



Remote Connections & Passwords.  
Everywhere!

# User Manual

2021.1



# Table of Contents

<b>Part I Overview</b>	<b>8</b>
1 Remote Desktop Manager.....	9
2 Security .....	10
3 System Requirements.....	12
Prerequisite Software .....	13
4 The Devolutions Platform.....	14
Remote Desktop Manager Agent .....	15
Remote Desktop Manager Jump .....	17
<b>Part II Getting Started</b>	<b>21</b>
1 Using Remote Desktop Manager.....	22
2 Checklist for Individuals.....	22
Select the Data Source type - Individuals .....	24
3 Checklist for Teams.....	26
Select the Data Source type - Teams .....	28
Set up a team folder for default settings .....	30
4 Creating an Entry.....	32
5 Managing Credentials.....	34
<b>Part III Installation</b>	<b>36</b>
1 Client .....	37
Ancillary Files .....	38
Configuration File Location .....	40
Custom Installer Service .....	42
Installer File Generator.....	44
Option Selection Dialog.....	46
Custom Installer Manager.....	50
For All Users .....	59
Portable (USB) .....	60
Registration .....	64
Enterprise Edition.....	65
End of License.....	67
Free Edition.....	68
Register from Devolutions Portal.....	72
Trial Request.....	75
Remote Desktop Services .....	76
2 Database Upgrade.....	80
3 Uninstall .....	81
4 Update .....	82
<b>Part IV User Interface</b>	<b>84</b>

<b>1</b>	<b>Main Screen .....</b>	<b>85</b>
<b>2</b>	<b>Style .....</b>	<b>86</b>
<b>3</b>	<b>Theme .....</b>	<b>90</b>
<b>4</b>	<b>Top Pane .....</b>	<b>91</b>
	Quick Access Toolbar .....	92
<b>5</b>	<b>Navigation Pane.....</b>	<b>94</b>
	Opened Sessions .....	96
	Favorite Entries .....	99
	Most Recently Used Entries .....	102
<b>6</b>	<b>Content Area.....</b>	<b>103</b>
	Embedded Sessions .....	104
	Dashboard .....	106
<b>7</b>	<b>Panes (Footer).....</b>	<b>108</b>
	Attachments .....	110
<b>8</b>	<b>Status Bar .....</b>	<b>112</b>
	Search/Filter .....	112
	Grab Input .....	115
<b>9</b>	<b>Tray Icon .....</b>	<b>116</b>
<b>Part V Data Sources</b>		<b>118</b>
<b>1</b>	<b>2-Factor Authentication.....</b>	<b>123</b>
	Google Authenticator .....	126
	Yubikey .....	129
	Duo .....	131
	AuthAnvil .....	135
<b>2</b>	<b>Caching .....</b>	<b>137</b>
<b>3</b>	<b>Create a data source.....</b>	<b>139</b>
<b>4</b>	<b>Data Source Types.....</b>	<b>143</b>
	<b>Advanced Data Sources .....</b>	<b>150</b>
	Devolutions Online Database.....	151
	Devolutions Server.....	156
	MariaDB.....	163
	MySQL.....	170
	Microsoft SQL Server.....	178
	Configure SQL Server.....	189
	Recovery Model.....	192
	Encrypting Connections to SQL Server.....	192
	Microsoft SQL Azure.....	194
	Configure SQL Azure.....	203
	Enable Azure Active Directory Authentication.....	206
	Configure the Active Directory Admin.....	206
	Create an Azure Active Directory App Registration.....	211
	Configure RDM Active Directory Interactive (with MFA).....	217
	Configure Azure Active Directory user in RDM.....	220
	Password Hub Business.....	222
	User Vault.....	224
	<b>DropBox .....</b>	<b>226</b>
	<b>Google Drive .....</b>	<b>232</b>
	<b>Devolutions Online Drive .....</b>	<b>234</b>

Password Hub Personal .....	240
SQLite .....	242
WebDAV .....	249
XML .....	252
<b>5 Import/Export Data Source.....</b>	<b>257</b>
<b>6 Lock Data Source.....</b>	<b>259</b>
<b>7 Offline mode.....</b>	<b>260</b>
Offline Read/Write .....	264
<b>8 Manage Cache.....</b>	<b>268</b>
<b>9 User Vault .....</b>	<b>270</b>

## **Part VI Commands 271**

<b>1 Context Menu.....</b>	<b>272</b>
Open with Parameters .....	273
Documentation .....	275
Editor.....	276
Entry History .....	284
<b>2 File .....</b>	<b>287</b>
Go Offline/Online .....	291
My Data Source Information .....	292
Devolutions Account .....	296
Backup .....	299
Settings.....	299
Restore.....	301
Refresh .....	304
Change Master Key .....	304
Data Sources .....	305
Background Services .....	308
My Account Settings .....	309
My Personal Credentials.....	311
User Specific Settings List.....	313
Import .....	314
Import Computer Wizard.....	317
Import Session CSV Wizard.....	323
Import Strategies and file format.....	325
Import Network Scan.....	328
Import Sessions.....	328
Import Logins.....	330
Import Contacts.....	331
Export .....	332
Encrypted Html.....	336
Templates .....	337
Creating Templates.....	342
Default Settings.....	348
Password Templates.....	350
Options .....	355
Advanced.....	357
Import Options.....	365
Export Options.....	367
<b>3 Home .....</b>	<b>369</b>



<b>4 Actions</b>	<b>369</b>
<b>Commands</b>	<b>374</b>
RDP.....	374
VNC.....	375
SSH Shell (Rebex).....	376
Telnet.....	378
<b>5 Edit</b>	<b>380</b>
<b>Entries</b>	<b>386</b>
Checkout system.....	386
Credential Redirection.....	391
Dynamic Credential Linking.....	396
Entry Credentials Options.....	399
<b>Edit</b>	<b>401</b>
Play List.....	401
Create and Edit a Play List.....	401
Play List Management.....	409
<b>Setting Overrides</b>	<b>410</b>
Specific Settings.....	410
<b>Batch</b>	<b>413</b>
Batch Edit.....	413
<b>6 View</b>	<b>417</b>
<b>Task List</b>	<b>420</b>
<b>Activity Logs</b>	<b>423</b>
<b>Advanced Search</b>	<b>425</b>
<b>Documentation Search</b>	<b>428</b>
<b>7 Administration</b>	<b>431</b>
<b>Management</b>	<b>434</b>
User Management.....	434
User Types.....	443
Integrated Security.....	445
User Groups Management.....	446
<b>Reports</b>	<b>448</b>
Reports.....	448
Export Reports.....	449
Deleted Entries.....	453
<b>Settings</b>	<b>455</b>
Vault Settings.....	455
Default security for entries.....	455
System Settings.....	456
General.....	456
Security.....	459
Allow Password Access From External System.....	460
Application.....	463
Offline.....	466
Serial Number.....	467
Type availability.....	469
Version Management.....	470
System Permissions.....	472
Security Providers.....	477
<b>Clean up</b>	<b>484</b>
Clean Up Deleted History.....	484
Clean Up Entry History.....	486
Clean Up Activity Logs.....	487

	Pack Data Source (Optimize).....	489
<b>8 Tools</b>		<b>490</b>
	<b>Generators</b> .....	<b>493</b>
	Password Generator.....	493
	SSH Key Generator.....	501
	Certificate Generator.....	503
	Port Generator.....	507
	<b>Tools</b> .....	<b>508</b>
	Devolutions Localizer.....	508
	Password Analyzer.....	510
	Key Agent Manager.....	513
	PowerShell (RDM CmdLet).....	518
	More Tools.....	519
	Chocolatey Console.....	519
	Local RDP/RemoteApp Manager.....	522
	Playback (Ansi).....	528
	RDM Agent.....	531
<b>9 Help</b>		<b>540</b>
	<b>Support</b> .....	<b>542</b>
	Application Log.....	542
	Diagnostic.....	545
	Profiler.....	548
	Record.....	551

## Part VII Devolutions Web Login 552

<b>1 Overview</b>		<b>553</b>
<b>2 Installation</b>		<b>554</b>
	Chrome .....	555
	Firefox .....	557
	Edge .....	558
	Opera .....	562
<b>3 First Login</b>		<b>563</b>
	Password Hub .....	563
	Devolutions Server .....	566
	Remote Desktop Manager .....	570
<b>4 Exploring Devolutions Web Login.....</b>		<b>572</b>
	Menu .....	572
	Settings.....	573
	Retrieve Credentials .....	577
	Remote Desktop Manager.....	578
	Secure Devolutions Web Login .....	579
	Unpair a Browser Extension.....	584
	Keyboard Shortcuts .....	584

## Part VIII User Groups Based Access Control 587

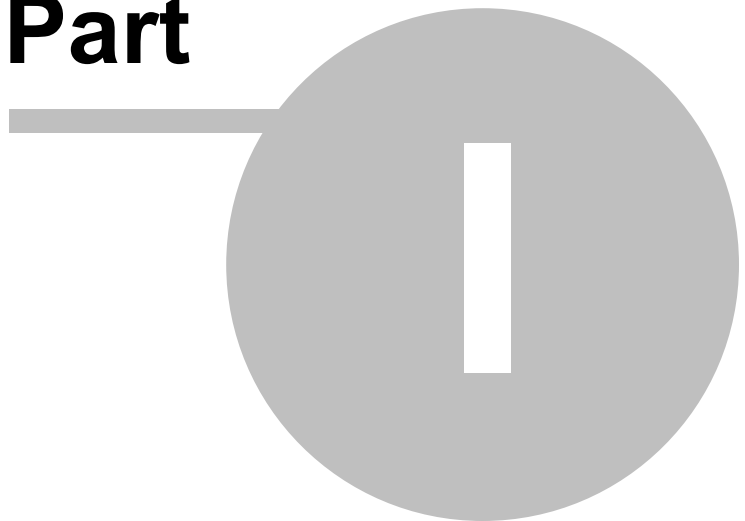
<b>1 Permission</b>		<b>598</b>
<b>2 Scenarios</b>		<b>600</b>
	Simplified Security .....	600
	Advanced Security .....	610
<b>3 Legacy Information.....</b>		<b>622</b>

---

Small to Medium Enterprise .....	622
<b>Part IX PowerShell Scripting</b>	<b>633</b>
1 Tips and tricks.....	634
2 PowerShell Module.....	636
Extract TeamViewer ID .....	637
Custom Export to CSV .....	638
Creating Group Folder Structure from CSV file .....	638
3 Custom PowerShell Commands.....	640
Change your Synchronizer source .....	644
Batch Actions Samples .....	646
<b>Part X Support/Resources</b>	<b>651</b>
1 Technical Support.....	652
2 Keyboard Shortcuts.....	653
3 Lexicon .....	658
4 Tutorials .....	660

# Overview

**Part**



# 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, Wayk Bastion, X Windows**, and more!

### THE REMOTE DESKTOP MANAGER ECOSYSTEM

Remote Desktop Manager is available in two editions:

<b>Free</b>	For individuals only, no information can be shared with colleagues. The most popular remote access technologies are supported, and passwords can be stored securely.
<b>Enterprise</b>	Used by teams, this edition offers user permissions, user groups, advanced logging, etc. Typically uses a Database Management System (DBMS) for storing the information and sharing it according to <b>your</b> security requirements. Devolutions also offers two specialized services for either 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	✓	✓
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. Please refer to Windows Credential Manager for more information.

## 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 one of the supported [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 security:

- Use an [Advanced Data Source](#) and grant user access by assigning permissions.
- Use encrypted communication with the database when available.
- Use the [Data Source Settings \(System Settings\)](#) 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 to add an additional layer of protection to the local cache. Go to **File – Options – Security**.
- Require a password to launch the application, and even better: require two factor authentication. **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 policies to enforce some of these settings at the system level.

## 1.3 System Requirements

### DESCRIPTION

Remote Desktop Manager requires the following prior to installation:

### MINIMUM REQUIREMENTS

#### Windows Desktop:

- Windows 10
  - Version 1607, 1703, 1709, 1803, 1809, 1903 and 1909
- 8.1
- 7 SP1

#### Windows Server:

- Windows Server 2019
  - Version 1709, 1803 and 1809
- 2016
- 2012 R2
- 2012
- 2008 R2 SP1

Microsoft .NET Framework 4.7.2

1 GHz or faster processor

512MB RAM

1024 x 768 screen resolution

500+ MB hard drive space

## 64-BIT SUPPORT

Remote Desktop Manager is compatible with all 64-bit versions of Windows.

## 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 are managed automatically by our installers. The only situations where one would perform a manual installation of the prerequisite software is when the zip archive is used for deployment or if there is no internet connection.

## SETTINGS

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

- [Microsoft .NET Framework 4.7.2](#).

## 1.4 The Devolutions Platform

### DESCRIPTION

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

The flagship product is Remote Desktop Manager, the strongest edition admittedly being for the Windows operating system.

APPLICATIONS	DESCRIPTION	INSTALLATION
<b>Remote Desktop Manager (RDM)</b>	Application used to manage and centralize remote access technologies, passwords, documents and shared information.	Windows, macOS, iOS, Android
<a href="#">Remote Desktop Manager Agent</a>	Tool used to run commands on remote systems. It listens for commands from a master Remote Desktop Manager. It resolves a lot of issues brought on by remote management, in particular removing the need to use Microsoft's WinRM and managing lists of <i>TrustedHosts</i> .	Windows
<a href="#">Remote Desktop Manager Jump</a>	Feature that uses the Remote Desktop Manager Agent to launch any of our supported technologies on a remote Windows Host. It transforms it in what is called alternatively a Jump Server, or Bastion Server, or Service Host.	Windows



APPLICATIONS	DESCRIPTION	INSTALLATION
<a href="#"><u>Devolutions Server (DVLS)</u></a>	Enterprise Grade data store for creating a centralized database for your team. Integrates with AD to drastically reduce time spent on managing permissions. It is installed on-premises and offers many advanced features.	Windows
<b>Devolutions Web Login (DWL)</b>	Web browser extension technology that interacts with our Remote Desktop Manager and Password Vault Manager desktop applications to obtain credentials and automatically fill authentication fields in your browser.	Windows, macOS

#### 1.4.1 Remote Desktop Manager Agent

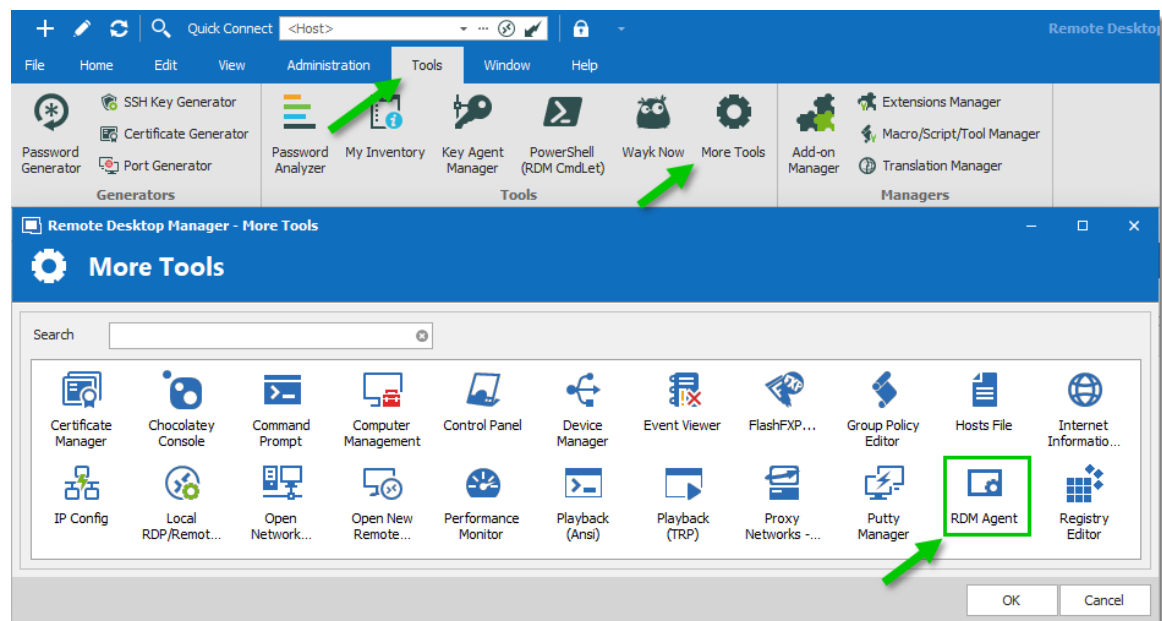
### DESCRIPTION



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.

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.



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.

## HOW DOES IT WORK?



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.

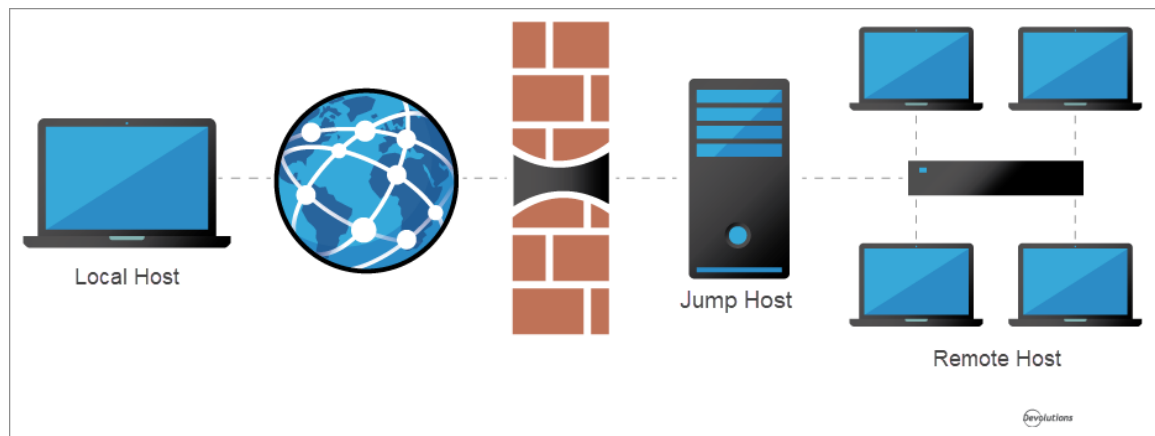
Please consult the Configure Remote Desktop Manager Jump topic.

## USAGE SCENARIOS

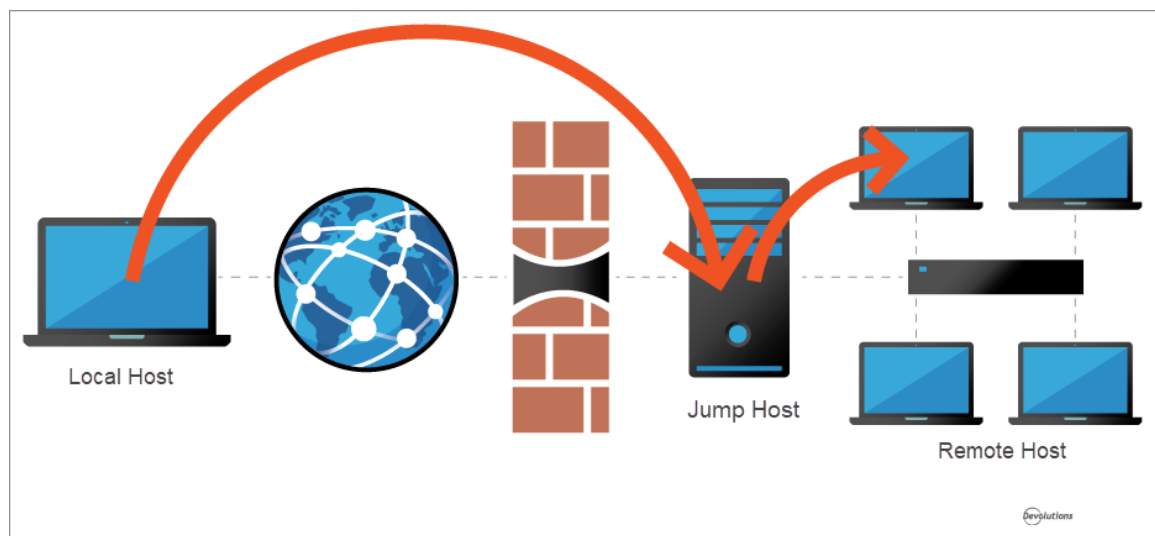
There are two targeted scenarios:

### 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.

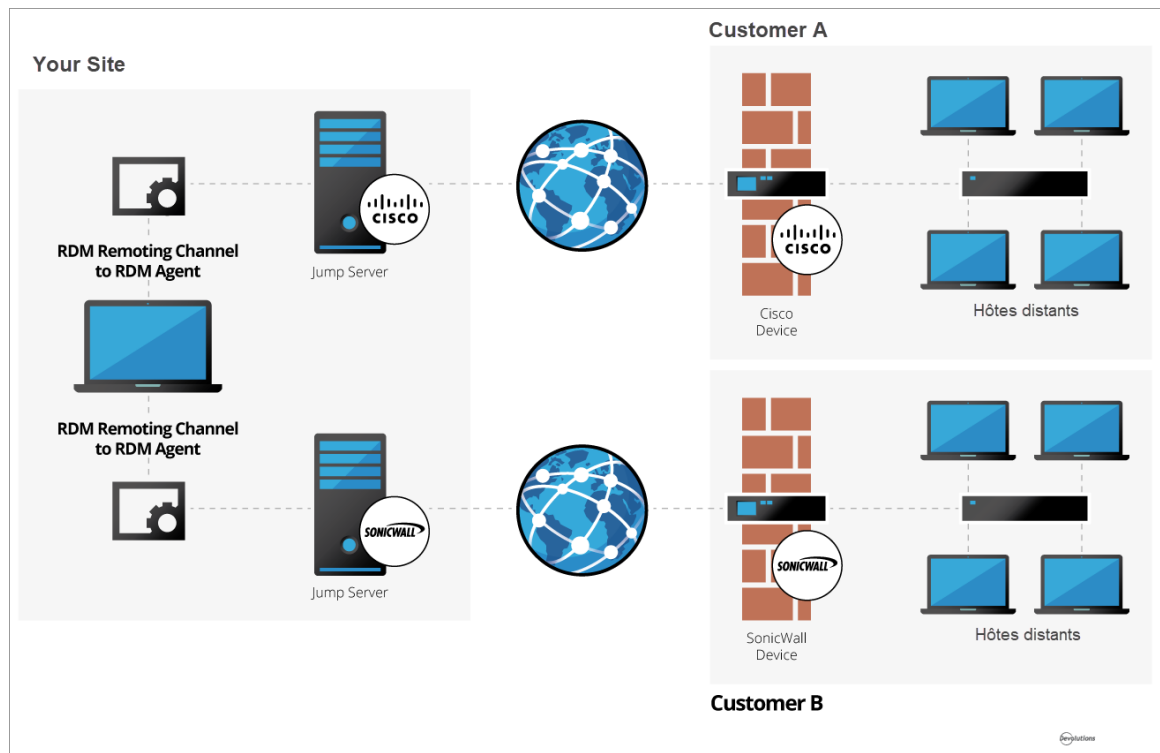


Remote Desktop Manager Jump helps achieve that goal simply and efficiently.

## 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.

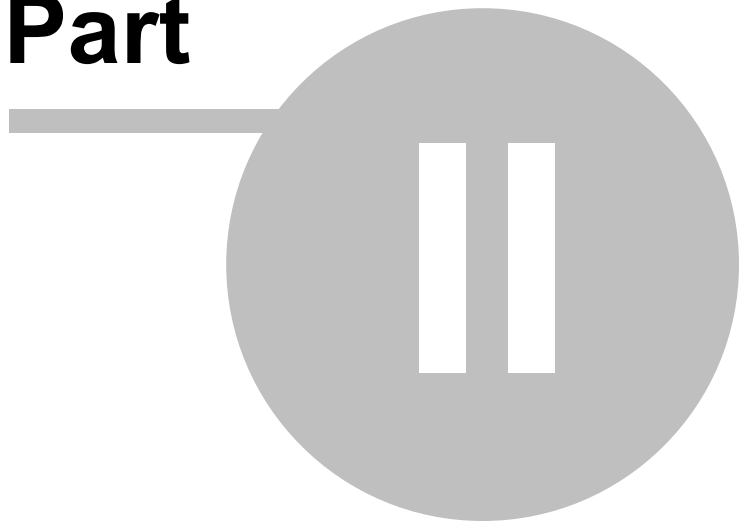




*Remote Desktop Manager Jump to handle incompatible VPN clients*

# Getting Started

**Part**



## 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
<p>Step 1 - Register your license:</p> <ul style="list-style-type: none"><li>• <a href="#">Enterprise Registration</a></li><li>• <a href="#">Trial Registration</a></li></ul>	<p>Remote Desktop Manager Enterprise Edition grants you a 30 day trial. If you decide not to register by 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 license key.</p> <p>Here is a video link to assist you: </p>

CHECKLIST FOR INDIVIDUALS (ENTERPRISE EDITION)	DESCRIPTION
Step 2 - Add your Data Source and set up your Devolutions account and a master key.	<p>Warning: When choosing any data source type that is not <b>on-premises</b>, 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 <a href="#">Security Provider</a> for <a href="#">Advanced Data Sources</a>. This ensures <b>only you</b> can read the data.</p> <p>Upon first launch, Remote Desktop Manager uses a local SQLite data source. For help selecting a data source tailored to your needs, please see <a href="#">Choosing your data source (Individuals)</a>.</p> <p>Here is a video link to assist you:  <a href="#">Watch Video</a></p>
Step 3 - Set up your Devolutions Online Backup .	<p>The <a href="#">Online Backup</a> allows you to securely backup 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.</p> <p>Here is a video link to assist you:  <a href="#">Watch Video</a></p>
Step 4 - Create your <a href="#">Default Settings</a> .	<p>In <b>File - Options</b> 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.</p> <p>Here is a video link to assist you:  <a href="#">Watch Video</a></p>
Step 5 - Create your folder structure	<p>Top level folders are at the foundation of a solid security structure. Your folder structure (Folder entries) should represent your company structure.</p>

CHECKLIST FOR INDIVIDUALS (ENTERPRISE EDITION)	DESCRIPTION
	Here is a video link to assist you:  <a href="#">Watch Video</a>
Step 6 - <a href="#">Import your Data</a> .	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 easy steps.  Here is a video link to assist you:  <a href="#">Watch Video</a>

### 2.2.1 Select the Data Source type - Individuals

#### DESCRIPTION

This topic is for individuals.

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
FTP, SFTP		X		X		Note 1
WebDav		X		Note 2		Note 2
Devolutions Online Database - Basic			X	X	X	3 users

## NOTES

### NOTE 1

There is no protection in the case of data contention issues. The last one saving the file will win! This is for **single** users with **multiple** computers, **not for multiple users** using the data concurrently.

## NOTE 2


The master XML is maintained by a single user and synchronized 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
<p>Step 1 - Register your license:</p> <ul style="list-style-type: none"> <li>• <a href="#">Enterprise Registration</a></li> <li>• <a href="#">Trial Registration</a></li> </ul>	<p>Remote Desktop Manager Enterprise Edition grants you a 30 day trial. If you decide not to register by 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 license key.</p>
<p>Step 2 - Add your <a href="#">Data Source</a> (for teams).</p>	<p>Warning: When choosing any data source type that is not <b>on-premises</b>, 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 <a href="#">Security Provider</a> for <a href="#">Advanced Data Sources</a>. This ensures <b>only you</b> can read the data.</p> <p>Upon first launch, Remote Desktop Manager uses a local SQLite data source. For help selecting a data source tailored to your needs, please see <a href="#">Choosing your data source (Teams)</a>.</p>

CHECKLIST FOR TEAMS	DESCRIPTION
Step 3 - Select your <a href="#">Security Provider</a> .	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 structure.	<p>Top level folders are at the foundation of a solid security structure. Your folder structure (Folder entries) should 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.</p> <p>Here is a video link to assist you:  <a href="#">Watch Video</a></p>
Step 5 - Create your <a href="#">Default Settings</a> .	In <b>File - Options</b> 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 <a href="#">Custom Installer</a> to share the pre-configured version with your team.
Step 6 - Create <a href="#">Users</a> .	Remote Desktop Manager supports advanced User Management. User accounts must be created manually by an administrator of the database.
Step 7 - Create <a href="#">User Groups</a> .	Create User Groups to easily 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 <a href="#">Entries</a> .	An Entry is how you save information about your sessions (e.g. RDP, SSH connections), credentials, websites, VPNs, Synchronizers and documents.
Step 9 - <a href="#">Grant Permissions</a> .	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.

	CHECKLIST FOR TEAMS	DESCRIPTION
	Step 10 - <a href="#">Import your Data</a> .	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 easy steps.

### 2.3.1 Select the Data Source type - Teams

#### DESCRIPTION

This topic is for teams that need 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. If you have multiple concerns, simply create the intersection of all sets to isolate a list of choices.

CONCERN	Devoluti ons Server	SQL SERVER	SQL AZURE	MYSQL/ MARIAD B	DODB PRO	DODB ENT
The database is not accessible to end users	X	Note 1 & 2	Note 1	Note 1	Note 1	Note 1
AD accounts used for	X	X				

CONCERN	Devoluti ons Server	SQL SERVER	SQL AZURE	MYSQL/ MARIAD B	DODB PRO	DODB ENT
<b>authentication</b>						
<b>AD group membership used to assign permissions</b>	X					
<b>The data is stored on-premises</b>	X	X		X		
<b>Activity Logs</b>	X	X	X	X		X
<b>Data accessible globally</b>	Note 3	Note 4	X	Note 4	X	X
<b>Optional local cache of connections</b>	X	X	X	X	X	X

## NOTES

### NOTE 1

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

### NOTE 2

Integrated Security is the name of a Microsoft technology that does not send credentials to get access to a SQL Server instance, but rather the token resulting from 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 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, you must ALSO protect against DDoS attacks. Cloud services, like Azure or Amazon Web Services, have that concern in the forefront. The default settings of the firewall should be to block everything, you will then open only the most limited set of ports, while filtering on a short list of acceptable origins for requests.

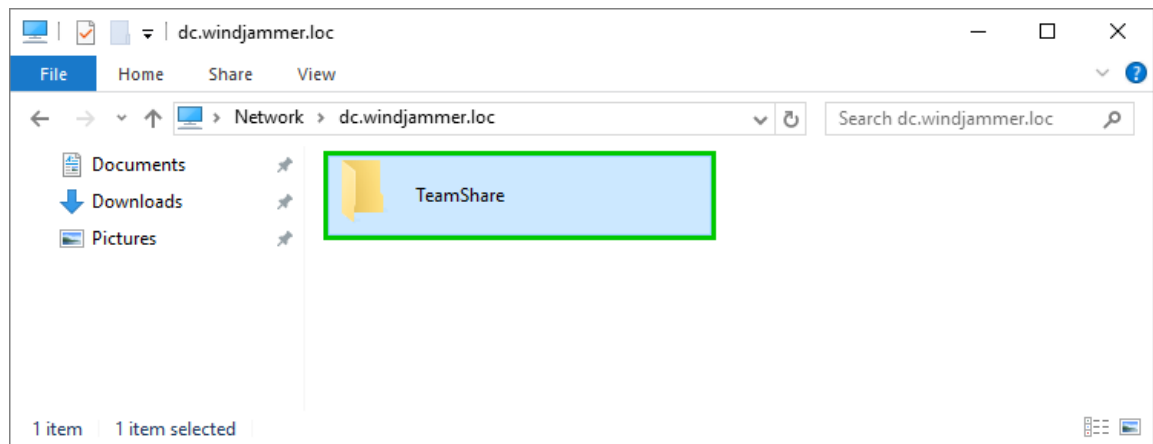
## 2.3.2 Set up a team folder for default settings

### 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.

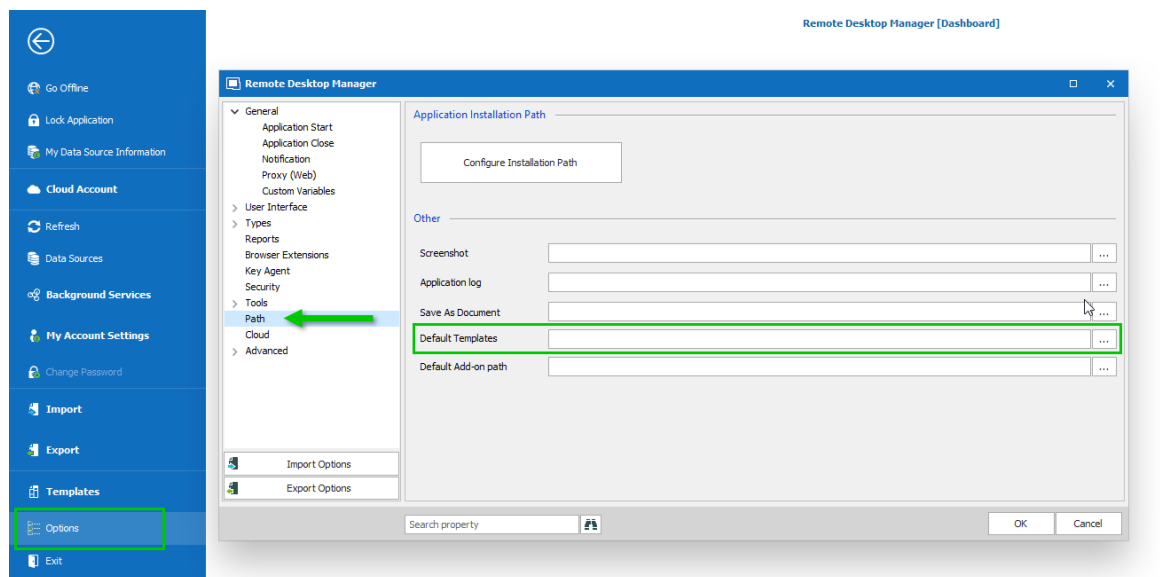
### SETTINGS

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



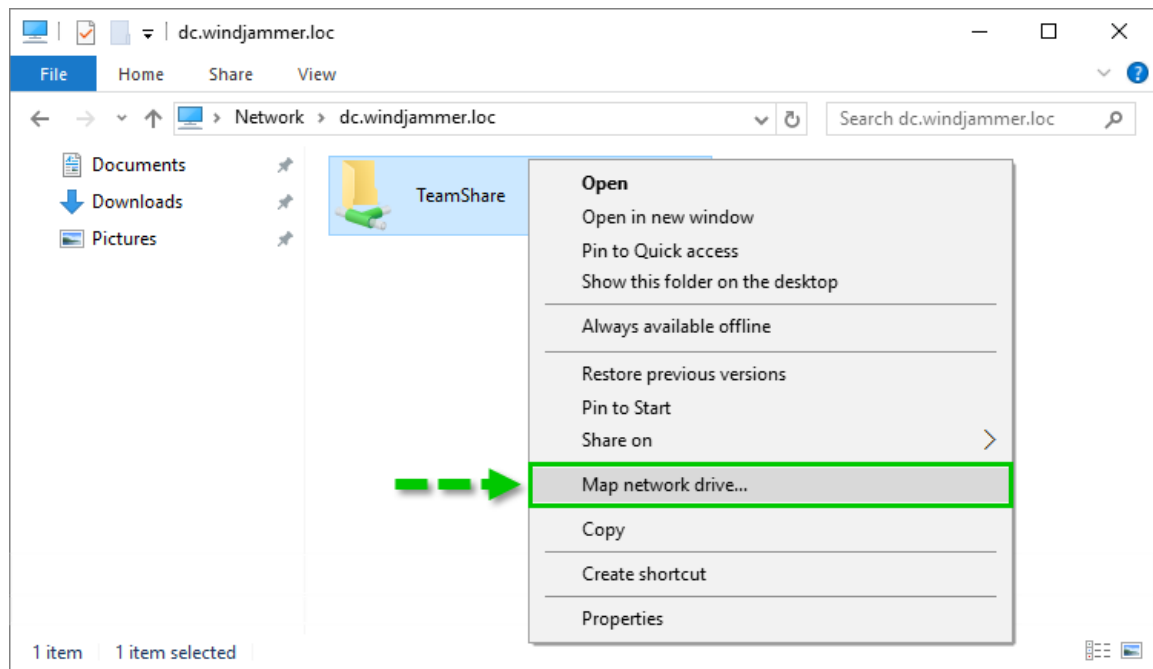
*Server Drive - Team Folder*

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 10.

*Map Network Drive*

## 2.4 Creating an Entry

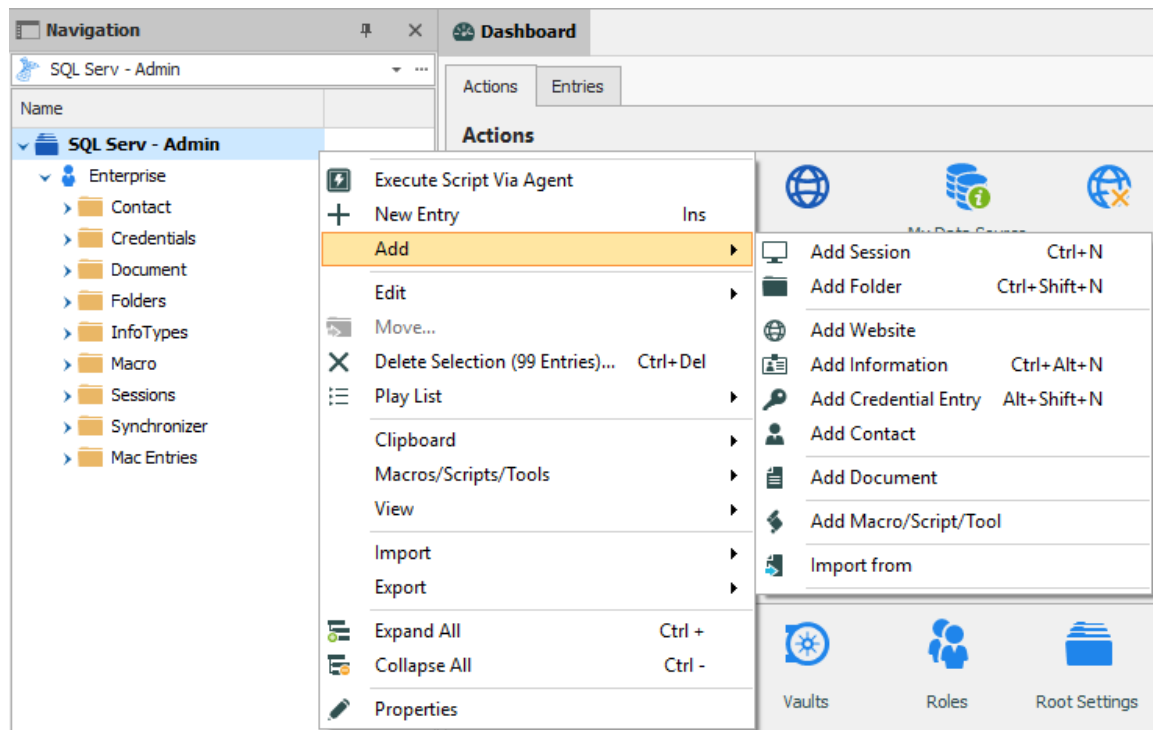
### DESCRIPTION

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.

## 2.5 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 launching **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**.

A few key points that the admin of the solution must be aware of:

<b>Password visibility</b>	You can store passwords in a <b>Credential</b> entry ( <b>Username / Password</b> entry, which (by default) makes the password <b>USABLE</b> , but not <b>VISIBLE</b> , by the end user. We provide multiple Credential entry types, you should always consider carefully which type you are using based on your security and administrative needs.
<b>Credentials set on folders</b>	Our folders can have credentials defined. This is useful because in the great majority of cases, one reuses the same credentials for a whole branch of the network infrastructure. To make use of credentials defined in a folder, the child sessions must be adjusted to use <b>Inherited Credentials</b> .
<b>Entry location</b>	When storing entries in the tree view, users with the <b>View</b> permissions on that entry (or folder by inheritance) will be able to make use of them. This is how you would share credentials with other members of your team. A <a href="#">User Vault</a> exists for users to store user centric information that should be seen by no one else. Credentials stored this way can still be accessed in the Public area of the system by referencing them or through the <b>User Specific Settings</b> feature described below.

### User Specific Settings

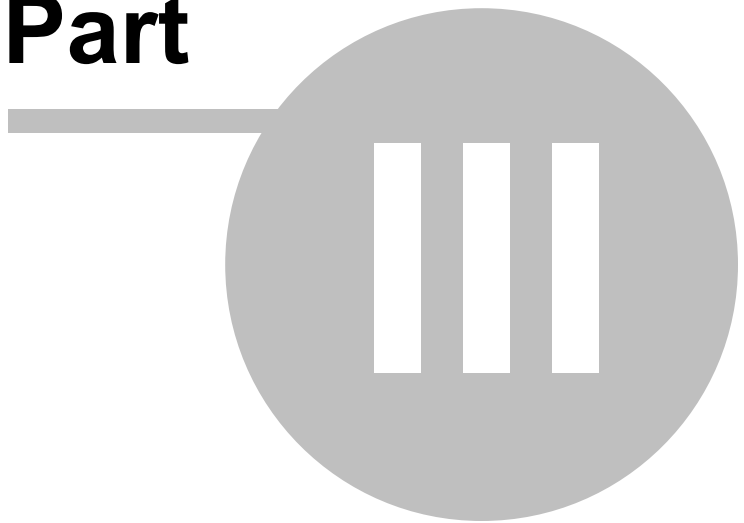
User Specific Settings are **partial overrides** for settings of your entries, most notably the **Credentials**. When applying such an override, one can choose the type in the credentials **directly** in the override or one can choose to instead link to credentials stored elsewhere, such as the User Vault.

Here are the most common scenarios and how to address them. In the majority of cases, we prefer to have sessions using **Inherited credentials**, meaning it climbs up the tree until it has access to a set of credentials, be it 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 <u>Vault Settings</u> . All children use <b>Inherited Credentials</b> .
Each user has its own credentials for many different branches (often corresponds to customers/departments, etc).	Make use of the <u>User Specific Settings</u> on each branch. All children use <b>Inherited Credentials</b> .
Each user has its own credentials managed by an administrator.	This solution involves a little more work. The admin must create a folder for each user, then grant permissions <b>ONLY</b> to that user. The user will then use <b>User Specific Settings</b> to specify that the credentials stored in that folder is used to override what is defined in the entries.
Each team uses the same credentials.	Much like directly above, but all the members of the team have access to the folder. All of them must use the <b>User Specific Settings</b> .
Each user uses their domain account.	Have the sessions configured to use <u>My personal credentials</u> . Each user will be prompted to define them once per workstation that they use.

# Installation

**Part**



## 3 Installation

### 3.1 Client

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 SQL Azure 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.

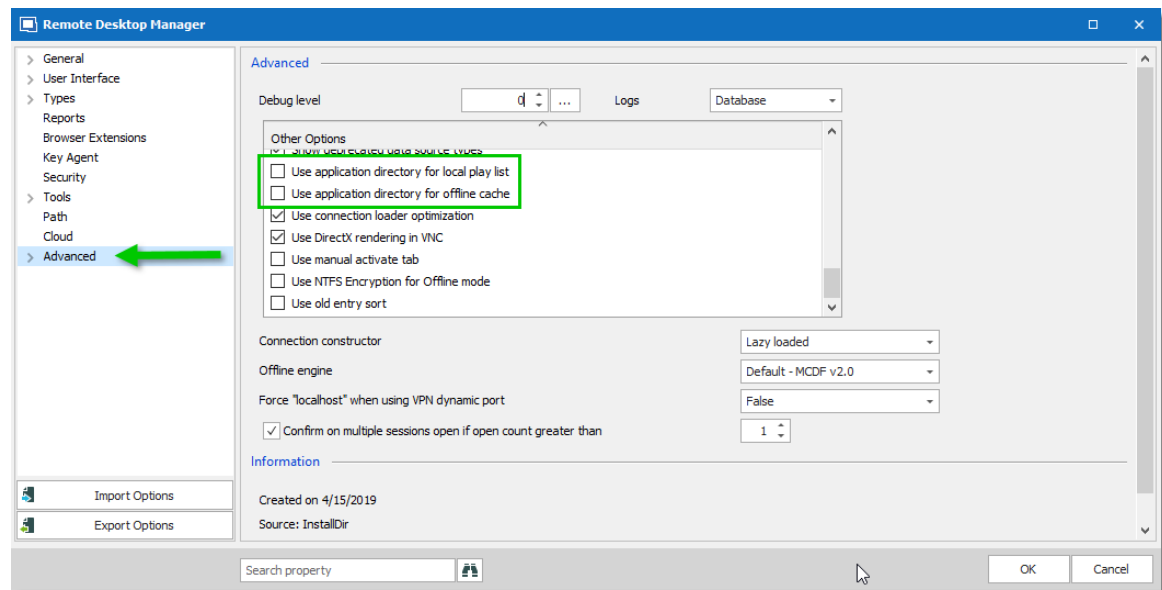
#### SUMMARY

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

FILE(S)	LOCATION	OVERRIDE SOURCE
Layout Files (*.lyt)	[CONFIG]	None
Log Files (*.log, *.debug)	[CONFIG]	None
Offline/Cache data (offline.db)	[PROFILE] \[Datasource]	<b>Use application directory for <i>online cache</i></b> will use instead [INSTALLDIR]
Local Play lists	[PROFILE] \[Datasource]\Playlists	<b>Use application directory for <i>local playlist</i></b> will use instead [INSTALLDIR]
Local Templates	They are serialized directly in the configuration file of the application.	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

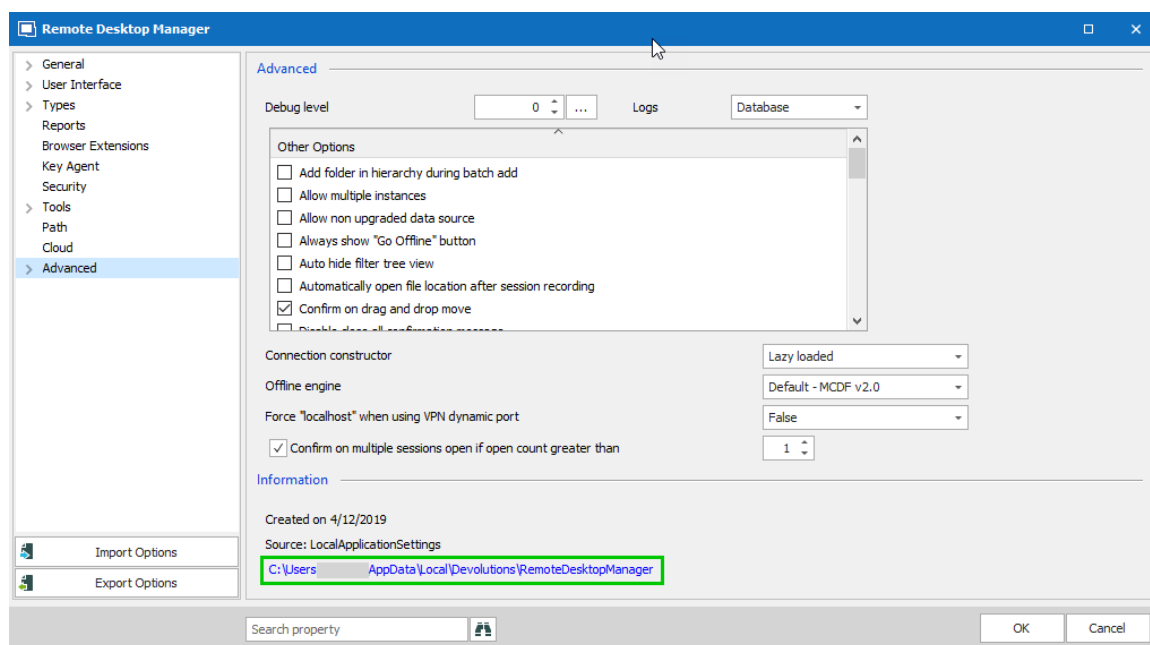
## DEFAULT LOCATION

Remote Desktop Manager saves its configuration in a file named **RemoteDesktopManager.cfg**. This file contains all of the application settings and configured data sources. All of the data source settings are encrypted for security reasons.



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
<b>Installed under "Program Files" or "Program Files (x86)"</b>	%LocalAppData%\Devolutions\RemoteDesktopManager
<b>Application running on Terminal Server</b>	%AppData%\Devolutions\RemoteDesktopManager. This is the roaming profile and avoids multi-user conflicts.
<b>Other</b>	Installation folder



Having the configuration file in the installation folder allows you to run multiple versions of the application side-by-side.

## 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	
<b>c:\RDM</b>	The config file is saved in the designated folder.
<b>.</b>	The period is used to specify the Remote Desktop Manager installation folder.
<b>%AppData%\Devolutions\RemoteDesktopManager</b>	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) or as an executable (.EXE 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.

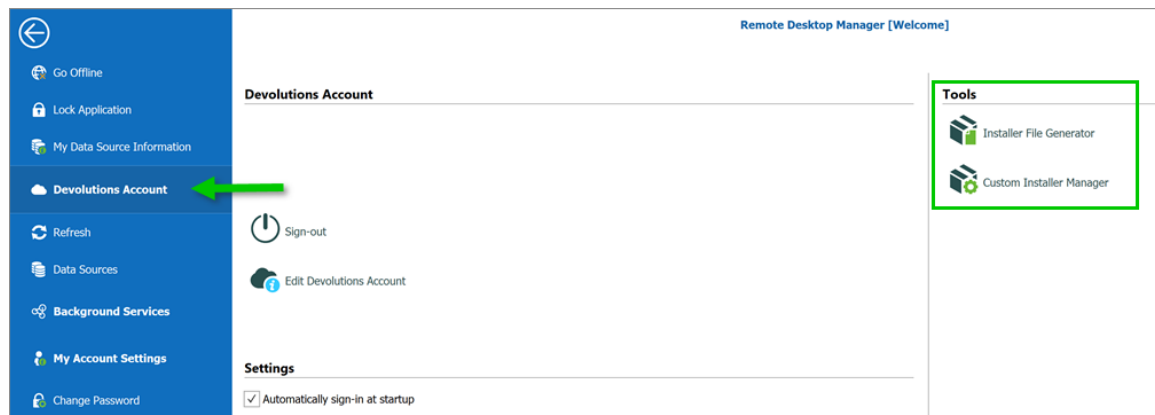


The Custom Installer Service uploads a configuration file to our online services. You should not use the service to redistribute passwords for data sources or an Online Database account.



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.

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](#)

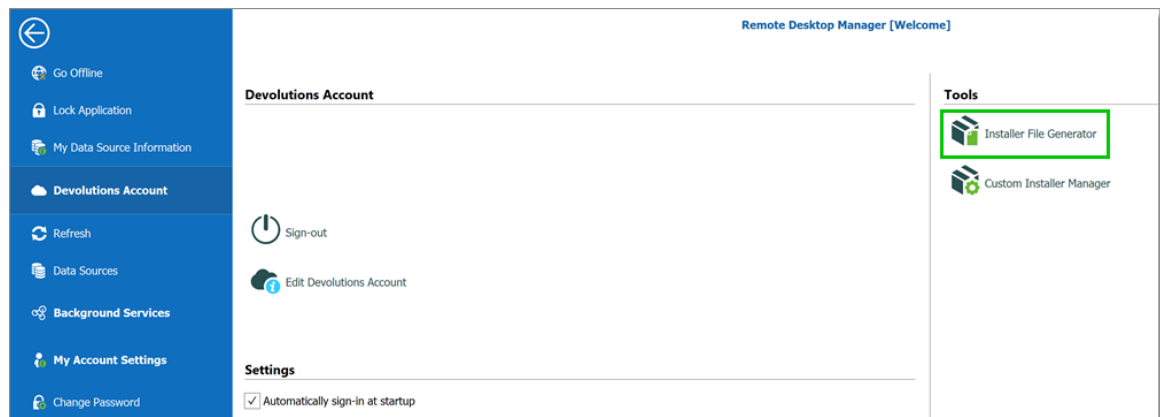
#### 3.1.3.1 Installer File Generator

### 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.

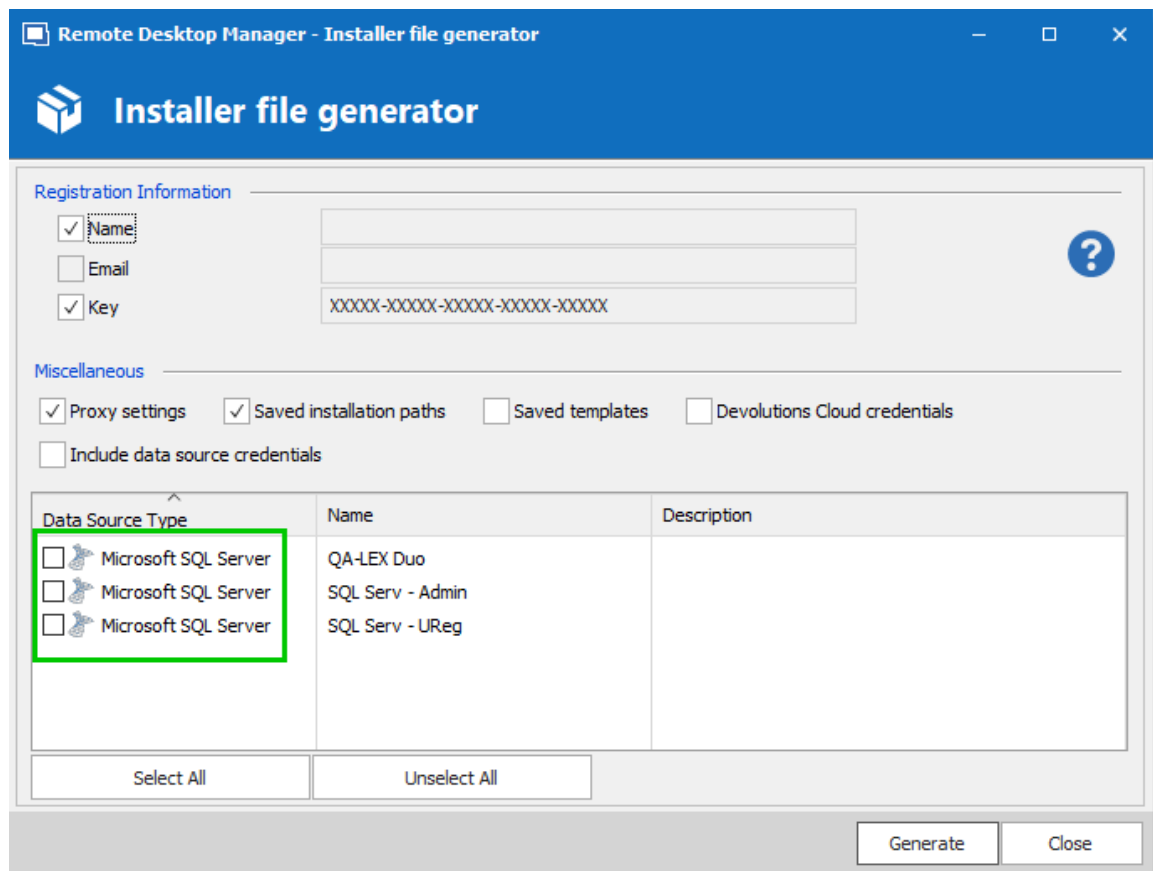
### CREATING AN INSTALLER FILE

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



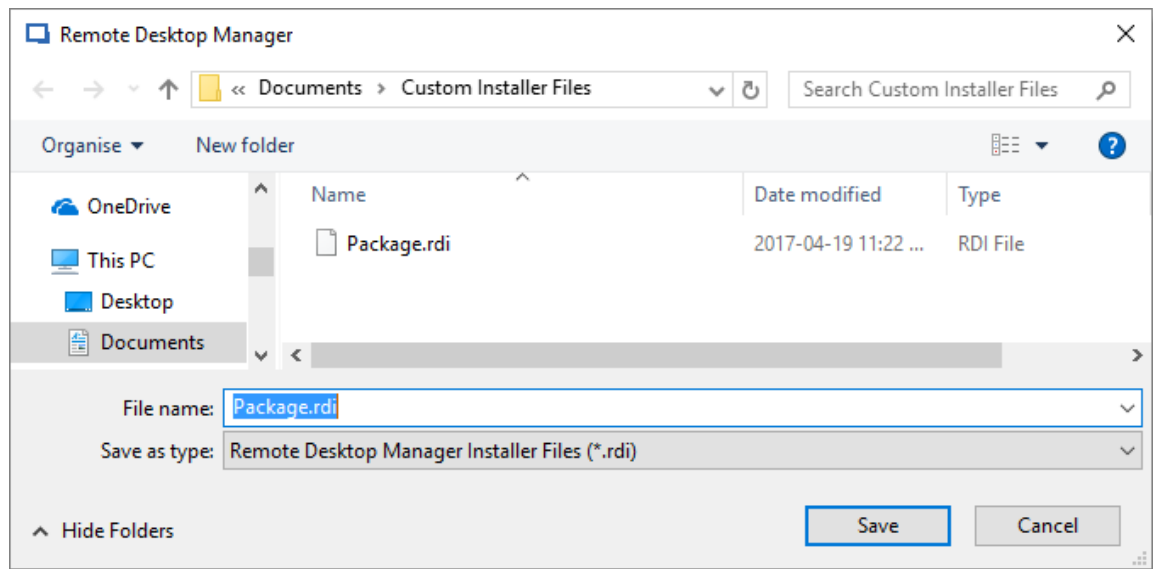
*File - Devolutions Account - Installer File Generator*

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



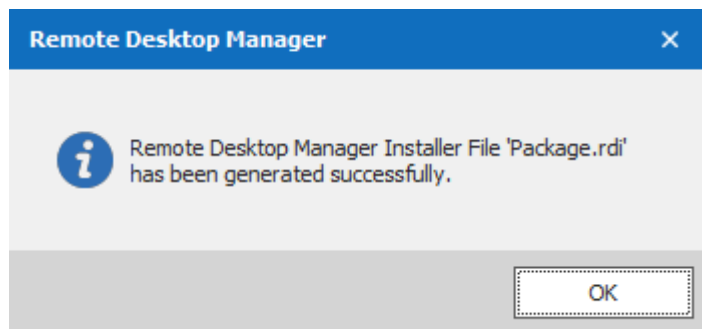
*Installer File Generator*

3. Click on **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 – General – Application Start**). 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**.

Remote Desktop Manager - Installer file generator

## Installer file generator

**Registration Information**

☒ Name ☐ Email ☒ Key

XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

**Miscellaneous**

☒ Proxy settings ☒ Saved installation paths ☐ Saved templates ☐ Devolutions Cloud credentials

☐ Include data source credentials

Data Source Type	Name	Description
<input type="checkbox"/> Microsoft SQL Server	QA-LEX Duo	
<input type="checkbox"/> Microsoft SQL Server	SQL Serv - Admin	
<input type="checkbox"/> Microsoft SQL Server	SQL Serv - UReg	

Select All Unselect All

Generate Close

Installer File Generator

## REGISTRATION INFORMATION

**Registration Information**

☒ Name ☐ Email ☒ Key

XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Installer File Generator - Registration Information

OPTION	DESCRIPTION
<b>Name</b>	Company registration name.
<b>Email</b>	Registration email if using a generic address.



OPTION	DESCRIPTION
<b>Key</b>	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.

### Miscellaneous


- ☒ Proxy settings
 ☒ Saved installation paths
 ☐ Saved templates
 ☐ Devolutions Cloud credentials
 ☐ Include data source credentials

### Installer File Generator - Miscellaneous

OPTION	DESCRIPTION
<b>Saved installation paths</b>	Preserves your installation paths configured for external third party applications. Use this only when all of the user's machines use the same paths.
<b>Saved templates</b>	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
<b>Filter history</b>	Preserves your search/filter history
<b>Proxy settings</b>	Includes your Internet proxy settings
<b>Devolutions Account credentials</b>	Includes your Devolutions Account credentials used to create the custom installer. Please, consult security warning above.
<b>Include data source credentials</b>	Includes the credentials for all selected data sources below. Please, consult security warning above.

## DATA SOURCES

Data Source Type	Name	Description
<input type="checkbox"/>  Microsoft SQL Server	QA-LEX Duo	
<input type="checkbox"/>  Microsoft SQL Server	SQL Serv - Admin	
<input type="checkbox"/>  Microsoft SQL Server	SQL Serv - UReg	

*Data Source List*

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



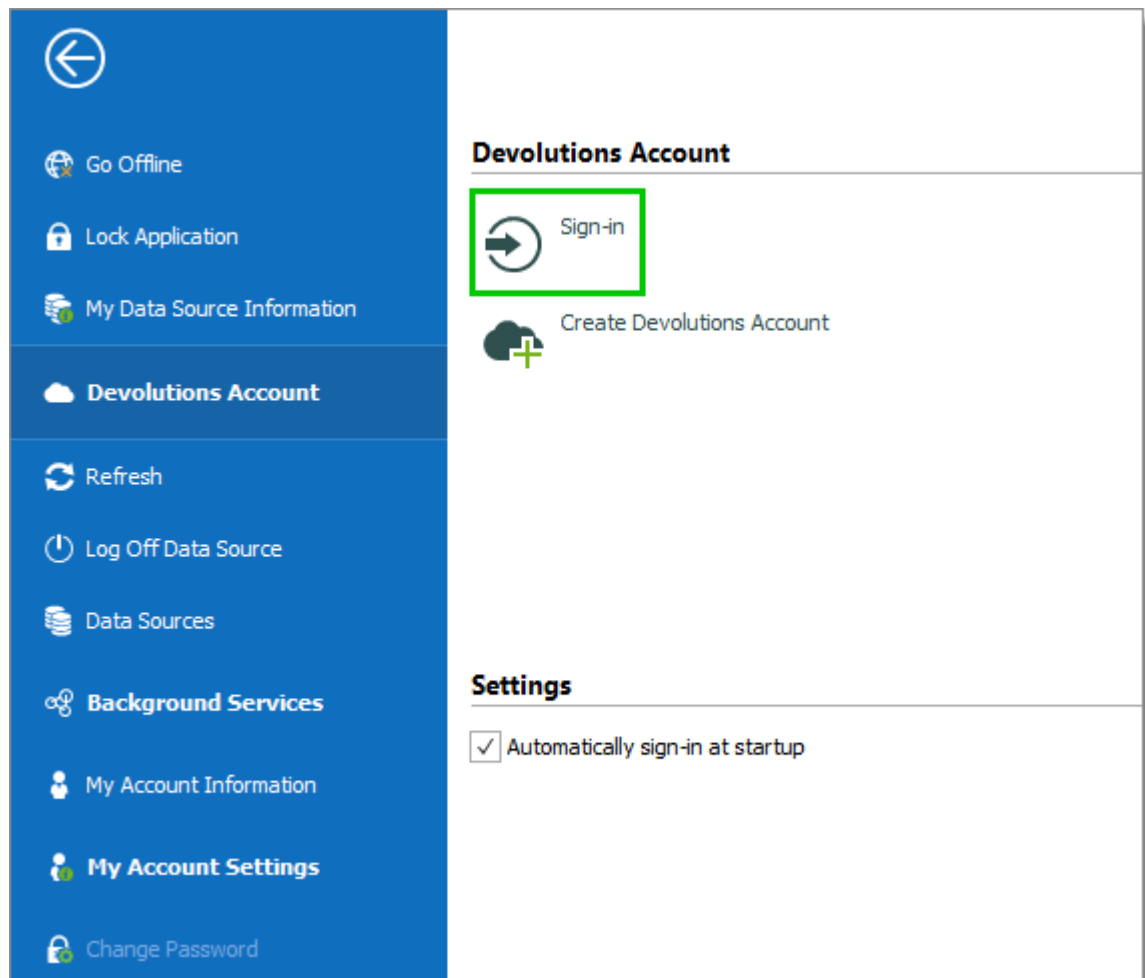
For stability reasons, in large installation bases, the latest official release is not available to the Custom Installer Service for an undetermined period while we ensure that no major issues are present. We recommend using this time with your organization to perform integration tests on a few workstations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

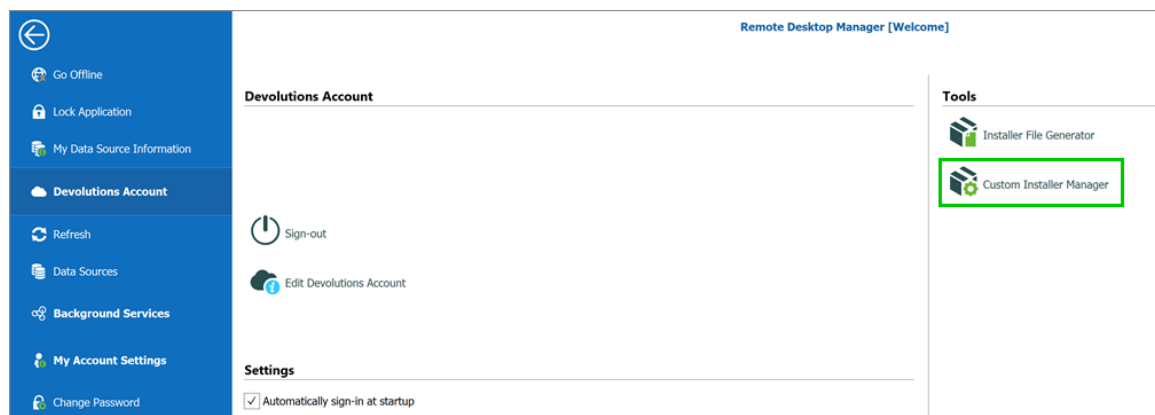
## CREATE AN INSTALLATION PACKAGE

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.

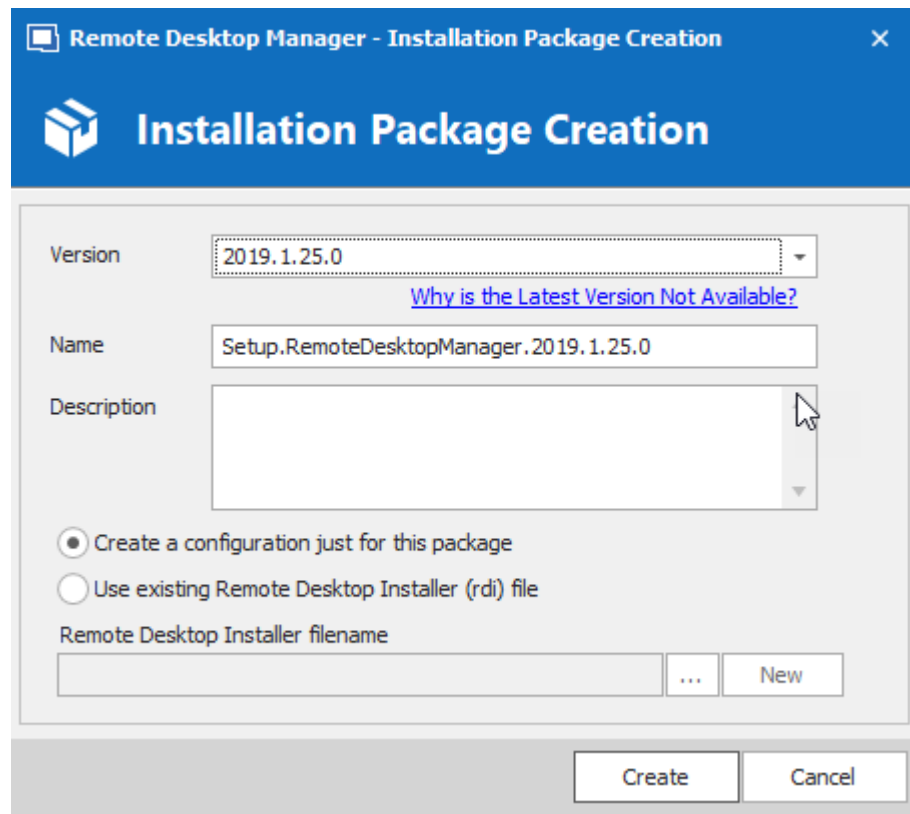


*File - Devolutions Account - Custom Installer Manager*

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.



Remote Desktop Manager - Installation Package Creation

## Installation Package Creation

Version: 2019.1.25.0 [Why is the Latest Version Not Available?](#)

Name: Setup.RemoteDesktopManager.2019.1.25.0

Description:

☒ Create a configuration just for this package  
☐ Use existing Remote Desktop Installer (rdi) file

Remote Desktop Installer filename: ... New

Create Cancel

*Installation Package Creation*

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

Remote Desktop Manager - Installer file generator

**Installer file generator**

Registration Information

☒ Name: UWutmate

☐ Email:

☒ Key: XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Miscellaneous

☒ Proxy settings ☒ Saved installation paths ☐ Saved templates ☐ Devolutions Cloud credentials

☐ Include data source credentials

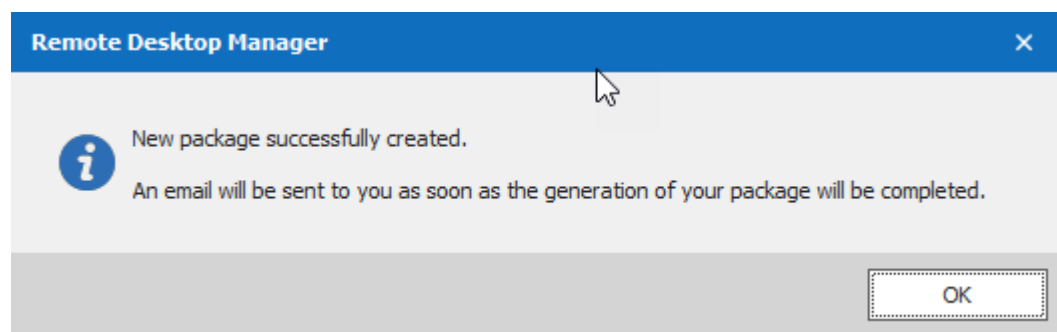
Data Source Type	Name	Description
<input type="checkbox"/> Microsoft SQL Server	QA-LEX Duo	
<input type="checkbox"/> Microsoft SQL Server	SQL Serv - Admin	
<input type="checkbox"/> Microsoft SQL Server	SQL Serv - UReg	

Select All Unselect All

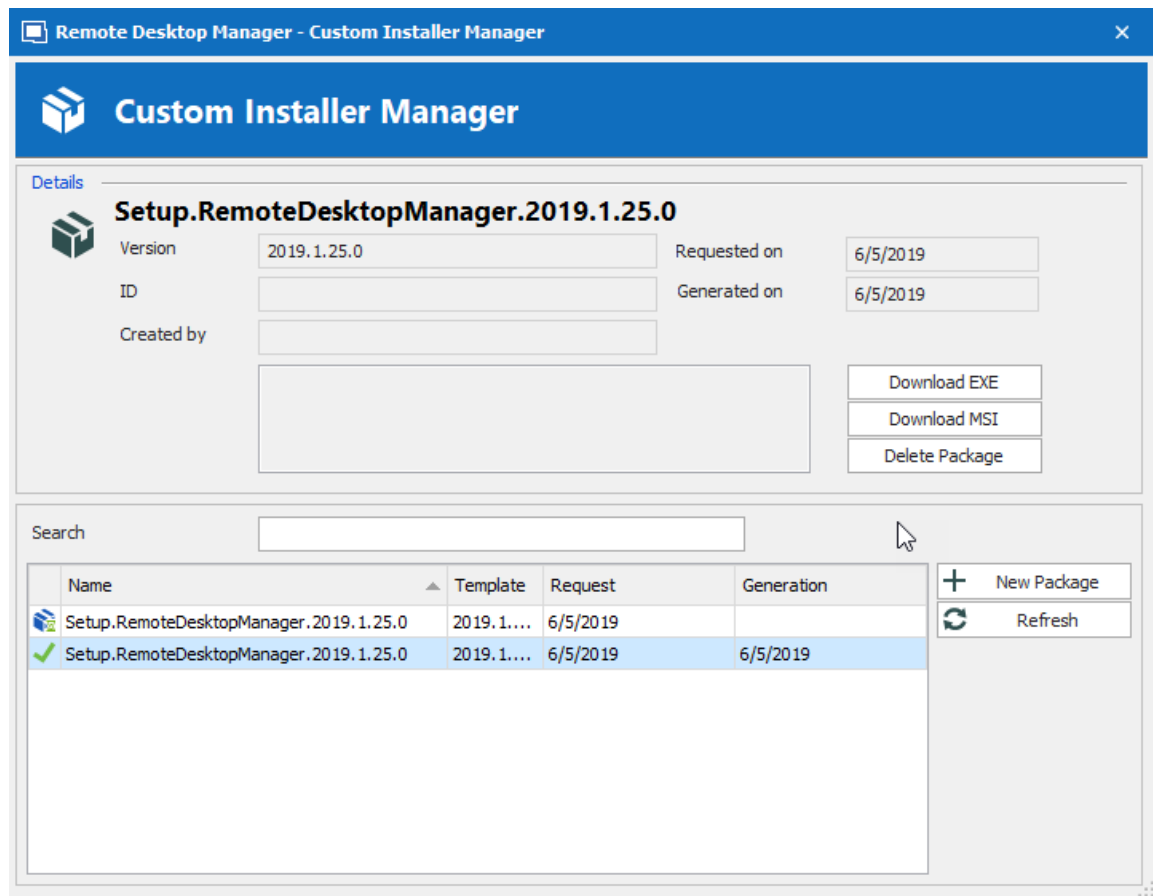
Generate Close

*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.



Custom Installer Manager

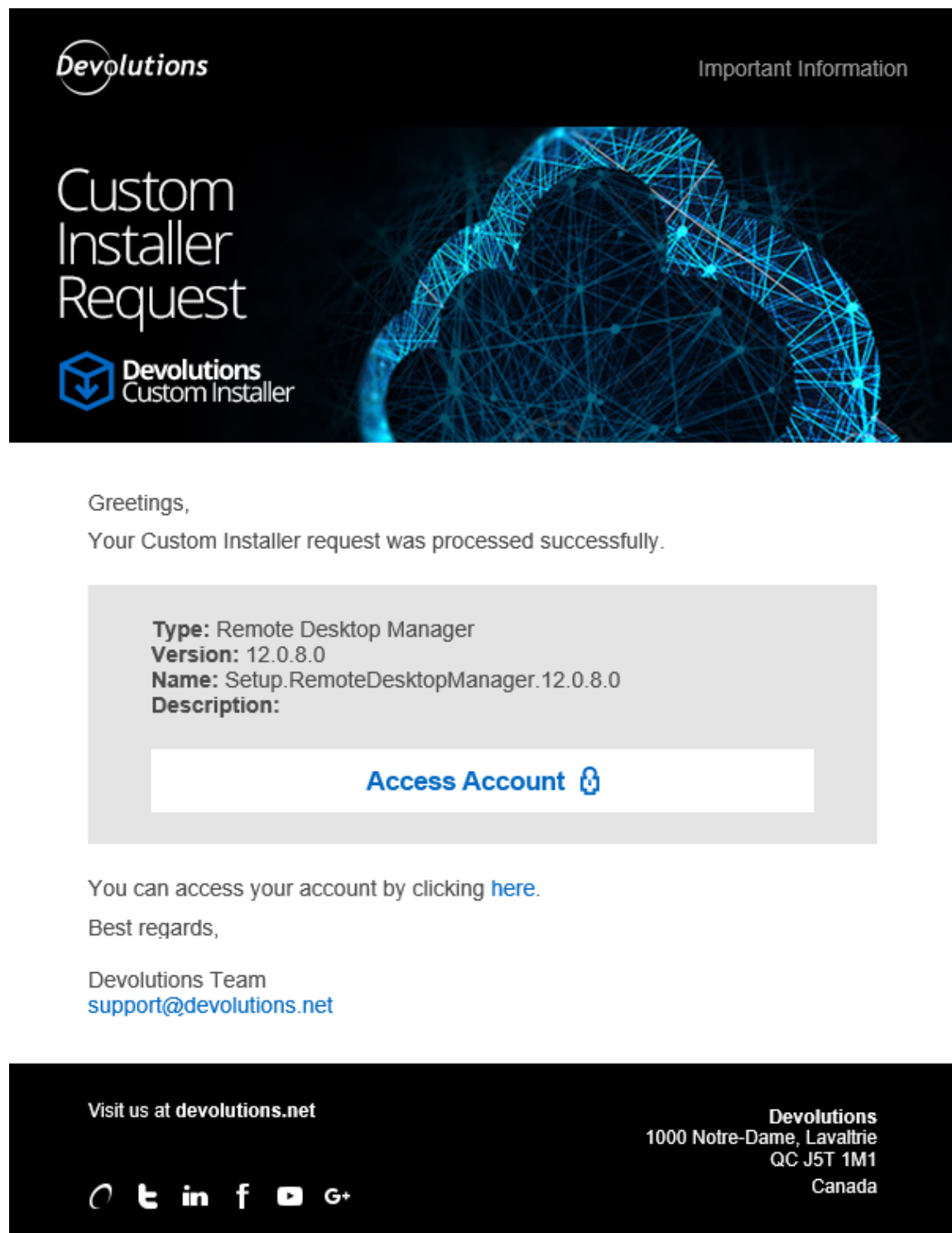


setup.exe is in fact what is called a **bootstrapper**, it will ensure the installer runs with the required privileges. Use the msi only if you are sure the installer will run with all rights and process elevation.

## DOWNLOADING AN INSTALLATION PACKAGE

Upon completion you will receive a confirmation email.



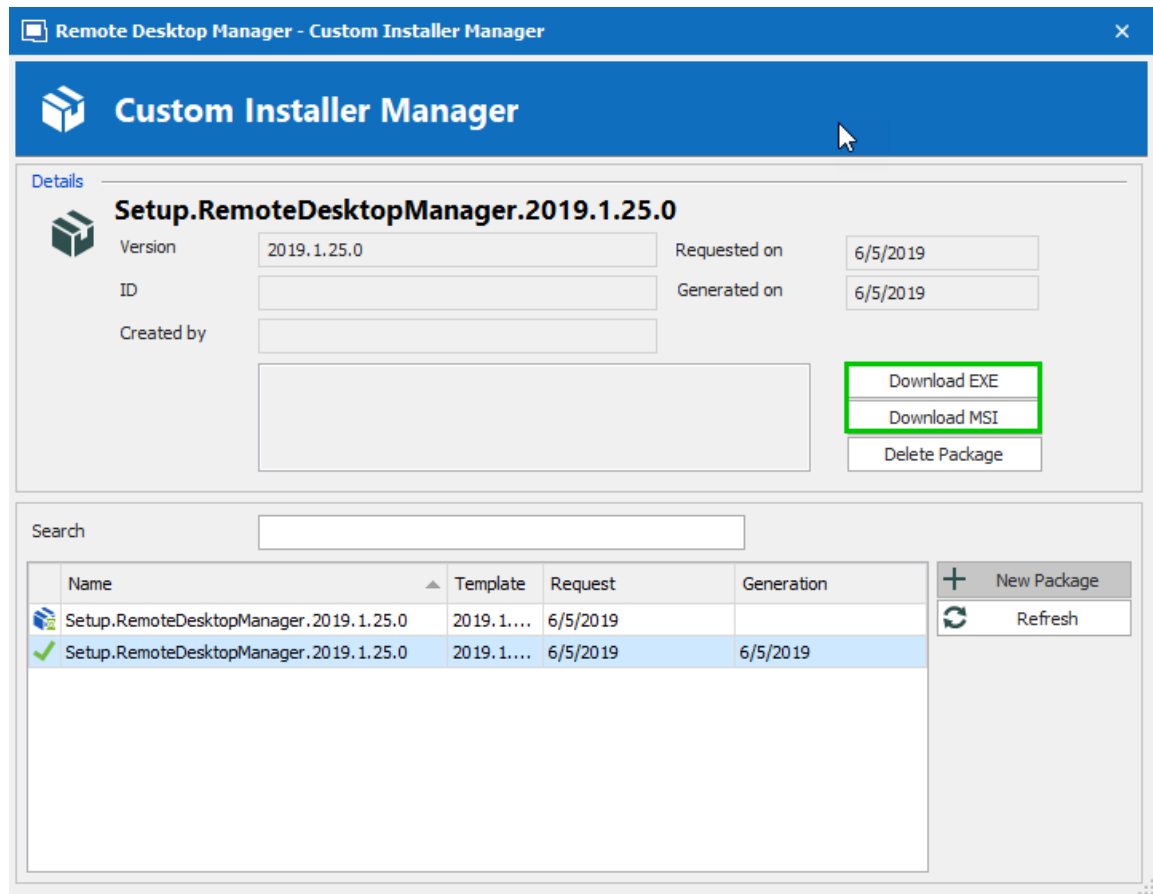


*Email Confirmation - Custom Installer Processed*

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

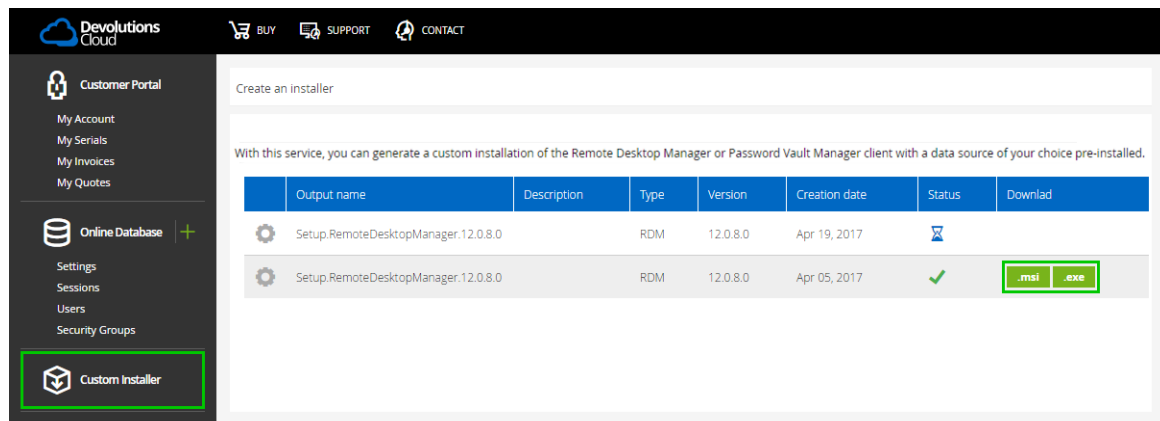
From the **Custom Installer Manager**, click on Download EXE or Download MSI.



*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** or **.exe** 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](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.



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.



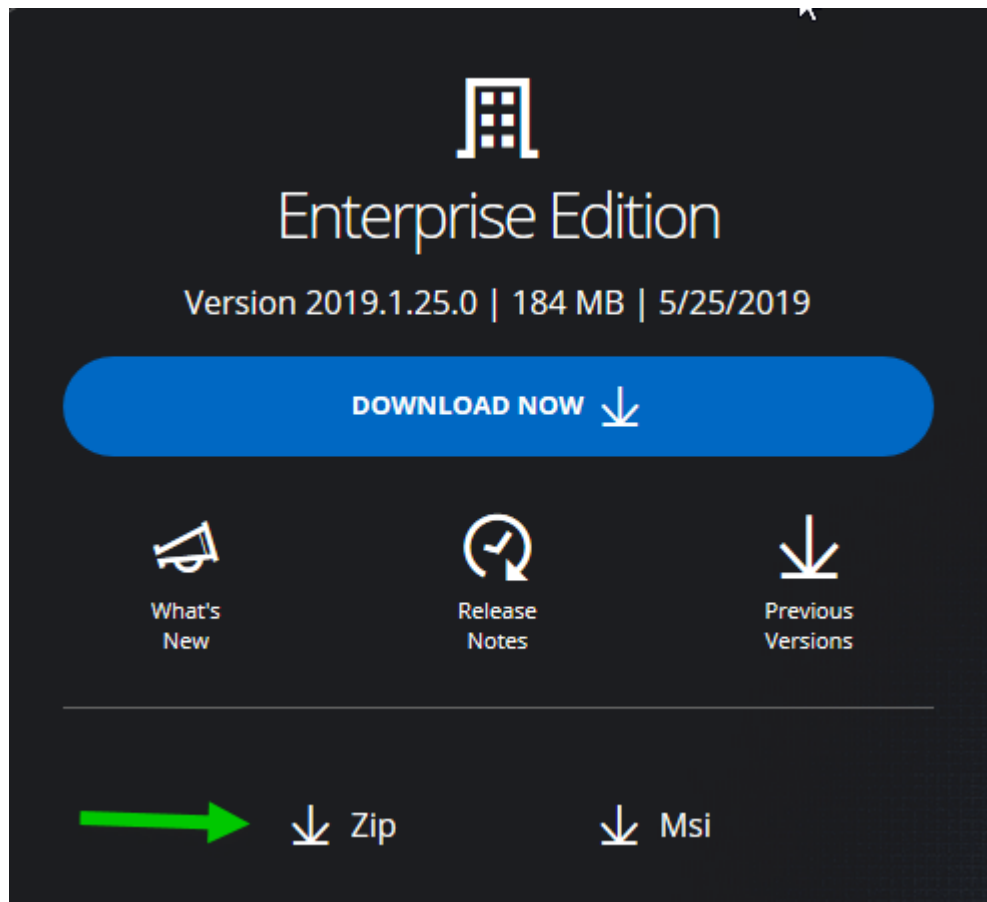
Remote Desktop Manager stores the offline cache in your Windows profile by default. If you are using an Advanced Data Source and plan to use the offline mode, use the Options in the Advanced category to have the offline cached stored in the application folder instead.



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

## PROCEDURE

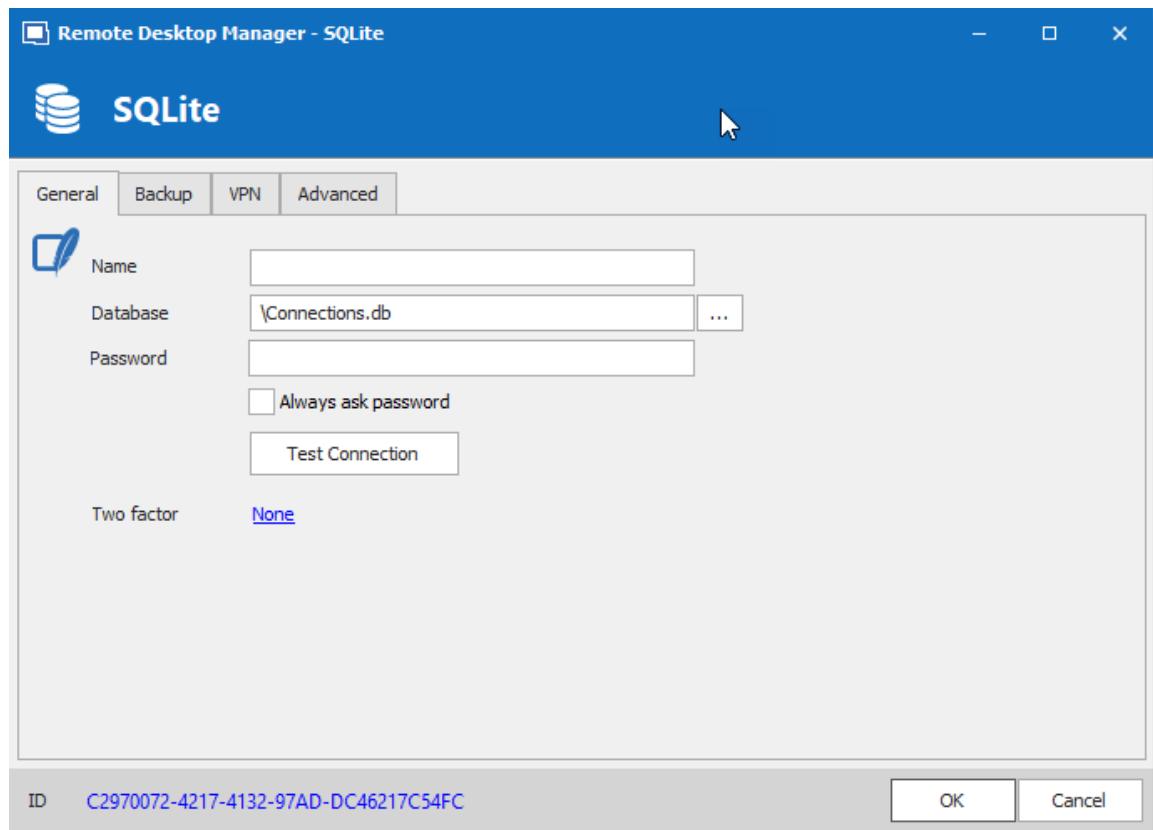
1. Download the "Zip" package of Remote Desktop Manager.



*Zip File Download*

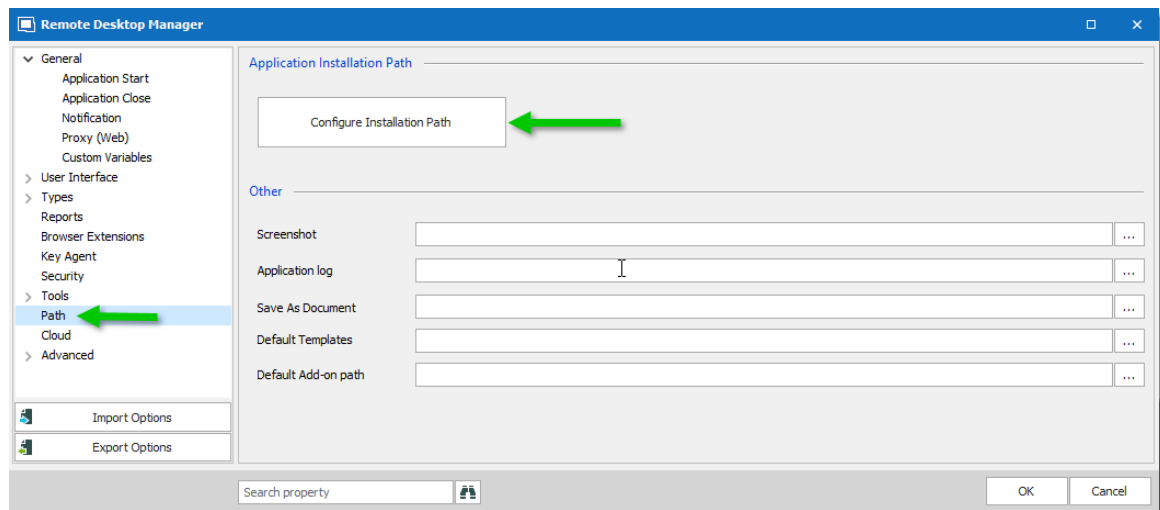
2. Create a RemoteDesktopManager folder on your portable device.
3. In the installation folder created in step 2, create two folders:
  - 3.1. A **config** folder.
  - 3.2. A **data** folder.
  - 3.3. A **tools** folder (optional, only if you intend to use external tools like Filezilla).

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`

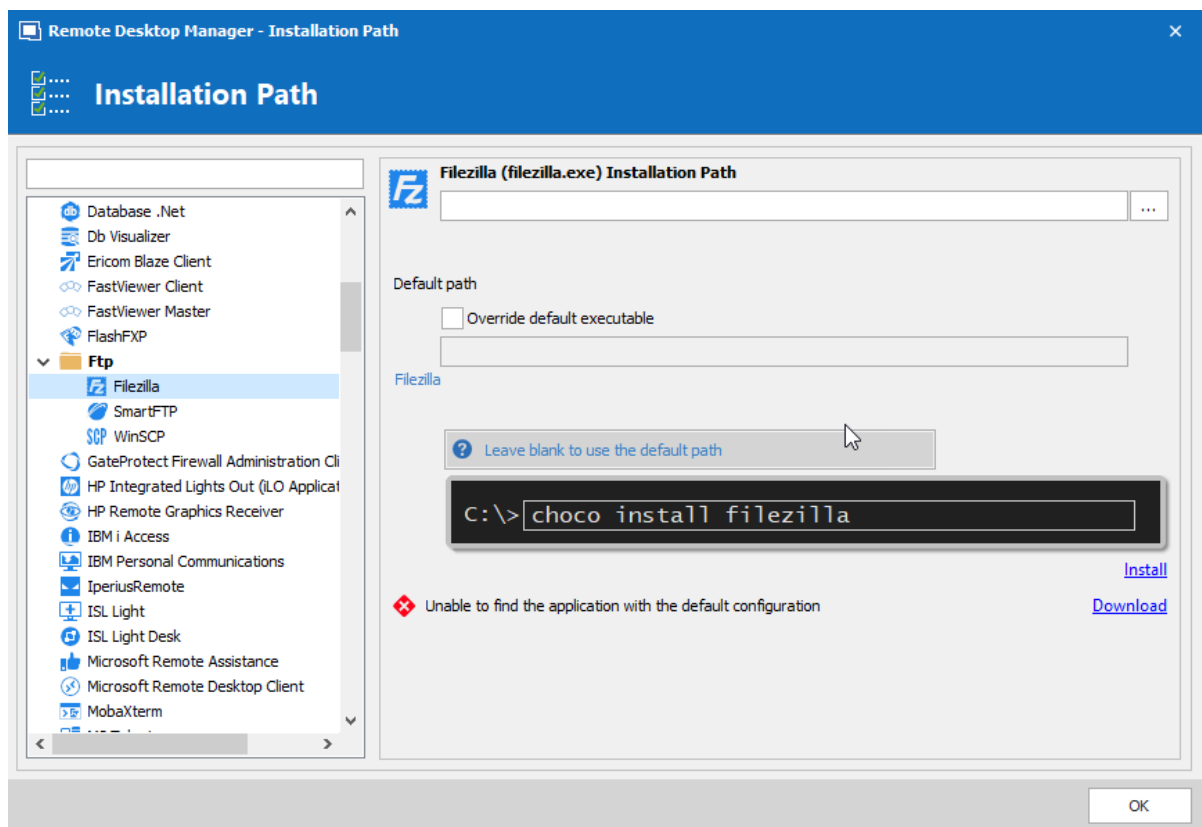


SQLite Data Source

10. 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.



*Options - Path - Configure Installation Path*



*Filezilla Installation Path*

11. 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](#) topic to properly register your version. If you decide not to register at the end of the 30 days 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 days trial to try Remote Desktop Manager - Enterprise Edition with all its features. For more information, please consult the [Trial Request](#) Topic.

### REMOTE DESKTOP MANAGER FREE EDITION

Remote Desktop Manager Free Edition is similar to the Enterprise edition. Remote Desktop Manager Free Edition must be registered following the 30 days trial period to ensure continued use. Registration is free, please refer to the [Free Edition](#) topic.

### DEVOLUTIONS SERVER

Consult [Create Devolutions Server Instance](#) to register a new Devolutions Server instance.

If you want to activate your renewal license key, consult [How To Activate Your Renewal Subscription for Devolutions Server](#).

### DEVOLUTIONS ONLINE DATABASE

Please consult [Online Database Registration](#) to register a new Devolutions Online Database.



### 3.1.6.1 Enterprise Edition

## DESCRIPTION

Remote Desktop Manager can be registered by [manually providing a license serial](#) or with a [license serial stored in a data source](#).

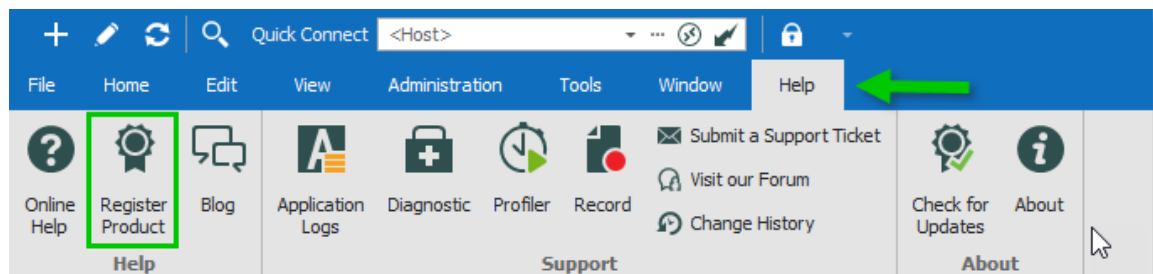


It is possible to [request a trial](#) to try Remote Desktop Manager for 30 days. If you decide not to register the application with an Enterprise Edition license serial at the end of the 30 days period, your data will not be altered or erased, and you will have full access to it once you provide a license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

## MANUAL REGISTRATION

Remote Desktop Manager Enterprise license serials are delivered by email.

1. Locate the email and copy the serial.
2. Open **Help – Register Product**.



*Help - Register Product*

3. Enter the Name, Email, and Serial number from the email, then click **OK**.

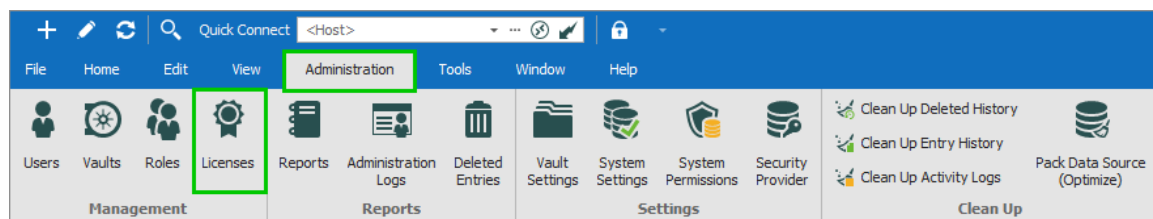
Register Enterprise Edition

## REGISTRATION FROM THE DATA SOURCE

When the license serial is stored in the [Data Source Settings \(System Settings\)](#) of 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.

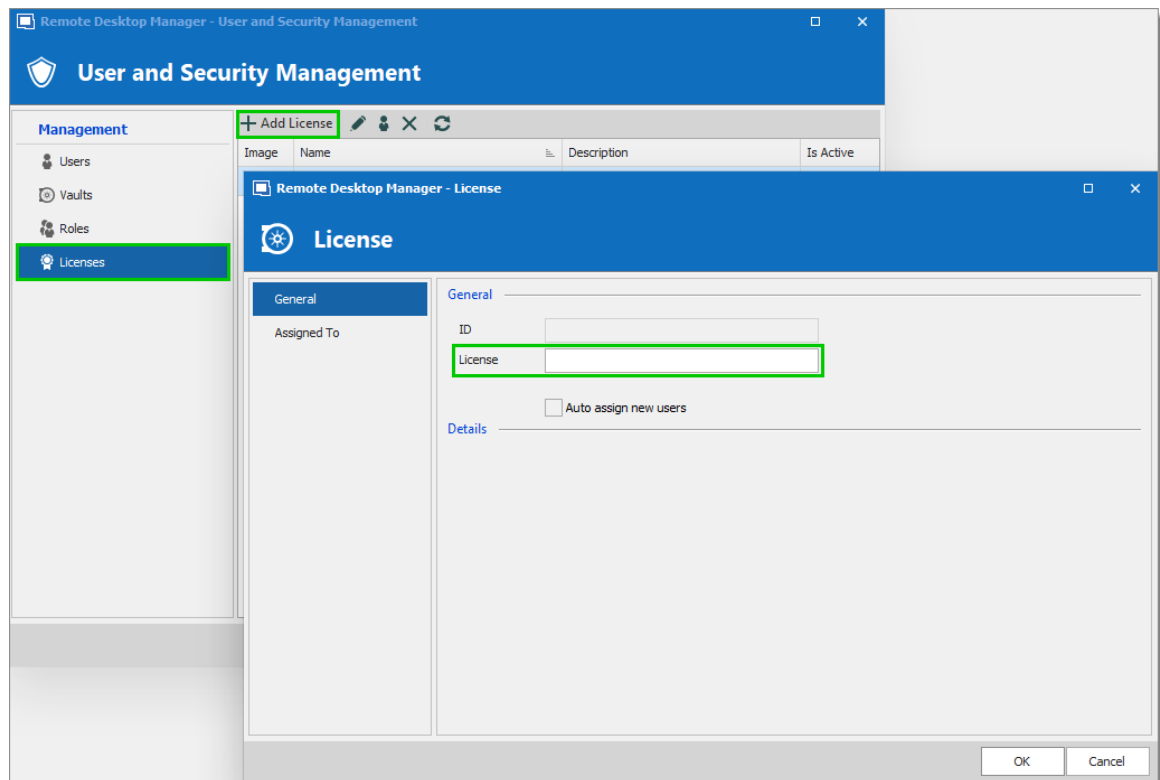
## FOR ADMINISTRATORS

To add a license serial, navigate to **Administration - Licenses**.



Administration - Licenses

In **Licenses**, click on **Add License**. Enter the license serial and click **OK**.



*User and Security Management - Add License*

#### 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.

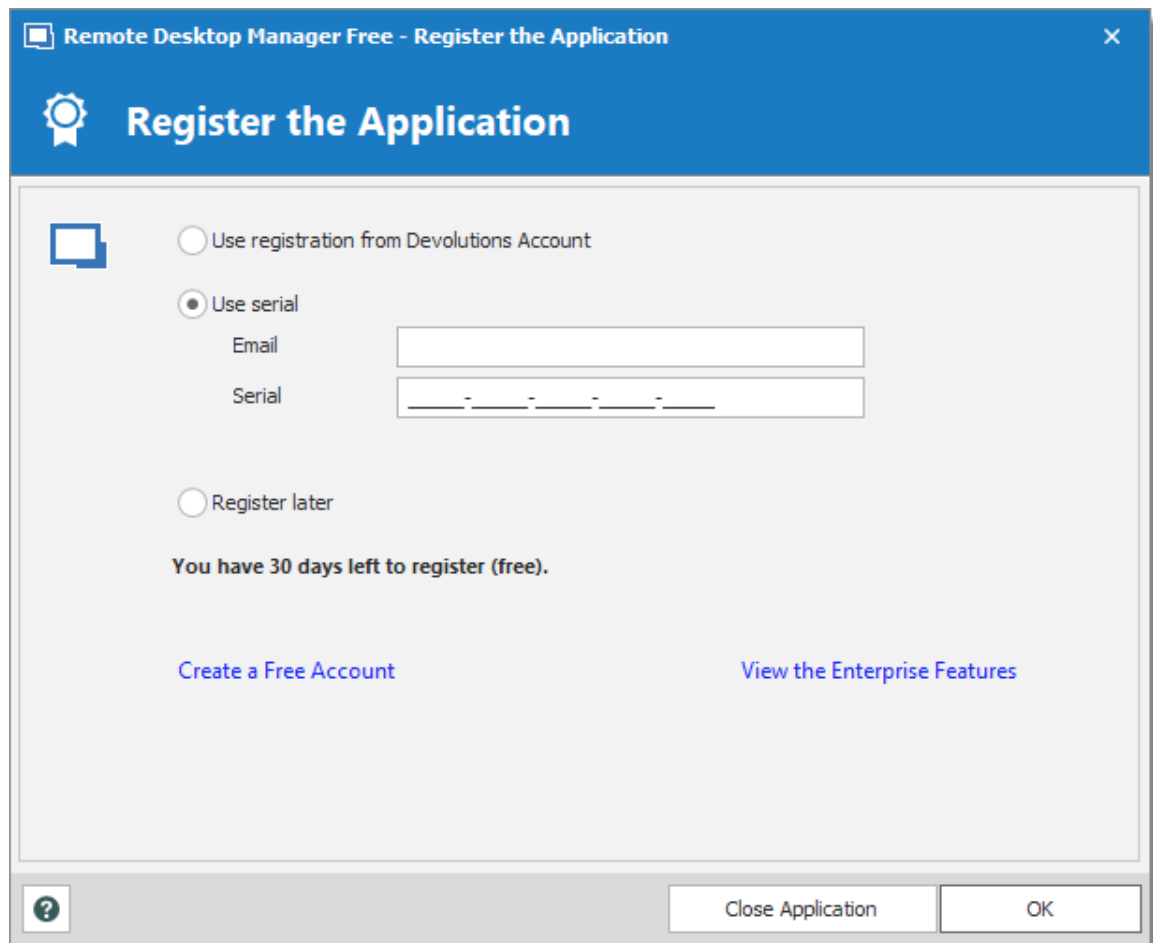
You need to renew your subscription agreement upon expiry. If you don't renew your subscription, access to your data will be limited.

### 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*

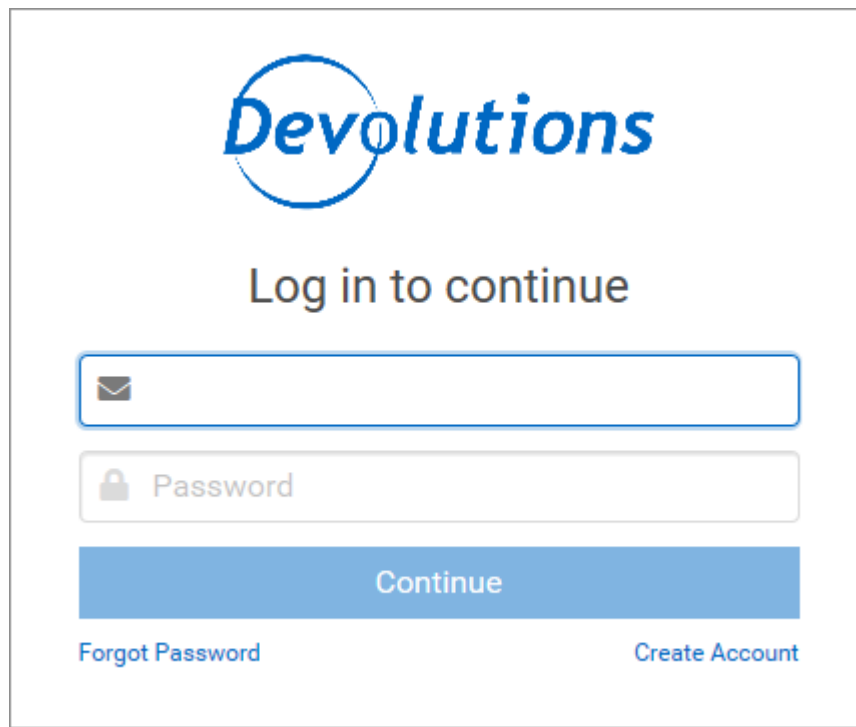
## USE REGISTRATION FROM DEVOLUTIONS ACCOUNT

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**.



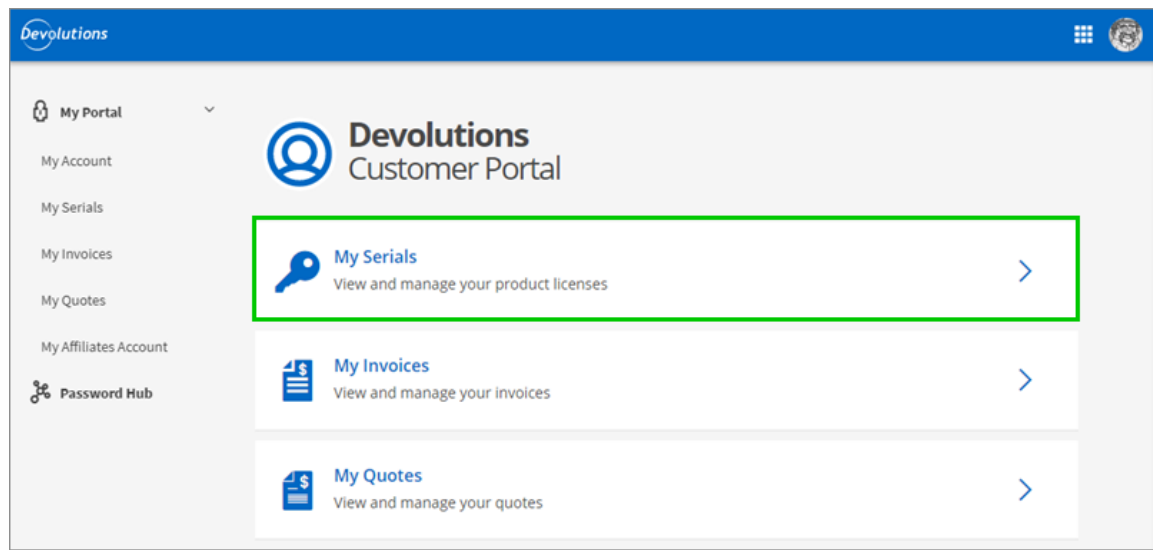
*Devolutions Account Login*

The license serial will be retrieved automatically.

## REGISTER THE FREE EDITION WITHOUT AN INTERNET CONNECTION

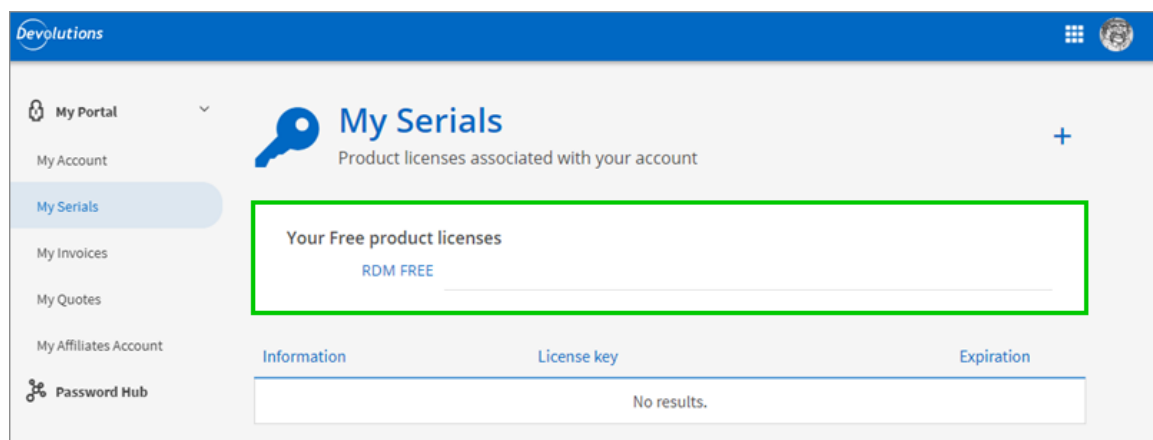
In the event that you need to register the application without an internet connection, the information must be entered manually. You will need the license serial from your [Customer Portal](#).

Log in to [Customer Portal](#) and click on **My Serials**.



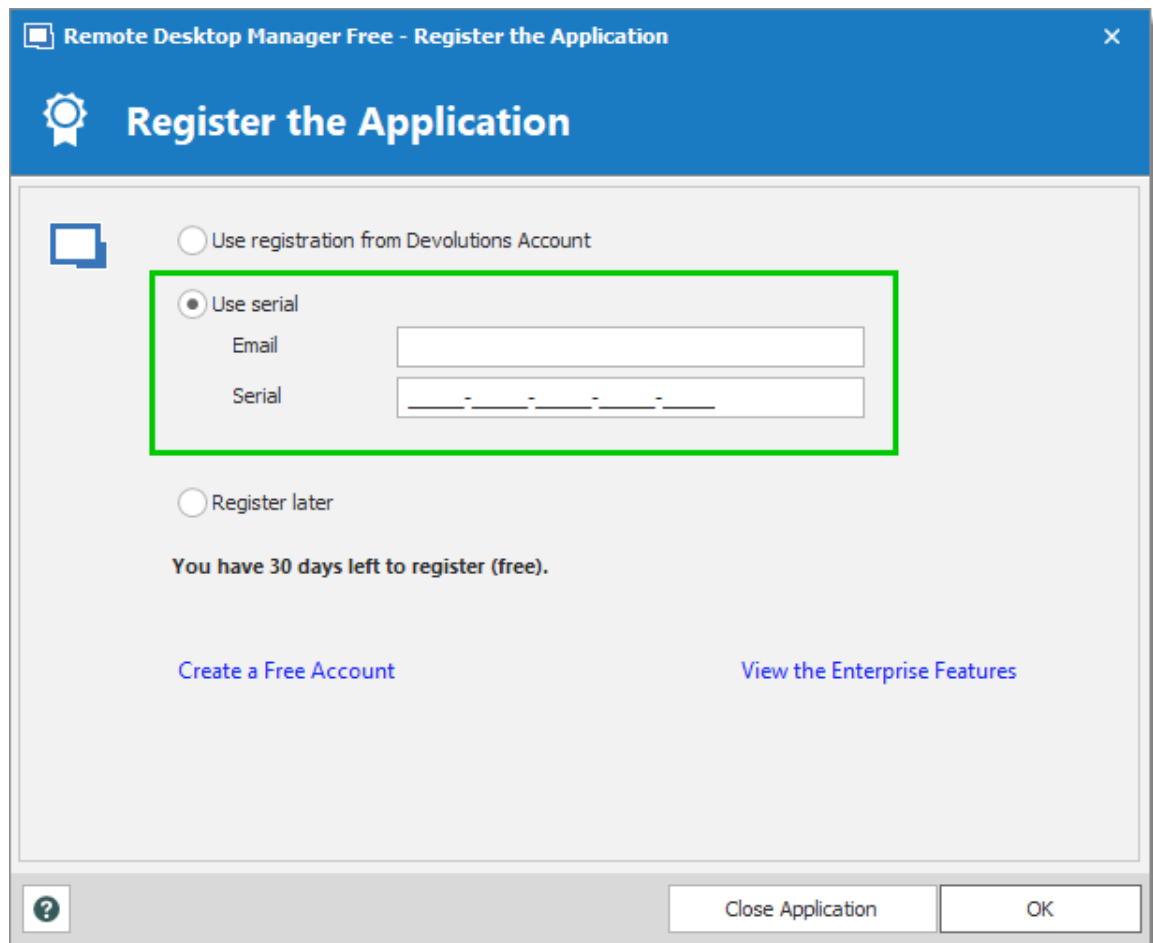
*Customer Portal - My Serials*

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*

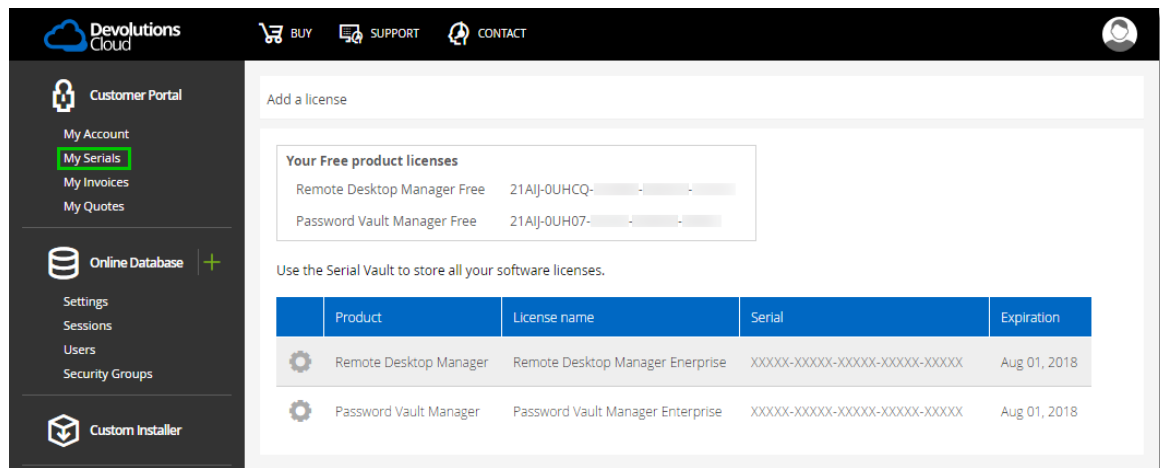
### 3.1.6.3 Register from Devolutions Portal

## DESCRIPTION

It is possible to register the product with a license serial stored in a Devolutions Customer Portal.

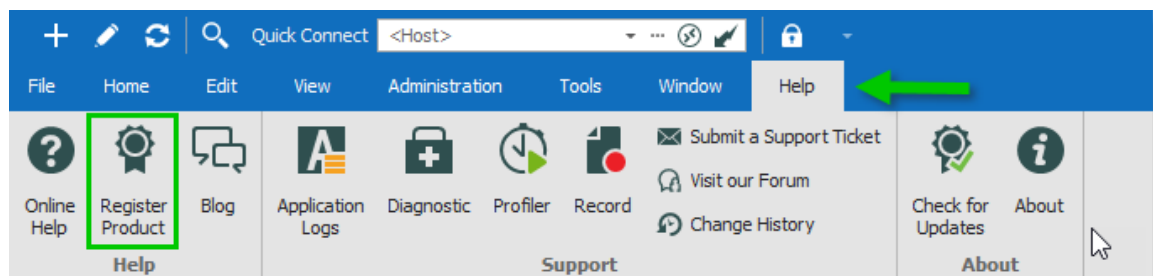
When creating a Devolutions Account a free license serial is provided for the free edition of Remote Desktop Manager. License serials purchased for the enterprise edition can be stored in the **My Serials** section of the Devolutions Customer Portal.





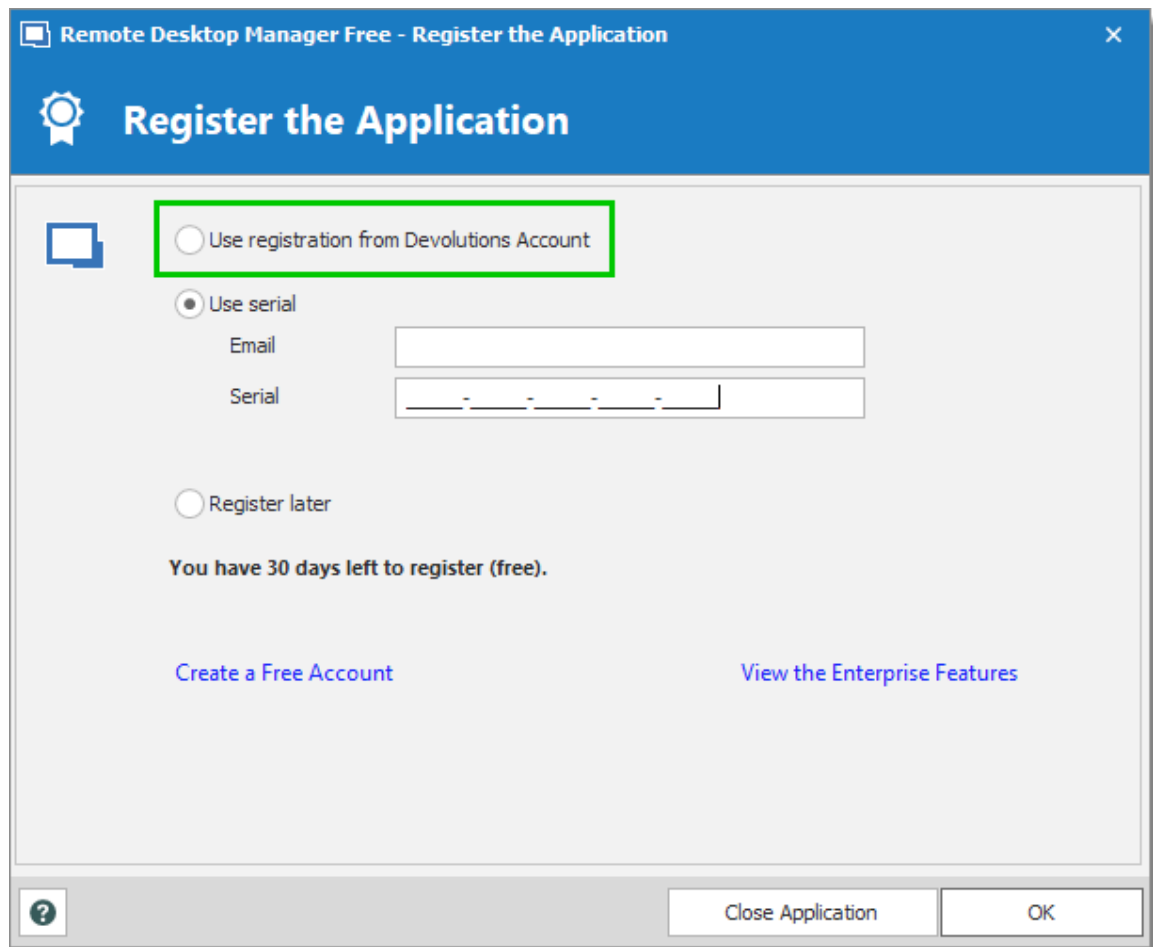
*Devolutions Customer Portal - My Serials*

1. To register the product, navigate to **Help – Register Product**.



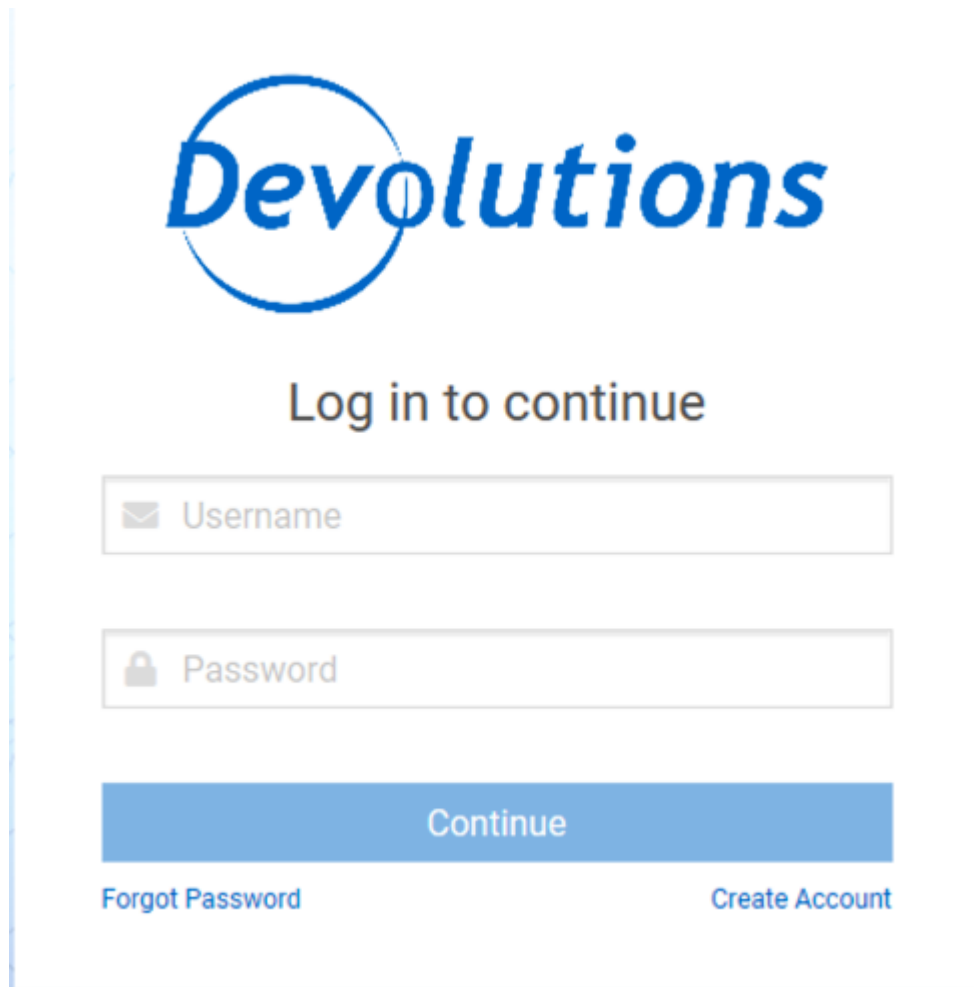
*Register product*

2. In the **Select your Application Edition** window, select **Use registration from Devolutions Account**.



*Select the Registration*

3. Enter the credentials of the Devolutions Account, then click **Connect**.

The image shows a login window for Devolutions. At the top is the Devolutions logo, which consists of the word "Devolutions" in a blue, italicized sans-serif font, with a blue circle around the "o". Below the logo is the text "Log in to continue" in a dark grey sans-serif font. There are two input fields: the first is labeled "Username" with an envelope icon on the left, and the second is labeled "Password" with a lock icon on the left. Below these fields is a large blue button with the text "Continue" in white. At the bottom left is a link "Forgot Password" and at the bottom right is a link "Create Account", both in blue text.

*Prompt for Devolutions Account credentials*

#### 3.1.6.4 Trial Request

### DESCRIPTION

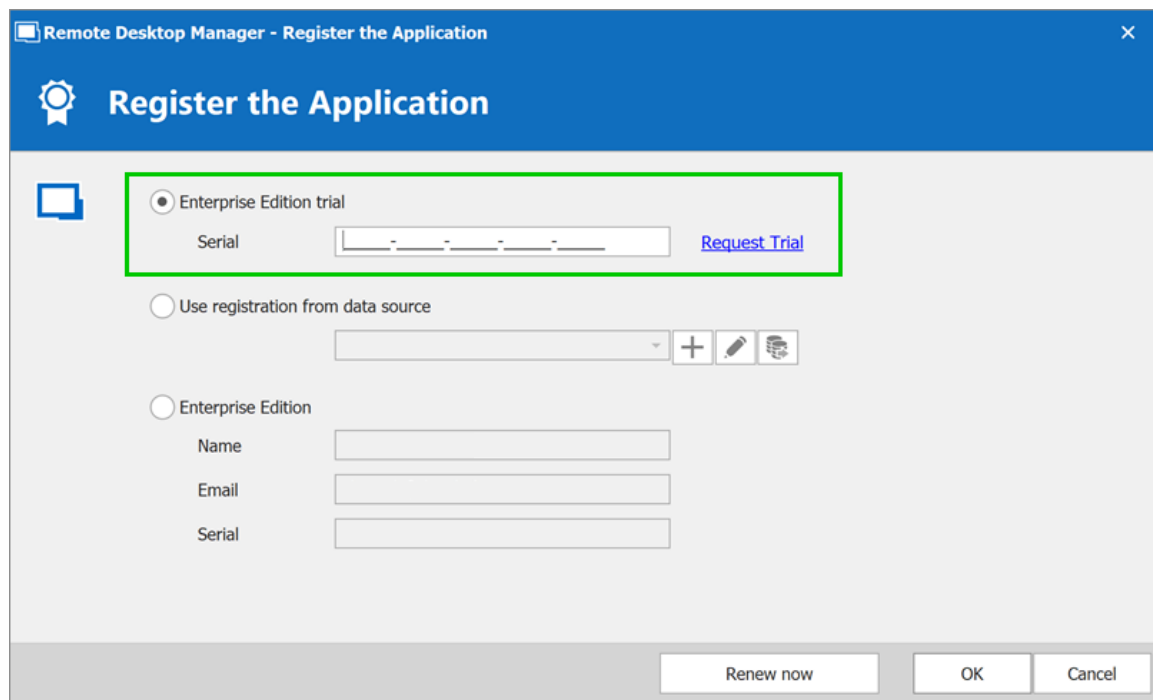
When launching Remote Desktop Manager for the first time, the application registration window is displayed. If you are not ready to buy Remote Desktop Manager, you must request a trial to use the application. The trial is valid for 30 day, after which the application cannot be used unless a valid Remote 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. Copy the trial license serial that you will receive in a confirmation email from Devolutions.
3. In Remote Desktop Manager navigate to **Help – Register Product**, select **Enterprise Edition trial** and paste the serial from your confirmation email.
4. 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 severely 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.



The **Devolutions Web Login (DWL)** was created for a normal desktop environment. It uses Inter-process communication (IPC) with the client application. Using it on a remote desktop server introduces a level of risk that may be unacceptable for corporate users.

Safe usage of **DWL** requires a manual configuration of both **RDM** and **DWL** on each user profiles. For more information about the subject visit our [Secure Devolutions Web Login](#) topic.

## 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%)

3. 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*



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**.

4. Move that file in the installation folder of Remote Desktop Manager, if you have used the default installation settings, it is under %ProgramFiles(x86)%\Devolutions\RemoteDesktopManager.

## 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.

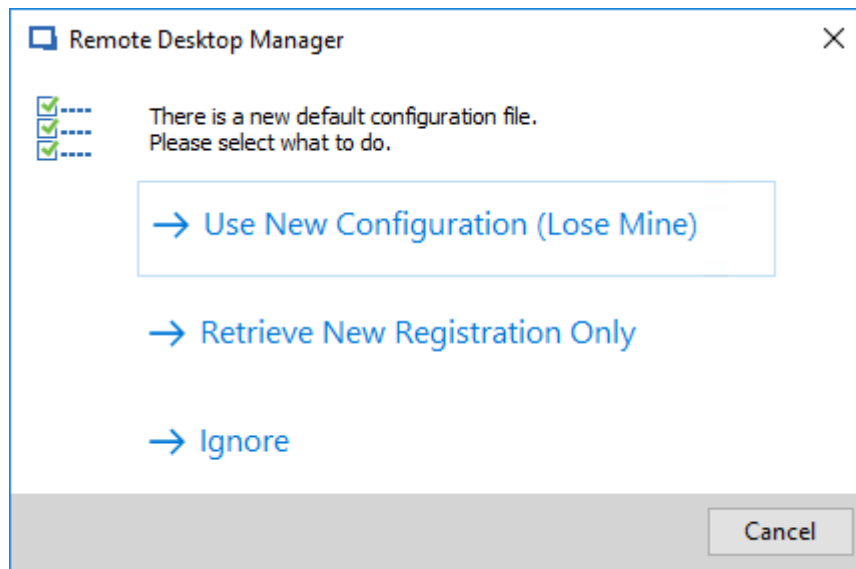


If the user chooses to ignore the new configuration file when presented with the dialog below, he will not be presented with the choice until the date/time of the *default.cfg* file has changed.



If the main concern is deploying a new license key, and you are using one of the [Advanced Data Sources](#), you should rather use the [Data source settings \(System Settings\) - Serial](#) feature.

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 your 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

## INSTRUCTIONS

Remote Desktop Manager doesn't 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, Remote Desktop Manager can be uninstalled easily.

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.

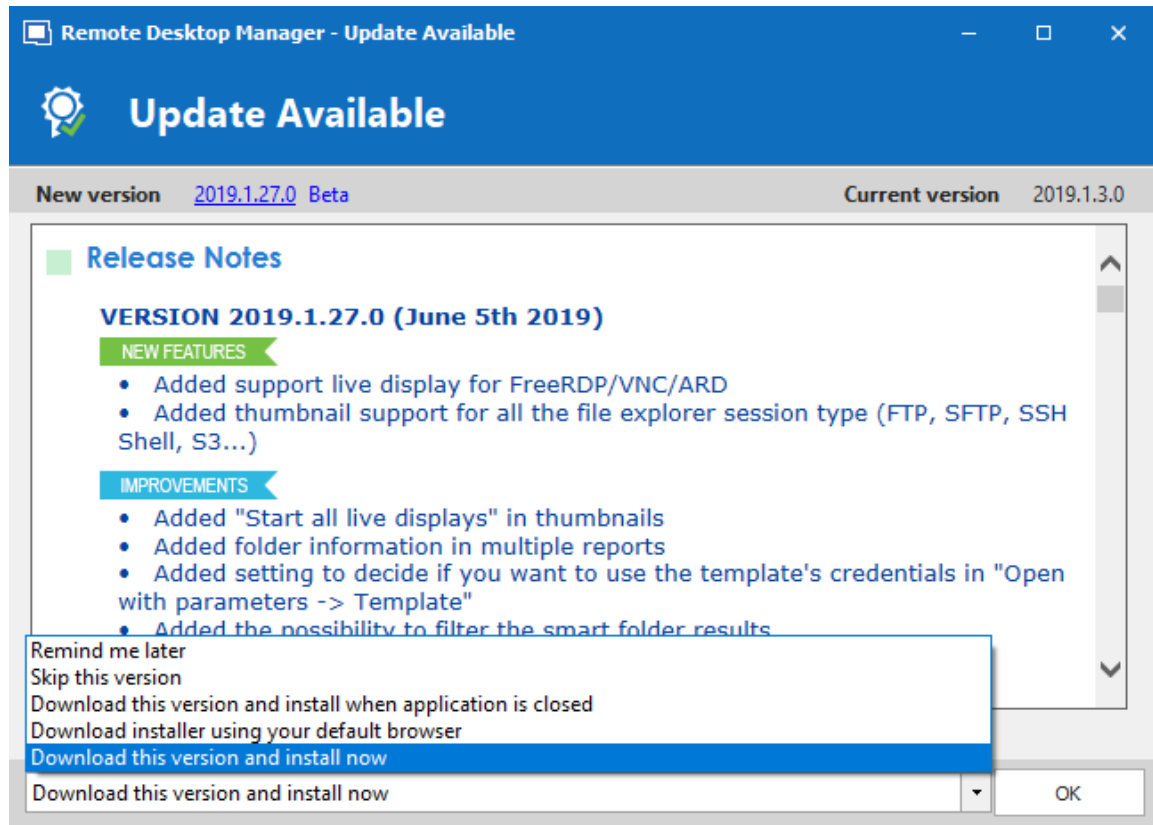
The application configuration files are saved in "%LocalAppData%\Devolutions\RemoteDesktopManager" or "%AppData%\Devolutions\RemoteDesktopManager" by default. It's possible that you may want to delete this folder for a complete uninstall.



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.



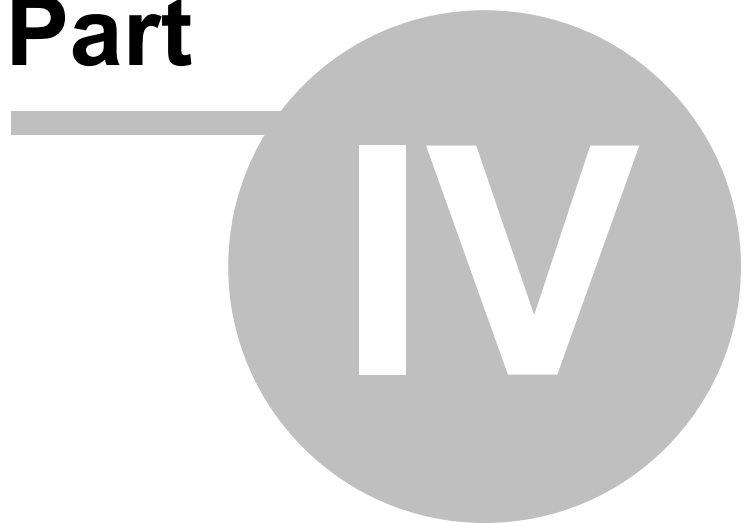
*Update*

OPTION	DESCRIPTION
<b>Remind me later</b>	Remind to update the next time the application is opened.
<b>Skip this version</b>	Do not update the application with this version.
<b>Download this version and install when the application is closed</b>	Download the version and wait for the application to be closed before installing.

OPTION	DESCRIPTION
<b>Download installer using your default browser</b>	Download the installer externally using your default web browser.
<b>Download this version and install now</b>	Immediately download the new version and install it.

# User Interface

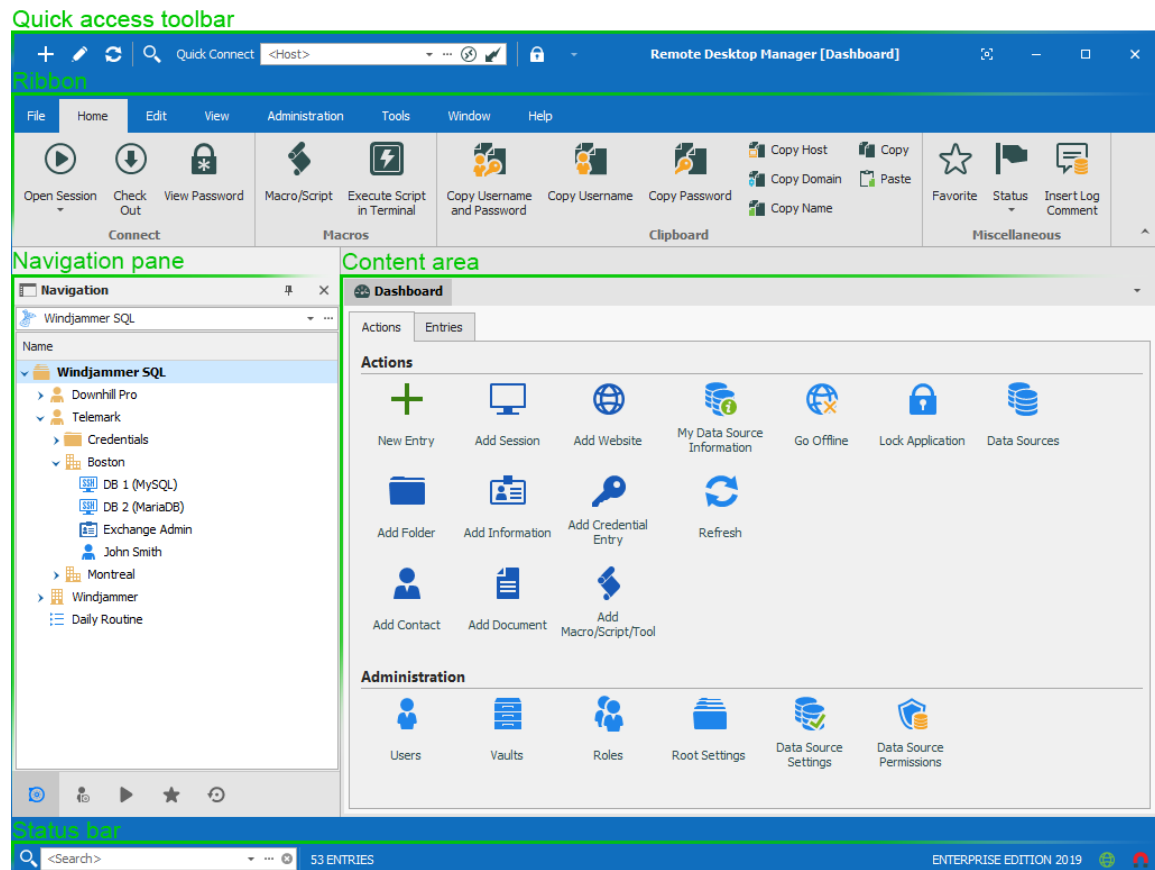
**Part**



## 4 User Interface

### 4.1 Main Screen

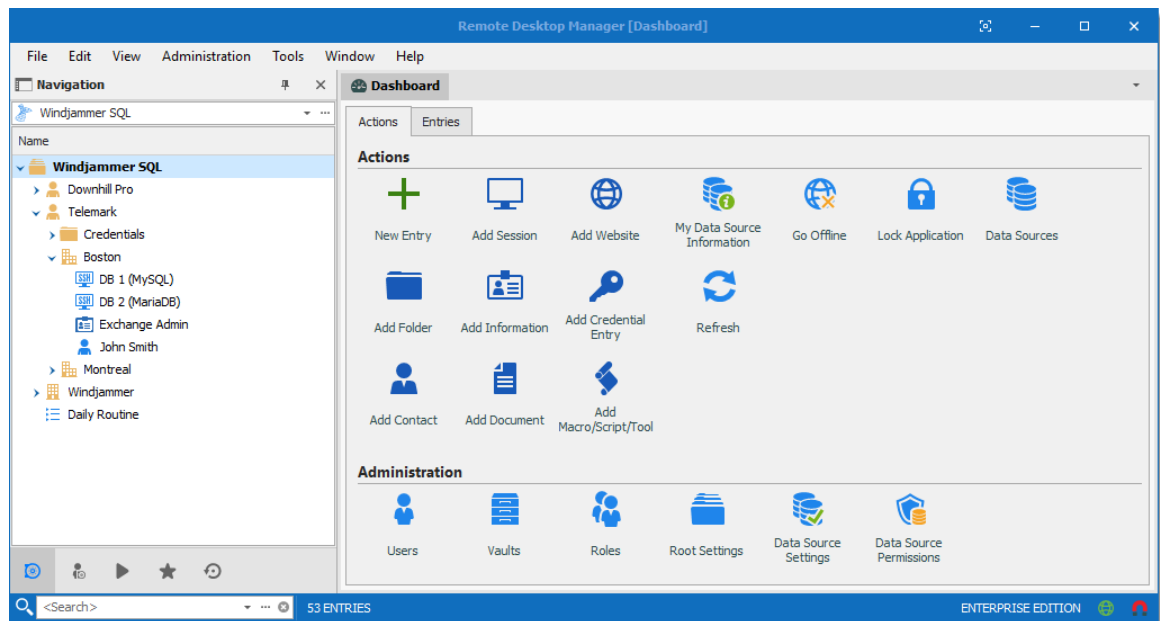
Illustrated below is the default Remote Desktop Manager main screen. Go to **File – Options – User Interface** to change the current style. We have various settings for you to customize your experience, such as different themes, shortcuts and more!



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*

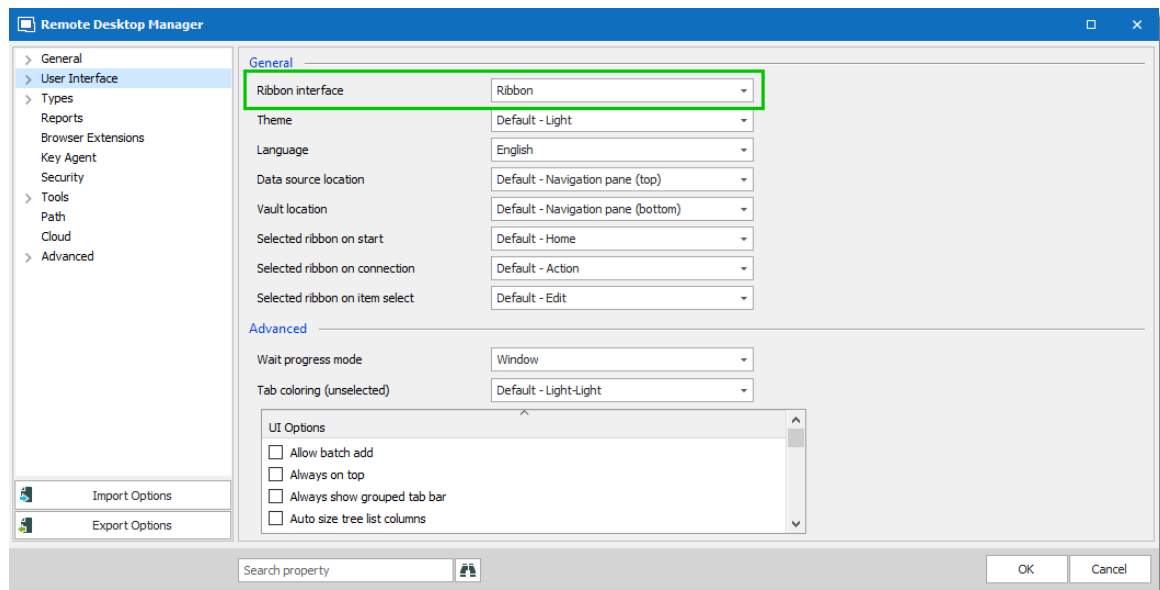
## 4.2 Style

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 **Ribbon interface**.

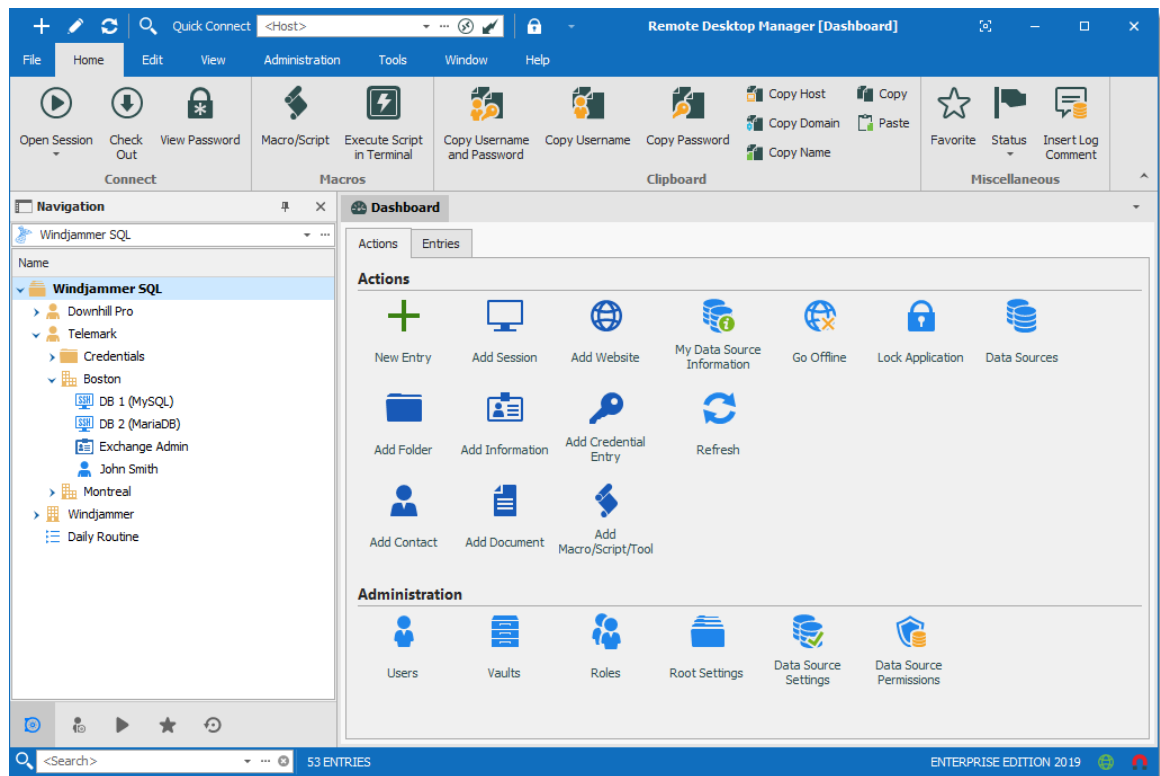


*Options - User Interface*

## EXISTING STYLES

### RIBBON

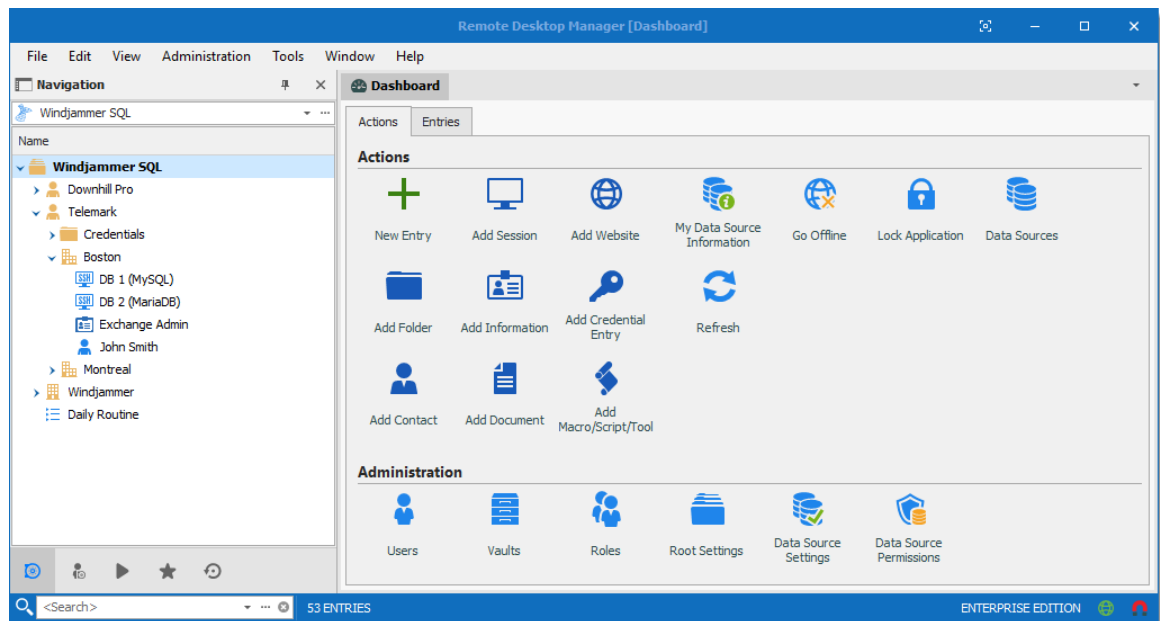
The latest style sports a ribbon. Icons and text makes it easy to explore features.

*Ribbon User Interface*

## MENU

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

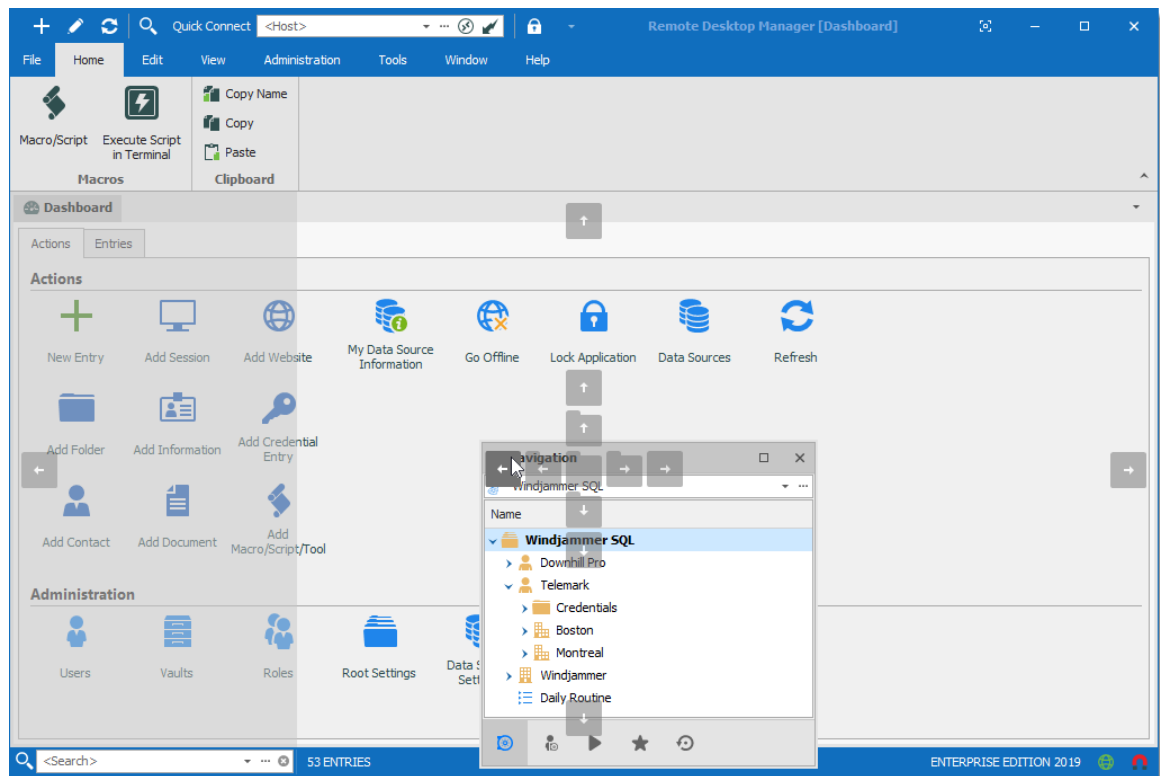




*Default User Interface*

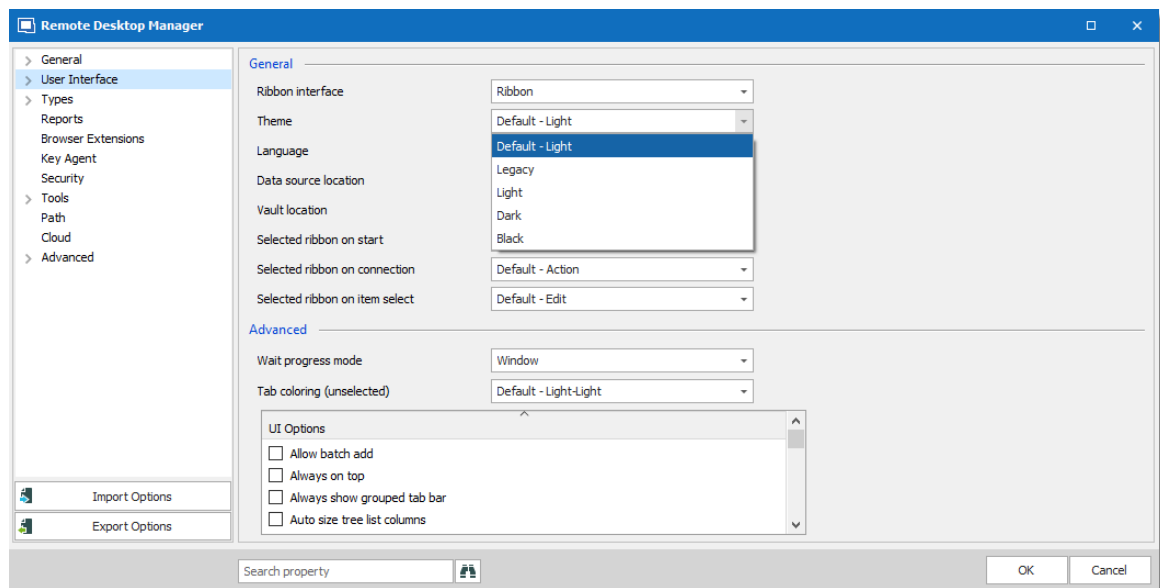
## CUSTOMIZING YOUR UI

Customizable styles (Default Ribbon and Default Menu) have dockable areas that can be rearranged to your liking. Simply left-clicking then dragging the sub-components will result in drop zones appearing. This allows you to drop the sub component where you choose, even outside of the main form if you'd like.



## 4.3 Theme

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

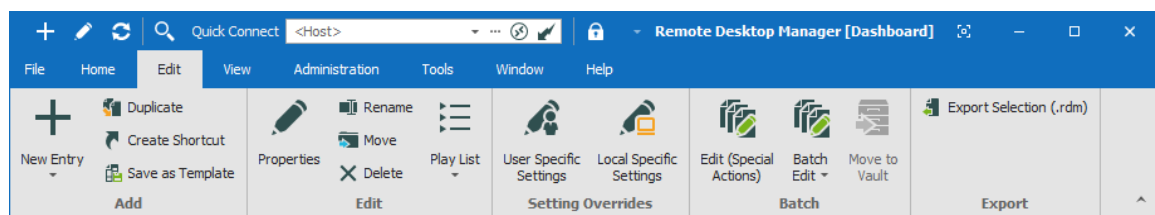


*User Interface - Theme*

OPTION	DESCRIPTION
<b>Default - Light</b>	Use the default theme, which is the Light theme.
<b>Legacy</b>	Use the old look of Remote Desktop Manager (version 7 of RDM)
<b>Light</b>	Use a clear theme with tones of white, gray, and blue.
<b>Dark</b>	Use a dark theme with tone of gray and black.
<b>Black</b>	Use the darkest theme, mainly with tones of black.

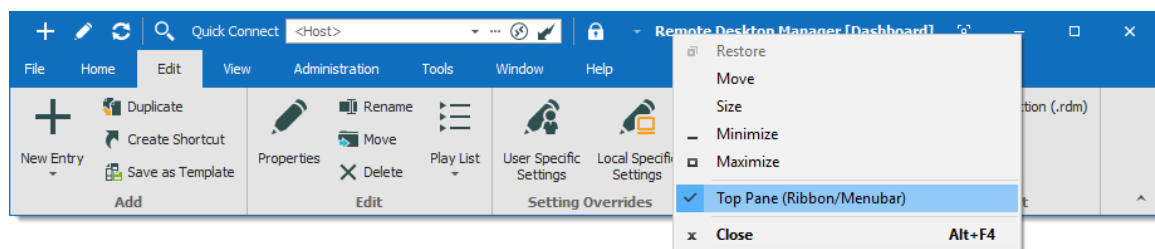
## 4.4 Top Pane

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

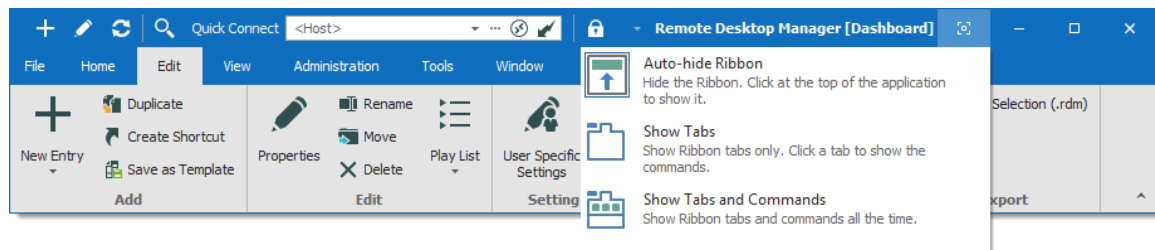


*Remote Desktop Manager top pane*

It can be hidden to maximize the work area.

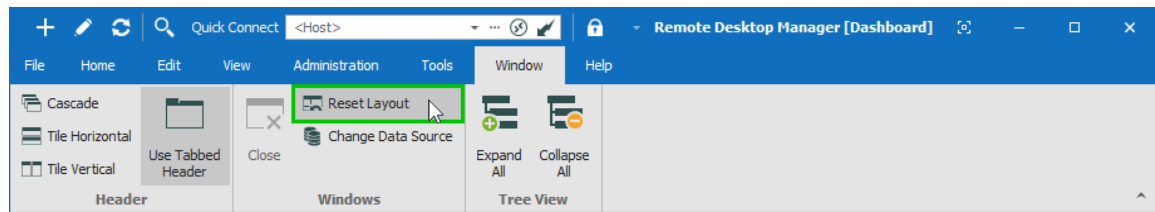


*Hide the top pane completely*



*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**.

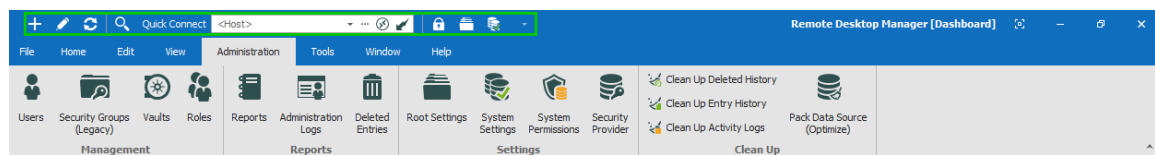


*Windows – Reset layout*

#### 4.4.1 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.



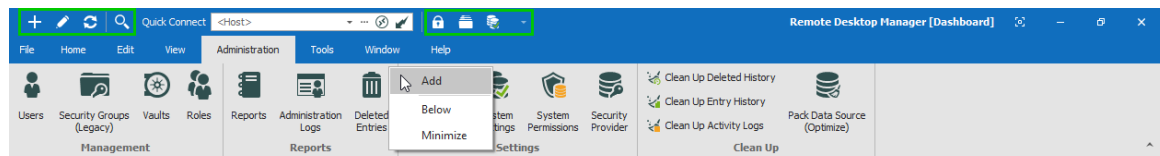
*Quick Access Toolbar*







**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.

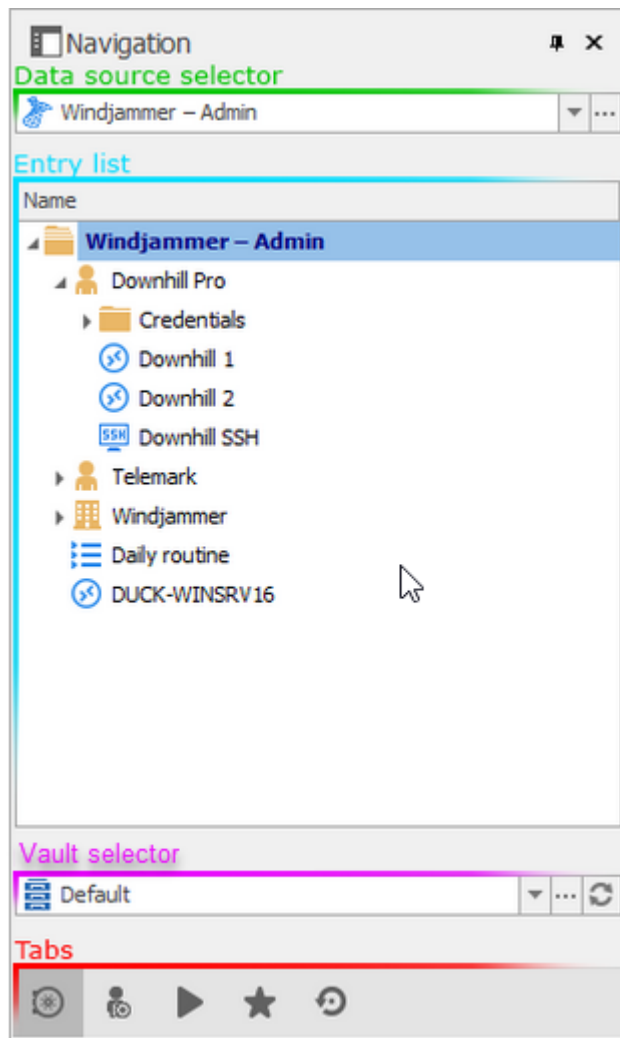
## LOCK APPLICATION COMMAND

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.

## 4.5 Navigation Pane

### DESCRIPTION

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



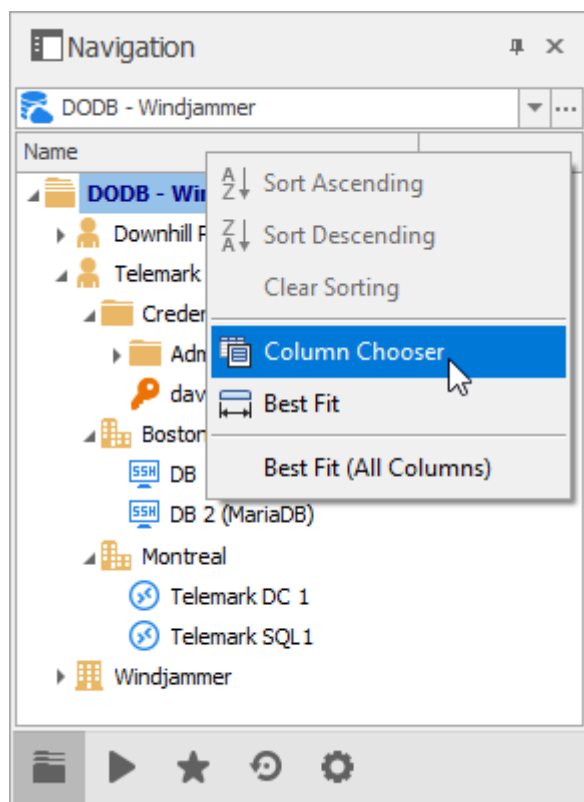
*Navigation Pane*

ELEMENT	DESCRIPTION
<b>Data source selector</b>	Allows to switch to another configured data source.

ELEMENT	DESCRIPTION
<b>Entry list</b>	Displays the content of the current data source, depending on the selected tab. It allows to select entries and perform action on them.
<b>Vault selector</b>	Allows to switch to another configured Vault in the data source.
<b>Tabs</b>	Allows to switch to different views of the entry list, such as the <a href="#">Favorite entries</a> or the <a href="#">Opened sessions</a> .

## 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:

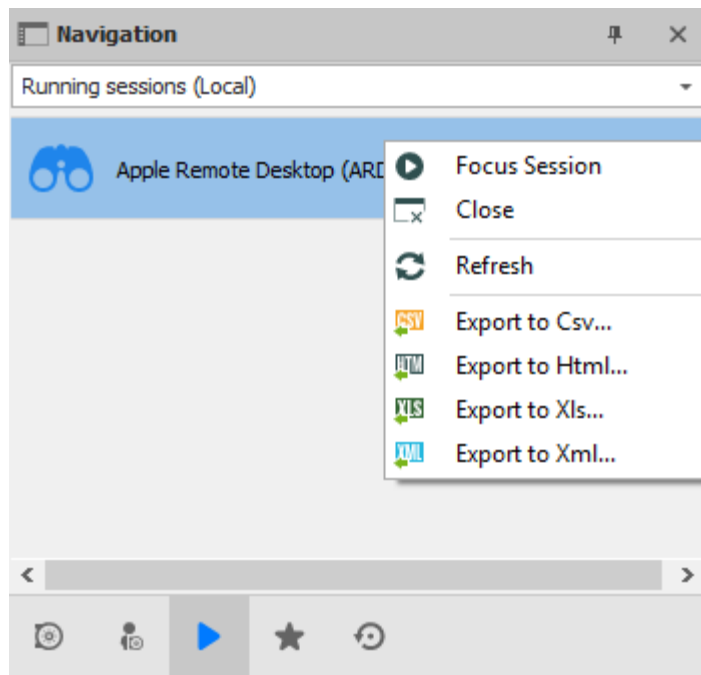
- Vault
- [User Vault](#)
- [Opened Sessions](#)
- [Favorite Entries](#)
- [Most Recently Used Entries](#)

#### 4.5.1 Opened Sessions

### DESCRIPTION

The **Opened Sessions** tab shows currently running sessions by type, and for the local machine only. 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.

