



**Remote Desktop
Manager**

Remote Connections & Passwords.
Everywhere!

 **for macOS**

User Manual

2022.2

Table of Contents

Part I Overview	7
1 Remote Desktop Manager.....	8
2 Security	9
3 System Requirements.....	11
4 The Devolutions Platform.....	11
Part II Getting Started	14
1 Using Remote Desktop Manager.....	15
2 Checklist for Individuals.....	15
Select the Data Source - Individuals	17
3 Checklist for Teams.....	18
Select the Data Source type - Teams	20
Part III Installation	23
1 Client	24
Ancillary Files	24
Configuration File Location	26
Registration	27
Enterprise Edition.....	28
Free Edition.....	30
Trial Request.....	34
Register from Devolutions Account.....	35
2 Database Upgrade.....	37
3 Configure SQL Server.....	40
4 Uninstall	41
Part IV User Interface	43
1 Main Screen	44
2 Style	45
3 Quick Access.....	47
Quick Connect	48
Search	49
4 Ribbon	51
5 Navigation Pane.....	52
Vault	54
My User Vault	54
User Vault Search.....	56
Opened Sessions	57
Favorite Entries	59
Most Recently Used Entries	60

6	Content Area	61
	Dashboard	62
	Session.....	63
	Information.....	64
	Folder	65
	Credentials.....	66
	Dashboard tabs.....	67
	Overview	68
	Documentation.....	69
	Macros/Scripts/Tools.....	70
	Embedded Sessions	72
	Split Windows	73
7	Panes (Footer).....	73
	Description	74
	Information	75
	Sub Connections	80
	Part V Data Sources	81
1	Create a New Data Source.....	84
2	Data Source Types.....	88
	Advanced Data Sources	93
	Devolutions Server.....	94
	Password Hub Business.....	99
	SQL Server (MSSQL).....	102
	Configure SQL Server.....	113
	Recovery Model.....	118
	Encrypting Connections to SQL Server.....	119
	Azure SQL.....	121
	Configure Azure SQL.....	129
	Dropbox	132
	Online Drive	136
	Password Hub Personal	141
	SQLite	143
	XML	147
3	Import/Export Data Source.....	151
4	Lock Data Source.....	151
5	2-Factor Authentication.....	153
	Google Authenticator	155
	Yubikey	157
	Duo	158
6	Caching	162
7	Manage Cache.....	164
	Part VI Commands	167
1	File	168
	Go Offline	169
	Lock Application	170
	My Data Source Information	171
	Devolutions Account	175
	Backup	175

	Refresh.....	176
	Settings.....	176
	Restore.....	178
	Data Sources	180
	Overview.....	180
	Manage Password	182
	Import	183
	Overview.....	183
	Import Sessions.....	185
	Export	186
	Overview.....	186
	Export Html Encrypted.....	188
	Preferences	190
	General.....	191
	User Interface.....	193
	Types.....	197
	Security.....	201
	Tools.....	203
	Advanced.....	206
	My Account Settings	208
	Templates	209
	Default Settings.....	212
	Default Credential Settings.....	214
2	Home	216
	Clipboard	218
	Status	220
	Favorite	221
	Insert Log Comment	224
3	Action	225
4	Edit	228
	Add Entries	229
	Creating a New Entry.....	229
	Shortcut Entries.....	232
	Edit Entries	235
	Entry Credentials Options	236
	Move to Another Group/Folder	237
	Setting Overrides	238
	User Specific Settings.....	239
	Override credentials.....	241
	General	243
	Settings	244
	More	248
	VPN	249
	Local Machine Specific Settings.....	250
	Batch Edit	252
	Batch Actions.....	259
	Play List	263
	Actions.....	264
	Management.....	275
	Default at Startup.....	279
	Export Entry	280
5	View	281
	Todo List	282

Add.....	282
Search.....	285
Export.....	286
Advanced Search	287
View Usage Log	290
6 Administration.....	293
Data Source Settings	294
General.....	295
Password Policy.....	297
Password Complexity.....	299
Version Management.....	302
System Message.....	304
Custom Variables.....	305
Security Provider	306
Licenses	309
User Management	311
Permissions.....	319
Integrated Security.....	321
Security Group Management	322
User Groups Management	325
Vault Settings	332
View Deleted	333
Reports	335
Credential Entry References Report.....	336
Entry List Report.....	337
VPN References Report.....	337
Change Current User Password	338
7 Tools	339
Password Generator	340
Entry Security Analyzer	347
8 Window	348
9 Help	349
Application Logs	350
Diagnostic	352
Profiler	355
Debug only.....	358

Part VII Devolutions Web Login 362

1 Overview	363
2 Installation	364
Chrome	364
Firefox	366
Edge	368
Opera	369
3 First Login	371
Password Hub Business Login	371
Password Hub Personal Login	375
Devolutions Server Login	379
Remote Desktop Manager Login	383
Enable Devolutions Web Login.....	386
4 Exploring Devolutions Web Login.....	387

Menu	387
Settings.....	388
Retrieve Credentials	393
Secure Devolutions Web Login	394
Unpair a Browser Extension.....	398
Keyboard Shortcuts	399

Part VIII Support/Ressources 402

1 Technical Support.....	403
2 Lexicon	404
3 Tutorials	405

Overview

Part



1 Overview

1.1 Remote Desktop Manager

DESCRIPTION



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

THE REMOTE DESKTOP MANAGER ECOSYSTEM

Remote Desktop Manager comes in two editions:

Free	For individuals only, no information can be shared with colleagues. The most popular remote access technologies are supported and passwords can be stored securely.
Enterprise	Used by teams, this edition offers permissions, security groups, advanced logging, etc. RDM uses a Database Management System (DBMS) for storing the information and sharing it according to your security requirements. Devolutions also offers two specialized services for 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	✓	✓
Linux	✓	✓
iOS		✓ (Free App)
Android		✓ (Free App)

1.2 Security

DESCRIPTION

All passwords stored in the application database 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.

U.S. FEDERAL GOVERNMENT APPROVED ENCRYPTION

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

This cipher is incredibly 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, implementing encryption of data in transit must be implemented by using the tools involving your chosen technologies. Most customers that have security concerns already choose one of the supported [Advanced Data Sources](#), follow instructions specific to the chosen solution.



The encryption 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 of the connection data*** that is stored in the data source. This will give you 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](#) to control many settings impacting security.
- Use the [Security Provider](#) to encrypt entries completely instead of just the password.
- If using the offline mode, add your own password for an additional layer of protection to the local cache. Go to ***File - Preferences - Security***.
- Require a password to launch the application and even require two-factor authentication. Go to ***File - Preferences - Security***.

- If your data source supports it, choose not to save password in the data source, which will prompt for the credential on the first connection.

1.3 System Requirements

DESCRIPTION

Remote Desktop Manager for Mac requires the following prior to installation.

MINIMUM REQUIREMENTS

- macOS Sierra (10.12)
- 1 GHz or faster processor
- 4GB RAM
- 1440 x 900 screen resolution
- 500 MB hard drive space

1.4 The Devolutions Platform

DESCRIPTION

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

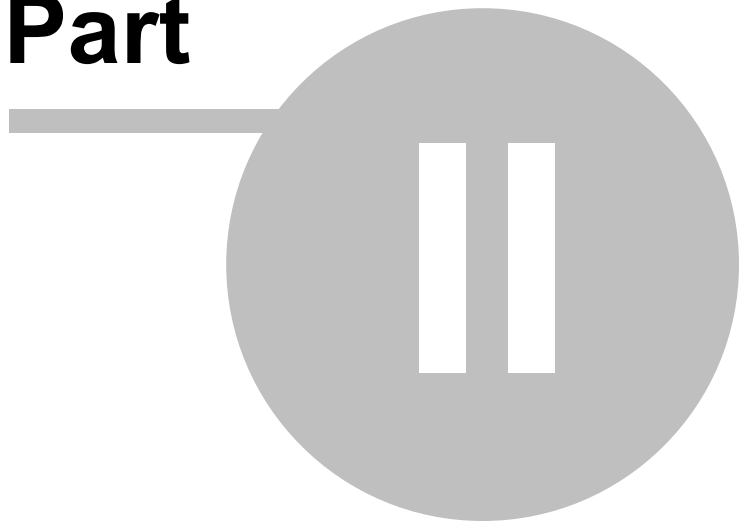
APPLICATIONS	DESCRIPTION	INSTALLATION
Remote Desktop Manager (RDM)	Application used to manage and centralize remote access technologies, privileged	Windows, macOS,

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

APPLICATIONS	DESCRIPTION	INSTALLATION
<u>Devolution Web Login (DWL)</u>	Devolution Web Login is a free browser 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.	Windows, macOS

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">• Enterprise Registration• Trial Registration	<p>Remote Desktop Manager Enterprise Edition grants you a 30-day trial. If you decide not to register by the end of the trial, your data will not be altered or erased, and you will have full access to it once you provide a license key.</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 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.</p> <p>Upon first launch, Remote Desktop Manager for Mac uses an SQLite data source. The different data sources are explained in the Data Source Types section. For help selecting a data source tailored to your needs, please see Choosing your data source (Individuals).</p>
Step 3 - Set up your Devolutions Online Backup.	<p>Devolutions Online Backup allows you to securely back up your information for selected data sources. The backup is automatically executed 30 seconds after any modifications made to the data source content. It is best practice to always back up your data source.</p>
Step 4 - Create your Default Settings .	<p>In File - Preferences, you can create, modify or reset default settings for your templates. Each entry type is supported and can have a default template defined to fit your requirements.</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>
Step 6 - Import your data .	<p>The final step is to import all of your data into Remote Desktop Manager. You can import your sessions, logins and contacts in a few steps.</p>

2.2.1 Select the Data Source - Individuals

DESCRIPTION

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

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



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

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

NOTES

NOTE 1

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

NOTE 2

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

2.3 Checklist for Teams

DESCRIPTION

We have created a checklist to help you get started with Remote Desktop Manager for Mac when working in a team environment.

CHECKLIST FOR TEAMS	DESCRIPTION
<p>Step 1 - Register your license:</p> <ul style="list-style-type: none">• Enterprise Registration• Trial Registration	<p>Remote Desktop Manager Enterprise Edition grants you a 30-day trial. If you decide not to register by the end of the trial, your data will not be altered or erased, and you will have full access to it once you provide a license key.</p>

CHECKLIST FOR TEAMS	DESCRIPTION
Step 2 - Add your Data Source (for teams) .	<p>Warning: When choosing any data source type that is not on-premises, you need to think about the safety of the data at rest and during transport. We strongly recommend that you further encrypt your data by applying a master key for file-based solutions, or a Security Provider for Advanced Data Sources. This ensures only you can read the data.</p> <p>Upon first launch, Remote Desktop Manager uses a local SQLite data source. The different data sources are explained in the Data Sources section. For help selecting a data source tailored to your needs, please see Choosing your data source (Teams).</p>
Step 3 - Select your Security Provider .	Select your Security Provider before importing or creating any data in your database so nobody can read your entry configuration data, even when people have a direct access to your database.
Step 4 - Create your folder structure.	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.
Step 5 - Create your Default Settings .	In File - Preferences , 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.
Step 6 - Create Users .	Remote Desktop Manager supports advanced User Management. User accounts must be created manually by an administrator of the database.
Step 7 - Create User Groups .	Create User Groups to 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.

	CHECKLIST FOR TEAMS	DESCRIPTION
	Step 8 - Create Entries.	An Entry is how you save information about your sessions (e.g. RDP, SSH connections), credentials, websites, VPNs, synchronizers and documents.
	Step 9 - Grant Permissions .	Once your users are created you can then grant Permissions for user groups based access control. The permissions granted on the folder can be inherited by each entry set under that folder.
	Step 10 - Import your Data .	The final step is to Import all of your data into Remote Desktop Manager. You can import your sessions, logins and contacts in a few steps.

2.3.1 Select the Data Source type - Teams

DESCRIPTION

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



When choosing any data source type that is not **on-premise**, you need to think of 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 make choosing the data source type easier, we are presenting a set of concerns and the list of data sources that can serve in that context. If you have multiple concerns simply create the intersection of all sets to isolate a list of choices.

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

NOTES

NOTE 1

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

NOTE 2

Integrated security is the name of a Microsoft technology that allows access to an instance of SQL Server without sending credentials, but rather by using the token provided by the authentication in your Windows computer. This therefore allows the

users to connect directly to the database using other tools. It should not be used if you need to prevent direct access to the database.

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

NOTE 3

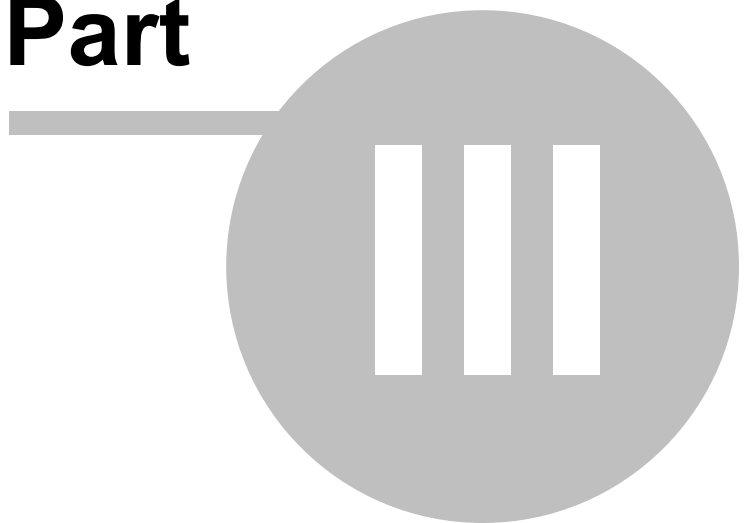
You should not expose a Devolutions Server instance to the Internet without being able to protect it from DDoS attacks. Strong passwords must be used as well as obscure account names that are not easily inferred using social data mining.

NOTE 4

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

Installation

Part



3 Installation

3.1 Client

DESCRIPTION

Remote Desktop Manager for Mac can be downloaded as a .dmg 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).

LICENCE

Remote Desktop Manager for Mac 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 has already been created using the SQLite format. You may add as many data sources as needed, please see [Data Source Overview](#) for more information.



To use a SQL Server/Azure SQL data source, please read the [Configure SQL Server](#) topic.

3.1.1 Ancillary Files

DESCRIPTION

Remote Desktop Manager for Mac 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%** variable to denote when a file is stored in a configuration folder that can be relocated, or **%PROFILE%** 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.

The **Override** 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
Encryption (*.enc, *.enb)	%CONFIG%	None
Layout Files (*.lyt)	%CONFIG%	None
Log Files (*.log, *.debug)	%CONFIG%	None
Local Play lists	%PROFILE% \{Datasource}\Playlists	Use for application directory for local playlist
Local Templates	They are serialized directly in the configuration file of the application	None

Offline/Cache data (offline.db)	%PROFILE%\{Datasource}	Use application directory for online cache
Sensitive (*.stv, *.stb)	%CONFIG%	None
Themes	%CONFIG%	None

3.1.2 Configuration File Location

DESCRIPTION

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

You can find the configuration file by following these steps:

1. Open Finder
2. Click Go in the menu
3. Select Go to folder
4. Paste this path: ~/Library/Application Support
5. Open the folder: com.devolutions.remotedesktopmanager
6. Locate the RemoteDesktopManager.cfg or RemoteDesktopManagerFree.cfg file

In order for us to provide you a secure link to share your file, send an email to service@devolutions.net.



3.1.3 Registration

DESCRIPTION

REMOTE DESKTOP MANAGER FOR MAC ENTERPRISE EDITION

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

REQUEST A TRIAL

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

REMOTE DESKTOP MANAGER FOR MAC FREE EDITION

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

3.1.3.1 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](#).

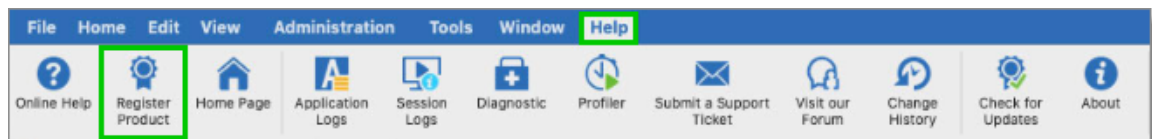


It is possible to request a trial to try Remote Desktop Manager for Mac for 30 days. If you decide not to register the application with an Enterprise Edition license serial at the end of the 30 days period, your data will not be altered or erased, and you will have full access to it once you provide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

MANUAL REGISTRATION

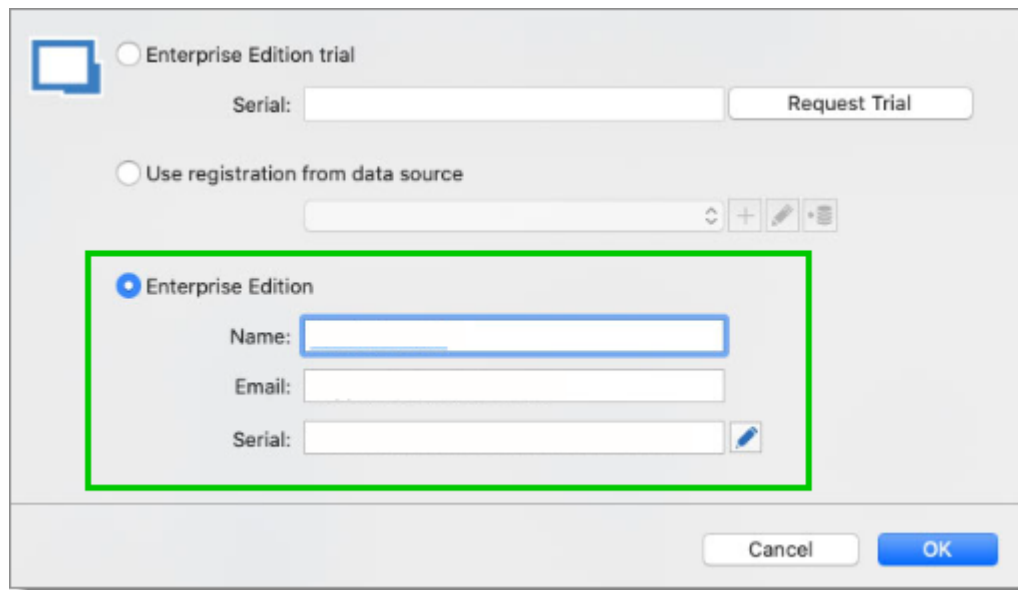
Remote Desktop Manager Enterprise license serials are delivered by email.

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**.



The screenshot shows a registration dialog box for Remote Desktop Manager. It has two main sections: 'Enterprise Edition trial' and 'Use registration from data source'. The 'Enterprise Edition trial' section is currently selected and highlighted with a green border. It contains a 'Serial' input field and a 'Request Trial' button. The 'Use registration from data source' section is unselected. Below it, there is a dropdown menu and three icons (up/down arrows, a plus sign, and a list icon). The 'Enterprise Edition' section is also highlighted with a green border and contains 'Name', 'Email', and 'Serial' input fields, along with a 'Cancel' button and an 'OK' button at the bottom right.

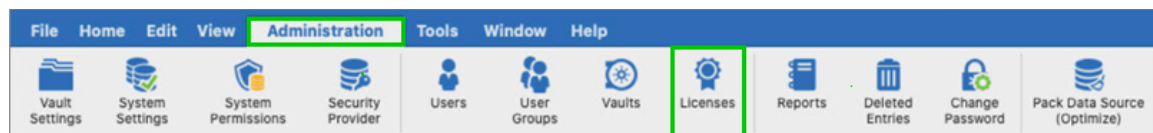
Register Enterprise Edition

REGISTRATION FROM THE DATA SOURCE

When the license serial is stored in the [Licenses](#) of an [Advanced Data Source](#), there is no need to register Remote Desktop Manager for Mac 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.

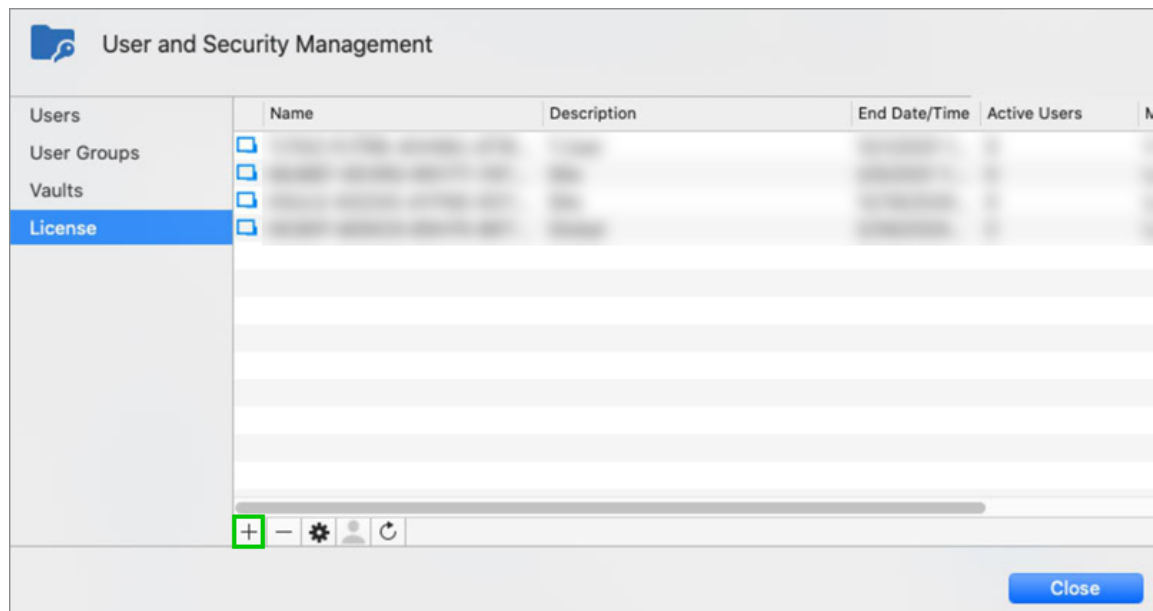
FOR ADMINISTRATORS

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



Administration - Licenses

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



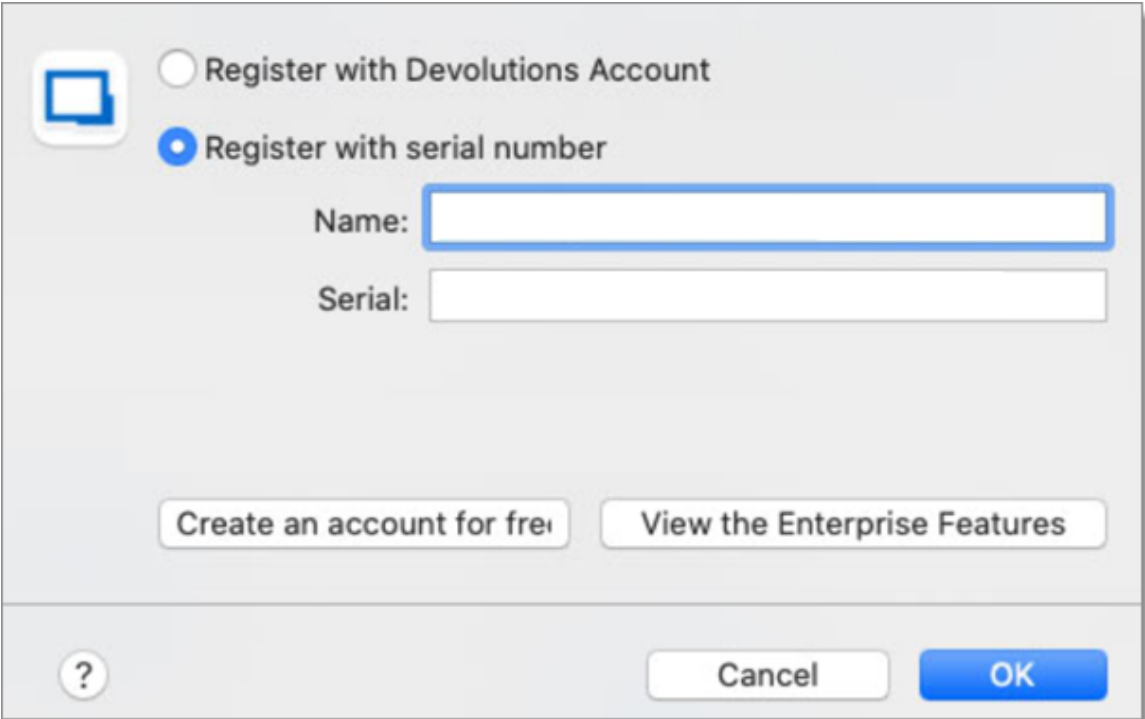
User and Security Management - License

3.1.3.2 Free Edition

DESCRIPTION

Remote Desktop Manager for Mac 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.

A registration dialog box with a light gray background. In the top-left corner is a blue icon of a computer monitor. To its right are two radio buttons: the first is unselected and labeled "Register with Devolutions Account"; the second is selected (indicated by a blue dot) and labeled "Register with serial number". Below these are two text input fields: the first is labeled "Name:" and the second is labeled "Serial:". At the bottom of the dialog are three buttons: a help button with a question mark icon on the left, a "Cancel" button in the center, and an "OK" button on the right. The "OK" button is highlighted in blue. Above the "Cancel" and "OK" buttons are two smaller buttons: "Create an account for free" and "View the Enterprise Features".

Register the Application

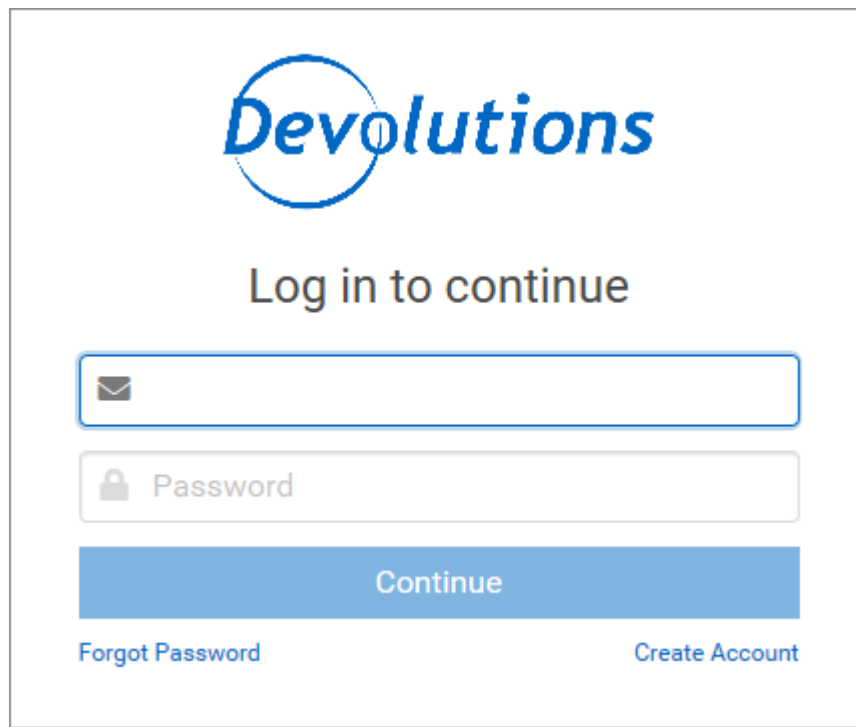
USE REGISTRATION FROM DEVOLUTIONS ACCOUNT

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**.



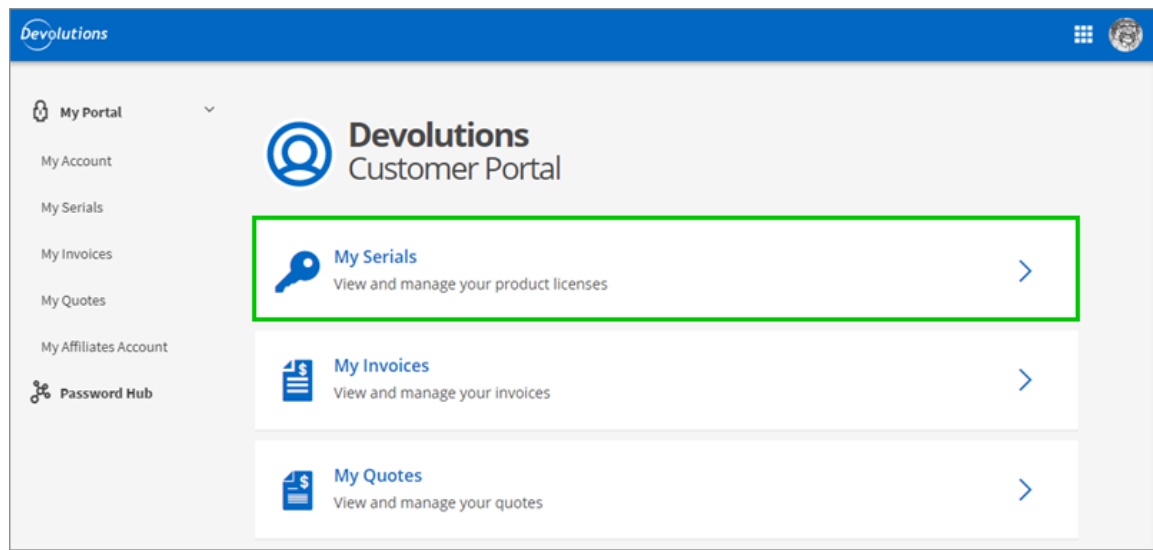
Devolutions Account Login

The license serial will be retrieved automatically.

REGISTER THE FREE EDITION WITHOUT AN INTERNET CONNECTION

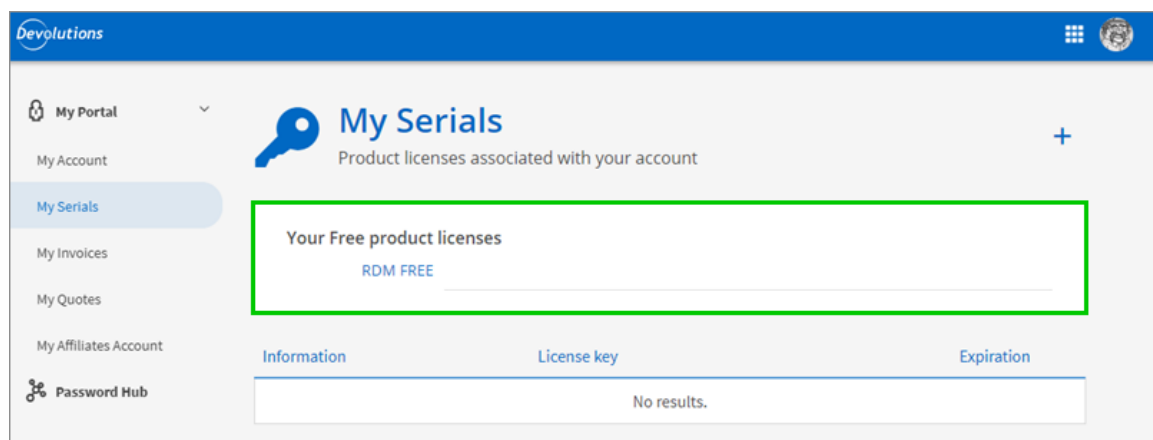
In the event that you need to register the application without an internet connection, the information must be entered manually. You will need the license serial from your [Customer Portal](#)

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



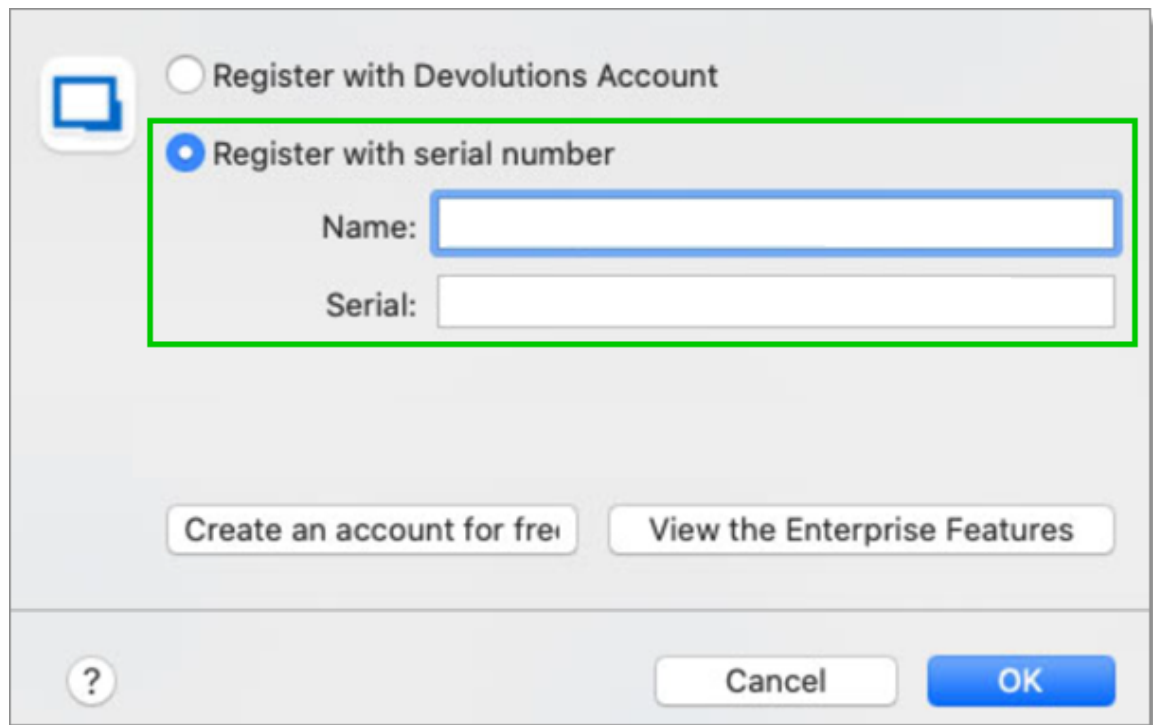
Customer Portal - My Serials

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*

3.1.3.3 Trial Request

DESCRIPTION

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



Request your Remote Desktop Manager Enterprise 30 day trial from our [website](#).

STEPS

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

2. 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**.

The screenshot shows a dialog box titled "Register Enterprise Edition trial license". It features a sidebar with a monitor icon. The main area has three radio buttons: "Enterprise Edition trial" (selected), "Use registration from data source", and "Enterprise Edition". The "Enterprise Edition trial" section includes a "Serial:" text box and a "Request Trial" button. The "Use registration from data source" section includes a dropdown menu and three icons: a plus sign, a pencil, and a list icon. The "Enterprise Edition" section includes "Name:", "Email:", and "Serial:" text boxes, with a pencil icon next to the "Serial:" box. At the bottom right are "Cancel" and "OK" buttons.

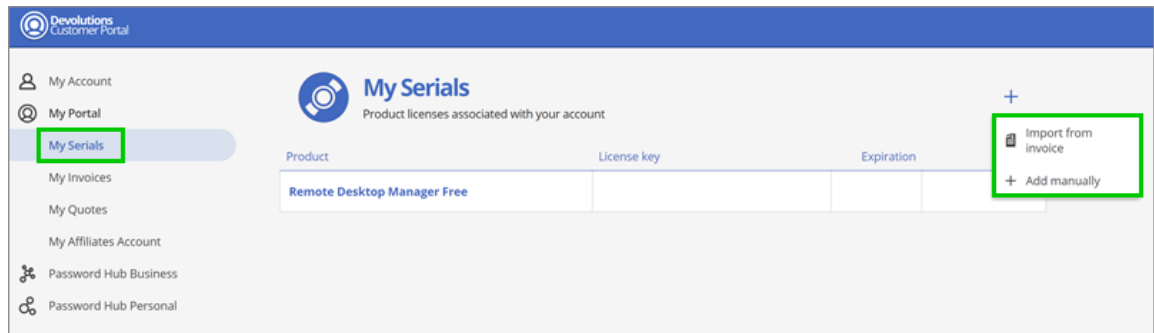
Register Enterprise Edition trial license

3.1.3.4 Register from Devolutions Account

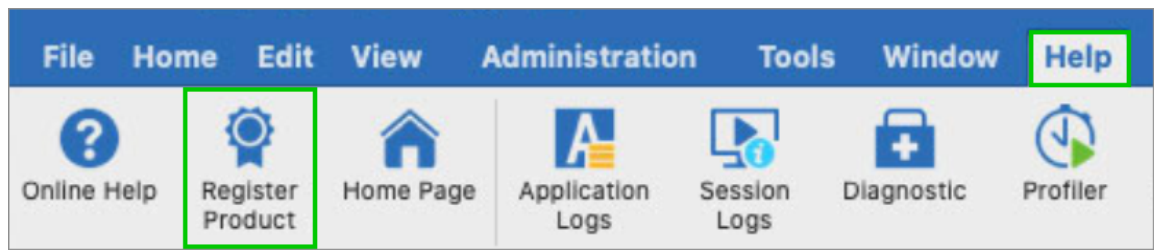
DESCRIPTION

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

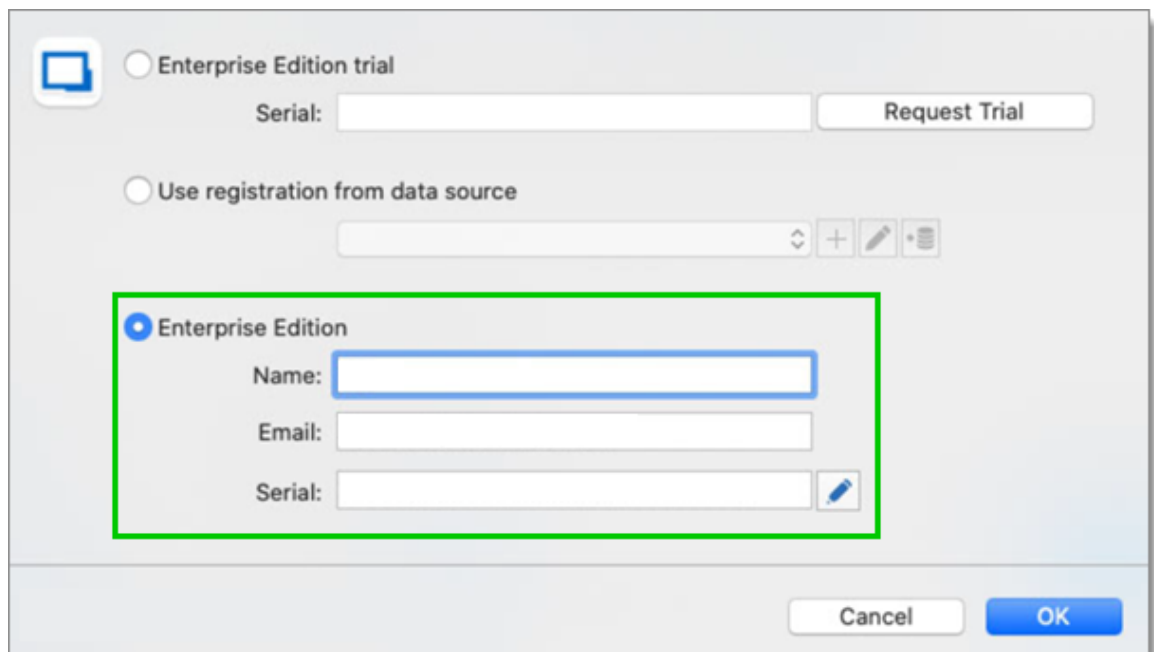
When creating a Devolutions Account a free license serial is provided for the free edition of our product. License serials purchased for the enterprise edition can be stored in the **My Serials** section of the Devolutions Customer Portal.

*Devolutions Customer Portal - My Serials*

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

*Register Product*

2. In the **Register Product** window, select **Enterprise Edition**. Enter your Devolutions Account credentials.

*Registration Devolutions Account*

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 for Mac releases must alter the database structure. These are performed automatically for you but it is a 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 actions on this screen must have administrative privileges on the database management system. You must also be **SYSDBA** or **DB_OWNER**.



Perform a database backup and ensure that you can quickly perform a restore if the need arises



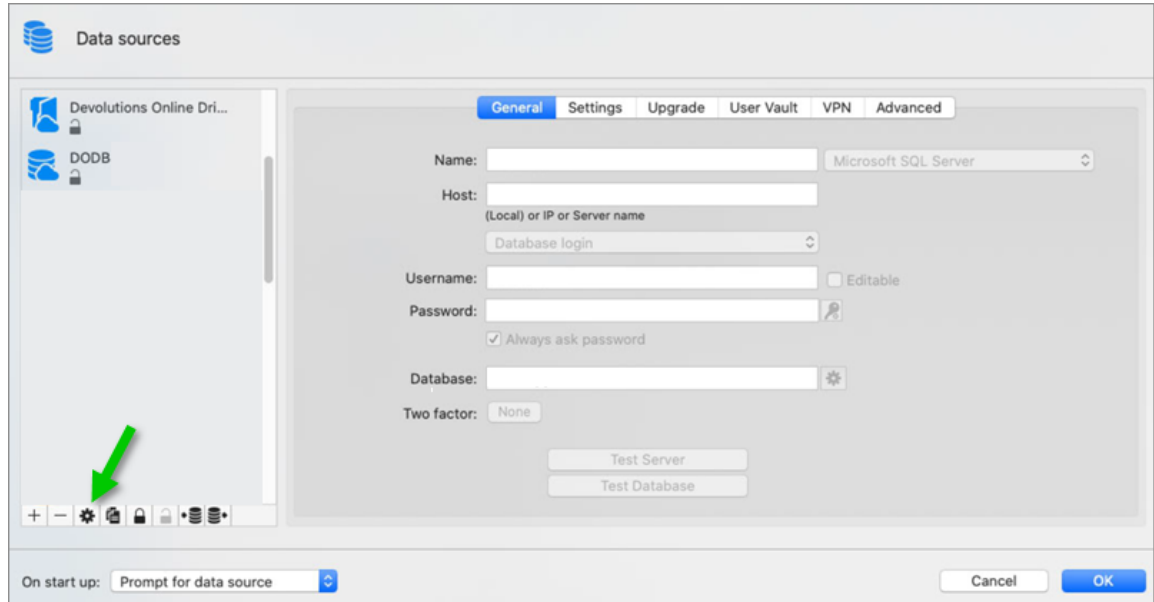
If your organization allows for a read/write offline cache, ensure that all of your users have merged their offline edits.

STEPS

Follow these steps for a successful version update:

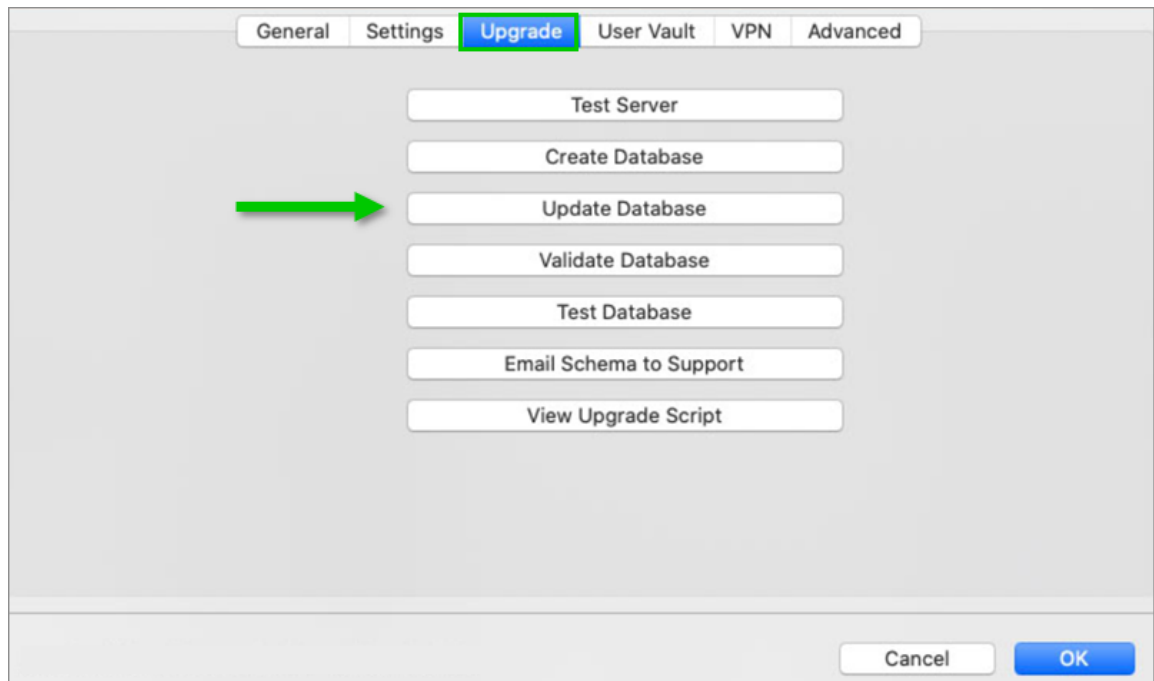
1. Ensure you are the sole user of the database during the upgrade process. If your environment allows for offline use, have your team switch to the offline mode; or have them switch to another datasource
2. Backup your database using the database tools.
3. Open Remote Desktop Manager for Mac while logged on as a user with administrative rights. You must also be SYSDBA or DB_OWNER.

4. 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 and edit your data source to upgrade.



Edit your data source

5. Switch to the **Upgrade** tab, then click on Update Database



Upgrade tab - Upgrade Database

Option	Description
Test Server	Test the connection with the server to validate if the proper information has been provided.
Create Database	Create the database on the SQL server.
Update Database	<p>Follow these steps for a successful version update:</p> <ol style="list-style-type: none">1. Ensure you are the sole user of the database during the upgrade process.2. Backup your database using the DBMS tools.3. Open Remote Desktop Manager for Mac while logged on as a user with administrative rights. You must also be SYSDBA or DB_OWNER.4. You may be prompted with an upgrade message when your data source is accessed. If so accept the upgrade.5. Update the client software on all workstations.
Test Database	Test the connection to the database to validate if the proper information has been provided. The test database uses the name of the database in the General tab.
View upgrade script	Allow viewing the updated script before the launch of the database update.

6. Wait for a success message
7. Close the dialog
8. Ensure your Remote Desktop Manager for Mac 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 most critical in your environment.
11. Update the client software on all workstations.

3.3 Configure SQL Server

DESCRIPTION

SERVER COMPUTER

1. Install SQL Server or SQL Server Express (that edition is free).



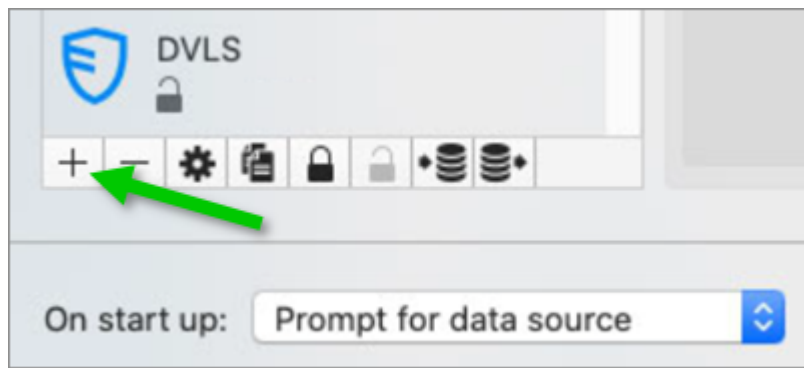
Newly installed SQL Server instances do not allow remote connections. Please follow the directions in SQL Server.



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

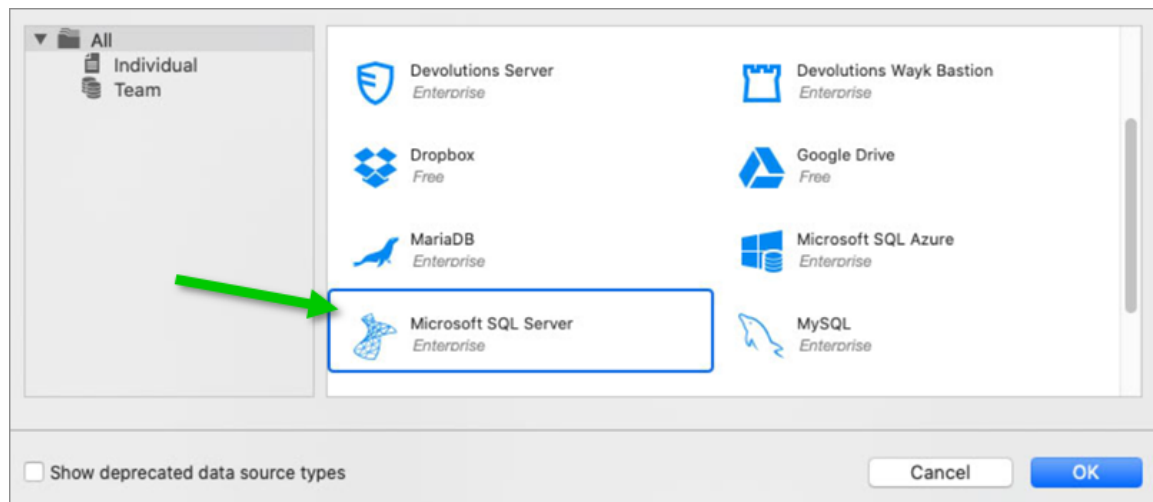
Please follow directions on <http://support.microsoft.com/kb/316898>

2. To create an empty database, select **File - Data Sources - Add** 

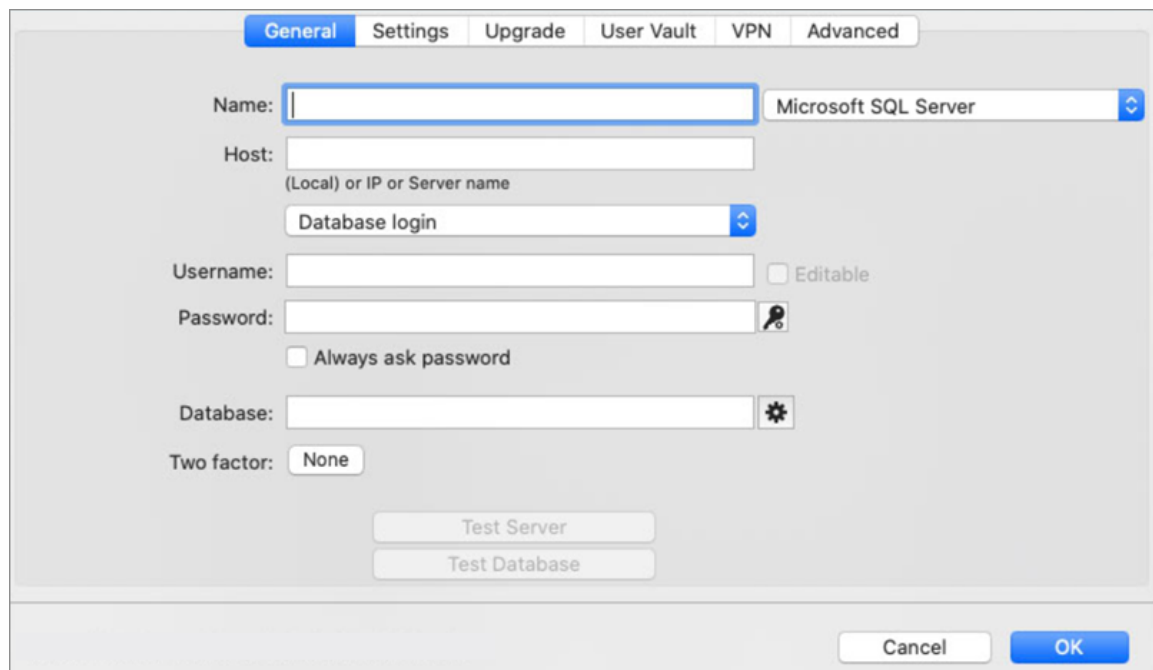


Data sources

3. Choose Microsoft SQL Server in the list.



4. Configure the connection and run a test using **Test Server**.



SQL Server Data Source Configuration

3.4 Uninstall

DESCRIPTION

INSTRUCTIONS

Move Remote Desktop Manager for Mac to the trash to uninstall the application.

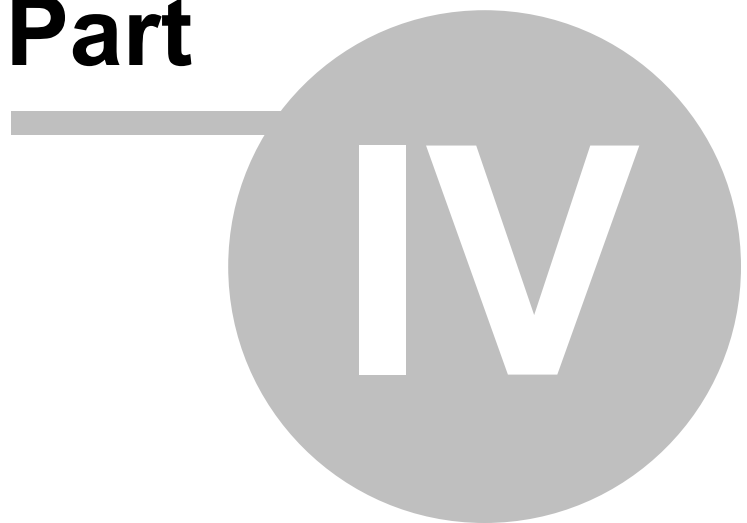
You also need to delete the ***com.devolutions.remotedesktopmanager*** folder to removed all the application local files from your computer. This folder is located in ***Macintosh HD/Users/Username/Library/Application Support***.

The ***com.devolutions.remotedesktopmanager*** folder contains the following files:

- Configuration file (RemoteDesktopManager.cfg)
- Layout configuration file (RemoteDesktopManager.lyt)
- Application logs (RemoteDesktopManager.log)
- Default XML data source
- Default SQLite data source

User Interface

Part

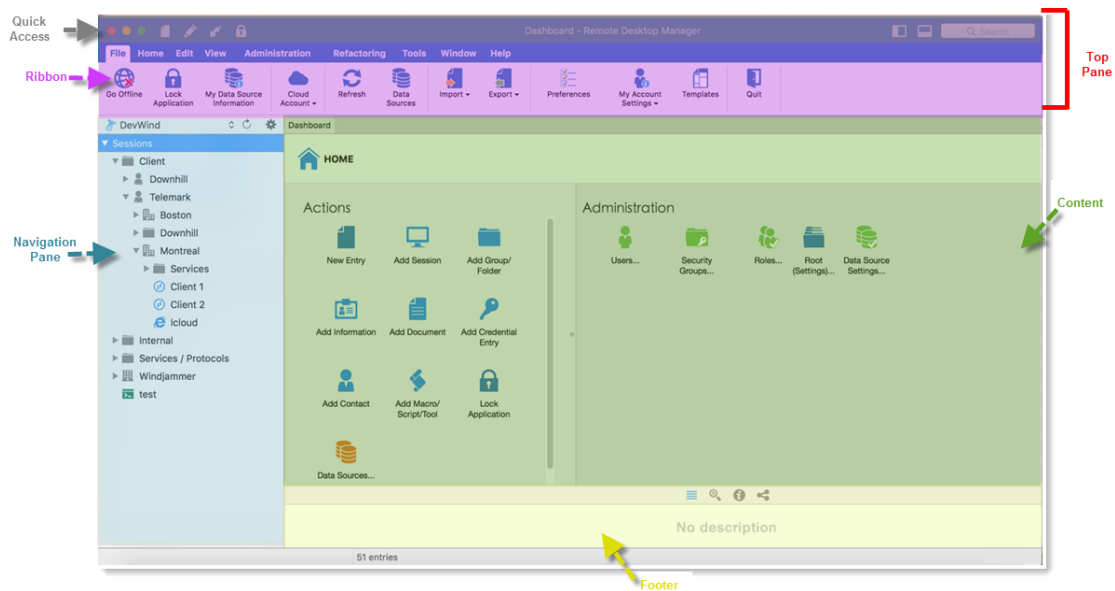


4 User Interface

4.1 Main Screen

DESCRIPTION

Below is an illustration of Remote Desktop Manager for Mac's main screen.



Main Screen

Refer to the the following topics for additional details:

- [Quick Access](#)
- [Navigation Pane](#)
- [Content Area](#)
- [Footer](#)

4.2 Style

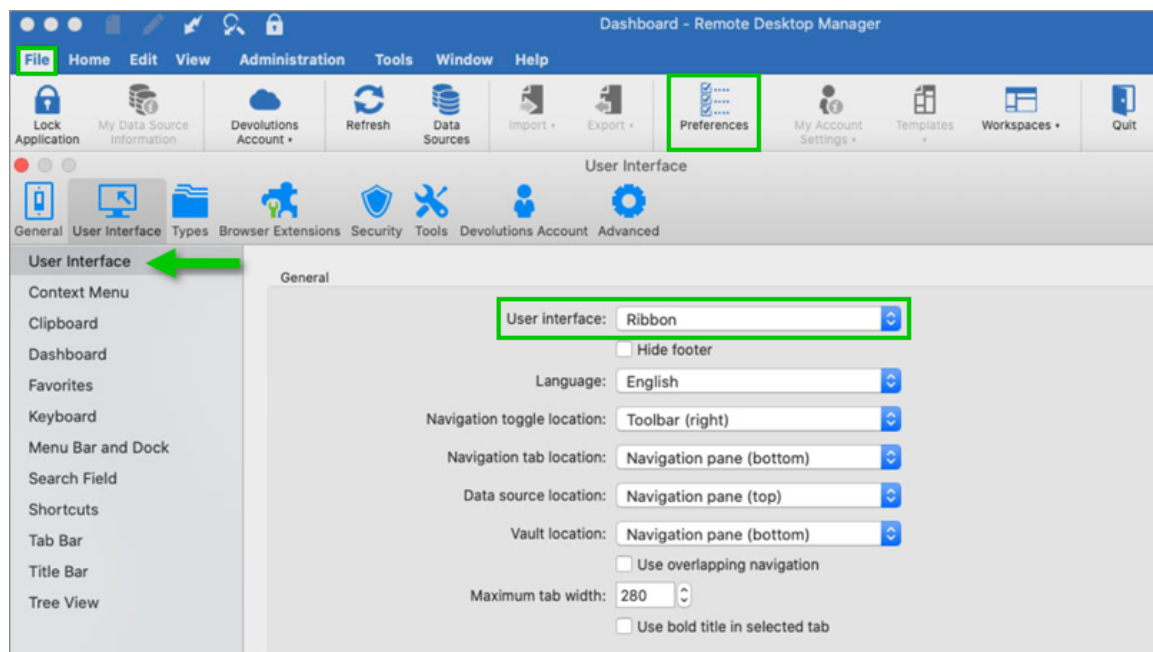
DESCRIPTION

Remote Desktop Manager for Mac 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. Two styles currently exist:

- Ribbon
- Classic

CONFIGURATION

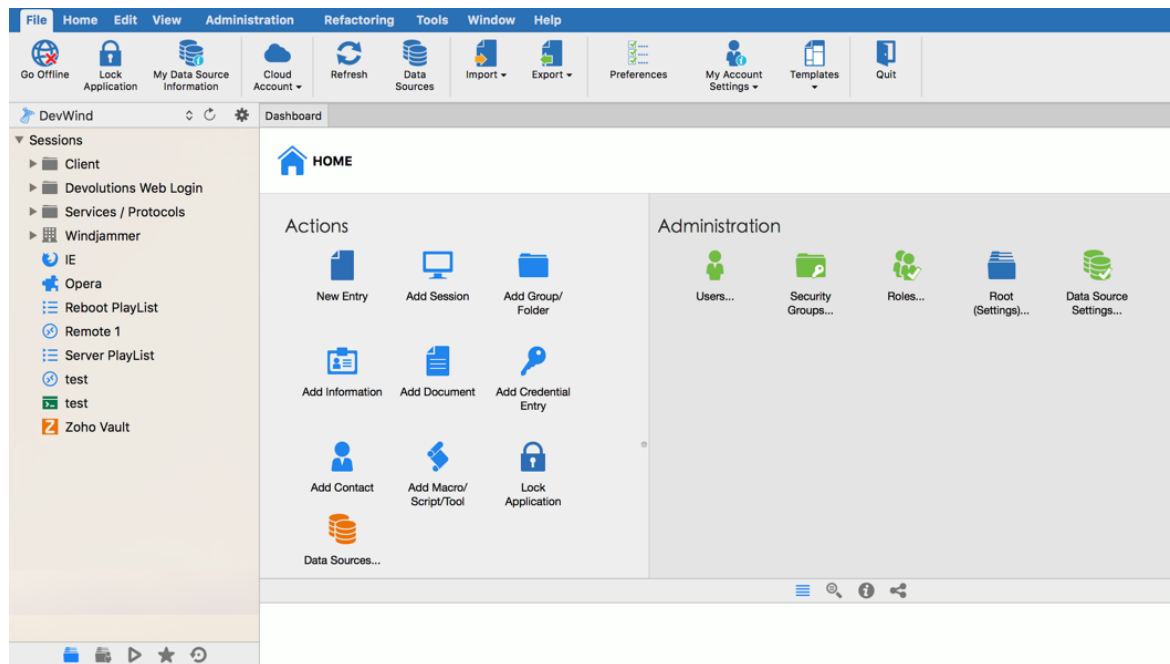
To select the User Interface style you must go in **File - Preferences - User Interface**.



User Interface - Options

RIBBON

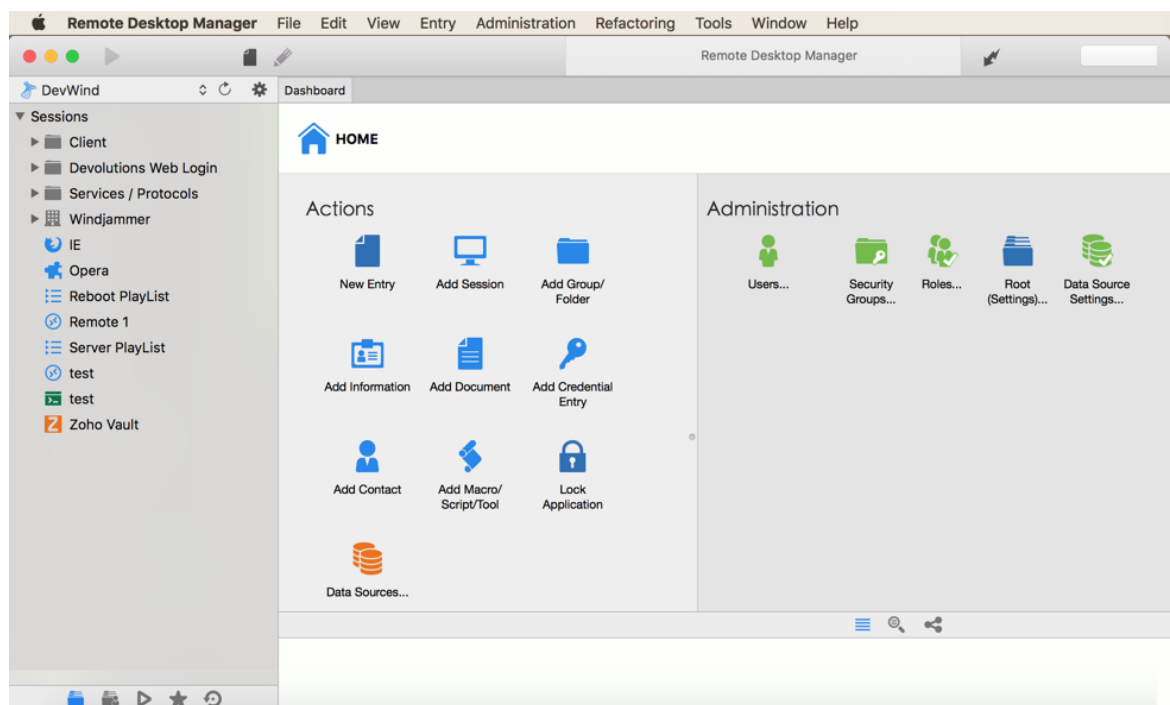
The ribbon is Remote Desktop Manager for Mac default style that sports an advanced control called ribbon. Icons and text makes it easy to learn what feature exists.



RDM main screen - Ribbon style

CLASSIC

Classic is Remote Desktop Manager for Mac previous generation style, it holds a standard menu to invoke commands.



RDM main menu - Classic style

4.3 Quick Access

DESCRIPTION

The **Quick Access** Toolbar normally sits at the top of the application. It is composed of multiple parts:

- Favorite commands
- Quick Connect
- Search
- Lock application





Quick Access Toolbar

SETTINGS

FAVORITE COMMANDS



Quick Access - Favorite commands

Command	Description
	Create a new entry in your current data source.
	Open the properties window of your selected entry.

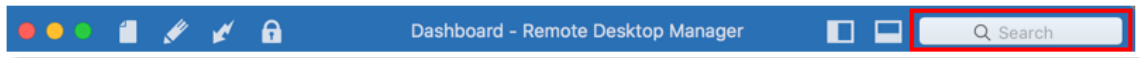
QUICK CONNECT



Quick Access - Quick Connect

Please refer to [Quick Connect](#)

SEARCH



Quick Access - Search

Please refer to [Search](#)

LOCK APPLICATION



Quick Access - Lock Application

Please refer to [Lock Application](#)

4.3.1 Quick Connect

DESCRIPTION

Via the **Quick Connect** feature, you can open an ad-hoc session by specifying the host and session type. It's also possible to create a template and have the connection established with it. In the template you set the desired settings, and Remote Desktop Manager will apply them when connecting to the specified host.

SETTINGS

The **Quick Connect** feature is accessible from the menu **View - Quick Connect** or via the **Quick Connect** button located in the Remote Desktop Manager for Mac [Toolbar](#).




Quick Connect

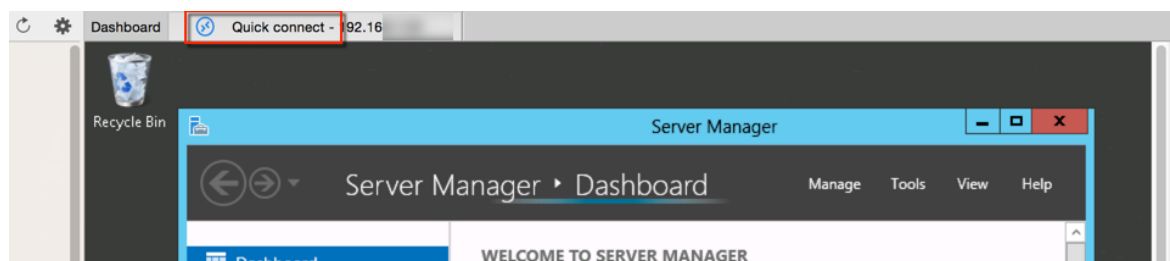
Enter the Host (IP Address), User name as well as the Password and click on **Connect**.

The **Browse** button will list network discoverable computer to allow you to select computer from the list. Listing network discoverable devices is a lengthy operation.

Quick Connect combo box

You can also select a previous host name by clicking on the  arrow.

The connection with the remote computer will automatically be established.



Quick Connection

4.3.2 Search

DESCRIPTION

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 Filter options.

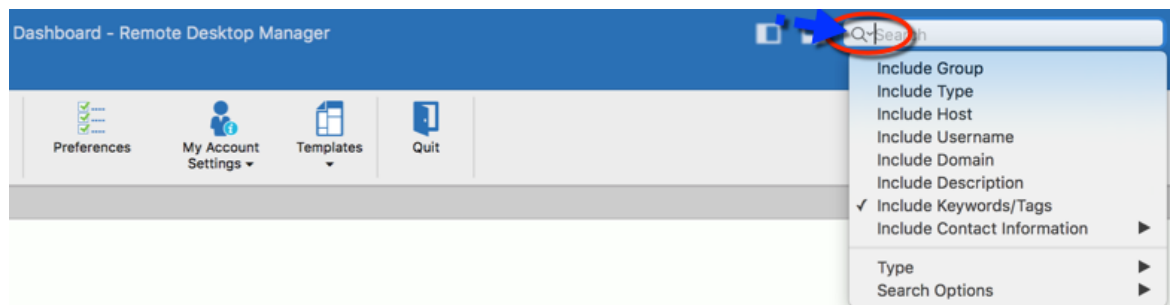
SETTINGS

The **Search** filter is accessible from the Remote Desktop Manager for Mac Quick Access [Toolbar](#).



Quick Access - Search

Click on the arrow in the Search box to display your search options.



Search box - Dropdown options

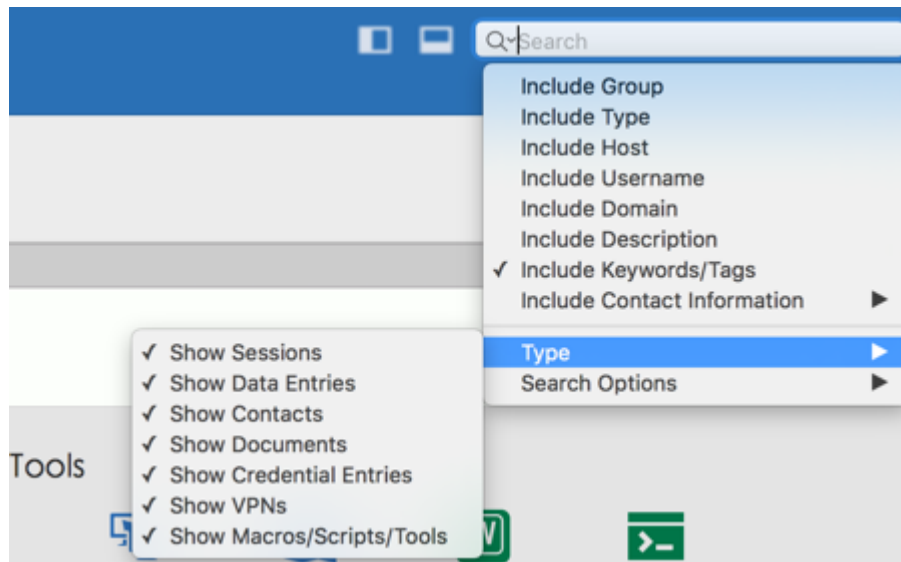
The filter expression is matched against fields as selected in the filter options such as:

- Group
- Type
- Host
- Username
- Domain
- Description
- Keywords/Tags
- Contact Information

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

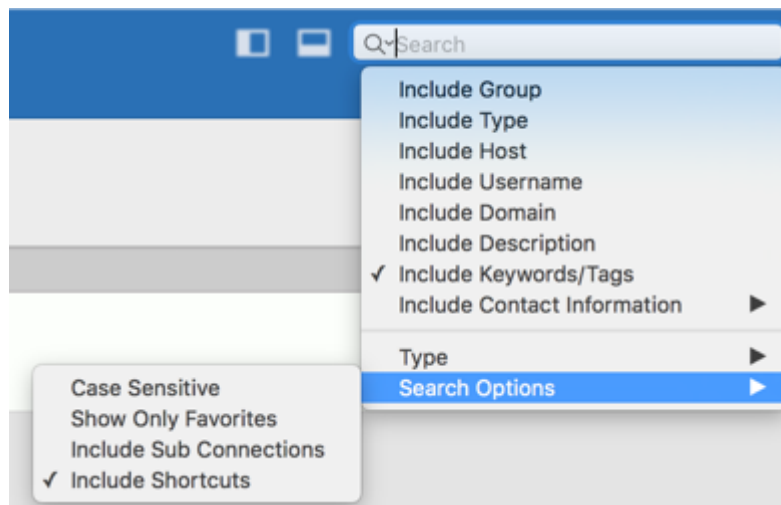
- Session types (credentials, script tools, VPN, etc.)
- If the session is marked as a Favorites

A search by types can be executed to include Sessions, Data Entries, Contacts, Documents, Credentials Entries, VPNs, Macros/Scripts/Tools, Show Sync.



Search - Type

The Search Options will offer you the possibility to include the shortcuts, the sub connections, show only the favorites and/or make the search case sensitive.



Search - Search Options

4.4 Ribbon

DESCRIPTION

Depending on your chosen User Interface style, commands are presented via the **Ribbon** or a standard menu.

RIBBON

The **Ribbon** is composed of multiple tabs, which contains commands, further classified in sections.



Ribbon

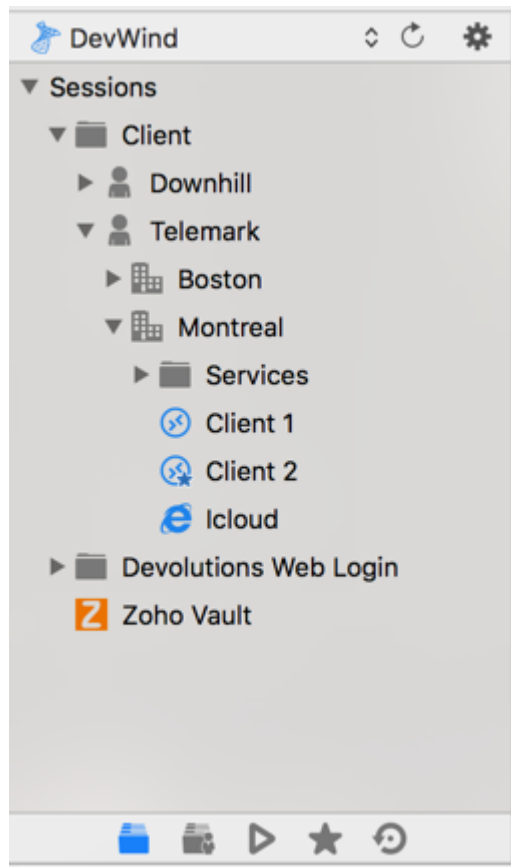
For more information on menu tab please see:

- [File](#)
- [Home](#)
- [Edit](#)
- [View](#)
- [Administration](#)
- [Tools](#)
- [Window](#)
- [Help](#)

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, allows to switch to another data source or repository, and perform actions on entries.



Navigation Pane

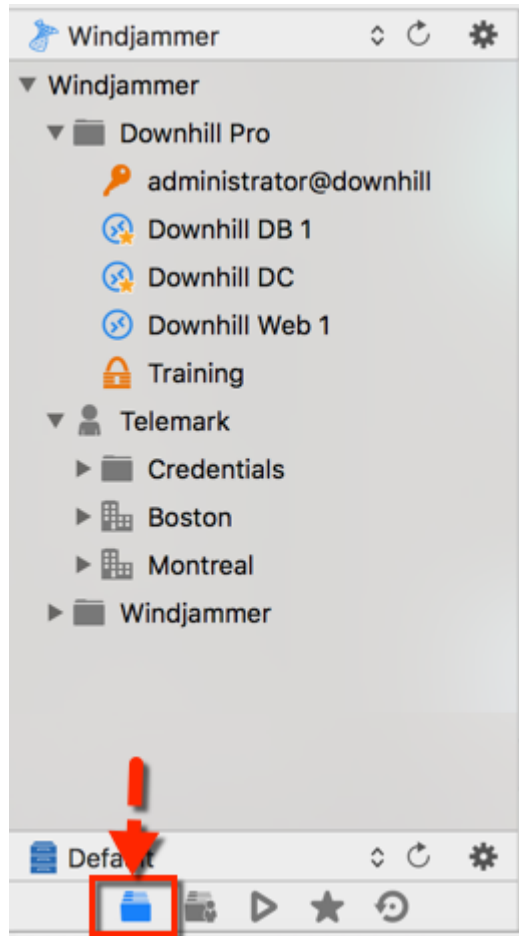
At the bottom of the Navigation Pane you will notice different icons which will open different view/tabs in your Navigation Pane. To learn more about each tab, follow the links below:

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

4.5.1 Vault

DESCRIPTION

The **Vault** lists all the various entries (sessions, information entries, credentials entries, etc) and is the principal way of launching sessions.



Navigation Pane - Vault

4.5.2 My User Vault

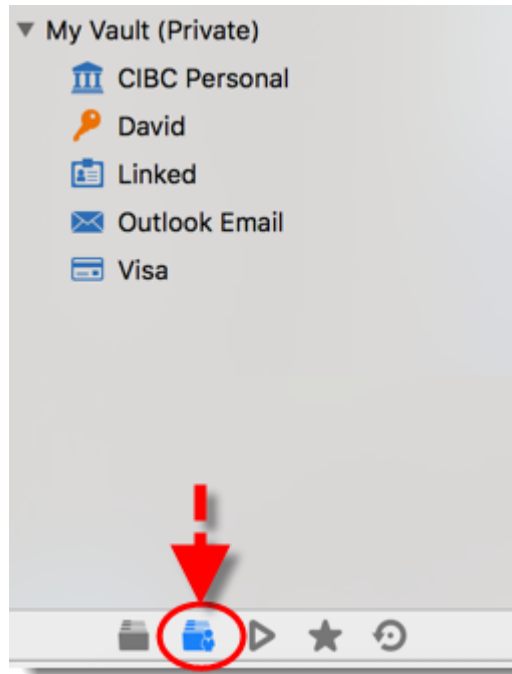
DESCRIPTION

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

To create a new entry in your User Vault, simply click on User Vault in your Navigation Pane and create your new entry directly from there.



The User Vault is only 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 in the **User Vault**.
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 itself, or by using our extension mechanism that is user specific.

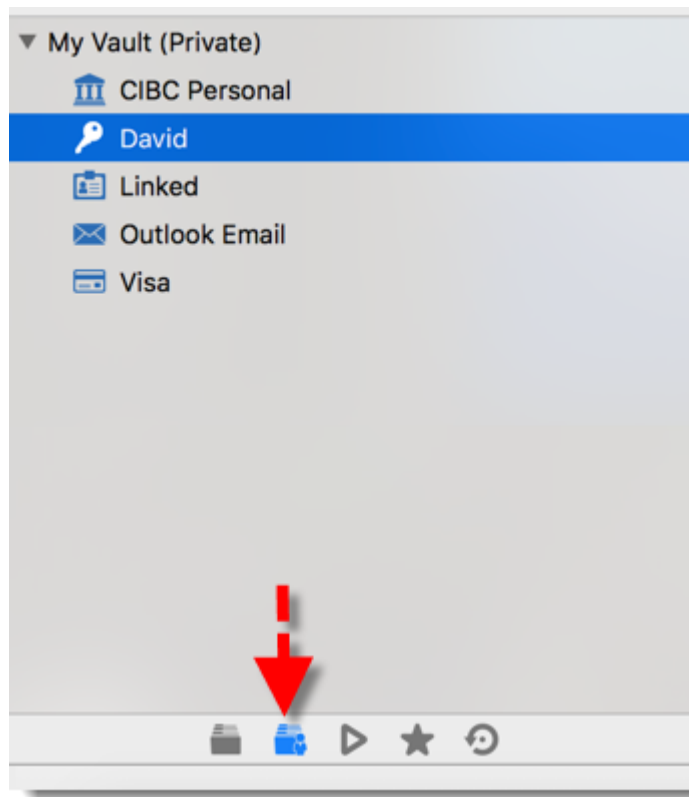
4.5.2.1 User Vault Search

DESCRIPTION

The **User Vault Search** allows to link a User Vault credential entry to a session by providing the name of the credential entry. Once the credential is found it will automatically be used to open your remote session.

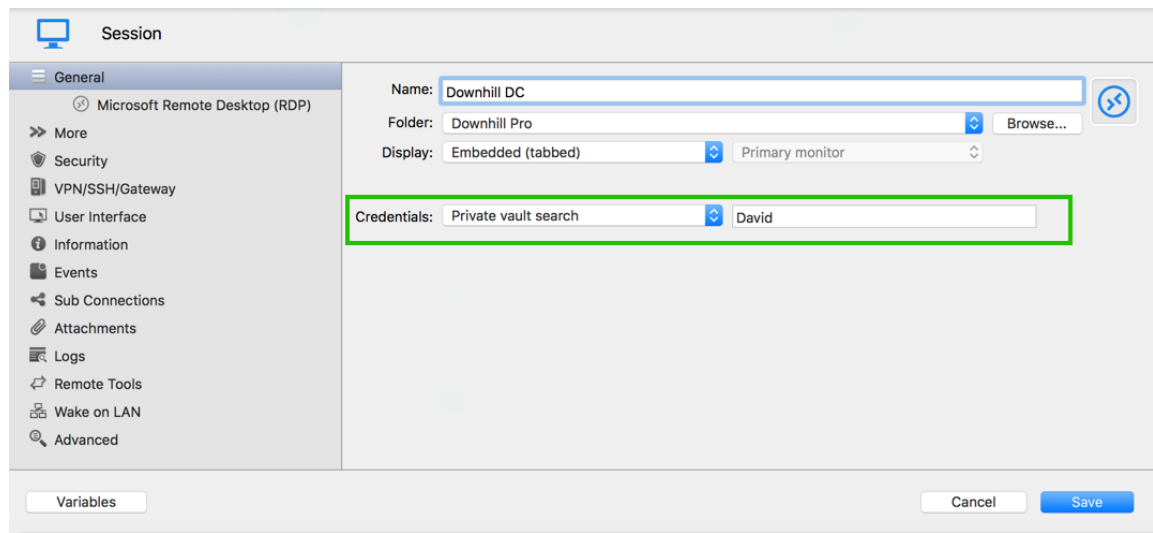
SETTINGS

1. Create a credential entry in the **User Vault**.



User Vault

2. In the remote session, set the Credentials property to User Vault search and enter the exact name of the User Vault credential. The search is not case sensitive, if more than one entry has the same name or if no entry matches the searched name, you will be prompted with a list of all available User Vault credentials. Variables are supported as well.



RDP Session - User Vault Search

3. Open the session as you would normally proceed. Once the credential is found it will automatically be used to open the remote session.



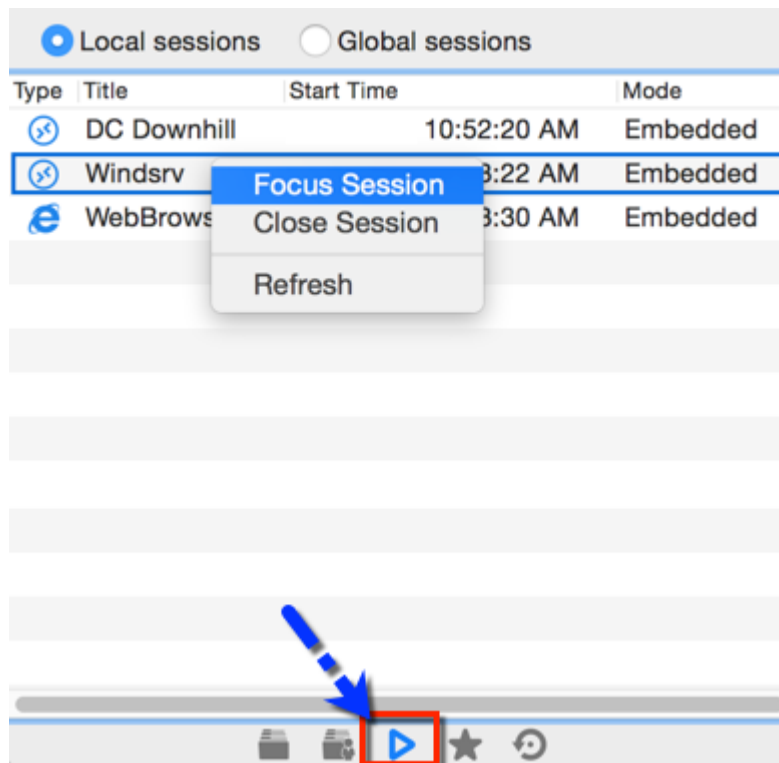
The User Vault is linked to the database user. Another user will never be able to see your User Vault credentials.

4.5.3 Opened Sessions

DESCRIPTION

The **Opened Sessions** shows currently running sessions by type for local machine only. You can focus and bring to front/close any opened session by selecting it from the list. All of the embedded sessions are listed and the external sessions will appear if Remote Desktop Manager for Mac is able to discover the specific type of session.

LOCAL SESSIONS



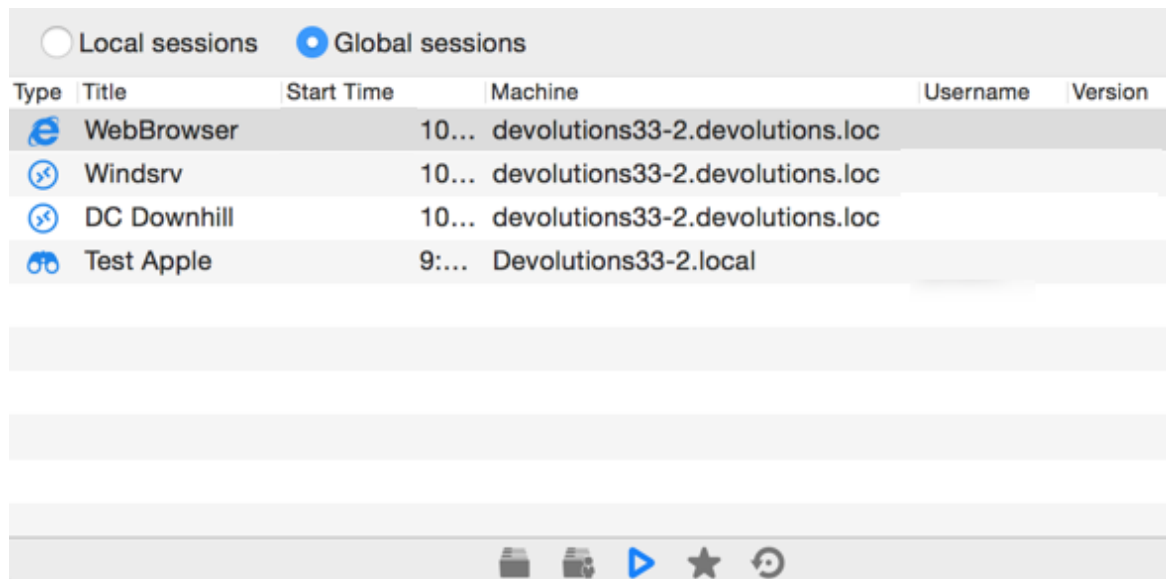
Local opened session view





NOTES

- Remote Desktop Manager for Mac 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 will not appear in the list.

GLOBAL OPENED SESSIONS

With the SQL Server and Remote Desktop Manager for Mac data source you can monitor currently running sessions if they have been opened within Remote Desktop Manager for Mac.



Type	Title	Start Time	Machine	Username	Version
	WebBrowser	10...	devolutions33-2.devolutions.loc		
	Windsrv	10...	devolutions33-2.devolutions.loc		
	DC Downhill	10...	devolutions33-2.devolutions.loc		
	Test Apple	9:...	Devolutions33-2.local		

Global opened session view

For many reasons beyond our control, it's possible for a session to be terminated without Remote Desktop Manager for Mac knowing that this has taken place. This can happen, for example, if Remote Desktop Manager for Mac 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.

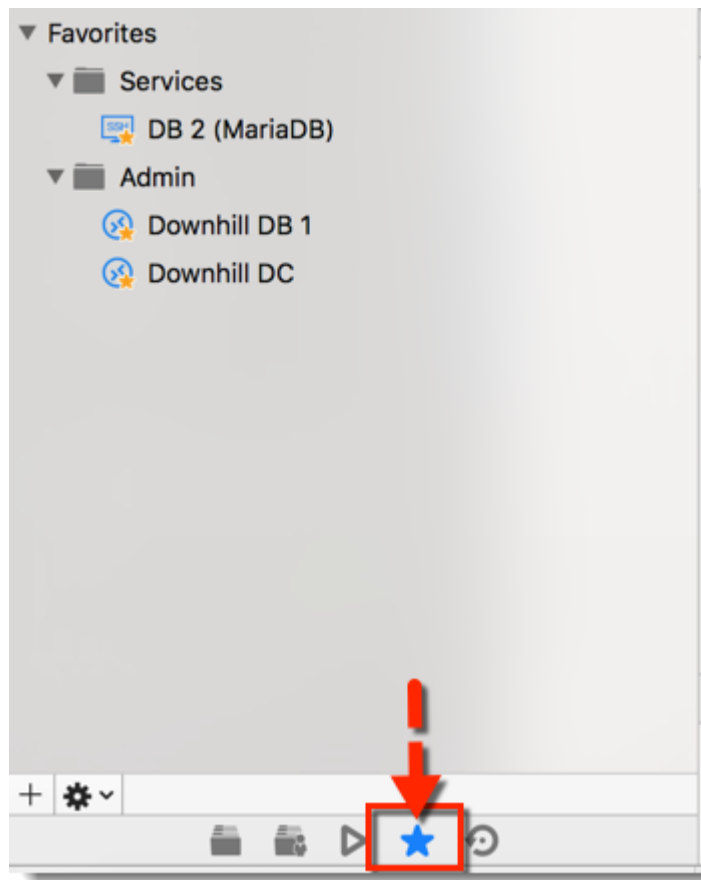
To review a detailed log, double click on a session entry.

4.5.4 Favorite Entries

DESCRIPTION

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

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

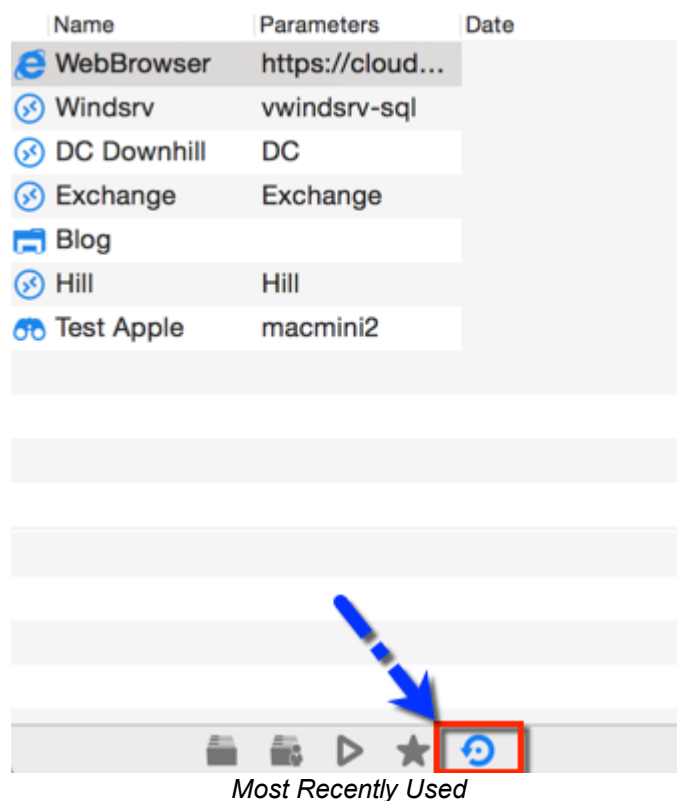


Favorites Tab

4.5.5 Most Recently Used Entries

DESCRIPTION

This tab show the most recently used sessions for a specific data source on the local computer.



By default, 10 items will be kept in the most recently used entries history.

4.6 Content Area

DESCRIPTION

The **Content Area** contains the various dashboards to manage Remote Desktop Manager for Mac as well as embedded sessions. There is a single dashboard active at a time depending on the currently selected node in the navigation pane.

Existing dashboards are described further in their own help topics:

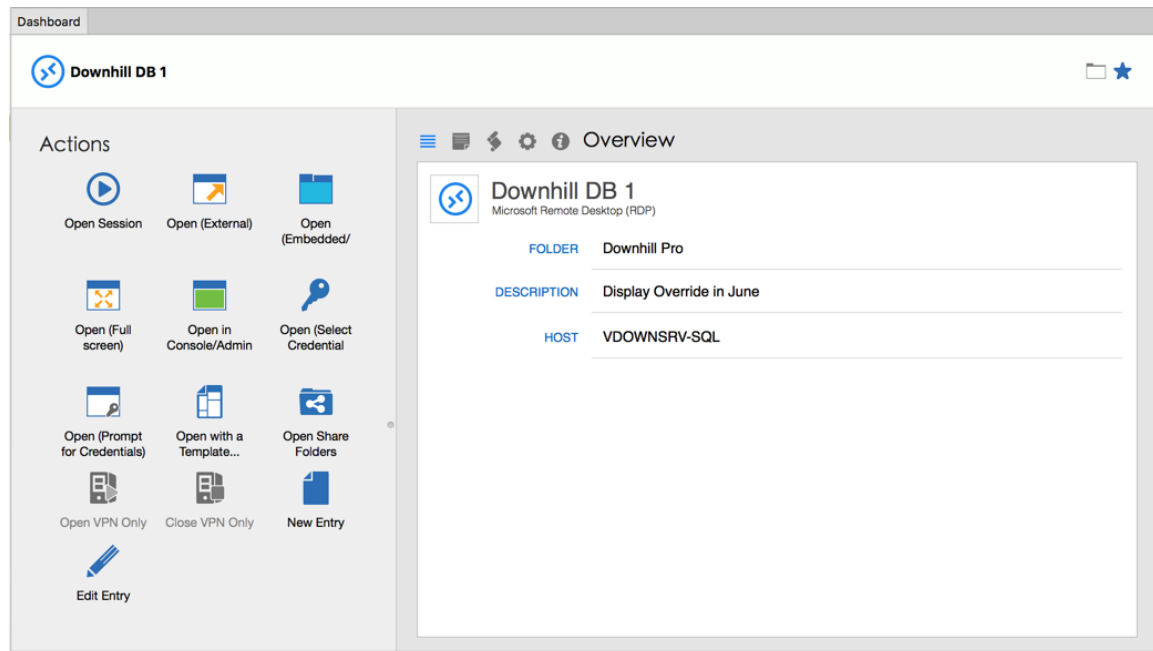
- [Sessions](#)
- [Information Entries](#)
- [Groups](#)
- [Credentials](#)

- [Macros/Scripts/Tools](#)

4.6.1 Dashboard

DESCRIPTION

The **Dashboard** displays commands and information related to the selected entry. The dashboard is context sensitive and its content depends on the type of the selected entry.



Dashboard for credential entry

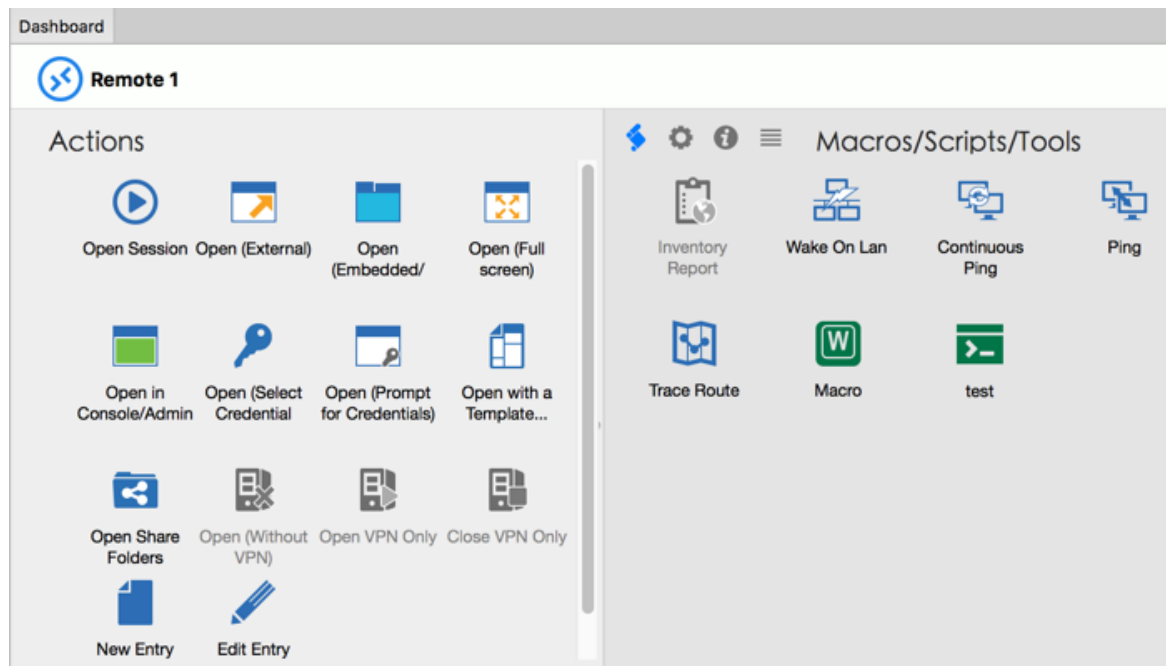
For more information about the dashboard of a specific type of entry, please consult the following topics:

- [Sessions](#)
- [Information entries](#)
- [GroupsFolders](#)
- [Credentials](#)

4.6.1.1 Session

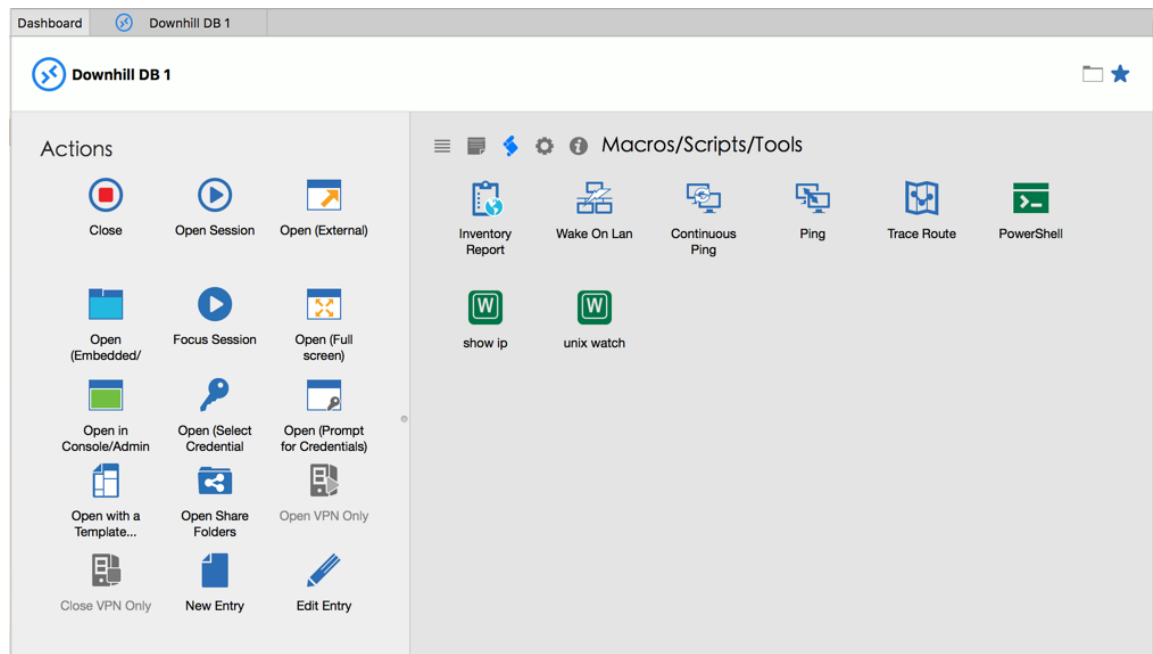
DESCRIPTION

The dashboard displays a quick view showing possible actions, or information for the selected entry. It contains the same actions that are found in the context menu and the ribbon.



Dashboard of a selected session

Once your session is open you will see that the **Actions** in the **Dashboard** will change.

