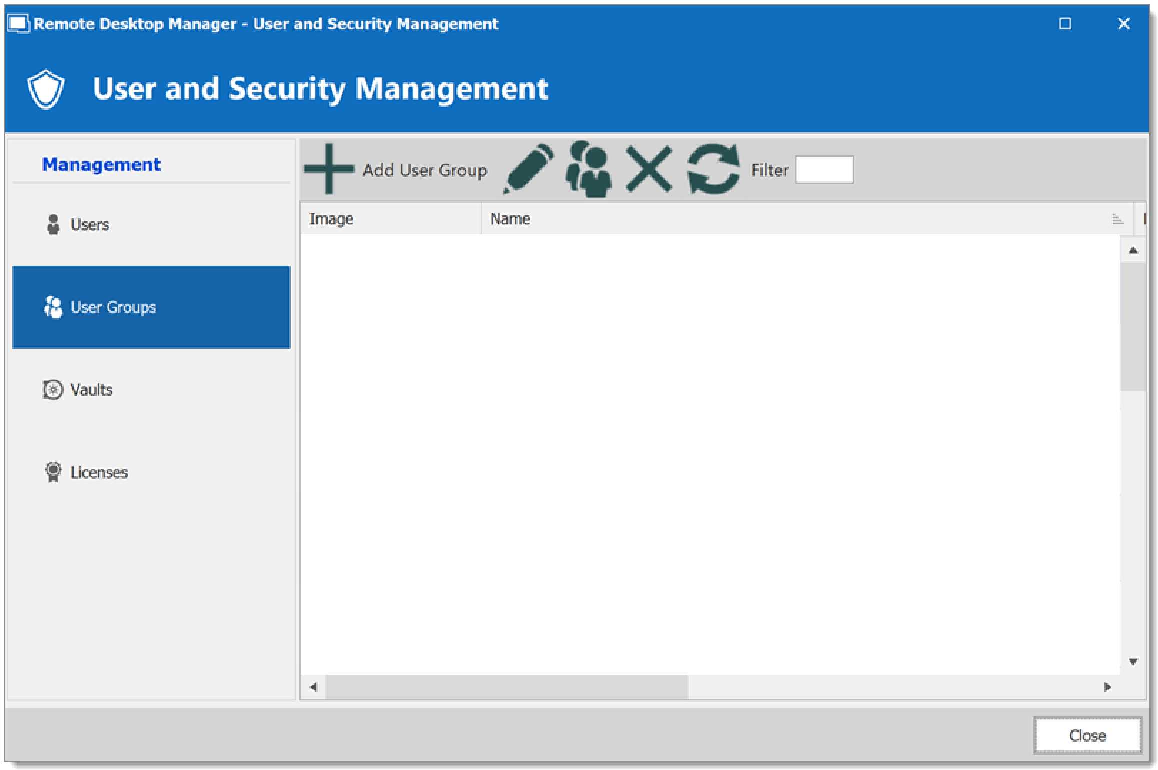
USER GROUPS CONFIGURATION

Now that the users are created, we will add the user groups which we will later grant the permissions to. We need to create the user groups and assign the respective user to each user group. There is no need to grant any privilege to these user groups since they are mainly empty shells used to group multiple users. This allows for controlling multiple users at once instead of granting permissions to each users, one at a time.

- ServiceDesk
- HelpDesk
- Consultants

To add a user group, click the **Add User Group** button, enter a name for the user group, and click **Ok**.

To assign users to a user group, select a user group and click the **Assign User Groups** button. Use the **Is Member** check boxes to add users to the user group.



User and Security Management - User Groups

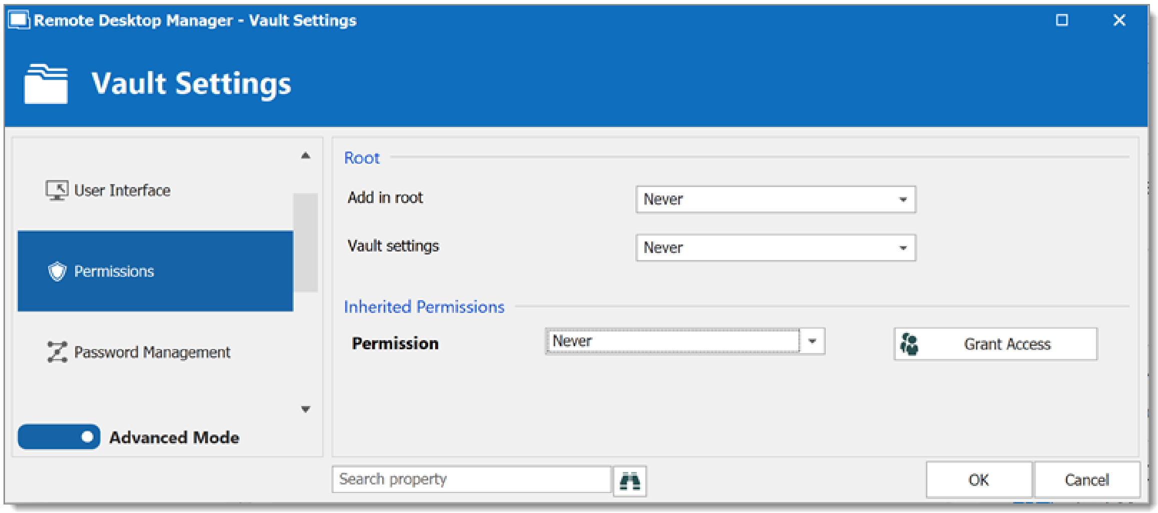
ENTRY CONFIGURATION

Now, everything is ready to grant or deny access to the user groups.

- All Vault folder permissions are set to **Never**. By inheritance, this denies the child items default access to everyone.
- The ServiceDesk has the permission to view and open all entries but is able to edit only the entries in the client's groups/folders.
- The HelpDesk has the permission to view and open entries in the client's groups/folders only and is not able to edit them.
- The Consultants have the permission to view and open entries in the Montreal folder only but is not able to edit it or its child items.

Vault Settings

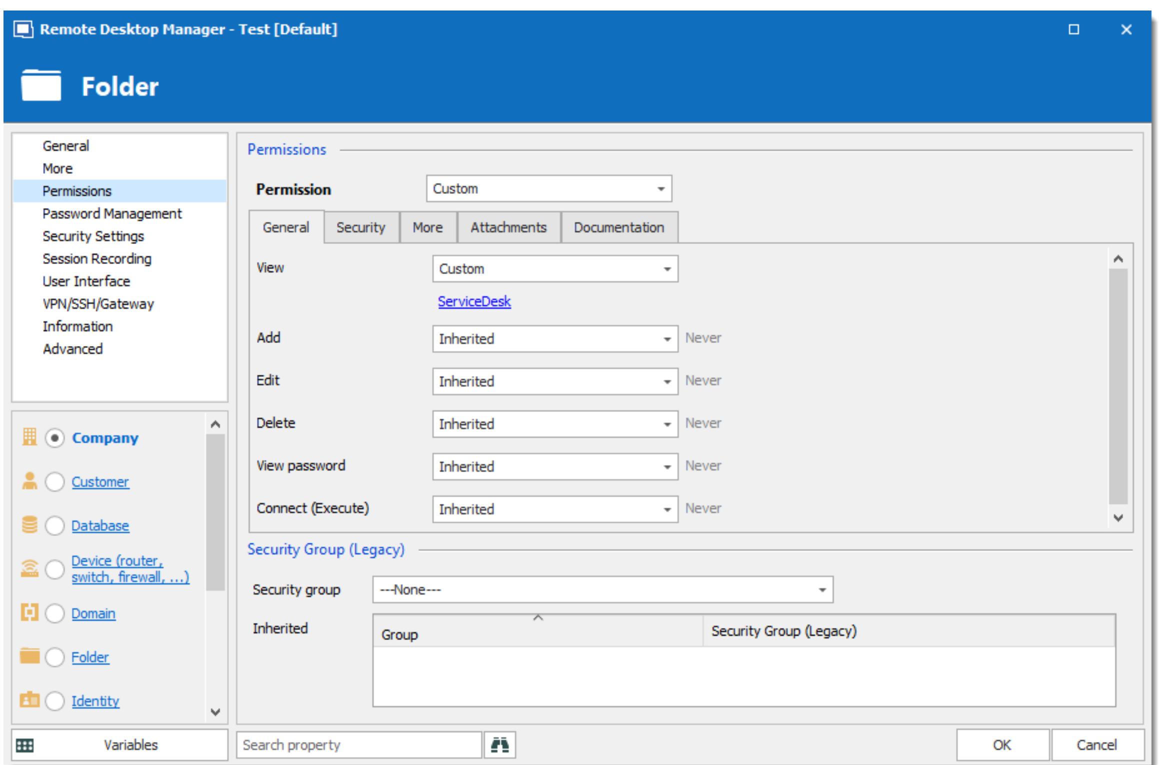
As mentioned above, **ALL** Vault settings folder permissions are set to **Never**. This denies the default access to other users.



Vault Settings - Permissions

Windjammer Downhill Pro, and Telemark, the Vault level groups/folders

The permission to view the Windjammer folder is set for the ServiceDesk only since we want them to be able to use the child entries. We don't want the ServiceDesk to add, edit or delete anything. We leave the **Add**, **Edit** and **Delete** permissions to **Inherited** so only the administrators can perform these action on the Windjammer folder and its child items.

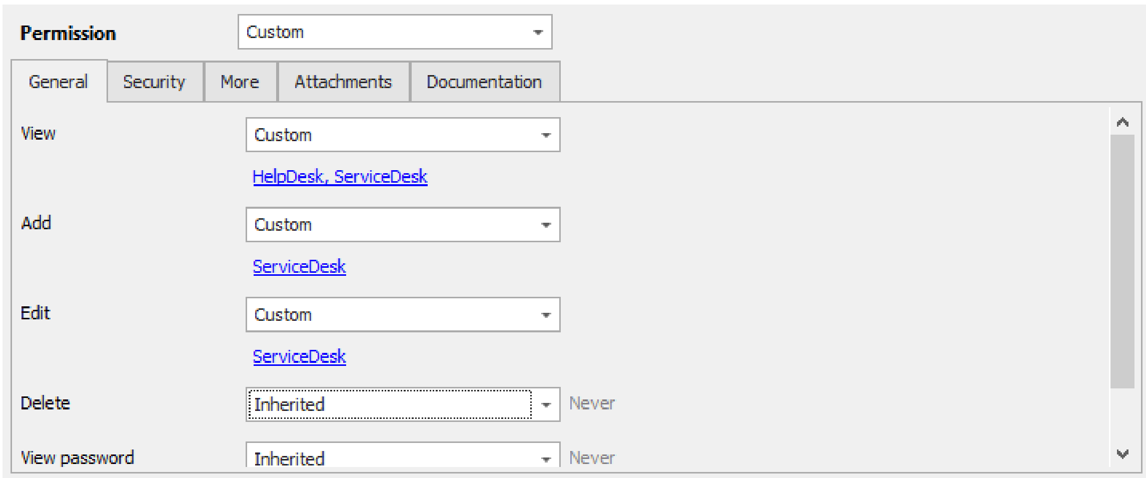


Windjammer - Permissions

- **View: Custom;** ServiceDesk.

- **Add: Inherited; Never** inherited from Vault. Only the administrator can add entries.
- **Edit: Inherited; Never** inherited from Vault. Only the administrator can edit entries.
- **Delete: Inherited; Never** inherited from Vault. Only the administrator can delete entries.

For Downhill Pro, we grant permissions to the ServiceDesk and the HelpDesk.

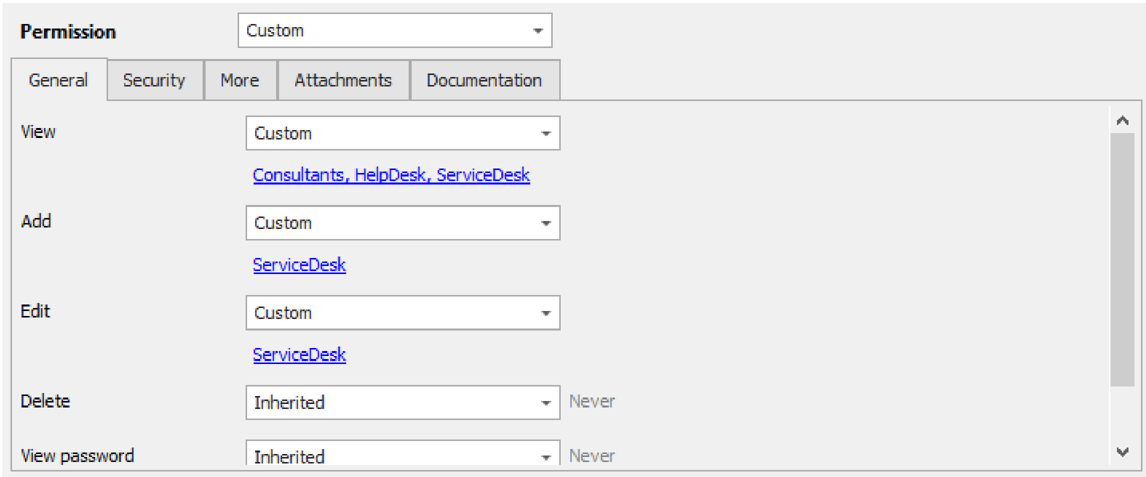


Downhill Pro - Permissions

- **View: Custom;** HelpDesk, ServiceDesk.
- **Add: Custom;** ServiceDesk.
- **Edit: Custom;** ServiceDesk.
- **Delete: Inherited; Never** inherited from Vault. Only the administrator can delete entries.