### LOCAL SESSIONS

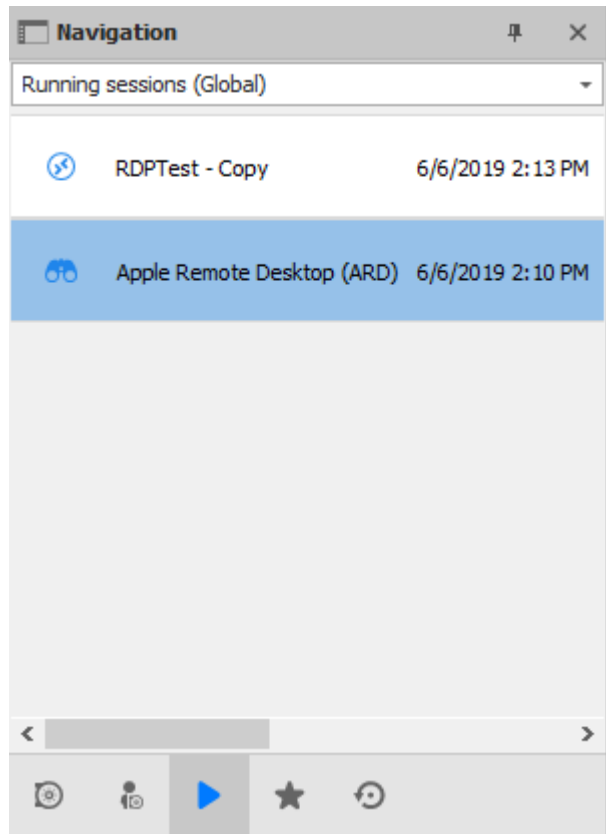


*Local Opened Sessions*

### GLOBAL SESSIONS



With the SQL Server and Devolutions Online Database data sources, you can monitor currently running sessions, provided that they have been opened within Remote Desktop Manager.



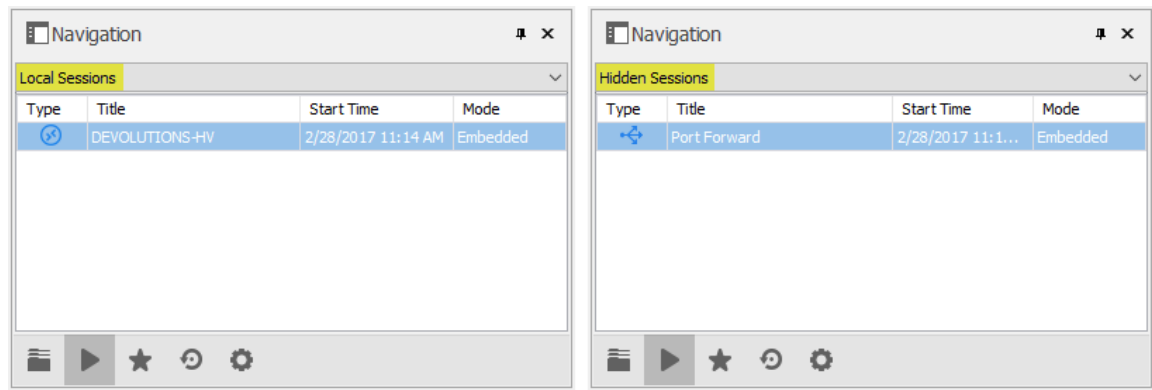
*Global Opened Sessions*

For many reasons beyond our control, it's possible for a session to be terminated without Remote Desktop Manager knowing that this has taken place. This can happen, for example, if Remote Desktop Manager isn't running when another application ends. As a result, 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 SESSIONS

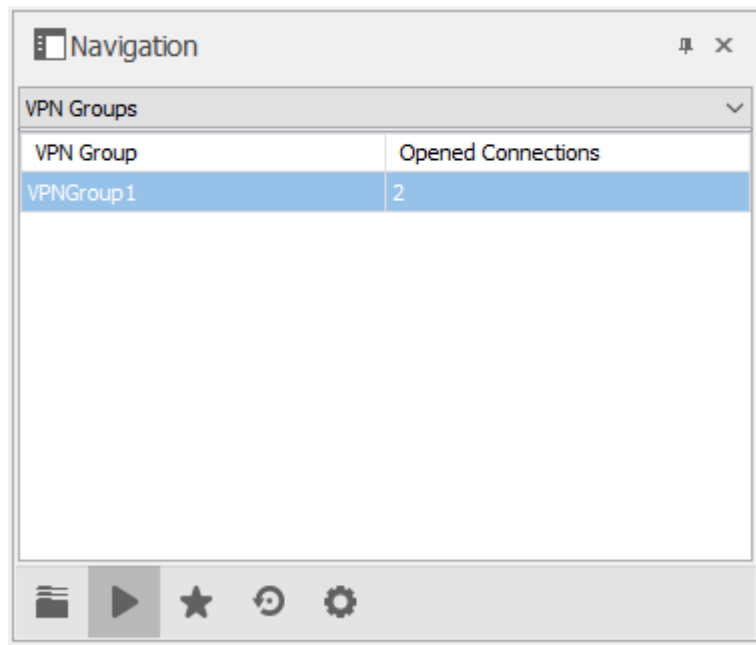
Some sessions, like **SSH Port Forward**, can be hidden from the dashboard when the connection is established. When these sessions are hidden, they are not displayed in the **Local Sessions**. Select **Hidden Sessions** from the combo box above the entry list to display hidden sessions only.



*Local Sessions Versus Hidden Sessions*

## VPN GROUPS

Sessions can be configured to use a VPN Group. When multiple session are using the same VPN group, it will appear in this section with the count of opened connections using this VPN group.



*VPN Groups*

## NOTES

- Remote Desktop Manager tries to detect opened sessions even if they weren't launched from the application. It uses the name of the process to accomplish this task.
- VPN sessions do not appear in the list.

#### 4.5.2 Favorite Entries

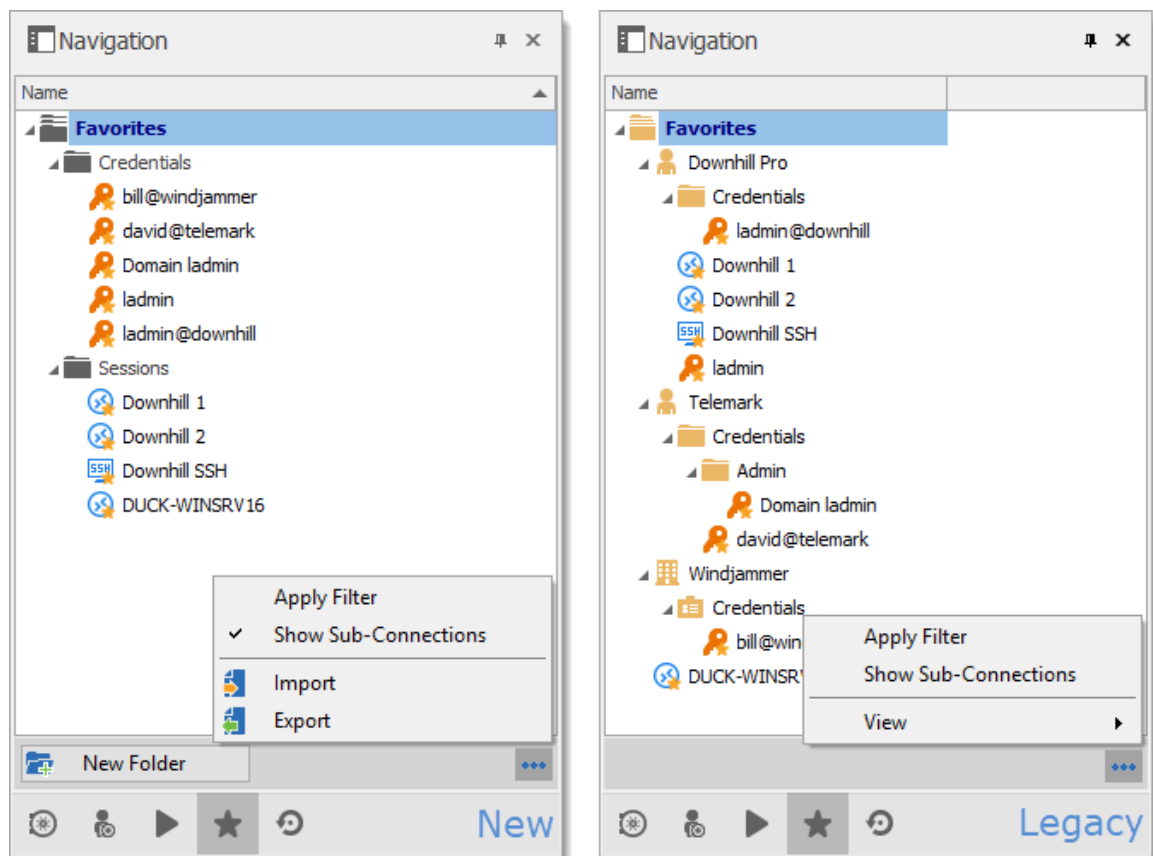
### DESCRIPTION

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.



The favorites feature has been completely reorganized in beta version 12.9.0.0. To revert to the legacy interface, navigate to **File – Options – User Interface – Favorites**, then enable the **Use legacy favorite UI** option.

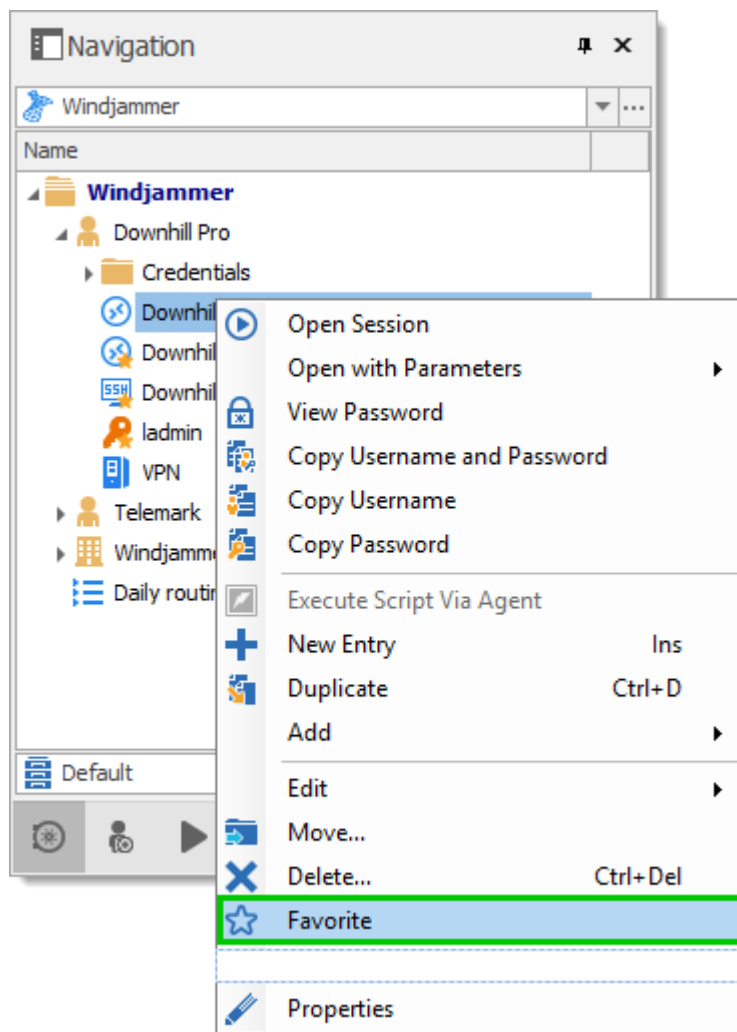


*New and Legacy favorite UI*

When using the legacy favorite interface, the favorites view can be personalized the same way as the Vault. Click on **...** to select a preferred **View**.

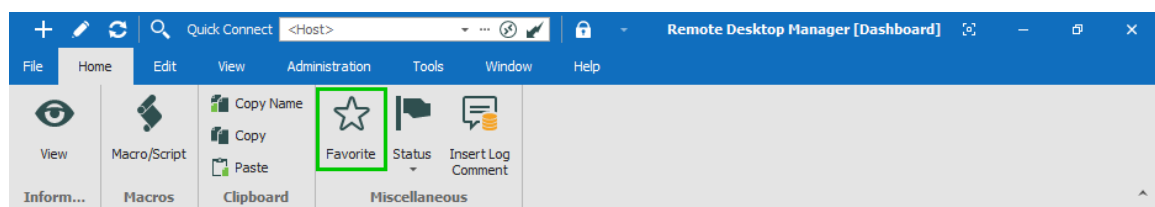
## FLAG AN ENTRY AS FAVORITE

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



*Flag an entry as favorite*

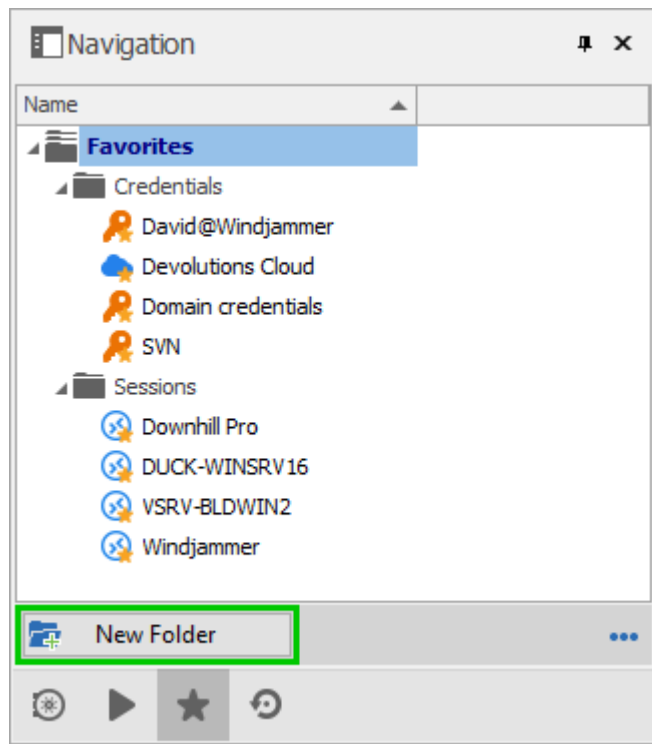
The same command is located in the ribbon **Home** tab in the **Miscellaneous** section.



*Home – Miscellaneous – Favorite*

## ORGANIZE THE FAVORITES

Favorites does not necessarily replicate the folder structure of the Vault. Add folders in the favorite view to organize your favorite entries, or enable the legacy favorite interface.



*Add folders to organize favorites*

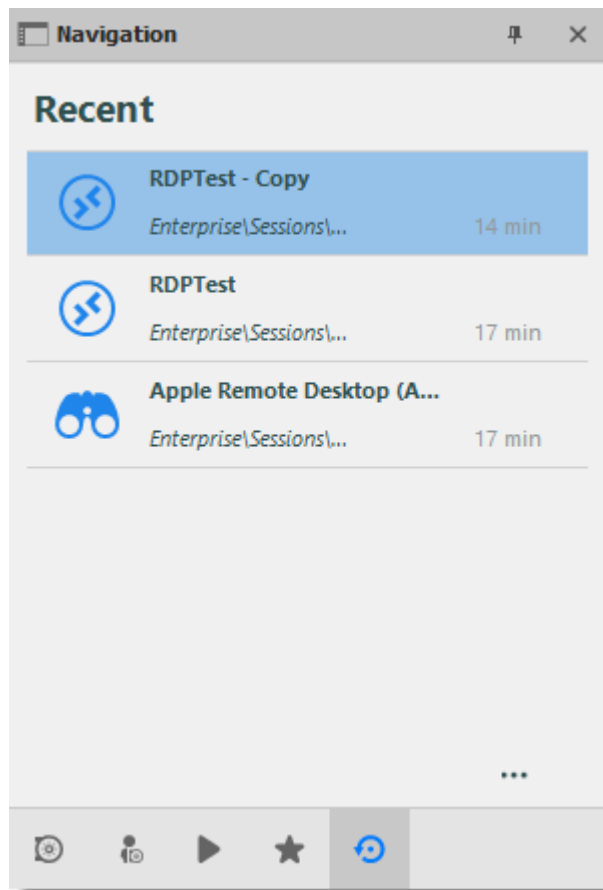
## ICON OVERLAY

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 connection list** option.

### 4.5.3 Most Recently Used Entries

## DESCRIPTION

This tab show the most recently used sessions on the local computer.



*Most Recently Used Entries*

The most recently used entries view can be personalized the same way as the tree view. Click on the **...** button to select your preferred view.

To delete the most recently used entries history, select **Clear Most Recently Used Entries...**

By default, 10 items will be kept in the most recently used entries history. This setting can be changed in **File - Options - General - Recent**.

## 4.6 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.

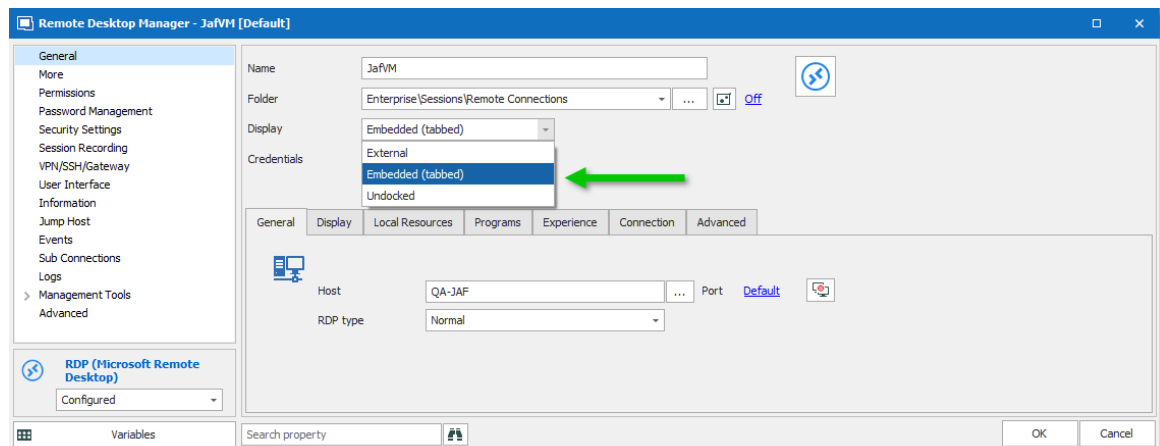
The options change depending on the entry:

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

#### 4.6.1 Embedded Sessions

### DESCRIPTION

The **Embedded (tabbed)** display mode allows you to open multiple sessions as tabs within 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**.

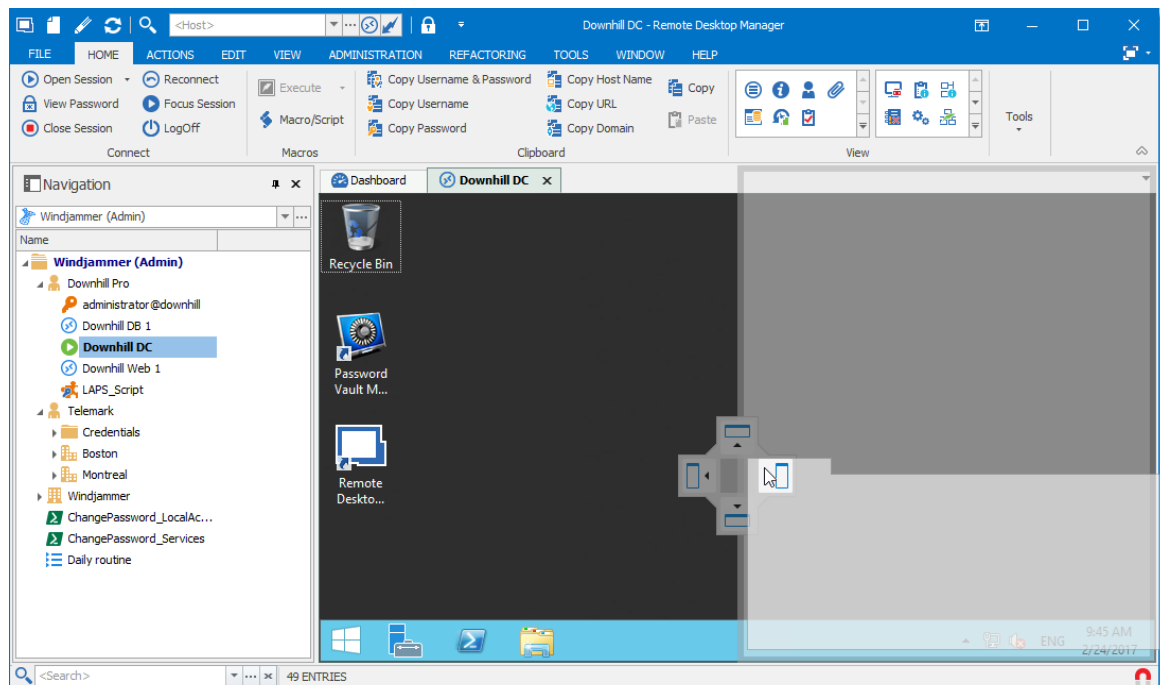


*Display Mode Settings*

### SPLIT WINDOWS

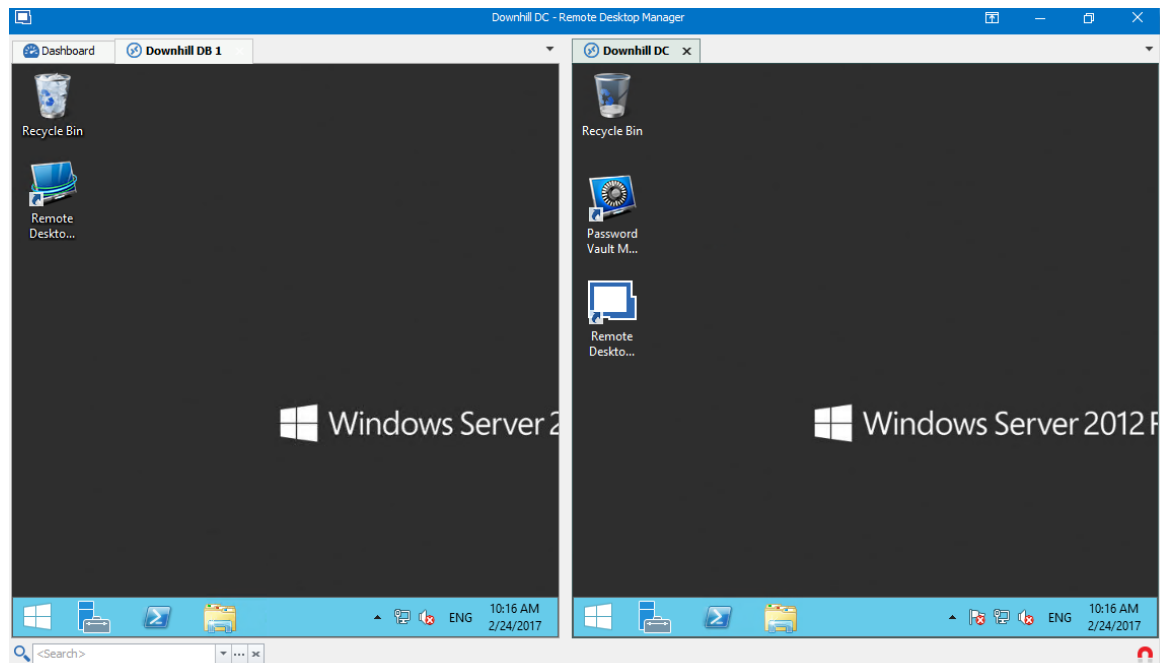
Within a Remote Desktop Manager embedded session is the option to display multiple tabbed windows simultaneously. As illustrated below, select and hold down on a tab and drag it towards the center of the screen to access the four-sided directional control. Aim the directional control to anchor the tab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





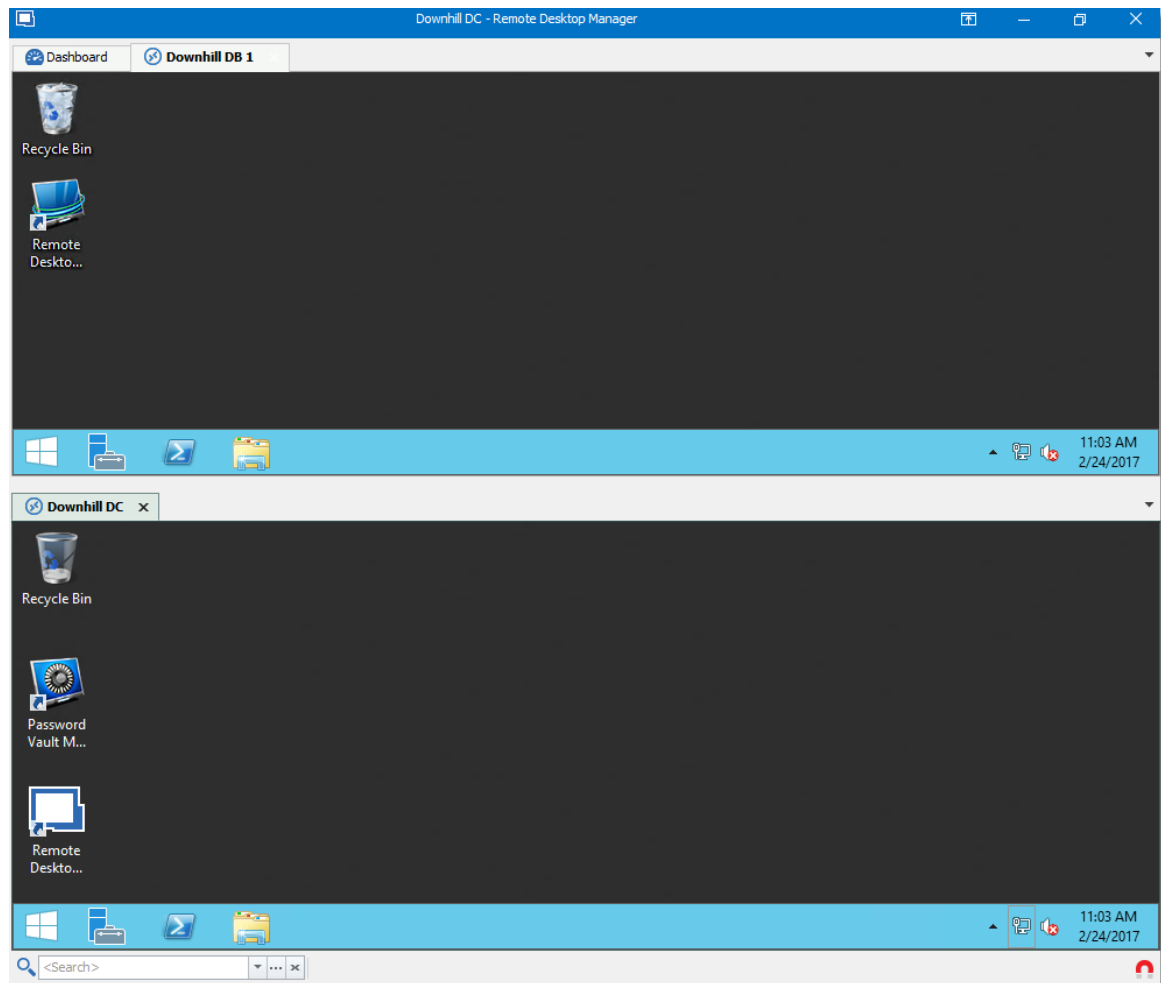
*Split Window - Drag And Drop*

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



*Split Window - Side-By-Side*

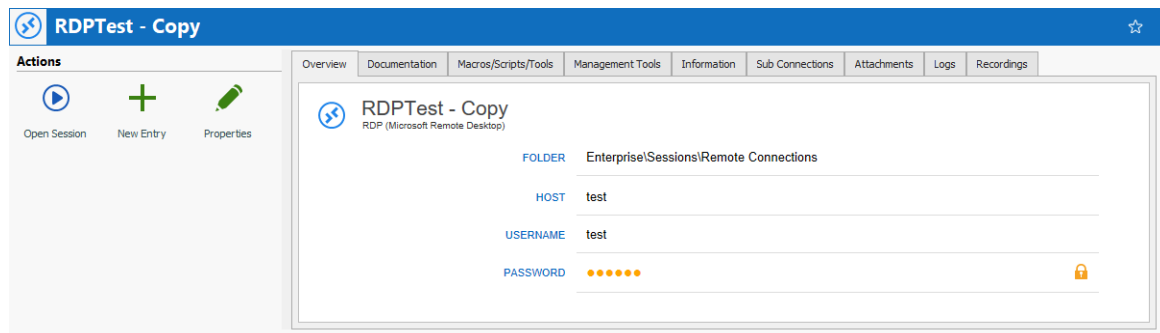
Below is an example of a top-down split window.



## 4.6.2 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*

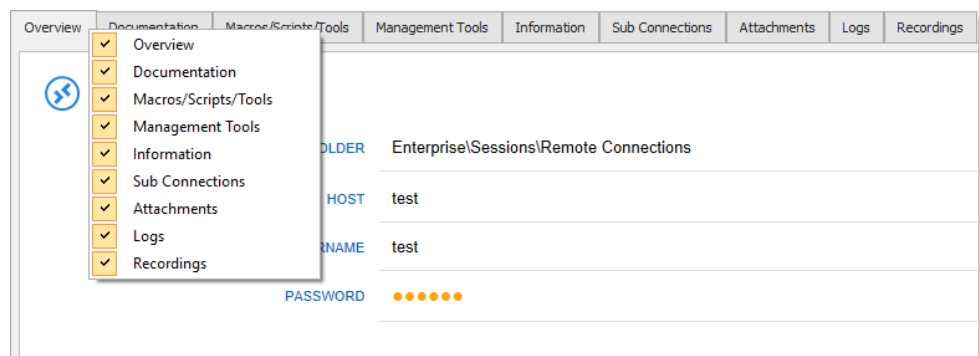
The different tabs available in the dashboard:

- **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.

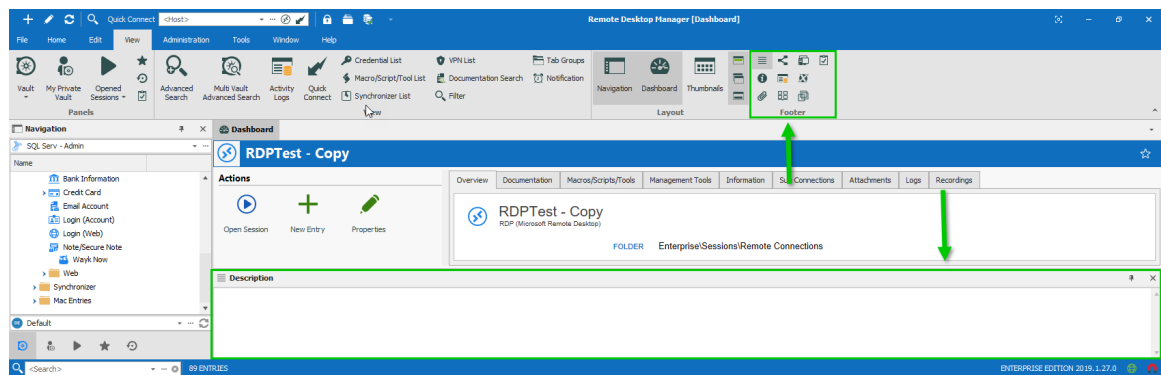


## 4.7 Panes (Footer)

### DESCRIPTION

Although the panes are by default in the footer, most tabbed windows can be moved around and docked to your liking. That applies to the Default (Ribbon) or Default (Menu) styles.

Use the **View – Footer** commands from the ribbon to control the visibility of individual panes.

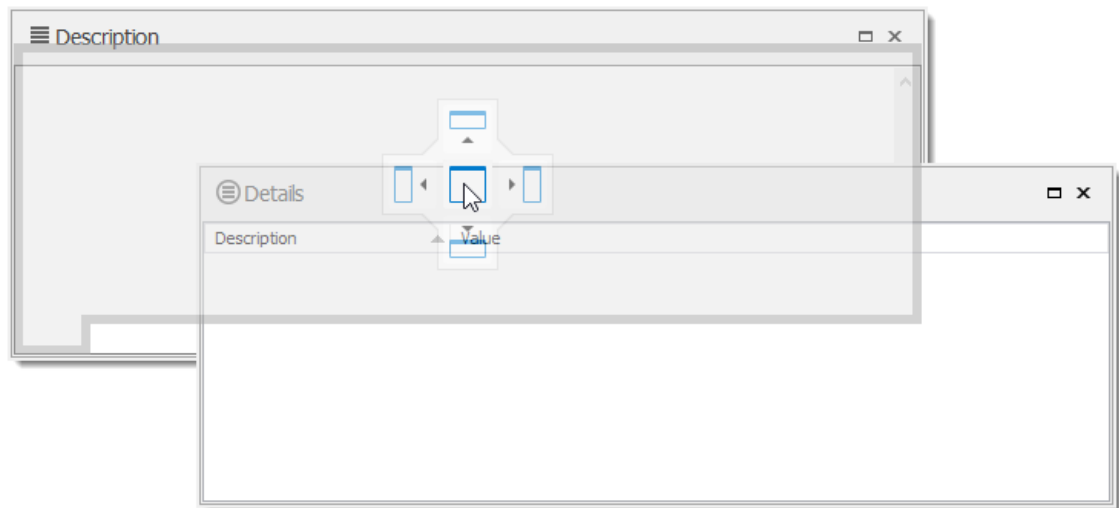


Footer Area

### DOCKED FOOTER

Upon first use, the footer panes are undocked by default. You can dock them to a single panel with a simple drag & drop. Just drag a pane into another one, then drop it in the center of the directional control.

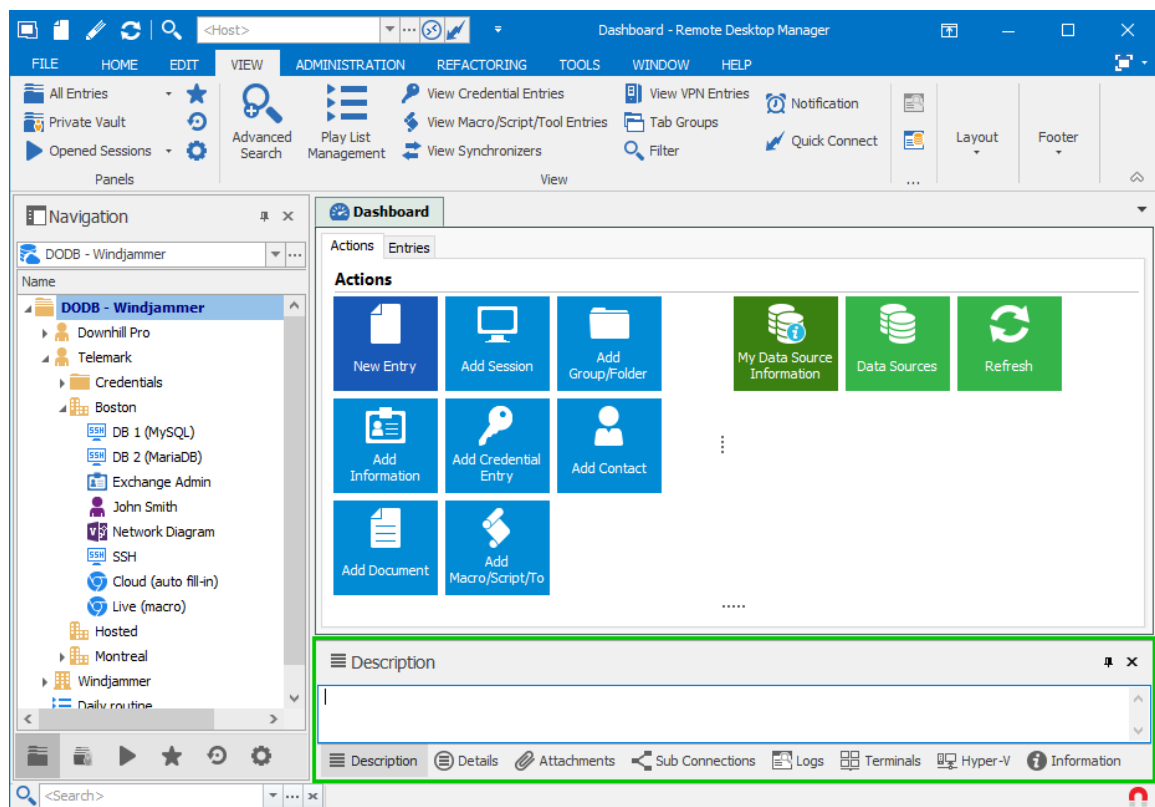
Here, we drop the **Details** pane to make it tabbed with the **Description** pane.



*Dock a footer pane into another*

You can use the same directional control to dock the footer panes into the main window.

Here is a personalized setup of the footer panes.



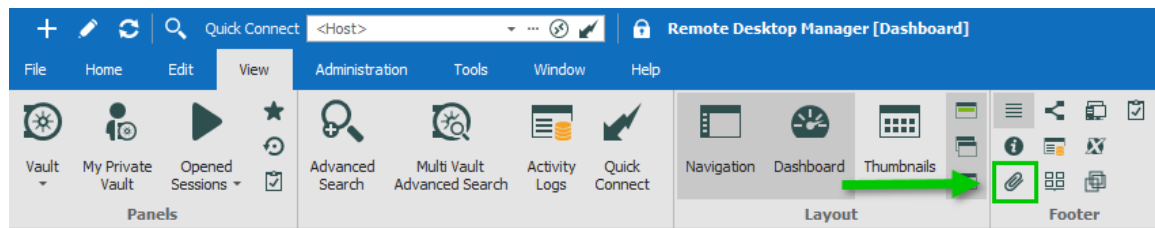
*Footer panes docked in the main window*

### 4.7.1 Attachments

## DESCRIPTION

Files are attached to an entry and are stored directly in the database.

To enable the attachment pane, navigate to **View – Footer** in the ribbon, then select **Attachments**.



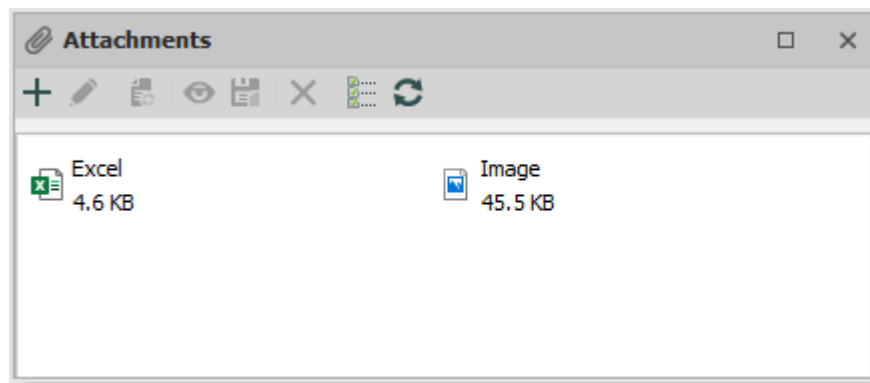
*View – Footer – Attachments*



This feature is only available when using an [Advanced Data Source](#).



The files in attachment are not available in offline mode.



*Attachment list*

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;

- 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 after an edit.

## ACTIONS

Use the toolbar above the attachment list to manage the selected attachment.



*Attachment toolbar*

OPTION	DESCRIPTION
<b>Add attachment</b> 	Select a local file to add.
<b>Edit attachment</b> 	Edit the selected attachment.
<b>Update document</b> 	Update the selected attachment.
<b>View attachment</b> 	Open the selected attachment.
<b>Save attachment as...</b> 	Save the attachment on a local drive.
<b>Delete attachment</b> 	Delete the selected attachment.
<b>Details</b> 	Display details about the selected attachment, above the attachment list.
<b>Refresh</b> 	Refresh the attachment list.

## 4.8 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.

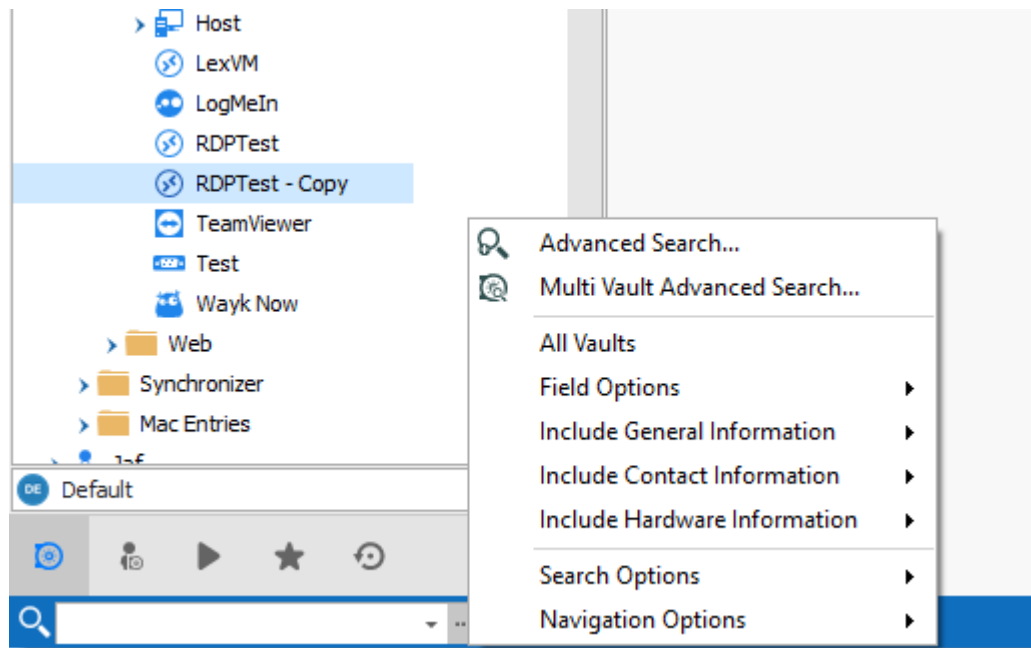
#### 4.8.1 Search/Filter

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*

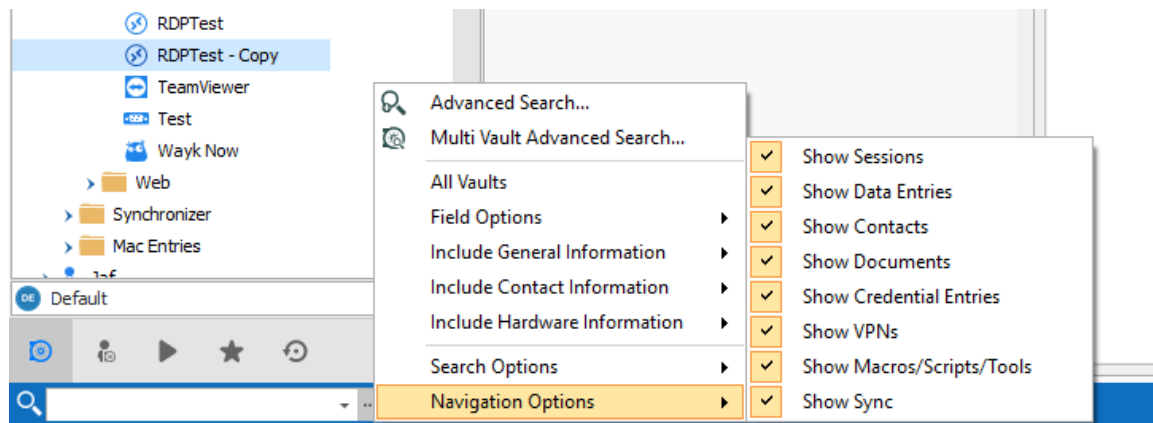
The filter expression is matched against fields as selected in the filter options such as:

- 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:

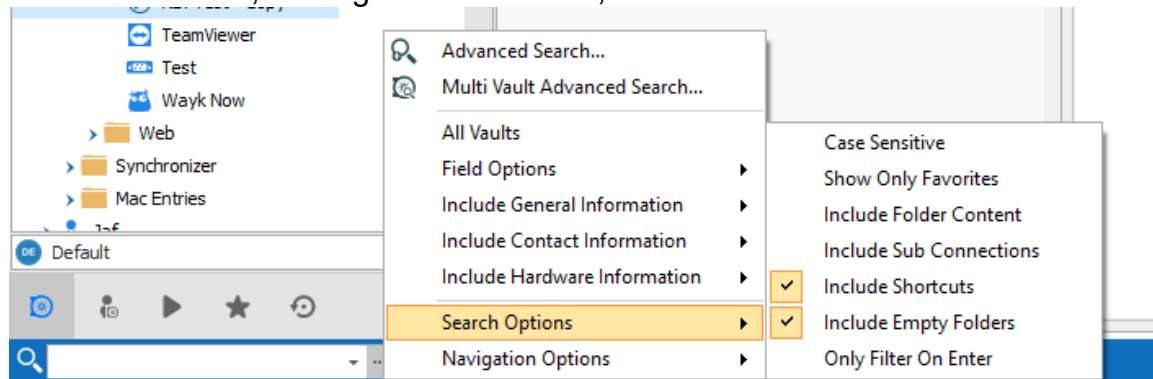
- Session types (credentials, script tools, VPN, etc.)
- If the session is marked as a Favorites

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)

## 4.8.2 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*

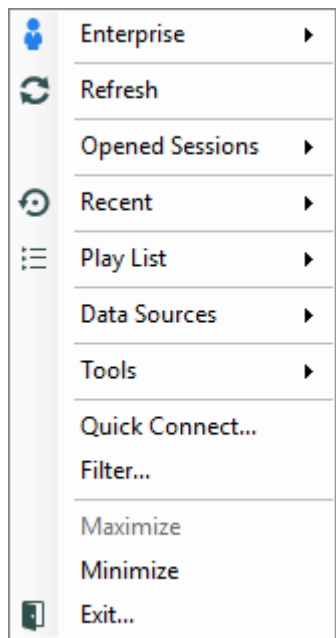
## 4.9 Tray Icon

### 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*

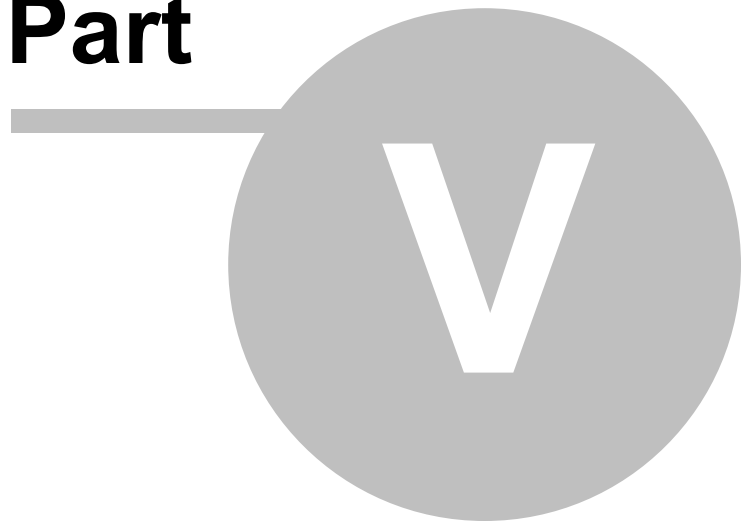
OPTION	DESCRIPTION
<b>Sessions List</b>	Displays the sessions from the current data source. Sessions are listed by default. It is possible to show only those marked as favorites.
<b>Refresh</b>	Refreshes the data source.
<b>Opened Sessions</b>	Lists all the currently open sessions.
<b>Recent</b>	Lists the <a href="#">Most Recently Used Entries</a> .
<b>Play List</b>	Allows the user to launch a <a href="#">Play List</a> from the tray icon.
<b>Data Sources</b>	Lists the available <a href="#">Data sources</a> and allows the user to switch from one to another. This section appears only if enabled and more than one data source is configured.
<b>Tools</b>	Lists all the configured tools.
<b>Quick Connect</b>	Prompts for the Quick Connect dialog to open an add-hoc connection with a specific type, or a selected template.
<b>Filter</b>	Launches the <a href="#">Search/Filter</a> feature.
<b>Maximize</b>	Restores the application to full screen.
<b>Restore</b>	Restores the application from minimize.
<b>Minimize</b>	Minimizes the application in the task bar.
<b>Exit</b>	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**



## 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.

The screenshot shows the 'Remote Desktop Manager' window with the 'General' tab selected. The configuration is for a data source named 'Test' of type 'SQL Server'. The host is 'TestSQL', login mode is 'Database login', username is 'test', and password is masked. The database is 'TestDB'. There are checkboxes for 'Always ask password' and 'Allow change username', both of which are unchecked. The 'Two factor' option is set to 'None'. At the bottom right, there are buttons for 'Test Server' and 'Test Database'. Below the configuration fields is a table listing data sources.

Type	Name	Locked
SQL Server	Test	
SQL Server	SQL Serv - UReg	
SQL Server	SQL Serv - Admin	
SQL Server	QA-LEX Duo	
Local Data Source	Local Data Source	

At the bottom of the window, there is an 'On start up' dropdown menu set to 'Last used data source', and 'OK' and 'Cancel' buttons.

*Data Source*

## CREATE A DATA SOURCE

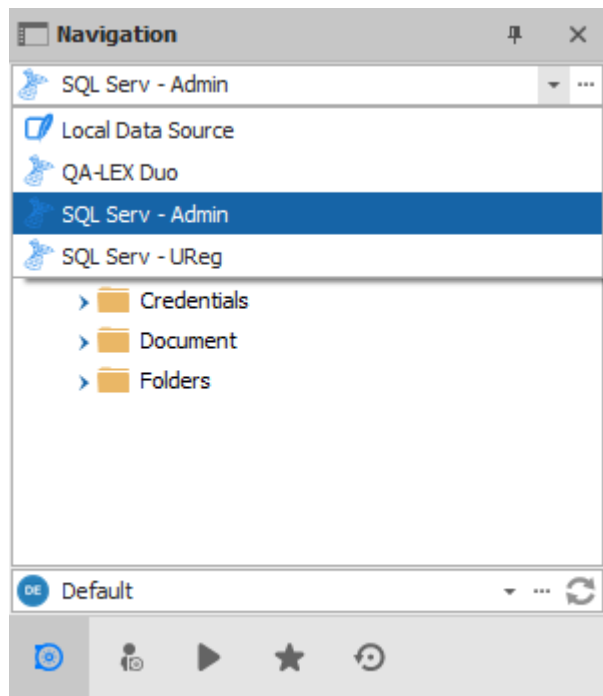
Please consult our [Create a new data source](#) topic for more information.

## 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.

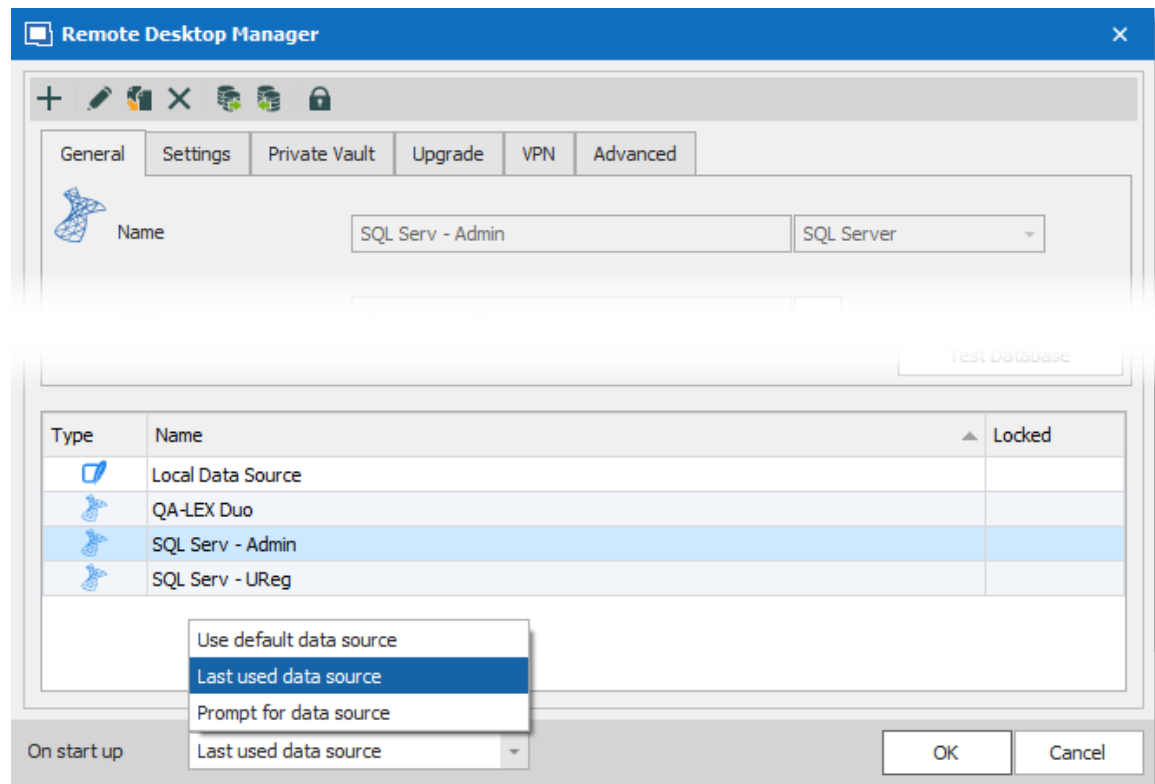




*Select a Data Source*

## STARTUP DATA SOURCE

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

*Startup Data Source*

OPTION	DESCRIPTION
<b>Use default data source</b>	Select the data source to connect to when the application starts.
<b>Last used data source</b>	Connect to the last used data source.
<b>Prompt for data source</b>	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](#), [MariaDB](#), Microsoft Access, [Microsoft SQL Azure](#), [Microsoft SQL Server](#), [MySQL](#) 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.

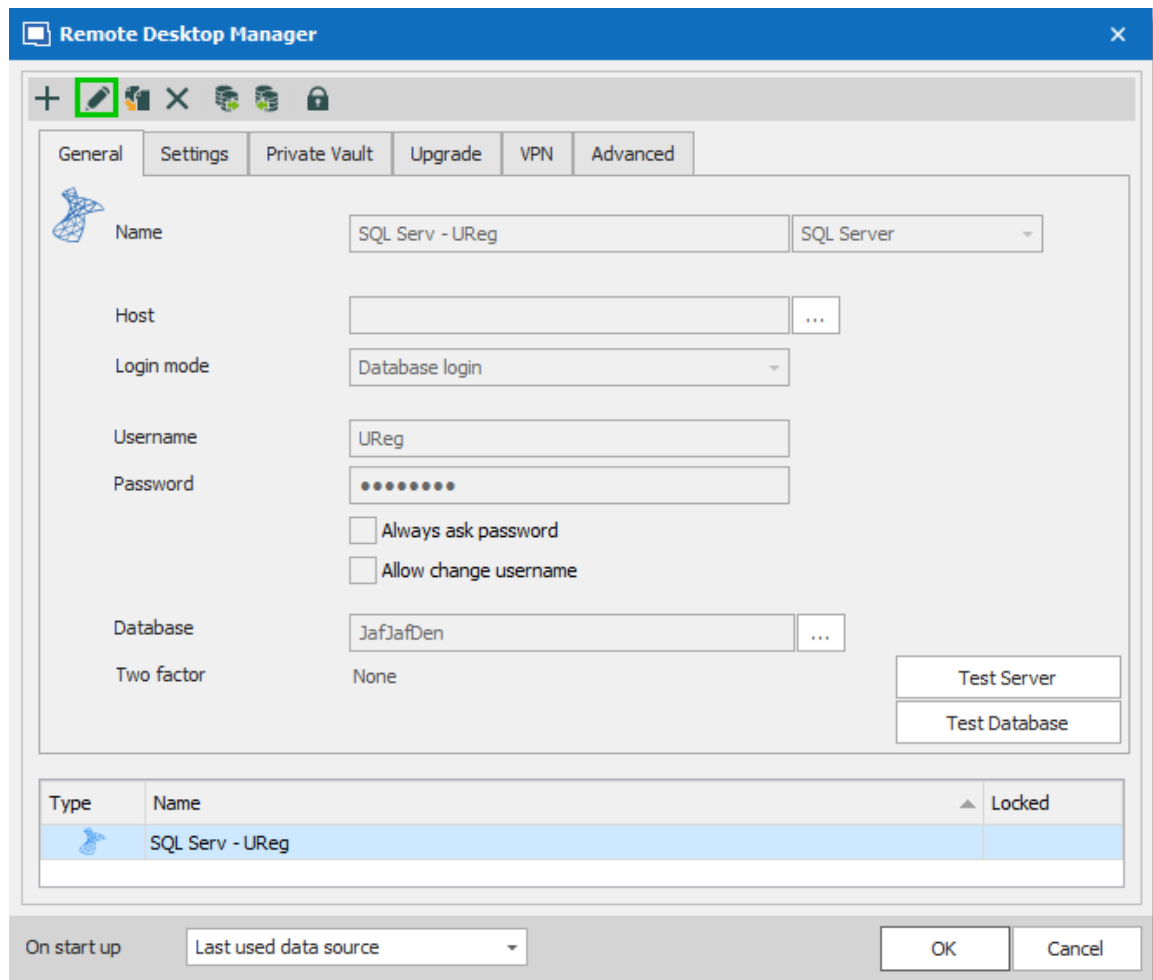
Remote Desktop Manager supports Google Authenticator, Yubikey, Duo and AuthAnvil.

### HOW TO CONFIGURE TWO-FACTOR AUTHENTICATION

*Example of how to configure 2FA with Google Authenticator*

### SETTINGS

1. Two factor authentication is set in the **Data Source Configuration**. You can set 2FA when creating a new data source or edit an existing data source. To edit your data source, click **File – Data Sources**. Click the pencil  to edit the data source.



*Edit - Data Source Configuration*

2. To set 2FA on the data source, click the **None** hyperlink.

The screenshot shows the 'Microsoft SQL Server' configuration window within the 'Remote Desktop Manager' application. The window has a blue header with the Microsoft SQL Server logo and title. Below the header are tabs for 'General', 'Settings', 'Private Vault', 'Upgrade', and 'Advanced'. The 'General' tab is selected. It contains fields for 'Name' (SQL Server), 'Host' (DEVOLUTIONS:\SQLEXPRESS), 'Login mode' (Database login), 'Username' (RDMAAdmin), 'Password' (masked with dots), and 'Database' (test). There are checkboxes for 'Always ask password' and 'Allow change username'. A 'Two factor' dropdown menu is highlighted with a green box, showing 'None' as the selected option. At the bottom right are buttons for 'Test Server', 'Test Database', 'OK', and 'Cancel'.

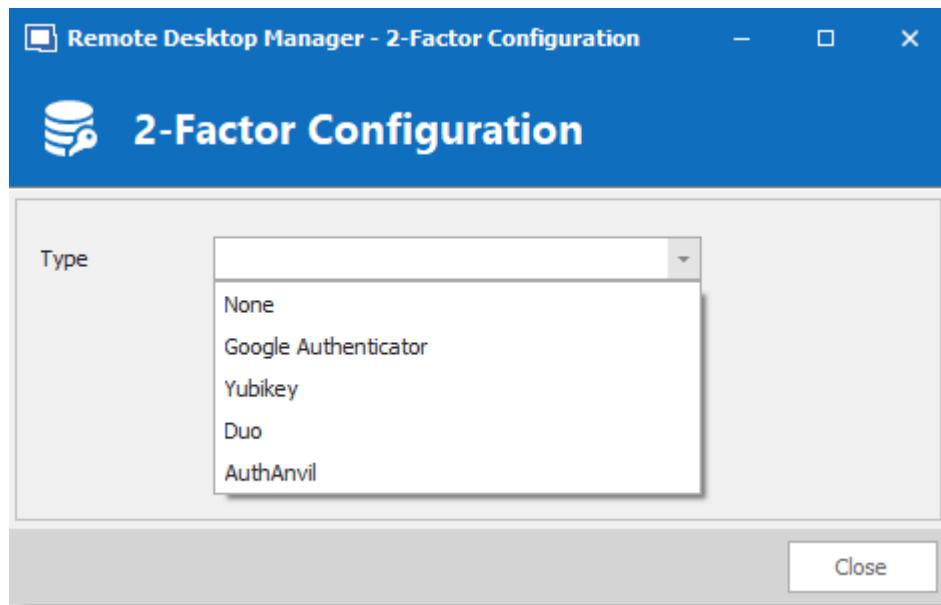
*Data Source Configuration*

3. In the next window, click **Change**.

The screenshot shows the '2-Factor Configuration' window within the 'Remote Desktop Manager' application. The window has a blue header with the Microsoft SQL Server logo and title. Below the header is a large text area with 'Type' and 'None' displayed. A blue underlined link 'Change' is visible below the text. At the bottom right is a button labeled 'Close'.

*Two-Factor Configuration window*

3. Choose the type of 2-Factor Authentication you wish to use.



*Two-Factor Configuration window*

4. Once you have selected your 2FA click **Save** to start the configuration.

To configure the 2FA you use, please see the topic about supported 2FA types:

- [Google Authenticator](#)
- [Yubikey](#)
- [Duo](#)
- [AuthAnvil](#)

### 5.1.1 Google Authenticator

## DESCRIPTION

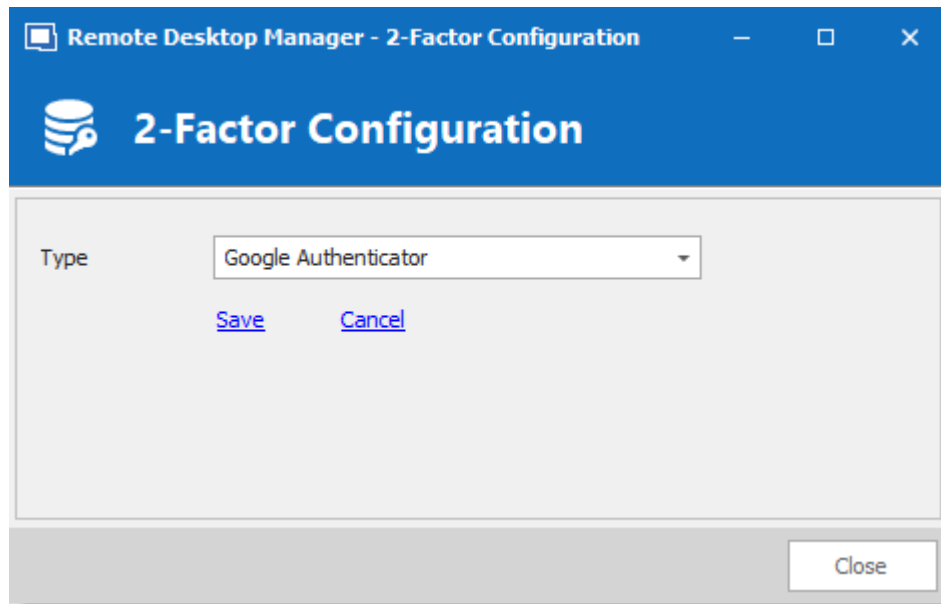
Remote Desktop Manager allows you to use Google Authenticator to provide an additional security layer when opening a data source.

## SETTINGS



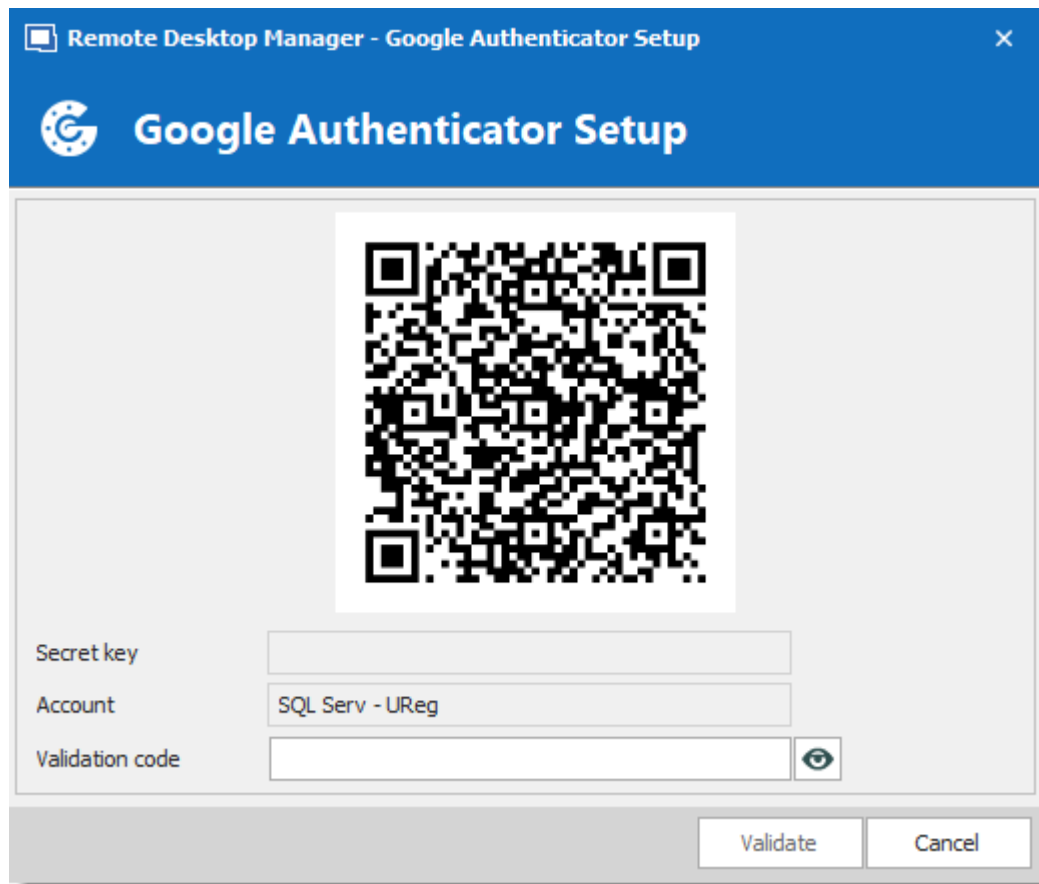
Before you start the configuration, make sure you have installed the [Google Authenticator](#) application on a supported device.

1. Select Google Authenticator as your 2-Factor Authentication and click on **Save**.



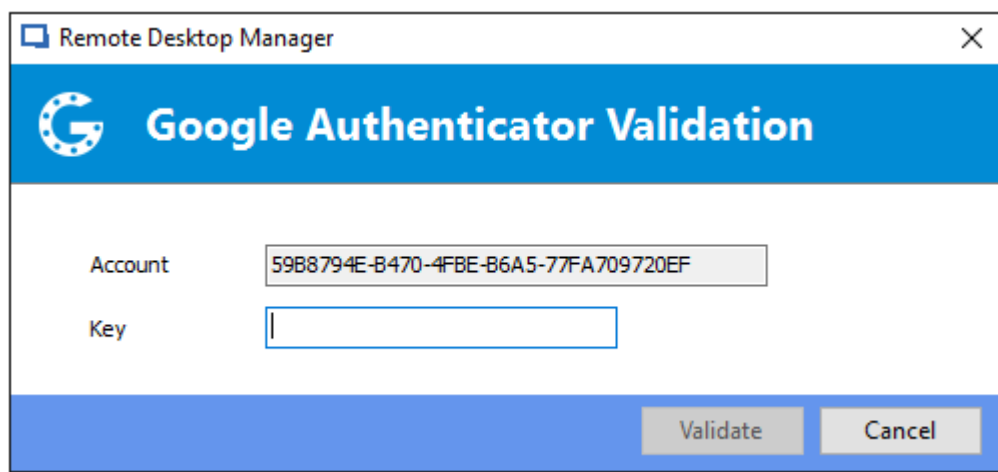
*Google Authenticator Configuration*

2. Once you have installed the application, scan the QR code on your screen with the Google Authenticator application to setup Remote Desktop Manager in Google Authenticator. When Remote Desktop Manager is configured in Google Authenticator, enter the Validation code provided by Google Authenticator in Remote Desktop Manager. Enter the Validation code and then click on **Validate**.



*Google Authenticator Setup*

3. Relaunch Remote Desktop Manager and select the protected data source to be prompted for the Google Authenticator code.



*Google Authenticator Validation*





Google Authenticator generates a new validation code every 30 seconds. Please consult your device application documentation for more details.

### 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.



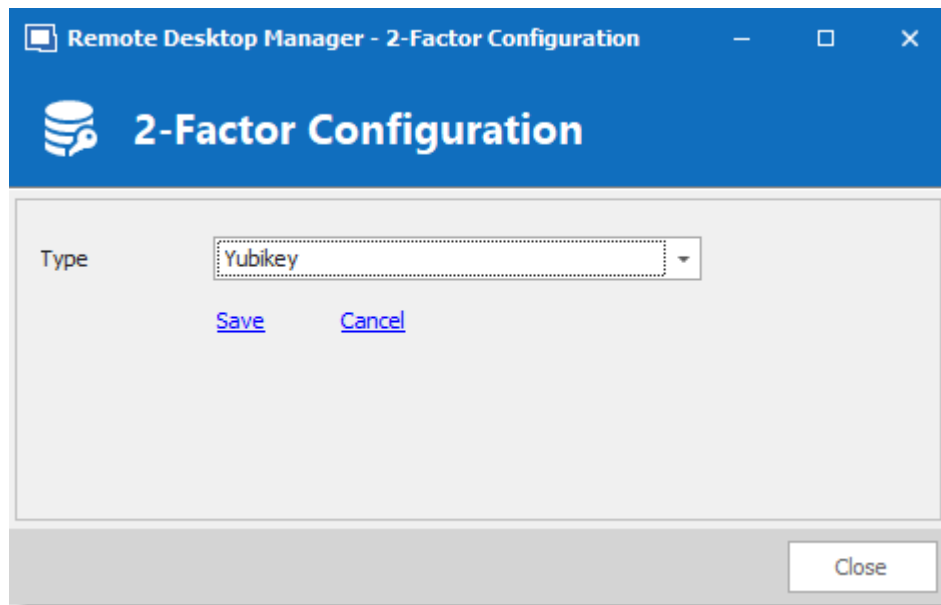
Remote Desktop Manager only support the Yubico OTP at this time.

#### SETTINGS



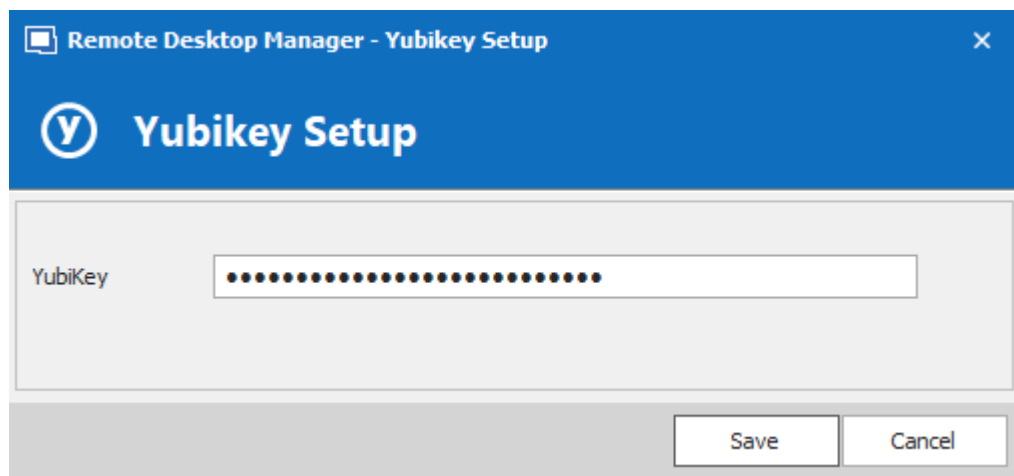
Before you start the configuration, make sure you have a [Yubikey](#) in your possession.

1. Select Yubikey as your 2-Factor Authentication and click on **Save**.



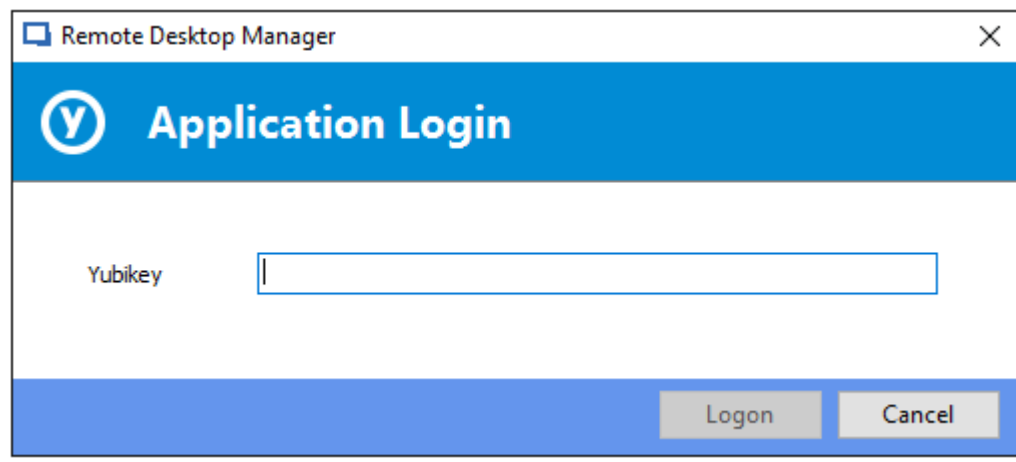
*Yubikey Configuration*

2. Insert the Yubikey into a USB port of your computer and hold the gold button on the Yubikey to have the code filled in the field, then click on **Save**.



*Yubikey Authentication*

3. Relaunch Remote Desktop Manager and select your protected data source to be prompted for a Yubikey code.



*Yubikey Application login*

### 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.

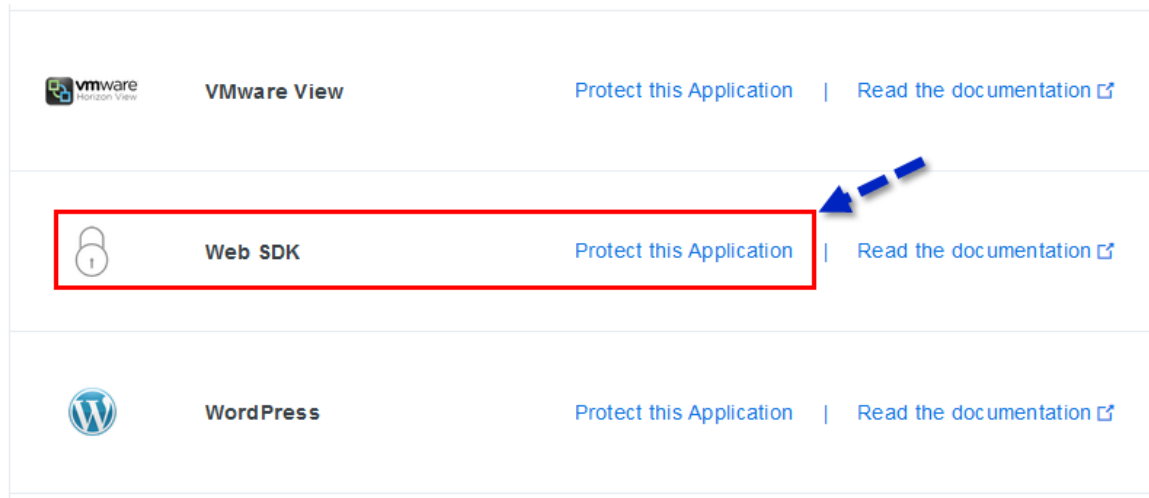
## SETTINGS



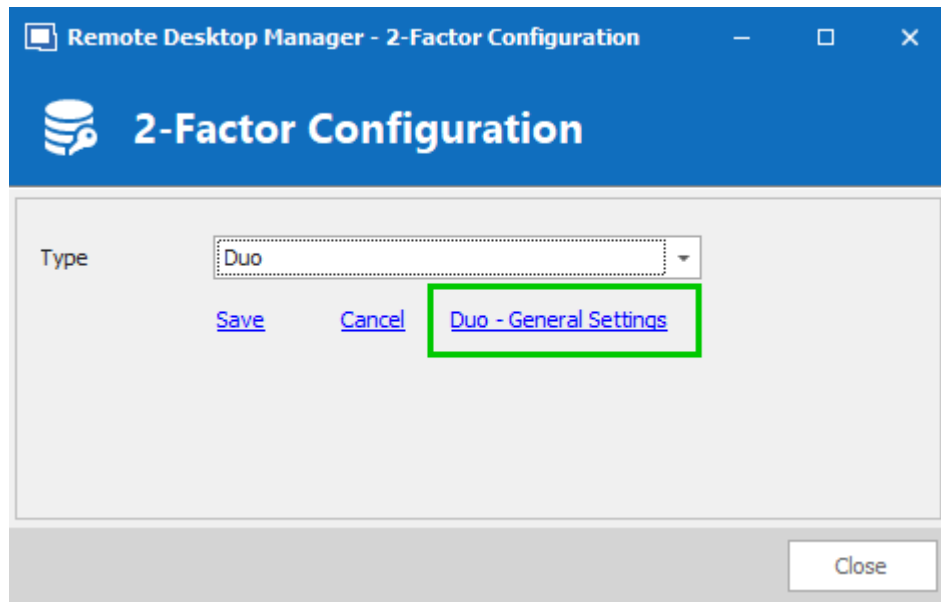
Before you start the configuration, make sure you have created yourself a Duo account and also have installed the Duo application on your compatible device.

There is three methods to use with Duo: by land line, by text message or by using their application.

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

*Web SDK application*

2. In Remote Desktop Manager select Duo as your Two factor authentication and click on **Duo – General Settings**.

*2-Factor Configuration*

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

[Dashboard](#) > [Applications](#) > Web SDK

## Web SDK

See the [Duo Web SDK Documentation](#) to integrate Duo into your custom web application.

### Details

Integration key	<input type="text" value="DIJCLD"/>	<a href="#">select</a>
Secret key	<input type="text" value="QwMZ"/>	<a href="#">select</a>
Don't write down your secret key or share it with anyone.		
API hostname	<input type="text" value="api-b8"/> <input type="text" value="duosecurity.com"/>	<a href="#">select</a>

*Duo Account - Web SDK*

4. Copy and paste all the information and click on **Check** to validate the information.

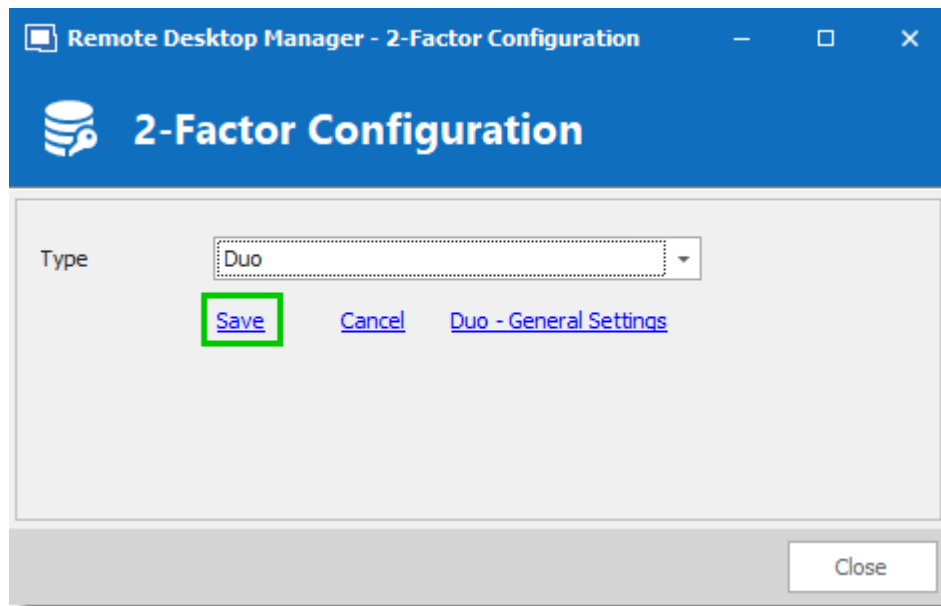
Remote Desktop Manager - Duo Settings

### Duo Settings

Integration key	<input type="text"/>
Secret key	<input type="text"/>
API Hostname	<input type="text"/>
Duo username	<input type="text"/>

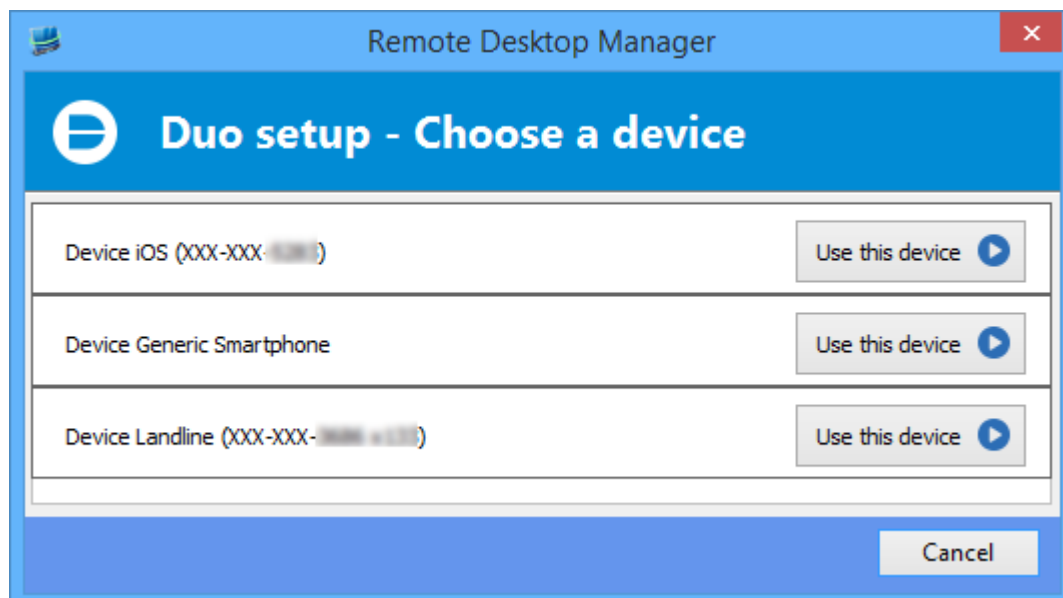
*Duo Settings*

5. Click on **Save** to authenticate yourself with your Duo account that has just been activated.



*Duo Configuration - Save settings*

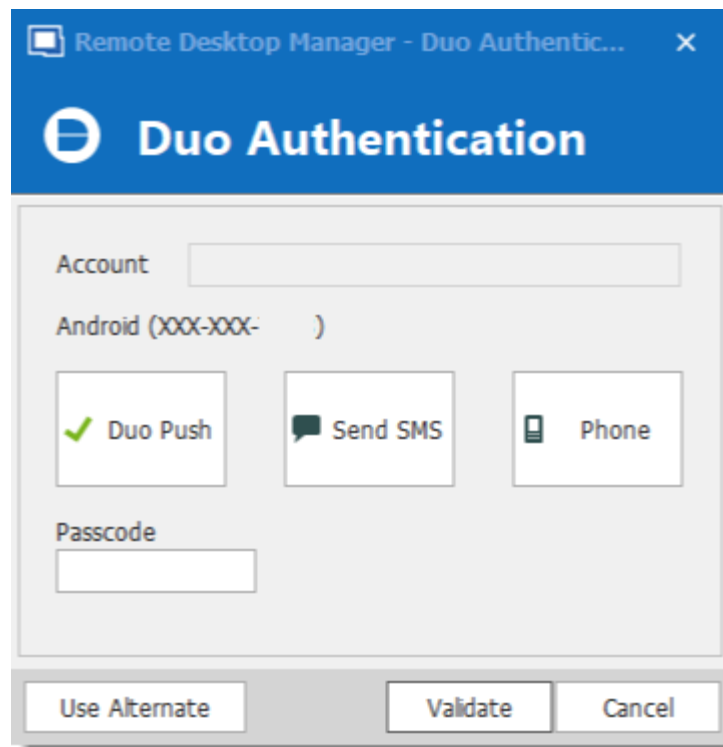
6. If you have more than one device connected to your Duo account, select the device you wish to use for your 2-Factor authentication.



*Duo setup - Choose a device*

7. 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.



*Duo Setup*

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

#### 5.1.4 AuthAnvil

### DESCRIPTION

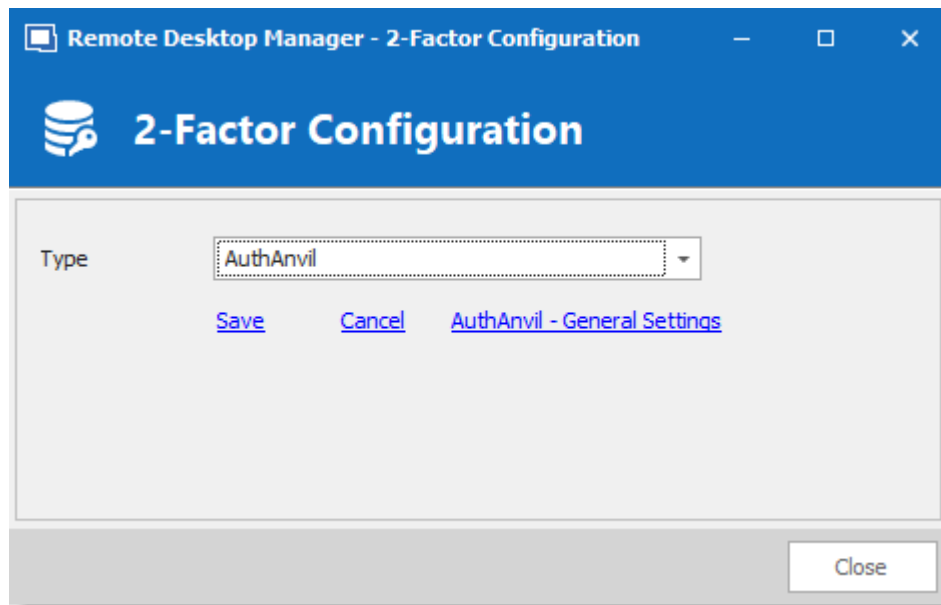
Remote Desktop Manager allows you to use AuthAnvil Authenticator to provide an additional security layer when opening a data source.

### SETTINGS



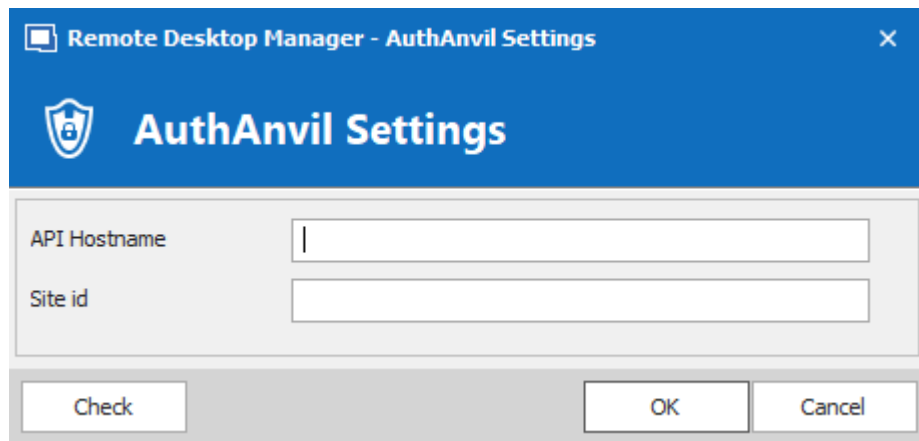
Before you start the configuration in Remote Desktop Manager, make sure you have created and configured your AuthAnvil account. For more information please consult <https://authanvil.com/features/two-factor-authentication>.

1. Select AuthAnvil in Remote Desktop Manager as your 2-Factor Authentication and click on **Save**.



*AuthAnvil Configuration*

2. Enter the information of your AuthAnvil account and click on **Check** to validate the entered information.



*AuthAnvil Settings*



## 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
<b>Disabled</b>	No client caching.

OPTION	DESCRIPTION
<b>Intelligent</b>	<p>Intelligent cache has the ability to handle many more sessions without experiencing performance degradation.</p> <p>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.</p> <p>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.</p>

## 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**.

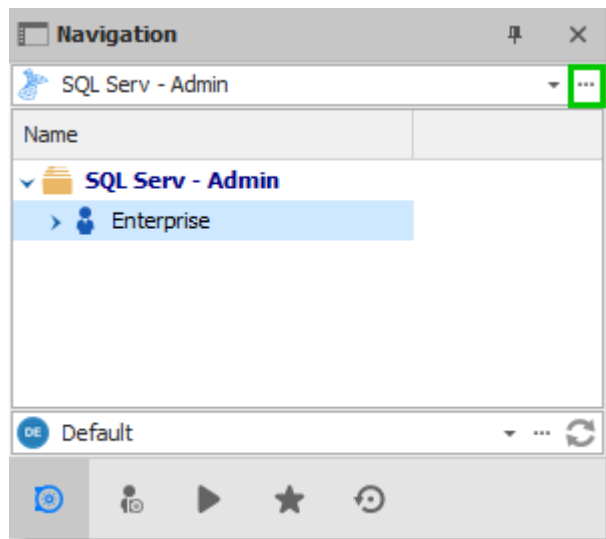


Depending on the configuration of the Caching mode & the [Offline mode](#) the offline file may still exist since the file servers as a dual purpose caching & offline line support.

## 5.3 Create a data source

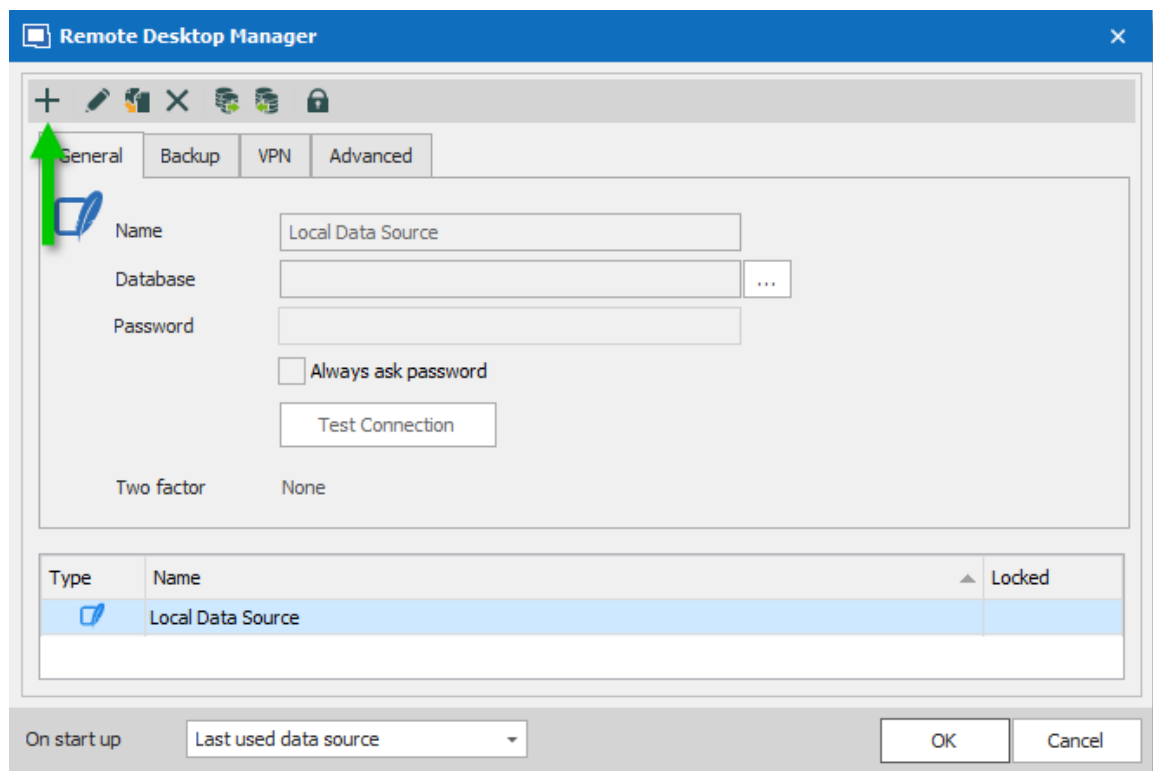
### SETTINGS

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.



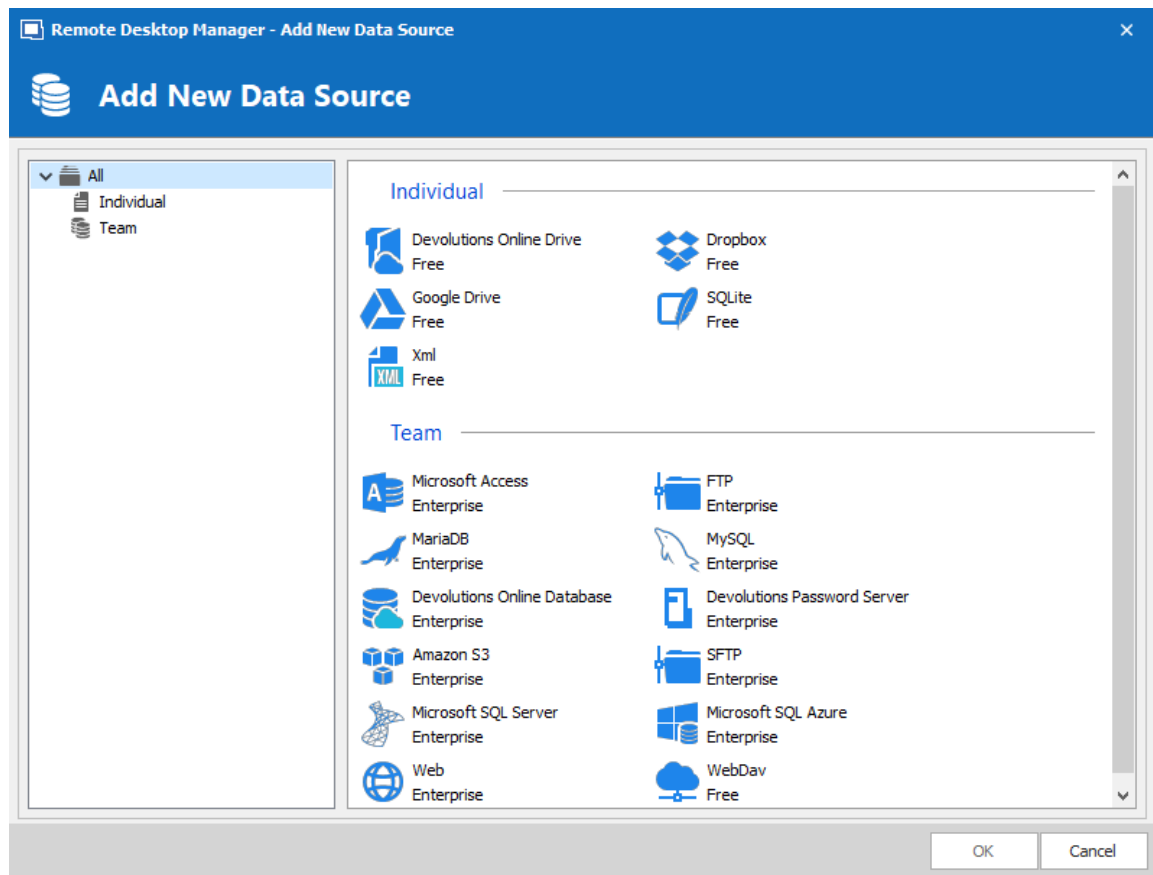
*Open Data Source menu*

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).

Remote Desktop Manager - Microsoft SQL Server

Microsoft SQL Server

General Settings Private Vault Upgrade VPN Advanced

Name  SQL Server

Host  ...

Login mode Database login

Username

Password

☐ Always ask password

☐ Allow change username

Database  ...

Two factor [None](#)

Test Server

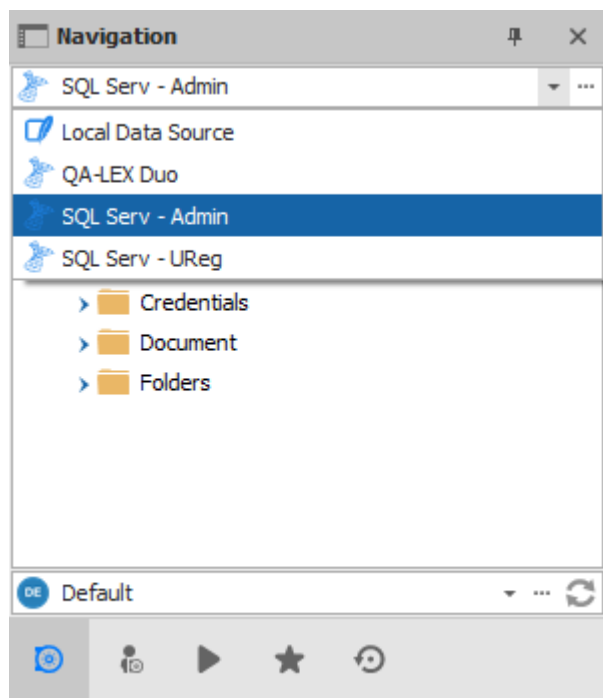
Test Database

ID 707CB610-6799-4562-9B62-EA06240A300F

OK Cancel

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. To start, decide which data source you'll be using.




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
<b>Devolution s Online</b>	Remote Desktop Manager connects to the Devolutions Online	Pros:



NAME	DESCRIPTION	PROS AND CONS
<b>Database</b> 	<p>Database vault.</p> <p>Note that there are different subscription levels for this product.</p> <p>The Basic is suitable for micro-teams (up to 3 users), while the Professional and Enterprise editions are for larger teams.</p> <p>For more information, please see the <a href="#">Online Database section</a>.</p>	<ul style="list-style-type: none"> <li>• Quick.</li> <li>• Reliable.</li> <li>• Secure.</li> <li>• Shareable.</li> </ul> <p>Cons:</p> <ul style="list-style-type: none"> <li>• Cannot be hosted on premises.</li> </ul>
<b>Devolution's Online Drive</b> 	<p>Remote Desktop Manager uses Devolutions Online Drive to store and synchronize your sessions. Access your sessions from anywhere using a simple Internet connection.</p> <p>For more information, please consult our <a href="#">Online Drive</a> topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> <li>• Quick.</li> <li>• Reliable.</li> <li>• The service is free.</li> </ul> <p>Cons:</p> <ul style="list-style-type: none"> <li>• No possibility for sharing.</li> <li>• No security management.</li> </ul>
<b>Devolution's Server</b> 	<p>Remote Desktop Manager uses Devolutions Server to store session information.</p> <p>For more information, please consult our <a href="#">Devolutions Server</a> topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> <li>• Quick.</li> <li>• Reliable.</li> <li>• Secure.</li> </ul>






NAME	DESCRIPTION	PROS AND CONS
		<ul style="list-style-type: none"><li>• Supports all features, such as <a href="#">attachments</a>, connection log, <a href="#">Offline Mode</a> and <a href="#">User Management</a>.</li><li>• Active Directory integration.</li></ul> <p>Cons</p> <ul style="list-style-type: none"><li>• Installation required.</li></ul>
<b>Dropbox</b> 	<p>Remote Desktop Manager uses the Dropbox API to retrieve the XML file from the configured repository.</p> <p>For more information, please consult our <a href="#">Dropbox</a> topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"><li>• Can be shared in read-only mode.</li><li>• Backups (by Dropbox) are automatic.</li><li>• Storage infrastructure is free (if within your free storage quota).</li></ul> <p>Cons:</p> <ul style="list-style-type: none"><li>• No security management.</li><li>• There is a possibility for conflict or data corruption to occur.</li><li>• Doesn't support all features, such as <a href="#">attachments</a>, connection logs and <a href="#">User Management</a>.</li><li>• The Dropbox integration uses the Dropbox SDK, so any features that are exclusive to the</li></ul>

NAME	DESCRIPTION	PROS AND CONS
		Business or Enterprise editions are NOT supported.
<b>MariaDB</b> 	<p>Remote Desktop Manager uses MariaDB to save and manage all sessions. This is one of the available data source for a multi-user environment.</p> <p>For more information, please consult our <a href="#">MariaDB</a> topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> <li>• Quick.</li> <li>• Reliable.</li> <li>• The database is free and can be installed on Linux.</li> <li>• Supports all features, such as <a href="#">attachments</a>, connection log, <a href="#">Offline mode</a> and <a href="#">User Management</a>.</li> </ul> <p>Cons:</p> <ul style="list-style-type: none"> <li>• MariaDB needs to be installed.</li> </ul>
<b>Microsoft SQL Azure</b> 	<p>Remote Desktop Manager uses the Microsoft cloud platform to save and manage all sessions.</p> <p>For more information, please consult our <a href="#">SQL Azure</a> topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> <li>• Quick.</li> <li>• Reliable.</li> <li>• Secure.</li> <li>• Supports all features, such as <a href="#">attachments</a>, connection log, <a href="#">Offline mode</a> and <a href="#">User Management</a>.</li> </ul> <p>Cons:</p>

NAME	DESCRIPTION	PROS AND CONS
		<ul style="list-style-type: none"> <li>• Microsoft Azure needs to be configured.</li> </ul>
<b>Microsoft SQL Server</b> 	<p>Remote Desktop Manager uses SQL Server to save and manage all sessions. This is one of the available data source for a multi-user environment.</p> <p>For more information, please consult our <a href="#">SQL Server (MSSQL)</a> topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> <li>• Quick.</li> <li>• Reliable.</li> <li>• Secure.</li> <li>• Supports all features, such as <a href="#">attachments</a>, connection log, <a href="#">Offline mode</a> and <a href="#">User Management</a>.</li> <li>• SQL Server Express is free.</li> </ul> <p>Cons:</p> <ul style="list-style-type: none"> <li>• SQL Server must be installed.</li> </ul>
<b>MySQL</b> 	<p>Remote Desktop Manager uses a MySQL database to save and manage all sessions. This is one of the available data source for a multi-user environment.</p> <p>For more information, please consult our <a href="#">MySQL</a> topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> <li>• Quick.</li> <li>• Reliable.</li> <li>• The database is free and can be installed on Linux.</li> <li>• Supports all features, such as <a href="#">attachments</a>, connection log, <a href="#">Offline mode</a> and <a href="#">User Management</a>.</li> </ul> <p>Cons:</p>

NAME	DESCRIPTION	PROS AND CONS
		<ul style="list-style-type: none"> <li>• MySQL needs to be installed.</li> </ul>
<b>Devolution s Password Hub Business</b>  	<p>Remote Desktop Manager connects to the Devolutions Password Hub Business vault.</p> <p>Note that there are different subscription levels for this product.</p> <p>For more information, please see the <a href="#">products features and highlights</a> and consult our <a href="#">topic</a>.</p>	<p>Pros:</p> <ul style="list-style-type: none"> <li>• Quick.</li> <li>• Reliable.</li> <li>• Secure.</li> <li>• Shareable.</li> </ul> <p>Cons:</p> <ul style="list-style-type: none"> <li>• Cannot be hosted on premises.</li> <li>• No offline mode</li> </ul>
<b>Devolution s Password Hub Personal</b>  	<p>Remote Desktop Manager uses Devolutions Password Hub Personal to store and synchronize your sessions. Access your sessions from anywhere using a simple Internet connection.</p> <p>For more information, please consult our <a href="#">Password Hub Personal</a> topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> <li>• Quick.</li> <li>• Reliable.</li> <li>• The service is free.</li> </ul> <p>Cons:</p> <ul style="list-style-type: none"> <li>• No possibility for sharing.</li> <li>• No offline mode</li> </ul>
<b>SQLite</b>	Remote Desktop Manager uses a SQLite database to store session information.	<p>Pros:</p> <ul style="list-style-type: none"> <li>• Quick.</li> <li>• Reliable.</li> </ul>

NAME	DESCRIPTION	PROS AND CONS
	<p>For more information, please consult our <a href="#">SQLite</a> topic.</p>	<ul style="list-style-type: none"> <li>• The database is free.</li> <li>• Supports all features, such as <a href="#">attachments</a> &amp; connection logs.</li> </ul> <p>Cons:</p> <ul style="list-style-type: none"> <li>• No possibility for sharing.</li> <li>• No security management.</li> </ul>
<b>WebDAV</b> 	<p>Remote Desktop Manager uses an HTTP connection to retrieve the XML file on a WebDav server.</p> <p>For more information. please consult our <a href="#">WebDAV</a> topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> <li>• Can be shared in read-only mode.</li> <li>• Easy to deploy online.</li> </ul> <p>Cons:</p> <ul style="list-style-type: none"> <li>• No security management.</li> </ul>
<b>XML</b> 	<p>Remote Desktop Manager saves the settings directly in a file with the XML format.</p> <p>For more information, please consult our <a href="#">XML</a> topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> <li>• Easy backup.</li> <li>• Can be edited manually or by an external system.</li> <li>• Nothing to install.</li> </ul> <p>Cons:</p> <ul style="list-style-type: none"> <li>• No possibility of sharing.</li> <li>• No security management.</li> </ul>

NAME	DESCRIPTION	PROS AND CONS
		<ul style="list-style-type: none"><li>• There is a possibility for conflict or data corruption to occur.</li><li>• Doesn't support all features, such as <a href="#">attachments</a>, connection logs and <a href="#">User Management</a>.</li></ul>

### 5.4.1 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.

Advanced Data Sources 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](#) and [User Groups based security system](#).
- [Offline mode](#).
- [Multi-Factor Authentication](#)

Currently the Advanced Data Sources are:

- [Devolutions Server](#).
- [MariaDB](#).
- [MySQL](#).
- [Microsoft SQL Azure](#).

- [Microsoft SQL Server \(MSSQL\)](#).
- [Devolutions Password Hub Business](#).

#### 5.4.1.1 Devolutions Online Database

## DESCRIPTION

Please consult topic [Online Database](#) for information on this service.



The [User Groups Management](#) feature is not available in Devolutions Online Database. Only the Security Group Management system is offered with this type of data source.

## SETTINGS

### GENERAL

Remote Desktop Manager - Devolutions Online Database

**Devolutions Online Database**

General User Vault VPN Advanced

Name  [Create an account for free](#)

Username

Connection mode

☐ Prompt for credentials

Database  ...

Database ID

Two factor [None](#)

ID OK Cancel

*Devolutions Online Database - General Tab*

OPTION	DESCRIPTION
<b>Name</b>	Name of the data source.
<b>Always ask password</b>	Always ask password when connecting to the data source.
<b>Create an account for free</b>	Create a new <a href="#">Devolutions Account</a> .
<b>Database</b>	Name of the data base created online. You must use the ellipsis button to select it from the list of online data sources available to the name.
<b>Database ID</b>	Unique Key to identify the data source.

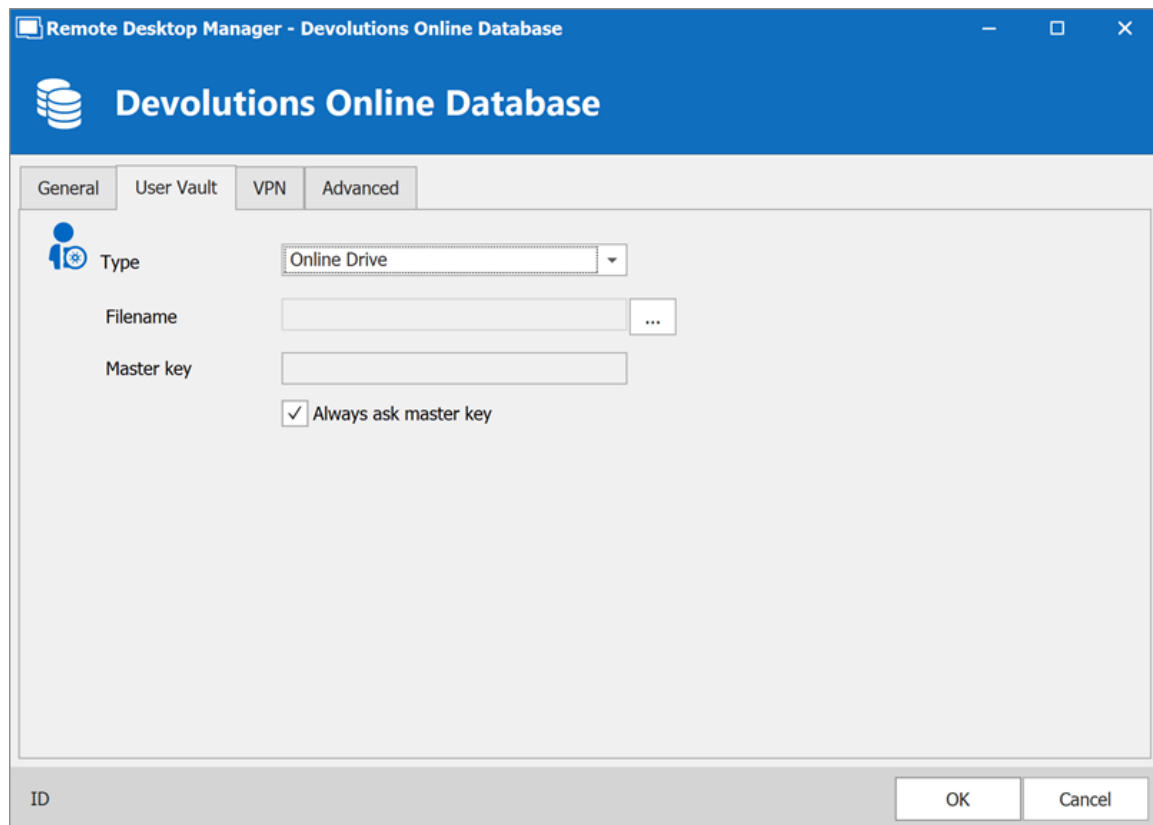


OPTION	DESCRIPTION
<b>Two factor</b>	Enable the <a href="#">2-Factor Authentication</a> to access your data source.
<b>Test Credentials</b>	Test the credentials that you have configured to connect on Remote Desktop Manager Online.

## USER VAULT

Connect your **Devolutions Online Database** to a **User Vault** stored in a **Devolutions Online Drive** file (.dod), thus creating your own **User Vault** containing entries and credentials that no one else has access to.

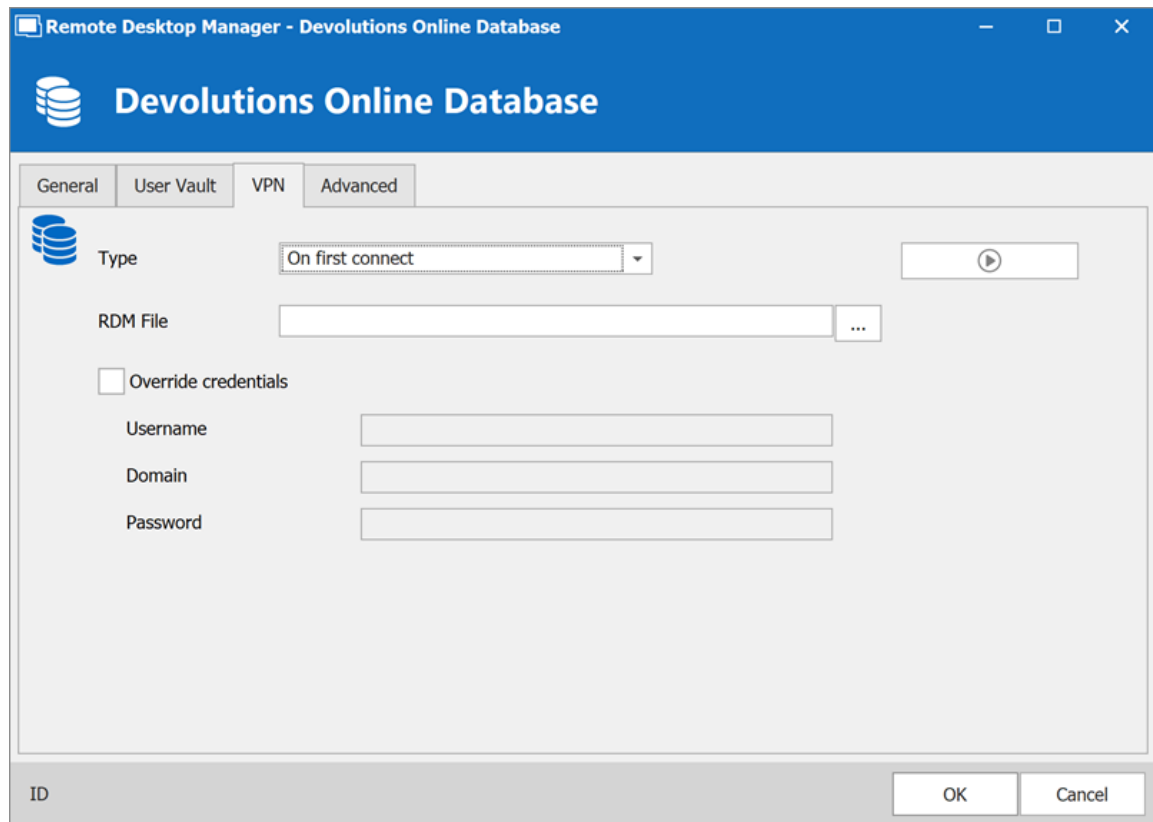
For more information please see [User Vault](#).



*Devolutions Online Database - User Vault*

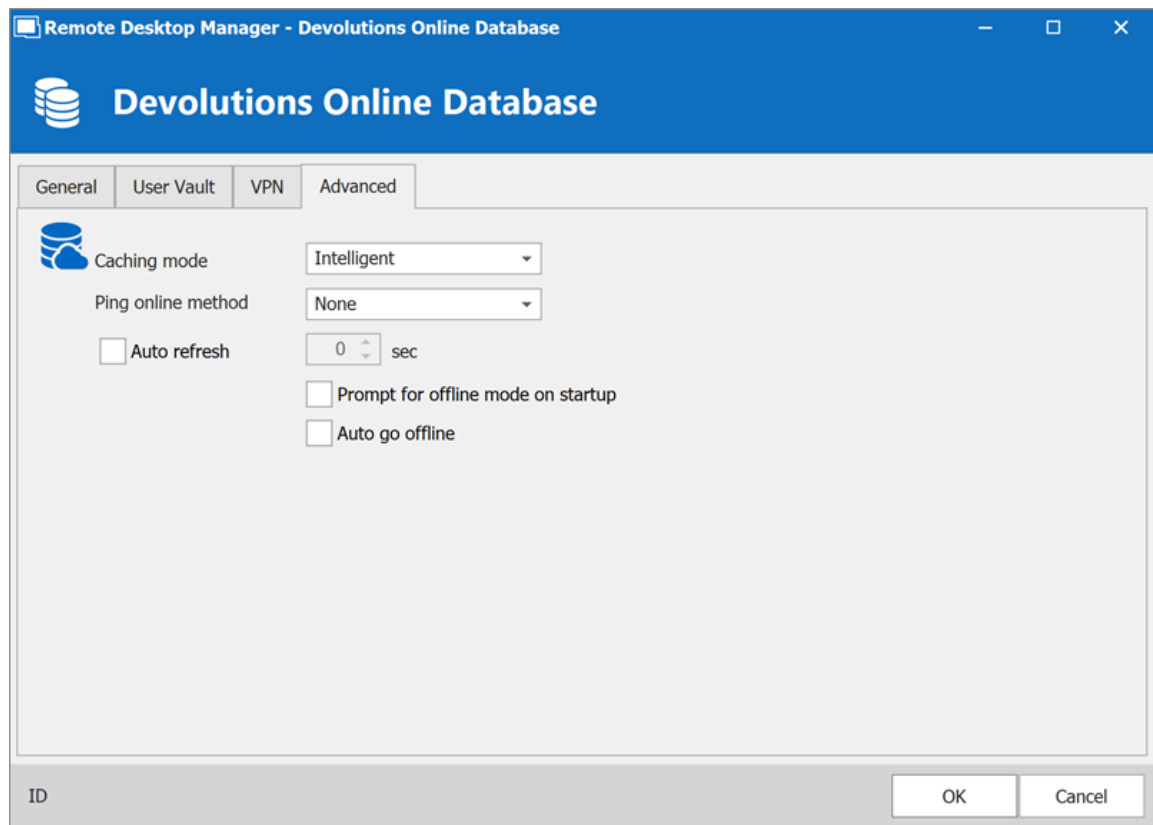
## VPN

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



*Devolutions Online Database - VPN*

## ADVANCED

*Devolutions Online Database - Advanced*

OPTION	DESCRIPTION
<b>Caching mode</b>	Determine how the entries will be loaded from the data source. See <a href="#">Caching</a> topic for more information.
<b>Ping online method</b>	Indicate the prefer ping online. Select between: <ul style="list-style-type: none"><li>• <b>None</b></li><li>• <b>Web request</b></li></ul>
<b>Auto refresh</b>	Set the interval for the automatic refresh.
<b>Prompt for offline mode on startup</b>	Every time you will connect to your data source, you will be prompted to use the data source in offline mode.

OPTION	DESCRIPTION
<b>Auto go offline</b>	If the ping online method doesn't work it will automatically go offline.
<b>Disable lock</b>	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.

#### 5.4.1.2 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 SQL Azure** 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

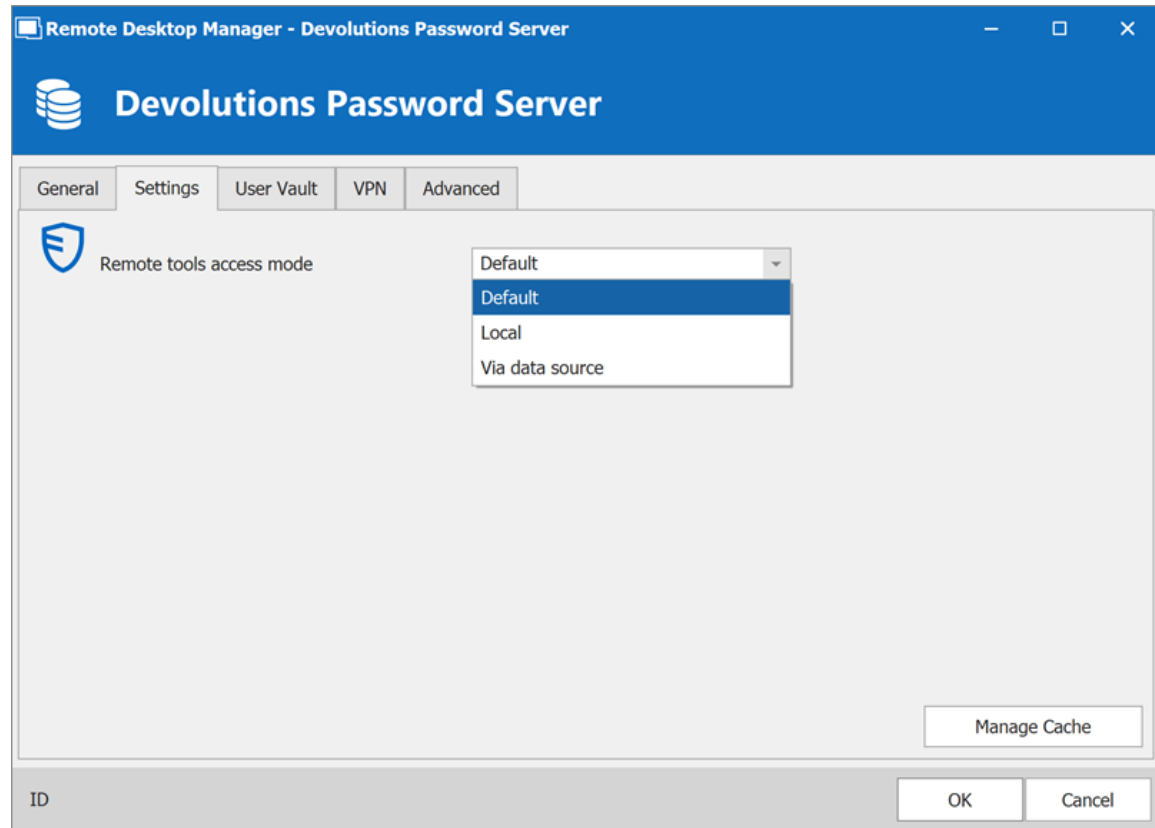
### GENERAL

The screenshot shows the 'Remote Desktop Manager - Devolutions Password Server' window. The title bar is blue with the application icon and name. Below the title bar is a blue header with the 'Devolutions Password Server' logo and name. The main area has a tabbed interface with 'General', 'Settings', 'User Vault', 'VPN', and 'Advanced'. The 'General' tab is active, showing a shield icon and several input fields: 'Name' (text box), 'Host' (dropdown menu), 'Username' (dropdown menu), and 'Password' (text box). There are also three checkboxes: 'Use Windows authentication', 'Use Office365 authentication', and 'Prompt for credentials'. At the bottom of the main area is a 'Test Connection' button. The footer bar is grey and contains an 'ID' label, an 'OK' button, and a 'Cancel' button.

*Devolutions Server - General*

OPTION	DESCRIPTION
<b>Name</b>	Enter a name for the data source.
<b>Host</b>	Enter the URL of the DVLS instance.  Example: <code>http://&lt;hostname or IP address&gt;/&lt;instance name&gt;</code>
<b>Use Windows authentication</b>	Use the same credentials as your current Windows user.
<b>Use Office365 authentication</b>	Use the same credentials as your current Office365 user. Choose an authentication option: <ul style="list-style-type: none"><li>• <b>Default:</b> Create a new authentication token each time and keeps it in the memory only.</li><li>• <b>Persistent:</b> Takes the saved token, if it does not exist, will create a new one and save it.</li><li>• <b>Linked account:</b> Takes a saved token from Windows (registry).</li></ul>
<b>Always prompt for credentials</b>	Always ask for the username and password when connecting to the data source.
<b>Username</b>	Enter the username to connect to the data source.
<b>Password</b>	Enter the password to connect to the data source.
<b>Always ask password</b>	Always ask for the password when connecting to the data source.
<b>Test Connection</b>	Test the connection with Devolutions Server to validate the credentials.

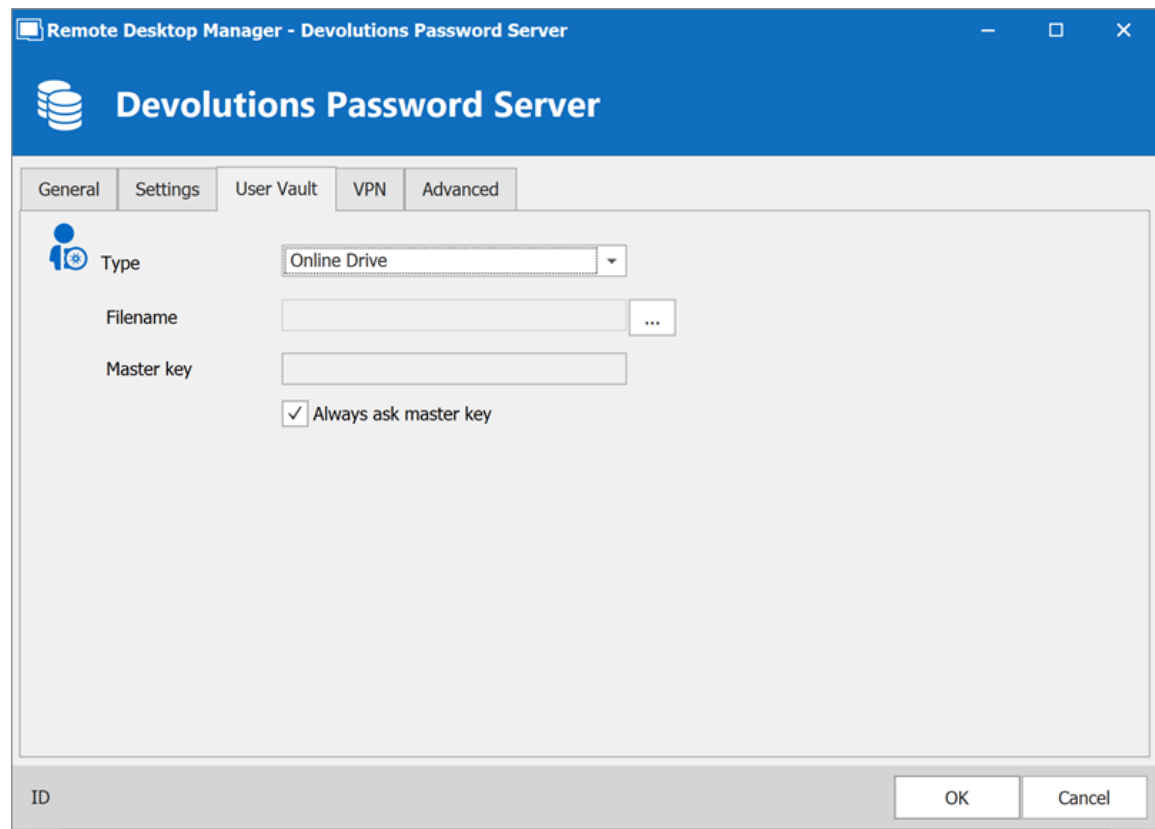
## SETTINGS



*Devolutions Server - Settings*

OPTION	DESCRIPTION
<b>Remote tools access mode</b>	Select whether the Remote Tools will be accessed locally or through the host.
<b>Manage Cache</b>	Manage the data source cache. On large data sources caching is a must and will increase performance significantly. For more information, please consult the <a href="#">Manage Cache</a> topic.

## USER VAULT

*Devolutions Server – User Vault*

OPTION	DESCRIPTION
<b>Type</b>	Select the type of <a href="#">User Vault</a> to use. Select between: <ul style="list-style-type: none"><li>• <b>Default:</b> use the default User Vault, which is stored in the database.</li><li>• <b>None:</b> disable the User Vault for all users.</li><li>• <b>Online Drive:</b> use a Devolutions Online Drive file (*.dod) as a User Vault.</li></ul>

## VPN

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



The screenshot shows the 'Remote Desktop Manager - Devolutions Password Server' window with the 'VPN' tab selected. The window has a blue header with the Devolutions logo and title. Below the header is a tab bar with 'General', 'Settings', 'User Vault', 'VPN', and 'Advanced'. The 'VPN' tab contains a 'Type' dropdown menu set to 'On first connect', an 'RDM File' text box with a browse button (...), and an 'Override credentials' checkbox. Below the checkbox are three text boxes for 'Username', 'Domain', and 'Password'. At the bottom of the window is an 'ID' label and 'OK' and 'Cancel' buttons.

Remote Desktop Manager - Devolutions Password Server

Devolutions Password Server

General Settings User Vault VPN Advanced

Type On first connect

RDM File

☐ Override credentials

Username

Domain

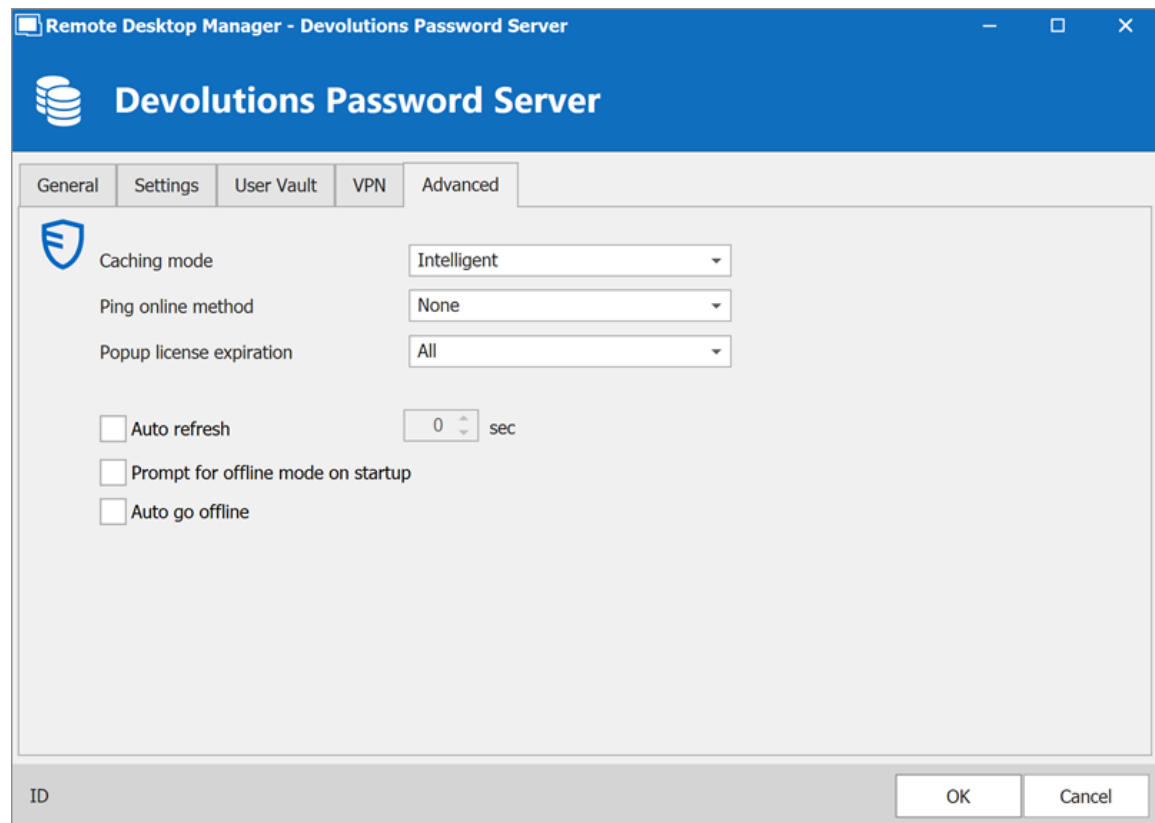
Password

ID

OK Cancel

*Devolutions Server - VPN*

## ADVANCED

*Devolutions Server - Advanced*

OPTION	DESCRIPTION
<b>Caching mode</b>	Determines how the entries will be reloaded in the data source. For more information, please consult the <a href="#">Caching</a> topic.
<b>Ping online method</b>	Indicate the preferred ping online method. Select between: <ul style="list-style-type: none"> <li>• <b>None</b></li> <li>• <b>Web request</b></li> </ul>
<b>Popup license expiration</b>	Determine how the application advises of the license expiration. Select between: <ul style="list-style-type: none"> <li>• <b>All</b></li> <li>• <b>Only Administrator(s)</b></li> <li>• <b>Disabled</b></li> </ul>

OPTION	DESCRIPTION
<b>Auto refresh</b>	Set the interval for the automatic refresh.
<b>Prompt for offline mode on startup</b>	Ask to use the data source in offline mode when the user connects to the data source.
<b>Auto go offline</b>	Use the data source in offline mode when the ping method does not respond.
<b>Disable lock</b>	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.

#### 5.4.1.3 MariaDB

### DESCRIPTION



Remote Desktop Manager uses **MariaDB** as a drop-in replacement for **MySQL**. It is only supported in the Enterprise edition.



For added security, you can enable SSL Encryption to communicate with your instance of MariaDB Server.

Please follow directions on <https://dev.mysql.com/doc/connector-net/en/connector-net-6-10-connection-options.html>.

### HIGHLIGHTS

- The data can be shared on a MariaDB database installed on any Operating System MySQL supports.

- Full connection log and attachments support.

## SETTINGS

### GENERAL

The screenshot shows the 'Remote Desktop Manager - MariaDB' window. The 'General' tab is selected, showing fields for Name, Host, Port (3306), Username, Password, and Schema. There are checkboxes for 'Always ask password' and 'Allow change username'. The 'Two factor' option is set to 'None'. At the bottom right are 'Test Host' and 'Test Schema' buttons. At the bottom left is an 'ID' field. At the bottom right are 'OK' and 'Cancel' buttons.

*MariaDB - General*

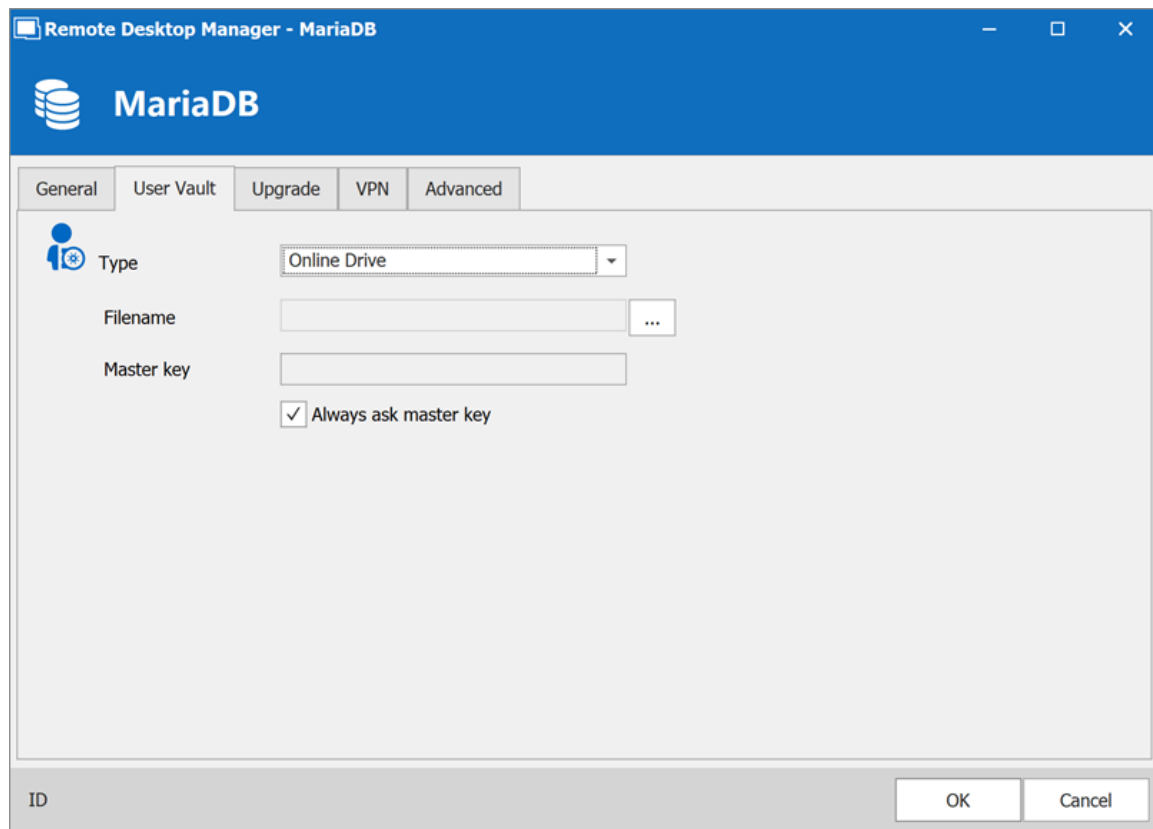
OPTION	DESCRIPTION
<b>Name</b>	Name of the data source.
<b>Host</b>	Name of the host (server name) where the data source will be stored.

OPTION	DESCRIPTION
<b>Username</b>	Username used to access the host server.
<b>Password</b>	Password used to access the host server.
<b>Always ask password</b>	Always prompts for the user to input a password when connecting to the data source.
<b>Allow change username</b>	Allows the user to change the username. This specific setting will save the currently type username (unlike similar features such as "Always prompt for credentials").
<b>Schema</b>	Name of the schema (database) on the MySQL server.
<b>Two factor</b>	Enable the <a href="#">2-Factor Authentication</a> to access your data source.
<b>Test Host</b>	Test the connection with the host (server name) to validate if the proper information has been provided.
<b>Test Schema</b>	Test the connection with the schema to validate if the proper information has been provided.

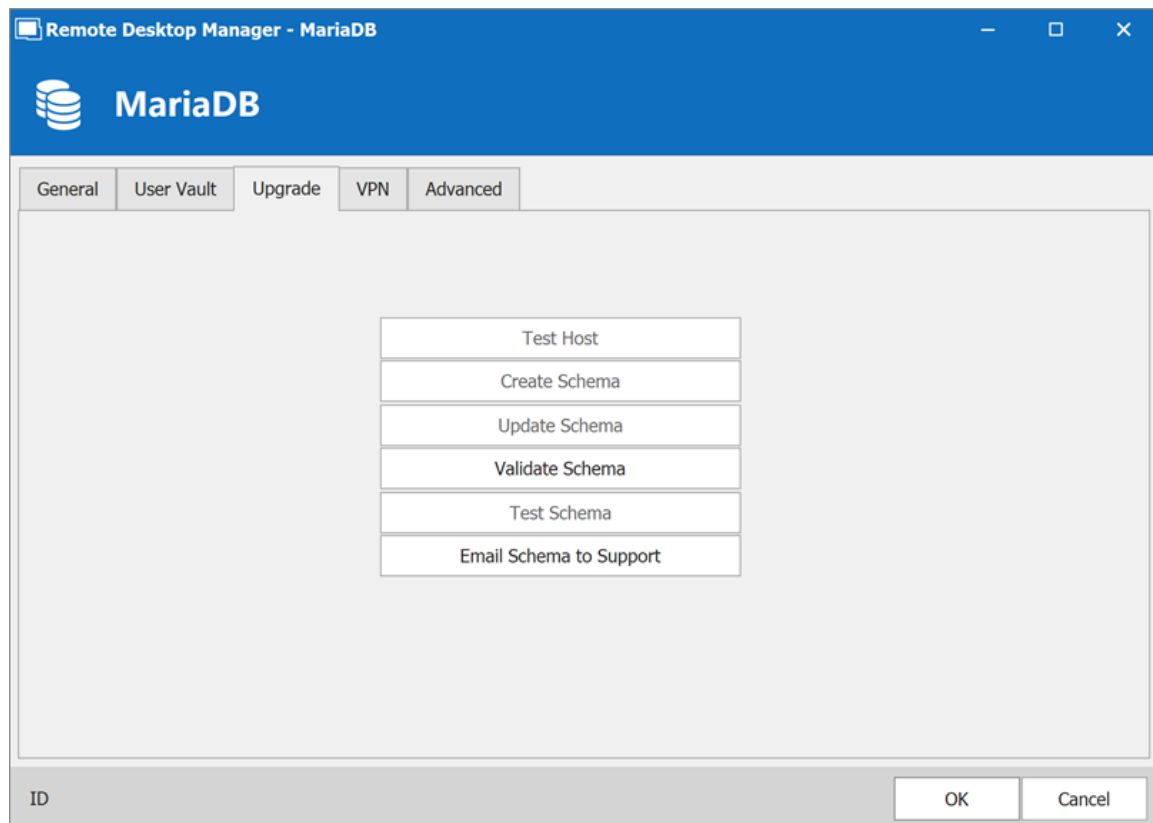
## USER VAULT

Connect your **MariaDB** to a **User Vault** stored in a **Devolutions Online Drive** file (.dod), thus creating your own **User Vault** containing entries and credentials that no one else has access to.

For more information please see [User Vault](#).

*MariaDB - User Vault*

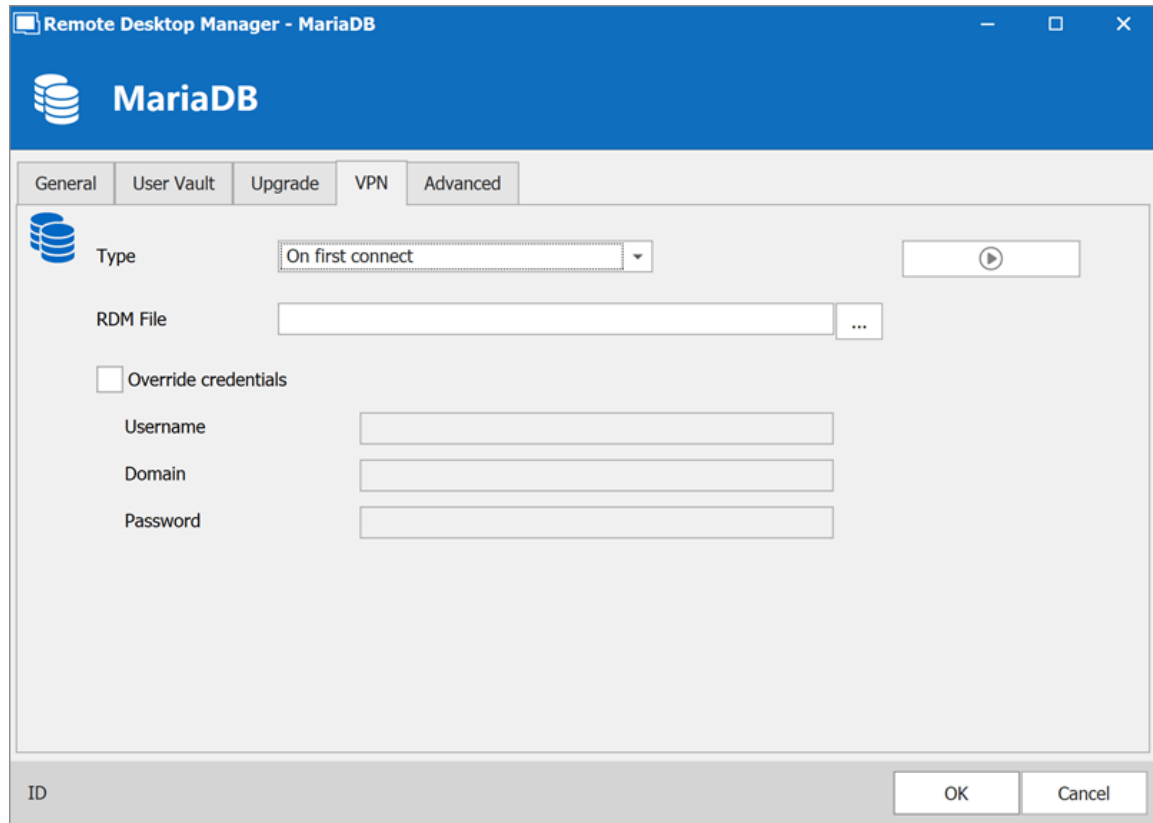
## UPGRADE

*MariaDB - Upgrade Tab*

OPTION	DESCRIPTION
<b>Test Host</b>	Test the connection with the Host (server name) to validate if the proper information has been provided.
<b>Create Schema</b>	Create the schema (database) on the MariaDB server to use Remote Desktop Manager.
<b>Update Schema</b>	Update the schema (database) on the MariaDB server, if required, to use Remote Desktop Manager.
<b>Test Schema</b>	Test the connection with the schema (database) to validate if the proper information has been provided.
<b>Email Schema to Support</b>	Send your schema (database) to the Devolutions Support team.

## VPN

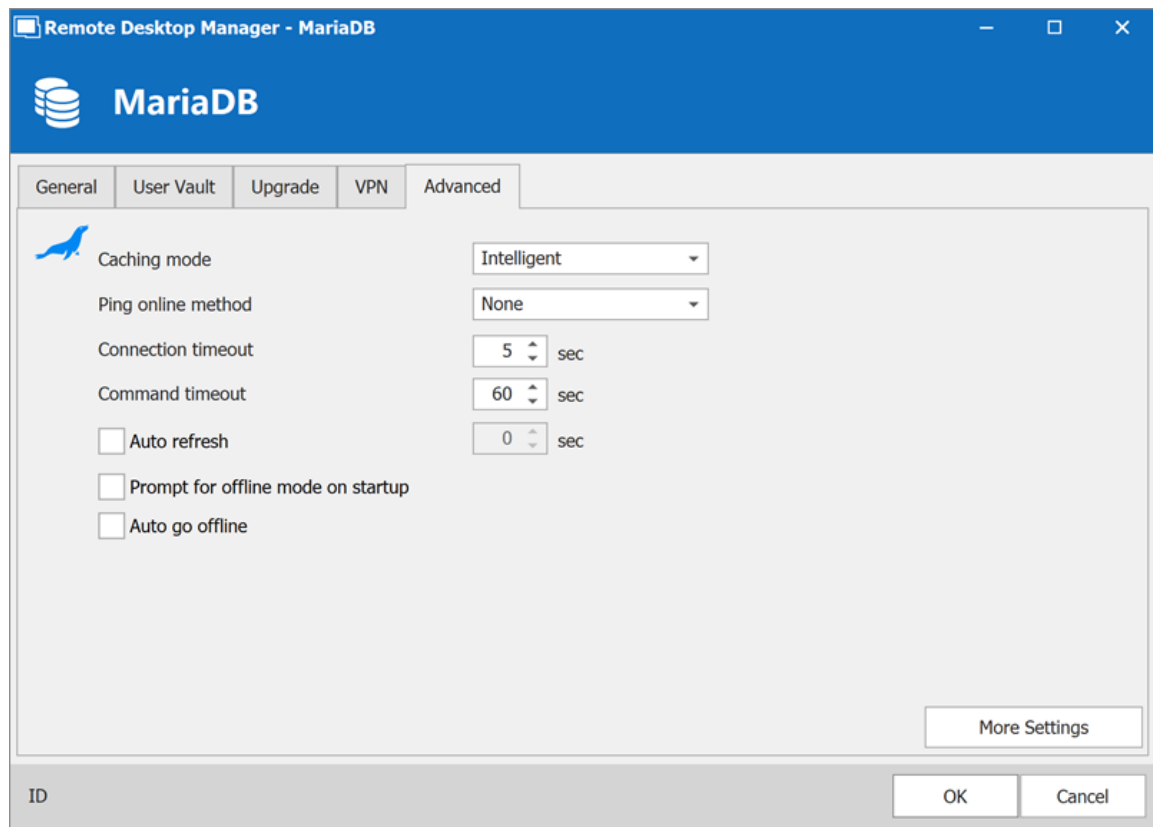
Open a VPN to access your data prior to connecting to your **MariaDB**.



*MariaDB - VPN*

## ADVANCED





MariaDB - Advanced

OPTION	DESCRIPTION
<b>Caching mode</b>	Determine how the entries will be reloaded in the data source. See <a href="#">Caching</a> topic for more information.
<b>Ping online method</b>	Indicate the prefer ping online. Select between: <ul style="list-style-type: none"> <li>• <b>None</b></li> <li>• <b>Port Scan</b></li> </ul>
<b>Connection timeout</b>	Waiting time before a connection timeout.
<b>Command timeout</b>	Waiting time before a command timeout.

OPTION	DESCRIPTION
<b>Auto refresh</b>	Set the interval for the automatic refresh.
<b>Prompt for offline mode on startup</b>	Every time you will connect to your data source, you will be prompted to use the data source in offline mode.
<b>Auto go offline</b>	If the ping online method doesn't work it will automatically go offline.
<b>Disable lock</b>	Disable the option to lock the data source directly. You can still lock the application but you won't be prompted for the database password if this option is disabled.
<b>More Settings</b>	Directly edit the connection string values.

#### 5.4.1.4 MySQL

### DESCRIPTION



Remote Desktop Manager uses a MySQL database to store the session data. It is only supported in the Enterprise edition.



For added security, you can enable SSL Encryption to communicate with your instance of MySQL Server.

Please follow directions in those links;

- <https://dev.mysql.com/doc/connector-net/en/connector-net-tutorials-ssl.html>
- <https://dev.mysql.com/doc/connector-net/en/connector-net-6-10-connection-options.html>



We recommend using MySQL version 5.5.62 for this data source.

## HIGHLIGHTS

- The data can be shared on a MySQL database installed on any Operating System MySQL supports.
- Full connection log and attachment support.
- Integrated Security support (Requires a v5.5.16 commercial distribution of MySQL).

## SETTINGS

### GENERAL

The screenshot shows the 'Remote Desktop Manager - MySQL' dialog box with the 'General' tab selected. The dialog has a blue header with the MySQL logo. Below the header are tabs for 'General', 'User Vault', 'Upgrade', 'VPN', and 'Advanced'. The 'General' tab contains the following fields and options:

- Name:** A text input field.
- Host:** A text input field.
- Port:** A spinner box set to 3306.
- Integrated security:** A checkbox.
- Username:** A text input field.
- Password:** A text input field.
- Always ask password:** A checkbox.
- Allow change username:** A checkbox.
- Schema:** A text input field with a dropdown arrow.
- Two factor:** A dropdown menu set to 'None'.

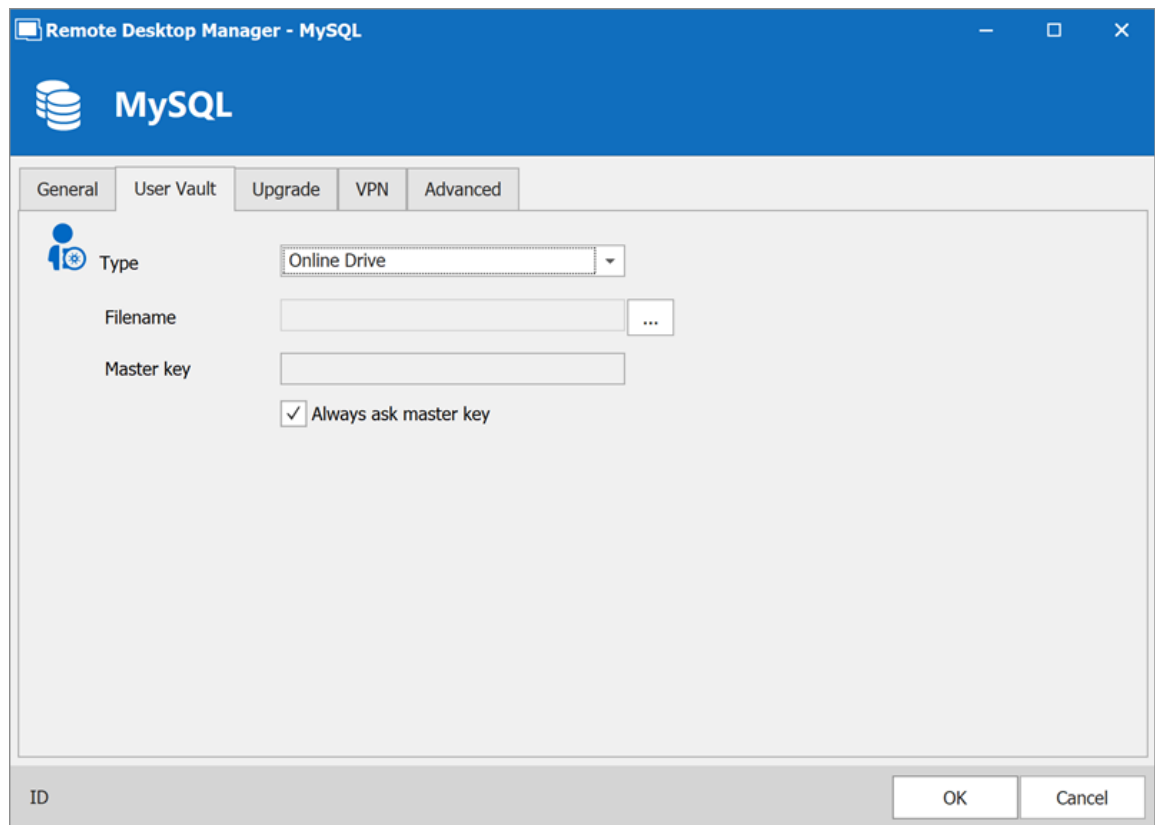
At the bottom right of the dialog are buttons for 'Test Host', 'Test Schema', 'OK', and 'Cancel'. The 'ID' field is visible at the bottom left.

*MySQL - General Tab*

OPTION	DESCRIPTION
<b>Name</b>	Name of the data source.
<b>Host</b>	Name of the server where the data source will be store.
<b>Port</b>	If not using the default port, enter your Port number.
<b>Integrated Security</b>	When enabling the Integrated Security, the user and password field will be disabled because the operating system will provide a cached copy automatically. Please see <a href="#">Integrated Security</a> for more information.
<b>Username</b>	Username to access the MySQL server.
<b>Password</b>	Password to access the MySQL server.

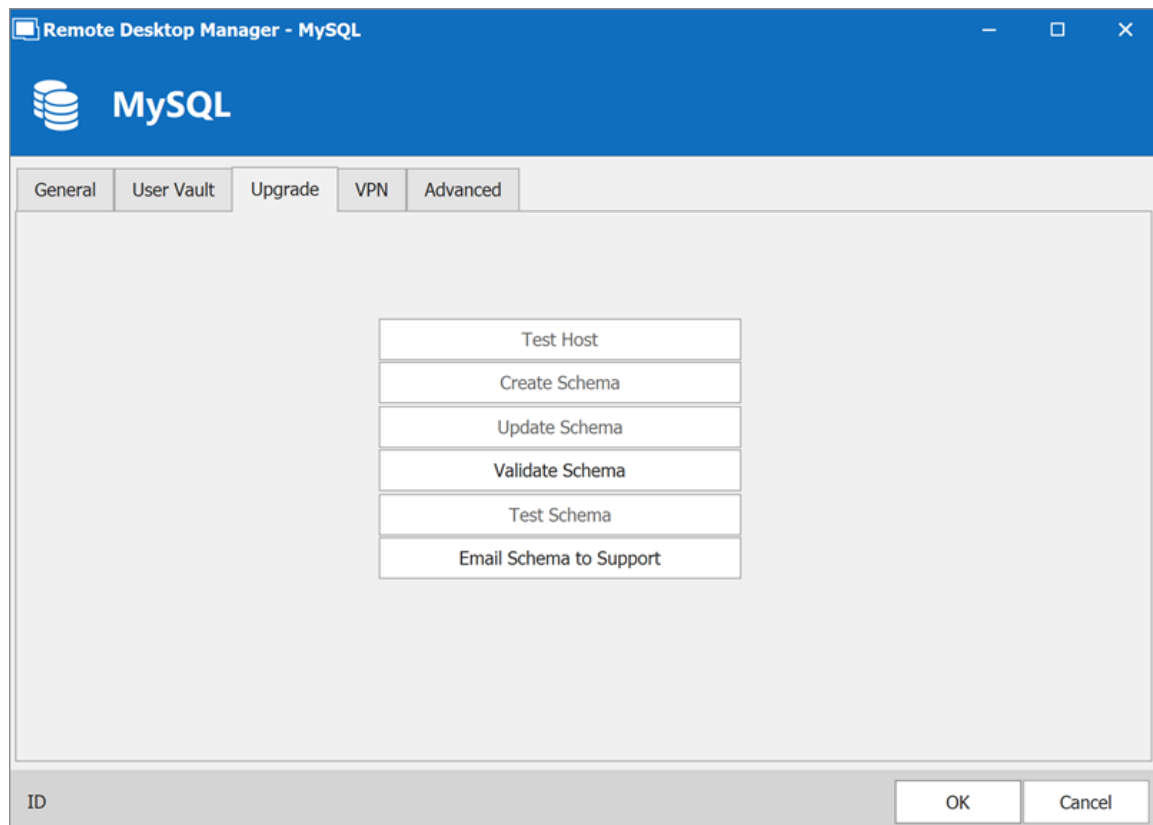
OPTION	DESCRIPTION
<b>Always ask password</b>	Prompt for the password when a user connects to the data source.
<b>Allow change username</b>	Allow the username to be edited when connecting to the data source. (Only with Always ask password enabled)
<b>Schema</b>	Name of the schema on the MySQL server for the utilization of Remote Desktop Manager.
<b>Two factor</b>	Enable the <a href="#">2-Factor Authentication</a> to access your data source.
<b>Test Host</b>	Test the connection with the Host (server) to validate if the proper information has been provided.
<b>Test Schema</b>	Test the connection with the schema to validate if the proper information has been provided

## USER VAULT

*MySQL - User Vault Tab*

OPTION	DESCRIPTION
Type	<p>Select the type of <a href="#">User Vault</a> to use. Select between:</p> <ul style="list-style-type: none"><li>• <b>Default:</b> use the default User Vault, which is stored in the database.</li><li>• <b>None:</b> disable the User Vault for all users.</li><li>• <b>Online Drive:</b> use a Devolutions Online Drive file (*.dod) as a User Vault.</li></ul>

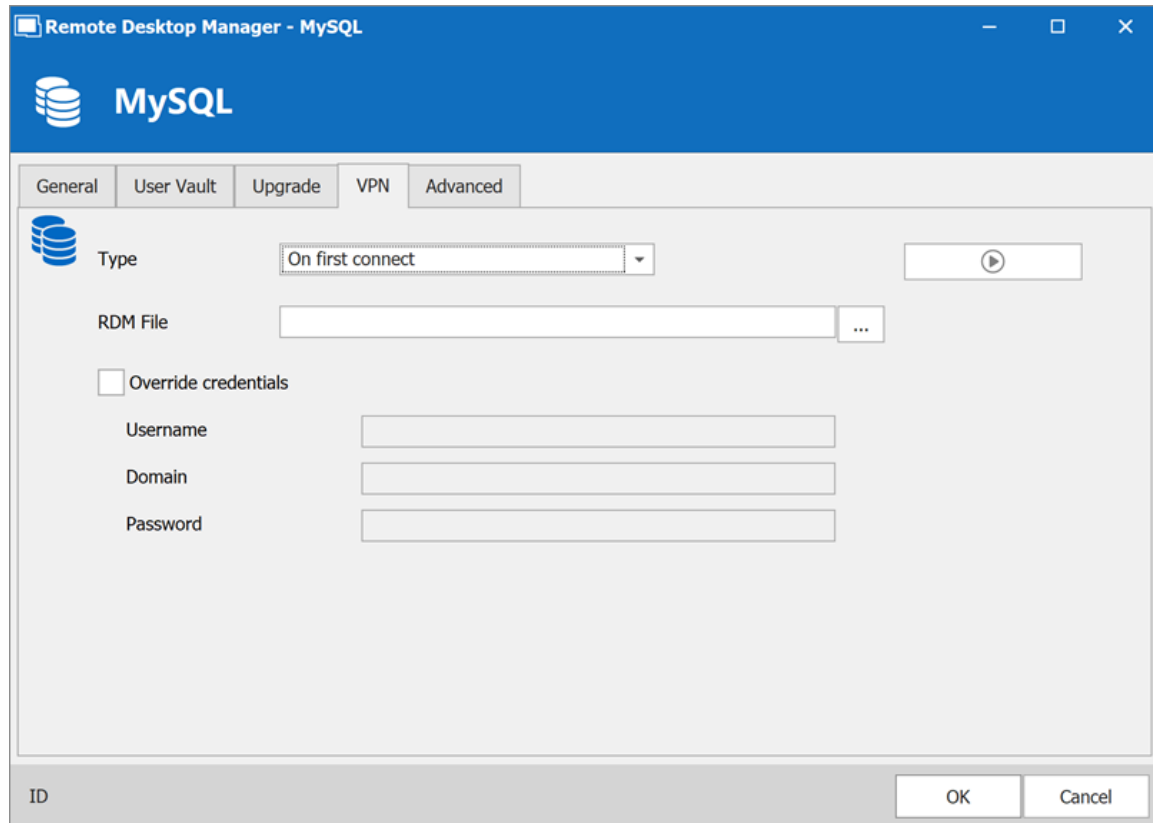
## UPGRADE

*MySQL - Upgrade Tab*

OPTION	DESCRIPTION
<b>Test Host</b>	Test the connection with the host (server) to validate if the proper information has been provided.
<b>Create Schema</b>	Create the schema on the MySQL server to use Remote Desktop Manager.
<b>Update Schema</b>	Update the schema on the MySQL server, if required, to use Remote Desktop Manager.
<b>Test Schema</b>	Test the connection with the schema to validate if the proper information has been provided.
<b>Email Schema to Support</b>	Send your schema to the Devolutions Support team.

## VPN

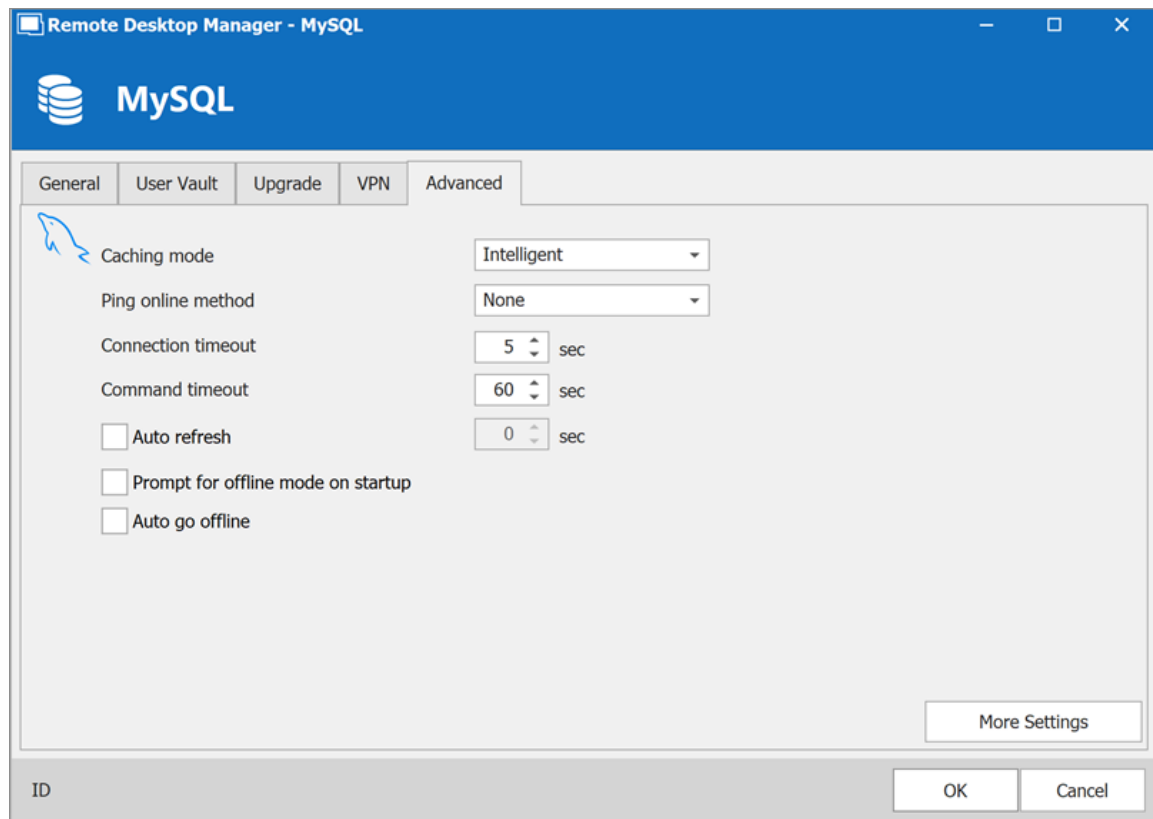
Open a VPN to access your data prior to connecting to your **MySQL** database.



MySQL - VPN Tab

## ADVANCED





MySQL - Advanced Tab

OPTION	DESCRIPTION
<b>Caching mode</b>	Determine how the entries will be reload in the data source. See <a href="#">Caching</a> topic for more information.
<b>Ping online method</b>	Indicate the preferred ping online method. Select between: <ul style="list-style-type: none"> <li>• <b>None</b></li> <li>• <b>Ping</b></li> <li>• <b>Port Scan</b></li> </ul>
<b>Connection timeout</b>	Waiting time before a connection timeout.
<b>Command timeout</b>	Waiting time before a command timeout.