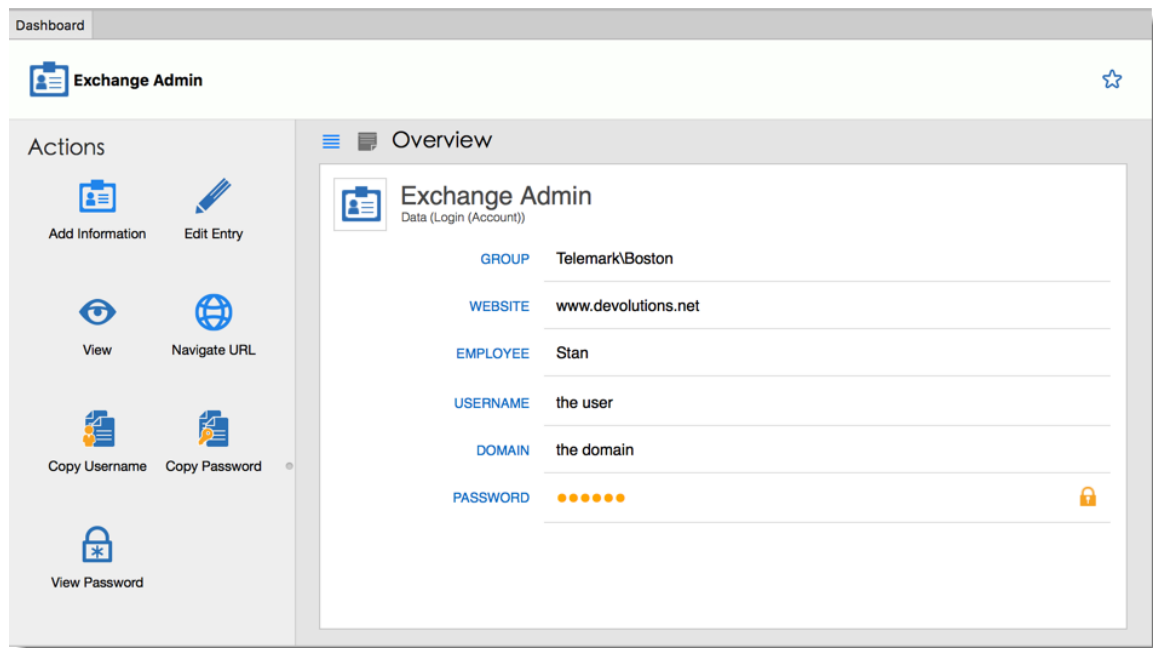


Dashboard for an open session

4.6.1.2 Information

DESCRIPTION

The dashboard displays a quick view showing possible actions and information for the currently selected information entry. It contains the same actions that are found in the context menu and the ribbon.

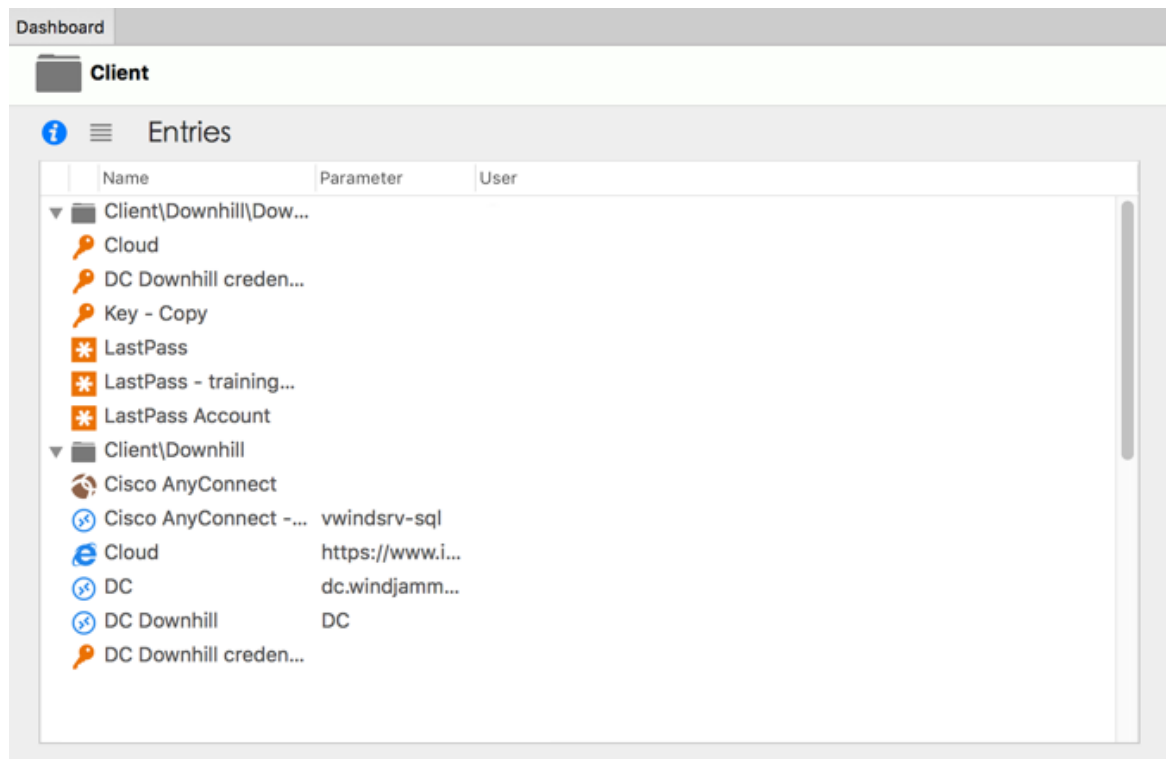


Dashboard for a selected information entry

4.6.1.3 Folder

DESCRIPTION

The dashboard displays the folder's entries. It's possible to display the group details directly or only the information regarding the selected entry in the dashboard.

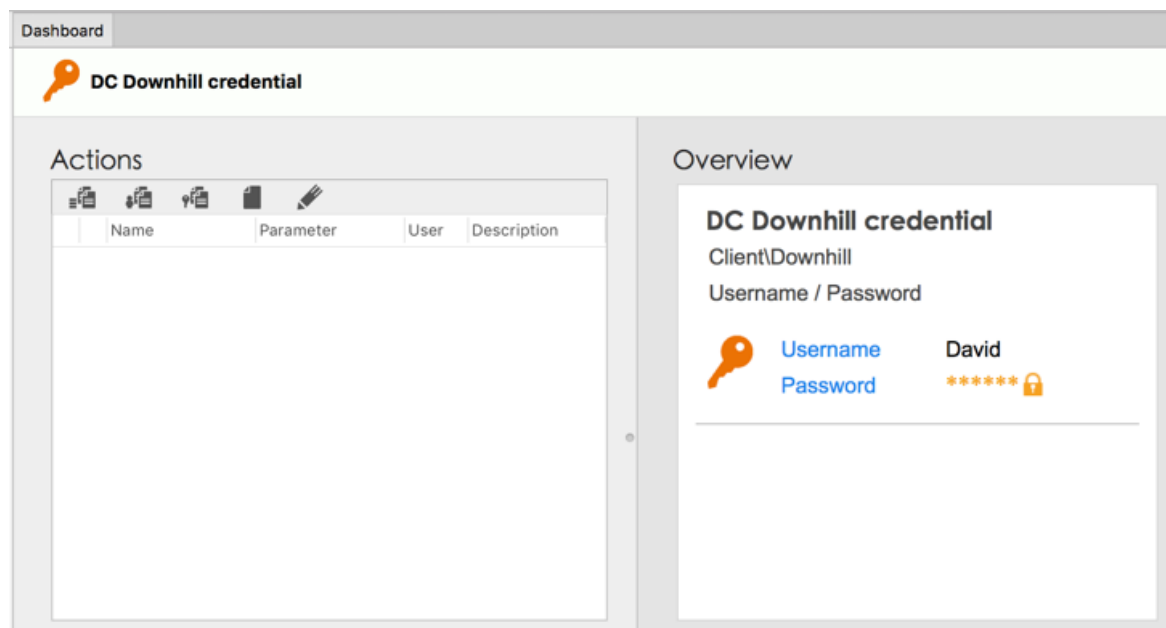


Dashboard of a selected Group folder

4.6.1.4 Credentials

DESCRIPTION

The dashboard displays a quick view showing possible actions or information for the current credential entry. It's possible to easily view which entries use the current credential entry.

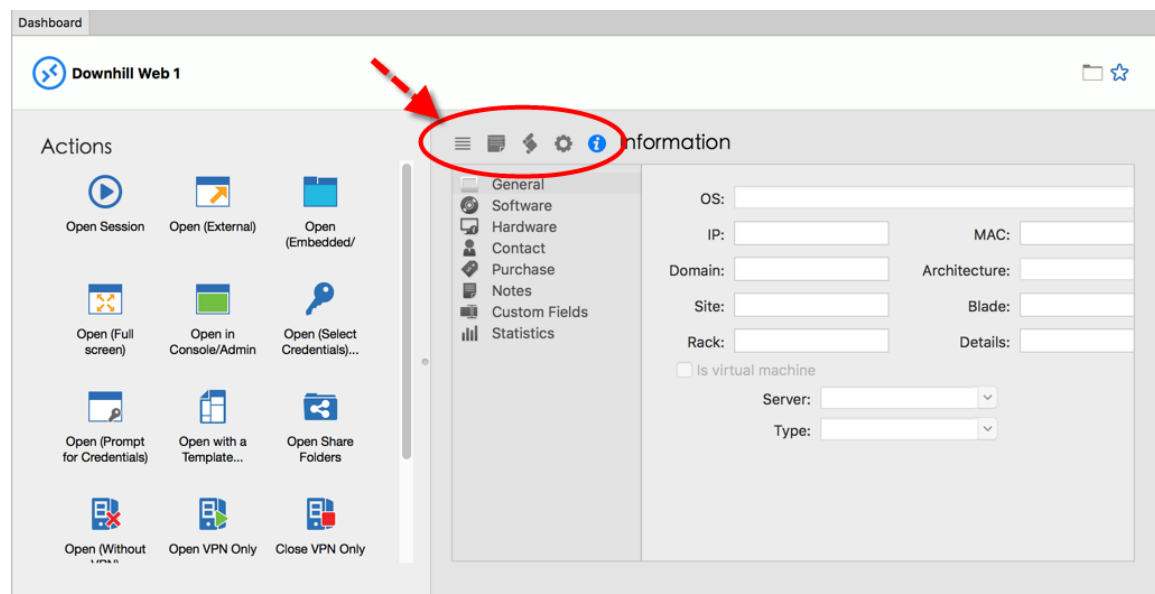


Dashboard of a selected credential

4.6.1.5 Dashboard tabs

DESCRIPTION

The Dashboard tabs allows you to quickly view information directly in your Dashboard regarding your selected entry. The available Dashboard tabs depends on the type of entry that is selected.



Dashboard tabs

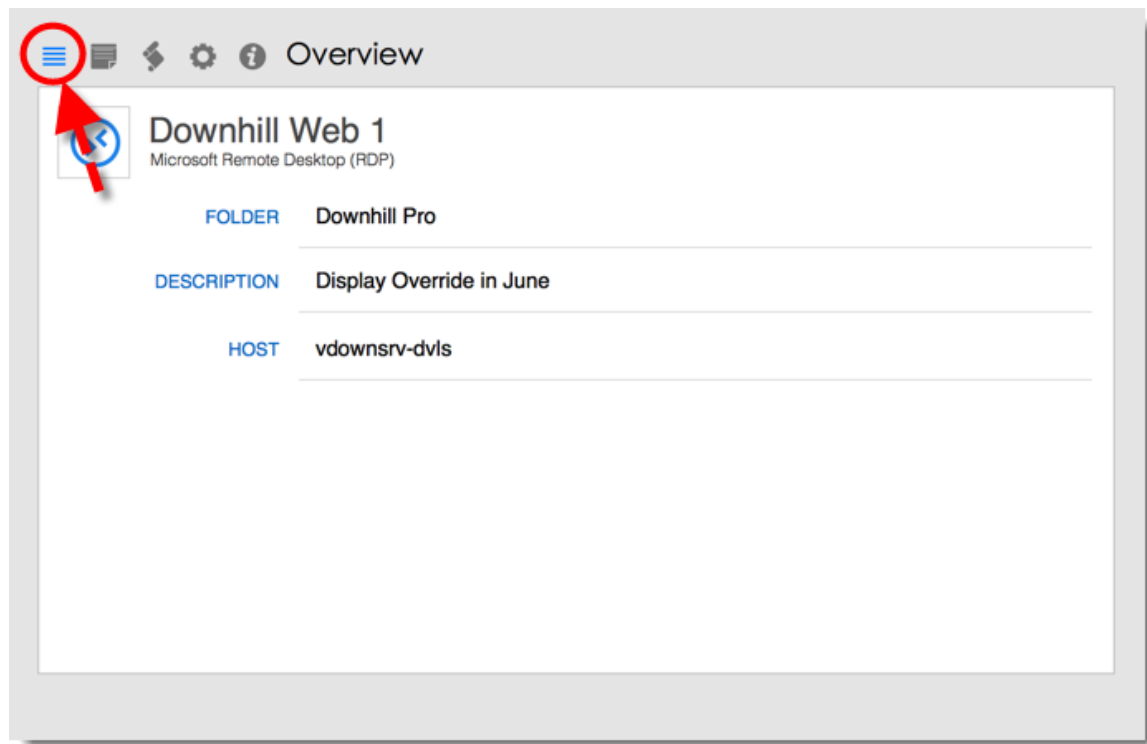
For more information on the Dashboard tabs please see:

- Overview
- Documentation
- Macros/Script/Tools
- Remote Tools
- Information

4.6.1.5.1 Overview

DESCRIPTION

The **Overview** tab displays information related to your selected entry directly in your dashboard. The information it displays depends on the type of entry that is selected.



Dashboard tabs - Overview

4.6.1.5.2 Documentation

DESCRIPTION

The **Documentation** tab allows to store 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.

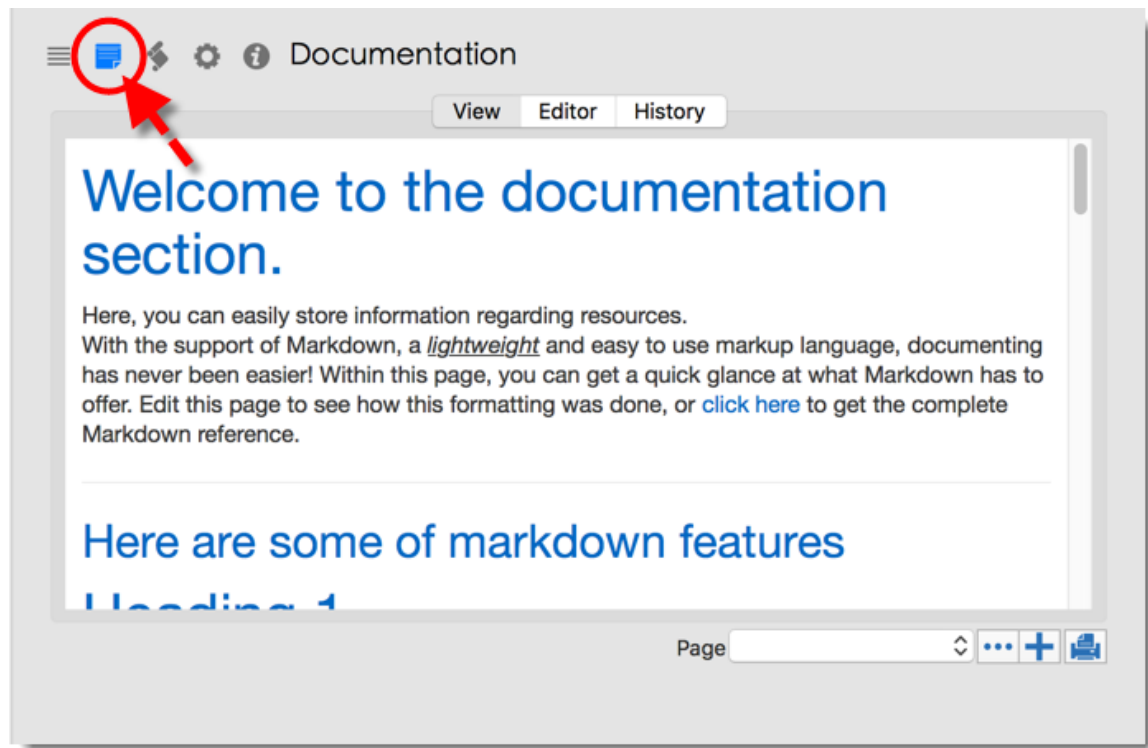


The **Documentation** feature is encrypted **only** for the data source Devolutions Server. If you are using data sources like SQL Server or Azure SQL, the **Documentation** feature is **not** encrypted.



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

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



Dashboard tabs - Documentation

4.6.1.5.3 Macros/Scripts/Tools

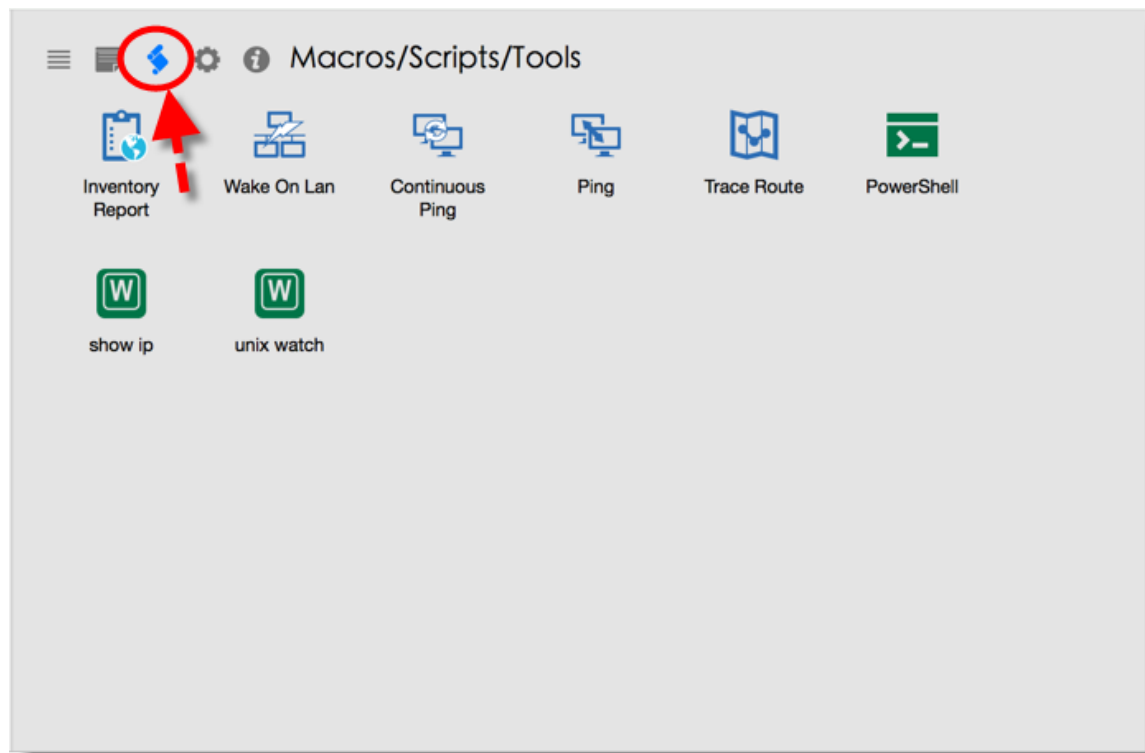
DESCRIPTION

Session tools are available in the dashboard tabs and in the session context menu **Macros/Scripts/Tools**.

SETTINGS

There are three types of tools:

- Build in tools
- Add-on session tools
- Session script tools



Dashboard tabs - Macros/Scripts/Tools

BUILT-IN TOOLS

These tools are implemented directly in Remote Desktop Manager and are available without any installation or special configuration.

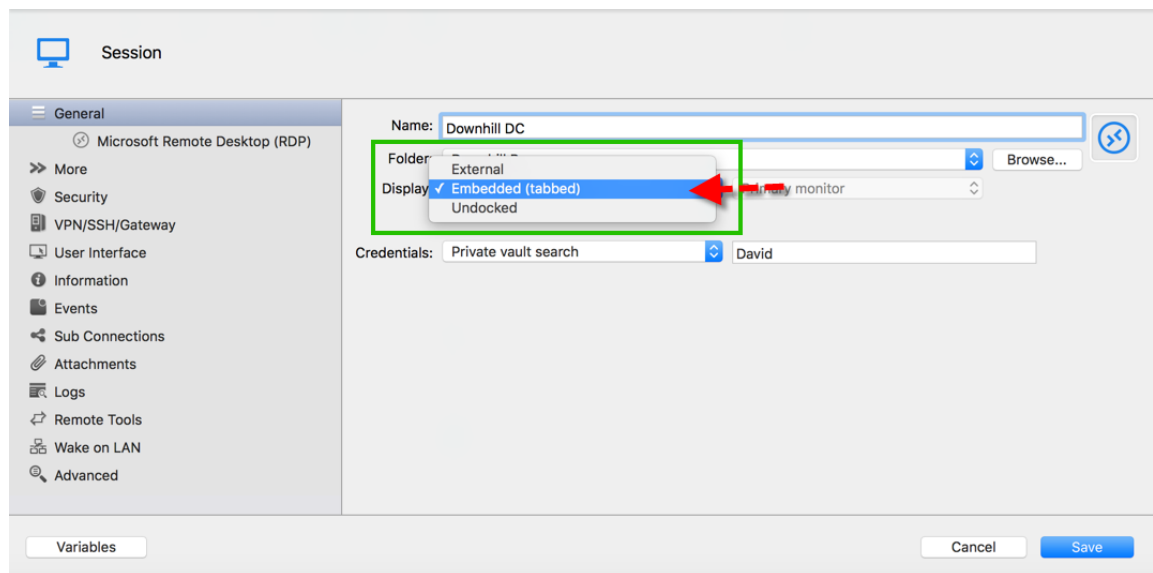
OPTION	DESCRIPTION
Inventory Report	Open a Inventory Report for a remote machine.
Wake On Lan	Sends the magic packet command for the Wake-on-Lan.
Continuous Ping	Opens the ping dialog of the selected host and performs a continuous ping.
Ping	Opens the ping dialog of the selected entry and displays the result.

OPTION	DESCRIPTION
Trace Route	Display the route and measuring transit delays of packets across a network.

4.6.2 Embedded Sessions

DESCRIPTION

The **Embedded** 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**.



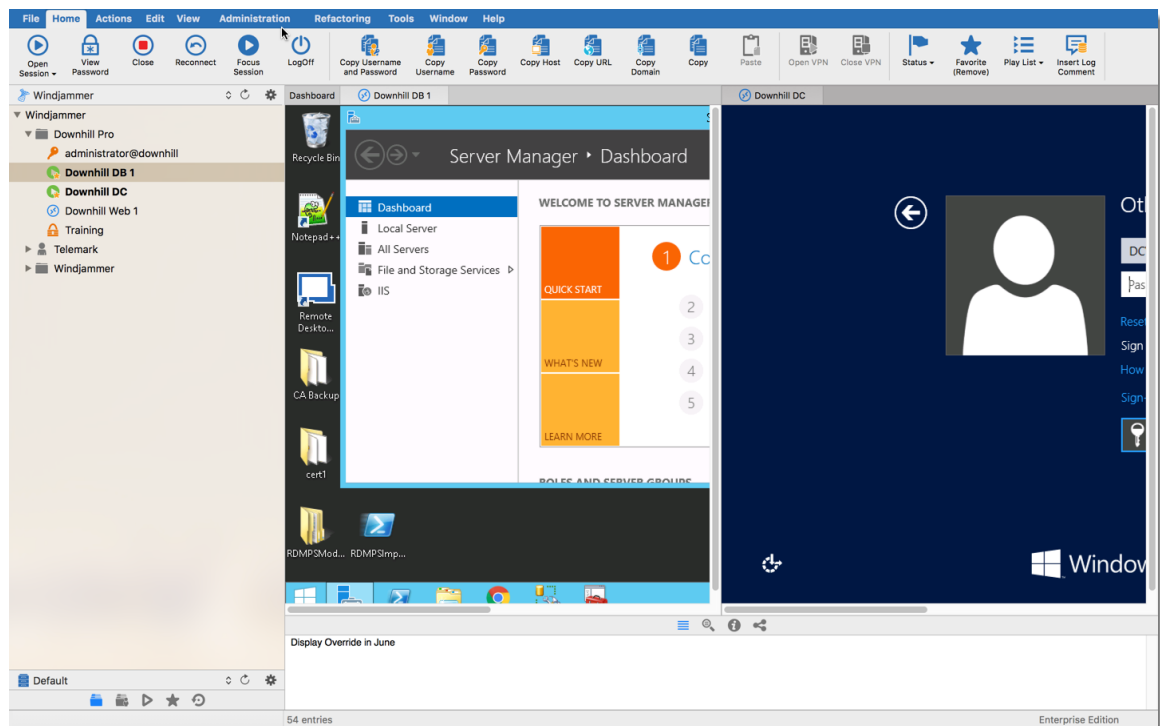
Display Mode Settings

The embedded display mode allows you as well to split the dashboard in order to display multiple sessions at once. For more information please consult our [Split View](#) topic.

4.6.2.1 Split Windows

DESCRIPTION

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 on the top, bottom, left or right of the adjacent tab.

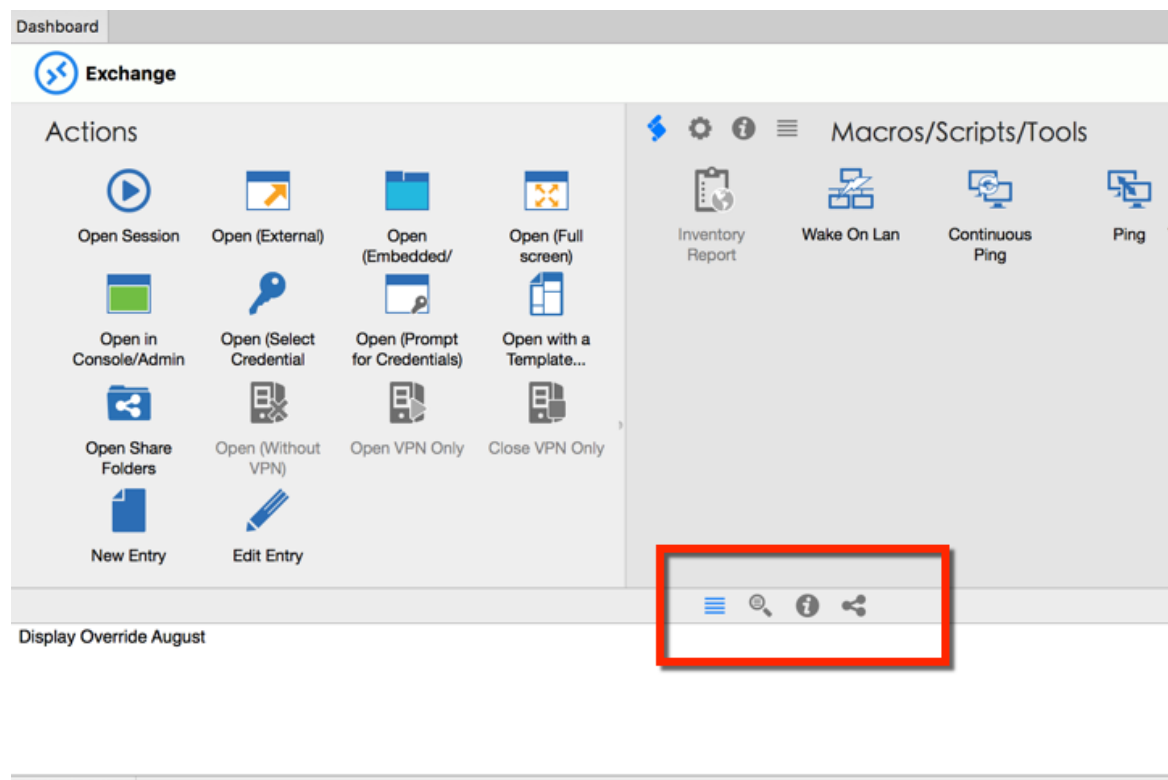


Split Window - Drag and Drop

4.7 Panes (Footer)

DESCRIPTION

The Footer section display various panes that are provided with Remote Desktop Manager for Mac.



Footer options

Please consult the following topics for more information:

- [Description](#)
- [Information](#)
- [Sub Connections](#)

4.7.1 Description

DESCRIPTION

The **Description** pane displays the content of the Description field of the entry. Enable the description pane by selecting **View - Footer - Description** in the ribbon.

*Footer - Description*

4.7.2 Information

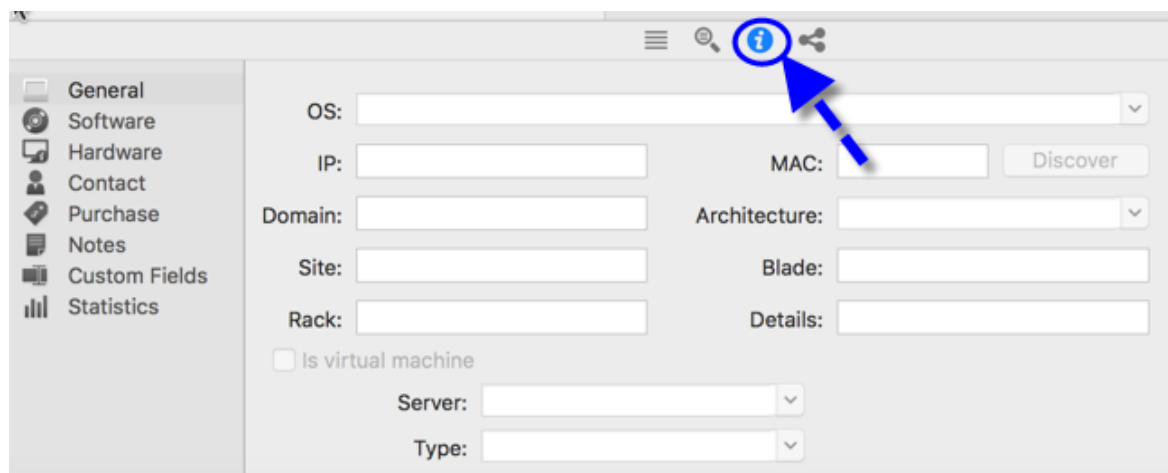
DESCRIPTION

The **Information** footer pane contains a wide assortment of information on the entry. Some purely informative and some of operational nature. It contains multiple tabs in order to present as much information as possible.

SETTINGS

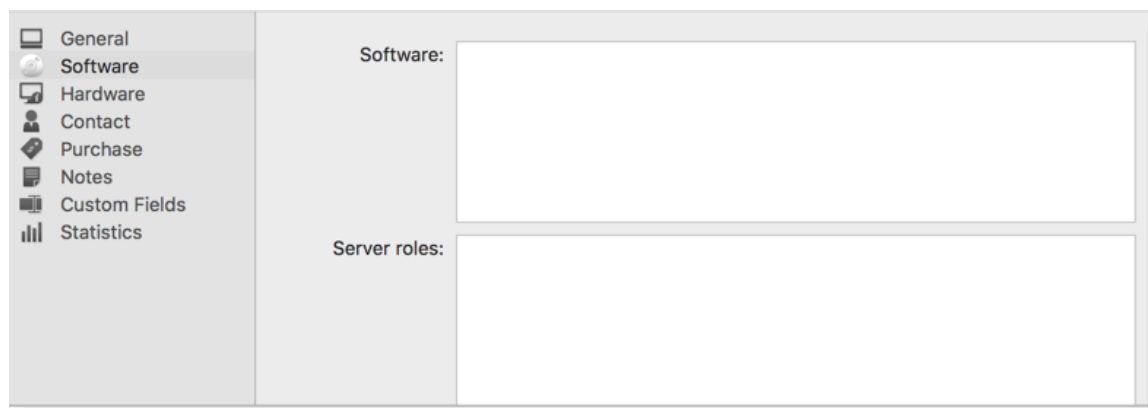
GENERAL

The **General** tab allows you to specify the computer specific information such as operating system, MAC address and the hardware description. For more information please consult General topic.

*Footer - Information*

SOFTWARE

The **Software** tab allows you to list all software installed on the remote computer. For more information please consult Software topic.

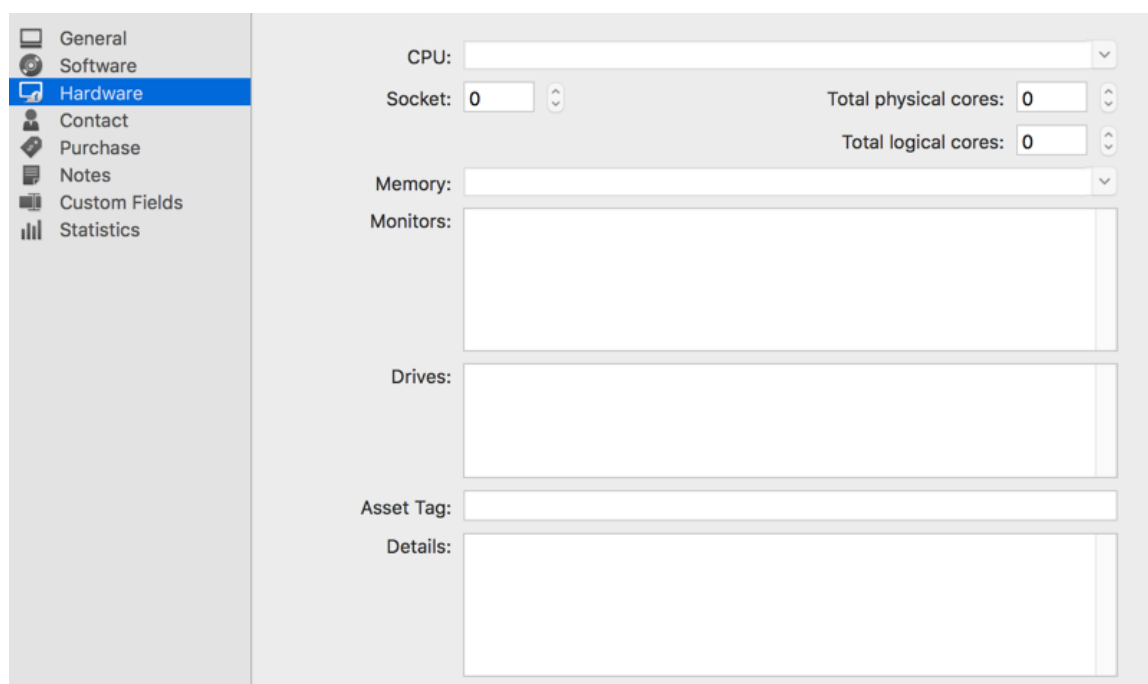


The screenshot shows the 'Software' tab selected in the left sidebar. The main area contains two large, empty text input fields. The top field is labeled 'Software:' and the bottom field is labeled 'Server roles:'.

Information - Software

HARDWARE

The **Hardware** tab allows you to specify the hardware information of the remote computer. For more information please consult Hardware topic.



The screenshot shows the 'Hardware' tab selected in the left sidebar. The main area contains several input fields for hardware specifications:

- CPU: A dropdown menu.
- Socket: A numeric input field with a value of 0 and a small up/down arrow.
- Total physical cores: A numeric input field with a value of 0 and a small up/down arrow.
- Total logical cores: A numeric input field with a value of 0 and a small up/down arrow.
- Memory: A dropdown menu.
- Monitors: A large, empty text input field.
- Drives: A large, empty text input field.
- Asset Tag: A text input field.
- Details: A large, empty text input field.

Information - Hardware

CONTACT

The **Contact** tab displays information on a person that has a link to the entry. It could be the technician managing the remote machine. For more information please consult Contact topic.

The screenshot shows a web application interface for managing contacts. On the left is a vertical sidebar with a menu containing the following items: General, Software, Hardware, **Contact** (highlighted with a blue bar), Purchase, Notes, Custom Fields, and Statistics. The main content area is titled 'Contact: Default' and contains a form with the following fields and controls:

- First name:** text input field
- Last name:** text input field
- Middle name:** text input field
- Prefix:** dropdown menu
- Gender:** dropdown menu (currently set to 'Unspecified')
- Job title:** text input field
- Credentials:** button
- Customer #:** text input field
- Company:** text input field
- Address:** text input field
- City:** text input field
- State:** text input field
- Zip code:** text input field
- Country:** dropdown menu with a location pin icon
- Email:** text input field with an envelope icon
- Home phone:** text input field
- Work phone:** text input field
- Mobile:** text input field
- Fax:** text input field
- Skype:** text input field with a Skype icon
- Website:** text input field with a globe icon

Information - Contact

PURCHASE

The **Purchase** tab allows you to enter information related to the invoice or the purchase of the equipment. For more information please consult Purchase topic.

Information - Purchase

NOTES

The **Notes** tab contains only one control. A text area where you can enter any information you require.

Information - Notes

CUSTOM FIELDS

The **Custom** tab contain five custom fields. The reason behind having discrete fields is that they are available via Field Variables and can therefore be accessed in sub connections while being defined in the parent connection (see Sub Connections Overview).

The screenshot shows a sidebar on the left with the following menu items: General, Software, Hardware, Contact, Purchase, Notes, Custom Fields (highlighted), and Statistics. The main area displays five 'Custom' fields. The first field is a text input containing '.....' with a checkmark icon to its right. The second, third, and fourth fields are empty text inputs, each with a checkbox icon to its right. The fifth field is a larger, empty text area.

Information - Custom Fields

STATISTICS

The Statistic tab simply displays some information on the creation and last modification of the entry. For more information please consult the Statistic topic.

The screenshot shows the same sidebar as the previous image, with 'Statistics' highlighted. The main area displays the following information:

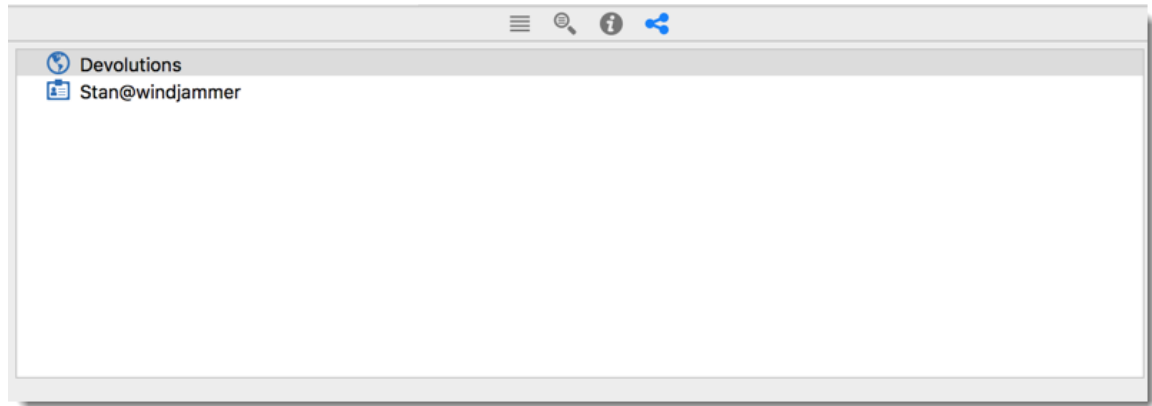
- Created by:
- Creation date:
- Last update by:
- Last update date:

Information - Statistics

4.7.3 Sub Connections

DESCRIPTION

The **Sub Connections** footer pane is used when having define sub connections for your current entry.

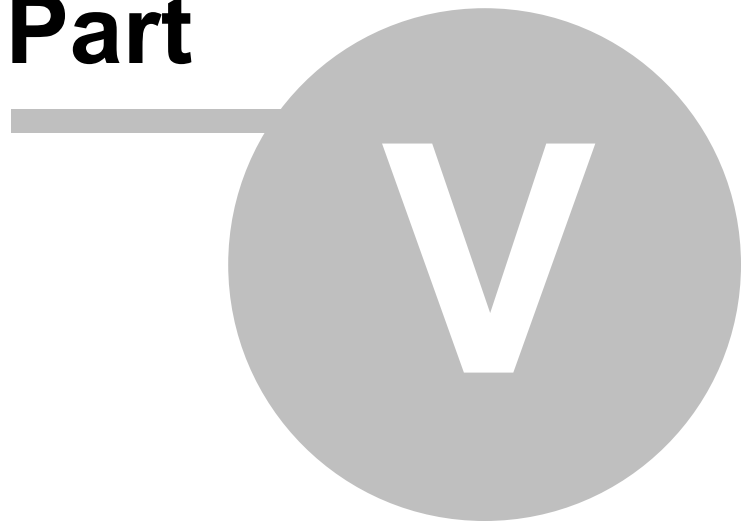


Footer - Sub Connections

Please refer to the Sub Connections topic for more information.

Data Sources

Part



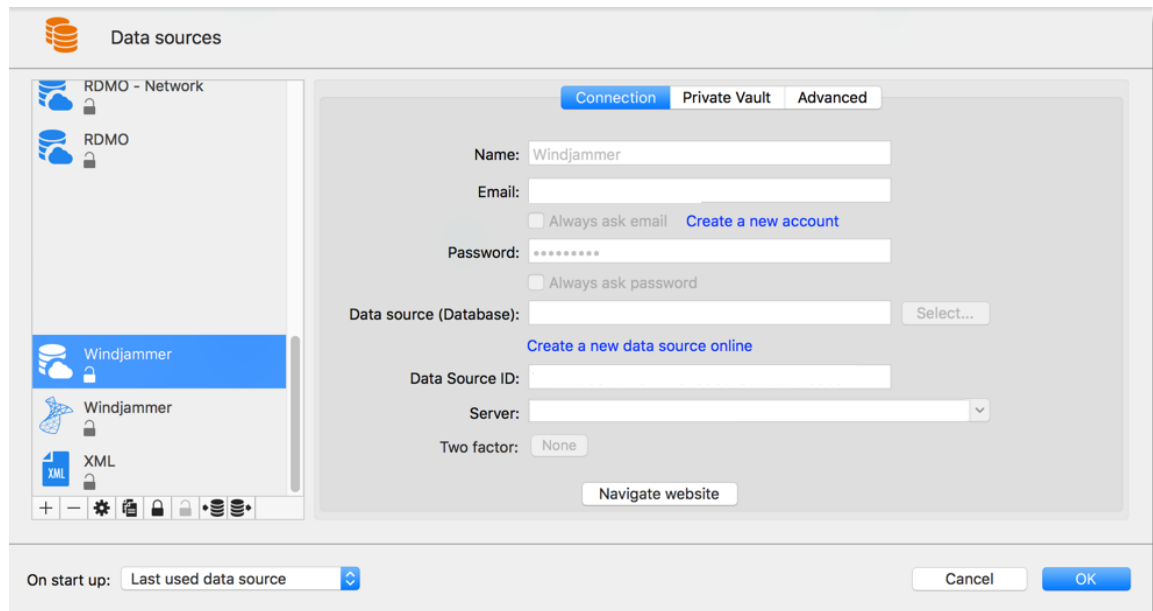
5 Data Sources

DESCRIPTION

The data source is at the heart of Remote Desktop Manager for Mac, it is the container that holds all of your entries.

SETTINGS

The data source can be a file or a database and you use multiple data sources at the time, as seen below. They need to be configured on all workstations.



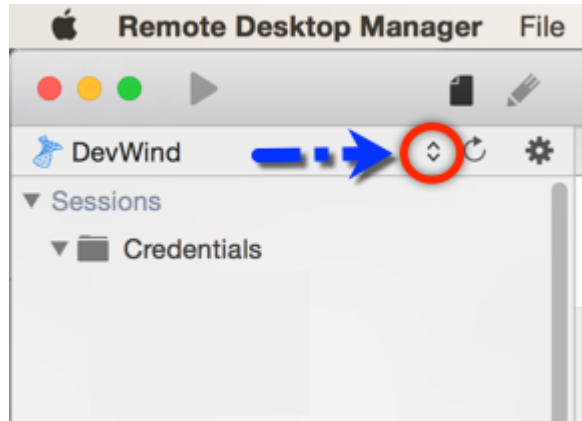
Data Sources

CREATE A NEW DATA SOURCE

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

MULTIPLE DATA SOURCES

You can configure multiple data sources within the application. These data sources can be of mixed types but there is only one active at a time. It is possible to switch from one data source to another via the data source combo box.



Choose your current data source

OPEN DATA SOURCE AT STARTUP

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

OPTION	DESCRIPTION
Use default data source	Set the data source that you always want to open at start up.
Last used data source	Open with the last used data source.
Prompt for data source	A message box will open on startup for the data source selection.

DATA SOURCE SETTINGS

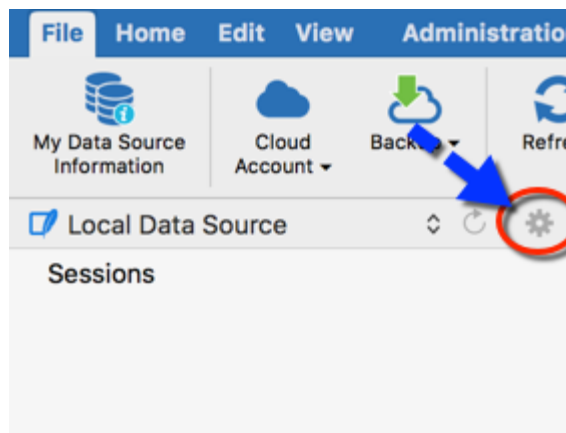
The [Advanced Data Sources](#) can contain specific settings or global policies. Those settings are saved directly in the database, see Data Source Settings topic for more information.

5.1 Create a New Data Source

DESCRIPTION

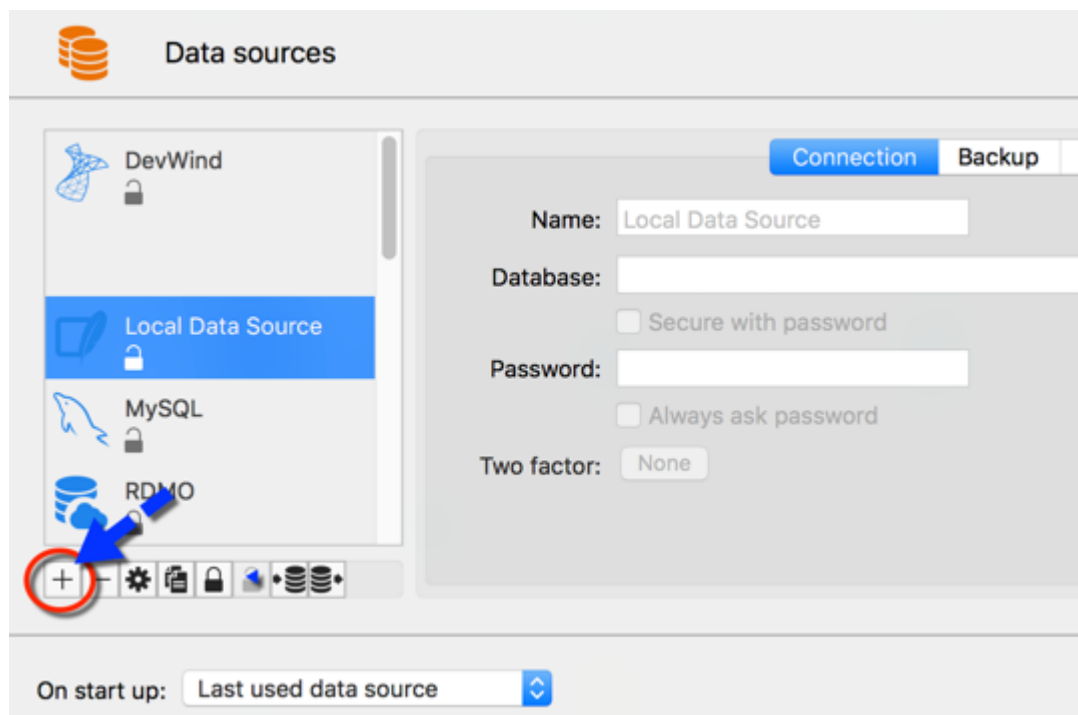
CREATE A NEW DATA SOURCE

1. To create a new data source click on the **setting** button next to the data source box.



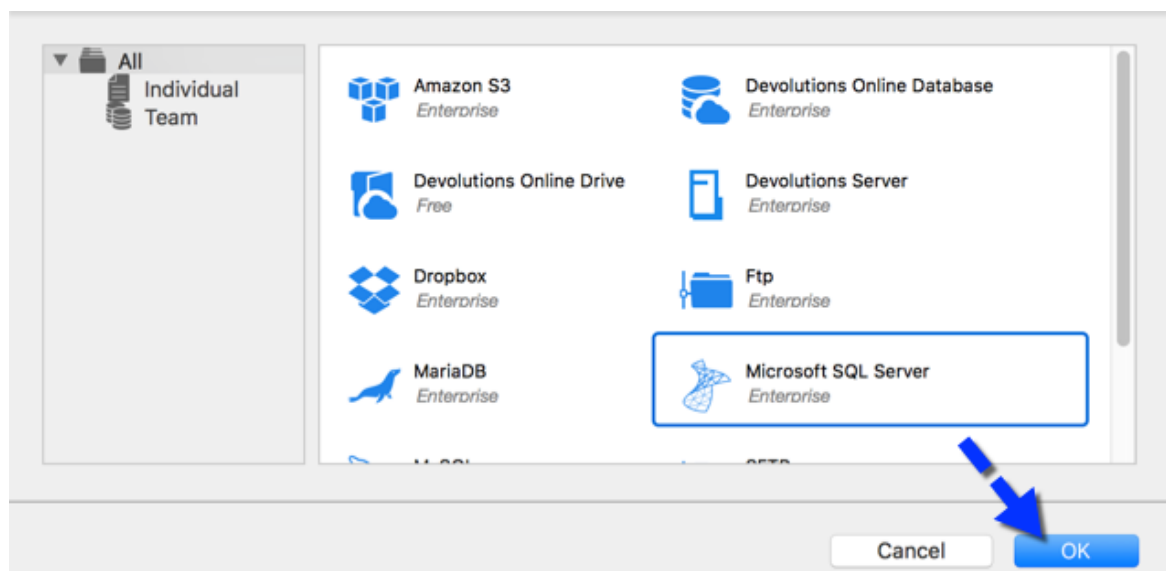
Data Source Setting button

2. Click on the **plus** to create a new data source.



Create a new data source

3. Select the [data source type](#) you wish to create and click on **OK**.



Select your data source type

4. Configure all your connection settings. You can verify the validity of the information entered by using **Test Server** or **Test Credentials** (depending on the type of data source you are creating).

The screenshot shows the 'Connection' tab for an SQL Server. The 'Name' field contains 'DevWind'. The 'Server' dropdown is set to 'SQL Server'. The 'Database login' dropdown is selected. The 'User' field is empty, and the 'Domain' field is empty. The 'Save password' checkbox is checked. The 'Password' field is masked with dots. The 'Database' field is empty, and the 'Browse...' button is visible. The 'Two factor' dropdown is set to 'None'. The 'Test Server' button is circled in red, and the 'Test Database' button is below it. The 'Cancel' and 'OK' buttons are at the bottom right.

SQL Server - Connection tab

5. If using an existing Database, click on the **ellipsis** next to **Database** to select your database and then click on **Test Database** to verify it's working properly.

The screenshot shows the 'Connection' tab of a dialog box for connecting to a SQL Server. The 'Name' field is set to 'DevWind'. The 'Server' field is empty, with a hint '(Local) or IP or Server name'. The 'Database login' dropdown is set to 'Database login'. The 'User' field is empty, and the 'Domain' field is also empty. The 'Save password' checkbox is checked. The 'Password' field is masked with dots. The 'Database' field is empty, and the 'Browse...' button next to it is circled in red. The 'Two factor' dropdown is set to 'None'. At the bottom, there are 'Test Server' and 'Test Database' buttons, and 'Cancel' and 'OK' buttons.

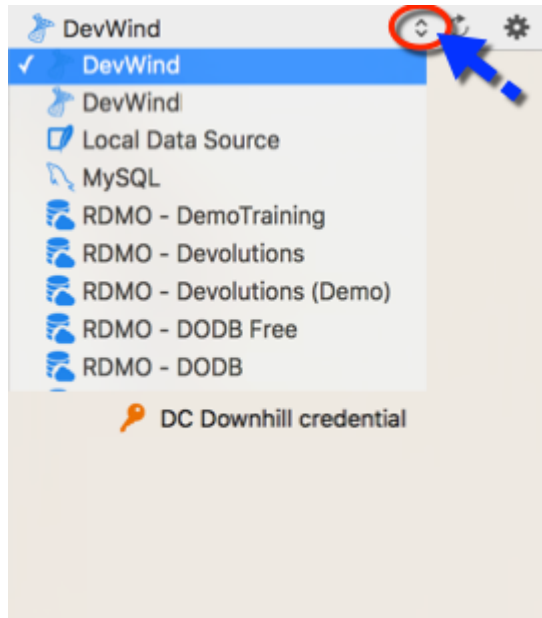
SQL Server - Connection tab - Browse

6. If you wish to create a new Database, click on the **Upgrade** tab and then select **Create Database**.

The screenshot shows the 'Upgrade' tab of a dialog box. The 'Test Server' button is at the top. Below it, the 'Create Database' button is circled in red, and a blue dashed arrow points to it. Below 'Create Database' are the 'Update Database', 'Test Database', and 'View upgrade script...' buttons. At the bottom, there is an ID field with the value '50B4660D-55ED-49D2-96E1-98B37CEC6030' and 'Cancel' and 'OK' buttons.

Upgrade tab - Create Database

7. Once you have completed all the steps, you can select your newly created data source by clicking on the arrow next to the data source combo box.



Select your active data source

5.2 Data Source Types



DESCRIPTION



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







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


DATA SOURCE TYPES

NAME	DESCRIPTION	PROS AND CONS
Devolutions Online Drive 	<p>Remote Desktop Manager for Mac uses Devolutions Online Drive to store and synchronize your sessions. Access your sessions from anywhere using an Internet connection.</p> <p>For more information, please consult our Online Drive topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Quick. • Reliable. • Free service. <p>Cons:</p> <ul style="list-style-type: none"> • No possibility for sharing. • No security management.
Devolutions Server 	<p>Remote Desktop Manager for Mac uses Devolutions Server to store session information.</p> <p>For more information, please consult our Devolutions Server topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Quick. • Reliable. • Secure. • Supports all features, such as attachments, Usage Logs, Offline Mode and User Management. • Active Directory integration. <p>Cons:</p> <ul style="list-style-type: none"> • Installation required.
Dropbox	<p>Remote Desktop Manager for Mac uses the Dropbox API to retrieve the XML file from the configured repository.</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Can be shared in read-only mode.

NAME	DESCRIPTION	PROS AND CONS
	<p>For more information, please consult our Dropbox topic.</p>	<ul style="list-style-type: none"> • Backups (by Dropbox) are automatic. • Storage infrastructure is free (if within your free storage quota). <p>Cons:</p> <ul style="list-style-type: none"> • No security management. • There is a possibility for conflict or data corruption to occur. • Does not support all features, such as attachments, Usage Logs, Offline Mode and User Management. • Dropbox integration uses the Dropbox SDK, so features exclusive to the Business or Enterprise editions are NOT supported.
<p>Microsoft Azure SQL</p> 	<p>Remote Desktop Manager for Mac uses the Microsoft cloud platform to save and manage all sessions.</p> <p>For more information, please consult our Azure SQL topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Quick. • Reliable. • Secure. • Supports all features, such as attachments, Usage Logs, Offline Mode and User Management.

NAME	DESCRIPTION	PROS AND CONS
		<p>Cons:</p> <ul style="list-style-type: none"> • Microsoft Azure needs to be configured.
Microsoft SQL Server 	<p>Remote Desktop Manager for Mac 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 SQL Server (MSSQL) topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Quick. • Reliable. • Secure. • Supports all features, such as attachments, Usage Logs, Offline Mode and User Management. • SQLServer Express is free. <p>Cons:</p> <ul style="list-style-type: none"> • SQLServer must be installed.
Devolutions Password Hub Business 	<p>Remote Desktop Manager for Mac 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 products features and highlights and consult our Password Hub Business topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Quick. • Reliable. • Secure. • Shareable. <p>Cons:</p>

NAME	DESCRIPTION	PROS AND CONS
		<ul style="list-style-type: none"> • Cannot be hosted on premises. • No offline mode.
Devolutions Password Hub Personal 	<p>Remote Desktop Manager for Mac uses Devolutions Password Hub Personal to store and synchronize your sessions. Access your sessions from anywhere using an Internet connection.</p> <p>For more information, please consult our Password Hub Personal topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Quick. • Reliable. • Free service. <p>Cons:</p> <ul style="list-style-type: none"> • No possibility for sharing. • No offline mode.
SQLite 	<p>Remote Desktop Manager for Mac uses a SQLite database to store session information.</p> <p>For more information, please consult our SQLite topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Quick. • Reliable. • Free database. • Supports all features, such as attachments and Usage Logs, Offline Mode and User Management. <p>Cons:</p> <ul style="list-style-type: none"> • No possibility for sharing. • No security management.

NAME	DESCRIPTION	PROS AND CONS
XML 	Remote Desktop Manager for Mac saves the settings directly in a file with the XML format. For more information, please consult our XML topic.	<p>Pros:</p> <ul style="list-style-type: none">• Easy backup.• Can be edited manually or by an external system.• No installation. <p>Cons:</p> <ul style="list-style-type: none">• No possibility of sharing.• No security management.• There is a possibility for conflict or data corruption to occur.• Does not support all features, such as attachments, Usage Logs, Offline Mode and User Management.

5.2.1 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 Devolutions Online Services.

Advanced Data Sources greatly increase the set of managing features available to administrators, such as:

- Document uploads and entry attachments.

- Audit and logging.
- Advanced security with [User Management](#) and [Security Group Management](#).
- [Offline mode](#).
- [2-Factor Authentication](#).

Currently, the Advanced Data Sources are:

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

5.2.1.1 Devolutions Server

DESCRIPTION



Devolutions Server is a self-hosted repository for storing and sharing your remote connections and credentials. You can find more information on the product's web site [here](#).

HIGHLIGHTS

- High-end security server for your company.
- Share your sessions with multiple users.
- Can be deployed online.
- Support Windows authentication and Active Directory group integration.
- Client and server side caching optimization.

- Requires the Remote Desktop Manager for Mac Enterprise client installed for management.



Devolutions Server supports only SQL Server as a data store at this time.

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 server. Ensure you use the correct protocol if SSL is required by the server (https).

Alternatively, you can export the data source information and then import the file in your client workstations as described [Import/Export Data Source](#).

SETTINGS

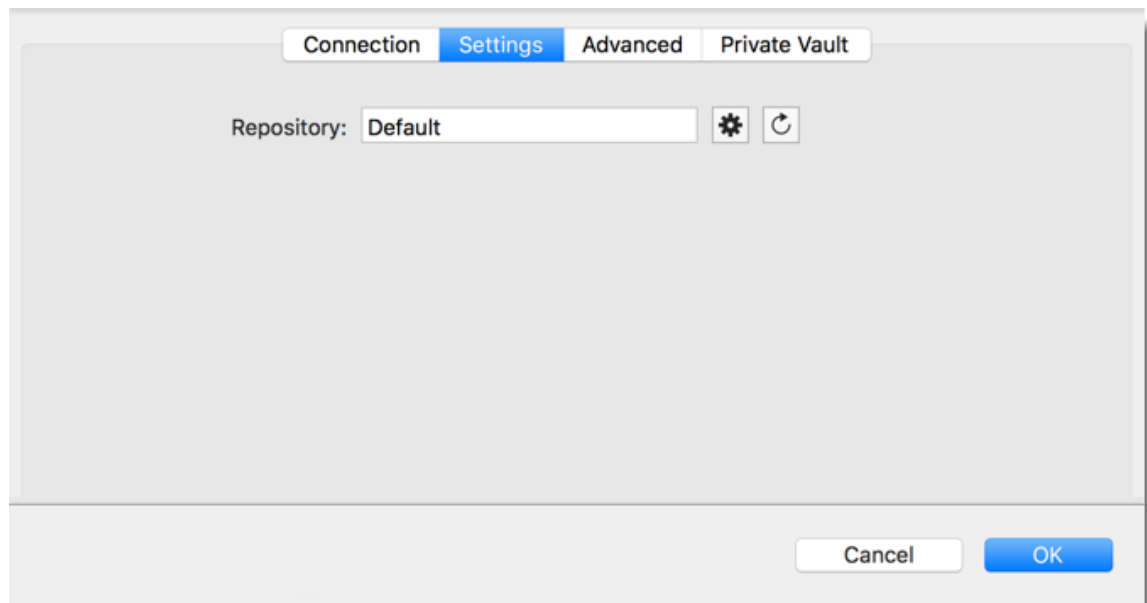
CONNECTION

The screenshot shows the 'Connection' tab of the Devolutions Server Connection dialog. It includes input fields for 'Name', 'Server', 'User name', and 'Password'. The 'Password' field is currently filled with six dots and is highlighted with a blue border. To the right of the 'User name' and 'Password' fields are checkboxes for 'Always ask user name' and 'Always ask password'. A 'Test connection' button is located below the 'Password' field. At the bottom right of the dialog are 'Cancel' and 'OK' buttons.

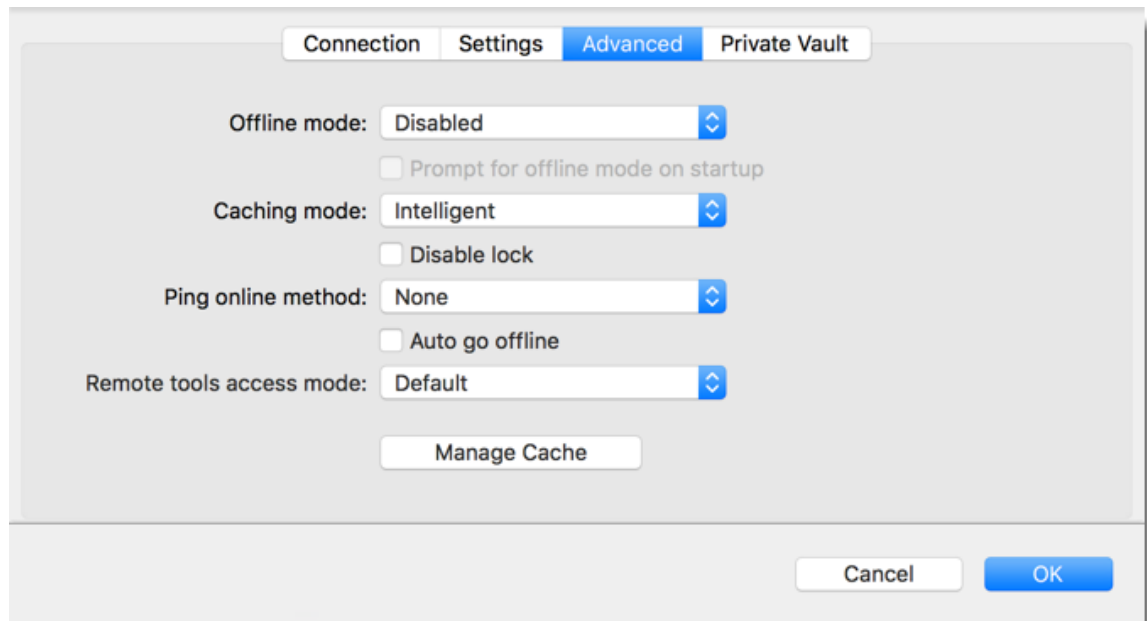
Devolutions Server Connection tab

OPTION	DESCRIPTION
Name	Name of the data source.
Server	Name of Devolutions Server instance.
Username	Username to connect to the data source.
Password	Password to connect to the data source.
Test connection	Test the connection with Devolutions Server to validate if the proper information has been provided.
Always ask username	Always ask for the username when connecting to the data source.
Always ask password	Always ask for the password when connecting to the data source.

SETTINGS

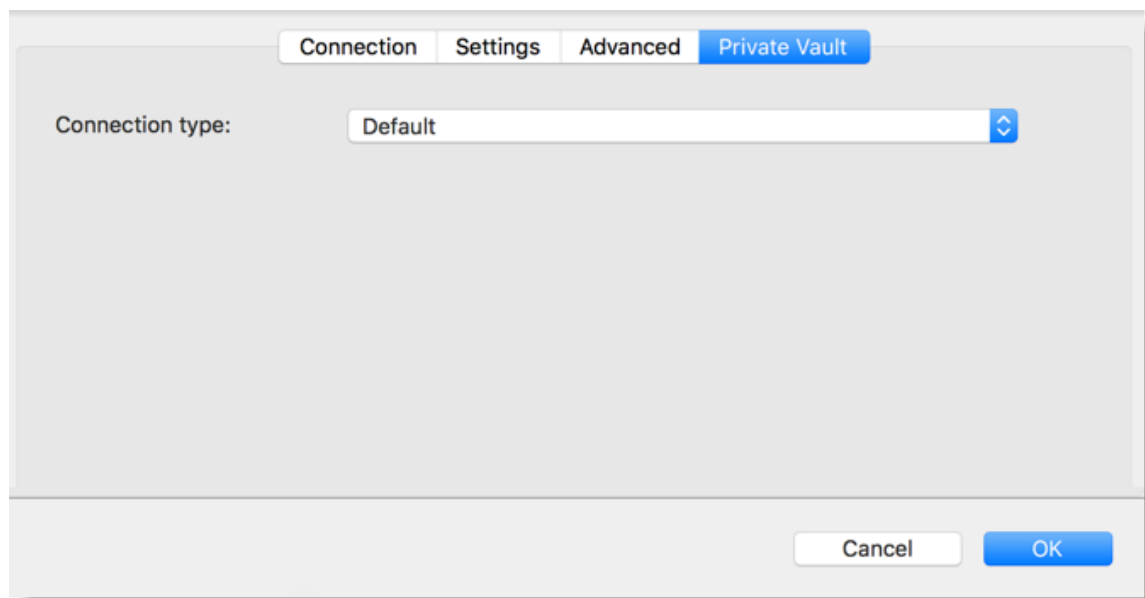
*Devolutions Server - Settings tab*

ADVANCED

*Devolutions Server - Advanced tab*

OPTION	DESCRIPTION
Offline mode	Determine if you want to use this data source in Offline mode. In offline mode, the data source can be available in Read Only or in Read/Write mode.
Prompt for offline mode on startup	Every time you will connect on your data source, you will be prompt to use the data source in offline mode.
Caching mode	Determine how the entries will be reload in the data source. See Caching Mode topic for more information.
Ping online method	Indicate the prefer ping online. Select between: <ul style="list-style-type: none">• None• Web request
Auto go offline	If the ping online method doesn't work it will automatically go offline.
Remote tools access mode	Select your remote tools access mode between: <ul style="list-style-type: none">• Local• Via data source
Manage Cache	Manage your cache on your computer to analyse, vacuum, repair or delete it. This can be very helpful when experiencing offline issues. For more information please follow this link .

USER VAULT

*Devolutions Server - User Vault*

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

5.2.1.2 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

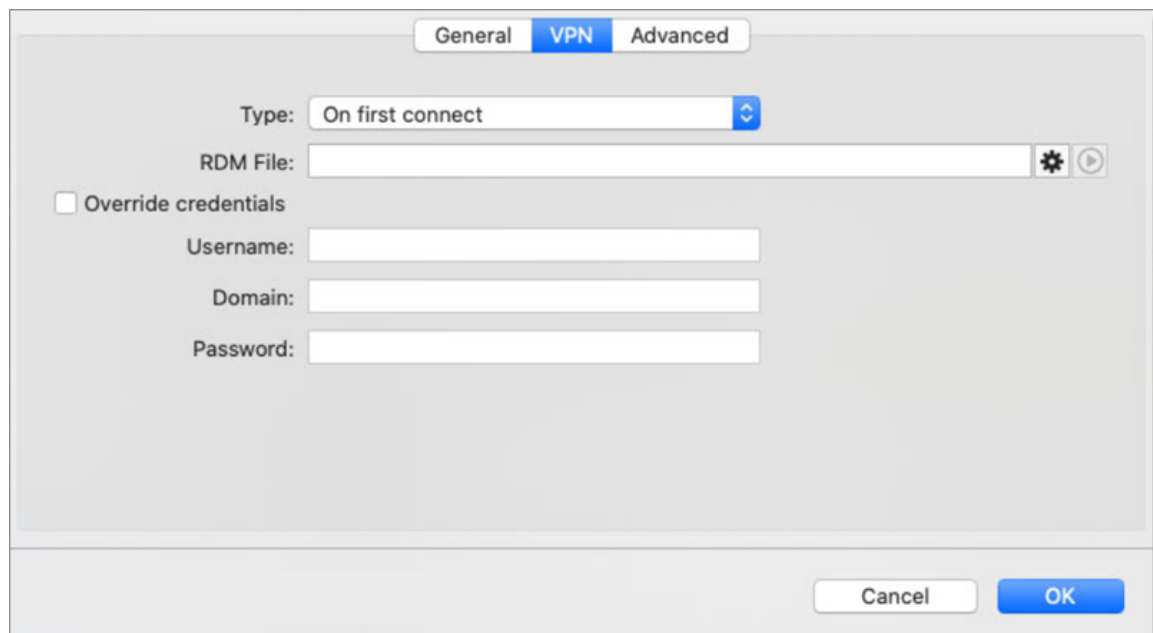
GENERAL

The screenshot shows the 'General' tab of the Remote Desktop Manager settings window. It features three input fields: 'Name', 'Username', and 'Host'. The 'Host' field includes a gear icon for configuration. The window has 'Cancel' and 'OK' buttons at the bottom right.

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

VPN

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



The screenshot shows a dialog box with three tabs: General, VPN (selected), and Advanced. The VPN tab contains the following fields and controls:

- Type:** A dropdown menu set to "On first connect".
- RDM File:** A text input field with a settings gear icon and a play button icon to its right.
- ☐ **Override credentials**
- Username:** A text input field.
- Domain:** A text input field.
- Password:** A text input field.

At the bottom right of the dialog are "Cancel" and "OK" buttons.

ADVANCED

Set the interval for the automatic refresh.



5.2.1.3 SQL Server (MSSQL)

DESCRIPTION



Remote Desktop Manager for Mac uses the power of Microsoft SQL Server to save and manage all sessions.

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

We also support the following features:

- ***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.



A proper database backup strategy should be implemented to minimize possible data loss, please refer to Backups topic.



Active directory in a SQL Server data source is no longer supported in Remote Desktop Manager for macOS.



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 **Database Login** 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 would consider this unacceptable. It is recommended to use our **Custom login** model.



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

CONFIGURATION

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

SETTINGS

CONNECTION

The screenshot shows a 'Connection' dialog box with the following fields and controls:

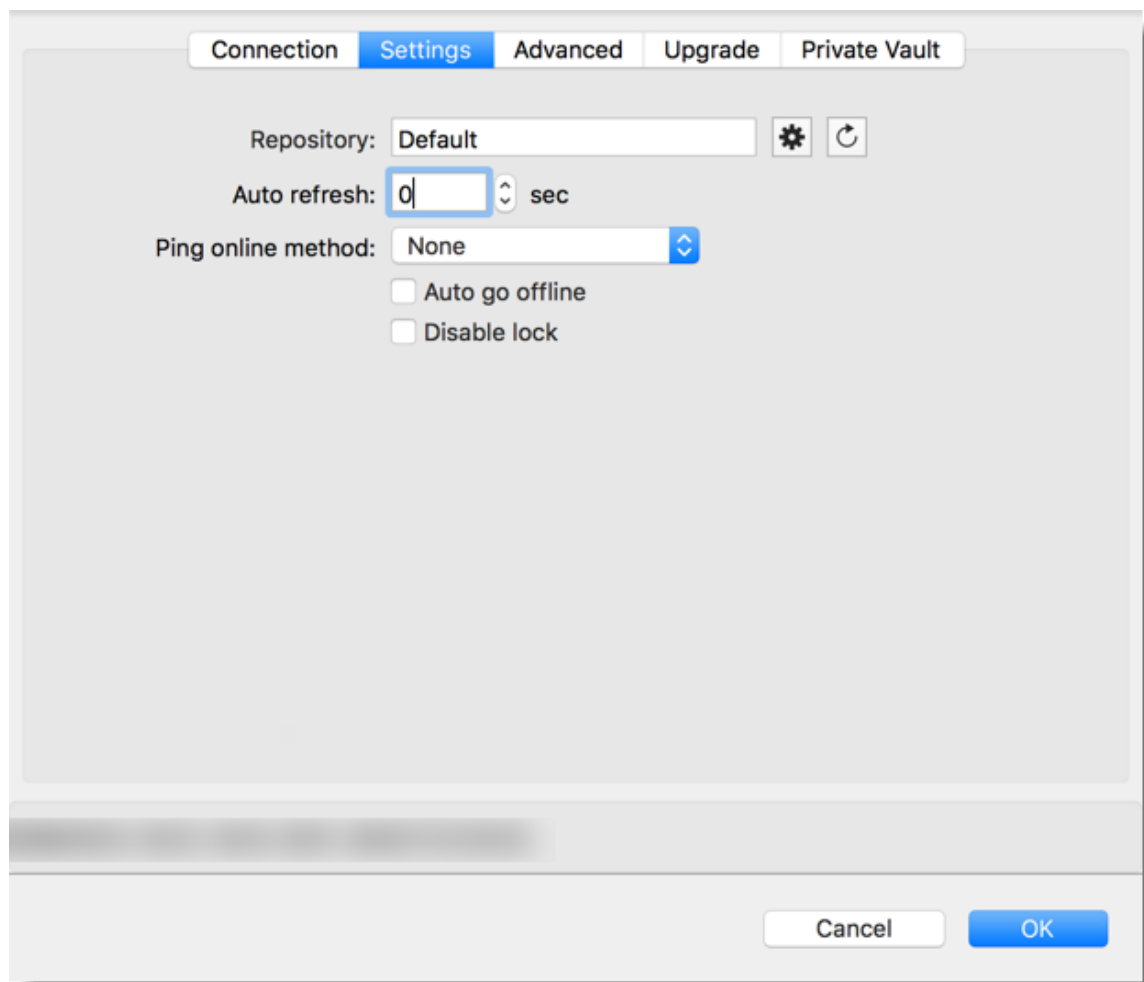
- Connection tab:** Active tab, with other tabs being 'Settings', 'Advanced', 'Upgrade', and 'Private Vault'.
- Name:** Text field containing 'DevWind'.
- SQL Server:** Dropdown menu currently set to 'SQL Server'.
- Server:** Text field with a placeholder '(Local) or IP or Server name' and a dropdown arrow.
- User:** Text field with an 'Editable' checkbox to its right.
- Domain:** Text field.
- Save password:** Checked checkbox.
- Password:** Password field with a masked password '.....' and a key icon.
- Database:** Text field with a 'Browse...' button.
- Two factor:** Dropdown menu set to 'None'.
- Buttons:** 'Test Server', 'Test Database', 'Cancel', and 'OK'.

SQL Server - Connection tab

OPTION	DESCRIPTION
Name	Name of the data source.
Server	Name of the server where the data source will be store.
SQL Server	Select your data source between the SQL Server or Azure SQL.
Login Mode	Specify the authentication mode to use. Select between: <ul style="list-style-type: none">• Database login

OPTION	DESCRIPTION
	<ul style="list-style-type: none">• Custom login
User	Username to access the SQL server.
Domain	Domain to access the SQL server.
Save password	By saving the password for your data source you will connect automatically to your SQL Server without having to enter your password every time.
Password	Password used to access the SQL server.
Database	Name of the database on the SQL server for the utilization of Remote Desktop Manager for Mac.
Two factor	Enable the 2-Factor Authentication to access your data source.
Test Server	Test the connection with the server to validate if the proper information has been provided.
Test Database	Test the connection with the database to validate if the proper information has been provided.

SETTINGS



SQL Server - Settings tab

OPTION	DESCRIPTION
Repository	If using Repositories click on the ellipsis to select the proper Repository.
Auto refresh	Set the interval for the automatic refresh.
Ping online method	Indicate the prefer ping online method. Select between: <ul style="list-style-type: none">• None• Ping

OPTION	DESCRIPTION
	<ul style="list-style-type: none">• <i>Port scan</i>
Auto go offline	Use the data source in offline mode when the ping method does not respond.
Disable lock	Disable the option to lock the data source directly. You can still lock the application but you won't be prompted for the database password if this option is disabled.

ADVANCED

The screenshot shows the 'Advanced' tab of a settings dialog box for a SQL Server connection. The dialog has five tabs: 'Connection', 'Settings', 'Advanced' (selected), 'Upgrade', and 'Private Vault'. The 'Advanced' tab contains the following settings:

- Offline mode:** A dropdown menu set to 'Read/write'.
- Prompt for offline mode on startup:** An unchecked checkbox.
- Caching mode:** A dropdown menu set to 'Intelligent'.
- Connection timeout:** A numeric input field set to '30' with a unit of 'sec'.
- Command timeout:** A numeric input field set to '60' with a unit of 'sec'.
- Allow beta database upgrade:** An unchecked checkbox.
- Buttons:** 'Manage Cache' and 'Advanced Settings'.

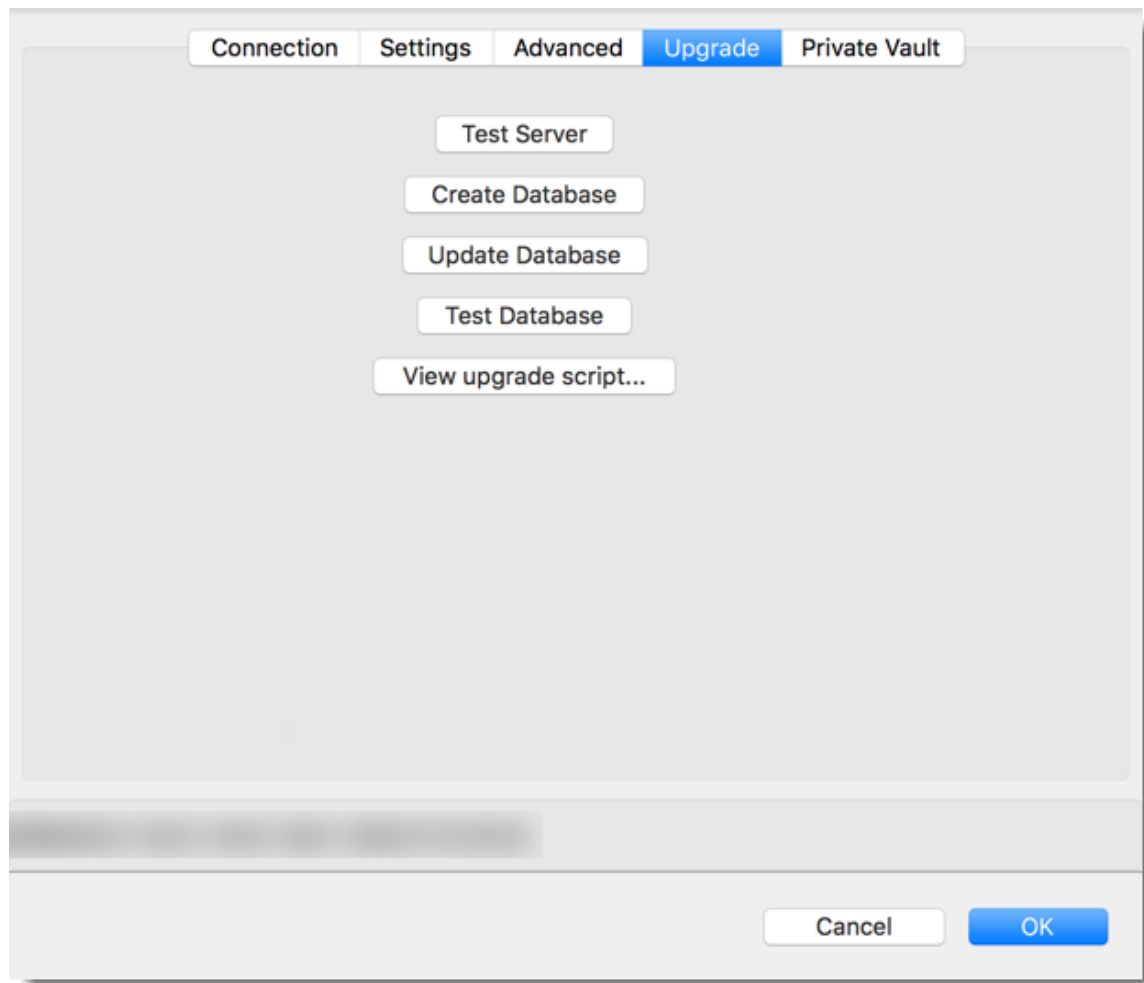
At the bottom right of the dialog are 'Cancel' and 'OK' buttons.

SQL Server - Advanced tab

OPTION	DESCRIPTION
Offline mode	Determine the Offline mode availability. Select between: <ul style="list-style-type: none">• <i>Disabled</i>• <i>Read-only</i>• <i>Read/write</i>
Prompt for offline mode on startup	Ask to use the data source in offline mode when the user connects to the data source.

OPTION	DESCRIPTION
Caching mode	Determine how the entries will be reloaded in the data source. For more information, please consult the Caching Mode topic.
Auto refresh	Set the interval for the automatic refresh.
Connection timeout	Waiting time before a connection timeout.
Command timeout	Waiting time before a command timeout.
Allow beta database upgrade	Allow beta upgrade of the database (when using a beta version of Remote Desktop Manager).
Manage Cache	Manage your cache on your computer to analyse, vacuum, repair or delete it. This can be very helpful if you have offline issues. For more information please follow this link .
Advanced Settings	Edit the connection string values directly.

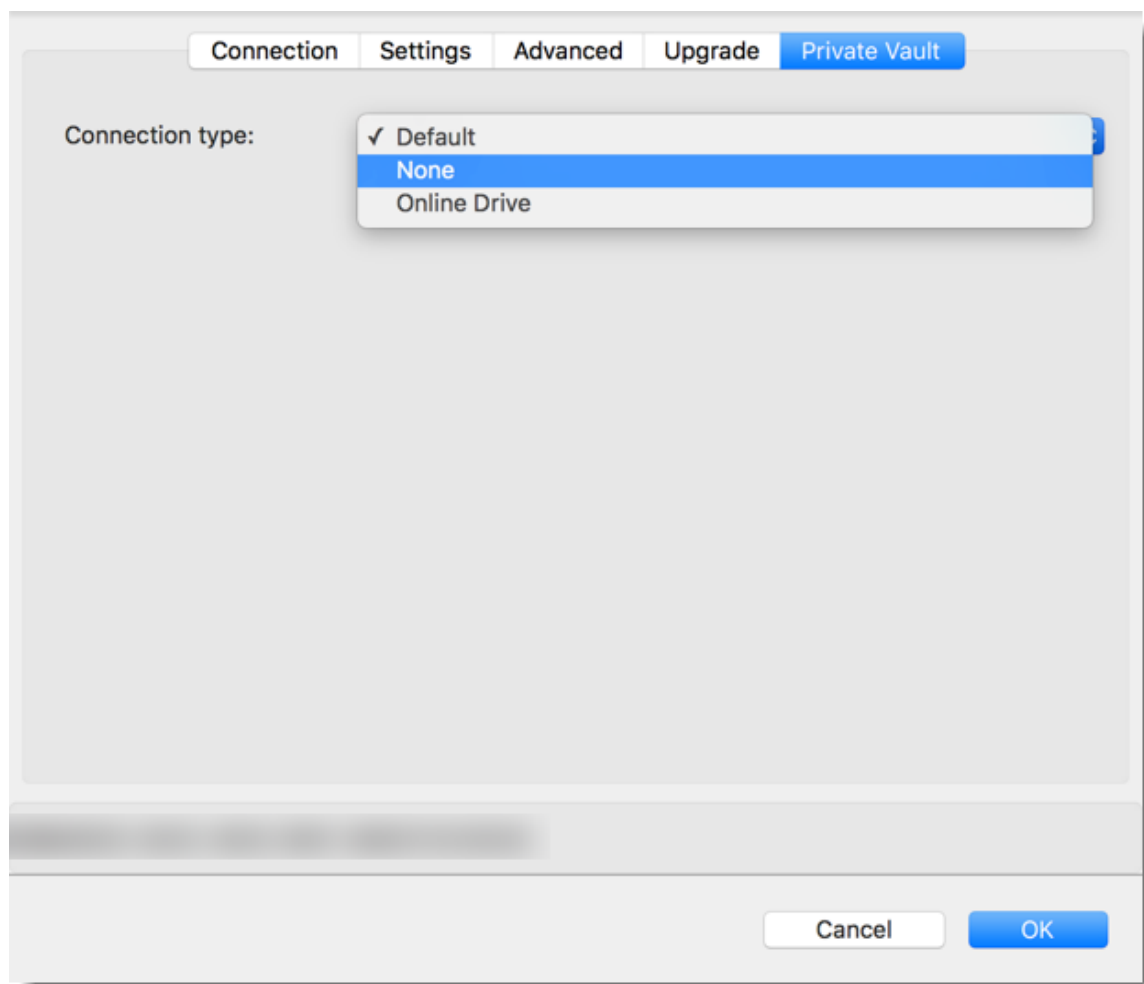
UPGRADE

*SQL Server - Upgrade tab*

OPTION	DESCRIPTION
Test Server	Test the connection with the server to validate if the proper information has been provided.
Create Database	Create the database on the SQL server to use Remote Desktop Manager.
Update Database	Update the database on the SQL server, if required to use Remote Desktop Manager.
Test Database	Test the connection with the database to validate if the proper information has been provided.

OPTION	DESCRIPTION
View upgrade script...	If you wish to process Database upgrade by hand instead of automatically you may use the upgrade script to do so.

USER VAULT



SQL Server - User Vault

OPTION	DESCRIPTION
Type	Select the type of User Vault to use. Select between:

OPTION	DESCRIPTION
	<p>Default: use the default User Vault, which is stored in the database.</p> <p>None: disable the User Vault for all users.</p> <p>Online Drive: use a Devolutions Online Drive file (*.dod) as a User Vault.</p>

5.2.1.3.1 Configure SQL Server

DESCRIPTION

1. Install SQL Server or SQL Server Express.

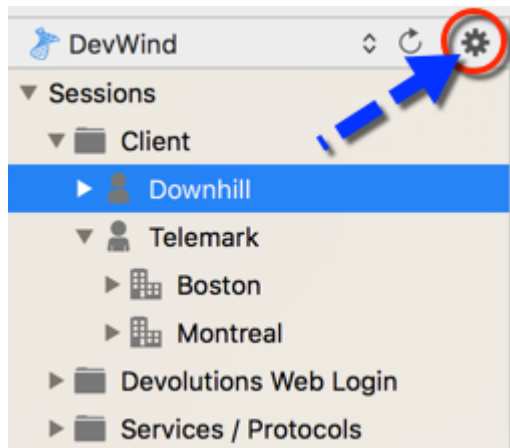


Newly installed SQL Server instances do not allow remote connections. Please follow the directions in [SQL Server](#).



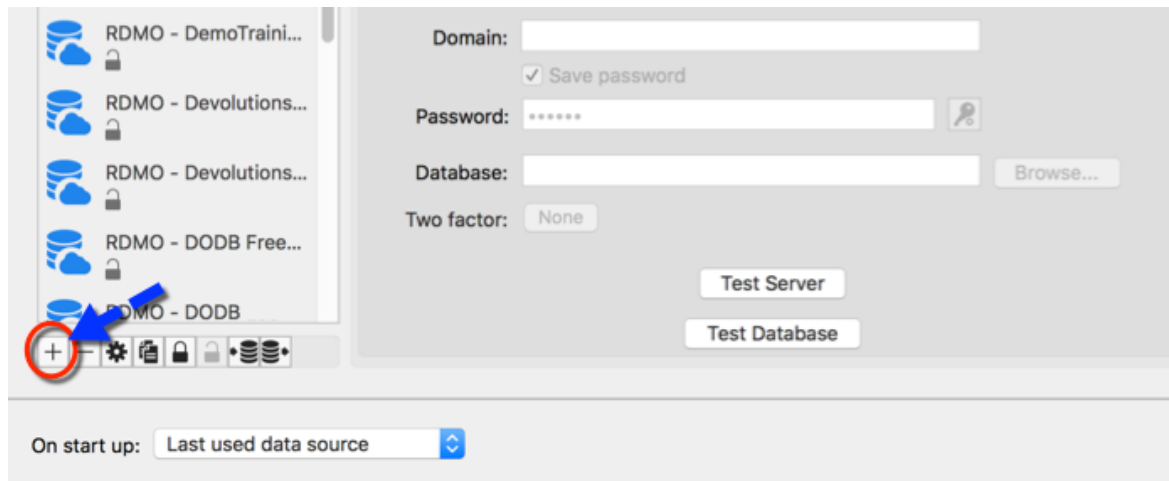
For added security, you can enable SSL Encryption to communicate with your instance of SQL Server. However, due to a framework limitation, this is not compatible with our iOS and Android versions of Remote Desktop Manager for Mac. Please follow directions on <https://support.microsoft.com/en-us/kb/316898>.

2. Click on the **setting** button in the Navigation Pane or go in **File - Data Sources**.



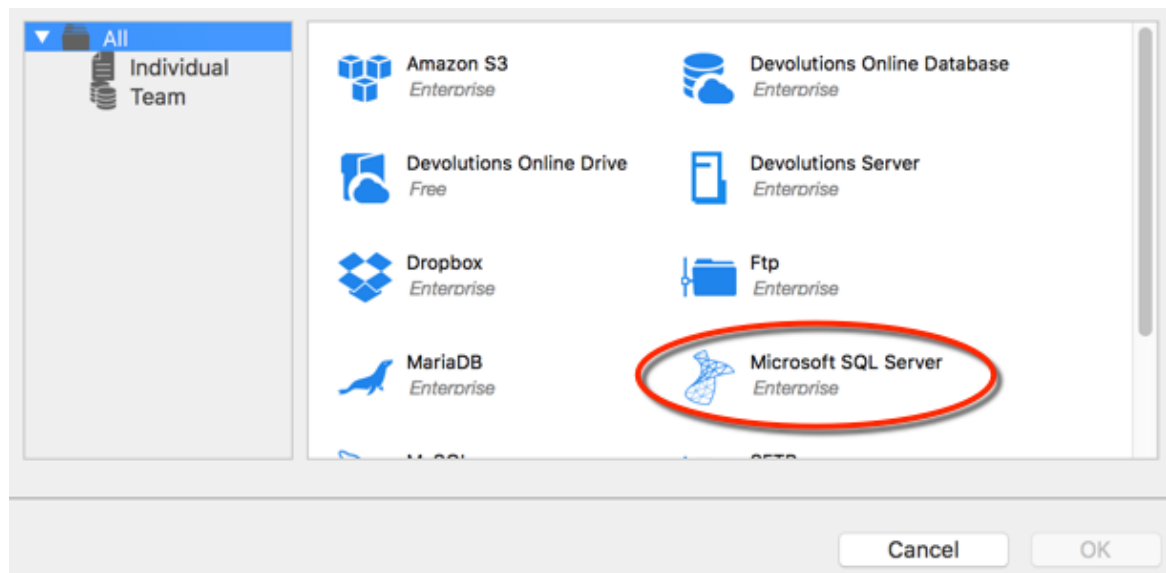
Setting button

3. Click on the **plus** to Add a New Data Source.



Data Source - Add a new data source

4. Select **Microsoft SQL Server**.



Select SQL Server data source

5. Provide the connection information for the SQL Server with a user having enough privileges to create the database.

The screenshot shows the 'Connection' tab of a configuration window. The 'Name' field is 'DevWind' and the 'Server' dropdown is 'SQL Server'. The 'Server' field is empty with the hint '(Local) or IP or Server name'. The 'Database login' dropdown is 'Database login'. The 'User' field is empty with an 'Editable' checkbox. The 'Domain' field is empty. The 'Save password' checkbox is checked. The 'Password' field is masked with dots and has a key icon. The 'Database' field is empty with a 'Browse...' button. The 'Two factor' dropdown is 'None'. There are 'Test Server' and 'Test Database' buttons. At the bottom are 'Cancel' and 'OK' buttons.

Field	Value
Name	DevWind
Server	SQL Server
Server (hint)	(Local) or IP or Server name
Database login	Database login
User	
Editable	<input type="checkbox"/>
Domain	
Save password	<input checked="" type="checkbox"/>
Password
Database	
Two factor	None

SQL Server data source configuration

6. Select the **Upgrade** tab and click the **Create Database** button. If the database is already created on the SQL Server, press the **Update Database** button to create the appropriate tables in the database.



SQL Server - Upgrade tab

7. Once the database is created, create a Remote Desktop Manager administrator account 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.

8. Connect to the SQL Server data source with the Remote Desktop Manager administrator account. To do so, go in **File - Data Source** and click on the setting button to edit the data source used to create the database and change the login information for the administrator account created with Remote Desktop Manager.

The screenshot shows the 'Connection' tab of the Remote Desktop Manager for macOS. The 'Name' field is 'DevWind' and the 'Server' type is 'SQL Server'. The 'Server' field is empty, with a hint '(Local) or IP or Server name'. The 'Database login' dropdown is set to 'SQL Server'. The 'User' field is highlighted with a red rectangle and is empty, with an 'Editable' checkbox to its right. The 'Domain' field is empty. The 'Save password' checkbox is checked. The 'Password' field is masked with dots. The 'Database' field is empty, with a 'Browse...' button to its right. The 'Two factor' dropdown is set to 'None'. There are 'Test Server' and 'Test Database' buttons. At the bottom are 'Cancel' and 'OK' buttons.

SQL Server - Connection tab - User

The SQL Server data source is now correctly configured.

5.2.1.3.2 Recovery Model

DESCRIPTION

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 backup 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>.

5.2.1.3.3 Encrypting Connections to SQL Server

DESCRIPTION

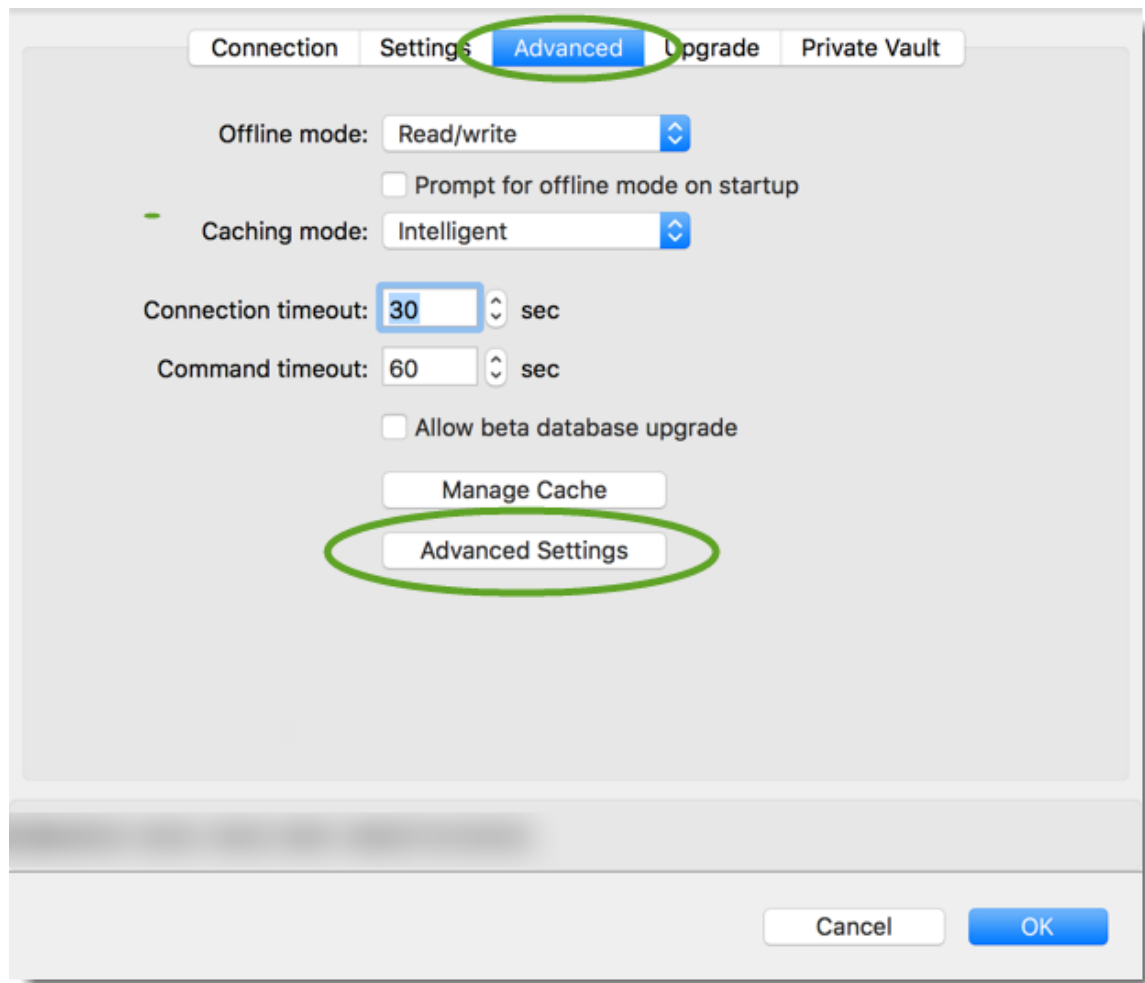
To ensure that the communication between Remote Desktop Manager for Mac and the SQL Server database is encrypted, an extensive procedure must be followed on the SQL Server instance.

Please consult this Microsoft technet article that provides detailed instruction: Encrypting Connection 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 Advanced Settings of the data source.

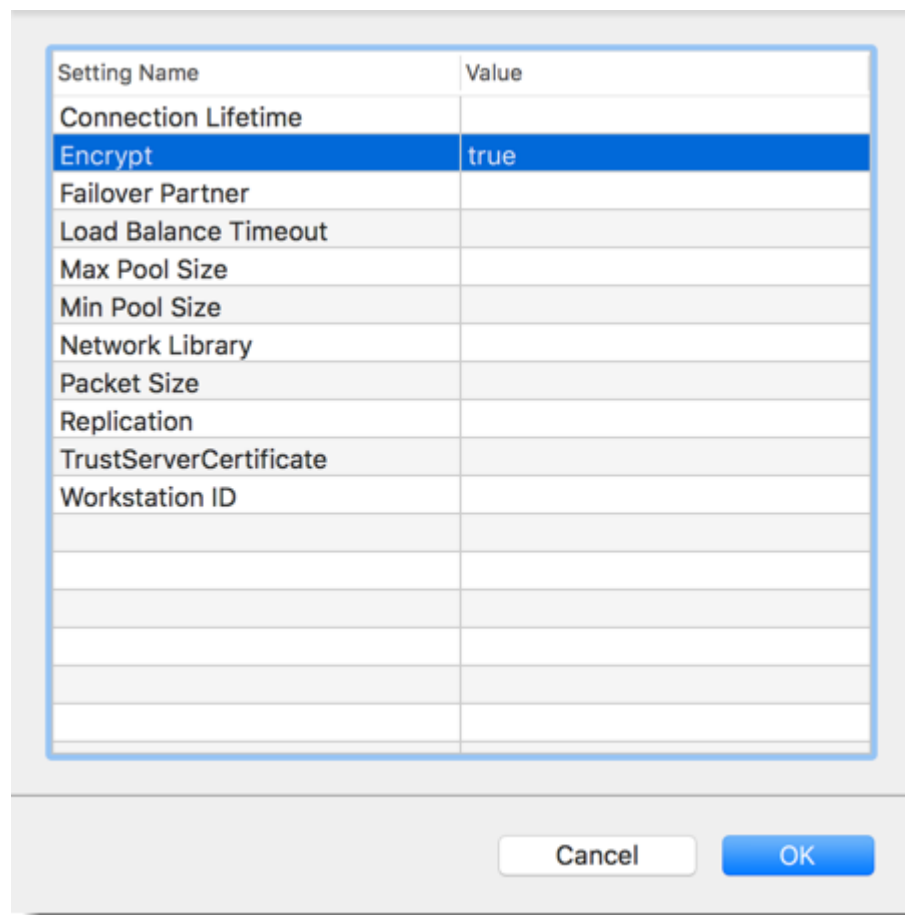
Procedure

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



SQL Server - Advanced tab

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



SQL Server - Advanced Settings

5.2.1.4 Azure SQL

DESCRIPTION



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

The following features are also supported:

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

MINIMUM REQUIREMENT FOR AZURE SQL DATABASE FOR RDM

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

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

Visit their website for more information.