We already have a good example of the flexibility of Remote Desktop Manager Security. ServiceDesk and HelpDesk users can view and use all the entries in the Downhill Pro folder, even the credential entries, but they will never see any passwords since the ServiceDesk and HelpDesk users do not have the privilege to reveal passwords.

Next, for the Telemark folder, we grant permissions to the ServiceDesk, the HelpDesk and the Consultants. This is where things get complex. If we want the Consultants to be able to view only the Montreal folder, which is a child item of Telemark, we must grant Consultants the permission to view the parent folder, thereby the entire Telemark content. Then we will grant permissions on child items only to the user group that should have access to these items. This last step will deny the view permission for the Consultants on the child items.



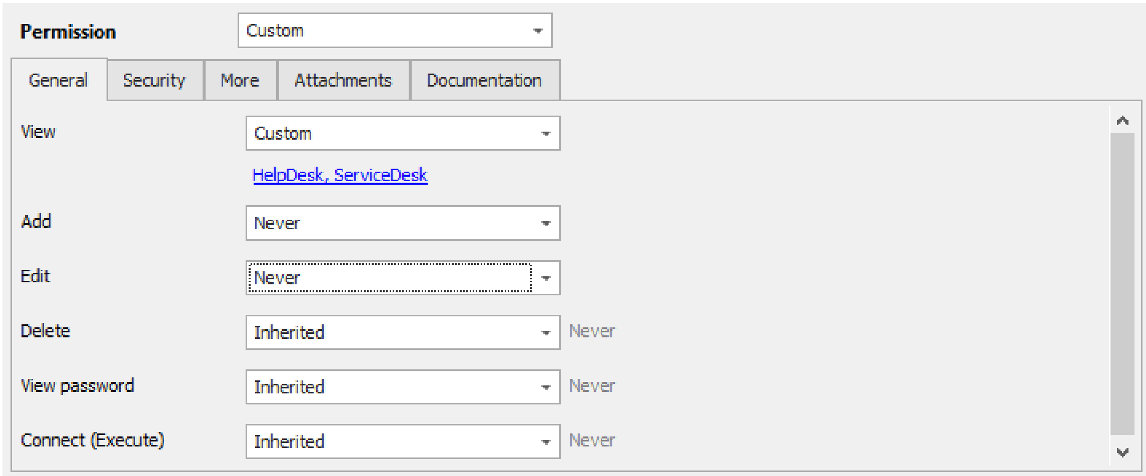
Telemark - Permissions

- **View: Custom;** Consultants, HelpDesk, ServiceDesk.
- **Add: Custom;** ServiceDesk.
- **Edit: Custom;** ServiceDesk.
- **Delete: Inherited; Never** inherited from Vault. Only the administrator can delete entries.

Telemark Child Items

Since we want the users to be able to use the credential entries, we grant the ServiceDesk and the HelpDesk the permission to view the Credentials folder. Therefore, the ServiceDesk and HelpDesk are able to use the entries in the folder without revealing the passwords. By specifying that only the HelpDesk and ServiceDesk have the **View** permission, we deny the view access to any user group or user that is not on the list of the permission.

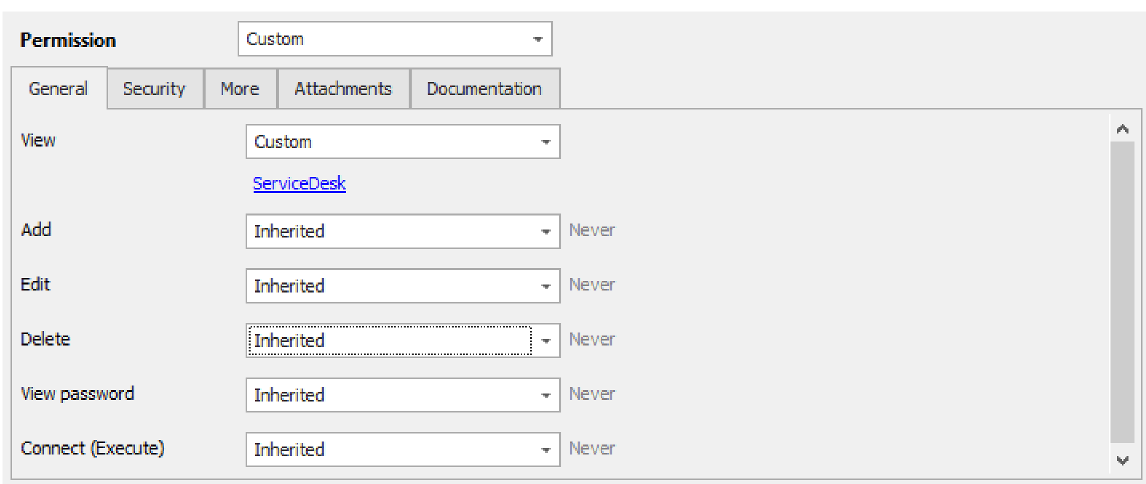
The **Add** and **Edit** permissions are set to **Never** and the **Delete** permission can be left to **Inherited** since it inherits the **Never** settings from the Vault. Only the administrators can perform these actions in groups/folders containing credentials.



Telemark/Credentials - Permissions

- **View: Custom;** HelpDesk, ServiceDesk.
- **Add: Never;** Only administrators can add credential entries.
- **Edit: Never;** Only administrators can edit entries.
- **Delete: Inherited; Never** inherited from Vault. Only administrators can delete entries.

We want the ServiceDesk to be able to use the **Domain Iadmin** credential entry, but not the HelpDesk. For this, we must grant the **View** permission to the ServiceDesk. The ServiceDesk is still be able to use the credential entry but will never see the password.

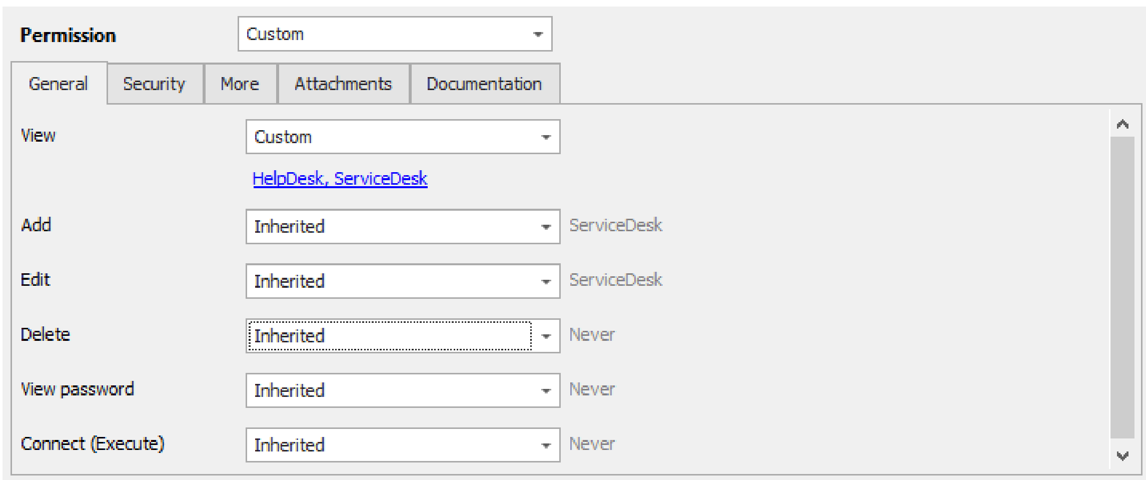


Telemark\Credentials\Admin - Permissions

- **View: Custom;** ServiceDesk.
- **Add: Inherited; Never** inherited from Vault. Only administrators can add credential entries.

- **Edit: Inherited; Never** inherited from Vault. Only administrators can edit credential entries.
- **Delete: Inherited; Never** inherited from Telemark\Credentials. Only administrators can delete credential entries.

The last step for the Telemark child items is to set the **View** permission to the ServiceDesk and the HelpDesk on the Boston folder and leave every other permissions of this folder to **Inherited**. This denies the Consultants to view the Boston folder. Now, the Consultants are able to view and open entries only in the Montreal folder.

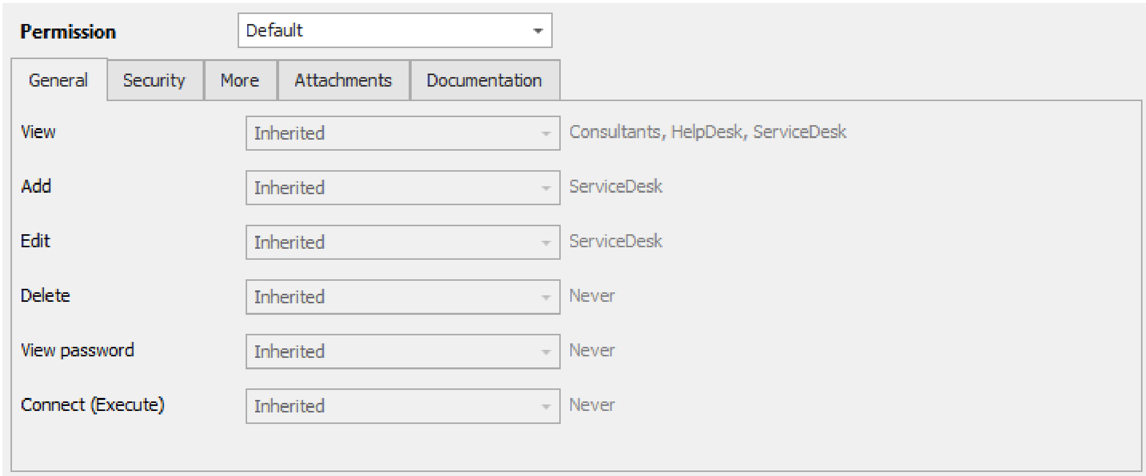


Telemark\Boston - Permissions

- **View: Custom;** HelpDesk, ServiceDesk.
- **Add: Inherited;** ServiceDesk inherited from Telemark.
- **Edit: Inherited;** ServiceDesk inherited from Telemark.
- **Delete: Inherited; Never** inherited from Vault.

> Every time a new folder is added as a child of the Telemark folder, the **View** permission must be set for ServiceDesk and/or HelpDesk to hide the new folder and its content from the Consultants.

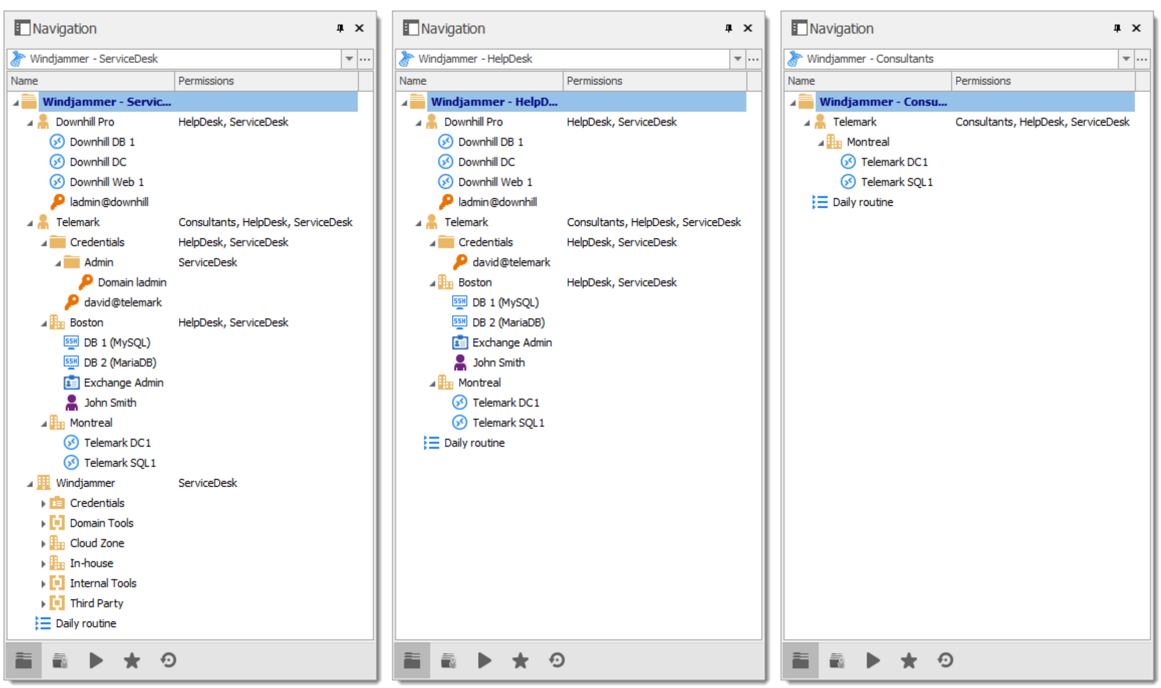
There is no need to set any permissions on the Montreal folder, since they all inherit values from parent folders.