OPTION	DESCRIPTION
<b>Auto refresh</b>	Set the interval for the automatic refresh
<b>Prompt for offline mode on startup</b>	Every time you will connect to your data source, you will be prompted to use the data source in offline mode.
<b>Auto go offline</b>	If the ping online method doesn't work it will automatically go offline.
<b>Disable lock</b>	Disable the option to lock the data source directly. You can still lock the application but you won't be prompted for the database password if this option is disabled.
<b>More Settings</b>	Edit the connection string values directly.

## TROUBLESHOOTING

Consult MySQL troubleshooting for more information.

### 5.4.1.5 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.

## CONFIGURATION

Consult the [Configure SQL Server](#) topic for more information on the configuration.

## SETTINGS

### GENERAL

Remote Desktop Manager - Microsoft SQL Server

**Microsoft SQL Server**

General Settings User Vault Upgrade VPN Advanced

Name

Host

Login mode

Username

Password

☐ Always ask password

☐ Allow change username

Database

Two factor [None](#)

Test Host

Test Database

ID

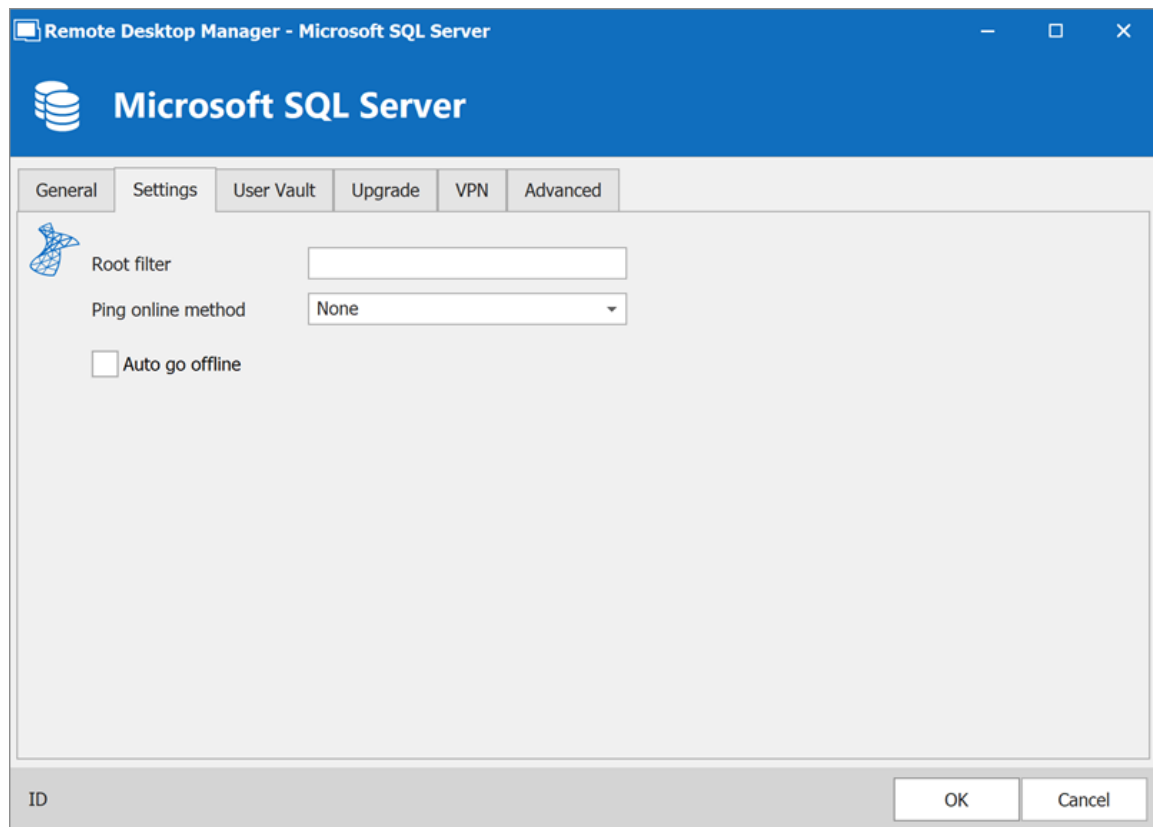
OK Cancel

Microsoft SQL Server - General Tab

OPTION	DESCRIPTION
<b>Name</b>	Enter a name for the data source.
<b>Host</b>	Enter the server hostname or IP address.
<b>Login mode</b>	Specify the authentication mode to use. Select between: <ul style="list-style-type: none"> <li>• <b>Database login</b></li> <li>• <b>Integrated Security (Active directory)</b></li> <li>• <b>Custom Login</b></li> </ul>
<b>Username</b>	Enter the username to access the SQL Azure database.
<b>Password</b>	Enter the password to access the SQL Azure database.

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

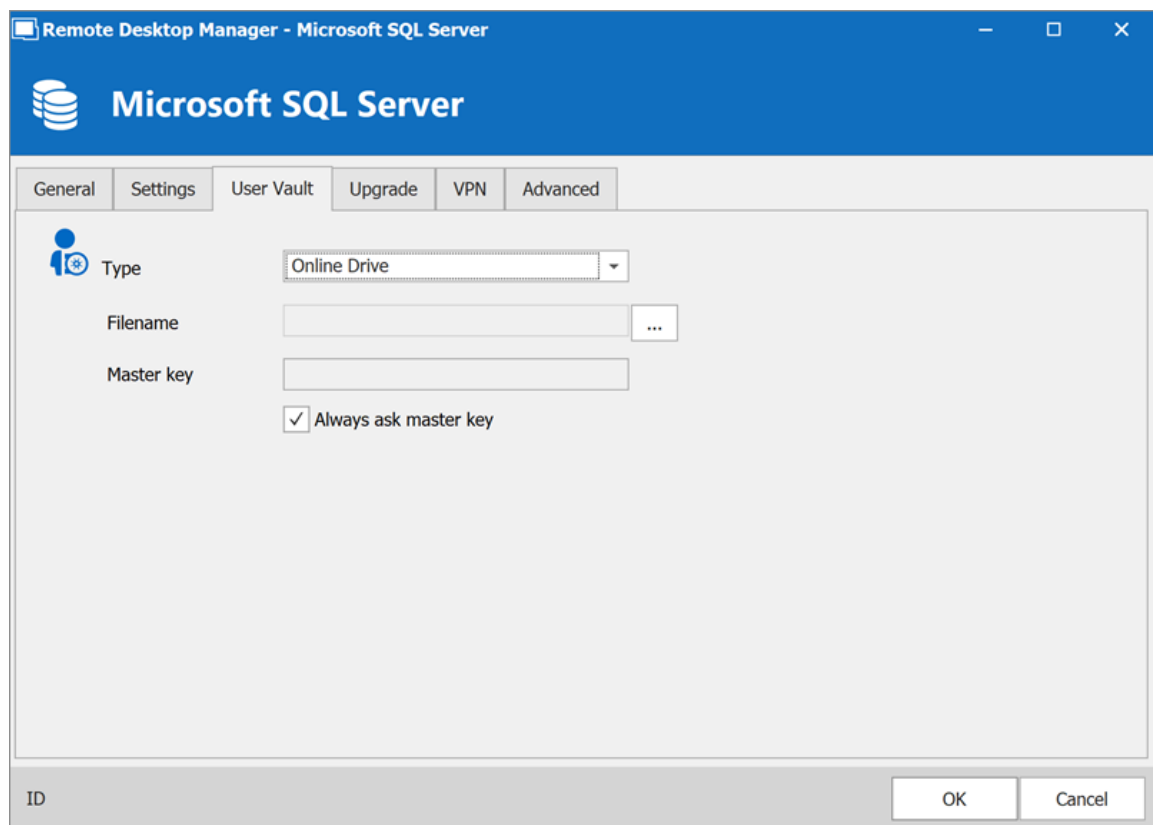
## SETTINGS

*Microsoft SQL Server - Settings Tab*

OPTION	DESCRIPTION
<b>Root filter</b>	Enter the name of a root level folder to display only the entries contained in that folder.
<b>Ping online method</b>	Indicate the preferred ping online method. Select between: <ul style="list-style-type: none"><li>• <b>None</b></li><li>• <b>Ping</b></li><li>• <b>Port Scan</b></li></ul>
<b>Auto go offline</b>	Use the data source in offline mode when the ping method does not respond.

OPTION	DESCRIPTION
<b>Disable lock</b>	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



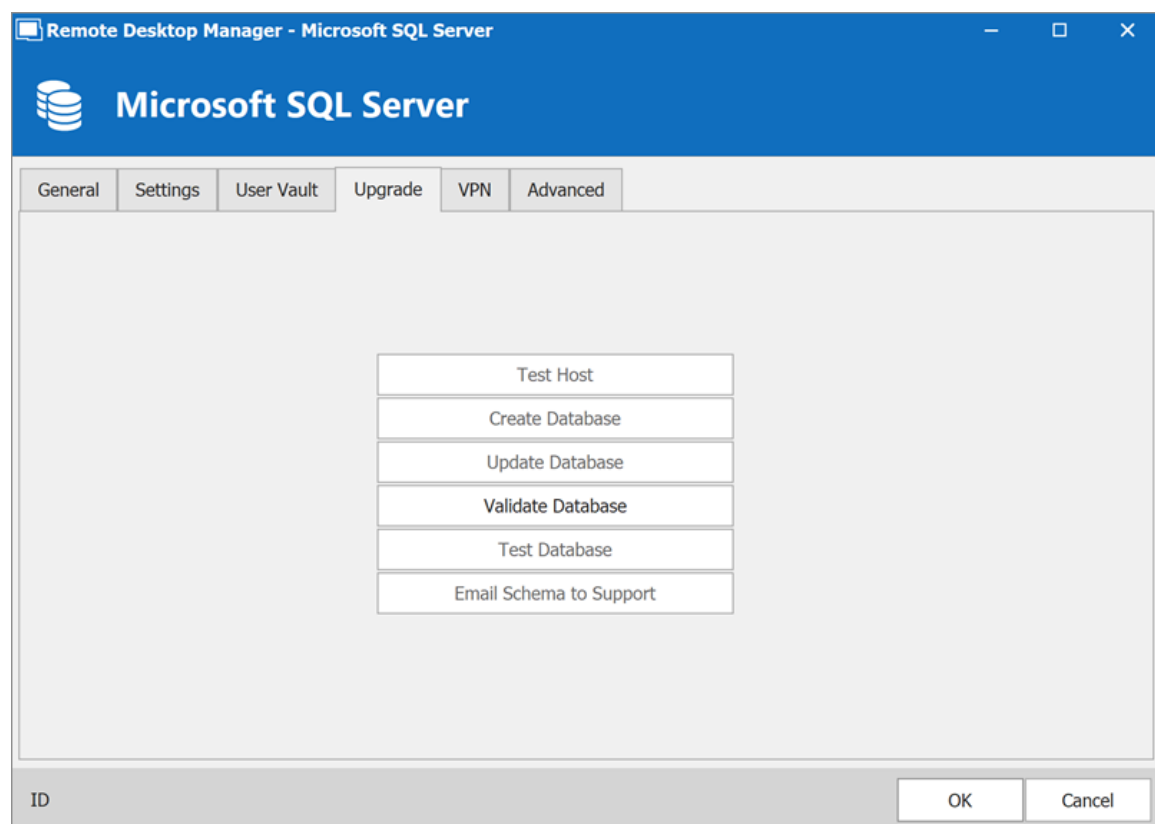
*Microsoft SQL Server - User Vault Tab*

OPTION	DESCRIPTION
<b>Type</b>	<p>Select the type of <a href="#">User Vault</a> to use. Select between:</p> <ul style="list-style-type: none"> <li>• <b>Default:</b> use the default User Vault, which is stored in the database.</li> </ul>



OPTION	DESCRIPTION
	<ul style="list-style-type: none"><li>• <b>None:</b> disable the User Vault for all users.</li><li>• <b>Online Drive:</b> use a Devolutions Online Drive file (*.dod) as a User Vault.</li></ul>

## UPGRADE



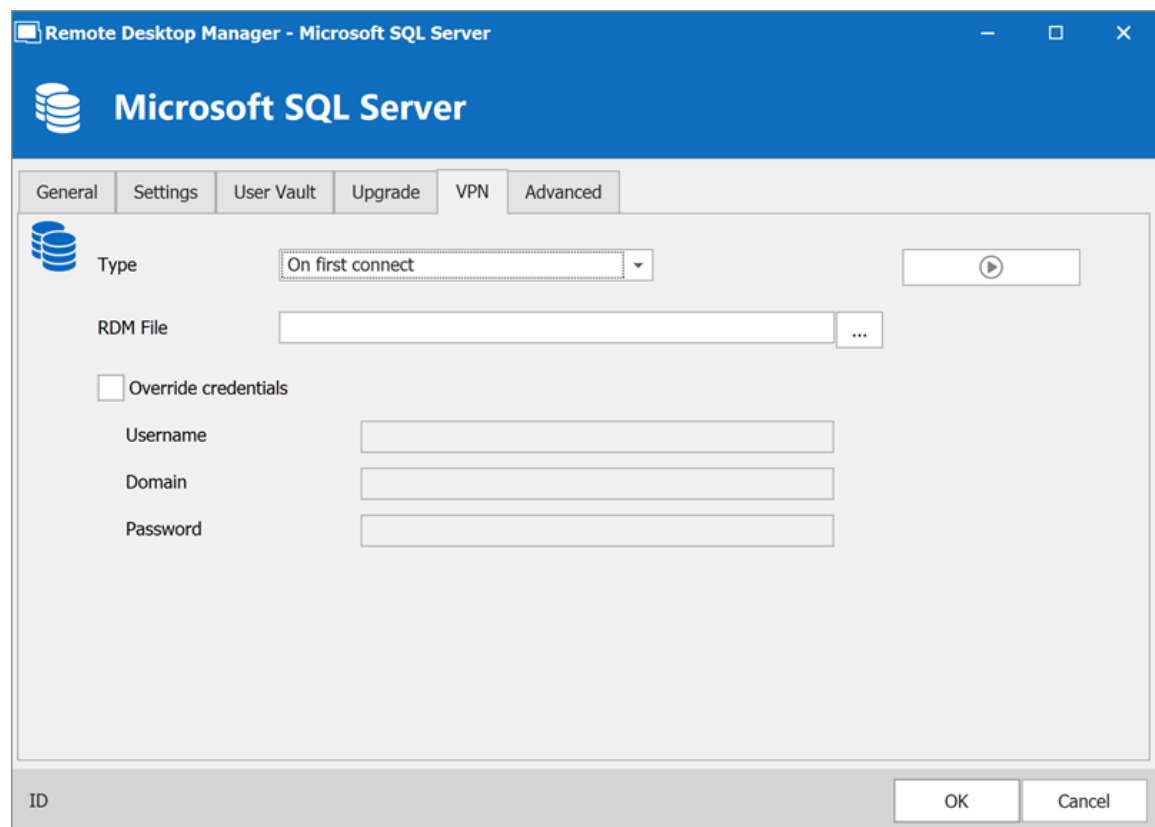
*Microsoft SQL Server - Upgrade Tab*

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

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

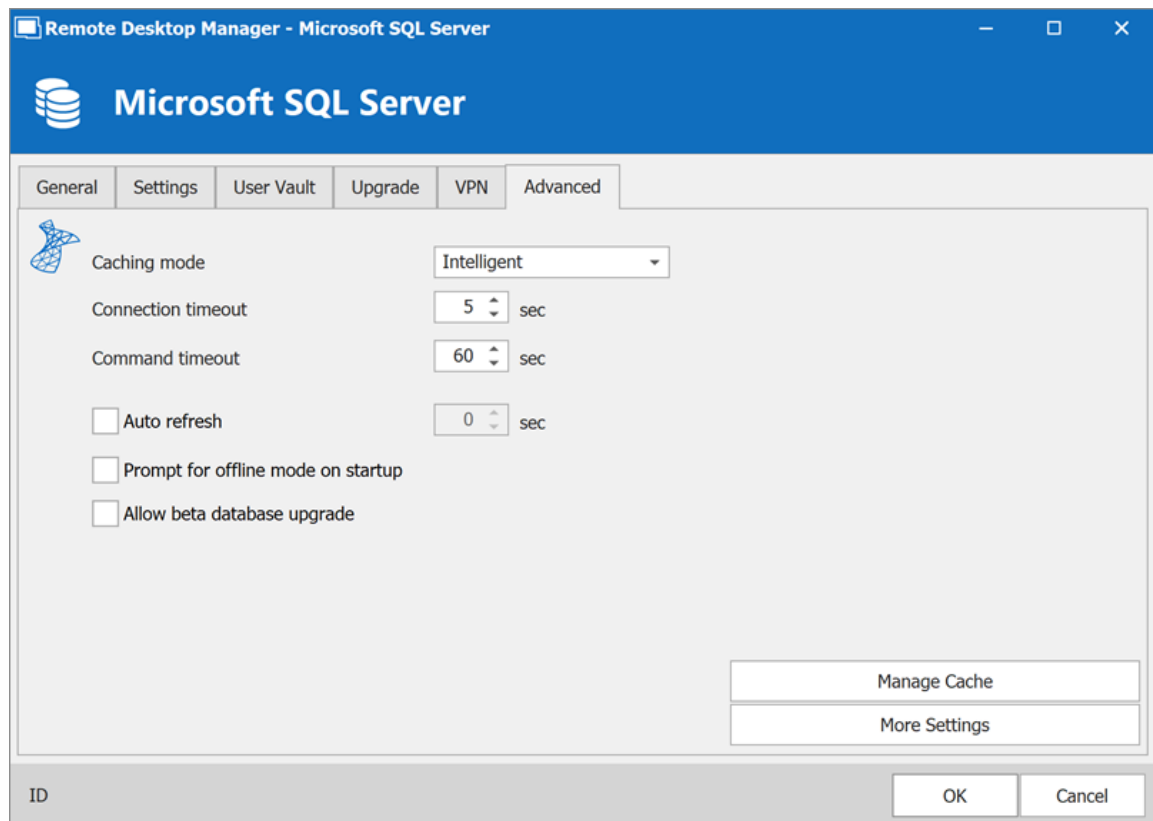
## VPN

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

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

#### 5.4.1.5.1 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.

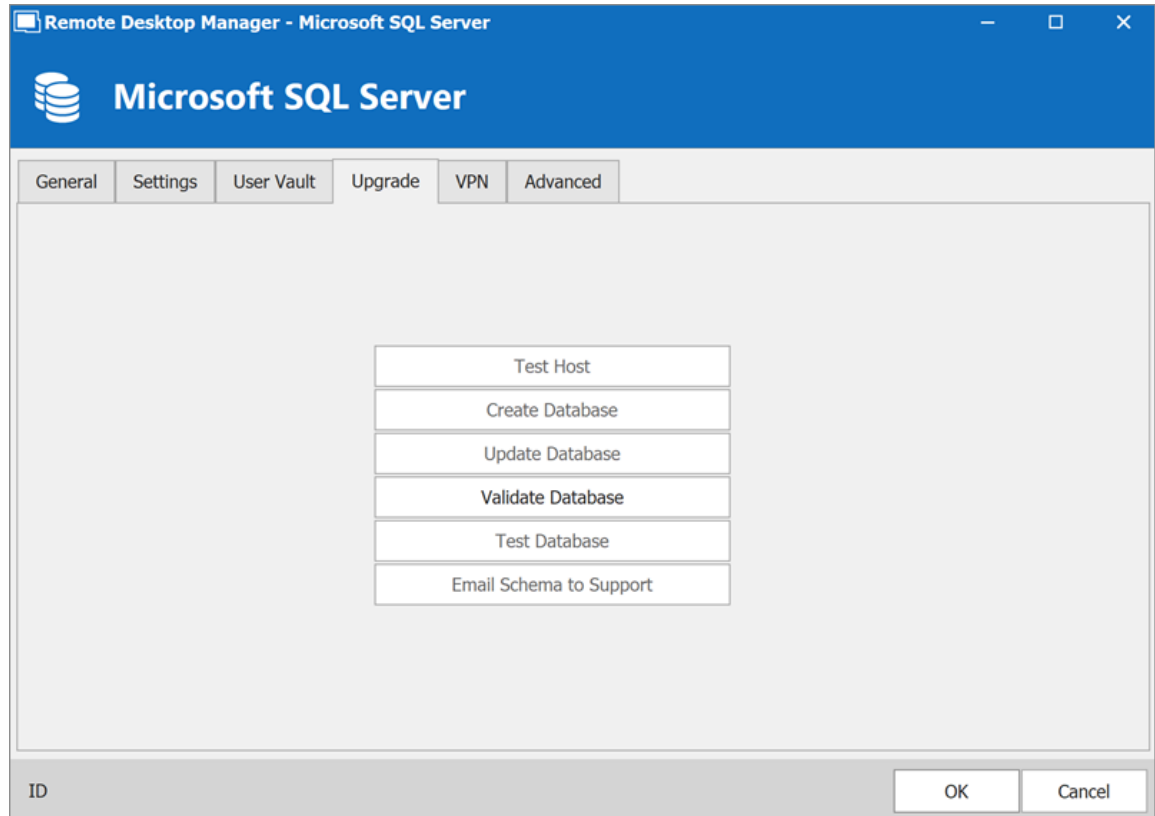


For added security, you can enable SSL Encryption to communicate with your instance of SQL Server. However, due to a framework limitation, this is not compatible with our iOS and Android versions of Remote Desktop Manager.

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.

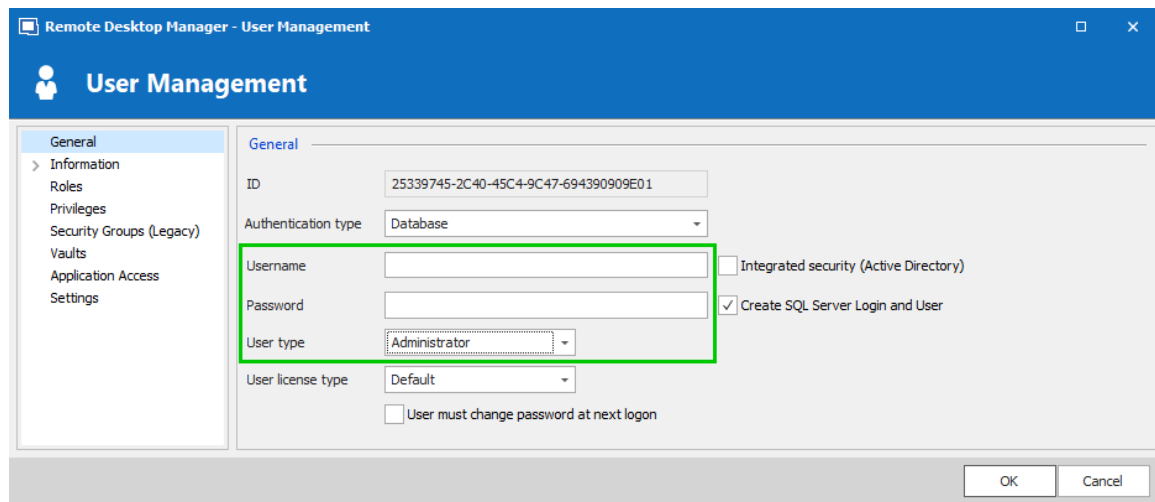


*Upgrade Tab*

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.



Remote Desktop Manager - User Management

User Management

General

Information  
Roles  
Privileges  
Security Groups (Legacy)  
Vaults  
Application Access  
Settings

General

ID: 25339745-2C40-45C4-9C47-694390909E01

Authentication type: Database

Username: [text box]

Password: [text box]

User type: Administrator

User license type: Default

☐ Integrated security (Active Directory)

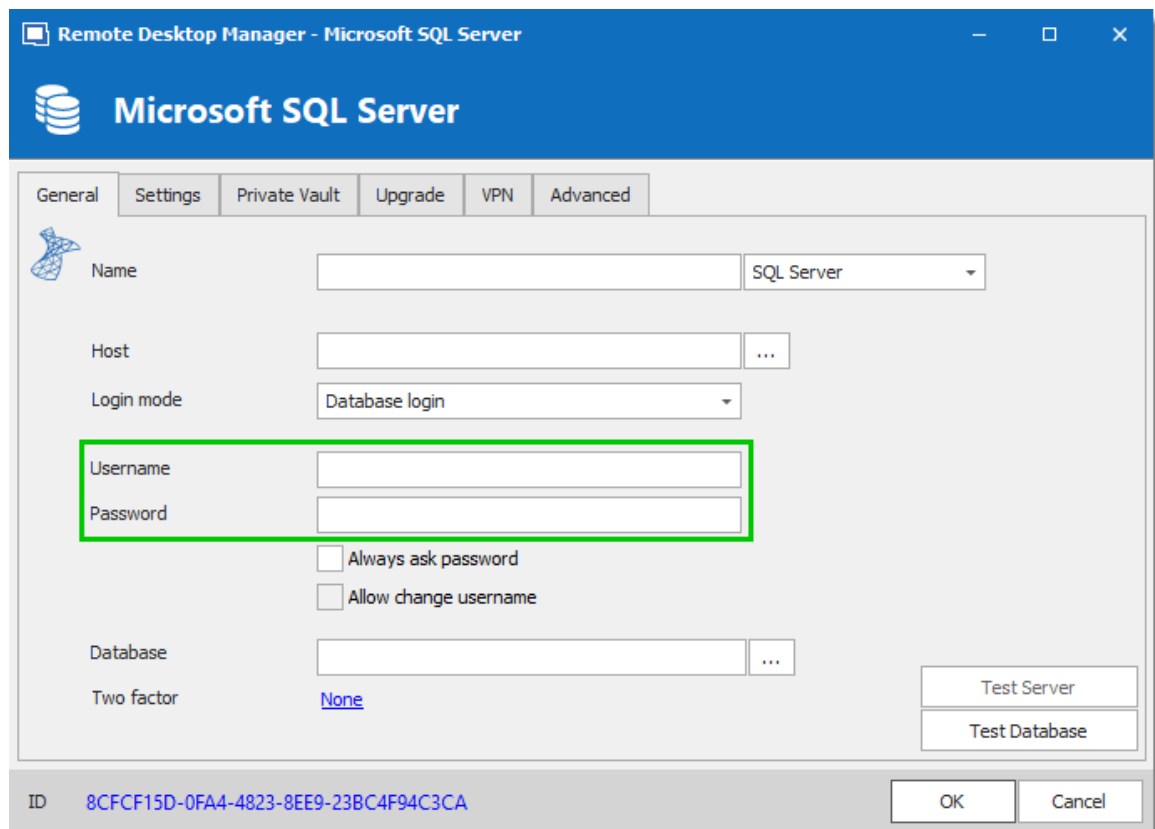
☒ Create SQL Server Login and User

☐ User must change password at next logon

OK Cancel

*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.



Remote Desktop Manager - Microsoft SQL Server

Microsoft SQL Server

General Settings Private Vault Upgrade VPN Advanced

Name: [text box] SQL Server

Host: [text box] ...

Login mode: Database login

Username: [text box]

Password: [text box]

☐ Always ask password

☐ Allow change username

Database: [text box] ...

Two factor: None

Test Server

Test Database

ID: 8CFCF15D-0FA4-4823-8EE9-23BC4F94C3CA

OK Cancel

*Connection to the Database with the RDM Administrator Account*

The Microsoft SQL Server data source is now correctly configured.

## 5.4.1.5.2 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>.

## 5.4.1.5.3 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.

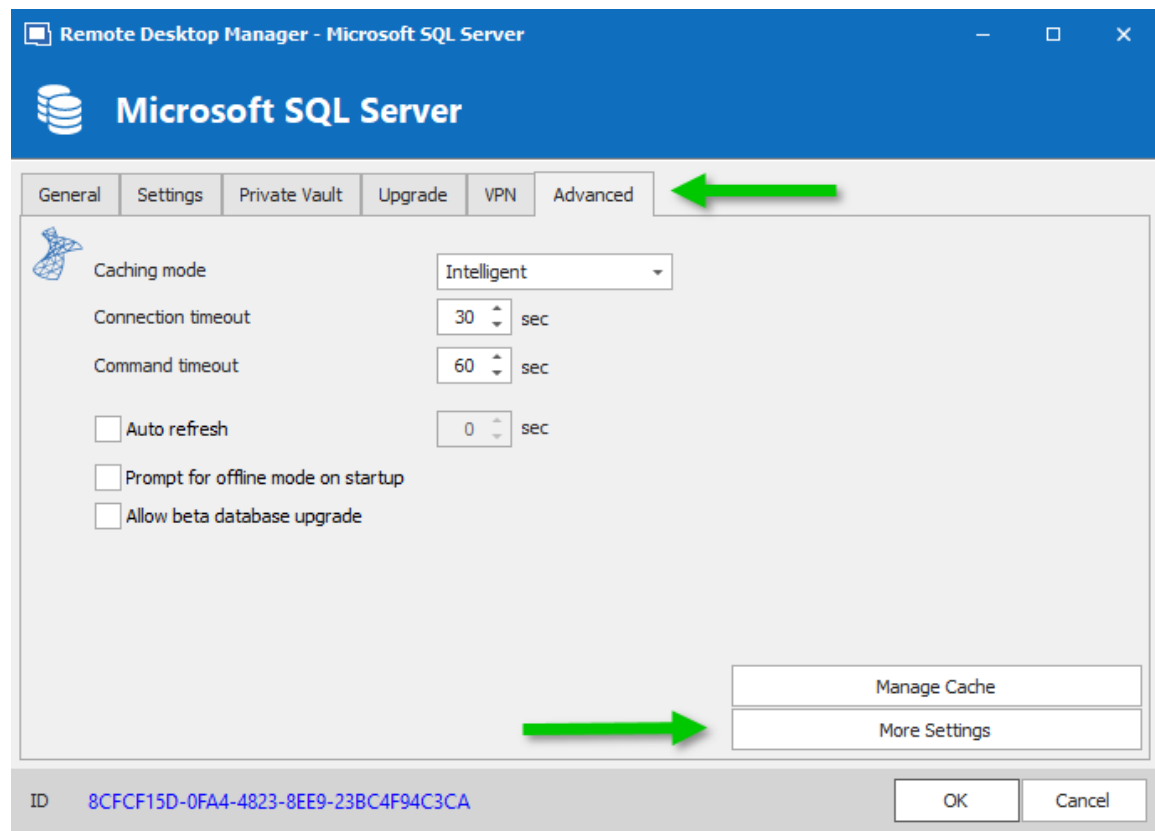
Please consult this Microsoft technet article that provides detailed instructions: [Encrypting Connections to SQL Server \(technet\)](#).

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.

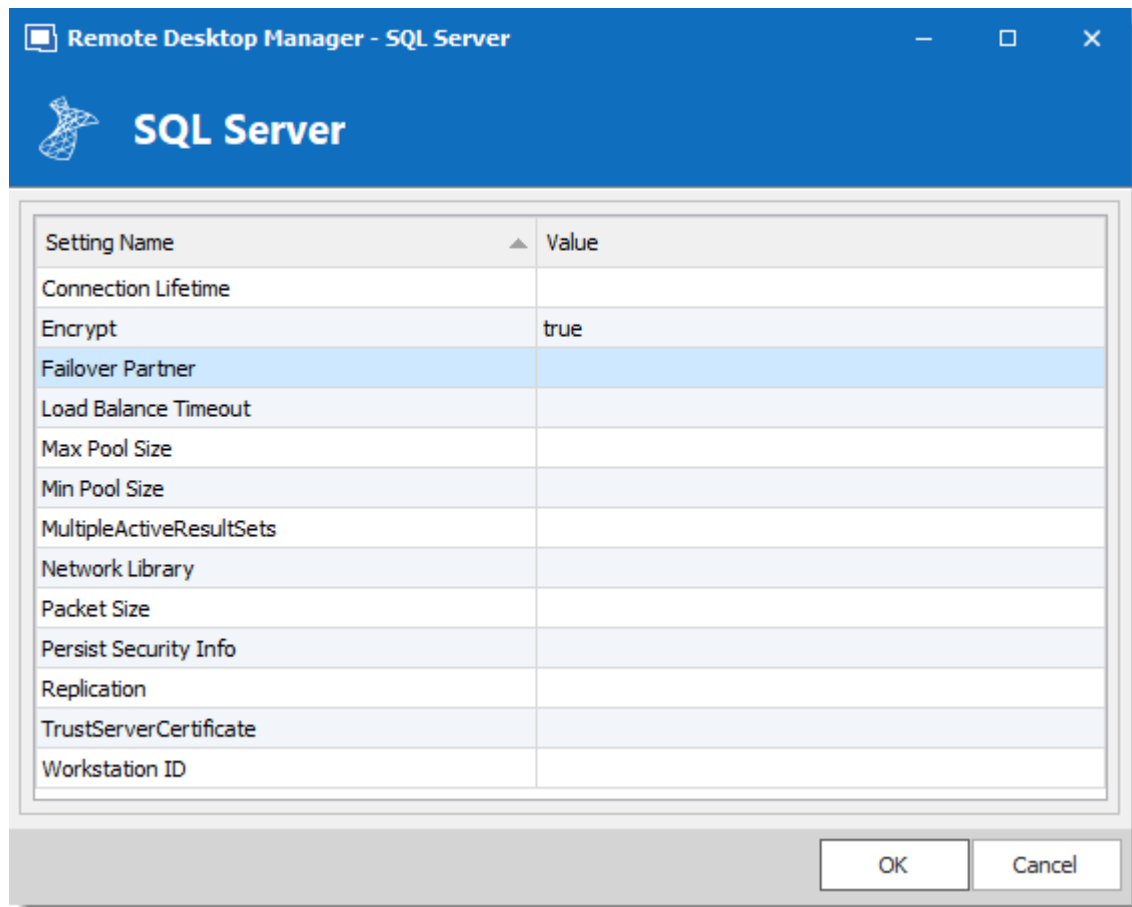
## PROCEDURE



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.



#### 5.4.1.6 Microsoft SQL Azure

### DESCRIPTION



With the Microsoft SQL Azure 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 SQL Azure 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.
- Used to create an online database. [Get more information on Microsoft SQL Azure](#).



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 SQL Azure](#) topic for more information on the configuration.

### SETTINGS

## GENERAL

Remote Desktop Manager - Microsoft SQL Azure

**Microsoft SQL Azure**

General Settings User Vault Upgrade VPN Advanced

Name  Microsoft SQL Azure ▼

Host  ...

Login mode Database login ▼

Username

Password

☐ Always ask password

☐ Allow change username

Database  ...

Two factor [None](#)

Test Database

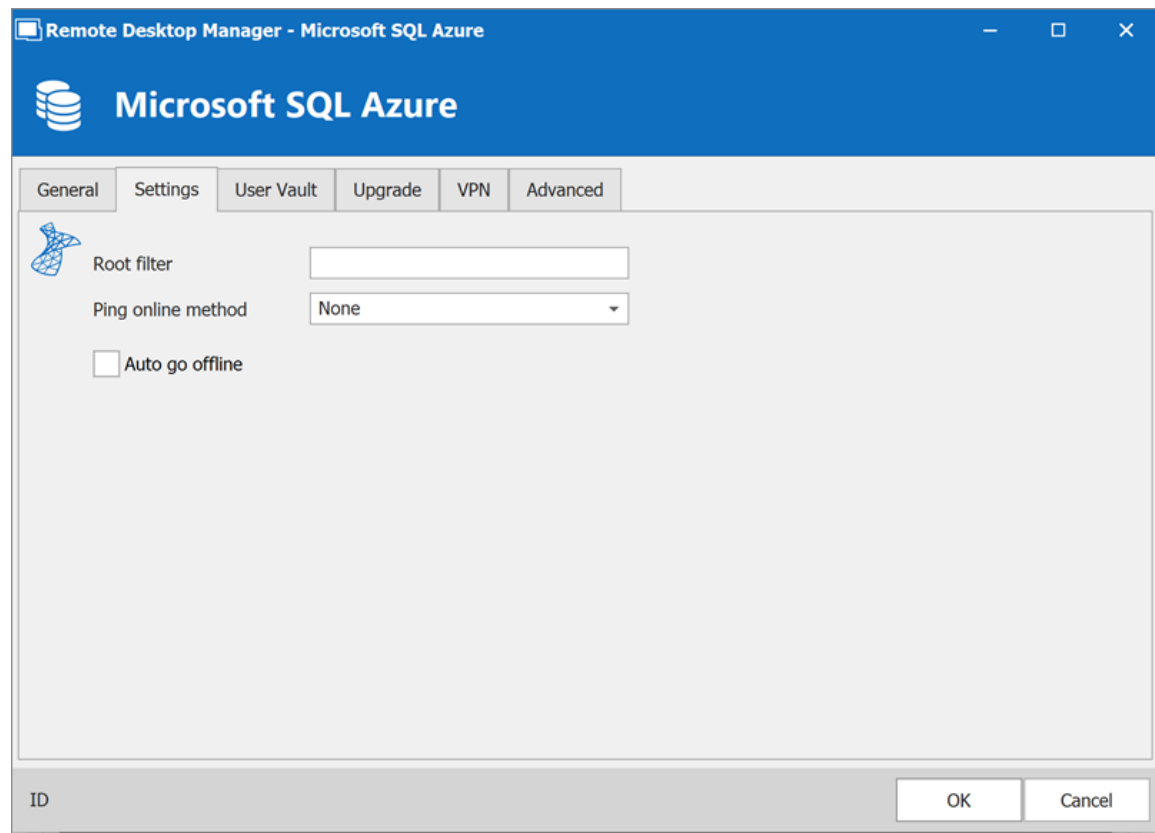
ID OK Cancel

*Microsoft SQL Azure - General*

OPTION	DESCRIPTION
<b>Name</b>	Enter a name for the data source.
<b>Host</b>	Enter the server hostname or IP address.
<b>Login mode</b>	Specify the authentication mode to use. Select between: <ul style="list-style-type: none"> <li>• <b>Database login</b></li> <li>• <b>Custom login</b></li> <li>• <b>Active Directory Password</b></li> <li>• <b>Active Directory Integrated</b></li> </ul>

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

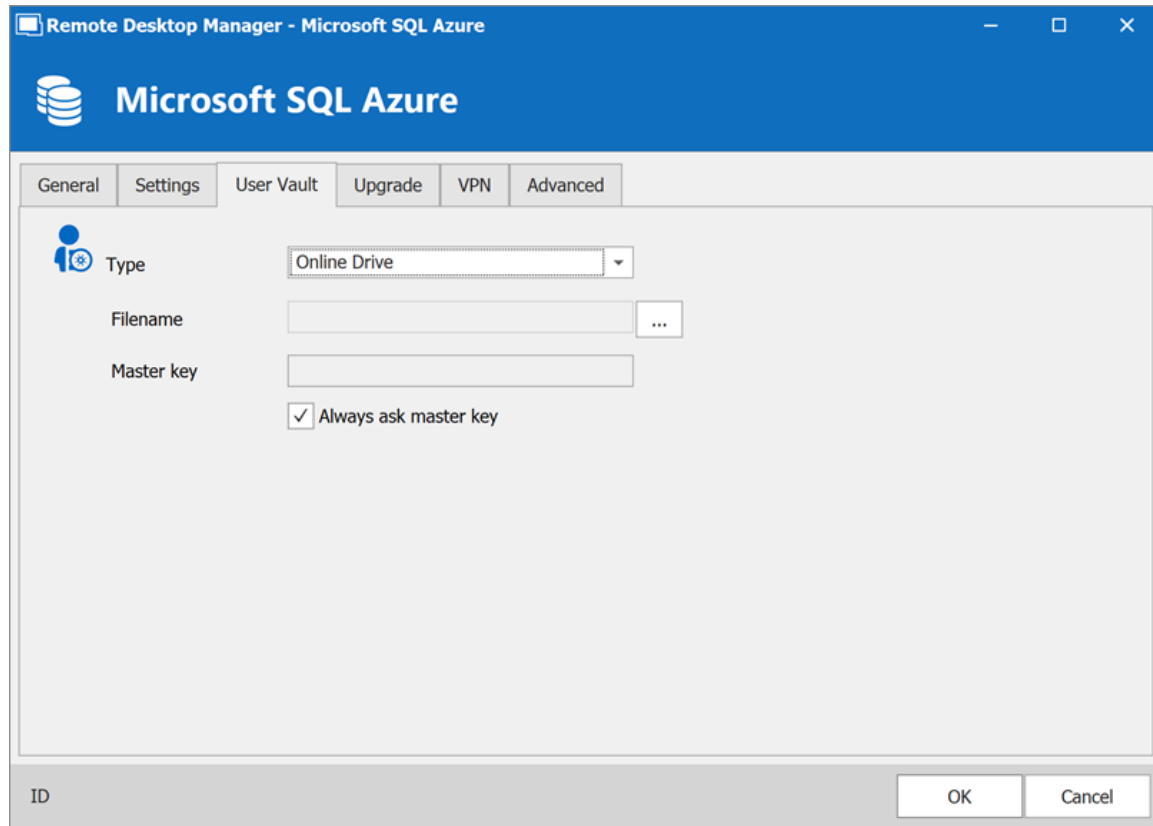
## SETTINGS



Microsoft SQL Azure - Settings Tab

OPTION	DESCRIPTION
<b>Root filter</b>	Enter the name of a root level folder to display only the entries contained in that folder.
<b>Ping online method</b>	Indicate the preferred ping online method. Select between: <ul style="list-style-type: none"> <li>• None</li> <li>• Ping</li> <li>• Port Scan</li> </ul>
<b>Auto go offline</b>	Use the data source in offline mode when the ping method does not respond.
<b>Disable lock</b>	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.

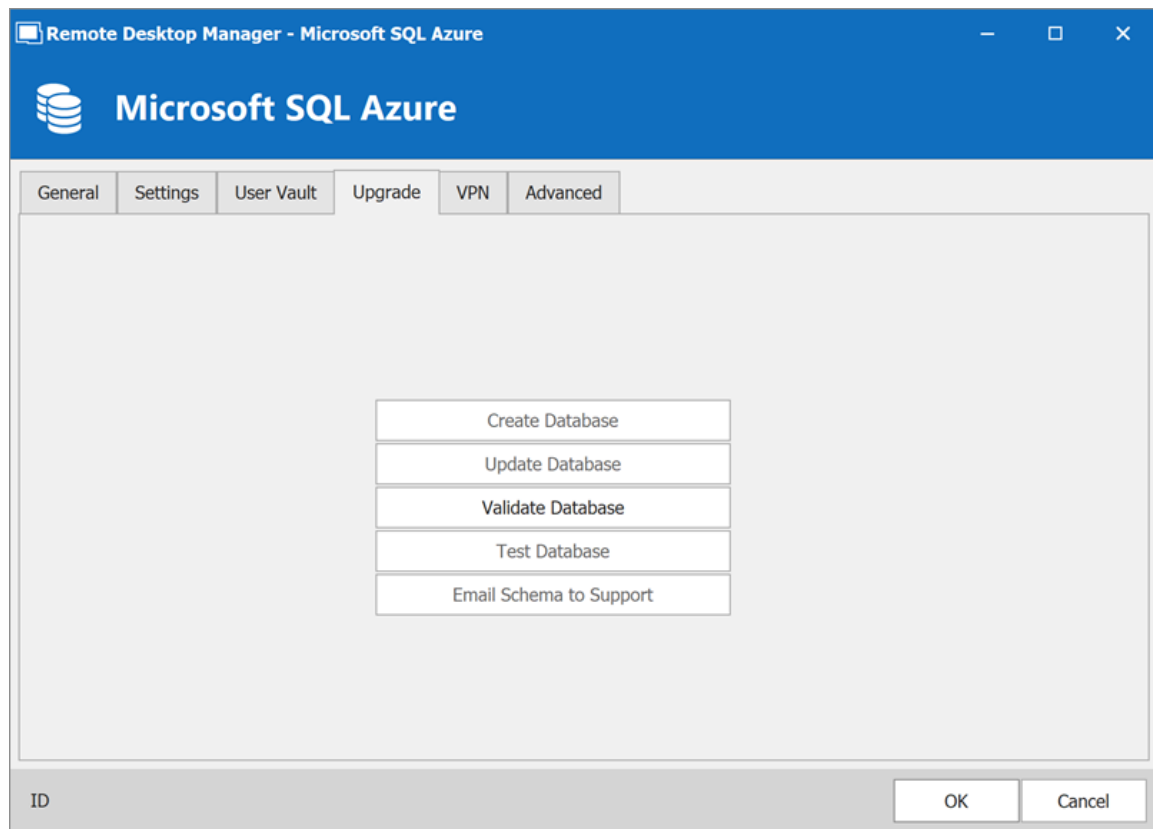
## USER VAULT



Microsoft SQL Azure - User Vault Tab

OPTION	DESCRIPTION
Type	Select the type of <a href="#">User Vault</a> to use. Select between: <ul style="list-style-type: none"><li>• <b>Default</b>: use the default User Vault, which is stored in the database.</li><li>• <b>None</b>: disable the User Vault for all users.</li><li>• <b>Online Drive</b>: use a Devolutions Online Drive file (*.dod) as a User Vault.</li></ul>

## UPGRADE

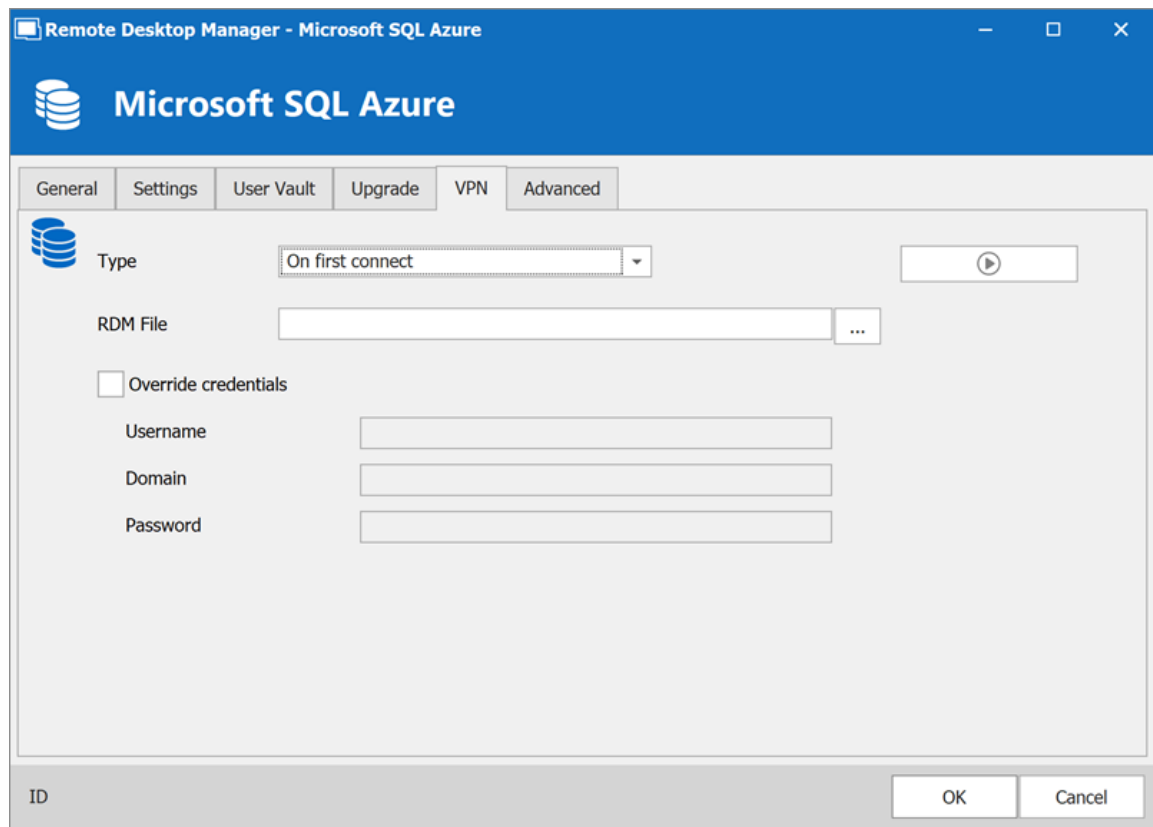
*Microsoft SQL Azure - Upgrade Tab*

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

## VPN

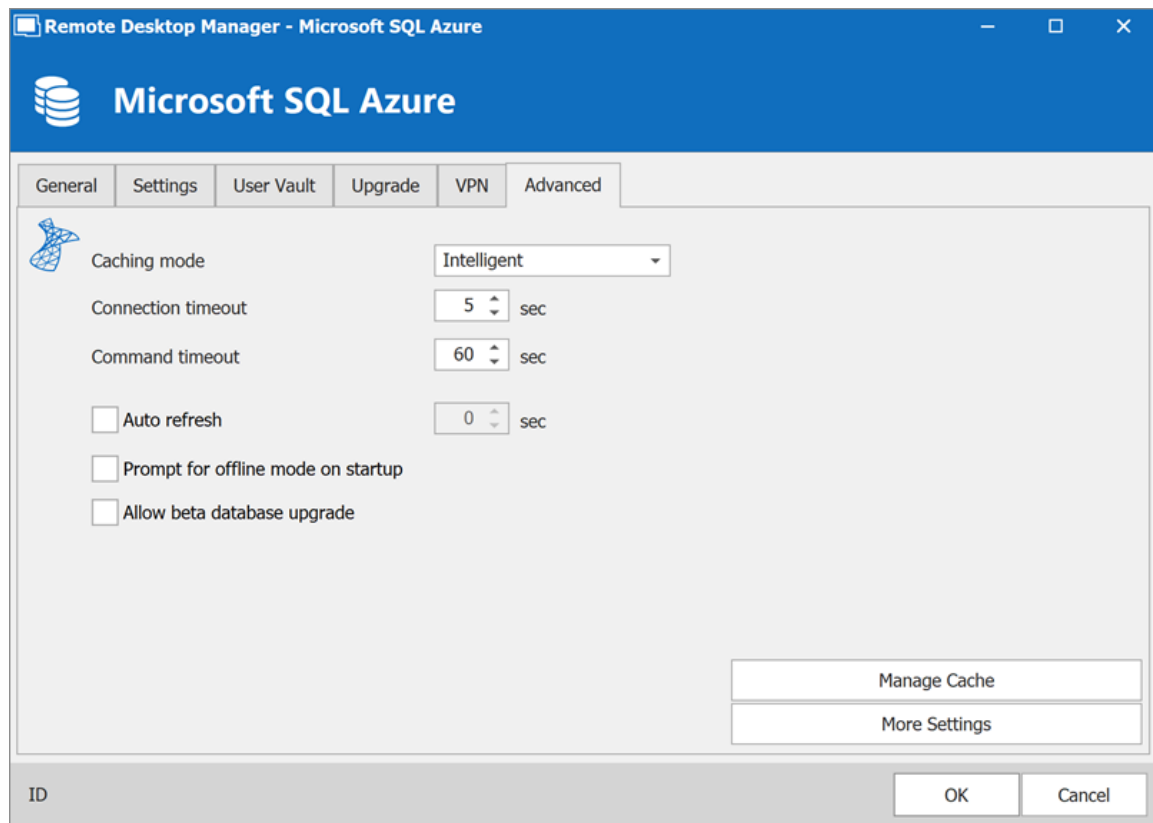


Open a VPN to access your data prior to connecting to your **Microsoft SQL Azure** database.



*Microsoft SQL Azure - VPN*

## ADVANCED



*Microsoft SQL Azure - Advanced Tab*

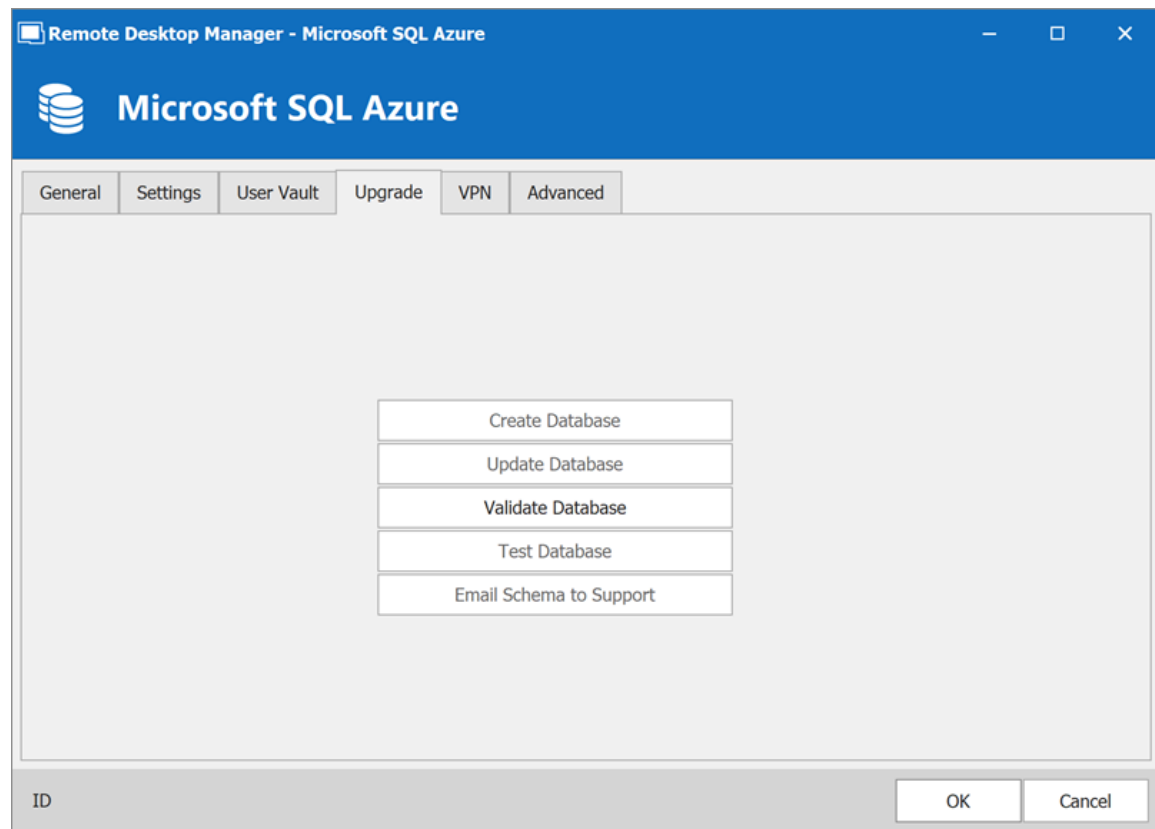
OPTION	DESCRIPTION
<b>Caching mode</b>	Determines how the entries will be reloaded in the data source. For more information, please consult the <a href="#">Caching</a> topic.
<b>Connection timeout</b>	Set the delay of the connection timeout.
<b>Command timeout</b>	Set the delay of the command timeout.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

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

#### 5.4.1.6.1 Configure SQL Azure

## DESCRIPTION

1. Make sure that you have a valid **Microsoft SQL Azure** 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 SQL Azure Server, click the **Update Database** button to add the appropriate tables to the database.

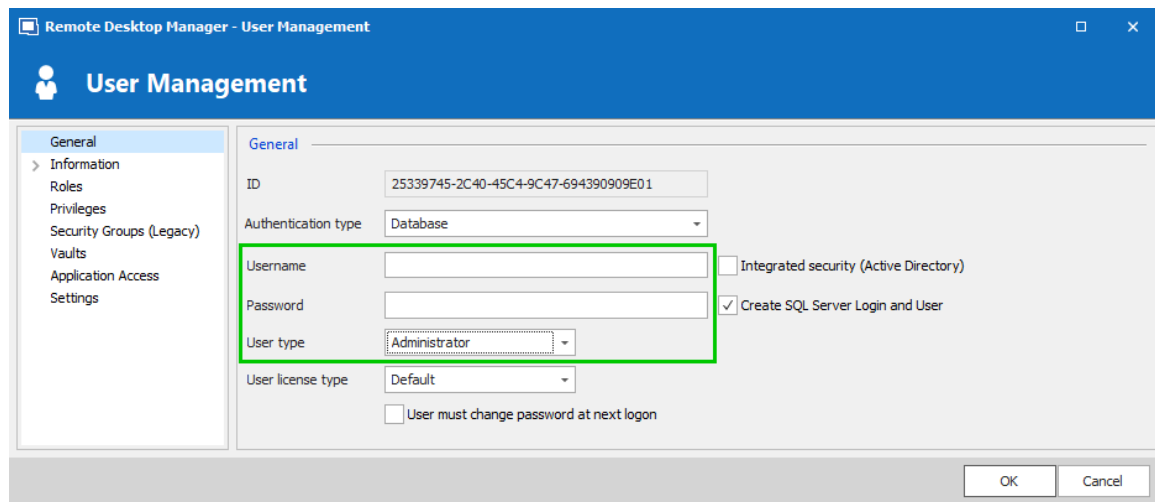


*Upgrade Tab*

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.



Remote Desktop Manager - User Management

**User Management**

General

ID: 25339745-2C40-45C4-9C47-694390909E01

Authentication type: Database

Username: [Text Box]

Password: [Text Box]

User type: Administrator

User license type: Default

☐ Integrated security (Active Directory)

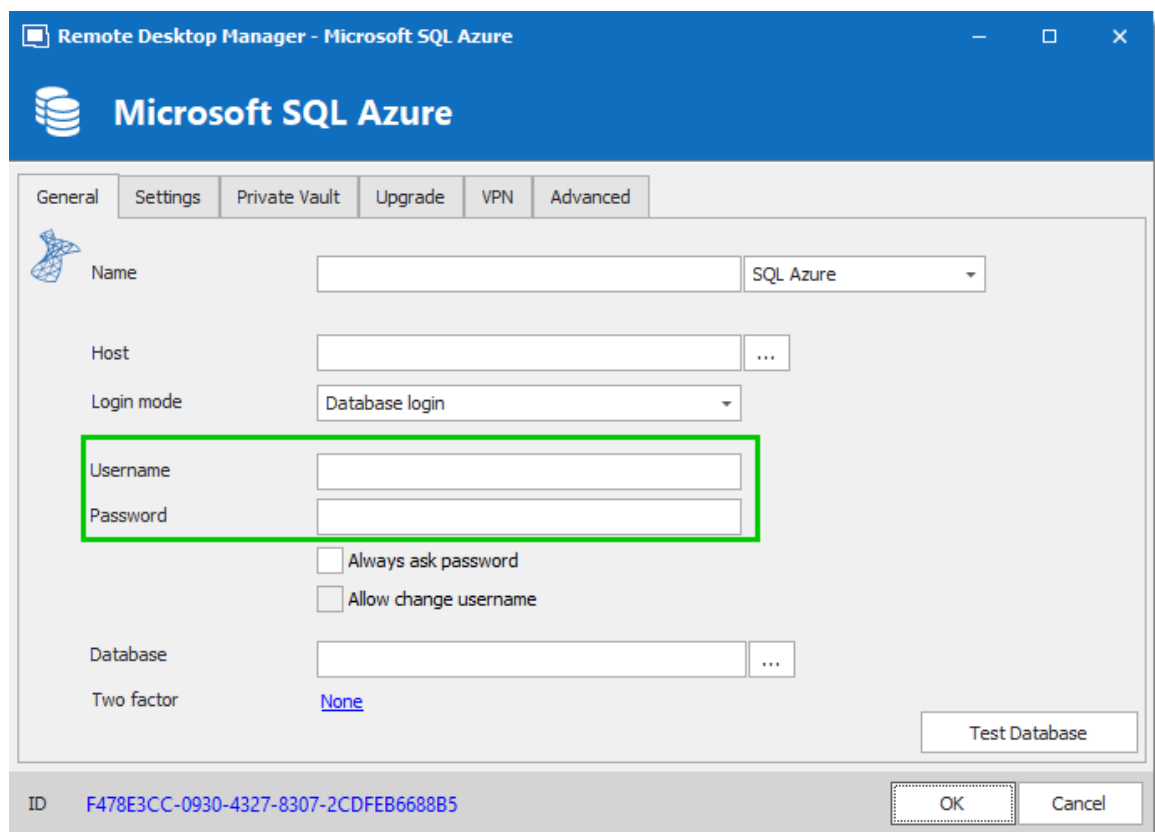
☒ Create SQL Server Login and User

☐ User must change password at next logon

OK Cancel

*Create a Remote Desktop Manager Administrator Account*

5. Connect on the Microsoft SQL Azure 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.



Remote Desktop Manager - Microsoft SQL Azure

**Microsoft SQL Azure**

General Settings Private Vault Upgrade VPN Advanced

Name: [Text Box] SQL Azure

Host: [Text Box] ...

Login mode: Database login

Username: [Text Box]

Password: [Text Box]

☐ Always ask password

☐ Allow change username

Database: [Text Box] ...

Two factor: [None](#)

Test Database

ID: F478E3CC-0930-4327-8307-2CDFEB6688B5

OK Cancel

*Connection to the Database with the RDM Administrator Account*

The Microsoft SQL Azure data source is now correctly configured.

## 5.4.1.6.2 Enable Azure Active Directory Authentication

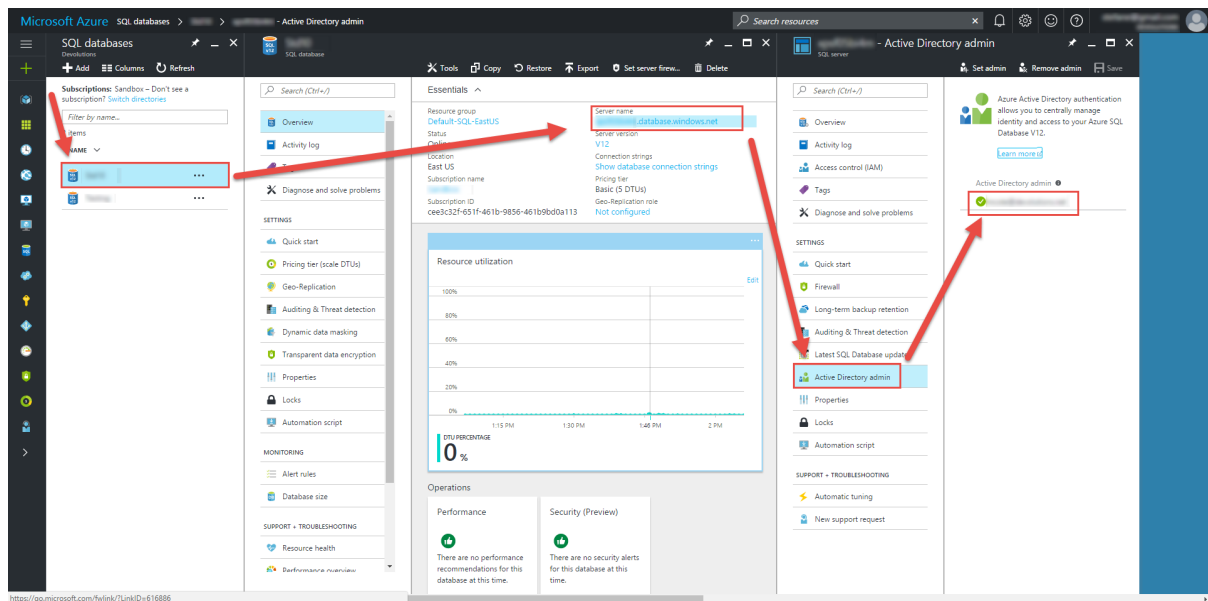
## 5.4.1.6.2.1 Configure the Active Directory Admin

## DESCRIPTION

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

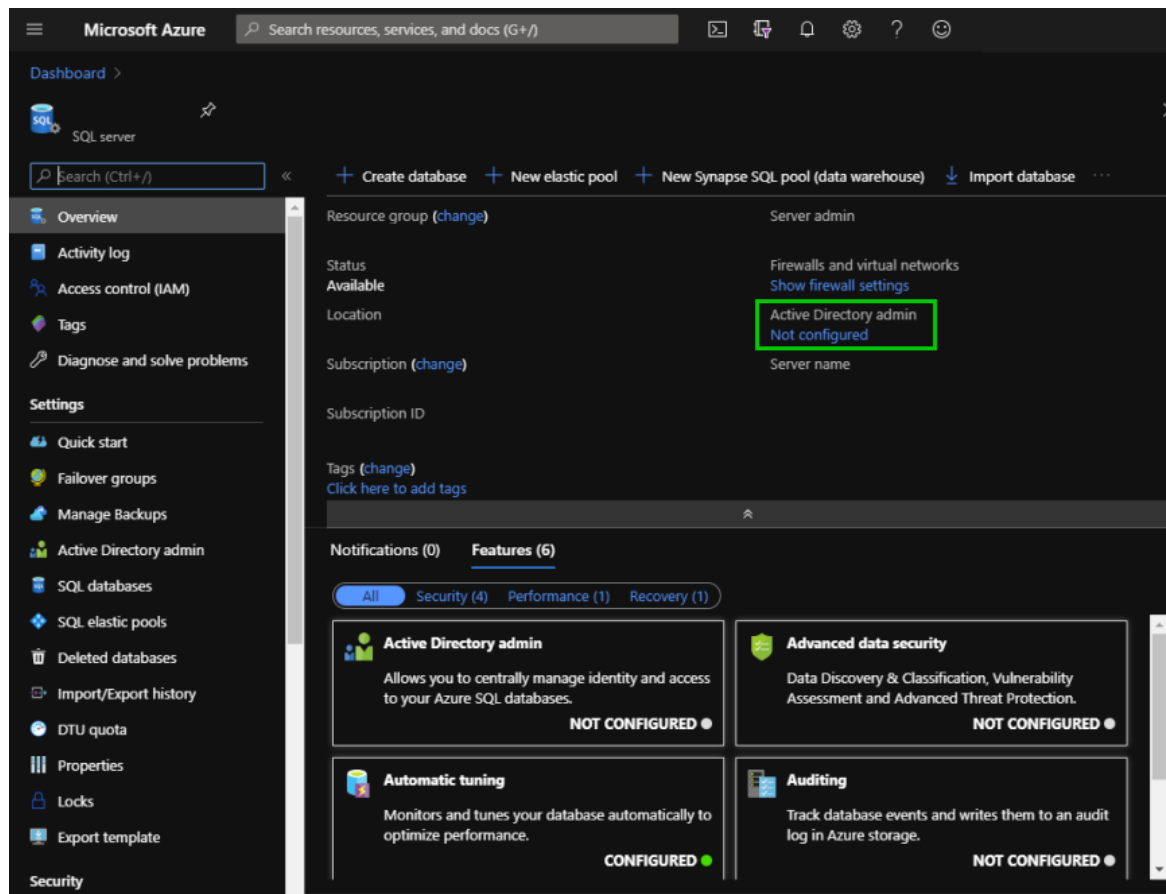


It may take a few minutes for this change to propagate. You might experience a time delay before being able to connect with this Active Directory account.

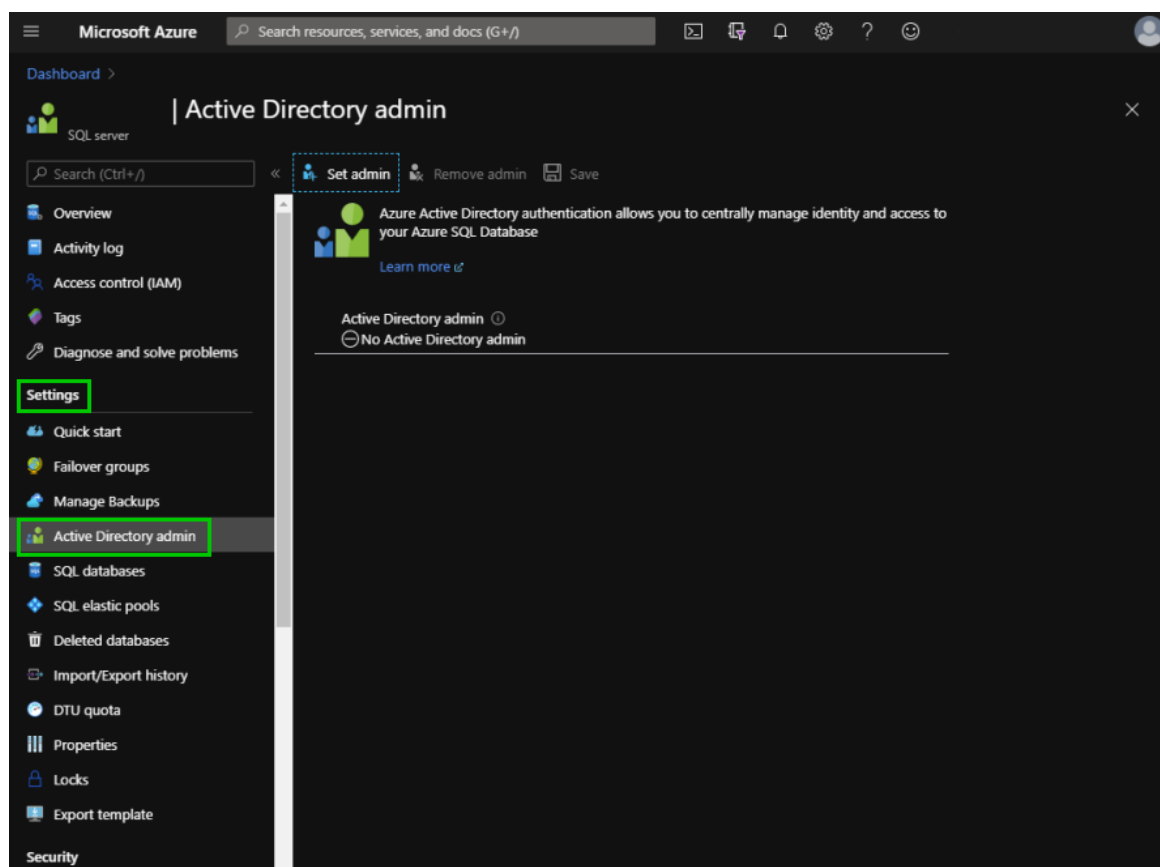


Azure AD Portal

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

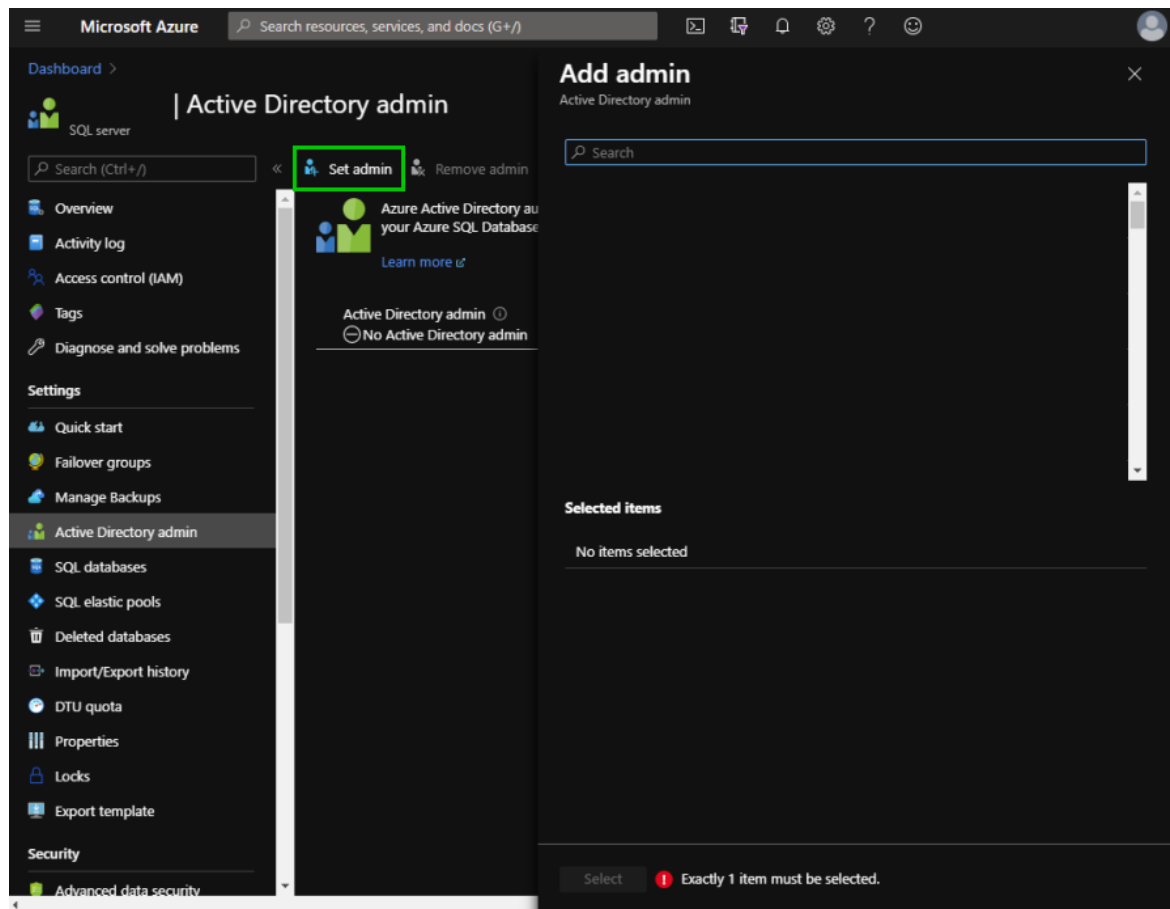


2. Click on **Active Directory admin** under **Settings** in the left menu.

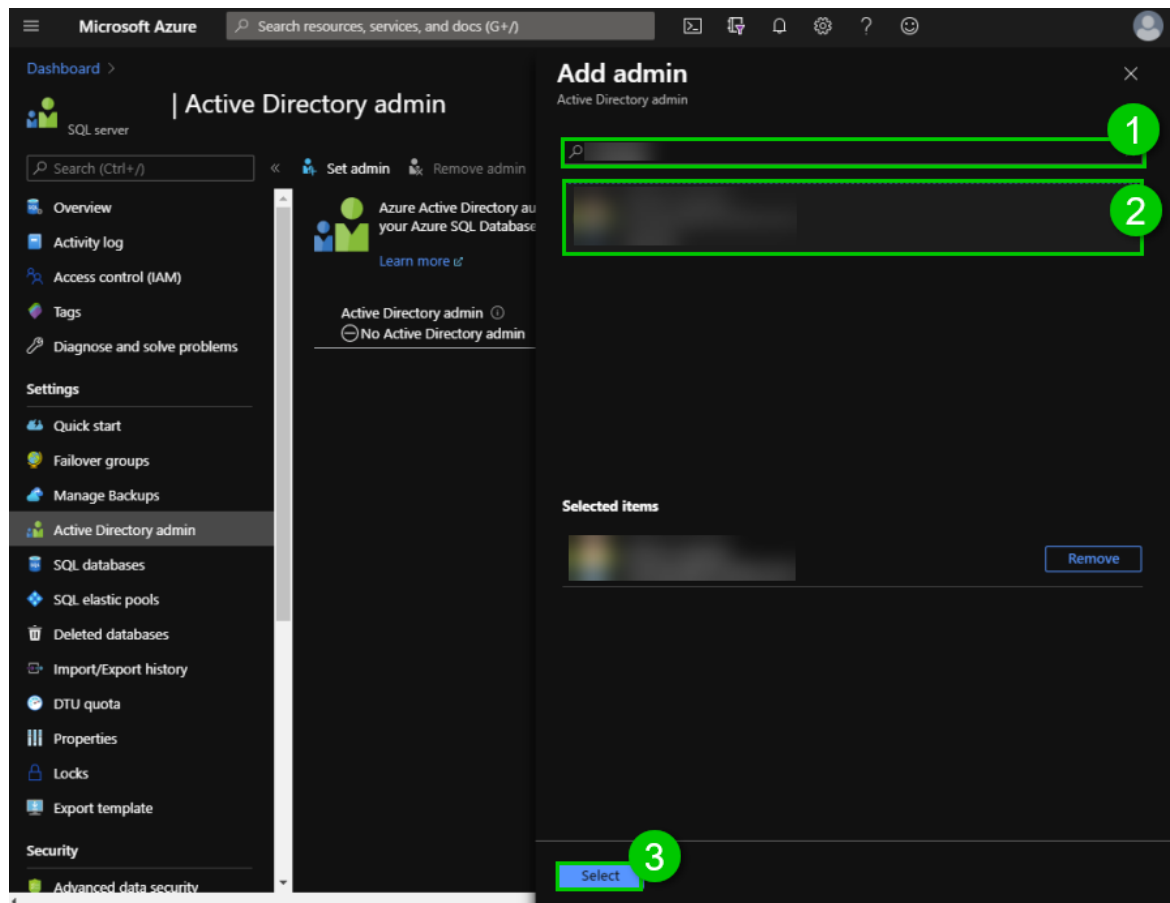


3. Click on **Set admin** to search for the admin.

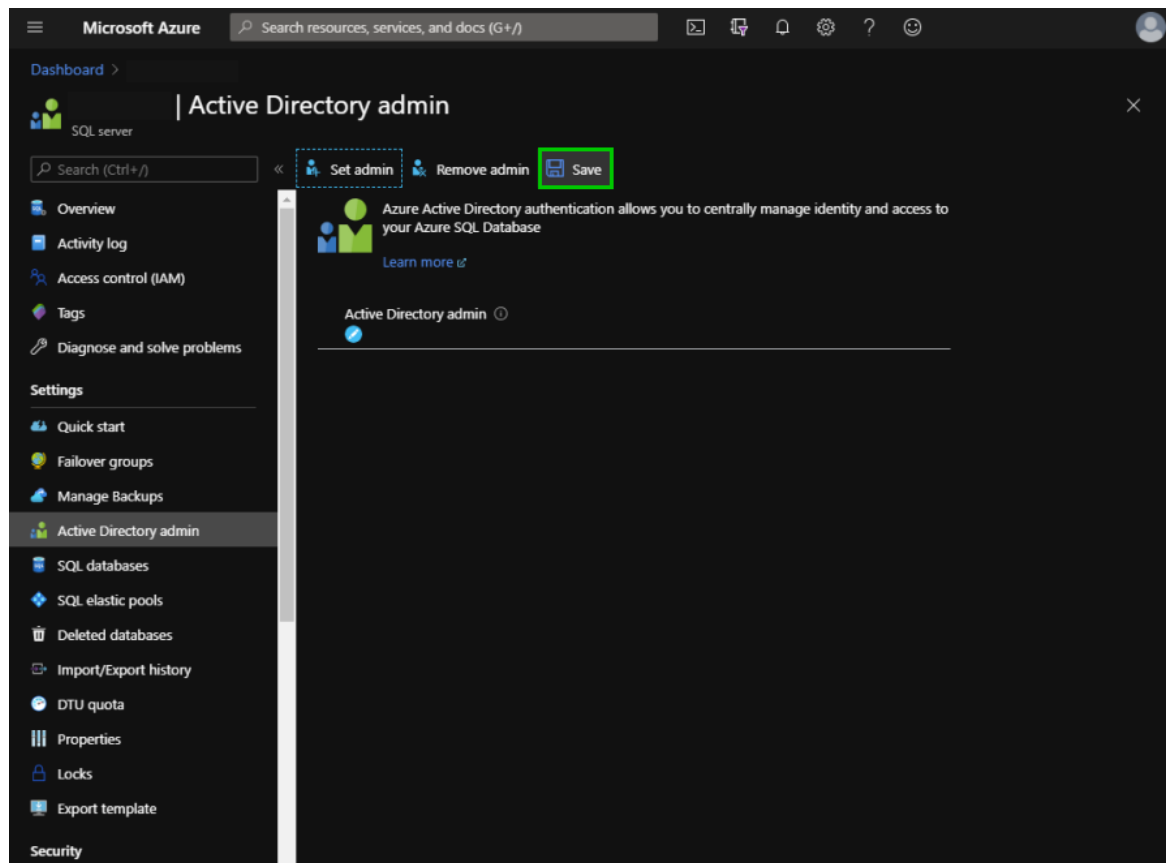




4. Type the admin name in the **Search** field, click on the admin in the list provided and then **Select**.



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



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

#### 5.4.1.6.2.2 Create an Azure Active Directory App Registration

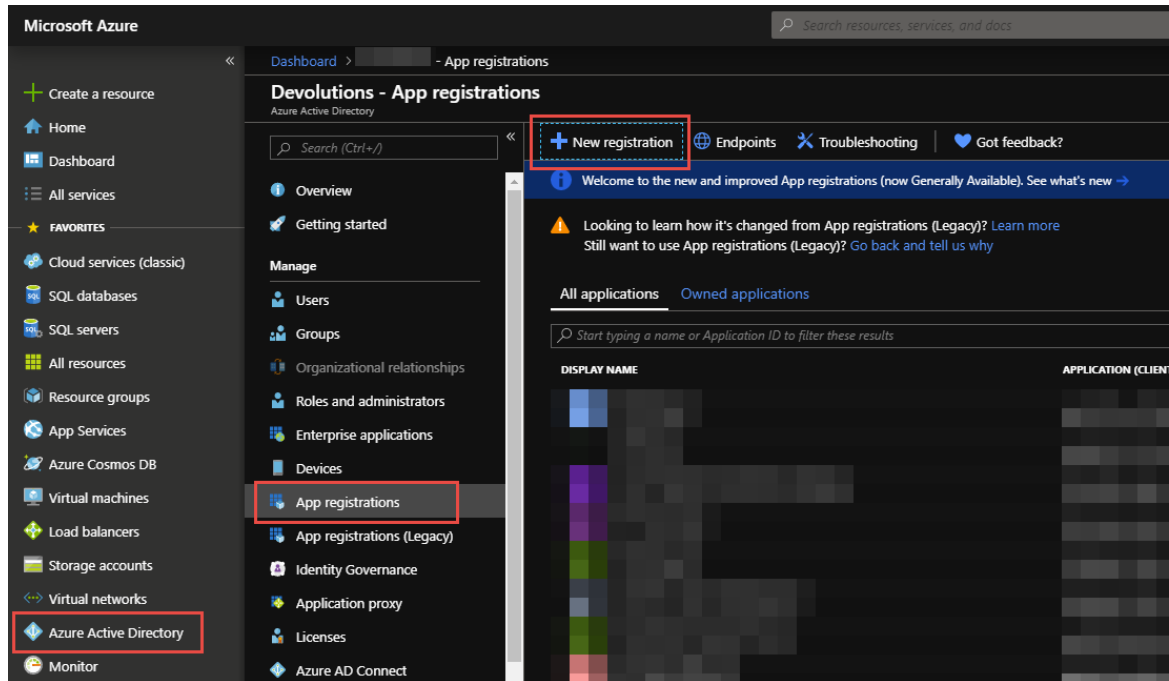
## DESCRIPTION

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 SQL Azure 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**, **Supported account types** and **Redirect URI** as indicated below and click **Register**.



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

## Register an application

**\* Name**  
The user-facing display name for this application (this can be changed later).

RDM-App-Registration ✓

**Supported account types**  
Who can use this application or access this API?

☒ Accounts in this organizational directory only (Devolutions only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

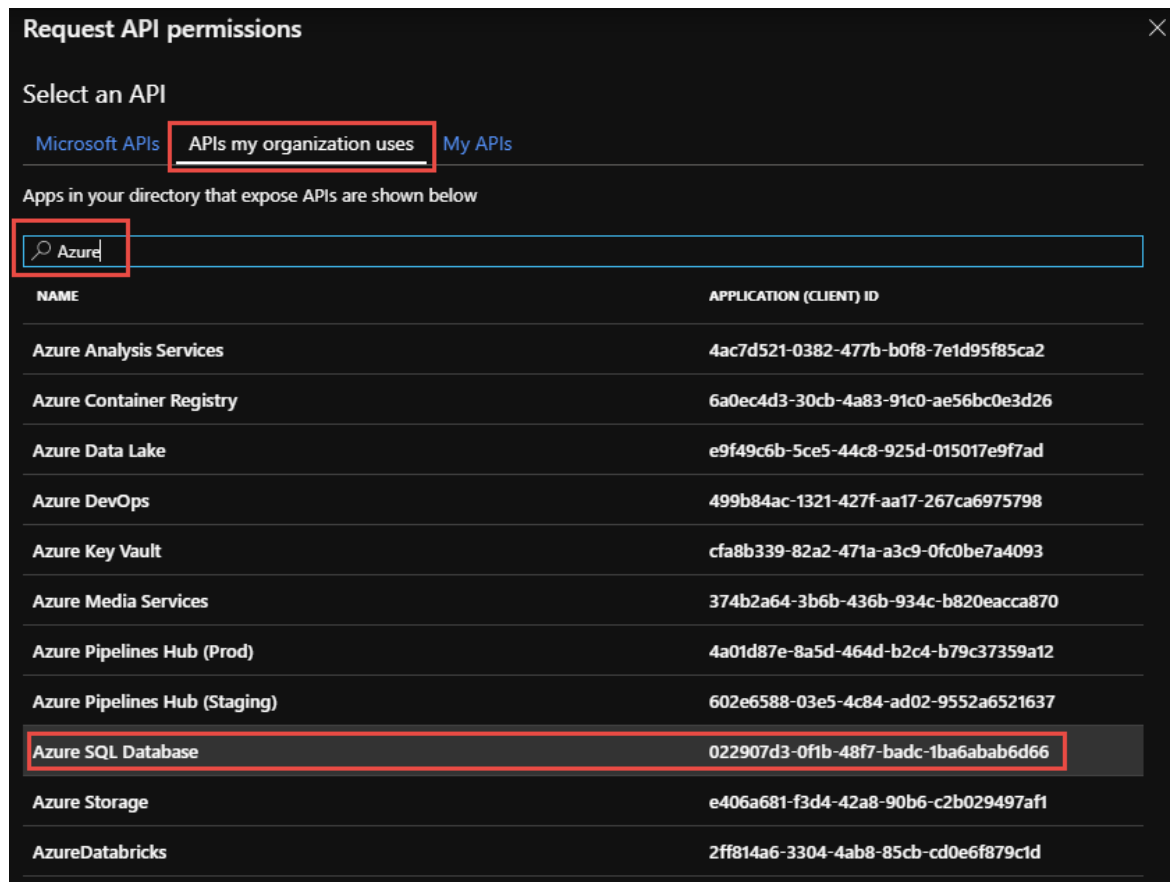
[Help me choose...](#)

**Redirect URI (optional)**  
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Public client/native (mobile ... ▼ https://mycompany.com ✓

*Supported Account Types*

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



*APIs my organization uses*

5. Select **Delegated permissions – user\_impersonation** and click **Add permissions**.

**Request API permissions**

< All APIs

Azure SQL Database  
AS https://database.windows.net/

What type of permissions does your application require?

**Delegated permissions**  
Your application needs to access the API as the signed-in user.

**Application permissions**  
Your application runs as a background service or daemon without a signed-in user.

Select permissions expand all

Type to search

PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> <b>user_impersonation</b> Access Azure SQL DB and Data Warehouse ⓘ	-

**Add permissions** Discard

*user\_impersonation*

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

**API permissions**

Applications are authorized to use APIs by requesting permissions. These permissions show up during the consent process where users are given the opportunity to grant/deny access.

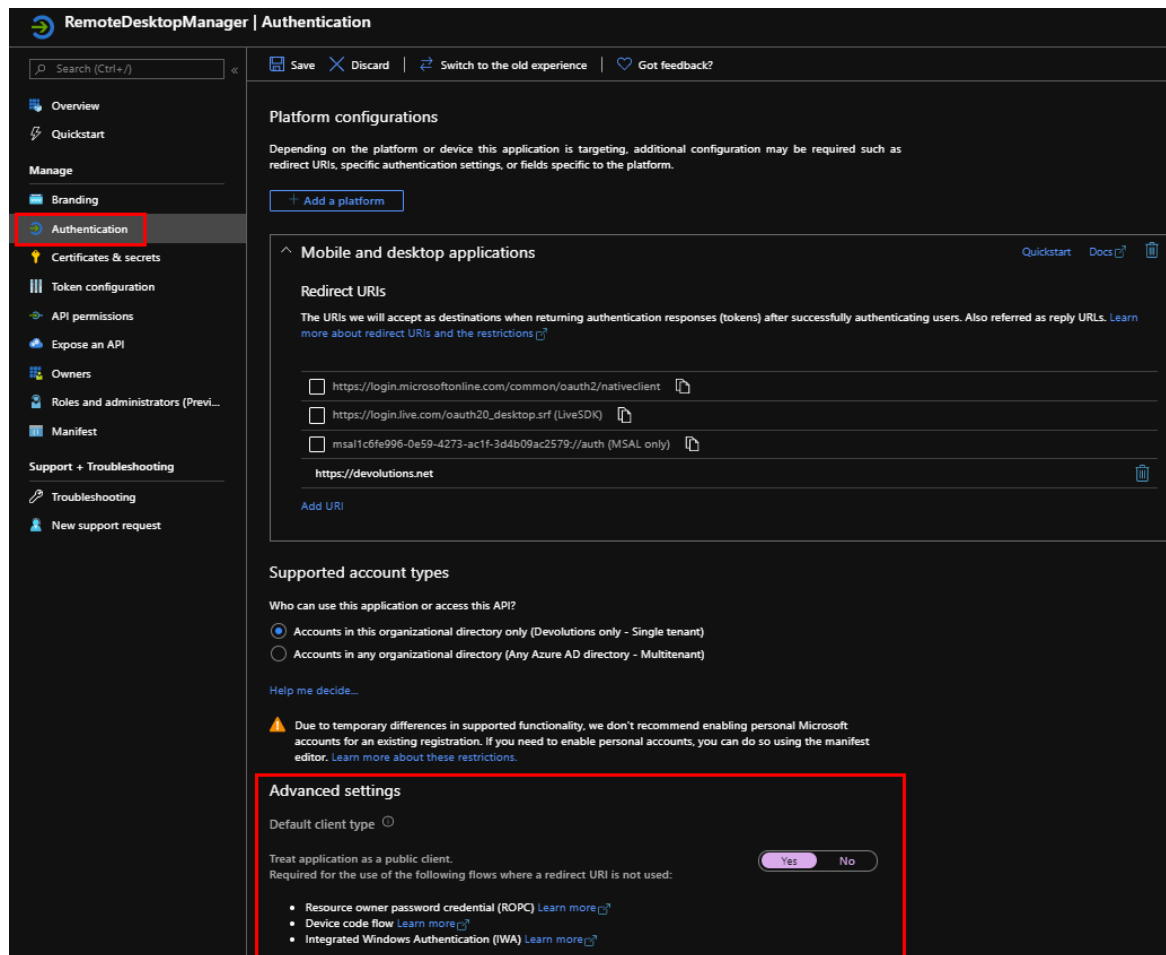
[+ Add a permission](#)

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED
▼ Azure SQL Database (1)			
user_impersonation	Delegated	Access Azure SQL DB and Data Warehouse	-
▼ Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	-

These are the permissions that this application requests statically. You may also request user consent-able permissions dynamically through code. [See best practices for requesting permissions](#)

*API / Permissions Name*

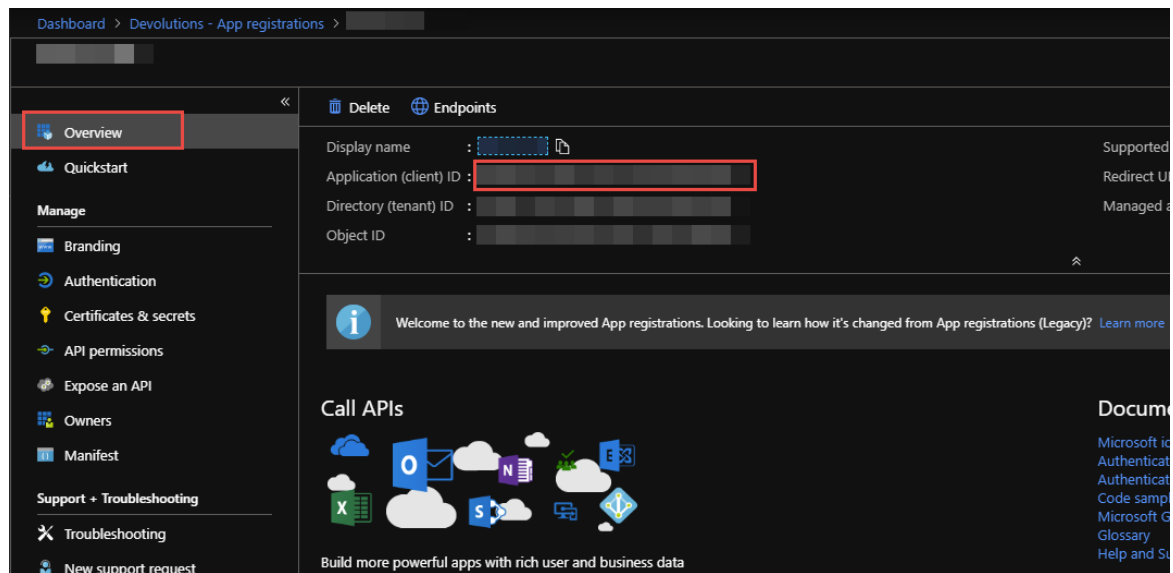
7. **Optional step:** Click on the **Authentication** section and switch to **Yes**, if you desire the **Integrated Windows Authentication (IWA)** option



### Authentication

8. Your **Azure Active Directory App Registration** is now completed.
9. Copy the **App Registration's Application (client) ID** needed in Remote Desktop Manager in the next step.





*Application (client) ID*

#### 5.4.1.6.2.3 Configure RDM Active Directory Interactive (with MFA)

## DESCRIPTION

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



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>.



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

Remote Desktop Manager - Microsoft SQL Azure

Microsoft SQL Azure

General Settings User Vault Upgrade VPN Advanced

Name: Windjammer Microsoft SQL Azure

Host: windjammer.database.windows.net ...

Login mode: Active Directory Interactive (with MFA support) Automatic

Username: admin@windjammer.com

Azure App Settings: [Configured](#)

☐ Allow change username

Database: RDM ...

Two factor: [None](#)

Test Database

ID OK Cancel

Azure with MFA

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
<b>Default</b>	<p>This is the default mode.</p> <p>The user will be prompted for credentials even if there is a token that meets the requirements already in the cache.</p>

OPTION	DESCRIPTION
<b>Automatic</b> <b>(Shared in older versions)</b>	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.

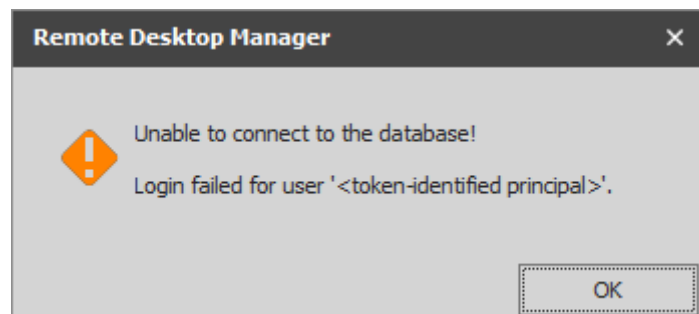


When it comes to Azure AD joined devices (registered devices). Azure AD may or may not prompt for MFA. **This is entirely controlled by Azure AD**, there is nothing we can do in RDM to force or bypass the MFA other than the **Default** or **Automatic** options mentioned above.

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

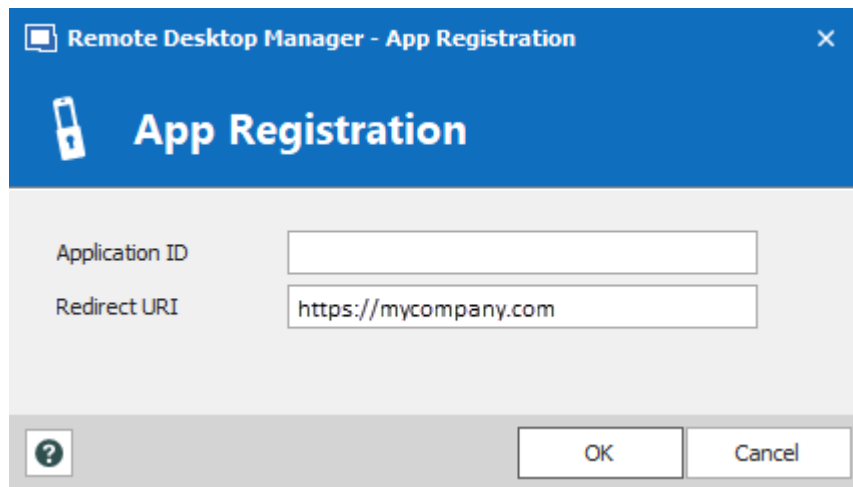


On first connect, the username must be the Active Directory Admin as defined in the [Configure the Active Directory Admin](#). Once you add other AD user in RDM they will be able to connect.



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.

*App Registration*

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

#### 5.4.1.6.2.4 Configure Azure Active Directory user in RDM

## DESCRIPTION

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

In the **Authentication 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 **Authentication type**, please validate that all the steps have been done in the following topics:

- [Configure the Active Directory Admin](#)
- [Create an Azure Active Directory App Registration](#)
- [Configure RDM Active Directory Interactive \(with MFA\)](#)

Remote Desktop Manager - User Management

## User Management

- General
- Information
- Roles
- Privileges
- Security Groups (Legacy)
- Vaults
- Application Access
- Settings

**General**

ID: A6AA8F25-332B-4F2B-A265-473CF02308C9

Authentication type: Office 365/Azure AD

Username:

Domain:

☐ Is guest/federated user

☒ Contained database user (recommended) ?

User type: User

User license type: Default

OK Cancel

Set the Authentication type to Office365/Azure AD



The option ***Is guest/federated user*** should only be checked in rare and special cases 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 an MFA prompt on registered devices and that's why you are not getting the MFA prompt in that case.

Details						
Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only	Additional Details
Date	Authentication method	Authentication method detail	Succeeded	Result detail	Requirement	
12/9/2020, 3:53:33 PM	Password	Password in the cloud	true		Primary authentication	
12/9/2020, 3:53:33 PM	Previously satisfied		true	MFA requirement skipped due to registered device	User	

#### 5.4.1.7 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

Remote Desktop Manager - Devolutions Password Hub Business

**Devolutions Password Hub Business**

General VPN Advanced

 Name

Username

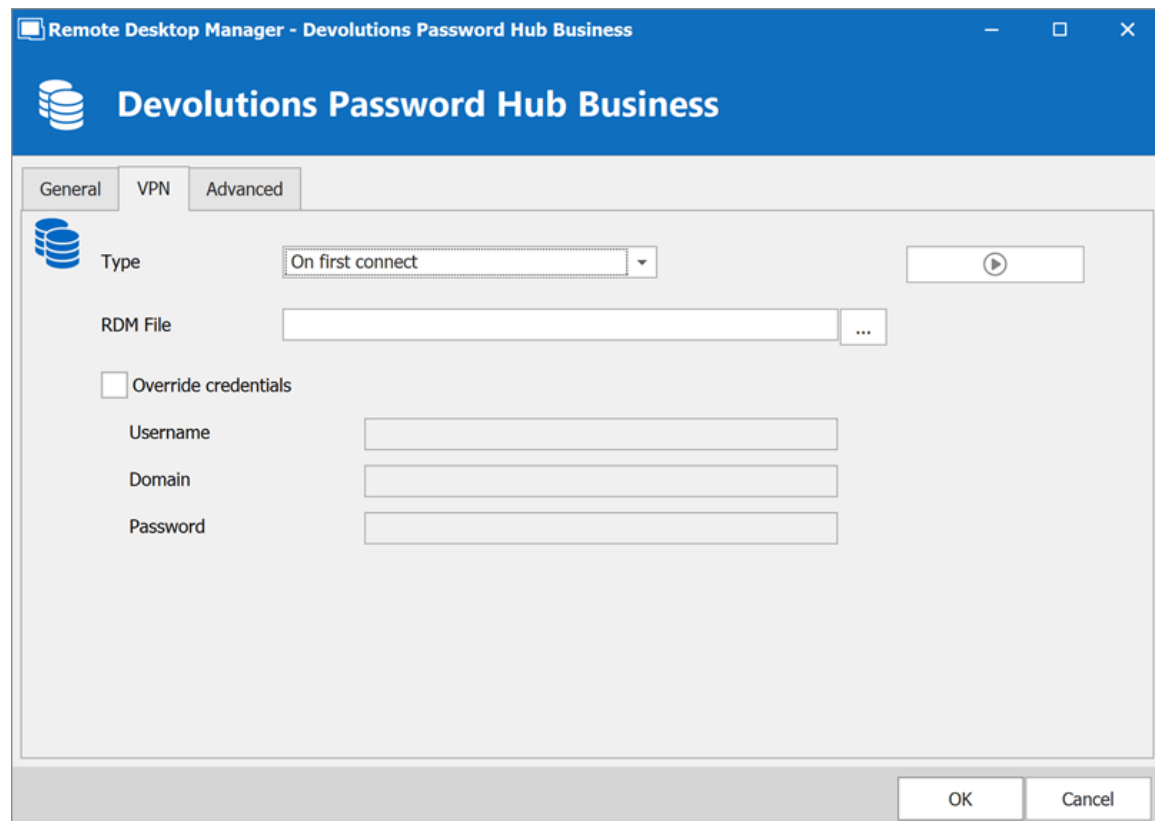
Host  ...

OK Cancel

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

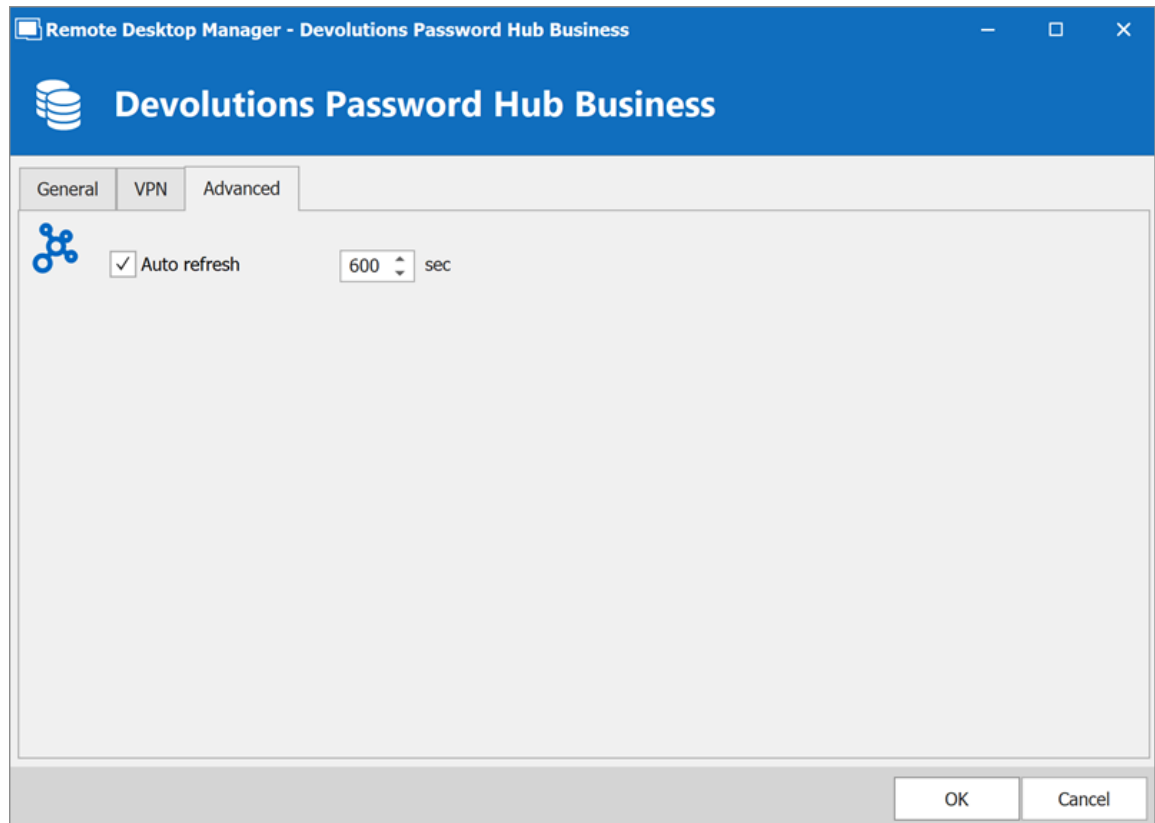
## VPN

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



## ADVANCED

Set the interval for the automatic refresh.



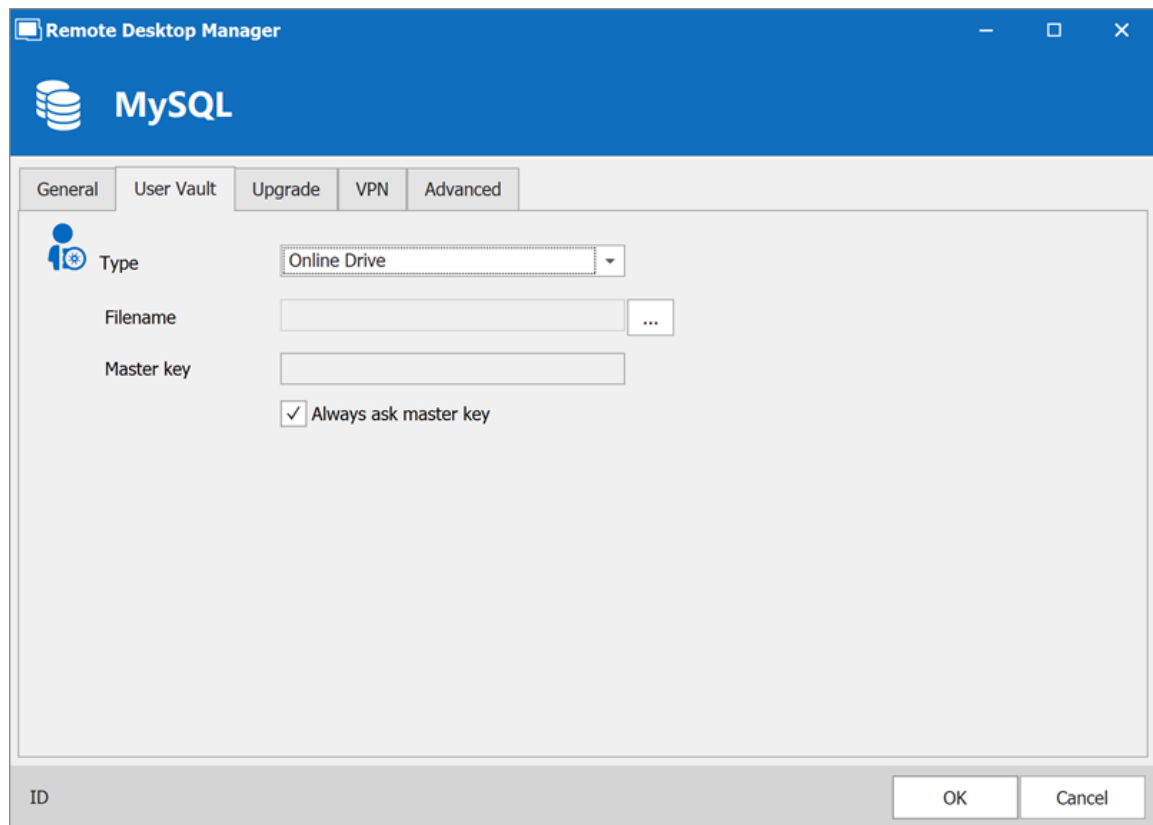
### 5.4.1.8 User Vault

## 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](#).

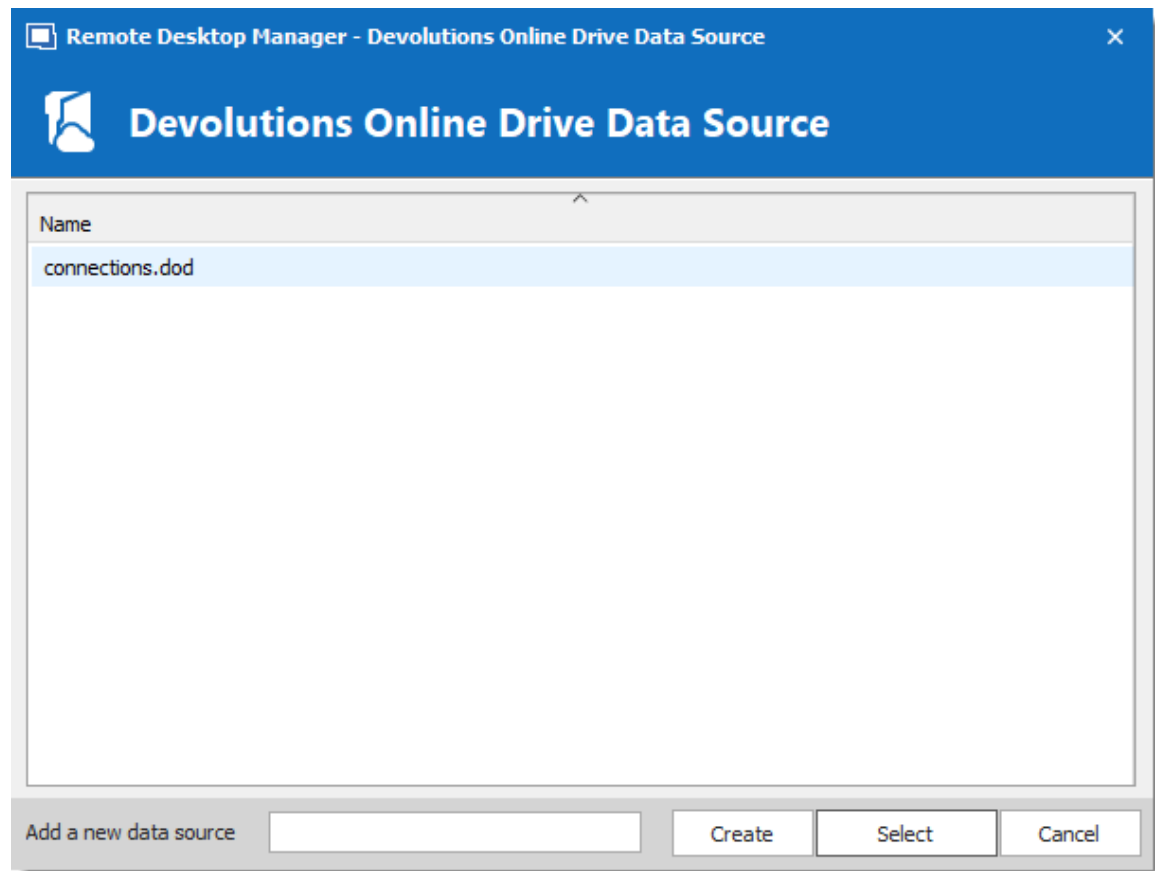
1. In the **User Vault** tab of your Advanced Data Source, select **Online Drive** in the **Type**.





*Devolutions Online Database Data Source*

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*

## 5.4.2 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

The screenshot shows the 'Remote Desktop Manager - Dropbox' window. The title bar includes the application name and standard window controls. The main area has a blue header with the Dropbox logo and name. Below this are three tabs: 'General' (selected), 'VPN', and 'Advanced'. The 'General' tab contains several configuration fields: 'Name' (text box with 'Dropbox'), 'Mode' (dropdown menu with 'Local' selected), 'Local path' (text box), 'Full local path' (text box with 'connections.xml'), 'Master key' (text box), a checked checkbox for 'Always ask master key', 'Dropbox directory' (text box), 'Filename' (text box with 'connections.xml'), and an unchecked checkbox for 'Compress database file'. At the bottom, there is an 'ID' field with the value 'AAAC170C-C03C-4077-BC4F-28A717C3CB4C' and 'OK' and 'Cancel' buttons.

Dropbox - General Tab



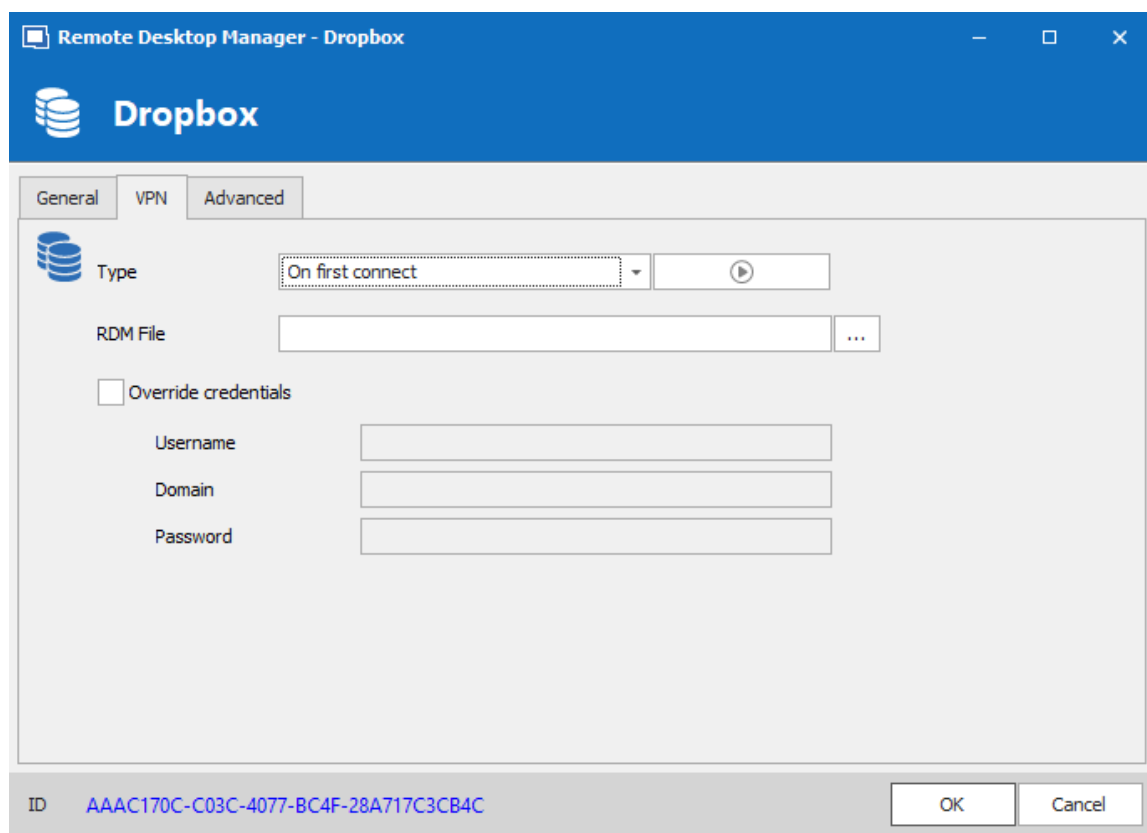
Remote Desktop Manager supports the 2-Factor Authentication of Dropbox. When the button **Validate with Dropbox** is pressed and the 2-Factor Authentication is enabled in Dropbox, a window prompt will open and ask for the Dropbox account password, then a second prompt will open for the security code.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

OPTION	DESCRIPTION
<b>Name</b>	Name of the data source.
<b>Mode</b>	<p>Select the mode that is preferred to configure the data source. Select between:</p> <ul style="list-style-type: none"> <li>• <b>Account</b></li> <li>• <b>Local</b></li> </ul>

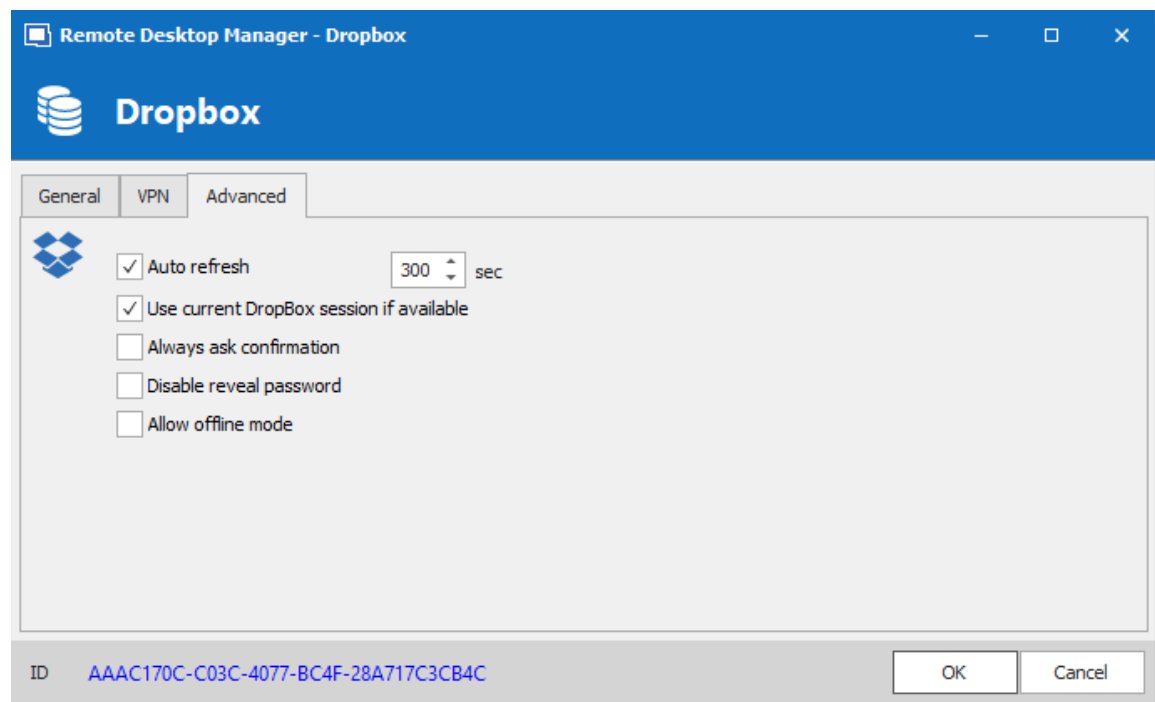
OPTION	DESCRIPTION
<b>Local path (Local Mode)</b>	Contains the local path where the Dropbox files are accessible.
<b>Email (Account Mode)</b>	Contains the email address associated with the Dropbox account.
<b>Validate with Dropbox (Account Mode)</b>	Button to validate the email address with the Dropbox account.
<b>Master key</b>	Add an additional layer of security to your data source by using master key.
<b>Always ask master key</b>	Connecting to the data source will always prompt for the master key.
<b>Dropbox directory</b>	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.
<b>Filename</b>	Indicate the filename used to store the data on the data source.
<b>Compress database file</b>	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
<b>Auto refresh</b>	Set the interval to use between each automatic refresh.
<b>Use current Dropbox session if available</b>	This option will use the Dropbox account who has been already validated without any other validation.
<b>Always ask for confirmation</b>	Always ask for confirmation when connecting to the data source.
<b>Disable reveal password</b>	Disable the reveal password feature when a user access this data source.
<b>Allow offline mode</b>	Allow the data source to be used in <a href="#">Offline mode</a> .

### 5.4.3 Google Drive

## DESCRIPTION



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

## GENERAL

Remote Desktop Manager - Google Drive

Google Drive

General VPN

Name

Email

Password

☐ Always ask password

Account status The account is not validated yet.

Validate Google Drive

Master key

☒ Always ask master key

Filename

ID B90C0576-E259-4C83-B929-6381577FC0A2

OK Cancel

Google Drive - General Tab

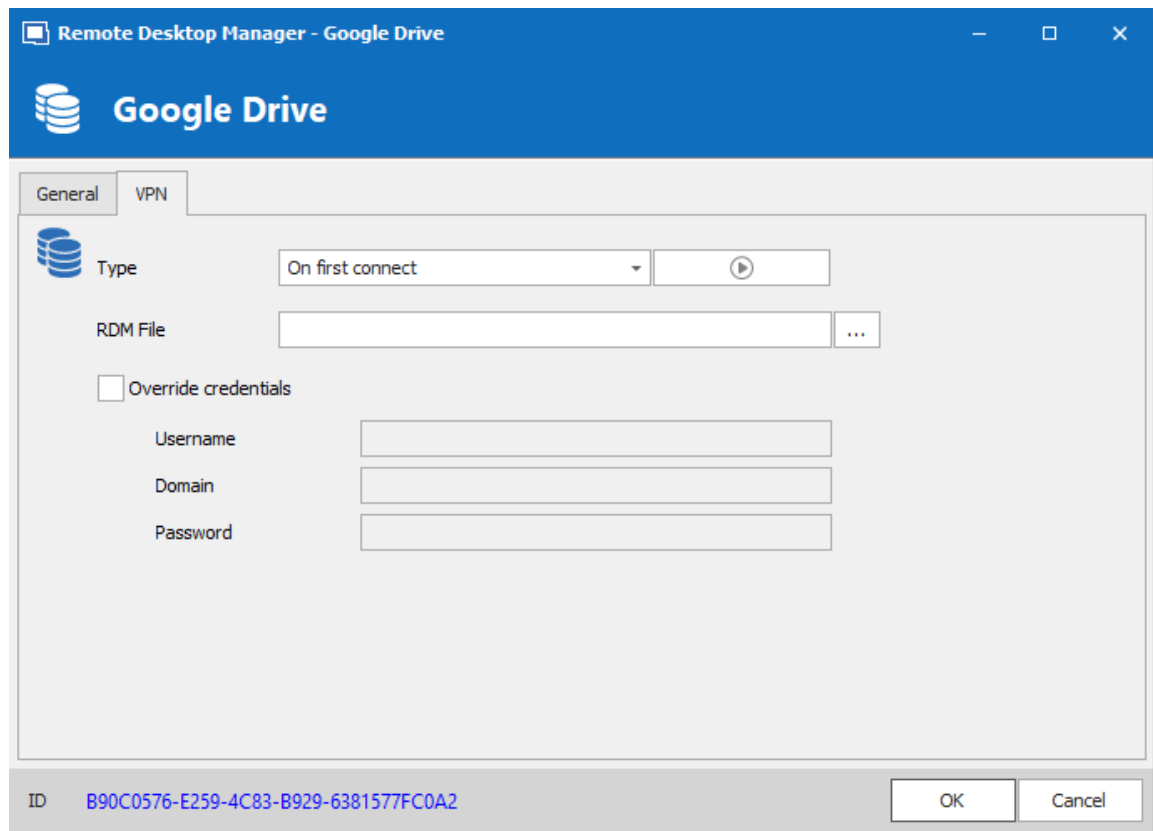
OPTION	DESCRIPTION
Name	Enter the name of the data source.
Email	Enter the Google email to access Google Drive.



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

#### 5.4.4 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

The screenshot shows the 'Remote Desktop Manager - Devolutions Online Drive' dialog box with the 'General' tab selected. The dialog has a blue header with the Devolutions logo and title. Below the header are four tabs: 'General', 'Backup', 'VPN', and 'Advanced'. The 'General' tab contains the following fields and options:

- Name:** A text field containing 'Devolutions Online Drive'. To its right is a link 'Create a Free Account'.
- Always ask password:** An unchecked checkbox.
- Test Connection:** A button.
- Filename:** A text field containing 'connections.dod' with a browse button '...' to its right.
- Master key:** A text field.
- Always ask master key:** A checked checkbox.

At the bottom of the dialog, there is an 'ID' field containing 'BF0B90F2-FC01-451C-8C3E-E307D3E352C4' and 'OK' and 'Cancel' buttons.

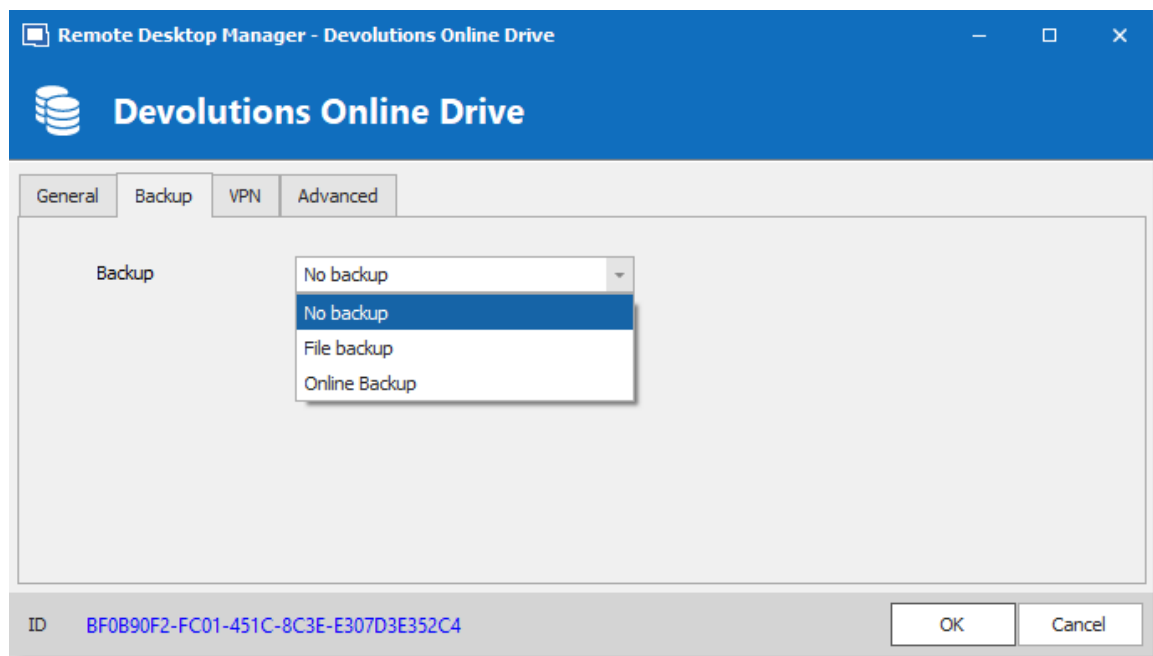
*Devolutions Online Drive - General Tab*

OPTION	DESCRIPTION
<b>Name</b>	Enter the name of the data source.

OPTION	DESCRIPTION
<b>Create a free account</b>	Create a new Devolutions Account.
<b>Always ask password</b>	Prompts for the password every time a connection to the Devolutions Online Drive is attempted.
<b>Test Connection</b>	Test the connection with Devolutions Online Drive to validate the provided credentials.
<b>Filename</b>	Indicate the filename used to store the data on the Devolutions Online Drive.
<b>Master key</b>	Contains a master key to access the data source.
<b>Always ask master key</b>	Ask for the master key every time a connection to the Devolutions Online Drive is attempted.

## BACKUP

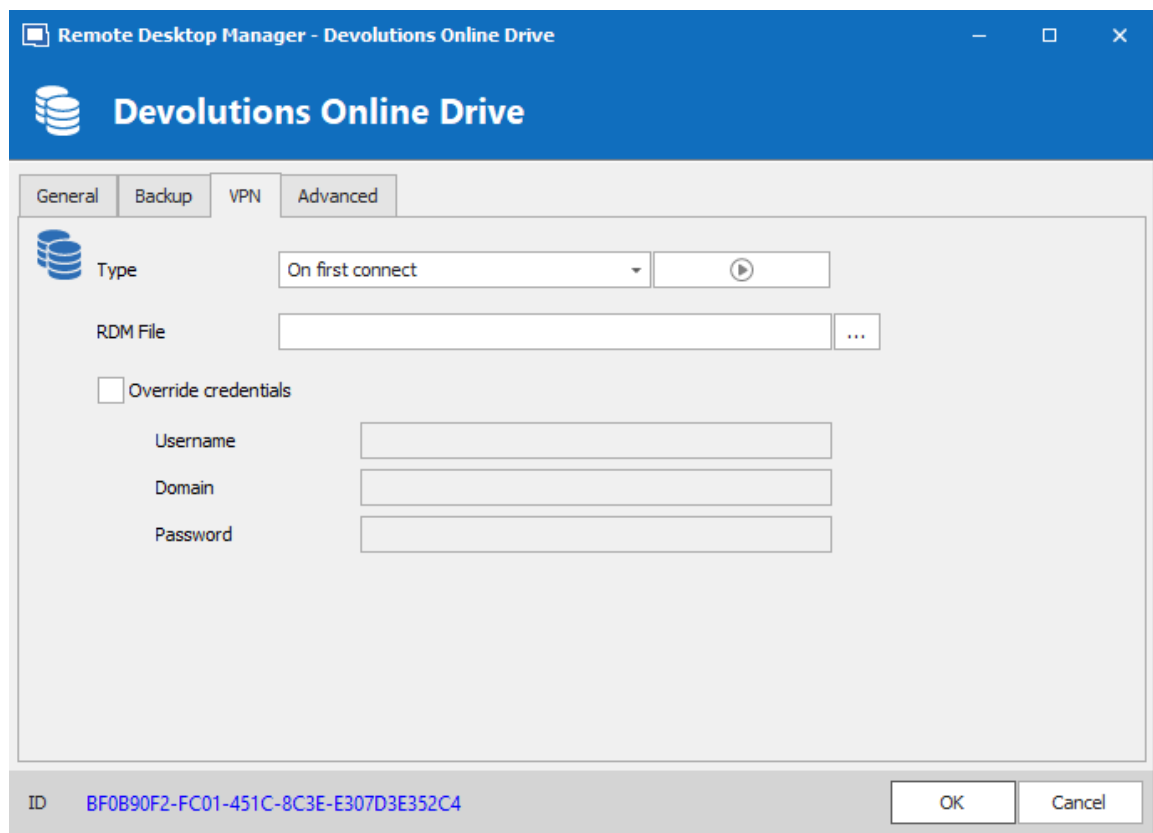
Please consult the [Online Backup](#) topic for information on this service.

*Devolutions Online Drive - Backup Tab*

OPTION	DESCRIPTION
<b>Backup</b>	<p>Choose the backup mode. Select between:</p> <ul style="list-style-type: none"><li>• <b>None:</b> No backup of the data source will be created.</li><li>• <b>File backup:</b> The backup will be saved to a local file when a modification occurs in the data source.</li><li>• <b>Online Backup:</b> An Online Backup (using the <a href="#">Online Backup</a>) will automatically be created when a modification occurs in the data source.</li></ul>

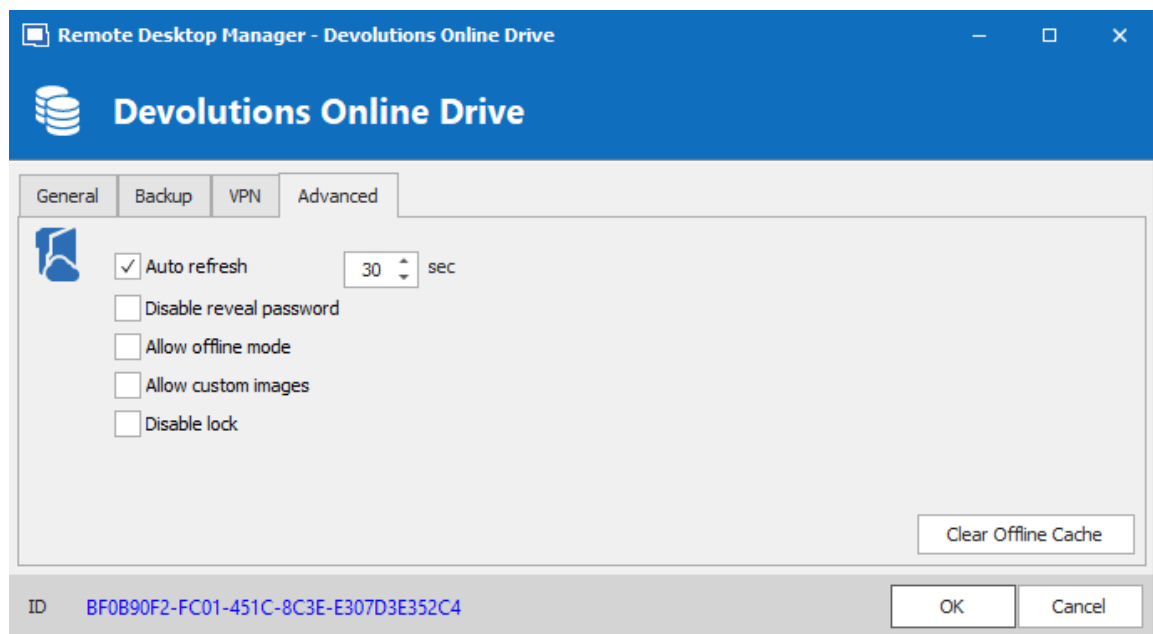
## VPN

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
<b>Auto refresh</b>	Set the interval to use between each automatic refresh.
<b>Disable reveal password</b>	Disable the reveal password feature when a user access the data source.
<b>Allow offline mode</b>	Allows the data source to be used in <a href="#">Offline mode</a> .
<b>Allow custom images</b>	Allows the use of custom images.
<b>Disable lock</b>	Disables the password query for locking application.
<b>Clear Offline Cache</b>	Clear the offline cache on the local computer. This can be very helpful when encountering offline issues.

### 5.4.5 Password Hub Personal

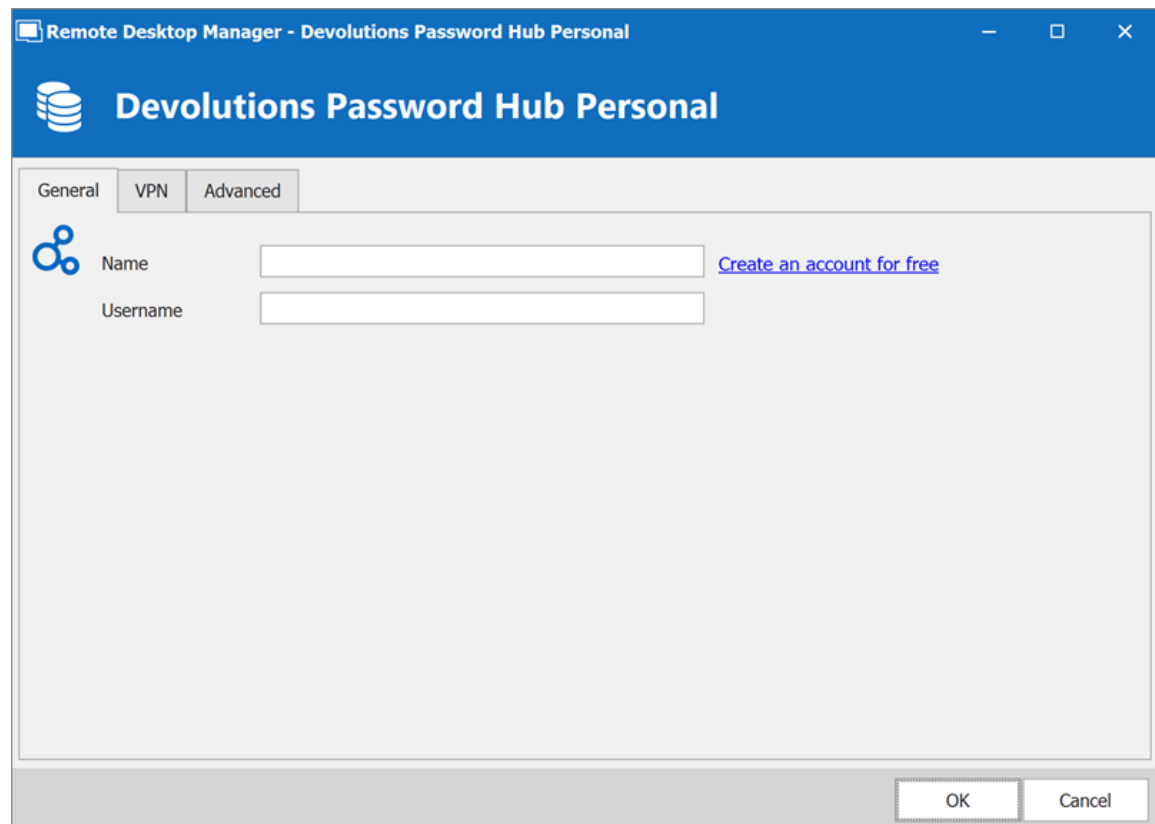
## DESCRIPTION

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



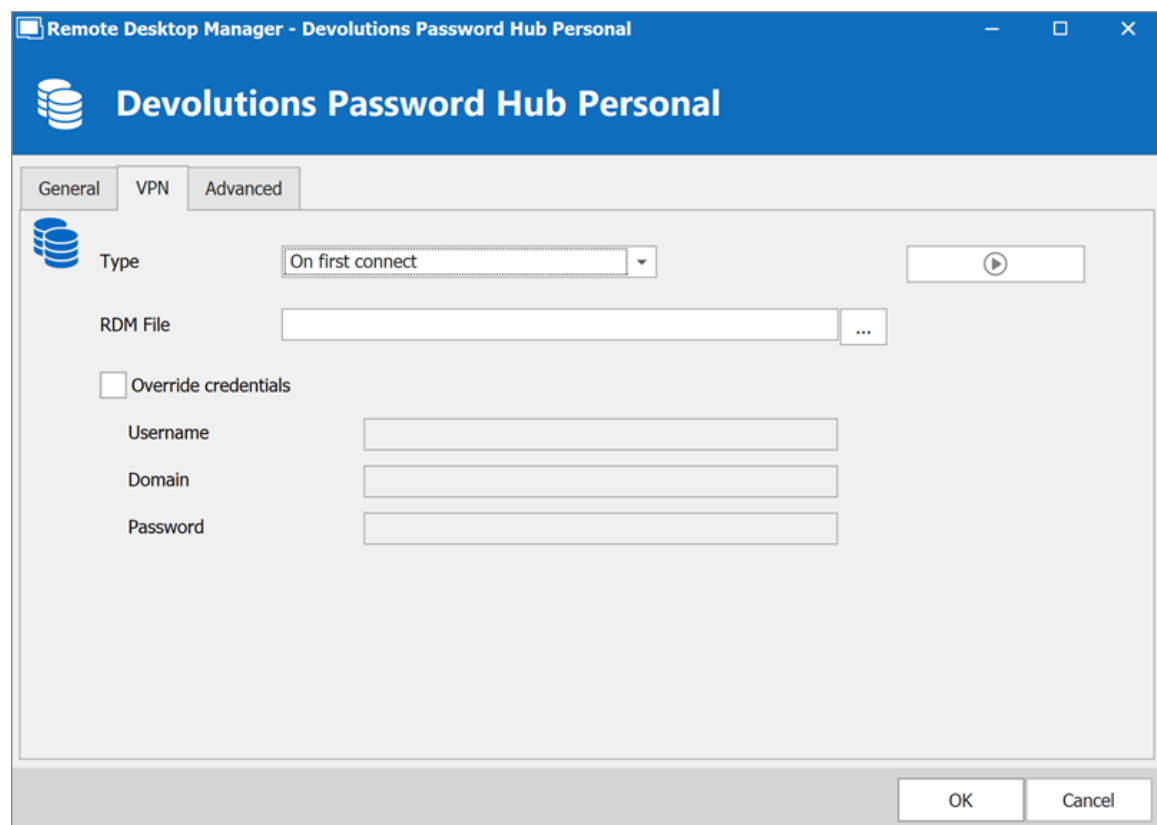
The screenshot shows a Windows-style dialog box titled "Remote Desktop Manager - Devolutions Password Hub Personal". The dialog has a blue header bar with the Devolutions logo and the text "Devolutions Password Hub Personal". Below the header, there are three tabs: "General", "VPN", and "Advanced". The "General" tab is selected. Inside the "General" tab, there is a Devolutions logo on the left. To the right of the logo, there are two text input fields: "Name" and "Username". To the right of the "Name" field, there is a blue link that says "Create an account for free". At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".



OPTION	DESCRIPTION
<b>Name</b>	Name of the data source.
<b>Username</b>	Your <a href="#">Devolutions Account</a> email address. You can create one for free, just follow the link provided.

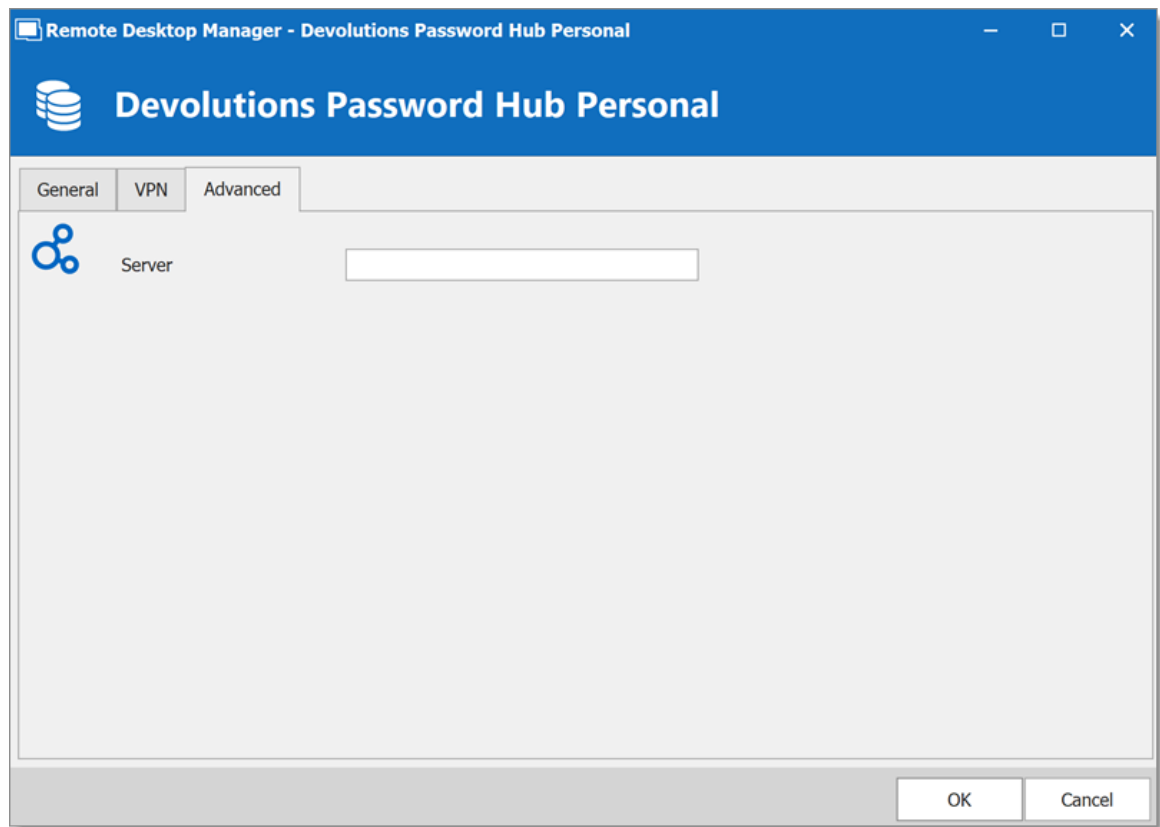
## VPN

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



## ADVANCED

This is the **Server** address.



#### 5.4.6 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.

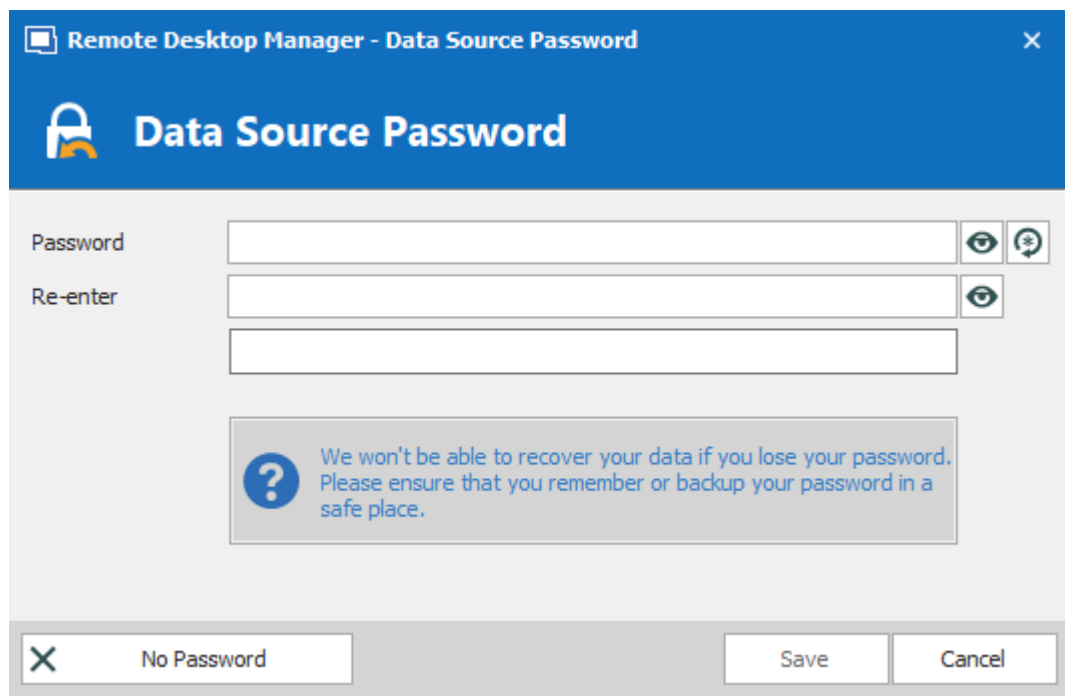


SQLite supports an unlimited number of simultaneous readers, but will only allow one writer at any instant in time. For this reason Remote Desktop Manager does not support sharing a SQLite data source between several users by storing it on a network drive. If you want to share your data and work in a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

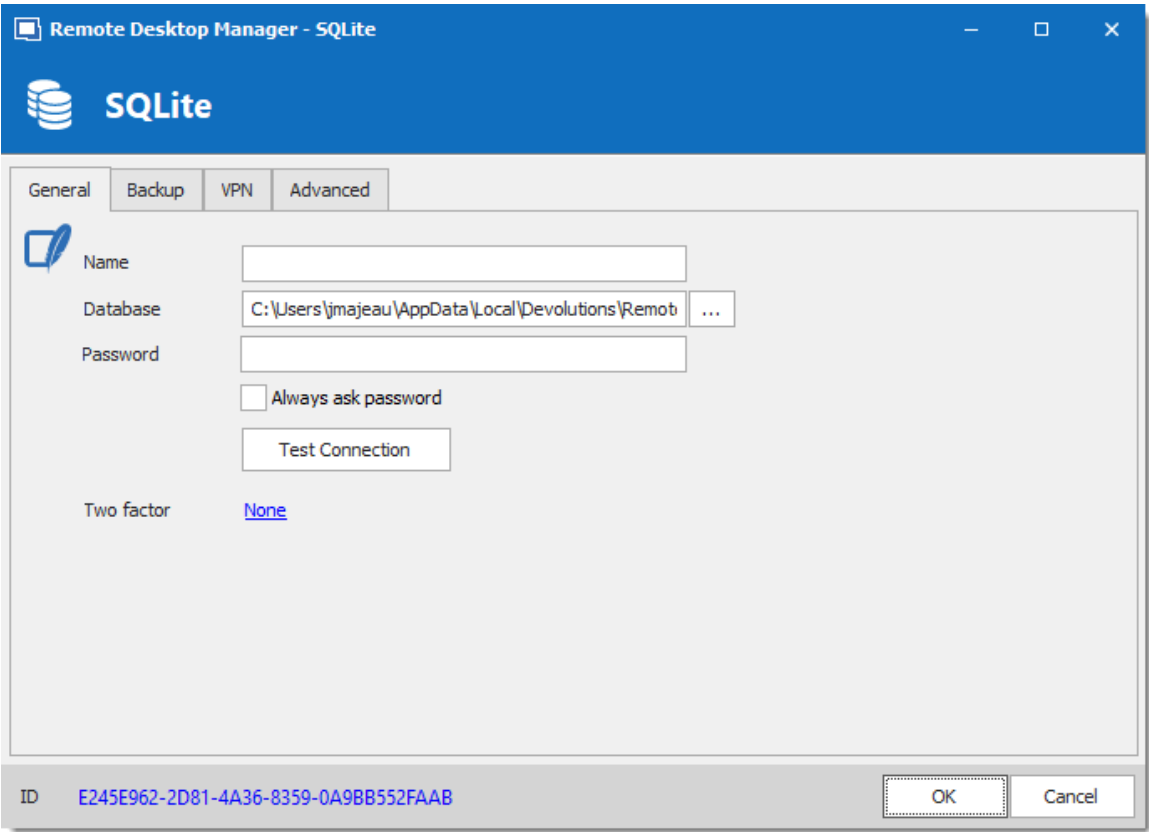


The image shows a Windows-style dialog box titled "Remote Desktop Manager - Data Source Password". The dialog has a blue header bar with a lock icon and the title "Data Source Password". Below the header, there are two text input fields labeled "Password" and "Re-enter". The "Password" field has a toggle icon (an eye with a slash) to its right, and the "Re-enter" field has a similar toggle icon. Below these fields is a warning box with a question mark icon and the text: "We won't be able to recover your data if you lose your password. Please ensure that you remember or backup your password in a safe place." At the bottom of the dialog, there are three buttons: "No Password" (with a close icon), "Save", and "Cancel".

*Manage password dialog*

## SETTINGS

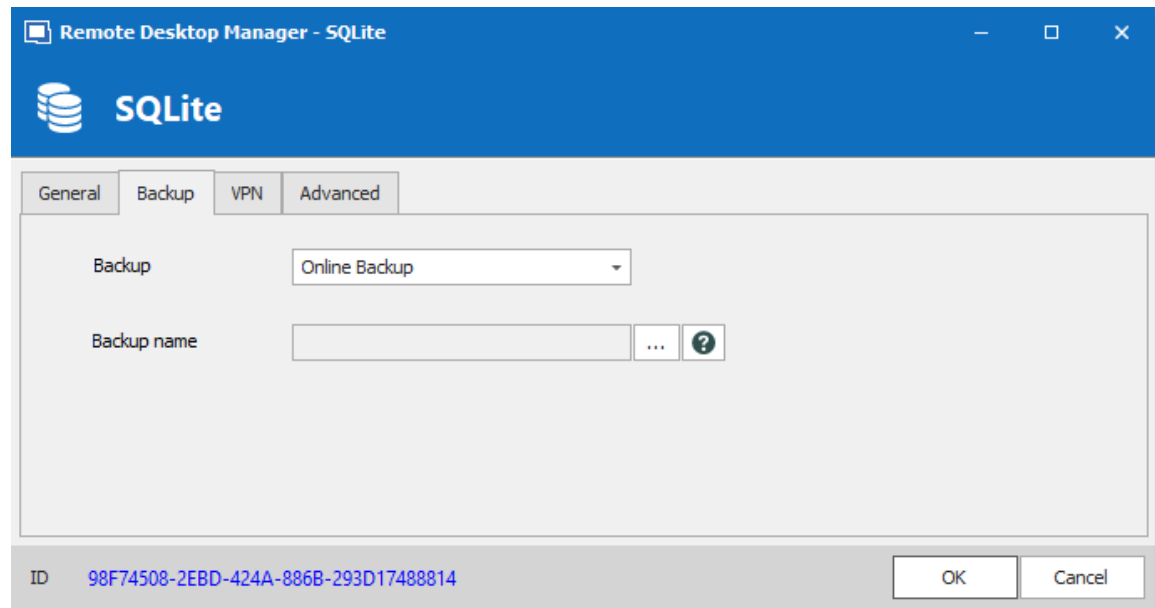
### GENERAL



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 <a href="#">2-Factor Authentication</a> to access your data source.

## BACKUP

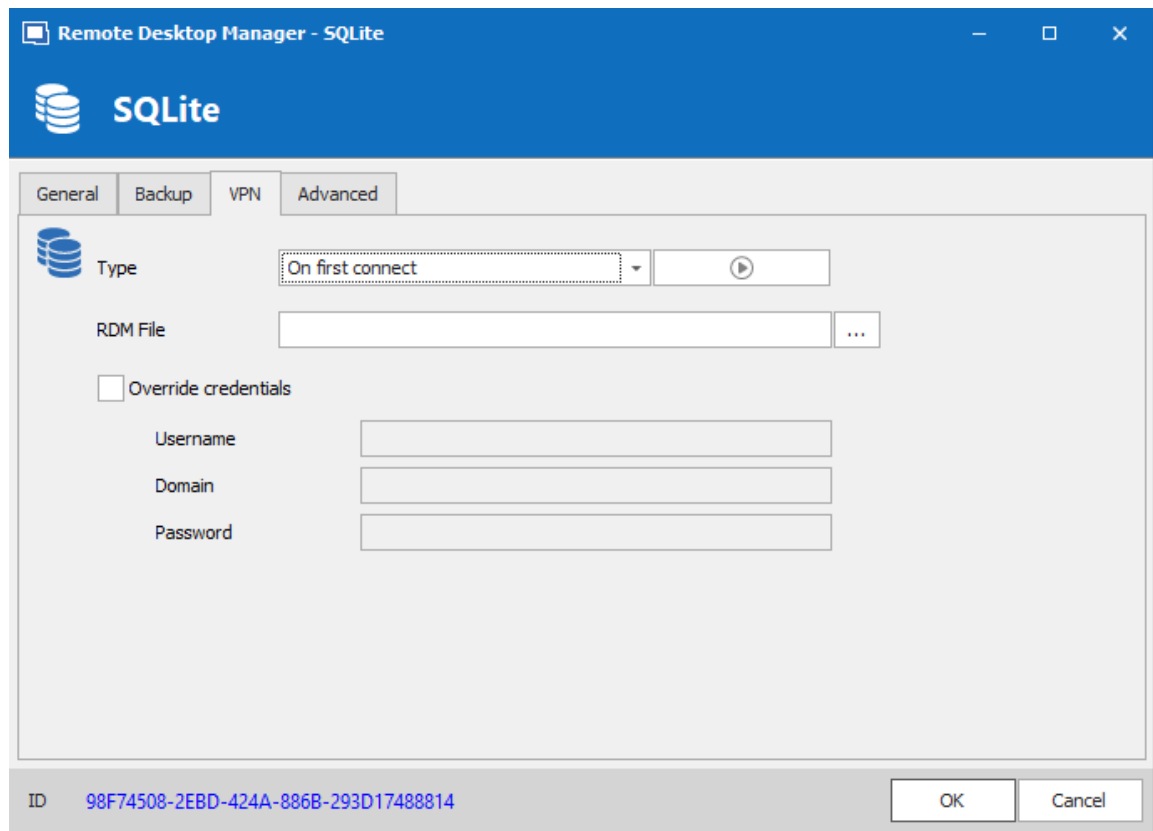


*SQLite - Backup Tab*

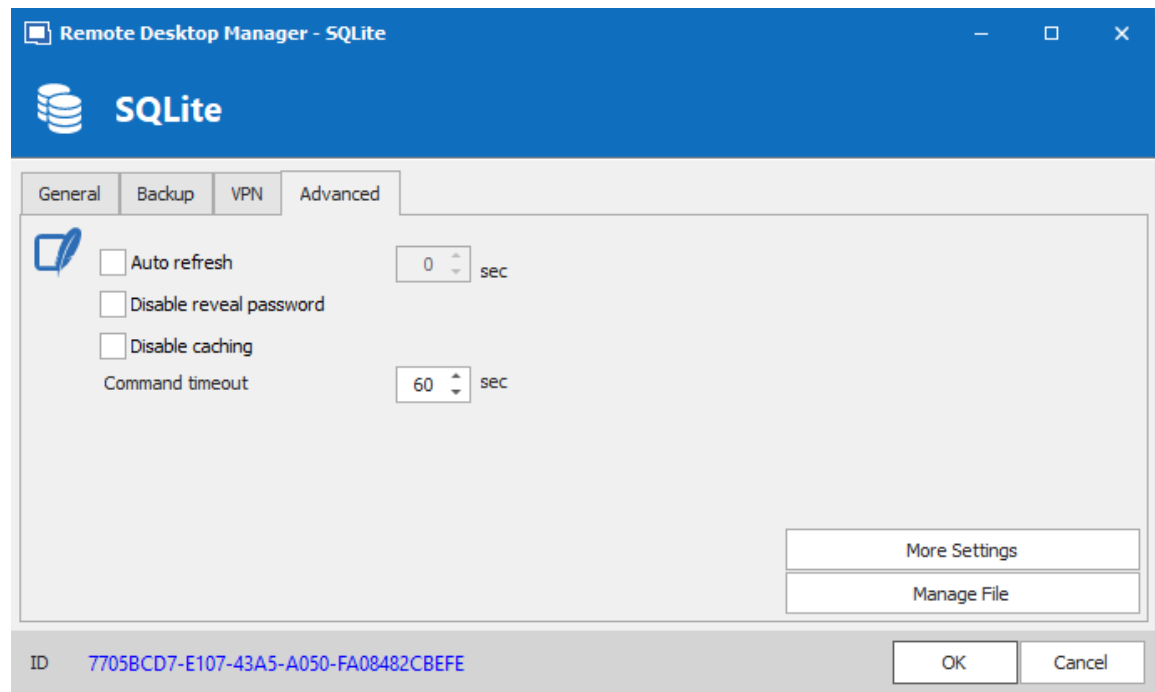
OPTION	DESCRIPTION
<b>Backup</b>	<p>Select between:</p> <ul style="list-style-type: none"><li>• <b>None:</b> No backup of your data source will be created.</li><li>• <b>File backup:</b> Your backup will be saved to a chosen file but will not automatically do backup every 30 seconds.</li><li>• <b>Online Backup:</b> An Online Backup (using <a href="#">Online Backup</a>) will automatically be created.</li></ul>

## VPN

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

*SQLite - VPN Tab*

## ADVANCED



SQLite - Advanced Tab

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



## 5.4.7 WebDAV

### DESCRIPTION



With the WebDAV data source, Remote Desktop Manager downloads and uploads the session settings directly from a file located on a WebDAV site.

### SETTINGS

#### GENERAL

The screenshot shows a dialog box titled 'Remote Desktop Manager - WebDav'. The 'General' tab is selected, showing fields for Name, Host, Port (set to 80), Username, Password, Master key, and Filename. There are checkboxes for 'Use SSL', 'Always ask password', 'Always ask master key' (checked), and 'Read-only'. The ID field at the bottom contains the value '33E54F5C-3AC4-4762-BA16-B63F4C19518F'. The dialog has 'OK' and 'Cancel' buttons at the bottom right.

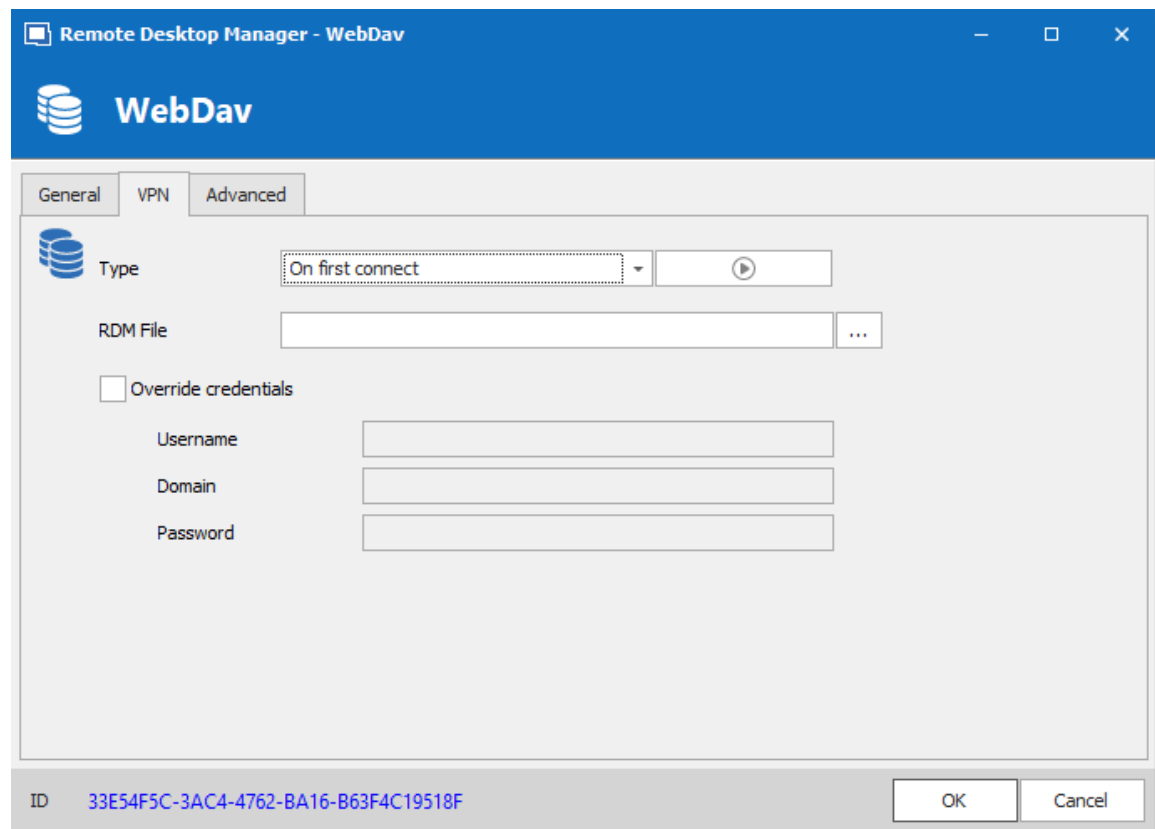
Field	Value / Option
Name	
Host	
Port	80
Use SSL	<input type="checkbox"/>
Username	
Password	
Always ask password	<input type="checkbox"/>
Master key	
Always ask master key	<input checked="" type="checkbox"/>
Filename	
Read-only	<input type="checkbox"/>
ID	33E54F5C-3AC4-4762-BA16-B63F4C19518F

WebDAV - General Tab

OPTION	DESCRIPTION
<b>Name</b>	Enter the name of the data source.
<b>Host</b>	Enter the hostname or IP address of the remote device.
<b>Port</b>	Enter the port of the remote device.
<b>Use SSL</b>	Use the SSL encryption.
<b>Username</b>	Enter the account username to access to the remote device.
<b>Password</b>	Enter the account password to access to the remote device.
<b>Always ask password</b>	Always ask password input when connecting to the data source.
<b>Master key</b>	Add an additional security layer by encrypting your data source with a master key.
<b>Always ask master key</b>	Always prompt for the master key when connecting to the data source.
<b>Filename</b>	Enter the file name. If it does not exists, it will be created automatically.
<b>Read-only</b>	Set the data source to read-only.

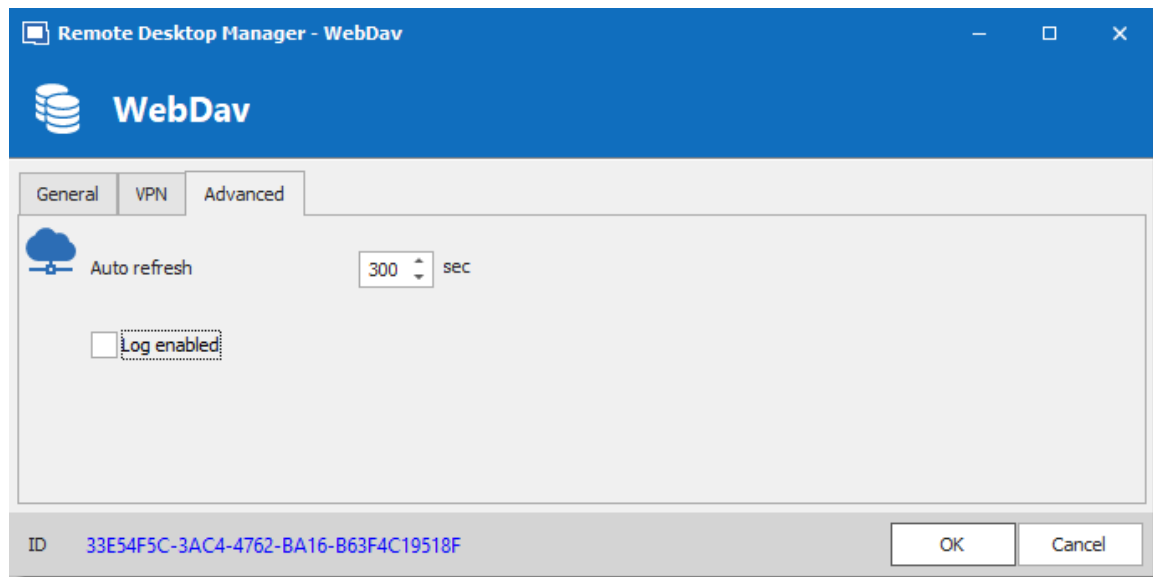
## VPN

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



*WebDAV - VPN Tab*

## ADVANCED

*WebDAV - Advanced Tab*

OPTION	DESCRIPTION
<b>Auto refresh</b>	Set the interval for the automatic refresh.
<b>Log enabled</b>	Enables logging and its features.

