



Remote Connections & Passwords. Everywhere!

# User Manual

## 2020.3



# Table of Contents

<b>Part I Overview</b>	<b>11</b>
.....1...Remote Desktop Manager.....	12
.....2...Security.....	13
.....3...System Requirements.....	15
....Prerequisite Software .....	16
.....4...The Devolutions Platform.....	16
....Remote Desktop Manager Agent .....	17
....Remote Desktop Manager Jump .....	19
<b>Part II Getting Started</b>	<b>23</b>
.....1...Using Remote Desktop Manager.....	24
.....2...Checklist for Individuals.....	24
....Select the Data Source type - Individuals .....	25
.....3...Checklist for Teams.....	27
....Select the Data Source type - Teams .....	29
....Set up a team folder for default settings .....	31
.....4...Creating an Entry.....	33
.....5...Managing Credentials.....	35
<b>Part III Installation</b>	<b>37</b>
.....1...Client.....	38
....Ancillary Files .....	39
....Configuration File Location .....	41
....Custom Installer Service .....	43
....Installer File Generator.....	44
....Custom Installer Manager.....	50
....For All Users .....	58
....Portable (USB) .....	59
....Registration .....	63
....Enterprise Edition .....	64
....Free Edition.....	68
....Register from Devolutions Portal .....	72
....Trial Request.....	75
....Remote Desktop Services .....	76
.....2...Database Upgrade.....	80
.....3...Uninstall.....	81
.....4...Update.....	81
<b>Part IV User Interface</b>	<b>83</b>
.....1...Main Screen.....	84
.....2...Style.....	85

.....3	Theme	89
.....4	Top Pane	90
.....	Quick Access Toolbar	91
.....5	Navigation Pane	93
.....	Opened Sessions	95
.....	Favorite Entries	98
.....	Most Recently Used Entries	101
.....6	Content Area	101
.....	Embedded Sessions	102
.....	Dashboard	105
.....	Wake-on-LAN	107
.....7	Panes (Footer)	110
.....	Attachments	112
.....8	Status Bar	114
.....	Search/Filter	114
.....	Grab Input	117
.....9	Tray Icon	118

## Part V Data Sources 120

.....1	2-Factor Authentication	125
.....	Google Authenticator	128
.....	Yubikey	131
.....	Duo	133
.....	AuthAnvil	137
.....2	Caching	139
.....3	Create a data source	141
.....4	Data Source Types	145
.....	Advanced Data Sources	150
.....	Devolutions Online Database	151
.....	Devolutions Password Server	156
.....	MariaDB	163
.....	Microsoft SQL Azure	170
.....	Microsoft SQL Server	199
.....	MySQL	214
.....	Private Vault	222
.....	DropBox	224
.....	Google Drive	230
.....	Devolutions Online Drive	232
.....	SQLite	238
.....	WebDAV	244
.....	XML	247
.....5	Import/Export Data Source	252
.....6	Lock Data Source	254
.....7	Offline mode	255
.....	Offline Read/Write	259
.....8	Manage Cache	263
.....9	Private Vault	265
.....	Private Vault Search	266

<b>Part VI Commands</b>	<b>269</b>
.....1...Context Menu.....	270
.....Open with Parameters .....	271
.....Documentation .....	272
.....Editor.....	273
.....Entry History .....	282
.....2...File.....	285
.....Go Offline/Online .....	289
.....My Data Source Information .....	290
.....Devolutions Account .....	294
.....Backup .....	296
.....Settings.....	296
.....Restore.....	299
.....Refresh .....	302
.....Change Master Key .....	302
.....Data Sources .....	303
.....Background Services .....	306
.....Import .....	307
.....Import Computer Wizard.....	310
.....Import Session CSV Wizard.....	316
.....Import Network Scan.....	320
.....Import Sessions.....	321
.....Import Logins.....	322
.....Import Contacts.....	323
.....Export .....	325
.....Encrypted Html.....	328
.....Options .....	330
.....Advanced .....	332
.....Import Options.....	337
.....Export Options.....	339
.....My Account Settings .....	342
.....My Personal Credentials.....	344
.....User Specific Settings List.....	346
.....Templates .....	348
.....Creating Templates.....	353
.....Default Settings.....	359
.....Password Templates.....	361
.....3...Home.....	366
.....4...Actions.....	366
.....Commands .....	371
.....RDP .....	371
.....VNC .....	372
.....SSH Shell (Rebex).....	373
.....Telnet.....	375
.....5...Edit.....	377
.....Entries .....	382
.....Checkout system.....	382
.....Credential Redirection.....	387
.....Dynamic Credential Linking.....	392
.....Edit .....	395
.....Play List.....	395



.....Setting Overrides .....	403
.....Specific Settings .....	403
.....Batch .....	406
.....Batch Edit .....	406
<b>.....6...View .....</b>	<b>410</b>
.....Panels .....	413
.....Task List .....	413
.....View .....	416
.....Activity Logs .....	416
.....Advanced Search .....	418
.....Documentation Search .....	421
<b>.....7...Administration .....</b>	<b>424</b>
.....Management .....	427
.....User Management .....	427
.....Role Management .....	440
.....Reports .....	441
.....Reports .....	441
.....Deleted Entries .....	446
.....Settings .....	449
.....Root (Settings) .....	449
.....System Settings .....	450
.....System Permissions .....	465
.....Security Providers .....	470
.....Clean up .....	476
.....Clean Up Deleted History .....	476
.....Clean Up Entry History .....	478
.....Clean Up Activity Logs .....	480
.....Pack Data Source (Optimize) .....	482
<b>.....8...Tools .....</b>	<b>483</b>
.....Generators .....	485
.....Password Generator .....	485
.....SSH Key Generator .....	493
.....Certificate Generator .....	495
.....Port Generator .....	498
.....Tools .....	500
.....Devolutions Localizer .....	500
.....Password Analyzer .....	502
.....Key Agent Manager .....	504
.....PowerShell (RDM CmdLet) .....	511
.....Wayk Now .....	512
.....More Tools .....	513
<b>.....9...Help .....</b>	<b>535</b>
.....Support .....	537
.....Application Log .....	537
.....Diagnostic .....	540
.....Profiler .....	544
.....Record .....	547
<b>Part VII Devolutions Web Login .....</b>	<b>548</b>
<b>.....1...Overview .....</b>	<b>549</b>
<b>.....2...Installation .....</b>	<b>550</b>
.....Chrome .....	551

.....Firefox .....	552
.....Microsoft Edge Beta .....	554
.....Opera .....	558
<b>.....3...First Login.....</b>	<b>559</b>
.....Password Hub .....	559
.....Multiple Password Hub.....	563
.....Password Server .....	569
.....Remote Desktop Manager .....	572
<b>.....4...Exploring Devolutions Web Login.....</b>	<b>574</b>
.....Menu .....	574
.....Settings.....	574
.....Retrieve Credentials .....	579
.....Remote Desktop Manager.....	580
.....Secure Devolutions Web Login .....	581
.....Keyboard Shortcuts .....	583

## **Part VIII Role Based Access Control 586**

<b>.....1...Permissions.....</b>	<b>596</b>
<b>.....2...Scenarios.....</b>	<b>598</b>
.....Simplified Security .....	598
.....Advanced Security .....	607
<b>.....3...Legacy Information.....</b>	<b>620</b>
.....Small to Medium Enterprise .....	620

## **Part IX PowerShell Scripting 632**

<b>.....1...Tips and tricks.....</b>	<b>634</b>
<b>.....2...PowerShell Samples.....</b>	<b>636</b>
.....Batch Actions Samples .....	636
.....Change your Synchronizer source .....	641
.....Creating an entry .....	644
.....Creating Group Folder Structure from CSV file .....	645
.....Custom Export to CSV .....	646
.....Extract TeamViewer ID .....	647
.....Remote Management .....	647
.....Script Execution Policy .....	648

## **Part X Knowledge Base 649**

<b>.....1...Protocols and application.....</b>	<b>650</b>
.....Remote Desktop Manager .....	650
.....Events.....	650
.....Wake-on-LAN.....	659
.....Add a web link in Macros/Scripts/Tools Session .....	663
.....Configure VPN for multiple sessions .....	664
.....Import Credentials From Keepass .....	670
.....Import and Export.....	676
.....Multiple Types of Connections to a single computer.....	680
.....Pwned Password Check.....	688
.....Vaults Overview.....	692
.....Quick Connect.....	702
.....Send application logs.....	704

..... Send error report .....	707
..... Upgrade from Free Edition to Enterprise Edition .....	710
..... Understand Remote Desktop Manager licensing .....	712
..... Web protocol handler .....	714
..... Create a saved search with Smart Folders .....	718
..... Add an RDP entry .....	719
..... Quick Start .....	720
..... SQL Server Always On Availability Groups .....	722
..... <b>Remote Desktop Manager Jump</b> .....	<b>723</b>
..... Configure Remote Desktop Manager Jump .....	723
..... <b>RDP</b> .....	<b>728</b>
..... Restoring the rdp file association with mstsc.exe .....	728
..... <b>SSH</b> .....	<b>729</b>
..... Configure an SSH Tunnel .....	729
..... <b>VMware</b> .....	<b>729</b>
..... Configuring VMware's PowerCLI for use by Remote Desktop Manager .....	729
..... <b>Tips and tricks</b> .....	<b>730</b>
..... Use Multiple Versions of a Third Party Application .....	730
..... Sending Windows Credentials inside TeamViewer .....	731
..... <b>2...Performance</b> .....	<b>736</b>
..... Memory Tuning Of RDP Sessions .....	736
..... <b>3...Security</b> .....	<b>738</b>
..... Blocking MS RDP to Only Use Remote Desktop Manager .....	738
..... Certificate validation .....	739
..... Windows Credential Manager .....	746

## Part XI Technical Support 748

## Part XII Support/Resources 750

..... <b>1...Keyboard Shortcuts</b> .....	<b>751</b>
..... <b>2...Command Line Arguments</b> .....	<b>756</b>
..... <b>3...Lexicon</b> .....	<b>758</b>
..... <b>4...Follow Us</b> .....	<b>760</b>
..... <b>5...Best Practices</b> .....	<b>761</b>
..... Credential Management For Teams .....	761
..... Use Credential Entries .....	765
..... Use VPN Entries .....	765
..... <b>6...How-To</b> .....	<b>766</b>
..... How to Add a Web Link in Macros/Scripts/Tools Session .....	766
..... How to apply policies .....	771
..... How to Backup Remote Desktop Manager .....	781
..... How to Configure Password Manager Pro in Remote Desktop Manager .....	781
..... How to Configure ConnectWise (ScreenConnect) 5 in Remote Desktop Manager .....	787
..... How to Configure the Google Authenticator 2-Factor Authentication .....	791
..... How to Configure the Yubikey 2-Factor Authentication .....	793
..... How to Disable Remote Desktop Manager Auto Update .....	795
..... How to Download the Keepass Plugin .....	796
..... How to Register Licenses in Older Version .....	798
..... How to Reinstall Remote Desktop Manager .....	799
..... How to Send an Error Report .....	800
..... How to Send a File Securely .....	802

.....How to Send the Application Logs Report .....	803
.....How to Send your Configuration File .....	805
.....How to Setup a SSH Tunnel .....	805
.....    How to Broadcast Action in SSH.....	812
.....How to Setup Remote Desktop Manager to Receive New Update .....	813
.....Setup the Usage of the Session Credentials to Launch a Tool .....	814
.....How to Subscribe to the Announcements Forums .....	815
.....How to Use a Typing Macro to Perform Authentication .....	816
.....How to use the Theme system .....	819
.....    Image List .....	820
<b>.....7...Tips And Tricks.....</b>	<b>836</b>
.....    Allow Open Multiple Connections .....	837
.....    Automating Remote Microsoft Management Console (MMC) .....	837
.....    Create a list of credentials .....	840
.....    Creating Shortcuts .....	843
.....    Data Migration .....	845
.....    Data Report .....	852
.....    Edit Hosts File .....	855
.....    Handling RDP Connections .....	859
.....    HTML Export Using Symmetric Encryption .....	860
.....    Keep Tabs Opened .....	861
.....    Open RD Gateway Only when Unable to Ping Host .....	863
.....    Passcode Prompt When Opening an Entry .....	864
.....    RDP Session Time Limits .....	866
.....    Remote Install with PSEXEC .....	870
.....    Run as Another User .....	871
.....        Built-in RunAs.....	872
.....        Manual RunAs.....	879
.....    Running Remote Desktop Manager as Another User .....	887
.....    SQL Server Data Source with Integrated Security .....	888
.....    SQL Server Maintenance Plans .....	895
.....    Tab Groups .....	896
.....    Team Tips .....	898
.....    Testing variables .....	901
.....    Use Different Version of Same Application .....	902
.....    VPN .....	902
.....        VPN Group.....	902
.....        VPN Routing.....	903
<b>.....8...Troubleshooting.....</b>	<b>905</b>
.....    1Password .....	905
.....    2-Factor Authentication .....	905
.....    Apple Remote Desktop .....	907
.....    BeyondTrust .....	908
.....    Clipboard .....	909
.....    Corrupted System File .....	910
.....    Data Recovery .....	910
.....    Data Sources .....	911
.....        Database Schema.....	913
.....        Devolutions Online Database.....	916
.....        MySQL.....	917
.....        SQL Azure.....	919
.....        SQL Server.....	921
.....    DB Upgrades .....	927

..... <b>FIPS (Encryption)</b> .....	<b>927</b>
..... <b>KeePass</b> .....	<b>928</b>
..... <b>LogMeIn</b> .....	<b>929</b>
..... <b>Microsoft Office</b> .....	<b>930</b>
..... <b>Microsoft RDP</b> .....	<b>931</b>
..... Automatic Logon .....	936
..... Cannot Store Password on Local Computer .....	942
..... Display Issues .....	943
..... Keyboard not working .....	945
..... Licensing Protocol Error .....	945
..... Logoff Access Denied .....	947
..... Logoff Issue .....	948
..... Memory and Performance issues .....	949
..... Missing mapped drives .....	952
..... Printer Redirection .....	953
..... Protocol Error .....	954
..... RDP Session Credentials .....	956
..... Remote Computer Requires Authentication to be Enabled Error .....	958
..... Reconnect .....	959
..... RD Gateway Credentials Prompt When Trying To Reconnect .....	960
..... RDM Hangs when logging off RDP sessions .....	961
..... Sessions work using mstsc.exe but not in RDM .....	963
..... <b>Network Devices</b> .....	<b>964</b>
..... <b>Non-Admin Users Cannot View Passwords</b> .....	<b>965</b>
..... <b>Password Manager Pro</b> .....	<b>966</b>
..... <b>Performance</b> .....	<b>969</b>
..... Data sources .....	969
..... Diagnostic .....	970
..... Startup .....	974
..... <b>Powershell</b> .....	<b>975</b>
..... <b>Putty</b> .....	<b>978</b>
..... <b>Remote Desktop Manager</b> .....	<b>979</b>
..... Application Requires DPS Version Greater or Equal .....	980
..... Caching .....	982
..... Debugging .....	983
..... High CPU Usage .....	985
..... HDPI Scaling Issues .....	986
..... Hung Remote Desktop Manager .....	989
..... Large Memory Aware Application .....	991
..... Missing Navigation Pane .....	993
..... Missing Sessions .....	994
..... Offline Mode .....	995
..... Profiler .....	996
..... Proxy Authentication Required Error .....	996
..... Red X in Navigation Pane or Credential List .....	997
..... Root Is Empty Error .....	997
..... Session Focus Issue .....	999
..... SQL Server Data Source Connection Refused .....	1000
..... Startup performance .....	1000
..... Unable to install or upgrade .....	1003
..... Unable to Uninstall .....	1003
..... Upgrade .....	1004
..... User Interface .....	1004
..... Version Compatibility for RDM and DPS .....	1006

.....RPC .....	1007
.....Secret Server .....	1008
.....Secure Note .....	1009
.....Session Tools .....	1010
.....SSH .....	1011
.....Synchronizers .....	1012
.....Active Directory Synchronizer.....	1012
.....VMWare .....	1013
.....Advanced Troubleshooting of the PowerCLI.....	1018
.....VPN .....	1020
.....Missing Opened VPN from List .....	1020
.....FortiClient.....	1020
.....Sonicwall Global VPN Client.....	1021
.....Microsoft VPN.....	1022
.....Cisco AnyConnect.....	1023
.....Web Browsers .....	1024
.....Internet Explorer .....	1024
.....Google Chrome.....	1027
.....Firefox.....	1028
.....Web Authentication.....	1029
.....WebDav .....	1033
.....Web traffic .....	1034
.....Welcome Page .....	1035
.....WMI .....	1037
..... <b>9...Tutorials</b> .....	<b>1038</b>
.....Overview .....	1039
.....Getting Started .....	1040
.....Spotlight On... .....	1041

# Overview

---

Part I



# 1 Overview

## 1.1 Remote Desktop Manager



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

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

## THE REMOTE DESKTOP MANAGER ECOSYSTEM

Remote Desktop Manager is available in two editions:

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

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



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



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

Platform	Free Edition	Enterprise Edition
Windows	✓	✓
macOS	✓	✓
iOS		✓ (Free App)
Android		✓ (Free App)

## 1.2 Security

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

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

### U.S. FEDERAL GOVERNMENT APPROVED ENCRYPTION

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

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

## TIPS



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



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

We recommend you follow these steps to ensure security:

- Use an [Advanced Data Source](#) and grant user access by assigning permissions.
- Use encrypted communication with the database when available.
- Use the [Data Source Settings \(System Settings\)](#) to control settings impacting security.
- Use the [Security Provider](#) to encrypt entries completely instead of just the password.
- If using the offline mode, add your own password to add an additional layer of protection to the local cache. Go to ***File – Options – Security***.
- Require a password to launch the application, and even better: require two factor authentication. ***File – Options – Security***.
- If your data source supports it, choose not to save password in the data source, which will prompt for the credentials on the first connection.
- Use our policies to enforce some of these settings at the system level.

## 1.3 System Requirements

Remote Desktop Manager requires the following prior to installation:

### MINIMUM REQUIREMENTS

#### Windows Desktop:

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

#### Windows Server:

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

Microsoft .NET Framework 4.7.2

1 GHz or faster processor

512MB RAM

1024 x 768 screen resolution

500+ MB hard drive space

### 64-BIT SUPPORT

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

## REMOTE DESKTOP SERVICES AND THIN CLIENT SUPPORT

Remote Desktop Manager can be installed on [Remote Desktop Services](#) and thin client.

## MANUAL/PORTABLE DEPLOYMENT

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

### 1.3.1 Prerequisite Software

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



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

## SETTINGS

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

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

## 1.4 The Devolutions Platform

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

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

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

APPLICATIONS	DESCRIPTION	INSTALLATION
	documents and shared information.	iOS, Android
<a href="#"><u>Remote Desktop Manager Agent</u></a>	Tool used to run commands on remote systems. It listens for commands from a master Remote Desktop Manager. It resolves a lot of issues brought on by remote management, in particular removing the need to use Microsoft's WinRM and managing lists of <i>TrustedHosts</i> .	Windows
<a href="#"><u>Remote Desktop Manager Jump</u></a>	Feature that uses the Remote Desktop Manager Agent to launch any of our supported technologies on a remote Windows Host. It transforms it in what is called alternatively a Jump Server, or Bastion Server, or Service Host.	Windows
<a href="#"><u>Devolutions Password Server (DPS)</u></a>	Enterprise Grade data store for creating a centralized database for your team. Integrates with AD to drastically reduce time spent on managing permissions. It is installed on-premises and offers many advanced features.	Windows
<b>Devolutions Web Login (DWL)</b>	Web browser extension technology that interacts with our Remote Desktop Manager and Password Vault Manager desktop applications to obtain credentials and automatically fill authentication fields in your browser.	Windows, macOS

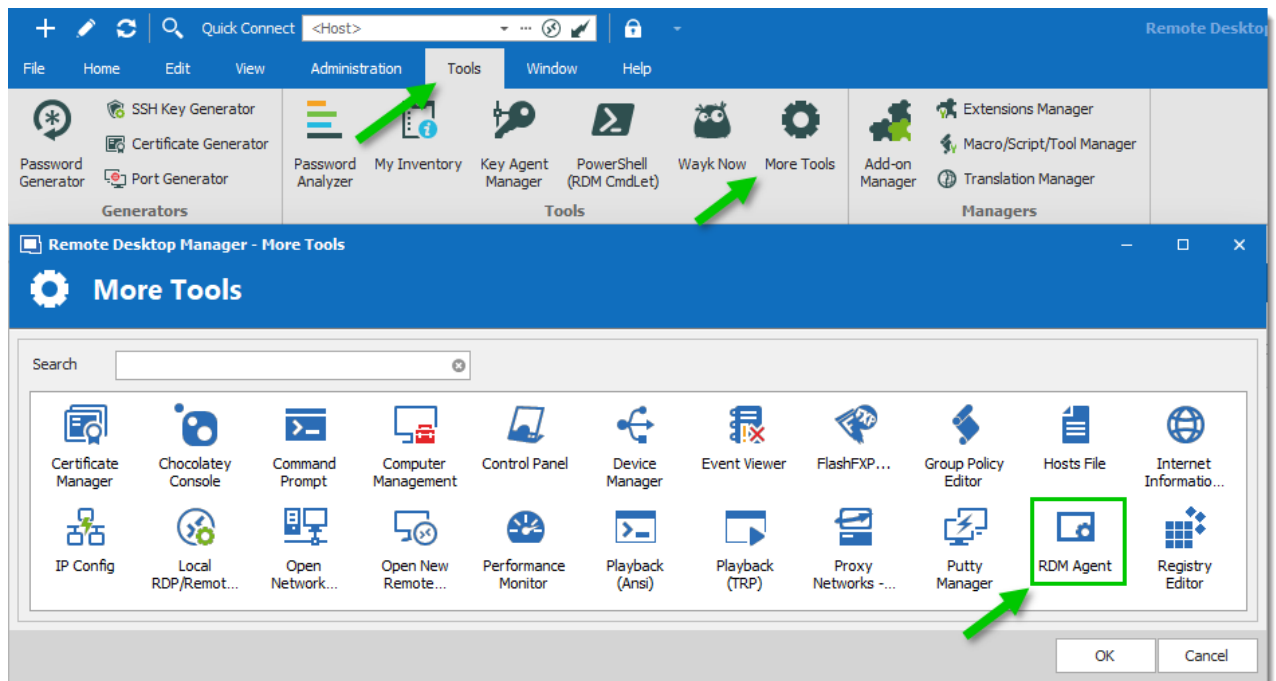
### 1.4.1 Remote Desktop Manager Agent



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

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

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



*RDM Agent*

## SCENARIOS

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

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

## INSTALLATION

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





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

1. Install Remote Desktop Manager and select Tools – More Tools – RDM Agent. It will launch and auto-register the Agent to automatically start with Windows.
2. Download Remote Desktop Manager Agent from <https://remotedesktopmanager.com/Home/Download>, and install the agent on the remote computer.
3. Copy the files Devolutions.Utils.dll, Devolutions.Windows.Utils.dll and RDMAgent.exe from the installation folder of the Remote Desktop Manager version that is used by your team, or download the zip file containing those files at <https://remotedesktopmanager.com/Home/Download> and deploy them on the remote host in the folder of your choice.
4. Via Chocolatey at <https://chocolatey.org/packages/rdmagent>.

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

*Chocolatey command line*

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

- Remote Desktop Manager on the remote host does not require a data source, it's an empty shell.
- The logging of the activity is brought back to your data source.
- Every technology supported by Remote Desktop Manager can be used remotely.

## 1.4.2 Remote Desktop Manager Jump

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

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



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



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

## HOW DOES IT WORK?

[Watch Video](#)

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

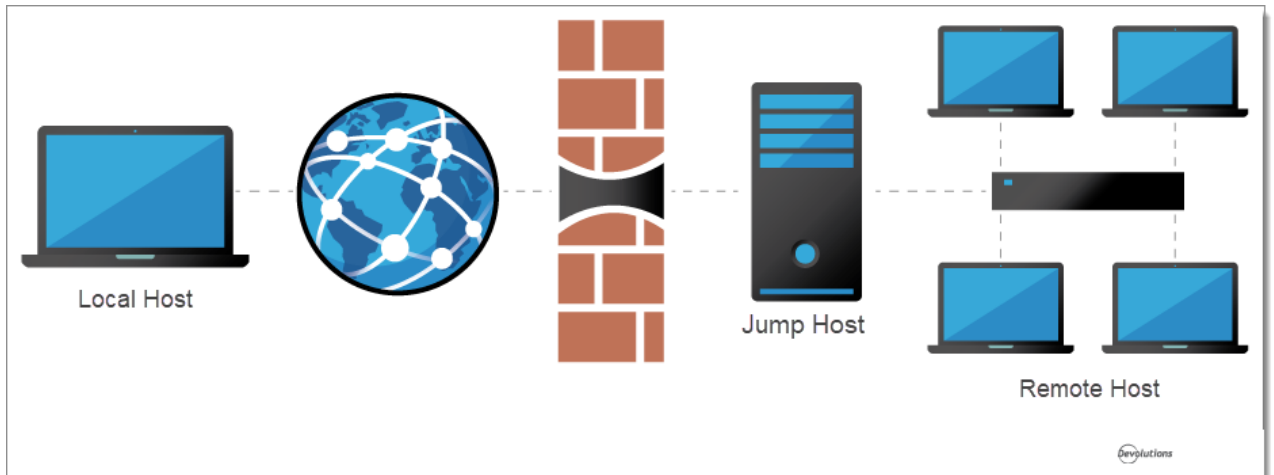
Please consult the Configure Remote Desktop Manager Jump topic.

## USAGE SCENARIOS

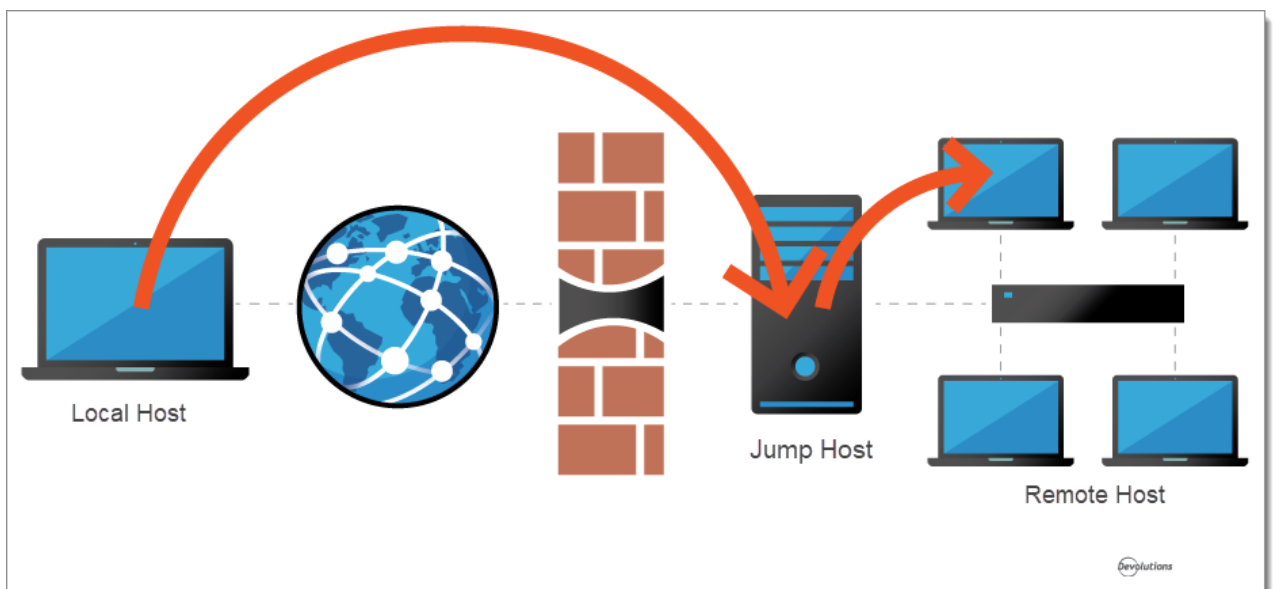
There are two targeted scenarios:

### 1. ACCESSING A SECURE NETWORK THROUGH A SINGLE HOST

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



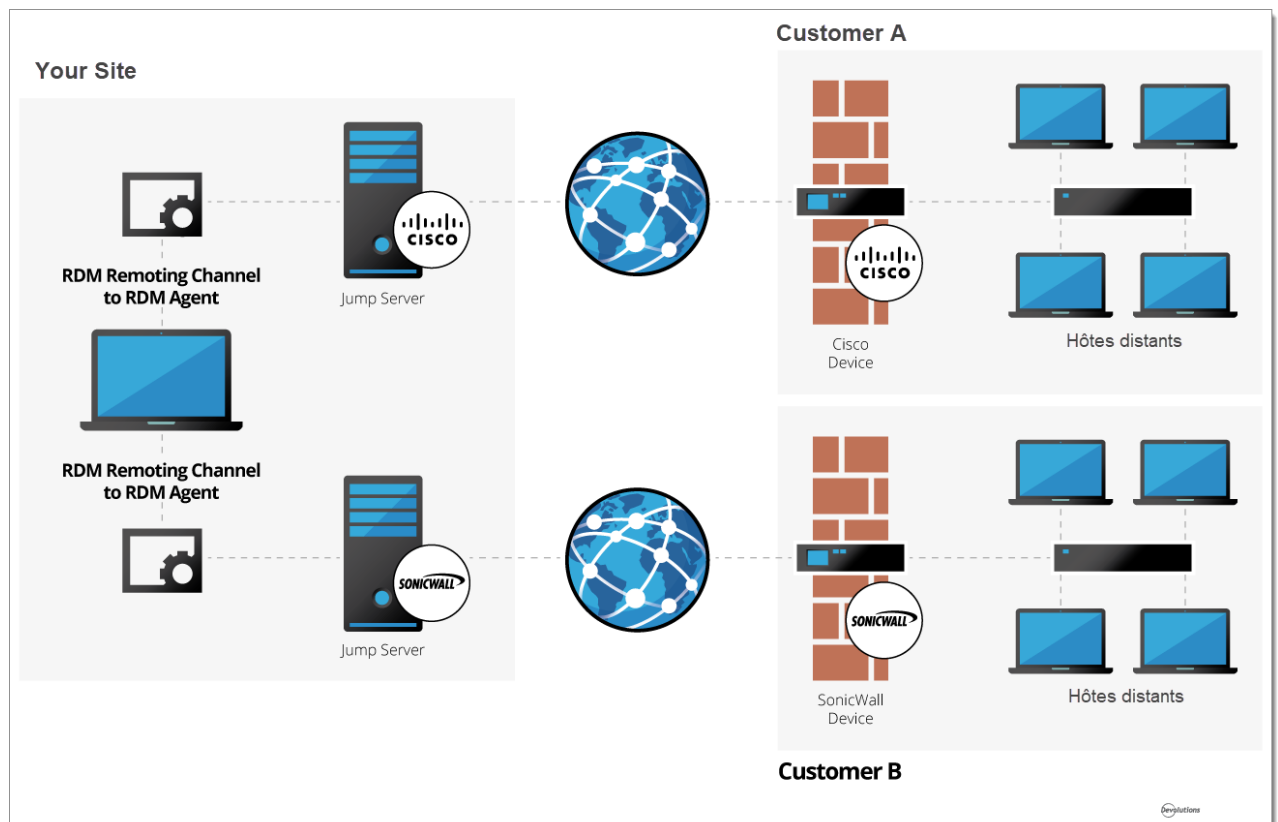
You need to access the remote hosts, but you want to limit risks and expose only the jump host to the internet traffic. This allows you to create strict firewall rules and to open only a single port. Therefore, it forces you to connect to the jump host before hopping to a remote host.



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

## 2. WORKAROUND LIMITATIONS OF SOME VPN CLIENTS

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



*Remote Desktop Manager Jump to handle incompatible VPN clients*

# Getting Started

---

Part II

## 2 Getting Started

### 2.1 Using Remote Desktop Manager

#### DESCRIPTION

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

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

### 2.2 Checklist for Individuals

Please follow these simple steps to get started with Remote Desktop Manager for **individuals** or for teams of **three users or less that do not want to implement security**.

CHECKLIST FOR INDIVIDUALS (ENTERPRISE EDITION)	
Step 1 - <a href="#">Register your license serial</a> .	
Step 2 - <a href="#">Choose a data source type (individuals)</a> .	
Step 3 - Set up your data source with a master key or encryption.	
Step 4 - Set up your Devolutions Online Backup with <a href="#">Devolutions Account</a> .	
Step 5 - <a href="#">Create your Default Settings</a> .	
Step 6 - <a href="#">Import your data</a> .	

#### REGISTER REMOTE DESKTOP MANAGER

Remote Desktop Manager Enterprise Edition grants you a 30 day trial. Refer to the procedure in the [Registration Enterprise Edition](#) topic to register your license key. If you decide not to register by the end of the 30 day trial, your

data will not be altered or erased, and you will have full access to it once you provide a license key. Please consult our [Free Edition](#) or [Enterprise Edition](#) topic to register.

## CHOOSE YOUR DATA SOURCE TYPE



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

Upon first launch, Remote Desktop Manager uses an SQLite data source. The data sources are elaborated further in the [Data Sources](#) overview topic. Consult [Choosing your data source \(Individuals\)](#) for help selecting a data source.

## SET UP YOUR DEVOLUTIONS ONLINE BACKUP

The [Online Backup](#) allows you to securely backup your information for the following data sources: [Devolutions Online Drive](#), [SQLite](#), [XML](#) and Microsoft Access. 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. If using another type of data source, please consult our Backup Best Practices topic to use the best solution for your chosen data source.

## CREATE YOUR DEFAULT SETTINGS

In **File - Templates - [Default Settings](#)**, you will be able to create, edit or reset your default settings when a new entry is created. Each entry type is supported and can have a default template defined to fit your requirements.

## 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 easy steps.

### 2.2.1 Select the Data Source type - Individuals

This topic is for individuals or for teams of **three users or less** that do not want to implement security.

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





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

DATA SOURCE	LOCAL	SELF-HOSTED	CLOUD BASED	SHARED BETWEEN YOUR COMPUTERS	WORKS OFFLINE	MULTI-USER
SQLite	X				X	
XML	X				X	
Devolutions Online Drive			X	X	X	
Dropbox (Note )			X	X		Note 1
Amazon S3,			X	X		Note 1
FTP, SFTP		X		X		Note 1
Web		X		Note 2		Note 2
Devolutions Online Database - Basic			X	X	X	3 users

## NOTES

**NOTE 1**

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

**NOTE 2**

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

**2.3 Checklist for Teams**

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

CHECKLIST FOR TEAMS	
Step 1 - <a href="#">Register your license</a> .	
Step 2 - Add <a href="#">your Data Source</a> (for teams).	
Step 3 - <a href="#">Select your Security Provider</a> .	
Step 4 - Create your folder structure.	
Step 5 - Create your <a href="#">Default Settings</a> .	
Step 6 - <a href="#">Create Users</a> .	
Step 7 - <a href="#">Create Roles</a> .	
Step 8 - Create Entries.	
Step 9 - <a href="#">Grant Permissions</a> .	

## CHECKLIST FOR TEAMS

Step 10 - [Import your Data](#).

## REGISTER REMOTE DESKTOP MANAGER

Remote Desktop Manager Enterprise Edition grants you a 30 day trial. Refer to the procedure in the [Registration Enterprise Edition](#) topic to register your license key. If you decide not to register by the end of the 30 day trial, your data will not be altered or erased, and you will have full access to it once you provide a license key. Please consult our [Free Edition](#) or [Enterprise Edition](#) topic to register.

## ADD A DATA SOURCE



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

Upon first launch, Remote Desktop Manager uses a local SQLite data source. Learn more about adding your own [Data Source](#).

For help selecting a data source tailored to your needs, please see [Choosing your data source \(Teams\)](#).

## 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.

## 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.

## CREATE YOUR DEFAULT SETTINGS



In **File - Options** you can set options for Remote Desktop Manager and create default settings [Templates](#). Each entry type is supported and can have a default template defined to fit your requirements. After you configure the options, use the [Custom Installer](#) to share the pre-configured version with your team.

## CREATE USERS

Remote Desktop Manager supports advanced [User Management](#). User accounts must be created manually by an administrator of the database.

## CREATE ROLES

Create [Roles](#) to easily manage your security system. You can then assign users to Roles, making it easy to grant permissions to a set of users instead of having to manage permissions individually.

## CREATE ENTRIES

An Entry is how you save information about your sessions (e.g. RDP, SSH connections), credentials, websites, VPNs, Synchronizers and documents.

## GRANT PERMISSIONS

Once your users are created you can then grant [Permissions](#) for role-based access control. The permissions granted on the folder can be inherited by each entry set under that folder.

## 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 easy steps.

### 2.3.1 Select the Data Source type - Teams

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



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

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

CONCERN	Devolutions Password Server	SQL SERVER	SQL AZURE	MYSQL/ MARIADB	DODB PRO	DODB ENT
The database is not accessible to end users	X	Note 1 & 2	Note 1	Note 1	Note 1	Note 1
AD accounts used for authentication	X	X				
AD group membership used to assign permissions	X					
The data is stored on-premises	X	X		X		
Activity Logs	X	X	X	X		X
Data accessible globally	Note 3	Note 4	X	Note 4	X	X
Optional local cache of connections	X	X	X	X	X	X

## NOTES

### NOTE 1

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

## NOTE 2

Integrated Security is the name of a Microsoft technology that does not send credentials to get access to a SQL Server instance, but rather the token resulting from authentication in your Windows computer. This therefore allows the users to connect directly to the database using other tools. It should not be used if you need to prevent direct access to the database.

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

## NOTE 3

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

## NOTE 4

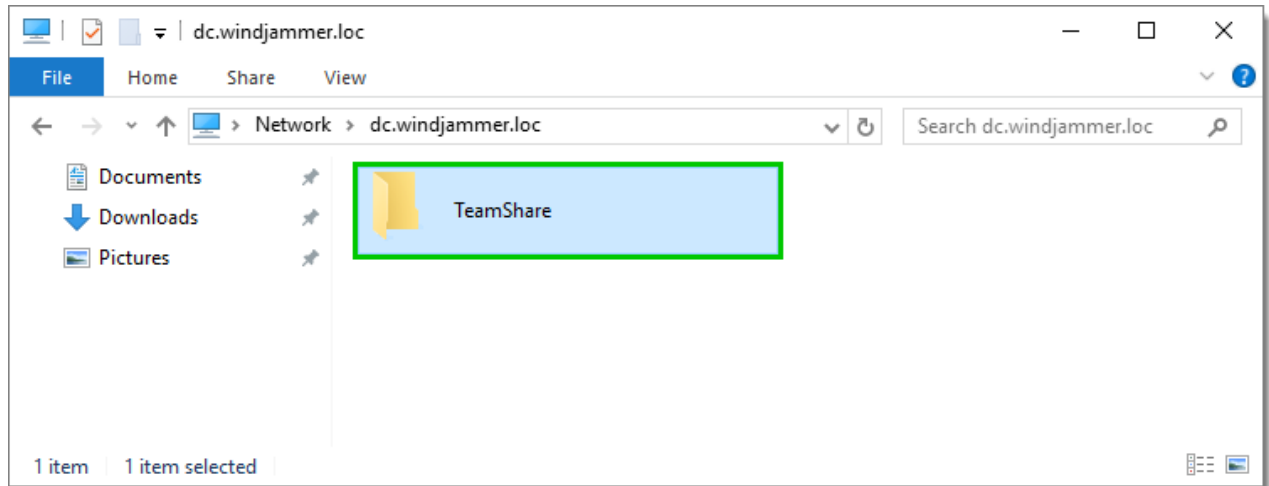
You can indeed expose a database to the Internet, but you must use SSL/TLS to encrypt traffic, you must ALSO protect against DDoS attacks. Cloud services, like Azure or Amazon Web Services, have that concern in the forefront. The default settings of the firewall should be to block everything, you will then open only the most limited set of ports, while filtering on a short list of acceptable origins for requests.

### 2.3.2 Set up a team folder for default settings

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

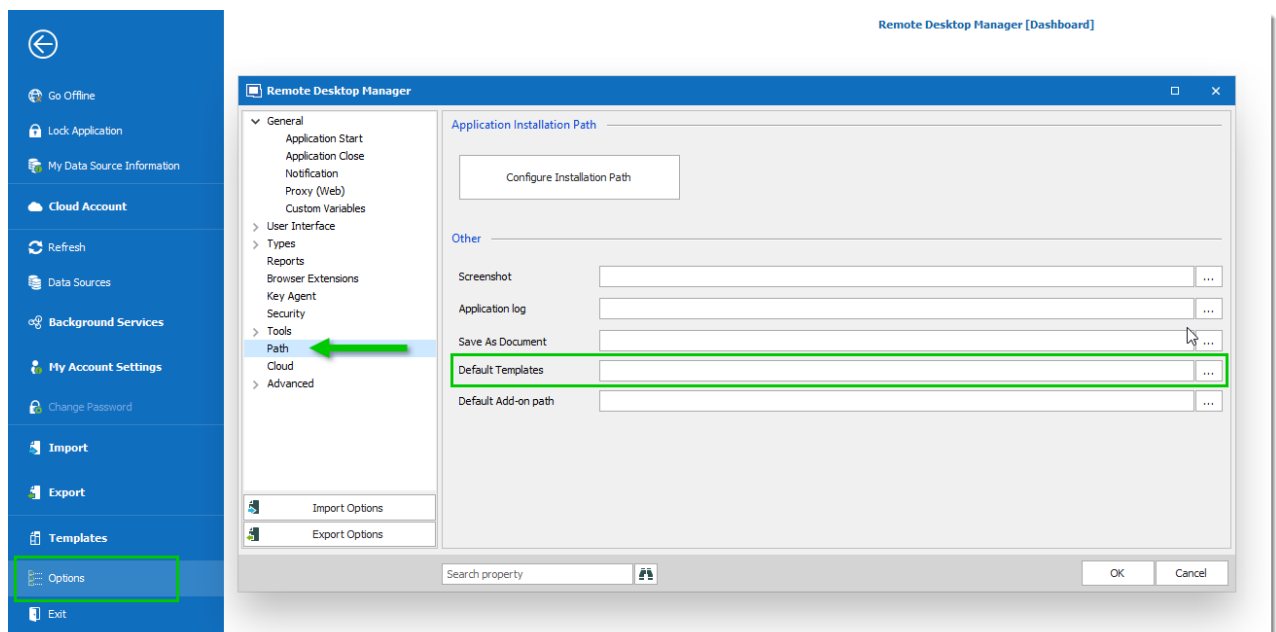
## SETTINGS

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



*Server Drive - Team Folder*

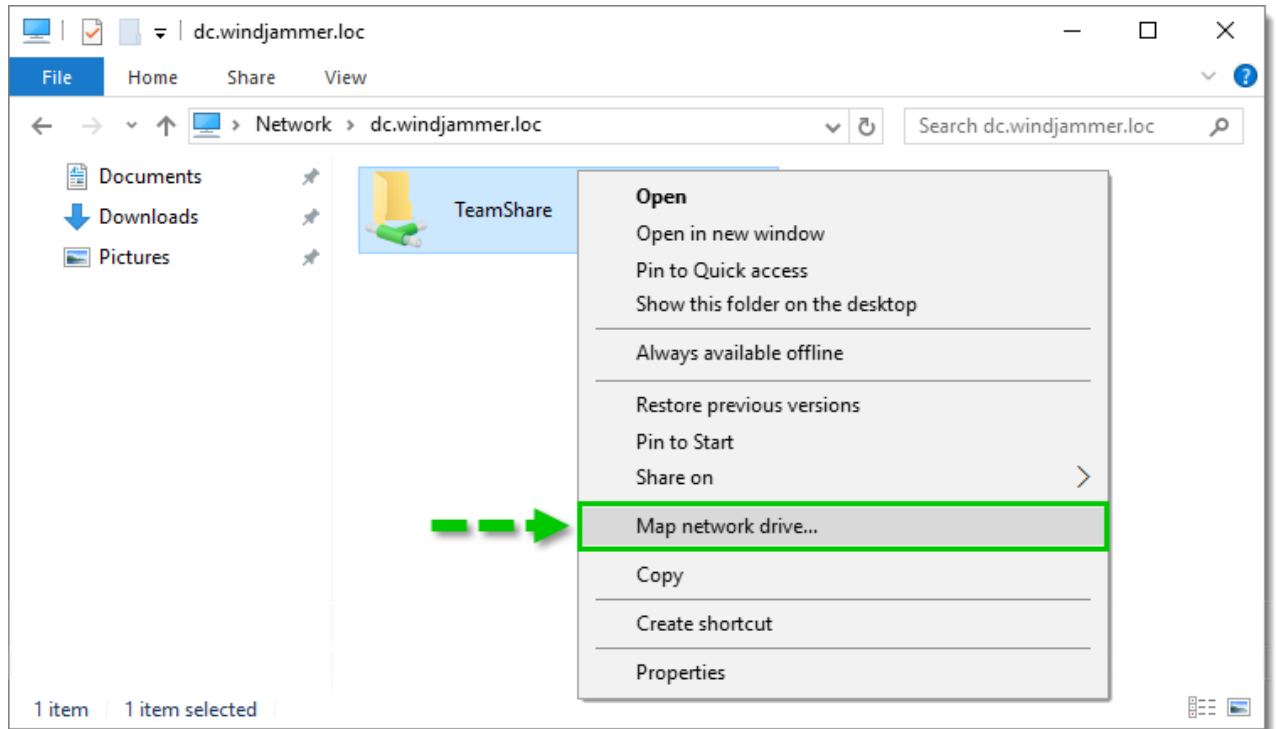
2. Go to **File - Options - Path** and enter the path of your newly created folder stored on your server drive. All your default templates will then automatically be saved in that folder.



*File - Options - Path*

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





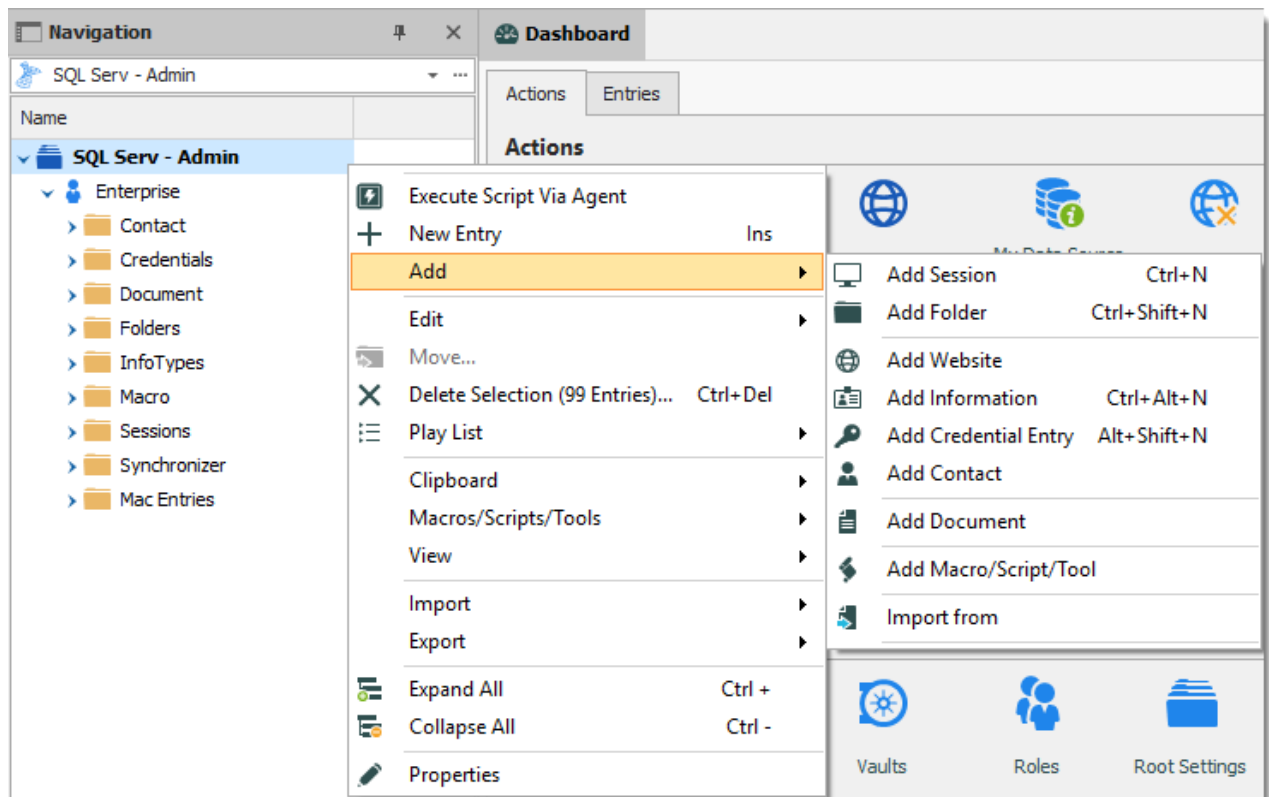
*Map Network Drive*

## 2.4 Creating an Entry

When getting started with Remote Desktop Manager, you must configure your entries. There are many types of entries; you should know what third party or technology you will use in order to choose the appropriate entry type(s) that you plan on configuring.

### CREATING AN ENTRY FROM THE CONTEXT MENU

On the main application window, simply right-click on **the name of the data source** and select **Add** from the menu. To initialize a new session, you can specify either the type of session, or a template. You will be prompted to customize your settings in the entry properties window.



*Adding a new entry*

## CREATING AN ENTRY WITH DRAG & DROP

You can also create a session by dragging and dropping an .rdp file in the main application window. By doing so, Remote Desktop Manager will ask you whether to import the content and create a new session, or create a session linked to the .rdp file. It is also possible to drag and drop the **LogMeIn** desktop shortcut to create a **LogMeIn** session.



It is possible that drag and drop will not work because of your security settings. They may prevent applications running in different contexts from interacting. For example, if Remote Desktop Manager is running in an elevated context (administrator mode) and Internet Explorer is running in default mode, Windows will not allow you to drag a URL link in the application.

## CREATING AN ENTRY BY IMPORTING ITS CONFIGURATION

You can also import entries by using the [Import Computer Wizard](#), or by importing its configuration directly from any compatible applications supported by our import tools. You can learn more in the [Import](#) section.

## 2.5 Managing Credentials

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



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

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

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

Here are the most common scenarios and how to address them. In the majority of cases, we prefer to have sessions using **Inherited credentials**, meaning it climbs up the tree until it has access to a set of credentials, be it defined, linked, or overridden in an entry.

SCENARIO	STRATEGY
One set of credentials is used by all of the staff, be it for the whole system or for a branch in your tree view (Customer, Department, etc).	Set the credentials on the <a href="#">Vault Settings</a> . All children use <b>Inherited Credentials</b> .
Each user has its own credentials for many different branches (often corresponds to customers/departments, etc).	Make use of the <a href="#">User Specific Settings</a> on each branch. All children use <b>Inherited Credentials</b> .
Each user has its own credentials managed by an administrator.	This solution involves a little more work. The admin must create a folder for each user, then grant permissions ONLY to that user. The user will then use <b>User Specific Settings</b> to specify that the credentials stored in that folder is used to override what is defined in the entries.
Each team uses the same credentials.	Much like directly above, but all the members of the team have access to the folder. All of them must use the <b>User Specific Settings</b> .
Each user uses their domain account.	Have the sessions configured to use <a href="#">My personal credentials</a> . Each user will be prompted to define them once per workstation that they use.

# Installation

---

Part III

## 3 Installation

### 3.1 Client

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

#### INSTALLATION

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

#### LICENSE

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

#### DATA SOURCE

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



To use a SQL Server or SQL Azure data source, refer to the [Configure SQL Server](#) topic.

#### EXTERNAL APPLICATIONS

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

#### REMOTE DESKTOP SERVICES

Please consult the [Remote Desktop Services](#) topic.

### 3.1.1 Ancillary Files

## DESCRIPTION

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

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

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

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

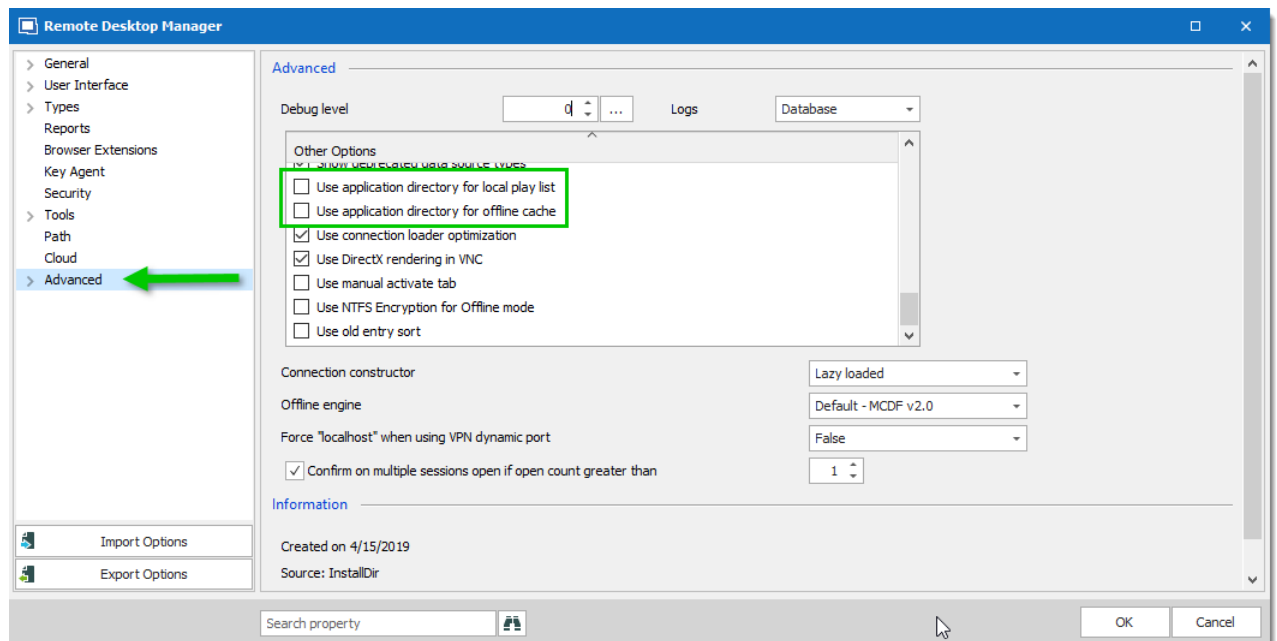
## SUMMARY

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

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

## OFFLINE AND LOCAL PLAY LIST OPTION

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



Options - Advanced



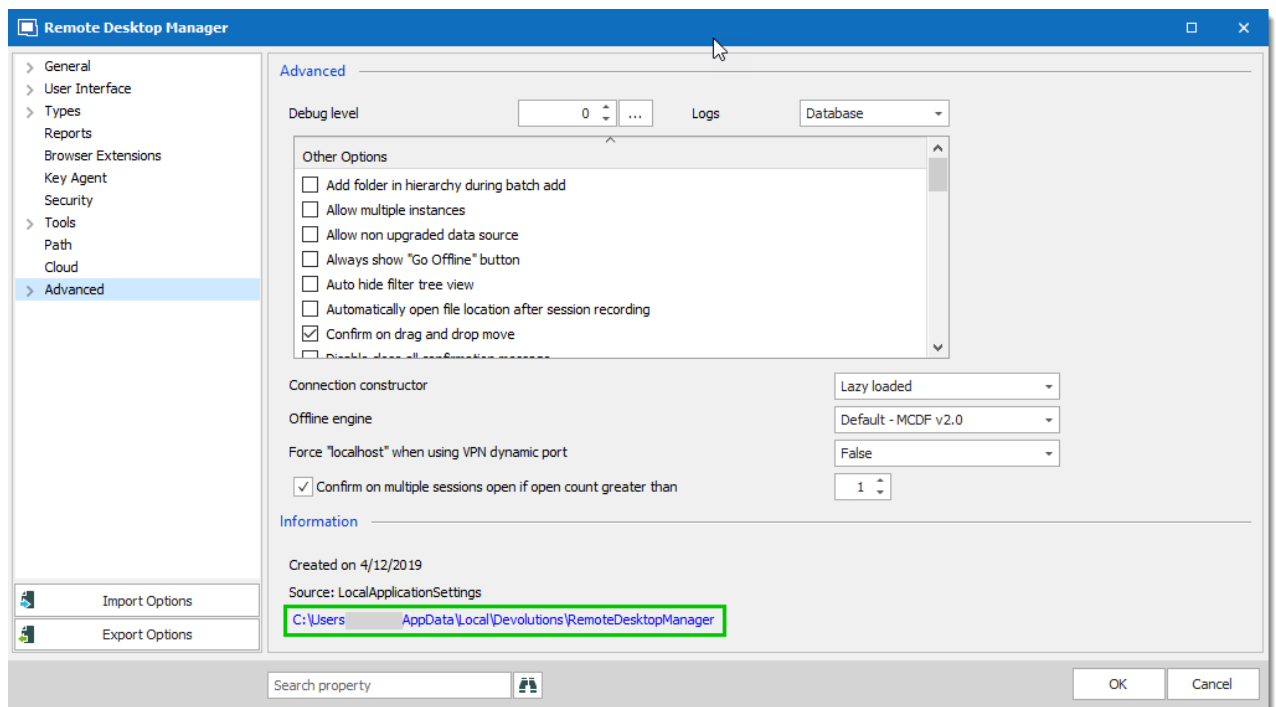
### 3.1.2 Configuration File Location

#### DEFAULT LOCATION

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



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



*Options - Advanced*

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

CASE	CONFIGURATION FILE LOCATION
Installed under "Program Files" or "Program Files (x86)"	%LocalAppData%\Devolutions\RemoteDesktopMa

CASE	CONFIGURATION FILE LOCATION
<b>Application running on Terminal Server</b>	%AppData%\Devolutions\RemoteDesktopManager. This is the roaming profile and avoids multi-user conflicts.
<b>Other</b>	Installation folder



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

## OVERRIDE THE DEFAULT PATH

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

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

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

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

## DEFAULT CONFIGURATION FOR REMOTE DESKTOP SERVICES ENVIRONMENT

Please refer to [Remote Desktop Services](#) for details.

### 3.1.3 Custom Installer Service

#### DESCRIPTION



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

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

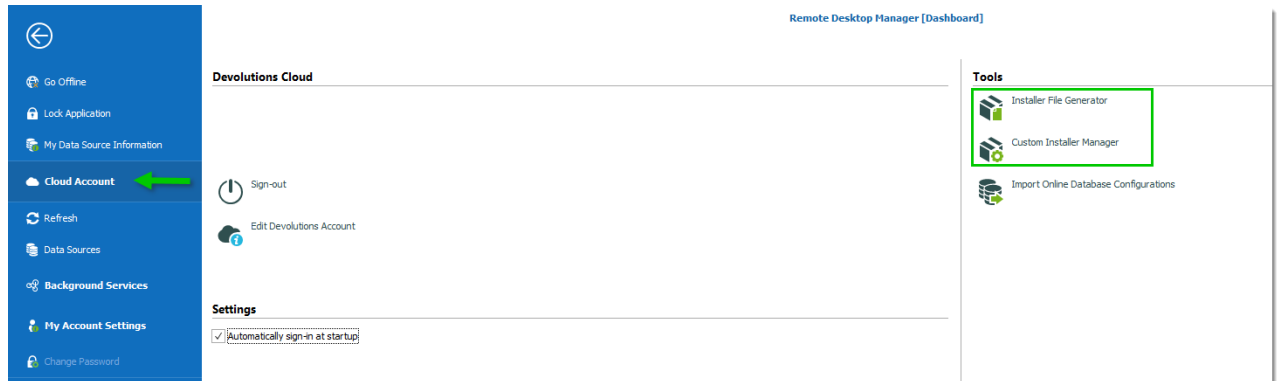


The Custom Installer Service uploads a configuration file to our online services. You should not use the service to redistribute passwords for data sources or an Online Database account.



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

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



*File - Devolutions Account - Tools*

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

- [Create an Installation Package](#)
- [Installer File Generator](#)
- [Option Selection Dialog](#)

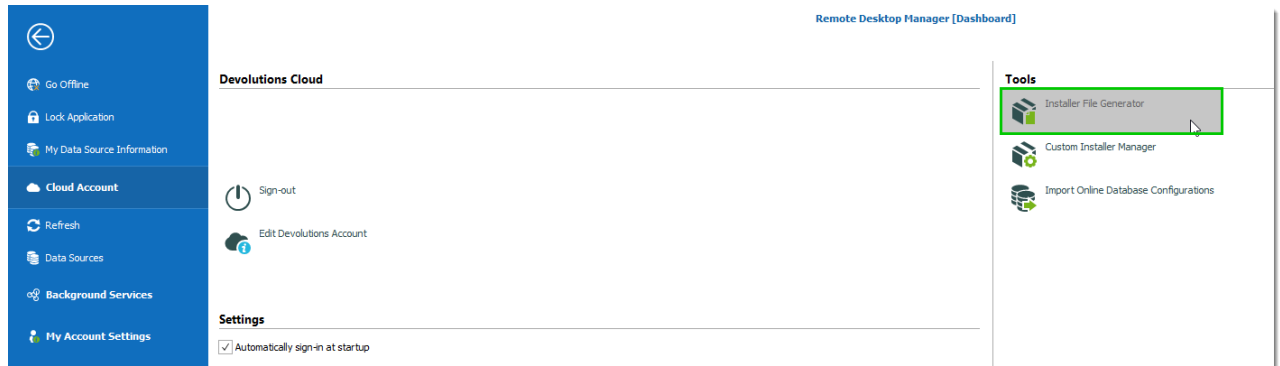
#### 3.1.3.1 Installer File Generator

## DESCRIPTION

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

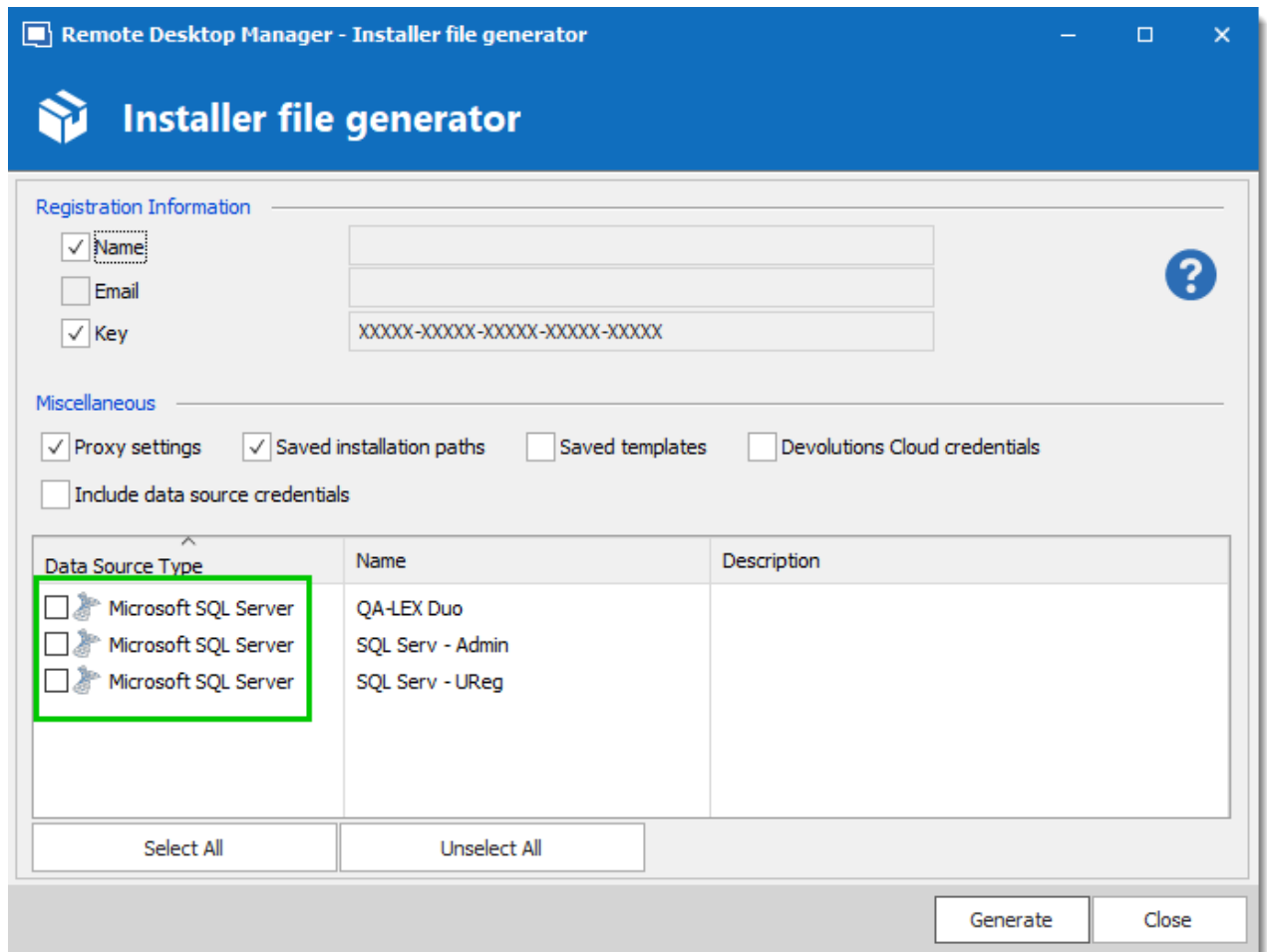
## CREATING AN INSTALLER FILE

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



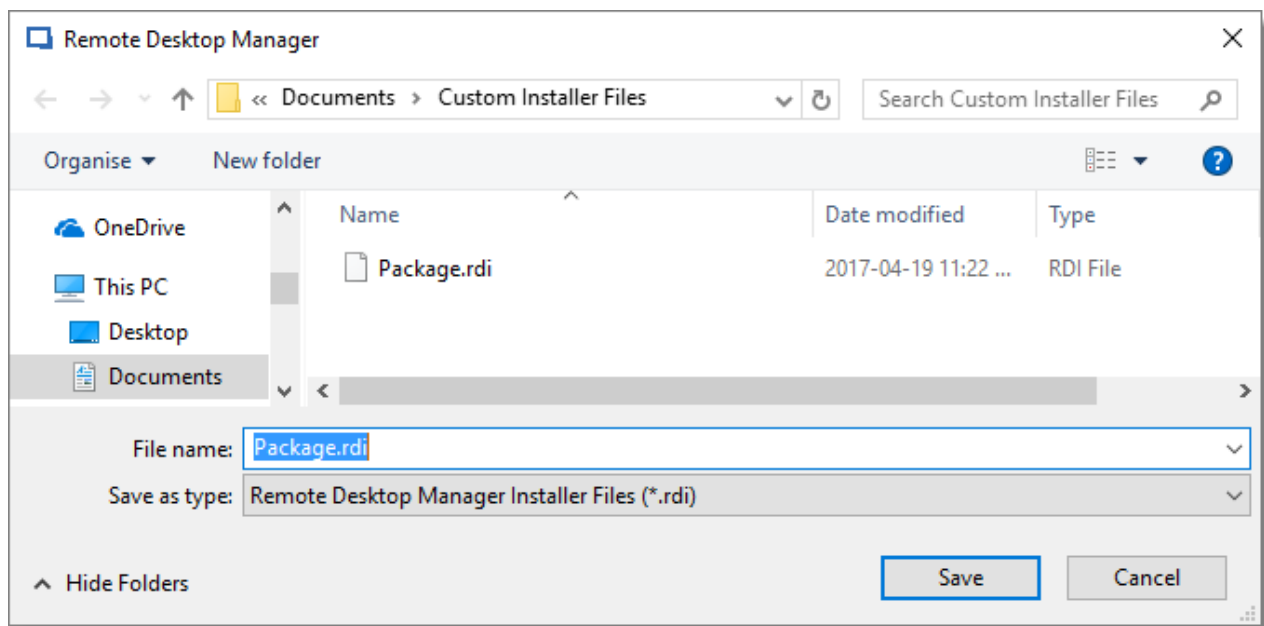
*File - Devolutions Account - Installer File Generator*

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



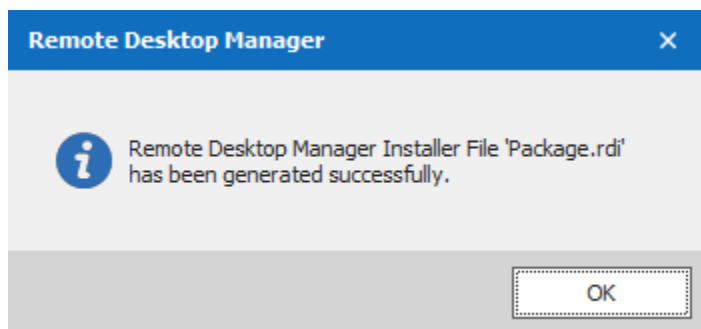
*Installer File Generator*

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



*Save the installer file*

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



*Package.rdi has been generated successfully*

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

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

#### 3.1.3.1.1 Option Selection Dialog

## DESCRIPTION

When generating the installer file, you must decide what to include in the configuration. This process will replicate the configuration of the Remote Desktop Manager instance currently used, and will generate an installer file (\*.rdi). Once it has been generated, the installer file can be used as many times as needed to create custom installers. For security reasons, some

settings that may contain credentials, such as **Saved Templates**, are disabled by default. Enable these at your own risk.



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



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

## SETTINGS

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

**Remote Desktop Manager - Installer file generator**

**Installer file generator**

**Registration Information**

☒ Name

☐ Email

☒ Key XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

**Miscellaneous**

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

☐ Include data source credentials

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

Select All Unselect All

Generate Close

*Installer File Generator*

## REGISTRATION INFORMATION

**Registration Information**

☒ Name

☐ Email

☒ Key XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

*Installer File Generator - Registration Information*

OPTION	DESCRIPTION
<b>Name</b>	Company registration name.



OPTION	DESCRIPTION
<b>Email</b>	Registration email if using a generic address.
<b>Key</b>	License serial.

## MISCELLANEOUS



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



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



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

Miscellaneous

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




☐ Include data source credentials

*Installer File Generator - Miscellaneous*

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

OPTION	DESCRIPTION
<b>Filter history</b>	Preserves your search/filter history
<b>Proxy settings</b>	Includes your Internet proxy settings
<b>Devolutions Account credentials</b>	Includes your Devolutions Account credentials used to create the custom installer. Please, consult security warning above.
<b>Include data source credentials</b>	Includes the credentials for all selected data sources below. Please, consult security warning above.

## DATA SOURCES

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

*Data Source List*

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

### 3.1.3.2 Custom Installer Manager

## DESCRIPTION



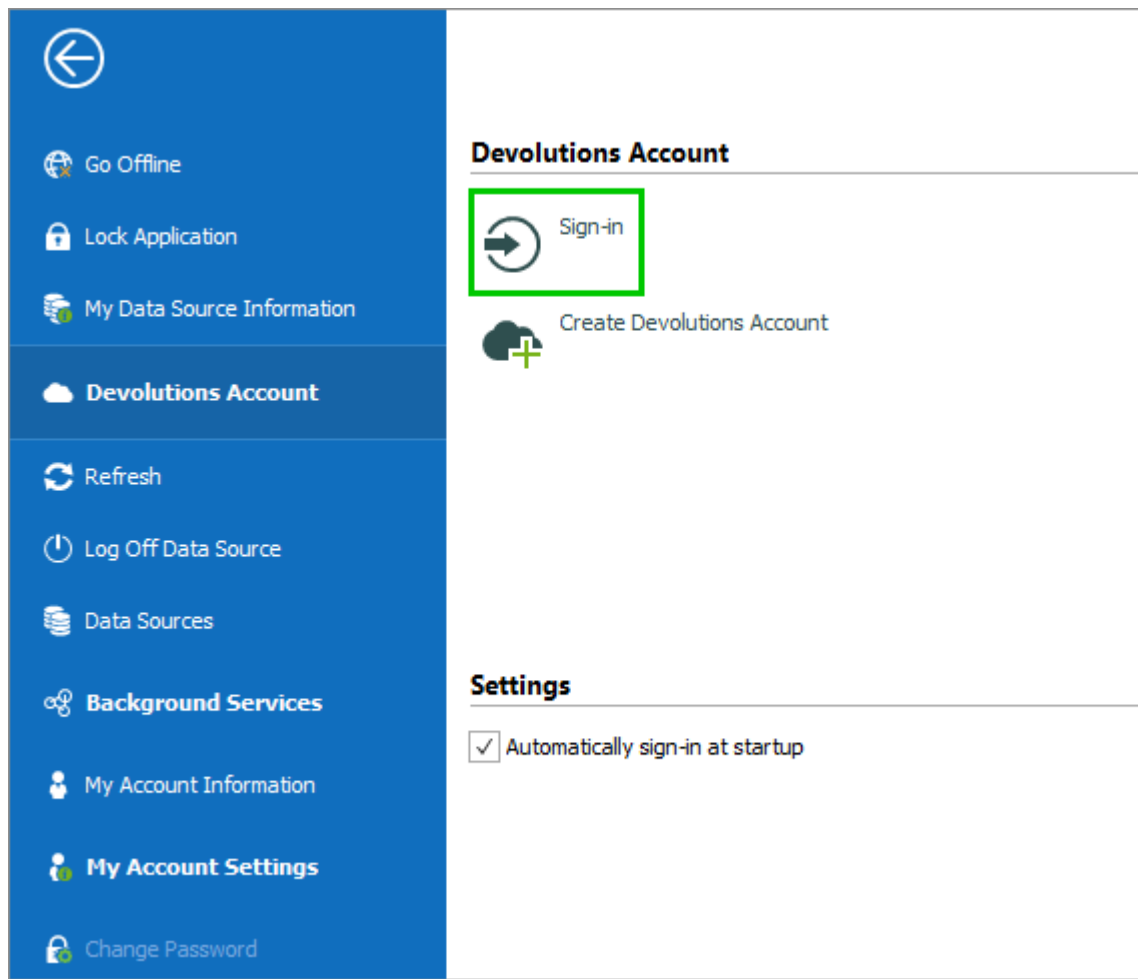
For stability reasons, in large installation bases, the latest official release is not available to the Custom Installer Service for an undetermined period while we ensure that no major issues are present. We recommend using this time with your organization to perform integration tests on a few workstations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



Please ensure you have read and understood the content of [Custom Installer Service Overview](#) prior to subscribing to the service.

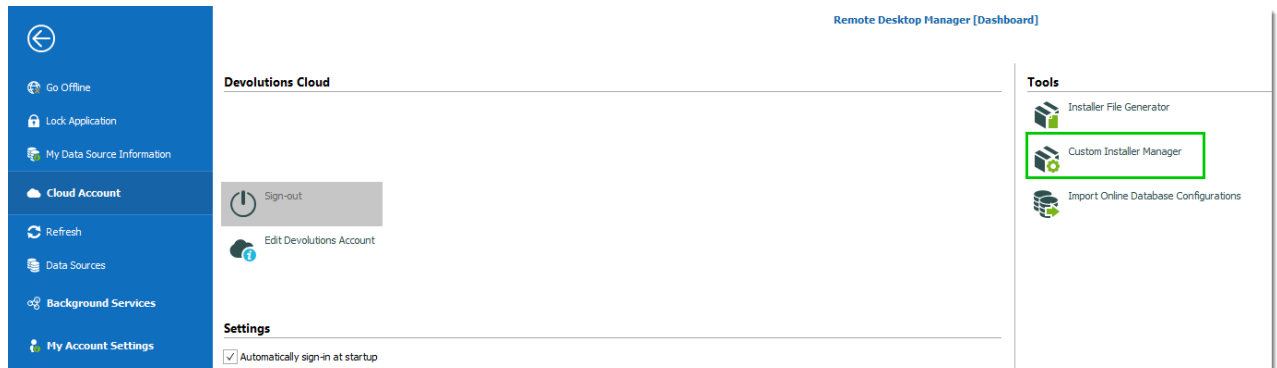
## CREATE AN INSTALLATION PACKAGE

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



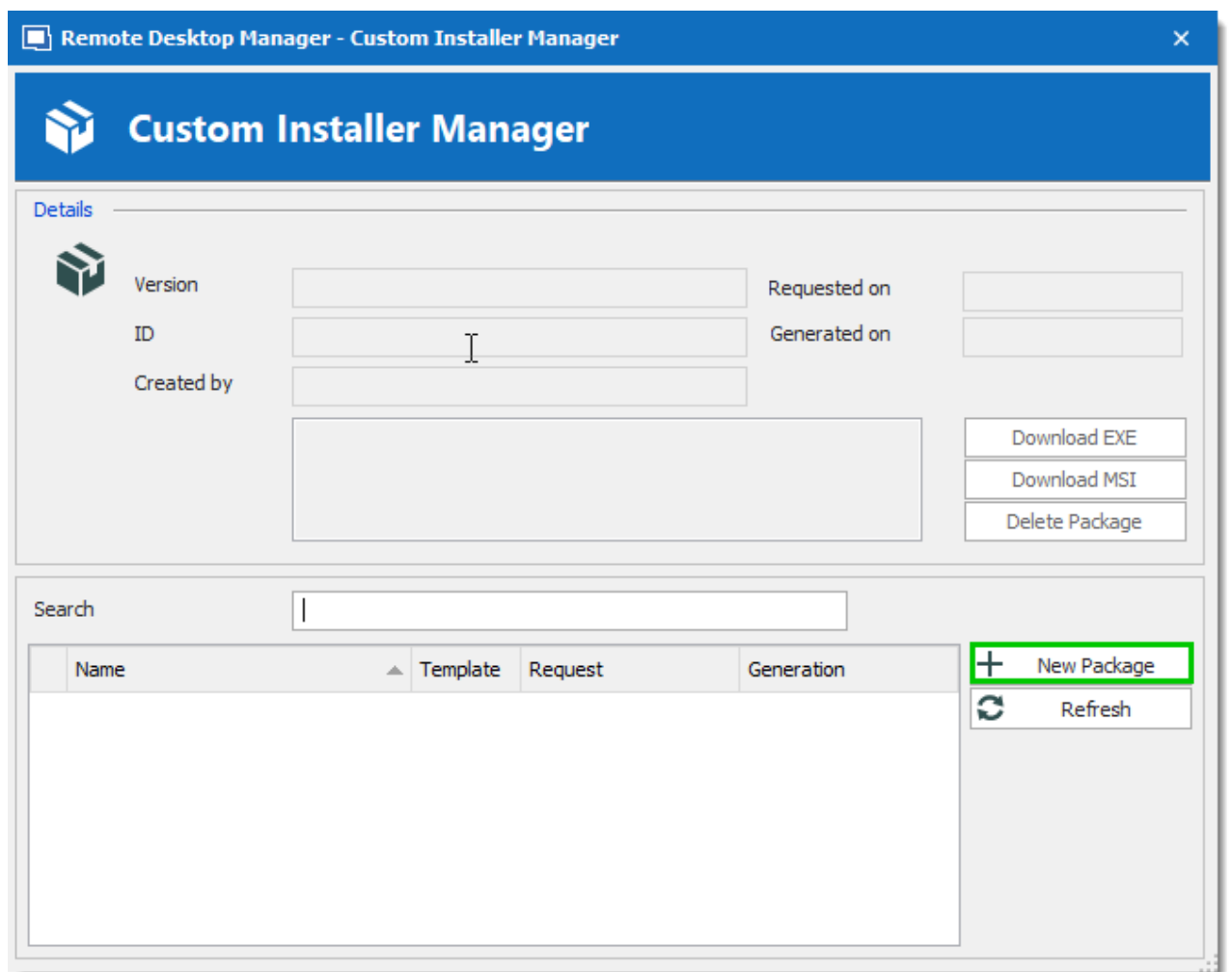
*Devolutions Account Sign-in*

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



*File - Devolutions Account - Custom Installer Manager*

- Click on **New Package**.



*Custom Installer Manager - New Package*

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

Remote Desktop Manager - Installation Package Creation

**Installation Package Creation**

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

Name: Setup.RemoteDesktopManager.2019.1.25.0

Description:

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

Remote Desktop Installer filename: ... New

Create Cancel

*Installation Package Creation*

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

**Registration Information**

☒ Name: UWutmate

☐ Email:

☒ Key: XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

**Miscellaneous**

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

☐ Include data source credentials

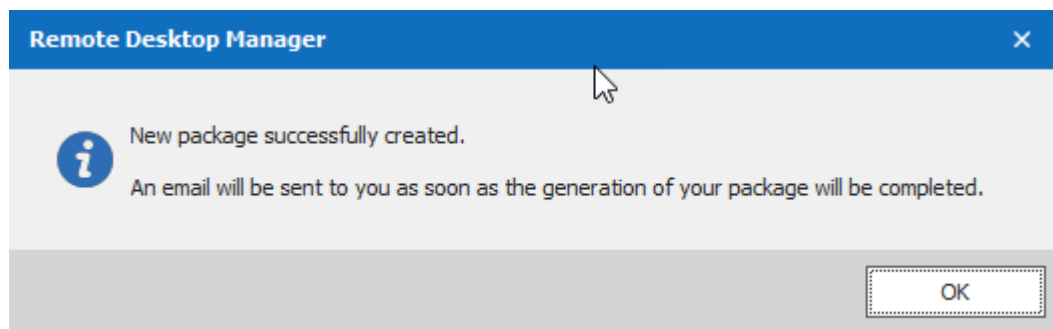
Data Source Type	Name	Description
<input type="checkbox"/> Microsoft SQL Server	QA-LEX Duo	
<input type="checkbox"/> Microsoft SQL Server	SQL Serv - Admin	
<input type="checkbox"/> Microsoft SQL Server	SQL Serv - UReg	

Select All Unselect All

Generate Close

*Installer File Generator*

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



*New package successfully created*

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

Remote Desktop Manager - Custom Installer Manager

## Custom Installer Manager

Details

**Setup.RemoteDesktopManager.2019.1.25.0**

Version: 2019.1.25.0      Requested on: 6/5/2019

ID:      Generated on: 6/5/2019

Created by:      Download EXE

Download MSI

Delete Package

Search:

Name	Template	Request	Generation
Setup.RemoteDesktopManager.2019.1.25.0	2019.1....	6/5/2019	
✓ Setup.RemoteDesktopManager.2019.1.25.0	2019.1....	6/5/2019	6/5/2019

+ New Package

↻ Refresh


Custom Installer Manager




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


## DOWNLOADING AN INSTALLATION PACKAGE

Upon completion you will receive a confirmation email.

Important Information




# Custom Installer Request



Greetings,

Your Custom Installer request was processed successfully.

**Type:** Remote Desktop Manager  
**Version:** 12.0.8.0  
**Name:** Setup.RemoteDesktopManager.12.0.8.0  
**Description:**






[Access Account](#) 

You can access your account by clicking [here](#).

Best regards,

Devolutions Team  
[support@devolutions.net](mailto:support@devolutions.net)

Visit us at [devolutions.net](https://devolutions.net)

**Devolutions**  
1000 Notre-Dame, Lavaltrie  
QC J5T 1M1  
Canada

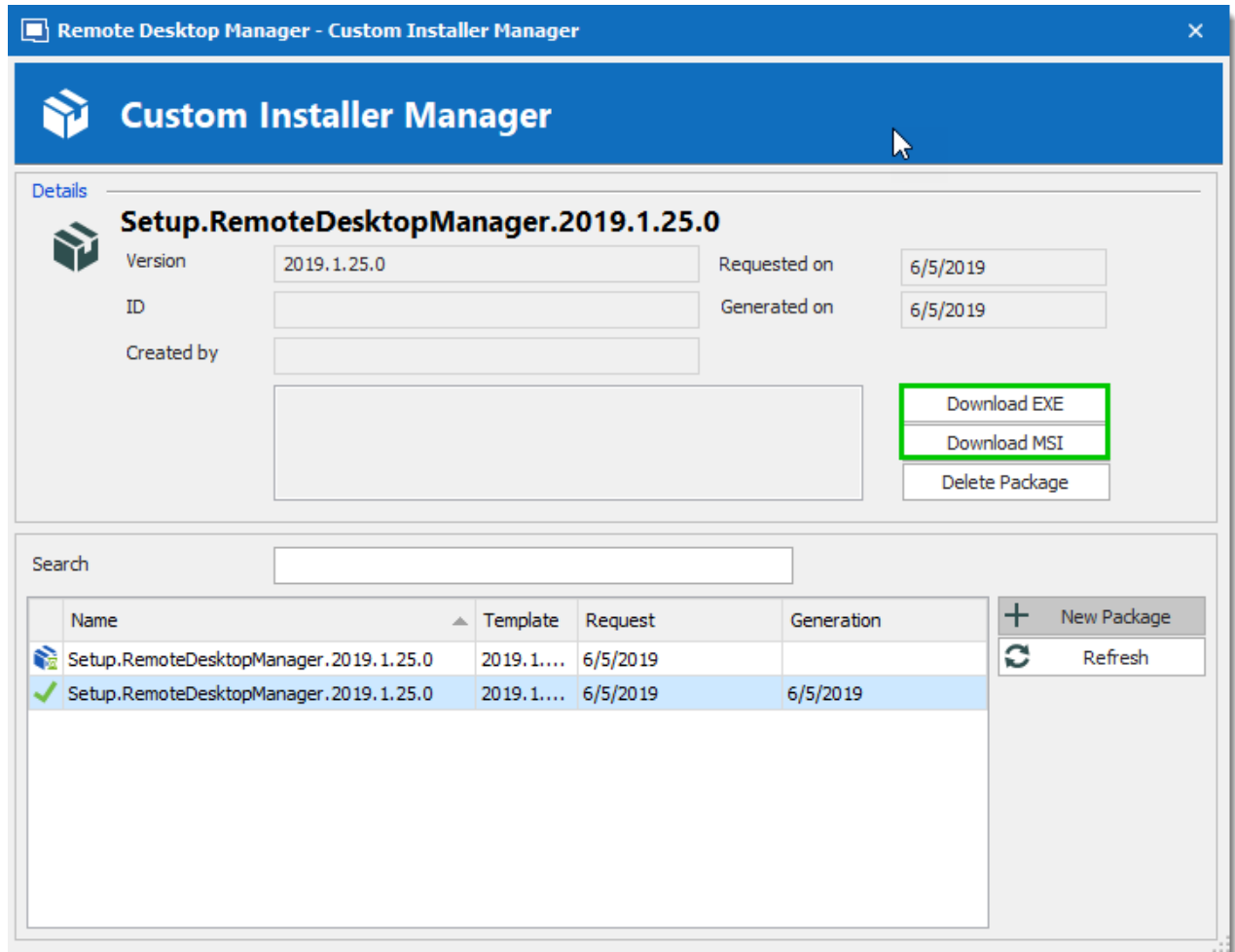
Email Confirmation - Custom Installer Processed



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

## DOWNLOAD WITH THE CUSTOM INSTALLER MANAGER

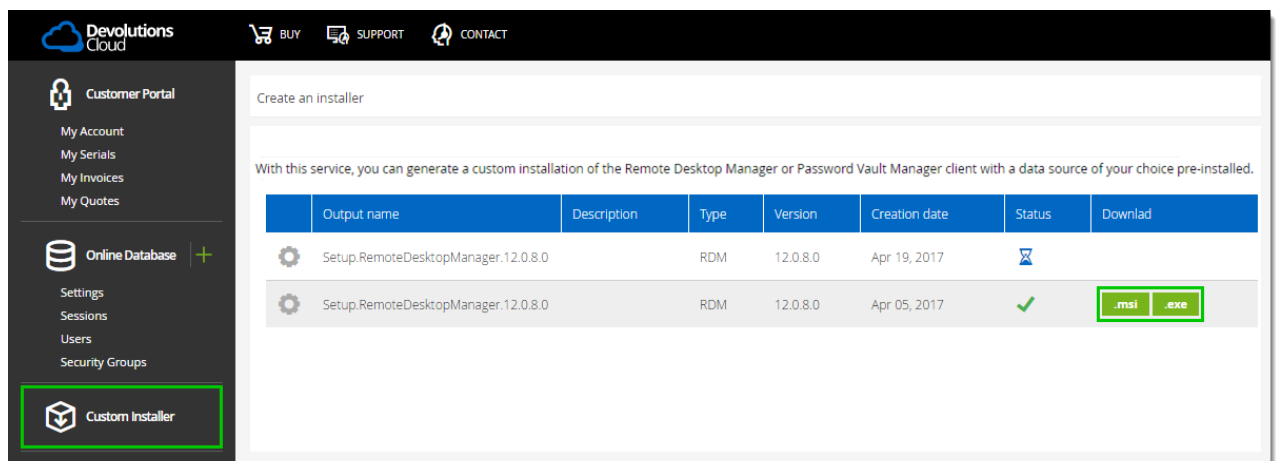
From the **Custom Installer Manager**, click on Download EXE or Download MSI.



Custom Installer Manager - Download Package

## DOWNLOAD FROM THE DEVOLUTIONS CUSTOMER PORTAL

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



*Devolutions Customer Portal - Download Custom Installer Package*

### 3.1.4 For All Users

## DESCRIPTION

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

## PROCEDURE



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

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

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

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

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

## NOTES

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

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

### 3.1.5 Portable (USB)

## DESCRIPTION

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



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



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



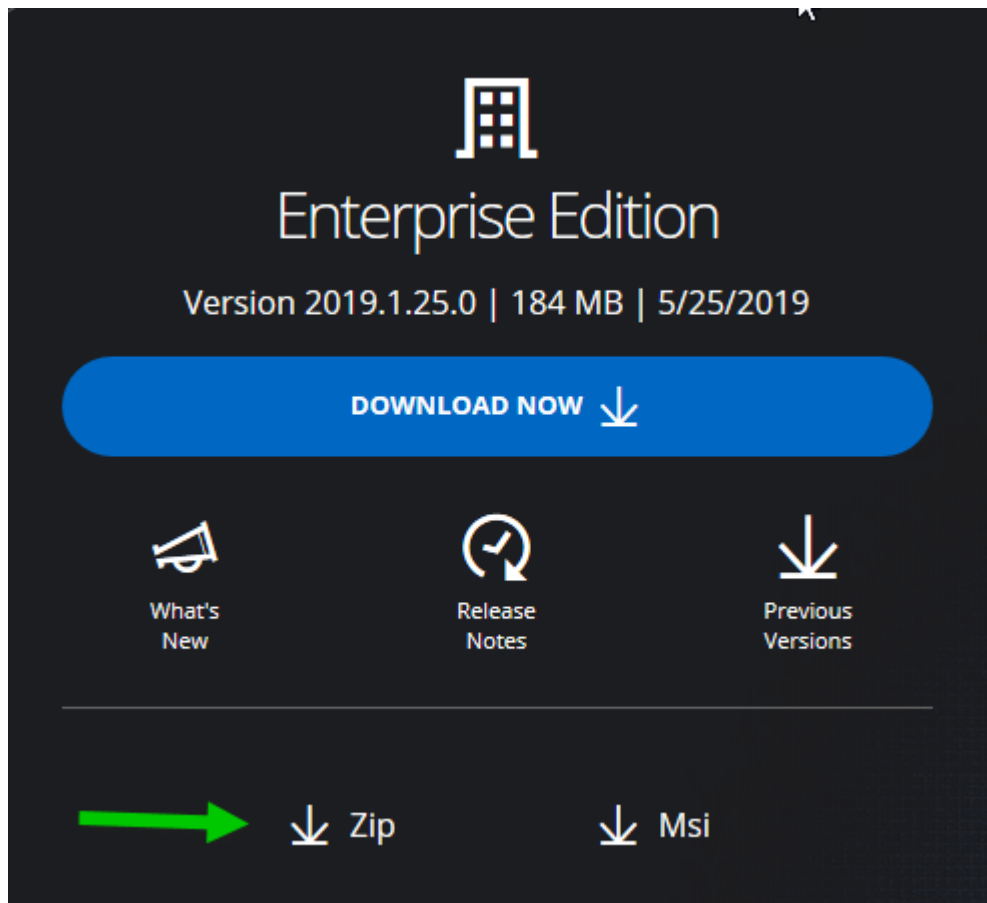
Remote Desktop Manager stores the offline cache in your Windows profile by default. If you are using an Advanced Data Source and plan to use the offline mode, use the Options in the Advanced category to have the offline cached stored in the application folder instead.



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

## PROCEDURE

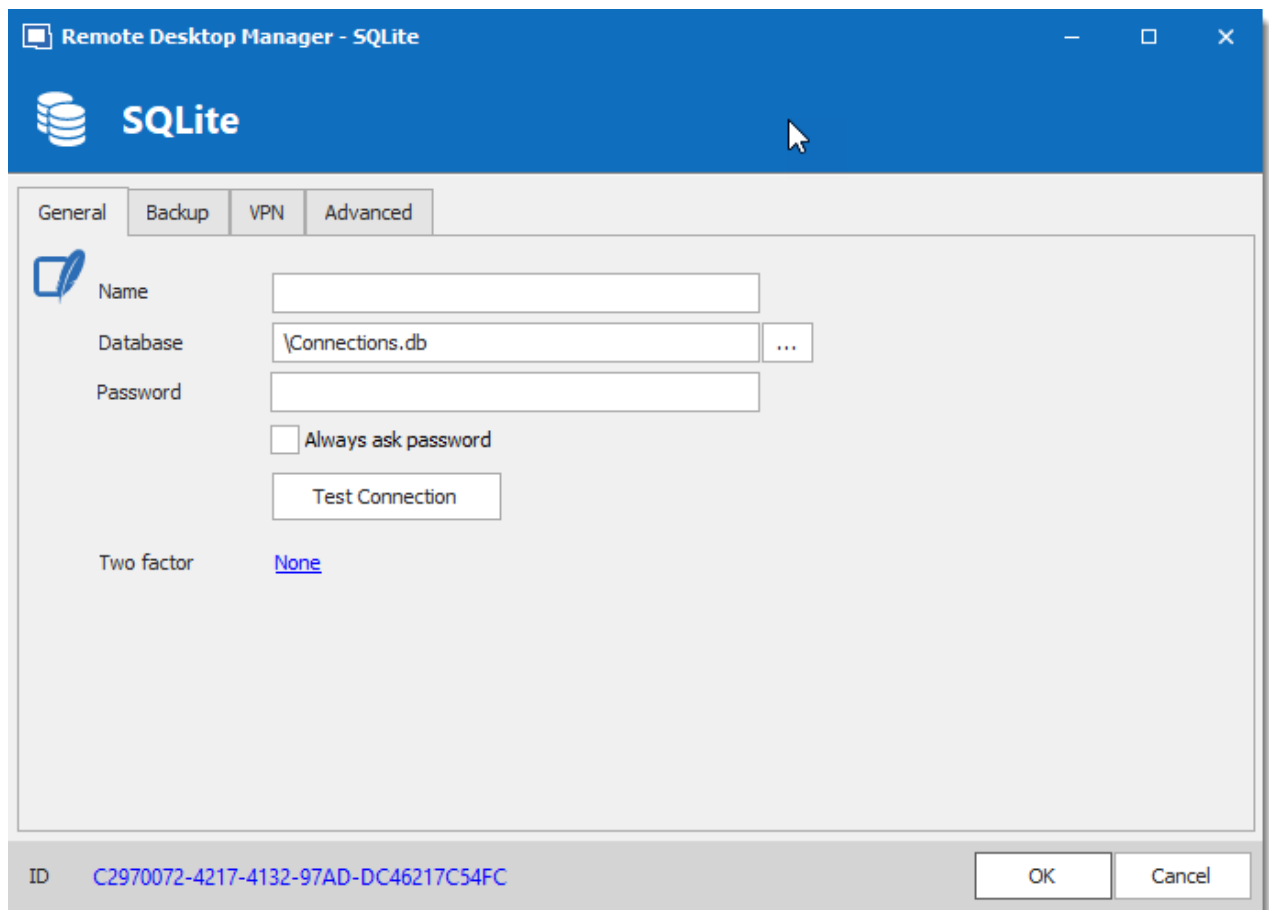
1. Download the "Zip" package of Remote Desktop Manager.



*Zip File Download*

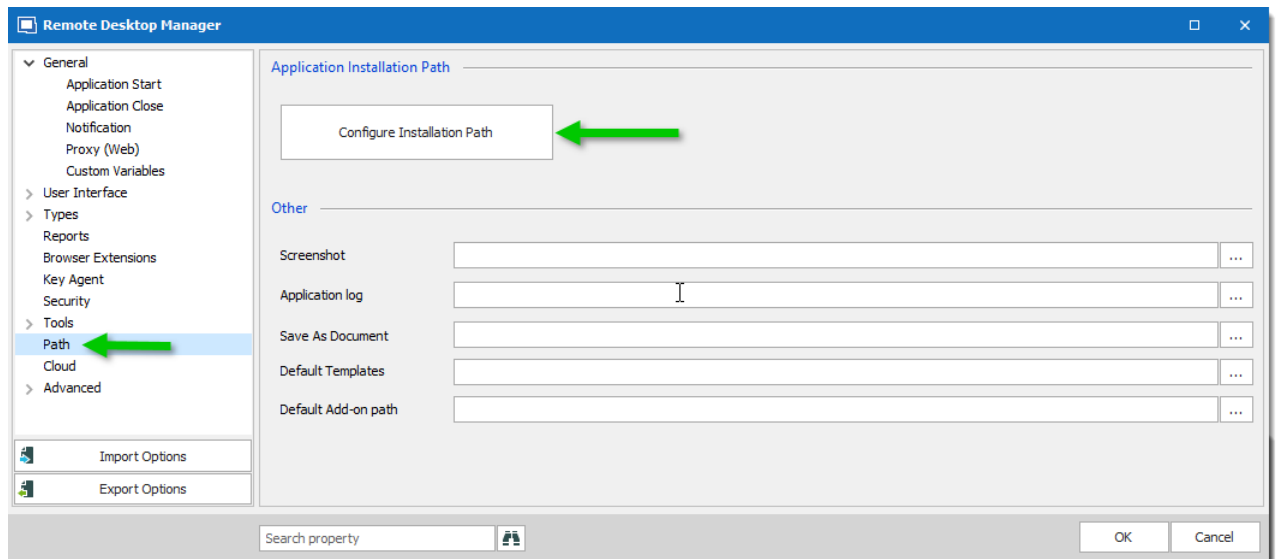
2. Create a RemoteDesktopManager folder on your portable device.
3. In the installation folder created in step 2, create two folders:
  - 3.1. A **config** folder.
  - 3.2. A **data** folder.
  - 3.3. A **tools** folder (optional, only if you intend to use external tools like Filezilla).

4. Unzip Remote Desktop Manager in the installation folder.
5. Create a text file named **override.cfg** in the installation folder. Set the content of the file to `.\config`
6. Open Remote Desktop Manager and display the data sources window using **File – Data sources**.
7. Create a new data source of a type that can be stored on your portable device. i.e. SQLite, XML, etc.
8. Configure the data source using a relative path so it is stored on the portable device: `.\Data\Connections.db`

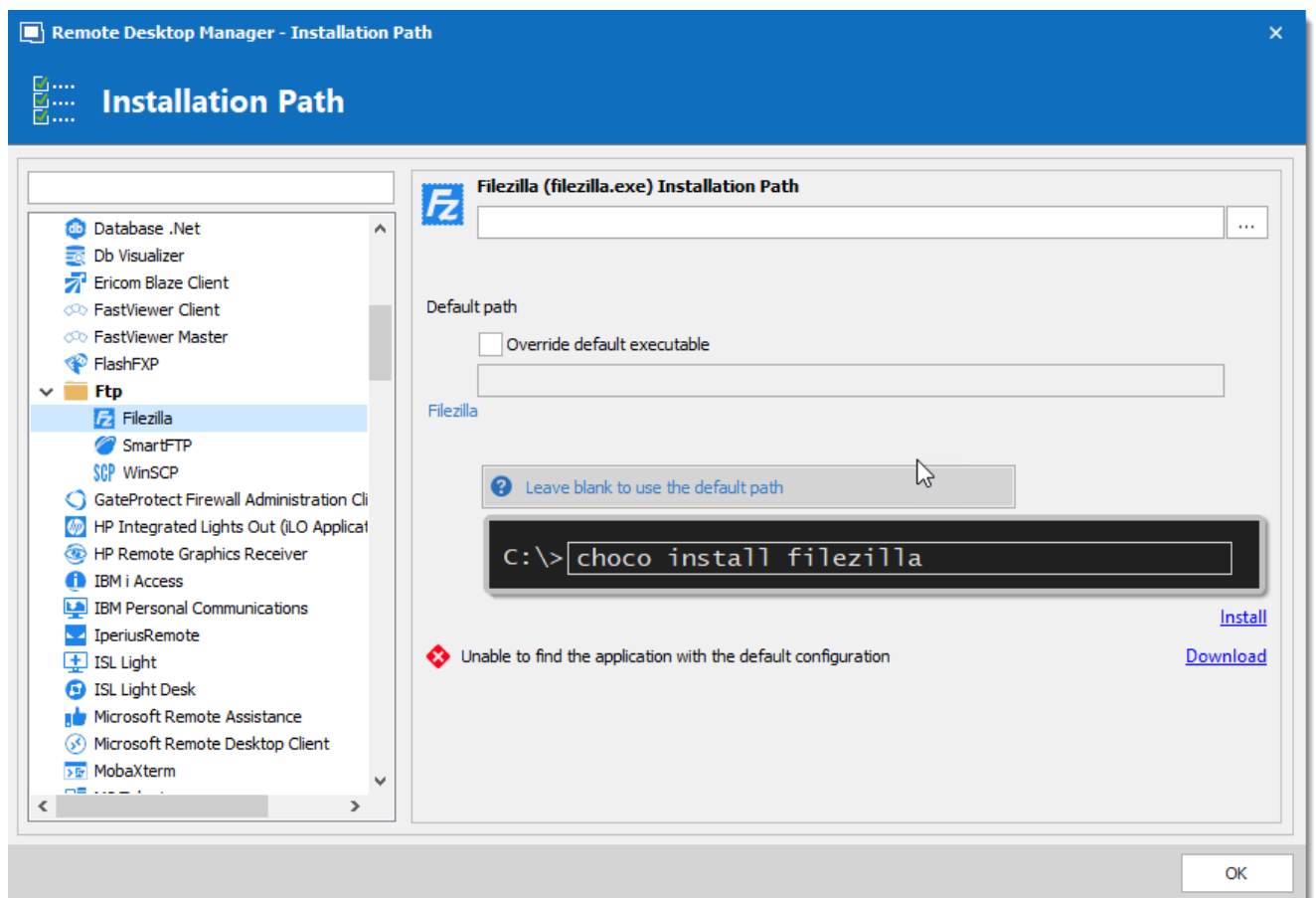


SQLite Data Source

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



Options - Path - Configure Installation Path



Filezilla Installation Path

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

### 3.1.6 Registration

## DESCRIPTION

### REMOTE DESKTOP MANAGER ENTERPRISE EDITION

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

### REQUEST A TRIAL

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

### REMOTE DESKTOP MANAGER FREE EDITION

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

### DEVOLUTIONS PASSWORD SERVER

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

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

### DEVOLUTIONS ONLINE DATABASE

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

### 3.1.6.1 Enterprise Edition

## DESCRIPTION

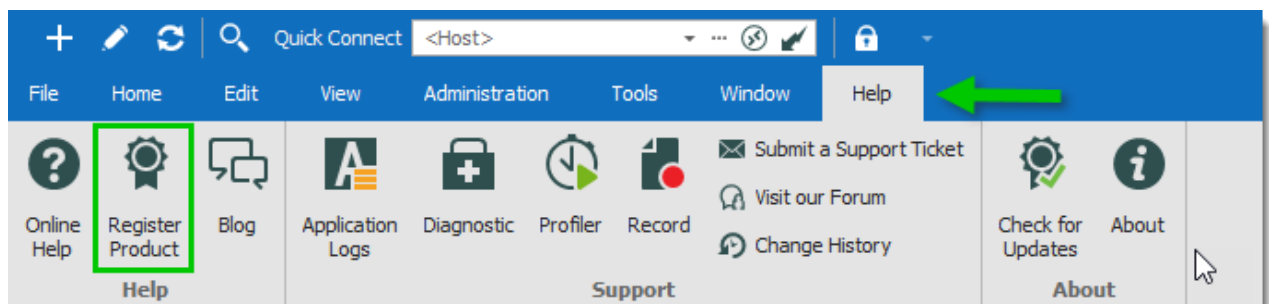
Remote Desktop Manager can be registered by [manually providing a license serial](#) or with a [license serial stored in a data source](#).



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

## MANUAL REGISTRATION

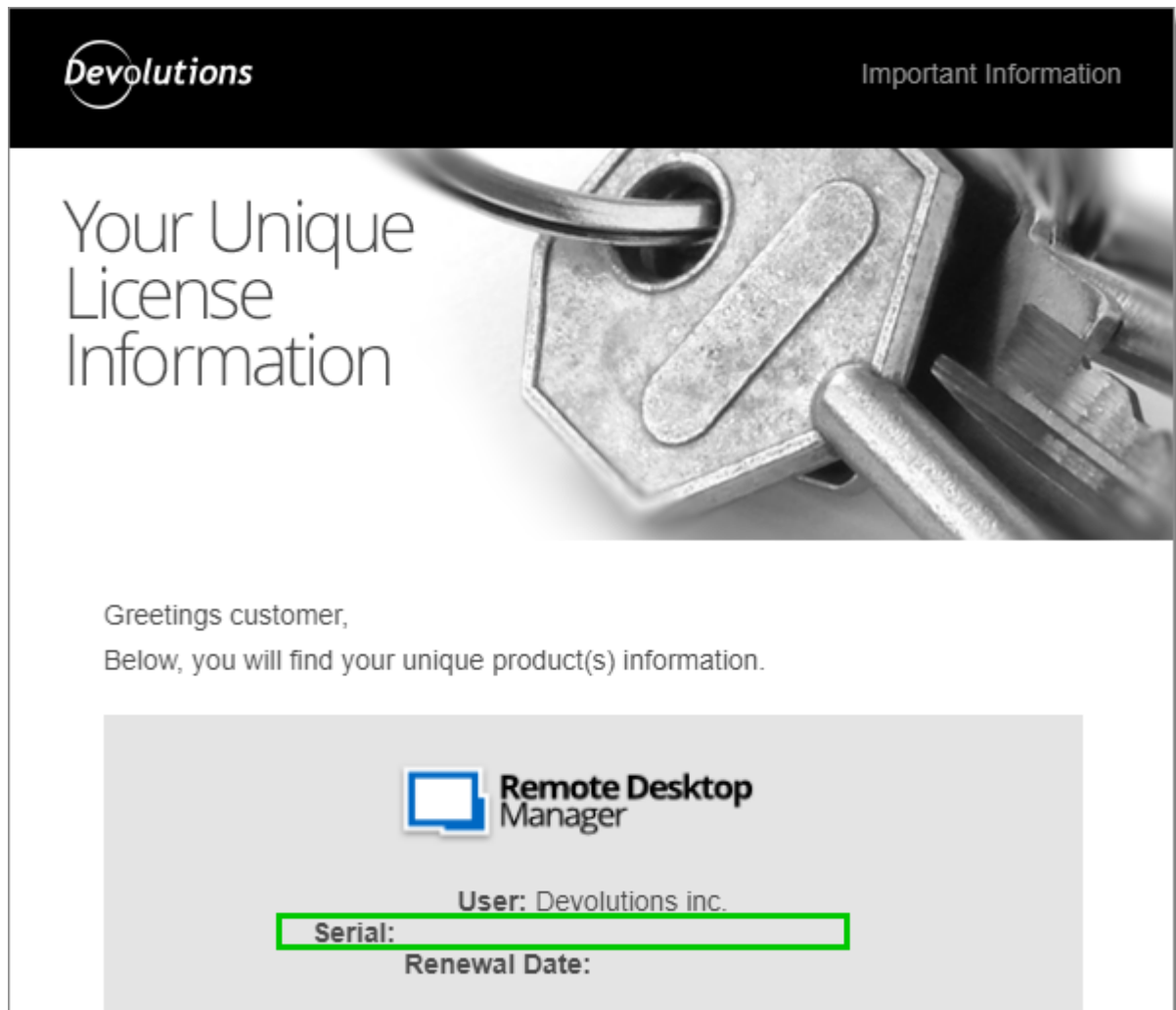
To register your Remote Desktop Manager - Enterprise Edition, open **Help – Register Product**.



*Help - Register Product*

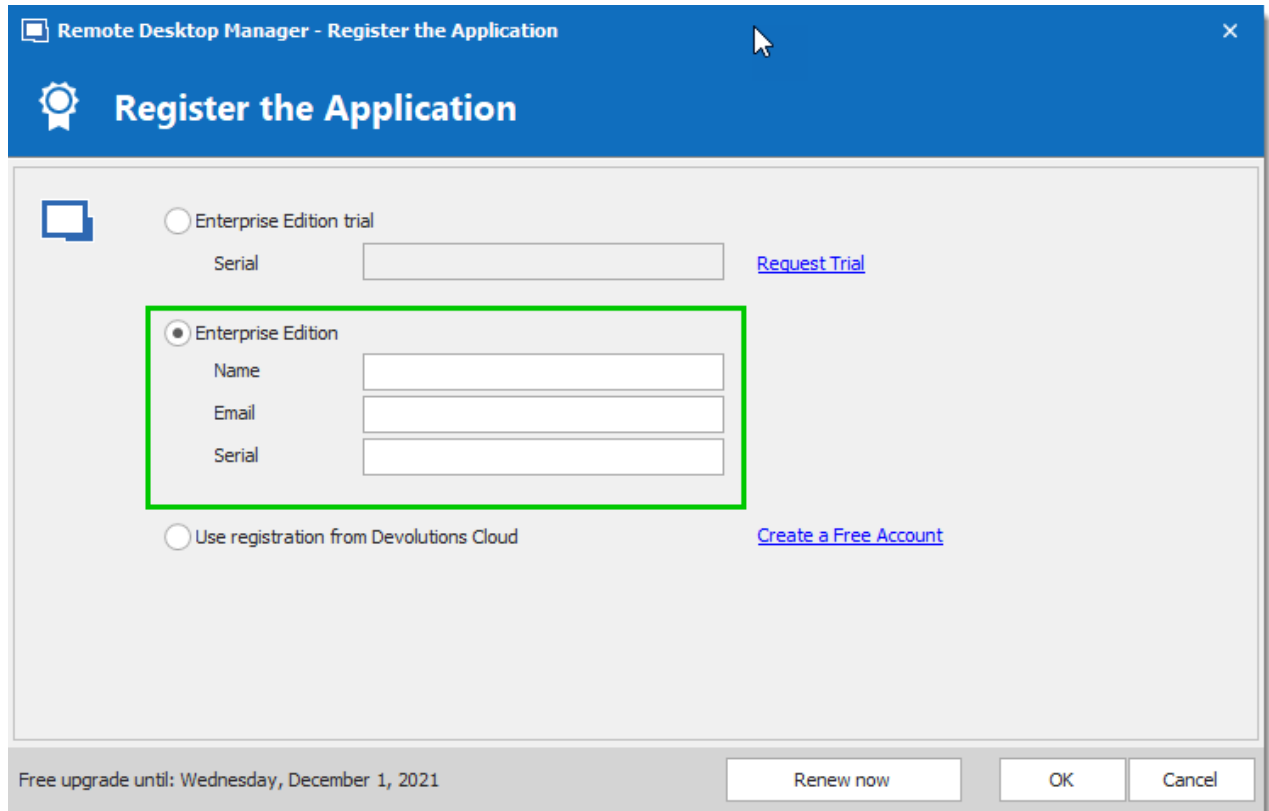
License serials are delivered by email. Locate the email containing the Remote Desktop Manager license serial.





*Devolutions License Serial Email*

Enter the username, email, and serial number, then click **OK**.



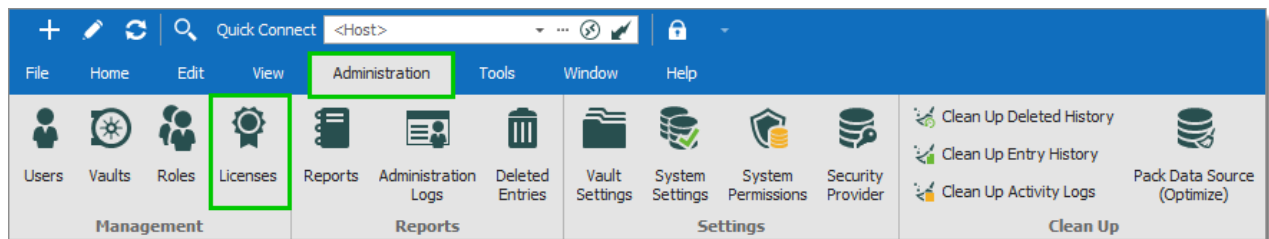
*Register Enterprise Edition*

## REGISTRATION FROM THE DATA SOURCE

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

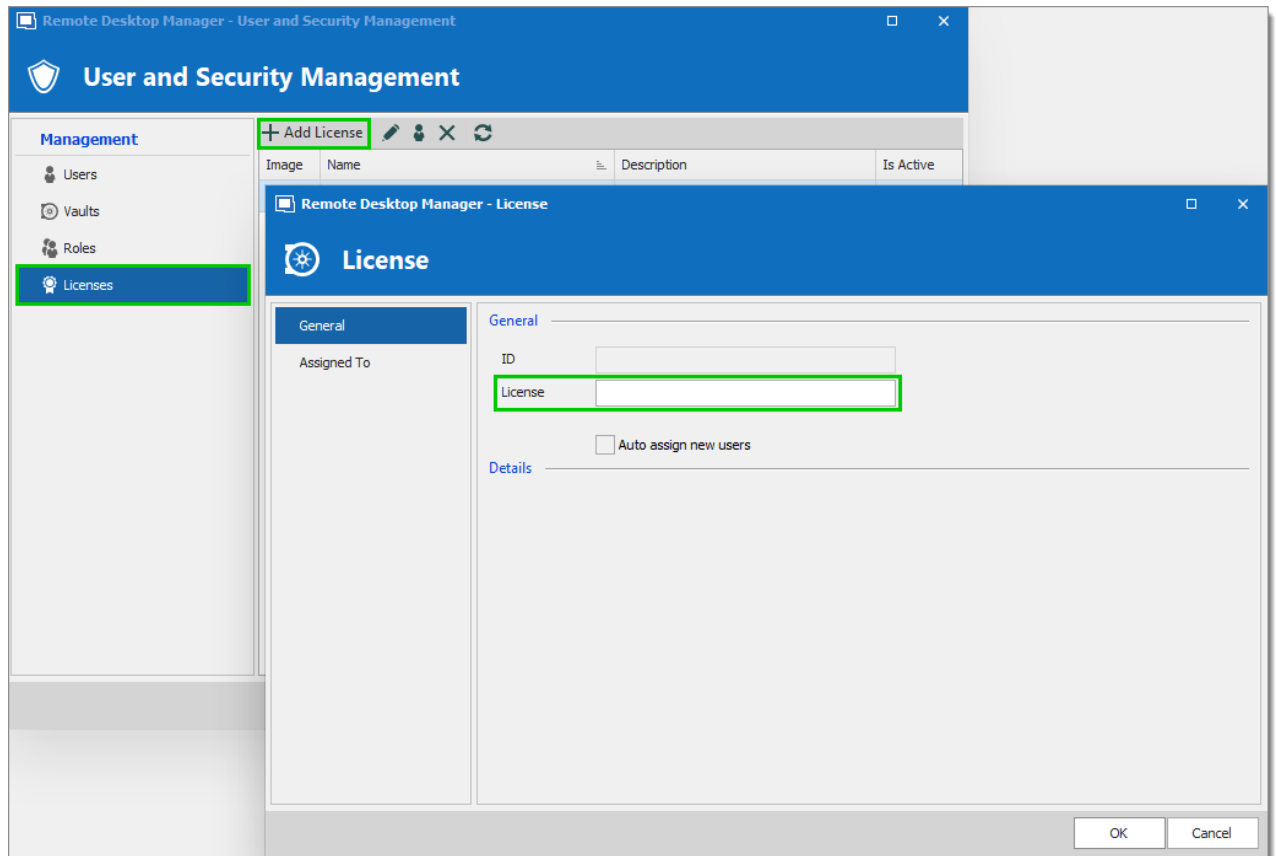
## FOR ADMINISTRATORS

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



*Administration - Licenses*

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



*User and Security Management - Add License*

#### 3.1.6.1.1 End of License

## DESCRIPTION

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

### PERPETUAL

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

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

## SUBSCRIPTION

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

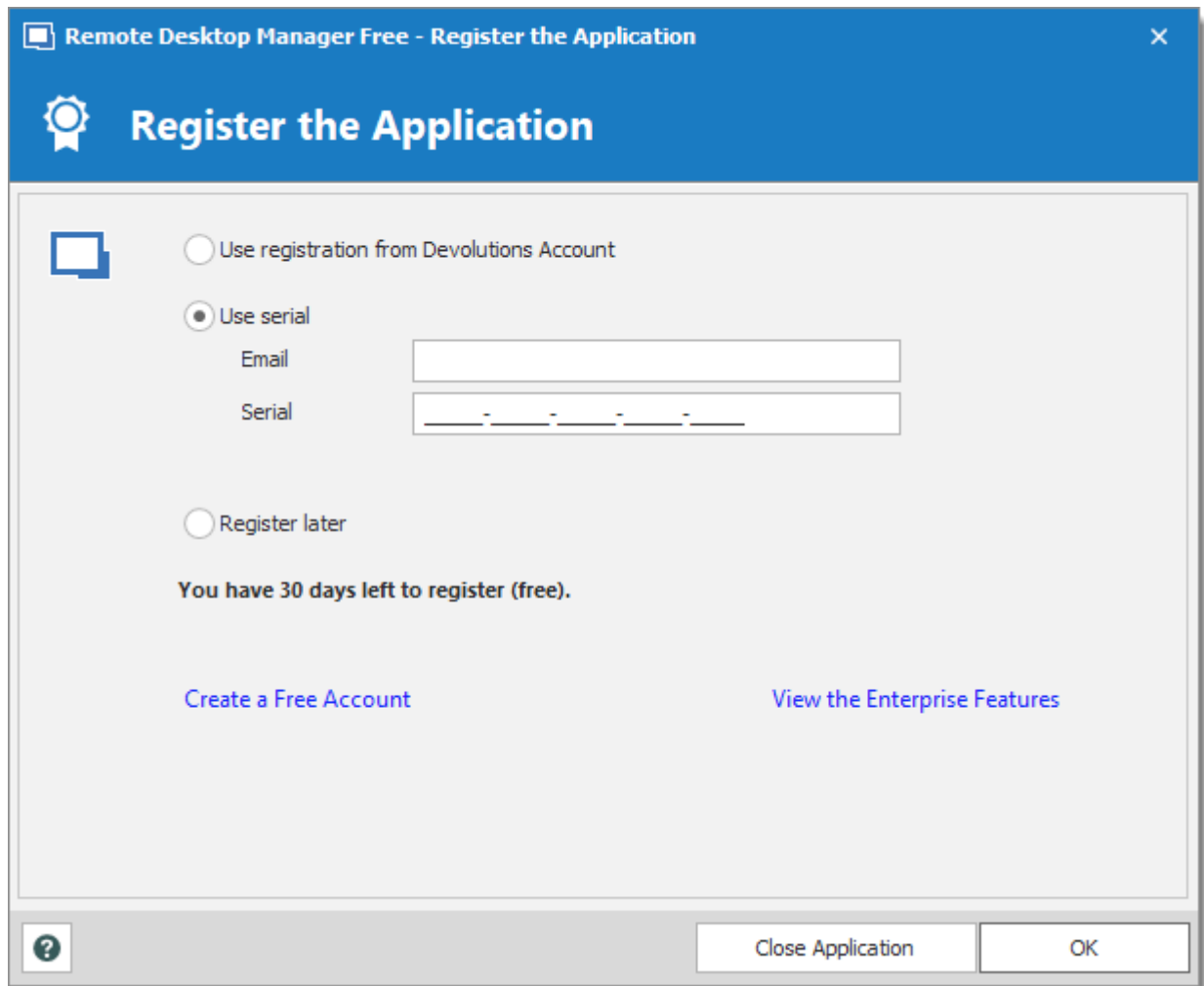
You need to renew your subscription agreement upon expiry. If you don't renew your subscription, access to your data will be limited.

### 3.1.6.2 Free Edition

## DESCRIPTION

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

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



*Register the Application*

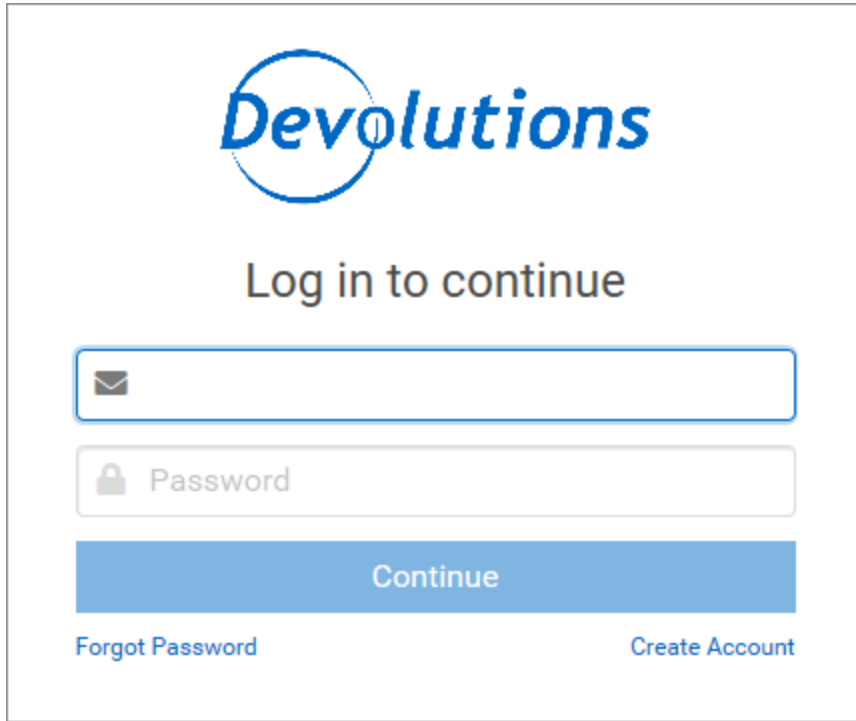
## USE REGISTRATION FROM DEVOLUTIONS ACCOUNT

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

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

To register your application follow these steps:

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

The image shows a login form for Devolutions. At the top is the Devolutions logo, which consists of the word "Devolutions" in a blue, italicized sans-serif font, with a blue circle around the "o". Below the logo is the text "Log in to continue" in a dark gray sans-serif font. There are two input fields: the first is for an email address, indicated by an envelope icon on the left, and the second is for a password, indicated by a lock icon on the left and the word "Password" in a light gray font. Below these fields is a large blue button with the word "Continue" in white. At the bottom of the form, there are two links: "Forgot Password" on the left and "Create Account" on the right, both in a blue sans-serif font.

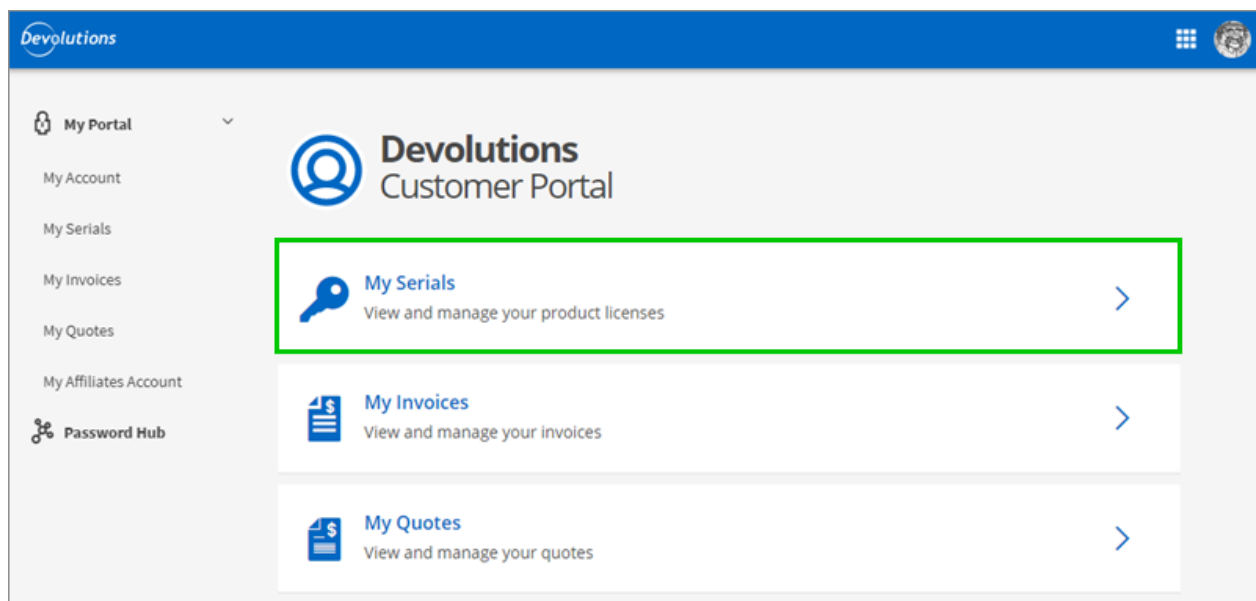
*Devolutions Account Login*

The license serial will be retrieved automatically.

## REGISTER THE FREE EDITION WITHOUT AN INTERNET CONNECTION

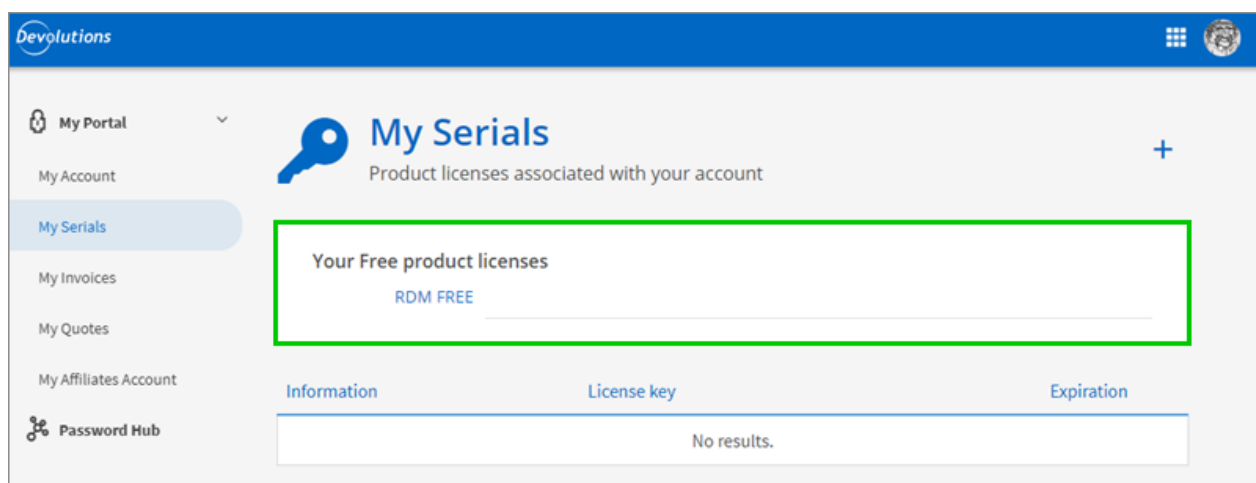
In the event that you need to register the application without an internet connection, the information must be entered manually. You will need the license serial from your [Customer Portal](#).

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.

Remote Desktop Manager Free - Register the Application

## Register the Application

☐ Use registration from Devolutions Account

☒ Use serial

Email

Serial

☐ Register later

You have 30 days left to register (free).

[Create a Free Account](#) [View the Enterprise Features](#)

Close Application OK

*Register Manually*

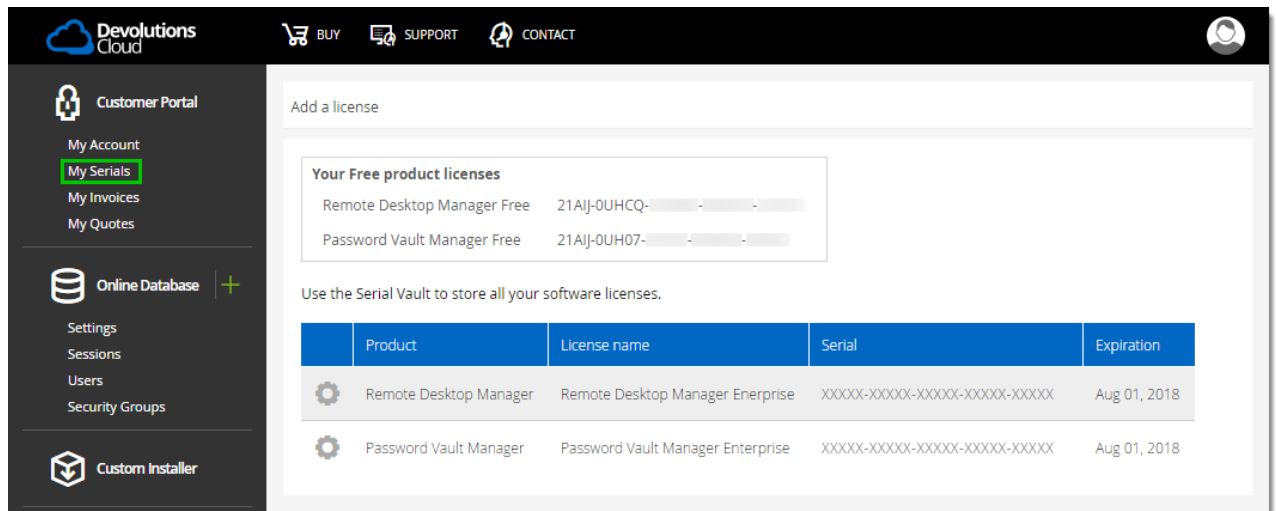
### 3.1.6.3 Register from Devolutions Portal

## DESCRIPTION

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

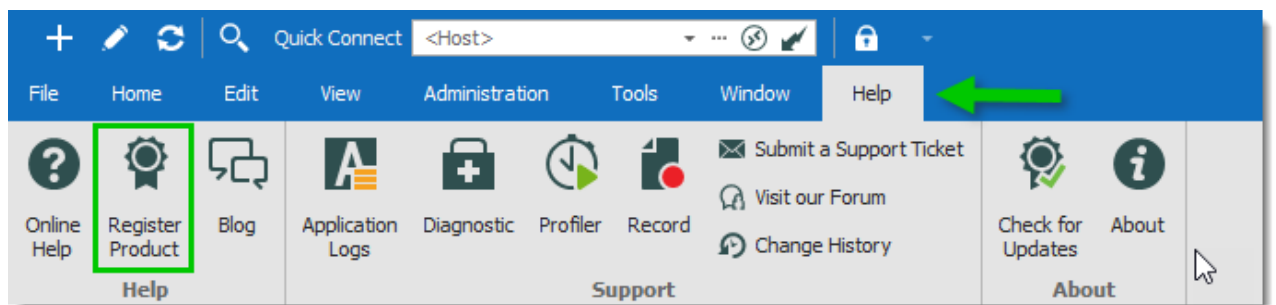
When creating a Devolutions Account a free license serial is provided for the free edition of Remote Desktop Manager. License serials purchased for the enterprise edition can be stored in the **My Serials** section of the Devolutions Customer Portal.





*Devolutions Customer Portal - My Serials*

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



*Register product*

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

Remote Desktop Manager Free - Register the Application

## Register the Application

☐ Use registration from Devolutions Account

☒ Use serial

Email

Serial

☐ Register later

You have 30 days left to register (free).

[Create a Free Account](#) [View the Enterprise Features](#)

Close Application OK

*Select the Registration*

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



**Devolutions**

Log in to continue

Username

Password

Continue

[Forgot Password](#) [Create Account](#)

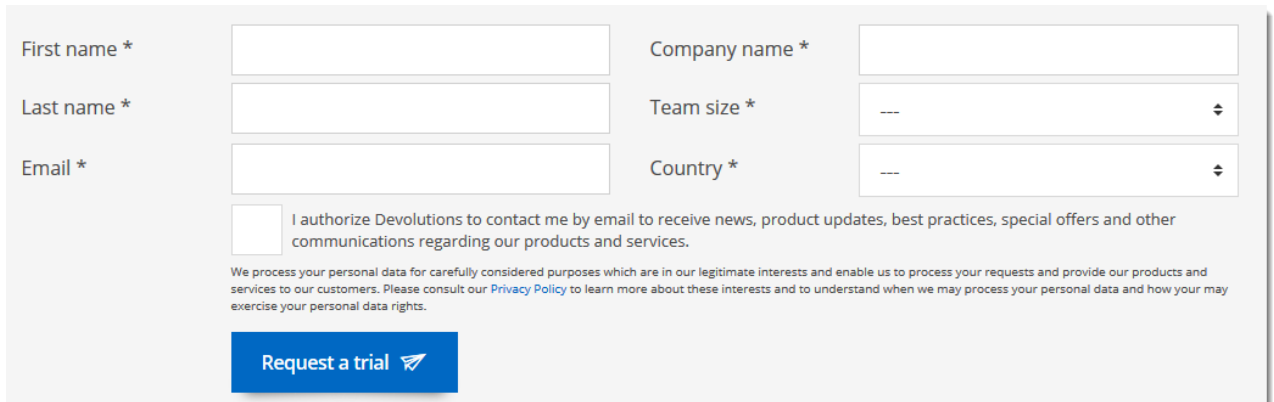
*Prompt for Devolutions Account credentials*

#### 3.1.6.4 Trial Request

### DESCRIPTION

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

Navigate to **Help – Register Product**, click on **Request Trial**, and fill in the form.



First name \*  Company name \*

Last name \*  Team size \*

Email \*  Country \*

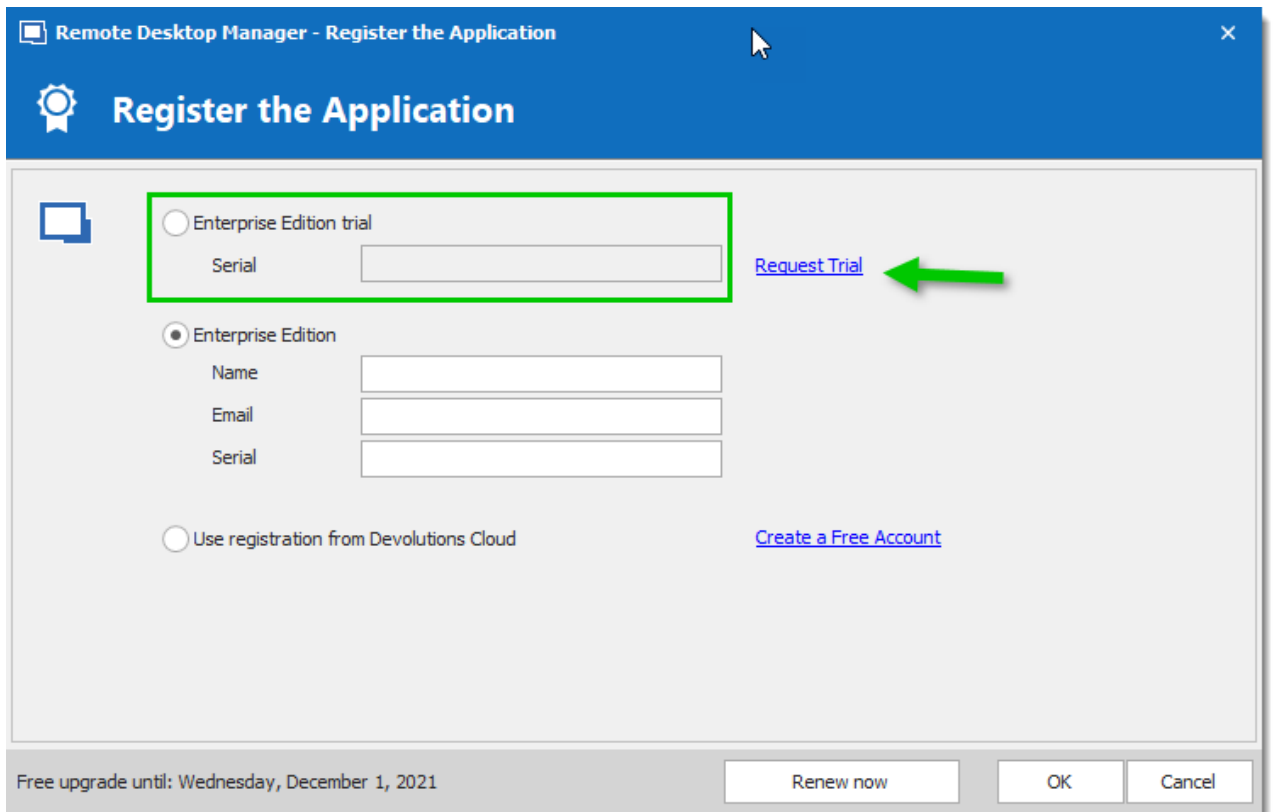
☐ I authorize Devolutions to contact me by email to receive news, product updates, best practices, special offers and other communications regarding our products and services.

We process your personal data for carefully considered purposes which are in our legitimate interests and enable us to process your requests and provide our products and services to our customers. Please consult our [Privacy Policy](#) to learn more about these interests and to understand when we may process your personal data and how you may exercise your personal data rights.

[Request a trial](#)

*Trial request for Remote Desktop Manager*

When the trial has been requested, an email containing the trial license serial is sent to the address provided in the form above.



Remote Desktop Manager - Register the Application

## Register the Application

☐ Enterprise Edition trial

Serial

[Request Trial](#)

☒ Enterprise Edition

Name

Email

Serial

☐ Use registration from Devolutions Cloud

[Create a Free Account](#)

Free upgrade until: Wednesday, December 1, 2021

[Renew now](#) [OK](#) [Cancel](#)

*Register Enterprise Edition Trial*

### 3.1.7 Remote Desktop Services

## DESCRIPTION

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



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

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



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



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

If you insist on using it, it is critical that each user is assigned a distinct port and that port be kept secret. An application key **must be set** as well. The first client application that starts will be able to use the port exclusively. ALL **Devolutions Web Login** calling on that port **will get the responses**, unless an application key is set.

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

## PROCEDURE

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

to protect against any modification by the users. Please refer to [Lock Data Source](#) for more information.



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

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

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

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



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

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

## WORKFLOW

### NEW USERS

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

## EXISTING USERS



A group policy exists to force the new configurations to be accepted automatically.

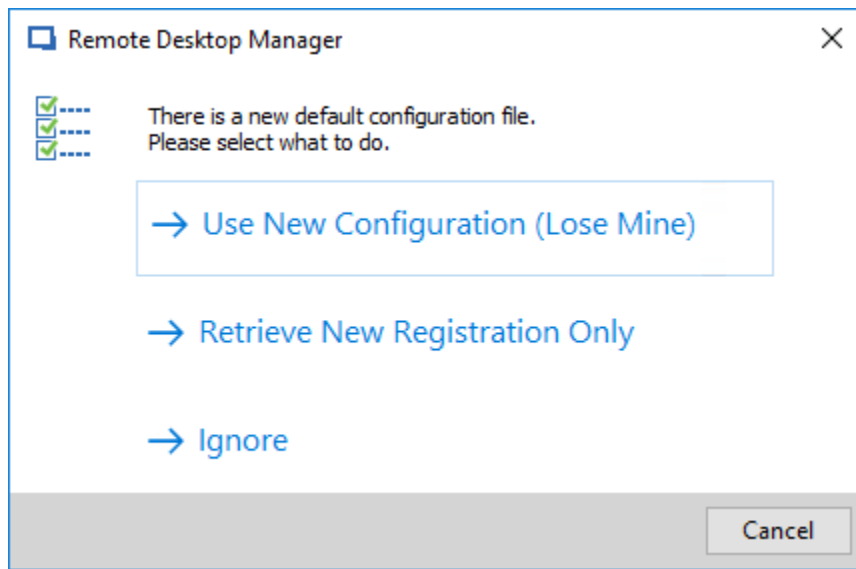


If the user chooses to ignore the new configuration file when presented with the dialog below, he will not be presented with the choice until the date/time of the *default.cfg* file has changed.



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

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



*New default.cfg detected*

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

## 3.2 Database Upgrade

### DESCRIPTION

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

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



The user performing the update must have administrative privileges on the underlying database. (**SYSDBA** or **DB\_OWNER**).



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



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

### STEPS

Follow these steps for a successful version update:

1. Ensure you are the sole user of the database during the upgrade process. If you environment allows for offline use, have your team switch to the offline mode; or have them switch to another data source.
2. Back up your database using the database tools.
3. Install the desired version of Remote Desktop Manager, using the [Portable \(USB\)](#) deployment model may be desirable if you are doing this on your personal workstation.
4. Open Remote Desktop Manager while logged on as a user with administrative rights. You must also be **SYSDBA** or **DB\_OWNER**.



5. You may be prompted with an upgrade message when your data source is accessed. If so accept the upgrade.  
**or**  
Using **File – Data sources**, locate your data source to upgrade and open its property window. Switch to the **Upgrade** tab, then click on **Update Database**
6. Wait for a confirmation dialog.
7. Close the dialog.
8. Ensure your Remote Desktop Manager application is currently using that data source.
9. Press CTRL-F5 to force a full refresh.
10. Validate the content and perform a check of the technologies that are critical in your environment.
11. Update the client software on all workstations.

### 3.3 Uninstall

#### INSTRUCTIONS

Remote Desktop Manager doesn't install anything in the Windows System directory. The only registry settings created are for the auto-run functionality and the installation path. As a result, Remote Desktop Manager can be uninstalled easily.

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

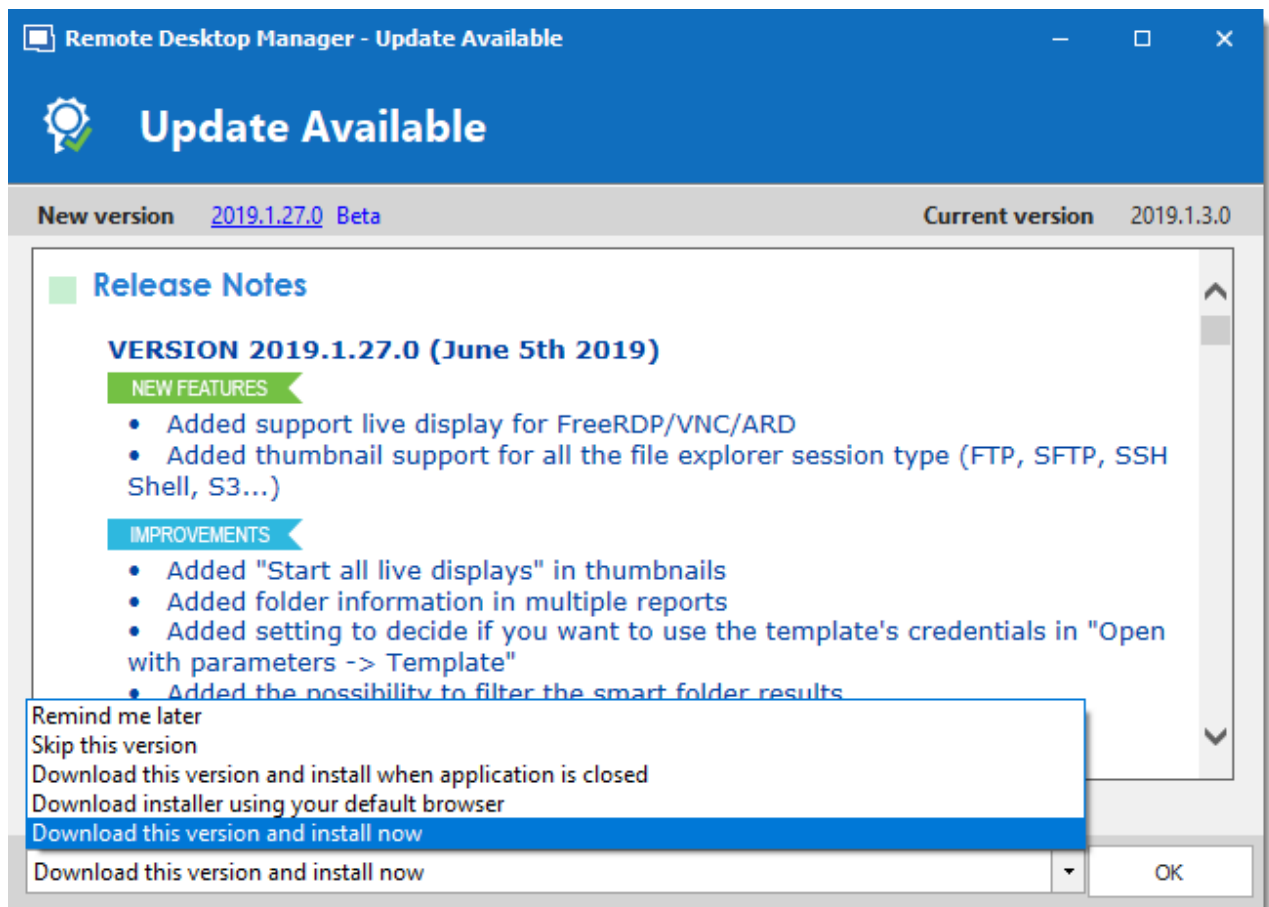
The application configuration files are saved in "%LocalAppData%\Devolutions\RemoteDesktopManager" or "%AppData%\Devolutions\RemoteDesktopManager" by default. It's possible that you may want to delete this folder for a complete uninstall.



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

### 3.4 Update

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



### Update

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

# User Interface

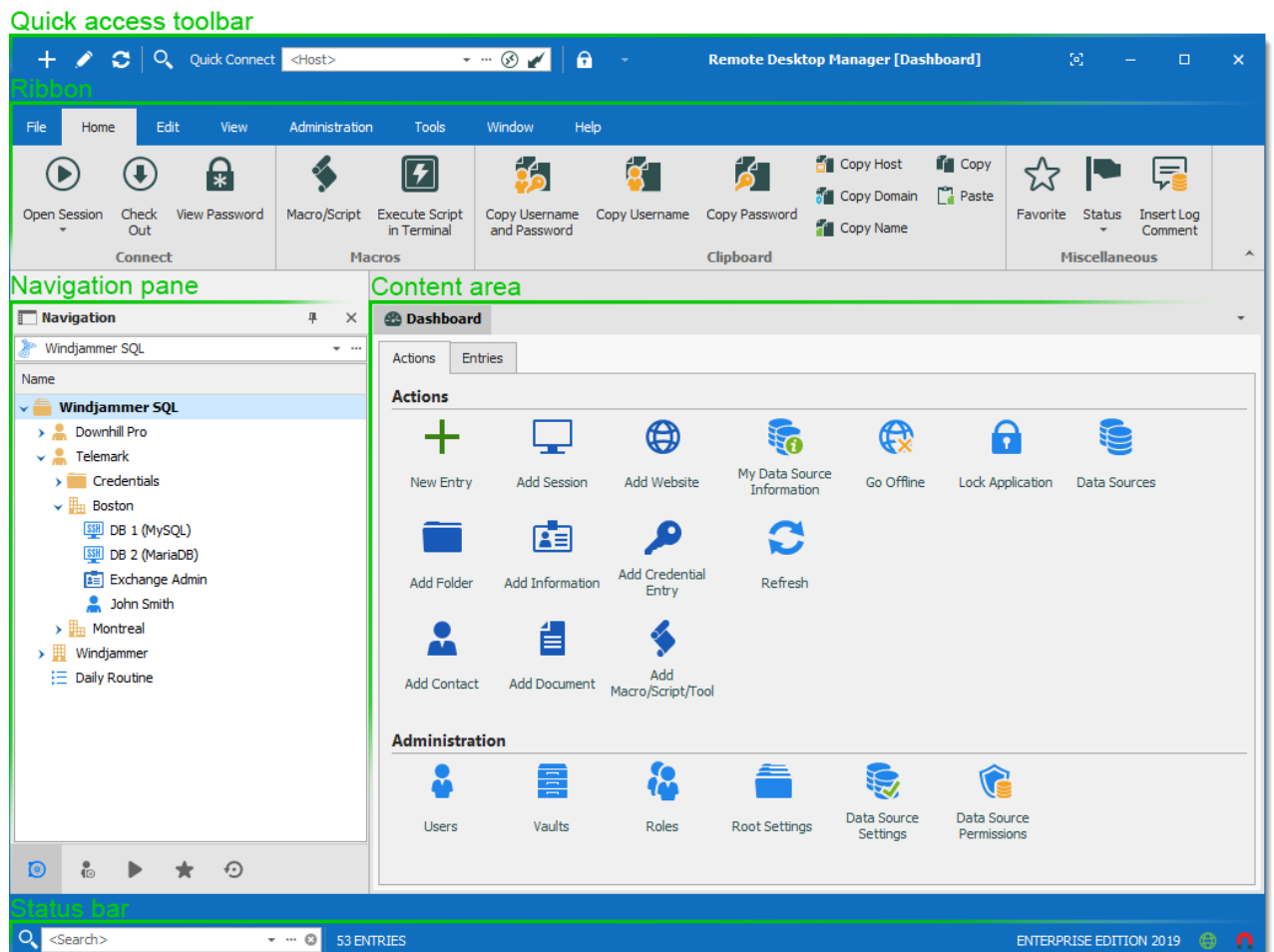
---

Part IV

## 4 User Interface

### 4.1 Main Screen

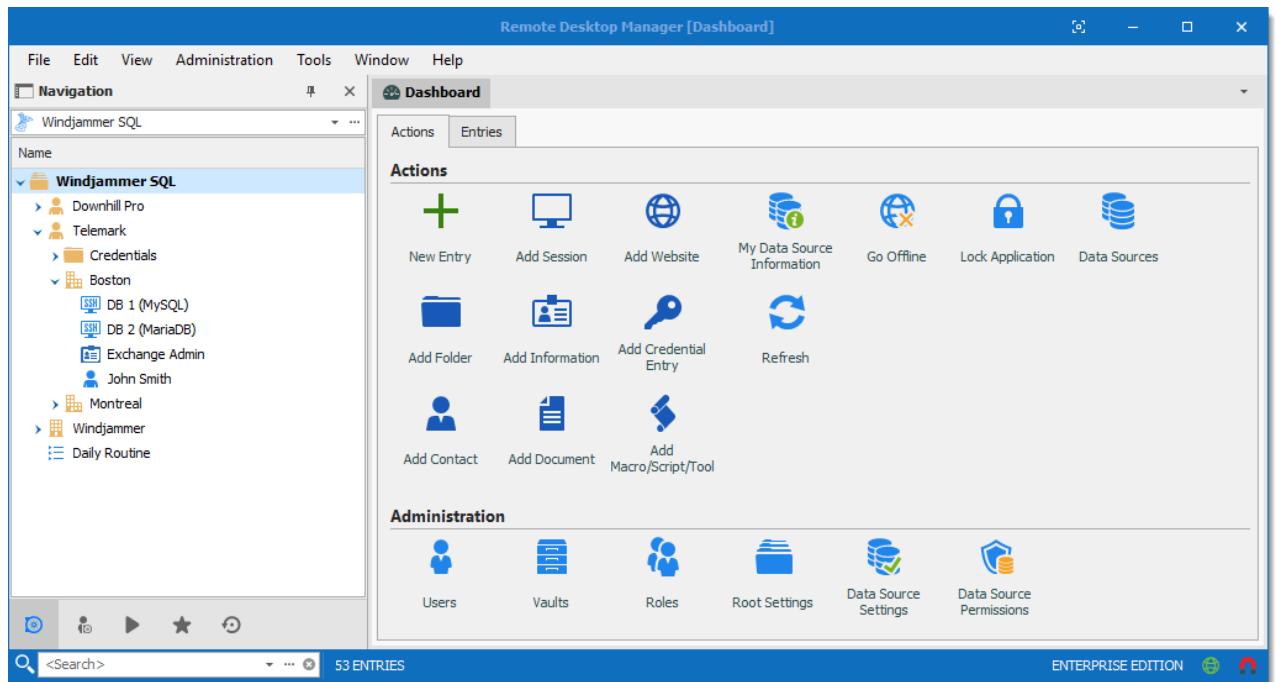
Illustrated below is the default Remote Desktop Manager main screen. Go to **File – Options – User Interface** to change the current style. We have various settings for you to customize your experience, such as different themes, shortcuts and more!



Overview of the default user interface

## MENU USER INTERFACE STYLE

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



*Menu user interface style*

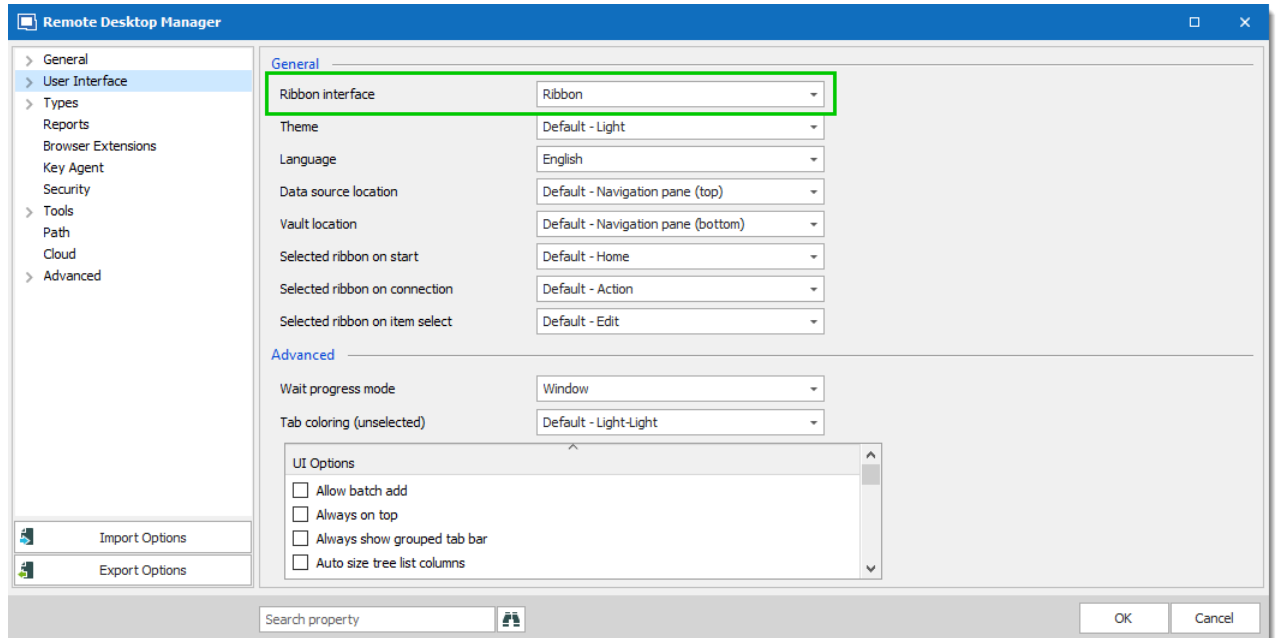
## 4.2 Style

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

- [Ribbon](#)
- [Menu](#)

## CONFIGURATION

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

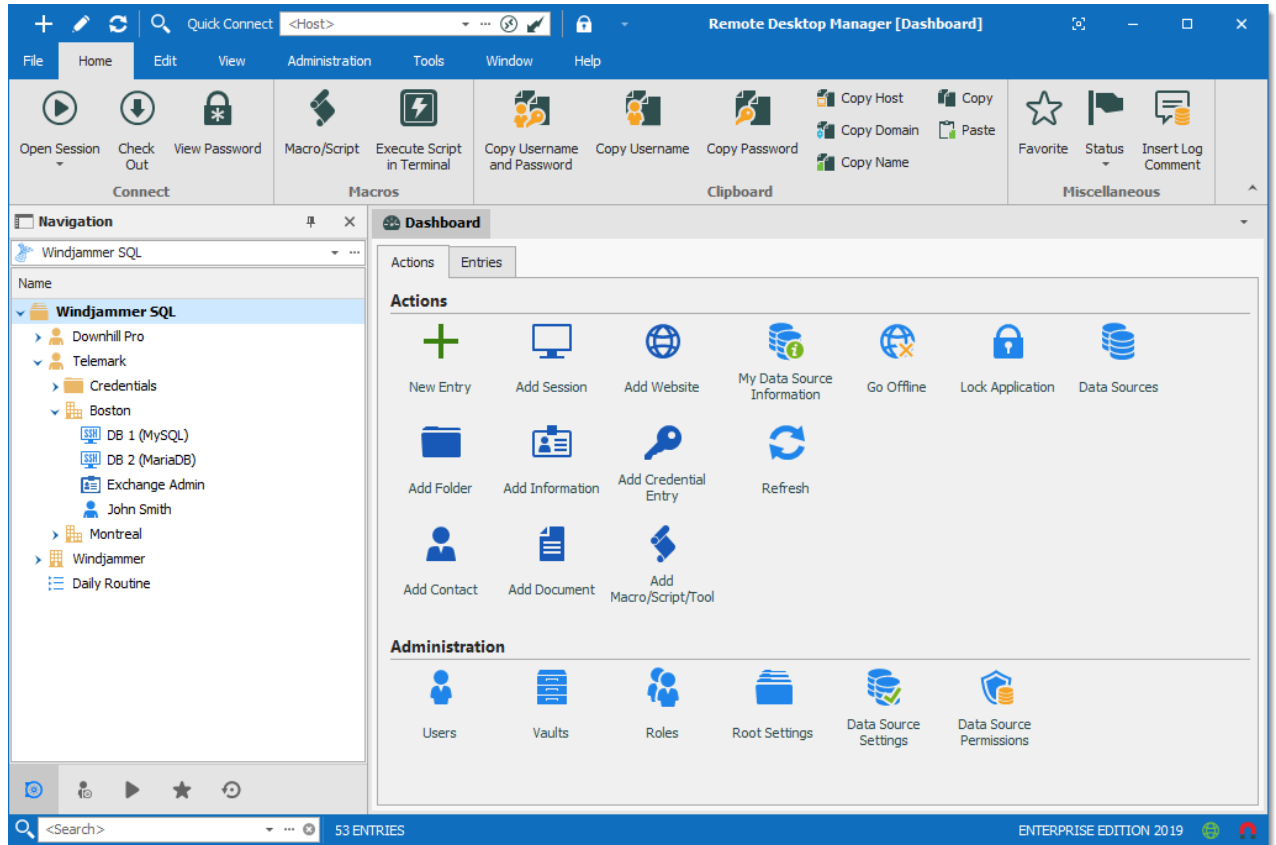


*Options - User Interface*

## EXISTING STYLES

### RIBBON

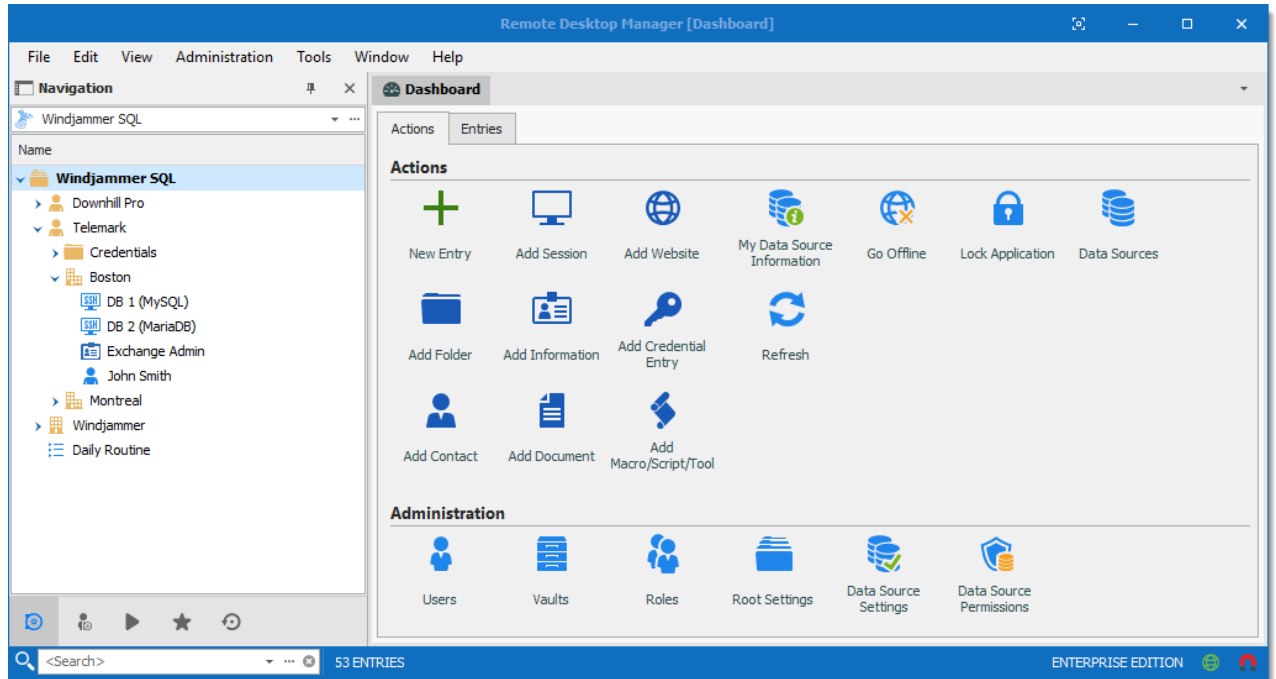
The latest style sports a ribbon. Icons and text makes it easy to explore features.



*Ribbon User Interface*

## MENU

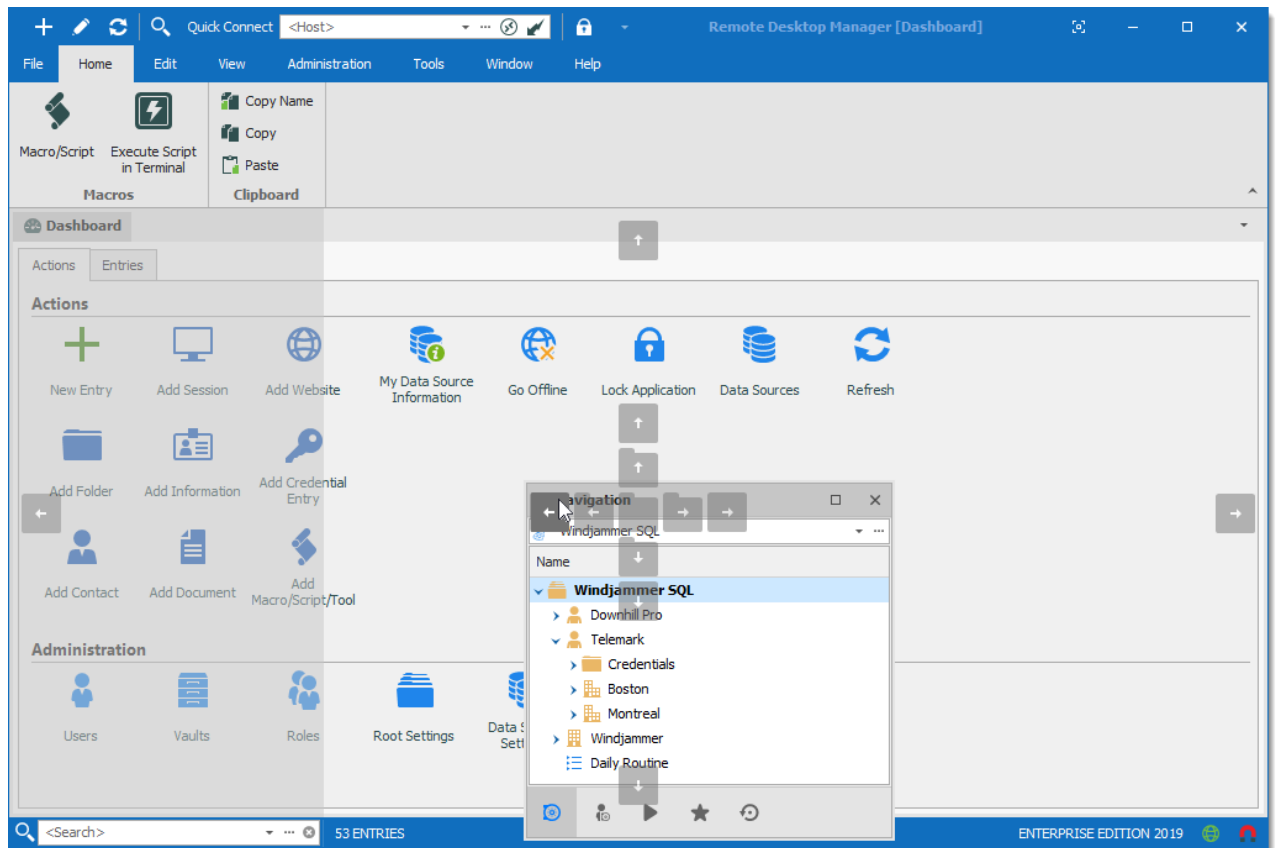
Previous generation style, it holds a standard menu to invoke commands.

*Default User Interface*

## CUSTOMIZING YOUR UI

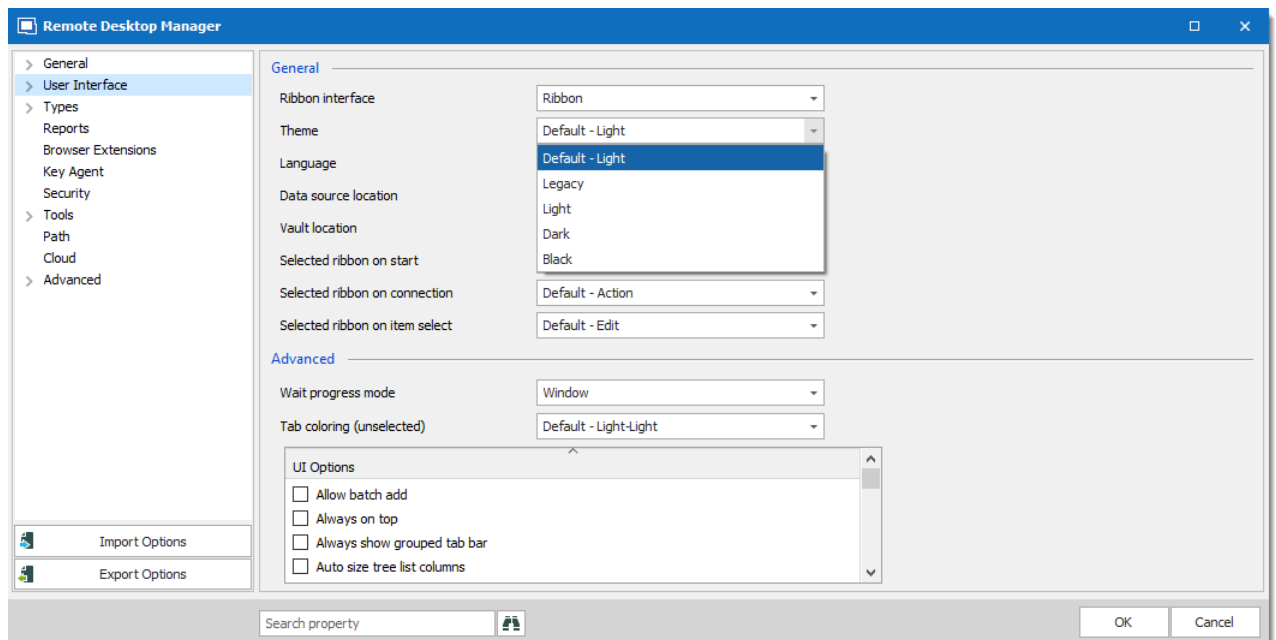
Customizable styles (Default Ribbon and Default Menu) have dockable areas that can be rearranged to your liking. Simply left-clicking then dragging the sub-components will result in drop zones appearing. This allows you to drop the sub component where you choose, even outside of the main form if you'd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





## 4.3 Theme

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

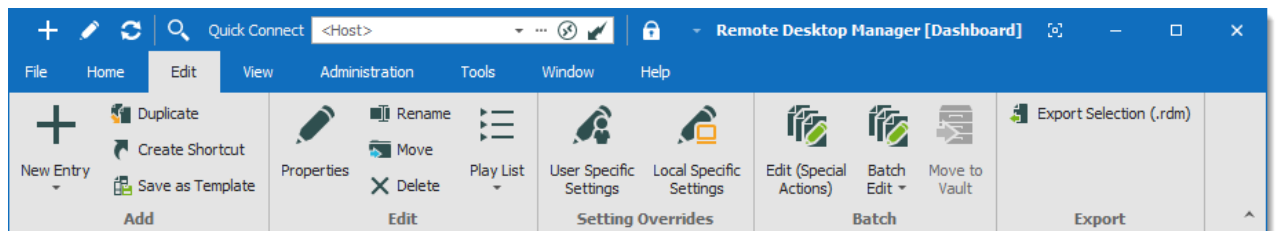


*User Interface - Theme*

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

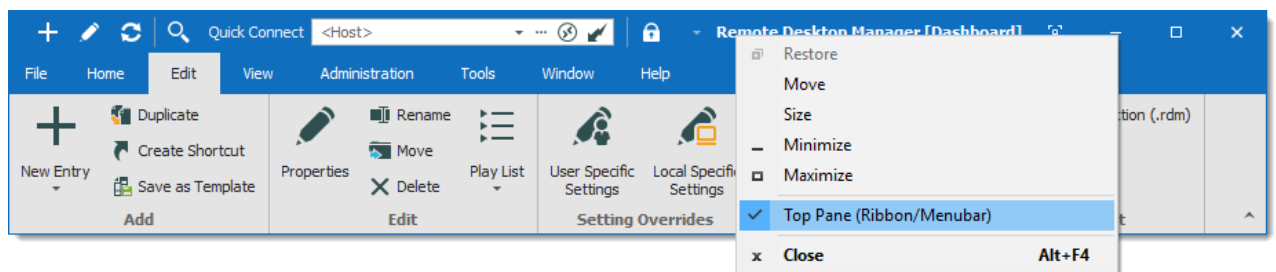
## 4.4 Top Pane

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

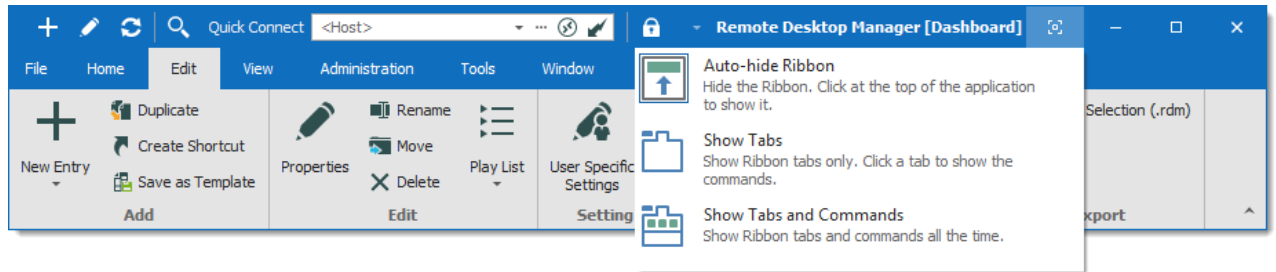


*Remote Desktop Manager top pane*

It can be hidden to maximize the work area.

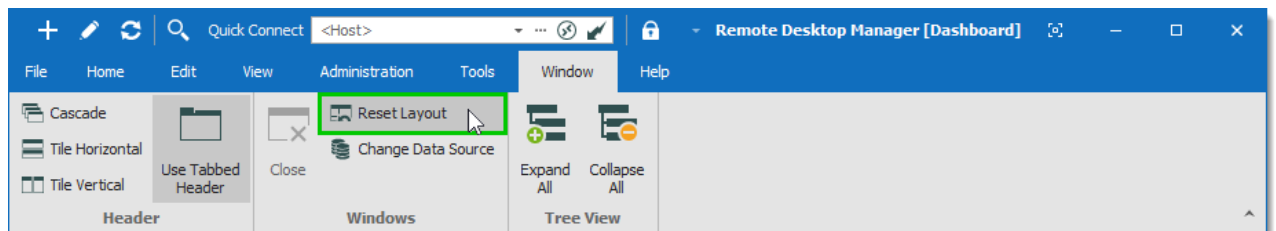


*Hide the top pane completely*



Hide the ribbon

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

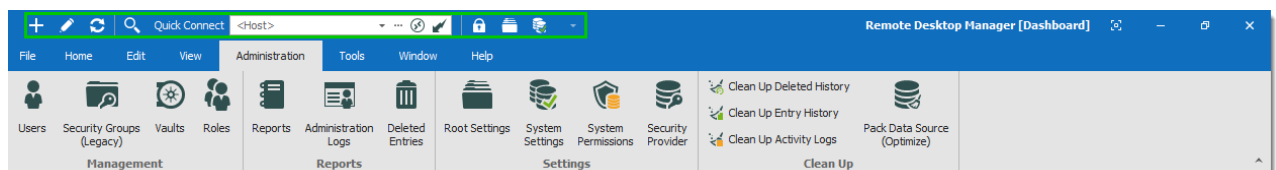


Windows – Reset layout

#### 4.4.1 Quick Access Toolbar

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

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



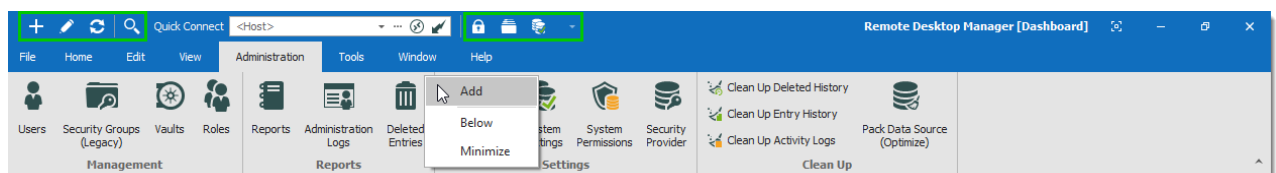
Quick Access Toolbar







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

## FAVORITE COMMANDS

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



*Favorite Commands*

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

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

## QUICK CONNECT CONTROL

Please refer to Quick Connect for a detailed description.

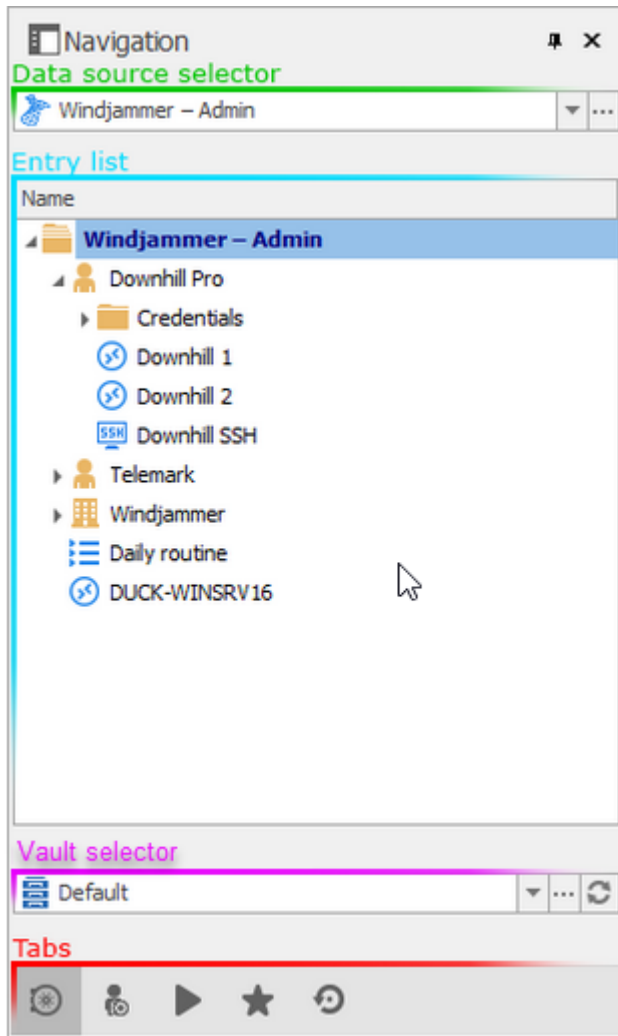
## LOCK APPLICATION COMMAND

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

## 4.5 Navigation Pane

### DESCRIPTION

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



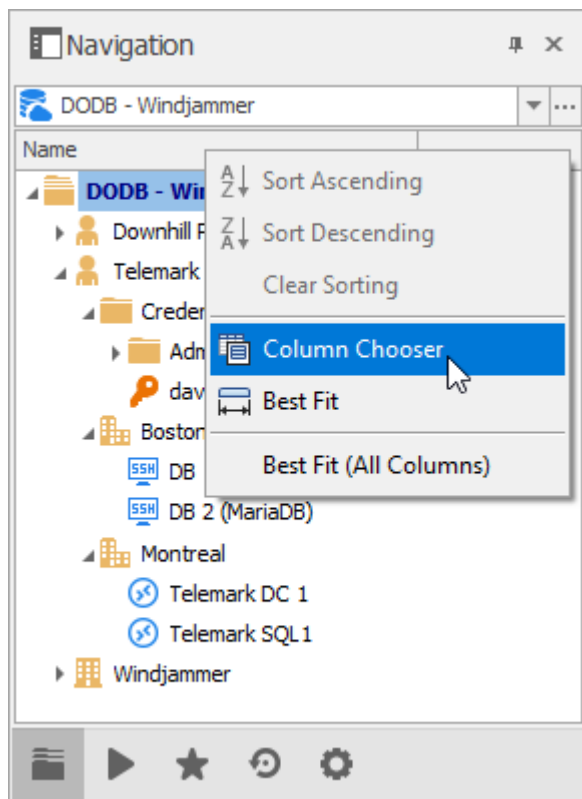
*Navigation Pane*

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

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

## COLUMN CHOOSER

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



*Navigation Pane – Column Chooser*

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

- Vault

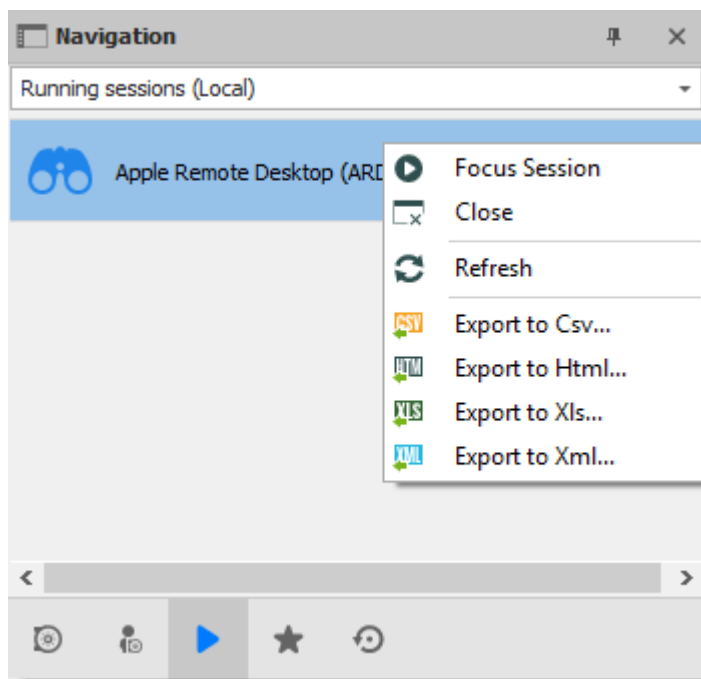
- [Private Vault](#)
- [Opened Sessions](#)
- [Favorite Entries](#)
- [Most Recently Used Entries](#)

## 4.5.1 Opened Sessions

### DESCRIPTION

The **Opened Sessions** tab shows currently running sessions by type, and for the local machine only. You can give the focus to an opened session by double-clicking it from the list. All of the embedded sessions are listed, and the external sessions will appear if Remote Desktop Manager is able to discover the specific type of session.

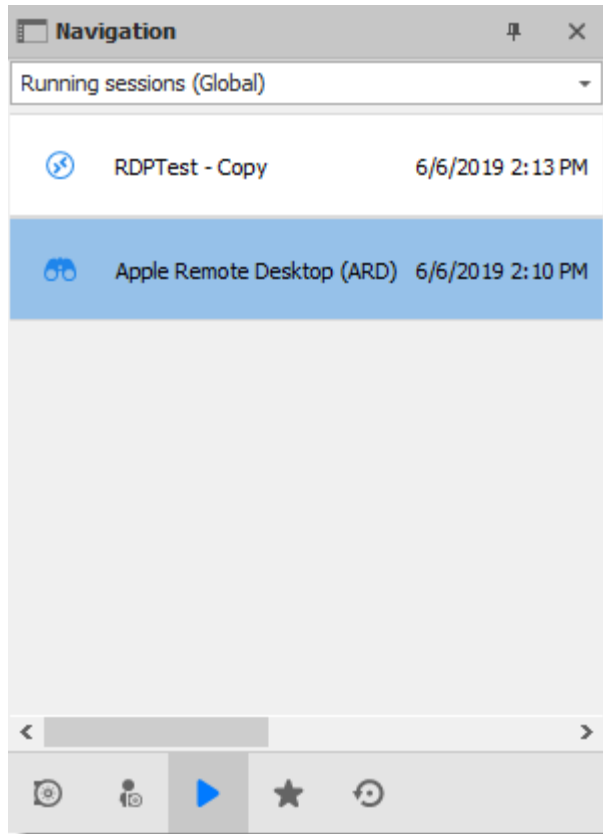
### LOCAL SESSIONS



*Local Opened Sessions*

### GLOBAL SESSIONS

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



*Global Opened Sessions*

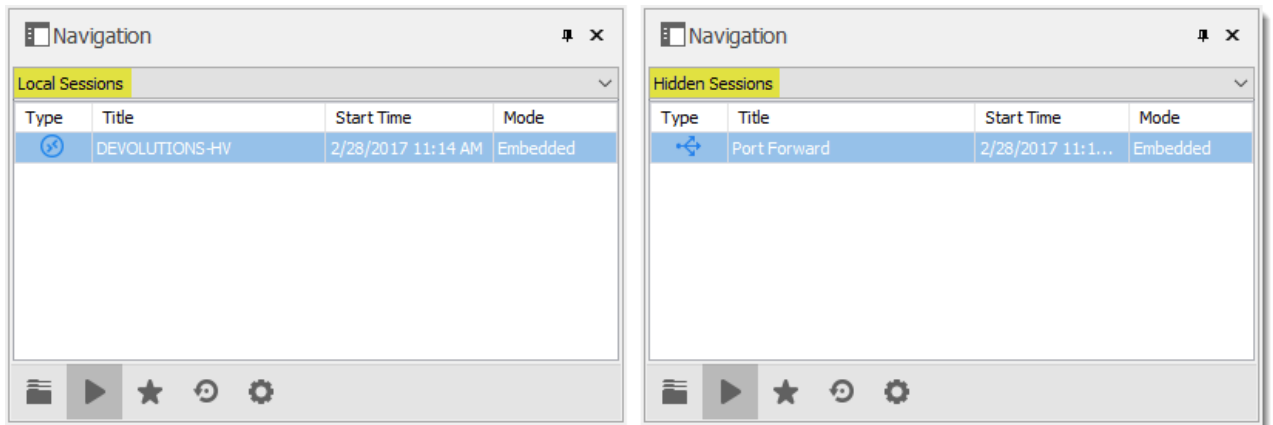
For many reasons beyond our control, it's possible for a session to be terminated without Remote Desktop Manager knowing that this has taken place. This can happen, for example, if Remote Desktop Manager isn't running when another application ends. As a result, any terminated session will remain listed in the log. You may manually mark it as closed via the contextual menu by selecting **Flag as Closed**.

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

## HIDDEN SESSIONS

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

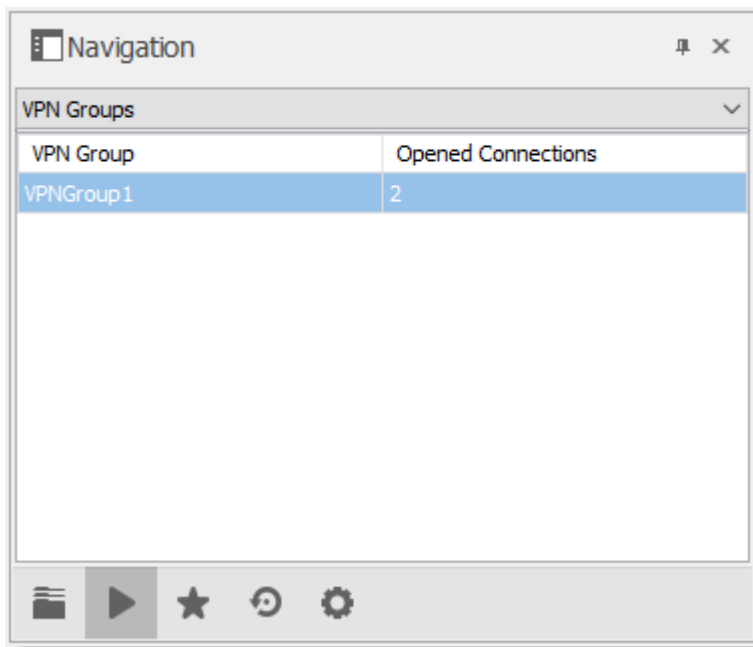




*Local Sessions Versus Hidden Sessions*

## VPN GROUPS

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



*VPN Groups*

## NOTES

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

- VPN sessions do not appear in the list.