Telemark\Montreal - Permissions

IN CONCLUSION

The permissions are now correctly set. Note that every entry added at Vault level are inheriting from the Vault as well. This means they would be available to admins only, unless their permissions were modified. This can be confirmed by looking at the screenshot below, in which the entry **Daily routine** is available for everyone (It's permissions have been changed to Everyone. Here is what each user should see in the tree view:



Side by Side Tree View

You can further customize permissions by using the **Security Settings** tab when editing entries. As always, great care must be taken when granting permissions.

8.3 Legacy Information

DESCRIPTION

Describing such a flexible security system takes a lot of effort. This chapter contains valuable information, but that may have been optimized by a newer topic.

8.3.1 Small to Medium Enterprise

DESCRIPTION

Here we will give you a security structure example that should be relevant for small to medium business.

In this scenario, all the options in the ***Privileges*** section of the user properties will be left disabled.

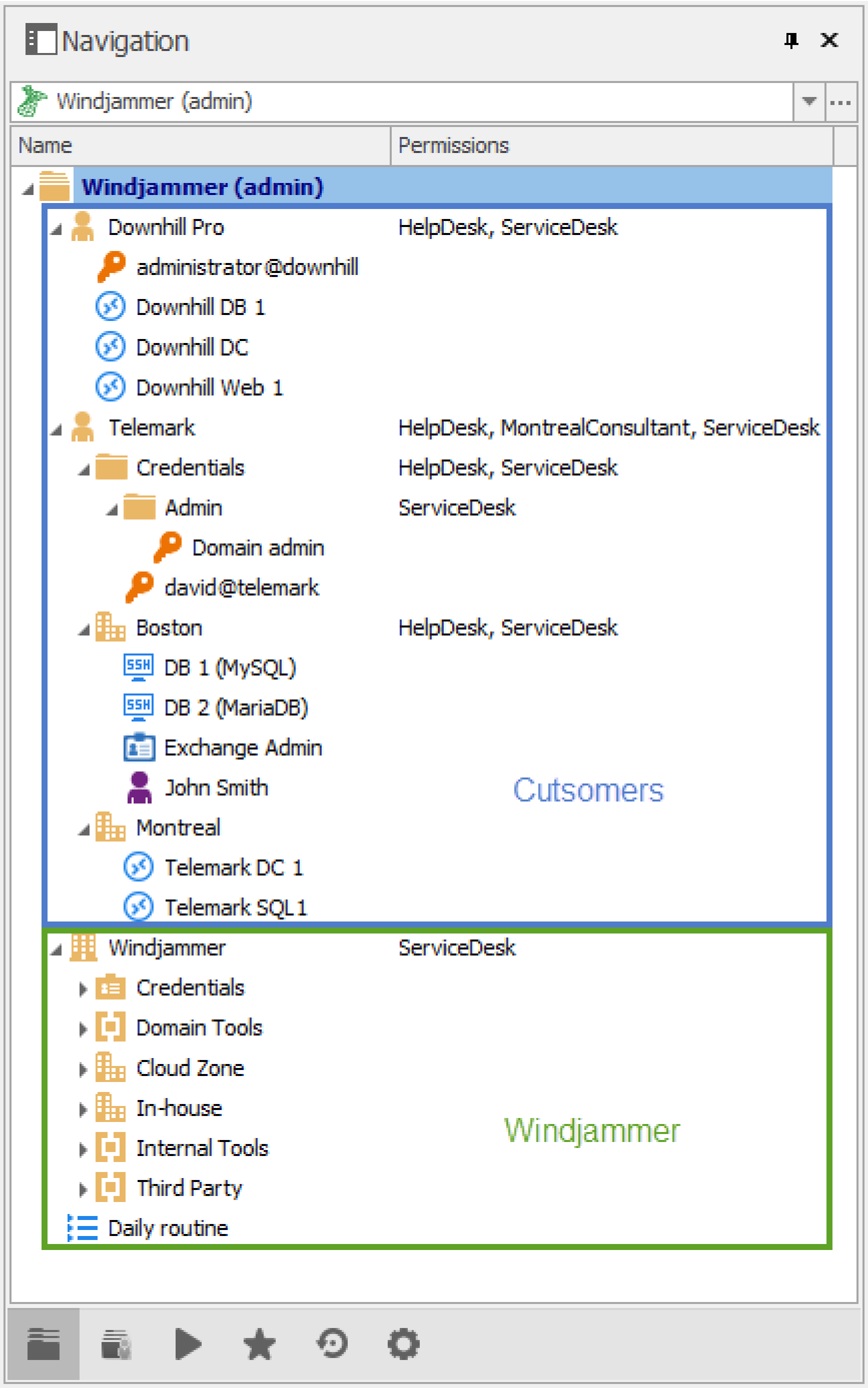
While this example might fit for many enterprises, please keep in mind that any privilege should be granted only if needed. Be extremely careful when granting permissions to a user or a user group.

This feature is only available when using an Advanced Data Source.

STEPS

Our fictional company *Windjammer* has a *HelpDesk* and a *ServiceDesk* department, an administrator and a *MontrealConsultant*. We can also see two customers: *Downhill Pro* and *Telemark*.

Here is a view of the data source tree view structure:



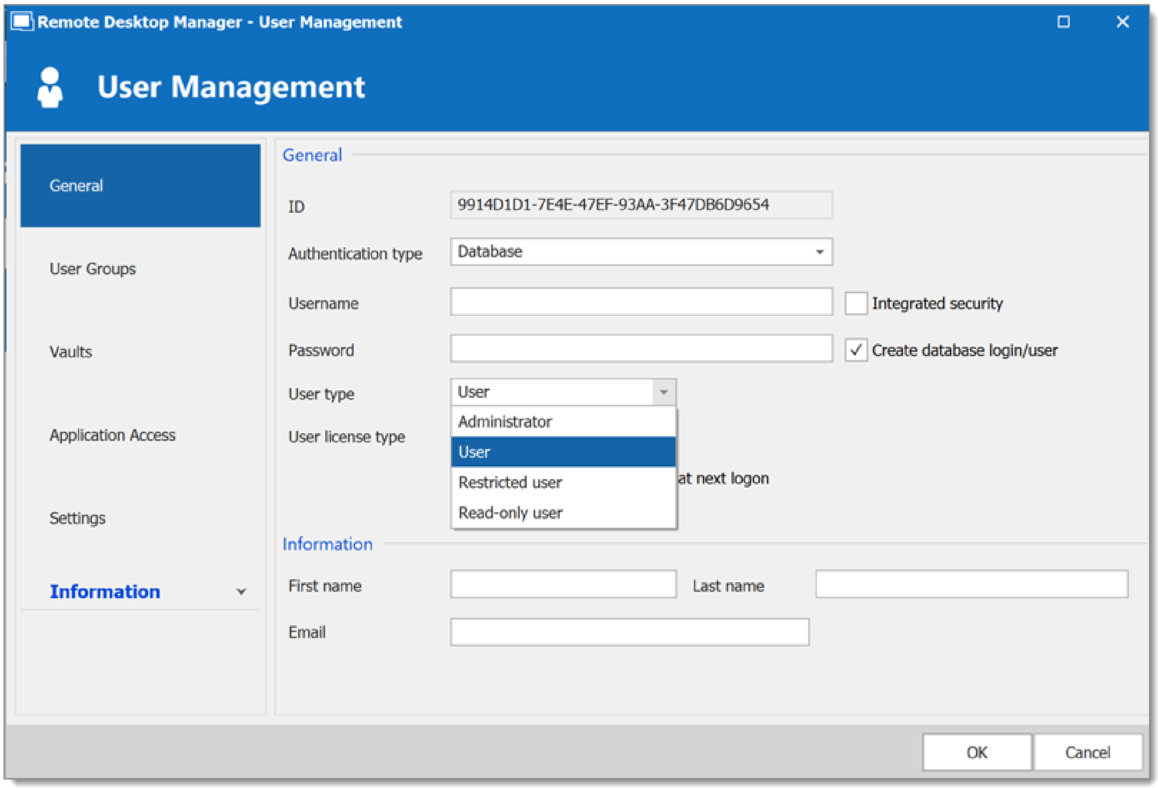
Windjammer tree view structure

USER CONFIGURATIONS

Here is an example for user configurations.

The administrator:

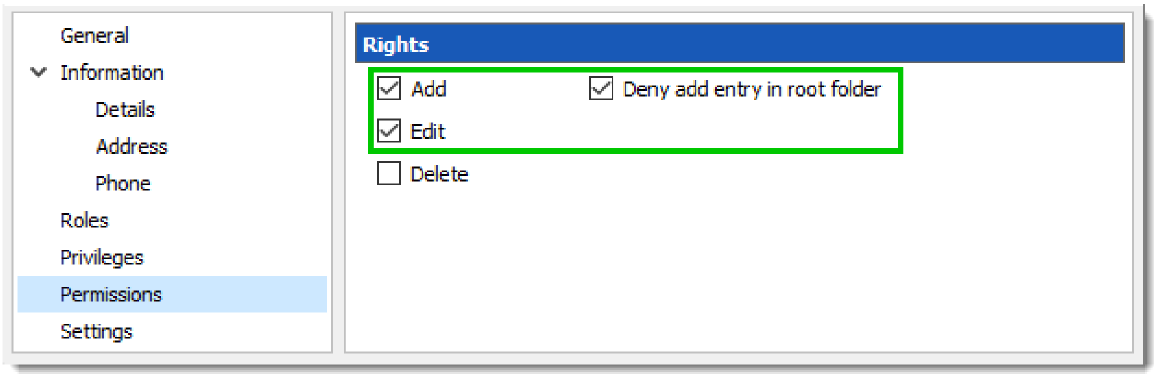
- When creating the user, select the ***Administrator*** in the dropdown menu to give it access to everything.



Administrator Permission

The *ServiceDesk*:

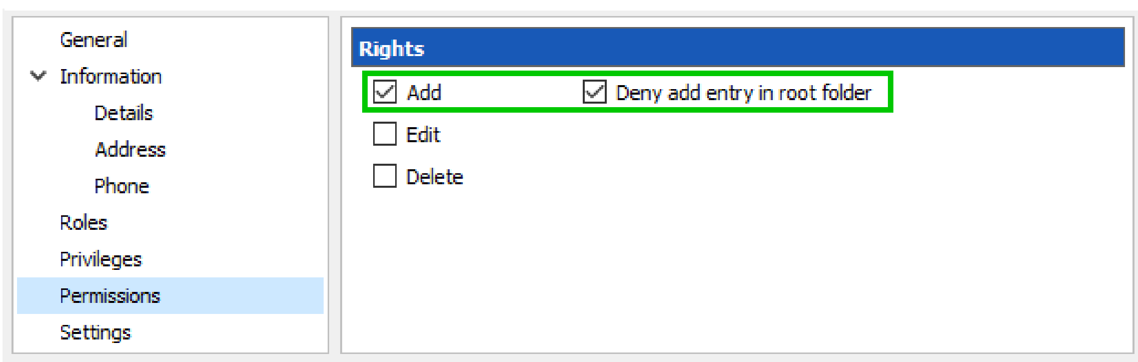
- ***Add***
- ***Edit***
- ***Deny add entry in root folder***



ServiceDesk Rights

The *HelpDesk*:

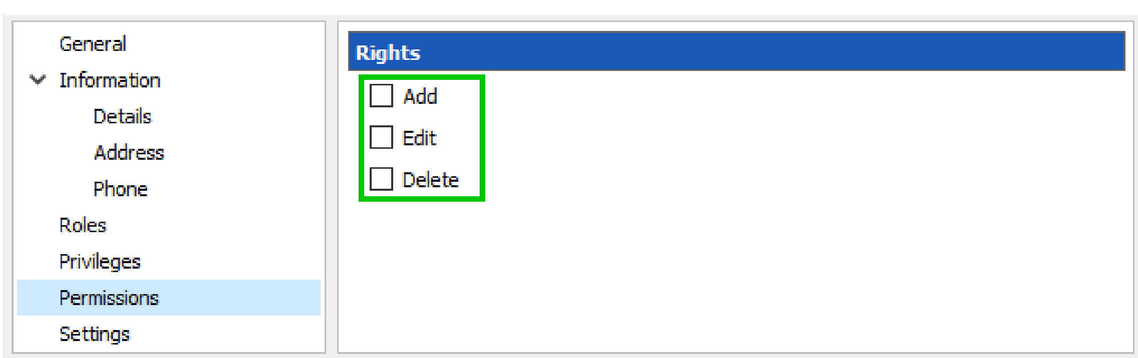
- ***Add***
- ***Deny add entry in root folder***



HelpDesk Rights

The MontrealConsultant has read-only access. He cannot see any password or entry detail.

- Leave everything disable for this user



MontrealConsultant Rights

USER GROUPS CONFIGURATION

Now that the users are created we will add the user groups to which we will later grant the permissions. We just need the user groups to assign users to them. No need to grant them any privileges.