HIGHLIGHTS

- Supports user management with a superior security model.
- Supports offline mode for when the server or network is unavailable.
- Supports entry logs and attachments.
- [Get more information on Microsoft Azure SQL.](#)



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

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



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

CONFIGURATION

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

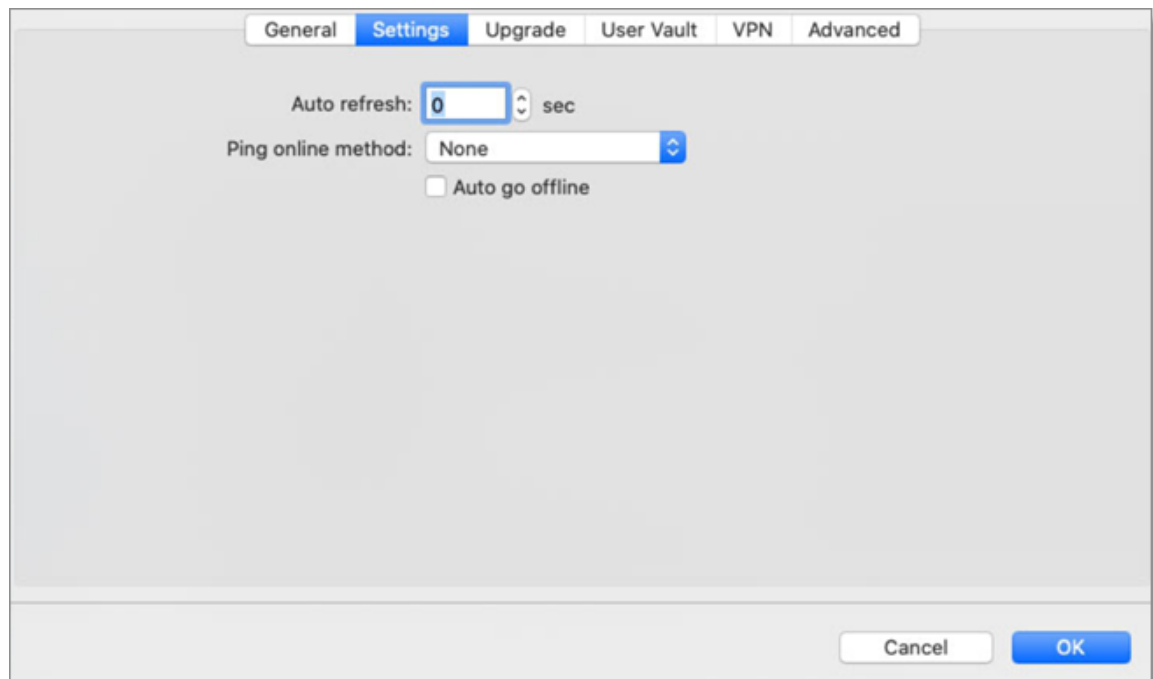
SETTINGS

GENERAL

OPTION	DESCRIPTION
Name	Enter a name for the data source.
Host	Enter the server hostname or IP address.

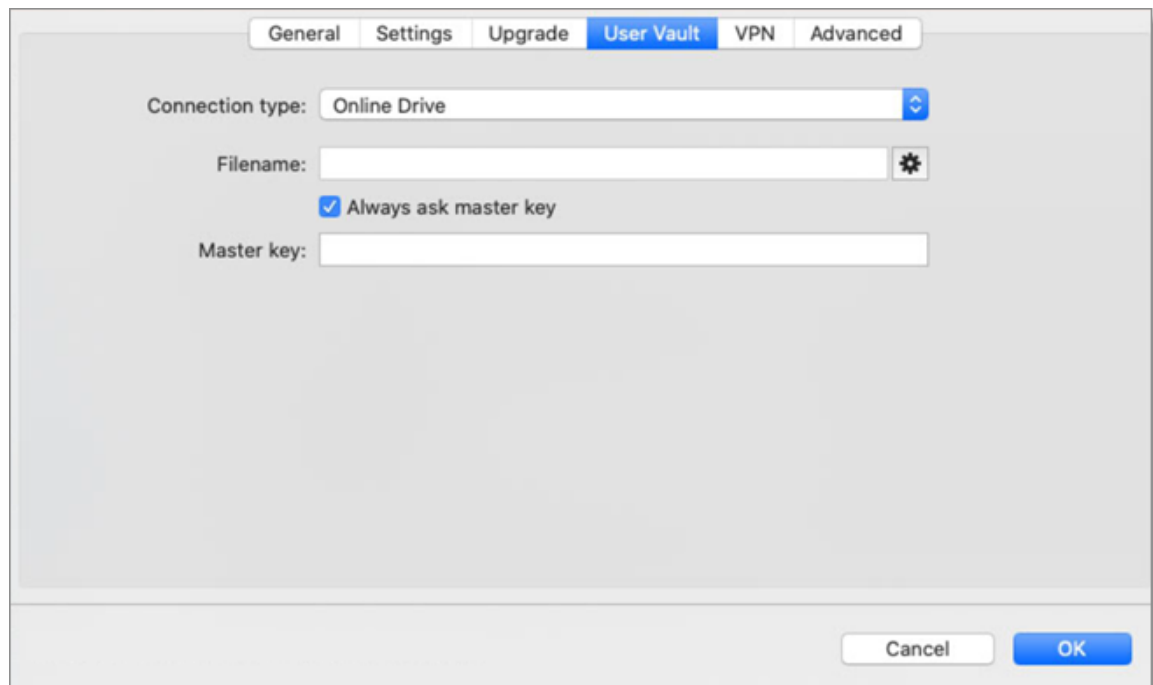
OPTION	DESCRIPTION
Login mode	Specify the authentication mode to use.
Username	Enter the username to access the Azure SQL database.
Password	Enter the password to access the Azure SQL database.
Always ask password	Prompt for the password when a user connects to the data source.
Database	Enter the name of the Azure SQL database.
Two factor	Enable the 2-Factor Authentication .
Test Database	Test the connection with the database to validate if the proper information has been provided.

SETTINGS



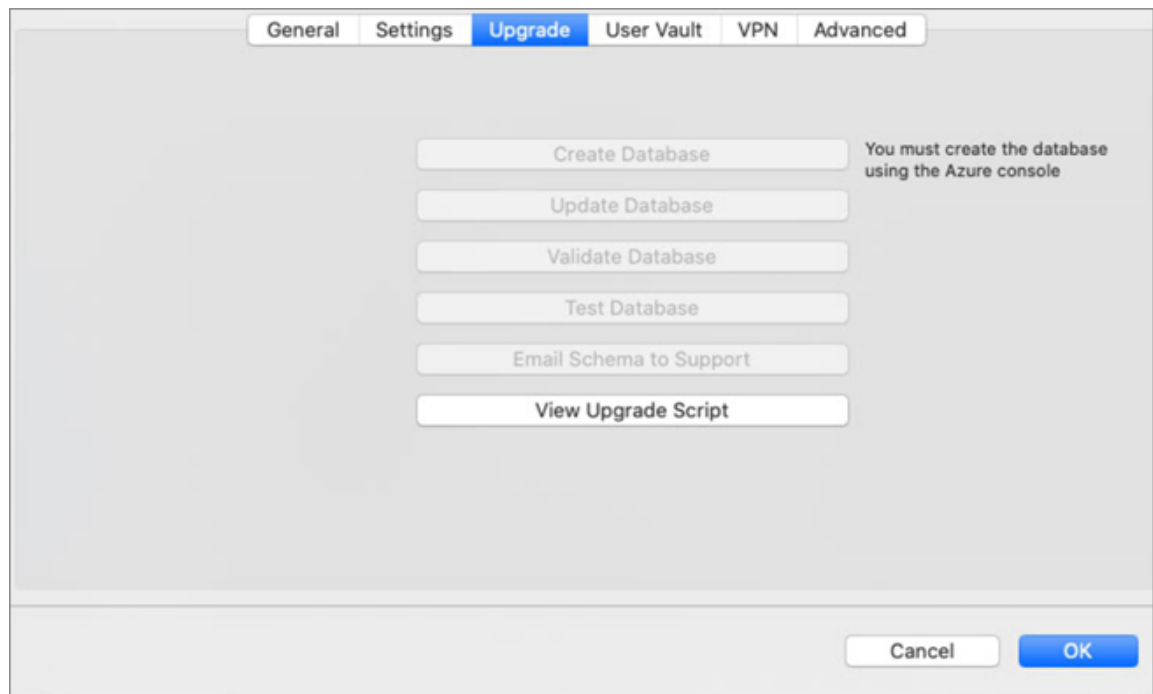
OPTION	DESCRIPTION
Auto refresh	Set the automatic refresh interval.
Ping online method	Indicate the preferred ping online method. Select between: <ul style="list-style-type: none">• None• Port Scan
Auto go offline	Use the data source in offline mode when the ping method does not respond.

USER VAULT



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

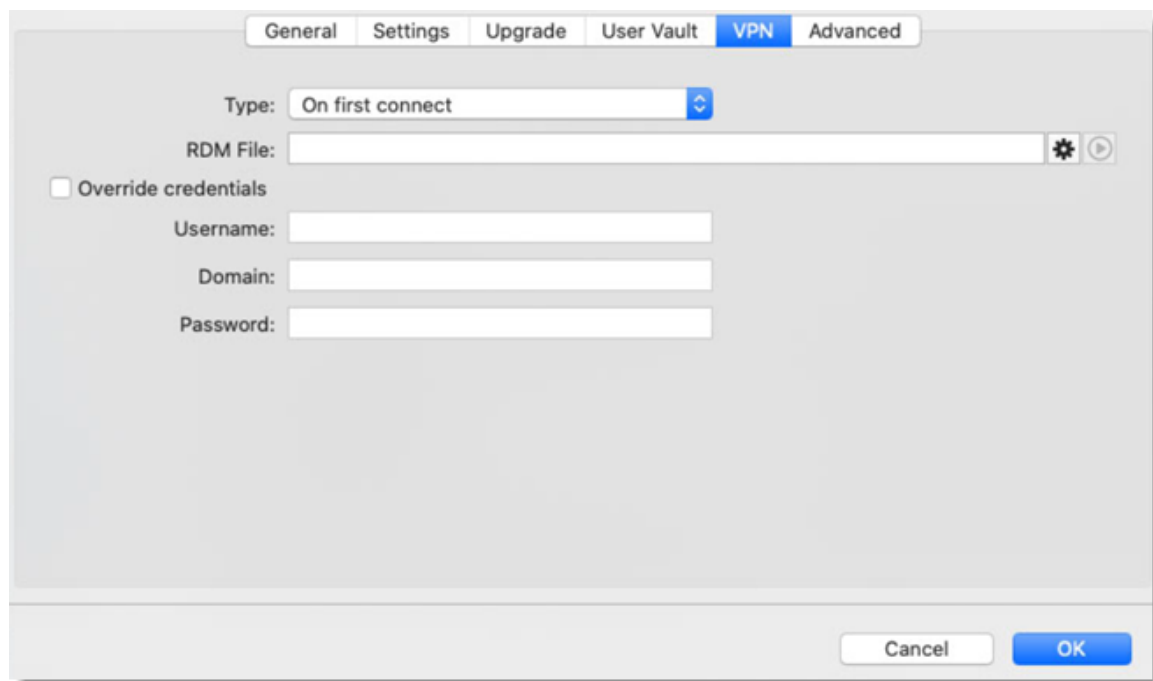
UPGRADE



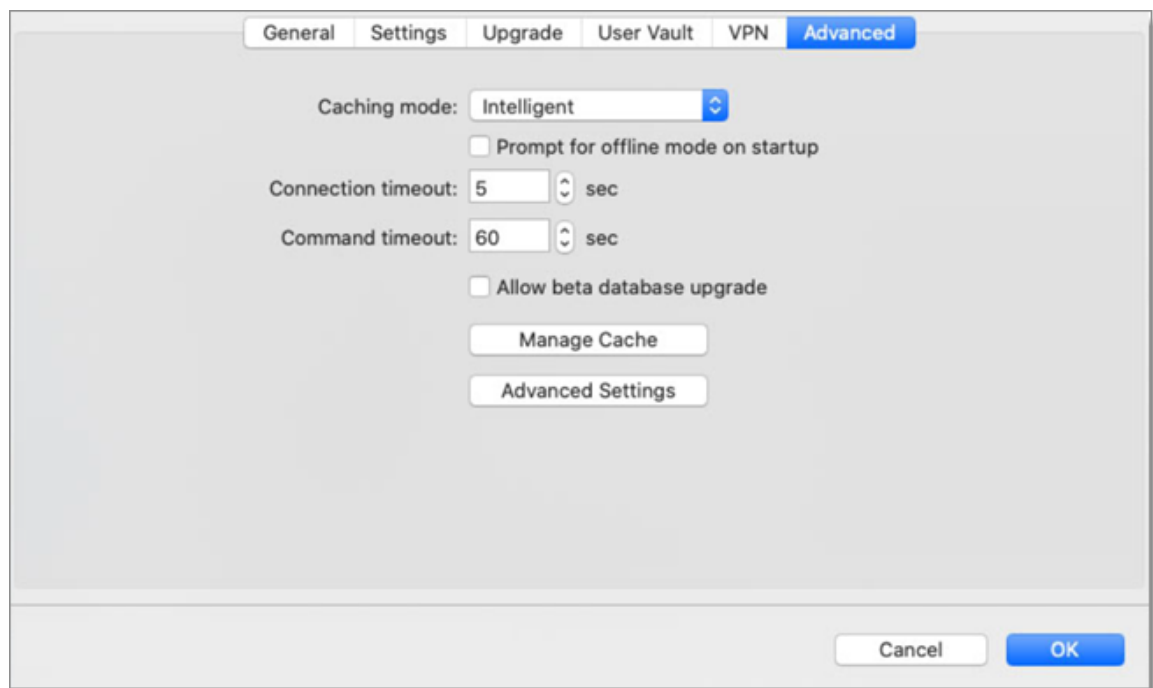
OPTION	DESCRIPTION
Create Database	Create the database on the SQL server to use Remote Desktop Manager.
Update Database	Update the database on the SQL server, if required to use Remote Desktop Manager.
Test Database	Test the connection with the database to validate if the proper information has been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

VPN

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



ADVANCED

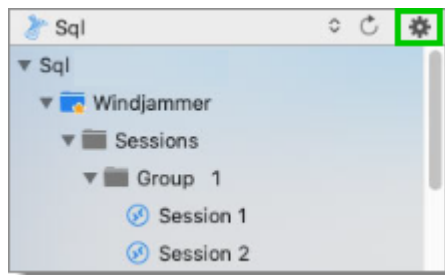


OPTION	DESCRIPTION
Caching mode	Determines how the entries will be reloaded in the data source. For more information, please consult the Caching topic.
Connection timeout	Set the delay of the connection timeout.
Command timeout	Set the delay of the command timeout.
Allow beta database upgrade	Allow beta upgrade of the database (when using a beta version of Remote Desktop Manager).
Manage Cache	Manage the data source cache. On large data sources caching is a must and will increase performance significantly.
Advanced Settings	Edit the connection string values directly.

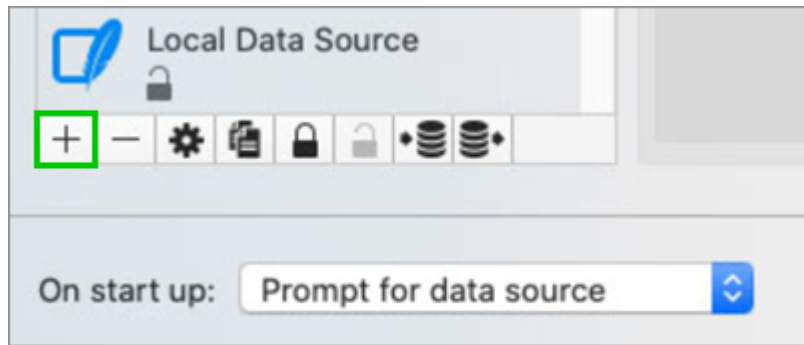
5.2.1.4.1 Configure Azure SQL

DESCRIPTION

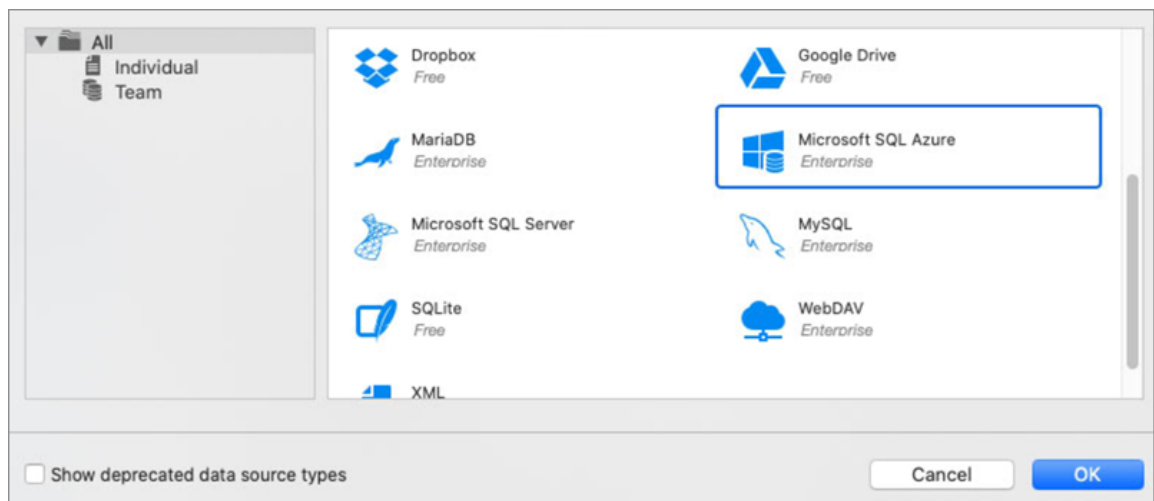
1. Make sure you have a valid Azure SQL subscription to be able to create your database.
2. Click on the gear button in the navigation pane or go to **File - Data sources**.



3. Click on the plus sign to create a new data source.



4. Select **Microsoft Azure SQL**.



5. Configure the connection to your Azure SQL with a user with sufficient privileges to create the database.

The screenshot shows a 'General' tab in a database configuration window. The 'Name' field is empty, and the 'Host' dropdown is set to 'Microsoft SQL Azure'. Below 'Host' is a text field for '(Local) or IP or Server name'. The 'Database login' dropdown is set to 'Database login'. The 'Username' field is empty, and the 'Password' field is empty with a key icon. There are checkboxes for 'Editable', 'Always ask password', and 'Two factor' (set to 'None'). A 'Test Database' button is at the bottom. 'Cancel' and 'OK' buttons are at the bottom right.

6. Click on the **Upgrade** tab and press the **Create Database** button. If the database is already created on Azure SQL, press the **Update Database** button to create the appropriate tables in the database.

The screenshot shows the 'Upgrade' tab in the same database configuration window. The 'Create Database' and 'Update Database' buttons are highlighted with a green box. A message next to them says 'You must create the database using the Azure console'. Below these are buttons for 'Validate Database', 'Test Database', 'Email Schema to Support', and 'View Upgrade Script'. 'Cancel' and 'OK' buttons are at the bottom right.

7. Once the database has been created, create a Remote Desktop Manager administrator account via the **Administration - Users menu**.



If your database was created using a Super User (example: SA), we recommend that you keep this user only for the creation of the database and/or for the upgrade of the database. A Remote Desktop Manager administrator account must first be created, and then users must be created with this Remote Desktop Manager administrator account.

8. Log in to the Azure SQL data source with the Remote Desktop Manager administrator account. To do this, go to **File - Data source** and click on the settings button to edit your SQL data source. Then enter the Remote Desktop Manager administrator account that you created in the username.

You can now start creating your sessions or creating your users.

5.2.2 Dropbox

DESCRIPTION



Remote Desktop Manager for Mac 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

CONNECTION

The screenshot shows a 'Dropbox - Connection' dialog box. It has two tabs: 'Connection' (selected) and 'Advanced'. The 'Connection' tab contains the following fields and controls:

- Name:** A text field containing 'Dropbox'.
- Mode:** A dropdown menu set to 'Account'.
- Email:** An empty text field.
- Account status:** A label indicating 'The account is not validated yet.'
- Validate with Dropbox:** A button to initiate validation.
- Dropbox directory:** An empty text field.
- File name:** A text field containing 'connections.xml'. Below it, a note states 'The file will be created if it does not exist'.
- Compress database file:** An unchecked checkbox.

At the bottom right of the dialog are 'Cancel' and 'OK' buttons.

Dropbox - Connection tab



Remote Desktop Manager for Mac support the 2-Factor Authentication of Dropbox. When the button **Validate with Dropbox** is press and the 2-Factor Authentication is enable in Dropbox, a first box will open and ask for the Dropbox account password. After, a second box will open to enter the security code. The security code can be received by SMS or generated by Google Authenticator.

OPTION	DESCRIPTION
Name	Name of the data source.
Mode	Select the mode that is preferred to configure the data source. Select between: <ul style="list-style-type: none"> • Account • Local
Email	Contains the email address associated with the Dropbox account.
Validate with Dropbox	Validate the email address with the Dropbox account.
Dropbox directory	Indicate the folder in Dropbox. It should not contains any drive since it's stored online. Leave it empty to use the default Dropbox root.
Filename	Indicate the filename used to store the data on the data source.
Compress database file	Activate this option if you wish to compress your database file.

ADVANCED

The screenshot shows a configuration window for a data source connection. At the top, there are two tabs: 'Connection' and 'Advanced', with 'Advanced' being the active tab. Below the tabs, there are three unchecked checkboxes: 'Always ask for password', 'Disable reveal password', and 'Allow offline mode'. Below these is a label 'Auto refresh:' followed by a text input field containing the number '300' and a small up/down arrow icon. Below the input field is a button labeled 'Manage Cache'. At the bottom left, there is a label 'ID:' followed by a blurred text field. At the bottom right, there are two buttons: 'Cancel' and 'OK'.

Dropbox - Advanced tab

OPTION	DESCRIPTION
Always ask for password	Always ask for password when connecting to the data source.
Disable reveal password	Disable the reveal password feature when a user access this data source.
Allow offline mode	Allow the data source to be used in Offline mode.
Auto refresh	Set the interval to use between each automatic refresh.
Manage Cache	You can clear the output, analyse, repair or delete the cache of your Dropbox. For more information please follow this link .

5.2.3 Online Drive

DESCRIPTION

The 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. 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 topic [Online Drive](#) 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

General Backup VPN Advanced

Name: [Create an account for free](#)

Username:

Connection mode:

Application password:

Filename:

The file will be created if it does not exist

Master key:

☒ Always ask master key

Server:

ID: B38AA0B6-0125-4827-9B9F-F6781A793183

Cancel OK

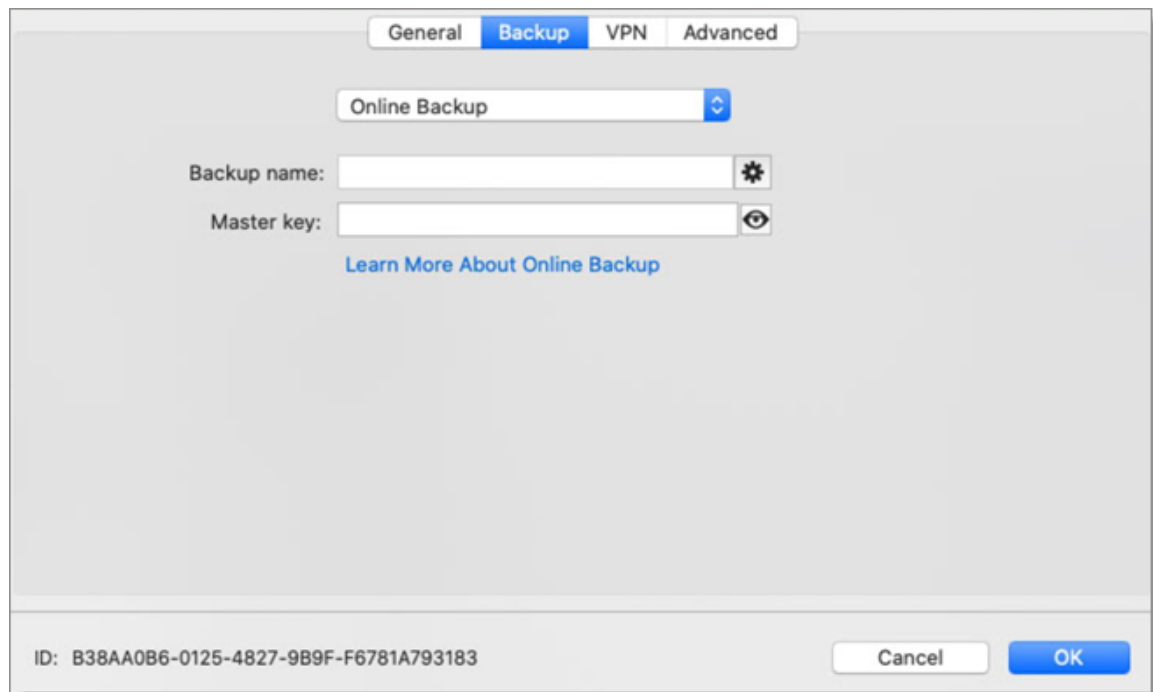
Online Drive - General tab

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

OPTION	DESCRIPTION
Master key	Contains a master key to access the data source.
Always ask master key	Ask for the master key every time a connection to the Devolutions Online Drive is attempted.

BACKUP

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



Online Drive - Backup

OPTION	DESCRIPTION
Backup	Choose the backup mode. Select between: <ul style="list-style-type: none">• None: No backup of your data source will be created.

OPTION	DESCRIPTION
	<ul style="list-style-type: none">• Online Backup: An Online Backup (using Online Backup Service) will automatically be created.• Save to file: Your backup will be saved to a chosen file but will not automatically do backup every 30 seconds.
Backup name	Specify the backup name that will allow you to automatically save your sessions in a safe online storage space and restore them in the event of problems.

VPN

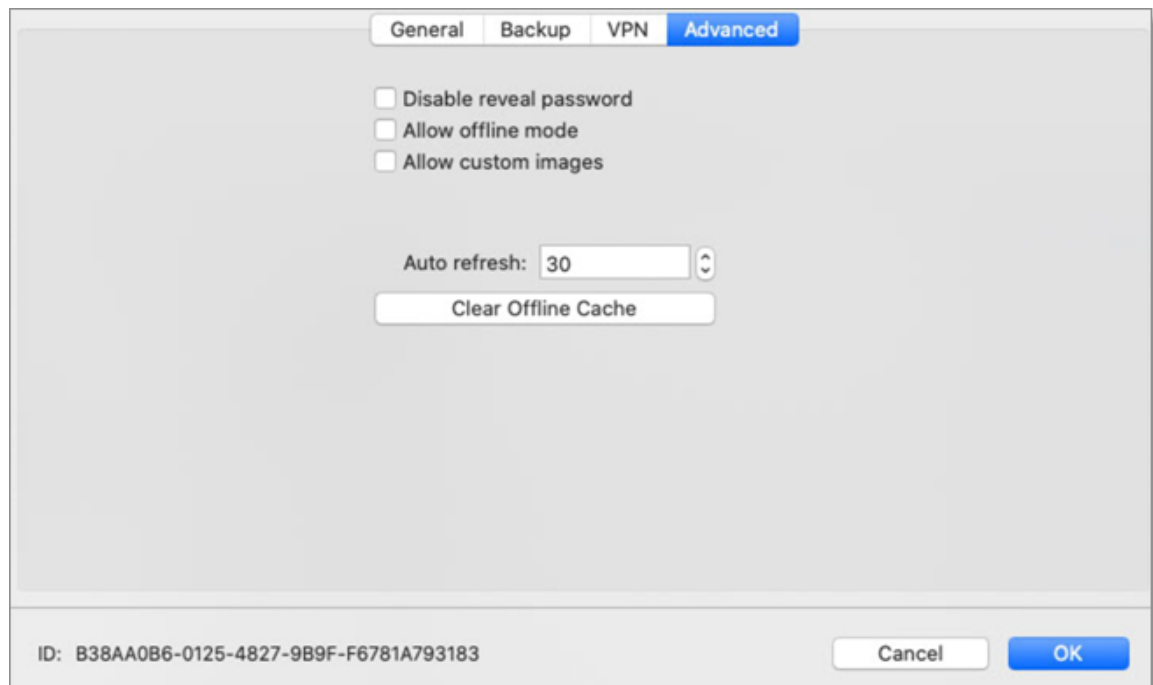
Open a VPN to access your data prior to connecting to your **Devolutions Online Drive**.

The screenshot shows a dialog box with four tabs: General, Backup, VPN (selected), and Advanced. The VPN tab contains the following fields and controls:

- Type: A dropdown menu set to "On first connect".
- RDM File: A text input field with a gear icon and a play button icon to its right.
- Override credentials: A checkbox that is currently unchecked.
- Username: A text input field.
- Domain: A text input field.
- Password: A text input field.

At the bottom of the dialog box, there is an ID field containing "ID: B38AA0B6-0125-4827-9B9F-F6781A793183", a Cancel button, and an OK button.

ADVANCED

*Online Drive - Advanced tab*

OPTION	DESCRIPTION
Disable reveal password	Disable the reveal password feature when a user access this data source.
Allow offline mode	Allow the data source to be used in Offline mode.
Allow custom images	Allows the user to use custom images. Too many custom images could dramatically increase the size of the data source and increase the load time at the same time.
Auto refresh	Set the interval for the automatic refresh
Clear Offline Cache	Clear the offline cache on your computer. This can be very helpful when encountering offline issues.

5.2.4 Password Hub Personal

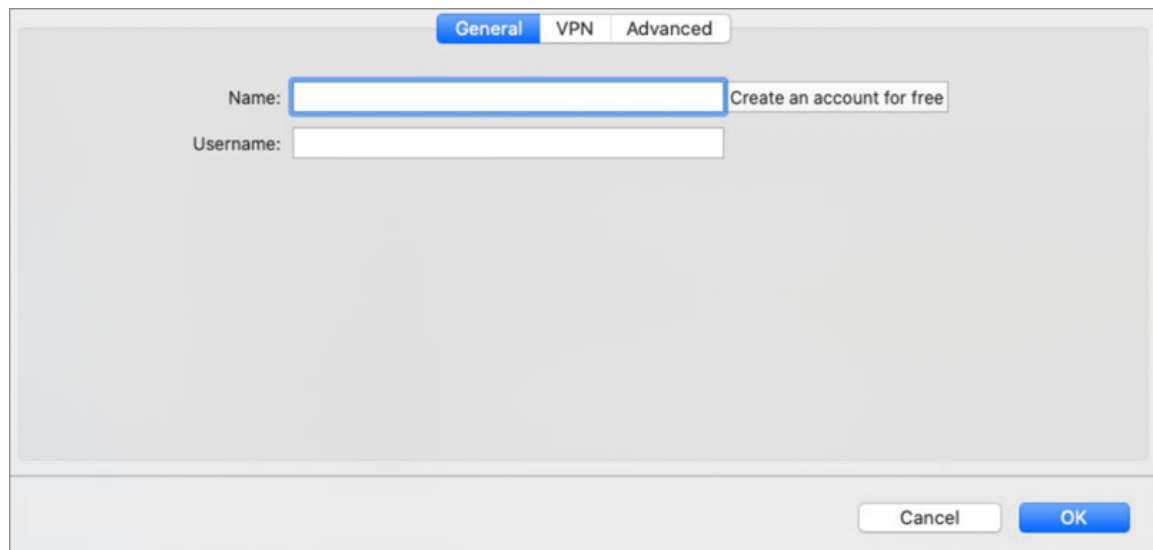
DESCRIPTION

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

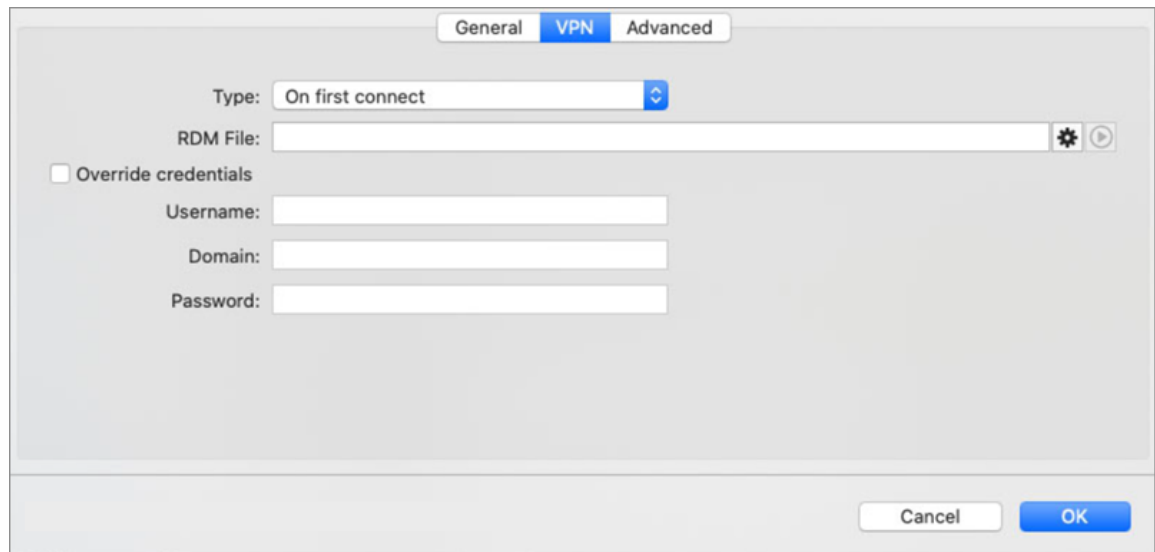
GENERAL

The image shows a settings dialog box for 'Password Hub Personal'. It has three tabs: 'General' (selected), 'VPN', and 'Advanced'. In the 'General' tab, there are two input fields: 'Name:' and 'Username:'. The 'Name' field is highlighted with a blue border. To the right of the 'Name' field is a button that says 'Create an account for free'. At the bottom right of the dialog are 'Cancel' and 'OK' buttons.

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

VPN

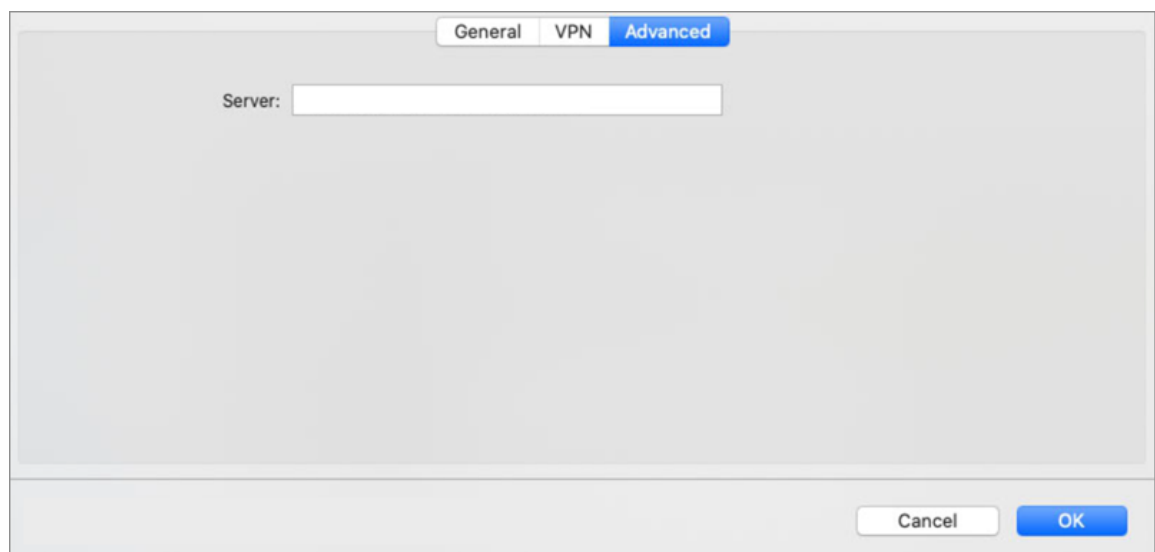
Open a **VPN** to access your data prior to connecting to your Devolutions Password Hub.



The screenshot shows the 'VPN' tab of a configuration window. At the top, there are three tabs: 'General', 'VPN' (selected), and 'Advanced'. The 'Type' dropdown menu is set to 'On first connect'. Below it is the 'RDM File' field, which is empty, followed by a gear icon and a play button icon. There is an unchecked checkbox labeled 'Override credentials'. Below this are three text input fields: 'Username:', 'Domain:', and 'Password:', all of which are empty. At the bottom right, there are 'Cancel' and 'OK' buttons.

ADVANCED

This is the **Server** address.



The screenshot shows the 'Advanced' tab of a configuration window. At the top, there are three tabs: 'General', 'VPN', and 'Advanced' (selected). The 'Server:' label is followed by a large, empty text input field. At the bottom right, there are 'Cancel' and 'OK' buttons.

5.2.5 SQLite

DESCRIPTION



Remote Desktop Manager for Mac SQLite data source is ***ideal for single user in a 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 for Mac. 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 for Mac does not support sharing an 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, you must enter your password when creating your SQLite data source.

SETTINGS

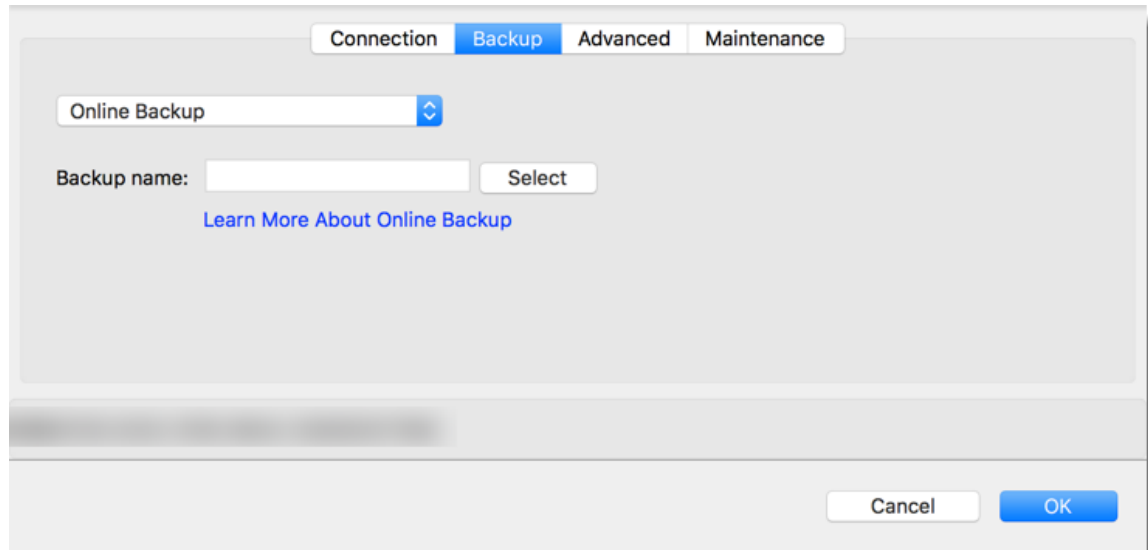
CONNECTION

The screenshot shows the 'SQLite - Connection tab' in the Remote Desktop Manager settings. The 'Connection' tab is selected, with other tabs being 'Backup', 'Advanced', and 'Maintenance'. The 'Name' field is set to 'SQLite'. The 'Database' field contains the path 'devolutions.remotedesktopmanager/Connections1.db' and has a 'Browse...' button next to it. There are two checkboxes: 'Secure with password' (unchecked) and 'Always ask password' (unchecked). The 'Password' field is empty. The 'Two factor' dropdown is set to 'None'. At the bottom, there is an 'ID' field with a blurred value, and 'Cancel' and 'OK' buttons.

SQLite - Connection 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.
Secure with password	Secure the data source with a password. This is used to encrypt the database content and it cannot be recovered if lost.
Always ask password	Always ask for the password when connecting to the data source.
Two Factor	Enable the 2-Factor Authentication to access your data source.

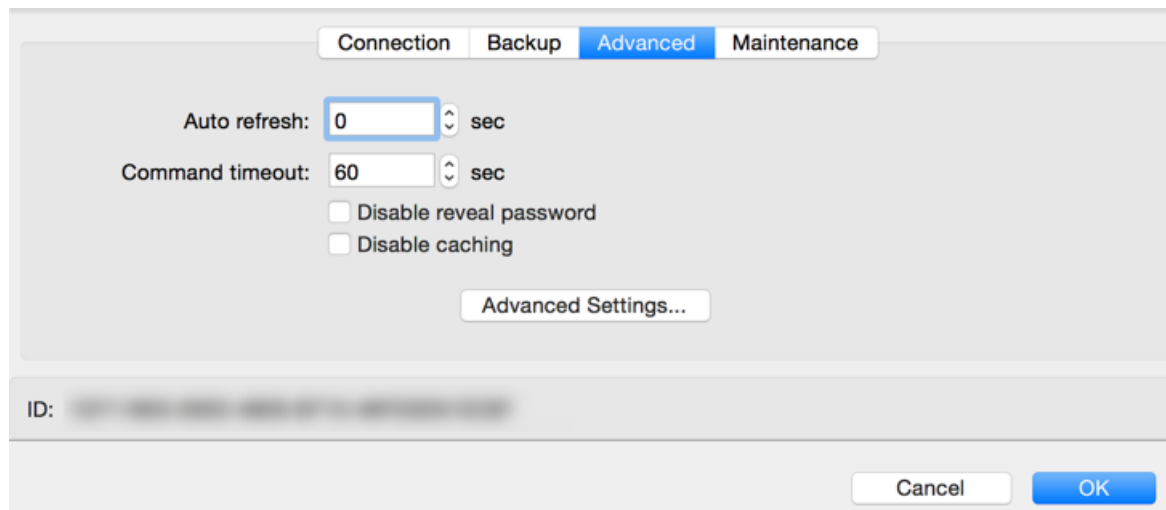
BACKUP



SQLite - Backup tab

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

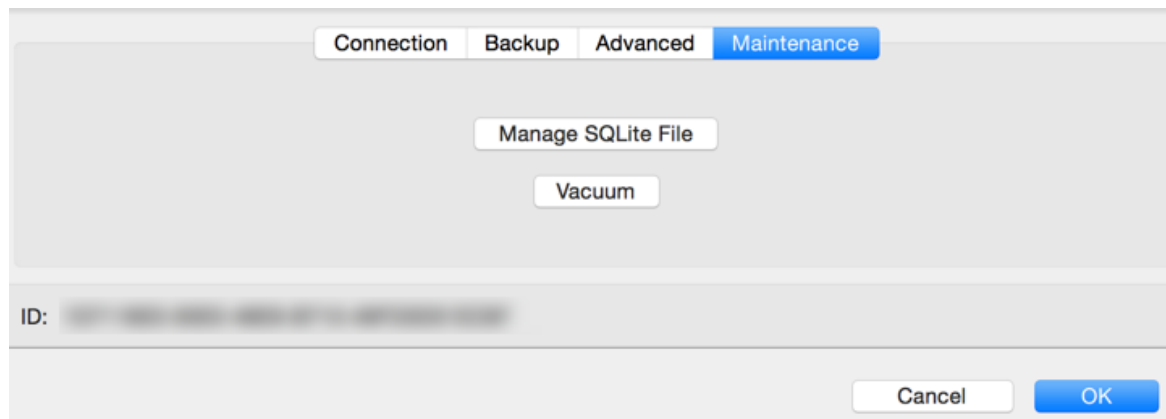
ADVANCED



SQLite - Advanced tab

OPTION	DESCRIPTION
Auto refresh	Set the interval for the automatic refresh.
Command timeout	Waiting time before a command timeout.
Disable reveal password	Disable the reveal password feature when a user access this data source.
Disable caching	Entries will be reload in Simple mode in the data source. See Caching Mode topic for more information.
Advanced Settings	Use to directly modify the connection string value.

MAINTENANCE

*SQLite - Maintenance tab*

OPTION	DESCRIPTION
Manage SQLite File	Manage all your SQLite file to analyse, vacuum, repair or delete them. For more information please follow this link .
Vacuum	Used to compress and clean up the current database file.

5.2.6 XML

DESCRIPTION



Remote Desktop Manager for Mac saves the settings directly in a file with the XML format.

HIGHLIGHTS

- It is a free data source.
- It's possible to configure an auto refresh interval.
- The [Online Backup Service](#) 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 and 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's 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

CONNECTION

The screenshot shows the 'CONNECTION' tab of the Remote Desktop Manager settings window. It features three tabs: 'Connection' (selected), 'Backup', and 'Advanced'. The 'Name' field is set to 'XML'. The 'File name' field contains the path 'olutions.remotedesktopmanager/Connections.xml', with a 'Browse...' button to its right. Below the 'File name' field, a note states: 'The file will be created if it does not exist'. An 'ID' field is visible below the 'File name' section. At the bottom right, there are 'Cancel' and 'OK' buttons.

XML - Connection tab

OPTION	DESCRIPTION
Name	Name of the data source.
Filename	Specify the full path of the XML file used to save the data. Relative paths and environment variables can be used as well.

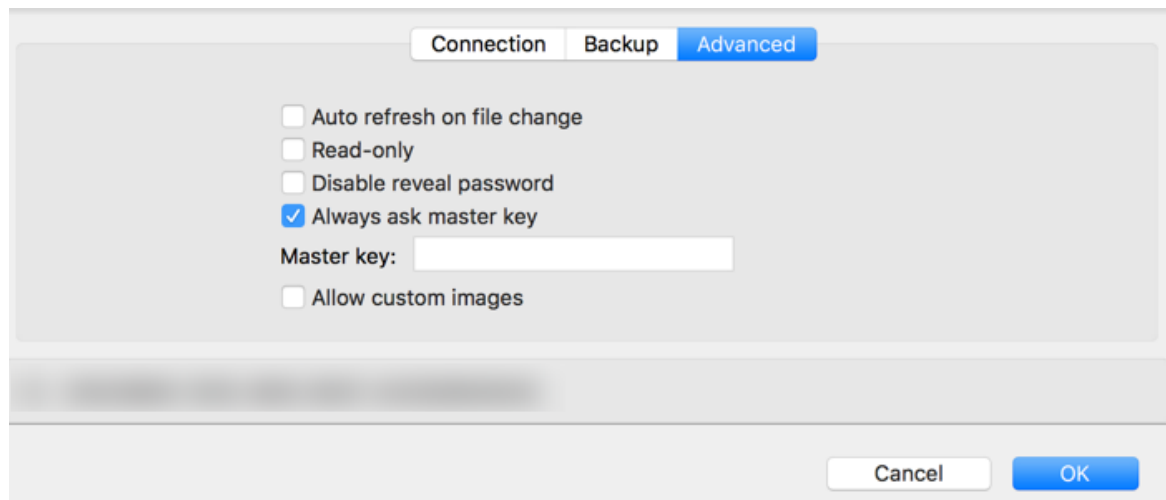
BACKUP

The screenshot shows a dialog box with three tabs: 'Connection', 'Backup' (selected), and 'Advanced'. In the 'Backup' tab, there is a dropdown menu currently set to 'Online Backup'. Below it, there is a text field for 'Backup name:' followed by a 'Select' button. A blue link 'Learn more about Online Backup' is positioned below the text field. At the bottom of the dialog, there is an 'ID:' label followed by a blurred text field. The bottom right corner contains 'Cancel' and 'OK' buttons.

XML - Backup tab

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

ADVANCED



XML - Advanced tab

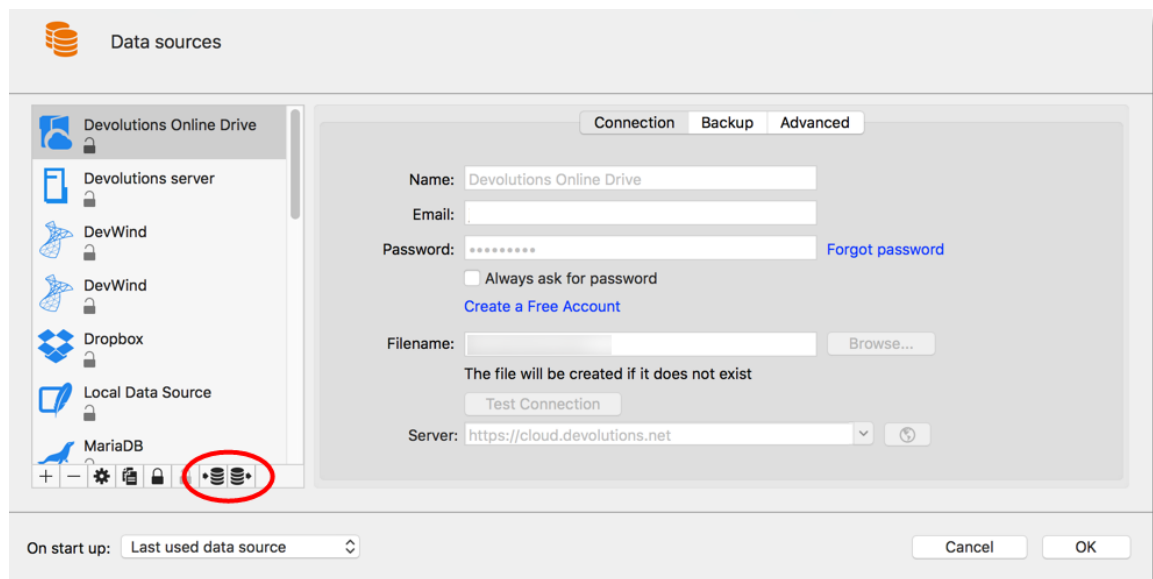
OPTION	DESCRIPTION
Auto refresh on file change	Indicate if the application monitor the file changes to automatically refresh the data source.
Read-only	Set the data source in read only. No new entry can be created and the existing data cannot be edit.
Disable reveal password	Disable the reveal password feature when a user accesses this data source.
Always ask master key	Always ask the Master key before opening the data source. This is used to encrypt the XML content and it could not be recovered if lost.
Master key	Enter the Master key that will be used before opening the data source.
Allow custom images	This will enable the loading of any custom images in the tree view.

5.3 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 [Export](#) functionality to backup or copy the database's content.

Use the data source dialog (**File-Data Sources...**) to access the import or export of the file.



Data Sources - Import/Export



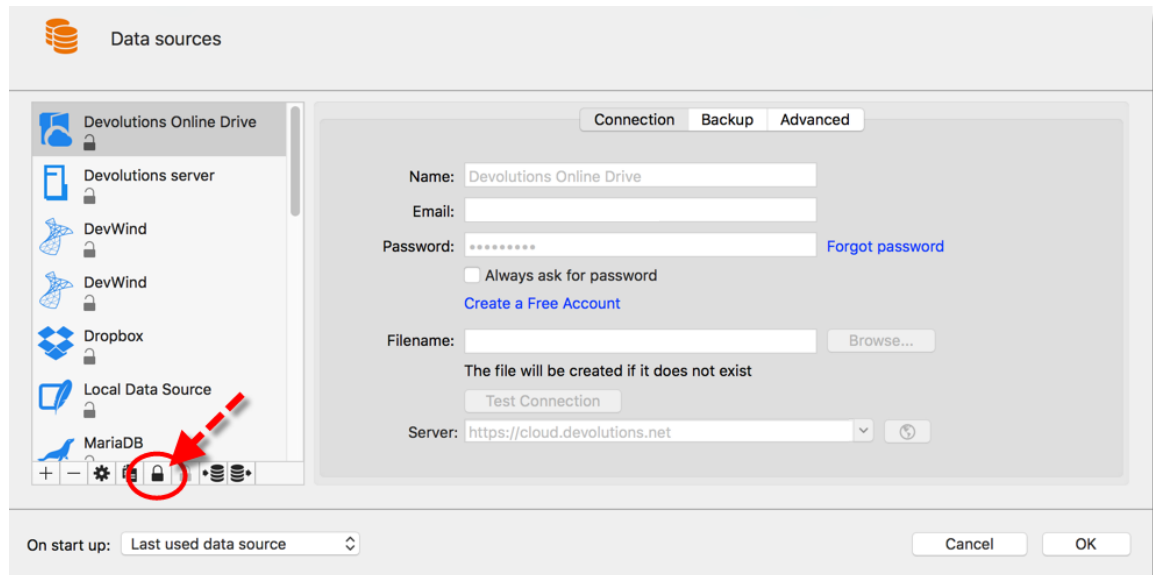
A locked data source can be exported and imported, but its content will not be accessible for use unless a password is entered when the data source is selected. See [Lock Data Source](#) for more information.

5.4 Lock Data Source

DESCRIPTION

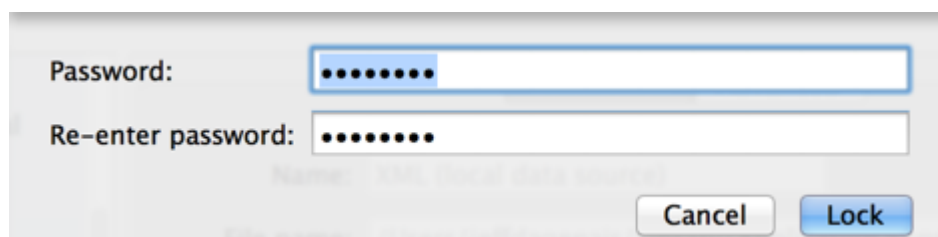
To protect sensitive data in your data source configuration (e.g. server URL or credentials), you may wish to lock the data source before you deploy it to your users. You can do it by using the Lock/Unlock button from the toolbar.

SETTINGS



Data Sources - Lock data source

The locked data source will require a password to be unlocked which must be specified when the lock is applied. Use the same password to unlock it in order 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.

5.5 2-Factor Authentication

DESCRIPTION



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

The **2-Factor Authentication (2FA)** provides unambiguous identification of users by means of the combination of two different components. These components may be something that the user knows or something that the user possess.

The use of two-factor authentication is used to prove one's identity is based on the premise that an unauthorized actor is unlikely to be able to supply both factors required for access. If in an authentication attempt at least one of the components is missing or supplied incorrectly, the user's identity is not established with sufficient certainty then access to the asset being protected by two-factor authentication will remain blocked.

Remote Desktop Manager has implemented two-factor authentication to our data sources using [Google Authenticator](#), [Yubikey](#) and [Duo](#).

1. When creating your data source select your 2-Factor Authentication method. To modify the option, click on **None**.

Connection Advanced Upgrade

Name: DevWind

Server: (Local) or IP or Server name

☐ Integrated security (Active Directory)

User: David Editable

Domain:

☒ Save password

Password: [masked] [key icon]

Database: new Browse...

Two factor: None

Test Server

Test Database

ID: 354F4BC2-69FD-44E8-9E59-4659AC056135

Cancel OK

SQL Server - Connection tab

2. In the next window click on **Change**.

2-Factor Configuration

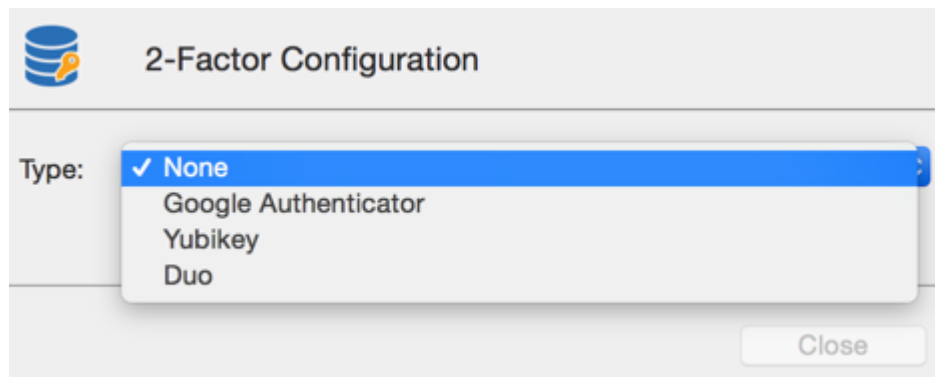
Type: None

Change

Close

Two Factor Configuration

3. Choose the type of 2-Factor Authentication you wish to use from our supported providers.



Two-Factor Configuration

4. Once you have selected your 2-Factor Authentication click on save to start the configuration.

For more information on the different 2-Factor Authentication method please see:

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

5.5.1 Google Authenticator

DESCRIPTION

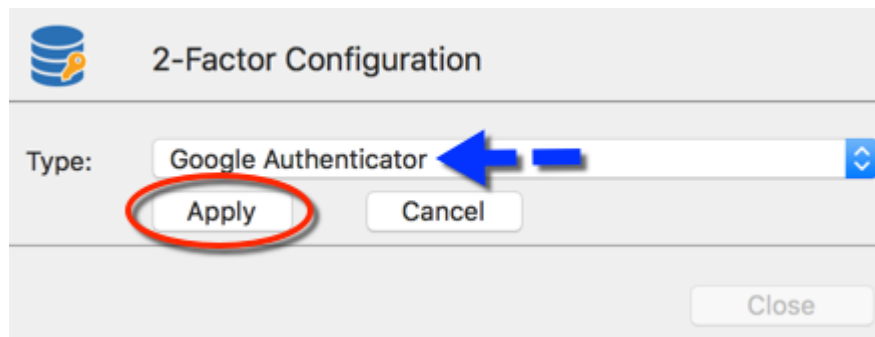
Remote Desktop Manager for Mac allows you to use **Google Authenticator** as a [2-Factor authentication](#) to provide an additional security layer when opening a data source.

SETTINGS



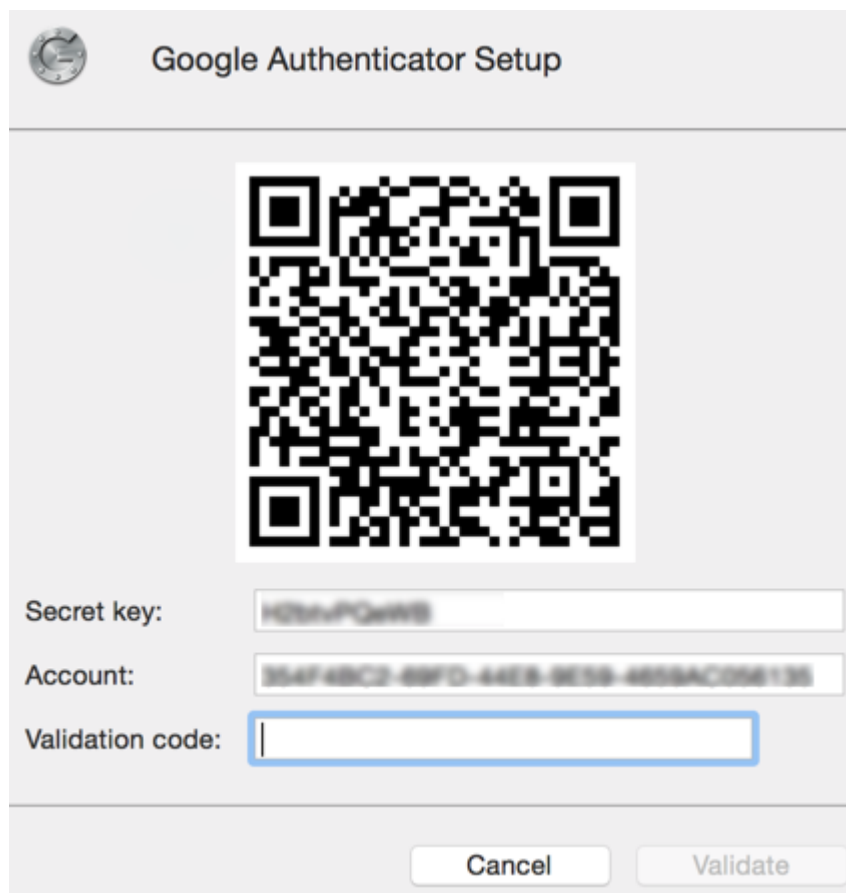
Before you start the configuration, make sure you have installed the [Google Authenticator](#) application on your Android device, Blackberry or on your Apple product (iPhone, iPad or iPod Touch).

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



2-Factor Configuration - Google Authenticator

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



Google Authenticator Setup

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



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

5.5.2 Yubikey

DESCRIPTION

Remote Desktop Manager for Mac allows you to configure a Yubikey as a [2-Factor authentication](#) to provide an additional layer of security when opening a selected 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, click on **Apply**.

2-Factor Configuration

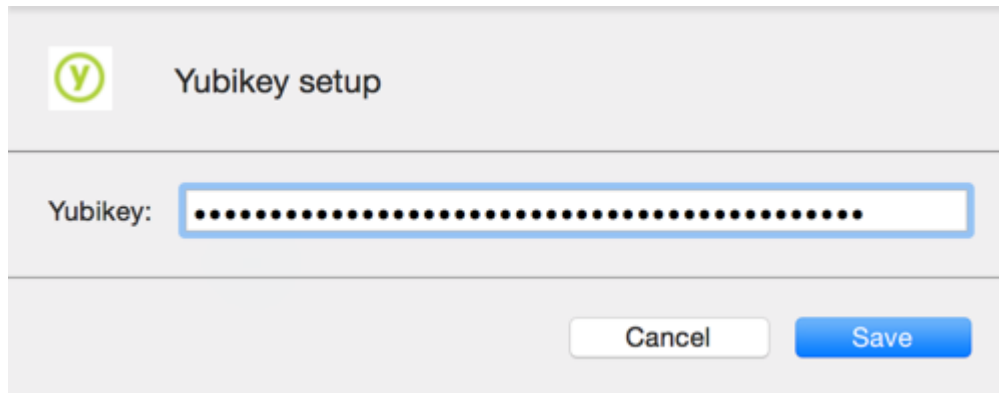
Type: Yubikey

Apply Cancel

Close

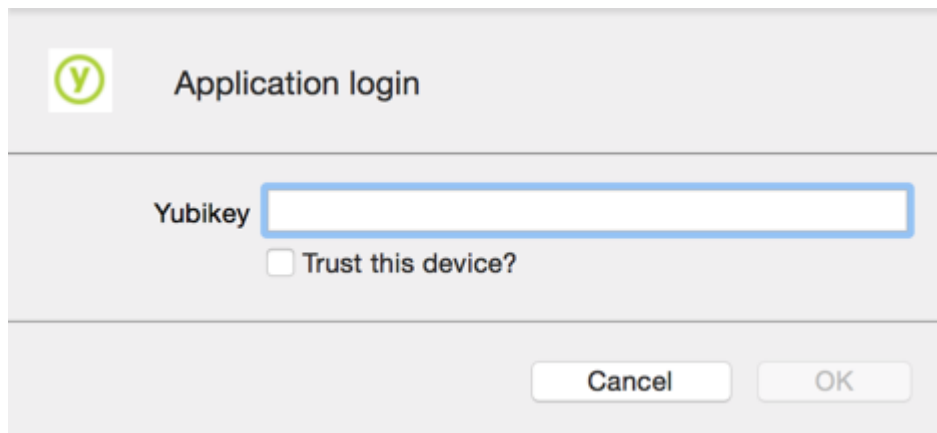
2-Factor Configuration

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 and click on **Save**.



Yubikey Authentication

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



Yubikey Application login

5.5.3 Duo

DESCRIPTION

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

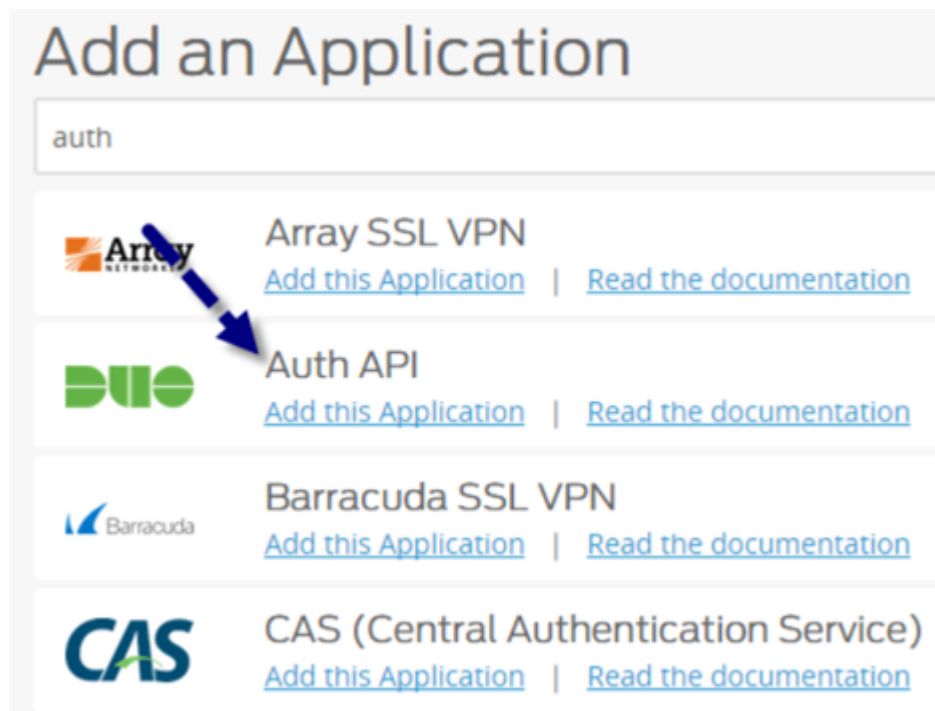
SETTINGS



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 are three methods to use the authentication with Duo: by land line, by text message or with their application.

1. Before starting, you will need to add the application **Auth API** from your Duo account.



Add Application - Duo

2. In Remote Desktop Manager for Mac select your Data source and in the Two Factor option click on **None** to change your Two factor Authentication mode. In the next window click on **Change**.

Connection Advanced Upgrade

Name: DevWind

Server: vwindsrv-sql
(Local) or IP or Server name

☐ Integrated security (Active Directory)

User: David ☐ Editable

Domain:

☒ Save password

Password:

Database: new Browse...

Two factor: None

Test Server

Test Database

ID: 354F4BC2-8BFD-44E8-9C58-4B5BAC08135

Cancel OK

SQL Connection Settings

3. Select Duo as your Two factor authentication. And then click on **Apply**

2-Factor Configuration

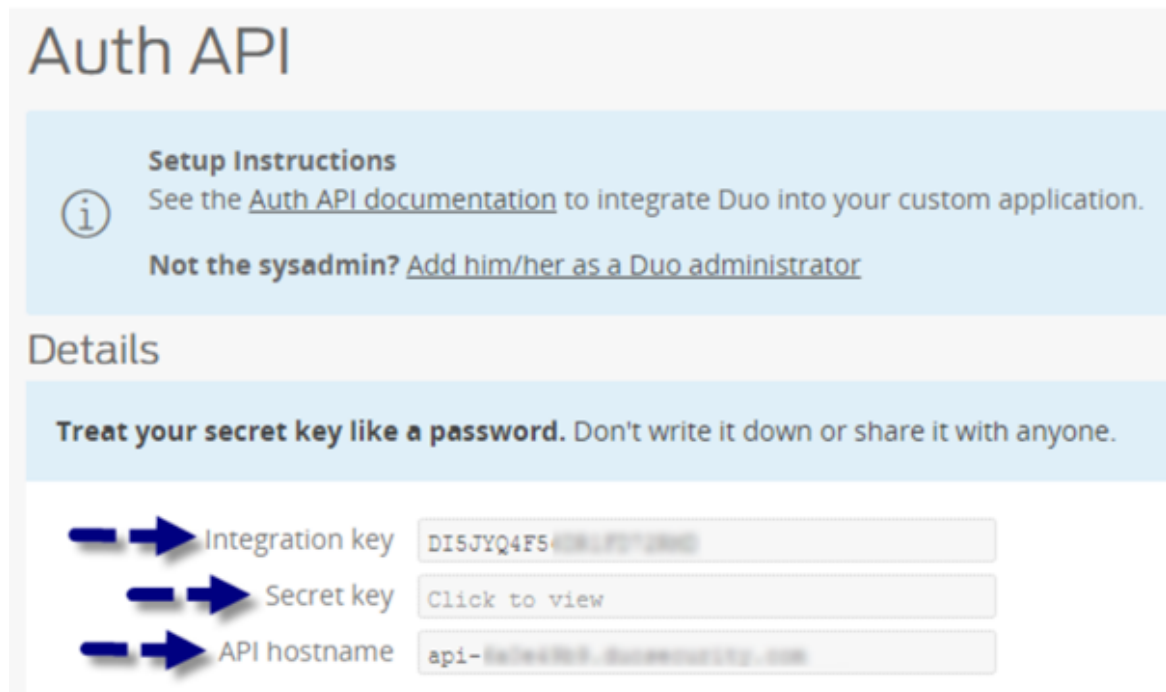
Type: Duo

Apply Cancel

Close

2-Factor Configuration

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



The image shows a web interface titled "Auth API". It has a light blue header. Below the header, there is a section titled "Setup Instructions" with an information icon (i) and text: "See the [Auth API documentation](#) to integrate Duo into your custom application." Below this, it says "Not the sysadmin? [Add him/her as a Duo administrator](#)".

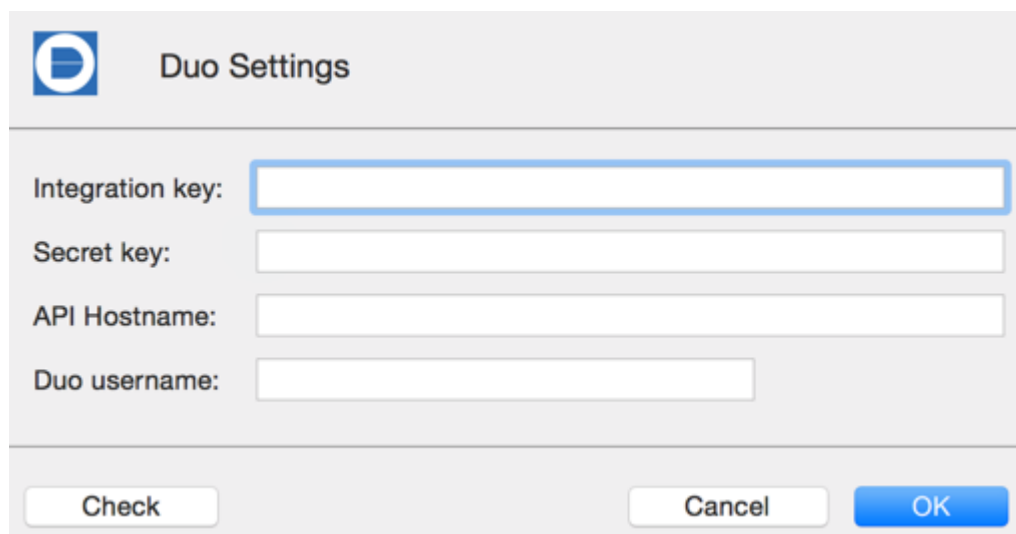
Below the instructions is a section titled "Details" with a light blue background. It contains the text: "Treat your secret key like a password. Don't write it down or share it with anyone."

Below the details section are three rows of configuration fields, each preceded by a blue arrow pointing right:

- Integration key:
- Secret key:
- API hostname:

Auth API from Duo account

5. Copy and paste all the information in Remote Desktop Manager for Mac and click on **Check** to validate the information.



The image shows a "Duo Settings" dialog box. It has a title bar with a Duo logo and the text "Duo Settings". Below the title bar, there are four text input fields:

- Integration key:
- Secret key:
- API Hostname:
- Duo username:

At the bottom of the dialog box, there are three buttons: "Check", "Cancel", and "OK".

Duo Settings

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

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.

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

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

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

5.6 Caching

DESCRIPTION

The caching mode will determine 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 using an [Advanced Data Source](#).

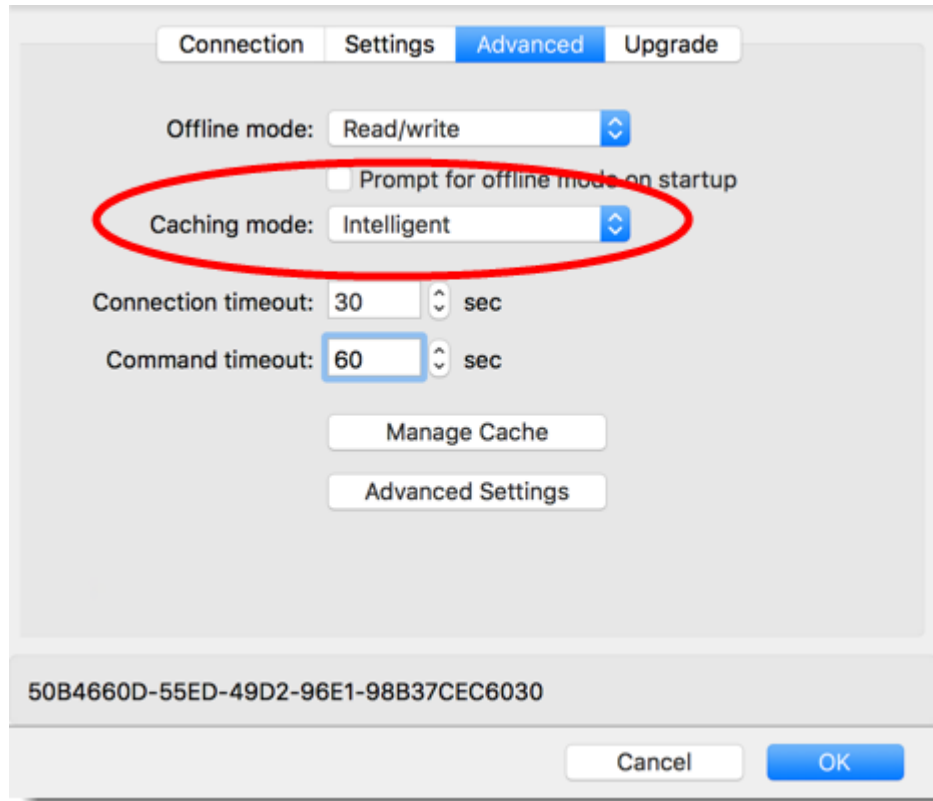


If the cache is outdated, press CTRL+Refresh or CTRL+F5 to refresh the local cache. This will force reading from the database to recreate the cache.

SETTINGS

The **Caching** mode option can be access via the **File - Data Sources - Edit Data Source - Advanced** tab of an [Advanced Data Source](#).

MODES



Data source settings - Advanced tab

OPTION	DESCRIPTION
Disabled	No client caching.
Simple	<p>Simple caching is the legacy caching mode. Performance may suffer when connected to data sources containing many sessions.</p> <p>On a modification of data within a data source the server cache token is changed. When Remote Desktop Manager for Mac performs a refresh it will compare it's local cache token with the data source token.</p>
Intelligent	Intelligent cache has the ability to handle many more sessions without experiencing performance degradation.

OPTION	DESCRIPTION
	<p>In the case of intelligent cache each modification performs a token update on the server. When Remote Desktop Manager for Mac 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 for Mac will load the session from the offline file then refresh to get the up-to date information.</p>

STORAGE

You can find the configuration file by doing a right click on your **Finder - Go to Folder** and in the Folder dialog type `~/Library`.

You can then follow the path **Application Support/com.devolutions.remotedesktopmanager** select the pertaining database where you will find the **offline.db** file.

The file is a SQLite database encrypted using a non-portable computed key hash.



You can enhance the security of the offline file by setting the Enhanced security in the **Data Sources Preferences - [Offline Security](#)**.



Depending on the configuration of the Caching Mode and of the Offline Mode the Offline.db file may still exist since the file has as a dual purpose caching and offline line support.

5.7 Manage Cache

DESCRIPTION

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



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



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

SETTINGS



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

Manage Cache

Connections rows :
Database version :
CacheID :
Offline expiry date :
Settings :

Properties
=====

Key	Value

Clear output Analyse Vacuum Repair Delete

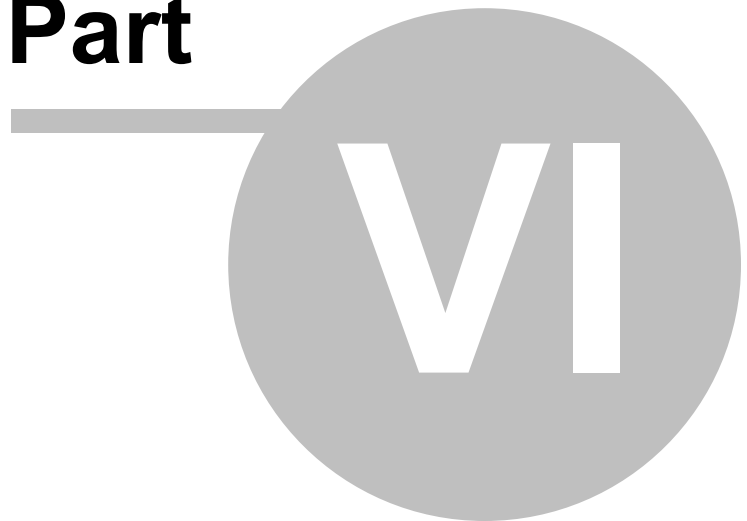
Close

Manage Cache

OPTION	DESCRIPTION
Clear output	Clear the output window.
Analyse	Analyse 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.
Vacuum	This will run an SQLite command to reduce your cache size. The Vacuum should only be used <i>after trying to execute a Repair</i> of your cache. If the repair hasn't solved your issue running a Vacuum will usually solve issues when dealing with a corrupted cache.
Repair	<p>The repair will run four different SQLite commands to repair a corrupted cache:</p> <ul style="list-style-type: none">• PRAGMA integrity_check• REINDEX DatabaseInfo• REINDEX Connections• REINDEX Properties
Delete	This option will delete the physical file (offline.db). Please not that this will <u><i>empty your Offline mode cache, always verify that your database is available before running a Delete.</i></u>

Commands

Part

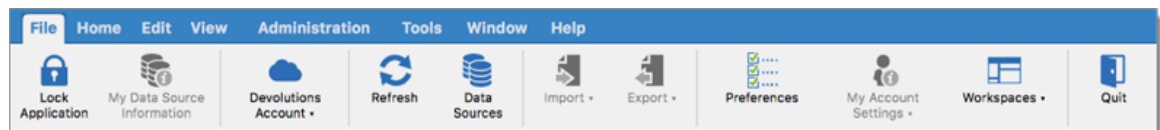


6 Commands

6.1 File

DESCRIPTION

The **File** menu contains several actions available to you regarding your data source. The options will change depending on the data source you are currently using.



File Menu

See the following topics to learn more about each setting:

- [Go Offline](#)
- [Lock Application](#)
- [My Data Source Information](#)
- [Devolutions Account](#)
- [Refresh](#)
- [Data Sources](#)
- [Manage Passwords](#)
- [Import](#)
- [Export](#)
- [Preferences](#)
- [My Account Settings](#)
- [Templates](#)

6.1.1 Go Offline

DESCRIPTION

Go offline connects to a local copy of the data source when the data source is not available. It can be used when a user is working from a disconnected network or when there is any kind of connectivity issues with the data source.



There are settings in both the data source and the user account that may prevent you from using the Offline Mode. Ask your administrator if the menu is not visible.



There are security considerations to take into account when enabling the Offline Mode.

Remote Desktop Manager will prompt for offline mode when the application is unable to reach the data source.

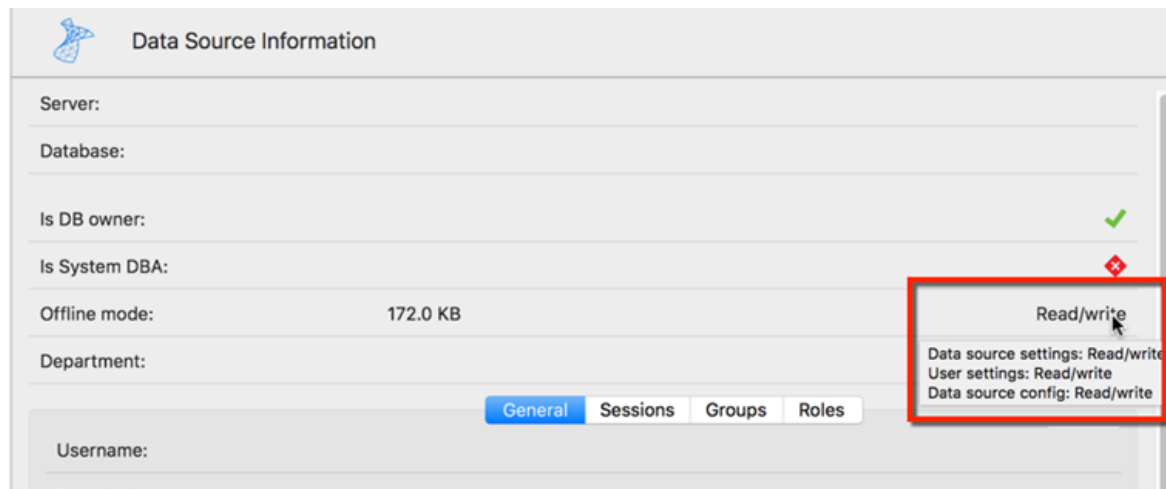
You can manually activate the offline mode by using the menu **File - Go Offline**. When the connection is back online use the menu **File - Go Online** or the **Refresh** icon to reconnect to the data source.

Some options will not be available in the Offline mode:

- Documents.
- Attachments and logs.
- [User management](#) (Add/Edit/Delete users).

OFFLINE MODE

In the **Data Source** tab of the **My Data Source Information** the offline mode displays the size of the offline file along with the effective mode (disabled, read-only or writable). Hover the mouse over the offline mode to get the full offline mode display.



My Data Source Information - Offline Mode

6.1.2 Lock Application

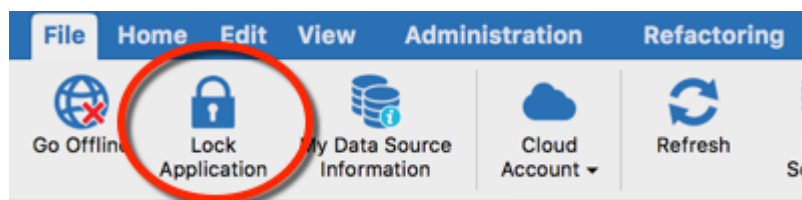
DESCRIPTION

The **Lock Application** button allows you the possibility to lock the application for security reasons when you're not in front of your computer.

SETTINGS

The **Lock Application** button is only available when a password has been setup to open the application. You can setup an application password in [File - Preferences - Security](#).

When a password has been setup, you can click on the **Lock Application** button to lock the application.



File - Lock Application

To unlock or open the application, the application password is required.



6.1.3 My Data Source Information

DESCRIPTION

Use the **File - My Data Source Information** to display the data source information details like the current username and security access. The **My Data Source Information** screen will also give you the data source configuration information such as database version and the effective Offline mode.



The display of My Data Source Information can be different depending on the [Data Source Types](#).

SETTINGS

GENERAL

The screenshot shows a window titled 'Data Source Information' with a blue icon of a person. It contains several fields for configuration:

- Server:
- Database:
- Is DB owner: (checked with a green checkmark)
- Is System DBA: (unchecked with a red X)
- Offline mode: (Read/write)
- Department: (...)

Below these fields is a tabbed interface with four tabs: 'General' (selected), 'Entries', 'Security Groups (Legacy)', and 'Roles'. The 'General' tab contains:

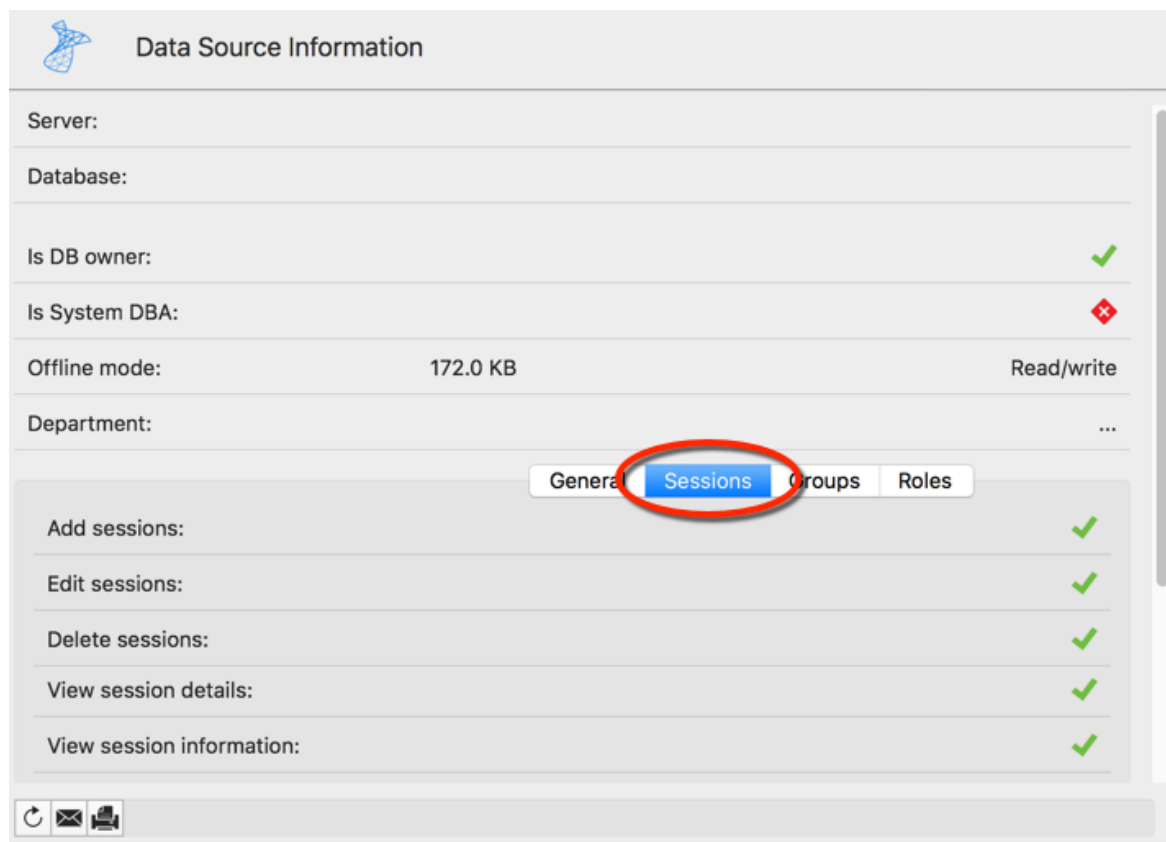
- User:
- Description:
- Is administrator: (checked with a green checkmark)
- Allow offline mode: (checked with a green checkmark)
- Allow drag-and-drop: (checked with a green checkmark)

My Data Source Information - General tab

The **General** displays information on the data source such as:

- Username
- Description
- Is administrator
- Allow offline mode
- Allow reveal password
- Allow drag-and-drop

SESSIONS



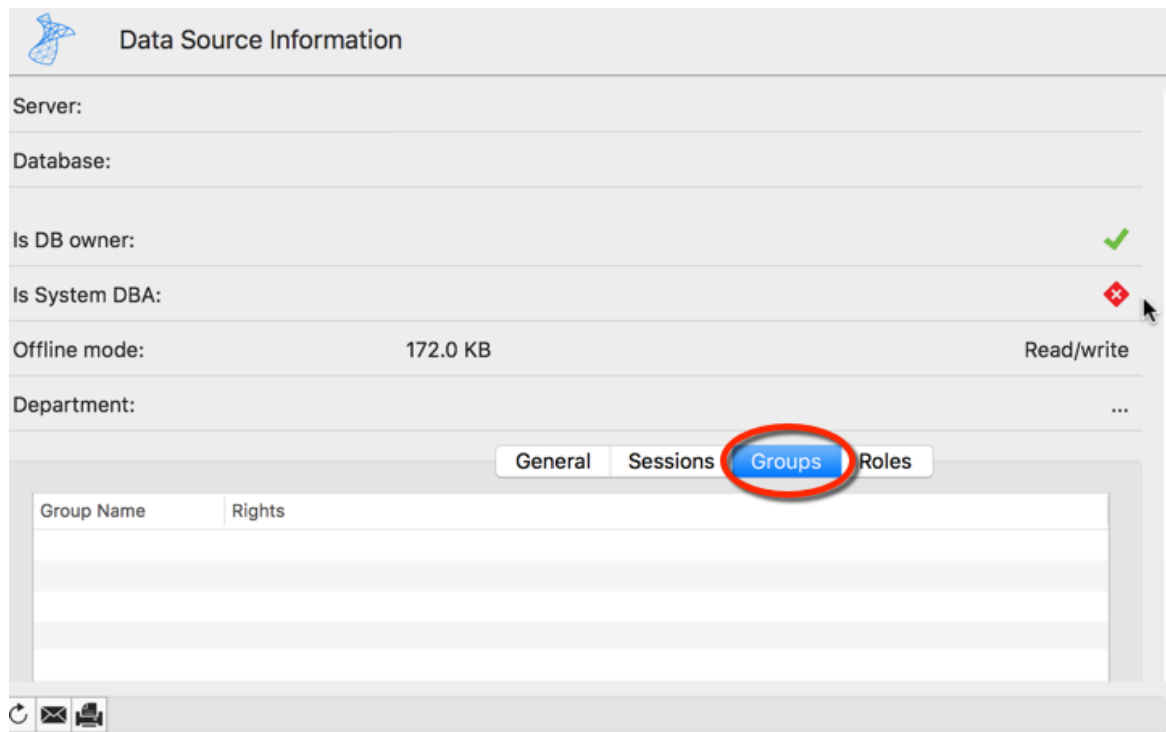
My Data Source Information - Sessions

The **Sessions** tab will display user rights on the sessions such as:

- Add sessions
- Edit sessions
- Delete sessions
- View session details
- View session information
- Import sessions
- Export sessions
- Allow add entry in root folder

GROUPS

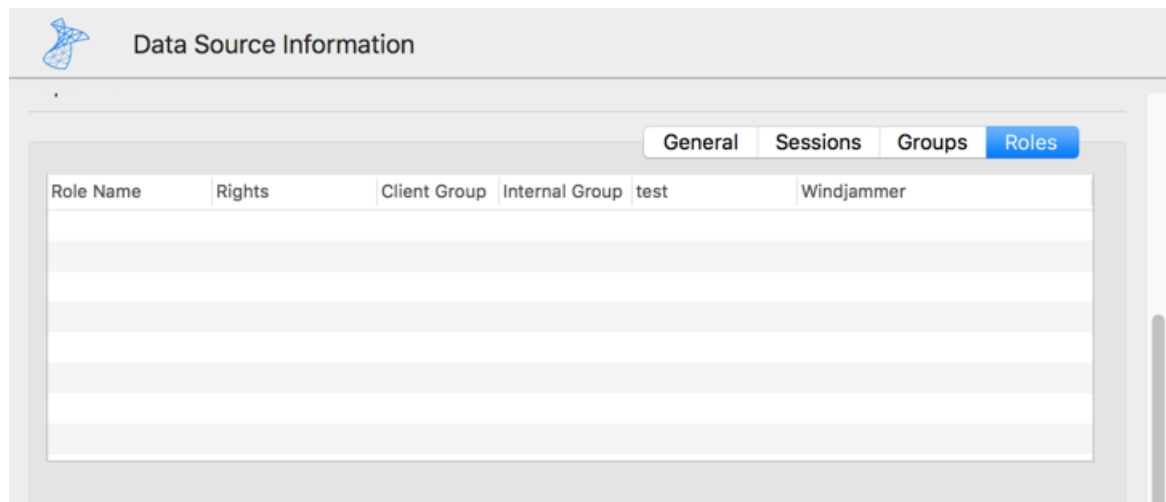
The **Groups** tab displays which rights the user has into which security groups.



My Data Source Information - Groups

USER GROUPS

The **Roles** tab displays the roles that the user is a member of and the rights related to those roles.

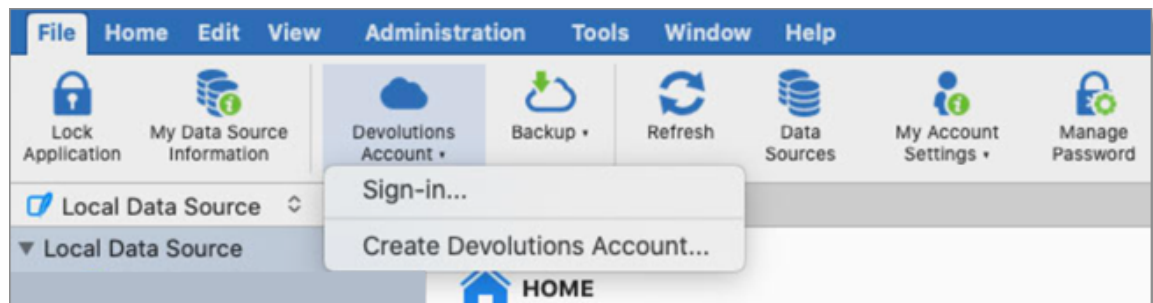


Data Source Information - Roles

6.1.4 Devolutions Account

DESCRIPTION

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



File - Devolutions Account

OPTION	DESCRIPTION
Sign-in	Sign-in your Devolutions Account.
Sign-out	Sign-out of your Devolutions Account.
Create Devolutions Account	Create a new Devolutions Account.

6.1.5 Backup

DESCRIPTION

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

6.1.5.1 Refresh

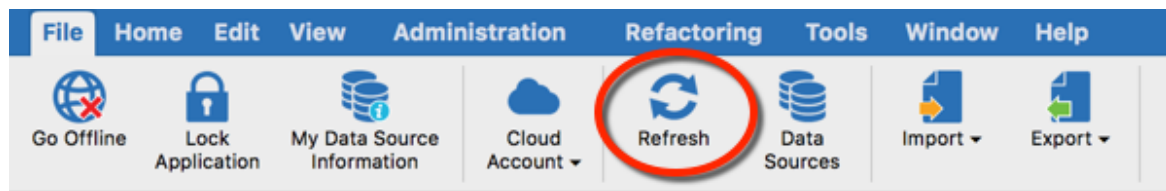
DESCRIPTION

Use **File - Refresh** to refresh your data source information. Performing a refresh will assure you that your data source is up to date.

A Refresh may also help when experiencing [Cache](#) issues.

SETTINGS

You can also perform a refresh of your data source by holding the Command plus R button.



File - Refresh

6.1.5.2 Settings

DESCRIPTION

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

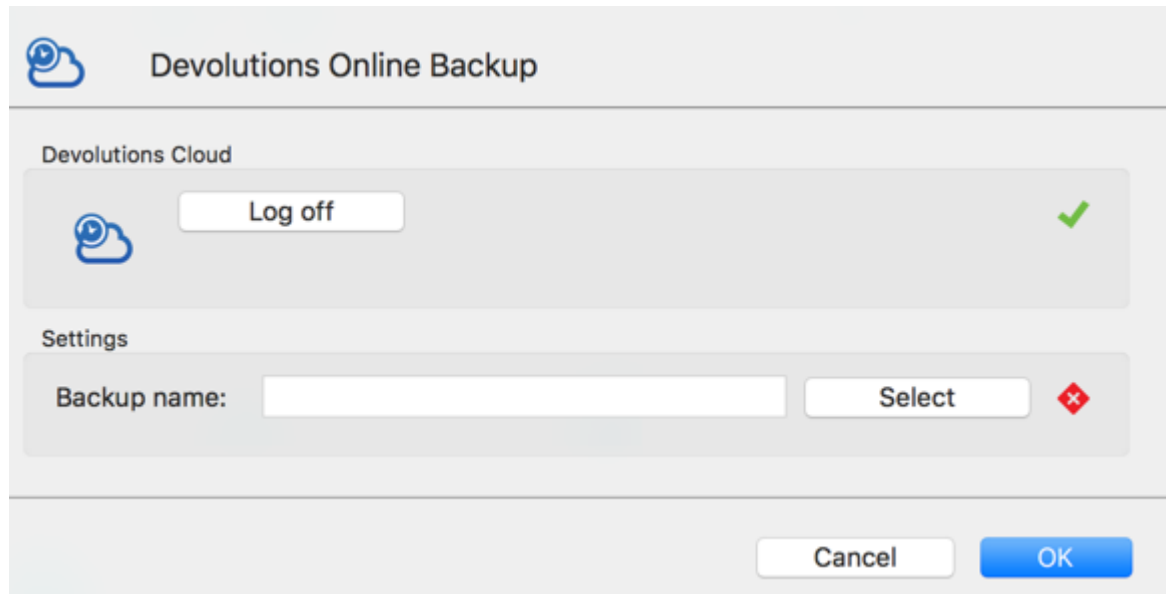
SETTINGS

SIGN IN

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

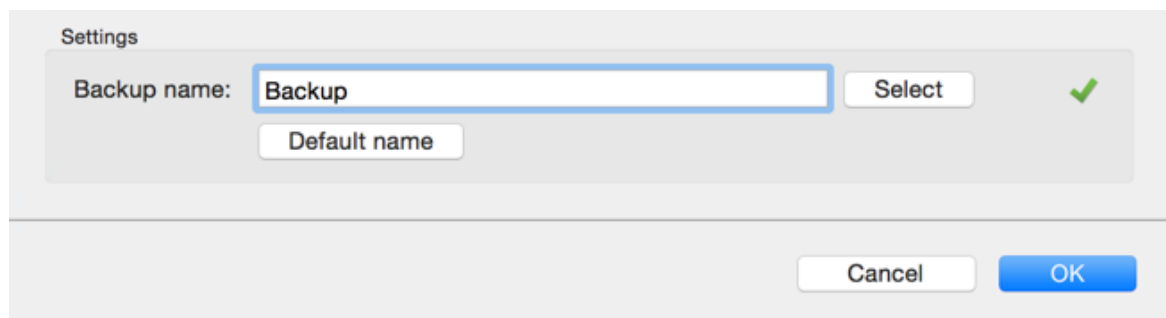
VIEW SUBSCRIPTION

- Click on **File - Backup - View Subscription** to activate your Online Backup subscription.



Online Backup subscription

- Specify a unique backup name, for each of your desired data source, which will be used to backup and restore the data source.



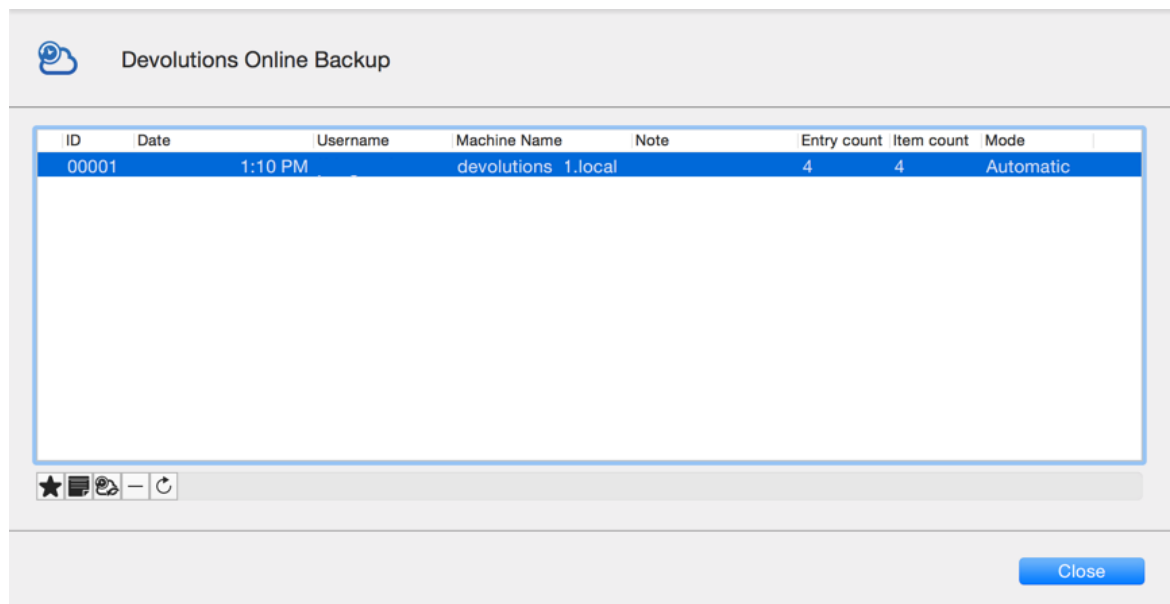
Backup name

EXECUTE BACKUP

- Once the backup name has been set, perform a change in the data source to properly activate the Online Backup and then click on **File - Execute Backup**.