## 4.5.2 Favorite Entries

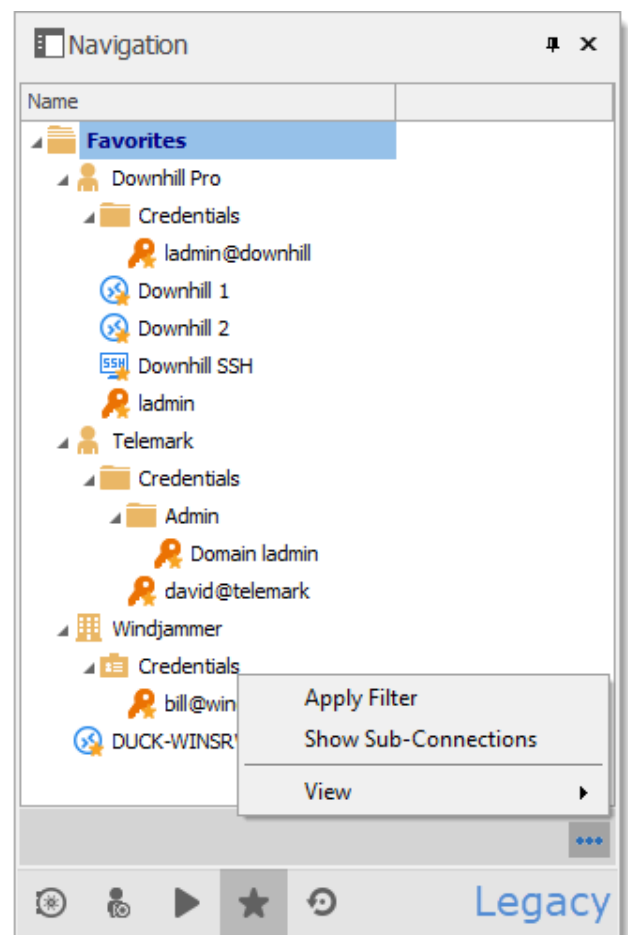
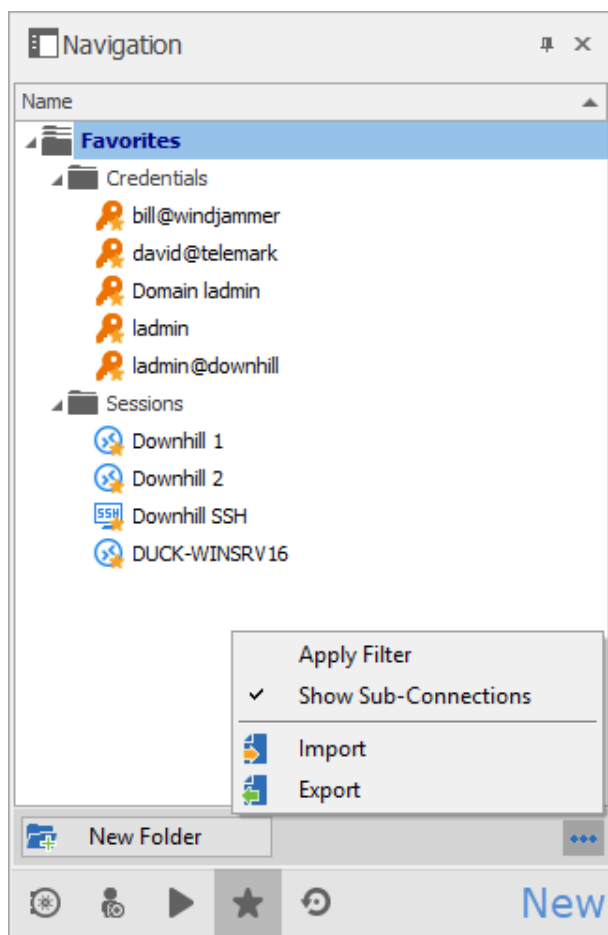
### DESCRIPTION

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

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



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

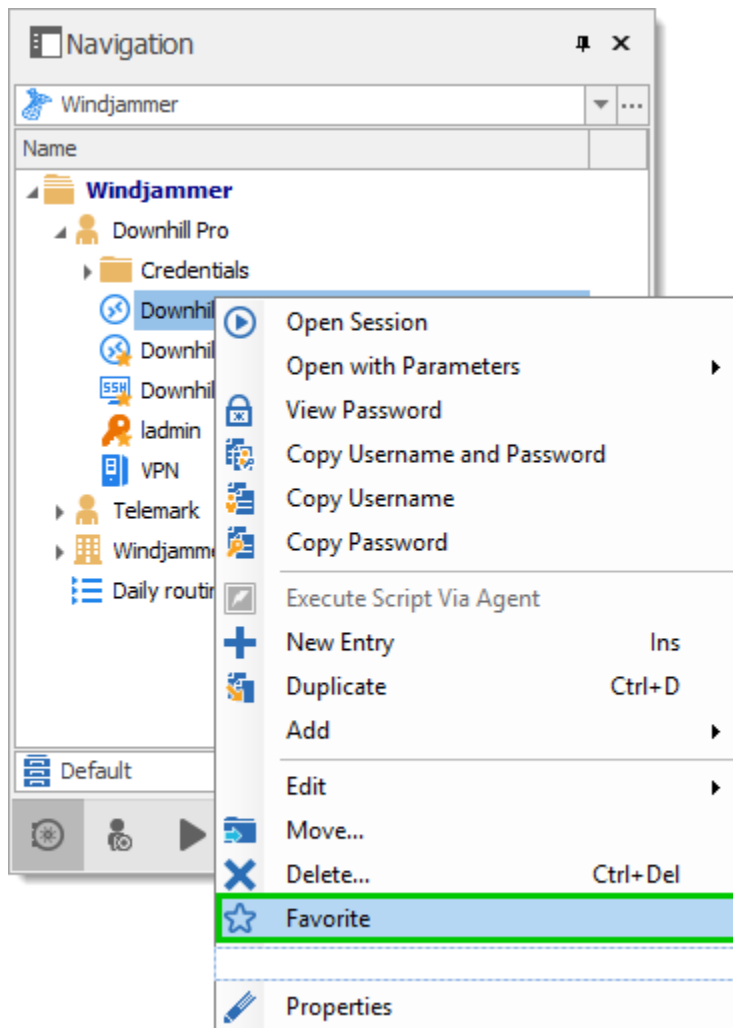


New and Legacy favorite UI

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

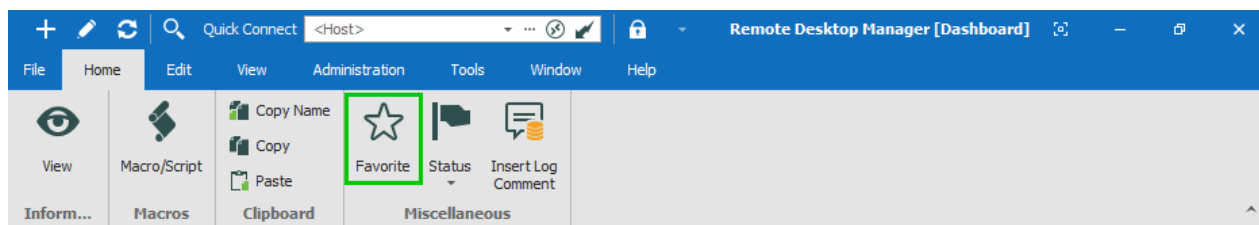
## FLAG AN ENTRY AS FAVORITE

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



*Flag an entry as favorite*

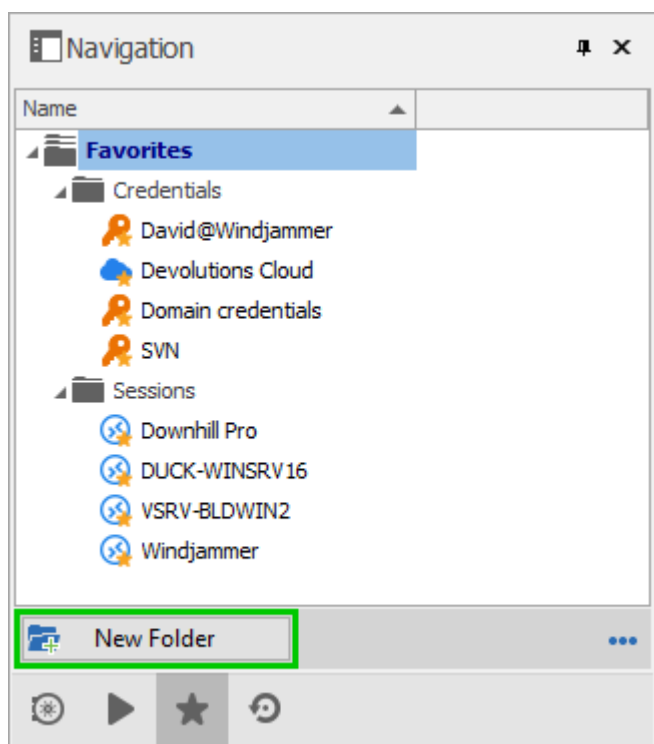
The same command is located in the ribbon **Home** tab in the **Miscellaneous** section.



*Home – Miscellaneous – Favorite*

## ORGANIZE THE FAVORITES

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



*Add folders to organize favorites*

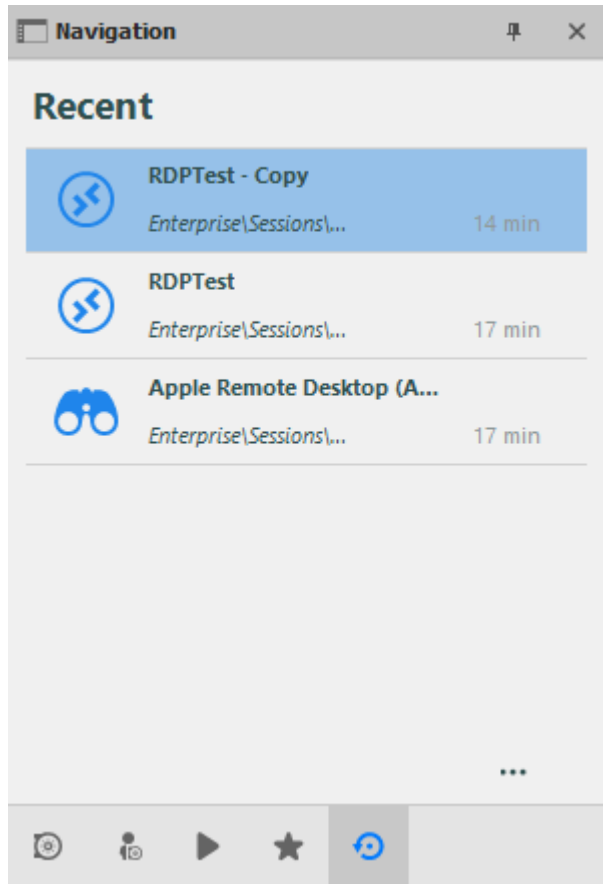
## ICON OVERLAY

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

### 4.5.3 Most Recently Used Entries

#### DESCRIPTION

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



*Most Recently Used Entries*

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

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

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

### 4.6 Content Area

#### DESCRIPTION

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

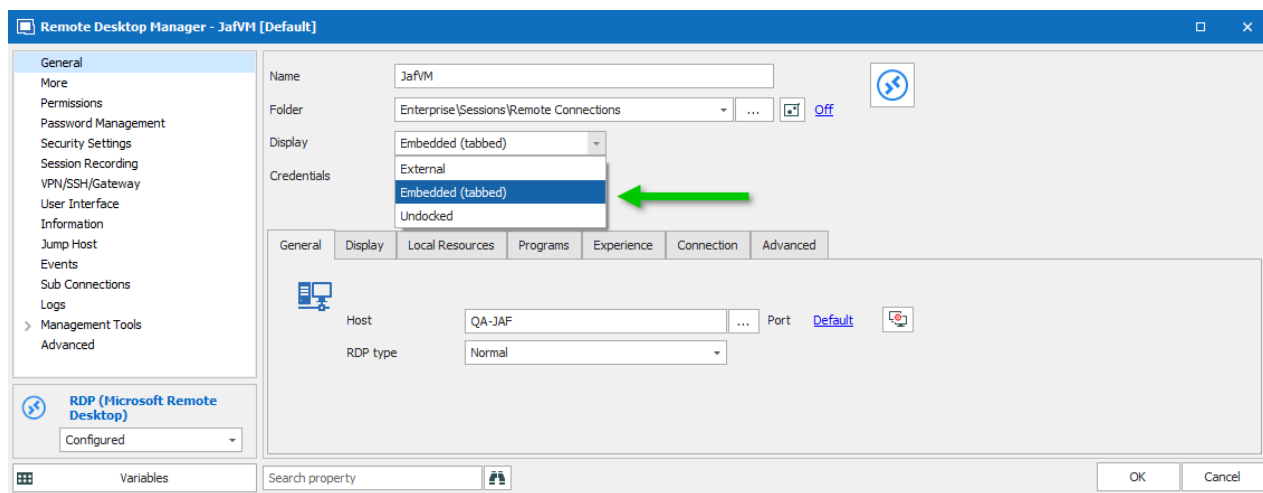
The options change depending on the entry:

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

#### 4.6.1 Embedded Sessions

### DESCRIPTION

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

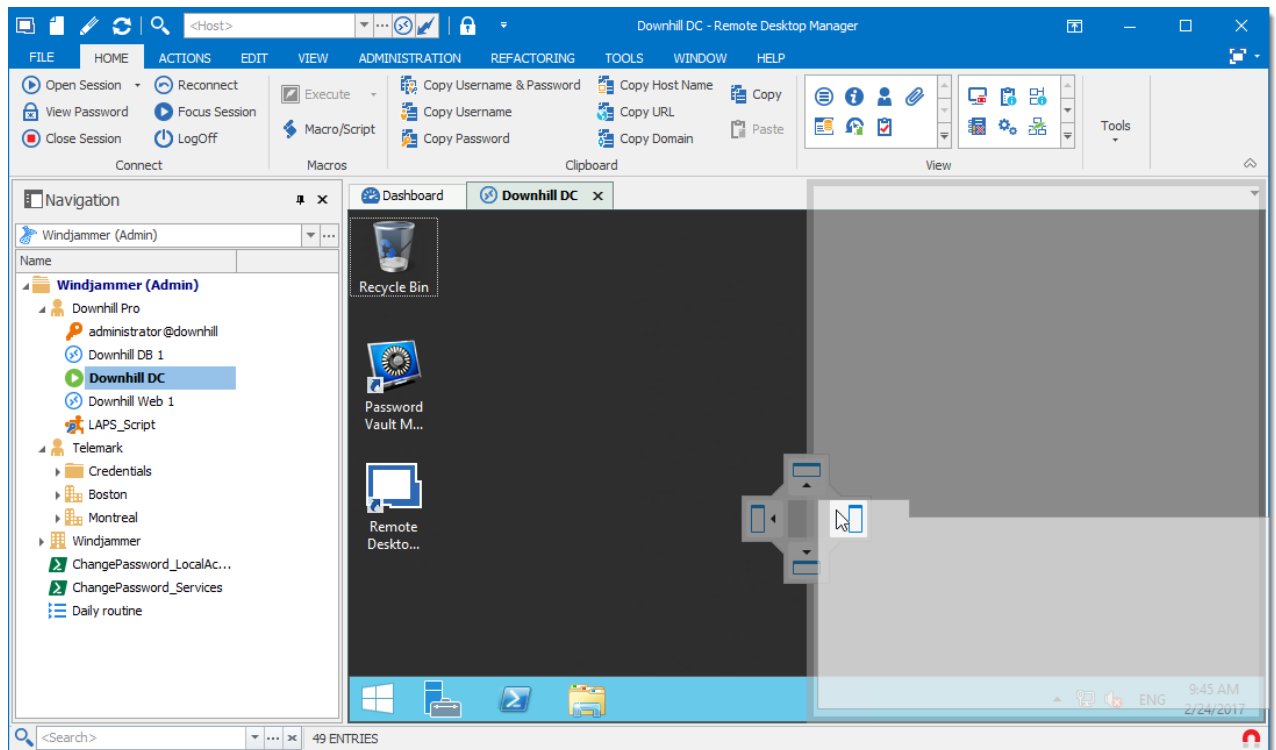


*Display Mode Settings*

### SPLIT WINDOWS

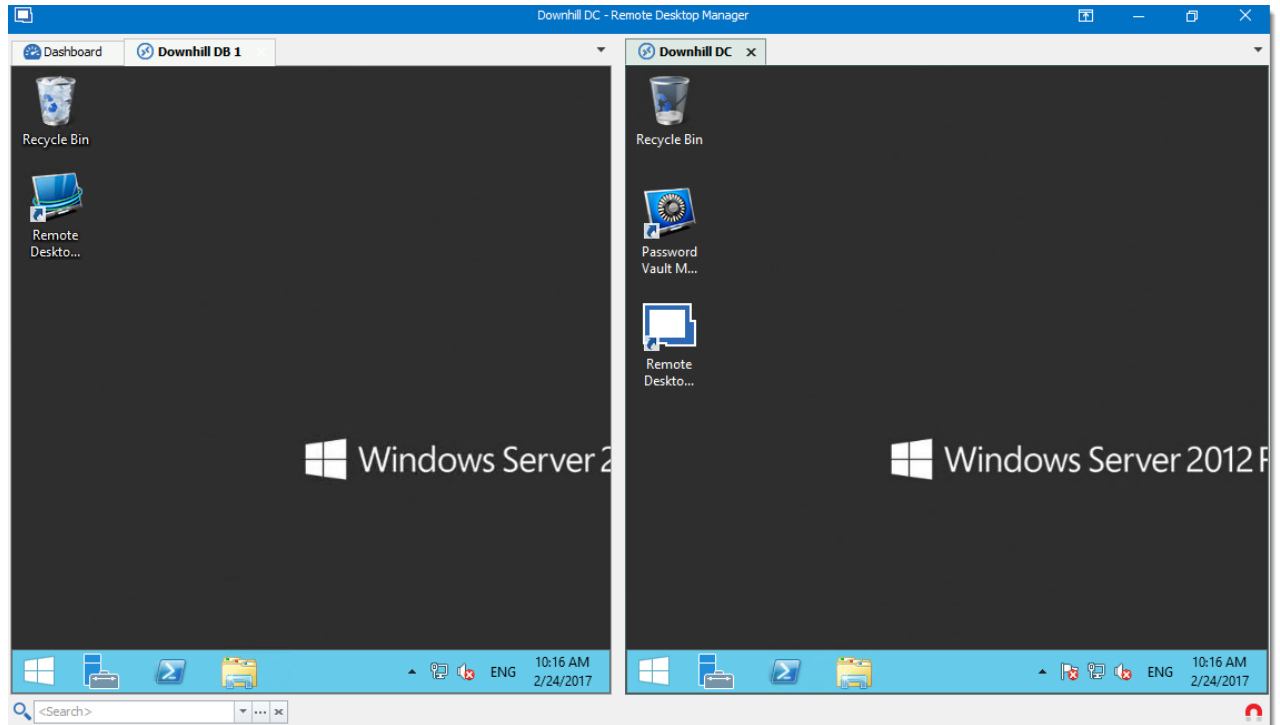
Within a Remote Desktop Manager embedded session is the option to display multiple tabbed windows simultaneously. As illustrated below, select and hold down on a tab and drag it

towards the center of the screen to access the four-sided directional control. Aim the directional control to anchor the tab to the top, bottom, left or right of the adjacent tab.



*Split Window - Drag And Drop*

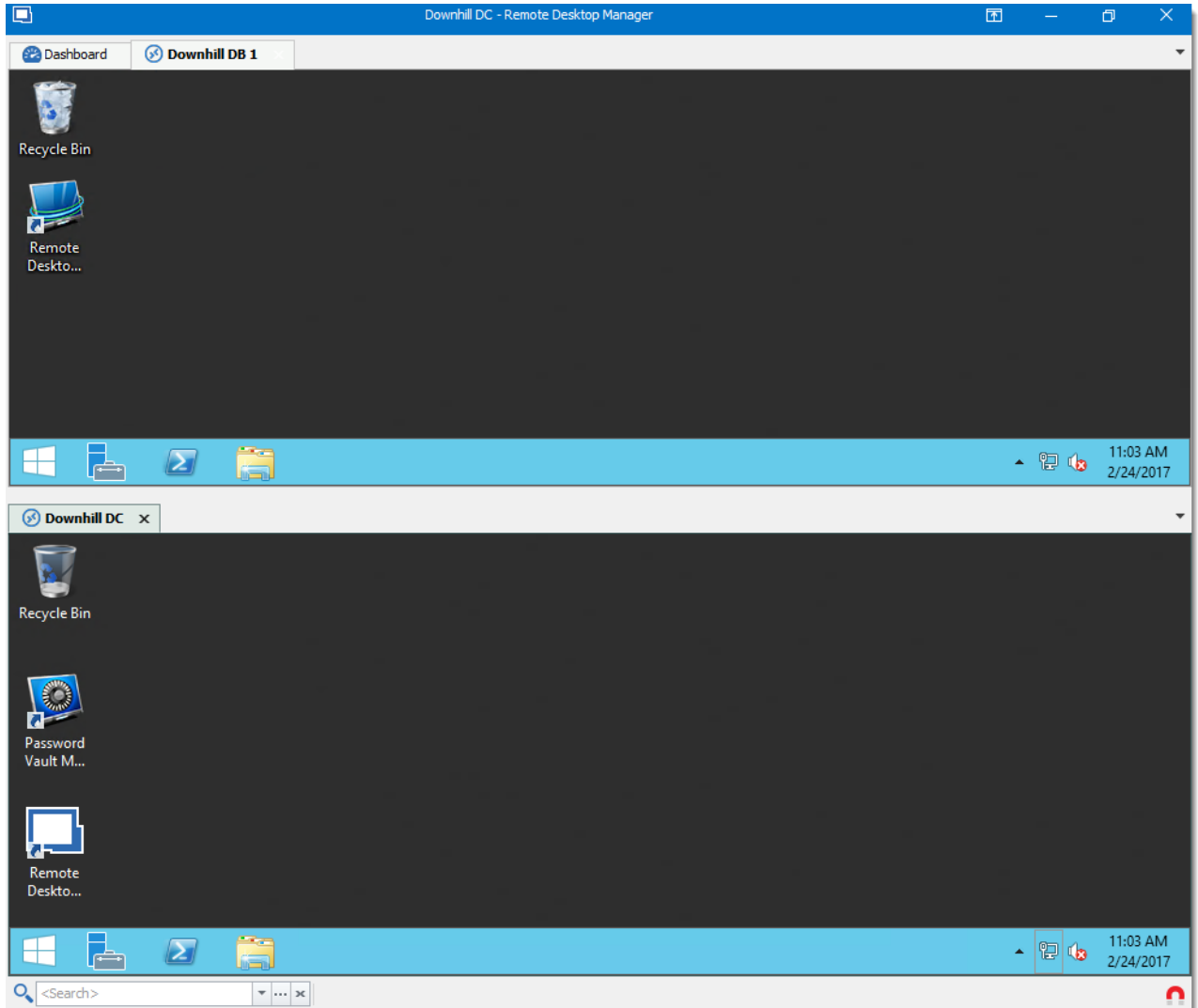
Below is an example of a side-by-side split window.



*Split Window - Side-By-Side*

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

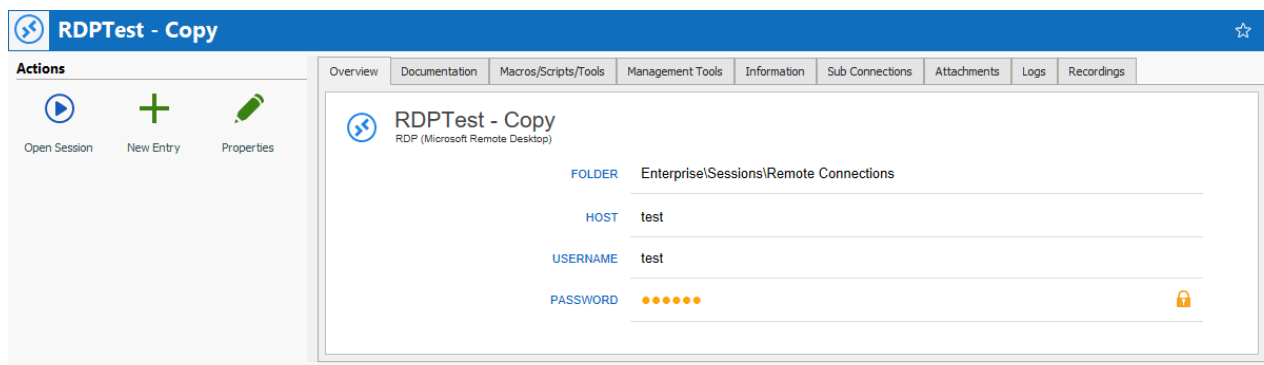




## 4.6.2 Dashboard

### DESCRIPTION

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



*Dashboard for credential entry*

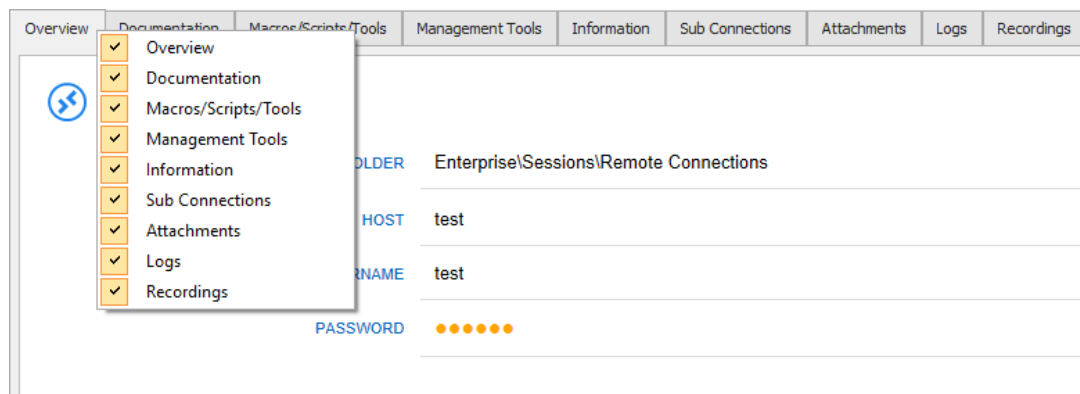
The different tabs available in the dashboard:

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



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

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



### 4.6.3 Wake-on-LAN

## DESCRIPTION

Wake-on-LAN is an Ethernet computer networking standard, which allows a computer to be turned on or woken up by a network message. This is an OS-agnostic feature that works by broadcasting a specially crafted “magic” packet at the data link layer. The target computer sits in a low-power state with only its network card switched on, and when it receives the magic packet, the network card “wakes up” the computer, powering it on and booting it up.

Wake-on-LAN is supported in the Enterprise edition of Remote Desktop Manager. Plus, the destination motherboard must support it, and it must be enabled. The computer must also be in the local area network (LAN) and not connected in a VPN.

An important thing to note is that Wake-on-LAN operates below the IP level. This means that the sending machine needs to be on the LAN, so we cannot send them over remote IP-based connections, such as over SSH or VPN. WOL broadcasts packets to the target computer over UDP. You can configure which port it uses, the default is 9. If you want to wake up a machine on a different subnet, your router must forward UDP port 9, or whatever you change the port assignment to. Most users do not have to configure their router or worry about this.

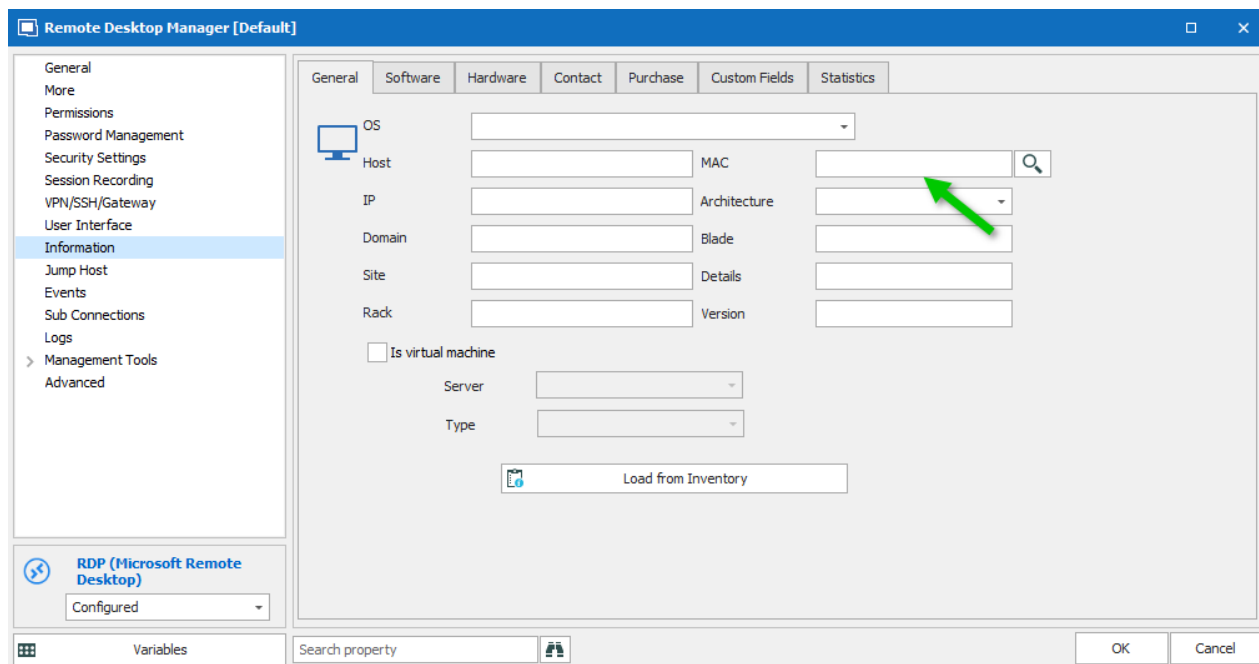
## ENABLING WAKE-ON-LAN

The first step is to check that your computer supports Wake-on-LAN. There’s a few things to check:

- Your network card must support Wake-on-LAN
- Your power supply must support Wake-on-LAN
- Wake-on-LAN must be enabled in BIOS
- Your router must be configured to forward broadcast packets
- Your OS must be configured to enable Wake-on-LAN

## CONFIGURE REMOTE DESKTOP MANAGER

You must add a valid MAC address (Media Access Control address) in the session's configuration. The input field can be found in the **Information** tab and in the **Computer** child tab. The field name is MAC.



*Session configuration - Wake-on-LAN*

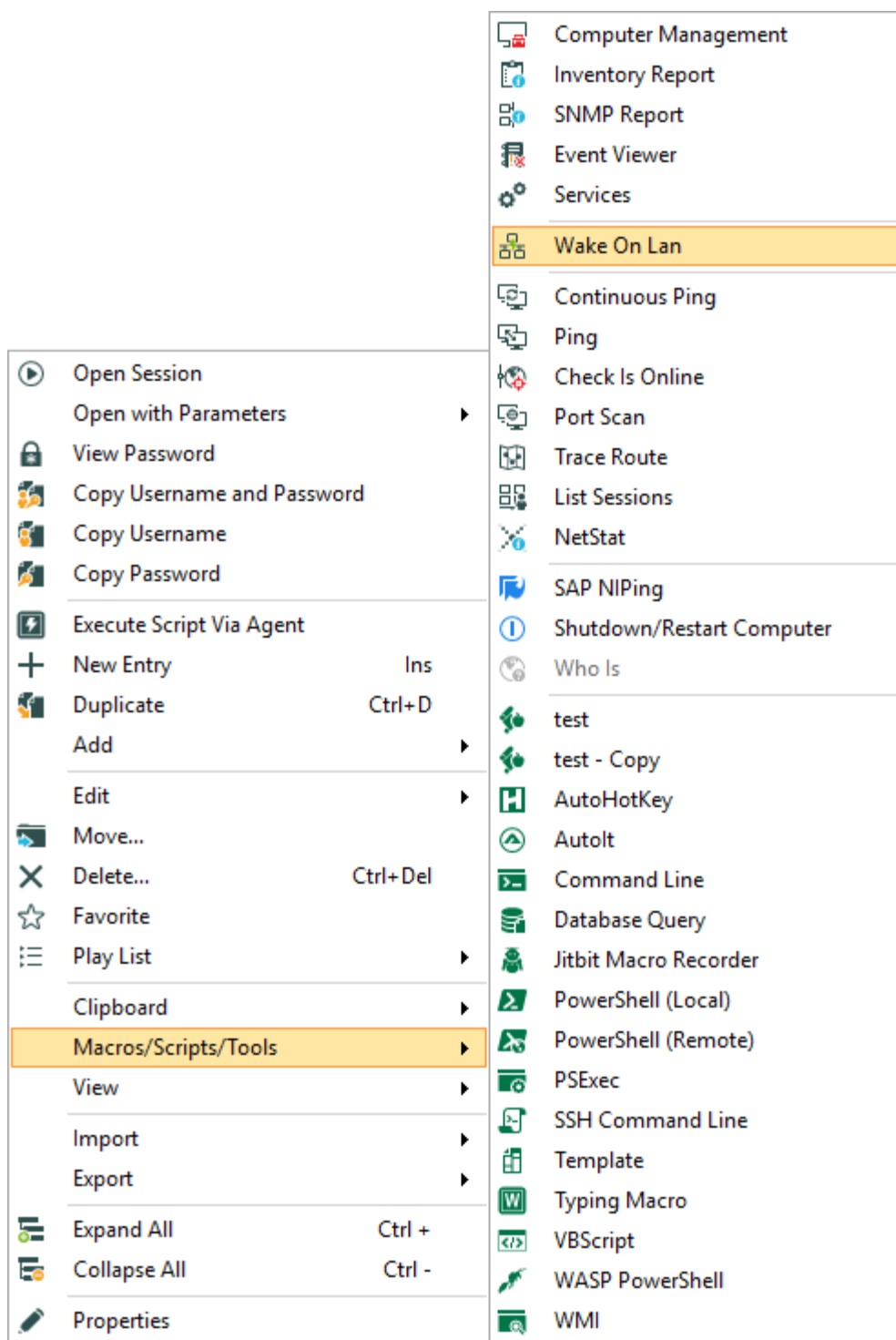
You can use the Discover button to automatically determine the MAC address. If this is unsuccessful, you will need to enter it manually.

## ABOUT THE MAC ADDRESS DISCOVERY

The discovery process will initially attempt using the ARP protocol. This is fast and does not require authentication, but there are requirements on the network aspect that may not be met. If ARP was not successful, another attempt is made using WMI. This is slower and requires authentication. RDM will use the credentials as configured in entry properties, or the credentials entered in the session tools tab (custom credentials or Credential repository).

## USE WAKE-ON-LAN

If the settings are correctly configured, you can invoke the Wake-on-LAN from the session's context menu, which can be found in the **Macros/Scripts/Tools - Wake-on-LAN** menu.



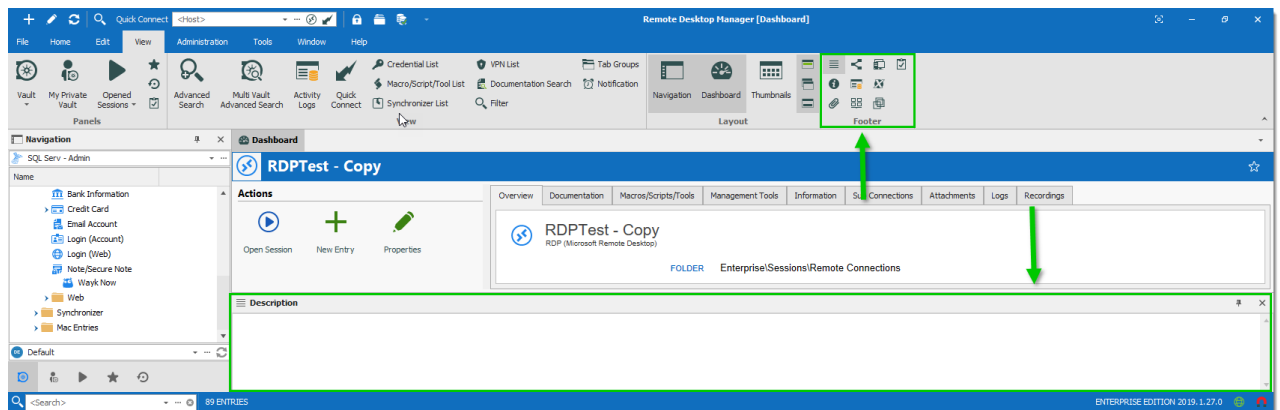
Session tools - Wake-on-LAN

## 4.7 Panes (Footer)

### DESCRIPTION

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

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

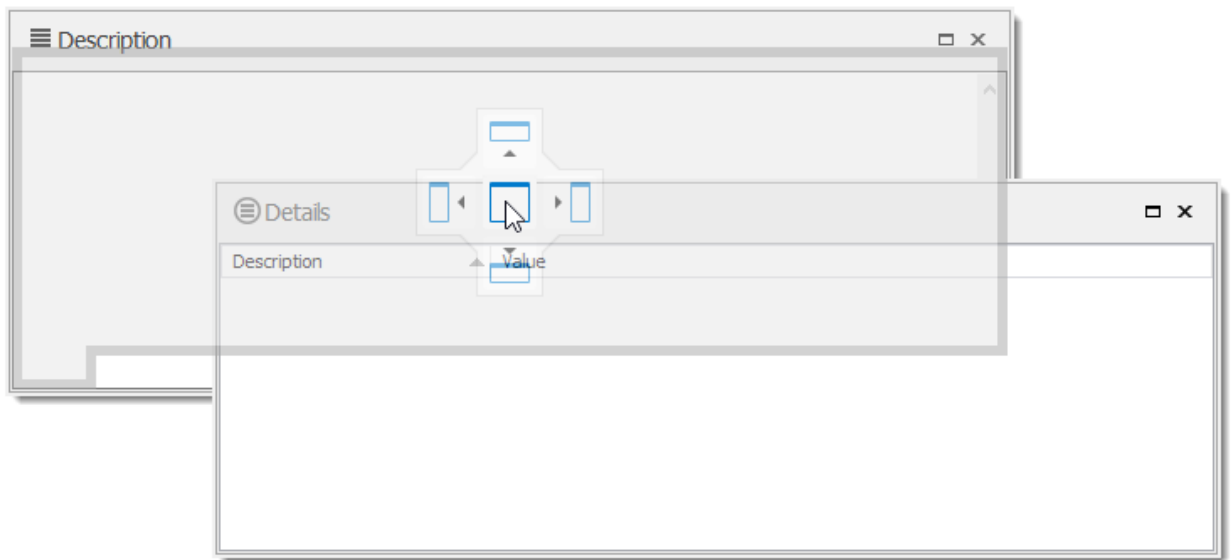


Footer Area

### DOCKED FOOTER

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

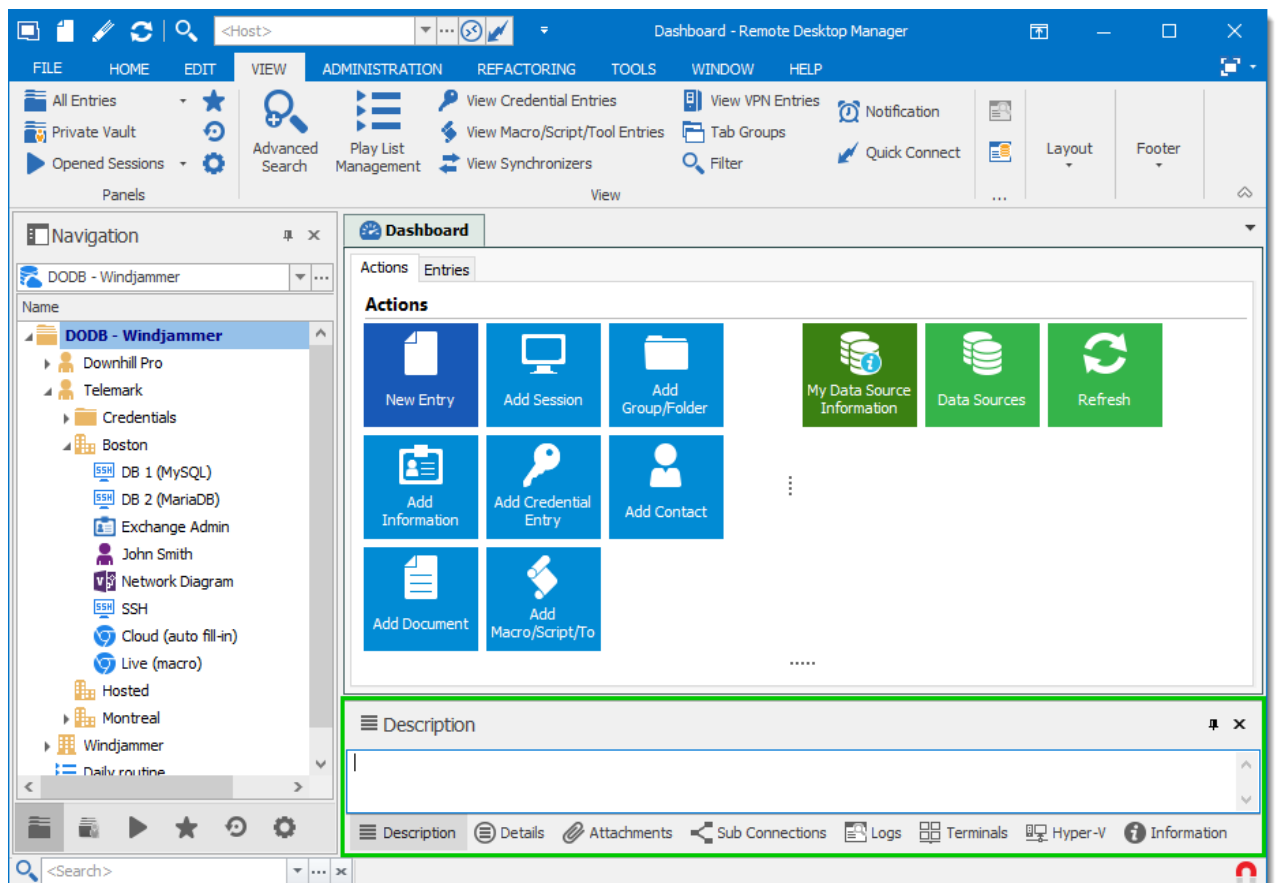
Here, we drop the **Details** pane to make it tabbed with the **Description** pane.



*Dock a footer pane into another*

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

Here is a personalized setup of the footer panes.



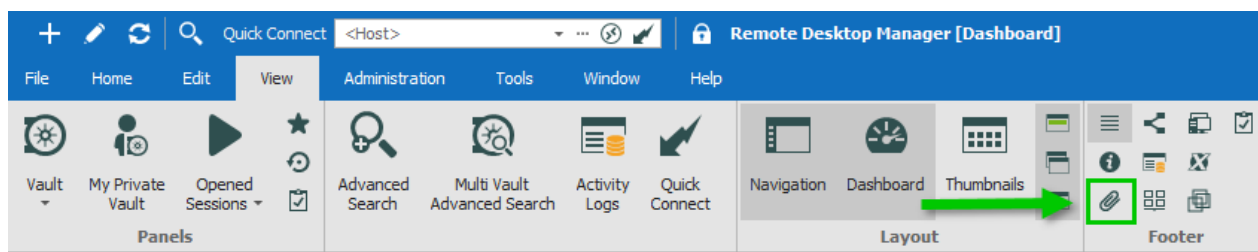
*Footer panes docked in the main window*

## 4.7.1 Attachments

### DESCRIPTION

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

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



*View – Footer – Attachments*



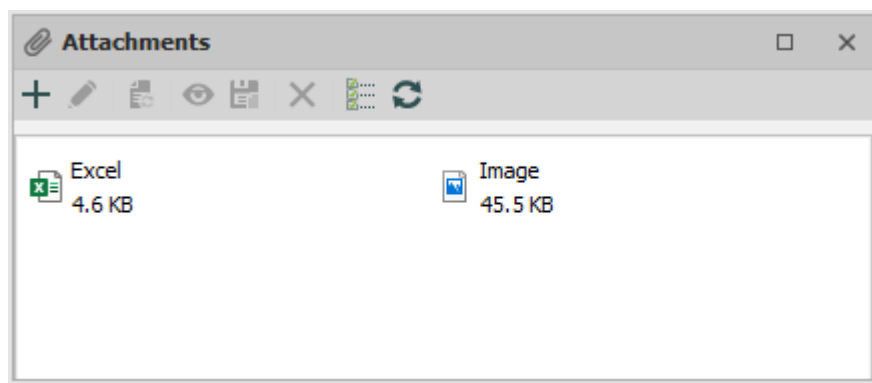
This feature is only available when using an [Advanced Data Source](#).



The files in attachment are not available in offline mode.



For architectural reasons, the documents stored in our Advanced Data Sources are **NOT** protected from deletion. Once they are deleted, **they cannot be restored**. Please keep a safe copy of all documents in another storage device. Support for this feature will be added in a coming update to our products.



*Attachment list*



The attachment type and size are limited only by your bandwidth and the data source. You can also view a saved attachment from:

- the session context menu;
- the session properties; or
- directly on the dashboard.

The refresh button allows you to update directly the selected document. Use it to save your local modifications after an edit.

## ACTIONS

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



*Attachment toolbar*

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

## 4.8 Status Bar

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

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



*Status bar*

### SEARCH / FILTER

Please consult the [Search/Filter](#) for detailed explanations.

### ONLINE / OFFLINE TOGGLE

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

### GRAB INPUT TOGGLE

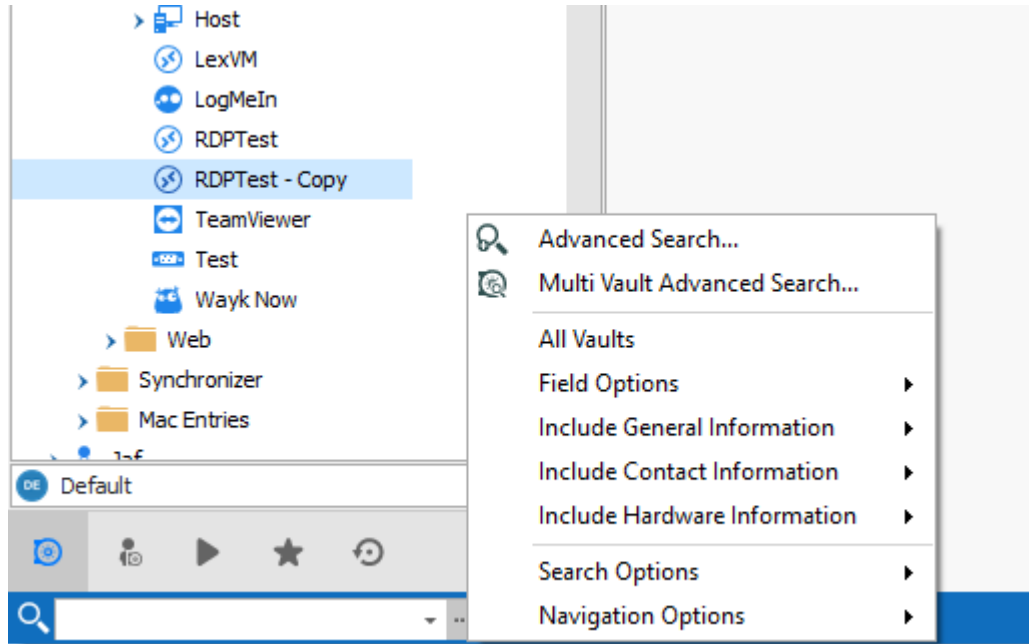
Please consult [Grab Input](#) for detailed explanations.

#### 4.8.1 Search/Filter

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

### ELLIPSIS BUTTON

Select the ellipsis button to display the options.



*Ellipsis button*

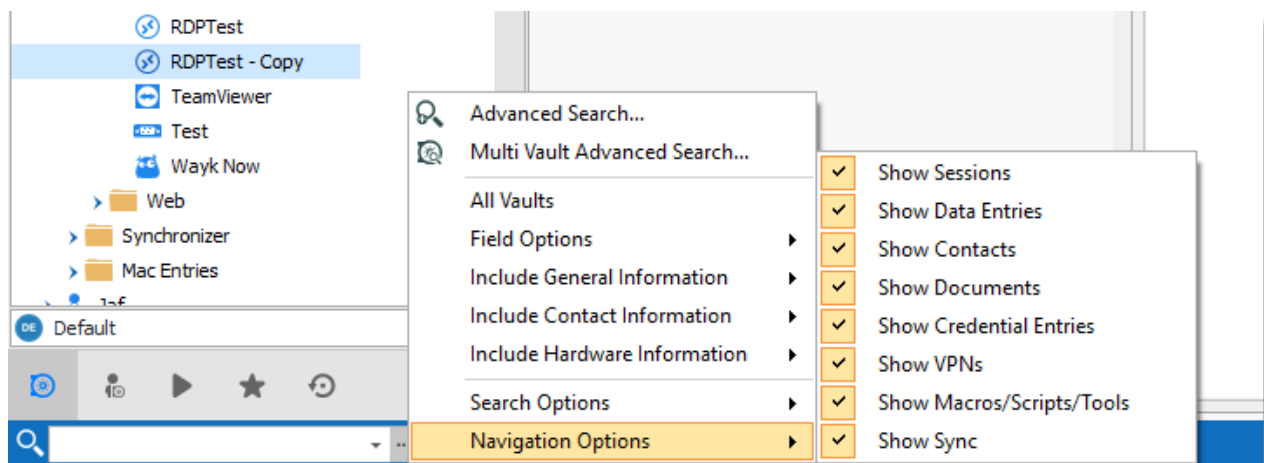
The filter expression is matched against fields as selected in the filter options such as:

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

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

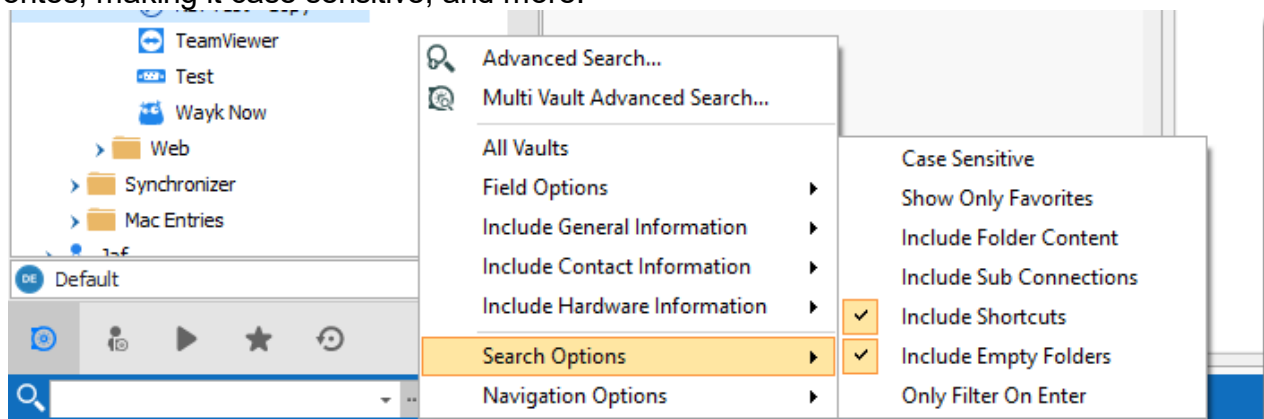
- Session types (credentials, script tools, VPN, etc.)
- If the session is marked as a Favorites

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



### Search Types

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



### Search Options

## KEYBOARD SHORTCUT

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

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

## BOOLEAN FILTER

Here a few implementation notes for the Boolean filter:

- We use the C# nomenclature (&& for AND, || for OR)

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

### EXAMPLES (THIS WILL WORK)

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

### EXAMPLES (THIS WILL NOT WORK AS EXPECTED)

- Laptop && "Baton Rouge"
  - Will work but filter for the string "Baton Rouge" and not the string Baton Rouge
- Laptop && (Baton Rouge || Boise)
  - Will work but filter for Laptop and the string (Baton Rouge || Boise)

## 4.8.2 Grab Input

### DESCRIPTION

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

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



*Grab keyboard input*

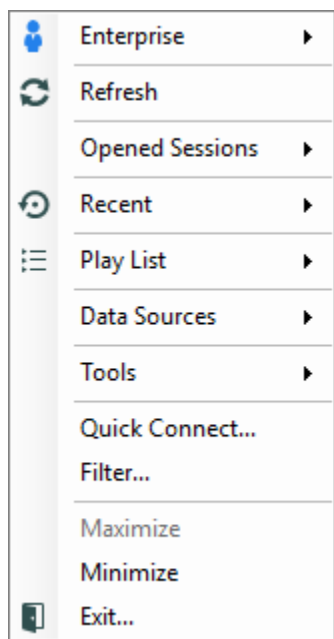
## 4.9 Tray Icon

### DESCRIPTION

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

### TRAY ICON CONTEXT MENU

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



*Tray Icon Context Menu*

OPTION	DESCRIPTION
<b>Sessions List</b>	Displays the sessions from the current data source. Sessions are listed by default. It is possible to show only those marked as favorites.

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

## TRAY ICON PREFERENCES

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

# Data Sources

---

Part V



## 5 Data Sources

### DESCRIPTION

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

### SETTINGS

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

**Remote Desktop Manager**

General Settings Private Vault Upgrade VPN Advanced

Name: Test SQL Server

Host: TestSQL ...

Login mode: Database login

Username: test

Password: .....

☐ Always ask password

☐ Allow change username

Database: TestDB ...

Two factor: None

Test Server

Test Database

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

On start up: Last used data source

OK Cancel

*Data Source*

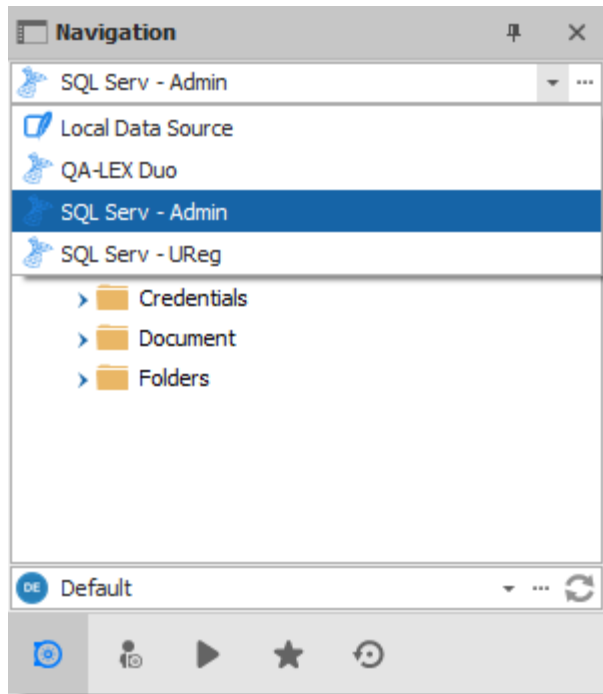
## CREATE A DATA SOURCE

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

## MULTIPLE DATA SOURCES

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

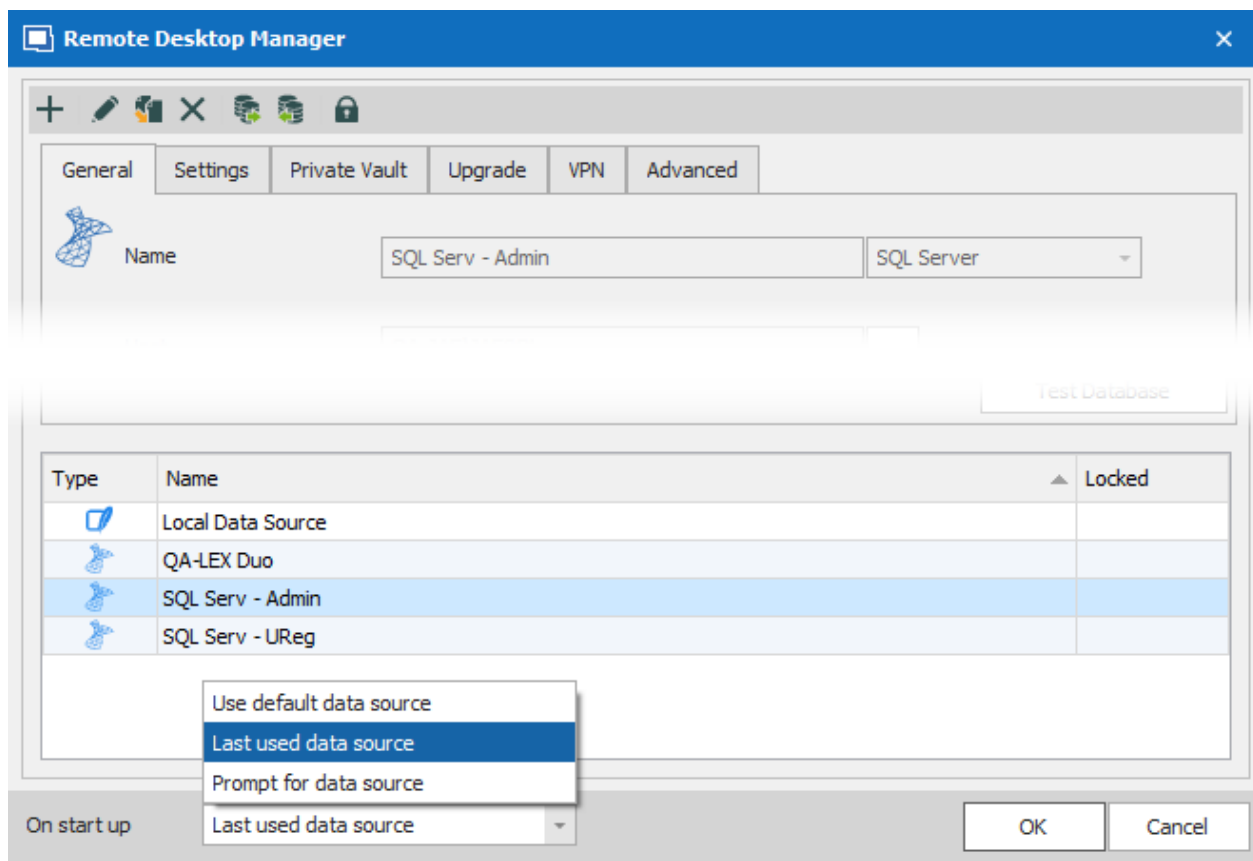
Switch from one data source to another by using the data source drop down list.



*Select a Data Source*

## STARTUP DATA SOURCE

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



Startup Data Source

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

## DATA SOURCE SETTINGS (SYSTEM SETTINGS)

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

## 5.1 2-Factor Authentication

### DESCRIPTION



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

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


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

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

### HOW TO CONFIGURE TWO-FACTOR AUTHENTICATION

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

### SETTINGS

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

**Remote Desktop Manager**

General Settings Private Vault Upgrade VPN Advanced

**Name** SQL Serv - UReg SQL Server

**Host** ...

**Login mode** Database login

**Username** UReg

**Password** .....  
☐ Always ask password  
☐ Allow change username

**Database** JafJafDen ...

**Two factor** None

Test Server  
Test Database

Type	Name	Locked
	SQL Serv - UReg	

On start up Last used data source

OK Cancel

*Edit - Data Source Configuration*

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

The screenshot shows the 'Microsoft SQL Server' configuration window. The 'General' tab is selected. The 'Name' field is 'SQL Server'. The 'Host' field is 'DEVOLUTIONS\SQLEXPRESS'. The 'Login mode' is 'Database login'. The 'Username' is 'RDMAAdmin'. The 'Password' is masked with dots. There are checkboxes for 'Always ask password' and 'Allow change username', both of which are unchecked. The 'Database' field is 'test'. The 'Two factor' dropdown is set to 'None' and is highlighted with a green box. At the bottom right, there are buttons for 'Test Server', 'Test Database', 'OK', and 'Cancel'.

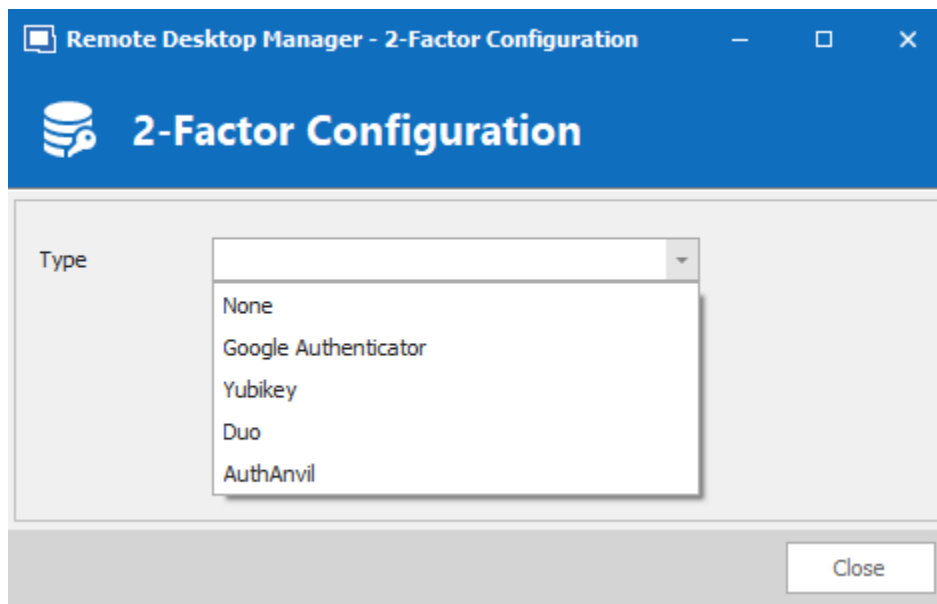
*Data Source Configuration*

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

The screenshot shows the '2-Factor Configuration' window. The 'Type' is set to 'None'. Below the 'Type' field, there is a blue hyperlink labeled 'Change'. At the bottom right, there is a 'Close' button.

*Two-Factor Configuration window*

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



*Two-Factor Configuration window*

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

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

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

### 5.1.1 Google Authenticator

## DESCRIPTION

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

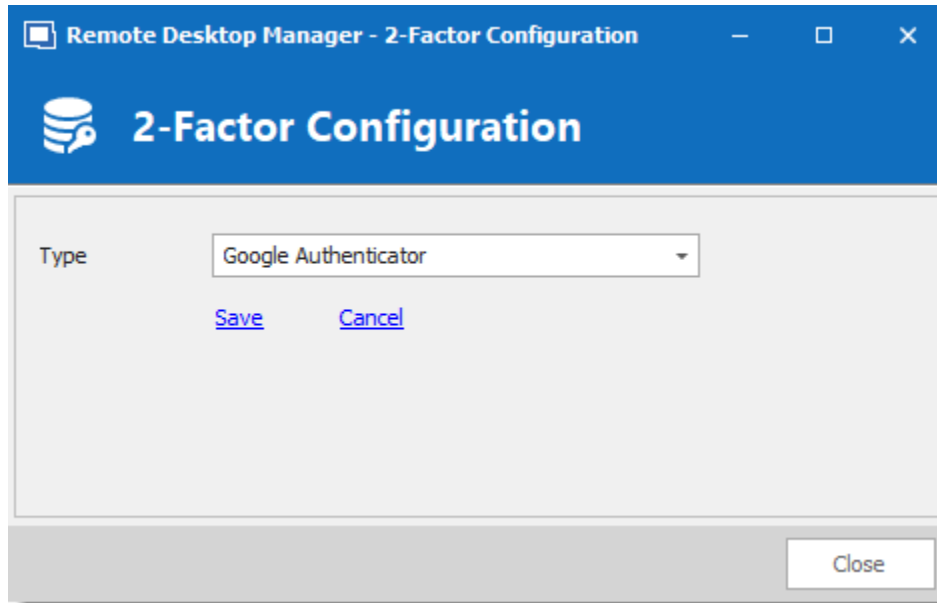
## SETTINGS





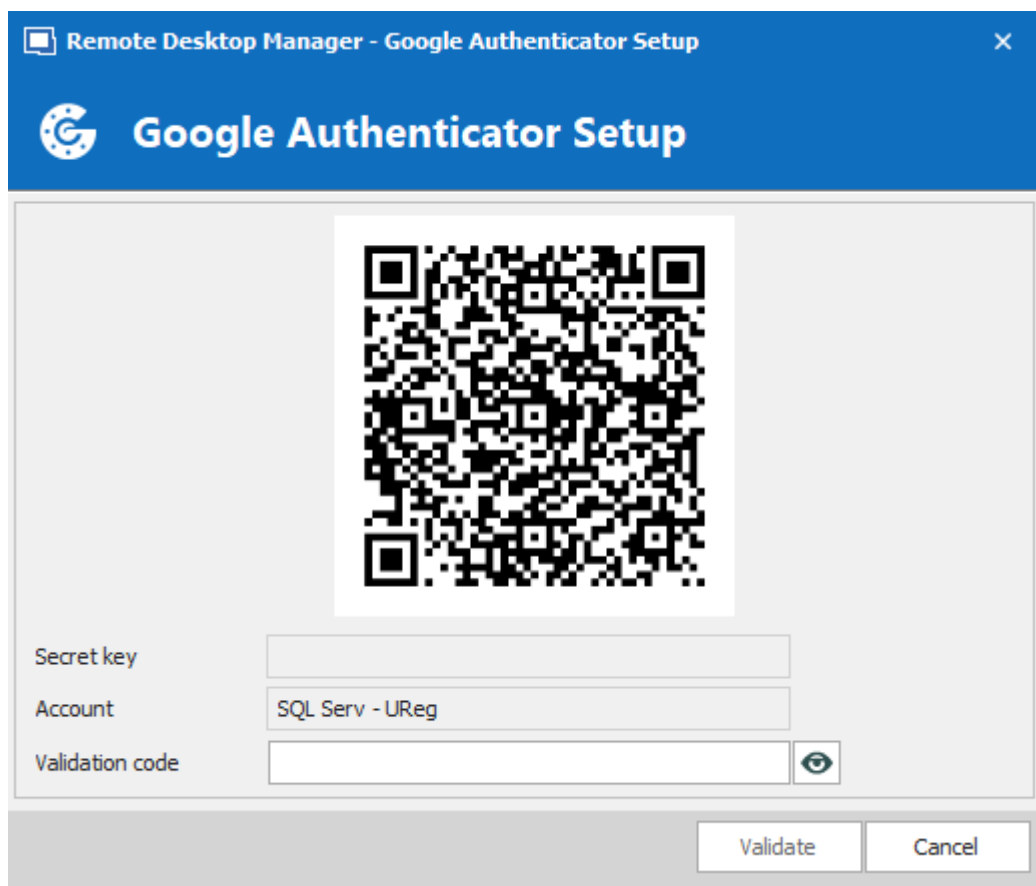
Before you start the configuration, make sure you have installed the [Google Authenticator](#) application on a supported device.

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



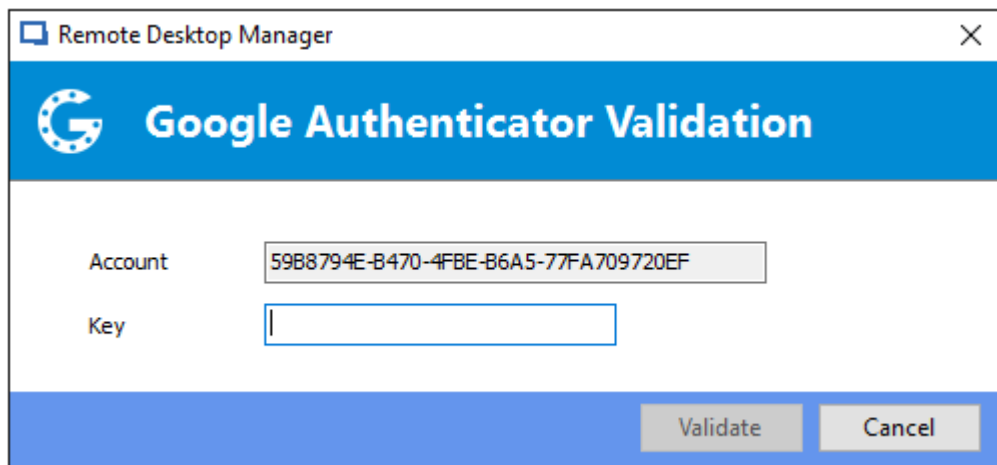
*Google Authenticator Configuration*

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



*Google Authenticator Setup*

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



*Google Authenticator Validation*



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

## 5.1.2 Yubikey

### DESCRIPTION

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



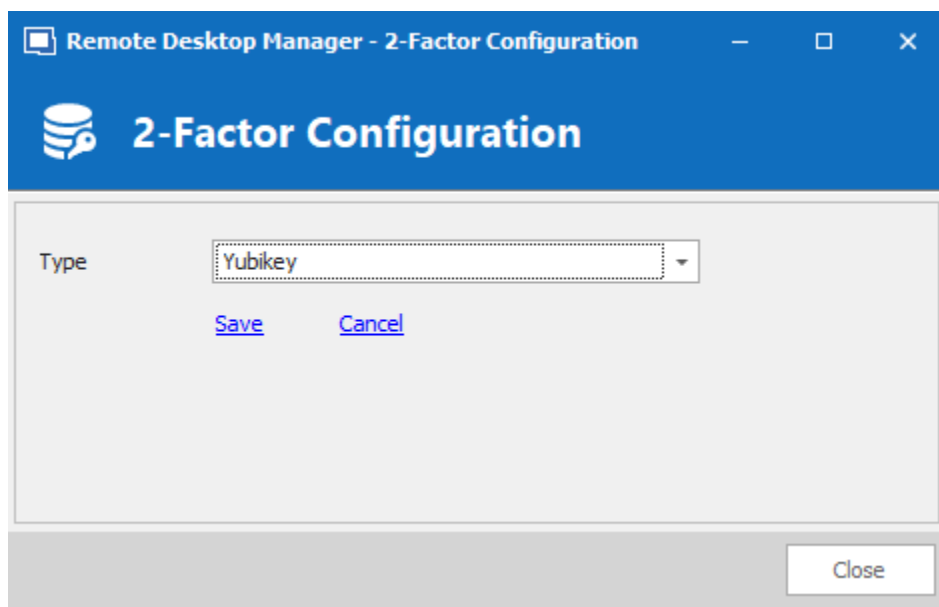
Remote Desktop Manager only support the Yubico OTP at this time.

### SETTINGS



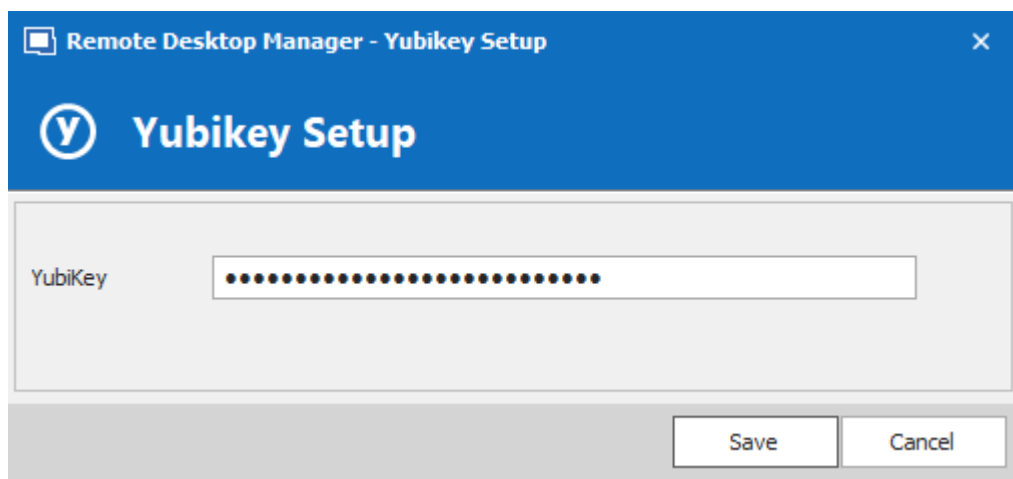
Before you start the configuration, make sure you have a [Yubikey](#) in your possession.

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



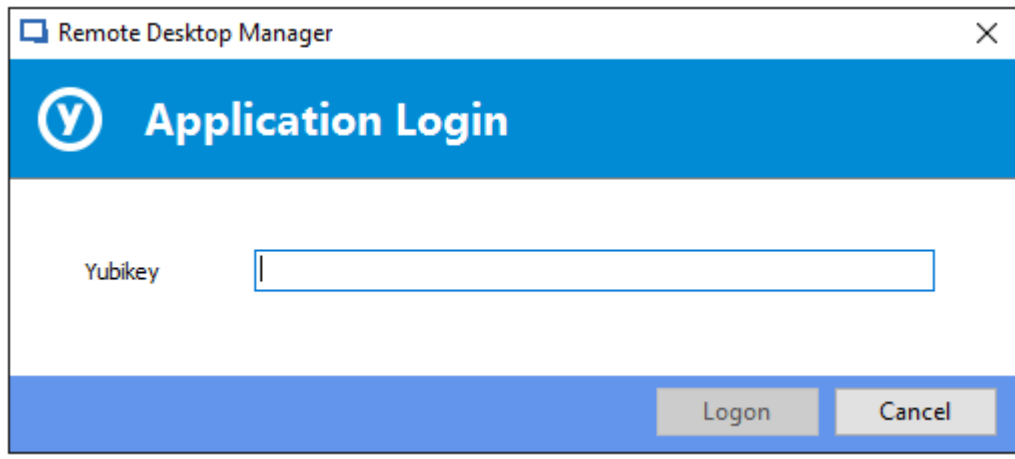
*Yubikey Configuration*

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



*Yubikey Authentication*

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



*Yubikey Application login*

### 5.1.3 Duo

#### DESCRIPTION

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

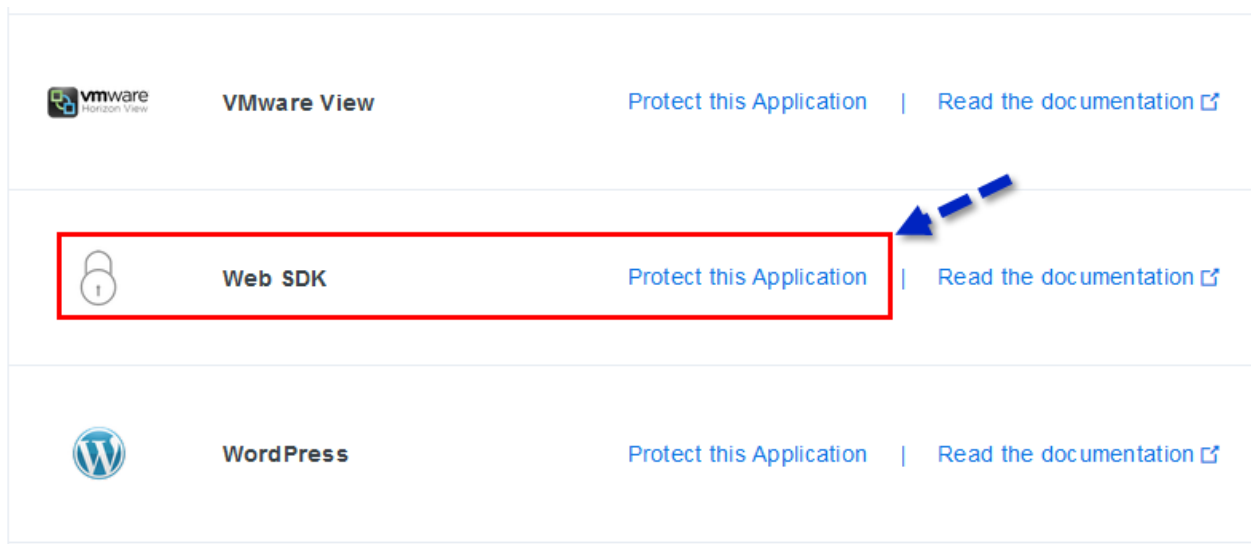
#### SETTINGS



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

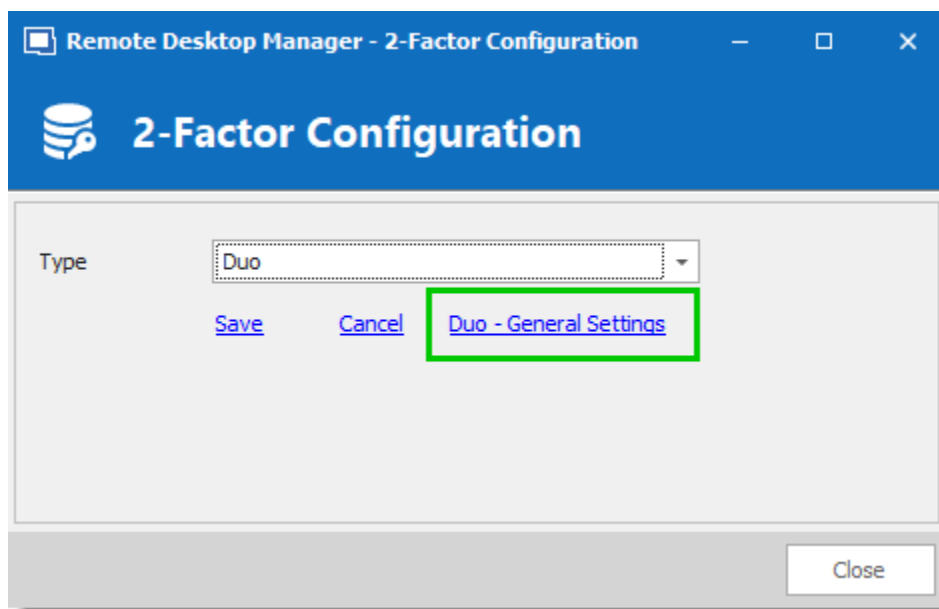
There is three methods to use with Duo: by land line, by text message or by using their application.

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



*Web SDK application*

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



*2-Factor Configuration*

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

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

## Web SDK

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

### Details

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

*Duo Account - Web SDK*

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

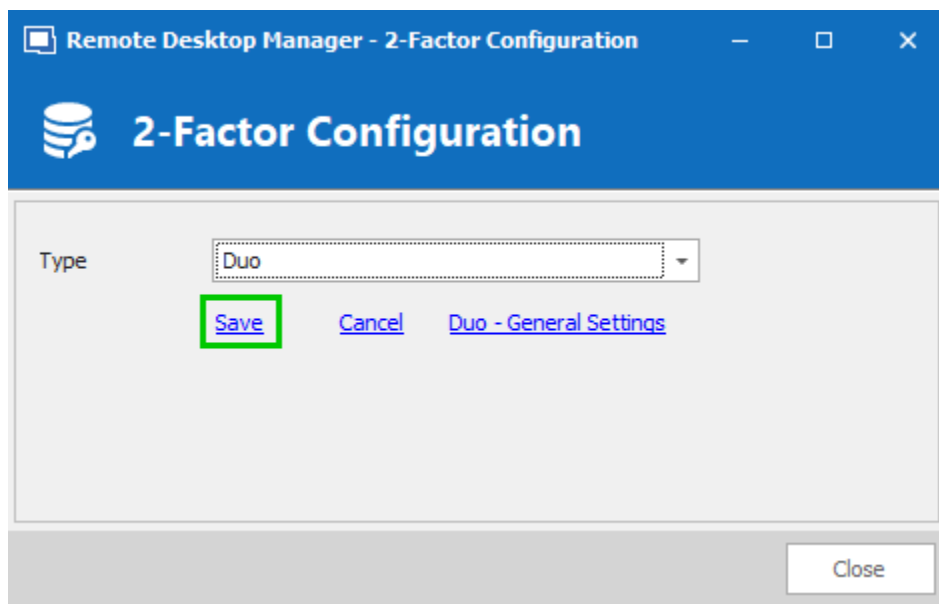
Remote Desktop Manager - Duo Settings

**Duo Settings**

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

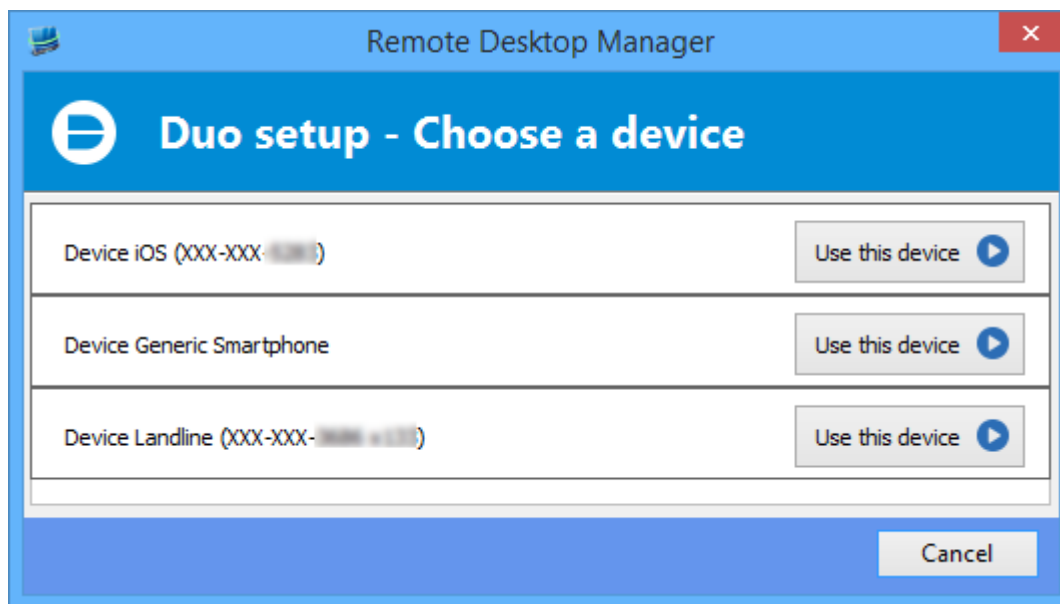
*Duo Settings*

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



*Duo Configuration - Save settings*

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



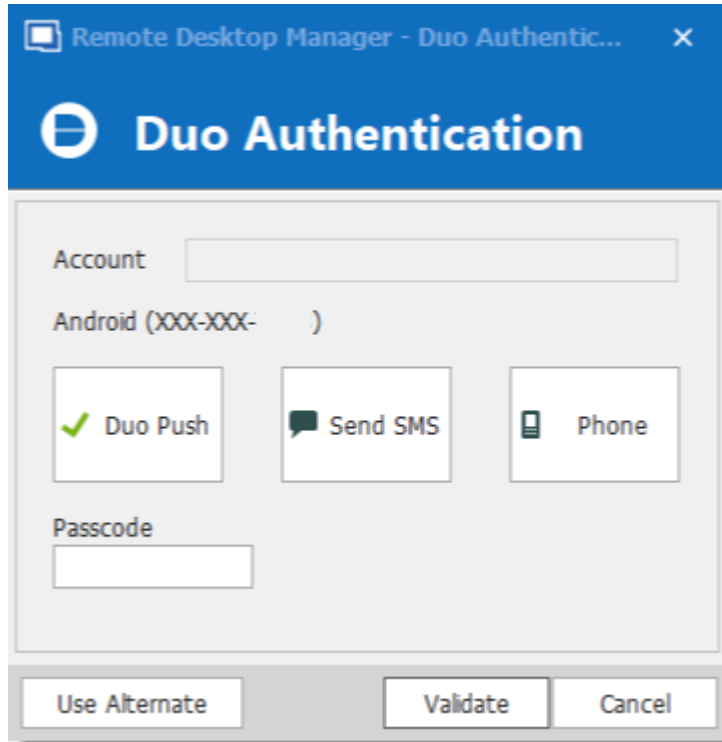
*Duo setup - Choose a device*

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

- **Duo Push:** The code is "pushed" to your Duo application.



- **Send SMS:** You will receive the code by SMS on your registered phone number.
- **Phone:** You will receive a phone call and a computer generated voice will dictate the code to you.



*Duo Setup*

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

#### 5.1.4 AuthAnvil

### DESCRIPTION

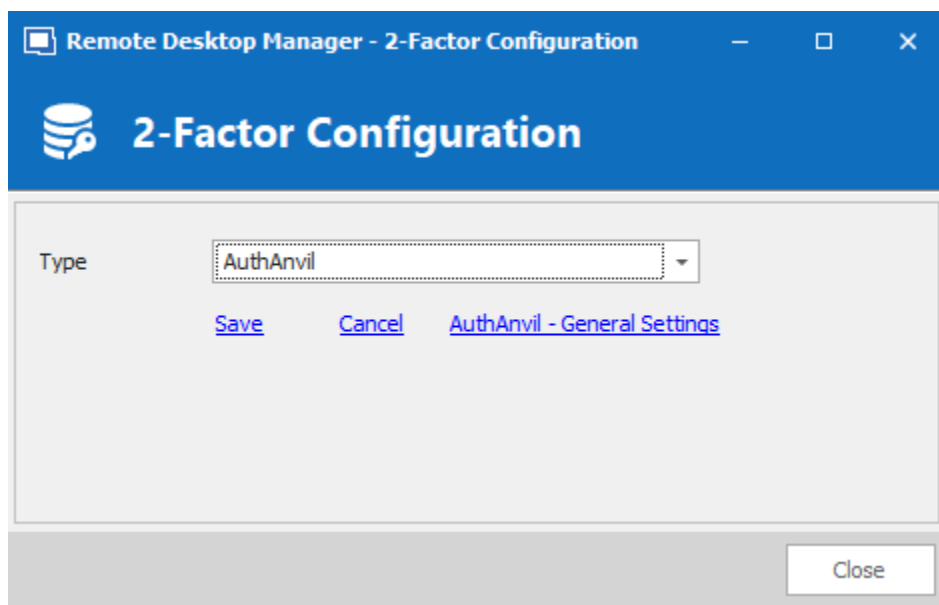
Remote Desktop Manager allows you to use AuthAnvil Authenticator to provide an additional security layer when opening a data source.

### SETTINGS



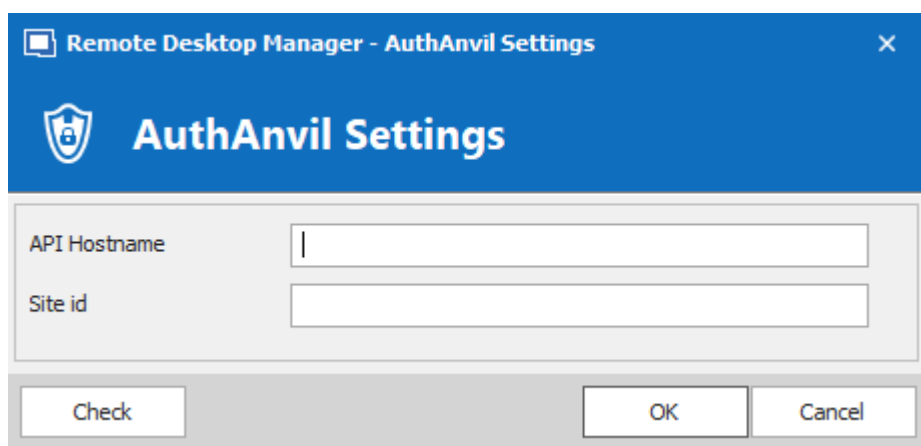
Before you start the configuration in Remote Desktop Manager, make sure you have created and configured your AuthAnvil account. For more information please consult <https://authanvil.com/features/two-factor-authentication>.

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



*AuthAnvil Configuration*

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



*AuthAnvil Settings*

## 5.2 Caching

### DESCRIPTION

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



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



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

### SETTINGS

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

*Caching Mode*

OPTION	DESCRIPTION
<b>Disabled</b>	No client caching.

OPTION	DESCRIPTION
<b>Intelligent</b>	<p>Intelligent cache has the ability to handle many more sessions without experiencing performance degradation.</p> <p>In the case of intelligent cache each modification performs a token update on the server. When Remote Desktop Manager performs a refresh action it will query the data source for any changes (delta) of changes to be applied client side since it last checked the data source. The delta of the changes is then sent to the application and applied locally.</p> <p>When first opening the data source Remote Desktop Manager will load the session from the offline file then refresh to get the up-to date information.</p>

## LOCATION

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

There are three engines for the cache:

- SQLite (offline.db).
- MCDF (offline.mcdf).
- MCDF v2.0 (offline.mcdf2).

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

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



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

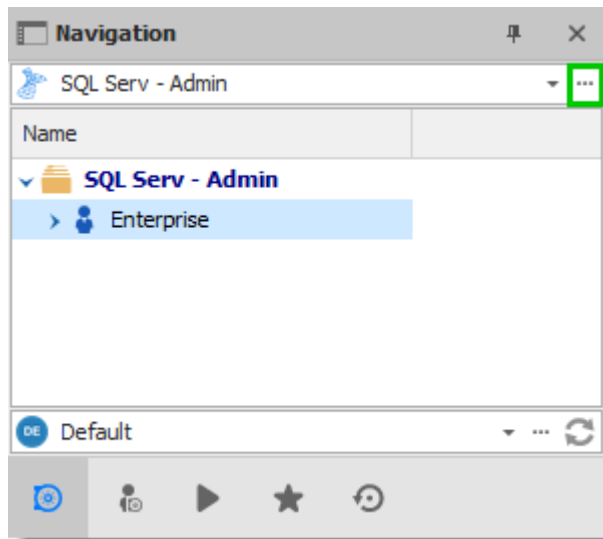


Depending on the configuration of the Caching mode & the [Offline mode](#) the offline file may still exist since the file servers as a dual purpose caching & offline line support.

## 5.3 Create a data source

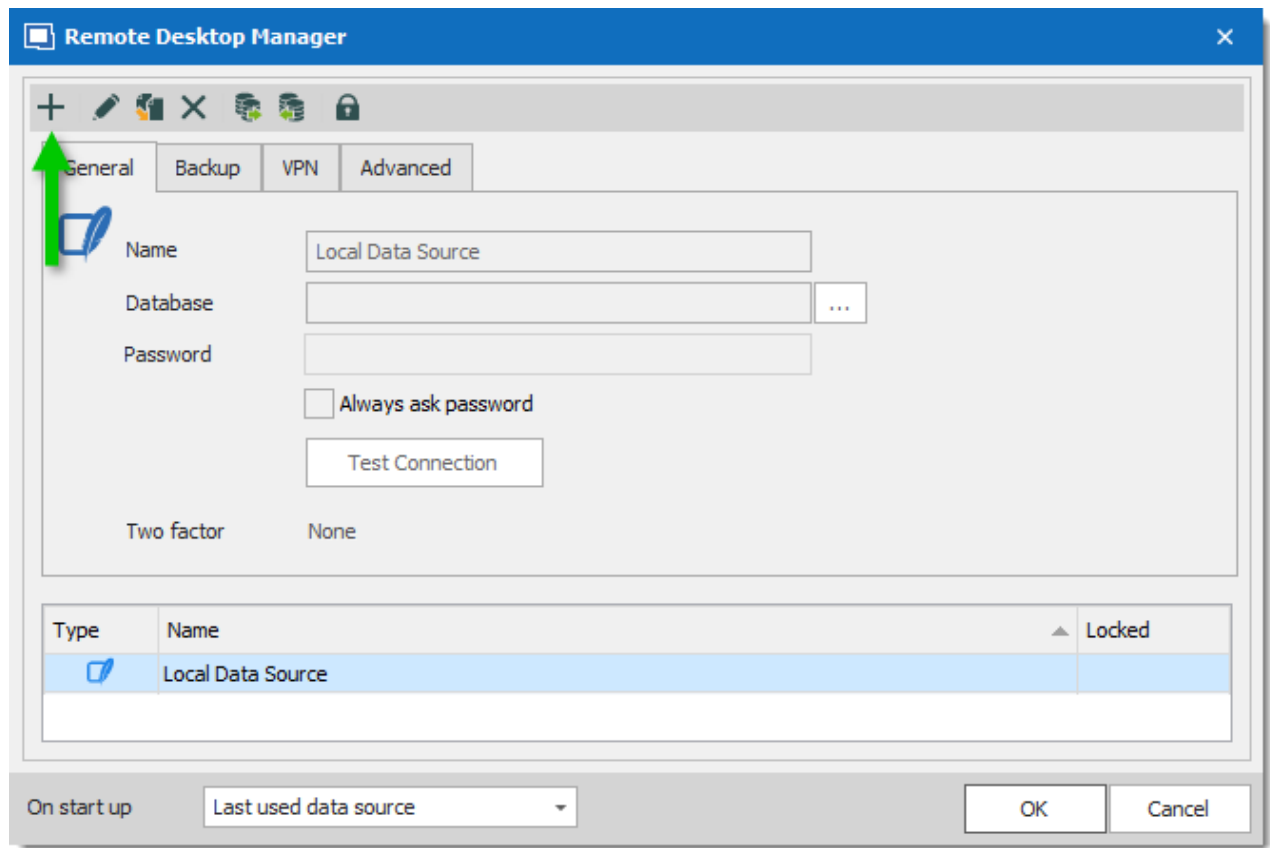
### SETTINGS

1. Open the **Data Source Configuration** window by clicking the **ellipsis** button at the top of the Navigation Pane.



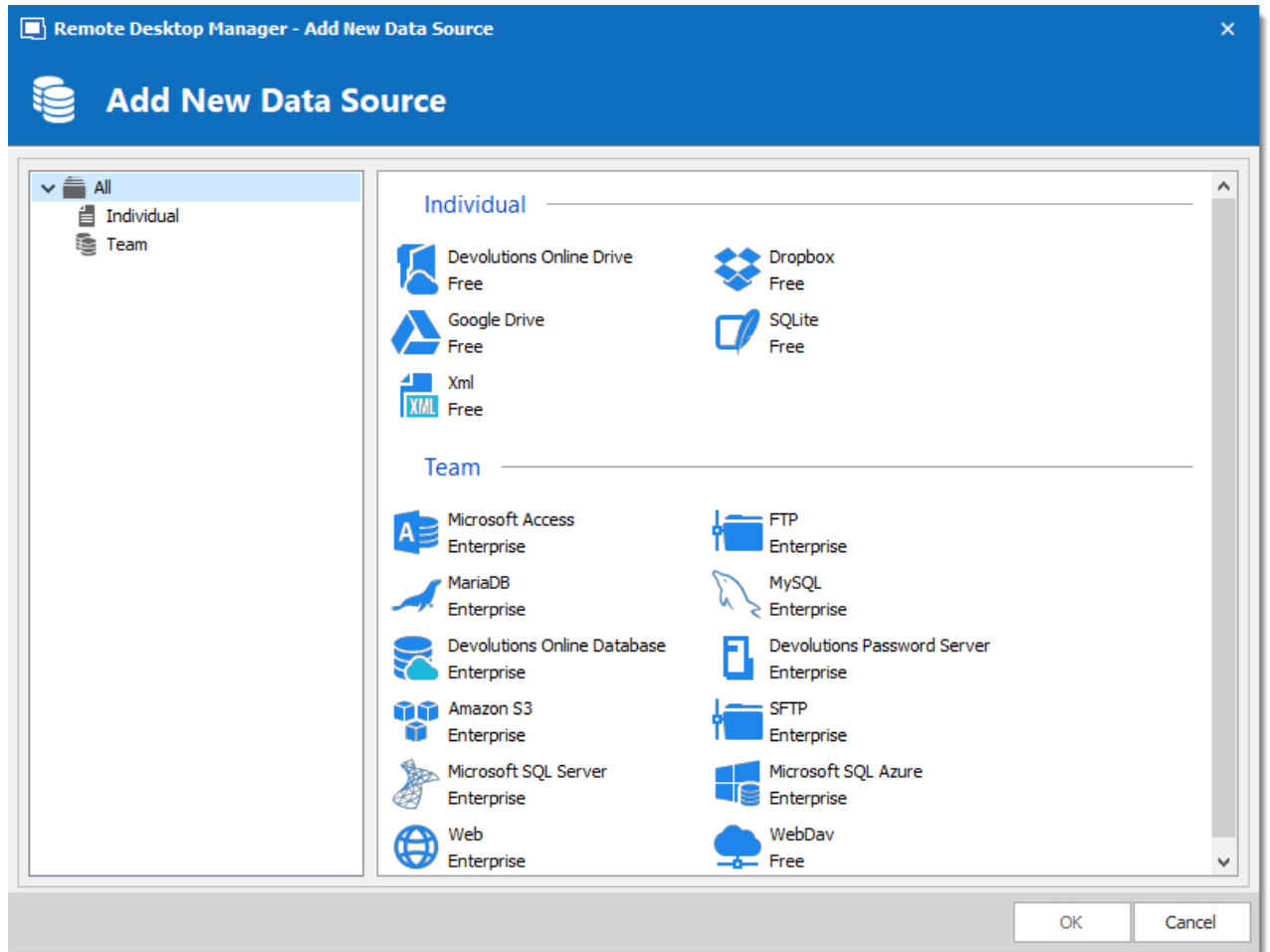
*Open Data Source menu*

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



*Add a new Data Source*

3. Select the type of data source to create.



*Select your Data Source type*

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

Remote Desktop Manager - Microsoft SQL Server

Microsoft SQL Server

General Settings Private Vault Upgrade VPN Advanced

Name  SQL Server

Host  ...

Login mode Database login

Username

Password

☐ Always ask password

☐ Allow change username

Database  ...

Two factor [None](#)

Test Server

Test Database

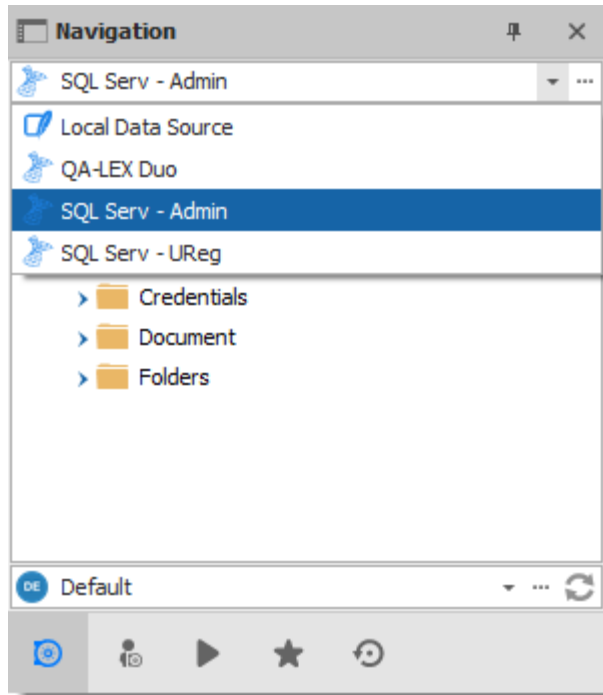
ID 707CB610-6799-4562-9B62-EA06240A300F

OK Cancel

SQL Server - Connection Tab

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





*Select your Data Source*

## 5.4 Data Source Types

### DESCRIPTION




Remote Desktop Manager supports multiple types of data source. To start, decide which data source you'll be using.







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



### DATA SOURCE TYPES


NAME	DESCRIPTION	PROS AND CONS
<b>Devolutions Online</b>	Remote Desktop Manager uses Devolutions Online Drive to store and synchronize your sessions. Access	Pros: <ul style="list-style-type: none"> <li>• Quick.</li> </ul>

NAME	DESCRIPTION	PROS AND CONS
<b>Drive</b>  	<p>your sessions from anywhere using a simple Internet connection.</p> <p>For more information, please consult our <a href="#">Online Drive</a> topic.</p>	<ul style="list-style-type: none"> <li>• Reliable.</li> <li>• The service is free.</li> </ul> <p>Cons:</p> <ul style="list-style-type: none"> <li>• No possibility for sharing.</li> <li>• No security management.</li> </ul>
<b>Devolutions Password Server</b>  	<p>Remote Desktop Manager uses Devolutions Password Server to store session information.</p> <p>For more information, please consult our <a href="#">Devolutions Password Server</a> topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> <li>• Quick.</li> <li>• Reliable.</li> <li>• Secure.</li> <li>• Supports all features, such as <a href="#">attachments</a>, connection log, <a href="#">Offline Mode</a> and <a href="#">User Management</a>.</li> <li>• Active Directory integration.</li> </ul> <p>Cons</p> <ul style="list-style-type: none"> <li>• Installation required.</li> </ul>
<b>Dropbox</b>  	<p>Remote Desktop Manager uses the Dropbox API to retrieve the XML file from the configured repository.</p> <p>For more information, please consult our <a href="#">Dropbox</a> topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> <li>• Can be shared in read-only mode.</li> <li>• Backups (by Dropbox) are automatic.</li> <li>• Storage infrastructure is free (if within your free storage quota).</li> </ul>

NAME	DESCRIPTION	PROS AND CONS
		<p>Cons:</p> <ul style="list-style-type: none"> <li>• No security management.</li> <li>• There is a possibility for conflict or data corruption to occur.</li> <li>• Doesn't support all features, such as <a href="#">attachments</a>, connection logs and <a href="#">User Management</a>.</li> <li>• The Dropbox integration uses the Dropbox SDK, so any features that are exclusive to the Business or Enterprise editions are NOT supported.</li> </ul>
<b>MariaDB</b> 	<p>Remote Desktop Manager uses MariaDB to save and manage all sessions. This is one of the available data source for a multi-user environment.</p> <p>For more information, please consult our <a href="#">MariaDB</a> topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> <li>• Quick.</li> <li>• Reliable.</li> <li>• The database is free and can be installed on Linux.</li> <li>• Supports all features, such as <a href="#">attachments</a>, connection log, <a href="#">Offline mode</a> and <a href="#">User Management</a>.</li> </ul> <p>Cons:</p> <ul style="list-style-type: none"> <li>• MariaDB needs to be installed.</li> </ul>
<b>Microsoft SQL Azure</b>	Remote Desktop Manager uses the Microsoft cloud platform to save and manage all sessions.	<p>Pros:</p> <ul style="list-style-type: none"> <li>• Quick.</li> <li>• Reliable.</li> </ul>

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

NAME	DESCRIPTION	PROS AND CONS
	<p>For more information, please consult our <a href="#">MySQL</a> topic.</p>	<ul style="list-style-type: none"> <li>• The database is free and can be installed on Linux.</li> <li>• Supports all features, such as <a href="#">attachments</a>, connection log, <a href="#">Offline mode</a> and <a href="#">User Management</a>.</li> </ul> <p>Cons:</p> <ul style="list-style-type: none"> <li>• MySQL needs to be installed.</li> </ul>
<b>SQLite</b>  	<p>Remote Desktop Manager uses a SQLite database to store session information.</p> <p>For more information, please consult our <a href="#">SQLite</a> topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> <li>• Quick.</li> <li>• Reliable.</li> <li>• The database is free.</li> <li>• Supports all features, such as <a href="#">attachments</a> &amp; connection logs.</li> </ul> <p>Cons:</p> <ul style="list-style-type: none"> <li>• No possibility for sharing.</li> <li>• No security management.</li> </ul>
<b>WebDAV</b>  	<p>Remote Desktop Manager uses an HTTP connection to retrieve the XML file on a WebDav server.</p> <p>For more information. please consult our <a href="#">WebDAV</a> topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> <li>• Can be shared in read-only mode.</li> <li>• Easy to deploy online.</li> </ul> <p>Cons:</p>

NAME	DESCRIPTION	PROS AND CONS
		<ul style="list-style-type: none"> <li>• No security management.</li> </ul>
<b>XML</b>  	<p>Remote Desktop Manager saves the settings directly in a file with the XML format.</p> <p>For more information, please consult our <a href="#">XML</a> topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> <li>• Easy backup.</li> <li>• Can be edited manually or by an external system.</li> <li>• Nothing to install.</li> </ul> <p>Cons:</p> <ul style="list-style-type: none"> <li>• No possibility of sharing.</li> <li>• No security management.</li> <li>• There is a possibility for conflict or data corruption to occur.</li> <li>• Doesn't support all features, such as <a href="#">attachments</a>, connection logs and <a href="#">User Management</a>.</li> </ul>

### 5.4.1 Advanced Data Sources

## DESCRIPTION

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

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

- Document uploads and Entry Attachments.
- Auditing and logging.
- Advanced security with [User management](#) and [Role-based security system](#).
- [Offline mode](#).
- [Multi-Factor Authentication](#)



For architectural reasons, the documents stored in our Advanced Data Sources are **NOT** protected from deletions. Once they are deleted, **they cannot be restored**. Please keep a safe copy of all documents in another storage device. Support for this feature will be added in a coming update to our products.

Currently the Advanced Data Sources are:

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

#### 5.4.1.1 Devolutions Online Database

## DESCRIPTION

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



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

## SETTINGS

### GENERAL

The screenshot shows the 'Remote Desktop Manager - Devolutions Online Database' window. The title bar includes the application name and standard window controls. The main header is blue with the Devolutions logo and the text 'Devolutions Online Database'. Below the header are four tabs: 'General' (selected), 'Private Vault', 'VPN', and 'Advanced'. The 'General' tab contains a database icon and several fields: 'Name' (text input), 'Always ask password' (checkbox), 'Database' (text input with a dropdown arrow and a globe icon), 'Database ID' (text input), and 'Two factor' (set to 'None'). There are also links for 'Create a Free Account' and a 'Test Credentials' button. At the bottom, the 'ID' field displays a long alphanumeric string, and there are 'OK' and 'Cancel' buttons.

Devolutions Online Database - General Tab

OPTION	DESCRIPTION
<b>Name</b>	Name of the data source.
<b>Always ask password</b>	Always ask password when connecting to the data source.
<b>Create a Free account</b>	Create a new <a href="#">Devolutions Account</a> .
<b>Database</b>	Name of the data base created online. You must use the ellipsis button to select it from the list of online data sources available to the name.
<b>Database ID</b>	Unique Key to identify the data source.
<b>Two factor</b>	Enable the <a href="#">2-Factor Authentication</a> to access your data source.



OPTION	DESCRIPTION
<b>Test Credentials</b>	Test the credentials that you have configured to connect on Remote Desktop Manager Online.

## PRIVATE VAULT

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

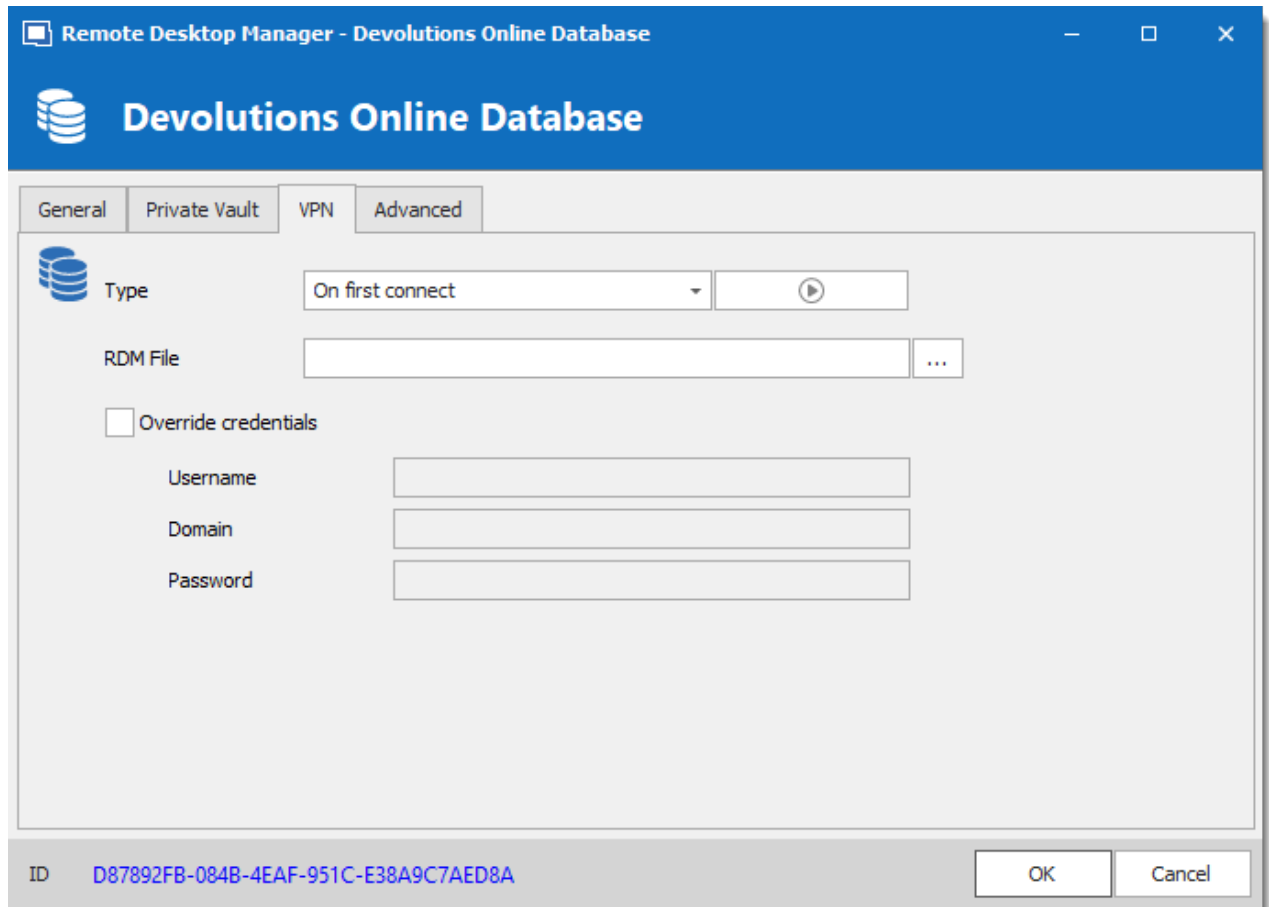
For more information please see [Private Vault](#).

The screenshot shows a window titled "Remote Desktop Manager - Devolutions Online Database". The window has a blue header bar with the Devolutions logo and the text "Devolutions Online Database". Below the header, there are four tabs: "General", "Private Vault", "VPN", and "Advanced". The "Private Vault" tab is selected. The "Private Vault" tab contains a "Type" dropdown menu set to "Online Drive", a "Filename" text box with a browse button "...", a "Master key" text box, and a checkbox labeled "Always ask master key" which is checked. At the bottom of the window, there is an "ID" field with the value "60229194-32B8-4EC9-AB61-2111D76812D6" and "OK" and "Cancel" buttons.

*Devolutions Online Database - Private Vault*

## VPN

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



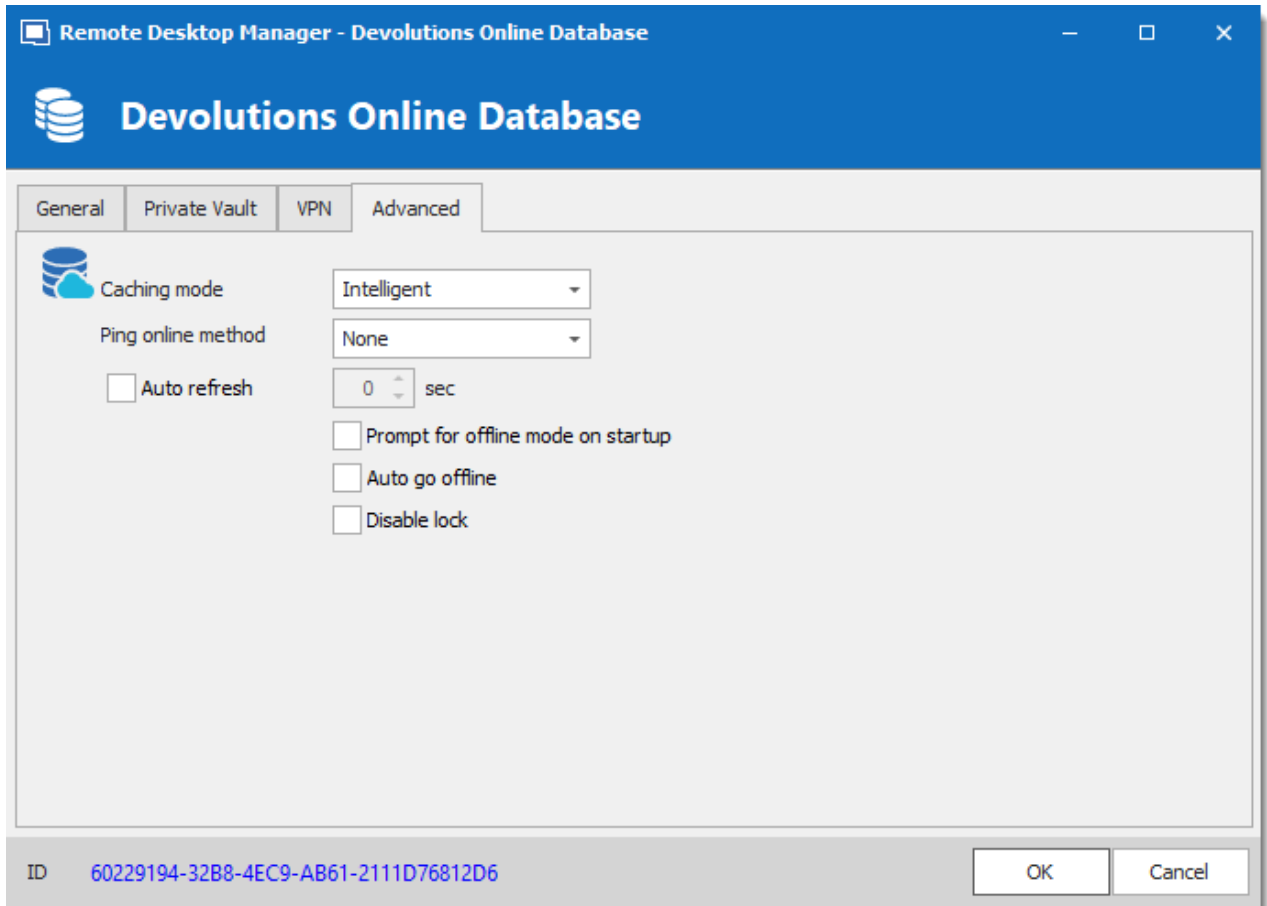
The screenshot shows a window titled "Remote Desktop Manager - Devolutions Online Database". The window has a blue header bar with the Devolutions logo and the text "Devolutions Online Database". Below the header, there are four tabs: "General", "Private Vault", "VPN", and "Advanced". The "VPN" tab is selected. The main area of the window contains the following fields and controls:

- Type:** A dropdown menu set to "On first connect" with a play button icon to its right.
- RDM File:** A text input field with a browse button (three dots) 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 window, there is a status bar with the text "ID D87892FB-084B-4EAF-951C-E38A9C7AED8A" and two buttons: "OK" and "Cancel".

*Devolutions Online Database - VPN*

## ADVANCED



*Devolutions Online Database - Advanced*

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

OPTION	DESCRIPTION
<b>Auto go offline</b>	If the ping online method doesn't work it will automatically go offline.
<b>Disable lock</b>	Disable the option to lock the data source directly. The application still can be locked but the user is not prompted for the data source password when unlocking the application.

#### 5.4.1.2 Devolutions Password Server

### DESCRIPTION



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

### HIGHLIGHTS

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



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

For more information, please consult these topics:

- [Devolutions Password Server installation instructions](#)
- [Devolutions Password Server Security Checklist](#)

## CONFIGURE THE SERVER DATA SOURCE ON ALL YOUR CLIENT MACHINES

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

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

## SETTINGS

### GENERAL

The screenshot shows the 'Remote Desktop Manager - Devolutions Password Server' window. The title bar is blue with the application icon and name. Below the title bar is a blue header with the Devolutions logo and 'Devolutions Password Server'. The main area has a tabbed interface with 'General', 'Settings', 'Private Vault', 'VPN', and 'Advanced'. The 'General' tab is active, showing a list of settings on the left and their values on the right. The settings include 'Name' (text field), 'Host' (dropdown menu), 'Use Windows authentication' (checkbox), 'Use Office365 authentication' (checkbox), 'Always prompt for credentials' (checkbox), 'Username' (dropdown menu), 'Password' (text field), and 'Always ask password' (checkbox). A 'Test Connection' button is at the bottom right. The status bar at the bottom shows the ID 'E2B0D26F-C0AA-4DF2-B679-C4ACE1527806' and 'OK'/'Cancel' buttons.

Setting	Value
Name	
Host	
Use Windows authentication	<input type="checkbox"/>
Use Office365 authentication	<input type="checkbox"/>
Always prompt for credentials	<input type="checkbox"/>
Username	
Password	
Always ask password	<input type="checkbox"/>

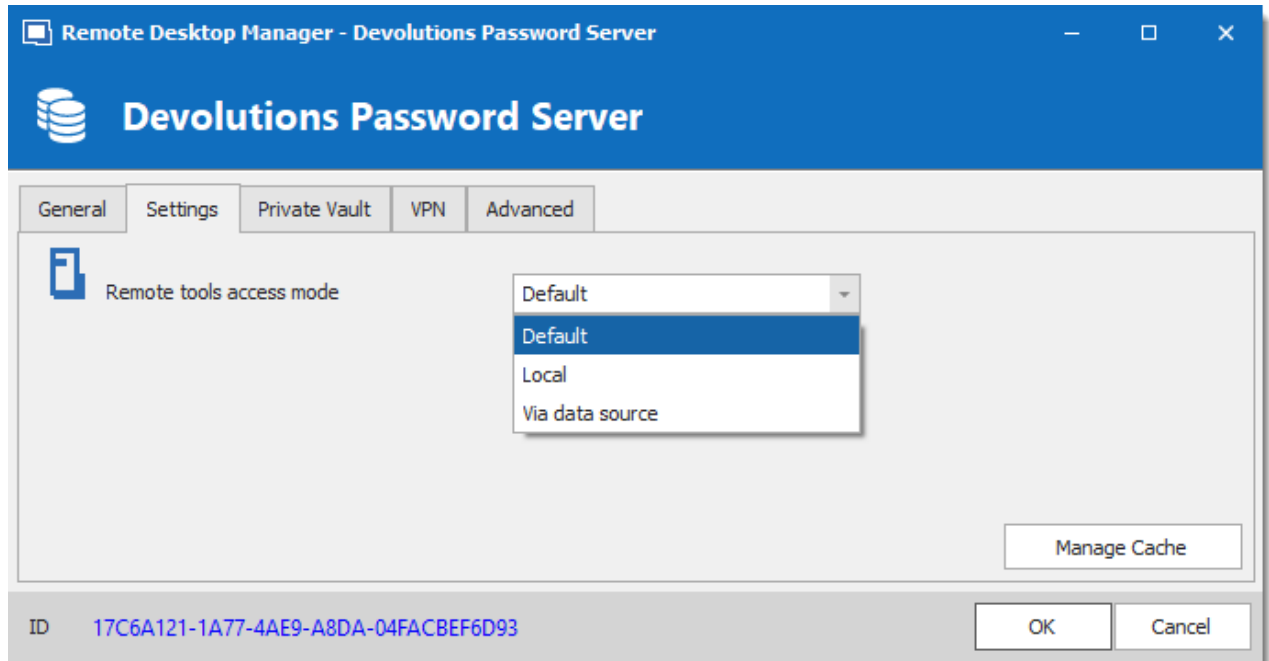
Test Connection

ID E2B0D26F-C0AA-4DF2-B679-C4ACE1527806 OK Cancel

*Devolutions Password Server - General*

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

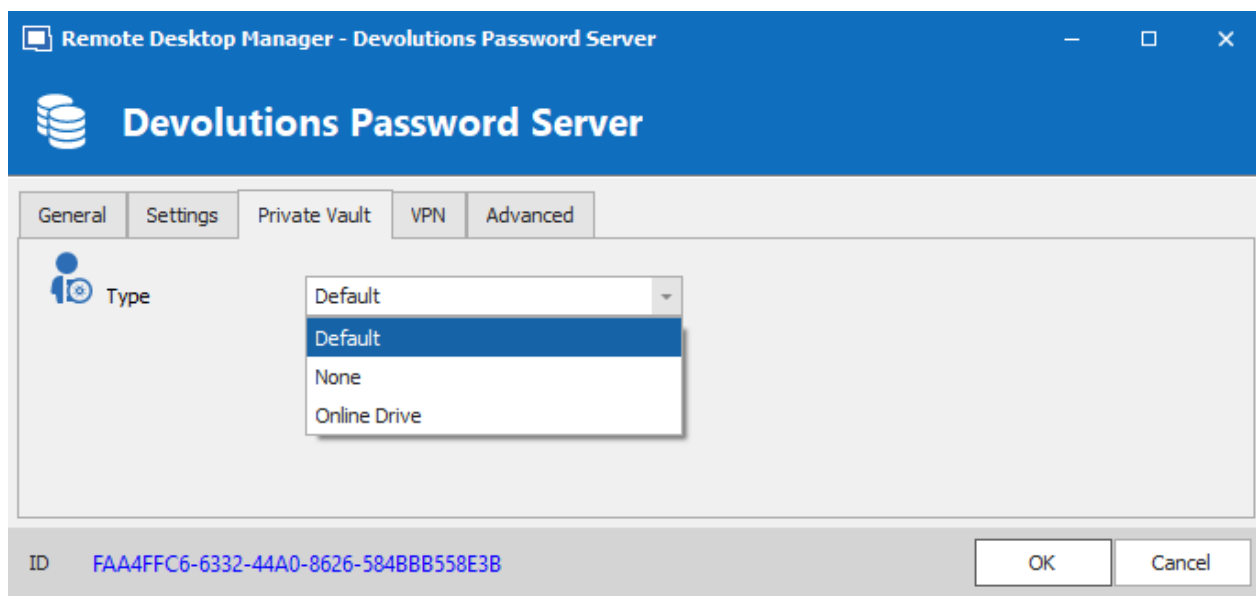
## SETTINGS



*Devolutions Password Server - Settings*

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

## PRIVATE VAULT



*Devolutions Password Server – Private Vault*

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

## VPN

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



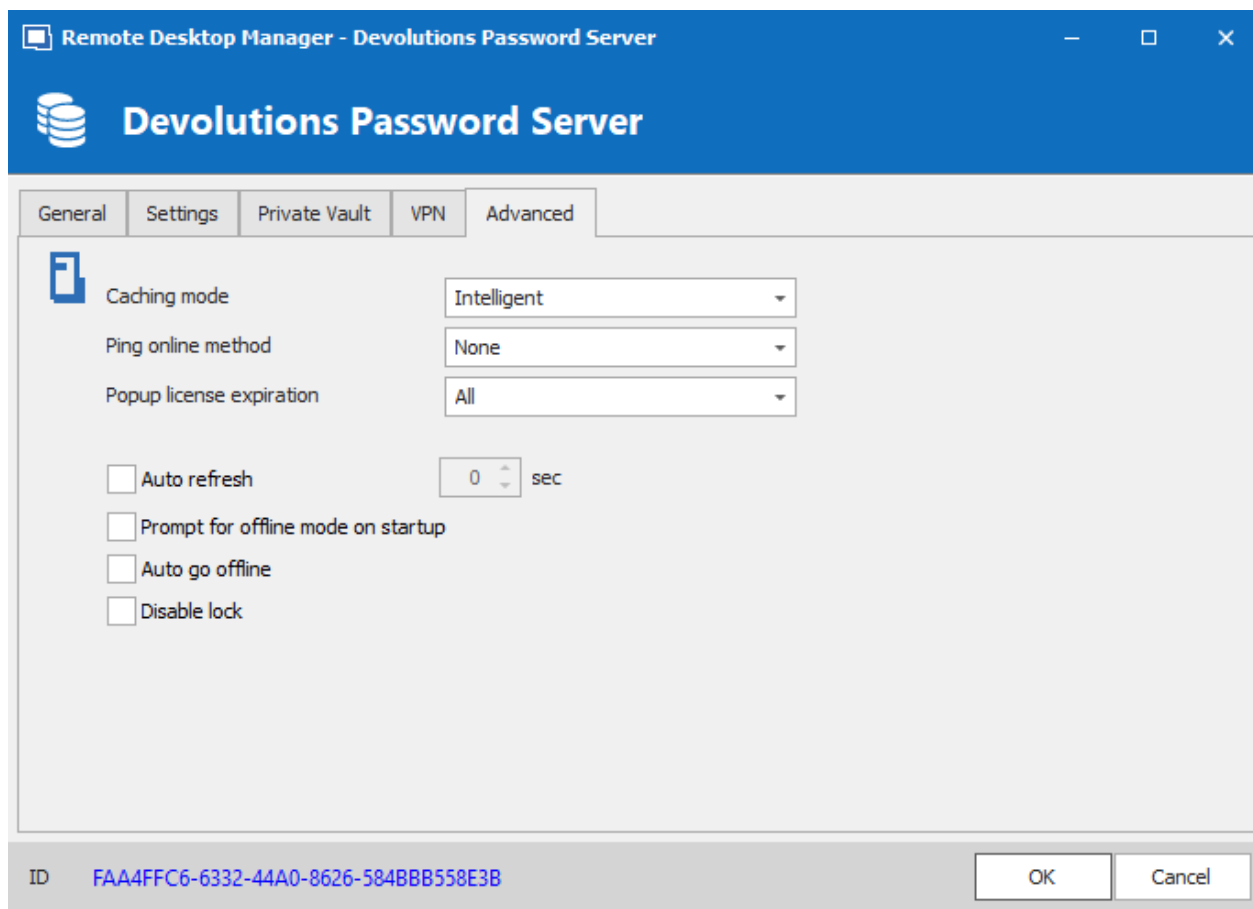
The screenshot shows a Windows-style application window titled "Remote Desktop Manager - Devolutions Password Server". The window has a blue header bar with the Devolutions logo and the text "Devolutions Password Server". Below the header is a tabbed interface with five tabs: "General", "Settings", "Private Vault", "VPN", and "Advanced". The "VPN" tab is currently selected. The main content area of the "VPN" tab contains the following elements:

- A "Type" dropdown menu set to "On first connect" with a play button icon to its right.
- An "RDM File" text input field with a browse button ("...") to its right.
- An "Override credentials" checkbox, which is currently unchecked.
- Below the checkbox, three text input fields labeled "Username", "Domain", and "Password".

At the bottom of the window, there is a status bar showing the ID "72D2AB22-1E9C-4D7F-A189-A740EDCA3290" and two buttons: "OK" and "Cancel".

*Devolutions Password Server - VPN*

## ADVANCED

*Devolutions Password Server - Advanced*

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

OPTION	DESCRIPTION
	<ul style="list-style-type: none"> <li>• <b>Disabled</b></li> </ul>
<b>Auto refresh</b>	Set the interval for the automatic refresh.
<b>Prompt for offline mode on startup</b>	Ask to use the data source in offline mode when the user connects to the data source.
<b>Auto go offline</b>	Use the data source in offline mode when the ping method does not respond.
<b>Disable lock</b>	Disable the option to lock the data source directly. The application still can be locked but the user is not prompted for the data source password when unlocking the application.

#### 5.4.1.3 MariaDB

## DESCRIPTION



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



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

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

## HIGHLIGHTS

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

- Full connection log and attachments support.

## SETTINGS

### GENERAL

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

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

At the bottom right of the settings area are two buttons: 'Test Host' and 'Test Schema'. At the very bottom of the window, there is an 'ID' field showing '20ACD0FB-60FC-4386-B44F-FF5E89F9C48D' and 'OK' and 'Cancel' buttons.

*MariaDB - General*

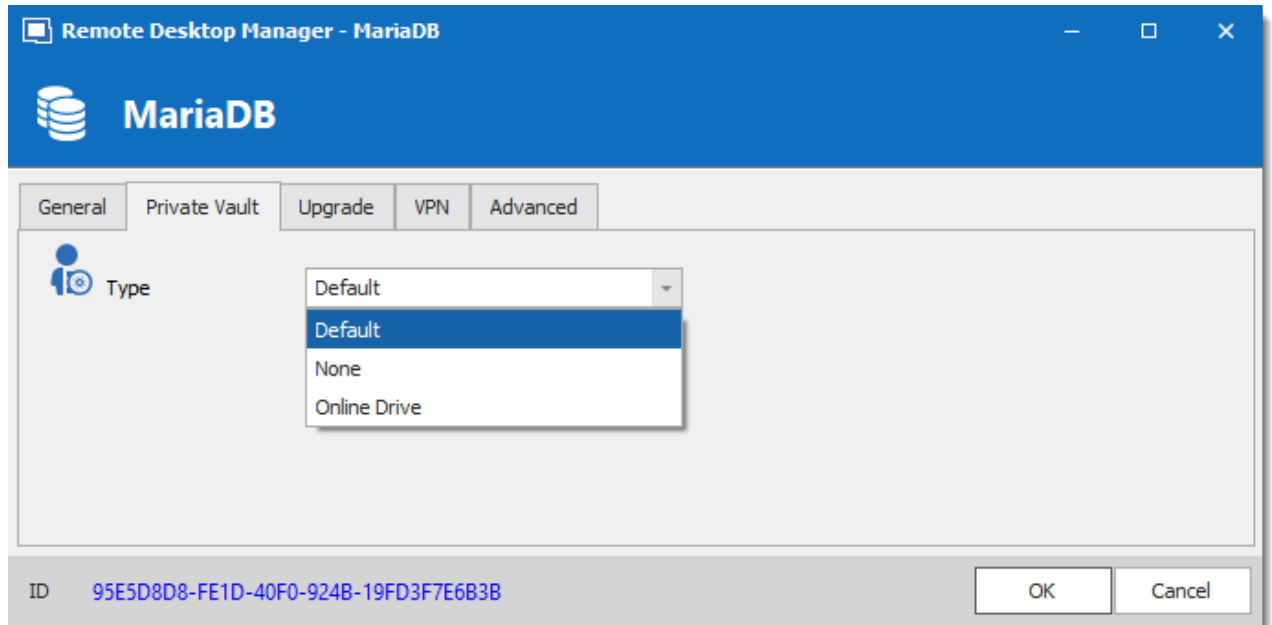
OPTION	DESCRIPTION
<b>Name</b>	Name of the data source.
<b>Host</b>	Name of the host (server name) where the data source will be stored.
<b>Username</b>	Username used to access the host server.

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

## PRIVATE VAULT

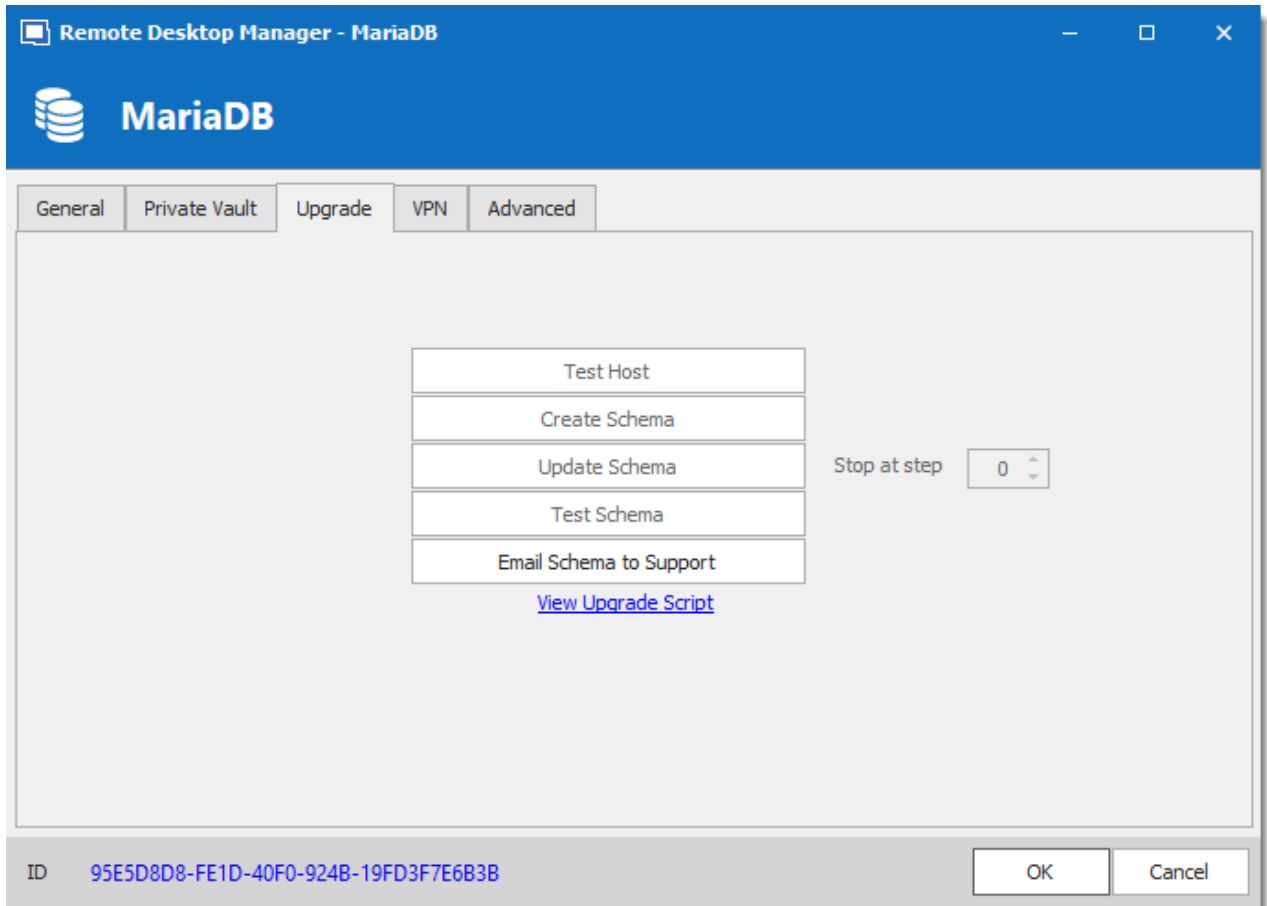
Connect your **MariaDB** to a **Private Vault** stored in a **Devolutions Online Drive** file (.dod), thus creating your own **Private Vault** containing entries and credentials that no one else has access to.

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



*MariaDB - Private Vault*

## UPGRADE

*MariaDB - Upgrade Tab*

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

OPTION	DESCRIPTION
<b>Email Schema to Support</b>	Send your schema (database) to the Devolutions Support team.
<b>View Upgrade Script</b>	Prompts a window to provide information about the Upgrade Script.

## VPN

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

The screenshot shows the 'Remote Desktop Manager - MariaDB' window with the 'VPN' tab selected. The window has a blue header with the MariaDB logo and title. Below the header are tabs for 'General', 'Private Vault', 'Upgrade', 'VPN', and 'Advanced'. The 'VPN' tab contains the following fields:

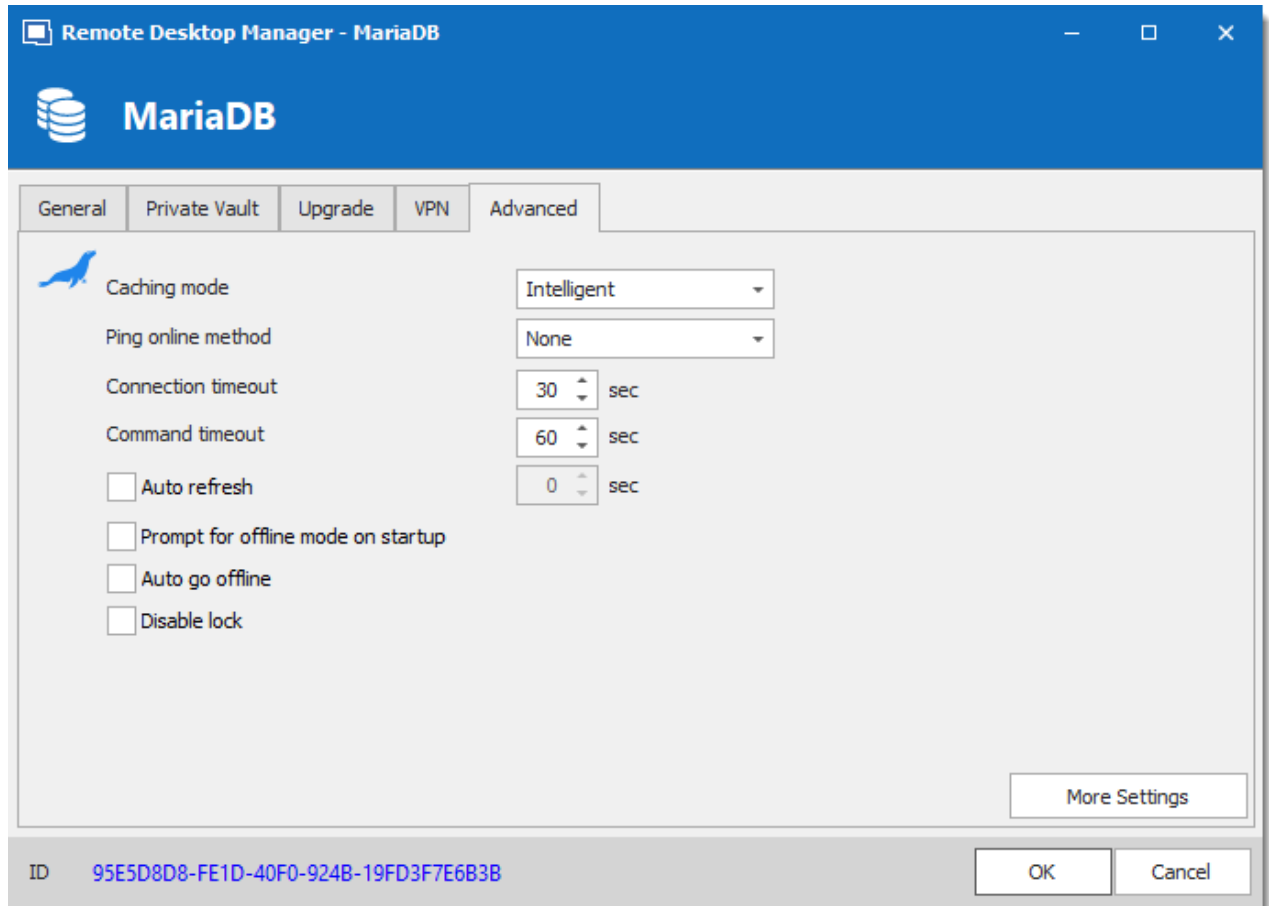
- Type:** A dropdown menu set to 'On first connect' with a play button icon to its right.
- RDM File:** A text input field with a browse button (three dots) to its right.
- Override credentials:** An unchecked checkbox.
- Username:** A text input field.
- Domain:** A text input field.
- Password:** A text input field.

At the bottom of the window, there is an 'ID' field with the value '95E5D8D8-FE1D-40F0-924B-19FD3F7E6B3B' and 'OK' and 'Cancel' buttons.

*MariaDB - VPN*

## ADVANCED





MariaDB - Advanced

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

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

#### 5.4.1.4 Microsoft SQL Azure

### DESCRIPTION



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

The following features are also supported:

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

## MINIMUM REQUIREMENT FOR AZURE SQL DATABASE FOR RDM

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

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

Visit their website for more information.

### HIGHLIGHTS

- Supports [User Management](#) with a superior security model.
- Supports [Offline mode](#) for when the server or network is unavailable.
- Supports entry logs and attachments.
- Used to create an online database. [Get more information on Microsoft SQL Azure](#).



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

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



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

### CONFIGURATION

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

### SETTINGS

#### GENERAL

Remote Desktop Manager - Microsoft SQL Azure

Microsoft SQL Azure

General Settings Private Vault Upgrade VPN Advanced

Name  SQL Azure

Host  ...

Login mode Database login

Username

Password

☐ Always ask password

☐ Allow change username

Database  ...

Two factor [None](#)

Test Database

ID 6C7F8787-BBEF-46A0-85D2-40AED736190C

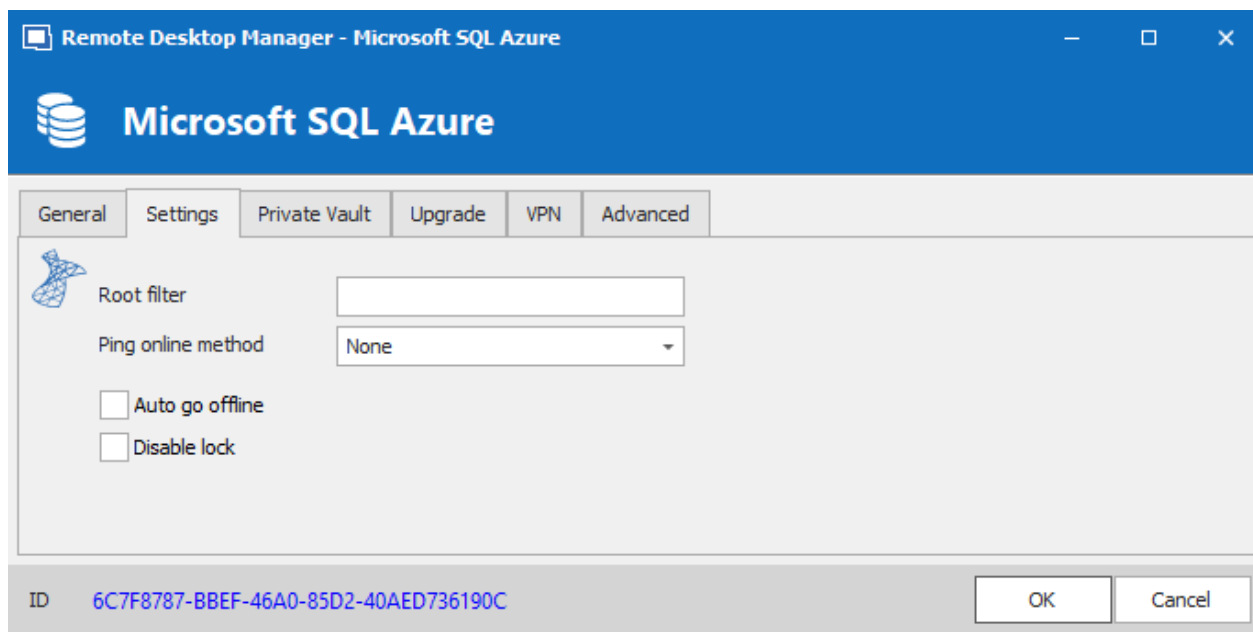
OK Cancel

Microsoft SQL Azure - General

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

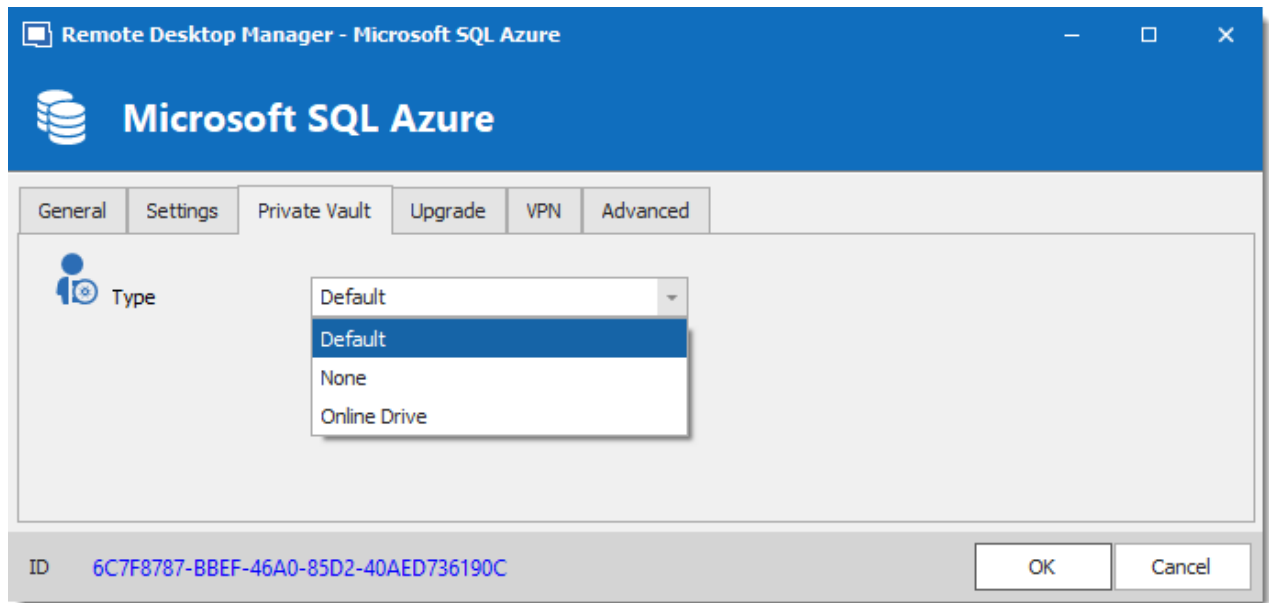
OPTION	DESCRIPTION
<b>Username</b>	Enter the username to access the SQL Azure database.
<b>Password</b>	Enter the password to access the SQL Azure database.
<b>Always ask password</b>	Prompt for the password when a user connects to the data source.
<b>Allow change username</b>	Allow the username to be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

## SETTINGS

*Microsoft SQL Azure - Settings Tab*

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

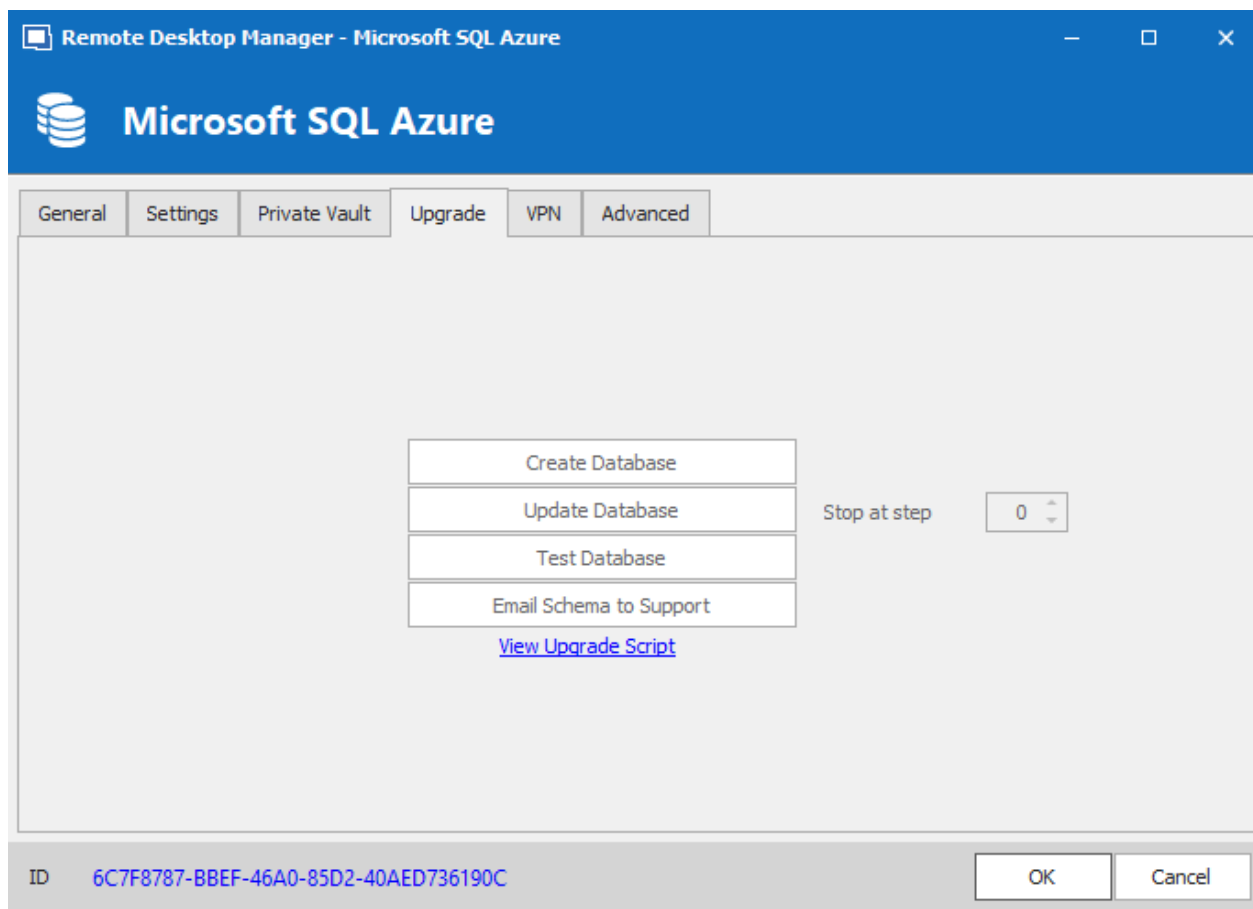
## PRIVATE VAULT



Microsoft SQL Azure - Private Vault Tab

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

## UPGRADE



*Microsoft SQL Azure - Upgrade Tab*

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



OPTION	DESCRIPTION
<b>View Upgrade Script</b>	Prompts a window to provide information about the Upgrade Script.

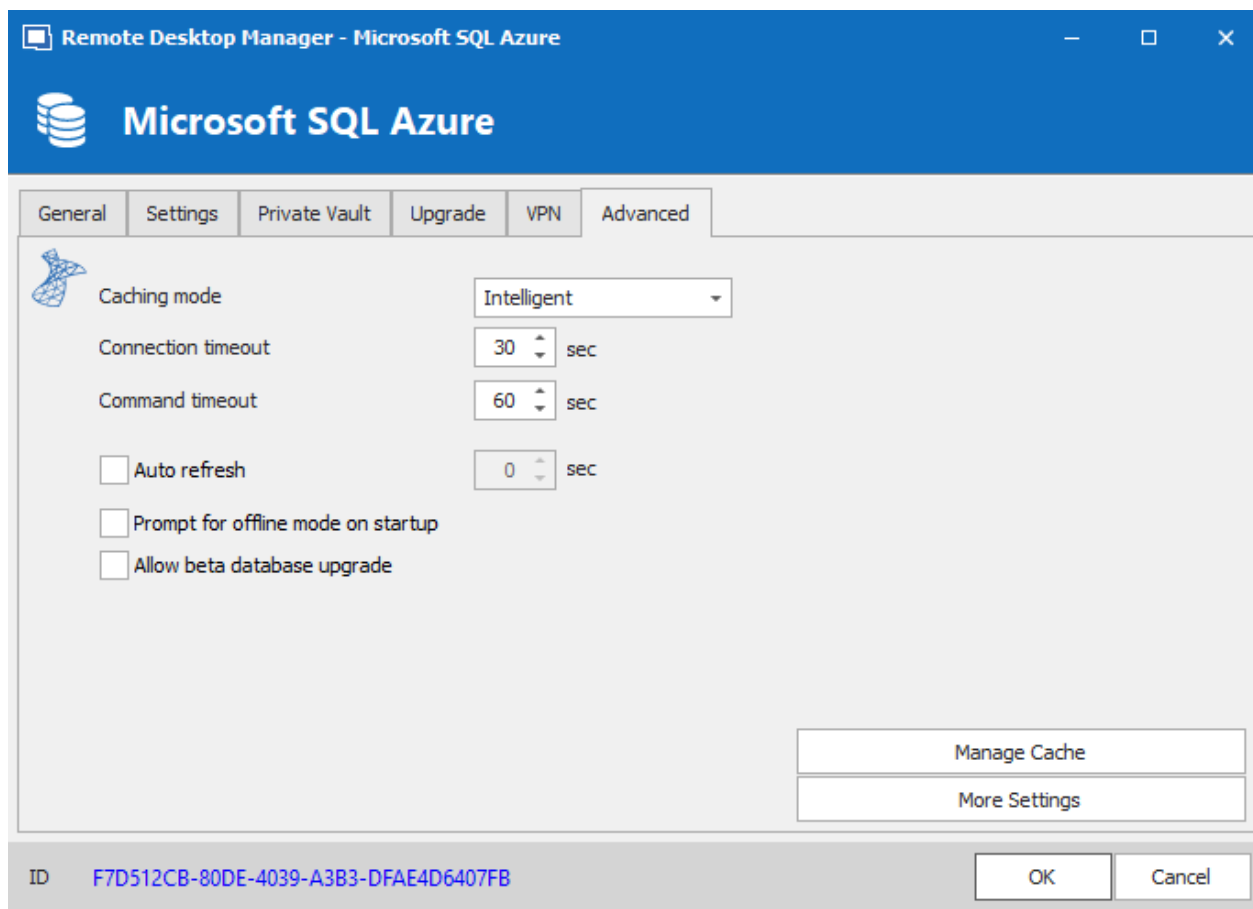
## VPN

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

The screenshot shows the 'Remote Desktop Manager - Microsoft SQL Azure' window. The 'VPN' tab is selected. The 'Type' dropdown is set to 'On first connect'. The 'RDM File' field is empty. The 'Override credentials' checkbox is unchecked. The 'Username', 'Domain', and 'Password' fields are empty. The 'ID' field at the bottom left displays '6C7F8787-BBEF-46A0-85D2-40AED736190C'. The 'OK' and 'Cancel' buttons are at the bottom right.

Microsoft SQL Azure - VPN

## ADVANCED



*Microsoft SQL Azure - Advanced Tab*

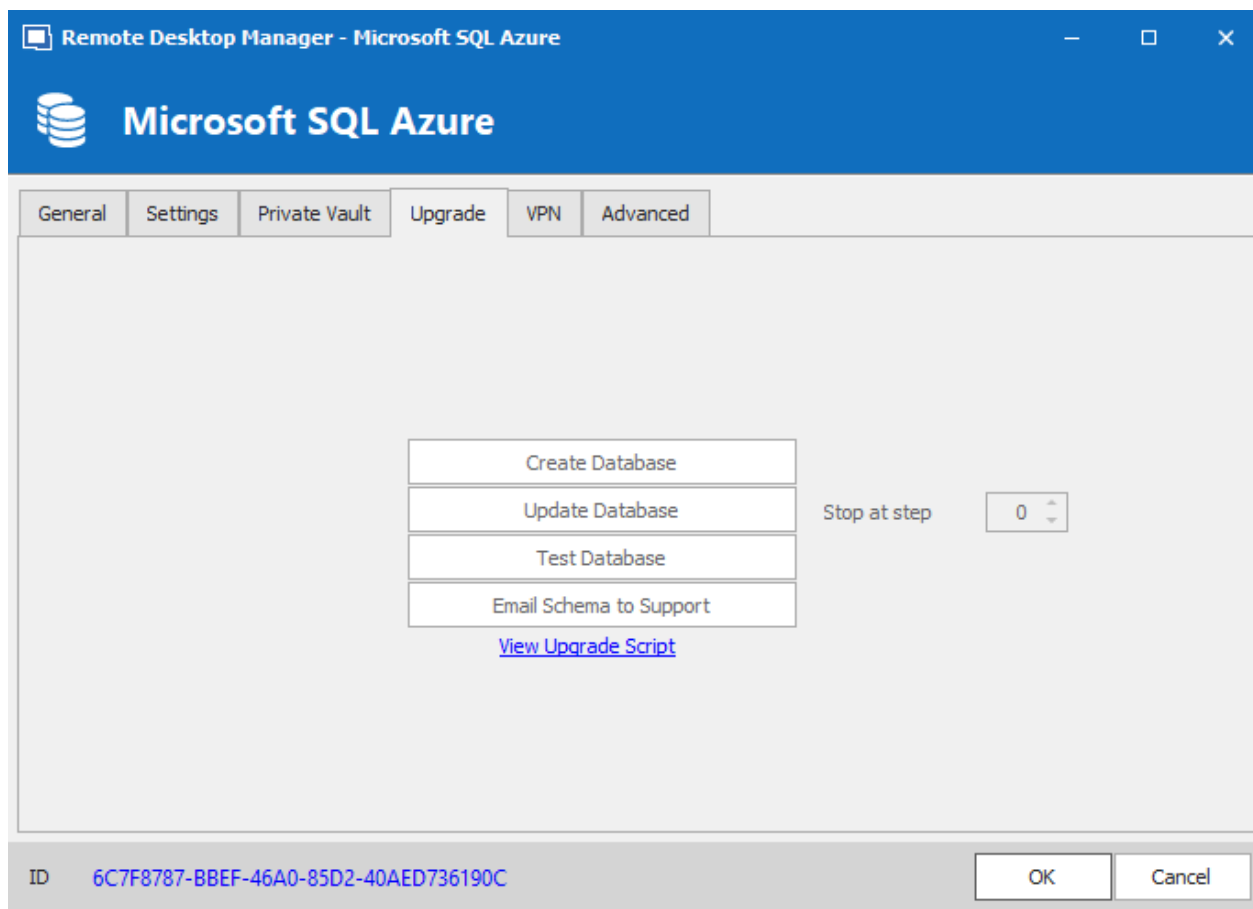
OPTION	DESCRIPTION
<b>Caching mode</b>	Determines how the entries will be reloaded in the data source. For more information, please consult the <a href="#">Caching</a> topic.
<b>Connection timeout</b>	Set the delay of the connection timeout.
<b>Command timeout</b>	Set the delay of the command timeout.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

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

#### 5.4.1.4.1 Configure SQL Azure

## DESCRIPTION

1. Make sure that you have a valid **Microsoft SQL Azure** subscription to be able to create your database.
2. Follow the steps in the [Create a data source](#) topic. On Step 4, before testing server or otherwise verifying the connection, continue with the steps below.
3. Select the **Upgrade** tab and click the **Create Database** button. If the database is already created on the Microsoft SQL Azure Server, click the **Update Database** button to add the appropriate tables to the database.

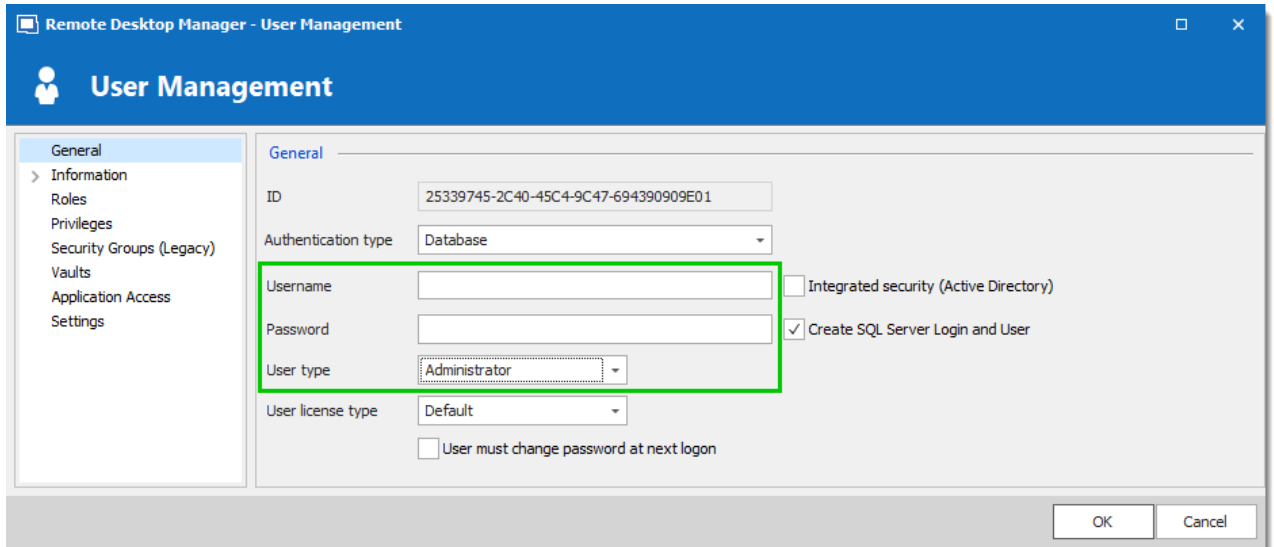


*Upgrade Tab*

4. Once the database is created, create an administrator account for the database via the [Administration - User Management](#) menu.



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



Remote Desktop Manager - User Management

**User Management**

General

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

General

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

Authentication type: Database

Username:

Password:

User type: Administrator

User license type: Default

☐ Integrated security (Active Directory)

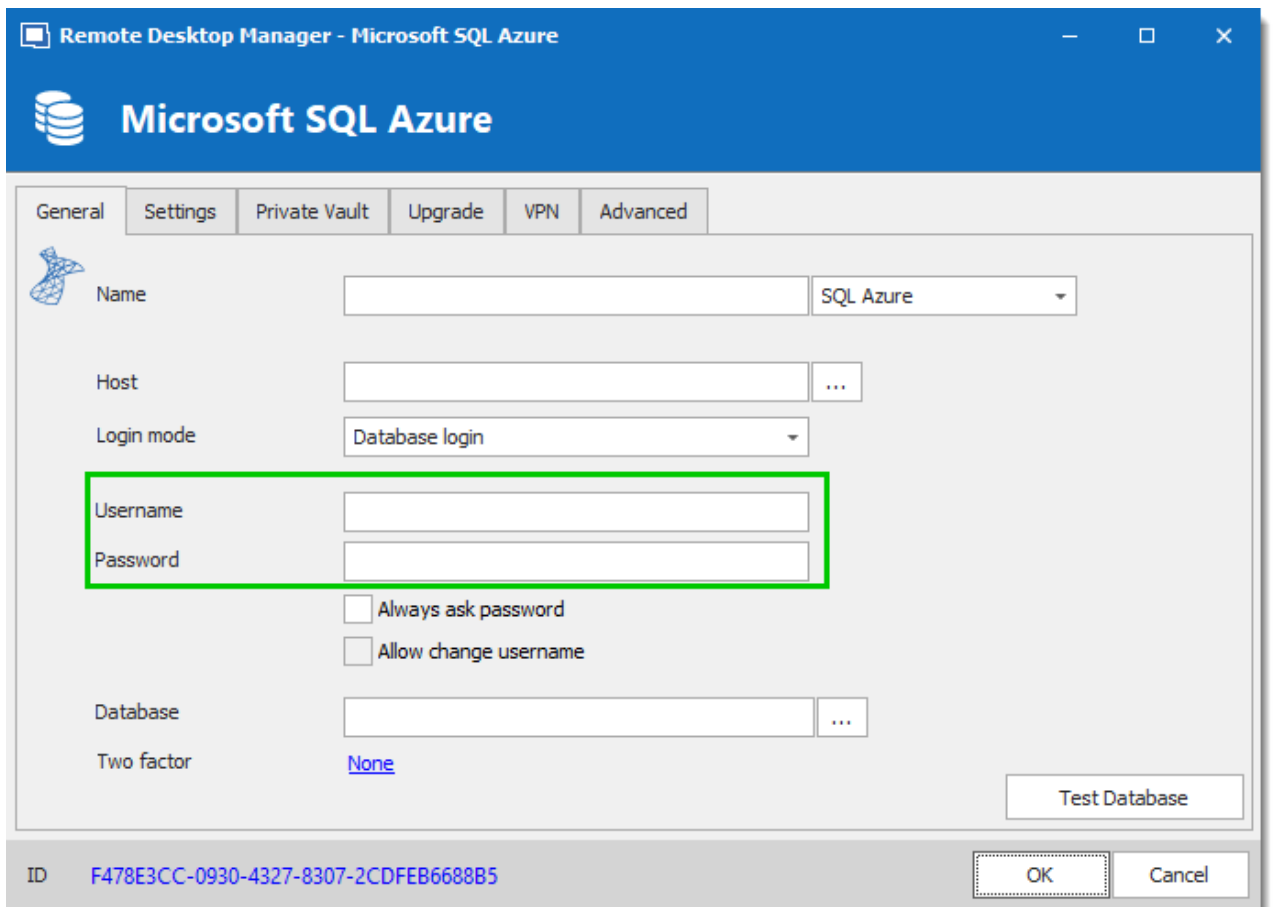
☒ Create SQL Server Login and User

☐ User must change password at next login

OK Cancel

*Create a Remote Desktop Manager Administrator Account*

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



Remote Desktop Manager - Microsoft SQL Azure

**Microsoft SQL Azure**

General Settings Private Vault Upgrade VPN Advanced

Name:  SQL Azure

Host:  ...

Login mode: Database login

Username:

Password:

☐ Always ask password

☐ Allow change username

Database:  ...

Two factor: [None](#)

Test Database

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

OK Cancel

*Connection to the Database with the RDM Administrator Account*

The Microsoft SQL Azure data source is now correctly configured.

#### 5.4.1.4.2 Enable Azure Active Directory Authentication

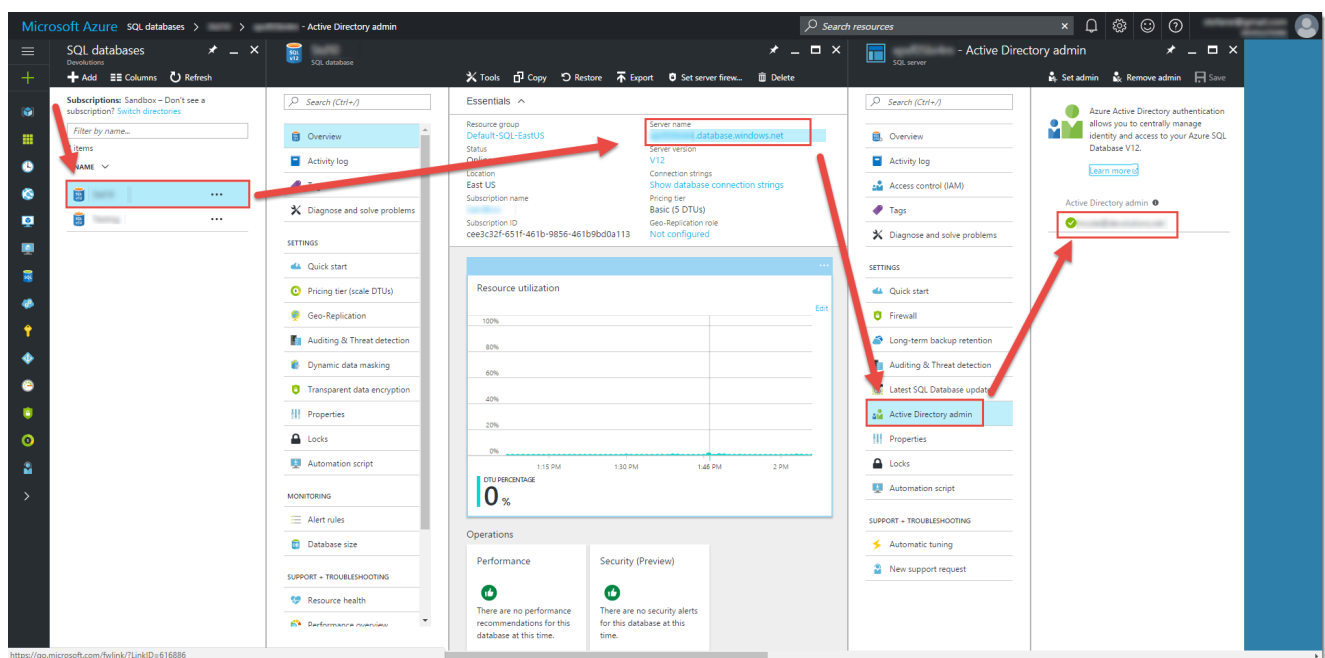
##### 5.4.1.4.2.1 Configure the Active Directory Admin

## DESCRIPTION

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

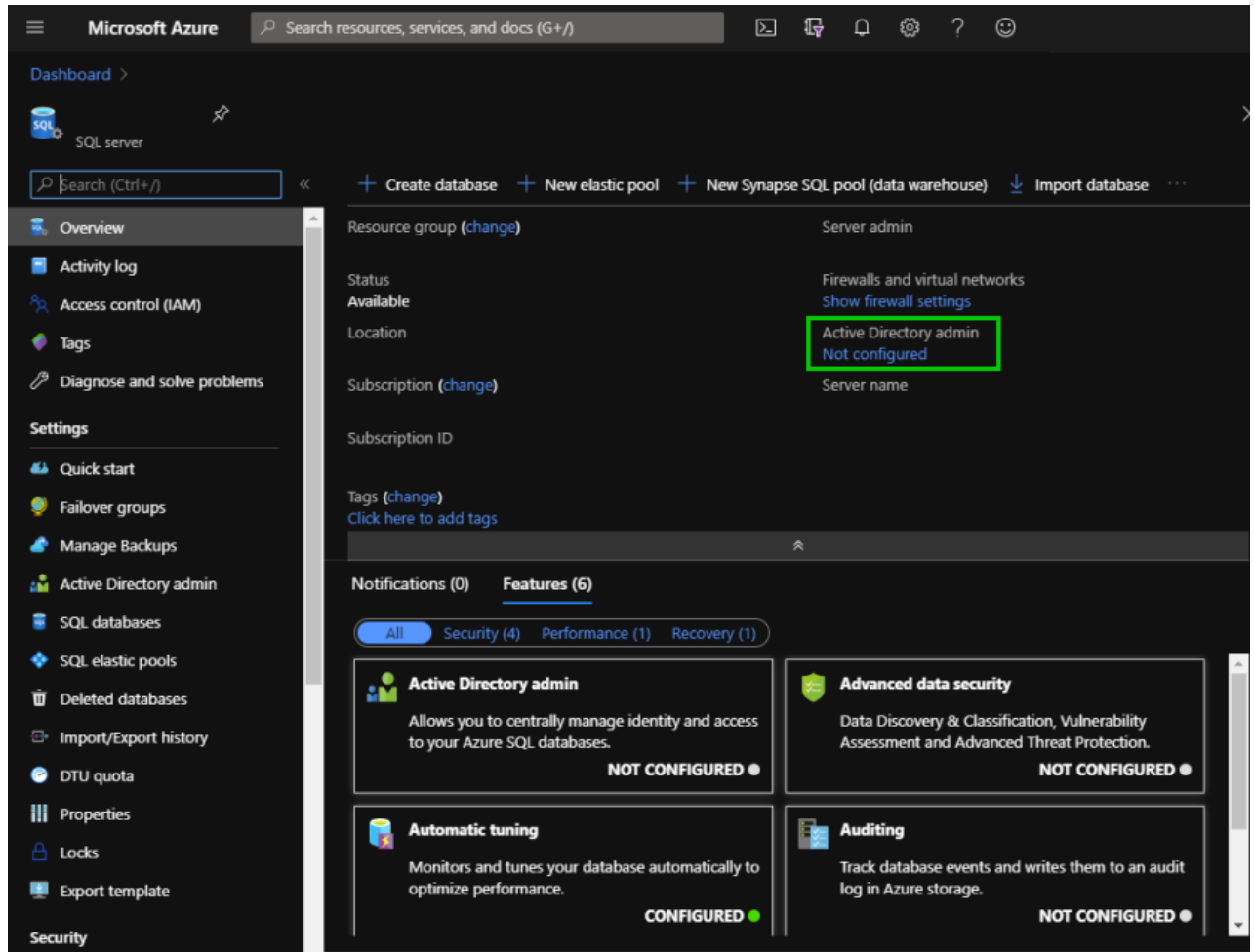


It may take a few minutes for this change to propagate. You might experience a time delay before being able to connect with this Active Directory account.

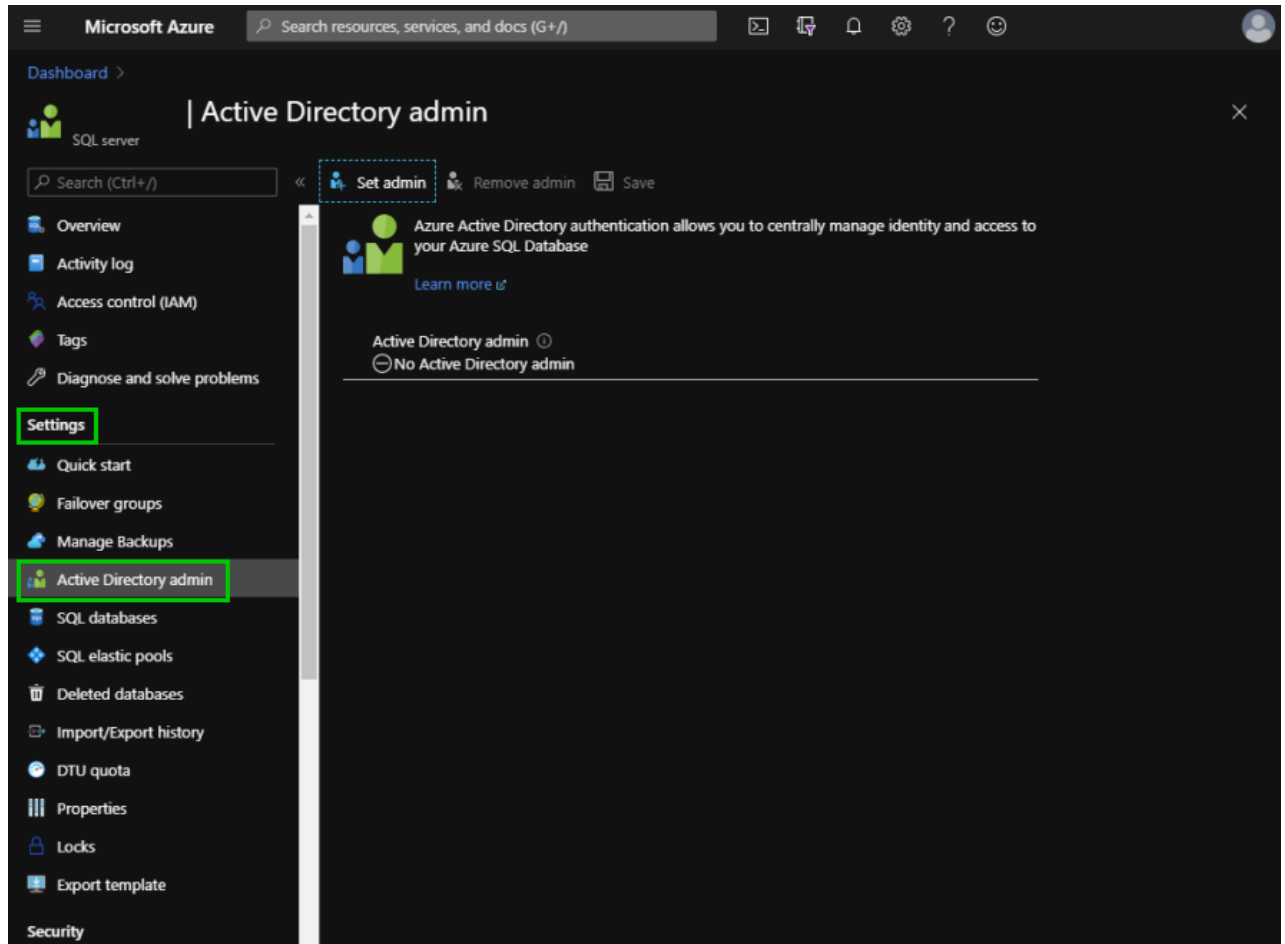


Azure AD Portal

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

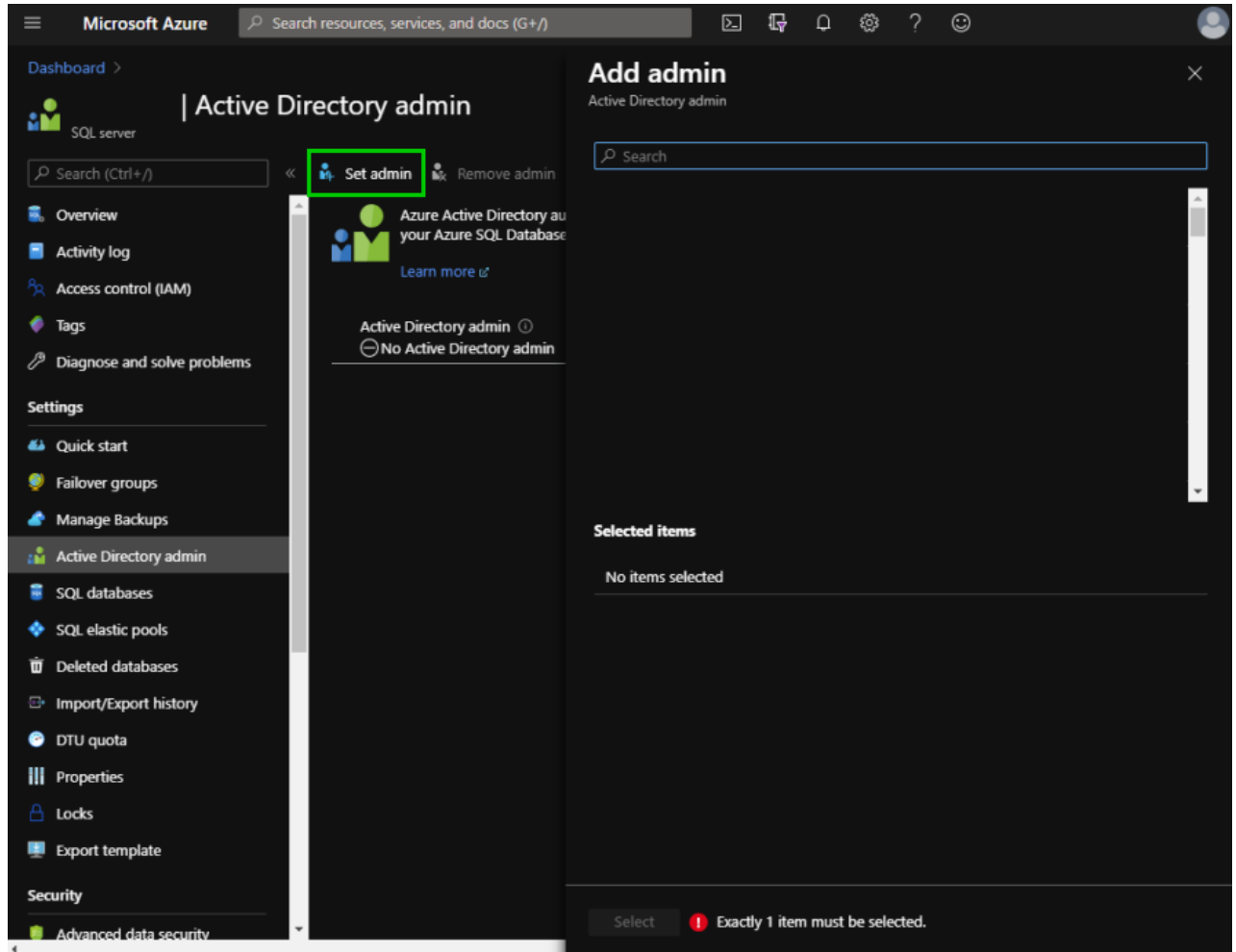


2. Click on **Active Directory admin** under **Settings** in the left menu.

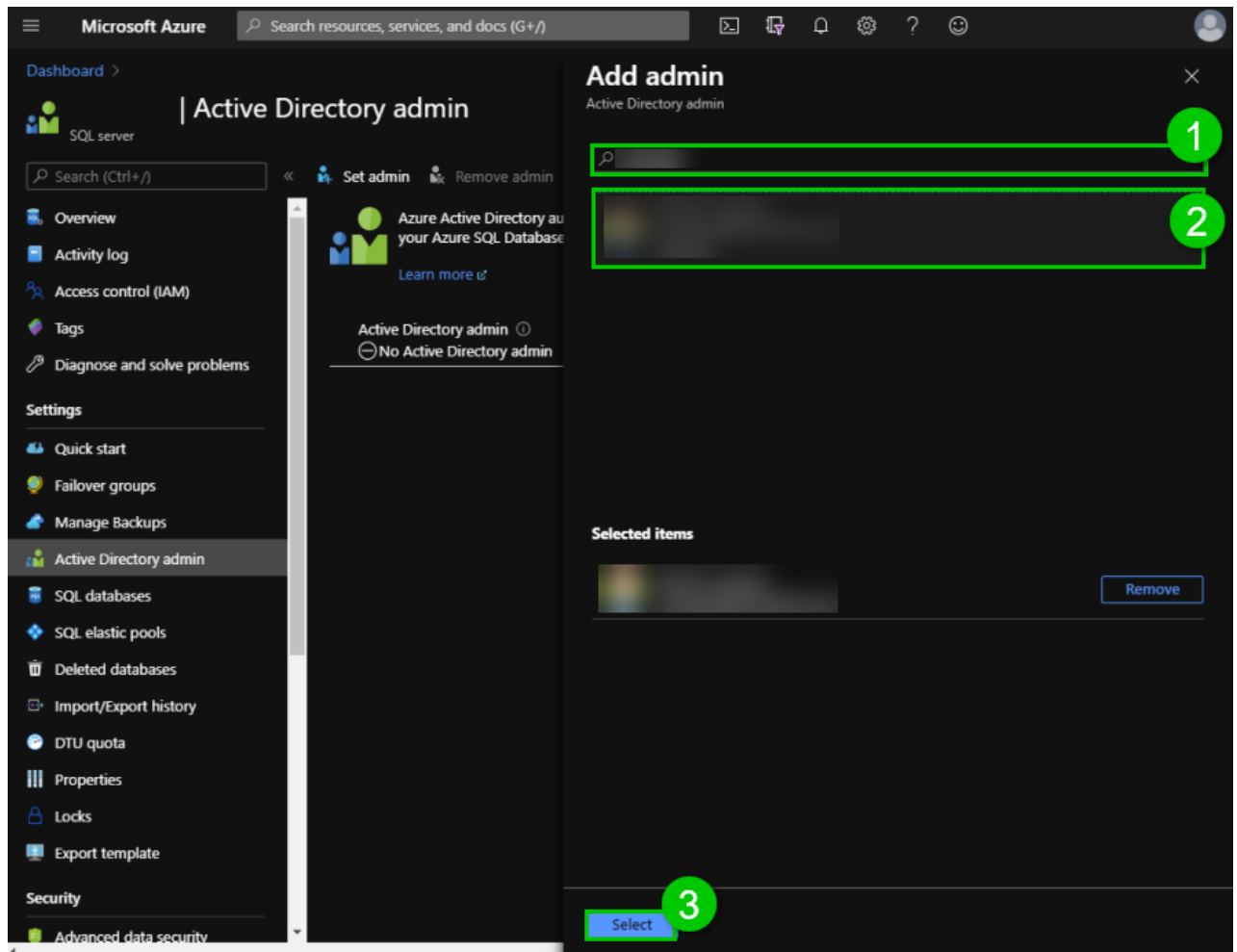


3. Click on **Set admin** to search for the admin.

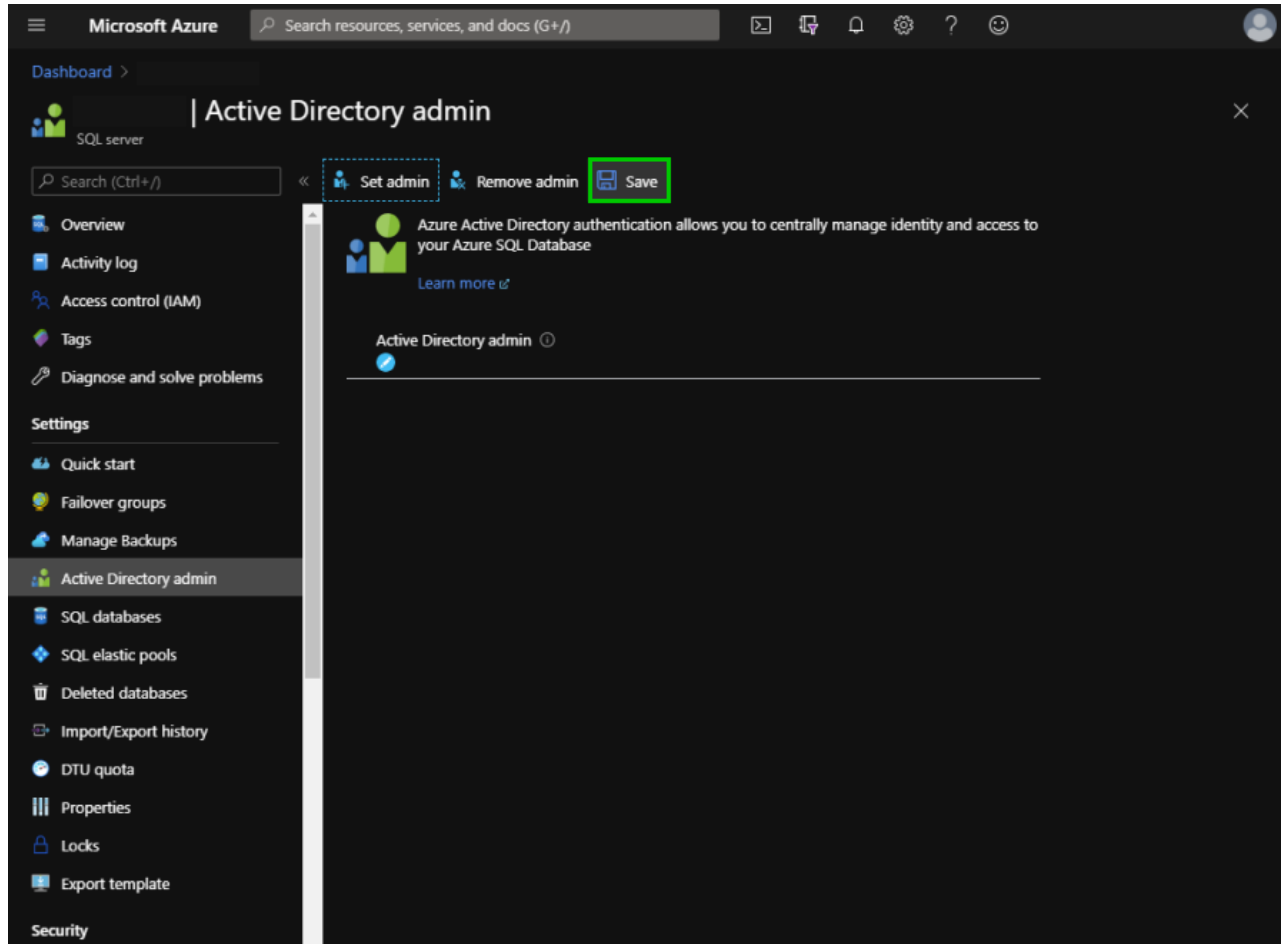




4. Type the admin name in the **Search** field, click on the admin in the list provided and then **Select**.



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



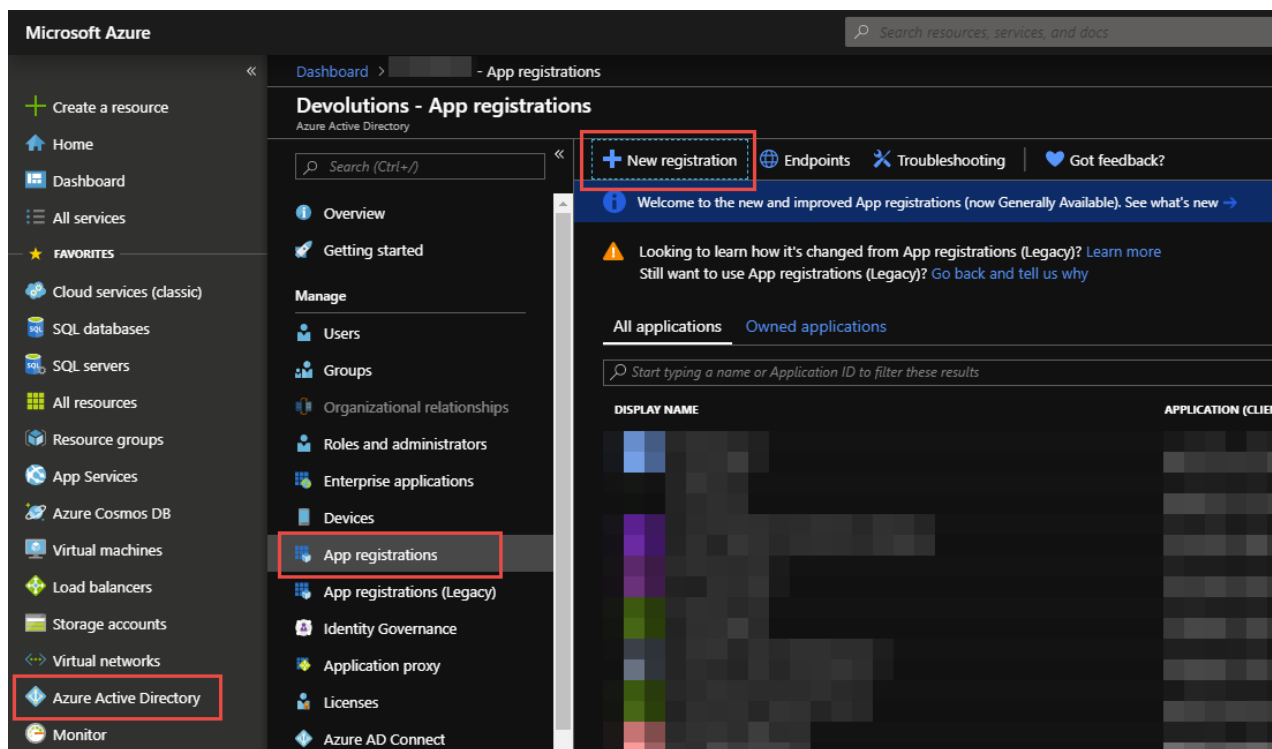
#### 5.4.1.4.2.2 Create an Azure Active Directory App Registration

## DESCRIPTION

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

## SETTINGS

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



App Registration

3. Configure the **Name**, **Supported account types** and **Redirect URI** as indicated below and click **Register**.



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

## Register an application

### \* Name

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

RDM-App-Registration ✓

### Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Devolutions only - Single tenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[Help me choose...](#)

### Redirect URI (optional)

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

Public client/native (mobile ... ▼

https://mycompany.com ✓

*Supported Account Types*

4. Click on the **API Permissions** section and configure it as indicated below.

Dashboard > Devolutions - App registrations > [App Name] - API permissions

## [App Name] - API permissions

Overview Quickstart

**Manage**

- Branding
- Authentication
- Certificates & secrets
- API permissions**
- Expose an API
- Owners
- Manifest

**Support + Troubleshooting**

- Troubleshooting
- New support request

### API permissions

Applications are authorized to use APIs by requesting permissions. You can grant/deny access.