- ServiceDesk
- HelpDesk
- MontrealConsultant

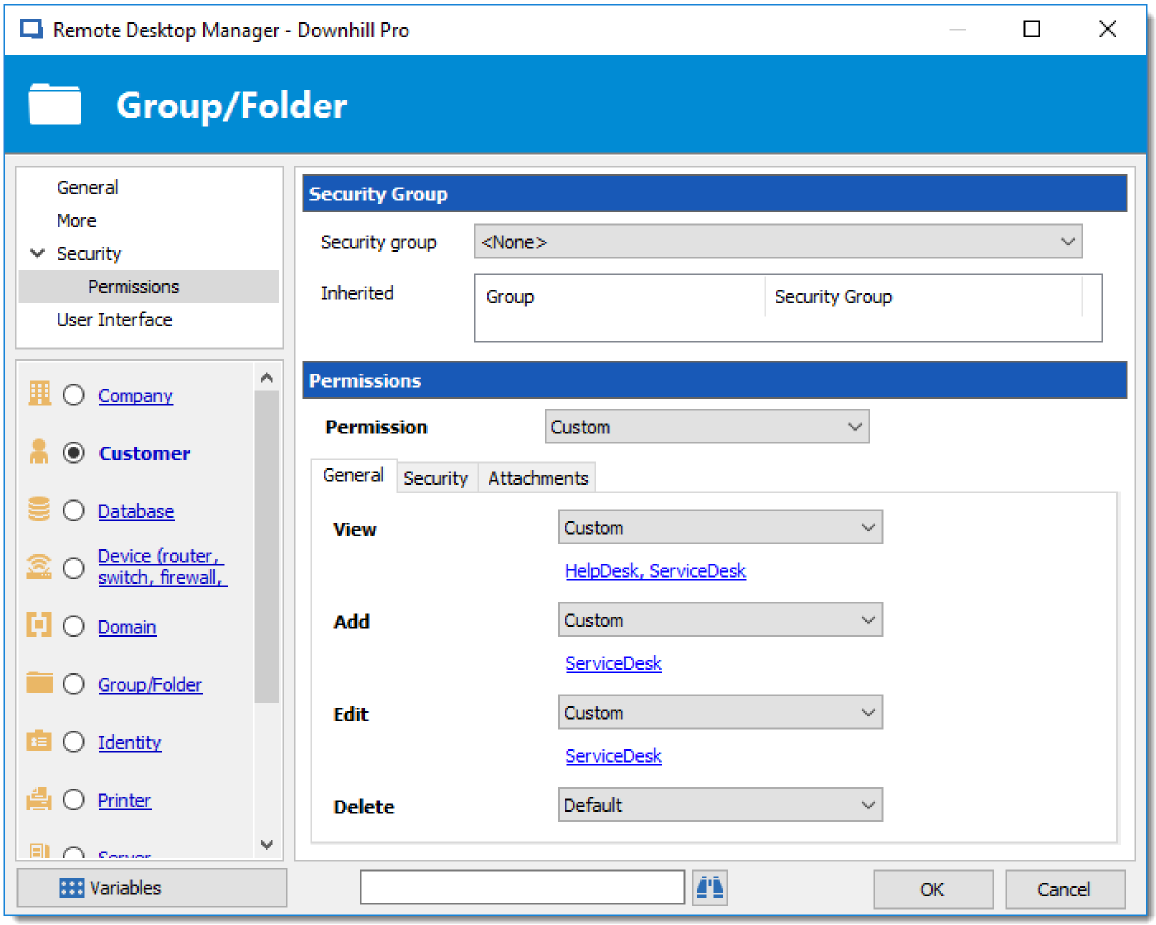
ENTRIES CONFIGURATION

Now everything is ready to grant or deny access to the user groups.

- The ServiceDesk will have the permission to view and open all entries but will be able to edit only the entries in the customer groups/folders.
- The HelpDesk will have the permission to view and open entries on the customer groups/folders only and will not be able to edit them.
- The MontrealConsultant will have the permission to view and open entries on the Montreal goup/folder only and will not be able to edit it nor its child items.

We will begin with the root level groups/folders: Downhill Pro, Telemark and Windjammer.

For Downhill Pro, we will grant permissions to the ServiceDesk and the HelpDesk.

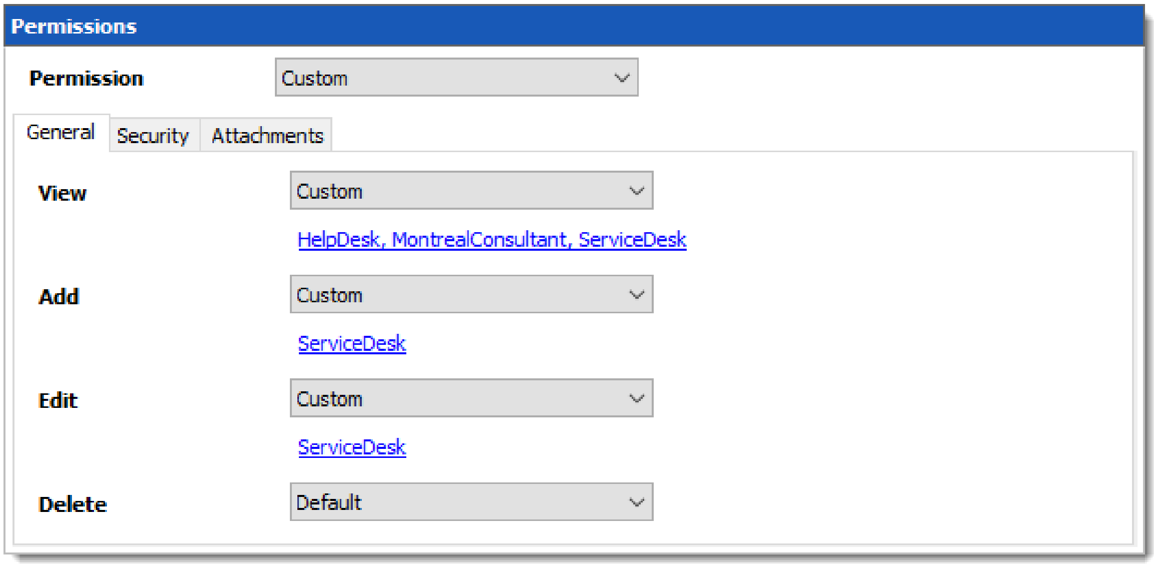


Downhill Pro - Permissions

- ***View***: HelpDesk, ServiceDesk
- ***Add***: ServiceDesk
- ***Edit***: ServiceDesk
- ***Delete***: Since no user have the delete right we can leave this permission to ***Default***.

We already have a good example of the flexibility of Remote Desktop Manager's Security. A ServiceDesk user can view and open all the entries in the Downhill Pro folder, even the credential entry, but it will never be able to see any password.

Next for the Telemark folder, we will grant permissions to the ServiceDesk, the HelpDesk and the MontrealConsultant. This is where things get complex. If we want the MontrealConsultant to be able to view only the Montreal folder which is a child item of Telemark, we must grant to the consultant the permission to view the entire Telemark content. Then we will grant permissions on child items only to the user group that should have access to these items. This last step will deny the view permission for the consultant on the child items.

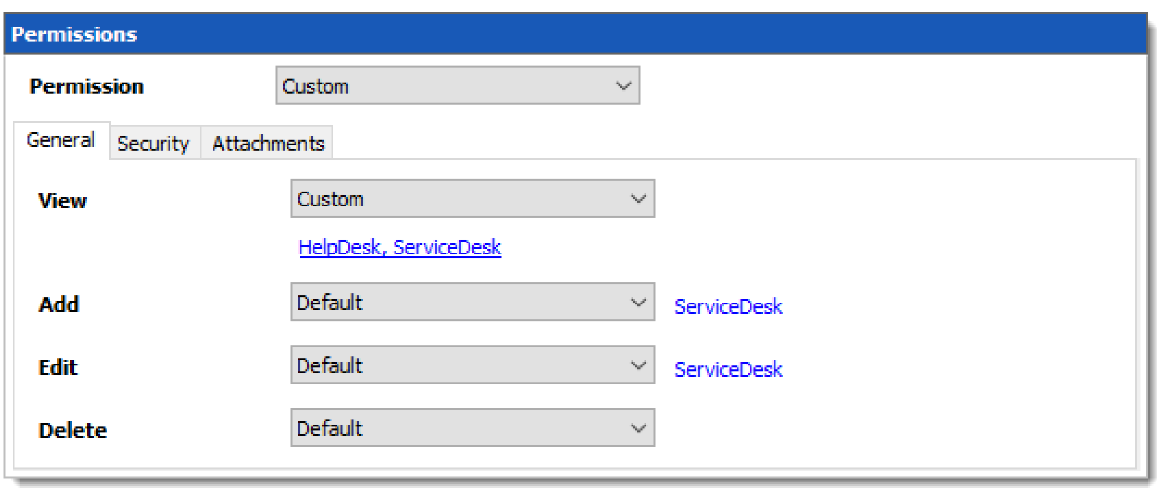


Telemark - Permissions

- ***View***: HelpDesk, MontrealConsultant, ServiceDesk
- ***Add***: ServiceDesk
- ***Edit***: ServiceDesk
- ***Delete***: Default

Since we want the users to be able to use the credential entries, we will grant the ServiceDesk and the HelpDesk the permission to View the Credentials folder. This way they will be able to use the entries without being able to view the passwords.

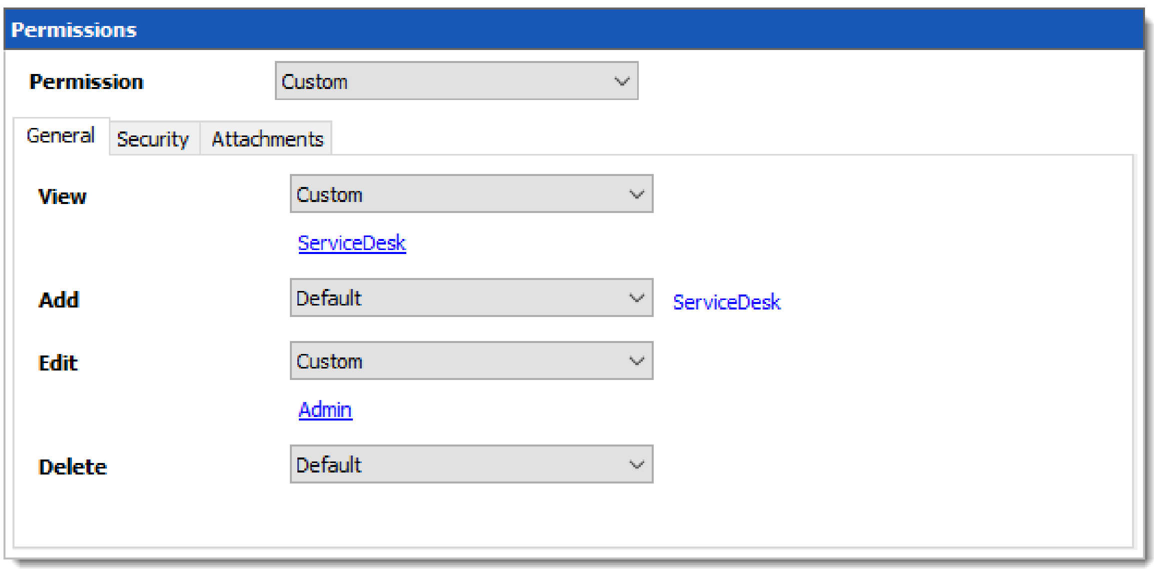
The ***Add*** and ***Edit*** permissions can be left to ***Default*** since the ServiceDesk is the only user group that has been granted these permissions in the parent folder.



Telemark\Credentials - Permissions

* ***View***: HelpDesk, ServiceDesk
* ***Add***: Default
* ***Edit***: Default
* ***Delete***: Default

We want the ServiceDesk to be able to use the Domain Admin credential entry as well but not the HelpDesk. For this we must grant the ***View*** permission to the ServiceDesk only and change the ***Add*** and ***Edit*** permission to ***Never***. The ServiceDesk will still be able to edit the credential entry but will never see the password. If you prefer you can set the ***Edit*** permission to an Administrator user or user group to deny it to the ServiceDesk.