VIEW HISTORY

- Click on **File - Backup - View History** to validate that the Online Backup has been configured properly



View History



You must perform this for all your [SQLite](#) or [XML](#) data source in order to be fully secured.



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

6.1.5.3 Restore

DESCRIPTION

You may need to restore a backup of your [Devolutions Online Drive](#), [SQLite](#) or an [XML](#) data source at some point. The restore option is accessible from the menu **File - Backup - Restore**.

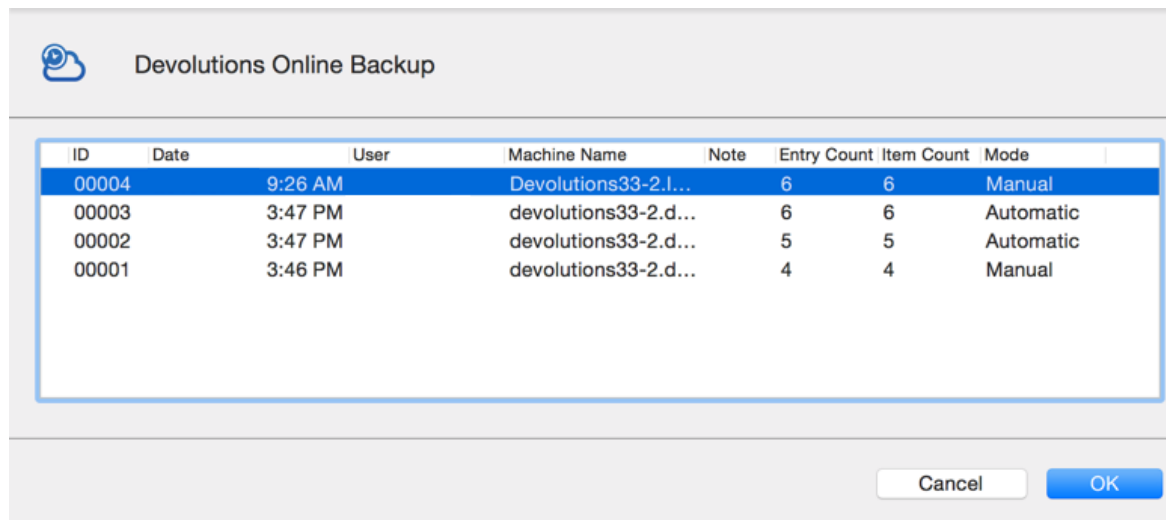


Before being able to restore a backup, you **MUST** create an empty data source and define the backup name before being able to use it. A quick step is written below:

- Create a new [Devolutions Online Drive](#), [SQLite](#) or an [XML](#) data source in **File - Data Sources**.

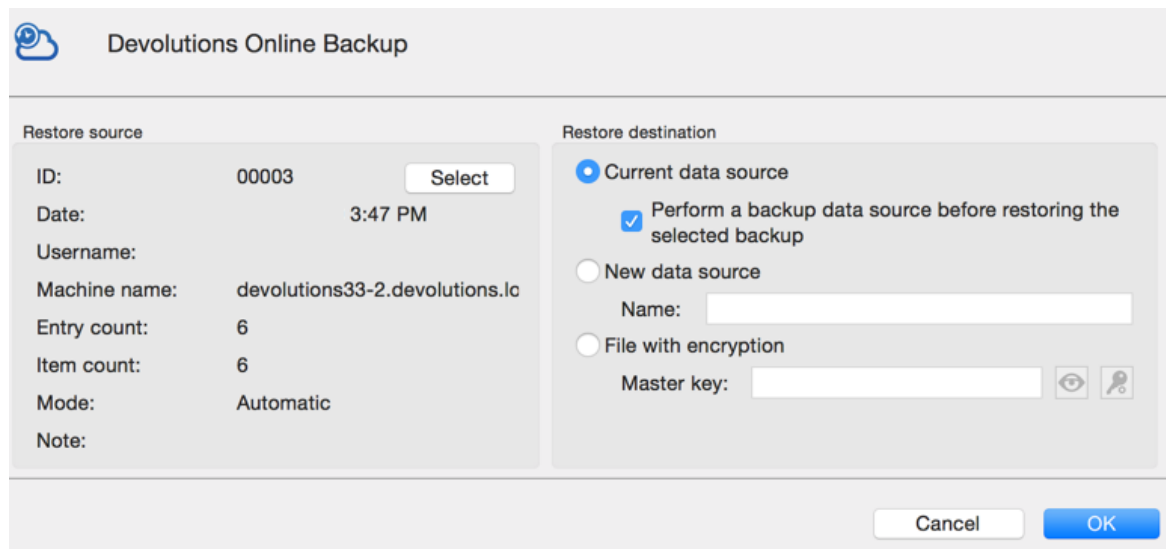
SETTINGS

1. To restore a data source from a backup, select it as the current data source.
2. Click on **File - Backup - Restore** to display the list of all your backup.



Devolutions Online Backup

3. Select the backup you want to restore and click on **OK**.
4. The Online Backup wizard will display a brief description of the backup as well as the restore destination.

*Backup Wizard*

5. Click on **OK** to complete your backup restore.

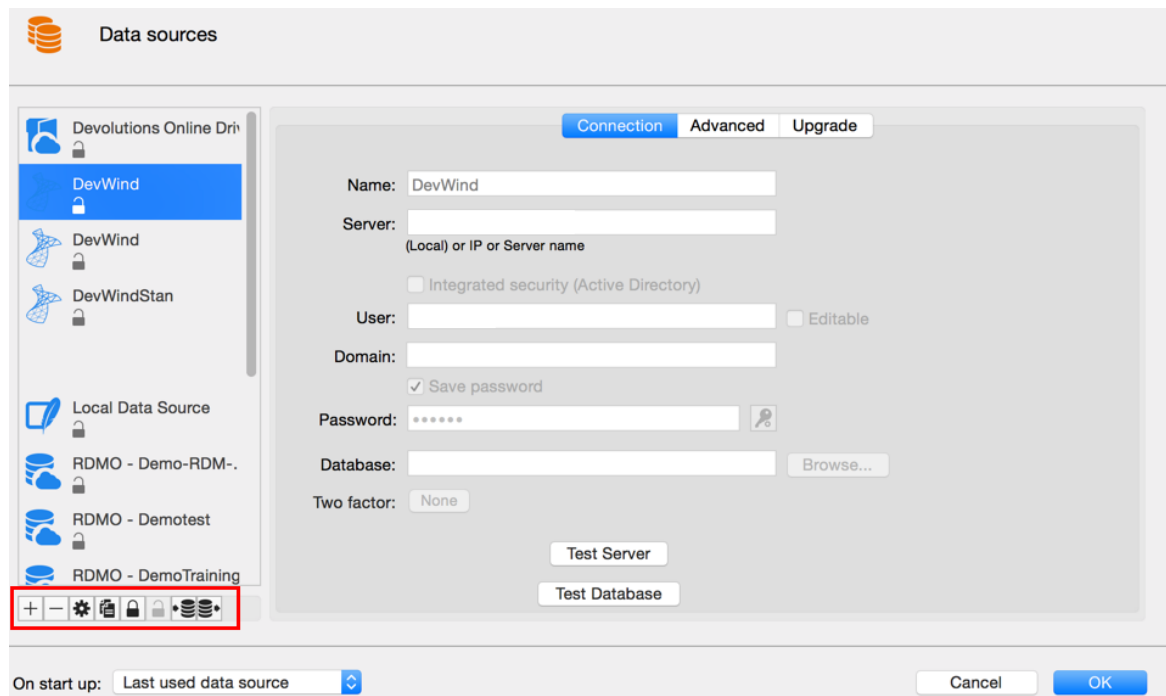
6.1.6 Data Sources

6.1.6.1 Overview

DESCRIPTION

Use **File - Data Sources** to manage your data sources. Remote Desktop Manager for Mac supports multiple types of data sources however some of them are only available in the Enterprise edition.


Please refer to the topic [Data Source Types](#) for more details on all of our supported data sources.





Your active Data sources

SETTINGS

ADD A NEW DATA SOURCE

Use the button  to create a new data source configuration.


DELETE AND EDIT A DATA SOURCE

Use buttons   to delete or edit a data source configuration.




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


DUPLICATE DATA SOURCE

Use the button  to duplicate a data source configuration.

LOCK DATA SOURCE

Use the Lock button  to lock the data source with a password to prevent any modification of a data source configuration. This is useful when you have some sensitive credentials that you don't want to share with the user.

UNLOCK DATA SOURCE

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

IMPORT DATA SOURCE

Use the Import button  to import a data source.

EXPORT DATA SOURCE

Use the Export button  to export one of your data source.

ON START UP

Remote Desktop Manager for Mac will automatically open the last used data source on startup **or** you can set a selected data source to open on startup.

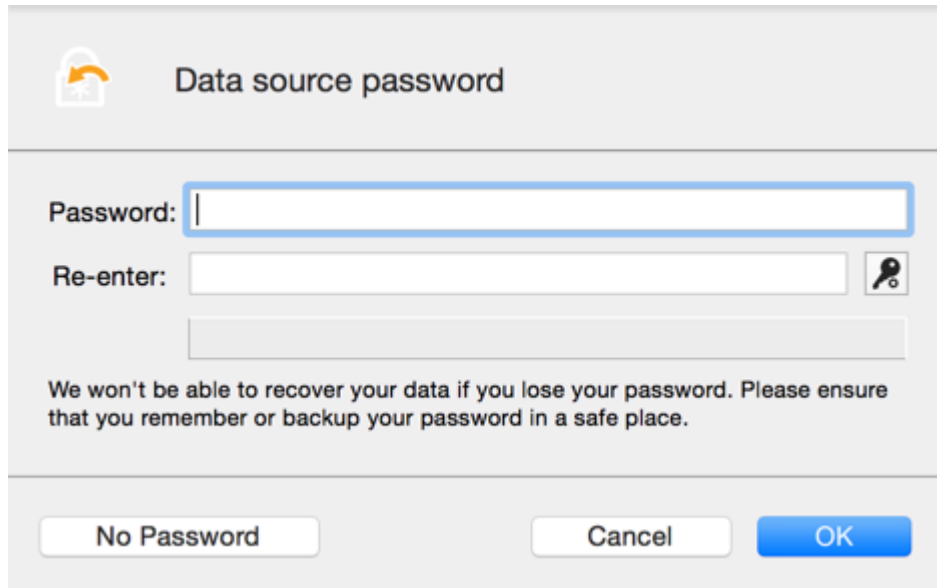
6.1.7 Manage Password

DESCRIPTION

You can apply a Master Key to encrypt the data files of the following data source:

- [XML](#)

- [Dropbox](#)



Master Key

It is generally recommended to apply a Master Key to your XML or Dropbox Data Sources as it adds another layer of security protecting your Remote Sessions.

The use of a Master Key function will stop unauthorized users from being able to easily see/access the stored Sessions within your Data Source.



If you ever lose your master key it will be impossible for us to recover your data. Please ensure that you remember or backup your master key in a safe place.

6.1.8 Import

6.1.8.1 Overview

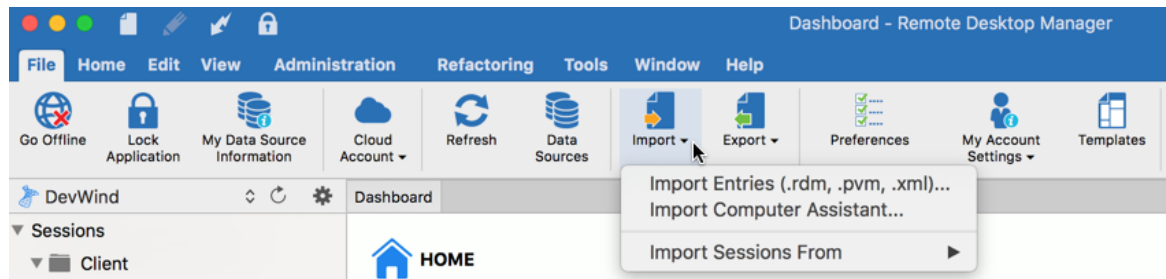
DESCRIPTION

Use the **File - Import** option to import entries in Remote Desktop Manager for Mac. You can import multiple entry types from a multitude of sources. We support native import formats from many popular tools on the market and in case we don't support the native format or the third party, we have wizards available 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)
- .xml (it must be a specific format compatible with the application)

IMPORT COMPUTER ASSISTANT

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

- Network neighborhood
- Host list

IMPORT SESSIONS FROM

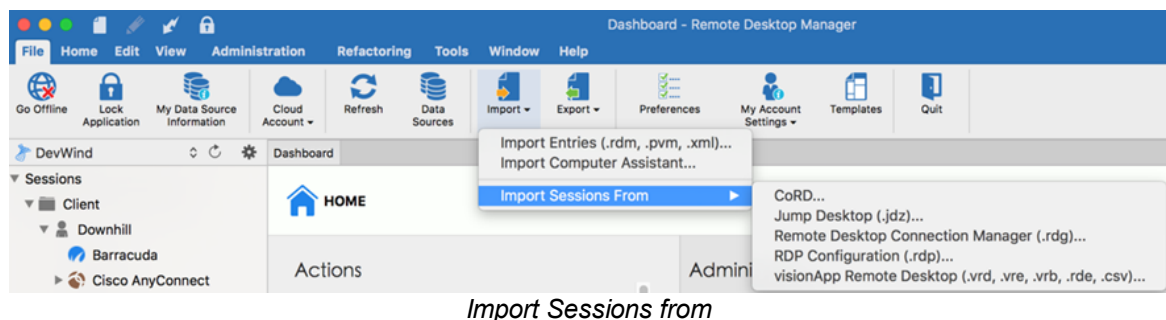
Please consult [Import Sessions](#) topic for more information.

6.1.8.2 Import Sessions

DESCRIPTION

Use the **File - Import - Import Sessions From** to import sessions into Remote Desktop Manager for Mac.

SETTINGS



Import Sessions from

IMPORT SESSIONS FROM

You can import your sessions from an existing application or an existing file format. Some application encrypt the data which makes it impossible to parse the content, therefore you must use a plain text export format. Please note that all of the entries will be imported in the current folder. For some applications it might be impossible to extract the password.

You can import sessions from the following applications:

- CoRD
- Jump Desktop (.jdz)
- Remote Desktop Connection Manager (.rdg)
- RDP Configuration (.rdp)
- visionApp Remote Desktop (.vrd, .vre, .vrb, .rde, .csv)

6.1.9 Export

6.1.9.1 Overview

DESCRIPTION

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

- Export All Entries (.rdm)
- Export Selection (.rdm)
- Export Entry as Remote Desktop File (.rdp)
- Export Special (All entries .csv, .html, .xml and All Selection (.csv, .html, .xml))

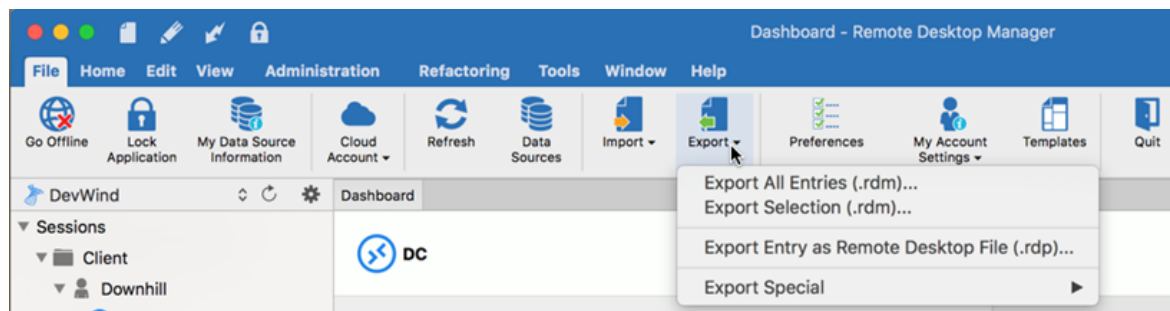


The export feature is only active if the import [Permission](#) has been enabled inside the user account



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 for Mac data source. You can also include the 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.



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.

☐ Credentials

☒ Use Master Key  

Cancel OK

Export all entries (.rdm)

EXPORT SELECTION (.RDM)

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

EXPORT ENTRY AS REMOTE DESKTOP FILE (.RDP)

Export the selected entry in a .rdp file to easily use it outside Remote Desktop Manager for Mac.

EXPORT SPECIAL (.CSV)

Export 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 SPECIAL (.HTML)

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

EXPORT SPECIAL (.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.