[+ Add a permission](#)

API / PERMISSIONS NAME	TYPE
Microsoft Graph (1)	
User.Read	Dele

These are the permissions that this application requests statically. You can also request permissions dynamically through code. [See best practices for](#)

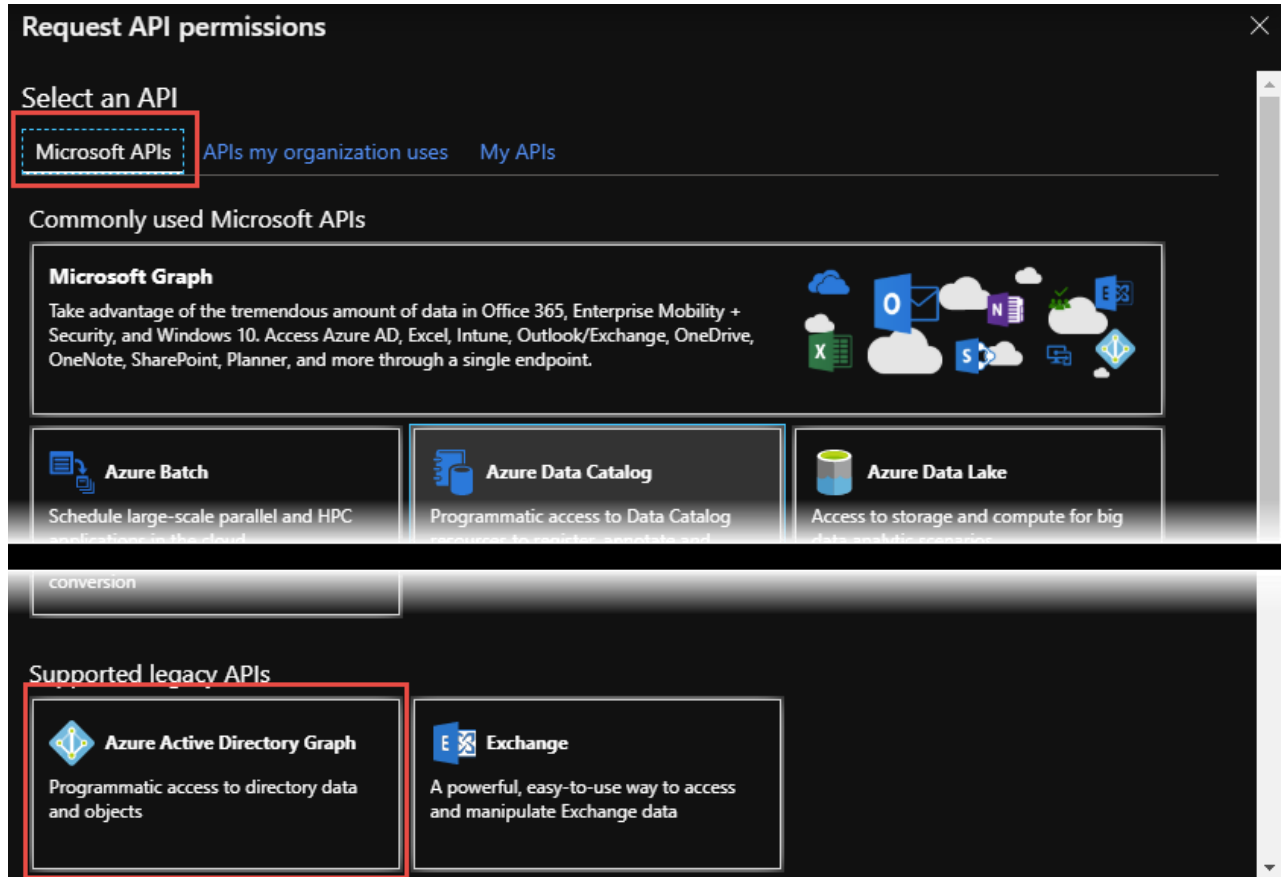
### Grant consent

As an administrator, you can grant consent on behalf of all users in your organization. This means that end users will not be shown a consent screen when using the application.

[Grant admin consent for Devolutions](#)

API Permissions

5. Select **Microsoft APIs** and scroll down to the **Supported Legacy APIs** and select **Azure Active Directory Graph**.





*Azure Active Directory Graph*

6. Select **Delegated Permissions – User – User.Read** and click on **Add Permissions**.

## Request API permissions

< All APIs

 **Azure Active Directory Graph**  
<https://graph.windows.net/> [Docs](#)

 Azure Active Directory Graph APIs are available via the Microsoft Graph API. You may want to consider using Microsoft Graph instead.

What type of permissions does your application require?

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

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

Select permissions expand all

Type to search

PERMISSION	ADMIN CONSENT REQUIRED
▶ Directory	
▶ Group	
▶ Member	
▼ User (1)	
<input checked="" type="checkbox"/> <b>User.Read</b> Sign in and read user profile ⓘ	-
<input type="checkbox"/> <b>User.Read.All</b> Read all users' full profiles ⓘ	Yes
<input type="checkbox"/> <b>User.ReadBasic.All</b> Read all users' basic profiles ⓘ	-

Add permissions

Discard

User.Read

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



**Request API permissions**

Select an API

[Microsoft APIs](#) **APIs my organization uses** [My APIs](#)

Apps in your directory that expose APIs are shown below

NAME	APPLICATION (CLIENT) ID
Azure Analysis Services	4ac7d521-0382-477b-b0f8-7e1d95f85ca2
Azure Container Registry	6a0ec4d3-30cb-4a83-91c0-ae56bc0e3d26
Azure Data Lake	e9f49c6b-5ce5-44c8-925d-015017e9f7ad
Azure DevOps	499b84ac-1321-427f-aa17-267ca6975798
Azure Key Vault	cfa8b339-82a2-471a-a3c9-0fc0be7a4093
Azure Media Services	374b2a64-3b6b-436b-934c-b820eacca870
Azure Pipelines Hub (Prod)	4a01d87e-8a5d-464d-b2c4-b79c37359a12
Azure Pipelines Hub (Staging)	602e6588-03e5-4c84-ad02-9552a6521637
<b>Azure SQL Database</b>	<b>022907d3-0f1b-48f7-badc-1ba6abab6d66</b>
Azure Storage	e406a681-f3d4-42a8-90b6-c2b029497af1
AzureDatabricks	2ff814a6-3304-4ab8-85cb-cd0e6f879c1d

*APIs my organization uses*

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

**Request API permissions**

< All APIs

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

What type of permissions does your application require?

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

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

Select permissions expand all

Type to search

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

**Add permissions** **Discard**

*user\_impersonation*

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

**API permissions**

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

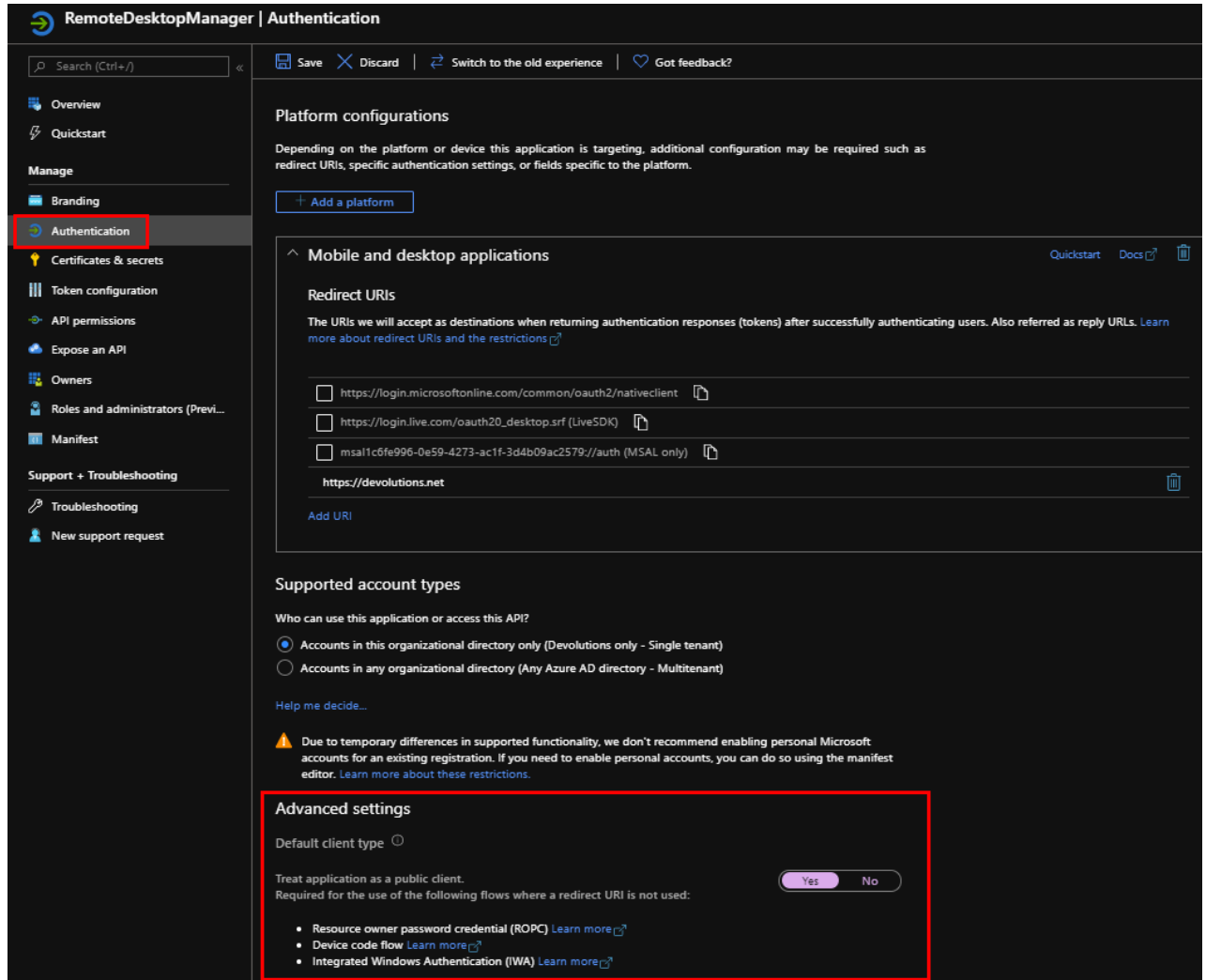
[+ Add a permission](#)

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

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

*API / Permissions Name*

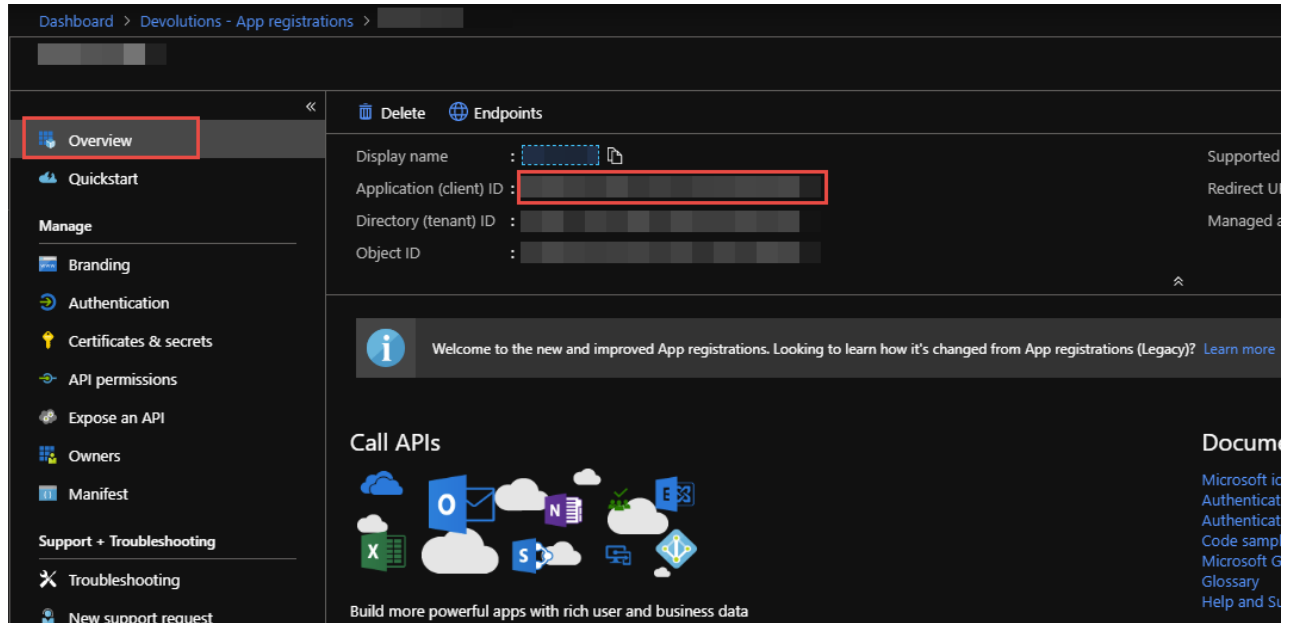
10. **Optional step:** Click on the **Authentication** section and switch to **Yes**, if you desire the **Integrated Windows Authentication (IWA)** option



### Authentication

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

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



Application (client) ID

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

## DESCRIPTION

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



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

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



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

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

## SETTINGS

Remote Desktop Manager - Microsoft SQL Azure

Microsoft SQL Azure

General Settings Private Vault Upgrade VPN Advanced

Name SQL Azure

Host .database.windows.net

Login mode Active Directory Interactive (with MFA support) Shared

Username @devolutions.net

Azure App Settings Configured

☐ Allow change username

Database

Two factor None

Test Database

ID

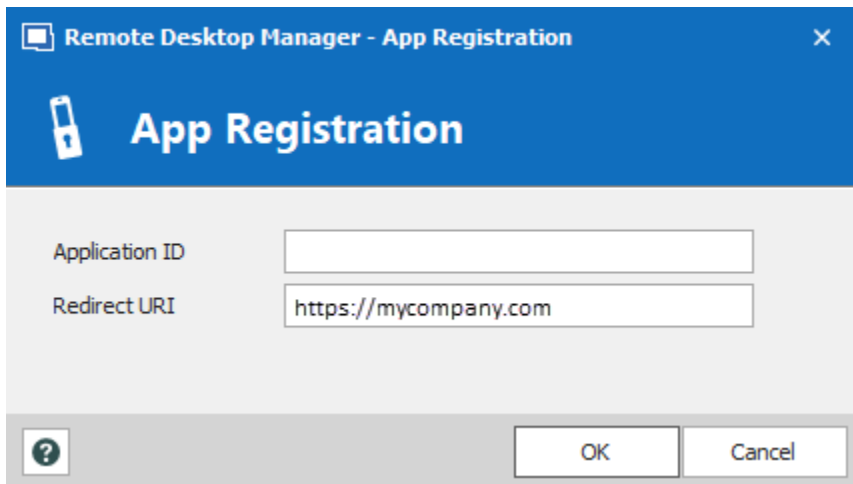
OK Cancel

Azure with MFA

1. Select **Active Directory Interactive (with MFA Support)** from the **Login mode** dropdown menu.
2. If you have several [Microsoft SQL Azure](#) data sources, you would need to decide if you want to authenticate on each of them at the first connection or only once for all of them.

OPTION	DESCRIPTION
<b>Default</b>	Prompt to authenticate on each data source.
<b>Shared</b>	Prompt to authenticate on the first data source and will use the same login on the other data sources. Easier to switch from one data source to another if you have several of them.

3. Enter the complete email address to authenticate in the **Username** field.
4. Click on **Configure** to set the [Azure App Settings](#) and enter the application ID from the Azure Active Directory App Registration and the corresponding Redirect URI.



*App Registration*

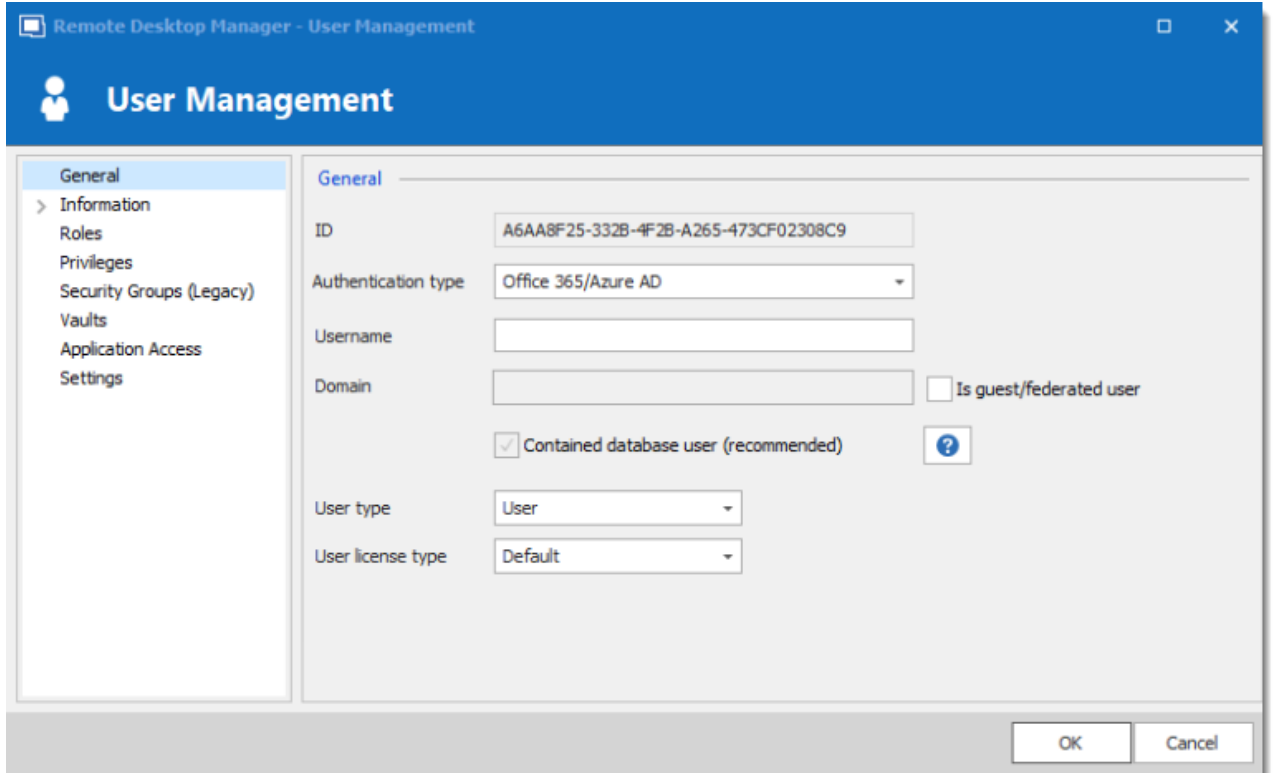
5. Configure the database to authenticate in the **Database** field.

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

## DESCRIPTION

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

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



Remote Desktop Manager - User Management

## User Management

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

**General**

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

Authentication type: Office 365/Azure AD

Username:

Domain:

☐ Is guest/federated user

☒ Contained database user (recommended) ?

User type: User

User license type: Default

OK Cancel

*Set the Authentication type to Office365/Azure AD*



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

#### 5.4.1.5 Microsoft SQL Server

## DESCRIPTION



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

### **Supported Microsoft SQL Server:**

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

The following features are also supported:

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

## **HIGHLIGHTS**

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



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





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



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

## CONFIGURATION

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

## SETTINGS

### GENERAL

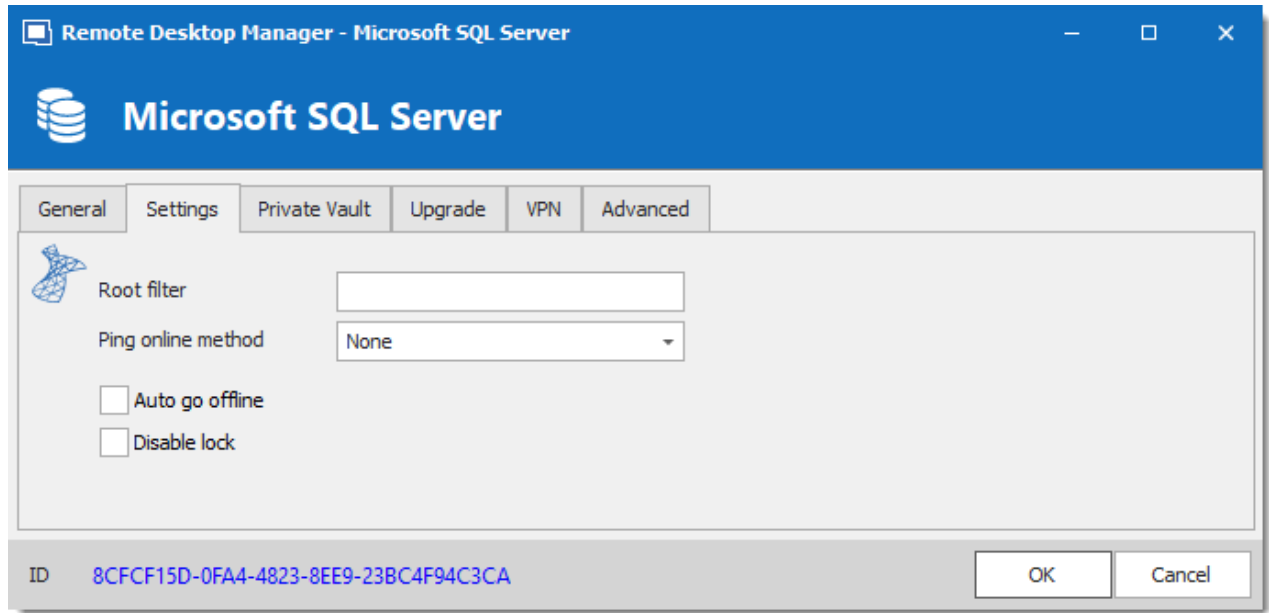
The screenshot shows the 'Remote Desktop Manager - Microsoft SQL Server' window. The title bar includes standard window controls. Below the title bar is a blue header with the Microsoft SQL Server logo and name. A tabbed interface at the top shows 'General' as the active tab, with other tabs like 'Settings', 'Private Vault', 'Upgrade', 'VPN', and 'Advanced' visible. The 'General' tab contains several input fields: 'Name' (text box), 'Host' (text box with a browse button), 'Login mode' (dropdown menu set to 'Database login'), 'Username' (text box), 'Password' (text box), and 'Database' (text box with a browse button). There are also two checkboxes: 'Always ask password' and 'Allow change username'. A 'Two factor' section shows 'None' as the selected option. At the bottom right of the main area are 'Test Server' and 'Test Database' buttons. The bottom status bar displays an 'ID' field with the value '5E049217-8A7A-4C88-AA6D-33D5CFC29593' and 'OK' and 'Cancel' buttons.

Microsoft SQL Server - General Tab

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

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

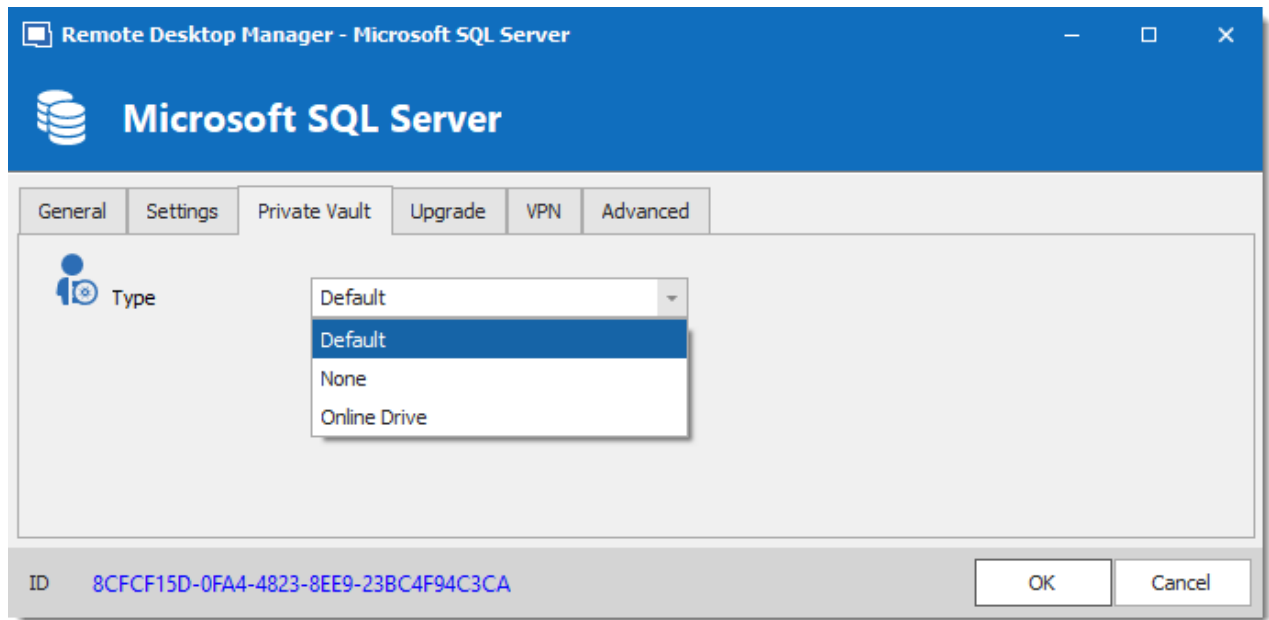
## SETTINGS



Microsoft SQL Server - Settings Tab

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

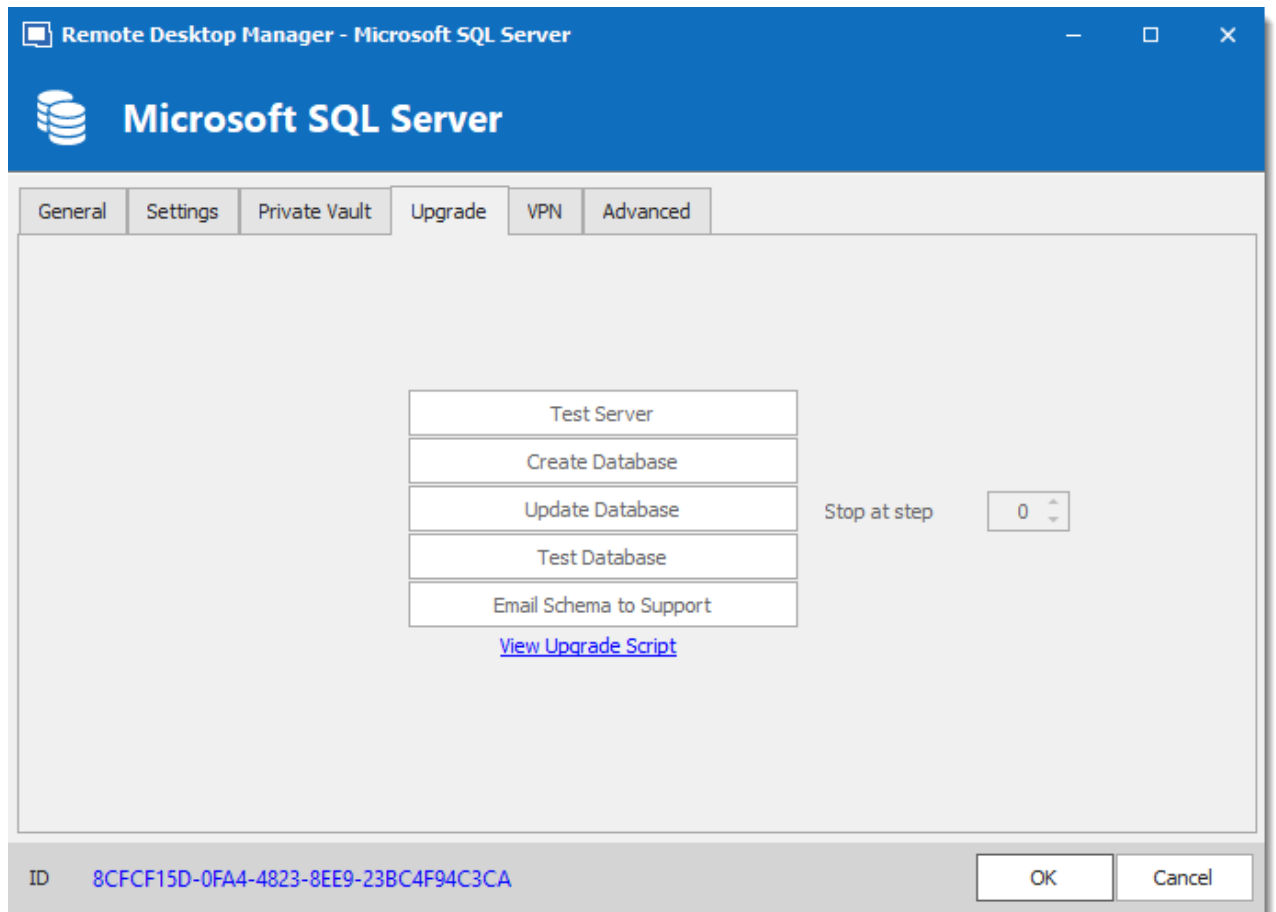
## PRIVATE VAULT



Microsoft SQL Server - Private Vault Tab

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

## UPGRADE



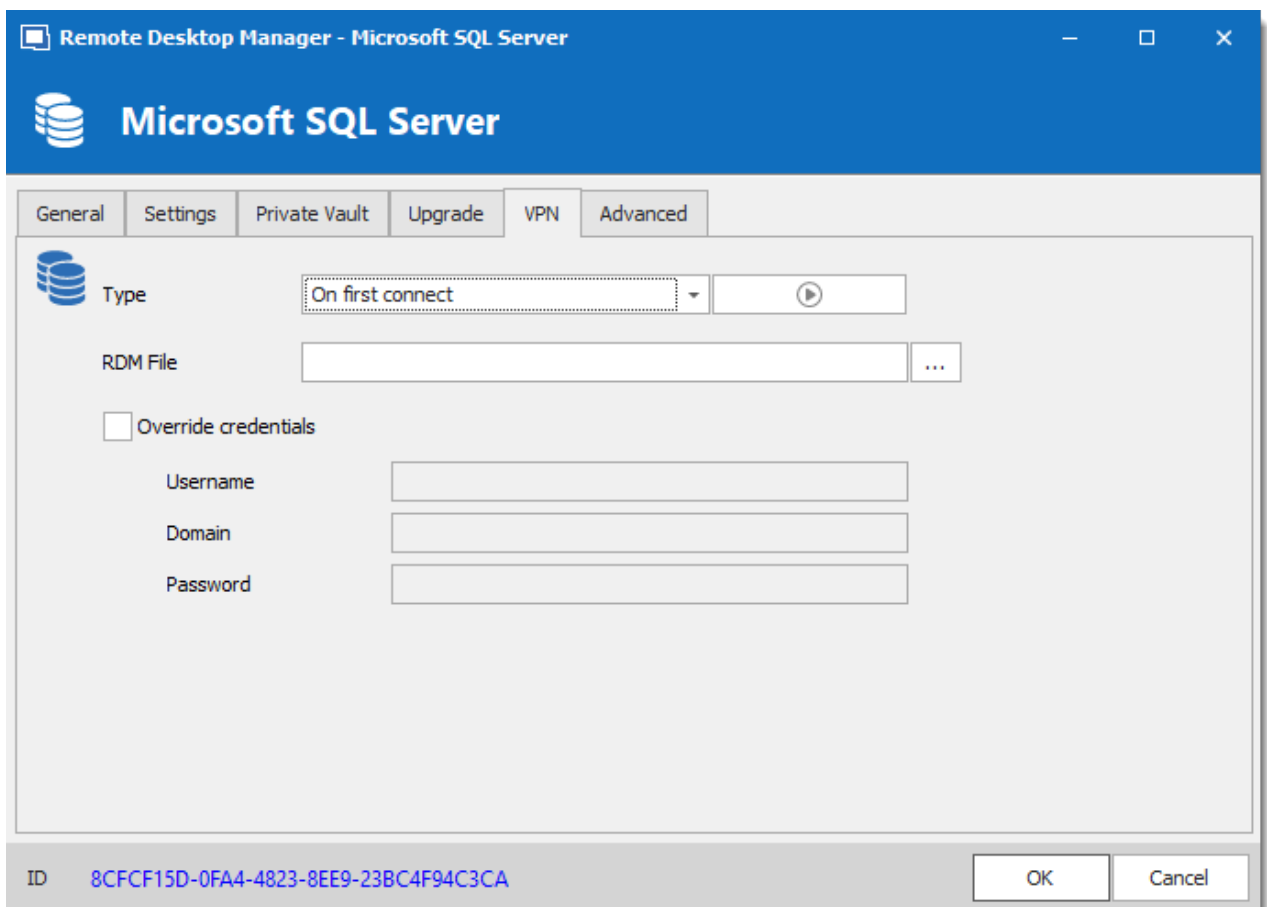
*Microsoft SQL Server - Upgrade Tab*

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

OPTION	DESCRIPTION
<b>View Upgrade Script</b>	Open the upgrade script in a new window.

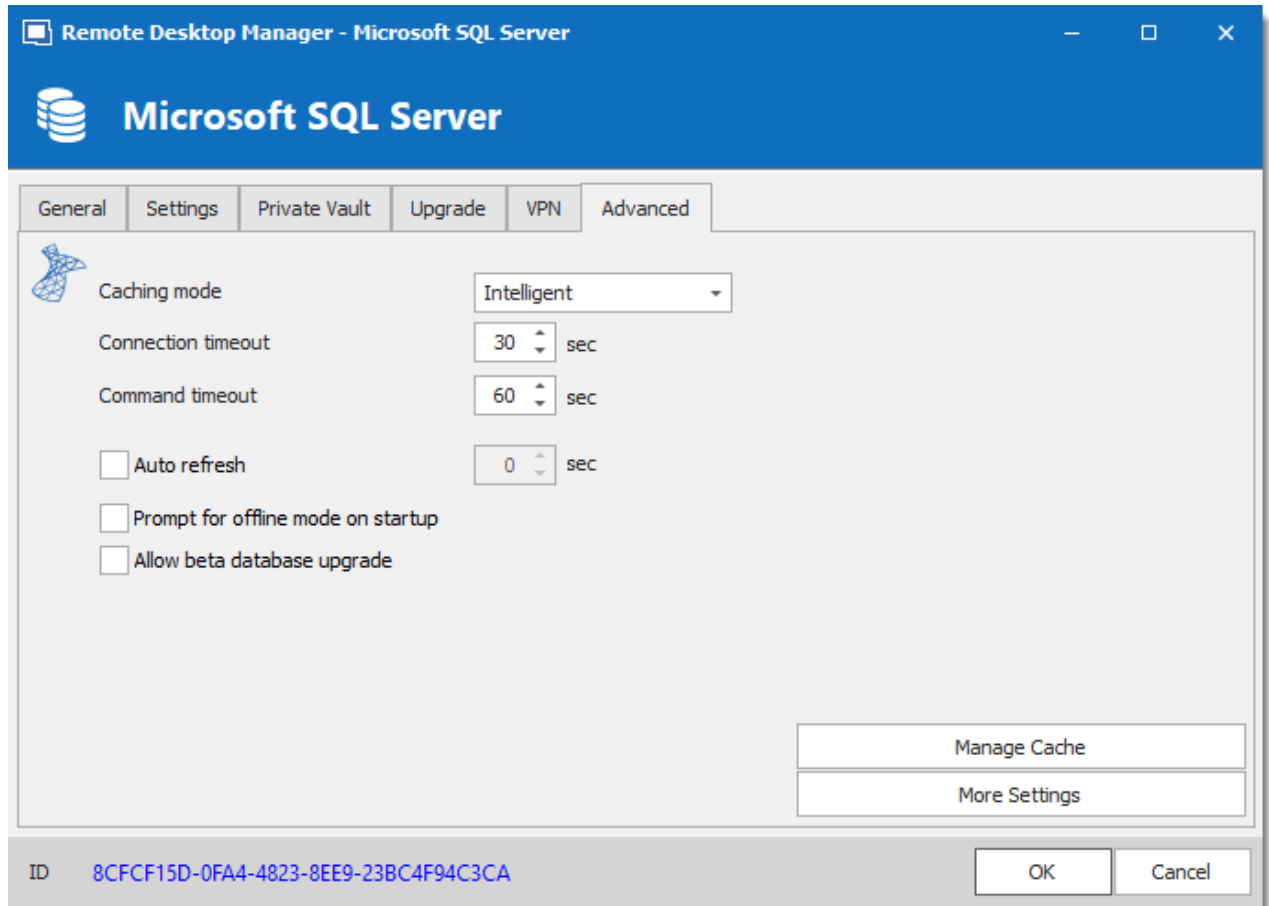
## VPN

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



*Microsoft SQL Server - VPN Tab*

## ADVANCED



Microsoft SQL Server - Advanced Tab

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



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

#### 5.4.1.5.1 Configure SQL Server

## DESCRIPTION

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



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

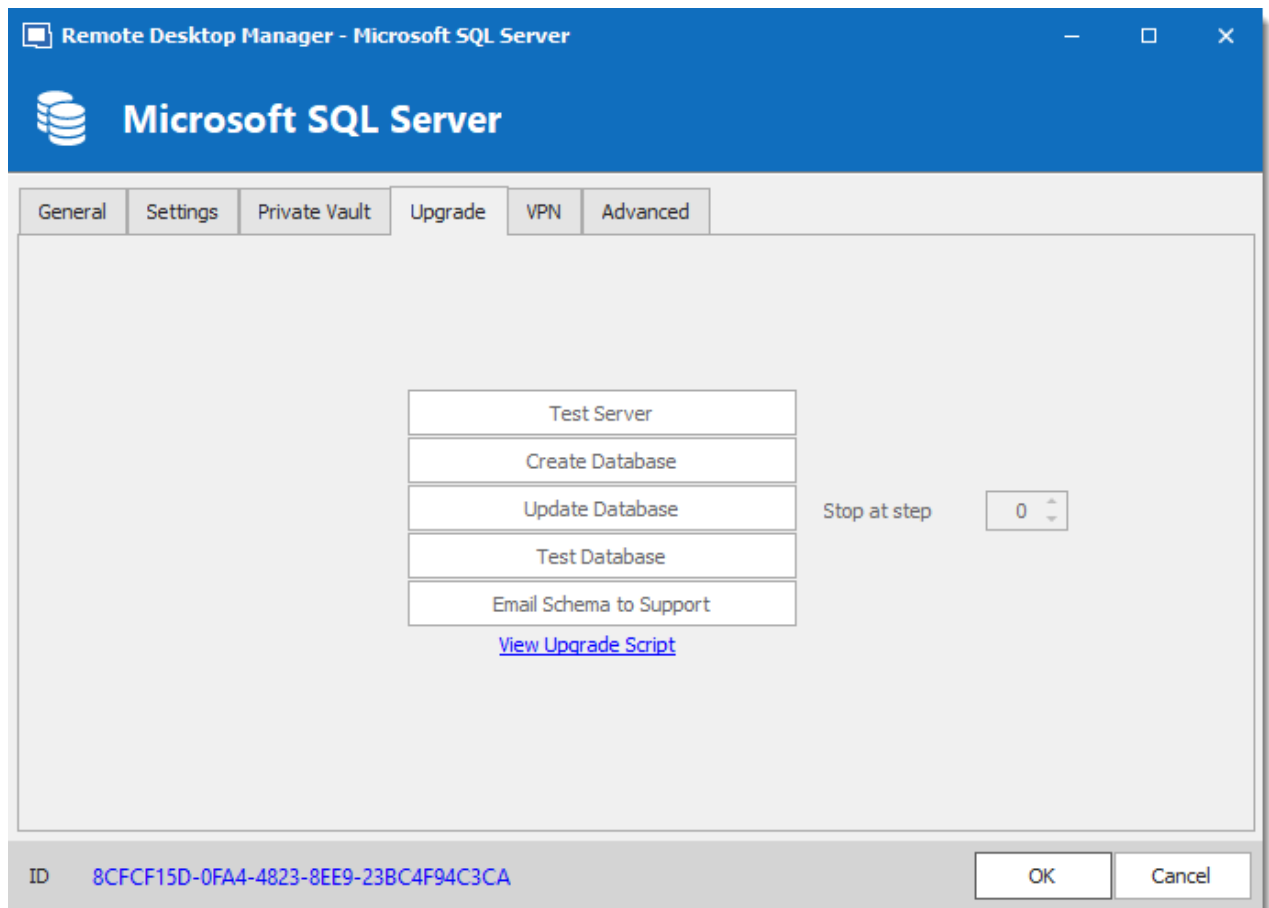


For added security, you can enable SSL Encryption to communicate with your instance of SQL Server. However, due to a framework limitation, this is not compatible with our iOS and Android versions of Remote Desktop Manager.

Please follow directions on <https://support.microsoft.com/en-us/kb/316898>

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

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

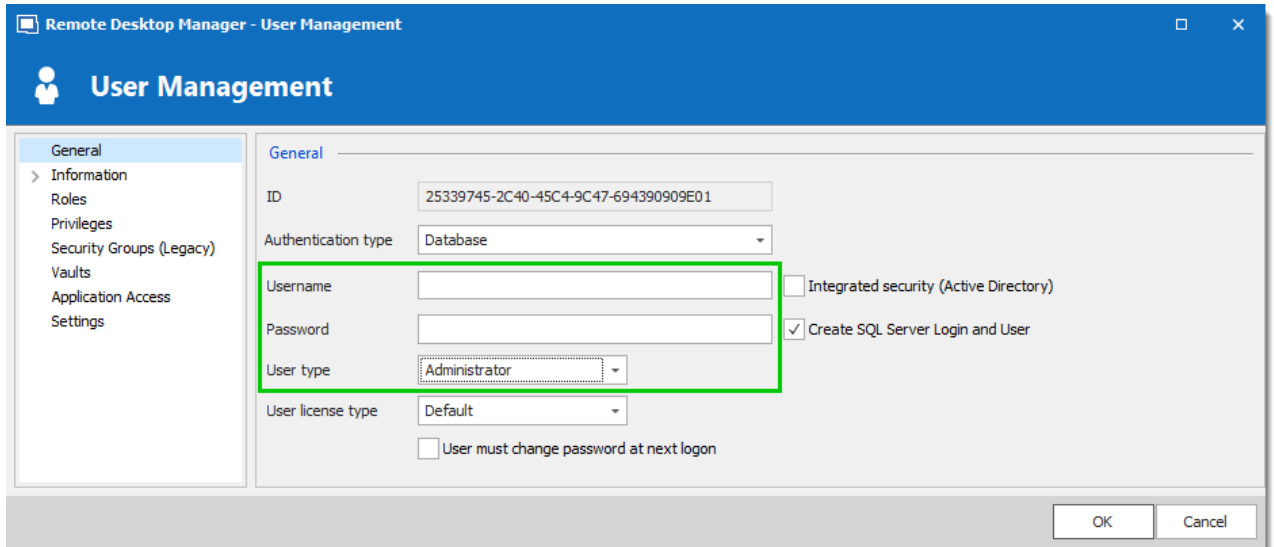


*Upgrade Tab*

4. Once the database is created, create an administrator account for the database via the [Administration - Users](#) menu.



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



Remote Desktop Manager - User Management

**User Management**

General

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

General

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

Authentication type: Database

Username:

Password:

User type: Administrator

User license type: Default

☐ Integrated security (Active Directory)

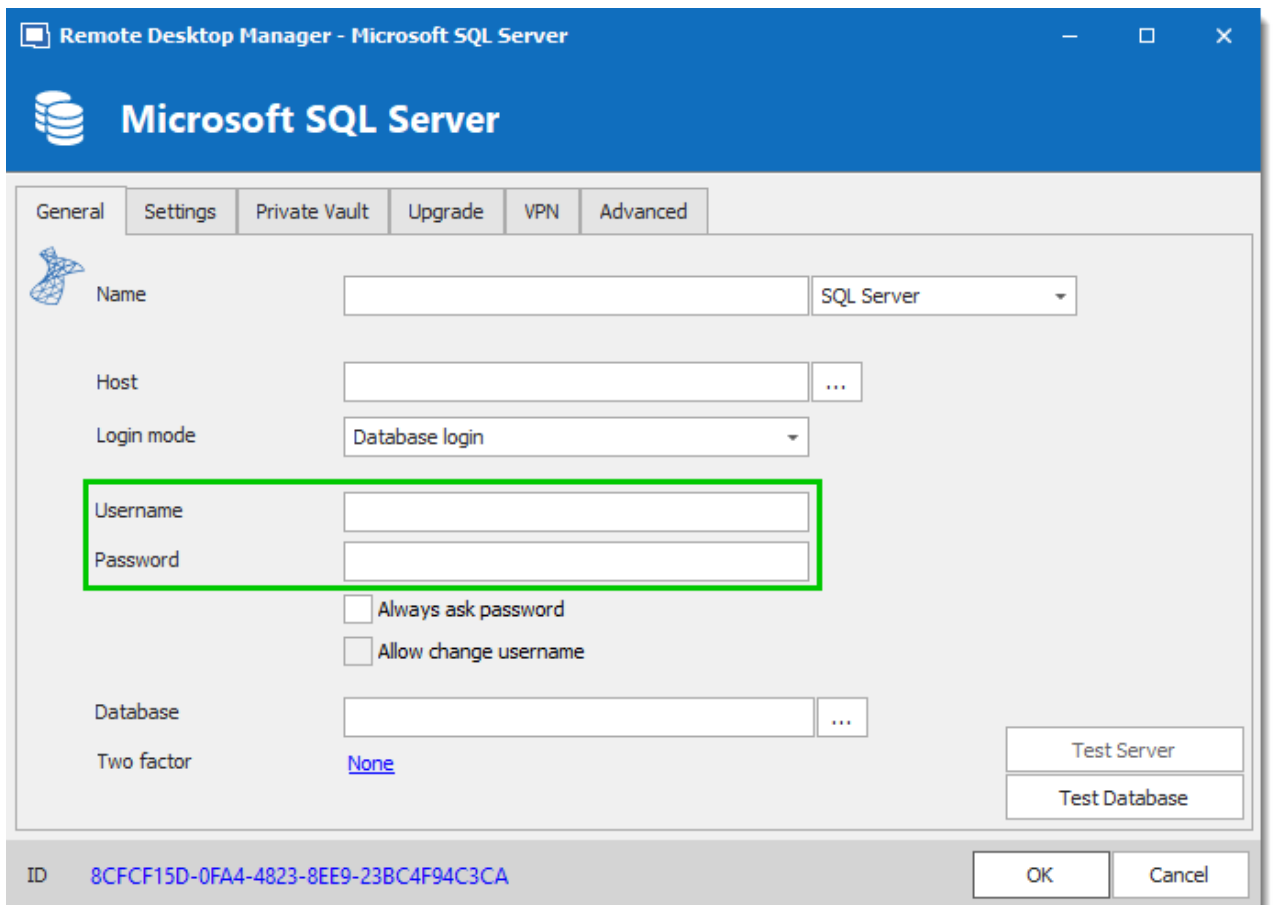
☒ Create SQL Server Login and User

☐ User must change password at next logon

OK Cancel

*Create a Remote Desktop Manager Administrator Account*

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



Remote Desktop Manager - Microsoft SQL Server

**Microsoft SQL Server**

General Settings Private Vault Upgrade VPN Advanced

Name:  SQL Server

Host:  ...

Login mode: Database login

Username:

Password:

☐ Always ask password

☐ Allow change username

Database:  ...

Two factor: [None](#)

Test Server

Test Database

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

OK Cancel

*Connection to the Database with the RDM Administrator Account*

The Microsoft SQL Server data source is now correctly configured.

#### 5.4.1.5.2 Recovery Model

## DESCRIPTION

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



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



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

#### 5.4.1.5.3 Encrypting Connections to SQL Server

## DESCRIPTION

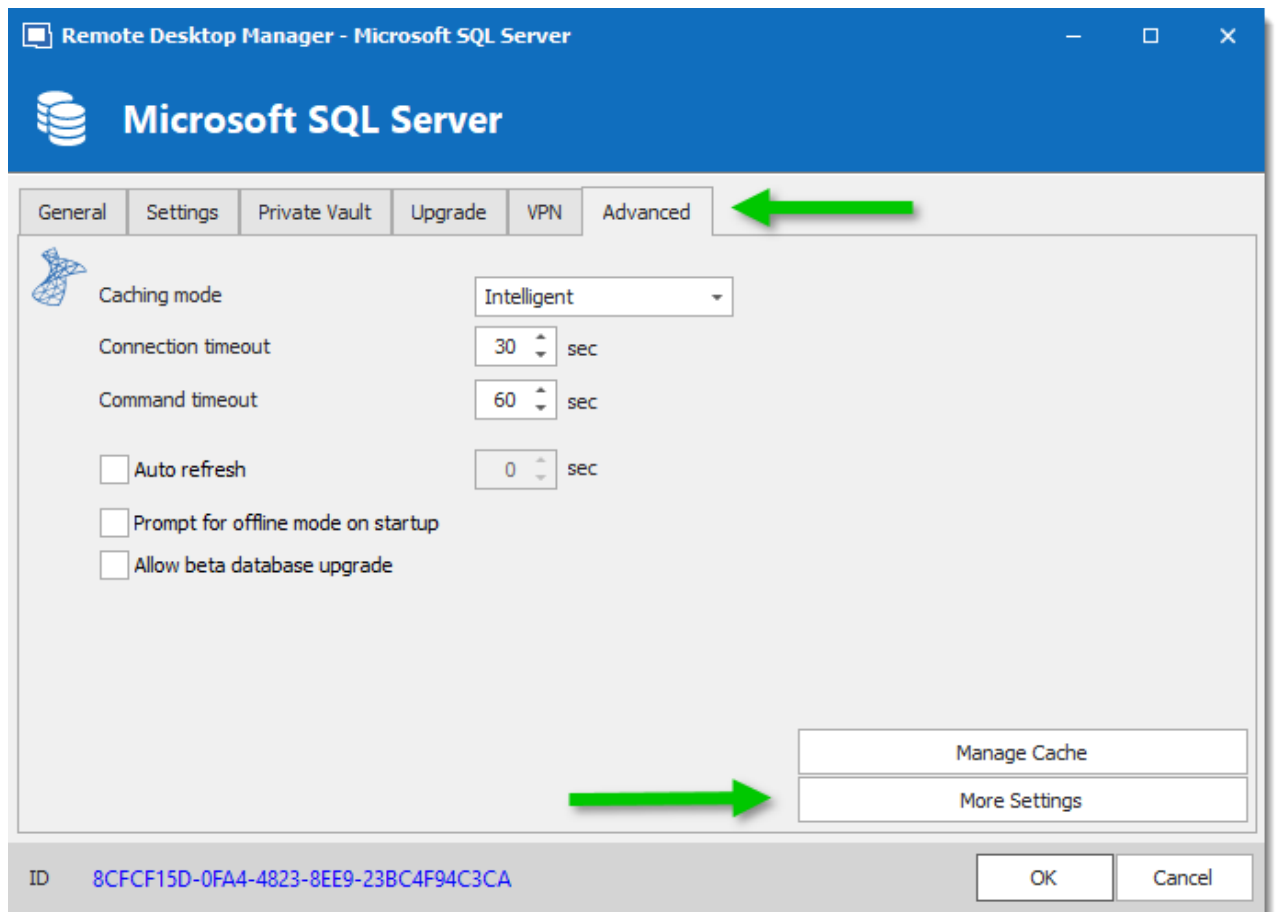
To ensure that the communication between Remote Desktop Manager and the Microsoft SQL Server database is encrypted, an extensive procedure must be followed on the Microsoft SQL Server instance.

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

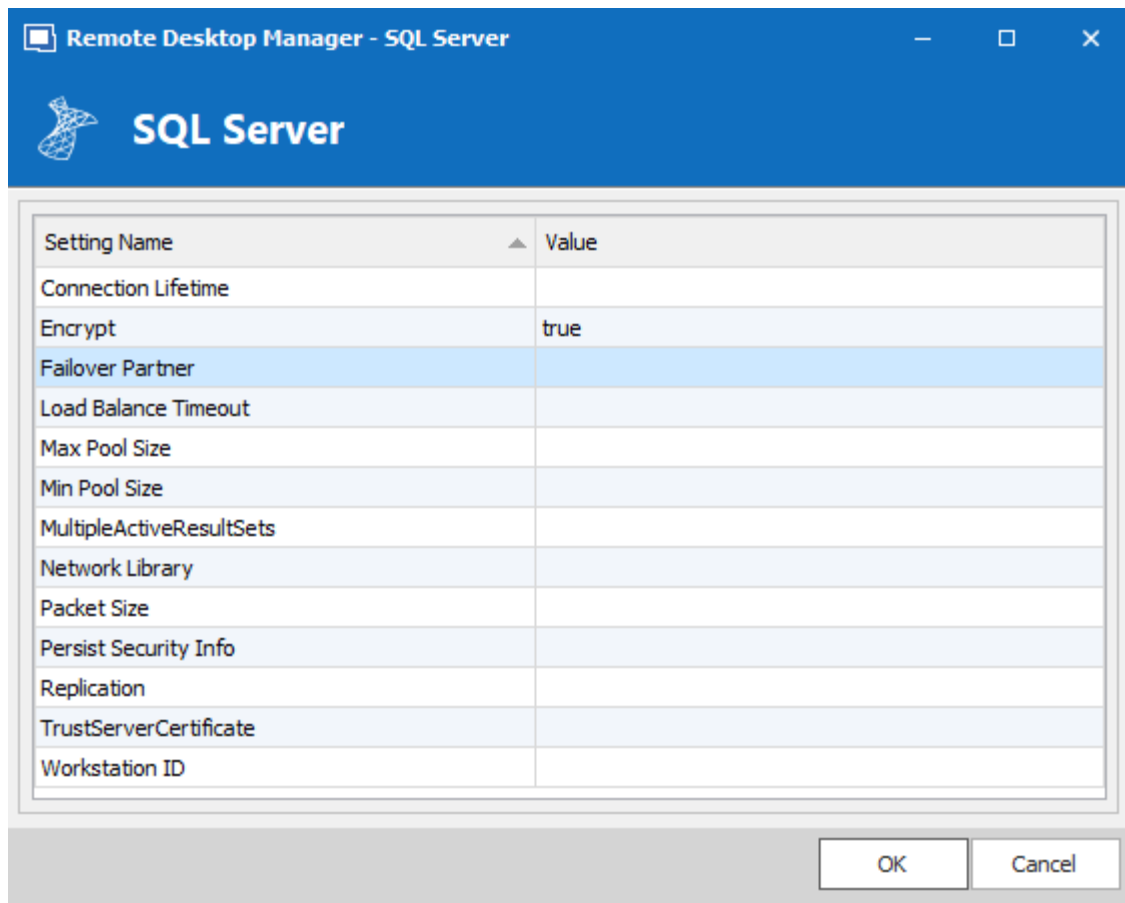
After it has been properly configured, the only modification to perform in Remote Desktop Manager is to set a property in the **More Settings** of the data source.

## PROCEDURE

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



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



#### 5.4.1.6 MySQL

### DESCRIPTION



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



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

Please follow directions in those links;

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



We recommend using MySQL version 5.5.62 for this data source.

## HIGHLIGHTS

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

## SETTINGS

### GENERAL

Remote Desktop Manager - MySQL

MySQL

General Private Vault Upgrade VPN Advanced

Name

Host  Port

☐ Integrated security (Active Directory)

Username

Password

☐ Always ask password

☐ Allow change username

Schema  ...

Two factor [None](#)

Test Host

Test Schema

ID 05424A15-C61D-48FD-9286-F06199005D06

OK Cancel

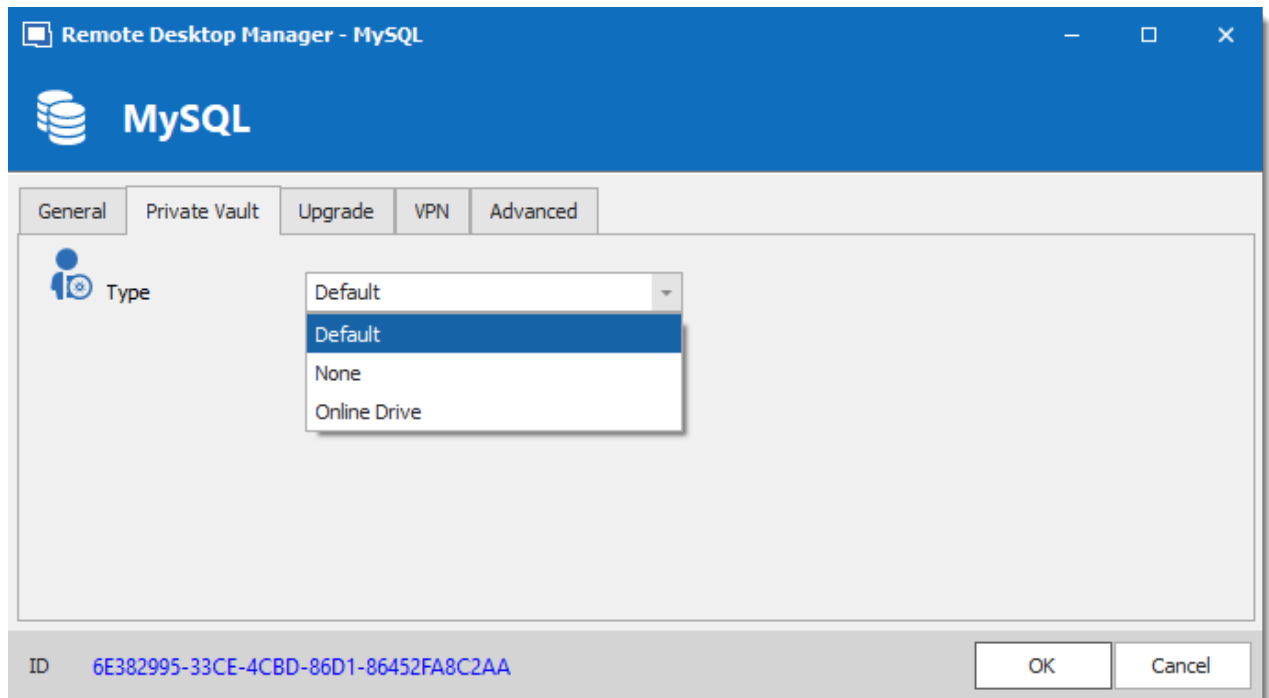
MySQL - General Tab

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



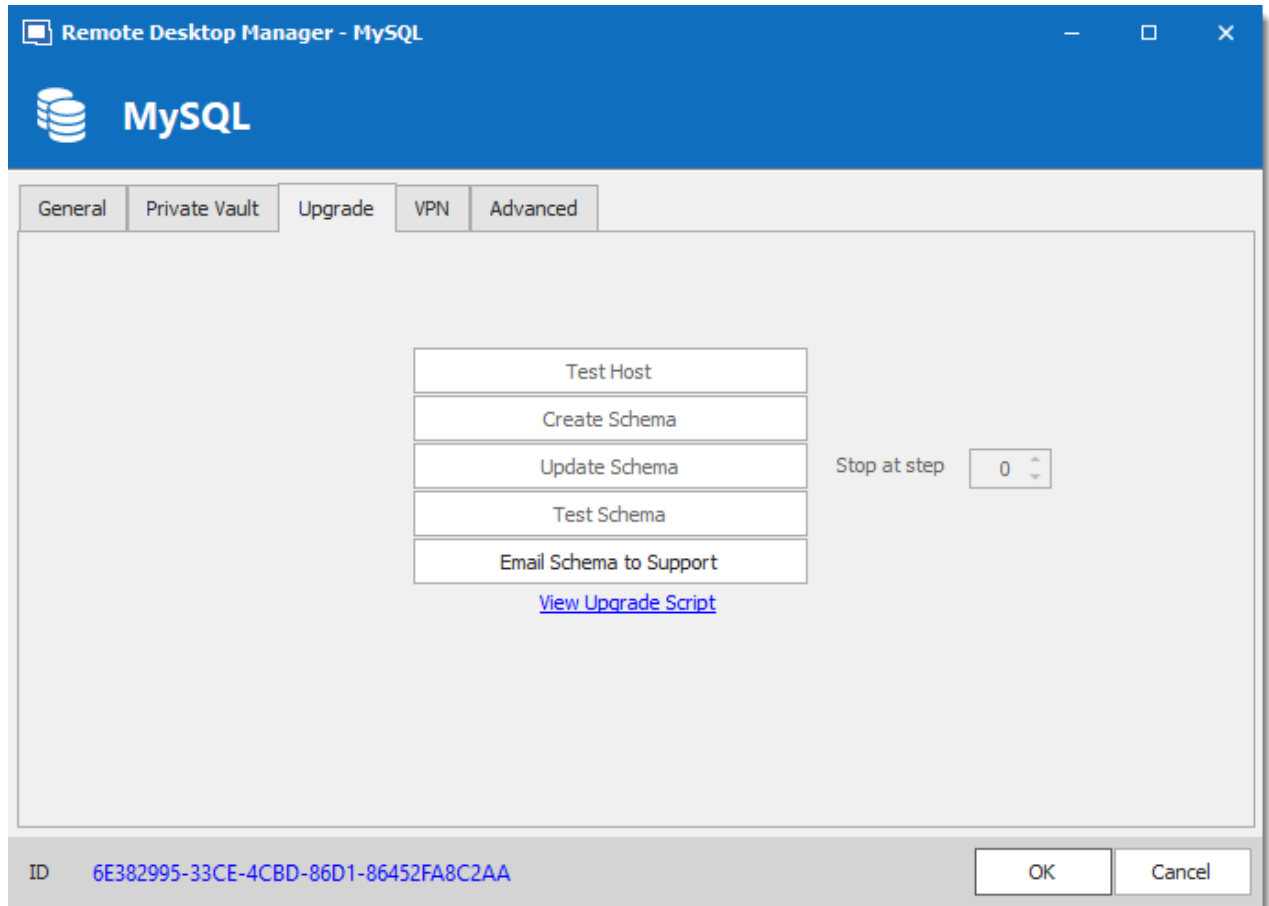
OPTION	DESCRIPTION
<b>Always ask password</b>	Prompt for the password when a user connects to the data source.
<b>Allow change username</b>	Allow the username to be edited when connecting to the data source. (Only with Always ask password enabled)
<b>Schema</b>	Name of the schema on the MySQL server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

## PRIVATE VAULT

*MySQL - Private Vault Tab*

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

## UPGRADE



MySQL - Upgrade Tab

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

OPTION	DESCRIPTION
<b>Email Schema to Support</b>	Send your schema to the Devolutions Support team.
<b>View Upgrade Script</b>	Open the upgrade script in a new window.

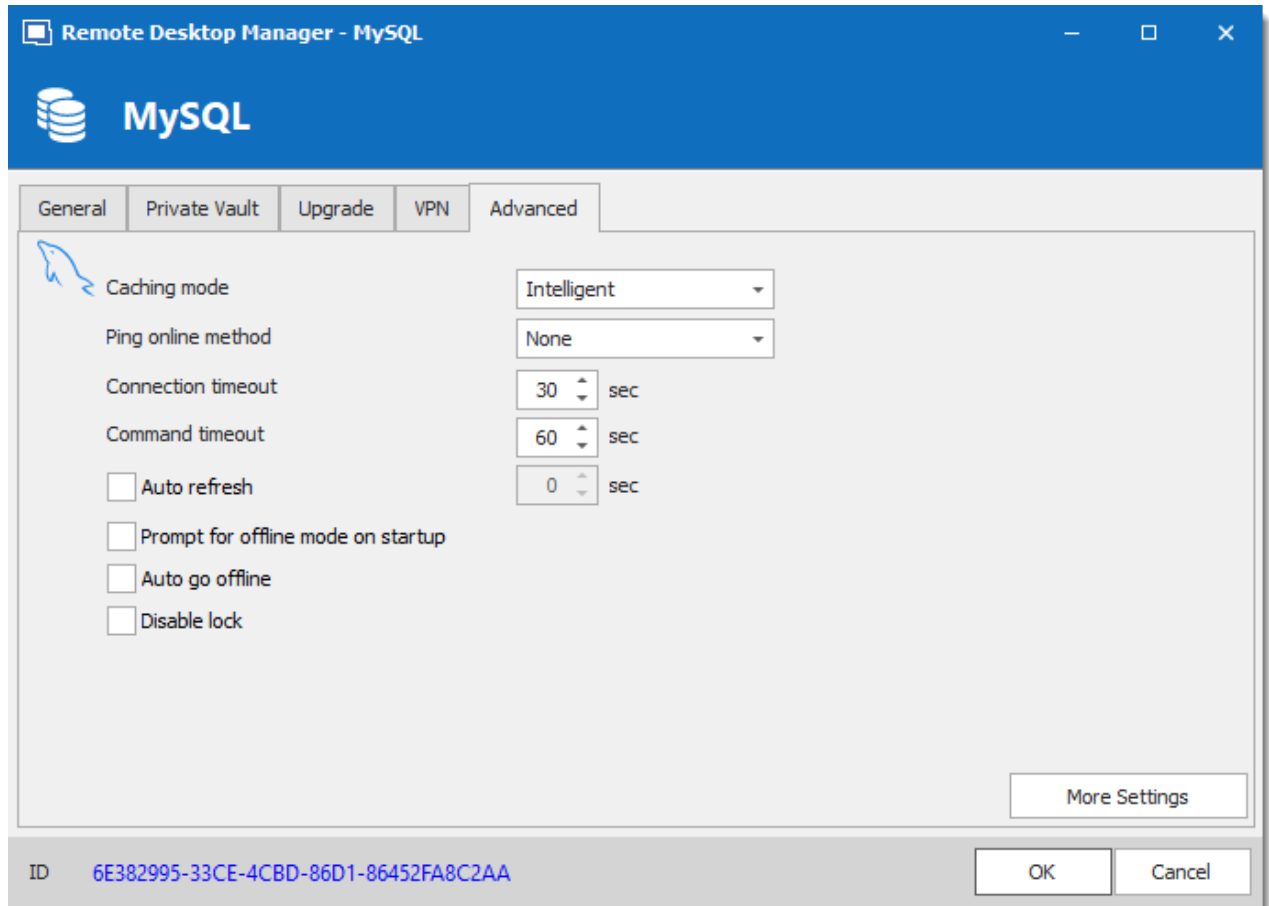
## VPN

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

The screenshot shows the 'Remote Desktop Manager - MySQL' window with the 'VPN' tab selected. The window has a blue header with the MySQL logo. Below the header are tabs for 'General', 'Private Vault', 'Upgrade', 'VPN', and 'Advanced'. The 'VPN' tab contains a 'Type' dropdown menu set to 'On first connect' with a play button icon. Below this is an 'RDM File' text box with a browse button (...). There is an unchecked checkbox for 'Override credentials'. Below this are three text boxes for 'Username', 'Domain', and 'Password'. At the bottom of the window, there is an 'ID' field with the value '6E382995-33CE-4CBD-86D1-86452FA8C2AA' and 'OK' and 'Cancel' buttons.

MySQL - VPN Tab

## ADVANCED



MySQL - Advanced Tab

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

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

## TROUBLESHOOTING

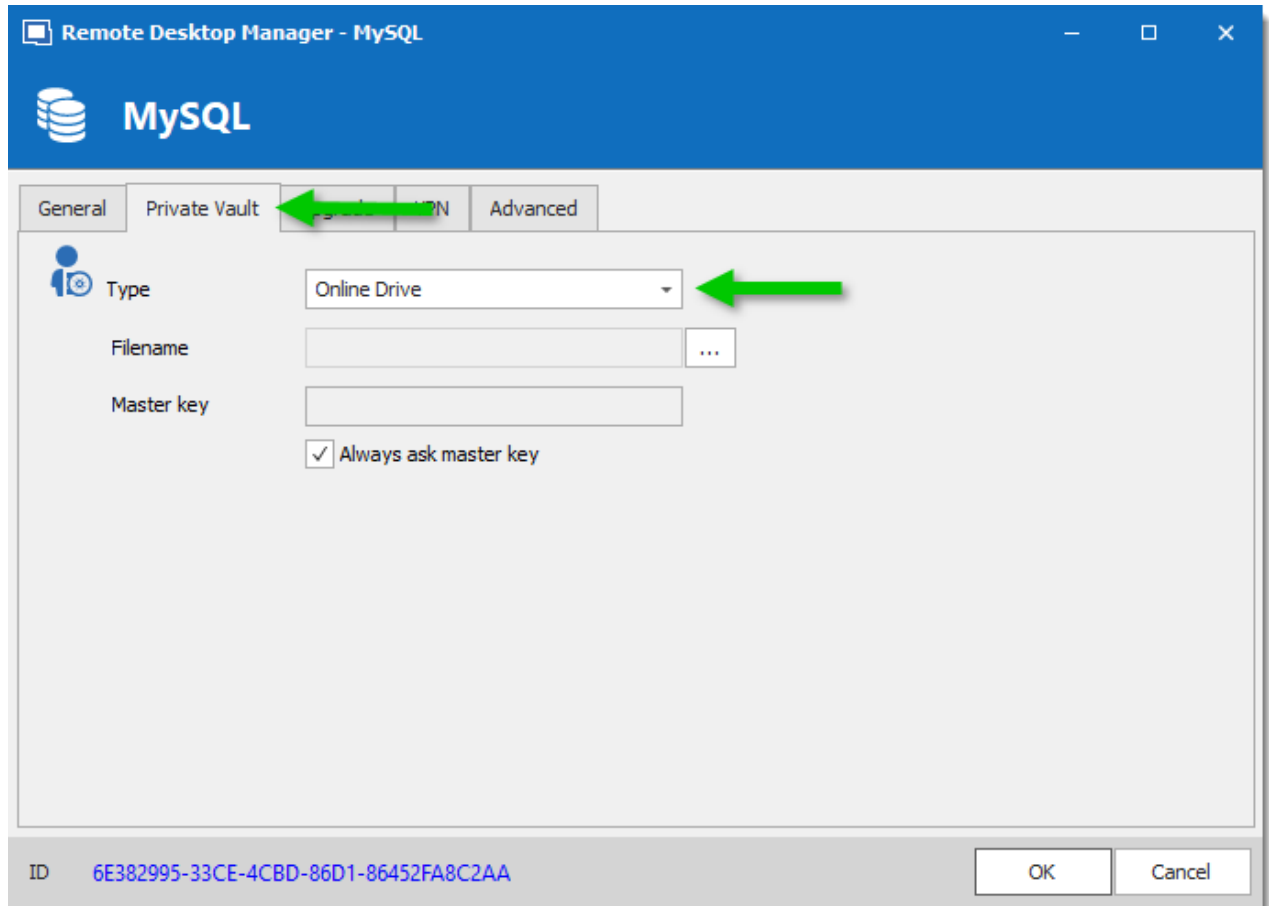
Consult MySQL troubleshooting for more information.

### 5.4.1.7 Private Vault

## DESCRIPTION

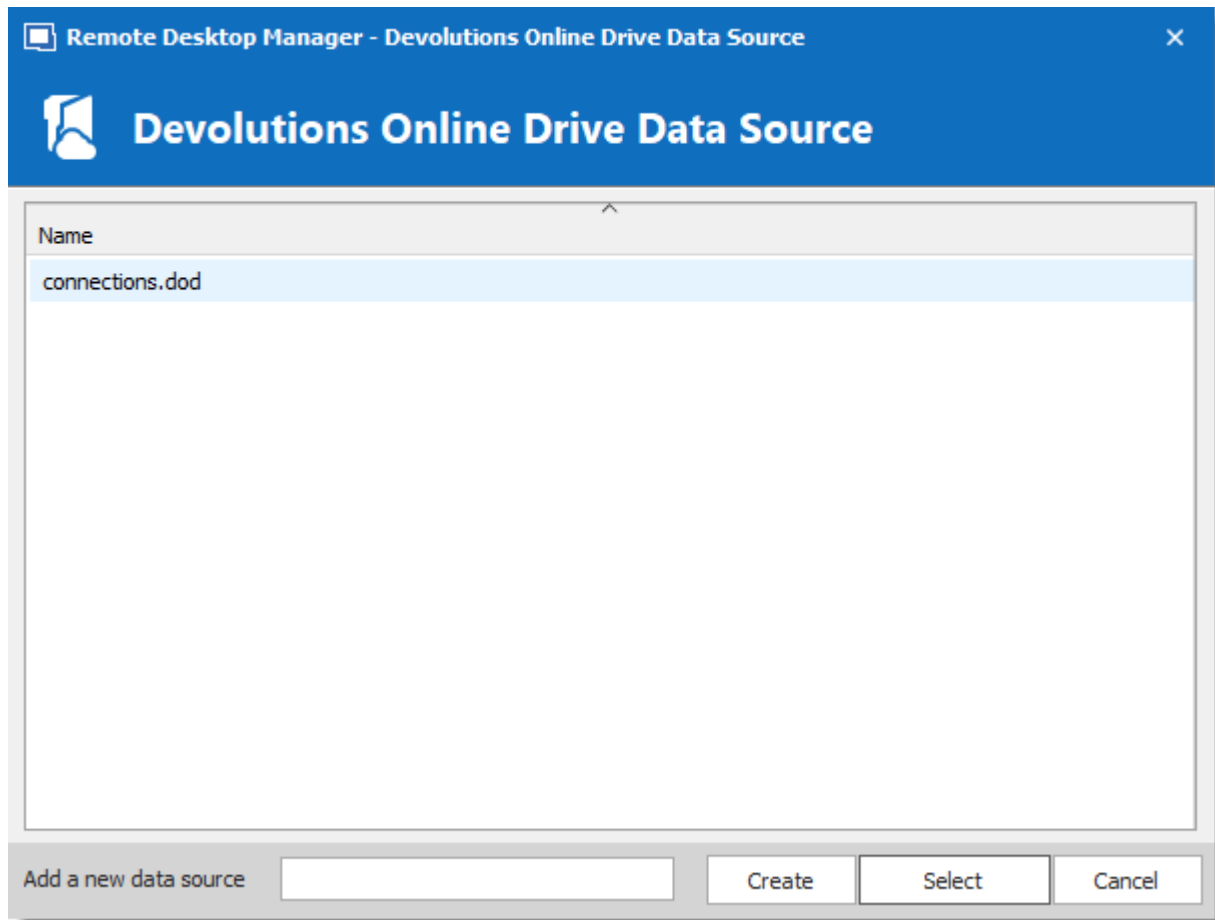
The **Private Vault** allows you to connect a personal Vault stored in a **Devolutions Online Drive** file directly to your **Advanced Data Source**, thus allowing you to store information that only you can have access to. For more information about the Private Vault please follow this [link](#).

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



*Devolutions Online Database Data Source*

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

*Devolutions Online Drive Data Source*

## 5.4.2 DropBox

### DESCRIPTION



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



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



## HIGHLIGHTS

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



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

## SETTINGS

### GENERAL

The screenshot shows the 'Remote Desktop Manager - Dropbox' window with the 'General' tab selected. The window has a blue header with the Dropbox logo and title. Below the header are three tabs: 'General', 'VPN', and 'Advanced'. The 'General' tab contains the following fields and options:

- Name:** A text field containing 'Dropbox'.
- Mode:** A dropdown menu set to 'Local'.
- Local path:** An empty text field.
- Full local path:** A text field containing 'connections.xml'.
- Master key:** An empty text field.
- Always ask master key:** A checked checkbox.
- Dropbox directory:** An empty text field.
- Filename:** A text field containing 'connections.xml'.
- Compress database file:** An unchecked checkbox.

At the bottom of the window, there is an 'ID' field with the value 'AAAC170C-C03C-4077-BC4F-28A717C3CB4C' and two buttons: 'OK' and 'Cancel'.

*Dropbox - General Tab*

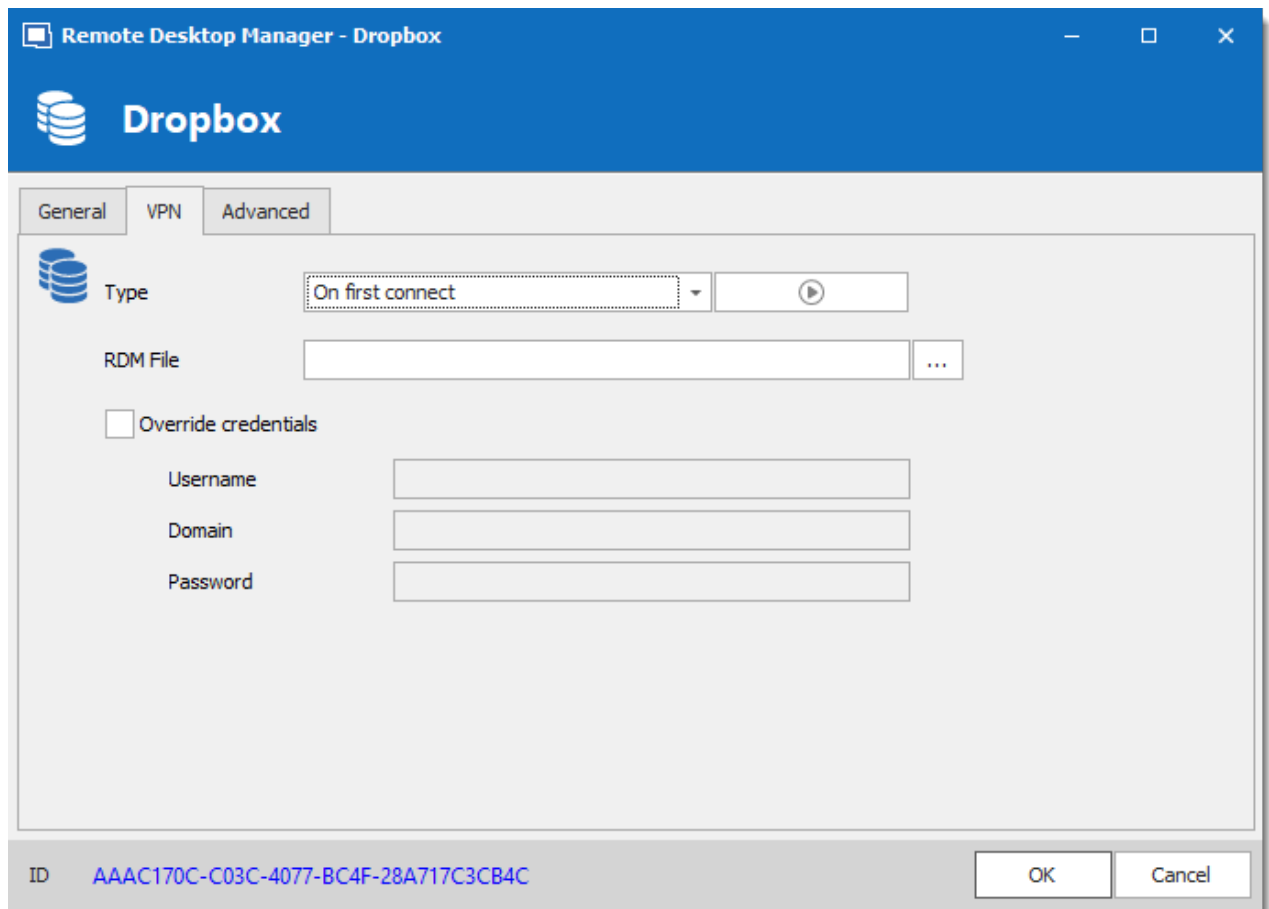
Remote Desktop Manager supports the 2-Factor Authentication of Dropbox. When the button **Validate with Dropbox** is pressed and the 2-Factor Authentication is enabled in Dropbox, a window prompt will open and ask for the Dropbox account password, then a second prompt will open for the security code.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

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

OPTION	DESCRIPTION
	<ul style="list-style-type: none"> <li>• <b>Local</b></li> </ul>
<b>Local path (Local Mode)</b>	Contains the local path where the Dropbox files are accessible.
<b>Email (Account Mode)</b>	Contains the email address associated with the Dropbox account.
<b>Validate with Dropbox (Account Mode)</b>	Button to validate the email address with the Dropbox account.
<b>Master key</b>	Add an additional layer of security to your data source by using master key.
<b>Always ask master key</b>	Connecting to the data source will always prompt for the master key.
<b>Dropbox directory</b>	Indicate the folder in Dropbox. It should not contains any drive since it's stored online. Leave it empty to use the default Dropbox root.
<b>Filename</b>	Indicate the filename used to store the data on the data source.
<b>Compress database file</b>	Activate this option if you wish to compress your database file.

## VPN

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



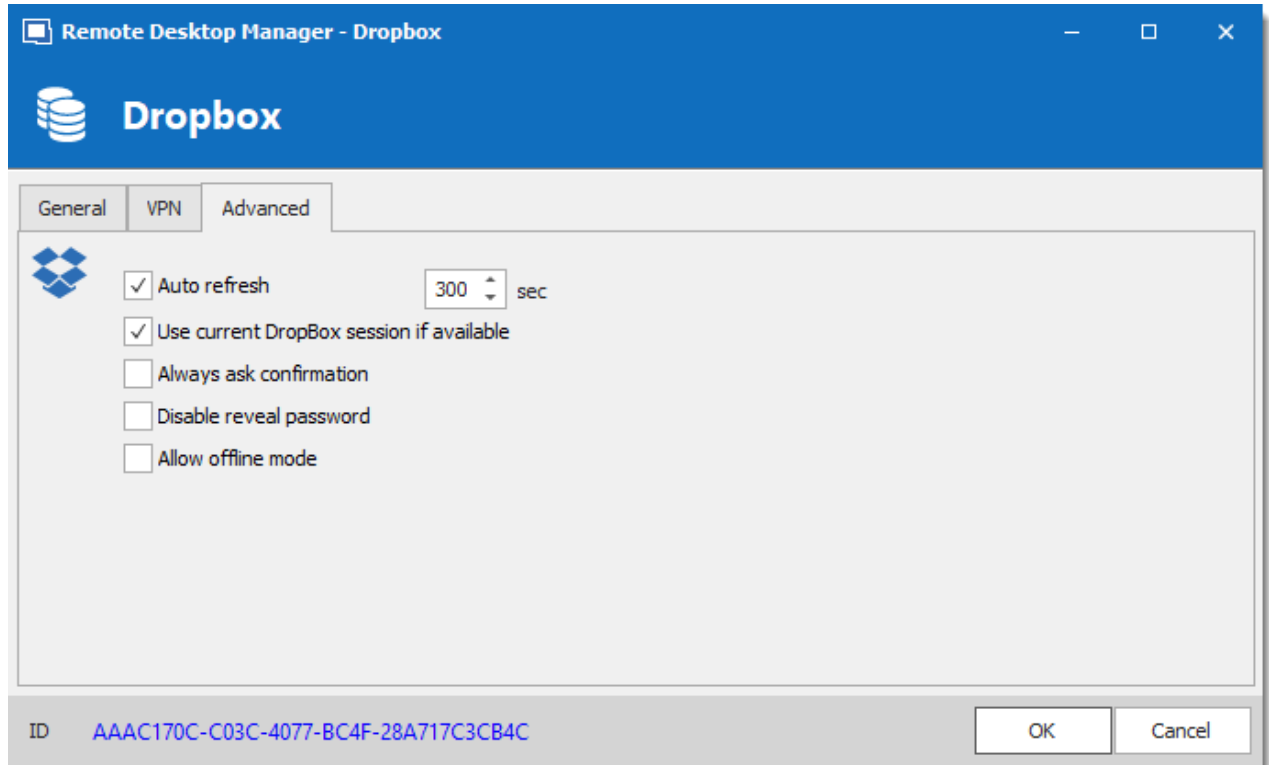
The screenshot shows a window titled "Remote Desktop Manager - Dropbox". The window has a blue header bar with the Dropbox logo and name. Below the header, there are three tabs: "General", "VPN", and "Advanced". The "VPN" tab is selected. The main area of the window contains the following fields and controls:

- Type:** A dropdown menu set to "On first connect" with a play button icon to its right.
- RDM File:** A text input field with a browse button (three dots) 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 window, there is a status bar with the text "ID AAAC170C-C03C-4077-BC4F-28A717C3CB4C" and two buttons: "OK" and "Cancel".

*Dropbox - VPN Tab*

## ADVANCED



Dropbox - Advanced Tab

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

### 5.4.3 Google Drive

#### DESCRIPTION



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

#### GENERAL

The screenshot shows a window titled 'Remote Desktop Manager - Google Drive'. The window has a blue header bar with the Google Drive logo and the text 'Google Drive'. Below the header, there are two tabs: 'General' (selected) and 'VPN'. The 'General' tab contains the following fields and options:

- Name:** A text input field.
- Email:** A text input field.
- Password:** A text input field.
- Always ask password:** A checkbox, currently unchecked.
- Account status:** A label followed by the text 'The account is not validated yet.' and a 'Validate Google Drive' button.
- Master key:** A text input field.
- Always ask master key:** A checkbox, currently checked.
- Filename:** A text input field.

At the bottom of the window, there is a status bar with the ID 'B90C0576-E259-4C83-B929-6381577FC0A2' and 'OK' and 'Cancel' buttons.

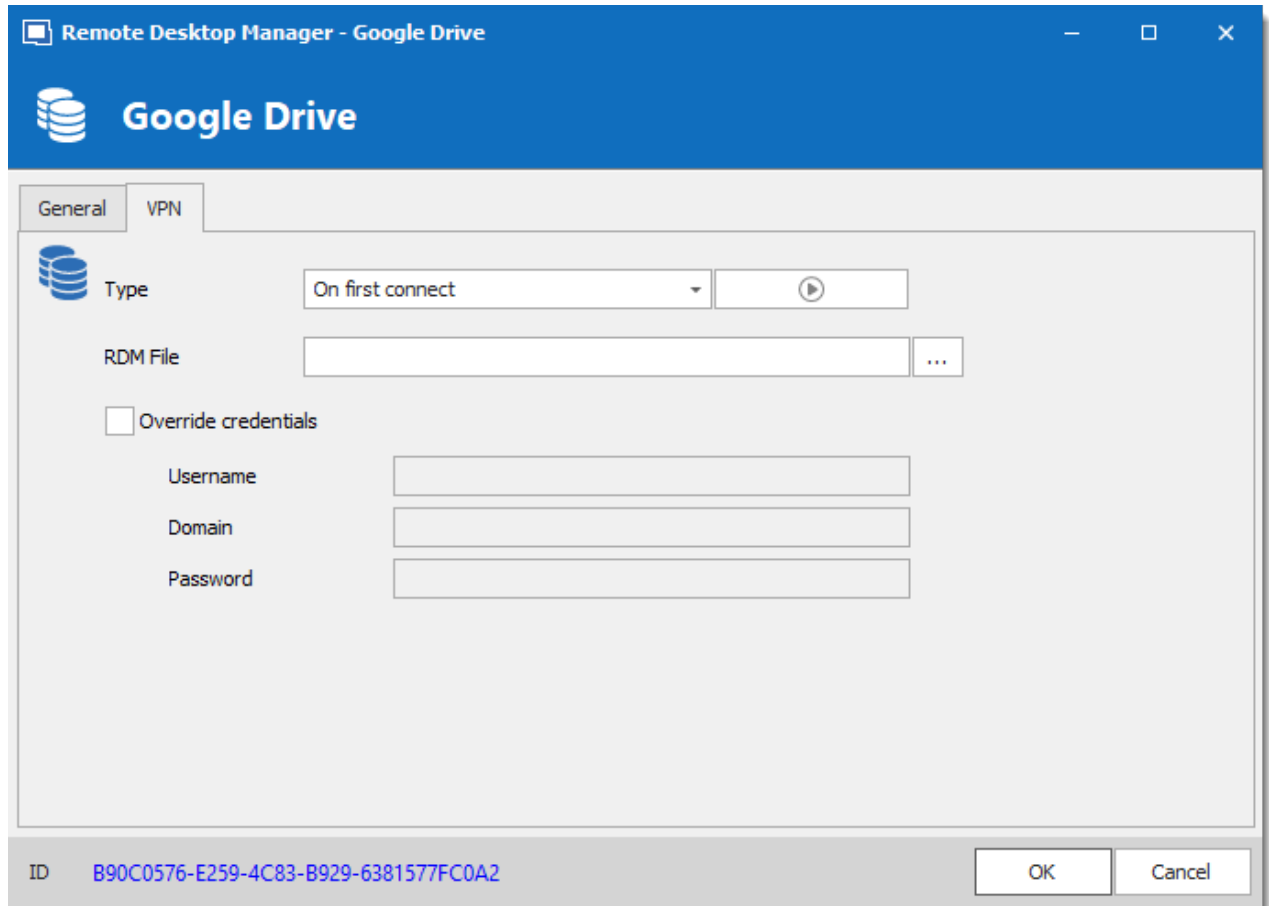
Google Drive - General Tab

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

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

## VPN

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



Google Drive - VPN Tab

## 5.4.4 Devolutions Online Drive

### DESCRIPTION

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

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

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



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





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

## SETTINGS

### GENERAL

The screenshot shows the 'Remote Desktop Manager - Devolutions Online Drive' window. The title bar is blue with the Devolutions logo and the text 'Devolutions Online Drive'. Below the title bar is a tabbed interface with 'General', 'Backup', 'VPN', and 'Advanced' tabs. The 'General' tab is active. It contains a 'Name' field with the value 'Devolutions Online Drive', a 'Create a Free Account' link, an 'Always ask password' checkbox, a 'Test Connection' button, a 'Filename' field with the value 'connections.dod', a 'Master key' field, and an 'Always ask master key' checkbox which is checked. At the bottom, there is an 'ID' field with the value 'BF0B90F2-FC01-451C-8C3E-E307D3E352C4', and 'OK' and 'Cancel' buttons.

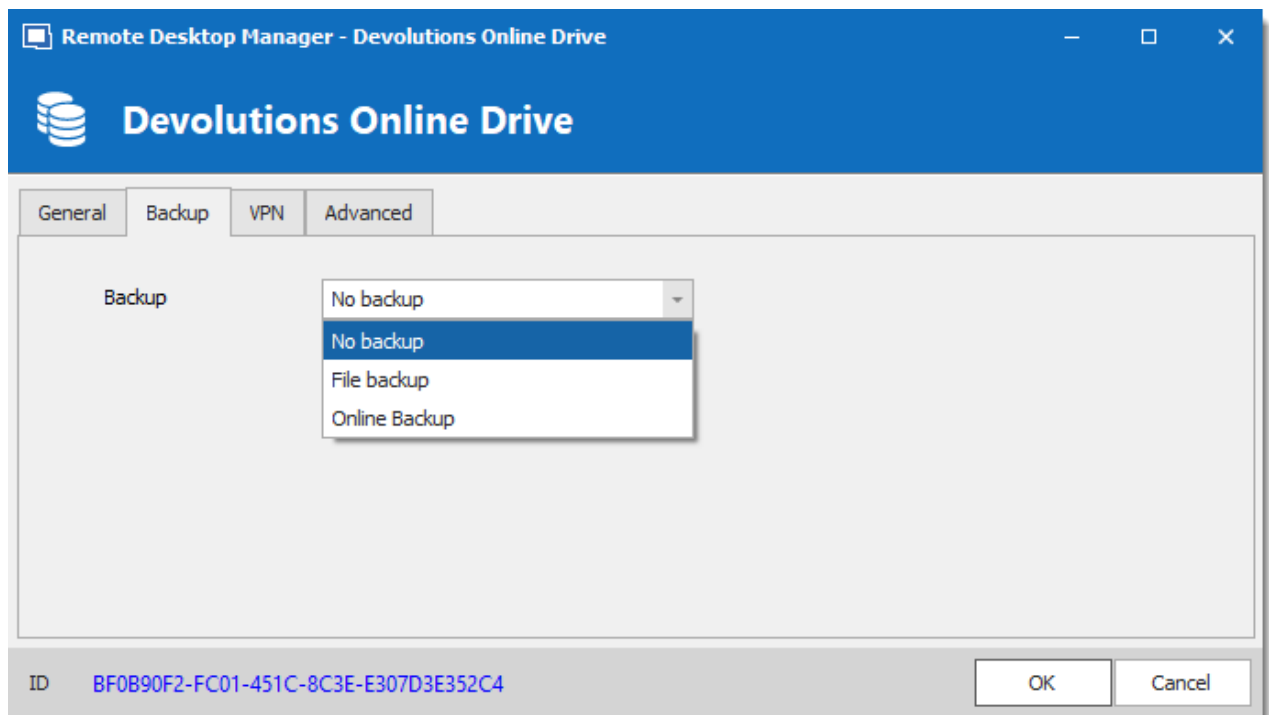
*Devolutions Online Drive - General Tab*

OPTION	DESCRIPTION
<b>Name</b>	Enter the name of the data source.
<b>Create a free account</b>	Create a new Devolutions Account.

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

## BACKUP

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



*Devolutions Online Drive - Backup Tab*

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

## VPN

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

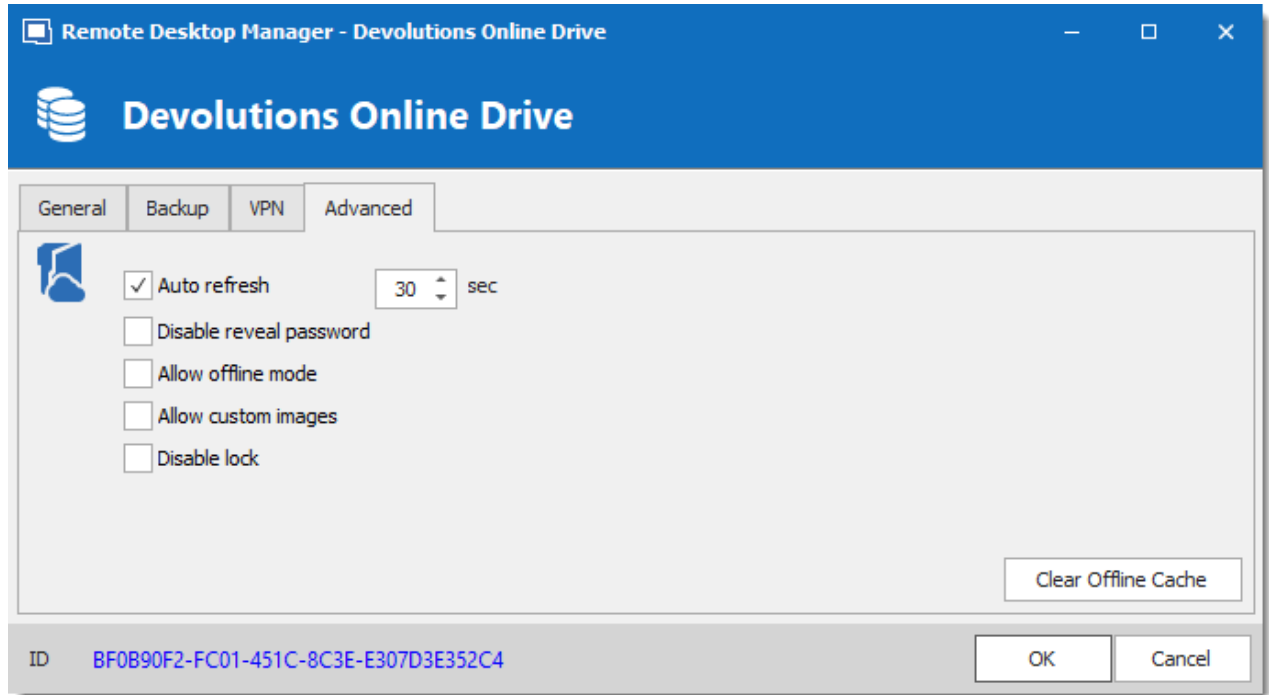
The screenshot shows a window titled "Remote Desktop Manager - Devolutions Online Drive". The window has a blue header bar with the Devolutions logo and the title "Devolutions Online Drive". Below the header, there are four tabs: "General", "Backup", "VPN", and "Advanced". The "VPN" tab is currently selected. The main area of the window contains the following fields and controls:

- Type:** A dropdown menu set to "On first connect" with a play button icon to its right.
- RDM File:** A text input field with a browse button (three dots) 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 window, there is a status bar showing the ID "BF0B90F2-FC01-451C-8C3E-E307D3E352C4" and two buttons: "OK" and "Cancel".

*Devolutions Online Drive - VPN Tab*

## ADVANCED



*Devolutions Online Drive - Advanced Tab*

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

## 5.4.5 SQLite

### DESCRIPTION



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

### HIGHLIGHTS

- Full connection log and attachments support
- The [Online Backup Service](#) is available for this data source



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



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

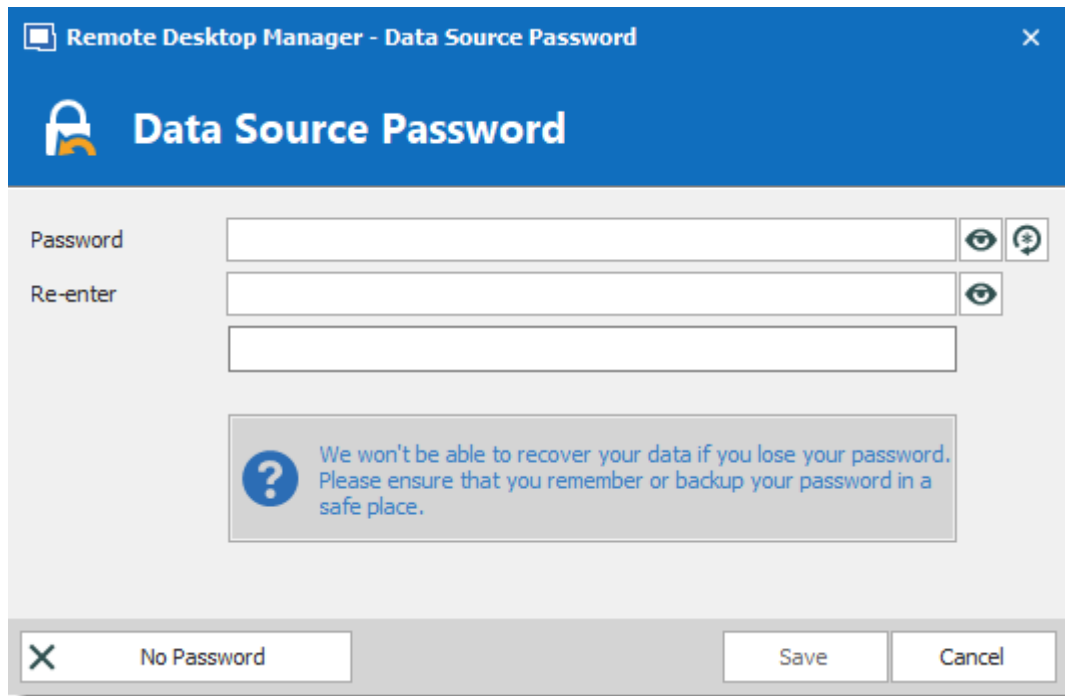


SQLite supports an unlimited number of simultaneous readers, but will only allow one writer at any instant in time. For this reason Remote Desktop Manager does not support sharing a SQLite data source between several users by storing it on a network drive. If you want to share your data and work in a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

### PASSWORD MANAGEMENT

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

Change or clear the password of a SQLite data source.



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

*Manage password dialog*

## SETTINGS

### GENERAL

Remote Desktop Manager - SQLite

SQLite

General Backup VPN Advanced

Name

Database  ...

Password

☐ Always ask password

Two factor [None](#)

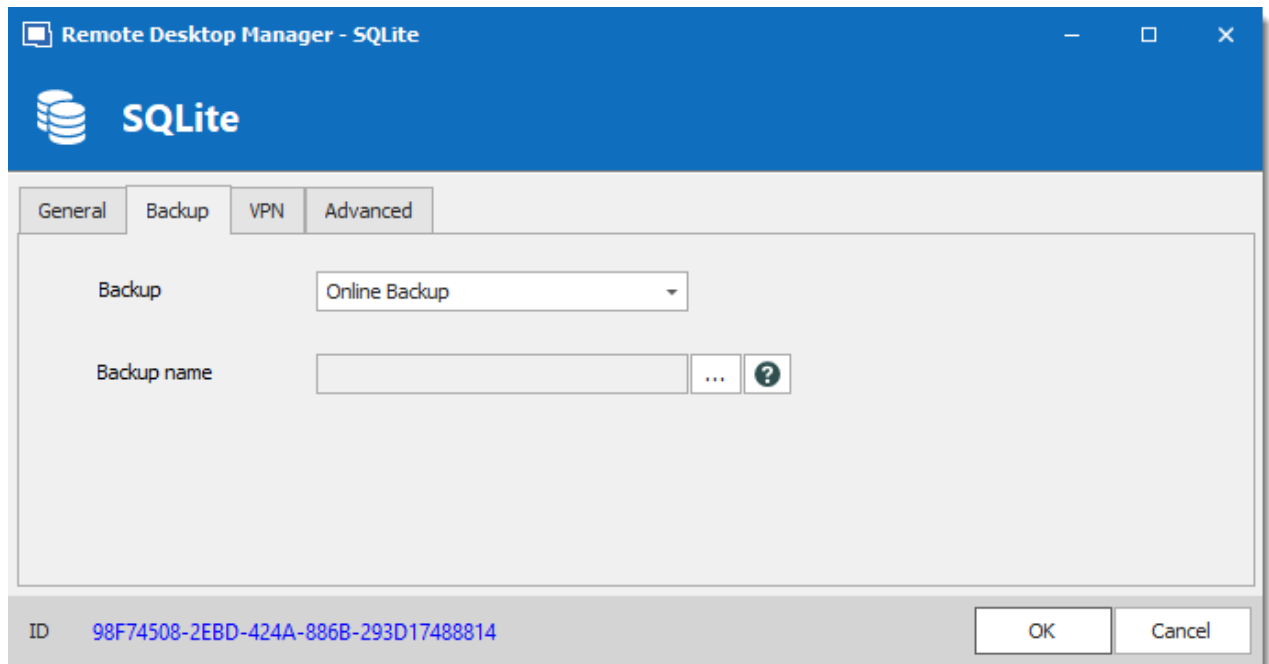
ID [E245E962-2D81-4A36-8359-0A9BB552FAAB](#)

SQLite - General Tab

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



## BACKUP

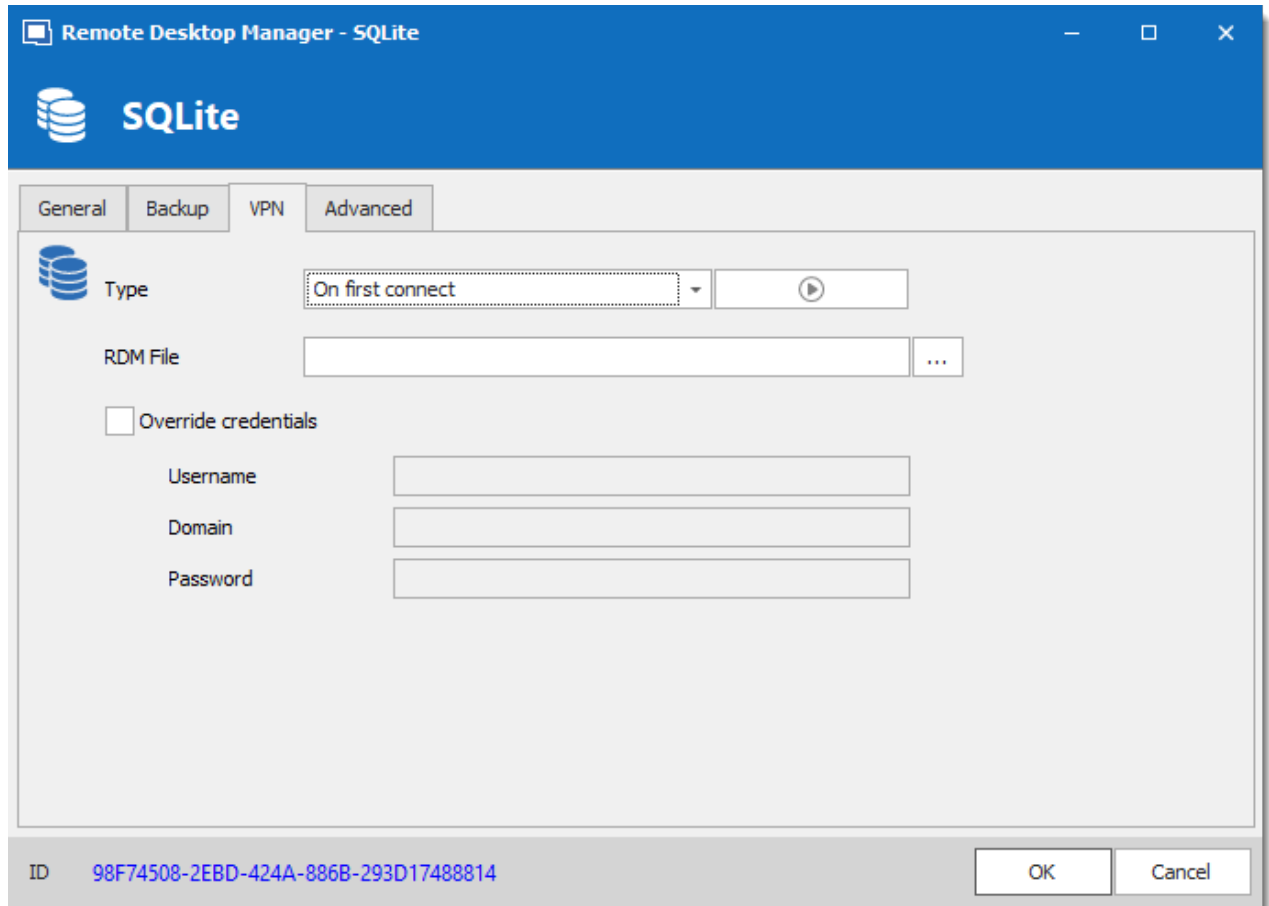


SQLite - Backup Tab

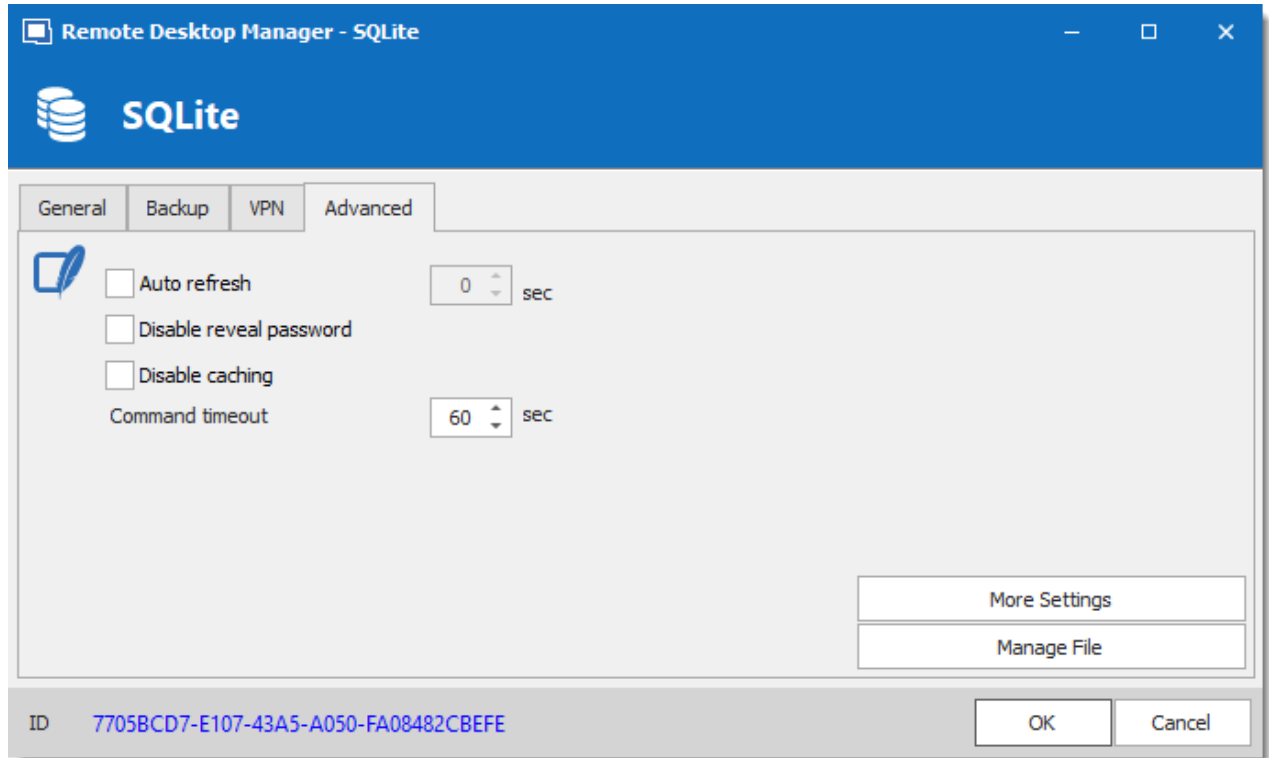
OPTION	DESCRIPTION
<b>Backup</b>	<p>Select between:</p> <ul style="list-style-type: none"><li>• <b>None:</b> No backup of your data source will be created.</li><li>• <b>File backup:</b> Your backup will be saved to a chosen file but will not automatically do backup every 30 seconds.</li><li>• <b>Online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

## VPN

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

*SQLite - VPN Tab*

## ADVANCED



SQLite - Advanced Tab

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

## 5.4.6 WebDAV

### DESCRIPTION



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

### SETTINGS

#### GENERAL

The screenshot shows the 'Remote Desktop Manager - WebDav' dialog box with the 'General' tab selected. The dialog has a blue header bar with the 'WebDav' logo and title. Below the header, there are three tabs: 'General', 'VPN', and 'Advanced'. The 'General' tab contains the following fields and options:

- Name:** A text input field.
- Host:** A text input field.
- Port:** A spinner box set to 80.
- Use SSL:** An unchecked checkbox.
- Username:** A text input field.
- Password:** A text input field.
- Always ask password:** An unchecked checkbox.
- Master key:** A text input field.
- Always ask master key:** A checked checkbox.
- Filename:** A text input field.
- Read-only:** An unchecked checkbox.

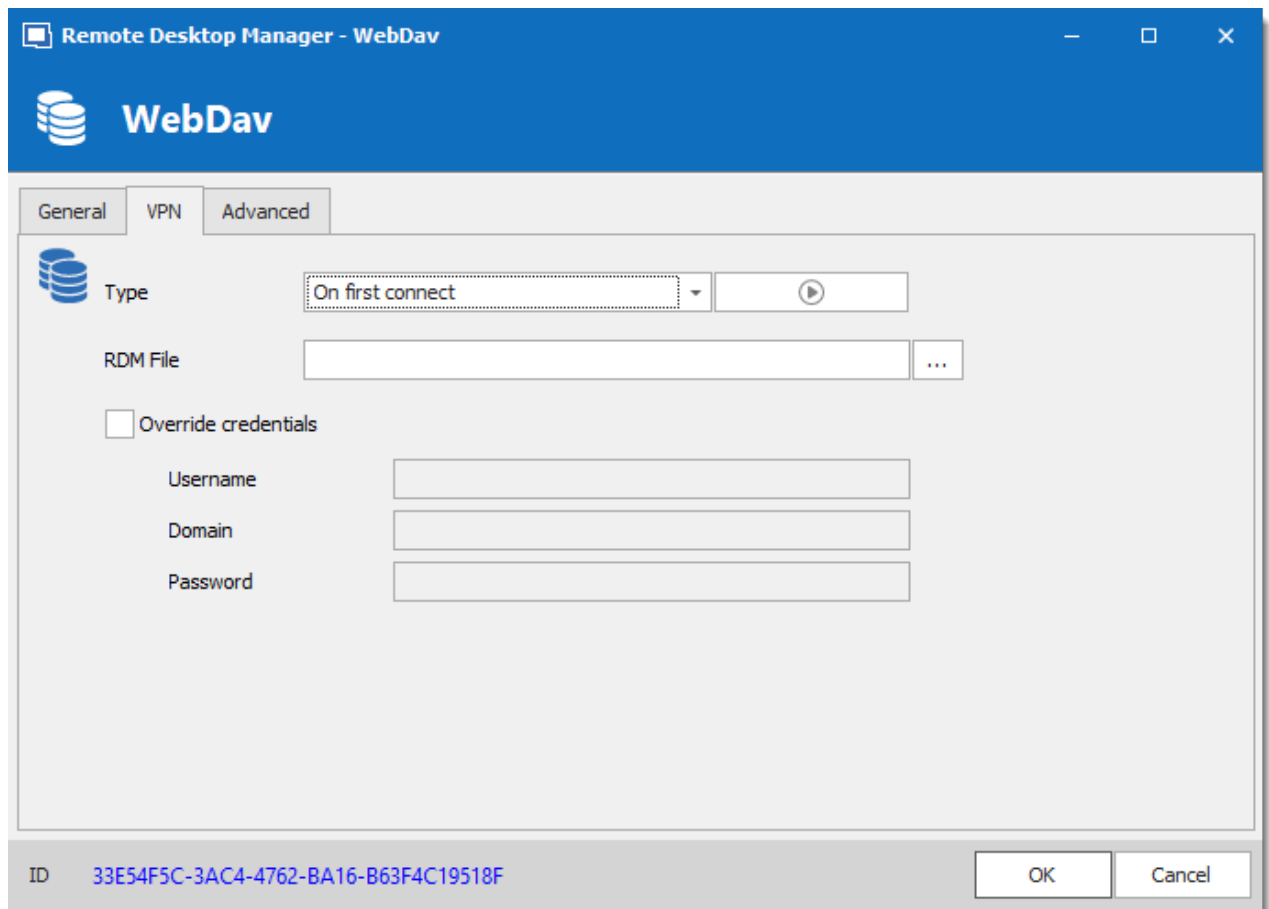
At the bottom of the dialog, there is an 'ID' field with the value '33E54F5C-3AC4-4762-BA16-B63F4C19518F' and two buttons: 'OK' and 'Cancel'.

WebDAV - General Tab

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

## VPN

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



The screenshot shows the 'Remote Desktop Manager - WebDav' window. The title bar is blue with the application name and standard window controls. Below the title bar is a blue header with the 'WebDav' logo and name. The main area has three tabs: 'General', 'VPN', and 'Advanced'. The 'VPN' tab is selected. Inside the 'VPN' tab, there is a 'Type' dropdown menu set to 'On first connect' with a play button icon. Below this is an 'RDM File' text field with a browse button ('...'). There is an unchecked checkbox for 'Override credentials'. Below this are three text fields for 'Username', 'Domain', and 'Password'. At the bottom of the window, there is a grey bar containing an 'ID' field with the value '33E54F5C-3AC4-4762-BA16-B63F4C19518F' and 'OK' and 'Cancel' buttons.

Remote Desktop Manager - WebDav

WebDav

General VPN Advanced

Type On first connect

RDM File

☐ Override credentials

Username

Domain

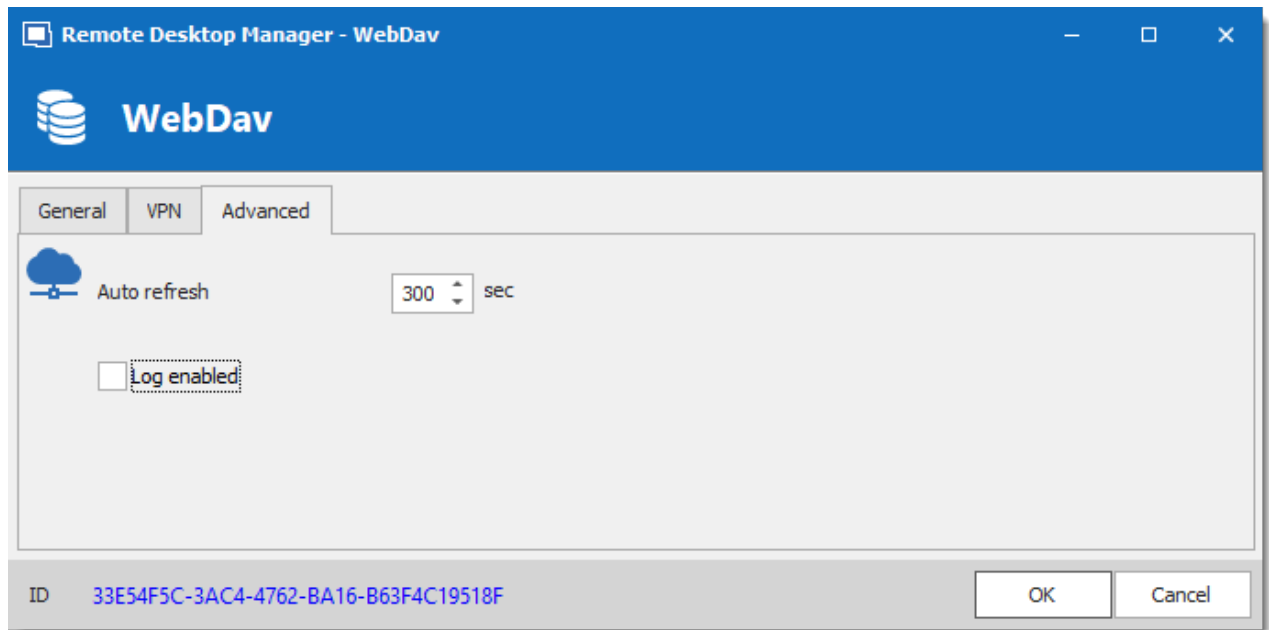
Password

ID 33E54F5C-3AC4-4762-BA16-B63F4C19518F

OK Cancel

*WebDAV - VPN Tab*

## ADVANCED

*WebDAV - Advanced Tab*

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

#### 5.4.7 XML

### DESCRIPTION



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

### HIGHLIGHTS

- It is possible to configure an auto refresh interval.
- The [Online Backup](#) is available for this data source.



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



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

## SETTINGS

### GENERAL

The screenshot shows the 'Remote Desktop Manager - Xml' window with the 'General' tab selected. The window has a blue header bar with the title and standard window controls. Below the header is a tab bar with 'General', 'Backup', 'VPN', and 'Advanced'. The 'General' tab contains an XML icon, a 'Name' field, a 'Filename' field with a file path and a browse button (...), a 'Master key' field, and a checked checkbox for 'Always ask master key'. At the bottom, there is an 'ID' field with a long alphanumeric string and 'OK' and 'Cancel' buttons.

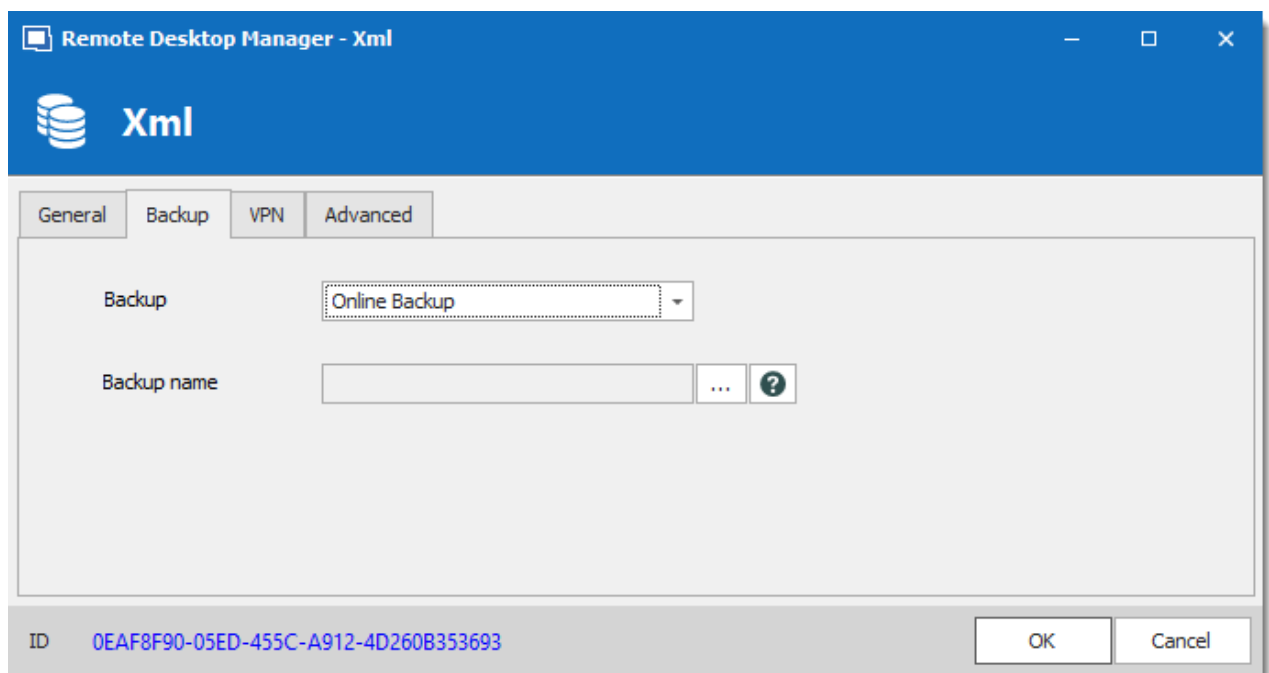
Field	Value
Name	
Filename	C:\Users\jmajeau\AppData\Local\Devolutions\Remo ...
Master key	
Always ask master key	<input checked="" type="checkbox"/>
ID	0EAF8F90-05ED-455C-A912-4D260B353693

XML - General Tab



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

## BACKUP



XML - Backup Tab

OPTION	DESCRIPTION
<b>Backup</b>	<p>Select between:</p> <ul style="list-style-type: none"><li>• <b>None</b>: No backup of your data source will be created.</li><li>• <b>File backup</b>: Your backup will be saved to a chosen file but will not automatically do backup every 30 seconds.</li><li>• <b>Online Backup</b>: An Online Backup (using <a href="#">Online Backup</a>) will automatically be created.</li></ul>
<b>Backup name</b>	<p>Specify the backup name that will allow you to automatically save your sessions in a safe online storage space and restore them in the event of problems.</p>

## VPN

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

The screenshot shows a Windows-style dialog box titled "Remote Desktop Manager - Xml". It has a blue header bar with a database icon and the text "Xml". Below the header are four tabs: "General", "Backup", "VPN", and "Advanced", with "Advanced" being the active tab. The main area contains a "Type" dropdown menu set to "On first connect" with a play button icon to its right. Below this is an "RDM File" text field with a browse button "...". A checkbox labeled "Override credentials" is unchecked. Underneath are three text fields for "Username", "Domain", and "Password". At the bottom, there is an "ID" label followed by the text "1DC1E4B2-F219-424D-9CB6-24C02EE2E970" and two buttons: "OK" and "Cancel".

Remote Desktop Manager - Xml

Xml

General Backup VPN Advanced

Type On first connect

RDM File

☐ Override credentials

Username

Domain

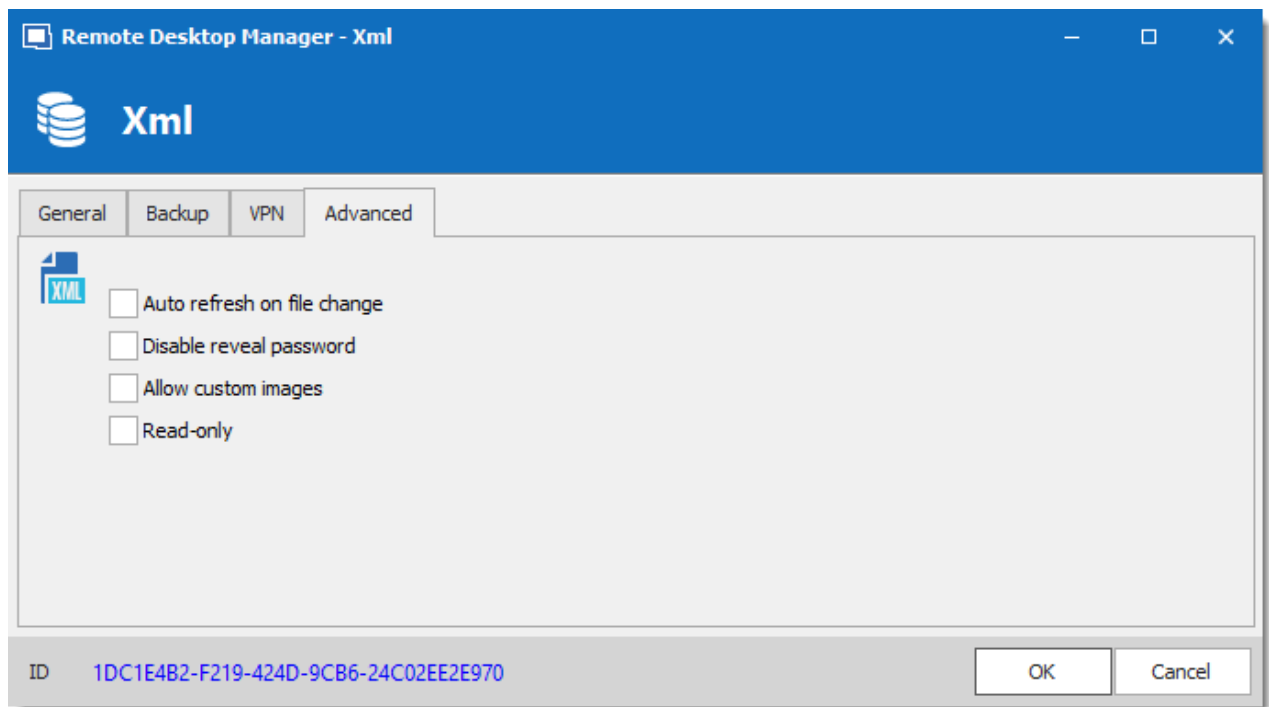
Password

ID 1DC1E4B2-F219-424D-9CB6-24C02EE2E970

OK Cancel

*XML - VPN Tab*

## ADVANCED

*XML - Advanced Tab*

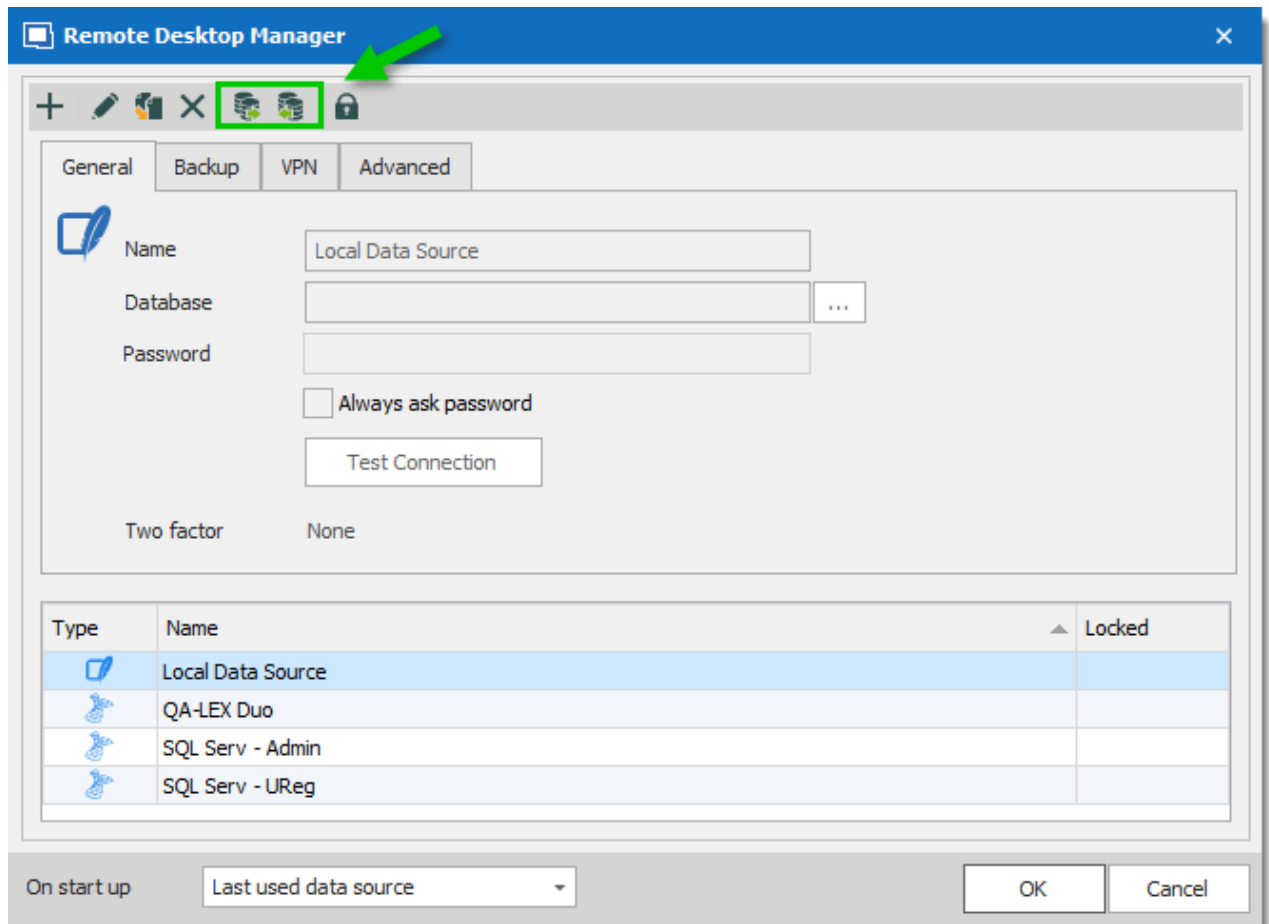
OPTION	DESCRIPTION
<b>Auto refresh on file change</b>	Indicate if the application monitor the file changes to automatically refresh the data source.
<b>Disable reveal password</b>	Disable the reveal password feature when a user accesses this data source.
<b>Allow custom images</b>	This will enable the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

## 5.5 Import/Export Data Source

### DESCRIPTION

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

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



*Data Sources - Import and Export*



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



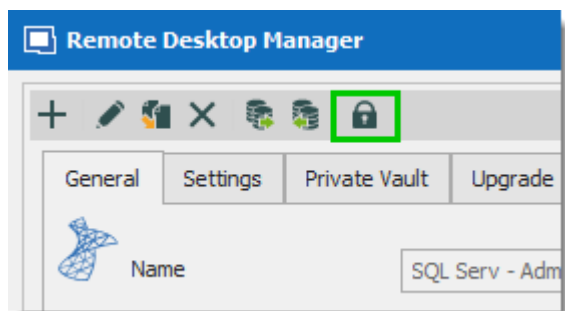
A locked data source can be exported and imported, but the content will be locked unless a password is entered when the data source is selected. See [Lock Data Source](#) for more information.

## 5.6 Lock Data Source

### LOCK DATA SOURCE

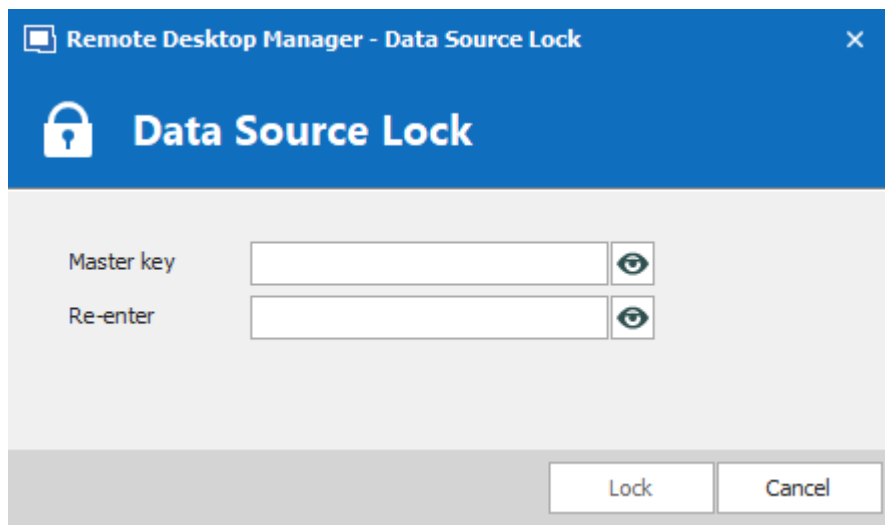
To protect sensitive data in your data source configuration (e.g. server URL or credentials), you may wish to lock the data source configuration before you deploy it to your users. You can do it by using the Lock/Unlock button from the toolbar.

### SETTINGS



*Lock Data Source toolbar*

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



*Lock Data Source dialog*



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

## 5.7 Offline mode

### DESCRIPTION

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

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



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



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

For added security, offline files are set to expire after a delay. The default expiry is set to 7 days but can be modified via the [Data Source Settings \(System Settings\)](#).

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

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

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

### AVAILABILITY

The offline mode availability relies on several settings:

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

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

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

Data Source Information		
ID		
Server		
Database		
Is DB owner	✓	
Is System DBA	✓	
Offline mode	64.0 KB	Read/write
Group Policy settings		Read/write
System settings		Read/write
User settings		Read/write
Data source config		Intelligent
Vault		Allow offline
Vault	Default	

*My Data Source Information - Offline mode*

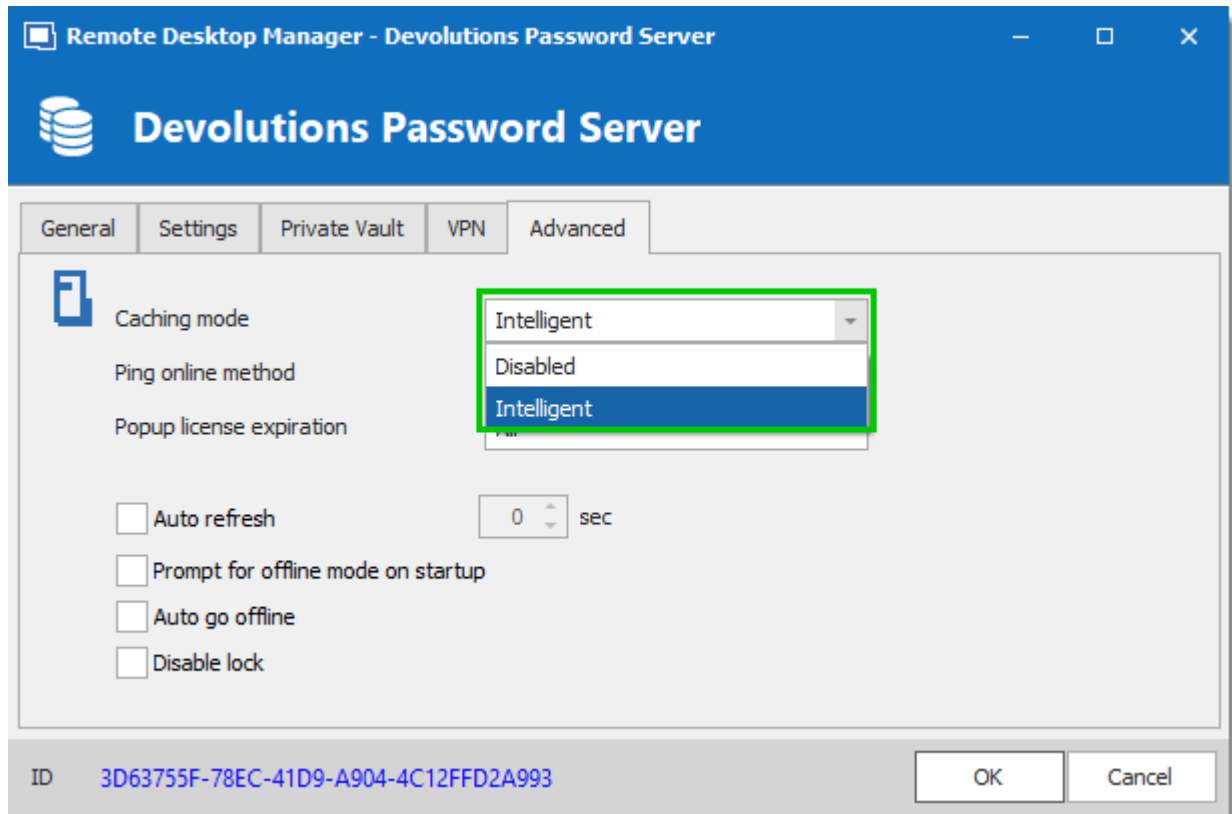
## CACHING MODE

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





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



*Data Source configuration – Advanced – Caching mode*

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



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



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

## GRANT/DENY OFFLINE



Watch Video

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

Beyond the group policies, the Offline mode is controlled at four levels:

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

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

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

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



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

### 5.7.1 Offline Read/Write

## DESCRIPTION

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



Some functionalities are not available while offline and you may not be able to perform all actions. Note that the [Private Vault](#) is still available in offline mode.

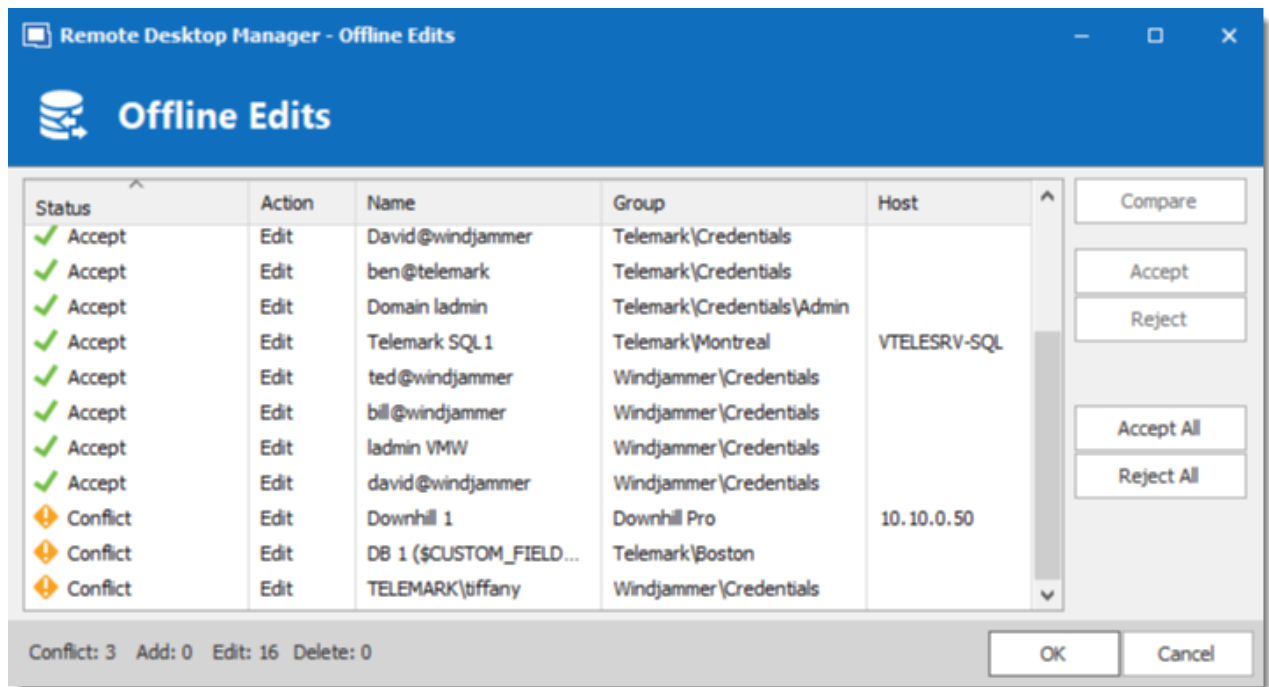
Once offline, the users security settings still applies. Add/Edit/Delete privileges granted by the administrator are still in effect. See [User Management](#).

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

## OFFLINE EDITS WORKFLOW

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

The **Offline Edits** window is displayed:



Offline Edits

Use this dialog to accept/reject your offline changes.

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

Entries will be marked:

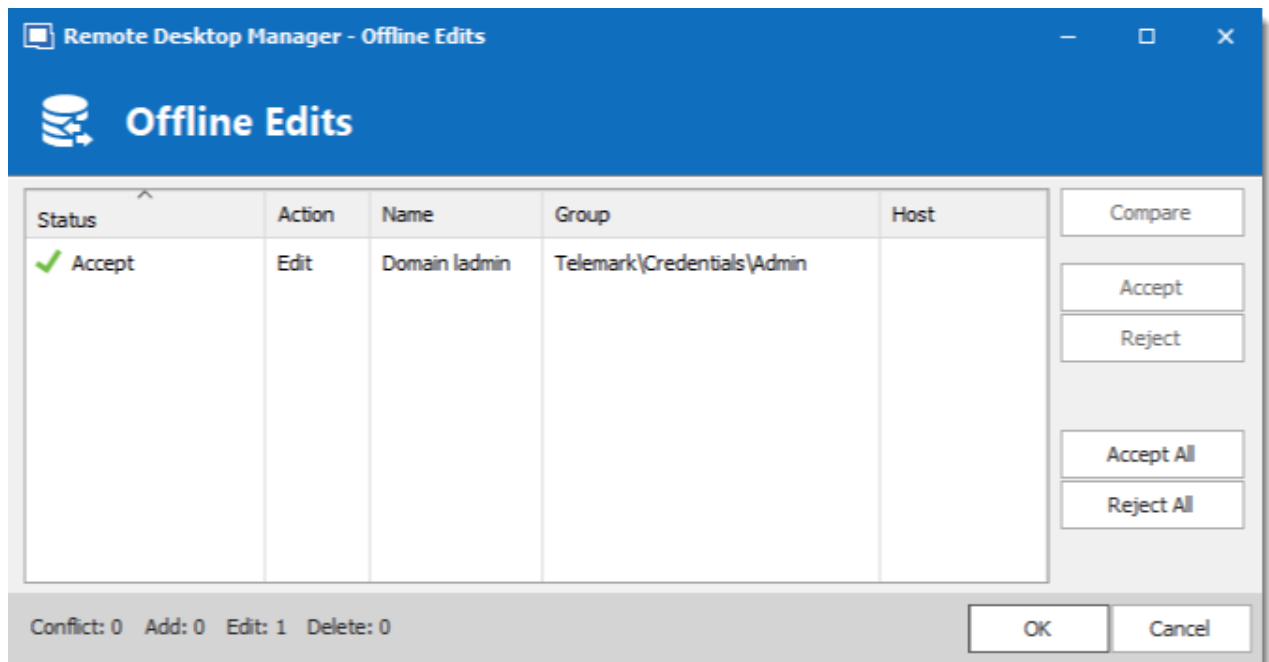
- Accept - when no outside changes have been detected.
- Conflict - when outside changes have been detected since you were last connected.

## MULTIPLE OFFLINE EDITS

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

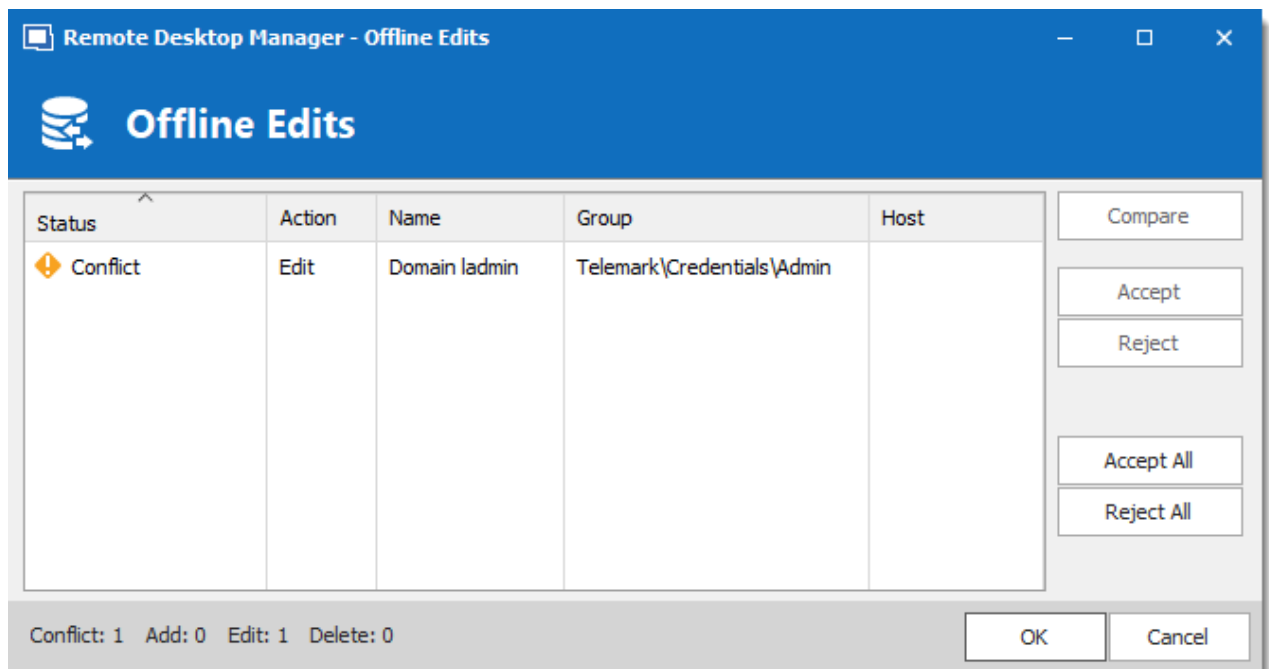
Here is an example of such a case to help resolving conflicts properly:

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



*Offline Edits For The First User Back Online*

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



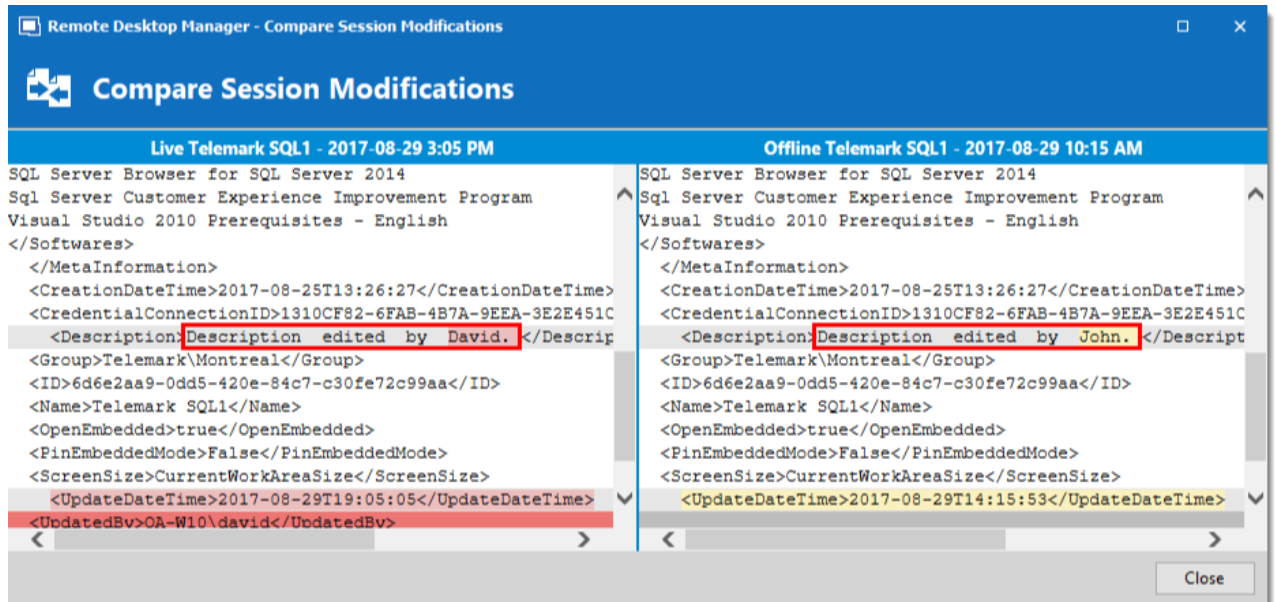
*Offline Edits For The Second User Back Online*

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

## COMPARE VERSIONS OF AN ENTRY

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

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



Compare Session Modification

## 5.8 Manage Cache

### DESCRIPTION

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



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

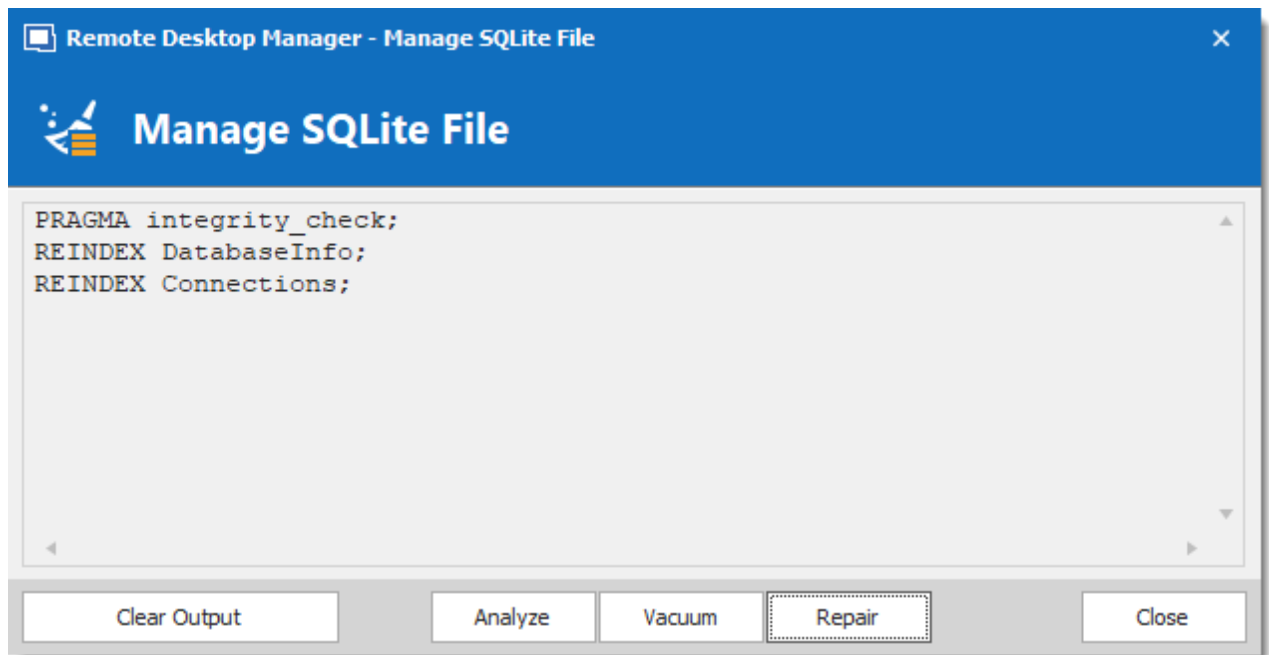


The Manage Cache options should usually only be used **upon request from our Support Team** when experiencing cache issue.

## SETTINGS



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



*Manage Cache*

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



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

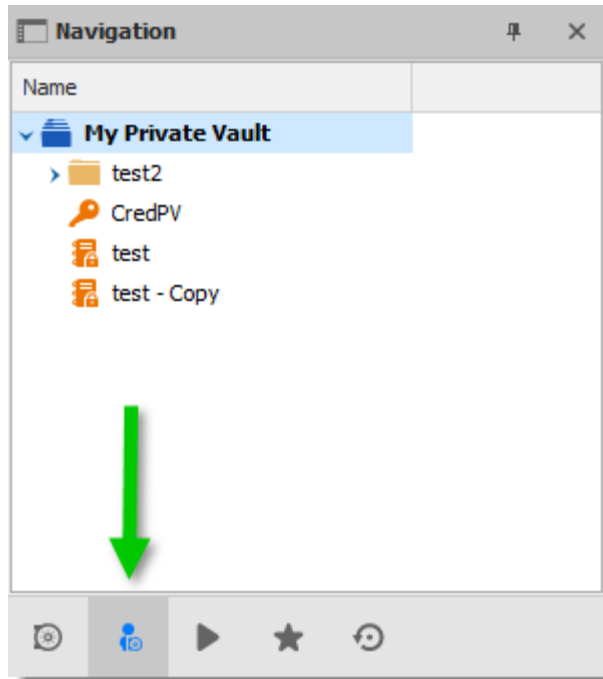
## 5.9 Private Vault

### DESCRIPTION

The **Private Vault** is a user specific Vault for entries of any type. It allows each user to create entries that only them can access. Not even administrators can access a user's Private Vault.



The Private Vault is available for all [Advanced Data Sources](#).



*Navigation Pane – Private Vault*

## A NOTE ON CREDENTIALS

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

1. From a session using the **Private Vault search**.
2. When using the [User Specific Settings](#) feature.

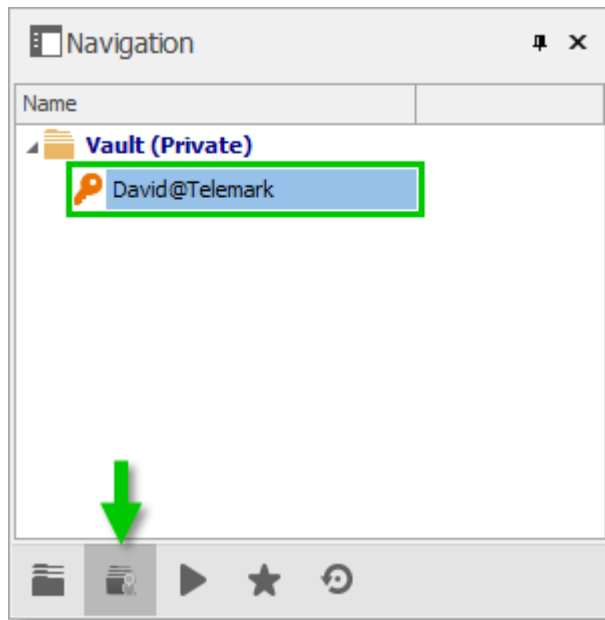
These restrictions can easily be understood when you keep in mind that the Private Vault is in fact contained in the user area of the database. It must be used from within the Private Vault, or by using our extension mechanism that is user specific.

### 5.9.1 Private Vault Search

The **Private Vault Search** links a Private 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.

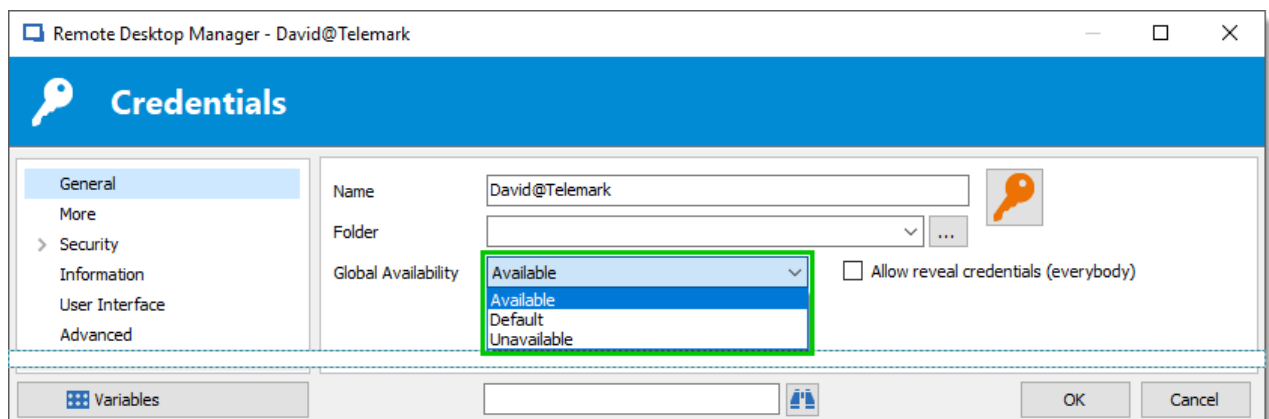
## SETTINGS

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



Private Vault

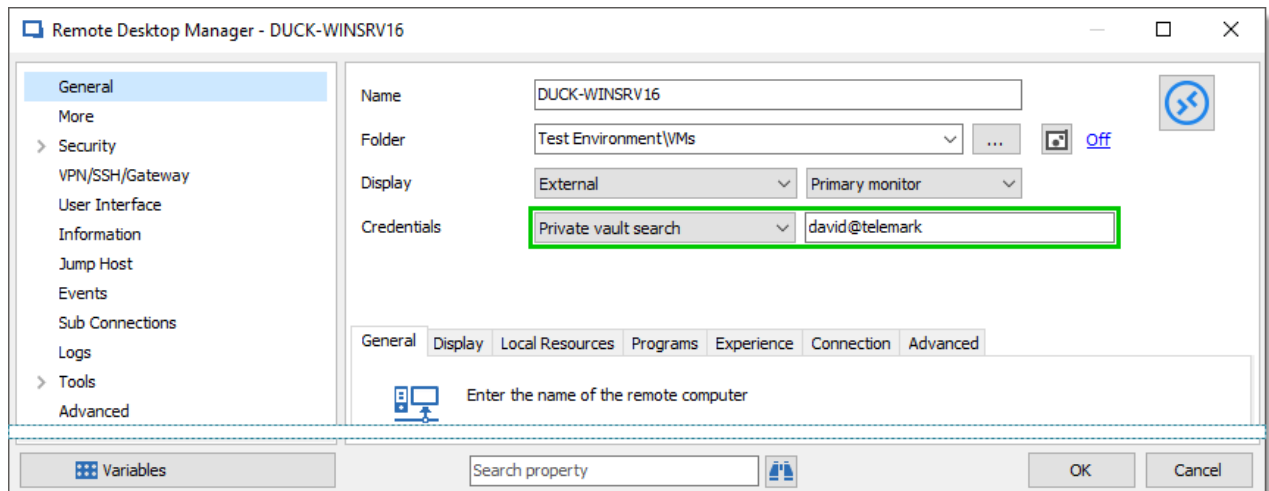
- Set the **Global Availability** property of the Private Vault credential to **Available**.



Global Availability

OPTION	DESCRIPTION
<b>Available</b>	Make the credential entry available for Private Vault search.
<b>Default</b>	Use the setting defined in <b>File - Options - Types - Credentials - Global Availability</b> .
<b>Unavailable</b>	Ignore the credential entry when using the Private Vault search.

3. In the remote session, set the **Credentials** property to **Private Vault search** and enter the **exact name** of the Private 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 Private Vault credentials. Variables are supported as well.



*RDP Session - Private Vault Search*

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



The Private Vault is linked to the database user. Another user will never be able to see your Private Vault credentials even when the **Global Availability** is set to **Available**.

# Commands

---

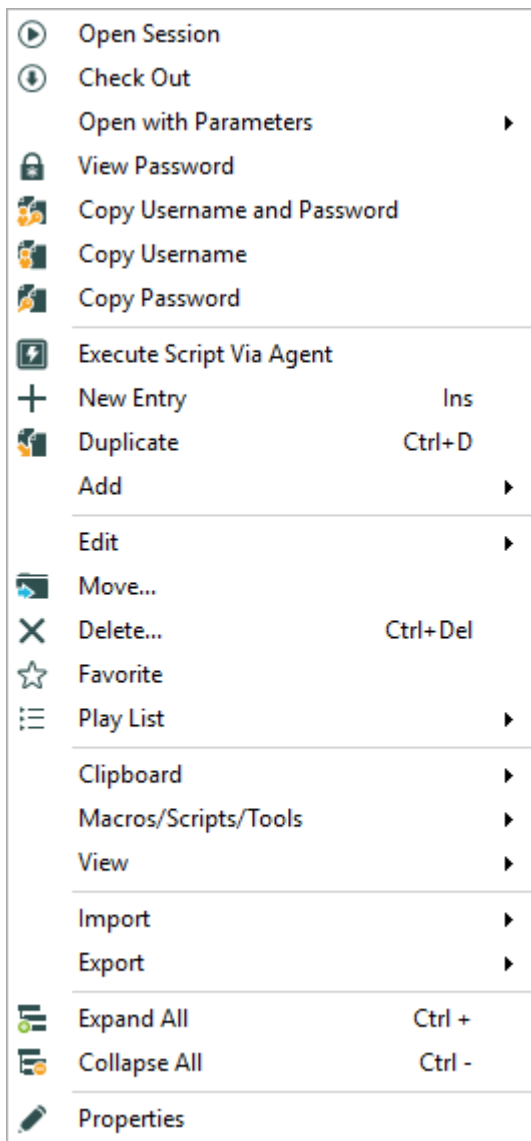
Part VI

## 6 Commands

### 6.1 Context Menu

#### DESCRIPTION

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

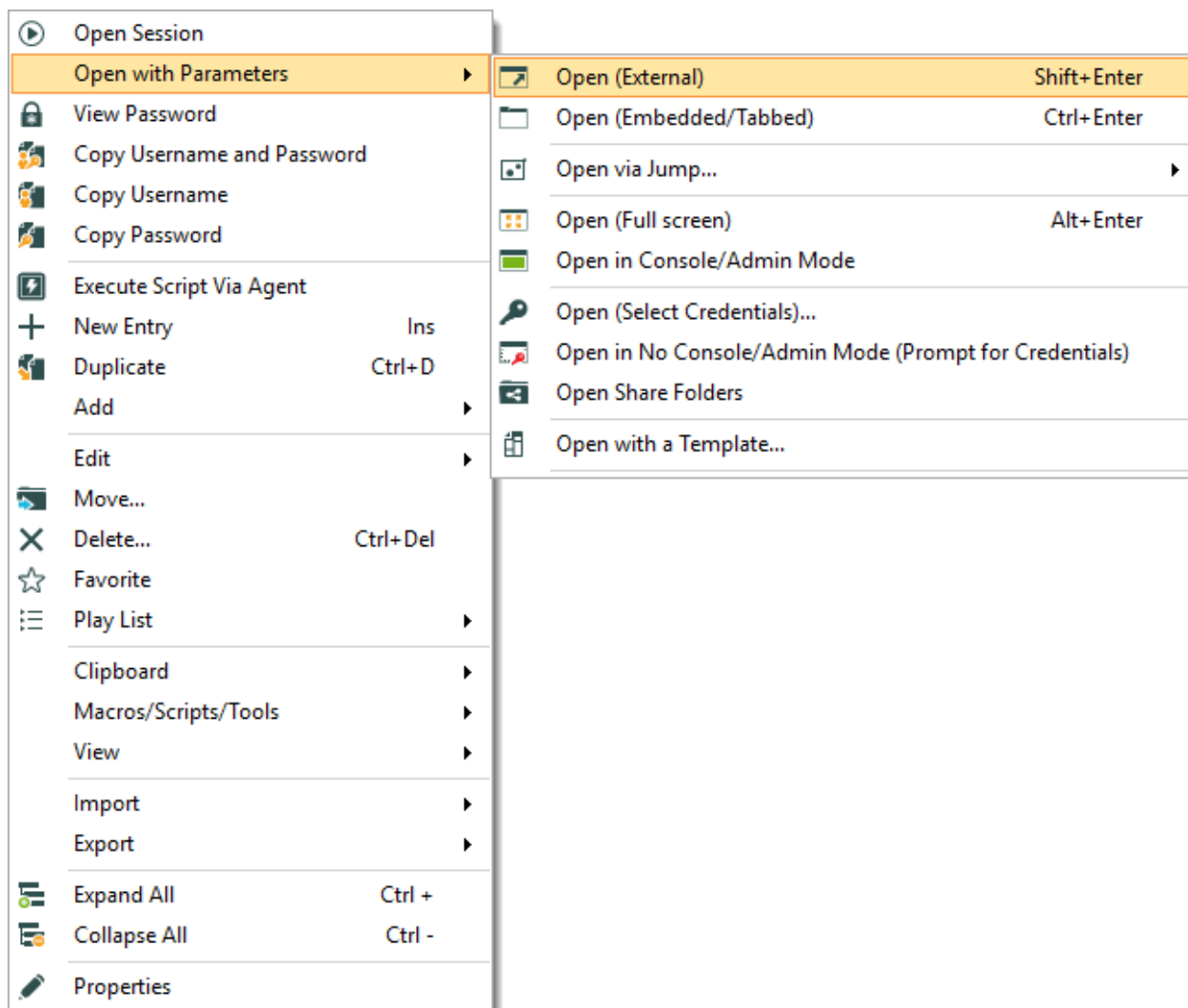


*Context Menu*

## 6.1.1 Open with Parameters

### DESCRIPTION

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



*Open with Parameters*

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

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

## 6.1.2 Documentation

### DESCRIPTION



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

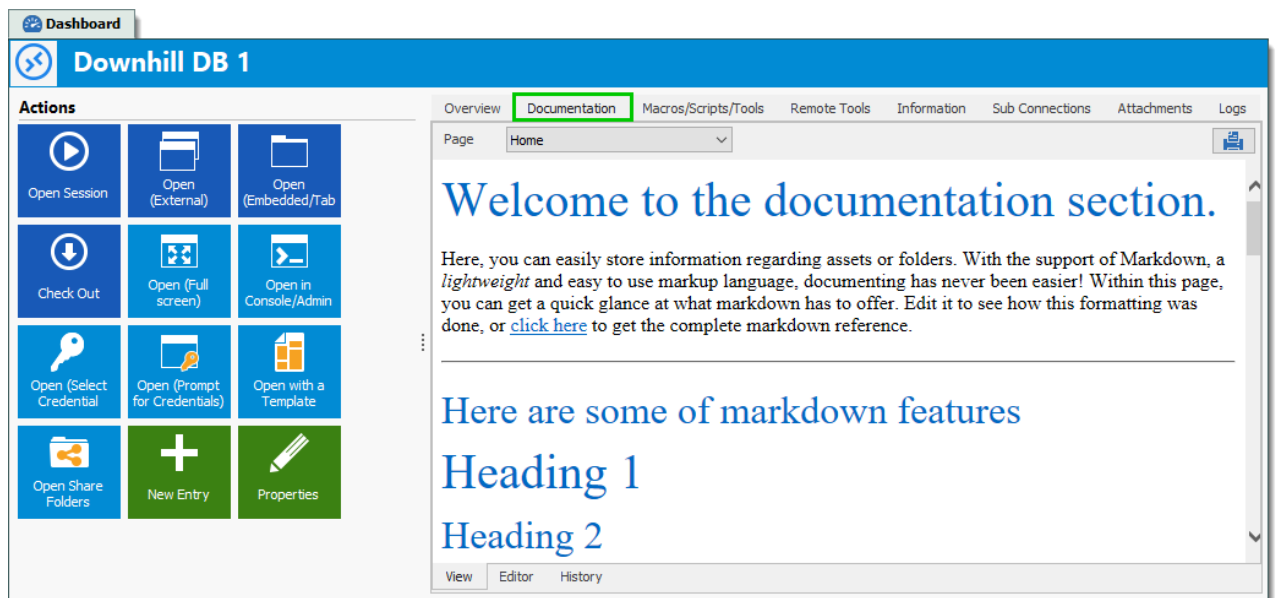
The documentation is written using [Markdown](#), a plain text formatting syntax.



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



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

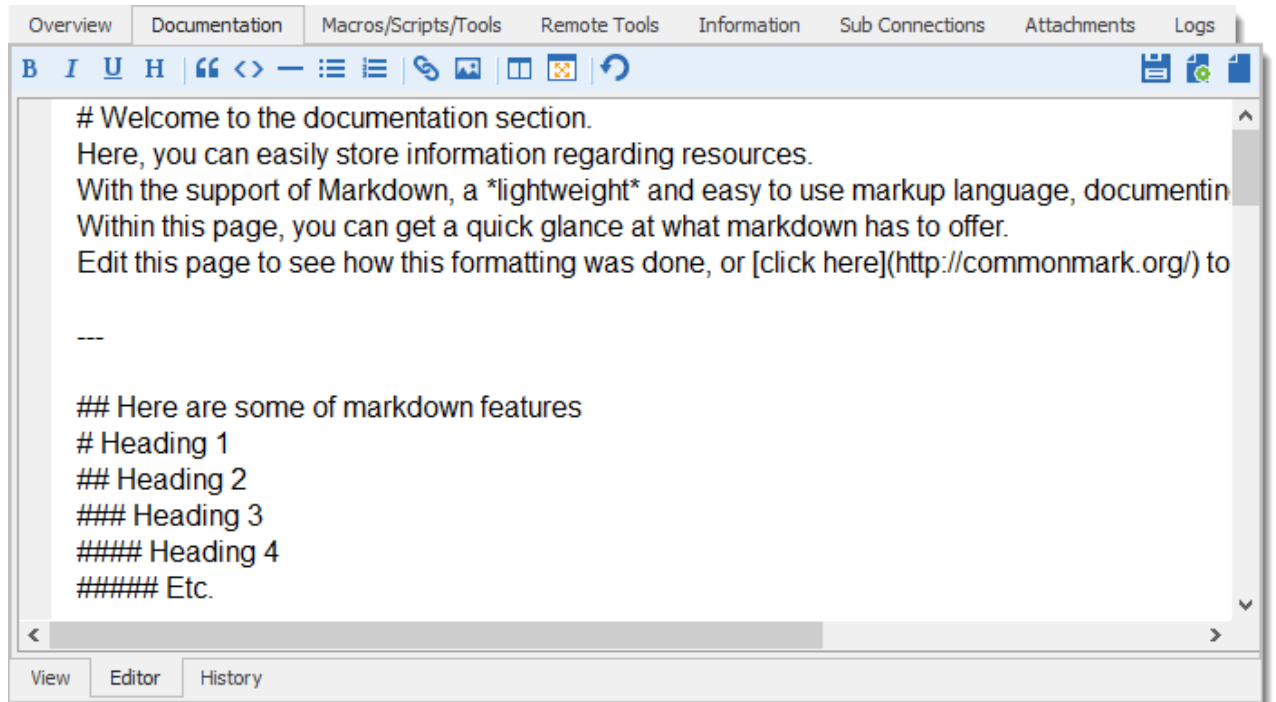


*Documentation of an entry*

### 6.1.2.1 Editor

## DESCRIPTION

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

*Documentation editor*

## MARKDOWN FORMATTING TAGS

- [Paragraphs](#)
- [Emphasis](#)
- [Headers](#)
- [Lists](#)
- [Horizontal rulers](#)
- [Links](#)
- [Images](#)
- [Blockquotes](#)
- [Code examples](#)

## PARAGRAPHS

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

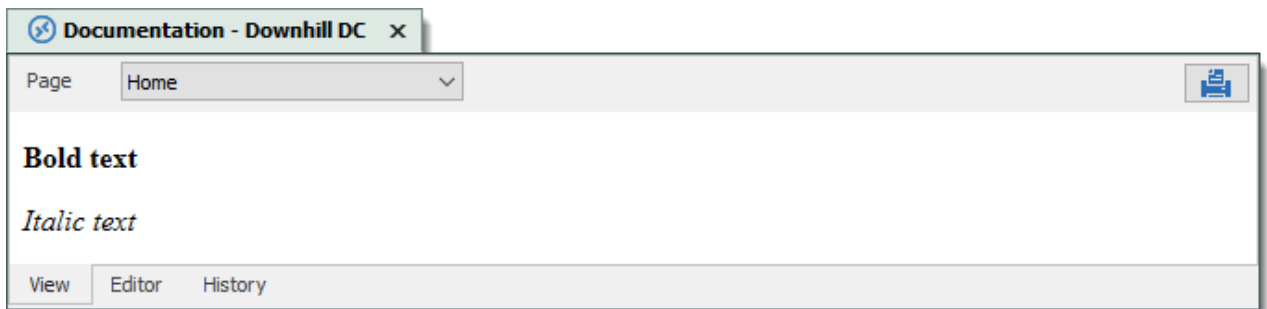
## EMPHASIS

Two methods of text emphasis are available:

`**Bold text**`

`*Italic text*`

Output:



## HEADERS

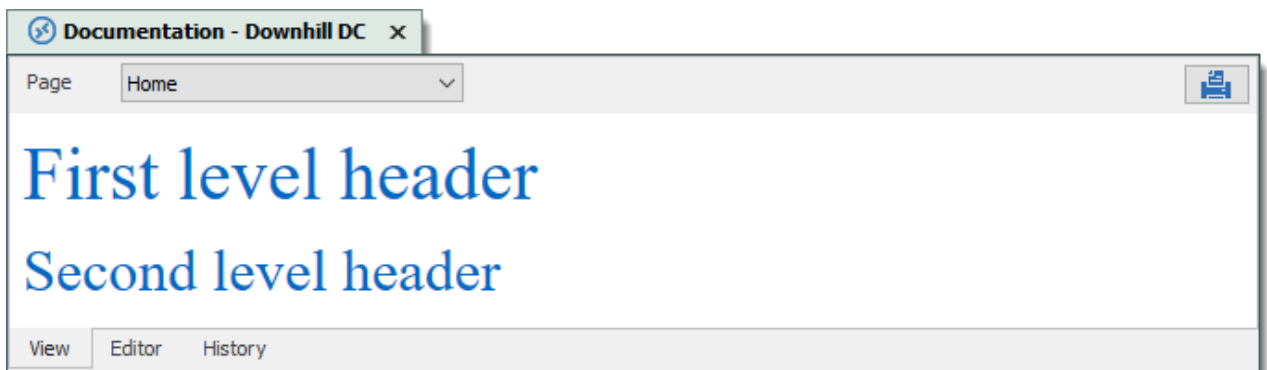
There are two ways of creating headers with Markdown.

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

`First level header`  
`=====`

`Second level header`  
`-----`

Output:



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

# First level header

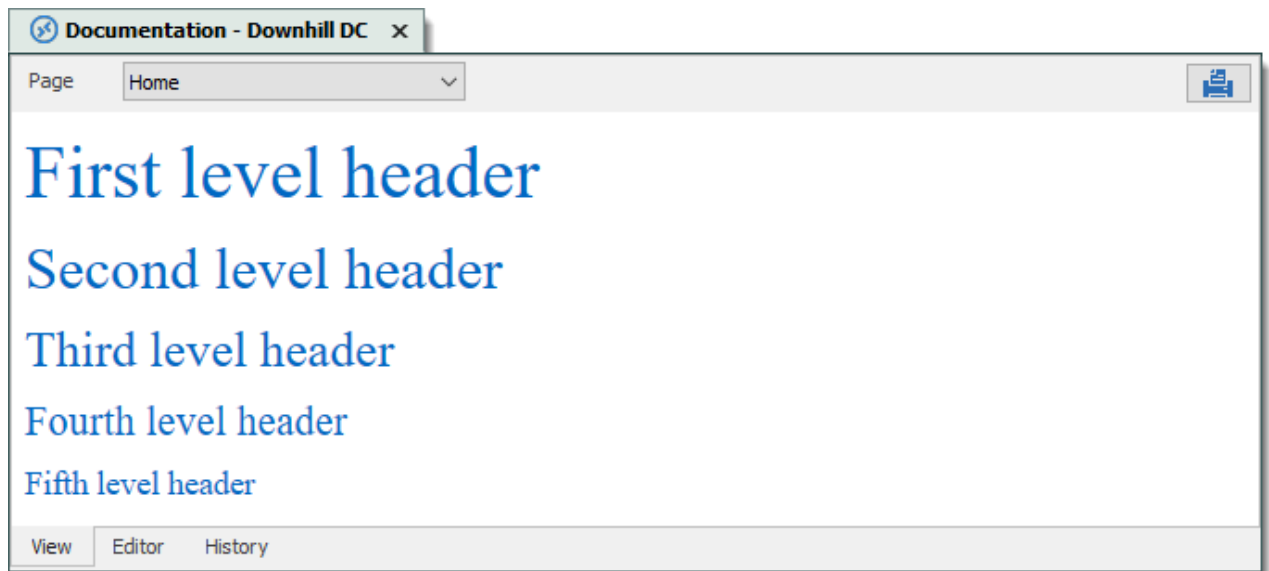
## Second level header

### Third level header

#### Fourth level header

##### Fifth level header

Output:



## LISTS

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

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

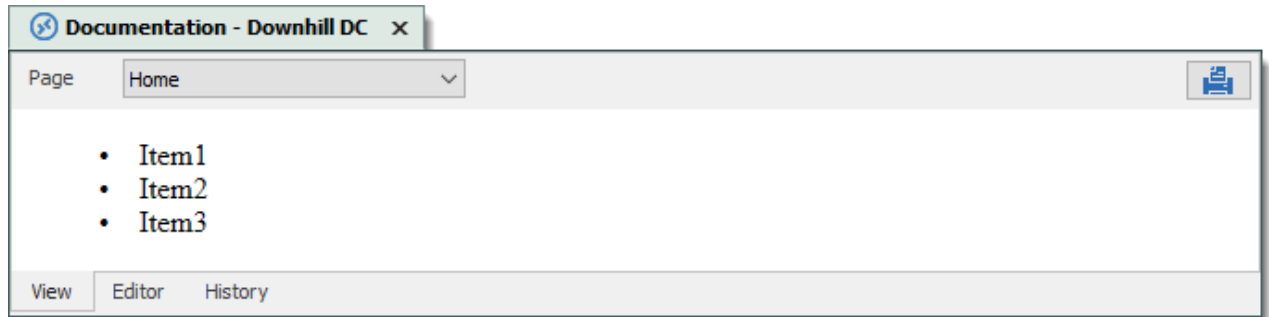
or

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

or

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

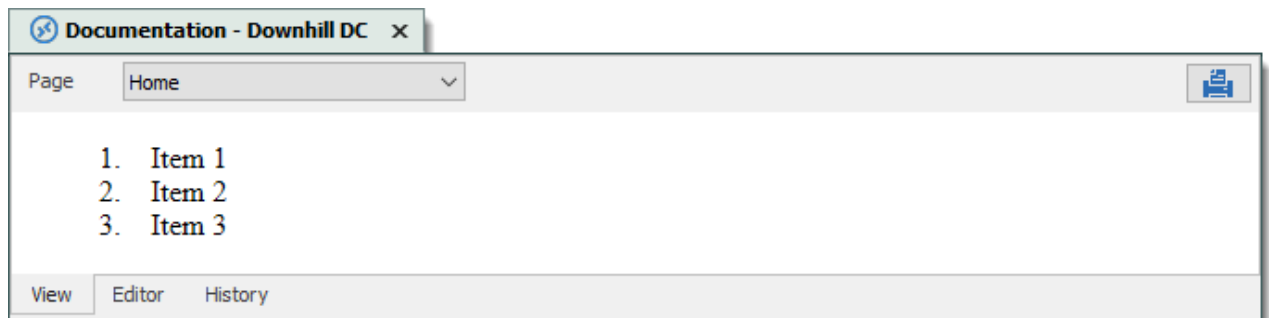
Output:



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

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

Output:



## HORIZONTAL RULERS

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

---

or

\*\*\*

or

---

Output:



## LINKS

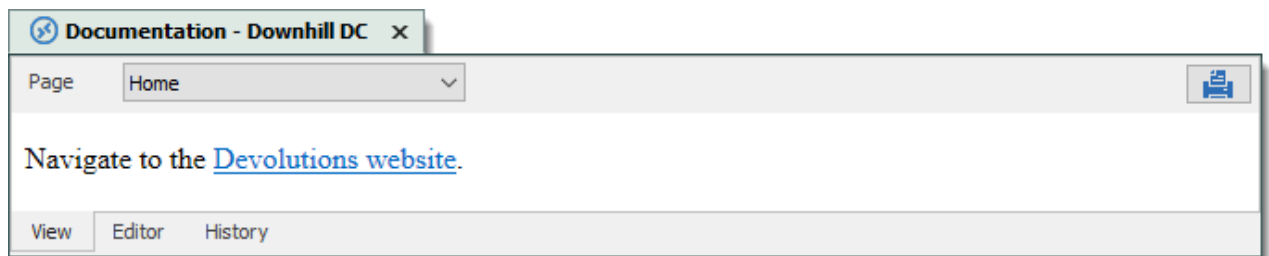
Use square brackets to delimit the text you want to turn into a link.

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

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

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

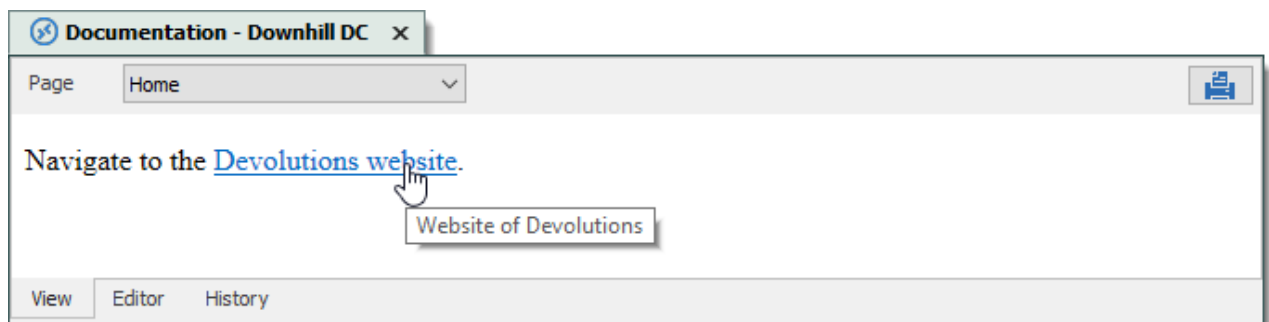
Output:



Optionally a title attribute may be included in the parentheses.