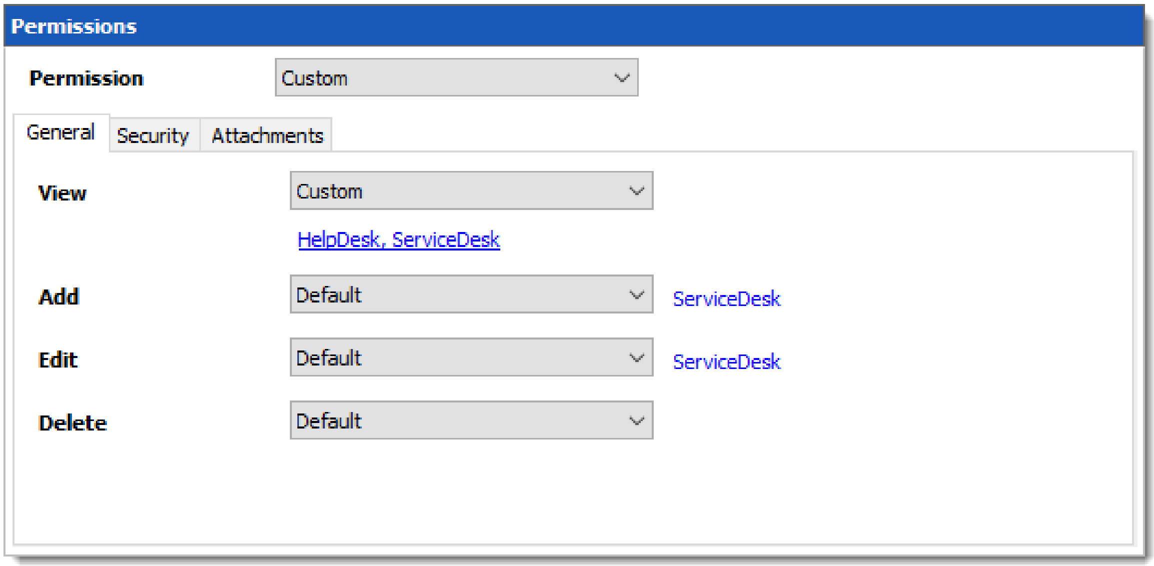


Telemark\Credentials\Admin - Permissions

* ***View***: ServiceDesk
* ***Add***: Default (ServiceDesk)
* ***Edit***: Default or Administrator user/user group
* ***Delete***: Default

The last step for the Telemark child items would be to set the ***View*** permission to the ServiceDesk and the HelpDesk on the Boston folder and leave every other permission to ***Default***.

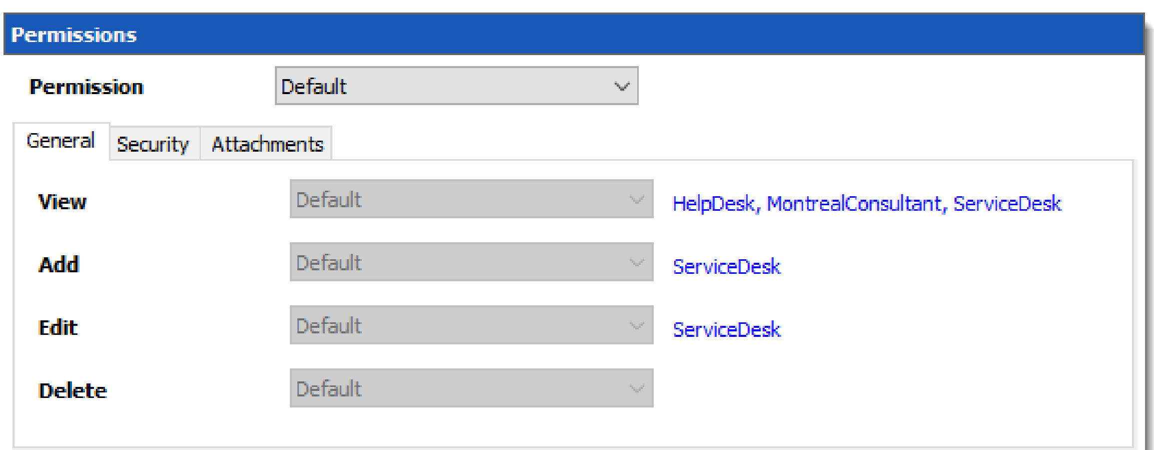
Now the MontrealConsultant will be able to view and open entries only in the Montreal folder. Every time a new folder is added the ***View*** permission must be set for ServiceDesk and HelpDesk to hide the new folder and its content from the consultant.



Telemark\Boston - Permissions

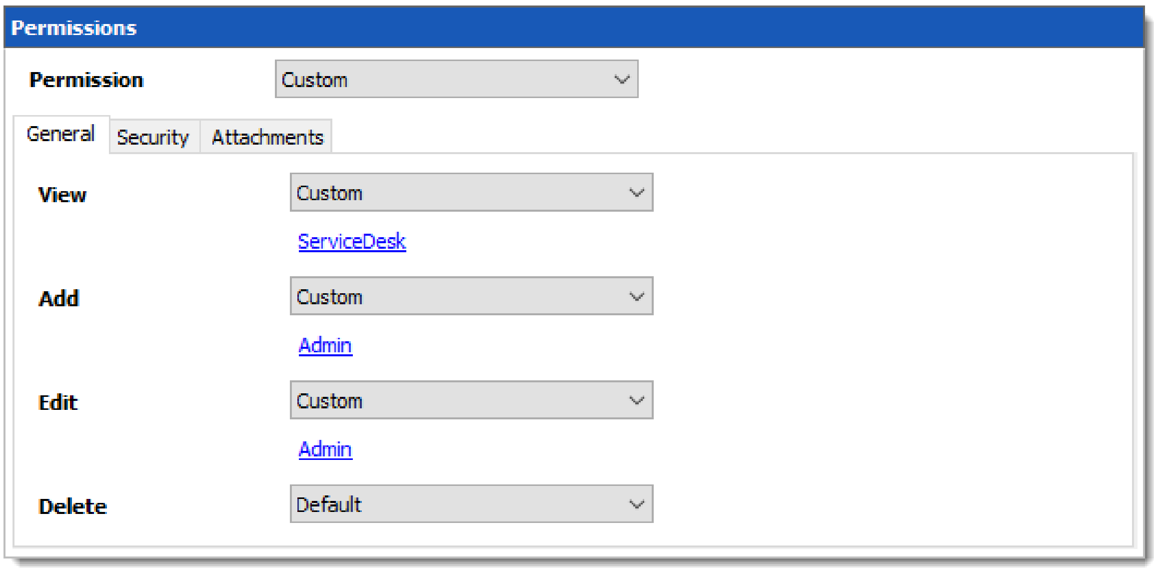
- ***View***: HelpDesk, ServiceDesk
- ***Add***: Default (ServiceDesk)
- ***Edit***: Default (ServiceDesk)
- ***Delete***: Default

No need to set any permissions on the Montreal folder, since they are inherited from the parent folders.



Telemark\Montreal - Permissions

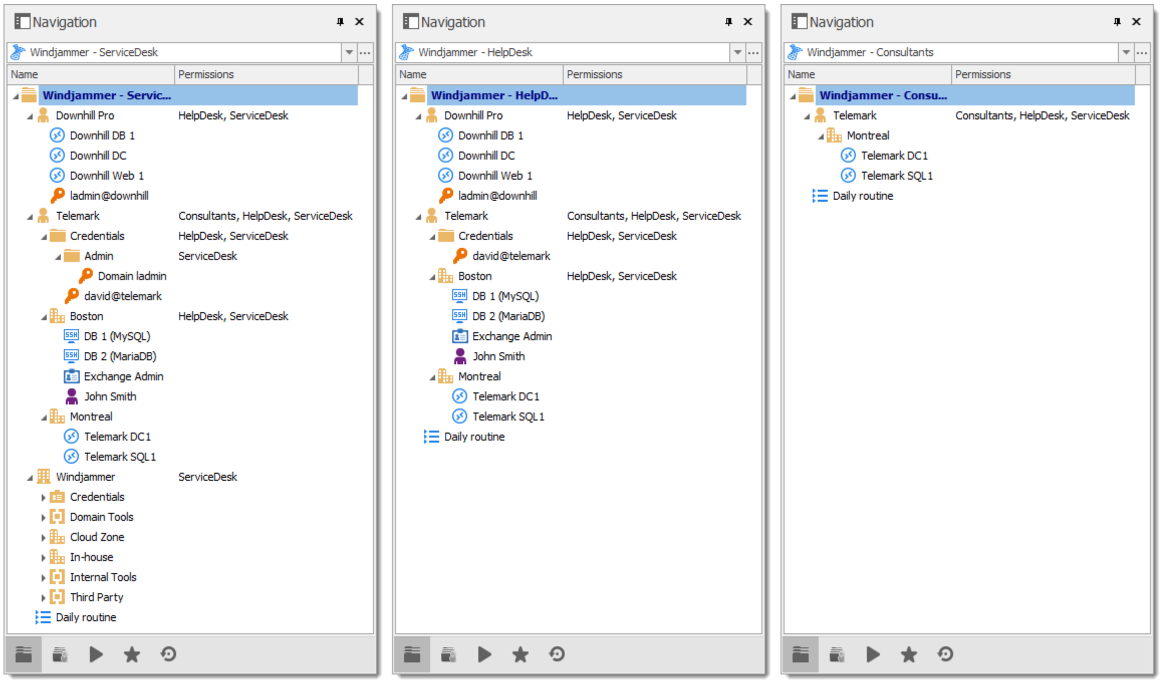
Finally, the permission to view the Windjammer folder will be set for the ServiceDesk only since we want them to be able to use its child entries. We don't want them to add or edit anything so we will set the ***Add*** and ***Edit*** permissions to the Administrator user/user group.



Windjammer - Permissions

IN CONCLUSION

The permissions are now correctly set. Note that every entry added higher than the root level groups/folders will have no security by default. This means they would be available for anyone, even the consultant. This can be confirmed by looking at the screenshot below in which the entry Daily routine is available for everyone. Here is what each user should see in the tree view:



Side by side tree views

You can go further with granting permissions by using the ***Security*** and ***Attachments*** tabs of the permissions section. As always, a great care must be taken when granting permissions and users should have very strict privileges.

PowerShell Scripting

Part

IX

9 PowerShell Scripting

DESCRIPTION

> We have moved to a GitHub repository to hold our various samples and recipes. Please consult the content of our GitHub repository to see what's available. Questions and samples should be requested on our forum and our team will be glad to assist you.

There are two ways to interact with Remote Desktop Manager using PowerShell:

Module	Remote Desktop Manager PowerShell Module: a module that exposes many cmdlets that are used to "pilot" a LOCAL installation of Remote Desktop Manager. As such, its quite different from most of the modules available out there since the great majority is used to communicate with a remote service. This means that it requires an interactive Windows session in a user context.
Custom Actions	Snippets of PowerShell code that can be executed directly in Remote Desktop Manager. The actions can be initiated using ***Edit – Edit (Special Actions), Custom PowerShell Command.*** The advantages of this approach are: 1. No need to handle loading of the appropriate module for the instance of Remote Desktop Manager. 2. No need to handle filtering of entries, most of the times you would perform manual selection directly in your navigation pane, or even better use the advanced search to select entries in one fell swoop.

9.1 Tips and tricks

DESCRIPTION

We are always asked for a full list of property names and sadly it is extremely hard to provide for multiple reasons. The best way is still to look at the xml structure of an entry of the proper type to identify the field names.

REVERSE ENGINEERING AN ENTRY'S STRUCTURE

1. Create an entry of the needed type, add only mandatory data at this time. Save the entry.
2. Right-click on the entry, then use ***Clipboard – Copy***.
3. In the dialog that appears, switch to the **Preview** tab, copy the xml structure to a text file. This is the **BEFORE**.
4. Manually perform the modification to the entry that you would like to automate using PowerShell, save the entry.
5. Using ***Clipboard – Copy***, save the modified xml to another file. This is the **AFTER**.
6. Compare the two files with your favorite difference tool, you will see the fields that have changed, and the values that have been assigned. This indicates what your script should do.

ESSENTIAL INFORMATION ABOUT REMOTE DESKTOP MANAGER'S XML FORMAT

- To save space, most fields have a default value and when the field contains that default value, it simply does NOT appear in the content. That is why you must watch out for new fields that appear in the AFTER content.
- Credentials are handled in a special way. They contain a GUID when they refer to other entries, but they hold Well-Known static GUIDs when they use other mechanisms.

SETTING	WELL KNOWN GUID
Default	""
Credential repository ***--- Prompt on connection ---***	"45479560-173E-435D-8848-C22F863FDC96"
Embedded	should be used for backwards compatibility only, we prefer not to list it here.
Parent (only for sub-connections)	"E2CC9029-CA3A-4308-BA54-16D5029BC8ED"
Inherited	"1310CF82-6FAB-4B7A-9EEA-3E2E451CA2CF"

SETTING	WELL KNOWN GUID
My personal credentials	"9F3C3BCF-068A-4927-B996-CA52154CAE3B"
None	"B87B29D9-9239-4D7B-86D8-9B53DCD3BA9F"
User Vault, paired with *PersonalConnectionID*	"245A4245-48E7-4DF5-9C4C-11861D8E1F81"
User Vault Search, paired with *CredentialPrivateVaultsearchString*	"88E4BE76-4C5B-4694-AA9C-D53B7E0FE0DC"

TIPS AND TRICKS

- To find properties and paths, reverse engineer the session XML file format. Create a sample session in RDM and export it using the right click menu Import/Export - Export Session (.rdm).... Once exported, open the .rdm file with your favorite editor. Browse the XML structure to find the property path and name.
- To list all properties of an entry, pipe the session object to Get-Member cmdlet.

```
$session  = Get-RDMSession -Name "MyRDPSession"
$session | Get-Member
```

- Use the AddDataEntryKind method to set the data entry kind to Web (11 in this case). This is not actually documented – it’s just a bonus tip that we use here at Devolutions all the time!