6.1.9.2 Export Html Encrypted

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

```

Encrypted value

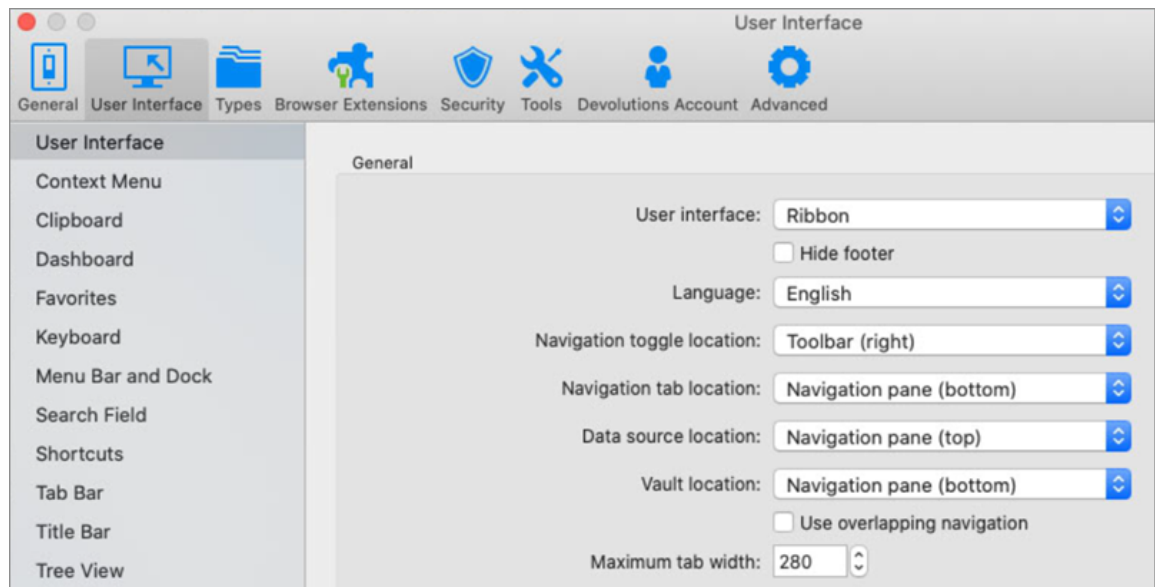
SAFE & SMART VIRTUAL BACKUP

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.

6.1.10 Preferences

DESCRIPTION

There are multiple options available to manage and customize your Remote Desktop Manager for Mac in the menu **File - Preferences**.



File - Preferences

Please see the following topics for more information each tab:

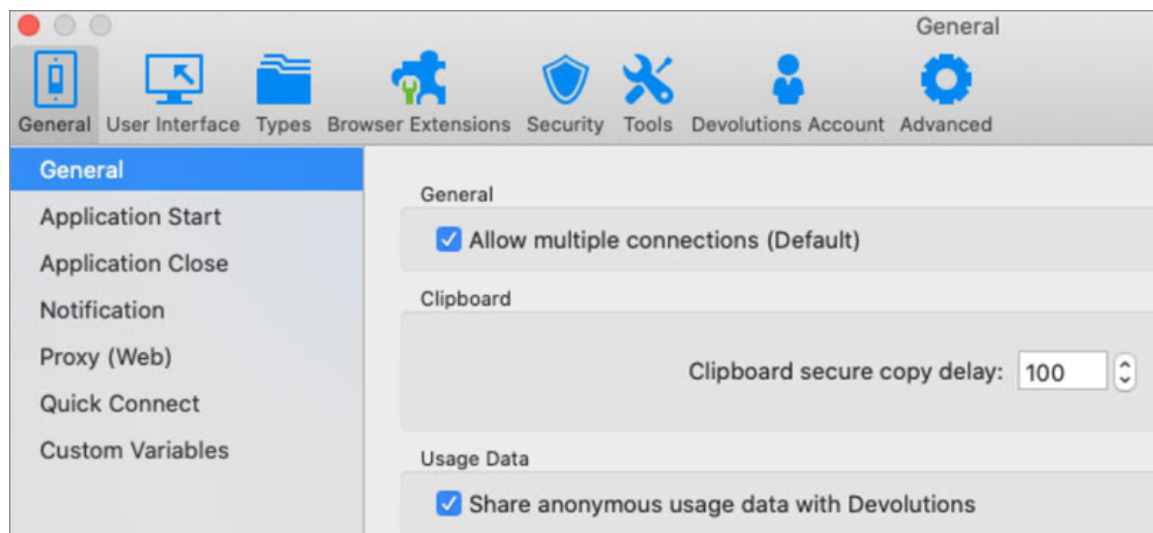
- [General](#)
- [User Interface](#)
- [Types](#)
- [Security](#)
- [Tools](#)
- [Advanced](#)

6.1.10.1 General

DESCRIPTION

Use **File - Preferences - General** to configure options related to the functionality of the application.

SETTINGS



GENERAL

OPTION	DESCRIPTION
Allow Multiple connections (Default)	Allows you to open multiple concurrent connections (tabs) within the same session. If not enabled, selecting Open Session will simply set the focus on the existing connection.

APPLICATION START

OPTION	DESCRIPTION
Check for updates at startup	Application will perform a verification for new releases available at startup.

APPLICATION CLOSE

OPTION	DESCRIPTION
Ask confirmation on application close	Application will prompt you for confirmation when attempting to close.
Verify opened session on close	Application will warn you about running sessions when attempting to close.

QUICK CONNECT

OPTION	DESCRIPTION
Open embedded by default (if available)	Open the session in embedded mode by default if the embedded mode is available.

CUSTOM VARIABLES

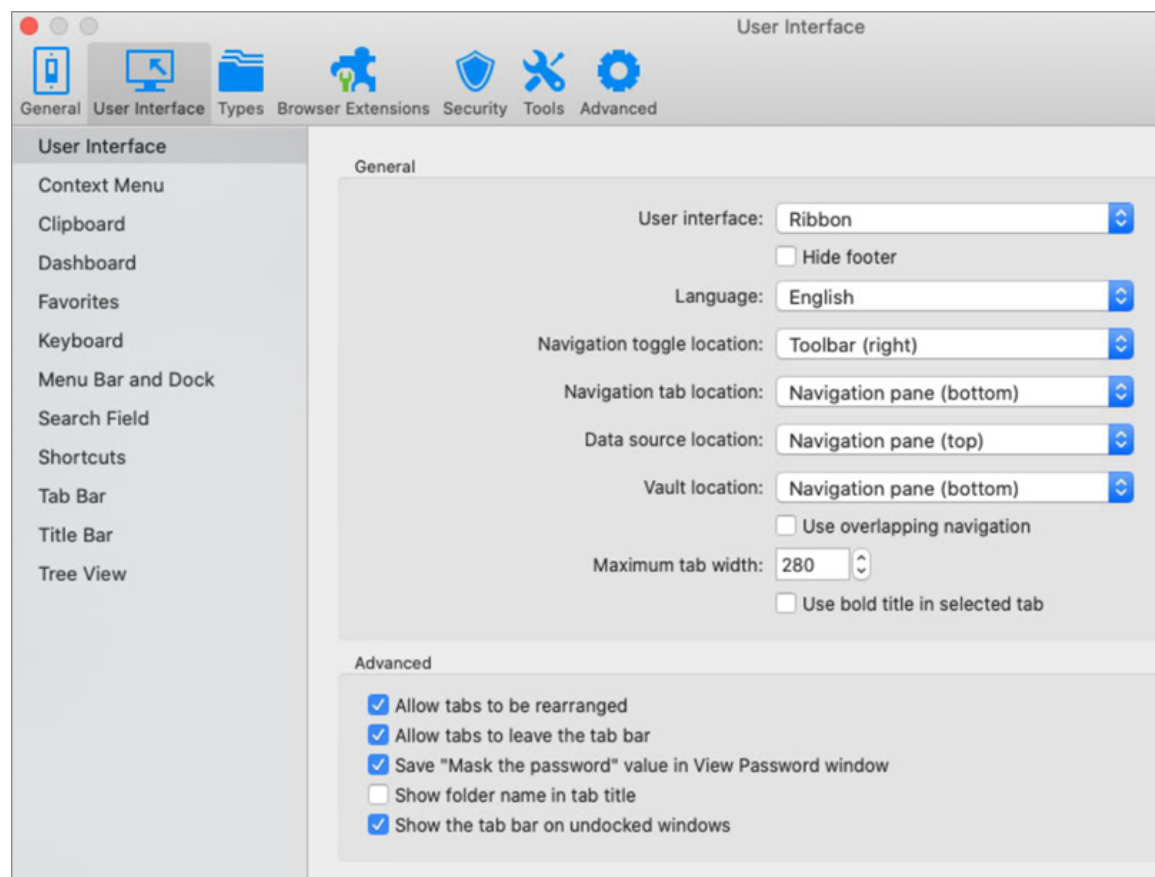
OPTION	DESCRIPTION
Custom Variables	Custom variables option has been implemented to customize your own variables in the application. Click on the plus sign to create a new variable to use. Enter the name and the value of the variable.

6.1.10.2 User Interface

DESCRIPTION

Use **File - Preferences - User Interface** to configure options related to the user interface.

SETTINGS



Preferences - User Interface

CONTEXT MENU

OPTION	DESCRIPTION
Include Properties Menu	Display the Properties menu in the context menu when a session is selected.
Use legacy edit context menu	Use the Legacy theme edit context menu (old Remote Desktop Manager interface).

USER INTERFACE

OPTION	DESCRIPTION
User Interface	Choose between the Classic and the Ribbon User Interface.
Hide footer	When using the Ribbon User Interface select this option to hide your footer.
Language	Select Remote Desktop Manager for Mac default application language.
Navigation toggle location	Specify the default location of the toolbar: <ul style="list-style-type: none">• Toolbar (right)• Toolbar (left)
Navigation tab location	Specify the default location of the Navigation tab between: <ul style="list-style-type: none">• Navigation Pane (top)• Navigation Pane (bottom)
Data Source location	Specify the location of the data source on your screen between:

OPTION	DESCRIPTION
	<ul style="list-style-type: none">• <i>Navigation Pane (top)</i>• <i>Navigation Pane (bottom)</i>• <i>Status bar</i>• <i>None</i>
Show the tab bar on undocked windows	Display the tab bar when the session is undocked.
Allow tabs to be rearranged	Allow tabs to be moved from one position to another in the tab bar.
Allow tabs to leave the tab bar	Tabs can be move out of the tab bar.

DASHBOARD

OPTION	DESCRIPTION
Auto Focus Dashboard	When option is activated if an active entry is selected in the tree view the corresponding dashboard is displayed and focus is immediately set on it.
Use classic dashboard overview	The classic dashboard will be displayed instead of the new dashboard with larger buttons.

MENU BAR

OPTION	DESCRIPTION
Show icon in menu bar	Shows the icon in the menu bar.
Include entry list menus	Includes the entries in the list menu.
Include opened entry menus	Includes a sub-menu for opened sessions.
Include Show/Hide menu	Includes a menu to show and hide certain options.
Include "Maximize" menu	Includes a menu to maximize the application window to take the full area of the screen.
Include data source menus (only if more than one)	Includes a sub-menu for the data sources. This requires more than one data source to function.
Include "Quick Connect" menu	Includes a menu to perform a Quick Connect to a host.
Include most recently used menu	Includes a menu that contain the Most Recently Used entries.
Include "Play list" menu	The Play List will appear in the menu.
Only show favorites entries in icon menu	Only the Favorite Entries will appear in the menu.
Show credentials in icon menu	Indicate if the credentials are listed in the menu.

TREE VIEW

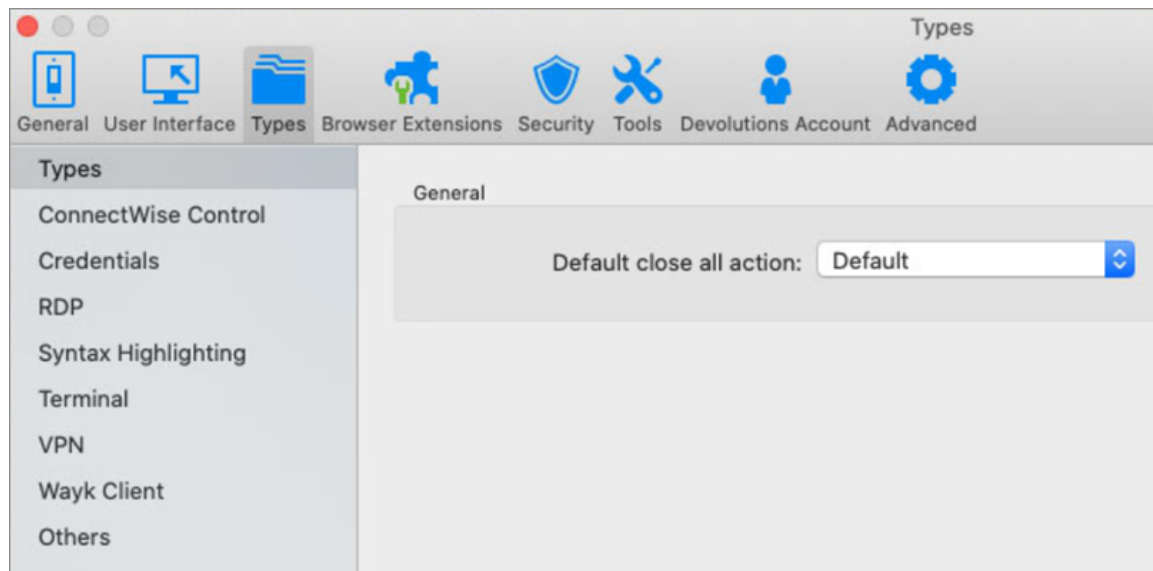
OPTION	DESCRIPTION
Shortcut overlay	Determine on which items the shortcut icon is visible. Choose between: <ul style="list-style-type: none">• <i>All</i>• <i>None</i>• <i>All except original</i>
Disable entry drag-and-drop	This setting disables moving entries with drag-and-drop. Use this option to avoid any unwanted session create by drag and drop by mistake.
Merge credential list with sessions	Credentials will appear within the list of Sessions instead of in their own vault.
Merge session tool list with sessions	Session tool list will appear within the list of Sessions instead of in their own vault.

6.1.10.3 Types

DESCRIPTION

Use **File - Preferences - Types** to control settings applied to Session entries.

SETTINGS



Preferences - Types

SESSION TYPE

OPTION	DESCRIPTION
Default close all action	<p>Select the Default action for the Close all button when multiple tabs are open at the same time in the dashboard:</p> <ul style="list-style-type: none"> • Disconnect (disconnect all opened tab connected session) • Log off (Log off all opened tab session) • Default (Close all opened tab sessions)

CREDENTIALS

OPTION	DESCRIPTION
Global Availability	<p>Define the default setting of the Global Availability for the User Vault Search between:</p>

OPTION	DESCRIPTION
	<ul style="list-style-type: none">• <i>Available</i>• <i>Unavailable</i>

RDP

OPTION	DESCRIPTION
Screen sizing mode	<p>You can choose a preferred screen sizing mode for your RDP session between:</p> <ul style="list-style-type: none">• <i>Scrollbar</i>• <i>Smart reconnect</i>• <i>Smart sizing</i>• <i>Server resolution</i>• <i>None</i>
Display	<p>Determinate the preferred display for the session. Select between:</p> <ul style="list-style-type: none">• <i>Default</i>• <i>External</i>• <i>Embedded (tabbed)</i>• <i>Undocked</i> <p>You can then choose the preferred monitor to display on:</p> <ul style="list-style-type: none">• <i>Primary monitor:</i> This is the monitor that is marked as main display in Windows

OPTION	DESCRIPTION
	<ul style="list-style-type: none">• Secondary monitor: The other non-primary monitor, obsolete, use Monitor 1, 2, 3 or 4 instead• Current monitor: The monitor that RDM is running in• Configured: See Systems Options• Default: Will not move the application, it will be Windows default mode• Monitor 1: Monitor 1 is primary• Monitor 2: Monitor 2 is primary• Monitor 3: Monitor 3 is primary• Monitor 4: Monitor 4 is primary• Monitor 5: Monitor 5 is primary• Monitor 6: Monitor 6 is primary
Activate sandboxing	The sandboxing isolate the RDP connection in another process. This is more stable and more reliable since it's an independent application embedded in RDP. This means that RDP can more easily recover from a disconnection or a fatal error.
Use OpenGL	If using OpenGL on your Mac activate this option to enhance your screen performance.
RDP Engine	Select between: <ul style="list-style-type: none">• Default• V2• V3• V4

OPTION	DESCRIPTION
Gateway Transport	Select between: <ul style="list-style-type: none">• Auto• Http• RPC

OTHERS

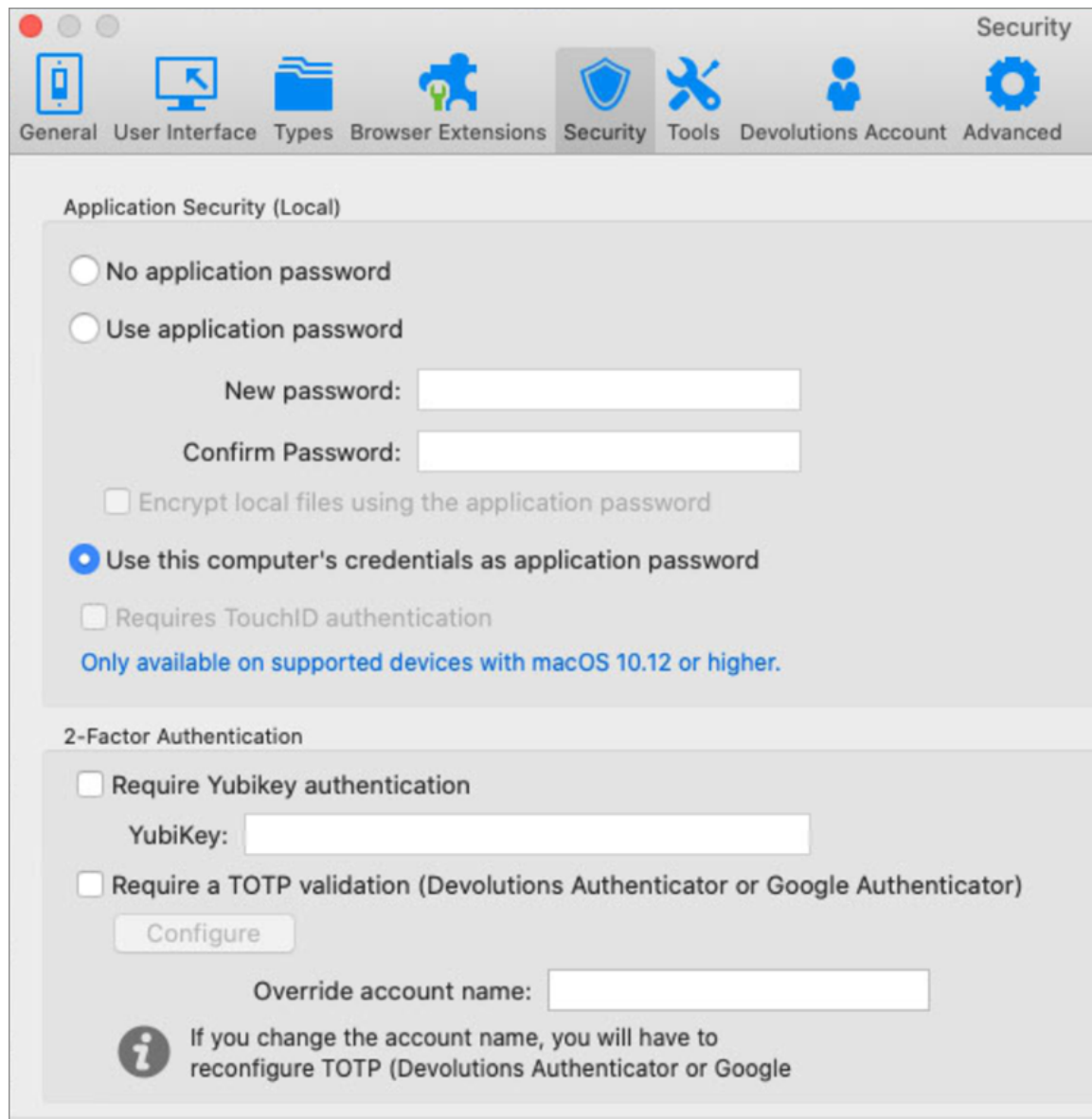
OPTION	DESCRIPTION
Screen display	When using ARD session you will be prompt to know which screen display to use. By default it will take the primary screen.

6.1.10.4 Security

DESCRIPTION

Use ***File - Preferences - Security*** to configure the security of the application.

SETTINGS

*Preferences - Security*

APPLICATION SECURITY

OPTION	DESCRIPTION
No application password	No password will be requested to access the application.

OPTION	DESCRIPTION
Use application password	Define a specific password to access the application.
Use computer credentials as application password	Requires the same credential as your computer credential to access the application.

2-FACTOR AUTHENTICATION

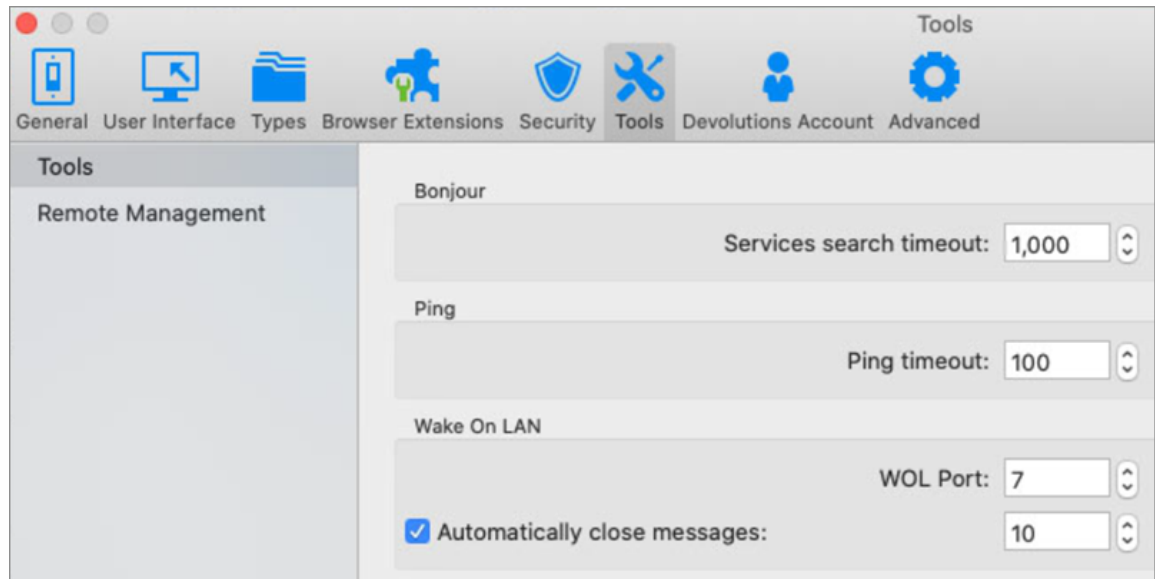
OPTION	DESCRIPTION
Require Yubikey authentication	Use a Yubikey device to get access to the application when it starts or when it's locked.
Require Google Authenticator	Use a Google Authenticator device to get access to the application when it starts or when it's locked.
Override account name	If you wish to use a different Google Authenticator account than the one previously linked to your RDM account, you could override the account name but you will have to reconfigure Google Authenticator.

6.1.10.5 Tools

DESCRIPTION

Use **File - Preferences - Tools** to configure the delay of time before the tool timeout.

SETTINGS



Preferences - Tools

TOOLS

OPTION	DESCRIPTION
Services search timeout	Indicate the time that the Bonjour service will search before the service timeout.
Ping timeout	Indicate the time before the ping service timeout.
WOL Port	Indicate the time before the Wake on LAN service timeout.
Automatically close messages	Indicate the time before the message window automatically closes.

REMOTE MANAGEMENT

OPTION	DESCRIPTION
Event Log	<p>Select the preferred event log to be open by default when launching the remote event on a remote computer:</p> <ul style="list-style-type: none">• <i>All</i>• <i>Application</i>• <i>Security</i>• <i>System</i>• <i>DFS Replication</i>• <i>Directory Service</i>• <i>DNS Server</i>• <i>Hardware Events</i>• <i>Internet Explorer</i>• <i>Key Management Service</i>• <i>Windows PowerShell</i>
Event Type	<p>Select the preferred event type to be open by default when launching the remote event on a remote computer:</p> <ul style="list-style-type: none">• <i>All</i>• <i>Error</i>• <i>Warning</i>• <i>Information</i>• <i>Security Audit Success</i>• <i>Security Audit Failure</i>
Time Range	<p>Define the time range for the Remote Event:</p>

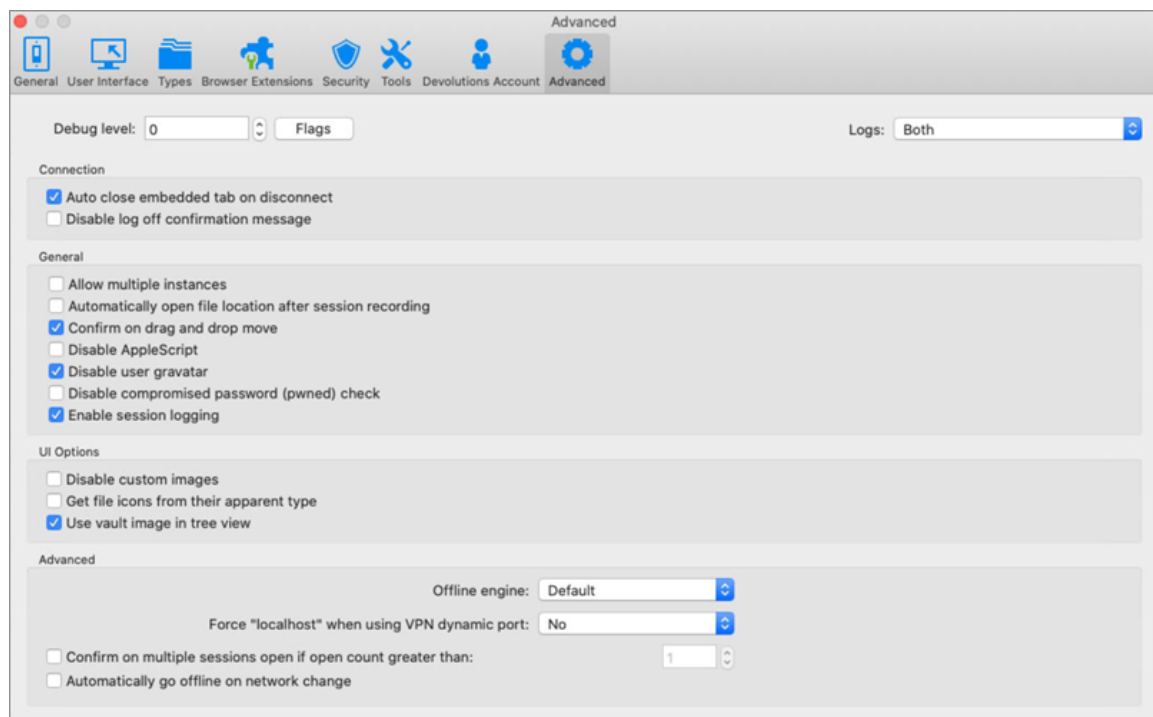
OPTION	DESCRIPTION
	<ul style="list-style-type: none">• <i>Last week</i>• <i>Today</i>• <i>Yesterday</i>• <i>Last Month</i>• <i>Current Month</i>• <i>Last 7 days</i>• <i>Last 30 days</i>• <i>Last 31 days</i>• <i>Last 60 days</i>• <i>Last 90 days</i>

6.1.10.6 Advanced

DESCRIPTION

Use ***Remote Desktop Manager - Preferences - Advanced*** to modify the advanced settings of Remote Desktop Manager for Mac.

SETTINGS



Preferences - Advanced

OPTION	DESCRIPTION
Debug level	Set the level of debugging information that Remote Desktop Manager for Mac will capture. This should only be modified upon request from a Devolutions support technician and could slow down your system.
Auto close embedded tab on disconnect	When a session is disconnected, the embedded tab will automatically close.
Disable logoff confirmation message	When pressing the logoff button in a embedded RDP session, Remote Desktop Manager, will disconnect the session without the logoff confirmation message.
Use Secret Server Legacy Interface	Enable if you wish to use the Secret Server Legacy Interface (meaning the way it used to look as oppose to it's current look).
Confirm on drag and drop move	Every time executing a drag and drop a confirmation window will be prompted to confirm the move.

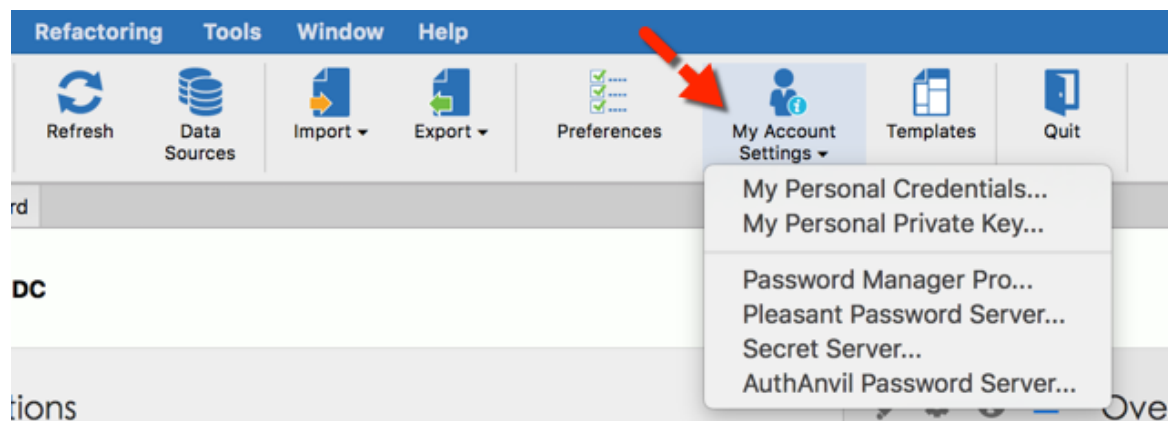
OPTION	DESCRIPTION
Disable AppleScript	AppleScript is enabled by default, if you wish you can disable it here.
Enable Action Queue	The Enable Action Queue is a default option. If you are experiencing performance issues with Remote Desktop Manager for Mac our Support team might ask you to disable the Action Queue but we wouldn't recommend doing so without a request from one of our Support team member.
Disable custom images	Disable the loading of any custom images in the tree view. Too many custom images could dramatically increase the size of the data source and increase the load time at the same time.

6.1.11 My Account Settings

DESCRIPTION

Use **File - My Account Settings** to configure different accounts that can be used to connect on different web platforms. This allow you to setup your account settings one time and use it in the creation of your entries as many time as you want. You can also manage your Personal Credentials, Personal Private Key and your User Specific Settings List.

SETTINGS



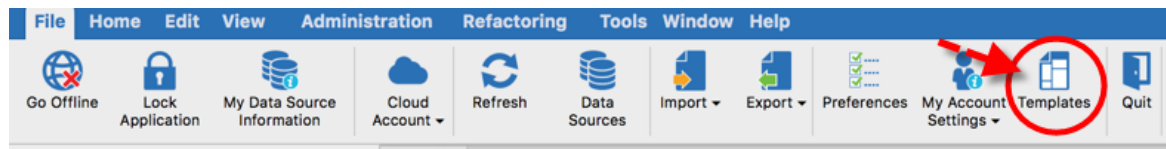
File - My Account Settings

OPTION	DESCRIPTION
My Personal Credentials	Please consult My Personal Credentials topic for more information.
My Personal Private Key	With a Personal Private Key configure, you can select My Personal Private Key in the drop down menu to use this key instead of typing your private key every time.
Password Manager Pro	Configure the username, workstation and token to connect on Password Manager Pro.
Pleasant Password Server	Configure the username and password to connect on Pleasant Password.
Secret Server	Configure the username to connect on Secret Server.

6.1.12 Templates

DESCRIPTION

Templates are available from the menu ***File - Templates***.

*File - Templates*

This allows you to create predefined configuration such as:

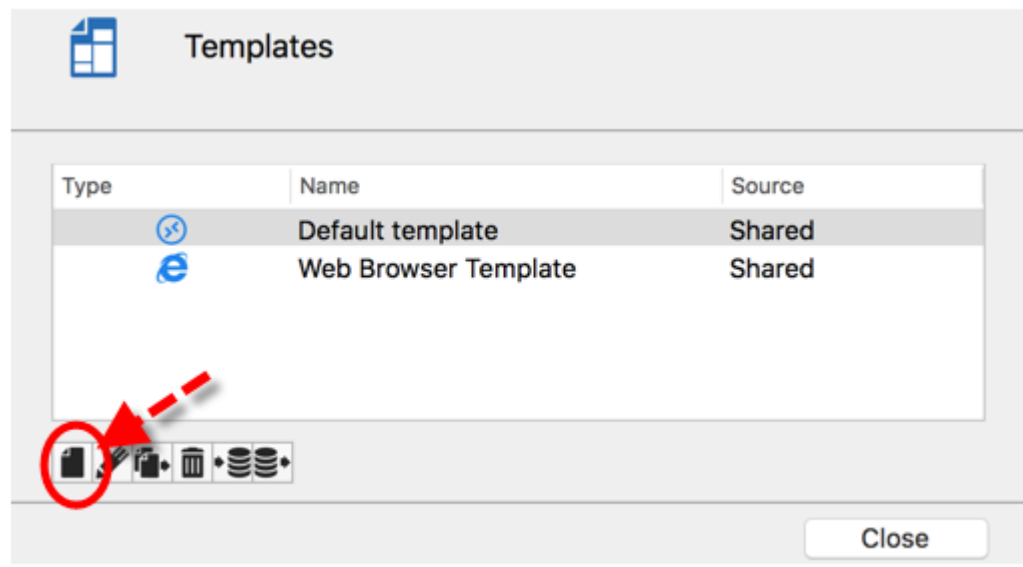
- Create a new session
- Quickly connect
- Open as a template

Templates can be useful if you want to have predefined values when you create a specific entry.

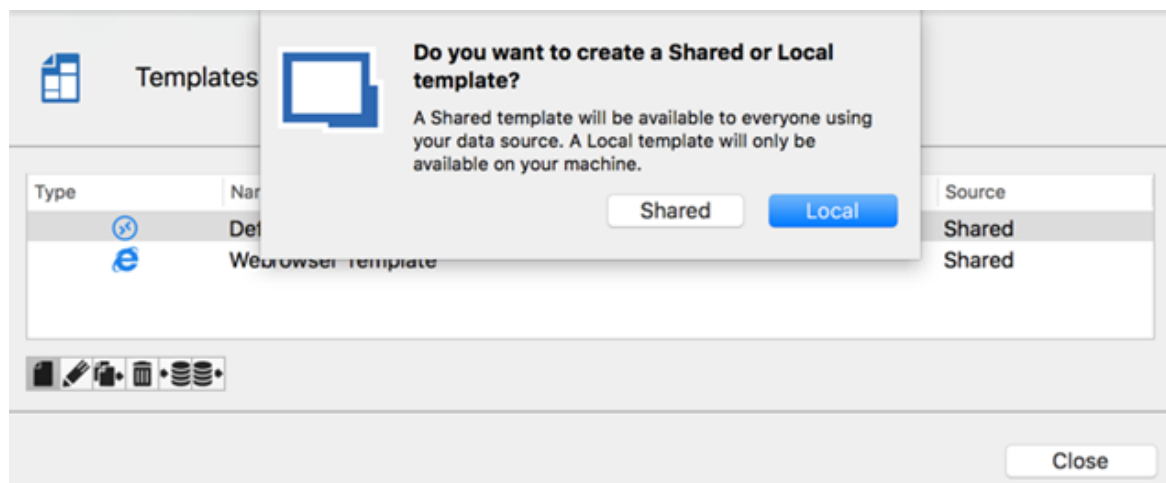
This allows you to create predefined templates that are available with the quick connect toolbar or when creating or importing a new session.

SETTINGS

Simply click on **Templates** and then click on **Add Template** to create a new template.

*Templates - Create a New Template*

You can choose to create a **Local templates** or a **Shared Templates**.



Select Shared or Local template

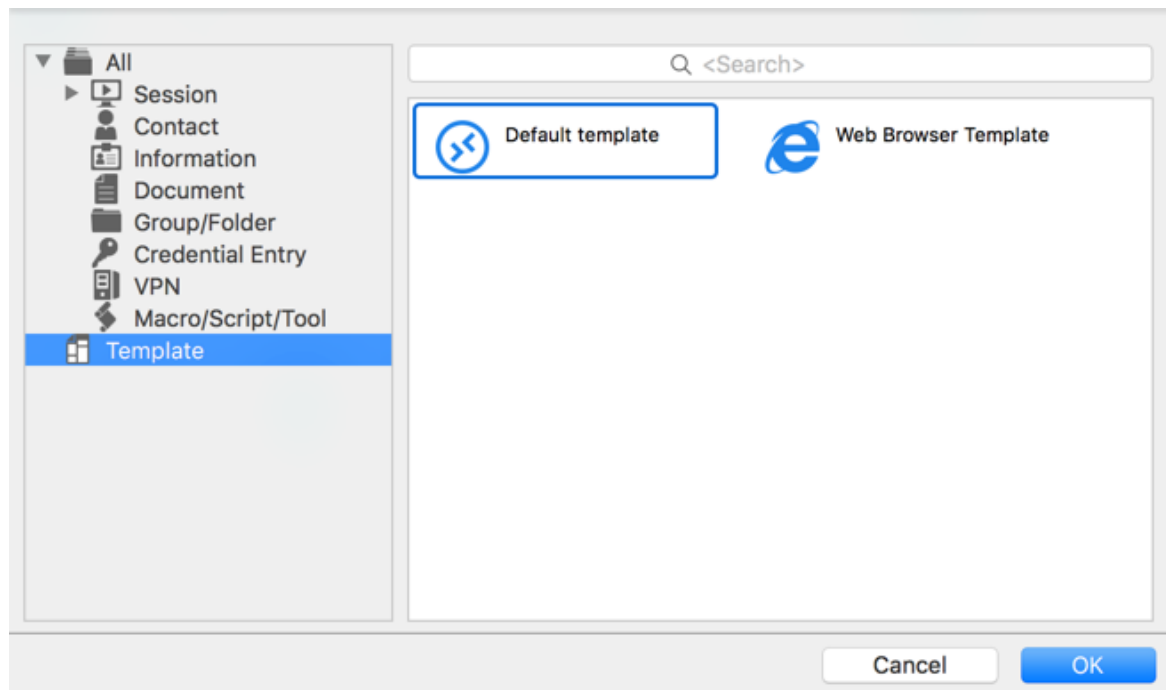
OPTION	DESCRIPTION
Local Template	Local templates are saved on the local computer and are not available to other users.
Shared Template	Shared templates are saved in the database and can be used by every users.

USAGE

Templates can be used in the following cases:

CREATING A NEW ENTRY

When creating a new entry, select **Template** to have access to your previously created template, click on the one you wish to use to create your new entry.



Create a new entry - Template

6.1.12.1 Default Settings

DESCRIPTION

You can access the default session settings from **File - Template - Default session settings**.

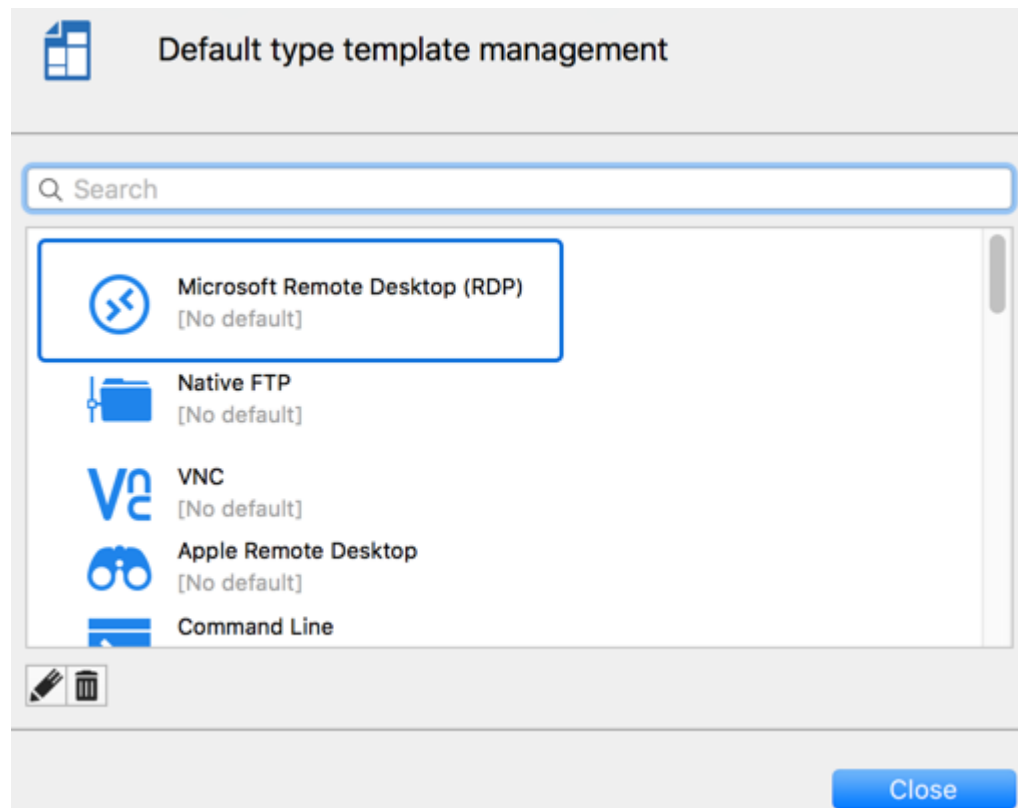
This allows you to edit or reset your default settings that are used whenever a new entry is created. Every entry type is supported and can have a default template defined.

By editing your default template you will be able to save settings often used when creating new entries.

SETTINGS

NO TEMPLATE DEFINED

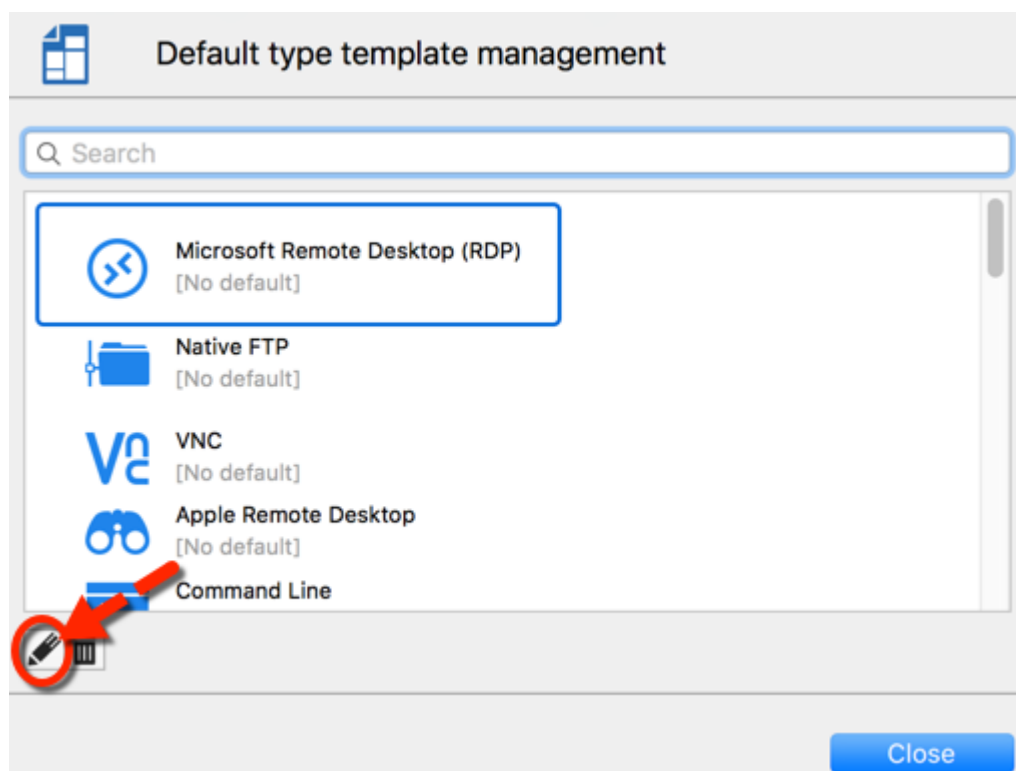
Notice that a **[No default]** notice is displayed below each type that doesn't have a default template defined.



Template - No default

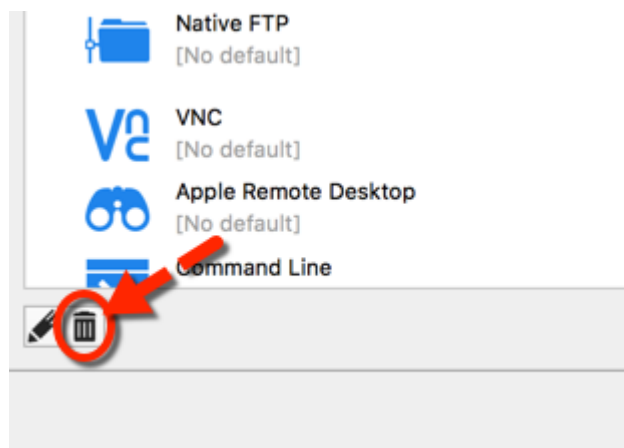
TEMPLATE DEFINED

All entry types without the **[No default]** notice may have a default template defined for them. You can double-click on the type to edit the template or press the edit button.



Type - Edit button

If you want to remove the default settings template, press the delete button.



Type - Delete button

6.1.12.2 Default Credential Settings

DESCRIPTION

You can access the default session settings from **File - Templates - Default credential settings**.

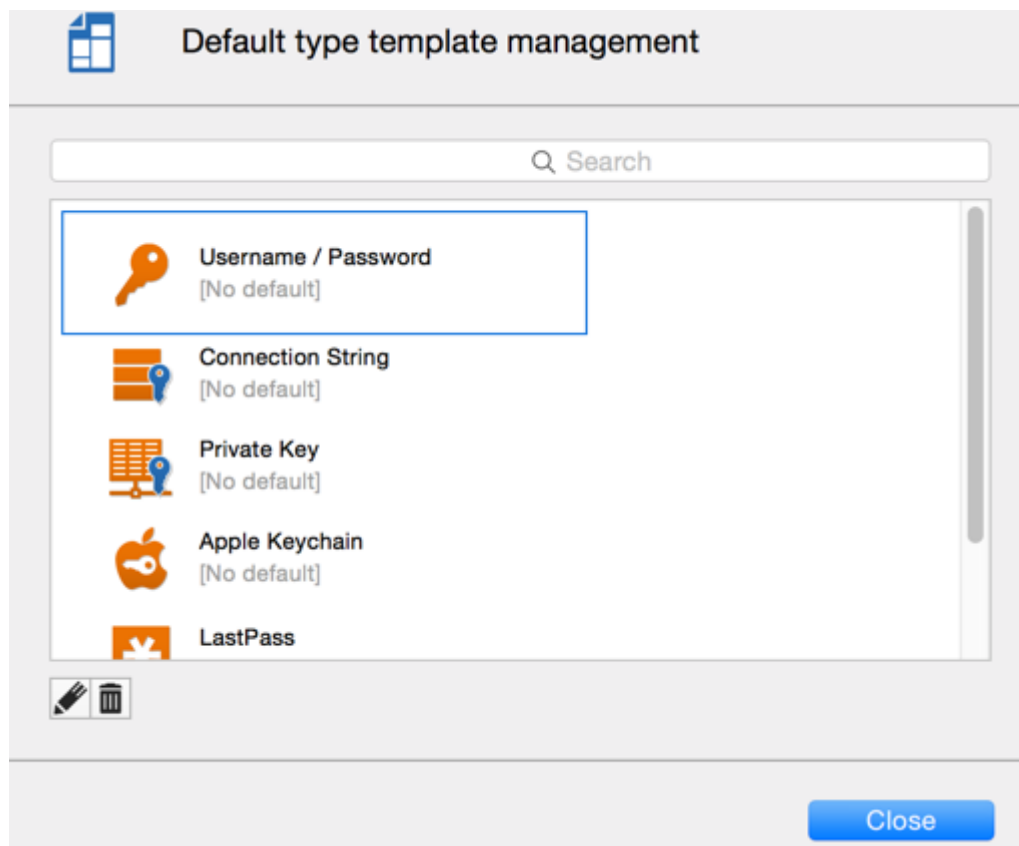
This allows you to edit or reset your credential default settings that are used whenever a new entry is created. Every credential type is supported and can have a default template defined.

By editing your default template, you will be able to save settings that you want used at the creation of new entries.

SETTINGS

NO TEMPLATE DEFINED

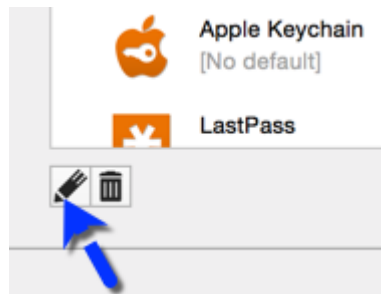
Notice that a **[No default]** notice is displayed below each credential type that doesn't have a default template defined.



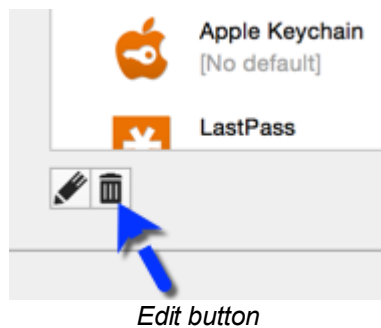
Default Template - No default

TEMPLATE DEFINED

All the Credentials without the **[No default]** notice has a default template. You can double-click on the type to edit the template or press the edit button.



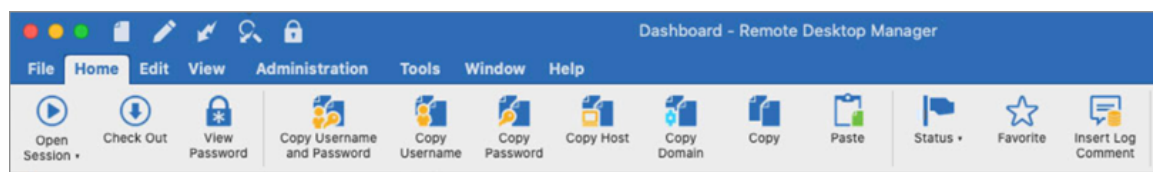
If you wish to remove the default settings template press the delete button.



6.2 Home

DESCRIPTION

The **Home** ribbon allows you to apply an action to the currently selected entry. The actions available in the ribbon will depend on the type of entry that is selected in your Navigation Pane.



Home Ribbon menu - RDP embedded session selected

SETTINGS

OPEN SESSION

Open session opens your selected session. Click on the drop-down menu to select the way you want your session to open, depending on the type of session you have selected the menu will be different.

VIEW PASSWORD

View your selected session password.

EXECUTE

Execute a selected macro or script in the current tab.

COPY

For more information on all the copy options please see [Clipboard](#).

OPEN VPN

This feature is enabled when a VPN is configured inside your session, it will open a VPN before starting the connection to the session.

CLOSE VPN

This feature is enabled when a VPN is configured inside your session, it will close a VPN while leaving the session open.

STATUS

For more information please see [Status](#).

FAVORITE

For more information please see [Favorite](#).

NEW PLAYLIST

For more information please see [Playlist](#).

INSERT LOG COMMENT

Add a log comment to the session that will be saved in the session logs, for more information please see [Insert Log Comment](#).

6.2.1 Clipboard

DESCRIPTION

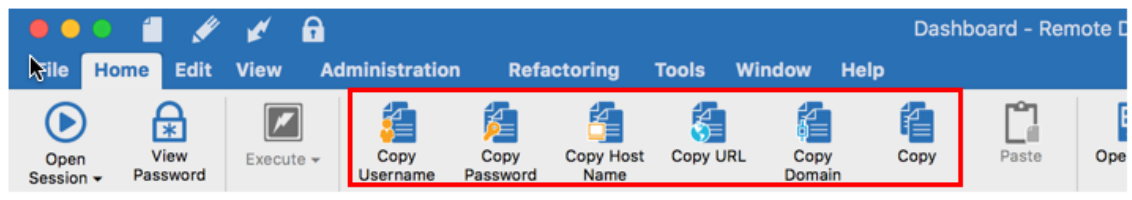
The **Copy** options in the **Home** ribbon holds the options to copy data entry values in your clipboard such as:

- **Username**
- **Password**
- **Domain**
- **Host Name**
- **URL**



When using an [Advanced Data Source](#), the administrator can control the copy passwords rights in the [Data Source Settings](#).

SETTINGS



Home - Copy options

COPY USERNAME

Copy the username define in your session to the clipboard.

COPY PASSWORD

Copy the password define in your session to the clipboard. The copy password to clipboard feature must be enabled in order to be accessible. Check the ***Allow Reveal Password*** in the [User Management Privileges](#).

COPY HOST NAME

Copy the host name define in your session to the clipboard.

COPY URL

Copy the URL define in your session to the clipboard.

COPY DOMAIN

Copy the domain define in your session to the clipboard.

COPY/PASTE

The copy/paste of a session entry is also possible. You can paste the session into a different data source or simply create a copy of it. It is a quick way to move/duplicate an item.



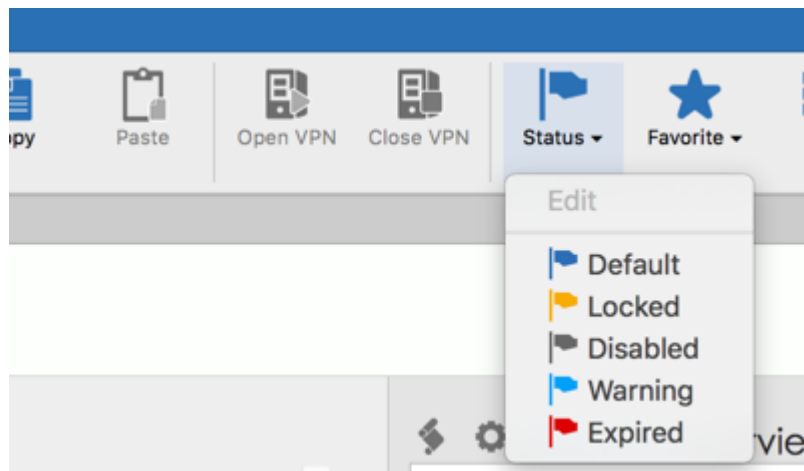
When using an [Advanced Data Source](#), the user must have Add Session rights in the [User Management](#) to be able to copy/paste sessions.

6.2.2 Status

DESCRIPTION

The **Status** allows you to change the status of a session.

SETTINGS



Home - Status

OPTION	DESCRIPTION
Edit	This will allow you to write a session status message that will be displayed every time a user open a session.
Default	This will set the status back to its default setting.

OPTION	DESCRIPTION
Locked	This allow the user who has locked the session to use it and block the others
Disabled	A disabled session can't be opened. It's mostly used when you don't want to delete it but avoid any unattended connection. It's also useful to disable an account for one of your former customer.
Warning	This status allows the session to be used, but displays a message to the user before it is opened.
Expired	An expired session can't be opened. It can be set manually or automatically if the session expiration date is set in his property.

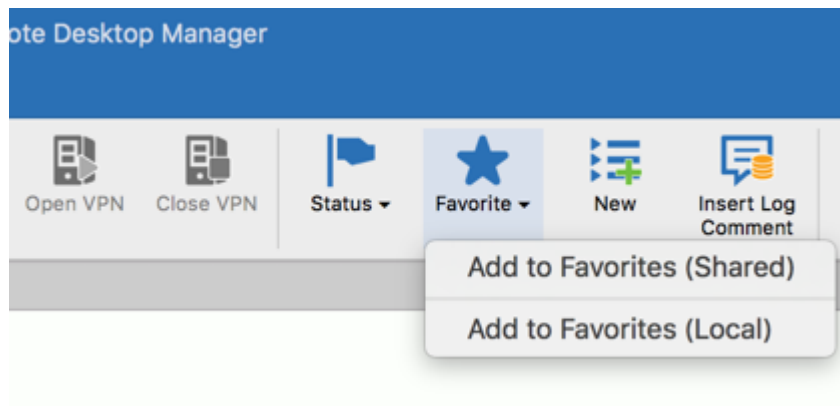


If using the **Locked** option, the session will be locked for other users only but the holder of the lock can still use it.

6.2.3 Favorite

DESCRIPTION

This is useful when the number of managed entries becomes too great or if you must maintain a strict directory structure to hold your entries. You can create a list of your Favorite entries to make it easier to access them.



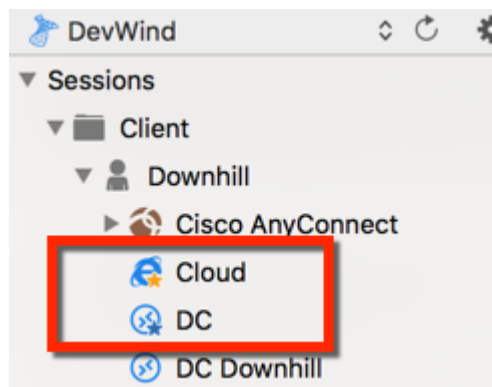
Home - Favorite

SETTINGS

There are two types of favorite sessions:

- **Shared favorites:** Shared by all users who are connected to the data source, and are directly configured from the session.
- **Local favorites:** Flagged locally on the current machine by the current user. The settings are saved in the application settings.

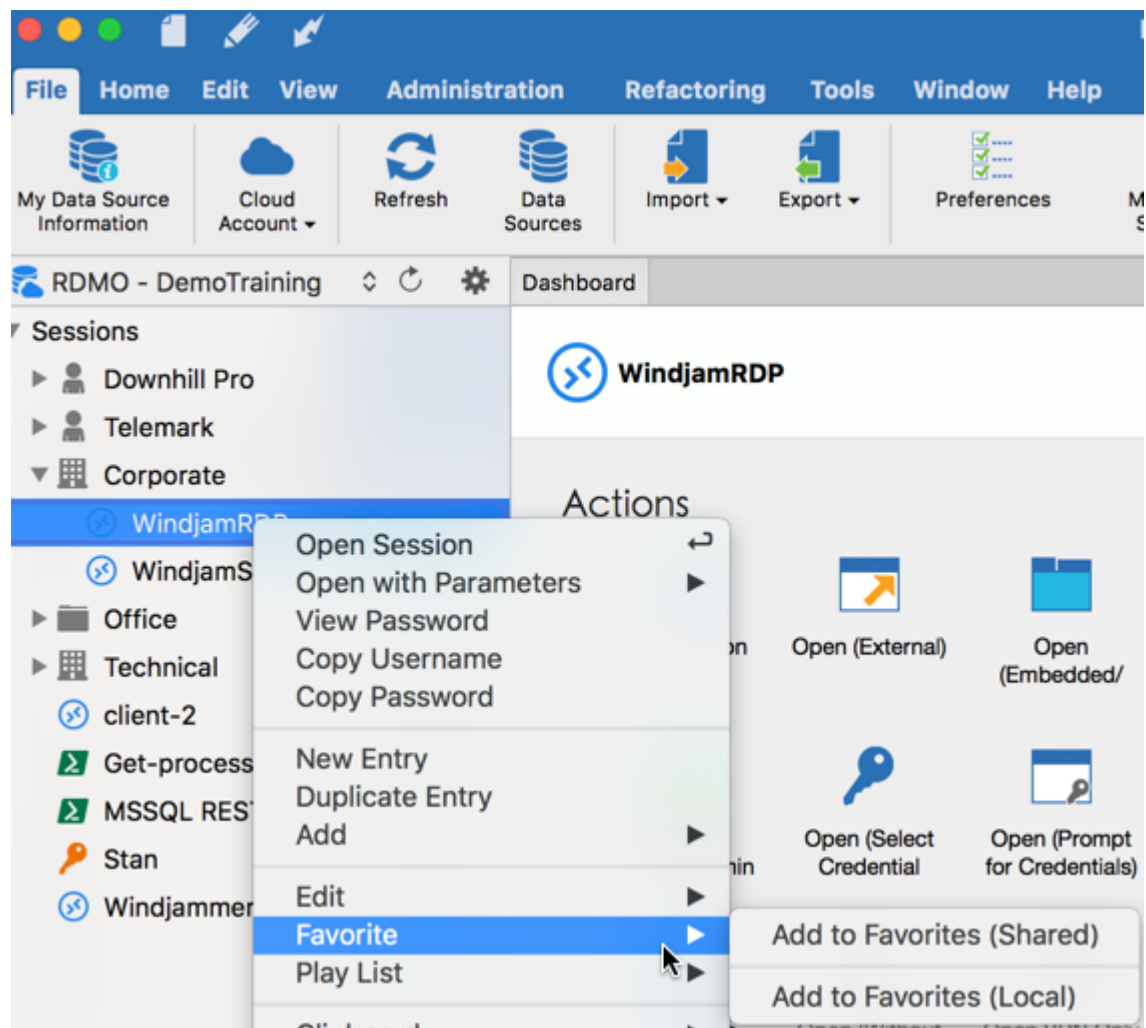
The blue star indicates a shared favorite and the yellow star a local favorite.



Local and Shared favorite

ADDING A SESSION TO THE FAVORITES

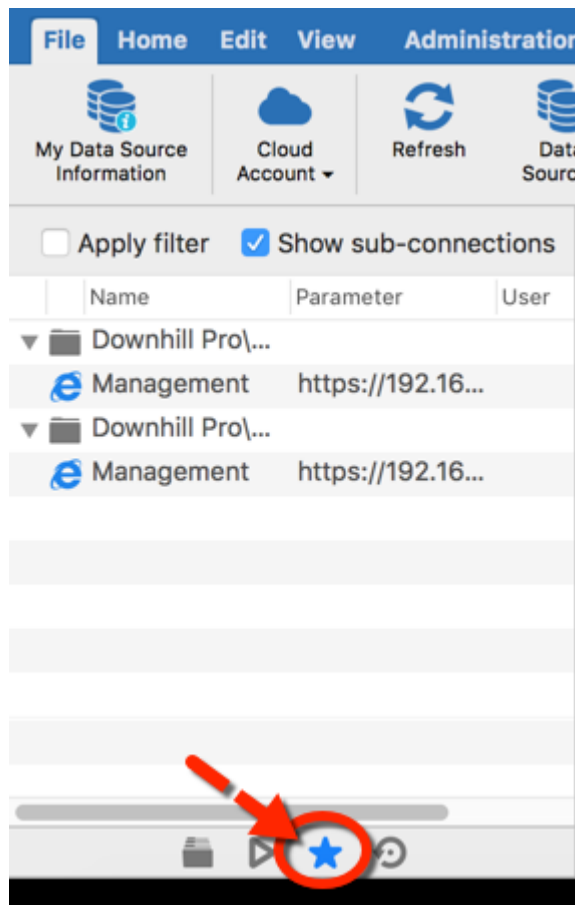
Select your entry in your Navigation Pane and then click on **Favorites** to add the entry to your Shared or Local list. You could also select your entry, do a right click and then select



Add to favorite

VIEW FAVORITES

To view a list of all your favorite entries, click on the star at the bottom of your Navigation Pane.

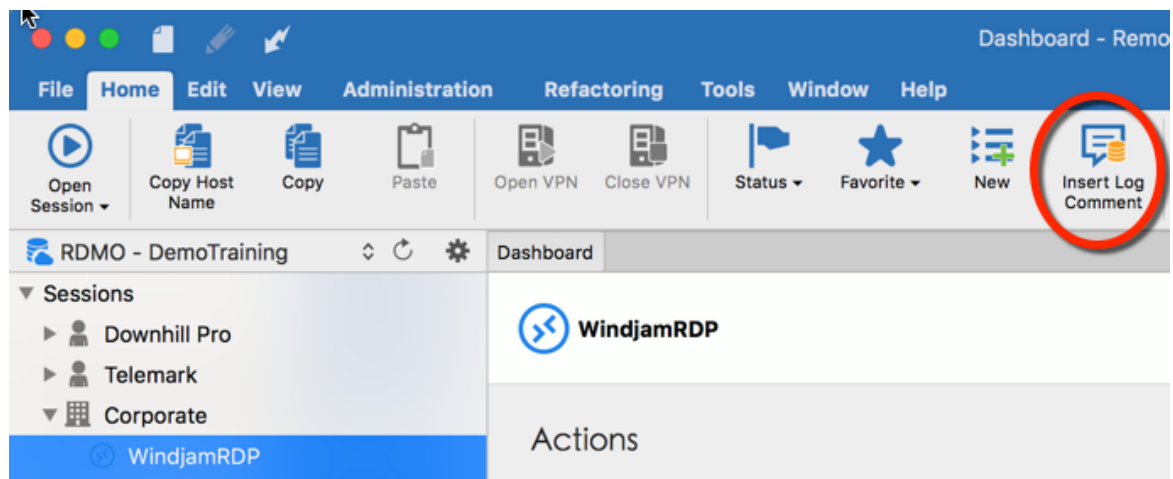


View Favorite List

6.2.4 Insert Log Comment

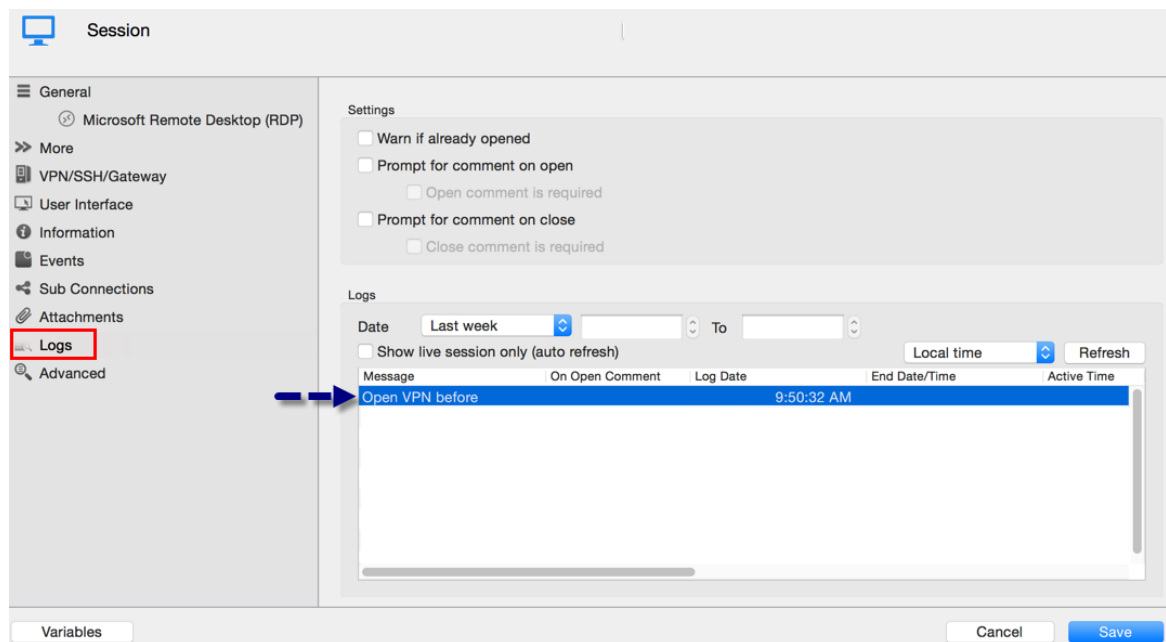
DESCRIPTION

You can add a log comment to the session that will be saved in the session log. Select your entry in the Navigation Pane and then click on **Home - Insert Log Comment**.



Home - Insert Log Comment

To consult the session log you can right-click on the session and select **View - Log** or when editing the session in the tab Logs you will see your session log with your Log Comment as well.

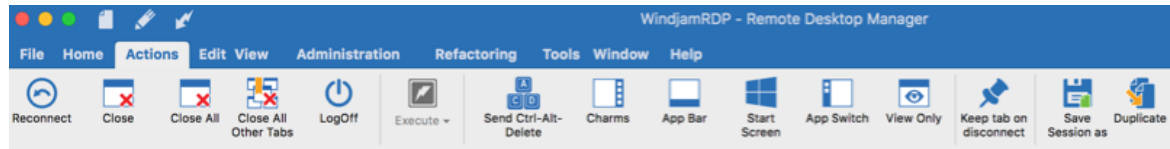


Session Logs

6.3 Action

DESCRIPTION

The **Actions** ribbon contains operations that can only be performed on a running session. The Actions menu will not be visible if there is no active running session. For our example we are running an RDP session, the ribbon will display the following tab when the session is in embedded mode.



Actions Ribbon

Alternatively, the **Actions** are also available by right-clicking on the tab of an embedded session.

SETTINGS

CONNECT

The Connect actions allows you to reconnect/disconnect from one or multiple session(s) simultaneously. Actions are different depending on your selected session type.

OPTION	DESCRIPTION
Reconnect	Quickly close the session and then re-open it automatically. Use it to update the resolution of your embedded RDP connections when you resize the window.
Close	Close the active session.
Close All	Close all the opened sessions.
Close All Other tabs	Close all the opened sessions except the active one.
Logoff	Logoff the active session.

OPTION	DESCRIPTION
Execute	Execute the selected macro or script in the previous window or in the current tab.

COMMANDS

The Commands are actions sent to the remote session, they are therefore different depending on your session type.

OPTION	DESCRIPTION
Send Ctrl+Alt+Delete	Send the key combination CTRL+ALT+DELETE to the host.
Charms	On Windows 8 or Windows 2012 server, displays the Charms bar (Search, Share, Start, Devices, and Settings bar).
App Bar	On Windows 8 or Windows 2012 server, displays the App bar to show navigation, commands, and tools.
App Switch	On Windows 8 or Windows 2012 server, switches from one application to another.
View Only	Prevent the session from receiving any input from the keyboard or the mouse. This feature was requested to allow monitoring while preventing manipulation errors. Use it to have a read only access to the remote server.

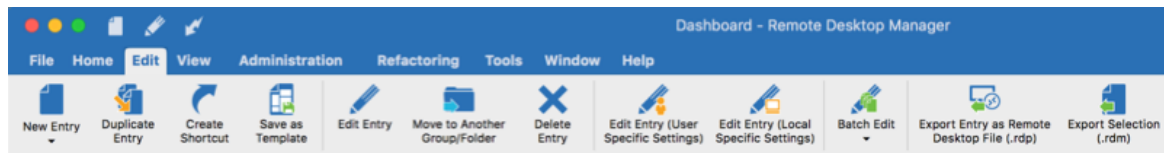
SETTINGS

OPTION	DESCRIPTION
Keep tab on disconnect	Your session tab will stay open after a session disconnect.
Save Session as	Save your open session as a new entry.
Duplicate	Open a duplicate tab your opened session.

6.4 Edit

DESCRIPTION

The **Edit** ribbon contains operations to rapidly Add, Edit, Overrides, Batch Edit or Export entries.



Edit ribbon

To learn more please see:

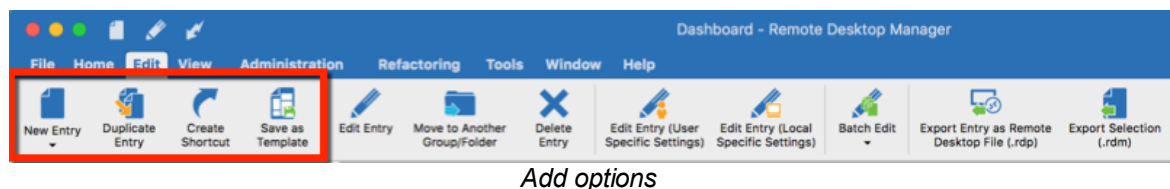
- [Add Entries](#)
- [Edit Entries](#)
- [Setting Overrides](#)
- [Batch Edit](#)
- [Export](#)

6.4.1 Add Entries

DESCRIPTION

The **Add** options lets you quickly create new entries, duplicate them, create shortcut or rapidly save your entry as a template.

SETTINGS



OPTION	DESCRIPTION
New Entry	Create a new entry (session, group/folder, data entry, credentials, etc...).
Duplicate Entry	Create a duplicate of your entry.
Create Shortcut	Link your entry to more than one group. See Shortcut/Linked Entries for more information.
Save as Template	Save your selected entry as a local or shared template .

6.4.1.1 Creating a New Entry

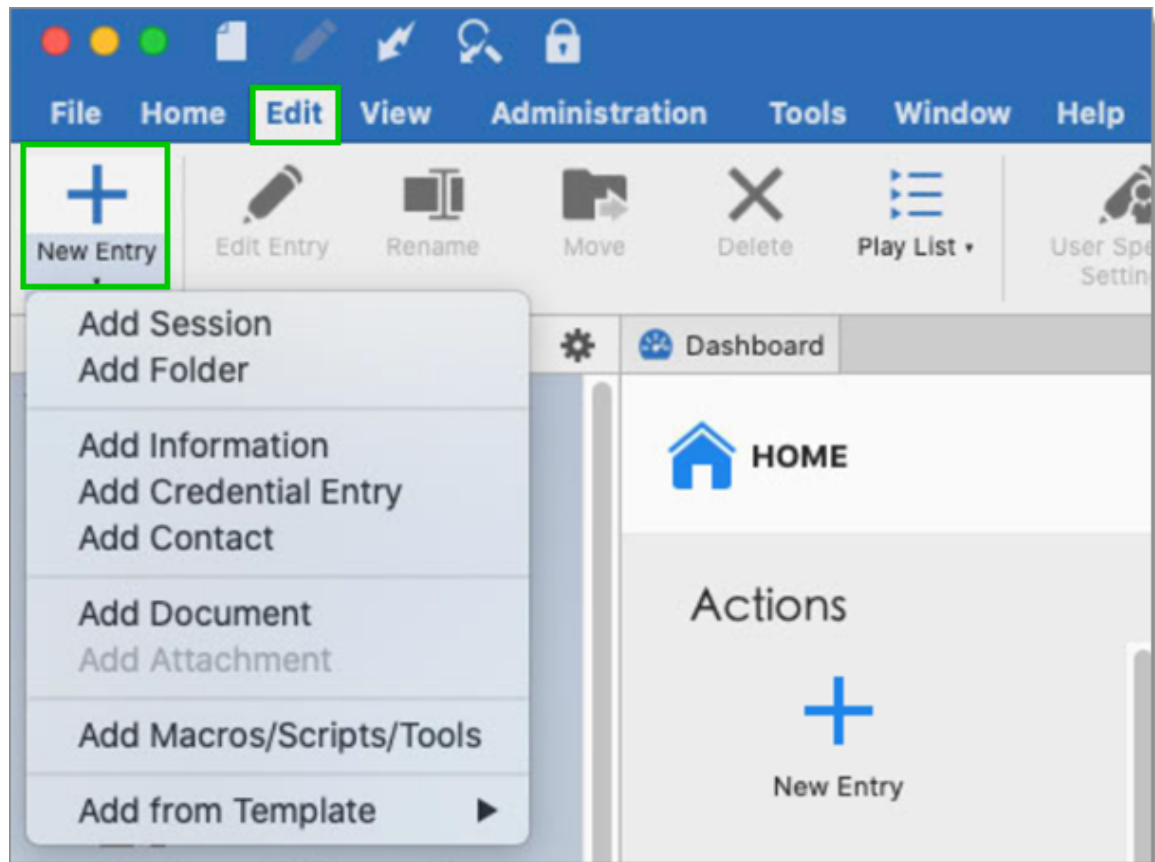
DESCRIPTION

When getting started with Remote Desktop Manager for Mac, you must first configure your entries. There are many type of entries; you should know what third party or

technology you will use to connect remotely in order to choose the appropriate entry type(s) that you plan on configuring.

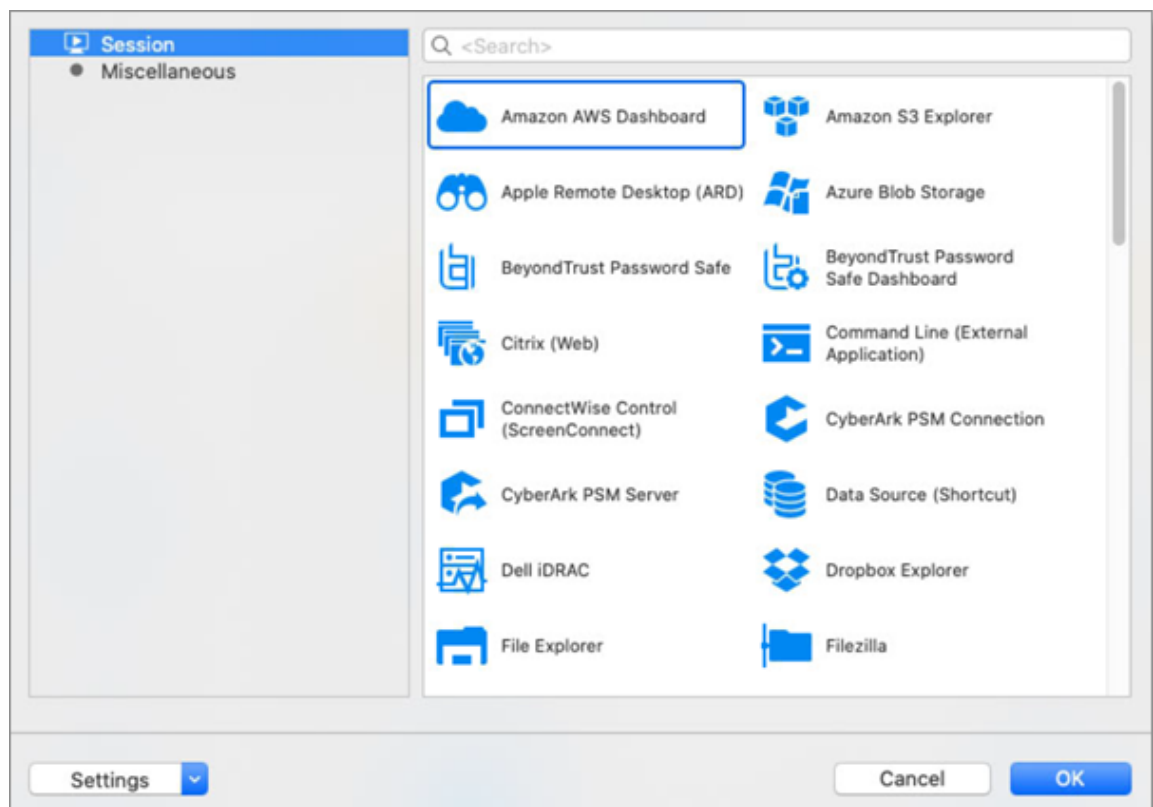
CREATING A NEW ENTRY FROM THE NEW ENTRY MENU

1. The simplest way to create a new entry is through the **Edit** Ribbon menu and **New Entry**.



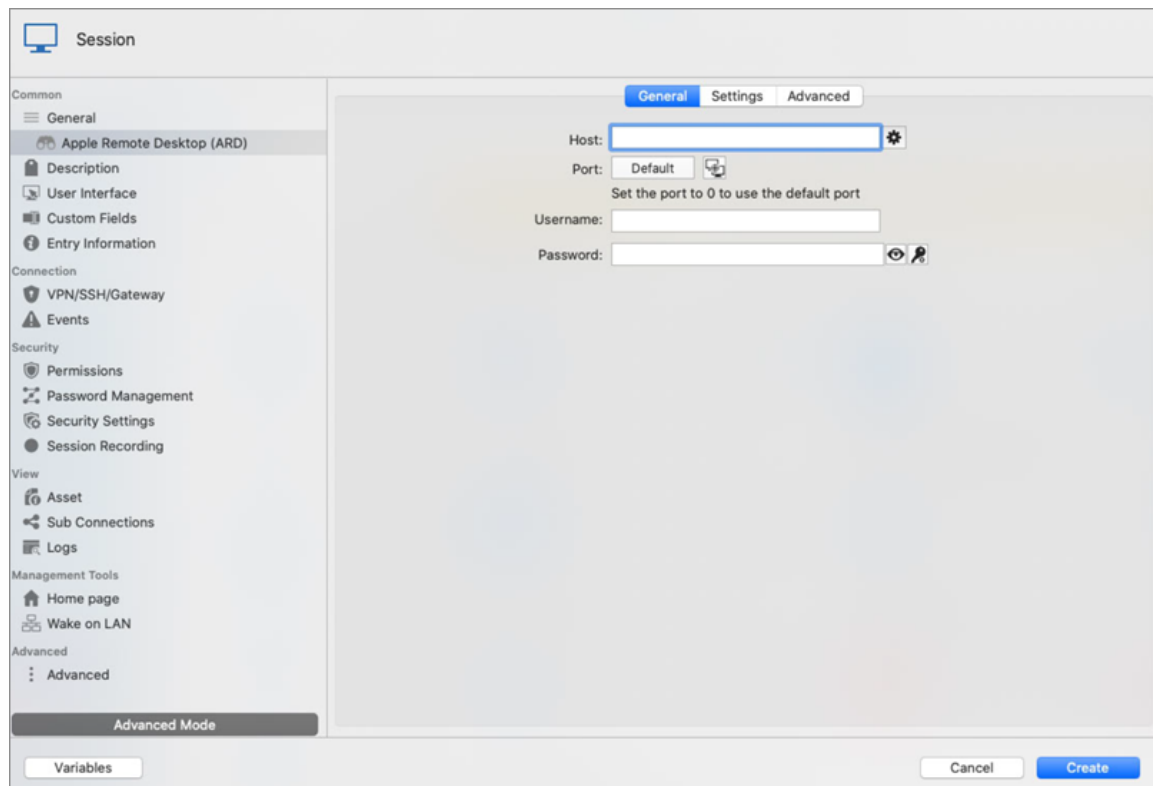
Add a New Entry

2. Select the type of entry or template you wish to create.



Entry type

3. You will be prompted to customize your settings in the session property window.



Session settings

CREATING A SESSION VIA IMPORT MENU

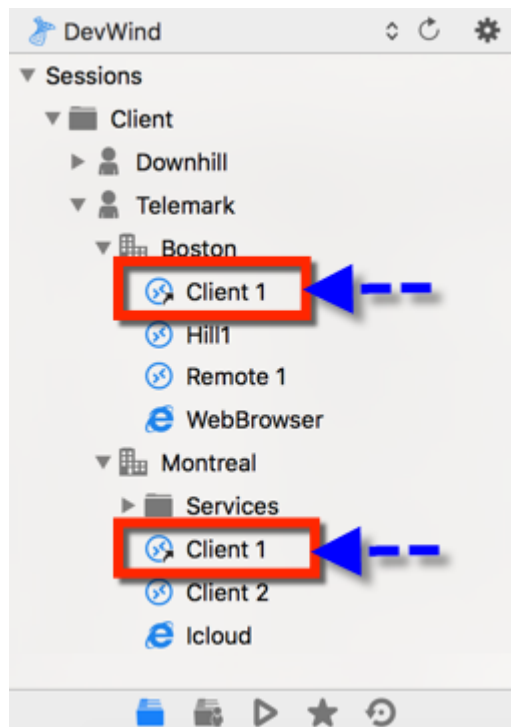
You can also import a session by using the Import menu in **File - Import**. For more information, refer to the [Import](#) topic.

6.4.1.2 Shortcut Entries

DESCRIPTION

There are many scenarios where it makes sense for an entry to appear more than once in the Navigation Pane. For example, you might want to:

- Assign different access to the folder;
- Create a favorite folder with everything centralized;
- Reuse a document for different scenarios.

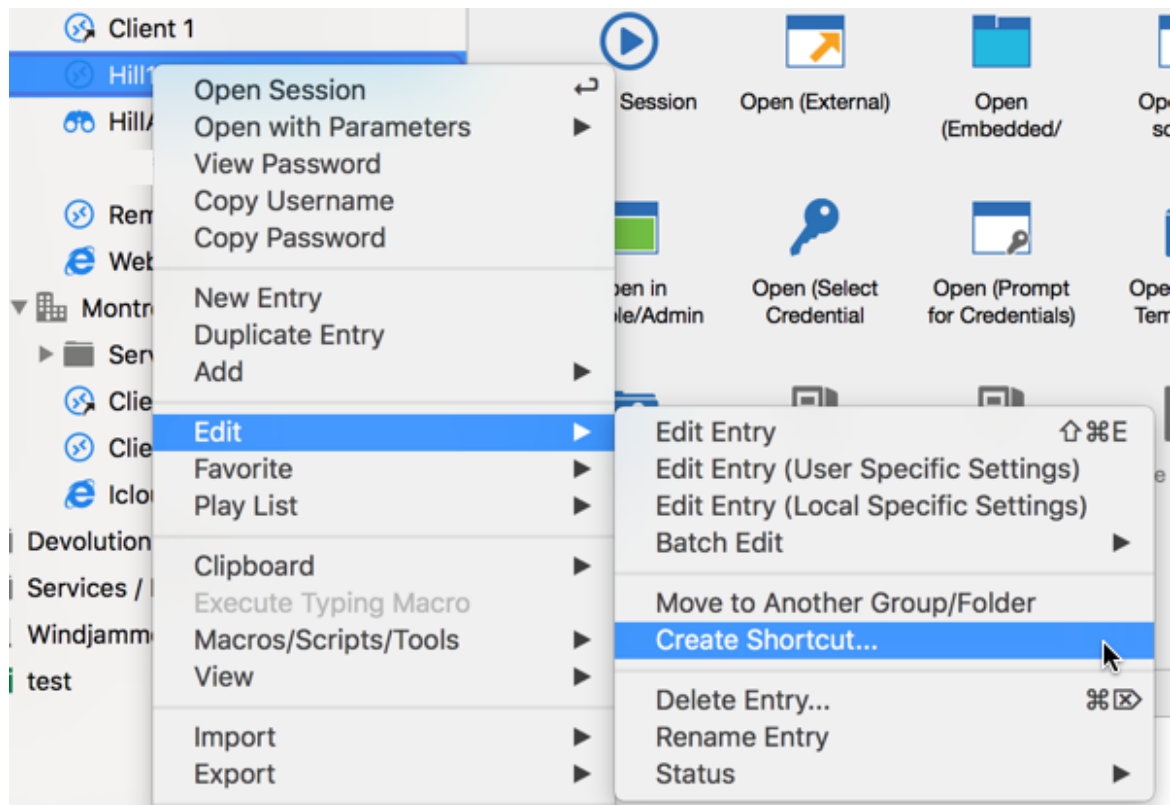


Two shortcut selected

Creating shortcuts is simplified by saving the entry once in the database while linking it to more than one group. So when the application loads the data, it automatically creates a link to the original entry.

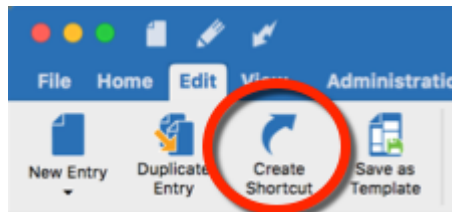
CREATING A SHORTCUT: OPTION 1

One way to create a shortcut is by doing a right-click on the chosen entry and then using the menu **Edit-Create Shortcut...**



Context menu - Create Shortcut

Another way to create a shortcut is using the **Edit menu - Create Shortcut**.



Edit ribbon - Create Shortcut

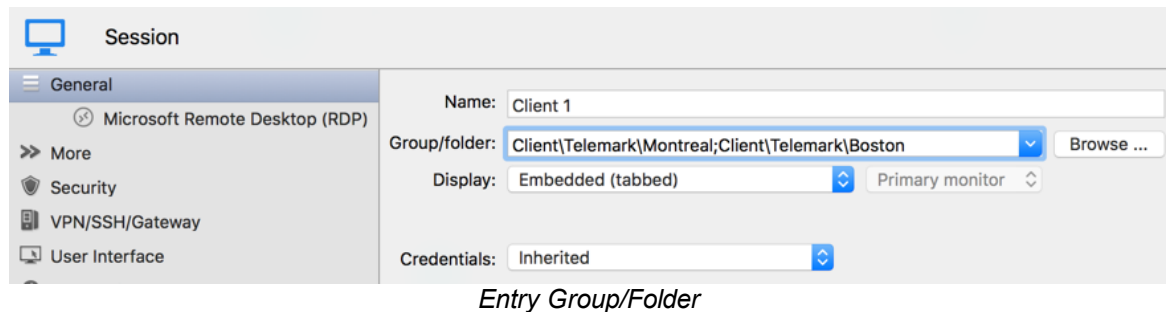


There is no visual differences between the shortcut and the original entry. Therefore, you'll need to delete all entries to completely remove them.

CREATING A SHORTCUT: OPTION 2

A second way to create a shortcut is via the session properties. Since the shortcut is based on a group list, simply add a session in multiple groups by setting two or more destinations, and separating them by a semi-colon ";". You can also use the browse

button (...) and select more than one group by holding the Ctrl key while clicking on the tree node.

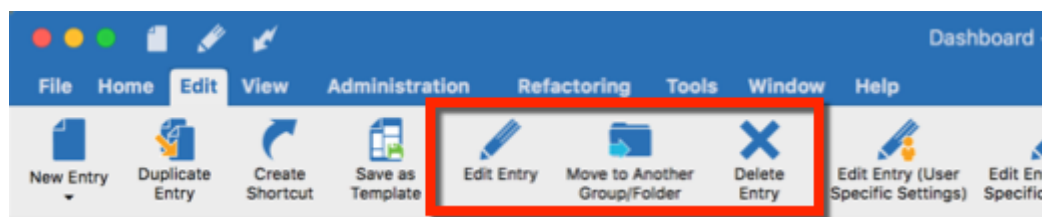


6.4.2 Edit Entries

DESCRIPTION

The Edit options is used to Edit one of your entry. You may edit the properties, rename your entry or quickly delete your entry.

SETTINGS



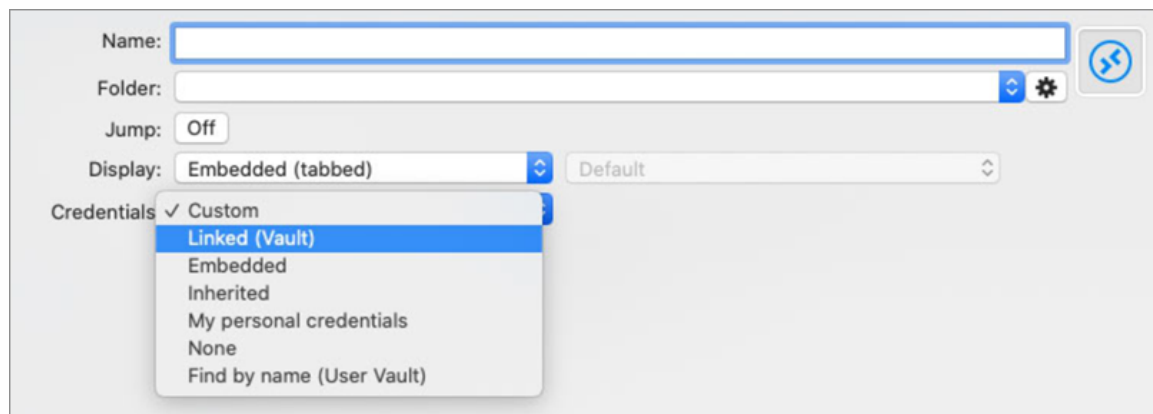
OPTION	DESCRIPTION
Edit Entry	Edit the options of your selected entry.
Move to Another Group/Folder	Move your selected entry to another Group or Folder.

OPTION	DESCRIPTION
Delete Entry	Delete your selected entry. A confirmation window will appear to confirm the deletion of the entry.

6.4.3 Entry Credentials Options

DESCRIPTION

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



OPTION	DESCRIPTION
Custom	This option allows to enter custom credentials in the General section of the entry.
Linked (Vault)	Link your entry to use an existing Credential entry in the same vault.
Embedded (Legacy)	Embed a Credential entry in the entry itself. This mode is deprecated and not recommended. Please review other options available.

OPTION	DESCRIPTION
Inherited	The credentials used by this entry will be inherited and defined by climbing up the navigation tree until it has access to a set of credentials in a parent folder.
My personal credentials	Will use the credentials set in My personal credentials feature. This allows you to centralize one credential to replace or emulate the ones for your Windows session.
None	No credentials will be allowed to be saved or linked to this entry.
Find by name (User Vault)	Will search your User Vault for the name specified. If the box is left empty, when launch, a Credential list will open with all available Credentials entry from your User Vault .

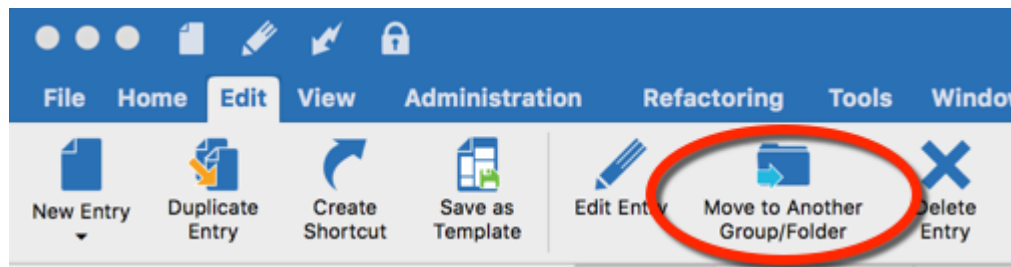
6.4.4 Move to Another Group/Folder

DESCRIPTION

If you wish to move an entry under a different Group or Folder you have the option of selecting your entry with your mouse and move it under the right Group or Folder, but to avoid easily made mistakes and move it under the wrong Group we highly suggest to use the option **Move to Another Group/Folder**.

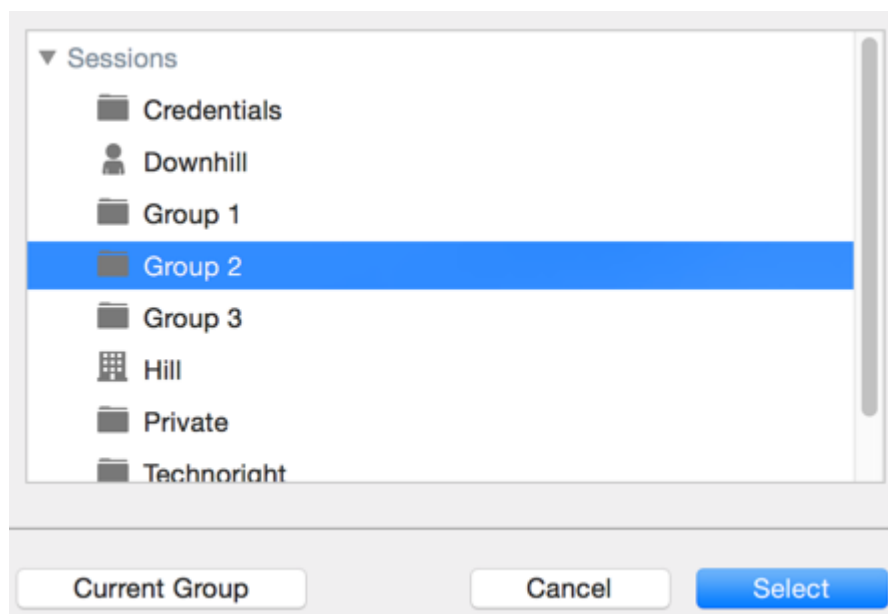
SETTINGS

1. Select your entry in your Navigation Pane and then use the menu **Edit - Move to Another Group/Folder**



Move to Another Group/Folder

2. Select the Folder or Group under which you want to move your entry and then click on **Select**.



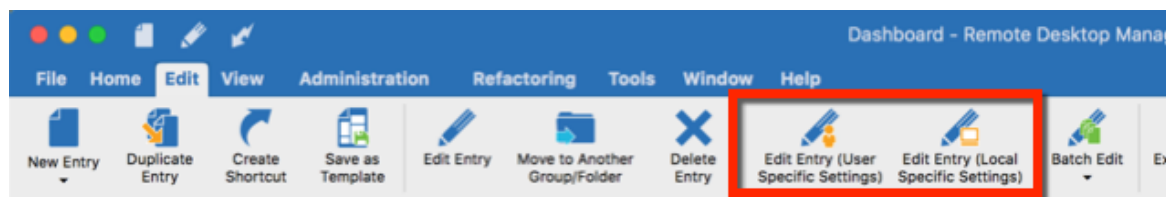
Select Group/Folder

6.4.5 Setting Overrides

DESCRIPTION

Setting Overrides options are used to override the user specific settings or the local specific settings of a session.

SETTINGS

*Edit - Setting Overrides*

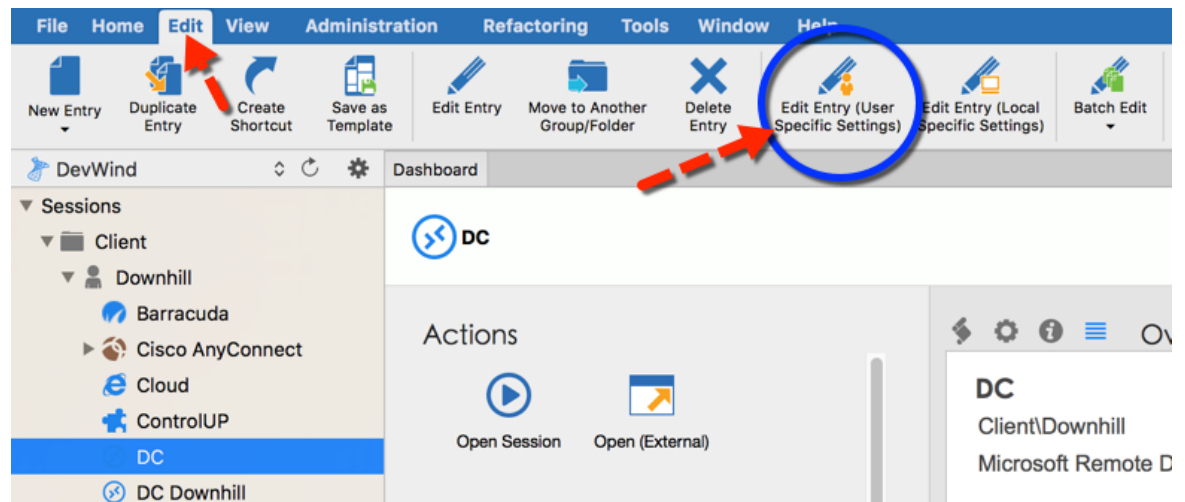
OPTION	DESCRIPTION
Edit Entry (User Specific Settings)	Allows session setting override for a user. For more information see User Specific Settings.
Edit Entry (Local Specific Settings)	Allow session setting override for the local machine. For more information see Local Machine Specific Settings.

6.4.5.1 User Specific Settings

DESCRIPTION

Allows session setting override for a user. Several settings can be overridden, such as user name, password or display.

In your **Navigation Panel** select the entry you wish to override and then do a right click **Edit - Edit Entry (User Specific Settings)** or in the Ribbon simply select **Edit - Edit Entry (User Specific Settings)**.



Edit - Edit Entry (User Specific Settings)

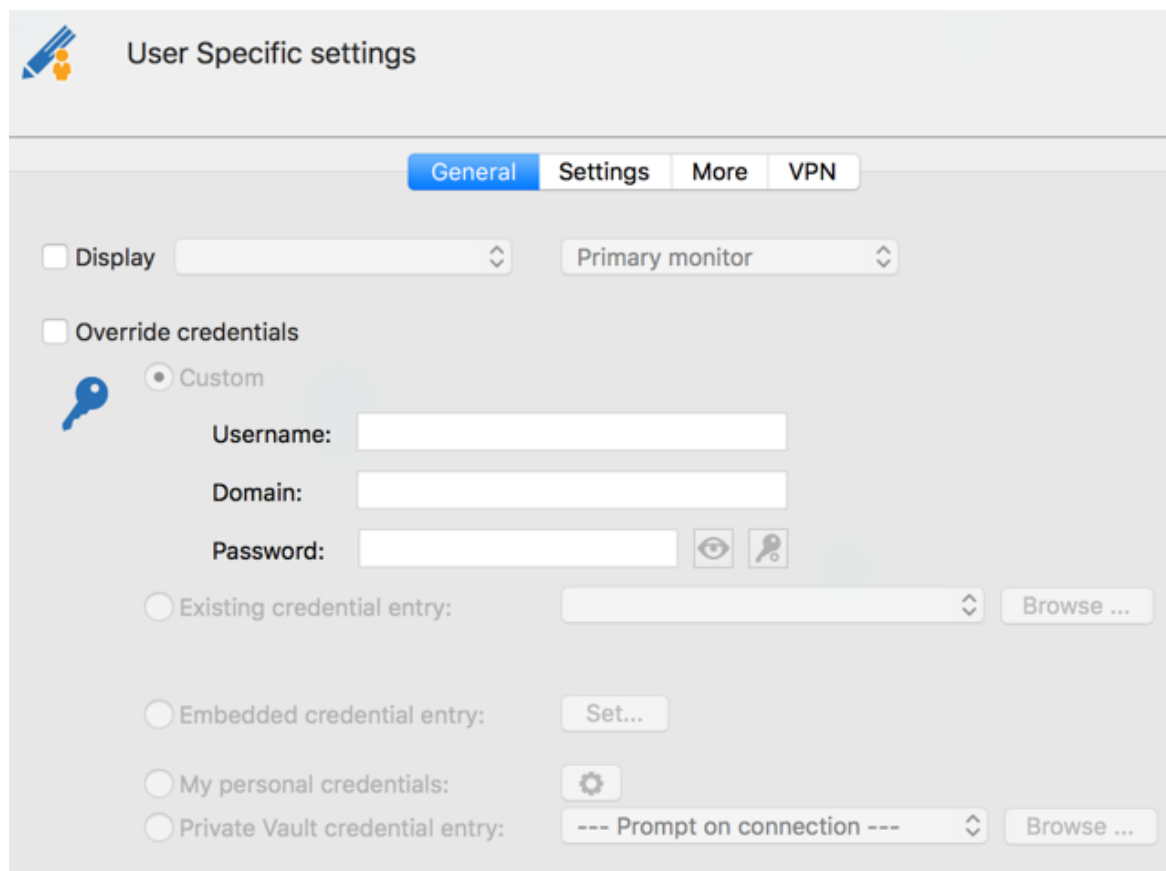
SETTINGS



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



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



User Specific settings

General Settings More VPN



☐ Display Primary monitor

☐ Override credentials

☒ Custom

Username:

Domain:

Password:  

☐ Existing credential entry: Browse ...

☐ Embedded credential entry: Set...

☐ My personal credentials: gear icon

☐ Private Vault credential entry: --- Prompt on connection --- Browse ...

User Specific settings

Please consult each tabs for more information:

- [Override Credentials](#)
- [General](#)
- [Settings](#)
- [More](#)
- [VPN](#)

6.4.5.1.1 Override credentials

DESCRIPTION

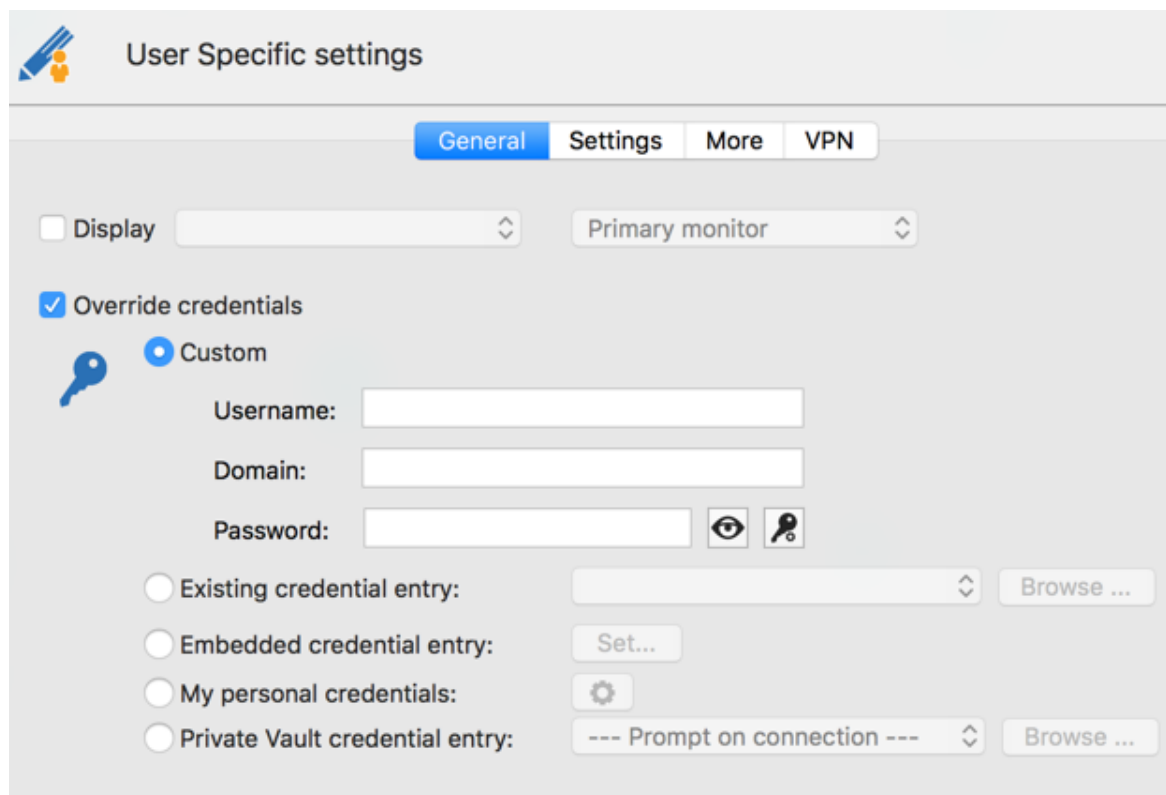
Override Credentials allows you to specify other credentials than the one stored in an entry. You can choose from multiple sources according to your security practices and policies.



The Override credentials is available for all type of entries.

GENERAL

Simply check the **Override credentials** and select your credential to start overriding your credentials. To stop overriding credentials uncheck the **Override credentials** option.