#### 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

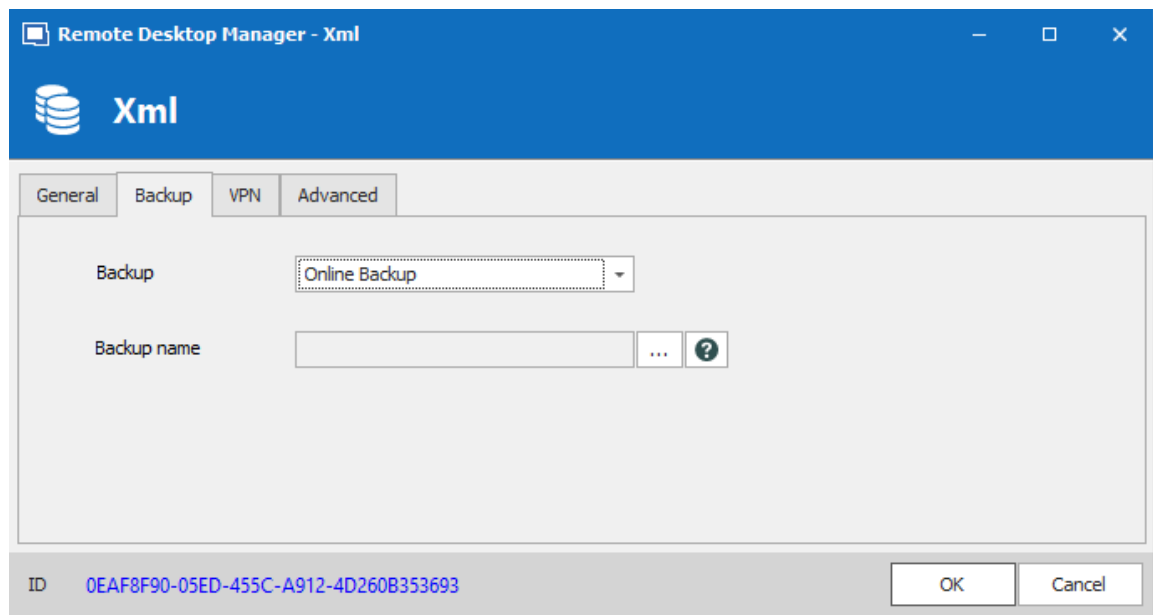
### GENERAL

The screenshot shows the 'Remote Desktop Manager - Xml' settings window. The title bar is blue with the text 'Remote Desktop Manager - Xml' and standard window controls. Below the title bar is a blue header with a database icon and the word 'Xml'. The main area has four tabs: 'General' (selected), 'Backup', 'VPN', and 'Advanced'. Under the 'General' tab, there is an 'XML' icon and three input fields: 'Name' (empty), 'Filename' (containing 'C:\Users\jmajeau\AppData\Local\Devolutions\Remo' with a browse button), and 'Master key' (empty). Below these fields is a checkbox labeled 'Always ask master key' which is checked. At the bottom, there is an 'ID' field containing '0EAF8F90-05ED-455C-A912-4D260B353693' and two buttons: 'OK' and 'Cancel'.

XML - General Tab

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

## BACKUP

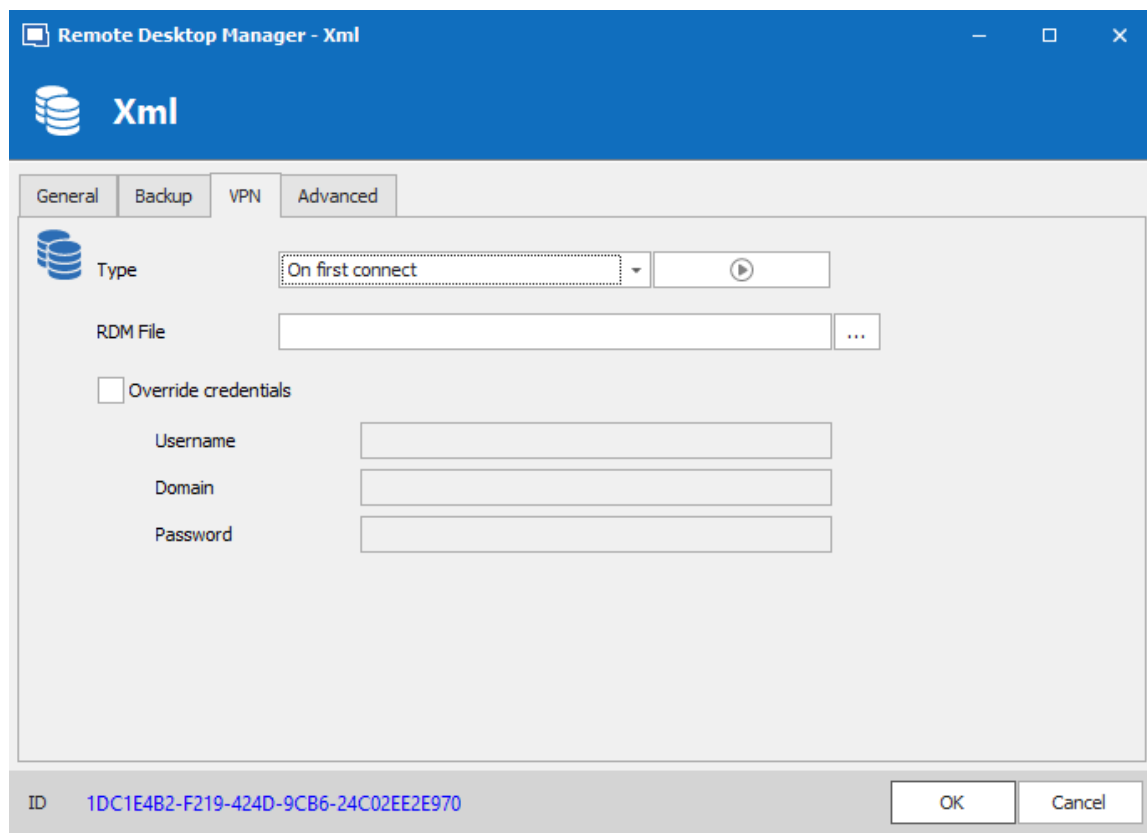


XML - Backup Tab

OPTION	DESCRIPTION
<b>Backup</b>	<p>Select between:</p> <ul style="list-style-type: none"><li>• <b>None:</b> No backup of your data source will be created.</li><li>• <b>File backup:</b> Your backup will be saved to a chosen file but will not automatically do backup every 30 seconds.</li><li>• <b>Online Backup:</b> An Online Backup (using <a href="#">Online Backup</a>) will automatically be created.</li></ul>
<b>Backup name</b>	<p>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.</p>

## VPN

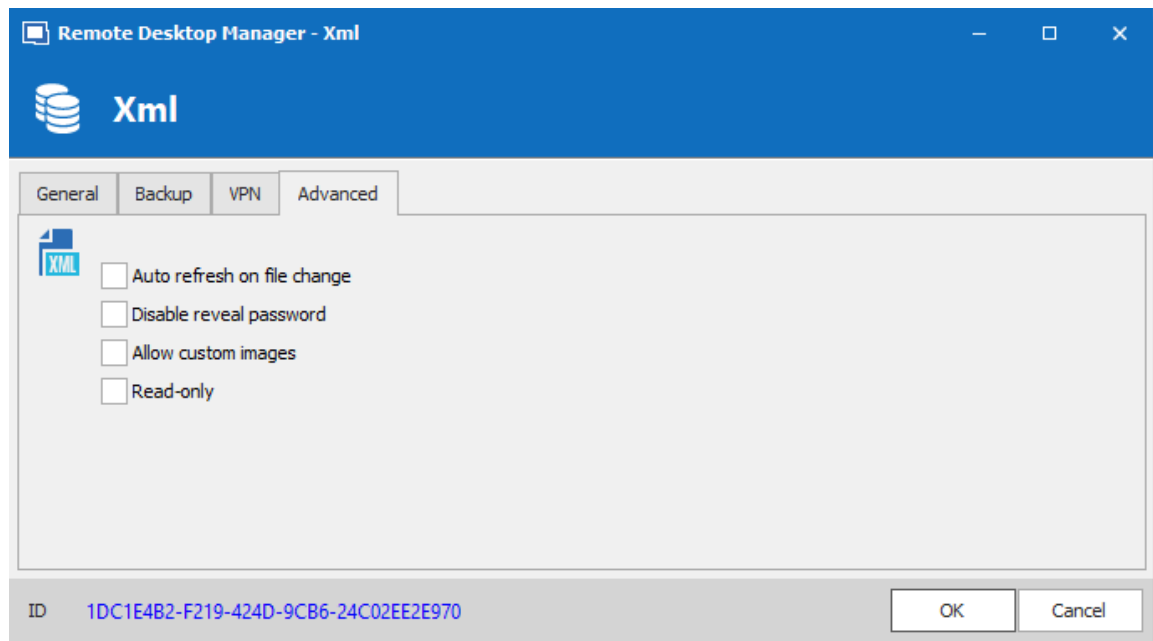
Open a VPN to access your data prior to connecting to your **XML**.



XML - VPN Tab

## ADVANCED



*XML - Advanced Tab*

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

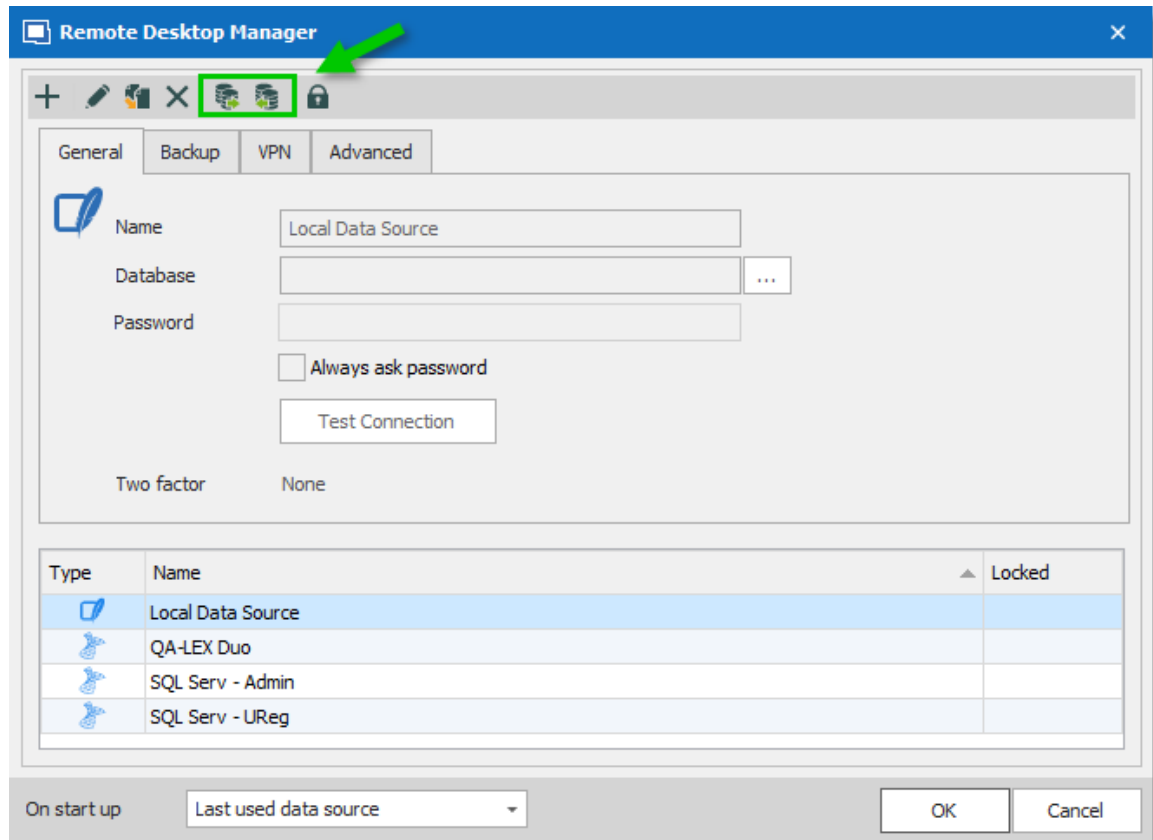
## 5.5 Import/Export Data Source

### 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.



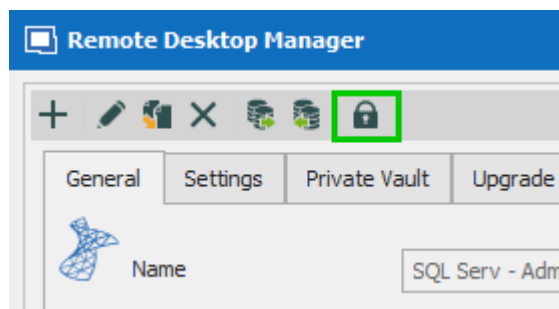
A locked data source can be exported and imported, but the content will be locked unless a password is entered when the data source is selected. See [Lock Data Source](#) for more information.

## 5.6 Lock Data Source

### LOCK DATA SOURCE

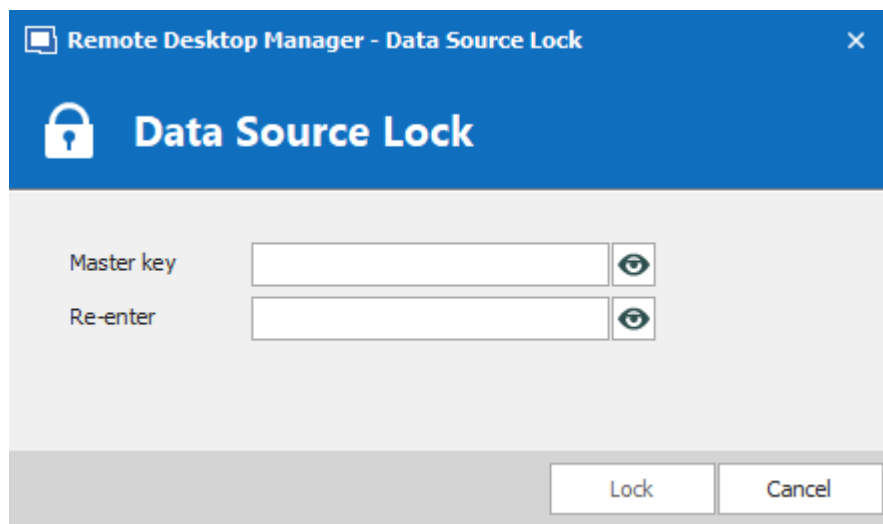
To protect sensitive data in your data source configuration (e.g. server URL or credentials), you may wish to lock the data source configuration before you deploy it to your users. You can do it by using the Lock/Unlock button from the toolbar.

### 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.

## 5.7 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 [Data Source Settings \(System Settings\)](#).

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).

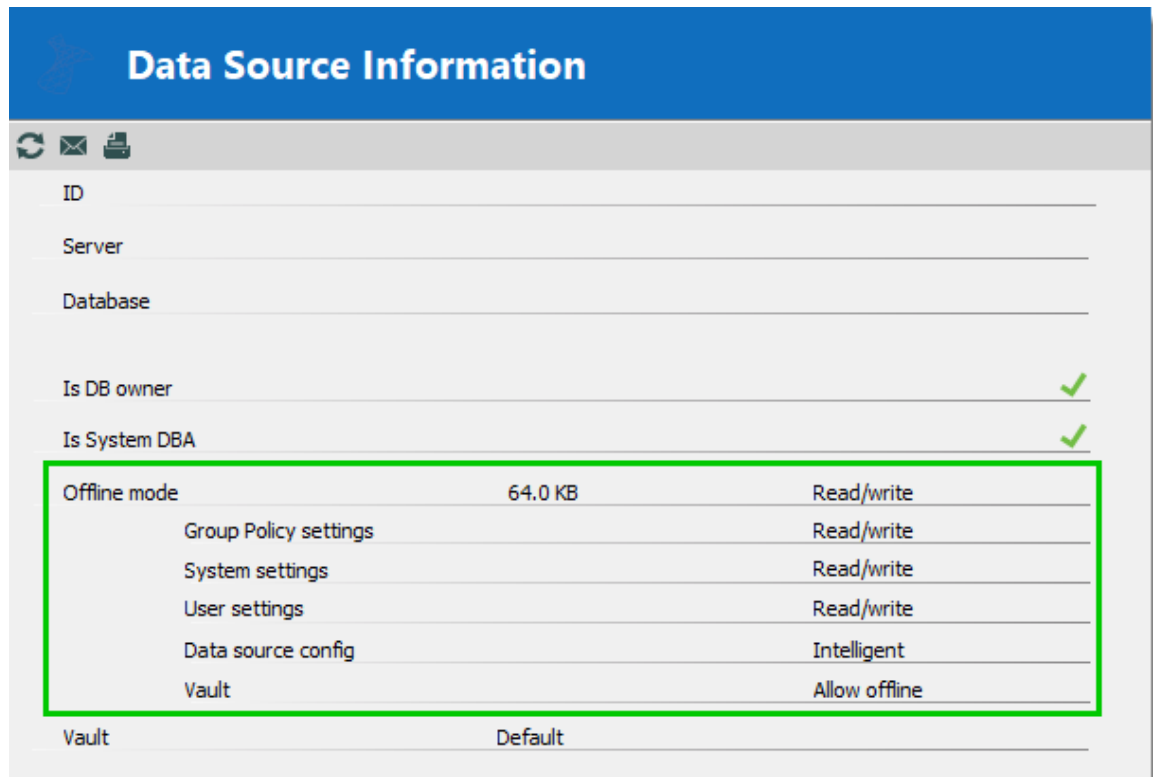
## AVAILABILITY

The offline mode availability relies on several settings:

- The data source offline cache must be enabled. (**This step needs to be done before you export your data source to other computers**)
- The user's account.
- The data source settings.
- The group policies.
- At the Vault level.

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**

Refresh, Email, Print icons

ID \_\_\_\_\_

Server \_\_\_\_\_

Database \_\_\_\_\_

Is DB owner ✓

Is System DBA ✓

Offline mode	64.0 KB	Read/write
Group Policy settings		Read/write
System settings		Read/write
User settings		Read/write
Data source config		Intelligent
Vault		Allow offline

Vault \_\_\_\_\_ Default \_\_\_\_\_

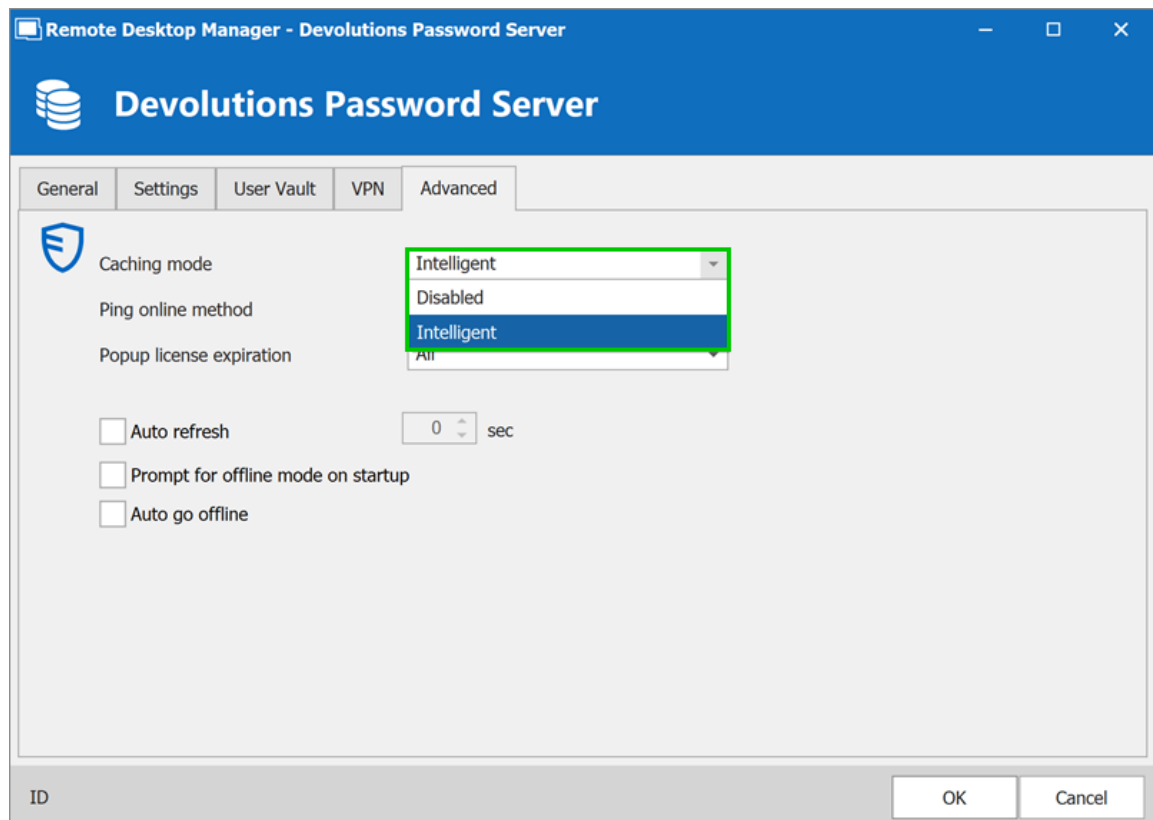
*My Data Source Information - Offline mode*

## 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
<b>Disabled</b>	Prevent an offline cache from being used.
<b>Intelligent</b>	Use the offline cache only for recent changes.



[Read/Write](#) offline mode is not available with the Basic subscription of [Devolutions Online Database](#).



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
<b>Disabled</b>	Prevents an offline cache from being used.
<b>Read-only</b>	Allow to view and use entries only. The content of the data source cannot be modified.
<b><a href="#">Read/Write</a></b>	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 at four levels:

- User permissions.
- Data source settings (System Settings) (server configuration).
- In a Vault's configuration.

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

USER PERMISSIONS	DATA SOURCE SETTINGS (SYSTEM SETTINGS)	Vault CONFIGURATION	EFFECTIVE ACCESS
Disabled or Read-only or Read/write	Disabled or Read-only or Read/write	<b>Allow offline disabled</b>	<b>Disabled</b>
Disabled or Read-only or Read/write	Disabled or Read-only or Read/write	Allow offline enabled	<b>Disabled</b>

USER PERMISSIONS	DATA SOURCE SETTINGS (SYSTEM SETTINGS)	Vault CONFIGURATION	EFFECTIVE ACCESS
Disabled or Read-only or Read/write	<b>Disabled</b>	Allow offline enabled	<b>Disabled</b>
<b>Disabled</b>	Disabled or Read-only or Read/write	Allow offline enabled	<b>Disabled</b>
Read-only or Read/write	Read-only or Read/write	<b>Allow offline disabled</b>	<b>Disabled</b>
Read-only or Read/write	Read-only or Read/write	Allow offline enabled	<b>Read-only</b>
Read-only or Read/write	<b>Read-only</b>	Allow offline enabled	<b>Read-only</b>
<b>Read-only</b>	Read-only or Read/write	Allow offline enabled	<b>Read-only</b>
<b>Read/write</b>	<b>Read/write</b>	<b>Allow offline enabled</b>	<b>Read/write</b>



You want to know the current effective Offline mode while connected?  
See [My Data Source Information](#).

### 5.7.1 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.

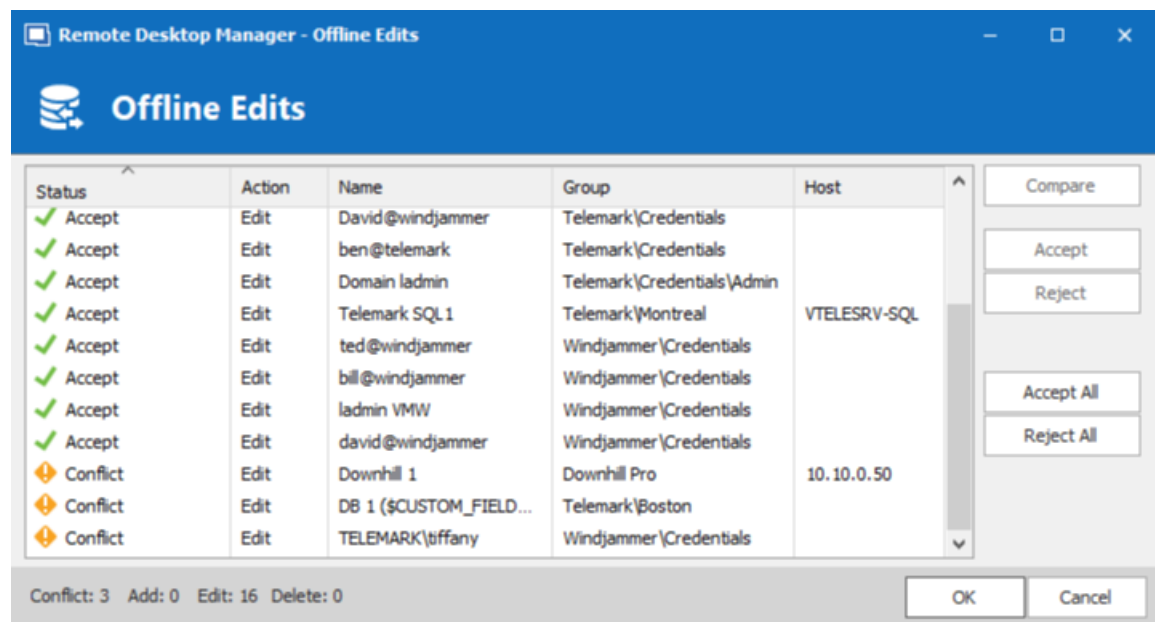
Once offline, the users security settings still applies. Add/Edit/Delete privileges granted by the administrator are still in effect. See [User Management](#).

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:

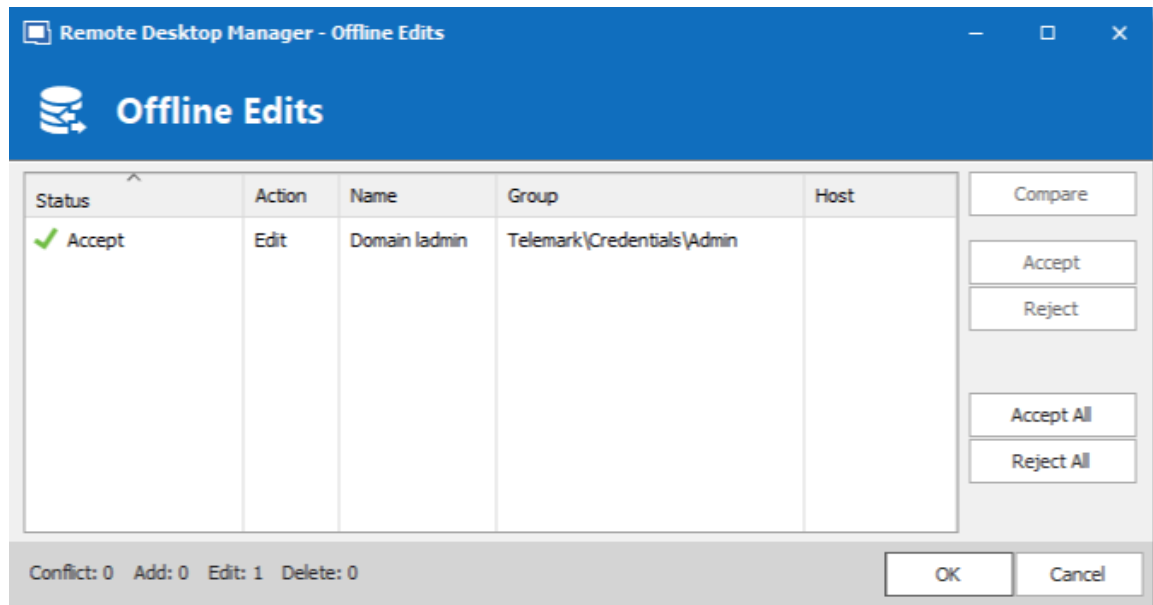
- Accept - when no outside changes have been detected.
- Conflict - when outside changes have been detected since you were last connected.

## MULTIPLE OFFLINE EDITS

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

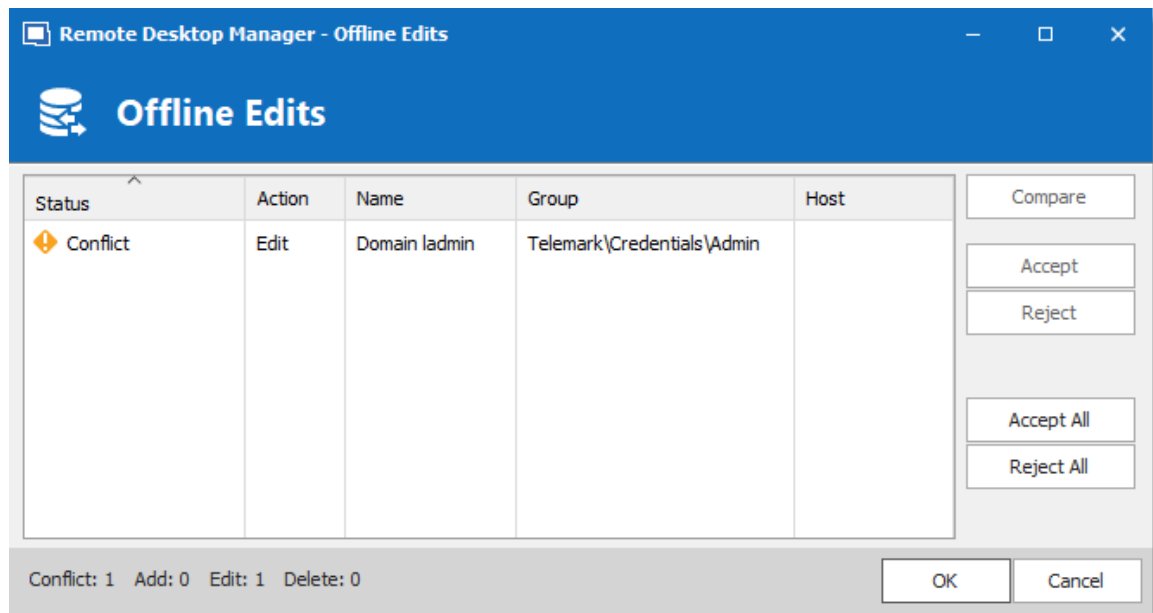
Here is an example of such a case to help resolving conflicts properly:

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.



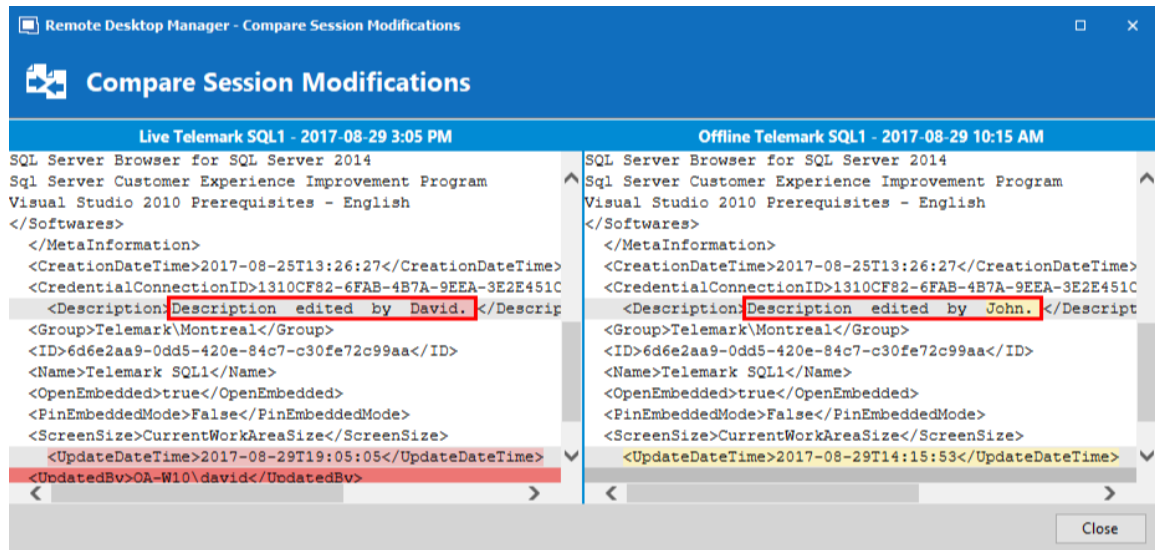
*Offline Edits For The Second User Back Online*

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

## 5.8 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**.

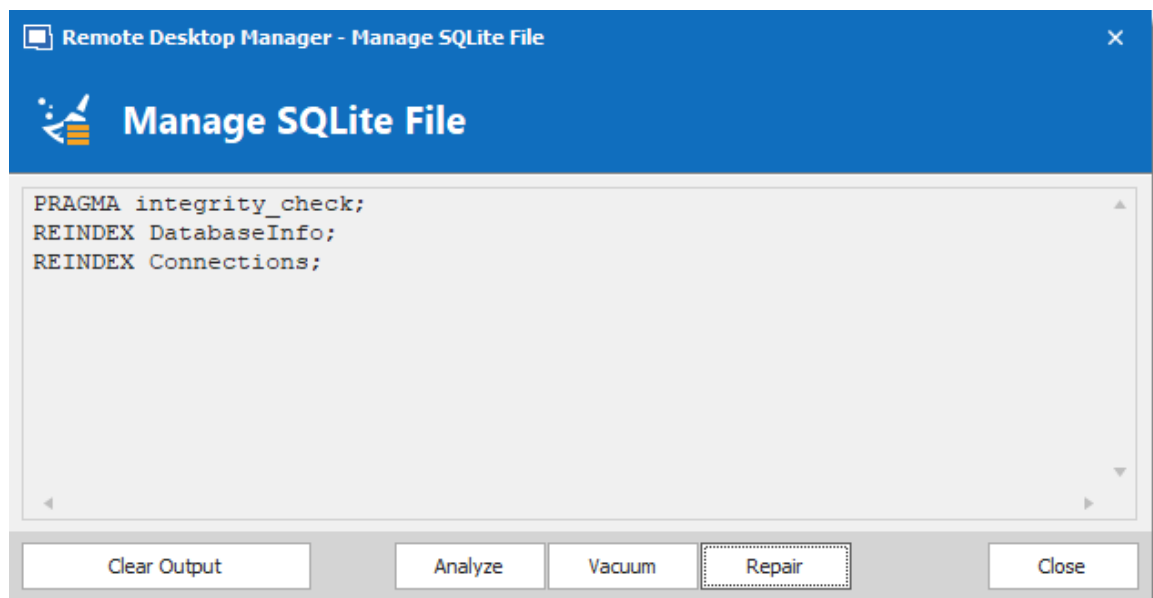


The Manage Cache options should usually only be used **upon request from our Support Team** when experiencing cache issue.

### SETTINGS



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



*Manage Cache*

OPTION	DESCRIPTION
<b>Clear output</b>	Clear the output window.
<b>Analyze</b>	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.
<b>Vacuum</b>	This will run an SQLite command to reduce your cache size. The Vacuum should only be used <b>after trying to execute a Repair</b> of your cache. If the repair hasn't solved your issue running a Vacuum will usually solve issues when dealing with a corrupted cache.
<b>Repair</b>	<p>The repair will run four different SQLite commands to repair a corrupted cache:</p> <ul style="list-style-type: none"> <li>▪ PRAGMA integrity_check</li> <li>▪ REINDEX DatabaseInfo</li> <li>▪ REINDEX Connections</li> <li>▪ REINDEX Properties</li> </ul>

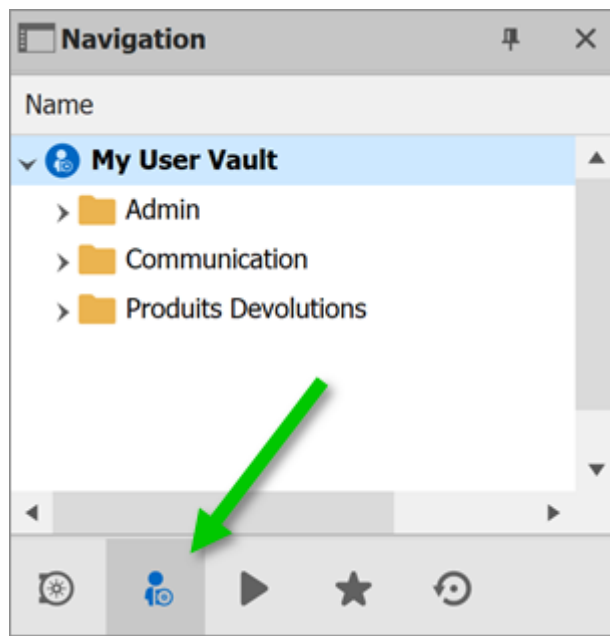
## 5.9 User Vault

### 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

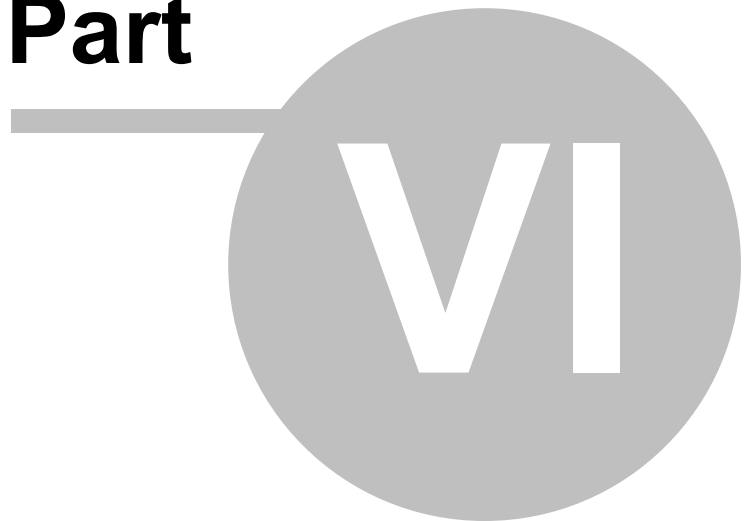
Credentials in the User Vault can be used in two ways:

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**

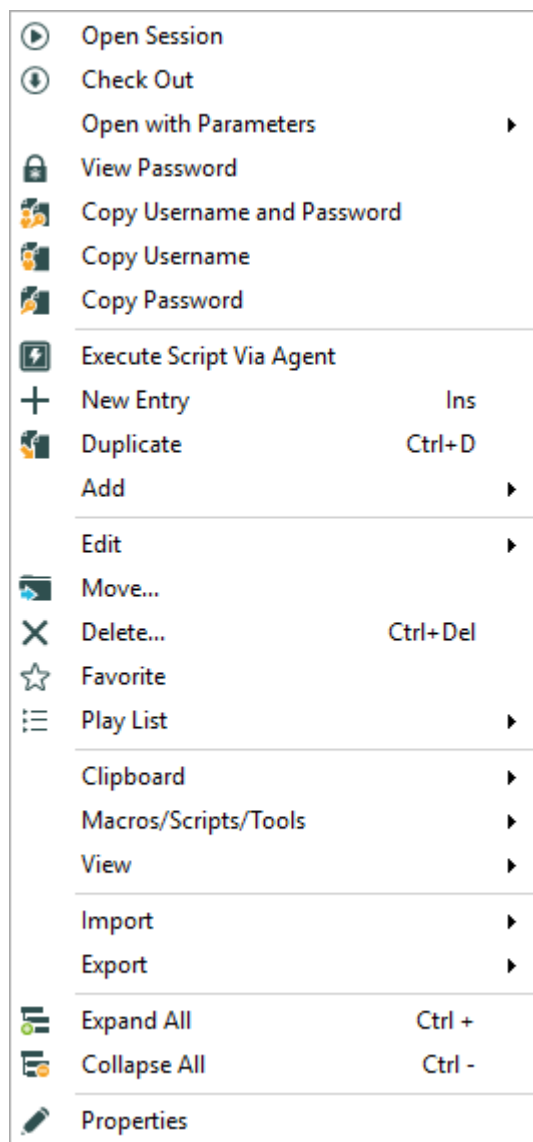


## 6 Commands

### 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.



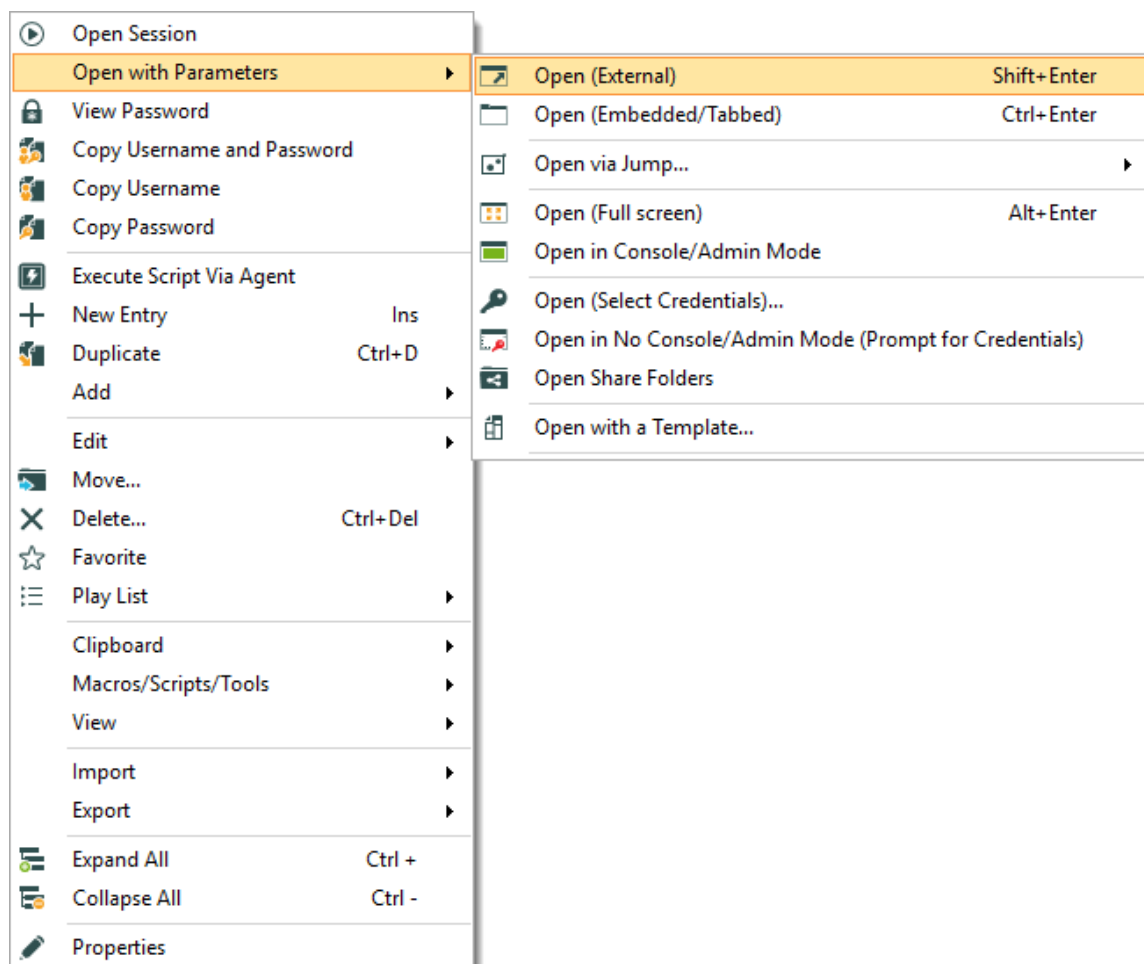
*Context Menu*



### 6.1.1 Open with Parameters

## DESCRIPTION

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



*Open with Parameters*

OPTION	DESCRIPTION
<b>Open (External)</b>	Open a session as an external process, with no direct link to Remote Desktop Manager.
<b>Open (Embedded/Tabbed)</b>	Open the session within the confines of the Remote Desktop Manager dashboard and display tabs at the top

OPTION	DESCRIPTION
	of the window.
<b>Open via Jump...</b>	Open the session through a <a href="#">Jump</a> host.
<b>Open (Full Screen)</b>	Open the session with the full screen display mode.
<b>Open in Console/Admin Mode</b>	Connect to the console session of a server using Remote Desktop for Administration.
<b>Open (Select Credentials)...</b>	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.
<b>Open in No Console/Admin Mode</b> <b>(Prompt for Credentials)</b>	Open your session normally and prompt your for your credentials to connect.
<b>Open Share Folders</b>	Open the shared folders of the remote computer.
<b>Open with a Template...</b>	Open from a template that you have already created.
<b>VPN</b>	Select between: <ul style="list-style-type: none"><li>• <b>Open (Without VPN).</b></li><li>• <b>Open VPN Only.</b></li><li>• <b>Close VPN Only.</b></li></ul>

## 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.



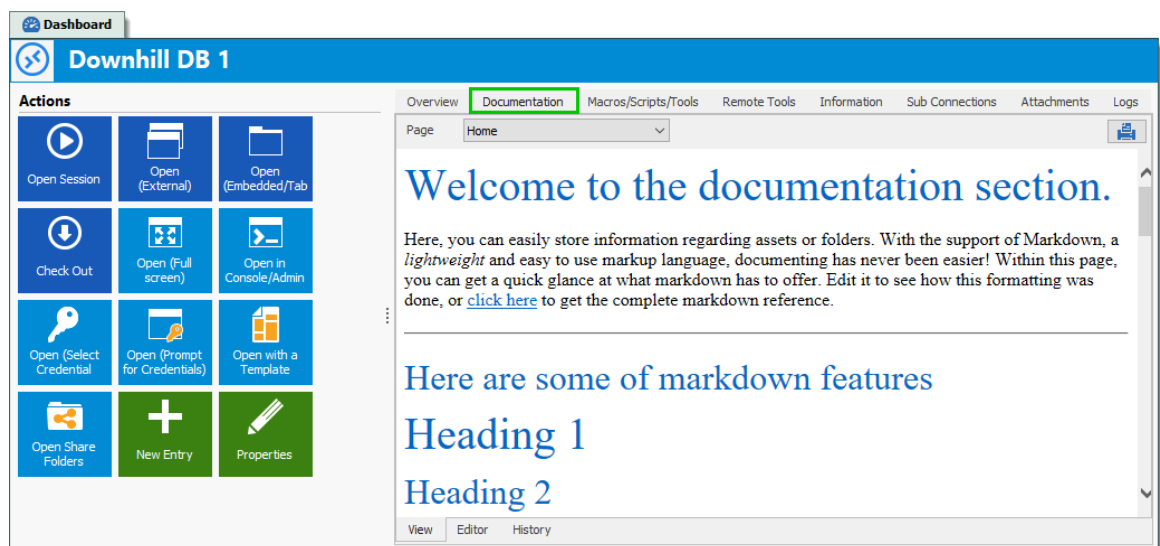
This feature is available with Devolutions Server, MariaDB, MySQL and SQL Server data sources.



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



The Documentation feature is not available offline.

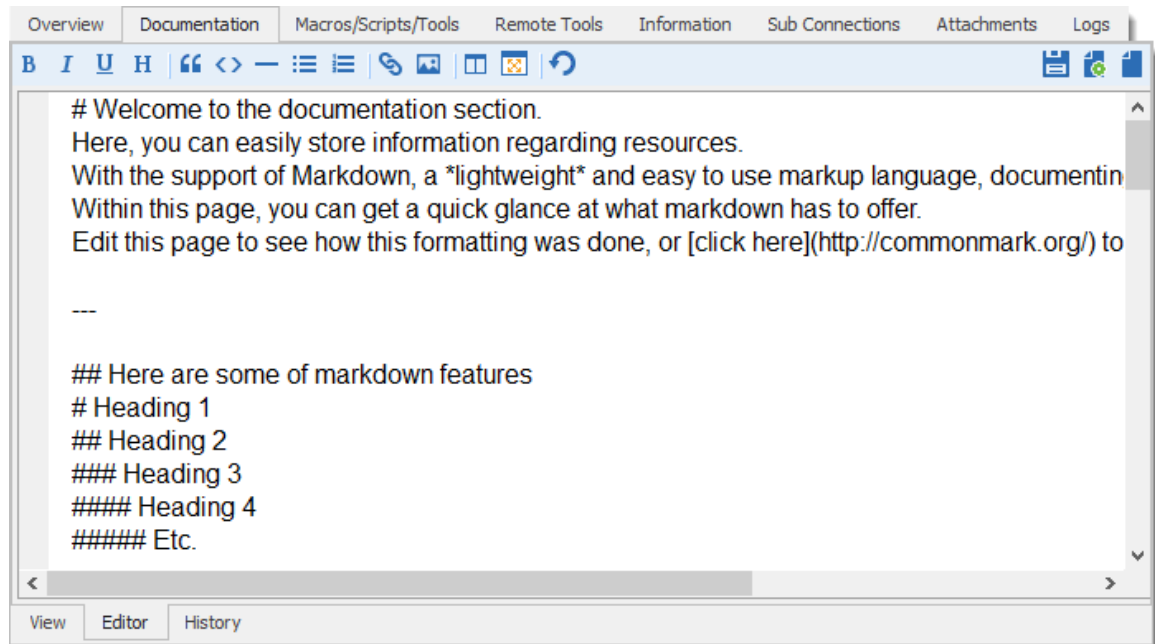


Documentation of an entry

### 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.

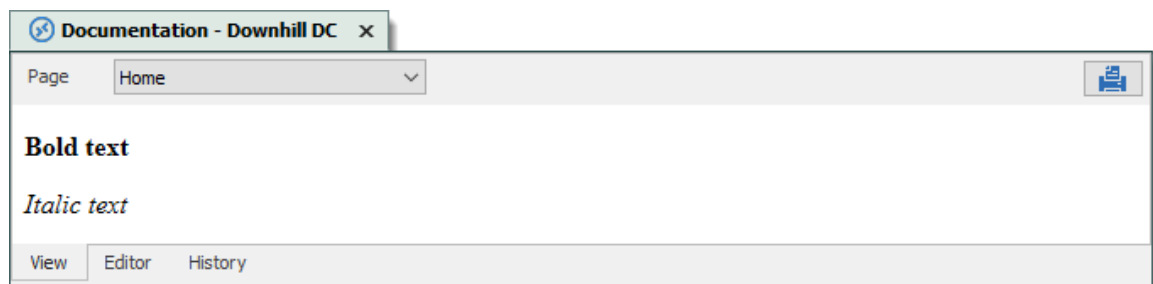
## EMPHASIS

Two methods of text emphasis are available:

`**Bold text**`

`*Italic text*`

Output:



## HEADERS

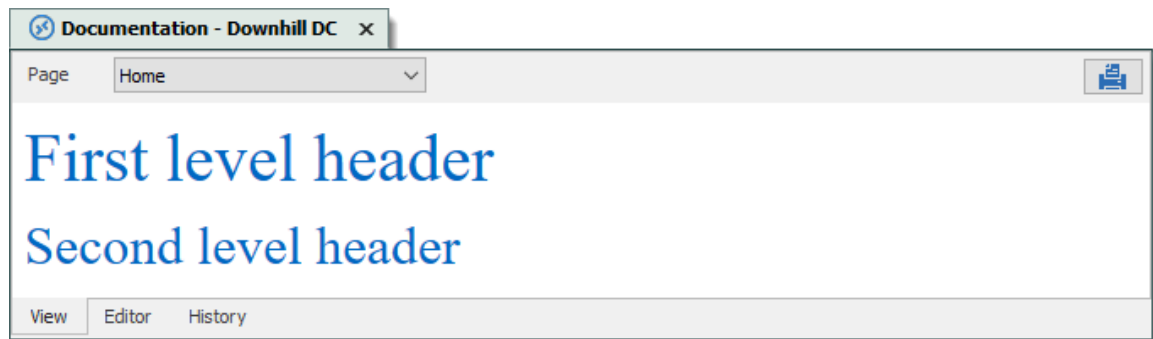
There are two ways of creating headers with Markdown.

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

`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

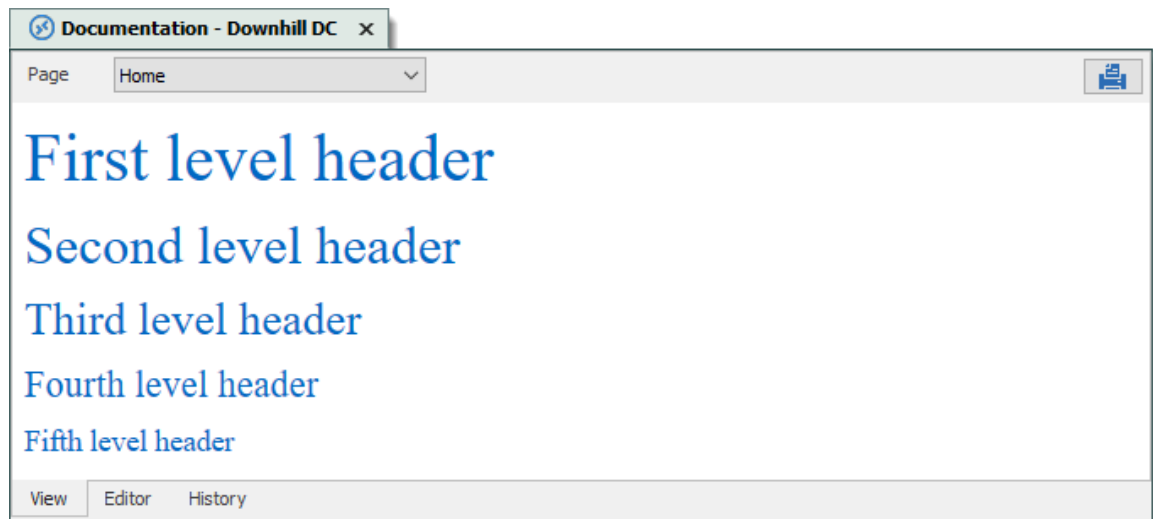
## Second level header

### 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 interchangeable.

- \* Item 1
- \* Item 2
- \* Item 3

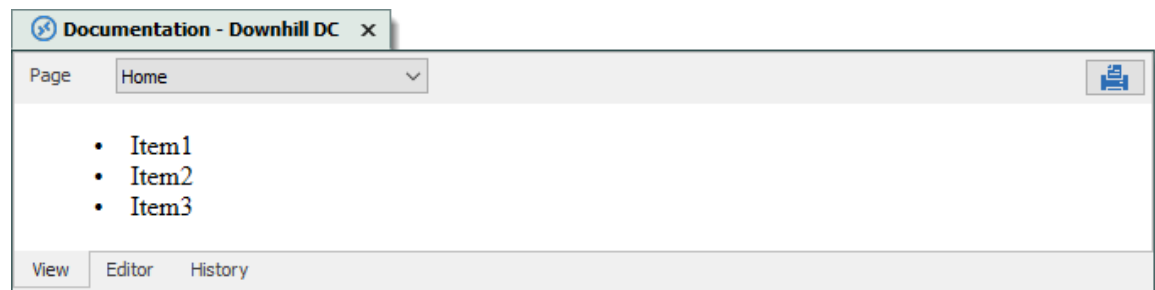
or

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

or

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

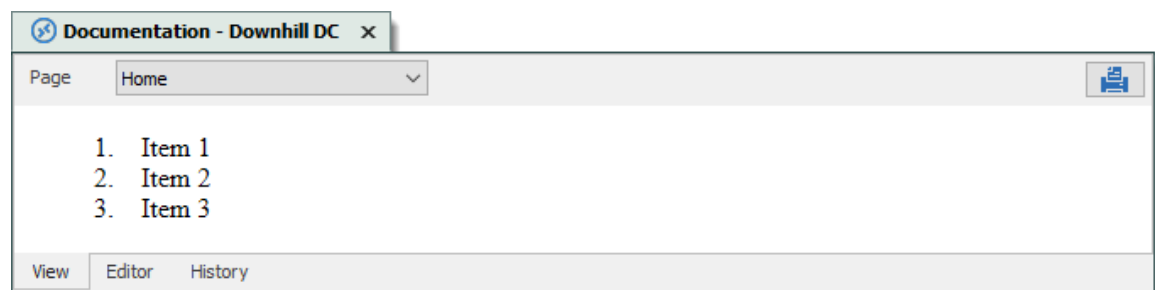
Output:



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 underscores, asterisks, or hyphens to create a horizontal ruler.

---

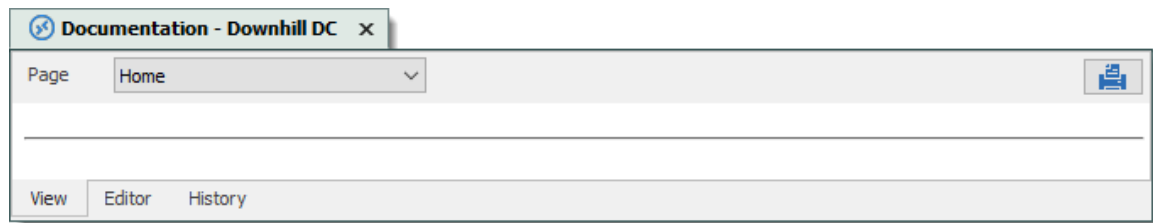
or

\*\*\*

or

---

Output:



## LINKS

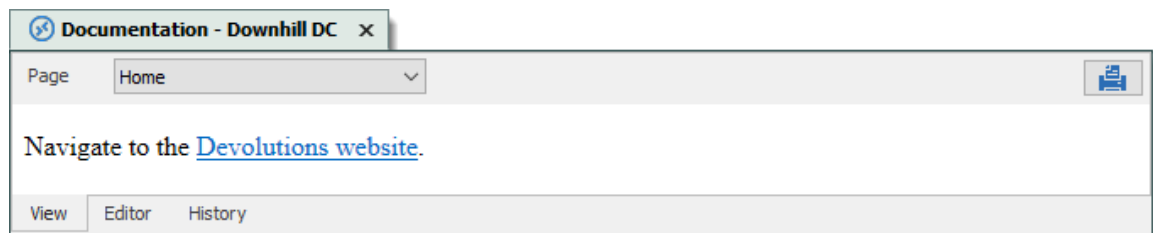
Use square brackets to delimit the text you want to turn into a link.

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).

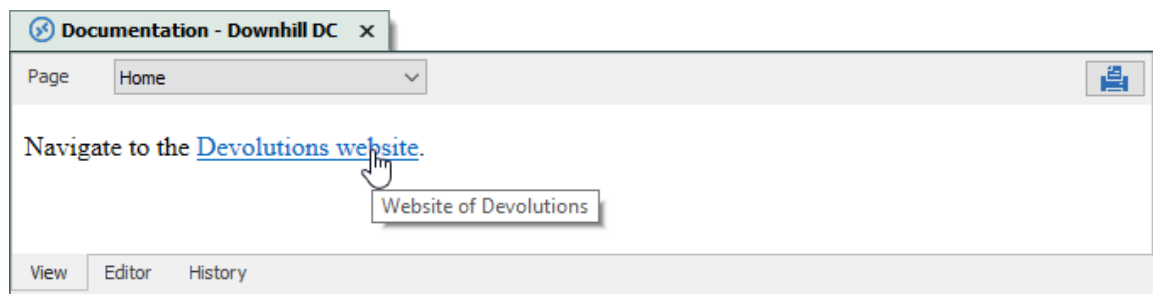
Output:



Optionally a title attribute may be included in the parentheses.

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

Output:



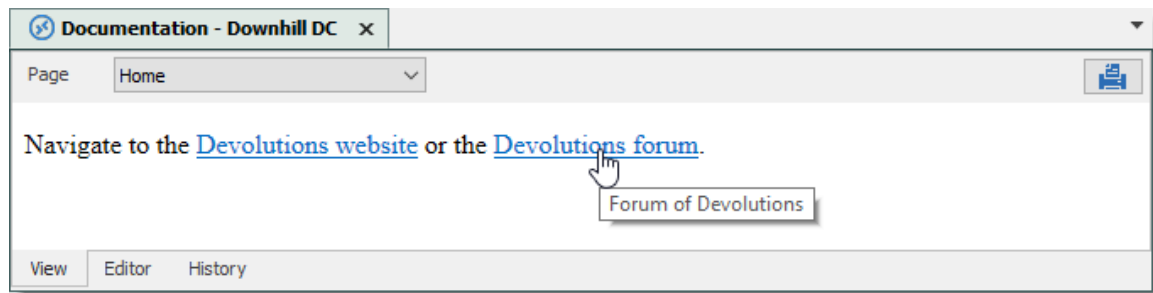
For reference-style links, define the links elsewhere in the document, then refer to a link by its name in another set of square brackets.

Navigate to the [Devolutions website][mainwebsite] or the [Devolutions forum][forumwebsite].

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

Output:




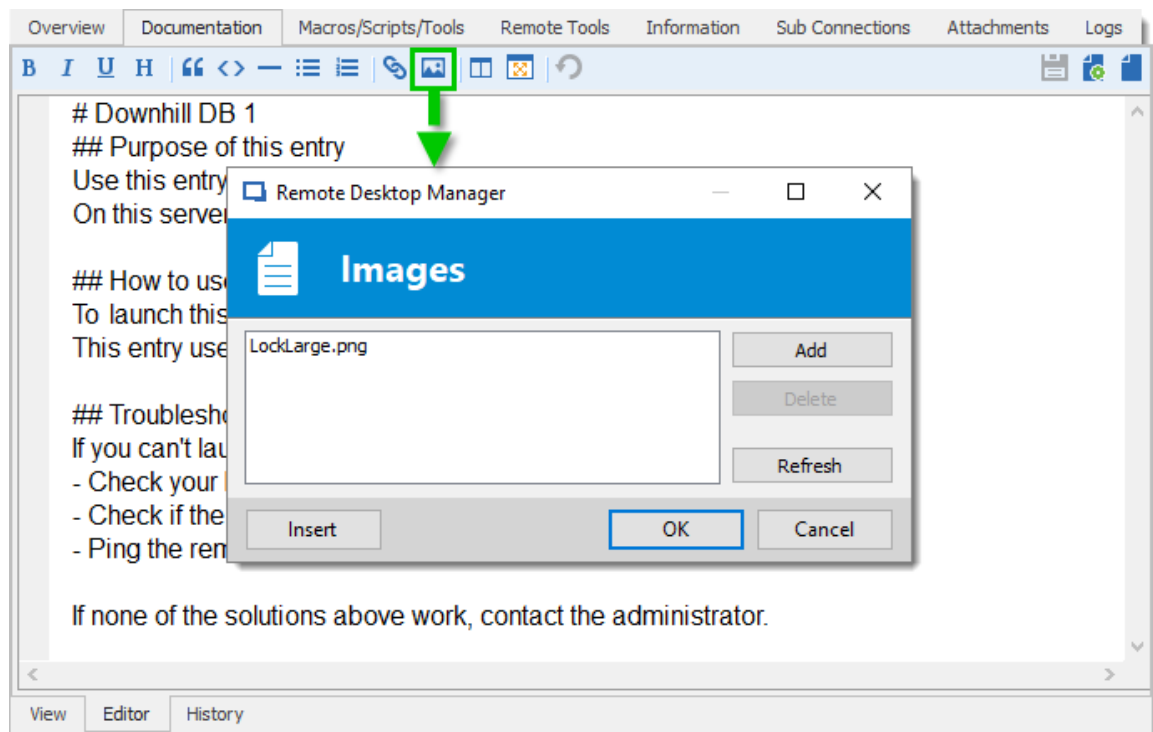


The title attribute is optional again. Link names may contain letters, numbers and spaces, but are not case sensitive.

## IMAGES

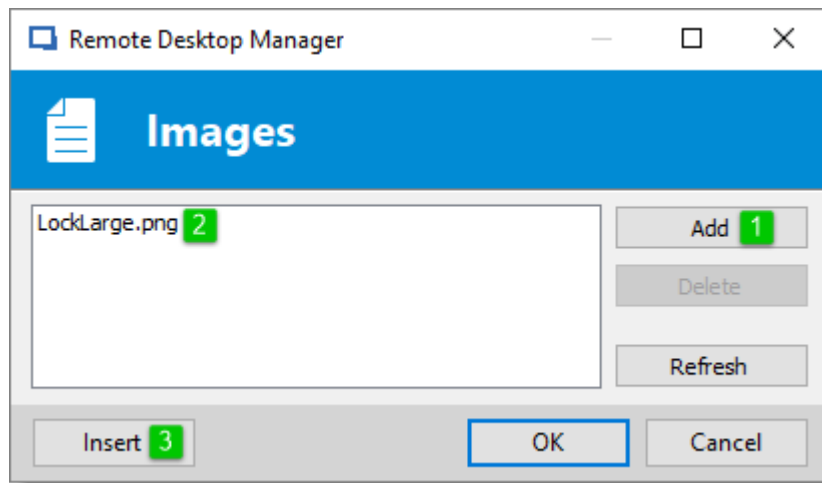
Image syntax is very similar to link syntax. Images must be added in the image manager before referencing them.

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.



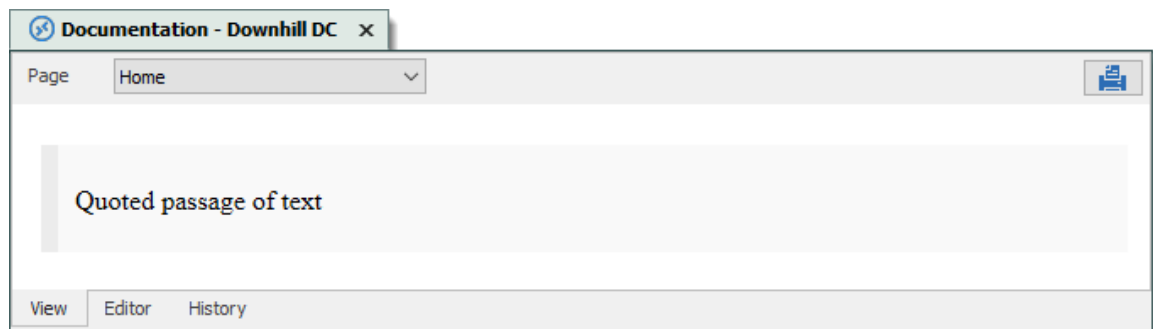
*Documentation editor - Add an image*

## 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:

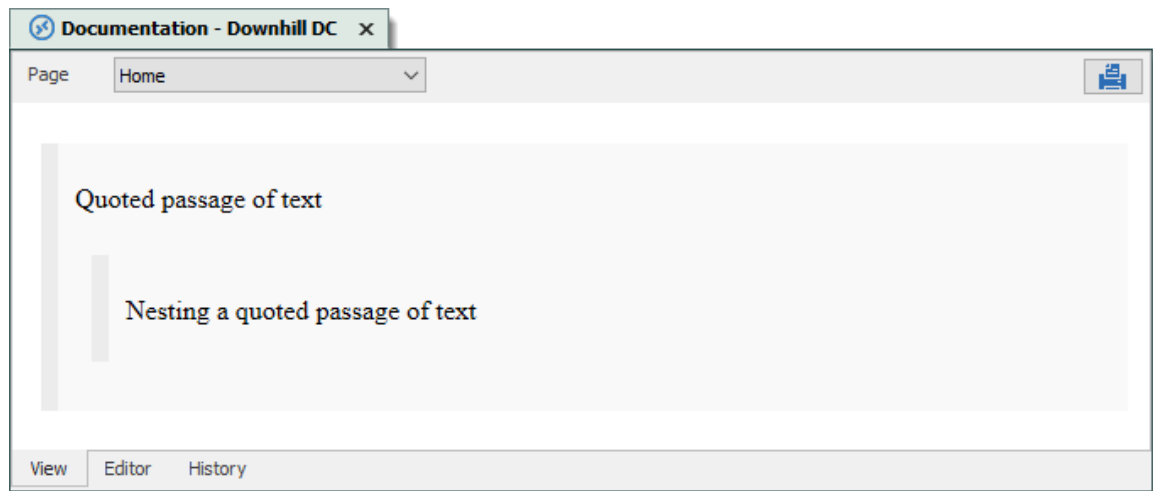


Blockquotes can easily be nested.

> Quoted passage of text

>> Nesting a quoted passage of text

Output:

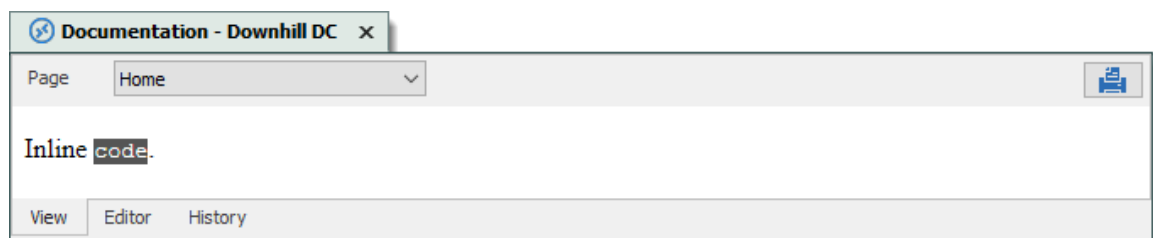


## CODE EXAMPLES

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

Inline `code`.

Output:



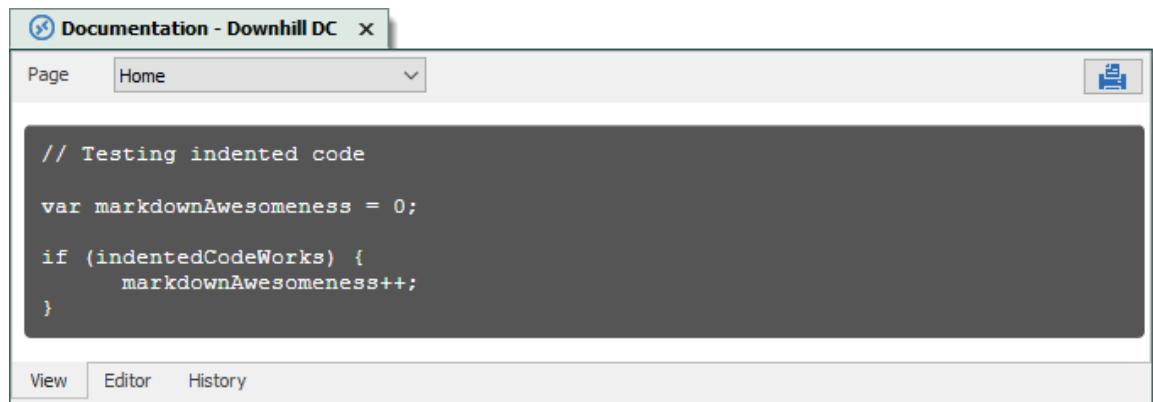
Code blocks are created by indenting the text with four spaces at the beginning of each line. There must be an empty line before.

```
// Testing indented code

var markdownAwesomeness = 0;

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

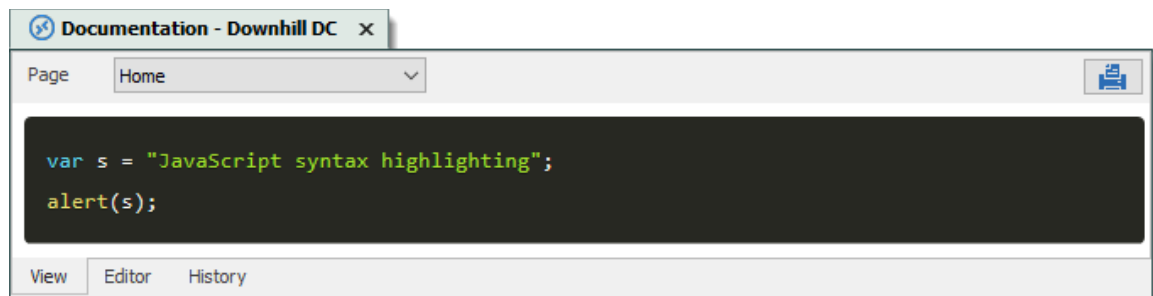
Output:



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.

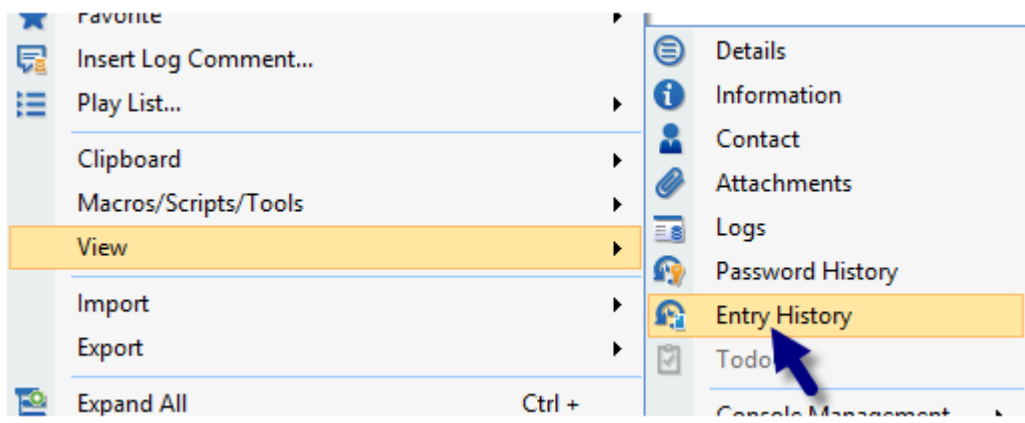


This feature requires an [Advanced Data Source](#).



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

## SETTINGS

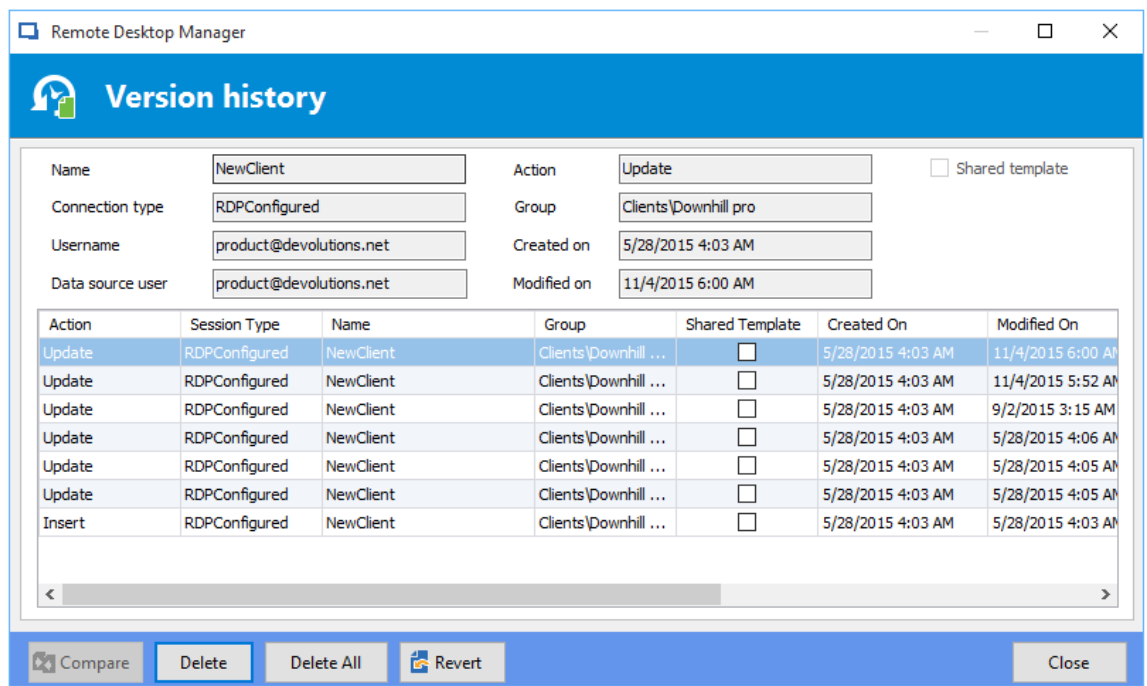


Home - Entry History

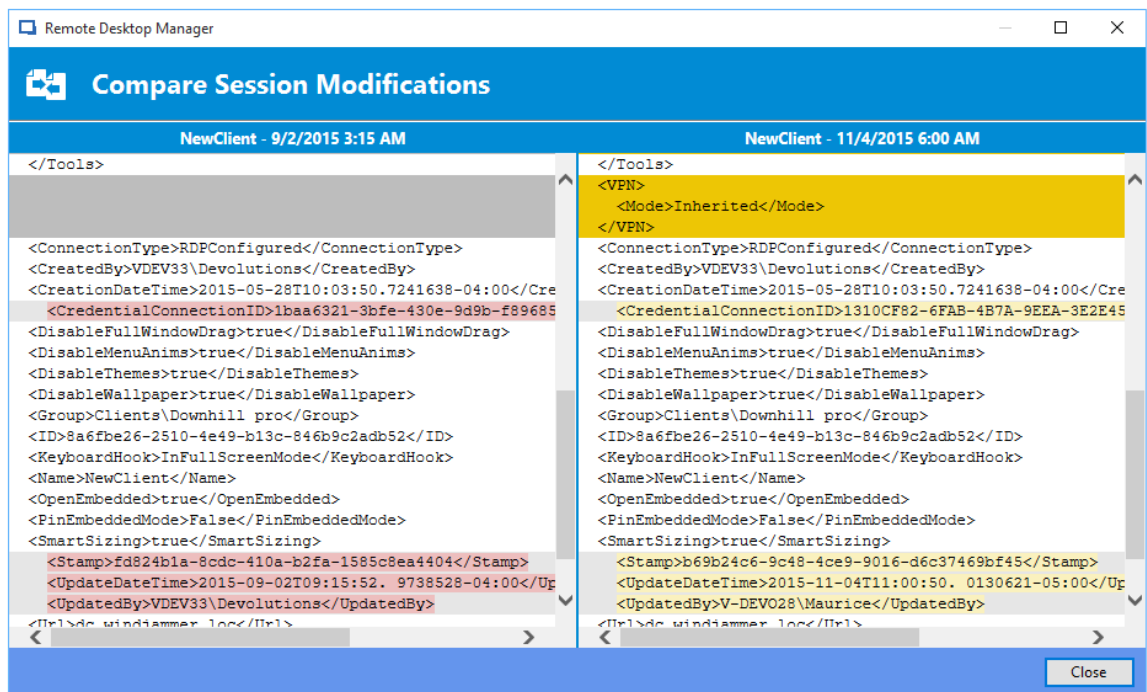
To display the entry history, **right-click** on an entry and select **View - Entry History**.

## 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.



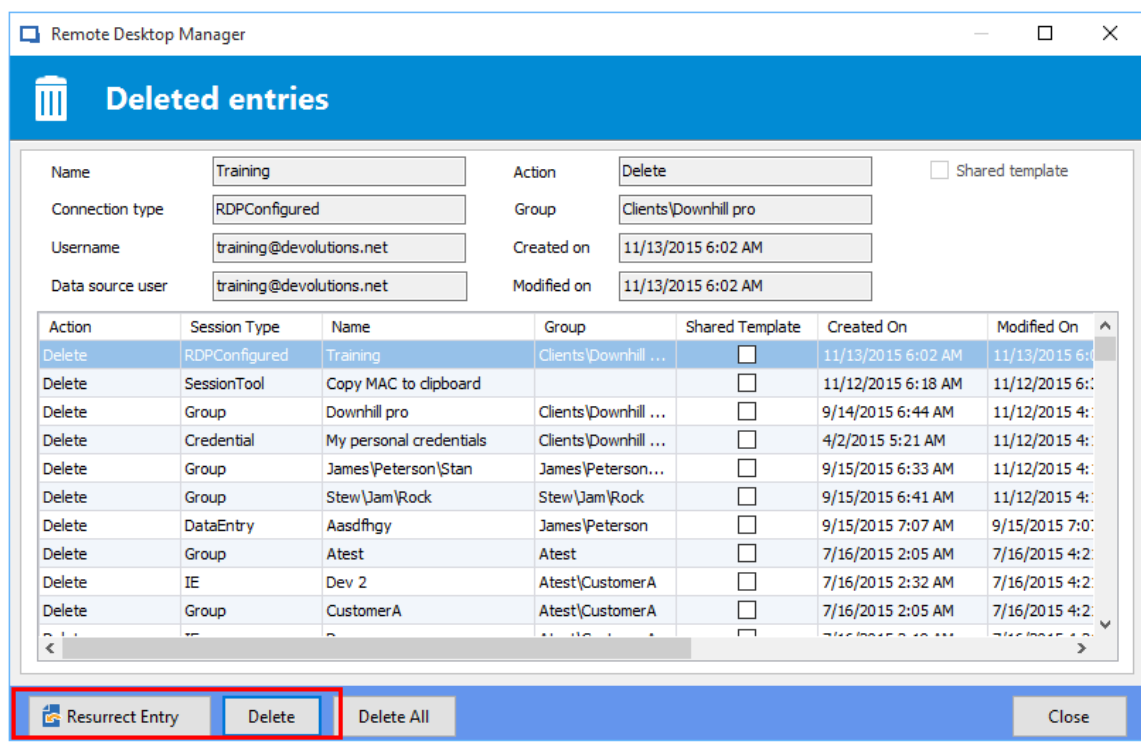
Entry history view



Compare session modifications

## VIEW DELETED ENTRIES

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

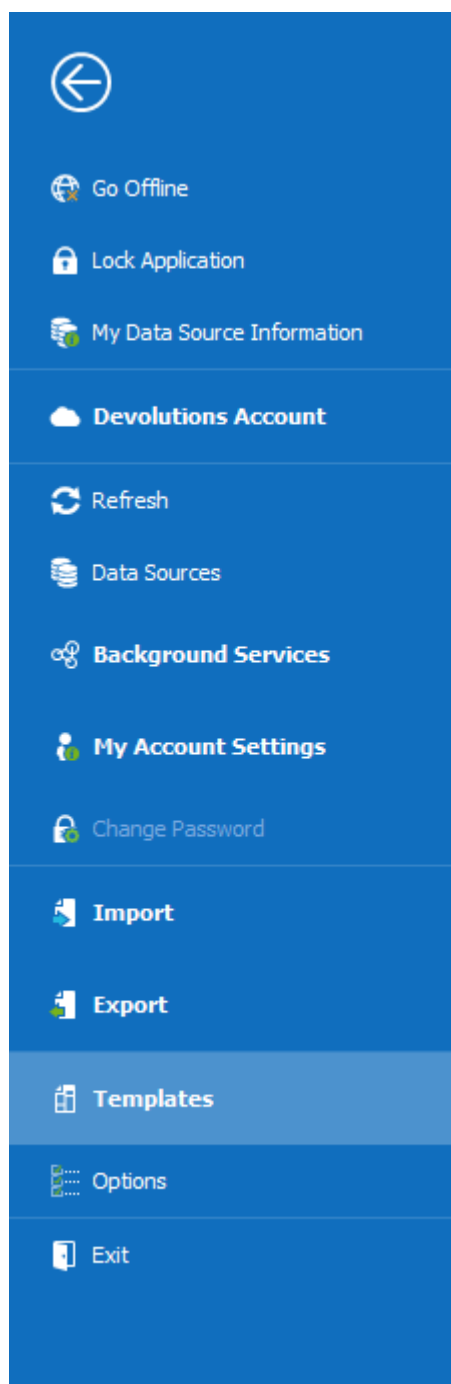


*Deleted Entries*

## 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).

| Offline mode          | Size    | Permissions   |
|-----------------------|---------|---------------|
| Offline mode          | 64.0 KB | Read/write    |
| Group Policy settings |         | Read/write    |
| System settings       |         | Read/write    |
| User settings         |         | Read/write    |
| Data source config    |         | Intelligent   |
| Vault                 |         | Allow offline |

*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.



## Data Source Information

|                       |             |
|-----------------------|-------------|
| Server                |             |
| Database              |             |
| Is DB owner           | ✓           |
| Is System DBA         | ✗           |
| Offline mode          | Read/write  |
| Group policy settings | Read/write  |
| System settings       | Read/write  |
| User settings         | Read/write  |
| Data source config    | Intelligent |

General

Entries

User Groups

|                             |         |
|-----------------------------|---------|
| Database user               |         |
| User                        |         |
| Description                 |         |
| User vault                  | Default |
| Is administrator            | ✓       |
| Allow offline mode          | ✓       |
| Allow drag-and-drop         | ✓       |
| Is Auto Refresh             | ✗       |
| Auto refresh interval       | 0 sec   |
| Is Two Factor Configuration | ✗       |

File – My Data Source Information

## USER AND SECURITY

### GENERAL

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

| General                     | Entries | User Groups |
|-----------------------------|---------|-------------|
| Database user               |         |             |
| User                        |         |             |
| Description                 |         |             |
| User vault                  |         | Default     |
| Is administrator            |         | ✓           |
| Allow offline mode          |         | ✓           |
| Allow drag-and-drop         |         | ✓           |
| Is Auto Refresh             |         | ✗           |
| Auto refresh interval       | 0       | sec         |
| Is Two Factor Configuration |         | ✗           |

*My Data Source Information - General*

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

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

## ENTRIES

| General                        | Entries | User Groups |   |
|--------------------------------|---------|-------------|---|
| Add entries                    |         |             | ✓ |
| Edit entries                   |         |             | ✓ |
| Delete entries                 |         |             | ✓ |
| View information section       |         |             | ✓ |
| Import entries                 |         |             | ✓ |
| Export entries                 |         |             | ✓ |
| Allow add entry in root folder |         |             | ✓ |


*My Data Source Information – Entries*

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

| OPTION                                 | DESCRIPTION  |
|--|--|
| <b>Import and Export entries</b>       | Indicates if the user has the privilege to import or export entries.   |
| <b>Allow add entry in Vault folder</b> | 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/SQL Azure](#) and a [Devolutions Server \(DVLS\)](#) data source.

General

Entries

User Groups

Name

◀

▶

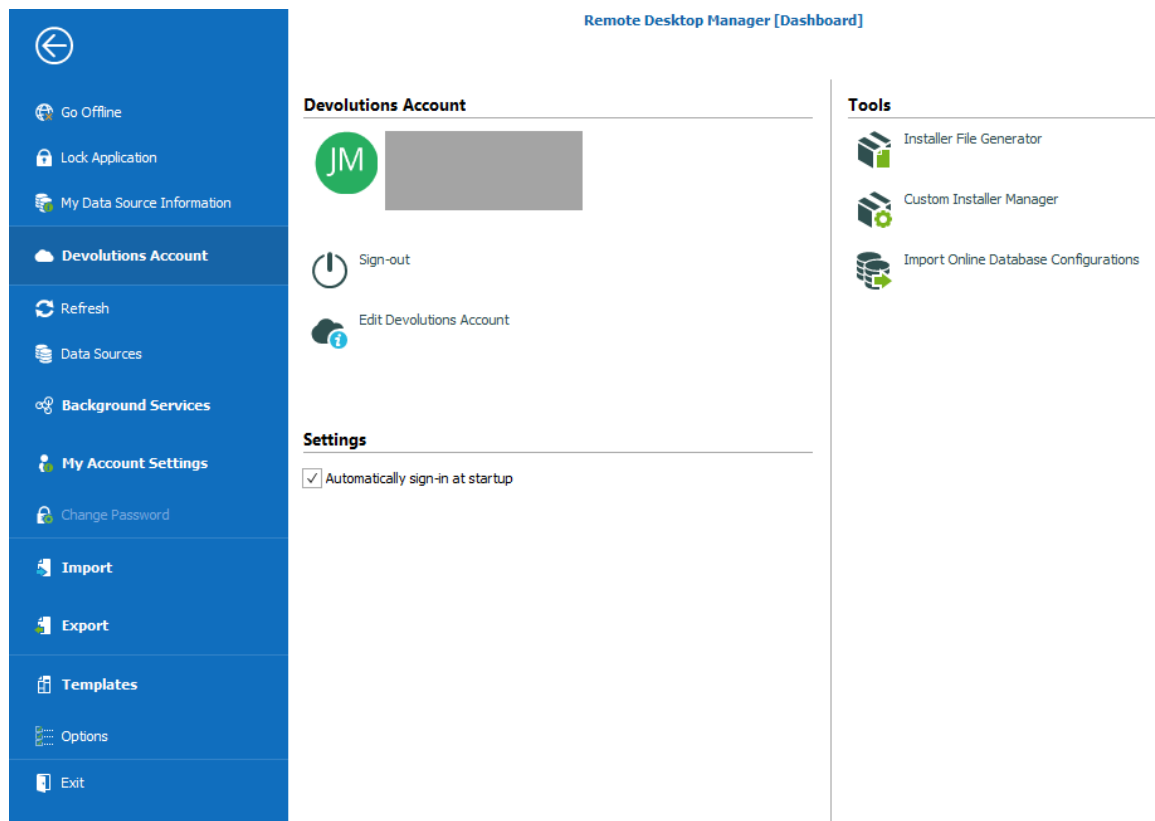
### 6.2.3 Devolutions Account

## DESCRIPTION



Use **File – Devolutions Account** to create/connect Remote Desktop Manager to your Devolutions Online Database account. The Devolutions Online Database is free for customers and includes access to the custom installer manager.

## SETTINGS



*Devolutions Account*

## DEVOLUTIONS ACCOUNT

| OPTION              | DESCRIPTION   |
|---------------------|---|
| Sign-in or Sign-out | Sign-in with your <a href="#">Devolutions Online Database (DODB)</a> account that has already been created. |
|                     | Sign-out of your <a href="#">Devolutions Online Database (DODB)</a> account.                                |

| OPTION                                  | DESCRIPTION  |
|---|--|
| <b>Create a New Devolutions Account</b> | Create a new <a href="#">Devolutions Online Database (DODB)</a> account. |
| <b>Edit Devolutions Account</b>         | Edit your <a href="#">Devolutions Online Database (DODB)</a> account.    |

## SETTINGS

| OPTION                                  | DESCRIPTION   |
|---|---|
| <b>Automatically sign-in at startup</b> | Automatically sign-in to your <a href="#">Devolutions Online Database (DODB)</a> account at the startup of the application. This feature is of particular importance if you are using a <a href="#">Devolutions Online Database data source</a> or our <a href="#">Online Backup</a> service. |

## TOOLS

| OPTION                                       | DESCRIPTION   |
|--|---|
| <b>Installer File Generator</b>              | Create a Remote Desktop Manager Installer File (.rdi). Consult topic <a href="#">Installer File Generator</a> . |
| <b>Custom Installer Manager</b>              | Consult topic <a href="#">Custom Installer Manager</a> .  |
| <b>Import Online Database Configurations</b> | Import Online database configuration in the application.  |

## 6.2.4 Backup

### DESCRIPTION

Please consult topic [Online Backup](#) for information on this service.

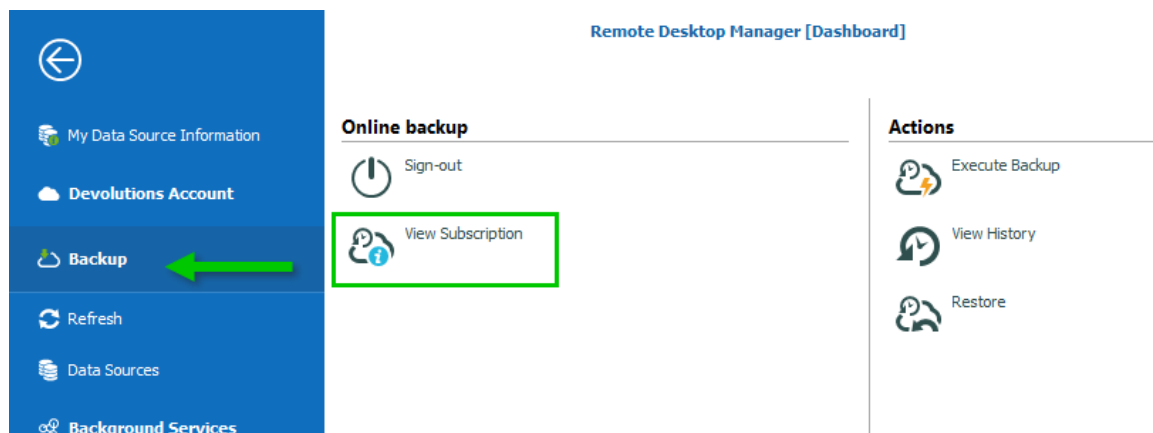
#### 6.2.4.1 Settings

### DESCRIPTION

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

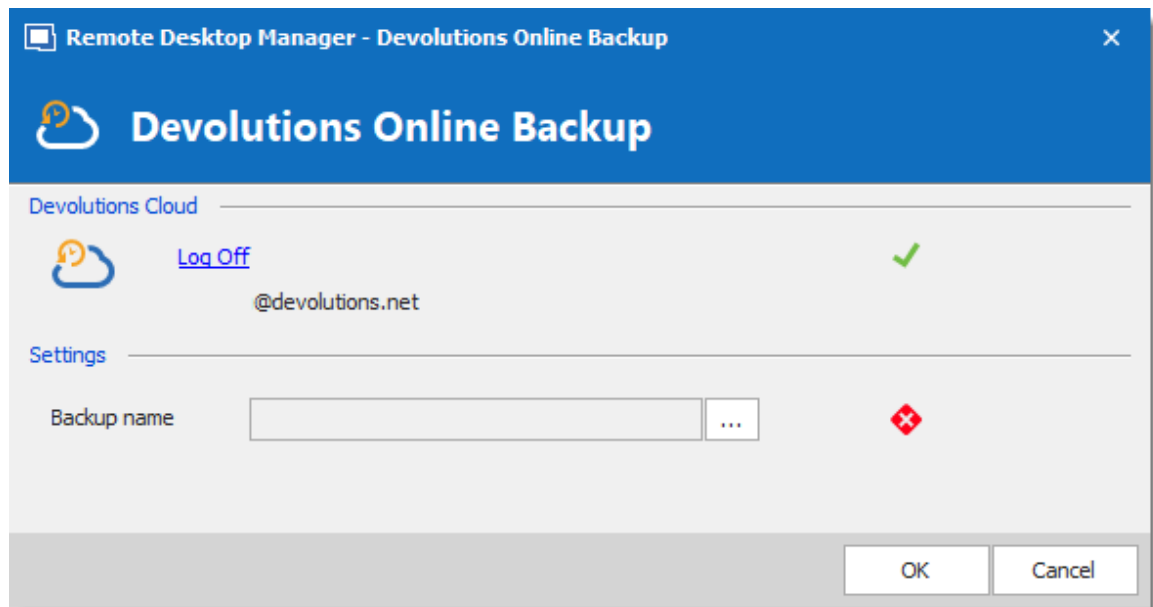
### SETTINGS

1. Click on **File – Backup** to Sign-in with your [Devolutions Account](#).
2. Click on **View Subscription**.

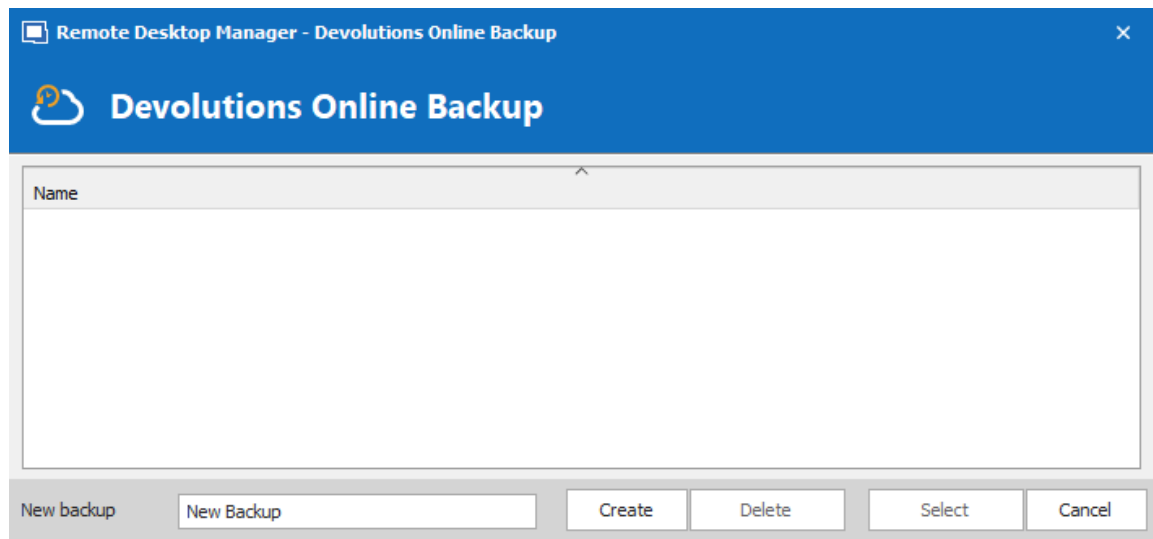


*Online Backup - View Subscription*

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

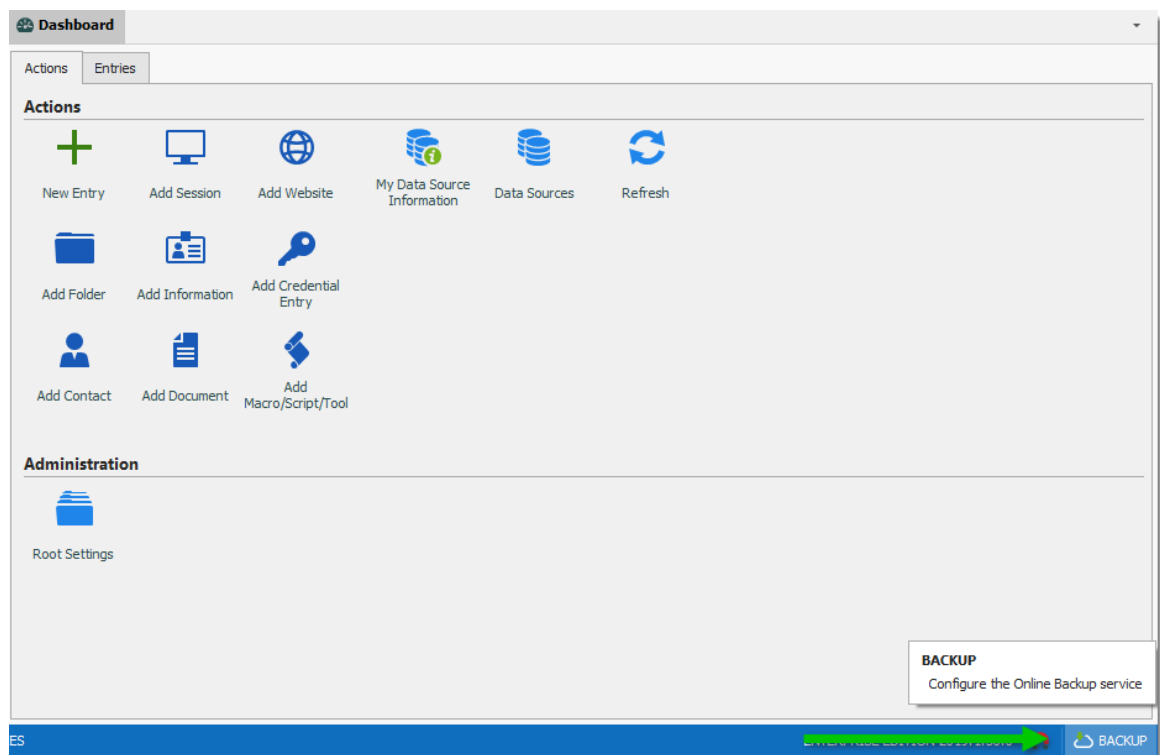
*Backup Name*

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](#), [XML](#) or Microsoft Access 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

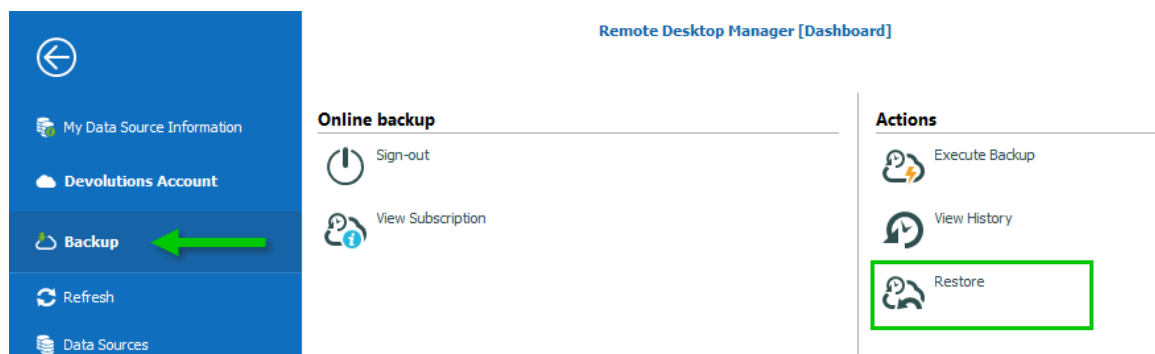


Before being able to restore a backup, you **MUST** create an empty data source and define the backup name before being able to use it. You need to create a new SQLite, XML, Online Drive or Microsoft Access data source in **File – Data Sources**.

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

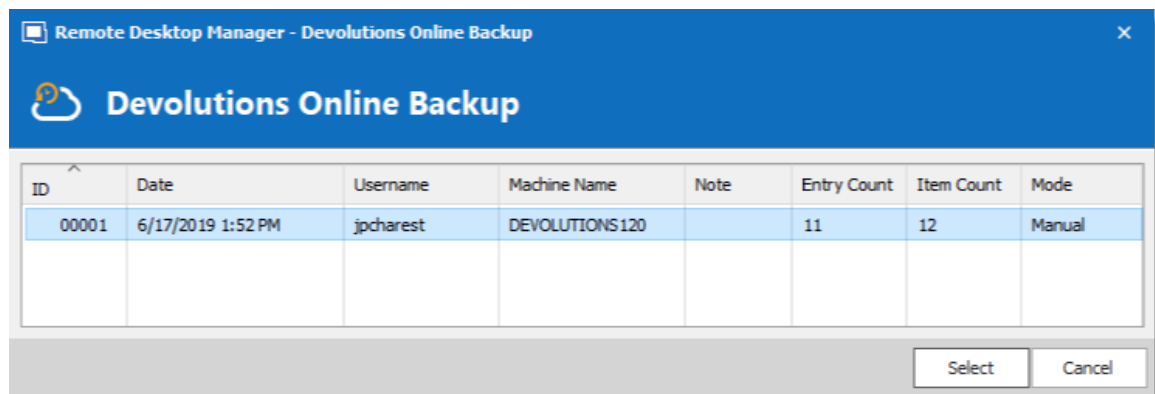
## SETTINGS

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



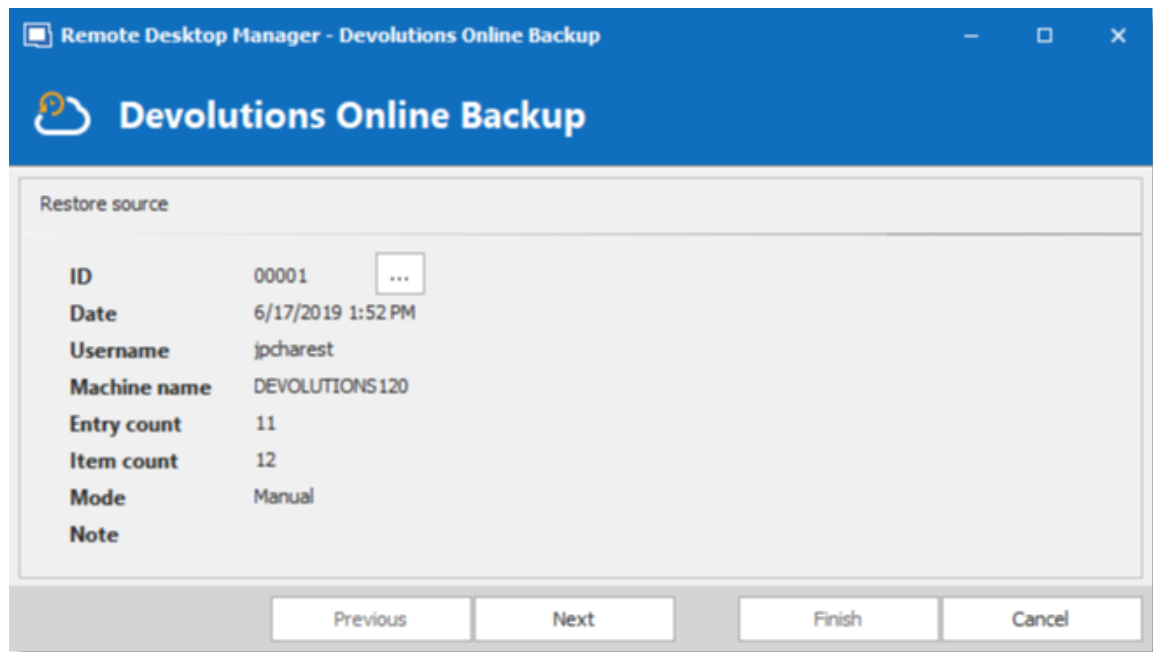
*Backup Restore*

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

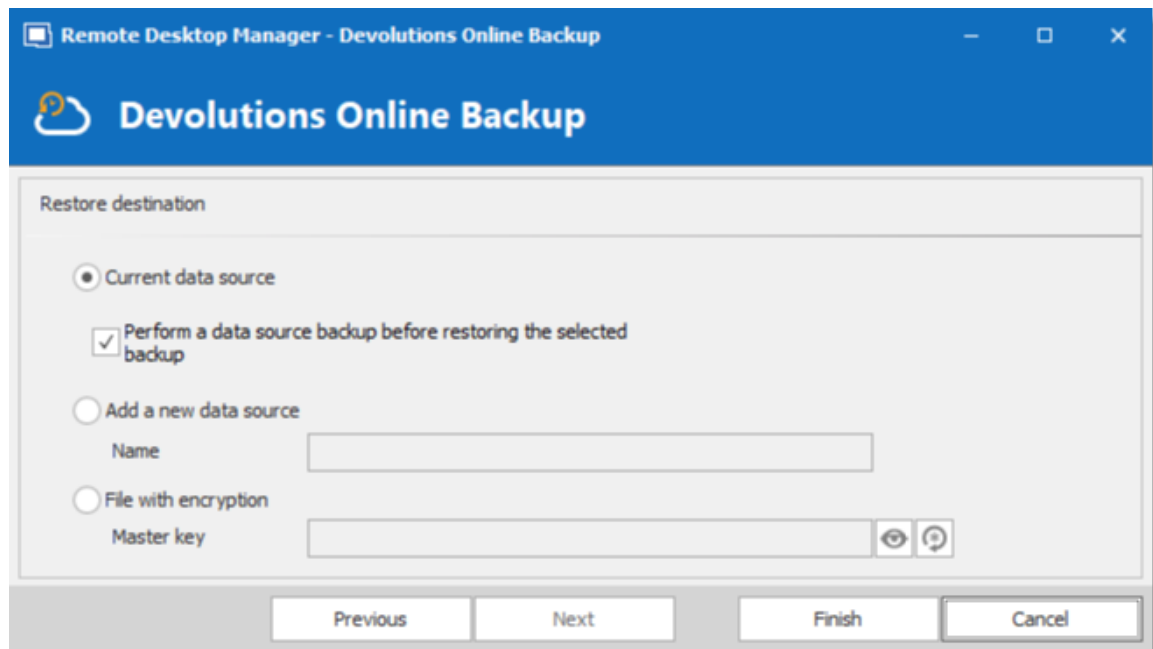


*Select your Backup*

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

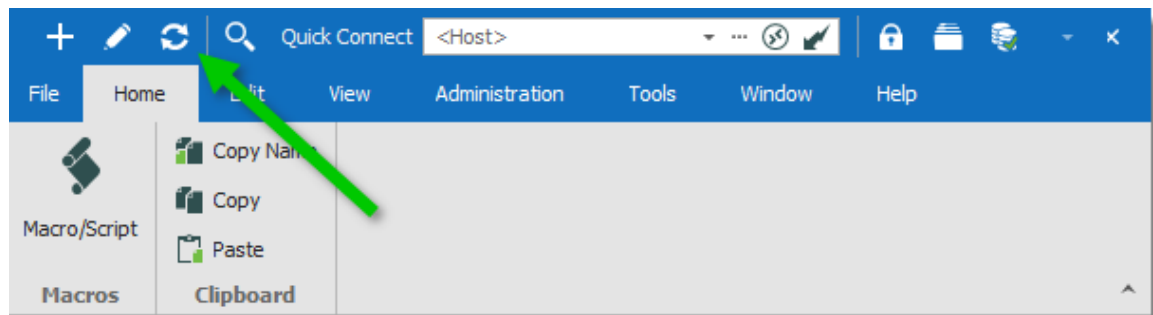
### DESCRIPTION

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.



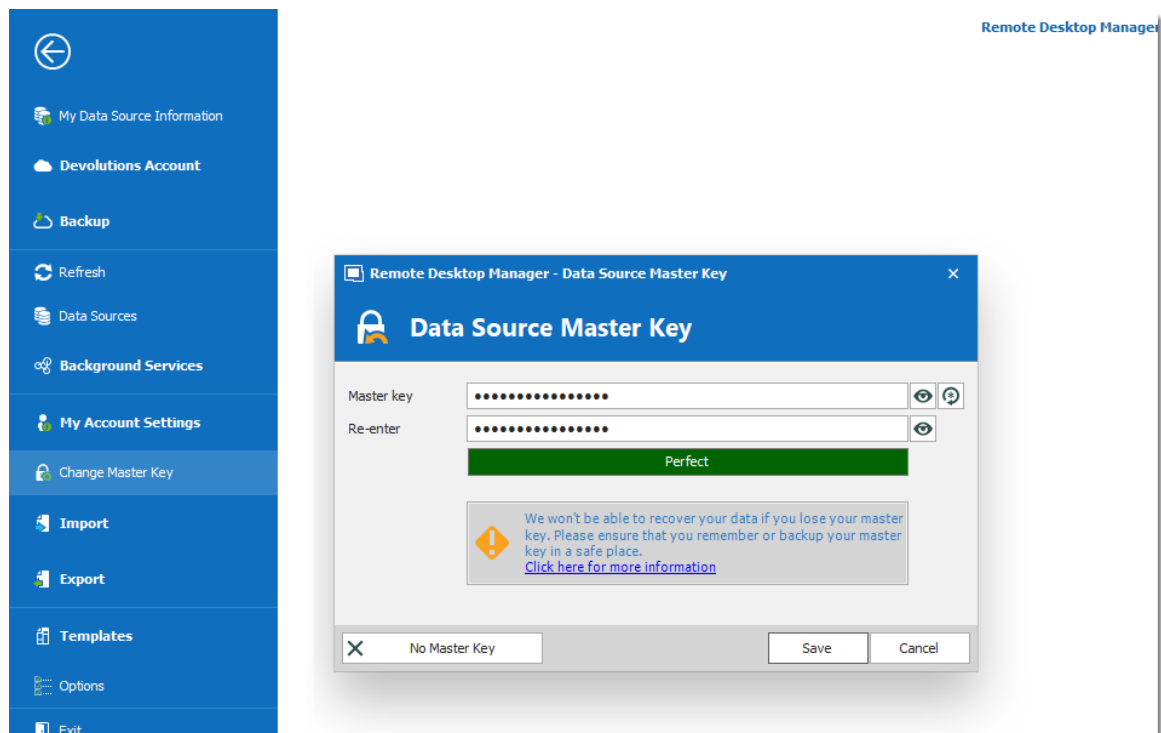
The master key prevents unauthorized users to access the data source without knowing the master key. It is highly recommended to apply a master key to the data source if you're using Remote Desktop Manager in a portable environment (i.e. USB Flash Drive, USB Hard Drive).

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

- Devolutions Online Drive
- Dropbox
- FTP
- Google Drive
- WebDAV
- 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).



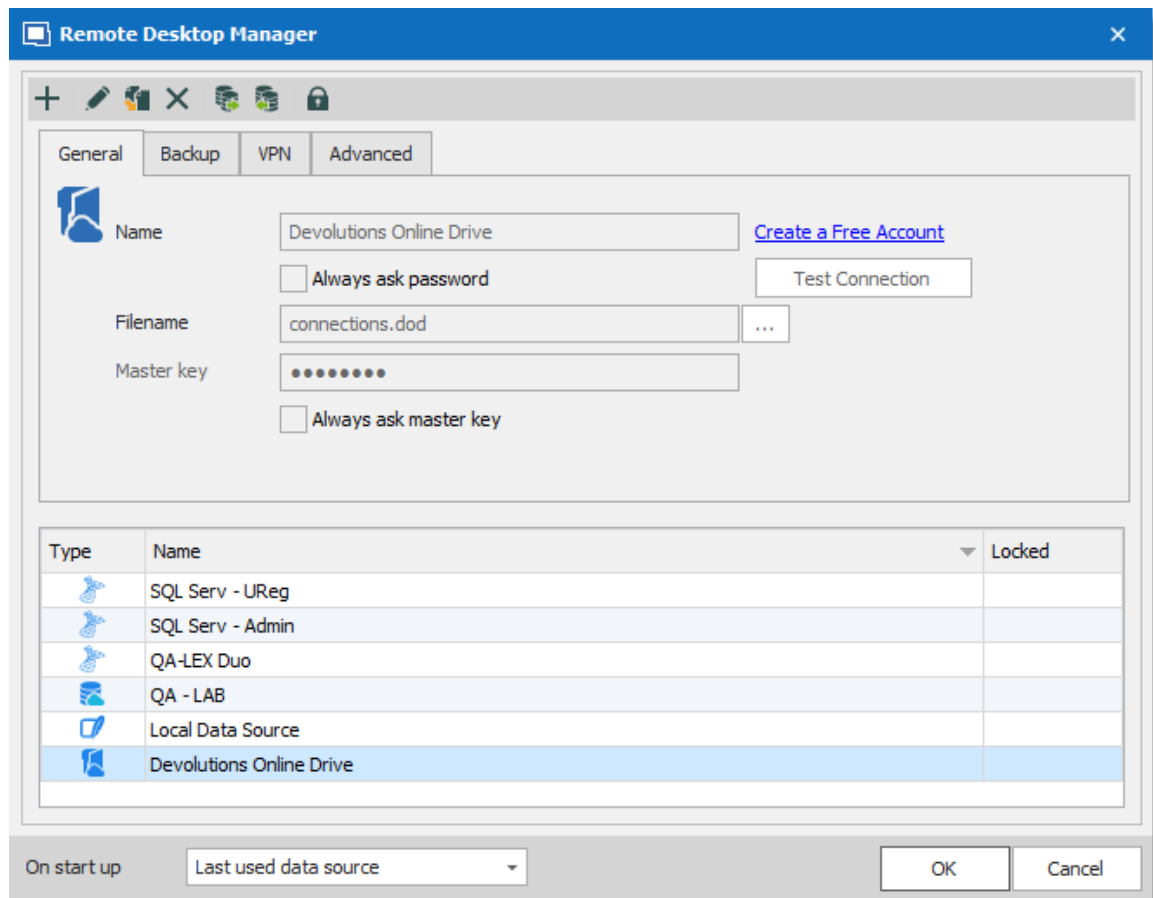
*Change Master Key*

## 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 Sources*

## 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   |
|--------------------------------|---|
| <b>Use default data source</b> | Set the data source that you always want to open at start up. |
| <b>Last used data source</b>   | Open with the last used data source.                          |

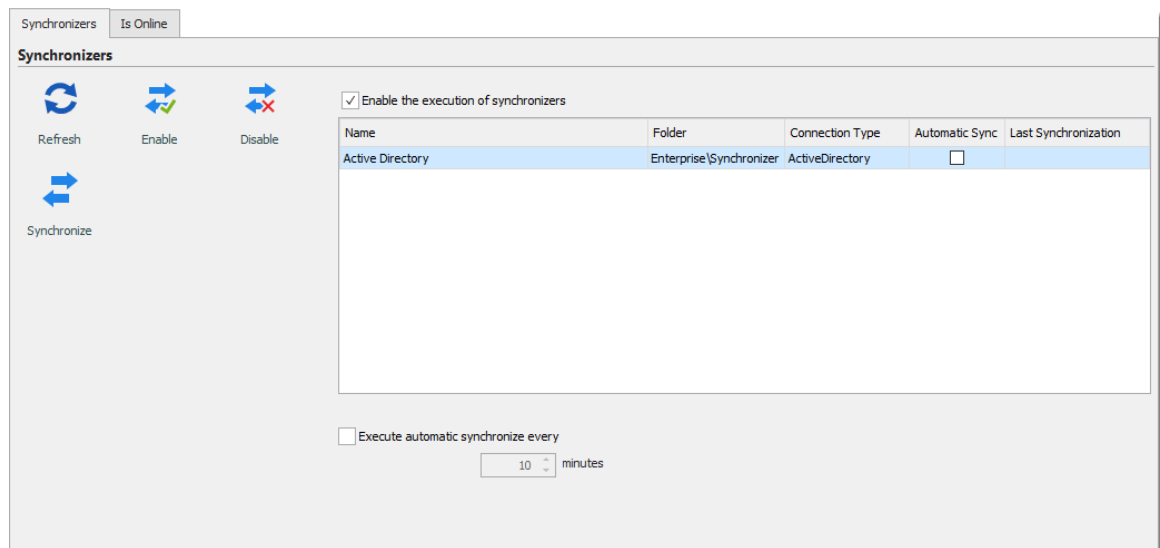
| OPTION                        | DESCRIPTION   |
|-------------------------------|---|
| <b>Prompt for data source</b> | A message box will open on startup for the data source selection. |

## 6.2.8 Background Services

### SYNCHRONIZERS

**Synchronizers** centralizes all your synchronizers entry in one place.

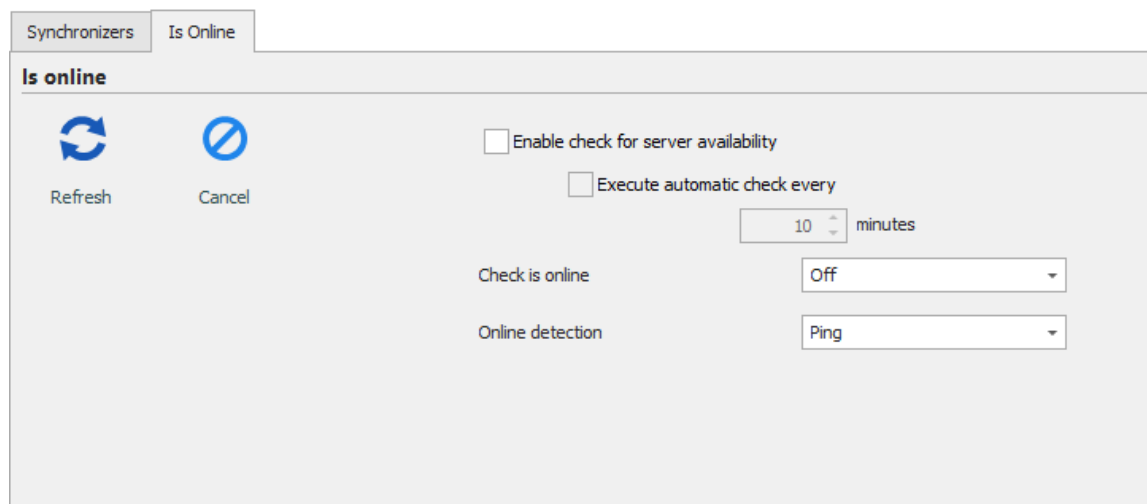
When experiencing a performance degradation with Remote Desktop Manager you will be able to verify if a synchronizer is running in the background causing the system to slow down.



*Synchronizers*

### IS ONLINE

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

*Is Online*

| OPTION                                      | DESCRIPTION  |
|---|--|
| <b>Enable check for server availability</b> | Server is ping to determine if they are available. Server will be displayed in "red" in the tree view if not available.  |
| <b>Execute automatic check every</b>        | Execute the online check automatically each determined amount of minutes.  |
| <b>Check is online</b>                      | If the option is <b>On</b> the application will verify if the server is online.  |
| <b>Online detection</b>                     | If <b>Check is online</b> option is enable, select the detection method between: <ul style="list-style-type: none"> <li>• Ping</li> <li>• Port scan</li> </ul> |

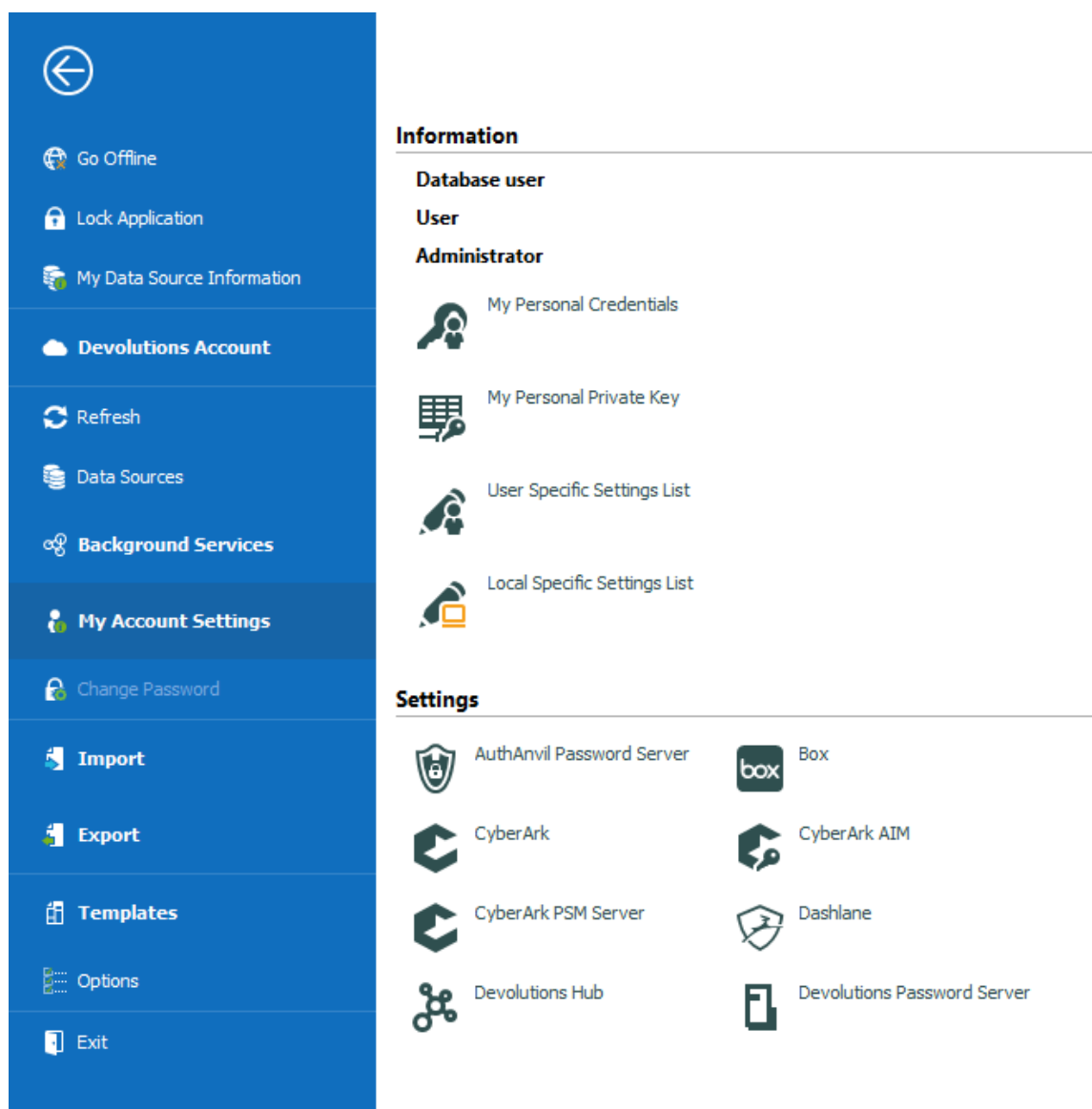
## 6.2.9 My Account Settings

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

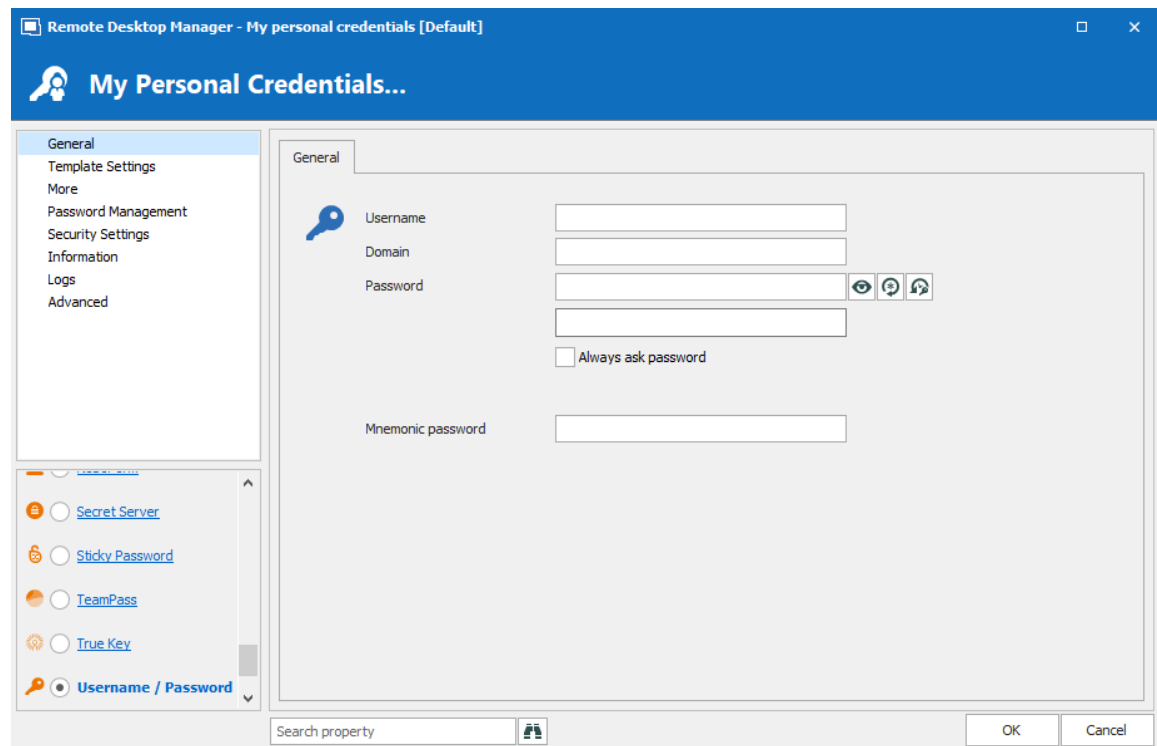
The **My Personal Credentials** feature is a single credential entry which is locally stored on your computer in your Windows profile.

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**.



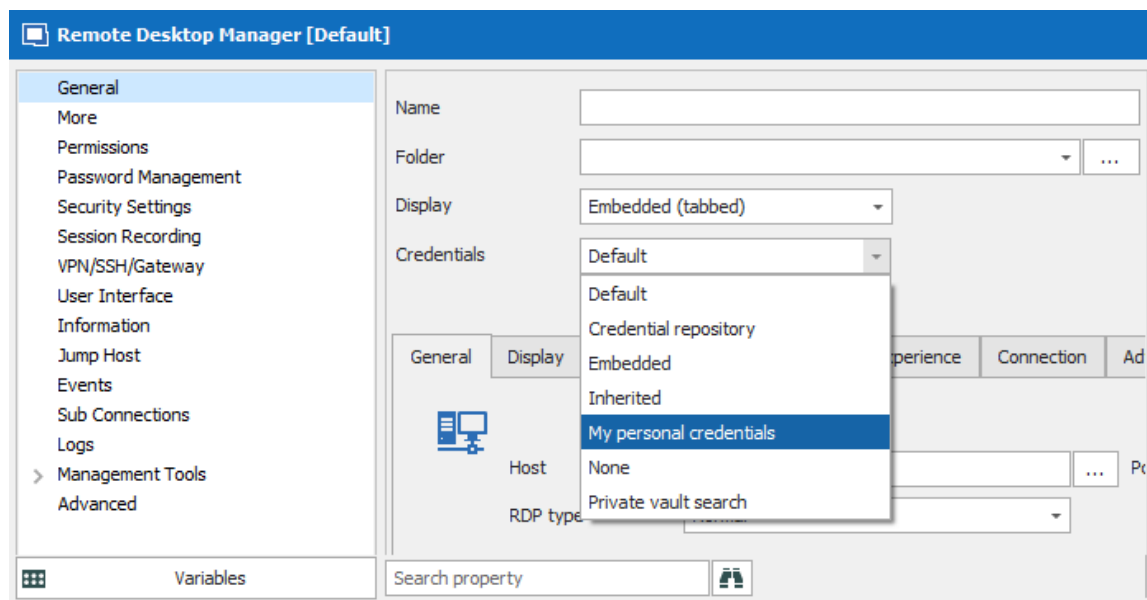
If you want to change the credential type, go in *%LOCALAPPDATA% (Default)* or *%APPDATA% (Remote Desktop Services)* **\\Devolutions\\RemoteDesktopManager** and delete the **Credentials.rdt** file to reset it.



*My Personal Credentials*

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



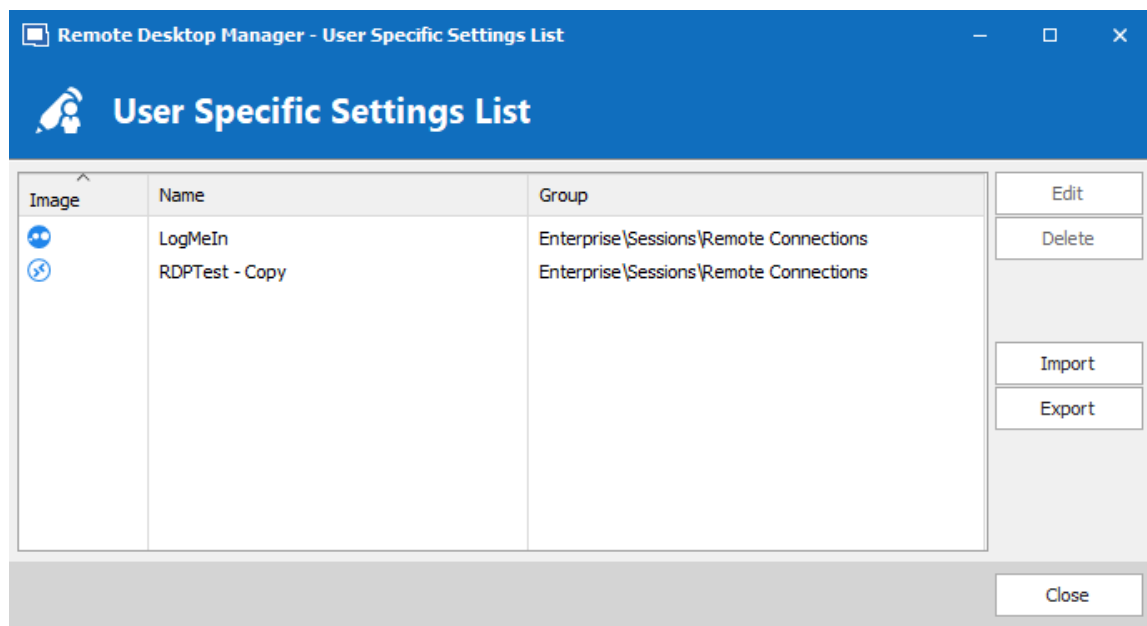


*Credentials - My personal credentials*

#### 6.2.9.2 User Specific Settings List

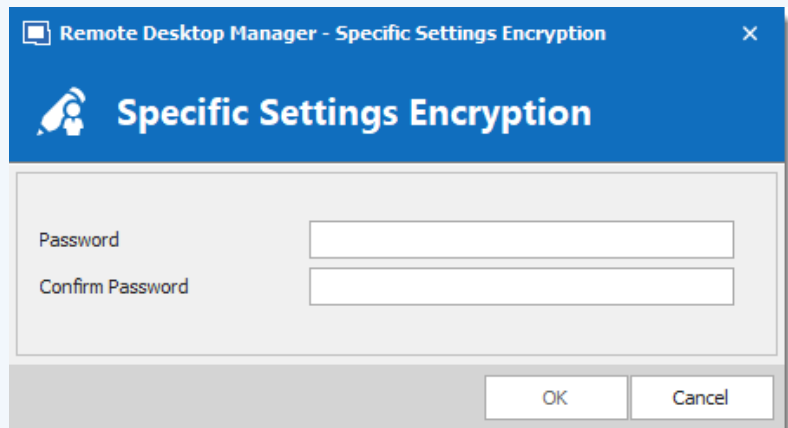
### DESCRIPTION

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



*User Specific Settings List dialog*

| OPTION        | DESCRIPTION  |
|---------------|--|
| <b>Edit</b>   | Edit the selected <a href="#">User Specific Settings</a> .   |
| <b>Delete</b> | Delete the selected <a href="#">User Specific Settings</a> .   |
| <b>Import</b> | 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. |
| <b>Export</b> | 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

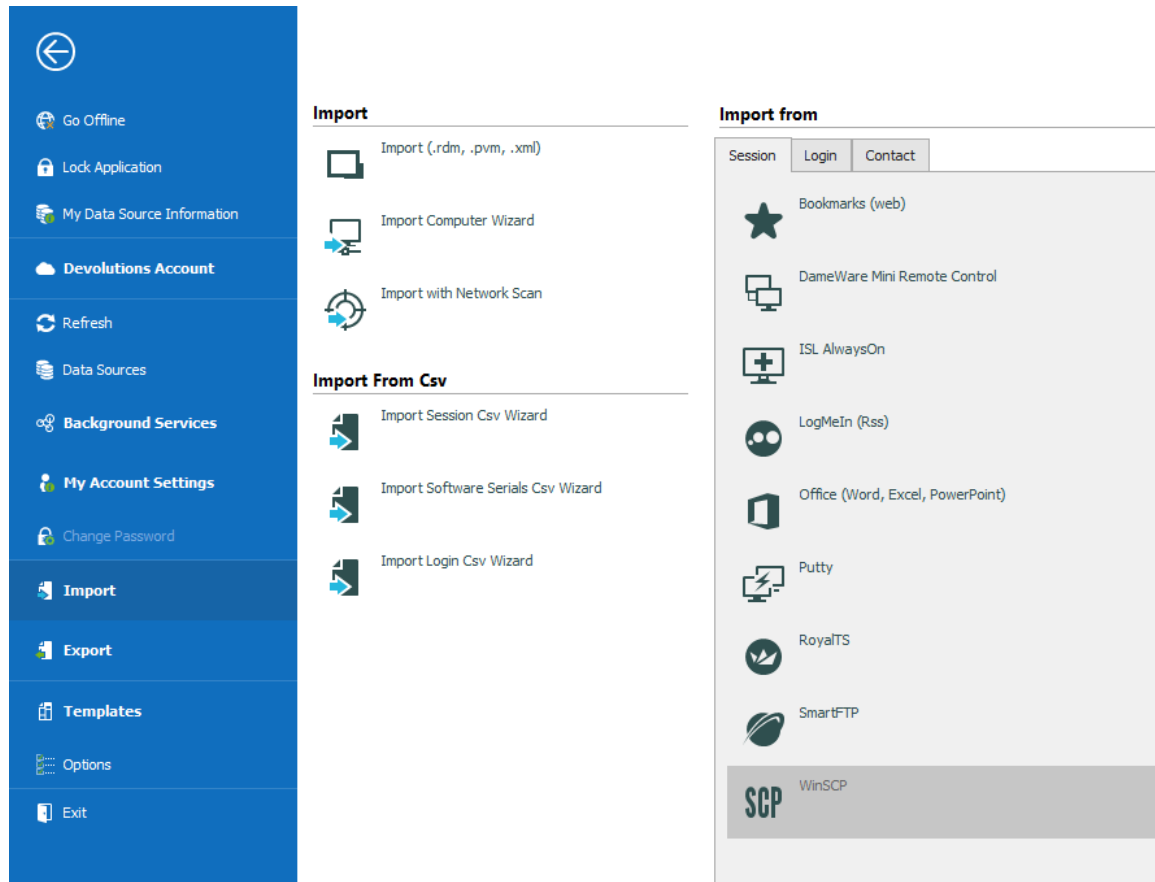
Use the **File – Import** to import entries in Remote Desktop Manager. You can import entry types from multiple sources.

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 Permission has been enabled inside the user account.

## SETTINGS



*File - Import*

## IMPORT ENTRIES

Import Entries is used to import sessions stored in files, such as:

- .rdm (Remote Desktop Manager native export format)
- .pvm (Password Vault Manager native export format)
- .xml (it must be a specific format compatible with the application)

## IMPORT COMPUTER WIZARD



The Import Computer Wizard is only available in the Enterprise edition.

You can import computers from different sources. These sources includes:

- Network neighborhood
- Your current domain or another domain on your network
- List of computers from a file

Please refer to [Import Computer Wizard](#) for more information.

## IMPORT WITH NETWORK SCAN

Consult Import with Network Scan to learn more about this option.

## IMPORTING FROM CSV FILES

Three wizards are available to import content from csv files:

- Import Session
- Import Software Serials
- Import Login

Each wizard specifies the list of supported columns and identifies which are mandatory.

## IMPORT FROM

Consult topics below to import sessions, logins and contact from many tools:

- [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:

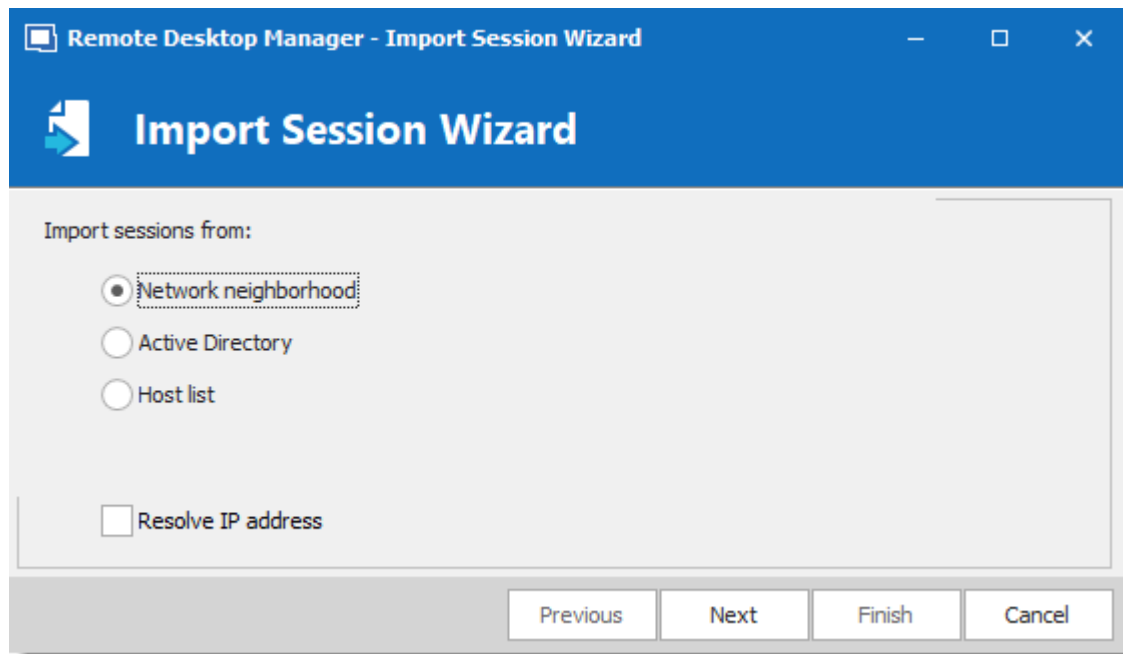
1. select computers by using one of the three sources;
2. optionally apply a template from which to base new sessions on; and
3. optionally edit each newly created session prior to them being saved.

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.

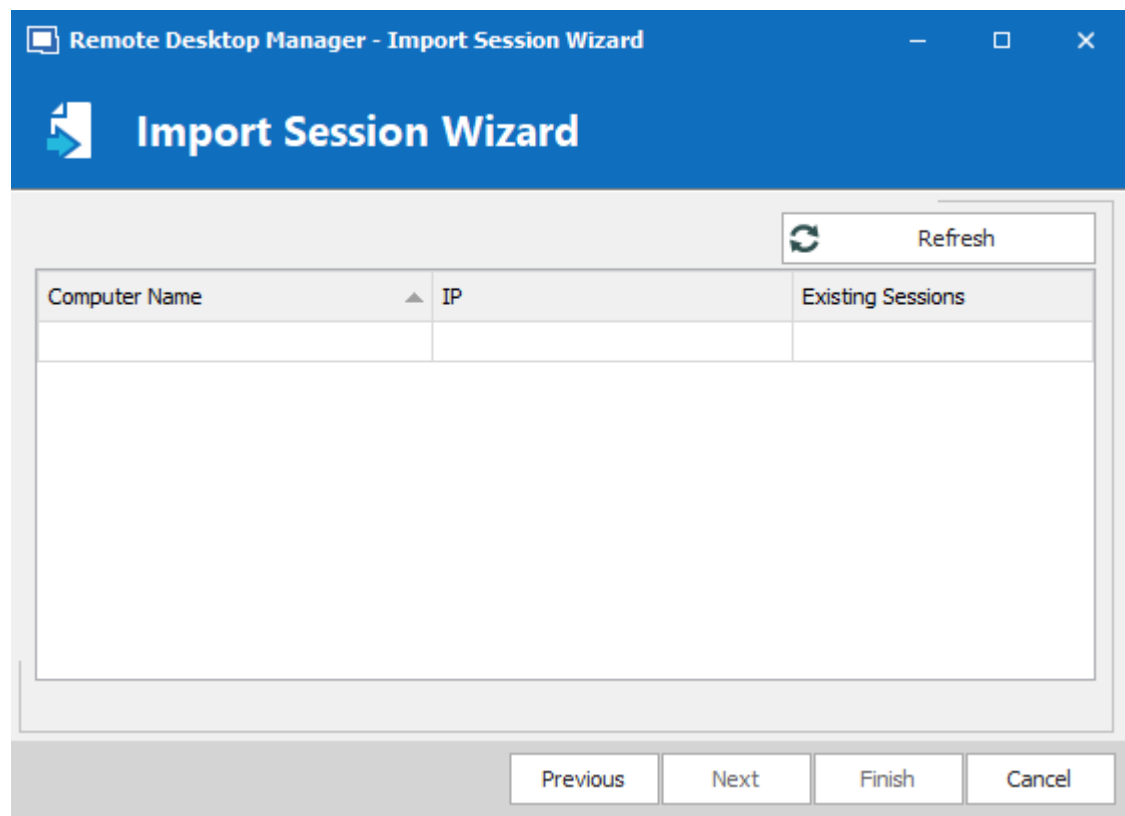


*Import Session Wizard*

Refer to the sections below depending on the chosen source.

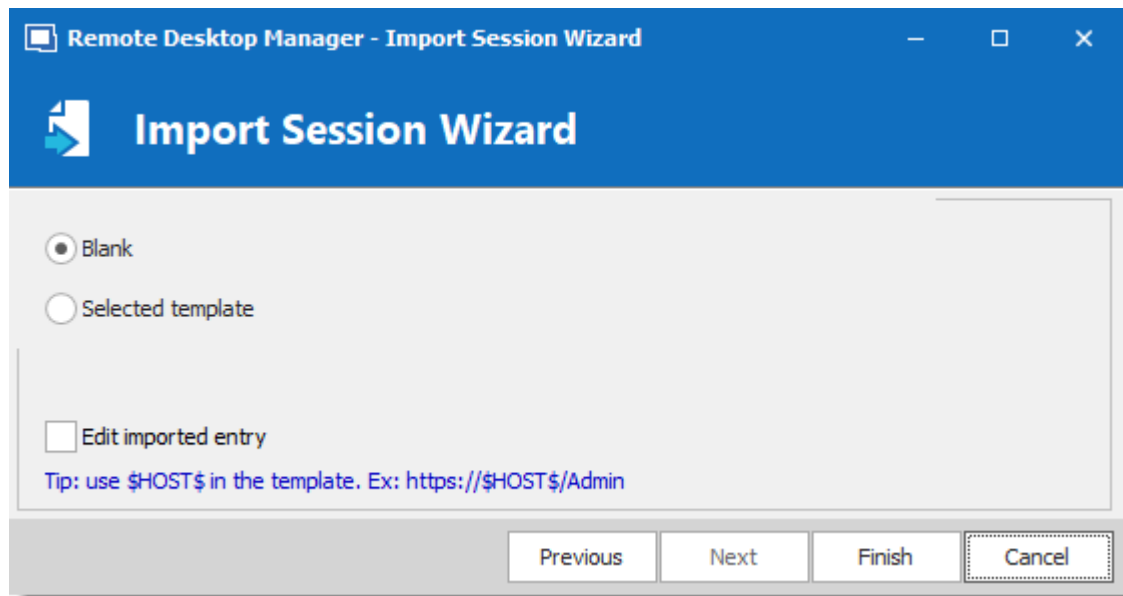
## NETWORK NEIGHBORHOOD

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



*Import Session Wizard - Network Neighborhood*

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.



*Import Session Wizard - Template*

## ACTIVE DIRECTORY

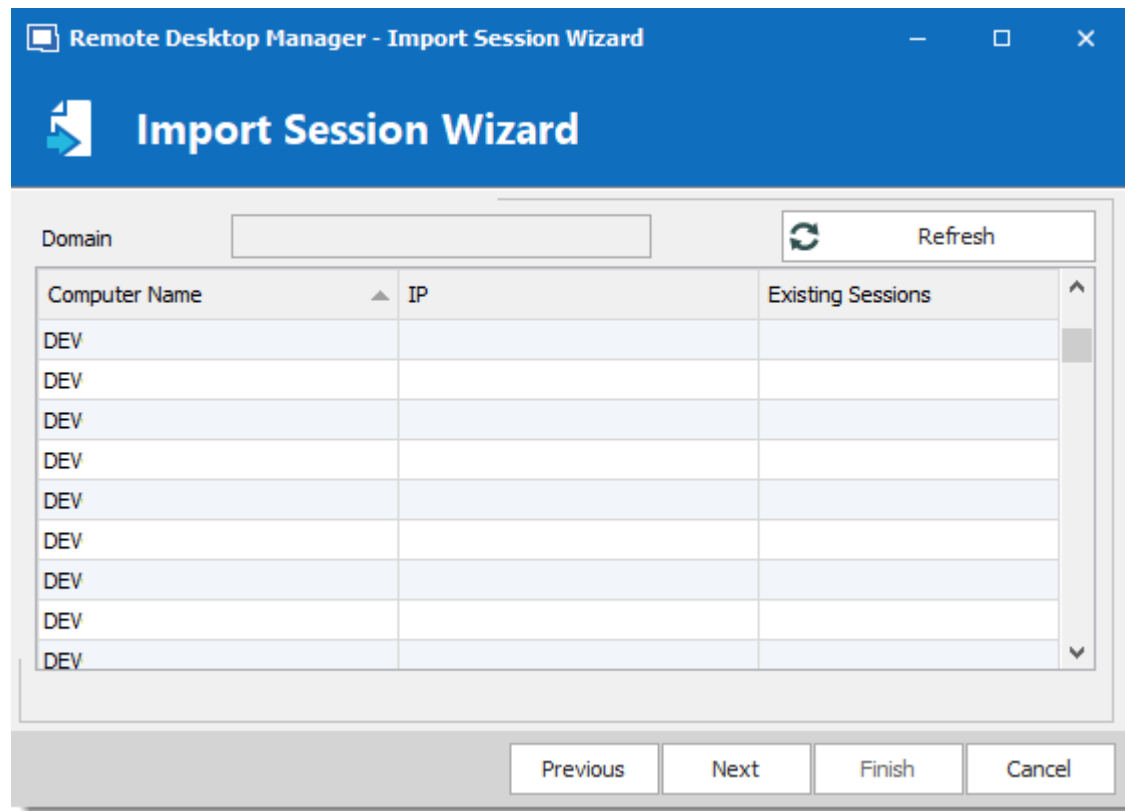
The following screen allows you to select the domain to interrogate after which you must press refresh to load the list of computers that are available.



The screenshot shows the 'Import Session Wizard' window from Remote Desktop Manager. The window has a blue title bar with the text 'Remote Desktop Manager - Import Session Wizard' and standard window controls. Below the title bar is a blue header area with a folder icon and the text 'Import Session Wizard'. The main area is light gray and contains several input fields and checkboxes. The 'Domain' field is a dropdown menu. The 'Destination folder' field is a text box with a browse button ('...'). The 'Other filter' field is a text box with a help button ('?'). The 'Preview' field is a text box containing '(objectClass=Computer)' with up and down arrow buttons. Below these fields are two checkboxes: 'Import description' and 'Create folders from OU/containers'. The 'Create folders from OU/containers' checkbox is checked. Below this checkbox is a 'Level' field with a spinner box set to '0' and a help button ('?') with the text '0 is the top container'. At the bottom of the window are four buttons: 'Previous', 'Next' (which is highlighted with a dashed border), 'Finish', and 'Cancel'.

*Import Session Wizard - Active Directory*

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

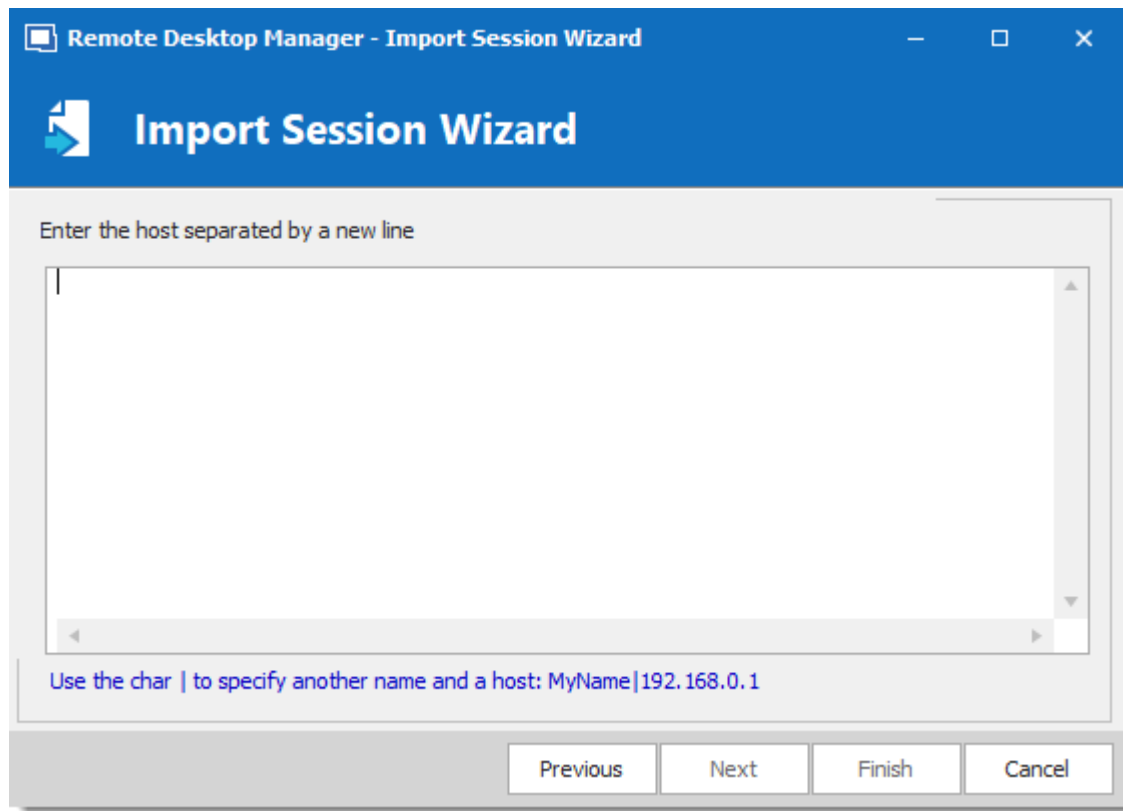


*Import Session Wizard - Domain list*

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.



*Import Session Wizard - Host List*

Proceed to Template Selection below.

## TEMPLATE SELECTION

The template selection is an optional step, but its the only way that you have to choose a protocol type other then 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 Session CSV Wizard

## DESCRIPTION

This version of the wizard has been greatly enhanced to support not only all entries general fields but also sub-fields. This gives you access to all properties, even for types provided by add-ons, therefore unknown by Remote Desktop Manager.

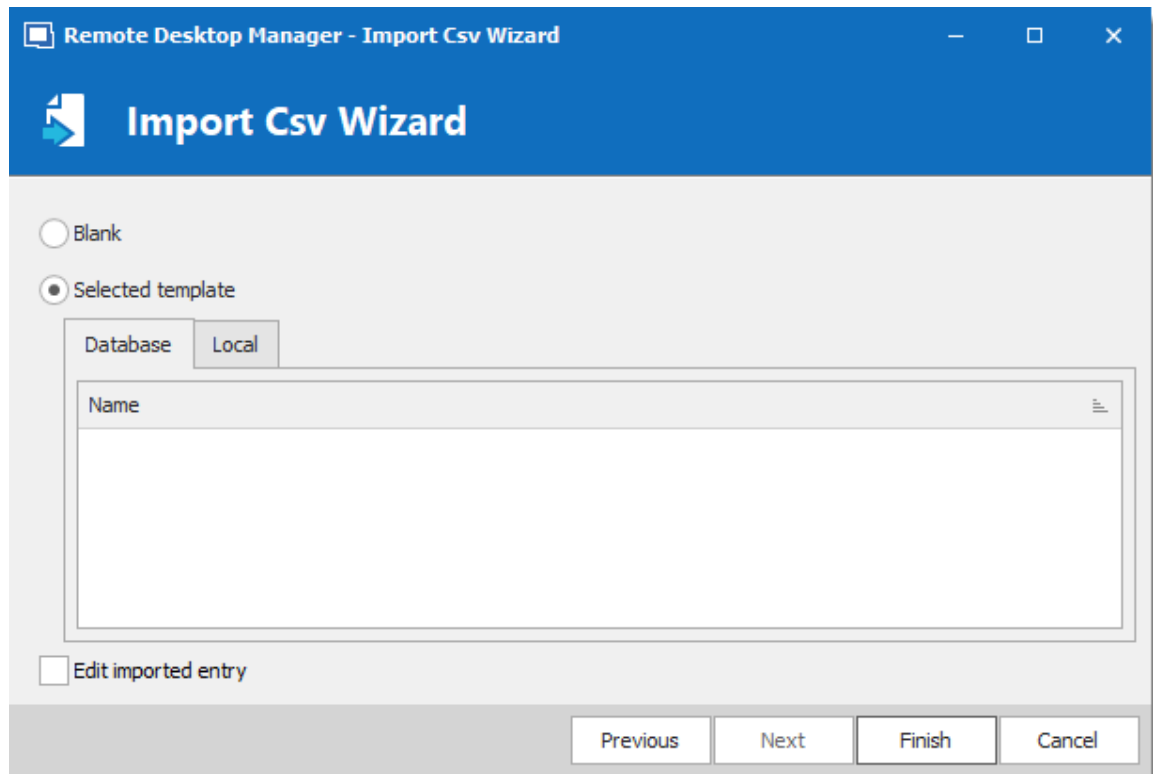


For a discussion on the CSV file format, and the impact of decisions made in this entry, please consult [Import Strategies and file format](#)

## SETTINGS

Once you've selected the CSV file to process you will be presented with the template selection screen.

If you have selected a template as suggested, you will see a list of templates available to your system.



*Import Csv Wizard*

If you wish to review each and every session as they are imported you can check the **Edit imported entry**, but it is not really recommended for a large number of sessions.

Press finish and the import will proceed using your chosen settings.

## 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. Please consult [CSV Samples](#) below.

## 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, only the **Host** field is 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: "**MetalInformation\OS**" or "**MetalInformation\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  |
|------------------------|--|
| <b>Host</b>            | Host name of the device, <b>this is the only mandatory field.</b>  |
| <b>Name</b>            | Name of the entry  |
| <b>ConnectionType</b>  | Token representing the connection type. It is best to use the <b>Clipboard-Copy</b> method to obtain the acceptable values.  |
| <b>Group</b>           | 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. |
| <b>Description</b>     | Description of the entry.  |
| <b>Open (Embedded)</b> | Boolean value ( <b>true</b> or <b>false</b> ) that indicates to open the session embedded. The default value is false, meaning that  |

| OPTION                                    | DESCRIPTION  |
|---|--|
|   | the native client will be used depending on the technology. MSTSC.EXE for instance.  |
| <b>Username</b>                           | Username used to open a session to the device.   |
| <b>Domain</b>                             | Domain used to open a session to the device.   |
| <b>Password</b>                           | Password used to open a session to the device. Please note that this field is encrypted and stored into another field upon being imported. |
| <b>MetalInformation\S<br/>erialNumber</b> | Serial Number of the device.   |
| <b>MetalInformation\S<br/>erviceTag</b>   | Service Tag of the device  |
| <b>MetalInformation\P<br/>urchaseDate</b> | Purchase date in a ISO8601 format, i.e. yyyy-mm-dd   |

## CSV SAMPLES

### WITH SPECIFIED SESSION TYPES

```
Host,Name,Template,ConnectionType,ConnectionSubType,SubMode,Group,Username,Domain,Password
192.168.10.001,one,,Microsoft Remote Desktop (RDP),,,QA Lab,,,Description001,
http://online.remotedesktopmanager.com,two,,Web Browser (http/https),,,QA Lab,,,Description002,
192.168.10.003,three,,LogMeIn,,,QA Lab,,,Description003,
192.168.10.004,four,, "Telnet, SSH, RAW, rLogin",,,0,QA Lab,,, "This is the Putty sub-t
192.168.10.005,five,, "Telnet, SSH, RAW, rLogin",,,1,QA Lab,,, "This is the Telnex (Reb
192.168.10.006,six,, "Telnet, SSH, RAW, rLogin",,,2,QA Lab,,, "This is the SSH Shell (Re
192.168.10.007,seven,, "Telnet, SSH, RAW, rLogin",,,3,QA Lab,,, "This is the SSH (Rebex
192.168.10.008,eight,,VNC,,,QA Lab,,,Description008,
192.168.10.009,nine,,Citrix,,,QA Lab,,,Description009,
```

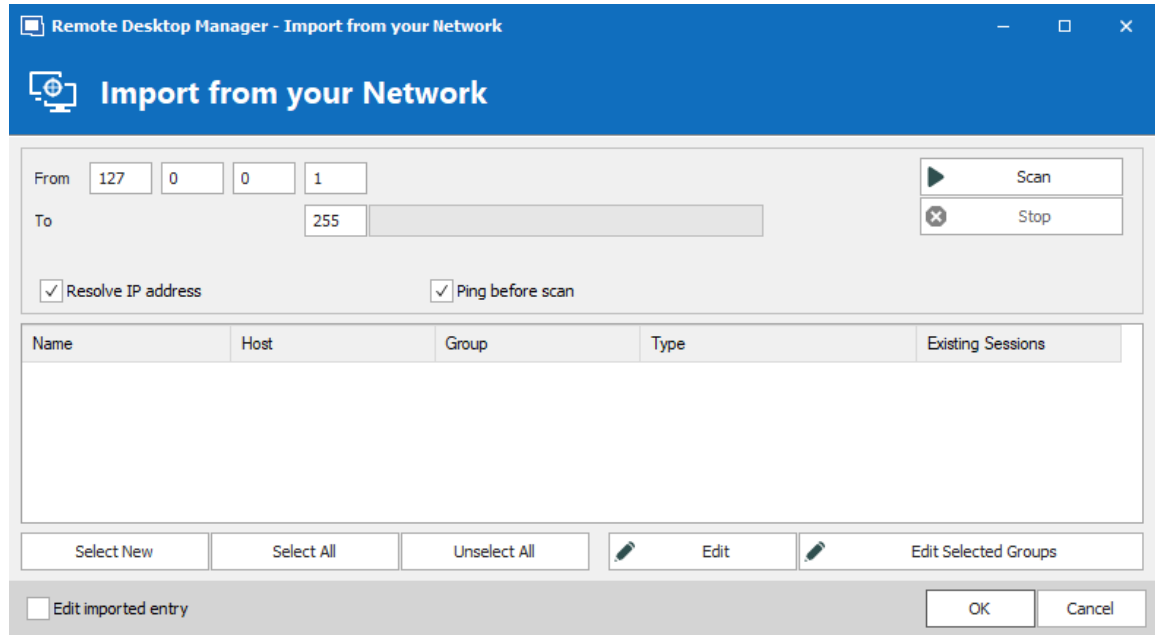
### 6.2.10.3 Import Network Scan

## DESCRIPTION

The **Import from Network** allows you to perform a network scan based on a predefined 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.



*Import from your Network*

### 6.2.10.4 Import Sessions

## DESCRIPTION

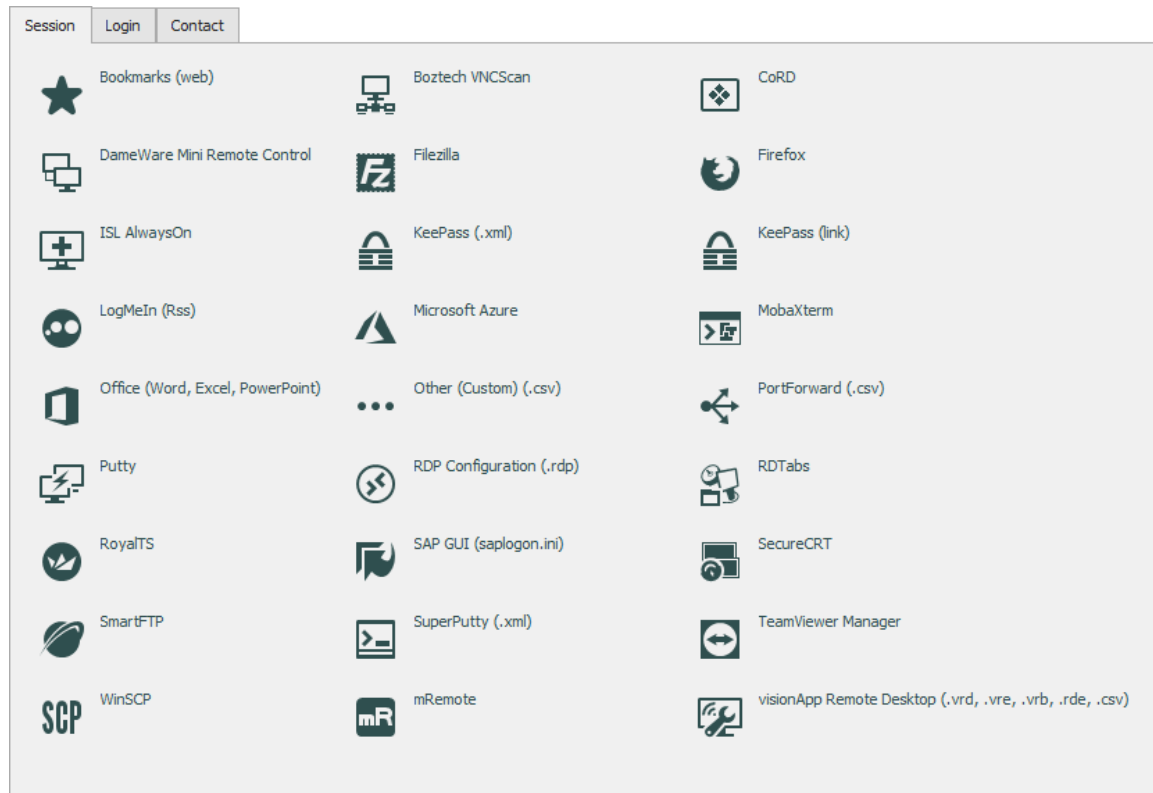
Use the **File – Import – Import from – Session** to import sessions from other software into Remote Desktop Manager.





The import feature is only active if the import Permission has been enable inside the user account.

## SETTINGS



*Import from Session*

## IMPORT FROM SESSION

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. Please note that all entries will be imported in the current folder. For some applications it's not possible to extract the password.

We support a Multitude of Sessions, explore to your heart's content!

### 6.2.10.5 Import Logins

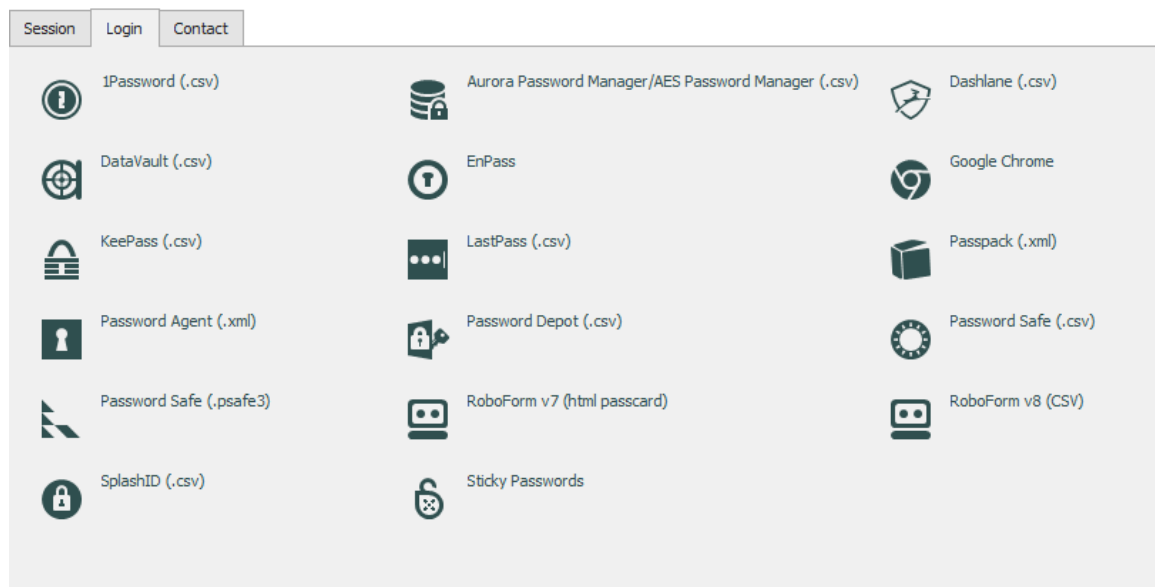
## DESCRIPTION

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



The import feature is only active if the import Permission has been enable inside the user account.

## SETTINGS



*Import from Login*

## IMPORT FROM LOGIN

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. Please note that all the entries will be imported in the current folder. We support a multitude of Login imports, explore to your heart's content!

### 6.2.10.6 Import Contacts

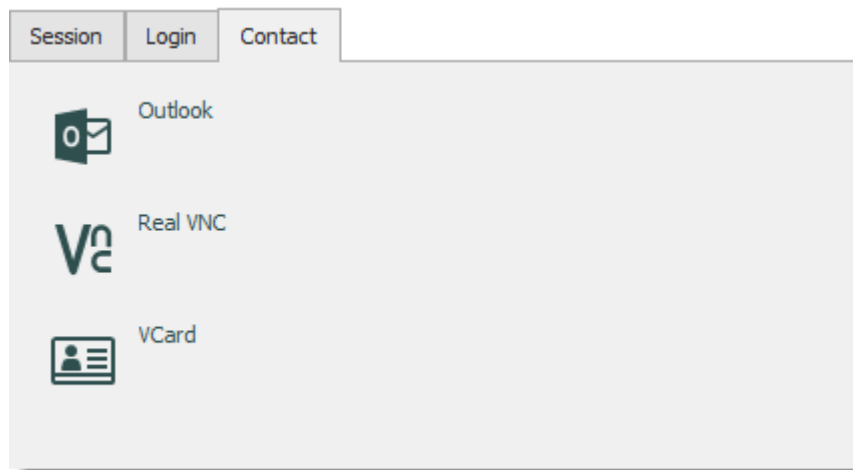
## DESCRIPTION

Use the **File – Import – Import from – Contact** to import contacts from other software into Remote Desktop Manager.



The import feature is only active if the import Permission has been enable inside the user account.

## SETTINGS



*Import Contact menu*

## IMPORT FROM CONTACT

It's now possible to import the contact from different sources:

- Microsoft Outlook
- Real VNC
- VCard

Please note the all the entries will be imported in the current folder.



Microsoft Outlook contacts sub-folders are also supported.

### 6.2.11 Export

#### DESCRIPTION

Use the **File – Export** to export entries from Remote Desktop Manager. Below is a list of export options:

- Export All Entries (.rdm).
- Export All Host List (.csv).
- Export All Entries (.csv).
- Export All Entries (.html).
- Export All Entries (.xml) (It's exactly the same content as a .rdm file but with the XML extension).



If you have used **Document** entries in the **Stored in database** mode, or used **attachments**, the binary content of the documents is NOT exported in any of our export formats. These documents/attachments MUST be handled manually.

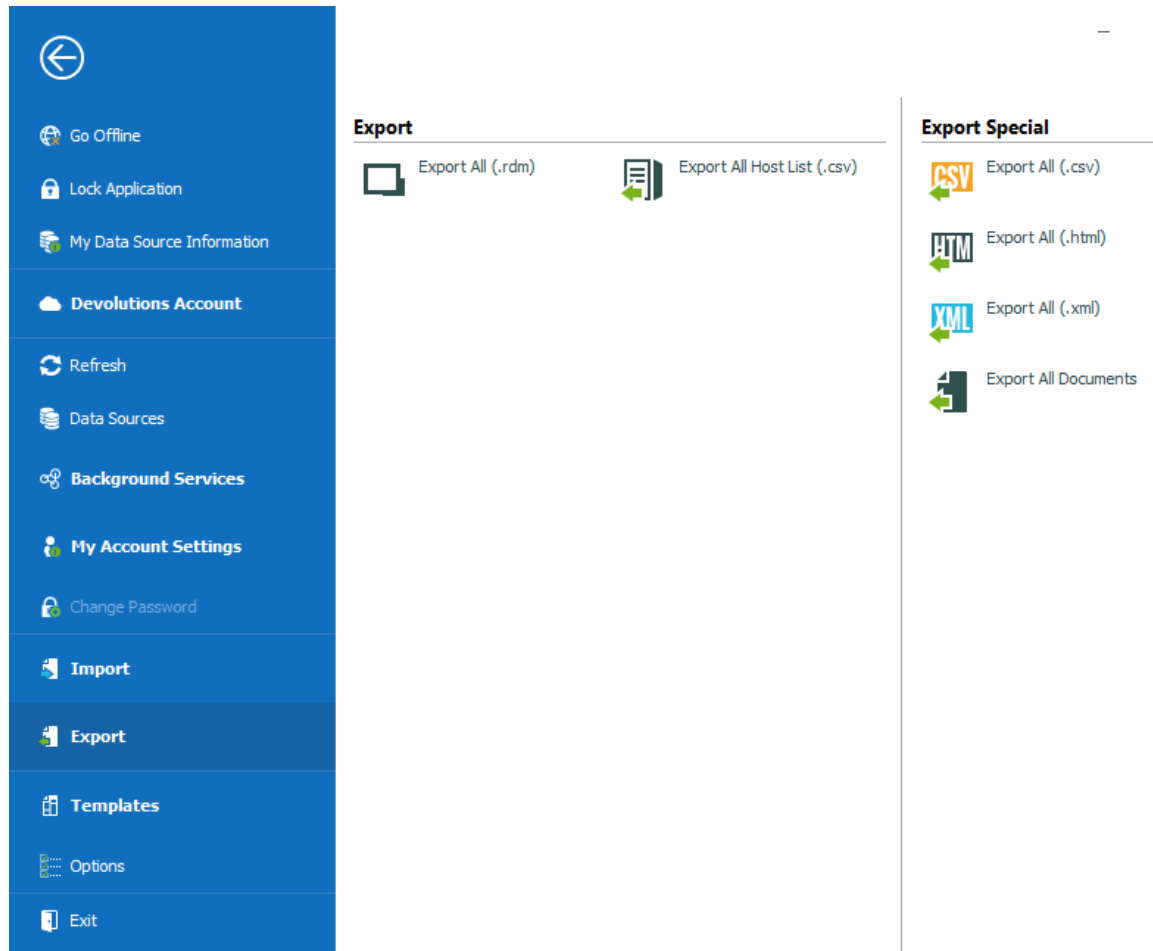


The export feature is only active if the import Permission has been enabled inside the user account.



The only appropriate format to import the entries back into Remote Desktop Manager is the .rdm 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). See Security Group Management for more information.

## EXPORT ALL ENTRIES (.RDM)

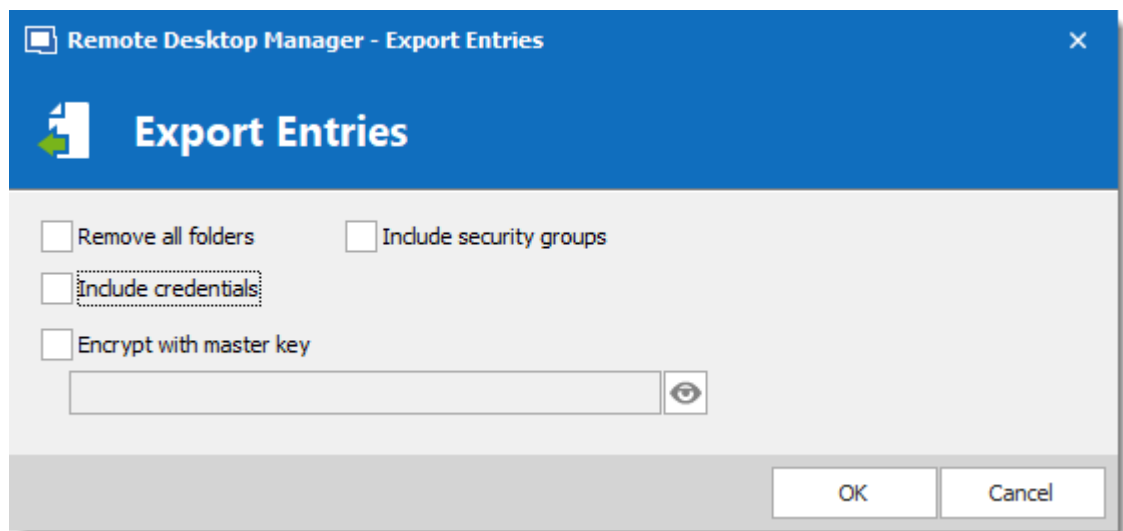
Export all entries in a .rdm file that can be imported into any Remote Desktop Manager data source. You can also include credentials in this export format and secure your file with a master key.



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 entries in .rdm*

## 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 ALL ENTRIES (.CSV)

Export all entries 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.

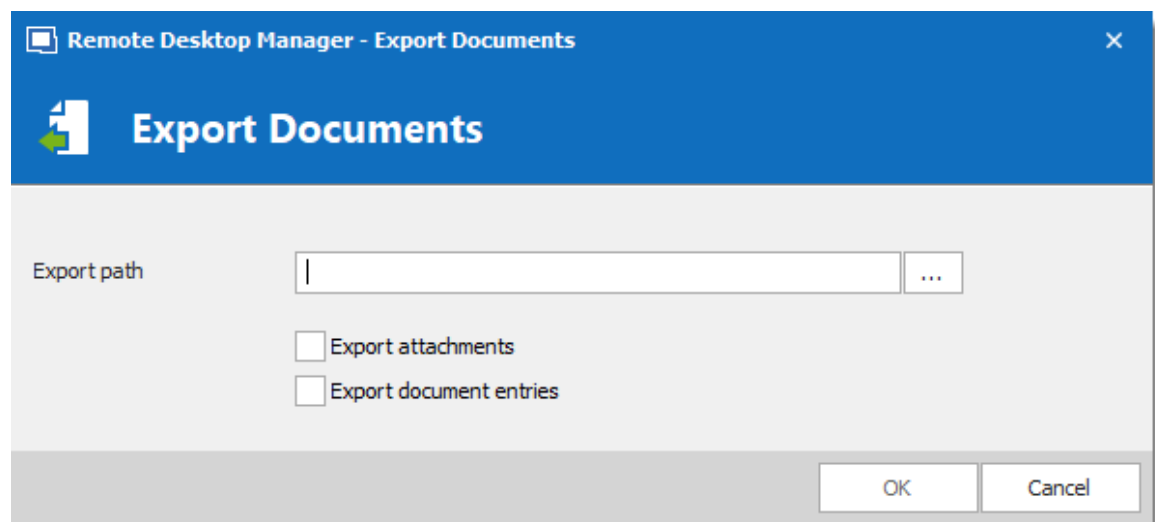
## EXPORT ALL ENTRIES (.HTML)

Export all entries within a AES-256 to encrypt self contained html file. See [Export Html Encrypted](#) topic for more information.

## EXPORT ALL ENTRIES (.XML)

Because it brought confusion to our user base, this export format has been converted to perform the exact same export as the "Export all entries" 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.

### 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 all entries. **Right-click** and select **Export – Export Special – Export All Entries (.html)** or use **File – Export – Export All Entries (.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.