9.2 PowerShell Module

DESCRIPTION

Starting with Remote Desktop Manager version 2021.2.x, the PowerShell module is available for download on PowerShell Gallery.

Remote Desktop Manager supports Windows PowerShell. PowerShell is a powerful scripting shell that lets administrators automate Remote Desktop Manager. They are provided in a PowerShell module.

MANUALLY INSTALL AND IMPORT THE POWERSHELL MODULE

The Remote Desktop Manager PowerShell Module is now available on PowerShell Gallery and can be downloaded here. It can also be installed and imported like the following commands. Please see this knowledge base article for further instructions about the PowerShell module usage.

```
Install-Module -Name RemoteDesktopManager
Import-Module RemoteDesktopManager
```

COMMANDS

To list all cmdlet commands, please enter this command:

```
Get-Command -Module RemoteDesktopManager
```

For more information on those commands, use the following command:

```
get-help [command name]
```

Here's how to generate a text file with all the commands:

```
Get-Command -Module RemoteDesktopManager -Type Cmdlet `
  | Sort-Object -Property Name `
  | Format-Table -Property Name `
  | out-file $env:temp\pshelp.txt
```

```
Get-Command -Module RemoteDesktopManager `
  | ForEach-Object { get-help -name $_.Name -full } `
  | out-file -append $env:temp\pshelp.txt
```

9.2.1 Extract TeamViewer ID

DESCRIPTION

You can use Powershell to extract the TeamViewer ID from a session.

SETTINGS

Here a script to extract the TeamViewer ID from a session:

$sessions = Get-RDM-Session | where {$_.Session.Kind -eq "TeamViewer"}

$sessions[0].Session.GetProperty("TeamViewer", "ID")

9.2.2 Custom Export to CSV

DESCRIPTION

Many customers ask for a special export that would contain specific fields.

SETTINGS

Here is a small script that can be used to generate URLs for our new web protocol handler. We generate a csv file that contains the name and the URL.

```
## get the data source ID, note that the "Create Web Url" button generates a different
$dsid = Get-RDM-DataSource | where {$_.IsCurrent -eq "X"} | select -expand "ID"
## get the RDP sessions, create a new object with the desired fields.
## Simply append "add-member" commands to include a new field
$s = Get-RDM-Session |
 where {$_.Session.Kind -eq "RDPConfigured"} |
 foreach {
  new-Object Object |
      Add-Member NoteProperty Name $_.Name –PassThru |
      Add-Member NoteProperty URL "rdm://open?DataSource=$dsid&Session=$($_.ID)" –Pas
 };
```

```
## save to csv, the field names are used as column headers.
$s | export-csv c:\temp\sessions.csv -notypeinformation;
```

9.2.3 Creating Group Folder Structure from CSV file

DESCRIPTION

Please note that the CSV file must be encoded in UTF-8 to support special characters.

This sample creates a Group Folder structure from a CSV file.

SAMPLE

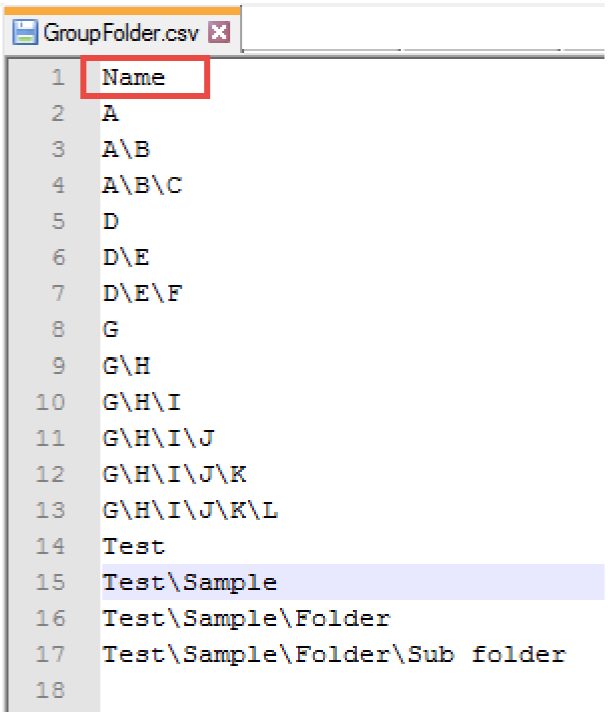
```
$csv = Import-Csv "c:\YourFolder\GroupFolder.csv"

foreach ($csvEntry in $csv) {
    $groupName = $csvEntry.Name

      # Extract the group folder name
      if ($groupName.Contains("\")) {
      $groupName = $groupName.Substring($groupName.LastIndexOf("\"), $groupName.Lengt
      $groupName = $groupName.TrimStart("\")
            }

      # Create the group folder if it is not null, empty or fill in with space charac
      if (![string]::IsNullOrWhiteSpace($groupName)) {
          $session = New-RDMSession -Type "Group" -Name $groupName
          $session.Group = $csvEntry.Name
          Set-RDMSession $session
          Write-Host "Group Folder $groupName created" -f Yellow
      }
}

Update-RDMUI
```

NOTES

The CSV file must have only one column with the title set as Name.

The full path must be specified for each sub folder.

Here is an example of this CSV file :




```
Name
A
A\B
A\B\C
D
D\E
D\E\F
G
G\H
G\H\I
G\H\I\J
G\H\I\J\K
G\H\I\J\K\L
Test
Test\Sample
Test\Sample\Folder
Test\Sample\Folder\Sub folder
```

CSV File example

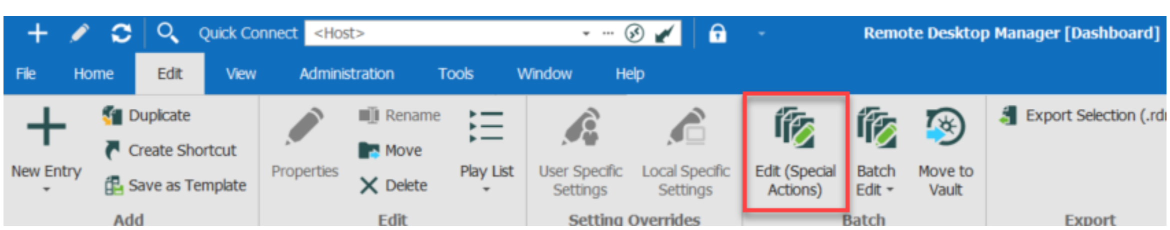
CMDLETS REFERENCE

9.3 Custom PowerShell Commands

DESCRIPTION

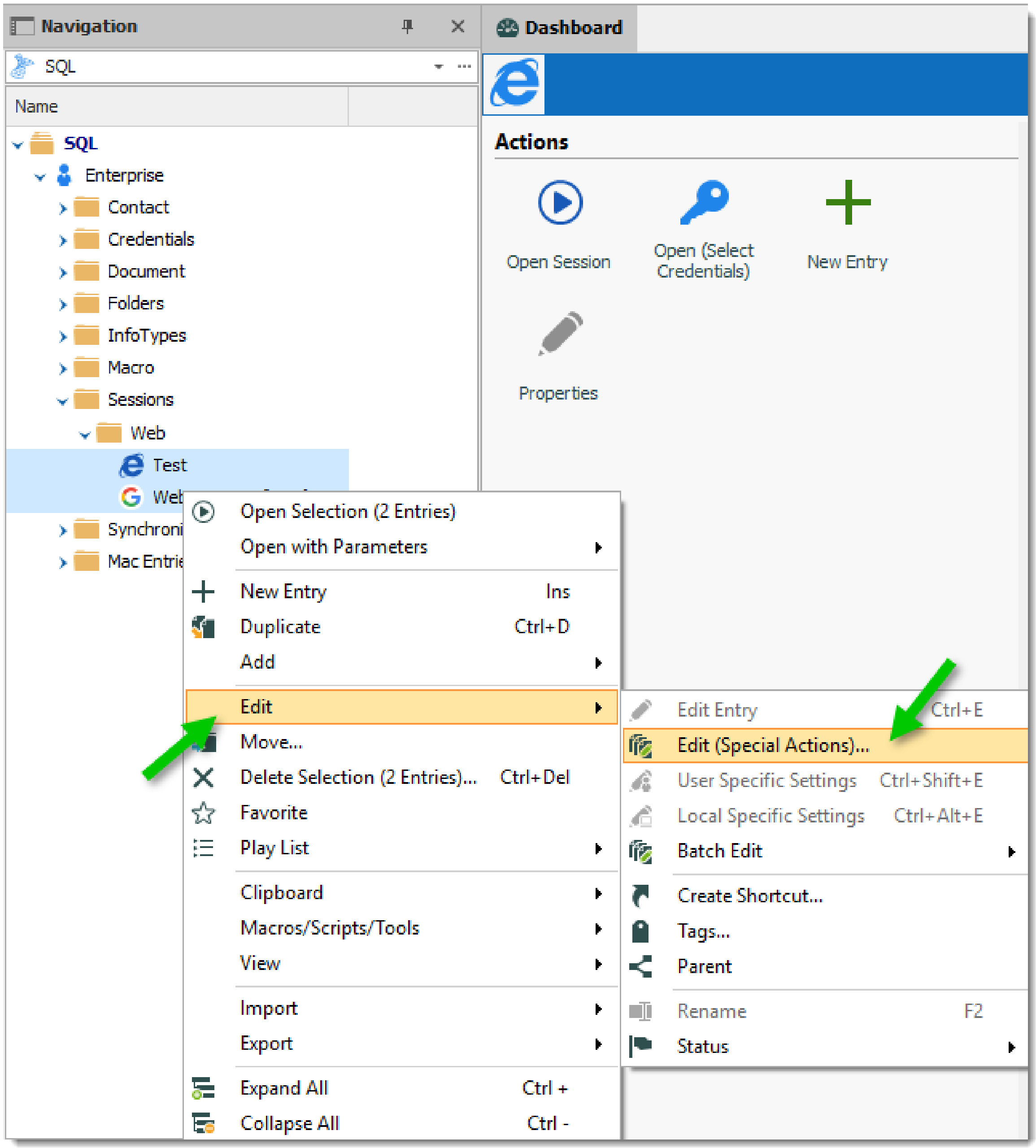
Custom Powershell Command will act on currently selected entries in your navigation panel. Use click & ctrl-click to build up your list, or an advanced search to select a great number of entries. After your selection is done, the command is available using either :

- ***Edit - Batch - Edit (Special Actions)***.



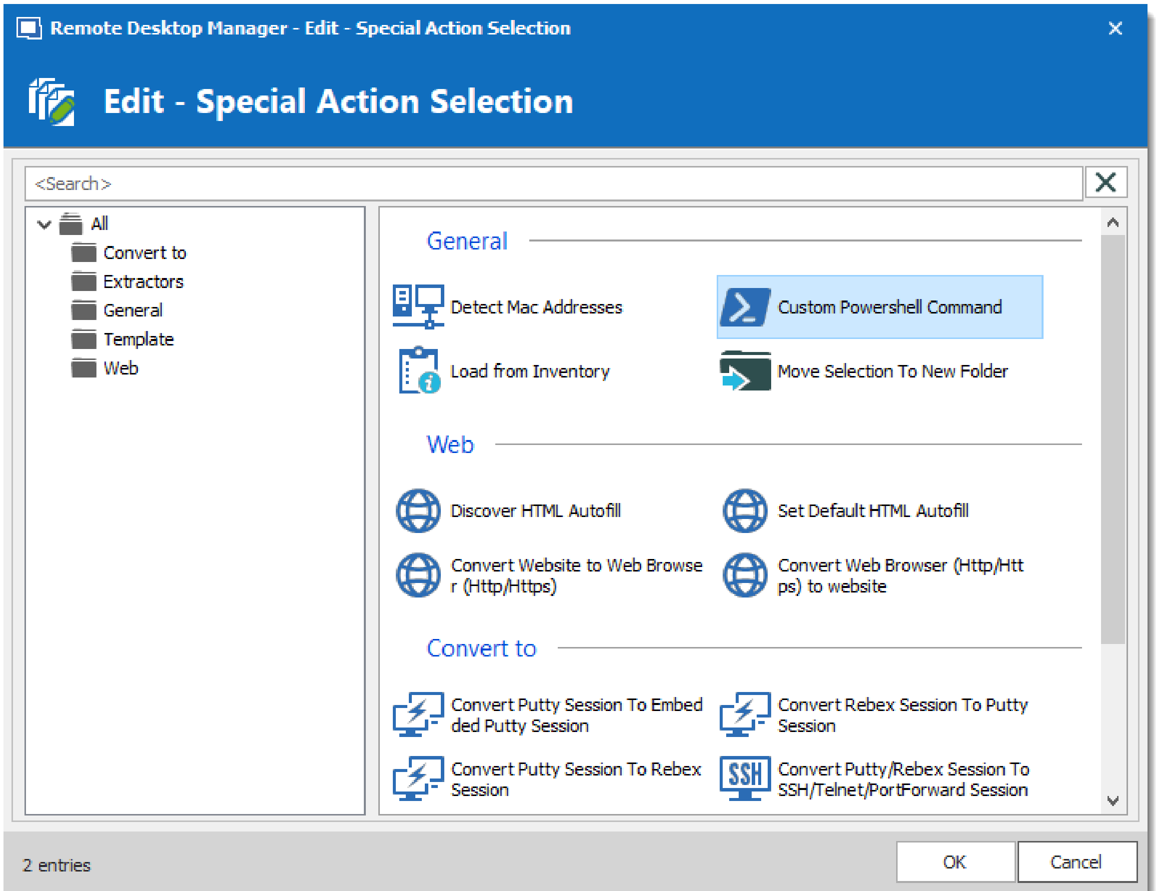
Edit Toolbar

- Right-click then ***Edit – Edit (Special Actions)***.