The image shows a 'User Specific settings' dialog box with a light gray background. At the top left is a small icon of a pencil and a person. The title 'User Specific settings' is in the top left. Below the title are four tabs: 'General' (selected, highlighted in blue), 'Settings', 'More', and 'VPN'. Under the 'General' tab, there is a 'Display' section with a checkbox and a dropdown menu set to 'Primary monitor'. Below that is the 'Override credentials' section, which has a checked checkbox and a key icon. Under this, there are four radio button options: 'Custom' (selected), 'Existing credential entry:', 'Embedded credential entry:', and 'My personal credentials:'. The 'Custom' option has fields for 'Username:', 'Domain:', and 'Password:'. The 'Existing credential entry:' option has a dropdown menu and a 'Browse ...' button. The 'Embedded credential entry:' option has a 'Set...' button. The 'My personal credentials:' option has a gear icon. The 'Private Vault credential entry:' option has a dropdown menu set to '--- Prompt on connection ---' and a 'Browse ...' button. There are also eye and key icons next to the password field.

User Specific Settings - Override credentials

The following choices are offered depending on the type of entry being overridden, as well as the location of that entry.

OPTION	DESCRIPTION
Custom	Use a specific User name, Domain and Password.
Existing credential entry	Use an existing credential entry.
Embedded credential entry	Use an Embedded credential entry.
My personal credentials	Use the credentials stored in My Personal Credentials
User Vault credential entry	Use a User Vault credential entry.

6.4.5.1.2 General

DESCRIPTION

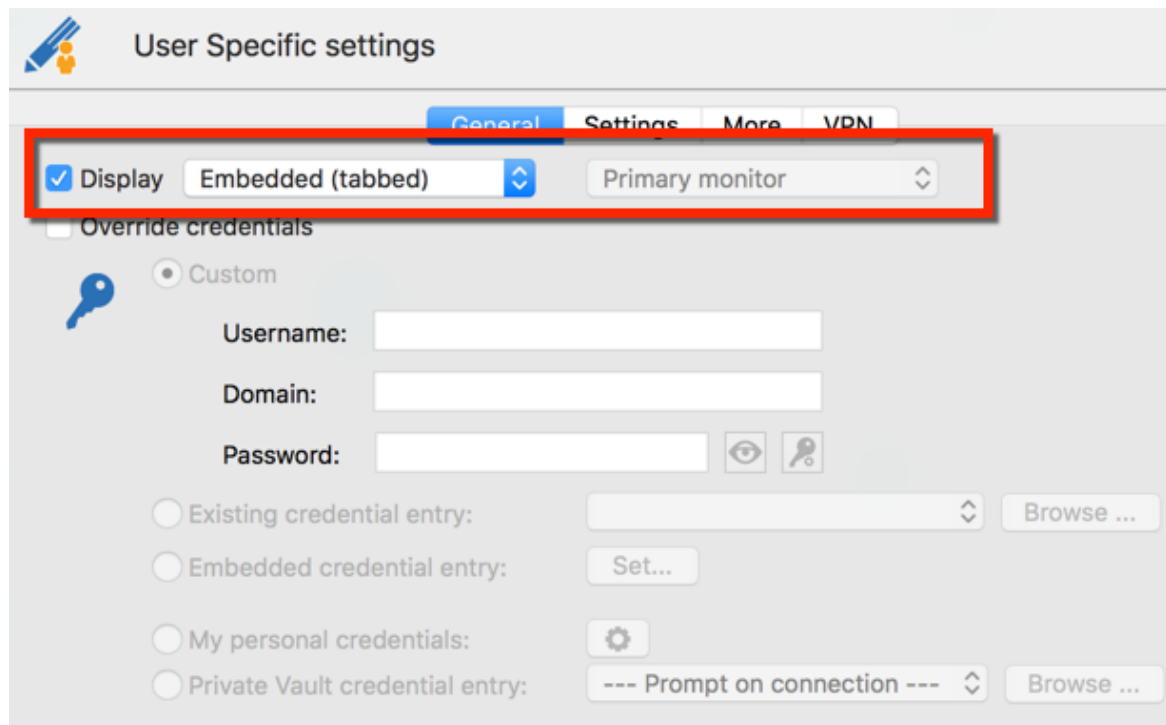
The **General** tab allows you to override the Display mode and the credentials.

SETTINGS

DISPLAY



The **Display override** is only available for Sessions entry type.

*Display Override*

Please consult Display Mode for more information on available settings and their usage.

CREDENTIAL

For more information on Override credentials follow this [link](#).

6.4.5.1.3 Settings

DESCRIPTION

The **Settings** tab allows you to override the screen size, the gateway and your hard drives.

SETTINGS

SCREEN SIZE



Override screen size is only visible for RDP sessions.

Override Screen Size allows you to customize the size of the local window hosting the remote session.

The screenshot shows the 'User Specific settings' window with the 'Settings' tab selected. A red rectangle highlights the 'Override screen size' section, which includes a checked checkbox, a monitor icon, a 'Remote desktop size' dropdown set to 'Default', 'Custom width' and 'Custom height' input fields both set to 0, and a 'Screen sizing mode' dropdown set to 'Scrollbar'. Below this section are other settings like 'Override gateway', 'Override hard drives', and disk redirection options.

User Specific settings - Override screen size

OPTION	DESCRIPTION
Remote desktop size	Indicate the proper window size.
Custom width	Define the custom width of the window.

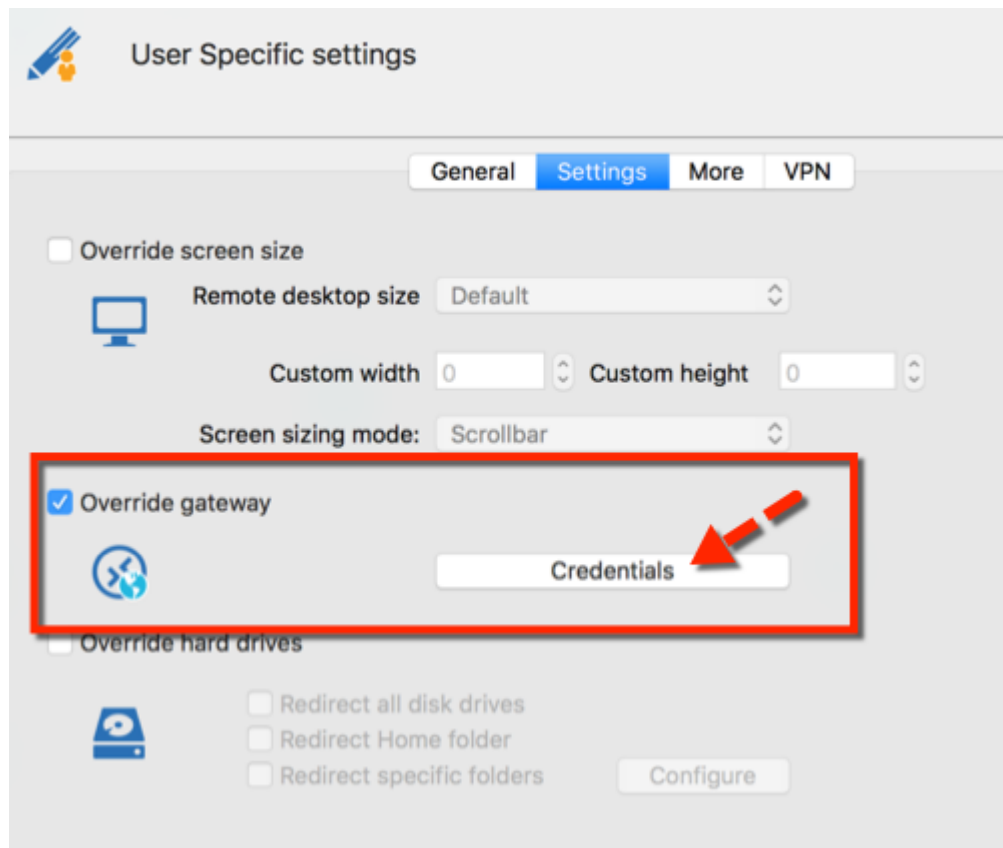
OPTION	DESCRIPTION
Custom height	Define the custom height of the window.
Screen sizing mode	<p>You can select the screen sizing mode between:</p> <ul style="list-style-type: none">• Scrollbar• Smart reconnect• Smart sizing• Server resolution• None

GATEWAY

Override gateway allows you to customize the RDP Gateway credentials used on the remote session. You must select the new credentials to be used, to learn more about the options for credentials override please follow this [link](#).



Override gateway is only visible for RDP sessions.



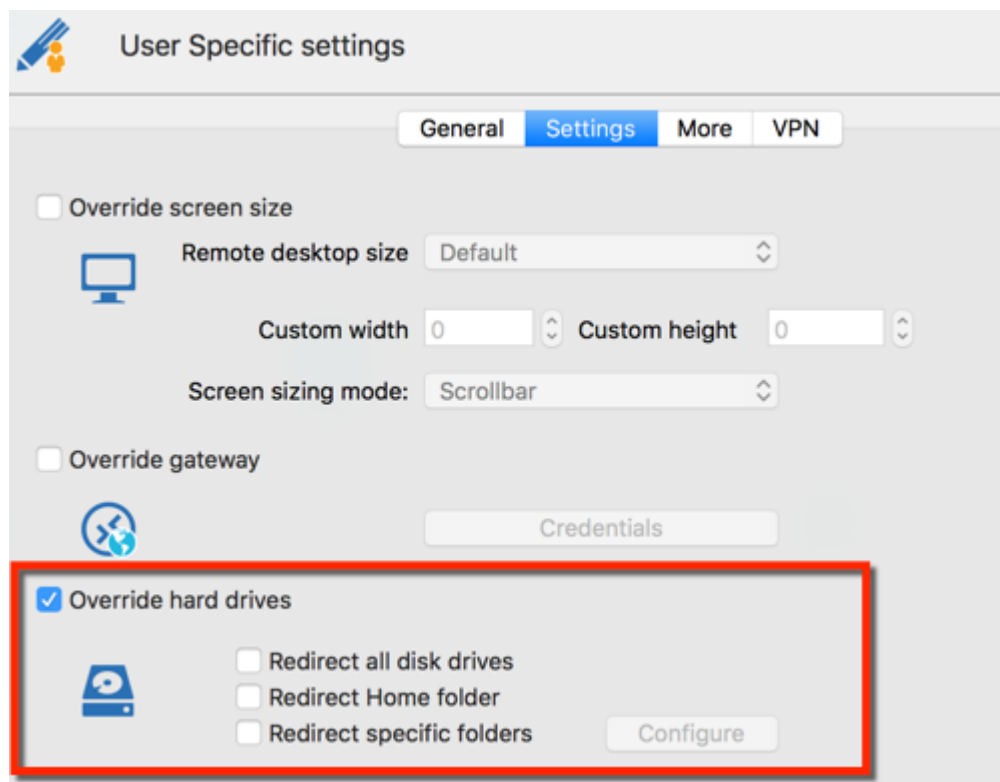
User Specific settings - Override gateway

HARD DRIVES

Override hard drives allows you to customize the RDP hard drives that are shared with the remote desktop connection.



Override hard drives is only visible for RDP sessions.



User Specific settings - Override hard drives

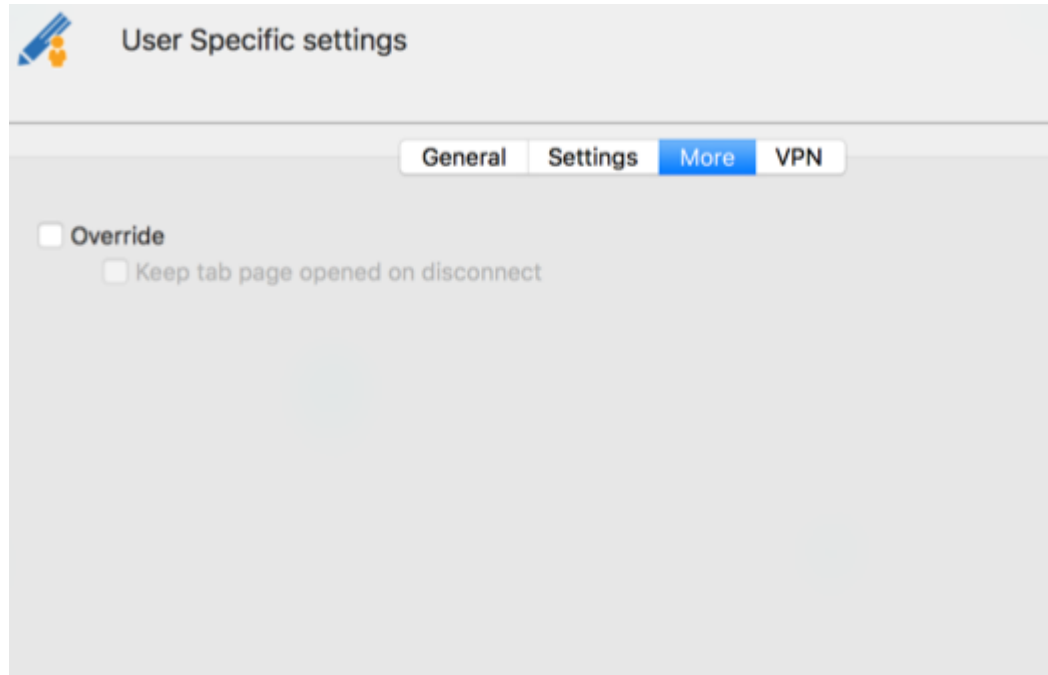
OPTION	DESCRIPTION
Redirect all disk drives	Share all of your hard drives in the remote session.
Redirect Home folder	Share your home folders in the remote session.
Redirect specific folders	Share one or more specific hard drives that you want in the remote session.

6.4.5.1.4 More

DESCRIPTION

Override from the tab More allows you to keep the tab page of your session open even when disconnecting.

SETTINGS



User Specific Settings - More tab

6.4.5.1.5 VPN

DESCRIPTION

When using a VPN on your session this allows you to override the VPN credentials.

SETTINGS

Select the credentials you wish to use to override your VPN credentials. For more information on the credentials please see [Override credentials](#).

The [User Vault](#) credential entry is only available under the following conditions:

1. the User Vault is available for your data source;
2. You are overriding at the folder level;

3. You are overriding a session that is itself in the User Vault.

User Specific settings

General Settings More **VPN**

☒ Override credentials

☒ Custom

Username:

Domain:

Password:

☐ Existing credential entry:

☐ Embedded credential entry:

☐ My personal credentials:

☐ Private Vault credential entry:

User Specific settings - VPN

OPTION	DESCRIPTION
Remote desktop size	Indicate the proper window size.
Custom width	Define the custom width of the window.
Custom height	Define the custom height of the window.

6.4.5.2 Local Machine Specific Settings

DESCRIPTION

Allow session setting override for the local machine. Several settings can be overridden such as user name, password and display.

LOCAL MACHINE SPECIFIC SETTINGS



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

In the majority of cases this dialog will appear.

Local Specific Settings

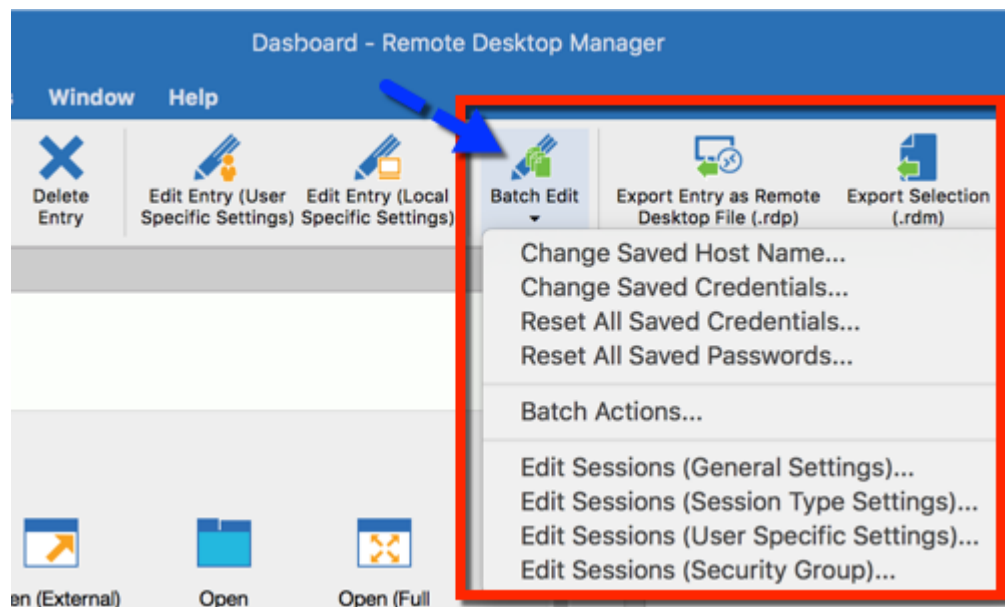
Please consult each specific override topic for more information.

- [Override Credentials](#)
- [General](#)
- [Settings](#)
- [More](#)
- [VPN](#)

6.4.6 Batch Edit

DESCRIPTION

Use the **Edit - Batch Edit** or the **Batch Edit** option in the context menu to change the settings of multiple sessions in one operation. It can be used for example to remove or update all of the credentials of a group of sessions.



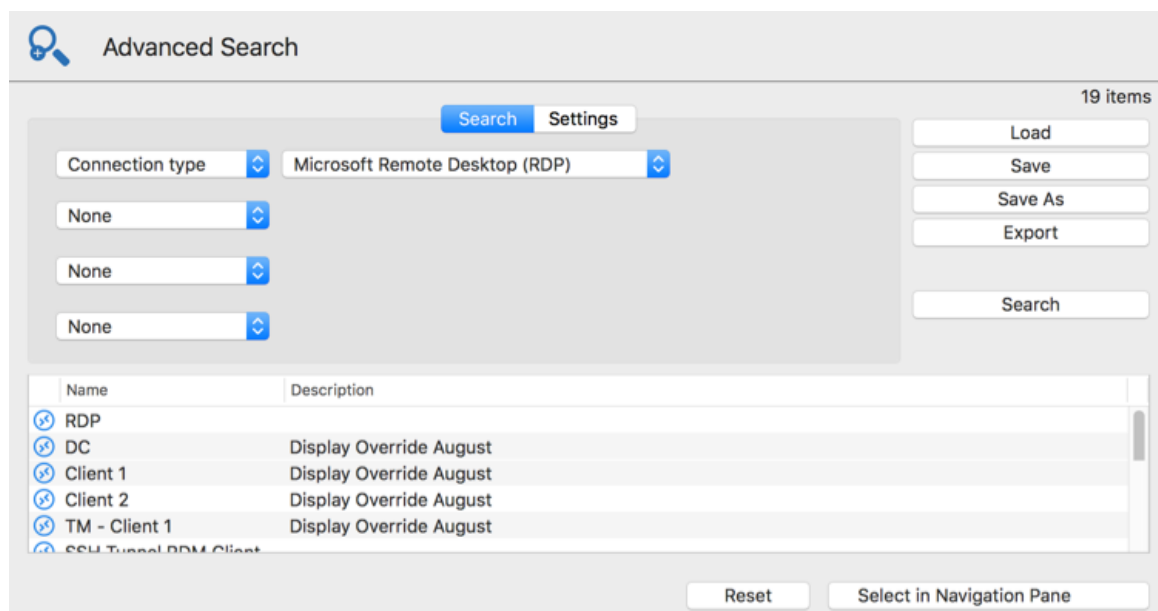
Batch Edit

You could also change:

- Host Name
- Credentials
- Passwords
- General Settings
- Session Type Settings
- User Specific Settings
- Security Group

ADVANCED SEARCH

You can select multiple entries by using **Command** and mouse click. For a method with a little more power, use our [Advanced Search](#) dialog, accessible from **View - Advanced Search**. The Advanced Search allows you to select multiple criteria at once.



The Advanced Search dialog box features a search bar at the top with a magnifying glass icon and the text "Advanced Search". Below the search bar, there are two tabs: "Search" (active) and "Settings". The "Search" tab contains four dropdown menus for filtering results. The first dropdown is labeled "Connection type" and is set to "Microsoft Remote Desktop (RDP)". The other three dropdowns are labeled "None". To the right of the filters, there are buttons for "Load", "Save", "Save As", "Export", and "Search". Below the filters, there is a table with two columns: "Name" and "Description". The table contains five rows of data, each with a selection icon (a circle with a cross) in the "Name" column. The rows are: "RDP", "DC", "Client 1", "Client 2", and "TM - Client 1". The "Description" column for all rows is "Display Override August". At the bottom right of the dialog, there are buttons for "Reset" and "Select in Navigation Pane".

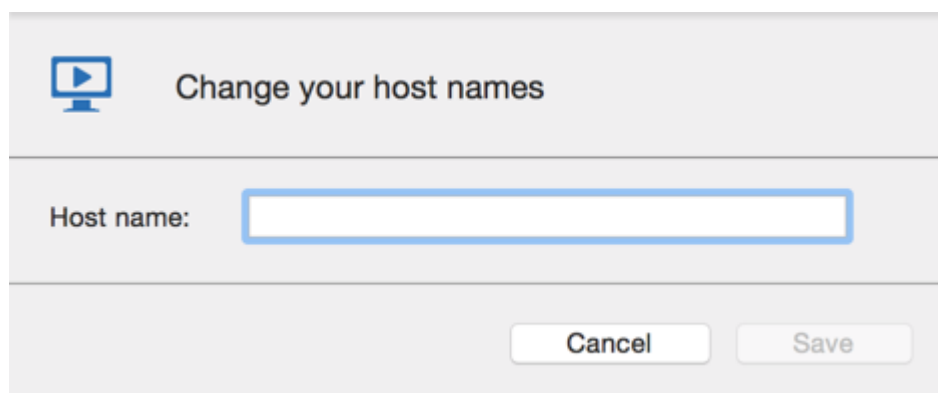
Name	Description
RDP	Display Override August
DC	Display Override August
Client 1	Display Override August
Client 2	Display Override August
TM - Client 1	Display Override August

Advanced Search

After you've tweaked your criteria to get the results you want, press on **Select in Navigation Pane** and then **Action - Batch Edit**.

SETTINGS

CHANGE SAVED HOST NAME



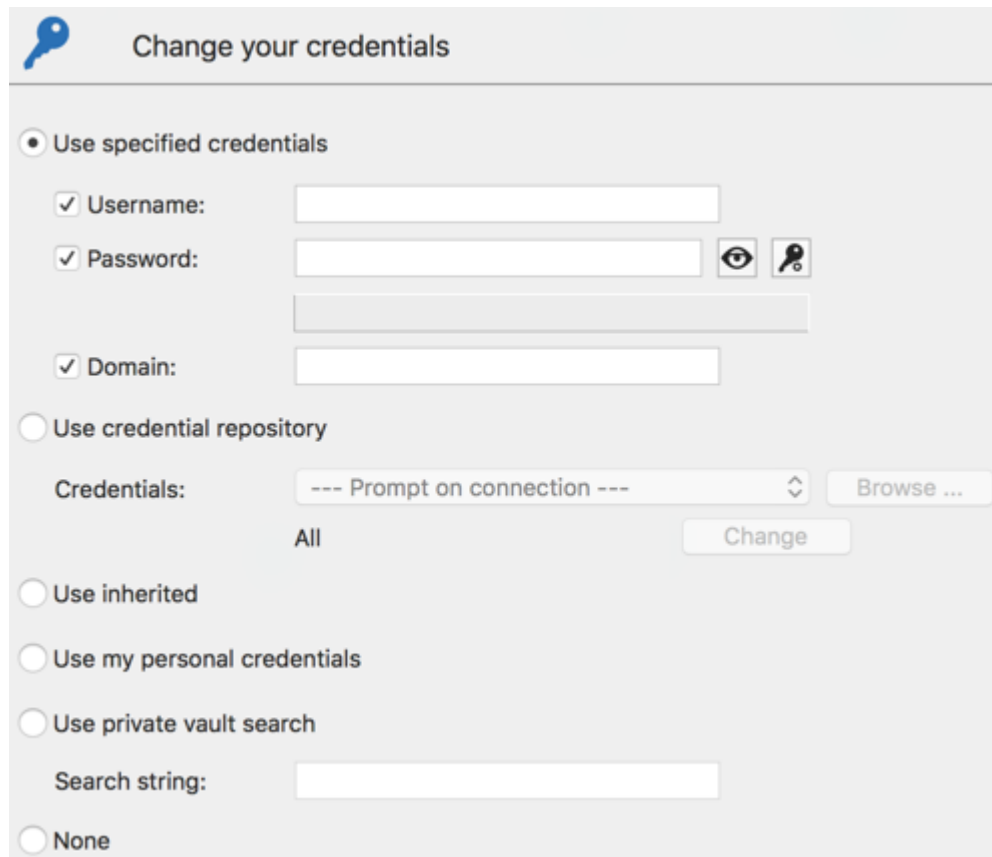
The "Change your host names" dialog box has a title bar with a monitor icon and the text "Change your host names". Below the title bar, there is a label "Host name:" followed by a text input field. At the bottom right, there are two buttons: "Cancel" and "Save".

Change Saved Host Name

You can change multiple host name at the same time.

CHANGE SAVED CREDENTIALS

You can change the configured credentials for multiple sessions in a batch.



Change Saved credentials

OPTION	DESCRIPTION
Use specified credentials	Use a specific username, password and domain.
Use credential repository	Use a Credential entry linked entry which can can be external credentials like KeePass for example. This is very useful for sharing or reusing existing credentials among entries.

OPTION	DESCRIPTION
Use inherited	Use the credentials of it's parent entry or group.
Use my personal credentials	This allows you to use one set of credentials to replace or emulate the ones from your Windows session. See My Personal Credentials topic.
Use User Vault search	Use credentials stored in your User Vault .
None	Do not use any credentials.

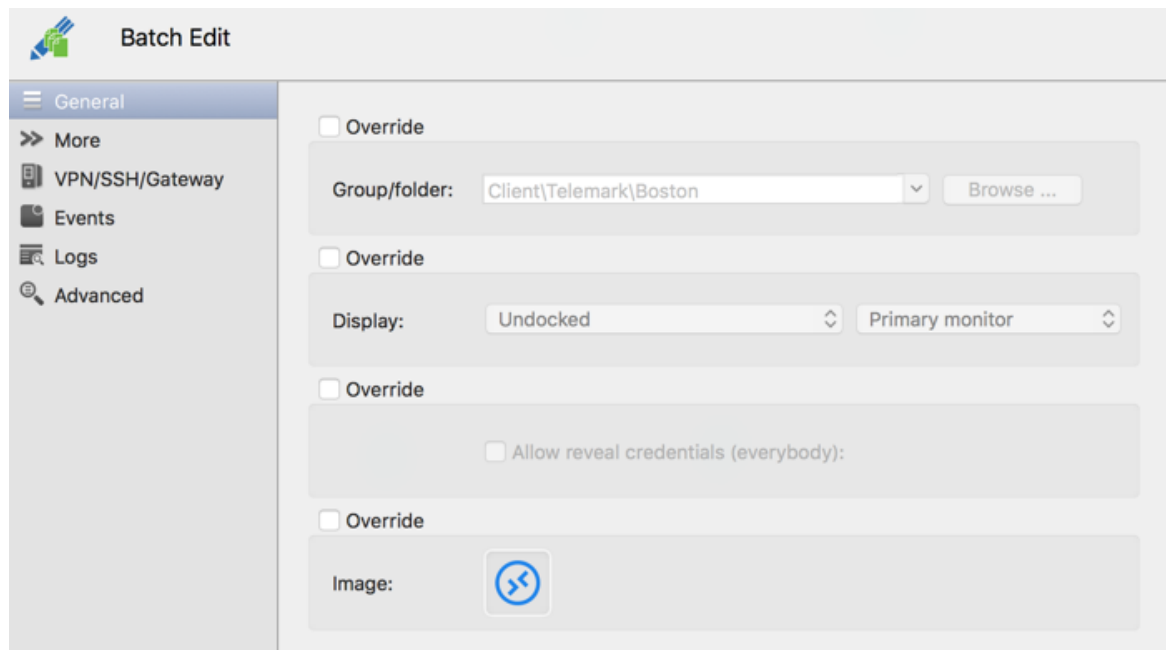
RESET ALL SAVED CREDENTIALS

Clear all existing credentials for the selected sessions.

RESET ALL SAVED PASSWORDS

Clear all existing passwords for the selected sessions.

EDIT SESSIONS (GENERAL SETTINGS)



Batch Edit - General Settings

Edit Sessions (General Settings) allows you to change common sessions settings simultaneously. The session can be of any type, because a common set of options are shared among sessions. The following common general settings can be changed:

- Group/Folder
- Display
- Allow show credentials (everybody)
- Image
- Description
- Keywords/Tags
- VPN
- Events
- Logs
- Advanced Settings tab

EDIT SESSIONS (SESSION TYPE SETTINGS)



Edit Sessions Session Type Settings is only available for specific session types like RDP.

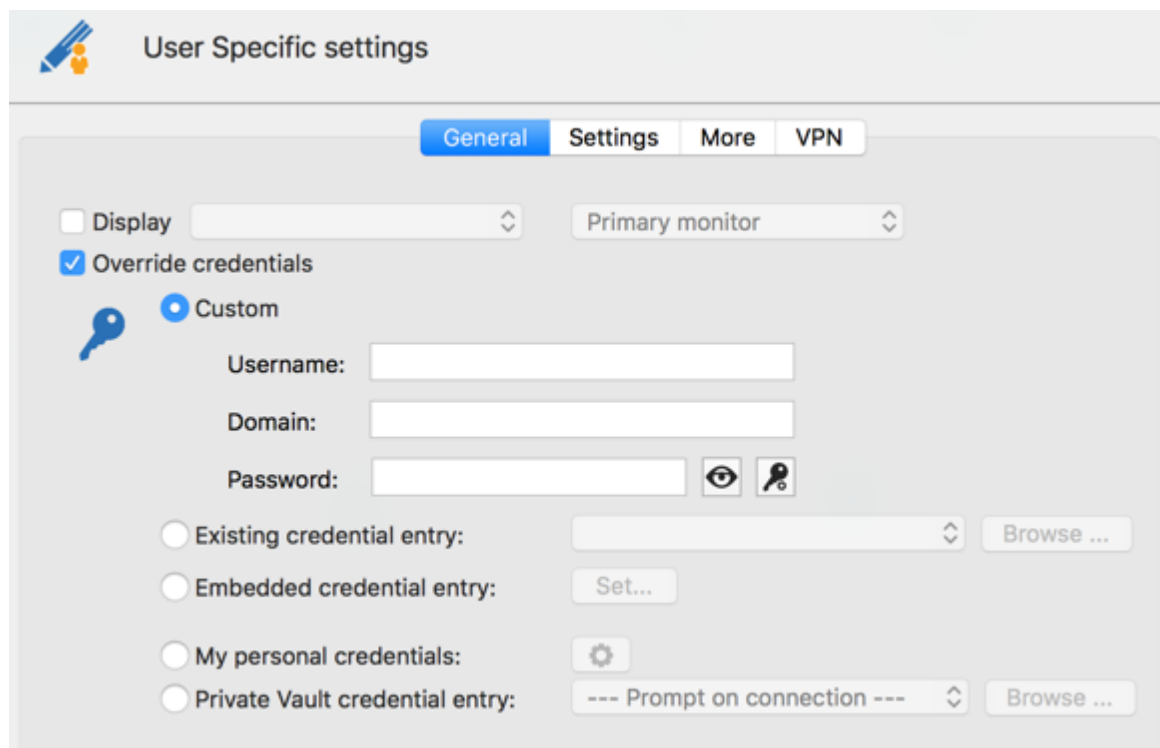
The screenshot shows the 'Batch Edit' dialog box with the 'General' tab selected. The dialog has a title bar with a blue icon and the text 'Batch Edit'. Below the title bar are tabs for 'General', 'Display', 'Local Resources', 'Programs', 'Experience', 'Connection', and 'Advanced'. The 'General' tab contains the following fields and options:

- Computer name:** A text input field with a 'Browse ...' button to its right.
- Port:** A dropdown menu showing 'Default' with a copy icon to its right. Below it is the text 'Set the port to 0 to use the default port'.
- Username:** A text input field.
- Domain:** A text input field.
- Password:** A text input field with an eye icon and a key icon to its right.
- ☐ **Edit logon settings in batch**
- ☐ **Open console (Admin mode)**
- ☐ **Always ask for credentials**
- RDP type:** A dropdown menu showing 'Normal'.
- RDP Engine:** A dropdown menu showing 'Default'.

Batch Edit - Session Type

EDIT SESSIONS (USER SPECIFIC SETTINGS)

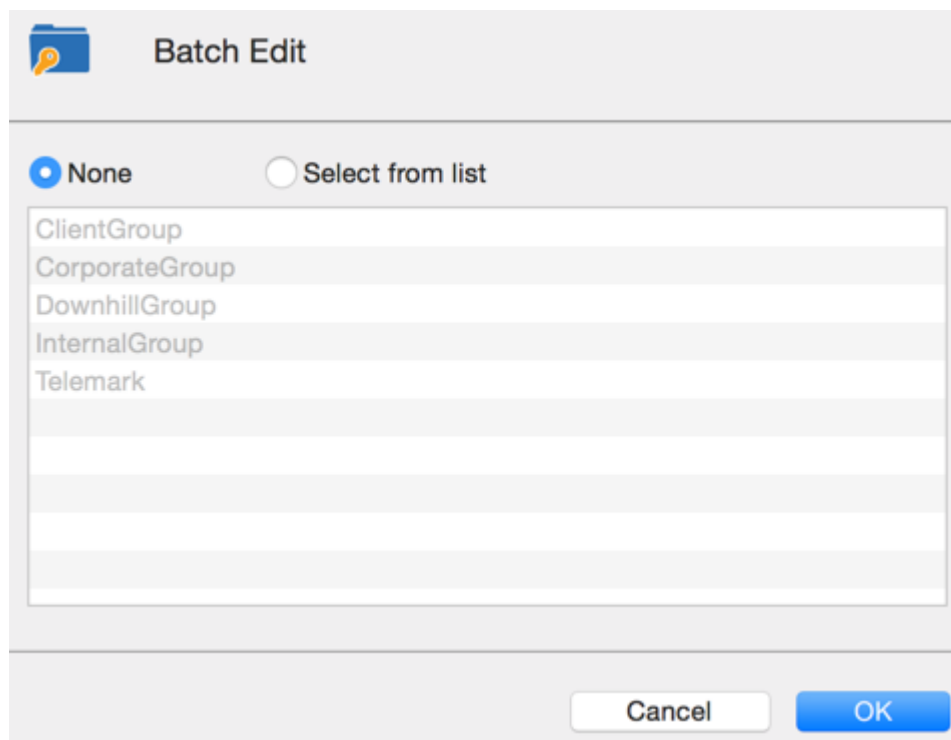
User Specific Settings can be modified in a batch if they're supported by the session type.



Batch Edit - User Specific settings

EDIT SESSIONS (SECURITY GROUP)

Use the Edit Sessions (Security Group) option to apply a new security group on multiple sessions.



Batch Edit - Security Group

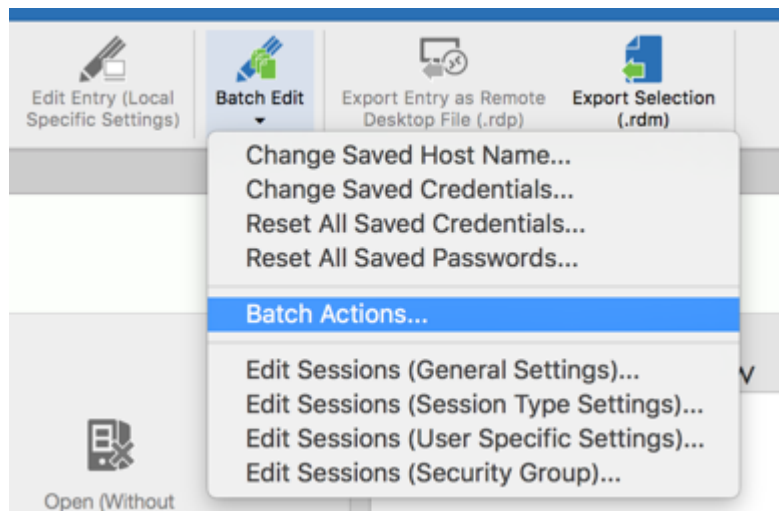
6.4.6.1 Batch Actions

DESCRIPTION

Use the **Edit - Batch Edit - Batch Actions** to change the settings of multiple sessions in one operation. It can be used for a batch action command on a group of sessions.



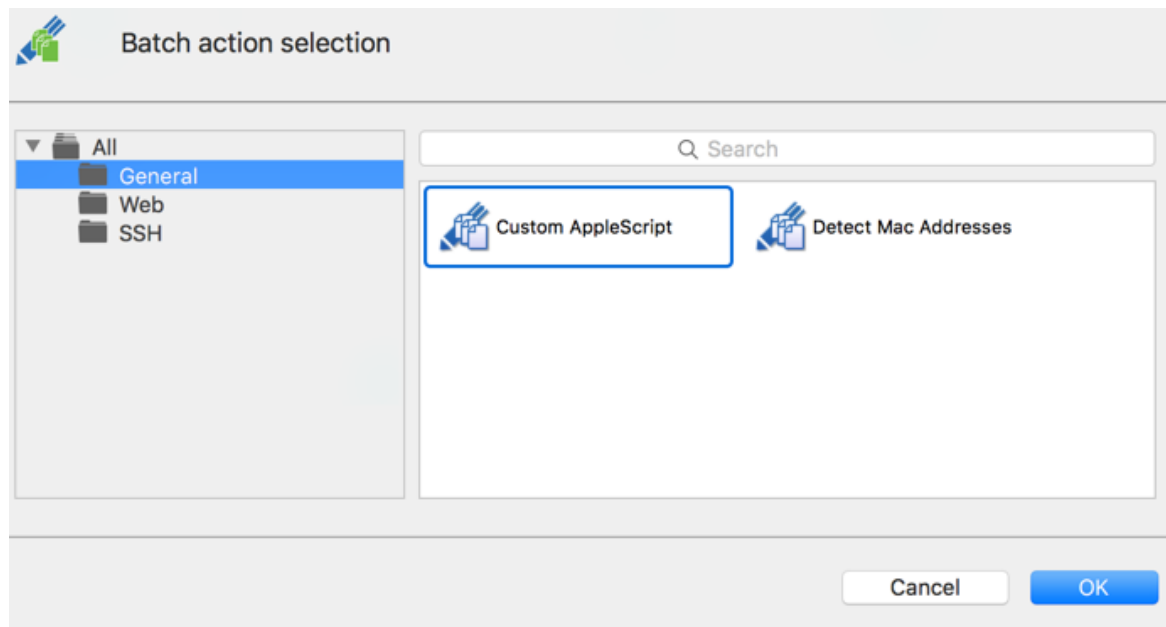
Batch Actions are only applied to entries currently selected in your navigation pane.



Batch Edit - Batch Actions

SETTINGS

GENERAL



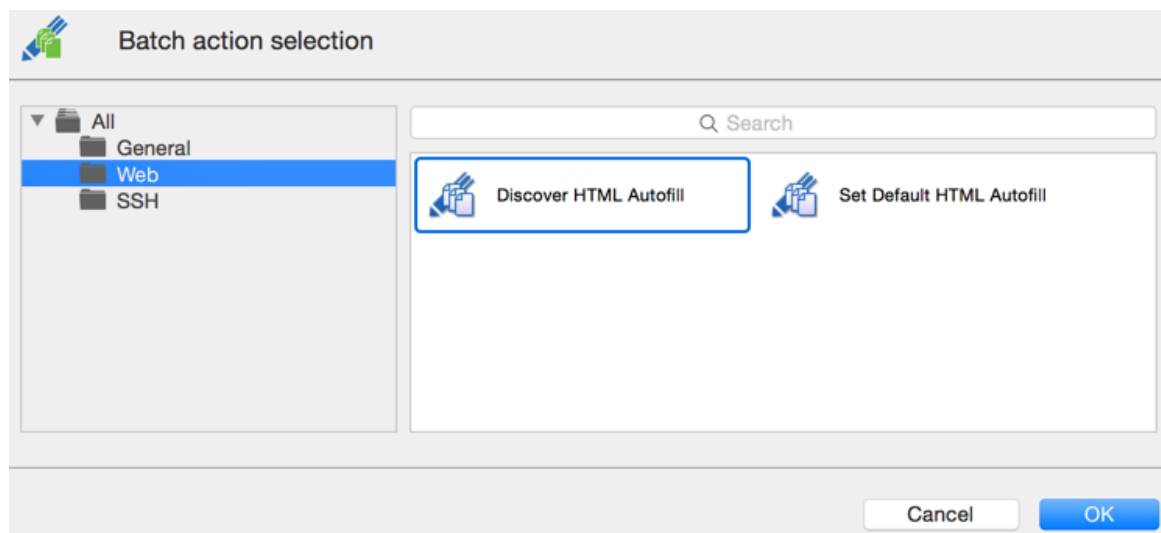
Batch action - General

OPTION	DESCRIPTION
Custom AppleScript	Run a custom Applescript command on multiple selected sessions all at once to update the properties.
Detect Mac Addresses	It will scan all of your sessions in your current database to detect if there is any mac addresses.

WEB



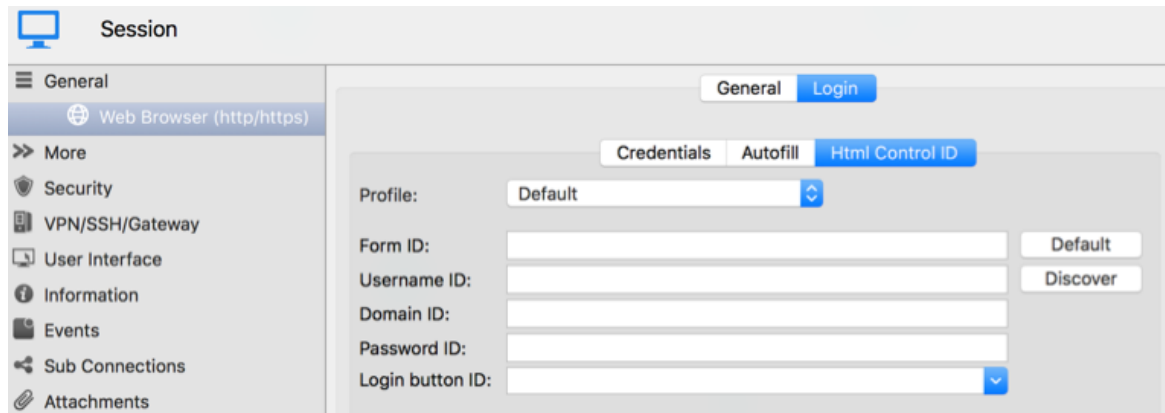
These options will only work for Web Browser session



Batch Action - Web

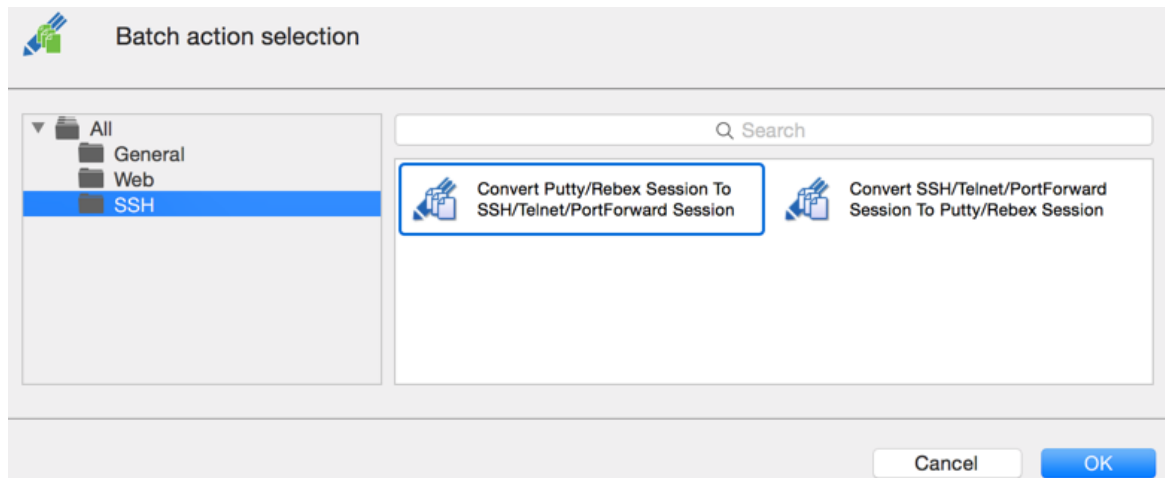
OPTION	DESCRIPTION
Discover HTML Autofill	Once you have selected your web browser sessions and run the batch action, it will automatically fill in the HTML login information.

OPTION	DESCRIPTION
Set Default HTML Autofill	Once you have selected your web browser sessions and run the batch action, it will automatically fill in the Username ID and Password ID fields with the default values.



Web Browser Html Control ID settings

SSH



Batch Action - Web

OPTION	DESCRIPTION
Convert Putty/Rebex	It will automatically convert your selected Putty/Rebex sessions into SSH/Telnet/PortForward sessions.

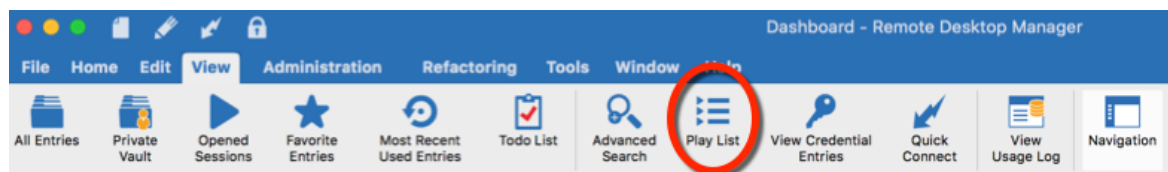
OPTION	DESCRIPTION
Session to SSH/Telnet/PortForward Session	
Convert SSH/Telnet/PortForward Session to Putty/Rebex Session	It will automatically convert your selected SSH/Telnet/PortForward sessions into Putty/Rebex sessions.

6.4.7 Play List

DESCRIPTION

The Play List feature in Remote Desktop Manager for Mac is a lot like a music play list. 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.

The Play List feature is accessible from **View - Play List**.



View ribbon - Play List

For more information, please consult the following topics:

- [Actions](#)
- [Management](#)
- [Default at Startup](#)

6.4.7.1 Actions

DESCRIPTION

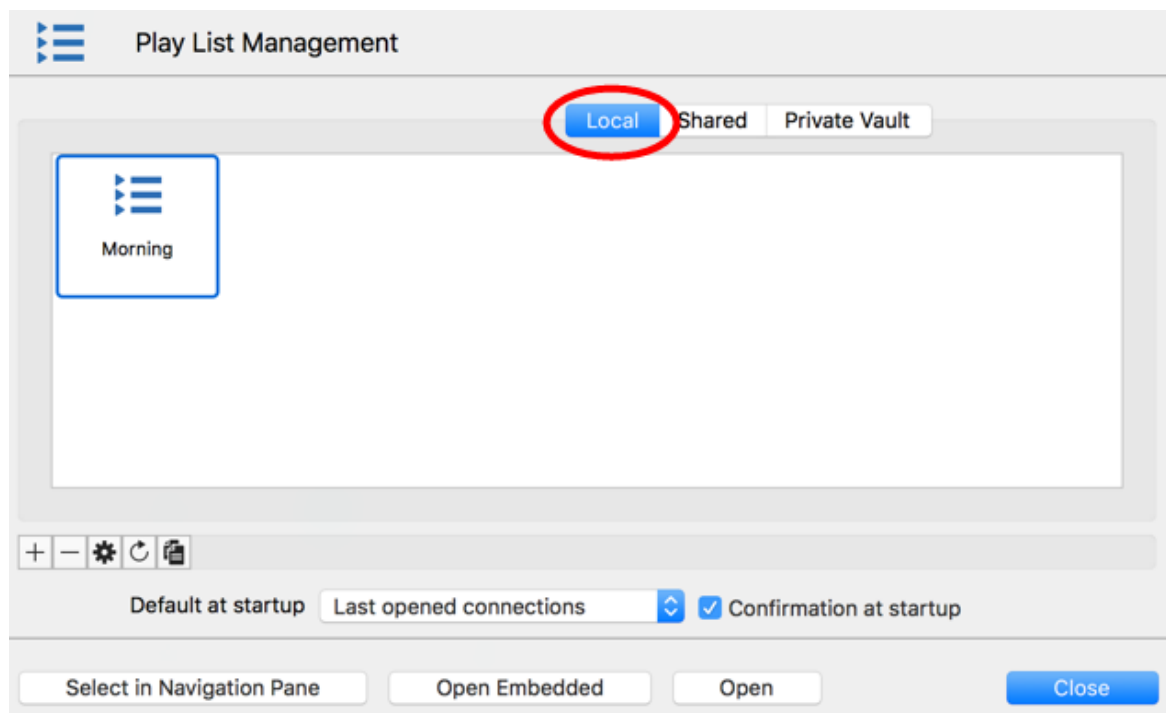
You can create Local or Shared play List in Remote Desktop Manager. There's several methods to create or edit a Play List:

- Create Play List by selecting entries in the Navigation Panel
- Create Play List with Opened Tabbed Sessions
- Create Play List with No Selection
- Edit an existing Play List

SETTINGS

LOCAL PLAY LIST

Local Play List is saved on the local computer and is not available to other users.

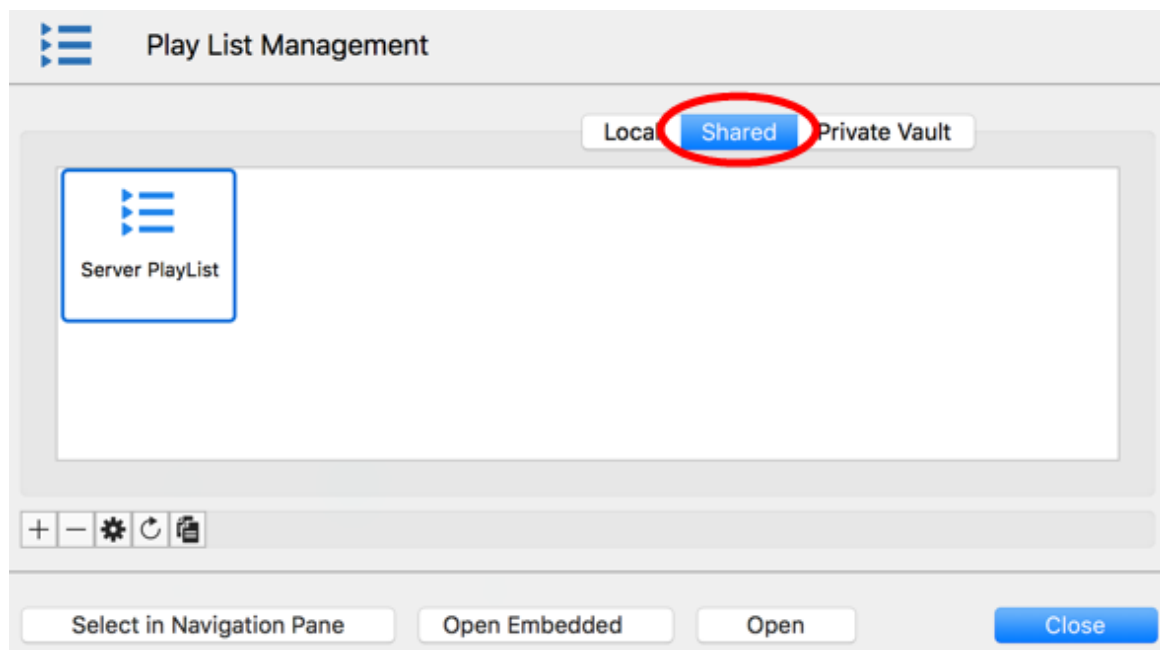


Play List Management - Local Play List

SHARED PLAY LIST

The **Shared Play List** is saved in the database and can be used by all users. The Shared Play List can be launched from the Navigation Pane as well as from the menu **View - Play List**.

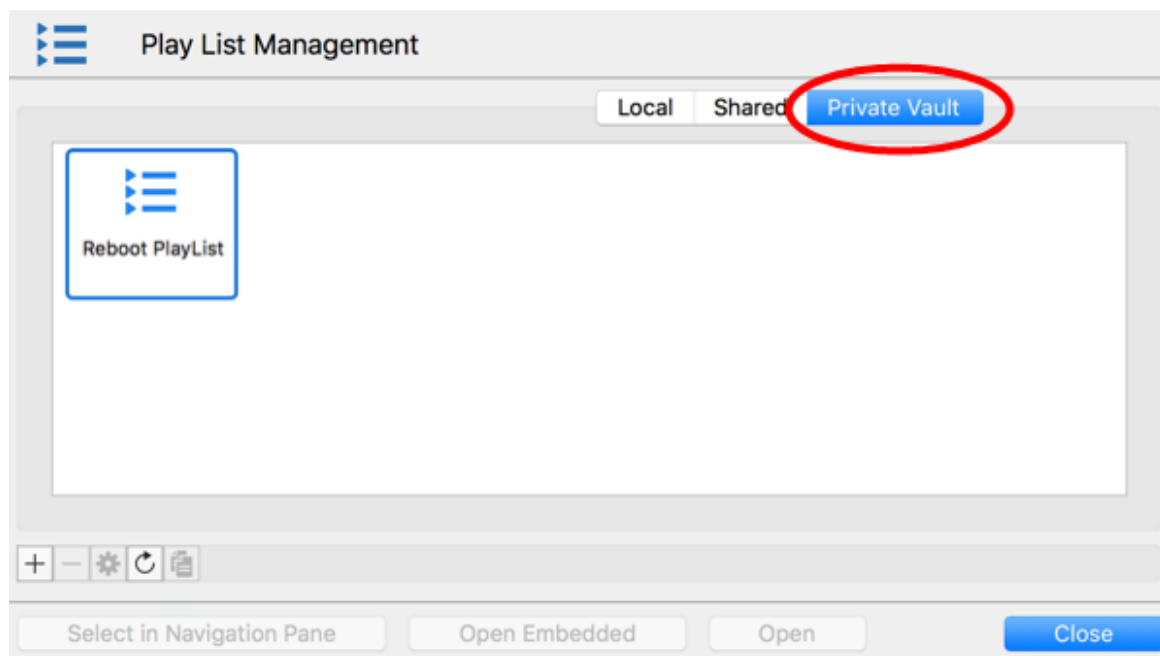
Please consult the Play List Entry topic for more information on the Shared Play List session.



Play List Management - Shared Play List

USER VAULT PLAY LIST

The **User Vault Play List** is saved inside your User Vault which is a user centric repository, it allows each user to create Play List that only them can access.

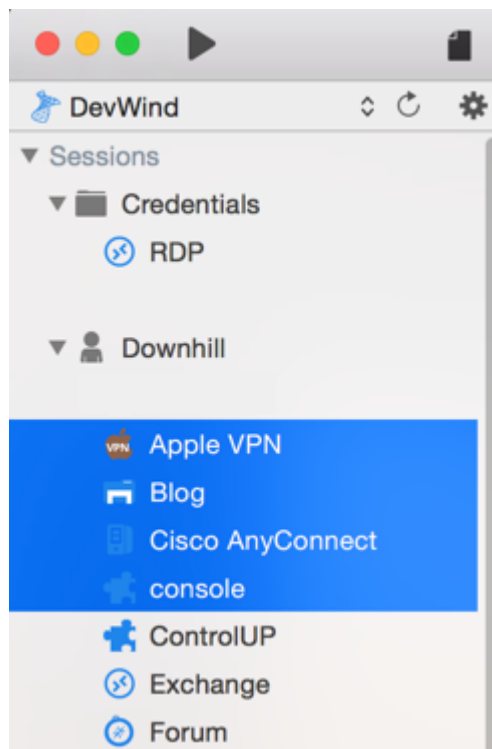


Play List Management - User Vault Play List

ACTIONS

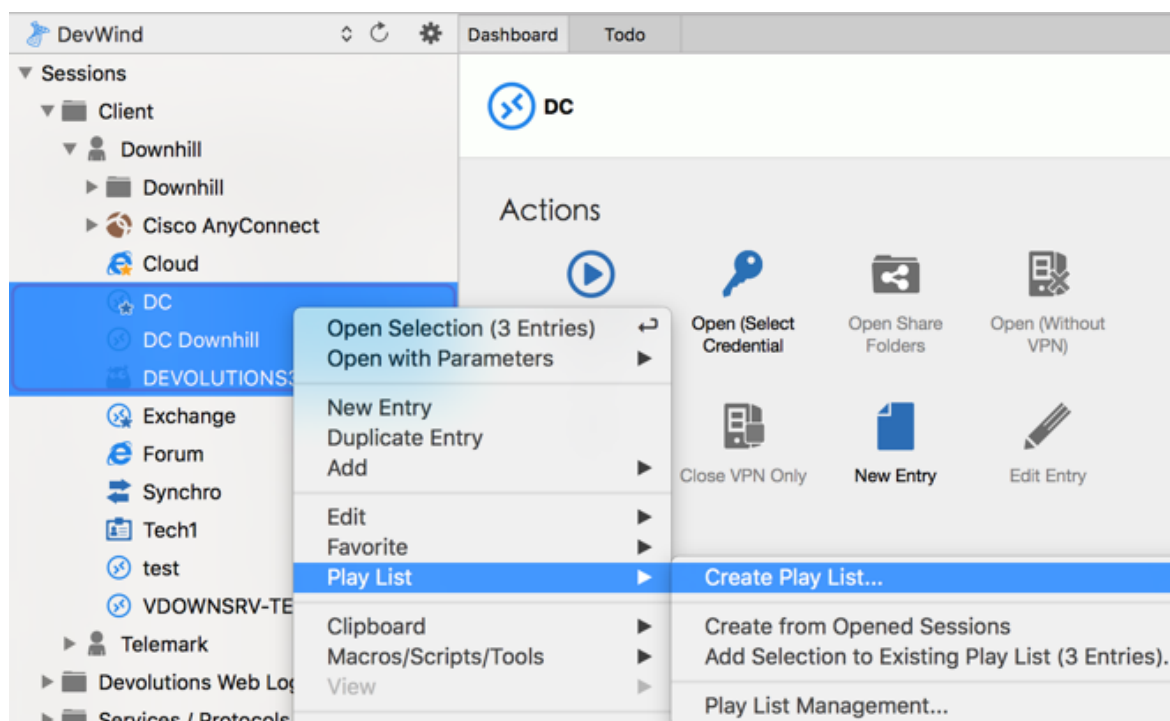
CREATE PLAY LIST BY SELECTING ENTRIES IN THE NAVIGATION PANE

1. Select the entries for your Play List in your Navigation Pane using Command + click.



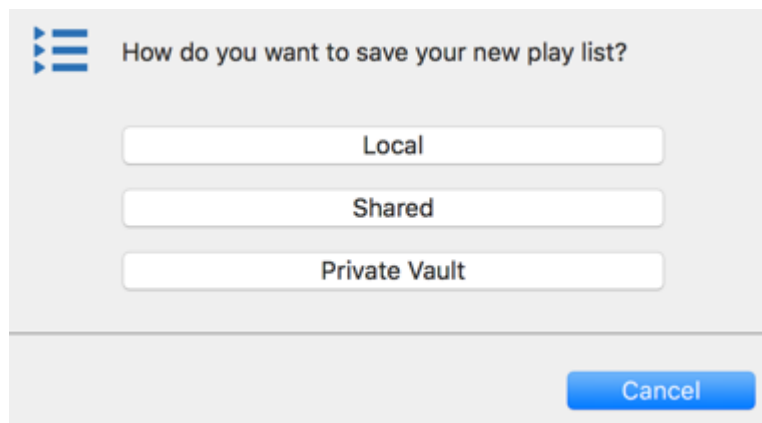
Navigation Pane

2. Right click in your Navigation Pane and select ***Play List - Create Play List***.



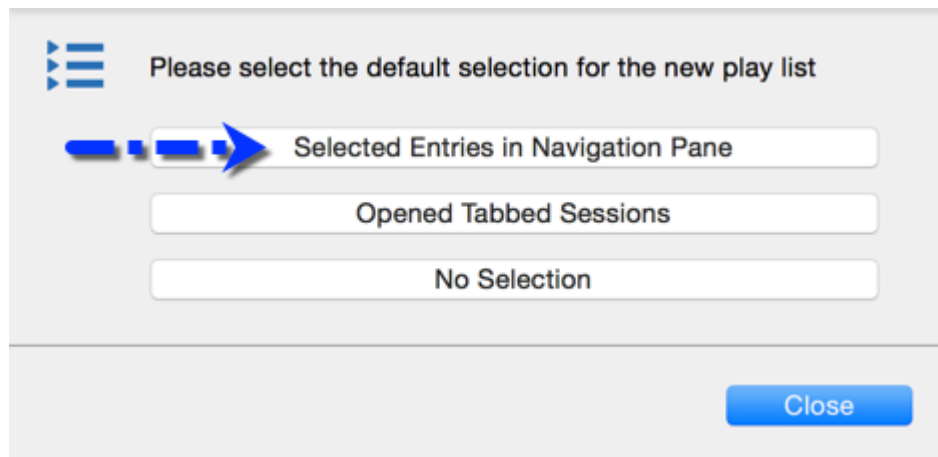
Create Play List

3. Choose if you wish to save your Play List Locally, Shared or in your User Vault.



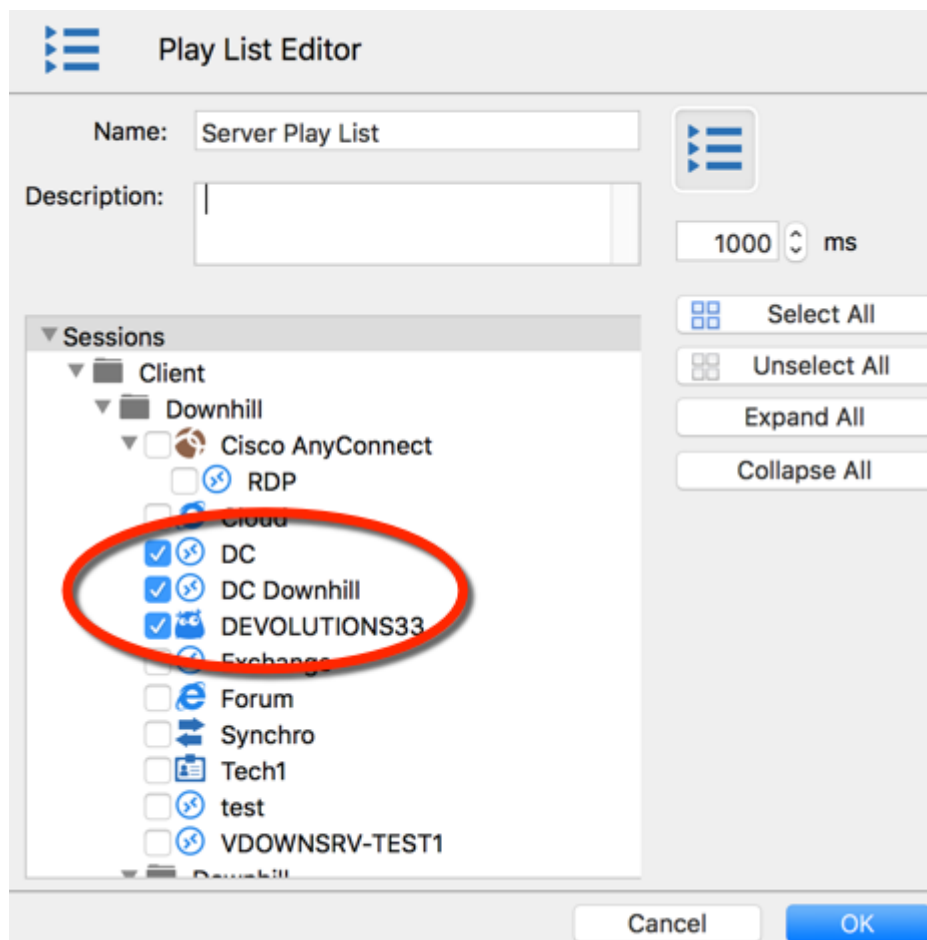
Save Play List

4. Then click on **Selected Entries in Navigation Pane.**



Selected Entries in Navigation Pane

3. You will notice that all your preselected entries from your Navigation Pane are already selected in the Play List Editor. Provide a name and a short description for your Play List and click **OK**

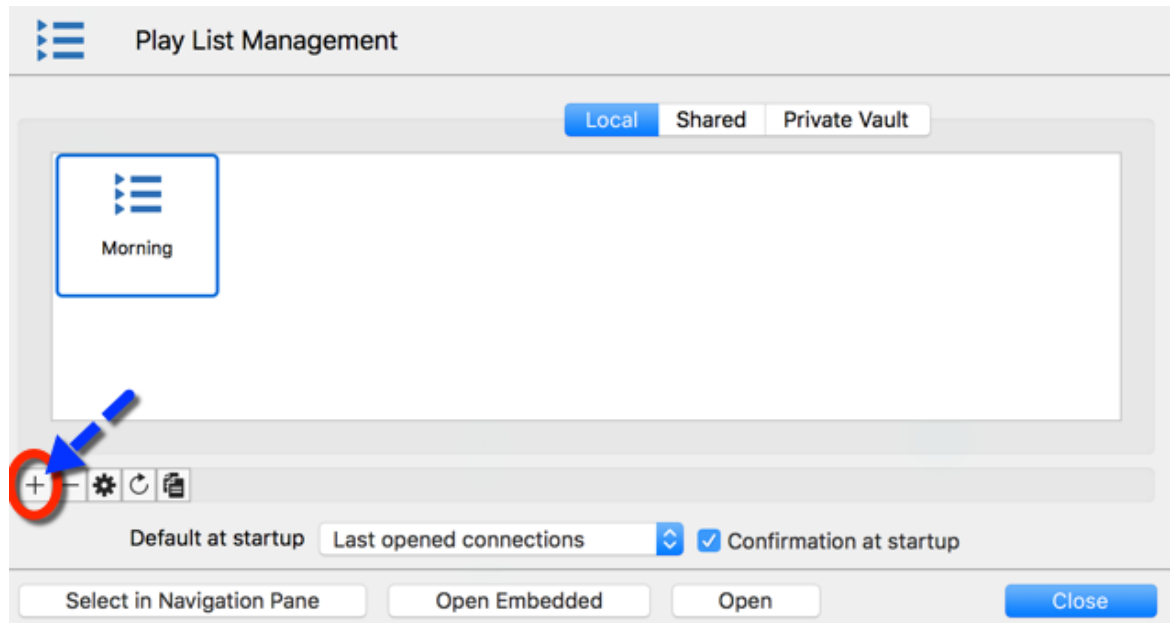


Play List Editor



The ***wait time*** is used to set the delay between opening different entries.

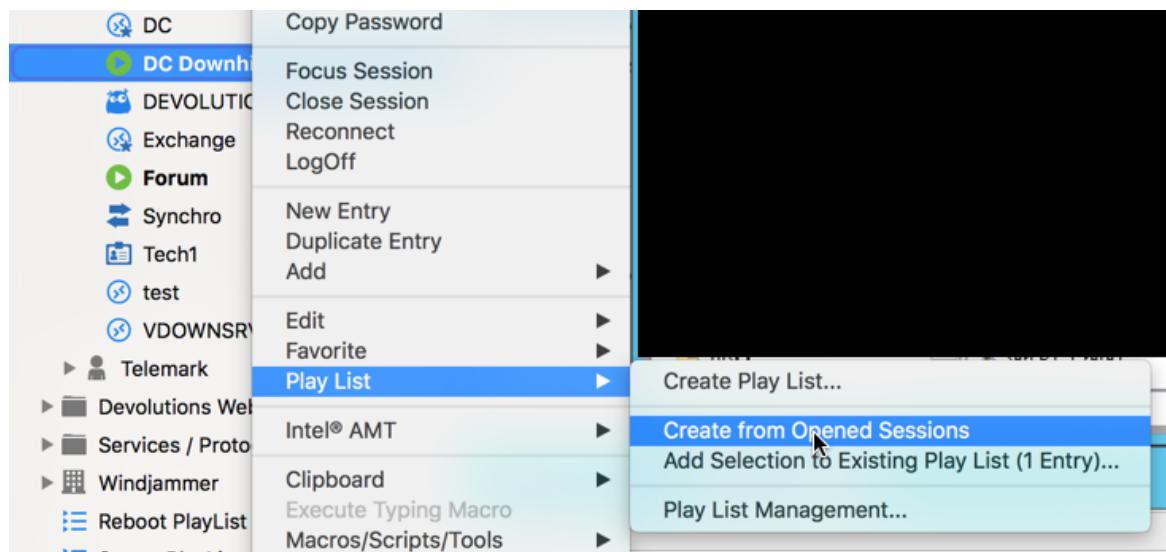
You could also create a new Play List by using the ***View - Play List*** and then clicking on the plus to create a New Play List.



Create a New Play List

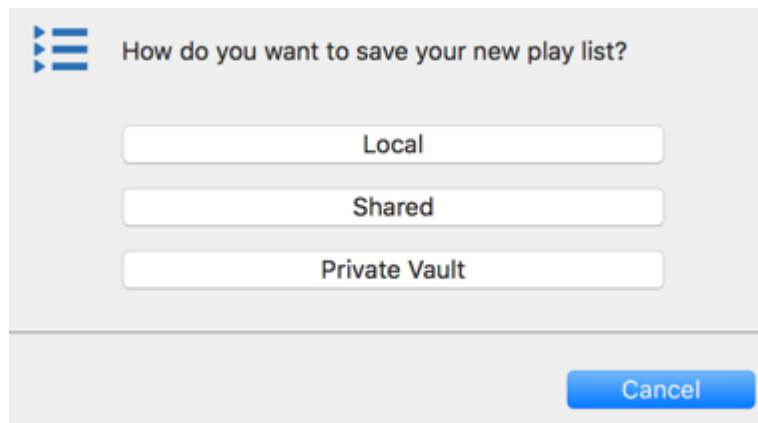
CREATE PLAY LIST WITH OPENED TABBED SESSIONS

1. Open all the sessions you wish to add to your new Play List in Embedded mode.
2. Right click in your Navigation Pane and select ***Play List - Create from Opened Sessions***.



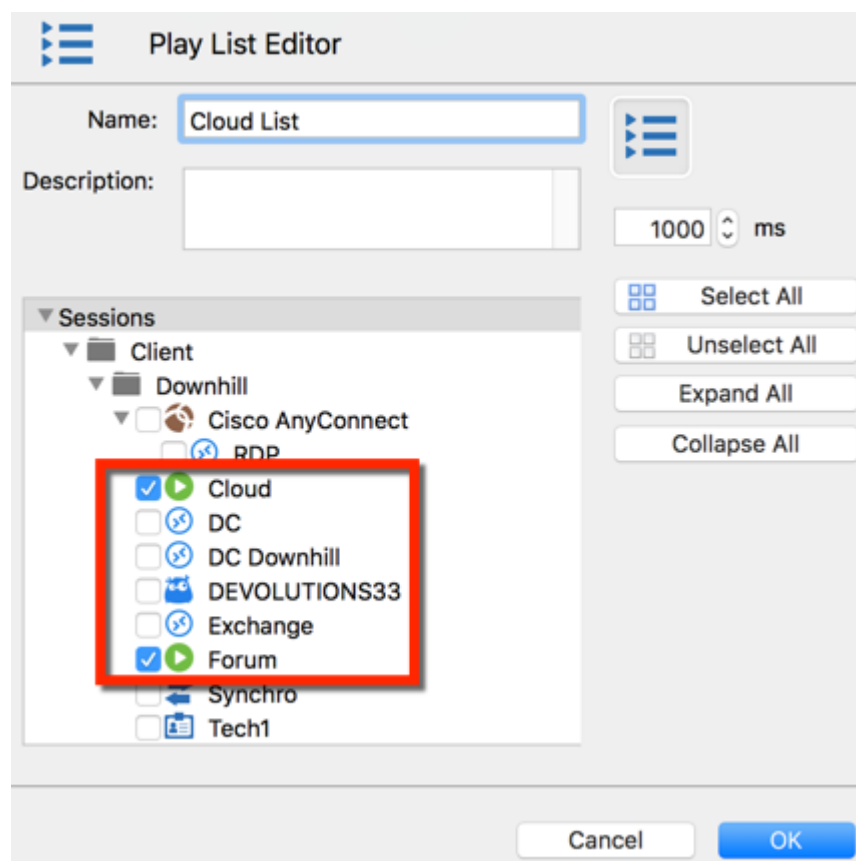
Play List - Create from Opened Sessions

3. Select if you wish to save your Play List Locally, Shared or in your User Vault.



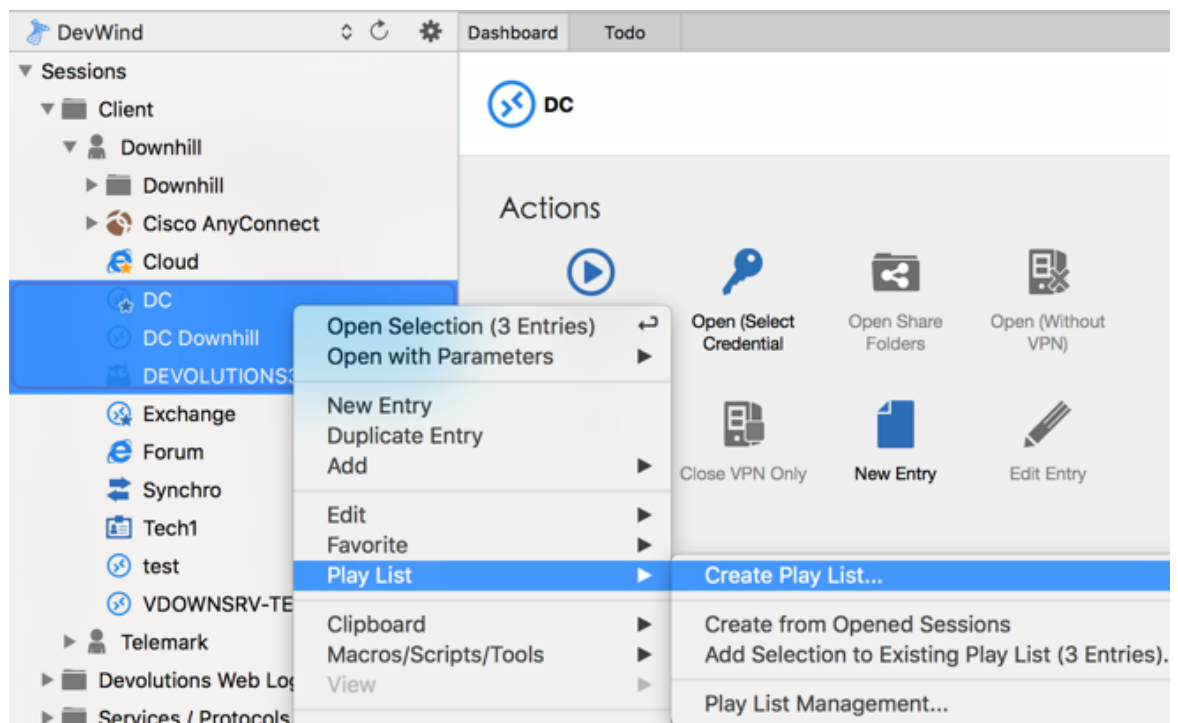
Save Play List

3. You will notice that your opened sessions are already preselected in your Play List Editor. Provide a name and a short description to your Play List and click **OK**.

*Play List Editor*

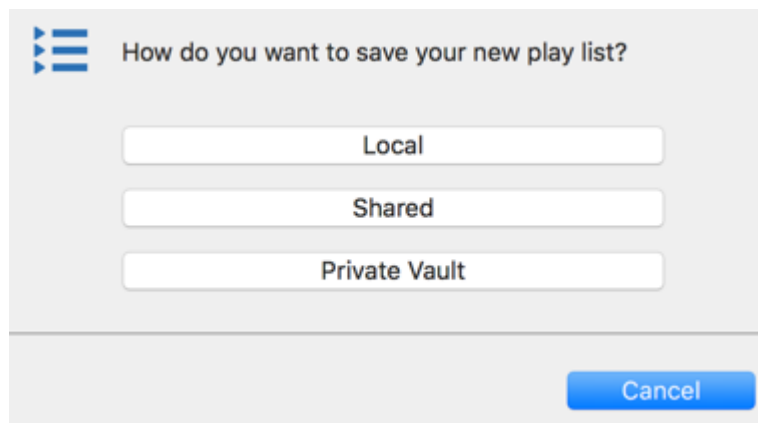
CREATE PLAY LIST WITH NO SELECTION

1. Right click in your Navigation Pane and select ***Play List - Create Play List.***



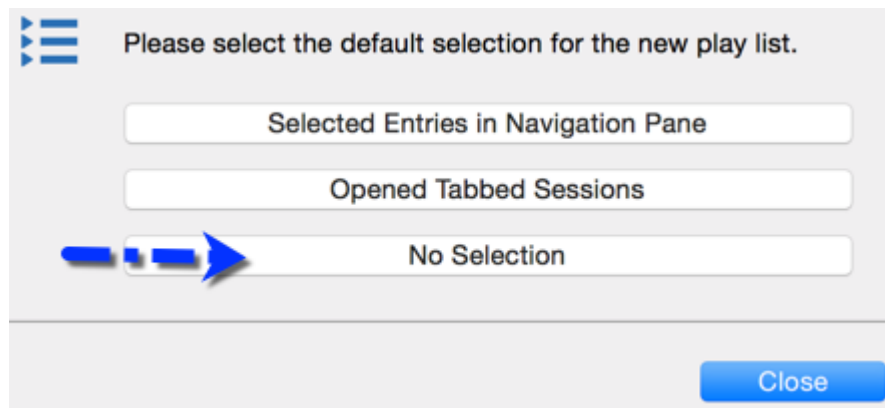
Create Play List

2. 3. Choose if you wish to save your Play List Locally, Shared or in your User Vault.



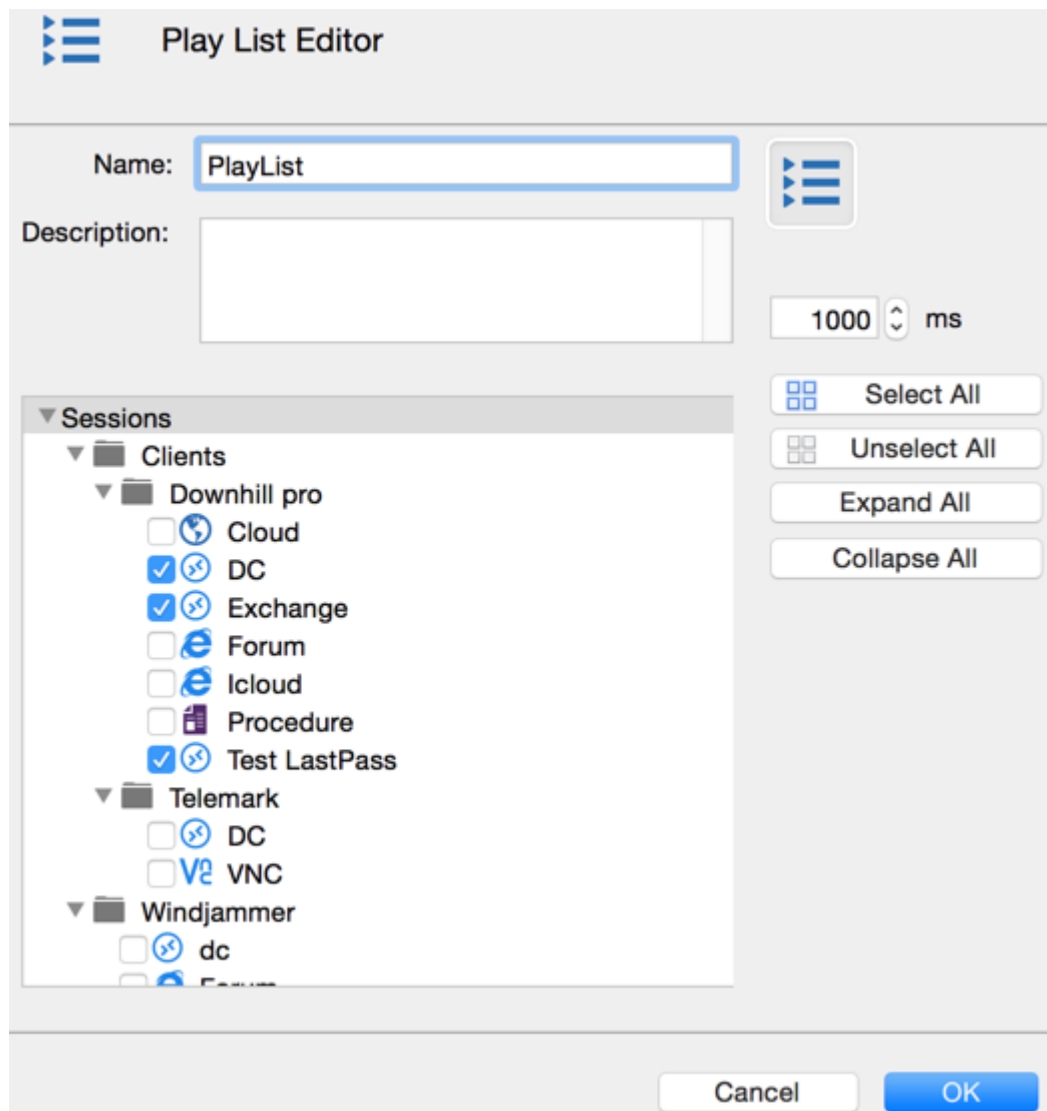
Save Play List

3. In **Entry - Play List - Create Play List** select the option **No Selection**.



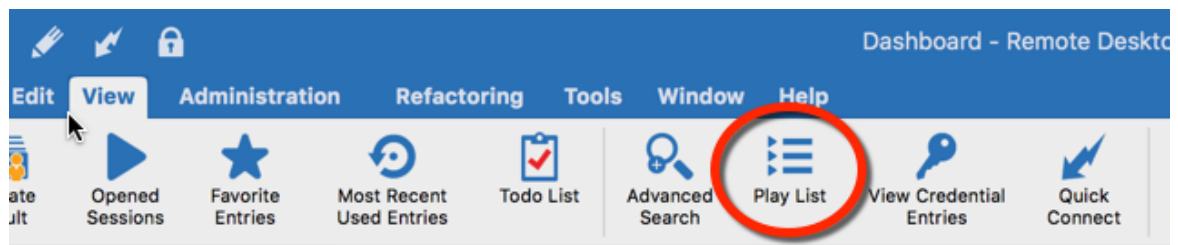
No Selection

2. Select the entries you wish too add to your Play List by checking the box beside the entry name. Provide a name and a short description to your Play List and click **OK**.

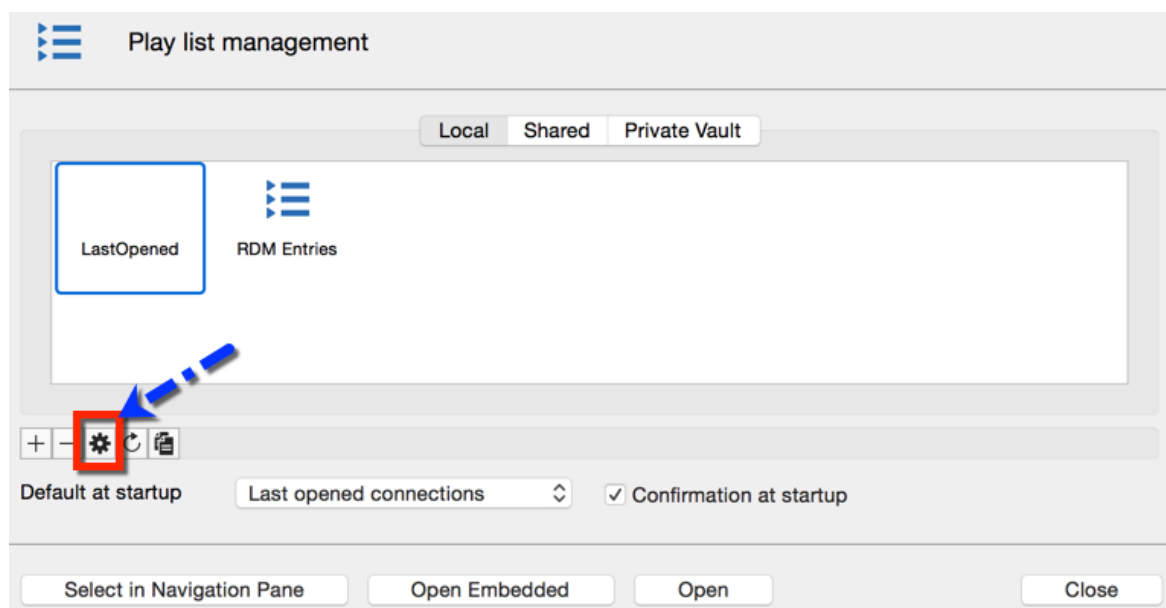


*Play List Editor***EDIT AN EXISTING PLAY LIST**

1. You can edit a Play List in **View - Play List**.

*View - Play List*

2. Select the Play List you wish to modify and then click on the wheel to edit the entry.

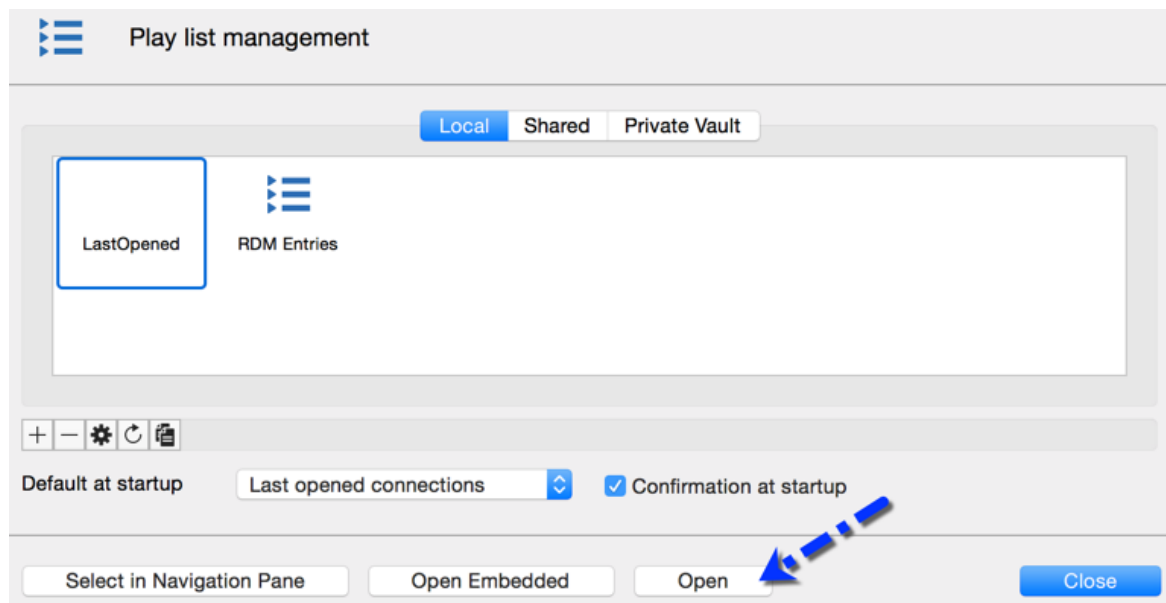
*Play List Management - Edit***6.4.7.2 Management****DESCRIPTION**

There's 3 way to Open a Play List:

OPTION	DESCRIPTION
Open	Items will open using the specified mode in each session.
Open Embedded	Items will all open using the embedded mode.
Select in Navigation Pane	Items will be selected in the Navigation Pane, this allow you to choose another command to run on the section as a second step.

OPEN ITEMS IN DEFAULT MODE

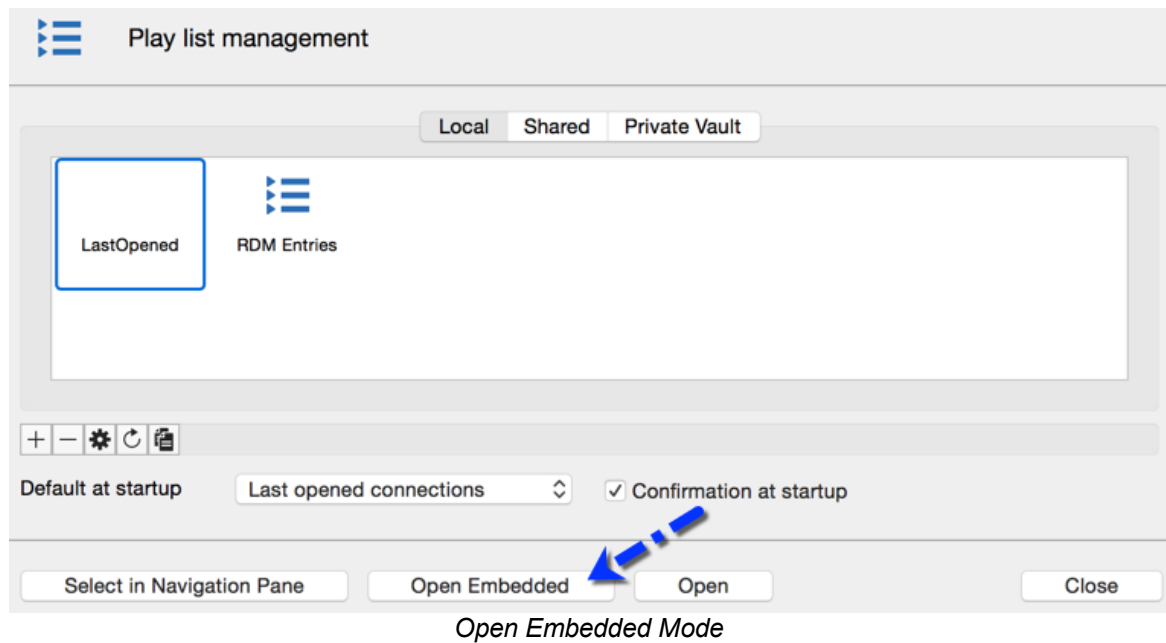
In **View - Play List** and select the Play List to open and click on **Open**



Open Default Mode

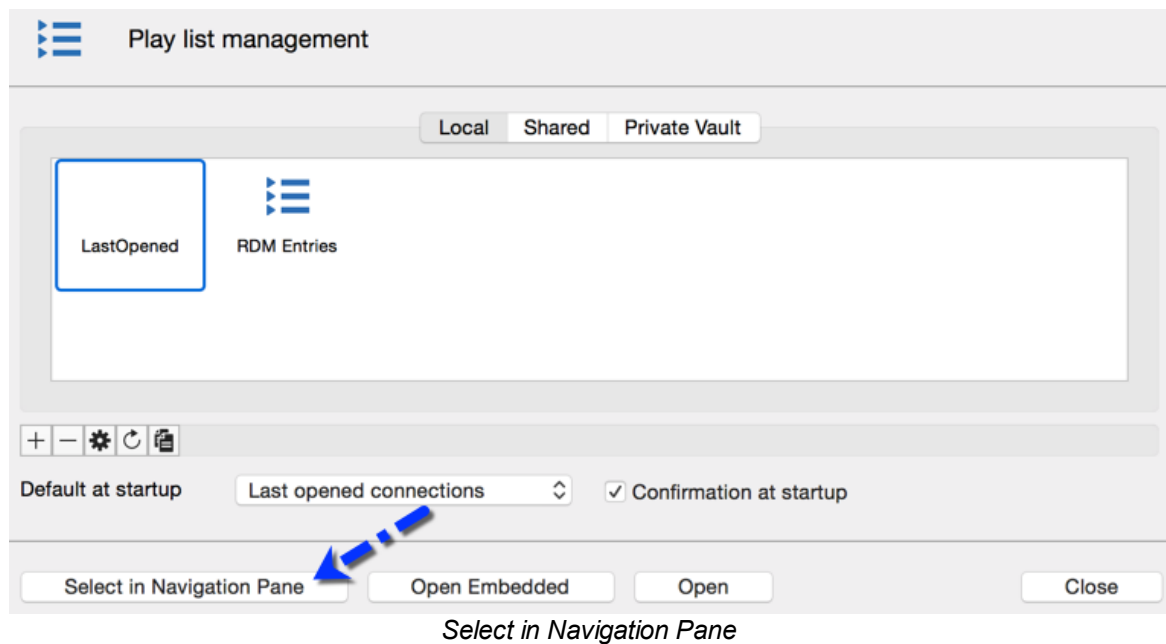
OPEN ITEMS IN EMBEDDED MODE

In **View - Play List** select the Play List to open and click on **Open Embedded**.



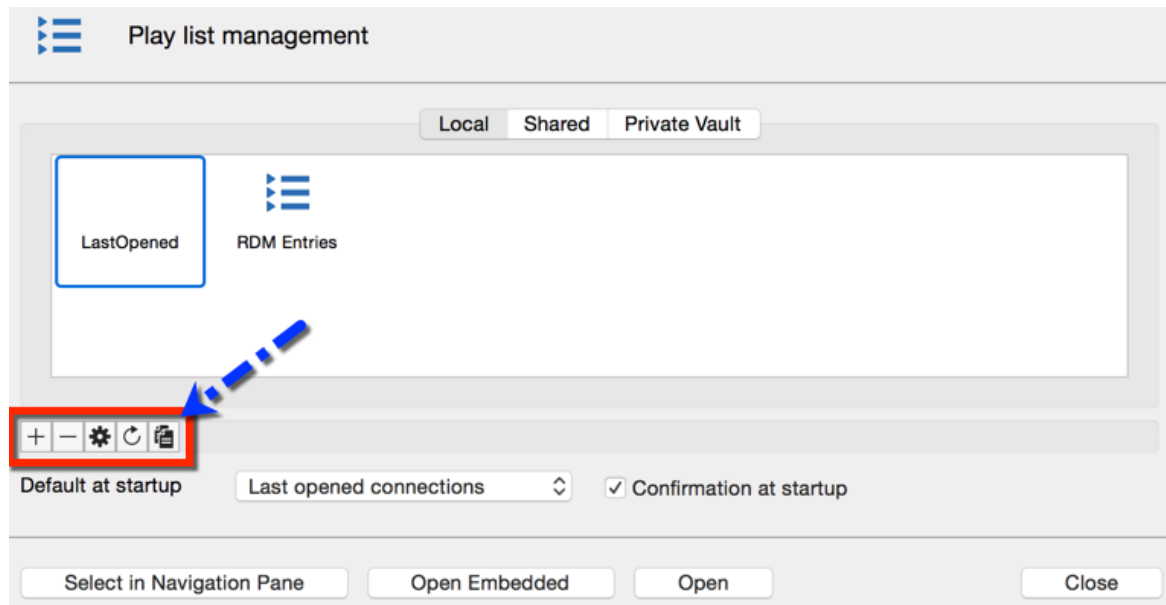
OPEN ITEMS WITH SELECT IN NAVIGATION PANE

In **View - Play List** select the Play List to open and click on **Select in Navigation Pane**. Then select the desired entries in your **Navigation Pane** using Command + click.








MENU

You can use the menu in the Play List Management for multiple options.



Play List Management Menu

SETTINGS

OPTI ON	DESCRIPTION
	Create a new Play List.
	Delete an existing Play List.
	Edit the selected Play List.
	Refresh your Play List Management.
	Copy the selected Play List.

6.4.7.3 Default at Startup

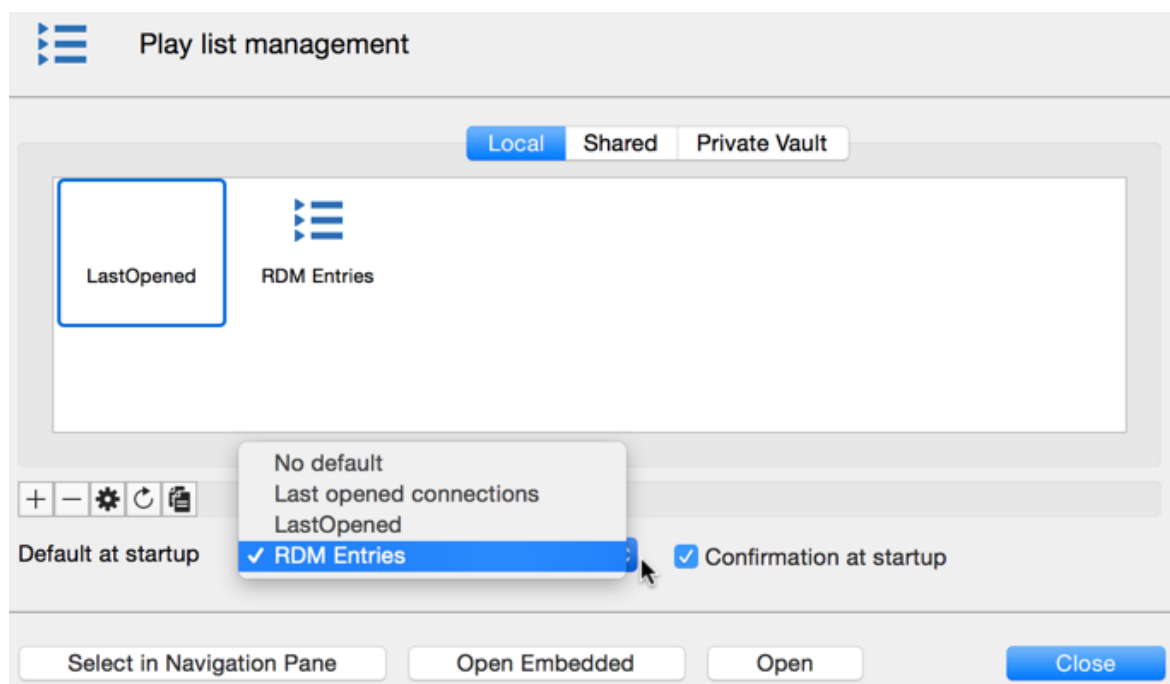
DESCRIPTION

A Play List can be set to be launched when Remote Desktop Manager for Mac is opened.

SETTINGS

DEFAULT PLAY LIST AT STARTUP

To define a default Play List, click **Edit - Play List - Play List Management**. Then select your Play List in the **Default at startup** drop down.



Default at startup



If you check the **Confirmation at startup** box a confirmation window will be displayed before opening your Play List. You can then enable or disable sessions manually or you can cancel the process completely.

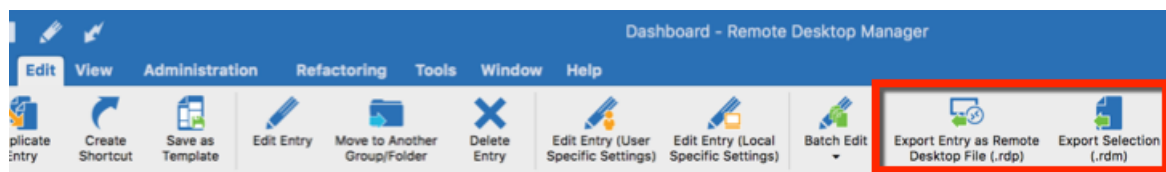
The last opened connections option will offer to reopen the sessions that were opened at the time you closed Remote Desktop Manager for Mac. That Play List is maintained automatically at every Remote Desktop Manager for Mac closing.

6.4.8 Export Entry

DESCRIPTION

Use the Export options to export selected entries from Remote Desktop Manager for Mac.

SETTINGS



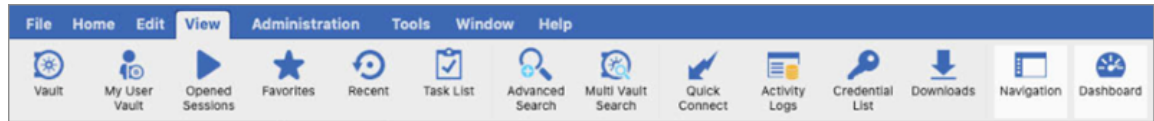
Edit ribbon - Export options

OPTION	DESCRIPTION
Export Entry as Remote Desktop File (.rdp)	Export your selected entries in a Remote Desktop File (.rdp) format.
Export Selection (.rdm)	Export your selected entries in a .rdm file that can then be imported into any Remote Desktop Manager for Mac 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 View

DESCRIPTION

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



View Tab

Refer to the following topics for more information:

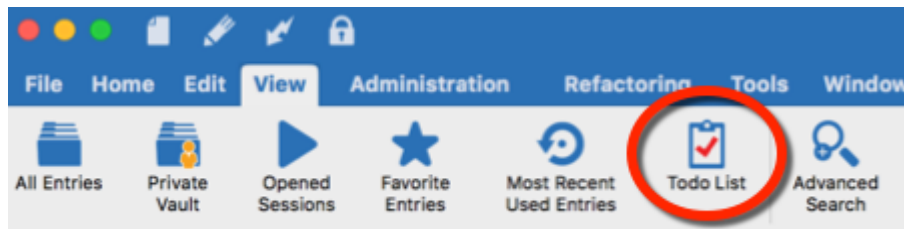
- [Vault](#) and [My User Vault](#)
- [Opened Sessions](#)
- [Favorites](#)
- [Recent](#)
- [Task List](#)
- [Advanced Search](#)
- Multi Vault Search
- [Quick Connect](#)
- [Activity Logs](#)
- Credential List
- Downloads
- [Navigation](#)
- [Dashboard](#)

6.5.1 Todo List

DESCRIPTION

ToDo lists helps you follow the work that needs to be done by your staff on specific entries.

To view a complete list of all the current Todo List in your current data source click on Todo List in the View ribbon.



View ribbon - Todo List



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

To learn more about Todo List please see:

- [Add](#)
- [Search](#)
- [Export](#)

6.5.1.1 Add

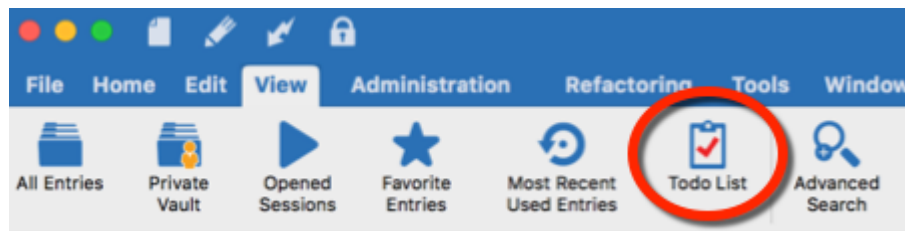
DESCRIPTION

Create tasks in the ToDo List to help you follow what work needs to be performed by your staff.

SETTINGS

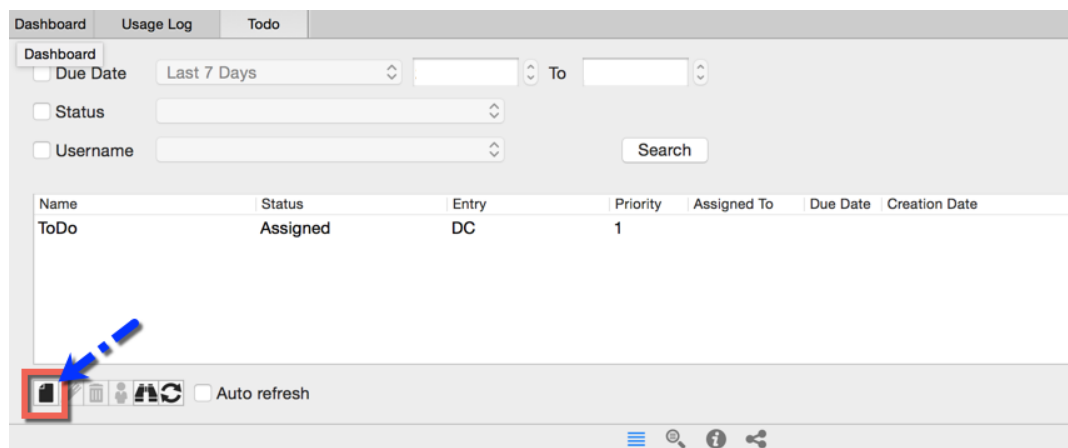
CREATION OF A TASK

1. In the **View** ribbon click on **ToDo List**.



View ribbon - Todo List

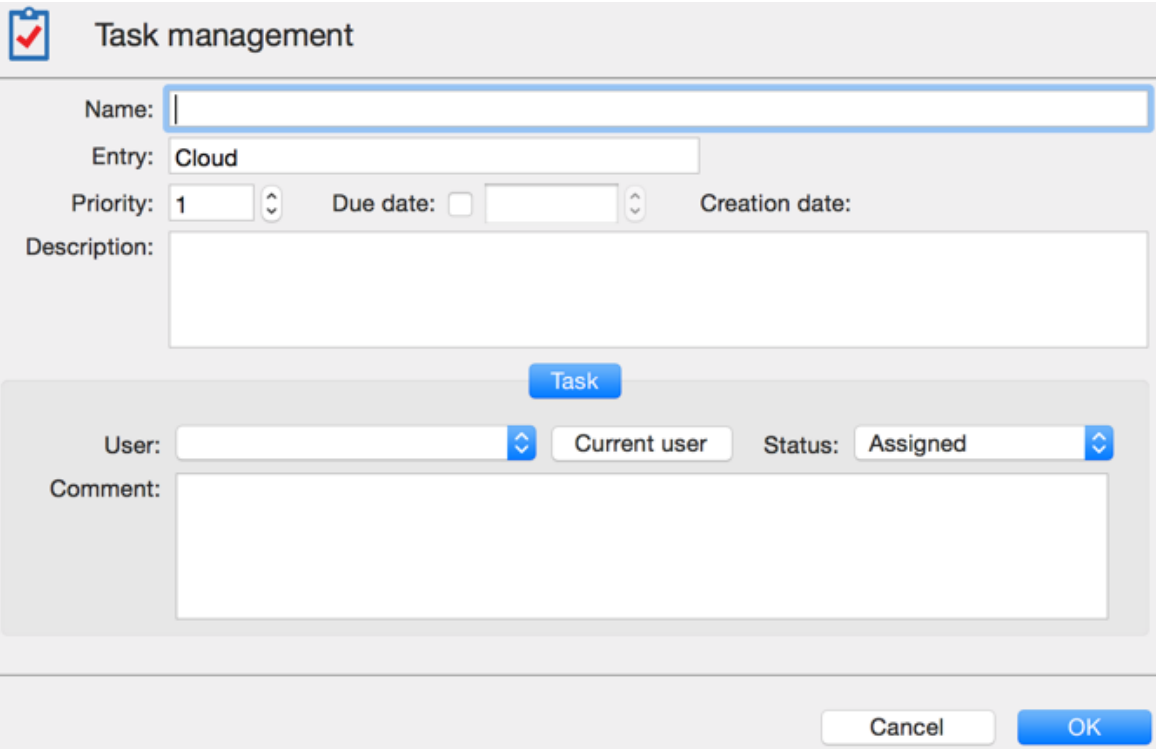
2. Click on **Add new Todo**



Add new todo

Add new todo

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



The image shows a macOS-style dialog box titled "Task management" with a clipboard icon. It contains several input fields: "Name:" (empty), "Entry:" (set to "Cloud"), "Priority:" (set to "1"), "Due date:" (checkbox and empty date field), and "Creation date:" (empty). There is a large "Description:" text area. A blue "Task" button is centered below the description. Below this, there is a "User:" dropdown menu (showing a blue arrow), a "Current user" button, and a "Status:" dropdown menu (set to "Assigned" with a blue arrow). A "Comment:" text area is at the bottom. At the very bottom of the dialog are "Cancel" and "OK" buttons.

Task Management



Tasks can be assigned to a user.

CURRENT USER

You can use **Current user** to set your identity instantly.

STATUS


Different status can be applied to a task:

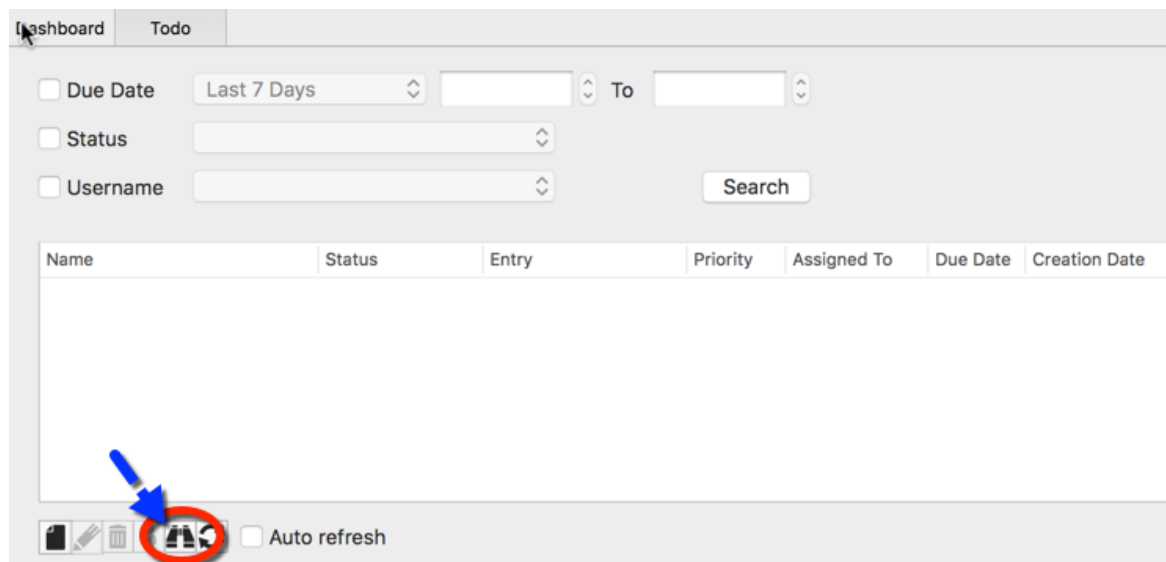
- Assigned
- Canceled
- Closed
- Done

- In progress
- Open
- Postponed

6.5.1.2 Search

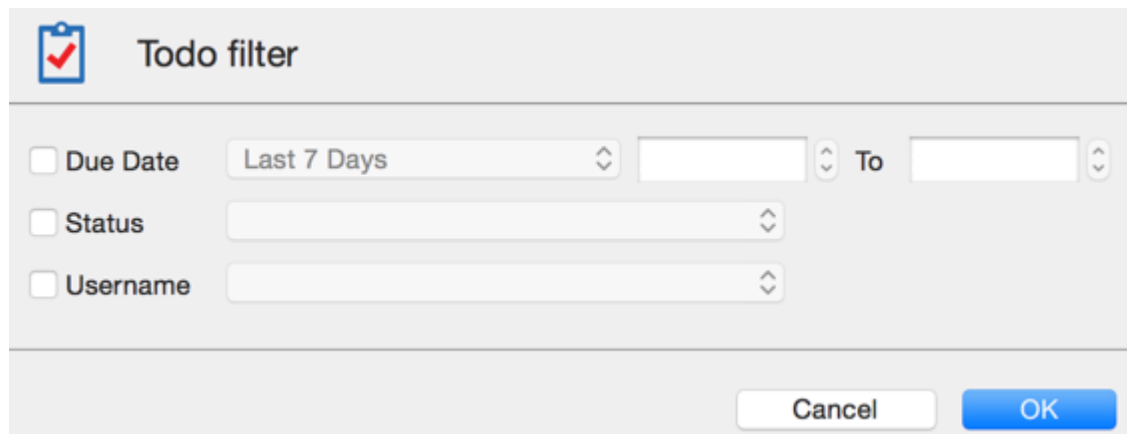
DESCRIPTION

When multiple tasks are created in Remote Desktop Manager for Mac, perform a search by clicking on the Search button  to filter out the list of displayed tasks.



Todo Search

You can filter your search by Due Date, User name or by Status.

*Todo filter*

6.5.1.3 Export

DESCRIPTION

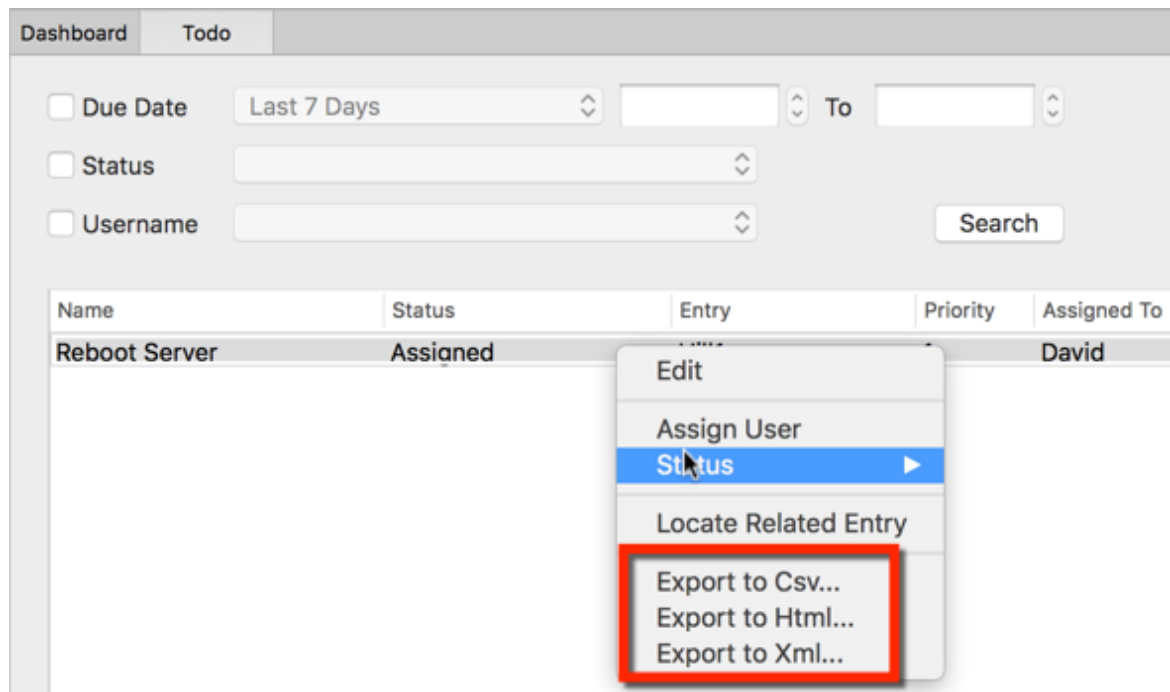
Tasks can be exported in different types of files for printing or for reviewing.

HOW TO EXPORT TASKS



Before exporting tasks, you can perform a [Search](#) to filter out the task list.

Right-Click on a task and select the file format.



Export Todo List

Export options

EXPORT FILE TYPE

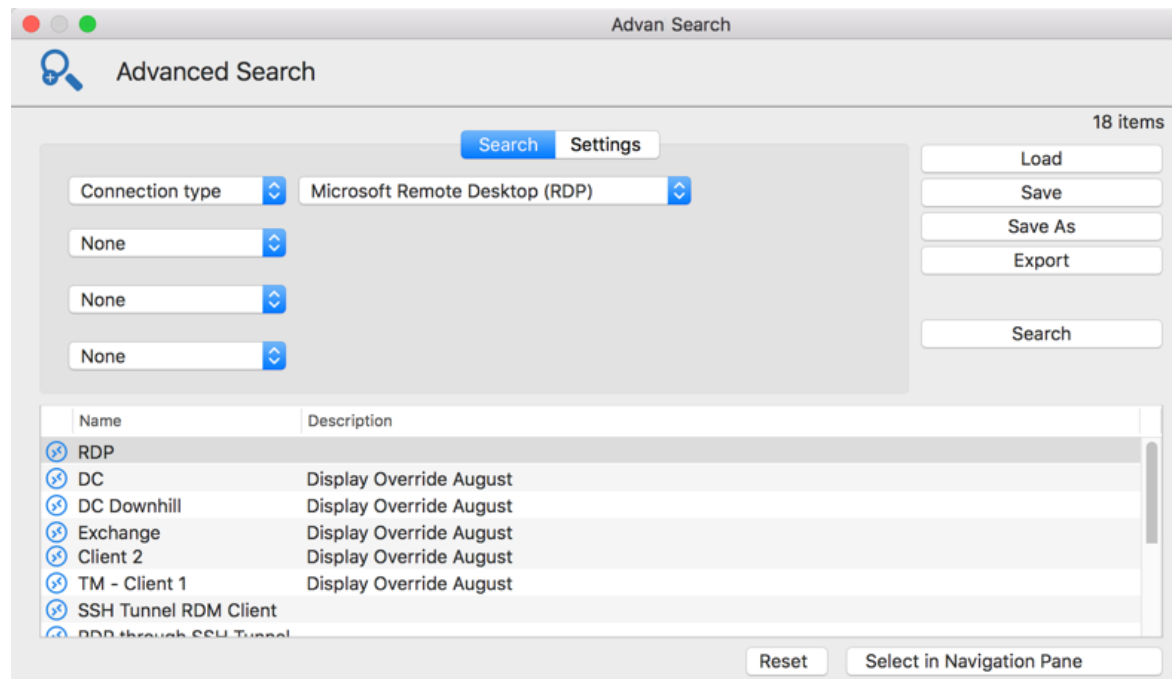
You can export tasks in these file formats:

- CSV
- HTML
- XML

6.5.2 Advanced Search

DESCRIPTION

The **Advanced Search** feature allows you to make powerful searches with multiple criteria at once. You can then easily select your search result in your Navigation Pane.



Advanced Search

SETTINGS

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

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

OPTION	DESCRIPTION
Select in Navigation Pane	Select your search result in your Navigation Pane. This option can be used in combination with a Batch Edit.

There will be a drop-down list next to certain 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.

6.5.3 View Usage Log

DESCRIPTION

The shared session log offers a robust log 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 **View-Logs**, 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 Usage Log

☒ Date: Yesterday To

☐ Username: ☐ Machine name:

☐ Message: ☐ On Open Comments:

☐ Group/Folder: ☐ On Close Comments:

Group	Connection	Message	On Open Comment	Log Date	End Date/Time	Activ
	Server PlayList	New entry added				
Client\Telemark\...	Client 1	Entry edited				
Client\Telemark\...	Client 1	Entry shortcut deleted				
	My personal credentials	Exported entry (Native)				
Client\Telemark\...	Client 1	New entry shortcut added				
Client\Telemark\...	Client 1	Entry edited				
Client\Downhill\...	LastPass Account	Entry edited				
Client\Downhill\...	LastPass - training@d...	Entry edited				
Client\Downhill\...	LastPass	Entry edited				
Client	Cloud	Entry deleted				
Client\Telemark\...	Firefo	Entry deleted				

View - Log - Usage Log

You can use the **View Logs** to find information for multiple sessions for a specific time or for a specific user. The window is similar to a search window and offers multiple filter types, including:

- Time period
- User name
- Machine name
- Message
- Group/Folder
- Open or Close comments

Here is a list of the columns found in your Usage Log.

OPTION	DESCRIPTION
Group	The Group/Folder where your entry is situated.
Connection	The connection being used to open your entry.
Message	Indicate the action that was done on your entry or session.

OPTION	DESCRIPTION
On Open Comment	The Open Comment is defined in the Log tab of your session, to learn more please see Logs Options.
On Close Comment	The Close Comment is defined in the Log tab of your session, to learn more please see Logs Options.
Log Date	Indicate the date and time your session was opened or your entry was edited.
End Date/Time	Indicate the date and time when the session or entry was closed.
Active Time	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 session is opened but your view is on your Dashboard tab and not on your session tab, no Active Time will be recorded. (Please see Note 1)
Duration	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. (Please see Note 1)
User	Indicate the Windows user name and domain.
Database user name	Indicate the database user name.
Connection user	Indicate the Connection user.
Machine	Indicate the machine name.

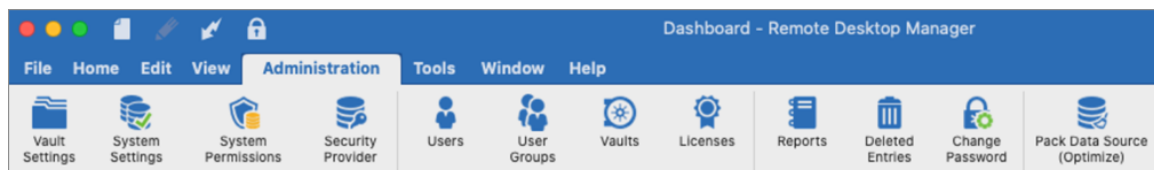
OPTION	DESCRIPTION
Connection Type	Indicate the connection type that was used.

6.6 Administration

DESCRIPTION

The Administration ribbon is only available for the Administrator of the data source since it is mostly used to manage settings and users of a data source. If the options are grayed out contact your administrator.

Also most features contained in the Administration menu requires an [Advanced Data Source](#).



Administration ribbon

Refer to the following topics for more information:

- [System Settings](#)
- [Security Provider](#)
- [User Management](#)
- [User Groups](#)
- [Vault Settings](#)
- [Deleted Entries](#)
- [Reports](#)
- [Change Password](#)

6.6.1 Data Source Settings

DESCRIPTION

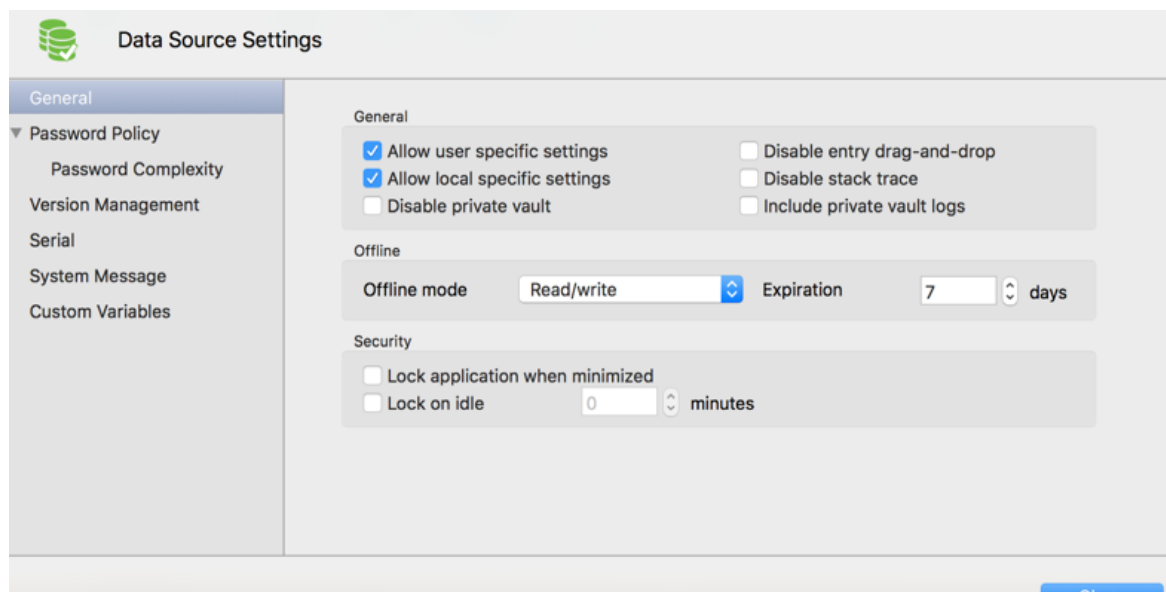
Data Source Settings is available from **Administration - Data Source Settings**.

Data source settings allows you to control many global aspects of the data source, such as Offline Mode, password policies and version management. properties. You can define general policies applicable for the whole data source.



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

SETTINGS



Data Source Settings

For more information on the different options held in the Data Source settings please see:

- [General](#)
- [Password](#)

- [Version Management](#)
- [Serial](#)
- [System Message](#)
- [Custom Variables](#)

6.6.1.1 General

DESCRIPTION

In the **General** side menu, you will be able to manage different right access specific to the data source.

Data Source Settings

General

- ☒ Allow user specific settings
- ☒ Allow local specific settings
- ☐ Disable private vault
- ☐ Disable entry drag-and-drop
- ☐ Disable stack trace
- ☐ Include private vault logs

Offline

Offline mode: Read/write Expiration: 7 days

Security

- ☐ Lock application when minimized
- ☐ Lock on idle: 0 minutes

Close

Data Source Settings - General

GENERAL

OPTION	DESCRIPTION
Allow user specific settings	Enables the use of user specific settings. See User Specific Settings for more information.

OPTION	DESCRIPTION
Allow local machine specific settings	Enables the use of local machine specific settings.
Disable User Vault	Disable the usage of the User Vault for all users of the data source.
Disable entry drag-and-drop	Entry group modification using the drag and drop will be disabled. Use this setting to avoid accidental drag and drop.
Disable stack trace	Disable the stack trace details when an error appears during the execution of the application.
Include User Vault logs	Include the logs for the User Vault for all users of the data source.

OFFLINE

OPTION	DESCRIPTION
Offline mode	Set the global data source support for Offline Mode. Useful when using a VPN connection that makes using local network impossible.
Expiration	Number of days that the local copy will be considered valid for the offline cache. You should go online prior to the end of that period to re-validate the data.

SECURITY

OPTION	DESCRIPTION
Lock application when minimized	Automatically lock the application when minimized in the taskbar for every user of the data source.
Lock on idle	Automatically lock the application when it is not used after a determined number of minutes.

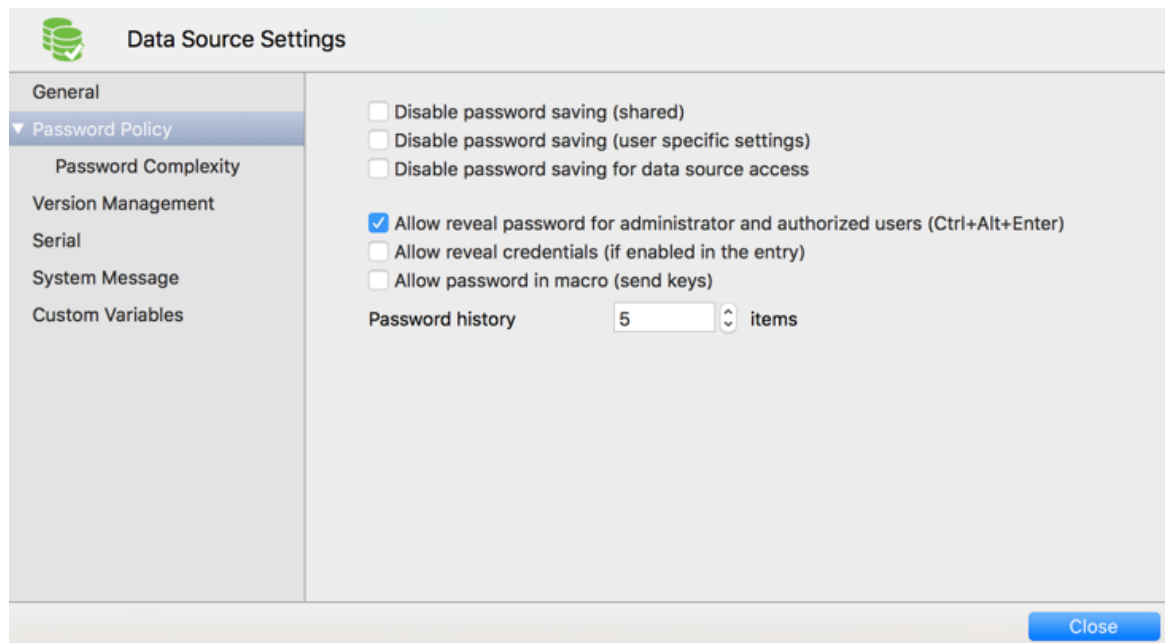
6.6.1.2 Password Policy

DESCRIPTION

Password Policy allows you to manage the different password policy and settings for your data source. For more information regarding the Password Complexity follow this [link](#).

Some of these settings could be overridden using Group Policies. For more information see [How to modify Group Policy Templates](#).

SETTINGS



Data Source Settings - Password Policy

OPTION	DESCRIPTION
Disable password saving (shared)	Users will not be able to save passwords within session.
Disable password saving (user specific settings)	Users will not be able to save password in the User Specific Settings.
Disable password saving for data source access	Users will not be able to save a new password to access the data source.
Allow reveal password for administrator and authorized users (Ctrl+Alt+Enter)	Controls if reveal password is enabled for authorized users.
Allow reveal credentials (if enabled in the entry)	Allow to show the credentials if the box "Allow show credentials (everybody)" is check inside the session.
Allow password in macro (send keys)	Renders \$MACRO_PASSWORD\$ variable useless for this data source.

OPTION	DESCRIPTION
Password history	Indicates the maximum saved password history count. See Password History for more information.

6.6.1.2.1 Password Complexity

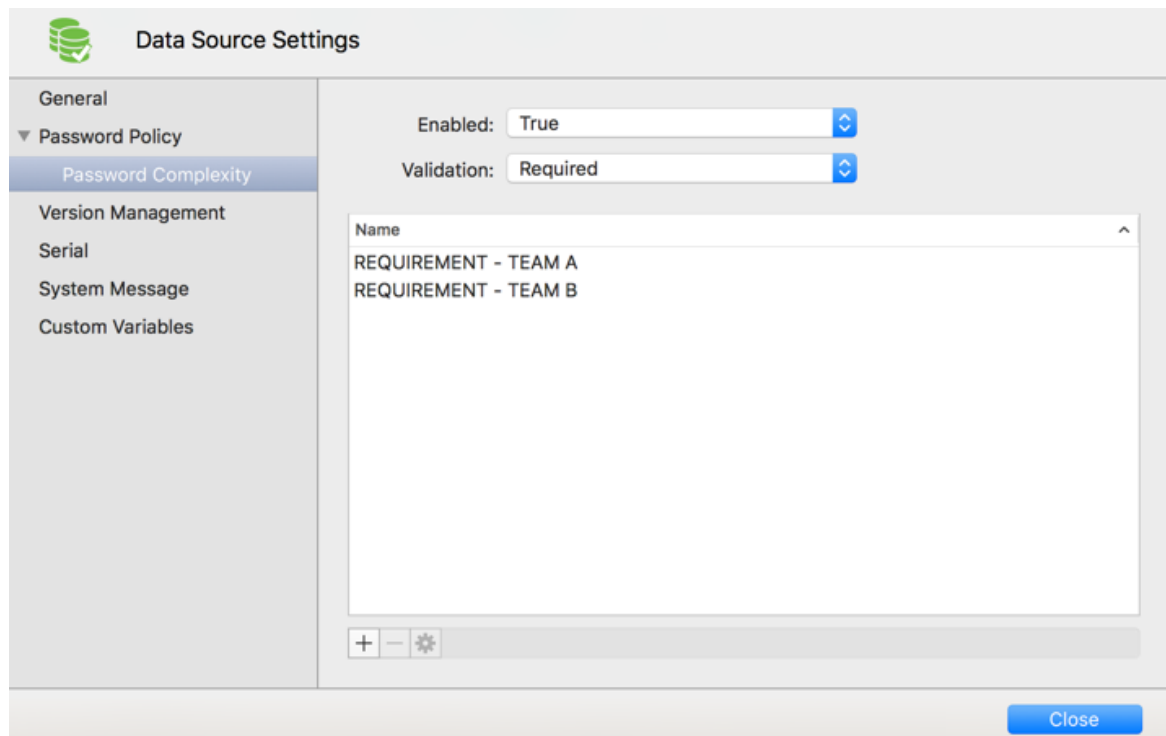
DESCRIPTION

This security setting determines whether passwords must meet predetermined complexity requirements that has been configured in your Data source settings. Complexity requirements are enforced when passwords are changed or a new entry is created. If this policy is enable then new passwords must meet some of the following minimum requirements:

- Minimum length
- Minimum lowercase characters
- Minimum uppercase characters
- Minimum numeric characters
- Minimum symbols

SETTINGS

The settings set in the Password Complexity Data source will determine what is the Default value of the Session settings.

*Data Source Settings - Password Complexity*

ENABLED

The Enable option set in the data source settings will determine the Default option of your Password Complexity session entry.

Option	Description
True	Enable the use of the Password Complexity requirements, doing so will force users of the data source to meet the password requirement set by the administrator of the data source.
False	Disable the Password Complexity requirements.
Inherited	Inherit the usage set in the parent folder. When using Inherited you will have to set a password to use as Inherited in the top folder of the entry.

VALIDATION

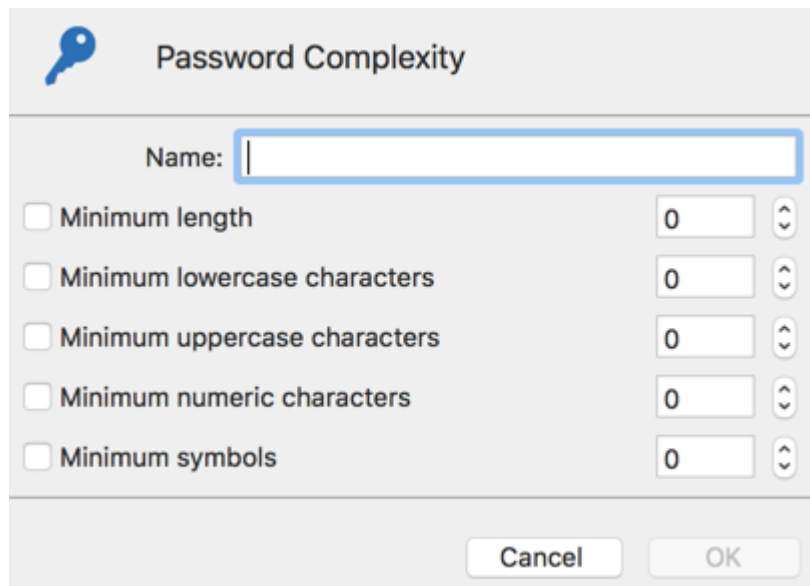
If the usage is enabled and you try to change or create a password for one of your entry, the reaction will depend on the chosen Validation mode.