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

Output:



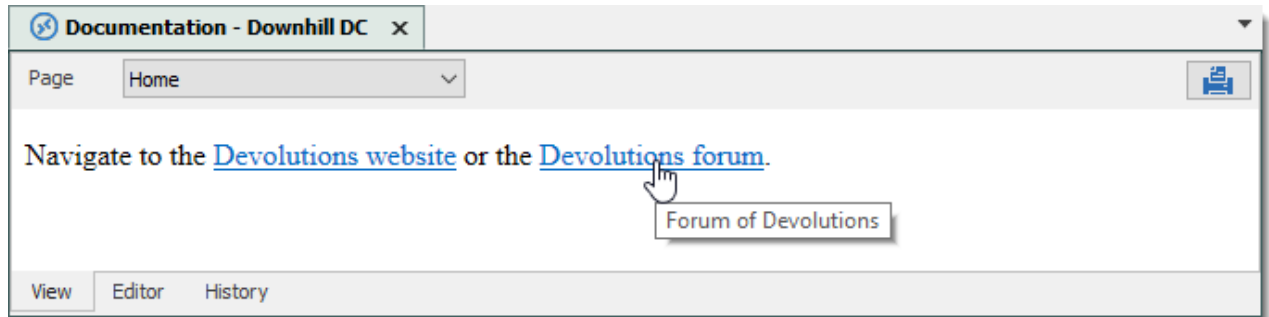
For reference-style links, define the links elsewhere in the document, then refer to a link by its name in another set of square brackets.

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

[mainwebsite]: https://devolutions.net/ "Website of Devolutions"

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


Output:

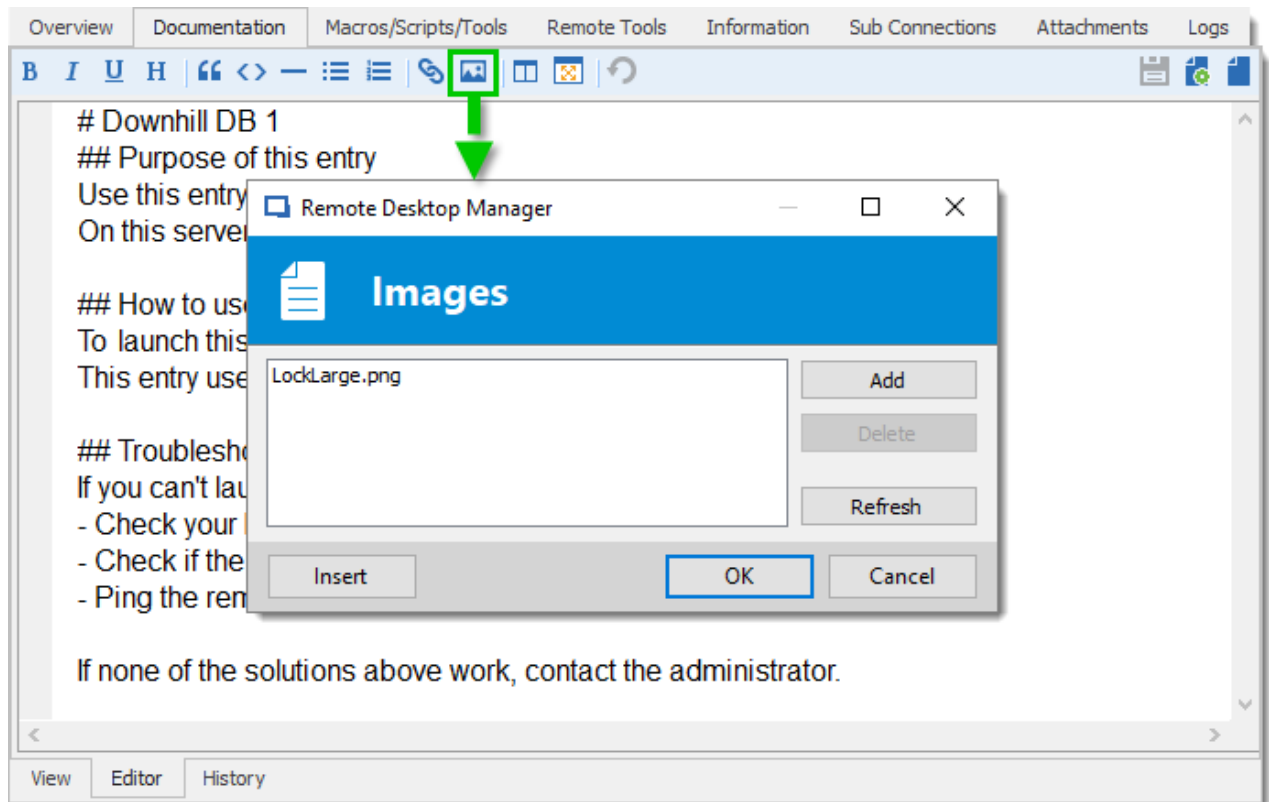


The title attribute is optional again. Link names may contain letters, numbers and spaces, but are not case sensitive.

## IMAGES

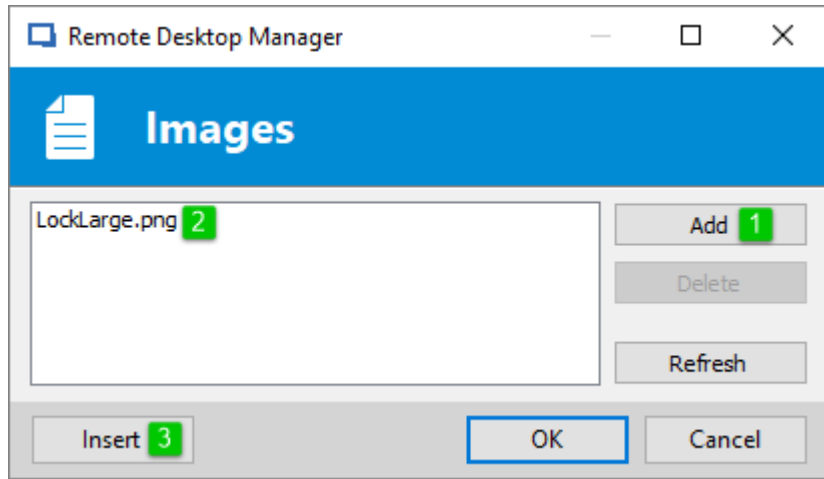
Image syntax is very similar to link syntax. Images must be added in the image manager before referencing them.

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



*Documentation editor – Image manager*

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



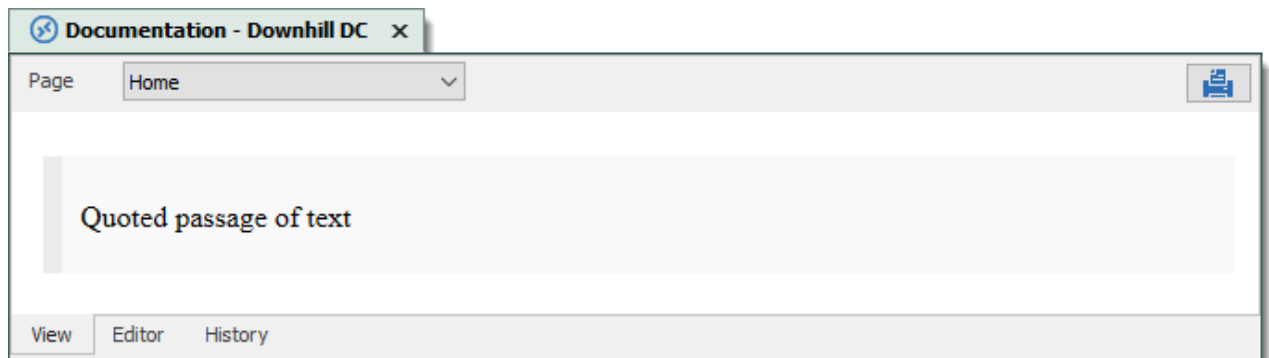
*Documentation editor - Add an image*

## BLOCKQUOTES

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

> Quoted passage of text

Output:



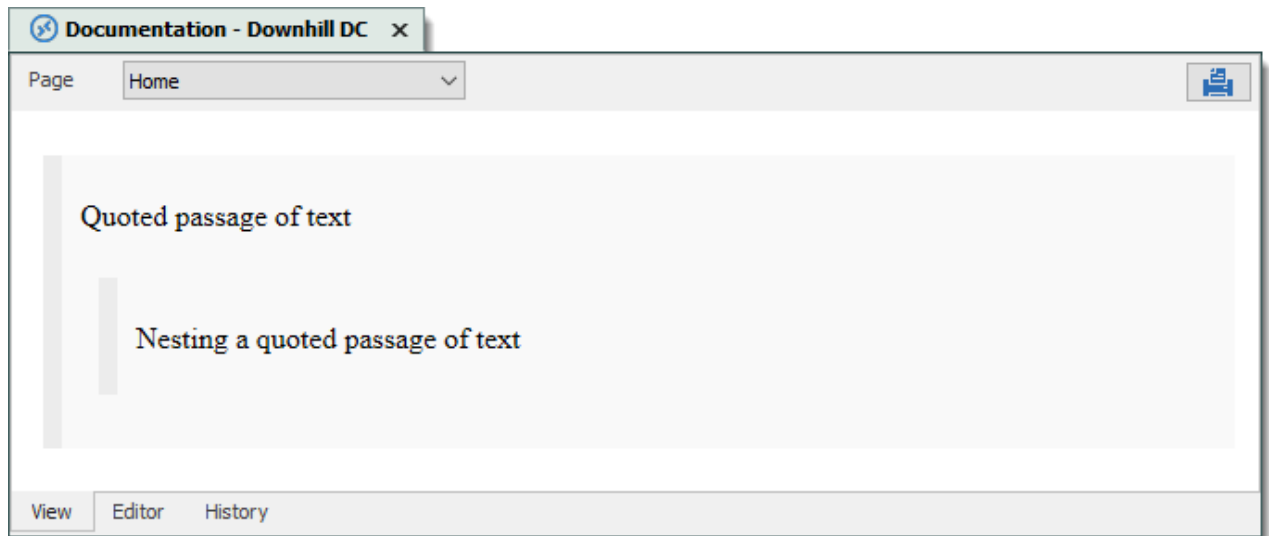
Blockquotes can easily be nested.

> Quoted passage of text

>> Nesting a quoted passage of text

Output:



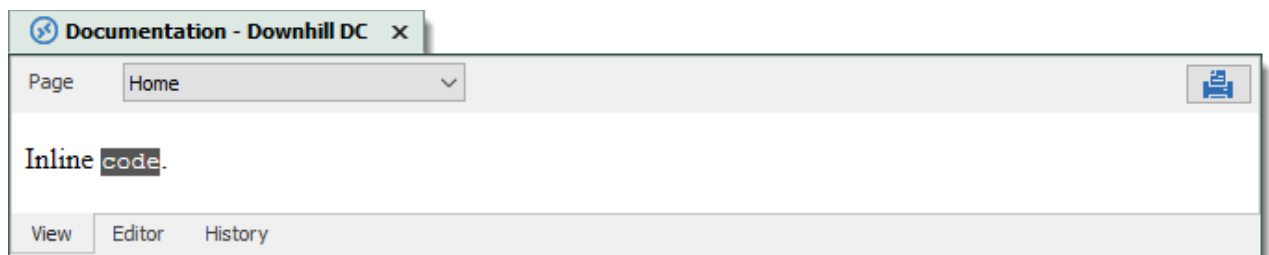


## CODE EXAMPLES

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

Inline ``code``.

Output:



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

```
// Testing indented code

var markdownAwesomeness = 0;

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

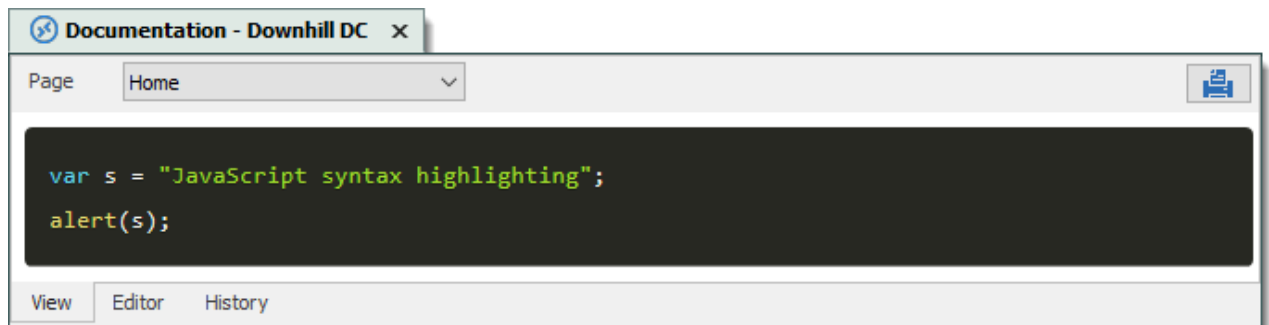
Output:



A specific syntax highlighting can be specified as well.

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

Output:



### 6.1.3 Entry History

## DESCRIPTION

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



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

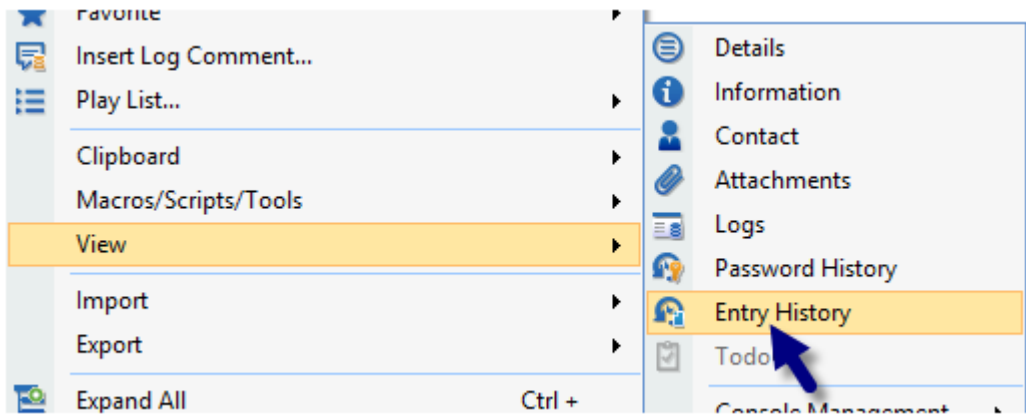


For architectural reasons, the documents stored in our Advanced Data Sources are **NOT** protected from modifications. Once they are modified, the previous version **cannot be restored**. Please keep a safe copy of all documents in another storage device. Support for this feature will be added in a coming update to our products.



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

## SETTINGS



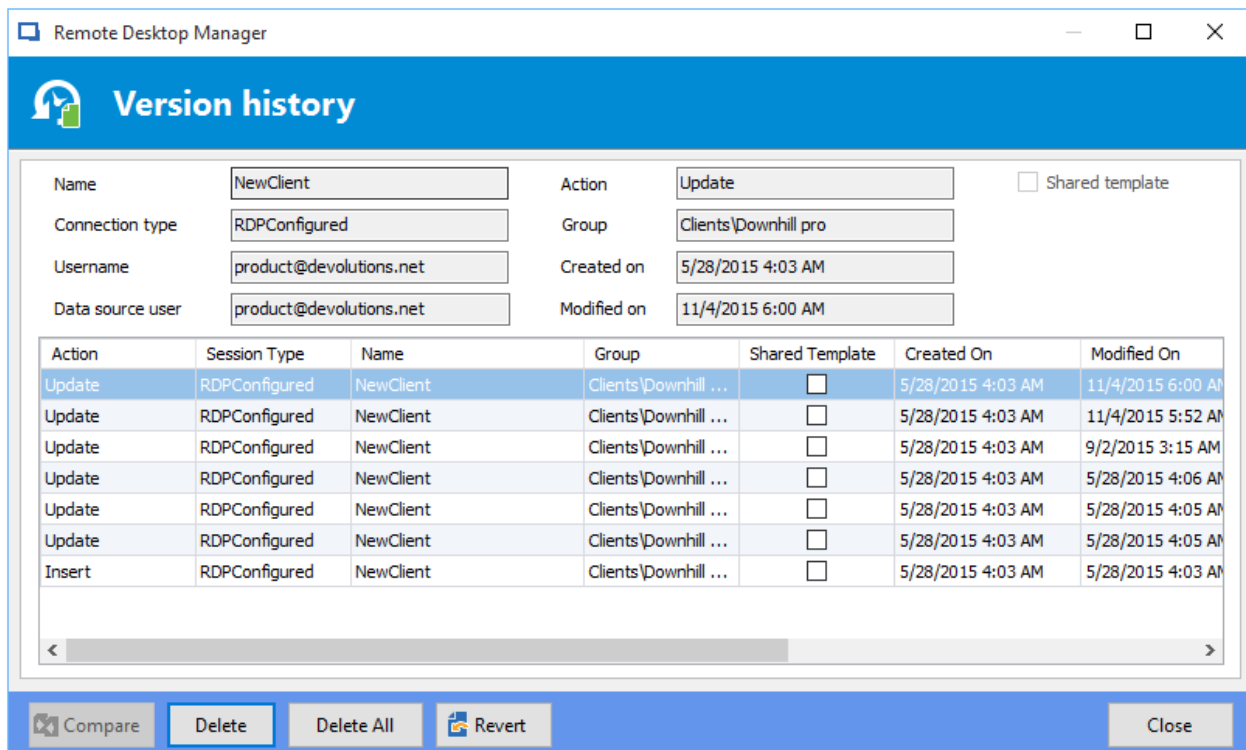
Home - Entry History

### Session History

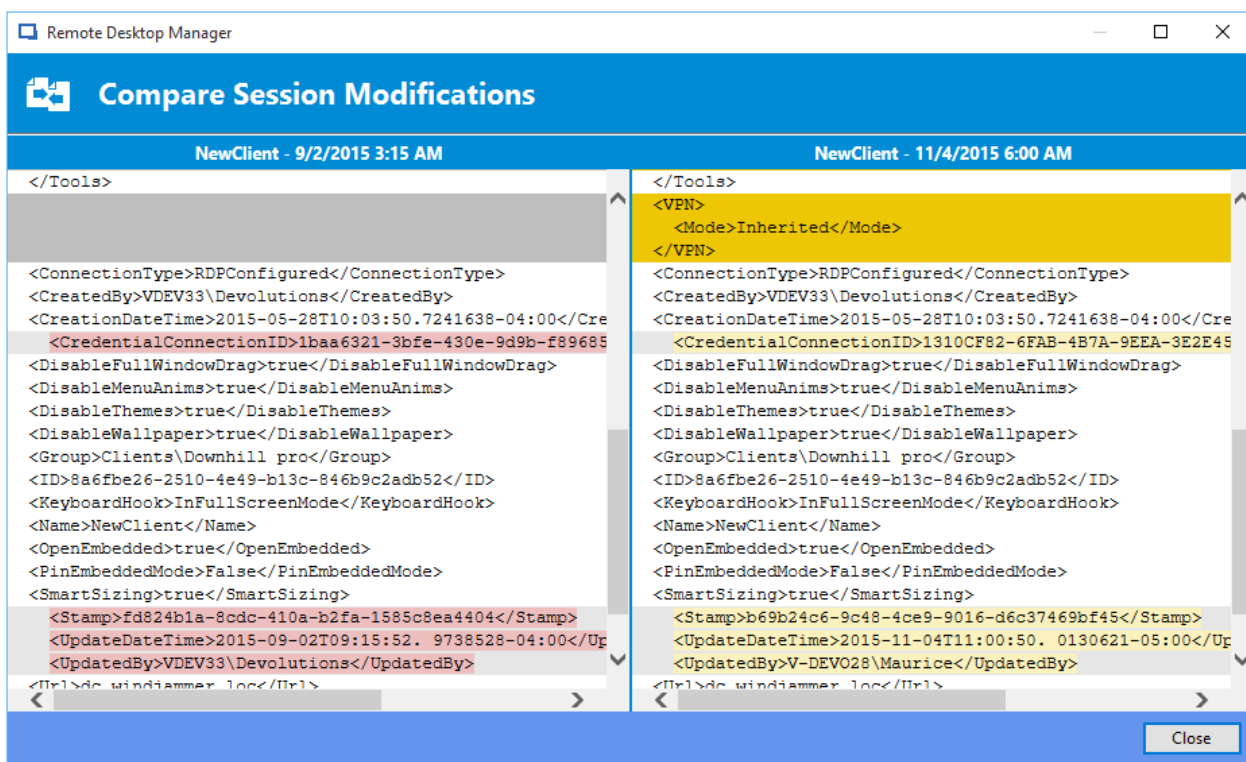
To display the entry history, **right-click** on an entry and select **View - Entry History**.

## ENTRY HISTORY VIEW

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



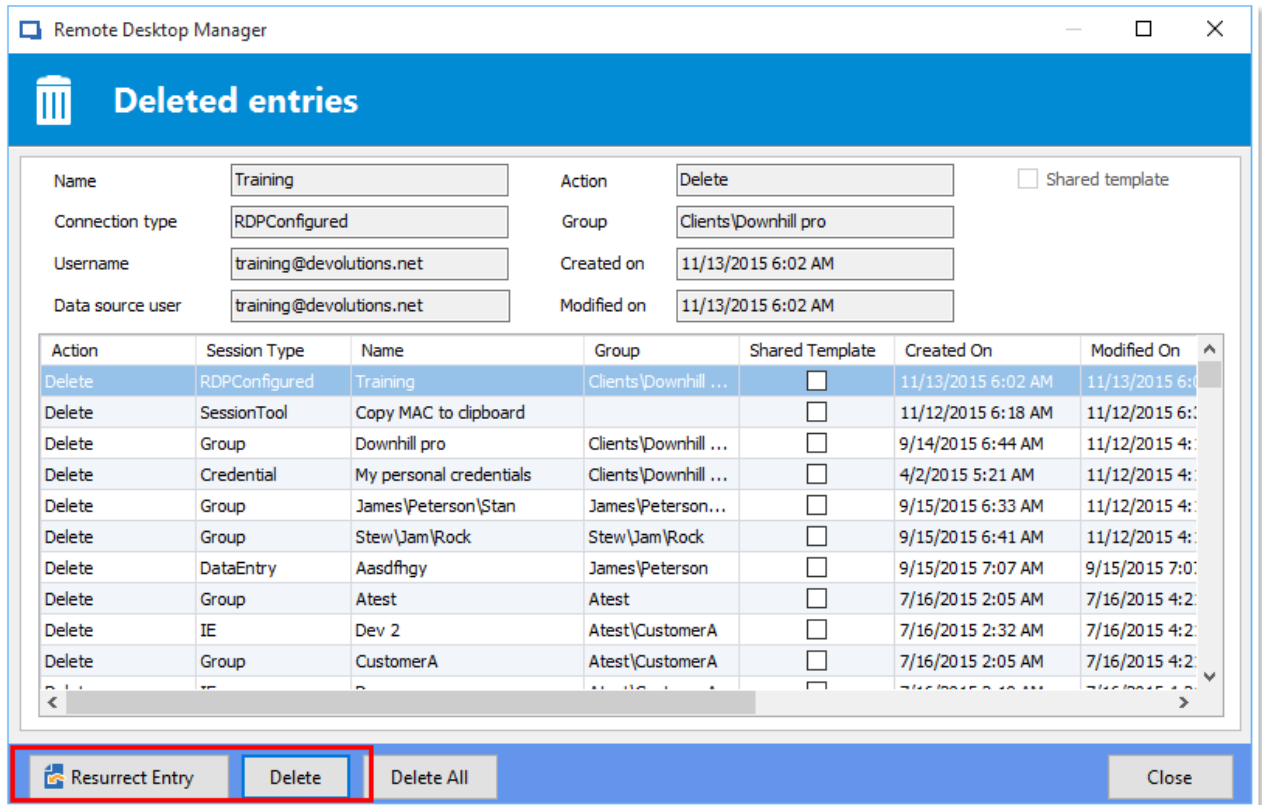
Entry history view



Compare session modifications

## VIEW DELETED ENTRIES

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

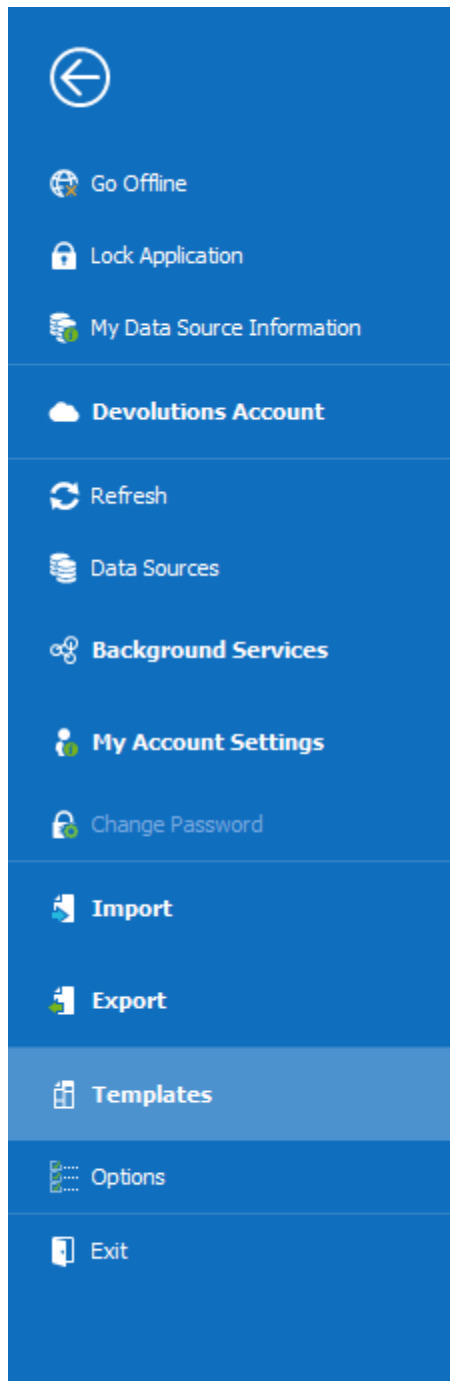


*Deleted Entries*

## 6.2 File

### DESCRIPTION

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

*File*

## GO OFFLINE/ONLINE

Toggle the data source offline mode.

For more information, please consult the [Offline mode](#) topic.

## LOCK APPLICATION

Lock and minimize the application.

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

## MY DATA SOURCE INFORMATION

Display configuration information relative to the current data source.

For more information, please consult the [My Data Source Information](#) topic.

## DEVOLUTIONS ACCOUNT

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

For more information, please consult the [Devolutions Account](#) topic.

## REFRESH

Refresh the data source and retrieve the most recent data.

For more information, please consult the [Refresh](#) topic.

## DATA SOURCES

Open the data source configuration screen.

For more information, please consult the [Data Sources](#) topic.

## BACKGROUND SERVICES

View and execute synchronizers.

For more information, please consult the [Background Services](#) topics.

## MY ACCOUNT SETTINGS

View information about the current user and edit personal credentials.

For more information, please consult the [My Account Settings](#) topic.

## CHANGE MASTER KEY

Prompts to change the current Master Key

For more information, please consult the [Change Master Key](#) topic.

## IMPORT

Import entries in the data source.

For more information, please consult the [Import](#) topic.

## EXPORT

Export entries from the data source.

For more information, please consult the [Export](#) topic.

## OPTIONS

Edit the application options.

For more information, please consult the [Options](#) topic.

## TEMPLATES

Edit templates and default settings for entries.

For more information, please consult the [Templates](#) topic.



## 6.2.1 Go Offline/Online

### DESCRIPTION

Toggle the data source [Offline Mode](#).

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



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

The offline mode availability relies on several settings, refer to the [Offline Mode](#) topic.

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

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

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

*Data Source Information - Offline mode*

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

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


## 6.2.2 My Data Source Information

### DESCRIPTION




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



The **My Data Source Information** view can be different depending on the [Data Source Type](#). This topic uses an SQL Server data source.



## Data Source Information

|                       |               |            |           |
|-----------------------|---------------|------------|-----------|
| ID                    |               |            |           |
| Server                |               |            |           |
| Database              | TCP           | v1.523     | JafJafDen |
| Is DB owner           | ✓             |            |           |
| Is System DBA         | ✓             |            |           |
| Offline mode          | 64.0 KB       | Read/write |           |
| Group Policy settings | Read/write    |            |           |
| System settings       | Read/write    |            |           |
| User settings         | Read/write    |            |           |
| Data source config    | Intelligent   |            |           |
| Vault                 | Allow offline |            |           |
| Vault                 | Default       |            |           |

General
Entries
Security Groups (Legacy)
Roles

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

File – My Data Source Information

## USER AND SECURITY

## GENERAL

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

| General                     | Entries | Security Groups (Legacy) | Roles |
|-----------------------------|---------|--------------------------|-------|
| Database user               |         |                          |       |
| User                        |         |                          |       |
| Description                 |         |                          |       |
| Is administrator            |         |                          |       |
| Allow offline mode          |         |                          |       |
| Allow drag-and-drop         |         |                          |       |
| Is Auto Refresh             |         |                          |       |
| Auto refresh interval 0 sec |         |                          |       |
| Is Two Factor Configuration |         |                          |       |

*My Data Source Information - General*

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

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

## ENTRIES

| General | Entries                        | Security Groups (Legacy) | Roles |
|---------|--------------------------------|--------------------------|-------|
|         | Add entries                    |                          | ✓     |
|         | Edit entries                   |                          | ✓     |
|         | Delete entries                 |                          | ✓     |
|         | View information section       |                          | ✓     |
|         | Import entries                 |                          | ✓     |
|         | Export entries                 |                          | ✓     |
|         | Allow add entry in root folder |                          | ✓     |

*My Data Source Information – Entries*

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

| OPTION                                      | DESCRIPTION   |
|---|---|
| <b>View information section</b>             | Indicates if the user can view the information section of entries.          |
| <b>Import and Export entries</b>            | Indicates if the user has the privilege to import or export entries.        |
| <b>Allow add entry in vault root folder</b> | Indicates if the user can add entries in the vault root of the data source. |

## SECURITY GROUPS

The **Security Groups** are now a Legacy setting. We strongly recommend using roles instead.

## ROLES

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



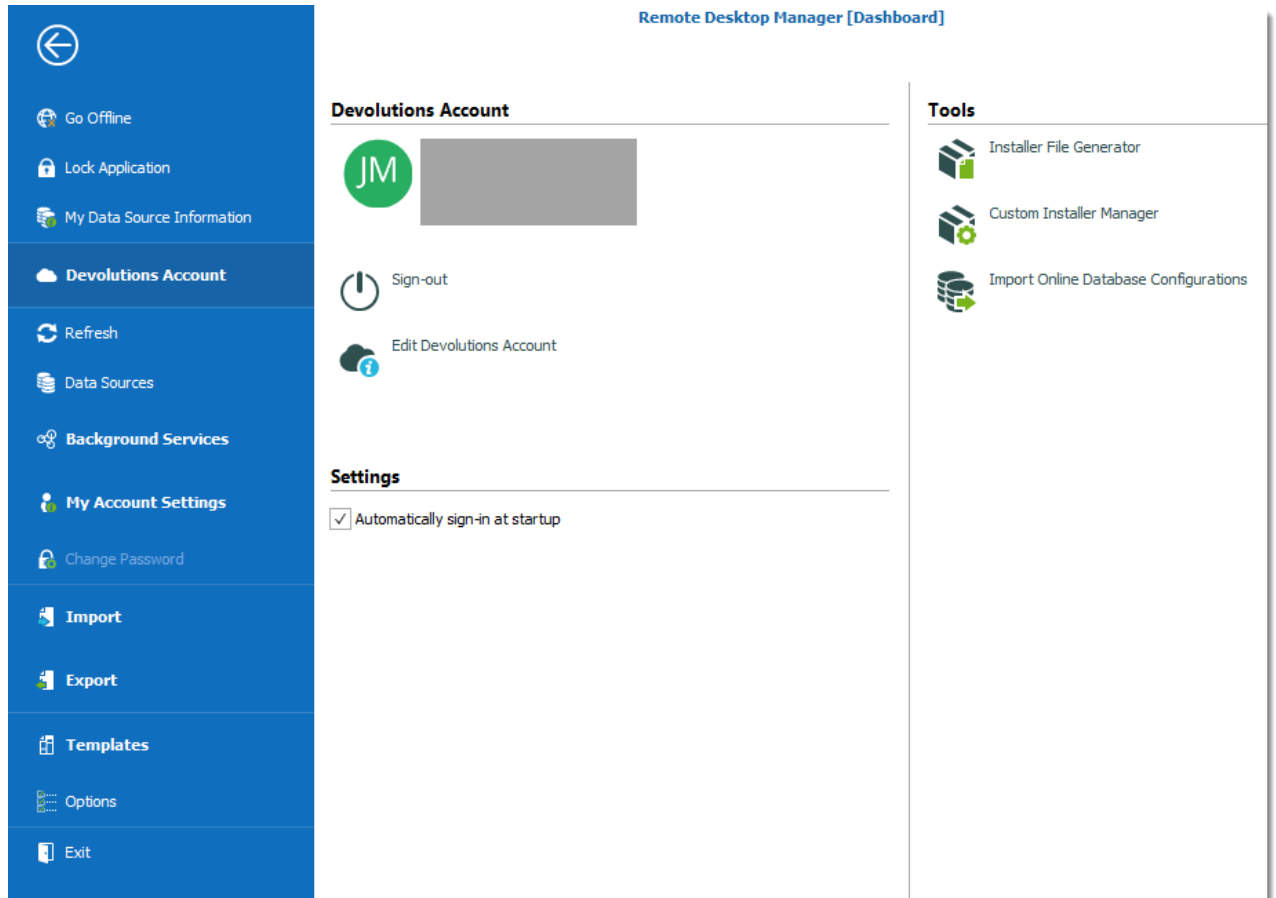
This feature is only available with an [SQL Server/SQL Azure](#) and a [Devolutions Password Server \(DPS\)](#) data source.

### 6.2.3 Devolutions Account

## DESCRIPTION

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

## SETTINGS



Devolutions Account

## DEVOLUTIONS ACCOUNT

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

## SETTINGS

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

## TOOLS

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

### 6.2.4 Backup

#### DESCRIPTION

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

#### 6.2.4.1 Settings

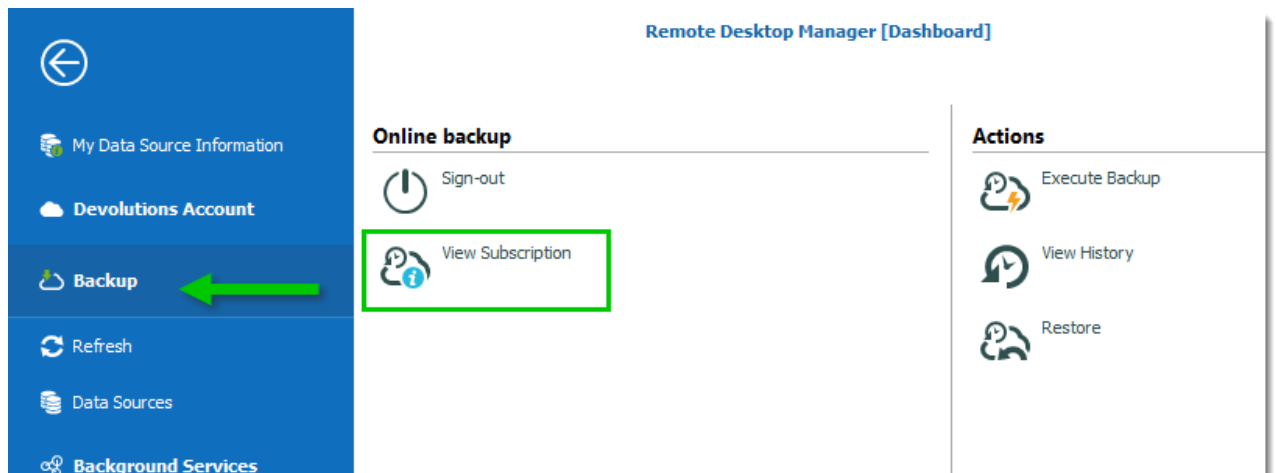
#### DESCRIPTION



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

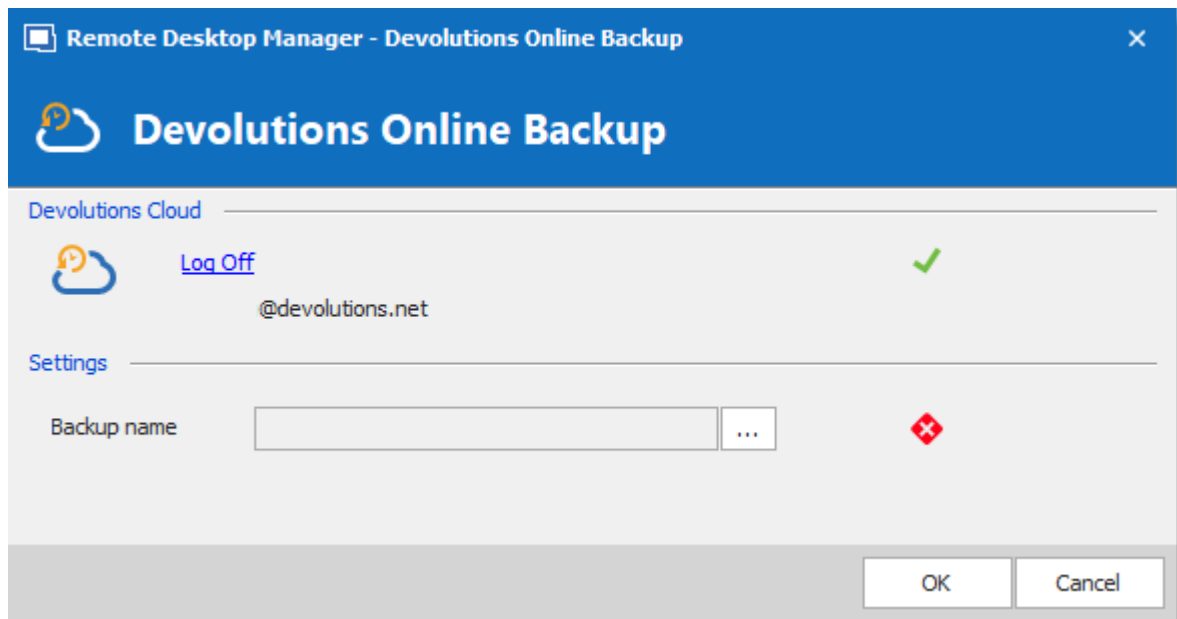
## SETTINGS

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



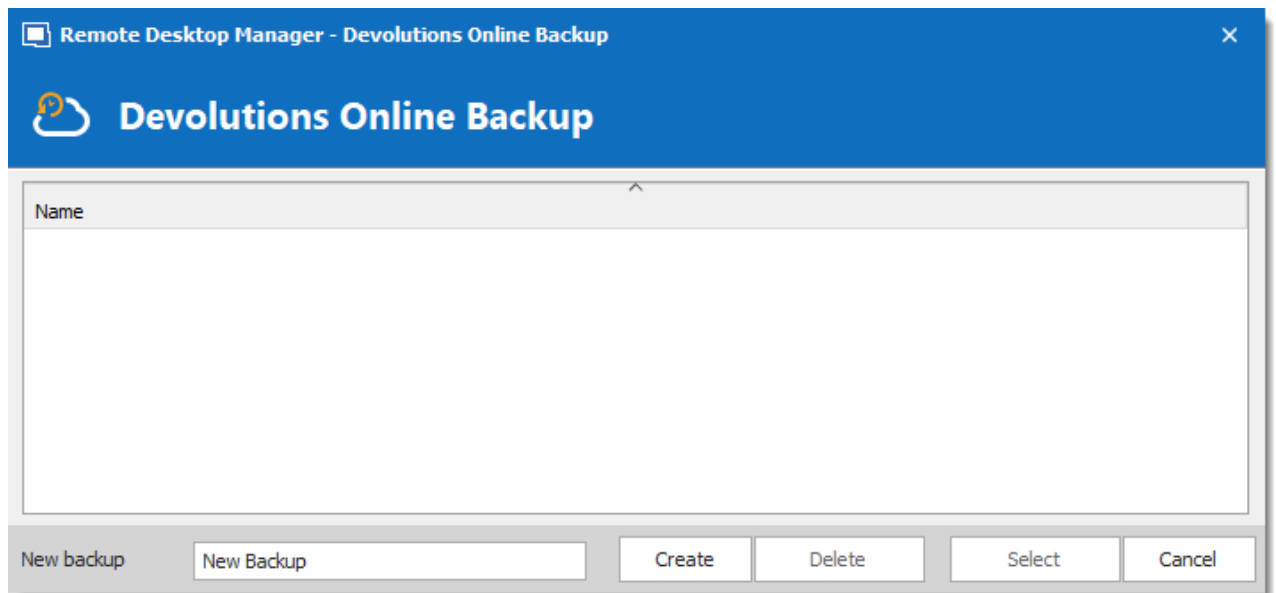
Online Backup - View Subscription

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



Backup Name

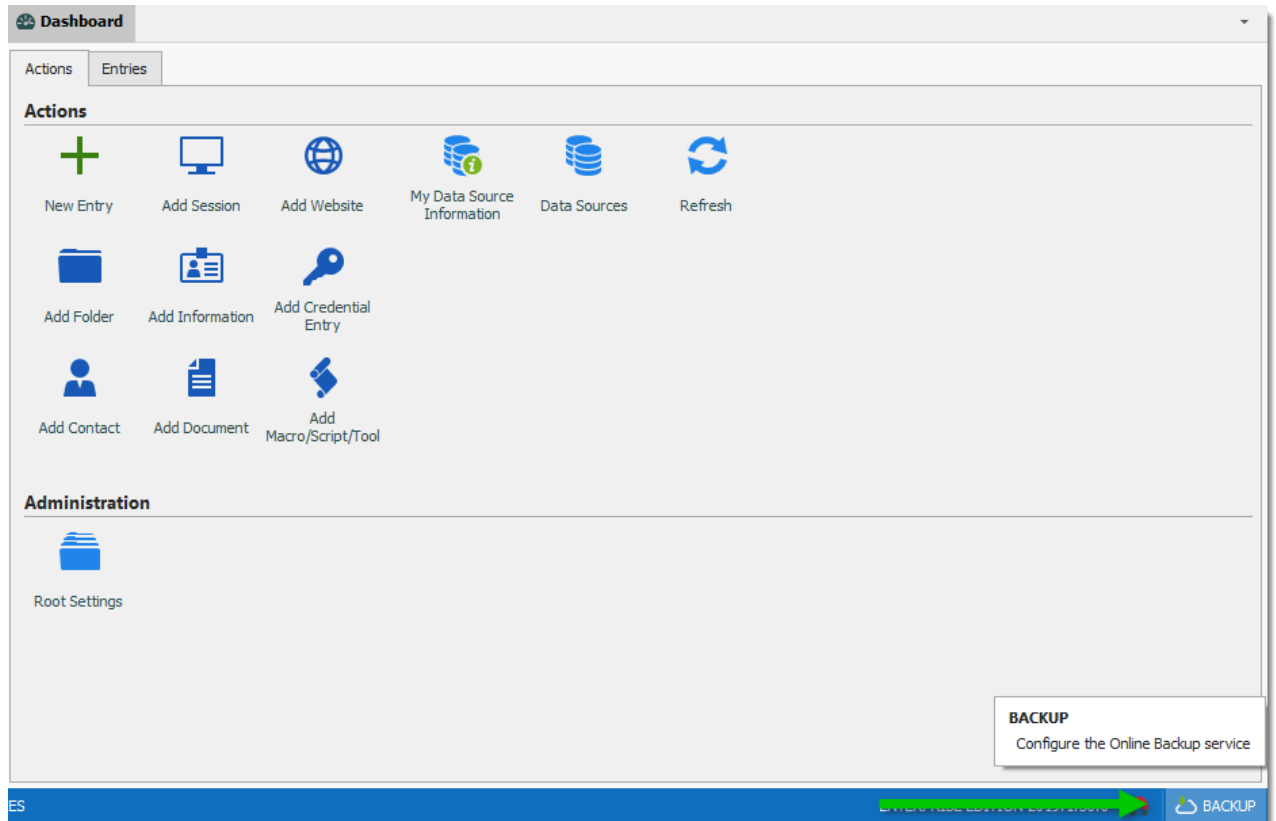
4. You will need to specify a unique backup name in the field **New backup** for each of your data source which will then be used to backup and restore the data source. Click on **Create** to automatically create your Online Backup.



*Create Backup*

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

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



*Online Backup Activated*



You must perform this for all your [Devolutions Online Drive](#), [SQLite](#), [XML](#) or Microsoft Access data sources in order to be fully protected!



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

#### 6.2.4.2 Restore

### DESCRIPTION

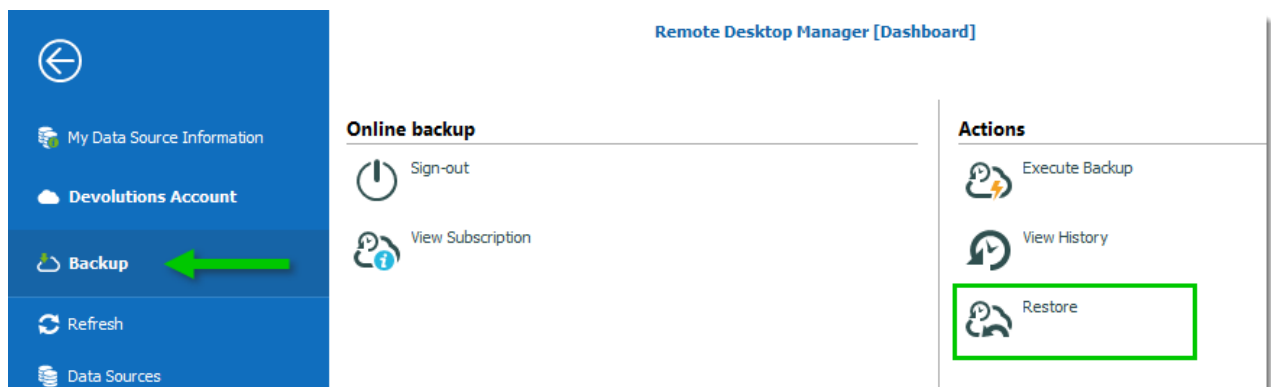


Before being able to restore a backup, you **MUST** create an empty data source and define the backup name before being able to use it. You need to create a new SQLite, XML, Online Drive or Microsoft Access data source in **File – Data Sources**.

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

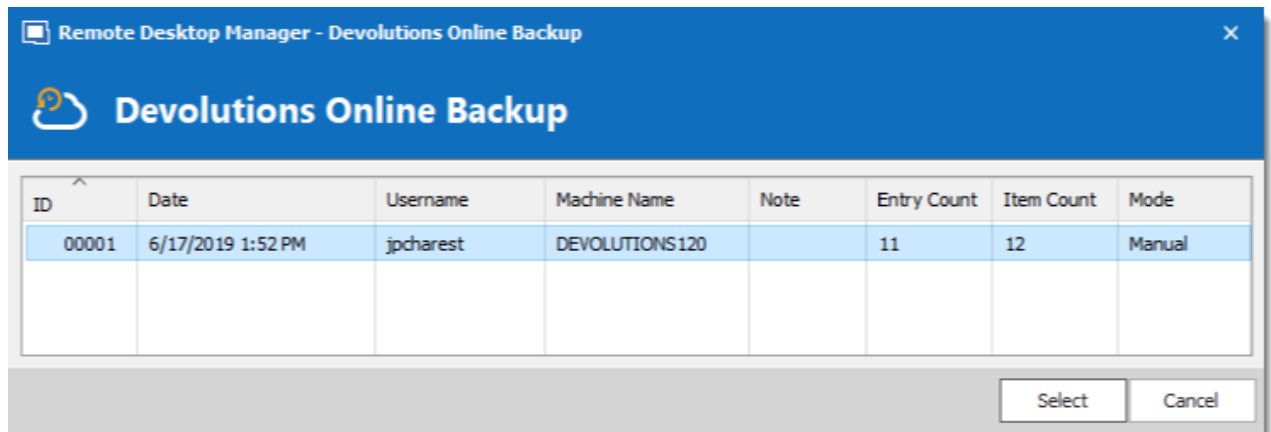
## SETTINGS

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



*Backup Restore*

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



*Select your Backup*

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

The screenshot shows the 'Restore source' dialog box. It has a blue header with the Devolutions Online Backup logo and title. Below the header, the dialog is titled 'Restore source'. It contains a list of fields: ID (00001), Date (6/17/2019 1:52 PM), Username (jpcharest), Machine name (DEVOLUTIONS120), Entry count (11), Item count (12), Mode (Manual), and Note. At the bottom, there are four buttons: Previous, Next, Finish, and Cancel.

|              |                   |
|--------------|-------------------|
| ID           | 00001             |
| Date         | 6/17/2019 1:52 PM |
| Username     | jpcharest         |
| Machine name | DEVOLUTIONS120    |
| Entry count  | 11                |
| Item count   | 12                |
| Mode         | Manual            |
| Note         |                   |

*Backup Wizard*

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

The screenshot shows the 'Restore destination' dialog box. It has a blue header with the Devolutions Online Backup logo and title. Below the header, the dialog is titled 'Restore destination'. It contains three radio button options: 'Current data source' (selected), 'Add a new data source' (with a text field for 'Name'), and 'File with encryption' (with a text field for 'Master key'). There is also a checkbox labeled 'Perform a data source backup before restoring the selected backup' which is checked. At the bottom, there are four buttons: Previous, Next, Finish, and Cancel.

*Restore Destination*

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

## 6.2.5 Refresh

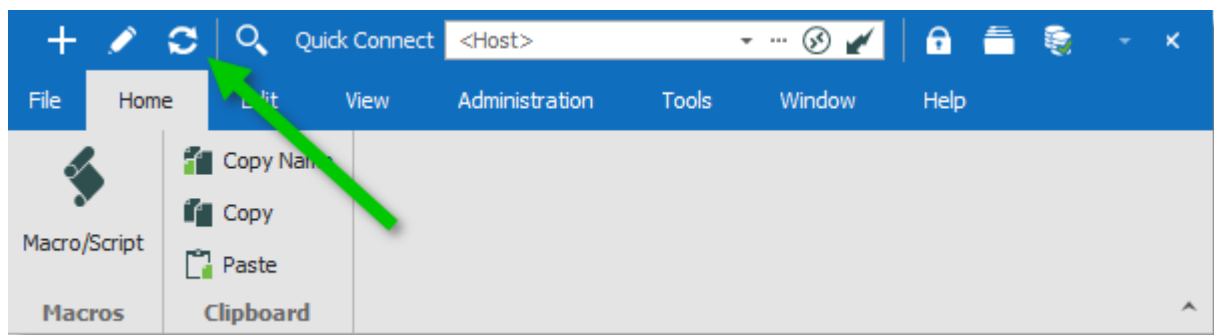
### DESCRIPTION

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

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


### SIMPLE REFRESH

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



*Refresh the Data Source*

### LOCAL CACHE REFRESH

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

## 6.2.6 Change Master Key

### DESCRIPTION

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

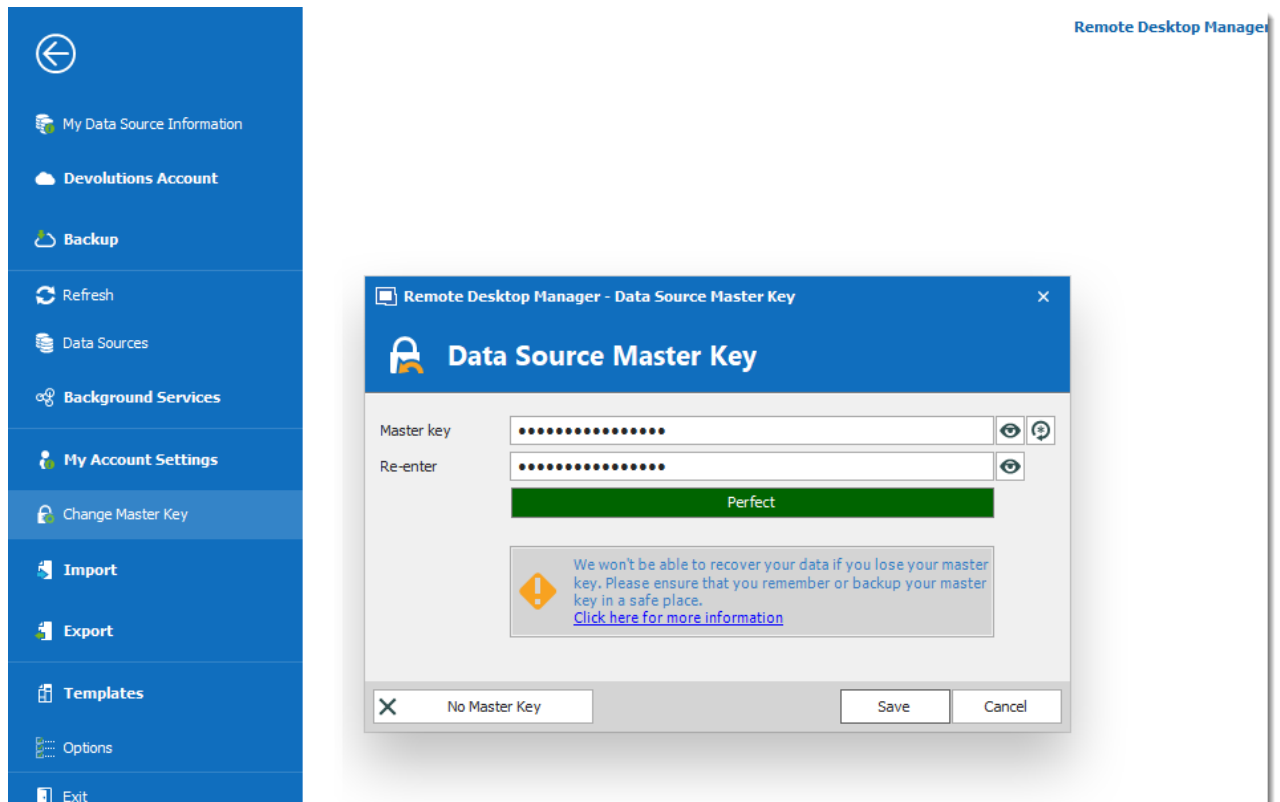
The master key prevents unauthorized users to access the data source without knowing the master key. It is highly recommended to apply a master key to the data source if you're using Remote Desktop Manager in a portable environment (i.e. USB Flash Drive, USB Hard Drive).

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

- Devolutions Online Drive
- Dropbox
- FTP
- Google Drive
- WebDAV
- XML



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



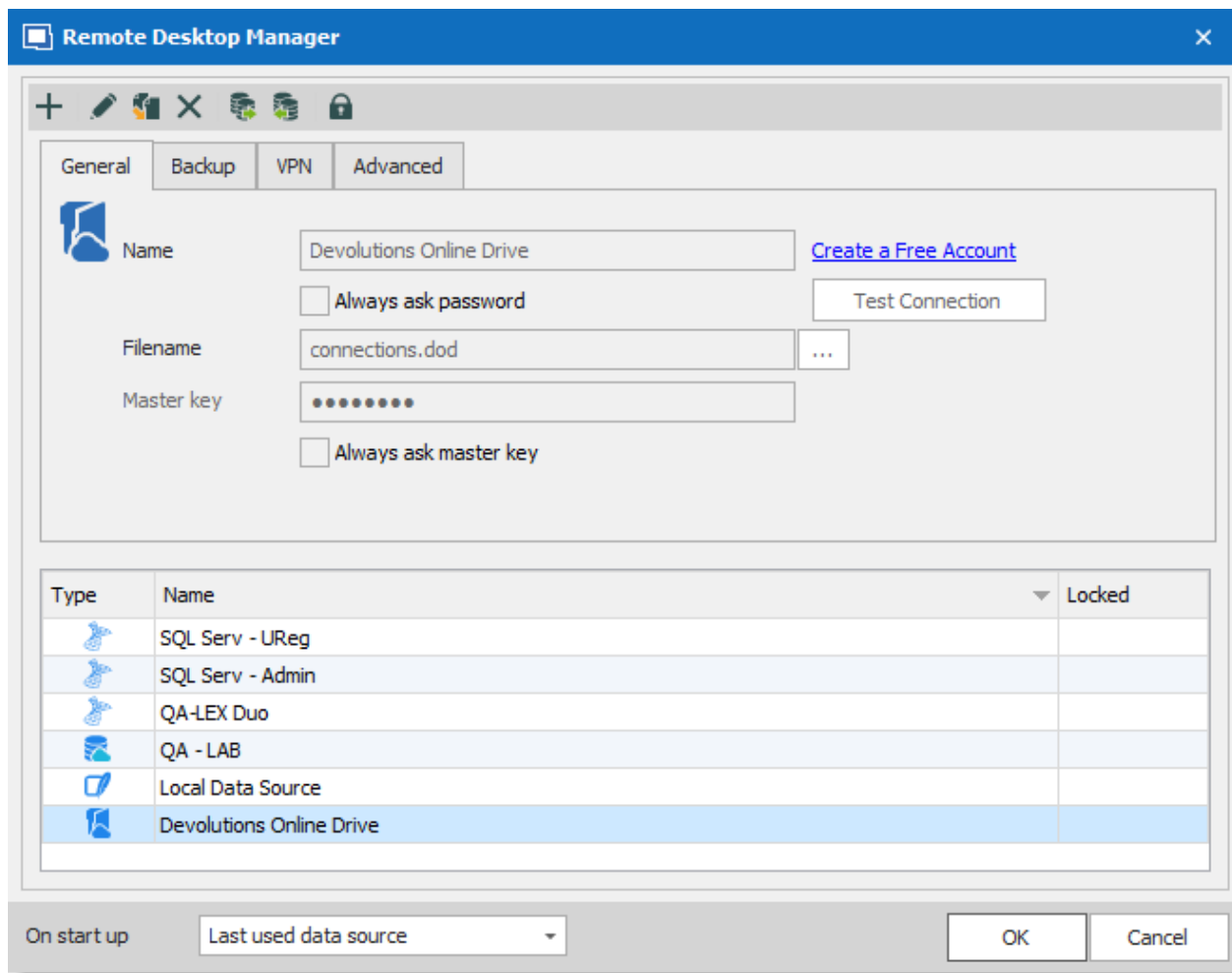
*Change Master Key*

## 6.2.7 Data Sources

### DESCRIPTION

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

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



*Data Sources*




## SETTINGS

### ADD A NEW DATA SOURCE

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





## EDIT/DUPLICATE/DELETE DATA SOURCE

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




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


## IMPORT/EXPORT DATA SOURCE CONFIGURATION

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

## LOCK DATA SOURCE

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

## UNLOCK DATA SOURCE

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

## ON START UP

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

| OPTION                         | DESCRIPTION   |
|--------------------------------|---|
| <b>Use default data source</b> | Set the data source that you always want to open at start up. |

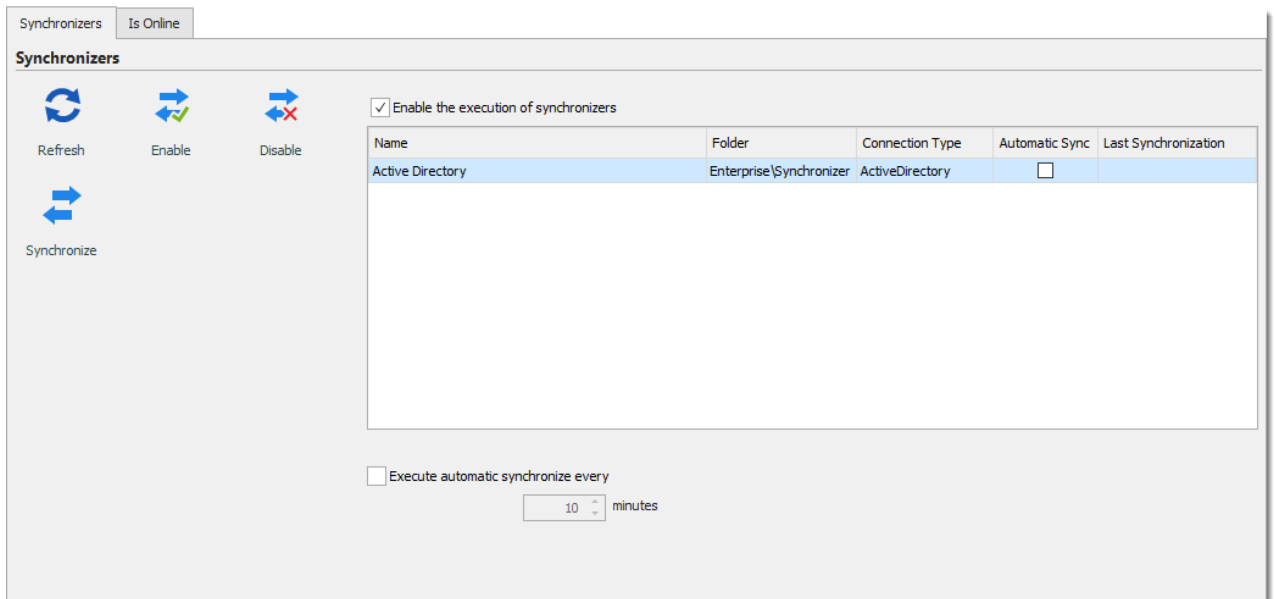
| OPTION                        | DESCRIPTION   |
|-------------------------------|---|
| <b>Last used data source</b>  | Open with the last used data source.                              |
| <b>Prompt for data source</b> | A message box will open on startup for the data source selection. |

## 6.2.8 Background Services

### SYNCHRONIZERS

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

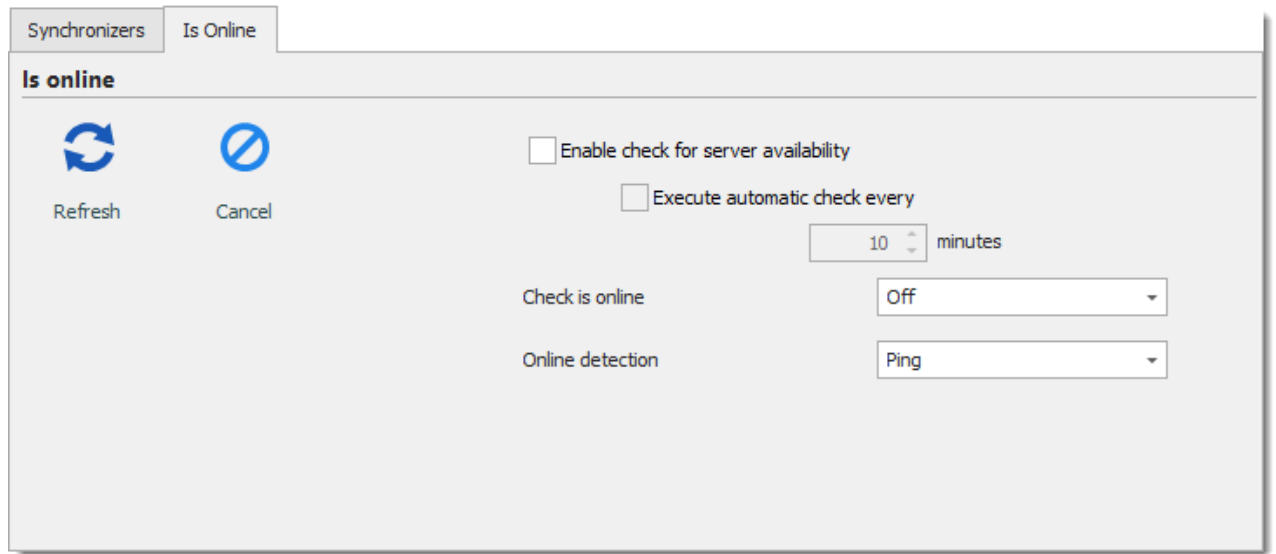
When experiencing a performance degradation with Remote Desktop Manager you will be able to verify if a synchronizer is running in the background causing the system to slow down.



*Synchronizers*

### IS ONLINE

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

*Is Online*

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

### 6.2.9 Import

## DESCRIPTION

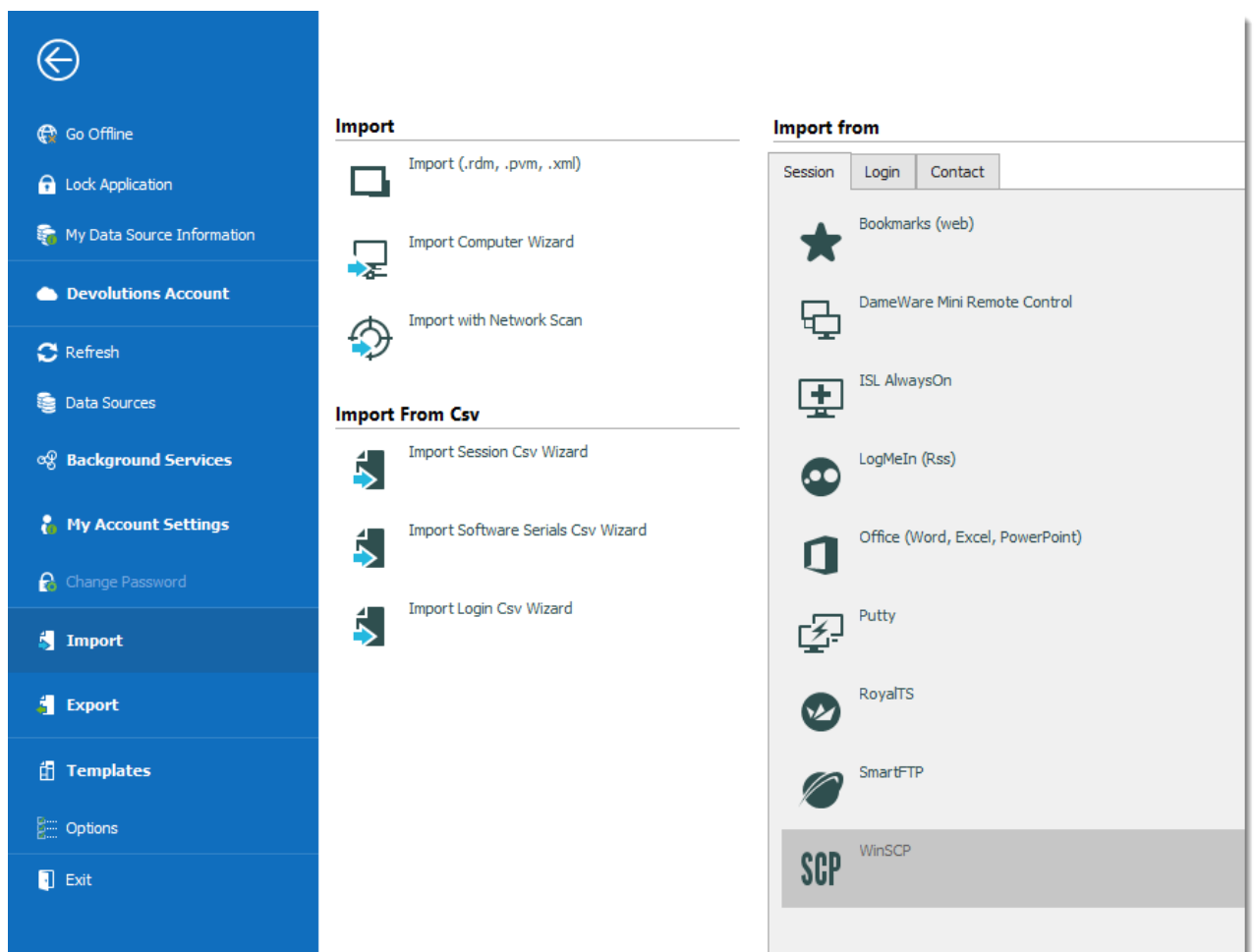
Use the **File – Import** to import entries in Remote Desktop Manager. You can import entry types from multiple sources.

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



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

## SETTINGS



*File - Import*

## IMPORT ENTRIES

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

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

## IMPORT COMPUTER WIZARD



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

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

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

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

## IMPORT WITH NETWORK SCAN

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

## IMPORTING FROM CSV FILES

Three wizards are available to import content from csv files:

- Import Session
- Import Software Serials
- Import Login

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

## IMPORT FROM

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

- [Import Sessions](#)
- [Import Logins](#)
- [Import Contacts](#)

### 6.2.9.1 Import Computer Wizard

## DESCRIPTION



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

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

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

## OVERVIEW

The wizard has a few major-steps:

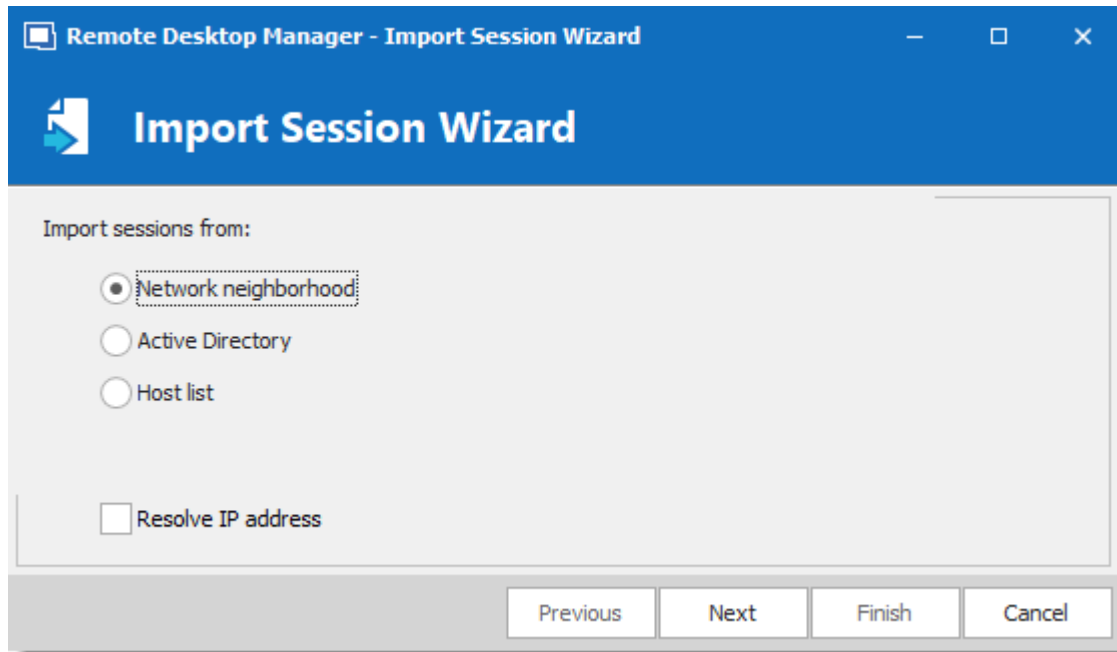
1. select computers by using one of the three sources;
2. optionally apply a template from which to base new sessions on; and
3. optionally edit each newly created session prior to them being saved.

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

## WORKFLOW

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

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

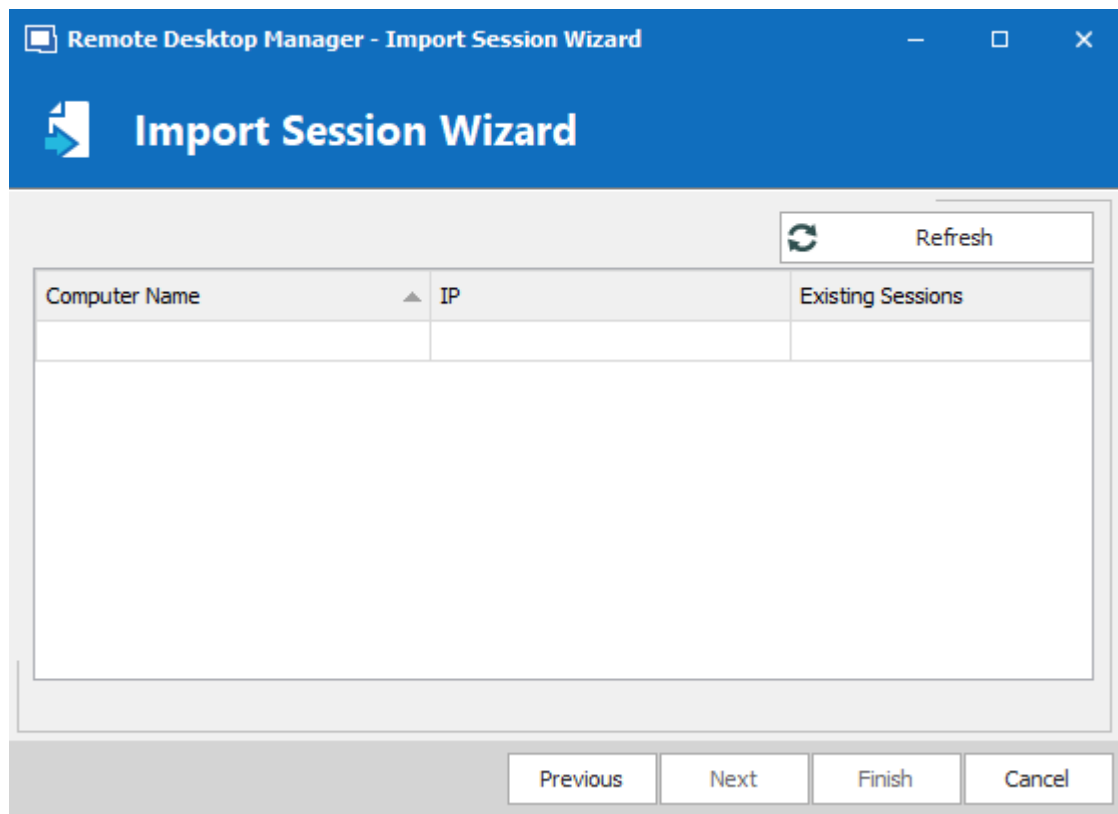


*Import Session Wizard*

Refer to the sections below depending on the chosen source.

## NETWORK NEIGHBORHOOD

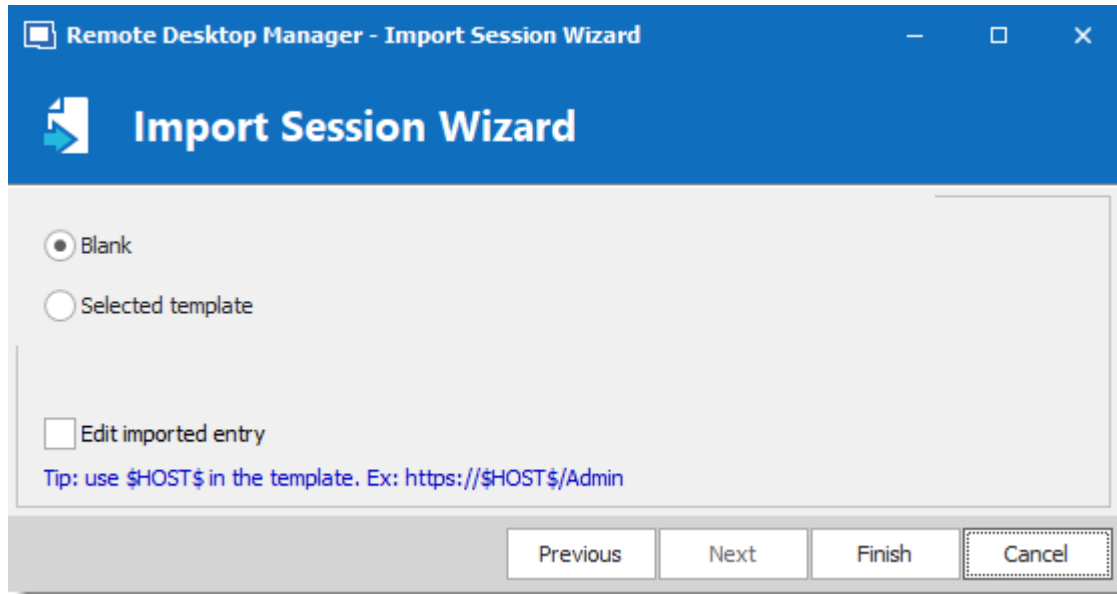
The next screen will immediately be populated with the result of the network discovery.



*Import Session Wizard - Network Neighborhood*

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

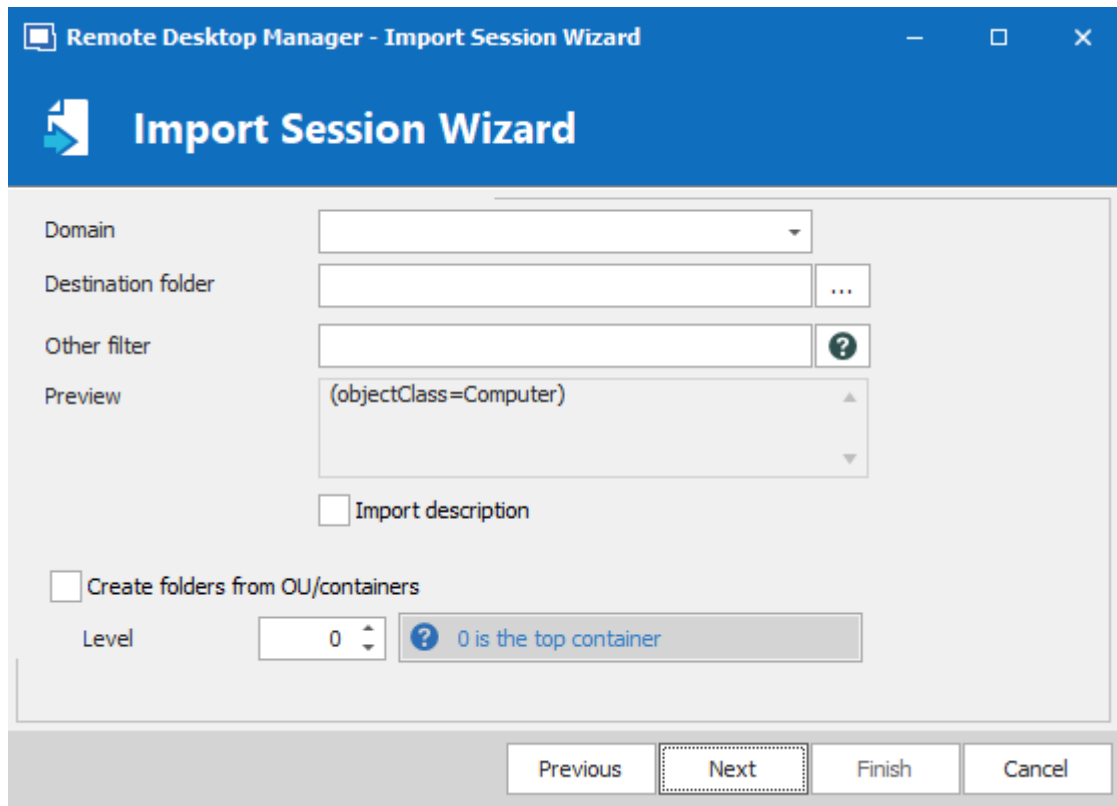




*Import Session Wizard - Template*

## ACTIVE DIRECTORY

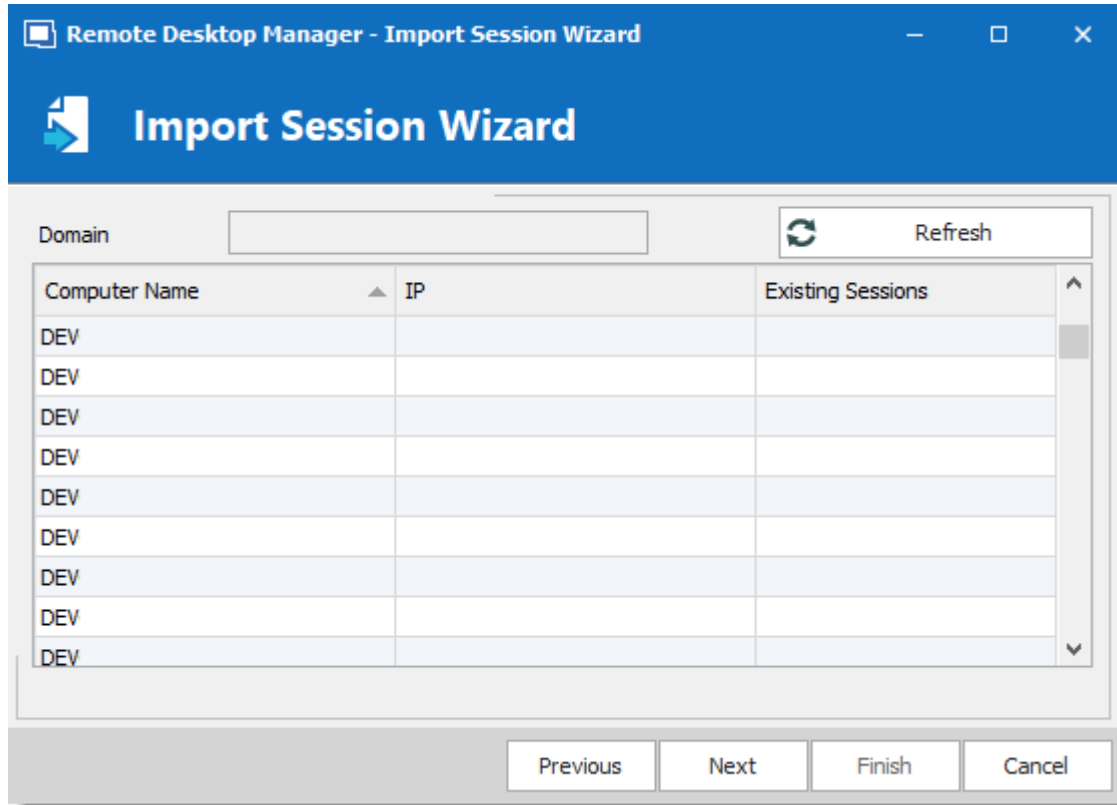
The following screen allows you to select the domain to interrogate after which you must press refresh to load the list of computers that are available.



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

*Import Session Wizard - Active Directory*

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

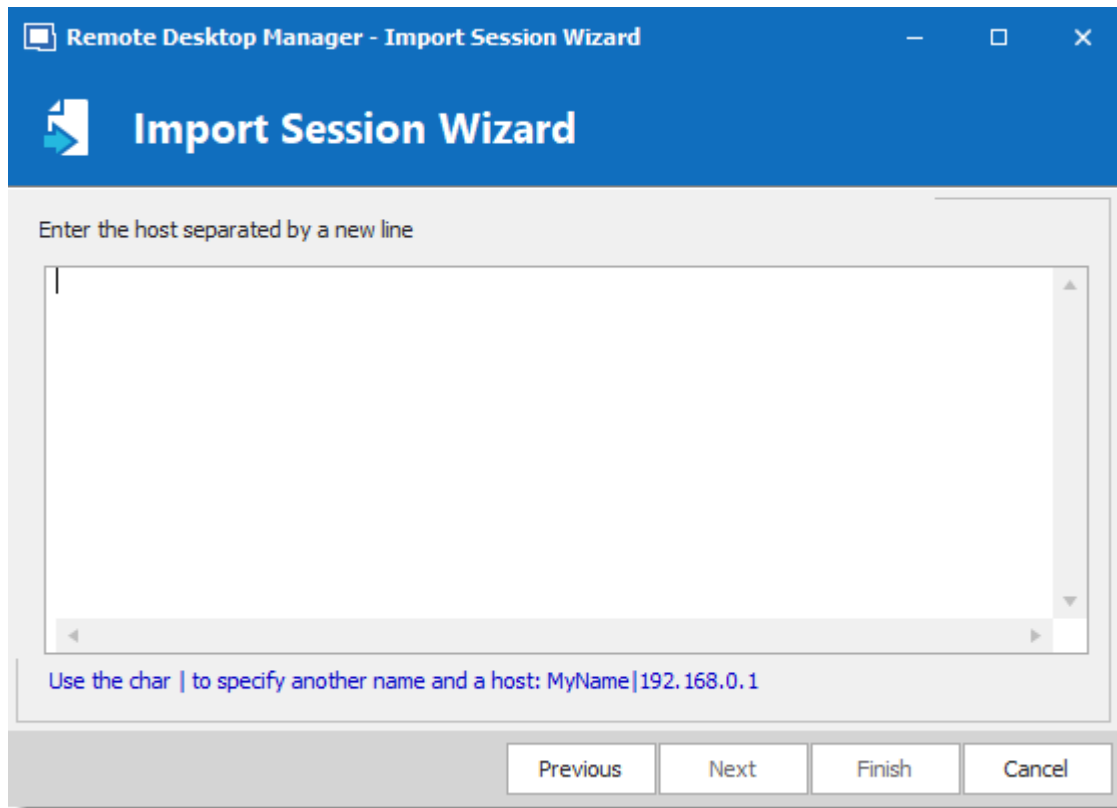


*Import Session Wizard - Domain list*

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

## HOST LIST

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



*Import Session Wizard - Host List*

Proceed to Template Selection below.

## TEMPLATE SELECTION

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

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

### 6.2.9.2 Import Session CSV Wizard

## DESCRIPTION

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

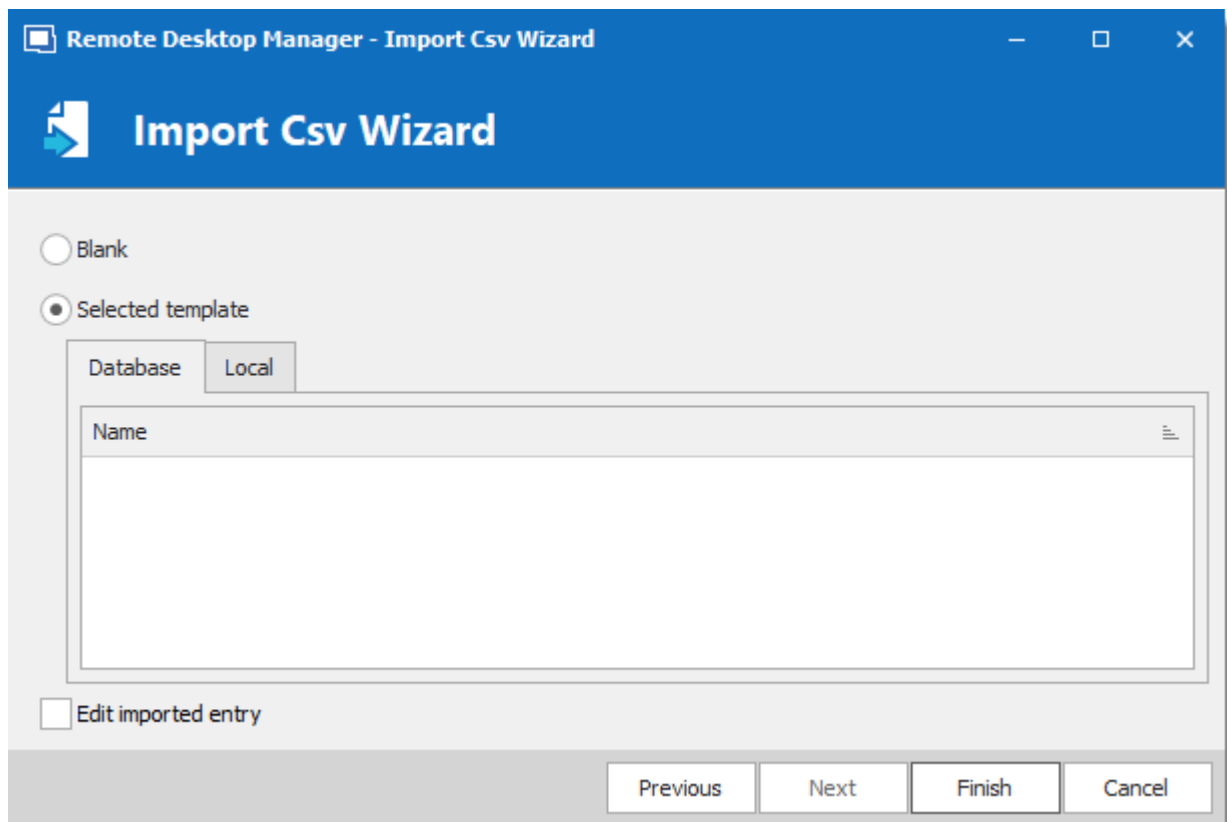


For a discussion on the CSV file format, and the impact of decisions made in this entry, please consult [Import Strategies and file format](#)

## SETTINGS

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

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



*Import Csv Wizard*

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

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

## DESCRIPTION

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

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

If you need finer control, you can specify the template to use in a **Template** column of the CSV file. But since you're able to specify the entry type from within the CSV file it may not be necessary. Please consult [CSV Samples](#) below.

## COLUMNS



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

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

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



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



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

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



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

Here is a list of some relevant fields.

| OPTION                 | DESCRIPTION   |
|------------------------|---|
| <b>Host</b>            | Host name of the device, <b>this is the only mandatory field</b> .  |
| <b>Name</b>            | Name of the entry   |
| <b>ConnectionType</b>  | Token representing the connection type. It is best to use the <b>Clipboard-Copy</b> method to obtain the acceptable values.   |
| <b>Group</b>           | Destination folder. Note that if the import process itself had a Destination Folder defined as well, the folder listed here would be created below the one from the process.  |
| <b>Description</b>     | Description of the entry.   |
| <b>Open (Embedded)</b> | Boolean value ( <b>true</b> or <b>false</b> ) that indicates to open the session embedded. The default value is false, meaning that the native client will be used depending on the technology. MSTSC.EXE for instance. |
| <b>Username</b>        | Username used to open a session to the device.  |
| <b>Domain</b>          | Domain used to open a session to the device.  |
| <b>Password</b>        | Password used to open a session to the device. Please note that this field is encrypted and stored into another field upon being imported.  |

| OPTION                               | DESCRIPTION  |
|--------------------------------------|--|
| <b>MetalInformation\SerialNumber</b> | Serial Number of the device.                       |
| <b>MetalInformation\ServiceTag</b>   | Service Tag of the device                          |
| <b>MetalInformation\PurchaseDate</b> | Purchase date in a ISO8601 format, i.e. yyyy-mm-dd |

## CSV SAMPLES

### WITH SPECIFIED SESSION TYPES

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

#### 6.2.9.3 Import Network Scan

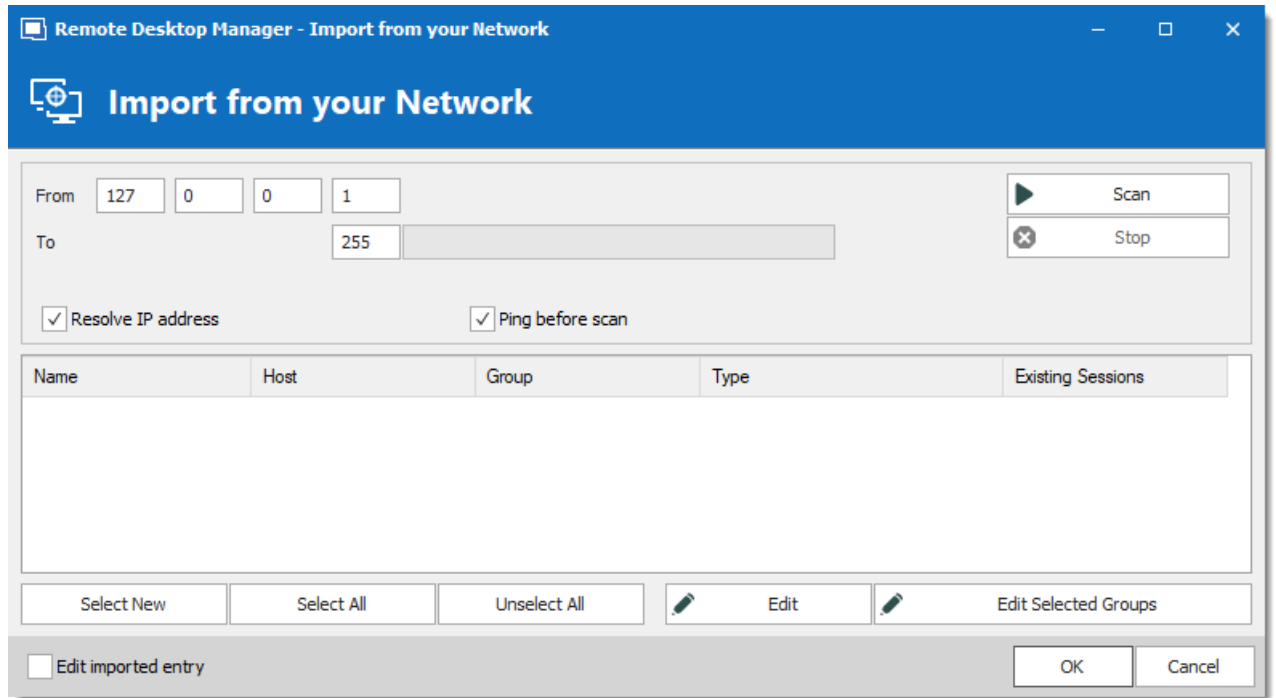
### DESCRIPTION

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

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

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





*Import from your Network*

#### 6.2.9.4 Import Sessions

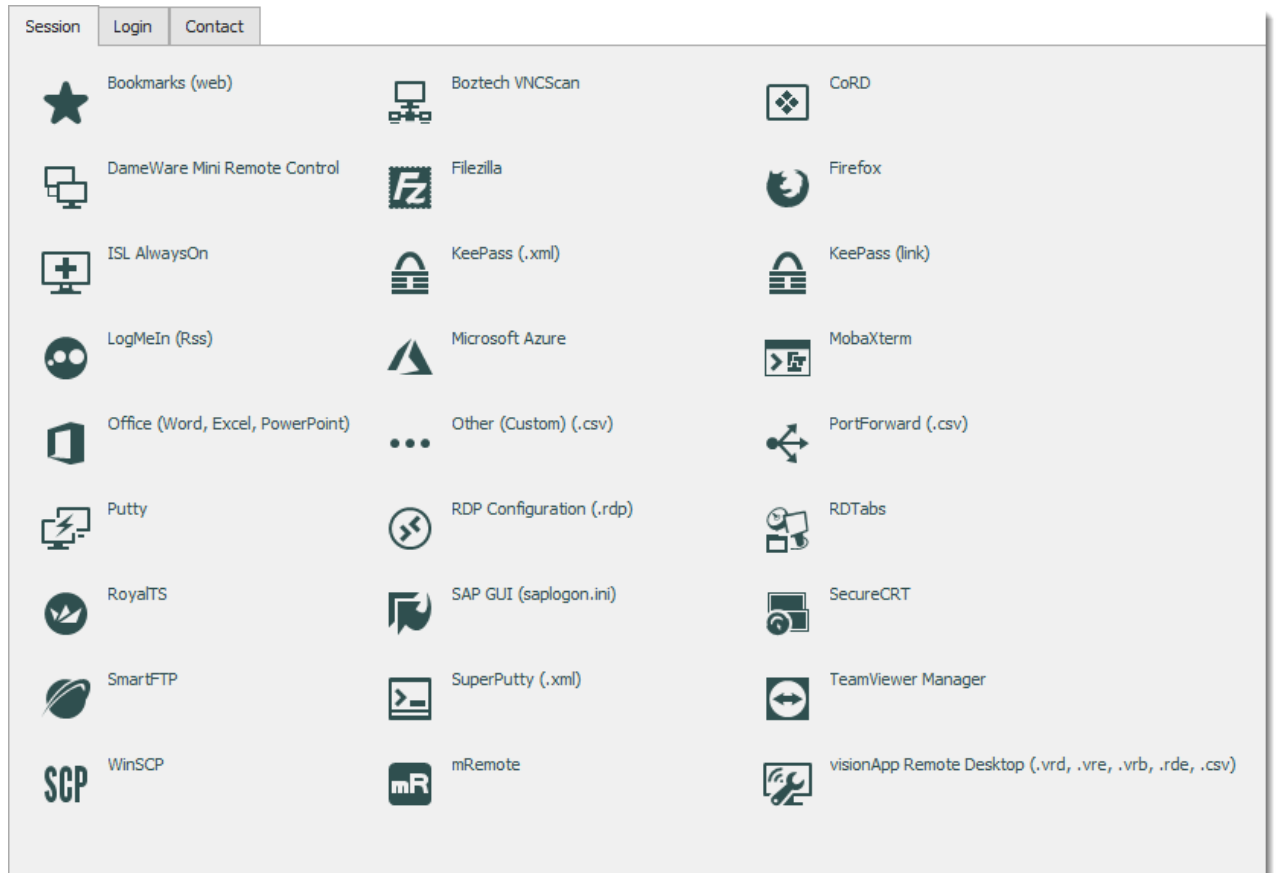
### DESCRIPTION

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



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

### SETTINGS



*Import from Session*

## IMPORT FROM SESSION

You can import your sessions from an existing application or an existing file format. Some application encrypt the data but it must be in plain text to allow the application to parse the content. Please note that all entries will be imported in the current folder. For some applications it's not possible to extract the password.

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

### 6.2.9.5 Import Logins

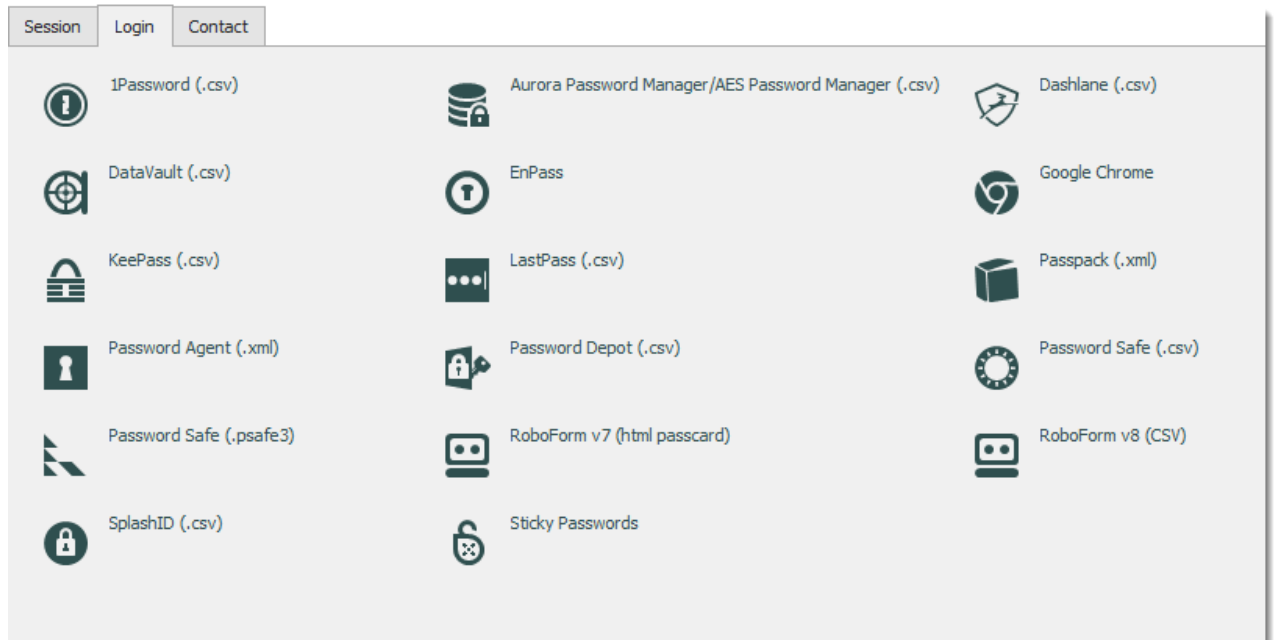
## DESCRIPTION

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



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

## SETTINGS



*Import from Login*

## IMPORT FROM LOGIN

You can import the credentials from a wide array of formats exported by various password management solutions. The export content must not be encrypted in order to parse the content. Please note that all the entries will be imported in the current folder. We support a multitude of Login imports, explore to your heart's content!

### 6.2.9.6 Import Contacts

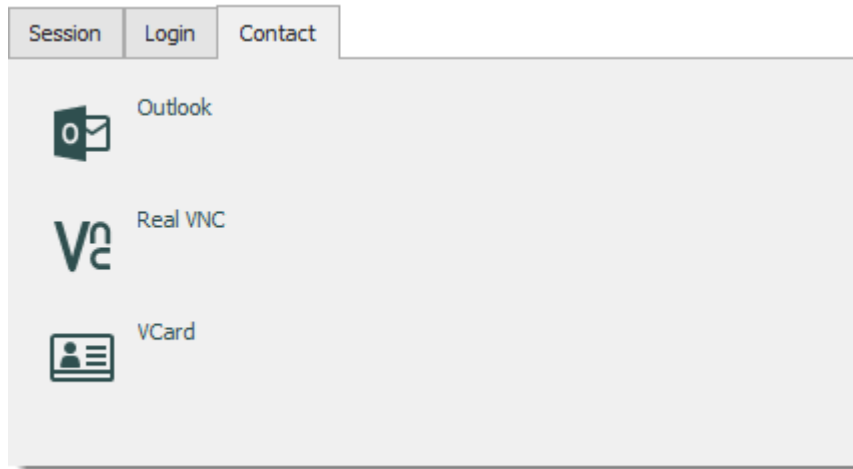
## DESCRIPTION

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



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

## SETTINGS



*Import Contact menu*

## IMPORT FROM CONTACT

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

- Microsoft Outlook
- Real VNC
- VCard

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



Microsoft Outlook contacts sub-folders are also supported.

## 6.2.10 Export

### DESCRIPTION

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

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



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

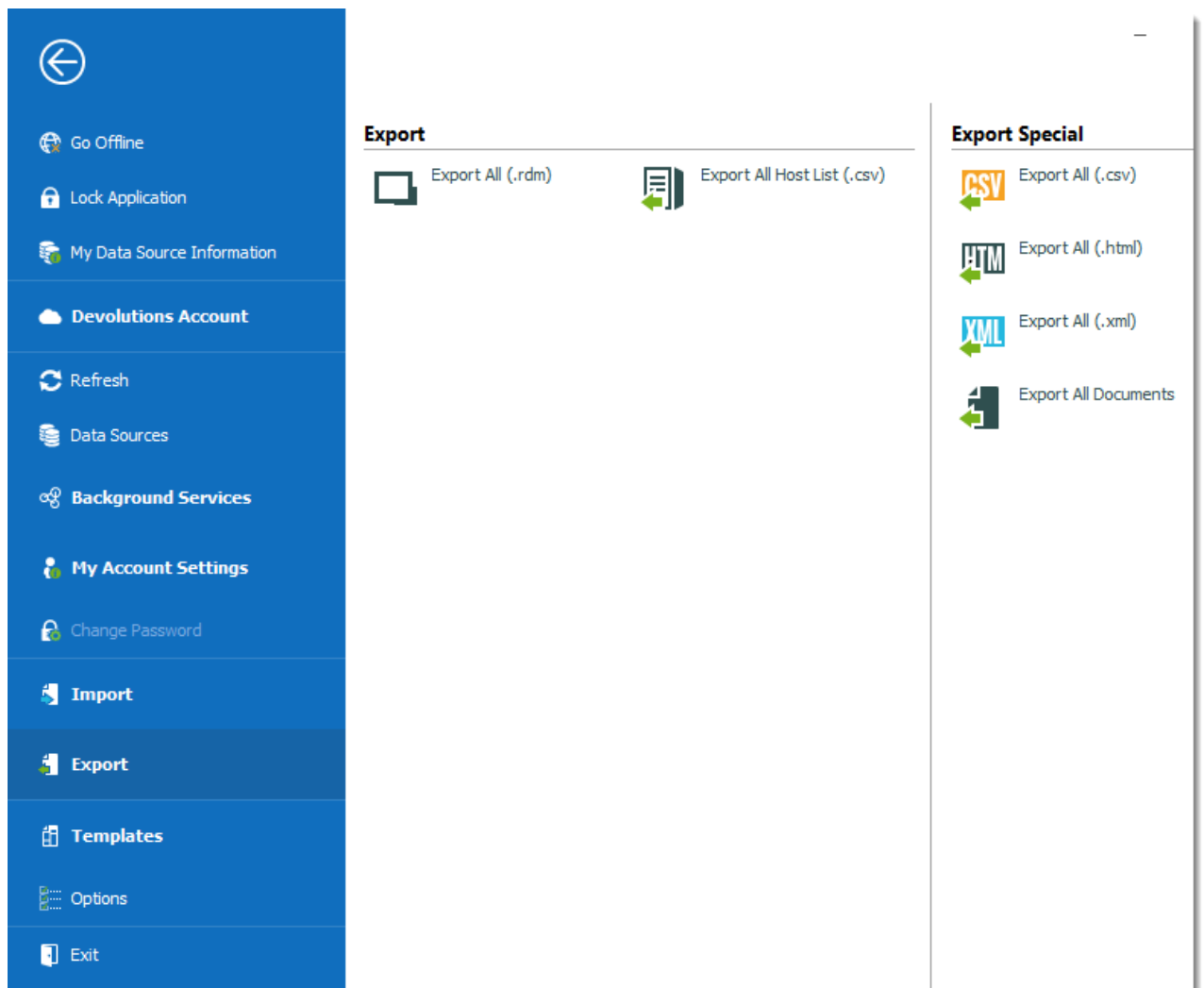


The export feature is only active if the import Permission has been enabled inside the user account.



The only appropriate format to import the entries back into Remote Desktop Manager is the .rdm format.

### SETTINGS

*File - Export*

When using an [Advanced Data Source](#), export capabilities can be disabled via security policies at the data source level (no one can export) or at a user level (particular users can't export). See Security Group Management for more information.

## EXPORT ALL ENTRIES (.RDM)

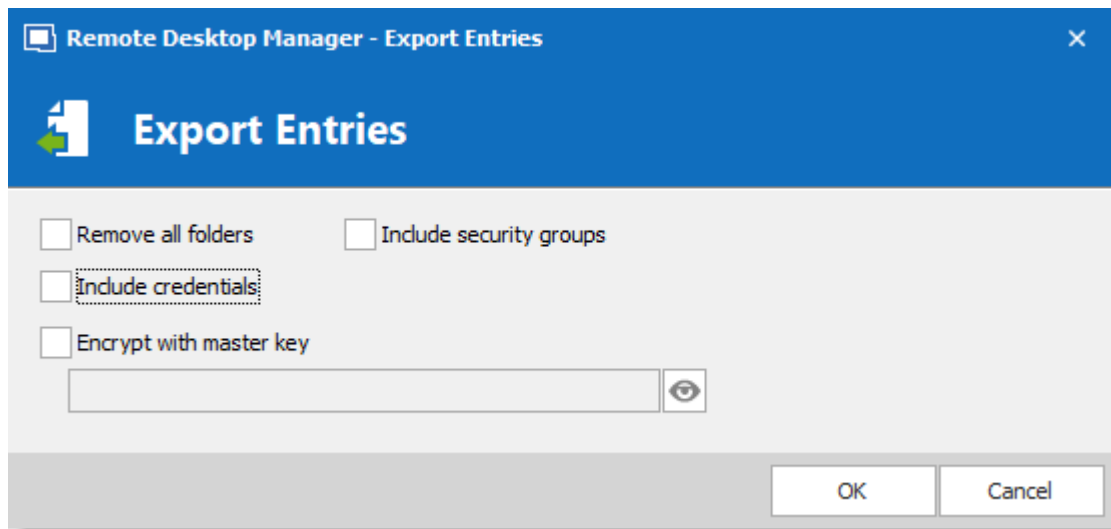
Export all entries in a .rdm file that can be imported into any Remote Desktop Manager data source. You can also include credentials in this export format and secure your file with a master key.



By default the credentials are NOT included. It's critical to check the **Credentials** option in order for the exported data to include the credentials.



Specifying a master key will encrypt the whole content of the .rdm file to protect its content. It is highly recommended as a backup measure, but the key is absolutely necessary for decryption. Preserve this as well in a separate storage device for safekeeping.



*Export entries in .rdm*

## EXPORT ALL HOST LIST (.CSV)

Export a simple host list in .csv format. You will be prompted to see if you wish the export to be slightly more detailed and include the following information: Host, Description, Display Name, Group, Security Group.

## EXPORT ALL ENTRIES (.CSV)

Export all entries using the .csv format file. For security reasons the .csv file will be contained within a password encrypted zip file. This type of security can be hacked using brute force attacks, it should be used only when the zip file is under your exclusive control.



Please note that the csv columns will vary depending on entry types being exported. This makes it the wrong format if ever you want to import the data back in Remote Desktop Manager. Use this only to migrate to another system.

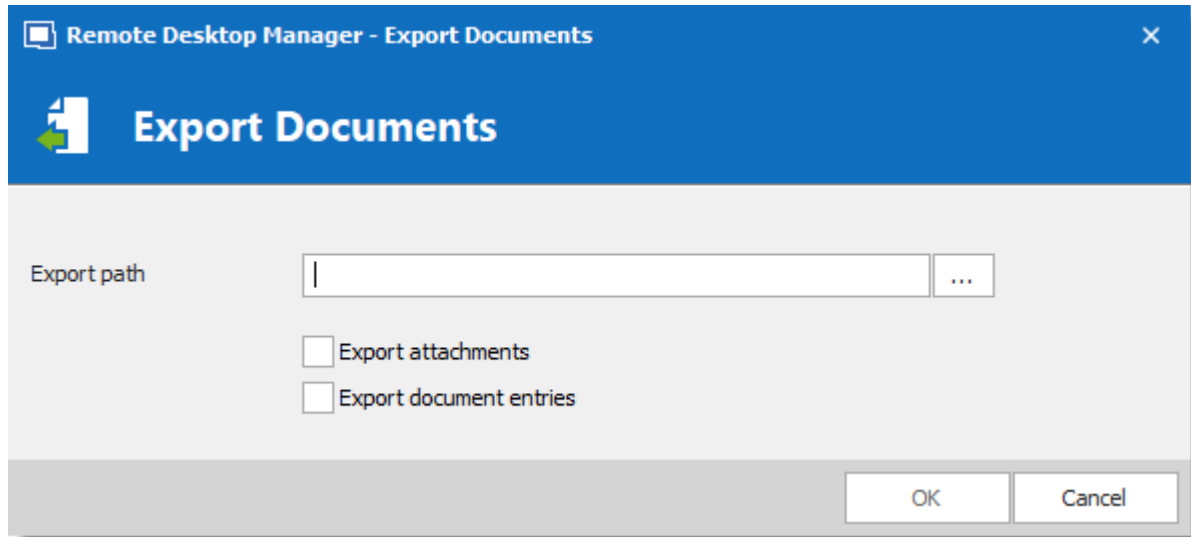
## EXPORT ALL ENTRIES (.HTML)

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

## EXPORT ALL ENTRIES (.XML)

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

## EXPORT ALL DOCUMENTS



*Export Documents*

Export all attachments or all document entries that are linked to your data source.

### 6.2.10.1 Encrypted Html

## DESCRIPTION



The Html Encrypted export format was designed for simple and secure exports of entries. It allows for an html export of the entry information while using symmetric encryption (AES-256) to encrypt sensitive information such as passwords. The file is an ultra portable self contained html file that requires no external script files or installs. As long as you have a web browser with JavaScript enabled you can get to your encrypted data.



With a secure encrypted document you can freely send the information via email or any other protocol without compromising the sensitive data. Use the export as means of sharing or as a backup for sensitive information.

## SETTINGS

Select the entries to export or export all entries. **Right-click** and select **Export – Export Special – Export All Entries (.html)** or use **File – Export – Export All Entries (.html)**. You will be prompted for a password for the symmetric encryption key. Select the file name for the new document. Once the export is completed the file will open in your default browser.



Ensure you do not forget the password as you will not be able to decrypt the data without it.

When exporting multiple entries that are all contained within the same file, at decrypt time, each encrypted value must be decrypted individually for security reasons. Once you're done with the sensitive data simply hit **F5** to refresh the file or simply close it. Your data is now safe from prying eyes.

## AES-256

We use AES-256 to encrypt/decrypt your sensitive data. Since the decryption is done entirely in the browser, there's no need for external tools, downloads or installs.

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

*Encrypted Value*

## SAFE & SMART VIRTUAL BACKUP

In addition, HTML Export using symmetric encryption is a great way to securely backup your passwords and other sensitive information. It allows you to share information via email or simply send the file to your personal email account as a backup.

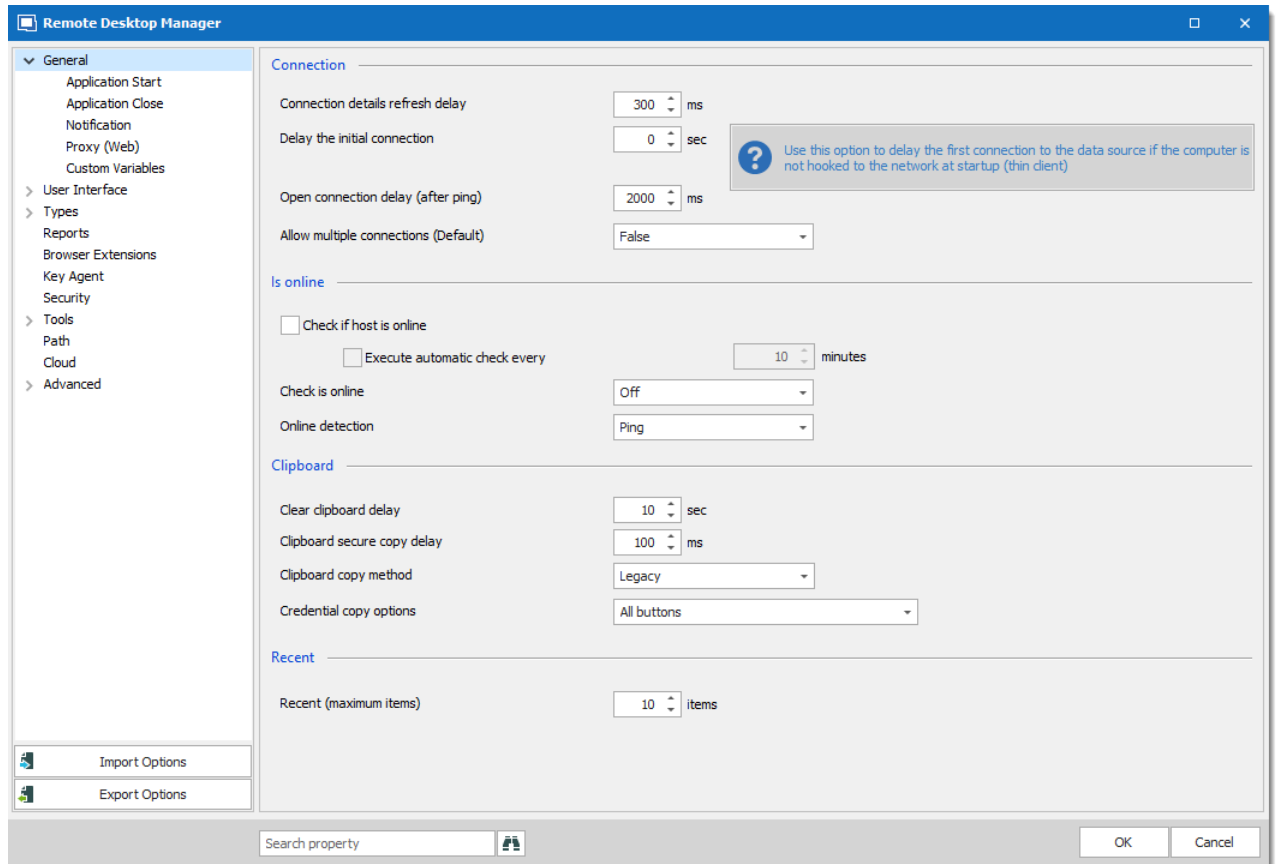
### 6.2.11 Options

#### DESCRIPTION

There are multiple options available to manage and customize your Remote Desktop Manager in the menu **File – Options**. Most of these options are related to changes to the local instance.

Use the **Search property** to find a specific option.





File - Options

Options you configure:

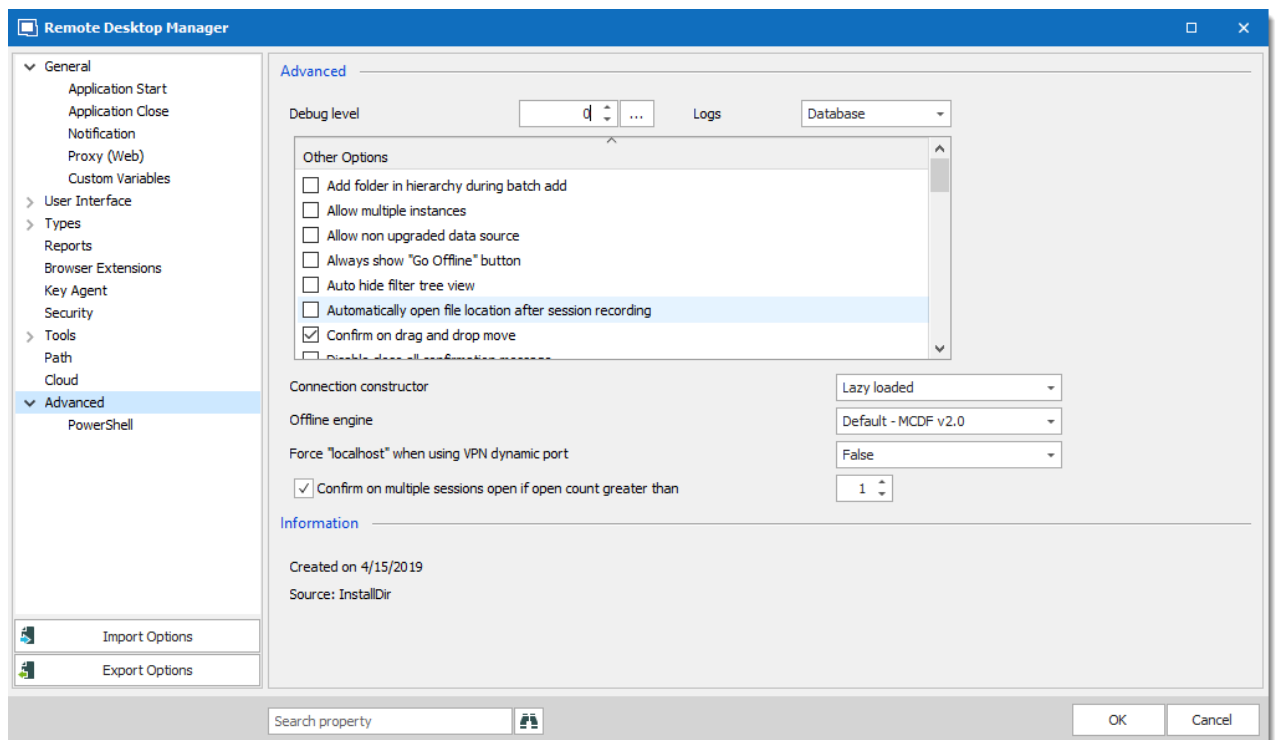
- **General:** Application Start (including update options), Application Close, Notification, Proxy (Web), Custom Variables
- **User Interface**
- **Types:** Settings for different types of entry, terminal, ssh keys, etc.
- **Reports**
- **Browser Extensions:** Settings for Devolutions Web Login
- **Key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

- Import Options
- Export Options
- Search Option Property

### 6.2.11.1 Advanced

## DESCRIPTION

Use the **File – Options – Advanced** tab to control the application behavior as it pertains to low level settings.



*Options - Advanced*

## SETTINGS

## ADVANCED

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

## OTHER OPTIONS - CONNECTIONS

OPTION	DESCRIPTION
<b>Auto close embedded tab on disconnect</b>	Automatically closes all tabs for embedded sessions when they are disconnected.
<b>Confirm on multiple sessions open</b>	When opening more than one session you will be presented with a confirmation dialog. This typically occurs when doing an Open session on a folder.
<b>Disable embedded 32 shell execute</b>	Disable the shell embedded 32 execute in Windows for embedded sessions.
<b>Disable logoff confirmation message</b>	When pressing the logoff button in an embedded RDP session, Remote Desktop Manager, will disconnect the session without the logoff confirmation message.
<b>Disable multi-thread loading</b>	This setting allows Remote Desktop Manager to use multiple threads to load the data. Disabling this option will decrease the performance.
<b>Disable multi-thread offline file</b>	This setting allows Remote Desktop Manager to use multiple threads in offline file. Disabling this option will decrease the performance.
<b>Disable RDP virtual channel</b>	Turning off virtual channel disables some Remote Desktop Services features such as clipboard and printer redirection.
<b>Enable advanced Logging for Telnet and SSH (AdvancedTelnetSSH.log)</b>	This option creates an AdvancedTelnetSSH.log file in % LocalAppData%\Devolutions\RemoteDesktopManager. This file can be helpful when retrieving logs for Telnet/SSH connections.
<b>Enable offline read/write locks</b>	Activate locks for the Offline read/write rights.
<b>Ensure that KeePass is running</b>	Validate that KeePass is running on your computer before accessing any KeePass data.

OPTION	DESCRIPTION
<b>Force refresh before edit entry</b>	Perform a refresh of the entry before entering in edit mode. This is useful in a multi-user environment with a shared data sources. This ensure that you are editing the most recent version of the entry.
<b>Force restore application with desktop shortcut</b>	When double-clicking on the desktop shortcut it will restore the application that is already open. If the option is unchecked a second Remote Desktop Manager window will open.
<b>Open shortcut session silent</b>	Disable the command line warning message when using a shortcut.
<b>Use connection loader optimization</b>	Only enable this option upon request from our Support team.
<b>Use DirectX rendering in VNC</b>	By default this option is enabled to use DirectX rendering when available for VNC connection.
<b>Use NTFS Encryption for Offline mode</b>	When using <a href="#">Offline Mode</a> , a local file is created to hold a copy of the data source. If this is enabled the local file is encrypted using the built-in NTFS encryption of Windows. This setting may cause delays when accessing the data source because the local file is refreshed on every access.
<b>Use Secret Server Legacy Interface</b>	Enable to use the Secret Server Legacy interface.

## OTHER OPTIONS - GENERAL

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

OPTION	DESCRIPTION
<b>Allow non upgraded data source</b>	Allow Remote Desktop Manager to work on an older data source that has not being upgraded.
<b>Confirm on drag and drop move</b>	When session(s) are moved by drag and drop, a confirmation message will appear to confirm the move.
<b>Disable Analytics</b>	Disable the computational analysis of data or statistics.
<b>Disable stack trace</b>	Disable the stack trace details when an error occurs in Remote Desktop Manager. This is a security feature.
<b>Focus content on application activation</b>	Set focus on the last embedded session when the application is activated.
<b>Use application directory for local play list</b>	Use the installation folder to save the local play list that has been created.
<b>Use application directory for offline cache</b>	Use the installation folder to save the offline cache file.

## OTHER OPTIONS - UI OPTIONS

OPTION	DESCRIPTION
<b>Always show "Go Offline" button</b>	Always display the "Go Offline" button in the status bar when <a href="#">Offline Mode</a> is active.
<b>Disable custom images</b>	Disable the loading of any custom images in the tree view. Too many custom images could dramatically increase the size of the data source and increase the load time at the same time.



OPTION	DESCRIPTION
<b>Expand all tree nodes on select credential entry</b>	After creating a new credential entry, the tree nodes expands automatically.
<b>Hide last opened play list in play list management</b>	Hide the last opened play list at startup in the play list dialog.
<b>Use old entry sort</b>	Use the old entry sort from previous version of Remote Desktop Manager.

## INFORMATION

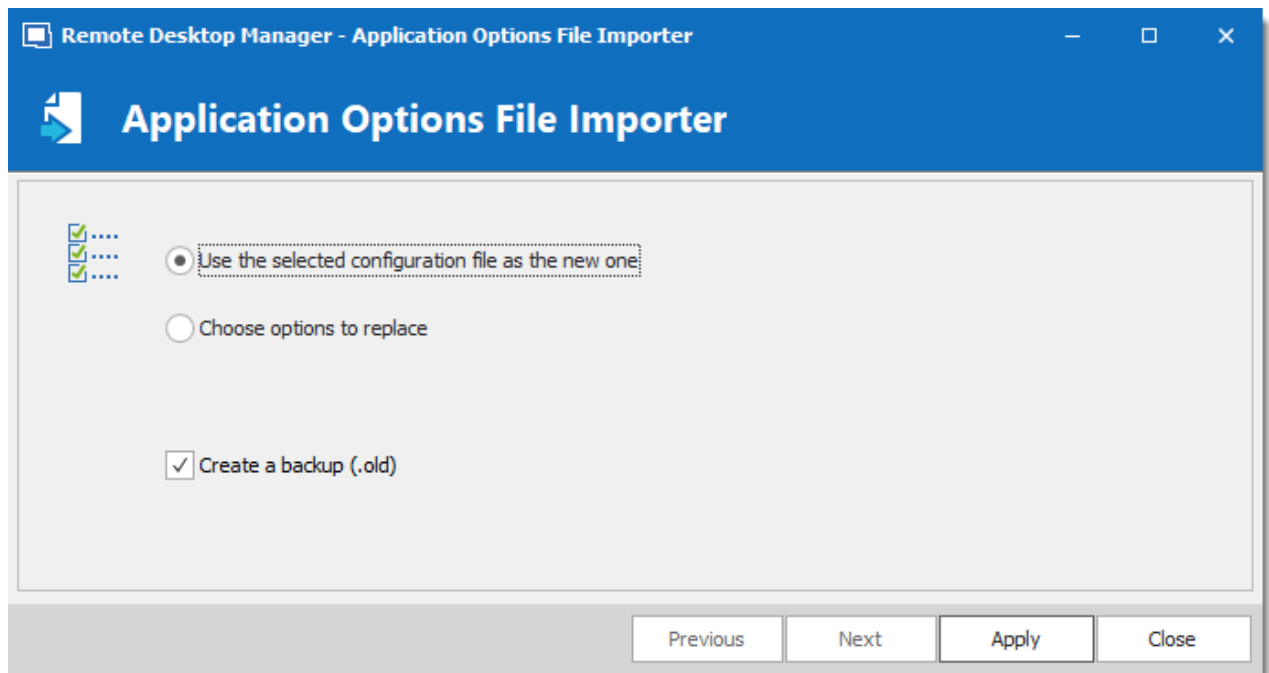
OPTION	DESCRIPTION
<b>Created on</b>	Creation date of Remote Desktop Manager configuration folder.
<b>Source</b>	Source of Remote Desktop Manager configuration settings.
<b>Path</b>	Shortcut to access the configuration folder directly.

### 6.2.11.2 Import Options

## SETTINGS

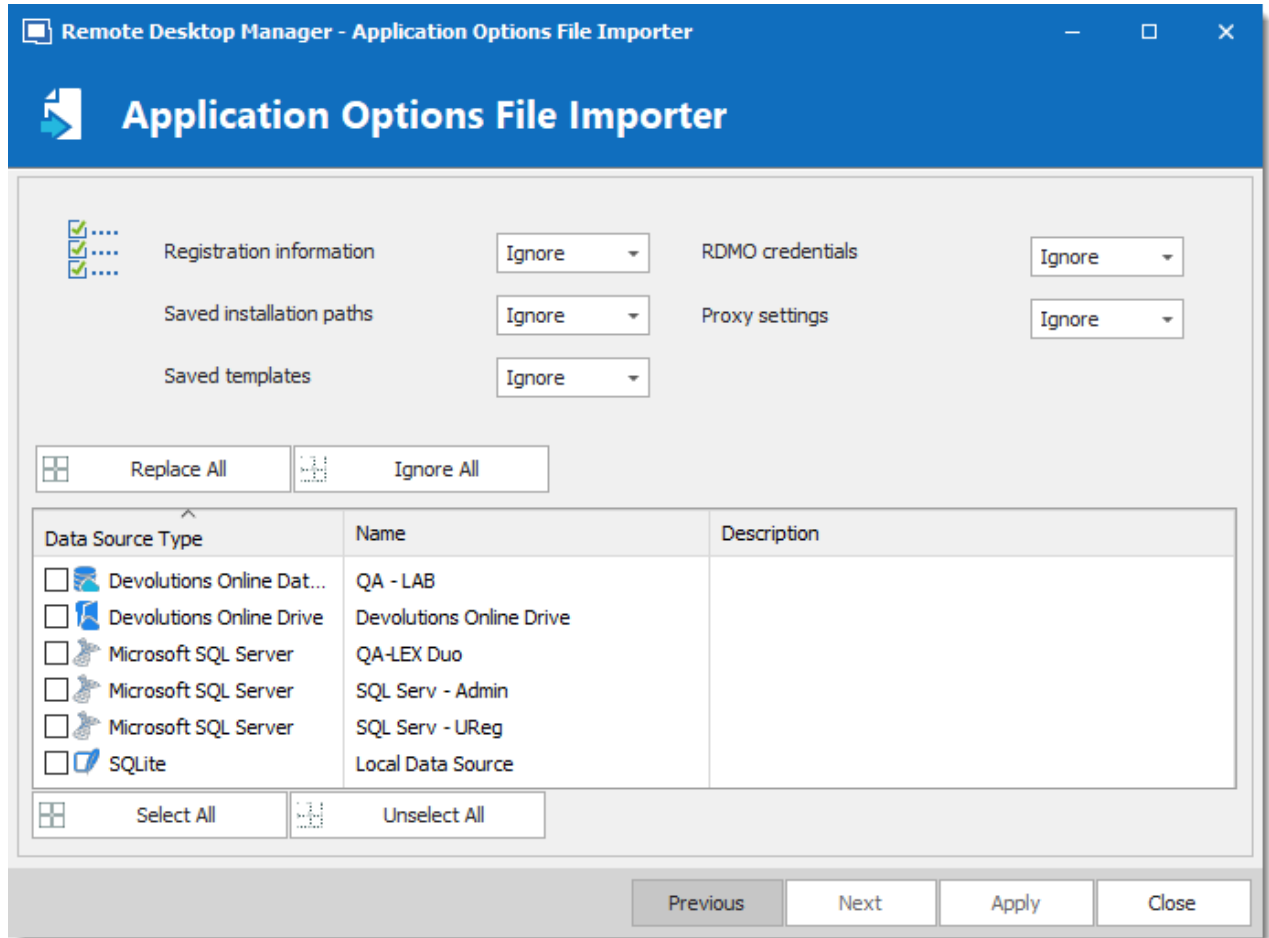
Select the [Configuration File](#) to import in Remote Desktop Manager and click on **Open**.

## REMOTE DESKTOP MANAGER OPTIONS FILE IMPORTER

*Application Options File Importer*

OPTION	DESCRIPTION
<b>Use the selected configuration file as the new one</b>	Use the RemoteDesktopManager.cfg file as a new configuration file for your application.
<b>Choose options to replace</b>	Select which options to replace in your actual RemoteDesktopManager.cfg file. See below for more information.
<b>Create a backup (.old)</b>	Create a backup of your old RemoteDesktopManager.cfg

## CHOOSE OPTIONS TO REPLACE



*Application Options File Importer*

Decide which options to replace with the one from RemoteDesktopManager.cfg that you wish to import. Select **Replace** to replace an existing setting with a new one or select **Ignore** if you want to keep the setting that you already have.

### 6.2.11.3 Export Options

## DESCRIPTION

Use **File – Options – Export Options** to control the options to export from your application configuration. Use this to easily transfer settings to another machine.



Sharing the exported file with a colleague would effectively give that person whatever credentials you have set in your data source definitions, including credentials set in your DODB.

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

**Remote Desktop Manager - Configuration file export**

## Configuration file export

**Registration Information**

☒ Name

☐ Email

☒ Key XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

**Miscellaneous**

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

☒ Include data source credentials

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

Select All Unselect All

Export Close

Configuration file export dialog

## SETTINGS

### REGISTRATION INFORMATION

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

## MISCELLANEOUS



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

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

## DATA SOURCES



The data source configurations you select will be exported with the username/password as they are currently configured. If you are creating a file to quickly set up new employees, you must be careful not to give away your credentials. Using the [Custom Installer Service](#) is recommended for this case.

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

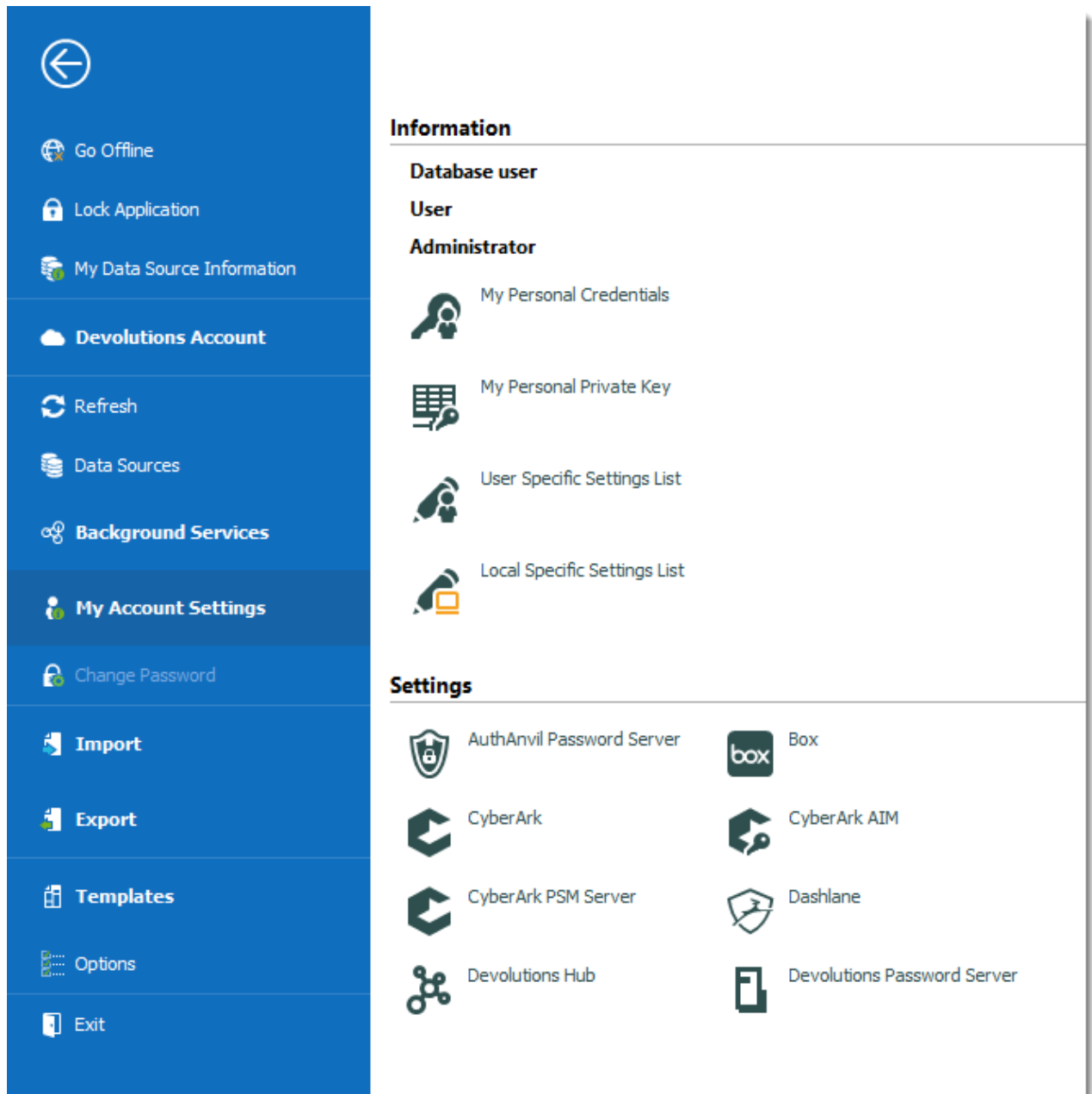
When your settings are customized to your liking, click on **Export**. You will be prompted to save your settings in a RemoteDesktopManager.cfg file.

## 6.2.12 My Account Settings

### DESCRIPTION

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

### SETTINGS



*My Account Settings*

## INFORMATION

OPTION	DESCRIPTION
<b>Database user</b>	Indicates the current user connected to the application.

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

## SETTINGS

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

### 6.2.12.1 My Personal Credentials

## DESCRIPTION

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

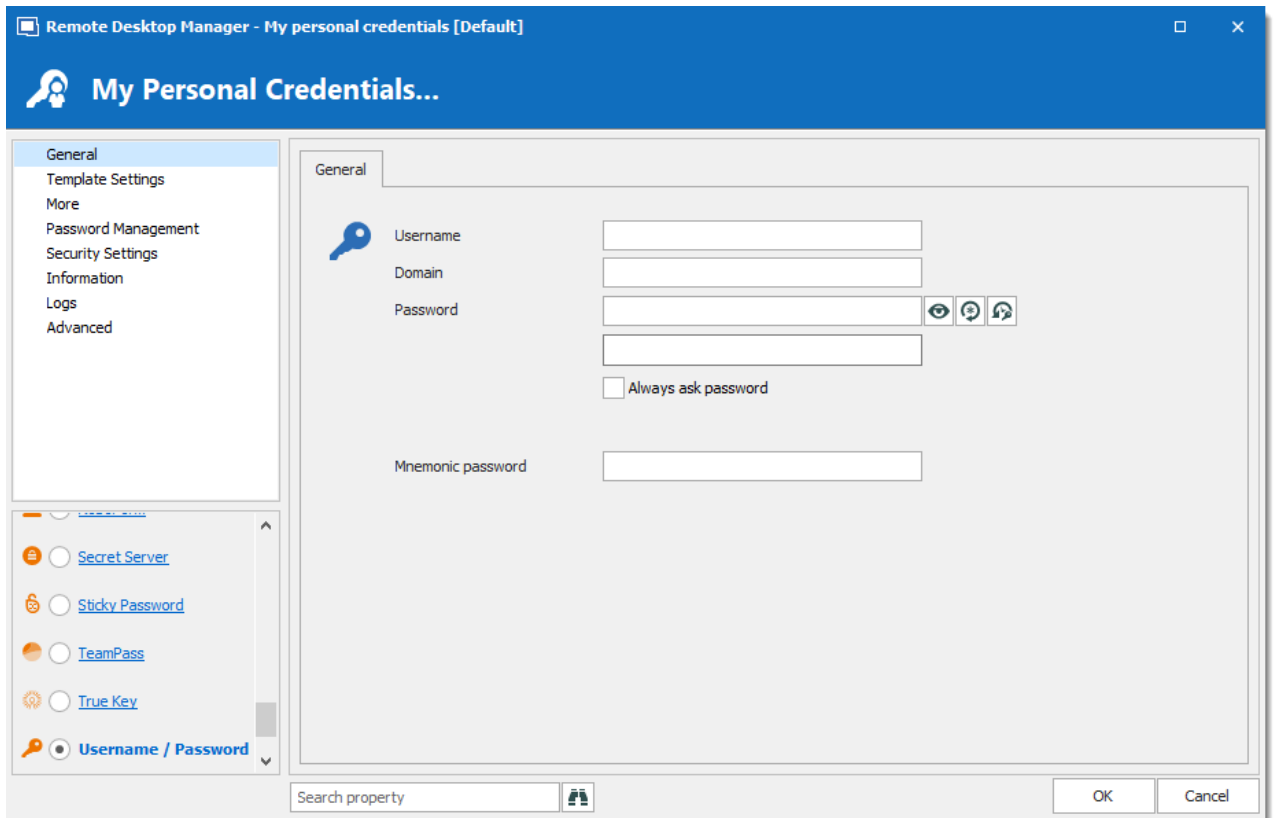
It is typically used to hold the Windows credentials for your running sessions because Remote Desktop Manager can't access them. If you can't use integrated security then you must store your credentials in **My Personal Credentials**.

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



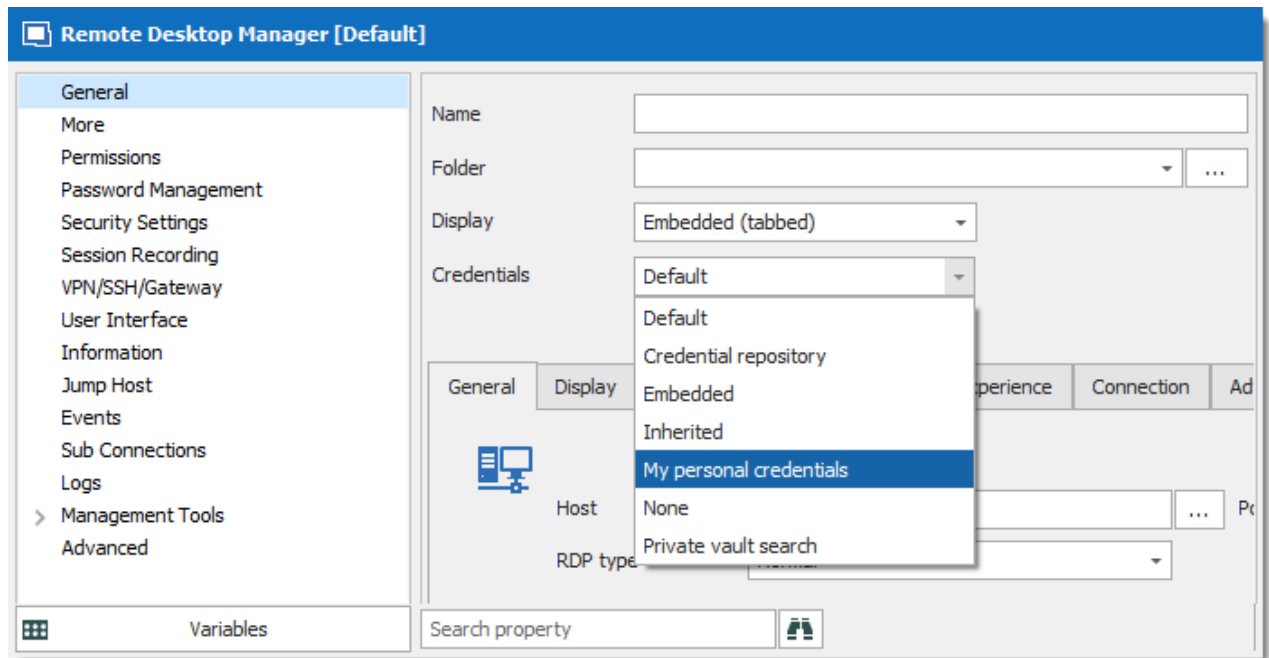


If you want to change the credential type, go in %LOCALAPPDATA% (*Default*) or %APPDATA% (*Remote Desktop Services*) \Devolutions\RemoteDesktopManager and delete the **Credentials.rdt** file to reset it.



*My Personal Credentials*

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

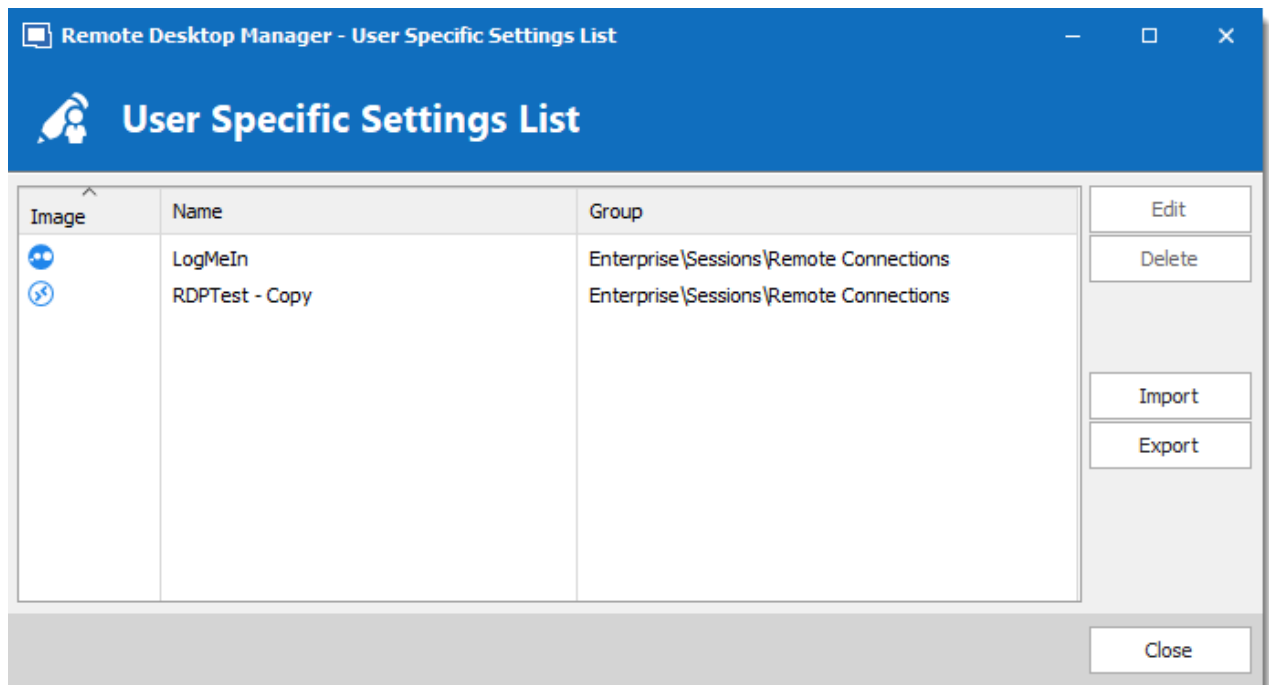


*Credentials - My personal credentials*

#### 6.2.12.2 User Specific Settings List

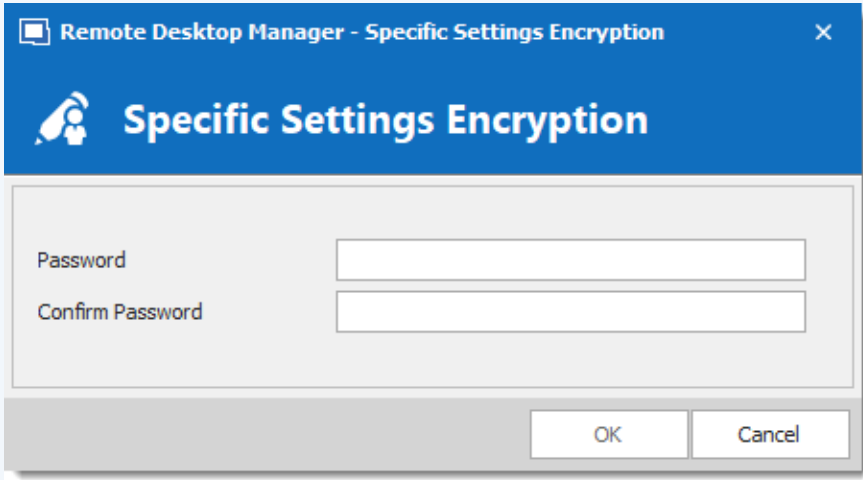
## DESCRIPTION

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



*User Specific Settings List dialog*

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

OPTION	DESCRIPTION
	

## 6.2.13 Templates

### DESCRIPTION

Templates are useful to have predefined values when creating an entry. Use templates to:

- [Add preconfigured entries](#)
- [Use with the Quick connect feature](#)
- Open entries as a template
- [Create an import wizard](#)
- Create password templates

To access and manage templates, navigate to **File – Templates**.

It's possible to create local and database templates.

- Local templates are saved in the Remote Desktop Manager configuration file. They are available only to the current user of the machine.
- Database templates are saved in the database. They are available to all users of the data source.

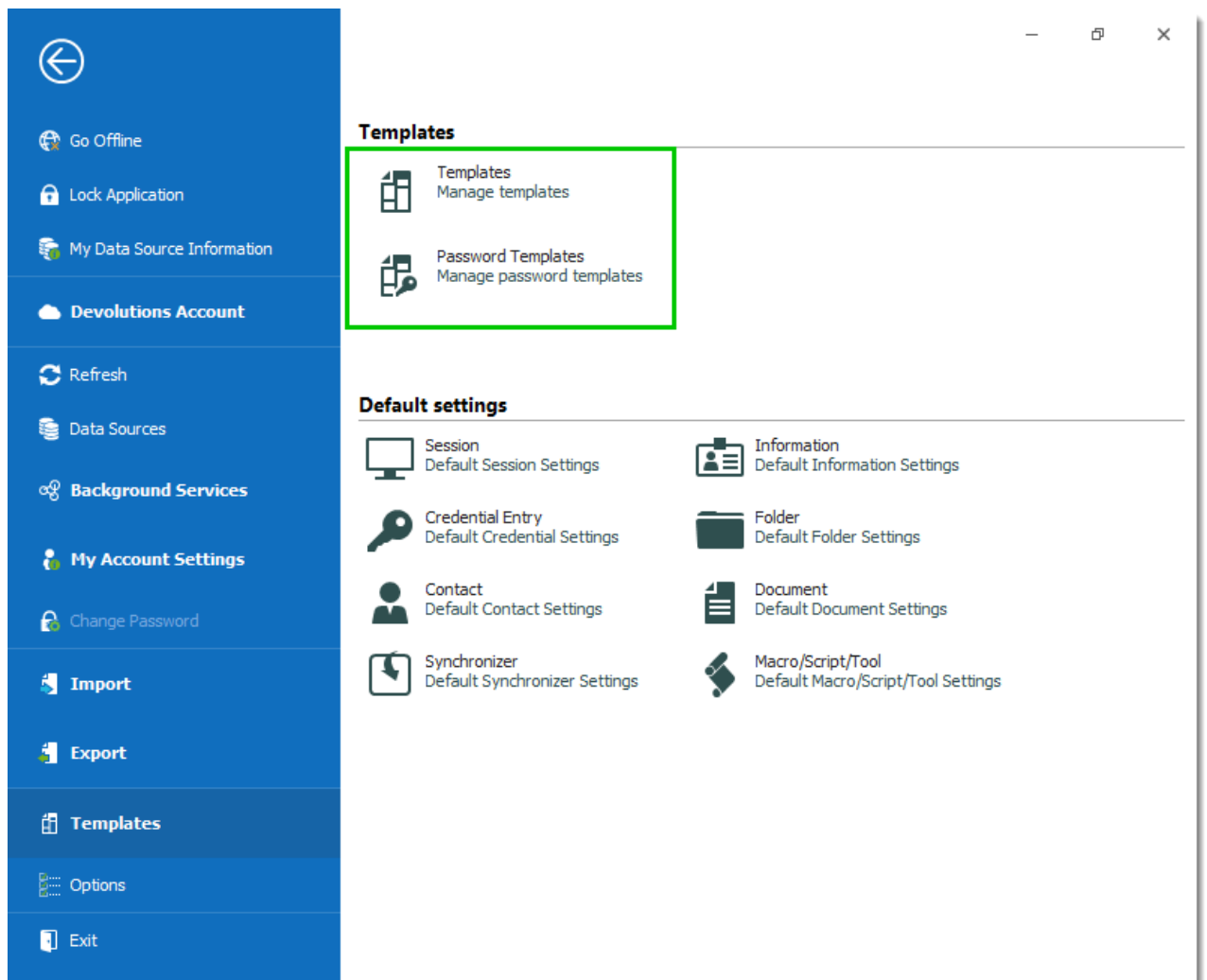
This allows for creating predefined templates available to use with the quick connect feature or when creating or importing a entries.



By default, standard users cannot create or manage templates. To allow users to create or manage templates, the permission must be granted to users using the **Management** section of the [Data source permissions \(System Permissions\)](#).



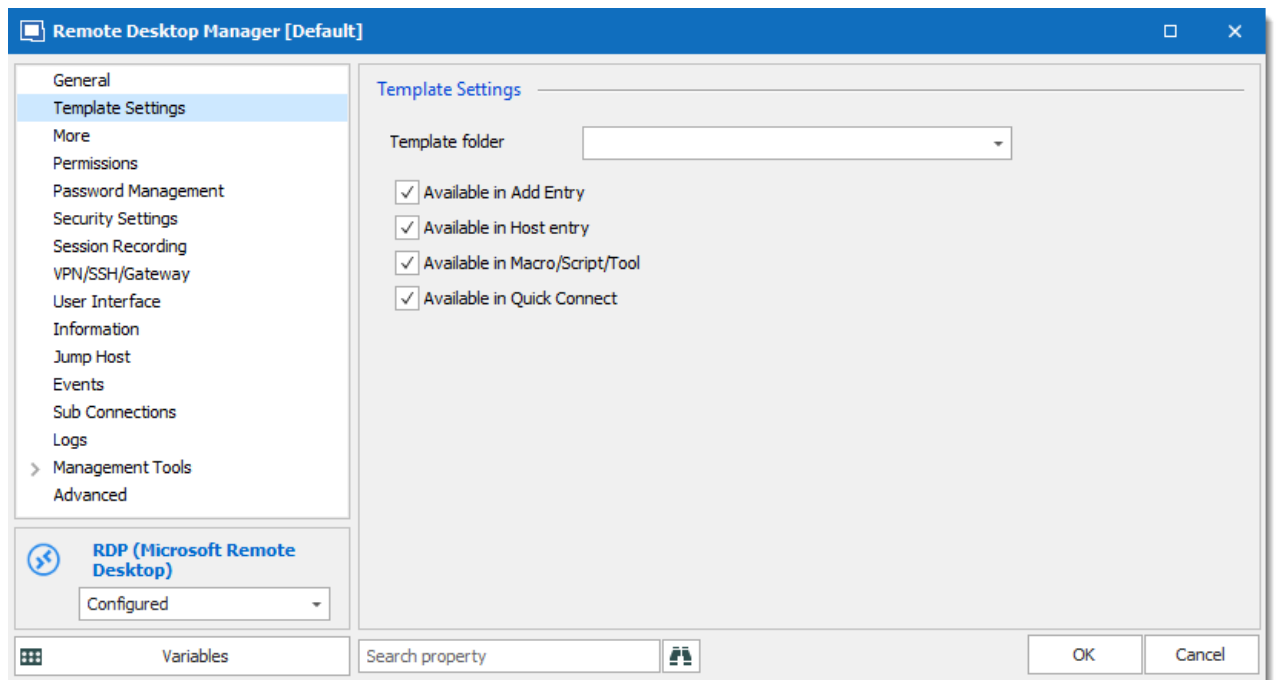
In Advanced Data Sources , local templates are disabled by default. They can be enabled from the [Data Source Settings \(System Settings\)](#).



*File – Templates*

## AVAILABILITY

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



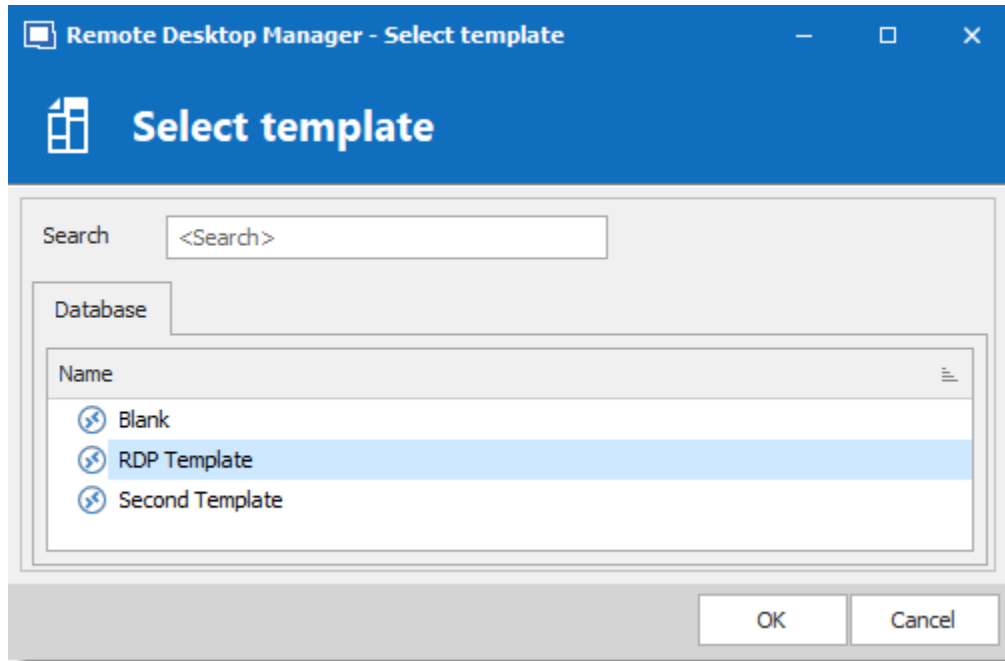
*Template properties – Template Settings*

## USAGE

Templates can be used in the following cases:

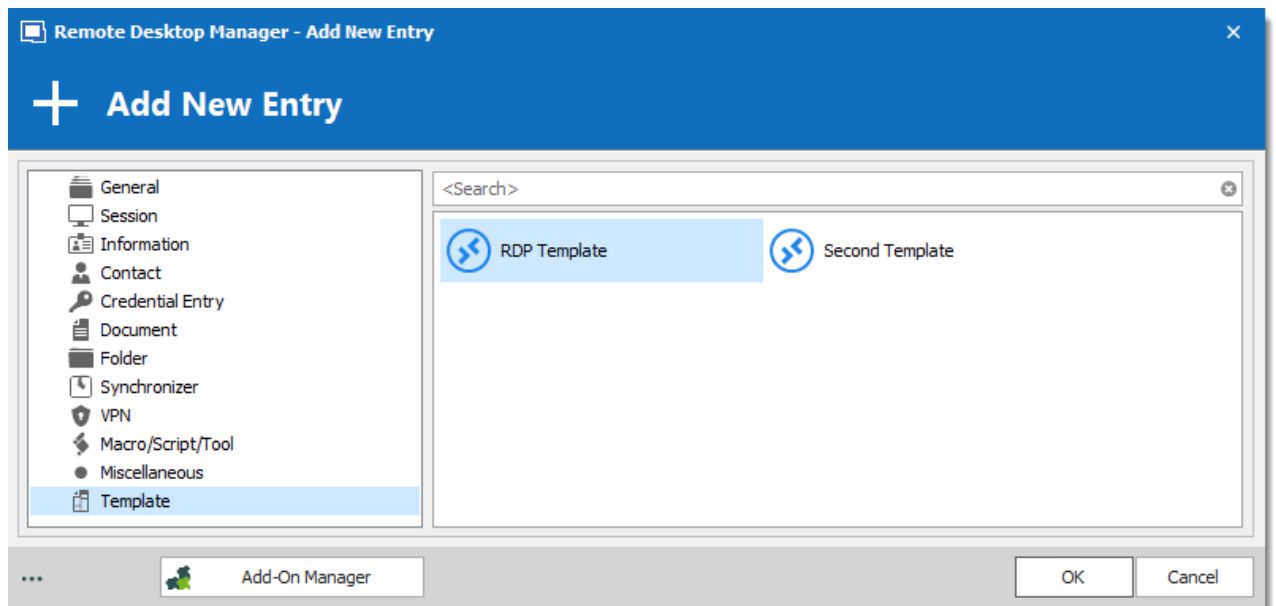
### CREATE A NEW ENTRY

By default, when creating an entry of a type that has templates configured for, the user is prompted for a template to use. This behavior can be modified in the [Data Source Settings \(System Settings\)](#).



*Select a template*

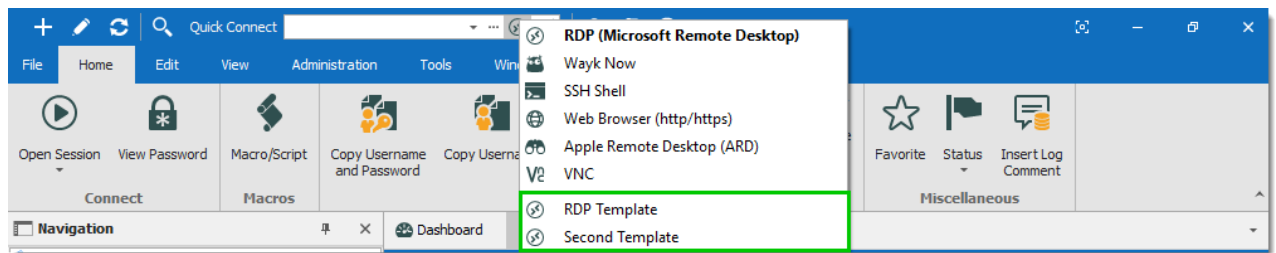
The template can be selected before creating the entry as well. Simply use the **Template** section of the **Add New Entry** window.



*Add New Entry – Template*

## RUN A QUICK CONNECT SESSION

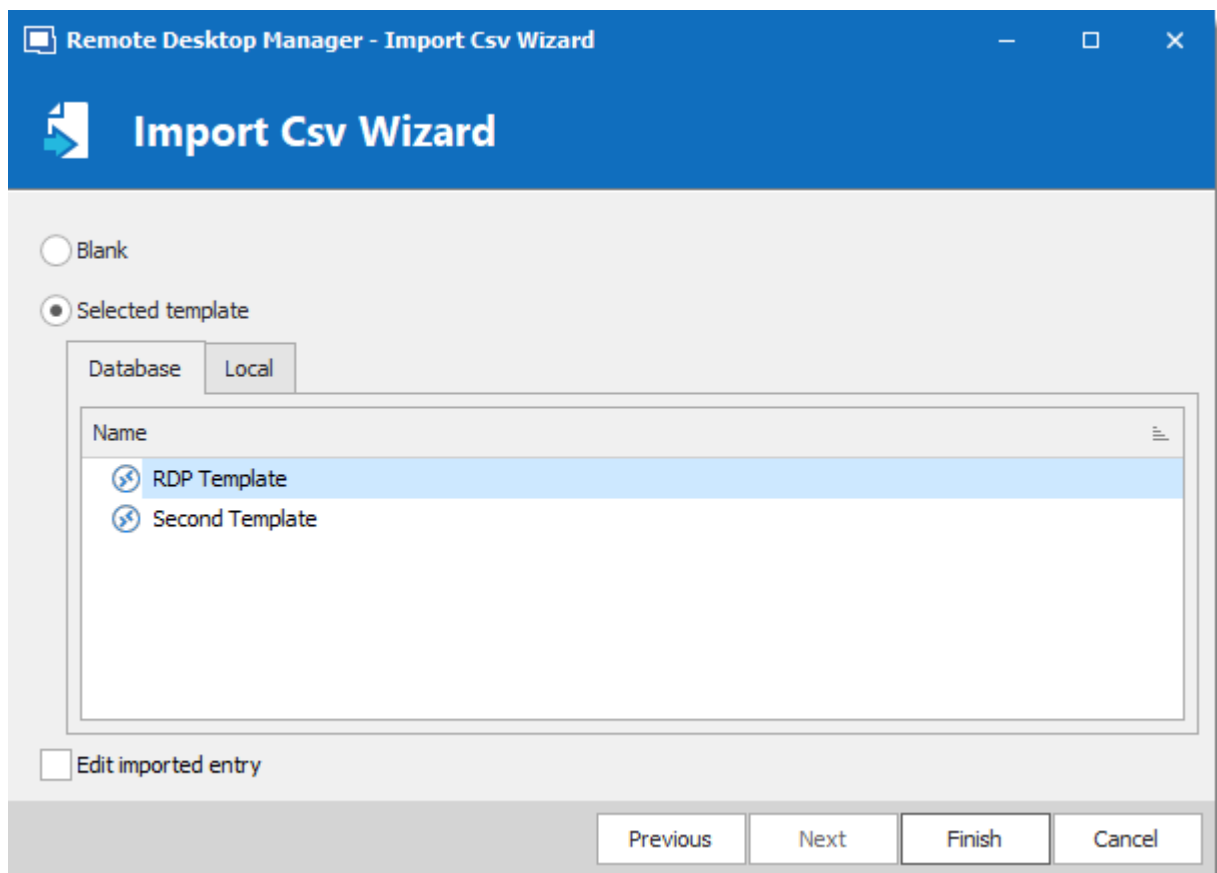
Templates can be used with the **Quick Connect** feature. For example, the same template can be used to connect to different hosts.



*Quick Connect*

## IMPORT WIZARD

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



*Import Session Csv Wizard*



### 6.2.13.1 Creating Templates

## DESCRIPTION

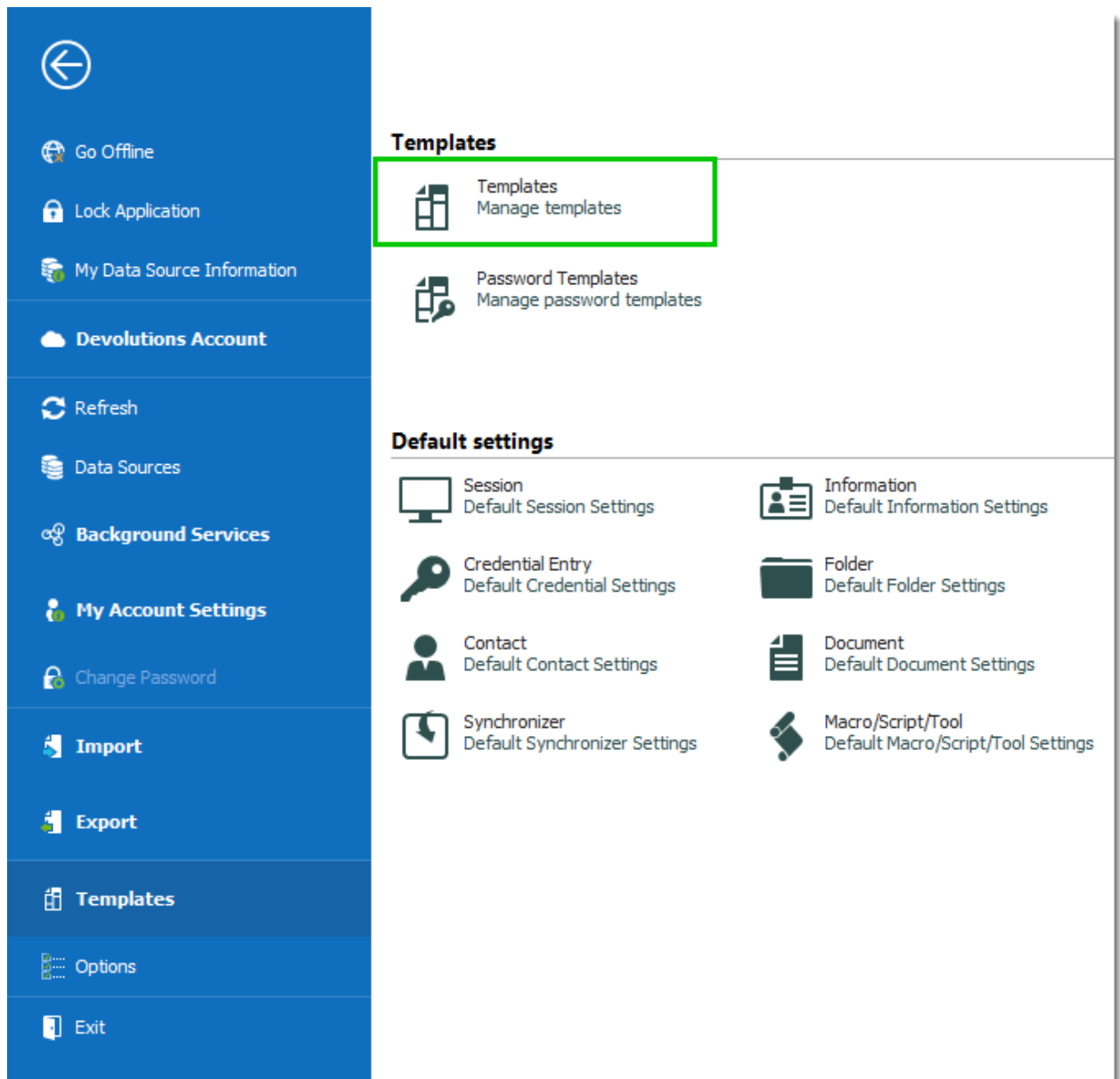
There are many ways to create template for entries. You can create a new template, save an entry as a template, import entries as templates, and duplicate a existing template. It is also possible to create group templates.

In this topic:


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

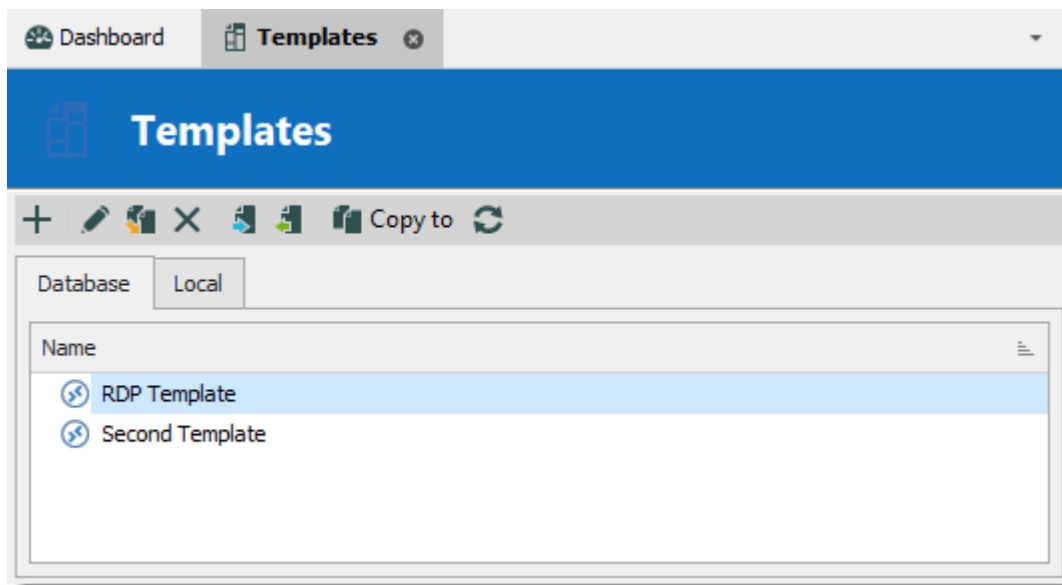
## CREATE A NEW TEMPLATE

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



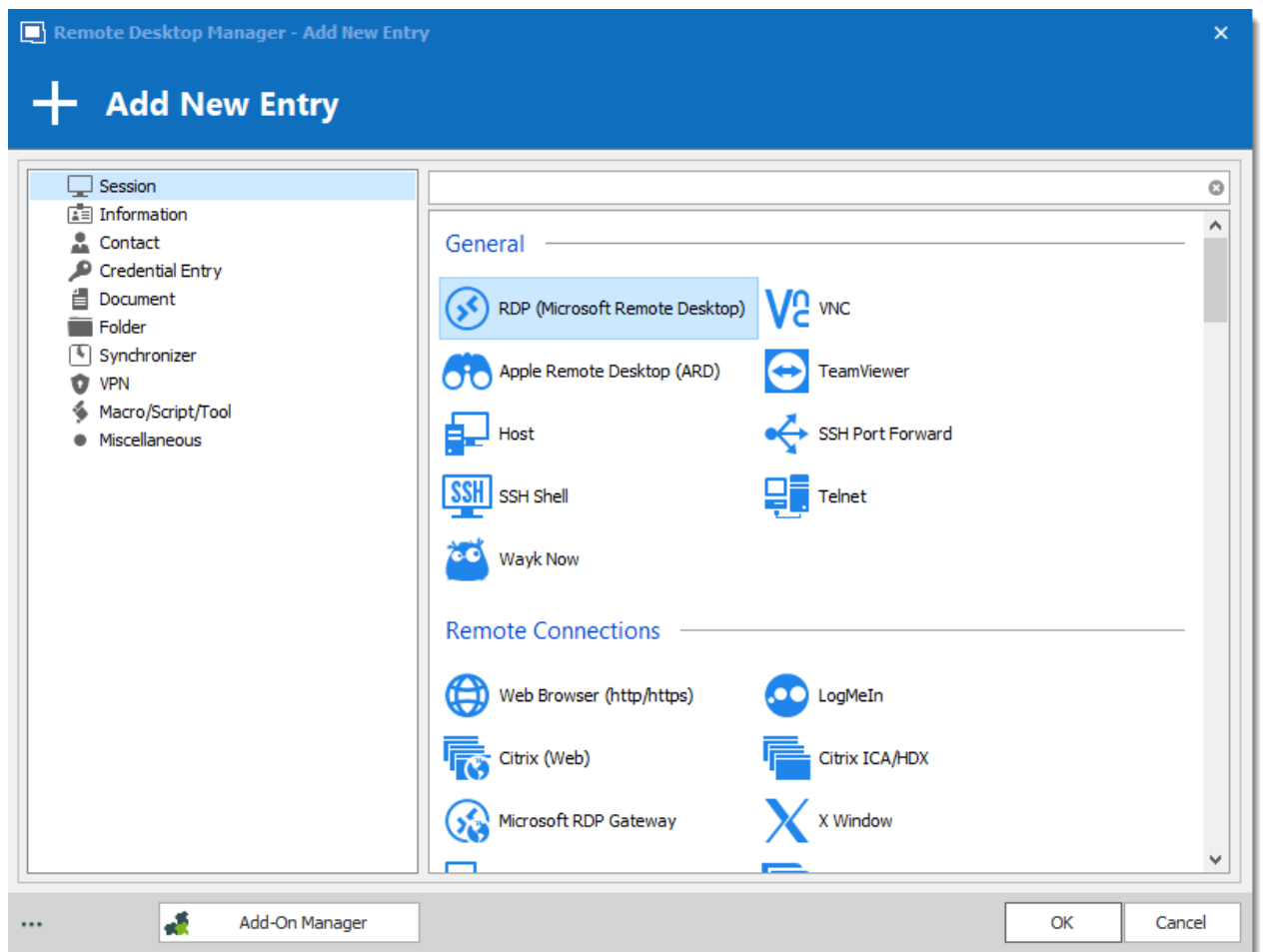
File – Templates

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



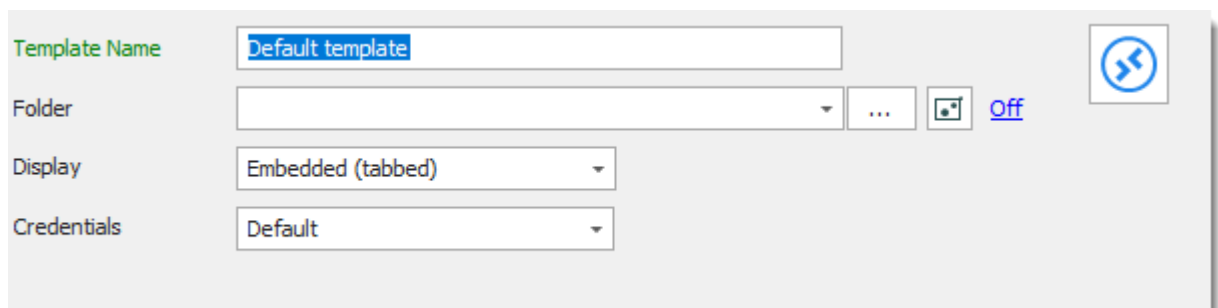
*Add a new template*

3. Select an entry to create the template for.



*Select an entry to create the template for*

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

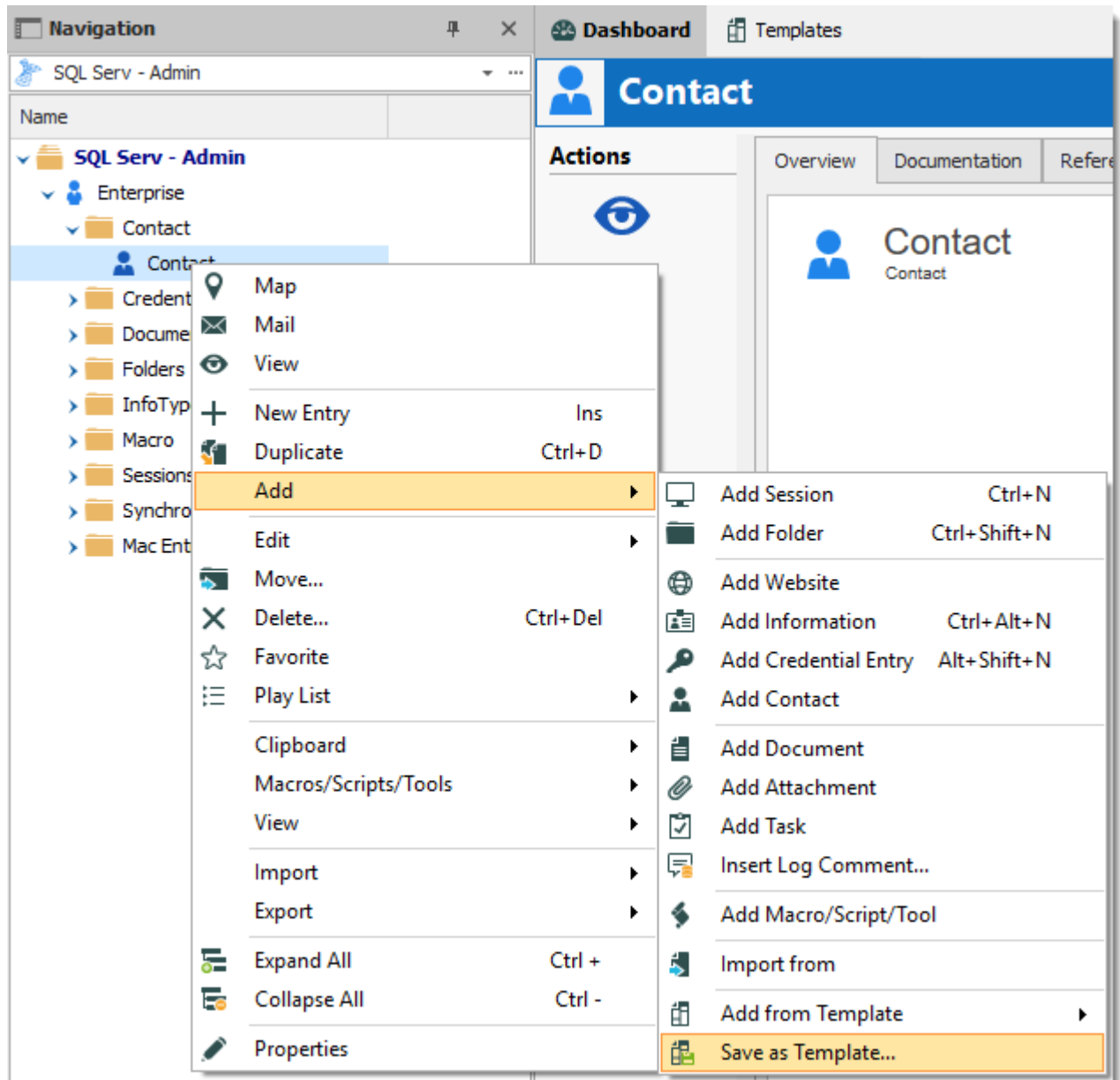


*Template Properties*

## SAVE ENTRY AS TEMPLATE

It is possible to save entries as templates to use their properties in other entries. Furthermore, this can be achieved on folders to include all their child items in the template.

From the Navigation Pane, **right-click** an entry and select **Add – Save as Template...**



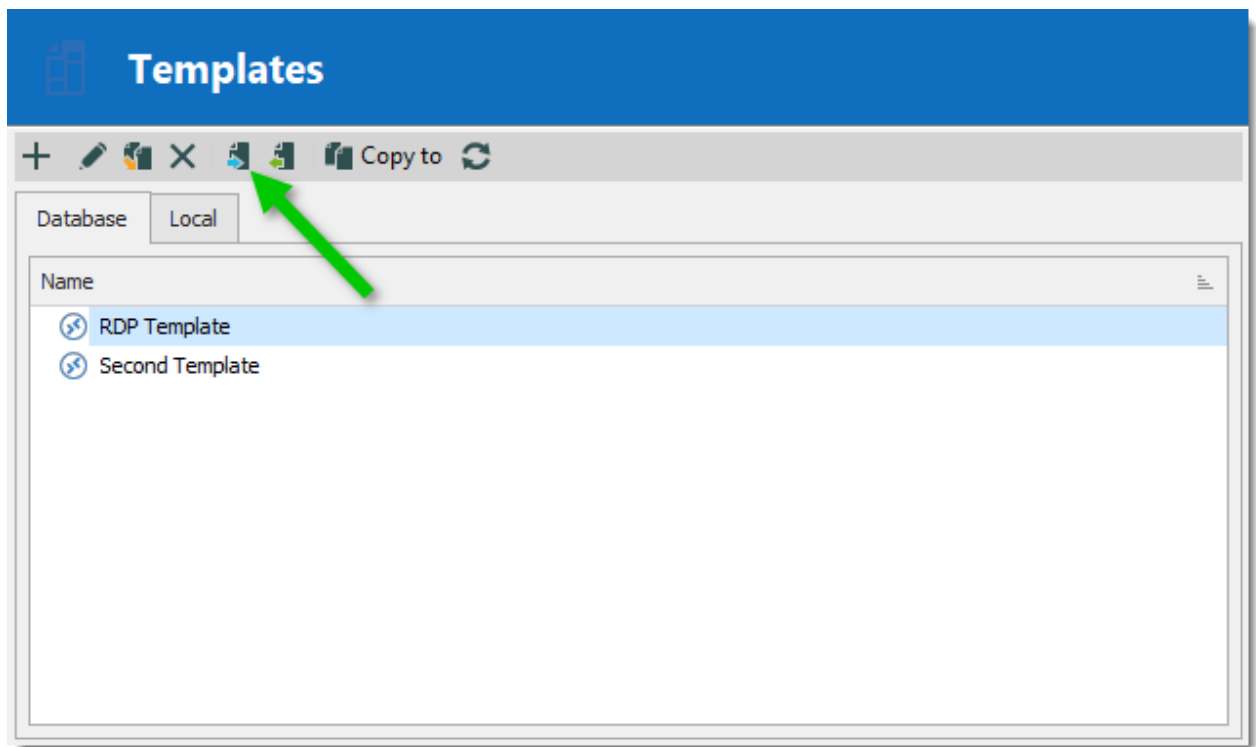
*Save as Template...*

## IMPORT TEMPLATE

It is possible to import previously exported entries as templates.

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

- 1.1. From the **Templates** window, click on the **Import template**  button.



*Import Template*

2. Select the **\*.rdm** file to import to create a template for each entry in the file.

## DUPLICATE TEMPLATE

It is possible to duplicate a template to edit a copy of the properties.

Navigate to **File – Templates**, and select **Templates**. From the **Templates** window, click on the **Duplicate template**  button.

Change the template name to distinguish the copy from the original, and edit the properties to meet your requirements.

## TEMPLATE GROUPS

It is possible to save a set of selected entries or a folder and all its child items to a unique template.

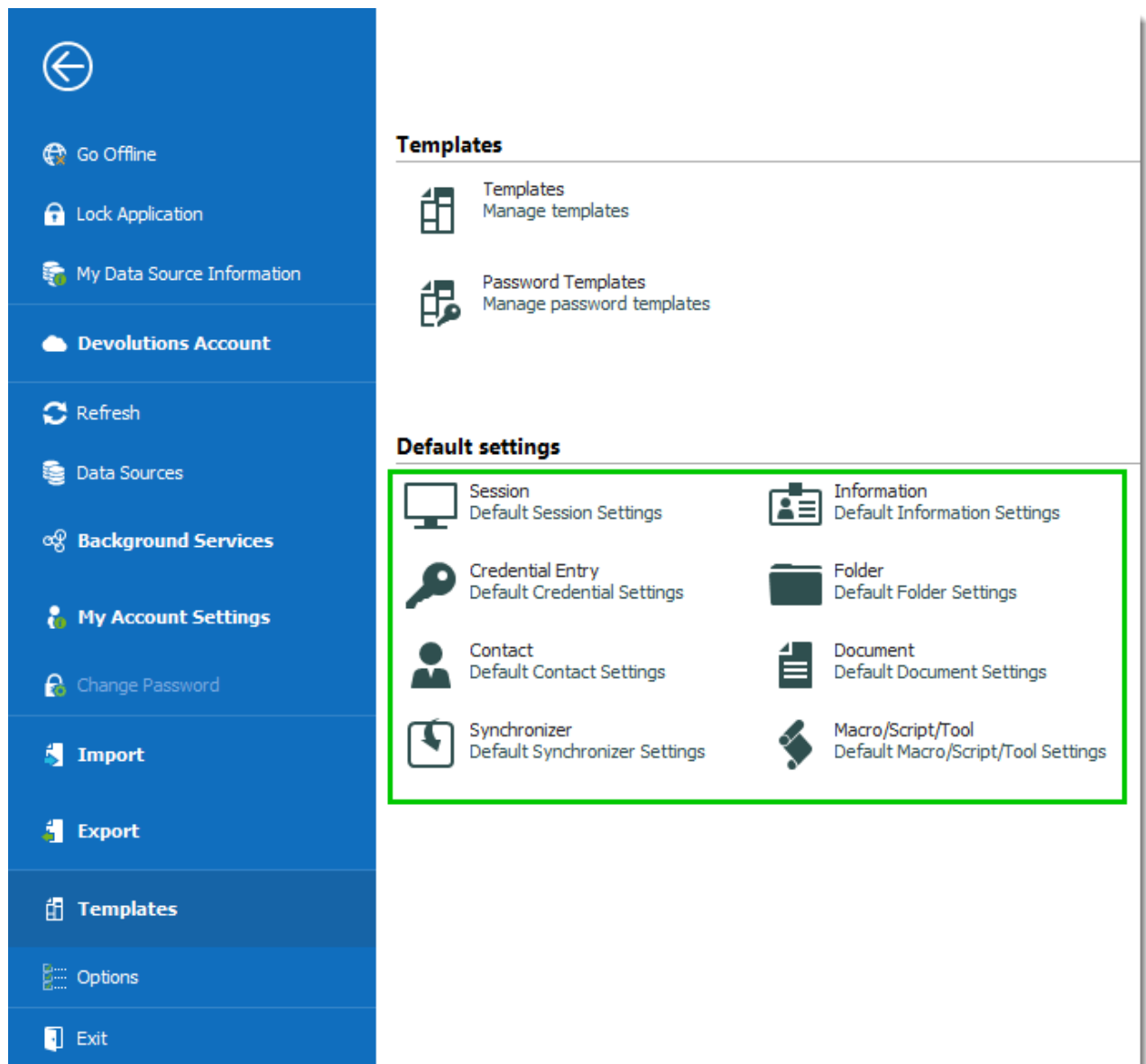
**Right-click** a selection of entries or a folder, select **Add**, then **Save as Template...**

#### 6.2.13.2 Default Settings

### DESCRIPTION

Default Templates create default settings for new entries. Every entry type is supported and can have a default settings template defined.

- **Session**
- **Information**
- **Credential Entry**
- **Folder**
- **Contact**
- **Document**
- **Synchronizer**
- **Macros/Scripts/Tools**



*File - Templates - Default settings*


## SETTINGS

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

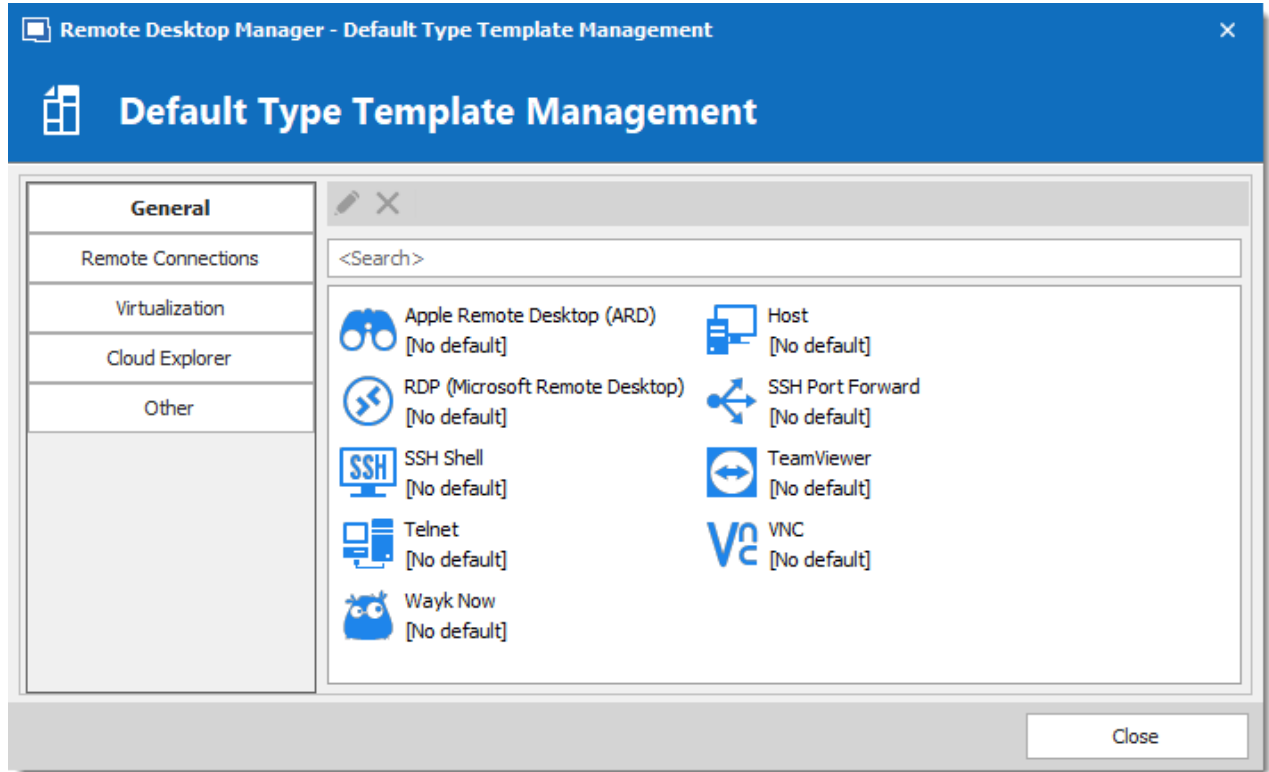
Select a category of entry from the **File – Templates** menu, then select the specific entry type to be edited.

Please note that a **[No default]** notice is displayed below each type that does not have a default template defined.



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

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



*Default Type Template Management*

### 6.2.13.3 Password Templates

## DESCRIPTION

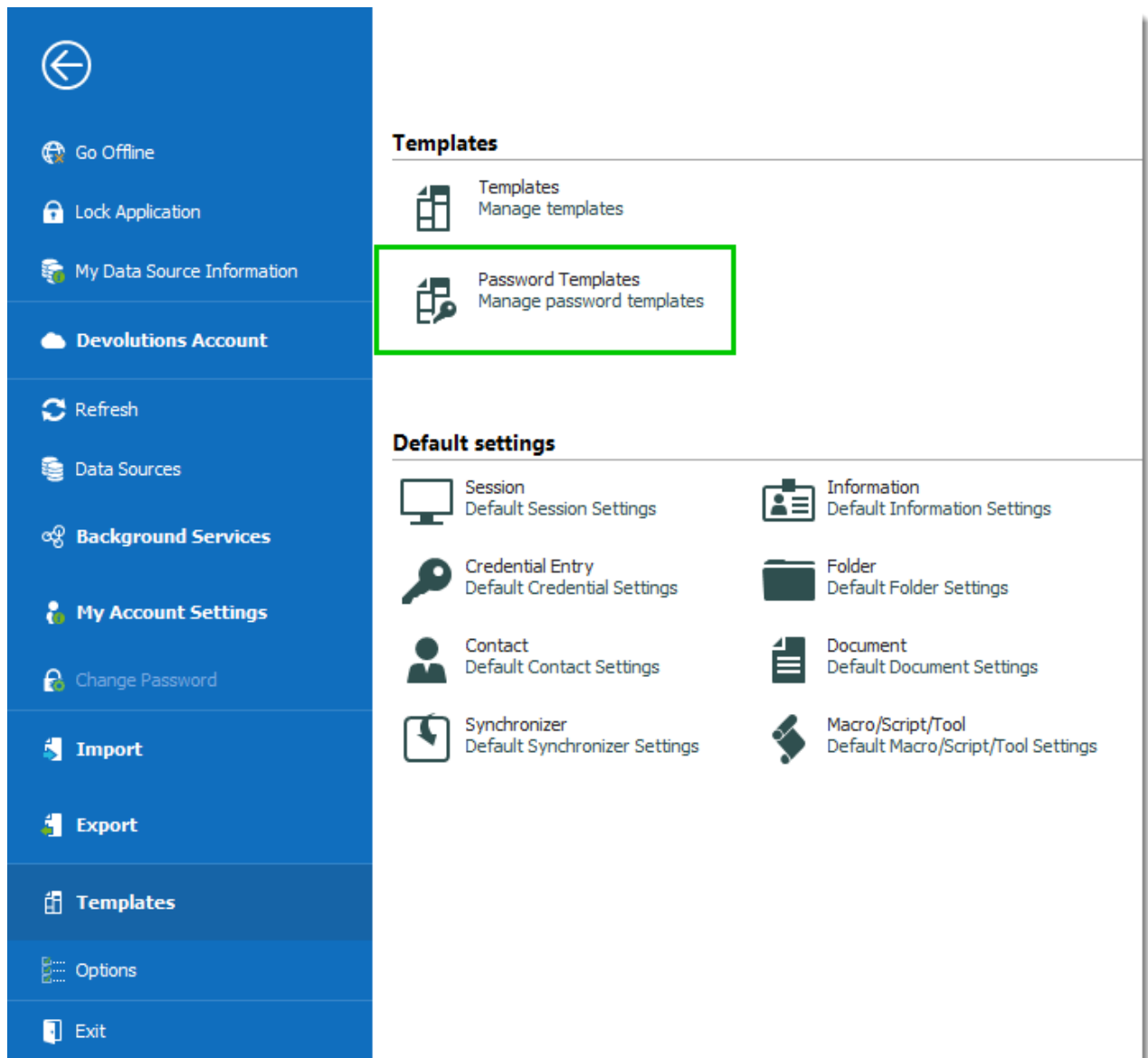
Password templates set requirements for the password format: characters usage, patterns, readability.

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

## SETTINGS

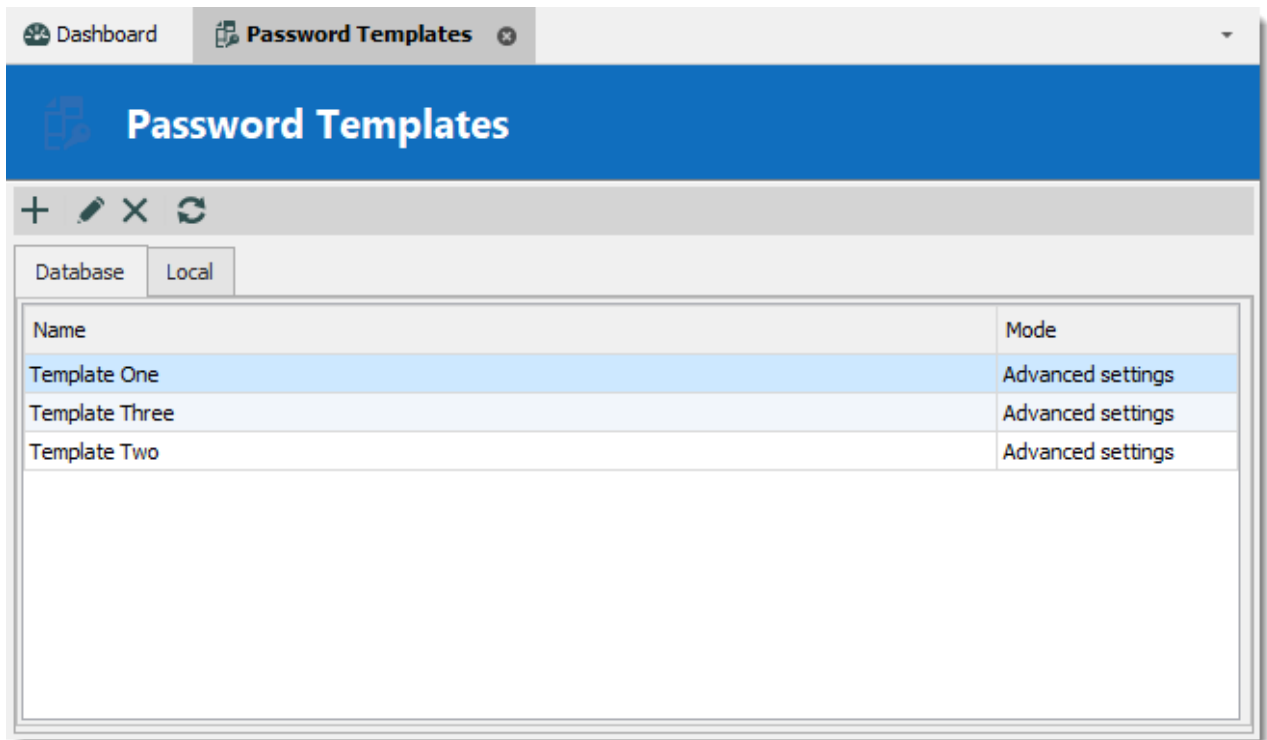
## CREATE A PASSWORD TEMPLATE

1. Go to **File – Templates**, and click **Password Templates**.



*File – Templates – Password Templates*

2. The **Password Templates** window provides an overview of current templates, as well as add, edit and delete commands.



*Password Template Window*

3. To add a new template click **Add** (plus sign).
4. a) Enter a template name.
- b) Choose a **Mode** and configure the settings.

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

OPTION	DESCRIPTION
<b>Pronounceable password</b>	Settings for length, case, digits and characters.

c) Choose specific settings

Remote Desktop Manager - Password Templates

**Password Templates**

Name: Cloud Services

Mode: Advanced settings

Password length: 20

☒ Upper-case (A, B, C, ...) 6

☒ Lower-case (a, b, c, ...) 0

☒ Digits (0, 1, 2, ...) 0

☒ Minus (-) 0

☒ Underline ( \_ ) 0

☐ Space ( ) 0

☒ Special (!, \$, %, &, ...) 0

☐ Brackets ([, ], {, }, (, ), <, >) 0

☐ High ANSI characters 0

☐ XML Compliant

Include the following characters:

Exclude the following characters:

OK Cancel

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

## USE A PASSWORD TEMPLATE WITH PASSWORD GENERATOR

1. On the **Tools** tab, click **Password Generator**. Or open the password generator from an entry .

2. To choose a password template, select the title from the list. **Default** is equivalent to no template, until it is configured by an administrator. When you select a template the options are unavailable because they were saved in the template.

3. Click **Generate** to list possible passwords.

*Password Generator using a password template*

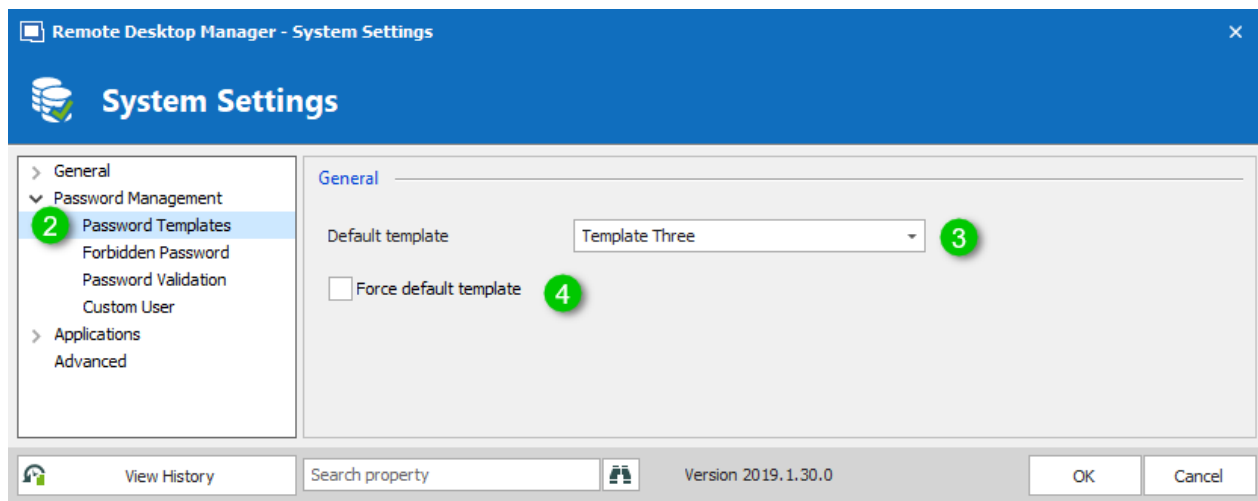
## SET A DEFAULT PASSWORD TEMPLATE

The default template in the **Password Generator** is set to "no template" until an administrator configures the template.

1. On **Administration**, click **Data Source Settings (System Settings)**.

2. Click **Password Templates**.

3. Choose the template. The chosen template will now be the **Default** in Password Generator.
4. If you want to force one template, check **Force default template**. No other choices will be available in the password generator.

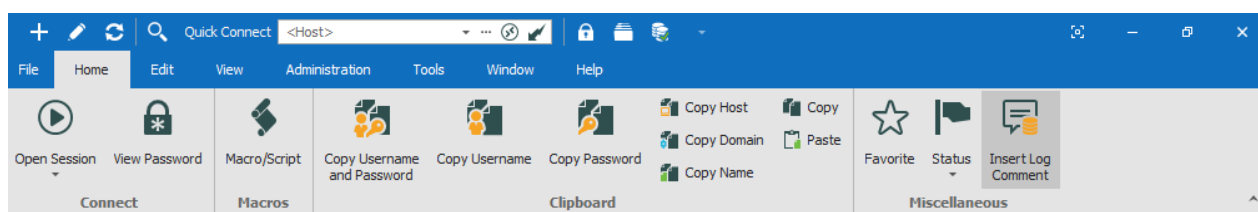


*System Settings – Password Templates*

## 6.3 Home

### DESCRIPTION

The **Home** ribbon tab allows you to apply an action on the currently selected session. The ribbon will display the following tab when the session is embedded.



*Ribbon - Home*

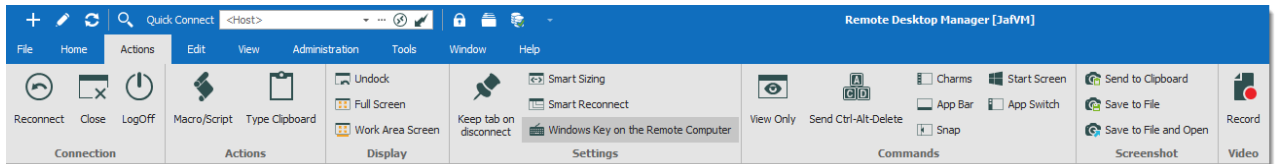
- Connect.
- Macros.
- Clipboard: Configure clipboard in **File – Options**.
- Miscellaneous.

## 6.4 Actions

### DESCRIPTION

The **Actions** tab is only available when a session is open. Available actions differ depending on the action.

For our example we are running an RDP session. The ribbon will display the following tab when the session runs with the Embedded (tabbed) display mode.



*Ribbon - Actions*

## CONNECTION

OPTION	DESCRIPTION
<b>Reconnect</b>	Quickly close the session and then re-open it automatically. Use it to update the resolution of your embedded RDP connections when you resize the window.
<b>Close</b>	Close the active session.
<b>LogOff</b>	Logoff the RDP session. See Logoff topic for more information.

## ACTIONS

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

Option	Description
Type Clipboard	Send the content of the clipboard over to the opened session.

## DISPLAY

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

## SETTINGS

OPTION	DESCRIPTION
Keep tab on disconnect	Your session tab will stay after a session disconnect. For more information, see Keep Tab Opened topic.
Smart Sizing	Enable or disable the RDP smart sizing. This setting will determine whether or not the client computer can scale the content on the remote computer to fit the window size of the client computer.



OPTION	DESCRIPTION
<b>Smart Reconnect</b>	Automatically reconnect your session with the most appropriate band.
<b>Windows Key on the Remote Computer</b>	When enabling <b>Windows key</b> , it will send the function to your host instead of running it on your computer.

## COMMANDS

This tab contains multiple type of commands and keystrokes combinations to affect the current session in a variety of instances. As such, these commands depend on the currently selected (and opened) entry. For a few example scenarios, refer to the following topics:

- [RDP](#)
- [VNC](#)
- [SSH Shell \(Rebex\)](#)
- [Telnet](#)



Session add-ons may add custom command in this section, they will not be documented in these topics but rather in the add-on documentation.

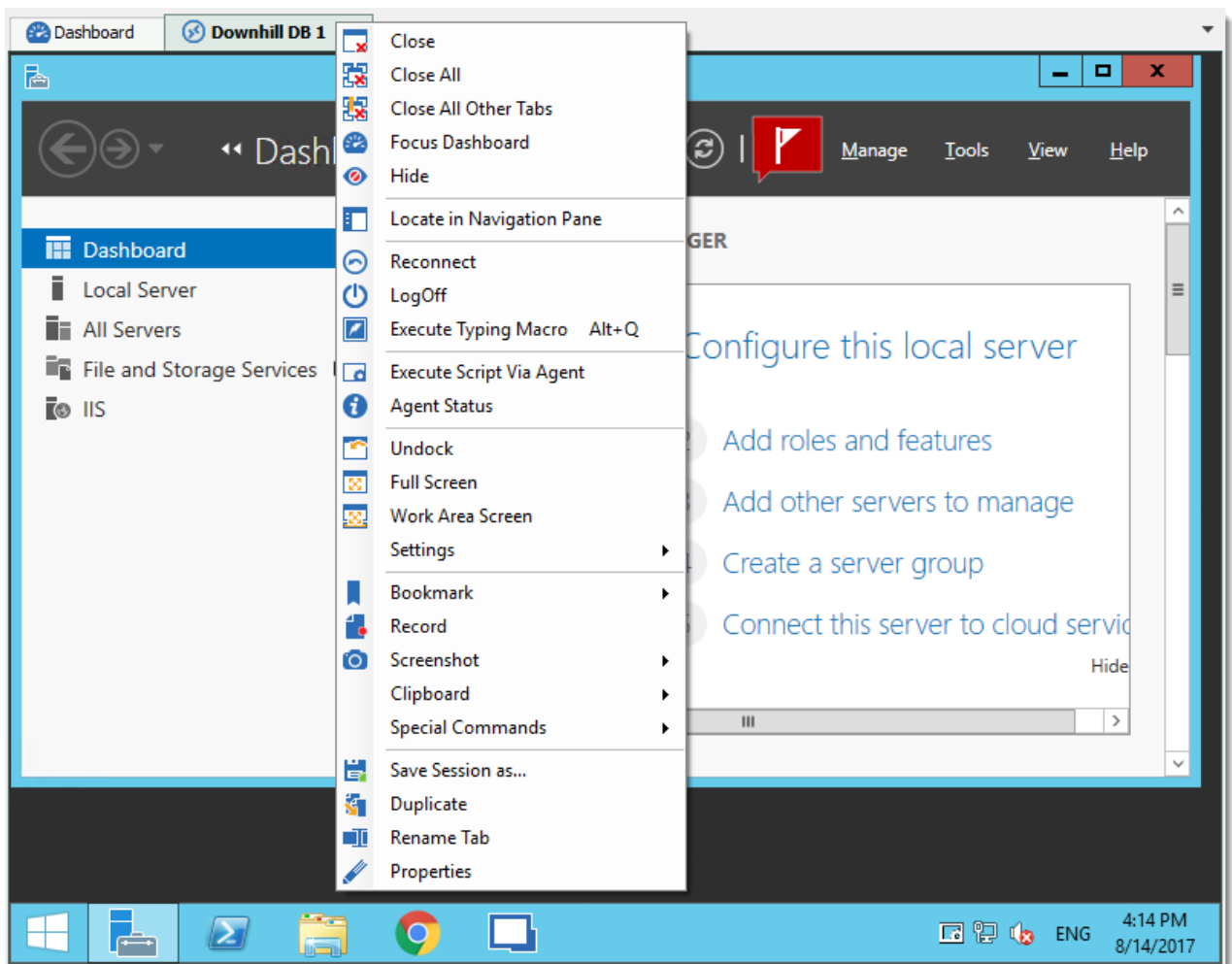
## SCREENSHOT

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

## VIDEO

OPTION	DESCRIPTION
<b>Record</b>	Record your screen in an MP4 format. We recommend the use of a VLC player to view the recorded video.

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



*Actions Context Menu of an Embedded Session*

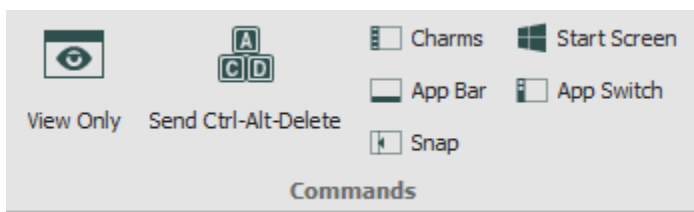
## 6.4.1 Commands

### 6.4.1.1 RDP

## DESCRIPTION

The commands for an RDP session allows you to send remote commands to your host.

## SETTINGS



*RDP Commands*

OPTION	DESCRIPTION
<b>View Only</b>	Prevent the session from receiving any input from the keyboard or the mouse. This feature was requested to allow monitoring while preventing manipulation errors. Use it to have a read only access to the remote server.
<b>Send Ctrl+Alt+Delete</b>	Send the key combination CTRL+ALT+DELETE to the host.
<b>Charms</b>	On Windows 8 or Windows 2012 server, displays the Charms bar (Search, Share, Start, Devices, and Settings bar).
<b>App Bar</b>	On Windows 8 or Windows 2012 server, displays the App bar to show navigation, commands, and tools.
<b>Snap</b>	On Windows 8 or Windows 2012 server, allows you to run two applications side-by-side.
<b>Start Screen</b>	Open the Start menu on the host computer.

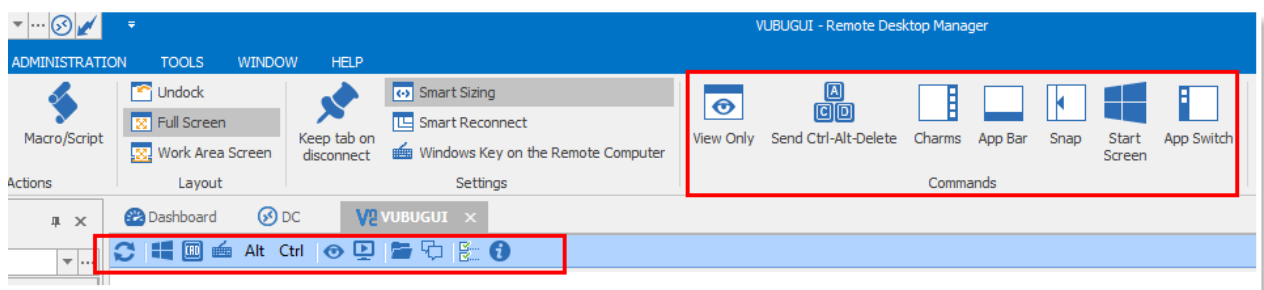
OPTION	DESCRIPTION
<b>App Switch</b>	On Windows 8 or Windows 2012 server, switches from an application to another.

#### 6.4.1.2 VNC

## DESCRIPTION

The VNC Commands allows you to send remote commands to your host. You will also notice another toolbar holding more defined commands for a VNC session.

## SETTINGS



*VNC Commands*

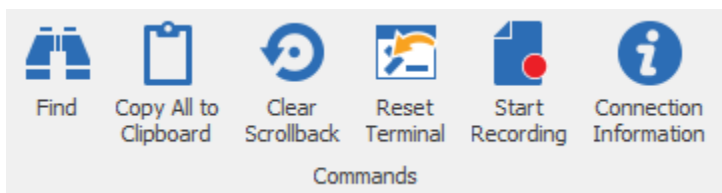
OPTION	DESCRIPTION
<b>Refresh Screen</b>	Refresh the host screen.
<b>Window Start Menu</b>	Open the Start menu on the host computer.
<b>Send Ctrl-Alt-Delete</b>	Send the key combination CTRL+ALT+DELETE to the host.
<b>Send Custom Keys</b>	Send custom keys combination to the host.
<b>Alt</b>	Send ALT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

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

#### 6.4.1.3 SSH Shell (Rebex)

### DESCRIPTION

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

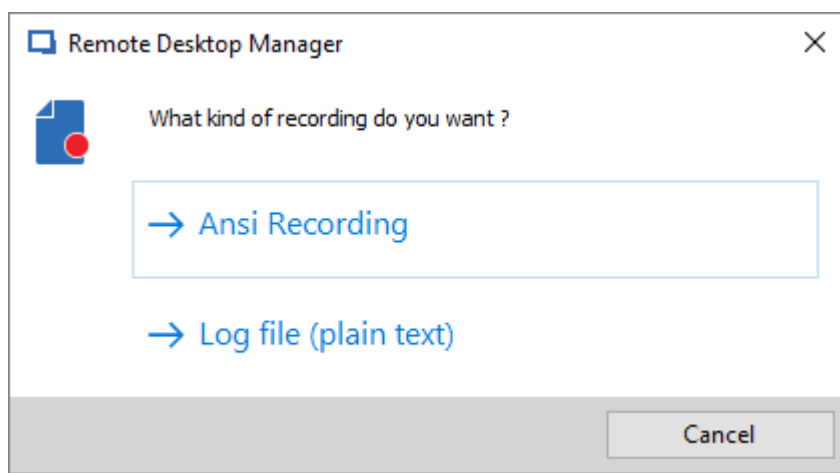


*Actions – SSH Shell (Rebex) Commands*

OPTION	DESCRIPTION
<b>Find</b>	Open a find window to search for a specific word.

OPTION	DESCRIPTION
<b>Copy All to Clipboard</b>	Copy all selected text to the Clipboard.
<b>Clear Scrollback</b>	Clear the scrolling display that precedes the current line.
<b>Reset Terminal</b>	Reset host terminal connection.

## START RECORDING

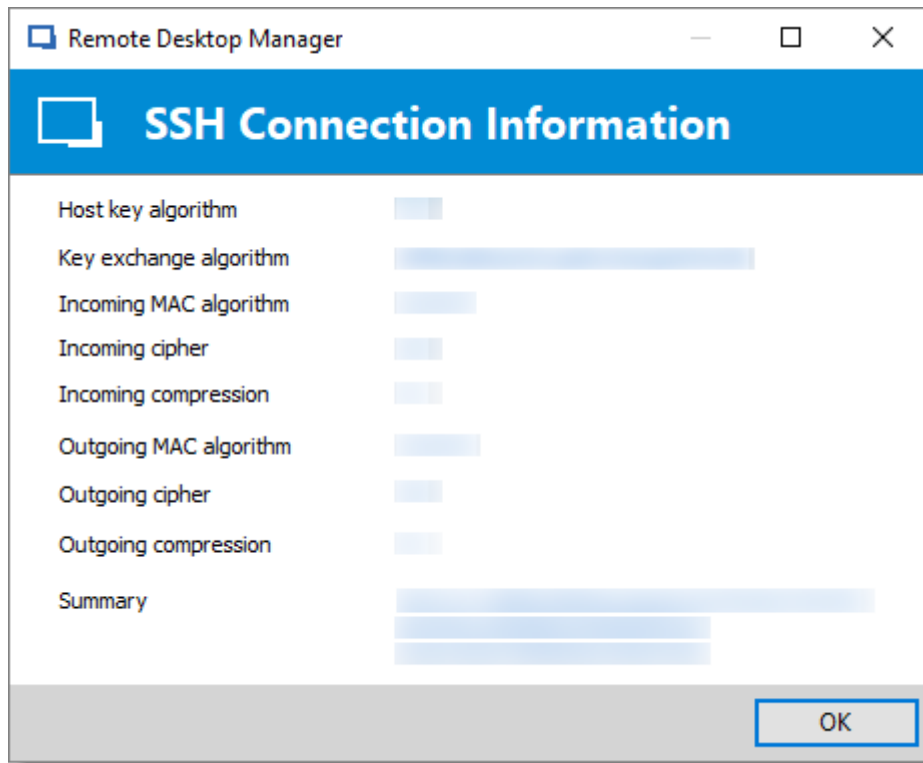


*Recording type*

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

## CONNECTION INFORMATION

Provides connection host information in a form as shown below.



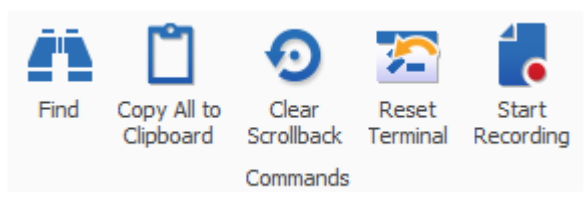
*SSH Connection Information*

### 6.4.1.4 Telnet

## DESCRIPTION

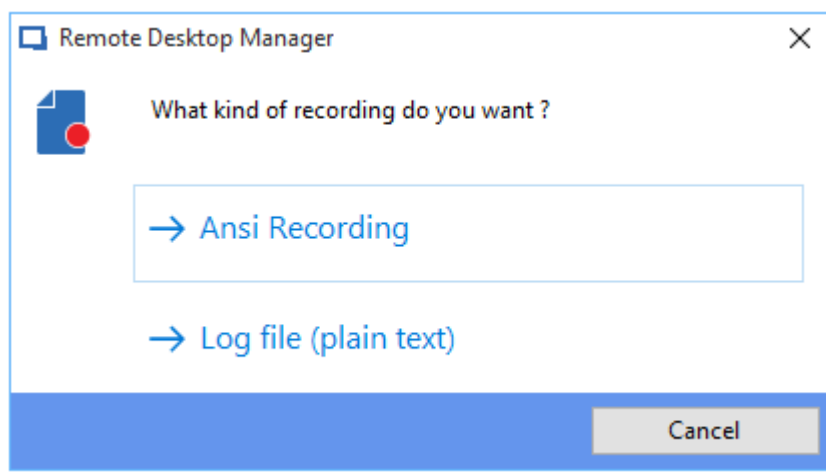
The actions for a Telnet session allows you to send remote commands to your host.

## SETTINGS



*Telnet Commands Actions*

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

**START RECORDING**

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

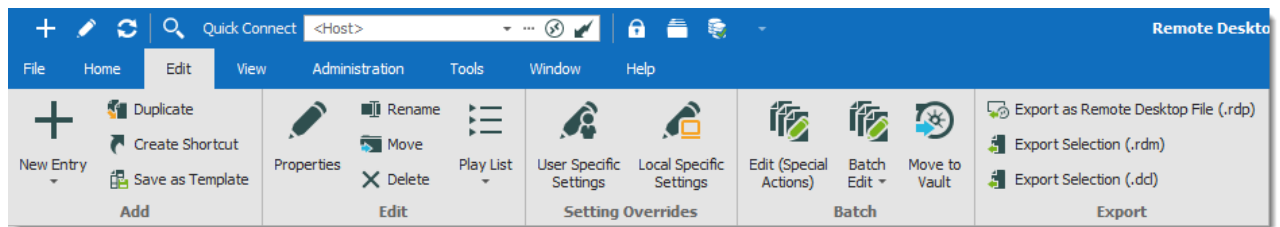


OPTION	DESCRIPTION
<b>Log file (plain text)</b>	Will record all of the activity in the SSH session using a text format.

## 6.5 Edit

### DESCRIPTION

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



*Ribbon - Edit*

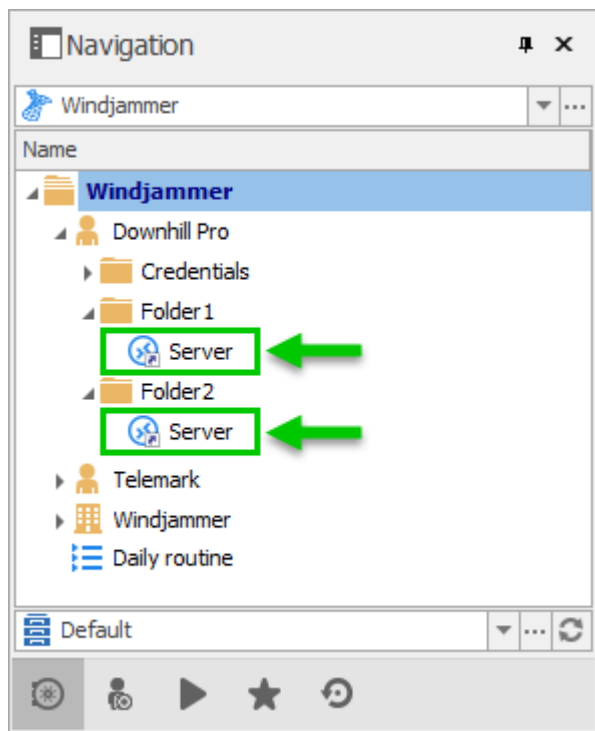
### ADD

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

A shortcut is the reiteration of an existing entry. In contrast to a duplicated entry, which has its own ID and properties, a shortcut is a link to an entry and its properties. You can create shortcuts easily by right-clicking the entry **Edit – Create Shortcut** or by using the aforementioned button in the **Edit** tab. There are a few scenarios where a user would want to use the same entry differently, such as connecting to two different hosts with a single RDP session.

For example, it is possible to:

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



*These two entries are the exactly the same*

Entries reiterated this way also have both folder paths indicated in their Folder field in their properties, the paths are separated by a semi-colon.



There is no visual differences between the shortcut and the original entry. Therefore, you'll need to delete all entries to completely remove said entry. You will be asked for confirmation when attempting to delete said shortcut.

## EDIT

OPTION	DESCRIPTION
<b>Properties</b>	Edit the properties of the selected entry.
<b>Rename</b>	Rename the selected entry.
<b>Move</b>	Move the selected entry to another folder.
<b>Delete</b>	Delete the selected entry. A confirmation dialog is displayed to confirm the action.
<b>Play List</b>	Use the various play list features.

The **Play List** feature in Remote Desktop Manager is a lot like a music play list. It opens a list of entries, in a specific order, automatically. The Play List can be used to create groups of sessions for a specific task or for security reasons. You can build your own Play List and start all entries from a Play List at the same time.

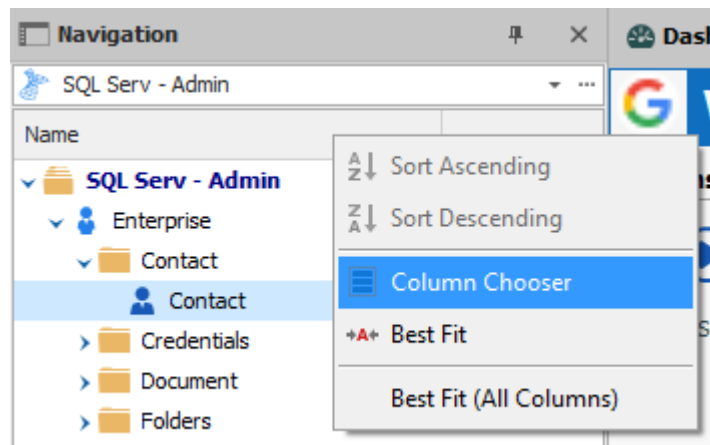
- [Create and Edit a Play List](#)
- [Using a Play List](#)

## SETTING OVERRIDES

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



A Specific Settings column can be added in the Navigation Pane. **Right-click** on the column **Name** in the Navigation Pane and select **Column Chooser**. **Double-Click** on **Specific Settings** to add the column. Now, if there is a specific setting applied to an entry, it is displayed next to the entry's name.



*Navigation Pane - Column Chooser*

## BATCH

OPTION	DESCRIPTION
<b>Edit (Special Actions)</b>	Perform special actions on the selected entries, such as change the type, run a script, and more. For more information, please consult the <a href="#">Batch Actions Samples</a> .
<b>Batch Edit</b>	Perform an action on multiple entries at once. This is particularly useful for doing mass modifications of entries (such as changing the display mode after modifying the workspace or their credential entries when changing your passwords). Multiple entries must be selected for this feature to be visible. For more information, please consult the <a href="#">Batch Edit</a> topic.
<b>Move to Vault</b>	Transfer the selected entries to another Vault in the database.

## EXPORT

OPTION	DESCRIPTION
<b>Export Entry as Remote Desktop File (.rdp)</b>	Export the selected entries in a Remote Desktop File (.rdp) format.
<b>Export Selection (.rdm)</b>	Export the selected entries in a .rdm file that can then be imported into any Remote Desktop Manager data source. You could choose to include the credentials of your entry in your export format and secure your file with a master key.

## 6.5.1 Entries

### 6.5.1.1 Checkout system

## DESCRIPTION

The **Checkout** system locks an entry while it is being used or modified. It prevents users from using or editing an entry at the same time.

The checkout system can be enabled for **sessions**, **documents**, **credentials**, and **information entries**.

You can set the check out mode at the root, folder or entry level.



This feature is only available when using [SQL Server](#) or [Devolutions Password Server](#) data sources.

## CHECKOUT SYSTEM OVERVIEW

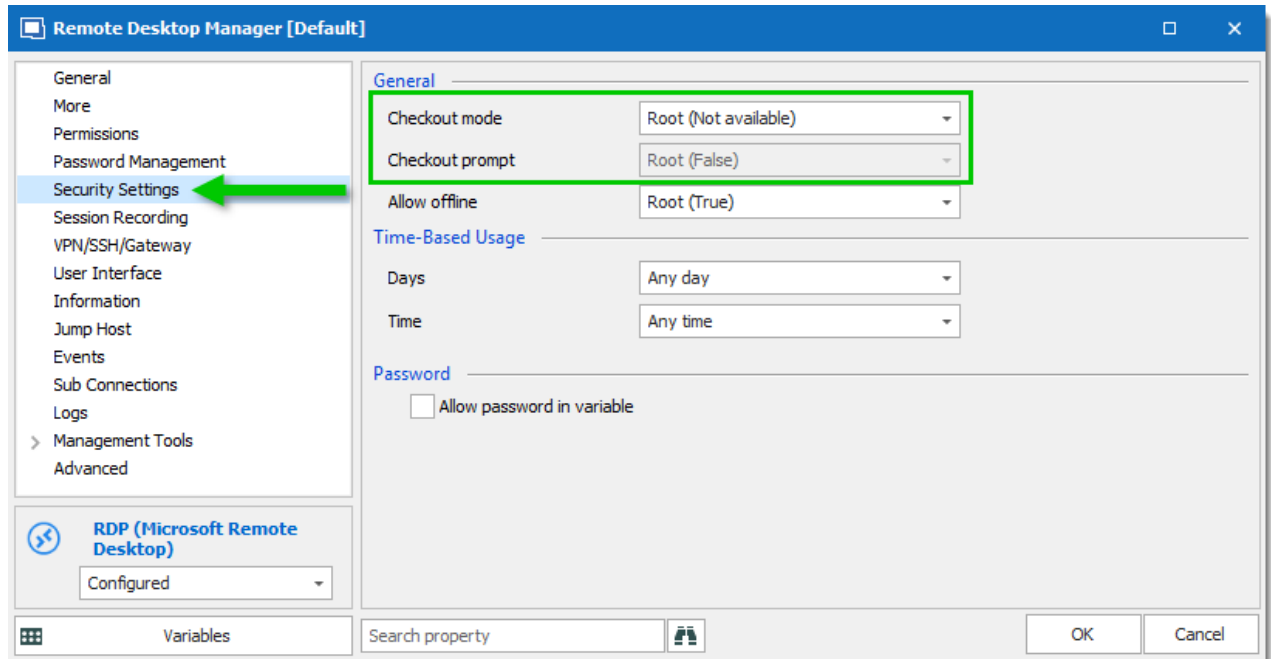
*Learn more about checkout modes and setting check out on the root and folders*

## USE MANUAL CHECKOUT MODE

*Configure Manual mode and avoid some common mistakes*

## SETTINGS

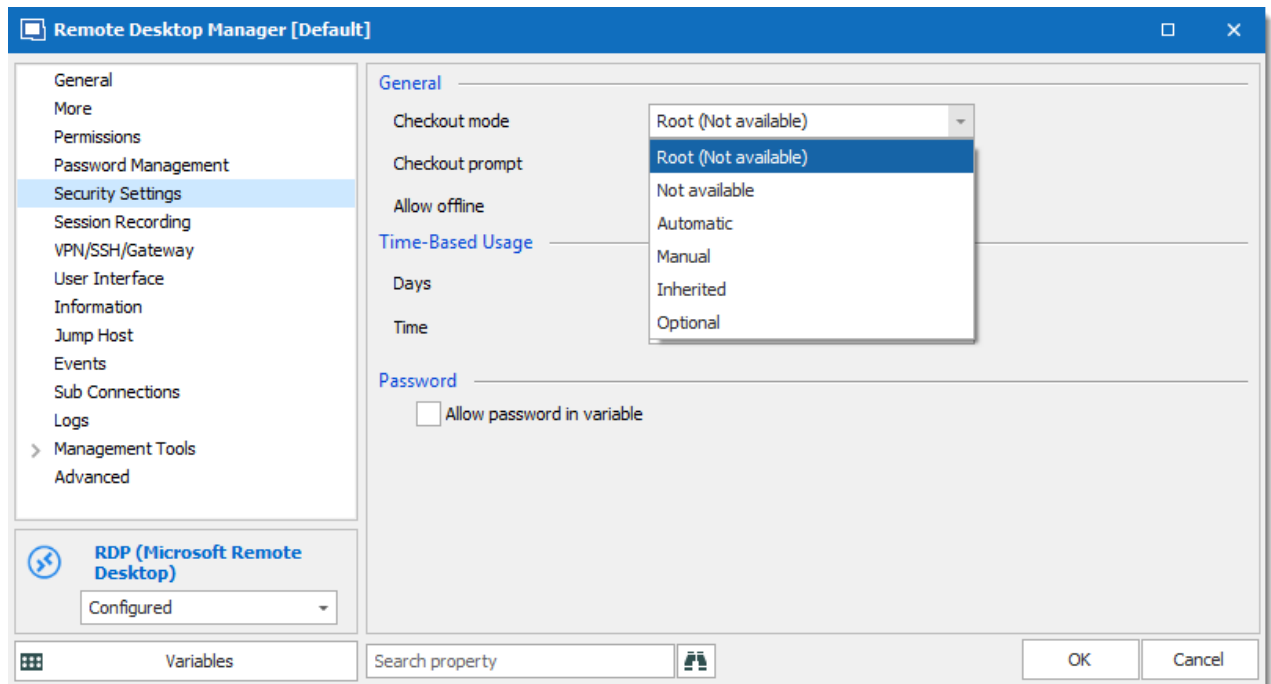
To access the check out system, edit an entry that supports checkout, and navigate to the **Security** section.



Entry properties – Security – Checkout settings

## CHECKOUT MODE

**Checkout mode** enables or disables the checkout system. It also decides how the checkout mode functions.



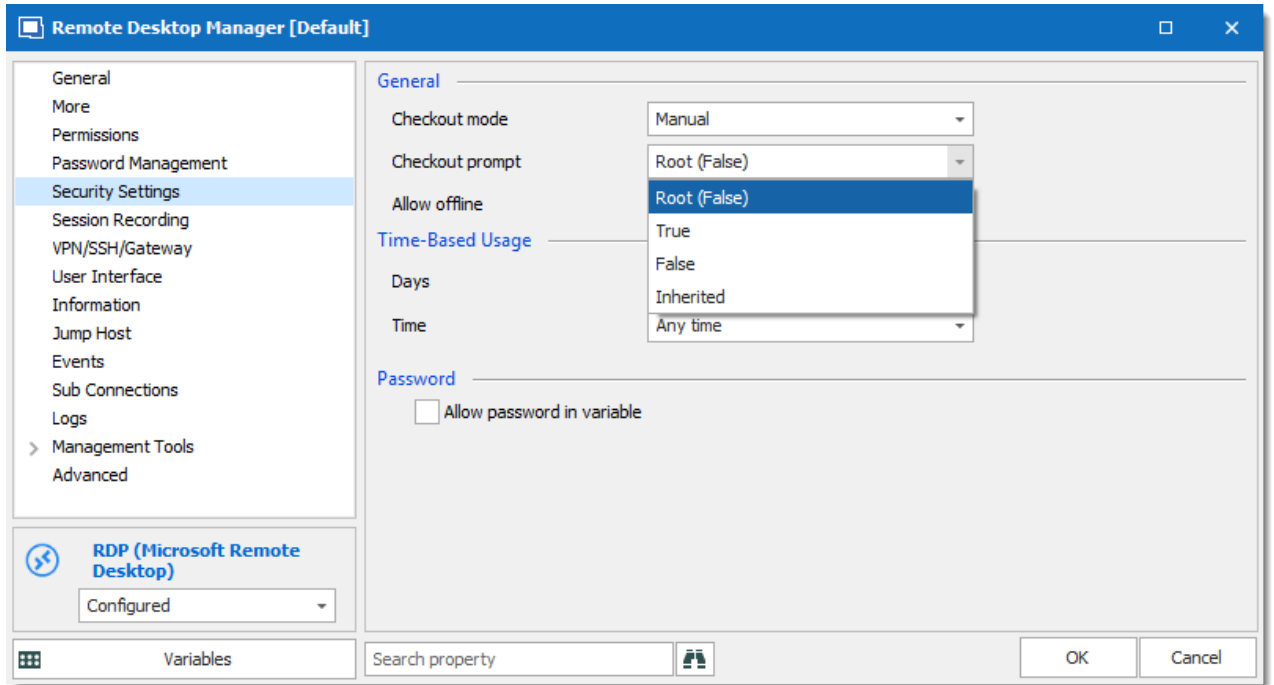
Checkout mode

OPTION	DESCRIPTION
<b>Root</b>	Inherits the checkout mode setting from the root folder.
<b>Not available</b>	Disables the checkout system.
<b>Automatic</b>	Checks out an entry automatically when the entry is opened and automatically checks the entry in when the entry is closed. User can edit properties without checking out the entry.
<b>Manual</b>	Users need to check out the entry manually prior to opening or editing the entry. No action can be performed without checking out the entry.
<b>Inherited</b>	Inherits the check out mode from the parent folder.
<b>Optional</b>	Offers the option to check out an entry manually or use (open and edit) the entry without checking it out.

## CHECKOUT PROMPT

**Checkout prompt** sets if a user must enter a comment when they check out the entry. Administrators can monitor the comments through the logs available on the entry or Activity Logs.





*Checkout required*

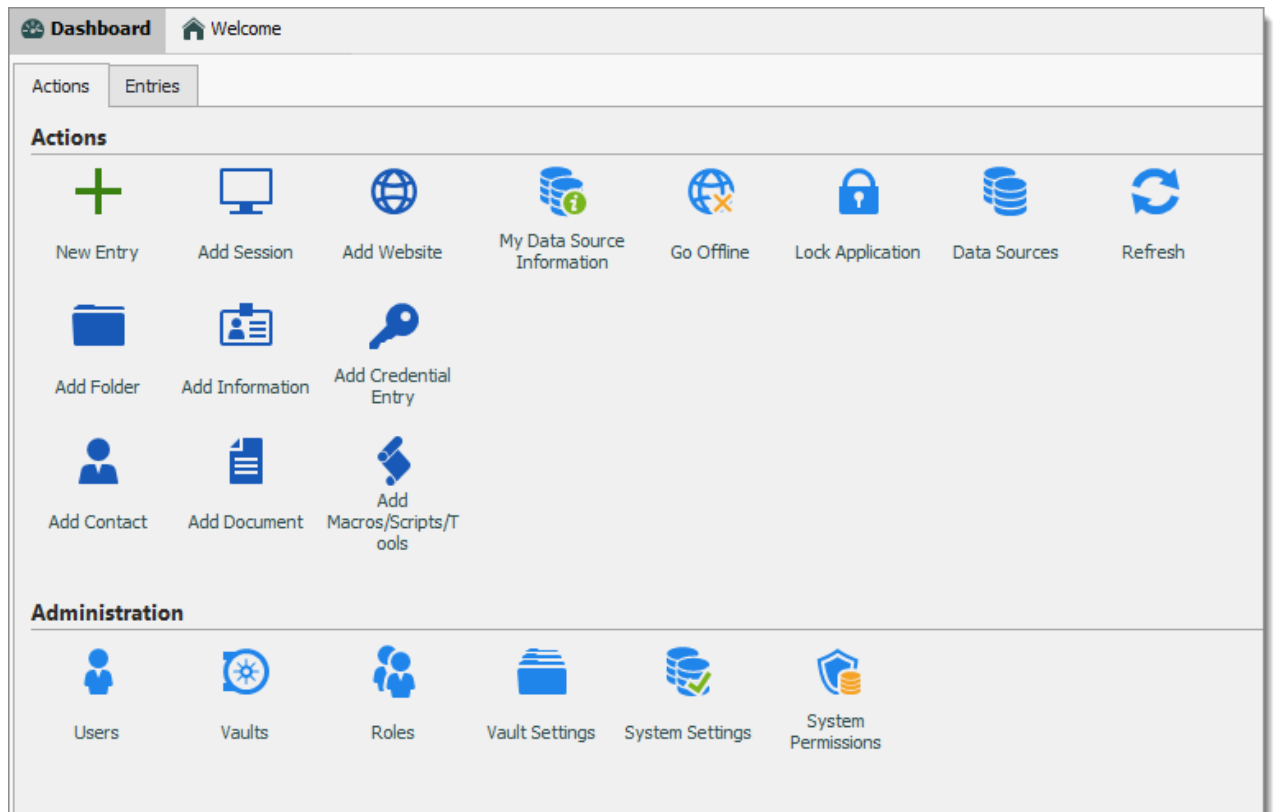
OPTION	DESCRIPTION
<b>Root</b>	Uses the checkout prompt setting from the root folder.
<b>True</b>	Prompts the user for comment when they checkout an entry.
<b>False</b>	Removes the prompt for comment.
<b>Inherited</b>	Inherits the setting from a parent folder.

## VAULT SETTING

The checkout system **Vault** refer to the settings in the vault root folder.

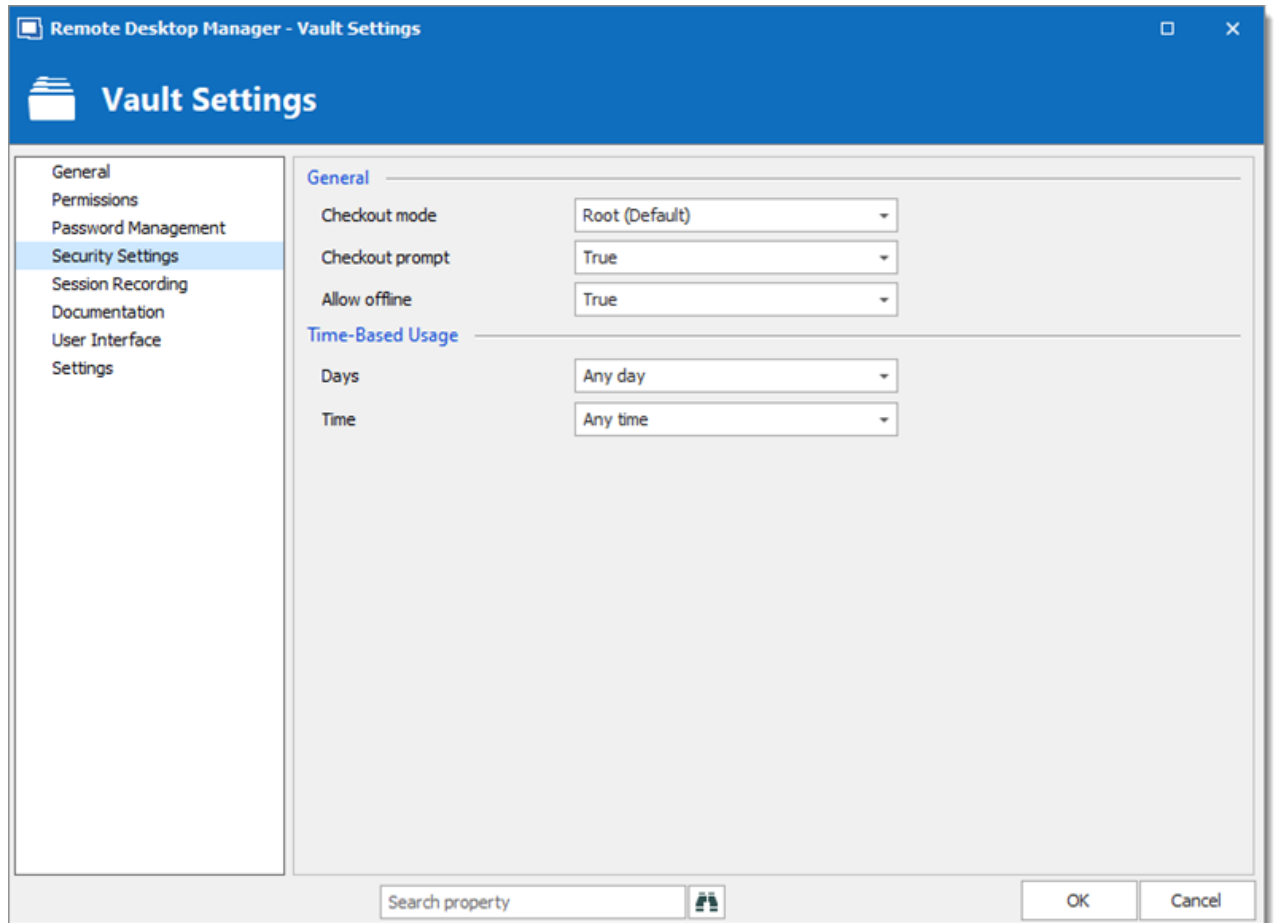
To set the checkout system vault settings:

1. Select the vault root folder in the **navigation pane**.
2. Click on the **Vault Settings** button in the **Dashboard**.



*Access the Vault Settings*

3. In the vault settings, navigate to the **Security** section.



*Checkout system - Vault Folder*

### 6.5.1.2 Credential Redirection

## DESCRIPTION

Some tools do not provide an Application Programming Interface (API) or support command line parameters to interact with them. 1Password, Firefox Password Manager, Google Password Manager and LastPass are such tools.

In order to leave the credentials in the external tool, and be able to use these credentials with Remote Desktop Manager, we have implemented a mechanism to request the credentials from the tool, then redirect them to a chosen resource.

This is achieved by running a local-access only applicative web server, then displaying a page that will allow you to store the credentials in your Credential repository. Remote Desktop Manager redirects the credentials from your chosen repository to the remote resource.

## PRE-REQUISITES

- The tool must be installed on your computer or used with a web browser as an extension.
- The browser extension for your Credential repository must be installed and enabled. Follow your repository documentation for details (see [below](#) for the URLs that are currently valid).

## PROCEDURE

There are three steps:

1. Create the credential entry.
2. Use a link to these credentials in a Remote Desktop Manager entry.
3. Open the session and use your provider to fill in the credentials.

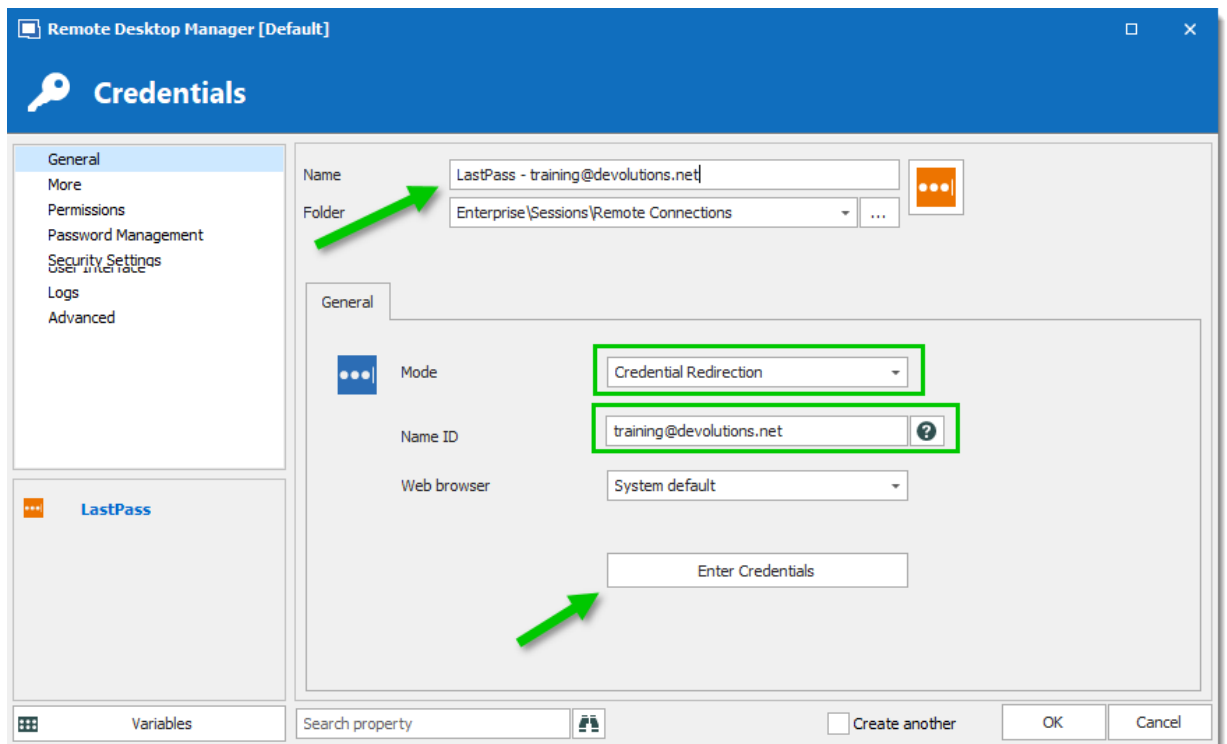
We will use LastPass in our example, but the steps are the same for 1Password.



Your chosen tool may require to be unlocked once or multiple times depending on your configuration. These steps are not covered by this guide as it may change for each installation.

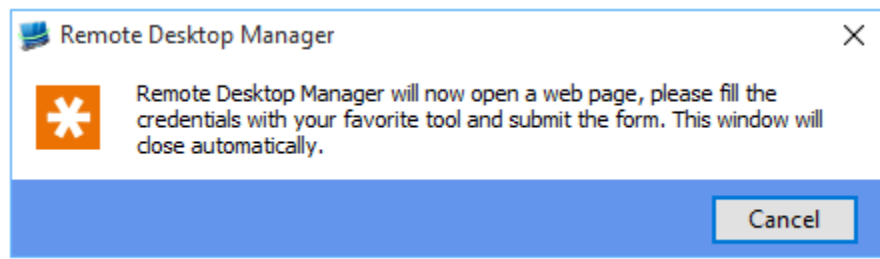
## CREATING THE CREDENTIAL ENTRY

1. Create a new **LastPass** entry.
2. Enter a name for your LastPass entry.
3. Select the option Credential redirection.
4. Enter a **Name ID** (case sensitive). This must be unique within your LastPass repository. It will be used to identify the credentials and will be exposed as a subdirectory of the URL used to intercept the credentials.



*LastPass credential*

5. Optionally select a specific browser, or use the default one.
6. Press the Enter Credentials button. This will launch the following sequence of events.
7. Remote Desktop Manager displays the following dialog.



*RDM - LastPass*

8. The chosen browser is launched for a URL that looks like <http://127.0.0.1:8000/training@devolutions.net/login.aspx>. Notice the middle part is the **Name ID** entered previously.
9. Enter your credentials to save in the browser

10. Depending on the configuration of your provider, you have to press a keyboard combination, or press on a button for the tool to save the credentials. Please refer to the documentation of your tool for more information.

11. In Remote Desktop Manager, save your credential entry.

12. Using your password provider, confirm that the credentials are saved.

## CREATING A SESSION USING THE CREDENTIAL ENTRY

1. Create a new entry, we will use an RDP session for the example.

2. Enter a name for your RDP session.

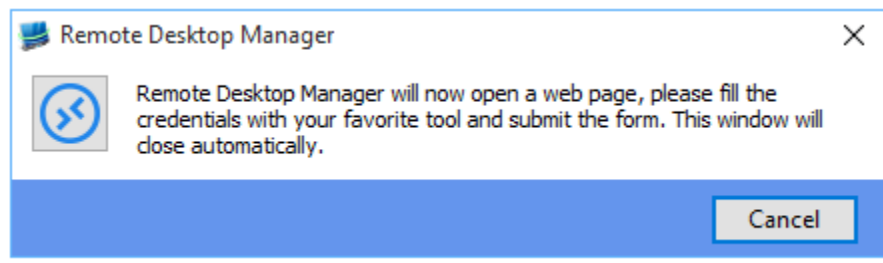
3. For **Credentials** select **Credential repository** and then your newly created credential entry

*Credential repository*

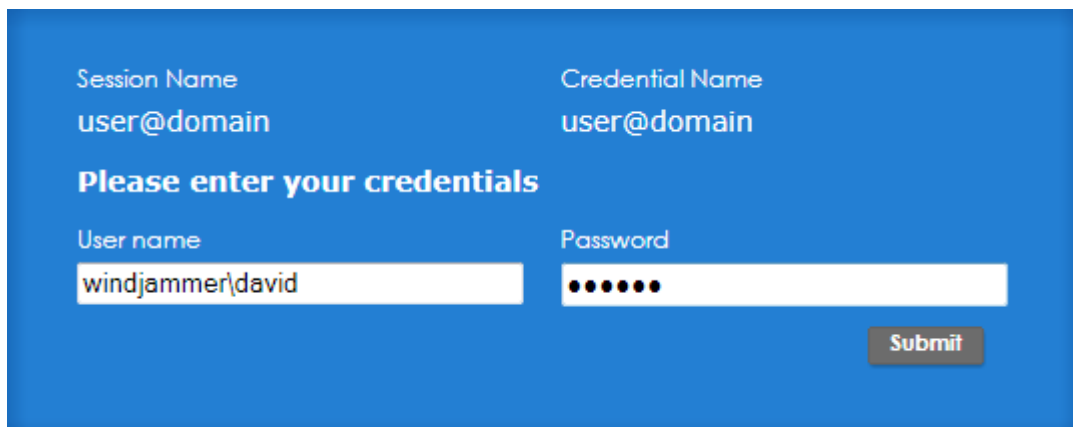
## USING THE SESSION

Select your session then launch it. This will initiate the following sequence of events:

1. Remote Desktop Manager will display this informative dialog



2. The chosen browser is launched with the URL associated to the session
3. Depending on your configuration, the credentials are entered automatically, or you have to press a key combination to initiate your tool. Please refer to the documentation of your tool for more information.

A web browser interface with a blue background. At the top, it displays "Session Name" as "user@domain" and "Credential Name" as "user@domain". Below this, a bold instruction says "Please enter your credentials". There are two input fields: "User name" containing "windjammer\david" and "Password" containing seven black dots. A "Submit" button is located at the bottom right.

4. In the web browser, press submit. The page will be closed after a delay
5. The RDP session is launched and authentication is successful

## SEE ALSO

Lastpass downloads: [https://lastpass.com/misc\\_download2.php](https://lastpass.com/misc_download2.php)

1Password instructions: <https://support.1password.com/browser-extension/>

### 6.5.1.3 Dynamic Credential Linking

## DESCRIPTION

Dynamic credential linking creates a single credential entry for a supported credential manager and use this credential with any entry type that supports the Credential repository.

## SUPPORTED CREDENTIAL MANAGERS

Here is the list of all implemented credential managers that support dynamic credential linking:

- **1Password**
- **AuthAnvil Password Server**
- **Bitwarden**
- **Dashlane**
- **Devolutions Password Hub**
- **Devolutions Password Server**
- **KeePass**
- **Keeper**
- **LastPass**
- **Mateso Password Safe**
- **PassPortal**
- **Password List**
- **Password Manager Pro**
- **Password Safe**
- **PasswordState**
- **Password Vault Manager**
- **Pleasant Password Server**



- RoboForm
- Secret Server
- Sticky Password
- TeamPass
- True Key
- Zoho Vault



A dynamic credential link can also be applied to a Folder or a VPN entry type if desired.

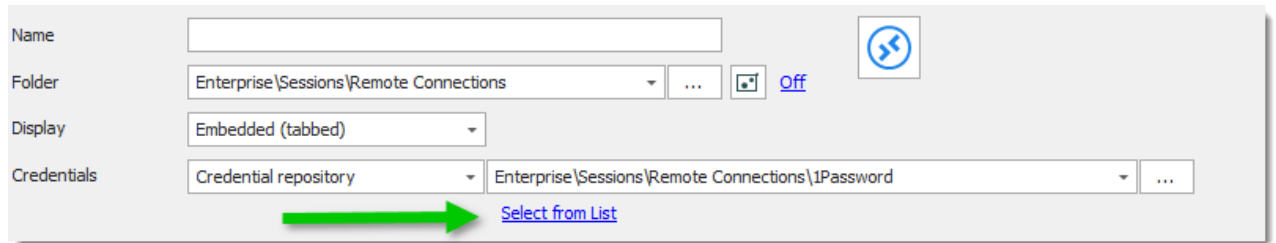
## SETTINGS

1. Create a credential entry and check **Always prompt with list**.

The screenshot shows the 'General' tab of the '1Password Settings' dialog. Under 'Logon Settings', the 'Mode' is set to 'Integrated'. Below this, there are fields for 'Database', 'Password', 'Title', and 'Uuid'. The 'Always prompt with list' checkbox is checked, and a green arrow points to it.

*1Password Settings*

2. When creating a entry, select **Credential repository** from the **Credentials** drop down list, then select the credential entry created in the previous step. Notice that a new action appears just below the credential selection drop down list.



Name:

Folder: Enterprise\Sessions\Remote Connections ... [Off](#)

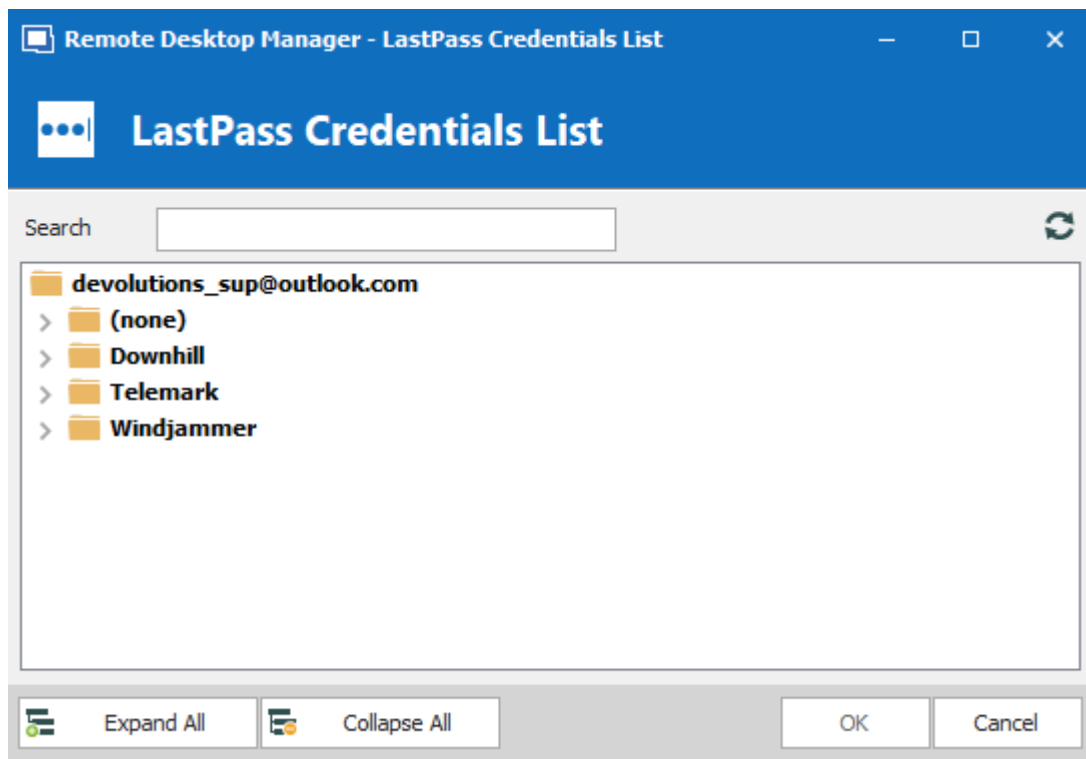
Display: Embedded (tabbed)

Credentials: Credential repository Enterprise\Sessions\Remote Connections\1Password ...

[Select from List](#)

*Select from List*

3. Select a credential from the list.



*LastPass Credentials list*

4. The link changes to the name of the credential. To remove linked credential and bring back automatic list prompt, simply click on the "X".



Name:

Folder: LAB Environment\by Services / Protocols\Credentials\Lastpass\LP Standard - E... ... [Off](#)

Display: Embedded (tabbed)

Credentials: Credential repository LAB Environment\by Services / Protocols\Credentials\Lastpass\LP Standard - E... ...

[X ted@telemark](#)

*Name of the credential*

## 6.5.2 Edit

### 6.5.2.1 Play List

#### 6.5.2.1.1 Create and Edit a Play List

## DESCRIPTION

You can create Local or Shared play List in Remote Desktop Manager. There's several methods to create or edit a Play List:

- Using the Play List Management.
- Create Play List depending on entries state and selection.
- Edit an existing Play List

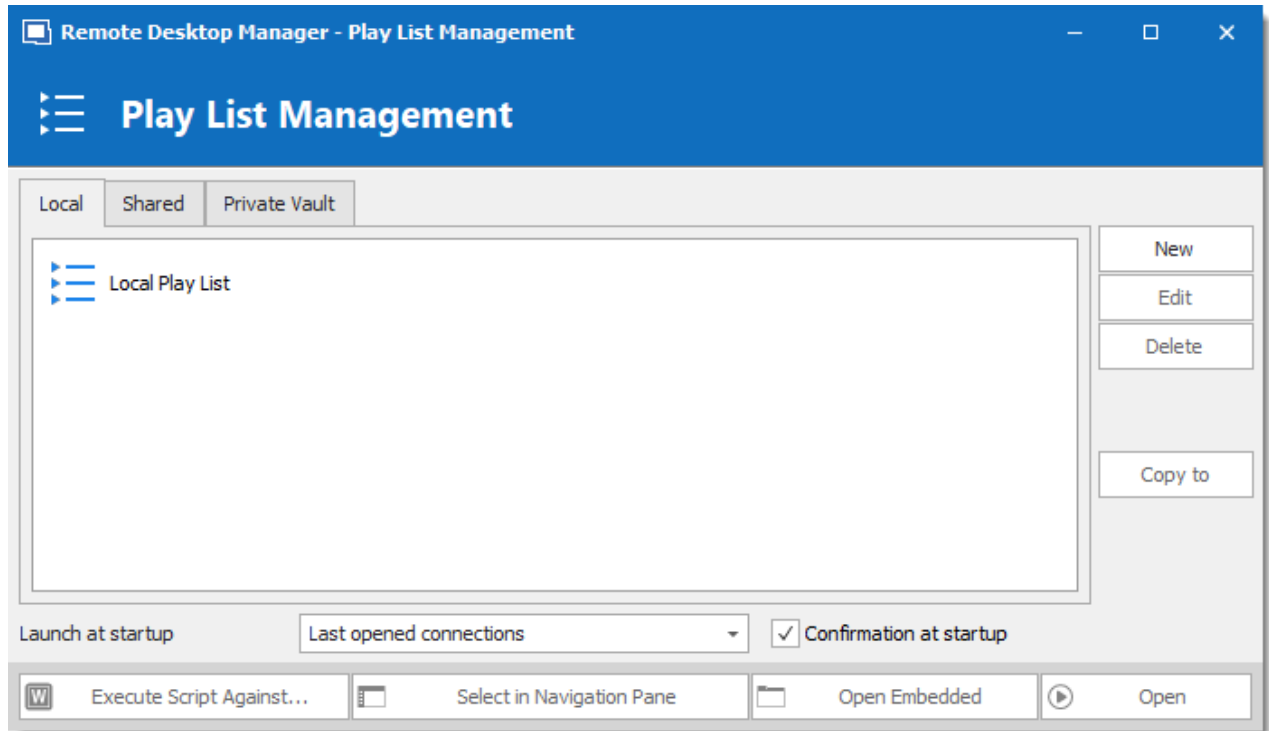


You can also use the context menu to create and edit your **Play List**. When your entries are selected, **right-click** in the Navigation Pane and select **Play List – Create Play List** or **Add to Play List**.

## SETTINGS

### USE THE PLAY LIST MANAGEMENT

You can access this by selecting Play List Management in the ribbon.

*Local Play List*

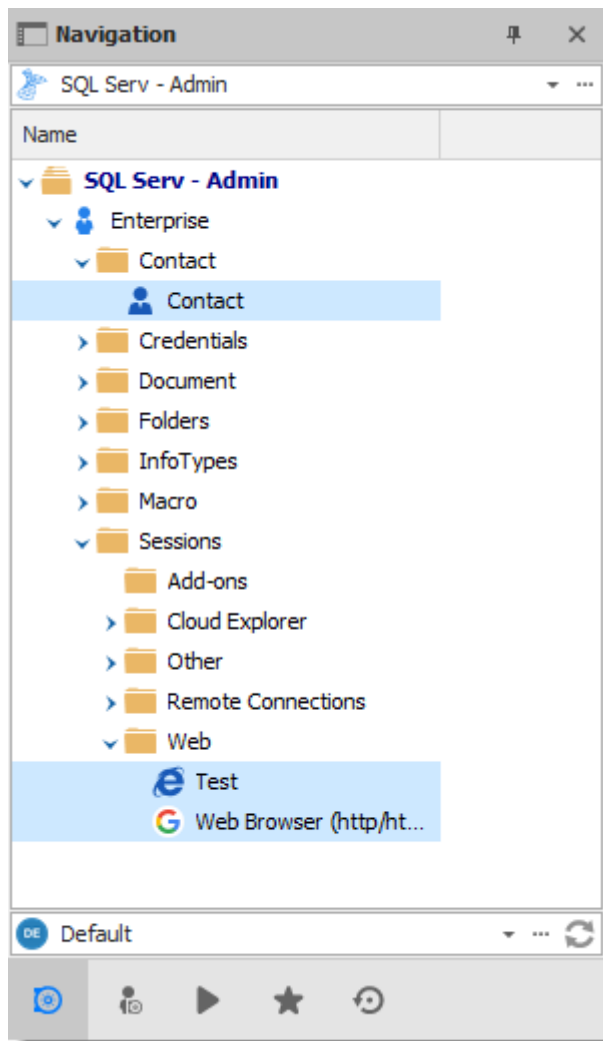
Play lists can be saved three different ways:

OPTION	DESCRIPTION
<b>Local</b>	The Play List is saved locally and can only be accessed as such. These can only be launched through the Play List Management.
<b>Shared</b>	The Play List is saved in the database. It can be accessed by anyone on the data source. These can be launched through the Play List Management or by using the entry itself.
<b>Private Vault</b>	The Play List is saved in your Private Vault and can only be accessed by the user. These can be launched through the Play List Management or by using the entry itself.

## ACTIONS

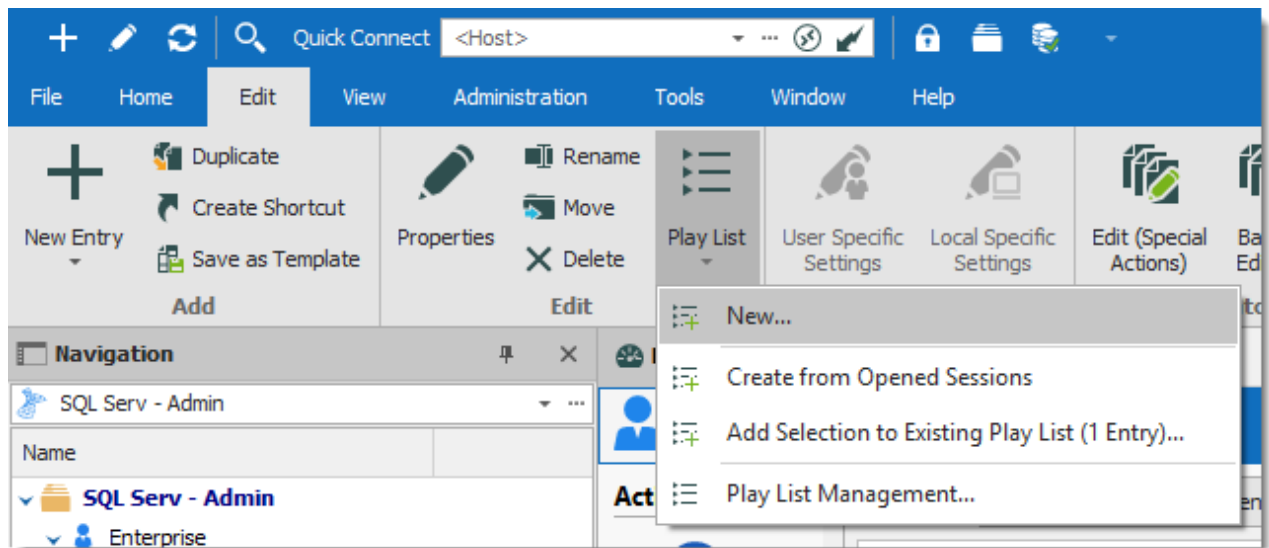
### CREATE PLAY LIST DEPENDING ON ENTRIES STATE AND SELECTION

1. If you wish to pre-determine a list of entries, select them for your Play List in the Navigation Pane.



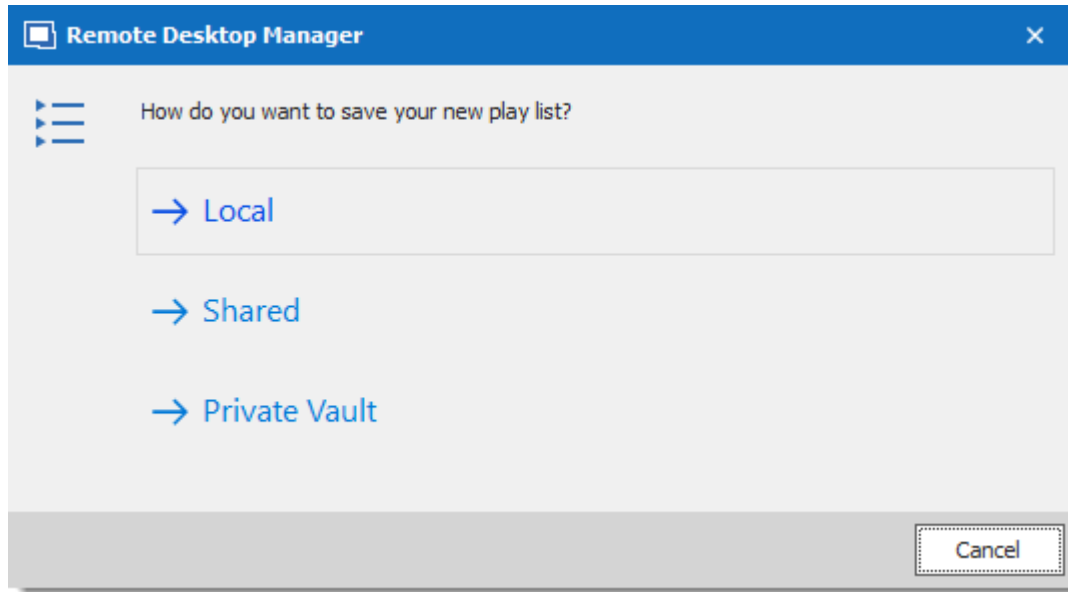
*Selected Entries in the Navigation Pane*

2. On the **Edit** ribbon menu, click **Play List**, then select whichever setting you prefer.

*Edit - Play List - New*

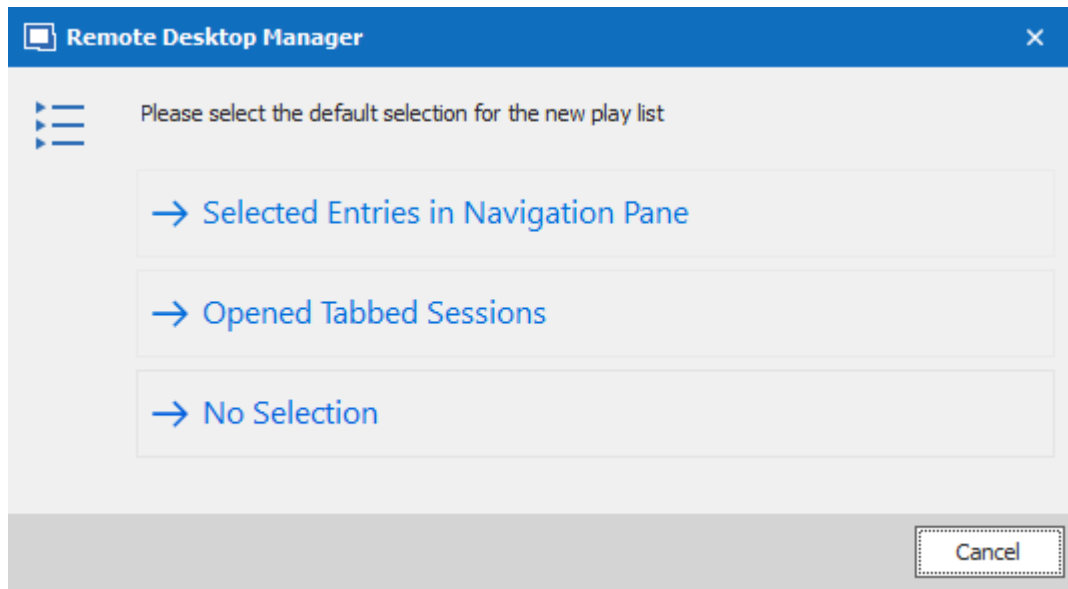
OPTION	DESCRIPTION
<b>New</b>	Creates a new Play List directly, a window prompt will ask you where you wish to save it and which selection you would like to highlight.
<b>Create from Opened Sessions</b>	Brings up the window for creating a new Play List with all currently opened session already selected for the Play List. You can select and remove additional entries if desired.
<b>Add Selection to Existing Play List (X Entry)</b>	Prompts a window where you can select currently accessible Play Lists and adds the selection in the Navigation Pane to the Play List.

3. Choose if you wish to save your Play List locally, in a shared Vault or in your Private Vault. Saving it locally will prompt a different window. This window will contain everything needed for a local Play List.



*Save New Play List*

4. The next window lets you choose how you want your current selection or opened sessions to affect your playlist.

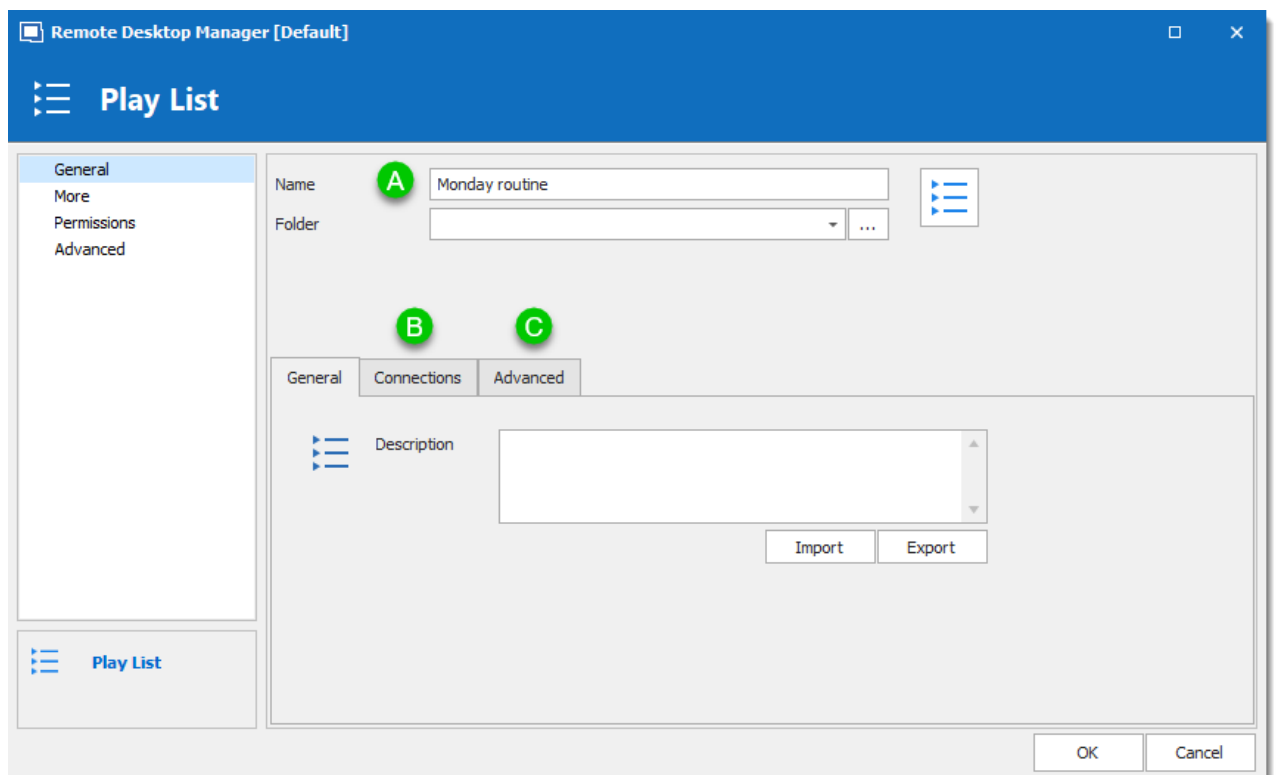


*Selected Entries in Navigation Pane*

OPTION	DESCRIPTION
<b>Selected Entries in Navigation</b>	All currently selected entries in the Navigation Pane will already be selected for your Play List. You can still add and remove entries to

OPTION	DESCRIPTION
<b>Pane</b>	the Play List if you desire.
<b>Opened Tabbed Sessions</b>	All currently opened sessions (Embedded only) will already be selected for your Play List. You can still add and remove entries to the Play List if you desire.
<b>No Selection</b>	No pre-determined selection will be taken into account, create your Play List from a fresh start.

5. a) Enter a name for your Play List.
- b) You can review, add or remove entries from the play list on the connections tab.
- c) In Advanced you can set how the entries open.



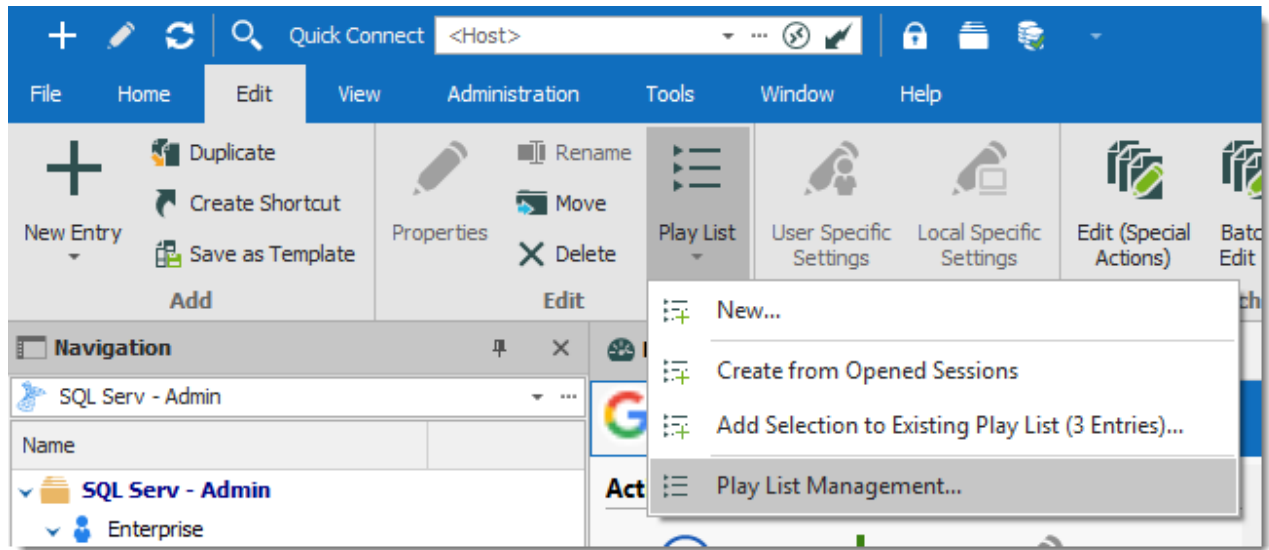
*Play List Editor*

And there you have it, your Play List is ready for use.

## EDIT EXISTING PLAY LIST

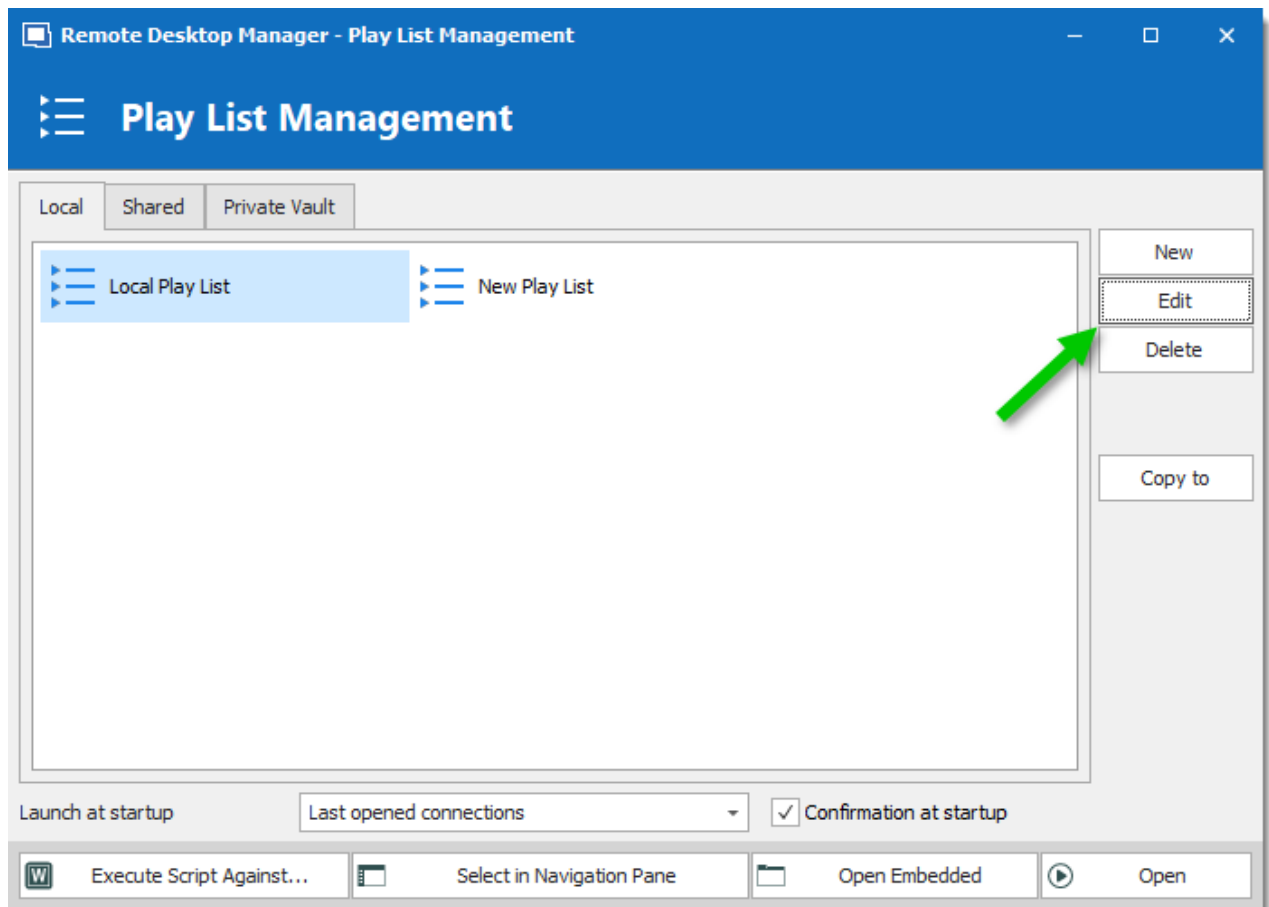


1. On Edit, click **Play List Management**.



*View - Play List Management*

2. Select the Play List you wish to modify and click **Edit**.



*Play List Management*



If the Play List is shared or saved in your Private Vault, you can also **right-click** the entry and click Properties to access it.

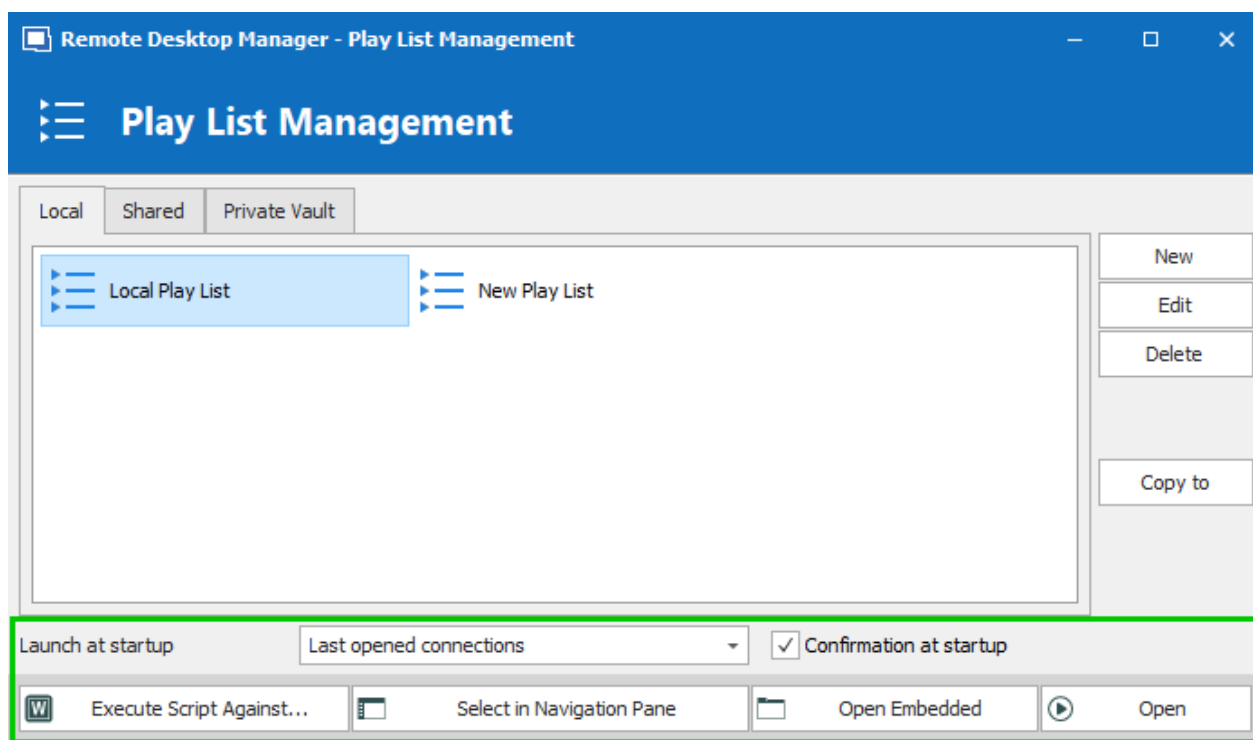
#### 6.5.2.1.2 Play List Management

## SETTINGS

### USING A PLAY LIST

First, open your Play List Management **Edit – Play List – Play List Management**.

There are five methods to using your Play List.



*Default Mode*

OPTION	DESCRIPTION
<b>Open</b>	Launch the selected Play List.

OPTION	DESCRIPTION
<b>Open Embedded</b>	Overrides the display selection of entries inside the Play Lists and launches them as Embedded (some entries might not support this).
<b>Select in Navigation Pane</b>	Selects all entries the Play List contains in the Navigation Pane.
<b>Execute Script Against...</b>	This will prompt for you to select the <b>Typing Macro</b> (exclusively) you wish to execute against your Play list.
<b>Launch at startup</b>	Here you can select a specific Play List you would like launched whenever the application starts. You can also default back to <b>None</b> or <b>Last opened Connections</b> .

### 6.5.3 Setting Overrides

#### 6.5.3.1 Specific Settings

## DESCRIPTION

**Specific Settings** are used to override the properties of an entry. Several settings can be overridden, such as the credentials or the display mode. There are two types of Specific Settings: user Specific Settings and local machine Specific Settings.

- **User Specific Settings** override an entry's properties for a single user.
- **Local Specific Settings** override an entry's properties for all users of a specific device.



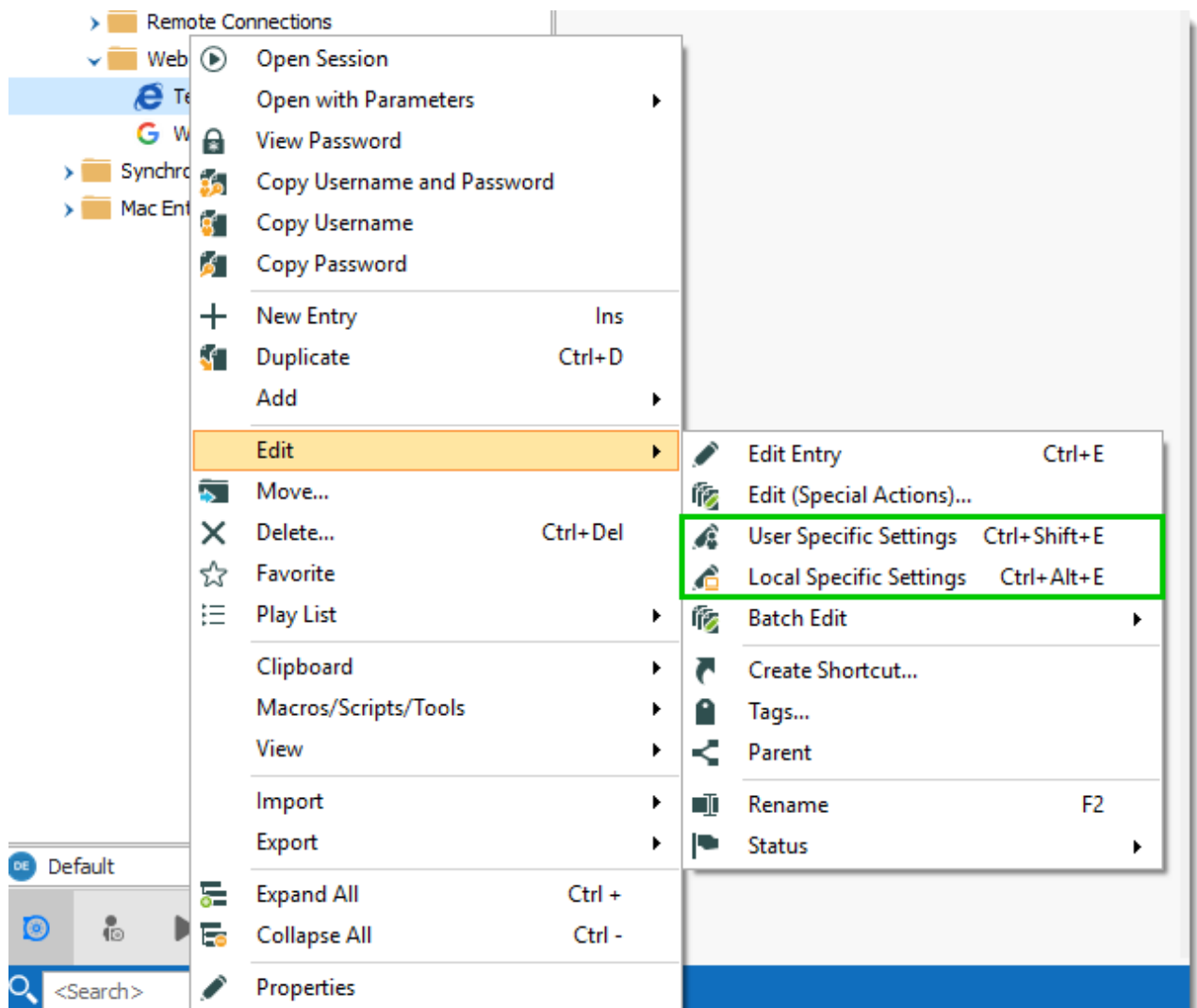
This feature is only available when using an [Advanced Data Source](#). A setting on the data source allows usage of Specific Settings. Contact your administrator if the menu is grayed out.



If both User Specific Settings and Local Specific Settings are defined on the same entry, Local Specific Settings have the priority.



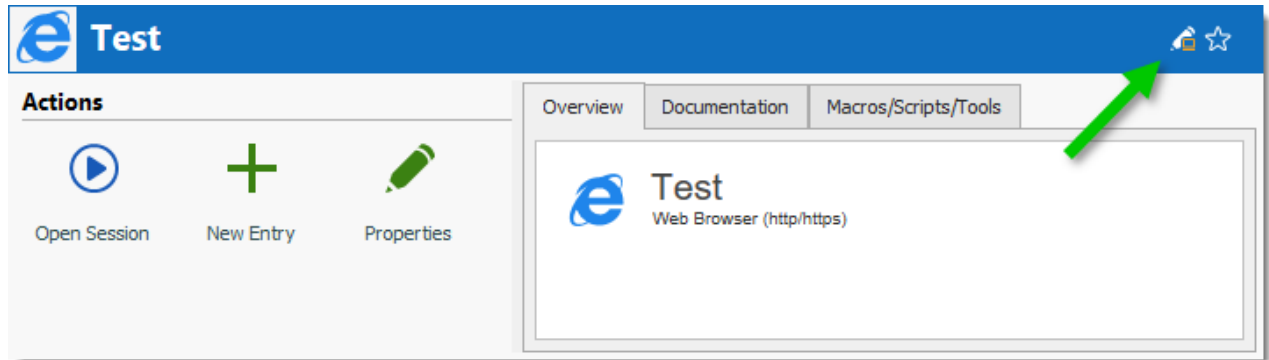
These can also be accessed by using the right-click on an entry and going to **Edit – User/Local Specific Settings**.



Context menu – Edit – User and Local Specific Settings

## SPECIFIC SETTINGS INDICATOR

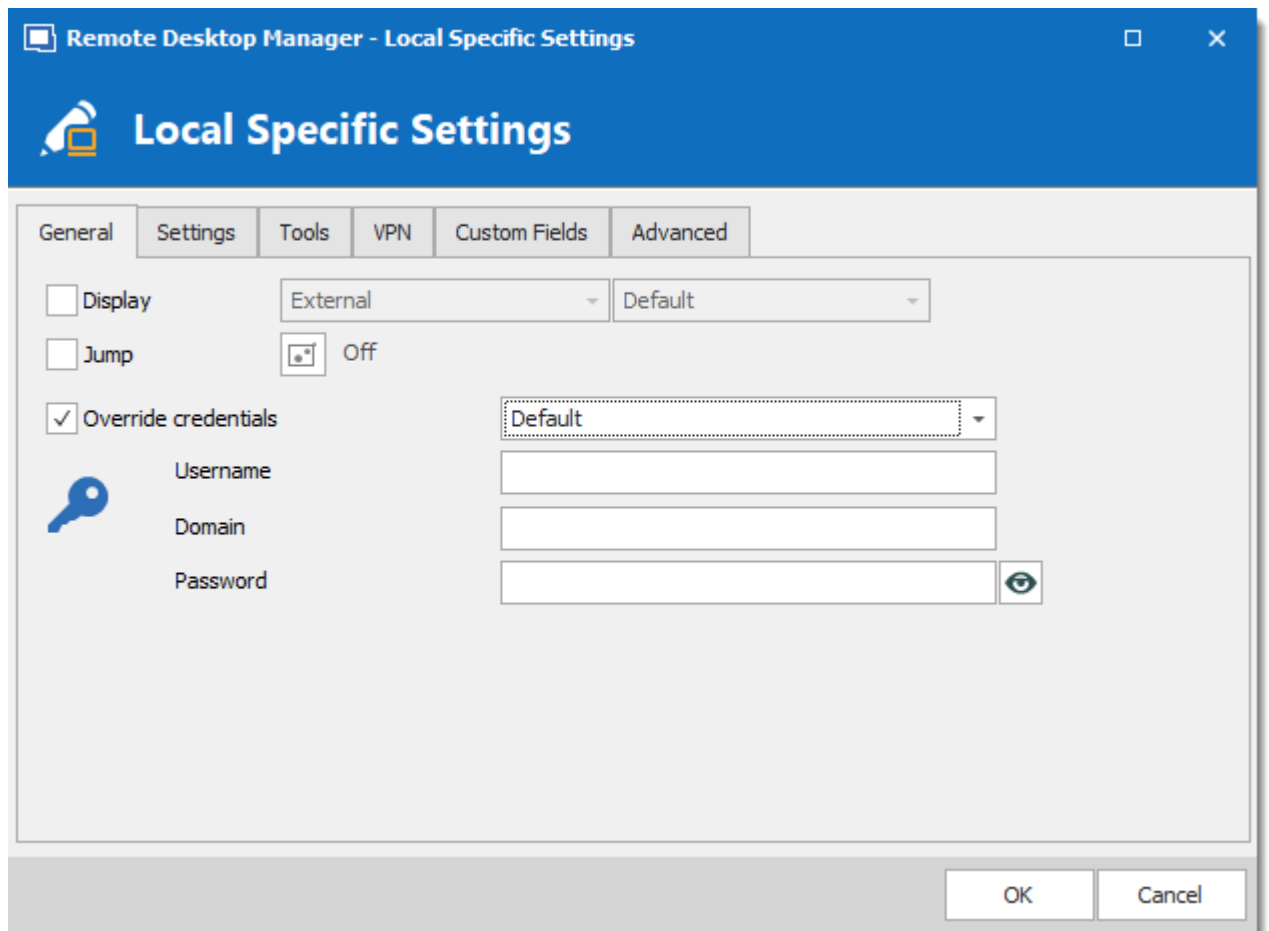
An indicator icon is displayed in the dashboard when an entry with **Specific Settings** is selected. Click on the icon to open the **Specific Settings** dialog.



*Specific Settings indicator*

## WORKFLOW

In the majority of cases, editing the **Specific Settings** displays the following dialog:



*User Specific Settings*



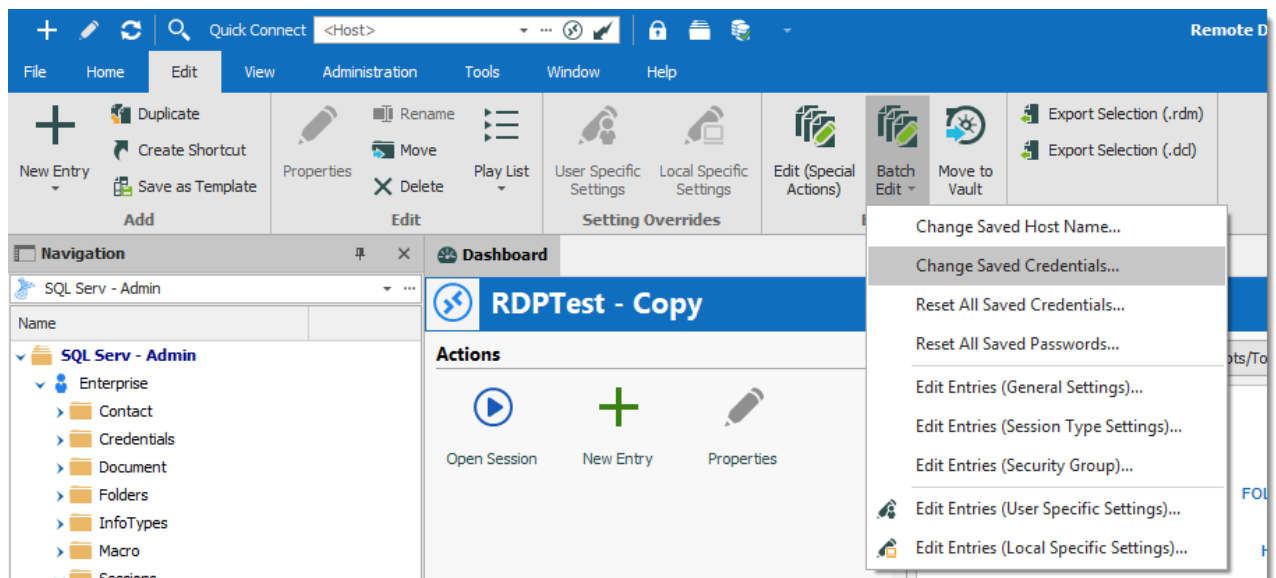
Specific settings are context sensitive, and several settings might not be available for some entry types.

## 6.5.4 Batch

### 6.5.4.1 Batch Edit

## DESCRIPTION

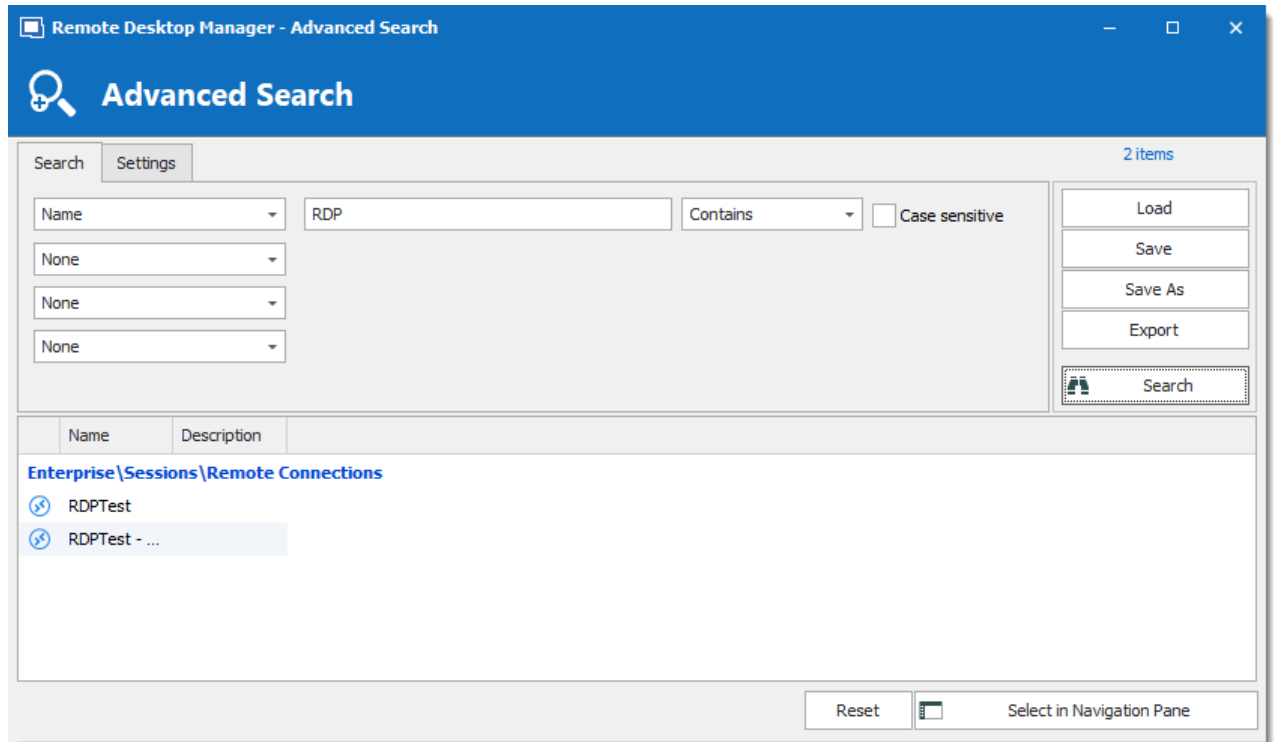
The **Batch Edit** feature changes the settings of multiple entries in one operation. For example, it can be used to remove or update the credentials of a group of sessions.



*Edit - Batch Edit*

## ADVANCED SELECTION

Select multiple entries by using the usual **Ctrl/Shift + Left-click**, etc. For a method with a little more power, use the [Advanced Search](#) feature, which allows to select multiple entries at once, based on the defined criteria. The advanced search is available in **View – Advanced Search**. If required, you can achieve similar result with the **Multi Vault Advanced Search**.



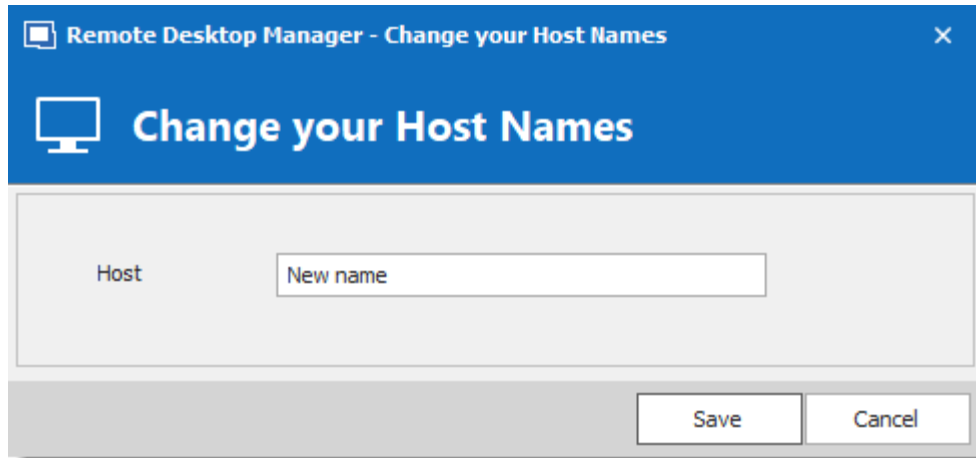
Advanced Search

Press on **Select in Navigation Pane** to select the same entries as in the **Advanced Search** dialog. Then use **Edit – Batch Edit** to edit all the selected entries.

## SETTINGS

### CHANGE SPECIFIC SETTING

You can choose to change a specific setting, for instance, the Host name.



*Change Host Name*

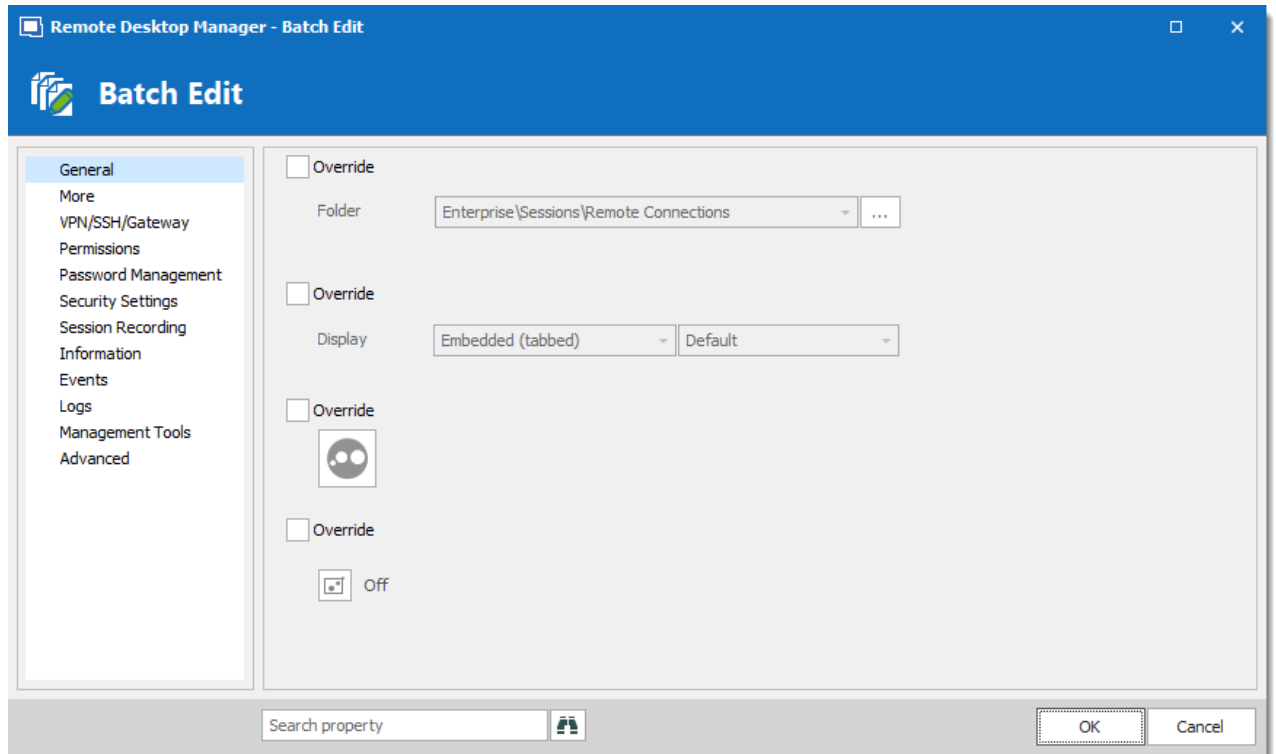
## RESET ALL SAVED CREDENTIALS OR PASSWORD

Clear all the existing credentials of all the selected sessions or specifically the password if desired.

## EDIT SESSIONS (GENERAL SETTINGS)

Edit Sessions (General Settings) allows you to change the common settings of all the selected entries.

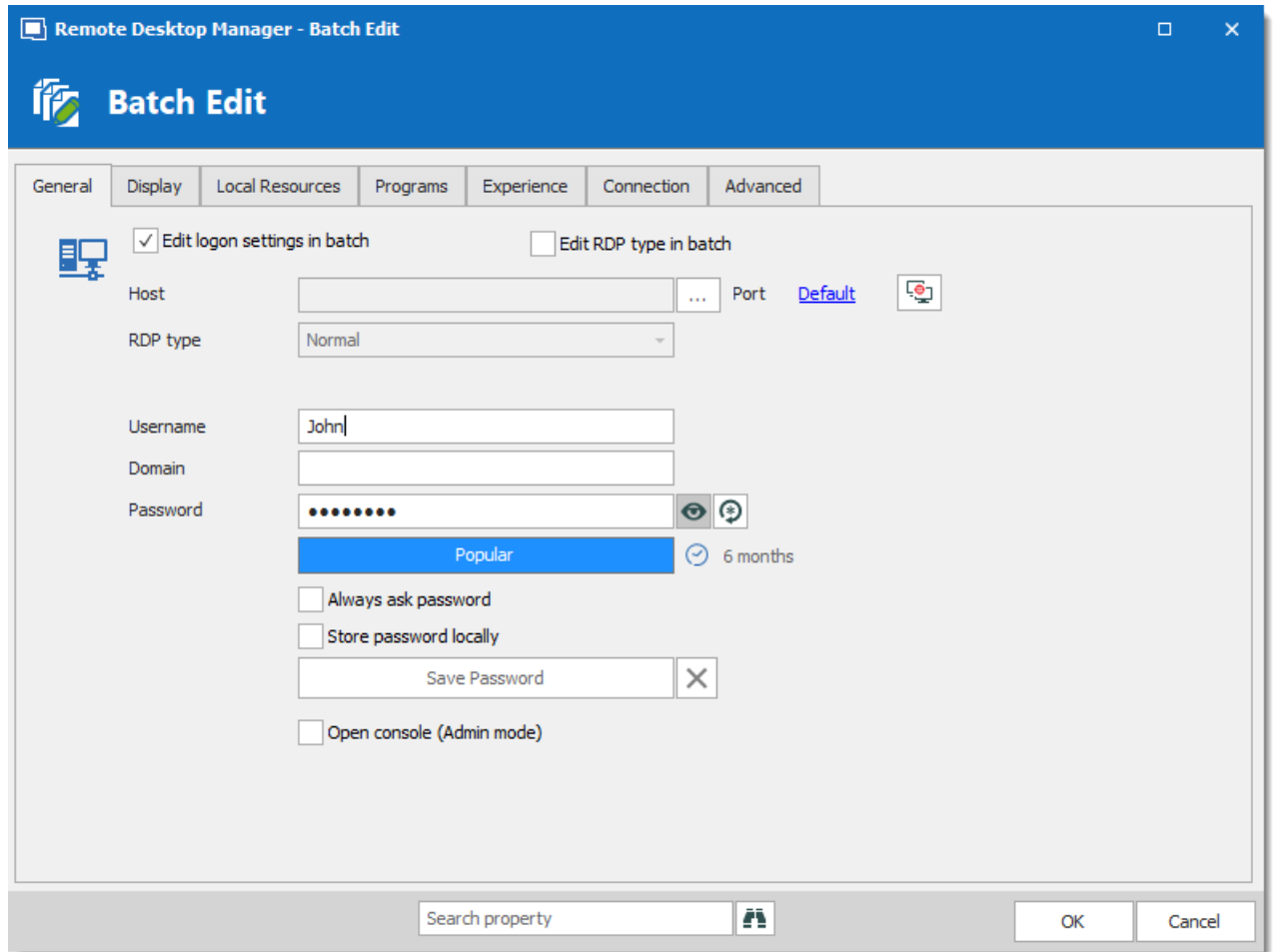




*Batch Edit – Common settings*

## EDIT SESSIONS (SESSION TYPE SETTINGS)

Change settings that are available only for specific session types, such as Microsoft RDP.



*Session Type Settings*

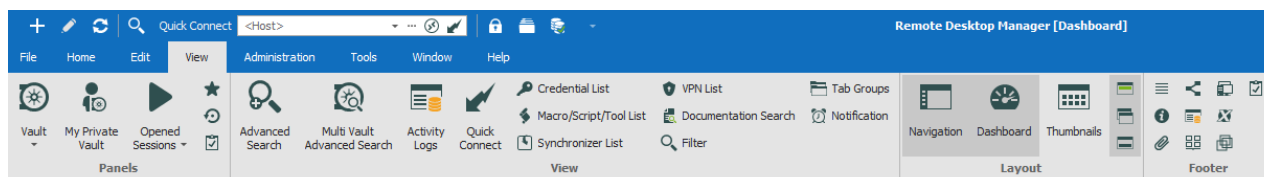
## EDIT SESSIONS (USER/LOCAL SPECIFIC SETTINGS)

[Specific Settings](#) can be modified in a batch if supported by the type of the edited entries.

## 6.6 View

### DESCRIPTION

The **View** ribbon is used to control different features regarding the views, layout and logs of Remote Desktop Manager.



Ribbon - View

Refer to the following topics for more information:

## PANELS

OPTION	DESCRIPTION
<b>Vault</b>	Access the view mode for your Navigation Pane for the current Vault.
<b>My Private Vault</b>	Display your Private Vault in the Navigation Pane.
<b>Opened Sessions</b>	Display the currently <a href="#">Opened Sessions</a> in your Navigation Pane.
<b>Favorites</b>	Display your <a href="#">Favorite</a> entries and folder in your Navigation Pane.
<b>Recent</b>	Display your <a href="#">Recently Opened Sessions</a> in your Navigation Pane.
<b>Task List</b>	Display your current <a href="#">Task List</a> .

## VIEW

OPTION	DESCRIPTION
<b>Advanced Search</b>	Use the <a href="#">Advanced Search</a> feature.
<b>Multi Vault Advanced Search</b>	This functions essentially the same way as <b>Advanced Search</b> , but it searches all the Vaults of the database.

OPTION	DESCRIPTION
<b>Activity Logs</b>	Open the <a href="#">Activity Logs</a> .
<b>Quick Connect</b>	Launch a Quick Connect session.
<b>Entry Lists</b>	Prompts a window that displays all the Credential, Macros/Scripts/Tools, VPN or Synchronizer entries in the database (restricted by user rights).
<b>Documentation Search</b>	Allows you to filter entries through their <a href="#">Documentation</a> , such as Description or Procedure.
<b>Filter</b>	This prompts a window to filter the Navigation Pane.
<b>Tab Groups</b>	Open a docked window to browse through the various Tab Groups.
<b>Notification</b>	Open an undocked window to browse through the various notifications (such as entries expired or about to be, or tasks).

## LAYOUT

OPTION	DESCRIPTION
<b>Navigation</b>	Toggle the Navigation Pane.
<b>Dashboard</b>	Toggle the Dashboard.
<b>Thumbnails</b>	Toggle the Thumbnails.
<b>Top Pane (Ribbon/Menubar)</b>	Toggle the Ribbon. (Right-click the Application header to bring it back or use <b>Alt+F11</b> ).
<b>Grouped Tab Bar</b>	Toggle the grouped tab bar. (Must have group tabs to work).

OPTION	DESCRIPTION
<b>Status Bar</b>	Toggle the Status bar.

## FOOTER

The **Footer** section allows you to show or hide the various panes that are provided with Remote Desktop Manager.



Although they are by default displayed in the footer, all those panes can be dragged and docked anywhere within Remote Desktop Manager.

### 6.6.1 Panels

#### 6.6.1.1 Task List

## DESCRIPTION

Create a list of tasks to keep track of work that needs to be done by the team. You can perform a search to filter out the list of displayed tasks. You can search by Due Date, username or by Status.

Task lists can be exported in different types of files for printing or reviewing. Right-click the task list to export in html, xls, xml or csv. You can also export filtered task lists.

Name	Status	Due Date
Create new Entries	Open	

*Task list*



This feature is only available for the following data sources: [Devolutions Password Server](#), [MariaDB](#), [MySQL](#), [SQL Azure](#), [SQL Server](#) and [SQLite](#).

## CREATING A TASK

1. Click on **Add new task**.

The screenshot shows the 'Task' tab in the application. At the top, there are filters for 'Due Date' (Last 7 Days, 6/11/2019 to 6/18/2019), 'Status', and 'Username'. Below these is a search bar. A toolbar contains icons for adding (+), editing (pencil), deleting (X), and a user icon, along with an 'Auto refresh' checkbox. The main table has columns for 'Name', 'Status', and 'Due Date'. The first row is 'Create new Entries' with status 'Open'. A green arrow points to the '+' icon in the toolbar.

*Add a task*

2. Enter your task information, like the name of the task, the priority, the due date, the description, etc.

Remote Desktop Manager - Task Management

**Task Management**

General

Name:

Entry: RDPTest

Priority: 1 ☐ Due Date: 2/24/2019 6/18/2019 - 11:39 AM

Description:

User:


Status: Open

Comment:

OK Cancel

*Task Management*

OPTION	DESCRIPTION
<b>Name</b>	Enter a custom name for the task
<b>Entry</b>	Displays the entry currently selected in the Navigation Pane. The task is assigned to this entry. Read-only field.
<b>Priority</b>	Set the priority of the task.
<b>Due date</b>	Set a deadline for the task.
<b>Description</b>	Enter a description of the task for the assigned user.
<b>User</b>	Assign a user to the task.
<b>Assign to me</b>	Click this button to assign the task to yourself.

OPTION	DESCRIPTION
<b>Clear assigned user</b> 	Clear the assigned user.
<b>Status</b>	Set a status for the task. Select between: <ul style="list-style-type: none"> <li>• <b>Open</b></li> <li>• <b>Assigned</b></li> <li>• <b>In progress</b></li> <li>• <b>Closed</b></li> <li>• <b>Done</b></li> <li>• <b>Canceled</b></li> <li>• <b>Postponed</b></li> </ul>
<b>Comment</b>	Enter a comment for the task.

## 6.6.2 View

### 6.6.2.1 Activity Logs

## DESCRIPTION

The shared session log offers a more robust solution. Through it, it's possible to monitor an opened session for all users that are using an Advanced Data Sources. The log is available for specific sessions in the context menu, in the session properties (Log tab page) and in the dashboard.

## SETTINGS

The log contains all the CRUD (add, edit and delete) operations, passwords being viewed, credentials being used by other sessions, etc...



Dashboard
Activity Logs

Date
Last 7 Days
6/11/2019
To
6/18/2019
Ticket #

Username
Folder
☒ All vaults

Message
On open comment
Local time

Machine name
On close comment

Folder	Message	On Open Comment	On Close Comment	Log Date	End Date/Time	Active Time
Jaf	Entry deleted			6/11/2019 9:32:22 ...		
Jaf\Credentials	Entry deleted			6/11/2019 9:32:22 ...		
Jaf\Sessions	Entry deleted			6/11/2019 9:32:22 ...		
Jaf\Sessions\A...	Entry deleted			6/11/2019 9:32:22 ...		
Enterprise\Sessi...	Viewed entry			6/11/2019 9:40:11 ...		
Jaf	Entry deleted			6/12/2019 7:18:50 ...		
Jaf\Sessions	Entry deleted			6/12/2019 7:18:50 ...		
Jaf\Sessions\A...	Entry deleted			6/12/2019 7:18:50 ...		
Enterprise\Sessi...	Viewed entry			6/12/2019 11:31:22...		
Enterprise\Sessi...	Viewed entry			6/12/2019 11:31:46...		
Enterprise\Sessi...	Viewed entry			6/12/2019 11:32:00...		
	Entry updated			6/12/2019 2:09:28 PM		

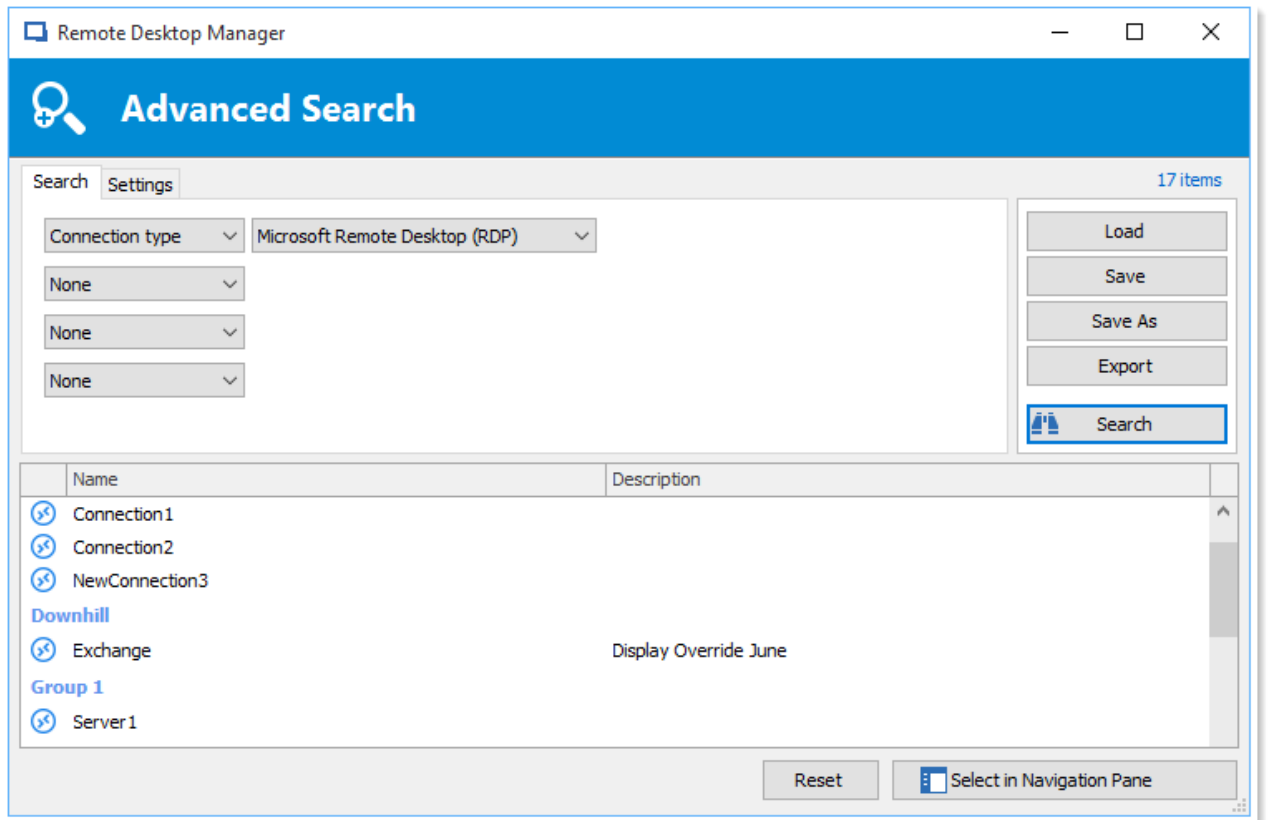
OPTION	DESCRIPTION
<b>Folder</b>	The Folder where your entry is situated.
<b>Connection</b>	The connection being used to open your entry.
<b>Message</b>	Indicate the action that was done on your entry or session.
<b>On Open Comment</b>	The Open Comment is defined in the Log tab of your session, to learn more please see Logs Options
<b>On Close Comment</b>	The Close Comment is defined in the Log tab of your session, to learn more please see Logs Options
<b>Log Date</b>	Indicate the date and time your session was opened or your entry was edited.
<b>End Date/Time</b>	Indicate the date and time when the session or entry was closed.
<b>Active Time</b>	Only available for sessions in embedded mode. It will record your session active time, meaning the time your session was opened in embedded mode and you were active in your session. If your session is opened but

OPTION	DESCRIPTION
	your view is on your Dashboard tab and not on your session tab, no Active Time will be recorded.
<b>Duration</b>	Only available for sessions in embedded mode. When sessions are opened in embedded mode the Duration time will be recorded, meaning that even if your view is on your Dashboard and you are not actively working in your session but your session tab is opened, Duration will record how long it was opened for.
<b>User</b>	Indicate the Windows username and domain.
<b>Database username</b>	Indicate the database username.
<b>Connection user</b>	Indicate the Connection user.
<b>Machine</b>	Indicate the machine name.
<b>Connection Type</b>	Indicate the connection type that was used.

#### 6.6.2.2 Advanced Search

## DESCRIPTION

The **Advanced Search** allows to search for entries based on multiple criterias.



Advanced Search Window

## SETTINGS

OPTION	DESCRIPTION
<b>Name</b>	<p>You can select between different criteria to tweak your search:</p> <ul style="list-style-type: none"> <li>• <b>Name</b></li> <li>• <b>Connection type</b></li> <li>• <b>Contact Reference</b></li> <li>• <b>Creation date</b></li> <li>• <b>Custom field</b></li> <li>• <b>Description</b></li> </ul>

OPTION	DESCRIPTION
	<ul style="list-style-type: none"> <li>• <b>Domain</b></li> <li>• <b>Group</b></li> <li>• <b>Host</b></li> <li>• <b>Is favourite</b></li> <li>• <b>Keywords/tags</b></li> <li>• <b>Last update date</b></li> <li>• <b>Name</b></li> <li>• <b>OS</b></li> <li>• <b>Password strength</b></li> <li>• <b>Security group</b></li> <li>• <b>Status</b></li> <li>• <b>Username</b></li> </ul>
<b>Load</b>	Load searches that has been previously saved.
<b>Save</b>	Allows you to save your search locally and reuse it.
<b>Save as</b>	Use to save a previously saved search but under another name.
<b>Export</b>	Export the entries of your search result as a Csv, Html, Xls or Xml file. Sensitive information will be encrypted using AES.
<b>Search</b>	Once you have selected your search criteria click on <b>Search</b> to display the search result.
<b>Reset</b>	Reset all your fields to proceed with a new Search.

OPTION	DESCRIPTION
<b>Select in Navigation Pane</b>	Select your search result in your Navigation Pane. This option can be used in combination with a Batch Edit.

There will be a drop-down list next to certain fields (ex: Name) to give you search options for:

- **Contains** - any name that includes the characters you have entered, anywhere in the field name.
- **Starts With** - any name beginning with the characters you have entered.
- **Ends With** - any name ending with the characters you have entered.
- **Exact Expression** - will find names that match every character you have entered, exactly as entered.

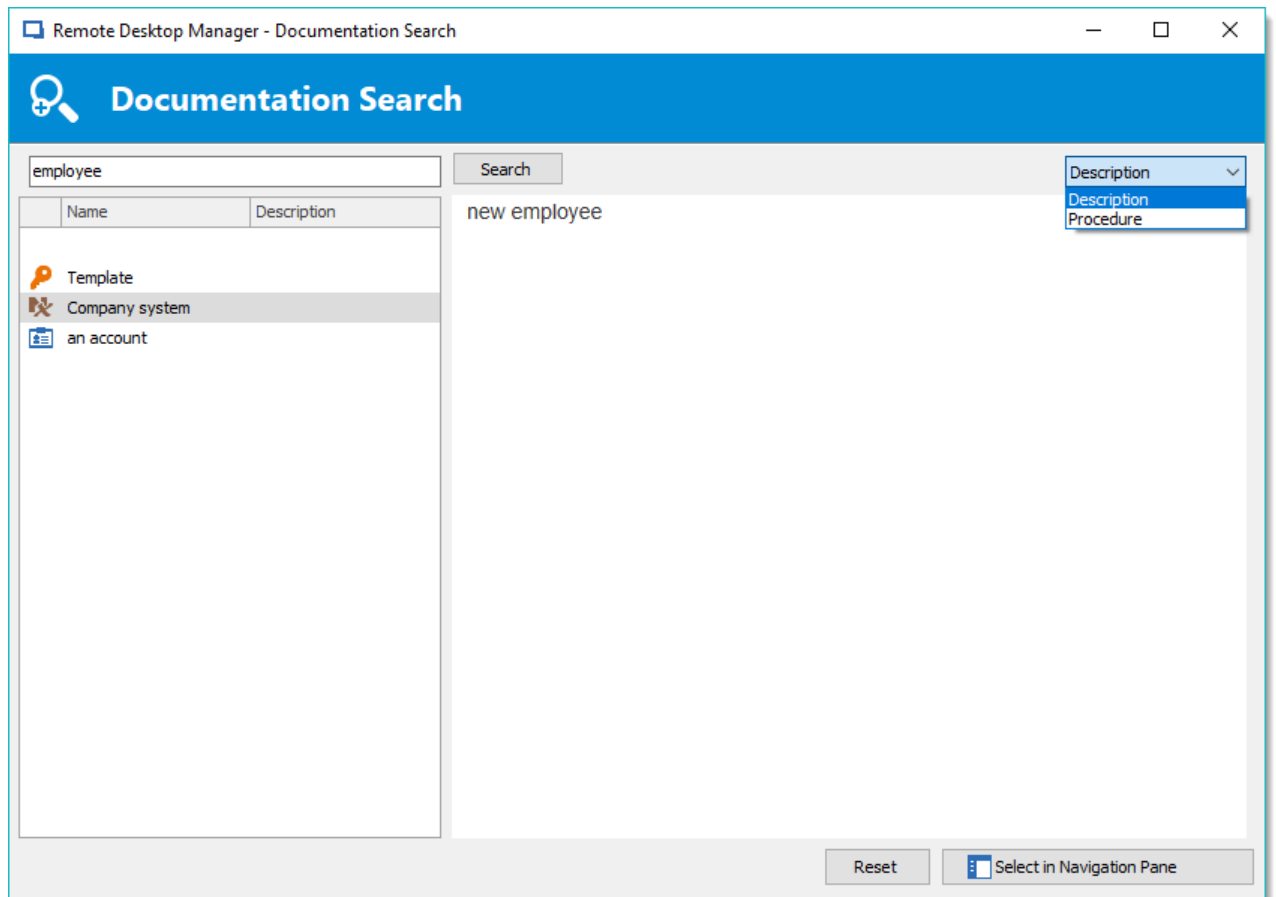
#### 6.6.2.3 Documentation Search

### DESCRIPTION

We can search documentation pages linked to entries. Documentation search provides a preview of the documentation pages, page title and related entry details. The tool searches the current repository.

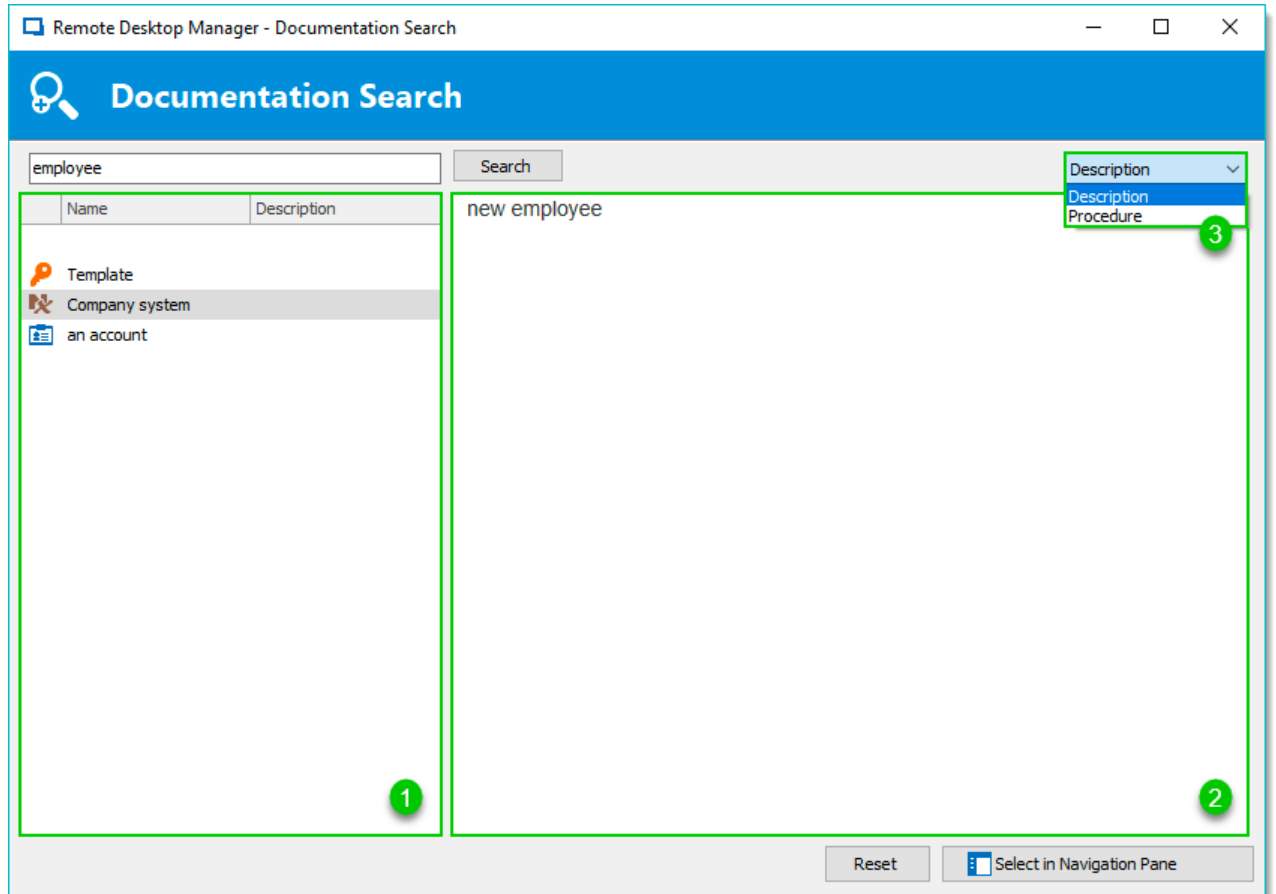


Documentation Search is available with Devolutions Password Server, MariaDB, MySQL and SQL Server data sources.



*Documentation search dialog window*

## USER INTERFACE

*Documentation search*

## USER INTERFACE

ELEMENTS	DESCRIPTION
<b>Navigation Pane (1)</b>	Lists search results by entry
<b>Content area (2)</b>	Page preview
<b>Drop down menu (3)</b>	Page title; When one entry contains multiple documentation pages with the search term, a list of the page titles is available.

## SELECT AN ENTRY

Click **Select in Navigation Pane** to choose the entry in your main tree view.

## CLEAR A SEARCH

Click **Reset** to clear the search results.

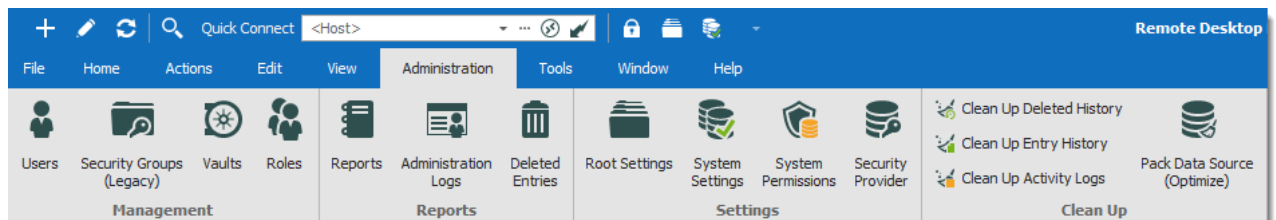
## 6.7 Administration

### DESCRIPTION

The **Administration** tab allows to manage settings and users of a data source, view reports such as the activity logs, and much more. This tab is only available to administrators of the data source.



Most features contained in the Administration tab are only available when using an [Advanced Data Source](#).



*Ribbon - Administration*

## MANAGEMENT



These feature requires an [Advanced Data Source](#).



OPTION	DESCRIPTION
<b>Users</b>	Opens the <a href="#">User Management</a> .
<b>Security Groups (Legacy)</b>	Security Groups are now a Legacy option, and although we have left documentation in the online help to help users identify it, we strongly recommend switching to Roles instead.
<b>Vaults</b>	Opens the Vault Management tab of User Management.
<b>Roles</b>	Opens the <a href="#">Role Management</a> tab of User Management.

## REPORTS



The logs feature requires an [Advanced Data Source](#).

OPTION	DESCRIPTION
<b>Reports</b>	Open the <a href="#">Reports</a> section to select which type of report best suit your current needs.
<b>Administration Logs</b>	Opens the Administration Logs.
<b>Deleted Entries</b>	Open a log of all <a href="#">Deleted Entries</a> (since last clean up).

## SETTINGS



This feature requires an [Advanced Data Source](#).

OPTION	DESCRIPTION
<b>Vault Settings</b>	Opens the Vault Settings. The Vault Root Folder is the one at the top of the navigation pane (in Tree View). It is the one from which all entries and folder stem. By default, lower level folders inherit settings and security from parent folder until reaching the vault root. Therefore, using permissions on the vault root folder allows to secure all entries below the vault root level. Refer to <a href="#">Default security for entries</a> for more information.
<b>System Settings (Data Source Settings)</b>	Opens the System Settings. There are many features here, all meant to help you customize your data source and security needs. Remember that these settings applies to all users that have access to the data source.
<b>System Permissions</b>	Modify <a href="#">System Permissions</a> .
<b>Security Provider</b>	Set up a <a href="#">Security Provider</a> for an additional layer of security.

## CLEAN UP



This feature requires an [Advanced Data Source](#).

OPTION	DESCRIPTION
<b>Clean Up Deleted History</b>	Perform a partial or full clean up of the <a href="#">Deleted History</a> .
<b>Clean Up Entry History</b>	Perform a partial or full clean up of the <a href="#">Entry History</a> .
<b>Clean Up Activity Logs</b>	Perform a partial or full clean up of the <a href="#">Activity Logs</a> . You also have the option to clean up the <b>Administration Logs</b> if desired.
<b>Pack Data Source (Optimize)</b>	The <a href="#">Pack Data Source (Optimize)</a> feature analyzes all entries, compress and save them, thus saving space in your data source.

## 6.7.1 Management

### 6.7.1.1 User Management

## DESCRIPTION

The **Users Management** allows to create and manage users and their privileges. You can set the default privileges on the user type in **Data Source Settings (System Settings)**. Remote Desktop Manager offers advanced user rights management that allows for restricting access to entries. Please note that availability of some features depends on the active data source.



This feature requires an [Advanced Data Source](#).



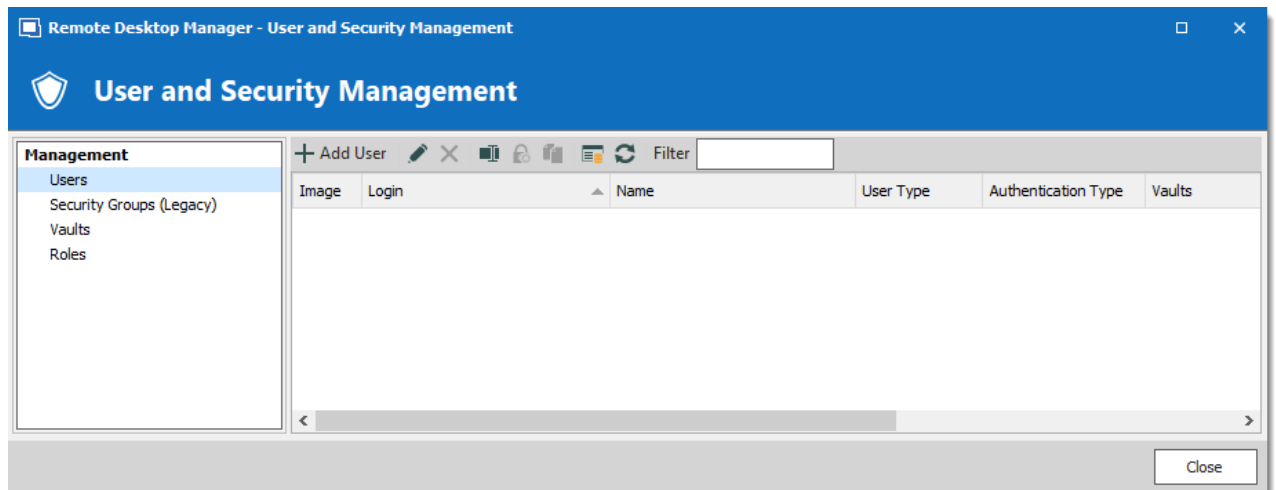
A user can be created using default security (specify the password) or [Integrated Security](#). Not all [Advanced Data Sources](#) support the use of [Integrated Security](#).



In order to create users and assign rights, you must be administrator of not only Remote Desktop Manager, but also of the underlying database.

## MANAGE USERS

To create, edit, delete, rename or otherwise manage users as a whole, simply use the buttons in the toolbar.



*User and Security Management - Toolbar*

## USER MANAGEMENT SETTINGS

### GENERAL

The screenshot shows the 'Remote Desktop Manager - User Management' window. The title bar includes a minimize button, a maximize button, and a close button. The window has a blue header with a user icon and the text 'User Management'. On the left is a sidebar with a tree view containing: General (selected), Information, Roles, Privileges, Security Groups (Legacy), Vaults, Application Access, and Settings. The main area is divided into two sections: 'General' and 'Information'. The 'General' section contains fields for ID (FAC9D92C-78BB-4B34-9D69-01EAA4AEE2DF), Authentication type (Database), Username, Password, User type (User), User license type (Default), and checkboxes for 'Integrated security (Active Directory)' (unchecked), 'Create SQL Server Login and User' (checked), and 'User must change password at next logon' (unchecked). The 'Information' section contains fields for First name, Last name, and Email. At the bottom right are 'OK' and 'Cancel' buttons.

*User Management - General*

OPTION	DESCRIPTION
<b>Authentication type</b>	<p>Select the user's authentication type:</p> <ul style="list-style-type: none"> <li>• <b>Custom (Devolutions)</b>: create a user specific to Remote Desktop Manager without creating an SQL login.</li> <li>• <b>Database (SQL Server)</b>: authenticate using the SQL login from your SQL Server.</li> </ul>
<b>Username</b>	Enter the username for the user. When using <a href="#">Integrated Security</a> the user must be selected from the directory.
<b>Integrated security (Active Directory)</b>	Specify to use Active Directory to authenticate to the data source. Applies only to SQL Server and Devolutions Password Server, depending on their configuration. For more information, please consult the <a href="#">Integrated Security</a> topic.
<b>Password</b>	Enter the user's Password. This field is disabled when using <a href="#">Integrated Security</a> .

OPTION	DESCRIPTION
<b>User type</b>	Select the type of user to create, select between: <ul style="list-style-type: none"><li>• <b>Administrator:</b> Grant full administrative rights to the user.</li><li>• <b>Read only user:</b> Grant only the view access to the user.</li><li>• <b>Restricted user:</b> Select which rights to grant to the user.</li><li>• <b>User:</b> Grant all basic rights to the user (Add, Edit, Delete).</li></ul> For more information, please consult the <a href="#">User Types</a> topic.
<b>User license type</b>	Select the license type of the user. Select between: <ul style="list-style-type: none"><li>• <b>Default</b></li><li>• <b>Connection Management</b></li><li>• <b>Password Management</b></li></ul>
<b>Full name</b>	Enter the First name and Last name of the user.
<b>Email</b>	Insert the user's email address.

## INFORMATION

The **Information** section allows to store information regarding the users, such as their name, address, and more. The Information section is divided in three sub-sections: **Details**, **Address**, **Phone**.

The screenshot shows the 'Remote Desktop Manager - User Management' window. The 'User Management' section is active, and the 'Information' tab is selected in the left sidebar. The main area displays the 'Information' tab with the following fields:

- Company:
- Job title:
- Department:
- Gravatar email:
- Language:

At the bottom right, there are 'OK' and 'Cancel' buttons.

*User Management - Information - Details*

## ROLES

Select roles to assign to the user.

The screenshot shows the 'Remote Desktop Manager - User Management' window. The 'User Management' section is active, and the 'Roles' tab is selected in the left sidebar. The main area displays the 'Roles' tab with a table of roles:

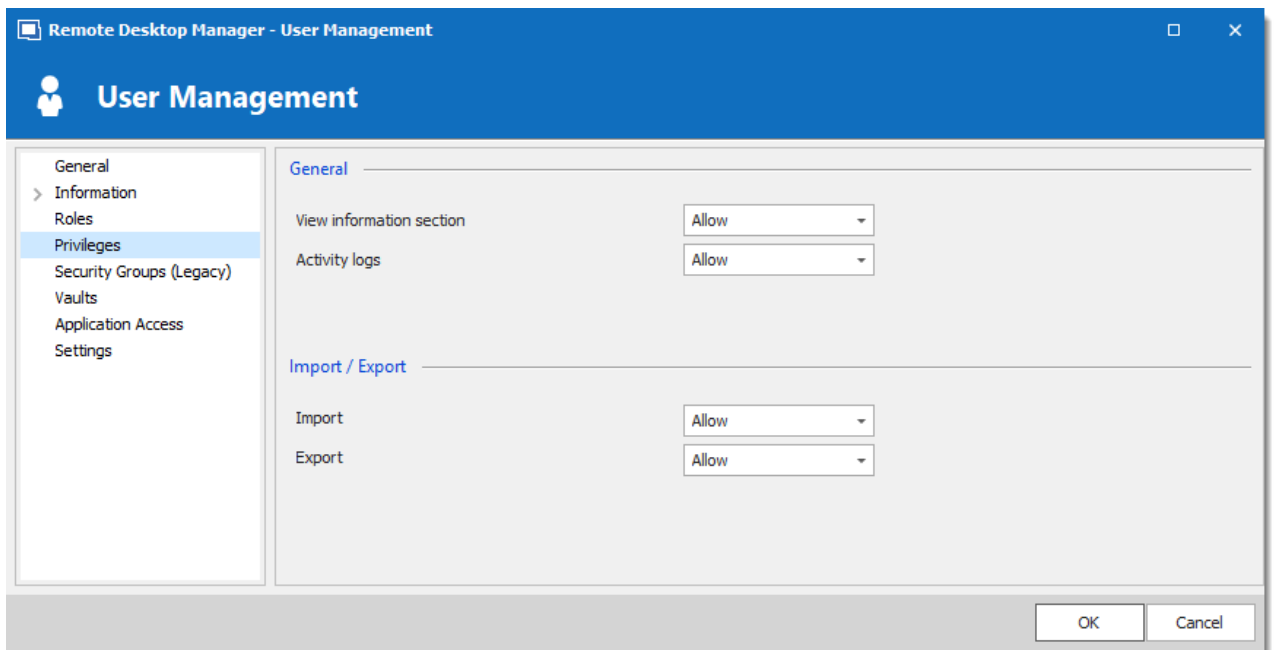
Name	Description	Is Member
Administrators		<input type="checkbox"/>
Level 1 Clearance		<input type="checkbox"/>
Level 2 Clearance		<input type="checkbox"/>

At the bottom right, there are 'OK' and 'Cancel' buttons.

*User Management - Roles*

OPTION	DESCRIPTION
<b>Roles</b>	Check the <b>Is Member</b> box to assign the role to the user. Consult <a href="#">Role Management</a> topic for more information.

## PRIVILEGES



*User Management - Privileges*

OPTION	DESCRIPTION
<b>View information section</b>	Allow the user to view the information section.
<b>Activity logs</b>	Allow the user to view the Activity logs.
<b>Import</b>	Allows the user to Import sessions (Clipboard - Paste as well).  The import menu ( <b>File – Import</b> ) and the import feature in the context menu will be grayed out if the option is not active.



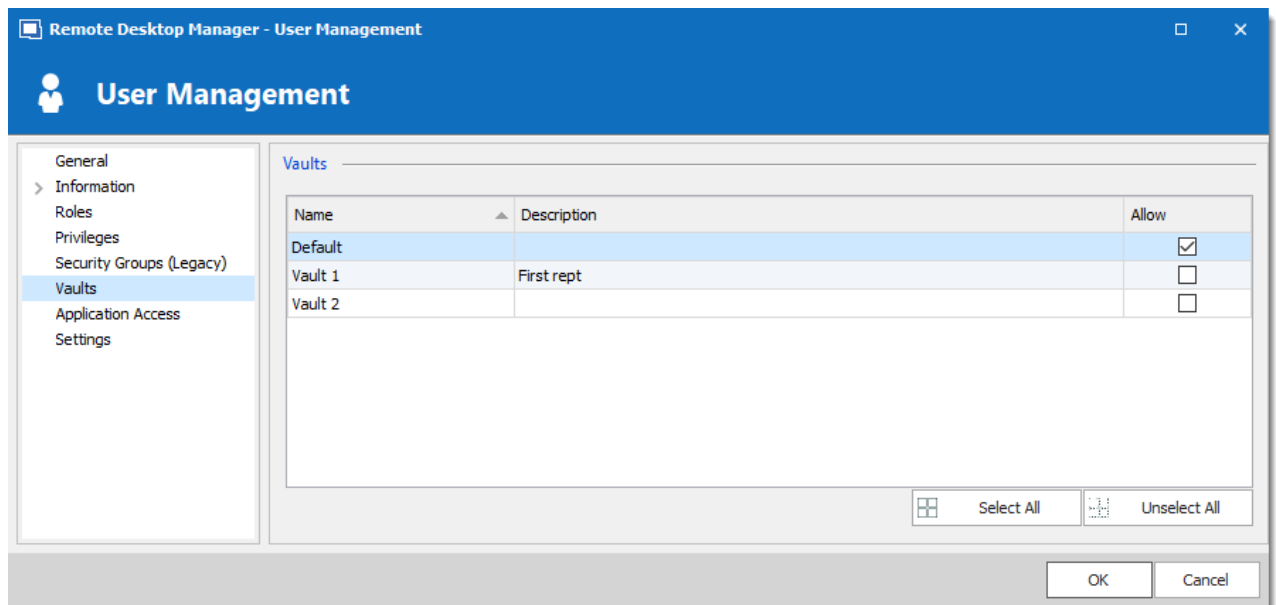
OPTION	DESCRIPTION
<b>Export</b>	<p>Allows the user to <a href="#">Export</a> sessions (Clipboard - Copy as well).</p> <p>The export menu (<b>File – Export</b>) and the export feature in the context menu will be grayed out if the option is not active.</p>

## SECURITY GROUPS (LEGACY)

Security Groups are a legacy setting, we strongly recommend switching over to Roles instead.

## VAULTS

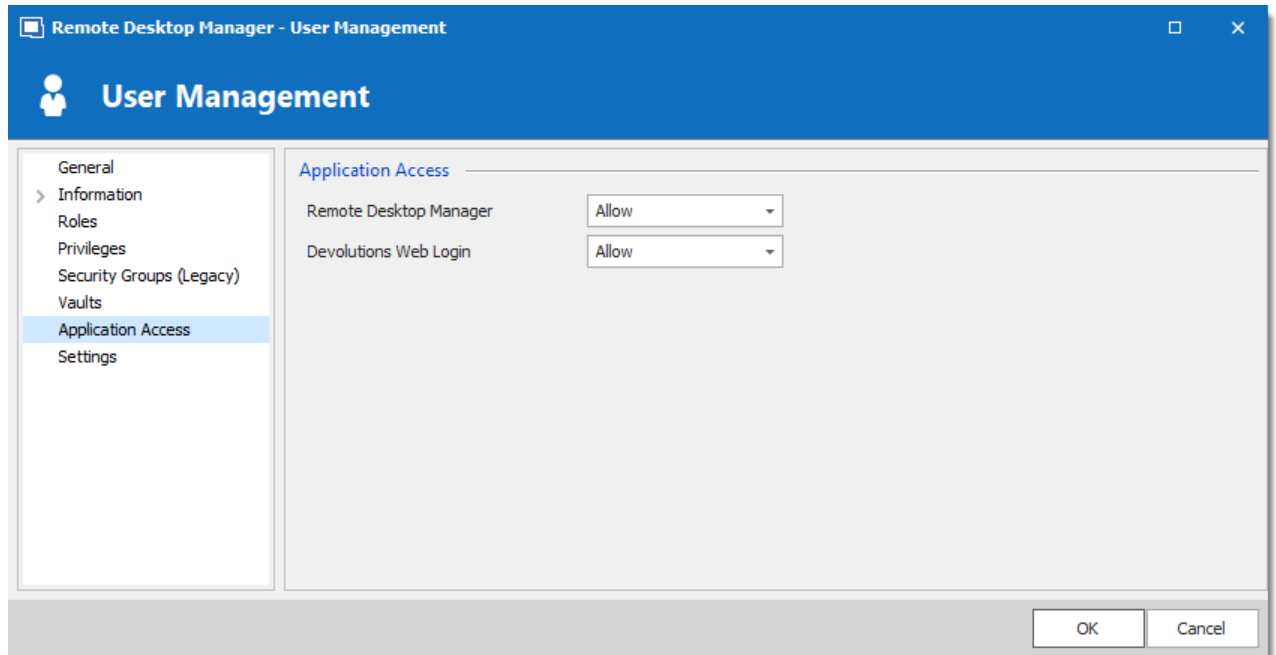
Select which repositories the user has access to. For more information, please consult the Vaults topic.



*User Management - Vaults*

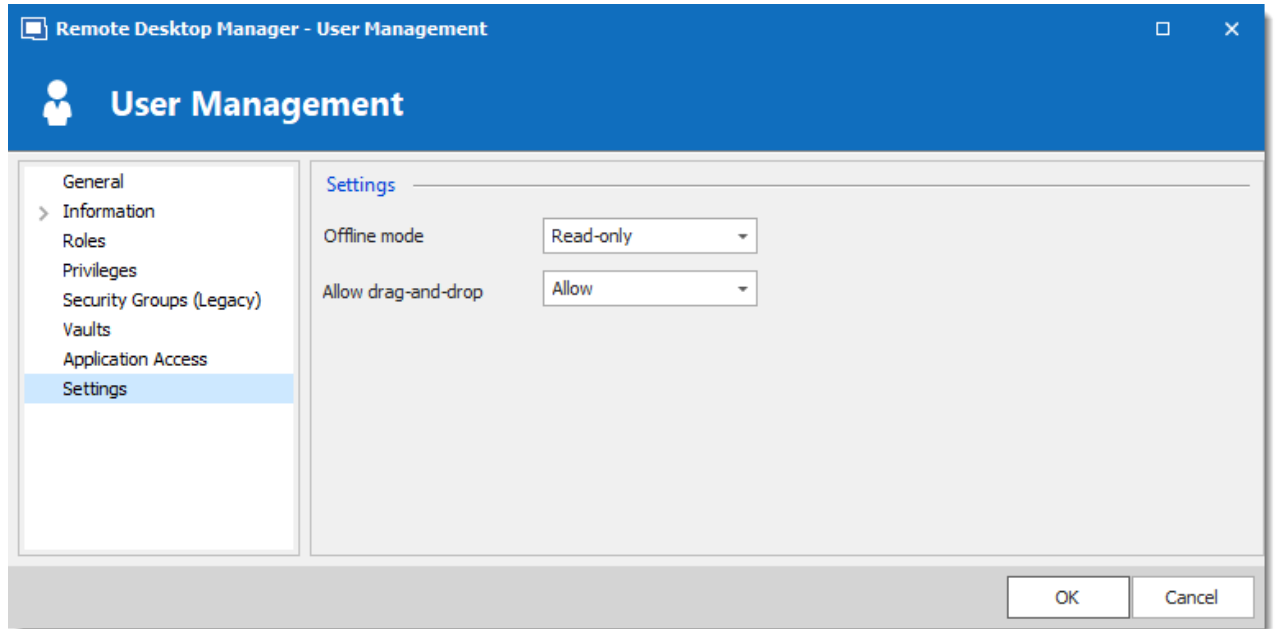
## APPLICATION ACCESS

The application access section allows to restrain access to Remote Desktop Manager or Devolutions Web Login.

*User Management - Application Access*

OPTION	DESCRIPTION
<b>Remote Desktop Manager</b>	Select if the user can access to the data source from Remote Desktop Manager.
<b>Devolutions Web Login</b>	Select if the user can access to the data source form Devolutions Web Login.

## SETTINGS



*User Management - Settings*

Allow the user to enable the [Offline Mode](#) on the data sources. This also depends on the data source being configured to allow it. There are 4 modes available:

OPTION	DESCRIPTION
<b>Disabled</b>	No offline cache allowed for the user.
<b>Cache only</b>	Allow to save a cache of the data source but not the offline mode.
<b>Read-only</b>	A read-only cache. The user will not be able to edit data in the data source. This mode is allowed for <a href="#">Advanced Data Sources</a> only.
<b>Read/Write</b>	An advanced cache, with change synchronization. This mode is allowed for <a href="#">Advanced Data Sources</a> only.

#### 6.7.1.1.1 User Types

## DESCRIPTION

When creating users in Remote Desktop Manager, four types of user are available. Basic rights are granted to the created users depending on their type.

Remote Desktop Manager - User Management

**User Management**

General

- Information
- Roles
- Privileges
- Security Groups (Legacy)
- Vaults
- Application Access
- Settings

**General**

ID: 89F53CFE-08AD-4FDC-972C-53DFF3934827

Authentication type: Database

Username:

Password:

User type: User

User license type: Administrator

☐ Integrated security (Active Directory)

☒ Create SQL Server Login and User

**Information**

First name:

Last name:

Email:

OK Cancel

User Management - User Type

TYPE	DESCRIPTION
<b>Administrator</b>	Grant all rights and permissions to the user.
<b>User</b>	Grant all the basic rights to the user (Add, Edit, Delete). For more information, please consult the <a href="#">Rights</a> section below in this topic.
<b>Restricted user</b>	Personalize the rights to grant to the user.
<b>Read only user</b>	Grant only the view access to the user.

## RIGHTS

When setting a user to the **Restricted User** type, rights must be granted manually. These rights have an immediate influence on which actions the user can perform on unsecured entries. Therefore, rights must be granted for users to be able to perform actions on entries, as permissions cannot override the absence of right.

Once rights are granted, they can be restricted with the [Role-Based Security](#) or Security Groups.

The **Add** right also displays the **Add in root** option. This must be enable for users to be able to add entries into the vault root folder of the data source.

Remote Desktop Manager - User Management

**User Management**

General

- Information
- Roles
- Privileges
- Security Groups (Legacy)
- Vaults
- Application Access
- Settings

General

ID: 89F53CFE-08AD-4FDC-972C-53DFF3934827

Authentication type: Database

Username:

Password:

User type: Restricted user

User license type: Default

☐ Integrated security (Active Directory)

☒ Create SQL Server Login and User

☐ User must change password at next logon

Rights

☐ Add ☐ Add in root

☐ Edit ☐ Move

☐ Delete

Information

First name: Last name:

Email:

OK Cancel

*User Management - Rights*

#### 6.7.1.1.2 Integrated Security

## DESCRIPTION

Integrated Security is a Microsoft technology, which uses the credentials of the current Windows session and send them automatically to the remote resources for authentication.



This feature is available with the [SQL Server](#) or [Devolutions Password Server](#) data sources.

## SETTINGS

To use the Integrated Security, enable the **Integrated Security** box in the **User Management** window. The **Password** field is disabled because the operating system will provide a cached copy automatically.

*Integrated Security*

When the option is activated, an ellipsis button either appears or is enabled. Click this button to display the **Select User** dialog.

*Select User*



Ensure the appropriate domain is displayed in the **From this location** field. Sometime the location defaults to the local computer. Click the **Locations** button to browse for the domain instead.

When using Integrated Security, the currently running windows session must be from a user of the domain. If you need to use other credentials, Remote Desktop Manager must be started using the RUNAS command as described in Running Remote Desktop Manager as Another User.

#### 6.7.1.1.3 TLS Options

## DESCRIPTION

MySQL and MariaDB databases can verify X509 certificate attributes alongside the usual authentication method.

For more information on TLS options, please consult the following topics:

- [MySQL GRANT syntax \(Other Account Characteristics\)](#)
- [Maria DB Knowledge base \(Per-Account SSL/TLS Options\)](#)

## CONFIGURATION

When the user is created, select the desired TLS option:

The screenshot shows the 'Remote Desktop Manager - User Management' window. The 'User Management' section is active. On the left, a sidebar lists 'General', 'Information', 'Roles', 'Vaults', and 'Settings'. The 'General' tab is selected. The 'General' section contains the following fields:

- ID: 33F4911C-8751-4A70-A728-D09754EFDA23
- Username: [Empty text box]
- Password: [Empty text box]
- TLS Option: A dropdown menu is open, showing options: 'Not specified' (selected), 'REQUIRE NONE', 'REQUIRE SSL', and 'REQUIRE X509'.
- User type: [Empty text box]
- Integrated security (Active Directory): [Unchecked checkbox]

Below the 'General' section is the 'Information' section, which includes:

- First name: [Empty text box]
- Last name: [Empty text box]
- Email: [Empty text box]

At the bottom right, there are 'OK' and 'Cancel' buttons.

OPTION	DESCRIPTION
<b>Not specified</b>	Do not specify any TLS option.
<b>REQUIRE NONE</b>	Allow the connection without any certificate.
<b>REQUIRE SSL</b>	Allow the connection only with SSL encryption.
<b>REQUIRE X509</b>	Allow the connection only with valid X509 certificate.

### 6.7.1.2 Role Management

## DESCRIPTION

Roles in Remote Desktop Manager manages multiple users at the same time by grouping them. The management of permissions granted to roles 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 role.



This feature is only available with an Advanced Data Source.

## ROLES IN DEVOLUTIONS PASSWORD SERVER

Roles in Devolutions Password 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 Password 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.

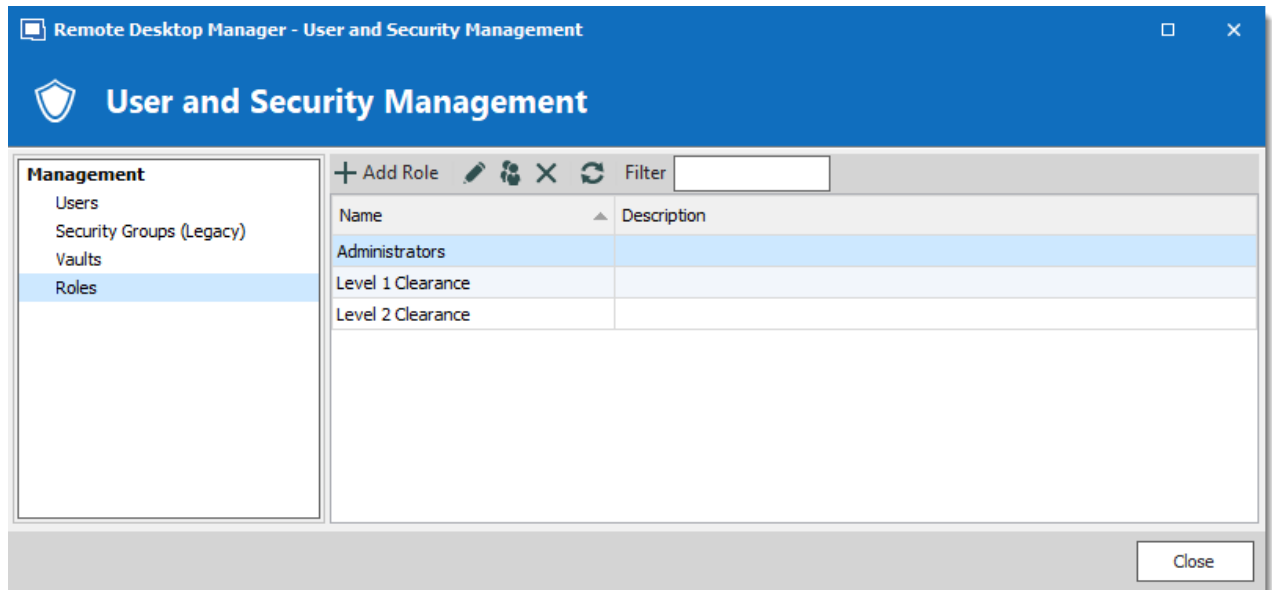
For more information please see [Devolutions Password Server Role Management](#).



## CREATE ROLES

Roles in Remote Desktop Manager are mainly used to group users. You can assign multiple roles to each user. The end result is the union of all permissions given to the roles.

To create a role, in the **User and Security Management** window, click the **Add User** button in the **Roles** section. From the same menu, you can also edit, assign users, delete or refresh.



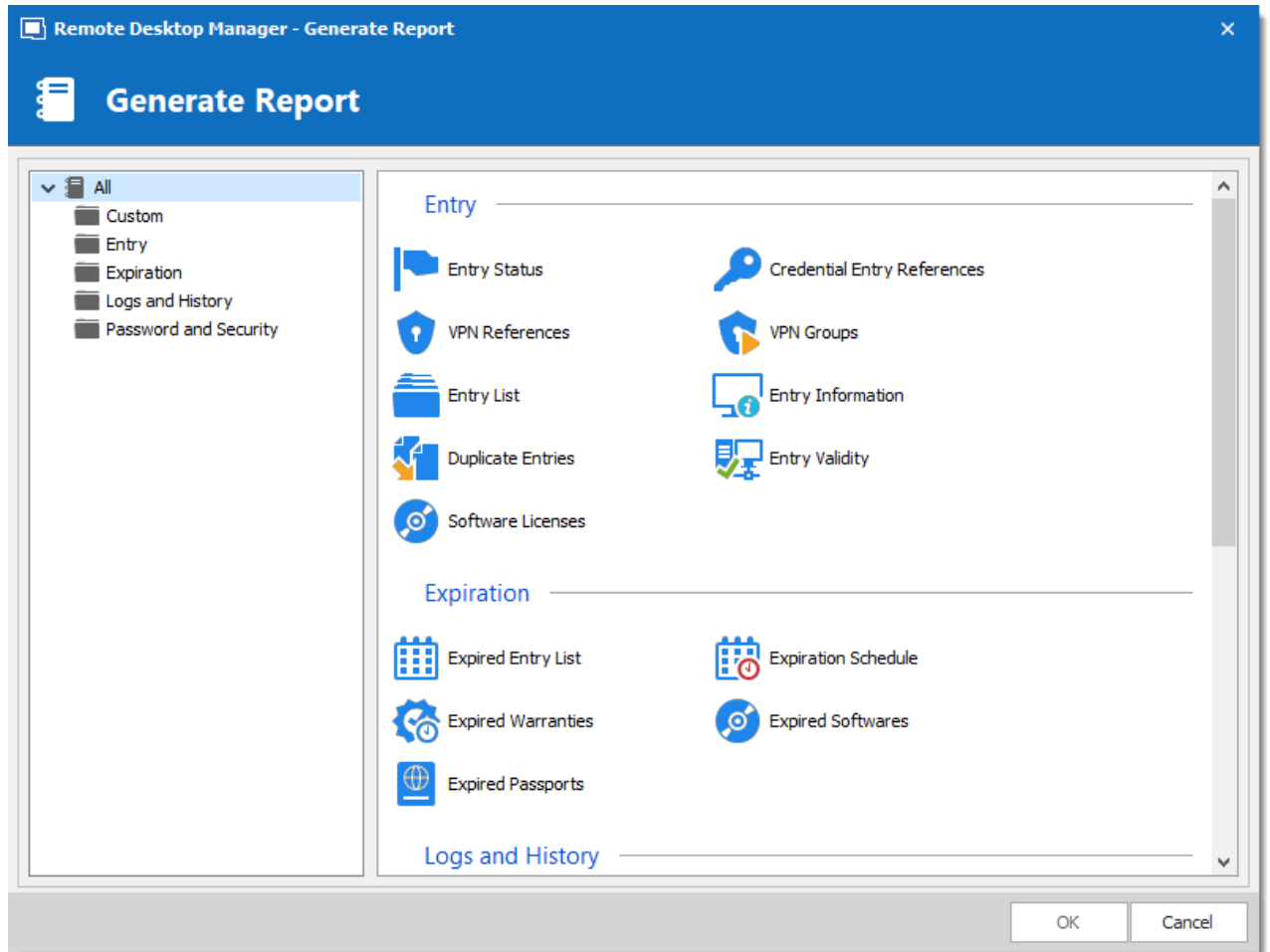
*Roles - Add Role*

### 6.7.2 Reports

#### 6.7.2.1 Reports

## DESCRIPTION

The **Reports** section automatically generates reports detailing Remote Desktop Manager usage related to: Entries, Expired Assets, Passwords, Security and Users. You have the option to export your generated report, as well as executing and exporting reports through a command line.



*Generate Report*

From this window, you can browse and select a wide variety of Report Types. Explore to your heart's content.

Once Generated, a report will provide you with all the information you selected during this step. These final results can take various shapes and have different features (such as editing a specific entry or printing the result) depending on what the report actually is.



These logs are still restricted by user rights. A user with restricted access wouldn't be able to select Password and Security for example.

## DESCRIPTION

The Export Reports is a way to execute and export reports through a command line. You can use this feature in a shortcut or in a batch file and use the Windows task scheduler to execute it.

You will be able to export Data Report, Inventory report as well as most of the reports found in our Generate Report list except for the Password Usage and Security Group.



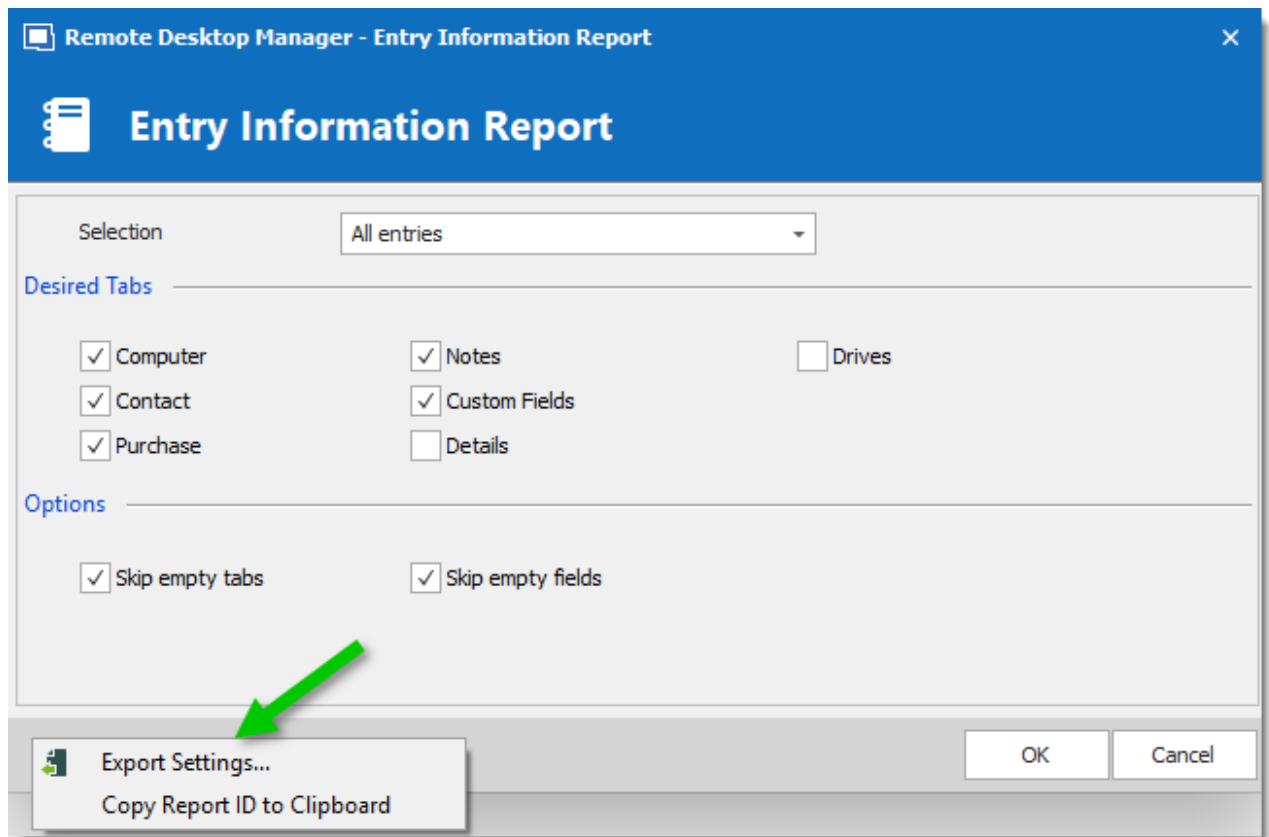
You must have the rights to run report in Remote Desktop Manager to use this feature.

## SETTINGS

[Watch Video](#)

For Reports containing settings, you will have to start with exporting your report settings to create the **\*.rdr** file that the command line use to generate the reports. Here is a list of reports containing settings:

1. Select your Report in **Administrations – Report** and then select the option **Export Settings** in the **More** text button. It will create an **\*.rdr** file containing all your report settings. This is also where you Report ID is located (this will be useful later on).

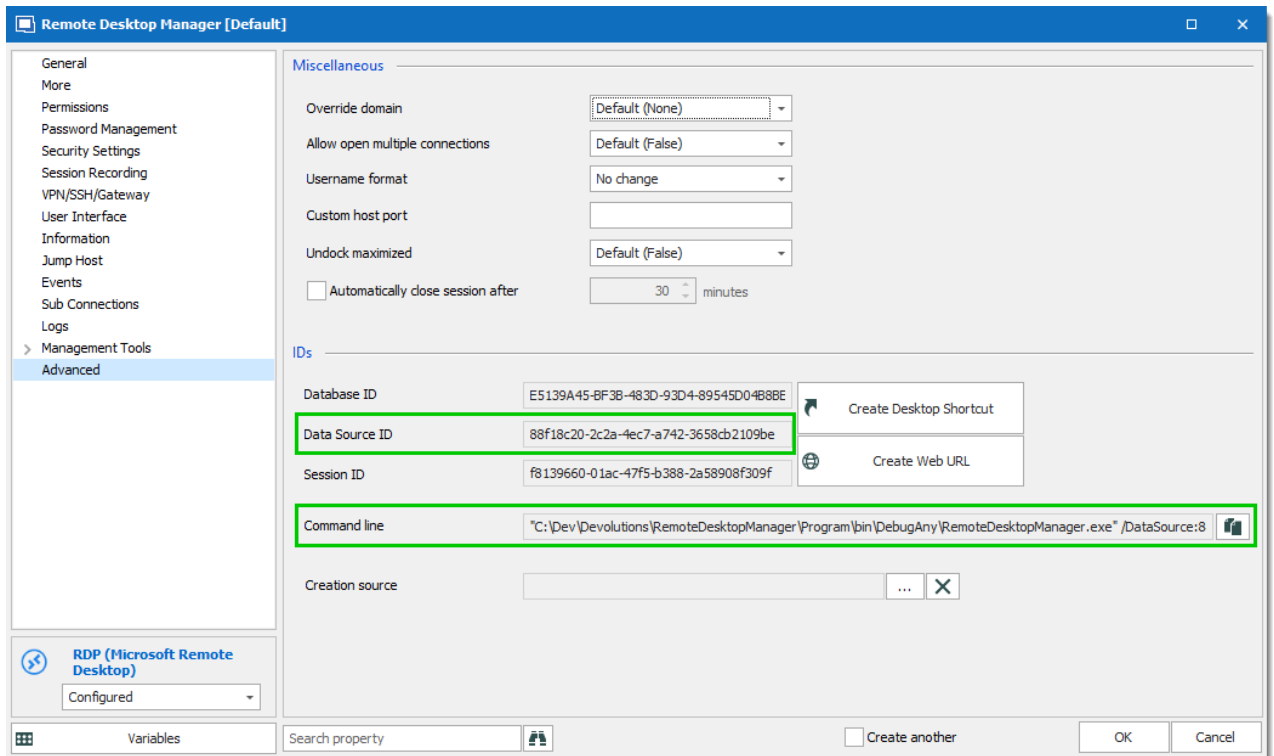
*Export Settings*

2. In your Windows Command Prompt enter the following command line:

```
C:\*** /DataSource:*** /report:***/reportoutput:"****" /reportsettings:"****.rdr"
```

PARAMETERS	DESCRIPTION
<b>C:\</b>	Enter the path used to start your Remote Desktop Manager application (path of the RemoteDesktopManager.exe file)
<b>/DataSource</b>	Specify the data source ID.
<b>/report</b>	Specify the type of report to generate or the report ID.
<b>/reportoutput</b>	Specify the path to save your report and the name for the newly generated report.
<b>/reportsettings</b>	Specify the path of your report settings file (.rdr).

To find your Data Source ID and the Command Line use to start Remote Desktop Manager edit one of your session from your data source and select the Advanced section.



*RDP Session - Advanced Section*

Here is a list of types of Reports you can find in Remote Desktop Manager and the name to enter in the command line to generate the report:

REPORT TYPE IN Remote Desktop Manager	REPORT NAME (TYPE) TO INSERT IN THE COMMAND LINE
<b>Usage Log</b>	SharedConnectionLog
<b>Entry Information</b>	EntryInformation
<b>Expiration Schedule</b>	CalendarExpiredEntry
<b>Expired Entry List</b>	ConnectionExpiredEntry
<b>Expired Passports</b>	ConnectionExpiredPassports

REPORT TYPE IN Remote Desktop Manager	REPORT NAME (TYPE) TO INSERT IN THE COMMAND LINE
<b>Expired Softwares</b>	ConnectionExpiredSoftwares
<b>Expired Warranties</b>	ConnectionExpiredWarranties
<b>Entry Status</b>	ConnectionStatus
<b>Credential Entry References</b>	CredentialEntryUsage
<b>Entry Validity Report</b>	EntryValidity
<b>VPN References</b>	VPNEntryUsage
<b>Entry List</b>	Connection
<b>Duplicate Entries</b>	DuplicateEntry
<b>Password Complexity</b>	PasswordComplexity
<b>Password Analyzer</b>	PasswordAnalyzer

Here is an example of a command line for an Entry Information Report:

```
C:\Program Files (x86)\Devolutions\Remote Desktop Manager\RemoteDesktopManager.exe /DataS
/reportoutput:C:\dev\devolutions\Rapport\rapportEntry.csv /reportsettings:C:\dev\devoluti
```

#### 6.7.2.2 Deleted Entries

## DESCRIPTION

The **Administration – View deleted** option allows you to view the deleted entries as well as restoring them.



This feature requires an [Advanced Data Source](#).



Administrators can permanently delete some or all deleted entries.



For architectural reasons, the documents stored in our Advanced Data Sources are **NOT** protected from deletions. Once they are deleted, **they cannot be restored**. Please keep a safe copy of all documents in another storage device. Support for this feature will be added in a coming update to our products.

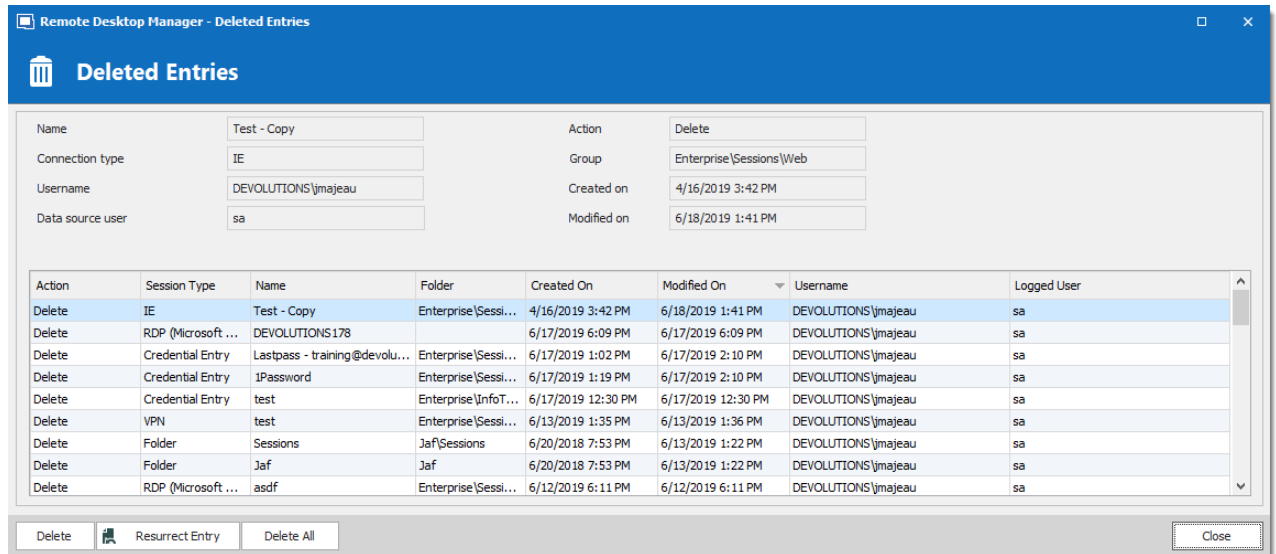


Sub-connections are not retained in the View Deleted window. To restore a sub-connection, please have a look at Entry History.

## SETTINGS

### MANAGE DELETED ENTRIES

The **Deleted Entries** will generate a list containing all the entries previously deleted from your data source. You may resurrect an entry, meaning it will become an active entry again and will be shown in your data source. You may also chose to permanently delete your entries, once you have permanently deleted your entries you won't be able to resurrect them afterward.

*Deleted Entries*

OPTION	DESCRIPTION
<b>Delete</b>	Permanently delete the selected entry.
<b>Resurrect Entry</b>	Use this button to restore an entry.
<b>Delete All</b>	Permanently delete all the deleted entries.



Deleted entries can be resurrected as long as the [Security Provider](#) has not been changed since the deleted action.

## EXPORT DELETED ENTRIES LIST

You can use the **Right-click** button on one or several lines to export them in CSV, HTML or XML format.



## 6.7.3 Settings

### 6.7.3.1 Root (Settings)

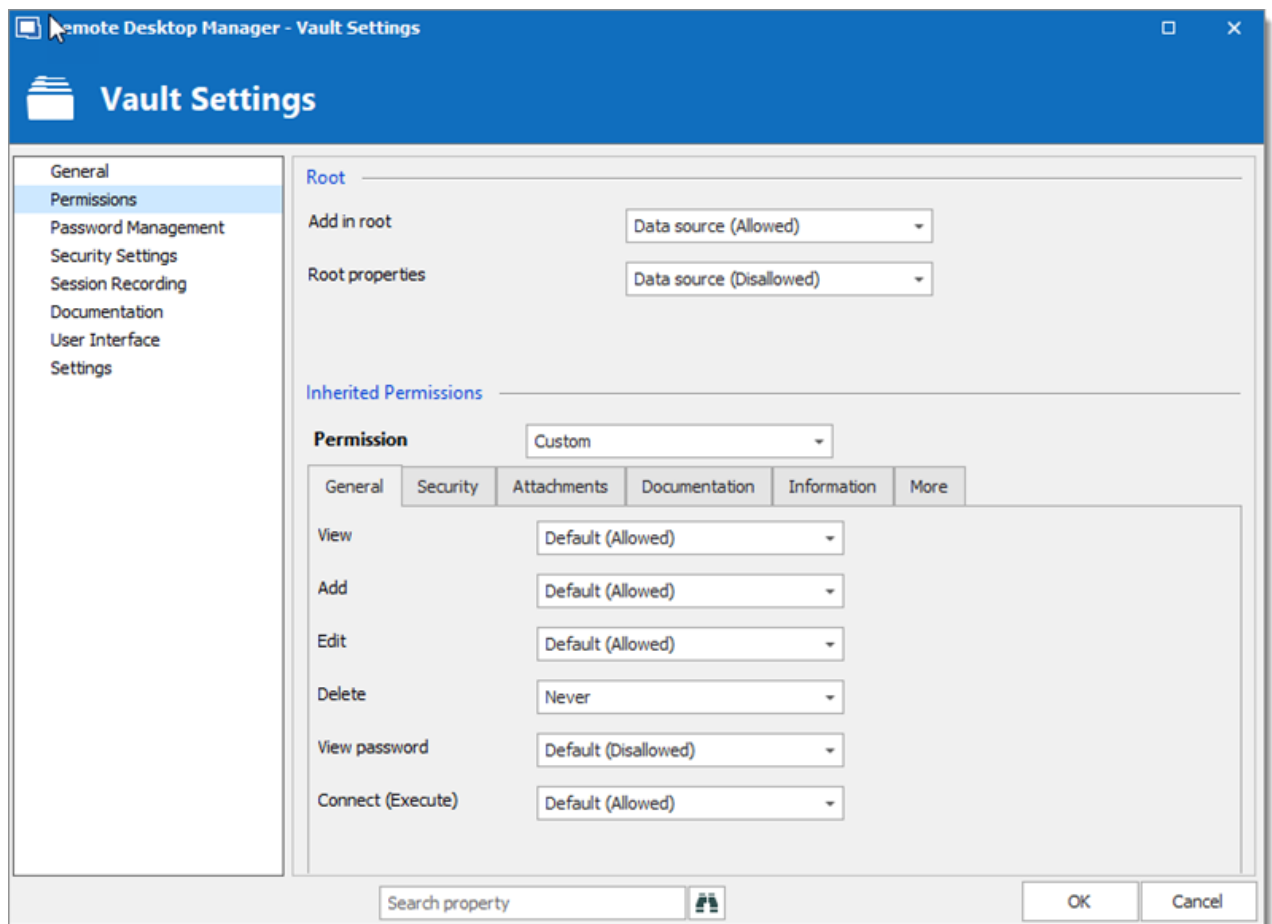
#### 6.7.3.1.1 Default security for entries

## DESCRIPTION

In the vault settings, navigate to the **Permissions** section. Under **Inherited Permissions**, change the **Permission** drop down list to the desired settings.

- **Custom** allows to select specific roles/users for each permission below.
- **Never** denies any access to all users.

For more information on the discrete permissions, please consult the Security – Permissions topic.



*Vault – Permissions*

To confirm the change, edit an entry below the vault root and navigate to the **Security – Permissions** section. All permissions set to **Default** inherit the value from Data Source Permissions (System Permissions) or the user. Inherited values are displayed next to the permissions.

## 6.7.3.2 System Settings

### 6.7.3.2.1 General

## GENERAL

The **General** section allows to manage the availability of different features related to the database.



These settings applies to all users that have access to the data source.

The screenshot shows the 'Remote Desktop Manager - System Settings' dialog box with the 'General' tab selected. The left sidebar contains a tree view with categories: General (expanded), Password Management, Applications, and Advanced. The 'General' section includes settings for user-specific settings, shortcuts, virtual folders, database clean up, entry states, automatic check-in, sub connections, entry mode, log comments editing, minimum length, and file size. The 'File Size' setting is set to 25 MB, with a note that it applies to documents and attachments. The bottom of the dialog has a 'View History' button, a search property field, the version number 'Version 2019.1.30.0', and 'OK' and 'Cancel' buttons.

**Remote Desktop Manager - System Settings**

**System Settings**

- General
  - Favorites
  - Private Vault
  - Security
  - System Message
  - User Template
- Password Management
  - Password Templates
  - Forbidden Password
  - Password Validation
  - Custom User
- Applications
  - Offline
  - Custom Variables
  - Paths
  - Serial Number
  - Type Settings
  - Type Availability
  - Version Management
- Advanced

**General**

- ☒ Allow user specific settings
- ☒ Allow shortcuts
- ☒ Allow virtual folders
- Allow sub connections: Default
- Add entry mode: Template list (include blank)
- ☒ Allow database clean up
- ☒ Allow entry states (Lock, Running, Checkout)
- ☒ Automatic check in after: 60 minutes

**Comments**

- ☐ Allow log comments editing
- Minimum length (char): 0

**File Size**

- Maximum file size (MB): 25. This setting applies to documents and attachments

View History Search property Version 2019.1.30.0 OK Cancel

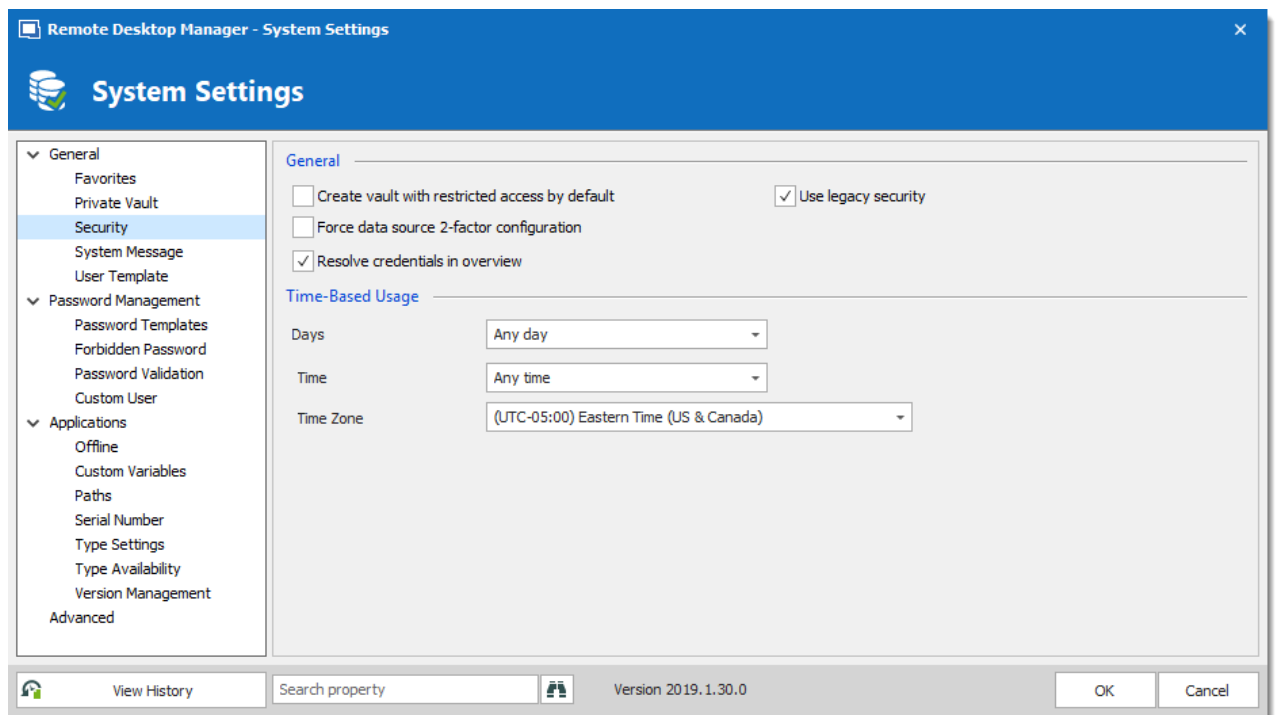
*System Settings - General*

GENERAL	DESCRIPTION
<b>Allow user Specific Settings</b>	Allow users to save <a href="#">User Specific Settings</a> .
<b>Allow database clean up</b>	Allows logs and deleted history to be cleaned up. For more information, please consult the <a href="#">Clean up</a> topic.
<b>Allow shortcuts</b>	Allow the reiteration of entries through the shortcut feature.
<b>Allow entry states (Lock, Running, Checkout)</b>	Allow entries to be locked when used or edited.
<b>Allow virtual folders</b>	Allow to store entries in virtual folders. (Not supported with Devolutions Password Server.)
<b>Automatic check in after</b>	Forces checked out entries to check in automatically after a set delay.
<b>Allow sub connections</b>	Allow users to create sub connections.
<b>Add entry mode</b>	<p>Select if users are prompted to choose a template when creating a new entry. Select between:</p> <ul style="list-style-type: none"> <li>• <b>Default</b></li> <li>• <b>Template list (include default)</b></li> <li>• <b>Template list only</b></li> <li>• <b>No template selection</b></li> </ul>
COMMENTS	DESCRIPTION
<b>Allow log comments editing</b>	Enable the log comment editing for all users.

COMMENTS	DESCRIPTION
<b>Minimum length (char)</b>	Set the minimum length (in characters) allowed for comments.
FILE SIZE	DESCRIPTION
<b>Maximum file size (MB)</b>	Limit the size of attachments and document entries to avoid to over load the data source.

## 6.7.3.2.1.1 Security

## SETTINGS



System Settings - General - Security

DATA SOURCE SECURITY	DESCRIPTION
<b>Create Vault with restricted access by default</b>	Automatically secure the vault settings when creating a repository. Therefore, the permissions settings are set to <b>Never</b> .
<b>Force data source 2-factor configuration</b>	Require the users to have a <a href="#">2-factor configuration</a> applied on the data source. Not shown with Devolutions Password Server as 2FA set elsewhere.
<b>Resolve credentials in overview</b>	Displays username and password fetched from a Credential repository in the entry overview in the dashboard. Uncheck this option if it takes too long to resolve.
<b>Use legacy security</b>	Use the old system of managing privileges: security groups.
TIME-BASED USAGE	DESCRIPTION
<b>Time of day</b>	<p>Select the hours which the data source is limited to. Select between:</p> <ul style="list-style-type: none"> <li>• <b>Any time</b>: the session can be used at any hour.</li> <li>• <b>Custom</b>: manually select the time frame the session is available for.</li> </ul>
<b>Time of week</b>	<p>Select which days the data source is available for. Select between:</p> <ul style="list-style-type: none"> <li>• <b>Any day</b>: the session can be used any day of the week or week-end.</li> <li>• <b>Week days</b>: the session can be used only the week days.</li> <li>• <b>Week ends</b>: the session can be used only the week ends.</li> <li>• <b>Custom</b>: manually select each day the session is available for.</li> </ul>

TIME-BASED USAGE	DESCRIPTION
<b>Time Zone</b>	Select the time zone you are currently in.

#### 6.7.3.2.1.2 Allow Password Access From External System

## DESCRIPTION



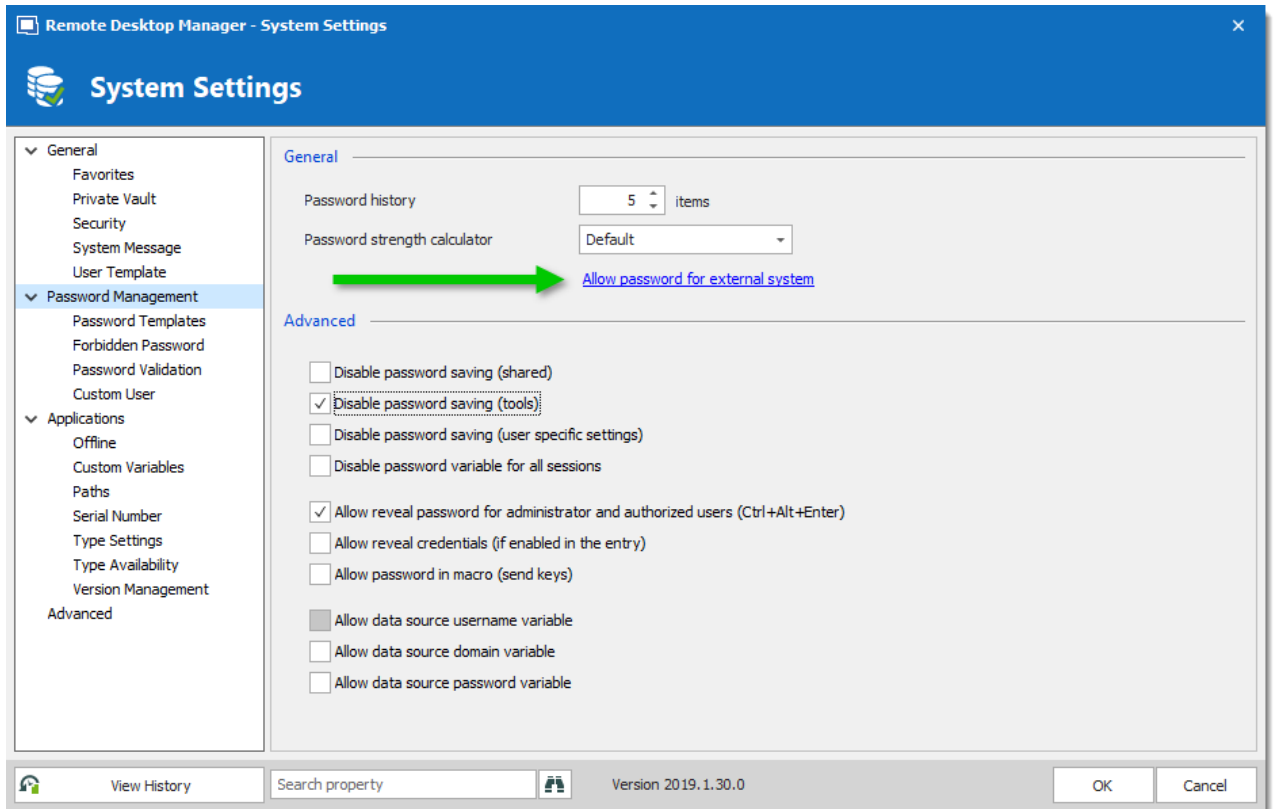
This feature is only available when using an [Advanced Data Source](#).

Accessing passwords stored in your data source by querying the underlying database is not possible because of the encryption we apply on the passwords. For those of you that need to access passwords directly in the database, for example by a CRM system, we have created a way to achieve this.

## SETTINGS

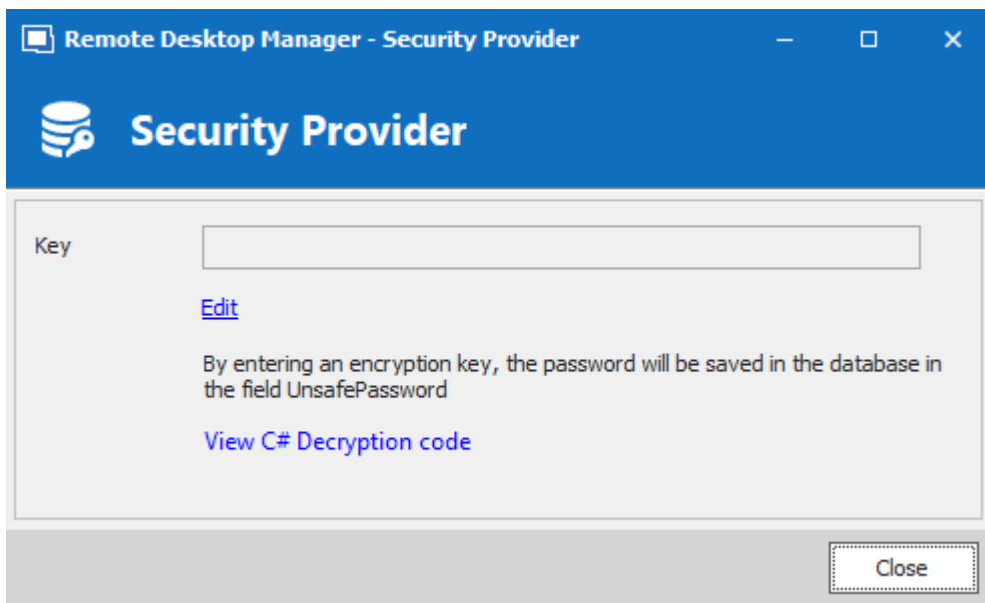
The session information, which is an XML structure, is stored in the **Data** field of the **Connections** table in the underlying database.

However, getting the encrypted password from the database requires the **Allow password for external system** to be configured.



*Password Policy - Allow Password For External System*

Enter an encryption key in the **Key** field. Once a key is provided it will cause the system to extract a copy of the password from our XML structure, this will then be re-encrypted using the **key** you have provided and stored back into the **UnsafePassword** field of the **Connections** table.



*Security Provider*

## DECRYPTION CODE

Use the following .net code to decrypt your passwords.