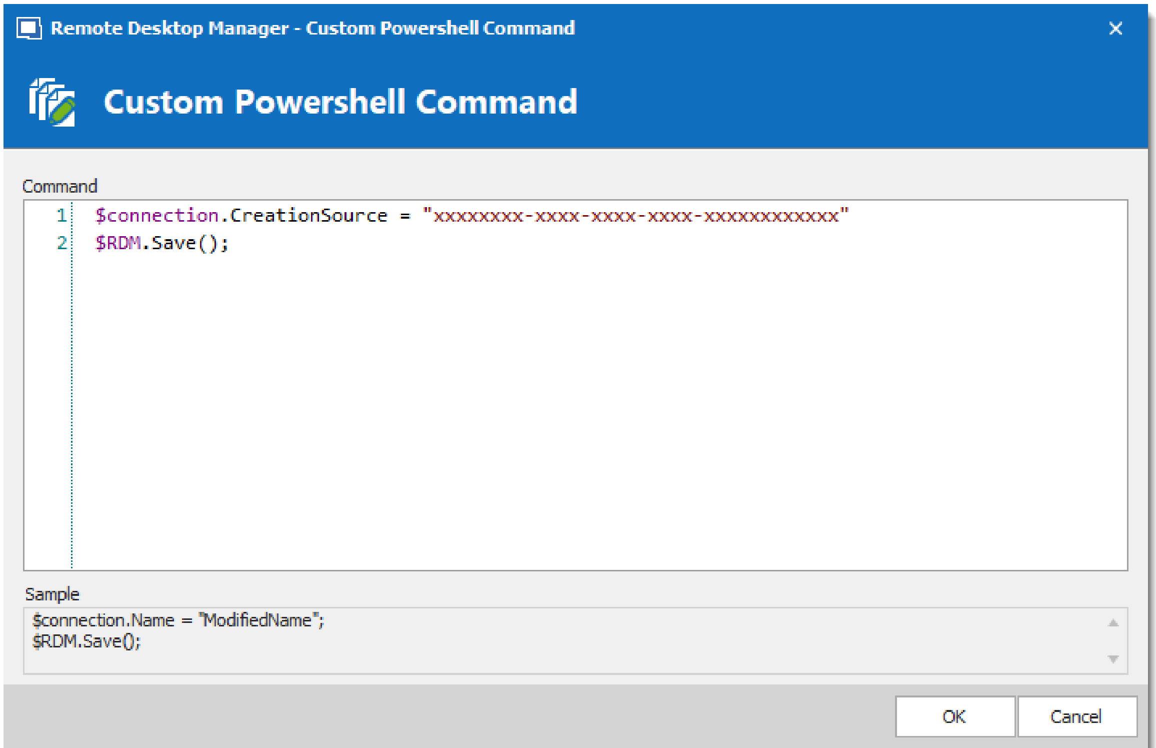
Selected entries - Edit (Special Actions)

- Once there, Select ***Custom PowerShell Command***.



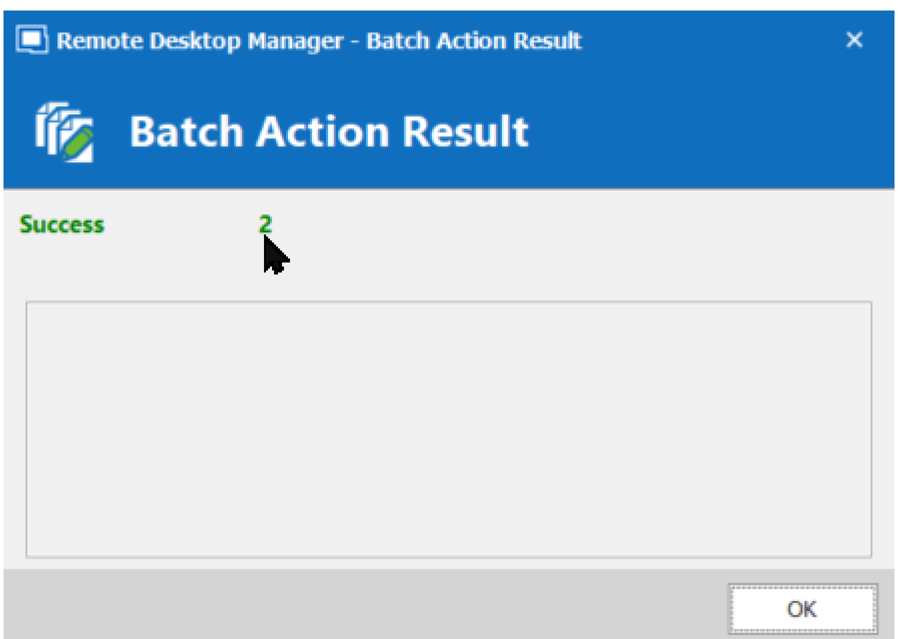
Edit (Special Actions)

- A window appears in which you can write a snippet of code. Note that is the last line must always be ***$RDM.Save();***

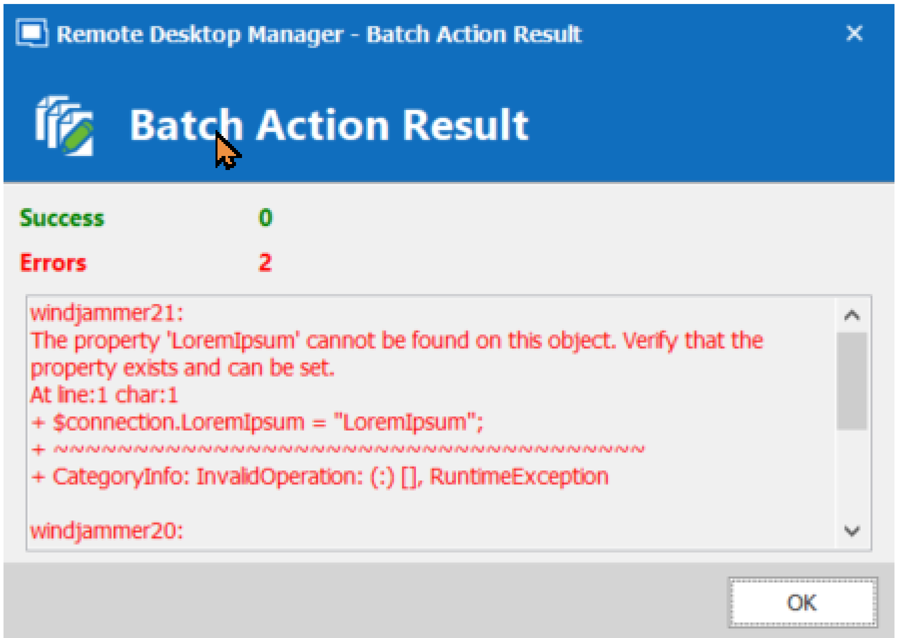


Custom Powershell Command

- Upon pressing Ok, a summary dialog appears to indicate success or failure.



Batch Action Result - Success



Batch Action Result - Failure

9.3.1 Change your Synchronizer source

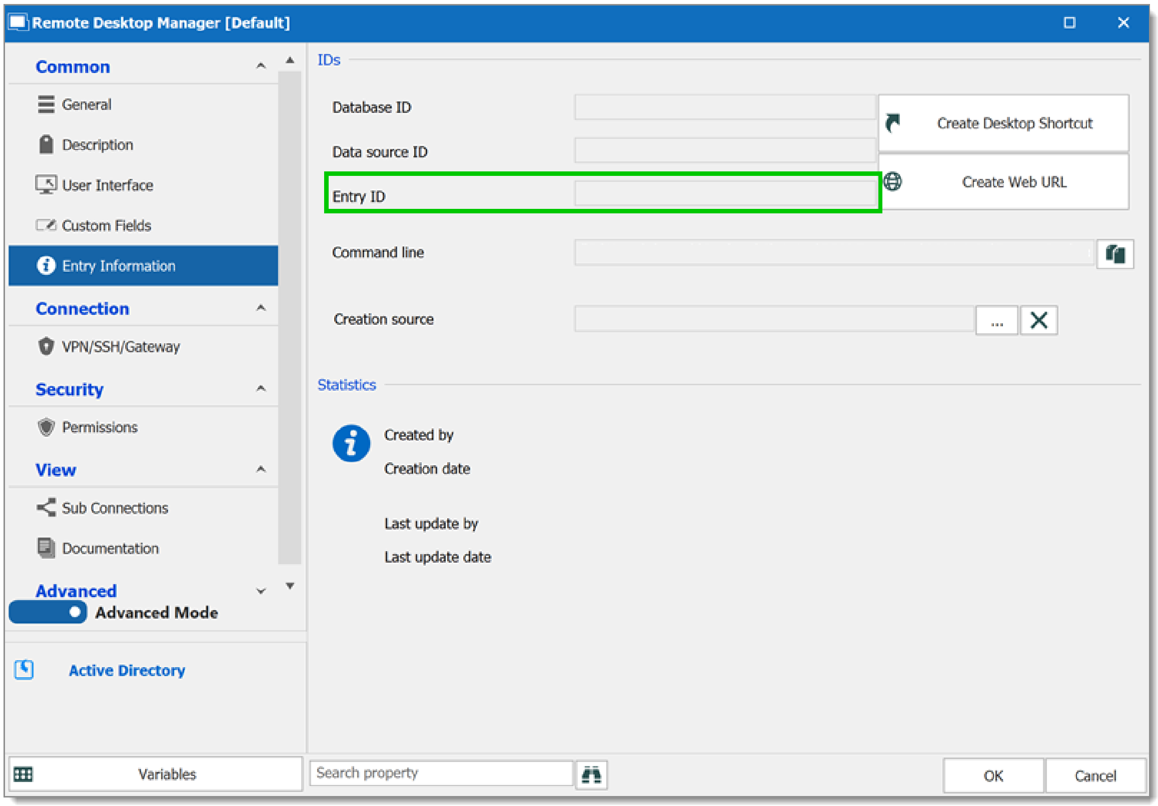
DESCRIPTION

If you have been using the Remote Desktop Manager version with the Synchronizer **Action on Entry Mismatch** feature, the following steps will allow you to easily change your source with a Powershell Command without having to recreate all your sessions, thus marking all selected entries as created by the synchronizer.

SETTINGS

1. Select your Synchronizer entry in your Tree view, right click and select **Properties**.

2. Copy the ***Entry ID*** in the ***Entry Information*** menu (you will then need that ID number to insert in your Powershell Command).

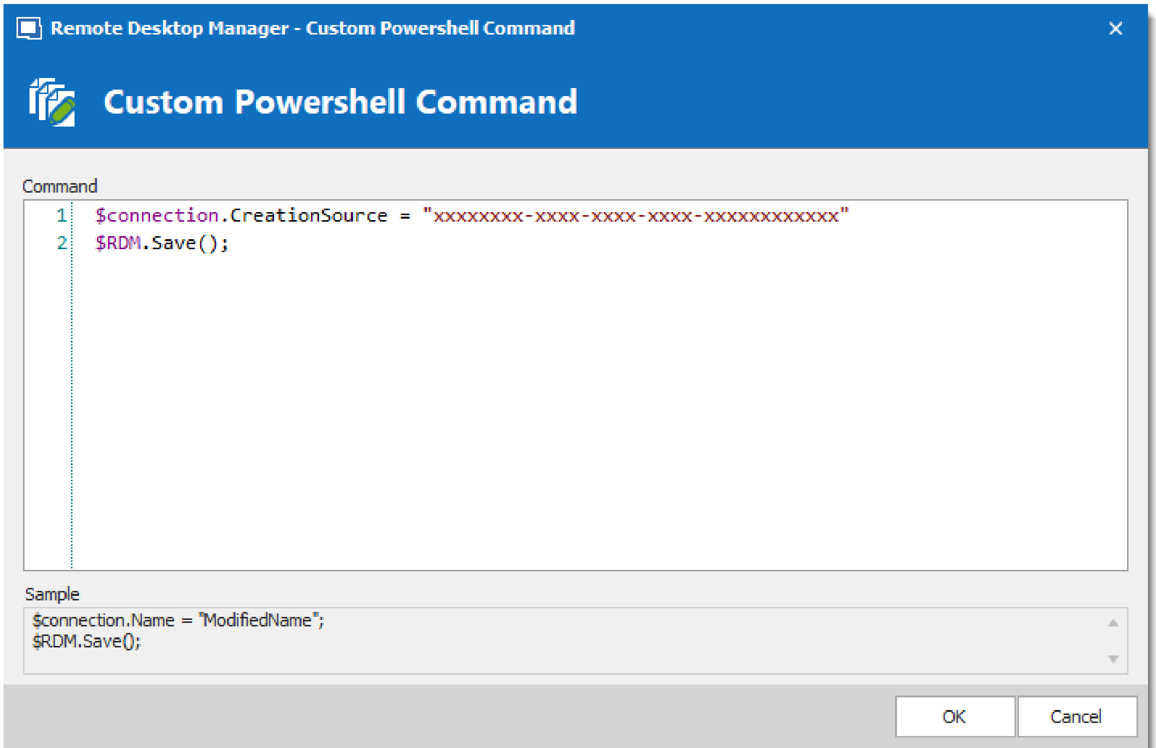


Advanced - Session ID

3. Select your entries and reach the Custom PowerShell Command dialog as described in [Custom PowerShell Commands]()

4. Write the following line for your Powershell Command:

```
$connection.CreationSource = "***** synchronizer ID obtained in step 2 *****"
$RDM.Save();
```



Custom Powershell Command

9.3.2 Batch Actions Samples

DESCRIPTION

The Batch Actions allow for a quick way to modify multiple sessions at once, but within Remote Desktop Manager itself.