The validation option determined in the data source settings will determine the Validation Default option of your Password Complexity session entry.

OPTION	DESCRIPTION
None	Will not use any kind of validation when changing or creating a new password.
Warn	Will warn you that your password does not comply with the Password Complexity requirements but will allow you to continue with that password or to edit it.
Required	The requirements of the Password Complexity are mandatory.
Inherited	Inherit the usage set in the validation folder. When using Inherited you will have to set a password to use as Inherited in the top folder of the session entry.

CREATE

You must create your own Password Complexity requirements template to then apply them to your sessions. Click on the plus button to create your Password Complexity template, enter a name and the desired requirements.



The image shows a 'Password Complexity' dialog box with a key icon in the top left. It features a 'Name:' label followed by a text input field. Below this are five rows of settings, each with an unchecked checkbox, a label, a numeric input field set to '0', and a spinner icon. The labels are: 'Minimum length', 'Minimum lowercase characters', 'Minimum uppercase characters', 'Minimum numeric characters', and 'Minimum symbols'. At the bottom right are 'Cancel' and 'OK' buttons.

Option	Value
<input type="checkbox"/> Minimum length	0
<input type="checkbox"/> Minimum lowercase characters	0
<input type="checkbox"/> Minimum uppercase characters	0
<input type="checkbox"/> Minimum numeric characters	0
<input type="checkbox"/> Minimum symbols	0


Data Source Settings - Password Complexity

6.6.1.3 Version Management

DESCRIPTION

You can manage your Remote Desktop Manager versions for Windows, Mac, Android or IOS.

VERSION MANAGEMENT


Data source settings

General
Password Policy
Version Management
Serial
System Message
Custom Variables

Mac

☐ Disable auto update notification

☐ Minimal version Current Ex: 1.0.0.0

☐ Maximal version Current

Download URL:

☒ Allow access from RDM (Mac)

☒ Allow access from PVM (Mac)

Windows

☐ Disable auto update notification

☐ Minimal version ex: 5.8.3

☐ Maximal version

Download URL:

☒ Allow access from RDM (Windows)

☒ Allow access from PVM (Windows)

Android

☒ Allow access from RDM (Android)

☒ Allow access from PVM (Android)

IOS

☒ Allow access from RDM IOS

☒ Allow access from PVM IOS

Close

Version Management tab

OPTION	DESCRIPTION
Disable auto update notification	Disable the auto update notification message. Use this when you want to manually update the application and not get notify when new versions are available..
Minimal version	Force users of the data source to use a minimal version. Enter the entire version number (7.9.10.0) to force a specific version or use partial number to force a subset version (7.9). Use this to disable connecting to the data source with an older version.

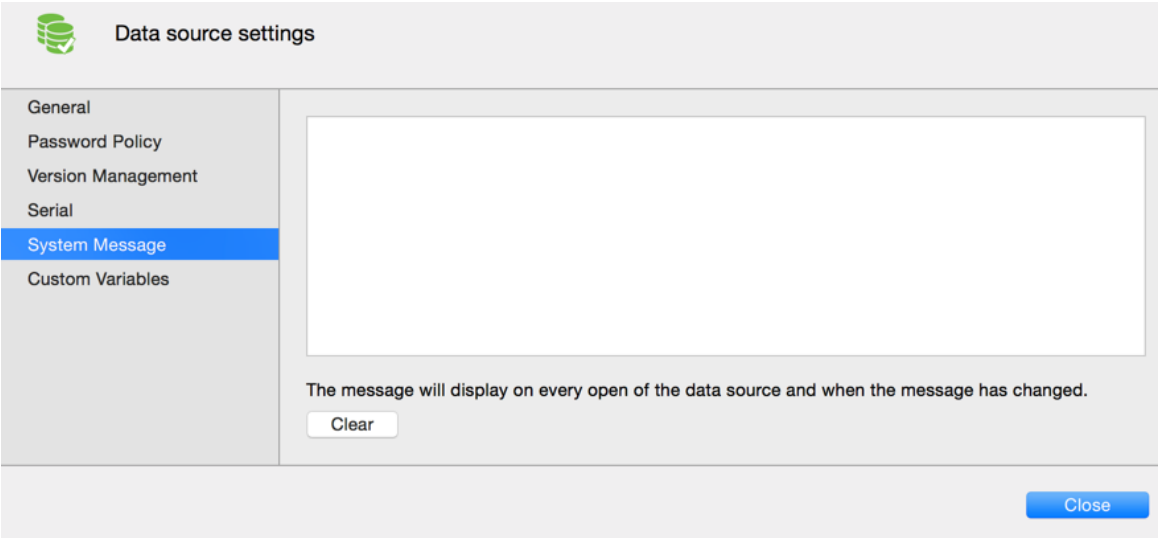
OPTION	DESCRIPTION
Maximal version	Force users of the data source to use a maximal version. Enter the entire version number (7.9.10.0) to force a specific version or use partial number to force a subset version (7.9). Use this to disable connecting to the data source with a newer version.
Download URL	Used 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.
Allow access from RDM	Disable option to exclude some client on different platform like Windows, Mac, IOS or Android.
Allow access from PVM	Disable option to deny access to your data source from Password Vault Management.

6.6.1.4 System Message

DESCRIPTION

Enter a system message for other users of the same data source to see when opening Remote Desktop Manager.

SYSTEM MESSAGE



Data source settings

General
Password Policy
Version Management
Serial
System Message
Custom Variables

The message will display on every open of the data source and when the message has changed.

Clear

Close

System Message tab

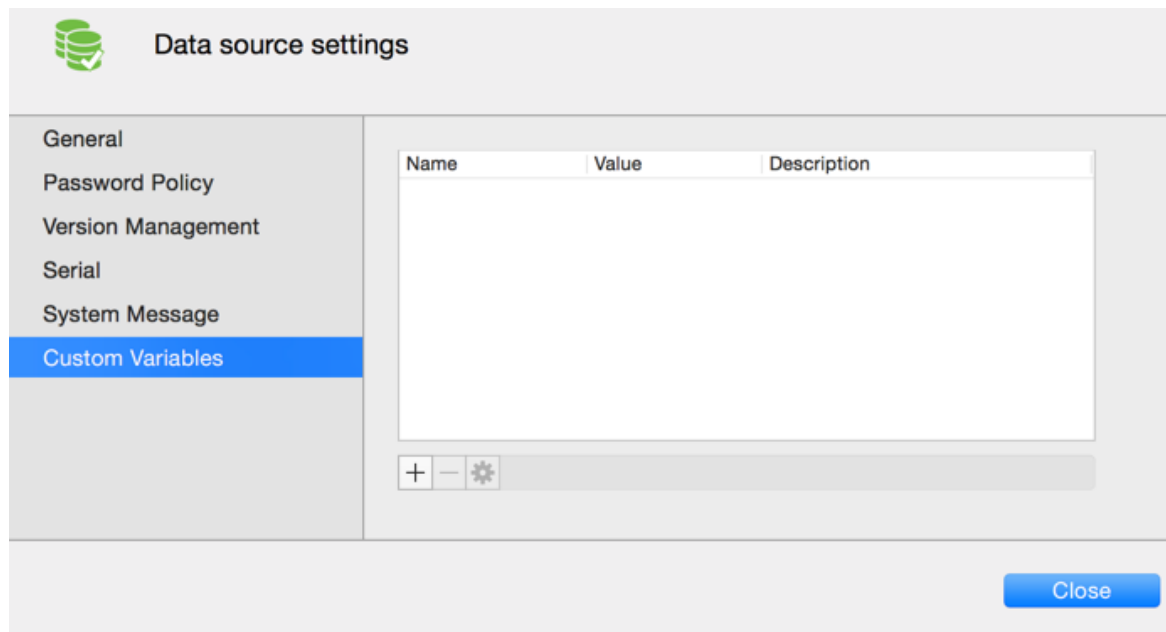
OPTION	DESCRIPTION
System message	The message will be displayed every time the data source is opened or when the message changes. Use Ctrl+ENTER to create a new line.
Clear	Delete the system message.

6.6.1.5 Custom Variables

DESCRIPTION

You can define your own custom variables to use in your data source configuration.

CUSTOM VARIABLES

*Custom Variables tab*

OPTION	DESCRIPTION
Custom Variables	Add a new custom variable to use in your data source configuration or with any templates.

6.6.2 Security Provider

DESCRIPTION

The security provider is available from **Administration - Security Provider**. The security provider is responsible for encrypting the data in the database.



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



Regardless of the security provider you've selected, the passwords that are stored in the data store are **ALWAYS** encrypted using AES 256 bit encryption.



By using a Security Provider, you ensure that nobody can read your entry configuration data, even when people have a direct access to your database(s) or a backup. You should always use this when you use a data source that is not local.

SETTINGS



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



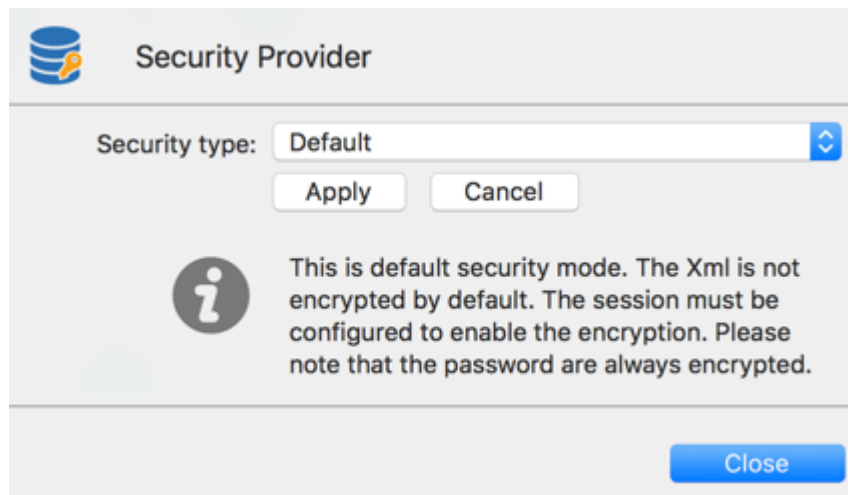
Applying a new security provider does process the whole database, therefore we advise you to create a backup prior to this operation.

1. Click on **Change security settings** to change the security provider.



Security Provider - Change security settings

2. Select your new security type from the drop down menu.



Security Provider - Security type

OPTION	DESCRIPTION
None	The session data will not be encrypted except for the passwords.
Basic	All of the data is encrypted with a key stored in Remote Desktop Manager and it's impossible for an external system to access it.
Default	This is the legacy security provider. The data is encrypted if the entry configuration is set accordingly in the advanced settings of the entries.
Shared passphrase	See below for more details.
Certificate	See below for more details.

SHARED PASSPHRASE

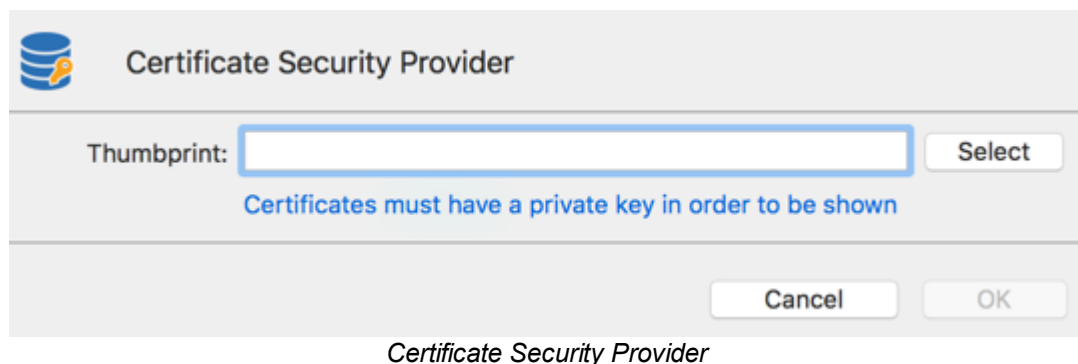


If the passphrase is lost, there is **nothing** that can be done to recover the data. Always copy it to a secure location when putting it in place.

All of the entries configuration data is encrypted with a mix of key stored in Remote Desktop Manager for Mac and the passphrase you've entered. The passphrase is required only when configuring the data source.

CERTIFICATE

If you have chosen Certificate as your Security Provider, it will encrypt the entry configuration data with a mix of key stored in Remote Desktop Manager and the private key contained in the certificate.



The image shows a dialog box titled "Certificate Security Provider" with a database icon. It contains a "Thumbprint:" label followed by a text input field and a "Select" button. Below the input field, a blue message states "Certificates must have a private key in order to be shown". At the bottom right, there are "Cancel" and "OK" buttons. The text "Certificate Security Provider" is centered below the dialog box.

OPTION	DESCRIPTION
Thumbprint	Select a certificate that already exist to use it for the encryption.

6.6.3 Licenses

DESCRIPTION

Managing Remote Desktop Manager registration globally for all your users can be done with a license serial stored in an advanced data source such as Devolutions Server, Microsoft SQL Server or Azure SQL.



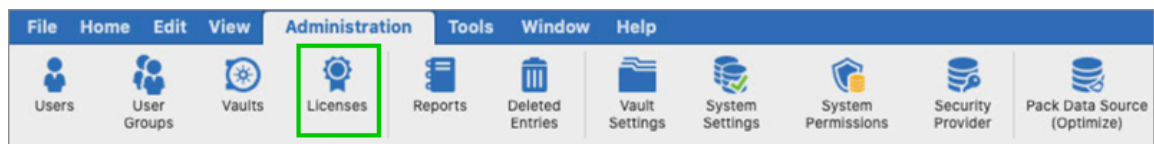
It is possible to request a trial to try Remote Desktop Manager for 30 days. If you decide not to register the application at the end of the 30 days period, your data will not be altered or erased, and you will have full access to it once you provide a valid license serial.



If you have more than one license, our [Sales team](#) can provide a co-terminated renewal to facilitate your license management.

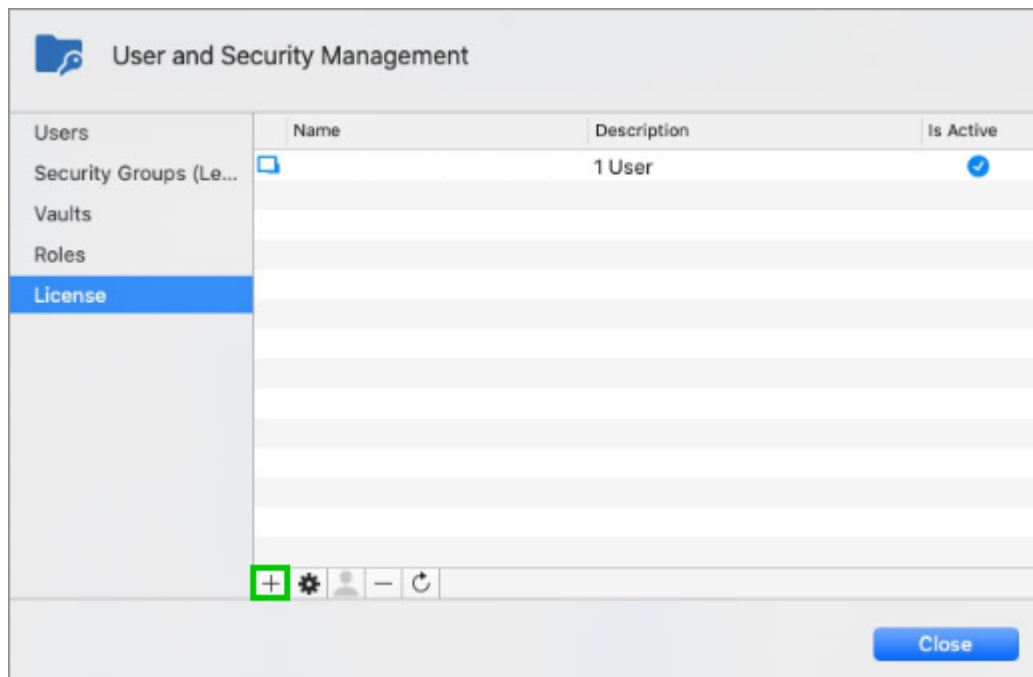
When the license is stored in an Advanced Data Source, there is no need to register Remote Desktop Manager as the license serial is retrieved directly from it. When launching the application for the first time, add the data source containing the serial.

1. To add a Remote Desktop Manager license serial, navigate to **Administration - Licenses**.



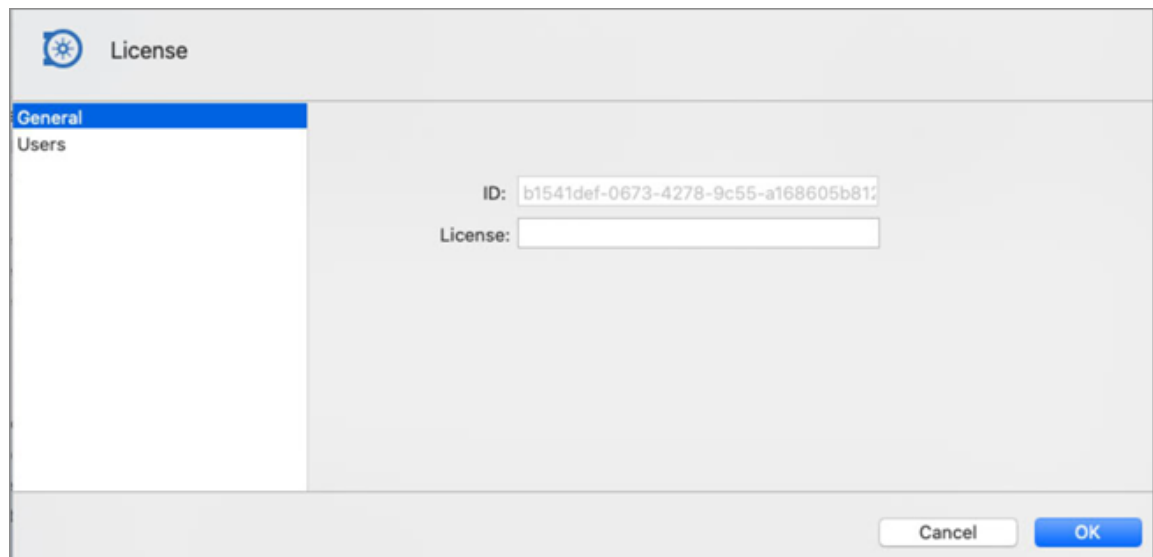
Administration - Licenses

2. In **License**, click on **Add License**.



User and Security Management - License

3. Enter the Remote Desktop Manager license serial and click on **Users**.



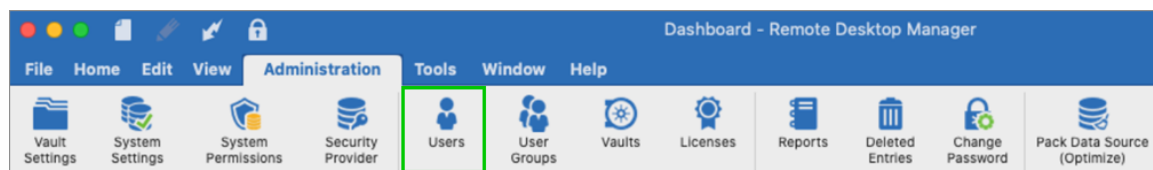
4. In the **Assigned** column, check next to each user you wish to grant a license or use the global action buttons. Click **OK** to save.

Your license is now saved in the advanced data source.

6.6.4 User Management

DESCRIPTION

The **User management** is available from the menu **Administration - Users**. Users management allows you to create, manage and assign rights to a user.



Administration - Users

Remote Desktop Manager for Mac allows for advanced user right management allowing you to control how a session is employed by each user. Note that some visibility control will depend on the active data source. There is currently no way to inherit security rights from a group as they must be assigned individually for each user. If using the [Devolutions Server](#) you will then be able to use Integrated Security with Active Directory.



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




In order to create users and assign rights, you must be administrator of not only Remote Desktop Manager for Mac, but also of the underlying database.

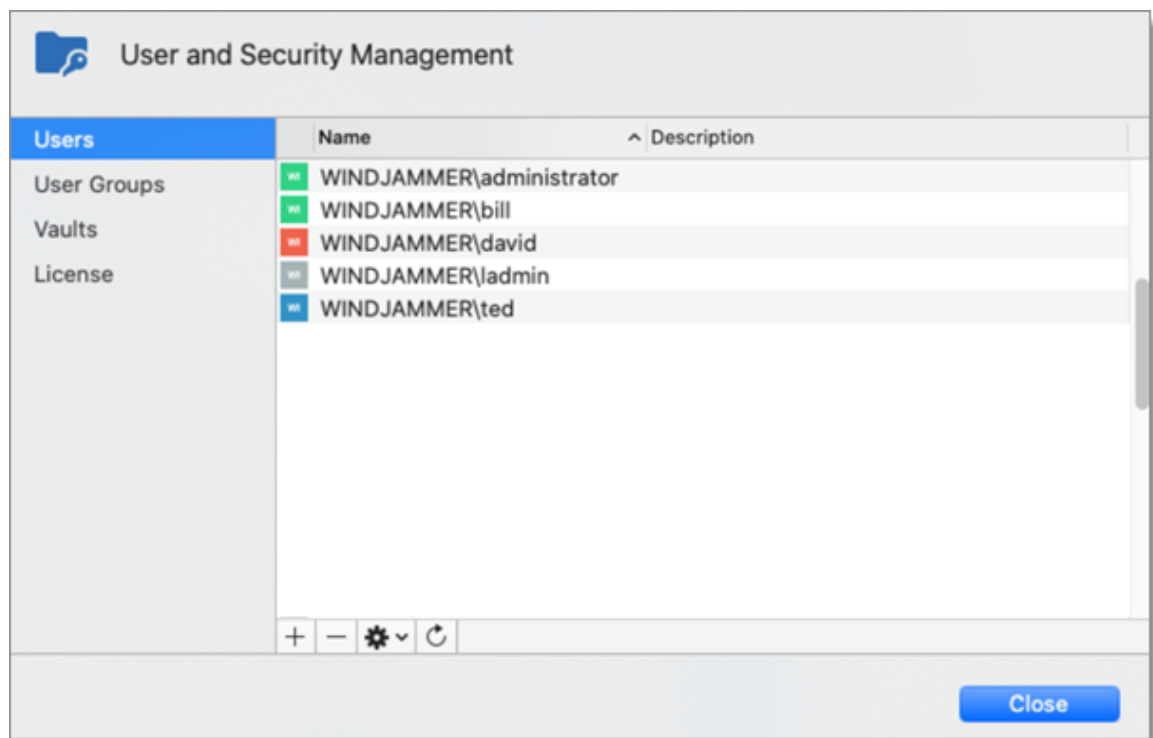


Not all [Advanced Data Sources](#) support the use of Integrated Security. To learn more please see [Integrated Security](#).

SETTINGS

CREATE USERS

To create a new user click on the . You can create a user using default security (specifying the password) or [Integrated Security](#). Consult the [Permissions](#) topic for more information on the rights that can be added to a user. You can assign different security options to the user such as allow the user to use the Offline mode.



User and Security Management



Not all [Advanced Data Sources](#) support the use of [Integrated Security](#). If using the [Devolutions Server](#) you will then be able to use Integrated Security with Active Directory. To learn more please see [Integrated Security](#).

USER MANAGEMENT SETTINGS

GENERAL

The screenshot shows the 'User Management' application window. On the left is a sidebar with a list of options: General, Information, User Groups, Privileges, Permissions, Vaults, Settings, and Application Access. The 'General' option is selected and highlighted in blue. The main content area is titled 'General' and contains the following fields and options:

- ID:** 1368020B-84ED-4385-8277-7F6C3393DDCC
- Authentication type:** Database (selected from a dropdown menu)
- Login:** (empty text field)
- ☐ Integrated security
- Email:** (empty text field)
- Password:** (empty text field)
- ☒ Create database login/user
- ☐ Administrator

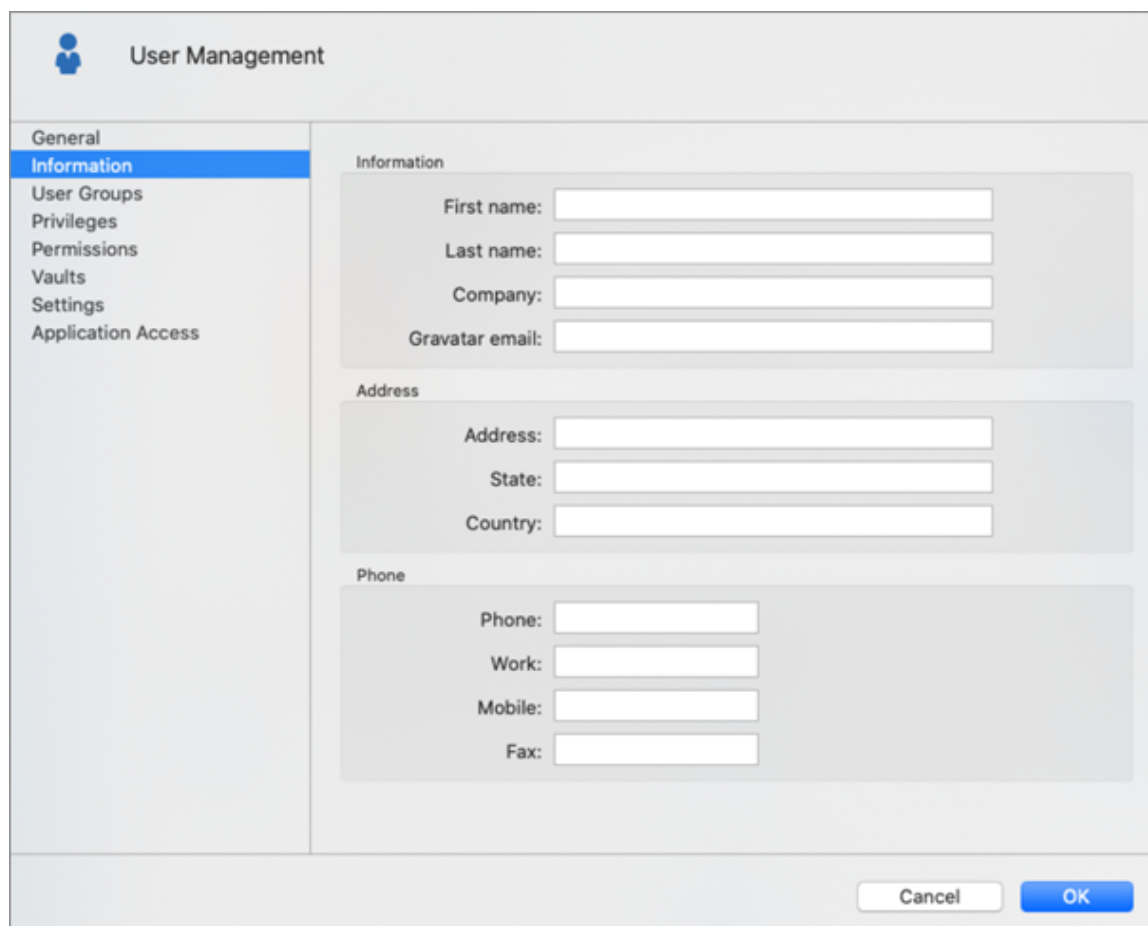
User Management - General

OPTION	DESCRIPTION
Authentication type	<p>Select your Authentication type between:</p> <ul style="list-style-type: none"> • Custom (Devolutions): If you wish to add an extra layer of security without using Integrated Security or without having to create new SQL login in your SQL Server the Custom Authentication type will be your best option. You will only need to create one SQL account within the SQL Server. • Database (SQL Server): Authenticate using the SQL login from your SQL Server.
Login	Login name for the user. When using Integrated Security you must select the user in the directory.
Integrated security	Specifies to use the Windows Integrated Authentication to authenticate to the data source. Applies only to SQL Server and Devolutions Server, depending on their configuration. When checked, an ellipsis button appears to allow you to browse for the user account in the directory. Consult Integrated Security topic for more information.
Email	Insert the user's email address.

OPTION	DESCRIPTION
Password	Enter the user Password. This field is disabled when using Integrated Security .
Administrator	Grants full administrative rights to the user. This is for the system as a whole.

INFORMATION

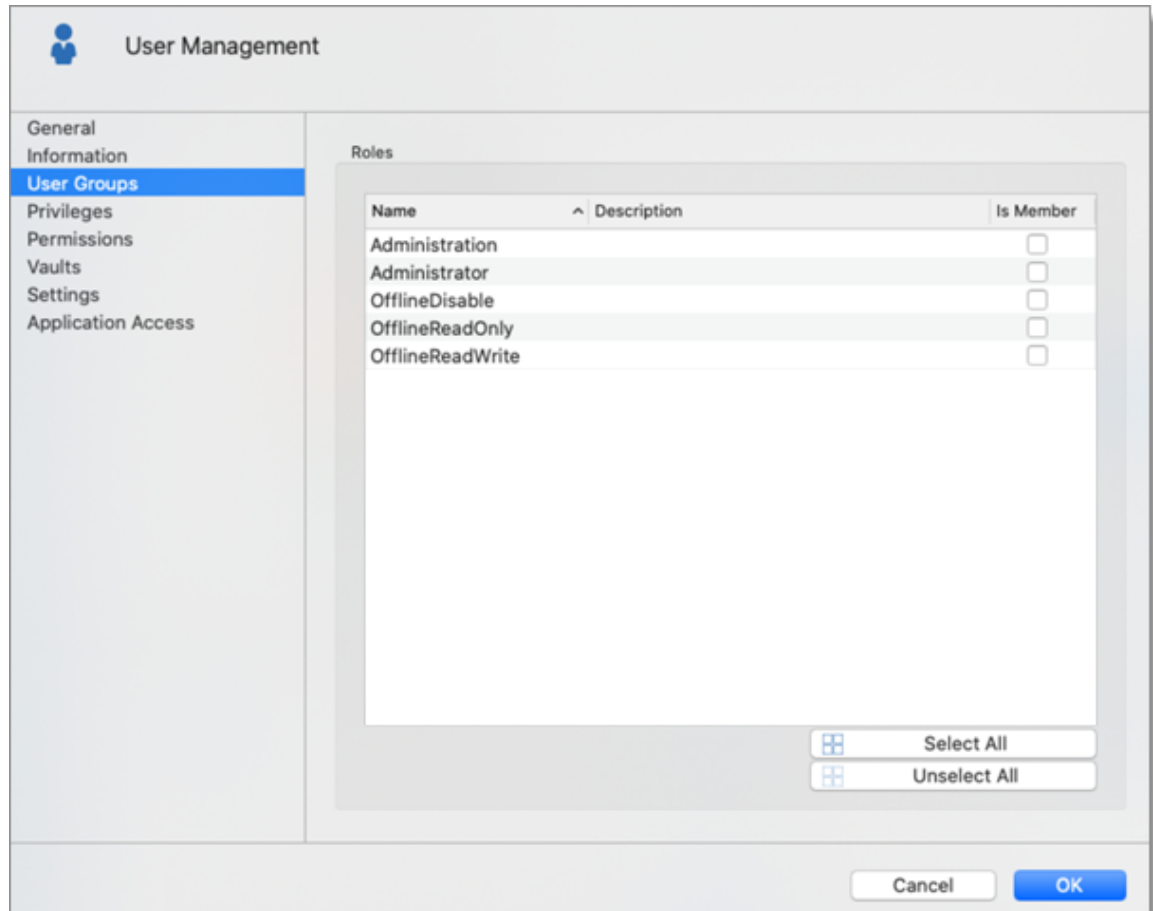
Enter all the information needed regarding your new user.



The image shows a software window titled "User Management" with a user icon. On the left is a sidebar menu with options: General, Information (highlighted), User Groups, Privileges, Permissions, Vaults, Settings, and Application Access. The main area is titled "Information" and contains three sections: "Information" with fields for First name, Last name, Company, and Gravatar email; "Address" with fields for Address, State, and Country; and "Phone" with fields for Phone, Work, Mobile, and Fax. At the bottom right are "Cancel" and "OK" buttons.

User Management - Information

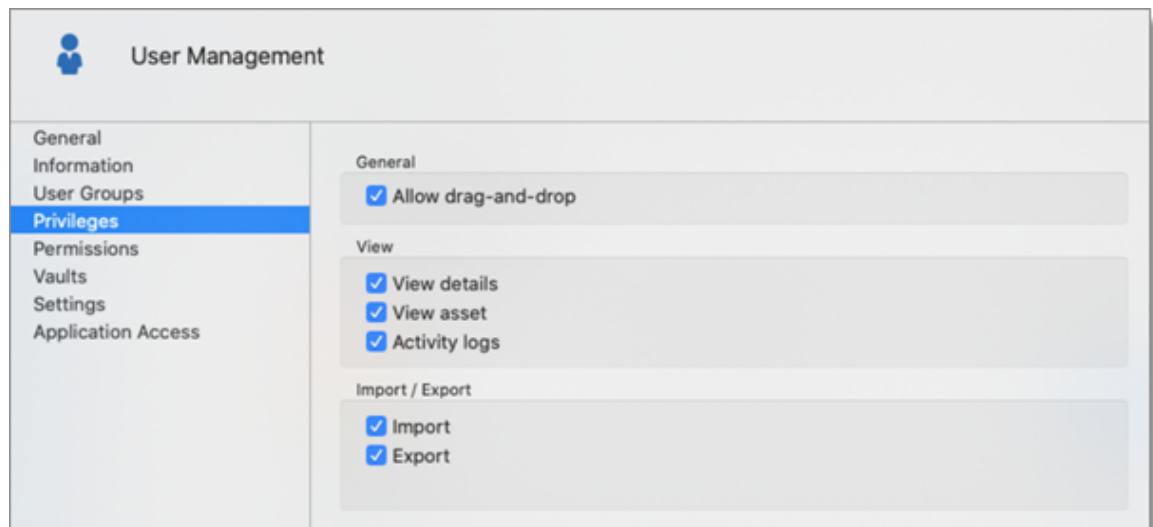
USER GROUPS



User Management - User Groups

OPTION	DESCRIPTION
User Groups	Consult User Groups Management topic for more information. When a user group needs to be added to a user, a description column will help you to select the proper user group.

PRIVILEGES



User Management - Privileges

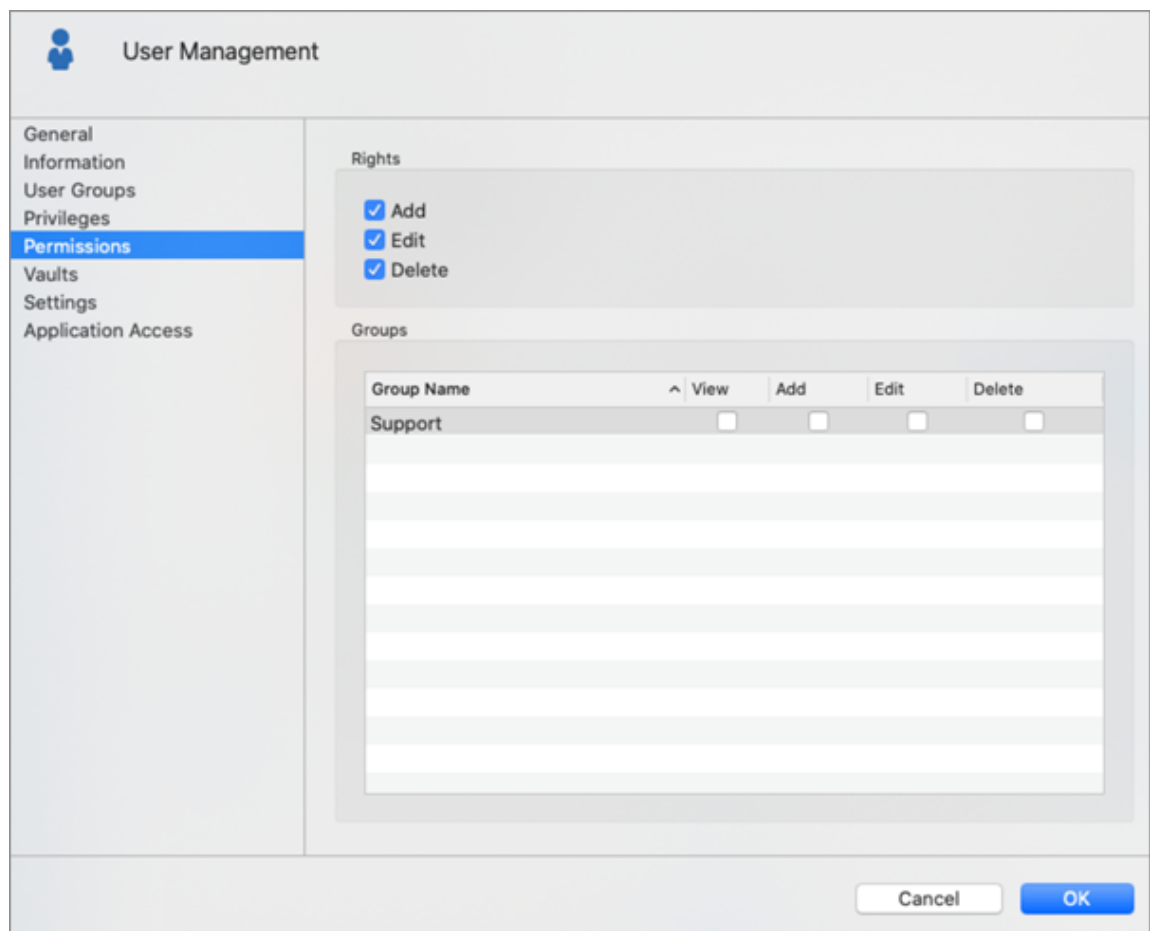
OPTION	DESCRIPTION
Allow reveal password	Allows the user to use the Reveal Password command.
Allow drag-and-drop	Allows the user to move the sessions using drag-and-drop from other applications.
View details	Allows the user to see the content of the Details tab for all sessions.
View information	Allows the user to see the content of the Information tab for all sessions.
View shared logs	Allows the user to see the content of the Logs that applies to a session.
Import	Allows the user to Import sessions (Clipboard - Paste as well). The import menu (File - Import) and the import feature in the context menu will be grayed out if the option is not active.
Export	Allows the user to Export sessions (Clipboard - Copy as well).

OPTION	DESCRIPTION
	The export menu (File - Export) and the export feature in the context menu will be grayed out if the option is not active.

PERMISSIONS

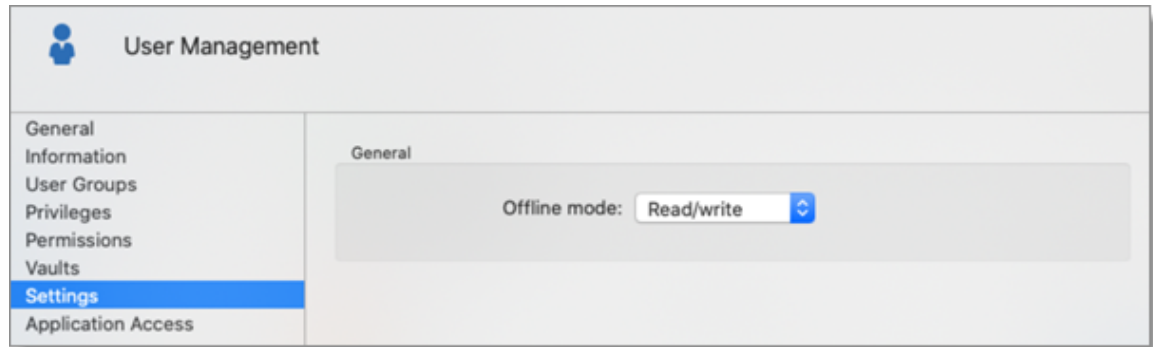
The **Permissions** section allows you to assign permissions. Controls are sometimes hidden depending on the data source or the state of other controls.

Consult the [Permissions](#) topic for more information on rights that can be added to a user.



User Management - Permissions

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. You can choose between:

OPTION	DESCRIPTION
Disabled	No offline cache allowed for that user.
Read-only	A read-only cache is allowed for Advanced Data Sources .
Read/Write	An advanced cache, with change synchronization, is allowed for Advanced Data Sources .

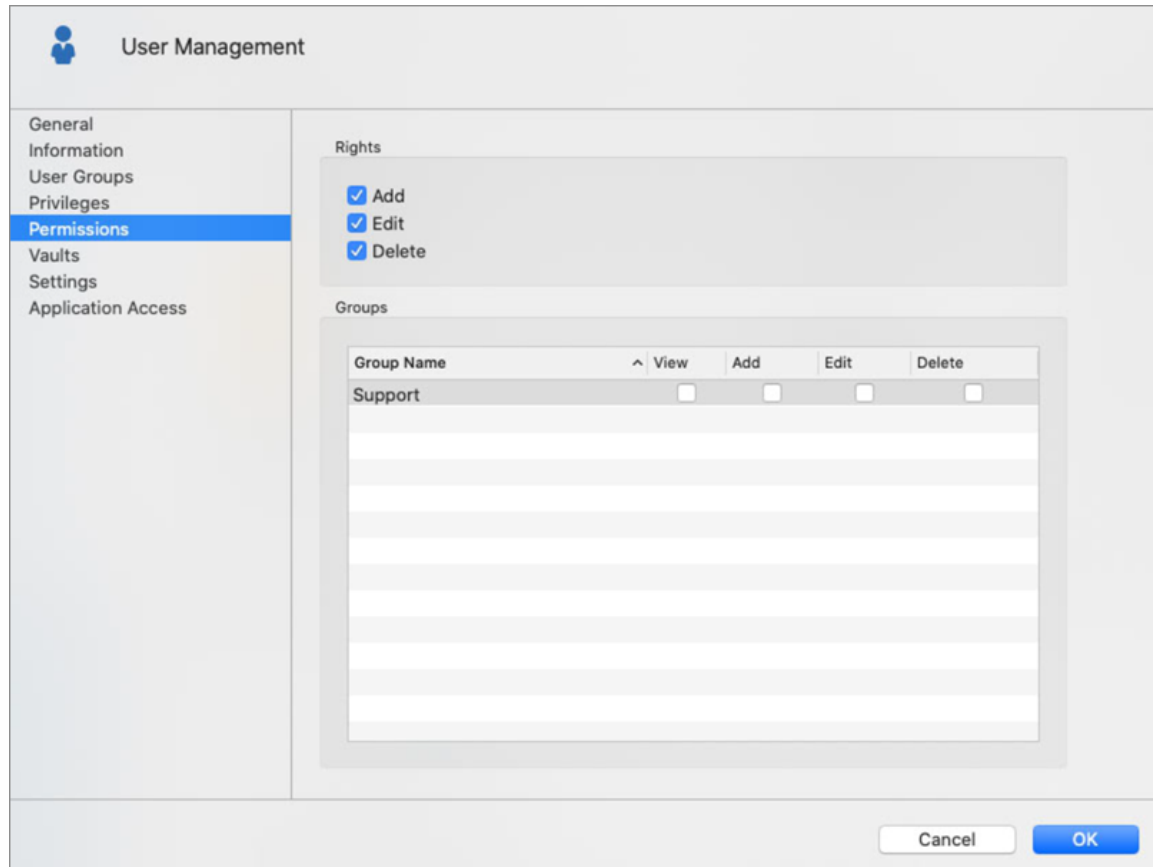
6.6.4.1 Permissions

DESCRIPTION

The **Permissions** section allows you to assign permissions. Controls are sometimes hidden depending on the data source or the state of other controls.

SETTINGS

PERMISSIONS



User Management - Permissions

The options directly above the grid are for **public** folders, meaning any folder that hasn't been assigned a security group will be assigned those rights. They also act as the most basic permission you can assign because they are needed in order to allow permissions for each of the security group listed below, when they are not checked the corresponding column of the grid is grayed out.

OPTION	DESCRIPTION
View	Allows the user to View AND USE the entries for that security group.
Add	Allows the user to add entries in group/folders for that security group. Will also grant the Add privilege for public groups. Also controls the visibility of the Add column in the Groups grid. The Add privilege need to be check if the user need to add sessions in the User Vault.

OPTION	DESCRIPTION
Edit	Allows the user to edit entries in groups/folders for that security group. Will also grant the Edit privilege for public groups. Also controls the visibility of the Edit column in the Groups grid. The Edit privilege need to be check if the user need to edit sessions in the User Vault.
Delete	Allows the user to delete entries in groups/folders for that security group. Will also grant the Delete privilege for public groups. Also controls the visibility of the Delete column in the Groups grid. The Delete privilege need to be check if the user need to delete sessions in the User Vault.



For higher security, its a best practice to set security groups on **all** the vault level folders. This ensures there are no public folders and that you have good control over the activity in your system.

All security groups are listed in the grid, and you can assign permissions using the corresponding columns.



Granting the **View** permission does allow the right to also launch/open the sessions of that group.

6.6.4.2 Integrated Security

DESCRIPTION

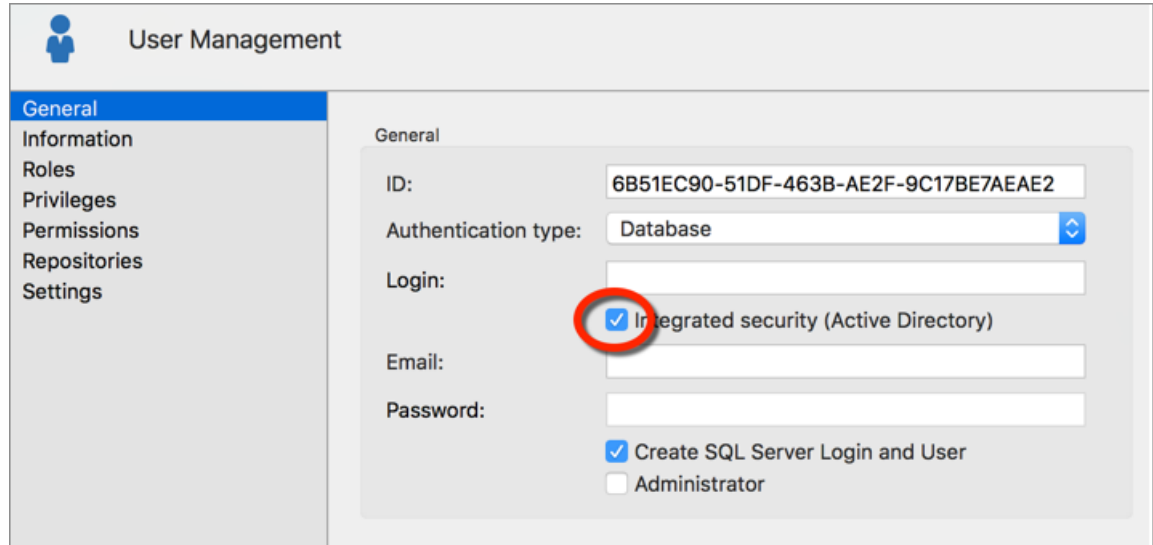
Integrated Security is the name Microsoft gives to the technology that uses the credentials of your current running session and passes them automatically to the remote resources for authentication.



This feature requires a Devolutions Server data source.

SETTINGS

In the **User Management** window when activating the **Integrated Security** checkbox, the password field will be disabled because the operating system will provide a cached copy automatically.



The screenshot shows the 'User Management' window with the 'General' tab selected. The 'Authentication type' is set to 'Database'. The 'Login' field is empty. The 'Integrated security (Active Directory)' checkbox is checked and circled in red. The 'Email' and 'Password' fields are also empty. At the bottom, there are two checkboxes: 'Create SQL Server Login and User' (checked) and 'Administrator' (unchecked).

User Management - Integrated Security

When using Integrated Security, you're currently running windows session must be from a user of that domain.

6.6.5 Security Group Management

DESCRIPTION

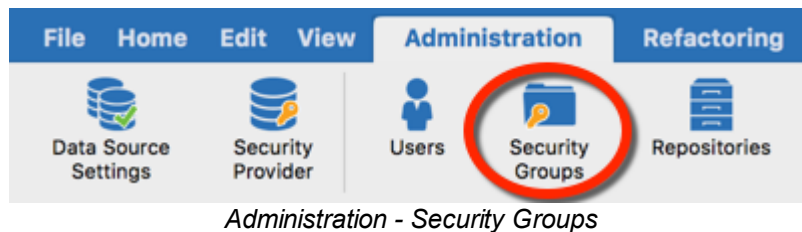
The Security Group Management is available from the menu **Administration - Security Groups**.

Security groups are used to protect sessions from a subset of system users. Assign sessions to security groups then control who has access and how much control they have on each security group.

Security groups are used to classify sessions and restrict access to certain users. There is no direct relationship between Active Directory and Security Groups. By default, every session is created without an assigned security group, and therefore is visible to all connected users.

Each entry in the navigation pane can be assigned to a single security group. Best practices dictates that you assign security groups to groups/folders that way all the entries they contain will inherit the same security group.

Security groups are used to protect sessions from a subset of system users. Assign sessions to security groups then control who has access and how much control they have on each security group.



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



All sessions without security groups are considered public, meaning anyone with access to the Data Source will be able to see all your entries.

SETTINGS

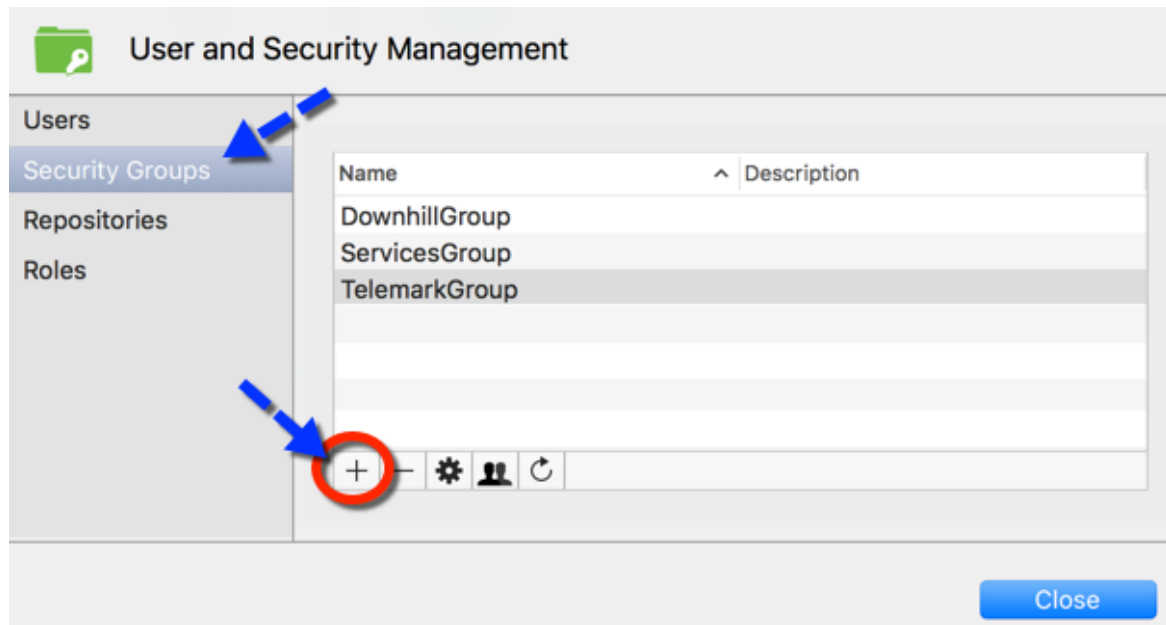
CREATE A SECURITY GROUP

Security groups are created from the menu **Administration - Security Group**.

Remote Desktop Manager's security groups are container for sessions, not for users. Folders are closely tied with Security Groups, so there's an overlap in usage. The key points are:

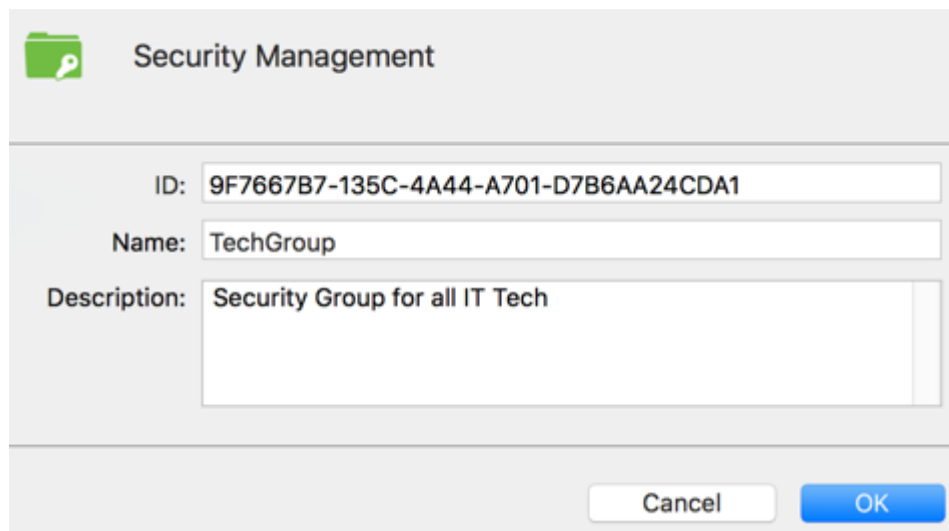
- **Security is inherited:** child items and folders are covered by a parent folder's security group.
- **Security is additive:** a security group added to a sub folder does not override the parent, it adds to it.
- **A folder has a single Security Group:** use Shortcuts to work around that limitation.

1. Click on the plus to create a new Security Group.



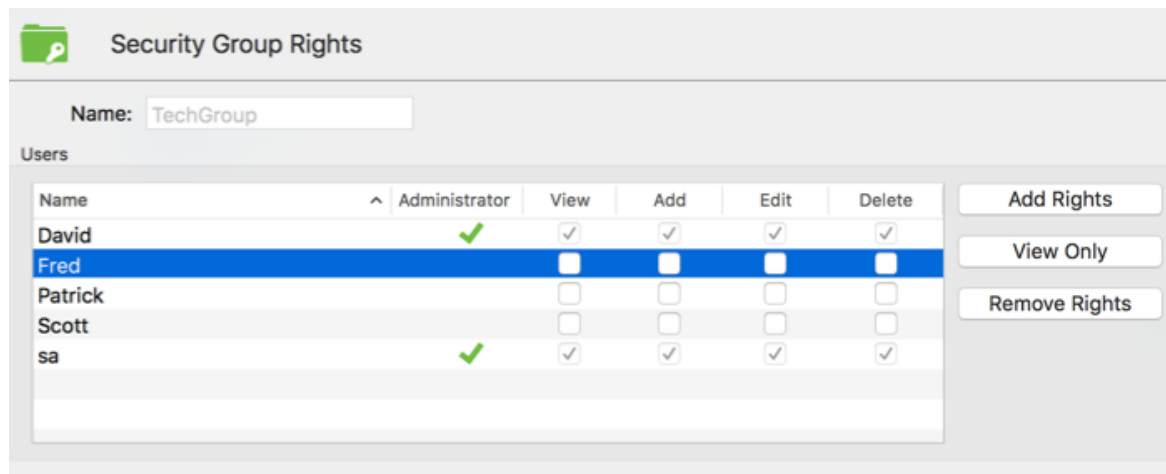
Security Groups - Add

2. A Security Group Management dialog will appear. Enter a name and a short description of your new Security Group.



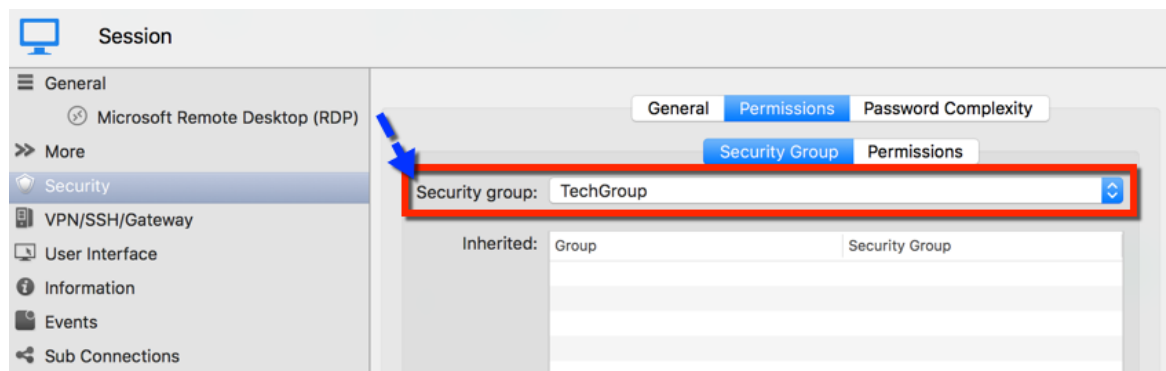
Security Management dialog

3. Assign the appropriate [permissions](#) for each user for your newly created Security Group.



Security Group Rights

4. Security groups can then be assigned to entries using the property window. Each entry can only have one security group assigned. For easy maintenance we recommend assigning security groups to groups/folders which will result in the child entries to inherit the security group.

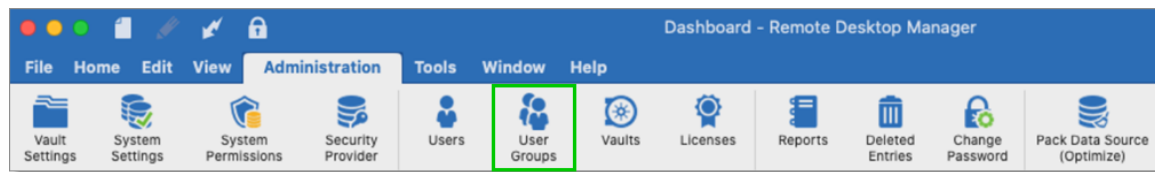


Session Security Group

6.6.6 User Groups Management

DESCRIPTION

User Groups in Remote Desktop Manager for Mac are mainly used to reduce the time taken to manage users. 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.



Administration - User Groups

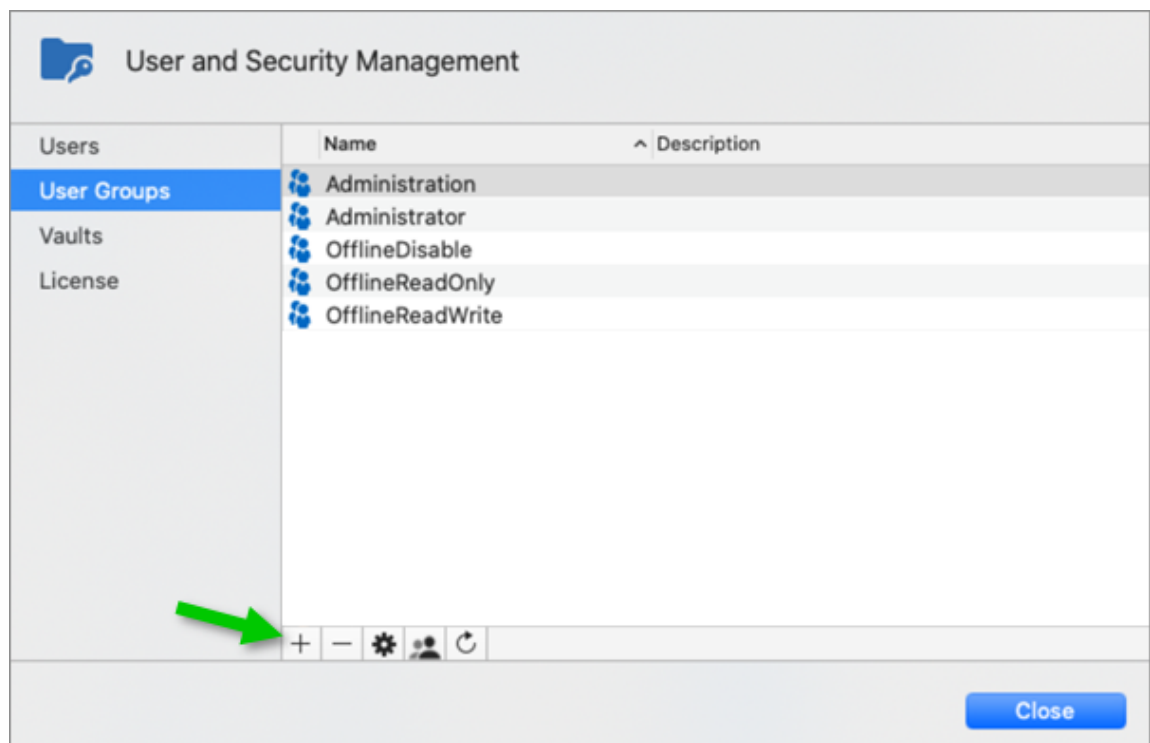


This feature is only available with an [SQL Server](#) and a [Devolutions Server](#) data source.

USER GROUPS IN REMOTE DESKTOP MANAGER FOR MAC

User groups in Remote Desktop Manager for Mac are simply permission sets that you assign to a user. You can assign multiple user groups to each user and the end result is the union of all permissions.

1. Create a new user groups in **Administration - User Groups** and click on the **plus** to create a new one.

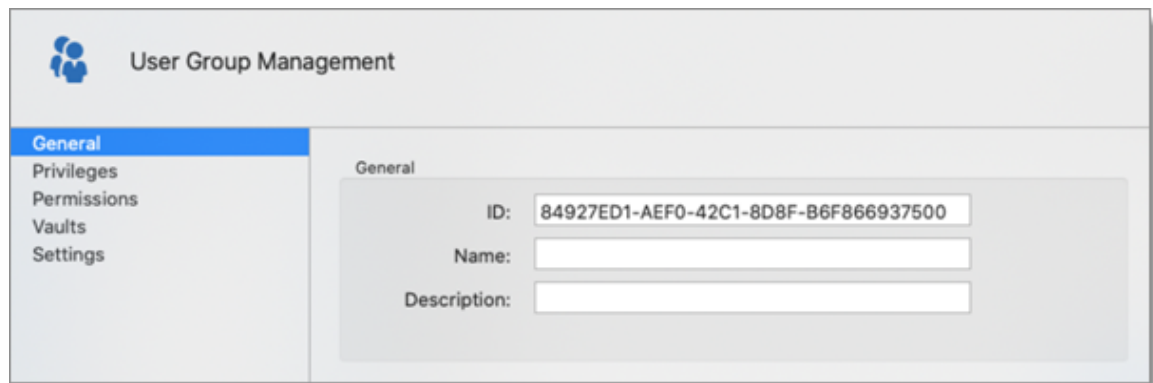


Add User Group

USER GROUPS MANAGEMENT

GENERAL

The **General** side menu is used to define general information about the new user group.



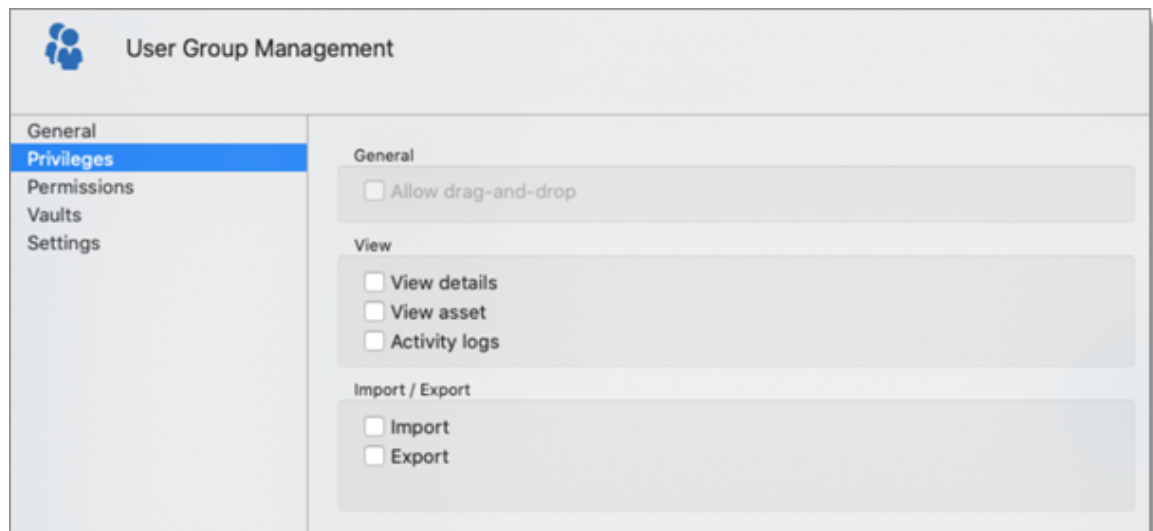
The screenshot shows the 'User Group Management' interface. On the left is a sidebar menu with 'General' selected. The main area is titled 'General' and contains three input fields: 'ID' with a pre-filled UUID, 'Name', and 'Description'.

User Group Management - General

OPTION	DESCRIPTION
Login	The Login name is the name displayed in your User Groups list.
Description	Enter a short description of your new User group.

PRIVILEGES

The **Privileges** side menu lets you add particular privileges to the user groups. These privileges need to be enabled for certain features to be available to users like the rights to import or export sessions.



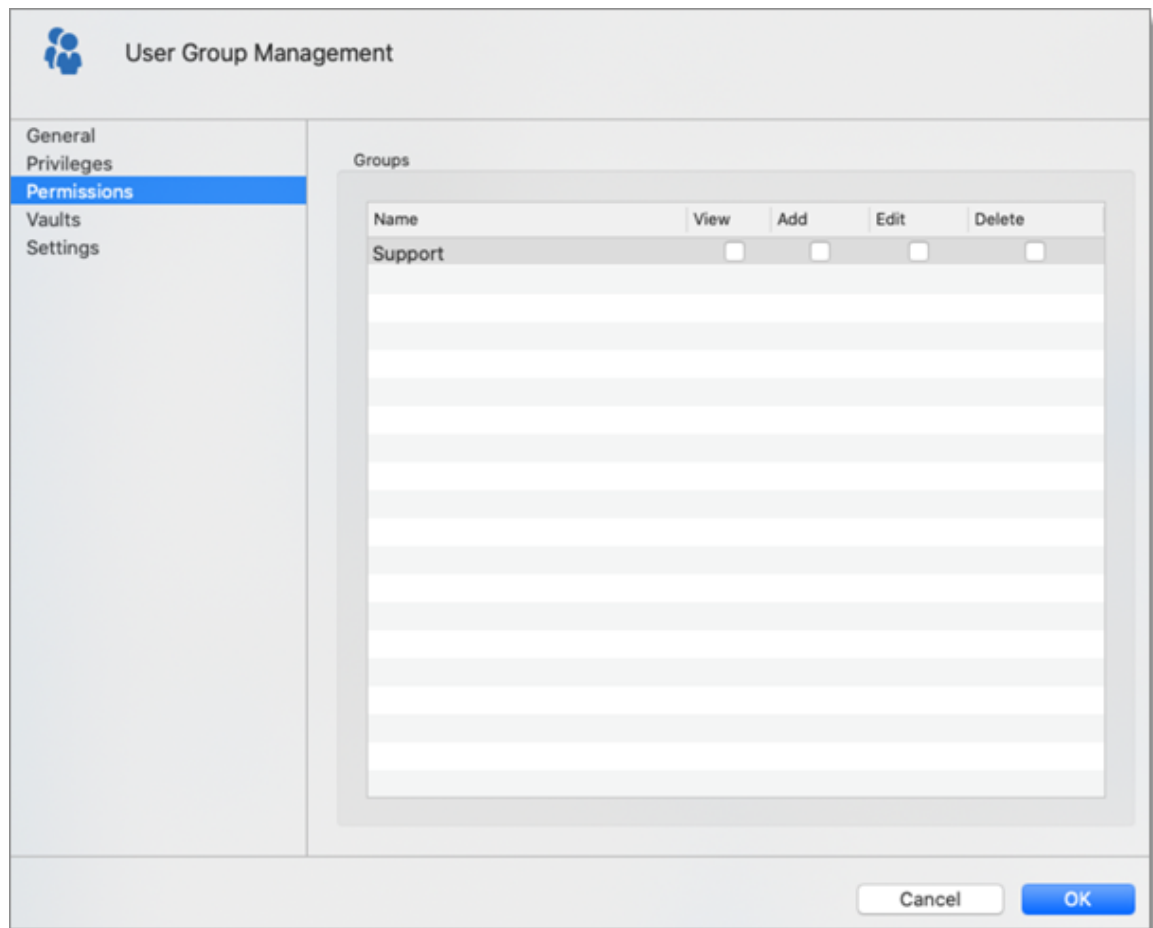
User Group Management - Privileges

OPTION	DESCRIPTION
Allow reveal password	Allows the user to use the Reveal Password command.
Allow drag-and-drop	Allows the user to move the sessions using drag-and-drop from other applications.
View details	Allows the user to see the content of the Details tab for all sessions.
View information	Allows the user to see the content of the Information tab for all sessions.
View shared logs	Allows the user to see the content of the Logs that applies to a session.
Import	Allows the user to Import sessions (Clipboard - Paste as well). The import menu (File - Import) and the import feature in the context menu will be grayed out if the option is not active.
Export	Allows the user to Export sessions (Clipboard - Copy as well).

OPTION	DESCRIPTION
	The export menu (File - Export) and the export feature in the context menu will be grayed out if the option is not active.

PERMISSIONS

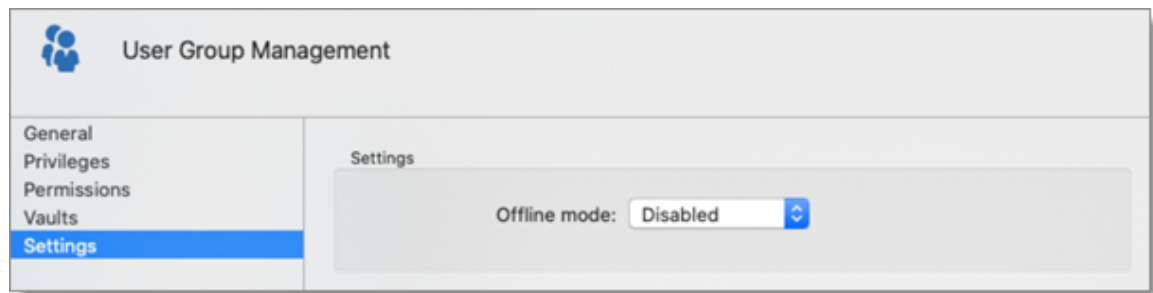
Use the **Permissions** side menu to assign the View, Add, Edit and Delete permissions to your User groups. For more information please see the [Permissions](#) topic.



User Group Management - Permissions

SETTINGS

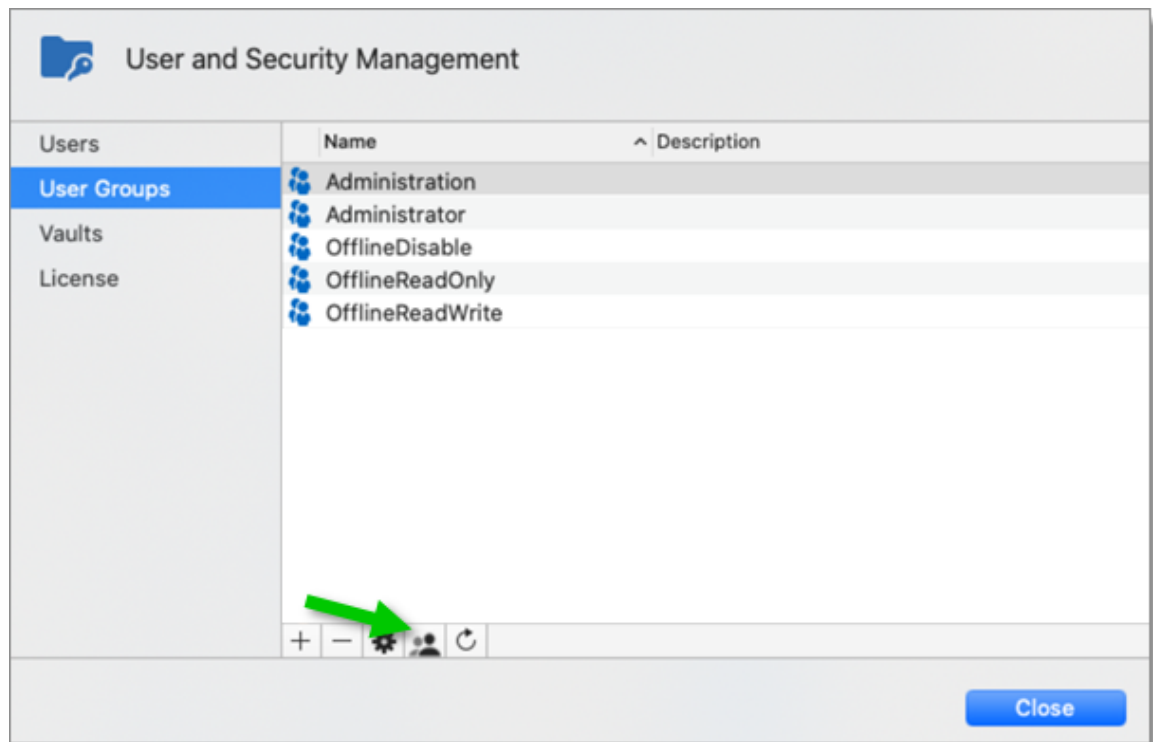
The **Settings** side menu lets you define the Offline mode rights for your User Groups.

*User Group Management - Settings*

OPTION	DESCRIPTION
Disabled	No offline cache allowed for that user group.
Read-only	A read-only cache is allowed for Advanced Data Sources .
Read/Write	An advanced cache, with change synchronization, is allowed for Advanced Data Sources .

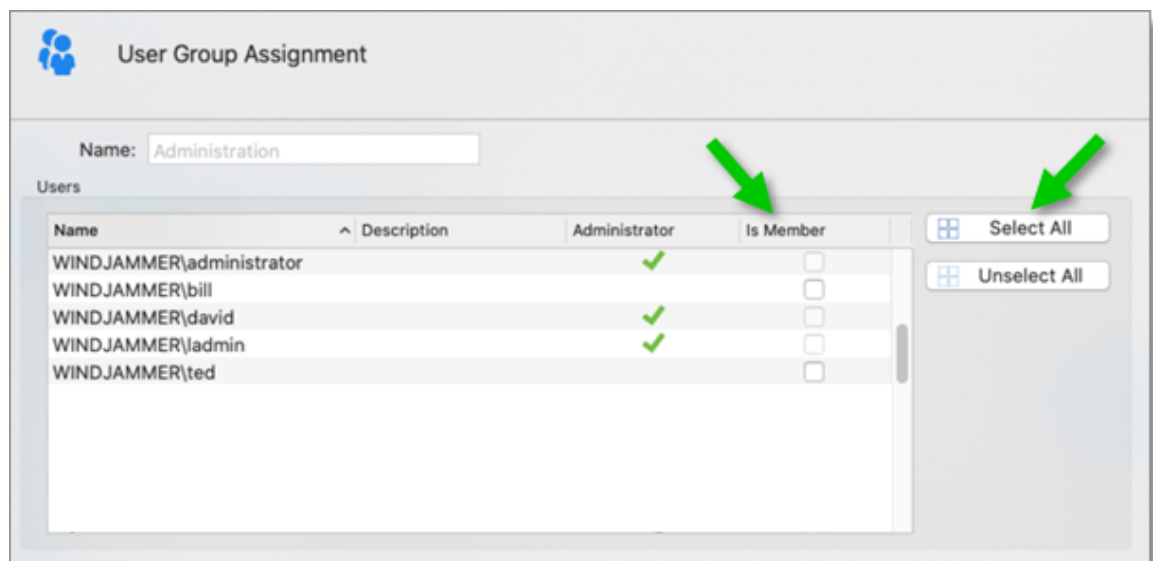
ASSIGN A USER GROUPS

To assign user group to a user or to manage user groups for a user go in **Administration - User groups** and click on **Assign user groups**.



User and Security Management - User Groups

It's possible to assign a user group to multiple users at the same time. Select the users you wish to apply the selected user group or you can simply click **Select All** or **Unselect All**.



User Group Assignment

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.



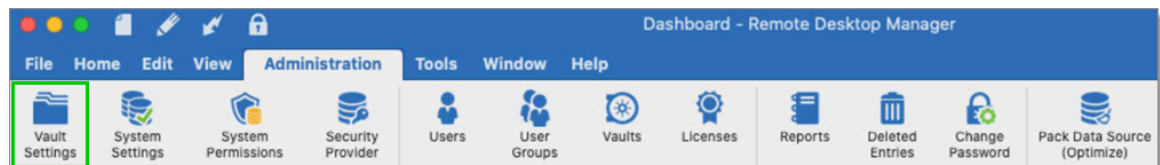
Please note that the Unsecured group permissions (the ones above the grid) are ignored. You must set them on each user individually.

For more information please see [Devolutions Server User Groups Management](#).

6.6.7 Vault Settings

DESCRIPTION

The **Vault Settings** serve as an extra layer of security that can be added to your Vault folder.

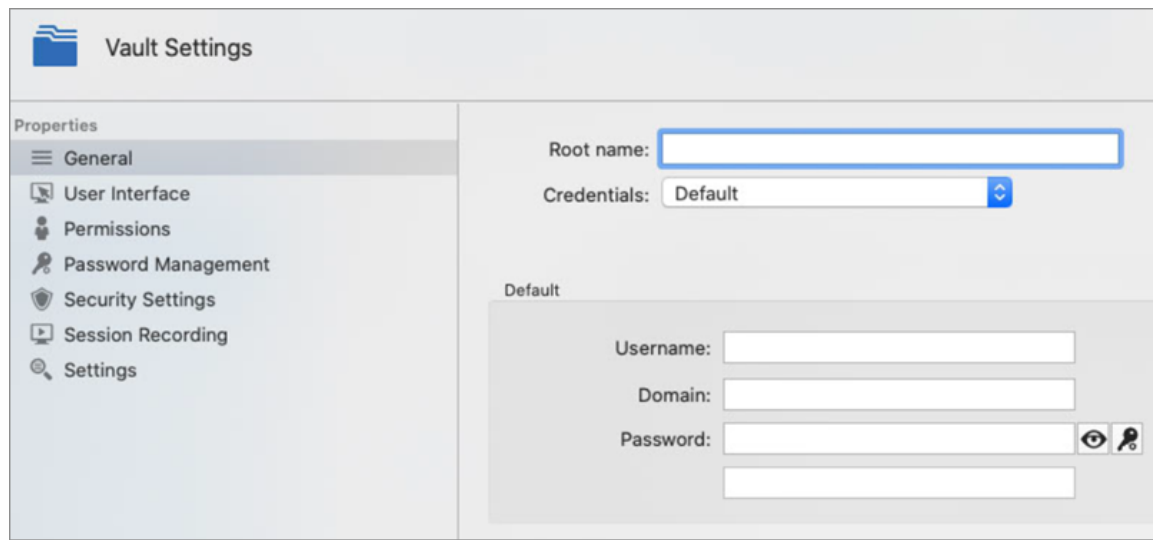


Administration - Vault Settings

SETTINGS

Vault Settings allows you to set a permission on your top-level folder (the vault folder), giving you the option of having all of your folders inherit the permissions set on the vault folder, saving you time by not having to define permissions on each top layer folder.

Click on **Administration - Vault Settings**. At the moment the only option you will be able to change is to override the credentials for all your entries. You can select to override your credentials with existing credentials or define a new one.



Vault Settings - General

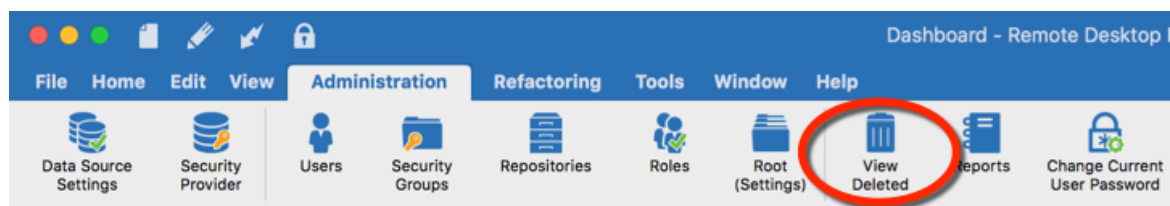


This feature is presently under construction as we are working hard on adding the Permissions feature which will allow you to make more changes directly from the Vault. We will update the information as soon as it is available.

6.6.8 View Deleted

DESCRIPTION

The **Administration - View deleted** option allows you to view the deleted entries as well as restoring them.



Administration - View Deleted



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



Administrators can permanently delete some or all deleted entries.



Deleted entries can be restored as long as they haven been permanently deleted and as long as the Security Provider has not been changed since the deleted action.

SETTINGS

MANAGE DELETED ENTRIES

The **View deleted** will generate a list containing all the entries previously deleted from your data source. You may resurrect an entry, meaning it will become an active entry again and will be shown in your data source. You may also chose to permanently delete your entries, once you have permanently deleted your entries you won't be able to resurrect them afterward.

Deleted entries

Name: Action: ☐ Shared template
 Connection type: Group:
 Username: Created on:
 Data source user: Modified on:

Action	Session Type	Name	Group	Shared Template	Created On	Modified On
Delete	Credential	OpenVPN	SQL	<input checked="" type="checkbox"/>		
Delete	Group	IPC Mississauga	IPC Mississa...	<input type="checkbox"/>		
Delete	Group	Global Passwords	IPC Mississa...	<input type="checkbox"/>		
Delete	Group	Switches	IPC Mississa...	<input type="checkbox"/>		
Delete	Group	Documents	IPC Mississa...	<input type="checkbox"/>		
Delete	Group	Network	IPC Mississa...	<input type="checkbox"/>		
Delete	Group	Routers	IPC Mississa...	<input type="checkbox"/>		
Delete	Group	User	[Firma] - [Do...	<input type="checkbox"/>		
Delete	Group	Windows Server - RDP	[Firma] - [Do...	<input type="checkbox"/>		
Delete	Group	Windows VMs - RDP	[Firma] - [Do...	<input type="checkbox"/>		
Delete	Group	Administrator	[Firma] - [Do...	<input type="checkbox"/>		
Delete	Group	User	[Firma] - [Do...	<input type="checkbox"/>		

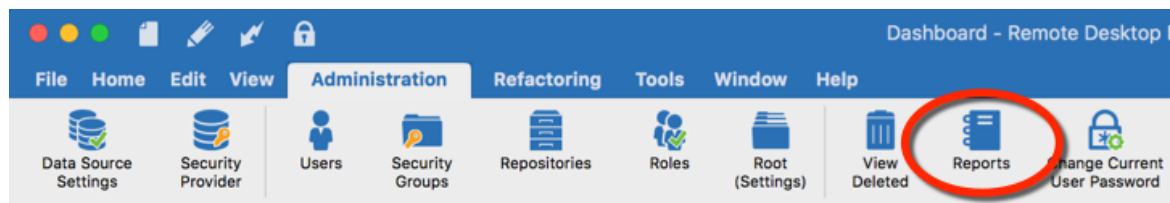
View Deleted

OPTION	DESCRIPTION
Resurrect Entry	Restore an entry in your database.
Delete	Permanently delete the selected deleted entry.
Delete All	Permanently delete all deleted entries.

6.6.9 Reports

DESCRIPTION

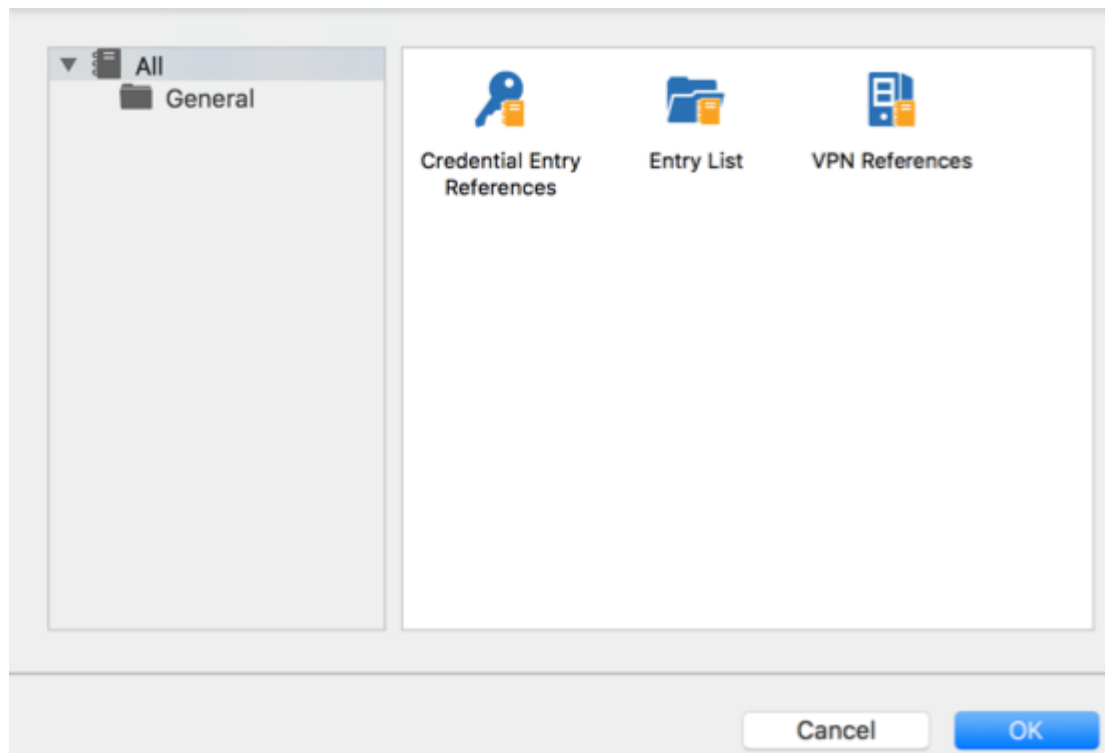
The **Reports** section automatically generate reports regarding your credentials, entries, logs and security. You will also have the option to export your generated report which is a way to execute and export reports through a command line.



Administration - Reports

They are 3 different types of reports:

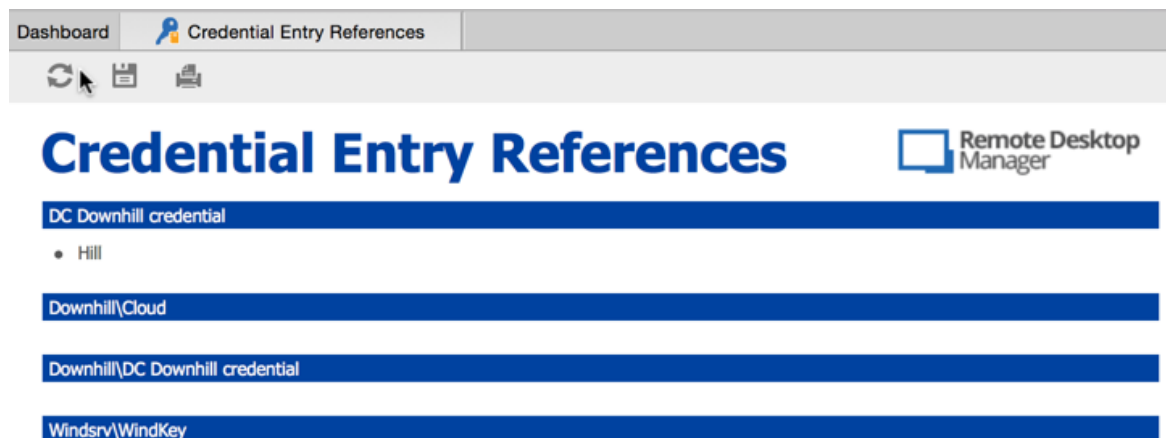
- [Credential Entry References](#)
- [Entry List](#)
- [VPN References](#)

*Administration - Reports*

6.6.9.1 Credential Entry References Report

DESCRIPTION

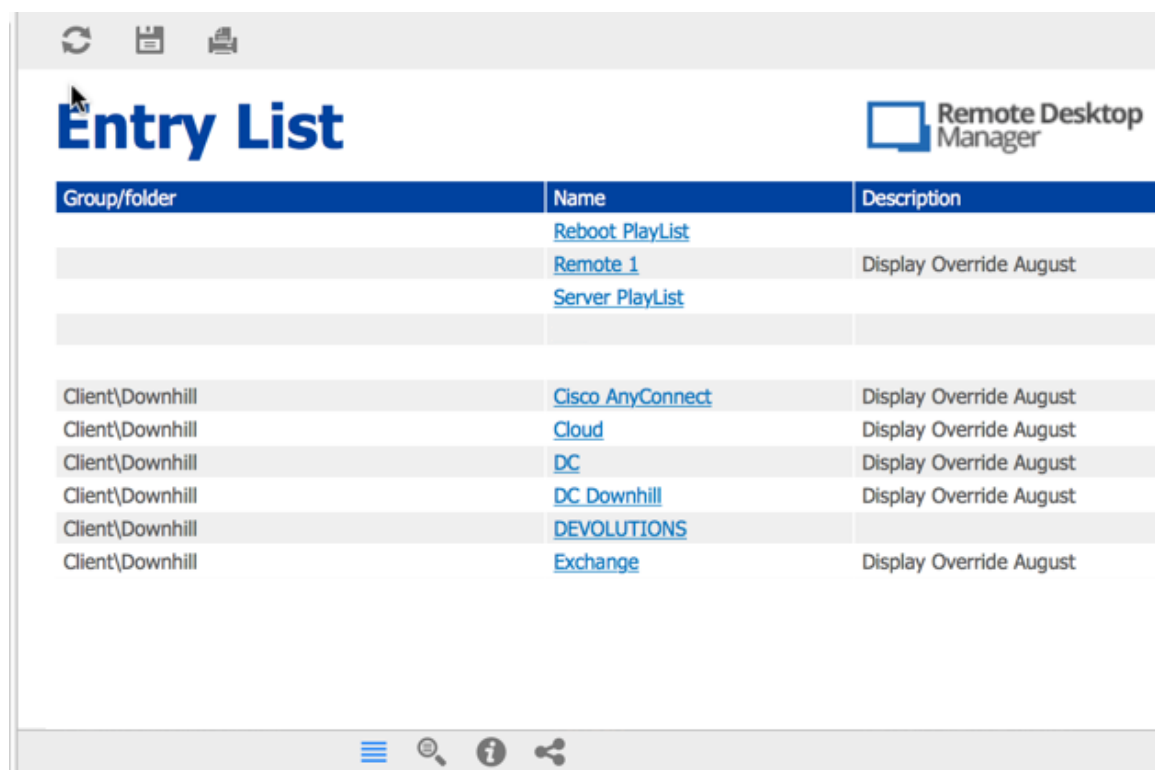
Generate a report to show in which Group/Folder credentials entries are used.

*Credential Entry References Report*

6.6.9.2 Entry List Report

DESCRIPTION

Generate a report to show a simplified list of all your entries; the Name column contains hyperlinks to the entry.



Group/folder	Name	Description
	Reboot PlayList	
	Remote 1	Display Override August
	Server PlayList	
Client\Downhill	Cisco AnyConnect	Display Override August
Client\Downhill	Cloud	Display Override August
Client\Downhill	DC	Display Override August
Client\Downhill	DC Downhill	Display Override August
Client\Downhill	DEVOLUTIONS	
Client\Downhill	Exchange	Display Override August

Entry List Report

6.6.9.3 VPN References Report

DESCRIPTION

Generate a report showing all VPN entries and the sessions using them in the VPN tab.

This report also displays SSH, VPN, Web or Command Line session type that are Linked to an existing session.

VPN References



Consult me first\Devolutions - VPN

- Test platforms\Domain joined\Windjammer Domain\Client-1

Consult me first\Devolutions - VPN

- Test platforms\Domain joined\Windjammer Domain\Client-1

Roadshow\VMServer (Proxy)

- Roadshow\\$_COMPUTER_HOST\$
- Roadshow\Client-1

Test platforms\No Domain\VDEVOSRV-TST

- Infrastructure\acomba

Test platforms\Services\RDP through SSH\dc.windjammer (through ssh tunnel)

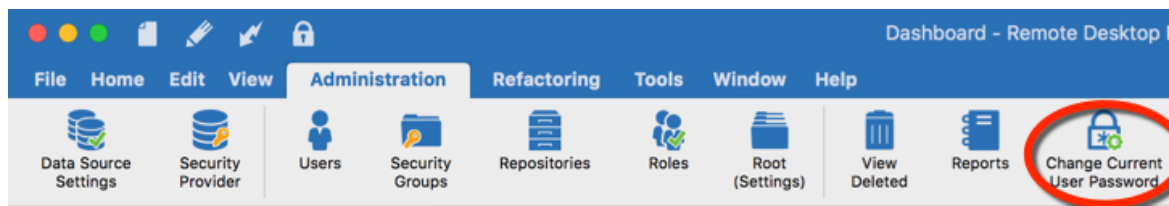
- Test platforms\Services\RDP through SSH\dc.windjammer (through ssh tunnel)

VPN Reference Report

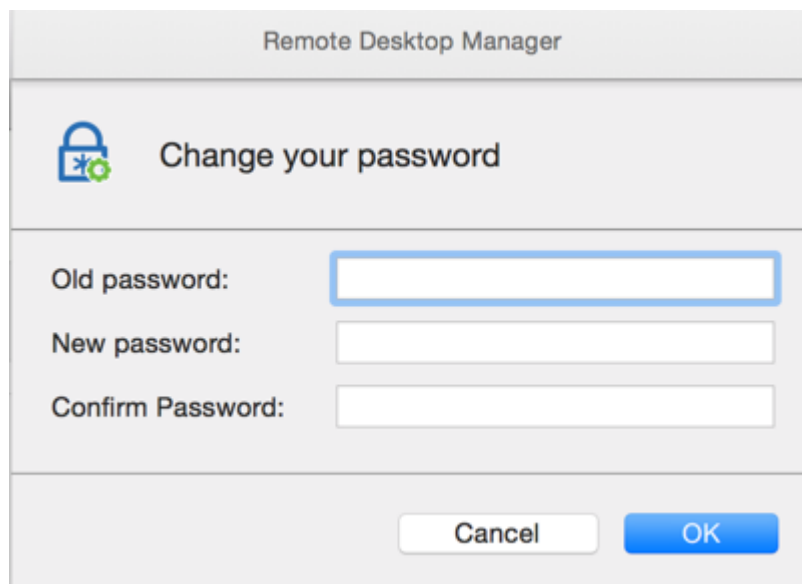
6.6.10 Change Current User Password

DESCRIPTION

You may change the password of the current user of the data source in **Administration - Change Current User Password**.



Administration - Change Current User Password



Change your password

6.7 Tools

DESCRIPTION

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



To learn more please see:

- [Password Generator](#)
- [Entry Security Analyzer](#)

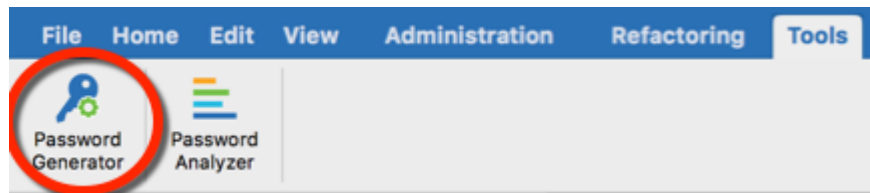
6.7.1 Password Generator

DESCRIPTION

The **Password Generator** enables you to create random passwords that are secured 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 more rapidly your passwords. After you have selected your mode and settings, you can create your template.

Password Generator is available in **Tools - Password Generator**.



Tools - Password Generator

SETTINGS

USE SPECIFIED SETTINGS

Choose all the character types you desire and generate a password.

Password generator

Template: Default template Add Delete

Mode: Use specified settings

Password length: 8

☒ Upper-case (A, B, C, ...) 0 ☐ 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

Also include the following characters: 0

Exclude the following characters:

lvPOHmET
UEygnEuO
0boVZCC7
63QmZi8b
FE7rdL28
NpMyRQ7B
vq5gVU84

Strong

NOVEMBER | papa | MIKE | yankee | ROMEO | QUEBEC | seven | BRAVO

Forbidden Password Close

Password generator - Use specified settings

READABLE PASSWORD

Each generated password will be readable, but will not be a word in the dictionary.

Password generator

Template: Default template Add Delete

Mode: Readable password

Syllables: 1

Numeric: 1

Symbols: 1

lem3#
Ca8~
Gi@3
Gi%0
wah6~
Pu1?
Go6*

Generate
Copy to Clipboard


Strong

lima | echo | mike | three | pound

Forbidden Password Close

Password generator - Readable password

USE A PATTERN

Press the  button and select any pattern you need to create your passwords. A list of the most recent used pattern will also be create.