```
public static string Decrypt(string encryptedString, string key)
{
    if (string.IsNullOrEmpty(encryptedString))
    {
        return encryptedString;
    }

    try
    {
        TripleDESCryptoServiceProvider tripleDesCryptoServiceProvider = new TripleDESCryptoServiceProvider();
        MD5CryptoServiceProvider cryptoServiceProvider = new MD5CryptoServiceProvider();

        string strTempKey = key;

        byte[] byteHash = cryptoServiceProvider.ComputeHash(Encoding.ASCII.GetBytes(strTempKey));

        tripleDesCryptoServiceProvider.Key = byteHash;

        tripleDesCryptoServiceProvider.Mode = CipherMode.ECB;

        byte[] byteBuff = Convert.FromBase64String(encryptedString);

        string strDecrypted =
            Encoding.UTF8.GetString(
                tripleDesCryptoServiceProvider.CreateDecryptor().TransformFinalBlock(
                    byteBuff, 0, byteBuff.Length));

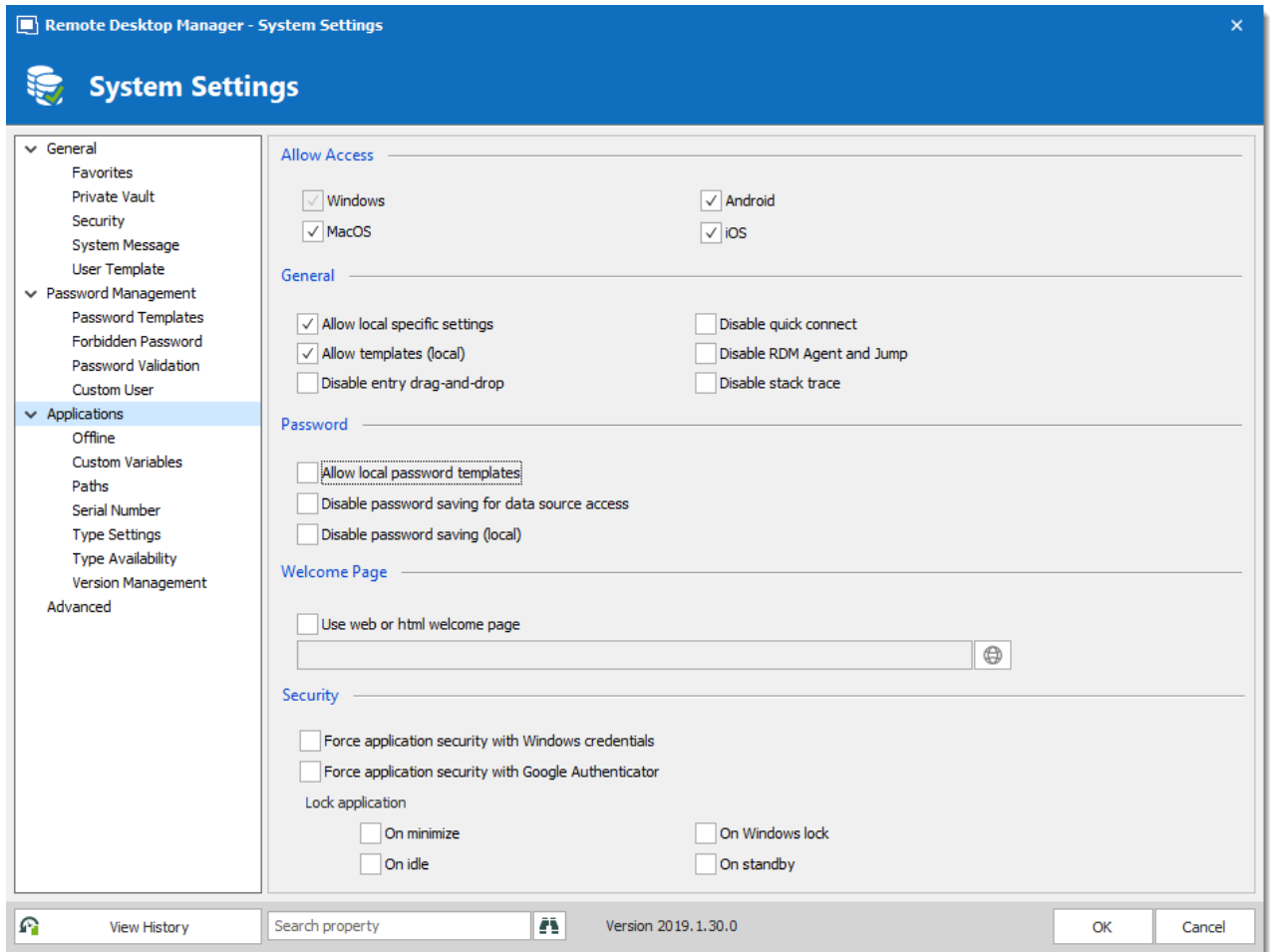
        return strDecrypted;
    }
    catch (Exception)
    {
        return null;
    }
}
```

### 6.7.3.2.2 Application

## DESCRIPTION

The **Applications** section manages the availability of different features related to Remote Desktop Manager application.





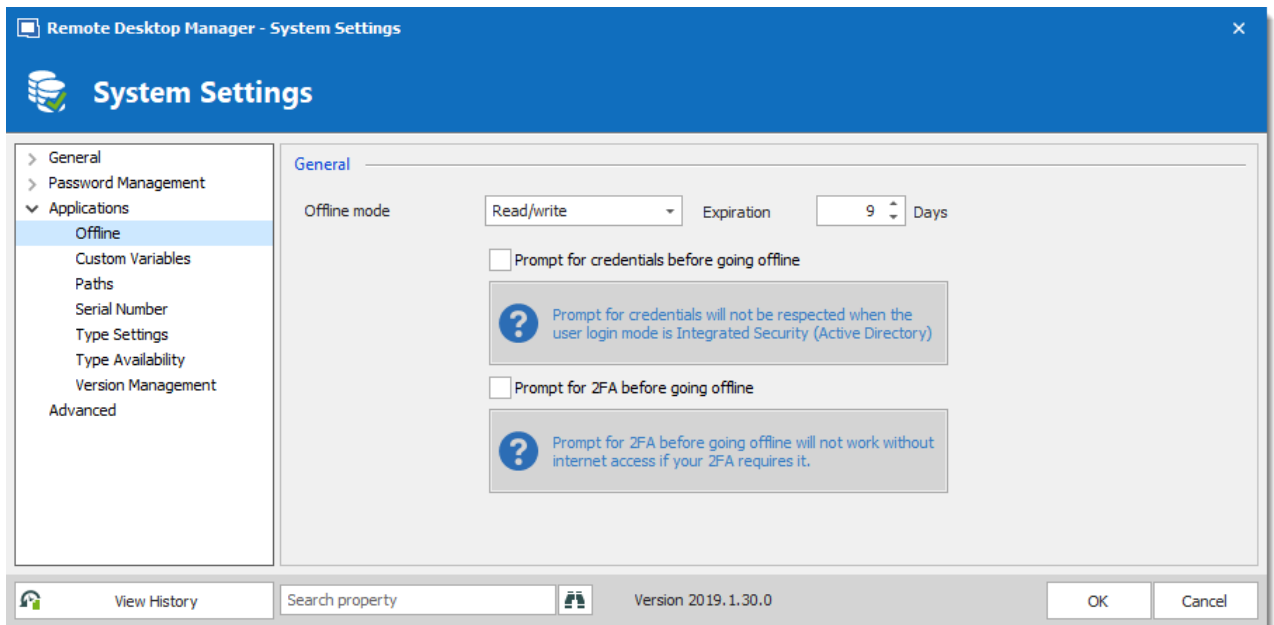
ALLOW ACCESS	DESCRIPTION
<b>Operating systems</b>	Enable access to the data source from the selected operating systems.
GENERAL	DESCRIPTION
<b>Allow local Specific Settings</b>	Allow users to save <a href="#">Local Specific Settings</a> .
<b>Allow templates (local)</b>	Allows to locally save entry's templates.
<b>Disable entry drag-and-drop</b>	Disable entries drag and drop from one folder to another. This setting is useful for avoiding accidental drag and drop.

GENERAL	DESCRIPTION
<b>Disable quick connect</b>	Disable the Quick Connect feature for all users of the data source.
<b>Disable RDM Agent and Jump</b>	Disable the option to activate a session as an RDM Agent or Jump.
<b>Disable stack trace</b>	Disable the stack trace details when an error occurs in Remote Desktop Manager. This is a security feature.
PASSWORD	DESCRIPTION
<b>Allow local password templates</b>	Allows password templates to be saved locally.
<b>Disable password saving for data source access</b>	Prevent users to save or change the passwords stored in the data source configurations.
<b>Disable password saving (local)</b>	Prevent users from saving passwords in the properties of entries.
WELCOME PAGE	DESCRIPTION
<b>Use web or html welcome page</b>	Enter an URL to use as the application's welcome page.
SECURITY	DESCRIPTION
<b>Force application security with Windows credentials</b>	Require the users to authenticate with their Windows credentials at application startup.

SECURITY	DESCRIPTION
<b>Force application security with Google Authenticator</b>	Require the users to authenticate with <a href="#">Google Authenticator</a> at application startup.
<b>Lock application</b>	<p>Set the application to lock:</p> <ul style="list-style-type: none"> <li>• <b>On Minimize:</b> lock application when minimized in the taskbar for all users of the data source.</li> <li>• <b>On Idle:</b> automatically lock the application when it is not used after a determined amount of time.</li> <li>• <b>On Windows lock:</b> lock the application on Windows lock.</li> <li>• <b>On standby:</b> lock the application when on standby.</li> </ul>

## 6.7.3.2.2.1 Offline

## DESCRIPTION



OPTION	DESCRIPTION
<b>Offline mode</b>	Set the global data source <a href="#">Offline Mode</a> availability. The offline mode is useful when using a VPN connection that makes using local network impossible.
<b>Expiration</b>	Number of days before the offline cache expires. You must go online prior to the end of that period to re-validate the data.
<b>Prompt for credentials before going offline</b>	Force the user to provide their credentials before going offline.
<b>Prompt for 2FA before going offline</b>	Force the user to provide their 2FA before going offline.



It is not recommended to set the **Expiration** to 0, as this will disable the expiration of the offline cache.

#### 6.7.3.2.2.2 Serial Number

## DESCRIPTION

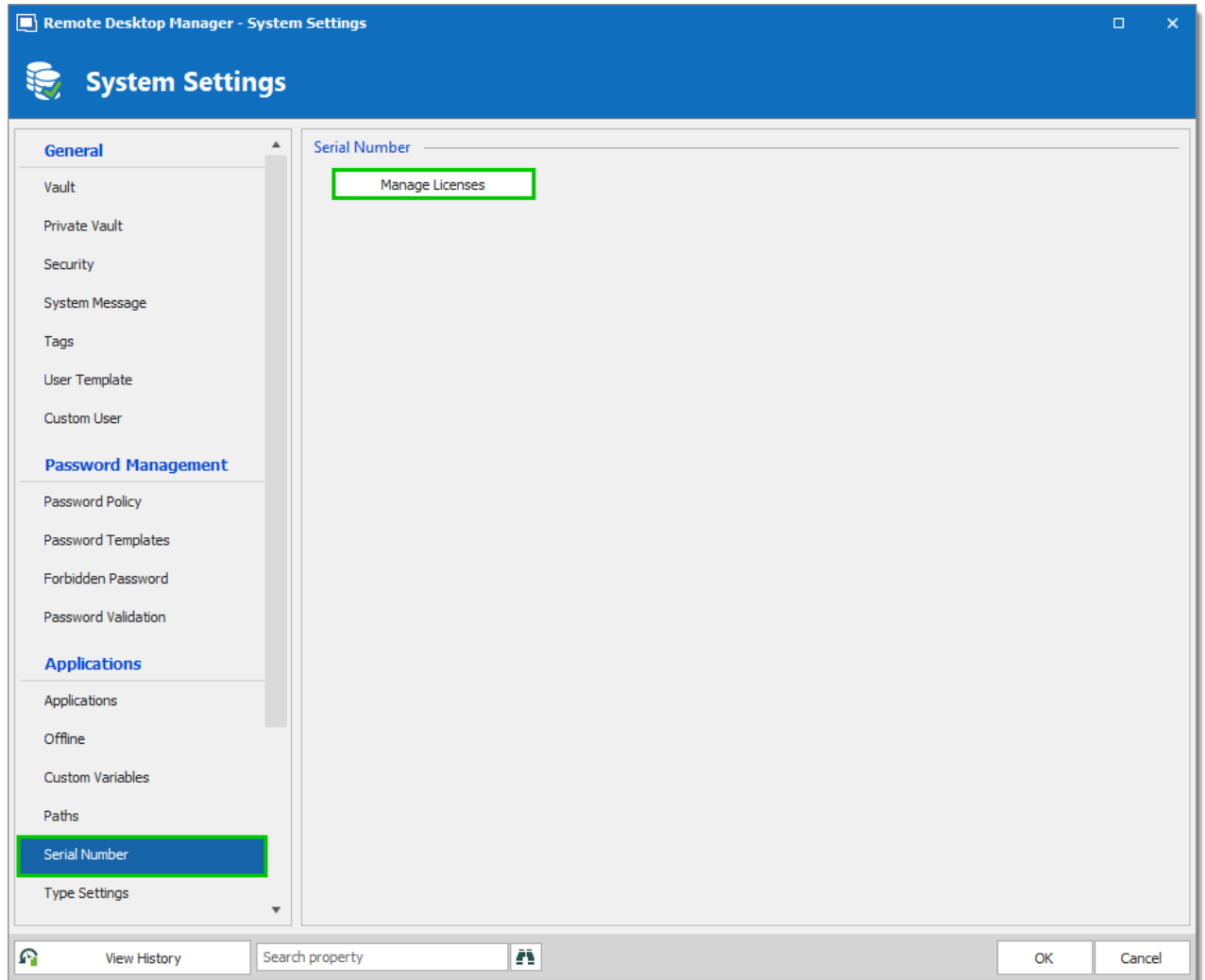
Store an Enterprise Edition Site or Global **License** serial to share in the data source.



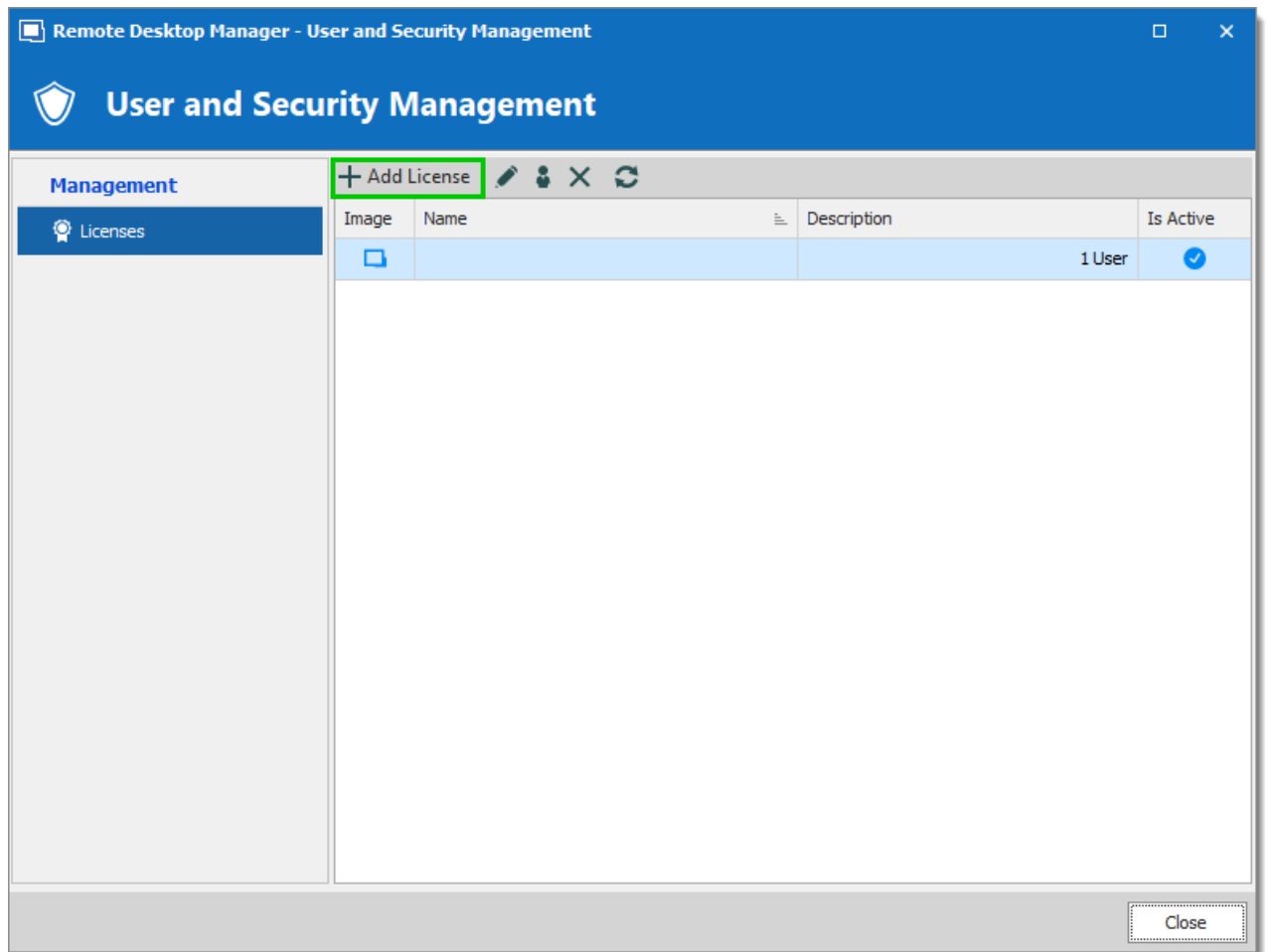
When you add a data source with a saved serial in an unregistered version of Remote Desktop Manager, the license serial is automatically retrieved from data source settings.

## SETTINGS

You can manage your licenses through a shortcut in **Administration - System settings - Serial Number**.



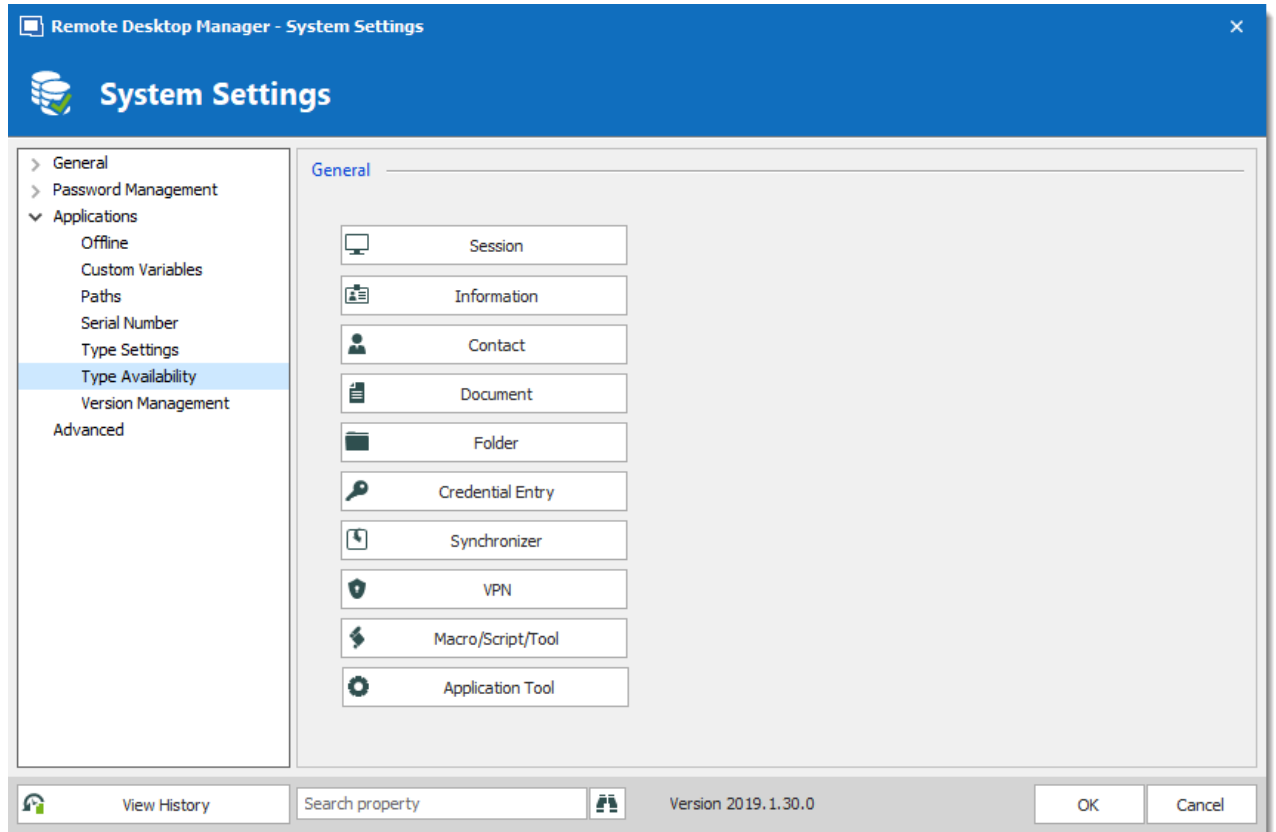
*System Settings - Serial Number*



*User and Security Management - Add License*

#### 6.7.3.2.2.3 Type availability

## SETTINGS



*System Settings - Types - Availability*

OPTION	DESCRIPTION
<b>Type Availability</b>	Select entry types to exclude. Excluded entries will not be in the <b>Add New Entry</b> window.

#### 6.7.3.2.2.4 Version Management

## DESCRIPTION

The **Version Management** allows the administrators to manage the data source availability in other versions of Remote Desktop Manager.

## WINDOWS AND MACOS

**Remote Desktop Manager - Data Source Settings**

**Data Source Settings**

- General
  - Favorites
  - Private Vault
  - Security
  - System Message
  - User Template
- Password Management
  - Password Templates
  - Forbidden Password
  - Password Validation
  - Custom User
- Applications
  - Offline
  - Custom Variables
  - Paths
  - Serial Number
  - Type Settings
  - Type Availability
  - Version Management**
  - Advanced

**Windows - Remote Desktop Manager**

☐ Minimal version  Current

☐ Minimal version custom message

☐ Maximal version  Current

☐ Maximal version custom message

☐ Disable auto update notification

Download URL

**Mac - Remote Desktop Manager**

☐ Minimal version

☐ Minimal version custom message

☐ Maximal version

☐ Maximal version custom message

☐ Disable auto update notification

Download URL

View History Search property OK Cancel

### Version Management

OPTION	DESCRIPTION
<b>Minimal version</b>	Forces users of the data source to use a minimal version of Remote Desktop Manager. Enter the entire version number (2019.1.0.0) to force a specific version. Use this to disable connecting to the data source with an older version.
<b>Minimal version custom message</b>	Enter a custom message for the minimal version notification.
<b>Maximal version</b>	Forces users of the data source to use a maximal version. Enter the entire version number (2019.1.0.0) to



OPTION	DESCRIPTION
	force a specific version. Use this to disable connecting to the data source with a newer version.
<b>Maximal version custom message</b>	Enter a custom message for the maximal version notification.
<b>Disable auto update notification</b>	Disable the auto update notification message. Use this to manually update the application and prevent from getting notified when new versions are available.
<b>Download URL</b>	Use in conjunction with the minimal or maximal version, once a minimal or maximal version requirement is not met the system will prompt the user that the version is no longer valid and it will open the link (path/URL) to download the newer or older version.

### 6.7.3.3 System Permissions

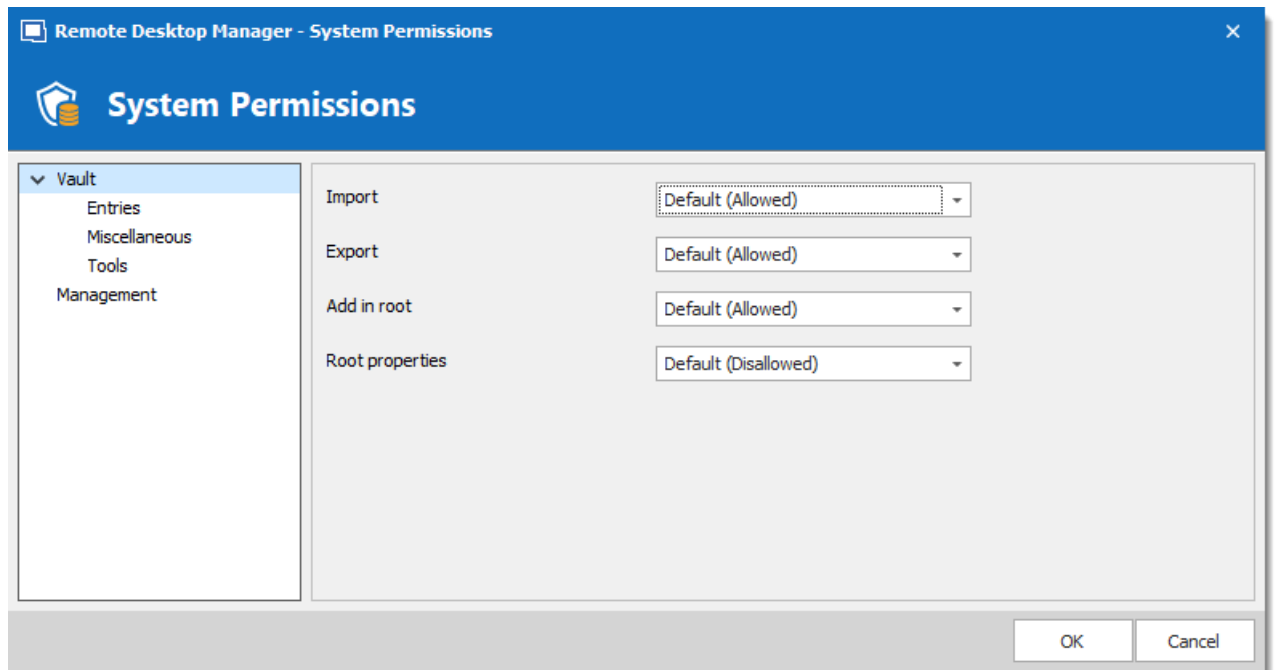
## DESCRIPTION

The **System Permissions** allows to grant some administrative permissions to standard users without making them administrators. The **Default** setting inherits the permission set on the user or role. For more information about permissions, consult General Security.



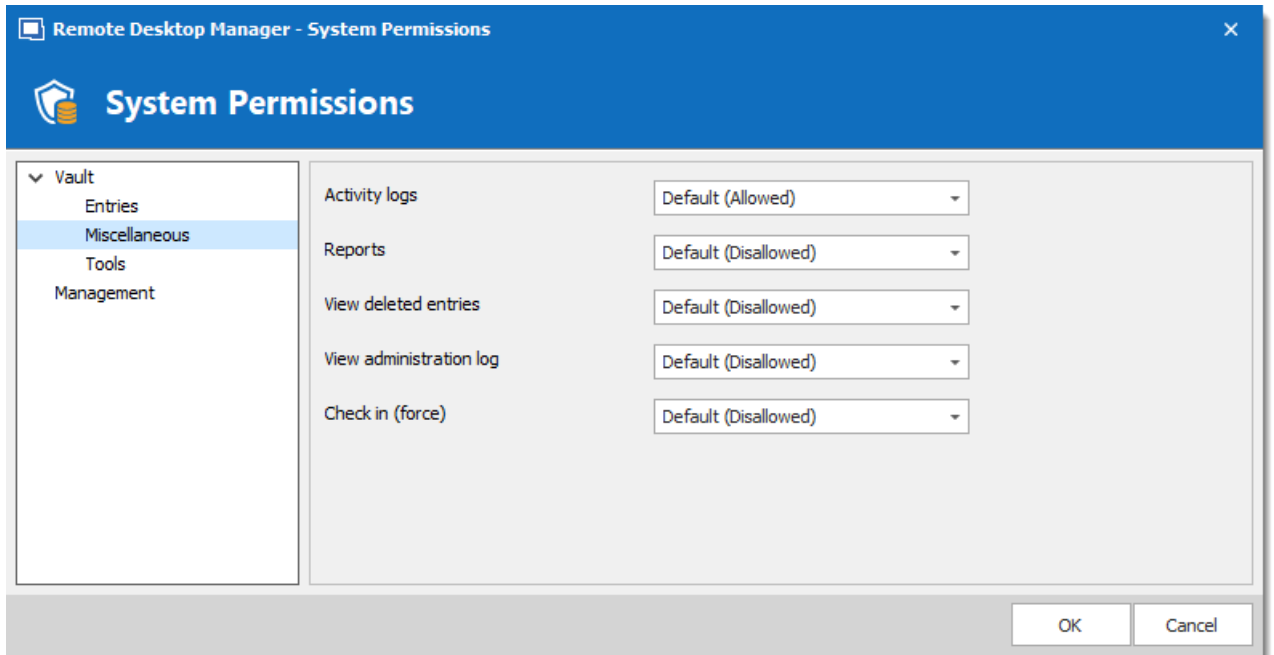
This feature is only available when using an [Advanced Data Source](#).

## ENTRIES

*System Permissions - Entries*

OPTION	DESCRIPTION
<b>Import</b>	Allow users/roles to import entries in the data source.
<b>Export</b>	Allow users/roles to export from the data source.
<b>Add in root</b>	Allow users/roles to create entries in the root folder.
<b>Root properties</b>	Allow users/roles to access the root properties.

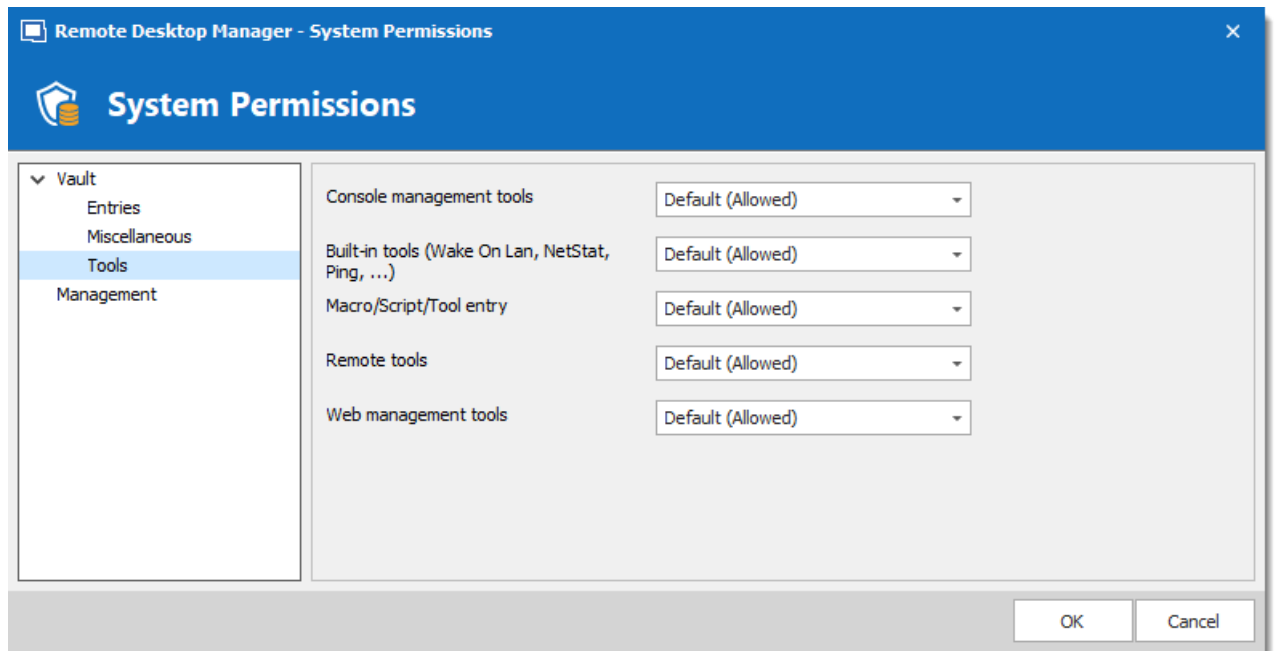
## MISCELLANEOUS



*System Permissions - Miscellaneous*

OPTION	DESCRIPTION
<b>Activity logs</b>	Allow users/roles to view the activity logs.
<b>Reports</b>	Allow users/roles to generate and view reports.
<b>View deleted entries</b>	Allow users/roles to view and restore deleted entries.
<b>View administration logs</b>	Allow users/roles to view the administration logs.
<b>Check in (force)</b>	Allow users/roles to check in entries with the checked out state.

## TOOLS



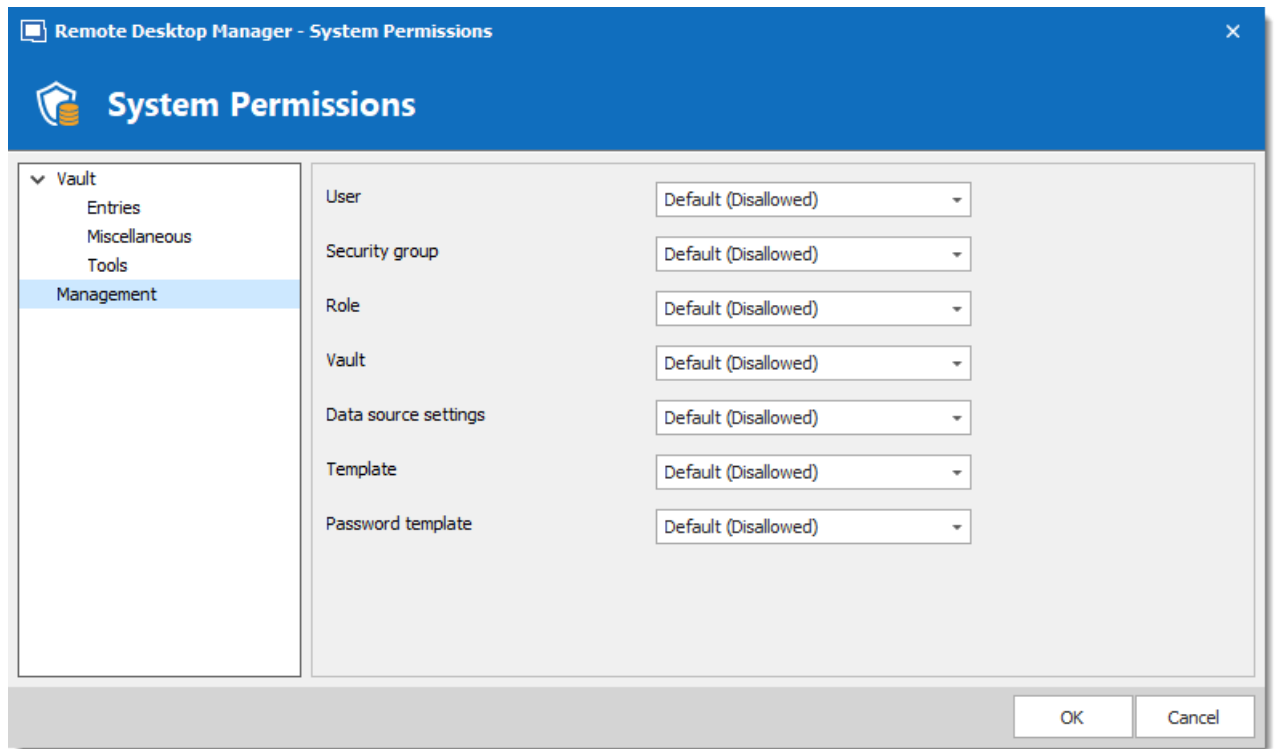
System Permissions - Tools

OPTION	DESCRIPTION
<b>Console management tools</b>	Allow users/roles to use console management tools.
<b>Built-in tools (Wake-on-LAN, NetStat, Ping, ...)</b>	Allow users/roles to use session related tools.
<b>Macros/Scripts/Tools entry</b>	Allow users/roles to use Macros/Scripts/Tools entries.
<b>Management Tools</b>	Allow users/roles to use Management Tools.
<b>Web management tools</b>	Allow users/roles to use web management tools.

## MANAGEMENT



The **Default** value in **Tools** is equivalent to **Never**.



*System Permissions - Management*

OPTION	DESCRIPTION
<b>User</b>	Allow users/roles to access the user management.
<b>Security Group</b>	Allow users/roles to access the security groups management.
<b>Role</b>	Allow users/roles to access the roles management.
<b>Vault</b>	Allow users/roles to manage Vaults.
<b>Data source settings (System Settings)</b>	Allow users/roles to access data source settings.

OPTION	DESCRIPTION
<b>Template</b>	Allow users/roles to create and manage templates.
<b>Password template</b>	Allow users/roles to create and manage password templates.

#### 6.7.3.4 Security Providers

### DESCRIPTION

The **Security Provider** allows for encrypting the data source content. To access the security provider, navigate to **Administration – Security Provider**.



This feature requires an [Advanced Data Source](#).



Regardless of the selected security provider, passwords stored in data sources are **ALWAYS** encrypted using AES 256 bit encryption.



By using a security provider, you ensure that nobody can read entries configuration data, even when people have a direct access to the database(s) or a backup. Shared data sources should always be secured with a security provider especially Devolutions Online Database.



Prior to applying a new or changing an existing security provider, make sure that every users are disconnected from the data source. If you are changing an existing Shared Passphrase or Certificate, please note that users will get back access to the data source when they the new Shared Passphrase or Certificate on their computer.

### SETTINGS

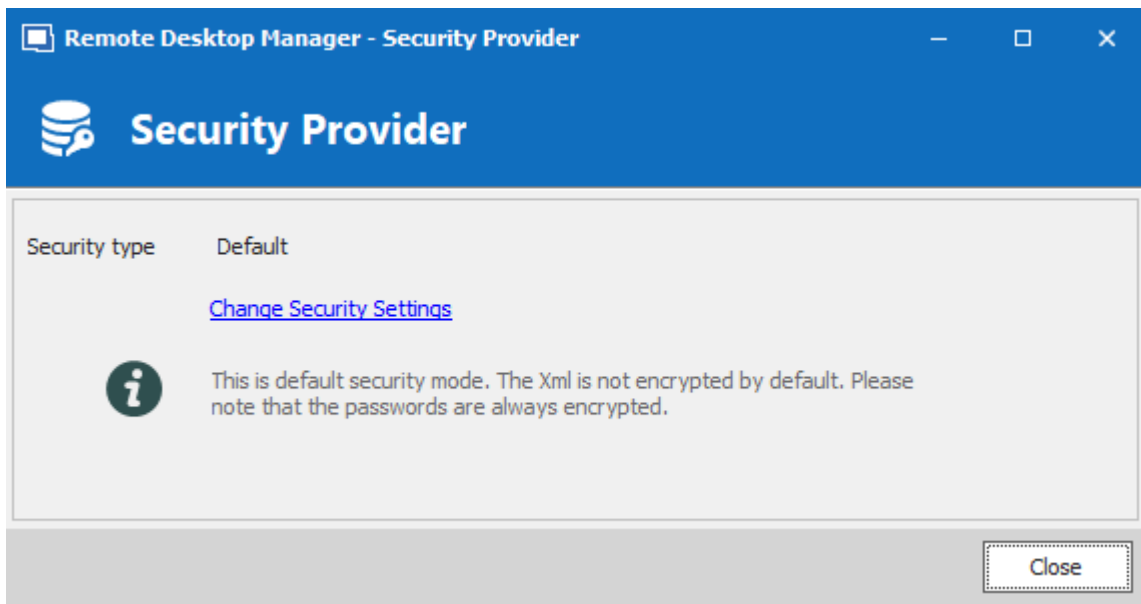


Please note that changing a security provider on a data source with a great number of entries is a lengthy operation.



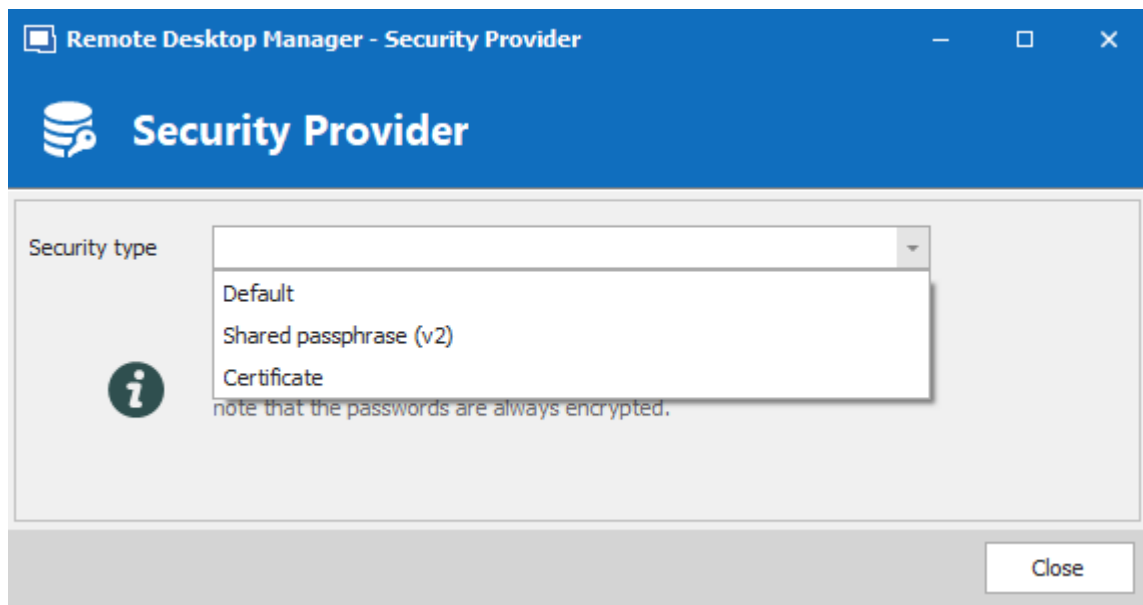
Applying a new security provider does process the whole database, therefore we advise you to create a backup prior to this operation.

1. Click on **Change Security Settings** to change the security provider.



*Security Provider*

2. Select a security type from the drop down list.



Security Type

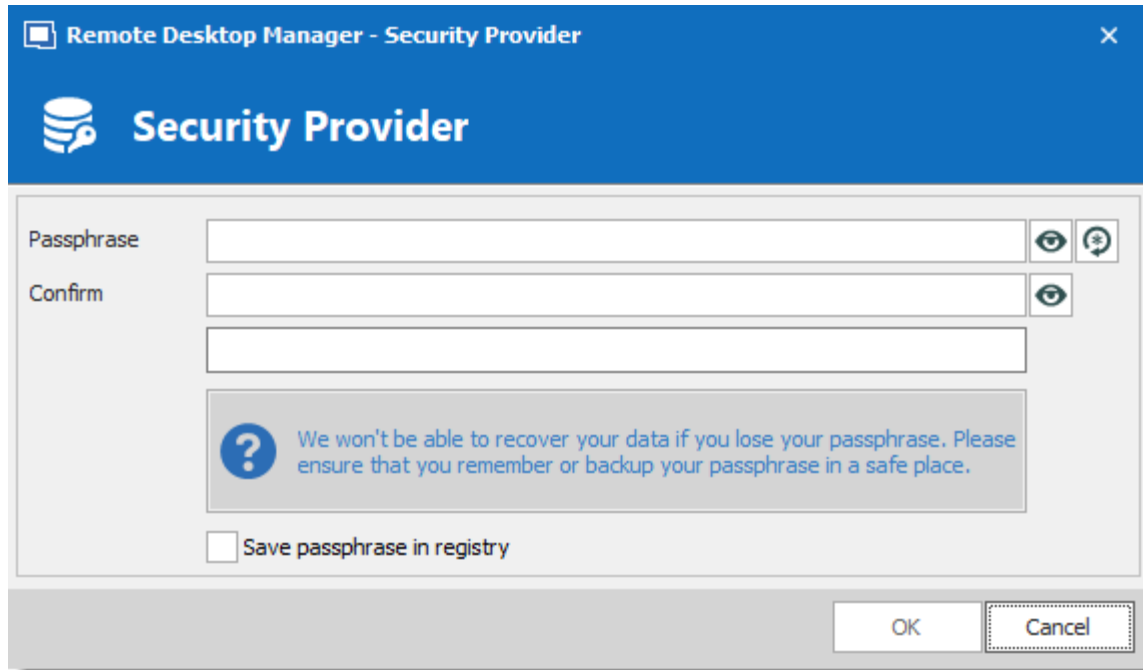
OPTION	DESCRIPTION
<b>Default</b>	This is the legacy security provider. The data is encrypted if the entry configuration is set accordingly in the advanced settings of the entries.
<b>Shared passphrase</b>	Set up a shared passphrase for the Security Provider.
<b>Certificate</b>	Set up a Certificate for the Security Provider.

## SHARED PASSPHRASE



If the passphrase is lost, **nothing** can be done to recover the data. When using a passphrase, always copy it to a secure location.





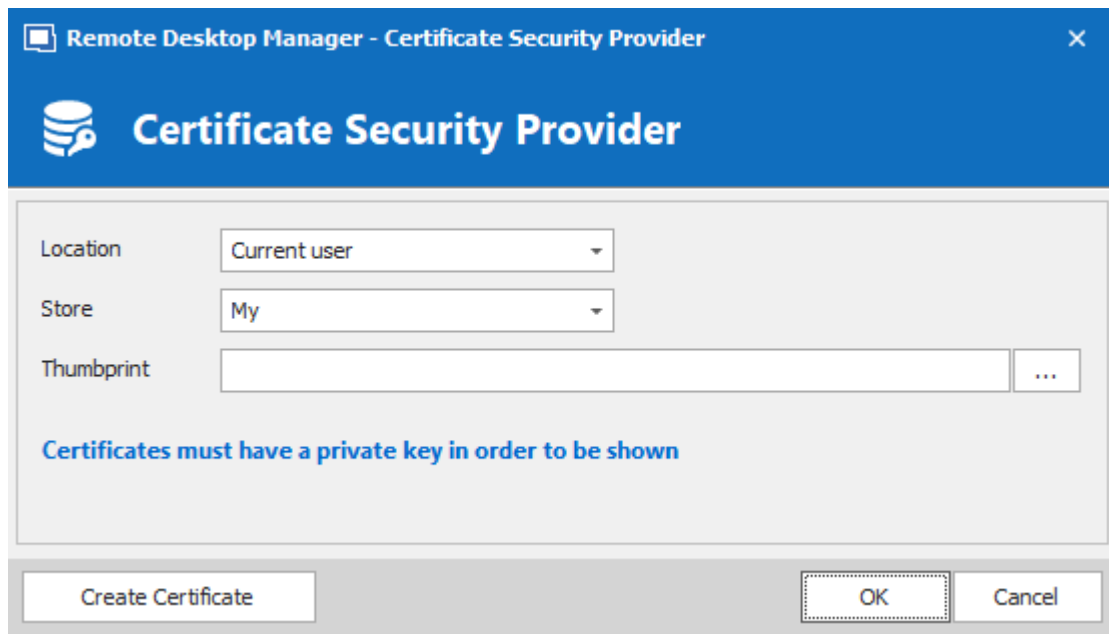
*Security Provider - Shared Passphrase*

Entries configuration data is encrypted using a mix of a key stored in Remote Desktop Manager and the passphrase you've entered.

The passphrase is required only when configuring the data source. A policy can be enabled to always prompt for the passphrase when connecting to the data source. For more information, please consult the [How to modify Group Policy Templates](#) topic.

## CERTIFICATE

When choosing **Certificate** as Security Provider, entries configuration data is encrypted using a mix of a key stored in Remote Desktop Manager and the private key contained in the certificate.



Security Provider - Certificate

OPTION	DESCRIPTION
<b>Location</b>	<p>Indicate the certificate location. Select between:</p> <ul style="list-style-type: none"> <li>• <b>Current user</b></li> <li>• <b>Local machine</b></li> </ul>
<b>Store</b>	<p>Indicate the store location of the certificate. Select between:</p> <ul style="list-style-type: none"> <li>• <b>Address book</b></li> <li>• <b>Authorization root</b></li> <li>• <b>Certificate authority</b></li> <li>• <b>Disallowed</b></li> <li>• <b>My</b></li> <li>• <b>Root</b></li> <li>• <b>Trusted people</b></li> <li>• <b>Trusted publisher</b></li> </ul>

OPTION	DESCRIPTION
<b>Thumbprint</b>	Select an existing certificate.

## CREATE CERTIFICATE

It is possible to create a Self Signed certificate by clicking on **Create Certificate**.

*Self Signed Certificate*

OPTION	DESCRIPTION
<b>Common name</b>	Name of the certificate.
<b>Key size (bits)</b>	Indicate the key size (bits) of the certificate. Select between:

OPTION	DESCRIPTION
	<ul style="list-style-type: none"> <li>• 384</li> <li>• 512</li> <li>• 1024</li> <li>• 2048</li> <li>• 4096</li> <li>• 8192</li> <li>• 16384</li> </ul>
<b>Valid from</b>	Start date of the certificate.
<b>Valid to</b>	End date of the certificate.
<b>Save to file (pfx)</b>	Save the certificate as a pfx file and secure this certificate with a password.
<b>Save to certificate store</b>	Indicate the location and the store to save the certificate.

## 6.7.4 Clean up

### 6.7.4.1 Clean Up Deleted History

## DESCRIPTION

The **Deleted History** permanently delete entries that had been previously deleted. Full history is always preserved because every entry "version" is kept in historical tables.



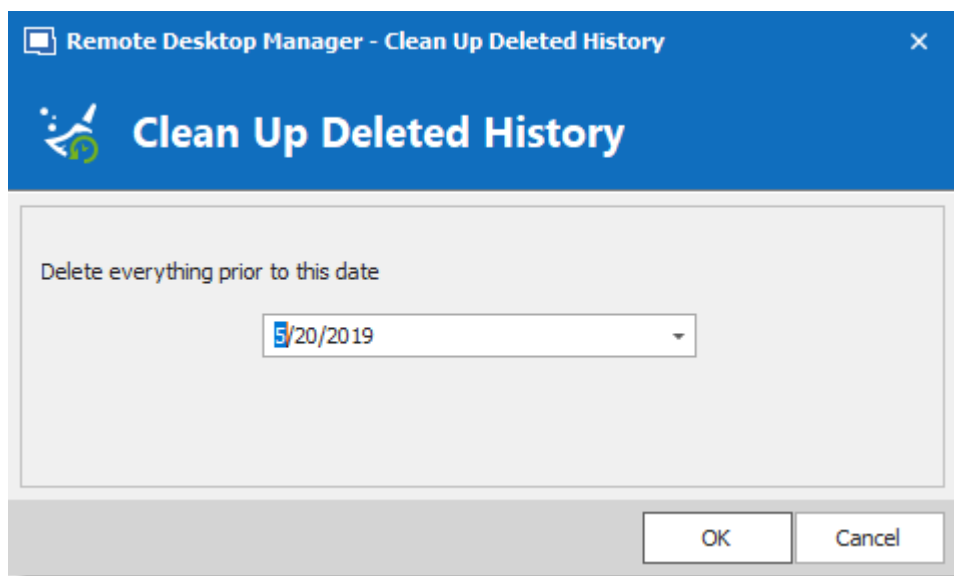
This feature requires an [Advanced Data Source](#).



You must be an administrator of the data source to perform this action.

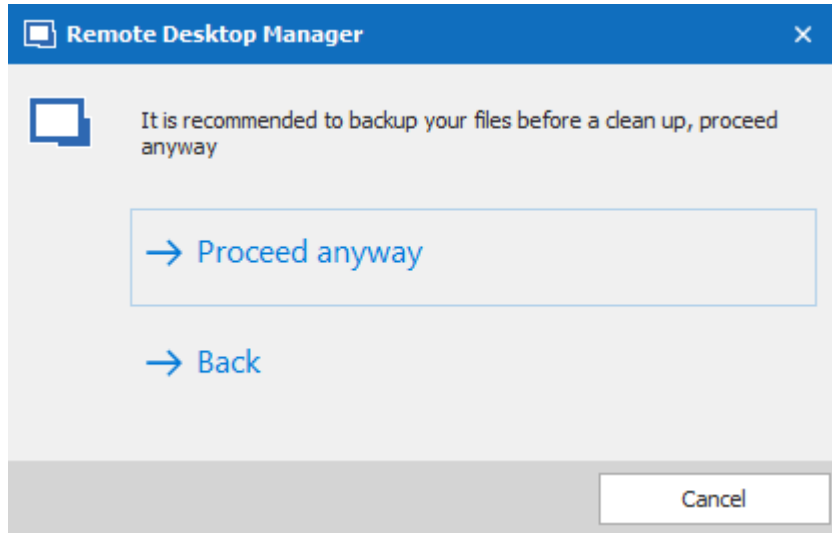
## SETTINGS

1. Select prior to which date you wish to permanently delete your deleted entries.



*Clean up Deleted History*

2. Confirm your choice prior to permanently delete your deleted entries.



Confirmation window



There will be no backup of your History. We strongly recommend to do a [Backup](#) before proceeding.

#### 6.7.4.2 Clean Up Entry History

## DESCRIPTION

The **Entry History** deletes the history attached to your entry, you can find the history by right clicking on your entry and selecting **View – Entry history**.



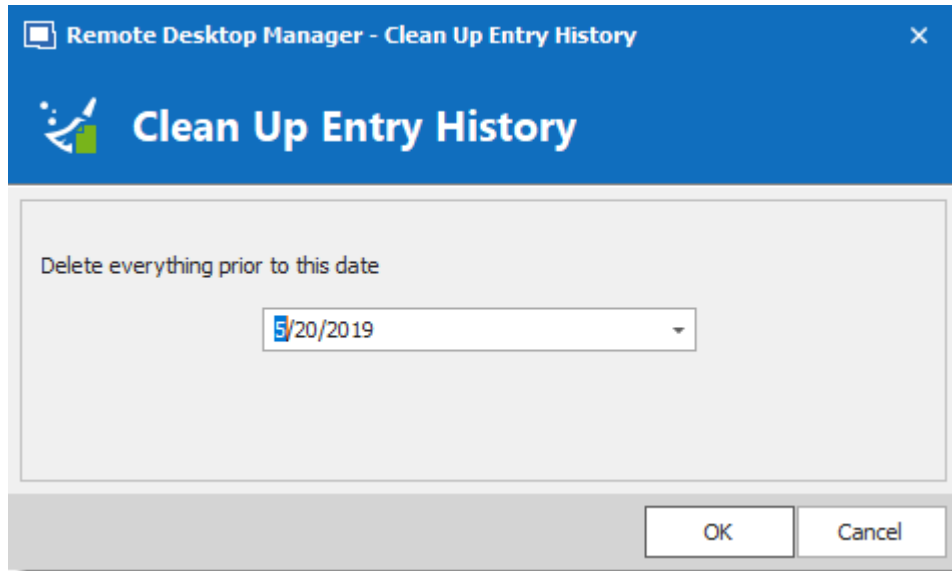
This feature requires an [Advanced Data Source](#).



You must be an administrator of the data source to perform this action.

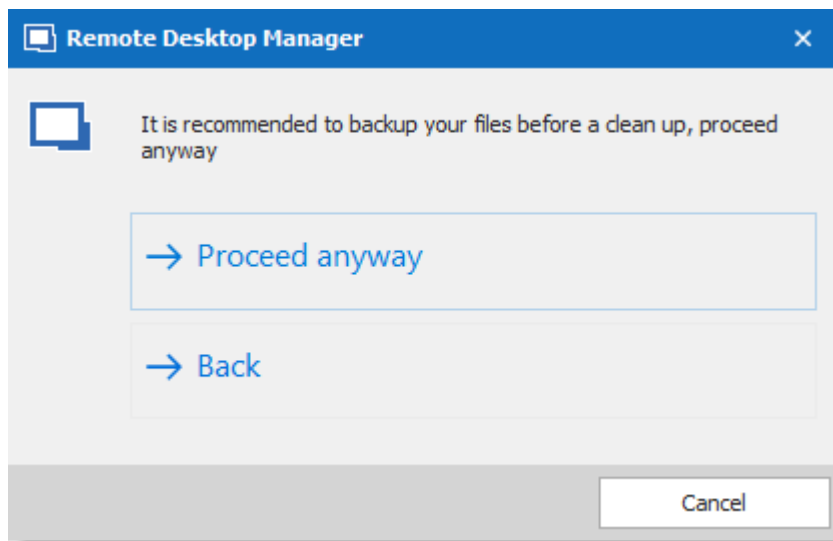
## SETTINGS

1. Select prior to which date you wish to permanently delete your Clean up entry history.



*Clean up Entry History*

2. Another window will appear to confirm your choice of deleting all the history prior to the chosen date.



*Confirmation window*



No History backup is created. We strongly recommend to do a [Backup](#) before proceeding.

### 6.7.4.3 Clean Up Activity Logs

## DESCRIPTION

The **Clean Up Activity Logs** will delete your data source's Activity Logs, you also have the option to clean up the **Administration logs** and set up a back up if desired..



This feature requires an [Advanced Data Source](#).

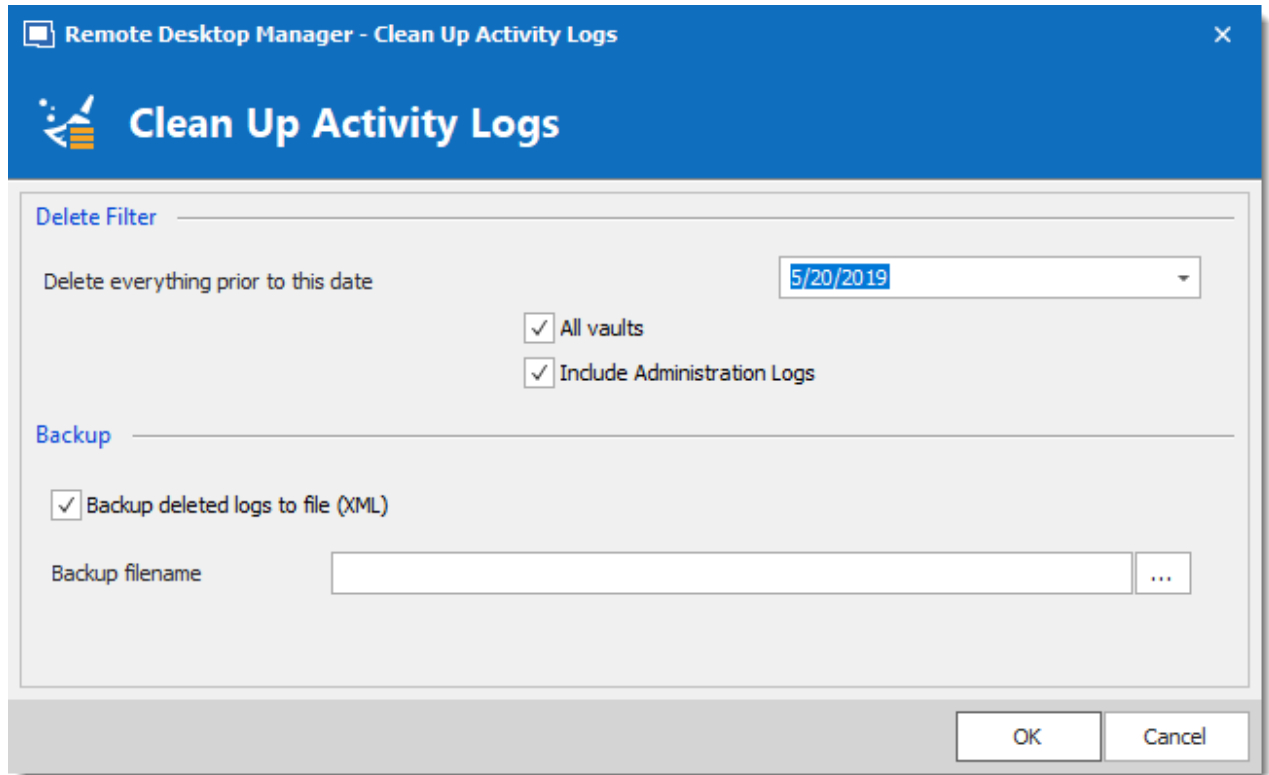


You must be an administrator of the data source to perform this action.

## SETTINGS

1. You must confirm your choice prior to permanently deleting your data source logs.





Remote Desktop Manager - Clean Up Activity Logs

## Clean Up Activity Logs

**Delete Filter**

Delete everything prior to this date: 5/20/2019

☒ All vaults

☒ Include Administration Logs

**Backup**

☒ Backup deleted logs to file (XML)

Backup filename:  ...

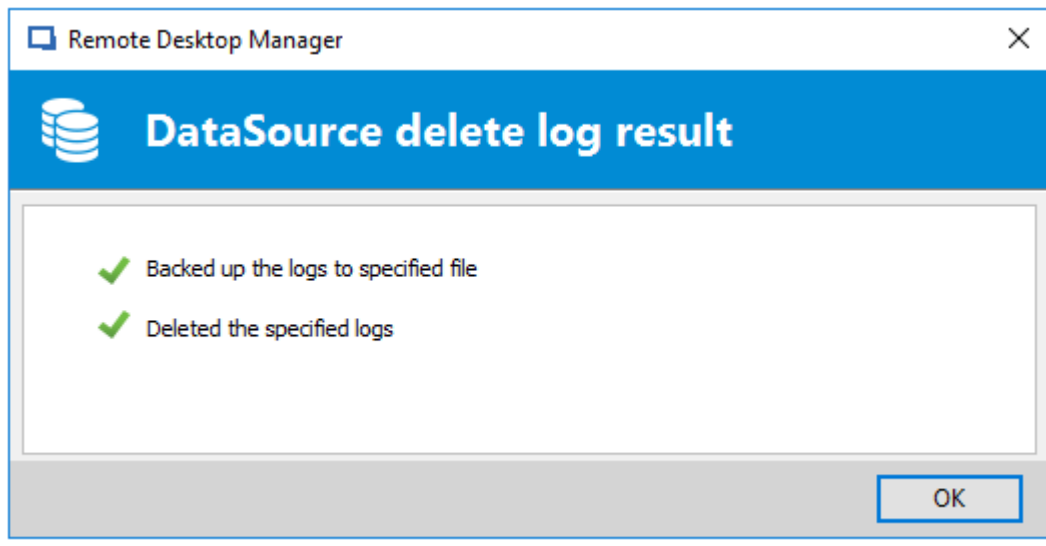
OK Cancel

*Clean up Data Source logs*



A backup of your log will be created as an XML file although it will then be impossible to import this file in Remote Desktop Manager.

2. Once you have entered your Backup file name and proceeded with the clean up a delete log result window will appear.



*Data Source Delete log result*

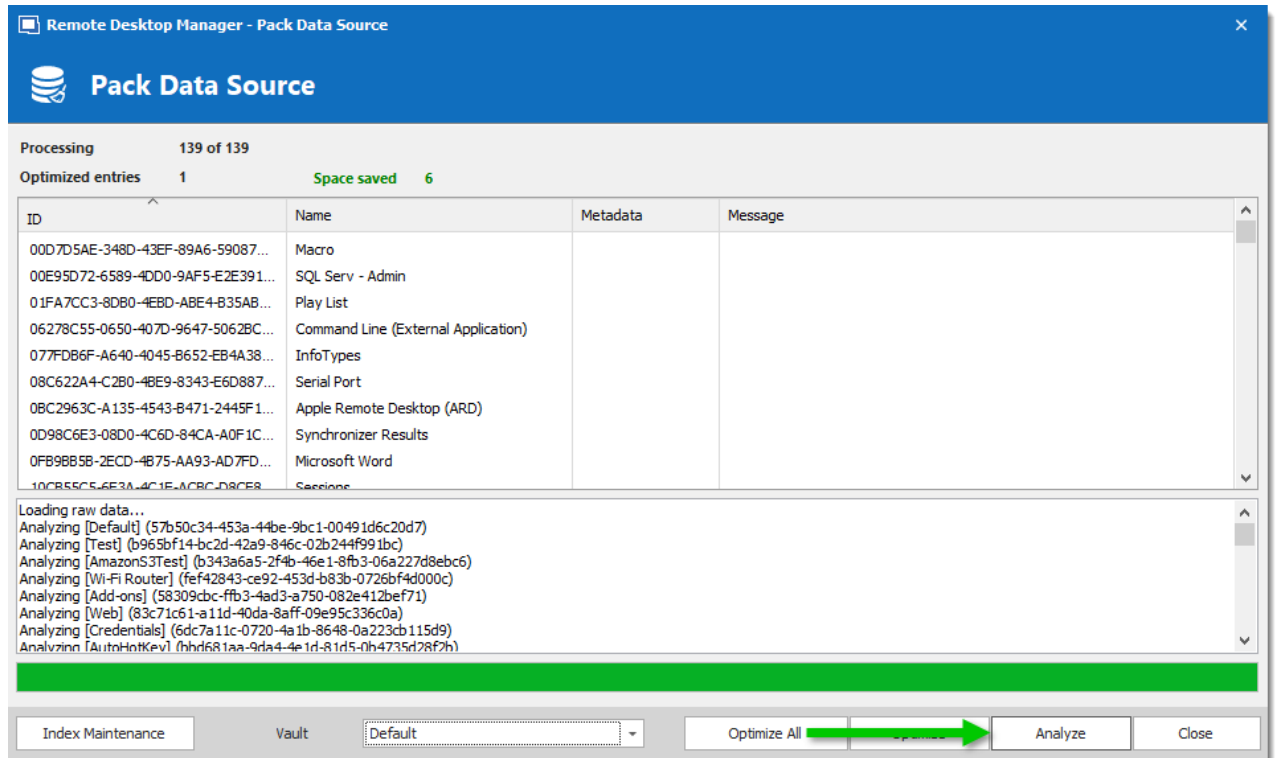
#### 6.7.4.4 Pack Data Source (Optimize)

### DESCRIPTION

When holding a great number of entries in your data source it is a best practice to compress them to avoid slowness issues when using your data source. The **Data Source (Optimize)** will analyze all your entries, compress them and then re-saves them, thus saving space in your data source.

### SETTINGS

1. Open the data source you wish to optimize. In **Administration** click on **Pack Data Source (Optimize)** and then click on **Analyze**.



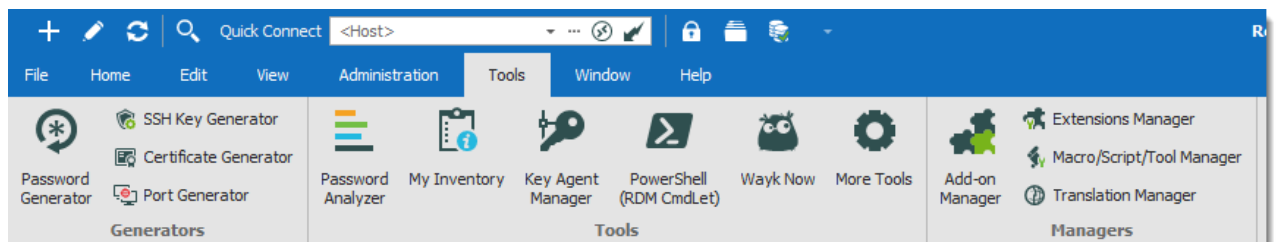
Pack Data Source (Optimize) - Analyze

2. Once the Analyze is completed click on **Optimize** to proceed with the optimization of your data source. You can select which **Vault** you wish to **Analyze** and **Optimize**, or use the **Optimize All** feature to perform the **Optimize** action on all available **Vaults**.

## 6.8 Tools

### DESCRIPTION

The **Tools** tab contains your Add-on and Extensions manager as well as your Devolutions Password Server Console, Generators and multiple useful tools.



Ribbon - Tools

## GENERATORS

OPTION	DESCRIPTION
<b>Password Generator</b>	Opens the <a href="#">Password Generator</a> window. You can use this to generate password according to pre-determined criteria for better security.
<b>SSH Key Generator</b>	Launches the <a href="#">SSH Key Generator</a> . SSH keys provide a secure way of logging into a virtual private server with SSH than using a password alone.
<b>Certificate Generator</b>	Launches the <a href="#">Certificate Generator</a> . With this you can create a self-signed certificate, which is an identity certificate that is signed by the same entity whose identity is certified.
<b>Port Generator</b>	Launches the <a href="#">Port Generator</a> . With this you can generate ports for your connections.

## TOOLS

OPTION	DESCRIPTION
<b>Password Analyzer</b>	Opens the <a href="#">Password Analyzer</a> . This is used to evaluate the strength of passwords stored in the data source. This feature is restricted to Administrators only.
<b>My Inventory</b>	Set up a My Inventory report.
<b>Key Agent Manager</b>	Opens the <a href="#">Key Agent Manager</a> . This is used to hold all your SSH Keys in memory, already decoded and ready for them to be used.

OPTION	DESCRIPTION
<b>PowerShell (RDM CmdLet)</b>	Opens the <a href="#">PowerShell (RDM CmdLet)</a> .
<b>Wayk Now</b>	Launches the <a href="#">Wayk Now</a> application.
<b>More Tools</b>	The <b>More Tools</b> window contains a variety of application tools such as: <a href="#">Chocolatey Console</a> , <a href="#">Local RDP/RemoteApp Manager</a> , <a href="#">Playback (Ansi)</a> , <a href="#">RDM Agent</a> and more.

## MANAGERS

OPTION	DESCRIPTION
<b>Add-on Manager</b>	Opens the Add-on Manager. It is used to simplify the management of different add-ons.
<b>Extensions Manager</b>	Opens the Extensions Manager. This is used to simplify the management and installation of Web Browser extensions and other miscellaneous extensions.
<b>Macros/Scripts/Tools Manager</b>	Opens the Macros/Scripts/Tools Manager. This is used to simplify the import of some pre-determined sessions tools.
<b>Translation Manager</b>	Opens the Translation Manager. A cloud based translation repository that is managed by an external application named Devolutions Localizer.

### 6.8.1 Generators

#### 6.8.1.1 Password Generator

## DESCRIPTION

The **Password Generator** is available in the **Tools – Password Generator** menu. It allows to create random passwords that are and difficult to interpret or predict, due to a mix of uppercase and lowercase letters, numbers and punctuation symbols.

You can also create password generator templates to generate passwords. After you have selected your mode and settings, you can then create your template.

## MODE

### DEFAULT

Customize all criteria you would want your password to have.

Remote Desktop Manager - Password Generator

**Password Generator**

Template: Default + X

Mode: Default

Minimum length: 8

Minimum lowercase characters: 1

Minimum uppercase characters: 1

Minimum numeric characters: 3

Minimum symbols: 1

B4m78v-K	xYq345t-	+4z-24K	j2yD3A4-
7-L80dhI	bj-F24C5	7j-62lPY	tv6nV-51
d_y352cK	U6_7v06p	5D01s_yD	593WzZ_N
KT6_o00m	U10_Rz7u	W_6et1S0	1wc_8sU6
@66P6knt	p002.Qbp	7G5H22.f	@N7n7a,7
6u74/XO1	K6T+10yV	e455%Y4G	!50L9rD#

Generate

Copy to Clipboard

Very Strong

BRAVO | four | mike | seven | eight | victor | hyphen | KILO

Count: 30

Forbidden Password

Close

*Password Generator - Default*

## ADVANCED SETTINGS

Select the type and amount of characters to include in the password.

Remote Desktop Manager - Password Generator

**Password Generator**

Template: Default + X

Mode: Advanced settings

Password length: 12

☒ Upper-case (A, B, C, ...) 2
 ☐ Underline ( ) 0
 ☐ High ANSI characters 0

☒ Lower-case (a, b, c, ...) 2
 ☐ Space ( ) 0
 ☐ XML Compliant

☒ Digits (0, 1, 2, ...) 5
 ☒ Special (!, \$, %, &, ...) 2

☒ Minus (-) 1
 ☐ Brackets ([, ], {, }, (, ), <, >) 0

Include the following characters:

Exclude the following characters:

3gY16x4J-l9+	35&q6%kYU-83	l0-02Q9W^e8/	=71B5-6cA*s4
.0&8D-i049oC	*#Cz6-F7w386	R15-7%1j?V2p	0@c2g&TB-630
bG,2h67W7?-4	4?26y?c5-92C	0F%1/E967u-b	6#W506:-j3Sl
y7=W67V-n@63	570Na^C\z45-	:2,-14hw177G	uN6Qx19:47&-
40TK28@0-gs;	1:-X44,Xe40q	w94C?6n9-3+P	7wT/n2!3L53-
n22YV-.#j030	#UxY9d\$902-9	xH3y20-5'^V6	99G9*n85-sD@

Perfect

three | golf | YANKEE | one | six | x-ray | four | JULIET | hyphen | backslash | nine | plus

Count: 30

Generate

Copy to Clipboard

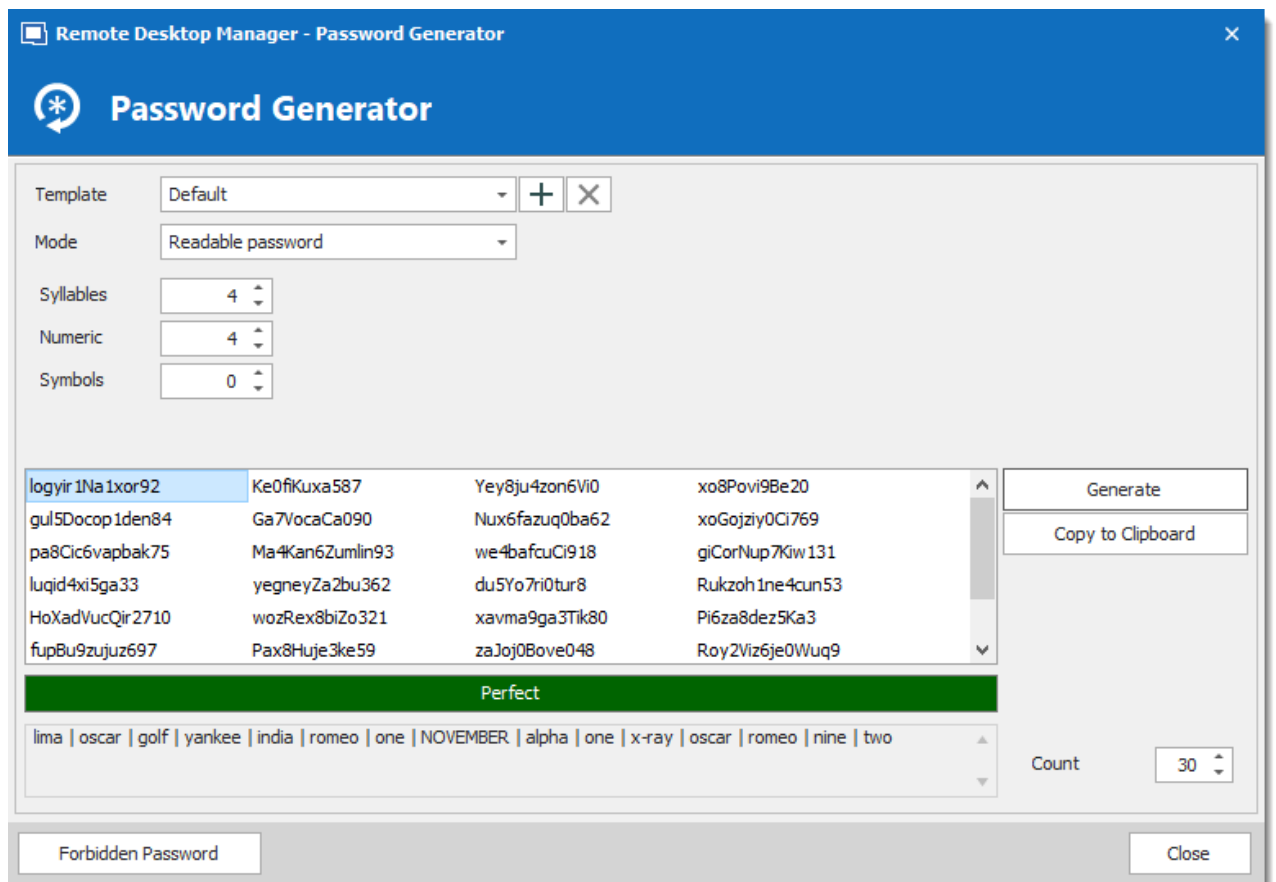
Forbidden Password

Close

*Password Generator - Advanced Settings*


## READABLE PASSWORD

Generate passwords that are readable but are not actual words.

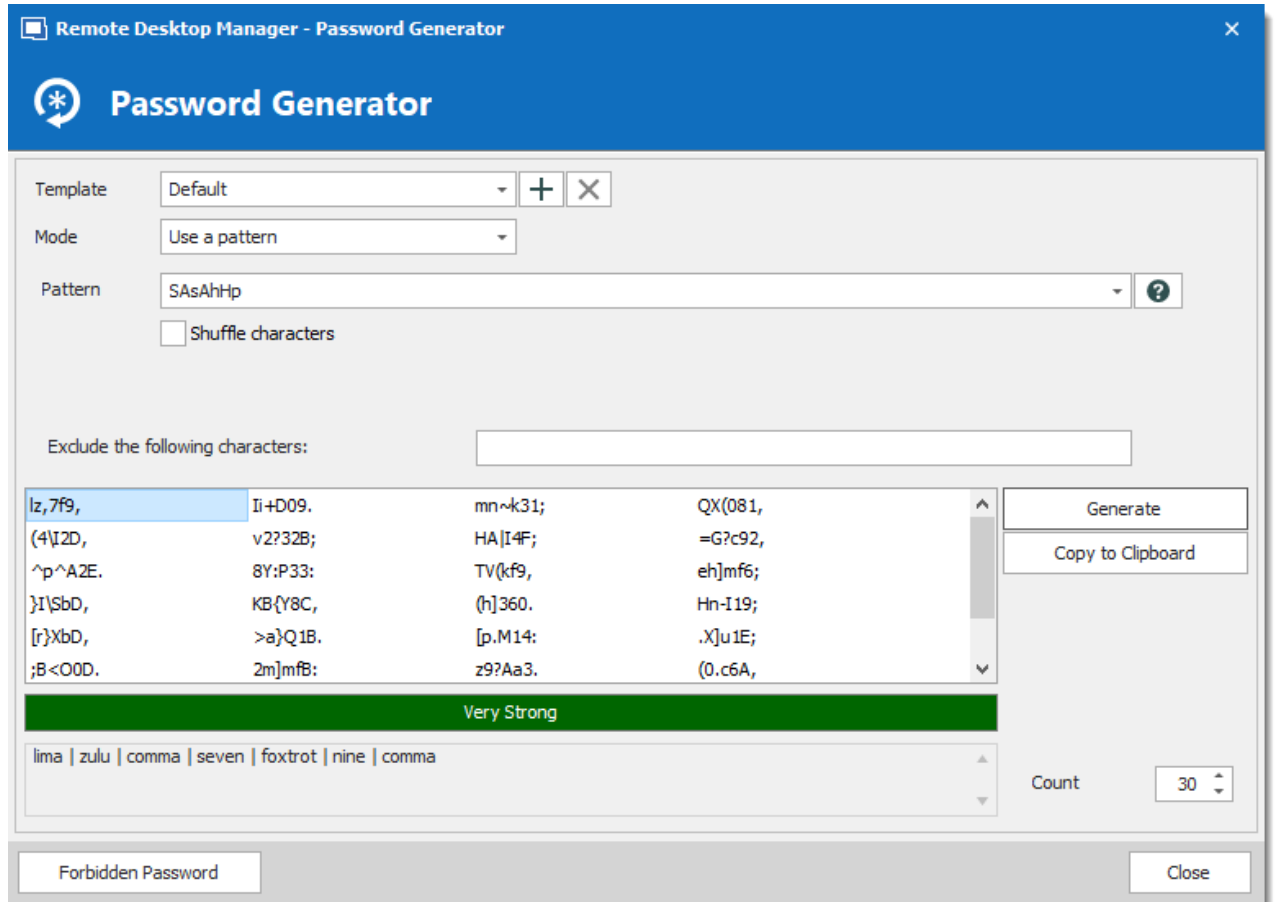


*Password Generator - Readable password*

## USE A PATTERN

Press the  button and select any pattern you need to create the passwords, you can also exclude certain characters if desired. A list of the most recent used pattern will also be created.





*Password Generator - Use a pattern*

The following are supported patterns:

DESCRIPTION	KEY	SAMPLE
<b>Lower-Case Alphanumeric</b>	a	abcdefghijklmnopqrstuvwxyz 0123456789
<b>Mixed-Case Alphanumeric</b>	A	ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklm nopqrstuvwxyz 0123456789
<b>Bracket</b>	b	()[]{}<>
<b>Lower-Case Consonant</b>	c	bcd fghjklmnpqrstvwxyz

DESCRIPTION	KEY	SAMPLE
<b>Mixed-Case Consonant</b>	C	BCDFGHJKLMNPQRSTUVWXYZ bcd fghjklmnpqrstwx yz
<b>Digit</b>	d	123456789
<b>Lower-Case Hex Character</b>	h	0123456789 abcdef
<b>Upper-Case Hex Character</b>	H	0123456789 ABCDEF
<b>Lower-Case Letter</b>	l	abcdefghijklmnopqrstuvwxyz
<b>Mixed-Case Letter</b>	L	ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklm nopqrstuvwxyz
<b>Punctuation</b>	p	,,:;
<b>Printable 7-Bit Special Character</b>	s	!"#\$%&'()*+,-./:;<=>?[ \^_{}~
<b>Printable 7-Bit ASCII</b>	S	A-Z, a-z, 0-9, !"#\$%&'()*+,-./:;<=>?[ \^_{}~
<b>Upper-Case Letter</b>	u	ABCDEFGHIJKLMNOPQRSTUVWXYZ
<b>Upper-Case Alphanumeric</b>	U	ABCDEFGHIJKLMNOPQRSTUVWXYZ 0123456789
<b>Lower-Case Vowel</b>	v	aeiou
<b>Mixed-Case Vowel</b>	V	AEIOU aeiou
<b>High ANSI</b>	x	From '~' to U255 (excluding U255)

DESCRIPTION	KEY	SAMPLE
Upper-Case Consonant	z	BCDFGHJKLMNPQRSTVWXYZ
Upper-Case Vowel	Z	AEIOU
Escape (Fixed Char)	\	Use following character as is
Escape (Repeat)	{n}	Repeats the previous character n times
Custom character	[x]	Define a custom character sequence

## PRONOUNCEABLE PASSWORD

Generate passwords that are pronounceable, but are not actual words.

**Remote Desktop Manager - Password Generator**

## Password Generator

Template: Default + X

Mode: Pronounceable password

Minimum password length: 11

Case mode: Mixed case

Include the following characters:

☒ Digits (0, 1, 2, ...)

☒ More pronounceable

Sty0Phe6K3	A6Kick9AVu0	Pre1Ty2GIKy9	E0Se0HaRiSha2
Rhezi1RuPi4	U0Na9Thu9Yichi3	La0HiTy6Que3	Ne9Mi7Re4Cy7
Qui8Nu2KuChu1	Na0Le8FiLe8	Vo0Ho7QuoDu9	Spu9Py0CiO1
Wro7BuHe2Ghoma6	E0Gu9Shed2	Myack4O7Su9	I4Ja0Te8OZi3
Ye0Phy0CeQui7	Va8Chi3XiFa2	A4No3Ju5IXey7	Ko6PhyNo7Thack7
E3ThaPyeRay3	Wi1YixackU5	Ti6Sha7Shu0	Rhycucki2Go6

Perfect

SIERRA | tango | yankee | zero | PAPA | hotel | echo | six | KILO | india | three

Count: 30

Forbidden Password

Generate

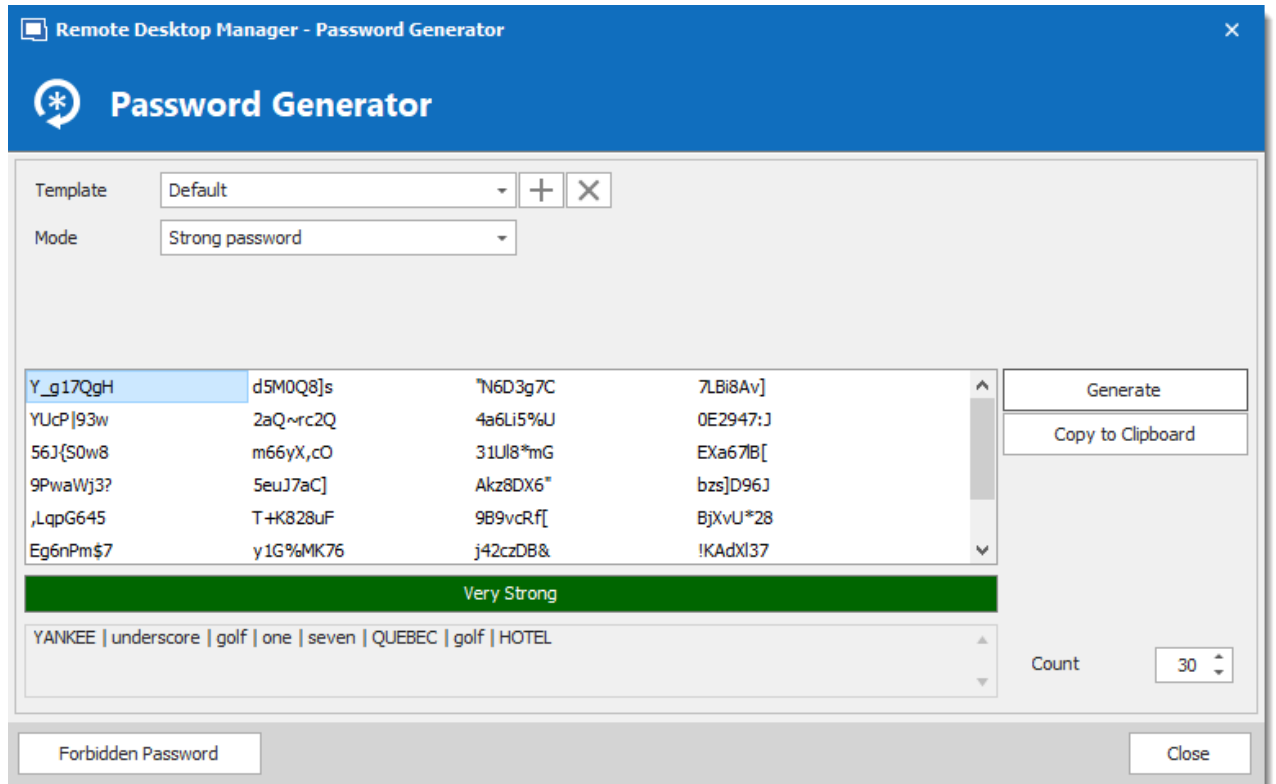
Copy to Clipboard

Close

*Password Generator - Pronounceable password*

## STRONG PASSWORD

Generate an 8 character passwords with alphanumeric and special characters.



*Password Generator - Strong password*

### 6.8.1.2 SSH Key Generator

## DESCRIPTION

SSH keys provide a secure way of logging into a virtual private server with SSH than using a password alone. While a password can eventually be cracked with a brute force attack, SSH keys are nearly impossible to decipher by brute force alone.

## SETTINGS

Remote Desktop Manager - SSH Key Generator

**SSH Key Generator**

Key algorithm: ☒ RSA ☐ DSA

Key size: 1024

Comment: username@hostname Generate

You can add this into OpenSSH's authorized keys file

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQGC/djD6Dv8P0eTWDVIK3XbSXrtwSXDuIAI1O7F9XeFNva/nT2e3QFBMSzrHa7c5
v6l6b2TRo7WdYVg6GMciVJ4TwdMIneuFflgsighKmj4uttvHbfUywoHXGIndDC1G99PC61wUKwOZ
+Y7ShrOLlWd1TwJss5/o+S9ztgD82ayrUQ== username@hostname
```

MD5 Fingerprint: 07:21:38:79:90:99:7a:3a:ee:36:29:fa:af:65:7a:a0

SHA-1 Fingerprint: 81:e6:4f:df:a4:4e:05:73:84:63:f5:31:37:e0:02:b5:f9:ff:dd:84

Passphrase:

Confirm passphrase:

Load Private Key... Save Public Key... Save Private Key...

Close

SSH Key Generator

OPTION	DESCRIPTION
<b>Key algorithm</b>	<p>You can choose between:</p> <p><b>RSA:</b> RSA can be used for signing/verification and also for encryption/decryption. When using RSA it is recommended to use a 2048 bits key size.</p> <p><b>DSA:</b> It is faster in signing but slower in verifying. It can only be used for signing/verification it <b><u>does not encrypt/decrypt</u></b>. When using DSA it is a recommended to use a 1024 bits key size.</p>
<b>Key size</b>	You can choose your SSH Key size between:

OPTION	DESCRIPTION
	<p><b>1024 bits:</b> Minimum key size</p> <p><b>2048 bits:</b> Default and recommended key size</p> <p><b>4096 bits:</b> Maximum key size</p>
<b>Comment</b>	Enter your username and the name of the computer you're transferring your key to.
<b>Load Private Key</b>	This feature will allow you to import a previously saved SSH Key.
<b>Save Public Key</b>	Saving the public key will generate a *.pub file. Simply enter a file name when prompted.
<b>Save Private Key</b>	<p>You will have the option of saving your Private Key in different format, choose between:</p> <ul style="list-style-type: none"> <li>• PKCS #8 Private Key (*.pri)</li> <li>• PuTTY Private Key (*.ppk)</li> <li>• OpenSSH Private Key (*.pri)</li> </ul>

If you did not specify a passphrase you will have to confirm that you do not wish to use a passphrase.



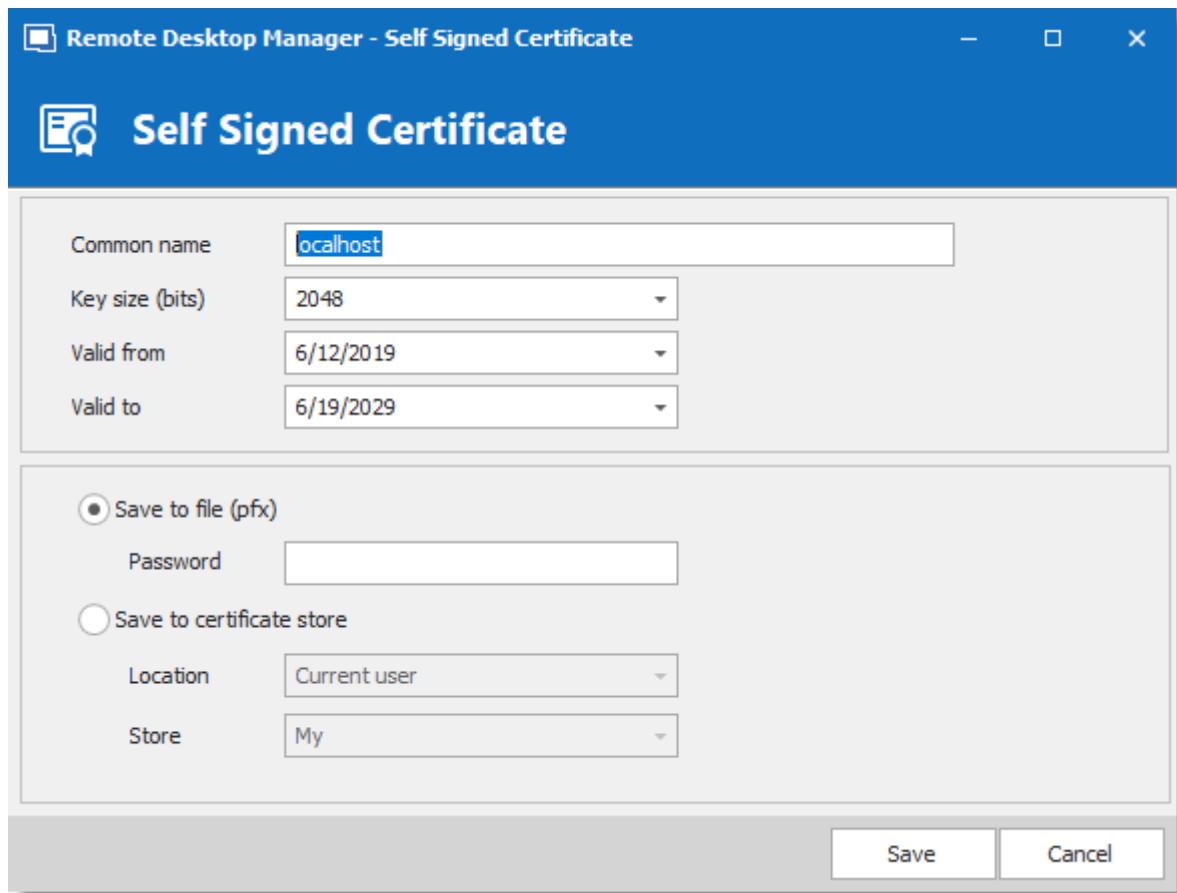
If using the [Key Agent Manager](#) you must chose the PuTTY Private Key (.ppk) file format or the OpenSSH Private Key (.pri) file format. The PKCS Private Key is not a supported file format for the Key Agent Manager.

### 6.8.1.3 Certificate Generator

## DESCRIPTION

The **Certificate Generator** allows you to create a self signed certificate which is an identity certificate that is signed by the same entity whose identity is certified.

## SETTINGS



Remote Desktop Manager - Self Signed Certificate

### Self Signed Certificate

Common name:

Key size (bits):

Valid from:

Valid to:

☒ Save to file (pfx)

    Password:

☐ Save to certificate store

    Location:

    Store:

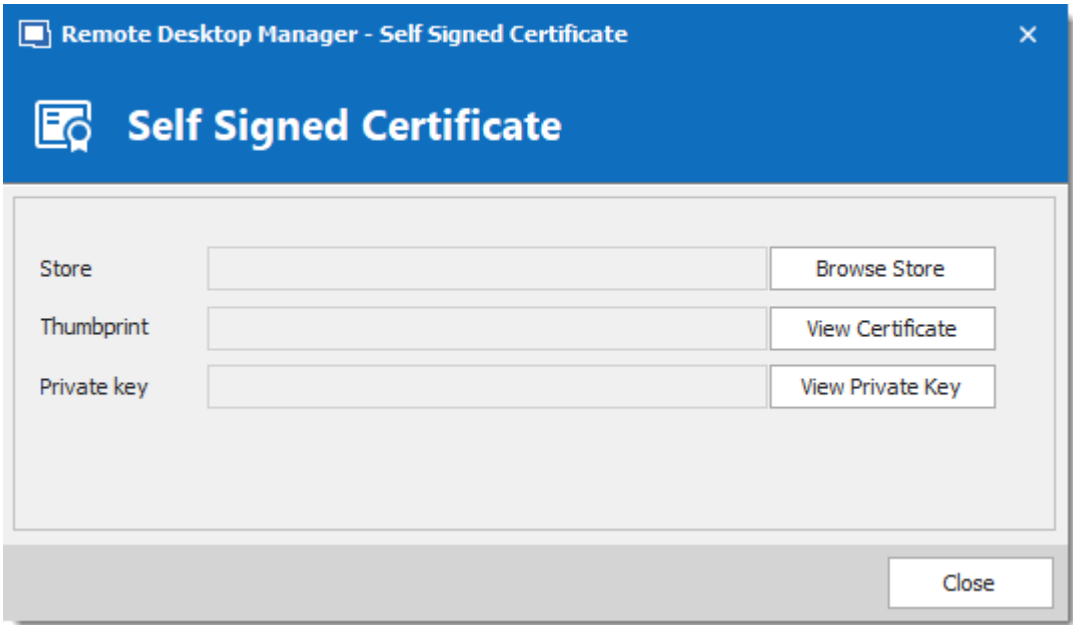
Save Cancel

*Certificate Generator - Self Signed Certificate*

OPTION	DESCRIPTION
<b>Common name</b>	Name of the certificate.
<b>Key size (bits)</b>	Indicates the key size (bits) of the certificate. Select between: <ul style="list-style-type: none"><li>• <b>1024</b></li><li>• <b>2048</b></li><li>• <b>4096</b></li><li>• <b>8192</b></li></ul>



OPTION	DESCRIPTION
	<ul style="list-style-type: none"><li>• <b>16384</b></li></ul>
<b>Valid from</b>	Starting date of the certificate.
<b>Valid to</b>	Expiration date of the certificate.
<b>Save to file (pfx)</b>	Save the certificate into a *.pfx file and secure this certificate with a password.
<b>Save to certificate store</b>	Indicate the location and the store to save the certificate.
<b>Location</b>	Indicate the location of the certificate. Select between: <ul style="list-style-type: none"><li>• <b>Current user</b></li><li>• <b>Local machine</b></li></ul>
<b>Store</b>	Indicate the store location of the certificate. Select between: <ul style="list-style-type: none"><li>• <b>Address book</b></li><li>• <b>Authorization root</b></li><li>• <b>Certificate authority</b></li><li>• <b>Disallowed</b></li><li>• <b>My</b></li><li>• <b>Root</b></li><li>• <b>Trusted people</b></li><li>• <b>Trusted publisher</b></li></ul>



Self Signed Certificate

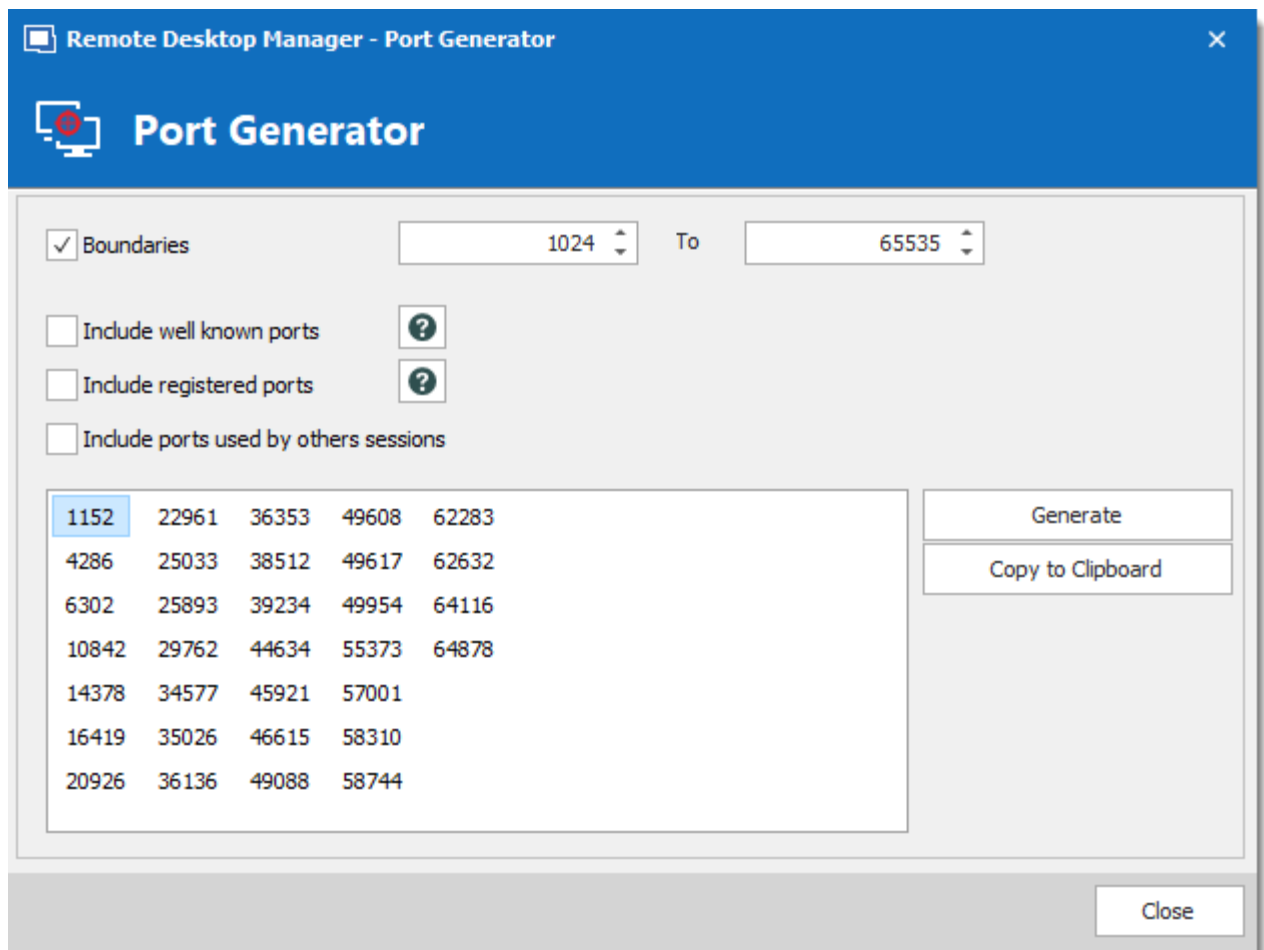
OPTION	DESCRIPTION
Store	Indicate the store where the certificate will be located.
Browse Store	Browse the store that is indicated in the store field.
Thumbprint	Display the certificate thumbprint.
View Certificate	Display the certificate that you have created.
Private Key	Display the certificate private key
View Private Key	View the private key file on your computer.

6.8.1.4 Port Generator

DESCRIPTION

The Port Generator allows you to generate ports for your connections.

## SETTINGS



*Port Generator*

OPTION	DESCRIPTION
<b>Boundaries</b>	Determinate the port range to generate the ports between those 2 numbers.
<b>Include well known ports</b>	Include ports from range 0 to 1023. They are the well-known ports or system ports. They are used by system processes that provide widely used types of network services
<b>Include registered ports</b>	Include ports from range 1024 to 49151. They are assigned by IANA for specific service upon application by a requesting

OPTION	DESCRIPTION
	entity. On most systems, registered ports can be used by ordinary users.
<b>Include ports used by others sessions</b>	Include the ports that are already used by other sessions.

## 6.8.2 Tools

### 6.8.2.1 Devolutions Localizer

## WHAT IS DEVOLUTIONS LOCALIZER?

Devolutions Localizer is our custom translation tool for our client applications.

So far, with the help of several generous and talented members of our community, Remote Desktop Manager has been translated from English to the following languages:

- Chinese (Simplified) Legacy
- Chinese (Traditional, Taiwan)
- Dutch
- French
- German
- Italian
- Polish
- Russian
- Swedish
- Ukrainian

## GETTING STARTED

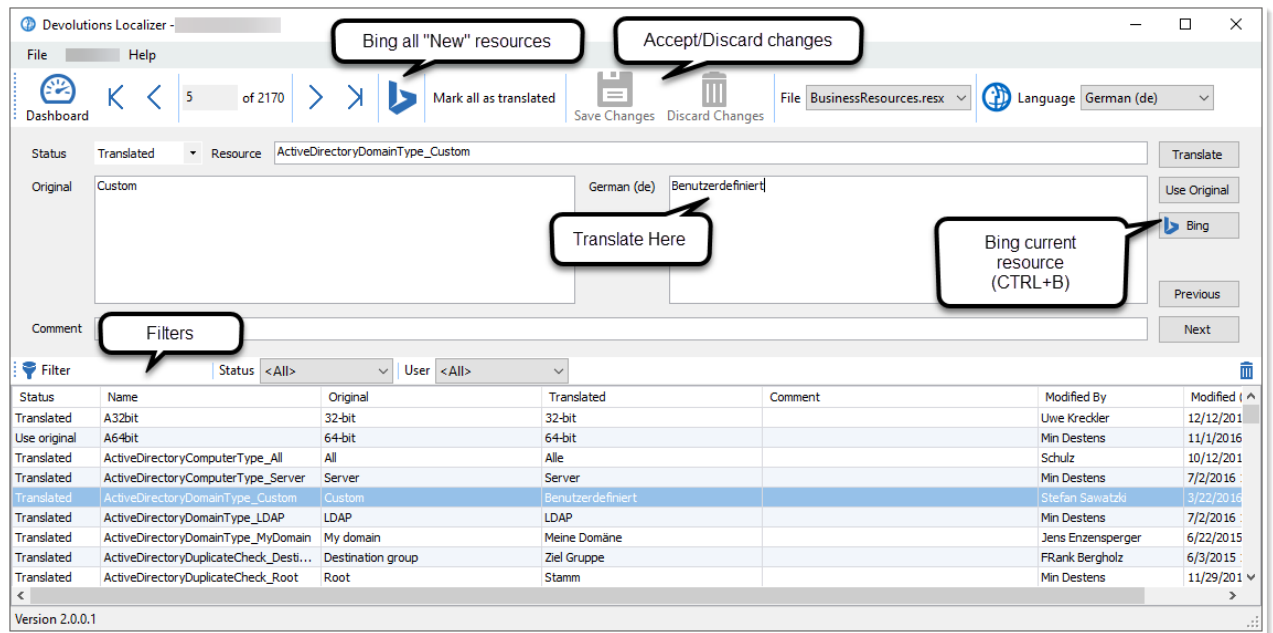


An account is required to use the Devolutions Localizer. You can join our team and get started by signing up here: <https://devolutions.net/Home/Contribute>.

If you're interested in helping your fellow IT pros around the world, please sign up to be one of our wonderful contributors. Our Localizer app makes the process very efficient, and you can work at your own pace, and whenever you have time!

## OVERVIEW

From the **dashboard view** you get a quick progress overview, simply click the “**Translate**” button and start translating.



*Devolutions Localizer*

## KEYBOARD SHORTCUTS

Devolutions Localizer also features several keyboard shortcuts to speed up the translation process:

- **CTRL+D:** Mark current resource as “**Translated**”.
- **CTRL+E:** Mark current resource as “**Use original**”, this ignores any translation text and will display the original value as is.
- **CTRL+DOWN:** Next resource.
- **CTRL+UP:** Previous resource.
- **CTRL+B:** Request Bing translation for the current string.
- **CTRL+S:** Save all pending changes.
- **CTRL+F:** Enable/disable filtering.

### 6.8.2.2 Password Analyzer

## DESCRIPTION



The information in this topic is how the "Legacy" mode of password analysis works. The mode can be changed in the System Settings for ZXCVCBN . The "Legacy" mode is not the default mode.

The **Password Analyzer** evaluates the strength of passwords stored in the data source. To access the password analyzer, navigate to **Tools – Password Analyzer**.

A password analyzer control is also displayed under most password fields of entries.

The screenshot shows the 'Entry Properties' dialog box with the 'General' tab selected. The 'Host' field contains 'QA-JAF', 'RDP type' is 'Normal', 'Username' is 'John', and 'Domain' is empty. The 'Password' field is highlighted with a green box and contains a series of dots. Below the password field, a green bar indicates the strength as 'Perfect'. To the right of the password field are icons for visibility, copy, and paste, and a '2 months' expiration date.

*Entry Properties - Password Field With Password Analyzer*

The password analyzer follows a set of rules to determine the strength of the password with a score from 0 to 100. There are two categories of rules.

## REINFORCE

These are the rules which make the passwords stronger:

- The password length
- The number of uppercase letters (A-Z)
- The number of lowercase letters (a-z)
- The number of digits (0-9)

- The number of symbols (!, @, #, \$, etc.)
- The number of digits or symbols in the middle of the password
- Three or more of the rules above are met

The minimum requirements for a **Strong** password are:


- The password is at least 5 characters long
- The password contains uppercase and lowercase characters
- The password contains digits

## WEAKENING

These are the rules which make the passwords weaker:

- The password contains only letters
- The password contains only digits
- The password has repeated characters
- The password has consecutive uppercase letters (two or more)
- The password has consecutive lowercase letters (two or more)
- The password has consecutive digits (two or more)
- The password has sequential letters (ABCD, DCBA)
- The password has sequential digits (1234, 4321)

## SETTINGS


**Password Analyzer**


**Settings**

☐ Show all
 ☐ Show private vault


☐ Show VPN analysis
 ☐ Show pwned password analysis

**Analysis**

Name	Folder	Username	Date	Since	Occurence	Password Strength	Password Length
Active Directory	Enterprise\Synchroni...	administrator	1/14/2019 9:11 AM	6 months	2	Weak	7
Active Directory Console	Enterprise\Sessions\...	administrator	12/19/2018 6:49 AM	7 months	2	Weak	7
BasicCred	Enterprise\Credentials	David	11/13/2018 10:45 ...	7 months	4	Popular	6
CredPV		David	1/2/2019 11:16 AM	6 months	4	Popular	6
Email Account	Enterprise\InfoTypes	Email	11/13/2018 8:42 AM	8 months	1	Good	9
Login (Account)	Enterprise\InfoTypes	TestLaccount	11/13/2018 8:17 AM	8 months	2	Weak	13
Login (Web)	Enterprise\InfoTypes	TestUsername	11/13/2018 8:35 AM	8 months	2	Weak	13
RDPTest	Enterprise\Sessions\...		4/30/2019 9:17 AM	2 months	1	Weak	4
RDPTest - Copy	Enterprise\Sessions\...	test	1/18/2019 3:19 PM	6 months	4	Popular	6
TeamViewer	Enterprise\Sessions\...	845370611	12/19/2018 11:08 ...	7 months	1	Good	6
test	Enterprise\Sessions\...	test	2/5/2019 9:51 AM	5 months	1	Popular	4
Wi-Fi Router	Enterprise\InfoTypes		11/13/2018 8:45 AM	8 months	1	Good	13
Windows Admin Center	Enterprise\Sessions\...	david	2/5/2019 10:02 AM	5 months	1	Perfect	8




Forbidden Password

 Export Settings

ID E3CF99F5-1027-47A5-9760-3EDDF4D196A6

## Tools - Password Analyzer

OPTION	DESCRIPTION
<b>Show all</b>	Shows you all the entries in your session, including those without password.
<b>Show VPN analysis</b>	Add the VPN Host column.
<b>Edit</b> 	Open the current entry to edit it.
<b>Forbidden Password</b>	Create a list of prohibited passwords.
<b>Export Settings</b>	Export the password analyzer settings.

## 6.8.2.3 Key Agent Manager

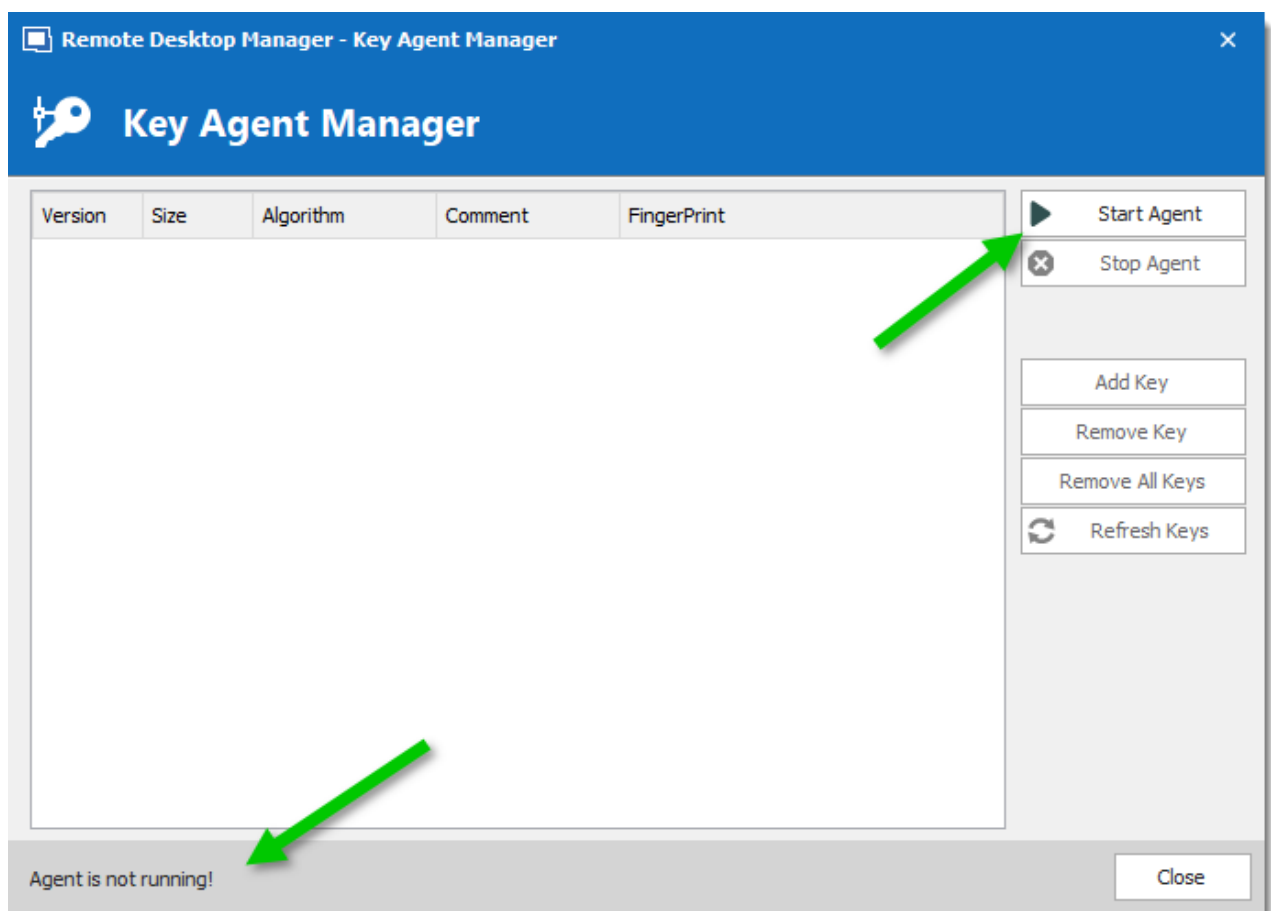
## DESCRIPTION



The **Key Agent Manager** is used to hold all your SSH Keys in memory, already decoded and ready for them to be used. It has the same use as Pageant (SSH Key Manager) has for Putty except that the Key Agent Manager is used with Remote Desktop Manager.

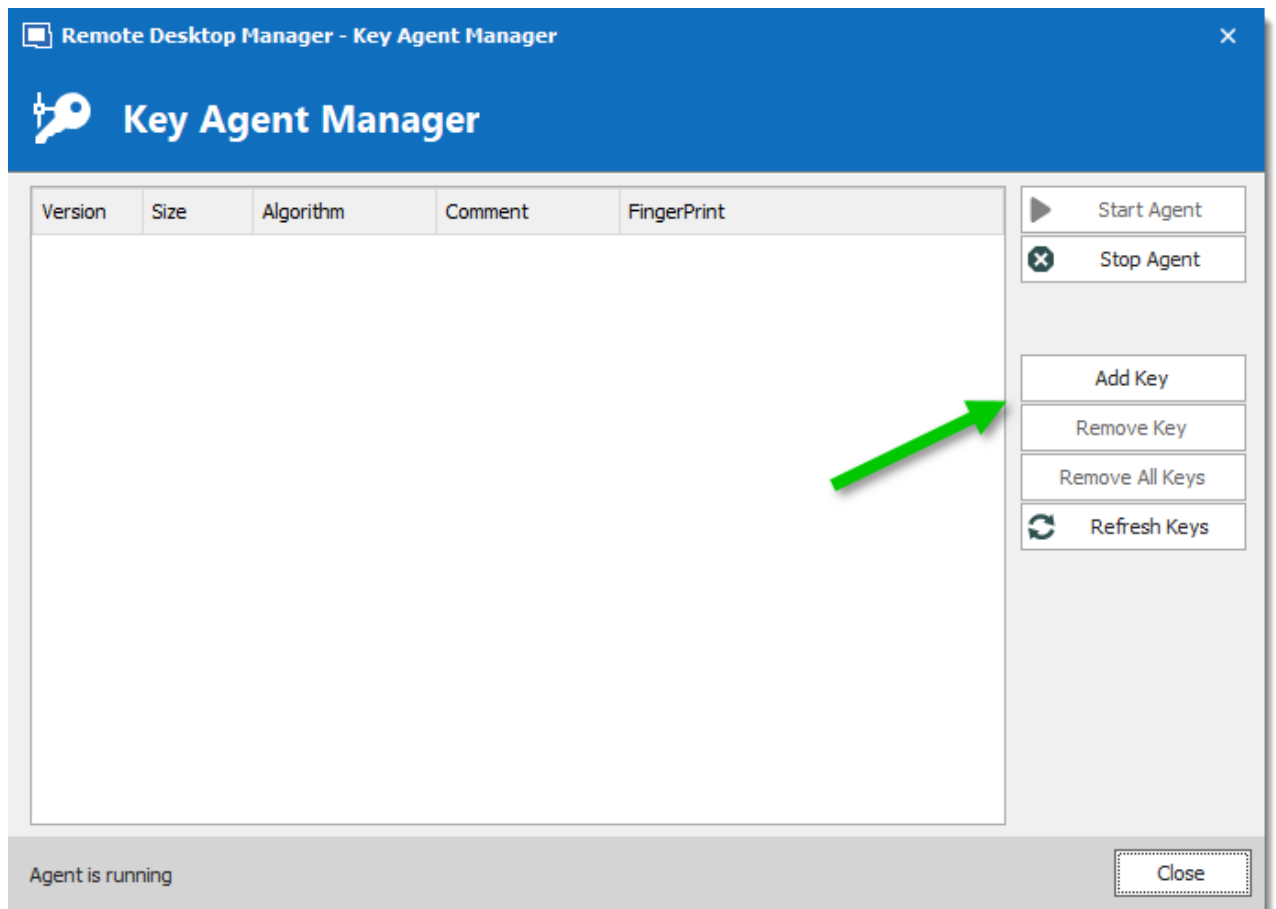
## SETTINGS

1. When opening the Key Agent Manager you will notice at the bottom right that the **agent is not running** you will need to click on **Start Agent**. If you wish to always have your Key Agent running you can activate the option in **File – Option – Key Agent – Start agent on application start**.



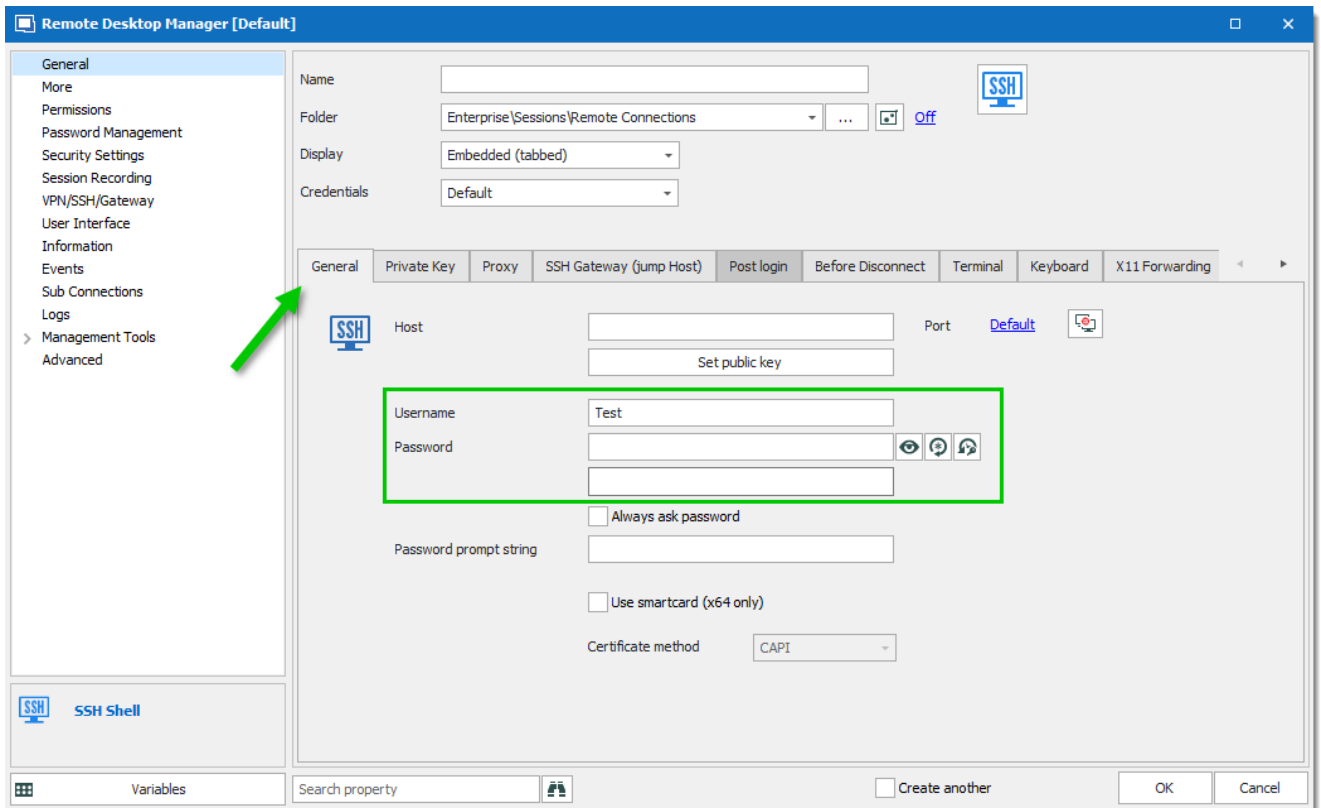
*Key Agent Manager - Start Agent*

2. Click on **Add key** and select the file to open your SSH key.



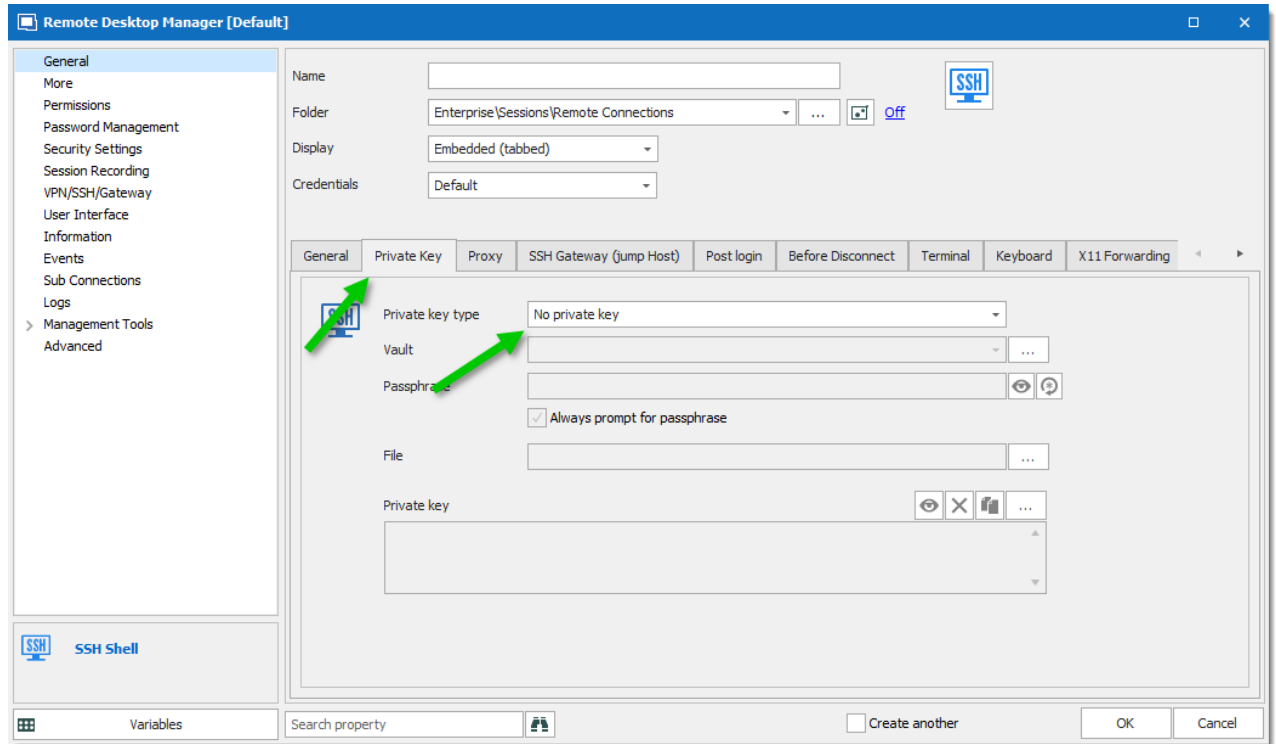
*Key Agent Manager - Add Key*

3. All your added SSH Key will appear in your Key Agent Manager.
4. In your SSH Shell Session in the **General** tab enter a Username and leave the Password field blank.



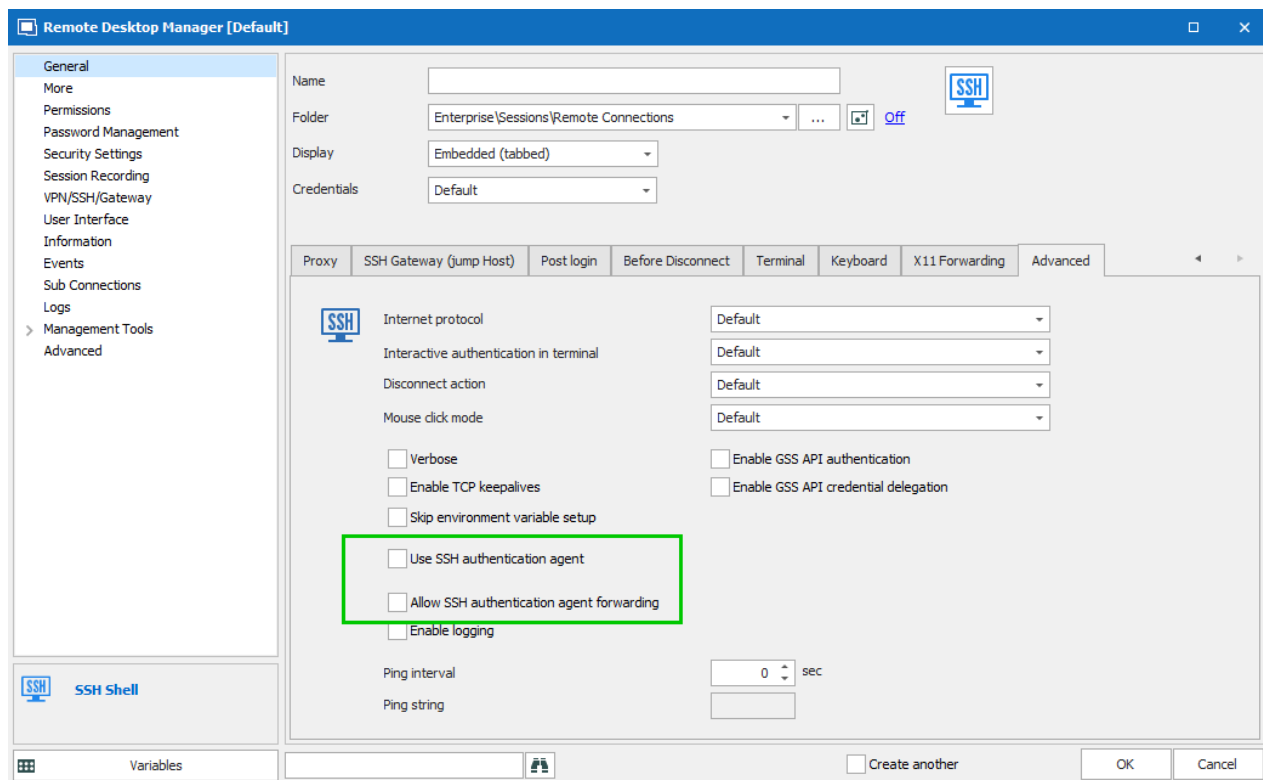
SSH Shell session - General Tab

5. In the **Private Key** tab of your SSH Shell session leave the option for the Private Key to **No Private Key**.



SSH Shell session - Private Key Tab

6. In the **Advanced** tab of your SSH Shell session activate the option **Use Agent**. The Use Agent automatically take the information of the SSH Key kept in your Key Agent Manager.

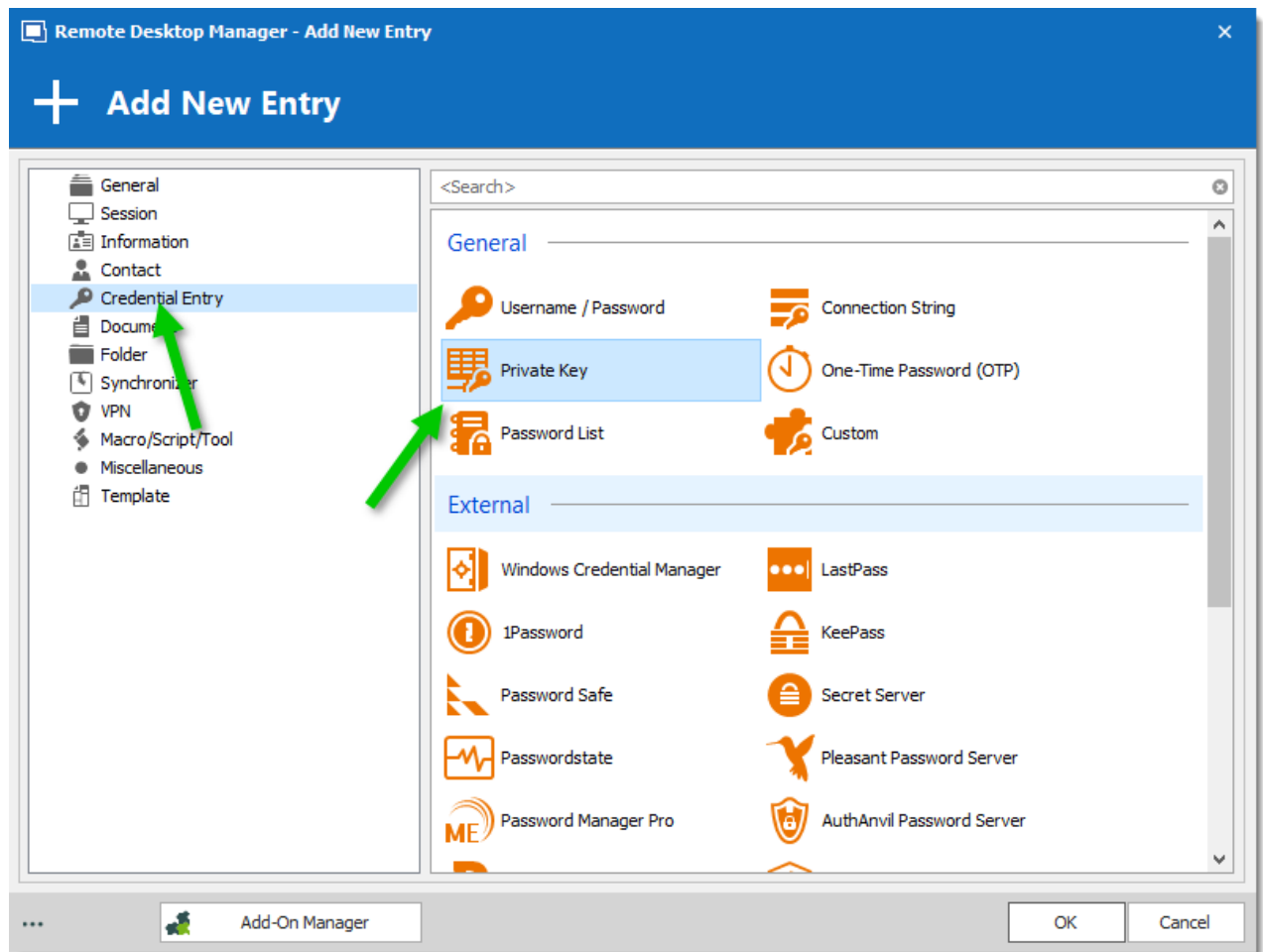


*SSH Shell session - Advanced*

## PRIVATE KEY CREDENTIAL

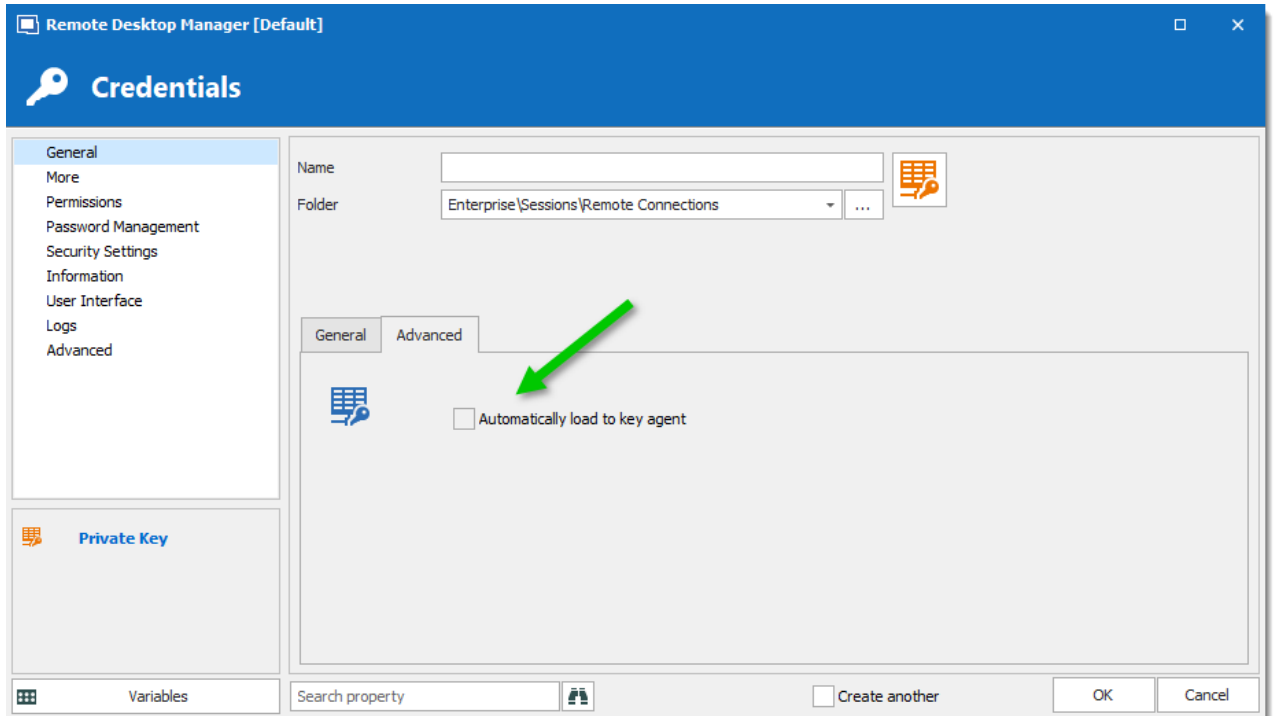
When creating new Private Key credential entry in Remote Desktop Manager you have the option of loading them automatically in your Key Agent Manager.

1. Create your new Private Key credential.



*New Credential Entry - Private Key*

2. In the **Advanced** tab of your Private Key entry activate the option **Automatically load to key agent**.



*Private Key - Advanced Tab*

#### 6.8.2.4 PowerShell (RDM CmdLet)

## DESCRIPTION

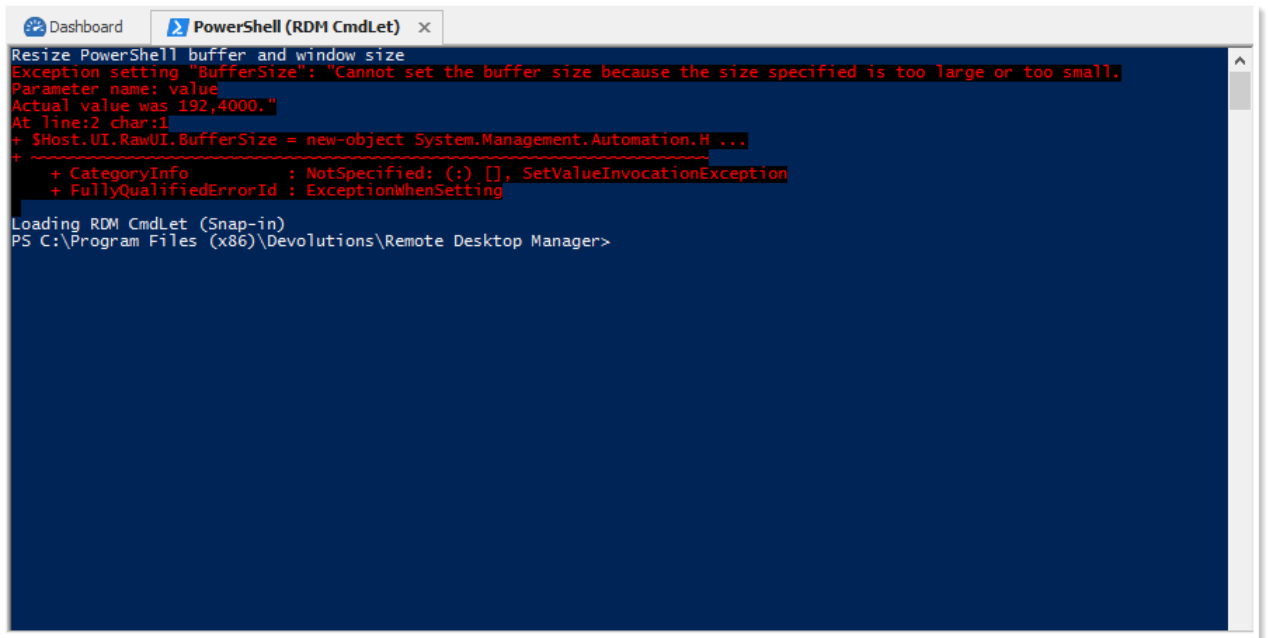
The **PowerShell (RDM CmdLet)** automatically opens an embedded PowerShell window. RDM snap-in allows for quick and robust automation of actions such as add/edit/open of sessions, the possibilities are endless.

Since its release, this highly-requested feature has become very useful in solving user requests. A quick search through our forum reveals many usages of the cmdlets, such as automating the creation of Windows Start Menu shortcuts for every RDM session.

To learn more, you can find full RDM cmdlet documentation available via the [PowerShell Scripting](#) topic or directly in PowerShell using the Get-Help cmdlet.

## SETTINGS

You will find on the [Forum](#) multiple PowerShell script to import edit or interact with the Remote Desktop Manager data.



```
Dashboard PowerShell (RDM CmdLet) x
Resize PowerShell buffer and window size
Exception setting "BufferSize": "Cannot set the buffer size because the size specified is too large or too small."
Parameter name: value
Actual value was 192,4000."
At line:2 char:1
+ $Host.UI.RawUI.BufferSize = new-object System.Management.Automation.H ...
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:) [], SetValueInvocationException
+ FullyQualifiedErrorId : ExceptionWhenSetting

Loading RDM CmdLet (Snap-in)
PS C:\Program Files (x86)\Devolutions\Remote Desktop Manager>
```

*PowerShell*

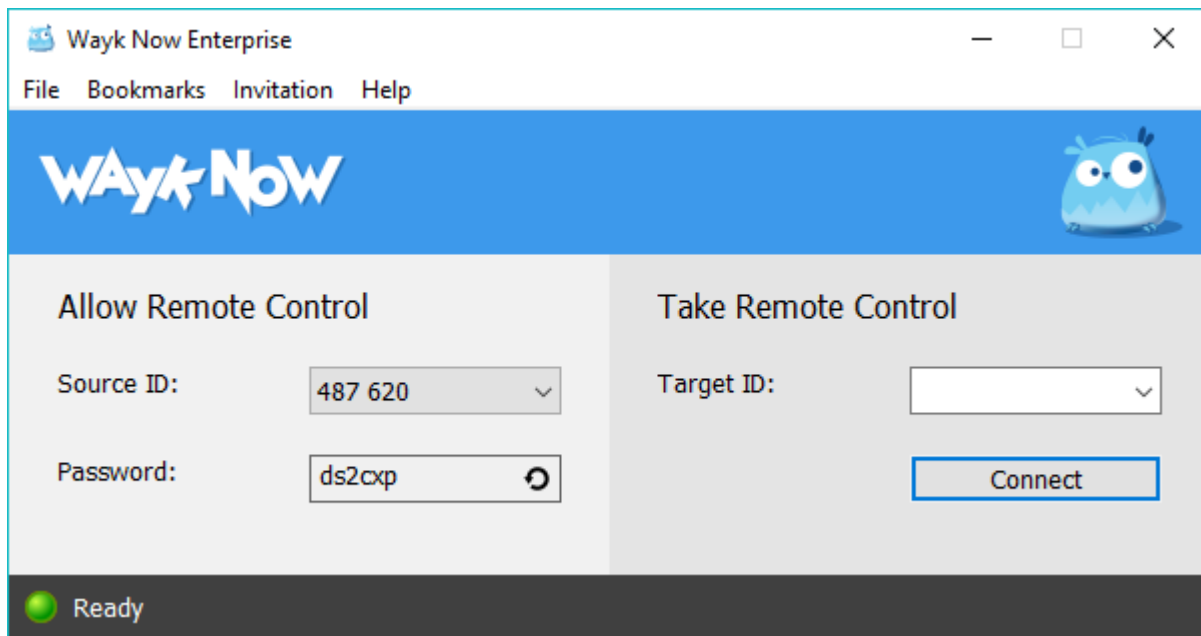
#### 6.8.2.5 Wayk Now

## DESCRIPTION

**Wayk Now** helps you provide remote assistance to others by allowing one user to connect to another person's computer. It is a **Devolutions** product that is integrated with Remote Desktop Manager.

Clicking on this tool opens Wayk Now application externally.





Wayk Now

For more information about using Wayk Now consult the Wayk Now [Online Help](#).

#### 6.8.2.6 More Tools

##### 6.8.2.6.1 Chocolatey Console

## DESCRIPTION




[Chocolatey](#) need to be installed on your computer to use the Chocolatey Console.

The Chocolatey Console is available in the **Tools – More Tools - Chocolatey Console** menu. It allows you to install all the supported applications from Chocolatey directly from Remote Desktop Manager.

## SETTINGS

Dashboard
Chocolatey Console



## AutoHotkey 1.1.23.01

[Open in gallery](#)

**25,517**  
Downloads

**1,161**  
Downloads of v1.1.23.01

**1/24/2016**  
Last update

[Project Site](#)  
[License](#)  
[Report Abuse](#)  
[Contact Maintainers](#)  
[Download](#)





AutoHotkey is a free, open source macro-creation and automation software utility that allows users to automate repetitive tasks. It is driven by a custom scripting language that is aimed specifically at providing keyboard shortcuts, otherwise known as hotkeys.

AutoHotkey\\_L is a fork of AutoHotkey which adds a long list of new features and fixes some bugs. Anything that can be done with AutoHotkey can also be done with AutoHotkey\\_L. Scripts written for AutoHotkey will also run on AutoHotkey\\_L, with some exceptions.

```
C:\> choco install autohotkey
```

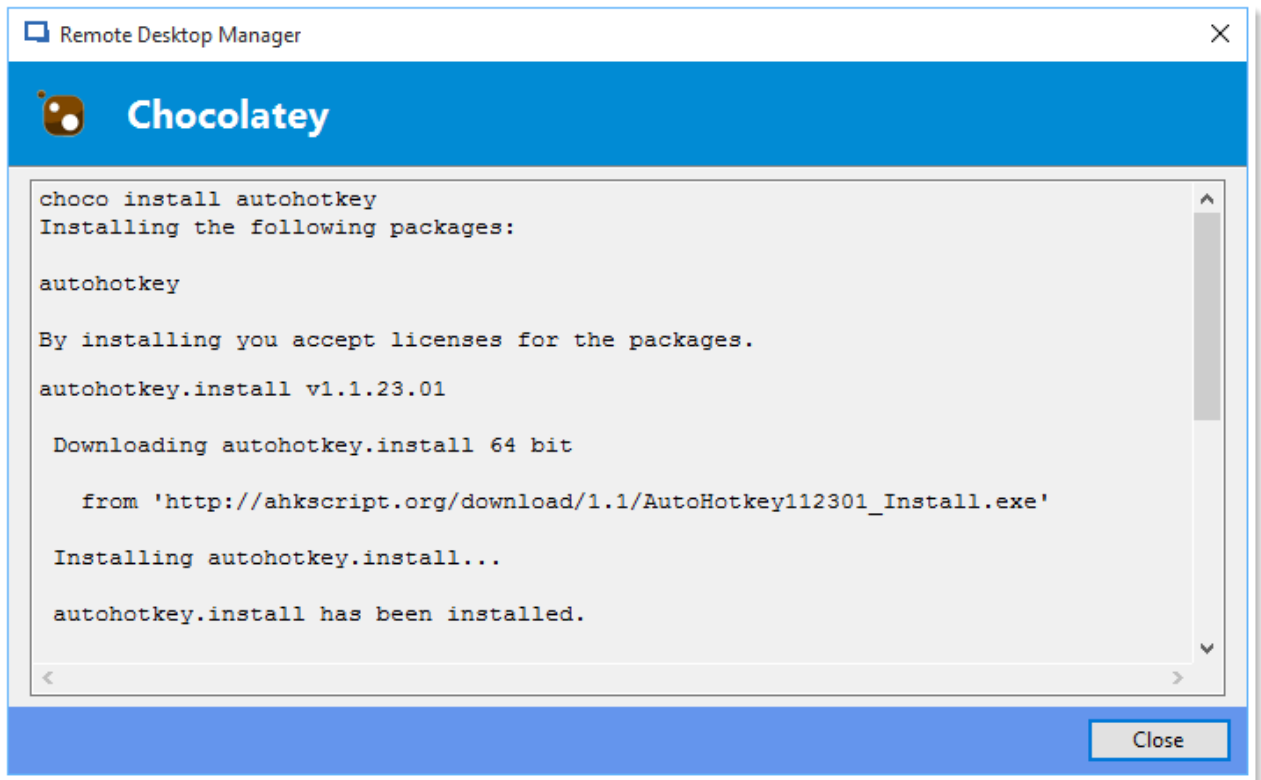
Name	Installed Version	Latest Version	Installed
autohotkey		1.1.23.01	<input type="checkbox"/>
autoit		3.3.14.2	<input type="checkbox"/>
filezilla		3.15.0.2	<input type="checkbox"/>
Firefox		44.0.2	<input type="checkbox"/>
GoogleChrome		48.0.2564.109	<input type="checkbox"/>
HeidiSQL		8.3.0.4694	<input type="checkbox"/>
javaruntime		8.0.66	<input type="checkbox"/>
keepass		2.31	<input type="checkbox"/>
mysql.workbench		6.3.6	<input type="checkbox"/>
powershell		4.0.20141001	<input type="checkbox"/>
putty.install	0.66	0.66	<input type="checkbox"/>
pvm		7.1.0.0	<input type="checkbox"/>
Radmin.Viewer		3.4.0.20120928	<input type="checkbox"/>
safari			<input type="checkbox"/>
skype		7.18.0.112	<input type="checkbox"/>
sysinternals		2016.02.02	<input type="checkbox"/>
teamviewer		11.0.53254	<input type="checkbox"/>
tightvnc		2.7.10.20140503	<input type="checkbox"/>

Chocolatey Console

OPTION	DESCRIPTION
	Install the selected application.
	Update the selected application.
	Uninstall the selected application.
	Refresh the Chocolatey details list.

## USAGE

During the installation, you will see the following window.



*Installation window*

When the installation is completed you will see a check mark in the **Installed** column.

Name	Installed Version	Latest Version	Installed
autohotkey	1.1.23.01	1.1.23.01	<input checked="" type="checkbox"/>
autoit	3.3.14.2	3.3.14.2	<input type="checkbox"/>
filezilla		3.15.0.2	<input type="checkbox"/>
Firefox		44.0.2	<input type="checkbox"/>
GoogleChrome		48.0.2564.109	<input checked="" type="checkbox"/>
HeidiSQL		8.3.0.4694	<input type="checkbox"/>
javaruntime		8.0.66	<input type="checkbox"/>
keepass	2.31	2.31	<input type="checkbox"/>
mysql.workbench		6.3.6	<input type="checkbox"/>

*Installation Complete*

## 6.8.2.6.2 Local RDP/RemoteApp Manager

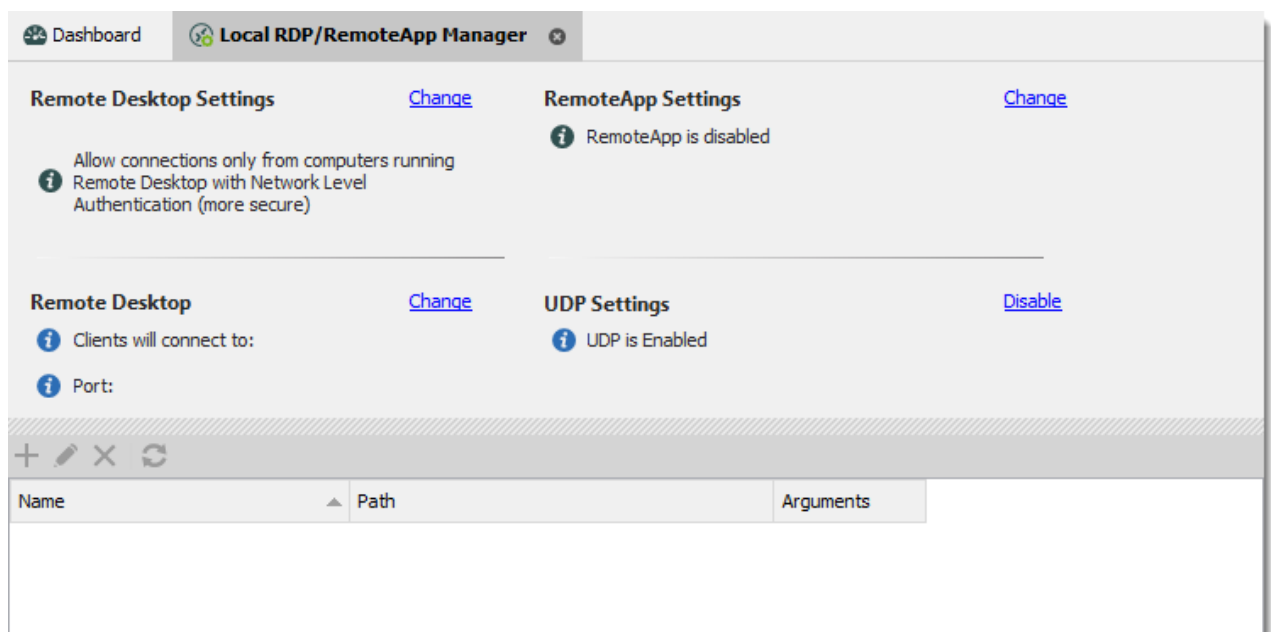
## DESCRIPTION

The local RDP settings and the RemoteApp settings are available from **Tools – More Tools - Local RDP/RemoteApp Manager**.

If you run Remote Desktop Manager on a Windows Server 2008 machine the TS RemoteApp MMC console will be launched.

If you are running on Windows Vista, the RemoteApp console built into Remote Desktop Manager will be launched because RemoteApp functionality is available in Windows 7 but not the MMC console. Therefore instead of having to modify the required registry entries you can use the Remote Desktop Manager RemoteApp Manager.

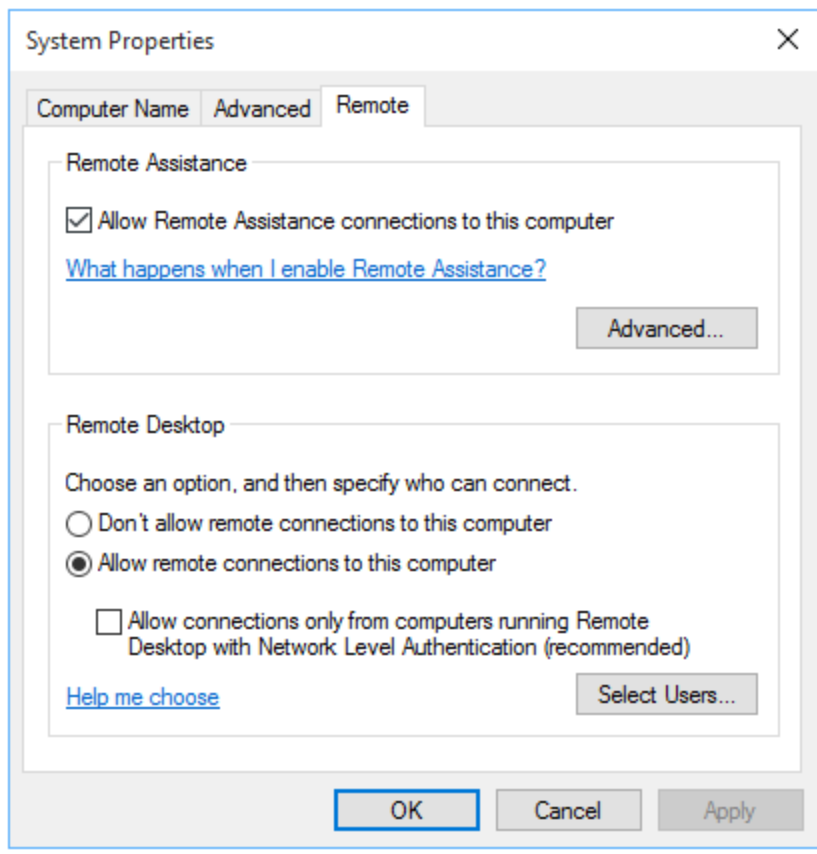
## SETTINGS



*More Tools - Local RDP/RemoteApp Manager*

## REMOTE DESKTOP SETTINGS

Allow or disallow the remote connections to your computer.



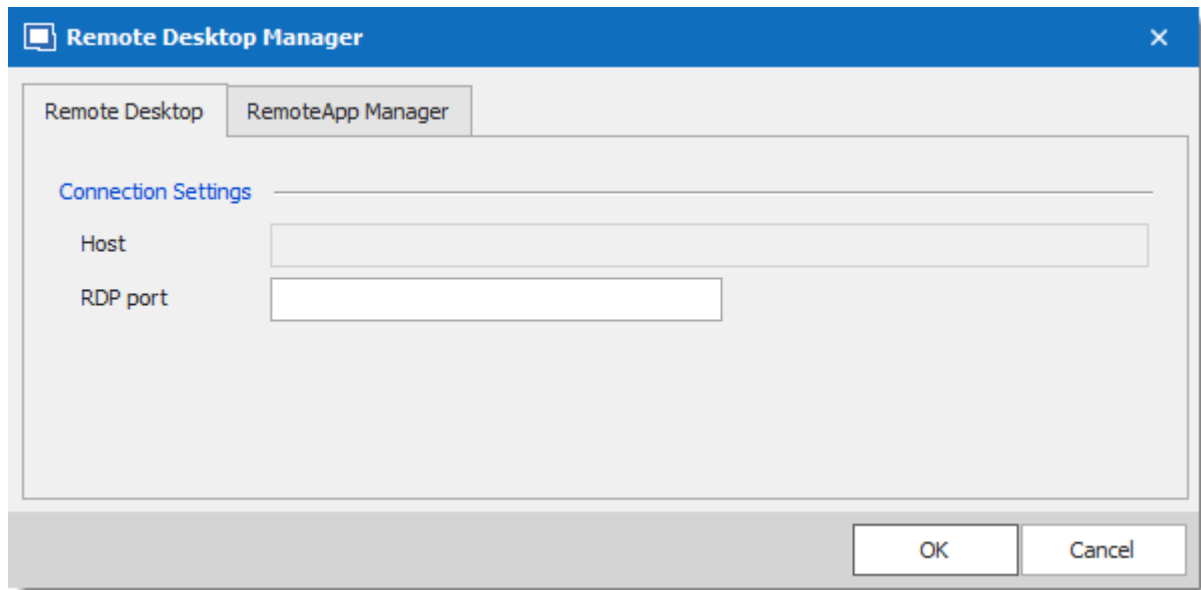
*Remote Desktop Settings*

## REMOTE DESKTOP

Allows you to modify the local RDP port.



Remote Desktop Manager must be run as an administrator to modify the Remote Desktop settings.



The screenshot shows a window titled "Remote Desktop Manager" with a close button (X) in the top right corner. Inside the window, there are two tabs: "Remote Desktop" and "RemoteApp Manager". The "RemoteApp Manager" tab is selected. Below the tabs, there is a section titled "Connection Settings" with a horizontal line underneath. Under this section, there are two labels: "Host" and "RDP port". To the right of "Host" is a text input field. To the right of "RDP port" is a text input field. At the bottom right of the window, there are two buttons: "OK" and "Cancel".

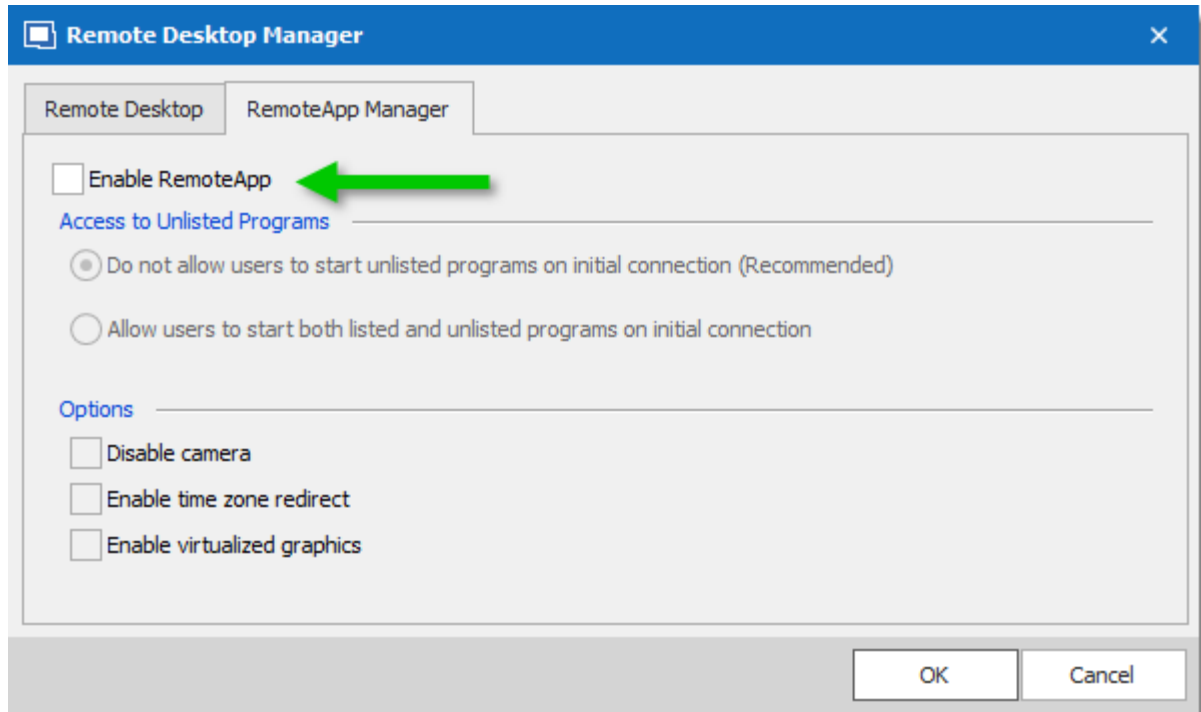
*Remote Desktop Connection Settings*

## REMOTEAPP SETTINGS

You must Enable RemoteApp to be able to create a New RemoteApp Setting.



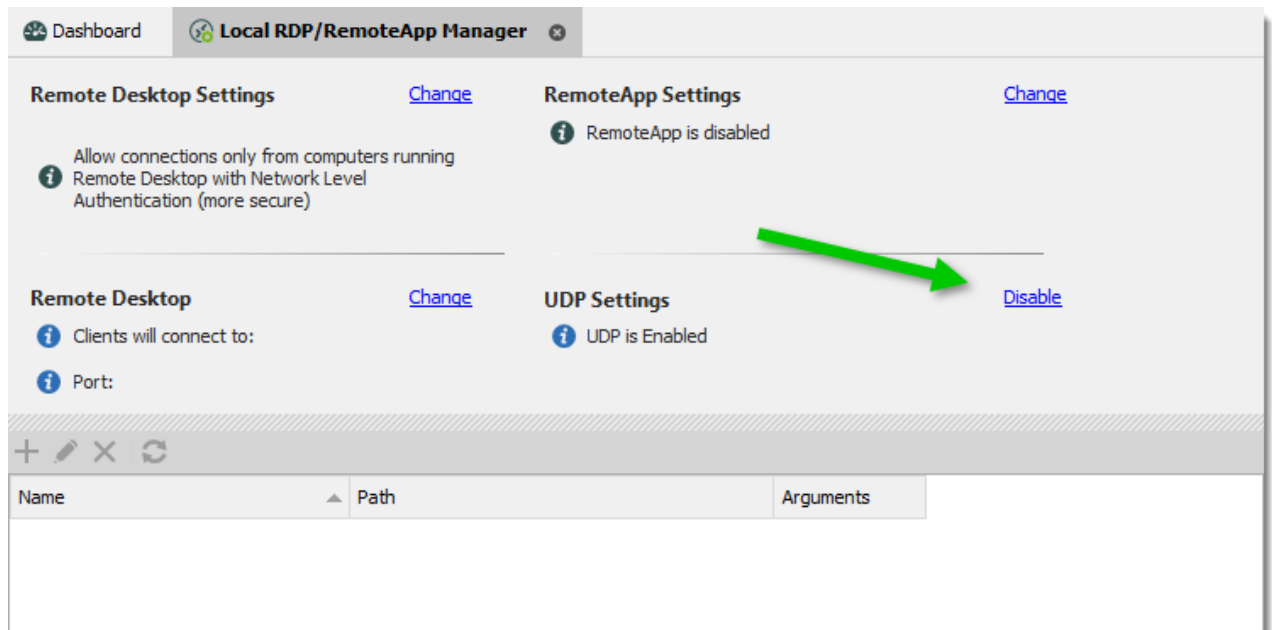
Remote Desktop Manager must be run as an administrator to modify the RemoteApp settings.