To be able to create your PowerShell script, you would need the name of the field(s) that you would like to update. To retrieve the exact name of the field, right-click on your session and select ***Clipboard – Copy***. You can then paste the information in a text editor to retrieve the name of the field(s) that you would like to modify via the Custom PowerShell Command.

Since they use the Powershell technology, we provides samples in this section because the fields are the same when accessed through our Batch Actions or through Powershell.

SAMPLES

DISABLE ONLY SEND PASSWORD IN HTML PASSWORD FIELD OPTION IN WEB BROWSER SESSIONS

```
$connection.Web.OnlySendPasswordInPasswordField = $false;
$RDM.Save ( ) ;
```

ENABLE VIEW URL EMBEDDED (INFORMATION ENTRIES)

```
$connection.DataEntry.ViewUrlDisplayMode = "Default";
$RDM.Save();
```

ViewUrlDisplayMode: "Default" = embedded, "External" = external.

OPEN URL (EXTERNAL) FOR WEB LOGIN (INFORMATION ENTRIES)

```
$connection.DataEntry.DefaultAction = "OpenUrlExternal";
$RDM.Save();
```

SSH SHELL BATCH EDIT (SESSION TYPE SETTINGS)

```
$connection.Terminal.MaxScrollbackLines = 2000;

$connection.Terminal.AlwaysAcceptFingerprint = $true;

$connection.Terminal.EnableLogging = $true;
$connection.Terminal.LogPath = '$LOGPATH$\$NAME$_$DATE_TEXT_ISO$_$TIME_TEXT_ISO$.
$connection.Terminal.LogMode = 1;
$connection.Terminal.LogOverwriteMode = 0;
$RDM.Save();
```

Here are some values that you can change for this command;

LogPath: your path between ' ' (single quotes). You can also use variables. i.e. %USERPROFILE%, $NAME$, etc. In this example $LOGPATH$ is a custom variable defined in the Data Source Settings (System Settings) - Custom Variables
LogMode: 1 = Printable Output, 0 = Event
TerminalLogOverwriteMode: 0 = default, 1 = prompt, 2 = append, 3 = overwrite
Here's also other options that you can modify;

$connection.Terminal.BellMode = 'Visual'
$connection.Terminal.CloseOnDisconnect = $false

CONVERT WEB BROWSER SESSIONS INTO LOGMEIN SESSIONS

```
$connection.ConnectionType = 'LogMeIn';
$connection.ConnectionSubType = '' ;
$connection.LogMeIn.Url = $connection.WebBrowserUrl;
$RDM.Save();
```

Enable the "Hide script errors in all your LogMeIn sessions."

```
$connection.LogMeIn.ScriptErrorsSuppressed = $true;
$RDM.Save();
```

Hide navigation bar.

```
$connection.LogMeIn.ShowUrl = $false;
$RDM.Save();
```

Change the Web Browser Application.

```
$connection.LogMeIn.WebBrowserApplication = "GoogleChrome";
$RDM.Save();
```

Enable the Sandbox Process.

```
$connection.LogMeIn.SandboxProcess = $true;
$RDM.Save();
```

Change the URL.

```
$connection.LogMeIn.Url = " ";
$RDM.Save();
```

Change the Portal Login field.

```
$connection.LogMeIn.DashboardHostUrl = " ";
$RDM.Save();
```

Change Username & Password.

Please run these two one at a time

Host;

```
$connection.LogMeIn.UserName = " ";
$RDM.Save();
$connection.LogMeIn.SafePassword = " ";
$RDM.Save();
```

Portal;

```
$connection.LogMeIn. DashboardEmail = " ";
$RDM.Save();
$connection.LogMeIn. SafePasswordDashboard = " ";
$RDM.Save();
```

CHANGE A CUSTOM FIELD VALUE WITHOUT CHANGING THE DATA

```
$connection.MetaInformation.CustomField3Title = "MyField"
$RDM.Save();
```

Please note that you would need to change "MyField" for the value that you want to replace Custom field #3 with.

BULK UPDATE FQDN INFO TO SESSIONS.

```
$connection.host = $Connection.name + ".mydomain.com"
$RDM.Save();
```

BULK CHANGE RECORDING FIELD FOR PUTTY SESSIONS

```
$connection.Putty.RecordingMode = 1;
$connection.Putty.RecordingFileName = "C:\path\to\your\file.log"
$RDM.Save();
```

CHANGE THE COMPUTER FIELD OF AN RDP SESSION

```
$connection.Url = " ";
$RDM.Save();
```

ENCODING

```
$connection.Putty.TelnetEncoding = "UTF-8";
$RDM.Save();
```

CHANGE THE EXPIRATION DATE OF AN RDP SESSION

The date must be specified using the ISO8601 format.

```
$connection.MetaInformation.Expiration = "2018-12-25T00:00:00-05:00";
$RDM.Save();
```

CHANGE THE EXPIRATION DATE OF AN RDP SESSION WITH A RELATIVE DATE

Use any date time operator supported by PowerShell.

```
$connection.MetaInformation.Expiration = (Get-Date).AddMonths(6);
$RDM.Save();
```

MODIFY PAGE TAB TITLE IN UI

```
$connection.TabTitle = '$COMPANY_NAME$ - $NAME$';
$RDM.Save();
```

CLEAR KEYWORDS IN SESSION

```
$connection.MetaInformation.Keywords = "";
$RDM.Save();
```

CHANGE HISTORY MAX LINES FOR SSH SHELL (REBEX)

```
$connection.Putty.HistoryMaxLength = 2000;
$RDM.Save();
```

CONVERT COMMAND LINE TOOL TO A COMMAND LINE SESSION

```
$connection.ConnectionType = 3;
$RDM.Save();
```

CHANGE KEYBOARD HOOK FOR AN RDP SESSION

```
$connection.KeyboardHook = "OnTheRemoteComputer";
$RDM.Save();
```

Support/Resources

Part X

10 Support/Resources

10.1 Technical Support

DESCRIPTION

Hours:	Monday to Friday 7:30 a.m. to 6:00 p.m. EST
Knowledge Base:	Find helpful information and procedures regarding our products.
Email:	service@devolutions.net
Forum:	https://forum.devolutions.net/
Language:	English-Français-Deutsch
Phone:	+1 844 463.0419

EXTENDED AND PREMIUM SUPPORT PLANS

Subscribers of a paid support plan have received a plan ID. You should send your plan ID in your tickets.

Please consult our Support Policy for more information.

10.2 Keyboard Shortcuts

DESCRIPTION

Here are the default keyboard shortcuts for various commands. These can be modified in ***File – Options – User Interface – Keyboard***.

ACTIONS

ACTION	SHORTCUT
Clipboard - Copy Connection String	Ctrl+Alt+H
Clipboard - Copy Domain	Ctrl+Alt+B
Clipboard - Copy Host	Ctrl+H
Clipboard - Copy Password	Ctrl+Shift+B
Clipboard - Copy Url	Ctrl+Shift+H
Clipboard - Copy Username	Ctrl+B
Execute Typing Macro	Ctrl+Shift+A
Navigate URL	Enter
Open (Embedded/Tabbed)	Ctrl+Enter

ACTION	SHORTCUT
Open (External)	Shift+Enter
Open Full screen	Alt+Enter
View Password	Ctrl+P

EDIT

ACTION	SHORTCUT
Add Credential Entry	Alt+Shift+N
Add Folder	Ctrl+Shift+N
Add Information	Ctrl+Alt+N
Add Session	Ctrl+N
Delete...	Ctrl+Del
Duplicate	Ctrl+D
Edit Entry	Ctrl+E
Local Specific Settings	Ctrl+Alt+E
New Entry	Ins
Rename	F2

ACTION	SHORTCUT
User Specific Settings	Ctrl+Shift+E

GENERAL

ACTION	SHORTCUT
Filter...	Ctrl+F
Force Refresh	Ctrl+F5
Online Help	F1
Quick Connect	Ctrl+Alt+Q
Quick Search...	Ctrl+Space
Refresh	F5

IMPORT/EXPORT

ACTION	SHORTCUT
Import (.rdm)...	Ctrl+Shift+I

NAVIGATION

ACTION	SHORTCUT
Change Data Source	Ctrl+Shift+D
File	Ctrl+Shift+F
Focus Dashboard	Ctrl+Shift+L
Focus Tab	Ctrl+Shift+Up
Focus Tree/List	Ctrl+L
Goto Bookmark 1	Ctrl+1
Goto Bookmark 2	Ctrl+2
Goto Bookmark 3	Ctrl+3
Goto Bookmark 4	Ctrl+4
Goto Bookmark 5	Ctrl+5
Goto Bookmark 6	Ctrl+6
Goto Bookmark 7	Ctrl+7
Goto Bookmark 8	Ctrl+8
Goto Bookmark 9	Ctrl+9
Select Next Tab	Ctrl+Shift+Right
Select Previous Tab	Ctrl+Shift+Left

ACTION	SHORTCUT
Set Bookmark 1	Ctrl+Shift+1
Set Bookmark 2	Ctrl+Shift+2
Set Bookmark 3	Ctrl+Shift+3
Set Bookmark 4	Ctrl+Shift+4
Set Bookmark 5	Ctrl+Shift+5
Set Bookmark 6	Ctrl+Shift+6
Set Bookmark 7	Ctrl+Shift+7
Set Bookmark 8	Ctrl+Shift+8
Set Bookmark 9	Ctrl+Shift+9
Switch Vault	Ctrl+Shift+R

VIEW

ACTION	SHORTCUT
Advanced Search...	F11
Dashboard	Alt+F6
Favorites	F9

ACTION	SHORTCUT
Grouped Tab Pane	Ctrl+Alt+F9
Header Pane	Alt+Shift+F6
Multi Vault Search...	F12
My User Vault	F7
Navigation Pane	Alt+F8
Opened Sessions	F8
Play List Management...	Ctrl+G
RDP Toggle View Only	Shift+F3
Recent	F10
Status Bar	Alt+F7
Tabbed Entries Pane	Alt+F9
Top Pane (Ribbon/Menubar)	Alt+F11
Vault	F6

10.3 Lexicon

DESCRIPTION

Remote Desktop Manager is a software that has an extensive set of functionalities. Here are the major concepts that are important to understand in order to use the program to its full potential.

CONNECTION

Any type of entry that allows you to connect to a remote host, service or device is a connection. An IP address or host name is normally used as well as credentials.

CREDENTIAL ENTRY

A credential is used to control access to a resource by identifying the user. It can be a classic username/password pair held by the application or even by an external source.

DATA SOURCE

It is a container for entries. It can be a local file or a database (either local or shared). You can use multiple distinct data sources in the application, although only one is considered active at one point in time. See Data Sources for more information.

ENTRY

All items in your data source are entries. There are multiple types. The entry is an abstract concept that serves as a container for all specific types.

INFORMATION ENTRY

An information entry can contain various items like account information, emails and serial numbers. Unlike credential entries, information entries are meant to be shared. Therefore, the data in the information entries is not encrypted. Its principal use in Remote Desktop Manager is to hold web site information, from the URL to the credentials. This allows auto log in on the specified web site.

SESSION

In the early days of Remote Desktop Manager, it was mainly aimed at managing Microsoft Remote Desktop. A session was a term that was in use back then to describe a connection to Microsoft Remote Desktop Services. It appears widely in our documentation. Any technology that connects and that needs to use authentication is a session.

10.4 Tutorials

DESCRIPTION

Our tutorials are published on the Devolutions YouTube channel.

Our focus is to deliver quality information as soon as possible after the release of a new or modified feature.

Please use our forums if documentation is missing or plain wrong, we will do our best to correct the situation.

Devolutions

Contact Us

For any questions, feel free to contact us:

Support: service@devolutions.net

Phone: +1 844 463.0419

Monday to Friday 7:30 a.m. to 6 p.m. EST

Head Office

Devolutions inc.

1000 Notre-Dame

Lavaltrie, QC J5T 1M1

Canada

WHERE IT MEETS SECURITY