```
<tr>
  <td class="label Password">Password</td>
  <td class="value Password">
    <span id="dff570b2-5fb1-459b-af38-0fcb4f677484" data="U2FsdGVkX1/TAub+TpB+UrMU2m1RSVdiU8FP7tPnXAaBLZdvSV9IiM2AKdIv0Siv">
      <a class="encrypted" onclick="javascript:decryptText('dff570b2-5fb1-459b-af38-0fcb4f677484')">*****</a>
    </span>
  </td>
</tr>
```

*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 an import wizard](#)
- 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.

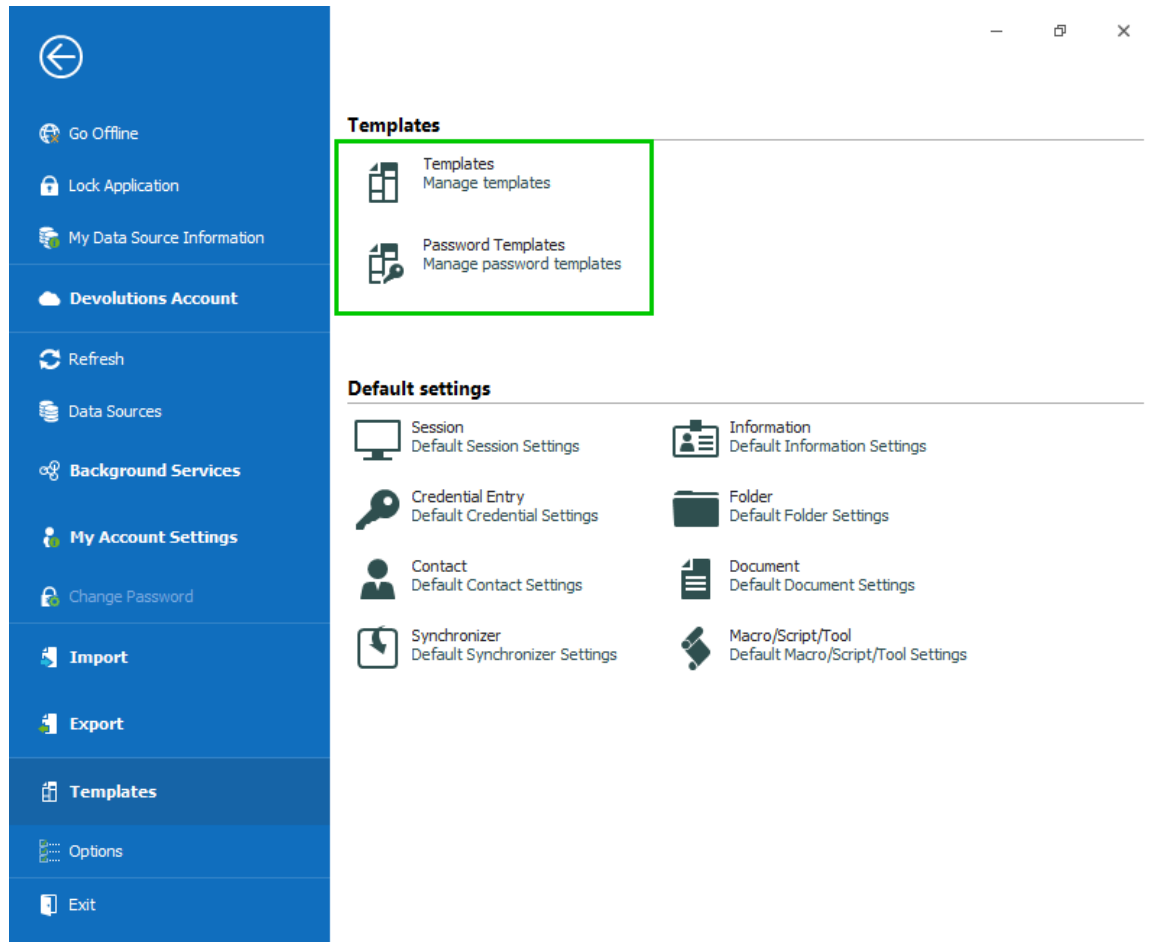
This allows for creating predefined templates available to use with the quick connect feature or when creating or importing a entries.



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 **Management** section of the [Data source permissions \(System Permissions\)](#).



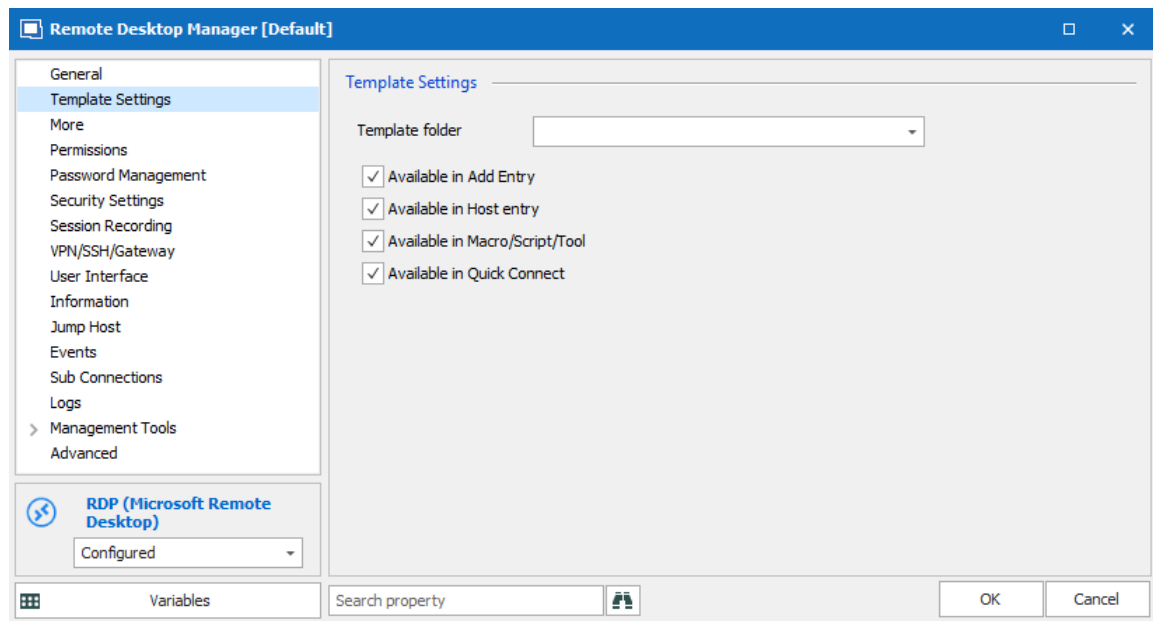
In Advanced Data Sources , local templates are disabled by default. They can be enabled from the [Data Source Settings \(System Settings\)](#).



*File – Templates*

## AVAILABILITY

When creating a template, its availability can be specified in the properties.



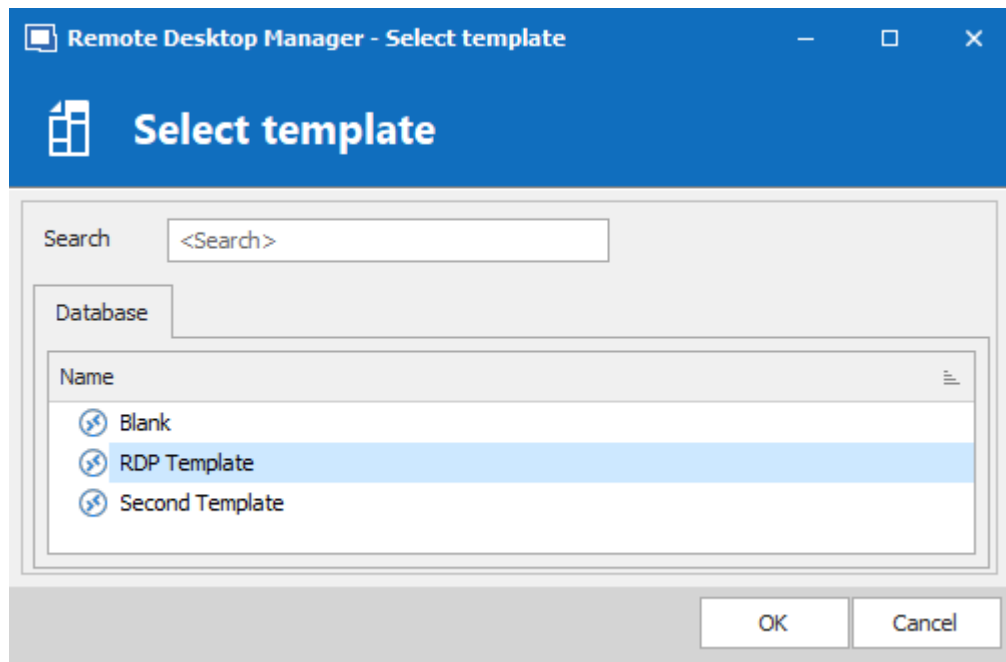
*Template properties – Template Settings*

## USAGE

Templates can be used in the following cases:

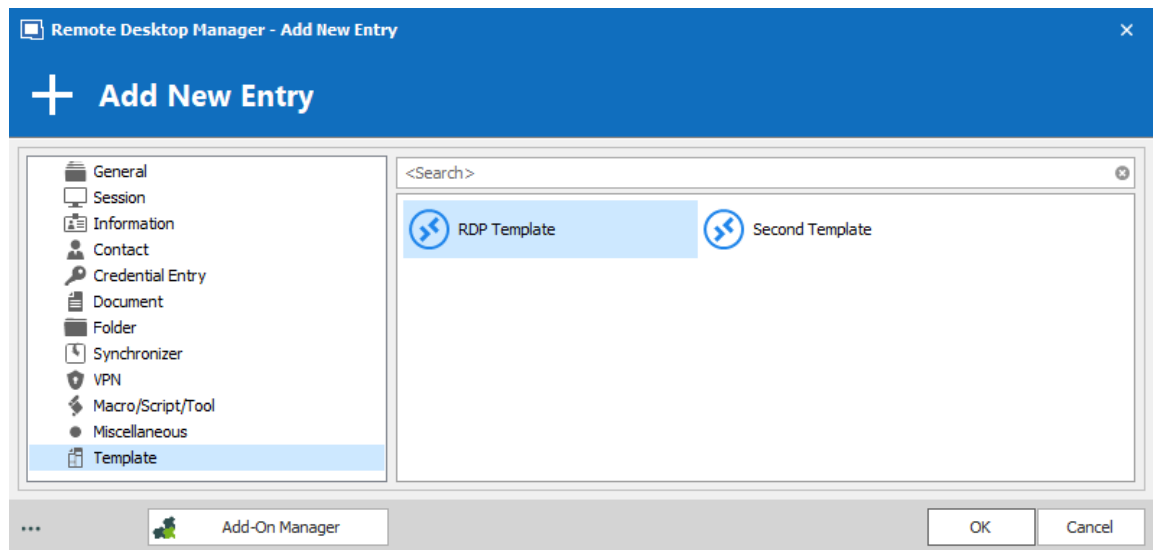
### CREATE A NEW ENTRY

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 [Data Source Settings \(System Settings\)](#).



*Select a template*

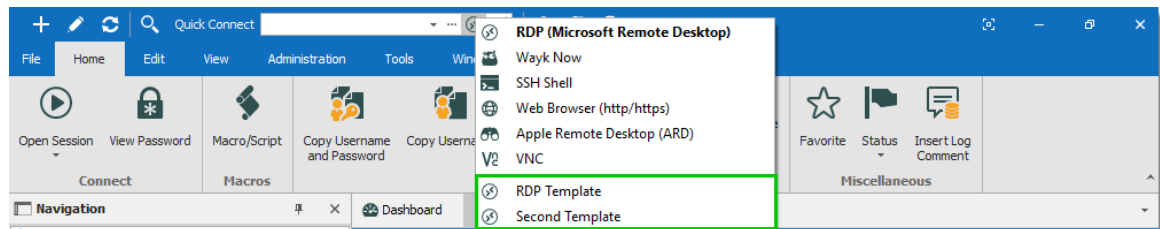
The template can be selected before creating the entry as well. Simply use the **Template** section of the **Add New Entry** window.



*Add New Entry – Template*

## RUN A QUICK CONNECT SESSION

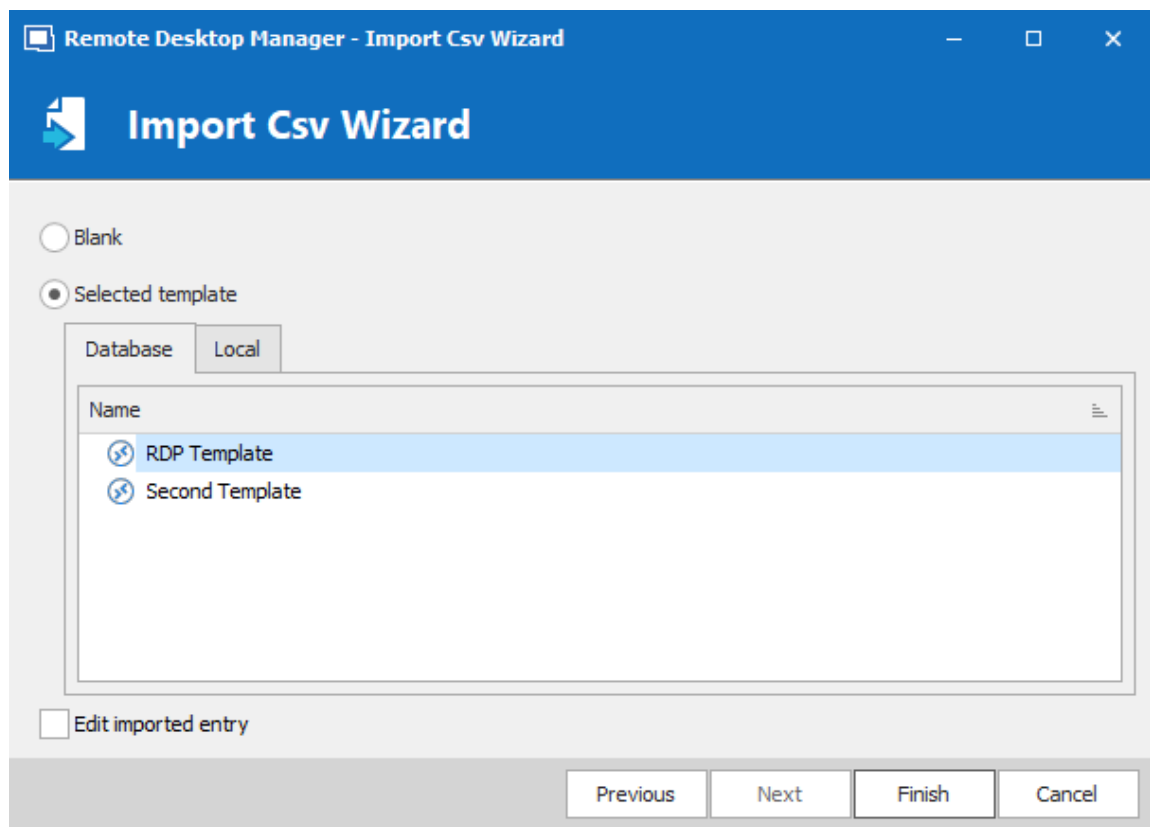
Templates can be used with the **Quick Connect** feature. For example, the same template can be used to connect to different hosts.



*Quick Connect*

## IMPORT WIZARD

The import session wizard uses a template for the imported sessions.



*Import Session Csv Wizard*

### 6.2.12.1 Creating Templates

## DESCRIPTION

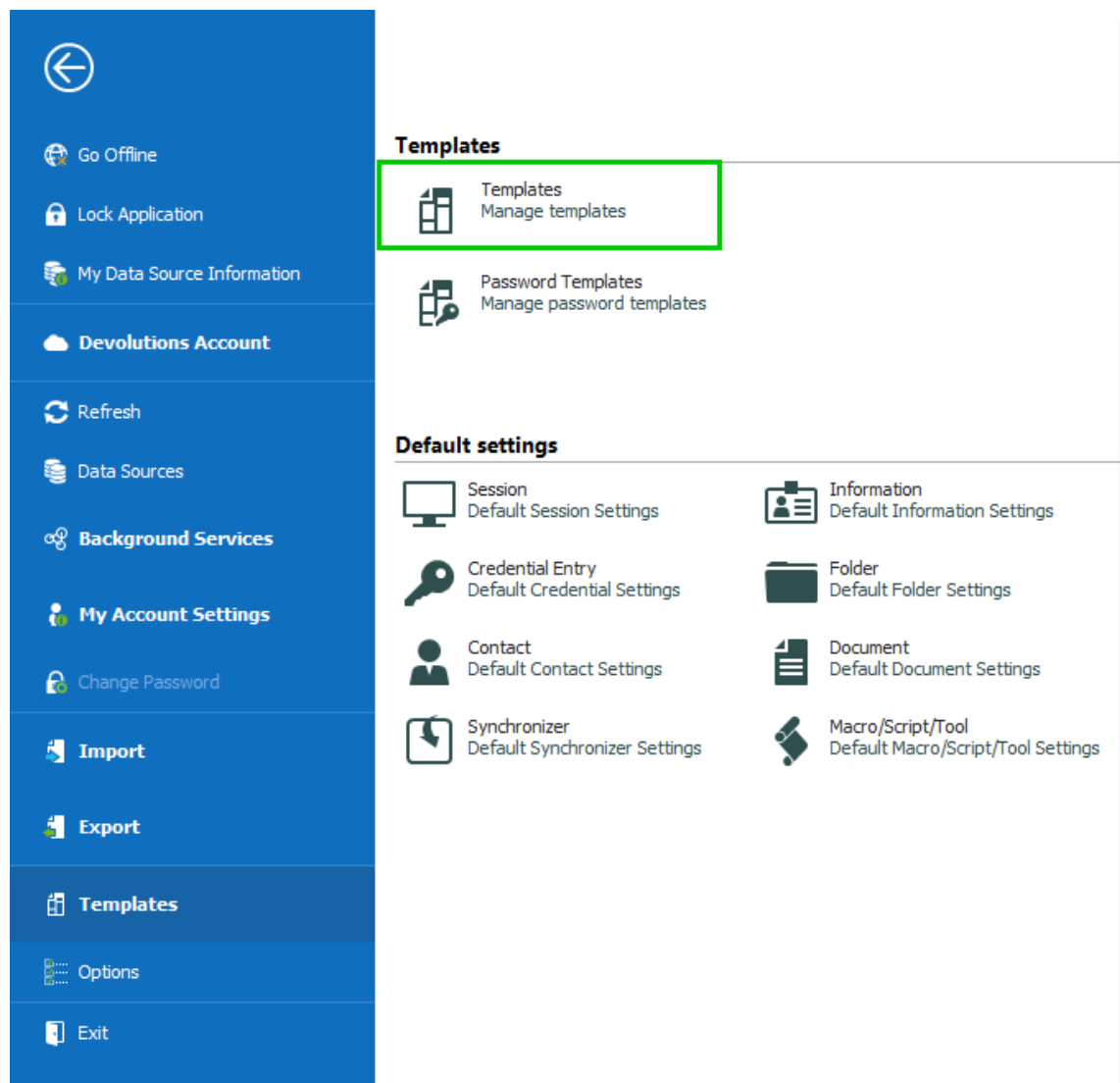
There are many ways to create template for entries. You can create a new template, save an entry as a template, import entries as templates, and duplicate a existing template. It is also possible to create group templates.

In this topic:


- [New Template](#)
- [Save as Template](#)
- [Import Template](#)
- [Duplicate Template](#)
- [Template Groups](#)

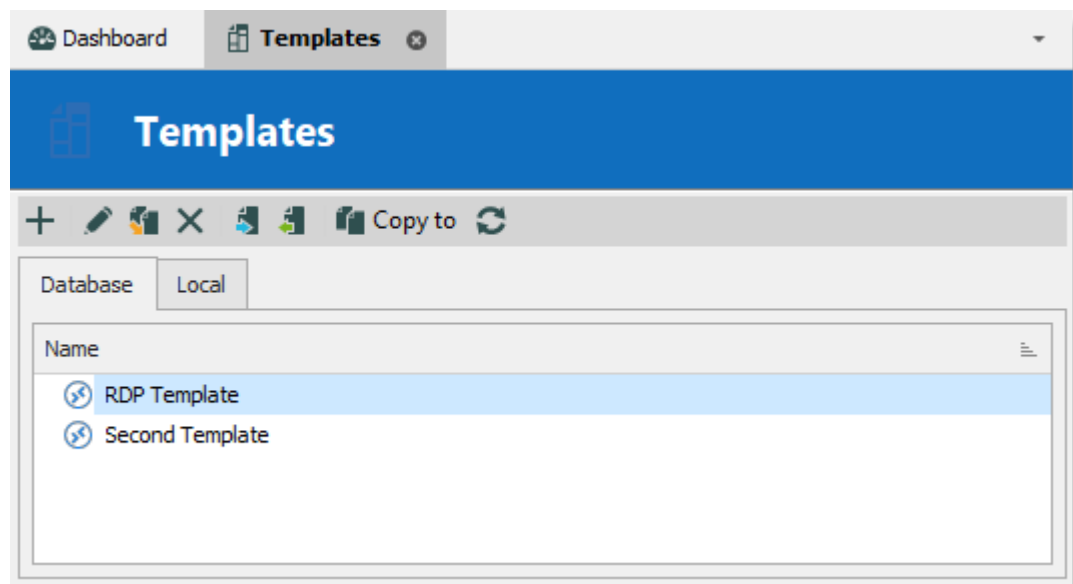
## CREATE A NEW TEMPLATE

1. Navigate to **File – Templates** and select **Templates**.



*File – Templates*

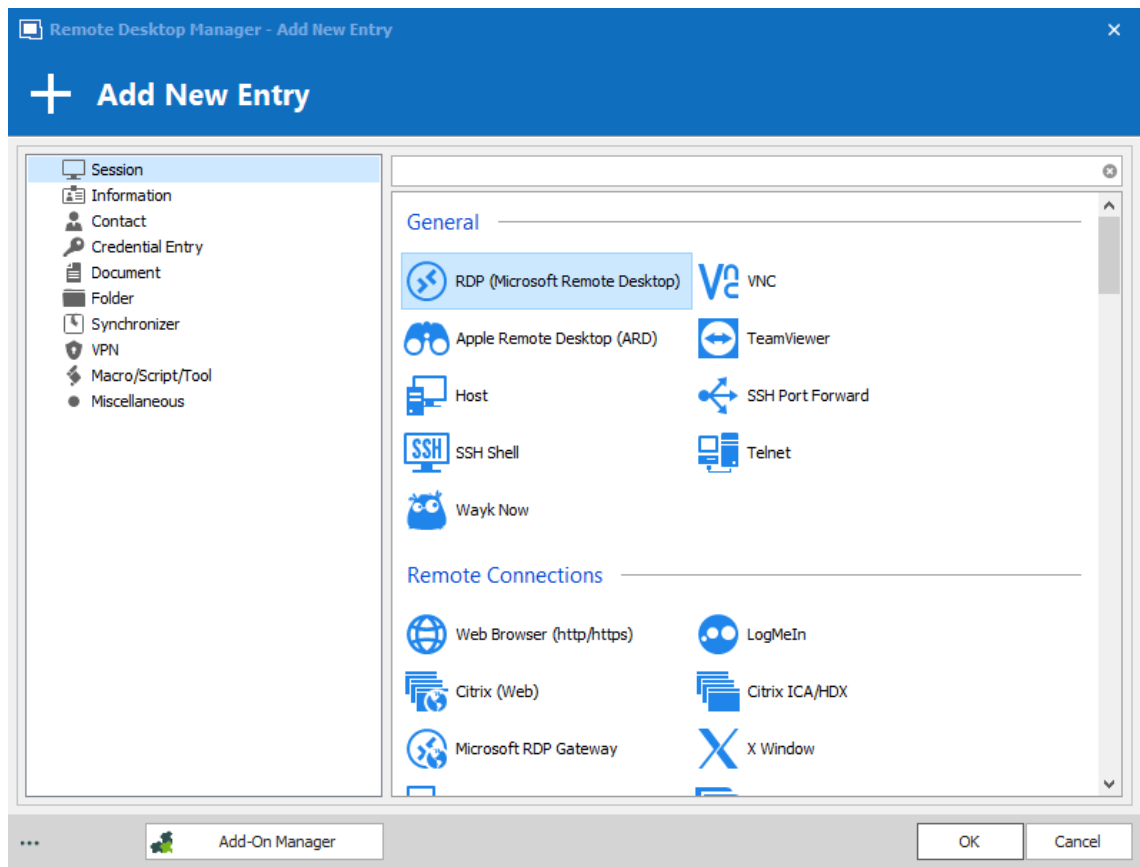
2. In the **Templates** window, click the **Add template**  button.



*Add a new template*

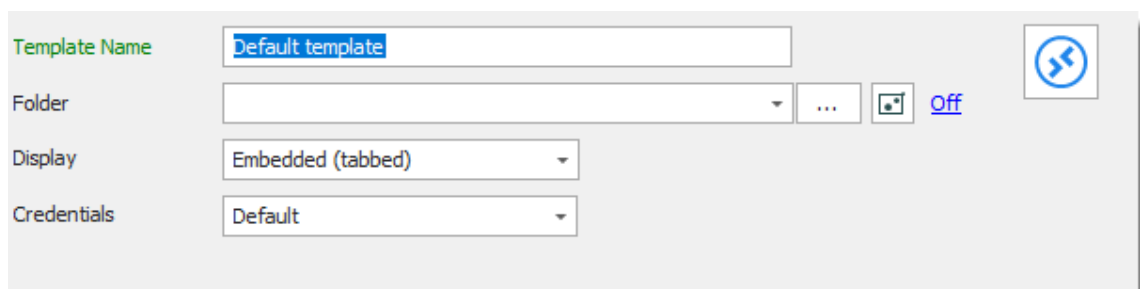
3. Select an entry to create the template for.





*Select an entry to create the template for*

4. Enter a name for the template, and configure the properties as necessary.

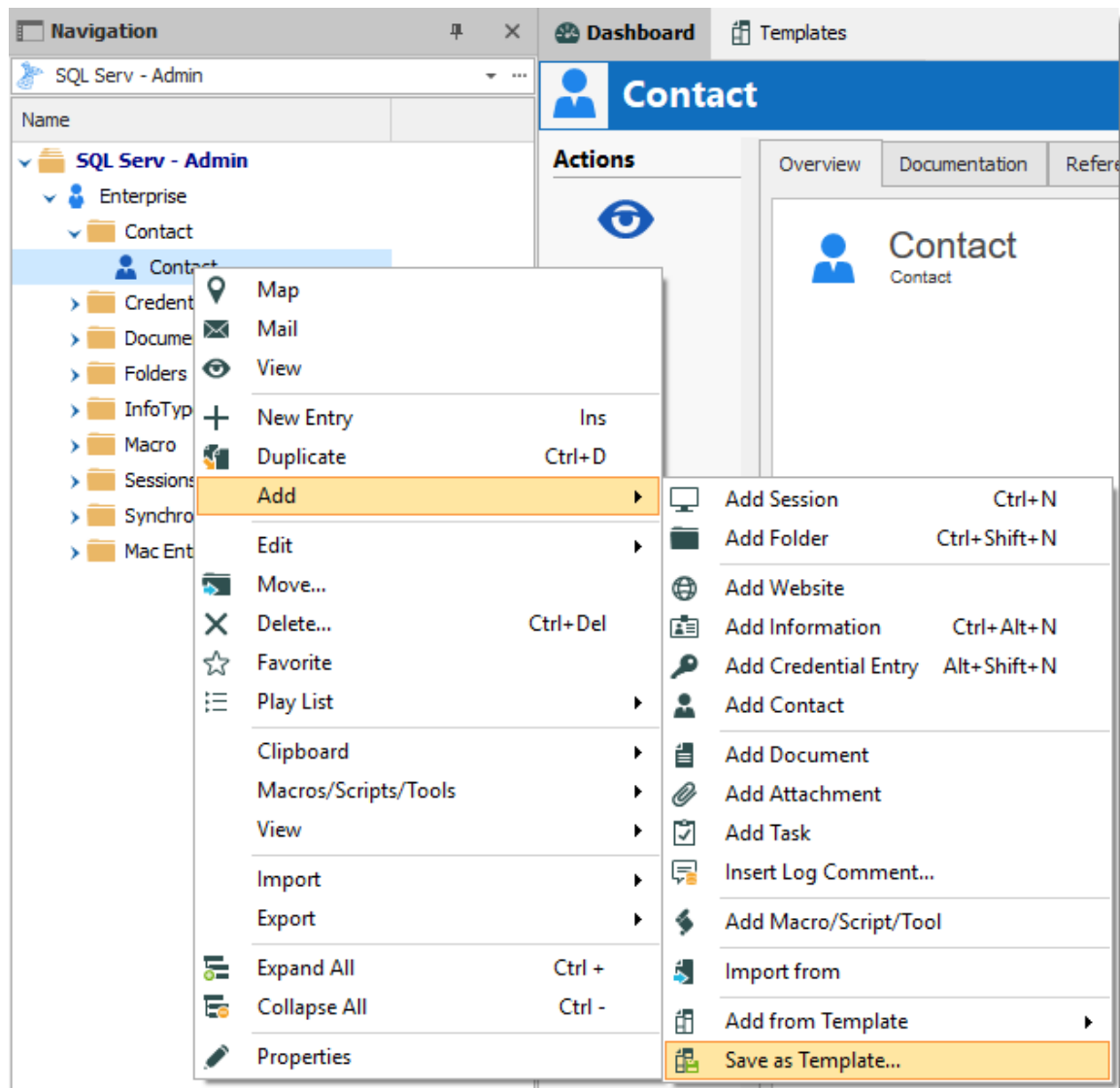


*Template Properties*

## SAVE ENTRY AS TEMPLATE

It is possible to save entries as templates to use their properties in other entries. Furthermore, this can be achieved 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...**



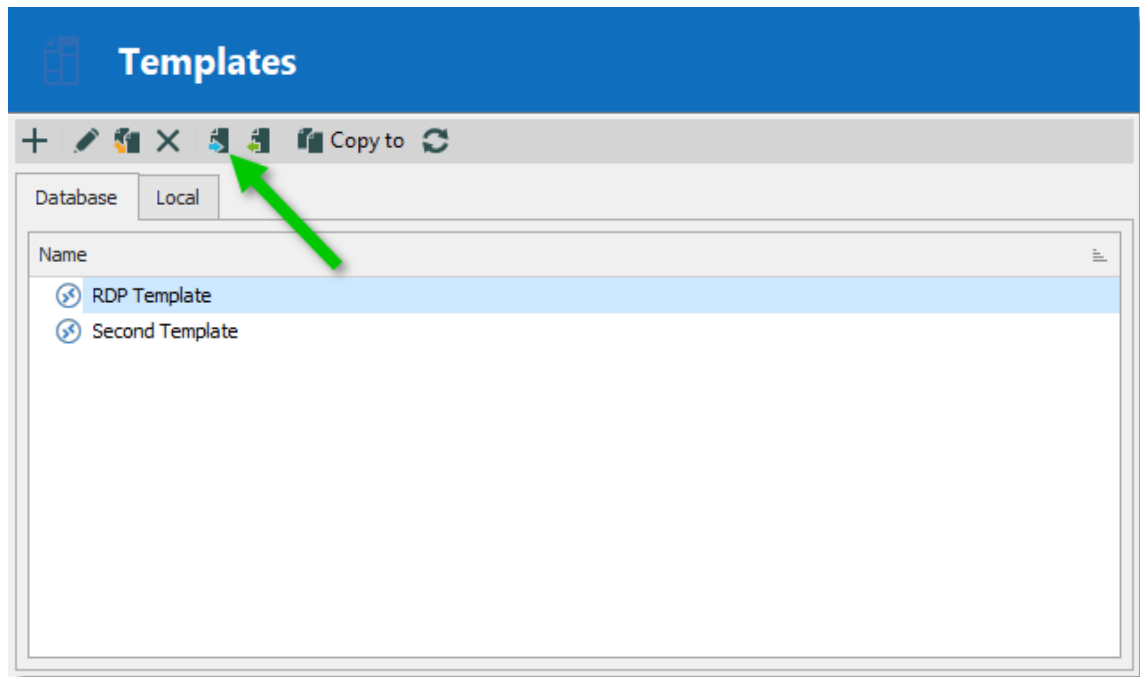
*Save as Template...*

## 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.

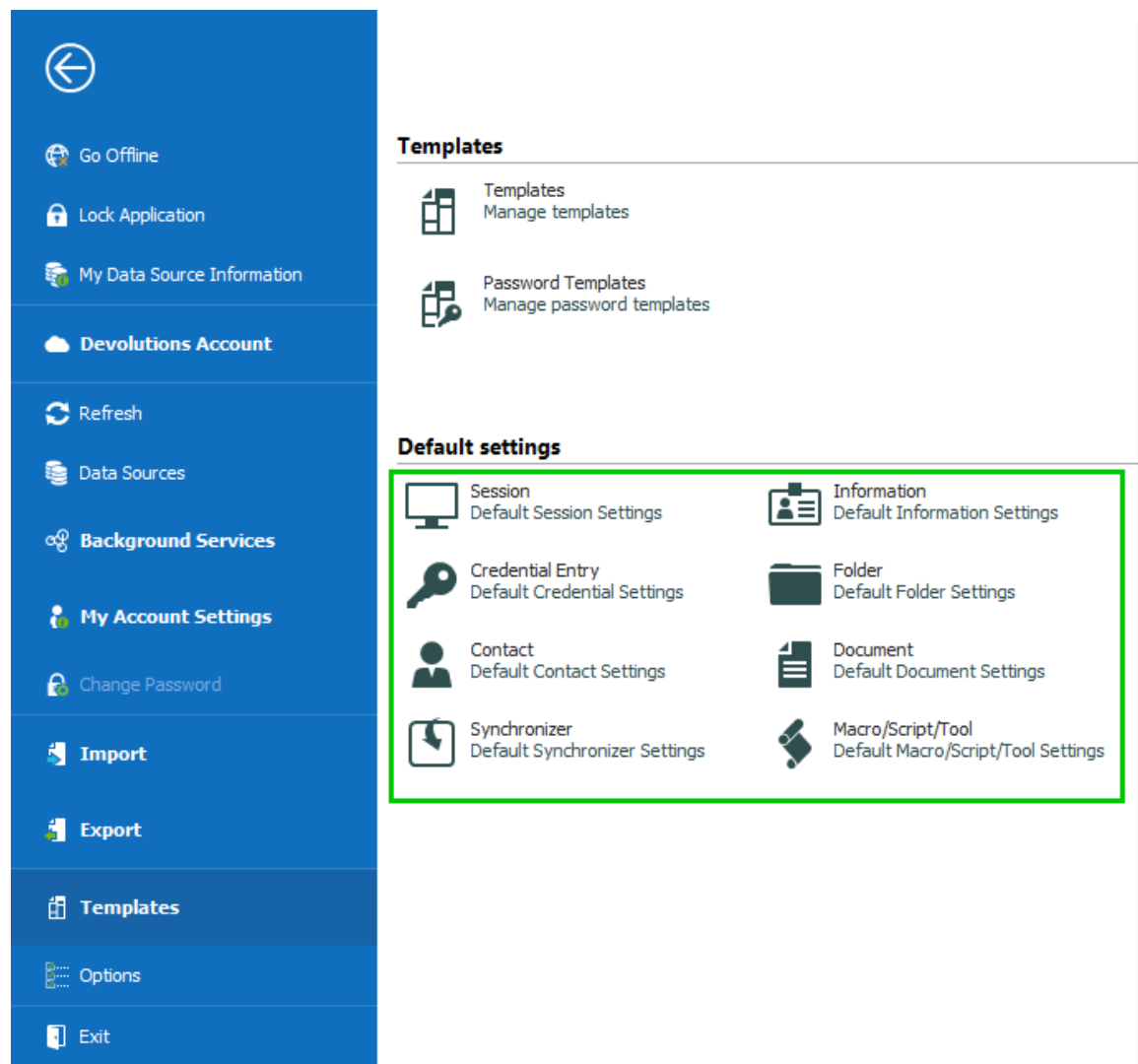
**Right-click** a selection of entries or a folder, select **Add**, then **Save as Template...**

#### 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

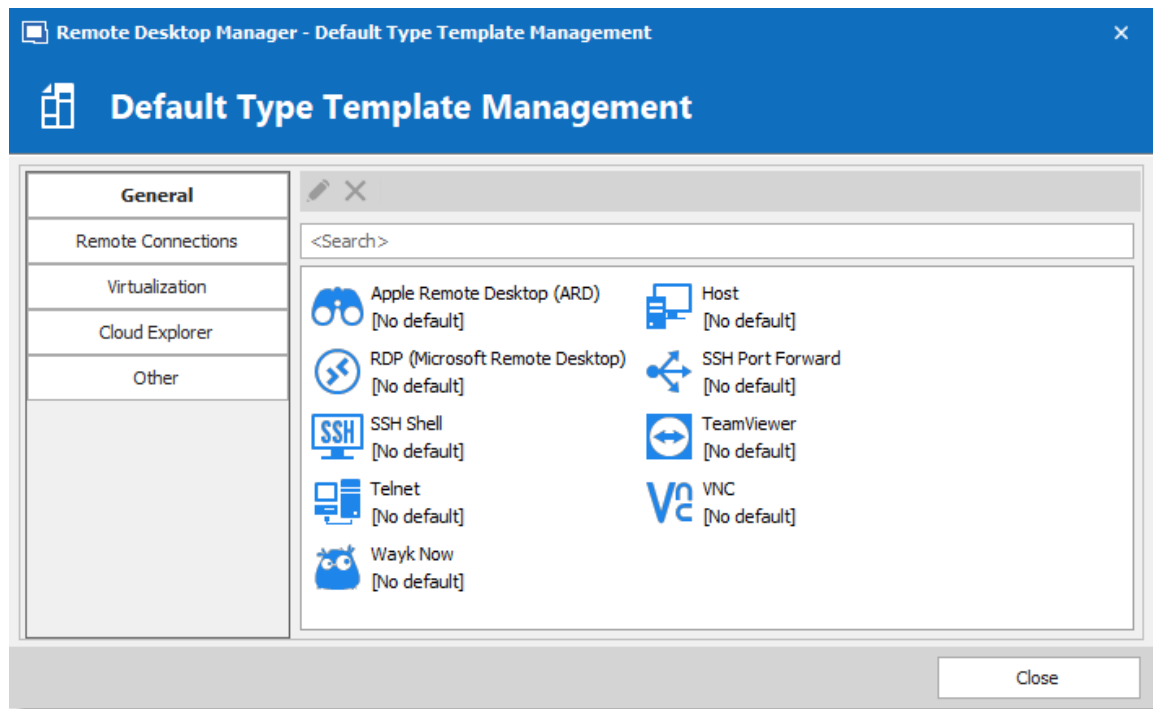
To help you locate the entry type you want to customize, all entry types are organized by category.

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

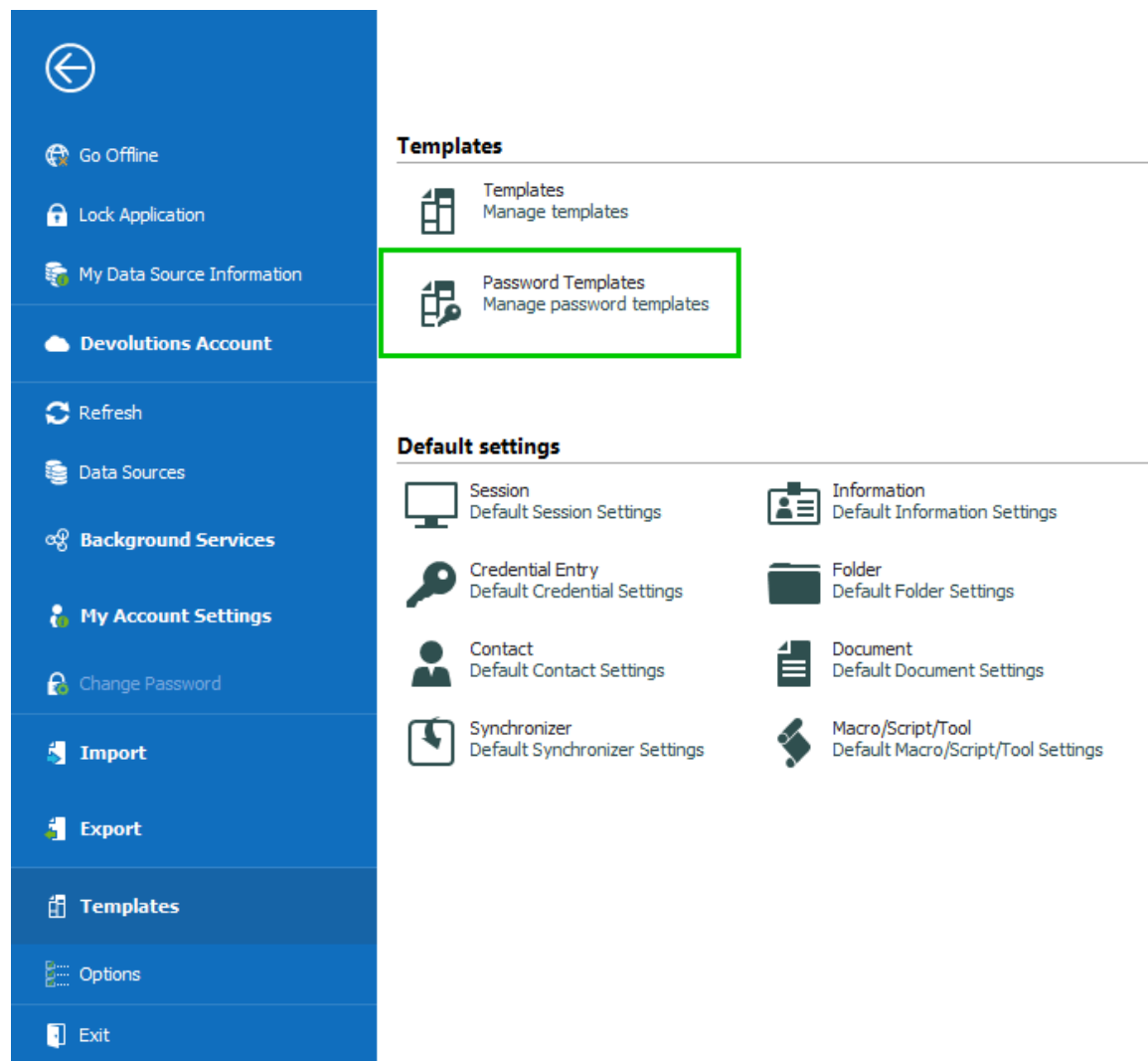
Password templates set requirements for the password format: characters usage, patterns, readability.

Password templates are available in the password generator. Password templates can be optional or required.

## SETTINGS

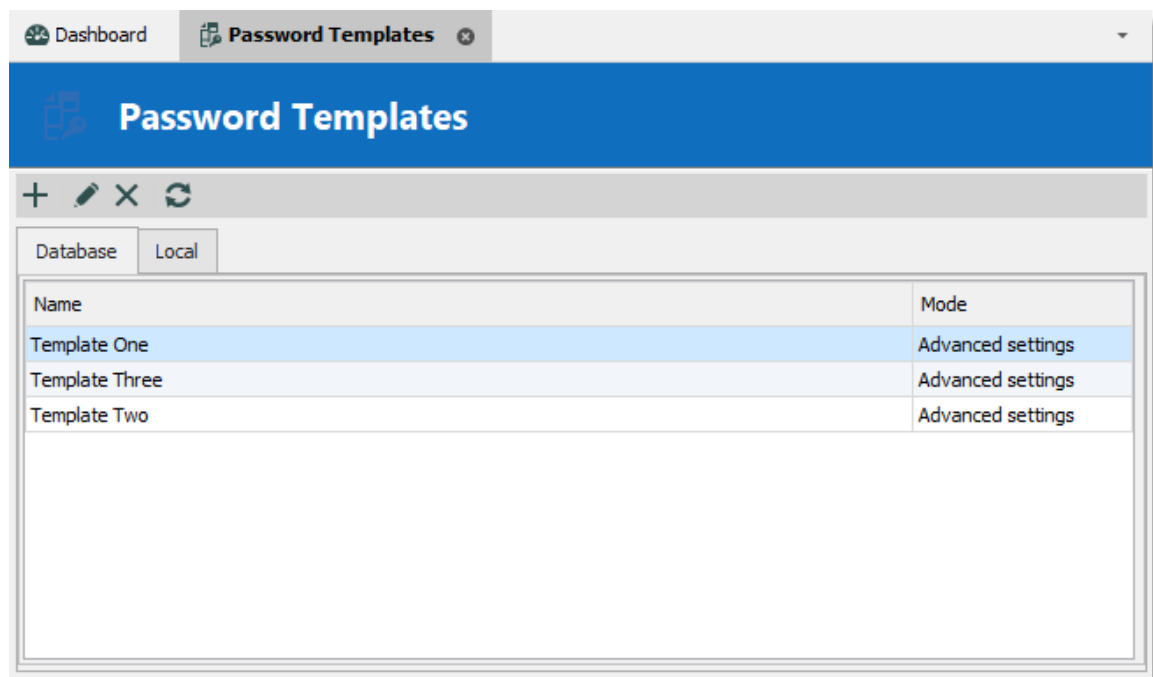
### CREATE A PASSWORD TEMPLATE

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
<b>Default</b>	General settings about length and minimum amounts for characters and symbols.
<b>Advanced settings</b>	Granular character settings (e.g. special characters and symbols, inclusions, exclusions).
<b>Readable password</b>	Settings for syllables, numbers and symbols.
<b>Use a pattern</b>	Set a pattern for the passwords using the <a href="#">key</a> .
<b>Pronounceable password</b>	Settings for length, case, digits and characters.



c) Choose specific settings

Remote Desktop Manager - Password Templates

**Password Templates**

Name: Cloud Services

Mode: Advanced settings

Password length: 20

☒ Upper-case (A, B, C, ...) 6 ☒ Underline ( \_ ) 0 ☐ High ANSI characters 0

☒ Lower-case (a, b, c, ...) 0 ☐ Space ( ) 0 ☐ XML Compliant

☒ Digits (0, 1, 2, ...) 0 ☒ Special (!, \$, %, &, ...) 0

☒ Minus ( - ) 0 ☐ Brackets ([, ], {, }, (, ), <, >) 0

Include the following characters:  0

Exclude the following characters:

OK Cancel

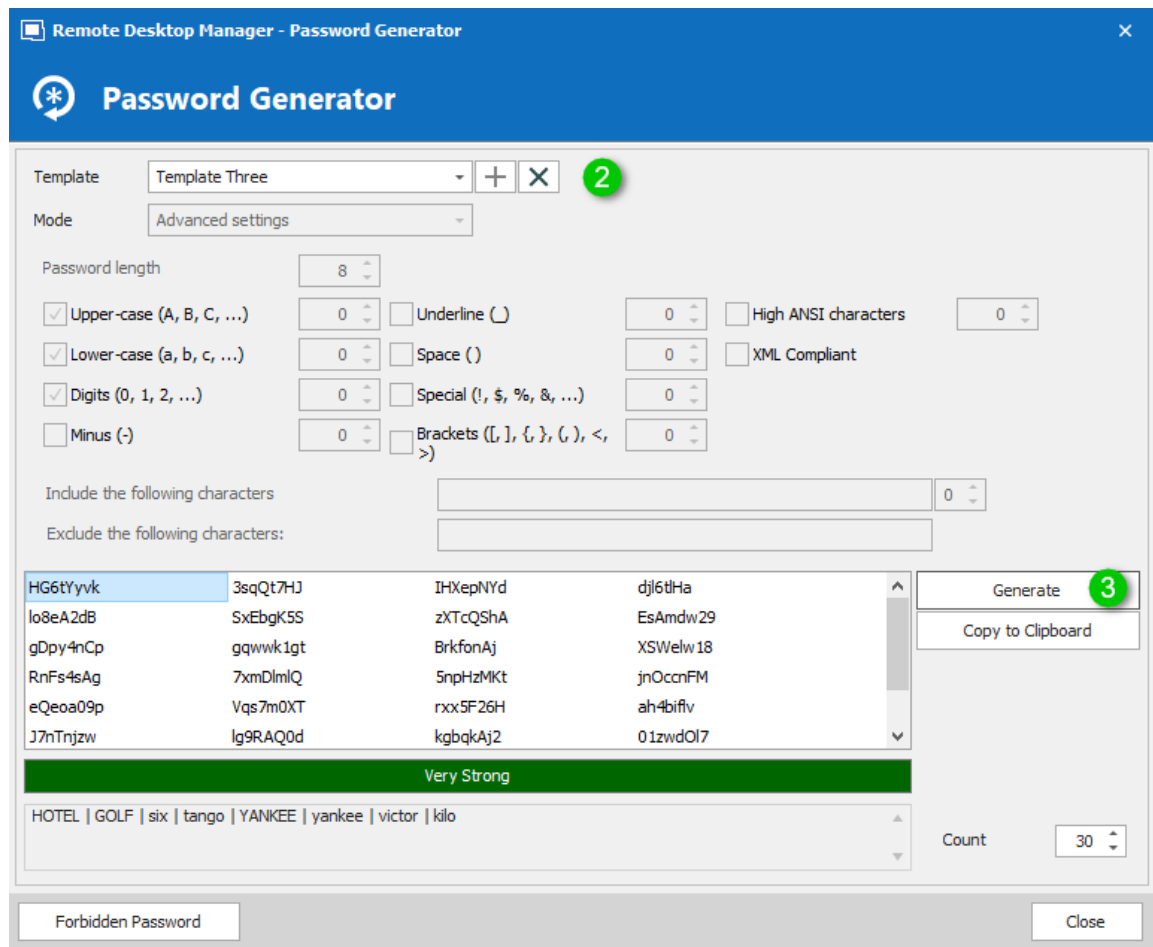
5. The password is now available in the **Password Generator** (**Tools** menu).

## 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.

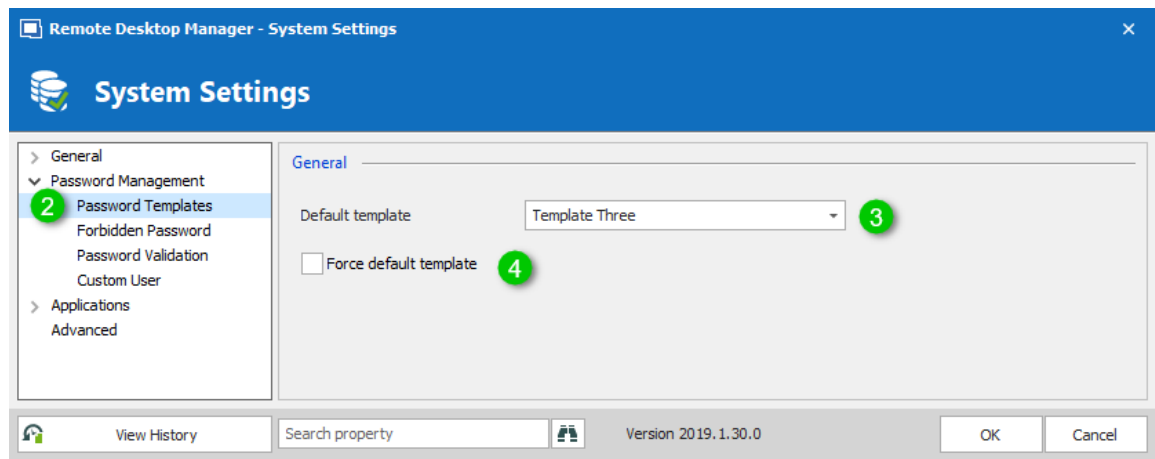


*Password Generator using a password template*

## 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.



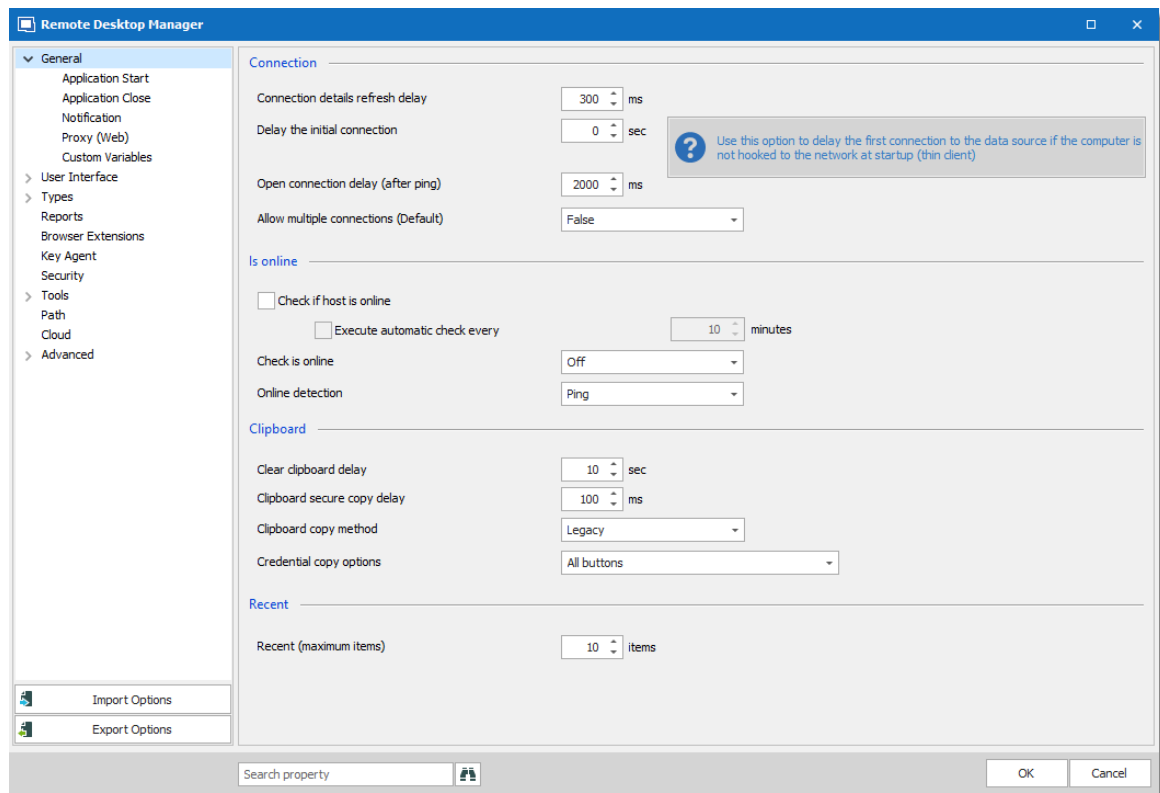
*System Settings – Password Templates*

### 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

Options you configure:

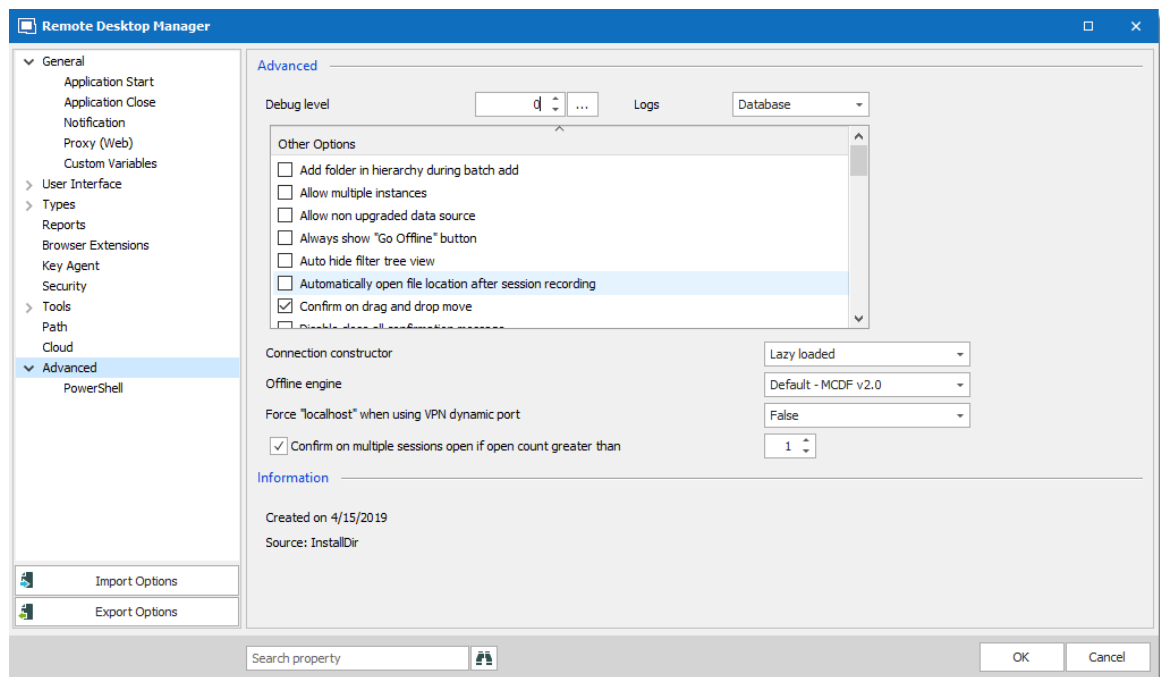
- **General:** Application Start (including update options), Application Close, Notification, Proxy (Web), Custom Variables
- **User Interface**
- **Types:** Settings for different types of entry, terminal, ssh keys, etc.
- **Reports**
- **Browser Extensions:** Settings for Devolutions Web Login
- **Key Agent:** Hold SSH Keys in memory already decoded and ready for them to be used. For more information see [Key Agent Manager](#)
- **Security:** Local application security only; You can set security for all users in the data source
- **Tools**
- **Path:** Customize installation paths for Remote Desktop Manager, logs, documents, templates and add-ons
- **Cloud**
- **Advanced**

- Import Options
- Export Options
- Search Option Property

### 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
<b>Debug level</b>	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 .
<b>Logs</b>	<p>The logs can be saved in a file or in a database file. Select between:</p> <ul style="list-style-type: none"> <li>• <b>Both:</b> Logs will be saved in a text file and in a database file.</li> <li>• <b>Database:</b> Logs will be saved in a file named RemoteDesktopManager.log.db. The file is located in the installation folder of the application.</li> <li>• <b>File:</b> Logs will be saved in a file named RemoteDesktopManager.log. The file is located in the installation folder of the application.</li> </ul>
<b>Connection constructor</b>	The connection constructor is used for memory optimization when using legacy. We strongly recommend to leave this option at Default. <b>Only change this option upon request from a Devolutions support technician.</b>
<b>Offline engine</b>	You can choose your Offline engine between the SQLite or OpenMCDF. <b>Only change this option upon request from a Devolutions support technician.</b>
<b>Force "localhost" when using VPN dynamic port</b>	Forces the use of "localhost" when using the VPN dynamic port.
<b>Confirm on multiple session open if open count greater than</b>	Select a target number where mass opening sessions will demand confirmation.

## OTHER OPTIONS - CONNECTIONS

OPTION	DESCRIPTION
<b>Automatically open file location after session recording</b>	After a session recording, it will open the destination folder where the file is saved.
<b>Disable close all confirmation message</b>	Disables the Close all confirmation message when closing/disconnecting multiple entries at the same time.
<b>Disable document selector (CTRL + Tab)</b>	When left enabled, it will allow to switch from multiple open tab connections.
<b>Disable embedded 32 shell execute</b>	Disable the shell embedded 32 execute in Windows for embedded sessions.
<b>Disable logoff confirmation message</b>	When pressing the logoff button in an embedded RDP session, Remote Desktop Manager, will disconnect the session without the logoff confirmation message.
<b>Disable multi-thread loading</b>	This setting allows Remote Desktop Manager to use multiple threads to load the data. Disabling this option will decrease the performance.
<b>Disable multi-thread offline file</b>	This setting allows Remote Desktop Manager to use multiple threads in offline file. Disabling this option will decrease the performance.
<b>Disable RDP virtual channel</b>	Turning off virtual channel disables some Remote Desktop Services features such as clipboard and printer redirection.
<b>Enable advanced Logging for Telnet and SSH</b>	This option creates an AdvancedTelnetSSH.log file in %LocalAppData%\Devolutions\RemoteDesktopManager.

OPTION	DESCRIPTION
<b>(AdvancedTelnetSSH.log)</b>	This file can be helpful when retrieving logs for Telnet/SSH connections.
<b>Enable global event logging for Telnet and SSH (DevolutionsTerminal.log)</b>	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.
<b>Enable global logging for Rebex terminals (AdvancedTelnetSSH.log)</b>	Enables global event logging for Rebex terminals. It will create the file AdvancedTelnetSSH.log at the same place the configuration file is located.
<b>Enable offline read/write locks</b>	Activate locks for the Offline read/write rights.
<b>Enable tags textbox in properties</b>	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.
<b>Ensure that KeePass is running</b>	Validate that KeePass is running on your computer before accessing any KeePass data.
<b>Force refresh before edit entry</b>	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.
<b>Force restore application with desktop shortcut</b>	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.
<b>Open shortcut session silent</b>	Disable the command line warning message when using a shortcut.



OPTION	DESCRIPTION
<b>Use connection loader optimization</b>	Only enable this option upon request from our Support team.
<b>Use DirectX rendering in VNC</b>	By default this option is enabled to use DirectX rendering when available for VNC connection.
<b>Use manual activate tab</b>	Only switch to an entry tab manually. This disables the behavior where opening a connection will automatically select the new tab.
<b>Use Microsoft Office instead of editors</b>	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.
<b>Use NTFS Encryption for Offline mode</b>	When using <a href="#">Offline Mode</a> , a local file is created to hold a copy of the data source. If this is enabled the local file is encrypted using the built-in NTFS encryption of Windows. This setting may cause delays when accessing the data source because the local file is refreshed on every access.

## OTHER OPTIONS - GENERAL

OPTION	DESCRIPTION
<b>Add folder in hierarchy during batch add</b>	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.
<b>Allow multiple instances</b>	Allows more than one instance of Remote Desktop Manager to run concurrently. This is not a recommended practice.

OPTION	DESCRIPTION
<b>Allow non upgraded data source</b>	Allow Remote Desktop Manager to work on an older data source that has not being upgraded.
<b>Confirm on drag and drop move</b>	When session(s) are moved by drag and drop, a confirmation message will appear to confirm the move.
<b>Disable form editor cache</b>	Disables the form editor cache and force RDM to always fetch the information. It is not recommended to disable this feature for performance reasons.
<b>Disable password pwned check</b>	Disables the pwned check feature if it isn't forced by the administrator in the System Settings - Password Validation option.
<b>Disable resilient database connection handling</b>	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.
<b>Disable stack trace</b>	Disable the stack trace details when an error occurs in Remote Desktop Manager. This is a security feature.
<b>Disable telemetry</b>	Disable the analysis of data or statistics. Telemetry is the equivalent of Google Analytics. Note that the statistics are anonymous.
<b>Focus content on application activation</b>	Set focus on the last embedded session when the application is activated.
<b>Lock integrated security: validate only against domain context</b>	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.
<b>No Internet connection</b>	Disable the application to access the internet.

OPTION	DESCRIPTION
<b>Show deprecated data source types</b>	We don't support some data sources anymore, enabling this option will show them again.
<b>Use application directory for local play list</b>	Use the installation folder to save the local play list that has been created.
<b>Use application directory for offline cache</b>	Use the installation folder to save the offline cache file.
<b>Use legacy login method</b>	Can be used as a workaround if logging into Devolutions Account isn't working, but it is not recommended.

## OTHER OPTIONS - UI OPTIONS

OPTION	DESCRIPTION
<b>Always show "Go Offline" button</b>	Always display the "Go Offline" button in the status bar when <a href="#">Offline Mode</a> is active.
<b>Auto hide filter tree view</b>	Changes if the filter tree view will be hidden automatically or not. This is relevant if you have the navigation pane unpinned and do a filter.
<b>Disable custom images</b>	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.
<b>Disable favicon cache</b>	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.

OPTION	DESCRIPTION
<b>Disable layout restoration</b>	Disable manually configured tab layout and restore the layout settings on a RDM restart.
<b>Disable user gravatar</b>	Disable the fetching of the gravatar in the Administration - Users window to improve the application performance.
<b>Expand all tree nodes on select credential entry</b>	After creating a new credential entry, the tree nodes expands automatically.
<b>Hide last opened play list in play list management</b>	Hide the last opened play list at startup in the play list dialog.
<b>Hide loading data sources progress bar</b>	Will hide the loading data sources progress bar when loading.
<b>Use old entry sort</b>	Use the old entry sort from previous version of Remote Desktop Manager.
<b>Use vault image in tree view</b>	Use the vault image in the tree view's root.

## INFORMATION

OPTION	DESCRIPTION
<b>Created on</b>	Creation date of Remote Desktop Manager configuration folder.
<b>Source</b>	Source of Remote Desktop Manager configuration settings.

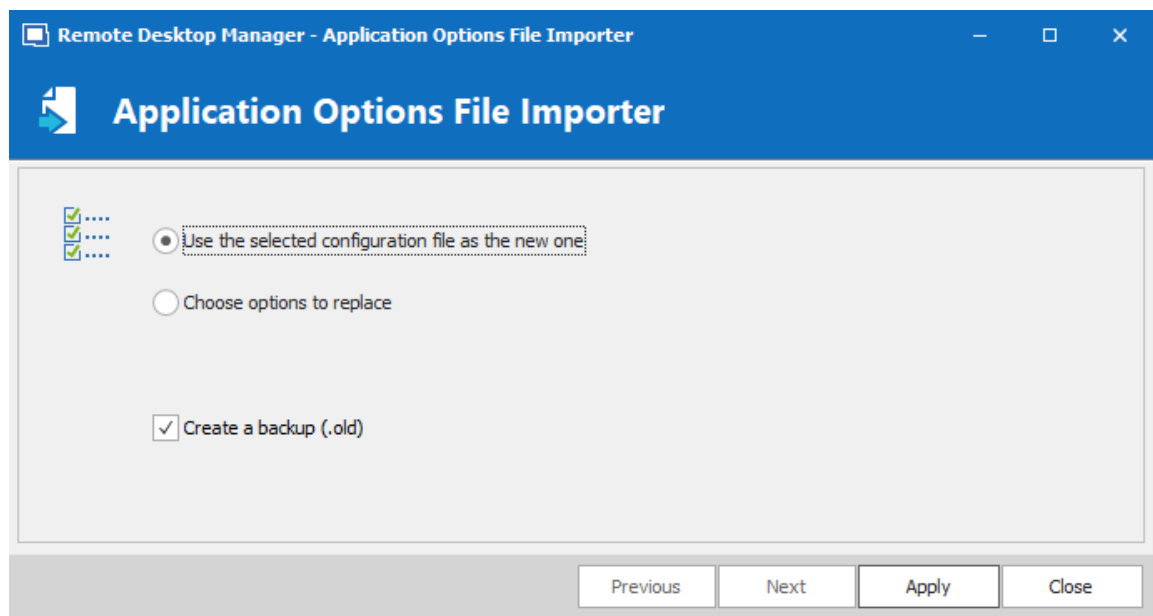
OPTION	DESCRIPTION
<b>Path</b>	Shortcut to access the configuration folder directly.

### 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

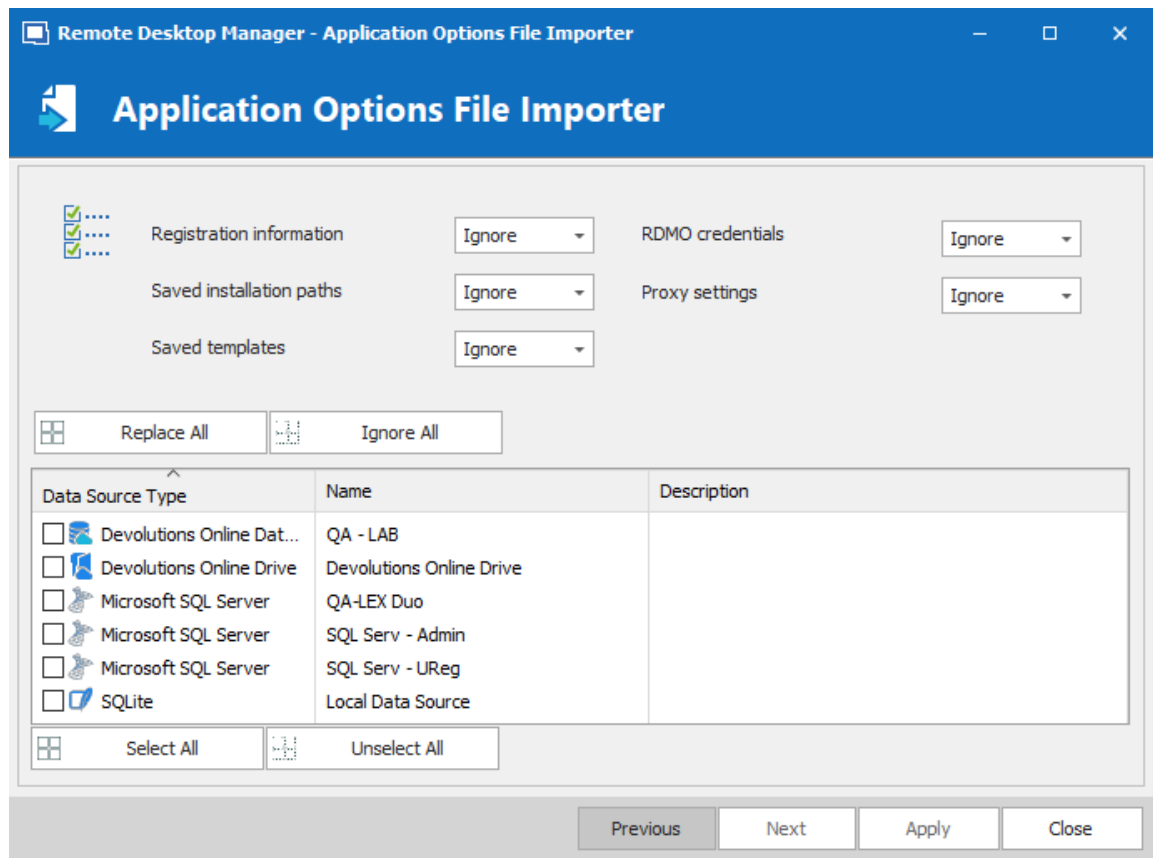


*Application Options File Importer*

OPTION	DESCRIPTION
<b>Use the selected configuration file as the new one</b>	Use the RemoteDesktopManager.cfg file as a new configuration file for your application.

OPTION	DESCRIPTION
<b>Choose options to replace</b>	Select which options to replace in your actual RemoteDesktopManager.cfg file. See below for more information.
<b>Create a backup (.old)</b>	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, including credentials set in your DODB.

Devolutions does not recommend sharing any credential to a team data source.

**Registration Information**

☒ Name

☐ Email

☒ Key

**Miscellaneous**

☒ Proxy settings ☒ Saved installation paths ☒ Saved templates ☒ Devolutions Account credentials

☒ Include data source credentials

Data Source Type	Name	Description
<input checked="" type="checkbox"/> Devolutions Online Dat...	QA - LAB	
<input checked="" type="checkbox"/> Devolutions Online Drive	Devolutions Online Drive	
<input checked="" type="checkbox"/> Microsoft SQL Server	QA-LEX Duo	
<input checked="" type="checkbox"/> Microsoft SQL Server	SQL Serv - Admin	
<input checked="" type="checkbox"/> Microsoft SQL Server	SQL Serv - UReg	
<input checked="" type="checkbox"/> SQLite	Local Data Source	

Select All Unselect All

Export Close

*Configuration file export dialog*

## SETTINGS

## REGISTRATION INFORMATION

OPTION	DESCRIPTION
<b>Name</b>	Company registration name.
<b>Email</b>	Registration email.
<b>Key</b>	Serial key.

## MISCELLANEOUS



The local templates may contain credentials, ensure you do not share the exported file.

OPTION	DESCRIPTION
<b>Proxy settings</b>	Includes your proxy settings.
<b>Saved installation paths</b>	Preserve your installation paths configured for the external application.
<b>Saved templates</b>	Include your local templates in the export.
<b>DODB Credentials</b>	Includes your Devolutions Online Database credentials.
<b>Include data source credentials</b>	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.

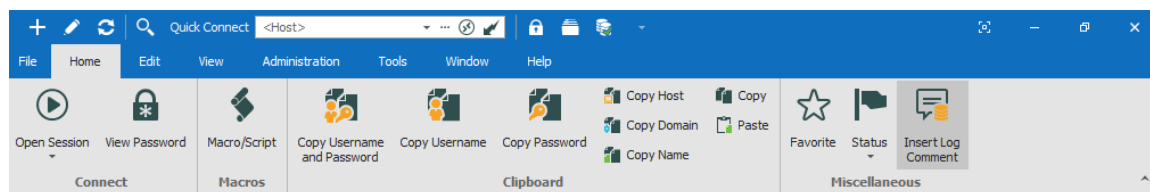
All your configured data sources will be displayed in this section. Select the one(s) that you want to include in the export. Please note that the content of the data source is not exported.

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*

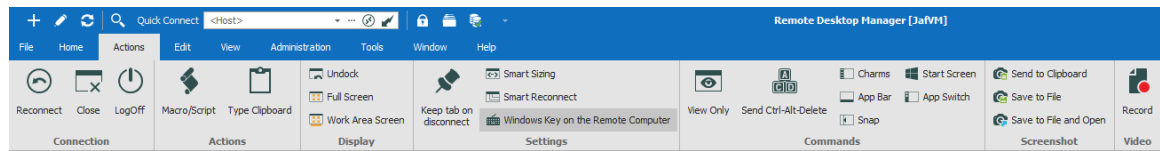
- Connect.
- Macros.
- Clipboard: Configure clipboard in **File – Options**.
- Miscellaneous.

## 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
<b>Reconnect</b>	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.
<b>Close</b>	Close the active session.
<b>LogOff</b>	Logoff the RDP session. See Logoff topic for more information.

## ACTIONS

Option	Description
<b>Execute</b>	Execute the selected macro or script in the previous window or in the current tab. This is only available when there is something to Execute.
<b>Macro/Script</b>	Displays a window where you can select a macro or script, as well as the execution options.
<b>Type Clipboard</b>	Send the content of the clipboard over to the opened session.

## DISPLAY

OPTION	DESCRIPTION
<b>Undock</b>	Undock your embedded session and move it anywhere outside Remote Desktop Manager or even on another monitor.
<b>Embedded</b>	Re-embed your session when your session is undocked. This option will only appear if your session is not already in an embedded mode.
<b>Full Screen</b>	Display your session in full screen outside Remote Desktop Manager.
<b>Work Area Screen</b>	This mode allows you to open the connection in full screen but to also have access to your local taskbar.

## SETTINGS

OPTION	DESCRIPTION
<b>Keep tab on disconnect</b>	Your session tab will stay after a session disconnect. For more information, see Keep Tab Opened topic.
<b>Smart Sizing</b>	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.
<b>Smart Reconnect</b>	Automatically reconnect your session with the most appropriate band.

OPTION	DESCRIPTION
<b>Windows Key on the Remote Computer</b>	When enabling <b>Windows key</b> , 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](#)
- [SSH Shell \(Rebex\)](#)
- [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.

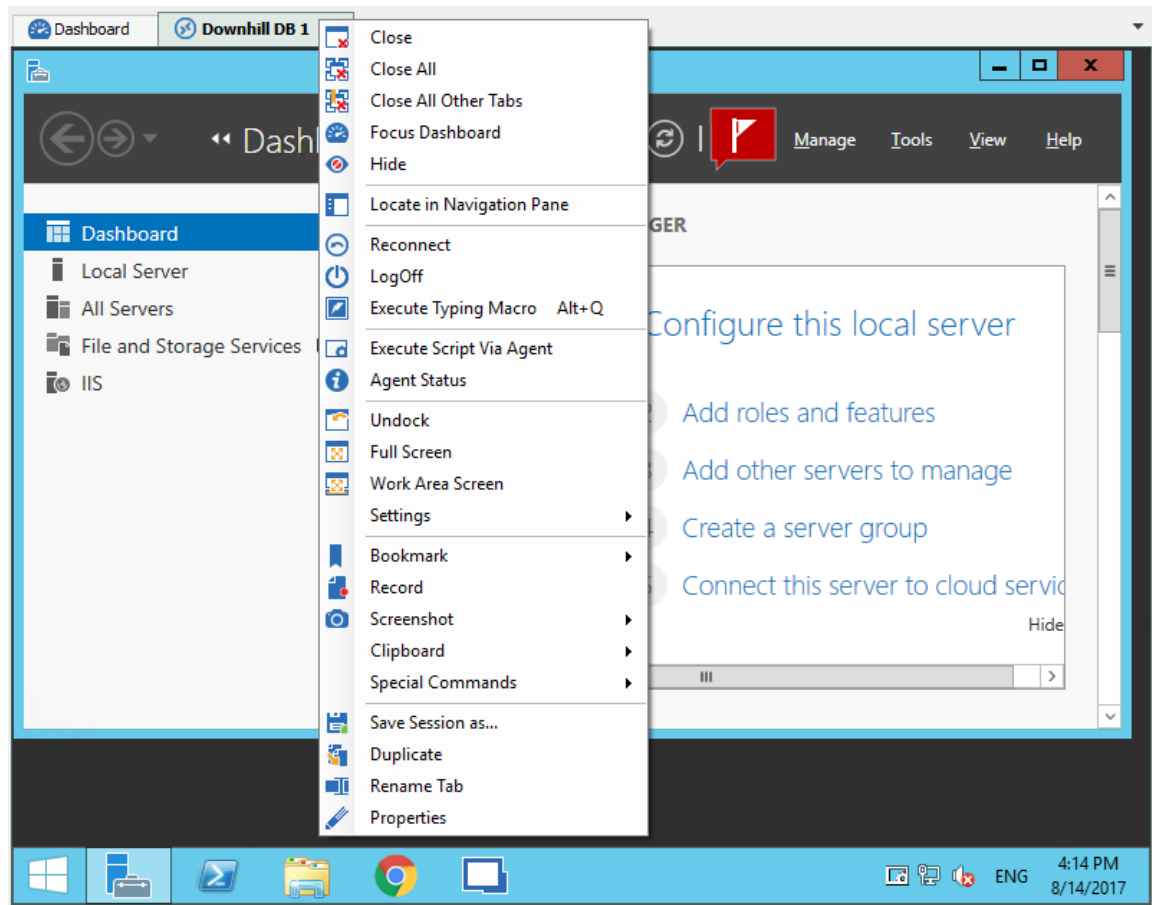
## SCREENSHOT

OPTION	DESCRIPTION
<b>Send to Clipboard</b>	Performs a typical capture to the clipboard.
<b>Save to File</b>	Prompts for a file name and saves the capture to that file.
<b>Save to File and Open</b>	Prompts for a file name and saves the capture to that file, then automatically open the file using your default editor.

## VIDEO

OPTION	DESCRIPTION
<b>Record</b>	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*

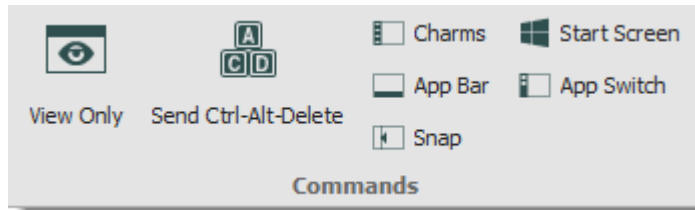
## 6.4.1 Commands

### 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
<b>View Only</b>	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.
<b>Send Ctrl+Alt+Delete</b>	Send the key combination CTRL+ALT+DELETE to the host.
<b>Charms</b>	On Windows 8 or Windows 2012 server, displays the Charms bar (Search, Share, Start, Devices, and Settings bar).
<b>App Bar</b>	On Windows 8 or Windows 2012 server, displays the App bar to show navigation, commands, and tools.
<b>Snap</b>	On Windows 8 or Windows 2012 server, allows you to run two applications side-by-side.

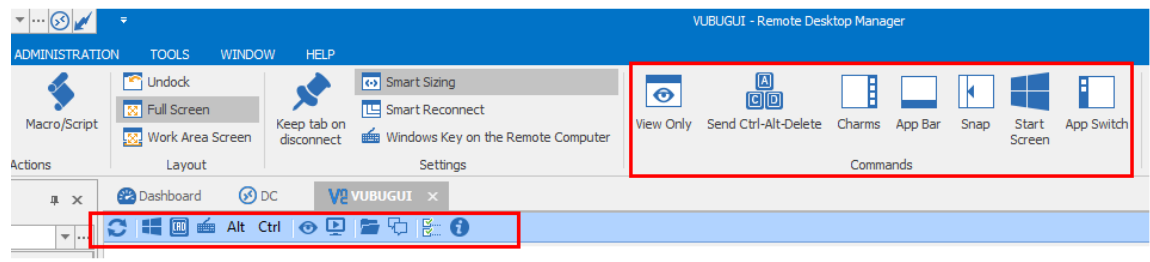
OPTION	DESCRIPTION
<b>Start Screen</b>	Open the Start menu on the host computer.
<b>App Switch</b>	On Windows 8 or Windows 2012 server, switches from an application to another.

#### 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
<b>Refresh Screen</b>	Refresh the host screen.
<b>Window Start Menu</b>	Open the Start menu on the host computer.
<b>Send Ctrl-Alt-Delete</b>	Send the key combination CTRL+ALT+DELETE to the host.

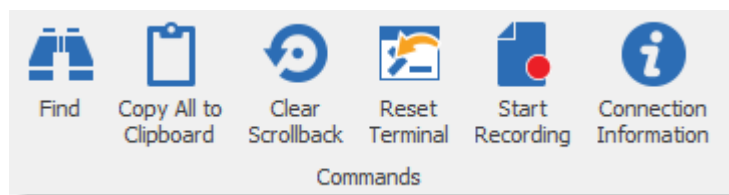
OPTION	DESCRIPTION
<b>Send Custom Keys</b>	Send custom keys combination to the host.
<b>Alt</b>	Send ALT to the host.
<b>Ctrl</b>	Send CTRL to the host.
<b>View only mode</b>	This will prevent the session from receiving any input from the keyboard or the mouse. This feature was requested to allow monitoring while preventing manipulation errors. Use it to have a read only access to the remote server.
<b>Remote input</b>	Keyboard and pointer events will be sent to the server and the local and remote clipboard will be synchronized.
<b>Open file transfer</b>	Open the file transfer with the host computer.
<b>Open chat dialog</b>	Open a chat dialog with the host computer.
<b>Options</b>	Open the Connection Options window.
<b>Information</b>	Open the window containing information regarding your VNC connection status and traffic.

#### 6.4.1.3 SSH Shell (Rebex)

### DESCRIPTION

The commands for a SSH Shell session allows you to send remote commands to your host.

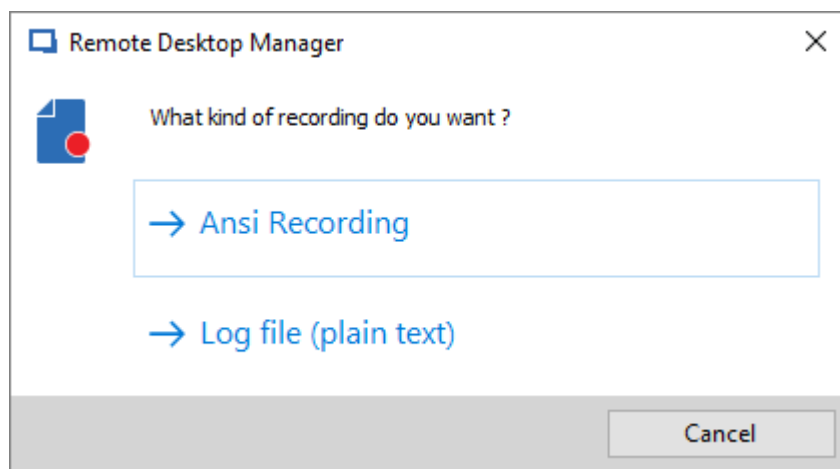




*Actions – SSH Shell (Rebex) Commands*

OPTION	DESCRIPTION
<b>Find</b>	Open a find window to search for a specific word.
<b>Copy All to Clipboard</b>	Copy all selected text to the Clipboard.
<b>Clear Scrollback</b>	Clear the scrolling display that precedes the current line.
<b>Reset Terminal</b>	Reset host terminal connection.

## START RECORDING

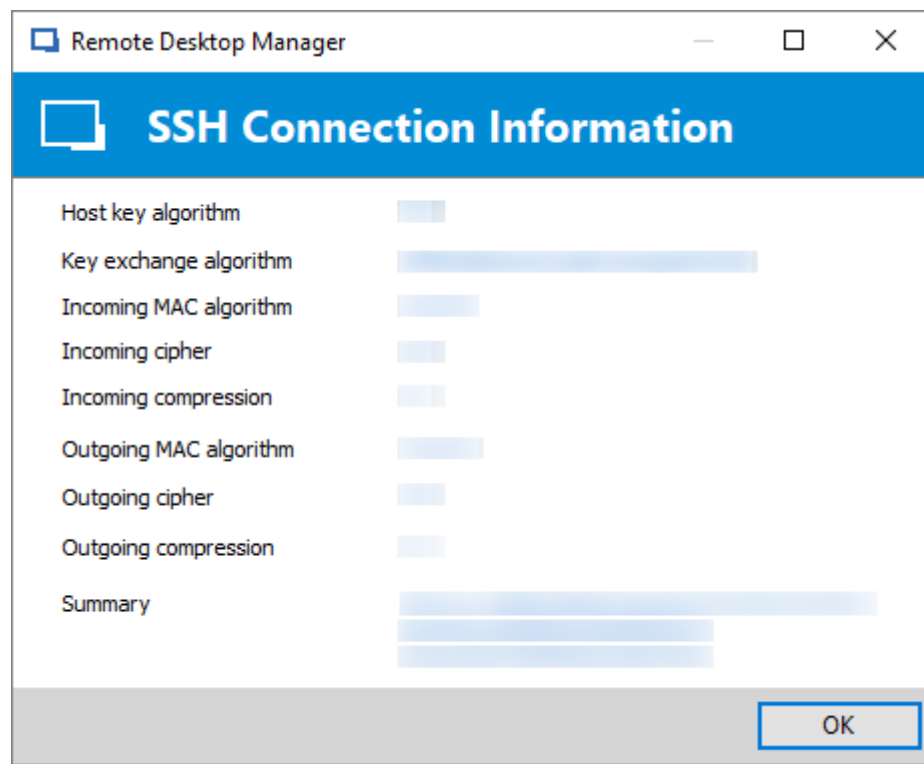


*Recording type*

OPTION	DESCRIPTION
<b>Ansi Recording</b>	Record all of the activity in the SSH session using the Ansi format. This can be replayed like a video using <b>Tools - Tools - Terminal playback (Ansi)</b> .
<b>Log file (plain text)</b>	Record all of the activity in the SSH Shell (Rebex) session using a text format.

## CONNECTION INFORMATION

Provides connection host information in a form as shown below.



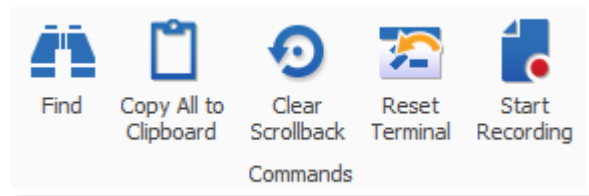
SSH Connection Information

### 6.4.1.4 Telnet

## DESCRIPTION

The actions for a Telnet session allows you to send remote commands to your host.

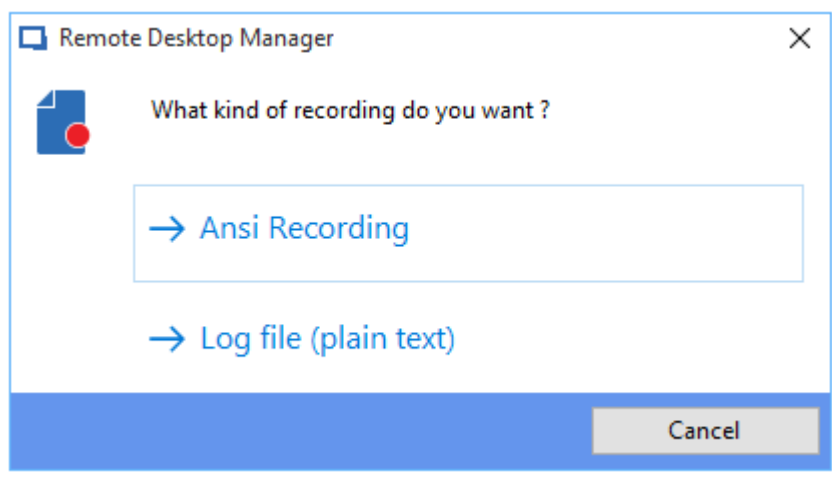
## SETTINGS



### *Telnet Commands Actions*

OPTION	DESCRIPTION
<b>Find</b>	Open a find window to search for specific words.
<b>Copy All to Clipboard</b>	Copy all selected text to the Clipboard.
<b>Clear Scrollback</b>	Clear the scrolling display that precedes the current line.
<b>Reset Terminal</b>	Reset host terminal connection.

## START RECORDING

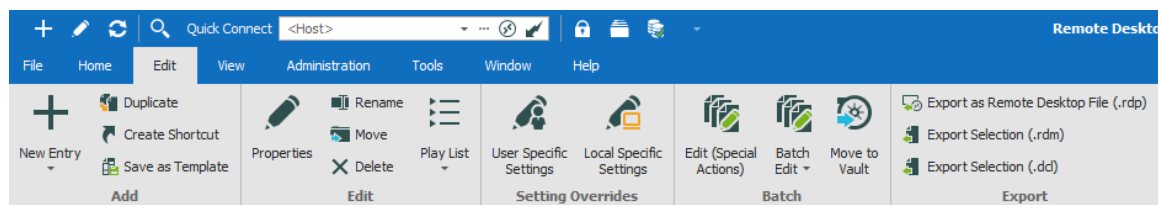


OPTION	DESCRIPTION
<b>Ansi Recording</b>	Will record all of the activity in the SSH session using the Ansi format. This can be replayed like a video using <b>Tools - Tools - Terminal playback (Ansi)</b> .
<b>Log file (plain text)</b>	Will record all of the activity in the SSH session using a text format.

## 6.5 Edit

### DESCRIPTION

The **Edit** tab contains operations to quickly Add, Edit, Overrides, Batch Edit or Export entries.



Ribbon - Edit

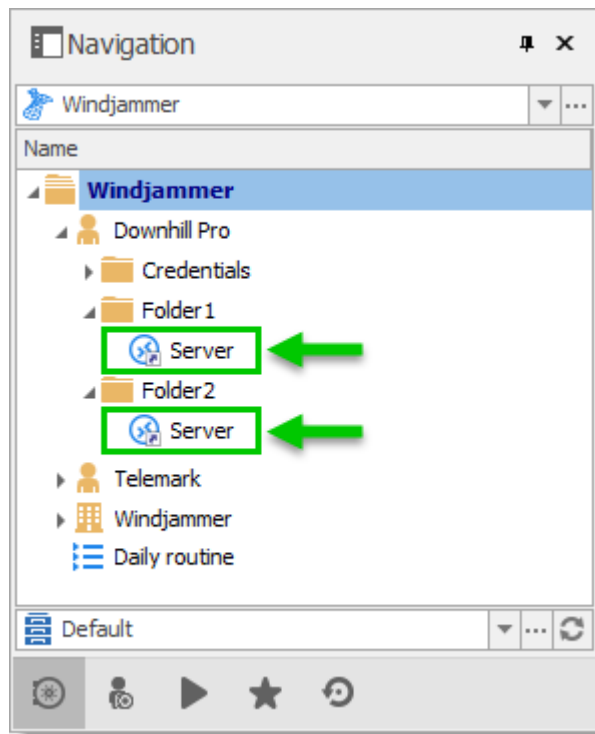
### ADD

OPTION	DESCRIPTION
<b>New Entry</b>	Create a new entry (session, folder, information entry, credentials, etc.).
<b>Duplicate</b>	Create a duplicate of your entry.
<b>Create Shortcut</b>	Link your entry to more than one group. For more information, consult the text below.
<b>Save as Template</b>	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
<b>Properties</b>	Edit the properties of the selected entry.

OPTION	DESCRIPTION
<b>Rename</b>	Rename the selected entry.
<b>Move</b>	Move the selected entry to another folder.
<b>Delete</b>	Delete the selected entry. A confirmation dialog is displayed to confirm the action.
<b>Play List</b>	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](#)

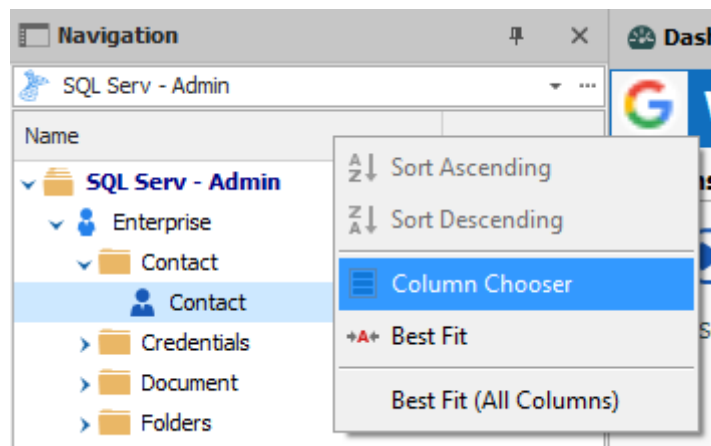
## SETTING OVERRIDES

OPTION	DESCRIPTION
<b>User Specific Settings</b>	Override properties of the selected entry with settings with settings specific to the current user. For more information, please consult the <a href="#">Specific Settings</a> topic.

OPTION	DESCRIPTION
<b>Local Specific Settings</b>	Override properties of the selected entry with settings specific to the local machine. For more information, please consult the <a href="#">Specific Settings</a> 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
<b>Edit (Special Actions)</b>	Perform special actions on the selected entries, such as change the type, run a script, and more. For more information, please consult the <a href="#">Batch Actions Samples</a> .
<b>Batch Edit</b>	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 <a href="#">Batch Edit</a> topic.
<b>Move to Vault</b>	Transfer the selected entries to another Vault in the database.

## EXPORT

OPTION	DESCRIPTION
<b>Export Entry as Remote Desktop File (.rdp)</b>	Export the selected entries in a Remote Desktop File (.rdp) format.
<b>Export Selection (.rdm)</b>	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 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.

## CHECKOUT SYSTEM OVERVIEW

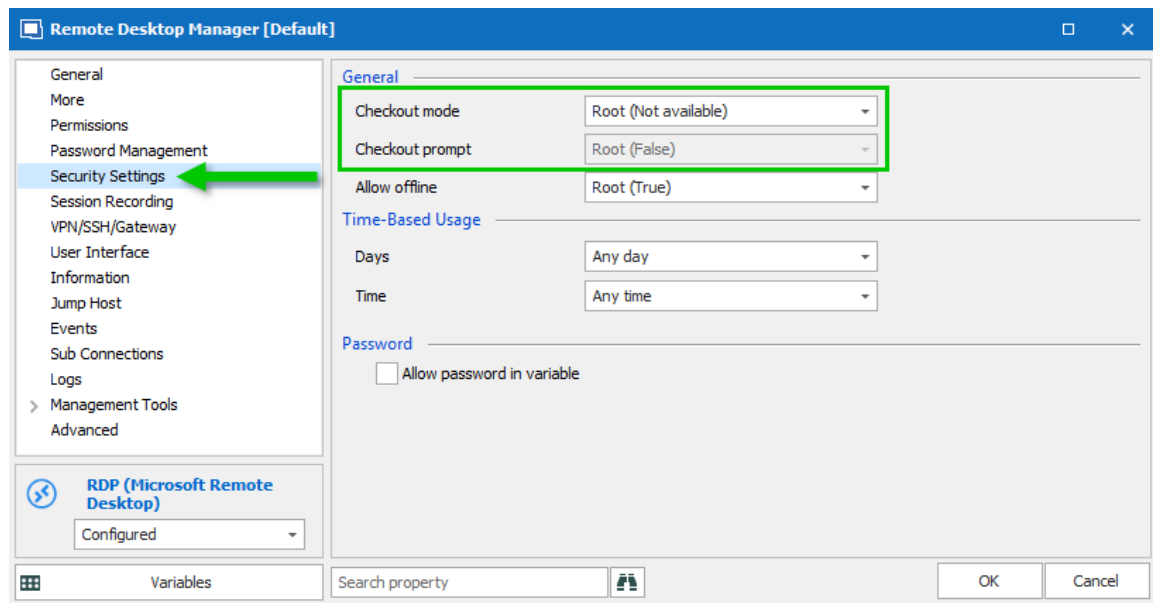
*Learn more about checkout modes and setting check out on the Vault and folders*

## USE MANUAL CHECKOUT MODE

*Configure Manual mode and avoid some common mistakes*

## SETTINGS

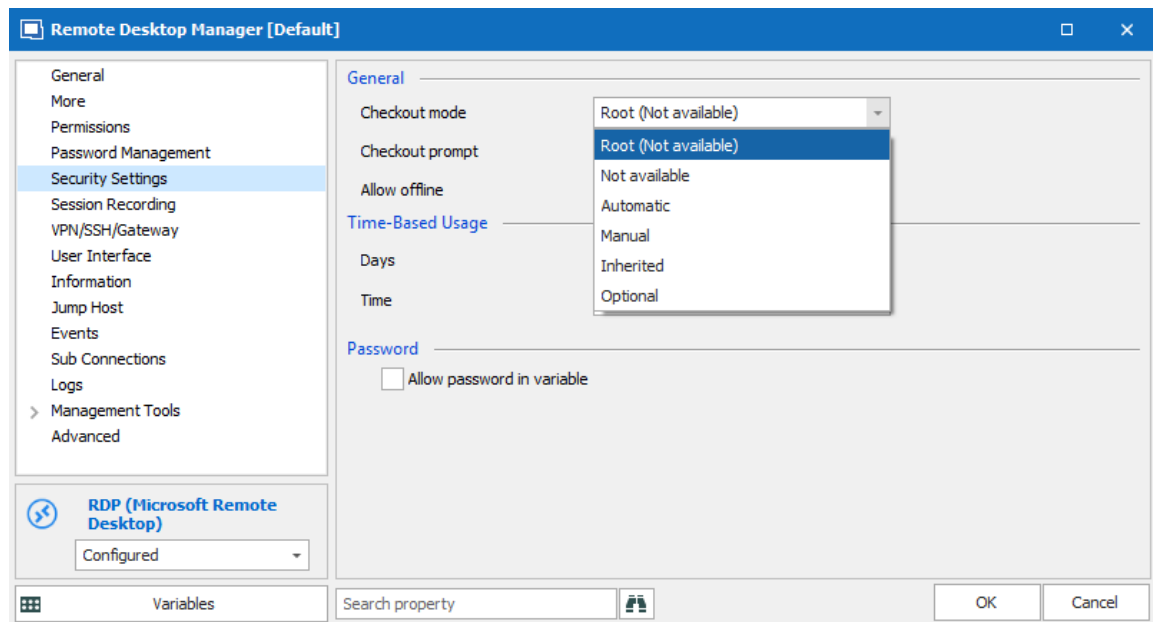
To access the check out system, edit an entry that supports checkout, and navigate to the **Security** section.



*Entry properties – Security – Checkout settings*

## CHECKOUT MODE

**Checkout mode** enables or disables the checkout system. It also decides how the checkout mode functions.

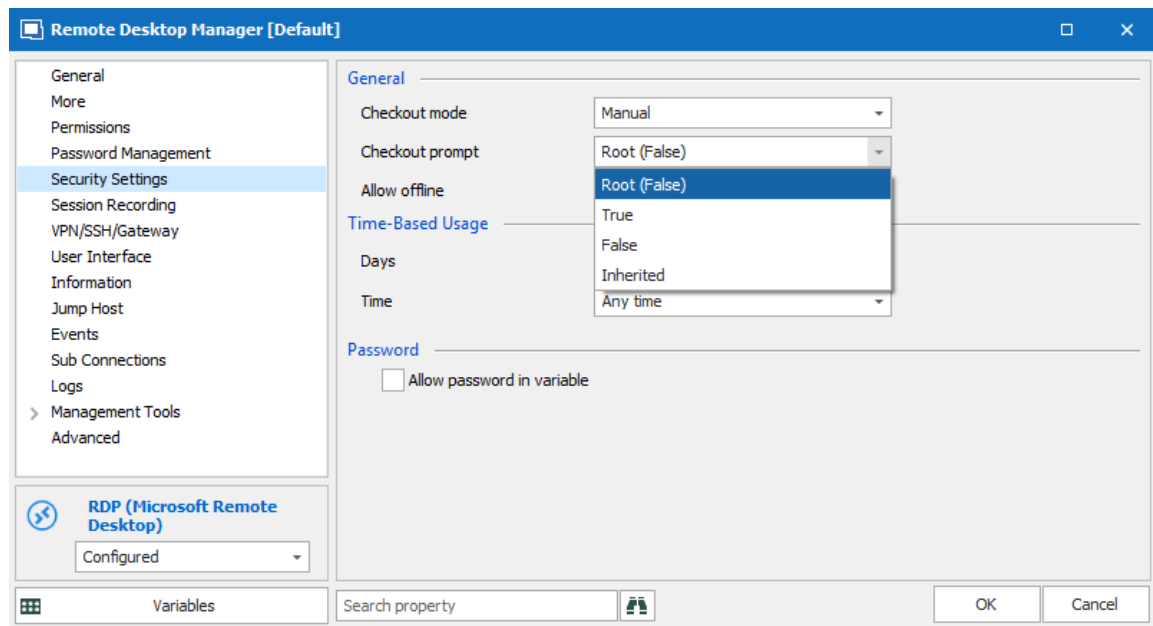


*Checkout mode*

OPTION	DESCRIPTION
<b>Root</b>	Inherits the checkout mode setting from the root folder.
<b>Not available</b>	Disables the checkout system.
<b>Automatic</b>	Checks out an entry automatically when the entry is opened and automatically checks the entry in when the entry is closed. User can edit properties without checking out the entry.
<b>Manual</b>	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.
<b>Inherited</b>	Inherits the check out mode from the parent folder.
<b>Optional</b>	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 Activity Logs.



*Checkout required*

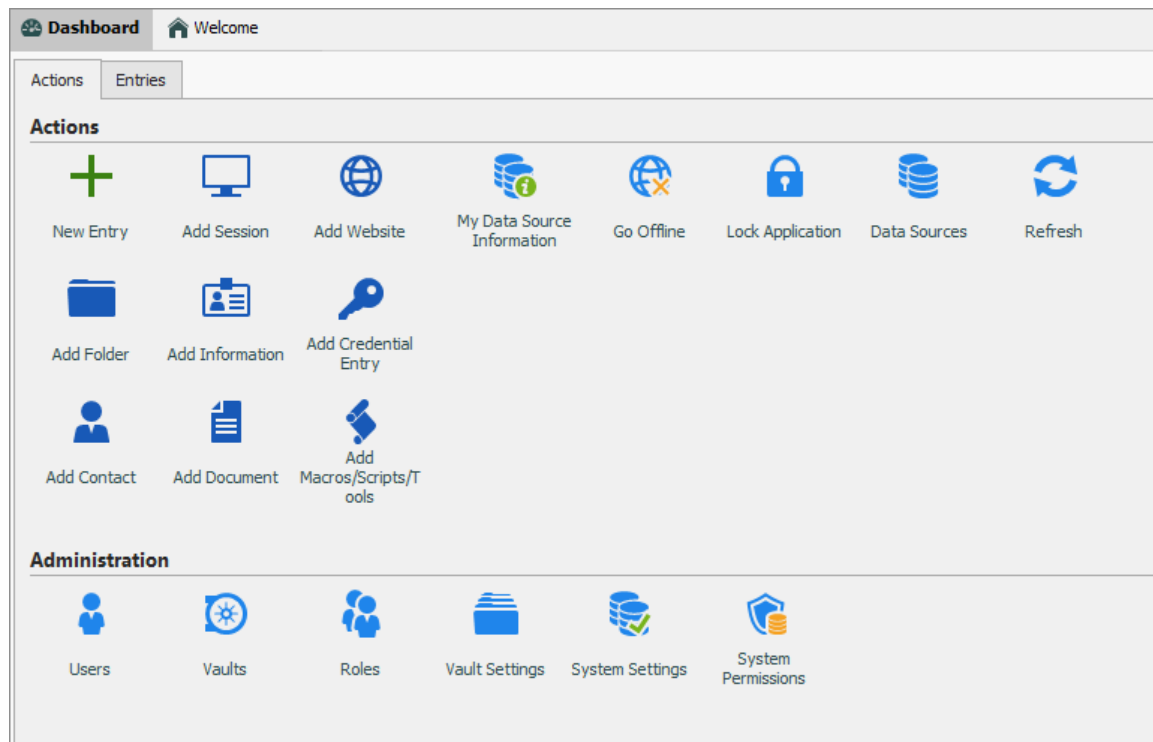
OPTION	DESCRIPTION
<b>Root</b>	Uses the checkout prompt setting from the root folder.
<b>True</b>	Prompts the user for comment when they checkout an entry.
<b>False</b>	Removes the prompt for comment.
<b>Inherited</b>	Inherits the setting from a parent folder.

## VAULT SETTINGS

The checkout system **Vault** refer to the settings in the Vault folder.

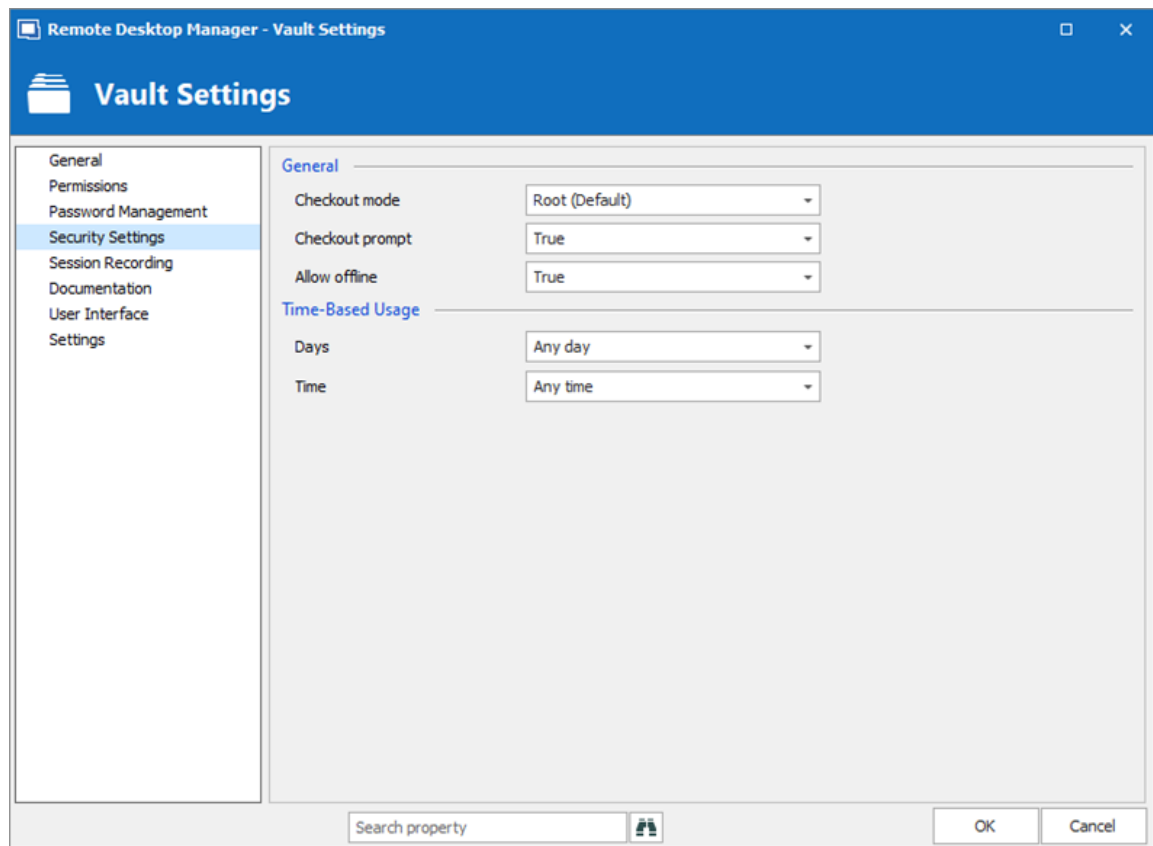
To set the checkout system Vault settings:

1. Select the Vault folder in the navigation pane.
2. Click on the Vault Settings button in the Dashboard.



*Access the Vault Settings*

3. In the Vault settings, navigate to the Security section.



*Checkout system - Vault Folder*

### 6.5.1.2 Credential Redirection

## DESCRIPTION

Some tools do not provide an Application Programming Interface (API) or support command line parameters to interact with them. 1Password, Firefox Password Manager, Google Password Manager and LastPass are such tools.

In order to leave the credentials in the external tool, and be able to use these credentials with Remote Desktop Manager, we have implemented a mechanism to request the credentials from the tool, then redirect them to a chosen resource.

This is achieved by running a local-access only applicative web server, then displaying a page that will allow you to store the credentials in your Credential repository. Remote Desktop Manager redirects the credentials from your chosen repository to the remote resource.

## PRE-REQUISITES

- The tool must be installed on your computer or used with a web browser as an extension.
- The browser extension for your Credential repository must be installed and enabled. Follow your repository documentation for details (see [below](#) for the URLs that are currently valid).

## PROCEDURE

There are three steps:

1. Create the credential entry.
2. Use a link to these credentials in a Remote Desktop Manager entry.
3. Open the session and use your provider to fill in the credentials.

We will use LastPass in our example, but the steps are the same for 1Password.

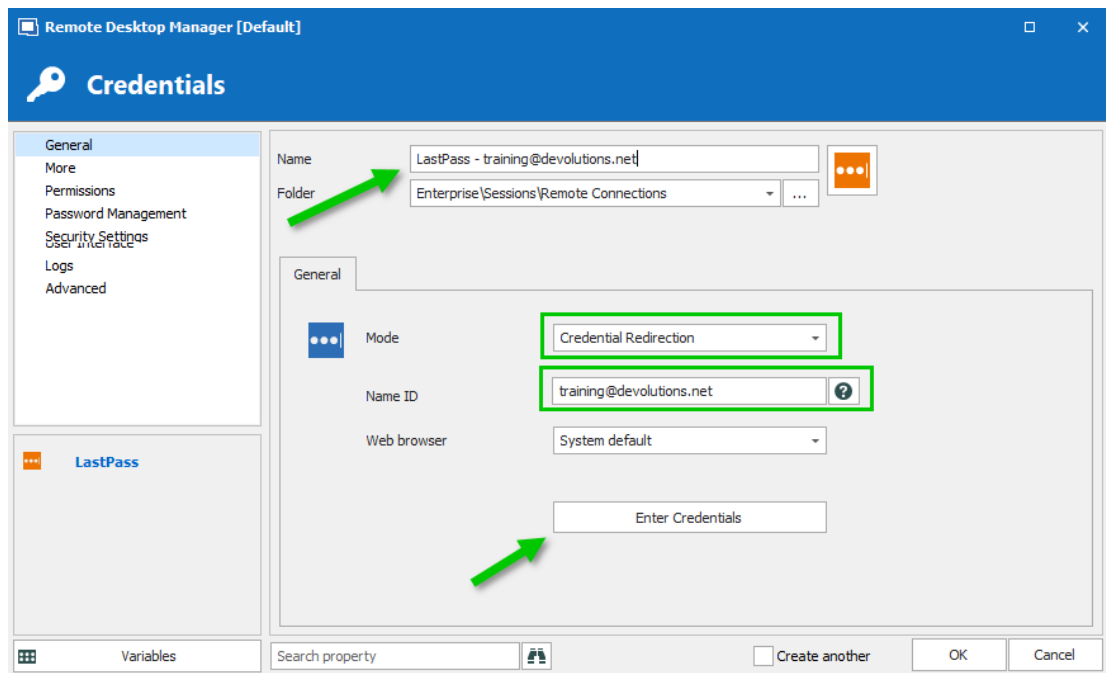


Your chosen tool may require to be unlocked once or multiple times depending on your configuration. These steps are not covered by this guide as it may change for each installation.

## CREATING THE CREDENTIAL ENTRY

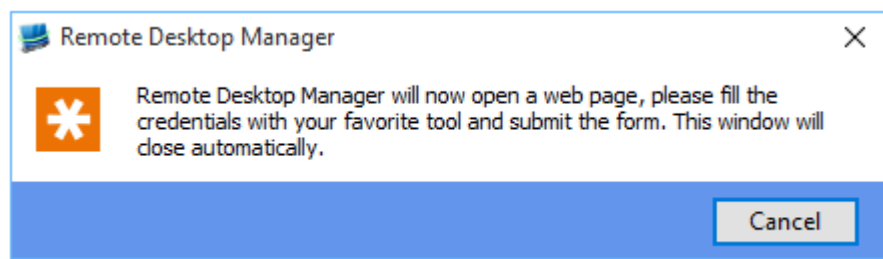
1. Create a new **LastPass** entry.
2. Enter a name for your LastPass entry.
3. Select the option Credential redirection.
4. Enter a **Name ID** (case sensitive). This must be unique within your LastPass repository. It will be used to identify the credentials and will be exposed as a subdirectory of the URL used to intercept the credentials.





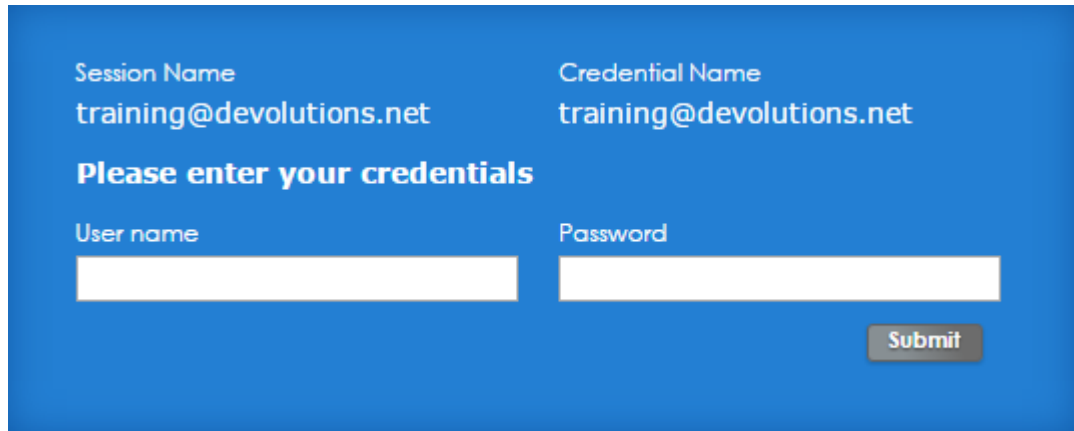
*LastPass credential*

5. Optionally select a specific browser, or use the default one.
6. Press the Enter Credentials button. This will launch the following sequence of events.
7. Remote Desktop Manager displays the following dialog.



*RDM - LastPass*

8. The chosen browser is launched for a URL that looks like `http://127.0.0.1:8000/training@devolutions.net/login.aspx`. Notice the middle part is the **Name ID** entered previously.
9. Enter your credentials to save in the browser



Session Name  
training@devolutions.net

Credential Name  
training@devolutions.net

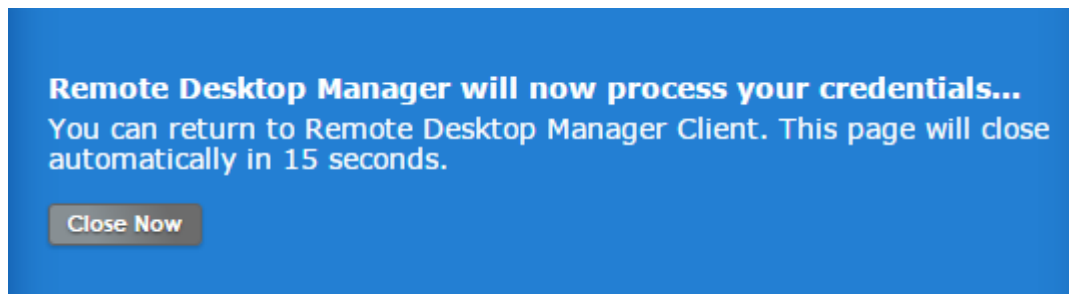
**Please enter your credentials**

User name

Password

Submit

10. Depending on the configuration of your provider, you have to press a keyboard combination, or press on a button for the tool to save the credentials. Please refer to the documentation of your tool for more information.



**Remote Desktop Manager will now process your credentials...**  
You can return to Remote Desktop Manager Client. This page will close automatically in 15 seconds.

Close Now

11. In Remote Desktop Manager, save your credential entry.

12. Using your password provider, confirm that the credentials are saved.

## CREATING A SESSION USING THE CREDENTIAL ENTRY

1. Create a new entry, we will use an RDP session for the example.

2. Enter a name for your RDP session.

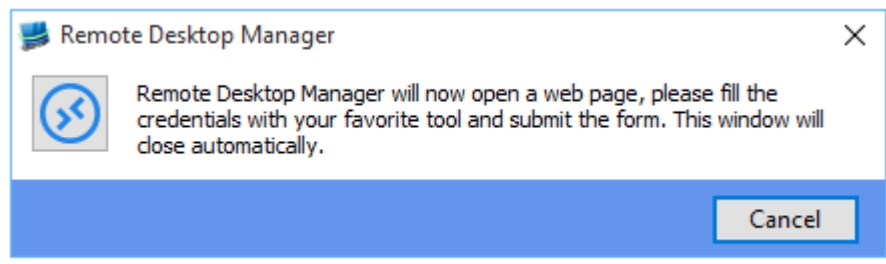
3. For **Credentials** select **Credential repository** and then your newly created credential entry

*Credential repository*

## USING THE SESSION

Select your session then launch it. This will initiate the following sequence of events:

1. Remote Desktop Manager will display this informative dialog



2. The chosen browser is launched with the URL associated to the session
3. Depending on your configuration, the credentials are entered automatically, or you have to press a key combination to initiate your tool. Please refer to the documentation of your tool for more information.

4. In the web browser, press submit. The page will be closed after a delay

5. The RDP session is launched and authentication is successful

## SEE ALSO

Lastpass downloads: [https://lastpass.com/misc\\_download2.php](https://lastpass.com/misc_download2.php)

1Password instructions: <https://support.1password.com/browser-extension/>

### 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**
- **AuthAnvil Password Server**
- **Bitwarden**
- **Dashlane**
- **Devolutions Password Hub**
- **Devolutions Server**
- **KeePass**
- **Keeper**
- **LastPass**
- **Mateso Password Safe**

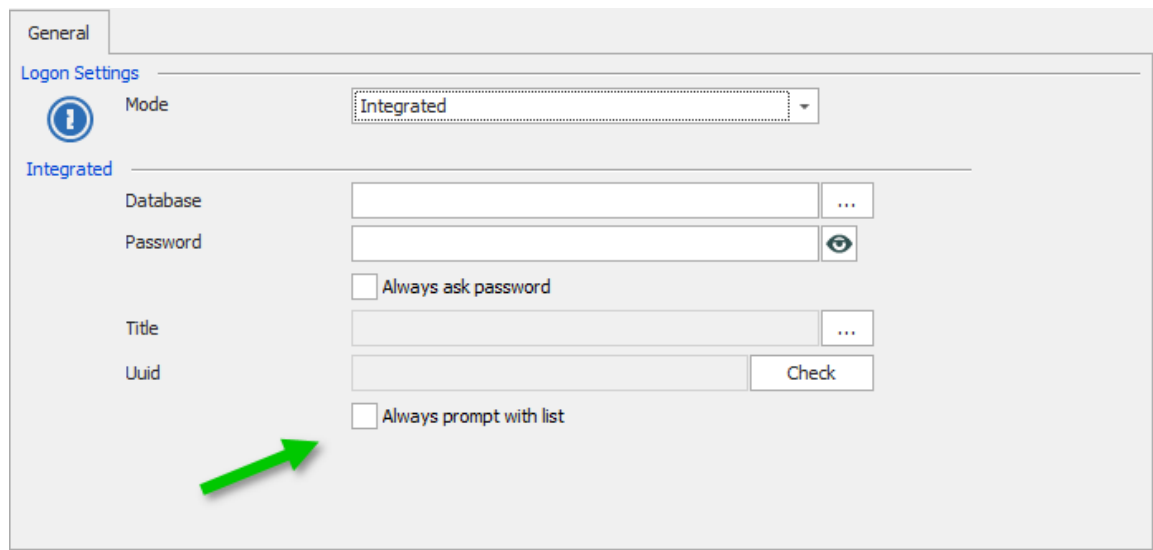
- PassPortal
- Password List
- Password Manager Pro
- Password Safe
- PasswordState
- Password Vault Manager
- Pleasant Password Server
- RoboForm
- Secret Server
- Sticky Password
- TeamPass
- True Key
- Zoho Vault



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**.



General

Logon Settings

Mode: Integrated

Integrated

Database: ...

Password: ...

☐ Always ask password

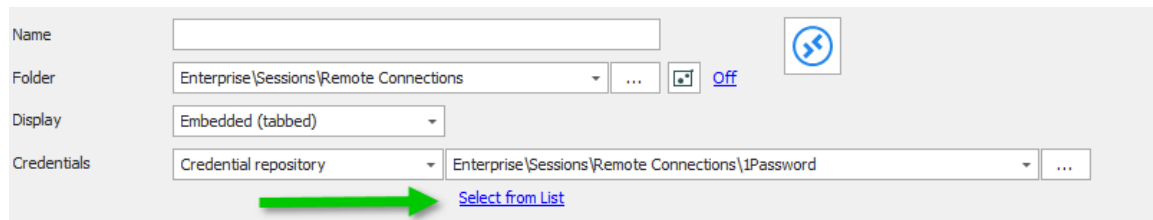
Title: ...

Uuid: ... Check

☐ Always prompt with list

*1Password Settings*

- 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.



Name: ...

Folder: Enterprise\Sessions\Remote Connections ... Off

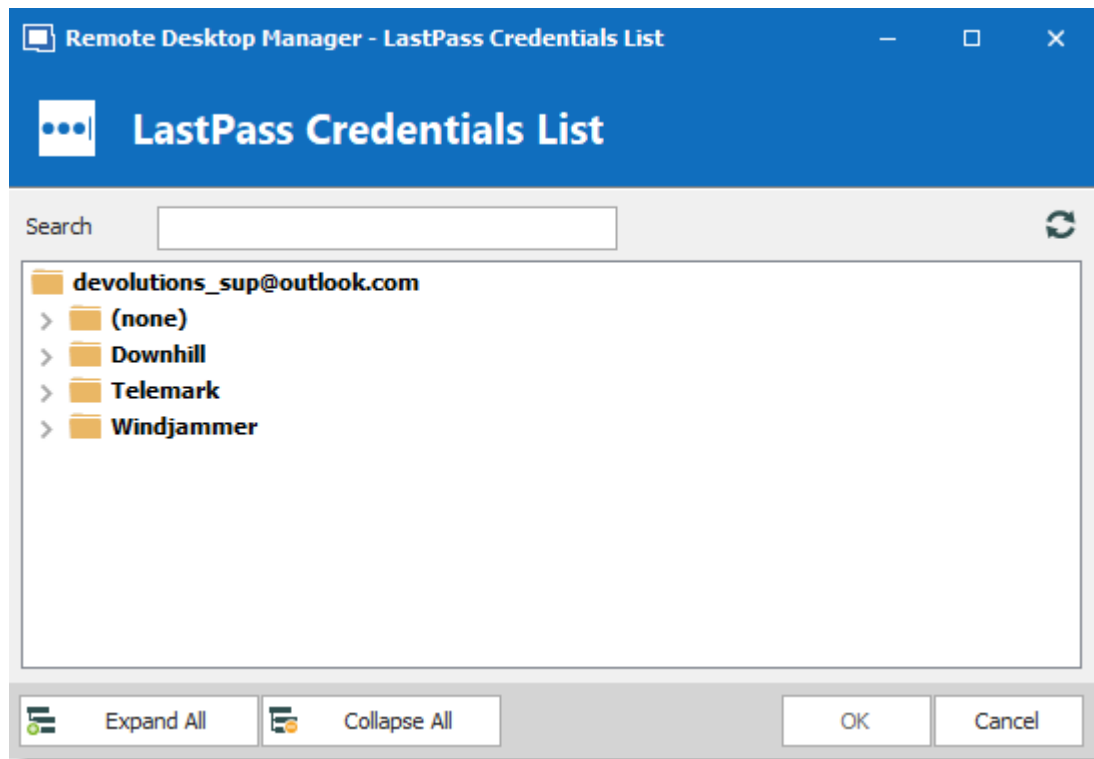
Display: Embedded (tabbed)

Credentials: Credential repository Enterprise\Sessions\Remote Connections\1Password ...

[Select from List](#)

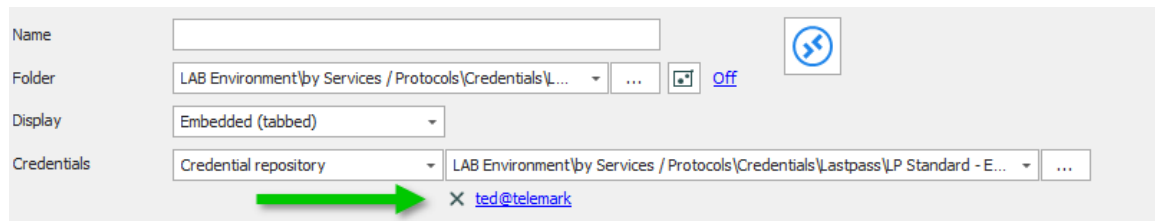
*Select from List*

- 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".

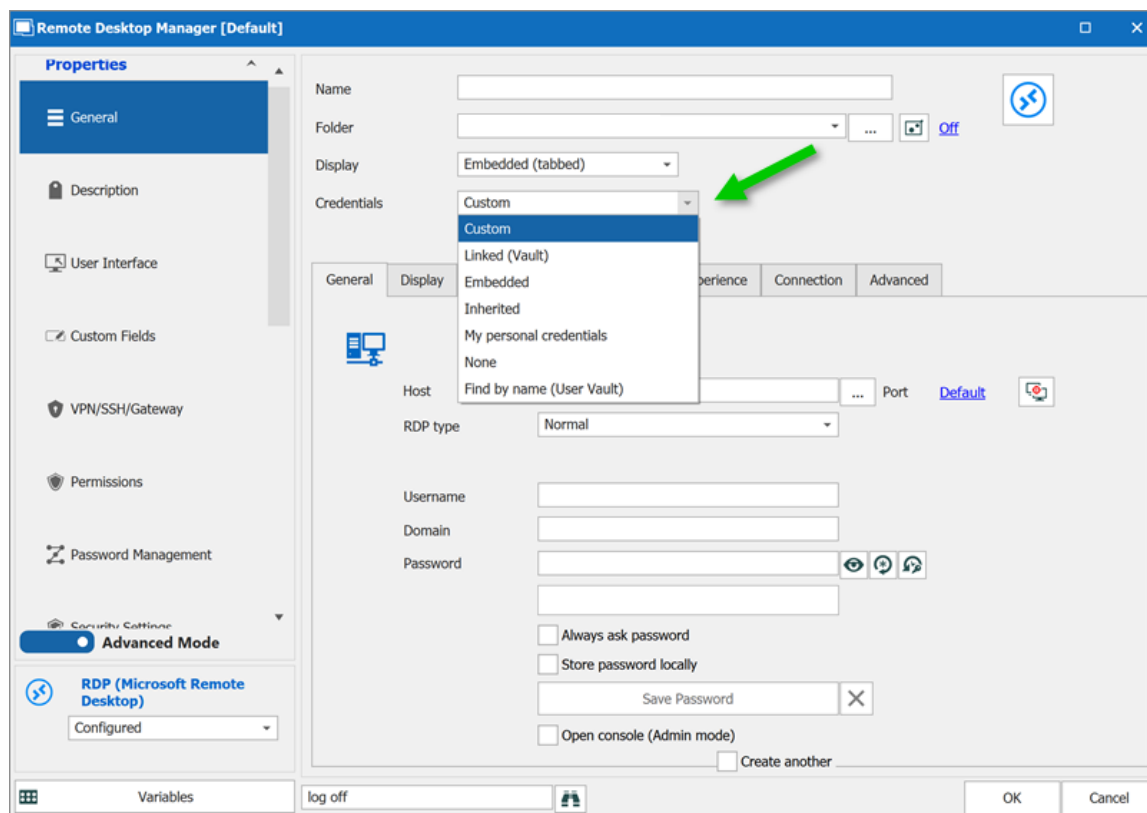


*Name of the credential*

#### 6.5.1.4 Entry Credentials Options

## DESCRIPTION

Multiple options are available to use for **Credentials** in your Remote Desktop Manager entries.



OPTION	DESCRIPTION
<b>Custom</b>	This option allows to enter custom credentials in the <b>General</b> section of the entry.
<b>Linked (Vault)</b>	Link your entry to use an existing <b>Credential</b> entry in the same vault.
<b>Embedded</b>	You can embed a specific <b>Credential</b> entry that would require, for example, specific information than just using the <b>Custom</b> option available in the entry itself.
<b>Inherited</b>	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.
<b>My personal credentials</b>	Will use the credentials set in <a href="#">My personal credentials</a> feature. This allows you to centralize one credential to



OPTION	DESCRIPTION
	replace or emulate the ones for your Windows session.
<b>None</b>	No credentials will be allowed to be saved or linked to this entry.
<b>Find by name (User Vault)</b>	Will search your <b>User Vault</b> for the name specified. If the box is left empty, when launch, a <b>Credential list</b> will open with all available <b>Credentials</b> entry from your <b>User Vault</b> .

## 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

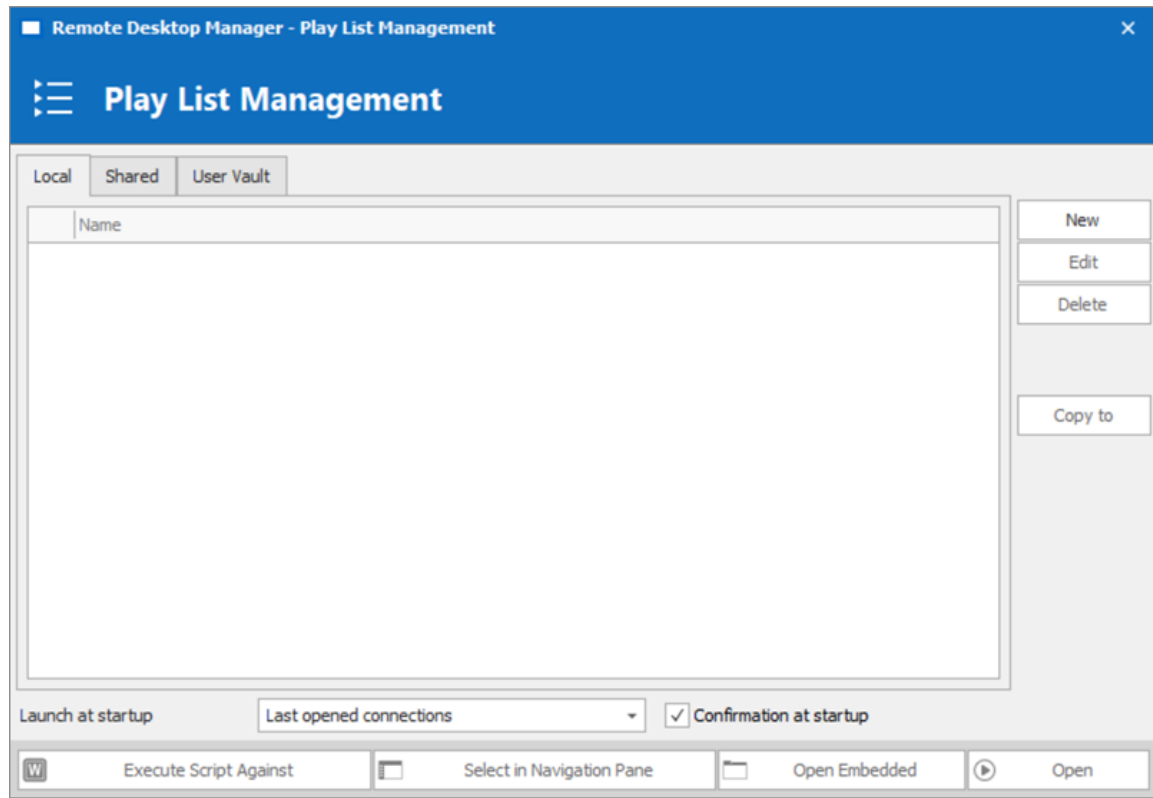


You can also use the context menu to create and edit your **Play List**. When your entries are selected, **right-click** in the Navigation Pane and select **Play List – Create Play List** or **Add to Play List**.

## SETTINGS

## USE THE PLAY LIST MANAGEMENT

You can access this by selecting Play List Management in the ribbon.



*Local Play List*

Play lists can be saved three different ways:

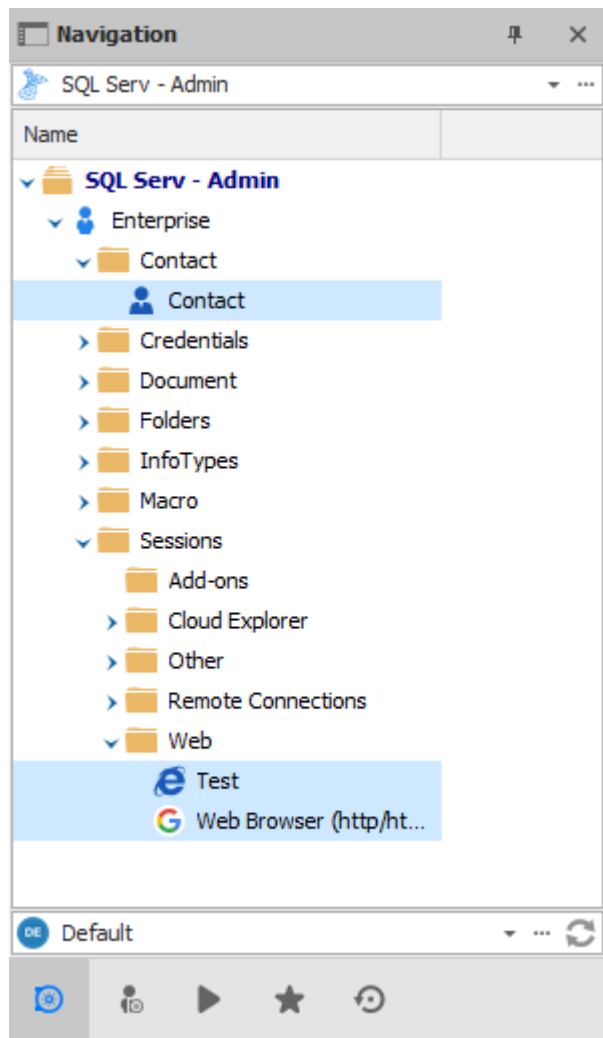
OPTION	DESCRIPTION
<b>Local</b>	The Play List is saved locally and can only be accessed as such. These can only be launched through the Play List Management.
<b>Shared</b>	The Play List is saved in the database. It can be accessed by anyone on the data source. These can be launched through the Play List Management or by using the entry itself.

OPTION	DESCRIPTION
<b>User Vault</b>	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

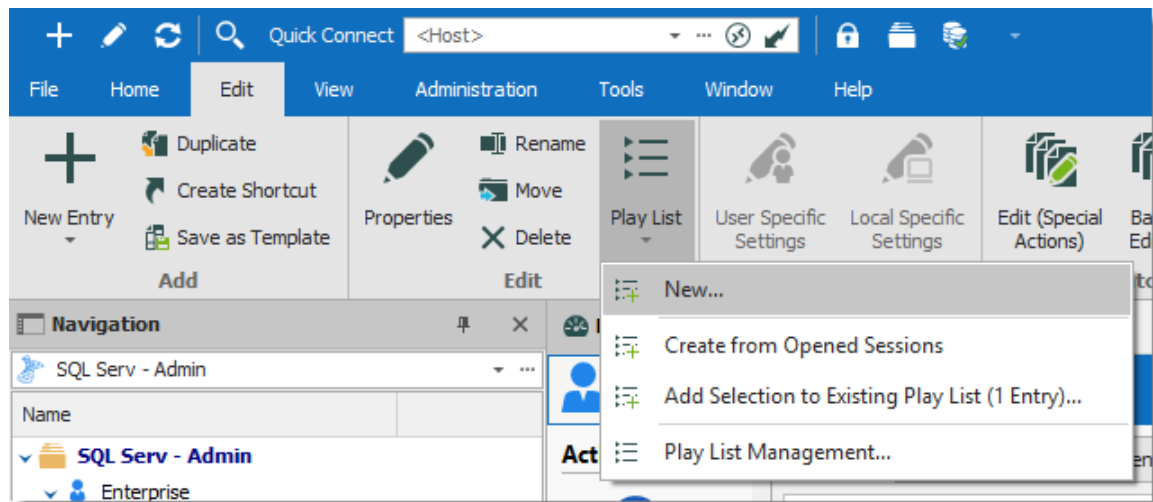
### CREATE PLAY LIST DEPENDING ON ENTRIES STATE AND SELECTION

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*

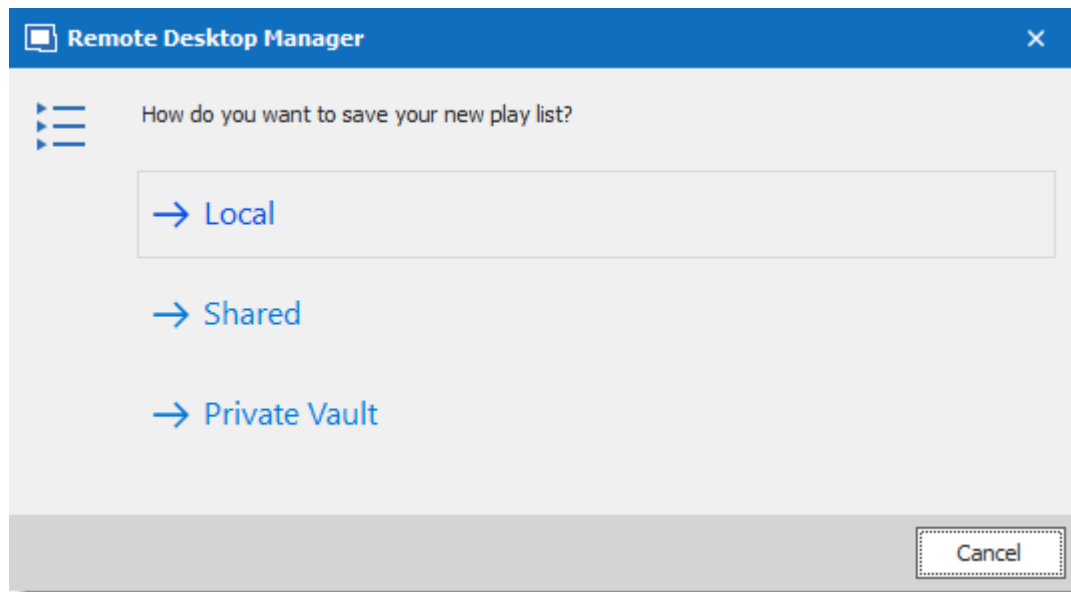
2. On the **Edit** ribbon menu, click **Play List**, then select whichever setting you prefer.



*Edit - Play List - New*

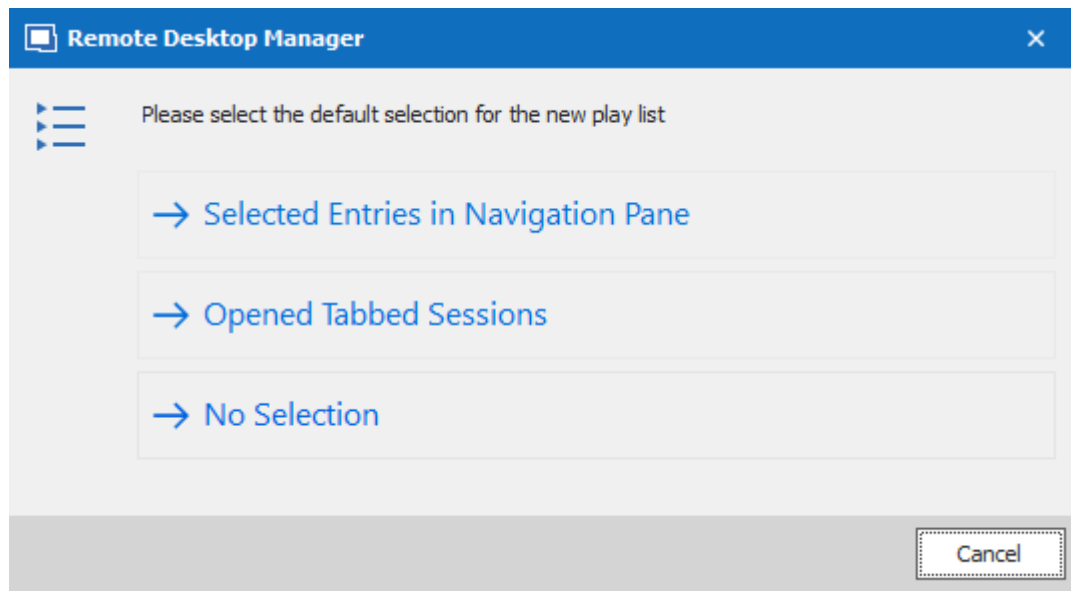
OPTION	DESCRIPTION
<b>New</b>	Creates a new Play List directly, a window prompt will ask you where you wish to save it and which selection you would like to highlight.
<b>Create from Opened Sessions</b>	Brings up the window for creating a new Play List with all currently opened session already selected for the Play List. You can select and remove additional entries if desired.
<b>Add Selection to Existing Play List (X Entry)</b>	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*

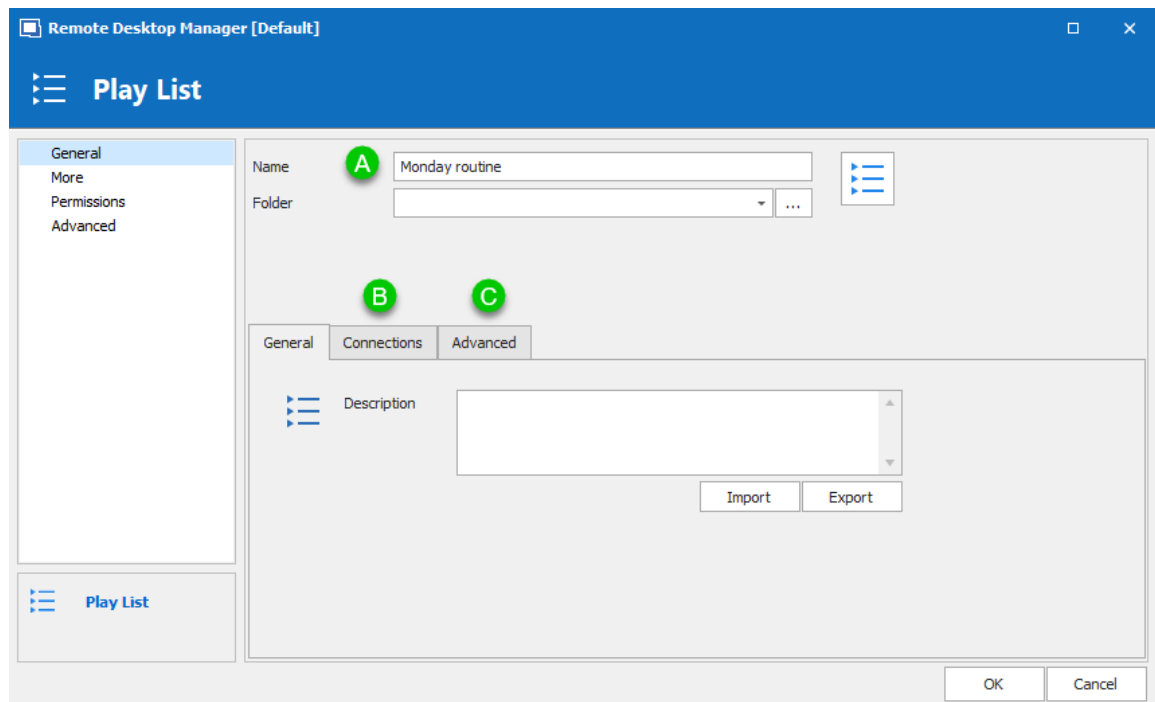
4. The next window lets you choose how you want your current selection or opened sessions to affect your playlist.



*Selected Entries in Navigation Pane*

OPTION	DESCRIPTION
<b>Selected Entries in Navigation Pane</b>	All currently selected entries in the Navigation Pane will already be selected for your Play List. You can still add and remove entries to the Play List if you desire.
<b>Opened Tabbed Sessions</b>	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.
<b>No Selection</b>	No pre-determined selection will be taken into account, create your Play List from a fresh start.

5. 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.

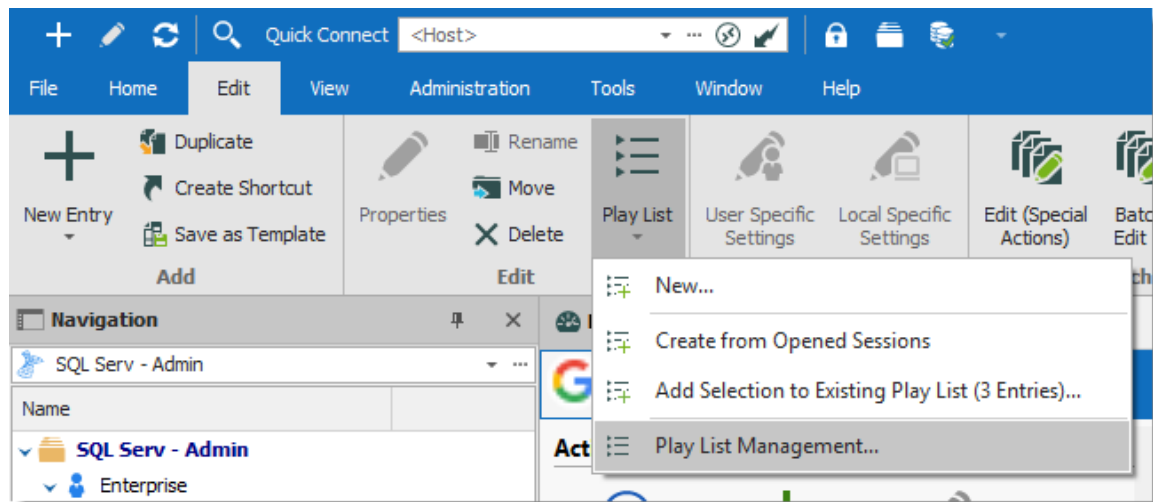


*Play List Editor*

And there you have it, your Play List is ready for use.

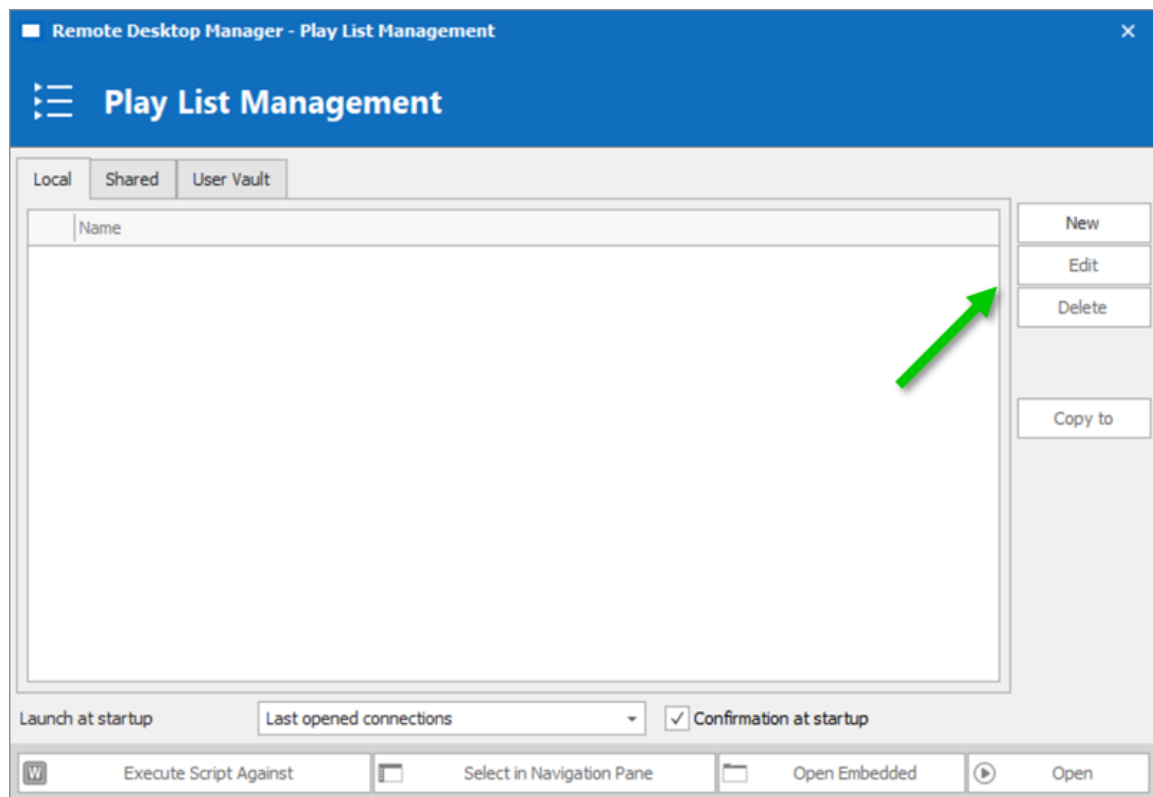
## EDIT EXISTING PLAY LIST

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.

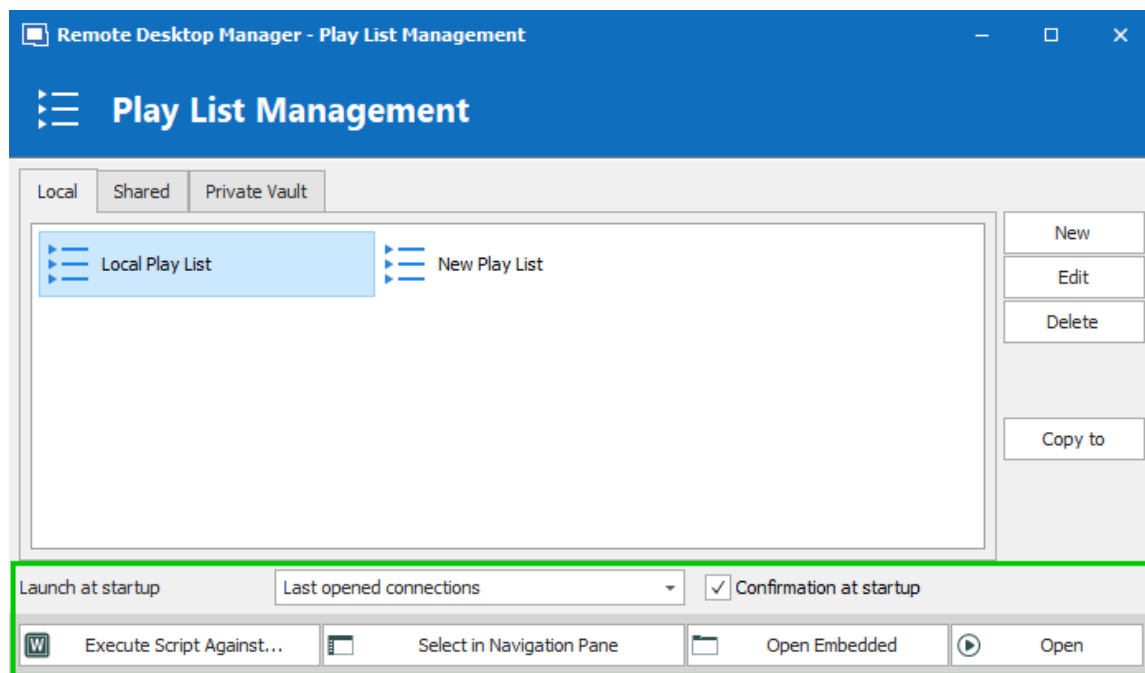
#### 6.5.2.1.2 Play List Management

## 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
<b>Open Embedded</b>	Overrides the display selection of entries inside the Play Lists and launches them as Embedded (some entries might not support this).
<b>Select in Navigation Pane</b>	Selects all entries the Play List contains in the Navigation Pane.
<b>Execute Script Against...</b>	This will prompt for you to select the <b>Typing Macro</b> (exclusively) you wish to execute against your Play list.
<b>Launch at startup</b>	Here you can select a specific Play List you would like launched whenever the application starts. You can also default back to <b>None</b> or <b>Last opened Connections</b> .

### 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.



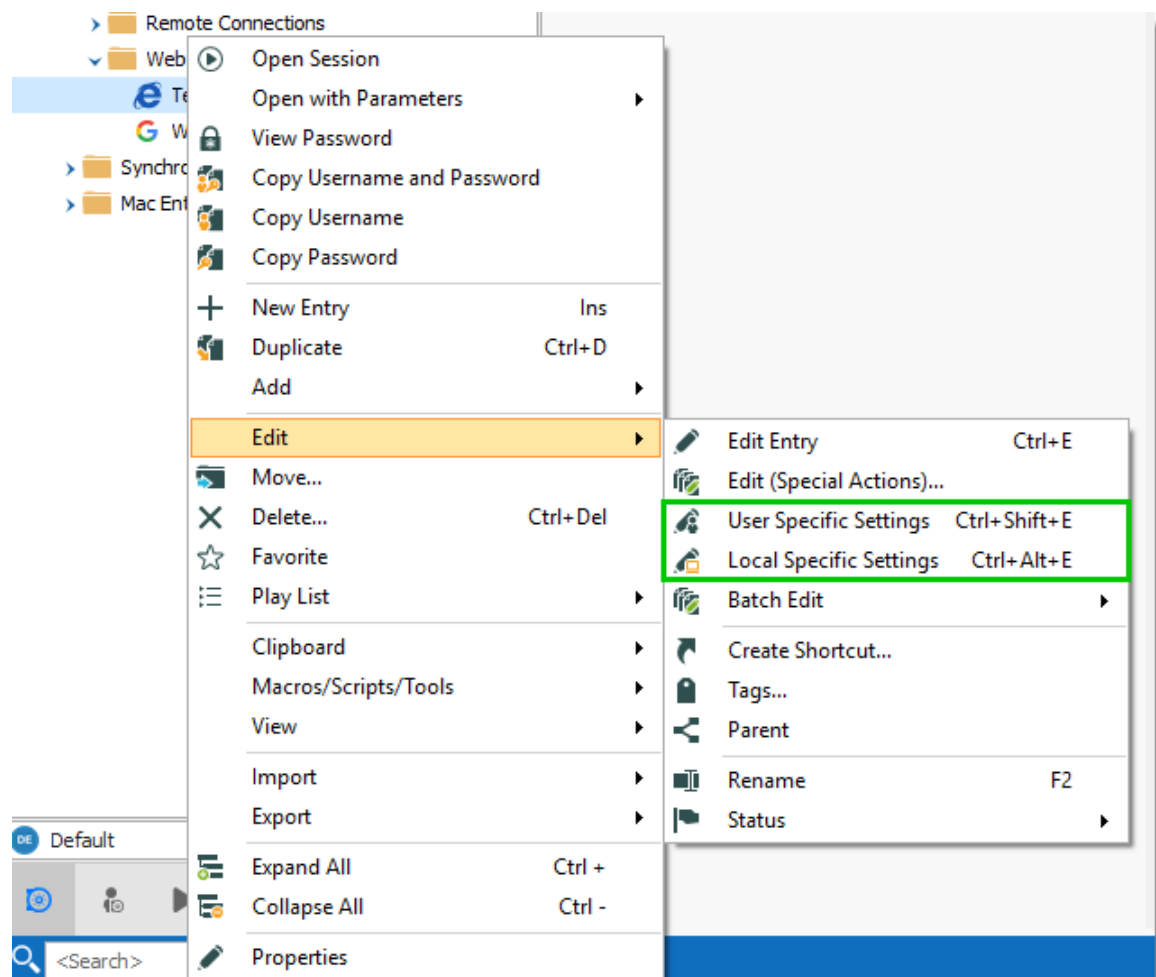
This feature is only available when using an [Advanced Data Source](#). A setting on the data source allows usage of Specific Settings. Contact your administrator if the menu is grayed out.



If both User Specific Settings and Local Specific Settings are defined on the same entry, Local Specific Settings have the priority.



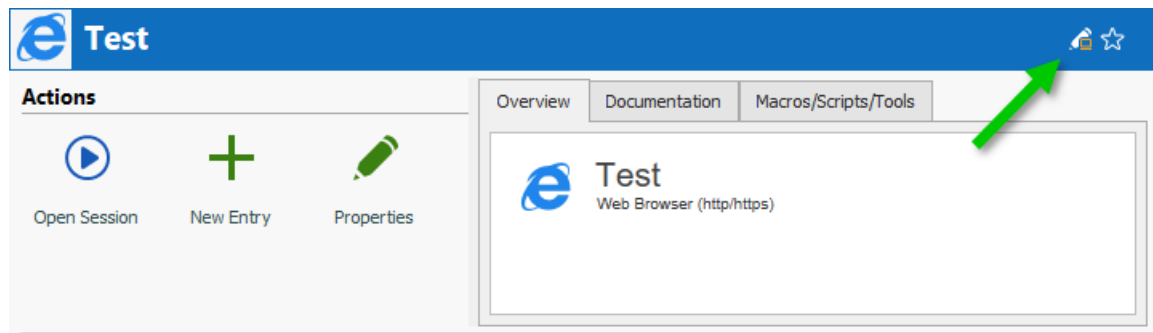
These can also be accessed by using the right-click on an entry and going to **Edit – User/Local Specific Settings**.



Context menu – Edit – User and Local Specific Settings

## SPECIFIC SETTINGS INDICATOR

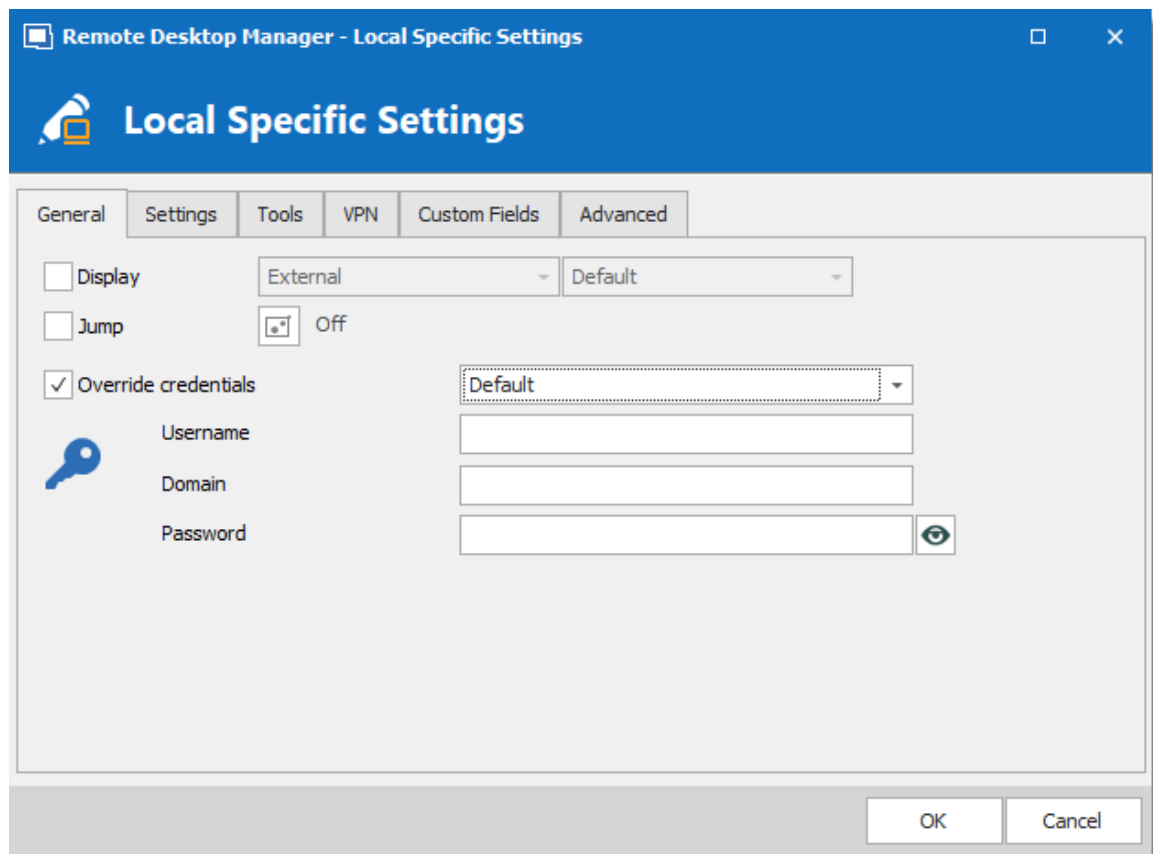
An indicator icon is displayed in the dashboard when an entry with **Specific Settings** is selected. Click on the icon to open the **Specific Settings** dialog.



*Specific Settings indicator*

## WORKFLOW

In the majority of cases, editing the **Specific Settings** displays the following dialog:



*User Specific Settings*



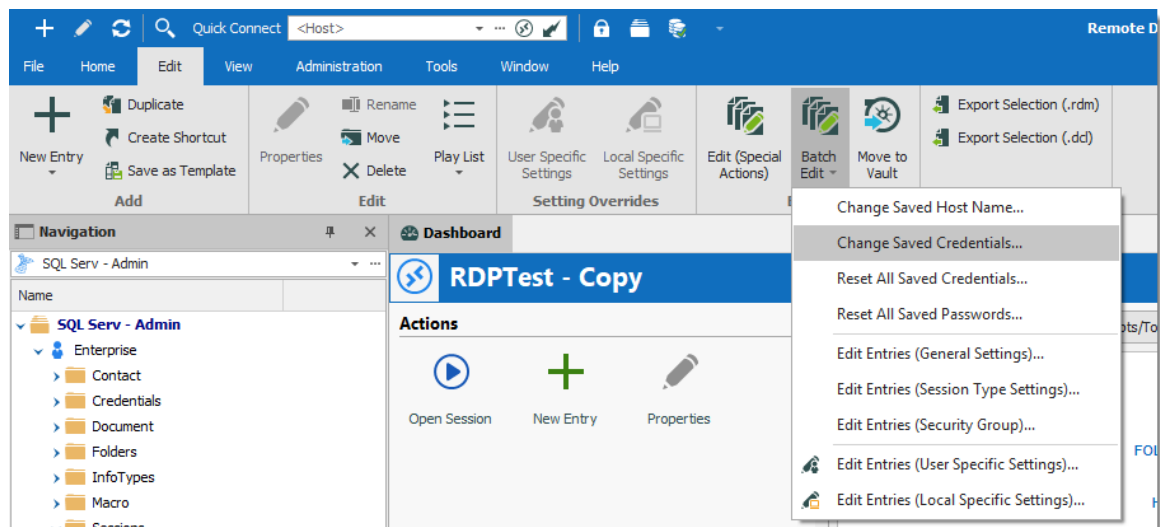
Specific settings are context sensitive, and several settings might not be available for some entry types.

## 6.5.4 Batch

### 6.5.4.1 Batch Edit

## DESCRIPTION

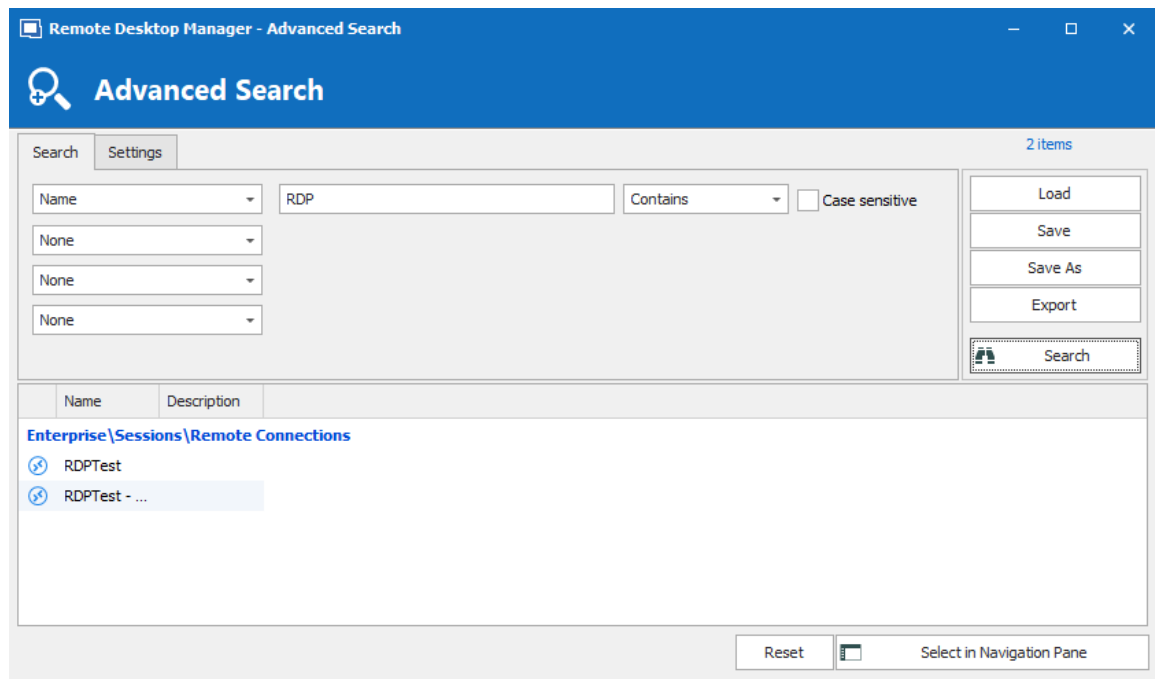
The **Batch Edit** feature changes the settings of multiple entries in one operation. For example, it can be used to remove or update the credentials of a group of sessions.



*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**.

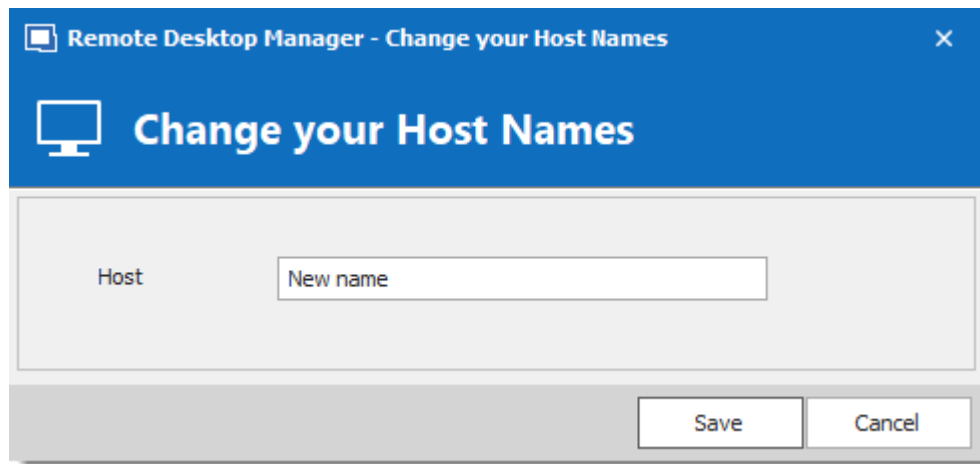
*Advanced Search*

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.



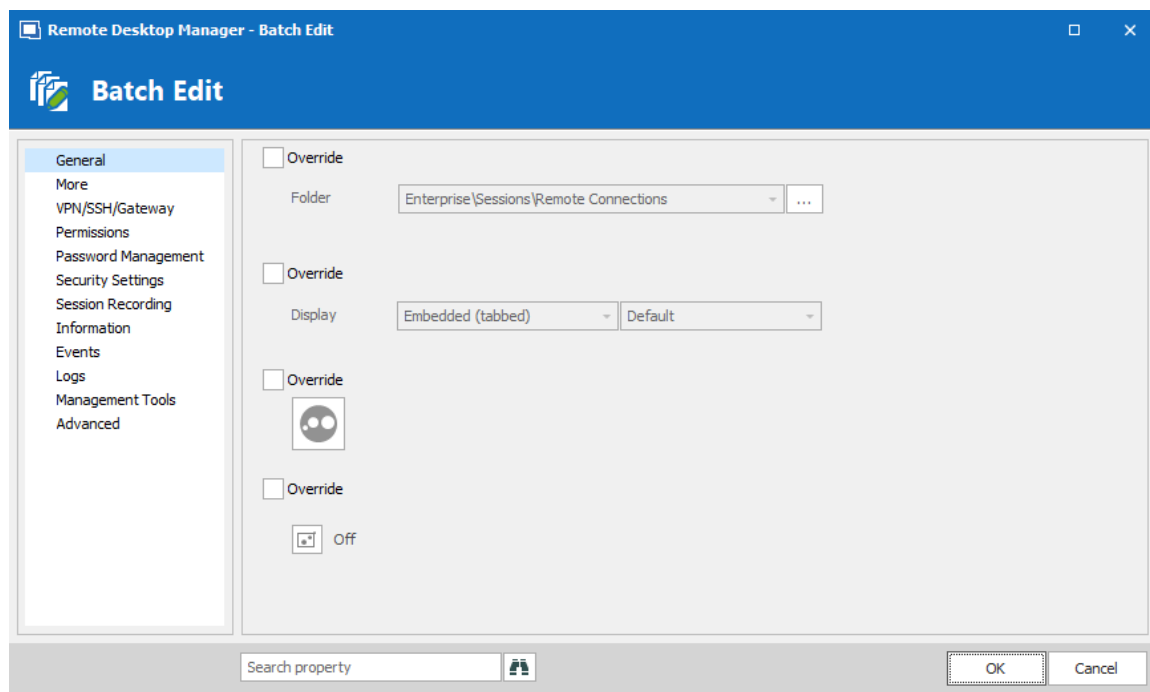
*Change Host Name*

## 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.

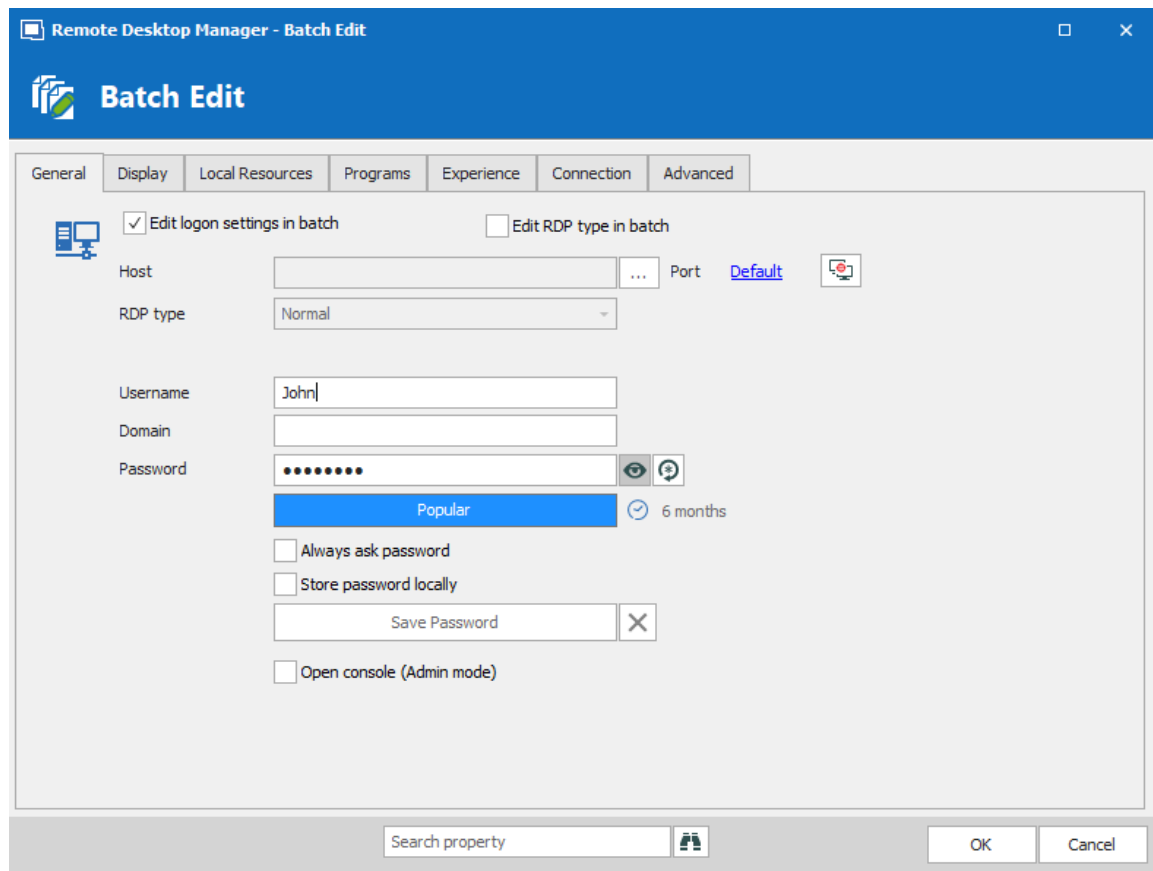


*Batch Edit – Common settings*

## EDIT SESSIONS (SESSION TYPE SETTINGS)

Change settings that are available only for specific session types, such as Microsoft RDP.





*Session Type Settings*

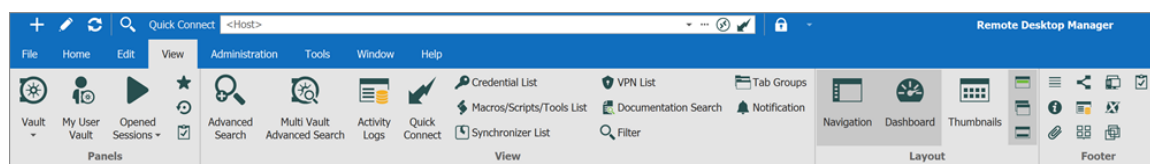
## EDIT SESSIONS (USER/LOCAL SPECIFIC SETTINGS)

[Specific Settings](#) can be modified in a batch if supported by the type of the edited entries.

### 6.6 View

## DESCRIPTION

The **View** ribbon is used to control different features regarding the views, layout and logs of Remote Desktop Manager.

*Ribbon - View*

Refer to the following topics for more information:

## PANELS

OPTION	DESCRIPTION
<b>Vault</b>	Access the view mode for your Navigation Pane for the current Vault.
<b>My User Vault</b>	Display your User Vault in the Navigation Pane.
<b>Opened Sessions</b>	Display the currently <a href="#">Opened Sessions</a> in your Navigation Pane.
<b>Favorites</b>	Display your <a href="#">Favorite</a> entries and folder in your Navigation Pane.
<b>Recent</b>	Display your <a href="#">Recently Opened Sessions</a> in your Navigation Pane.
<b>Task List</b>	Display your current <a href="#">Task List</a> .

## VIEW

OPTION	DESCRIPTION
<b>Advanced Search</b>	Use the <a href="#">Advanced Search</a> feature.

OPTION	DESCRIPTION
<b>Multi Vault Advanced Search</b>	This functions essentially the same way as <b>Advanced Search</b> , but it searches all the Vaults of the database.
<b>Activity Logs</b>	Open the <a href="#">Activity Logs</a> .
<b>Quick Connect</b>	Launch a Quick Connect session.
<b>Entry Lists</b>	Prompts a window that displays all the Credential, Macros/Scripts/Tools, VPN or Synchronizer entries in the database (restricted by user rights).
<b>Documentation Search</b>	Allows you to filter entries through their <a href="#">Documentation</a> , such as Description or Procedure.
<b>Filter</b>	This prompts a window to filter the Navigation Pane.
<b>Tab Groups</b>	Open a docked window to browse through the various Tab Groups.
<b>Notification</b>	Open an undocked window to browse threw the various notifications (such as entries expired or about to be, or tasks).

## LAYOUT

OPTION	DESCRIPTION
<b>Navigation</b>	Toggle the Navigation Pane.
<b>Dashboard</b>	Toggle the Dashboard.
<b>Thumbnails</b>	Toggle the Thumbnails.

OPTION	DESCRIPTION
<b>Top Pane (Ribbon/Menubar)</b>	Toggle the Ribbon. (Right-click the Application header to bring it back or use <b>Alt+F11</b> ).
<b>Grouped Tab Bar</b>	Toggle the grouped tab bar. (Must have group tabs to work).
<b>Status Bar</b>	Toggle the Status bar.

## FOOTER

The **Footer** section allows you to show or hide the various panes that are provided with Remote Desktop Manager.



Although they are by default displayed in the footer, all those panes can be dragged and docked anywhere within Remote Desktop Manager.

### 6.6.1 Task List

## DESCRIPTION

Create a list of tasks to keep track of work that needs to be done by the team. You can perform a search to filter out the list of displayed tasks. You can search by Due Date, username or by Status.

Task lists can be exported in different types of files for printing or reviewing. Right-click the task list to export in html, xls, xml or csv. You can also export filtered task lists.

The screenshot shows a web interface with a 'Task' tab selected. At the top, there are filters for 'Due Date' (Last 7 Days, 6/11/2019 to 6/18/2019), 'Status', and 'Username'. Below these is a search bar and an 'Auto refresh' checkbox. The main area is a table with columns 'Name', 'Status', and 'Due Date'. A single row is visible: 'Create new Entries' with status 'Open'.

Task list



This feature is only available for the following data sources: [Devolutions Server](#), [MariaDB](#), [MySQL](#), [SQL Azure](#), [SQL Server](#) and [SQLite](#).

## CREATING A TASK

1. Click on **Add new task**.

This screenshot is identical to the one above, but a green arrow points to the '+' icon in the table's toolbar, indicating where to click to add a new task.

Add a task

2. Enter your task information, like the name of the task, the priority, the due date, the description, etc.

Remote Desktop Manager - Task Management

**Task Management**

General

Name:

Entry: RDPTTest

Priority: 1 ☐ Due Date: 2/24/2019 6/18/2019 - 11:39 AM

Description:

User:

Status: Open

Comment:

OK Cancel

*Task Management*

OPTION	DESCRIPTION
<b>Name</b>	Enter a custom name for the task
<b>Entry</b>	Displays the entry currently selected in the Navigation Pane. The task is assigned to this entry. Read-only field.
<b>Priority</b>	Set the priority of the task.
<b>Due date</b>	Set a deadline for the task.
<b>Description</b>	Enter a description of the task for the assigned user.
<b>User</b>	Assign a user to the task.
<b>Assign to me</b>	Click this button to assign the task to yourself.

OPTION	DESCRIPTION
<b>Clear assigned user</b> ✕	Clear the assigned user.
<b>Status</b>	Set a status for the task. Select between: <ul style="list-style-type: none"> <li>• Open</li> <li>• Assigned</li> <li>• In progress</li> <li>• Closed</li> <li>• Done</li> <li>• Canceled</li> <li>• Postponed</li> </ul>
<b>Comment</b>	Enter a comment for the task.

## 6.6.2 Activity Logs

### DESCRIPTION

The shared session log offers a more robust solution. Through it, it's possible to monitor an opened session for all users that are using an Advanced Data Sources. The log is available for specific sessions in the context menu, in the session properties (Log tab page) and in the dashboard.

### SETTINGS

The log contains all the CRUD (add, edit and delete) operations, passwords being viewed, credentials being used by other sessions, etc...

Dashboard Activity Logs

Date: Last 7 Days 6/11/2019 To 6/18/2019 Ticket #

Username Folder

Message On open comment

Machine name On close comment

☒ All vaults Local time Search

Folder	Message	On Open Comment	On Close Comment	Log Date	End Date/Time	Active Time
Jaf	Entry deleted			6/11/2019 9:32:22 ...		
Jaf\Credentials	Entry deleted			6/11/2019 9:32:22 ...		
Jaf\Sessions	Entry deleted			6/11/2019 9:32:22 ...		
Jaf\Sessions\A...	Entry deleted			6/11/2019 9:32:22 ...		
Enterprise\Sessi...	Viewed entry			6/11/2019 9:40:11 ...		
Jaf	Entry deleted			6/12/2019 7:18:50 ...		
Jaf\Sessions	Entry deleted			6/12/2019 7:18:50 ...		
Jaf\Sessions\A...	Entry deleted			6/12/2019 7:18:50 ...		
Enterprise\Sessi...	Viewed entry			6/12/2019 11:31:22...		
Enterprise\Sessi...	Viewed entry			6/12/2019 11:31:46...		
Enterprise\Sessi...	Viewed entry			6/12/2019 11:32:00...		
	Entry updated			6/12/2019 2:09:28 PM		

OPTION	DESCRIPTION
<b>Folder</b>	The Folder where your entry is situated.
<b>Connection</b>	The connection being used to open your entry.
<b>Message</b>	Indicate the action that was done on your entry or session.
<b>On Open Comment</b>	The Open Comment is defined in the Log tab of your session, to learn more please see Logs Options
<b>On Close Comment</b>	The Close Comment is defined in the Log tab of your session, to learn more please see Logs Options
<b>Log Date</b>	Indicate the date and time your session was opened or your entry was edited.
<b>End Date/Time</b>	Indicate the date and time when the session or entry was closed.
<b>Active Time</b>	Only available for sessions in embedded mode. It will record your session active time, meaning the time your session was opened in embedded mode and you were active in your session. If your

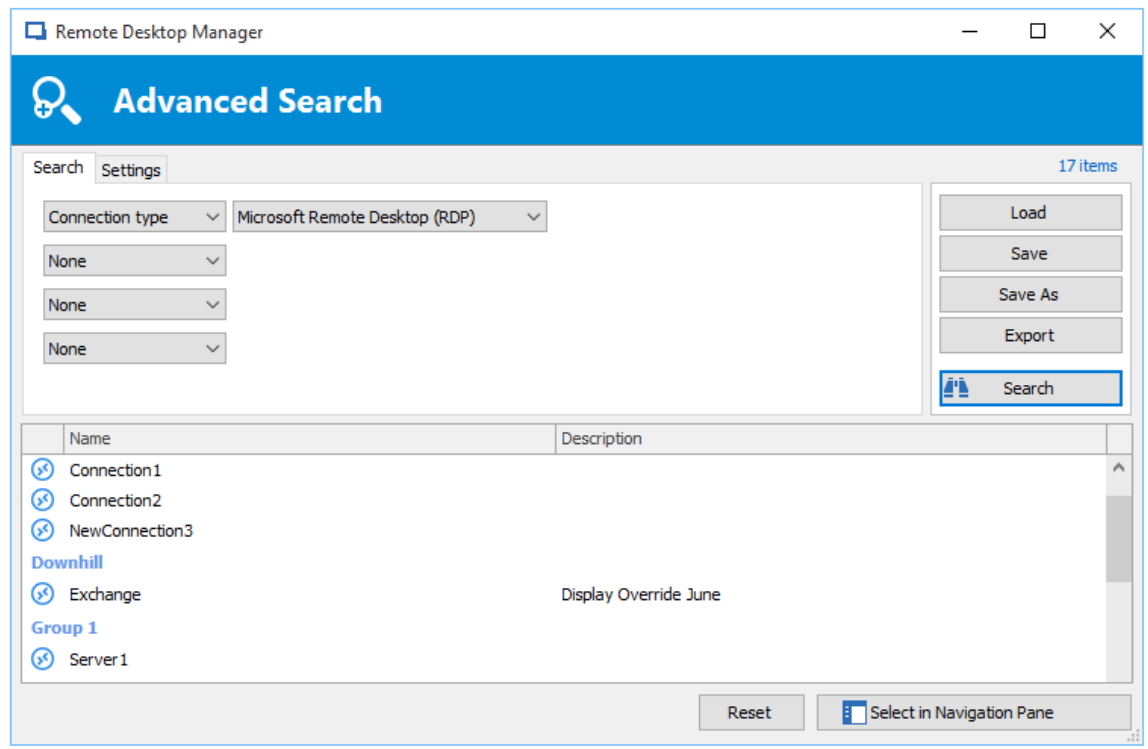


OPTION	DESCRIPTION
	session is opened but your view is on your Dashboard tab and not on your session tab, no Active Time will be recorded.
<b>Duration</b>	Only available for sessions in embedded mode. When sessions are opened in embedded mode the Duration time will be recorded, meaning that even if your view is on your Dashboard and you are not actively working in your session but your session tab is opened, Duration will record how long it was opened for.
<b>User</b>	Indicate the Windows username and domain.
<b>Database username</b>	Indicate the database username.
<b>Connection user</b>	Indicate the Connection user.
<b>Machine</b>	Indicate the machine name.
<b>Connection Type</b>	Indicate the connection type that was used.

### 6.6.3 Advanced Search

#### DESCRIPTION

The **Advanced Search** allows to search for entries based on multiple criterias.



Advanced Search Window

## SETTINGS

OPTION	DESCRIPTION
<b>Name</b>	<p>You can select between different criteria to tweak your search:</p> <ul style="list-style-type: none"> <li>• <b>Name</b></li> <li>• <b>Connection type</b></li> <li>• <b>Contact Reference</b></li> <li>• <b>Creation date</b></li> <li>• <b>Custom field</b></li> <li>• <b>Description</b></li> </ul>

OPTION	DESCRIPTION
	<ul style="list-style-type: none"><li>• <i>Domain</i></li><li>• <i>Group</i></li><li>• <i>Host</i></li><li>• <i>Is favourite</i></li><li>• <i>Keywords/tags</i></li><li>• <i>Last update date</i></li><li>• <i>Name</i></li><li>• <i>OS</i></li><li>• <i>Password strength</i></li><li>• <i>Security group</i></li><li>• <i>Status</i></li><li>• <i>Username</i></li></ul>
<b>Load</b>	Load searches that has been previously saved.
<b>Save</b>	Allows you to save your search locally and reuse it.
<b>Save as</b>	Use to save a previously saved search but under another name.
<b>Export</b>	Export the entries of your search result as a Csv, Html, Xls or Xml file. Sensitive information will be encrypted using AES.
<b>Search</b>	Once you have selected your search criteria click on <b>Search</b> to display the search result.
<b>Reset</b>	Reset all your fields to proceed with a new Search.

OPTION	DESCRIPTION
<b>Select in Navigation Pane</b>	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 fields (ex: Name) to give you search options for:

- **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.

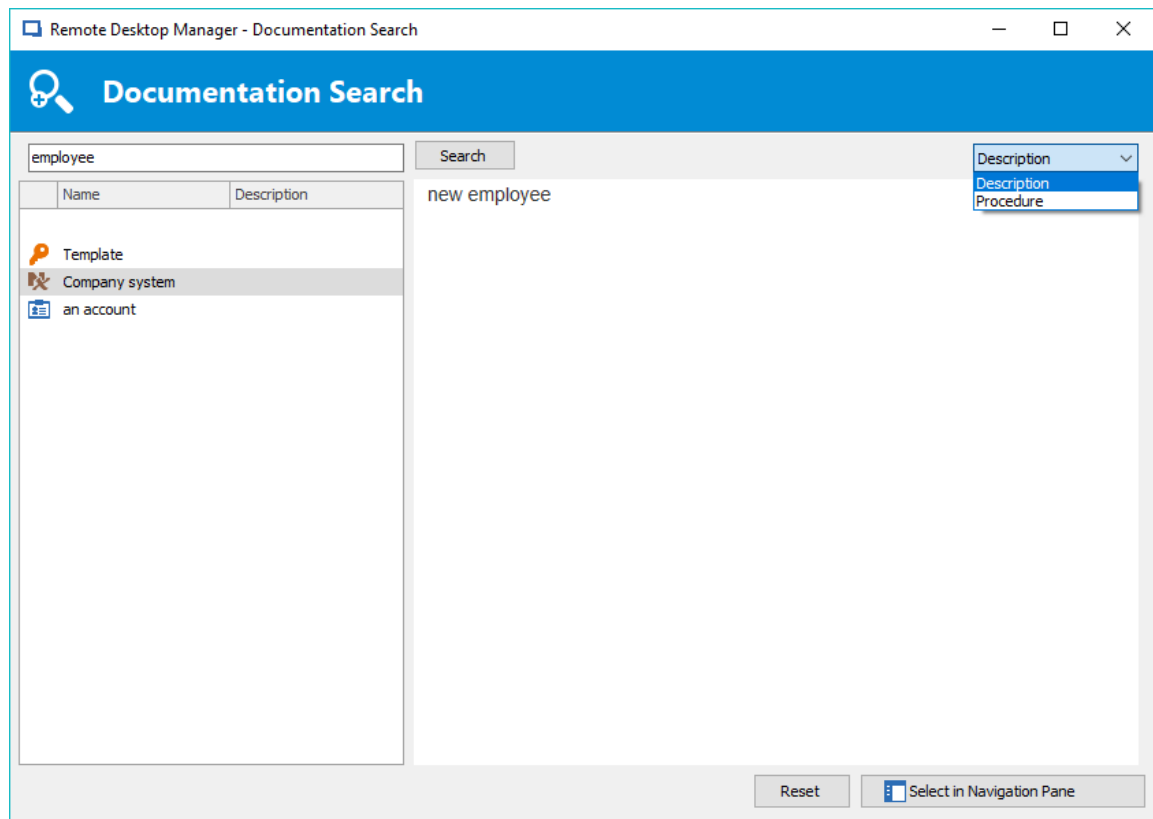
#### 6.6.4 Documentation Search

### 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.

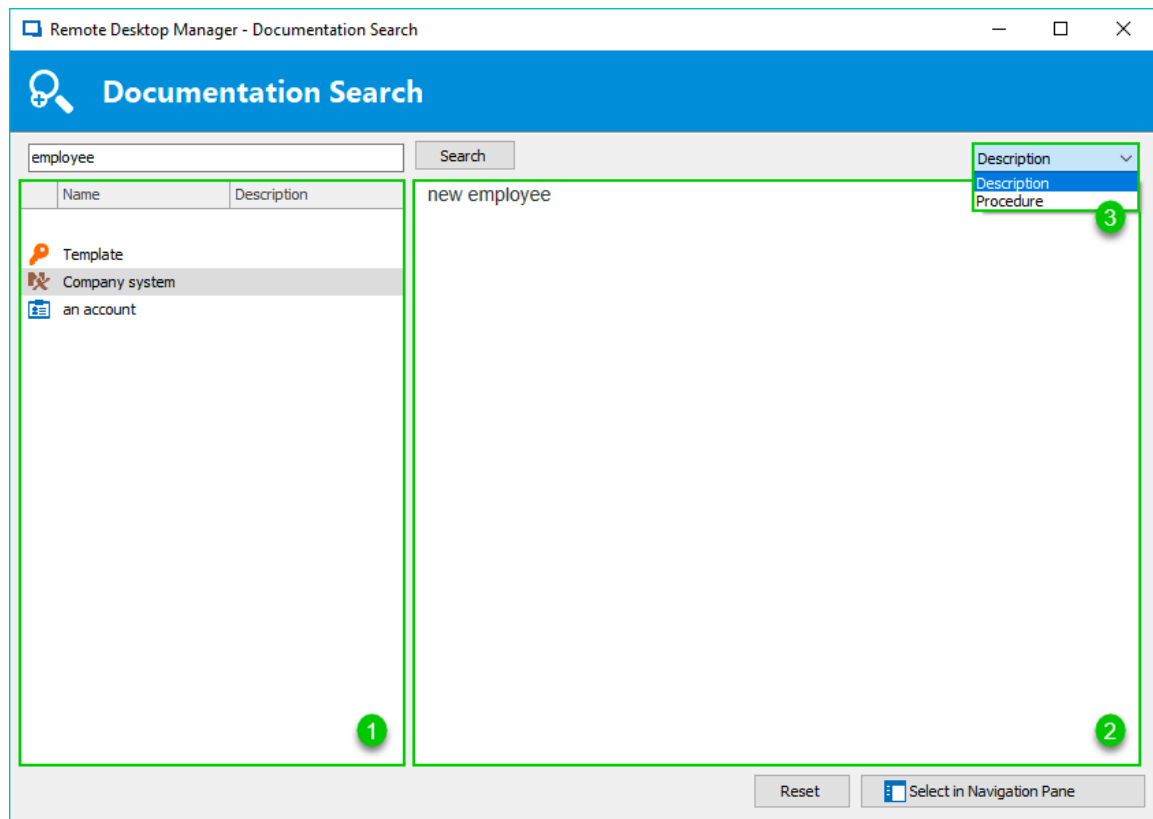


Documentation Search is available with Devolutions Server, MariaDB, MySQL and SQL Server data sources.



*Documentation search dialog window*

## USER INTERFACE



Documentation search

## USER INTERFACE

ELEMENTS	DESCRIPTION
<b>Navigation Pane (1)</b>	Lists search results by entry
<b>Content area (2)</b>	Page preview
<b>Drop down menu (3)</b>	Page title; When one entry contains multiple documentation pages with the search term, a list of the page titles is available.

## SELECT AN ENTRY

Click **Select in Navigation Pane** to choose the entry in your main tree view.

## CLEAR A SEARCH

Click **Reset** to clear the search results.

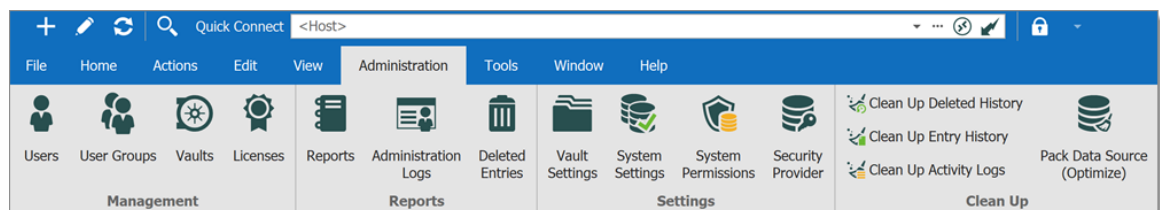
## 6.7 Administration

### 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
<b>Users</b>	Opens the <a href="#">User Management</a> .
<b>Security Groups (Legacy)</b>	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.
<b>Vaults</b>	Opens the Vault Management tab of User Management.
<b>User Groups</b>	Opens the <a href="#">User Groups Management</a> tab of User Management.

## REPORTS



The logs feature requires an [Advanced Data Source](#).

OPTION	DESCRIPTION
<b>Reports</b>	Open the <a href="#">Reports</a> section to select which type of report best suit your current needs.
<b>Administration Logs</b>	Opens the Administration Logs.
<b>Deleted Entries</b>	Open a log of all <a href="#">Deleted Entries</a> (since last clean up).

## SETTINGS





These feature requires an [Advanced Data Source](#).

OPTION	DESCRIPTION
<b>Vault Settings</b>	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 <a href="#">Default security for entries</a> for more information.
<b>System Settings (Data Source Settings)</b>	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.
<b>System Permissions</b>	Modify <a href="#">System Permissions</a> .
<b>Security Provider</b>	Set up a <a href="#">Security Provider</a> for an additional layer of security.

## CLEAN UP



This feature requires an [Advanced Data Source](#).

OPTION	DESCRIPTION
<b>Clean Up Deleted History</b>	Perform a partial or full clean up of the <a href="#">Deleted History</a> .

OPTION	DESCRIPTION
<b>Clean Up Entry History</b>	Perform a partial or full clean up of the <a href="#">Entry History</a> .
<b>Clean Up Activity Logs</b>	Perform a partial or full clean up of the <a href="#">Activity Logs</a> . You also have the option to clean up the <b>Administration Logs</b> if desired.
<b>Pack Data Source (Optimize)</b>	The <a href="#">Pack Data Source (Optimize)</a> 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](#).



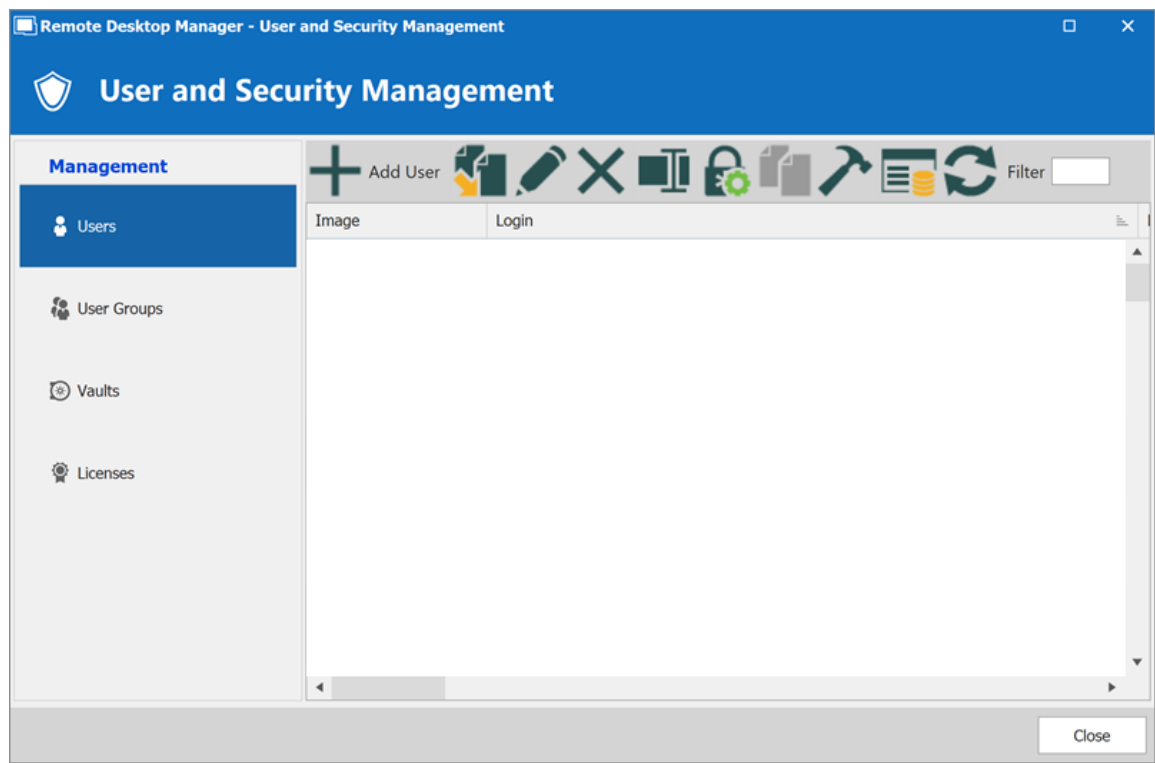
A user can be created using default security (specify the password) or [Integrated Security](#). Not all [Advanced Data Sources](#) support the use of [Integrated Security](#).



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

The screenshot shows the 'Remote Desktop Manager - User Management' dialog box with the 'General' tab selected. The left sidebar contains links for 'General', 'User Groups', 'Vaults', 'Application Access', 'Settings', and 'Information'. The 'General' tab has two sections: 'General' and 'Information'. The 'General' section includes fields for 'ID', 'Authentication type' (set to 'Database'), 'Username', 'Password', 'User type' (set to 'User'), 'User license type' (set to 'Default'), and a checkbox for 'User must change password at next login'. There are also checkboxes for 'Integrated security' and 'Create database login/user'. The 'Information' section includes fields for 'First name', 'Last name', and 'Email'. At the bottom right are 'OK' and 'Cancel' buttons.

*User Management - General*

OPTION	DESCRIPTION
<b>Authentication type</b>	<p>Select the user's authentication type:</p> <ul style="list-style-type: none"> <li>• <b>Custom (Devolutions):</b> create a user specific to Remote Desktop Manager without creating an SQL login.</li> <li>• <b>Database (SQL Server):</b> authenticate using the SQL login from your SQL Server.</li> </ul>
<b>Username</b>	<p>Enter the username for the user. When using <a href="#">Integrated Security</a> the user must be selected from the directory.</p>
<b>Integrated security (Active Directory)</b>	<p>Specify 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 <a href="#">Integrated Security</a> topic.</p>

OPTION	DESCRIPTION
<b>Password</b>	Enter the user's Password. This field is disabled when using <a href="#">Integrated Security</a> .
<b>User type</b>	<p>Select the type of user to create, select between:</p> <ul style="list-style-type: none"> <li>• <b>Administrator:</b> Grant full administrative rights to the user.</li> <li>• <b>Read only user:</b> Grant only the view access to the user.</li> <li>• <b>Restricted user:</b> Select which rights to grant to the user.</li> <li>• <b>User:</b> Grant all basic rights to the user (Add, Edit, Delete).</li> </ul> <p>For more information, please consult the <a href="#">User Types</a> topic.</p>
<b>User license type</b>	<p>Select the license type of the user. Select between:</p> <ul style="list-style-type: none"> <li>• <b>Default</b></li> <li>• <b>Connection Management</b></li> <li>• <b>Password Management</b></li> </ul>
<b>Full name</b>	Enter the First name and Last name of the user.
<b>Email</b>	Insert the user's email address.

## INFORMATION

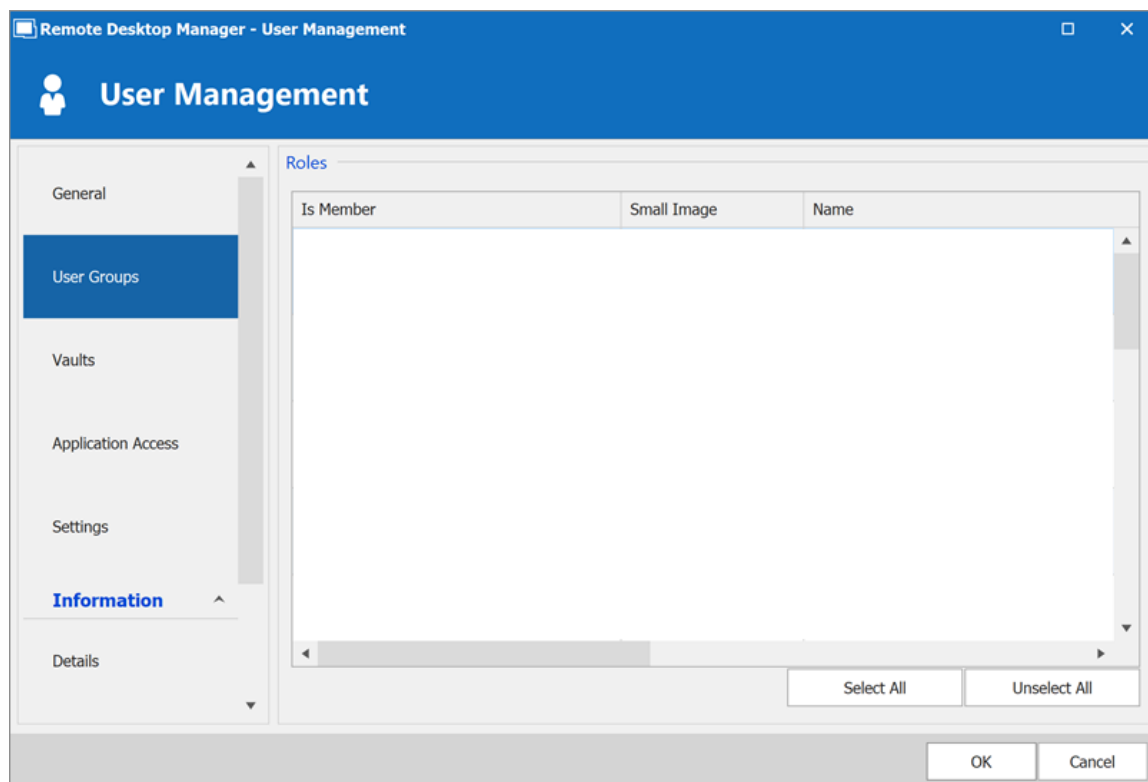
The **Information** section allows to store information regarding the users, such as their name, address, and more. The Information section is divided in three sub-sections: **Details, Address, Phone**.

The screenshot shows the 'Remote Desktop Manager - User Management' window. The title bar is blue with a white icon of a person and the text 'User Management'. The main area is divided into a left sidebar and a right content area. The sidebar has a blue header 'User Management' and a list of items: 'Vaults', 'Application Access', 'Settings', 'Information' (highlighted in blue), 'Details' (highlighted in blue), 'Address', and 'Phone'. The right content area is titled 'Information' and contains five input fields: 'Company', 'Job title', 'Department', 'Gravatar email', and 'Language' (a dropdown menu showing 'English'). At the bottom right of the window are 'OK' and 'Cancel' buttons.

*User Management - Information - Details*

## USER GROUPS

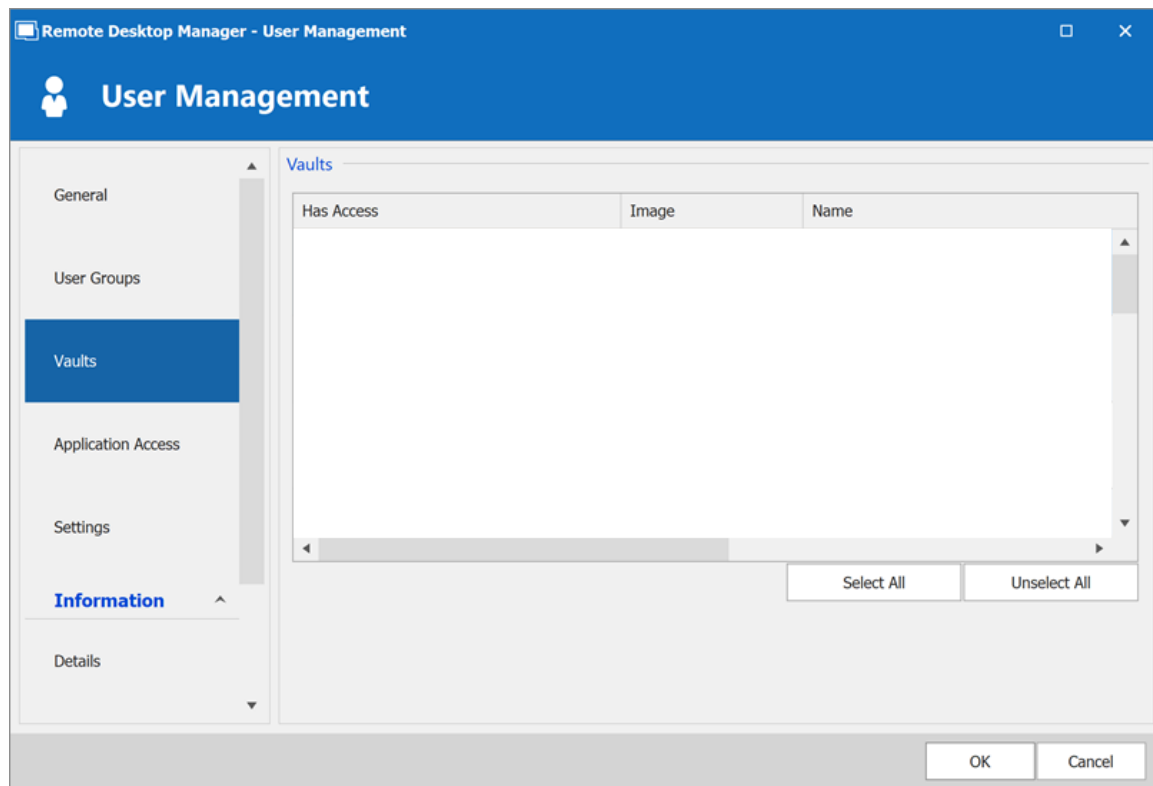
Select user groups to assign to the user.

*User Management - User Groups*

OPTION	DESCRIPTION
<b>User Groups</b>	Check the <b>Is Member</b> box to assign the user groups to the user. Consult <a href="#">User Groups Management</a> topic for more information.

## VAULTS

Select which repositories the user has access to. For more information, please consult the Vaults topic.

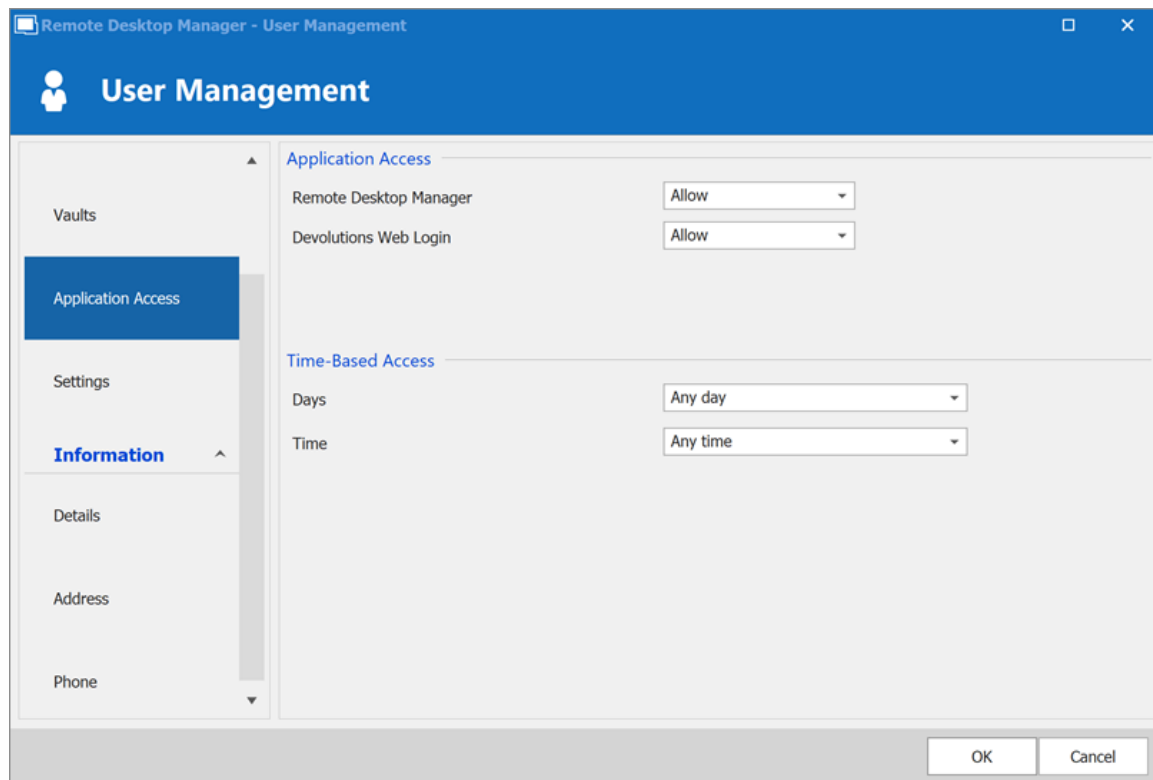


*User Management - Vaults*

## APPLICATION ACCESS

The application access section allows to restrain access to Remote Desktop Manager or Devolutions Web Login.

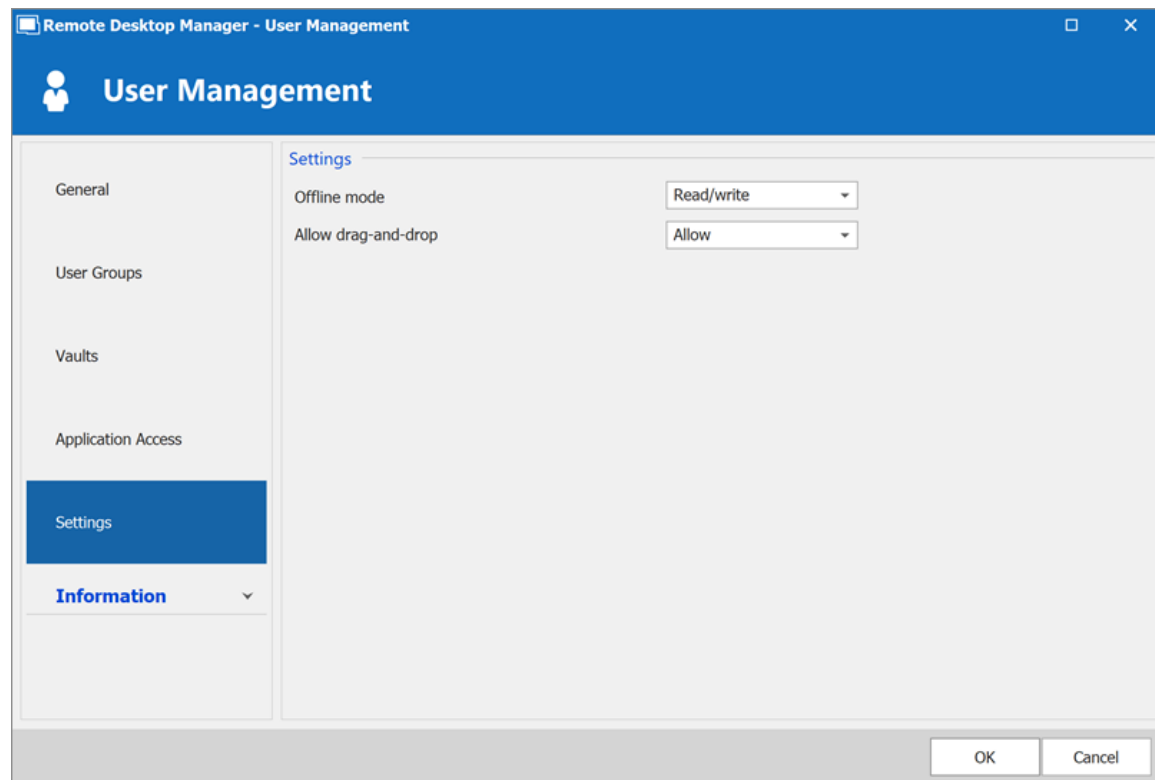




*User Management - Application Access*

OPTION	DESCRIPTION
<b>Remote Desktop Manager</b>	Select if the user can access to the data source from Remote Desktop Manager.
<b>Devolutions Web Login</b>	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
<b>Disabled</b>	No offline cache allowed for the user.
<b>Cache only</b>	Allow to save a cache of the data source but not the offline mode.
<b>Read-only</b>	A read-only cache. The user will not be able to edit data in the data source. This mode is allowed for <a href="#">Advanced Data Sources</a> only.
<b>Read/Write</b>	An advanced cache, with change synchronization. This mode is allowed for <a href="#">Advanced Data Sources</a> 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.

The screenshot shows the 'Remote Desktop Manager - User Management' window. The 'General' tab is selected in the left sidebar. The main area contains the following fields and options:

- ID:** 9914D1D1-7E4E-47EF-93AA-3F47DB6D9654
- Authentication type:** Database (dropdown)
- Username:** (empty text field)
- Password:** (empty text field)
- User type:** User (dropdown menu is open, showing options: User, Administrator, User (highlighted), Restricted user, Read-only user)
- User license type:** (empty text field)
- Integrated security:** ☐
- Create database login/user:** ☒
- Information tab (visible below):**
  - First name:** (empty text field)
  - Last name:** (empty text field)
  - Email:** (empty text field)

Buttons at the bottom right: OK, Cancel.

*User Management - User Type*

TYPE	DESCRIPTION
<b>Administrator</b>	Grant all rights and permissions to the user.
<b>User</b>	Grant all the basic rights to the user (Add, Edit, Delete).  For more information, please consult the <a href="#">Rights</a> section below in this topic.
<b>Restricted user</b>	Personalize the rights to grant to the user.

TYPE	DESCRIPTION
<b>Read only user</b>	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.

The screenshot shows the 'Remote Desktop Manager - User Management' window. The 'General' tab is selected in the left sidebar. The 'User type' dropdown is set to 'Restricted user'. The 'Rights' section is expanded, showing checkboxes for 'Add', 'Edit', 'Delete', and 'Move'. The 'Add' checkbox is checked. The 'Information' section at the bottom contains fields for 'First name', 'Last name', and 'Email'.

*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.

Remote Desktop Manager - User Management

**User Management**

General

- Information
- Roles
- Privileges
- Security Groups (Legacy)
- Vaults
- Application Access
- Settings

General

ID: 89F53CFE-08AD-4FDC-972C-53DFF3934827

Authentication type: Database

Username:  ... ☒ Integrated security (Active Directory)

Password:  ☒ Create SQL Server Login and User

User type: User

User license type: Default

Information

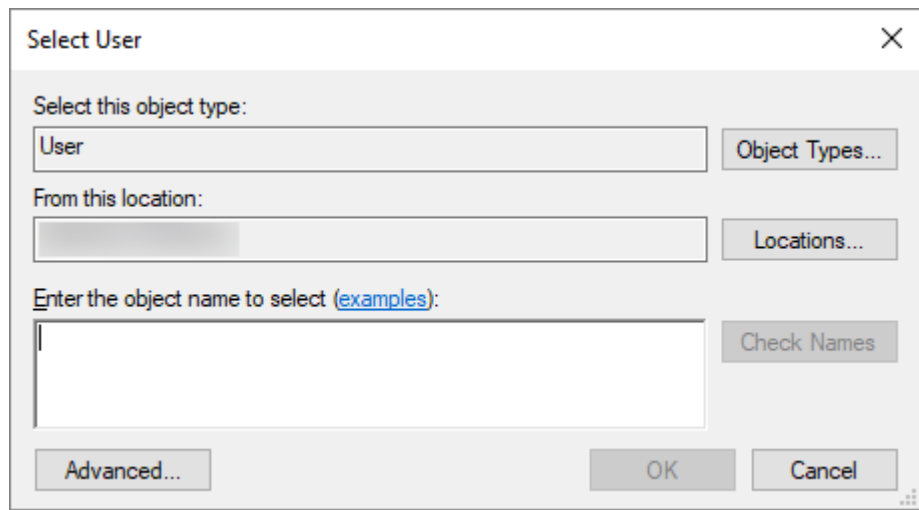
First name:  Last name:

Email:

OK Cancel

*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.



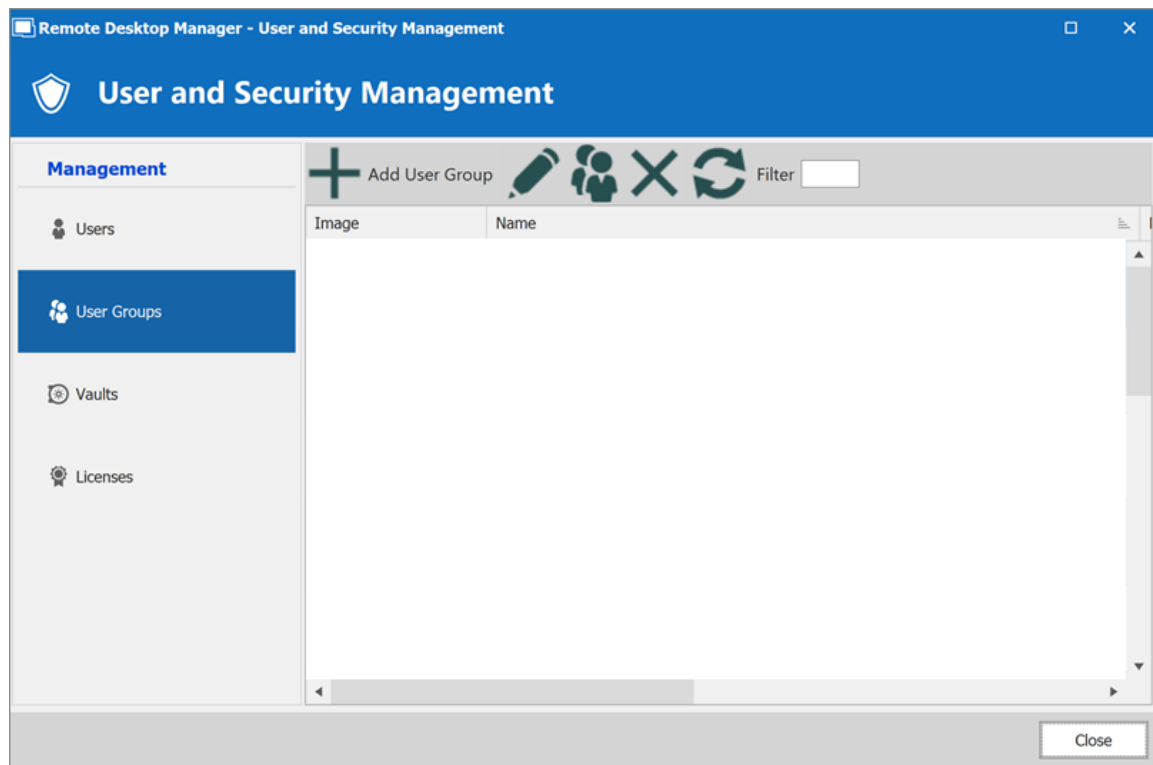
Please note that the Unsecured group permissions (the ones above the grid) are ignored. You must set them on each user individually.

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*

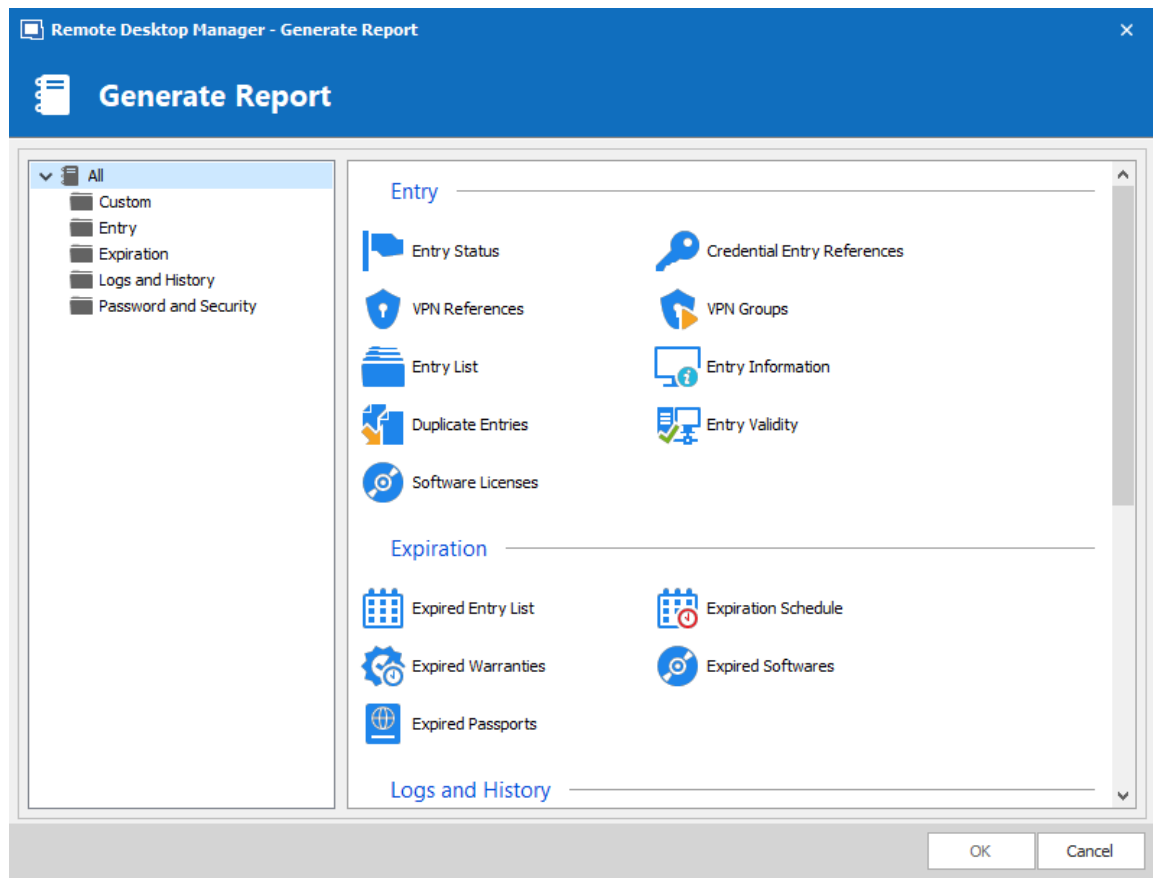
## 6.7.2 Reports

### 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.

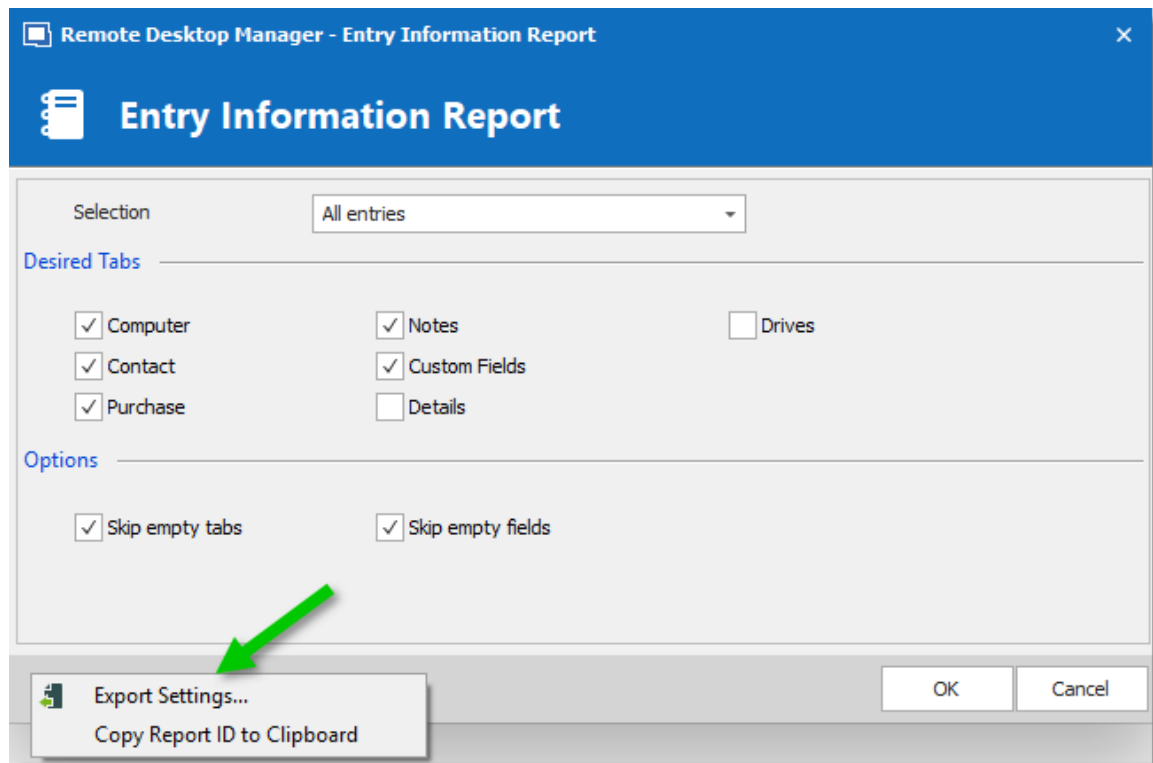
## SETTINGS



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).



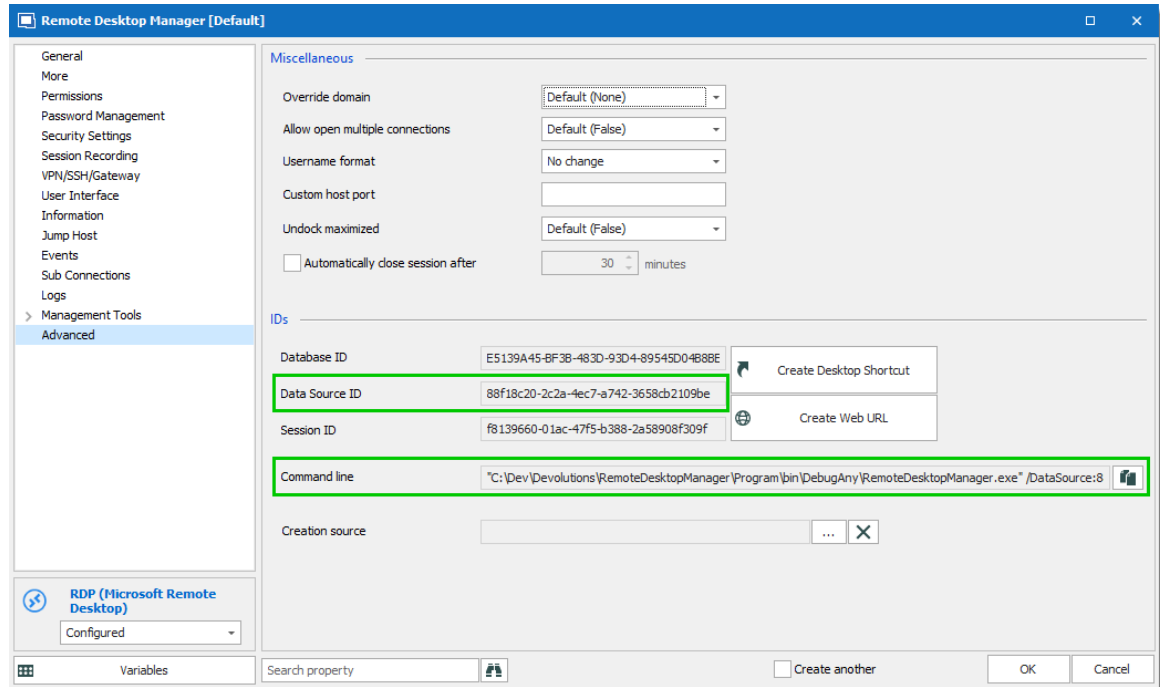
*Export Settings*

2. In your Windows Command Prompt enter the following command line:

```
C:\*** /DataSource:*** /report:***/reportoutput:"***" /reportsettings:"***.rdr"
```

PARAMETERS	DESCRIPTION
<b>C:\</b>	Enter the path used to start your Remote Desktop Manager application (path of the RemoteDesktopManager.exe file)
<b>/DataSource</b>	Specify the data source ID.
<b>/report</b>	Specify the type of report to generate or the report ID.
<b>/reportoutput</b>	Specify the path to save your report and the name for the newly generated report.
<b>/reportsettings</b>	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 IN Remote Desktop Manager	REPORT NAME (TYPE) TO INSERT IN THE COMMAND LINE
Usage Log	SharedConnectionLog
Entry Information	EntryInformation
Expiration Schedule	CalendarExpiredEntry
Expired Entry List	ConnectionExpiredEntry
Expired Passports	ConnectionExpiredPassports

REPORT TYPE IN Remote Desktop Manager	REPORT NAME (TYPE) TO INSERT IN THE COMMAND LINE
<b>Expired Softwares</b>	ConnectionExpiredSoftwares
<b>Expired Warranties</b>	ConnectionExpiredWarranties
<b>Entry Status</b>	ConnectionStatus
<b>Credential Entry References</b>	CredentialEntryUsage
<b>Entry Validity Report</b>	EntryValidity
<b>VPN References</b>	VPNEntryUsage
<b>Entry List</b>	Connection
<b>Duplicate Entries</b>	DuplicateEntry
<b>Password Complexity</b>	PasswordComplexity
<b>Password Analyzer</b>	PasswordAnalyzer

Here is an example of a command line for an Entry Information Report:

```
C:\Program Files (x86)\Devolutions\Remote Desktop Manager\RemoteDesktopManager.exe /D
/reportoutput:C:\dev\devolutions\Rapport\rapportEntry.csv /reportsettings:C:\dev\devo
```

#### 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.

Remote Desktop Manager - Deleted Entries

### Deleted Entries

Name	Test - Copy	Action	Delete
Connection type	IE	Group	Enterprise\Sessions\Web
Username	DEVOLUTIONS\jmajeau	Created on	4/16/2019 3:42 PM
Data source user	sa	Modified on	6/18/2019 1:41 PM

Action	Session Type	Name	Folder	Created On	Modified On	Username	Logged User
Delete	IE	Test - Copy	Enterprise\Sessi...	4/16/2019 3:42 PM	6/18/2019 1:41 PM	DEVOLUTIONS\jmajeau	sa
Delete	RDP (Microsoft ...	DEVOLUTIONS178		6/17/2019 6:09 PM	6/17/2019 6:09 PM	DEVOLUTIONS\jmajeau	sa
Delete	Credential Entry	Lastpass - training@devolu...	Enterprise\Sessi...	6/17/2019 1:02 PM	6/17/2019 2:10 PM	DEVOLUTIONS\jmajeau	sa
Delete	Credential Entry	JPasword	Enterprise\Sessi...	6/17/2019 1:19 PM	6/17/2019 2:10 PM	DEVOLUTIONS\jmajeau	sa
Delete	Credential Entry	test	Enterprise\InfoT...	6/17/2019 12:30 PM	6/17/2019 12:30 PM	DEVOLUTIONS\jmajeau	sa
Delete	VPN	test	Enterprise\Sessi...	6/13/2019 1:35 PM	6/13/2019 1:36 PM	DEVOLUTIONS\jmajeau	sa
Delete	Folder	Sessions	Jaf\Sessions	6/20/2018 7:53 PM	6/13/2019 1:22 PM	DEVOLUTIONS\jmajeau	sa
Delete	Folder	Jaf	Jaf	6/20/2018 7:53 PM	6/13/2019 1:22 PM	DEVOLUTIONS\jmajeau	sa
Delete	RDP (Microsoft ...	asdf	Enterprise\Sessi...	6/12/2019 6:11 PM	6/12/2019 6:11 PM	DEVOLUTIONS\jmajeau	sa

Delete Resurrect Entry Delete All Close

Deleted Entries

OPTION	DESCRIPTION
<b>Delete</b>	Permanently delete the selected entry.
<b>Resurrect Entry</b>	Use this button to restore an entry.
<b>Delete All</b>	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

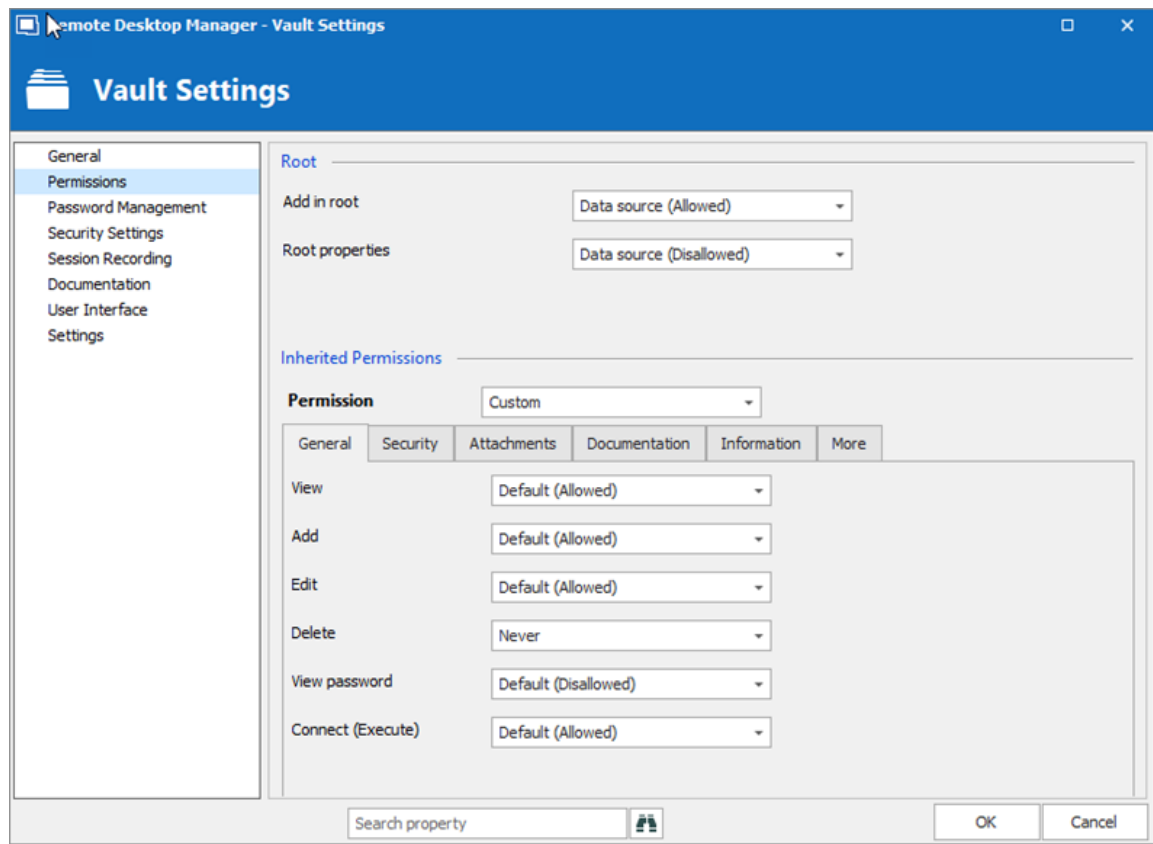
#### 6.7.3.1 Vault Settings

##### 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.

The screenshot shows the 'System Settings' window for Remote Desktop Manager. The 'General' tab is selected in the left sidebar. The main area contains several settings:

- General**
  - ☒ Allow user specific settings
  - ☒ Allow shortcuts
  - ☒ Allow virtual folders
  - Allow sub connections: Default
  - Add entry mode: Template list (include blank)
  - ☒ Allow database clean up
  - ☒ Allow entry states (Lock, Running, Checkout)
  - ☒ Automatic check in after: 60 minutes
- Comments**
  - ☐ Allow log comments editing
  - Minimum length (char): 0
- File Size**
  - Maximum file size (MB): 25 (This setting applies to documents and attachments)

At the bottom, there is a 'View History' button, a search bar, and the version '2019.1.30.0'. 'OK' and 'Cancel' buttons are in the bottom right.

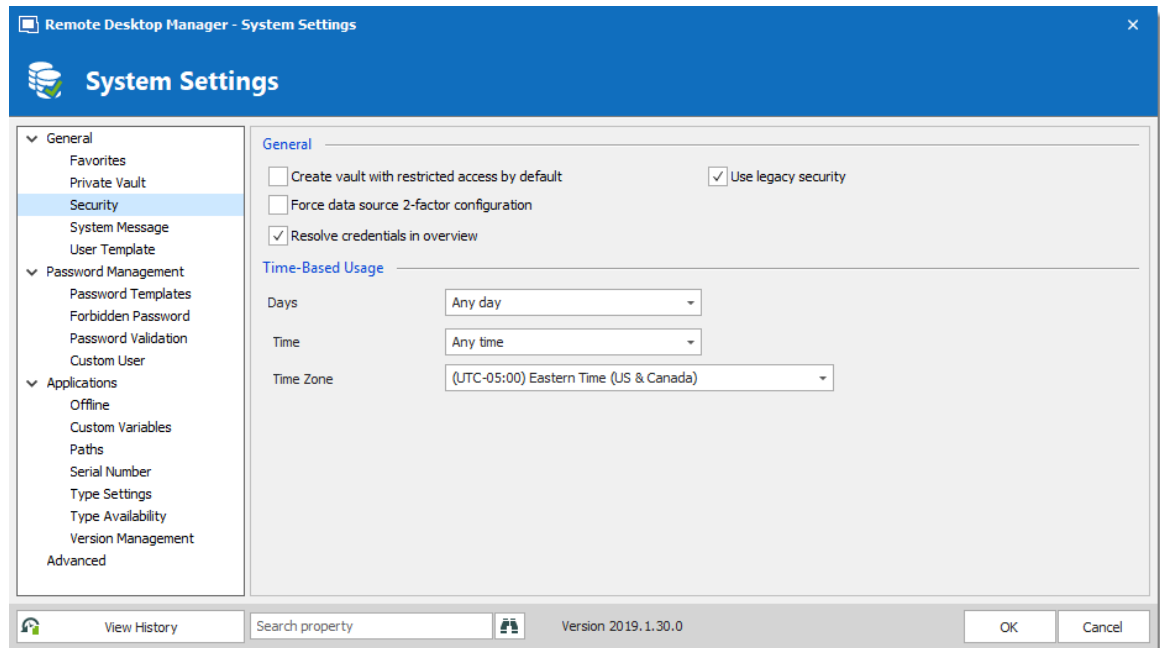
*System Settings - General*

GENERAL	DESCRIPTION
<b>Allow user Specific Settings</b>	Allow users to save <a href="#">User Specific Settings</a> .
<b>Allow database clean up</b>	Allows logs and deleted history to be cleaned up. For more information, please consult the <a href="#">Clean up</a> topic.
<b>Allow shortcuts</b>	Allow the reiteration of entries through the shortcut feature.
<b>Allow entry states (Lock, Running, Checkout)</b>	Allow entries to be locked when used or edited.

GENERAL	DESCRIPTION
<b>Allow virtual folders</b>	Allow to store entries in virtual folders. (Not supported with Devolutions Server.)
<b>Automatic check in after</b>	Forces checked out entries to check in automatically after a set delay.
<b>Allow sub connections</b>	Allow users to create sub connections.
<b>Add entry mode</b>	<p>Select if users are prompted to choose a template when creating a new entry. Select between:</p> <ul style="list-style-type: none"> <li>• <b>Default</b></li> <li>• <b>Template list (include default)</b></li> <li>• <b>Template list only</b></li> <li>• <b>No template selection</b></li> </ul>
COMMENTS	DESCRIPTION
<b>Allow log comments editing</b>	Enable the log comment editing for all users.
<b>Minimum length (char)</b>	Set the minimum length (in characters) allowed for comments.
FILE SIZE	DESCRIPTION
<b>Maximum file size (MB)</b>	Limit the size of attachments and document entries to avoid to over load the data source.

## 6.7.3.2.1.1 Security

## SETTINGS



System Settings - General - Security

DATA SOURCE SECURITY	DESCRIPTION
<b>Create Vault with restricted access by default</b>	Automatically secure the Vault settings when creating a repository. Therefore, the permissions settings are set to <b>Never</b> .
<b>Force data source 2-factor configuration</b>	Require the users to have a <a href="#">2-factor configuration</a> applied on the data source. Not shown with Devolutions Server as 2FA set elsewhere.
<b>Resolve credentials in overview</b>	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.

DATA SOURCE SECURITY	DESCRIPTION
<b>Use legacy security</b>	Use the old system of managing privileges: security groups.

TIME-BASED USAGE	DESCRIPTION
<b>Time of day</b>	<p>Select the hours which the data source is limited to. Select between:</p> <ul style="list-style-type: none"> <li>• <b>Any time:</b> the session can be used at any hour.</li> <li>• <b>Custom:</b> manually select the time frame the session is available for.</li> </ul>
<b>Time of week</b>	<p>Select which days the data source is available for. Select between:</p> <ul style="list-style-type: none"> <li>• <b>Any day:</b> the session can be used any day of the week or week-end.</li> <li>• <b>Week days:</b> the session can be used only the week days.</li> <li>• <b>Week ends:</b> the session can be used only the week ends.</li> <li>• <b>Custom:</b> manually select each day the session is available for.</li> </ul>
<b>Time Zone</b>	Select the time zone you are currently in.

6.7.3.2.1.2 Allow Password Access From External System

## DESCRIPTION



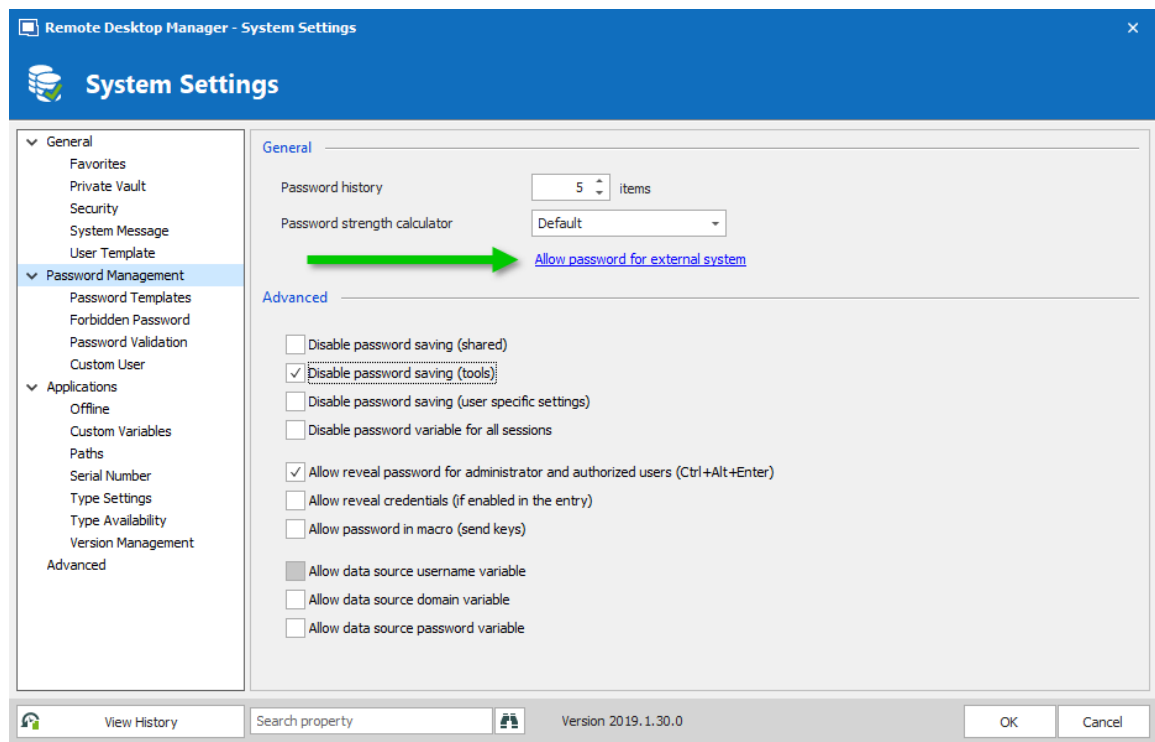
This feature is only available when using an [Advanced Data Source](#).

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.

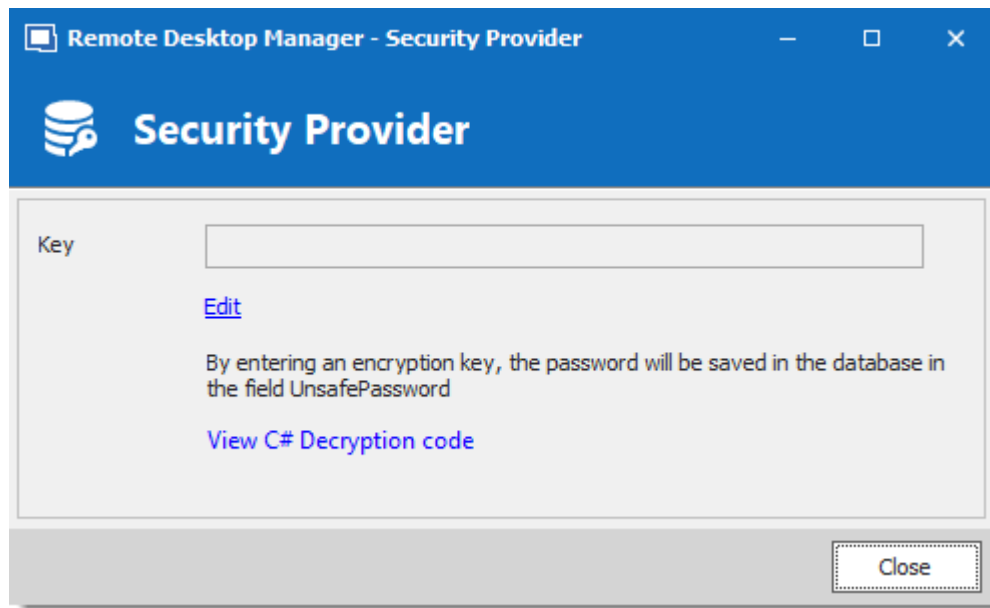
However, getting the encrypted password from the database requires the **Allow password for external system** to be configured.



*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 TripleDESCryptoServiceProvider();
        MD5CryptoServiceProvider cryptoServiceProvider = new MD5CryptoServiceProvider();

        string strTempKey = key;

        byte[] byteHash = cryptoServiceProvider.ComputeHash(Encoding.ASCII.GetBytes(strTempKey));

        tripleDesCryptoServiceProvider.Key = byteHash;

        tripleDesCryptoServiceProvider.Mode = CipherMode.ECB;

        byte[] byteBuff = Convert.FromBase64String(encryptedString);

        string strDecrypted =
            Encoding.UTF8.GetString(
                tripleDesCryptoServiceProvider.CreateDecryptor().TransformFinalBlock(
                    byteBuff, byteBuff.Length, 0));
    }
    catch { }
}
```

```

        byteBuff, 0, byteBuff.Length));

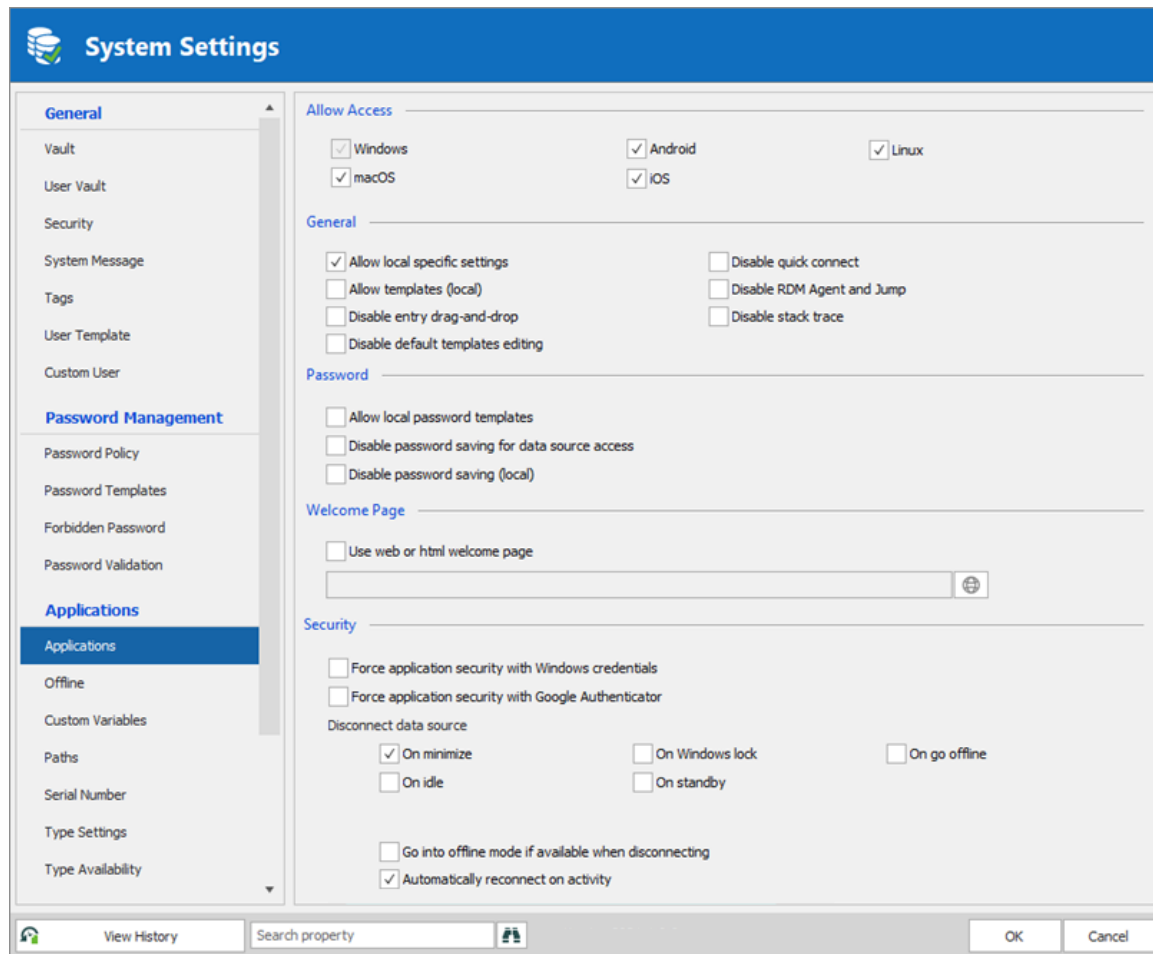
    return strDecrypted;
}
catch (Exception)
{
    return null;
}
}

```

#### 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
<b>Operating systems</b>	Enable access to the data source from the selected operating systems.

GENERAL	DESCRIPTION
<b>Allow local Specific Settings</b>	Allow users to save <a href="#">Local Specific Settings</a> .
<b>Allow templates (local)</b>	Allows to locally save entry's templates.
<b>Disable entry drag-and-drop</b>	Disable entries drag and drop from one folder to another. This setting is useful for avoiding accidental drag and drop.
<b>Disable quick connect</b>	Disable the Quick Connect feature for all users of the data source.
<b>Disable RDM Agent and Jump</b>	Disable the option to activate a session as an RDM Agent or Jump.
<b>Disable stack trace</b>	Disable the stack trace details when an error occurs in Remote Desktop Manager. This is a security feature.

PASSWORD	DESCRIPTION
<b>Allow local password templates</b>	Allows password templates to be saved locally.
<b>Disable password saving for data source access</b>	Prevent users to save or change the passwords stored in the data source configurations.

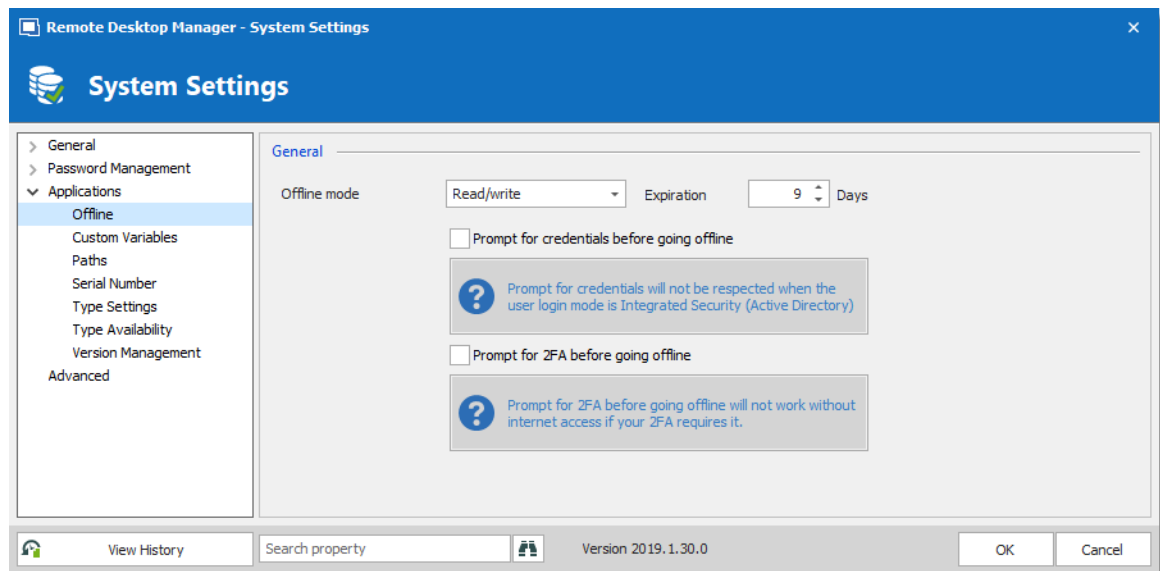


PASSWORD	DESCRIPTION
<b>Disable password saving (local)</b>	Prevent users from saving passwords in the properties of entries.
WELCOME PAGE	DESCRIPTION
<b>Use web or html welcome page</b>	Enter an URL to use as the application's welcome page.
SECURITY	DESCRIPTION
<b>Force application security with Windows credentials</b>	Require the users to authenticate with their Windows credentials at application startup.
<b>Force application security with Google Authenticator</b>	Require the users to authenticate with <a href="#">Google Authenticator</a> at application startup.
<b>Disconnect data source</b>	<p>Set the application to lock:</p> <ul style="list-style-type: none"><li>• <b>On Minimize:</b> lock application when minimized in the taskbar for all users of the data source.</li><li>• <b>On Idle:</b> automatically lock the application when it is not used after a determined amount of time.</li><li>• <b>On Windows lock:</b> lock the application on Windows lock.</li><li>• <b>On standby:</b> lock the application when on standby.</li></ul>
<b>Go into offline mode if available when disconnecting</b>	Will switch RDM from online to offline mode if available when disconnecting.

SECURITY	DESCRIPTION
<b>Automatically reconnect on activity</b>	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
<b>Offline mode</b>	Set the global data source <a href="#">Offline Mode</a> availability. The offline mode is useful when using a VPN connection that makes using local network impossible.
<b>Expiration</b>	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
<b>Prompt for credentials before going offline</b>	Force the user to provide their credentials before going offline.
<b>Prompt for 2FA before going offline</b>	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 Serial Number

## DESCRIPTION

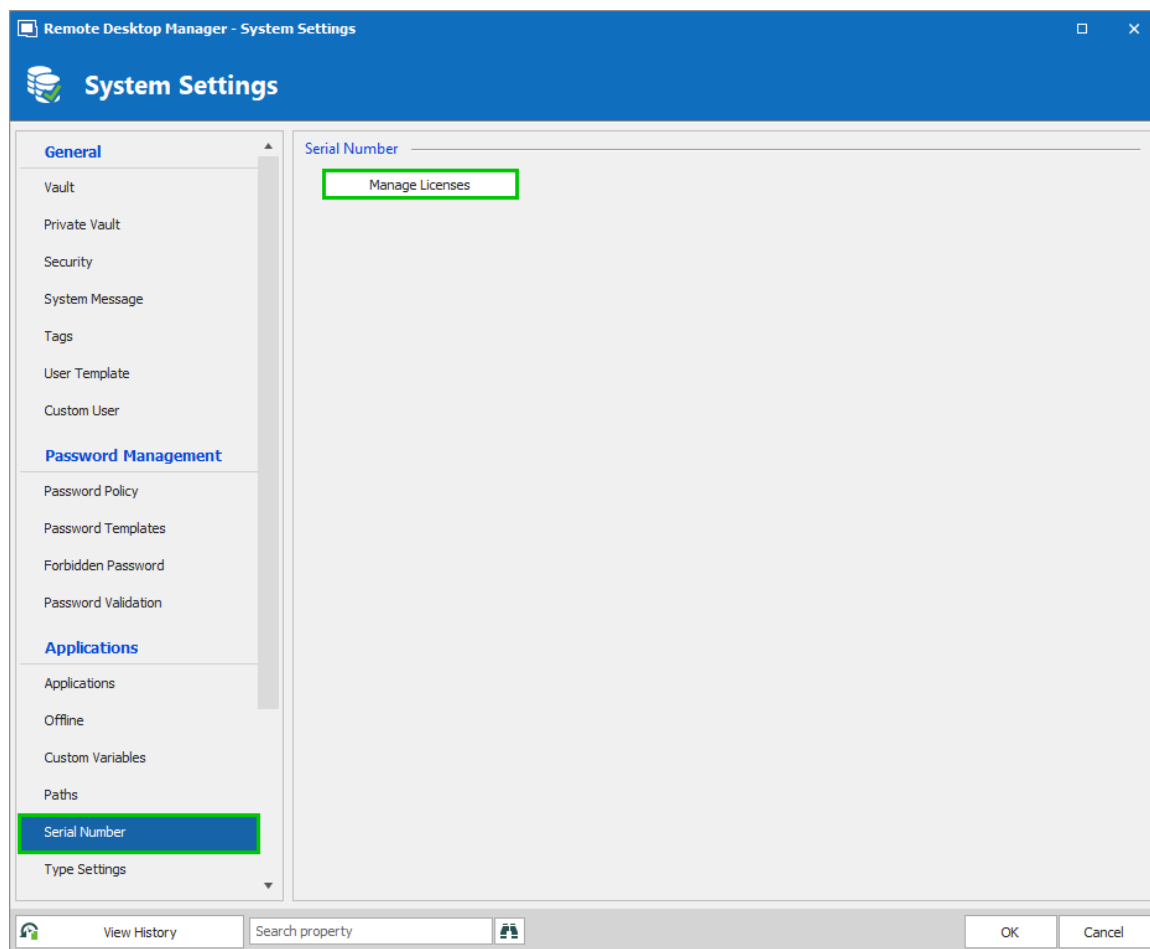
Store an Enterprise Edition Site or Global **License** serial to share in the data source.



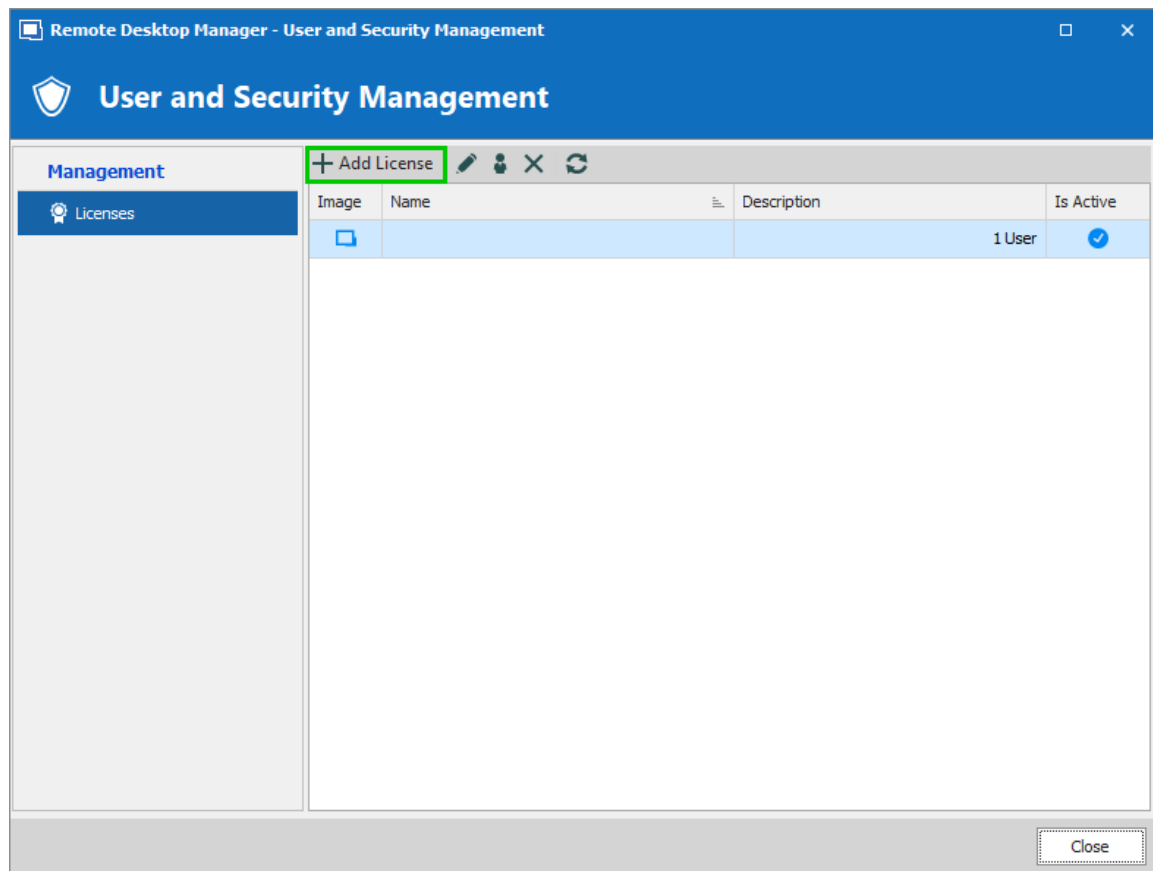
When you add a data source with a saved serial in an unregistered version of Remote Desktop Manager, the license serial is automatically retrieved from data source settings.

## SETTINGS

You can manage your licenses through a shortcut in **Administration - System settings - Serial Number**.



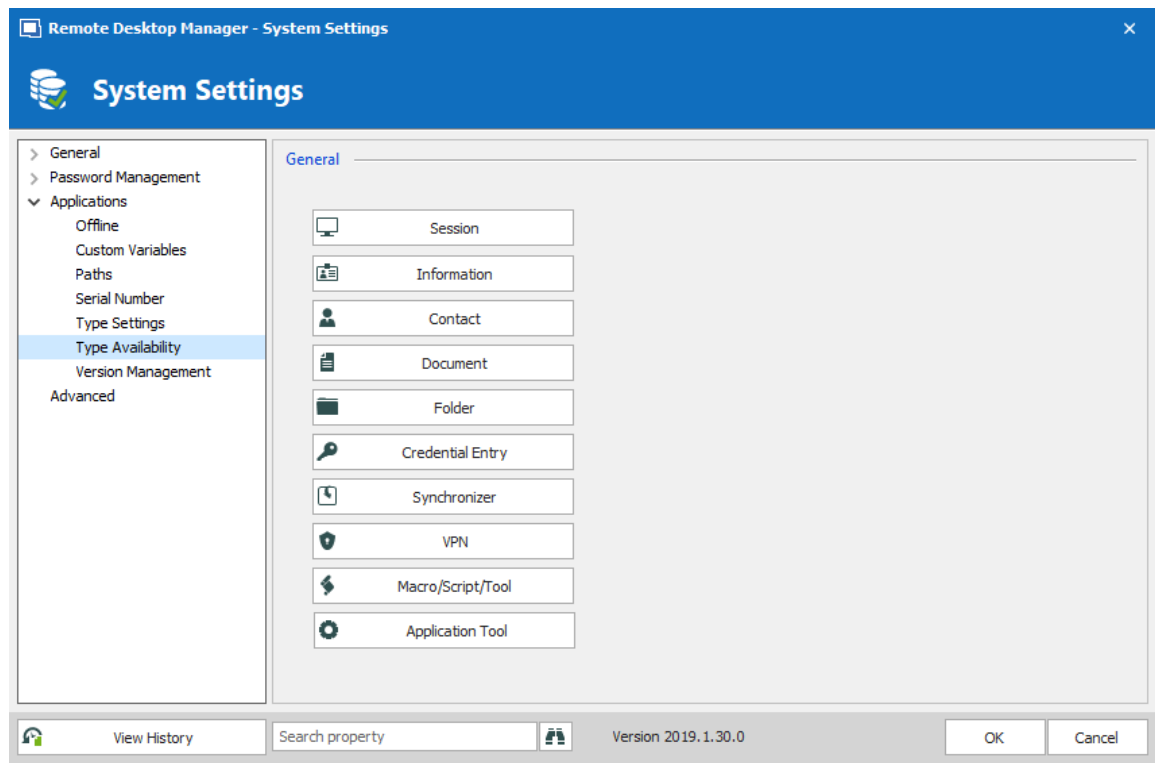
*System Settings - Serial Number*



*User and Security Management - Add License*

6.7.3.2.3 Type availability

## SETTINGS



*System Settings - Types - Availability*

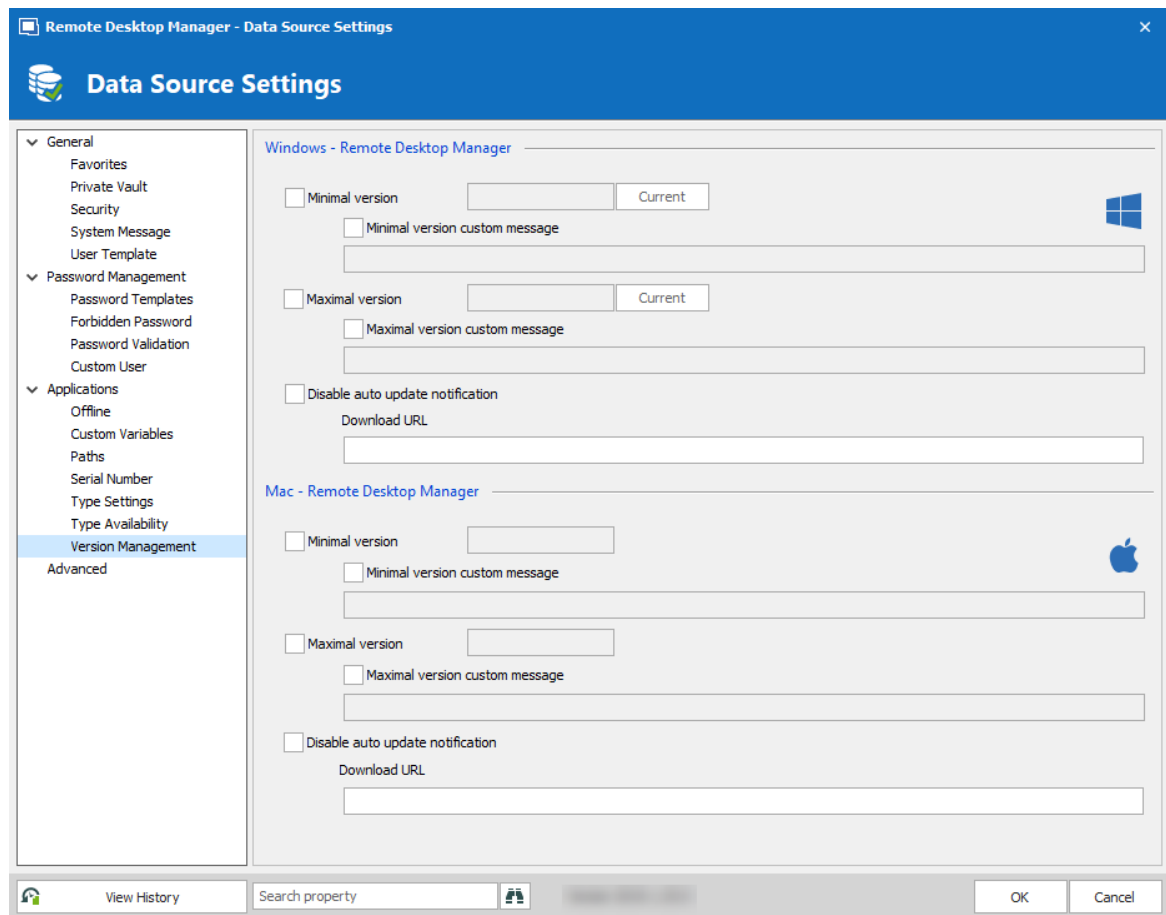
OPTION	DESCRIPTION
<b>Type Availability</b>	Select entry types to exclude. Excluded entries will not be in the <b>Add New Entry</b> window.

#### 6.7.3.2.2.4 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
<b>Minimal version</b>	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.
<b>Minimal version custom message</b>	Enter a custom message for the minimal version notification.
<b>Maximal version</b>	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.

OPTION	DESCRIPTION
<b>Maximal version custom message</b>	Enter a custom message for the maximal version notification.
<b>Disable auto update notification</b>	Disable the auto update notification message. Use this to manually update the application and prevent from getting notified when new versions are available.
<b>Download URL</b>	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

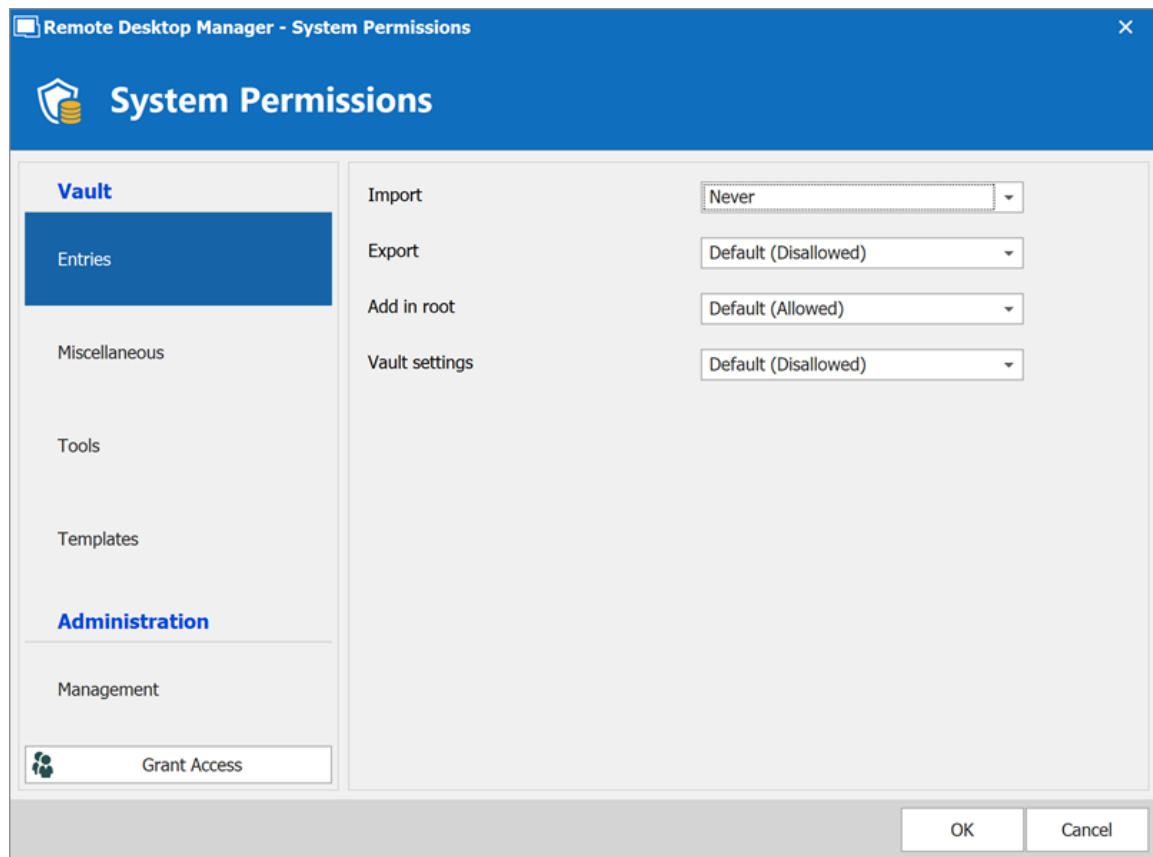
The **System Permissions** allows to grant some administrative permissions to standard users without making them administrators. The **Default** setting inherits the permission set on the user or user groups. For more information about permissions, consult General Security.



This feature is only available when using an [Advanced Data Source](#).

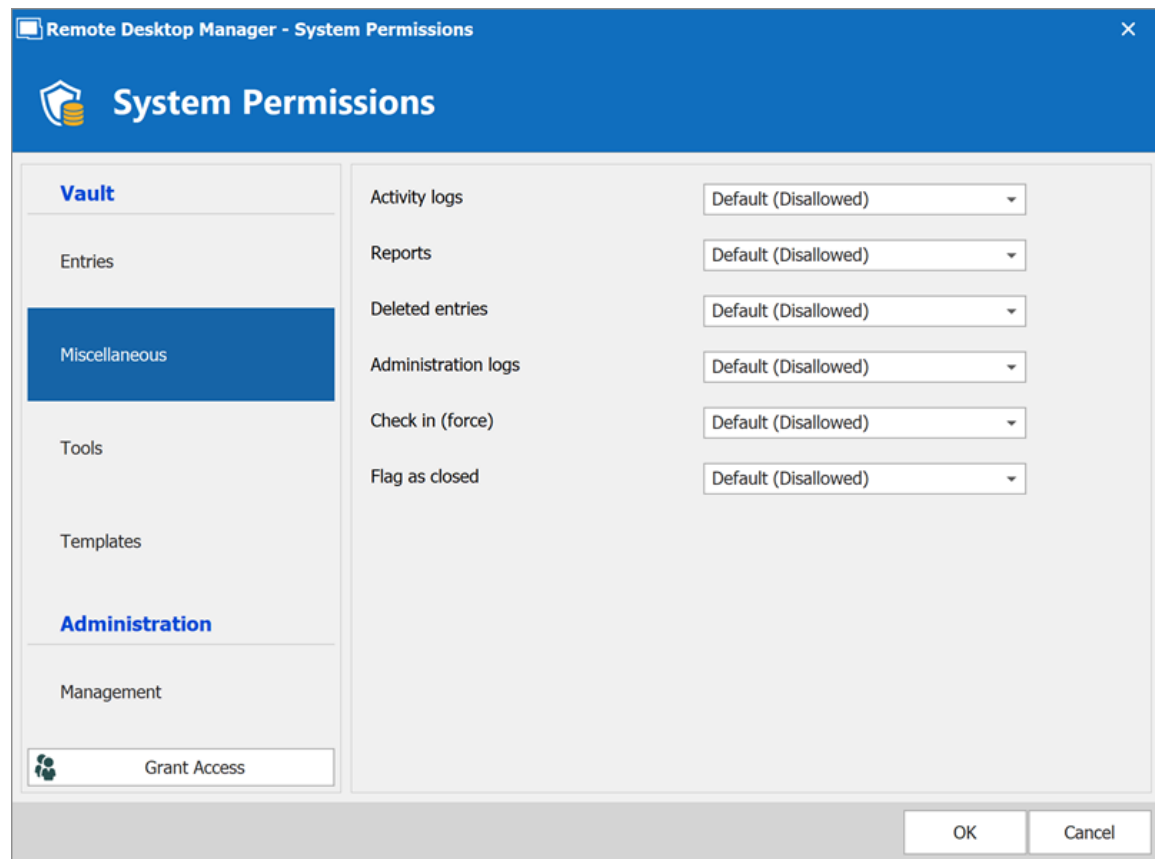
## ENTRIES



*System Permissions - Entries*

OPTION	DESCRIPTION
<b>Import</b>	Allow users/user groups to import entries in the data source.
<b>Export</b>	Allow users/user groups to export from the data source.
<b>Add in root</b>	Allow users/user groups to create entries in the root folder.
<b>Vault settings</b>	Allow users/user groups to access the Vault properties.

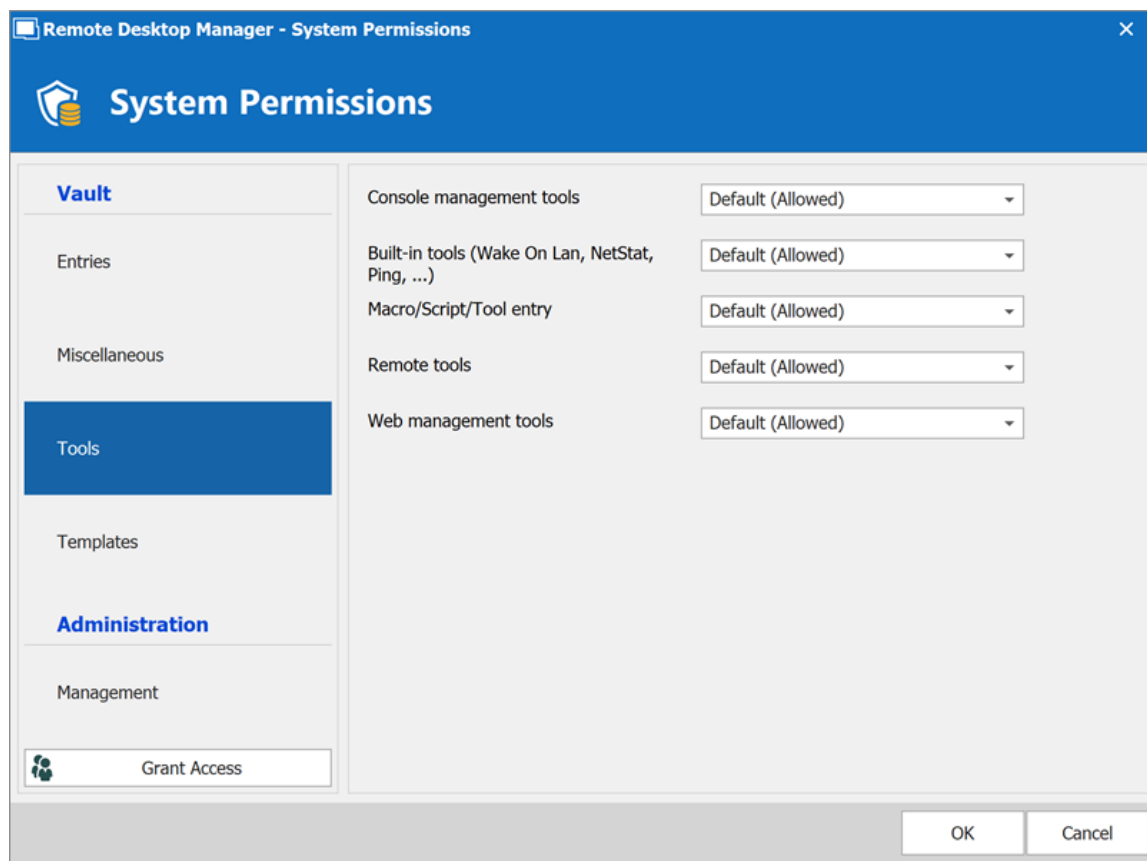
## MISCELLANEOUS



System Permissions - Miscellaneous

OPTION	DESCRIPTION
<b>Activity logs</b>	Allow users/user groups to view the activity logs.
<b>Reports</b>	Allow users/user groups to generate and view reports.
<b>View deleted entries</b>	Allow users/user groups to view and restore deleted entries.
<b>View administration logs</b>	Allow users/user groups to view the administration logs.
<b>Check in (force)</b>	Allow users/user groups to check in entries with the checked out state.

## TOOLS



*System Permissions - Tools*

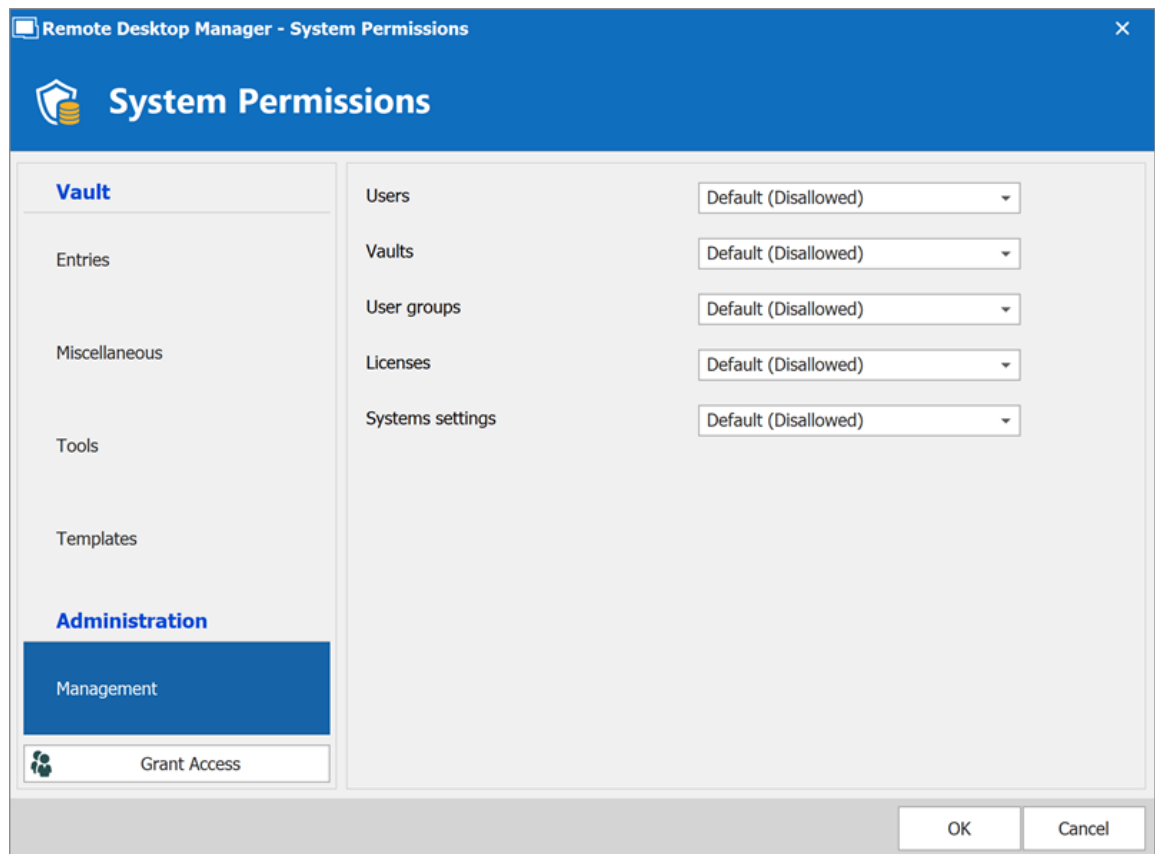
OPTION	DESCRIPTION
<b>Console management tools</b>	Allow users/user groups to use console management tools.
<b>Built-in tools (Wake-on-LAN, NetStat, Ping, ...)</b>	Allow users/user groups to use session related tools.
<b>Macros/Scripts/Tools entry</b>	Allow users/user groups to use Macros/Scripts/Tools entries.

OPTION	DESCRIPTION
<b>Management Tools</b>	Allow users/user groups to use Management Tools.
<b>Web management tools</b>	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.
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.



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 especially Devolutions Online Database.



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

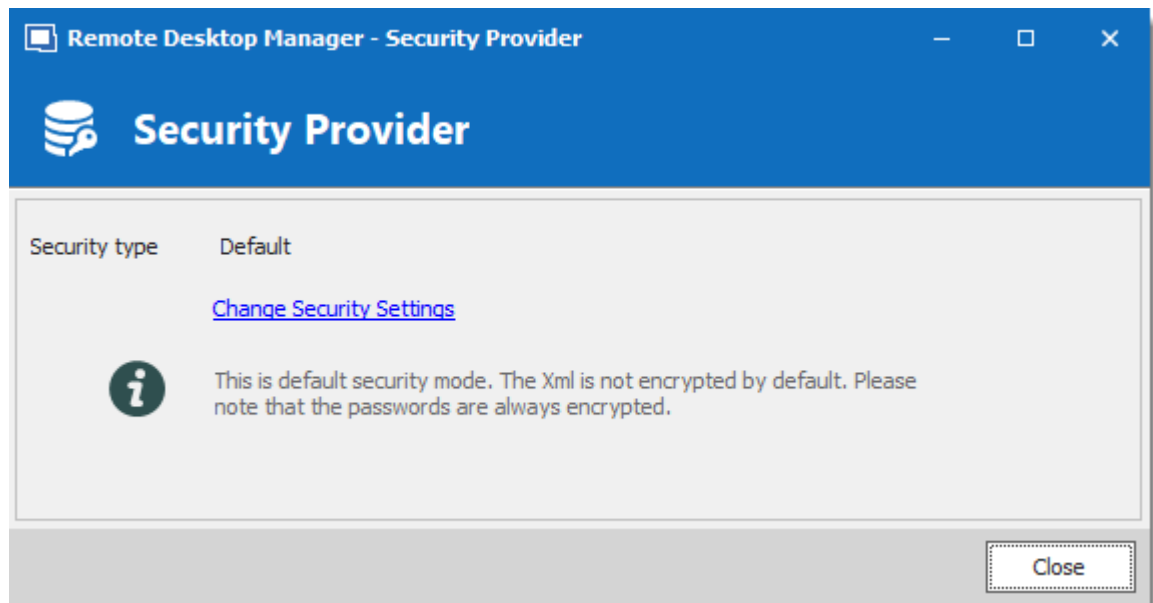


Please note that changing a security provider on a data source with a great number of entries is a lengthy operation.



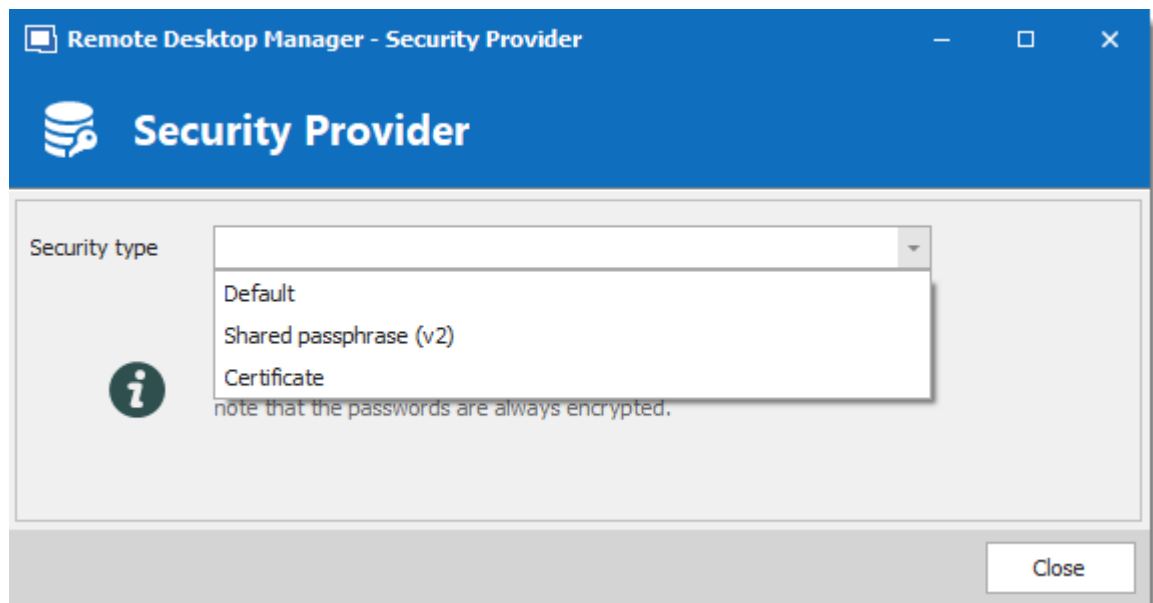
Applying a new security provider does process the whole database, therefore we advise you to create a backup prior to this operation.

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
<b>Default</b>	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
<b>Shared passphrase</b>	Set up a shared passphrase for the Security Provider.
<b>Certificate</b>	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*

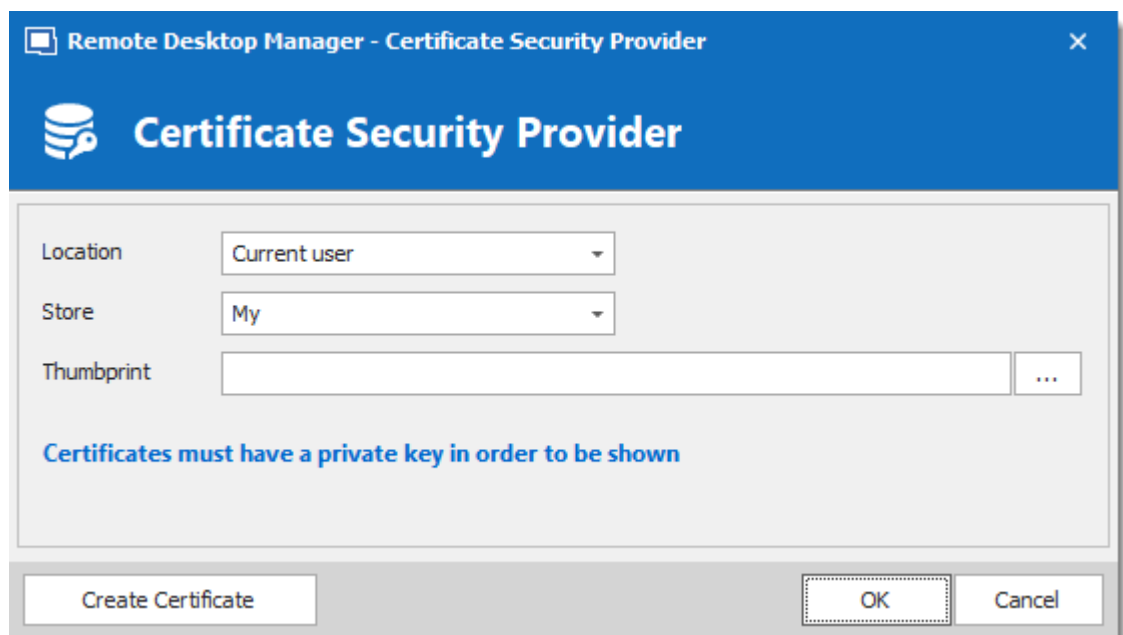
Entries configuration data is encrypted using a mix of a key stored in Remote Desktop Manager and the passphrase you've entered.



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. For more information, please consult the [How to modify Group Policy Templates](#) topic.

## 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
<b>Location</b>	Indicate the certificate location. Select between: <ul style="list-style-type: none"><li>• <b>Current user</b></li><li>• <b>Local machine</b></li></ul>
<b>Store</b>	Indicate the store location of the certificate. Select between: <ul style="list-style-type: none"><li>• <b>Address book</b></li></ul>

OPTION	DESCRIPTION
	<ul style="list-style-type: none"><li>• <b>Authorization root</b></li><li>• <b>Certificate authority</b></li><li>• <b>Disallowed</b></li><li>• <b>My</b></li><li>• <b>Root</b></li><li>• <b>Trusted people</b></li><li>• <b>Trusted publisher</b></li></ul>
<b>Thumbprint</b>	Select an existing certificate.

## CREATE CERTIFICATE

It is possible to create a Self Signed certificate by clicking on **Create Certificate**.

Remote Desktop Manager - Self Signed Certificate

## Self Signed Certificate

Common name: localhost

Key size (bits): 2048

Valid from: 6/12/2019

Valid to: 6/19/2029

☒ Save to file (pfx)

Password:

☐ Save to certificate store

Location: Current user

Store: My

Save Cancel

*Self Signed Certificate*

OPTION	DESCRIPTION
<b>Common name</b>	Name of the certificate.
<b>Key size (bits)</b>	Indicate the key size (bits) of the certificate. Select between: <ul style="list-style-type: none"><li>• 384</li><li>• 512</li><li>• 1024</li><li>• 2048</li><li>• 4096</li></ul>

OPTION	DESCRIPTION
	<ul style="list-style-type: none"><li>• 8192</li><li>• 16384</li></ul>
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.



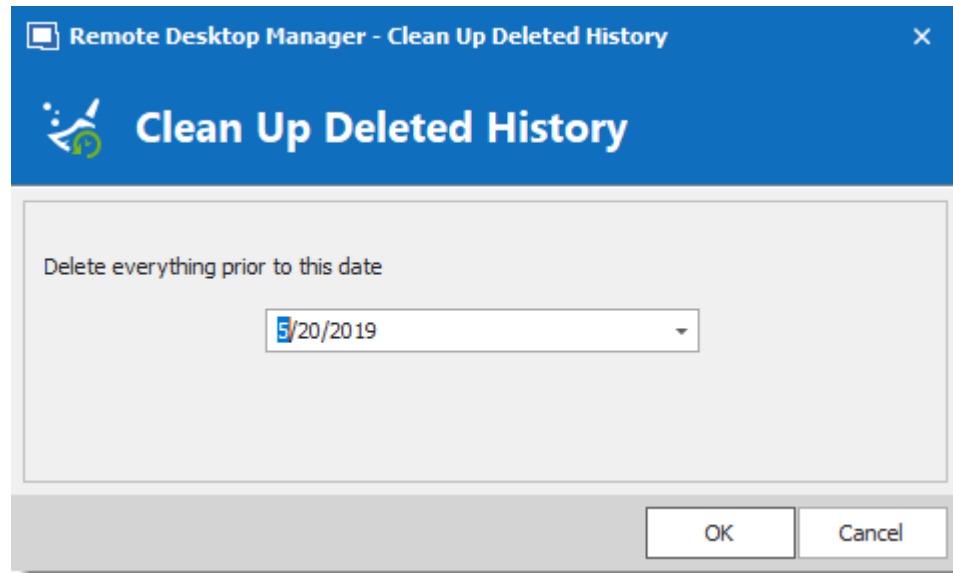
This feature requires an [Advanced Data Source](#).



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

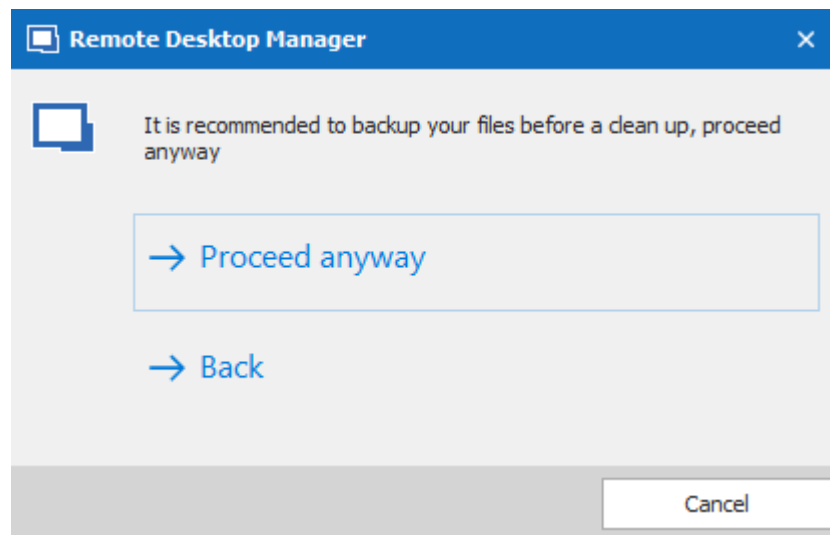
### SETTINGS

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**.



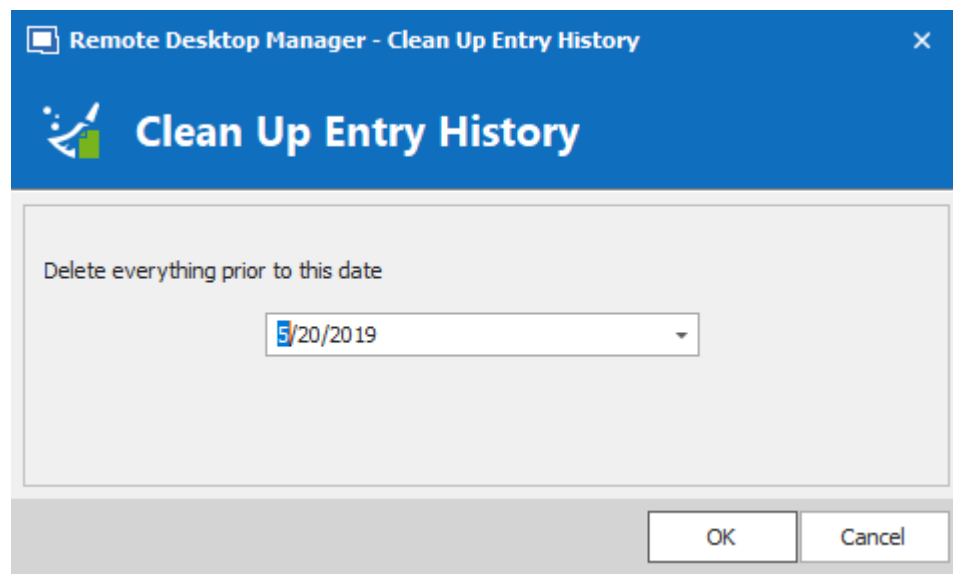
This feature requires an [Advanced Data Source](#).



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

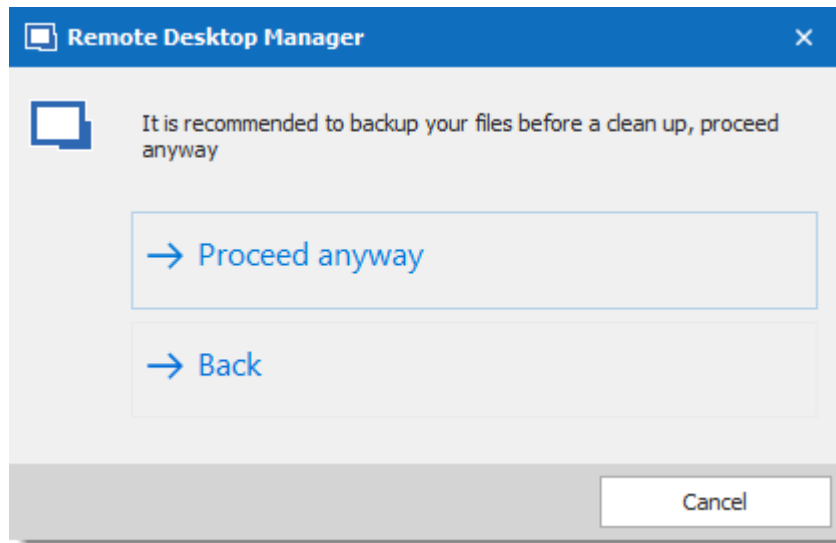
### SETTINGS

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..



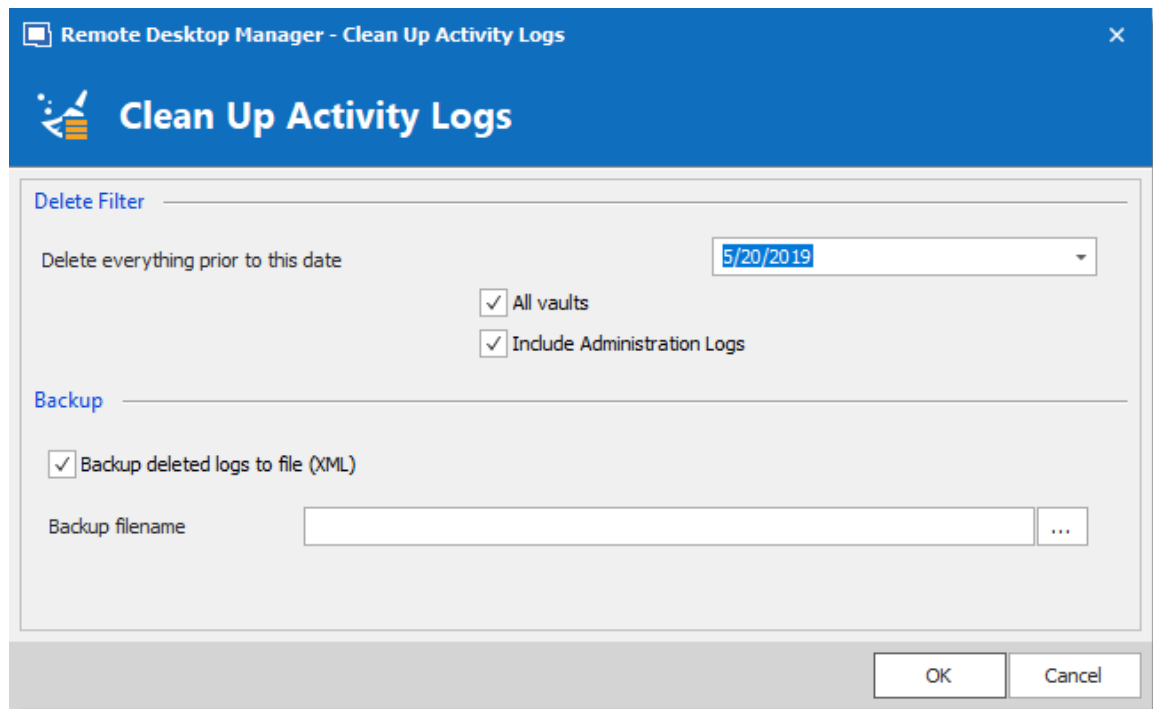
This feature requires an [Advanced Data Source](#).



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.



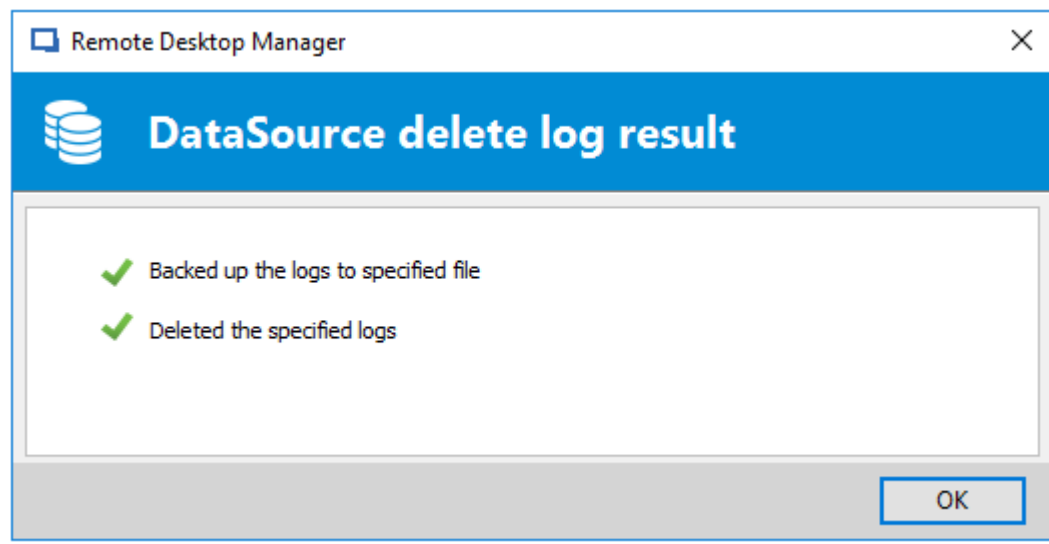
*Clean up Data Source logs*



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*

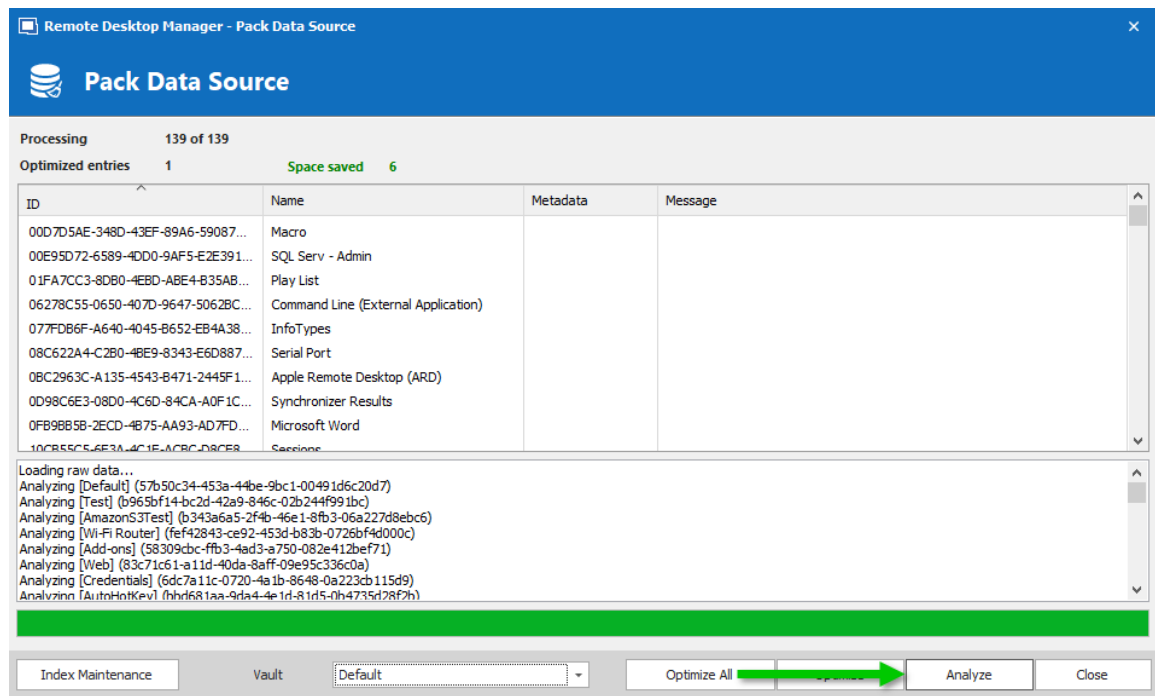
#### 6.7.4.4 Pack Data Source (Optimize)

### 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**.



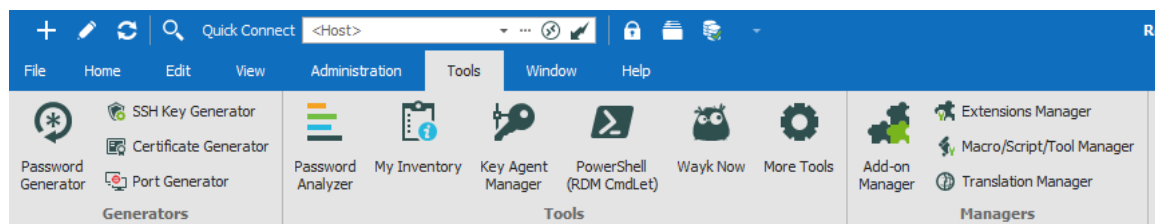
*Pack Data Source (Optimize) - Analyze*

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**.

## 6.8 Tools

### DESCRIPTION

The **Tools** tab contains your Add-on and Extensions manager as well as your Devolutions Server Console, Generators and multiple useful tools.



*Ribbon - Tools*

## GENERATORS

OPTION	DESCRIPTION
<b>Password Generator</b>	Opens the <a href="#">Password Generator</a> window. You can use this to generate password according to pre-determined criteria for better security.
<b>SSH Key Generator</b>	Launches the <a href="#">SSH Key Generator</a> . SSH keys provide a secure way of logging into a virtual private server with SSH than using a password alone.
<b>Certificate Generator</b>	Launches the <a href="#">Certificate Generator</a> . 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.
<b>Port Generator</b>	Launches the <a href="#">Port Generator</a> . With this you can generate ports for your connections.

## TOOLS

OPTION	DESCRIPTION
<b>Password Analyzer</b>	Opens the <a href="#">Password Analyzer</a> . This is used to evaluate the strength of passwords stored in the data source. This feature is restricted to Administrators only.
<b>My Inventory</b>	Set up a My Inventory report.
<b>Key Agent Manager</b>	Opens the <a href="#">Key Agent Manager</a> . This is used to hold all your SSH Keys in memory, already decoded and ready for them to be used.

OPTION	DESCRIPTION
<b>PowerShell (RDM CmdLet)</b>	Opens the <a href="#">PowerShell (RDM CmdLet)</a> .
<b>Wayk Bastion</b>	Launches the application.
<b>More Tools</b>	The <b>More Tools</b> window contains a variety of application tools such as: <a href="#">Chocolatey Console</a> , <a href="#">Local RDP/RemoteApp Manager</a> , <a href="#">Playback (Ansi)</a> , <a href="#">RDM Agent</a> and more.

## MANAGERS

OPTION	DESCRIPTION
<b>Add-on Manager</b>	Opens the Add-on Manager. It is used to simplify the management of different add-ons.
<b>Extensions Manager</b>	Opens the Extensions Manager. This is used to simplify the management and installation of Web Browser extensions and other miscellaneous extensions.
<b>Macros/Scripts/Tools Manager</b>	Opens the Macros/Scripts/Tools Manager. This is used to simplify the import of some pre-determined sessions tools.
<b>Translation Manager</b>	Opens the Translation Manager. A cloud based translation repository that is managed by an external application named Devolutions Localizer.