*RemoteApp Settings*

## UDP SETTINGS

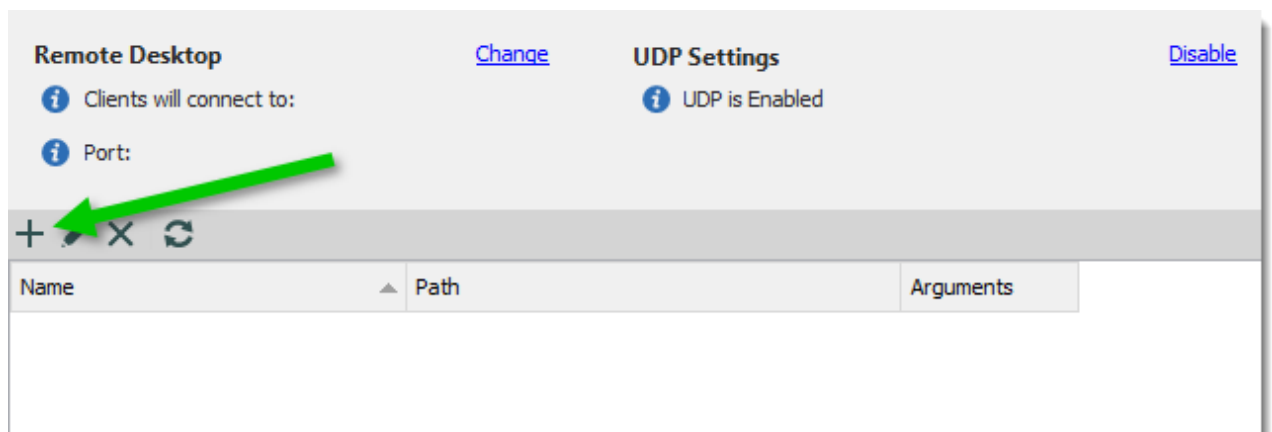
Enable or disable UDP (User Datagram Protocol) locally on your computer. UDP is a communication protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP).



*Local RDP/RemoteApp Manager - UDP is Enabled*

## USAGE

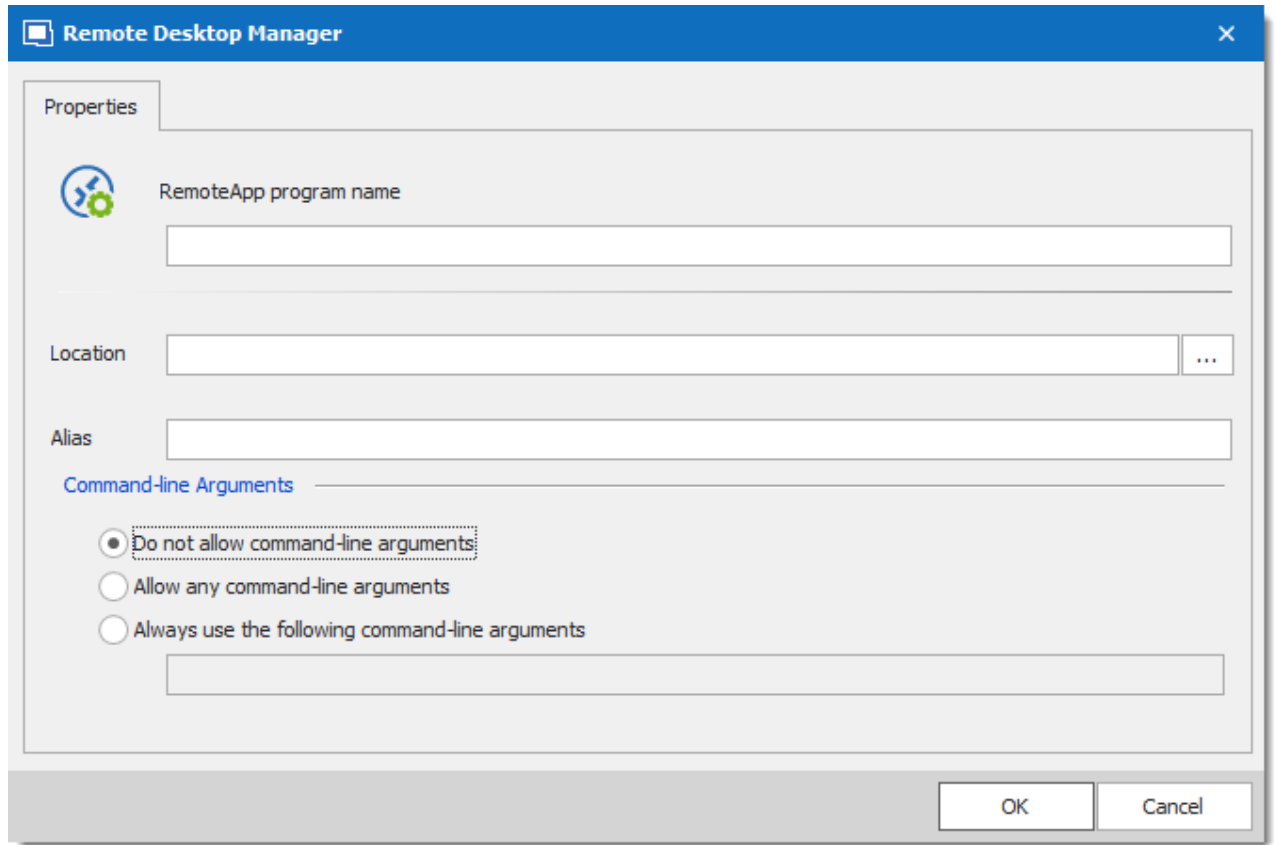
1. Click on **New RemoteApp Settings**.



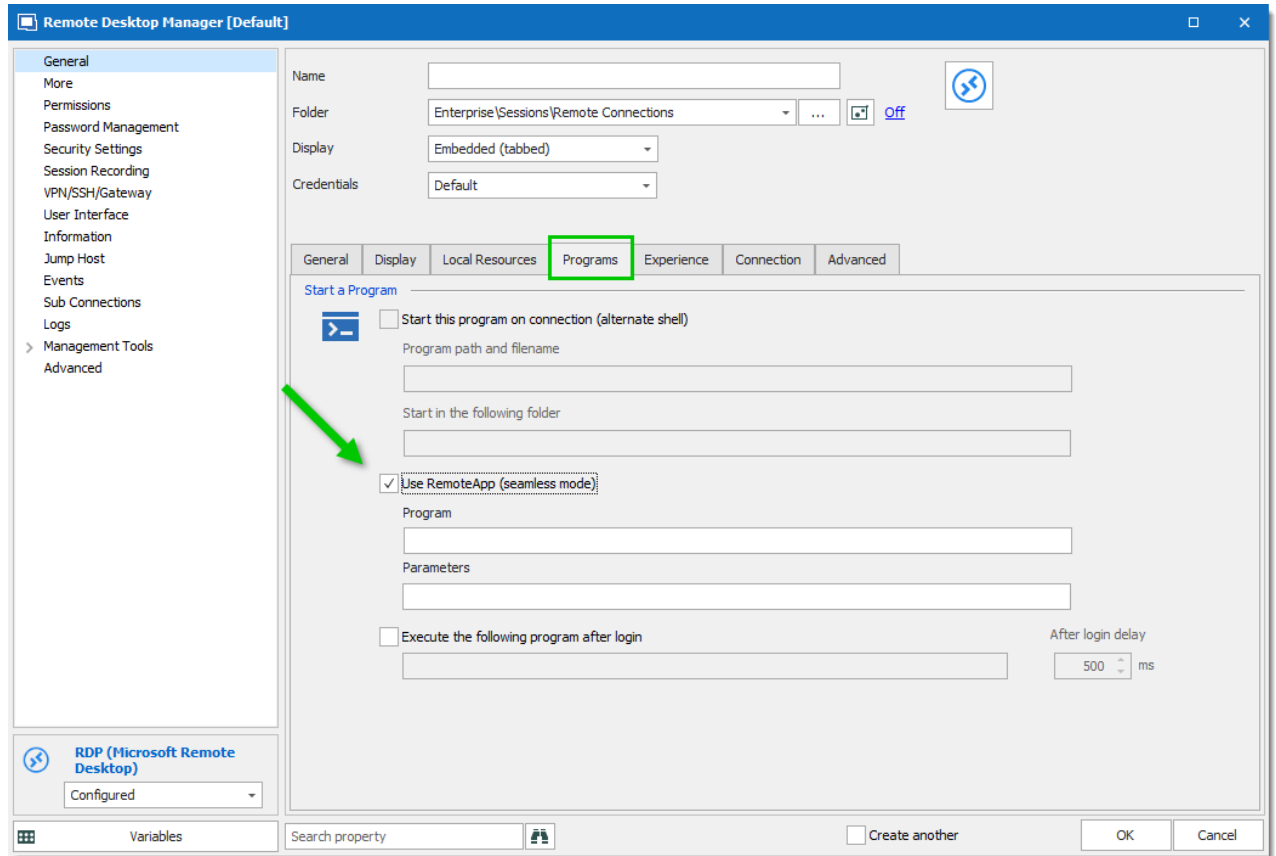
*New RemoteApp Settings*

2. Configure the RemoteApp





3. Create a new RDP session and select the **Programs** tab. Enable the **Use RemoteApp** option and then enter the name of the RemoteApp program and save the session. When the session is launched you will have the RemoteApp running locally.



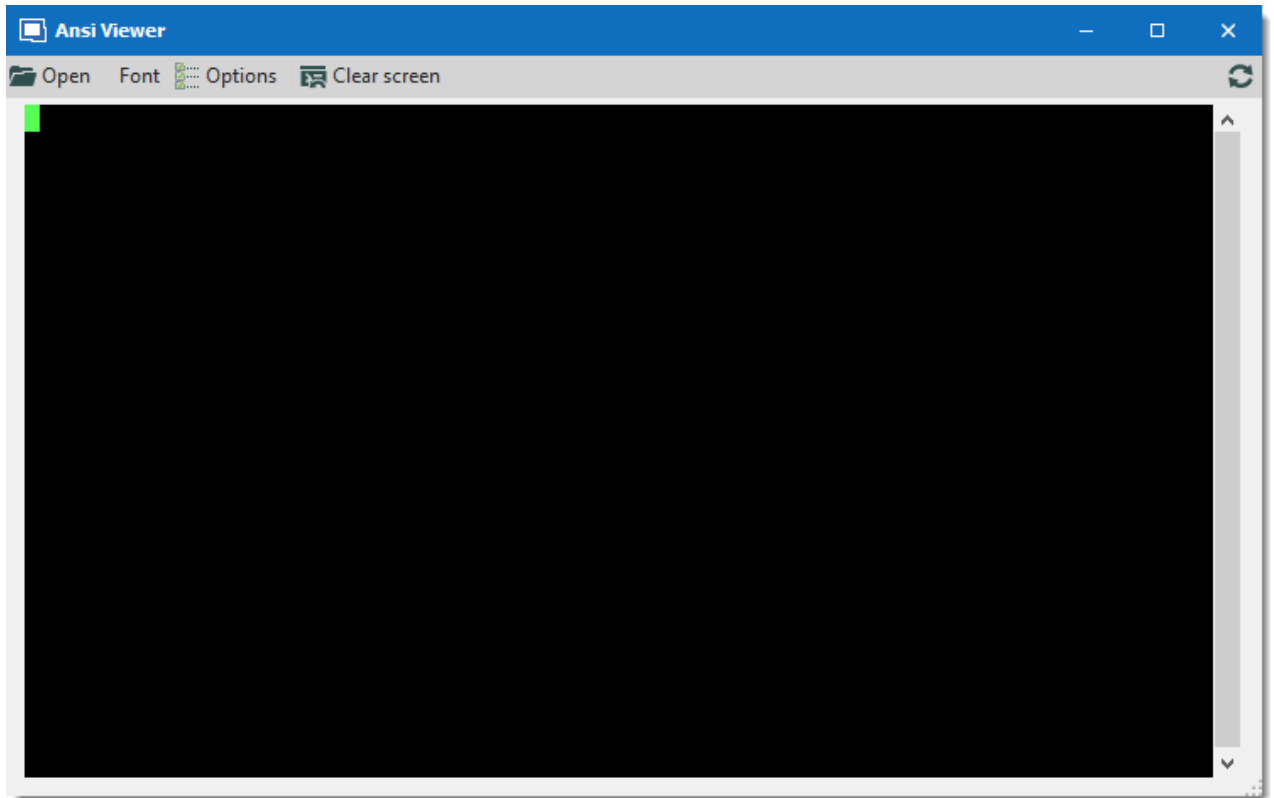
RDP session - Programs Tab

## 6.8.2.6.3 Playback (Ansi)




## DESCRIPTION

The **Playback (Ansi)** is available in **Tools – More Tools – Playback (Ansi)**.

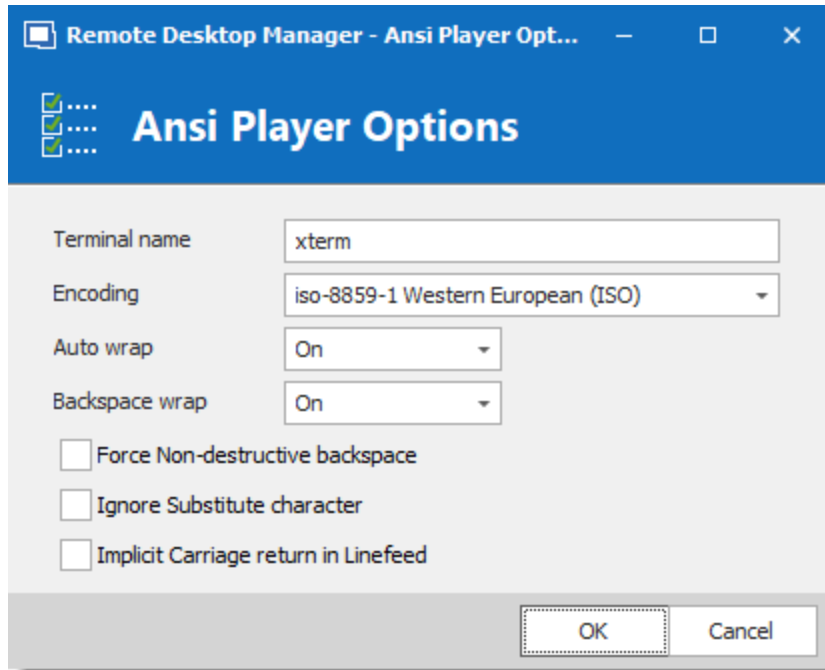
## SETTINGS



*More Tools - Playback (Ansi)*

OPTION	DESCRIPTION
 <b>Open</b>	Select the ansi file you wish to open in the Terminal Playback.
<b>Font</b>	Select the font for the Terminal Playback.
 <b>Options</b>	See <b>Options</b> section.
 <b>Clear screen</b>	Clear the screen to play another ansi file.

## OPTIONS



*Playback (Ansi) - Ansi Player Options*

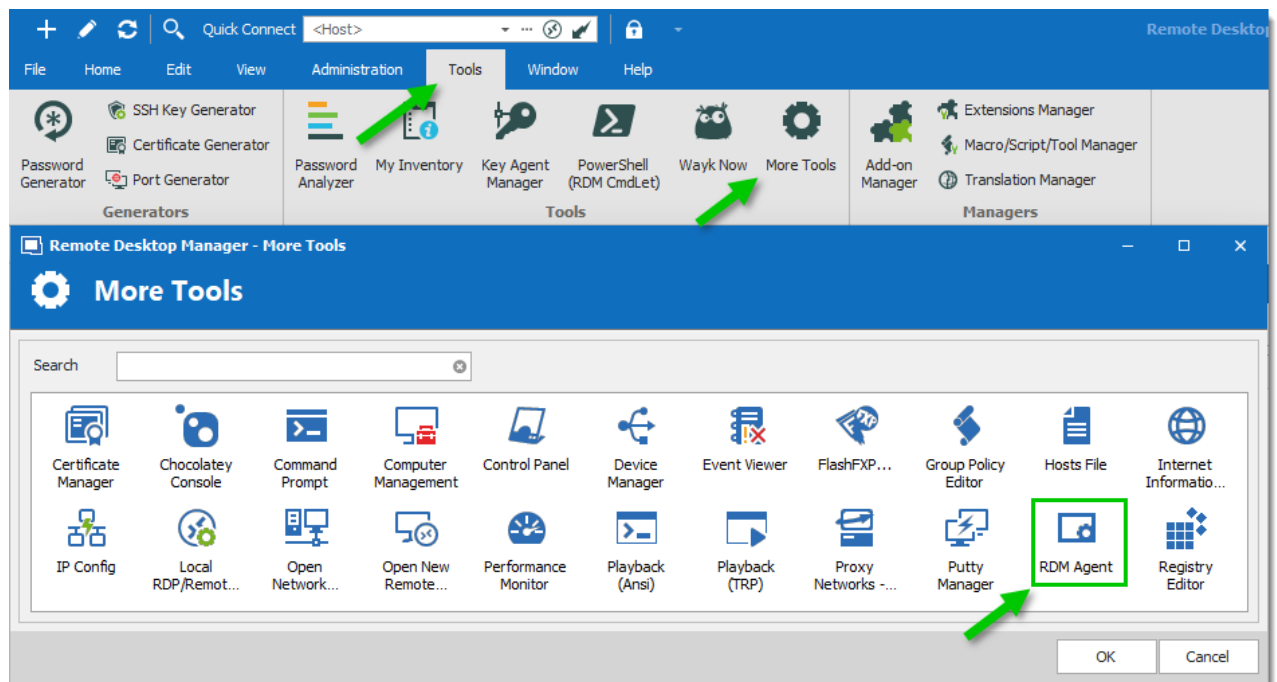
OPTION	DESCRIPTION
<b>Terminal name</b>	Indicate the terminal name.
<b>Encoding</b>	Indicate the encoding you wish to use.
<b>Auto wrap</b>	<p>Indicate what happen when text reaches the right-hand edge of the window. Select between:</p> <ul style="list-style-type: none"> <li>• <b>On</b></li> <li>• <b>Off</b></li> <li>• <b>Dos</b></li> </ul>
<b>Backspace wrap</b>	<p>This option allows you to choose what you want to do when you press backspace. Some terminals believe that the backspace key should send the same thing to the server as Control-H (ASCII code 8). Other terminals believe that the backspace key should send ASCII code 127 (usually known as Control-?) so that it can be distinguished from Control-H. Select between:</p>

OPTION	DESCRIPTION
	<ul style="list-style-type: none"><li>• On</li><li>• Off</li><li>• Dos</li></ul>
<b>Force Non-destructive backspace</b>	Allow to perform a normal backspace without deleting a character.
<b>Ignore Substitute character</b>	Ignore the substitute character that can be use in Putty.
<b>Implicit Carriage return in Linefeed</b>	<p>Most servers send two control characters, CR and LF, to start a new line on the screen. The CR character makes the cursor return to the left-hand side of the screen. The LF character makes the cursor move one line down (and might make the screen scroll).</p> <p>Some servers only send LF, and expect the terminal to move the cursor over to the left automatically. If you come across a server that does this, you will see a stepped effect on the screen. If this happens to you, try enabling the option and things might go back to normal.</p>

## 6.8.2.6.4 RDM Agent

## DESCRIPTION

The **Remote Desktop Manager Agent** is a very powerful tool that allows commands to be run on multiple machines.



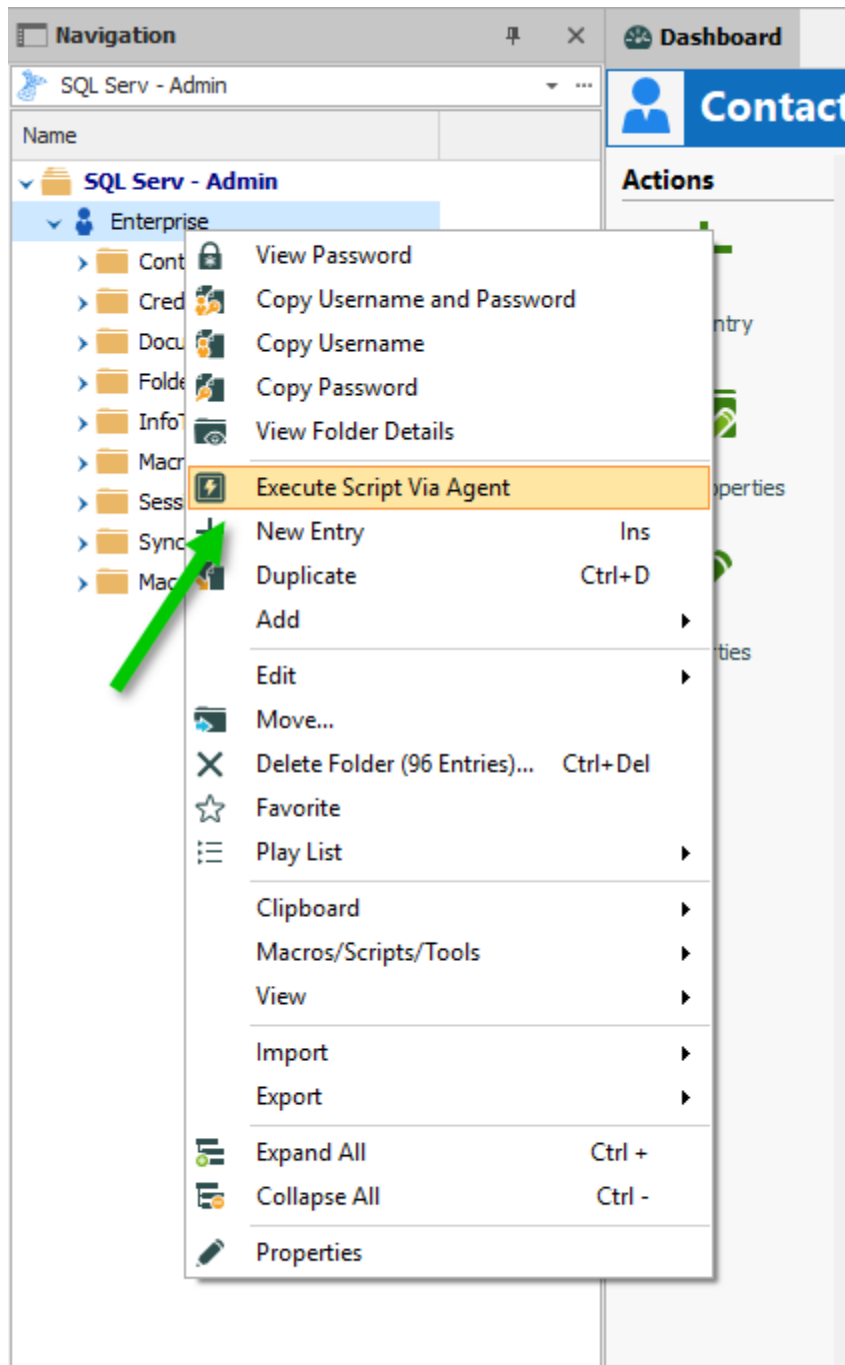
*More Tools - RDM Agent*

## SETTINGS

To launch a script through the **RDM Agent**, you first need to open an RDP connection to all the machines you wish to execute the script on. Once opened, select all the opened sessions in the [Navigation Pane](#), right-click them and select **Execute Script via Agent**.

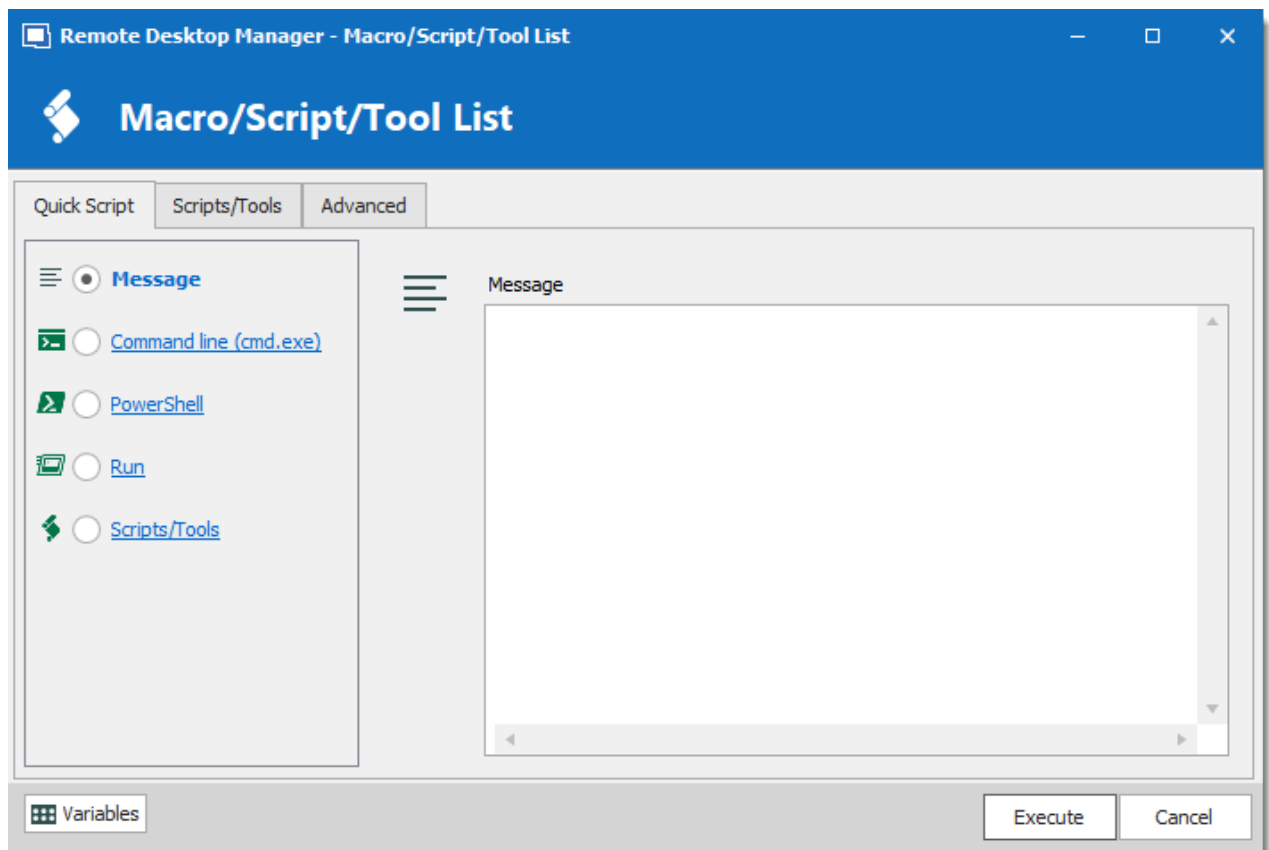


Execute script via Agent only needs the RDM Agent when the script is executed from the Quick Script tab. RDM needs to be fully installed on the remote computer when the script is executed from the Scripts/Tools tab.



*Execute Script Via Agent*

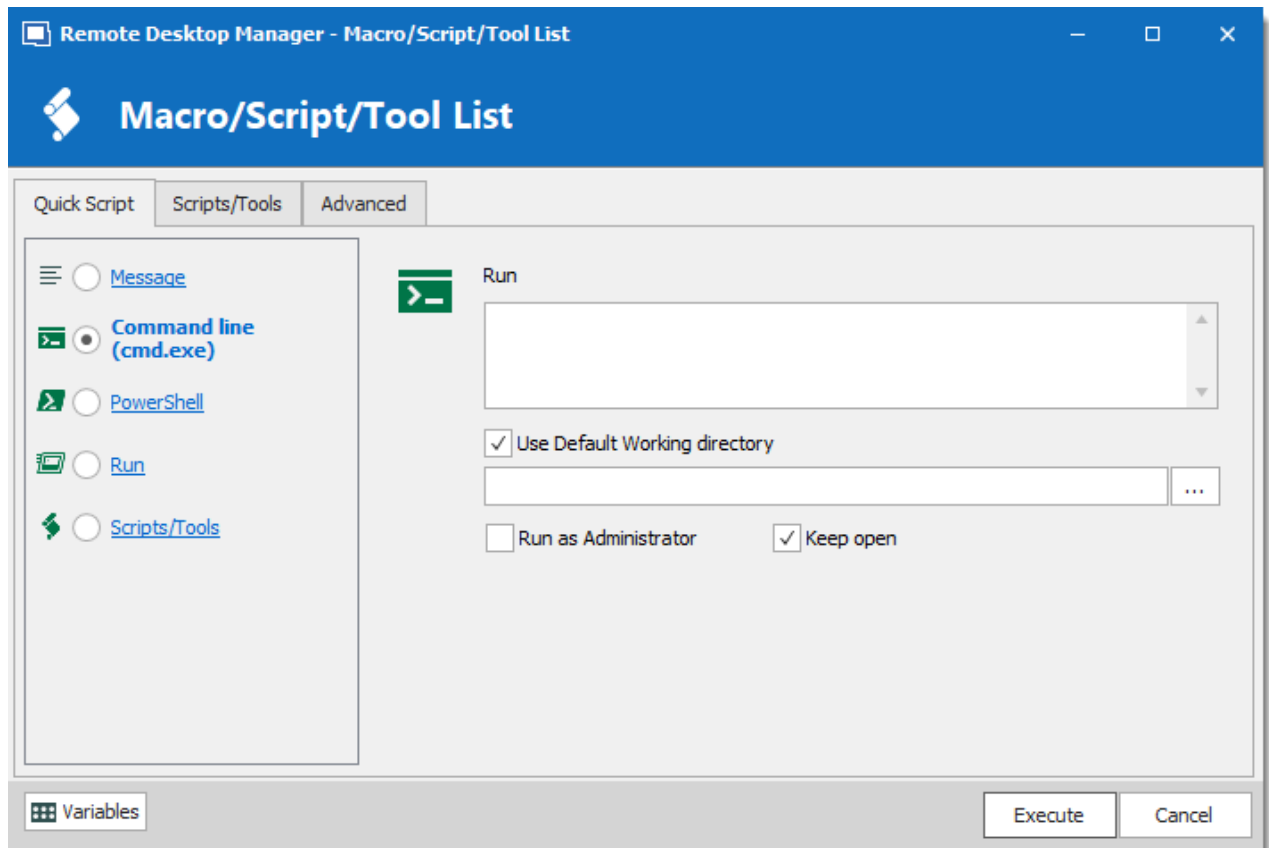
## QUICK SCRIPT - MESSAGE

*Quick Script - Message*

OPTION	DESCRIPTION
<b>Message</b>	Send a message to all targets.

## QUICK SCRIPT - COMMAND LINE (CMD.EXE)

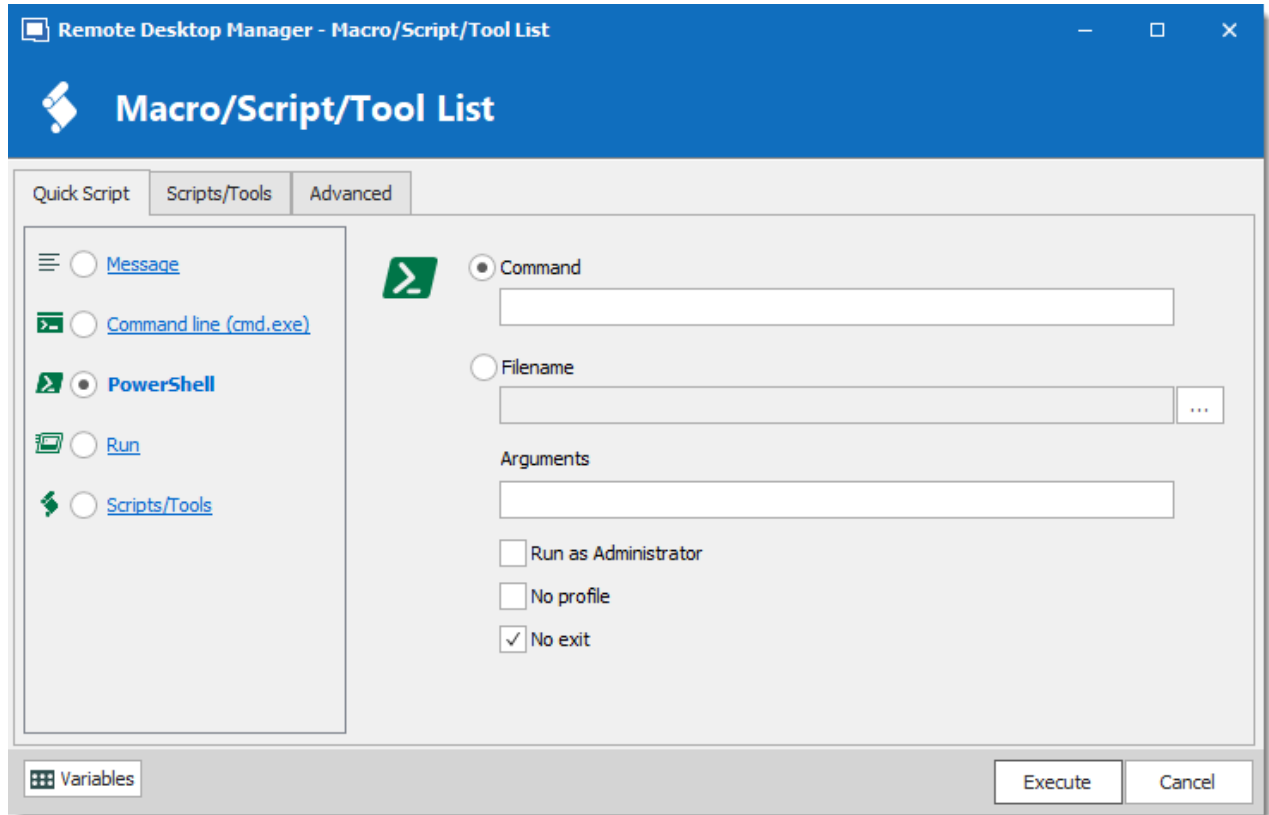




Quick Script - Command Line

OPTION	DESCRIPTION
<b>Run</b>	Indicate the command line that you want to execute.
<b>Use Default Working directory</b>	Use the default working directory when connect to the session.
<b>Run as Administrator</b>	Elevates the process to run as an administrator.
<b>Keep open</b>	Keep the window open after the execution of the command line.

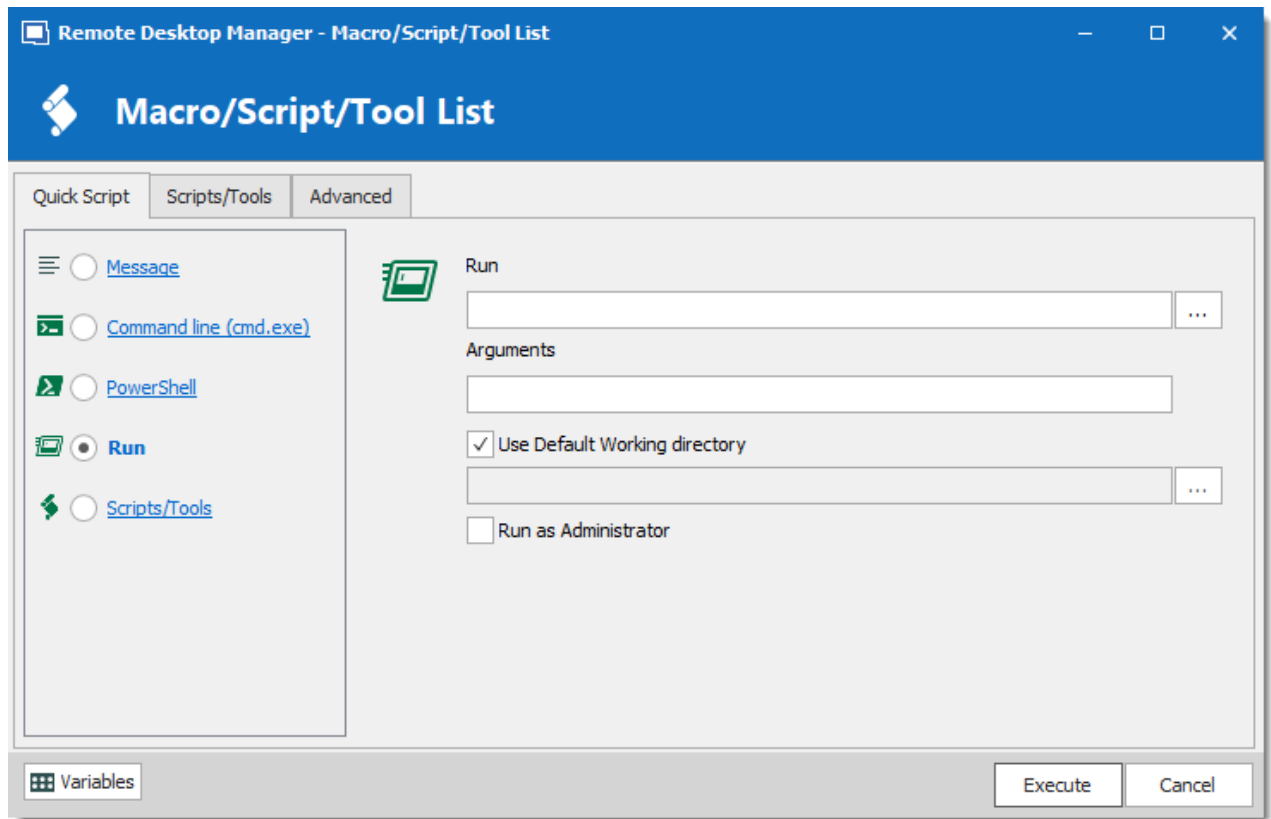
## QUICK SCRIPT - POWERSHELL



Quick Script - PowerShell

OPTION	DESCRIPTION
<b>Command</b>	Indicate the PowerShell command that you want to execute.
<b>Filename</b>	Select a PowerShell file on the network or on the computer.
<b>Arguments</b>	Arguments that are appended to the Command.
<b>Run as Administrator</b>	Elevates the process to run as an administrator.
<b>No Profile</b>	Does not load the Windows PowerShell profile.
<b>No exit</b>	Does not exit after running startup commands.

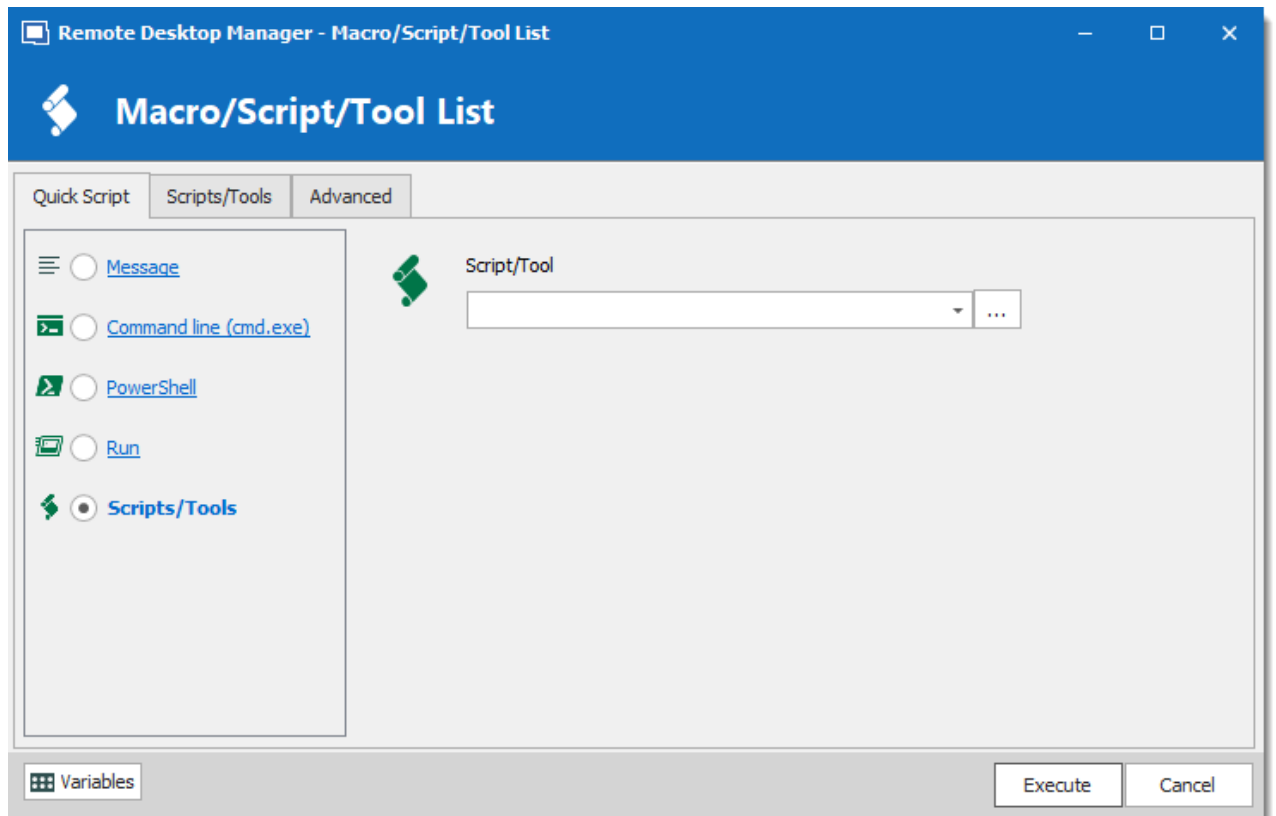
## QUICK SCRIPT - RUN



Quick Script - Run

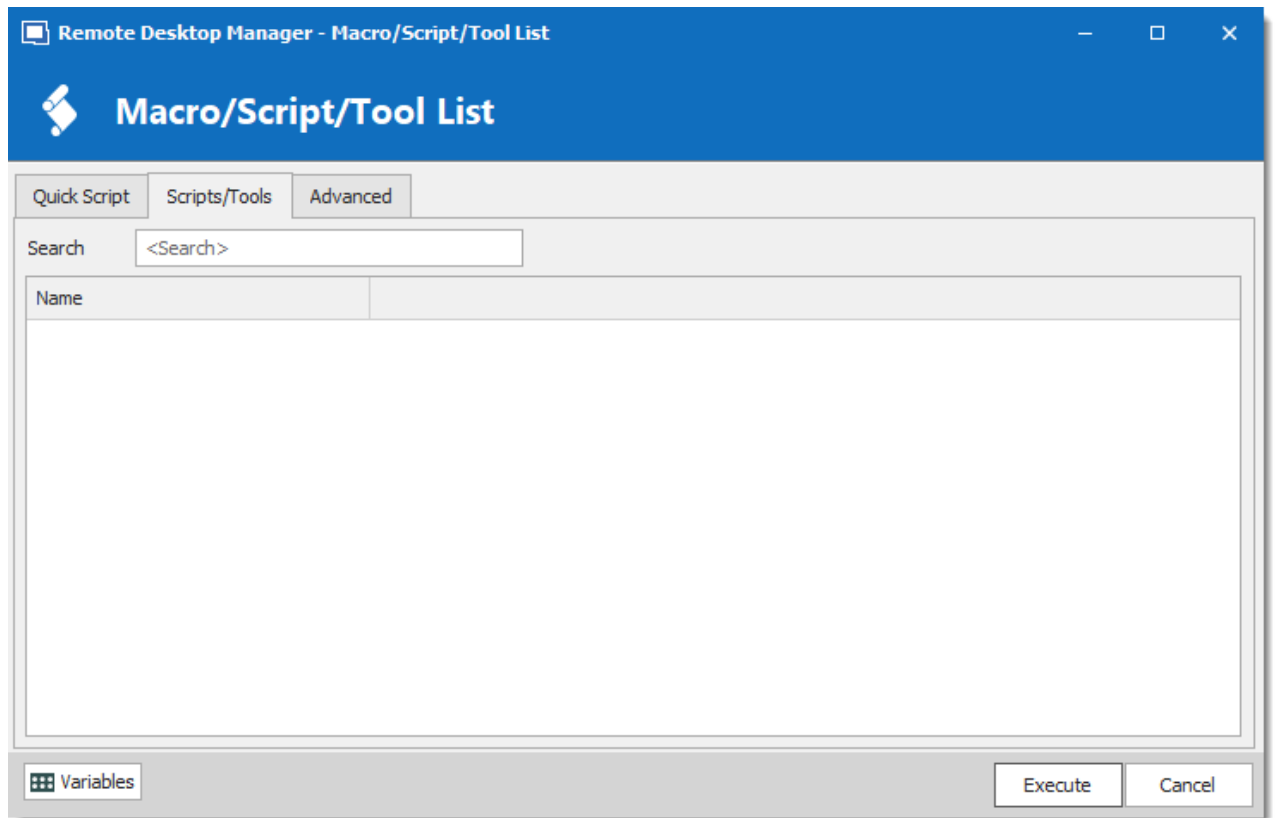
OPTION	DESCRIPTION
<b>Run</b>	Select the program or file that you want to execute.
<b>Arguments</b>	Arguments that are appended to the Command.
<b>Use Default Working directory</b>	Use the default working directory when connect to the session.
<b>Run as Administrator</b>	Elevates the process to run as an administrator.

## QUICK SCRIPT - SCRIPTS/TOOLS

*Quick Script - Scripts/Tools*

OPTION	DESCRIPTION
<b>Scripts/Tools</b>	Select a script or a tool session that you have already created in Remote Desktop Manager.

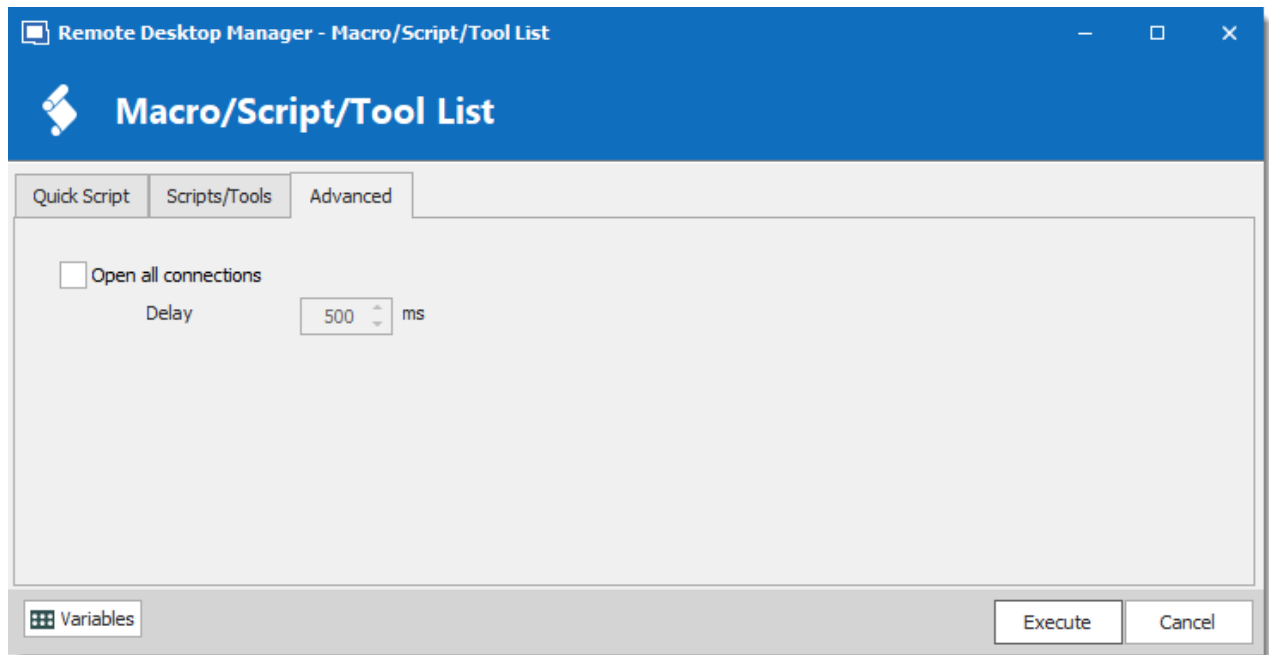
## SCRIPT/TOOLS



*Scripts/Tools*

Search for a script or a tool you wish to execute through the RDM Agent.

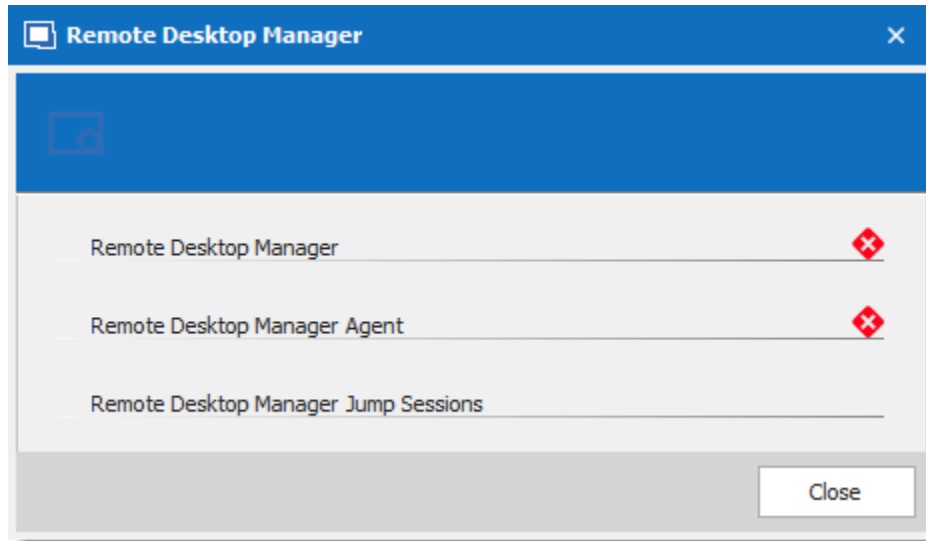
## SETTINGS

*Advanced*

OPTION	DESCRIPTION
<b>Open all connections</b>	When multiple sessions are selected to <b>Execute Script Via Agent</b> , it will open all the selected connections.
<b>Delay</b>	Enter the time delay between opening each selected session.

## AGENT STATUS

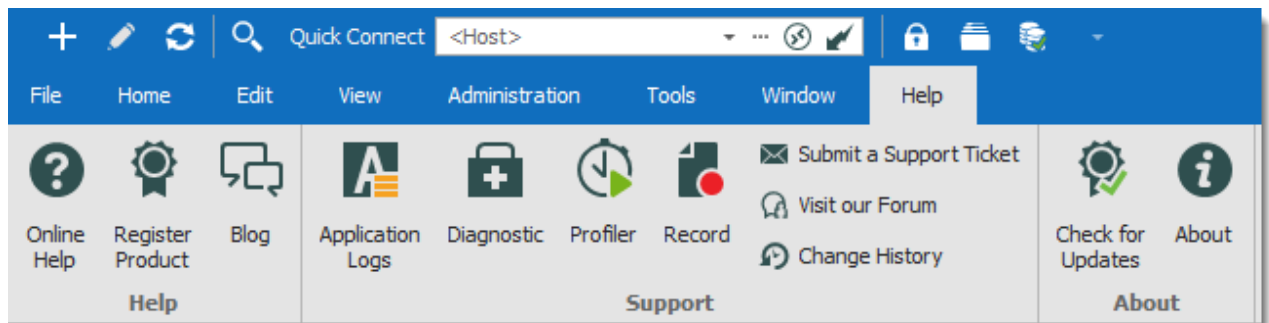
Open a RDP session, right-click on this single session and select Agent Status. The Agent Status will show you that Remote Desktop Manager is installed on the remote computer or not, that the Remote Desktop Manager Agent is active or not and how many Remote Desktop Manager Jump sessions are opened.

*Agent Status*

## 6.9 Help

### DESCRIPTION

The **Help** tab contain links to the Devolutions forum and Online Help, and many support related features, such as the **Application Logs**, the **Profiler**, and the **Recorder**.

*Ribbon - Help*

### HELP

OPTION	DESCRIPTION
<b>Online Help</b>	Launches the Online Help you are currently browsing!

OPTION	DESCRIPTION
<b>Register Product</b>	Register the Remote Desktop Manager with a Trial or Enterprise license serial. For more information, please consult the <a href="#">Register Enterprise Edition</a> topic.
<b>Blog</b>	Visit our <a href="#">Blog</a> . Learn about the Devolutions Team, as well as our Goals, Products and more.

## SUPPORT

OPTION	DESCRIPTION
<b>Applications Logs</b>	Opens the <a href="#">Application Logs</a> . This is useful for understanding encountered errors.
<b>Diagnostic</b>	Launches the <a href="#">Diagnostic</a> feature.
<b>Profiler</b>	Use the <a href="#">Profiler</a> to acquire specific information. Used to diagnose connectivity issues with a data source.
<b>Record</b>	Use the <a href="#">Recorder</a> . Used to help our Devolutions Support team troubleshoot the problem
<b>Submit a Support Ticket</b>	Submit a Support Ticket. Help us make your experience better by reporting experience issues or by asking for new features.
<b>Visit our Forum</b>	Visit our <a href="#">Forum</a> . You can create an account and experience the bleeding edge of our customer support.
<b>Change History</b>	Send you directly to our Remote Desktop Manager web page to view the <a href="#">new features and enhancements</a> when a new version is release.



## ABOUT

OPTION	DESCRIPTION
<b>Check for Updates</b>	Launch the Update Manager.
<b>About</b>	Learn about Remote Desktop Manager.

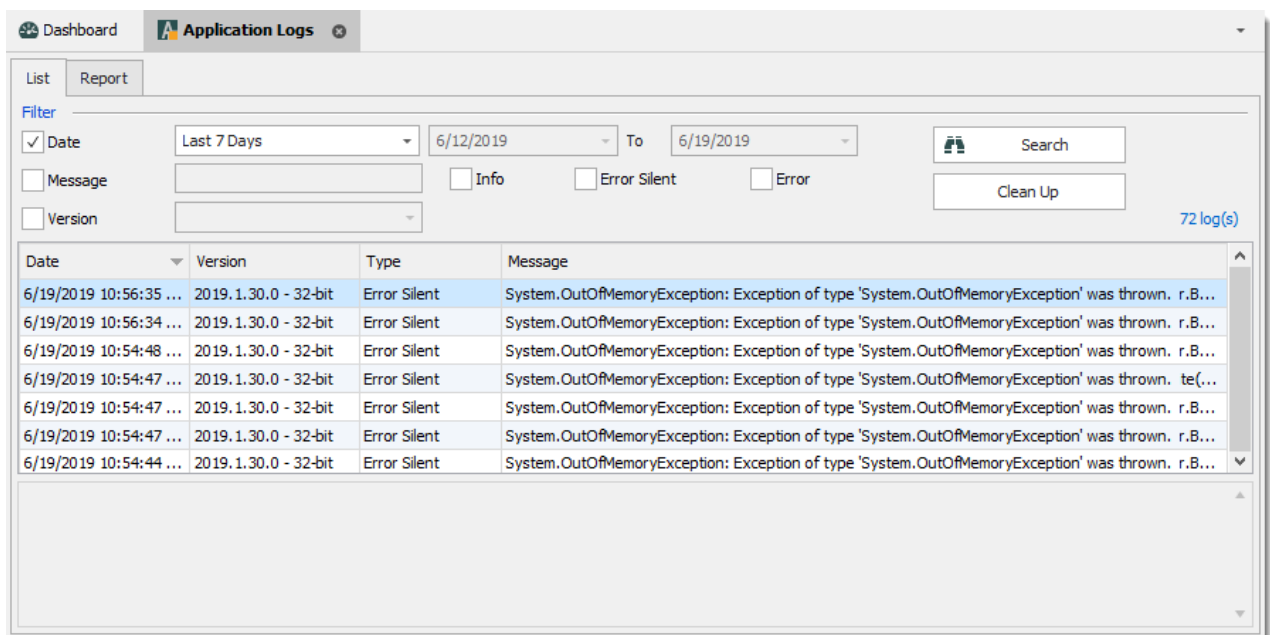
### 6.9.1 Support

#### 6.9.1.1 Application Log

## DESCRIPTION

When encountering errors, you can verify the local application log, which is available in **Help – Application Logs**.

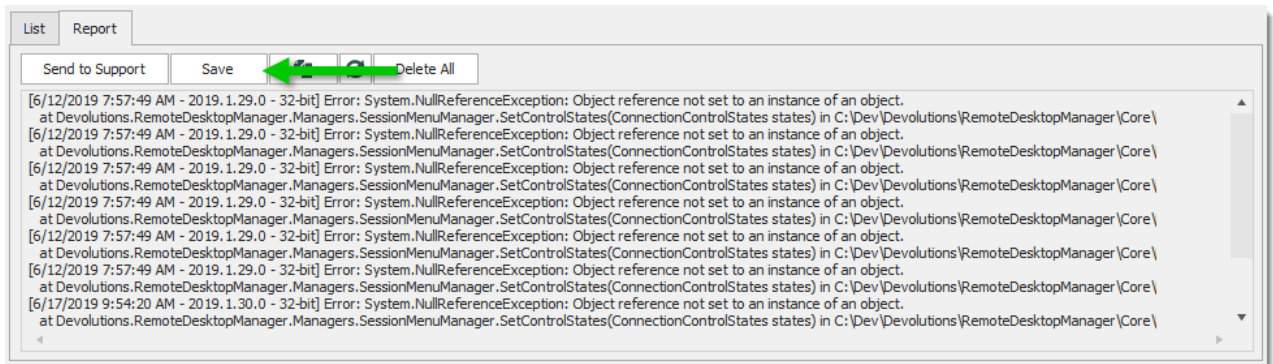
These logs are saved in **%LocalAppData%\Devolutions\RemoteDesktopManager\RemoteDesktopManager.log.db**. Logs are displayed as a list which can be filtered by date, message, version, or type of log.



View Application Log dialog

## REPORT

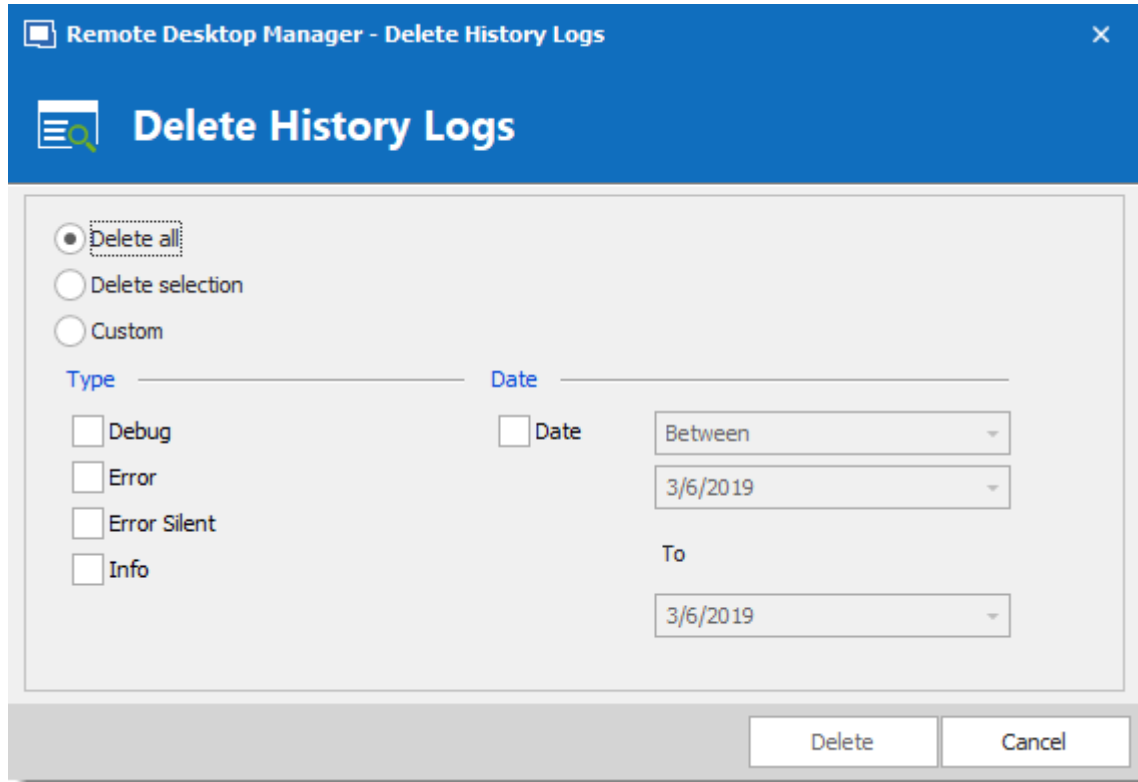
A report of the logs can be saved in a text file as well. Simply navigate to the **Report** tab of the application log, then click on the **Save** button to select a location to save the file.



## CLEAN UP

For security reason, it is a best practice is to clean up the application log once every month. To do so, in the application log, use the **Clean Up** feature.

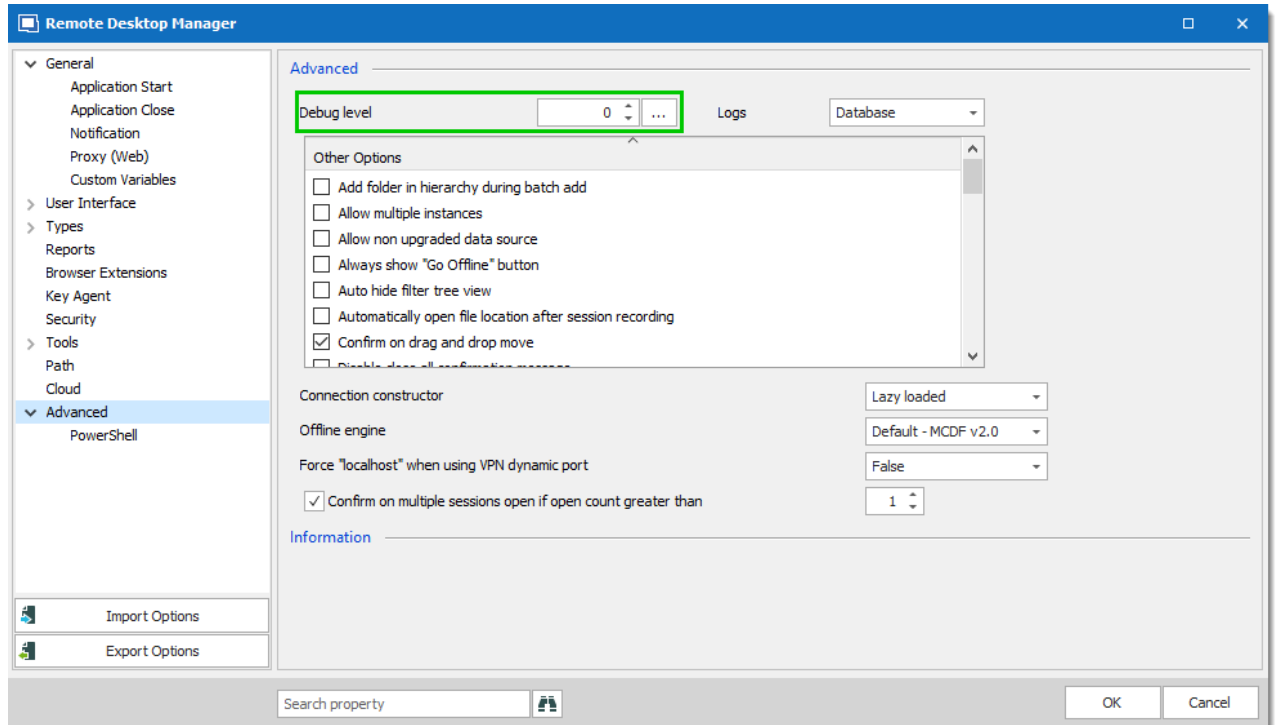
We strongly recommend to do a **Delete all**, but this can be customized to delete specific logs by type, date or selection.



## INCREASING THE DEBUG LEVEL

When experiencing issues with Remote Desktop Manager our support team might ask you to increase the debug level of the application during the support process. We strongly suggest to only increase the debug level when requested by our support team.

Increase the debug level in [File - Options - Advanced](#).



*File – Options – Advanced – Debug level*

### 6.9.1.2 Diagnostic

## DESCRIPTION

If you encounter a problem with Remote Desktop Manager, you can run a system diagnostic, which is available in **Help – Diagnostic**. This could help diagnose or give a pointer to what kind of issues you might be experiencing.

## SYSTEM

The administrator item could be the possible source for security problem. This happens often when a user has the SYSDBA or is DB\_OWNER of the SQL Server database.

Some other issues could be related to the fact that the application is running in Remote Desktop Services. However Remote Desktop Manager is fully compatible with Remote Desktop Services.

FIPS related issues and solutions can be found in the specific FIPS (Encryption) troubleshooting section.

If you have a [Remote Desktop Manager Jump](#) configured you can run a test of your Jump host by clicking on Jump Test.

**Remote Desktop Manager - System Diagnostic**

## System Diagnostic

System | Data Source | Policy

Windows 10 Version 1809 (OS Build 17763.379) 64-bit	✓ ?	Jump Test
Support local password saving	✓	
Is administrator	✓	
Is system administrator	✓	
Is database administrator	✓	
Is elevated privilege	✗	
Is running in Terminal Services	✗	
FIPS mode disabled	✓ ?	
Application Communicator is running	✓	
Workspace size	1621 / 822	
Is Internet connected	✓	
Allow multiple instances	✗	
Internet Explorer	11.379.17763.0 - Internet Explorer 11	
Debug level	0	
Running since	Running since: 2 hours 48 min 49 sec	
Font scaling	100% - Dpi aware: True	
Allow drag-and-drop	✓	
Is allowed by firewall	✓ ?	
RDP ActiveX version	10.0.17763.1 (WinBuild.160101.0800)	

Launch Profiler | Send | Close

System Diagnostic – System



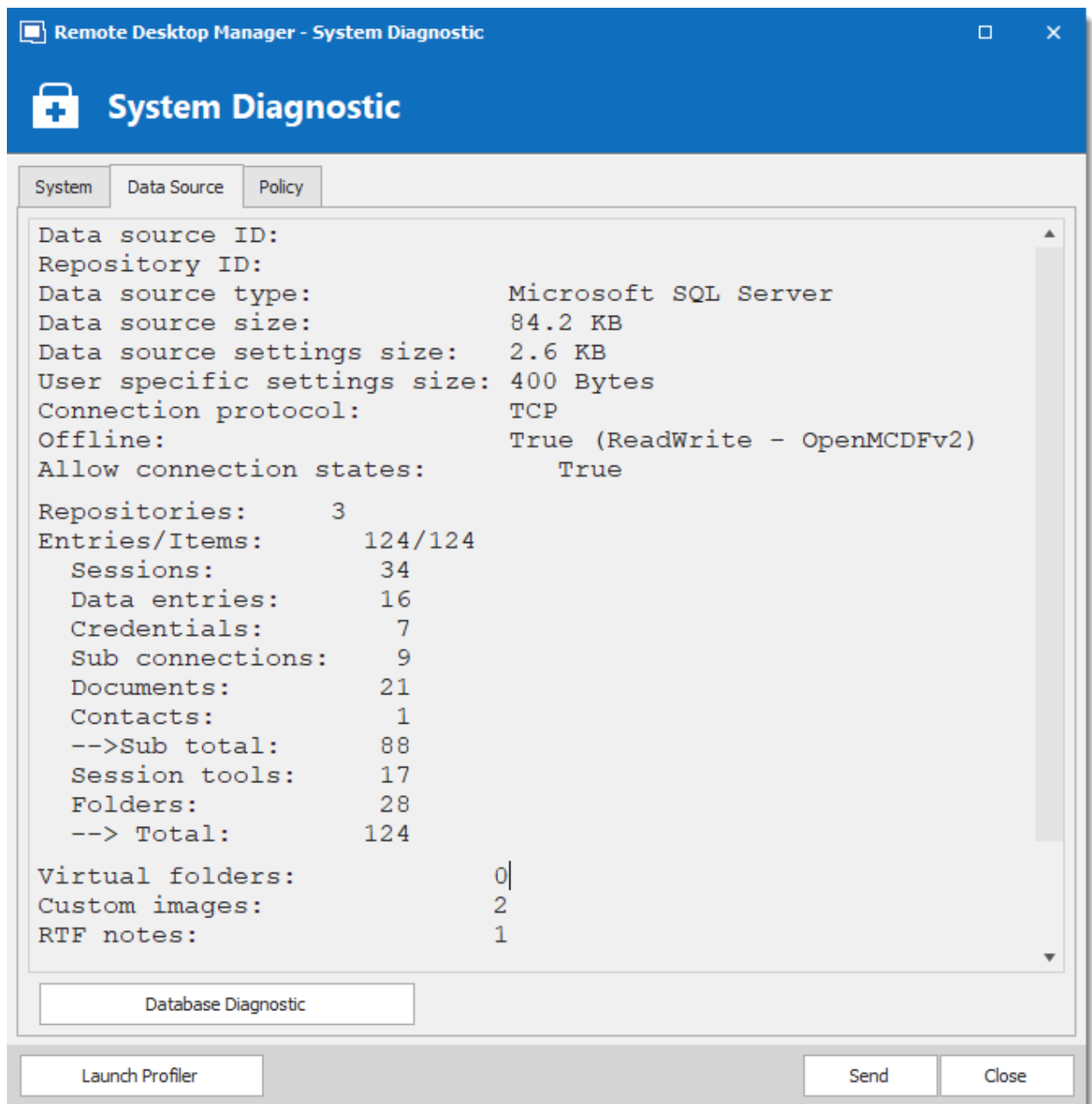
Please read the Troubleshooting topic if experiencing issues with Remote Desktop Manager, it lists error messages and could contain the fix/workaround for your problem.

## DATA SOURCE

The **Data Source** tab contains information regarding the current data source, such as the number of entries it contains, the size of your data source, the number of custom images and the offline state.



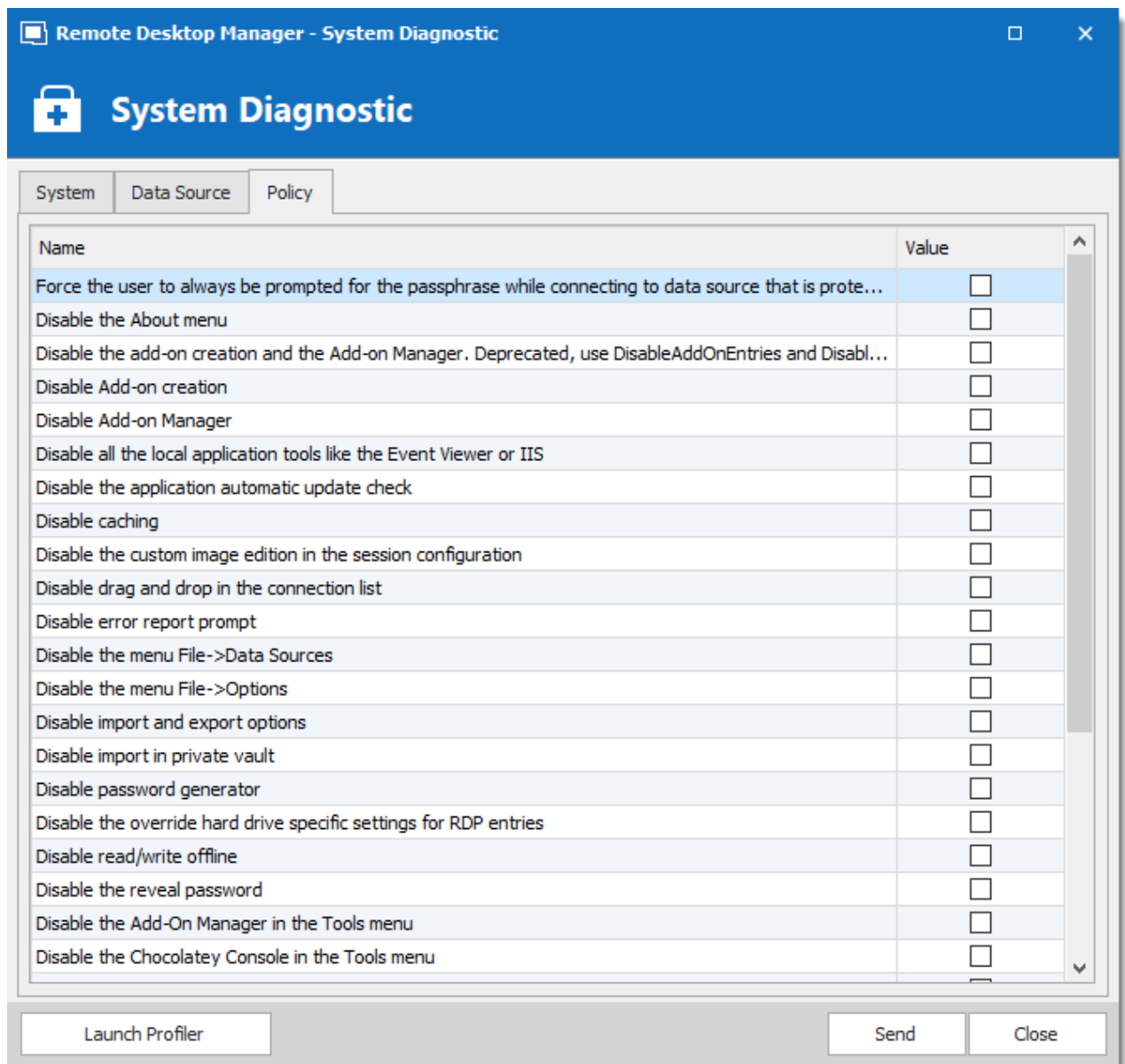
Too many custom images could dramatically increase the size of the data source and cause load time issue.



System Diagnostic - Data Source

## POLICY

The Policy tab display the list of Group Policy Templates to see if any of them has been applied.



System Diagnostic - Policy

### 6.9.1.3 Profiler

## DESCRIPTION

Remote Desktop Manager has a built-in profiler to diagnose connectivity issues with a data source.





Displaying the Profiler window might slow down the operations on the data source. Proceed with care.



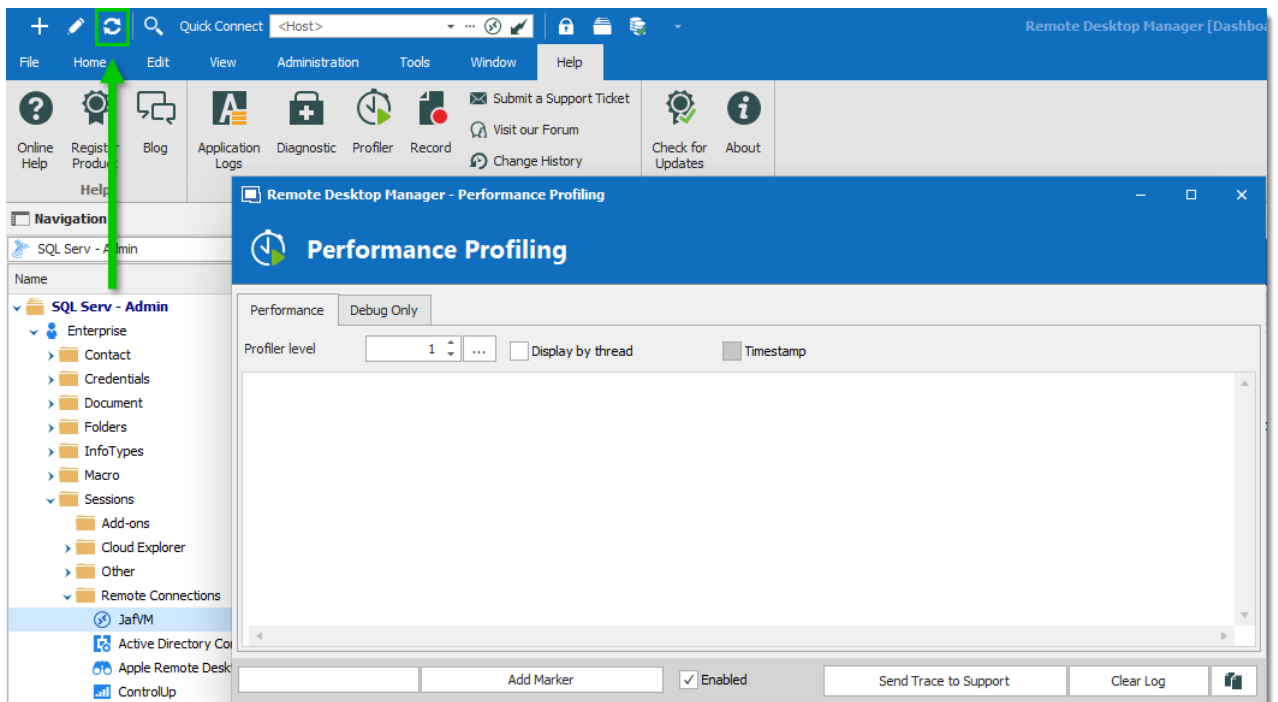
To diagnose startup issues, you can enable the profiler from the command line as described in Command Line Arguments

## PROCEDURE

1. Once the Profiler is opened, refresh the data source.

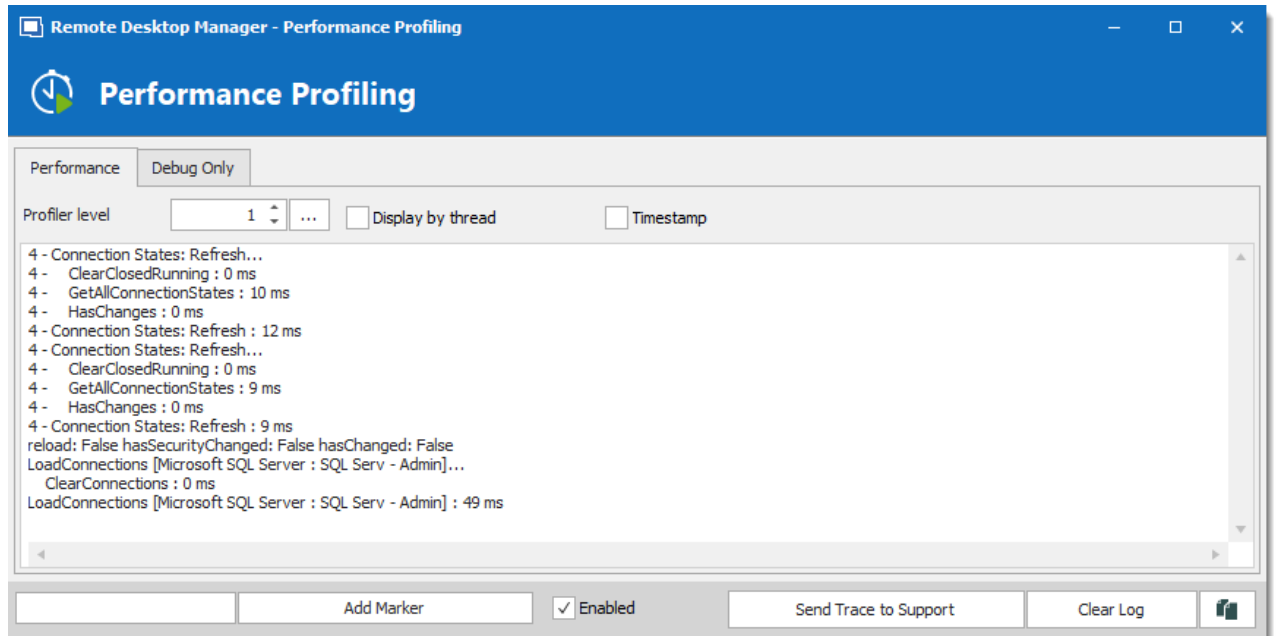


Holding the **Ctrl** key while performing the refresh should force a full reload of the data source, recreating the offline cache.



*Refresh Data Source*

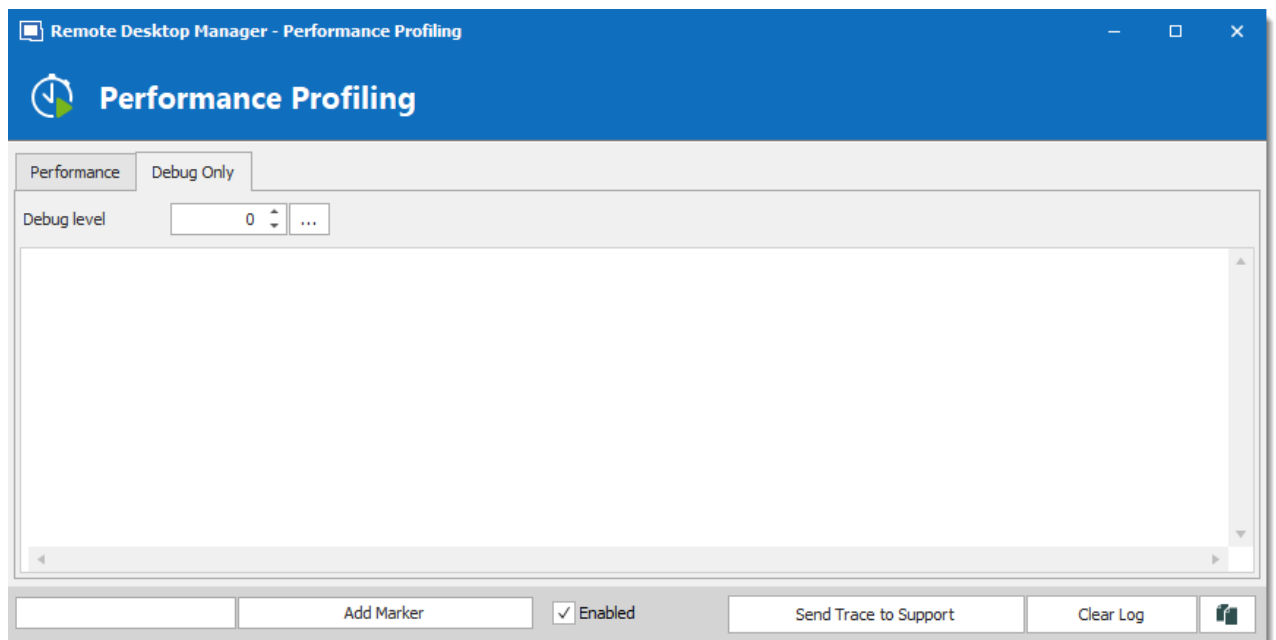
2. The Profiler data will appear in the **Performance Profiling** window.

*Performance Profiling*

3. Click on **Send Trace to Support** in order to send the Profiler data logs to our Devolutions support team. You can add a Marker when running multiple tests to separate them.

## DEBUG ONLY

To learn more about the **Debug only** tab please see the Debugging topic.

*Debug only*

#### 6.9.1.4 Record

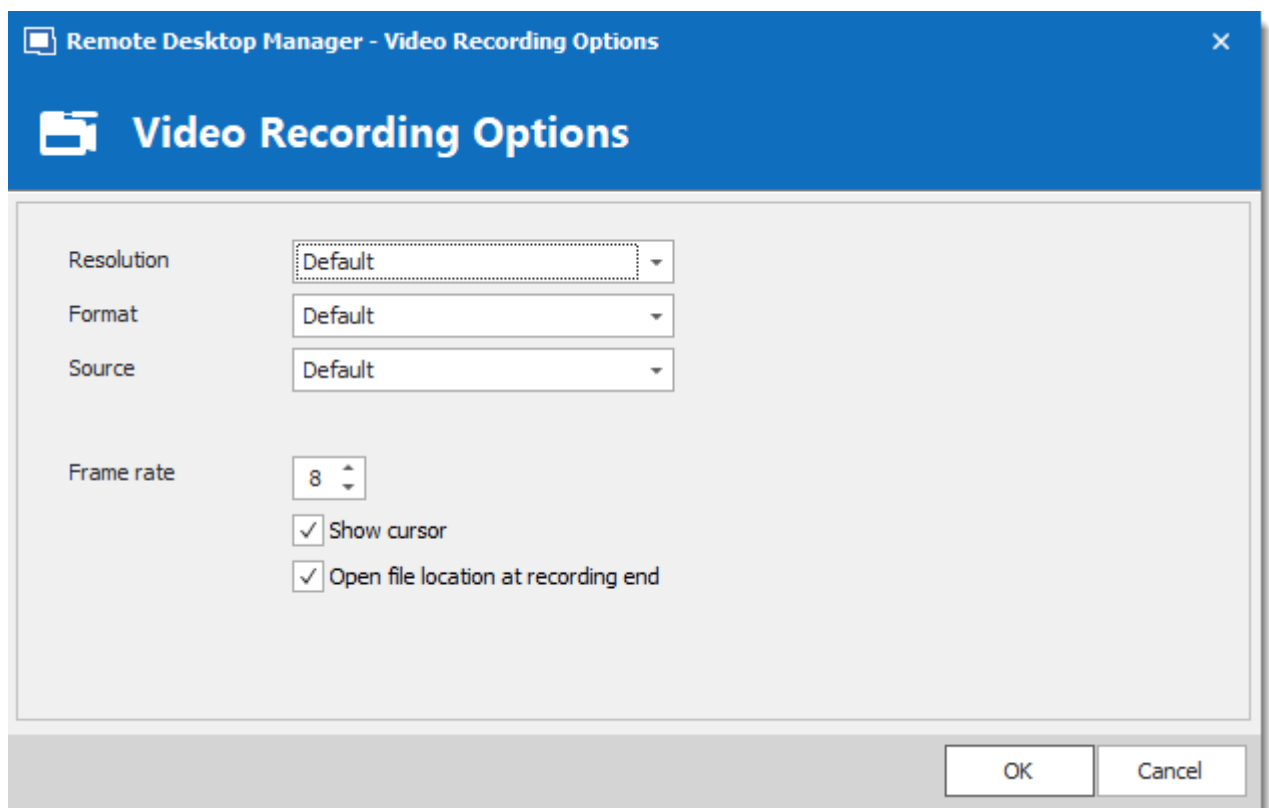
## DESCRIPTION

If you are experiencing issues with Remote Desktop Manager, you can help our Devolutions Support team troubleshoot the problem by sending them a short video of your issue. Launch this by using the **Record** feature located in the menu **Help – Record**.

The **Record** is an easy-to-use built-in screen recorder that could even be a useful for your in-house training as it is not limited to Remote Desktop Manager.

## SETTINGS

The Video Recording Options uses the MP4 format, which on Vanilla installs of Windows is not supported. If you encounter any difficulty viewing the video we strongly suggest the use of a [VLC player](#).



*Video Recording Options*

# Devolutions Web Login

---

Part VII

## 7 Devolutions Web Login




### 7.1 Overview

#### DESCRIPTION



**Devolutions Web Login** is a web browser password plugin used in conjunction with Remote Desktop Manager, Devolutions Password Server and Devolutions Password Hub, which allows users to securely inject passwords into websites using credentials stored in their vaults.

It gives system administrators full control over the management of passwords, without affecting the user's productivity.

 <p><b>Remote Desktop Manager</b></p> <p>Centralize, Manage and Secure Remote Connections</p>	 <p><b>Devolutions Password Server</b></p> <p>Secure, Manage and Monitor Access to Privileged Accounts</p>	 <p><b>Devolutions Password Hub</b></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 Password Server lets you control access to privileged accounts and manage remote sessions through a secure solution that can be deployed on-premises.</p>	<p>Devolutions 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.



#### **Warning for all Remote Desktop Manager users:**

**Devolutions Web Login** was created for a normal desktop environment. It uses inter process communication (IPC) with the client application. Using it on a terminal server introduces a level of risk that may be unacceptable for corporate users.

To use it in a safe manner, it is critical that each user is assigned a distinct port and that port be kept secret. An application passcode must be set as well to secure the port. The first client application that starts will be able to use the port exclusively. All **Devolutions Web Login** calling on that port **will get the responses**, unless an application passcode is required.

## 7.2 Installation

### DESCRIPTION

**Devolutions Web Login** is a free browser extension companion tools. It does require one of our products to function at this time.

Click on the browser link below to start the installation of Devolutions Web Login plugin:

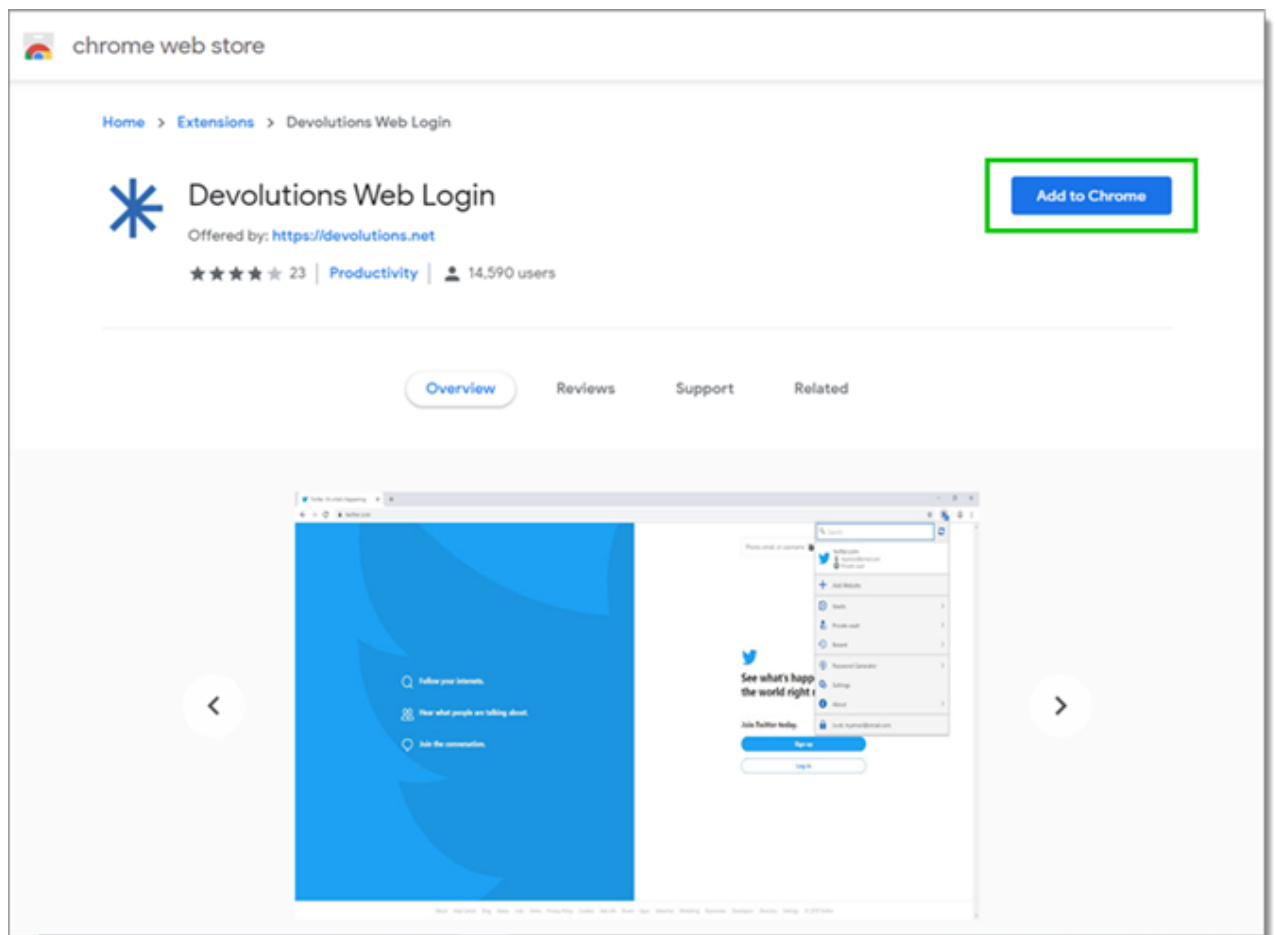
- [Chrome](#)
- [Firefox](#)
- [Microsoft Edge](#)
- [Opera](#)

## 7.2.1 Chrome

### DESCRIPTION

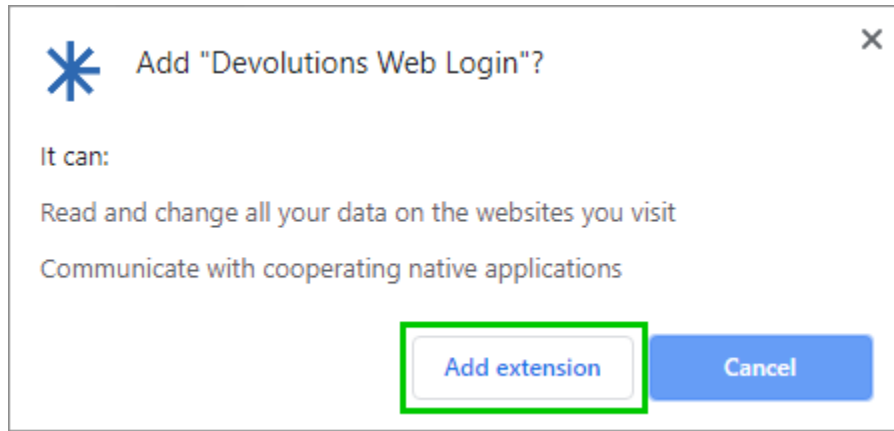
Follow the steps below to complete the installation of Devolutions Web Login in the Google Chrome web browser.

1. Open Google Chrome.
2. Navigate to [Devolutions Web Login extension](#) or use the link from our [Website](#)
3. Click the **Add To Chrome** button.



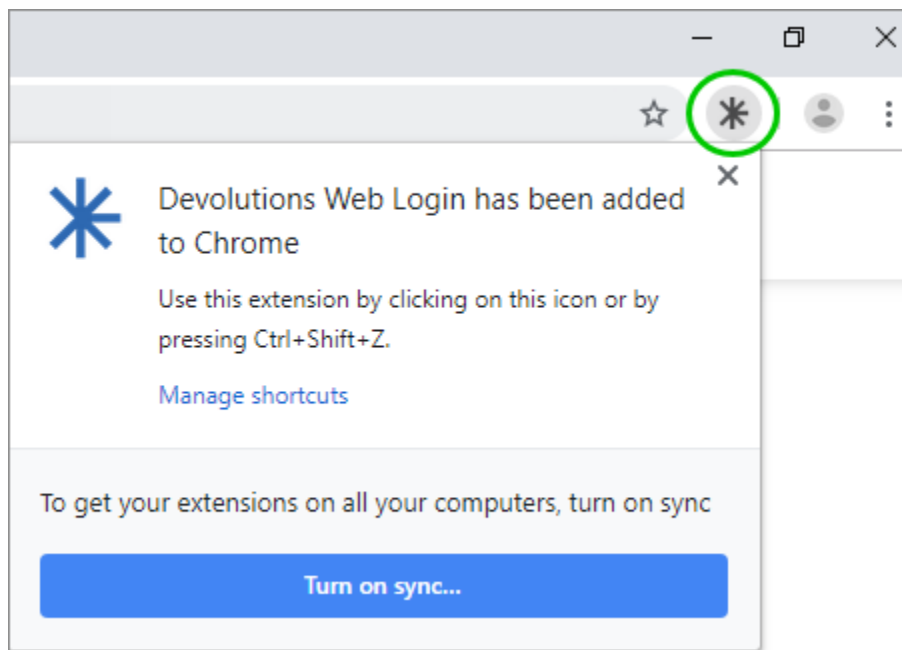
*Devolutions Web Login Chrome Web Store*

4. Click **Add extension** in the confirmation dialog.



*Extension Installation Confirmation*

Once installed, access the extension by clicking \* in the top-right corner of the Google Chrome web browser.



*Devolutions Web Login Extension Button*

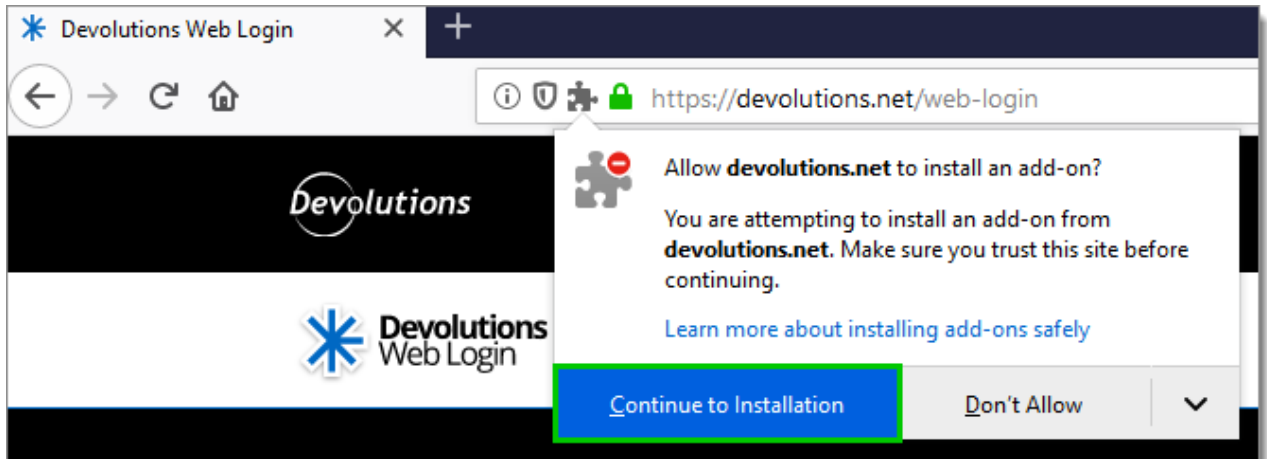
## 7.2.2 Firefox

### DESCRIPTION

Follow the steps below to complete the installation of Devolutions Web Login in the Firefox web browser.

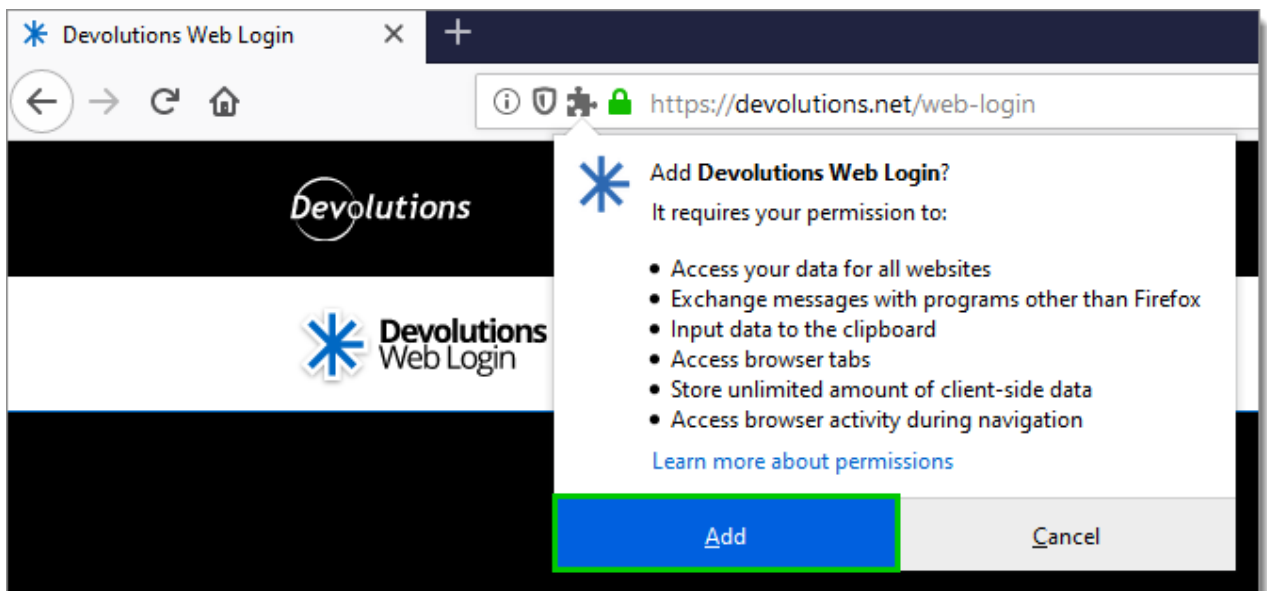


1. Open a Firefox window.
2. Download the extension from our [Devolutions Web Login](https://devolutions.net/web-login) website page.
3. Click **Continue to Installation** in the confirmation dialog.



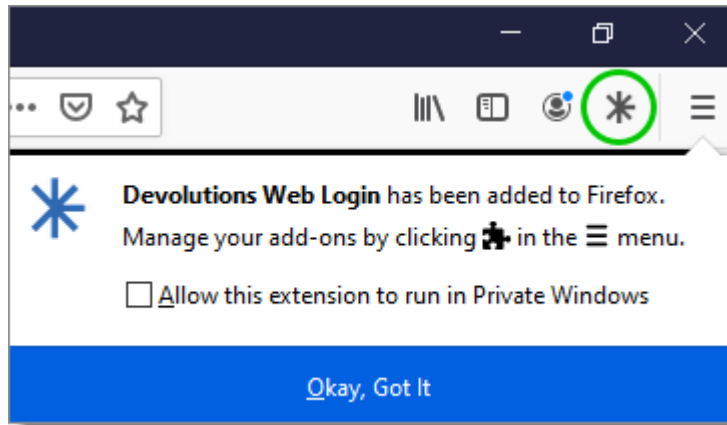
*Continue to Installation*

4. Click **Add**, when prompted to add Devolutions Web Login to the extension.



*Add the Extension*

5. Once installed, access the extension by clicking \* in the top-right corner of Firefox.



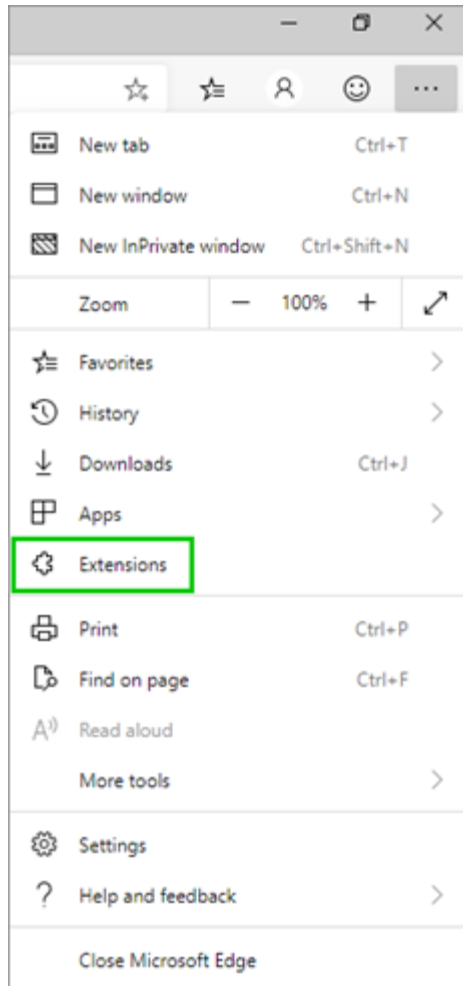
*Devolutions Web Login Extension Button*

### 7.2.3 Microsoft Edge Beta

#### DESCRIPTION

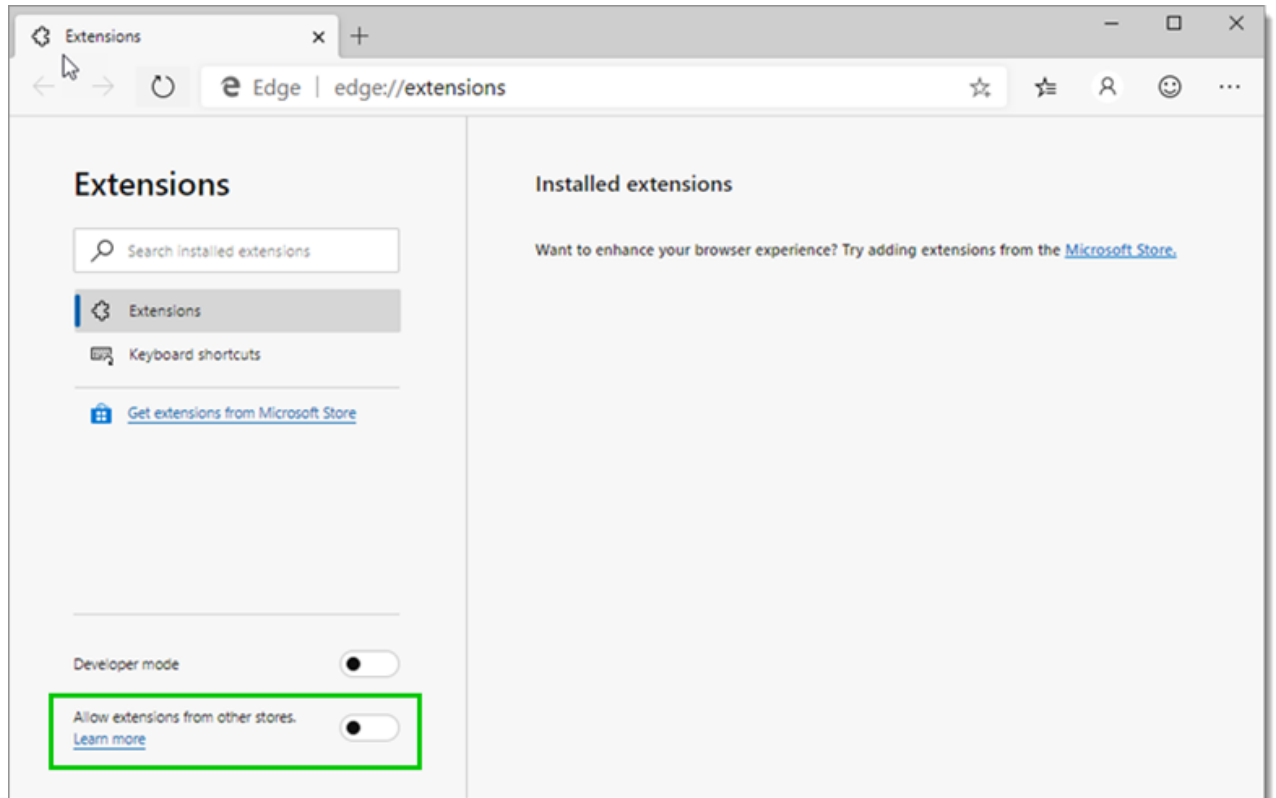
Here are the steps to install Devolutions Web Login on Microsoft Edge Beta.

1. Open [Microsoft Edge Beta](#).
2. Click on **Extensions** in the menu of the browser.



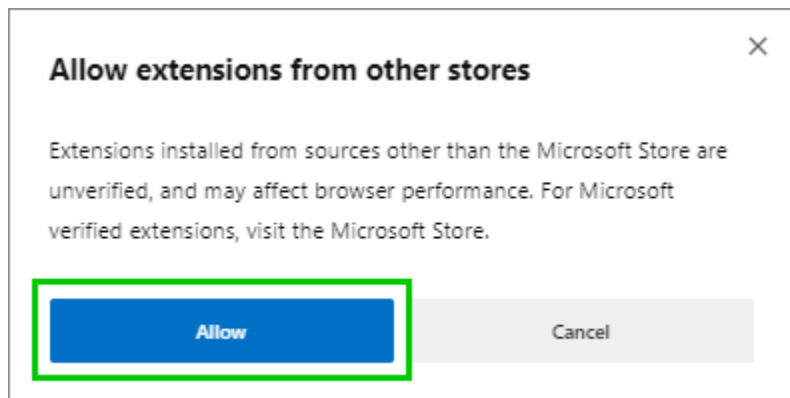
*Microsoft Edge Beta Menu*

3. Allow extensions from other stores.



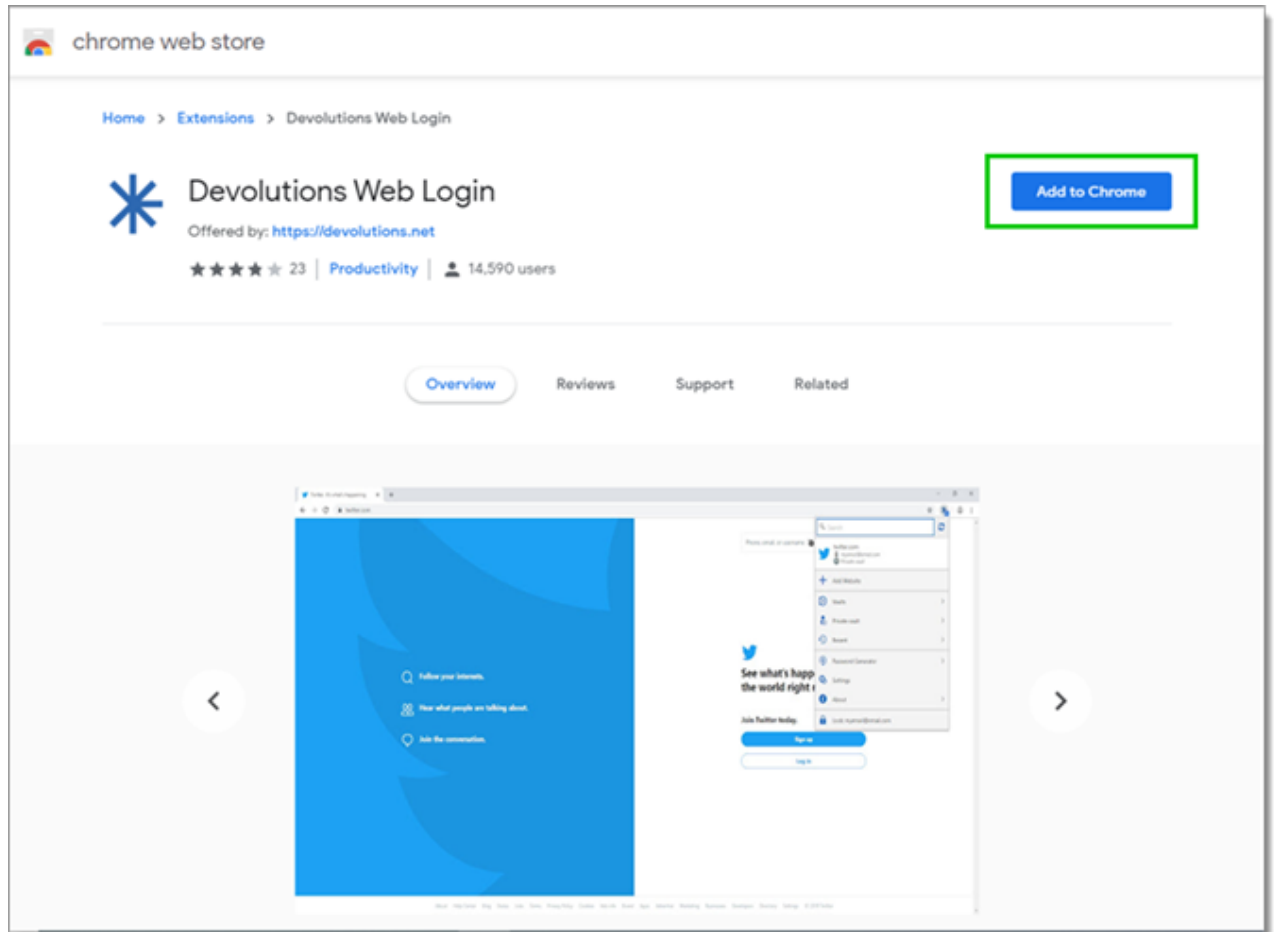
*Allow Extensions*

4. Allow Non Microsoft Store Extensions.



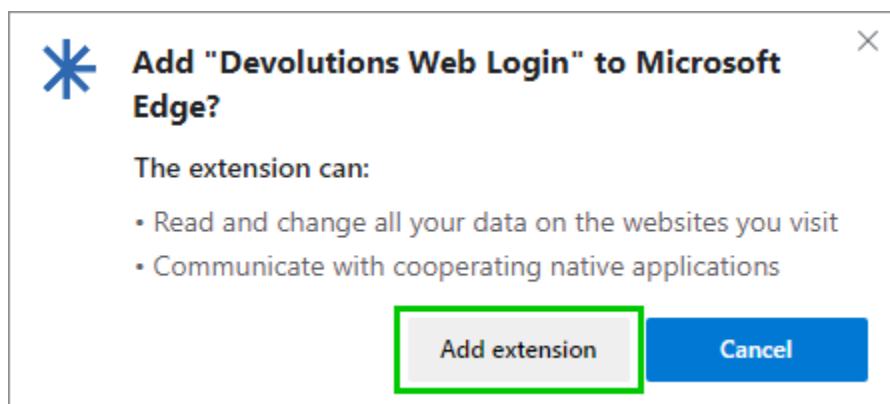
*Allow Non Microsoft Store Extensions*

5. Follow the extension from [Devolutions Web Login](#) website page to the Chrome Web Store.
6. Click **Add to Chrome**.



Chrome Web Store

7. Add the extension to Microsoft Edge Beta.



Add Devolutions Web Login to Microsoft Edge Beta

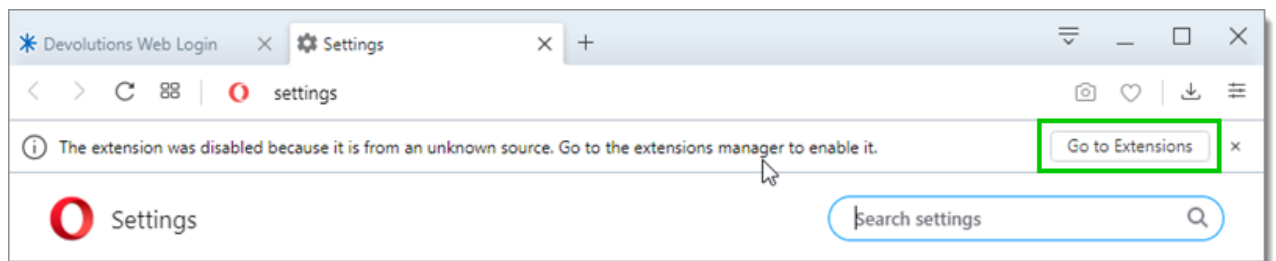
The extension is installed. Access it by clicking \* in the top-right corner of the Microsoft Edge Beta web browser.

## 7.2.4 Opera

### DESCRIPTION

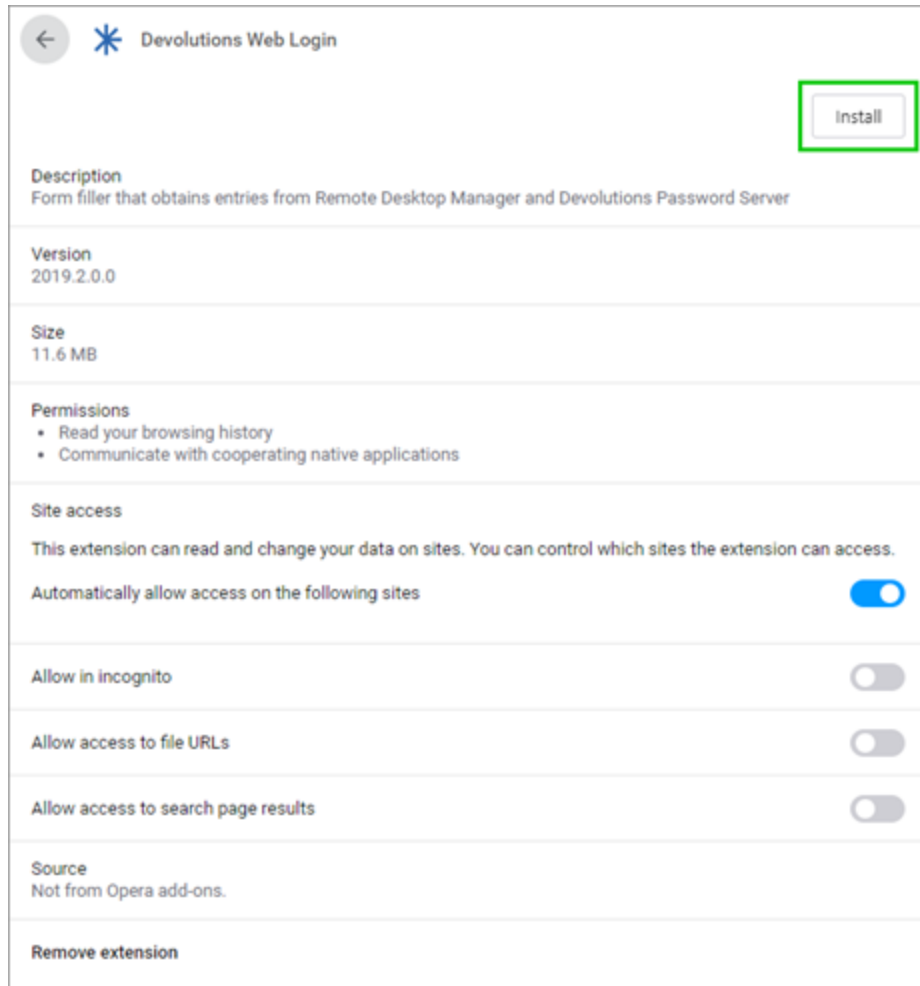
Follow the steps below to complete the installation of Devolutions Web Login in the Opera web browser.

1. Open Opera.
2. Download the extension of [Devolutions Web Login](#) from our website page.
3. Go to **Browser Settings** in the easy setup of Opera.
4. Drag and drop the .nex file from step 2 from the downloads in the web browser.
5. Click on **Go to Extension** from the information panel at the top.



*Opera Extensions Enabling*

6. Click **Install** and the **Yes, install** pop up.



*Opera Install Window*

7. Access the extension by clicking \* in the top-right corner of Opera.

## 7.3 First Login

### 7.3.1 Password Hub

## DESCRIPTION

## FIRST LOGIN WITH DEVOLUTIONS WEB LOGIN

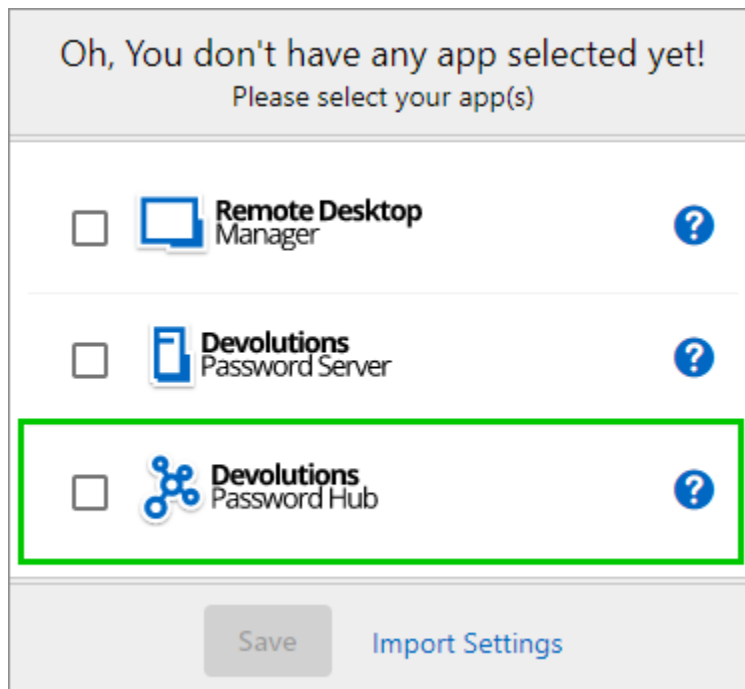
Follow these steps to connect Devolutions Password Hub to Devolutions Web Login extension:

1. Click on **Devolutions Web Login \*** extension at the top right corner of your browser.



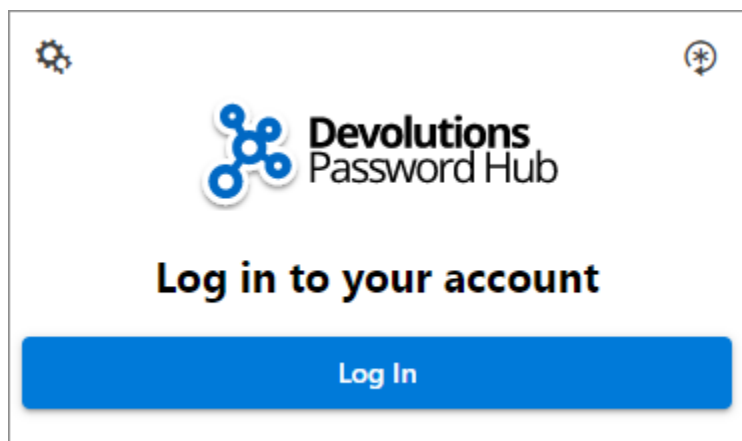
A Devolutions Password Hub access is required to continue.

2. Choose **Devolutions Password Hub** in the list and **Save**. You could at this point import settings; the option will also be available in the [Settings](#) menu after the log in.



*First Login*

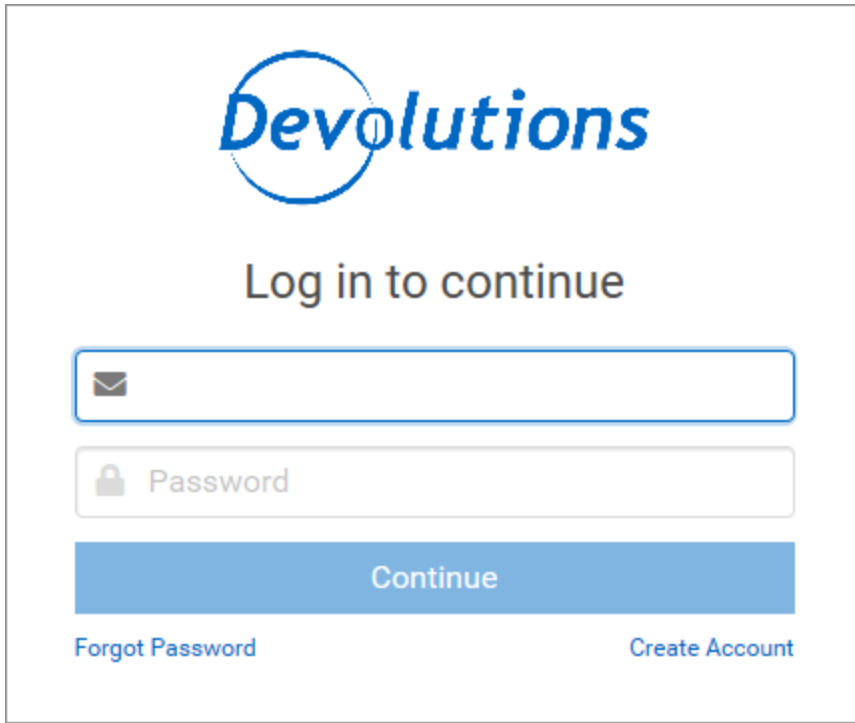
3. **Log in** to your account.



*Log In*



4. Enter the credentials from your Devolutions Account to continue.

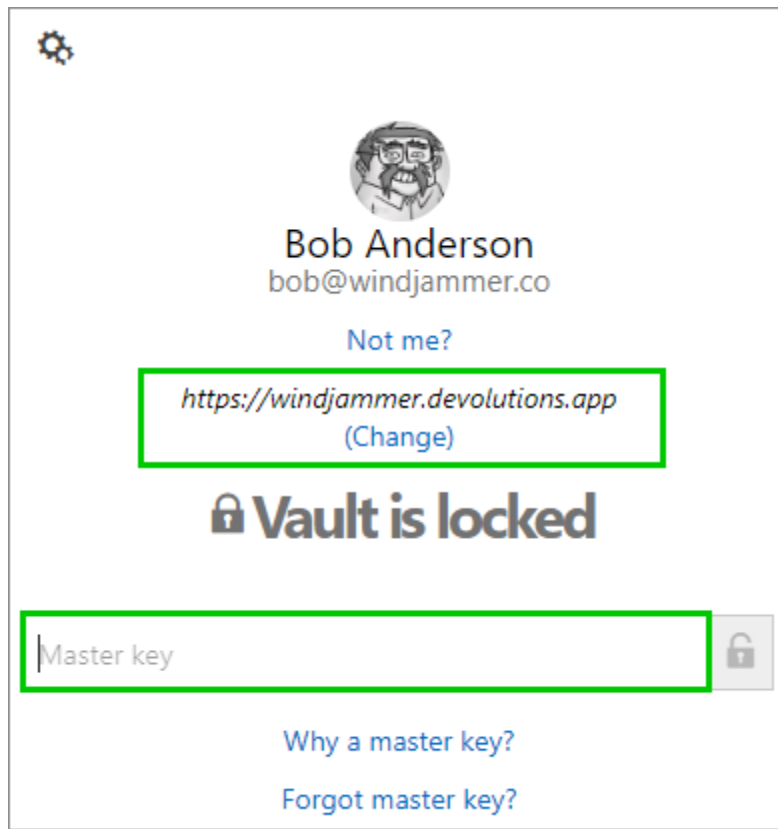
The image shows a login interface for Devolutions. At the top is the Devolutions logo, which consists of the word "Devolutions" in a blue, sans-serif font, with a blue circle around the letter "o". Below the logo is the text "Log in to continue" in a dark gray font. There are two input fields: the first is for an email address, indicated by an envelope icon on the left, and the second is for a password, indicated by a lock icon on the left and the word "Password" in a light gray font. Below these fields is a large blue button with the word "Continue" in white. At the bottom of the login area, there are two links: "Forgot Password" on the left and "Create Account" on the right, both in a blue font.

*Devolutions Account Login*


5. Unlock the vault with your master key.



Devolutions Web Login will recognize automatically the Password Hub linked to your Devolutions account. Click **Change** to modify the URL.





⚙️

  
**Bob Anderson**  
bob@windjammer.co

[Not me?](#)

<https://windjammer.devolutions.app>  
[\(Change\)](#)

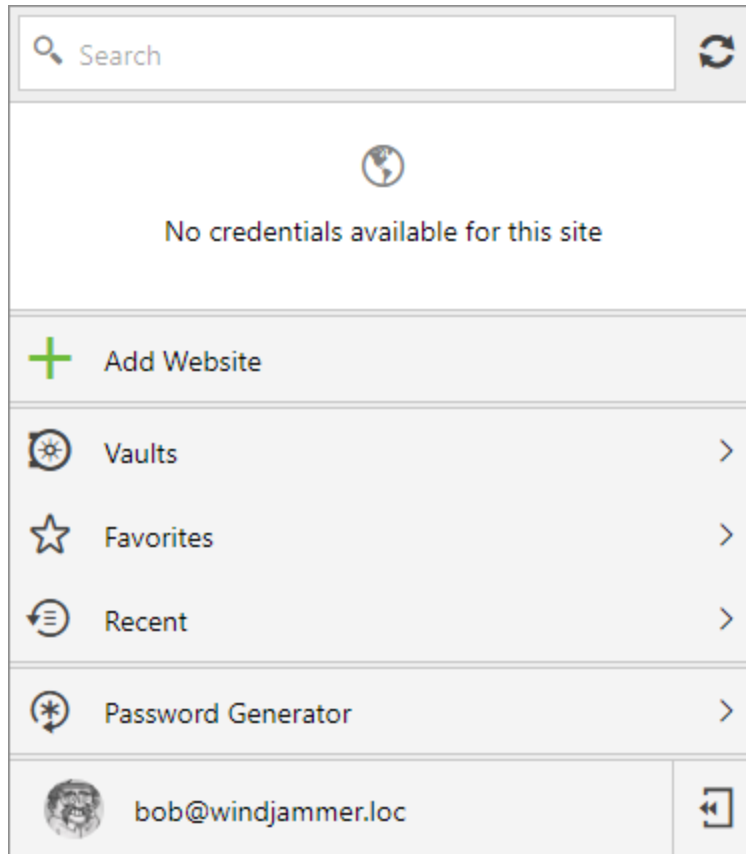
 **Vault is locked**



[Why a master key?](#)  
[Forgot master key?](#)

*Password Hub Master key*

Devolutions Web Login is now connected to your vaults.



*Devolutions Web Login Connected to Devolutions Password Hub*

#### 7.3.1.1 Multiple Password Hub

## DESCRIPTION

### MANAGING MULTIPLE PASSWORD HUB WITH DEVOLUTIONS WEB LOGIN

Devolutions Web Login will automatically acknowledge all Password Hub linked to your Devolutions account.

- [View active Password Hub](#)
- [Switch Password Hub in Devolutions Web Login](#)

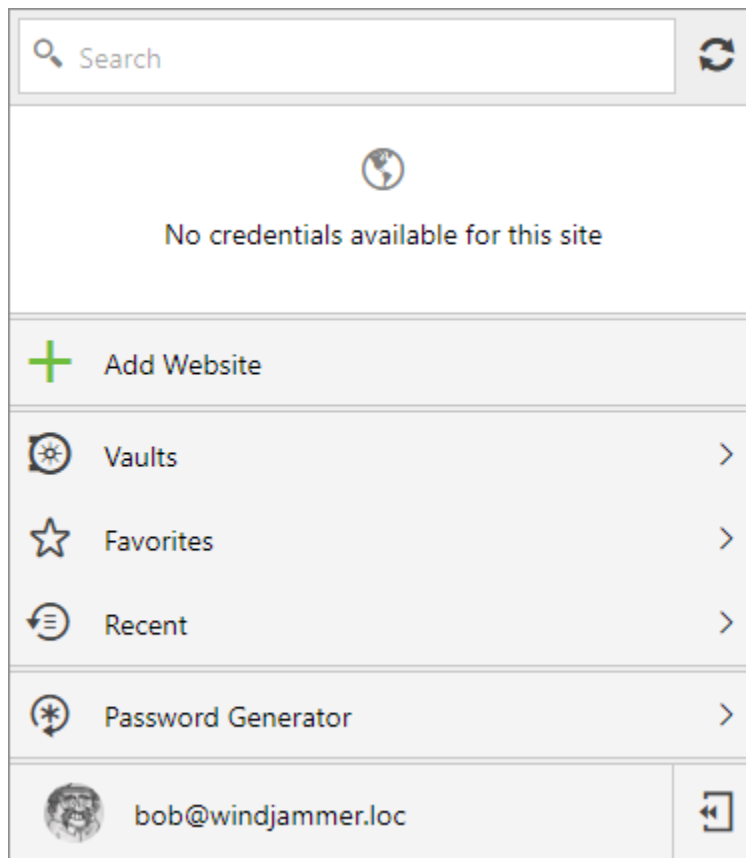


Devolutions Web Login will only recognize and apply credentials from the **active** Password Hub.

## VIEW ACTIVE PASSWORD HUB

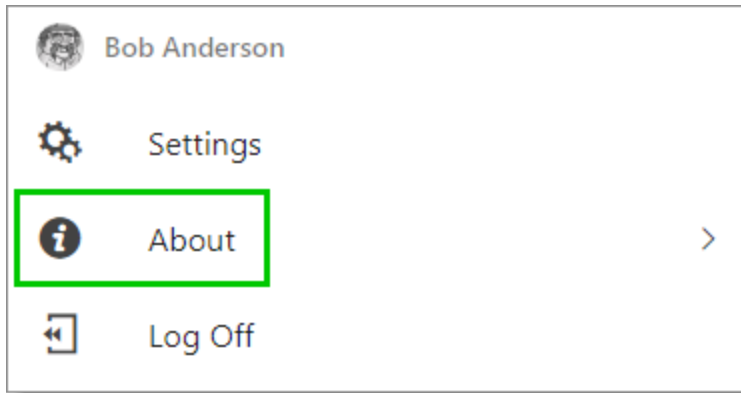
To view/validate the active Password Hub, click on the **Devolutions Web Login** \* extension at the top right corner of your browser.

1. Click on your avatar at the bottom of the window.



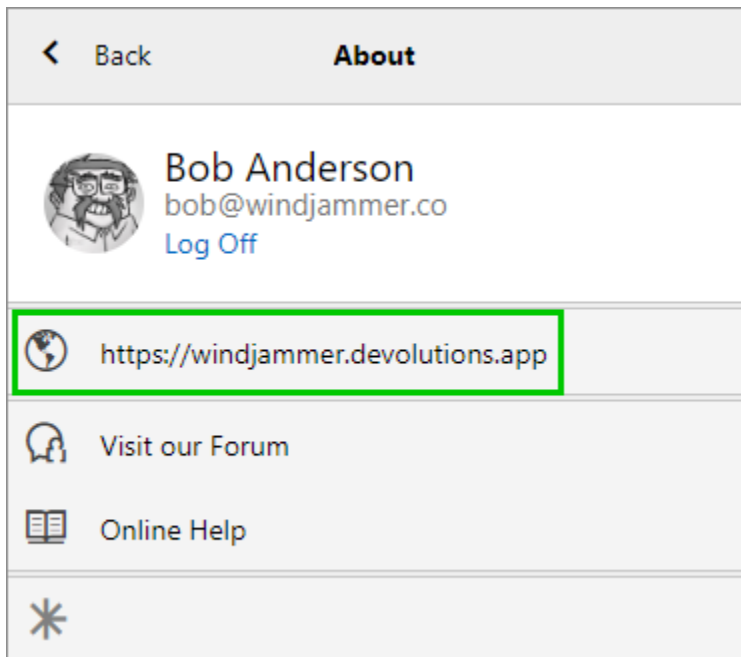
*Devolutions Web Login*

2. Click **About**.



*Devolutions Web Login About*

3. Validate the Password Hub URL.

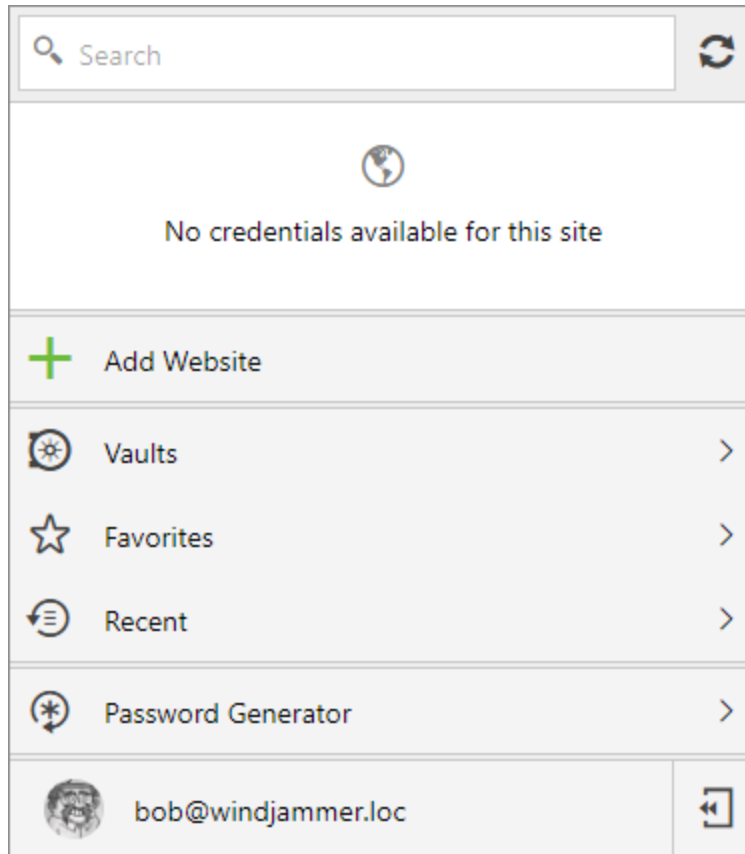


*Password Hub URL*

## SWITCH PASSWORD HUB IN DEVOLUTIONS WEB LOGIN

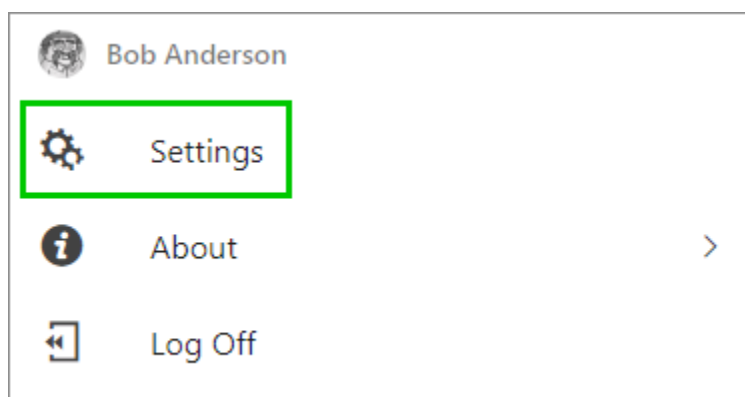
To switch Password Hub in Devolutions Web Login, click on the **Devolutions Web Login** \* extension at the top right corner of your browser.

1. Click on your avatar at the bottom of the window.



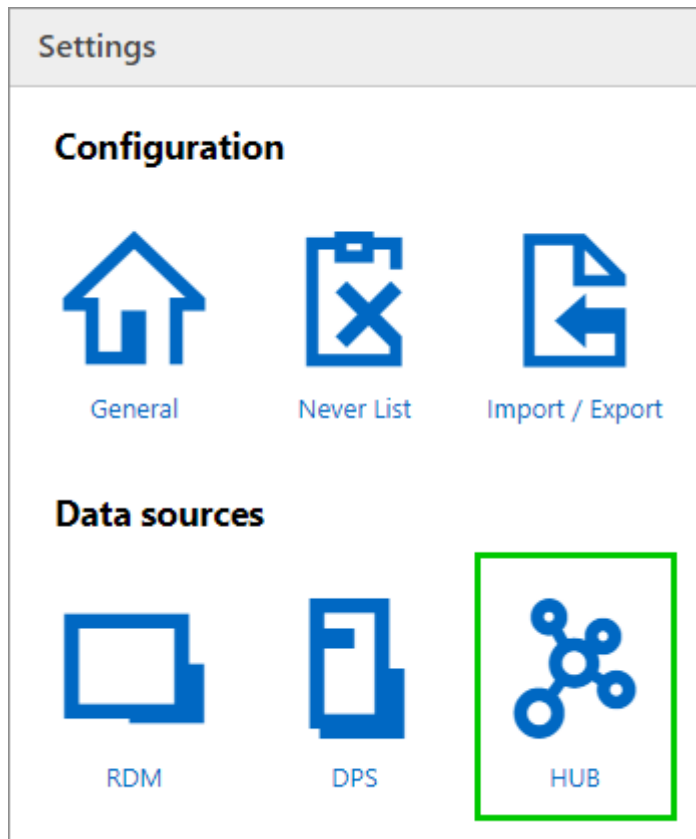
*Devolutions Web Login*

2. Click **Settings**.



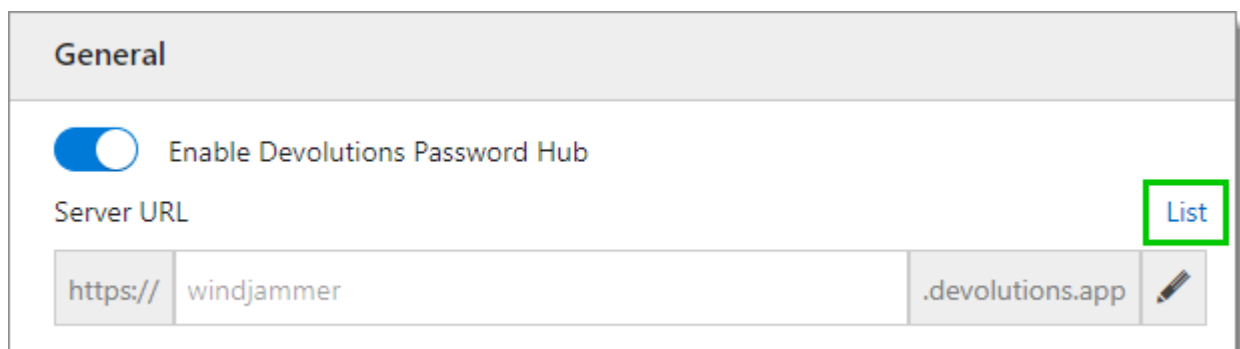
*Devolutions Web Login Settings*

3. Click **HUB**.



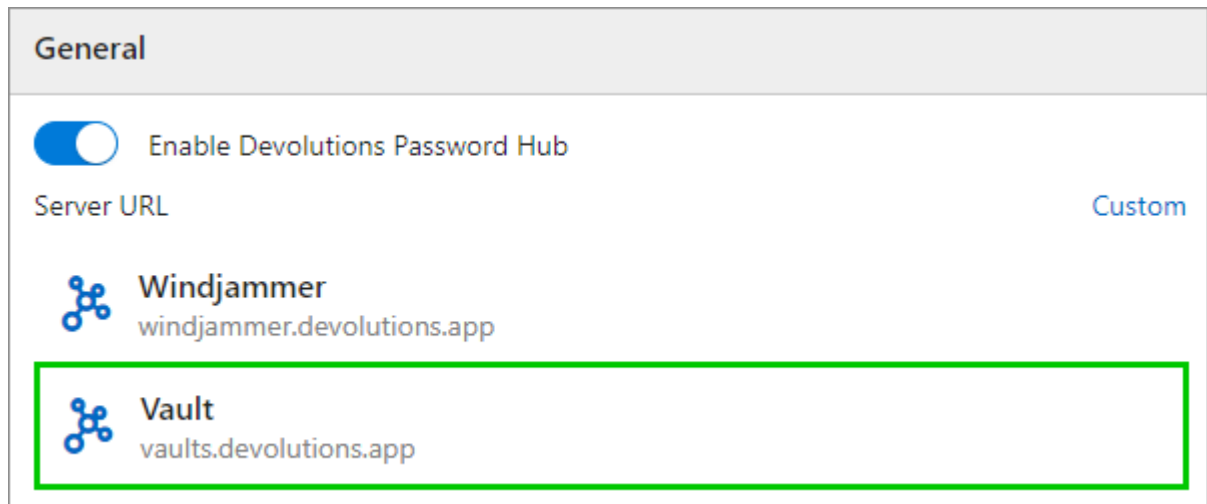
*Devolutions Web Login Settings Menu*

4. In the **General** section, click **List**.



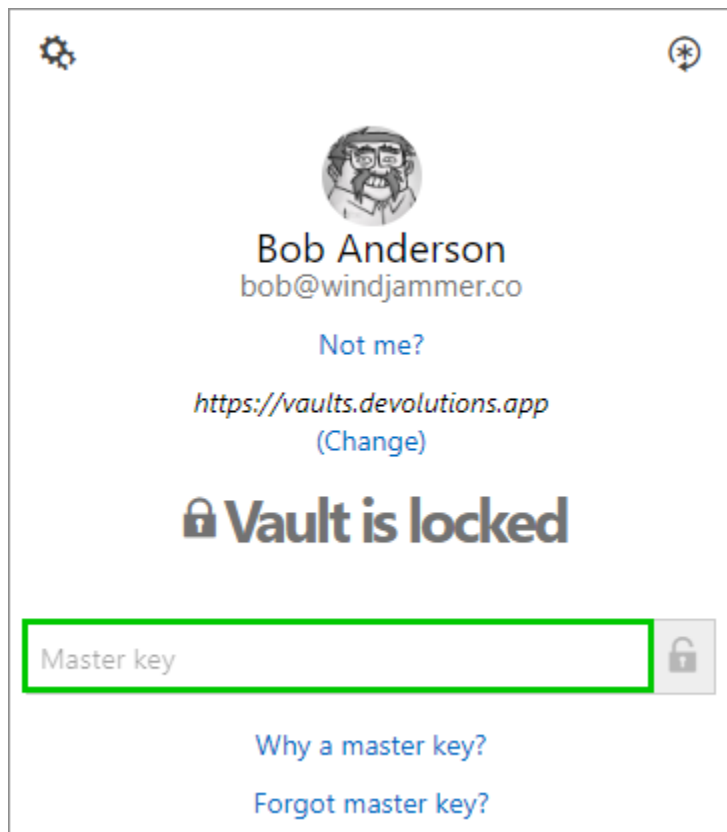
*Devolutions Web Login General Settings*

5. All the available Password Hub linked to your Devolutions account will show in the list. Switch by clicking once on the desired Password Hub.



*Password Hub List*

6. Click on the **Devolutions Web Login** \* extension at the top right corner of your browser and enter the Master key associated with this Password Hub.



*Password Hub Switch Master key*



## 7.3.2 Password Server

### DESCRIPTION

#### FIRST LOGIN WITH DEVOLUTIONS WEB LOGIN

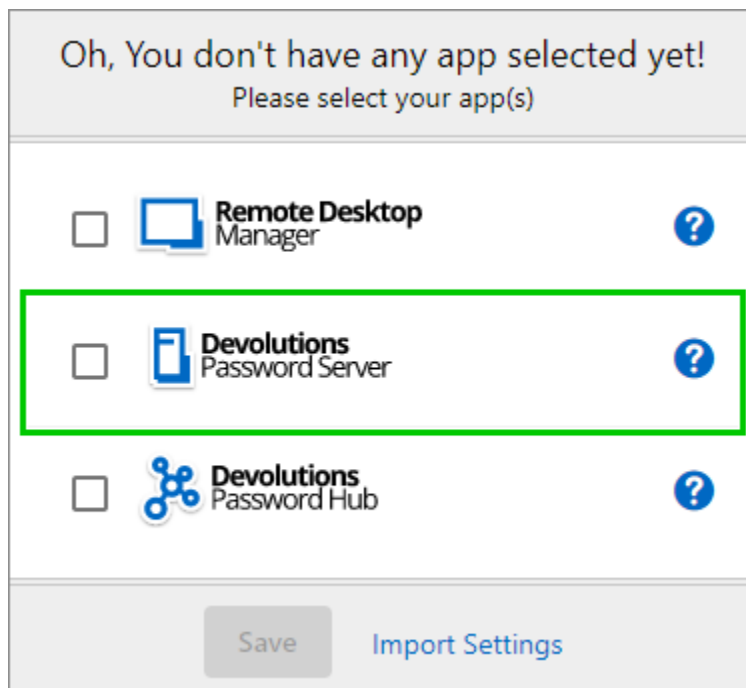
Follow these steps to connect Devolutions Password Server to Devolutions Web Login extension:

1. Click on **Devolutions Web Login** \* extension at the top right corner of your browser.



A Devolutions Password Server access is required to continue.

2. Choose **Devolutions Password Server** in the list and **Save**. You could at this point import settings; the option will also be available in the [Settings](#) menu after the log in.



*First Login*

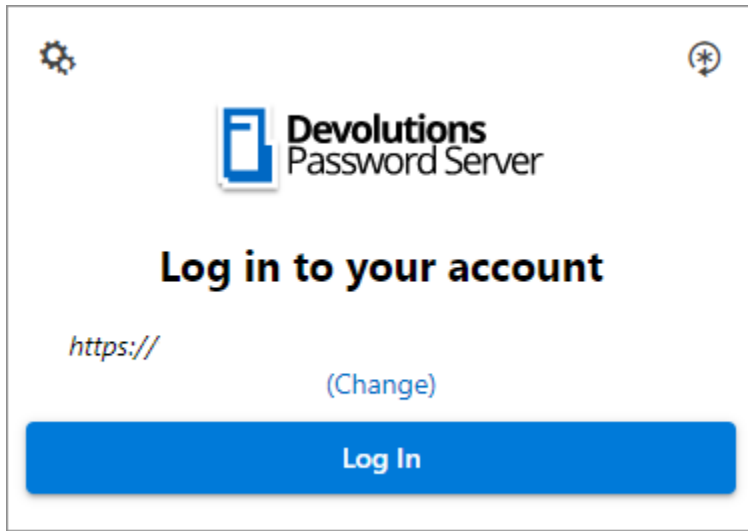
3. Enter the server address. Test the connection to validate it, then **Save**.



The screenshot shows a window titled "Devolutions Password Server". At the top left is a gear icon and at the top right is a circular icon with a star. The main heading is "Please enter the server address". Below this is a text input field. At the bottom are two buttons: "Test Connection" and "Save".

*Server Address*

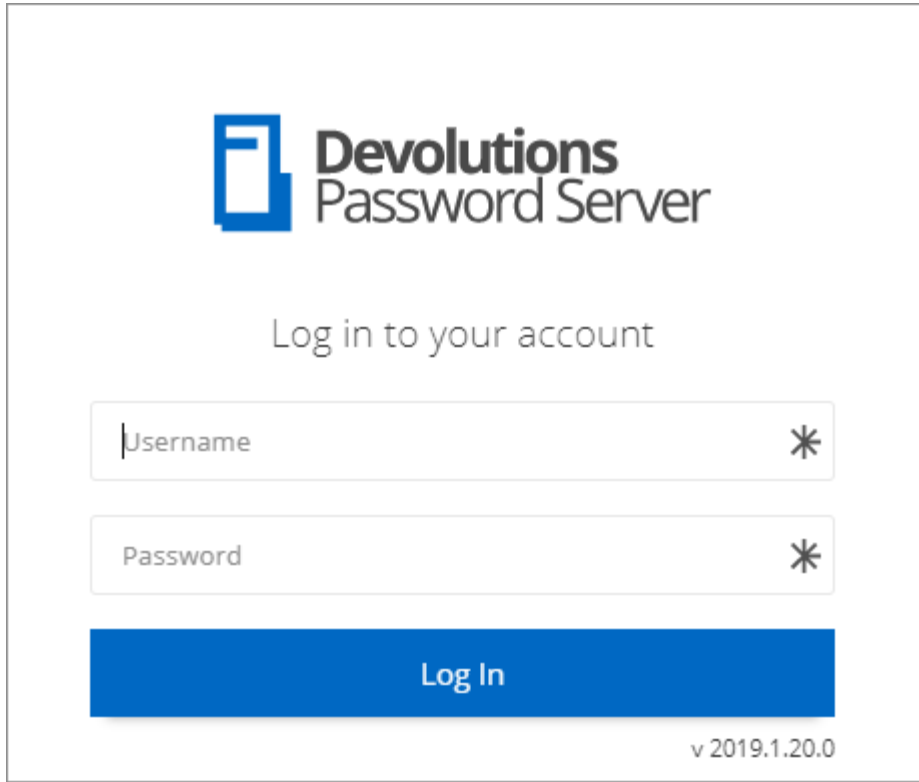
4. Press the **Log In** after you saved the address.



The screenshot shows a window titled "Devolutions Password Server". At the top left is a gear icon and at the top right is a circular icon with a star. The main heading is "Log in to your account". Below this is the text "https://" followed by a blue "(Change)" link. At the bottom is a large blue button labeled "Log In".

*Devolutions Web Login Login*

5. Enter your Devolutions Password Server credentials and log in.

The image shows a login form for Devolutions Password Server. At the top is the logo, which consists of a blue square icon with a white stylized 'D' and the text 'Devolutions Password Server' in a sans-serif font. Below the logo is the instruction 'Log in to your account'. There are two input fields: the first is labeled 'Username' and the second is labeled 'Password'. Both fields have a small asterisk icon to their right. Below the password field is a large blue button with the text 'Log In' in white. In the bottom right corner of the form, the version number 'v 2019.1.20.0' is displayed.

**Devolutions**  
Password Server

Log in to your account

Username \*

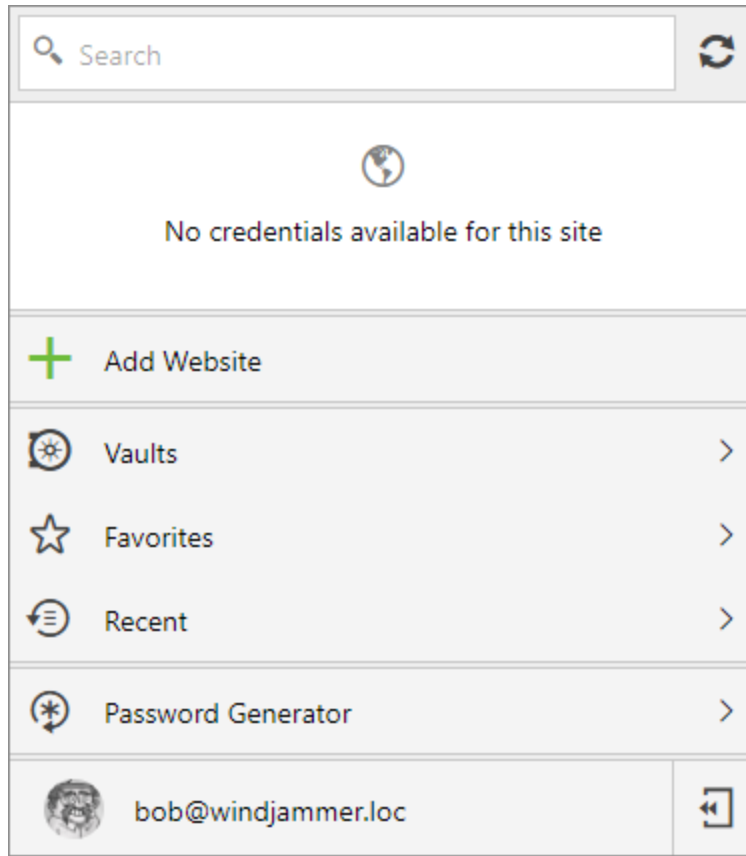
Password \*

Log In

v 2019.1.20.0

*Devolutions Password Server Login*

Devolutions Web Login is now connected to your vaults.



*Devolutions Web Login Connected*

### 7.3.3 Remote Desktop Manager

## DESCRIPTION

### FIRST LOGIN WITH DEVOLUTIONS WEB LOGIN

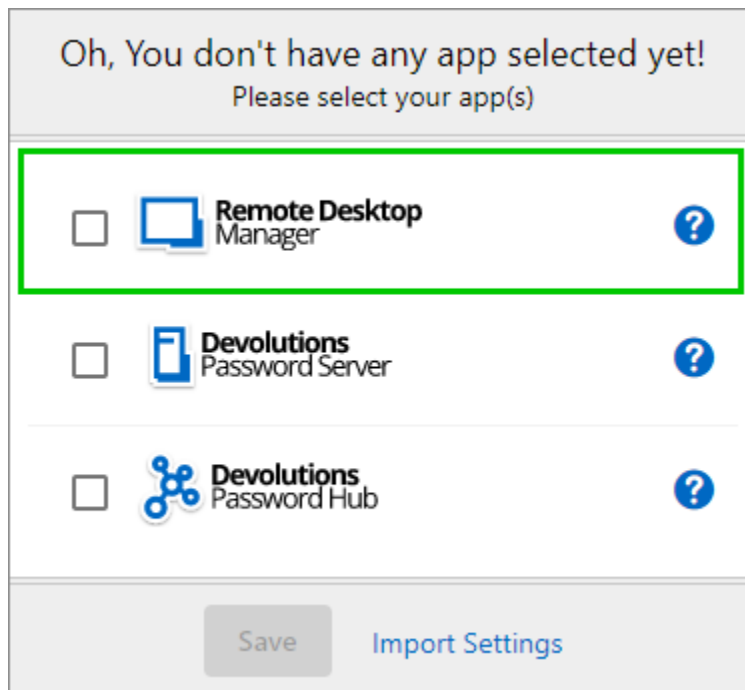
Follow these steps to connect your Remote Desktop Manager to Devolutions Web Login extension:

1. Click on Devolutions Web Login \* extension at the top right corner of your browser.



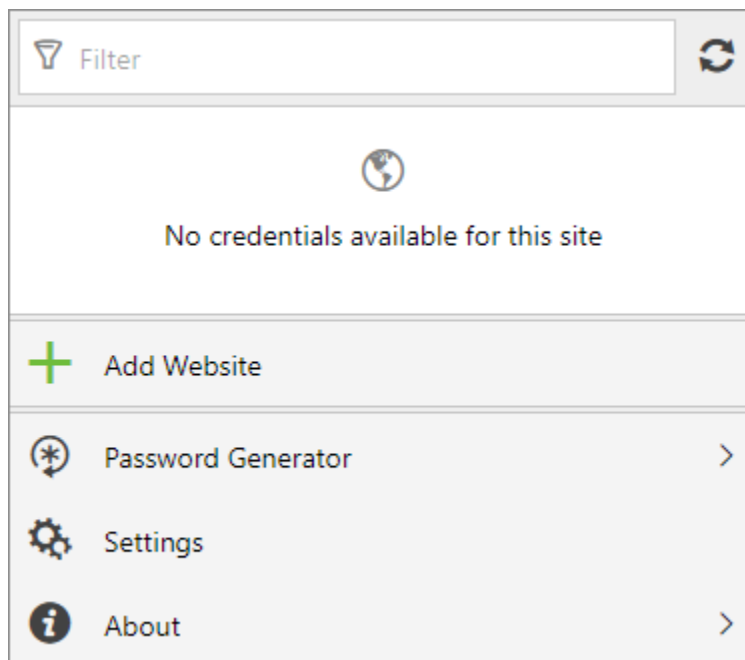
Remote Desktop Manager must be installed and running to continue.

2. Choose **Remote Desktop Manager** in the list and **Save**. You could at this point import settings; the option will also be available in the [Settings](#) menu after the log in.



*First Login*

You will be automatically connected to your vaults.



*Devolutions Web Login Connected*

## 7.4 Exploring Devolutions Web Login

### 7.4.1 Menu

#### DESCRIPTION

The user interface **Devolutions Web Login** is slightly different in appearance when connected to Remote Desktop Manager, Devolutions Password Server or Devolutions Password Hub.

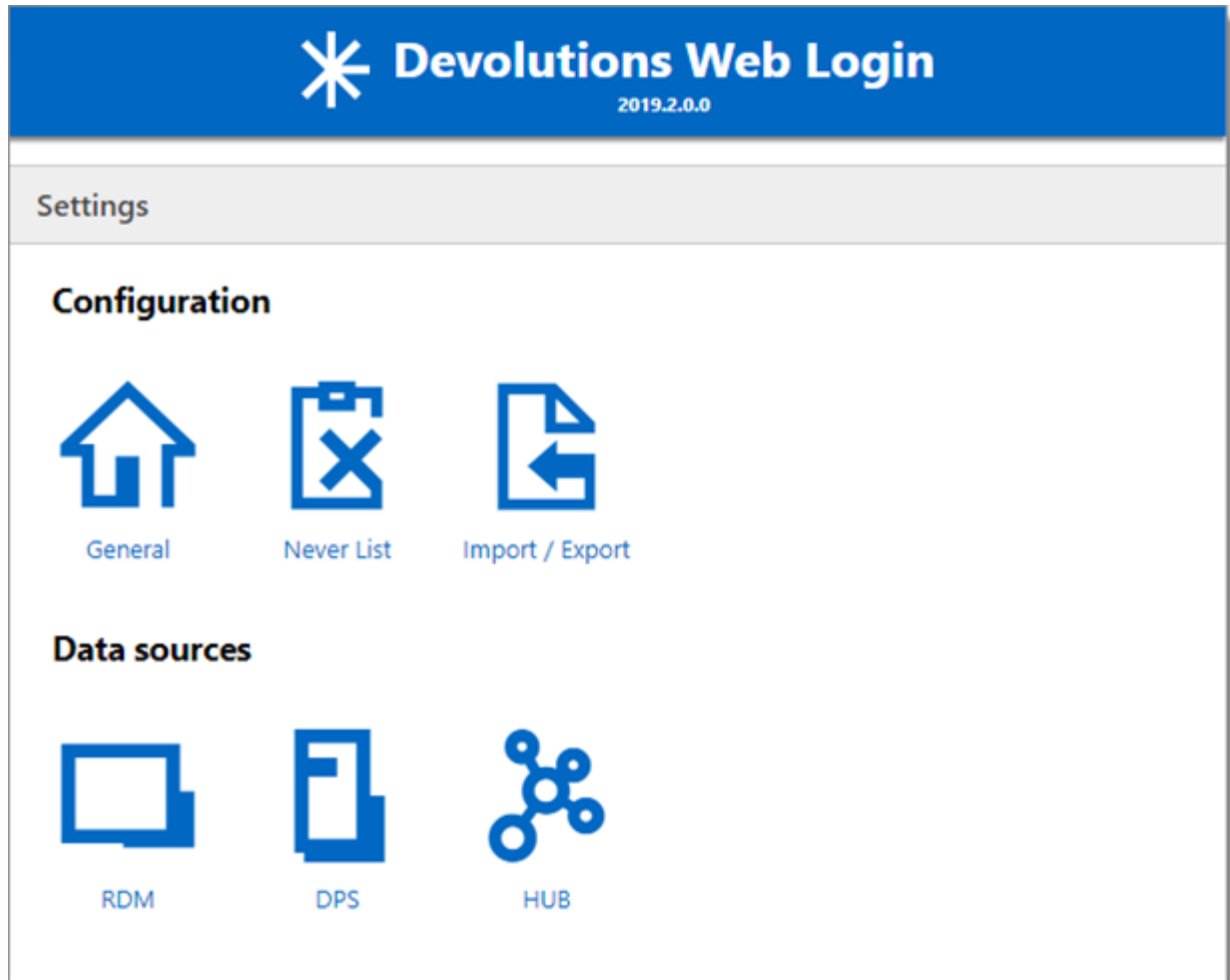
See below a list of the menu and information available from the Devolutions Web Login extension:

- Refine the credential list available with the **search**.
- **Add a website** from Devolutions Web Login in a specific folder located in a vault or your private vault.
- **Visualize the credential** stored in the vaults if you are connected with Devolutions Password Server or Devolutions Password Hub.
- Browse **recently used entry** or **favorites**.
- Use the **password generator** to create custom and more secure credentials.
- Set Devolutions Web Login [settings](#).

#### 7.4.1.1 Settings

#### DESCRIPTION

Devolutions Web Login settings are separated in two categories, [Configuration](#) and [Data sources](#).



*Devolutions Web Login Settings*

## CONFIGURATION

The **General** settings are about the user interface and interaction.

- Show Devolutions Web Login extension icon in the credentials fields.
- Show the prompt when saving credentials on new login.
- Color the fields that are filled with Devolutions Web Login
- Disable the analytics in the advanced setting.

The **Never list** displays the list of websites, added locally, to which the user will never be prompted to save credentials.

- Type can range from: Never add site, Never autofill, Never do anything too Never show icons in field.
- Matching options are: Base domains, Host, Starts with, RegEx and Exact.

To remove a website from the never list click the **trash can** icon next to it. To edit an entry, delete it and create another.

The **Import / Export** setting allows to save and transfer your currently set preferred settings.

- Import setting from other browsers or users.
- Choose to export Devolutions Web Login settings, password generator template and the never list.

## DATA SOURCES

The data sources settings are used to customize Devolutions Web Login interactions with [Remote Desktop Manager](#), [Devolutions Password Server](#) and [Devolutions Password Hub](#).

## REMOTE DESKTOP MANAGER

GENERAL OPTIONS	DESCRIPTION
<b>Enable Remote Desktop Manager app</b>	Retrieve entries from Remote Desktop Manager when the application is open.
<b>Use default port (19443)</b>	Communicate with the default port 19443 between the application.
<b>Add entry in private vault by default</b>	Save new entries in the private vault.
<b>Destination folder</b>	Choose the folder where the credentials are stored in the vault.



ACTION OPTIONS	DESCRIPTION
<b>Automatically retrieve credentials on page load</b>	<p>Devolutions Web Login automatically search for credentials in the data source when connecting to a website.</p> <p>If disabled, click on the Devolutions Web Login extension icon to manually retrieve credentials.</p>
<b>Automatically fill in credentials on load</b>	Fill automatically the credentials when loading a web page.
<b>Automatically submit the form after filling</b>	Submit the credentials automatically when the fields are filled.
ADVANCED OPTIONS	DESCRIPTION
<b>Application key</b>	<p>Secure the port with an application key by using the same code in Remote Desktop Manager and Devolutions Web Login.</p> <p>Navigate to <b>File – Options – Browser Extensions</b> in Remote Desktop Manager to set the application key.</p>
<b>Enable native messaging</b>	Exchange messages with a native application installed on the user's computer.
<b>Use legacy API</b>	Use the old browser extension API for compatibility with older versions of Remote Desktop Manager.

## DEVOLUTIONS PASSWORD SERVER

GENERAL OPTIONS	DESCRIPTION
<b>Enable Devolutions Password Server</b>	Retrieve entries from Devolutions Password Server.

GENERAL OPTIONS	DESCRIPTION
<b>Destination folder</b>	Choose the folder where the credentials are stored in the vault.
<b>Server URL</b>	Enter the URL of the Devolutions Password Server instance to connect to.
ACTION OPTIONS	DESCRIPTION
<b>Automatically retrieve credentials on page load</b>	<p>Devolutions Web Login automatically search for credentials in the data source when connecting to a website.</p> <p>If disabled, click on the Devolutions Web Login extension icon to manually retrieve credentials.</p>
<b>Automatically fill in credentials on load</b>	Fill automatically the credentials when loading a web page.
<b>Automatically submit the form after filling</b>	Submit the credentials automatically when the fields are filled.

## DEVOLUTIONS PASSWORD HUB

GENERAL OPTIONS	DESCRIPTION
<b>Enable Devolutions Password Hub</b>	Retrieve entries from Devolutions Password Hub.
<b>Server URL</b>	Enter the URL of the Devolutions Password Hub instance to connect to.
ACTION OPTIONS	DESCRIPTION
<b>Automatically fill in credentials on load</b>	Fill automatically the credentials when loading a web page.

ACTION OPTIONS	DESCRIPTION
Automatically submit the form after filling	Submit the credentials automatically when the fields are filled
ADVANCED OPTIONS	DESCRIPTION
Devolutions Account login	Set your Devolutions Account login URL.
Show favicon	Display the Devolutions Web Login favicon.

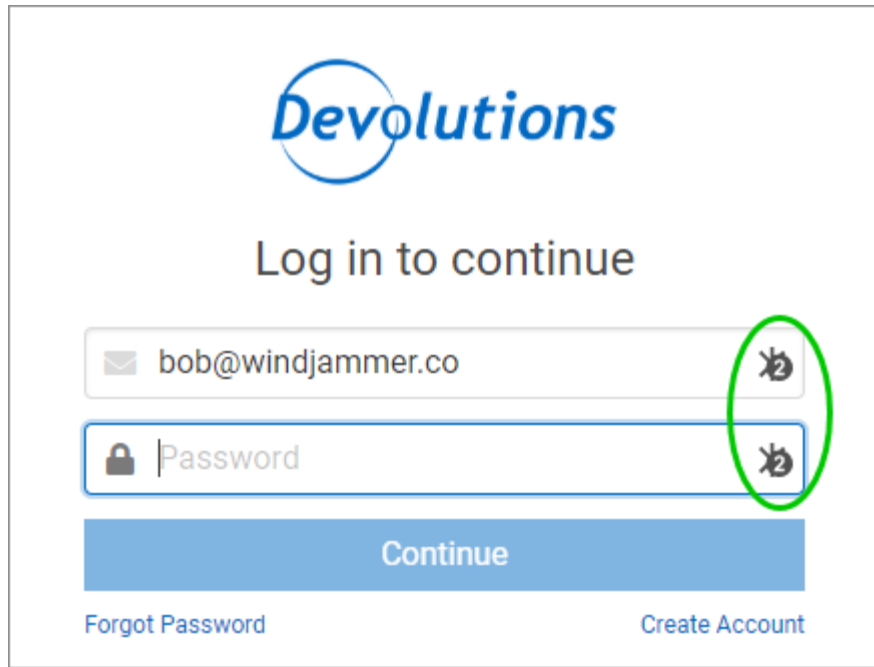
## 7.4.2 Retrieve Credentials

### DESCRIPTION

Once configured in your Devolutions product, credentials are automatically detected by **Devolutions Web Login** when connected to their respective applications.

### LOG IN TO A WEBSITE

Select an entry from the list in Devolutions Web Login or click on the icon in the credential field to fill in the login information and connect to the website.

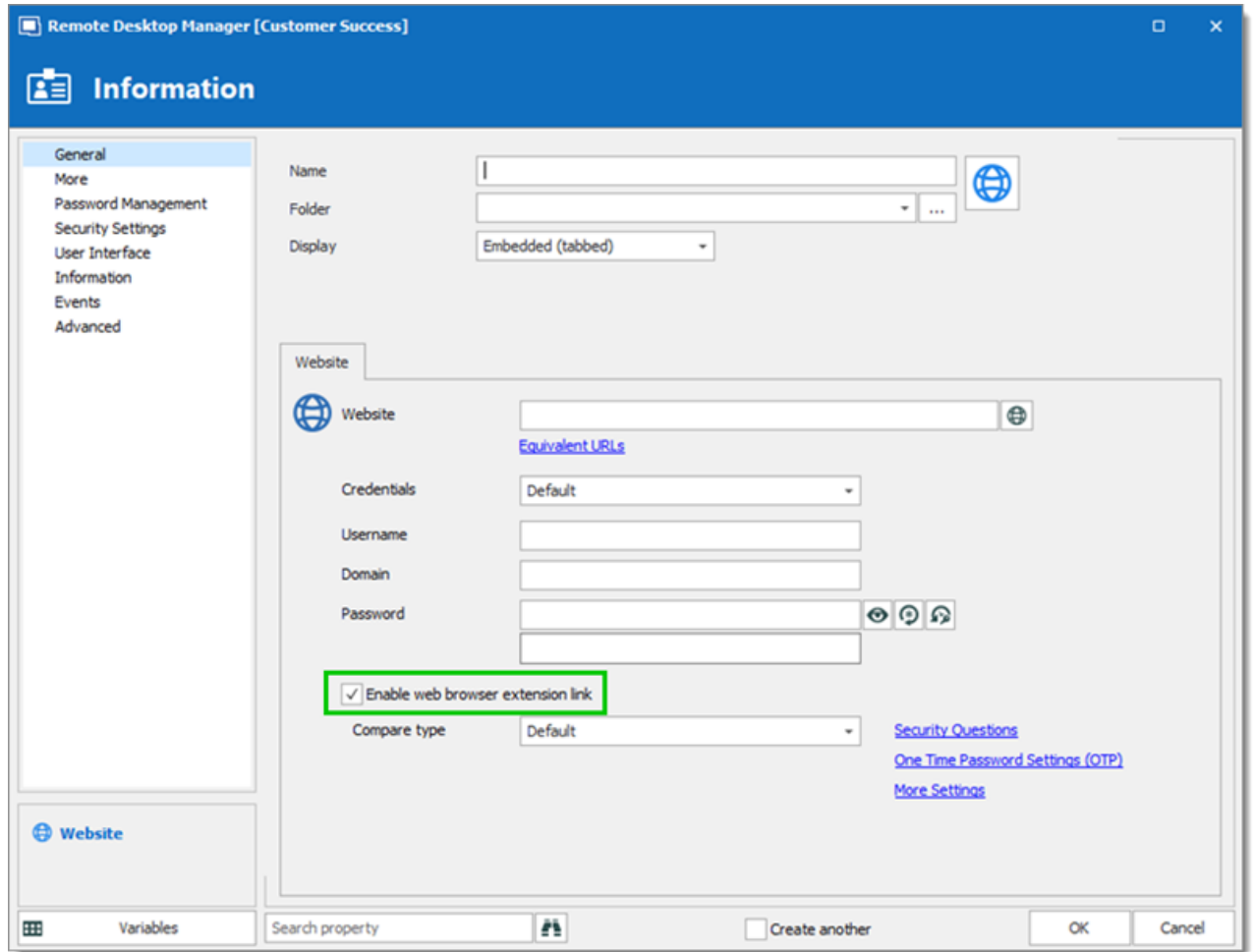


*Automatic Log In*

#### 7.4.2.1 Remote Desktop Manager

### DESCRIPTION

Checkmark **Enable web browser extension link** in Remote Desktop Manager entries to allow Devolutions Web Login extension to retrieve the credentials when connecting to its respective website.



*Enable web browser extension link*

### 7.4.3 Secure Devolutions Web Login

#### DESCRIPTION

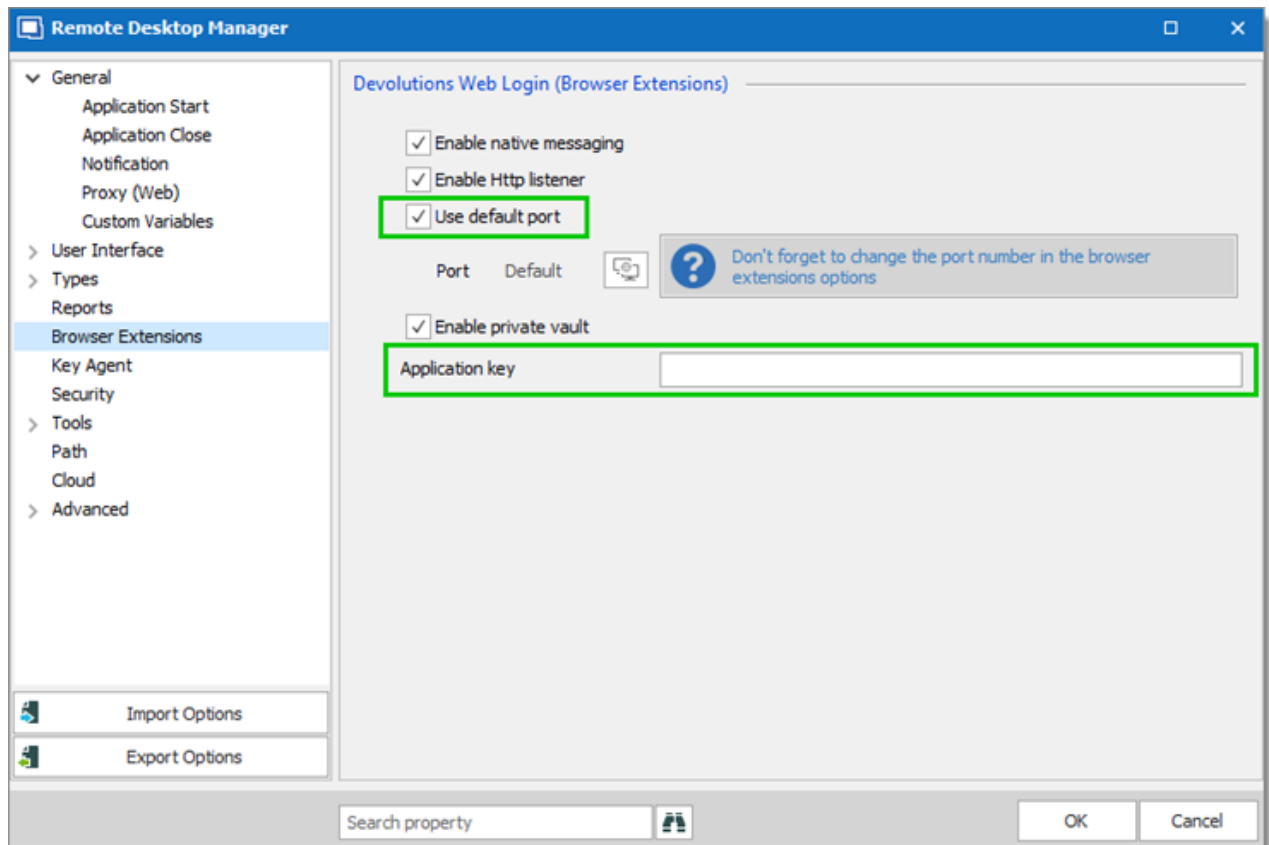
As mentioned in the Devolutions Web Login [Overview](#) topic, installing the extension in a Terminal Services environment can introduce security risks. In such environments, each user must have a distinct port assigned, as well as an application key to prevent any other Devolutions Web Login from listening in.



The application key is displayed in clear text, it must be kept secret by the user.

To enable the security layer in Remote Desktop Manager, follow these steps:

1. Navigate to **File – Options – Browser Extensions**.
2. Uncheck **Use default port**.
3. Enter a custom port.
4. Type an **Application key** then click **OK**



*Remote Desktop Manager Browser Extensions Options*

5. In your browser, click the Devolutions Web Login icon \* and go to Remote Desktop Manager Settings.
6. Disable **Use default port**.
7. Enter the custom port created earlier in Remote Desktop Manager.
8. Enter the same **Application key** as Remote Desktop Manager .

Devolutions Web Login  
2019.2.2.8

Settings > RDM

**General**

☒ Enable Remote Desktop Manager app

☐ Use default port (19443)

Port  
19443

☒ Add entry in private vault by default

Destination folder  
Devolutions Products

**Actions**

☒ Automatically retrieve credentials on page load

☒ Automatically fill in credentials on load

☐ Automatically submit the form after filling

**Advanced**

Application key

☐ Enable native messaging

☐ Use legacy API

*Devolutions Web Login Settings for Remote Desktop Manager*

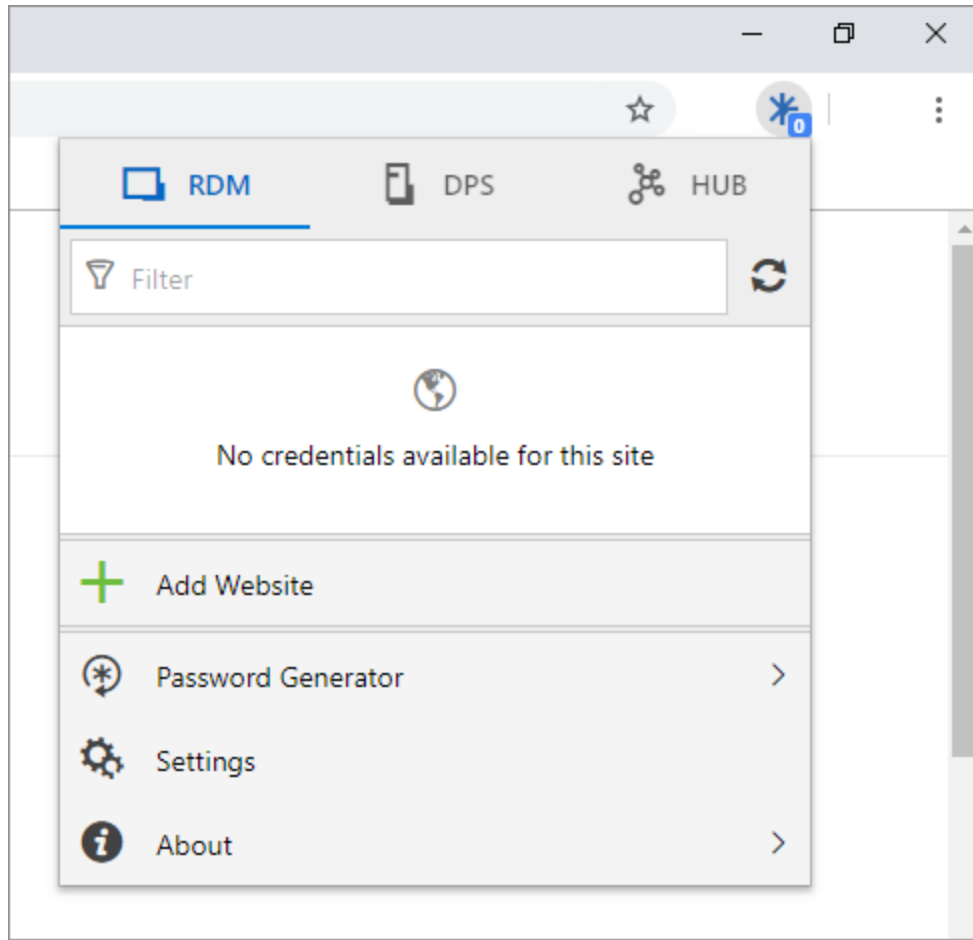
## 7.4.4 Keyboard Shortcuts

### DESCRIPTION

Here is the list of keyboard shortcuts available for Devolutions Web Login:

### CTRL+SHIFT+Z

Use this key shortcut to open Devolutions Web Login window in your active browser.

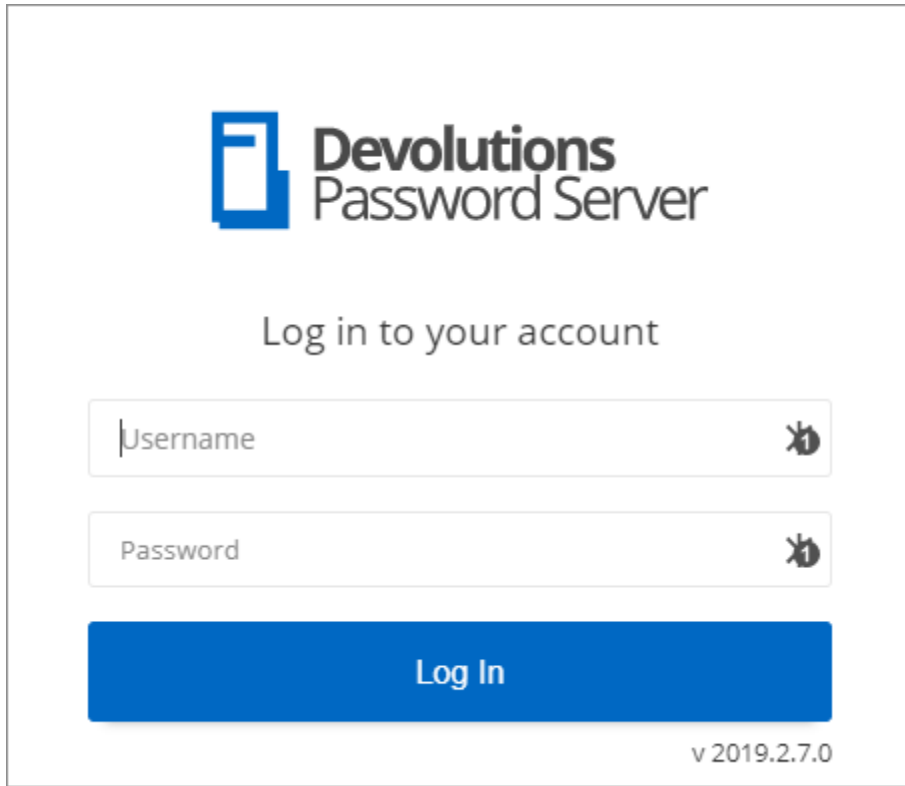


*Devolutions Web Login in Chrome*

## **CTRL+SHIFT+Y**

Use it to auto-fill your credential when only one is available for an entry.





The screenshot shows the Devolutions Password Server login interface. At the top left is the Devolutions logo, a blue square with a white stylized 'D'. To its right is the text 'Devolutions Password Server' in a bold, sans-serif font. Below the logo and title is the instruction 'Log in to your account'. There are two input fields: the first is labeled 'Username' and the second is labeled 'Password'. Both fields have a small icon on the right side, which appears to be a key or a similar symbol. Below the input fields is a large blue button with the text 'Log In' in white. In the bottom right corner of the login area, the version number 'v 2019.2.7.0' is displayed.

*One Credential Login with Devolutions Web Login*

# Role Based Access Control

---

Part VIII

## 8 Role Based Access Control

### DESCRIPTION

Remote Desktop Manager role-based access control allows to create a granular protection system that is quite flexible. However, flexibility comes at a price and sometimes making the wrong choices could increase the time involved in managing the system.

The following recommendations are based on our experience with the system and the ideas shared by our community. Follow these guidelines, as they will help you to use the role-based access control efficiently.

Here are the main key points of the role based access system:

- Security is inherited: child items and folders are covered by a parent folder's security.
- Permissions can be overridden: a permission set on a sub folder will override the parent item's permission.
- Permissions are granular: Multiple permissions can be set on entries at once.

### ENHANCE THE SECURITY

While the role based access control is a great feature to secure access to entries, many other features can be used to add more security layers. For more information, please consult the following topics:

- [Security Provider](#)
- Credential repository
- [Password Templates](#)
- [Two-factor authentication](#)
- One-time password

### SCENARIOS

Because of the great flexibility of our system, it becomes difficult to describe how to achieve the exact security system that matches your needs. For this reason, we have elected to describe the most popular systems that we have seen in use in our current community of users. We hope that one of them will closely match your needs. You can obviously mix and match the various strategies used in our scenarios to achieve your requirements.

Please consult the following:

- [Simplified security](#)
- [Advanced security](#)

## ROLE CONFIGURATION

When using the role-based access control, roles are mostly used to control user access for multiple users at once.

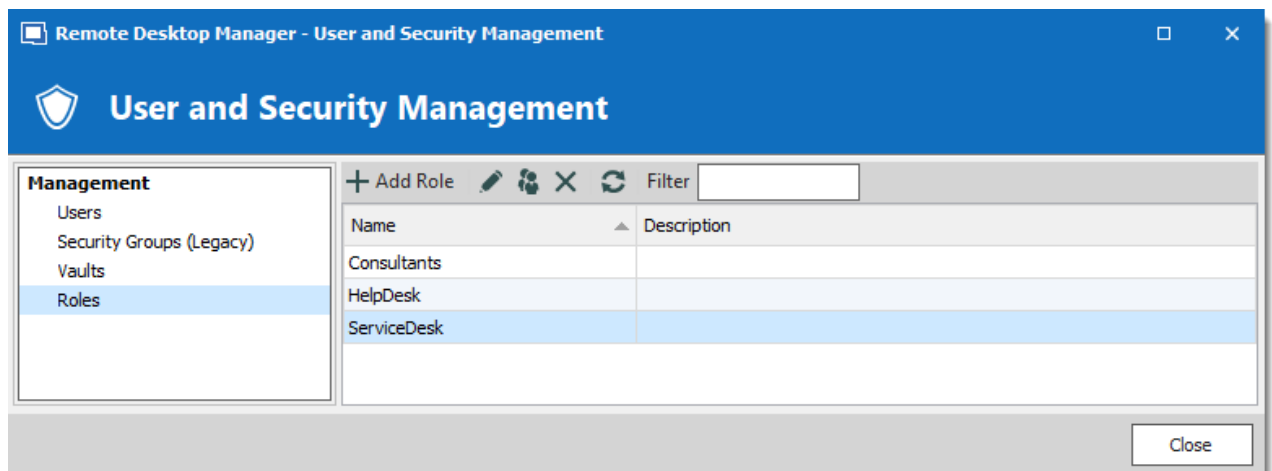
### Common roles can be:

- Service Desk: a single point of contact to handle incidents, problems and questions from staff and customers. Provide an interface for activities such as change requests, software licences, configuration management, and more.
- Help Desk: manage, co-ordinate and resolve support requests.
- Consultants: employed externally on a temporary basis, they usually are read-only users and can use only a subset of entries.