The screenshot shows a web application titled "Password generator". It has a "Template" dropdown set to "Default template" with "Add" and "Delete" buttons. The "Mode" dropdown is set to "Use a pattern". The "Pattern" input field contains "Pa\$\$w0rd\$" and has a help icon. A checkbox for "Shuffle characters" is checked. Below the pattern field is a list of generated passwords: d\$w\$\$P7r0, \$rwP\$\$08u, \$0wP\$nr\$3, wP\$1l0r\$\$, w\$0r\$6\$P, w\$\$Pc04\$r, and 22\$0r\$Pw\$. To the right of this list are "Generate" and "Copy to Clipboard" buttons. Below the list is a green bar indicating "Very Strong" strength. At the bottom of the list is a sample password: delta | dollar | whiskey | dollar | dollar | PAPA | seven | romeo | zero. At the very bottom of the interface are "Forbidden Password" and "Close" buttons.

Password generator - User a pattern

The following are the supported patterns:


KEY	DESCRIPTION	SAMPLE
a	Lower-Case Alphanumeric	abcdefghijklmnopqrstuvwxyz 0123456789
A	Mixed-Case Alphanumeric	ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789
b	Bracket	()[]{}<>
c	Lower-Case Consonant	bcdghjklmnpqrstvwxyz
C	Mixed-Case Consonant	BCDFGHJKLMNPQRSTVWXYZ bcdghjklmnpqrstvwxyz
d	Digit	123456789

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

KEY	DESCRIPTION	SAMPLE
\	Escape (Fixed Char)	Use following character as is
{n}	Escape (Repeat)	Repeats the previous character n times
[x]	Custom character	Define a custom character sequence

PRONOUNCEABLE PASSWORD

The application will generate a password that is pronounceable.

 Password generator

Template: Default template ⌵ Add Delete
 Mode: Pronounceable password ⌵

Password length: 8 ⌵
 Case mode: Mixed case ⌵
☒ Digits
☐ More pronounceable
 Also include the following characters

Nit2FaVu4
 GogSher4
 Ux2DiYef5
 Rhic5Phogh0
 OZif9Sop6
 GhopynChoj2
 ThiHavTuv2

Generate
Copy to Clipboard

Strong

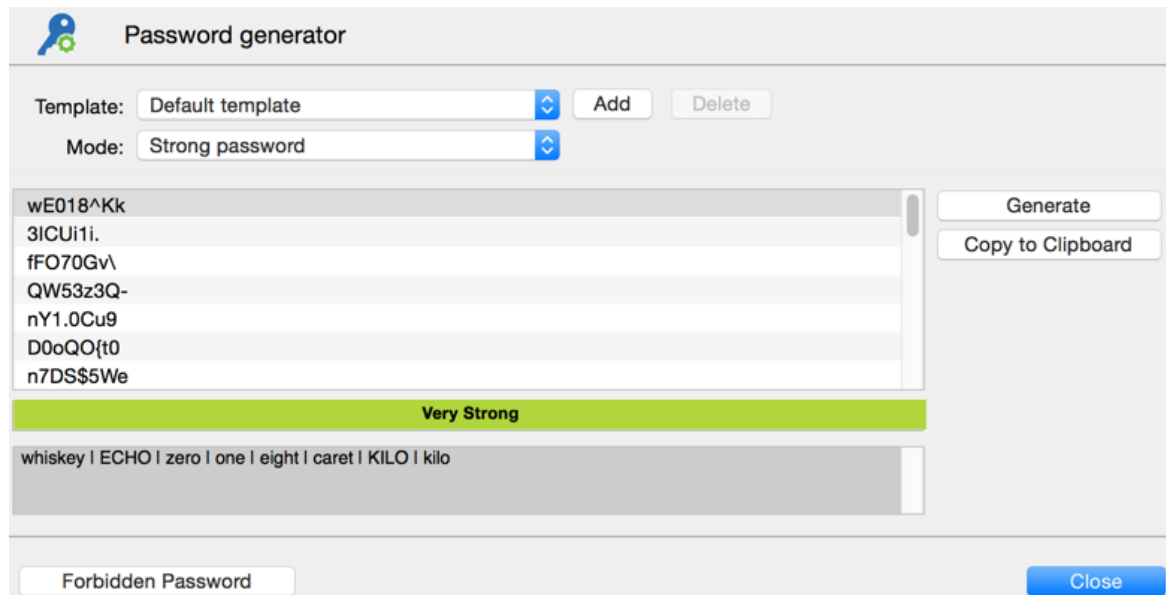
NOVEMBER | india | tango | two | FOXTROT | alpha | VICTOR | uniform | four

Forbidden Password Close

Password generator - Pronounceable password

STRONG PASSWORD

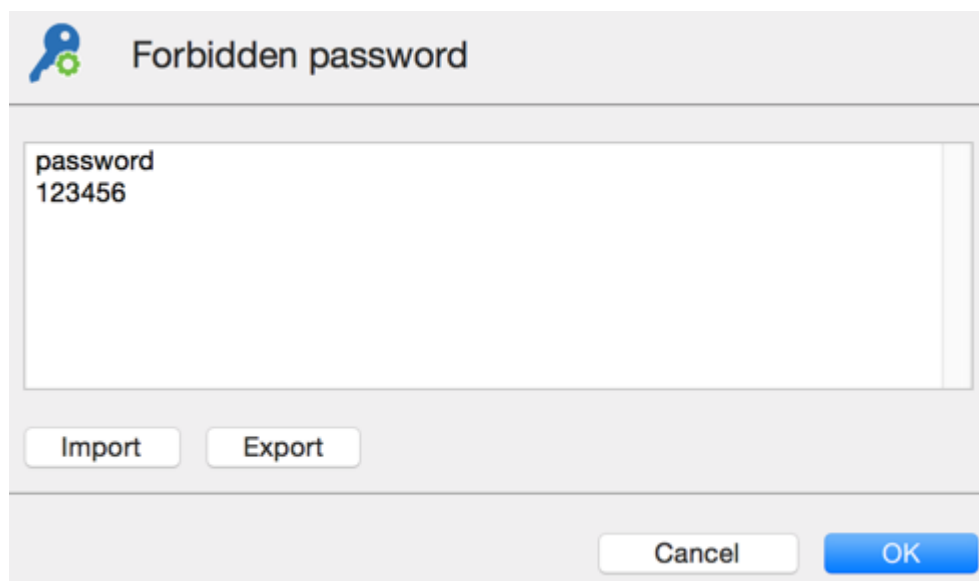
The application will generate an 8 characters password with mixed case alphanumerics and special characters.



Password generator - strong password

FORBIDDEN PASSWORD

You can generate your own list of forbidden password in the application.

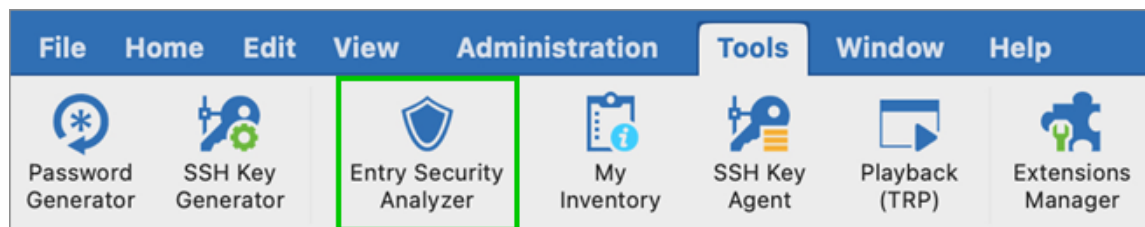


Forbidden password

6.7.2 Entry Security Analyzer

DESCRIPTION

The **Entry Security Analyzer** is available in the **Tools** menu. It will display the strength indicator for all passwords stored in your data source.



SETTINGS



In a single glance you can see the strength ratings of all your stored passwords.

OPTION	DESCRIPTION
Edit	Allows you to open the current entry so you can edit it.
Show all	When option is unchecked, only entries with actual password stored in them will be displayed.
Show compromised	Show if the password has been pwned. A pwned password is a password that has been exposed in data breaches (i.e., they are owned/pwned by hackers).

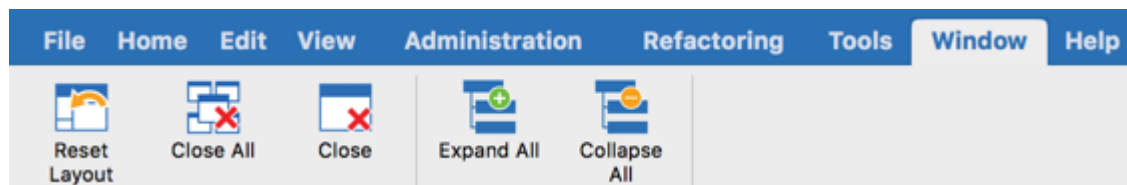
OPTION	DESCRIPTION
password (pwned)	
Forbidden Passwords	Display the password that you have in your blacklisted forbidden password.

6.8 Window

DESCRIPTION

The Window menu allows you to manage the overall display of Remote Desktop Manager for Mac.

SETTINGS



Windows ribbon

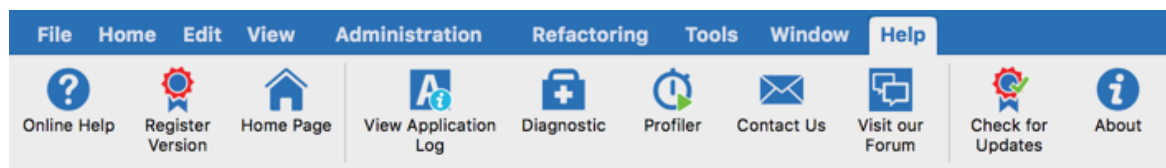
OPTION	DESCRIPTION
Reset Layout	Use the Reset Layout to apply the default layout settings.
Close All	Close all the opened session tabs.
Close	Close the active session tab.
Expand All	Expand all the groups in the Navigation pane when the Tree view mode is used.

OPTION	DESCRIPTION
Collapse All	Collapse all the groups in the Navigation pane when the Tree view mode is used.

6.9 Help

DESCRIPTION

The **Help** tab contain links to our Devolutions web site and Online Help. It also includes all the links to follow us on different social media platform. Our Support team might also ask you to perform some operations that you will find in the **Help** tab.



Help ribbon

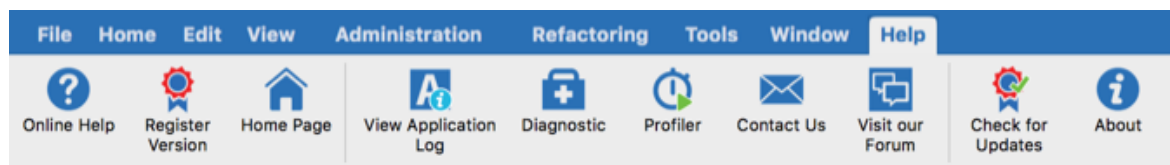
OPTION	DESCRIPTION
Online Help	Send you directly to our Windows Remote Desktop Manager Online Help.
Register Version	Enter your Trial or Enterprise license to register your Remote Desktop Manager version. For more information please see Register Enterprise Edition or Register Trial Edition .
Home Page	Send you directly to our Devolutions web site Home page.
View Application Log	To learn more please see Application Logs .

OPTION	DESCRIPTION
Diagnostic	To learn more please see Diagnostic .
Profiler	To learn more please see Profiler .
Contact Us	Automatically opens an email with our Support Devolutions address ready to be sent to us.
Visit our Forum	Sends you directly to our Forum.
Check for Updates	Verify if the latest version of Remote Desktop Manager for Mac is install on your computer. If not, the latest version can be install directly from this option.
About	Open a window containing multiple information regarding Remote Desktop Manager. It will display your Remote Desktop Manager version and your license information (if you are administrator).

6.9.1 Application Logs

DESCRIPTION

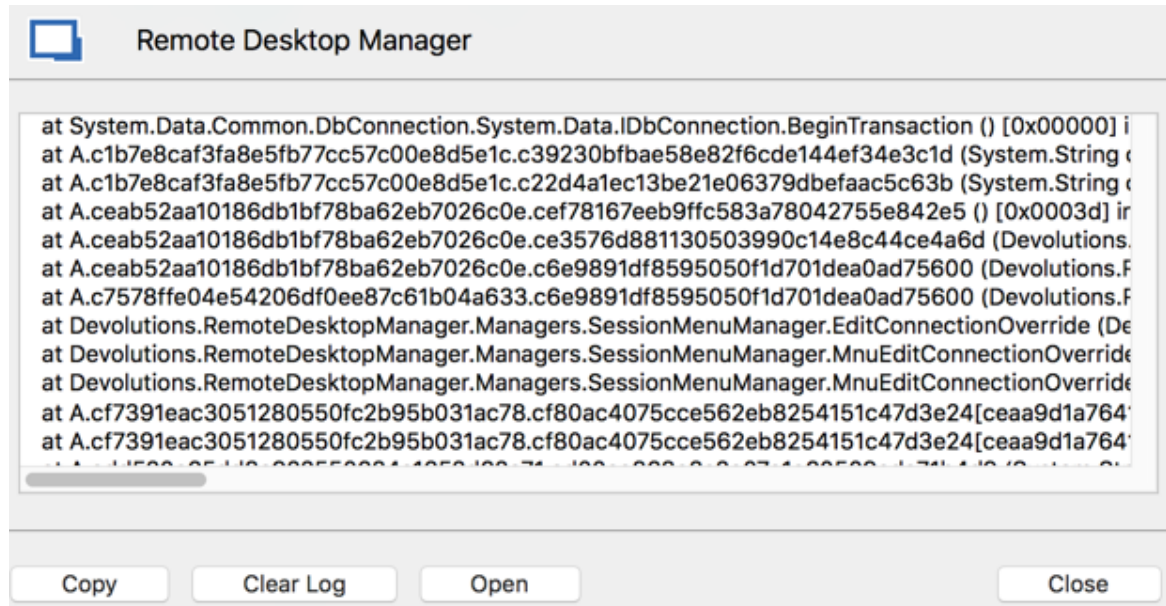
In case of error, you can verify the local application log, which is available from the menu in **Help - View Application Log**



Help ribbon

SETTINGS

Those logs are saved in **Macintosh HD/Users/Username/Library/Application Support/com.devolutions.remotedesktopmanager/RemoteDesktopManager.log**. You can view it as a list which can then be filter by Date, Message, Version, Info, Error or Error Silent.

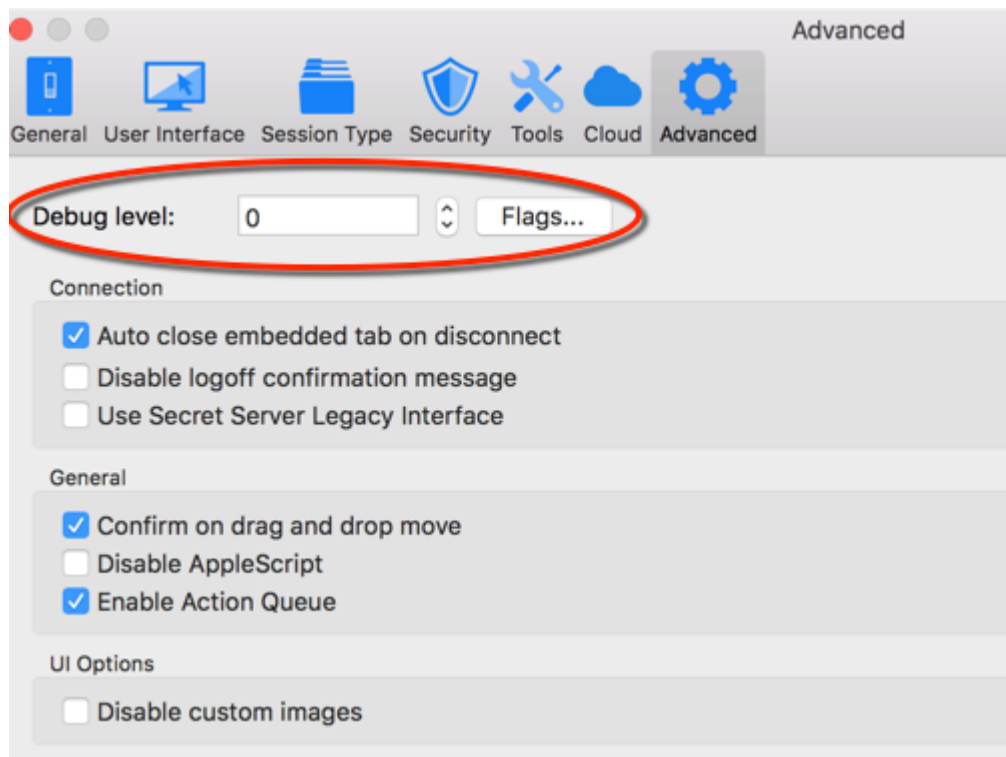


Application Logs

INCREASING THE LOG LEVEL

When requested by a Devolutions employee during a support process, you may be asked to increase the log level of the application to a higher level.

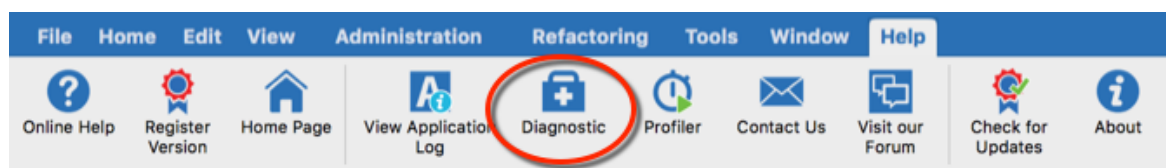
This can be done via **File - Preferences - [Advanced](#)** section.

*Advanced - Debug Level*

6.9.2 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.

*Help - Diagnostic*

SETTINGS

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 Terminal Services. However Remote Desktop Manager is fully compatible with Terminal Services.

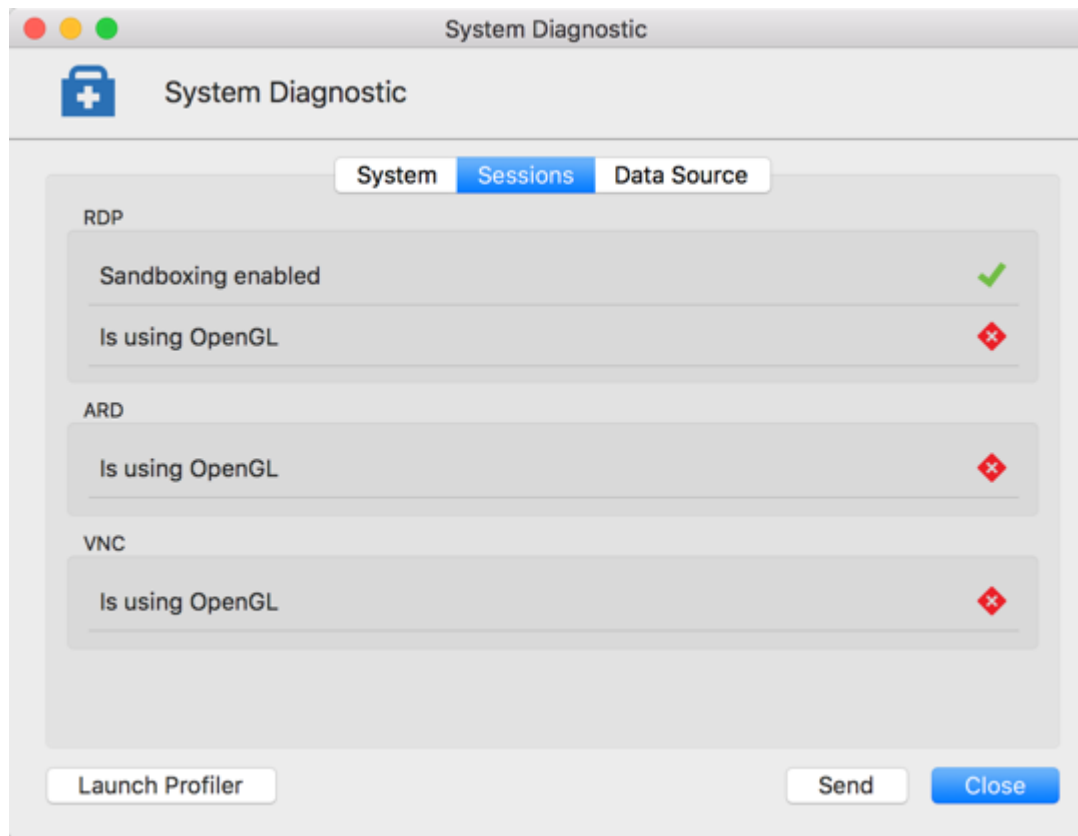
FIPS related issues and solutions can be found in the specific FIPS (Encryption) troubleshooting section.



System Diagnostic - System

SESSIONS

The **Sessions** tab contains information regarding your RDP, ARD and VNC sessions held in your Data Source.



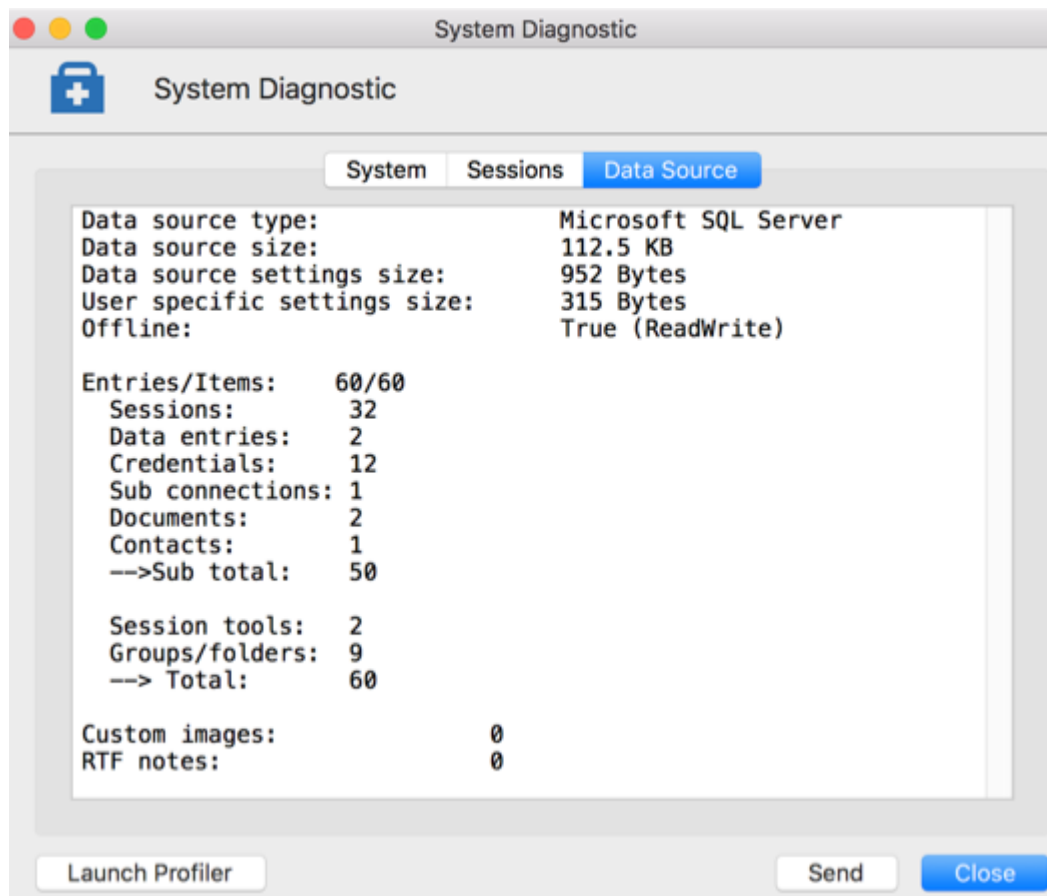
System Diagnostic - Sessions

DATA SOURCE

The Data Source tab contains information regarding your Data Source, including 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

6.9.3 Profiler

DESCRIPTION

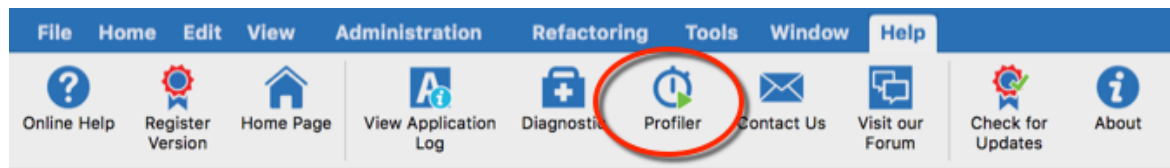
Remote Desktop Manager for Mac has a built-in profiler to diagnose connectivity issues with a data source.



Too many custom images could dramatically increase the size of the data source and cause load time issue.

PROCEDURE

1. Select **Help - Profiler**.

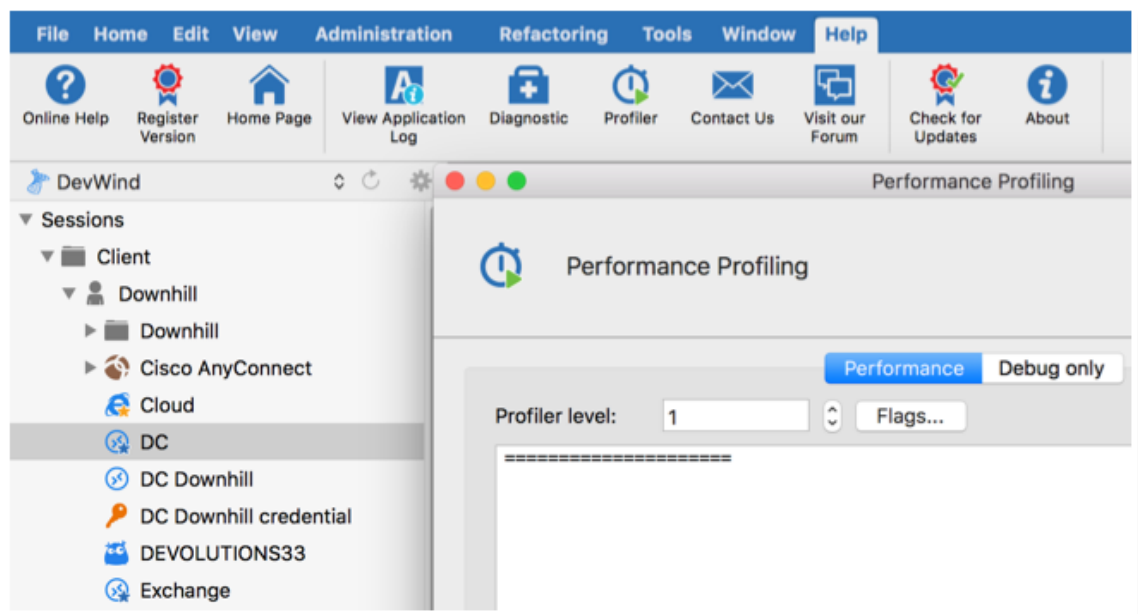


Help - Profiler

2. Move the window to the side in order to display the Remote Desktop Manager main window and refresh the data source by using the refresh button or by using **File - Refresh**.

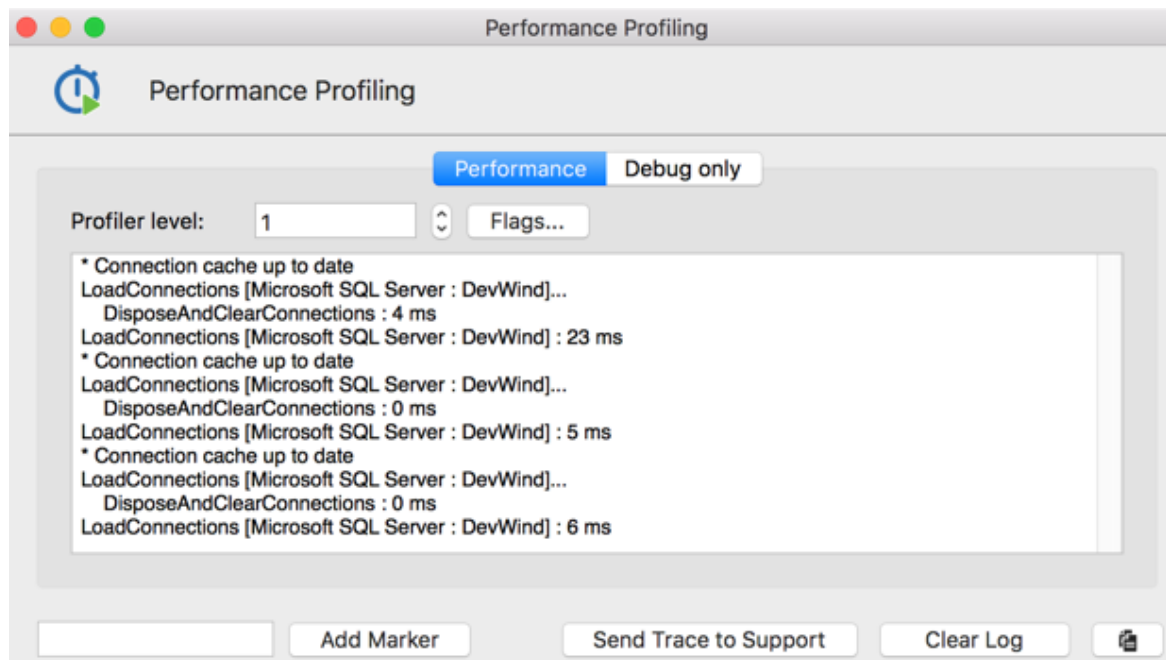


Holding the **CTRL** key while performing the refresh will force a full reload of the data source, thereby ignoring the cache.



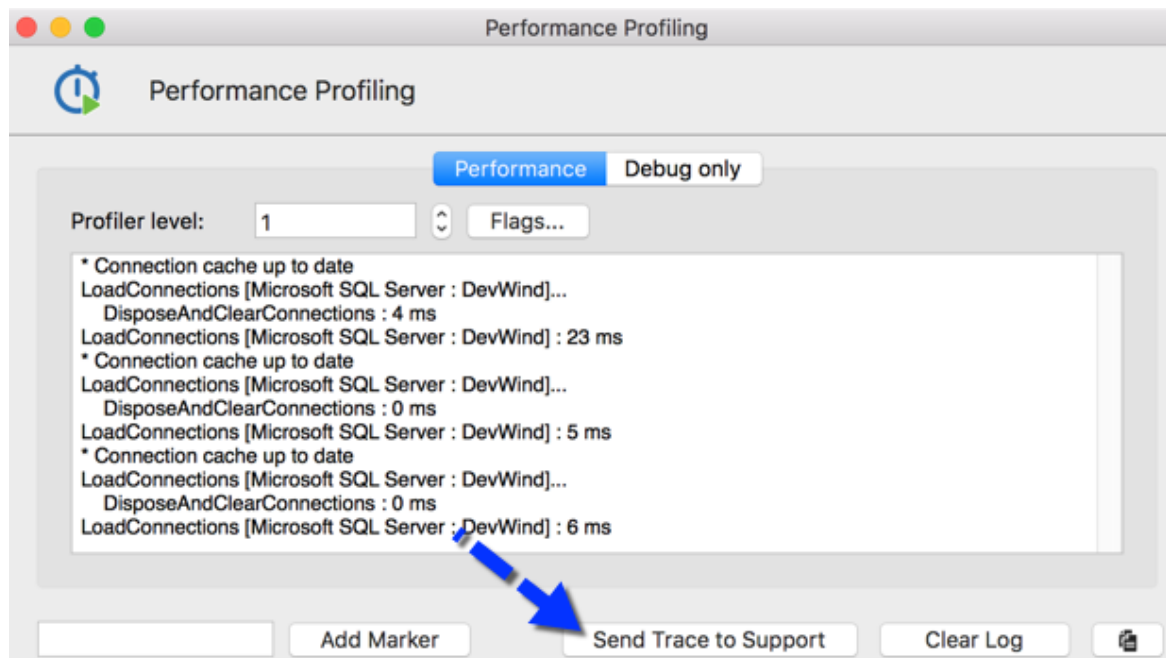
Performance Profiling

3. The Profiler data will appear in the **Performance Profiler** window.



Performance Profiling result

4. 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.



Send Trace to Support

DEBUG ONLY

To learn more about the debug option please see [Debug only](#).

6.9.3.1 Debug only

DESCRIPTION

Sometimes when an issue occurs while using Remote Desktop Manager for Mac, the support personnel may ask you to turn on debugging and send the information back.

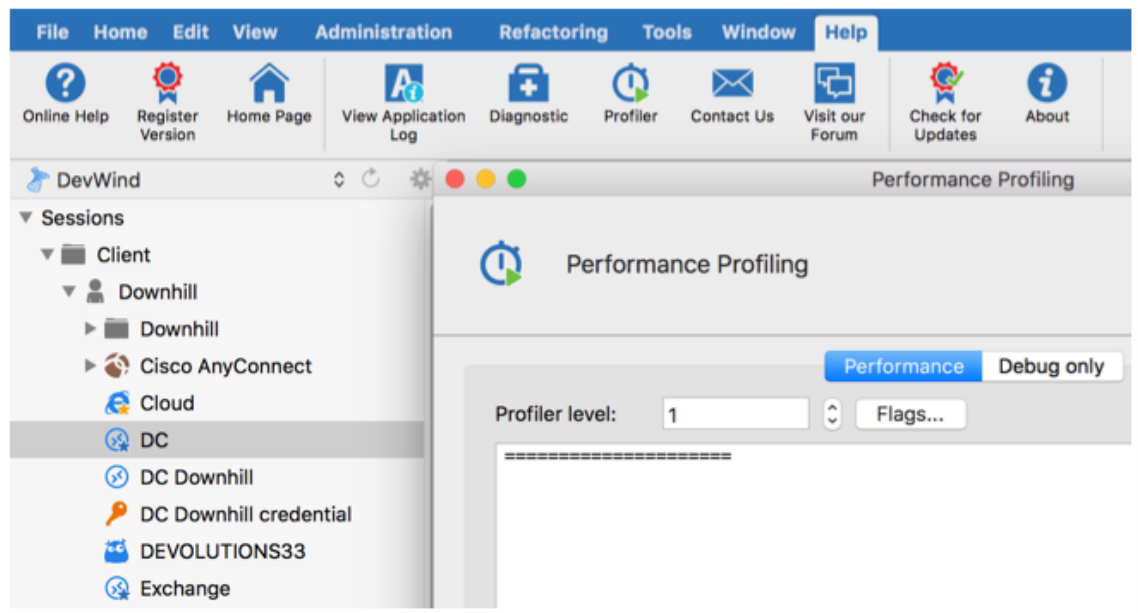


Any debug level other than zero will slow down the application and write a lot of information in the application logs. As soon as you have completed the diagnostics you should revert back the debug level to zero.

SETTINGS

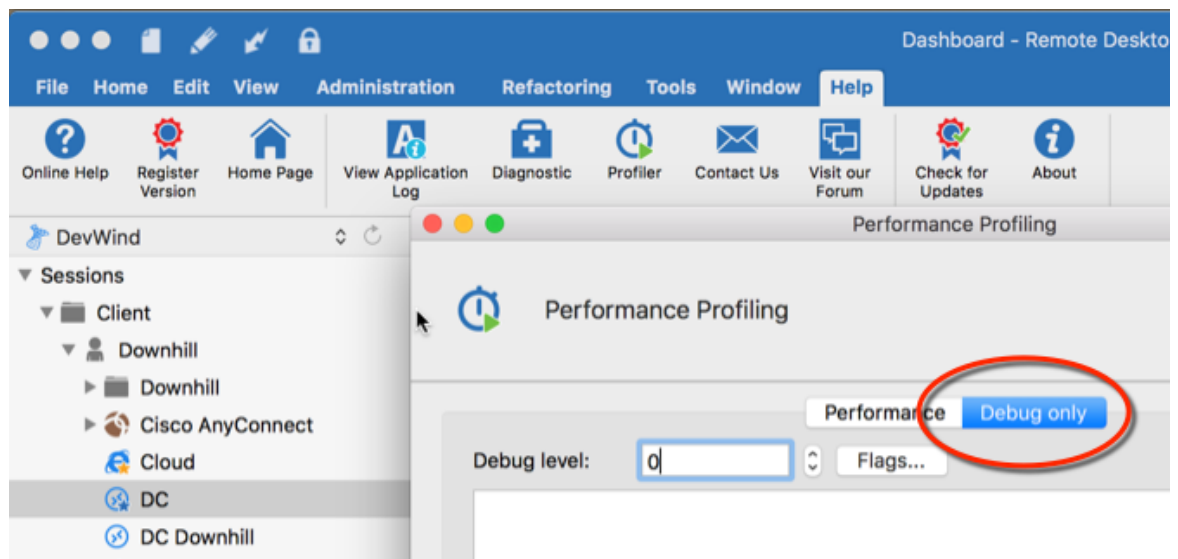
Use the debugging method whenever you need to diagnose the start-up or initial connection.

1. Start by clicking on Help - Profiler. Move the window aside to clear the main window of Remote Desktop Manager for Mac



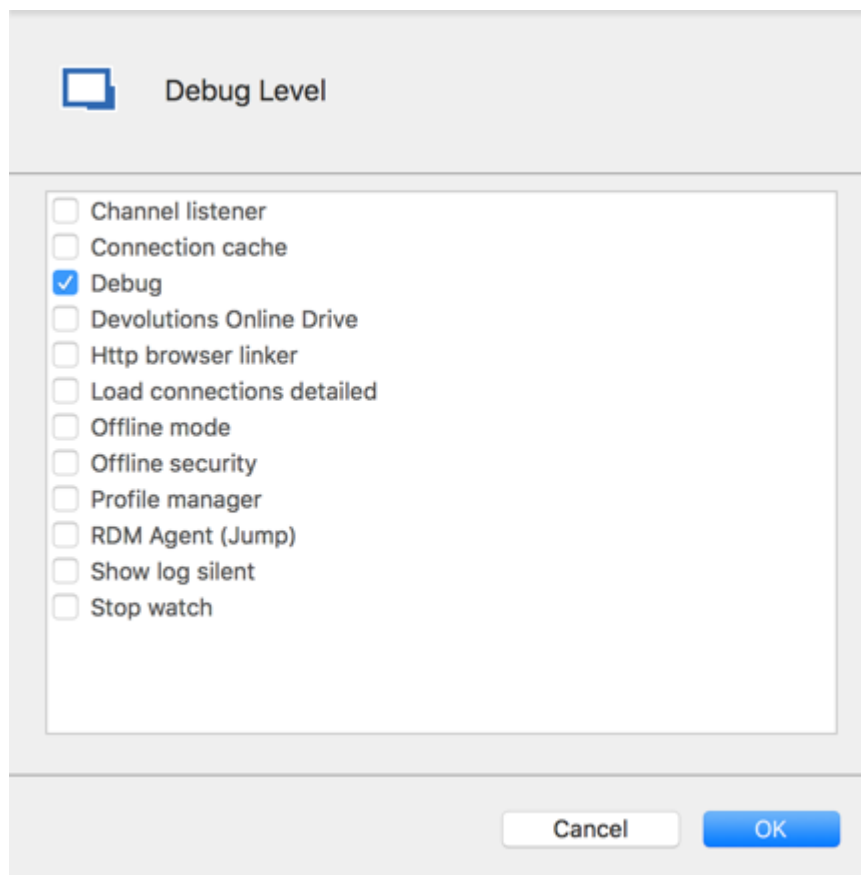
Performance Profiling

2. In the **Debug only** tab, click on the ellipsis button and activate the proper debug categories.



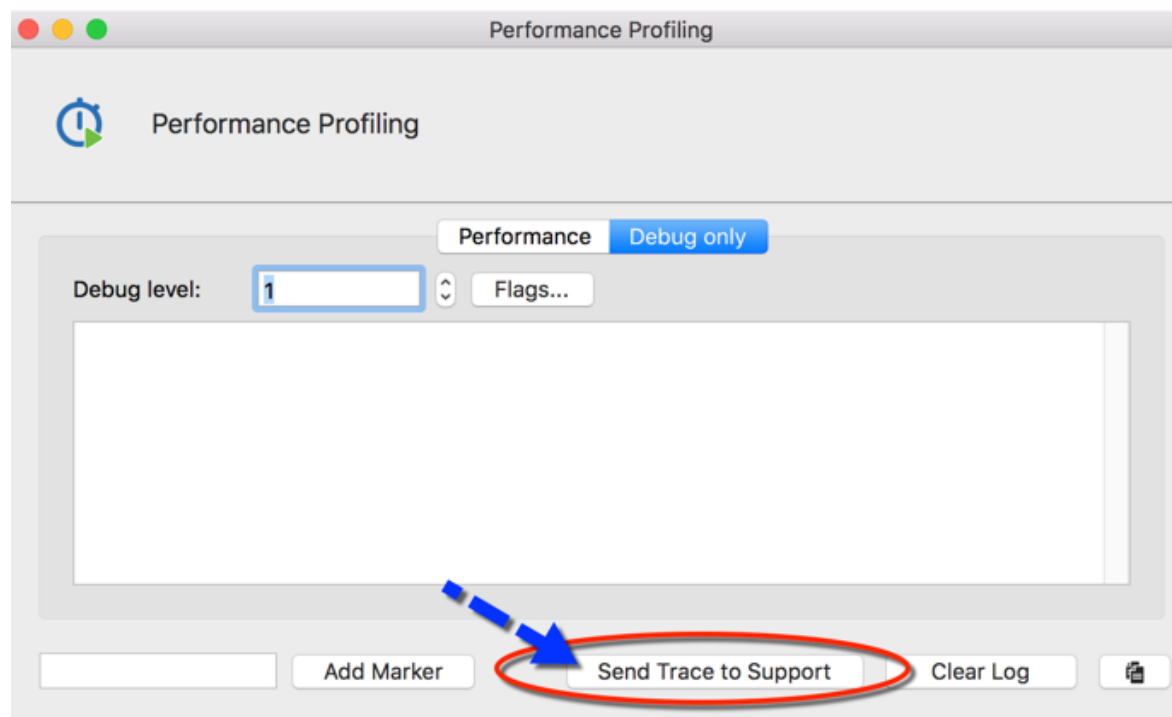
Help - Profiler - Debug only

3. In Remote Desktop Manager for Mac, click on Flags to check what perform the action that is under investigation.



Performance Profiling - Debug level

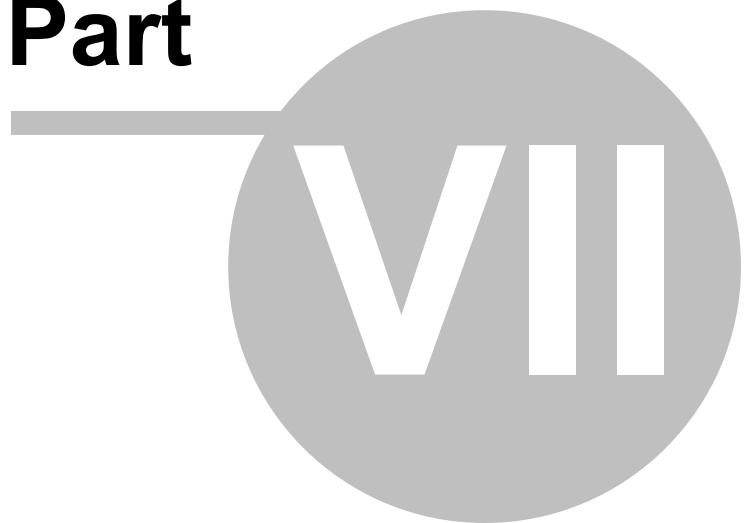
4. Then, click on **Send trace to support**. In the following dialog, ensure you specify enough information to link the report to the appropriate ticket, if the process was started from the forum include your forum user name.



Send trace to support

Devolutions Web Login

Part



7 Devolutions Web Login




7.1 Overview

DESCRIPTION



Devolution Web Login is a web browser password plugin used in conjunction with Remote Desktop Manager, Devolutions Server and Password Hub, which allows users to securely inject passwords into websites using credentials stored in their vaults.

It gives system administrators full control over the management of passwords, without affecting the user's productivity.

 <p>Remote Desktop Manager</p> <p>Centralize, Manage and Secure Remote Connections</p>	 <p>Devolutions Server</p> <p>Secure, Manage and Monitor Access to Privileged Accounts</p>	 <p>Password Hub</p> <p>Vault and Manage Business-User Passwords</p>
<p>Remote Desktop Manager centralizes all remote connections on a single platform that is securely shared between users and across the entire team.</p>	<p>Devolutions Server lets you control access to privileged accounts and manage remote sessions through a secure solution that can be deployed on-premises.</p>	<p>Password Hub is a secure and cloud-based password manager for teams.</p>



Advanced users, other browser extensions, or even JavaScript injection can all result in the password being read from the password edit control, even if it displays dots instead of the password. Any use of an external browser must be carefully weighed against your security requirements.

7.2 Installation

DESCRIPTION

Devolution 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 Devolution Web Login plugin:

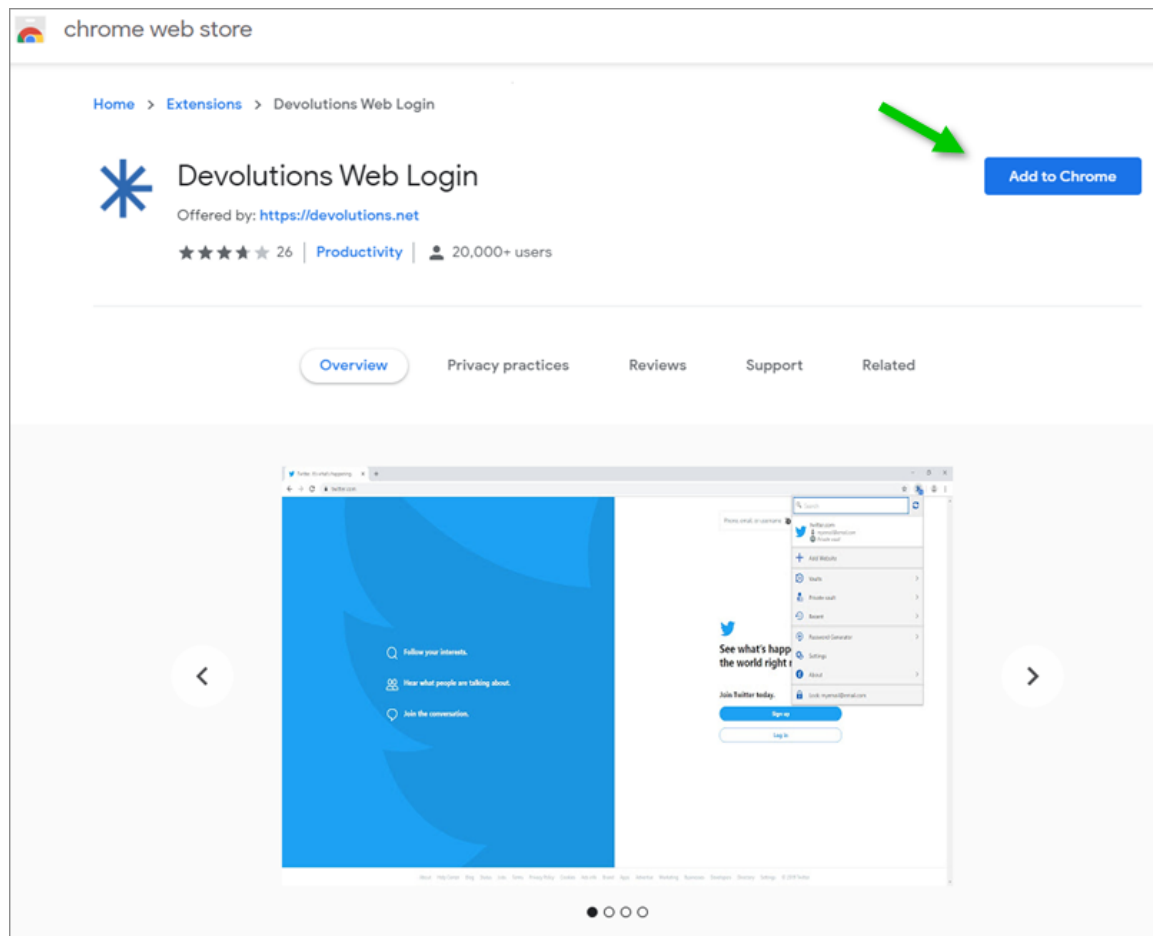
- [Chrome](#)
- [Firefox](#)
- [Edge](#)
- [Opera](#)

7.2.1 Chrome

DESCRIPTION

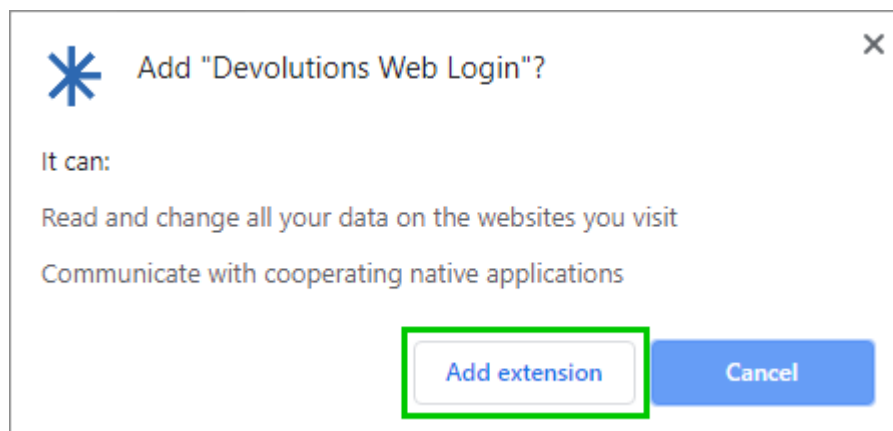
Follow the steps below to complete the installation of Devolution Web Login in the Chrome web browser.

1. Open Chrome.
2. Navigate to [Devolution Web Login extension](#) or use the link from our [Website](#).
3. Click the **Add To Chrome** button.



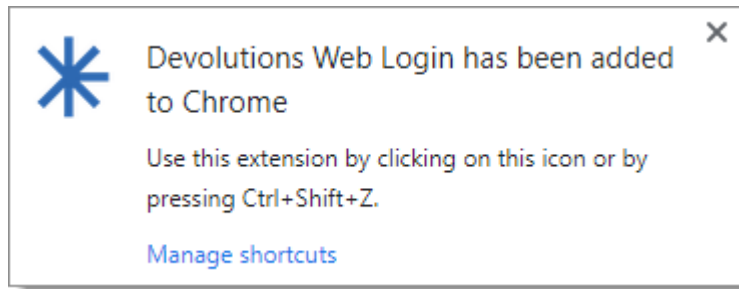
Devolutions Web Login Chrome Web Store

4. Click **Add extension** in the confirmation dialog.

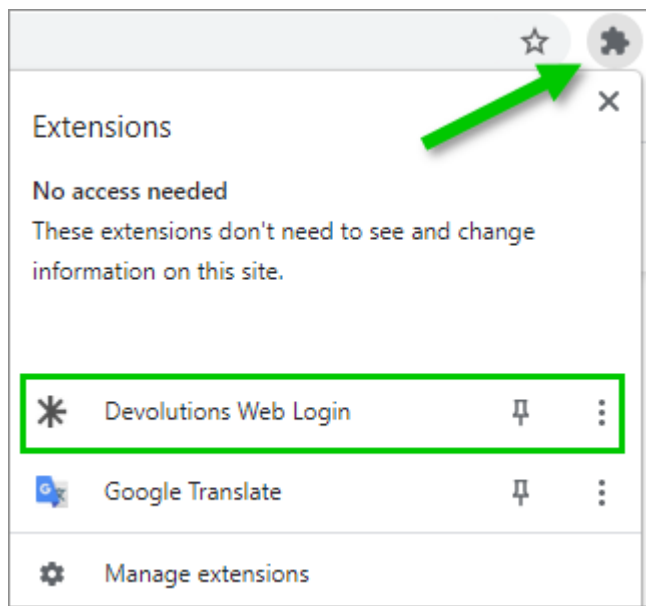


Extension Installation Confirmation

Once installed a confirmation box will appear.



5. Click the Chrome extension button and **Pin** Devolution Web Login to finish the installation.



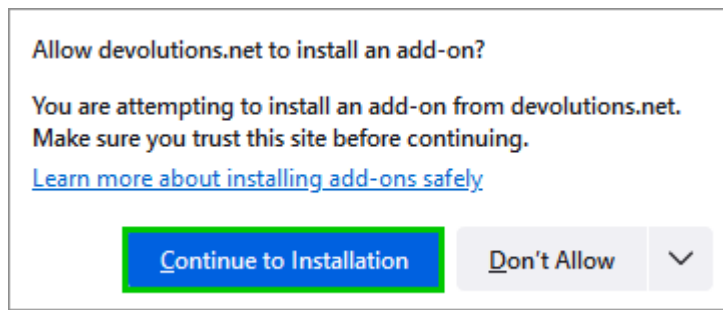
Devolution Web Login Extension Button

7.2.2 Firefox

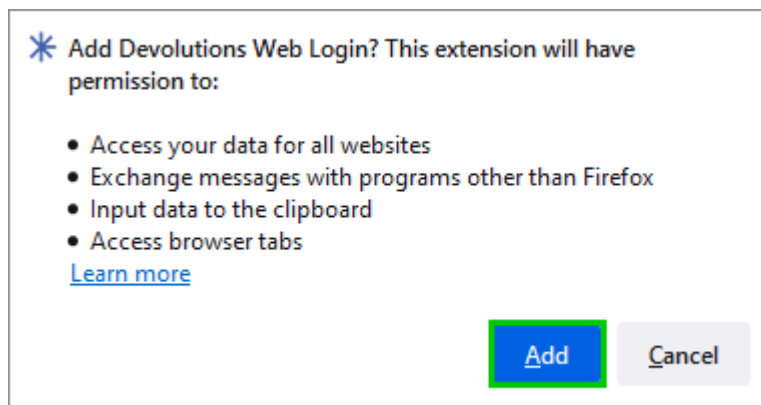
DESCRIPTION

Follow the steps below to complete the installation of Devolution Web Login in the Firefox web browser.

1. Open a Firefox window.
2. Download the extension from our [Devolution Web Login](#) website page.
3. Click **Continue to Installation** in the confirmation dialog.

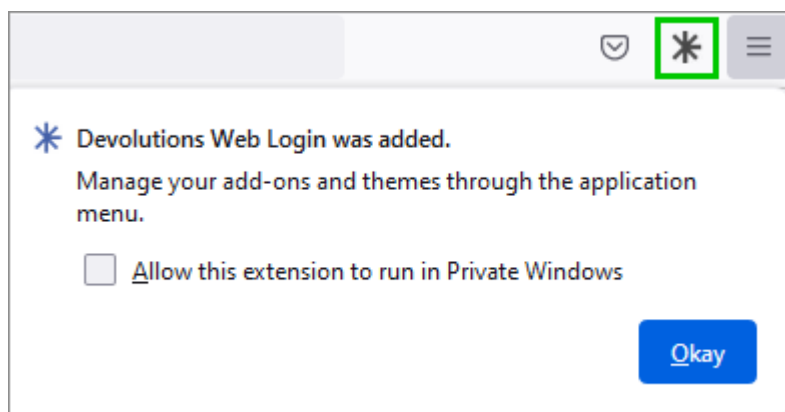


4. Click **Add**, when prompted to add Devolution Web Login to the extension.



Add the Extension

5. Once installed, access the extension by clicking * in the top-right corner of Firefox.



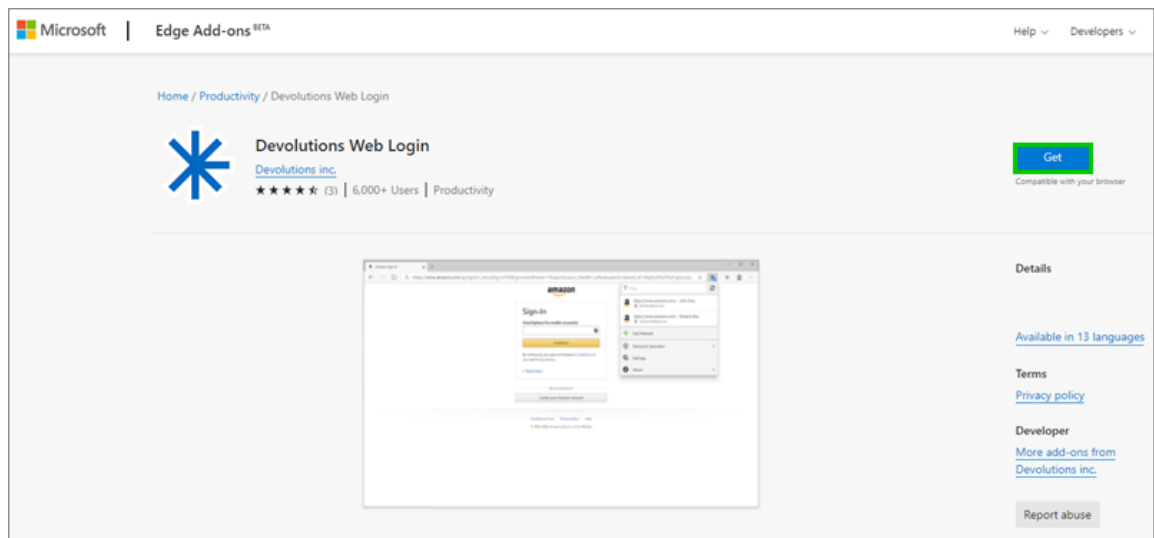
Devolution Web Login Extension Button

7.2.3 Edge

DESCRIPTION

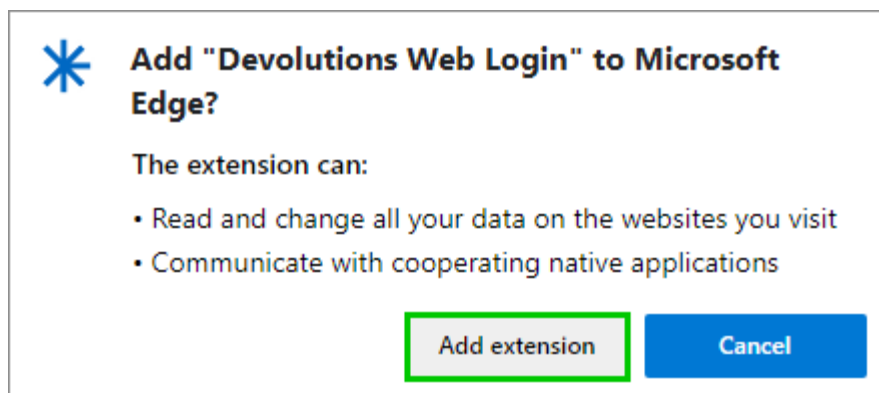
Here are the steps to install Devolution Web Login on Microsoft Edge.

1. Open a Microsoft Edge window.
2. Download the extension from [Devolution Web Login](#) website page.
3. Click **Get**.



Chrome Web Store

4. Add the extension to Microsoft Edge.



Add Devolution Web Login to Microsoft Edge Beta

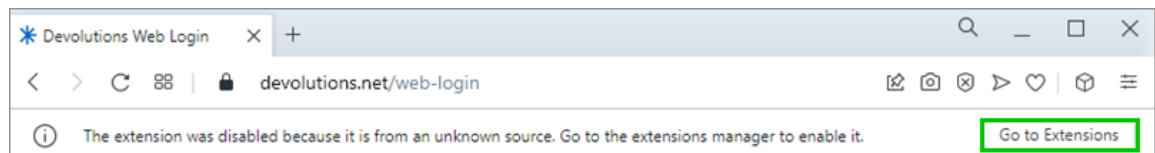
The extension is installed. Access it by clicking * in the top-right corner of the Microsoft Edge web browser.

7.2.4 Opera

DESCRIPTION

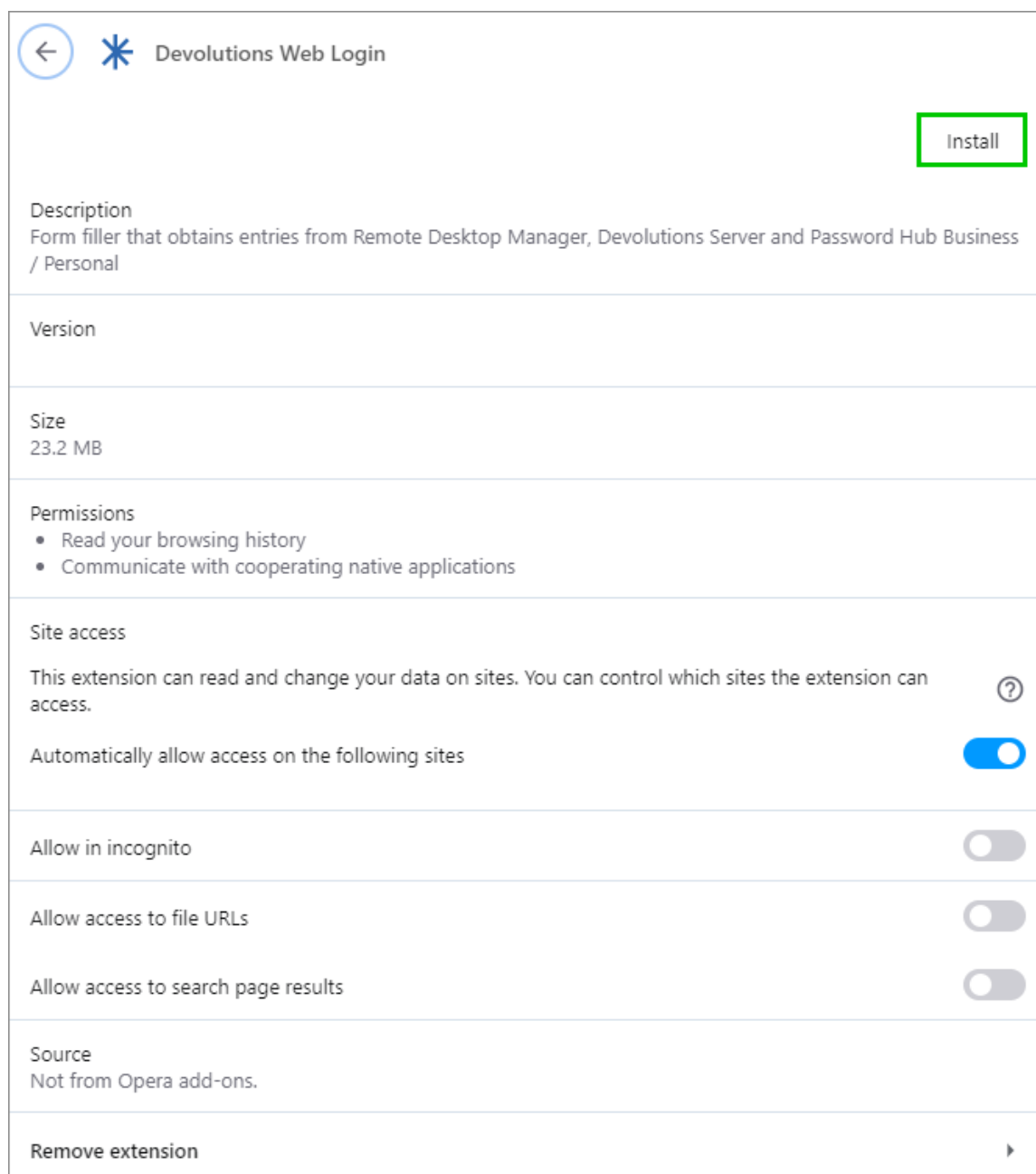
Follow the steps below to complete the installation of Devolution Web Login in the Opera web browser.

1. Open Opera.
2. Download the extension of [Devolution Web Login](#) from our website page.
3. Click on **Go to Extension** from the information panel at the top or click on the Extension button

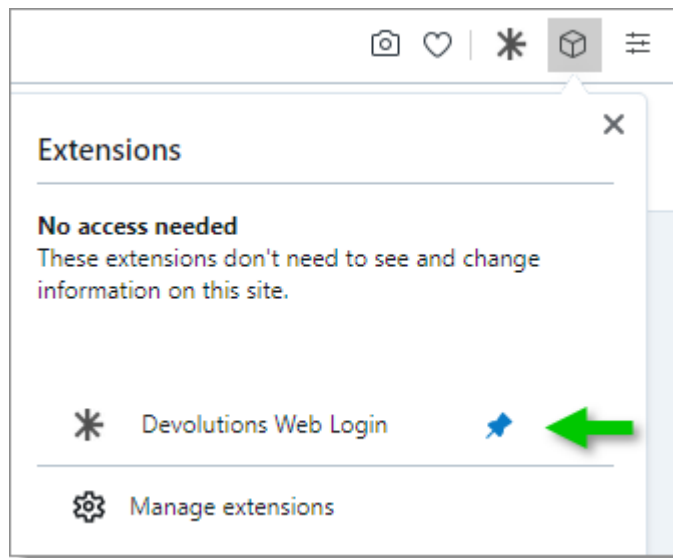


Opera Extensions Enabling

4. Click **Install** and the **Yes, install** pop up.

*Opera Install Window*

5. Click on the **Extensions** button of the browser and **Pin** the Devolution Web Login extension.



Access the extension by clicking * in the top-right corner of Opera.

7.3 First Login

7.3.1 Password Hub Business Login

DESCRIPTION

FIRST LOGIN WITH DEVOLUTION WEB LOGIN

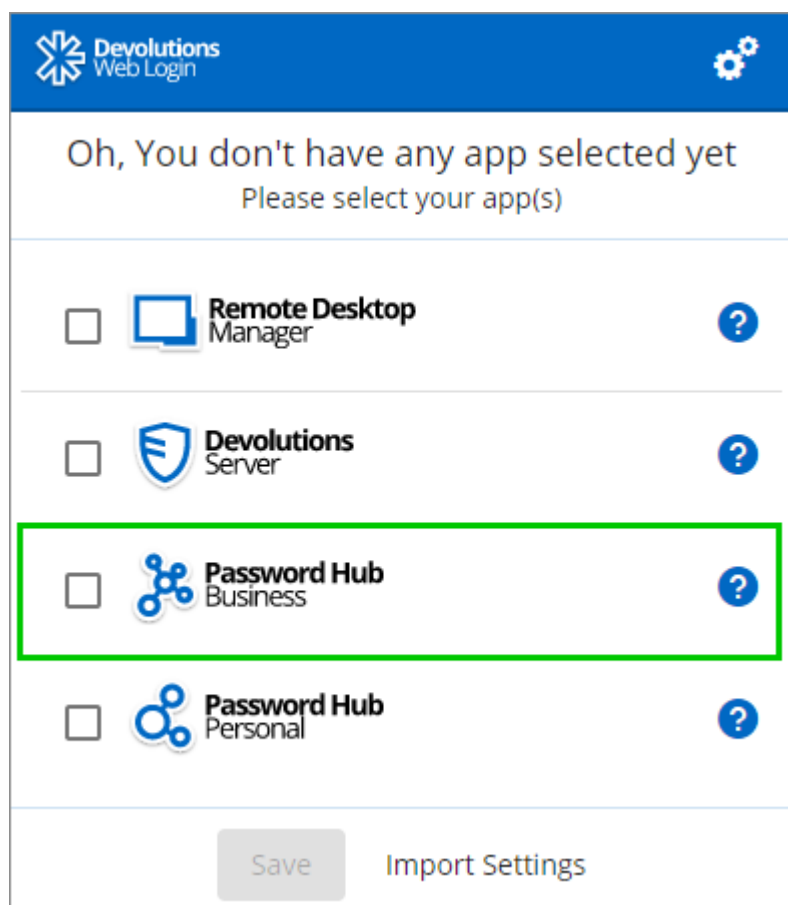
Follow these steps to connect Password Hub Business to Devolution Web Login extension:

1. Click on **Devolution Web Login** * extension at the top right corner of your browser.



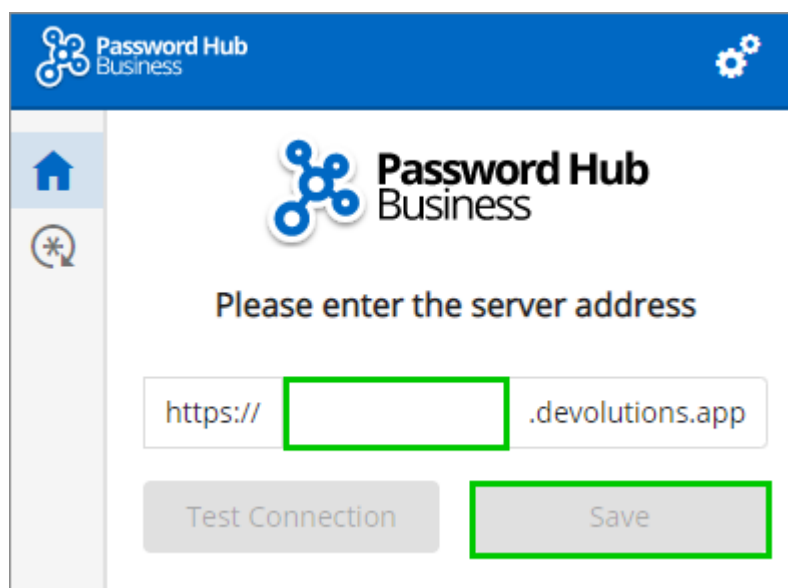
A Password Hub Business access is required to continue.

2. Choose **Password Hub Business** in the list and **Save**.



First Login

3. Enter your Password Hub Business server address and **Save**.

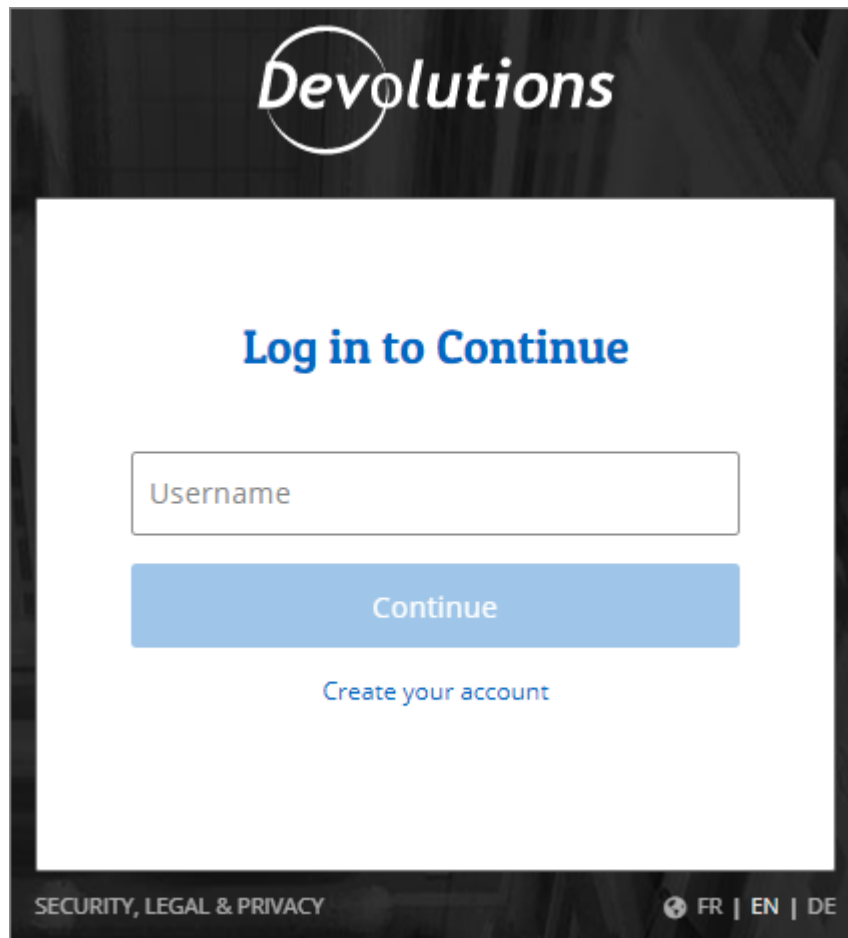


4. **Log in** to your Devolutions Account.



Log In

5. Enter the credentials from your Devolutions Account to continue.

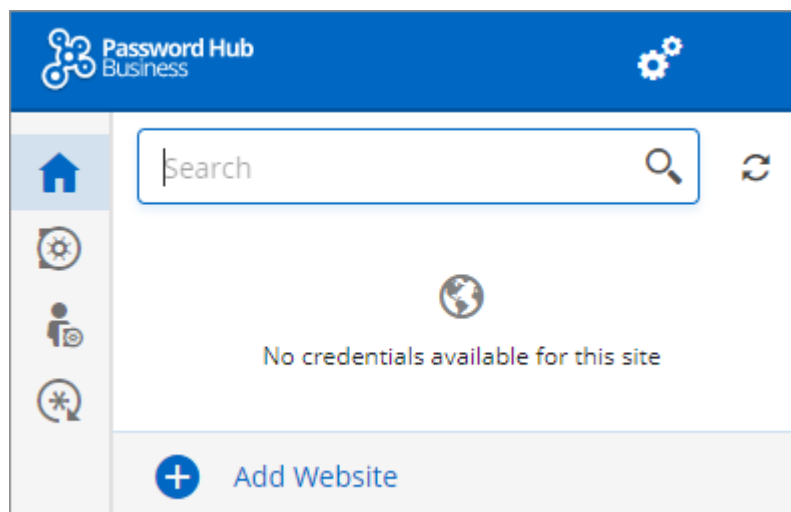


Devolutions Account Login

6. When complete, a log in confirmation message will appear.

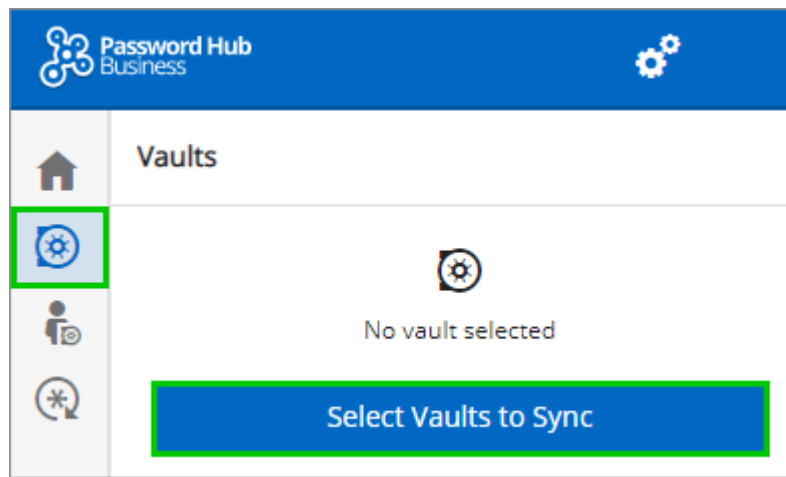


7. If you click on the * icon, you can validate that Devolution Web Login is now connected to your Password Hub Business.

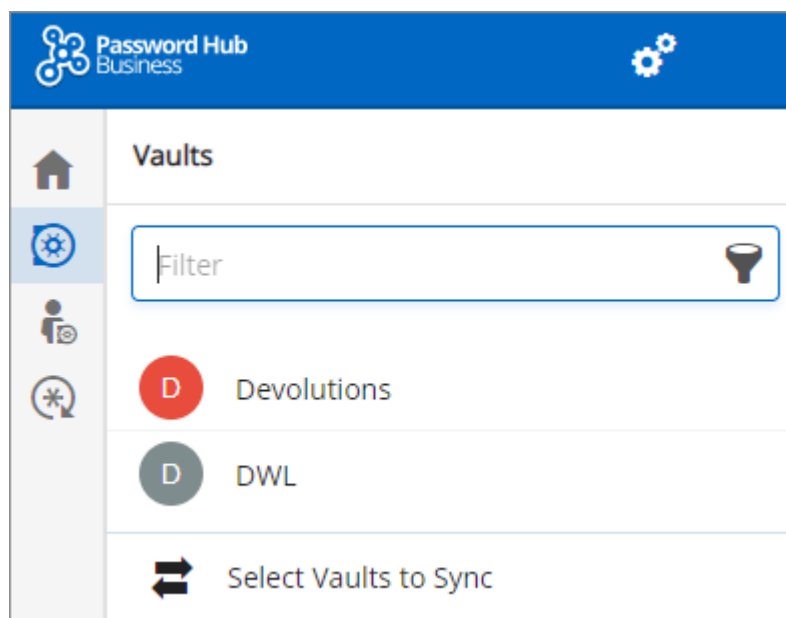


Devolution Web Login Connected to Password Hub Business

8. To select the vaults to be synchronized, click on the **Vaults** icon and the **Select Vaults to Sync** button. Afterward, you click on the **Select all** button, or refine your view by adding a check mark next to the specific vaults to synchronize.



9. When done selecting your vaults, click on the **Select Vaults to Sync** at the top of the panel, to get the following view.



7.3.2 Password Hub Personal Login

DESCRIPTION

FIRST LOGIN WITH DEVOLUTION WEB LOGIN

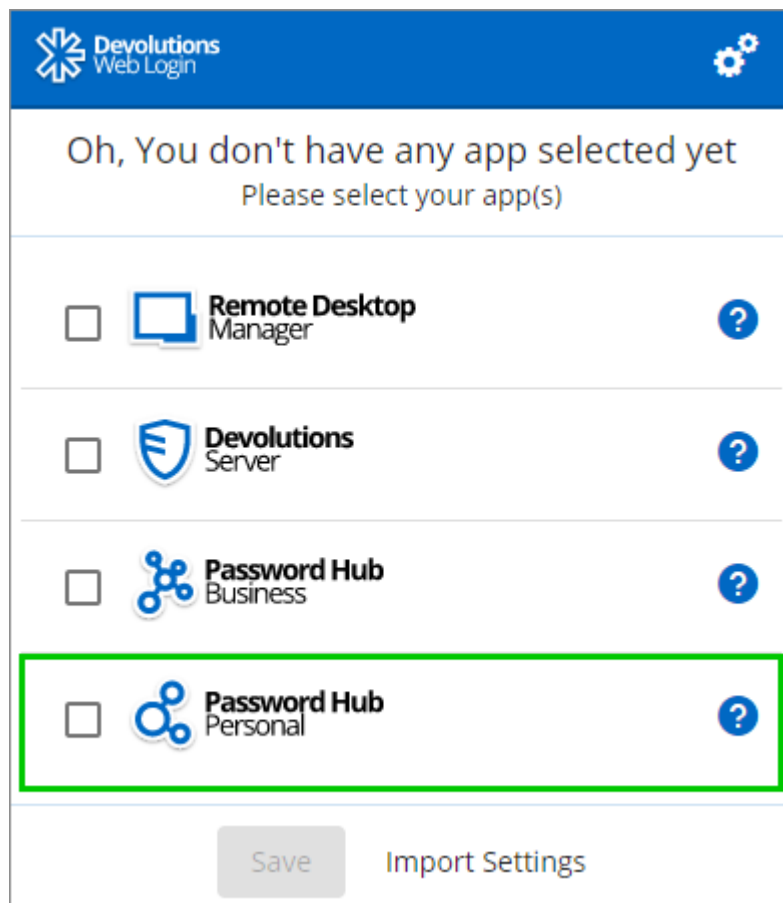
Follow these steps to connect Password Hub Personal to Devolution Web Login extension:

1. Click on **Devolution Web Login** * extension at the top right corner of your browser.

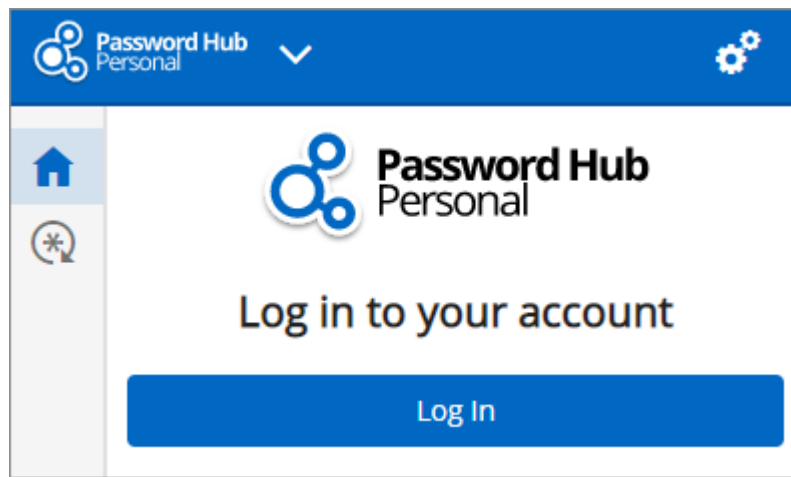


A Password Hub Personal access is required to continue.

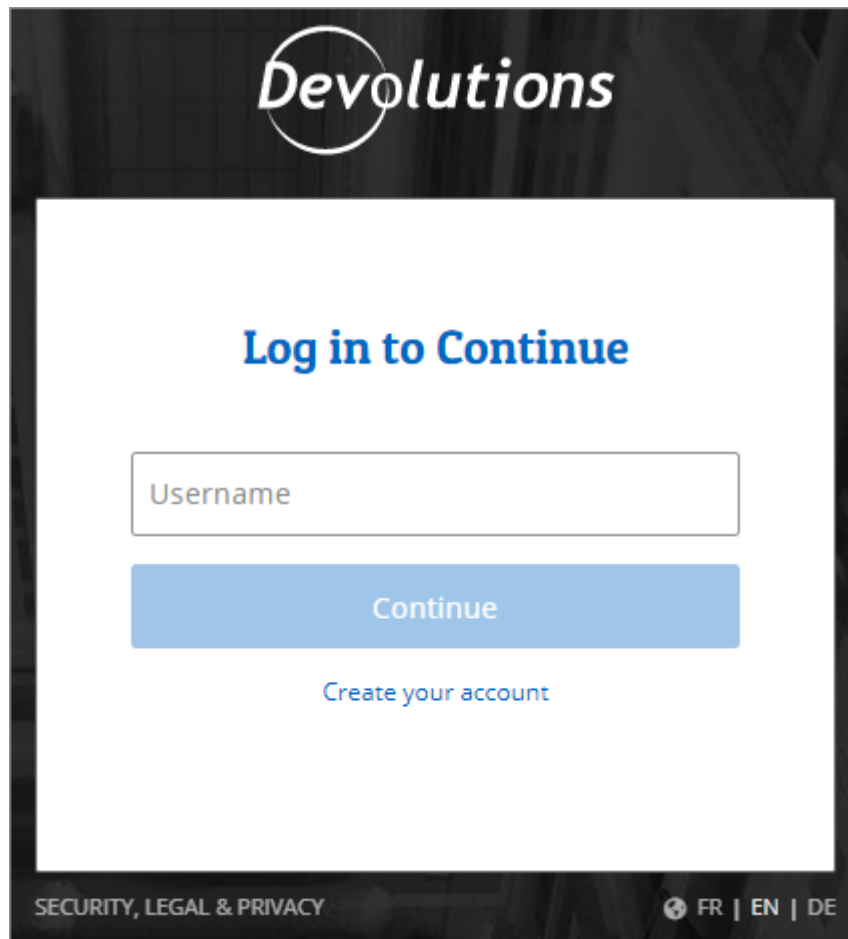
2. Choose **Password Hub Personal** in the list and **Save**.



3. **Log in** to your account.

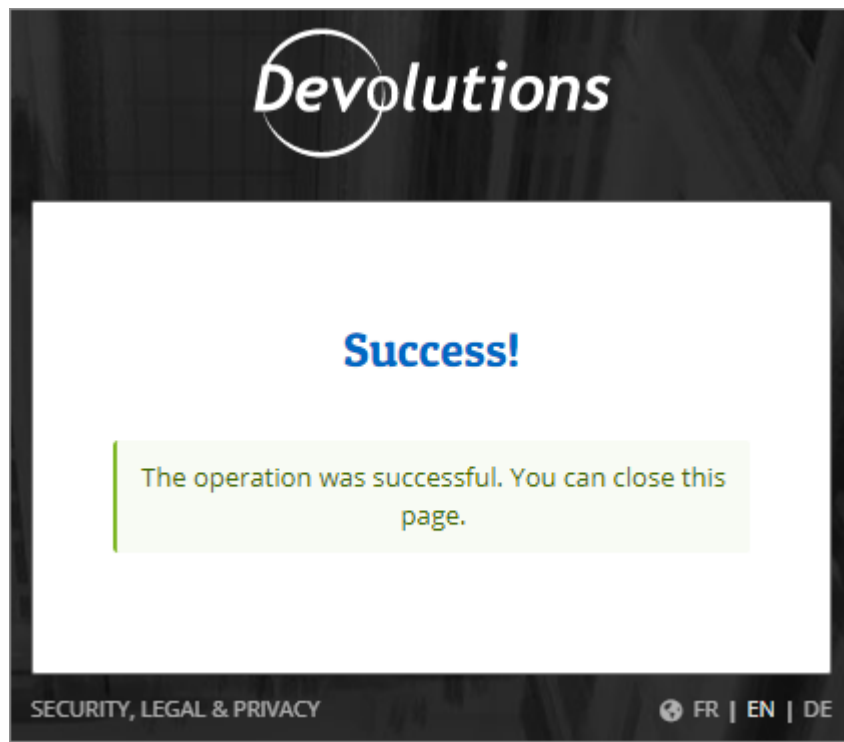


4. Enter the credentials from your Devolutions Account to continue.

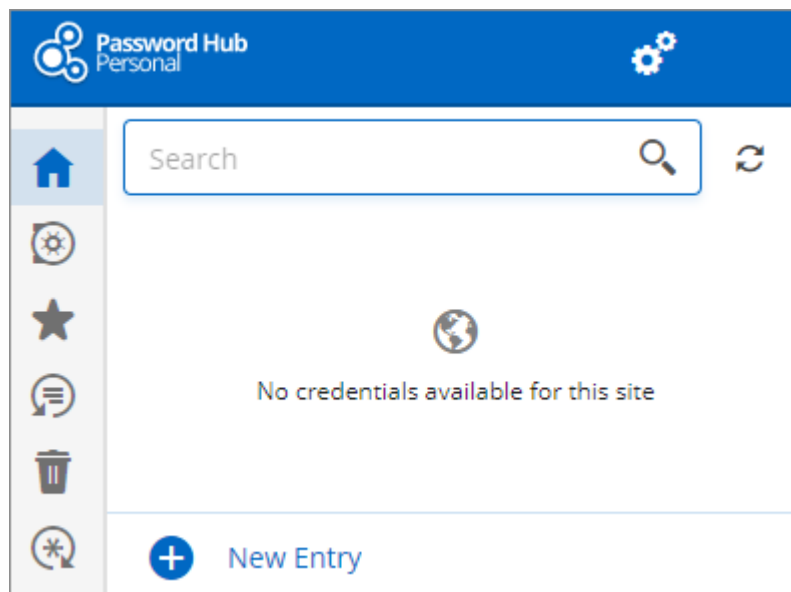


Devolutions Account Login

5. When complete, a log in confirmation message will appear.



6. If you click on the * icon, you can validate that Devolution Web Login is now connected to your Password Hub Personal.



7.3.3 Devolutions Server Login

DESCRIPTION

FIRST LOGIN WITH DEVOLUTION WEB LOGIN

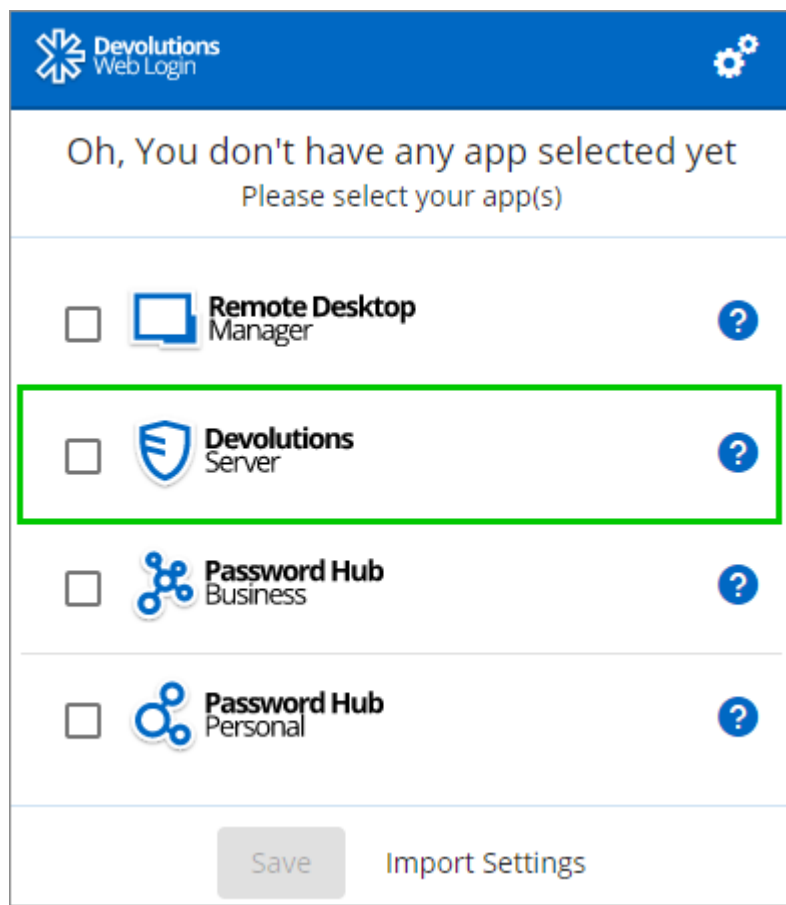
Follow these steps to connect Devolutions Server to Devolution Web Login extension:

1. Click on **Devolution Web Login** * extension at the top right corner of your browser.



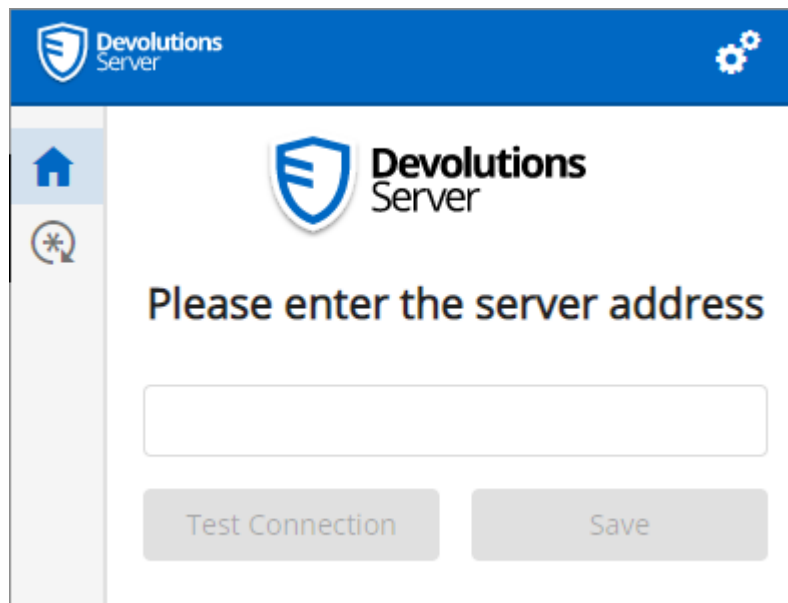
A Devolutions Server access is required to continue.

2. Choose **Devolutions Server** in the list and **Save**.



First Login

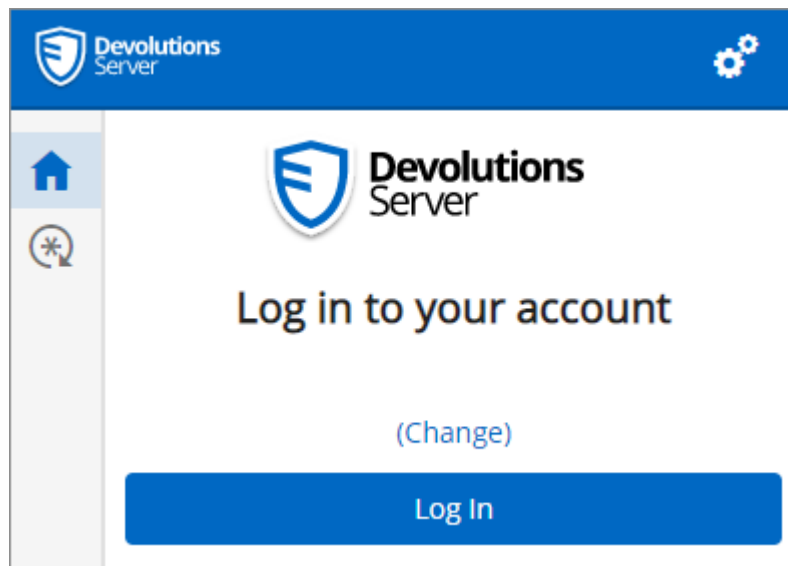
3. Enter the address of your server. You will need to input the same information that you would use to connect to the web interface of your Devolutions Server. Test the connection to validate it, then **Save**.



The screenshot shows the Devolutions Server web interface. At the top, there is a blue header with the Devolutions Server logo and a gear icon. Below the header, there is a sidebar with a home icon and a search icon. The main content area displays the Devolutions Server logo and the text 'Please enter the server address'. Below this text is a text input field. At the bottom of the main content area, there are two buttons: 'Test Connection' and 'Save'.

Server Address

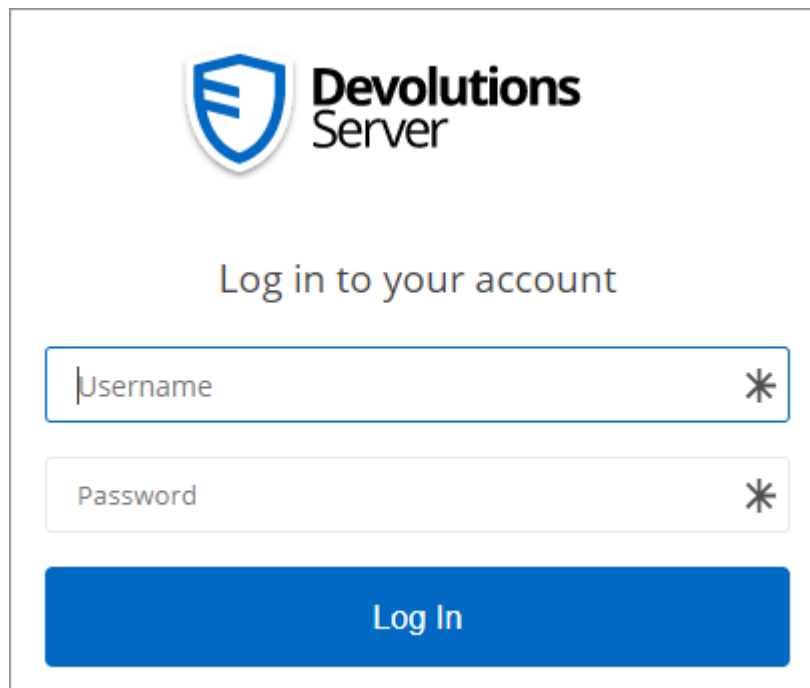
4. Click **Log In**.



The screenshot shows the Devolutions Server web interface. At the top, there is a blue header with the Devolutions Server logo and a gear icon. Below the header, there is a sidebar with a home icon and a search icon. The main content area displays the Devolutions Server logo and the text 'Log in to your account'. Below this text is a link labeled '(Change)'. At the bottom of the main content area, there is a blue button labeled 'Log In'.

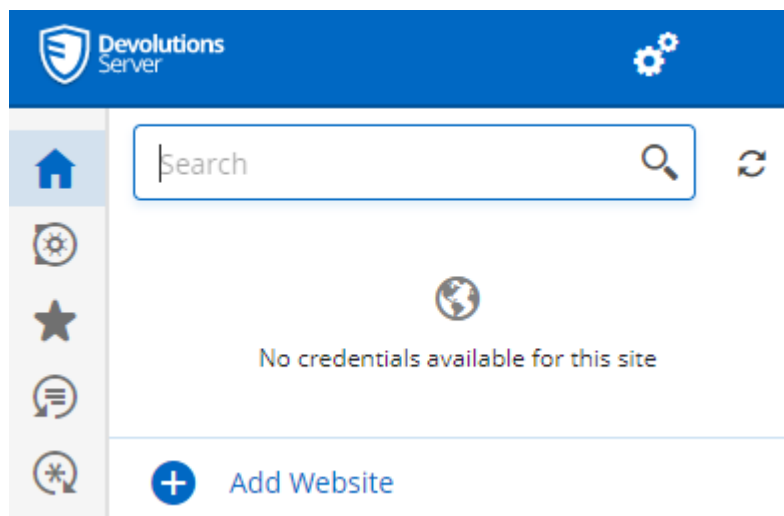
Devolution Web Login Login

5. Enter your Devolutions Server credentials and click **Log in**.

The image shows a login window for Devolutions Server. At the top left is the Devolutions Server logo, which consists of a blue shield with a white stylized 'E' and the text 'Devolutions Server' to its right. Below the logo, the text 'Log in to your account' is centered. There are two input fields: the first is labeled 'Username' and the second is labeled 'Password'. Both fields have a blue asterisk icon on the right side. Below the input fields is a large blue button with the text 'Log In' in white.

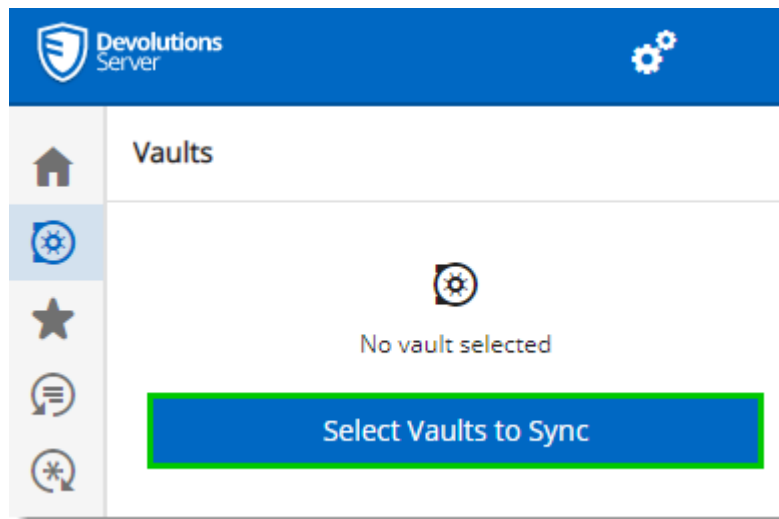
Devolutions Server Login

6. If you click on the * icon, you can validate that Devolution Web Login is now connected to your Devolutions Server.

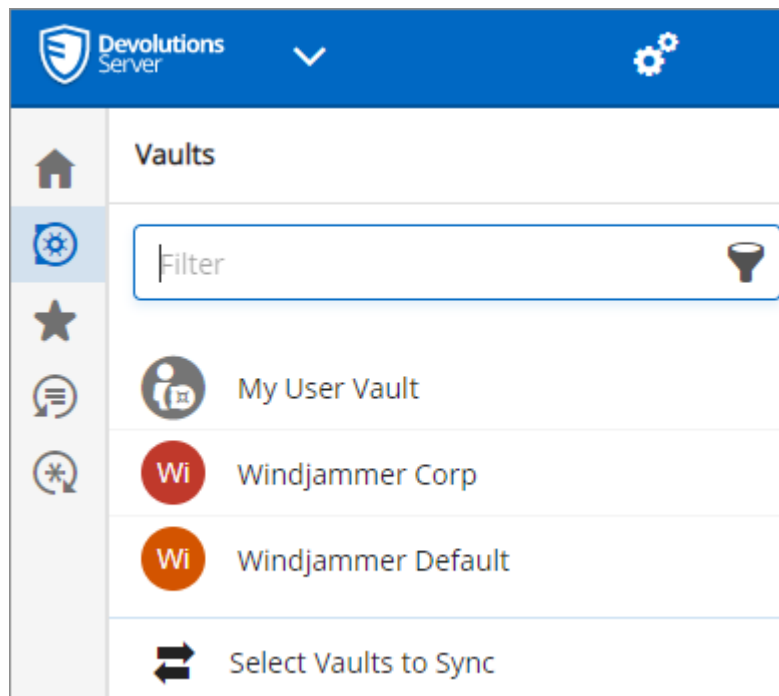


Devolution Web Login Connected

7. To select the vaults to be synchronized, click on the **Vaults** icon and the **Select Vaults to Sync** button. Afterward, you click on the **Select all** button, or refine your view by adding a check mark next to the specific vaults to synchronize.



8. When done selecting your vaults, click on the **Select Vaults to Sync** at the top of the panel, to get the following view.



7.3.4 Remote Desktop Manager Login

DESCRIPTION

FIRST LOGIN WITH DEVOLUTIONS WEB LOGIN

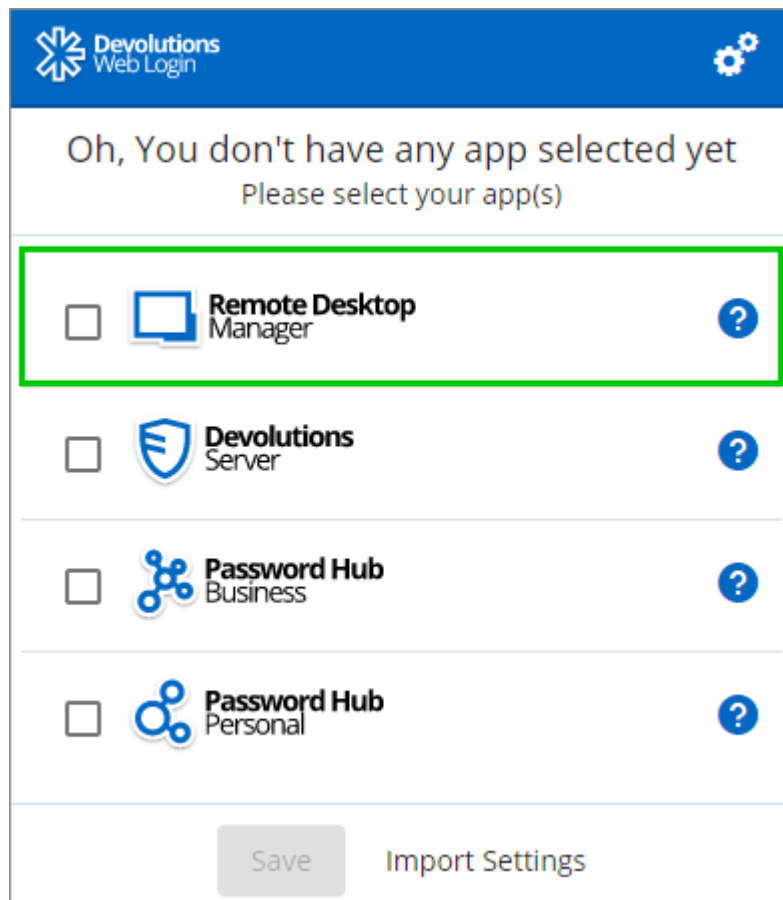
Follow these steps to connect your Remote Desktop Manager to Devolutions Web Login extension, you will be prompted to pair the two applications.

1. Click on Devolutions Web Login * extension at the top right corner of your browser.



Remote Desktop Manager must be installed and running to continue.

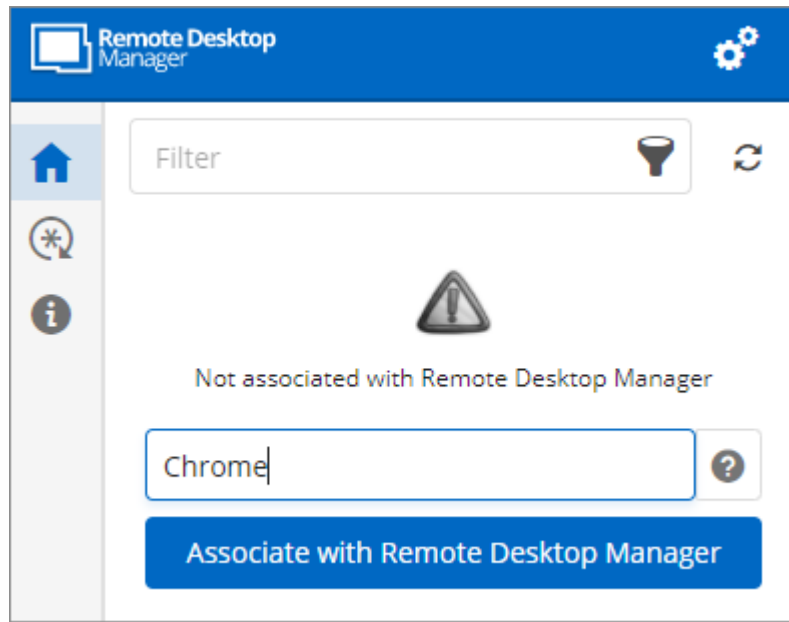
2. Choose **Remote Desktop Manager** in the list and **Save**.



3. Enter a name, for this association, in the text box.



This name can be used to identify a particular association and to deny access to it from Remote Desktop Manager. The default name is the name of the web browser running Devolution Web Login.

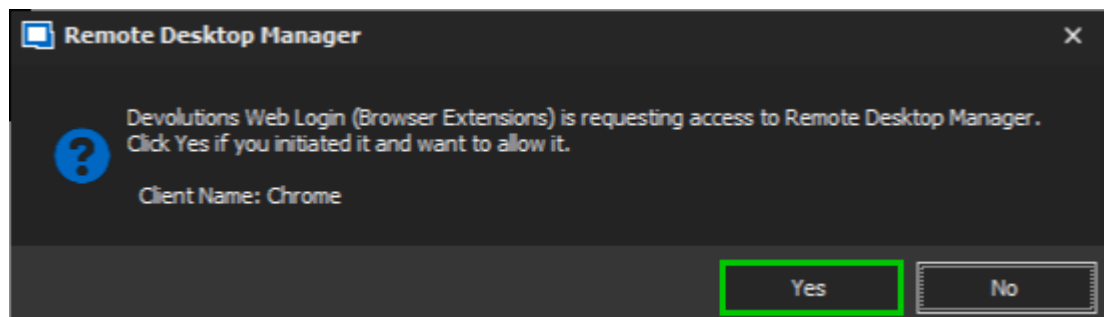


4. Click on **Associate with Remote Desktop Manager**.

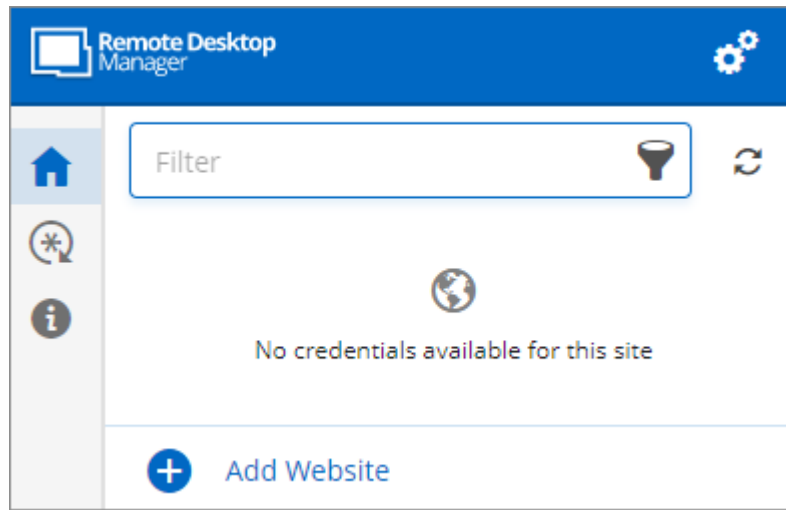


A popup window should appear on Remote Desktop Manager asking if the request was actually sent by you.

5. Click **Yes** in Remote Desktop Manager to accept the association request.



6. If you click on the * icon, you can validate that Devolution Web Login is now paired to your Remote Desktop Manager.

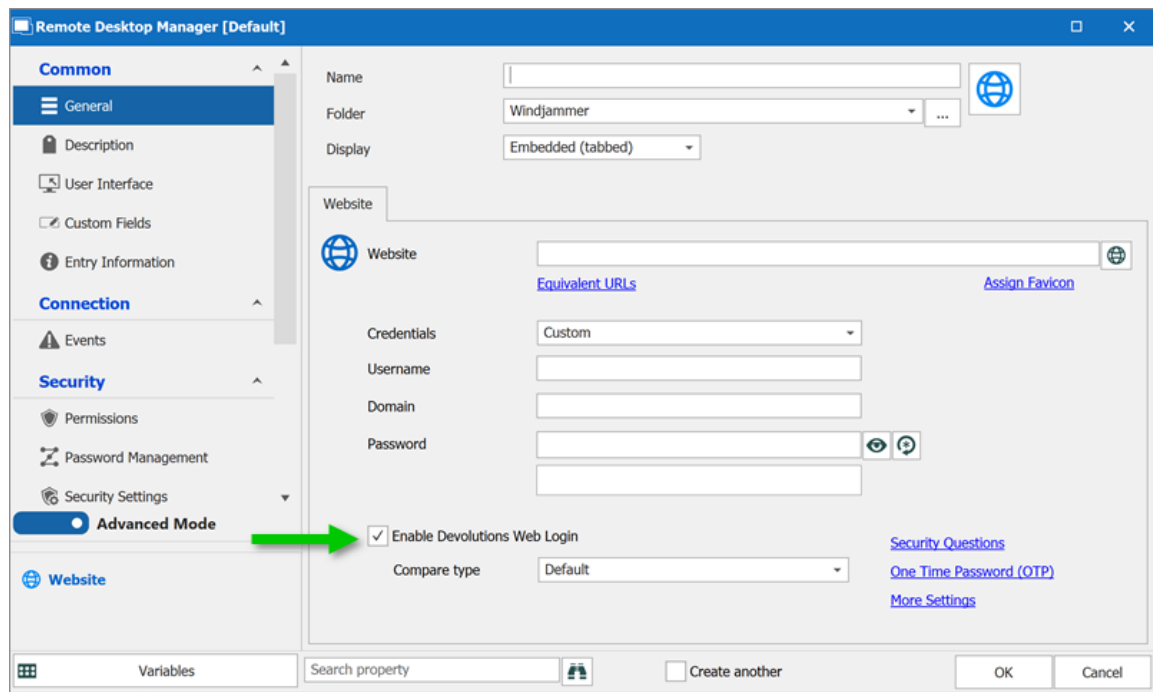


Note that, while Remote Desktop Manager can handle multiple associations (e.g., multiple browsers), Devolution Web Login can only be paired to a single instance of RDM at any time.

7.3.4.1 Enable Devolutions Web Login

DESCRIPTION

Checkmark ***Enable Devolution Web Login*** in Remote Desktop Manager entries to allow Devolution Web Login extension to retrieve the credentials when connecting to its respective website.



Enable Devolutions Web Login

7.4 Exploring Devolutions Web Login

7.4.1 Menu

DESCRIPTION

The user interface **Devolution Web Login** is slightly different in appearance when connected to Remote Desktop Manager, Devolutions Server or Password Hub Business and Personal.

See below a list of the menu and information available from the Devolution Web Login extension:

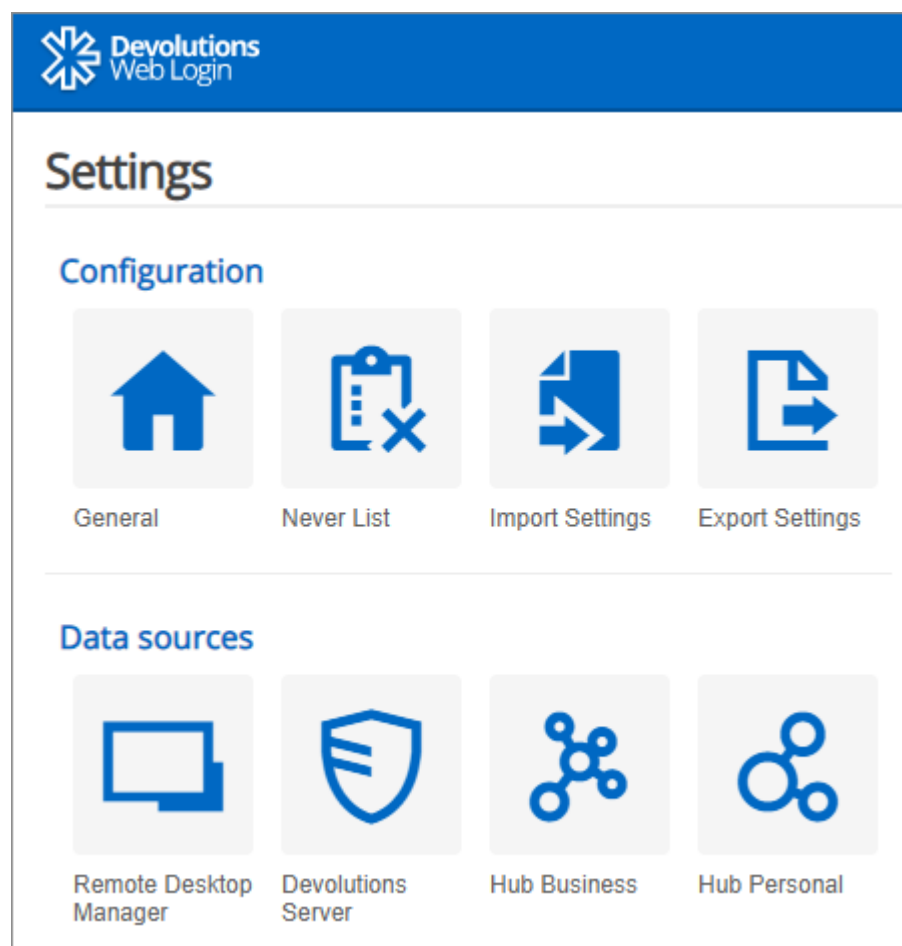
- Refine the credential list available with the **Filter** search bar.
- **Add Website** from Devolution Web Login in a specific folder located in a vault or your User Vault.
- **Visualize the credential** stored in the vaults if you are connected with Devolutions Server or Password Hub.

- Browse **Recent** entry or **Favorites**.
- Use the **Password generator** to create custom and more secure credentials.
- Set Devolution Web Login [Settings](#).

7.4.1.1 Settings

DESCRIPTION

Devolution Web Login settings are separated in two categories, [Configuration](#) and [Data sources](#).



Devolution Web Login Settings

CONFIGURATION

The **General** settings are about the user interface and interaction.

- Show Devolution Web Login extension icon in the credentials fields.
- Show the prompt when saving credentials on new login.
- Show the context menu options.
- Color the fields that are filled with Devolution Web Login
- Set the color **Theme** of the application.
- Disable the analytics telemetry in the **Advanced** setting.

The **Never list** displays the list of websites, added locally, to which the user will never be prompted to save credentials.

- Type can range from: **Never add site, Never autofill, Never do anything to Never show icons in fields.**
- Matching options are: **Base domains, Host, Starts with, RegEx** and **Exact.**

The **Import / Export Settings** allows to save and transfer your currently set preferred settings.

- Import setting from other browsers or users.
- Choose to export Devolution Web Login **Settings, Password Generator** template and the **Never List.**

DATA SOURCES

The data sources settings are used to customize Devolution Web Login interactions with [Remote Desktop Manager](#), [Devolutions Server](#) and [Password Hub](#) Business or Personal.

REMOTE DESKTOP MANAGER

GENERAL OPTIONS	DESCRIPTION
Enable Remote Desktop Manager app	Retrieve entries from Remote Desktop Manager when the application is open.

GENERAL OPTIONS	DESCRIPTION
Use default port (19443)	Communicate with the default port 19443 between the application.
Add entry in User Vault by default	Save new entries in the User Vault.
Destination folder	Choose the folder where the credentials are stored in the vault.

ACTION OPTIONS	DESCRIPTION
Automatically retrieve credentials on page load	<p>Devolution Web Login automatically search for credentials in the data source when connecting to a website.</p> <p>If disabled, click on the Devolution 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 Devolution Web Login.</p> <p>Navigate to File - Options - Browser Extensions in Remote Desktop Manager to set the application key.</p>

ADVANCED OPTIONS	DESCRIPTION
Enable native messaging	Exchange messages with a native application installed on the user's computer.
Use legacy API	Use the old browser extension API for compatibility with older versions of Remote Desktop Manager.

DEVOLUTIONS SERVER

GENERAL OPTIONS	DESCRIPTION
Enable Devolutions Server	Retrieve entries from Devolutions Server.
Destination folder	Choose the folder where the credentials are stored in the vault.
Server URL	Enter the URL of the Devolutions Server instance to connect to.

ACTION OPTIONS	DESCRIPTION
Automatically retrieve credentials on page load	<p>Devolution Web Login automatically search for credentials in the data source when connecting to a website.</p> <p>If disabled, click on the Devolution 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
Default compare type	Set a default comparing option type.
Sync all available vaults	Enable to synchronize all the available vaults from Devolutions Server.

PASSWORD HUB BUSINESS AND PERSONAL

GENERAL OPTIONS	DESCRIPTION
Enable Password Hub	Retrieve entries from Password Hub.
Server URL (Business only)	Enter the URL of the Password Hub instance to connect to.

ACTION OPTIONS	DESCRIPTION
Automatically fill in credentials on load	Fill automatically the credentials when loading a web page.
Automatically submit the form after filling	Submit the credentials automatically when the fields are filled

ADVANCED OPTIONS	DESCRIPTION
Devolutions Account login	Set your Devolutions Account login URL.
Show favicon	Display the Devolution Web Login favicon.
Default compare type	Set a default comparing option type.
Sync all available vaults (Business only)	Enable to synchronize all the available vaults from Devolutions Server.

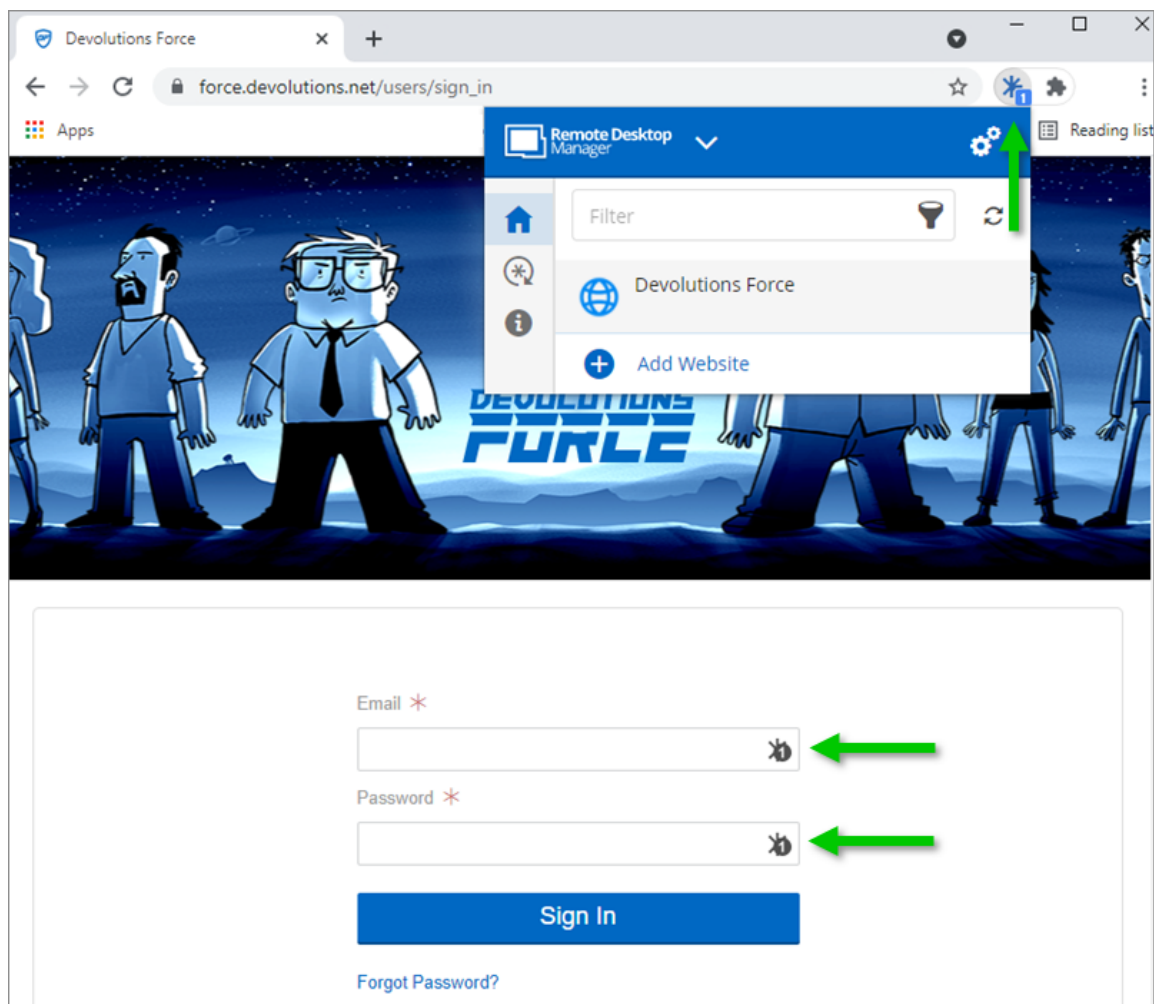
7.4.2 Retrieve Credentials

DESCRIPTION

Once configured in your Devolutions product, credentials are automatically detected by **Devolution Web Login** when connected to their respective applications.

LOG IN TO A WEBSITE

Select an entry from the list in Devolution Web Login or click on the icon in the credential field of the browser to fill in the login information and connect to the website.



Automatic Log In

7.4.3 Secure Devolutions Web Login

DESCRIPTION

In Remote Desktop Manager version 2021.1 and higher, we changed how our browser extension, Devolution 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 Devolution 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 Devolution 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 Devolution Web Login calling on that port will get the responses unless an application key is set. Follow this [link](#) for the steps.

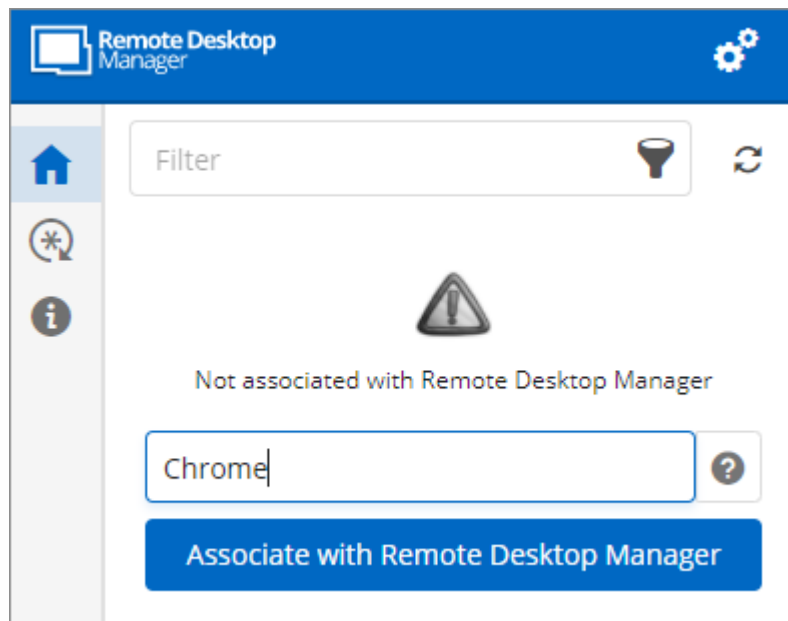
HOW TO SET UP DEVOLUTION WEB LOGIN FOR VERSION 2021.1 AND HIGHER



An application key is mandatory if you are using Devolution Web Login on a Terminal server. Please follow the steps describe [here](#).

When you will first open Devolution 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.



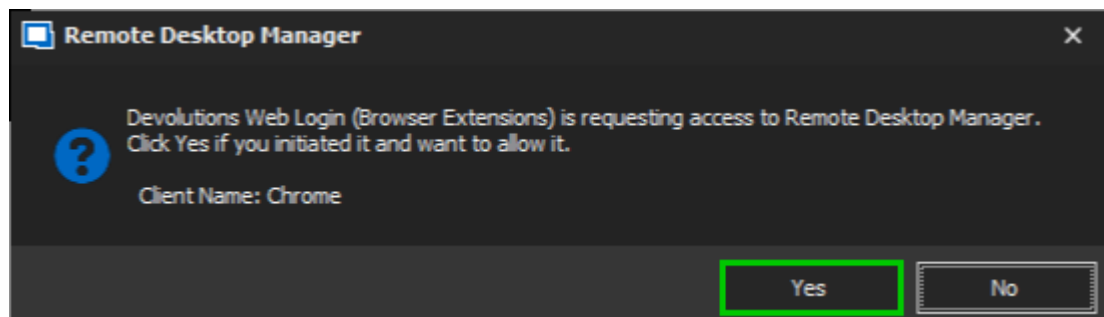
This can be used to identify a particular association and to deny access to it from Remote Desktop Manager. The default name is the name of the web browser running Devolution Web Login.

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), Devolution Web Login can only be paired to a single instance of RDM at any time.

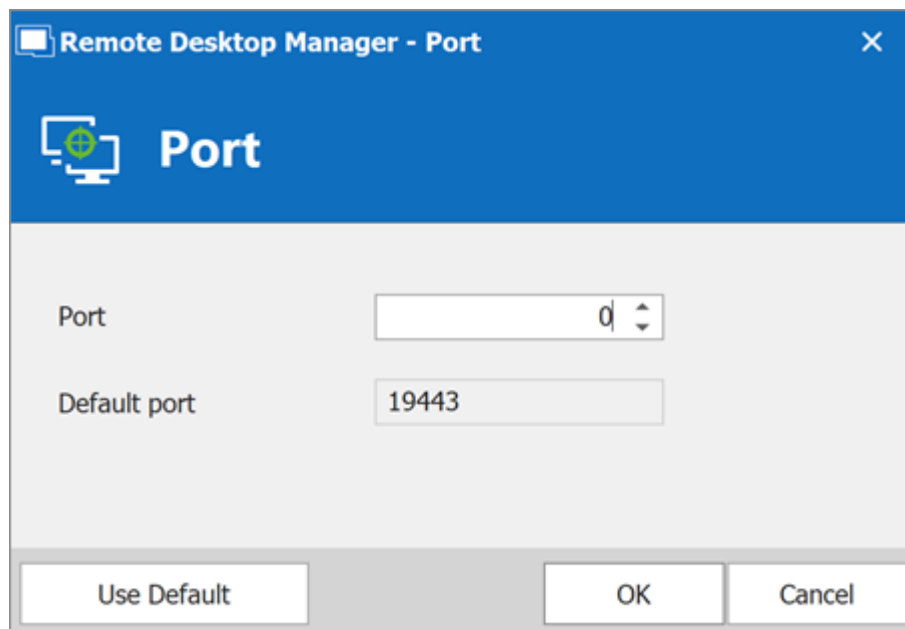
HOW TO SET UP DEVOLUTION WEB LOGIN FOR VERSION LOWER THAN 2021.1 AND FOR TERMINAL SERVER



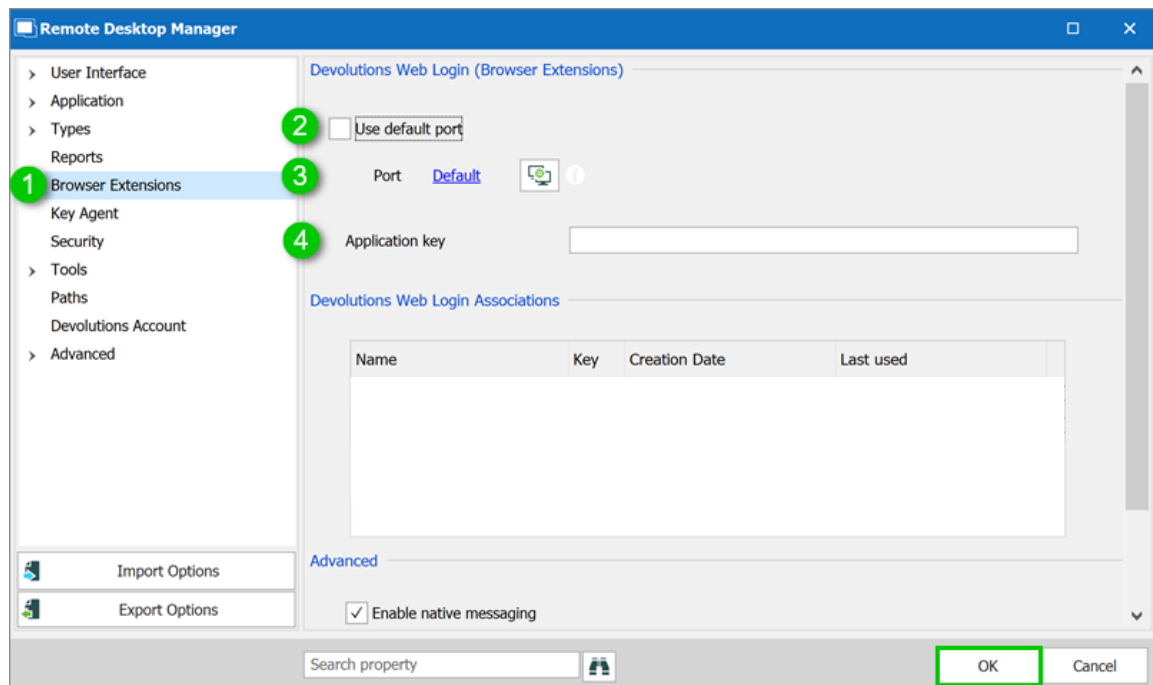
The application key is displayed in clear text, it must be kept secret by the user.

To enable the security layer in Remote Desktop Manager, follow these steps:

1. Navigate to **File - Options - Browser Extensions**.
2. Uncheck **Use default port**.
3. Click **Default** to enter a custom port and **OK** when done.

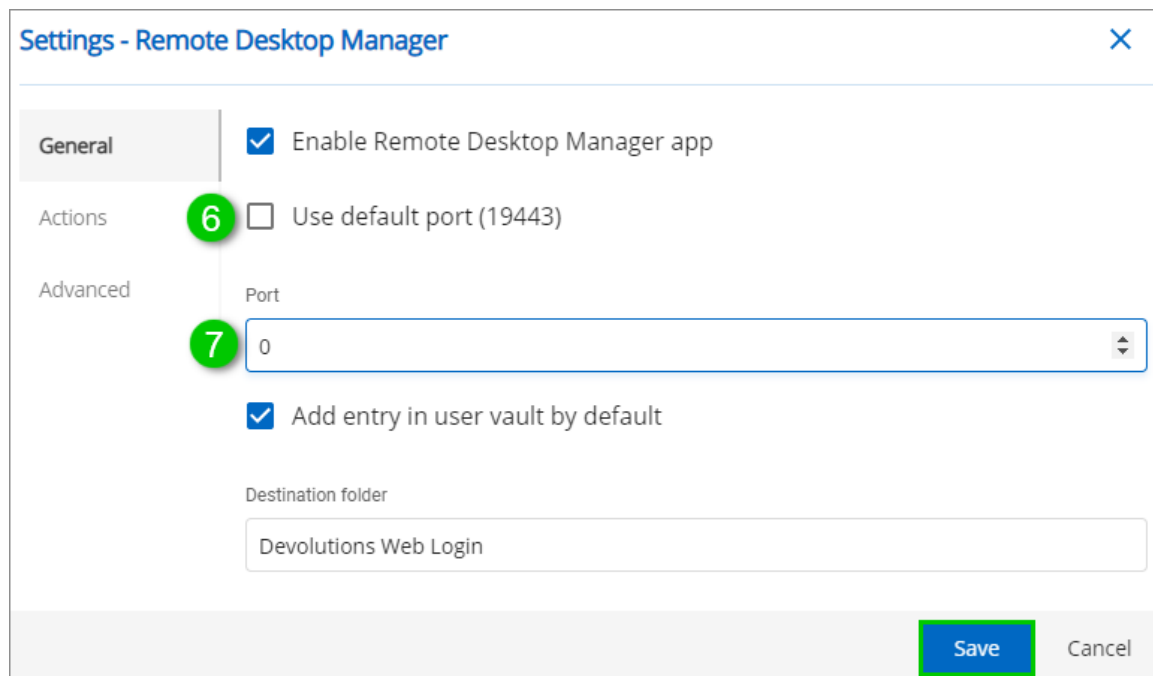


4. Type an **Application key** then click **OK** to save.

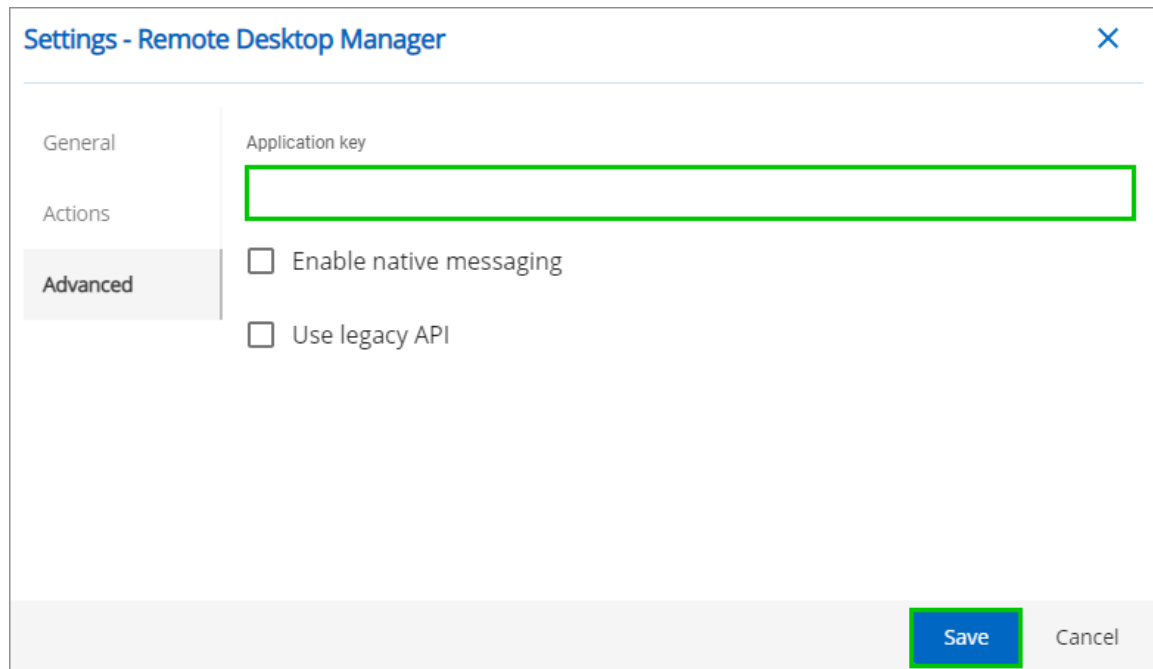


Remote Desktop Manager Browser Extensions Options

5. In your browser, click the Devolution Web Login icon * and go to **Settings - Data sources - Remote Desktop Manager**.
6. Disable **Use default port**.
7. Enter the custom port created earlier in Remote Desktop Manager and **Save**.



- Click **Advanced** and enter the same **Application key** as Remote Desktop Manager, **Save**.



Devolution Web Login Settings for Remote Desktop Manager

7.4.3.1 Unpair a Browser Extension

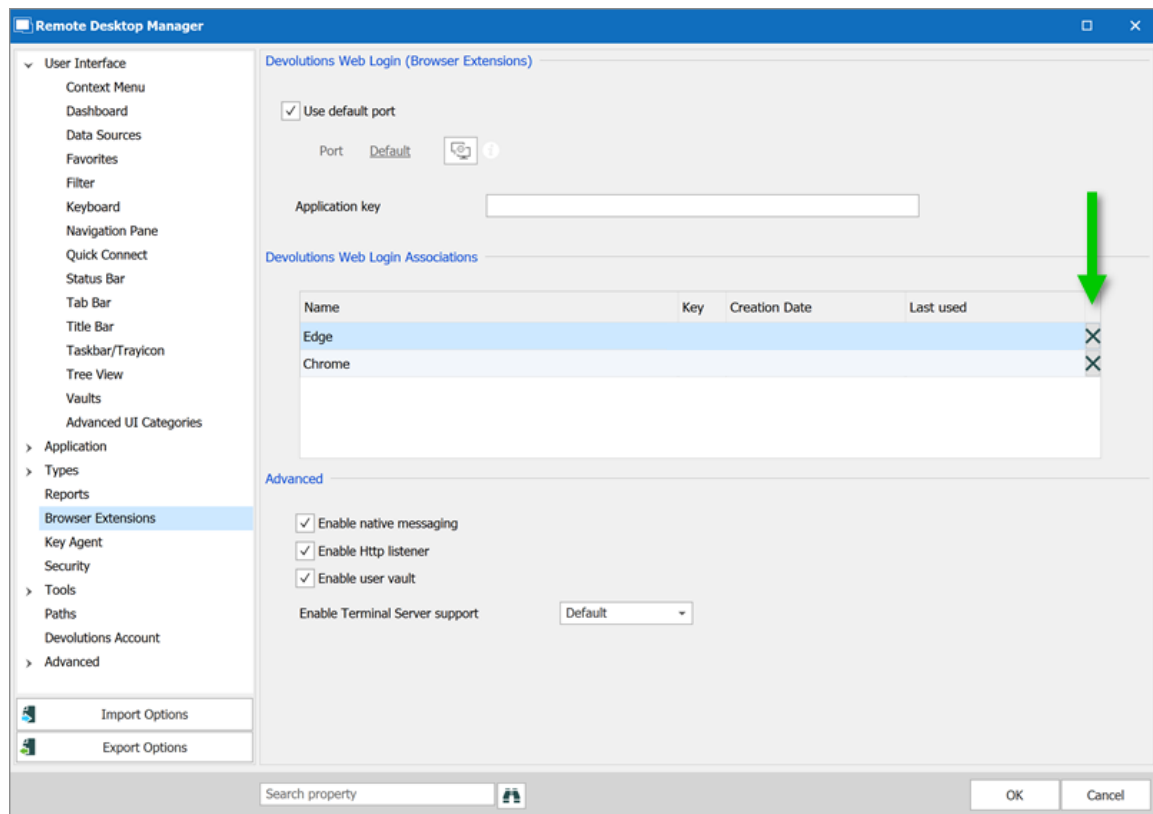
DESCRIPTION

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.

- In RDM go to **File - Options - Browser Extensions**.
- In the **Devolution Web Login Associations** section click the **X** button of the entry in the list and click **OK** to save the modifications.



In the **Devolution Web Login Associations** section, you will find a list of each association made to Remote Desktop Manager including some information to identify them. This includes the name specified at the time of association (which defaults to the web browser's name), a part of the encryption key used between the two, it's creation date and the date when it was last used.



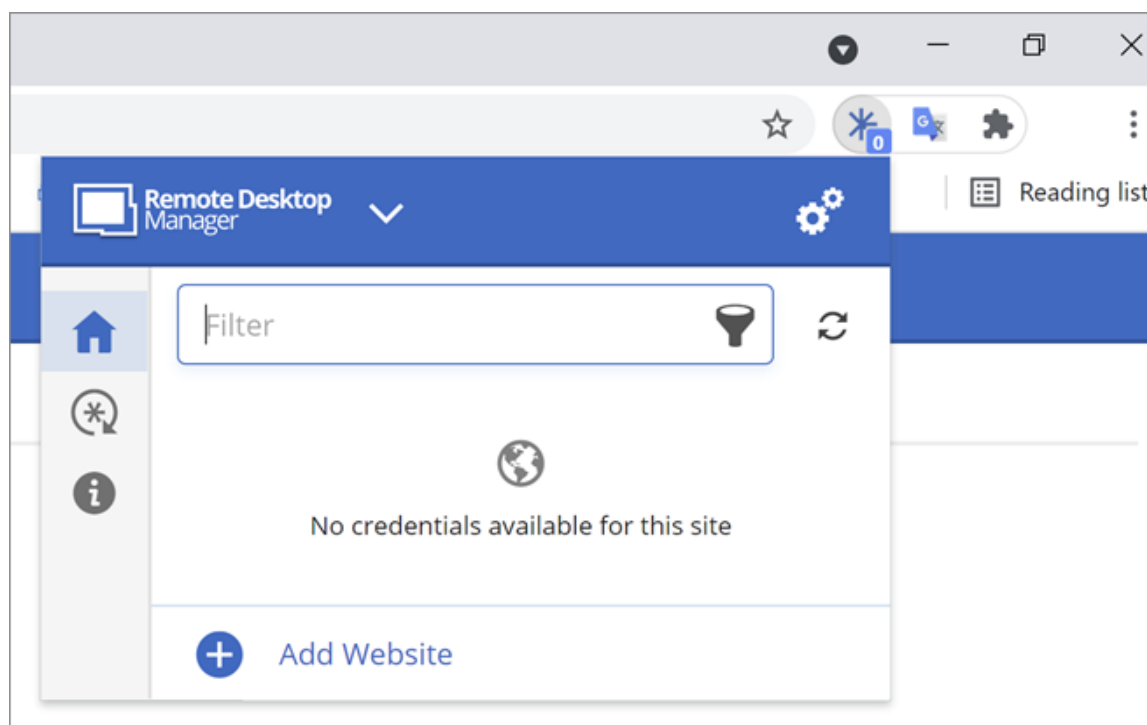
7.4.4 Keyboard Shortcuts

DESCRIPTION

Here is the list of keyboard shortcuts available for Devolution Web Login:

CTRL+SHIFT+Z


Use this key shortcut to open Devolution Web Login window in your active browser.



Devolution Web Login in Chrome

CTRL+SHIFT+Y

Use it to autofill your credential when only one is available for an entry.



**Devolutions
Server**

Log in to your account

Username *

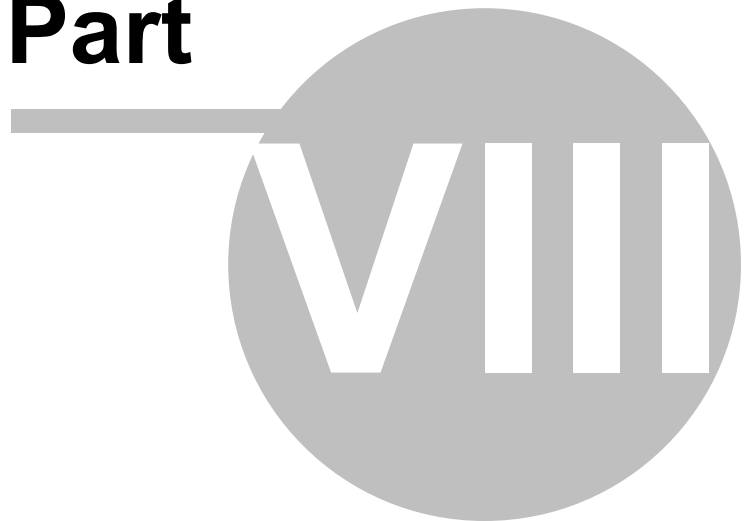
Password *

Log In

One Credential Login with Devolution Web Login

Support/Ressource s

Part



8 Support/Ressources

8.1 Technical Support

DESCRIPTION

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: service@devolutions.net

Forum: <https://forum.devolutions.net/>

Language: English-Français-Deutsch

Phone: +1 844 463.0419

EXTENDED AND PREMIUM SUPPORT PLANS

Subscribers of a paid support plan have received a plan ID. You should send your plan ID in your tickets.

Please consult our [Support Policy](#) for more information.



8.2 Lexicon

DESCRIPTION

Remote Desktop Manager is a software that has an extensive set of functionalities. Here are the major concepts that are important to understand in order to use the program to its full potential.

CONNECTION

Any type of entry that allows you to connect to a remote host, service or device is a connection. An IP address or host name is normally used as well as credentials.

CREDENTIAL ENTRY

A credential is used to control access to a resource by identifying the user. It can be a classic username/password pair held by the application or even by an external source.

DATA SOURCE

It is a container for entries. It can be a local file or a database (either local or shared). You can use multiple distinct data sources in the application, although only one is considered active at one point in time. See [Data Sources](#) for more information.

ENTRY

All items in your data source are entries. There are multiple types. The entry is an abstract concept that serves as a container for all specific types.

INFORMATION ENTRY

An information entry can contain various items like account information, emails and serial numbers. Unlike credential entries, information entries are meant to be shared. Therefore, the data in the information entries is not encrypted. Its principal use in Remote Desktop Manager is to hold web site information, from the URL to the credentials. This allows auto log in on the specified web site.

SESSION

In the early days of Remote Desktop Manager, it was mainly aimed at managing Microsoft Remote Desktop. A session was a term that was in use back then to describe a connection to Microsoft Remote Desktop Services. It appears widely in our documentation. Any technology that connects and that needs to use authentication is a session.

8.3 Tutorials

DESCRIPTION

Our tutorials are published on the [Devolutions YouTube channel](#).

Our focus is to deliver quality information as soon as possible after the release of a new or modified feature.

Please use our [forums](#) if documentation is missing or plain wrong, we will do our best to correct the situation.



Contact Us

For any questions, feel free to contact us:

Support: service@devolutions.net

Phone: +1 844 463.0419

Monday to Friday 7:30 a.m. to 6 p.m. EST

Head Office

Devolutions inc.

1000 Notre-Dame

Lavaltrie, QC J5T 1M1

Canada

**WHERE IT
MEETS SECURITY**