## 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.

Remote Desktop Manager - Password Generator

**Password Generator**

Template: Default + X

Mode: Default

Minimum length: 8

Minimum lowercase characters: 1

Minimum uppercase characters: 1

Minimum numeric characters: 3

Minimum symbols: 1

B4m78v-K	xYq345t-	-i4z-24K	j2yD3A4-
7-L80dhI	bj-F24C5	7j-62lPY	tv6nV-51
d_y352cK	U6_7v06p	5D01s_yD	593WzZ_N
KT6_o00m	U10_Rz7u	W_6et1S0	1wc_8sU6
@66P6knt	p002.Qbp	7G5H22.f	@N7n7a,7
6u74/XO1	K6T+10yV	e455%Y4G	!50L9rD#

Generate

Copy to Clipboard

Very Strong

BRAVO | four | mike | seven | eight | victor | hyphen | KILO

Count: 30

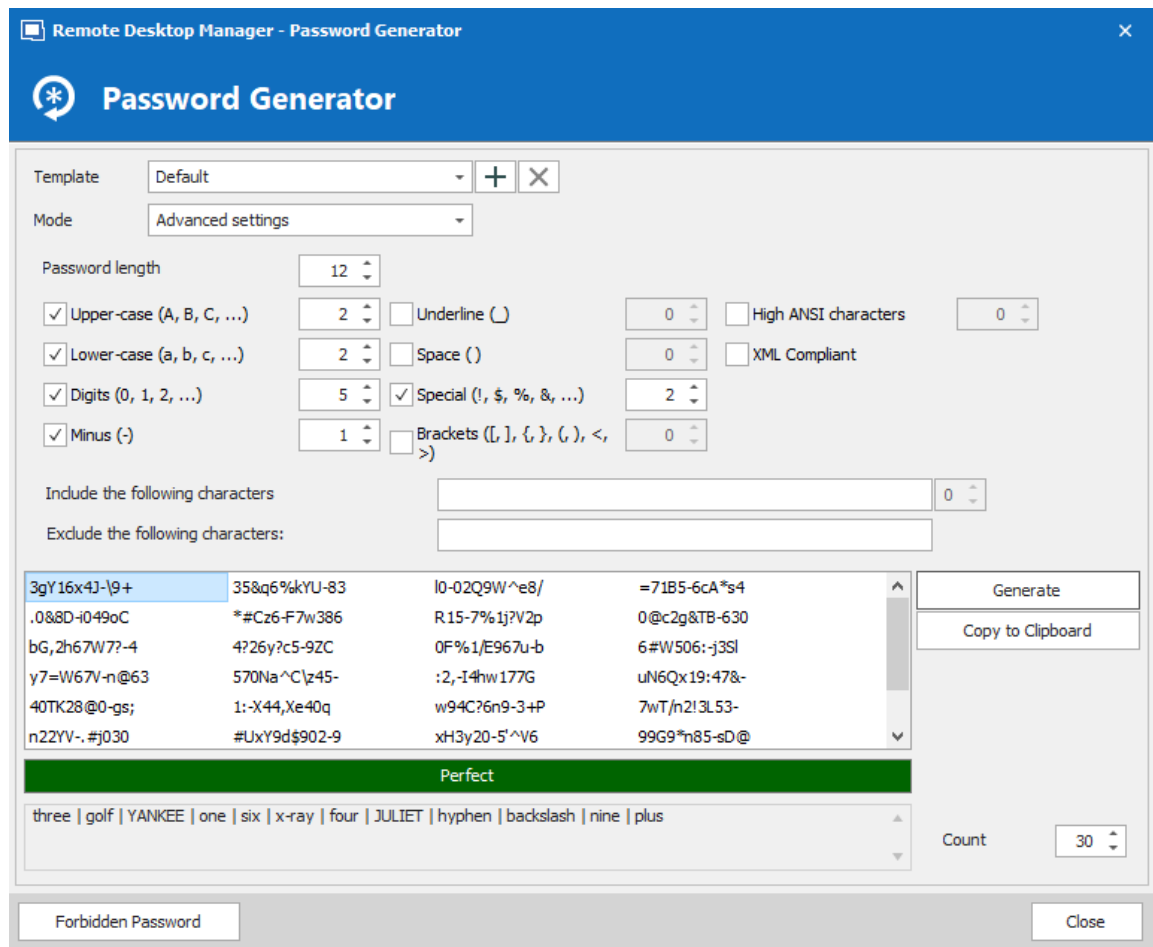
Forbidden Password

Close

*Password Generator - Default*

## ADVANCED SETTINGS

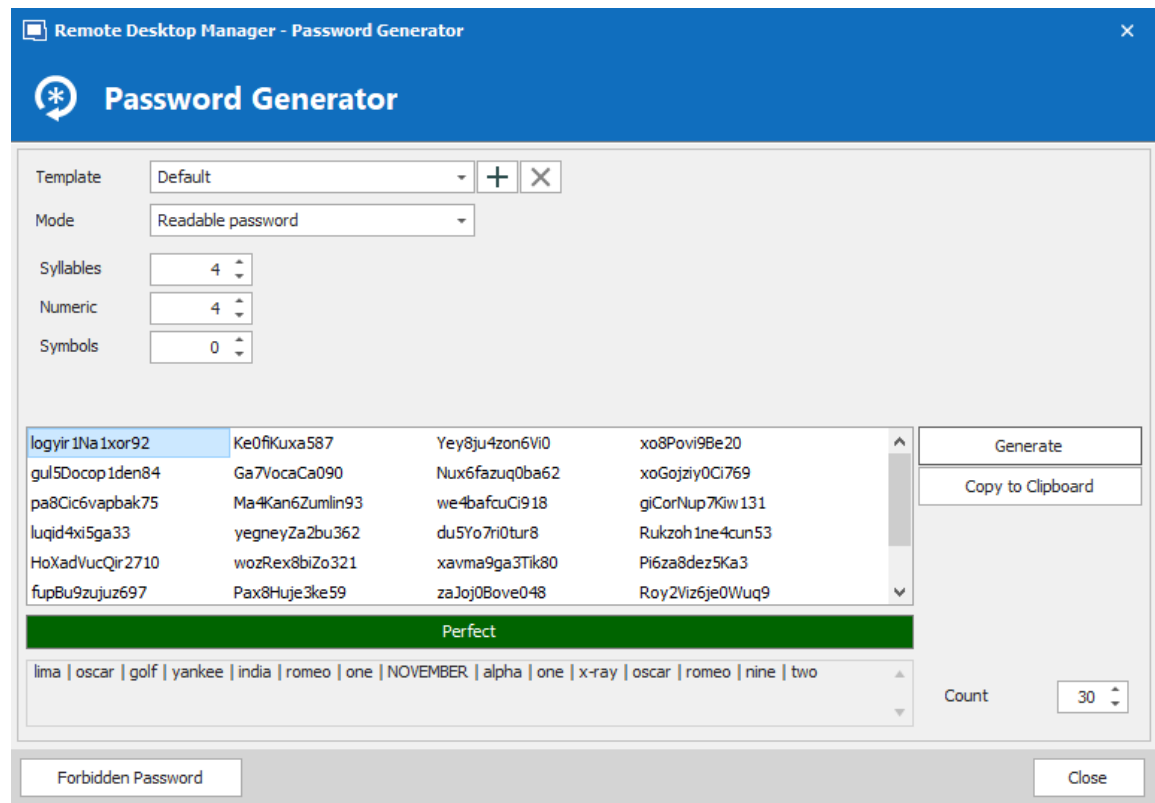
Select the type and amount of characters to include in the password.



*Password Generator - Advanced Settings*


## READABLE PASSWORD

Generate passwords that are readable but are not actual words.

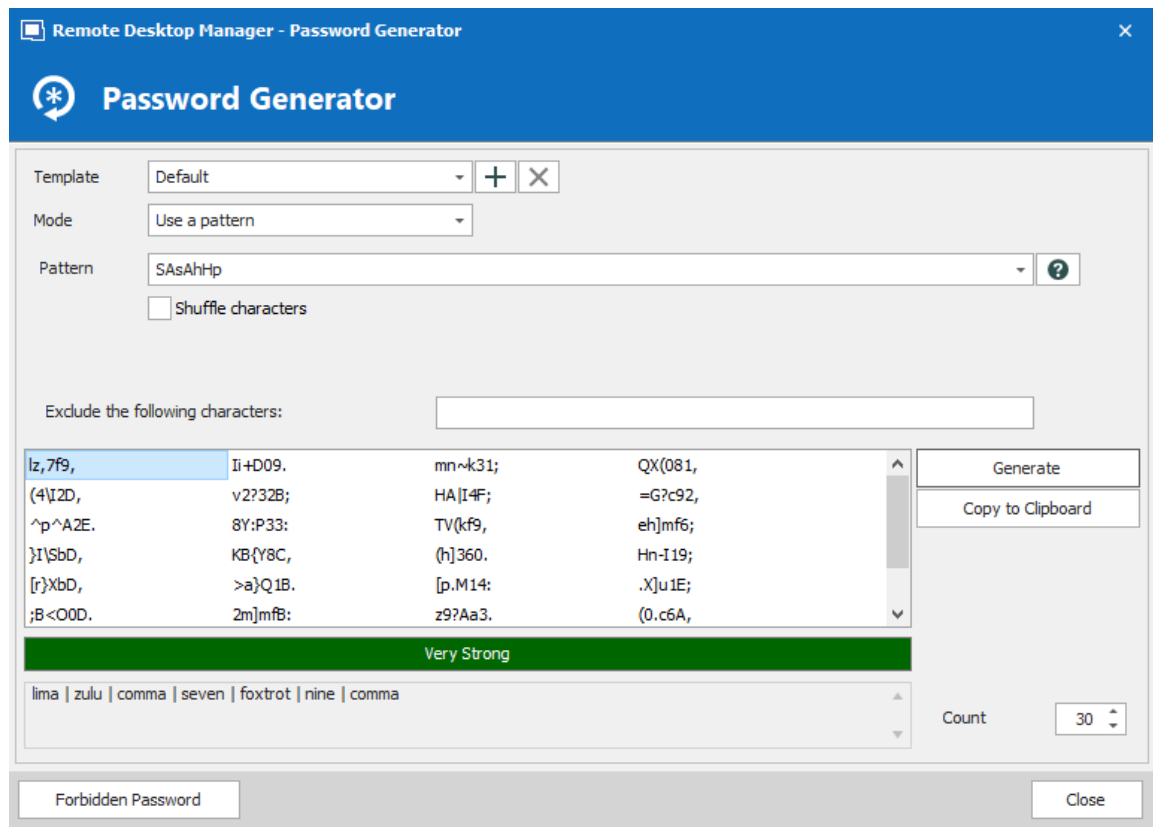


*Password Generator - Readable password*

## 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:

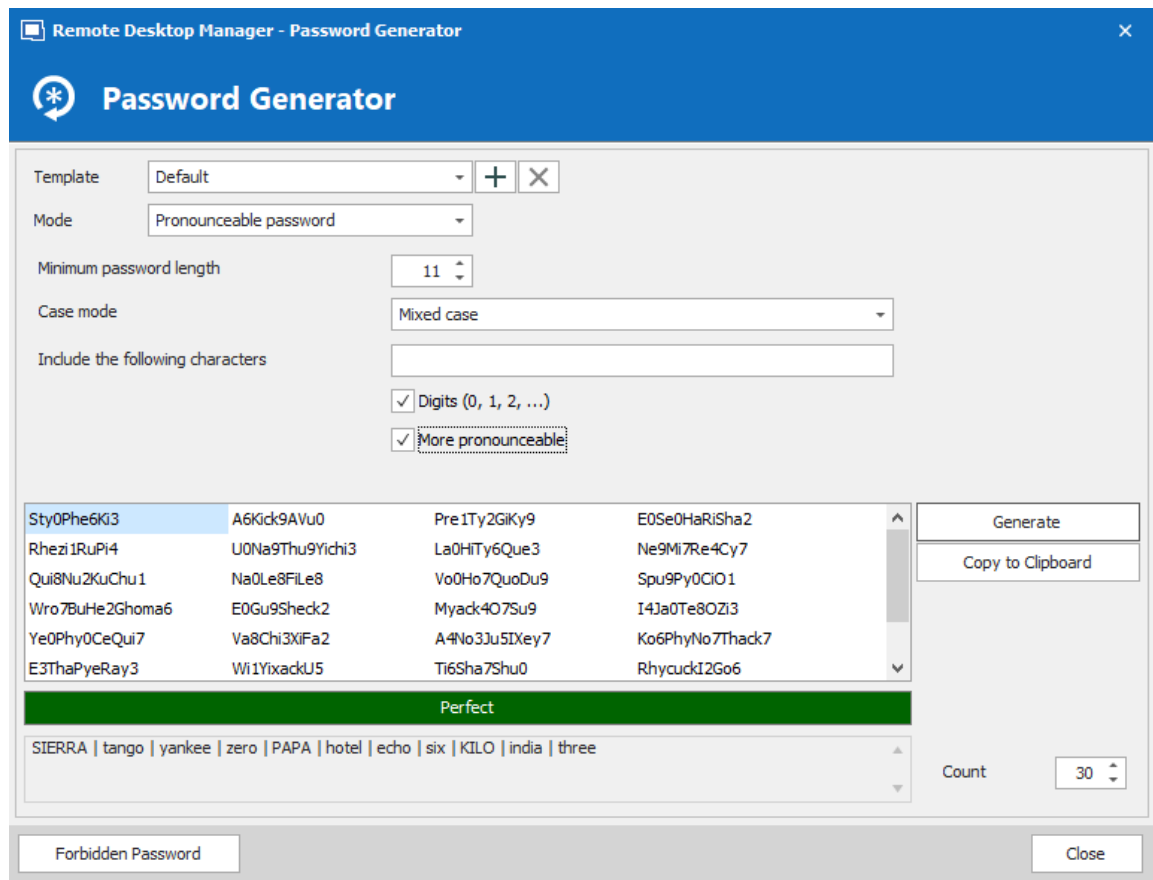
DESCRIPTION	KEY	SAMPLE
<b>Lower-Case Alphanumeric</b>	a	abcdefghijklmnopqrstuvwxyz 0123456789
<b>Mixed-Case Alphanumeric</b>	A	ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefgh ijklmnopqrstuvwxyz 0123456789
<b>Bracket</b>	b	()[]{}<>
<b>Lower-Case Consonant</b>	c	bcd fghjklmnpqrstvwxyz
<b>Mixed-Case Consonant</b>	C	BCDFGHJKLMNPQRSTUVWXYZ bcd fghjklmnpqrs twxyz

DESCRIPTION	KEY	SAMPLE
<b>Digit</b>	d	123456789
<b>Lower-Case Hex Character</b>	h	0123456789 abcdef
<b>Upper-Case Hex Character</b>	H	0123456789 ABCDEF
<b>Lower-Case Letter</b>	l	abcdefghijklmnopqrstuvwxyz
<b>Mixed-Case Letter</b>	L	ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefgh ijklmnopqrstuvwxyz
<b>Punctuation</b>	p	,.::
<b>Printable 7-Bit Special Character</b>	s	!"#\$%&'()*+,-./:;<=>?[ \^_{}~
<b>Printable 7-Bit ASCII</b>	S	A-Z, a-z, 0-9, !"#\$%&'()*+,-./:;<=>?[ \^_{}~
<b>Upper-Case Letter</b>	u	ABCDEFGHIJKLMNOPQRSTUVWXYZ
<b>Upper-Case Alphanumeric</b>	U	ABCDEFGHIJKLMNOPQRSTUVWXYZ 0123456789
<b>Lower-Case Vowel</b>	v	aeiou
<b>Mixed-Case Vowel</b>	V	AEIOU aeiou
<b>High ANSI</b>	x	From '~' to U255 (excluding U255)

DESCRIPTION	KEY	SAMPLE
<b>Upper-Case Consonant</b>	z	BCDFGHJKLMNPQRSTVWXYZ
<b>Upper-Case Vowel</b>	Z	AEIOU
<b>Escape (Fixed Char)</b>	\	Use following character as is
<b>Escape (Repeat)</b>	{n}	Repeats the previous character n times
<b>Custom character</b>	[x]	Define a custom character sequence

## PRONOUNCEABLE PASSWORD

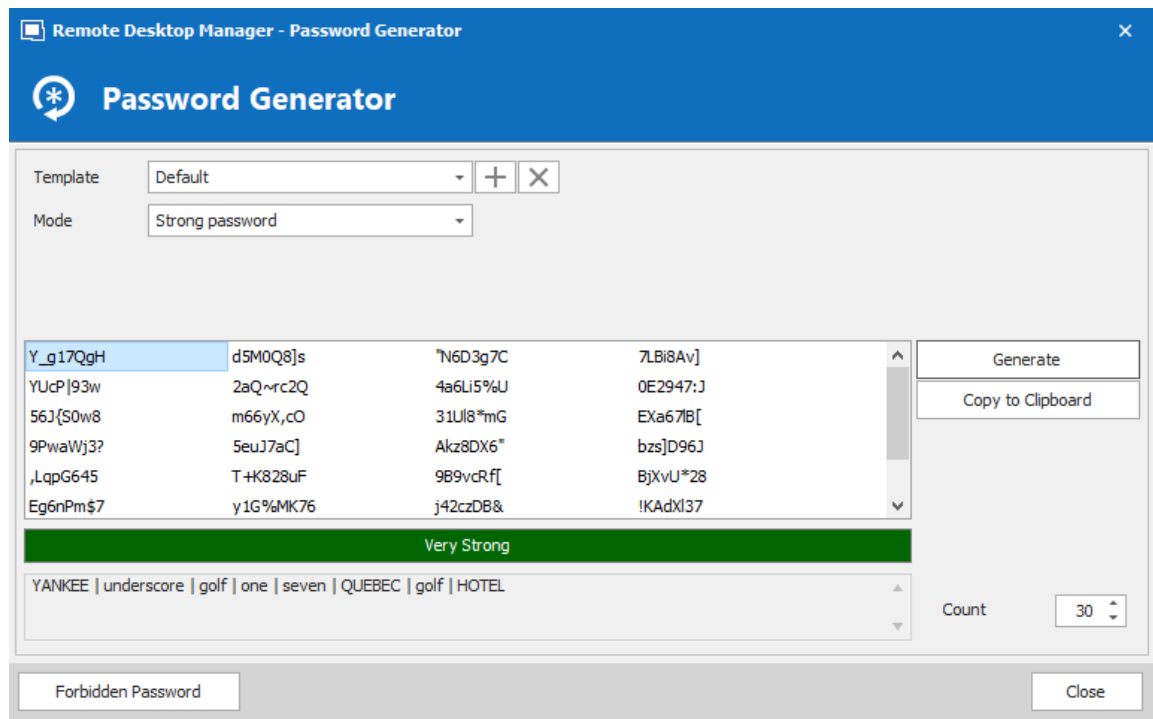
Generate passwords that are pronounceable, but are not actual words.



*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
<b>Key algorithm</b>	<p>You can choose between:</p> <p><b>RSA:</b> 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.</p> <p><b>DSA:</b> It is faster in signing but slower in verifying. It can only be used for signing/verification it <b><u>does not encrypt/decrypt</u></b>. When using DSA it is a recommended to use a 1024 bits key size.</p>
<b>Key size</b>	You can choose your SSH Key size between:

OPTION	DESCRIPTION
	<b>1024 bits:</b> Minimum key size <b>2048 bits:</b> Default and recommended key size <b>4096 bits:</b> Maximum key size
<b>Comment</b>	Enter your username and the name of the computer you're transferring your key to.
<b>Load Private Key</b>	This feature will allow you to import a previously saved SSH Key.
<b>Save Public Key</b>	Saving the public key will generate a *.pub file. Simply enter a file name when prompted.
<b>Save Private Key</b>	You will have the option of saving your Private Key in different format, choose between: <ul style="list-style-type: none"><li>• PKCS #8 Private Key (*.pri)</li><li>• PuTTY Private Key (*.ppk)</li><li>• OpenSSH Private Key (*.pri)</li></ul>

If you did not specify a passphrase you will have to confirm that you do not wish to use a passphrase.



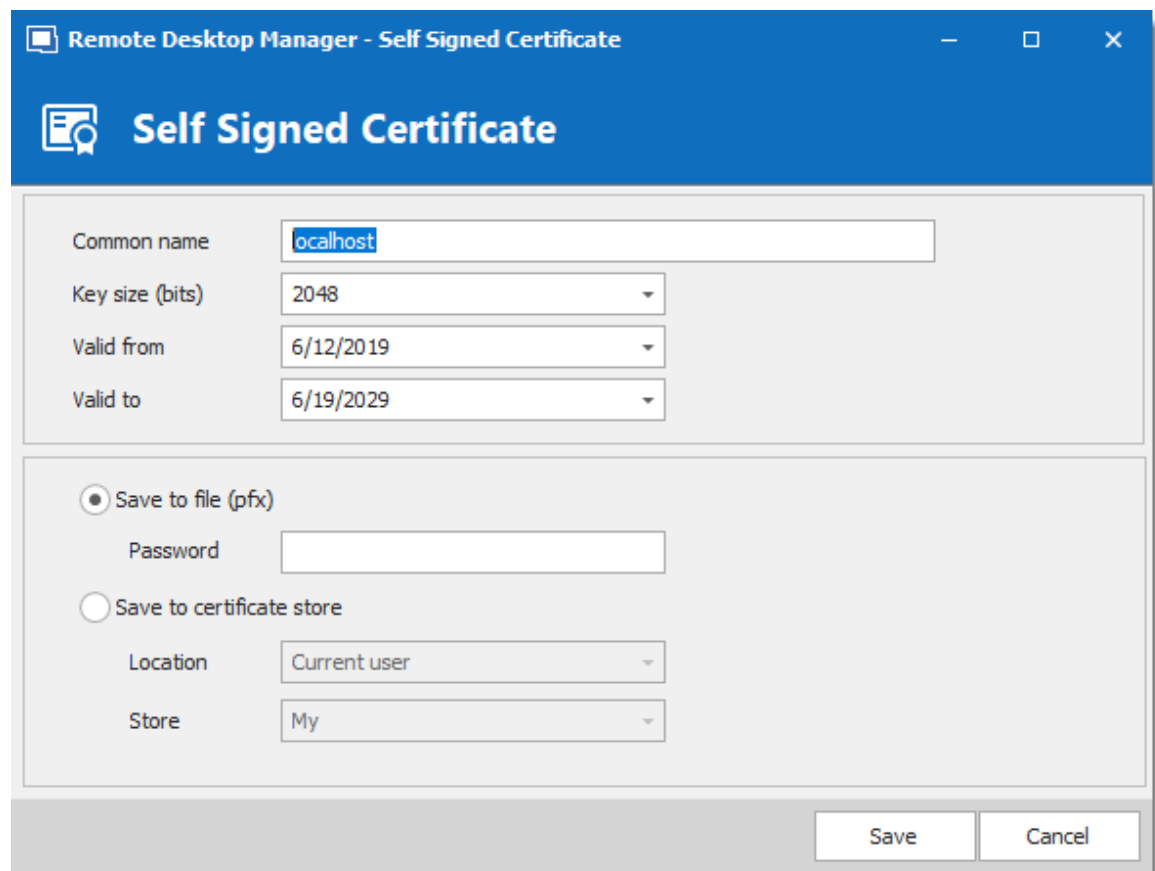
If using the [Key Agent Manager](#) you must chose the PuTTY Private Key (.ppk) file format or the OpenSSH Private Key (.pri) file format. The PKCS Private Key is not a supported file format for the Key Agent Manager.

### 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



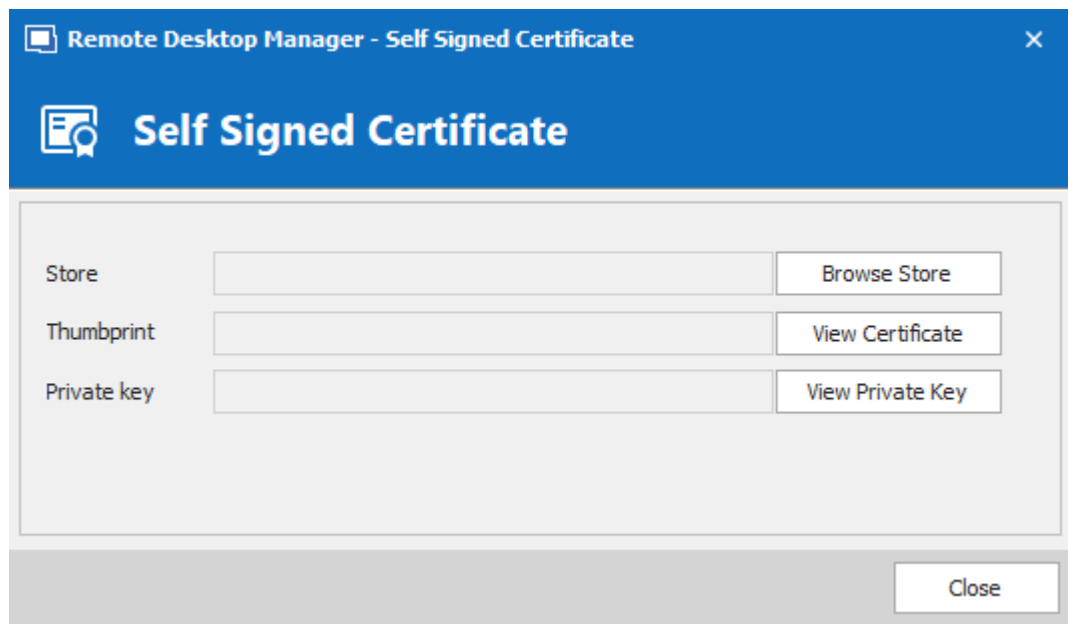
*Certificate Generator - Self Signed Certificate*

OPTION	DESCRIPTION
<b>Common name</b>	Name of the certificate.
<b>Key size (bits)</b>	Indicates the key size (bits) of the certificate. Select between: <ul style="list-style-type: none"><li>• 1024</li><li>• 2048</li></ul>



OPTION	DESCRIPTION
	<ul style="list-style-type: none"><li>• <b>4096</b></li><li>• <b>8192</b></li><li>• <b>16384</b></li></ul>
<b>Valid from</b>	Starting date of the certificate.
<b>Valid to</b>	Expiration date of the certificate.
<b>Save to file (pfx)</b>	Save the certificate into a *.pfx file and secure this certificate with a password.
<b>Save to certificate store</b>	Indicate the location and the store to save the certificate.
<b>Location</b>	Indicate the location of the certificate. Select between: <ul style="list-style-type: none"><li>• <b>Current user</b></li><li>• <b>Local machine</b></li></ul>
<b>Store</b>	Indicate the store location of the certificate. Select between: <ul style="list-style-type: none"><li>• <b>Address book</b></li><li>• <b>Authorization root</b></li><li>• <b>Certificate authority</b></li><li>• <b>Disallowed</b></li><li>• <b>My</b></li><li>• <b>Root</b></li><li>• <b>Trusted people</b></li></ul>

OPTION	DESCRIPTION
	<ul style="list-style-type: none"> <li>• <b>Trusted publisher</b></li> </ul>



Self Signed Certificate

OPTION	DESCRIPTION
<b>Store</b>	Indicate the store where the certificate will be located.
<b>Browse Store</b>	Browse the store that is indicated in the store field.
<b>Thumbprint</b>	Display the certificate thumbprint.
<b>View Certificate</b>	Display the certificate that you have created.
<b>Private Key</b>	Display the certificate private key

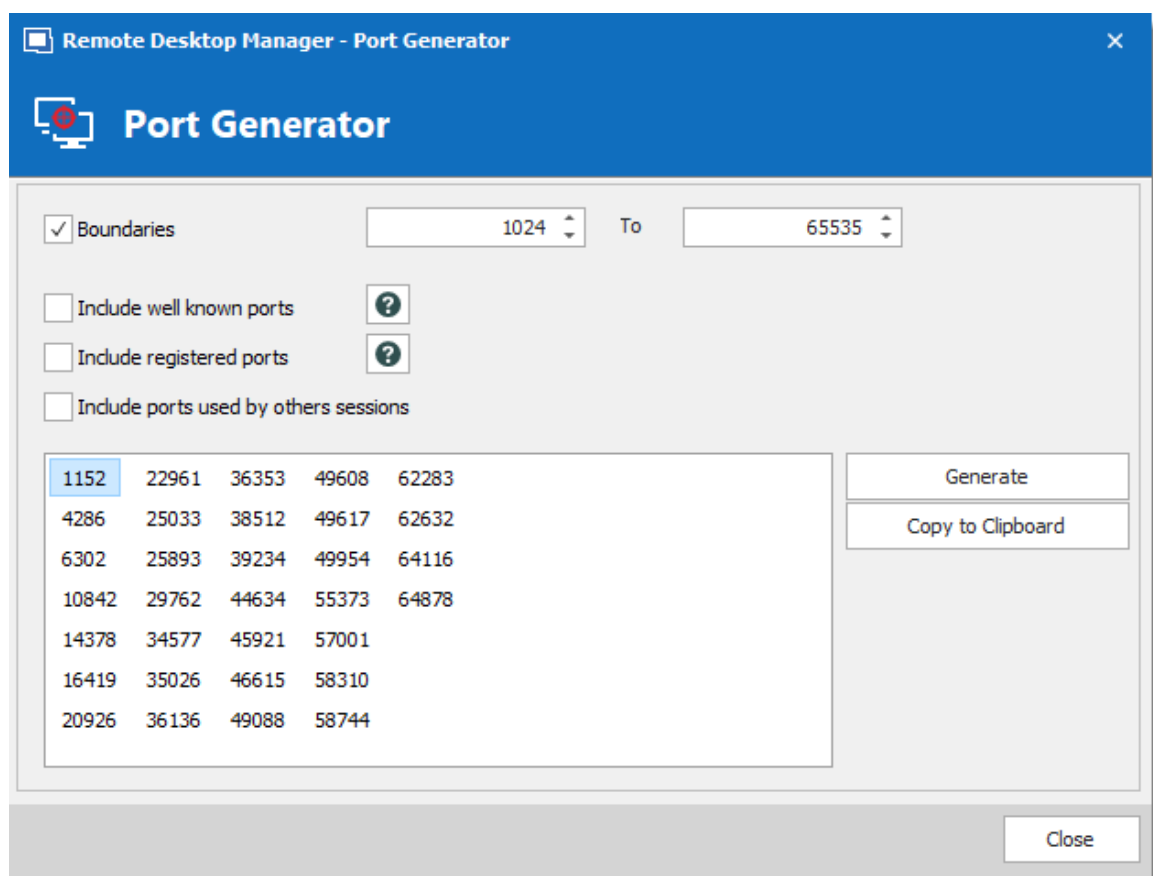
OPTION	DESCRIPTION
<b>View Private Key</b>	View the private key file on your computer.

#### 6.8.1.4 Port Generator

## DESCRIPTION

The Port Generator allows you to generate ports for your connections.

## SETTINGS



Port Generator

OPTION	DESCRIPTION
<b>Boundaries</b>	Determinate the port range to generate the ports between those 2 numbers.
<b>Include well known ports</b>	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
<b>Include registered ports</b>	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.
<b>Include ports used by others sessions</b>	Include the ports that are already used by other sessions.

## 6.8.2 Tools

### 6.8.2.1 Devolutions Localizer

## WHAT IS DEVOLUTIONS LOCALIZER?

Devolutions Localizer is our custom translation tool for our client applications.

So far, with the help of several generous and talented members of our community, Remote Desktop Manager has been translated from English to the following languages:

- Chinese (Simplified) Legacy
- Chinese (Traditional, Taiwan)
- Dutch
- French
- German
- Italian
- Polish
- Russian
- Swedish
- Ukrainian

## GETTING STARTED

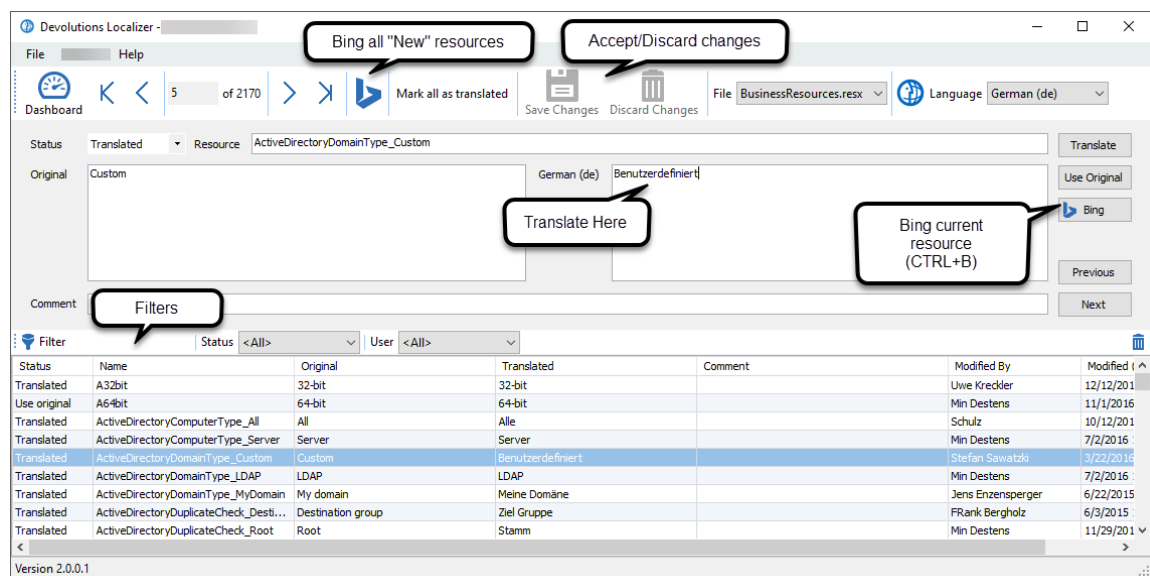


An account is required to use the Devolutions Localizer. You can join our team and get started by signing up here: <https://devolutions.net/Home/Contribute>.

If you're interested in helping your fellow IT pros around the world, please sign up to be one of our wonderful contributors. Our Localizer app makes the process very efficient, and you can work at your own pace, and whenever you have time!

## OVERVIEW

From the **dashboard view** you get a quick progress overview, simply click the **"Translate"** button and start translating.



*Devolutions Localizer*

## 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**: Next resource.
- **CTRL+UP**: Previous resource.
- **CTRL+B**: Request Bing translation for the current string.
- **CTRL+S**: Save all pending changes.
- **CTRL+F**: Enable/disable filtering.

#### 6.8.2.2 Password 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 ZXCVCN . The "Legacy" mode is not the default mode.

The **Password Analyzer** evaluates the strength of passwords stored in the data source. To access the password analyzer, navigate to **Tools – Password Analyzer**. This feature is restricted to Administrators only.

A password analyzer control is also displayed under most password fields of entries.

The screenshot shows the 'Entry Properties' dialog box with the 'General' tab selected. The 'Password' field is highlighted with a green box. Below the password field, a green bar indicates the password strength as 'Perfect'. To the right of the password field, there are icons for visibility, copy, and paste, and a duration of '2 months'.

*Entry Properties - Password Field With Password Analyzer*

The password 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

**Password Analyzer**

**Settings**

☐ Show all
 ☐ Show private vault

☐ Show VPN analysis
 ☐ Show pwned password analysis

**Analysis**

Name	Folder	Username	Date	Since	Occurrence	Password Strength	Password Length
Active Directory	Enterprise\Synchroni...	administrator	1/14/2019 9:11 AM	6 months	2	Weak	7
Active Directory Console	Enterprise\Sessions\...	administrator	12/19/2018 6:49 AM	7 months	2	Weak	7
BasicCred	Enterprise\Credentials	David	11/13/2018 10:45 ...	7 months	4	Popular	6
CredPV		David	1/2/2019 11:16 AM	6 months	4	Popular	6
Email Account	Enterprise\InfoTypes	Email	11/13/2018 8:42 AM	8 months	1	Good	9
Login (Account)	Enterprise\InfoTypes	TestLaccount	11/13/2018 8:17 AM	8 months	2	Weak	13
Login (Web)	Enterprise\InfoTypes	TestLusername	11/13/2018 8:35 AM	8 months	2	Weak	13
RDPTest	Enterprise\Sessions\...		4/30/2019 9:17 AM	2 months	1	Weak	4
RDPTest - Copy	Enterprise\Sessions\...	test	1/18/2019 3:19 PM	6 months	4	Popular	6
TeamViewer	Enterprise\Sessions\...	845370611	12/19/2018 11:08 ...	7 months	1	Good	6
test	Enterprise\Sessions\...	test	2/5/2019 9:51 AM	5 months	1	Popular	4
Wi-Fi Router	Enterprise\InfoTypes		11/13/2018 8:45 AM	8 months	1	Good	13
Windows Admin Center	Enterprise\Sessions\...	david	2/5/2019 10:02 AM	5 months	1	Perfect	8

ID

### Tools - Password Analyzer

OPTION	DESCRIPTION
<b>Show all</b>	Shows you all the entries in your session, including those without password.
<b>Show VPN analysis</b>	Add the VPN Host column.
<b>Edit</b>	Open the current entry to edit it.
<b>Forbidden Password</b>	Create a list of prohibited passwords.
<b>Export Settings</b>	Export the password analyzer settings.



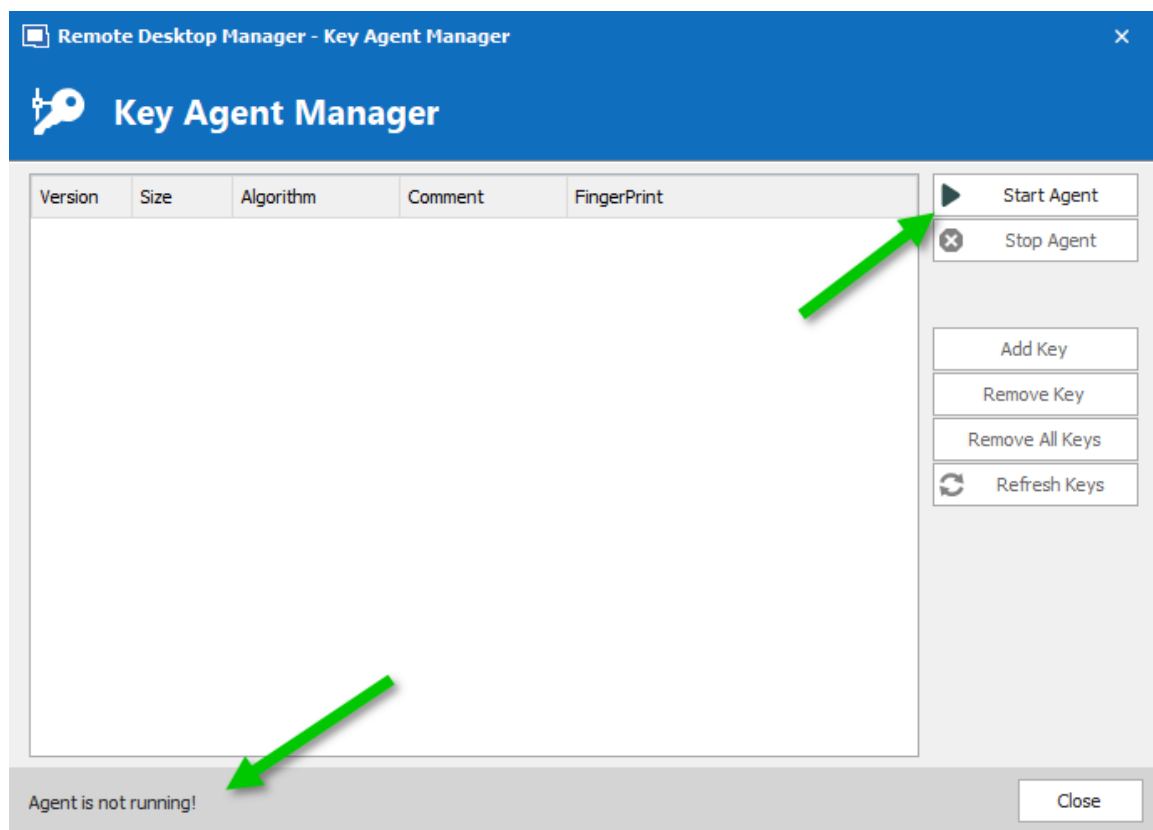
### 6.8.2.3 Key Agent Manager

## 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.

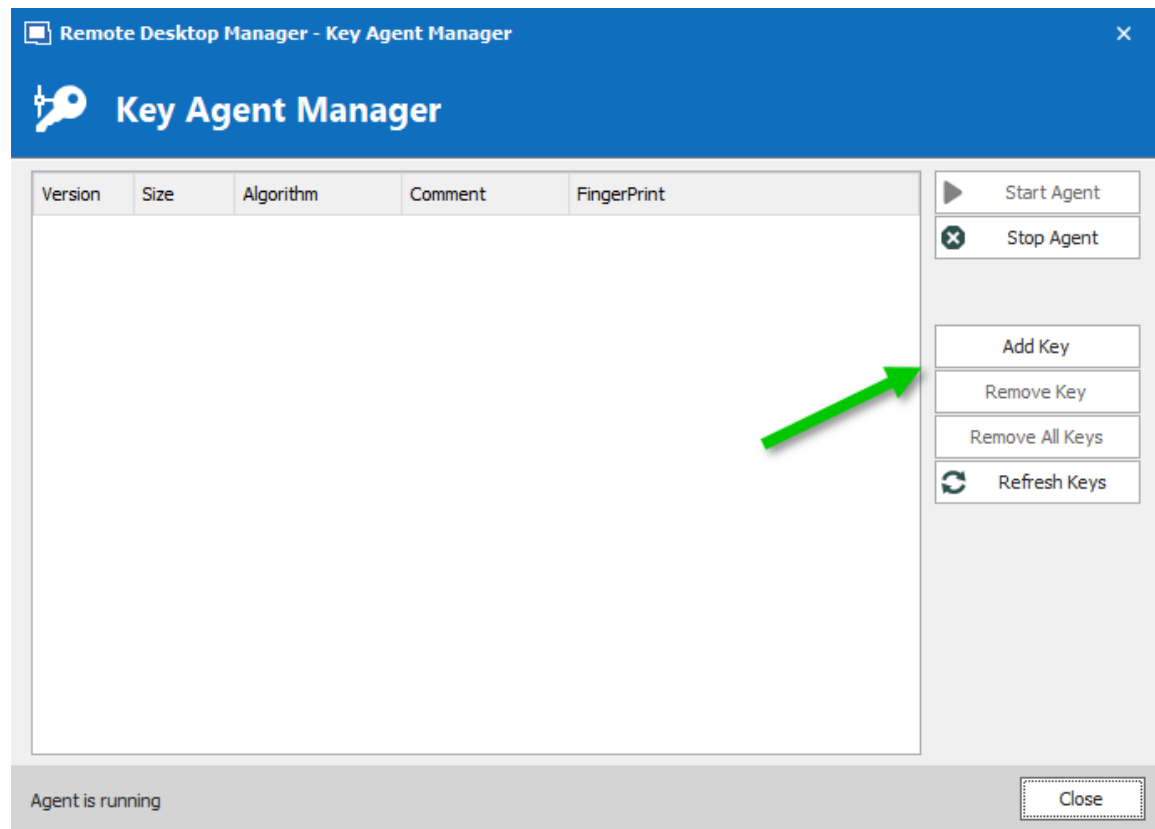
## SETTINGS

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**.



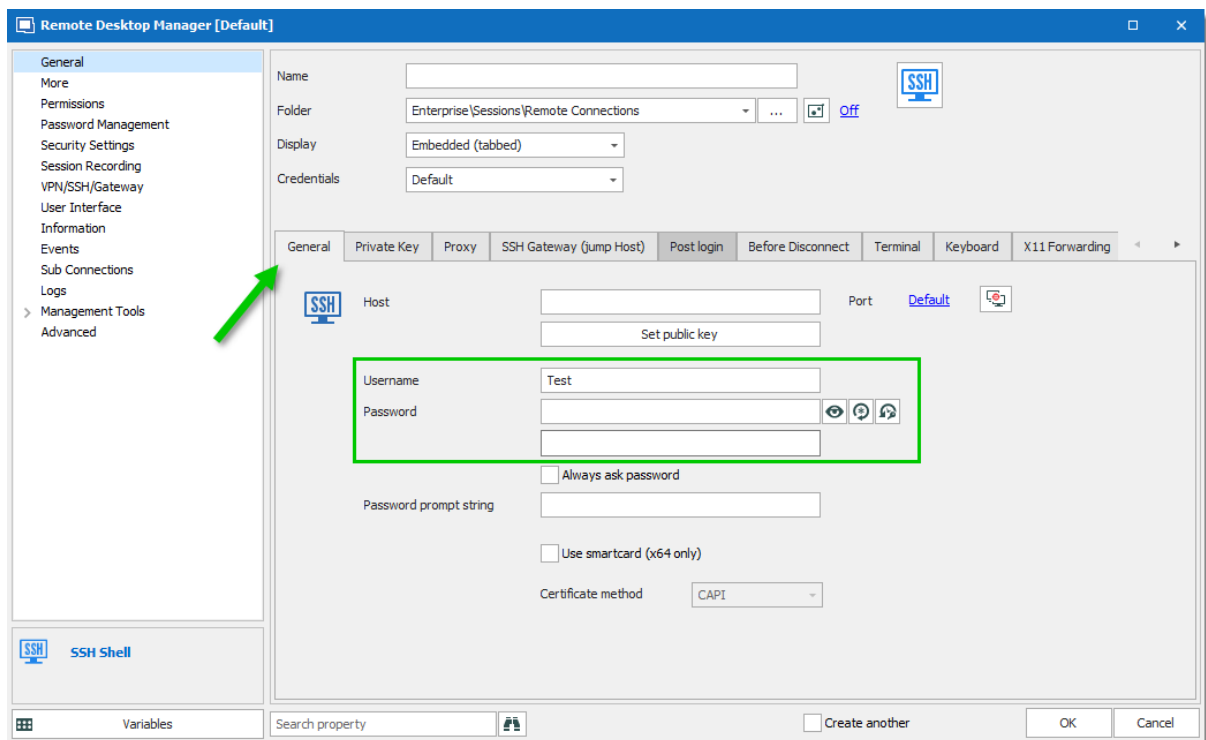
Key Agent Manager - Start Agent

2. Click on **Add key** and select the file to open your SSH key.



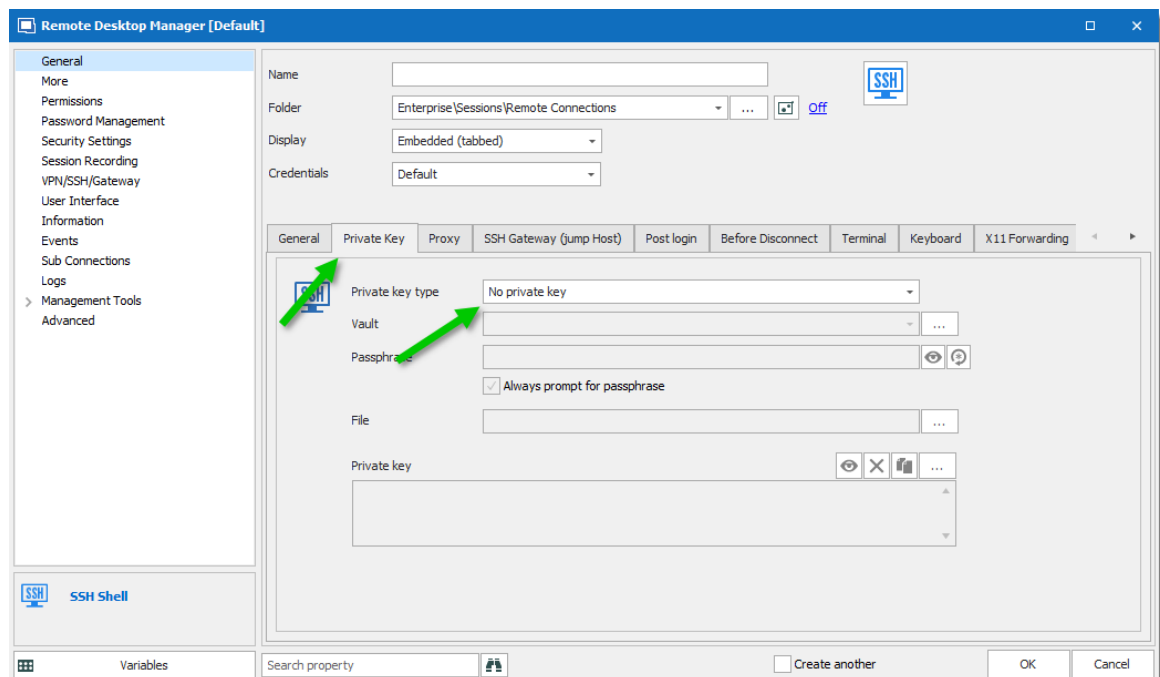
*Key Agent Manager - Add Key*

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.



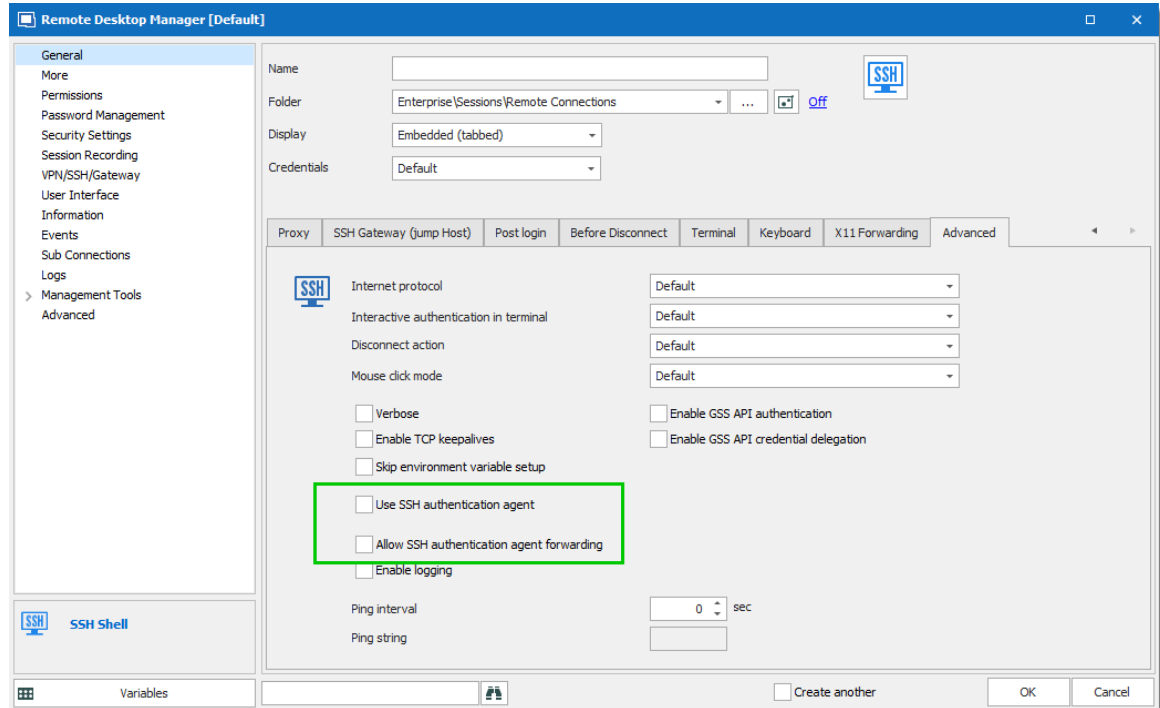
SSH Shell session - General Tab

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.

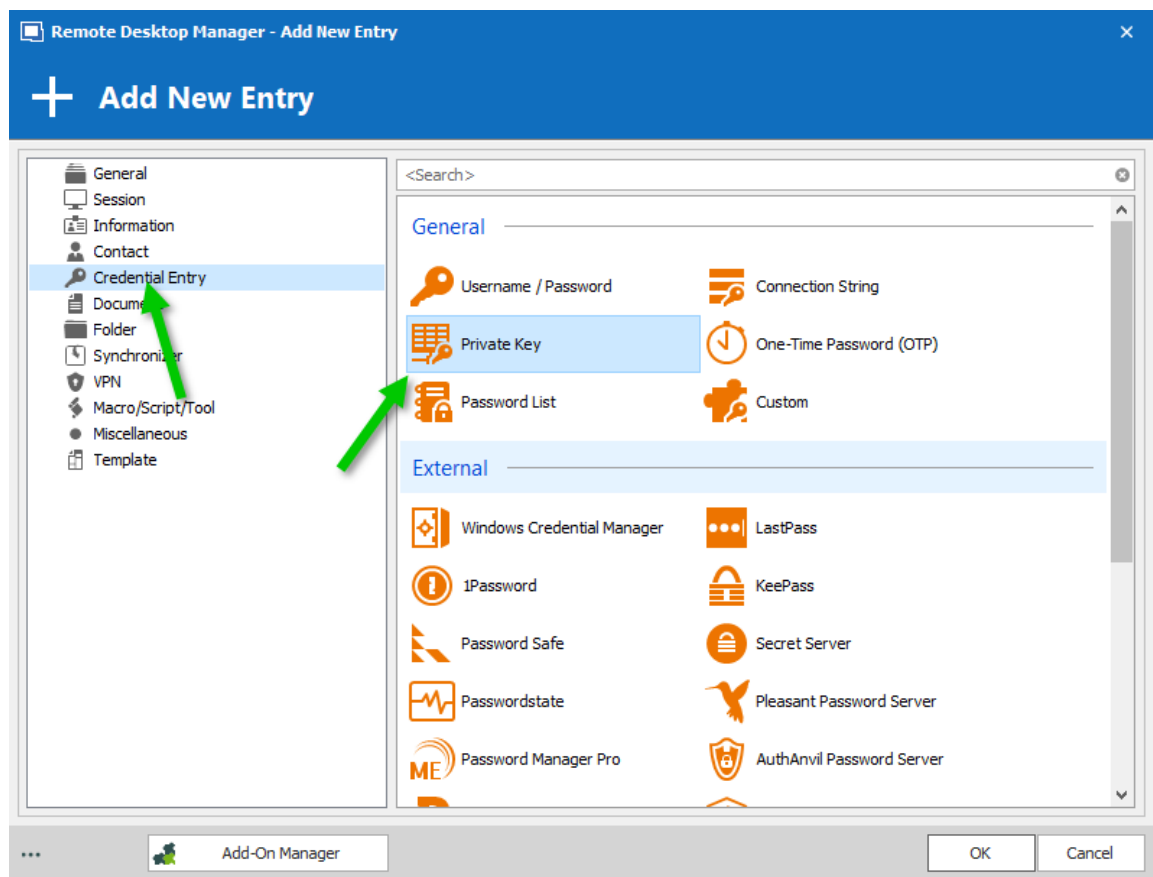


*SSH Shell session - Advanced*

## PRIVATE KEY CREDENTIAL

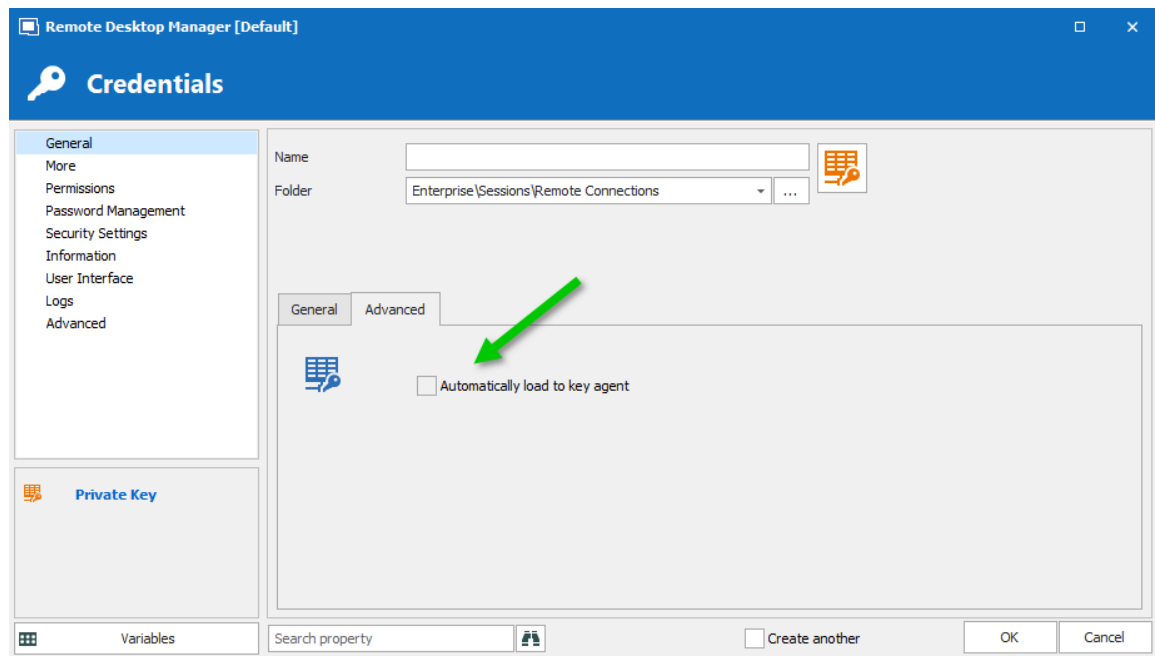
When creating new Private Key credential entry in Remote Desktop Manager you have the option of loading them automatically in your Key Agent Manager.

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

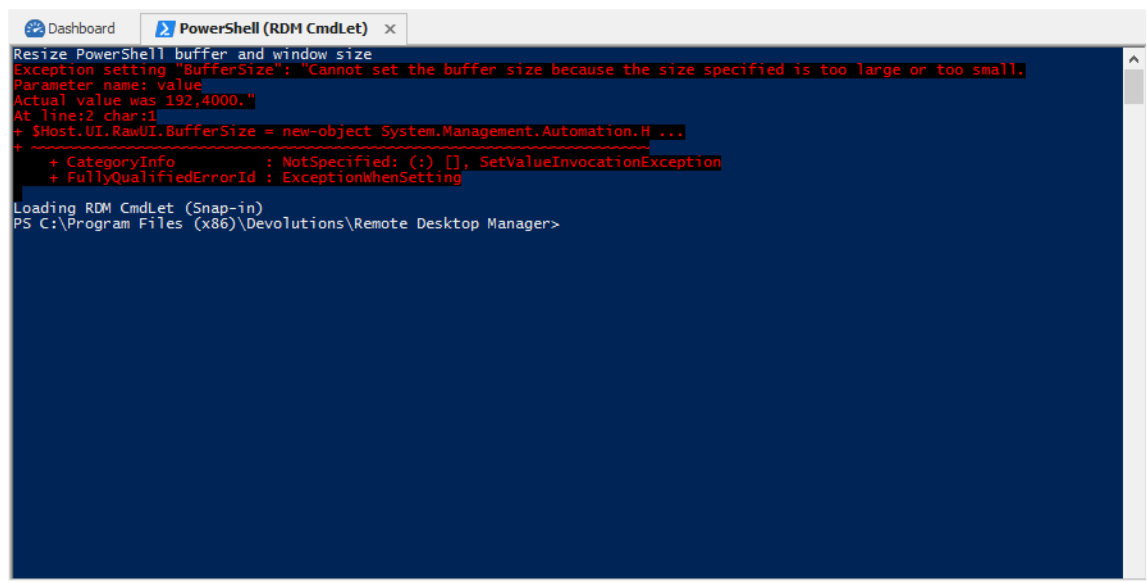
The **PowerShell (RDM CmdLet)** automatically opens an embedded PowerShell window. RDM snap-in allows for quick and robust automation of actions such as add/edit/open of sessions, the possibilities are endless.

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.



```
Dashboard PowerShell (RDM CmdLet) x
Resize PowerShell buffer and window size
Exception setting "BufferSize": "Cannot set the buffer size because the size specified is too large or too small.
Parameter name: value
Actual value was 192,4000."
At line:2 char:1
+ $Host.UI.RawUI.BufferSize = new-object System.Management.Automation.H ...
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:) [], SetValueInvocationException
+ FullyQualifiedErrorId : ExceptionWhenSetting

Loading RDM CmdLet (Snap-in)
PS C:\Program Files (x86)\Devolutions\Remote Desktop Manager>
```

*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

Dashboard
Chocolatey Console


**AutoHotkey** 1.1.23.01
[Open in gallery](#)

25,517 Downloads

1,161 Downloads of v1.1.23.01

1/24/2016 Last update

[Project Site](#)  
[License](#)  
[Report Abuse](#)  
[Contact Maintainers](#)  
[Download](#)





AutoHotkey is a free, open source macro-creation and automation software utility that allows users to automate repetitive tasks. It is driven by a custom scripting language that is aimed specifically at providing keyboard shortcuts, otherwise known as hotkeys.

AutoHotkey\\_L is a fork of AutoHotkey which adds a long list of new features and fixes some bugs. Anything that can be done with AutoHotkey can also be done with AutoHotkey\\_L. Scripts written for AutoHotkey will also run on AutoHotkey\\_L, with some exceptions.

```
C:\> choco install autohotkey
```

Name	Installed Version	Latest Version	Installed
autohotkey		1.1.23.01	<input type="checkbox"/>
autoit		3.3.14.2	<input type="checkbox"/>
filezilla		3.15.0.2	<input type="checkbox"/>
Firefox		44.0.2	<input type="checkbox"/>
GoogleChrome		48.0.2564.109	<input type="checkbox"/>
HeidiSQL		8.3.0.4694	<input type="checkbox"/>
javaruntime		8.0.66	<input type="checkbox"/>
keepass		2.31	<input type="checkbox"/>
mysql.workbench		6.3.6	<input type="checkbox"/>
powershell		4.0.20141001	<input type="checkbox"/>
putty.install	0.66	0.66	<input type="checkbox"/>
pvm		7.1.0.0	<input type="checkbox"/>
Radmin. Viewer		3.4.0.20120928	<input type="checkbox"/>
safari			<input type="checkbox"/>
skype		7.18.0.112	<input type="checkbox"/>
sysinternals		2016.02.02	<input type="checkbox"/>
teamviewer		11.0.53254	<input type="checkbox"/>
tightvnc		2.7.10.20140503	<input type="checkbox"/>

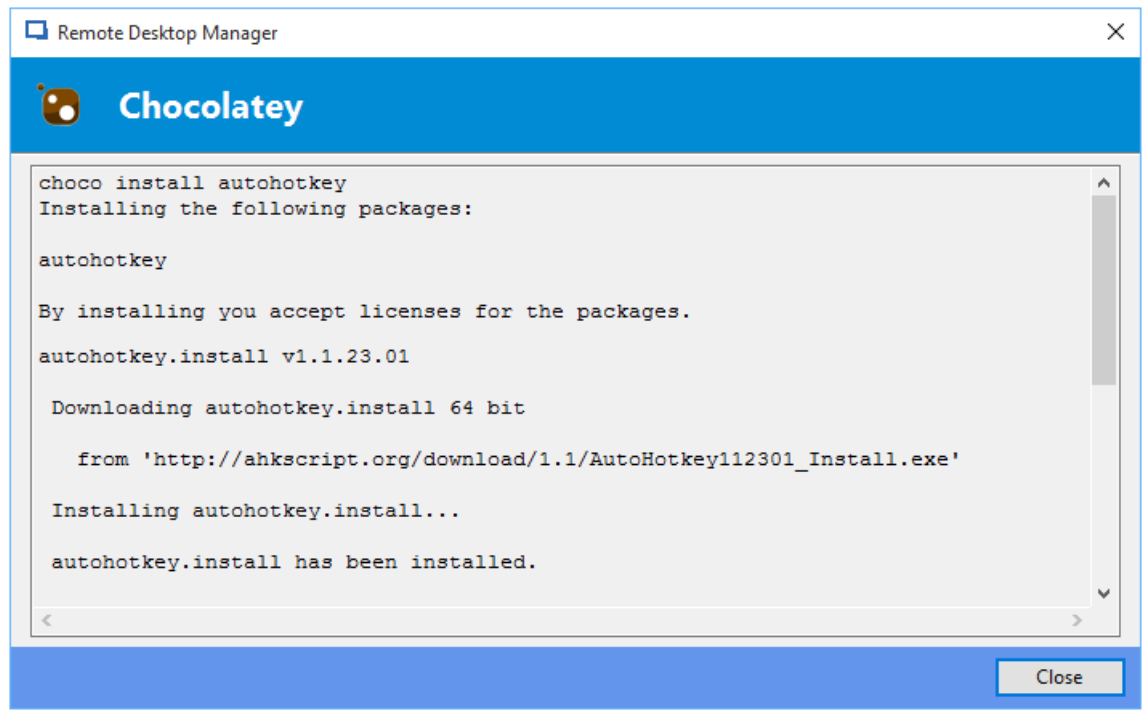
Chocolatey Console

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.

Name	Installed Version	Latest Version	Installed
autohotkey	1.1.23.01	1.1.23.01	<input checked="" type="checkbox"/>
autoit	3.3.14.2	3.3.14.2	<input type="checkbox"/>
filezilla		3.15.0.2	<input type="checkbox"/>
Firefox		44.0.2	<input type="checkbox"/>
GoogleChrome		48.0.2564.109	<input checked="" type="checkbox"/>
HeidiSQL		8.3.0.4694	<input type="checkbox"/>
javaruntime		8.0.66	<input type="checkbox"/>
keepass	2.31	2.31	<input type="checkbox"/>
mysql.workbench		6.3.6	<input type="checkbox"/>

*Installation Complete*

## 6.8.2.5.2 Local RDP/RemoteApp Manager

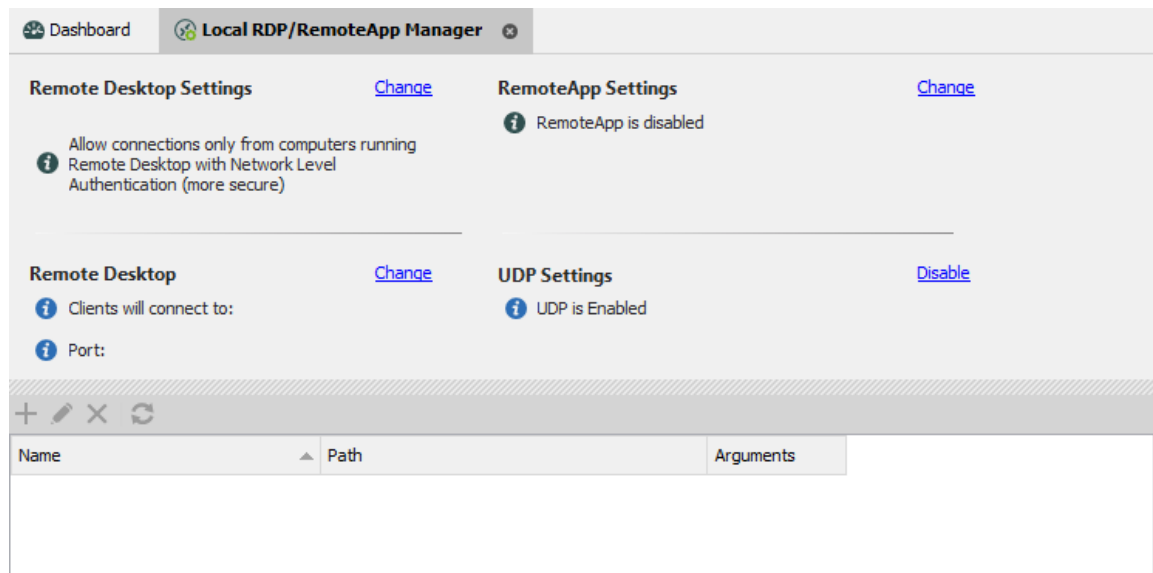
## DESCRIPTION

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.

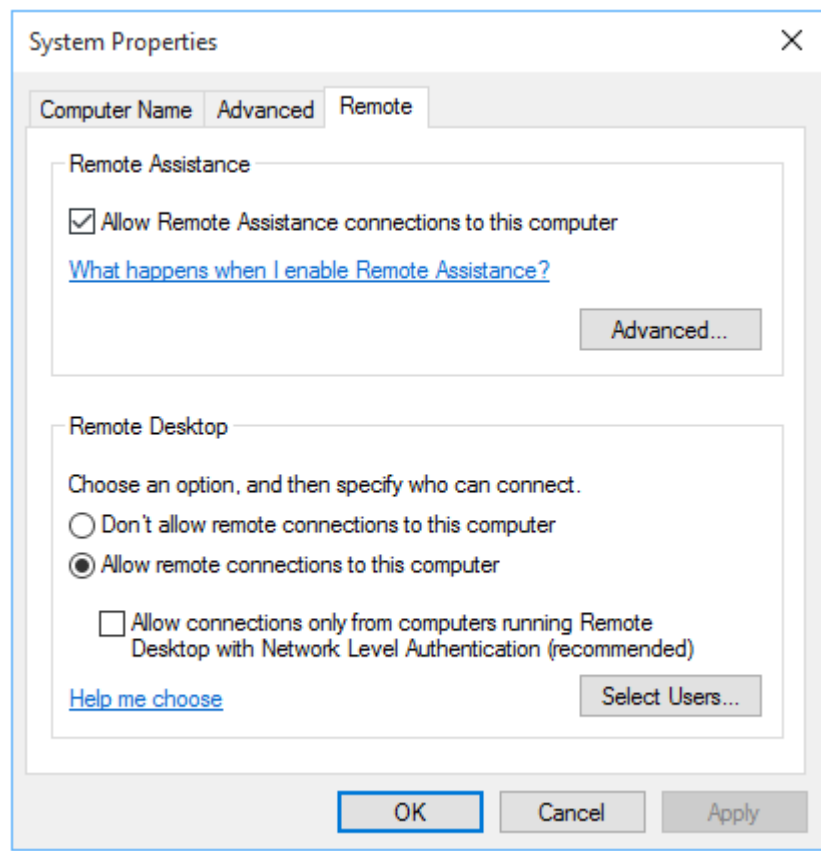
## SETTINGS



More Tools - Local RDP/RemoteApp Manager

## REMOTE DESKTOP SETTINGS

Allow or disallow the remote connections to your computer.



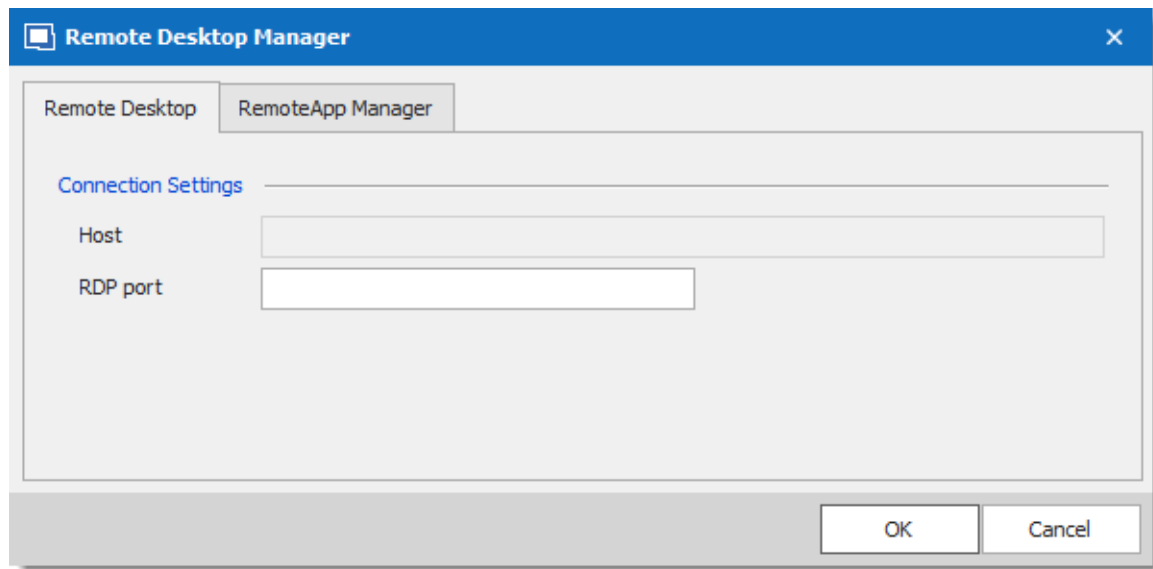
*Remote Desktop Settings*

## 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.



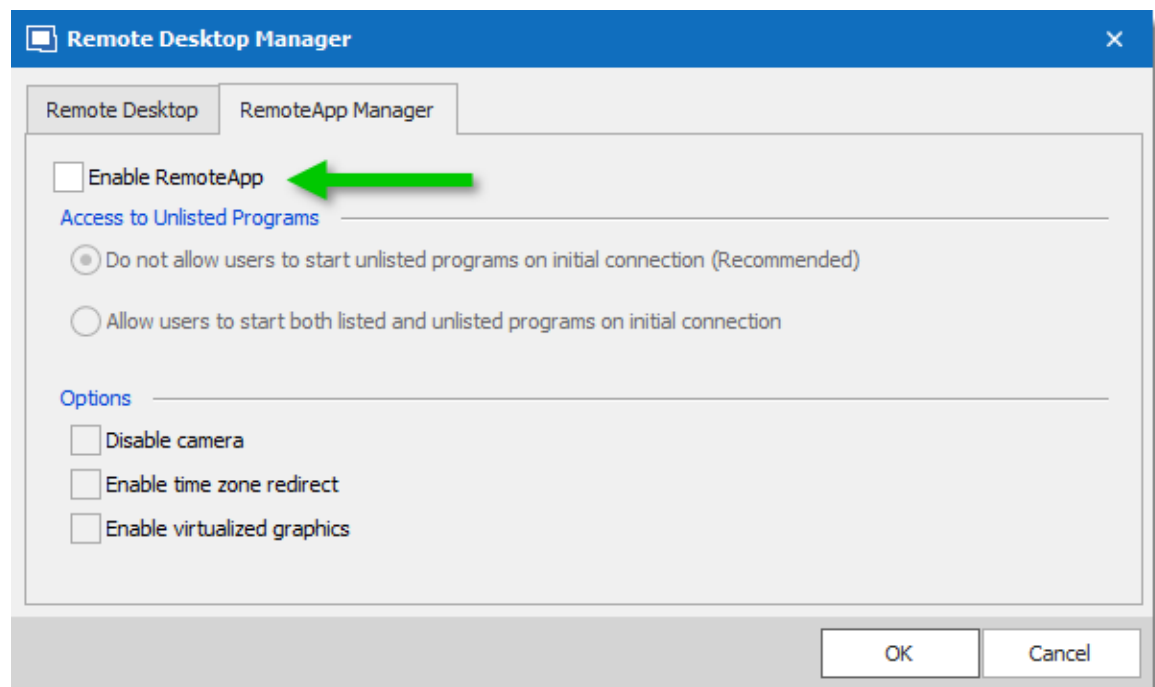
*Remote Desktop Connection Settings*

## REMOTEAPP SETTINGS

You must Enable RemoteApp to be able to create a New RemoteApp Setting.

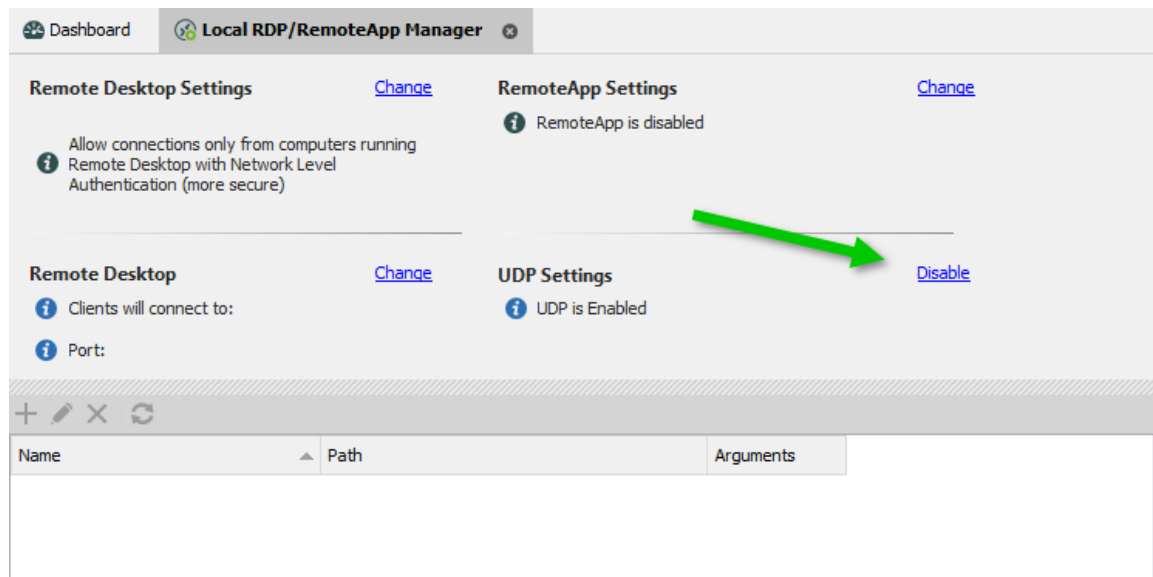


Remote Desktop Manager must be run as an administrator to modify the RemoteApp settings.

*RemoteApp Settings*

## UDP SETTINGS

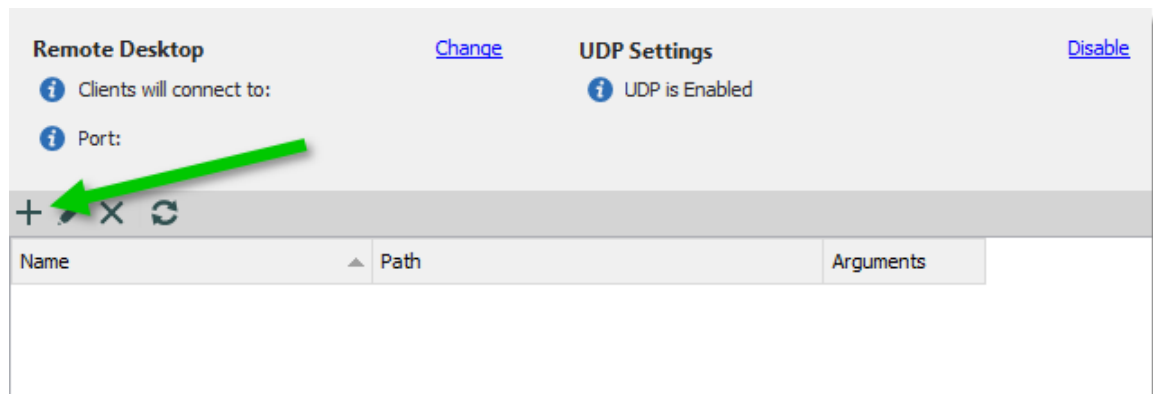
Enable or disable UDP (User Datagram Protocol) locally on your computer. UDP is a communication protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP).



*Local RDP/RemoteApp Manager - UDP is Enabled*

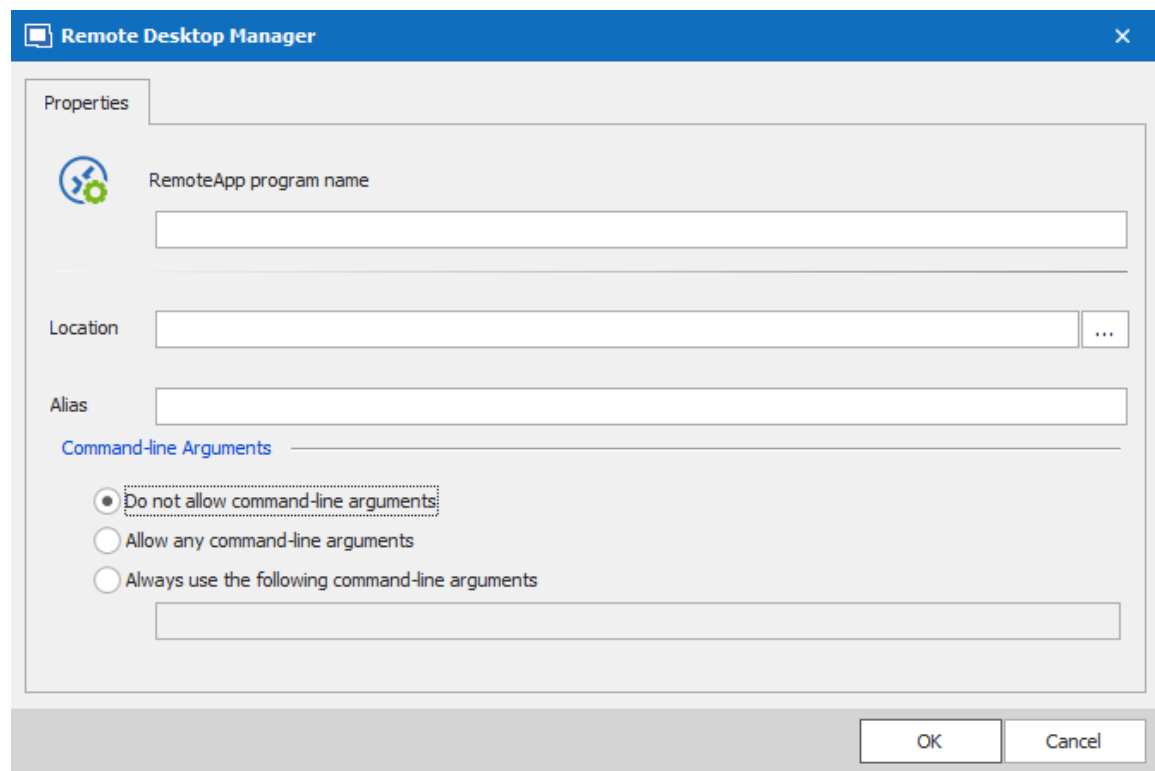
## USAGE

1. Click on **New RemoteApp Settings**.

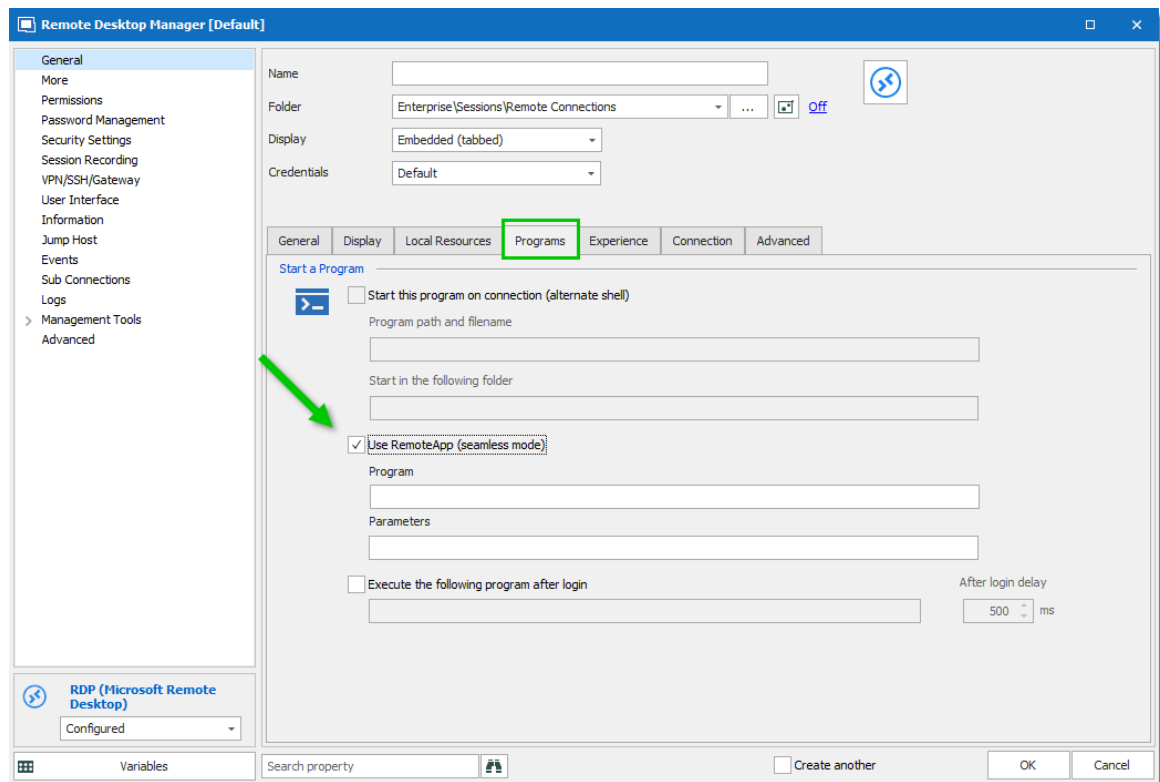


*New RemoteApp Settings*

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

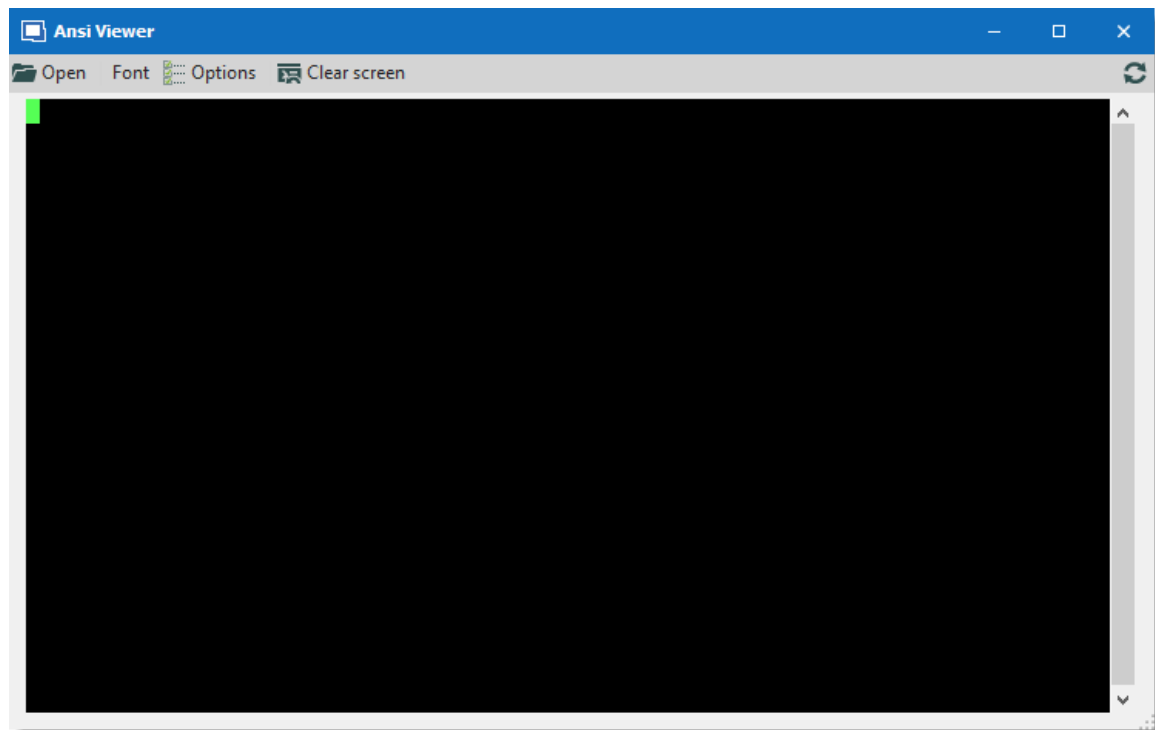
## 6.8.2.5.3 Playback (Ansi)

## DESCRIPTION




The **Playback (Ansi)** is available in **Tools – More Tools – Playback (Ansi)**.

## SETTINGS

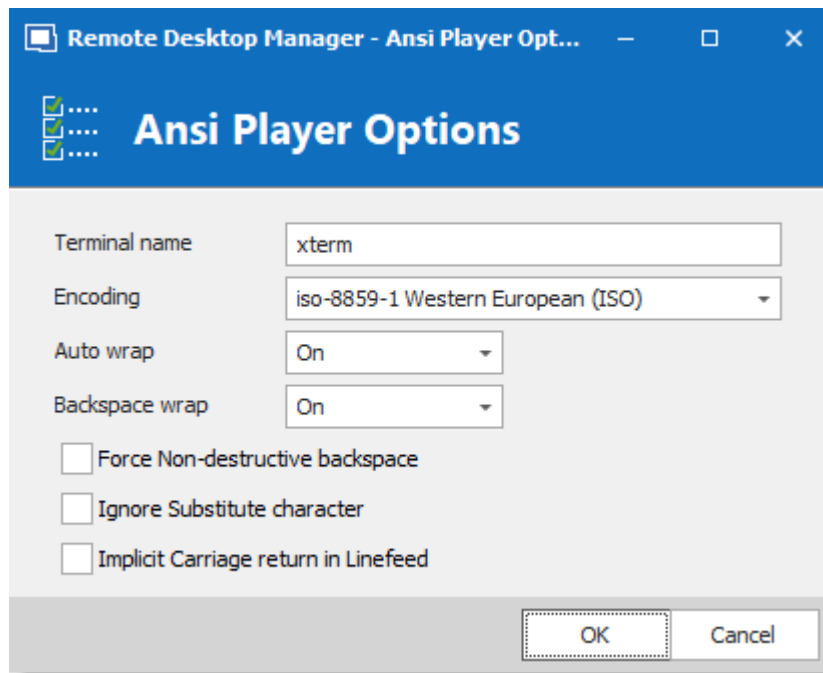




*More Tools - Playback (Ansi)*

OPTION	DESCRIPTION
 <b>Open</b>	Select the ansi file you wish to open in the Terminal Playback.
<b>Font</b>	Select the font for the Terminal Playback.
 <b>Options</b>	See <b>Options</b> section.
 <b>Clear screen</b>	Clear the screen to play another ansi file.

## OPTIONS



*Playback (Ansi) - Ansi Player Options*

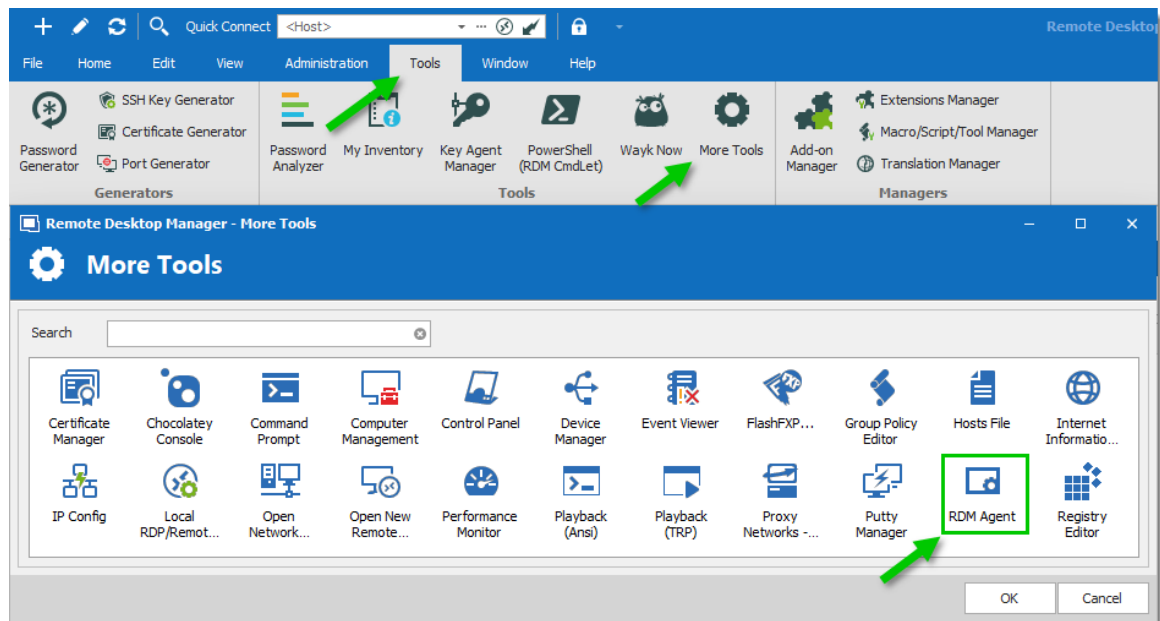
OPTION	DESCRIPTION
<b>Terminal name</b>	Indicate the terminal name.
<b>Encoding</b>	Indicate the encoding you wish to use.
<b>Auto wrap</b>	<p>Indicate what happen when text reaches the right-hand edge of the window. Select between:</p> <ul style="list-style-type: none"> <li>• On</li> <li>• Off</li> <li>• Dos</li> </ul>
<b>Backspace wrap</b>	<p>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:</p>

OPTION	DESCRIPTION
	<ul style="list-style-type: none"><li>• On</li><li>• Off</li><li>• Dos</li></ul>
<b>Force Non-destructive backspace</b>	Allow to perform a normal backspace without deleting a character.
<b>Ignore Substitute character</b>	Ignore the substitute character that can be use in Putty.
<b>Implicit Carriage return in Linefeed</b>	<p>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).</p> <p>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.</p>

#### 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.



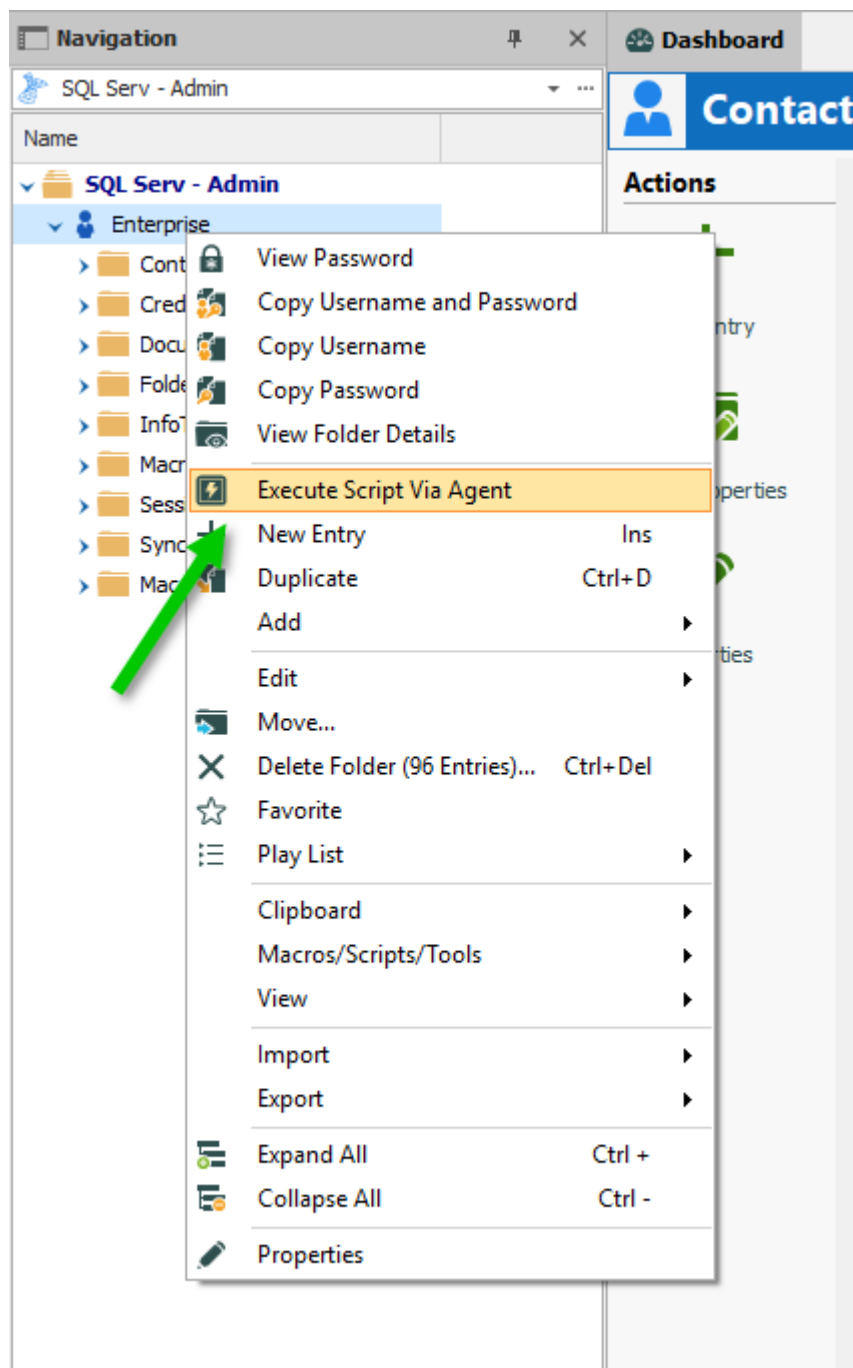
*More Tools - RDM Agent*

## 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**.

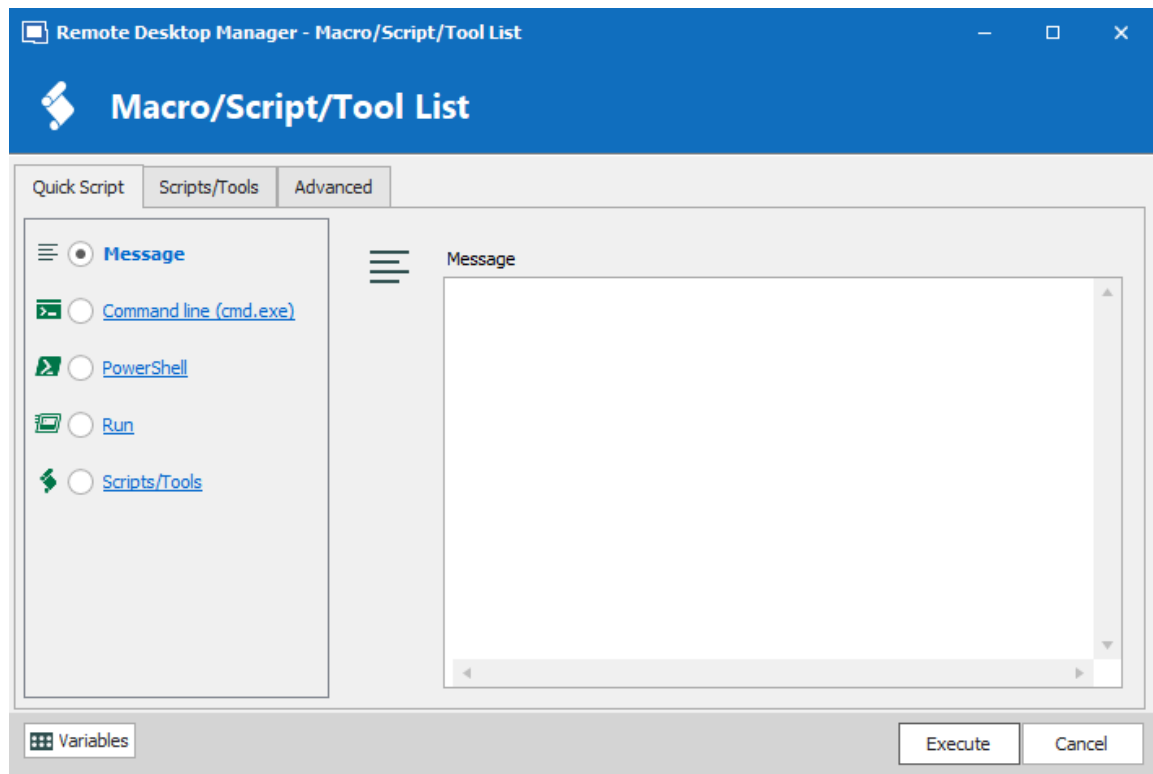


Execute script via Agent only needs the RDM Agent when the script is executed from the Quick Script tab. RDM needs to be fully installed on the remote computer when the script is executed from the Scripts/Tools tab.



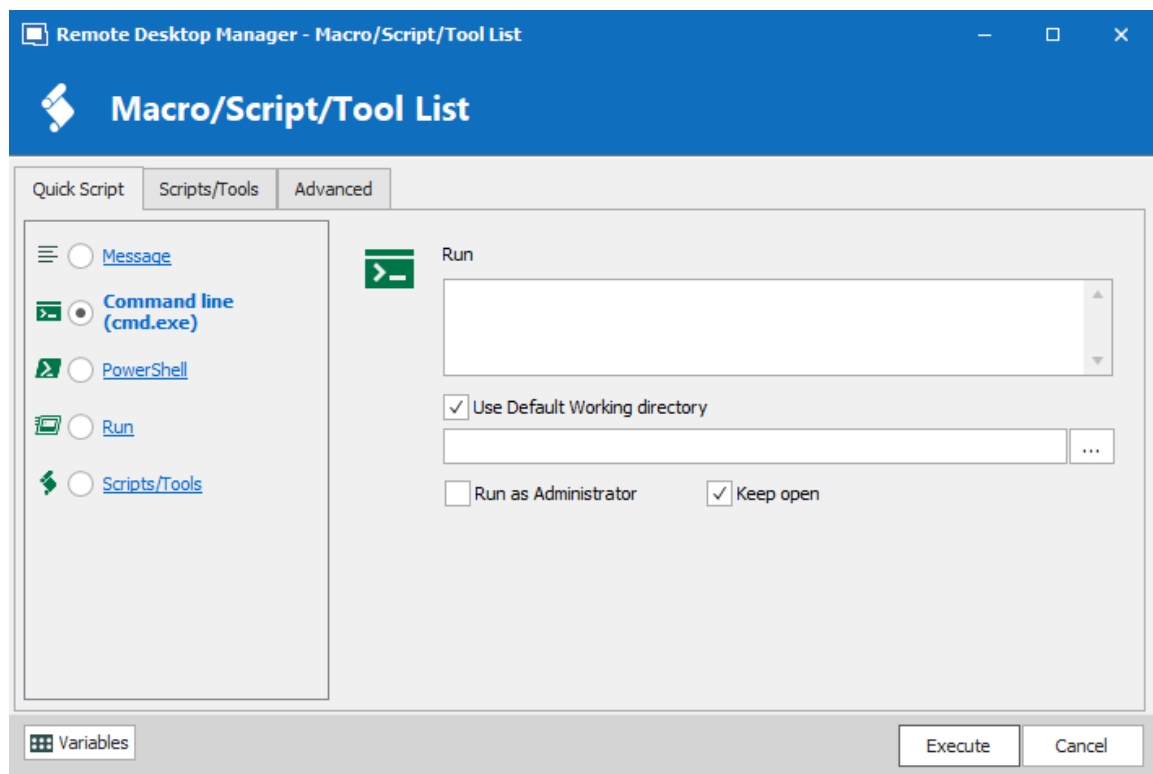
*Execute Script Via Agent*

## QUICK SCRIPT - MESSAGE

*Quick Script - Message*

OPTION	DESCRIPTION
<b>Message</b>	Send a message to all targets.

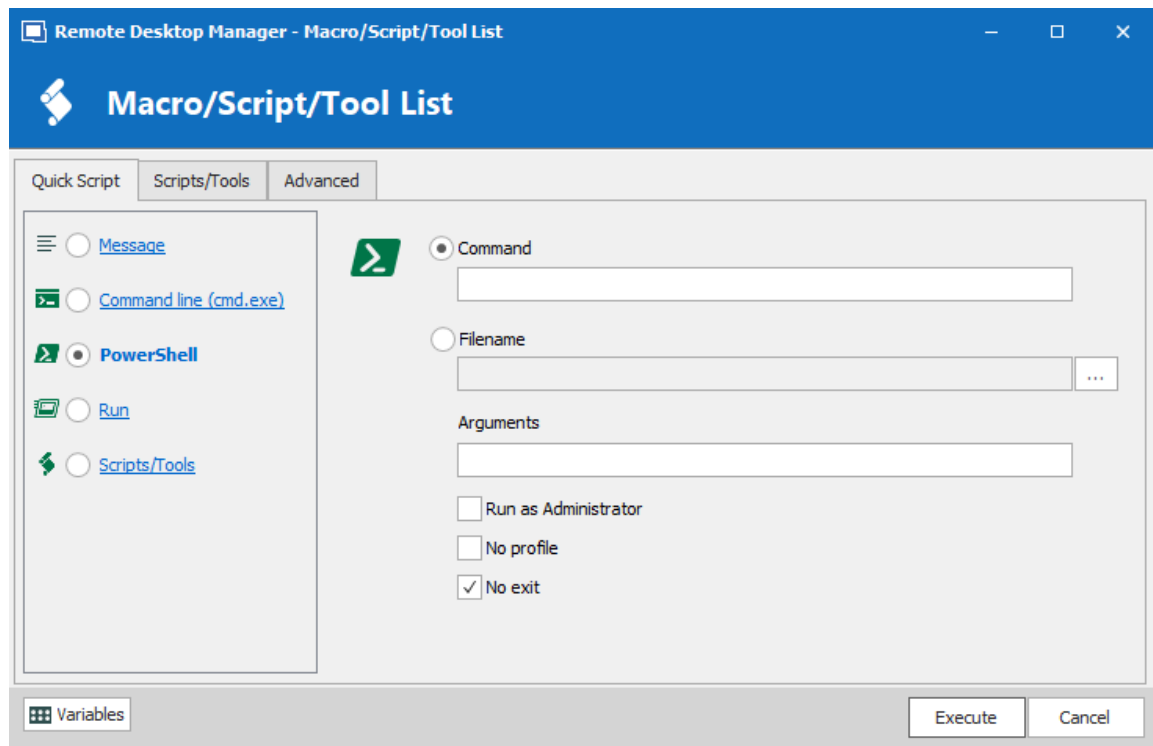
## QUICK SCRIPT - COMMAND LINE (CMD.EXE)



*Quick Script - Command Line*

OPTION	DESCRIPTION
<b>Run</b>	Indicate the command line that you want to execute.
<b>Use Default Working directory</b>	Use the default working directory when connect to the session.
<b>Run as Administrator</b>	Elevates the process to run as an administrator.
<b>Keep open</b>	Keep the window open after the execution of the command line.

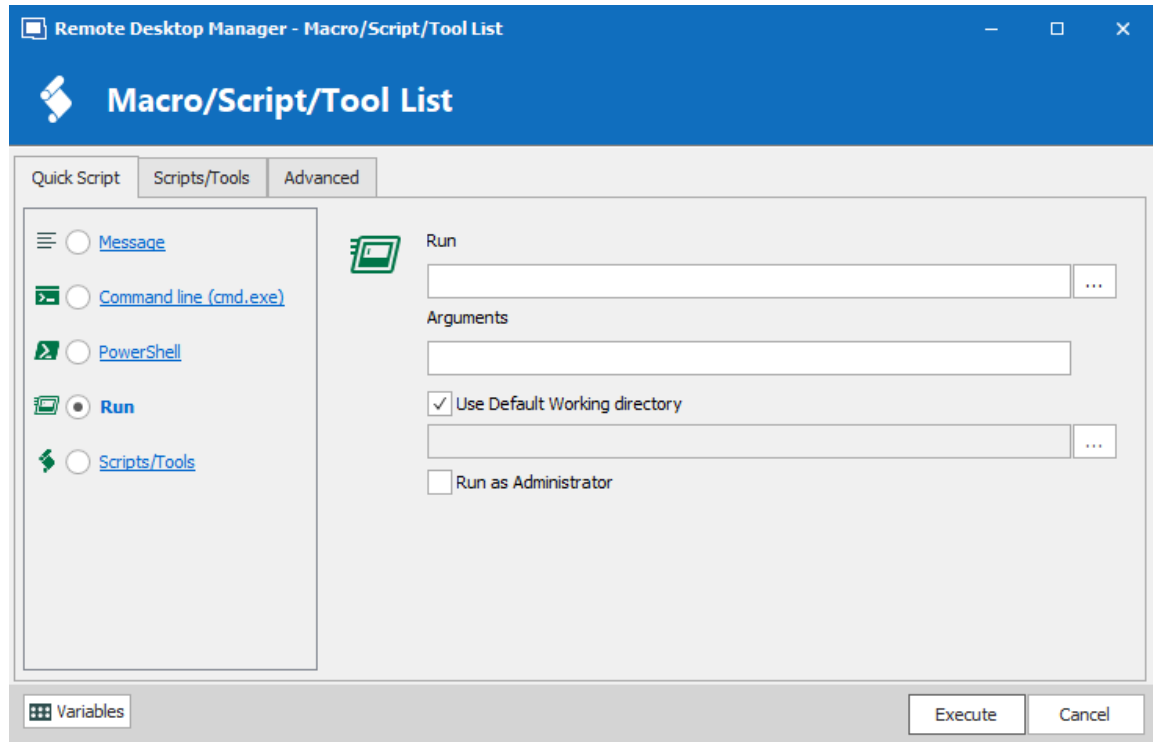
## QUICK SCRIPT - POWERSHELL

*Quick Script - PowerShell*

OPTION	DESCRIPTION
<b>Command</b>	Indicate the PowerShell command that you want to execute.
<b>Filename</b>	Select a PowerShell file on the network or on the computer.
<b>Arguments</b>	Arguments that are appended to the Command.
<b>Run as Administrator</b>	Elevates the process to run as an administrator.
<b>No Profile</b>	Does not load the Windows PowerShell profile.
<b>No exit</b>	Does not exit after running startup commands.



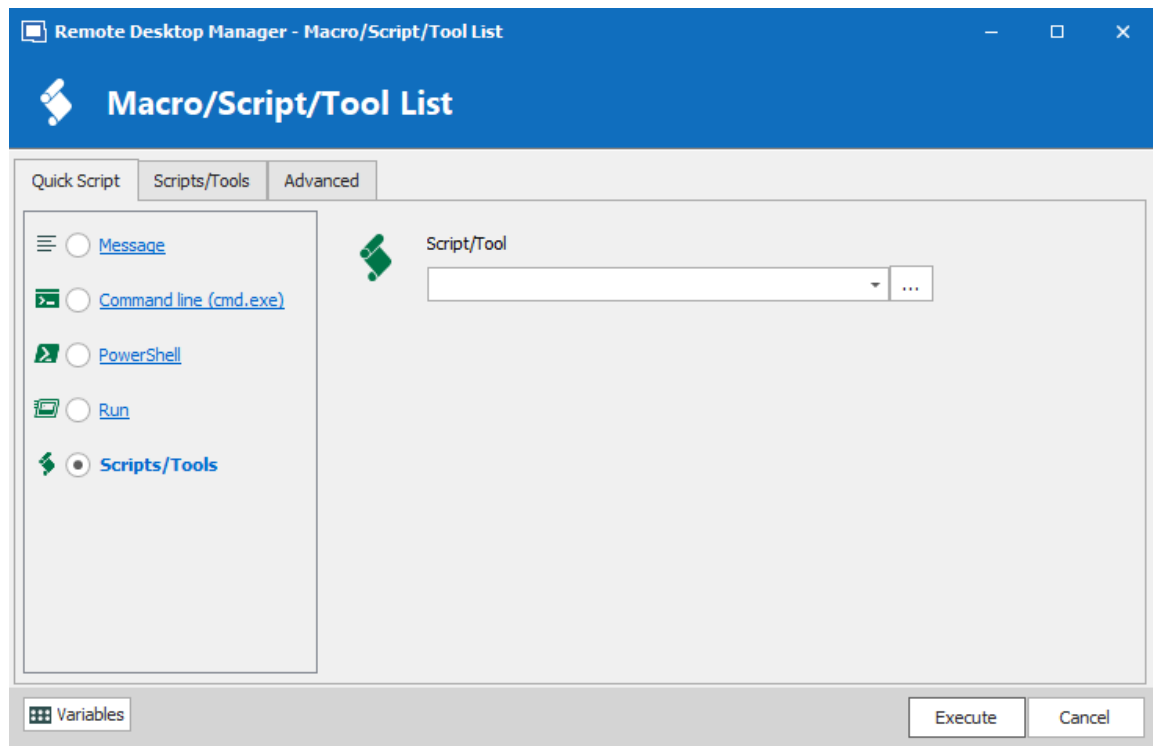
## QUICK SCRIPT - RUN



*Quick Script - Run*

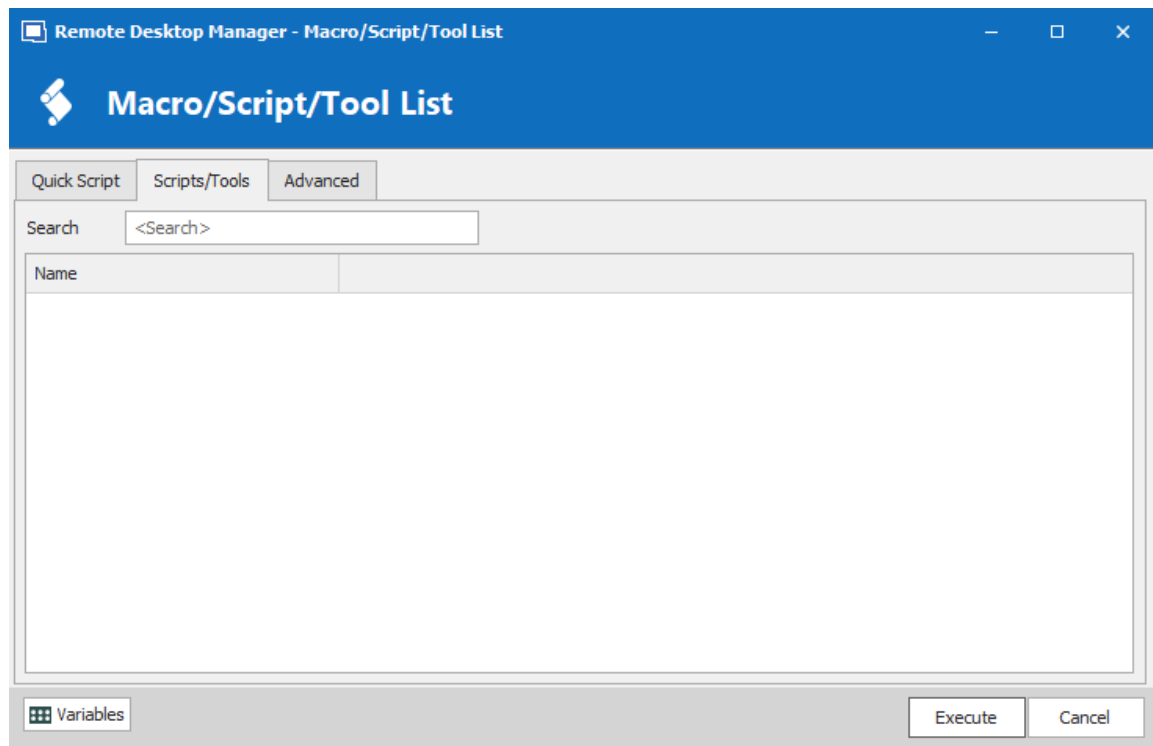
OPTION	DESCRIPTION
<b>Run</b>	Select the program or file that you want to execute.
<b>Arguments</b>	Arguments that are appended to the Command.
<b>Use Default Working directory</b>	Use the default working directory when connect to the session.
<b>Run as Administrator</b>	Elevates the process to run as an administrator.

## QUICK SCRIPT - SCRIPTS/TOOLS

*Quick Script - Scripts/Tools*

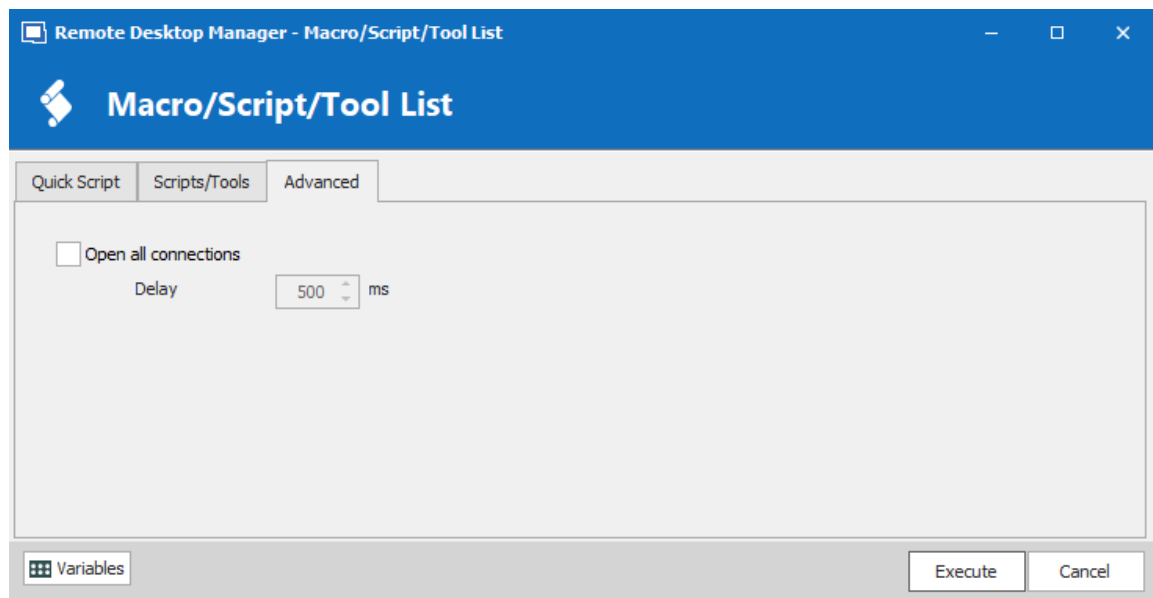
OPTION	DESCRIPTION
<b>Scripts/Tools</b>	Select a script or a tool session that you have already created in Remote Desktop Manager.

## SCRIPT/TOOLS

*Scripts/Tools*

Search for a script or a tool you wish to execute through the RDM Agent.

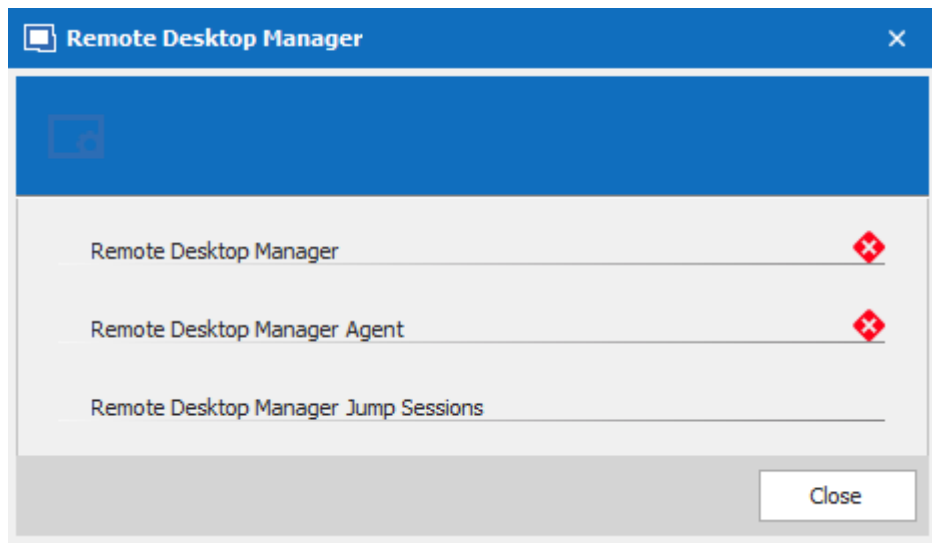
## SETTINGS

*Advanced*

OPTION	DESCRIPTION
<b>Open all connections</b>	When multiple sessions are selected to <b>Execute Script Via Agent</b> , it will open all the selected connections.
<b>Delay</b>	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.

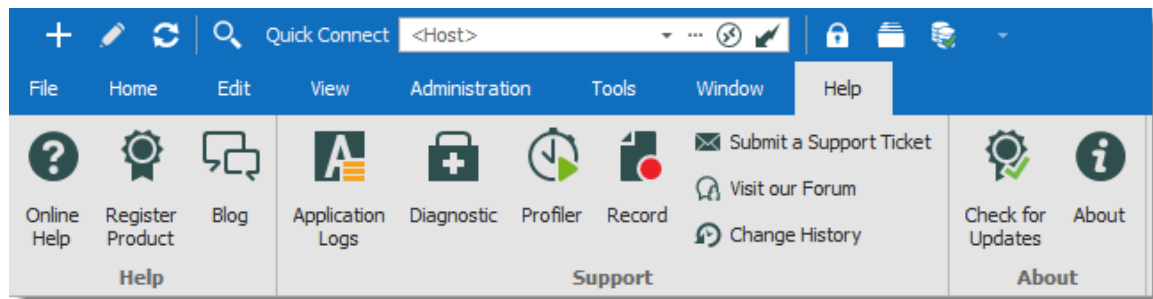


*Agent Status*

## 6.9 Help

### DESCRIPTION

The **Help** tab contain links to the Devolutions forum and Online Help, and many support related features, such as the **Application Logs**, the **Profiler**, and the **Recorder**.



Ribbon - Help

## HELP

OPTION	DESCRIPTION
<b>Online Help</b>	Launches the Online Help you are currently browsing!
<b>Register Product</b>	Register the Remote Desktop Manager with a Trial or Enterprise license serial. For more information, please consult the <a href="#">Register Enterprise Edition</a> topic.
<b>Blog</b>	Visit our <a href="#">Blog</a> . Learn about the Devolutions Team, as well as our Goals, Products and more.

## SUPPORT

OPTION	DESCRIPTION
<b>Applications Logs</b>	Opens the <a href="#">Application Logs</a> . This is useful for understanding encountered errors.
<b>Diagnostic</b>	Launches the <a href="#">Diagnostic</a> feature.
<b>Profiler</b>	Use the <a href="#">Profiler</a> to acquire specific information. Used to diagnose connectivity issues with a data source.

OPTION	DESCRIPTION
<b>Record</b>	Use the <a href="#">Recorder</a> . Used to help our Devolutions Support team troubleshoot the problem
<b>Submit a Support Ticket</b>	Submit a Support Ticket. Help us make your experience better by reporting experience issues or by asking for new features.
<b>Visit our Forum</b>	Visit our <a href="#">Forum</a> . You can create an account and experience the bleeding edge of our customer support.
<b>Change History</b>	Send you directly to our Remote Desktop Manager web page to view the <a href="#">new features and enhancements</a> when a new version is release.

## ABOUT

OPTION	DESCRIPTION
<b>Check for Updates</b>	Launch the Update Manager.
<b>About</b>	Learn about Remote Desktop Manager.

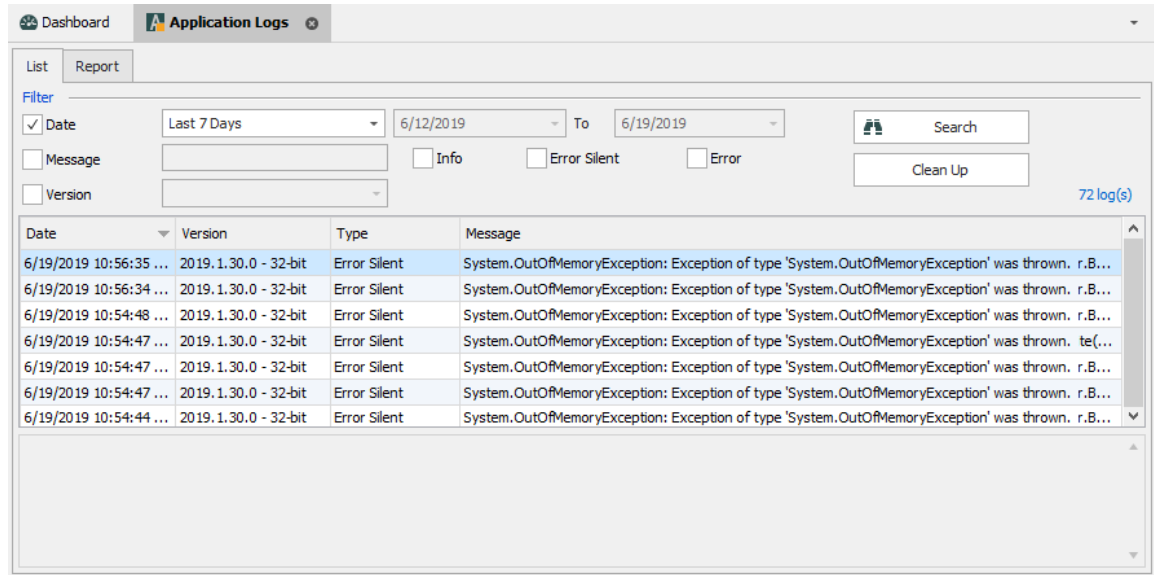
### 6.9.1 Support

#### 6.9.1.1 Application Log

## DESCRIPTION

When encountering errors, you can verify the local application log, which is available in ***Help – Application Logs***.

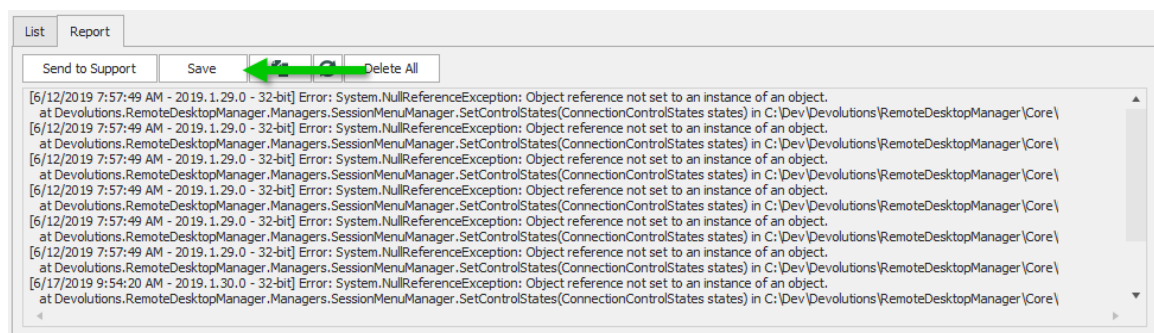
These logs are saved in **%LocalAppData%\Devolutions\RemoteDesktopManager\RemoteDesktopManager.log.db**. Logs are displayed as a list which can be filtered by date, message, version, or type of log.



View Application Log dialog

## REPORT

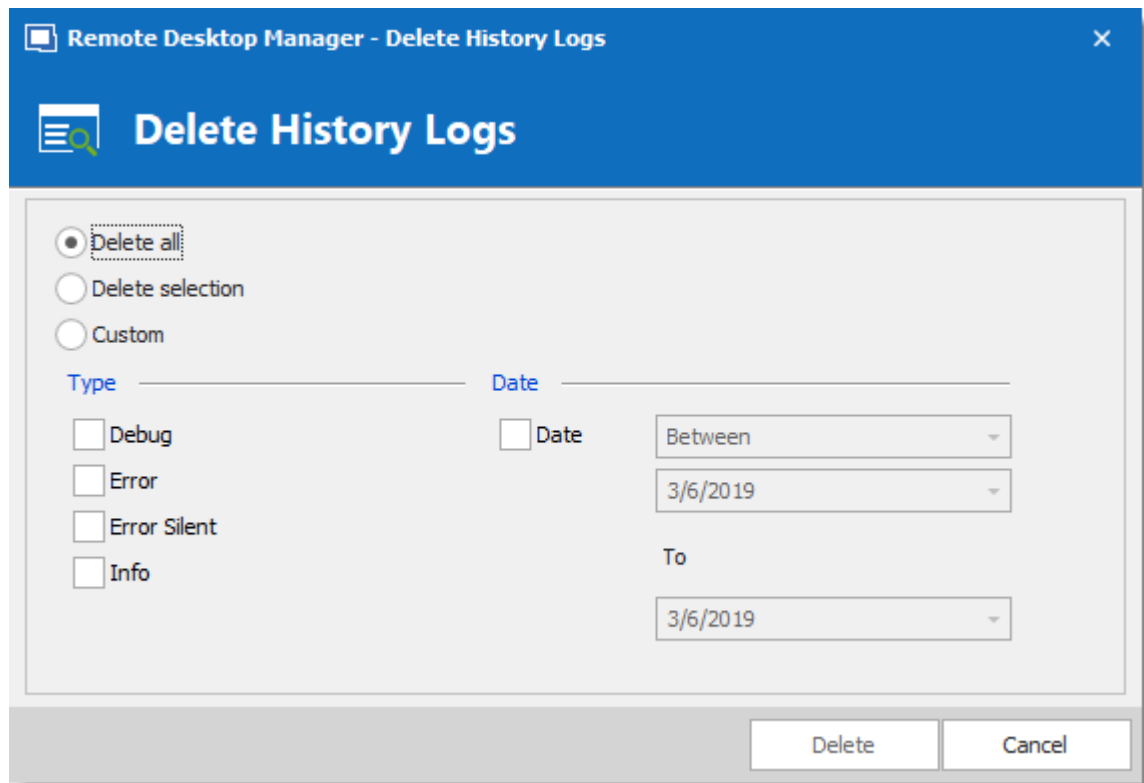
A report of the logs can be saved in a text file as well. Simply navigate to the **Report** tab of the application log, then click on the **Save** button to select a location to save the file.



## 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.

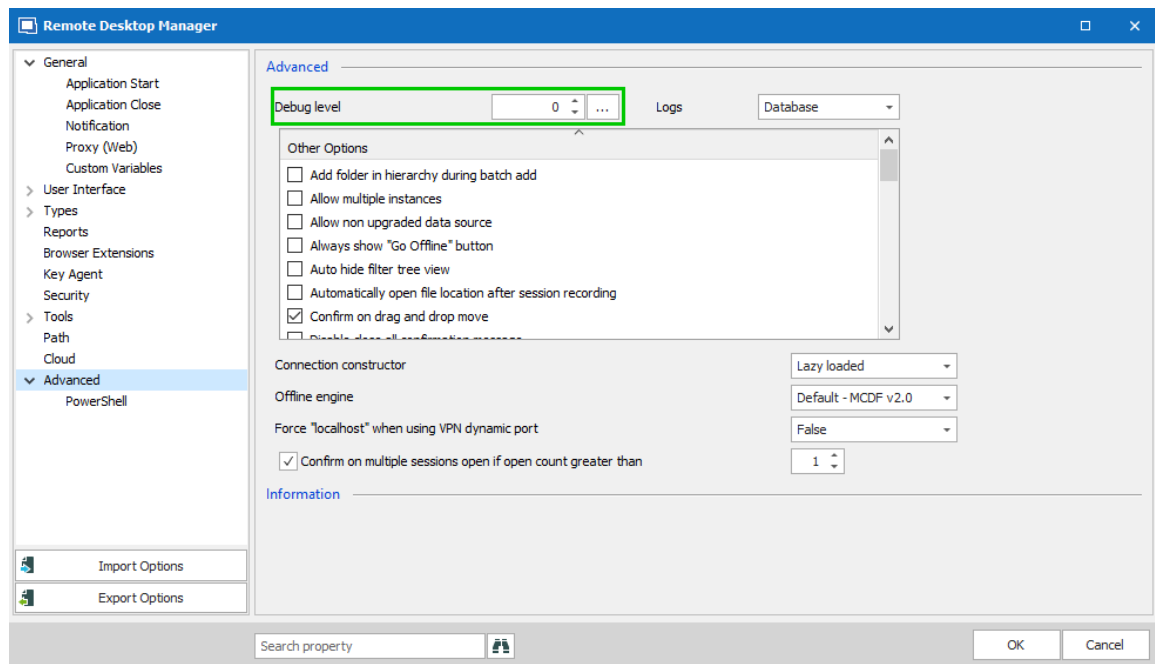


## INCREASING THE DEBUG LEVEL

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.

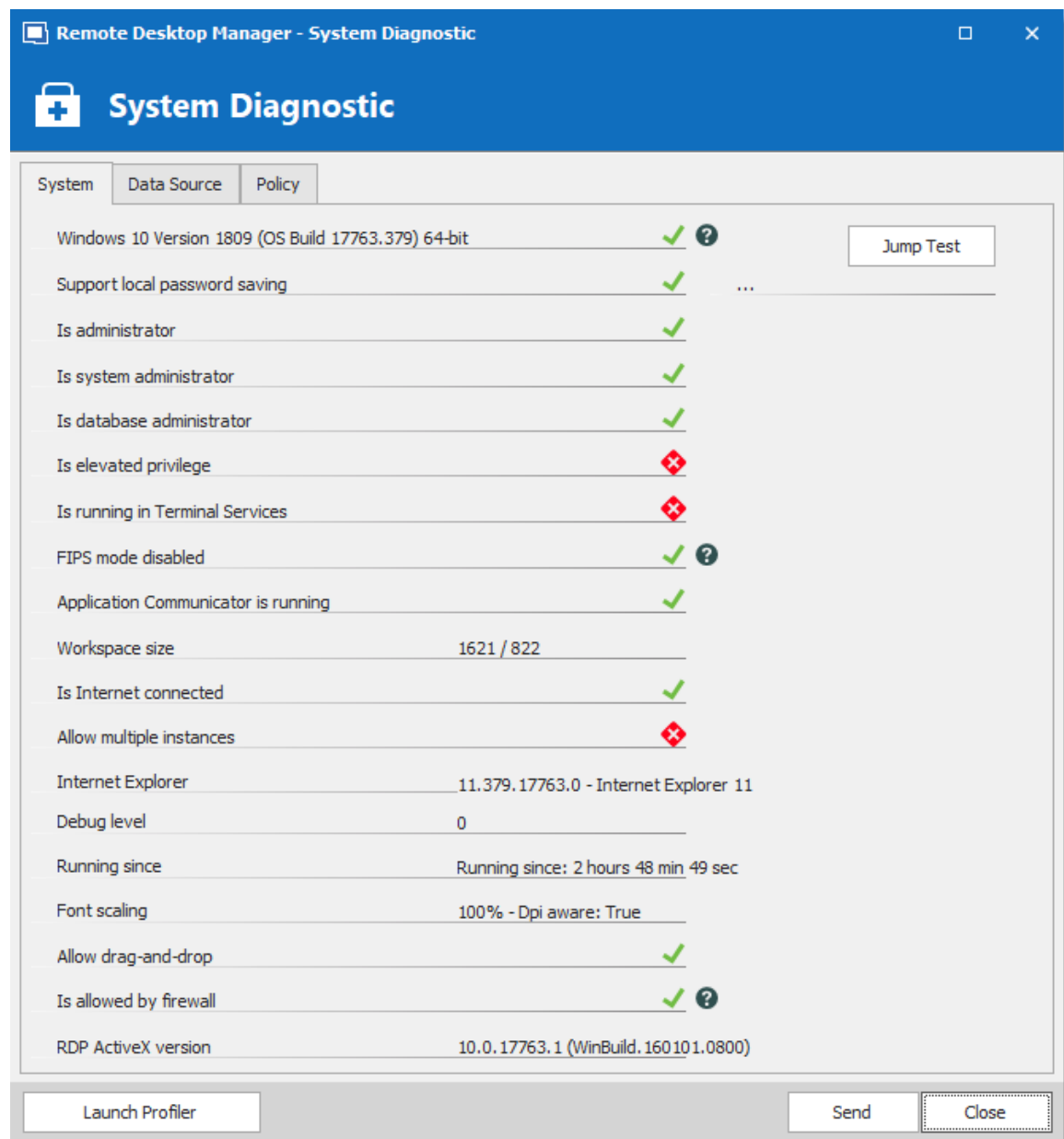
## SYSTEM

The administrator item could be the possible source for security problem. This happens 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



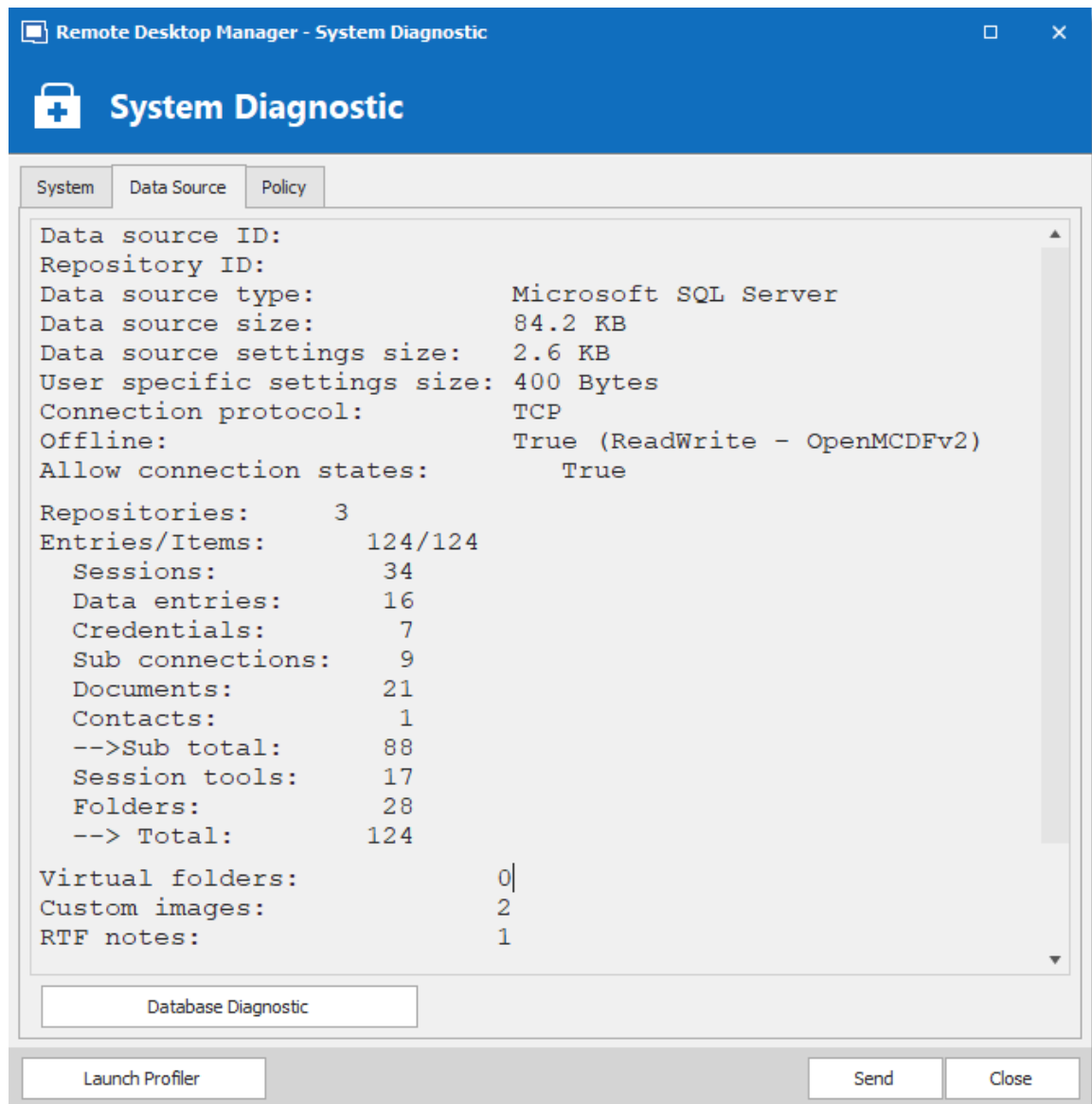
Please read the Troubleshooting topic if experiencing issues with Remote Desktop Manager, it lists error messages and could contain the fix/workaround for your problem.

## 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.



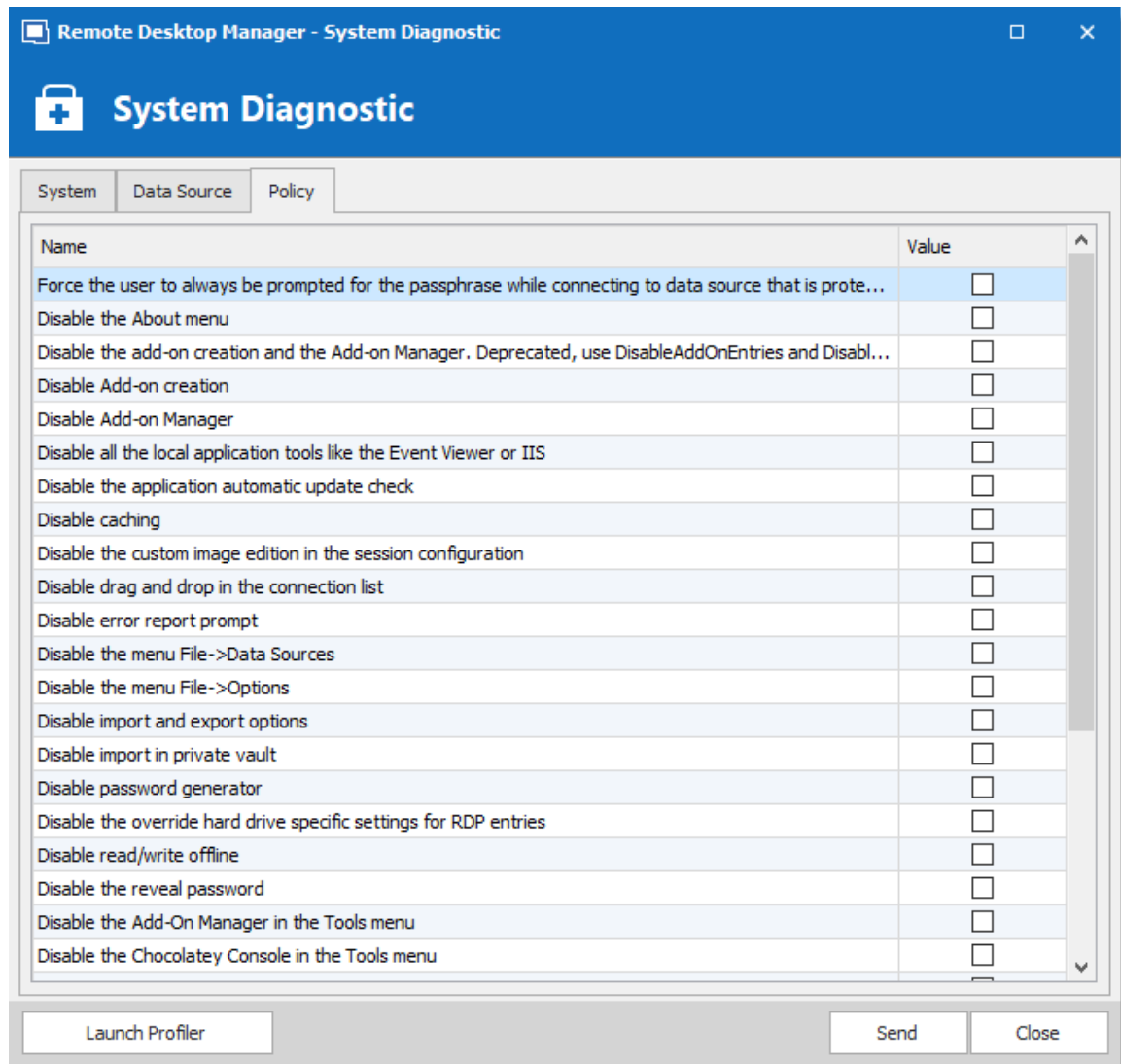
Too many custom images could dramatically increase the size of the data source and cause load time issue.



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.



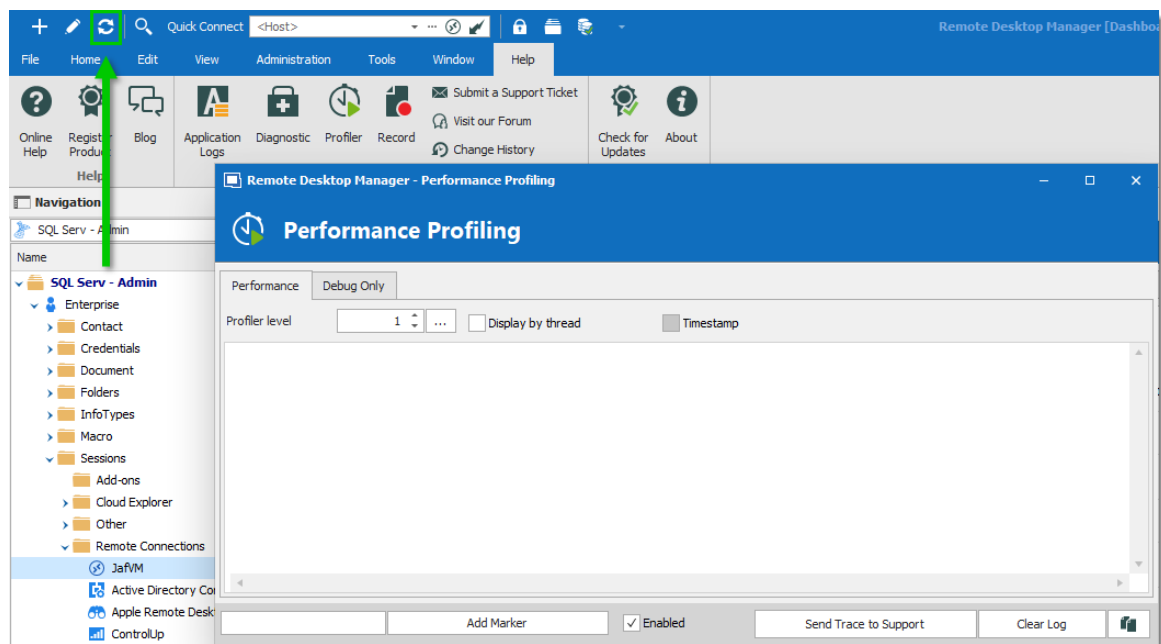
To diagnose startup issues, you can enable the profiler from the command line as described in Command Line Arguments

## PROCEDURE

1. Once the Profiler is opened, refresh the data source.

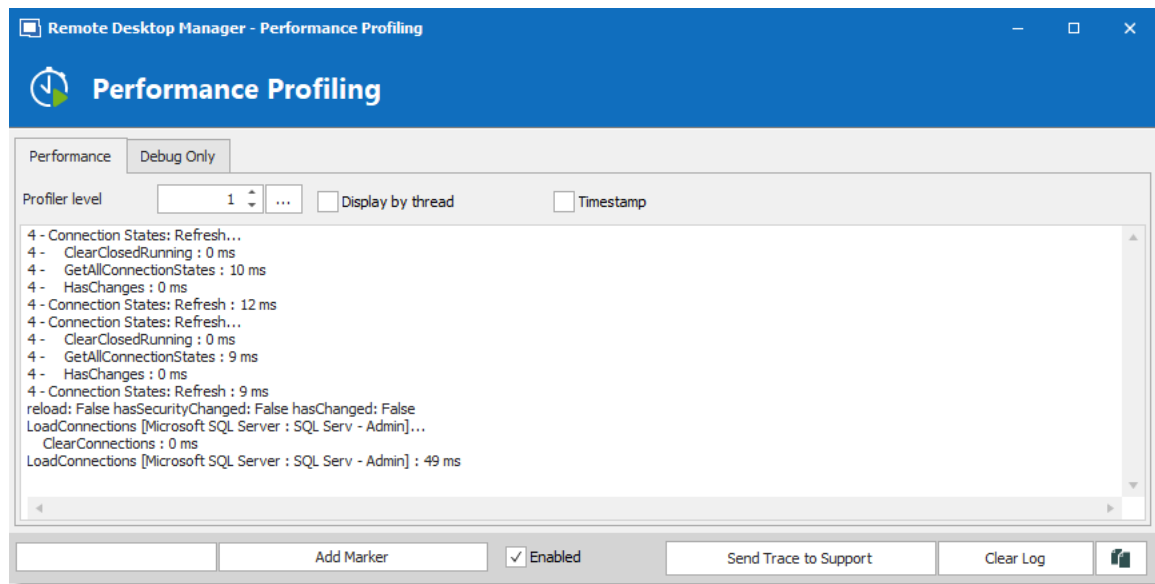


Holding the **Ctrl** key while performing the refresh should force a full reload of the data source, recreating the offline cache.



*Refresh Data Source*

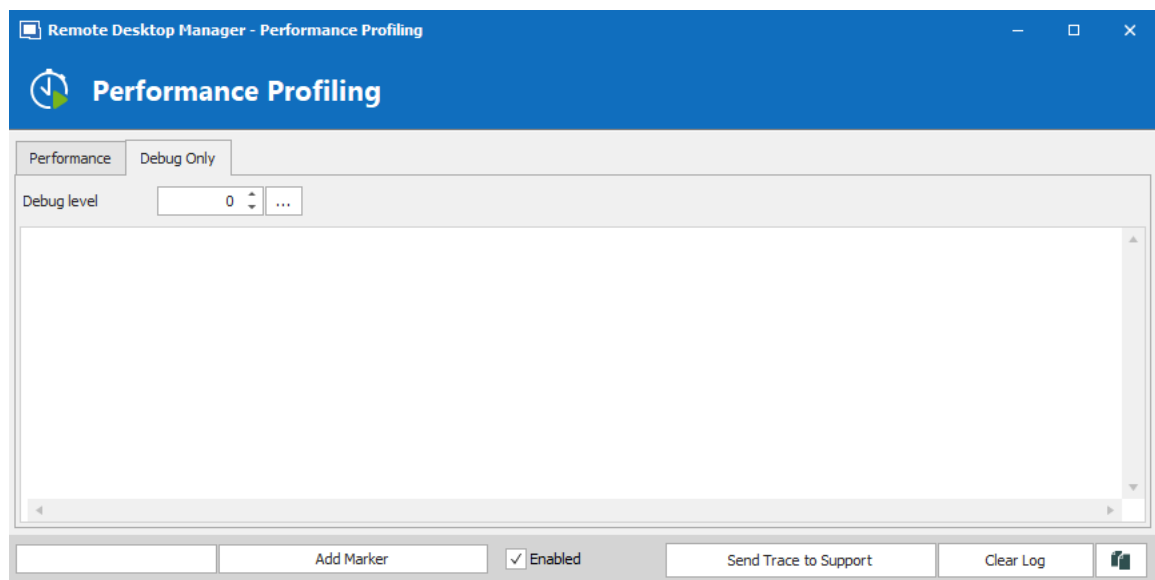
2. The Profiler data will appear in the **Performance Profiling** window.

*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

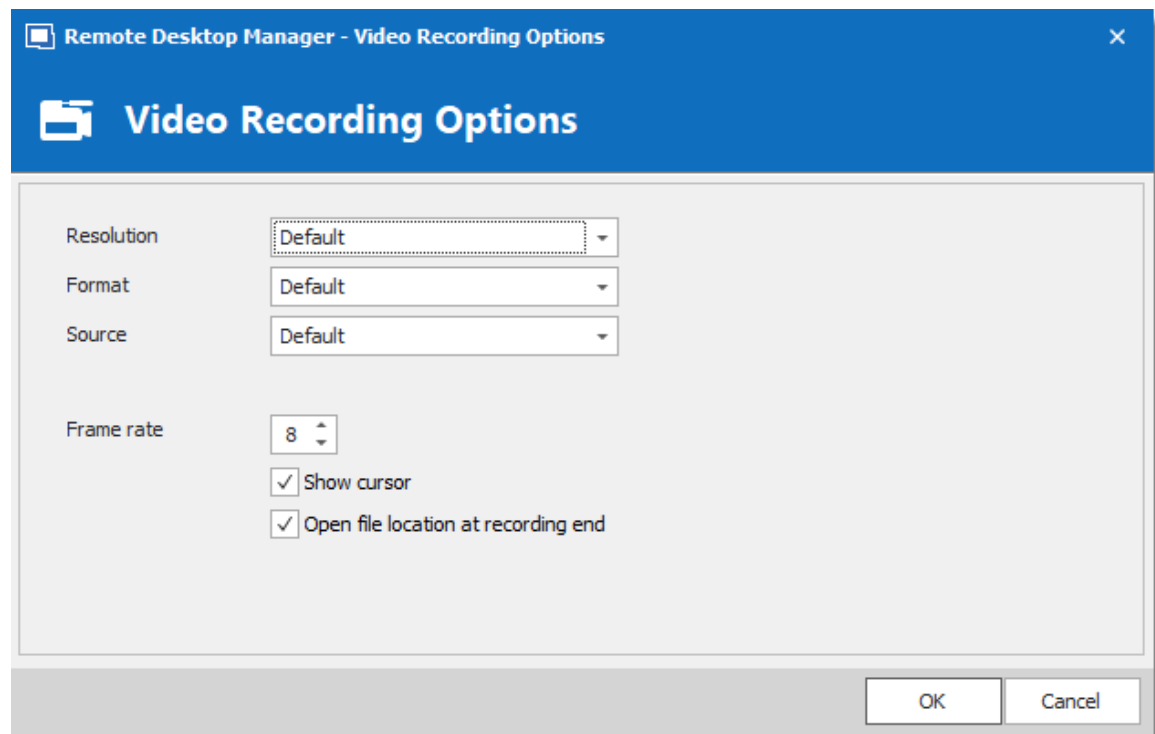
## DESCRIPTION

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

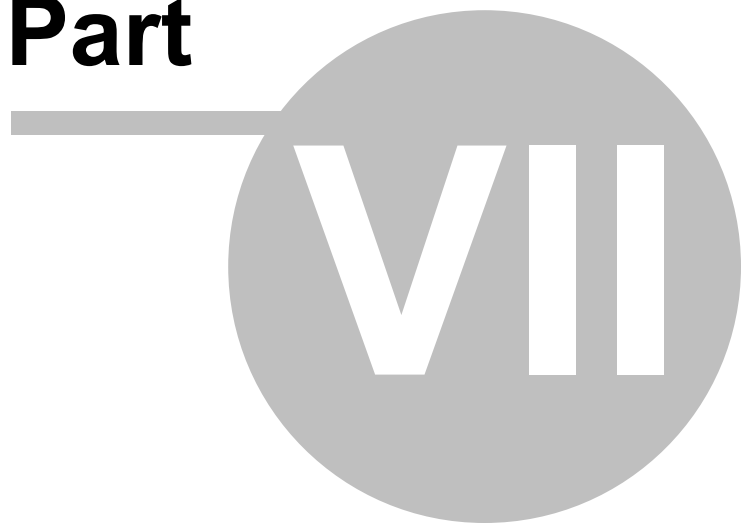
The Video Recording Options uses the MP4 format, which on Vanilla installs of Windows is not supported. If you encounter any difficulty viewing the video we strongly suggest the use of a [VLC player](#).



*Video Recording Options*

# Devolutions Web Login

**Part**









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 Devolutions 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.

 <b>Remote Desktop Manager</b> Centralize, Manage and Secure Remote Connections	 <b>Devolutions Server</b> Secure, Manage and Monitor Access to Privileged Accounts	 <b>Devolutions Password Hub</b> 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.	Devolutions 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.



**Warning for all Remote Desktop Manager users:**

The **Devolutions Web Login (DWL)** was created for a normal desktop environment. It uses Inter-process communication (IPC) with the client application. Using it on a remote desktop server introduces a level of risk that may be unacceptable for corporate users.

Safe usage of **DWL** requires a manual configuration of both **RDM** and **DWL** on each user profiles. For more information about the subject visit our [Secure Devolutions Web Login](#) topic.

## 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:

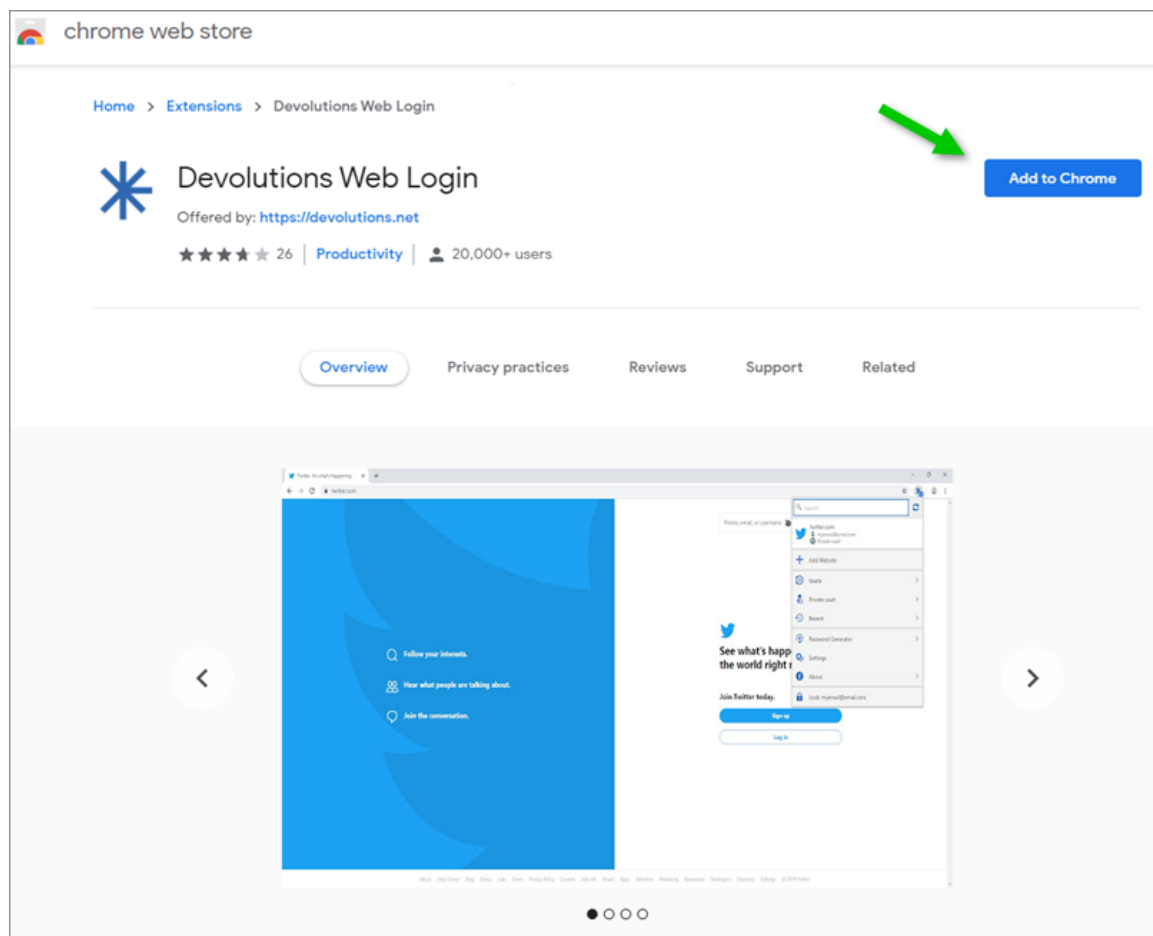
- [Chrome](#)
- [Firefox](#)
- [Edge](#)
- [Opera](#)

## 7.2.1 Chrome

### DESCRIPTION

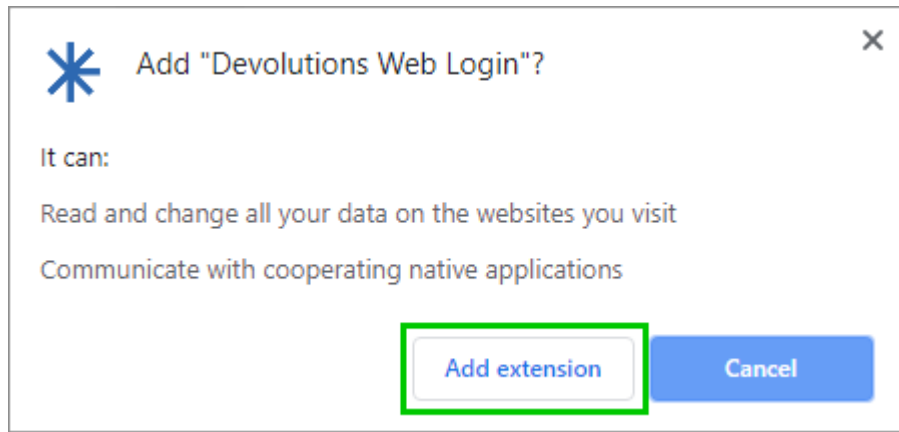
Follow the steps below to complete the installation of Devolutions Web Login in the Chrome web browser.

1. Open Chrome.
2. Navigate to [Devolutions Web Login extension](#) or use the link from our [Website](#).
3. Click the **Add To Chrome** button.



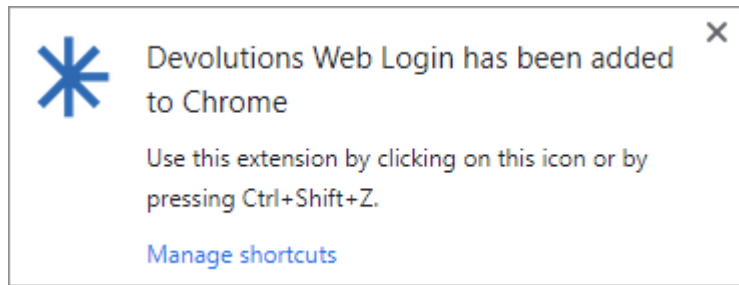
*Devolutions Web Login Chrome Web Store*

4. Click **Add extension** in the confirmation dialog.

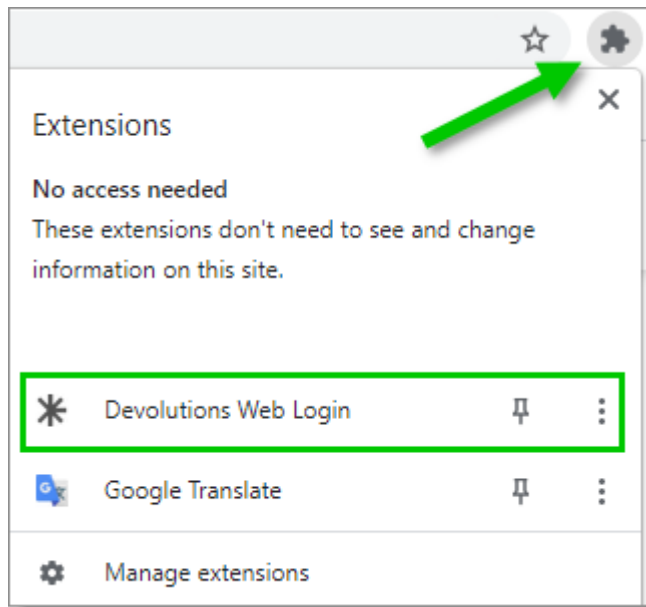


*Extension Installation Confirmation*

Once installed a confirmation box will appear.



5. Click the Chrome extension button and Pin Devolutions Web Login to finish the installation.



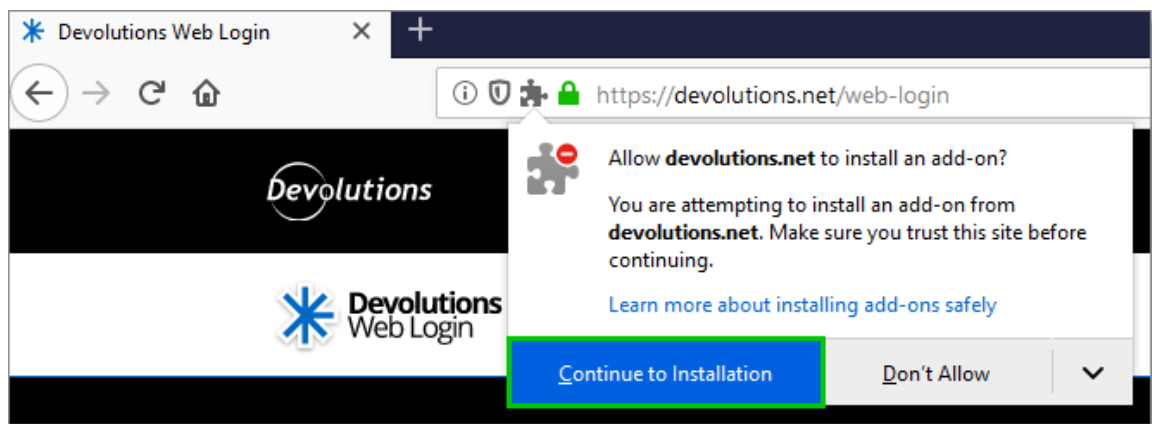
*Devolutions Web Login Extension Button*

## 7.2.2 Firefox

### DESCRIPTION

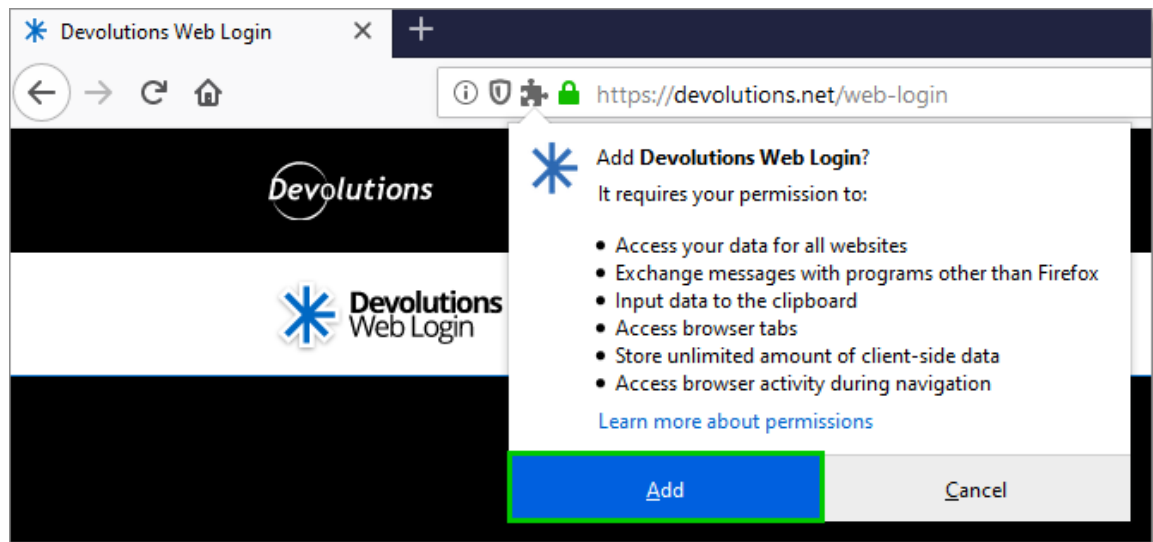
Follow the steps below to complete the installation of Devolutions Web Login in the Firefox web browser.

1. Open a Firefox window.
2. Download the extension from our [Devolutions Web Login](https://devolutions.net/web-login) website page.
3. Click ***Continue to Installation*** in the confirmation dialog.



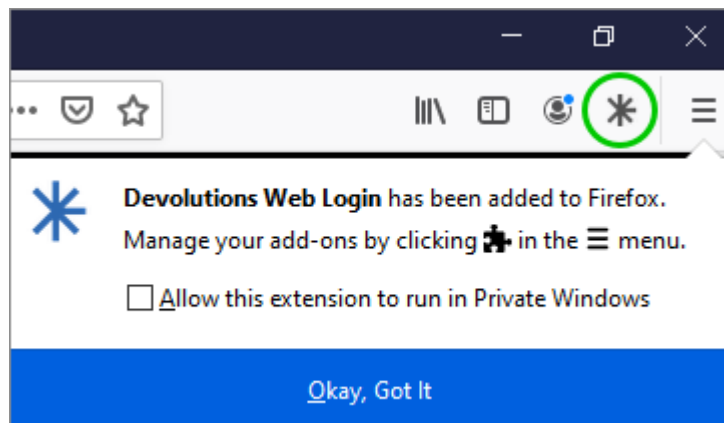
*Continue to Installation*

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.



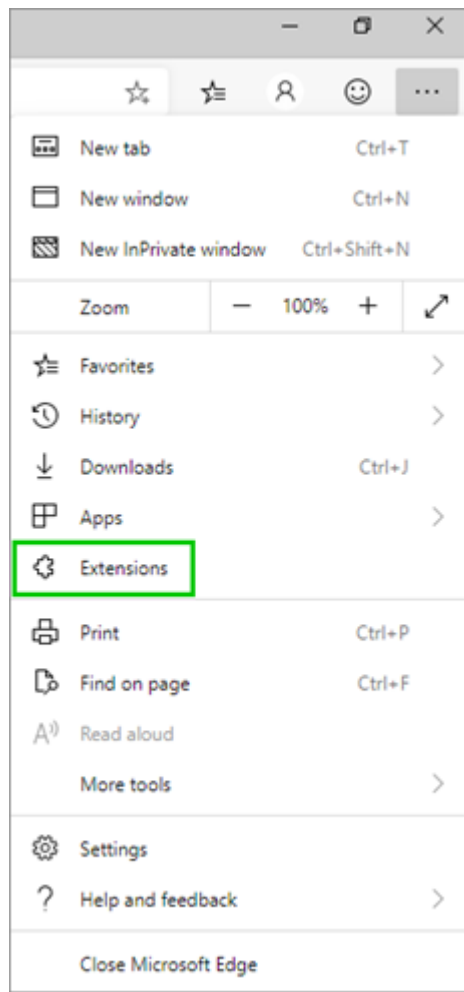
*Devolutions Web Login Extension Button*

### 7.2.3 Edge

#### DESCRIPTION

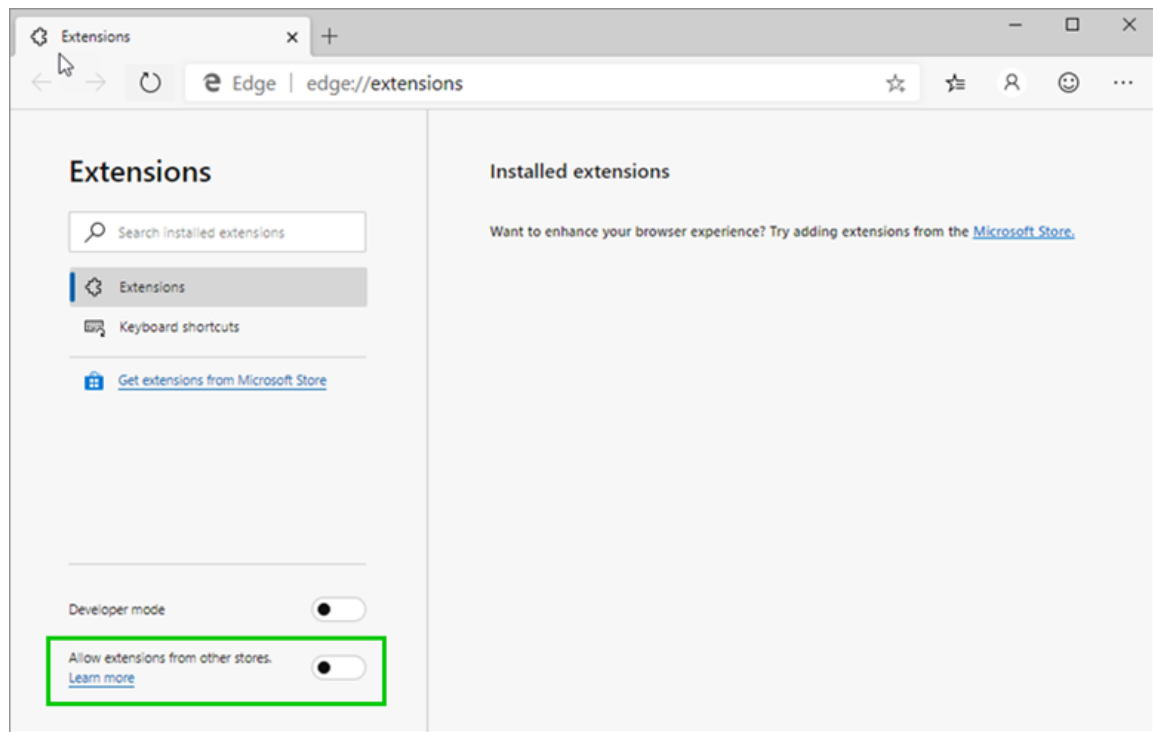
Here are the steps to install Devolutions Web Login on Microsoft Edge Beta.

1. Open [Microsoft Edge Beta](#).
2. Click on **Extensions** in the menu of the browser.



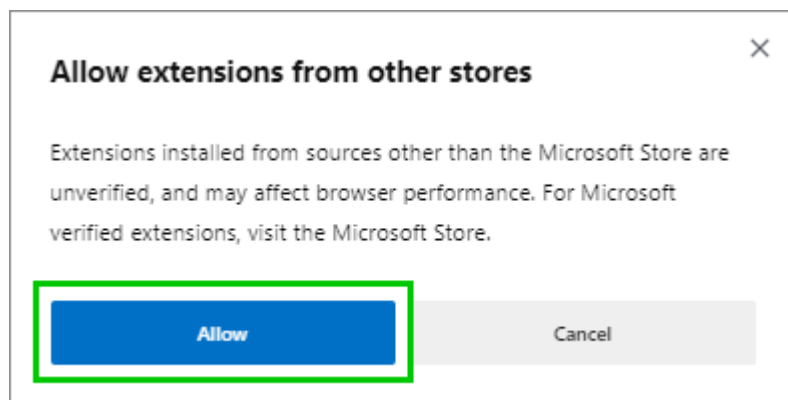
*Microsoft Edge Beta Menu*

3. Allow extensions from other stores.



*Allow Extensions*

4. Allow Non Microsoft Store Extensions.



*Allow Non Microsoft Store Extensions*

5. Follow the extension from [Devolutions Web Login](#) website page to the Chrome Web Store.
6. Click **Add to Chrome**.



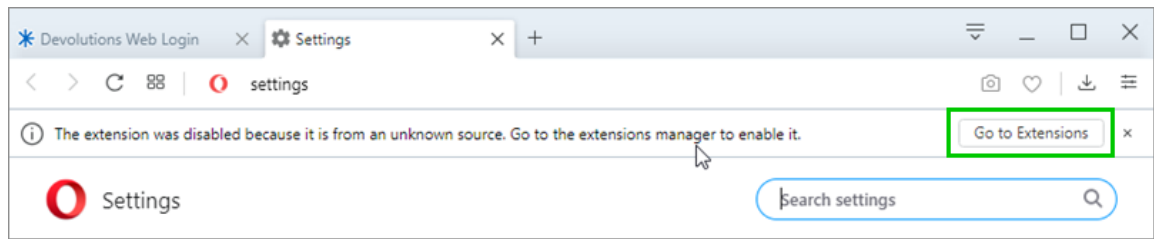


## 7.2.4 Opera

### DESCRIPTION

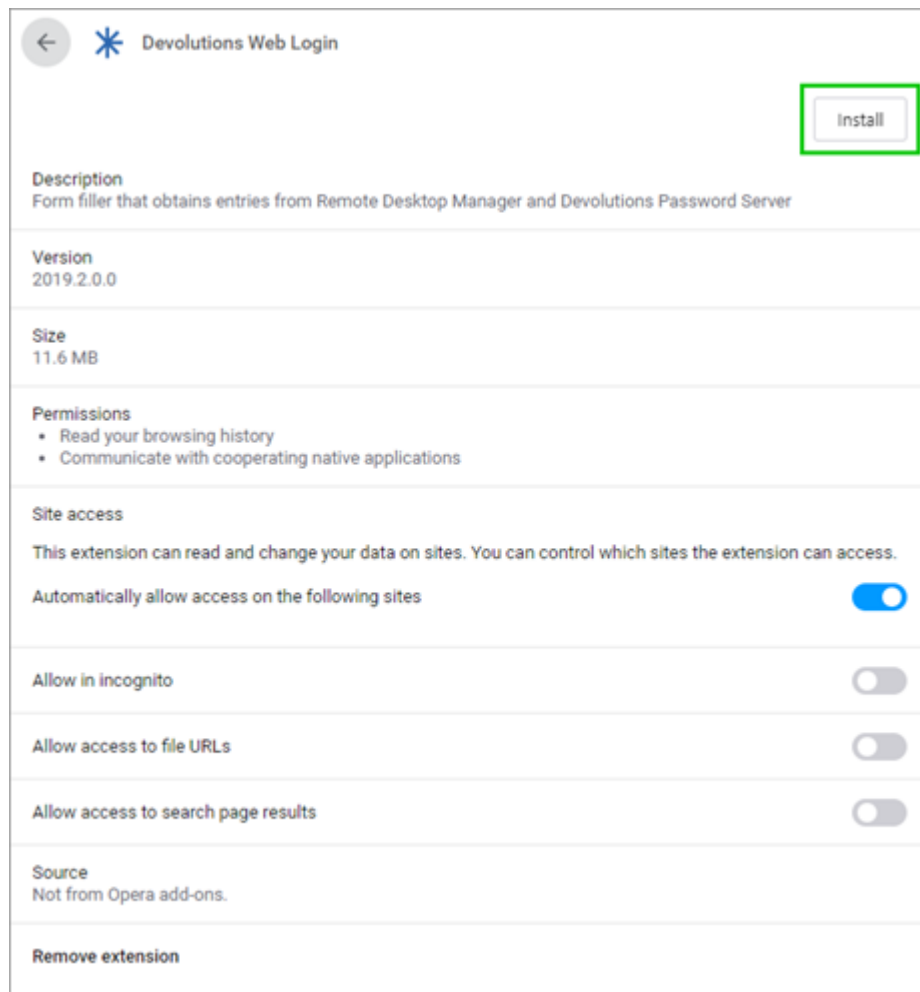
Follow the steps below to complete the installation of Devolutions Web Login in the Opera web browser.

1. Open Opera.
2. Download the extension of [Devolutions Web Login](#) from our website page.
3. Go to **Browser Settings** in the easy setup of Opera.
4. Drag and drop the .crx file from step 2 from the downloads in the web browser.
5. Click on **Go to Extension** from the information panel at the top.



*Opera Extensions Enabling*

6. Click **Install** and the **Yes, install** pop up.



*Opera Install Window*

7. Access the extension by clicking \* in the top-right corner of Opera.

## 7.3 First Login

### 7.3.1 Password Hub

## DESCRIPTION

## FIRST LOGIN WITH DEVOLUTIONS WEB LOGIN

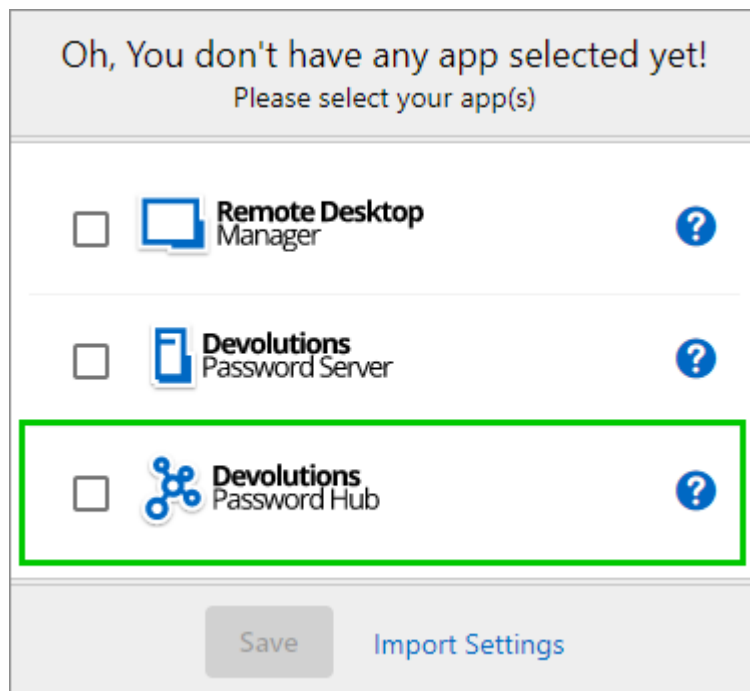
Follow these steps to connect Devolutions Password Hub to Devolutions Web Login extension:

1. Click on **Devolutions Web Login** \* extension at the top right corner of your browser.



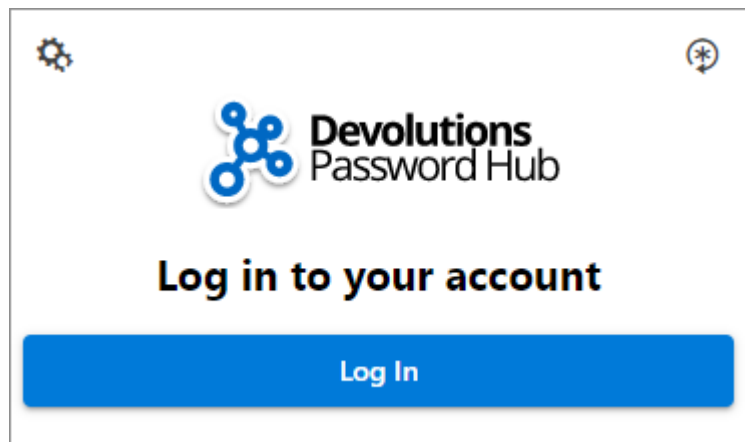
A Devolutions Password Hub access is required to continue.

2. Choose **Devolutions Password Hub** in the list and **Save**. You could at this point import settings; the option will also be available in the [Settings](#) menu after the log in.



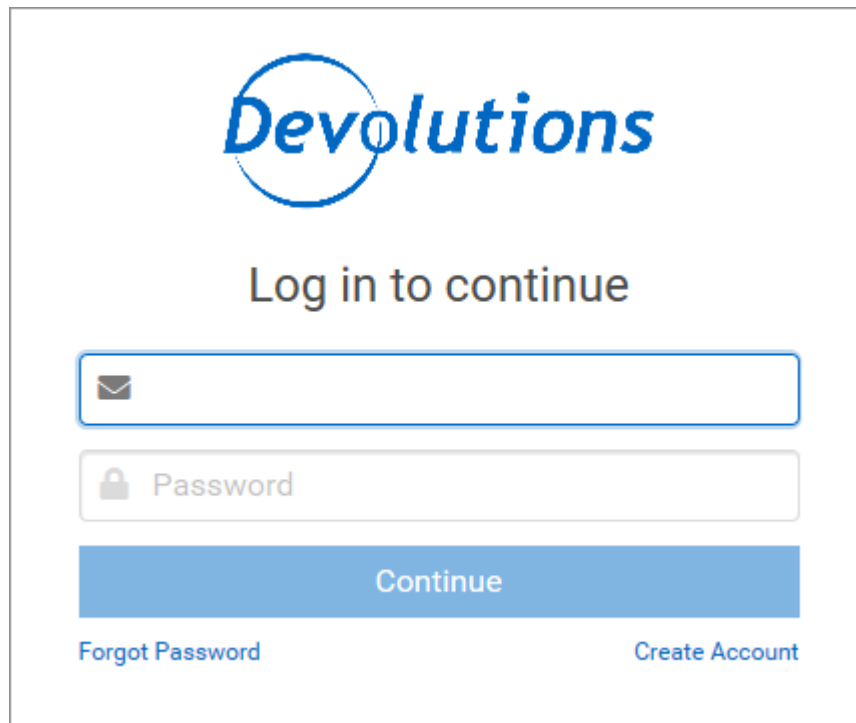
*First Login*

3. **Log in** to your account.




*Log In*

4. Enter the credentials from your Devolutions Account to continue.

The image shows the Devolutions Account Login screen. At the top is the "Devolutions" logo in a blue, stylized font. Below it is the text "Log in to continue". There are two input fields: the first is for an email address, indicated by an envelope icon, and the second is for a password, indicated by a lock icon and the label "Password". Below these fields is a large blue button with the text "Continue". At the bottom left is a link "Forgot Password" and at the bottom right is a link "Create Account".

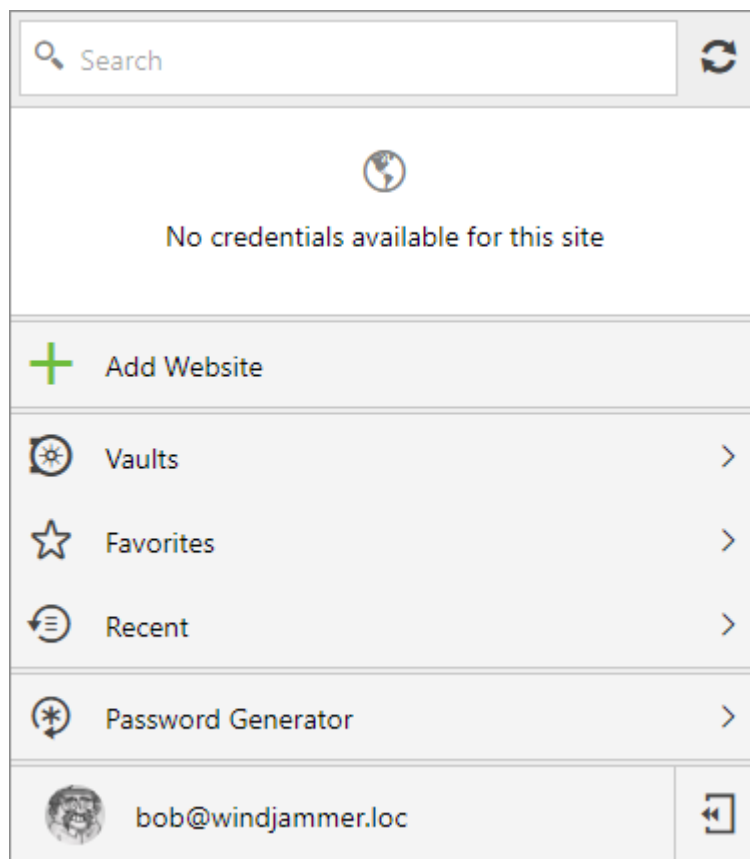
*Devolutions Account Login*

5. Unlock the vault with your master key.



Devolutions Web Login will recognize automatically the Password Hub linked to your Devolutions account. Click **Change** to modify the URL.

Devolutions Web Login is now connected to your vaults.



*Devolutions Web Login Connected to Devolutions Password Hub*

### 7.3.2 Devolutions Server

## 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**. You could at this point import settings; the option will also be available in the [Settings](#) menu after the log in.

Oh, You don't have any app selected yet!  
Please select your app(s)

<input type="checkbox"/>	 Remote Desktop Manager	
<input type="checkbox"/>	 Devolutions Password Server	
<input type="checkbox"/>	 Devolutions Password Hub	

Save Import Settings

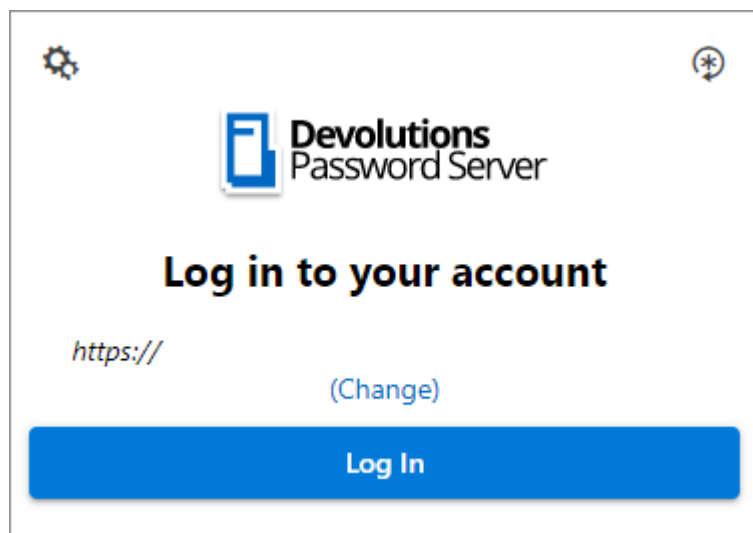
*First Login*

3. Enter the server address. Test the connection to validate it, then **Save**.



*Server Address*

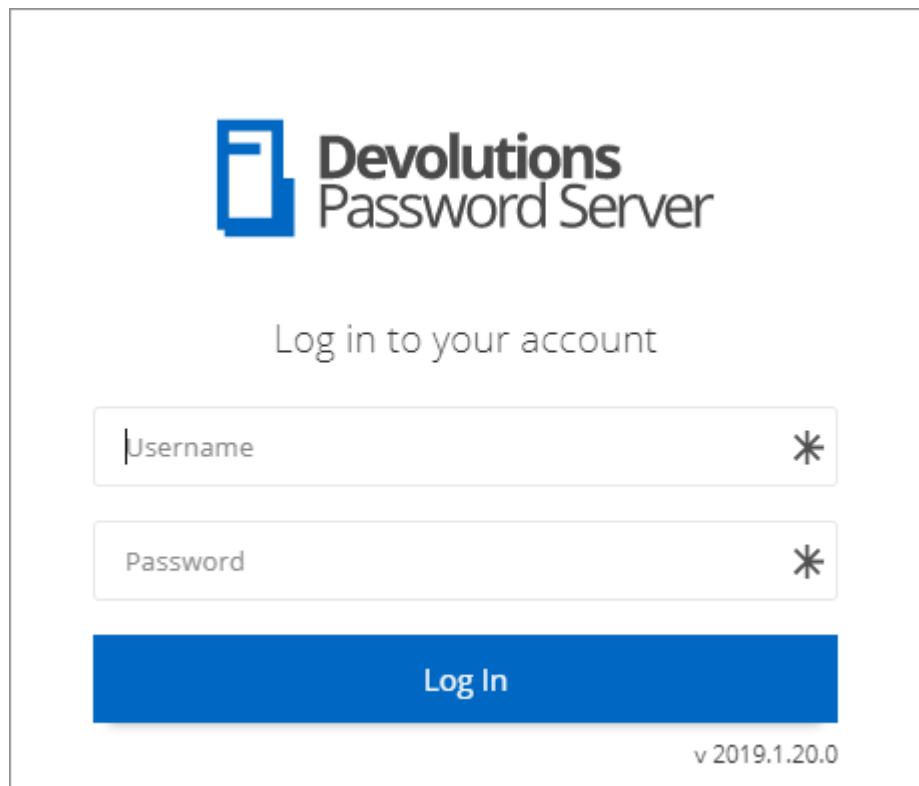
4. Press the **Log In** after you saved the address.



*Devolutions Web Login Login*

5. Enter your Devolutions Server credentials and log in.

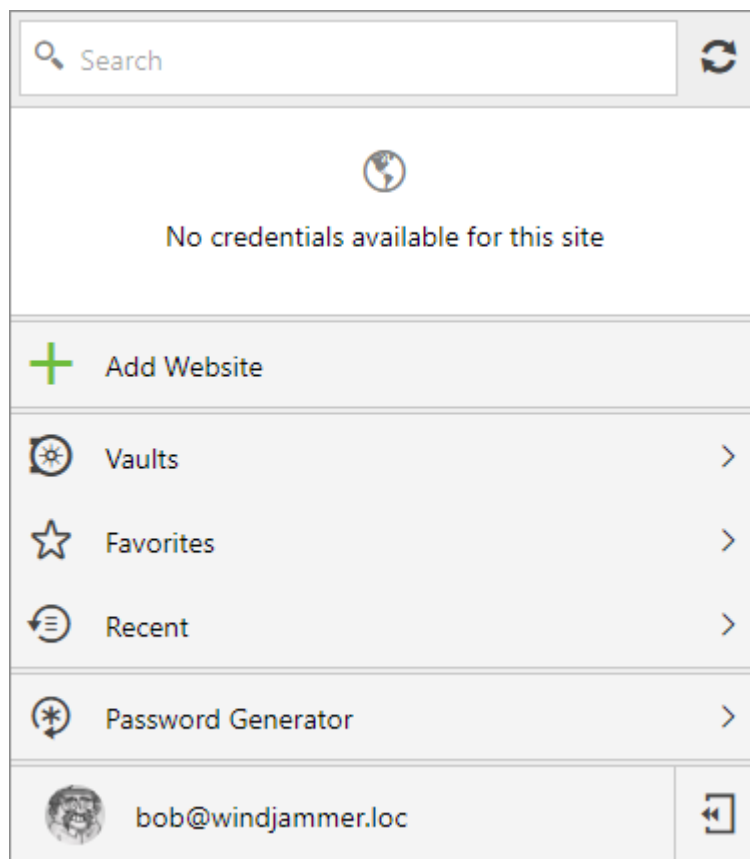




The image shows a login window for Devolutions Password Server. At the top left is the Devolutions logo, a blue square with a white 'F' shape inside. To its right is the text 'Devolutions Password Server'. Below this is the instruction 'Log in to your account'. There are two input fields: the first is labeled 'Username' and the second is labeled 'Password'. Both fields have a small asterisk icon to their right. Below the input fields is a large blue button with the text 'Log In'. In the bottom right corner of the window, the version number 'v 2019.1.20.0' is displayed.

*Devolutions Server Login*

Devolutions Web Login is now connected to your vaults.



*Devolutions Web Login Connected*

### 7.3.3 Remote Desktop Manager

## DESCRIPTION

### FIRST LOGIN WITH DEVOLUTIONS WEB LOGIN

Follow these steps to connect your Remote Desktop Manager to Devolutions Web Login extension:







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.

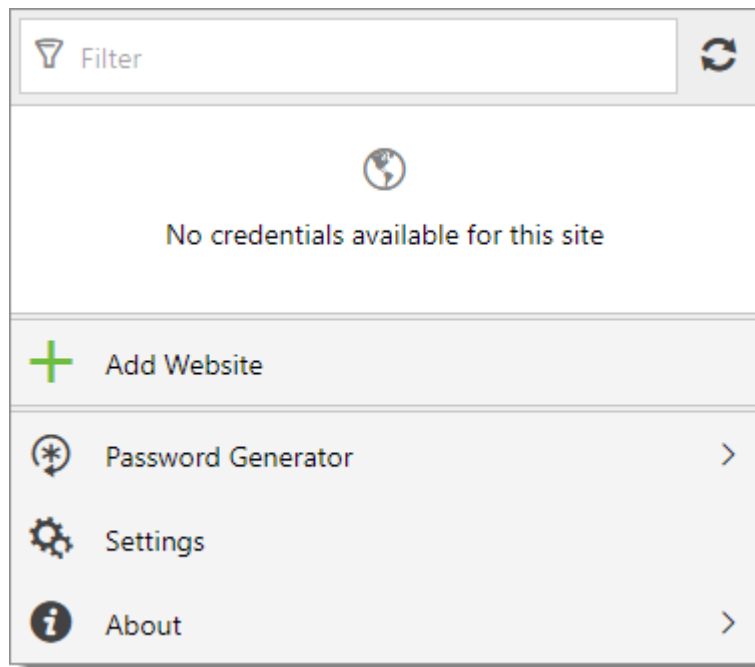
2. Choose **Remote Desktop Manager** in the list and **Save**. You could at this point import settings; the option will also be available in the [Settings](#) menu after the log in.

Oh, You don't have any app selected yet!  
Please select your app(s)

<input type="checkbox"/>	 <b>Remote Desktop Manager</b> 
<input type="checkbox"/>	 <b>Devolutions Password Server</b> 
<input type="checkbox"/>	 <b>Devolutions Password Hub</b> 

*First Login*

You will be automatically connected to your vaults.



*Devolutions Web Login Connected*

## 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 Devolutions Password Hub.

See below a list of the menu and information available from the Devolutions Web Login extension:

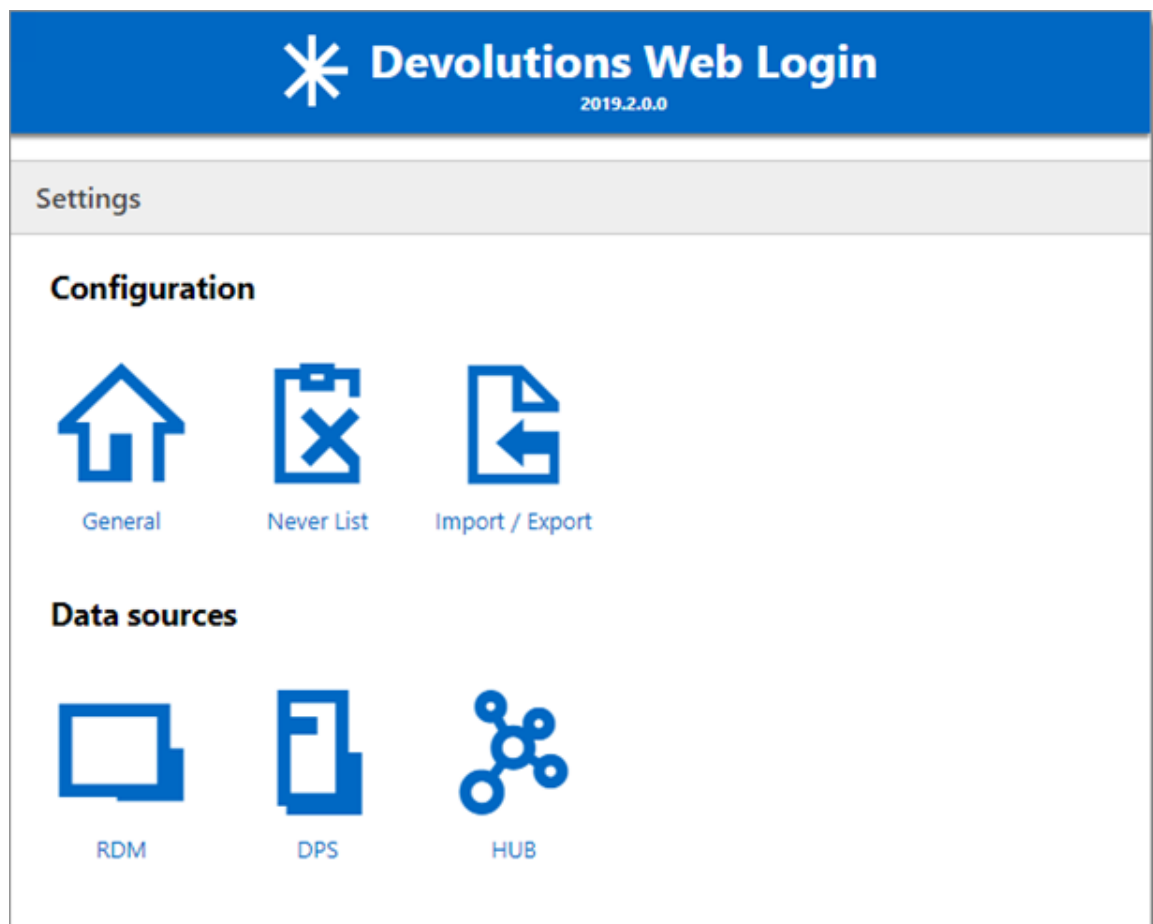
- Refine the credential list available with the **search**.
- **Add a website** from Devolutions Web Login in a specific folder located in a vault or your User Vault.
- **Visualize the credential** stored in the vaults if you are connected with Devolutions Server or Devolutions Password Hub.
- Browse **recently used 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.
- Color the fields that are filled with Devolutions Web Login
- Disable the analytics 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 too Never show icons in field.
- Matching options are: Base domains, Host, Starts with, RegEx and Exact.

To remove a website from the never list click the **trash can** icon next to it. To edit an entry, delete it and create another.

The **Import / Export** setting 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 [Devolutions Password Hub](#).

## 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	<p>Devolutions Web Login automatically search for credentials in the data source when connecting to a website.</p> <p>If disabled, click on the Devolutions Web Login extension icon to manually retrieve credentials.</p>
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	<p>Secure the port with an application key by using the same code in Remote Desktop Manager and Devolutions Web Login.</p> <p>Navigate to <b>File – Options – Browser Extensions</b> in Remote Desktop Manager to set the application key.</p>

ADVANCED OPTIONS	DESCRIPTION
<b>Enable native messaging</b>	Exchange messages with a native application installed on the user's computer.
<b>Use legacy API</b>	Use the old browser extension API for compatibility with older versions of Remote Desktop Manager.

## DEVOLUTIONS SERVER

GENERAL OPTIONS	DESCRIPTION
<b>Enable Devolutions Server</b>	Retrieve entries from Devolutions Server.
<b>Destination folder</b>	Choose the folder where the credentials are stored in the vault.
<b>Server URL</b>	Enter the URL of the Devolutions Server instance to connect to.

ACTION OPTIONS	DESCRIPTION
<b>Automatically retrieve credentials on page load</b>	<p>Devolutions Web Login automatically search for credentials in the data source when connecting to a website.</p> <p>If disabled, click on the Devolutions Web Login extension icon to manually retrieve credentials.</p>
<b>Automatically fill in credentials on load</b>	Fill automatically the credentials when loading a web page.
<b>Automatically submit the form after filling</b>	Submit the credentials automatically when the fields are filled.



## DEVOLUTIONS PASSWORD HUB

GENERAL OPTIONS	DESCRIPTION
<b>Enable Devolutions Password Hub</b>	Retrieve entries from Devolutions Password Hub.
<b>Server URL</b>	Enter the URL of the Devolutions Password Hub instance to connect to.
ACTION OPTIONS	DESCRIPTION
<b>Automatically fill in credentials on load</b>	Fill automatically the credentials when loading a web page.
<b>Automatically submit the form after filling</b>	Submit the credentials automatically when the fields are filled
ADVANCED OPTIONS	DESCRIPTION
<b>Devolutions Account login</b>	Set your Devolutions Account login URL.
<b>Show favicon</b>	Display the Devolutions Web Login favicon.

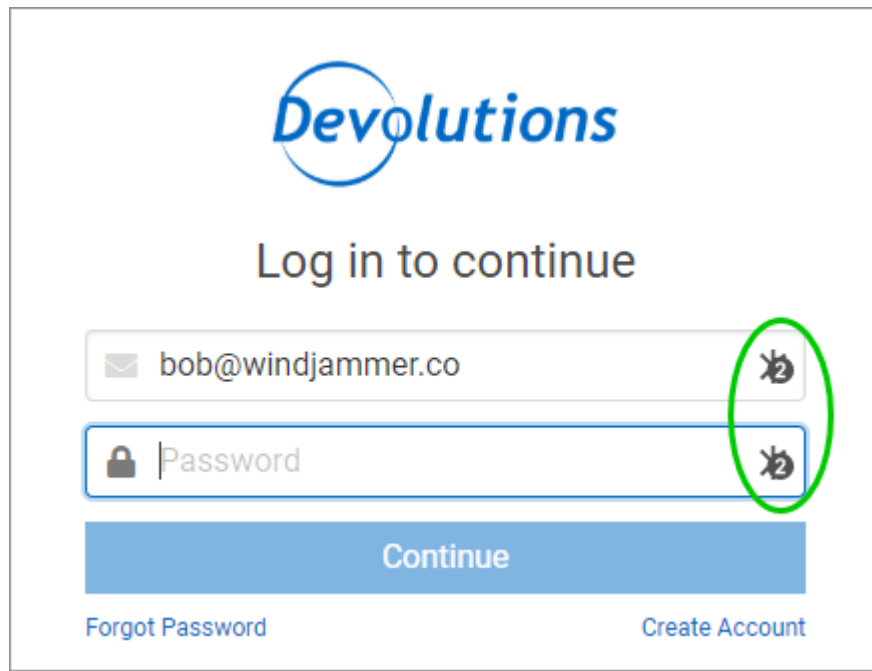
### 7.4.2 Retrieve Credentials

#### 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 to fill in the login information and connect to the website.

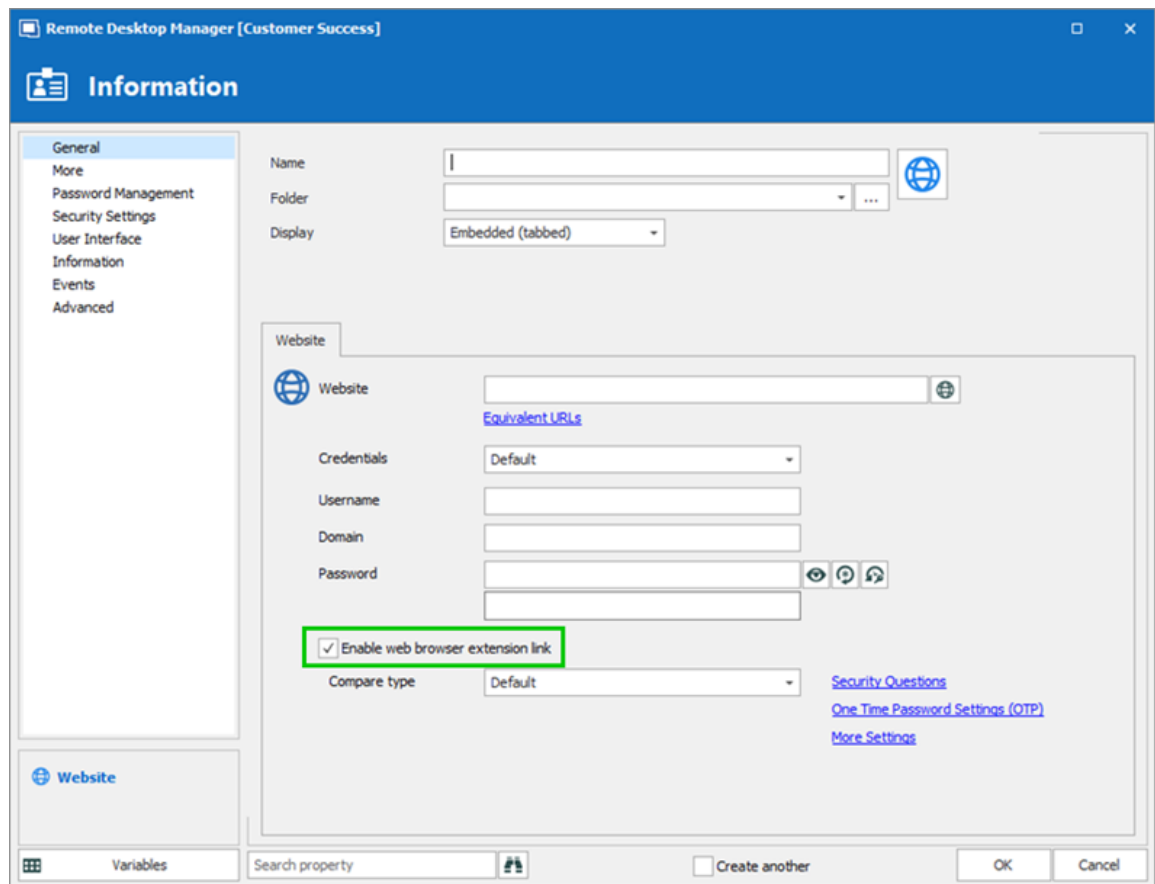
The image shows the Devolutions Web Login interface. At the top is the Devolutions logo. Below it is the text "Log in to continue". There are two input fields: the first contains the email "bob@windjammer.co" and the second is labeled "Password". To the right of each input field is a small icon of a person with a key, which is circled in green. Below the input fields is a blue "Continue" button. At the bottom, there are two links: "Forgot Password" on the left and "Create Account" on the right.

*Automatic Log In*

#### 7.4.2.1 Remote Desktop Manager

### DESCRIPTION

Checkmark **Enable web browser extension link** in Remote Desktop Manager entries to allow Devolutions Web Login extension to retrieve the credentials when connecting to its respective website.



Enable web browser extension link

### 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.

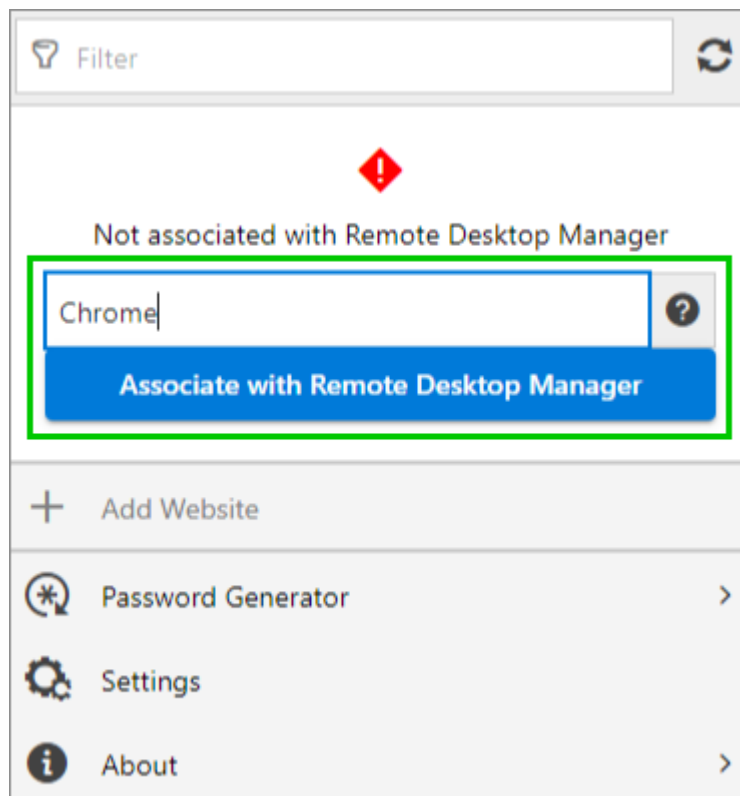
## HOW TO SET UP DEVOLUTIONS WEB LOGIN FOR VERSION 2021.1 AND HIGHER



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.





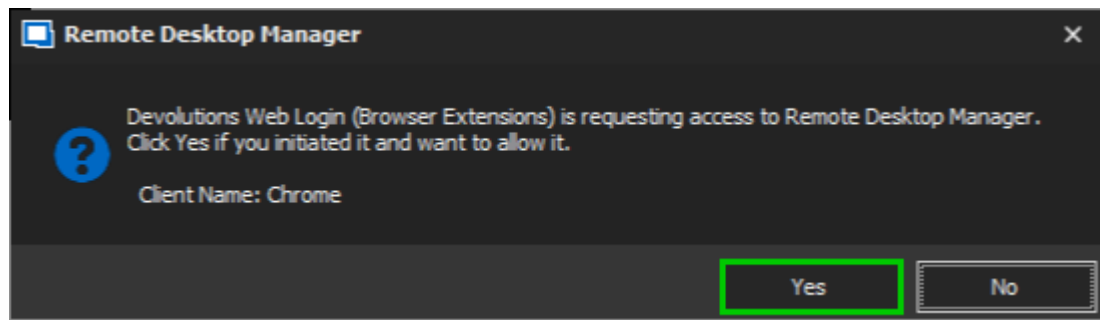
This can be used to identify a particular association and to deny access to it from Remote Desktop Manager. The default name is the name of the web browser running Devolutions Web Login.

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

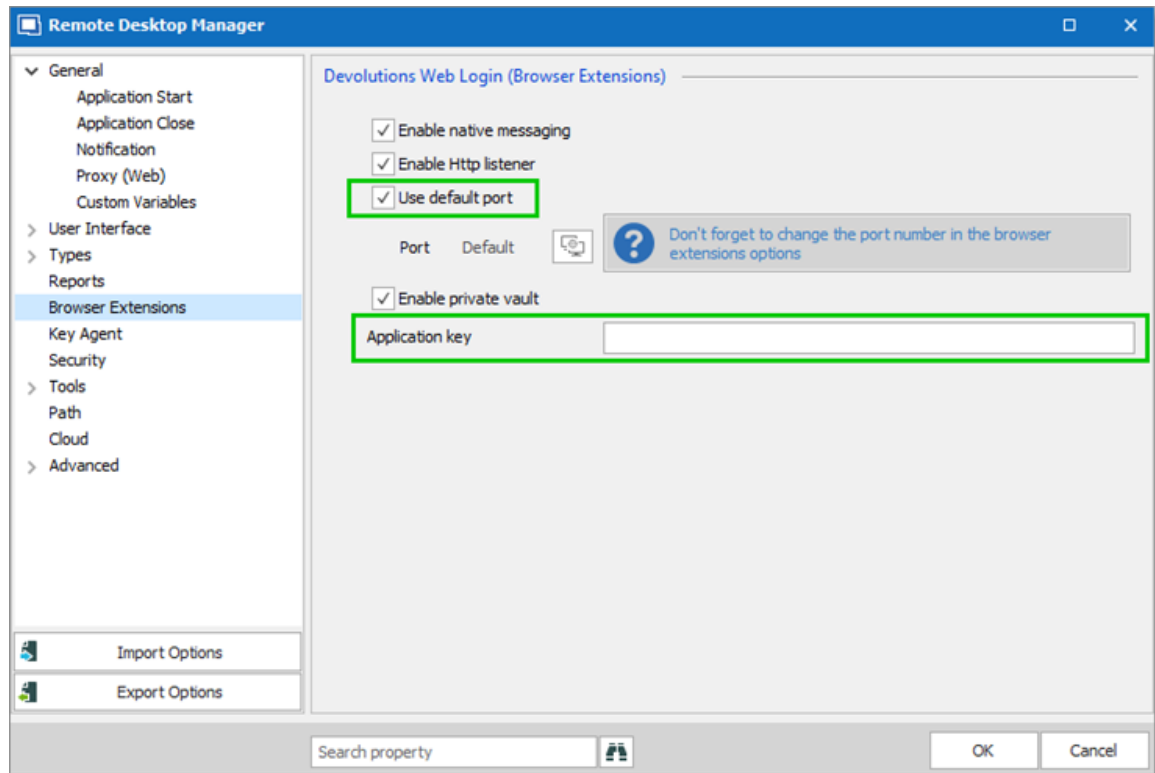


The application key is displayed in clear text, it must be kept secret by the user.

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. Enter a custom port.
4. Type an **Application key** then click **OK**



*Remote Desktop Manager Browser Extensions Options*

5. In your browser, click the Devolutions Web Login icon \* and go to **Settings - Data sources - RDM**.
6. Disable **Use default port**.
7. Enter the custom port created earlier in Remote Desktop Manager and **Save**.

**Settings - RDM**

**General**

☒ Enable Remote Desktop Manager app

**Actions**

☐ Use default port (19443) 6

**Advanced**

Port 7

19443

☒ Add entry in user vault by default

Destination folder

Devolutions Web Login

Save Cancel

8. Click **Advanced** and enter the same **Application key** as Remote Desktop Manager.

**Settings - RDM**

**General**

Application key

**Actions**

**Advanced**

☐ Enable native messaging

☐ Use legacy API

Save Cancel

*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, its creation date and the date when it was last used.

#### 7.4.4 Keyboard Shortcuts

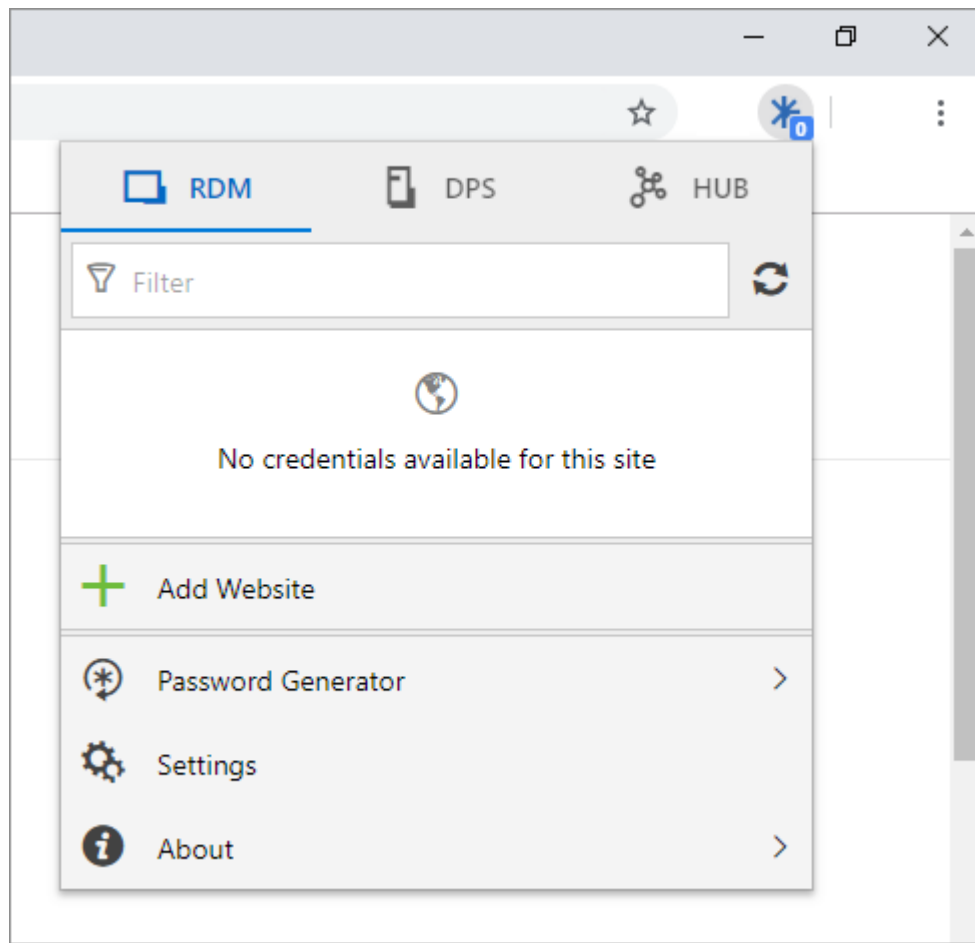
### DESCRIPTION

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.

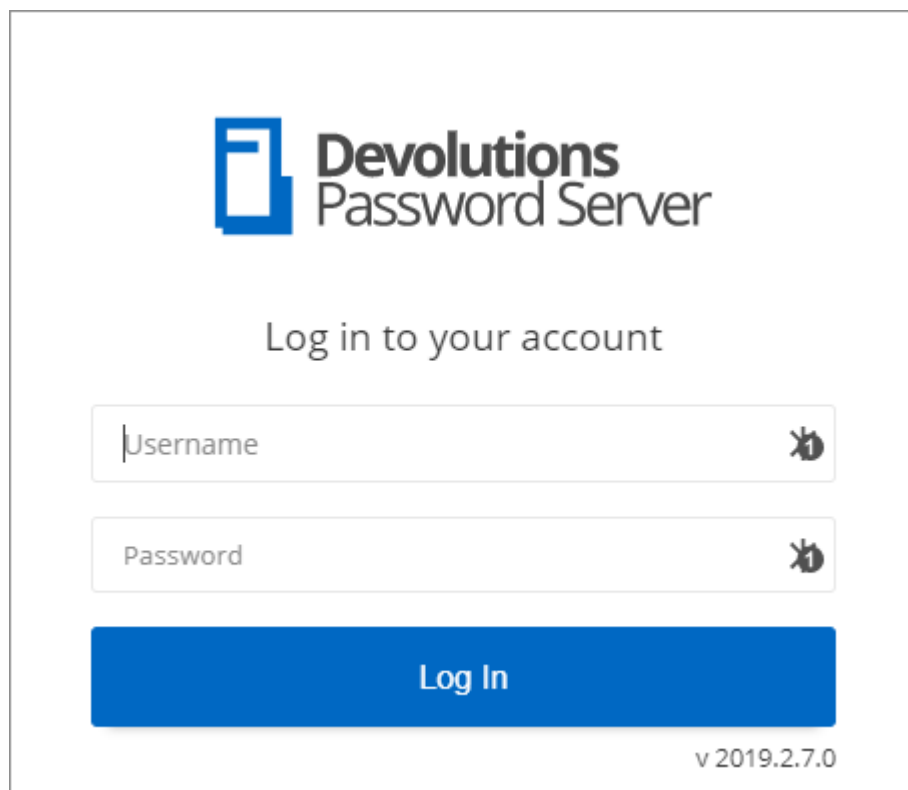




*Devolutions Web Login in Chrome*

## **CTRL+SHIFT+Y**

Use it to auto-fill your credential when only one is available for an entry.

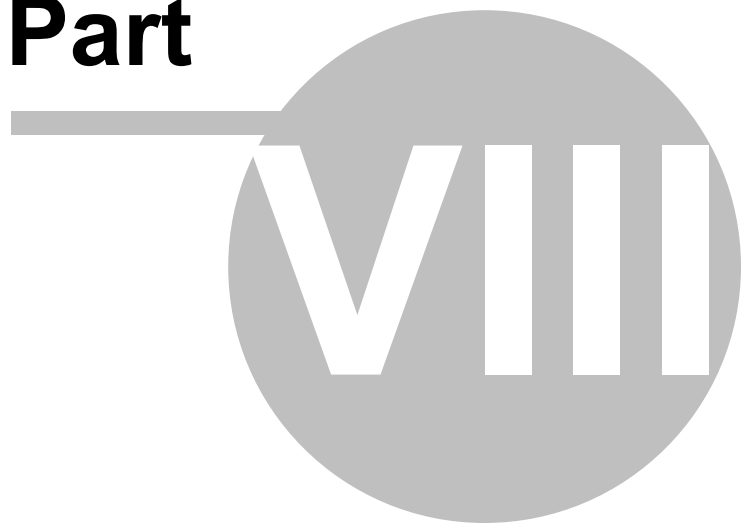


The screenshot shows the Devolutions Password Server login page. At the top is the Devolutions logo, which consists of a blue square with a white stylized 'D' inside, followed by the text 'Devolutions Password Server'. Below the logo is the instruction 'Log in to your account'. There are two input fields: the first is labeled 'Username' and the second is labeled 'Password'. Both fields have a small icon on the right side, which appears to be a key or a similar symbol. Below the input fields is a large blue button with the text 'Log In'. In the bottom right corner of the login area, the version number 'v 2019.2.7.0' is displayed.

*One Credential Login with Devolutions Web Login*

# User Groups Based Access Control

**Part**



## 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.

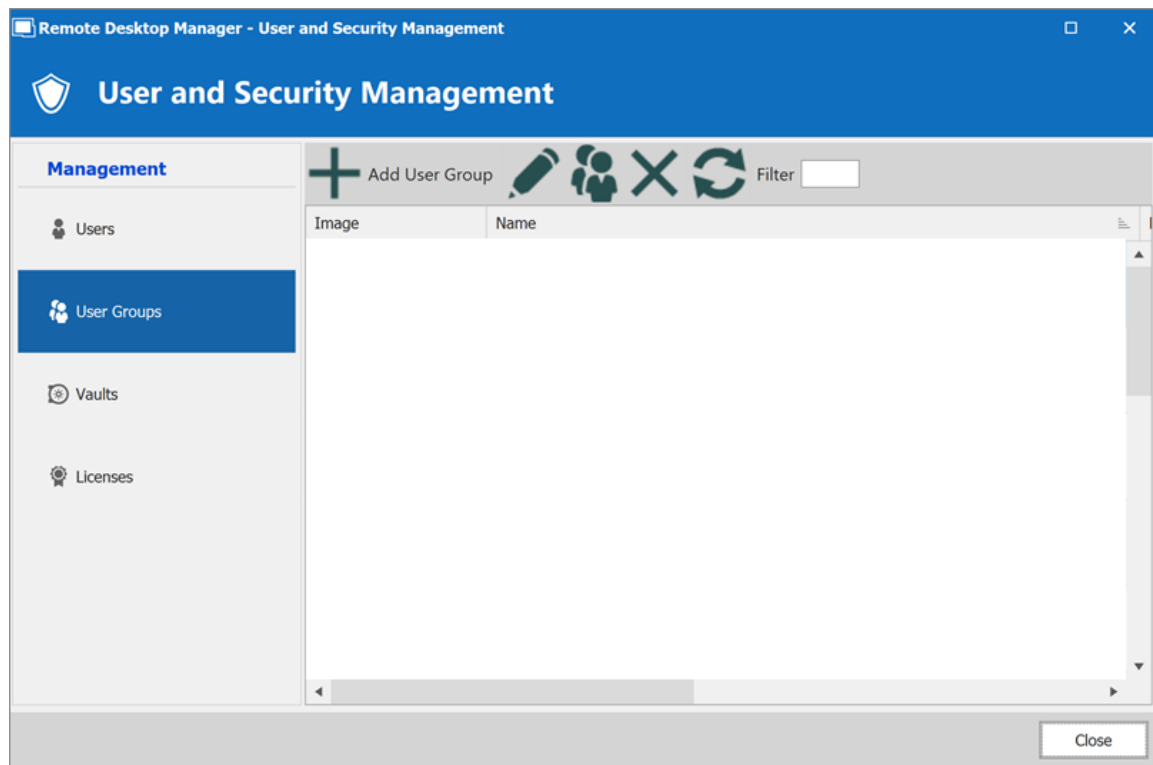
### Common user groups can be:

- 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.

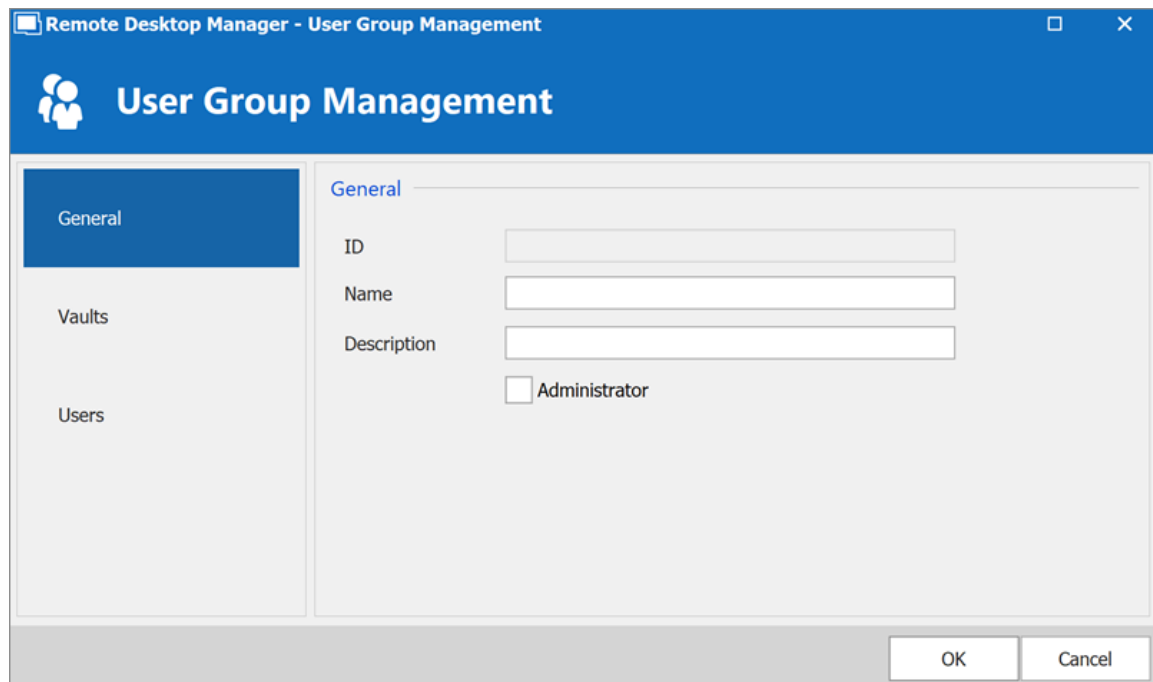
## CREATE THE USER GROUPS

To create user groups, navigate to **Administration – User Groups**, then click  **Add User Groups**.




*Create a User Group*

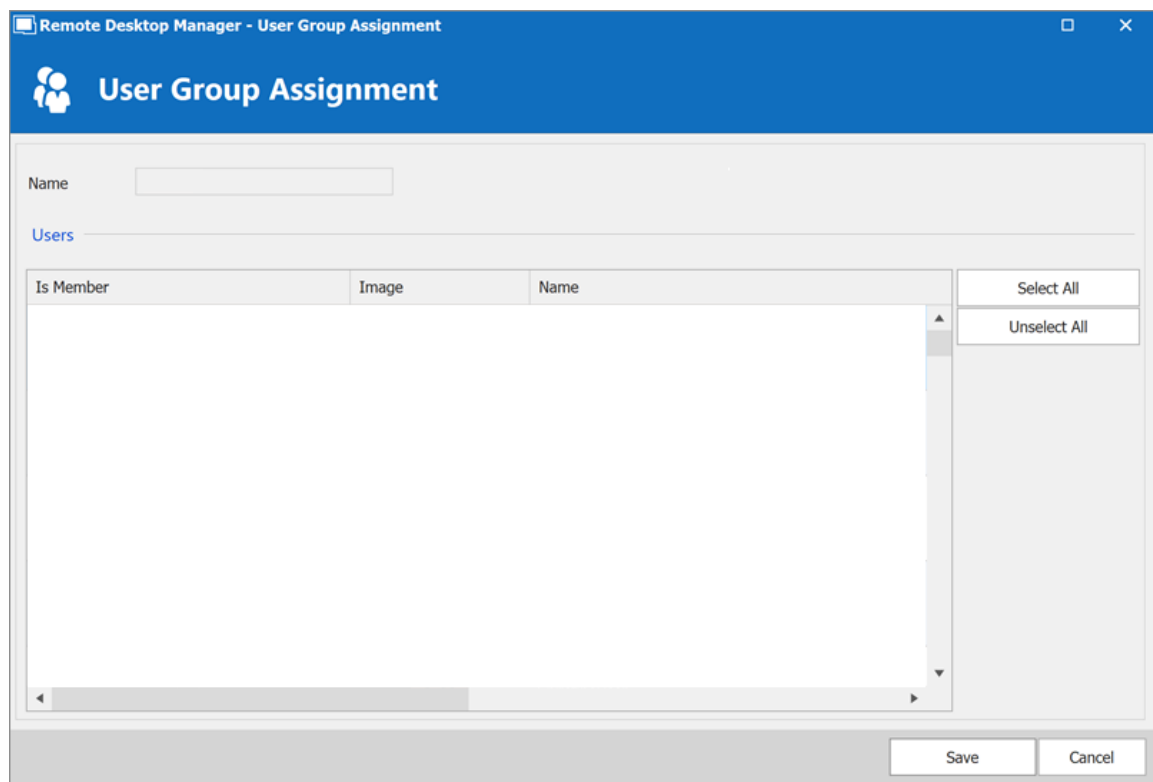
All settings can be left to default unless the user group contains only administrators. In this case, check the **Administrator** box when configuring the user group. Enter a **Name** for the user group, then click **Ok**.



The screenshot shows the 'Remote Desktop Manager - User Group Management' dialog box. The title bar is blue with the text 'Remote Desktop Manager - User Group Management' and standard window controls. Below the title bar is a blue header area with a user icon and the text 'User Group Management'. On the left is a sidebar with three items: 'General' (selected and highlighted in blue), 'Vaults', and 'Users'. The main area is titled 'General' and contains the following fields: 'ID' (text box), 'Name' (text box), 'Description' (text box), and an 'Administrator' checkbox. At the bottom right are 'OK' and 'Cancel' buttons.

*Configure a User Group*

To assign users to the user group, click , then check the **Is Member** box of the respective user.



The screenshot shows the 'Remote Desktop Manager - User Group Assignment' dialog box. The title bar is blue with the text 'Remote Desktop Manager - User Group Assignment' and standard window controls. Below the title bar is a blue header area with a user icon and the text 'User Group Assignment'. On the left is a sidebar with two items: 'Name' (text box) and 'Users' (selected and highlighted in blue). The main area is titled 'Users' and contains a table with three columns: 'Is Member', 'Image', and 'Name'. The table is currently empty. To the right of the table are two buttons: 'Select All' and 'Unselect All'. At the bottom right are 'Save' and 'Cancel' buttons.

*Assign a user to the User Groups*

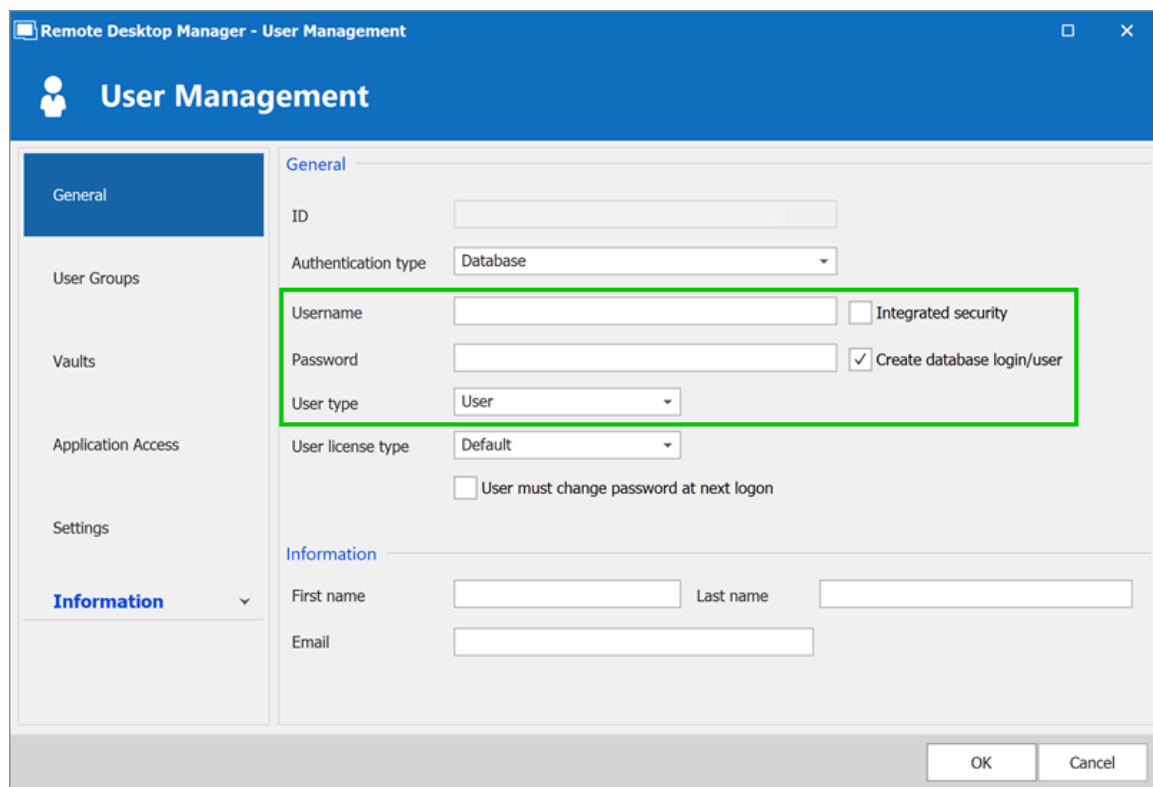
## USER CONFIGURATION

### 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

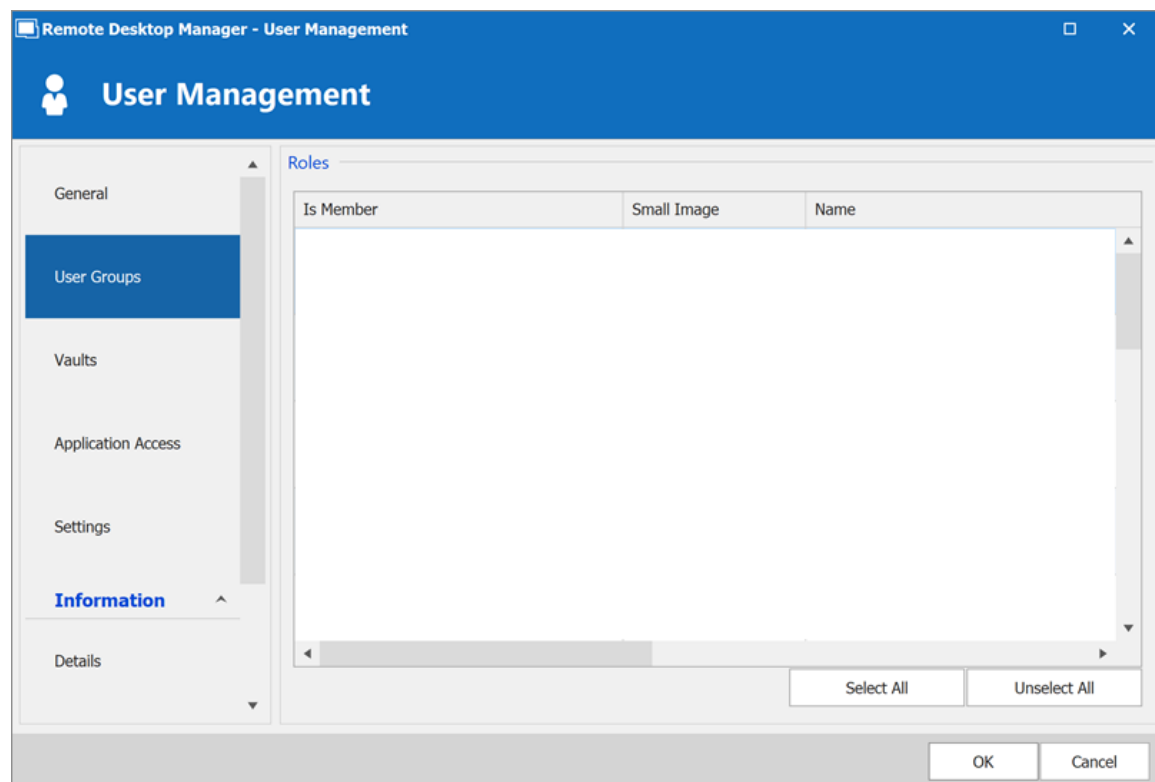
To create users, navigate to **Administration – Users**, then click **+ Add User**. Enter a **Login** and **Password** for the user and select the **User type**.



*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

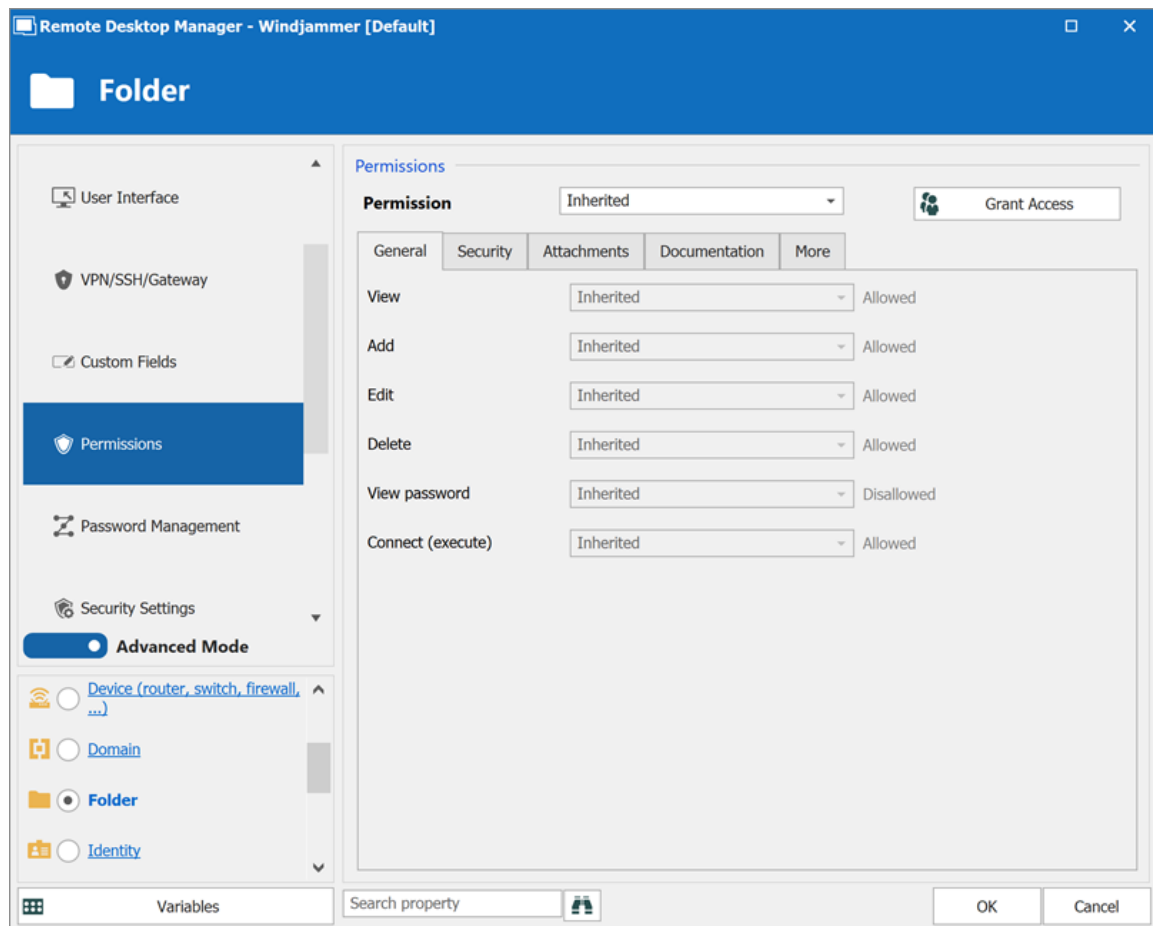
When creating users, some key points must be taken into consideration. Ask yourself the following questions while configuring a new user:

- 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 have very limited access.

## ENTRY CONFIGURATION

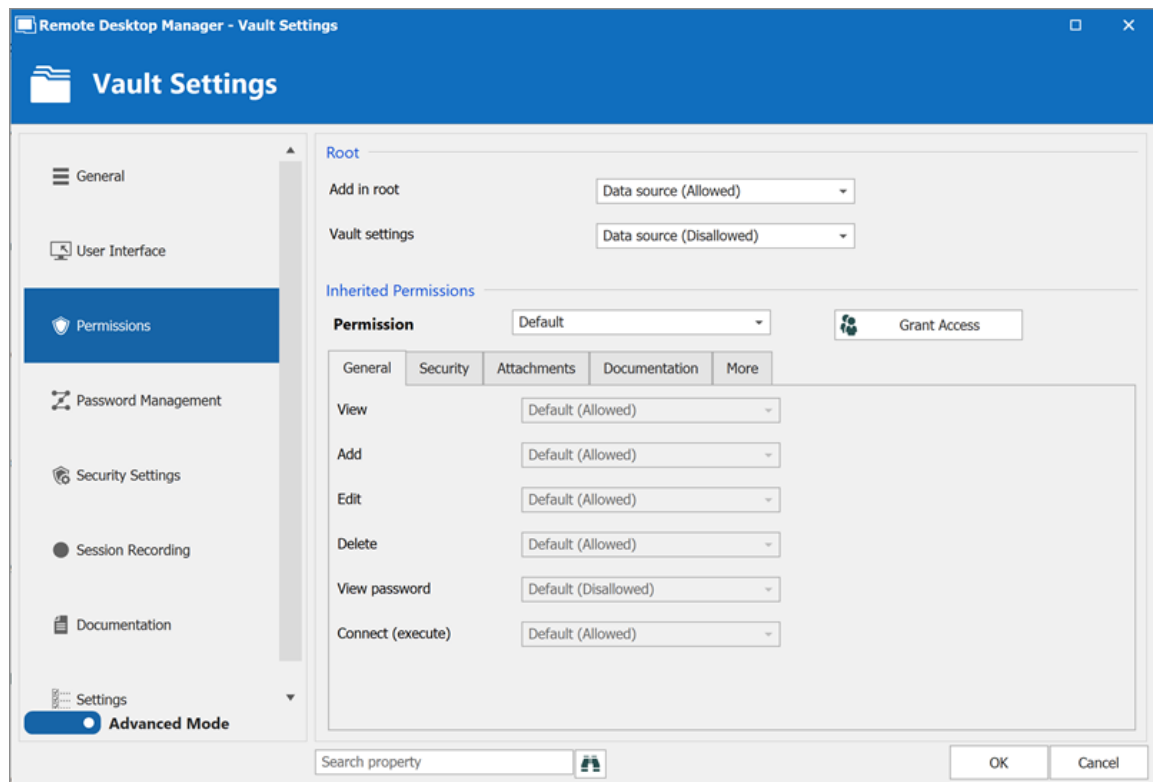
Access is granted or denied to users by setting permission on entries. Permissions can be set to users or user groups. The best practice is to grant permissions to user groups to control access for multiple users at once.

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.

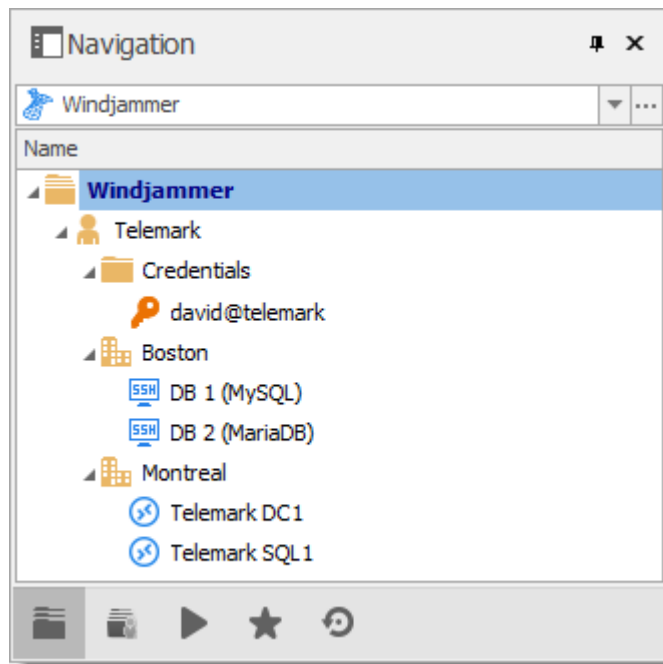


*Vault Settings Permissions*

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.

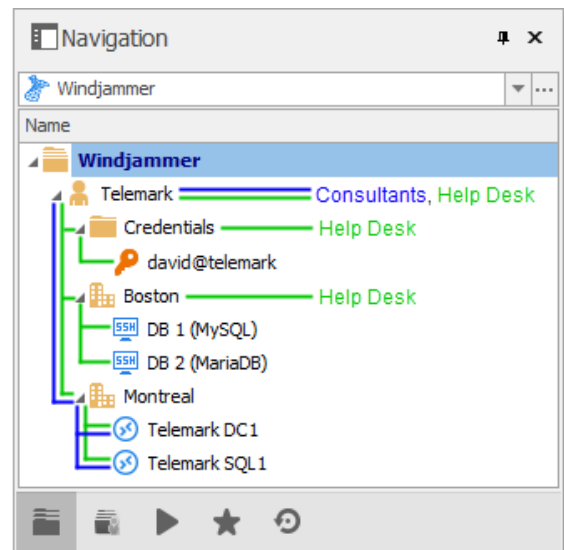
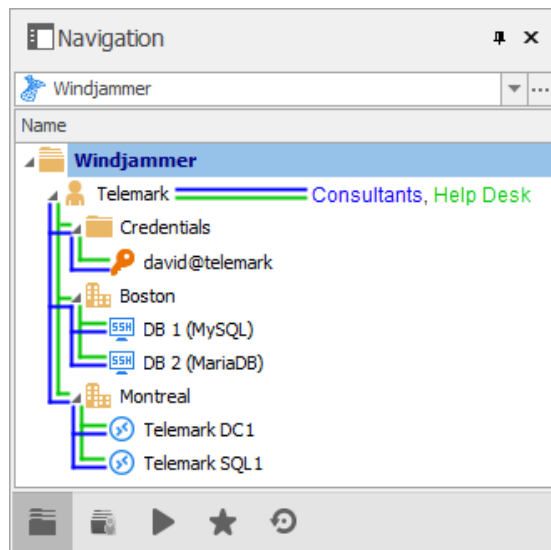
For a user to have access to a sub folder, the user must have at least the view permission on all parent folders.

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.



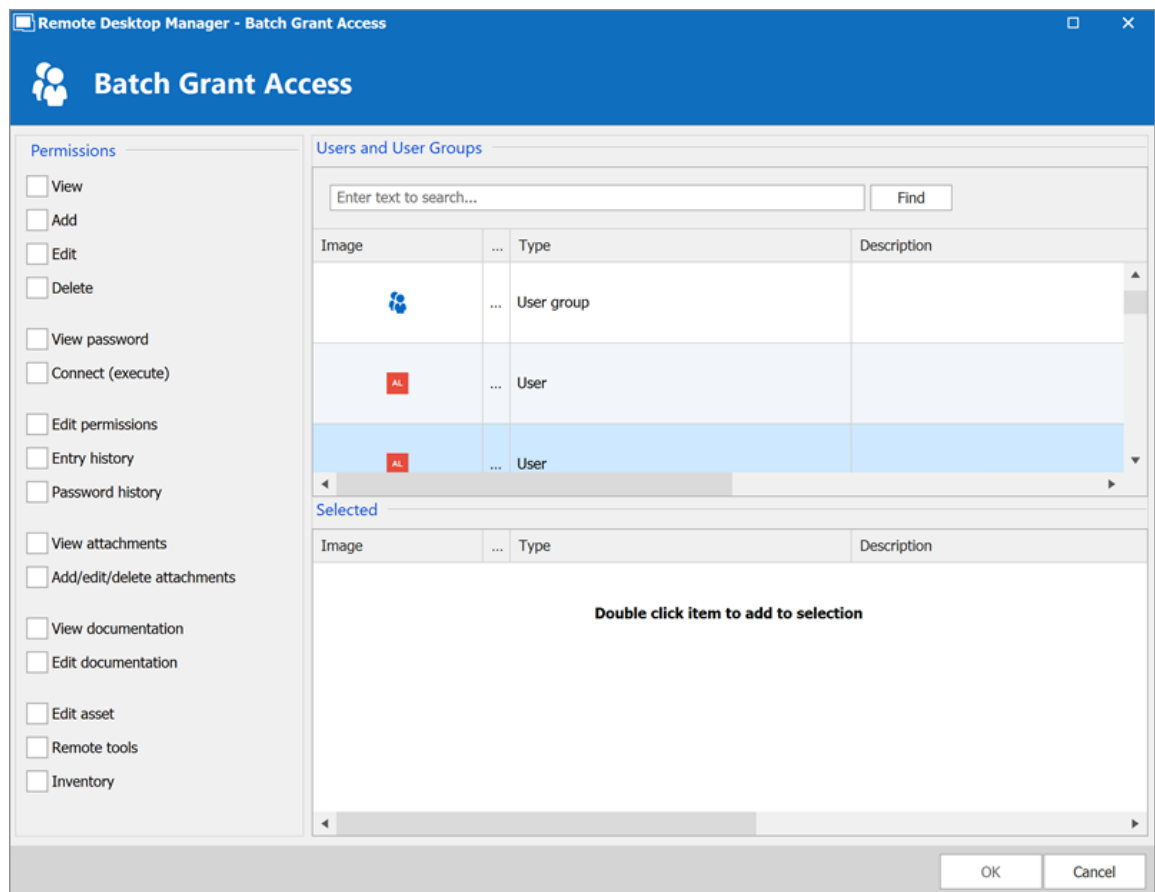
The [User Group Based Access Control](#) feature is not available using an [Devolutions Online Database](#).

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
<b>Permission</b>	<p>Sets the permission mode. Select between:</p> <ul style="list-style-type: none"> <li>• <b>Inherited (Default)</b>: will inherit the permissions from the parent groups.</li> <li>• <b>Custom</b>: lets you specify a custom value for each of the permission.</li> </ul>

OPTION	DESCRIPTION
	<ul style="list-style-type: none"> <li>• <b>Everyone:</b> everyone will be granted all the permissions below.</li> <li>• <b>Never:</b> no one but the administrators will be granted the permission.</li> </ul>
<b>Grant Access</b>	Allows batch granting access to a specific entry or entries.
<b>Inherited values</b>	Indicates what is inherited from parent groups.
<b>Select user groups or users</b>	Lets you select Users / User groups to be granted the permission. Available only if the permission is set to <b>Custom</b> .



Batch Grant Access

## 8.2 Scenarios

### 8.2.1 Simplified Security

#### DESCRIPTION



This feature is only available when using an [Advanced Data Source](#).



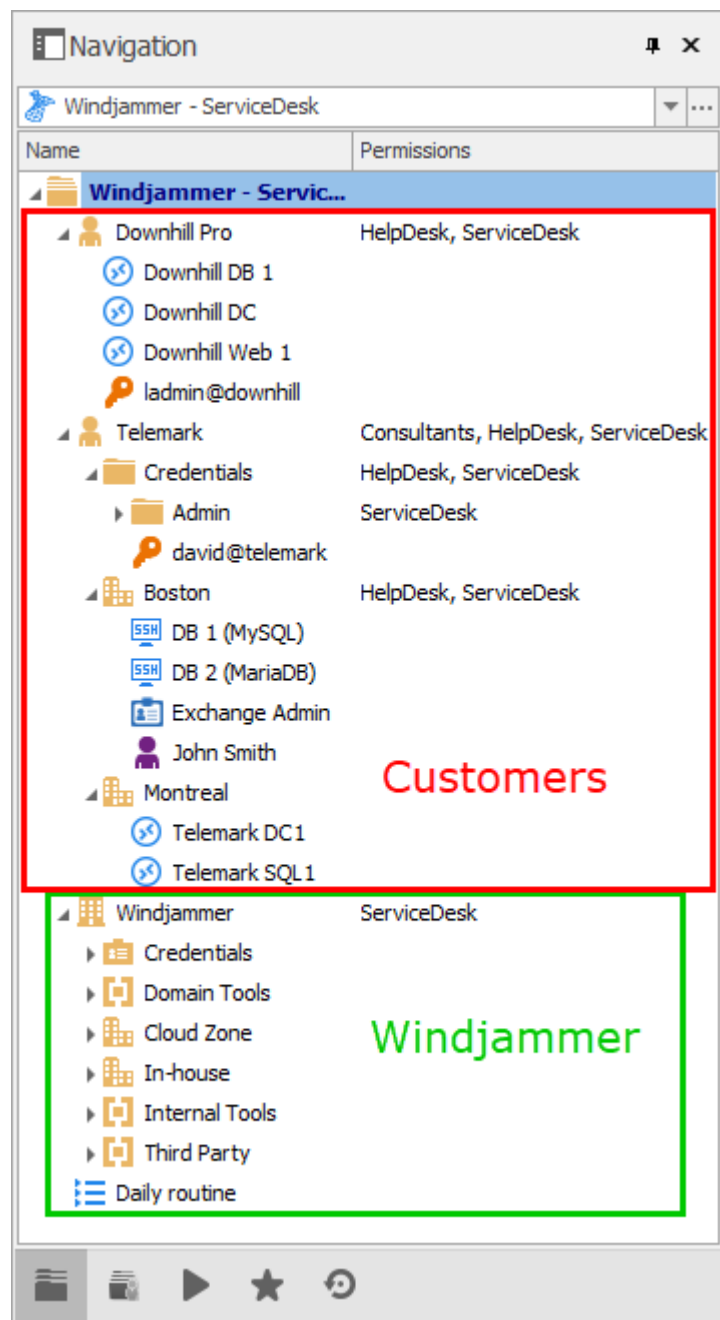
While the following scenario is relevant for small to medium enterprises, it is not recommended for a larger business. For a scenario more suited for large enterprises, please consult the [Advanced Security](#) scenario.



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

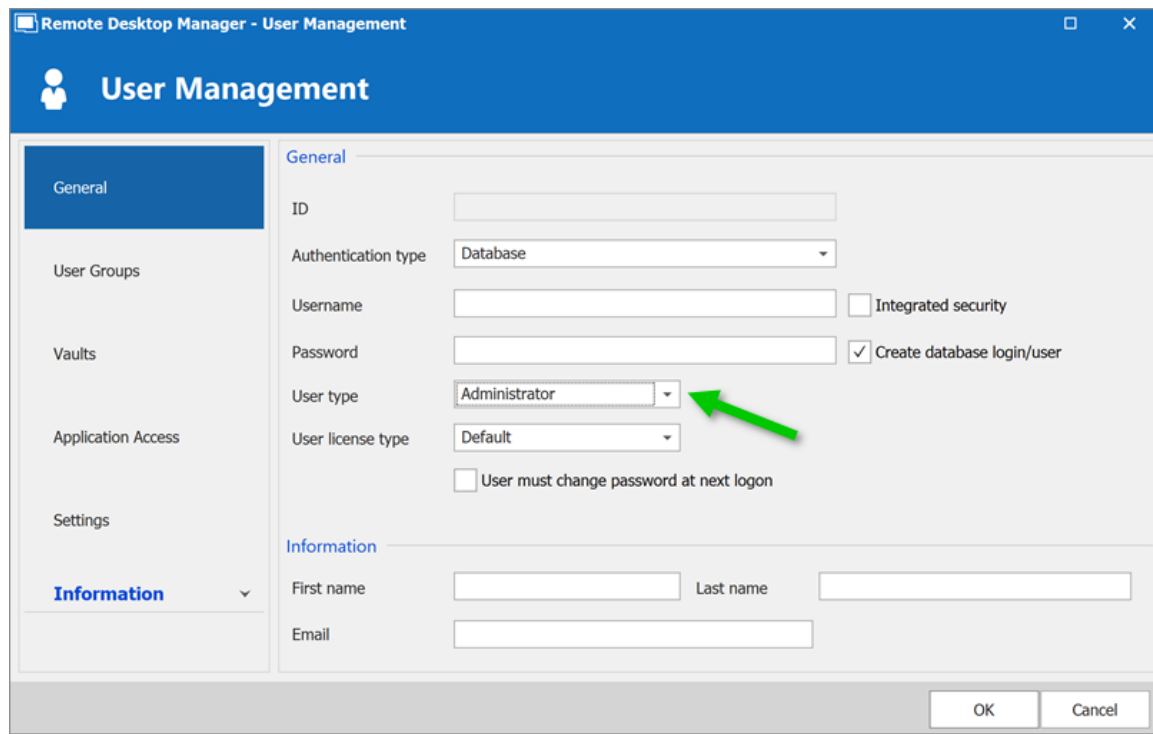
Here is an example for user configuration. To create users, navigate to **Administration – Users – Add User**.

The following rights selection is available when setting a user to **Restricted user**.

The screenshot shows the 'Remote Desktop Manager - User Management' window. The 'General' tab is selected in the left sidebar. The 'General' section contains fields for ID, Authentication type (set to 'Database'), Username, Password, User type (set to 'Restricted user'), and User license type (set to 'Default'). There are checkboxes for 'Integrated security' (unchecked) and 'Create database login/user' (checked). A checkbox for 'User must change password at next logon' is also present. The 'Rights' section, highlighted with a green box, contains checkboxes for 'Add', 'Edit', 'Delete', and 'Move', all of which are currently unchecked. The 'Information' section at the bottom has fields for First name, Last name, and Email. The window has 'OK' and 'Cancel' buttons at the bottom right.

*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.



Remote Desktop Manager - User Management

## User Management

**General**

User Groups

Vaults

Application Access

Settings

**Information**

ID

Authentication type: Database

Username

Password

User type: Administrator

User license type: Default

☐ Integrated security

☒ Create database login/user

☐ User must change password at next logon

**Information**

First name

Last name

Email

OK Cancel

*User Management - Administrator*

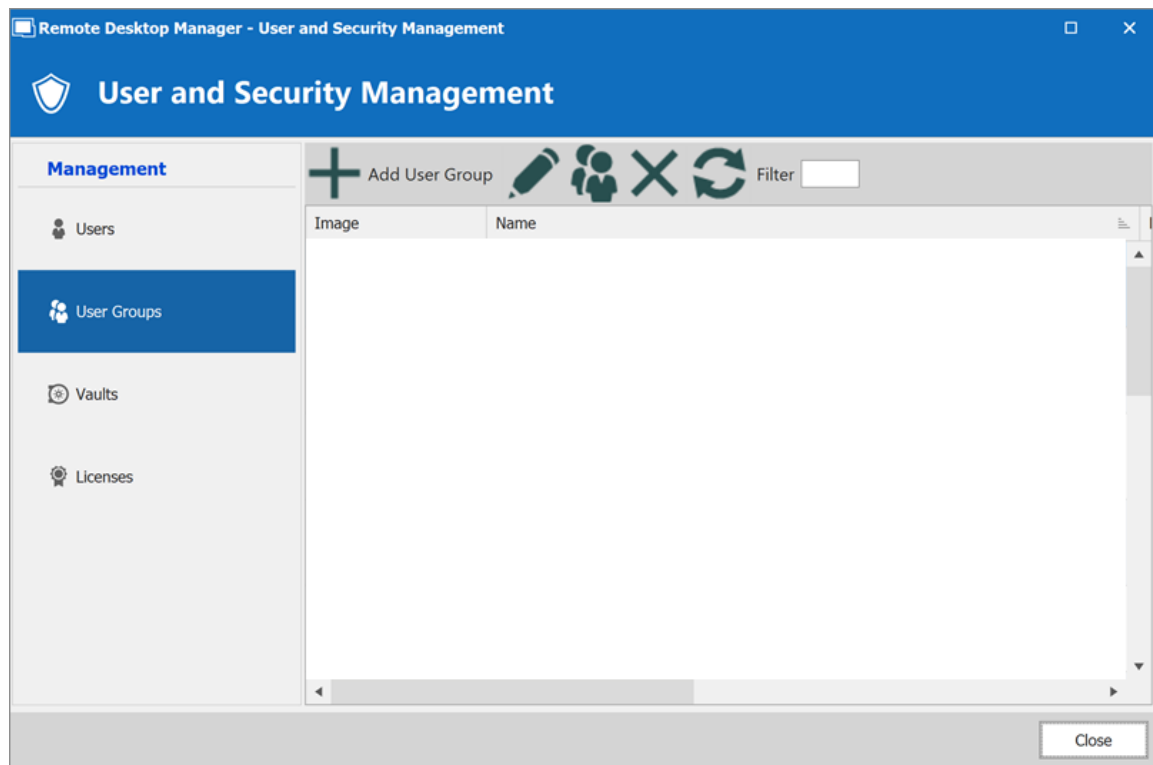
**Regular users (User):** these users have fewer rights than administrators. They essentially have all the basic rights (except for **View Password**) but are susceptible to all denied permissions. Later, we will deny these rights by specifying which users can actually perform these actions.

**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*

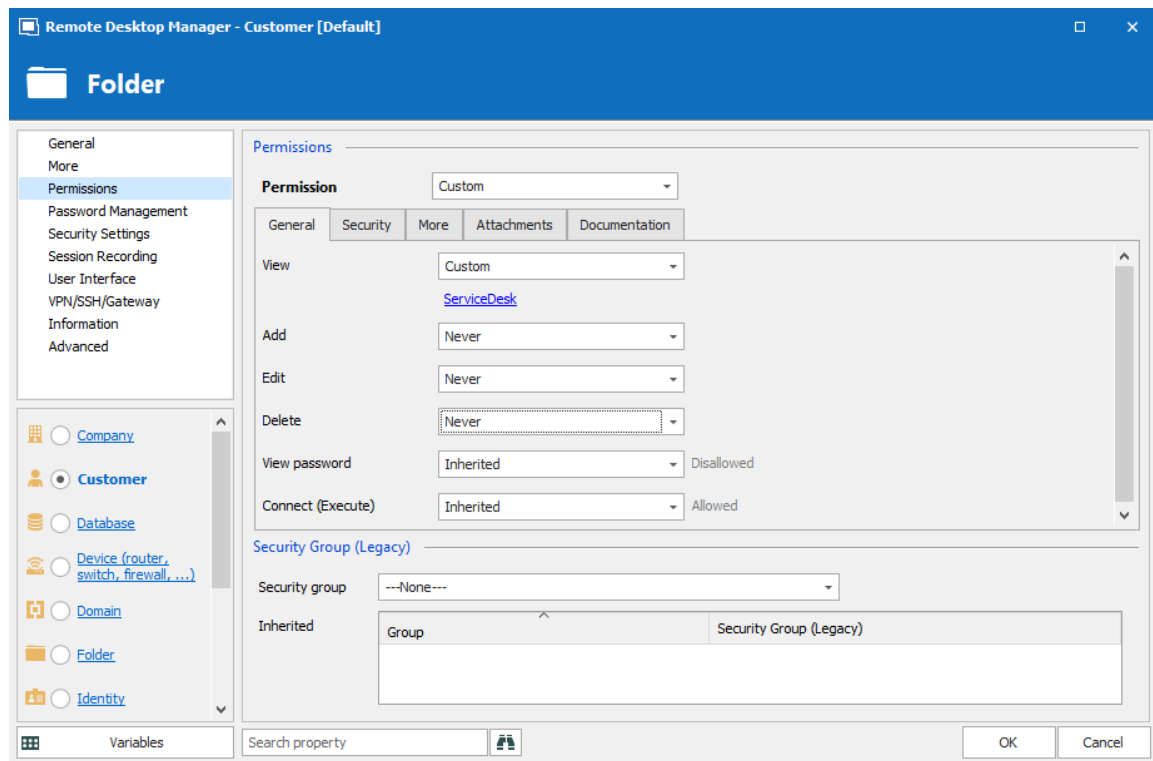
## ENTRIES CONFIGURATION

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.

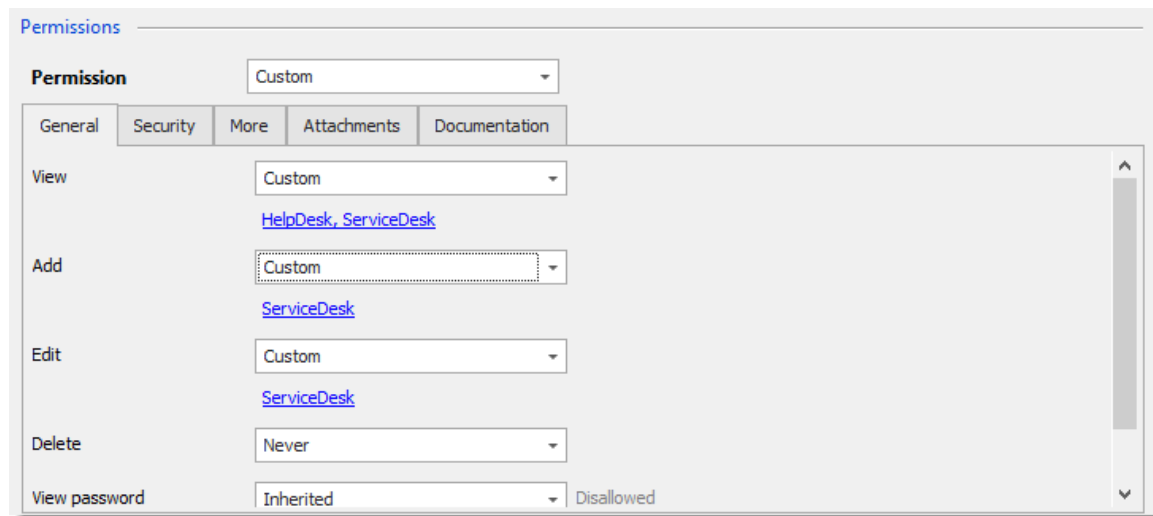
We will begin with the Vault level folders: Downhill Pro, Telemark and Windjammer.

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.

Permission		Custom
General	Security	More Attachments Documentation
View	Custom	HelpDesk, ServiceDesk
Add	Inherited	ServiceDesk
Edit	Inherited	ServiceDesk
Delete	Inherited	Never
View password	Inherited	Disallowed
Connect (Execute)	Inherited	Allowed

*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**.

Permission		Custom
General	Security	More Attachments Documentation
View	Custom	HelpDesk, ServiceDesk
Add	Inherited	ServiceDesk
Edit	Inherited	ServiceDesk
Delete	Never	
View password	Inherited	Disallowed
Connect (Execute)	Inherited	Allowed

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.



Permission		Custom
General	Security	More Attachments Documentation
View	Custom	<a href="#">HelpDesk, ServiceDesk</a>
Add	Inherited	ServiceDesk
Edit	Inherited	ServiceDesk
Delete	Never	
View password	Inherited	Disallowed
Connect (Execute)	Inherited	Allowed

*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.

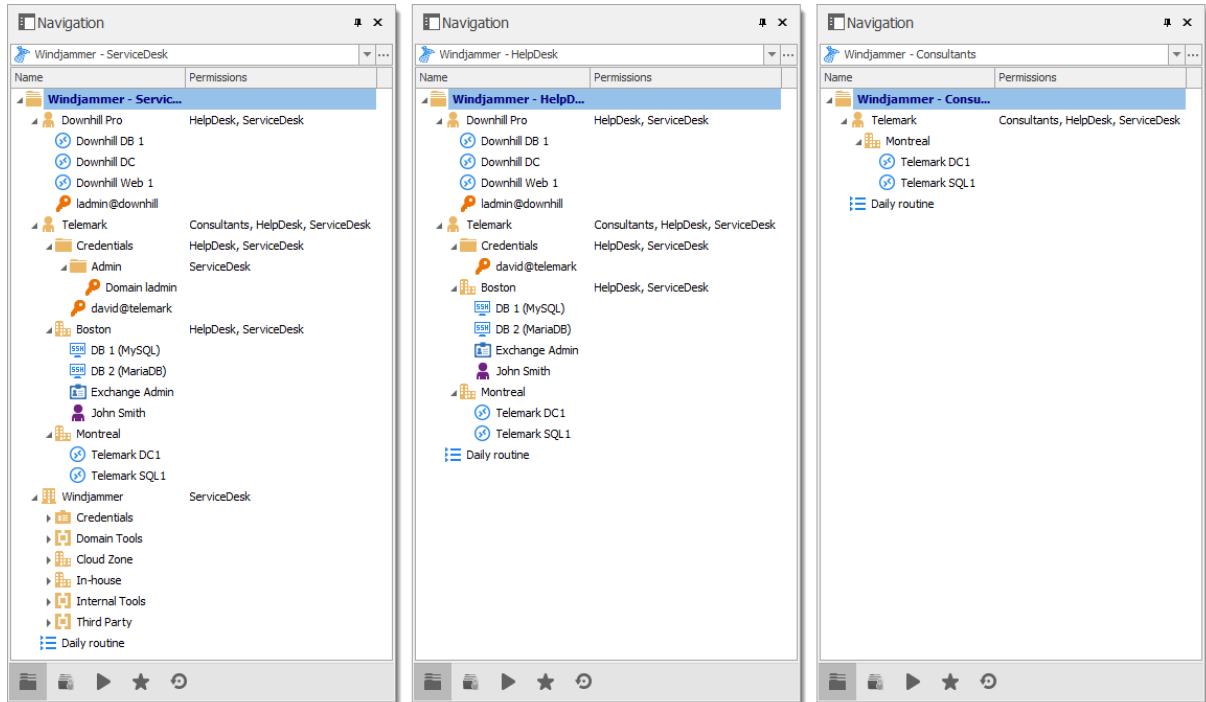
Permission		Default
General	Security	More Attachments Documentation
View	Inherited	Consultants, HelpDesk, ServiceDesk
Add	Inherited	ServiceDesk
Edit	Inherited	ServiceDesk
Delete	Inherited	Never
View password	Inherited	Disallowed
Connect (Execute)	Inherited	Allowed

*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](#).

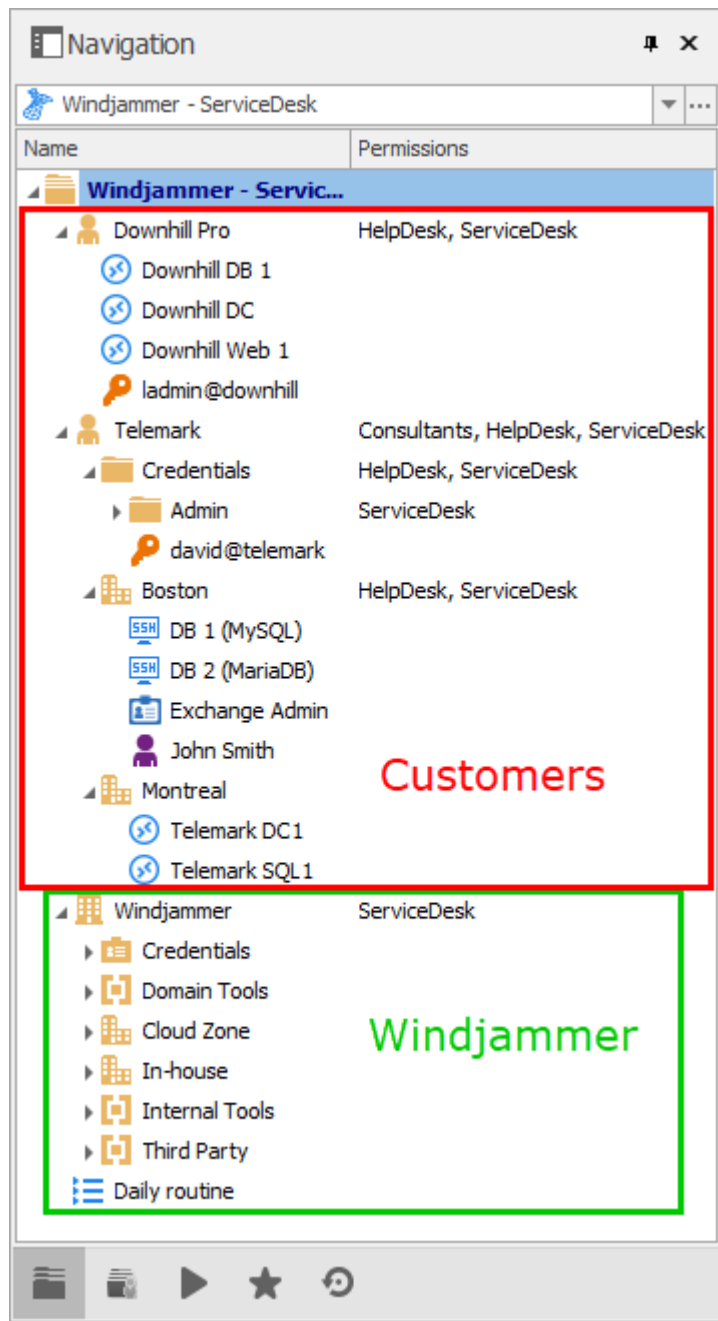


The following scenario is designed for large enterprises. For a scenario more suited for small enterprises, please consult our [Simplified Security](#) scenario.

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.

Remote Desktop Manager - User Management

**User Management**

General

ID:

Authentication type: Database

Username:  ☐ Integrated security

Password:  ☒ Create database login/user

User type: Restricted user

User license type: Default

☐ User must change password at next logon

**Rights**

☒ Add

☒ Edit

☐ Delete

☐ Move

**Information**

First name:  Last name:

Email:

OK Cancel

*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.

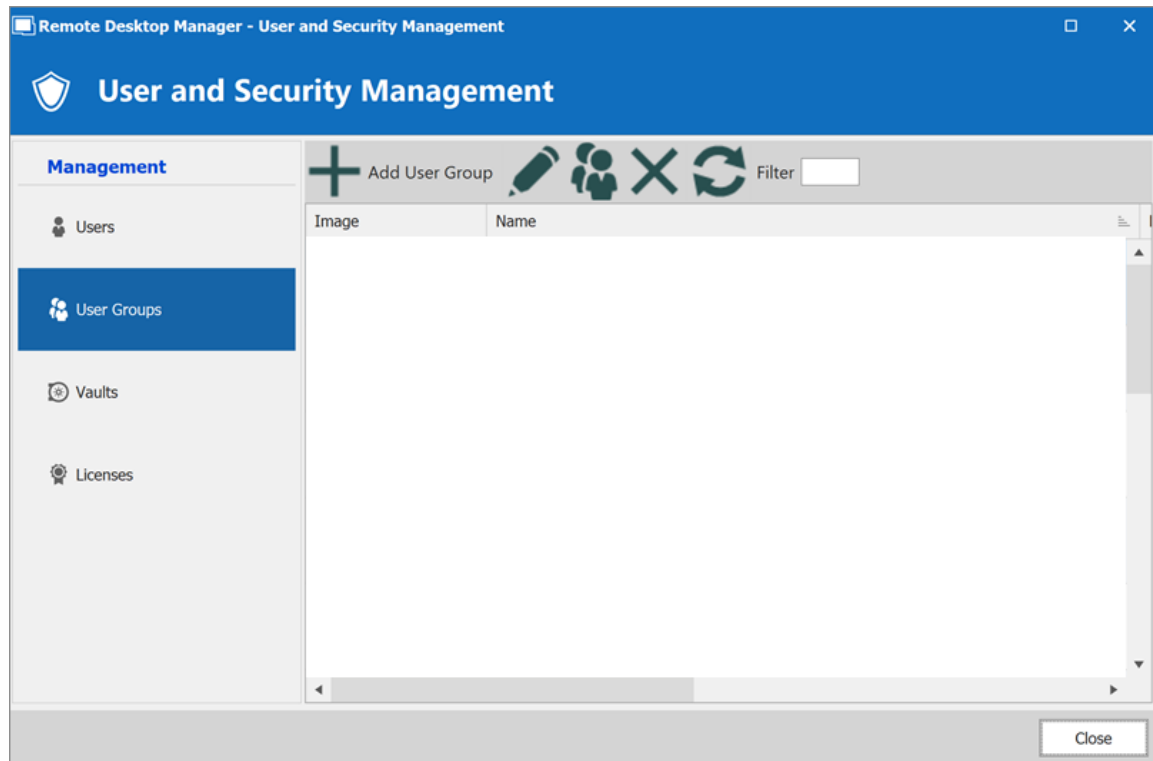
## USER GROUPS CONFIGURATION

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*

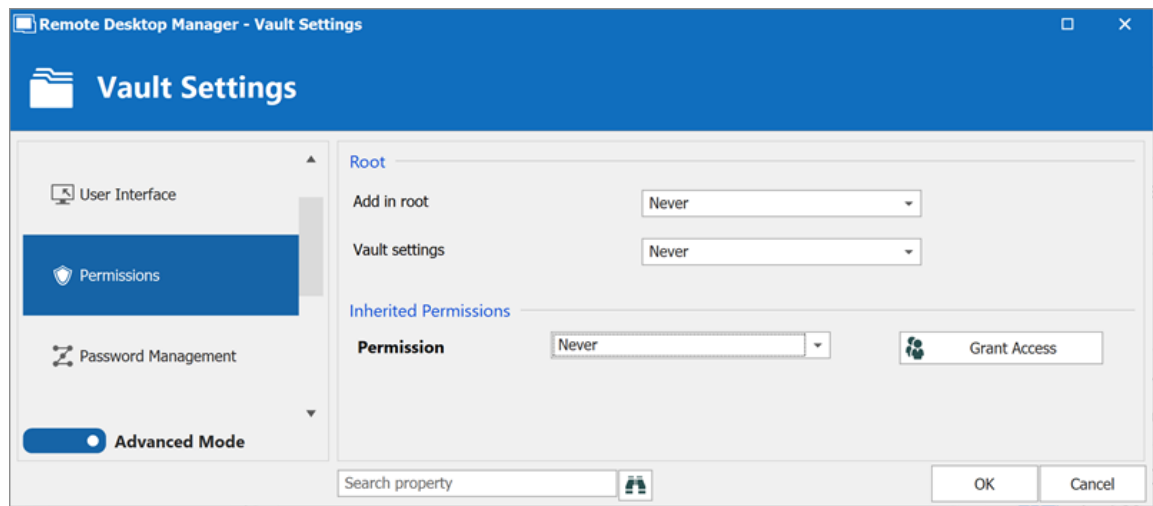
## ENTRY CONFIGURATION

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

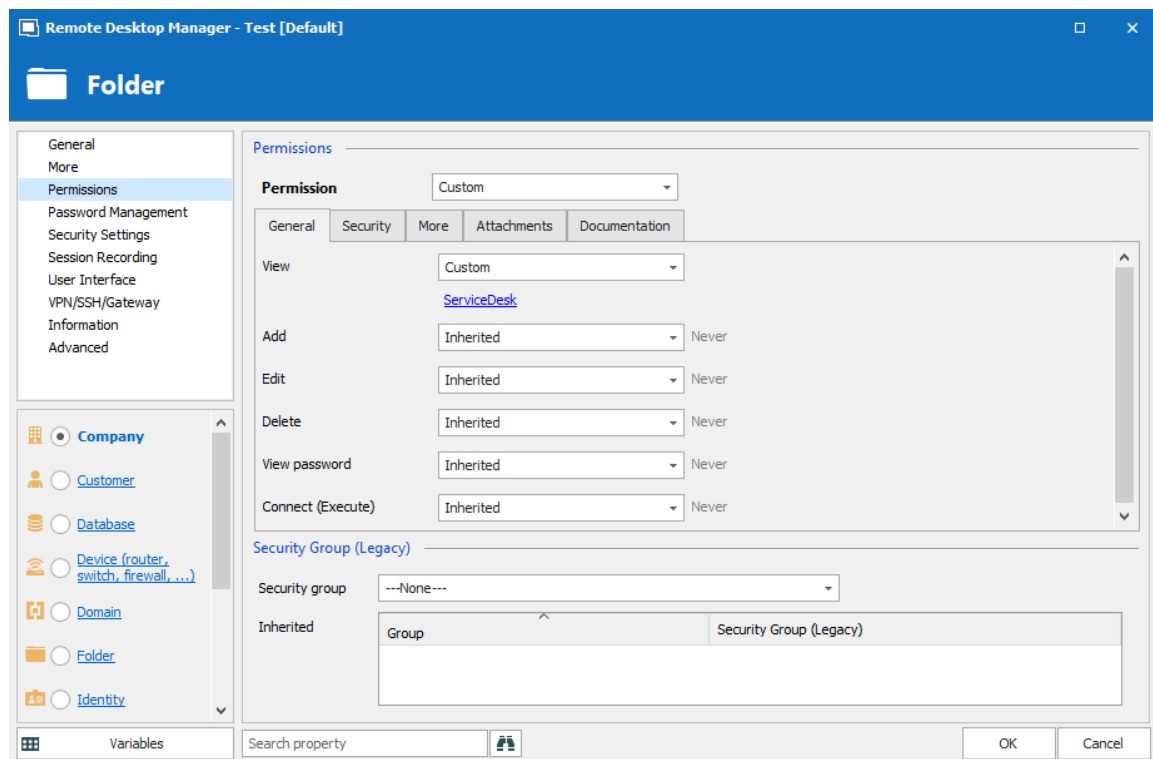
As mentioned above, **ALL** Vault settings folder permissions are set to **Never**. This denies the default access to other users.



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.

Permission	
General	Custom
Security	
More	
Attachments	
Documentation	
View	Custom <a href="#">HelpDesk, ServiceDesk</a>
Add	Custom <a href="#">ServiceDesk</a>
Edit	Custom <a href="#">ServiceDesk</a>
Delete	Inherited Never
View password	Inherited Never

*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.

Permission	Custom
View	Custom <a href="#">Consultants, HelpDesk, ServiceDesk</a>
Add	Custom <a href="#">ServiceDesk</a>
Edit	Custom <a href="#">ServiceDesk</a>
Delete	Inherited Never
View password	Inherited Never

*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.

Permission		Custom
General	Security	More
View	Custom	HelpDesk, ServiceDesk
Add	Never	
Edit	Never	
Delete	Inherited	Never
View password	Inherited	Never
Connect (Execute)	Inherited	Never

*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 admin** 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.

Permission		Custom
General	Security	More
View	Custom	ServiceDesk
Add	Inherited	Never
Edit	Inherited	Never
Delete	Inherited	Never
View password	Inherited	Never
Connect (Execute)	Inherited	Never

*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.

Permission	Value	Source
View	Custom	HelpDesk, ServiceDesk
Add	Inherited	ServiceDesk
Edit	Inherited	ServiceDesk
Delete	Inherited	Never
View password	Inherited	Never
Connect (Execute)	Inherited	Never

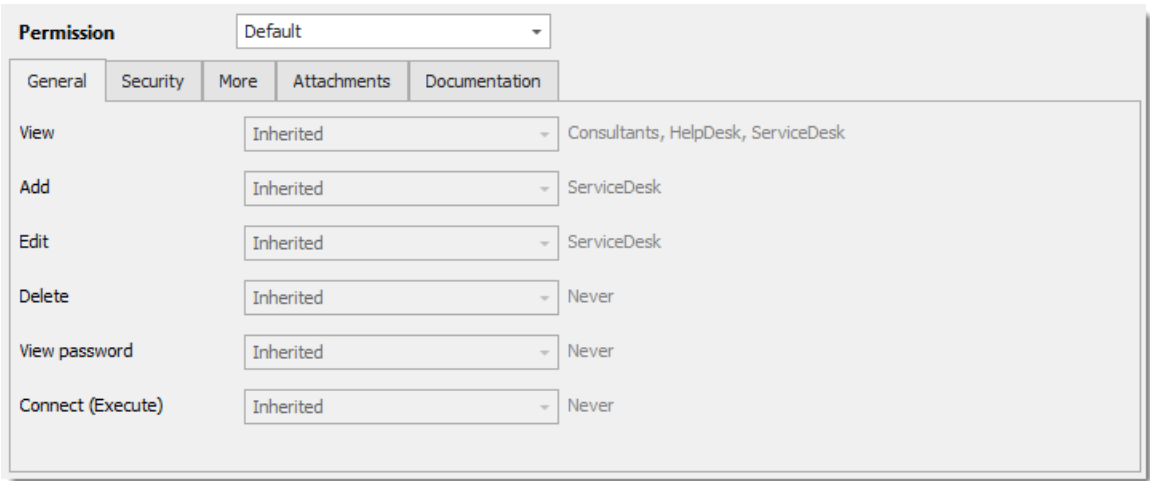
*Telemark\Boston - Permissions*

- **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.

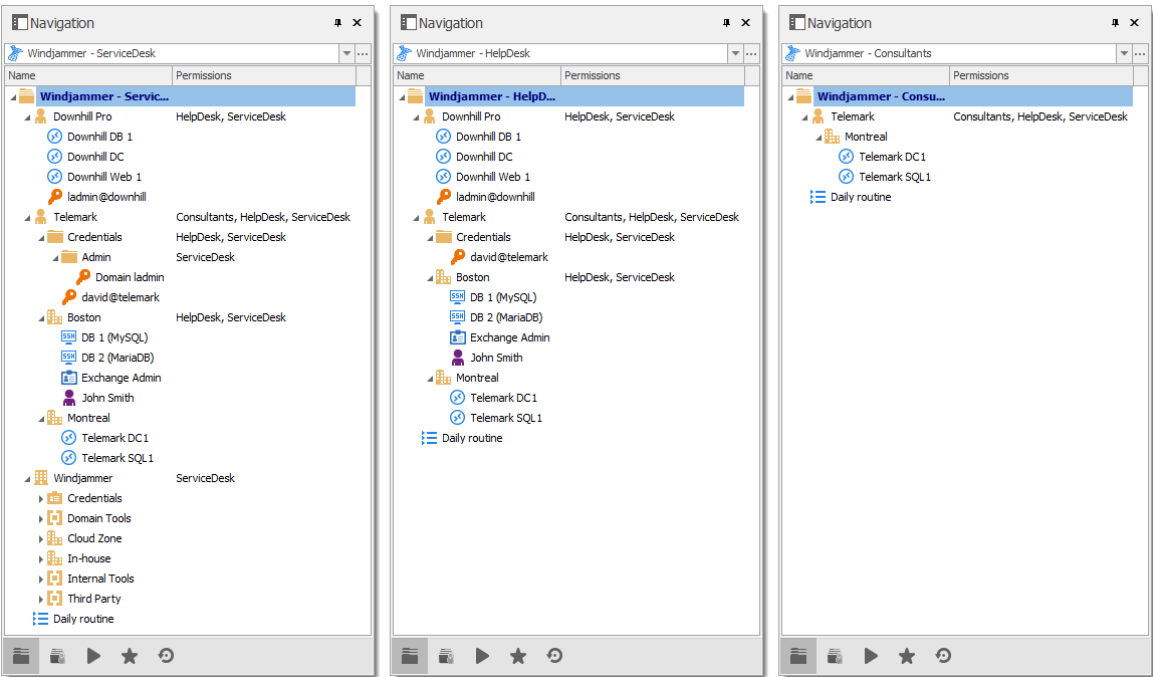
There is no need to set any permissions on the Montreal folder, since they all inherit values from parent folders.



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.

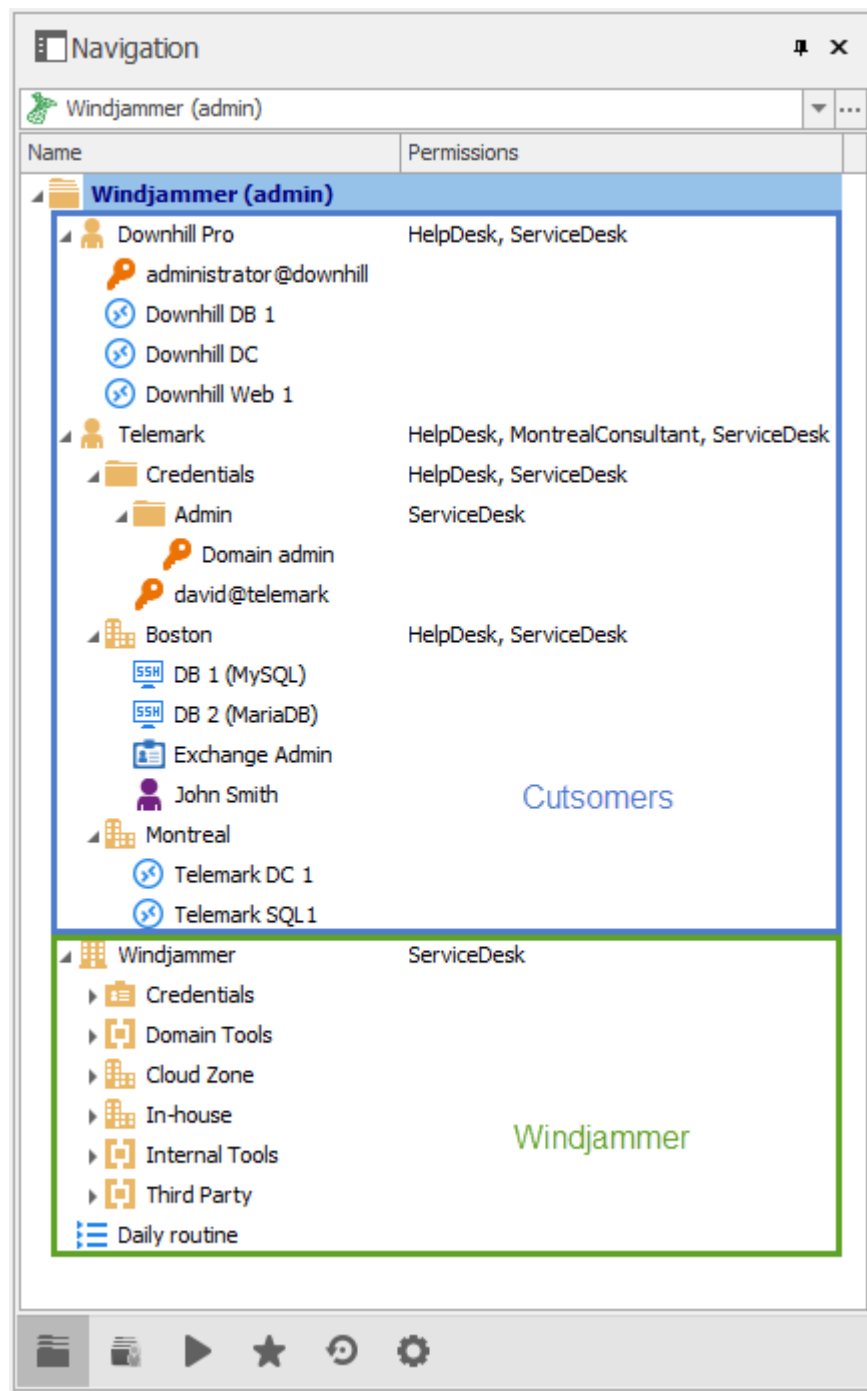


This feature is only available when using an [Advanced Data Source](#).

### 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.

Remote Desktop Manager - User Management

### User Management

**General**

ID: 9914D1D1-7E4E-47EF-93AA-3F47DB6D9654

Authentication type: Database

Username:

Password:

User type: **Administrator**

User license type: ☐ Integrated security

☒ Create database login/user

at next logon

**Information**

First name:  Last name:

Email:

OK Cancel

*Administrator Permission*

The *ServiceDesk*:

- **Add**
- **Edit**
- **Deny add entry in root folder**



The screenshot shows a configuration window with a left sidebar and a main content area. The sidebar contains a tree view with 'General' at the top, followed by 'Information' (expanded), 'Details', 'Address', 'Phone', 'Roles', 'Privileges', 'Permissions' (highlighted in blue), and 'Settings'. The main content area has a blue header labeled 'Rights'. Below the header, there are four checkboxes: 'Add' (checked), 'Edit' (checked), 'Delete' (unchecked), and 'Deny add entry in root folder' (checked). A green rectangular box highlights the 'Add', 'Edit', and 'Deny add entry in root folder' options.

*ServiceDesk Rights*

The *HelpDesk*:

- **Add**
- **Deny add entry in root folder**

This screenshot is identical to the one above, showing the 'ServiceDesk Rights' configuration. The 'Add', 'Edit', and 'Deny add entry in root folder' options are checked and highlighted with a green box.

*HelpDesk Rights*

The *MontrealConsultant* has read-only access. He cannot see any password or entry detail.

- Leave everything disable for this user

The screenshot shows the 'Rights' configuration for the 'MontrealConsultant' user. The sidebar is the same as in previous screenshots, with 'Permissions' highlighted. The main content area has a blue header labeled 'Rights'. Below the header, there are three checkboxes: 'Add' (unchecked), 'Edit' (unchecked), and 'Delete' (unchecked). A green rectangular box highlights these three unchecked options.

*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

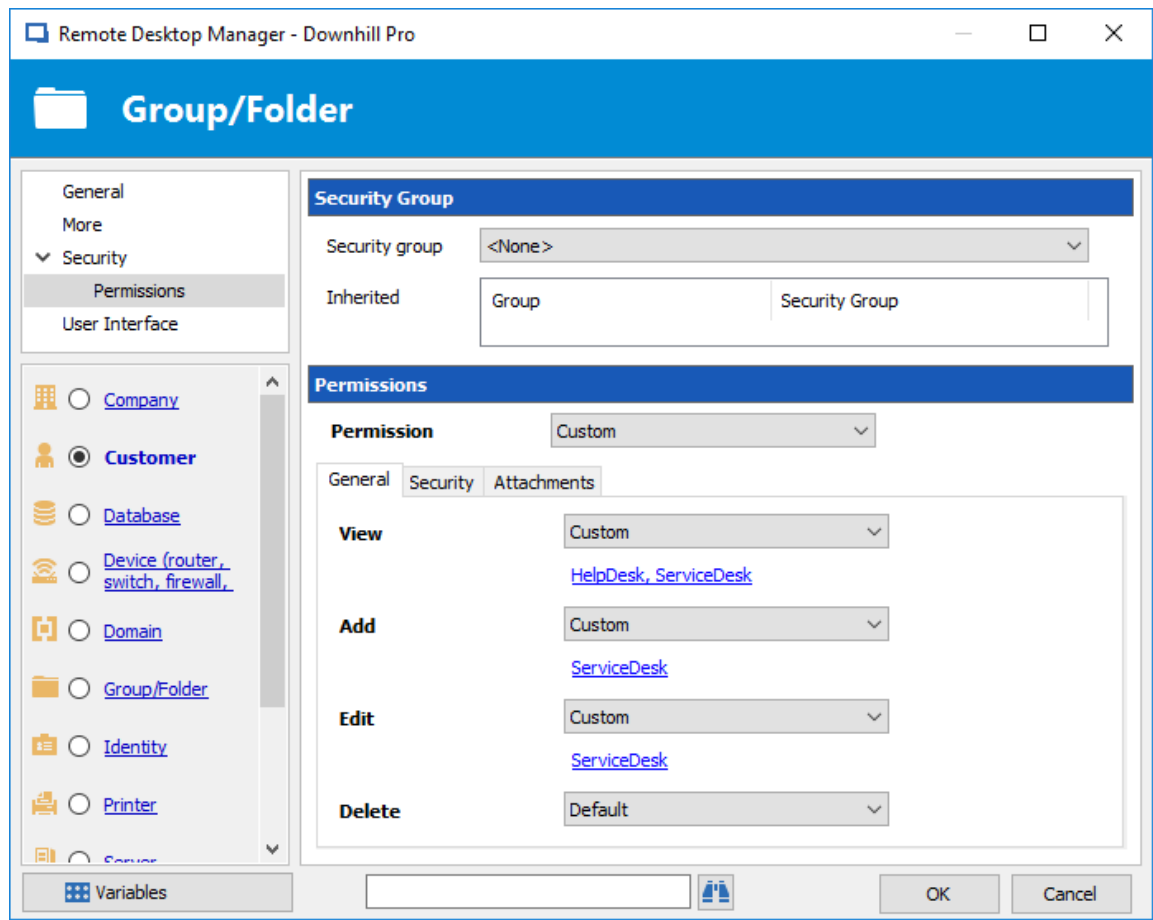
## ENTRIES CONFIGURATION

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 group/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.

Permissions	
Permission	Custom
General Security Attachments	
View	Custom <a href="#">HelpDesk, MontrealConsultant, ServiceDesk</a>
Add	Custom <a href="#">ServiceDesk</a>
Edit	Custom <a href="#">ServiceDesk</a>
Delete	Default

*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.

Permissions	
Permission	Custom
General Security Attachments	
View	Custom <a href="#">HelpDesk, ServiceDesk</a>
Add	Default <a href="#">ServiceDesk</a>
Edit	Default <a href="#">ServiceDesk</a>
Delete	Default

*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.

The screenshot shows a 'Permissions' dialog box with a blue header. Below the header, there's a 'Permission' dropdown menu set to 'Custom'. Underneath, there are three tabs: 'General', 'Security', and 'Attachments'. The 'General' tab is active. It contains four rows of permissions: 'View', 'Add', 'Edit', and 'Delete'. Each row has a dropdown menu. For 'View', the dropdown is 'Custom' and 'ServiceDesk' is listed below it. For 'Add', the dropdown is 'Default' and 'ServiceDesk' is listed to the right. For 'Edit', the dropdown is 'Custom' and 'Admin' is listed below it. For 'Delete', the dropdown is 'Default'.

*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.

Permissions	
Permission	Custom
General Security Attachments	
View	Custom <a href="#">HelpDesk, ServiceDesk</a>
Add	Default <a href="#">ServiceDesk</a>
Edit	Default <a href="#">ServiceDesk</a>
Delete	Default

*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.

Permissions	
Permission	Default
General Security Attachments	
View	Default <a href="#">HelpDesk, MontrealConsultant, ServiceDesk</a>
Add	Default <a href="#">ServiceDesk</a>
Edit	Default <a href="#">ServiceDesk</a>
Delete	Default

*Telemark\Montreal - Permissions*

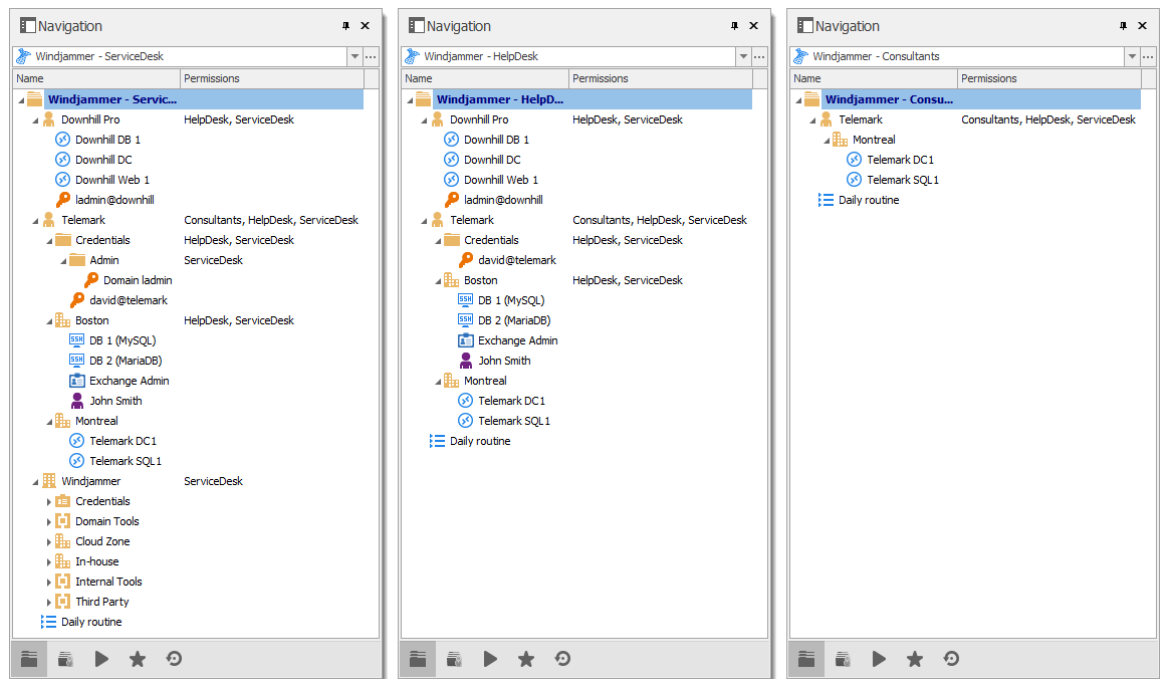
Finally, the permission to view the Windjammer folder will be set for the ServiceDesk only since we want them to be able to use its child entries. We don't want them to add or edit anything so we will set the **Add** and **Edit** permissions to the Administrator user/user group.

Permissions	
Permission	Custom
General Security Attachments	
View	Custom <a href="#">ServiceDesk</a>
Add	Custom <a href="#">Admin</a>
Edit	Custom <a href="#">Admin</a>
Delete	Default

*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:

<a href="#">Module</a>	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.
<a href="#">Custom Actions</a>	<p>Snippets of PowerShell code that can be executed directly in Remote Desktop Manager. The actions can be initiated using <b>Edit – Edit (Special Actions)</b>, <b>Custom PowerShell Command</b>. The advantages of this approach are:</p> <ol style="list-style-type: none"> <li>1. No need to handle loading of the appropriate module for the instance of Remote Desktop Manager.</li> <li>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.</li> </ol>

### 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
<b>My personal credentials</b>	"9F3C3BCF-068A-4927-B996-CA52154CAE3B"
<b>None</b>	"B87B29D9-9239-4D7B-86D8-9B53DCD3BA9F"
<b>User Vault, paired with <i>PersonalConnectionID</i></b>	"245A4245-48E7-4DF5-9C4C-11861D8E1F81"
<b>User Vault Search, paired with <i>CredentialPrivateVaultsearchString</i></b>	"88E4BE76-4C5B-4694-AA9C-D53B7E0FE0DC"

## TIPS AND TRICKS

- Use the Set-RDMPProperty cmdlet to set almost any value within the session object. 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.
- 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

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 IMPORT THE POWERSHELL MODULE

The Remote Desktop Manager PowerShell Module, which is called RemoteDesktopManager.PowerShellModule.dll, is located in the Remote Desktop Manager installation directory. The following path is for a default install of Remote Desktop Manager, adapt as per your requirements.

```
Import-Module "${env:ProgramFiles(x86)}\Devolutions\Remote Desktop Manager\RemoteDesk
```

## COMMANDS

To list all cmdlet commands, please enter this command:

```
Get-Command -Module RemoteDesktopManager.PowerShellModule
```

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.PowerShellModule -Type Cmdlet `
| Sort-Object -Property Name `
| Format-Table -Property Name `
| out-file $env:temp\pshelp.txt

Get-Command -Module RemoteDesktopManager.PowerShellModule `
| 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)" -PassThru
  };
## 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.Length)
        $groupName = $groupName.TrimStart("\")
    }

    # Create the group folder if it is not null, empty or fill in with space character
    if (![string]::IsNullOrEmpty($groupName)) {
        $session = New-RDMSession -Type "Group" -Name $groupName
        $session.Group = $csvEntry.Name
        Set-RDMSession $session
        Write-Host "Group Folder $groupName created" -f Yellow
    }
}

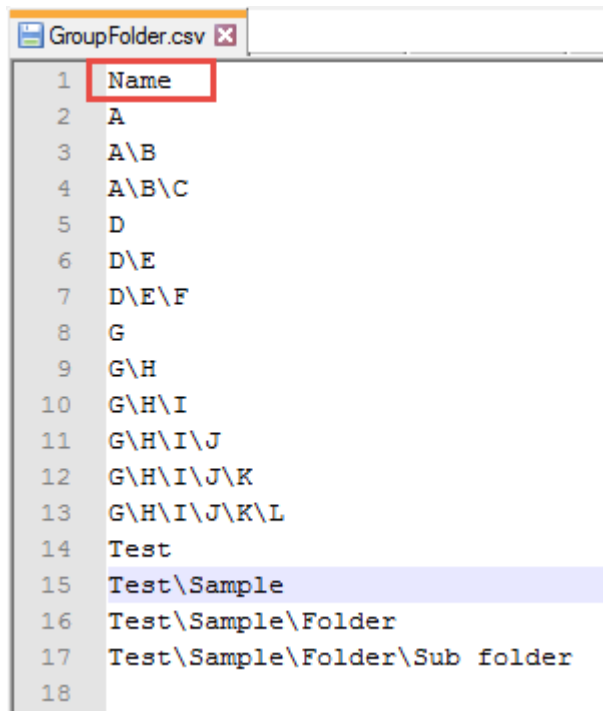
Update-RDMUI
```

## 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 :



CSV File example

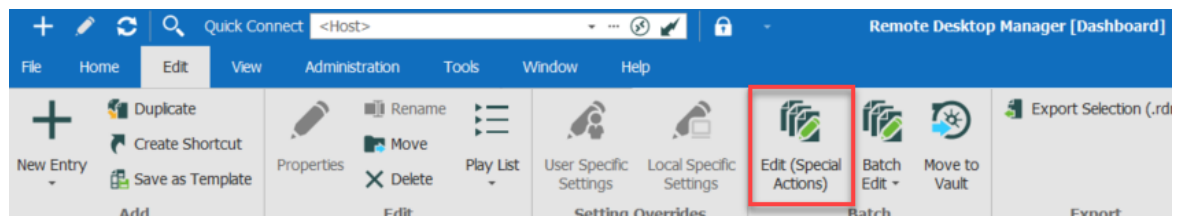
## CMDLETS REFERENCE

### 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 :

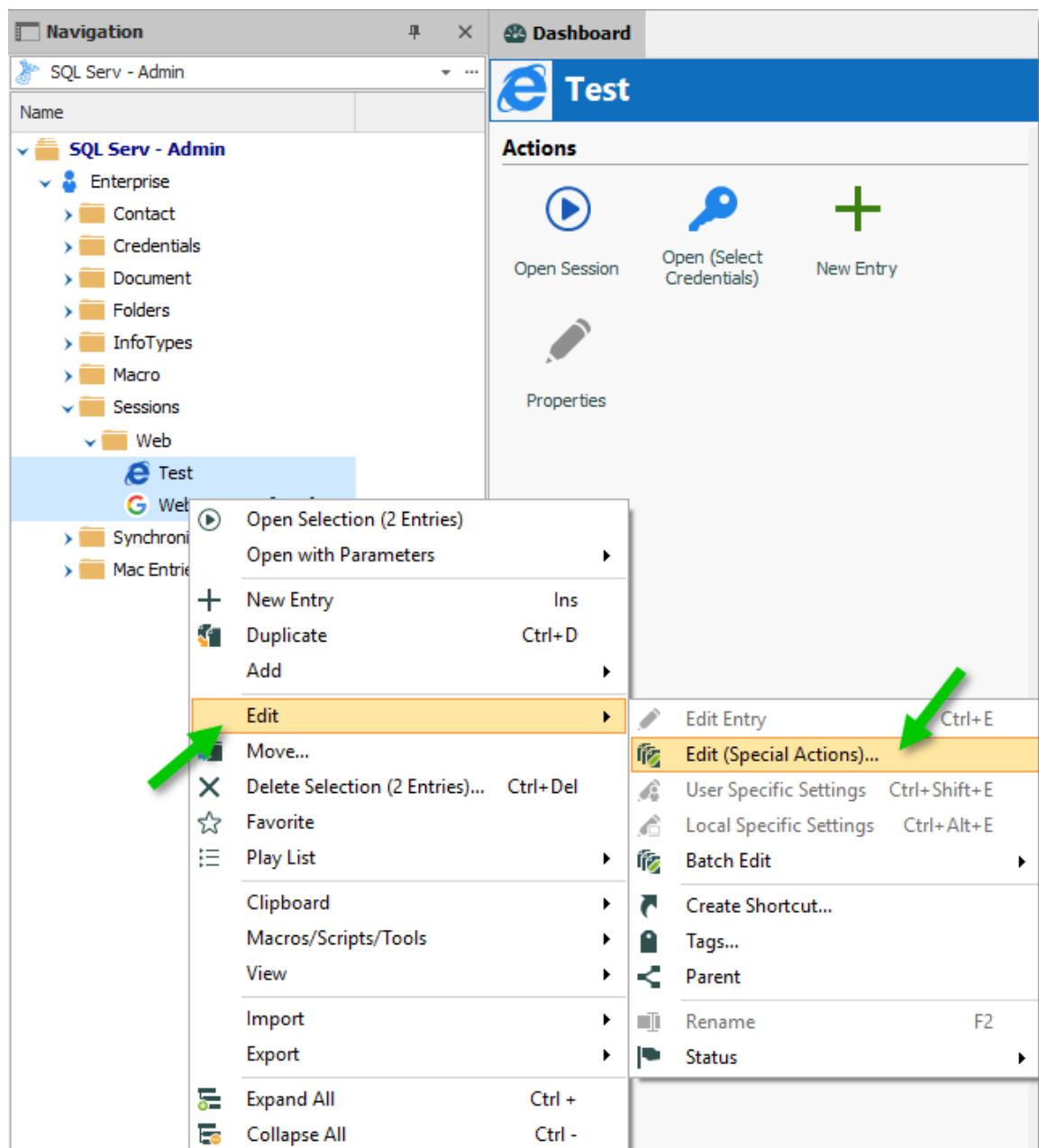
- **Edit - Batch - Edit (Special Actions).**



Edit Toolbar

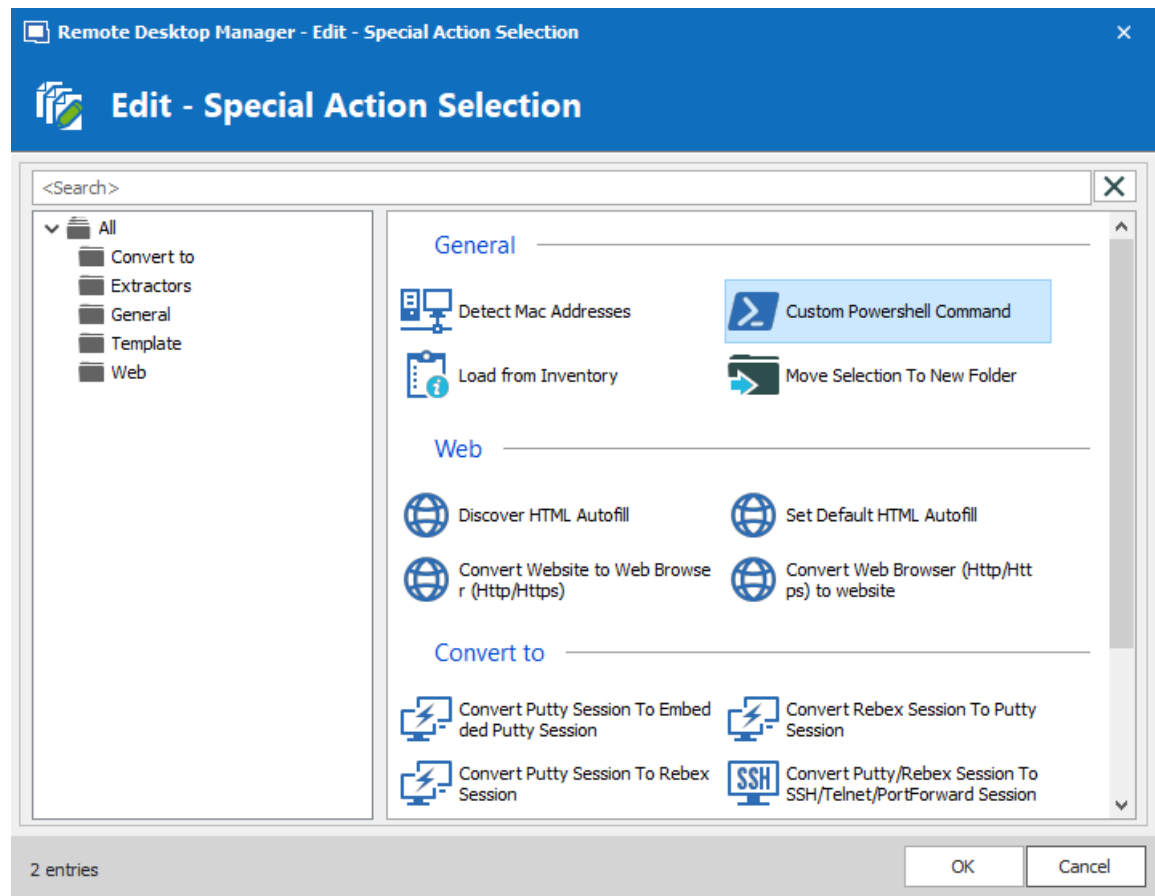
- Right-click then **Edit – Edit (Special Actions).**





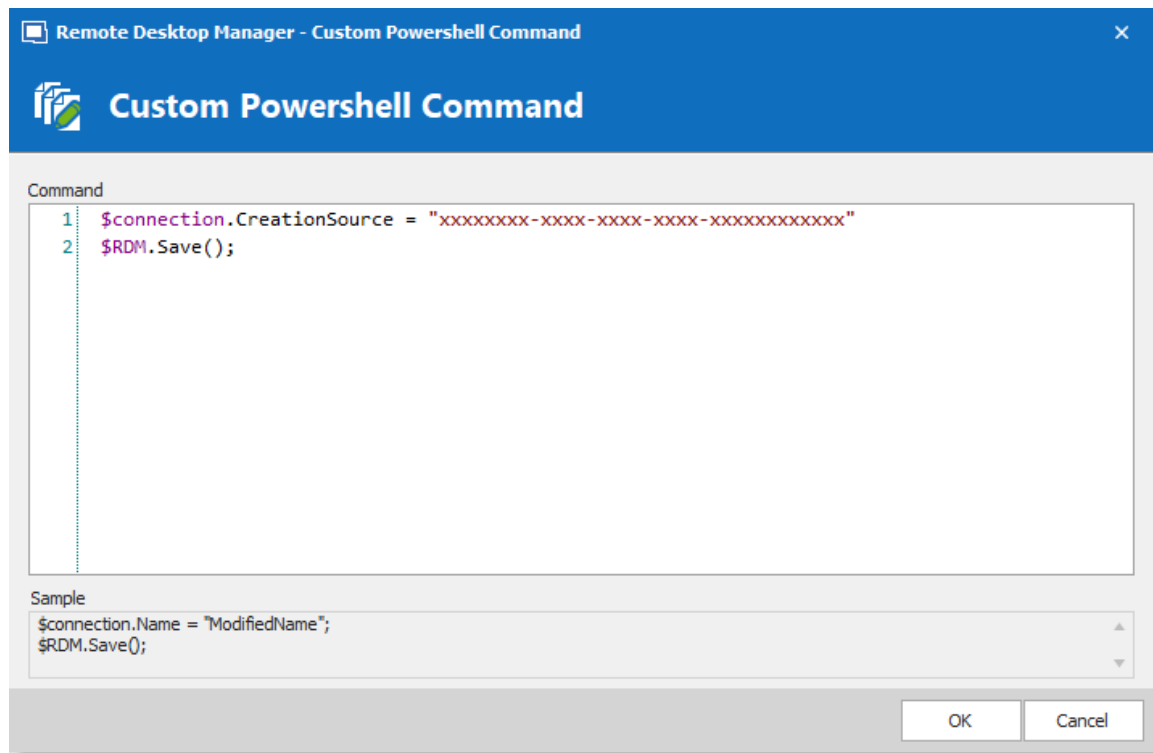
*Selected entries - Edit (Special Actions)*

- Once there, Select **Custom PowerShell Command**.



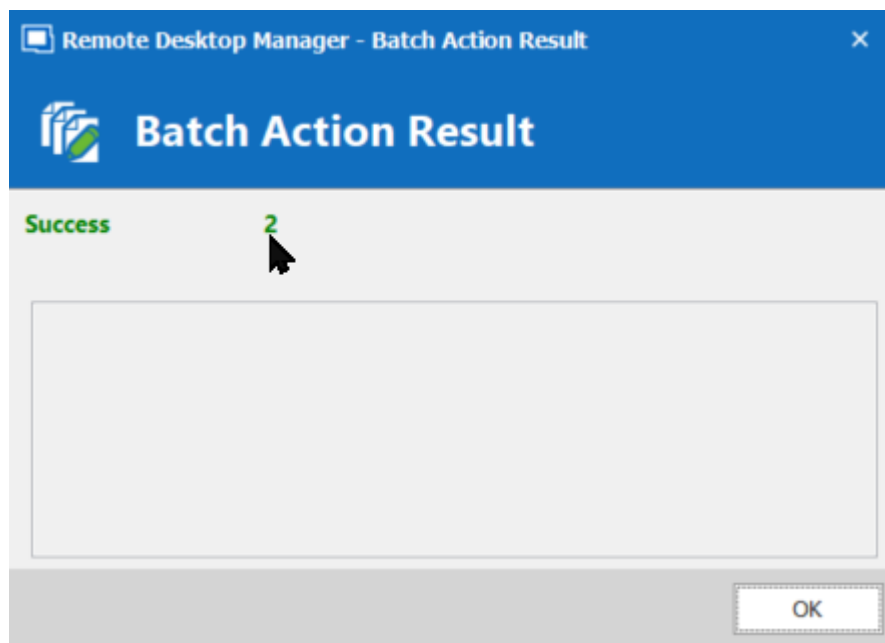
*Edit (Special Actions)*

- A window appears in which you can write a snippet of code. Note that is the last line must always be **`$RDM.Save();`**

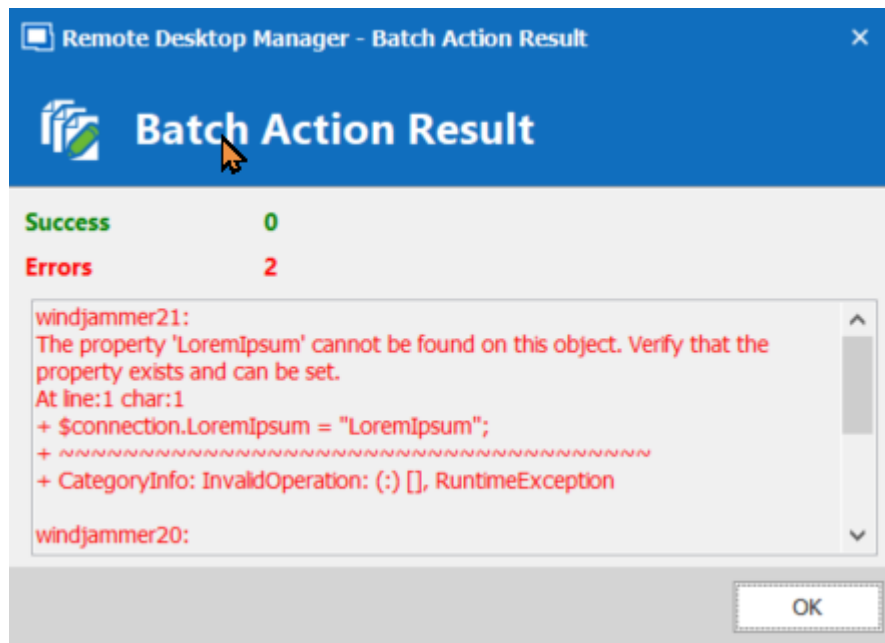


*Custom Powershell Command*

- Upon pressing Ok, a summary dialog appears to indicate success or failure.



*Batch Action Result - Success*



*Batch Action Result - Failure*

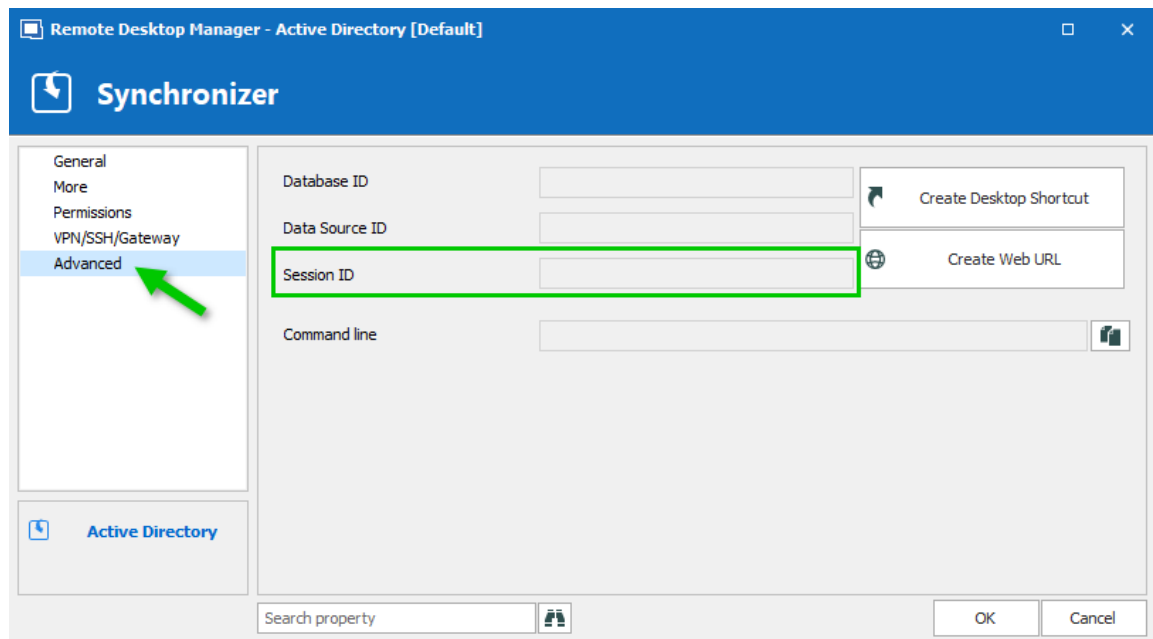
### 9.3.1 Change your Synchronizer source

## 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. In the **Advanced** side menu of the **Properties**, copy the **Session ID** (you will then need that ID number to insert in your Powershell Command).

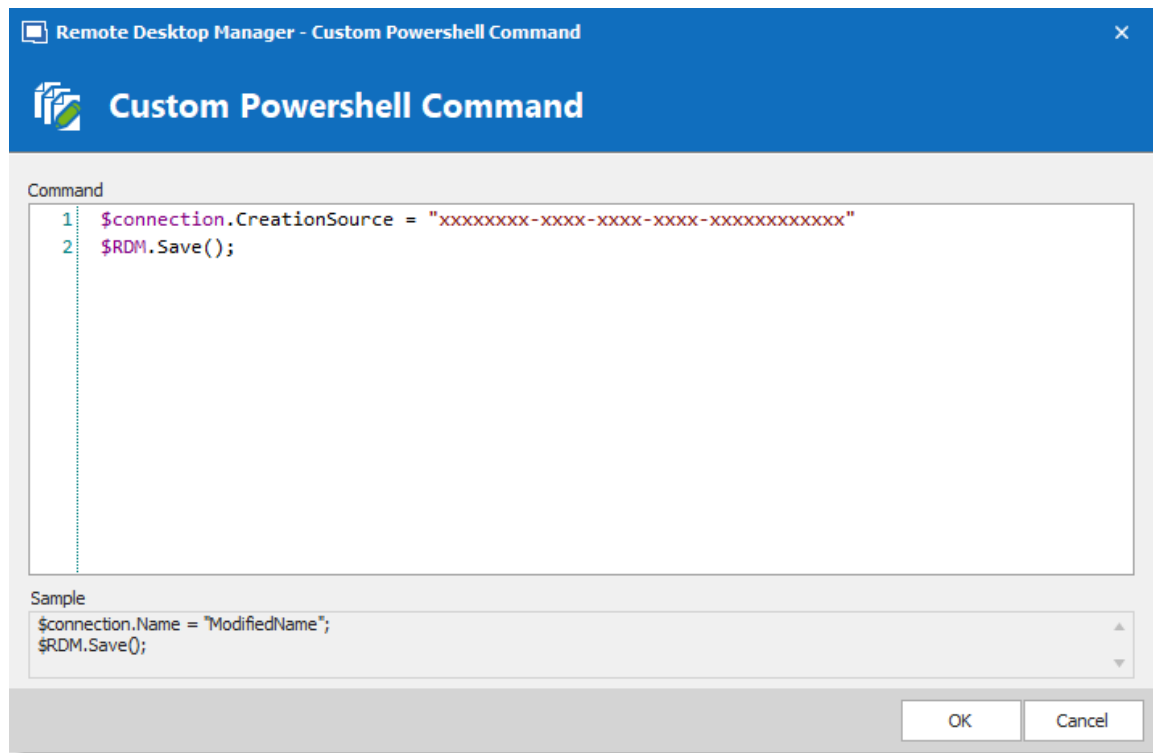


*Advanced - Session ID*

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

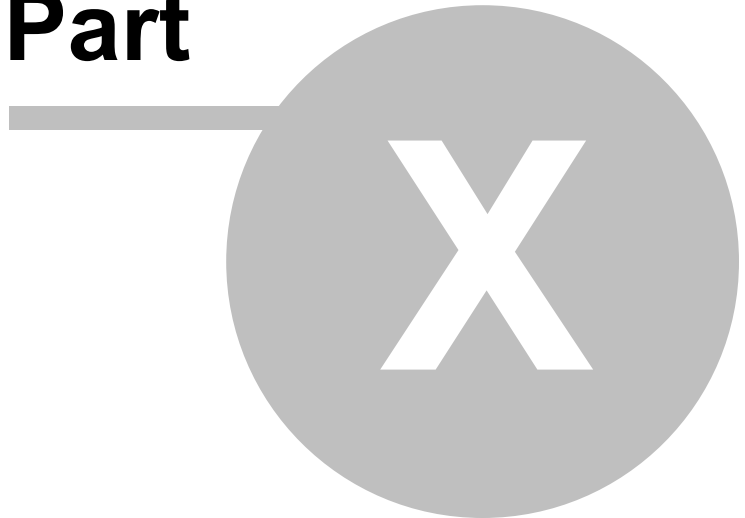
```
$connection.ConnectionType = 3;  
$RDM.Save();
```

## CHANGE KEYBOARD HOOK FOR AN RDP SESSION

```
$connection.KeyboardHook = "OnTheRemoteComputer";  
$RDM.Save();
```

# Support/Resources

**Part**



## 10 Support/Resources

### 10.1 Technical Support

**Hours:** Monday to Friday 7:30 a.m. to 6:00 p.m. EST

**Knowledge Base:** Find helpful information's and procedures regarding our [products](#).

**Email:** [ticket@devolutions.net](mailto:ticket@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 receive an email address and a plan ID. You should send your support requests to the appropriate email address and provide your plan ID in the subject line.

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**.

#### GENERAL

ACTION	SHORTCUT
Filter	Ctrl+F
Force Refresh	Ctrl+F5
Online Help	F1
Quick Connect	Ctrl+Alt+Q
Refresh	F5

#### EDIT

ACTION	SHORTCUT
Add Credential Entry	Alt+Shift+N
Add Folder	Ctrl+Shift+N
Add Information	Ctrl+Alt+N
Add Session	Ctrl+N

ACTION	SHORTCUT
<b>Delete</b>	Ctrl+Del
<b>Duplicate</b>	Ctrl+D
<b>Edit Entry</b>	Ctrl+E
<b>Local Specific Settings</b>	Ctrl+Alt+E
<b>New Entry</b>	Ins
<b>Rename Entry</b>	F2
<b>User Specific Settings</b>	Ctrl+Shift+E

## ACTIONS

ACTION	SHORTCUT
<b>Clipboard - Copy Connection String</b>	Ctrl+Alt+H
<b>Clipboard - Copy Domain</b>	Ctrl+Alt+B
<b>Clipboard - Copy Host Name</b>	Ctrl+H
<b>Clipboard - Copy Password</b>	Ctrl+Shift+B
<b>Clipboard - Copy Url</b>	Ctrl+Shift+H

ACTION	SHORTCUT
Clipboard - Copy Username	Ctrl+B
Execute Typing Macro	Ctrl+Shift+A
Navigate URL	Enter
Open (Embedded/Tabbed)	Ctrl+Enter
Open (External)	Shift+Enter
Open (Full screen)	Alt+Enter
View Password	Ctrl+P

## VIEW

ACTION	SHORTCUT
Dashboard	Alt+F6
Details	F12
Favorites	F10
Grouped Tab Pane	Ctrl+Alt+F9
Header Pane	Alt+Shift+F6
Large Icons	F6

ACTION	SHORTCUT
Navigation Pane	Alt+F8
Opened Sessions	F8
Play List Management	Ctrl+G
RDP Toggle View Only	Shift+F3
Recent (Recent Used Entries)	F9
Status Bar	Alt+F7
Tabbed Entries Pane	Alt+F9
Tiles	F3
Top Pane	Alt+F11
Tree View	F7

## NAVIGATION

ACTION	SHORTCUT
Change Data Source	Ctrl+Shift+D
File	Ctrl+Shift+F
Focus Dashboard	Ctrl+Shift+L



ACTION	SHORTCUT
<b>Focus Tab</b>	Ctrl+Shift+Up
<b>Focus Tree/List</b>	Ctrl+L
<b>Goto Bookmark 1</b>	Ctrl+1
<b>Goto Bookmark 2</b>	Ctrl+2
<b>Goto Bookmark 3</b>	Ctrl+3
<b>Goto Bookmark 4</b>	Ctrl+4
<b>Goto Bookmark 5</b>	Ctrl+5
<b>Goto Bookmark 6</b>	Ctrl+6
<b>Goto Bookmark 7</b>	Ctrl+7
<b>Goto Bookmark 8</b>	Ctrl+8
<b>Goto Bookmark 9</b>	Ctrl+9
<b>Select Next Tab</b>	Ctrl+Shift+Right
<b>Select Previous Tab</b>	Ctrl+Shift+Left
<b>Set Bookmark 1</b>	Ctrl+Shift+1
<b>Set Bookmark 2</b>	Ctrl+Shift+2
<b>Set Bookmark 3</b>	Ctrl+Shift+3

ACTION	SHORTCUT
<b>Set Bookmark 4</b>	Ctrl+Shift+4
<b>Set Bookmark 5</b>	Ctrl+Shift+5
<b>Set Bookmark 6</b>	Ctrl+Shift+6
<b>Set Bookmark 7</b>	Ctrl+Shift+7
<b>Set Bookmark 8</b>	Ctrl+Shift+8
<b>Set Bookmark 9</b>	Ctrl+Shift+9
<b>Switch Vault</b>	Ctrl+Shift+R

## IMPORT/EXPORT

ACTION	SHORTCUT
<b>Import Entries (.rdm, .pvm, .vnc, .rdp)</b>	Ctrl+Shift+I

## 10.3 Lexicon

### DESCRIPTION

Remote Desktop Manager is a feature-rich software that has an extensive set of functionality. Here are the major concepts that are important to understand in order to use the program to its full potential.

### DATA SOURCE

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 source [Overview](#) 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.

## 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.

## INFORMATION ENTRY

An information entry can contain various information like account information, emails, serial numbers. Unlike credential entries, information entries are meant to be shared. Therefore, the data in the information entries is not encrypted. It's 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.

## 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.

## SESSION

In Remote Desktop Manager infancy, 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 to something and that needs to use authentication is a **Session**.

## 10.4 Tutorials

### DESCRIPTION

Our tutorials are published on [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.



## Contact Us

For any questions, feel free to contact us:

**Support:** [ticket@devolutions.net](mailto:ticket@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