To be more specific, we will use these team names in our scenarios.

## CREATE THE ROLE

To create roles, navigate to **Administration – Roles**, then click **+ Add Role**.



*Create a Role*

All settings can be left to default unless the role contains only administrators. In this case, check the **Administrator** box when configuring the role. Enter a **Name** for the role, then click **Ok**.

**Remote Desktop Manager - Role Management**

**Role Management**

General

Privileges

Security Groups (Legacy)

Vaults

Users

General

ID: 3FC1998F-0A9F-411D-80CB-6064AD1884FD

Name: Service Desk

Description:

☐ Administrator

OK Cancel

*Configure a Role*

To assign users to the role, click , then check the **Is Member** box of the respective user.

**Remote Desktop Manager - Role Assignment**

**Role Assignment**

Name: ServiceDesk

Users

Name	Description	Administrator	Is Member
sa	hehesa	✓	<input type="checkbox"/>
Test			<input type="checkbox"/>
Testadmin		✓	<input type="checkbox"/>
UDelOnly			<input type="checkbox"/>
URead			<input type="checkbox"/>
UReadOnly			<input type="checkbox"/>
Ureg			<input type="checkbox"/>
URes6			<input type="checkbox"/>

Select All

Unselect All

Save Cancel

*Assign a user to the Role*

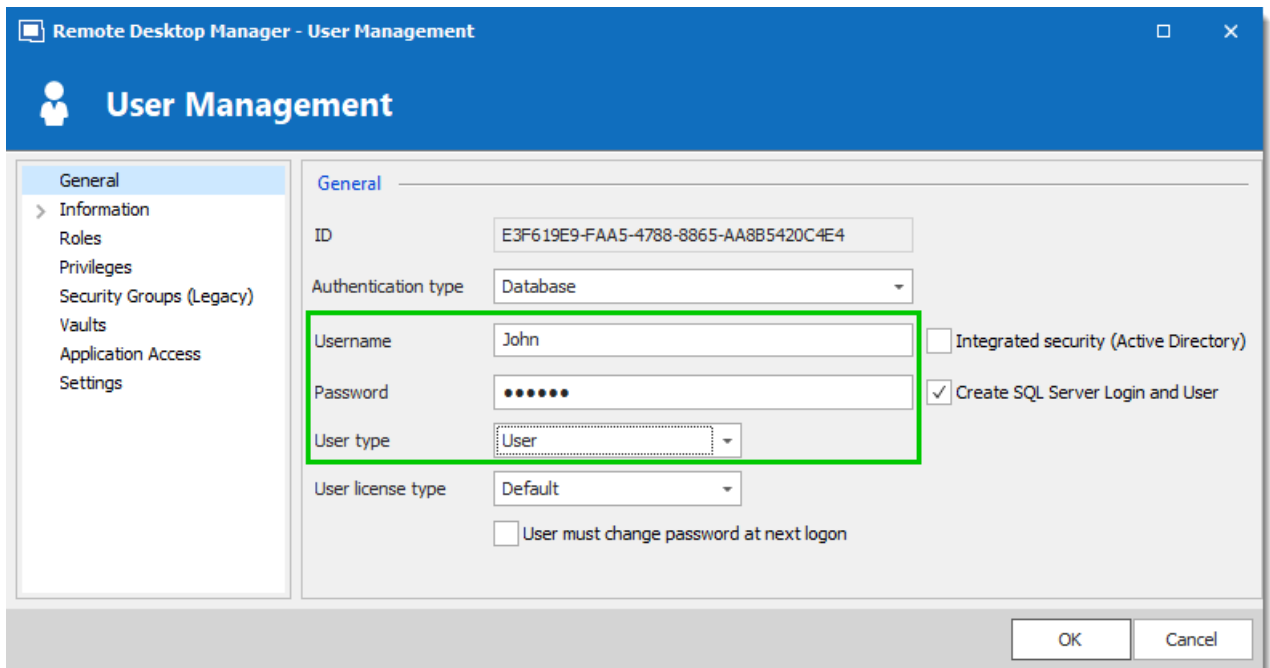
## USER CONFIGURATION

## USER TEMPLATE

It is possible to change the default user template. To do so, navigate to **File – Options – Security – User Template**. These settings control the default settings of a new user. The best practice is to disable all privileges.

## CREATE THE USER

To create users, navigate to **Administration – Users**, then click **+ Add User**. Enter a **Login** and **Password** for the user and select the **User type**.



Remote Desktop Manager - User Management

**User Management**

General

Information  
Roles  
Privileges  
Security Groups (Legacy)  
Vaults  
Application Access  
Settings

General

ID: E3F619E9-FAA5-4788-8865-AA8B5420C4E4

Authentication type: Database

Username: John

Password: •••••

User type: User

User license type: Default

☐ Integrated security (Active Directory)

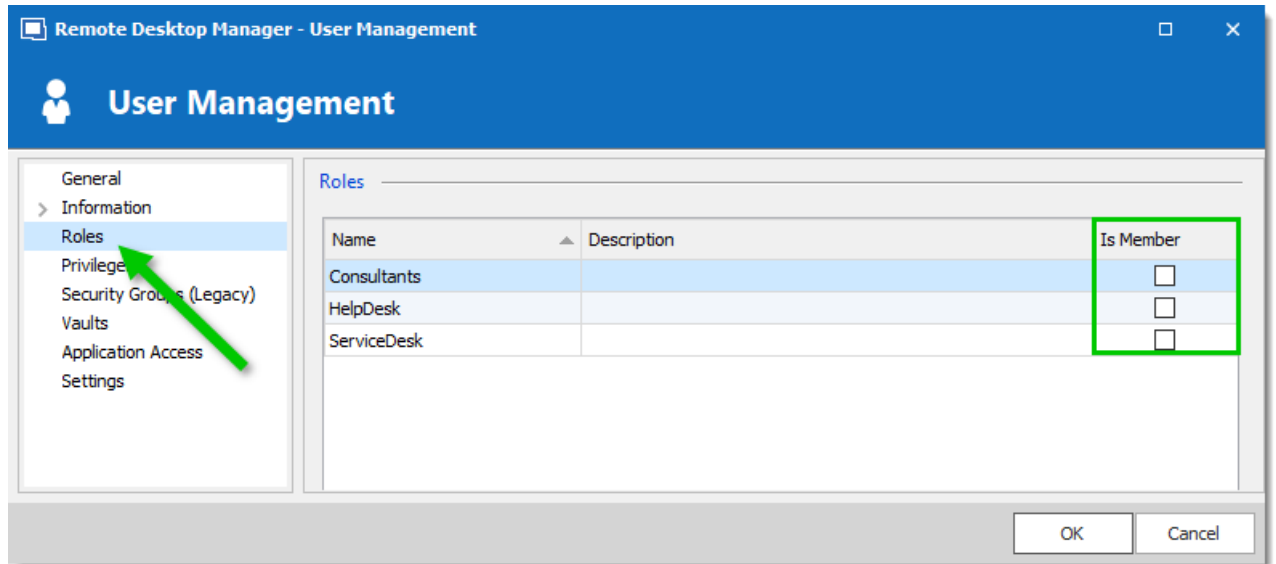
☒ Create SQL Server Login and User

☐ User must change password at next logon

OK Cancel

*Create a user*

A user can be assigned to multiple roles at once by checking the **Is Member** box of the respective roles in the **Roles** section of the **User Management**.



*Assign a user to a Role*

## ADMINISTRATORS

**Administrators** can do everything, regardless of the security. These users are usually the chief officers and senior management.

## RESTRICTED USERS

**Restricted users** have limited access to resources. They usually have the **Add** and **Edit** rights only. These users can be mid or first level executives, such as service desk and help desk.

## USERS

**Users** also have limited access to resources much like Restricted users. However, Users have by default the **Add**, **Edit** and **Delete** rights and can perform these actions on all unsecured entries.

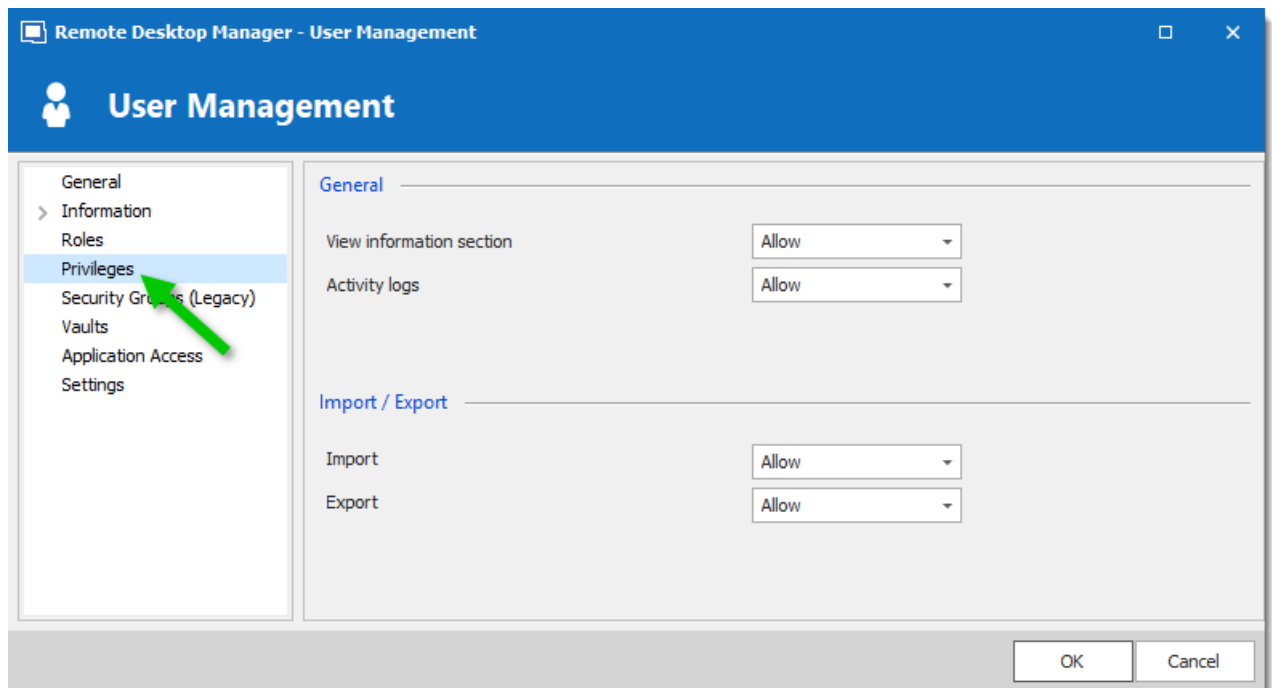
## READ ONLY USERS

**Read only users** can only view and use resources, but cannot edit them. These users are usually external consultants.

## SELECT THE APPROPRIATE USER TYPE

When creating users, some key points must be taken into consideration. Ask yourself the following questions while configuring a new user:

- Should they be able to access any resource without restriction? These are your **Administrators**.
- Should they be able to add, edit, or delete entries? A **User** would have all of these. Alternatively, you can select specific rights with **Restricted User**.
- Should they be able to see sensitive information, or import and export entries? **Read-Only** users are best used for those who should have very limited access. You can also use the privilege tab for additional control over users.



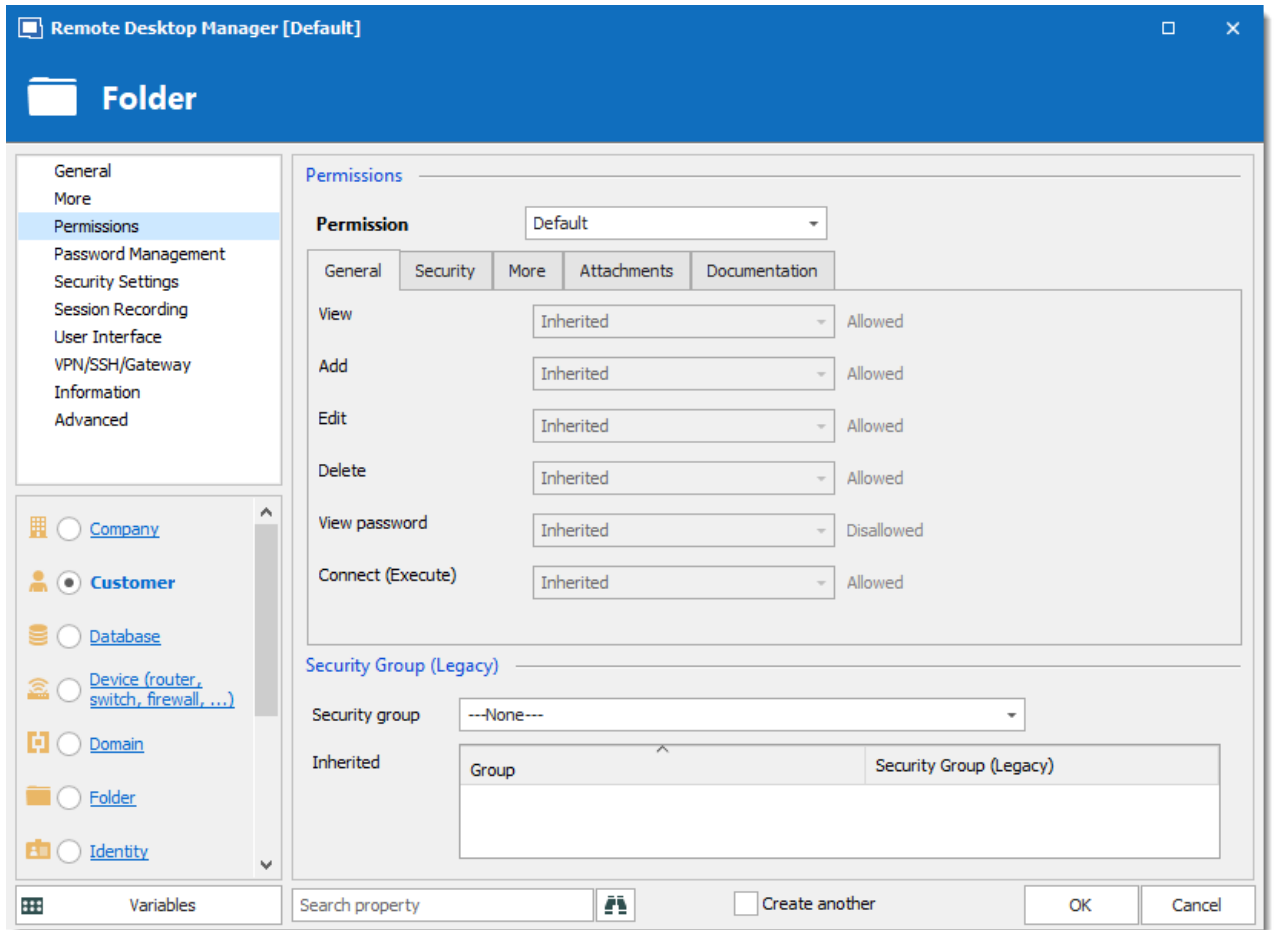
*User Management - Privileges*

## ENTRY CONFIGURATION

Access is granted or denied to users by setting permission on entries. Permissions can be set to users or roles. The best practice is to grant permissions to roles to control access for multiple users at once.

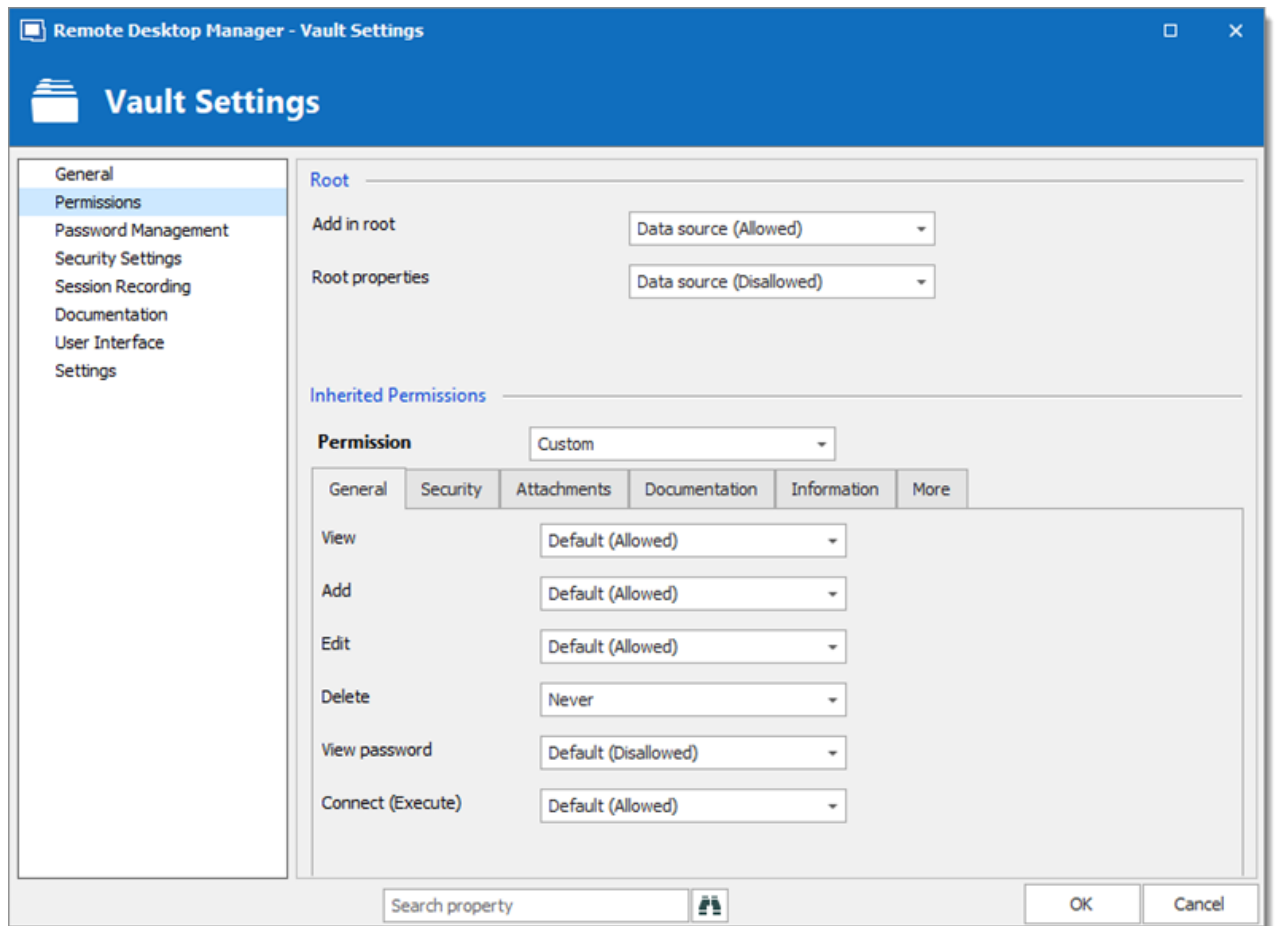
To set permissions on an entry, edit any entry, then navigate to the **Permissions** section.





*Entry's permissions*

Permissions are usually set on folders, and apply to all child entries. A best practice is to set all the permissions of the vault root folder to **Never**. As a result, all permissions of all entries are denied by default.

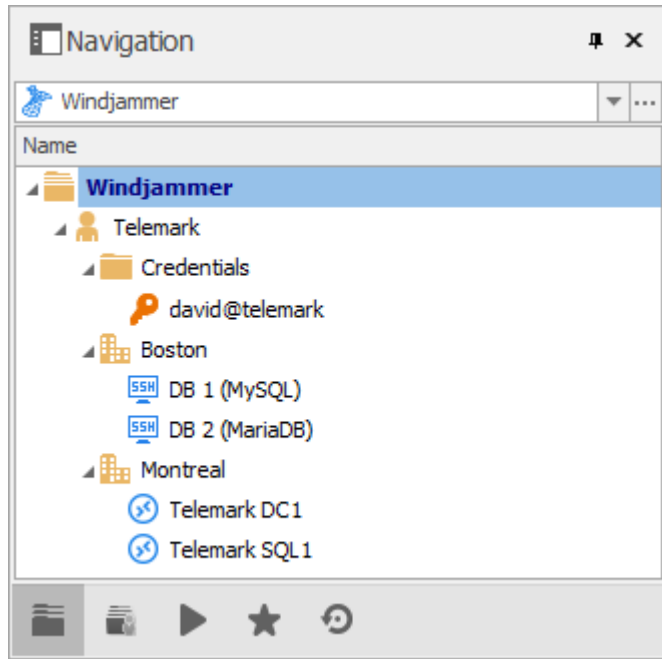


*Vault Root permissions*

Access is denied to users by expressly granting the access to other users. In other words, all users that are not on the list of a permission have the access denied.

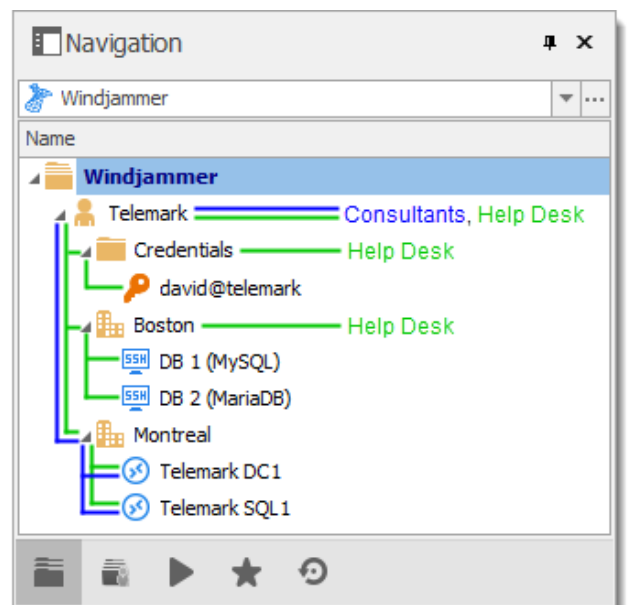
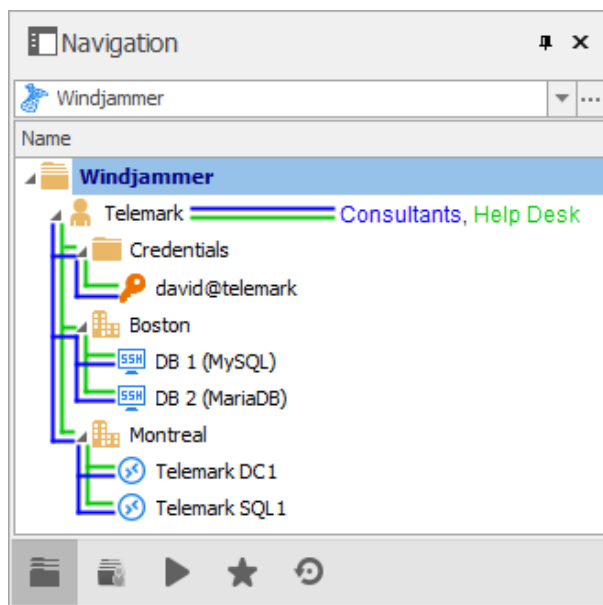
For a user to have access to a sub folder, the user must have at least the view permission on all parent folders.

Consider the following structure:



There are three levels of folders: the vault root, Telemark, and child items of Telemark.

Suppose that a user, such as a consultant, must have access to the Montreal folder only. The consultant must be granted the view permission on the Telemark folder as well. However, granting the view access to the Telemark folder gives to the consultant the permissions to view all child items of Telemark. To deny the view permissions for the consultant on specific child items, the view permissions of these items must be expressly set for other users.



## 8.1 Permissions

### DESCRIPTION

The Permissions window which is only available in an [Advanced Data Source](#), can be found in every entry properties in the **Permissions** section.



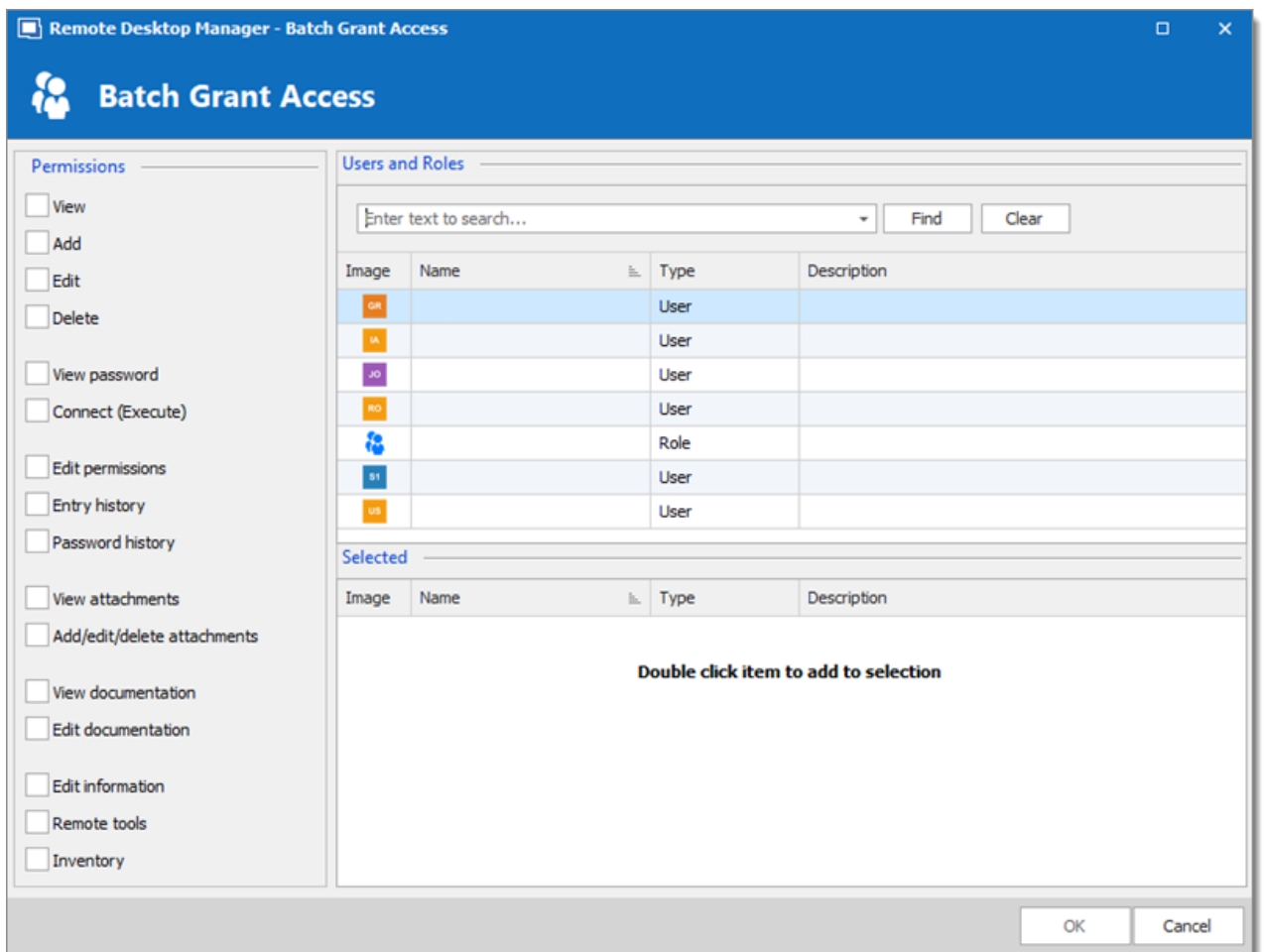
The [Role Based Access Control](#) feature is not available using an [Devolutions Online Database](#).

The role-based permissions system can give a very accurate control of the security. Here is an overview of the permissions window:

*Permissions panel*

OPTION	DESCRIPTION
<b>Permission</b>	<p>Sets the permission mode. Select between:</p> <ul style="list-style-type: none"> <li>• <b>Inherited (Default)</b>: will inherit the permissions from the parent groups.</li> <li>• <b>Custom</b>: lets you specify a custom value for each of the permission.</li> <li>• <b>Everyone</b>: everyone will be granted all the permissions below.</li> <li>• <b>Never</b>: no one but the administrators will be granted the permission.</li> </ul>

OPTION	DESCRIPTION
<b>Grant Access</b>	Allows batch granting access to a specific entry or entries.
<b>Inherited values</b>	Indicates what is inherited from parent groups.
<b>Select roles or users</b>	Lets you select Users / Roles to be granted the permission. Available only if the permission is set to <b>Custom</b> .



*Batch Grant Access*

For more details on each permission, please consult our Common Settings - Permission topic.

## 8.2 Scenarios

### 8.2.1 Simplified Security

#### DESCRIPTION



This feature is only available when using an [Advanced Data Source](#).



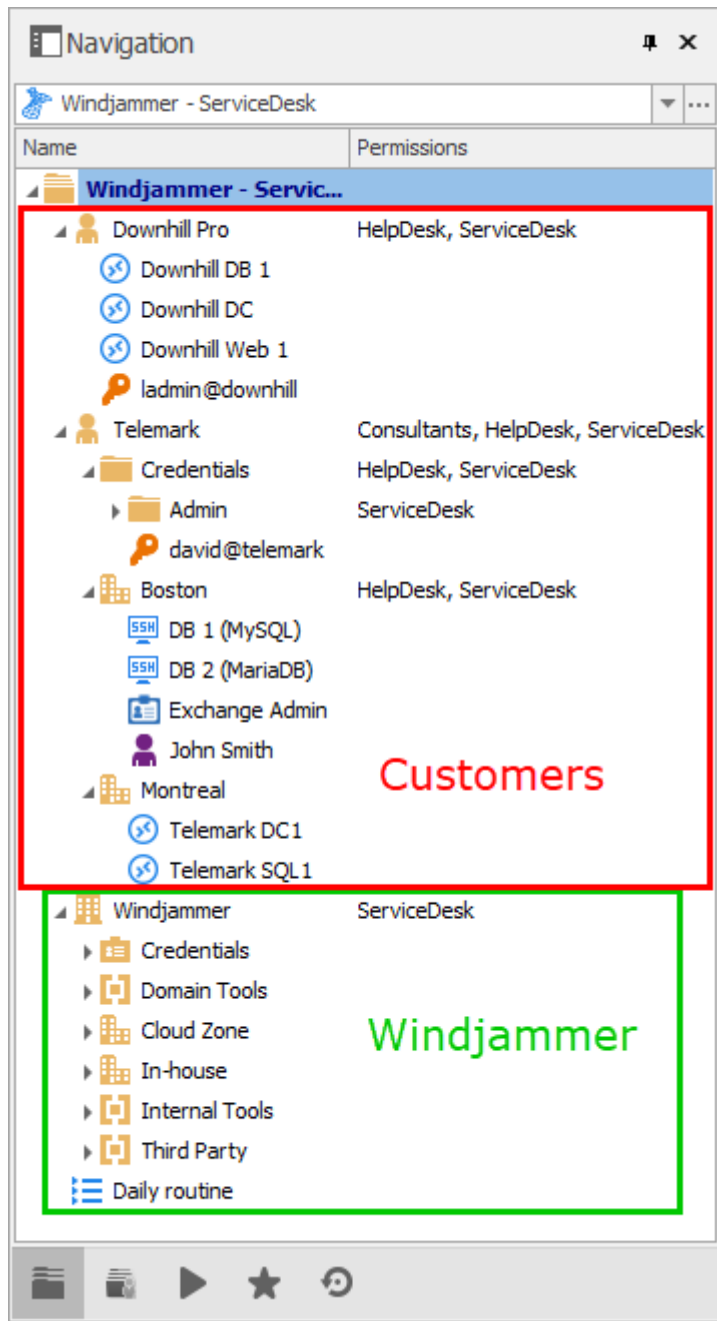
While the following scenario is relevant for small to medium enterprises, it is not recommended for a larger business. For a scenario more suited for large enterprises, please consult the [Advanced Security](#) scenario.



Watch Video

Our fictional company, Windjammer, has four roles: HelpDesk, ServiceDesk, Administrations, and Consultants. There are two client companies: Downhill Pro and Telemark.

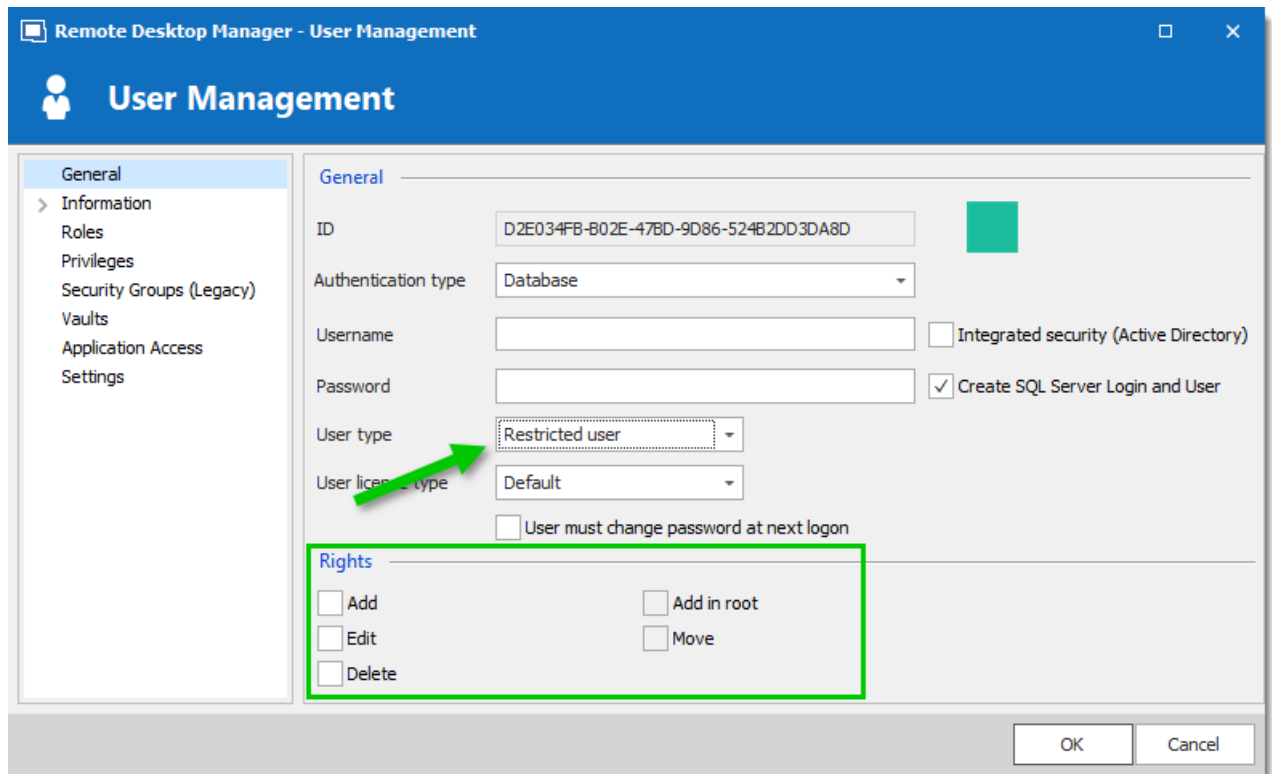
The following tree structure represents entries which users have access to once all permissions are set:



## USER CONFIGURATION

Here is an example for user configuration. To create users, navigate to **Administration – Users – Add User**.

The following rights selection is available when setting a user to **Restricted user**.



Remote Desktop Manager - User Management

## User Management

**General**

Information  
Roles  
Privileges  
Security Groups (Legacy)  
Vaults  
Application Access  
Settings

**General**

ID: D2E034FB-B02E-47BD-9D86-524B2DD3DA8D

Authentication type: Database

Username:

Password:

Integrated security (Active Directory): ☐

Create SQL Server Login and User: ☒

User type: **Restricted user**

User license type: Default

User must change password at next logon: ☐

**Rights**

☐ Add ☐ Add in root

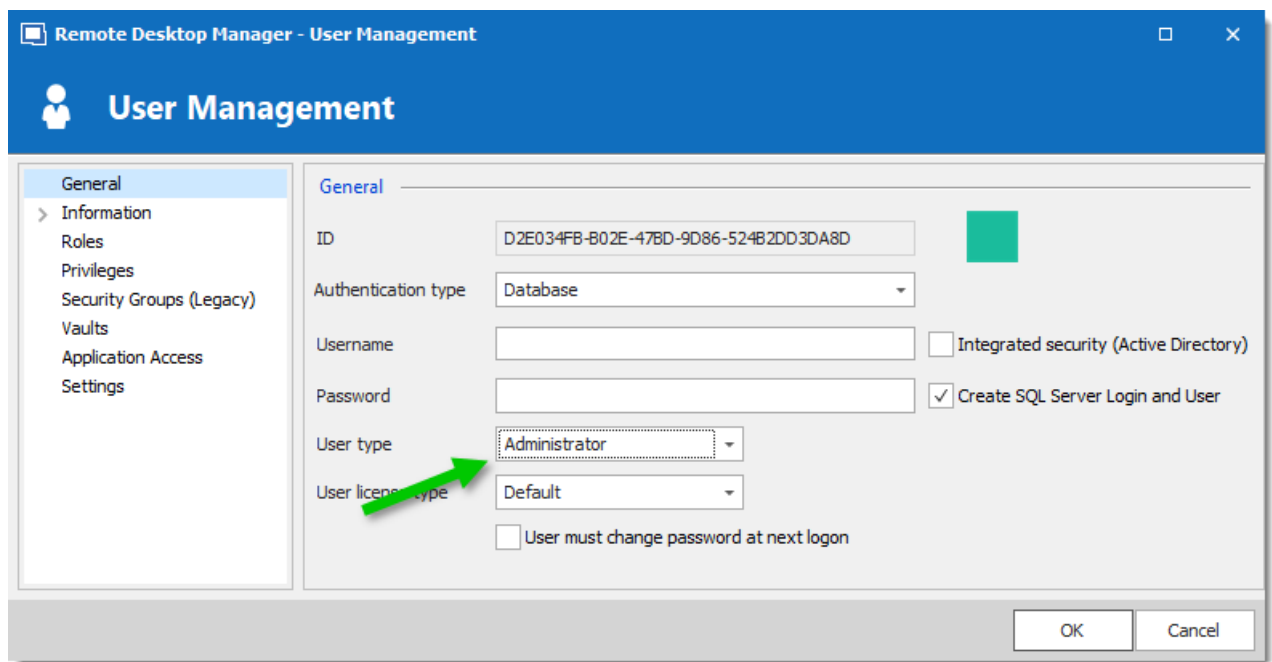
☐ Edit ☐ Move

☐ Delete

OK Cancel

*User Management - Permissions Section*

**Administrators:** administrators have a lot more access than regular users. When creating these users, set the User type to **Administrator** to give them access to everything. The administrator can access all entries, regardless of permissions.



Remote Desktop Manager - User Management

## User Management

**General**

Information  
Roles  
Privileges  
Security Groups (Legacy)  
Vaults  
Application Access  
Settings

**General**

ID: D2E034FB-B02E-47BD-9D86-524B2DD3DA8D

Authentication type: Database

Username:

Password:

Integrated security (Active Directory): ☐

Create SQL Server Login and User: ☒

User type: **Administrator**

User license type: Default

User must change password at next logon: ☐

OK Cancel

*User Management - Administrator*



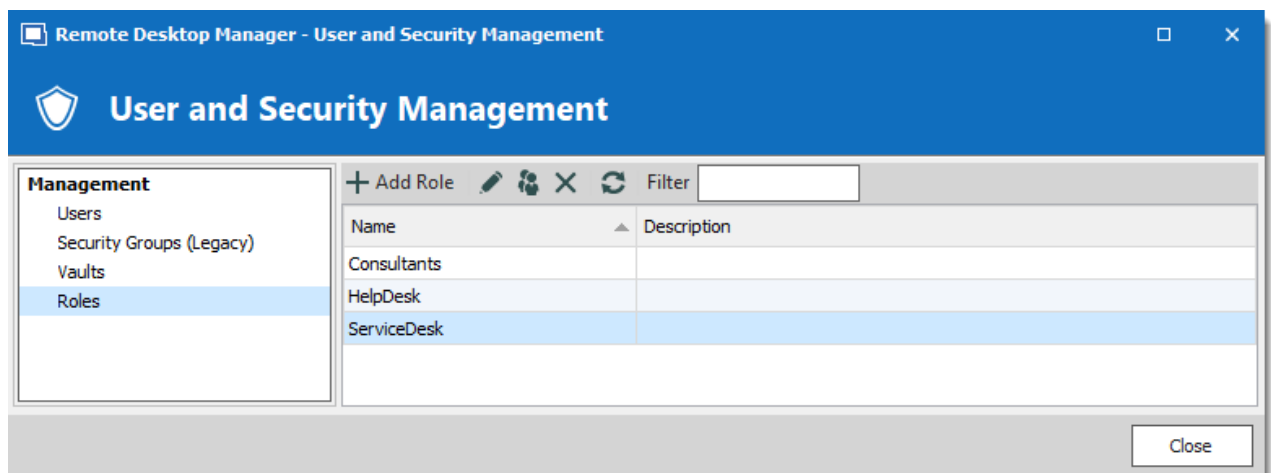
**Regular users (User):** these users have fewer rights than administrators. They essentially have all the basic rights (except for **View Password**) but are susceptible to all denied permissions. Later, we will deny these rights by specifying which users can actually perform these actions.

**Consultants:** consultants can only view a subset of entries, we will set those as **Read-Only**. They cannot add, edit or otherwise affect the information in any way.

## ROLES CONFIGURATION

Now that the users are created, we will add the roles which we will later grant the permissions to. We need to create the roles to assign users to them. There is no need to grant any privileges to these roles.

- ServiceDesk
- HelpDesk
- Consultants



*User and Security Management - Roles*

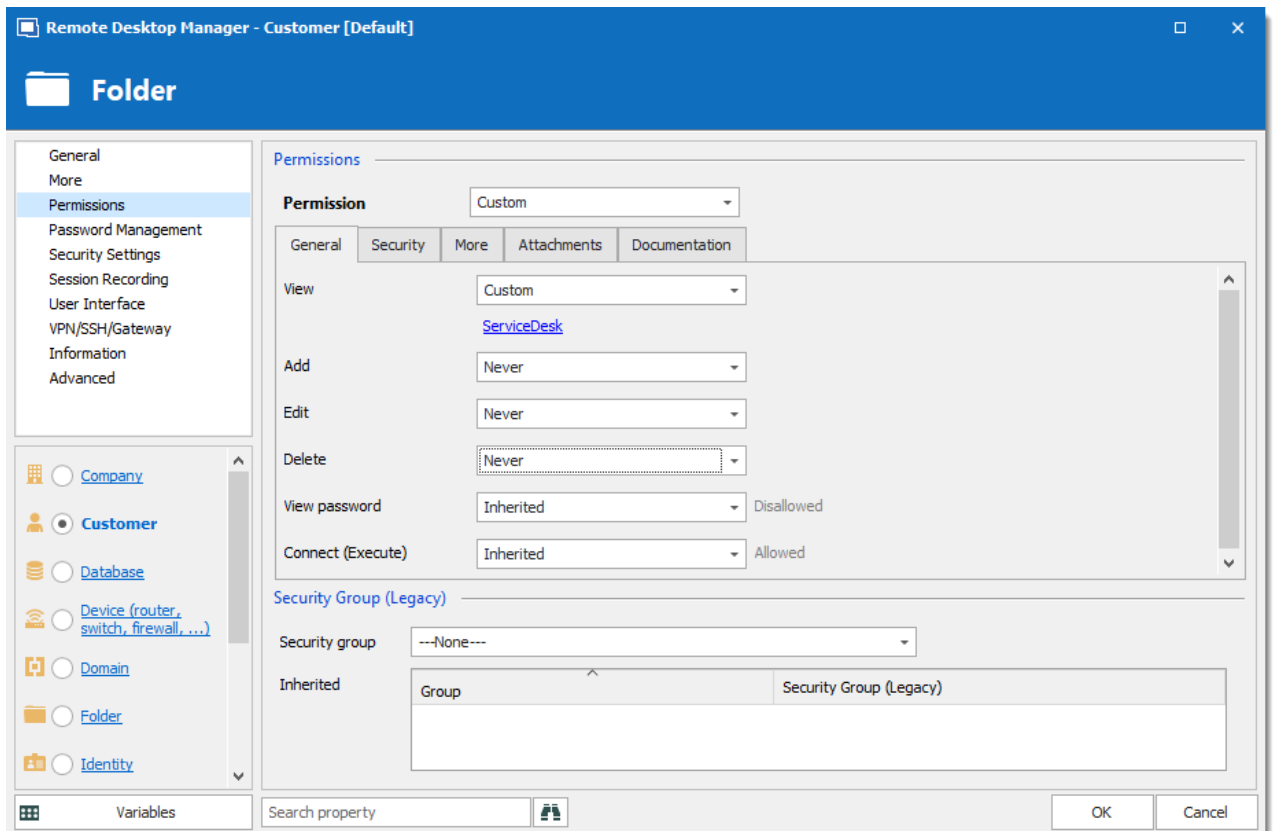
## ENTRIES CONFIGURATION

Now, everything is ready to grant or deny access to the roles.

- The ServiceDesk will have the permission to view and open all entries but will be able to edit only the entries in the customer groups/folders.
- The HelpDesk will have the permission to view and open entries in the customer groups/folders only and will not be able to edit them.
- The Consultants will have the permission to view and open entries in the Montreal folder only but will not be able to edit it nor its child items.

We will begin with the vault root level folders: Downhill Pro, Telemark and Windjammer.

The permission to view the Windjammer folder will be set for the ServiceDesk only since we want them to be able to use its child entries. We don't want the ServiceDesk to add or edit anything. We will set the **Add**, **Edit** and **Delete** permissions to **Never**. Only the administrator will be able to add or edit entries in the Windjammer folder.



*Windjammer - Permissions*

- **View: Custom;** ServiceDesk.
- **Add: Never;** Only the administrator can add entries.
- **Edit: Never;** Only the administrator can edit entries.
- **Delete: Never;** Only the administrator can delete entries.

For Downhill Pro, we will grant permissions to the ServiceDesk and the HelpDesk.

Permissions

Permission: Custom

General Security More Attachments Documentation

View: Custom  
[HelpDesk, ServiceDesk](#)

Add: Custom  
[ServiceDesk](#)

Edit: Custom  
[ServiceDesk](#)

Delete: Never

View password: Inherited Disallowed

*Downhill Pro - Permissions*

- **View: Custom;** HelpDesk, ServiceDesk.
- **Add: Custom;** ServiceDesk.
- **Edit: Custom;** ServiceDesk.
- **Delete: Never;** Only the administrator can delete entries.

We already have a good example of the flexibility of Remote Desktop Manager's Security. A ServiceDesk user can view and use all the entries in the Downhill Pro folder, even the credential entries, but it will never be able to see any password since View Password is Disallowed (from the vault root folder).

Next, for the Telemark folder, we will grant permissions to the ServiceDesk, the HelpDesk and the Consultants. This is where things get complex. If we want the Consultants to be able to view only the Montreal folder which is a child item of Telemark, we must grant to consultants the permission to view the entire Telemark content. Then we will grant permissions on child items only to the role that should have access to these items. This last step will deny the view permission for the consultants on the child items.

**Permissions**

**Permission** Custom

General Security More Attachments Documentation

View Custom  
Consultants, HelpDesk, ServiceDesk

Add Custom  
ServiceDesk

Edit Custom  
ServiceDesk

Delete Never

View password Inherited Disallowed

*Telemark - Permissions*

- **View: Custom;** Consultants, HelpDesk, ServiceDesk.
- **Add: Custom;** ServiceDesk.
- **Edit: Custom;** ServiceDesk.
- **Delete: Never;** Only the administrator can delete entries.

Since we want the users to be able to use the credential entries, we will grant the ServiceDesk and the HelpDesk the permission to view the Credentials folder. This way, the ServiceDesk and HelpDesk will be able to use the entries in the folder without revealing the passwords. Therefore, by specifying that only the HelpDesk and ServiceDesk have the **View** permission, we deny the view access to any role or user that is not in the list of the permission.

The **Add**, **Edit** and **Delete** permissions can be left to **Inherited** since they inherit the settings from the Telemark parent folder. The ServiceDesk is the only role that has been granted the **Add** and **Edit** permission in the parent folder and the **Delete** permission inherits the Never setting.

Permission		Custom
General	Security	More Attachments Documentation
View	Custom	<a href="#">HelpDesk, ServiceDesk</a>
Add	Inherited	ServiceDesk
Edit	Inherited	ServiceDesk
Delete	Inherited	Never
View password	Inherited	Disallowed
Connect (Execute)	Inherited	Allowed

*Telemark\Credentials - Permissions*

- **View: Custom;** HelpDesk, ServiceDesk.
- **Add: Inherited;** ServiceDesk inherited from Telemark folder.
- **Edit: Inherited;** ServiceDesk inherited from Telemark folder.
- **Delete: Inherited;** Never inherited from Telemark folder.

We want the ServiceDesk to be able to use the Domain Admin credential entry as well but not the HelpDesk. For this we must grant the **View** permission to the ServiceDesk. The ServiceDesk will still be able to edit the credential entry but will never see the password. The delete permission is set to **Never**.

Permission		Custom
General	Security	More Attachments Documentation
View	Custom	<a href="#">HelpDesk, ServiceDesk</a>
Add	Inherited	ServiceDesk
Edit	Inherited	ServiceDesk
Delete	Never	
View password	Inherited	Disallowed
Connect (Execute)	Inherited	Allowed

The last step for the Telemark child items is to set the **View** permission to the ServiceDesk and the HelpDesk on the Boston folder and leave every other permission of this folder to **Default**.

This denies the Consultants to view the Boston folder. Now, the Consultants will be able to view and open entries only in the Montreal folder.

Permission		Custom
General	Security	More Attachments Documentation
View	Custom	<a href="#">HelpDesk, ServiceDesk</a>
Add	Inherited	ServiceDesk
Edit	Inherited	ServiceDesk
Delete	Never	
View password	Inherited	Disallowed
Connect (Execute)	Inherited	Allowed

*Telemark\Boston - Permissions*



Every time a new folder is added, the **View** permission must be set for ServiceDesk and HelpDesk to hide the new folder and its content from the Consultants.

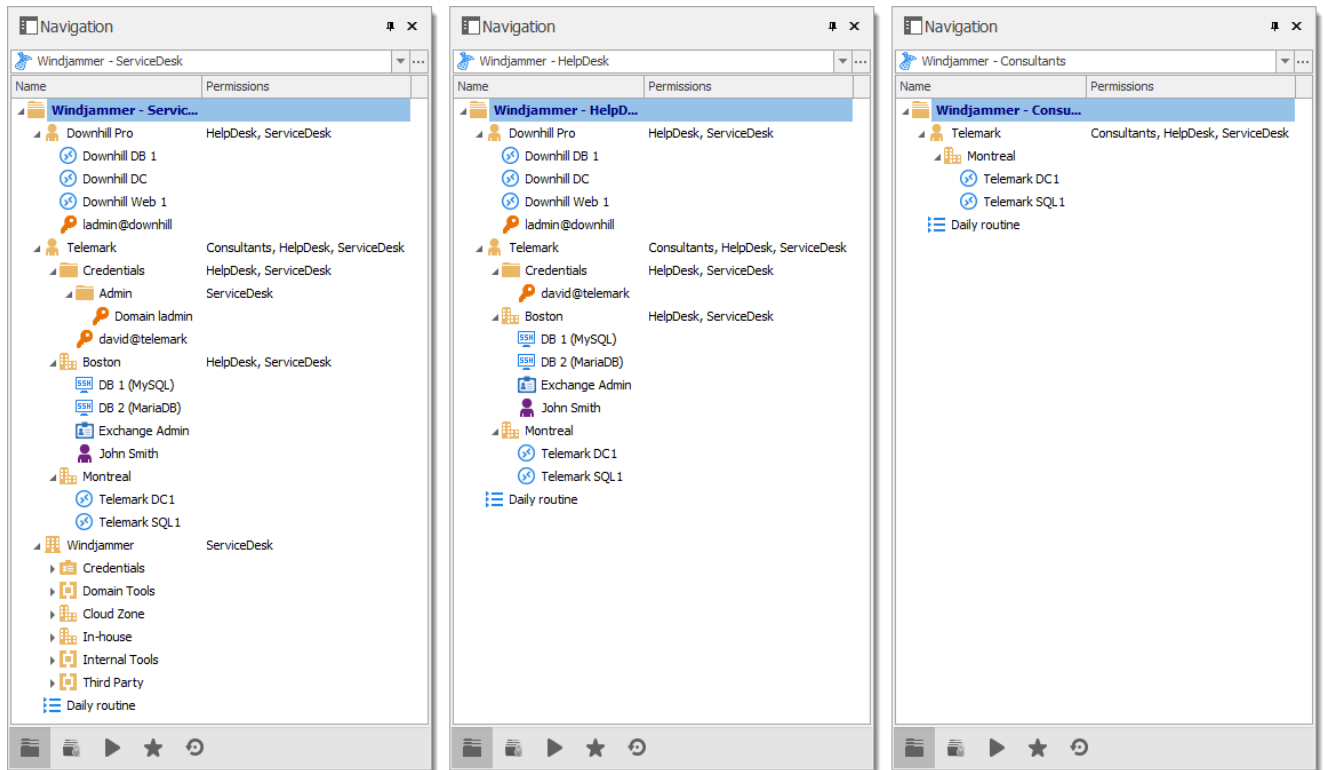
No need to set any permissions on the Montreal folder, since they are inherited from the parent folders.

Permission		Default
General	Security	More Attachments Documentation
View	Inherited	<a href="#">Consultants, HelpDesk, ServiceDesk</a>
Add	Inherited	ServiceDesk
Edit	Inherited	ServiceDesk
Delete	Inherited	Never
View password	Inherited	Disallowed
Connect (Execute)	Inherited	Allowed

*Telemark\Montreal - Permissions*

## IN CONCLUSION

The permissions are now correctly set. Note that every entry added at vault root level will have no security by default. This means they would be available for anyone, even the consultants. This can be confirmed by looking at the screenshot below in which the entry **Daily routine** is available for everyone. Here is what each user should see in the tree view:



Side by Side Tree View

You can further customize your permissions by using the **Security Settings** tab when editing entries, or the **Logs** tab to add more traces of coming and goings. As always, great care must be taken when granting permissions.

If you need more details on each permission, please consult our Common Settings – Permissions topic.

## 8.2.2 Advanced Security

### DESCRIPTION



This feature is only available when using an [Advanced Data Source](#).



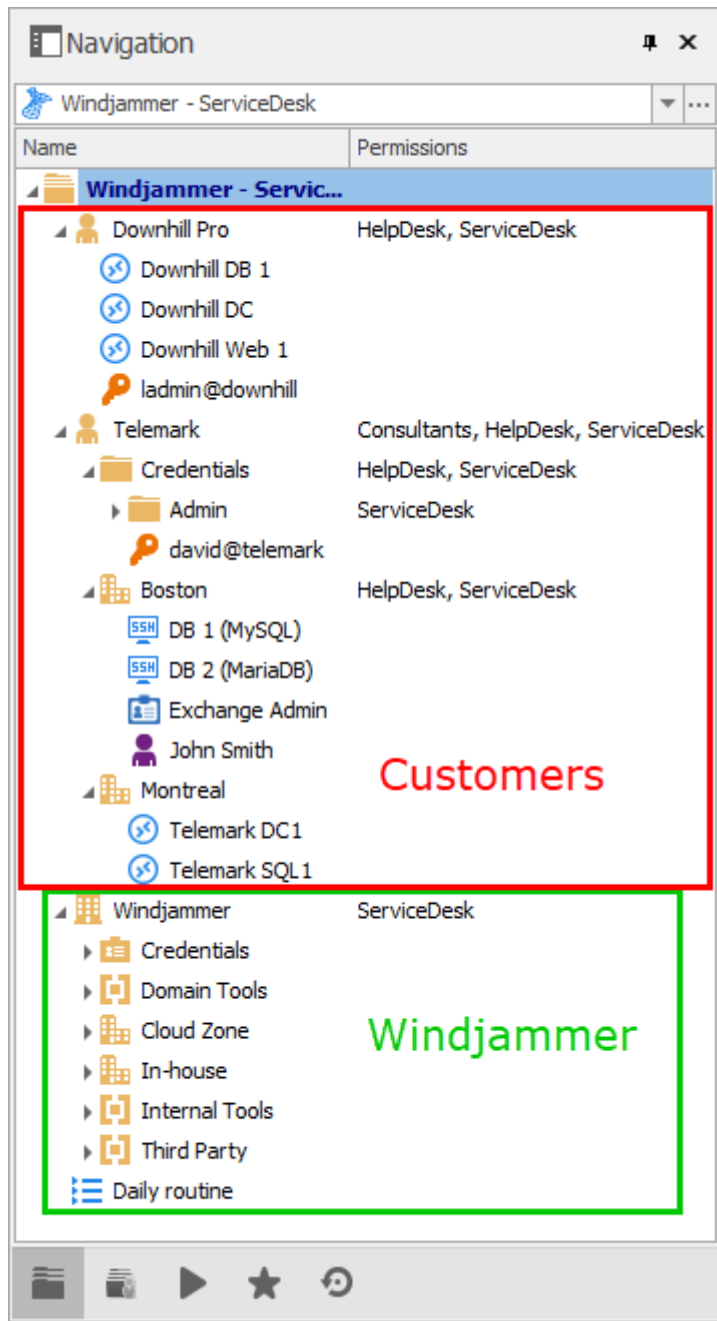
The following scenario is designed for large enterprises. For a scenario more suited for small enterprises, please consult our [Simplified Security](#) scenario.

While this example fits for large enterprises, please keep in mind that any privilege should be granted only as necessary. Be careful when granting permissions to a user or a role.

Our fictional company, Windjammer, has three roles: HelpDesk, ServiceDesk, and Consultants. There are two client companies: Downhill Pro and Telemark.

The following tree view structure represents entries which users have access to once all permissions are set:





## USER CONFIGURATION

Here is an example of user configuration. To create users, navigate to **Administration – Users – Add User**.



In this scenario, all the options in the **Privileges** section of the **User Management** are set to **None**.

Here we select the user type to give them the most basic rights (**Add**, **Edit**, and **Delete**).

**ServiceDesk** users are **Restricted users**. They have the **Add** and **Edit** rights. However, they cannot add entries into the root folder.

Remote Desktop Manager - User Management

**User Management**

General

- Information
- Roles
- Privileges
- Security Groups (Legacy)
- Vaults
- Application Access
- Settings

General

ID: F692711D-2B3B-4200-917B-9A9B01BAA388

Authentication type: Database

Username: I am Restricted ☐ Integrated security (Active Directory)

Password: ..... ☒ Create SQL Server Login and User

User type: Restricted user

User license type: Default ☐ User must change password at next logon

**Rights**

☒ Add ☐ Add in root

☒ Edit ☐ Move

☐ Delete

**Information**

First name: Last name:

Email:

OK Cancel

*User Management - ServiceDesk - Restricted User*

**HelpDesk** users are **Restricted Users** as well. They only have the **Add** right. However, they cannot add entries into the root folder.

**General**

ID: F692711D-2B3B-4200-917B-9A9B01BAA38B

Authentication type: Database

Username: I am Restricted ☐ Integrated security (Active Directory)

Password: •••••••• ☒ Create SQL Server Login and User

User type: Restricted user ☐ User must change password at next logon

User license type: Default

**Rights**

☒ Add ☐ Add in root

☐ Edit ☐ Move

☐ Delete

**Information**

First name: Last name:

Email:

*User Management - HelpDesk - Restricted User*


**Consultants** are **Read Only Users** and can only view a subset of entries. They cannot add or edit anything.

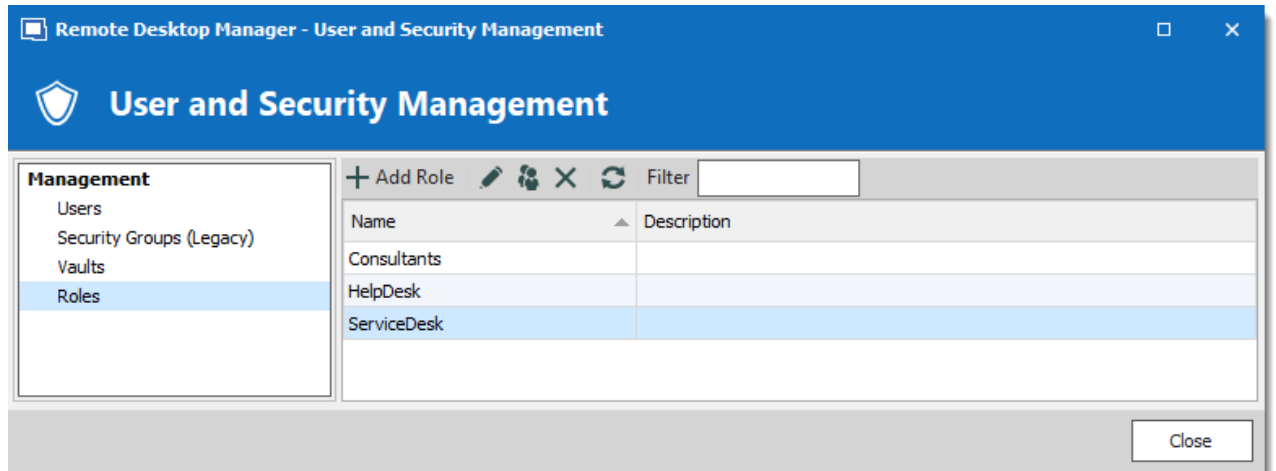
## ROLE CONFIGURATION

Now that the users are created, we will add the roles which we will later grant the permissions to. We need to create the roles and assign the respective user to each role. There is no need to grant any privilege to these roles since they are mainly empty shells used to group multiple users. This allows for controlling multiple users at once instead of granting permissions to each users, one at a time.

- ServiceDesk
- HelpDesk
- Consultants

To add a role, click the **Add Role**  button, enter a name for the role, and click **Ok**.

To assign users to a role, select a role and click the **Assign roles**  button. Use the **Is Member** check boxes to add users to the role.



*User and Security Management - Roles*

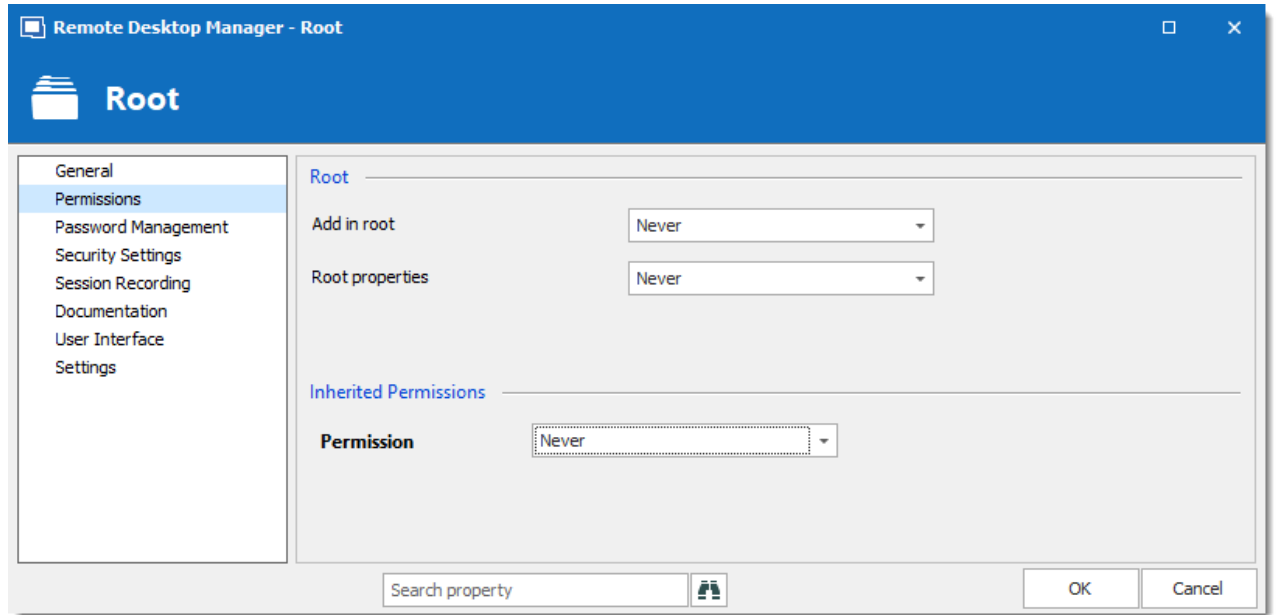
## ENTRY CONFIGURATION

Now, everything is ready to grant or deny access to the roles.

- All root folder permissions are set to **Never**. By inheritance, this denies the child items default access to everyone.
- The ServiceDesk has the permission to view and open all entries but is able to edit only the entries in the client's groups/folders.
- The HelpDesk has the permission to view and open entries in the client's groups/folders only and is not able to edit them.
- The Consultants have the permission to view and open entries in the Montreal folder only but is not able to edit it or its child items.

### Root

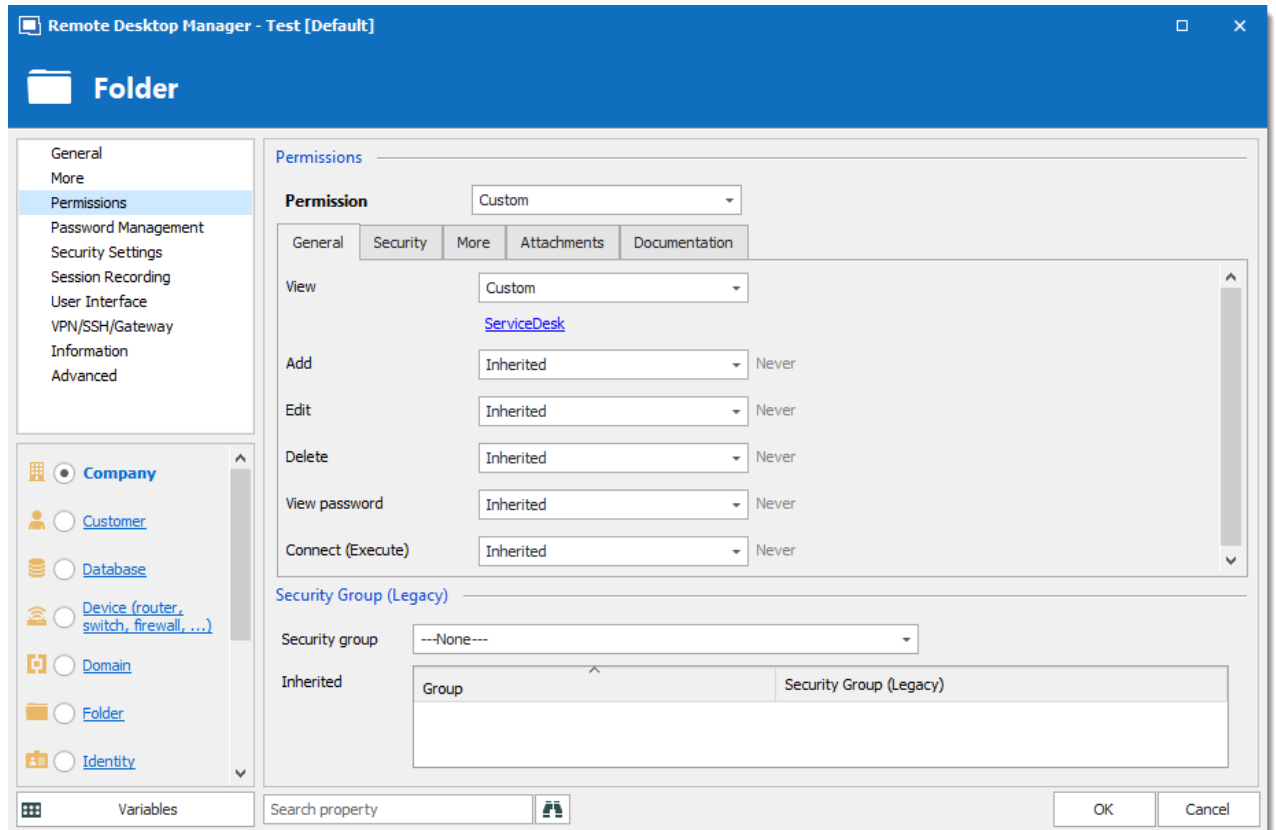
As mentioned above, **ALL** root folder permissions are set to **Never**. This denies the default access to other users.



*Root - Permissions*

### Windjammer Downhill Pro, and Telemark, the root level groups/folders

The permission to view the Windjammer folder is set for the ServiceDesk only since we want them to be able to use the child entries. We don't want the ServiceDesk to add, edit or delete anything. We leave the **Add**, **Edit** and **Delete** permissions to **Inherited** so only the administrators can perform these action on the Windjammer folder and its child items.

*Windjammer - Permissions*

- **View: Custom;** ServiceDesk.
- **Add: Inherited; Never** inherited from Root. Only the administrator can add entries.
- **Edit: Inherited; Never** inherited from Root. Only the administrator can edit entries.
- **Delete: Inherited; Never** inherited from Root. Only the administrator can delete entries.

For Downhill Pro, we grant permissions to the ServiceDesk and the HelpDesk.

Permission	Custom
View	Custom <a href="#">HelpDesk, ServiceDesk</a>
Add	Custom <a href="#">ServiceDesk</a>
Edit	Custom <a href="#">ServiceDesk</a>
Delete	Inherited <input checked="" type="checkbox"/> Never
View password	Inherited <input checked="" type="checkbox"/> Never

Downhill Pro - Permissions

- **View: Custom;** HelpDesk, ServiceDesk.
- **Add: Custom;** ServiceDesk.
- **Edit: Custom;** ServiceDesk.
- **Delete: Inherited; Never** inherited from Root. Only the administrator can delete entries.

We already have a good example of the flexibility of Remote Desktop Manager Security. ServiceDesk and HelpDesk users can view and use all the entries in the Downhill Pro folder, even the credential entries, but they will never see any passwords since the ServiceDesk and HelpDesk users do not have the privilege to reveal passwords.

Next, for the Telemark folder, we grant permissions to the ServiceDesk, the HelpDesk and the Consultants. This is where things get complex. If we want the Consultants to be able to view only the Montreal folder, which is a child item of Telemark, we must grant Consultants the permission to view the parent folder, thereby the entire Telemark content. Then we will grant permissions on child items only to the role that should have access to these items. This last step will deny the view permission for the Consultants on the child items.

Permission		Custom
General	Security	More
View	Custom	Consultants, HelpDesk, ServiceDesk
Add	Custom	ServiceDesk
Edit	Custom	ServiceDesk
Delete	Inherited	Never
View password	Inherited	Never

*Telemark - Permissions*

- **View: Custom;** Consultants, HelpDesk, ServiceDesk.
- **Add: Custom;** ServiceDesk.
- **Edit: Custom;** ServiceDesk.
- **Delete: Inherited; Never** inherited from Root. Only the administrator can delete entries.

### Telemark Child Items

Since we want the users to be able to use the credential entries, we grant the ServiceDesk and the HelpDesk the permission to view the Credentials folder. Therefore, the ServiceDesk and HelpDesk are able to use the entries in the folder without revealing the passwords. By specifying that only the HelpDesk and ServiceDesk have the **View** permission, we deny the view access to any role or user that is not on the list of the permission.

The **Add** and **Edit** permissions are set to **Never** and the **Delete** permission can be left to **Inherited** since it inherits the **Never** settings from the Root. Only the administrators can perform these actions in groups/folders containing credentials.



Permission		Custom
General	Security	More Attachments Documentation
View	Custom	<a href="#">HelpDesk, ServiceDesk</a>
Add	Never	
Edit	Never	
Delete	Inherited	Never
View password	Inherited	Never
Connect (Execute)	Inherited	Never

*Telemark\Credentials - Permissions*

- **View: Custom;** HelpDesk, ServiceDesk.
- **Add: Never;** Only administrators can add credential entries.
- **Edit: Never;** Only administrators can edit entries.
- **Delete: Inherited; Never** inherited from Root. Only administrators can delete entries.

We want the ServiceDesk to be able to use the **Domain admin** credential entry, but not the HelpDesk. For this, we must grant the **View** permission to the ServiceDesk. The ServiceDesk is still be able to use the credential entry but will never see the password.

Permission		Custom
General	Security	More Attachments Documentation
View	Custom	<a href="#">ServiceDesk</a>
Add	Inherited	Never
Edit	Inherited	Never
Delete	Inherited	Never
View password	Inherited	Never
Connect (Execute)	Inherited	Never

*Telemark\Credentials\Admin - Permissions*

- **View: Custom;** ServiceDesk.
- **Add: Inherited; Never** inherited from Root. Only administrators can add credential entries.
- **Edit: Inherited; Never** inherited from Root. Only administrators can edit credential entries.

- **Delete: Inherited; Never** inherited from Telemark\Credentials. Only administrators can delete credential entries.

The last step for the Telemark child items is to set the **View** permission to the ServiceDesk and the HelpDesk on the Boston folder and leave every other permissions of this folder to **Inherited**. This denies the Consultants to view the Boston folder. Now, the Consultants are able to view and open entries only in the Montreal folder.

Permission	Value	Source
View	Custom	HelpDesk, ServiceDesk
Add	Inherited	ServiceDesk
Edit	Inherited	ServiceDesk
Delete	Inherited	Never
View password	Inherited	Never
Connect (Execute)	Inherited	Never

*Telemark\Boston - Permissions*

- **View: Custom;** HelpDesk, ServiceDesk.
- **Add: Inherited;** ServiceDesk inherited from Telemark.
- **Edit: Inherited;** ServiceDesk inherited from Telemark.
- **Delete: Inherited; Never** inherited from Root.



Every time a new folder is added as a child of the Telemark folder, the **View** permission must be set for ServiceDesk and/or HelpDesk to hide the new folder and its content from the Consultants.

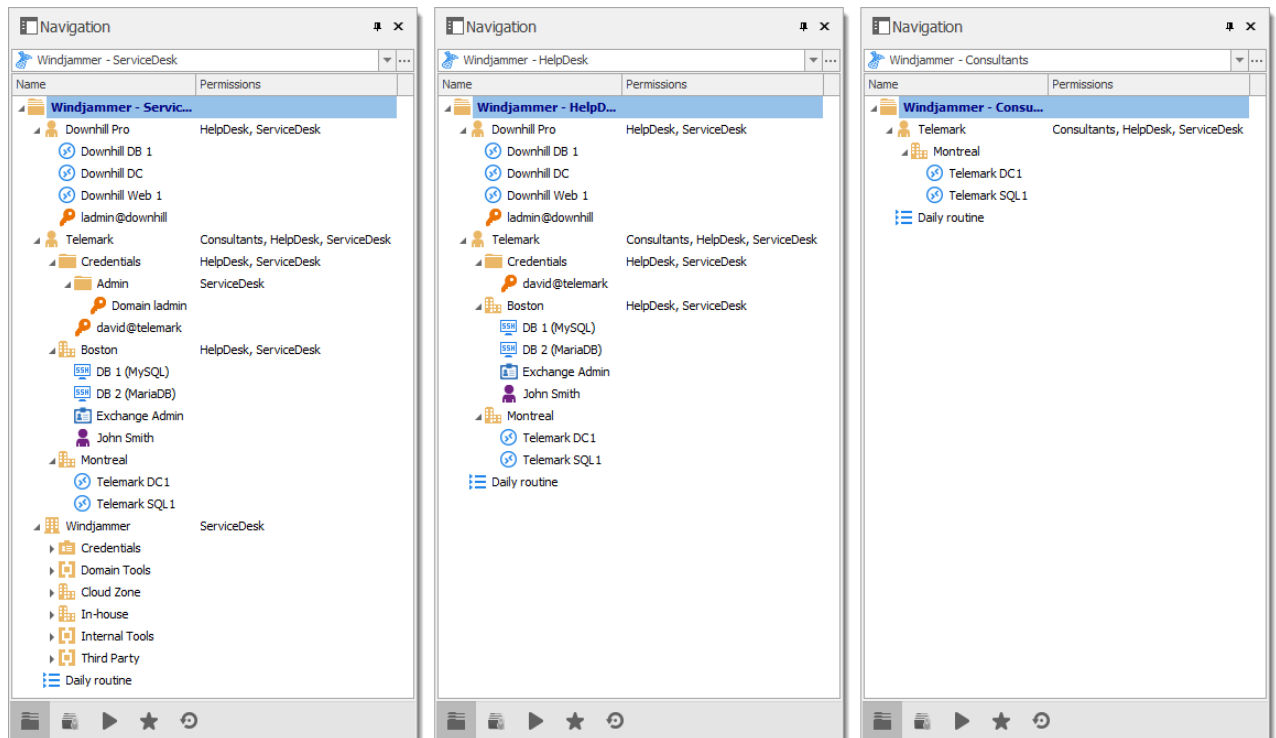
There is no need to set any permissions on the Montreal folder, since they all inherit values from parent folders.

Permission		Default
General	Security	More
View	Inherited	Consultants, HelpDesk, ServiceDesk
Add	Inherited	ServiceDesk
Edit	Inherited	ServiceDesk
Delete	Inherited	Never
View password	Inherited	Never
Connect (Execute)	Inherited	Never

*Telemark\Montreal - Permissions*

## IN CONCLUSION

The permissions are now correctly set. Note that every entry added at root level are inheriting from the Root as well. This means they would be available to admins only, unless their permissions were modified. This can be confirmed by looking at the screenshot below, in which the entry **Daily routine** is available for everyone (It's permissions have been changed to Everyone). Here is what each user should see in the tree view:



*Side by Side Tree View*

You can further customize permissions by using the **Security Settings** tab when editing entries. As always, great care must be taken when granting permissions.

If you need more details on each permission, please consult our Common Settings – Permissions topic.

## 8.3 Legacy Information

### DESCRIPTION

Describing such a flexible security system takes a lot of effort. This chapter contains valuable information, but that may have been optimized by a newer topic.

#### 8.3.1 Small to Medium Enterprise

### DESCRIPTION

Here we will give you a security structure example that should be relevant for small to medium business.

In this scenario, all the options in the **Privileges** section of the user properties will be left disabled.

While this example might fit for many enterprises, please keep in mind that any privilege should be granted only if needed. Be extremely careful when granting permissions to a user or a role.

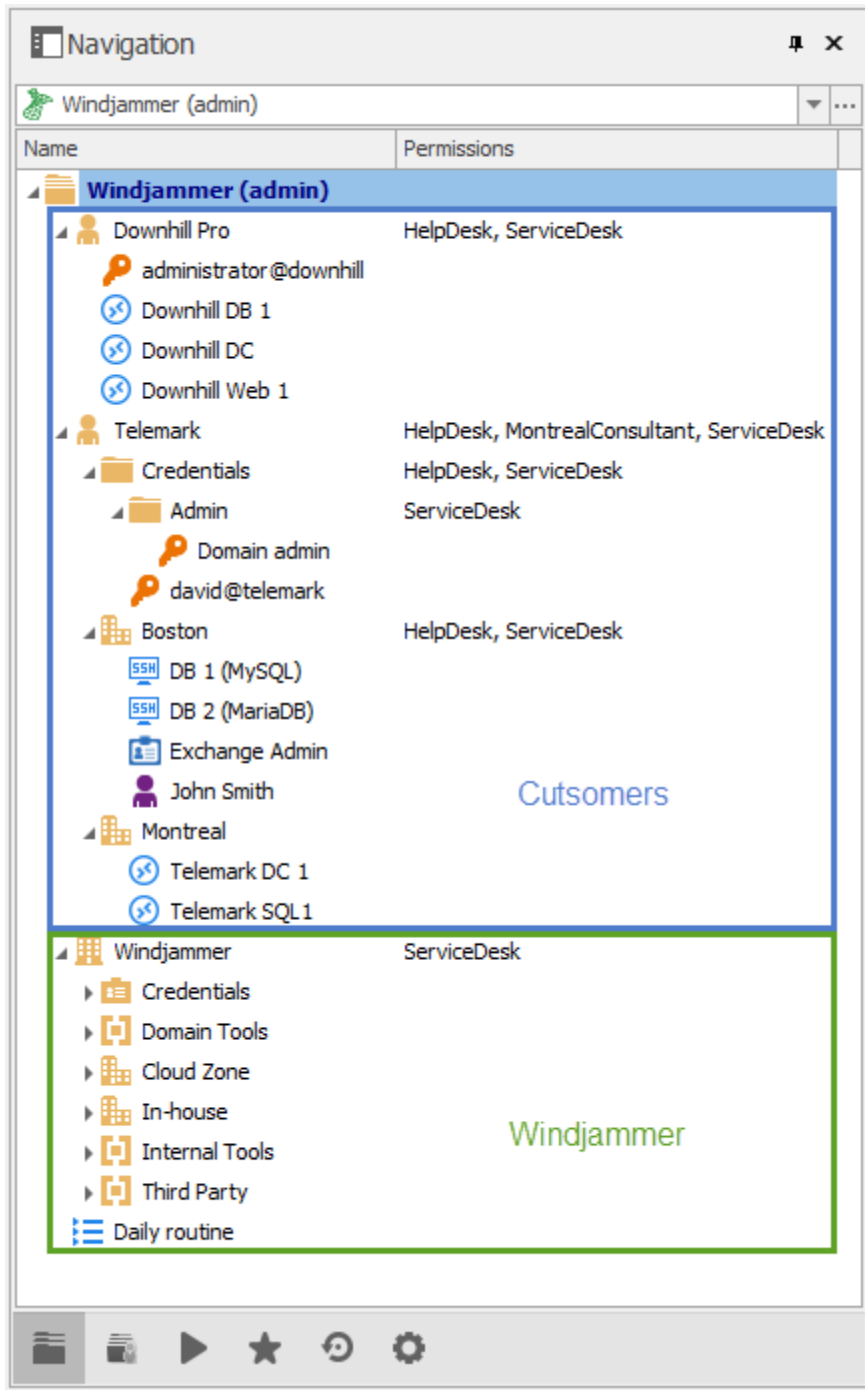


This feature is only available when using an [Advanced Data Source](#).

### STEPS

Our fictional company *Windjammer* has a *HelpDesk* and a *ServiceDesk* department, an administrator and a *MontrealConsultant*. We can also see two customers: *Downhill Pro* and *Telemark*.

Here is a view of the data source tree view structure:



## USER CONFIGURATIONS

Here is an example for user configurations.

The administrator:



The screenshot shows a web interface for configuring rights. On the left is a navigation menu with the following items: General, Information (expanded), Details, Address, Phone, Roles, Privileges, Permissions (highlighted in blue), and Settings. The main area is titled 'Rights' and contains a list of permissions: 'Add' (checked), 'Edit' (checked), and 'Delete' (unchecked). A green rectangular box highlights the 'Add' and 'Edit' permissions. To the right of the 'Add' permission, there is a checkbox labeled 'Deny add entry in root folder' which is also checked.

*ServiceDesk Rights*

The *HelpDesk*:

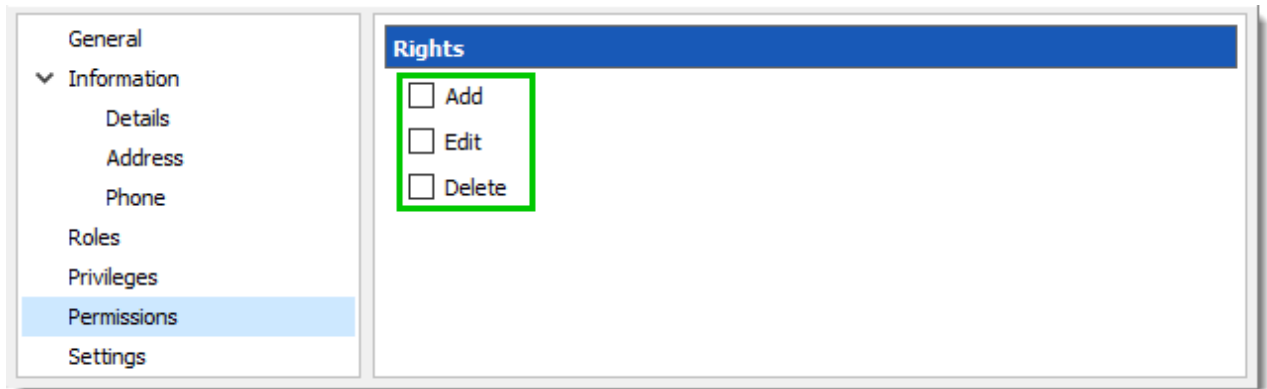
- **Add**
- **Deny add entry in root folder**

This screenshot shows the same 'Rights' configuration interface as the previous one. In this configuration, the 'Add' permission is checked and highlighted with a green box, while 'Edit' and 'Delete' are unchecked. The 'Deny add entry in root folder' checkbox is also checked. The left navigation menu is identical to the previous screenshot, with 'Permissions' highlighted.

*HelpDesk Rights*

The MontrealConsultant has read-only access. He cannot see any password or entry detail.

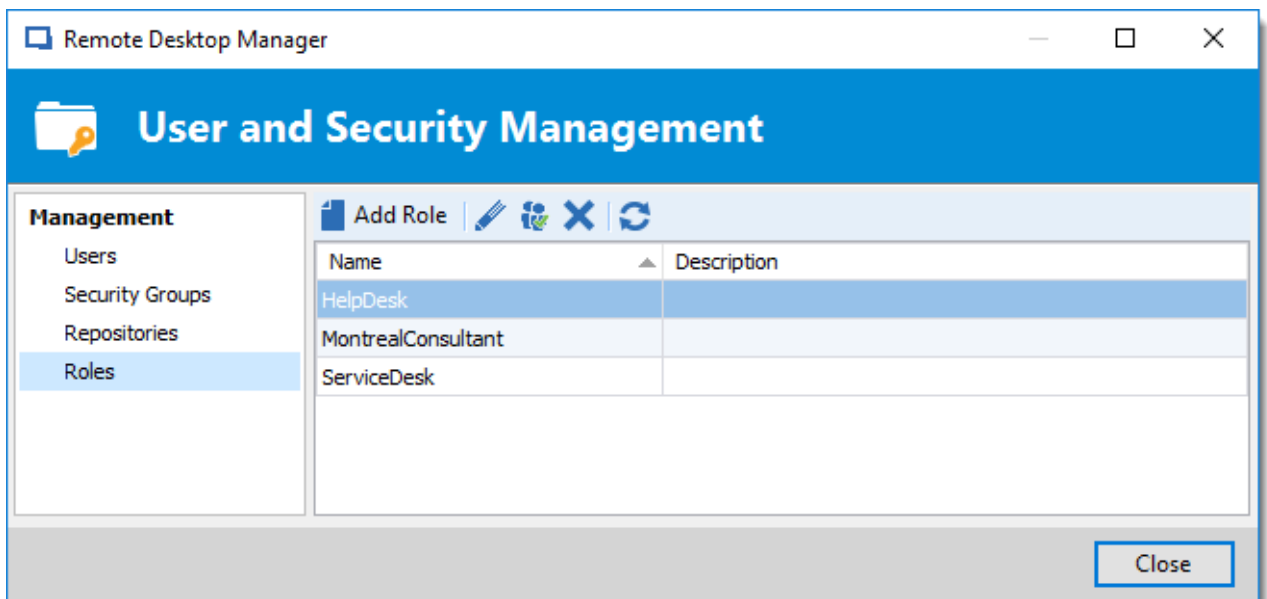
- Leave everything disable for this user

*MontrealConsultant Rights*

## ROLES CONFIGURATION

Now that the users are created we will add the roles to which we will later grant the permissions. We just need the roles to assign users to them. No need to grant them any privileges.

- ServiceDesk
- HelpDesk
- MontrealConsultant

*Roles*

## ENTRIES CONFIGURATION

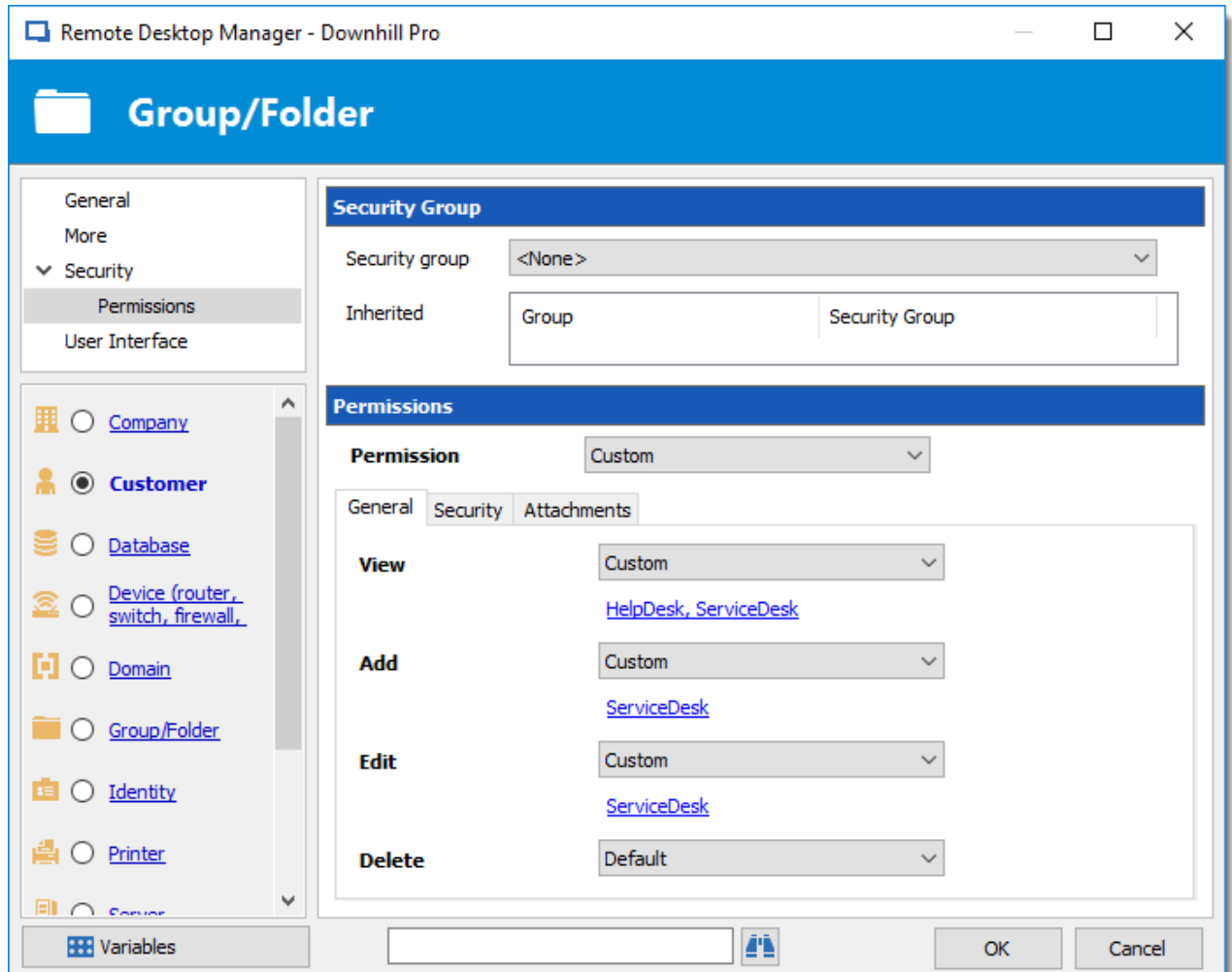
Now everything is ready to grant or deny access to the roles.



- The ServiceDesk will have the permission to view and open all entries but will be able to edit only the entries in the customer groups/folders.
- The HelpDesk will have the permission to view and open entries on the customer groups/folders only and will not be able to edit them.
- The MontrealConsultant will have the permission to view and open entries on the Montreal group/folder only and will not be able to edit it nor its child items.

We will begin with the root level groups/folders: Downhill Pro, Telemark and Windjammer.

For Downhill Pro, we will grant permissions to the ServiceDesk and the HelpDesk.



*Downhill Pro - Permissions*

- **View:** HelpDesk, ServiceDesk
- **Add:** ServiceDesk
- **Edit:** ServiceDesk
- **Delete:** Since no user have the delete right we can leave this permission to **Default**.

We already have a good example of the flexibility of Remote Desktop Manager's Security. A ServiceDesk user can view and open all the entries in the Downhill Pro folder, even the credential entry, but it will never be able to see any password.

Next for the Telemark folder, we will grant permissions to the ServiceDesk, the HelpDesk and the MontrealConsultant. This is where things get complex. If we want the MontrealConsultant to be able to view only the Montreal folder which is a child item of Telemark, we must grant to the consultant the permission to view the entire Telemark content. Then we will grant permissions on child items only to the role that should have access to these items. This last step will deny the view permission for the consultant on the child items.

Permissions	
<b>Permission</b>	Custom
General Security Attachments	
<b>View</b>	Custom <a href="#">HelpDesk, MontrealConsultant, ServiceDesk</a>
<b>Add</b>	Custom <a href="#">ServiceDesk</a>
<b>Edit</b>	Custom <a href="#">ServiceDesk</a>
<b>Delete</b>	Default

*Telemark - Permissions*

- **View:** HelpDesk, MontrealConsultant, ServiceDesk
- **Add:** ServiceDesk
- **Edit:** ServiceDesk
- **Delete:** Default

Since we want the users to be able to use the credential entries, we will grant the ServiceDesk and the HelpDesk the permission to View the Credentials folder. This way they will be able to use the entries without being able to view the passwords.

The **Add** and **Edit** permissions can be left to **Default** since the ServiceDesk is the only role that has been granted these permissions in the parent folder.

**Permissions**

**Permission** Custom

General Security Attachments

**View** Custom  
[HelpDesk, ServiceDesk](#)

**Add** Default ServiceDesk

**Edit** Default ServiceDesk

**Delete** Default

*Telemark\Credentials - Permissions*

- **View:** HelpDesk, ServiceDesk
- **Add:** Default
- **Edit:** Default
- **Delete:** Default

We want the ServiceDesk to be able to use the Domain Admin credential entry as well but not the HelpDesk. For this we must grant the **View** permission to the ServiceDesk only and change the **Add** and **Edit** permission to **Never**. The ServiceDesk will still be able to edit the credential entry but will never see the password. If you prefer you can set the **Edit** permission to an Administrator user or role to deny it to the ServiceDesk.

**Permissions**

**Permission** Custom ▾

General Security Attachments

**View** Custom ▾  
[ServiceDesk](#)

**Add** Default ▾ [ServiceDesk](#)

**Edit** Custom ▾  
[Admin](#)

**Delete** Default ▾

*Telemark\Credentials\Admin - Permissions*

- **View:** ServiceDesk
- **Add:** Default (ServiceDesk)
- **Edit:** Default or Administrator user/role
- **Delete:** Default

The last step for the Telemark child items would be to set the **View** permission to the ServiceDesk and the HelpDesk on the Boston folder and leave every other permission to **Default**.

Now the MontrealConsultant will be able to view and open entries only in the Montreal folder. Every time a new folder is added the **View** permission must be set for ServiceDesk and HelpDesk to hide the new folder and its content from the consultant.

**Permissions**

Permission: Custom

General | Security | Attachments

**View**: Custom  
[HelpDesk, ServiceDesk](#)

**Add**: Default ServiceDesk

**Edit**: Default ServiceDesk

**Delete**: Default

*Telemark\Boston - Permissions*

- **View**: HelpDesk, ServiceDesk
- **Add**: Default (ServiceDesk)
- **Edit**: Default (ServiceDesk)
- **Delete**: Default

No need to set any permissions on the Montreal folder, since they are inherited from the parent folders.

**Permissions**

Permission: Default

General | Security | Attachments

**View**: Default  
[HelpDesk, MontrealConsultant, ServiceDesk](#)

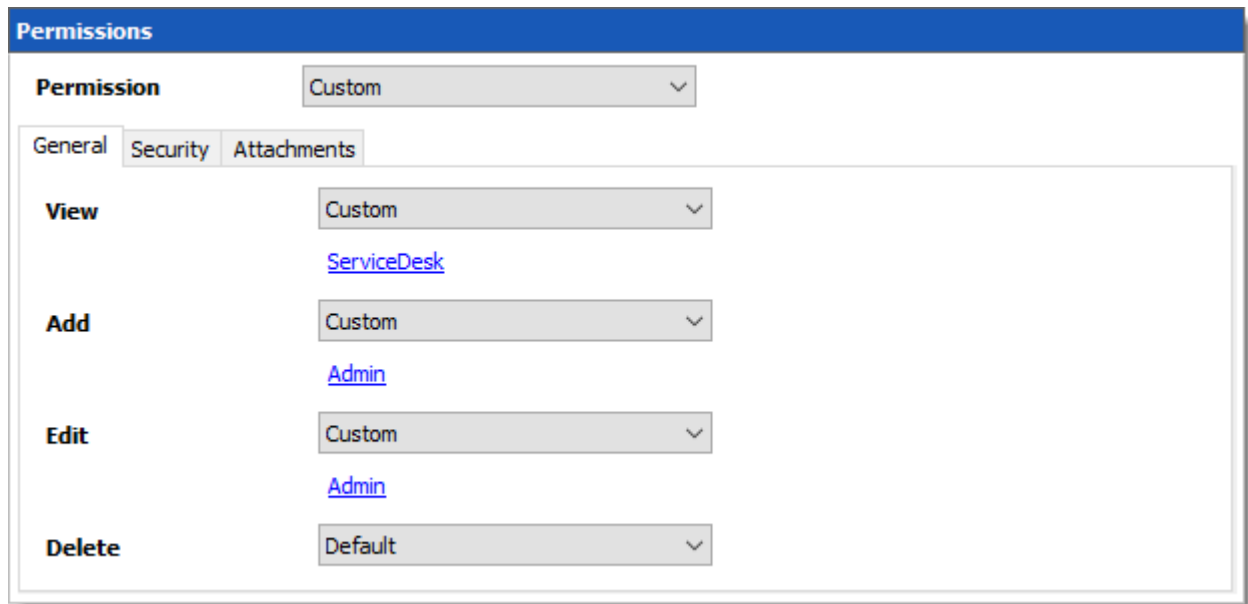
**Add**: Default ServiceDesk

**Edit**: Default ServiceDesk

**Delete**: Default

*Telemark\Montreal - Permissions*

Finally, the permission to view the Windjammer folder will be set for the ServiceDesk only since we want them to be able to use its child entries. We don't want them to add or edit anything so we will set the **Add** and **Edit** permissions to the Administrator user/role.

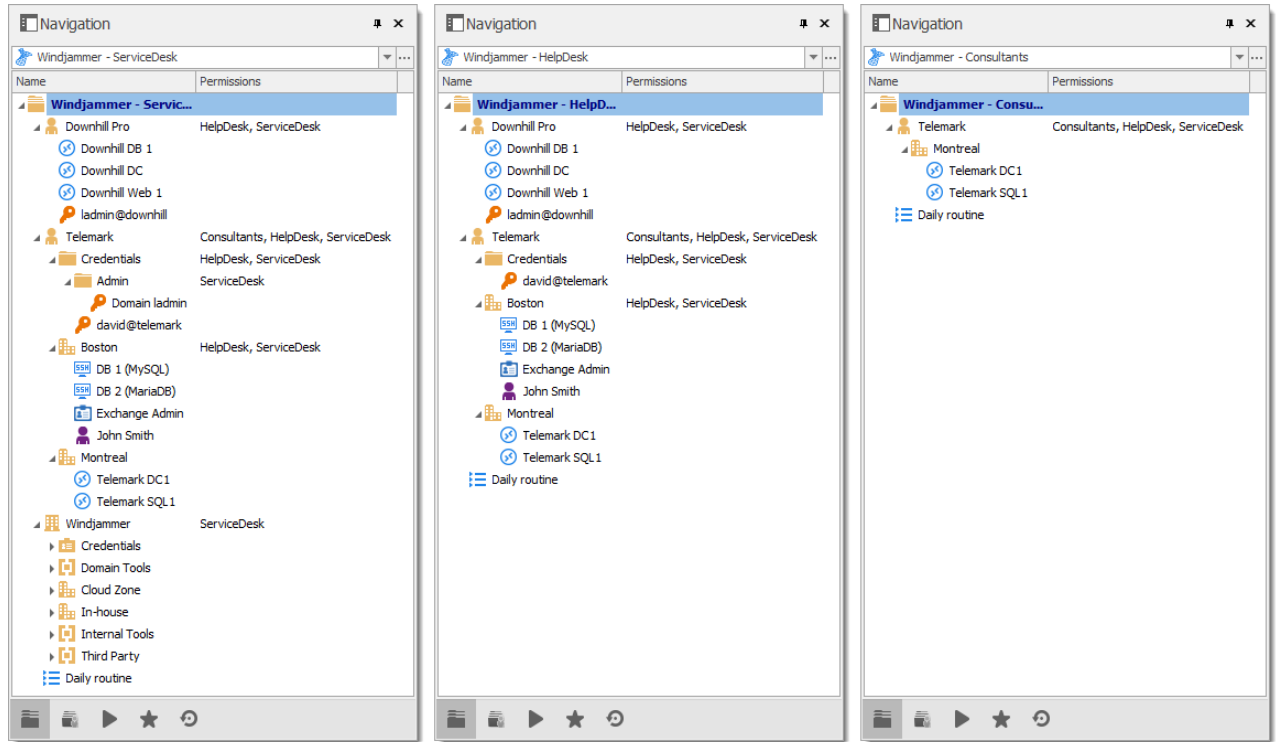


Permissions	
Permission	Custom
General Security Attachments	
View	Custom <a href="#">ServiceDesk</a>
Add	Custom <a href="#">Admin</a>
Edit	Custom <a href="#">Admin</a>
Delete	Default

*Windjammer - Permissions*

## IN CONCLUSION

The permissions are now correctly set. Note that every entry added higher than the root level groups/folders will have no security by default. This means they would be available for anyone, even the consultant. This can be confirmed by looking at the screenshot below in which the entry Daily routine is available for everyone. Here is what each user should see in the tree view:



*Side by side tree views*

You can go further with granting permissions by using the **Security** and **Attachments** tabs of the permissions section. As always, a great care must be taken when granting permissions and users should have very strict privileges.

If you need more details on each permission, please consult our Common Settings – Permissions topic.

# PowerShell Scripting

---

Part IX



## 9 PowerShell Scripting

### DESCRIPTION

Remote Desktop Manager supports Windows PowerShell. PowerShell is a powerful scripting shell that lets administrators automate Remote Desktop Manager. They are provided in a PowerShell module.

### MANUALLY IMPORT THE POWERSHELL MODULE

The Remote Desktop Manager PowerShell Module, which is called RemoteDesktopManager.PowerShellModule.dll, is located in the Remote Desktop Manager installation directory. If you want to manually import the module in another application, for instance PowerShell ISE, you can use the Import-Module CmdLet to load the module. Simply use the following command:

```
Import-Module "${env:ProgramFiles(x86)}\Devolutions\Remote Desktop Manager\RemoteDesktopM
```



If the sample above does not work due to a different Remote Desktop Manager installation directory, simply change **`${env:ProgramFiles(x86)}`** to **`\Devolutions\Remote Desktop Manager`** for the correct application path.

### COMMANDS

To list all cmdlet commands, please enter this command:

```
Get-Command -Module RemoteDesktopManager.PowerShellModule
```

For more information on those commands, use the following command:

```
get-help [command name]
```



Here's how to generate a text file with all the commands:

```
Get-Command -Module RemoteDesktopManager.PowerShellModule -Type Cmdlet `
| Sort-Object -Property Name >`
```

```

| Format-Table -Property Name `
| out-file $env:temp\pshelp.txt

Get-Command -Module RemoteDesktopManager.PowerShellModule `
| ForEach-Object { get-help -name $_.Name -full } `
| out-file -append $env:temp\pshelp.txt

```

For further information on the subject, or if you have questions, join us on the [forum](#) and our team will be glad to assist you.

## 9.1 Tips and tricks

### DESCRIPTION

We are always asked for a full list of property names and sadly it is extremely hard to provide for multiple reasons. The best way is still to look at the xml structure of an entry of the proper type to identify the field names.

### REVERSE ENGINEERING AN ENTRY'S STRUCTURE

1. Create an entry of the needed type, add only mandatory data at this time. Save the entry.
2. Right-click on the entry, then use **Clipboard – Copy**.
3. In the dialog that appears, switch to the **Preview** tab, copy the xml structure to a text file. This is the **BEFORE**.
4. Manually perform the modification to the entry that you would like to automate using PowerShell, save the entry.
5. Using **Clipboard – Copy**, save the modified xml to another file. This is the **AFTER**.
6. Compare the two files with your favorite difference tool, you will see the fields that have changed, and the values that have been assigned. This indicates what your script should do.

### ESSENTIAL INFORMATION ABOUT REMOTE DESKTOP MANAGER'S XML FORMAT

- To save space, most fields have a default value and when the field contains that default value, it simply does **NOT** appear in the content. That is why you must watch out for new fields that appear in the AFTER content.
- Credentials are handled in a special way. They contain a GUID when they refer to other entries, but they hold Well-Known static GUIDs when they use other mechanisms.

SETTING	WELL KNOWN GUID
Default	""

SETTING	WELL KNOWN GUID
<b>Credential repository --- Prompt on connection ---</b>	"45479560-173E-435D-8848-C22F863FDC96"
<b>Embedded</b>	should be used for backwards compatibility only, we prefer not to list it here.
<b>Parent (only for sub-connections)</b>	"E2CC9029-CA3A-4308-BA54-16D5029BC8ED"
<b>Inherited</b>	"1310CF82-6FAB-4B7A-9EEA-3E2E451CA2CF"
<b>My personal credentials</b>	"9F3C3BCF-068A-4927-B996-CA52154CAE3B"
<b>None</b>	"B87B29D9-9239-4D7B-86D8-9B53DCD3BA9F"
<b>Private Vault, paired with <i>PersonalConnectionID</i></b>	"245A4245-48E7-4DF5-9C4C-11861D8E1F81"
<b>Private Vault Search, paired with <i>CredentialPrivateVaultsearchString</i></b>	"88E4BE76-4C5B-4694-AA9C-D53B7E0FE0DC"

## TIPS AND TRICKS

- Use the Set-RDMPProperty cmdlet to set almost any value within the session object. To find properties and paths, reverse engineer the session XML file format. Create a sample session in RDM and export it using the right click menu Import/Export - Export Session (.rdm).... Once exported, open the .rdm file with your favorite editor. Browse the XML structure to find the property path and name.
- Use the AddDataEntryKind method to set the data entry kind to Web (11 in this case). This is not actually documented – it's just a bonus tip that we use here at Devolutions all the time!

## 9.2 PowerShell Samples

### DESCRIPTION

These are the recipes to perform various tasks using our PowerShell cmdlets.

Remote PowerShell allows you to run scripts on remote computers. This is an extremely powerful tool that can be used to extract a ton of information as well as modify the remote computer's settings.

### SETTINGS

Please consult the following topics for some PowerShell How-to:

- [Extract TeamViewer ID](#)
- [Custom Export to CSV](#)
- [Remote Management](#)
- [Script Execution Policy](#)
- [Change your Synchronize source](#)

### REFERENCES

<http://technet.microsoft.com/en-us/library/ee176949.aspx>

<http://www.howtogeek.com/117192/how-to-run-powershell-commands-on-remote-computers/>

### 9.2.1 Batch Actions Samples

### DESCRIPTION

The Batch Actions allow for a quick way to modify multiple sessions at once, but within Remote Desktop Manager itself.

To be able to create your PowerShell script, you would need the name of the field(s) that you would like to update. To retrieve the exact name of the field, right-click on your session and select **Clipboard – Copy**. You can then paste the information in a text editor to retrieve the name of the field(s) that you would like to modify via the Custom PowerShell Command.

Since they use the Powershell technology, we provides samples in this section because the fields are the same when accessed through our Batch Actions or through Powershell.

## SAMPLES

### DISABLE ONLY SEND PASSWORD IN HTML PASSWORD FIELD OPTION IN WEB BROWSER SESSIONS

```
$connection.Web.OnlySendPasswordInPasswordField = $false;
$RDM.Save ( ) ;
```

### ENABLE VIEW URL EMBEDDED (INFORMATION ENTRIES)

```
$connection.DataEntry.ViewUrlDisplayMode = "Default";
$RDM.Save ( ) ;
```

ViewUrlDisplayMode: "Default" = embedded, "External" = external.

### OPEN URL (EXTERNAL) FOR WEB LOGIN (INFORMATION ENTRIES)

```
$connection.DataEntry.DefaultAction = "OpenUrlExternal";
$RDM.Save ( ) ;
```

### SSH SHELL BATCH EDIT (SESSION TYPE SETTINGS)

```
$connection.Terminal.MaxScrollbackLines = 2000;

$connection.Terminal.AlwaysAcceptFingerprint = $true;

$connection.Terminal.EnableLogging = $true;
$connection.Terminal.LogPath = '$LOGPATH$\$NAME$_$DATE_TEXT_ISO$_$TIME_TEXT_ISO$.log';
$connection.Terminal.LogMode = 1;
$connection.Terminal.LogOverwriteMode = 0;
$RDM.Save ( ) ;
```

Here are some values that you can change for this command;

LogPath: your path between '' (single quotes). You can also use variables. i.e. %USERPROFILE%, \$NAME\$, etc. In this example \$LOGPATH\$ is a custom variable defined in the [Data Source Settings \(System Settings\) - Custom Variables](#)

LogMode: 1 = Printable Output, 0 = Event

TerminalLogOverwriteMode: 0 = default, 1 = prompt, 2 = append, 3 = overwrite

Here's also other options that you can modify;

```
$connection.Terminal.BellMode = 'Visual'
$connection.Terminal.CloseOnDisconnect = $false
```

### CONVERT WEB BROWSER SESSIONS INTO LOGMEIN SESSIONS

```
$connection.ConnectionType = 'LogMeIn';  
$connection.ConnectionSubType = '' ;  
$connection.LogMeIn.Url = $connection.WebBrowserUrl;  
$RDM.Save();
```

**Enable the "Hide script errors in all your LogMeIn sessions."**

```
$connection.LogMeIn.ScriptErrorsSuppressed = $true;  
$RDM.Save();
```

**Hide navigation bar.**

```
$connection.LogMeIn.ShowUrl = $false;  
$RDM.Save();
```

**Change the Web Browser Application.**

```
$connection.LogMeIn.WebBrowserApplication = "GoogleChrome";  
$RDM.Save();
```

**Enable the Sandbox Process.**

```
$connection.LogMeIn.SandboxProcess = $true;  
$RDM.Save();
```

**Change the URL.**

```
$connection.LogMeIn.Url = " ";  
$RDM.Save();
```

**Change the Portal Login field.**

```
$connection.LogMeIn.DashboardHostUrl = " ";  
$RDM.Save();
```

**Change Username & Password.**

Please run these two one at a time

### Host;

```
$connection.LogMeIn.UserName = " ";  
$RDM.Save();  
$connection.LogMeIn.SafePassword = " ";  
$RDM.Save();
```

### Portal;

```
$connection.LogMeIn. DashboardEmail = " ";  
$RDM.Save();  
$connection.LogMeIn. SafePasswordDashboard = " ";  
$RDM.Save();
```

## CHANGE A CUSTOM FIELD VALUE WITHOUT CHANGING THE DATA

```
$connection.MetaInformation.CustomField3Title = "MyField"  
$RDM.Save();
```

Please note that you would need to change "MyField" for the value that you want to replace Custom field #3 with.

## BULK UPDATE FQDN INFO TO SESSIONS.

```
$connection.host = $Connection.name + ".mydomain.com"  
$RDM.Save();
```

## BULK CHANGE RECORDING FIELD FOR PUTTY SESSIONS

```
$connection.Putty.RecordingMode = 1;  
$connection.Putty.RecordingFileName = "C:\path\to\your\file.log"  
$RDM.Save();
```

## CHANGE THE COMPUTER FIELD OF AN RDP SESSION

```
$connection.Url = " ";  
$RDM.Save();
```

## ENCODING

```
$connection.Putty.TelnetEncoding = "UTF-8";  
$RDM.Save();
```

## CHANGE THE EXPIRATION DATE OF AN RDP SESSION

The date must be specified using the ISO8601 format.

```
$connection.MetaInformation.Expiration = "2018-12-25T00:00:00-05:00";  
$RDM.Save();
```

## CHANGE THE EXPIRATION DATE OF AN RDP SESSION WITH A RELATIVE DATE

Use any date time operator supported by PowerShell.

```
$connection.MetaInformation.Expiration = (Get-Date).AddMonths(6);  
$RDM.Save();
```

## MODIFY PAGE TAB TITLE IN UI

```
$connection.TabTitle = '$COMPANY_NAME$ - $NAME$';  
$RDM.Save();
```

## CLEAR KEYWORDS IN SESSION

```
$connection.MetaInformation.Keywords = "";  
$RDM.Save();
```

## CHANGE HISTORY MAX LINES FOR SSH SHELL (REBEX)

```
$connection.Putty.HistoryMaxLength = 2000;  
$RDM.Save();
```

## CONVERT COMMAND LINE TOOL TO A COMMAND LINE SESSION

```
$connection.ConnectionType = 3;  
$RDM.Save();
```



## CHANGE KEYBOARD HOOK FOR AN RDP SESSION

```
$connection.KeyboardHook = "OnTheRemoteComputer";  
$RDM.Save();
```

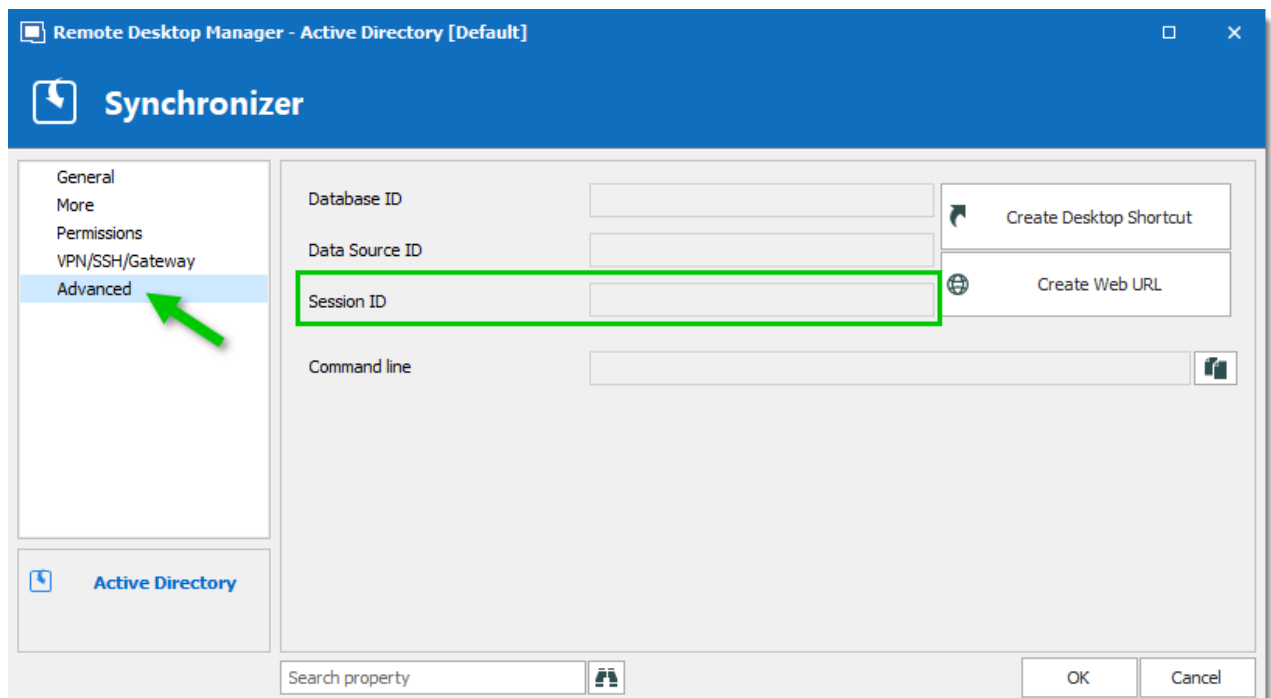
### 9.2.2 Change your Synchronizer source

## DESCRIPTION

If you have been using the Remote Desktop Manager version with the Synchronizer **Action on Entry Mismatch** feature, the following steps will allow you to easily change your source with a Powershell Command without having to recreate all your sessions, thus marking all selected entries as created by the synchronizer.

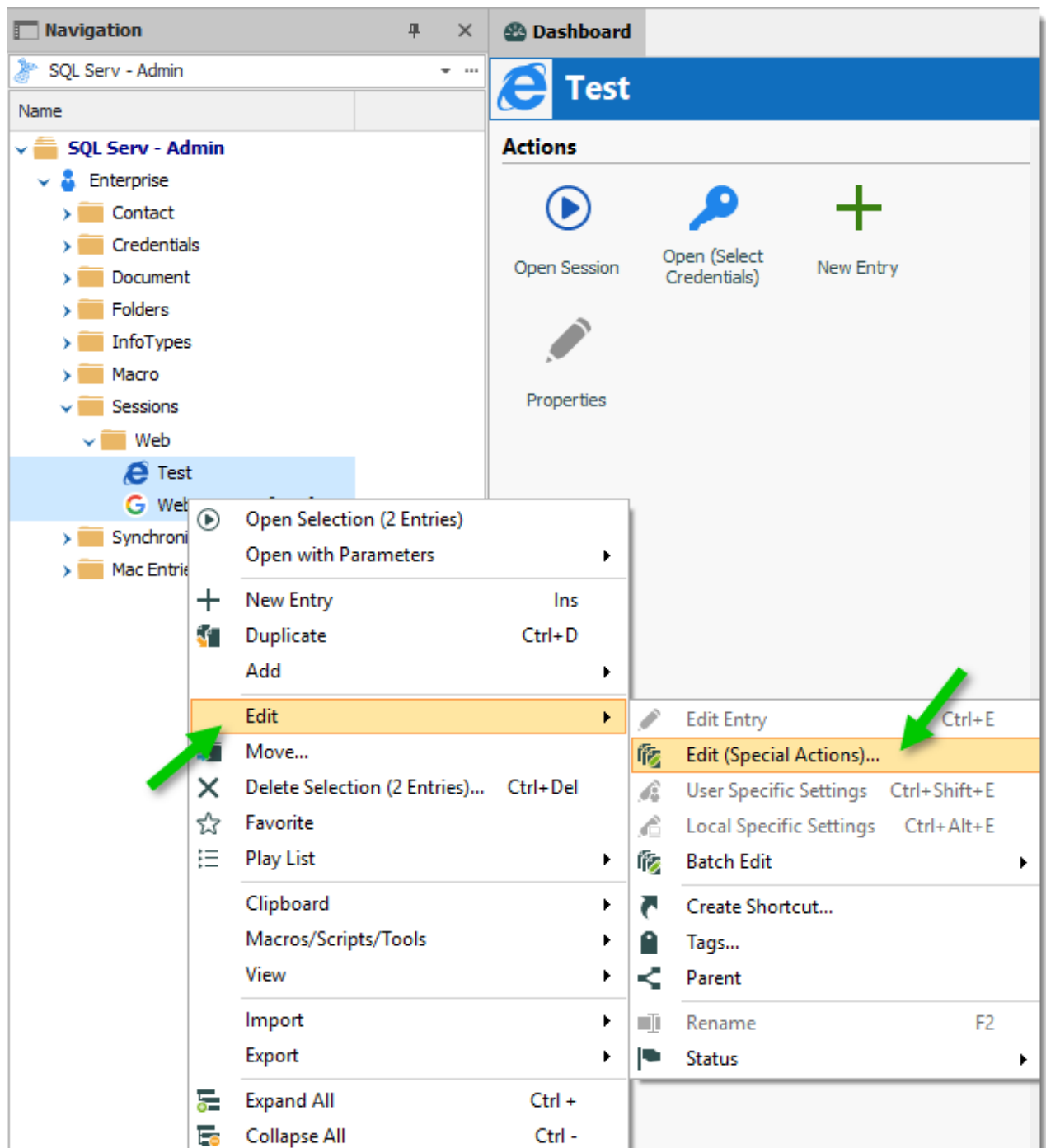
## SETTINGS

1. Select your Synchronizer entry in your Tree view, right click and select **Properties**.
2. In the **Advanced** side menu of the **Properties**, copy the **Session ID** (you will then need that ID number to insert in your Powershell Command).



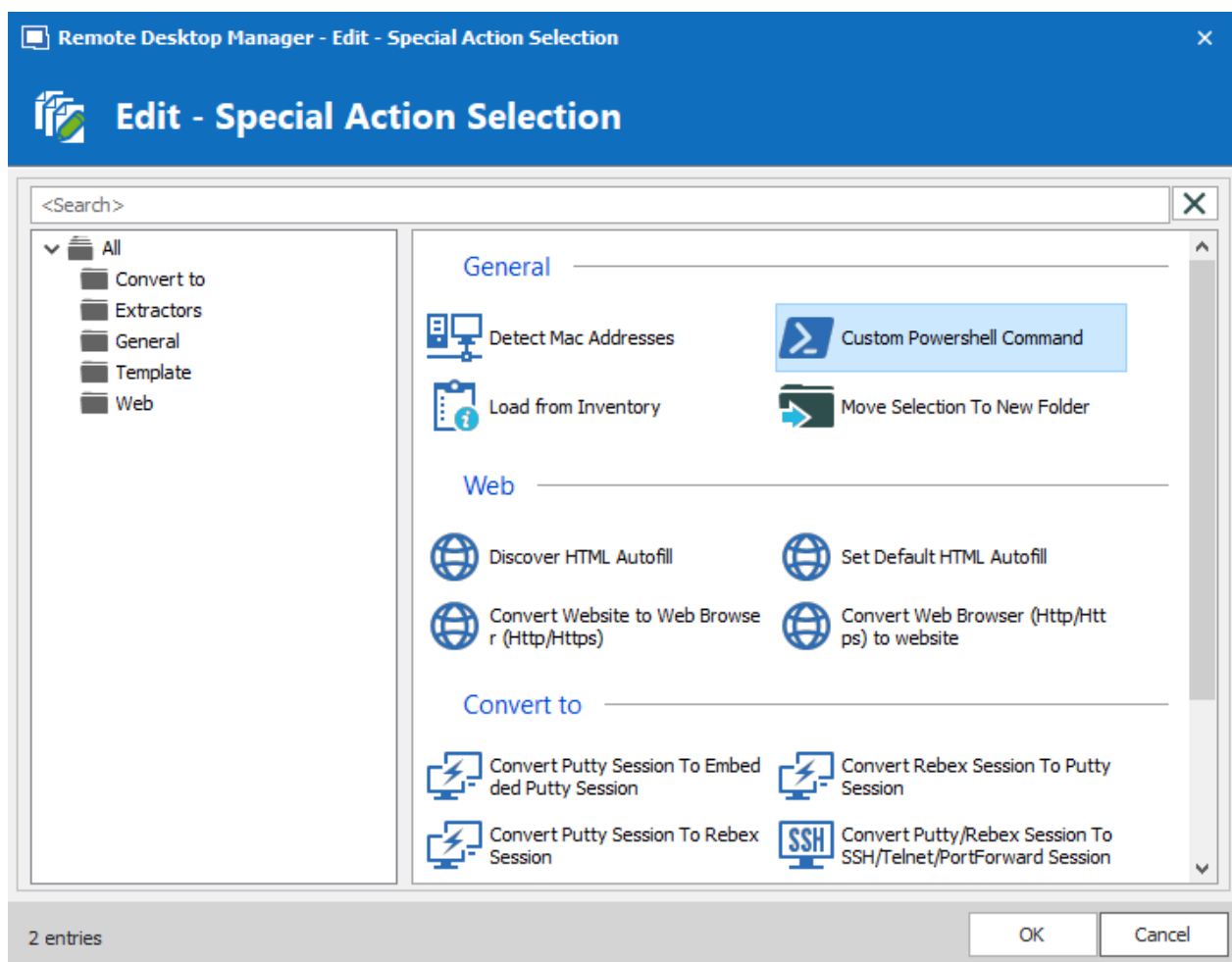
Advanced - Session ID

3. In your Tree view select the entries (ctrl+click) you wish to mark as created by the synchronizer. Then, right-click and go in **Edit – Edit (Special Actions)**.



*Selected entries - Edit (Special Actions)*

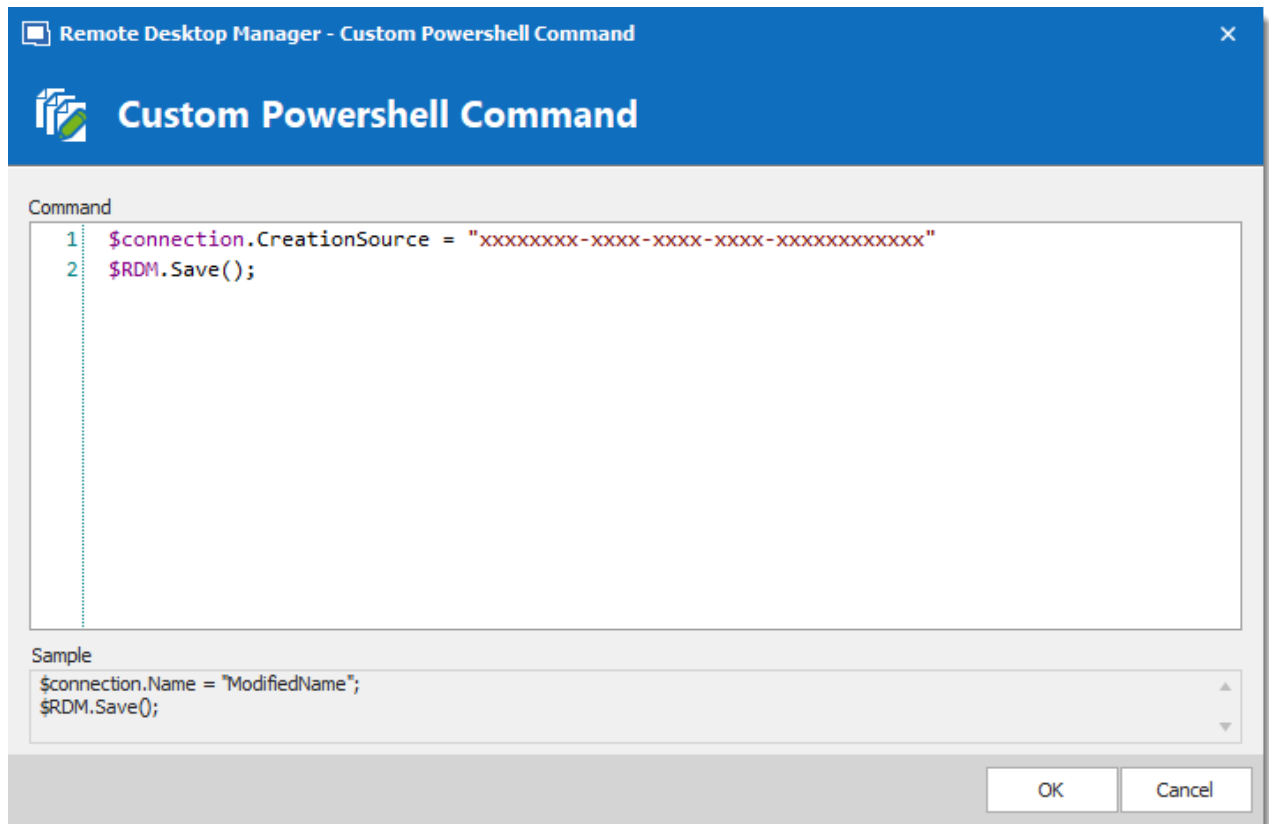
4. Select the **Custom Powershell Command**.



*Edit (Special Actions)*

5. Write the following line for your Powershell Command:

```
$connection.CreationSource = "enter synchronizer ID number"  
$RDM.Save();
```

*Custom Powershell Command*

### 9.2.3 Creating an entry

## DESCRIPTION

This sample creates an entry.

## SAMPLE

```
$computerName = "wind10";
$username = "david";
$domain = "windjammer";
$password = "123456";
$session = New-RDMSession -Host $computerName -Type "RDPCConfigured" -Name $computerName;
Set-RDMSession -Session $session -Refresh;
Update-RDMUI;
Set-RDMSessionUsername -ID $session.ID $username;
Set-RDMSessionDomain -ID $session.ID $domain;
$pass = ConvertTo-SecureString $password -asplaintext -force;
Set-RDMSessionPassword -ID $session.ID -Password $pass;
```

## NOTES

The Update-RMUI call is to allow the entry to be physically saved and available for the rest of the script. It may not be necessary for a types of data sources and our objective is to make it unnecessary for this scenario.

## CMDLETS REFERENCE

### 9.2.4 Creating Group Folder Structure from CSV file

## DESCRIPTION



Please note that the CSV file must be encoded in UTF-8 to support special characters.

This sample creates a Group Folder structure from a CSV file.

## SAMPLE

```
$csv = Import-Csv "c:\YourFolder\GroupFolder.csv"

foreach ($csvEntry in $csv) {
    $groupName = $csvEntry.Name

    # Extract the group folder name
    if ($groupName.Contains("\")) {
        $groupName = $groupName.Substring($groupName.LastIndexOf("\"), $groupName.Length - 1)
        $groupName = $groupName.TrimStart("\")
    }

    # Create the group folder if it is not null, empty or fill in with space characters
    if (![string]::IsNullOrEmpty($groupName)) {
        $session = New-RDMSession -Type "Group" -Name $groupName
        $session.Group = $csvEntry.Name
        Set-RDMSession $session
        Write-Host "Group Folder $groupName created" -f Yellow
    }
}

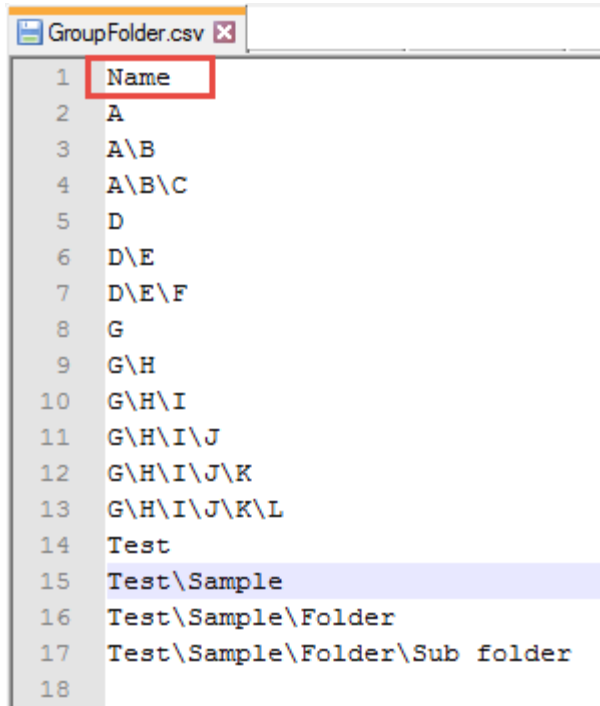
Update-RDMUI
```

## NOTES

The CSV file must have only one column with the title set as Name.

The full path must be specified for each sub folder.

Here is an example of this CSV file :



1	Name
2	A
3	A\B
4	A\B\C
5	D
6	D\E
7	D\E\F
8	G
9	G\H
10	G\H\I
11	G\H\I\J
12	G\H\I\J\K
13	G\H\I\J\K\L
14	Test
15	Test\Sample
16	Test\Sample\Folder
17	Test\Sample\Folder\Sub folder
18	

CSV File example

## CMDLETS REFERENCE

### 9.2.5 Custom Export to CSV

## DESCRIPTION

Many customers ask for a special export that would contain specific fields.

## SETTINGS

Here is a small script that can be used to generate URLs for our new web protocol handler. We generate a csv file that contains the name and the URL.

```
## get the data source ID, note that the "Create Web Url" button generates a different ID
$dsid = Get-RDM-DataSource | where {$_.IsCurrent -eq "X"} | select -expand "ID"
## get the RDP sessions, create a new object with the desired fields.
## Simply append "add-member" commands to include a new field
$s = Get-RDM-Session |
  where {$_.Session.Kind -eq "RDPCConfigured"} |
  foreach {
    new-Object Object |
      Add-Member NoteProperty Name $_.Name -PassThru |
      Add-Member NoteProperty URL "rdm://open?DataSource=$dsid&Session=$(($_.ID))" -PassThru
  };
## save to csv, the field names are used as column headers.
$s | export-csv c:\temp\sessions.csv -notypeinformation;
```

## 9.2.6 Extract TeamViewer ID

### DESCRIPTION

You can use Powershell to extract the TeamViewer ID from a session.

### SETTINGS

Here a script to extract the TeamViewer ID from a session:

```
$sessions = Get-RDM-Session | where {$_.Session.Kind -eq "TeamViewer"}
$sessions[0].Session.GetProperty("TeamViewer", "ID")
```

## 9.2.7 Remote Management

### DESCRIPTION

Default settings disallow remote management calls, there is also the firewall that is blocking requests on the associated ports. Luckily a single PowerShell command will perform all the necessary adjustments without prompting you for each step.

### SETTINGS

In an elevated privileges PowerShell session, run the command below:

```
Enable-PSRemoting -Force
```

## 9.2.8 Script Execution Policy

### DESCRIPTION

By default, no scripts can be run on a new installations. Not only must you enable script execution, but you must choose if you require scripts to have a digital signature.

### SETTINGS

In a PowerShell command window, type `Get-Help About_Signing` to see what is best for your scenario.

If you are satisfied by **RemoteSigned**, simply type in `Set-ExecutionPolicy RemoteSigned` in an PowerShell ses



# Knowledge Base

---

Part X

## 10 Knowledge Base

### 10.1 Protocols and application

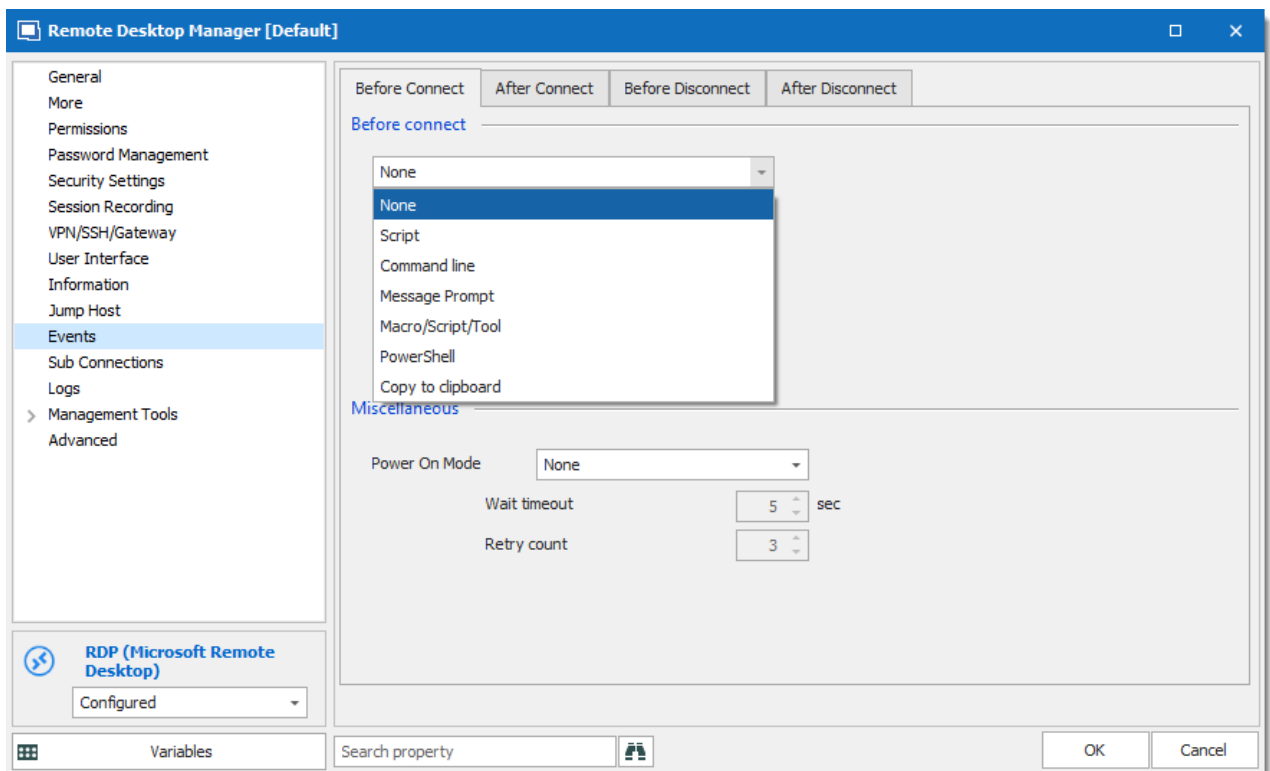
#### 10.1.1 Remote Desktop Manager

##### 10.1.1.1 Events

## DESCRIPTION

Remote Desktop Manager gives you the flexibility to automatically run operations before or after establishing a connection.

These operations are defined via the **Events** section of a session's properties. Define a script or a command line which executes at the appropriate time with the provided parameters, such as the session ID or username. For example, events can be used to execute an external batch file or application that prompts the user for more information, or to update a log on a remote server.



*Session properties – Events*

## SETTINGS

The **Events** section is composed of four tabs. All of them can execute the same events, but at specific times, such as before the connection is established or after its interruption.

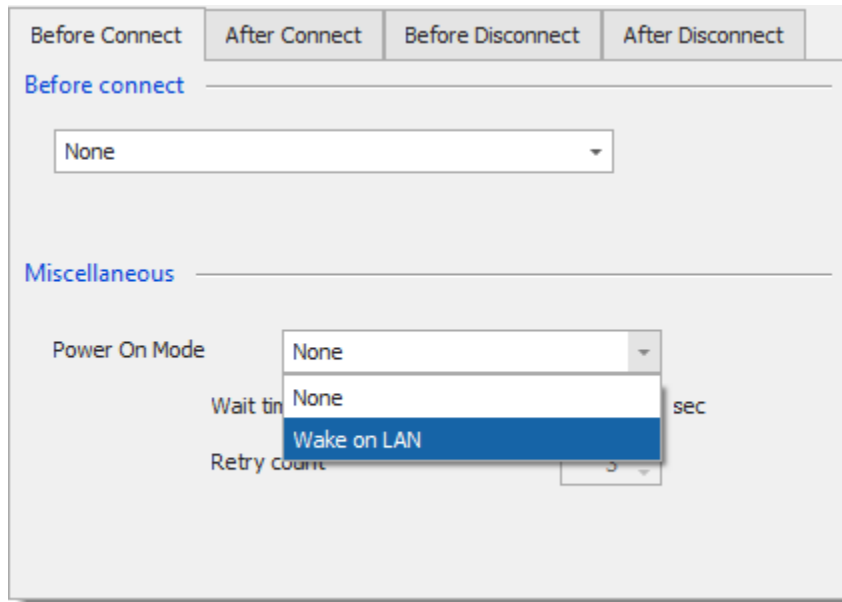
OPTION	DESCRIPTION
<b>None</b>	No script, command line or message prompt is executed.
<b>Script</b>	Select a script file to execute The VBScript (*.vbs) file is the only supported format.
<b>Command Line</b>	Enter a command line to execute.
<b>Message Prompt</b>	Enter a message to display.
<b>Macros/Scripts/Tools</b>	Select a Macros/Scripts/Tools entry from the data source.
<b>PowerShell</b>	Select a PowerShell script from a local drive.
<b>Copy to clipboard</b>	Provide text to copy to the clipboard.

## BEFORE CONNECT – MISCELLANEOUS

The **Miscellaneous** section of the **Before Connect** tab allows to power on the remote device before trying to establish the connection.

Please note that for the Wake-on-LAN feature to work:

- The remote device must support the Wake-on-LAN feature.
- The MAC address must be filled out in the **Information** section of the session properties.



*Before Connect – Miscellaneous*

OPTION	DESCRIPTION
<b>Power On Mode</b>	Enable the Wake-on-LAN.
<b>Wait timeout</b>	Enter the delay before retrying the to wake the remote device.
<b>Retry count</b>	Enter the number of time to try to wake the remote device.

## AFTER CONNECT – MACRO

*Event - After Connect*

This feature simply uses a basic mechanism of sending keystrokes provided by the .NET framework, emulating someone using the keyboard. It sends the keystrokes to the operating system itself, and they are handled by **WHATEVER** application has the focus at that time. If the focus is switched to another window, the credentials will most likely be revealed by being typed in a text area.

**Be advised that using this feature in an environment where passwords must be hidden from the user is highly discouraged.**

OPTION	DESCRIPTION
<b>Execute automatically</b>	Execute the macro automatically when the session is opened.
<b>Initial wait</b>	Enter the delay before the macro is executed.
<b>Type</b>	Select how the macro is executed. Select between: <ul style="list-style-type: none"> <li>• <b>Default:</b> enter a typing macro manually.</li> <li>• <b>Link:</b> select an existing Macros/Scripts/Tools from the data source.</li> </ul>

OPTION	DESCRIPTION
<b>Typing macro</b>	Enter the typing macro to execute. For more information, please consult the <a href="#">Typing Macro</a> topic.
<b>Macro password</b>	Enter a password to prompt for before executing the macro.
<b>Delay time</b>	Enter the delay time for the <b>{DELAY}</b> instruction.
<b>Command</b>	Enter the delay time between each command.

#### 10.1.1.1.1 Typing Macro

## DESCRIPTION

The **Typing Macro** automatically executes once a connection has been established.



This feature simply uses a basic mechanism of sending keystrokes provided by the .NET framework, emulating someone using the keyboard. It sends the keystrokes to the operating system itself, and they are handled by **WHATEVER** application has the focus at that time. If the focus is switched to another window, the credentials will most likely be revealed by being typed in a text area.

**Be advised that using this feature in an environment where passwords must be hidden from the user is highly discouraged.**

*Auto typing macro*

## SETTINGS

### TYPING MACRO

Keyboard keys are represented by predefined tags between braces. To specify a single keyboard character, use the character itself without braces. For example, represent the letter **A** by typing the "A" character in the typing macro. To represent more than one character, such as **Hello**, append each additional character to the preceding one: "Hello".

### SPECIAL KEYS

To specify characters that aren't displayed when you press a key, such as ENTER or TAB, as well as the keys that represents actions rather than characters, refer to the codes in the following table.

KEY	CODE
<b>BACKSPACE</b>	{BACKSPACE}, {BS}, or {BKSP}
<b>BREAK</b>	{BREAK}
<b>CAPS LOCK</b>	{CAPSLOCK}

KEY	CODE
<b>CTRL + ALT + DELETE`</b>	{CTRL-ALT-DEL}
<b>DEL or DELETE</b>	{DELETE} or {DEL}
<b>DOWN ARROW</b>	{DOWN}
<b>END</b>	{END}
<b>ENTER</b>	{ENTER}
<b>ESC</b>	{ESC}
<b>HELP</b>	{HELP}
<b>HOME</b>	{HOME}
<b>INS or INSERT</b>	{INSERT} or {INS}
<b>LEFT ARROW</b>	{LEFT}
<b>NUM LOCK</b>	{NUMLOCK}
<b>PAGE DOWN</b>	{PGDN}
<b>PAGE UP</b>	{PGUP}
<b>PRINT SCREEN</b>	{PRTSC}
<b>RIGHT ARROW</b>	{RIGHT}
<b>SCROLL LOCK</b>	{SCROLLLOCK}
<b>TAB</b>	{TAB}



KEY	CODE
<b>UP ARROW</b>	{UP}
<b>F1</b>	{F1}
<b>F2</b>	{F2}
<b>F3</b>	{F3}
<b>F4</b>	{F4}
<b>F5</b>	{F5}
<b>F6</b>	{F6}
<b>F7</b>	{F7}
<b>F8</b>	{F8}
<b>F9</b>	{F9}
<b>F10</b>	{F10}
<b>F11</b>	{F11}
<b>F12</b>	{F12}
<b>F13</b>	{F13}
<b>F14</b>	{F14}
<b>F15</b>	{F15}
<b>F16</b>	{F16}

KEY	CODE
<b>Keypad add</b>	{ADD}
<b>Keypad subtract</b>	{SUBTRACT}
<b>Keypad multiply</b>	{MULTIPLY}
<b>Keypad divide</b>	{DIVIDE}

To specify keys combined with any combination of the SHIFT, CTRL, and ALT keys, precede the key code with one or more of the following signs.

KEY	CODE
<b>SHIFT</b>	+
<b>CTRL</b>	^
<b>ALT</b>	%

To specify that any combination of SHIFT, CTRL, and ALT should be held down while several other keys are pressed, enclose the code for those keys in parentheses. For example, to specify to hold down SHIFT while E and C are pressed use "+(EC)". To specify to hold down SHIFT while E is pressed, followed by C, without SHIFT, use "+EC".

## SPECIAL COMMANDS

COMMANDS	DESCRIPTION
<b>{DELAY}</b>	This command introduces a delay of 300 ms (default value) before the next command.
<b>{WINDOW:???</b>	This command focus a window containing the specified name after the semi colon.

COMMANDS	DESCRIPTION
<b>{PREV-WINDOW}</b>	Select the previous window before executing the remaining commands.

## MACRO PASSWORD

You can define a password to be use within the typing macro exclusively. Use the variable **\$MACRO\_PASSWORD\$** to access the password.

### 10.1.1.2 Wake-on-LAN

## DESCRIPTION

Wake-on-LAN is an Ethernet computer networking standard, which allows a computer to be turned on or woken up by a network message. This is an OS-agnostic feature that works by broadcasting a specially crafted “magic” packet at the data link layer. The target computer sits in a low-power state with only its network card switched on, and when it receives the magic packet, the network card “wakes up” the computer, powering it on and booting it up.

Wake-on-LAN is supported in the Enterprise edition of Remote Desktop Manager. Plus, the destination motherboard must support it, and it must be enabled. The computer must also be in the local area network (LAN) and not connected in a VPN.

An important thing to note is that Wake-on-LAN operates below the IP level. This means that the sending machine needs to be on the LAN, so we cannot send them over remote IP-based connections, such as over SSH or VPN. WOL broadcasts packets to the target computer over UDP. You can configure which port it uses, the default is 9. If you want to wake up a machine on a different subnet, your router must forward UDP port 9, or whatever you change the port assignment to. Most users do not have to configure their router or worry about this.

## ENABLING WAKE-ON-LAN

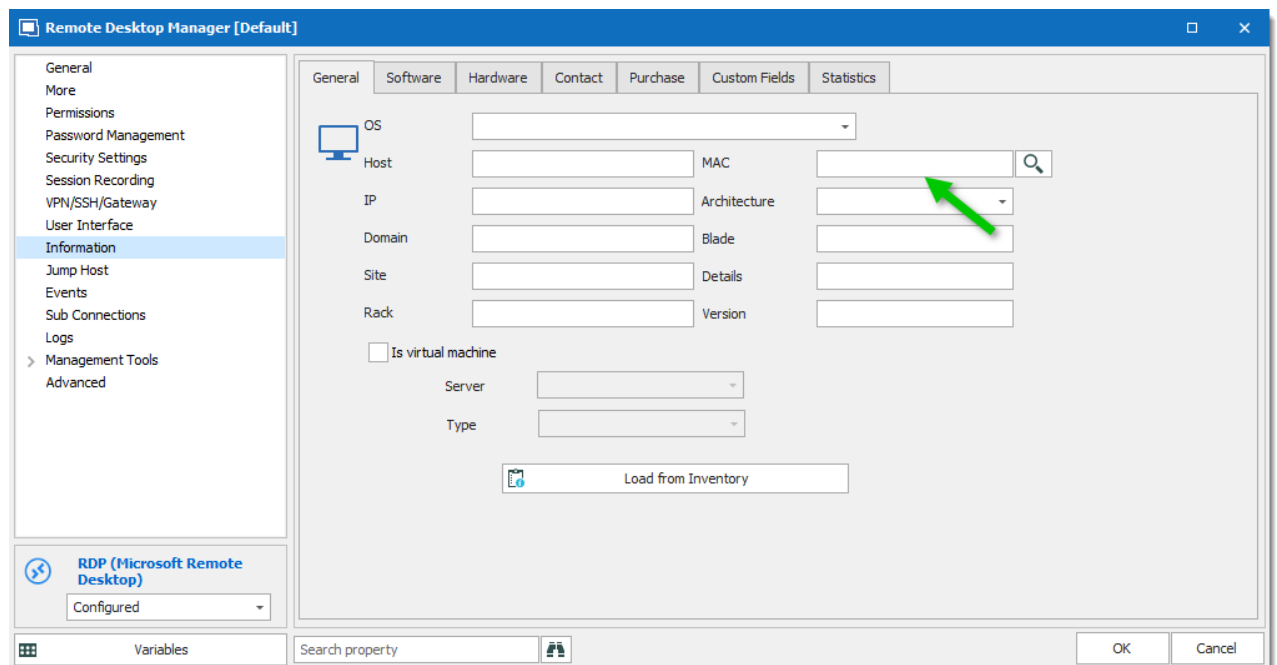
The first step is to verify that your computer supports Wake-on-LAN. There’s a few things to look out for:

- Your network card must support Wake-on-LAN.
- Your power supply must support Wake-on-LAN.
- Wake-on-LAN must be enabled in BIOS.

- Your router must be configured to forward broadcast packets.
- Your OS must be configured to enable Wake-on-LAN.

## CONFIGURE REMOTE DESKTOP MANAGER

You must add a valid MAC address (Media Access Control address) in the session's configuration. The input field can be found in the **Information** tab and in the **General** child tab. The field name is MAC.



The screenshot shows the 'Remote Desktop Manager [Default]' window. On the left is a sidebar with a tree view containing 'General', 'More', 'Permissions', 'Password Management', 'Security Settings', 'Session Recording', 'VPN/SSH/Gateway', 'User Interface', 'Information' (highlighted), 'Jump Host', 'Events', 'Sub Connections', 'Logs', 'Management Tools', and 'Advanced'. Below the sidebar is a section for 'RDP (Microsoft Remote Desktop)' with a 'Configured' dropdown. The main area has tabs for 'General', 'Software', 'Hardware', 'Contact', 'Purchase', 'Custom Fields', and 'Statistics'. The 'General' tab is active, showing fields for 'OS' (dropdown), 'Host' (text), 'IP' (text), 'Domain' (text), 'Site' (text), 'Rack' (text), 'MAC' (text with a search icon), 'Architecture' (dropdown), 'Blade' (text), 'Details' (text), and 'Version' (text). There is also a checkbox for 'Is virtual machine', 'Server' (dropdown), and 'Type' (dropdown). At the bottom of the main area is a 'Load from Inventory' button. The bottom status bar includes 'Variables', 'Search property', and 'OK'/'Cancel' buttons. A green arrow points to the 'MAC' input field.

### Session configuration - Wake-on-LAN

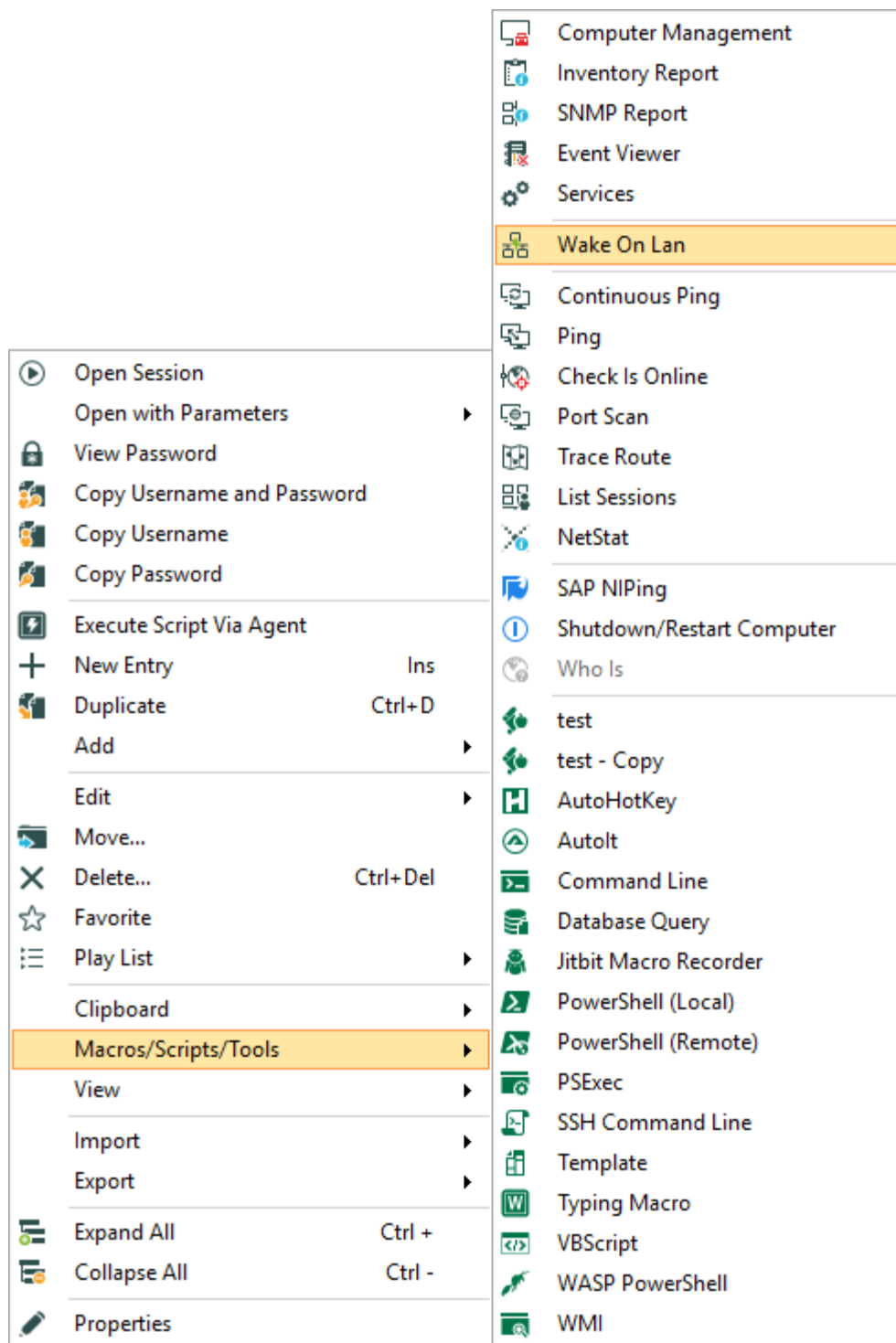
You can use the Ellipsis button to automatically determine the MAC address. If this is unsuccessful, you will need to enter it manually.

## ABOUT THE MAC ADDRESS DISCOVERY

The discovery process will initially attempt to use the ARP protocol. This is fast and does not require authentication, but there are requirements on the network aspect that may not be met. If ARP was not successful, another attempt is made using WMI. This is slower and requires authentication. RDM will use the credentials as configured in the entry's properties or the credentials entered in the Management Tools tab.

## USE WAKE-ON-LAN

If the settings are correctly configured, you can invoke the Wake-on-LAN from the session's context menu, which can be found in the **Macros/Scripts/Tools - Wake-on-LAN** menu.



Session tools - Wake-on-LAN

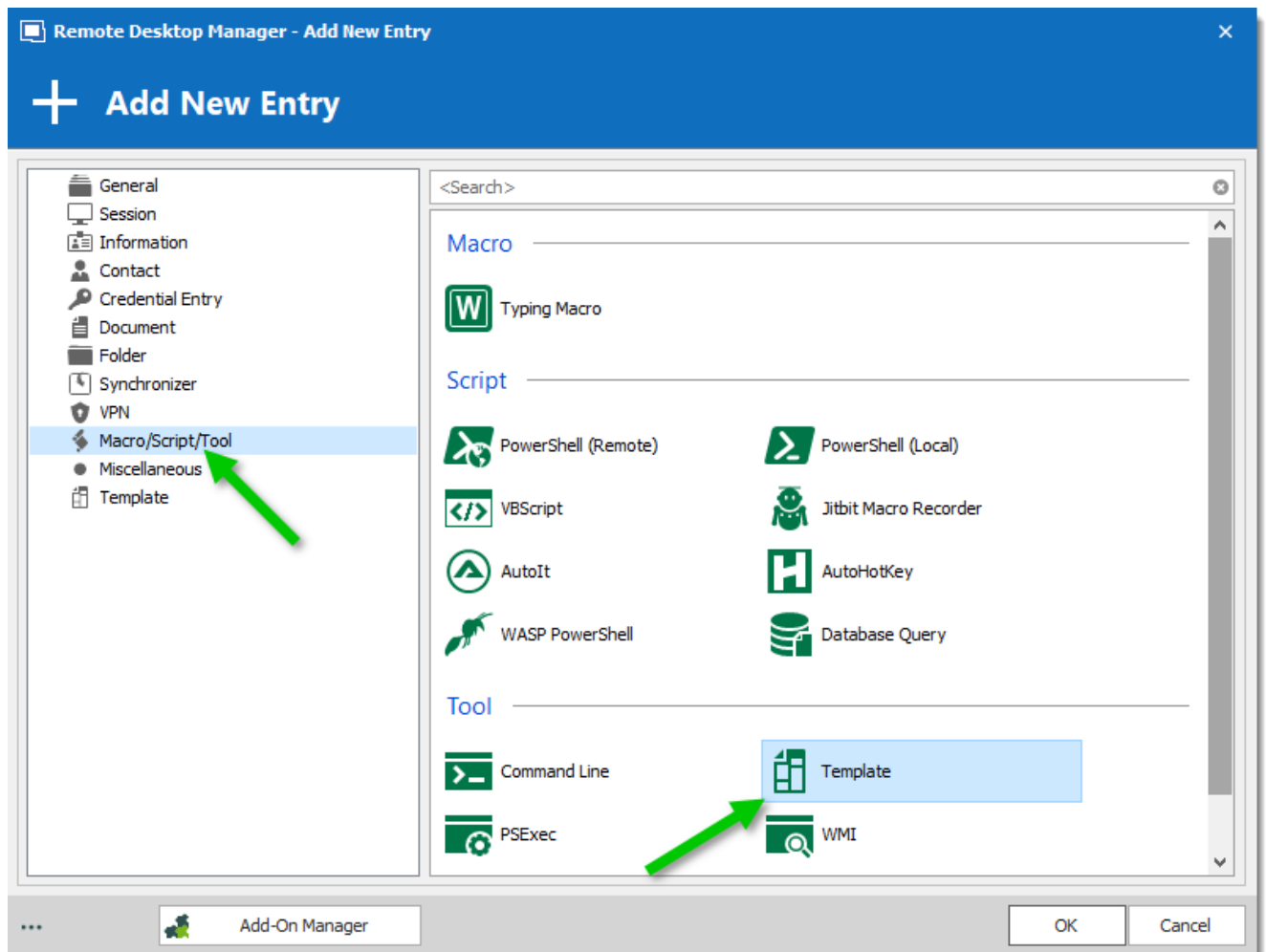
### 10.1.1.3 Add a web link in Macros/Scripts/Tools Session

## DESCRIPTION

Macros/Scripts/Tools sessions can be used to open web links in Remote Desktop Manager.

## CREATE THE EMBEDDED WEB LINK

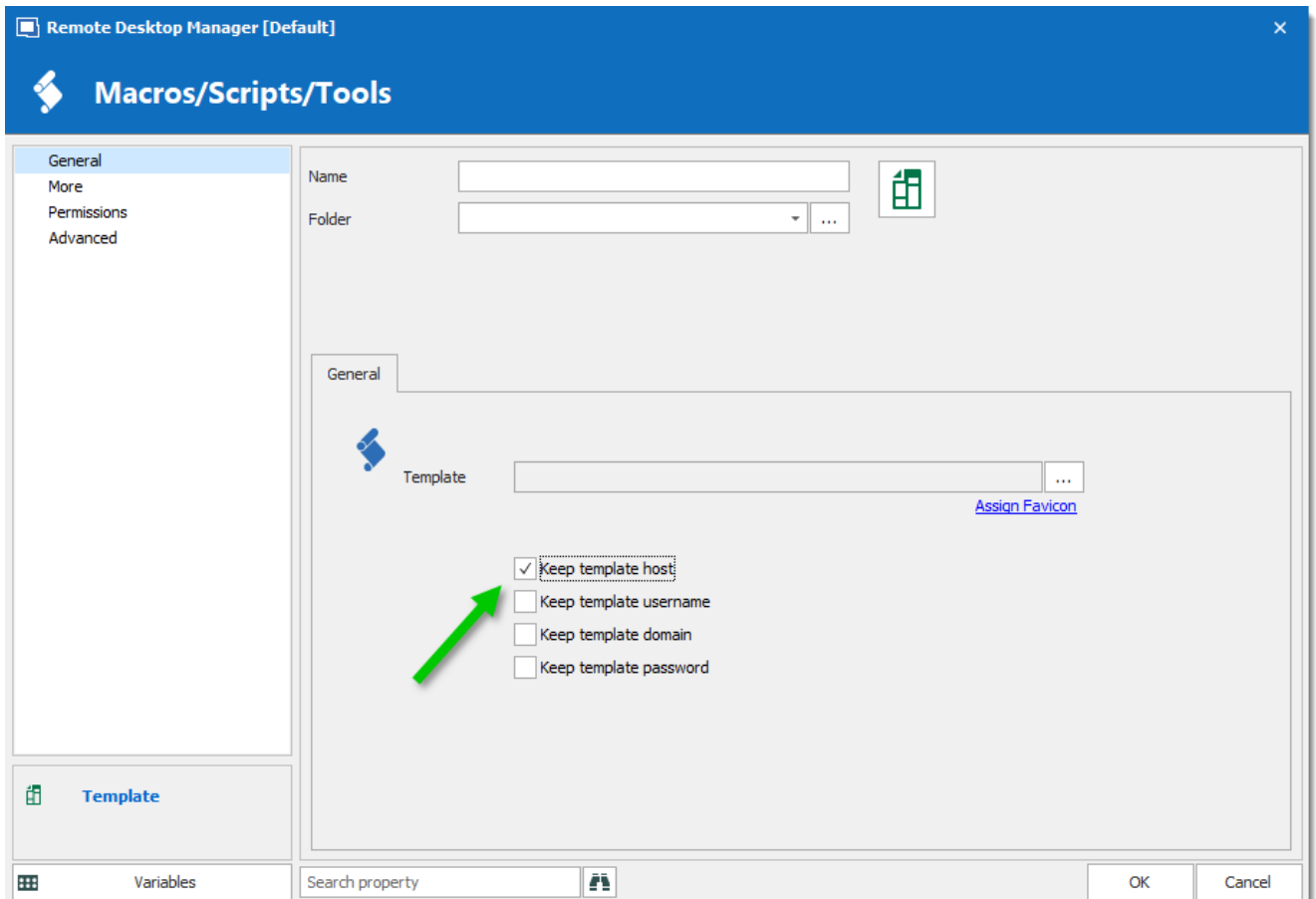
1. Create a **shared web session** [Template](#).
2. Once the template is created, add a new entry **Macros/Scripts/Tools – Template**.



3. Assign the new template to your newly created Macros/Scripts/Tools session using the ellipsis button.



Make sure to check the **Keep template host** option.



#### 10.1.1.4 Configure VPN for multiple sessions

## DESCRIPTION

Remote Desktop Manager automates opening a VPN when launching a remote session. This configuration is well suited to situations where you need one VPN for a group of servers at a remote location. This procedure sets the VPN configurations on the folder and the entries inherit the settings.

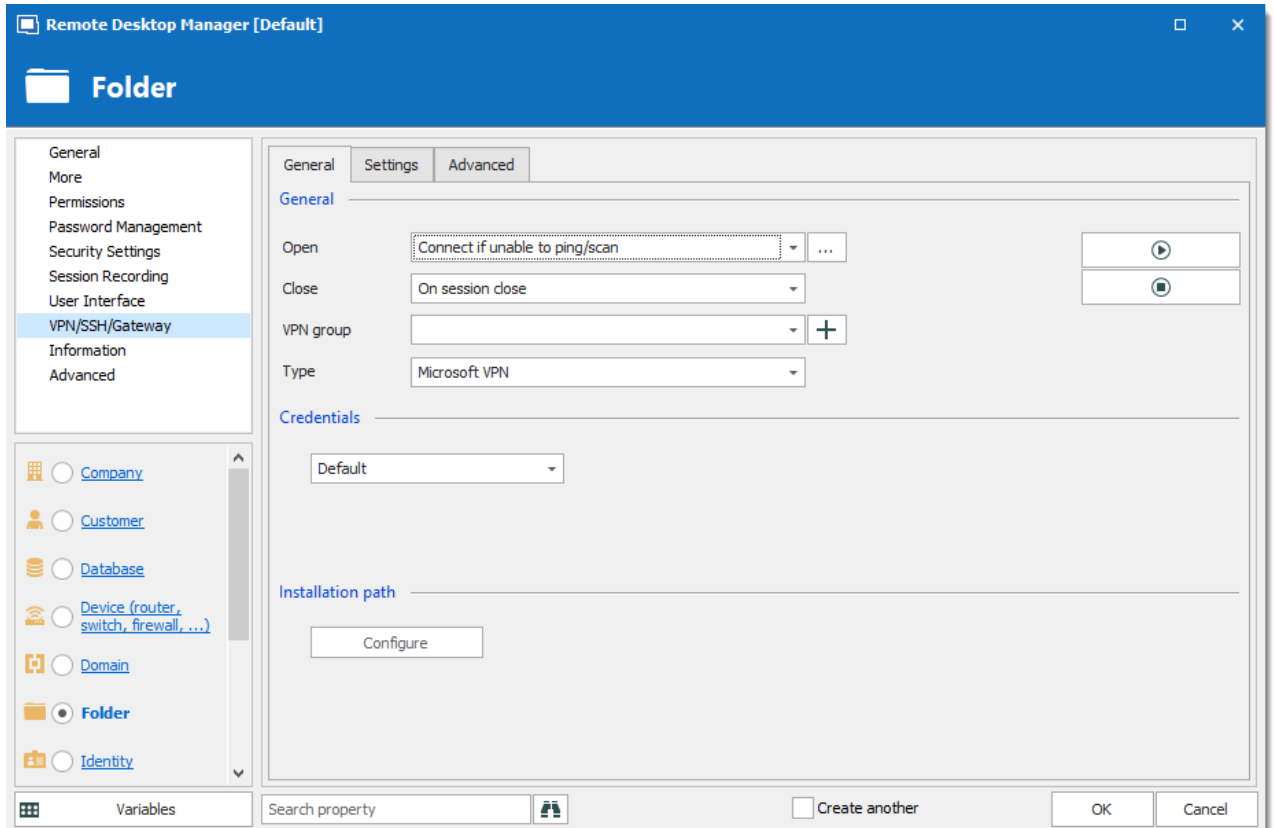
## STEPS



Before following the steps below, create a VPN entry and remote session entries, then place these entries in a folder. For more information about VPN entries, consult the VPN topic.

## CONFIGURE THE VPN SETTINGS ON THE FOLDER ENTRY

1. Select the folder and open its **Properties** then select **VPN/SSH/Gateway** from the menu on the left.



*Folder properties - VPN/SSH/Gateway*

2. In the **Open** list, select how the VPN opens when you launch a remote session. We recommend choosing **Connect if unable to ping/scan** on the folder, later we'll set **Inherited** for each session entry.

OPTION	DESCRIPTION
<b>None</b>	VPN does not open when the session is opened.
<b>Always connect</b>	VPN opens when the session is opened.

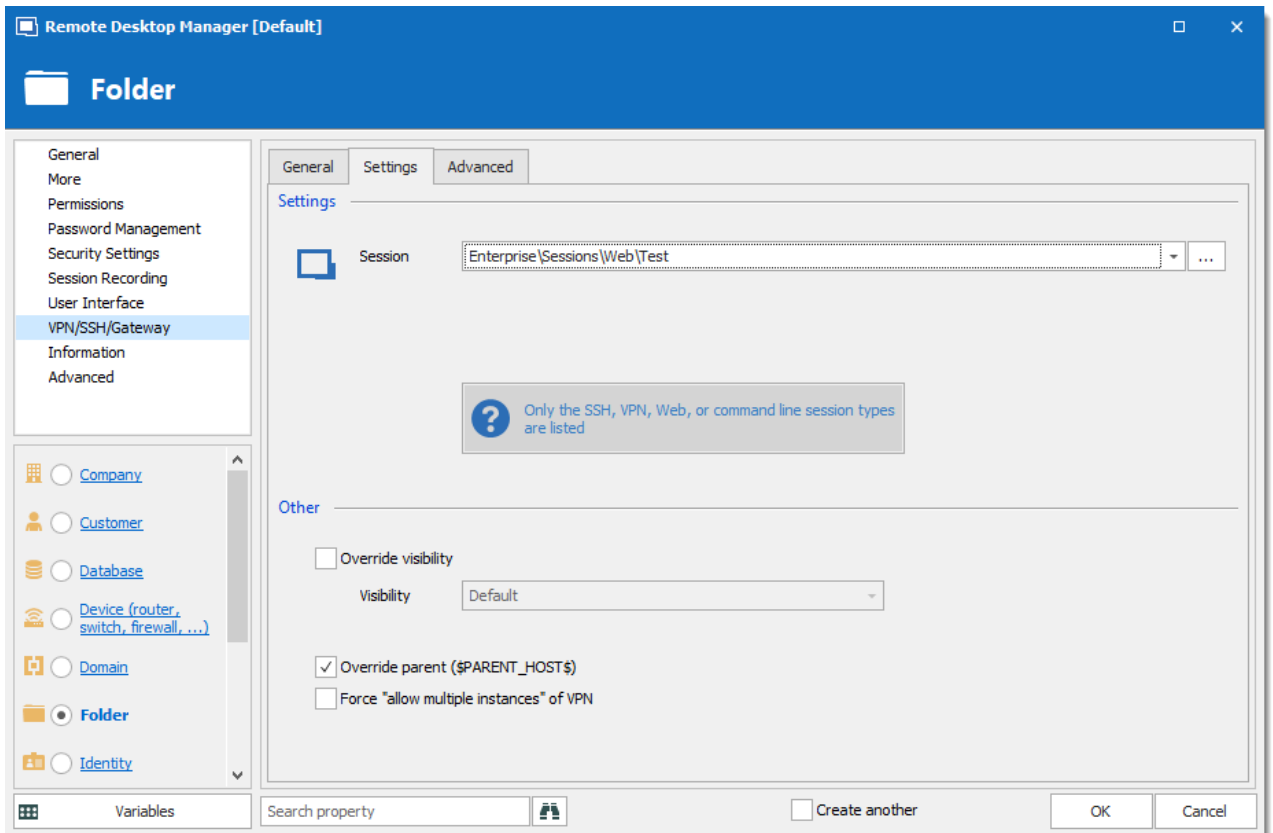
OPTION	DESCRIPTION
<b>Manual</b>	VPN requires user to manually activate the VPN before opening the session.
<b>Connect if unable to ping/scan</b>	Remote Desktop Manager tests if the host responds, if not the VPN opens.
<b>Inherited</b>	VPN inherits the settings.
<b>Ask for confirmation</b>	VPN prompts for confirmation before opening.
<b>Connect if network adapter not found</b>	Remote Desktop Manager tests if network adapter is installed and active, if not the VPN opens.
<b>Prompt if unable to ping/scan</b>	Tests if the host responds, if not VPN prompts for confirmation before opening.

3. In the **Close** list, select how the VPN closes at the end of a remote session. We recommend **On session close**.

OPTION	DESCRIPTION
<b>On session close</b>	VPN closes automatically when the session is closed.
<b>Manually Later</b>	VPN requires user to manually close the VPN entry when finished.
<b>Confirm disconnect</b>	VPN prompts to close the VPN when session is closed.

4. Create a **VPN group** so the VPN only closes when the last session in the **VPN group** is closed.
  - 4.1 Click the plus sign to add a new **VPN group**, then enter a group name.

5. In the **Type** list, click **Session**.
6. Click the **Settings** tab.

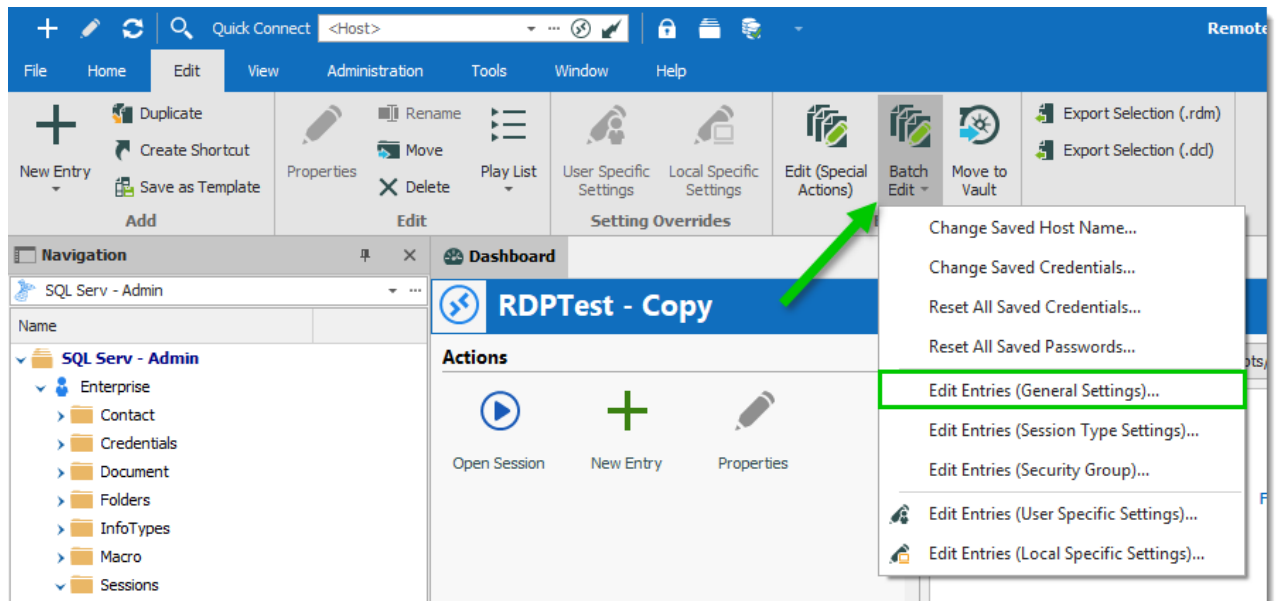


*Folder Properties - VPN/SSH/Gateway - Settings*

7. In the **Session** list, select the VPN entry you created.

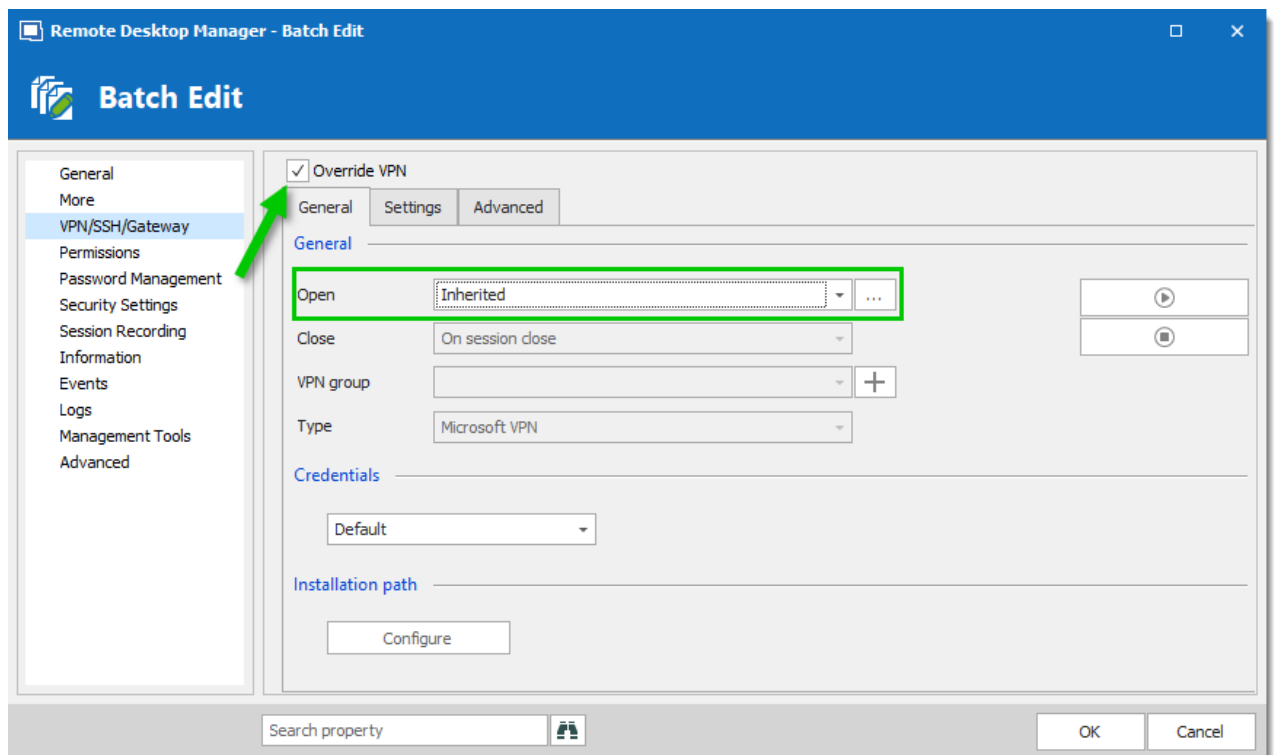
## PERFORM A BATCH EDIT TO CONFIGURE THE SESSION ENTRIES

1. Select the session entries in the folder.
2. On the **Edit** tab, click **Batch Edit**, then select **Edit Entries (General Settings)**. **Batch Edit** is also available in the right-click context menu.



*Batch Edit - Edit Entries (General Settings)*

3. On **VPN/SSH/Gateway**, select **Override VPN** box.

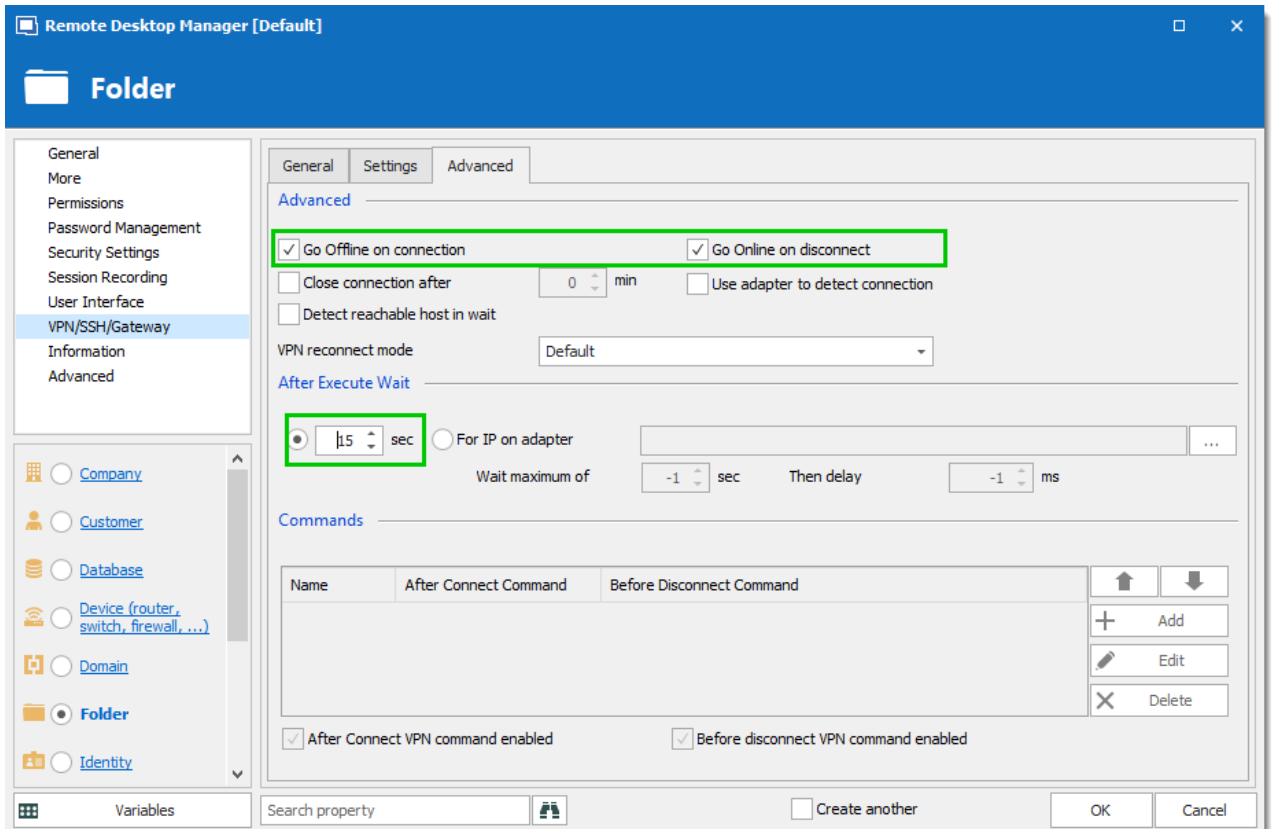


*Batch Edit - VPN/SSH/Gateway*

4. Select **Inherited** in the **Open** list. It will set all the **General** options to **Inherited**.

## SETTINGS FOR SPECIFIC SITUATIONS

There are many options to accommodate a range of VPN types. Below are two common situations and options to make using the VPN more efficient.



*VPN/SSH/Gateway - Advanced*

1. You lose connection to the data source when the VPN is active.

Automate going offline when the VPN opens.

Select **Go Offline on connection** and **Go Online on disconnect** check boxes.

2. The VPN is slow to connect.

You can adjust the time Remote Desktop Manager waits for the VPN to open.

In the **sec** box, enter the a time in seconds.

**-1 sec** is the default time (5 seconds). Change the default time for all VPN entries in **File – Options – Types – VPN – VPN default pause**.

### 10.1.1.5 Import Credentials From Keepass

## DESCRIPTION

Remote Desktop Manager imports credentials from Keepass. It is a simple way to build your data. The imported information can be converted into three types of entry: **Username/Password** and **Website**. The entries include credentials, url addresses and notes.

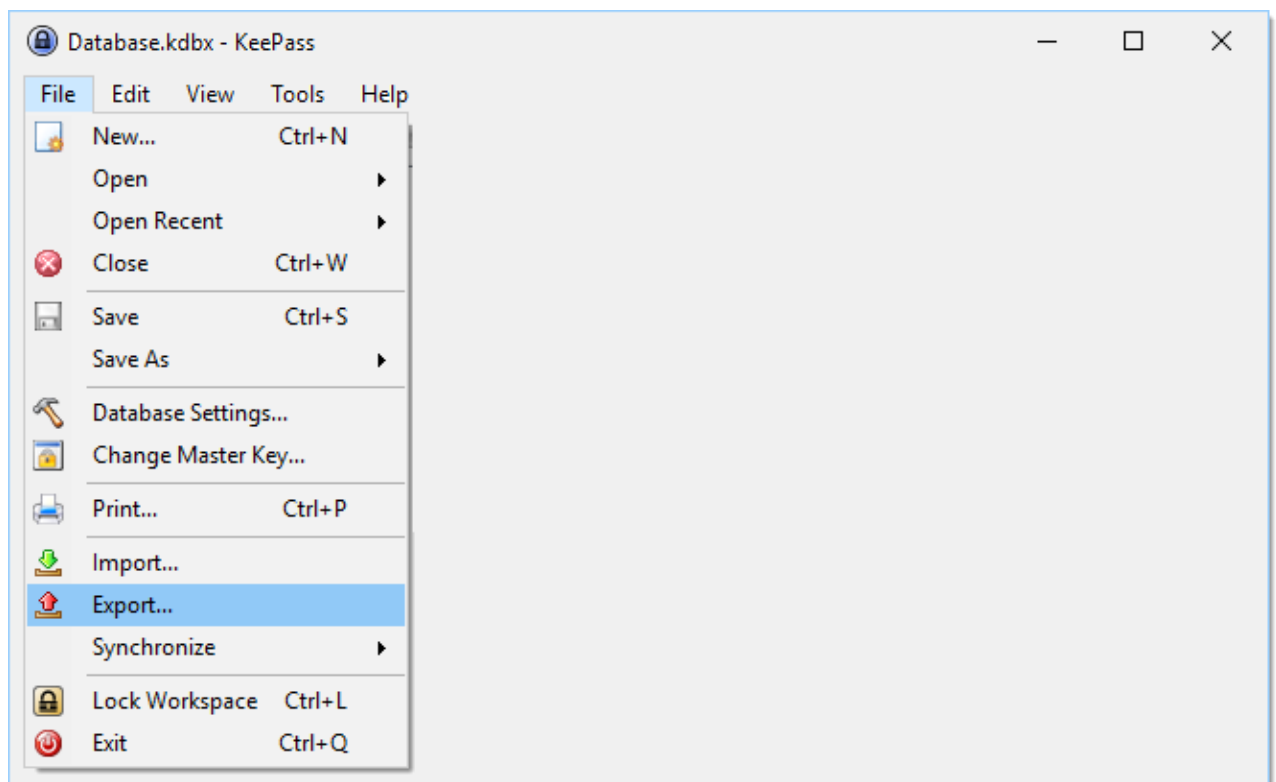
## HOW TO IMPORT VARIOUS ENTRIES

*Step-by-step instructions to import credentials and websites from Keepass*

## PROCEDURE

### EXPORT ENTRIES FROM KEEPASS

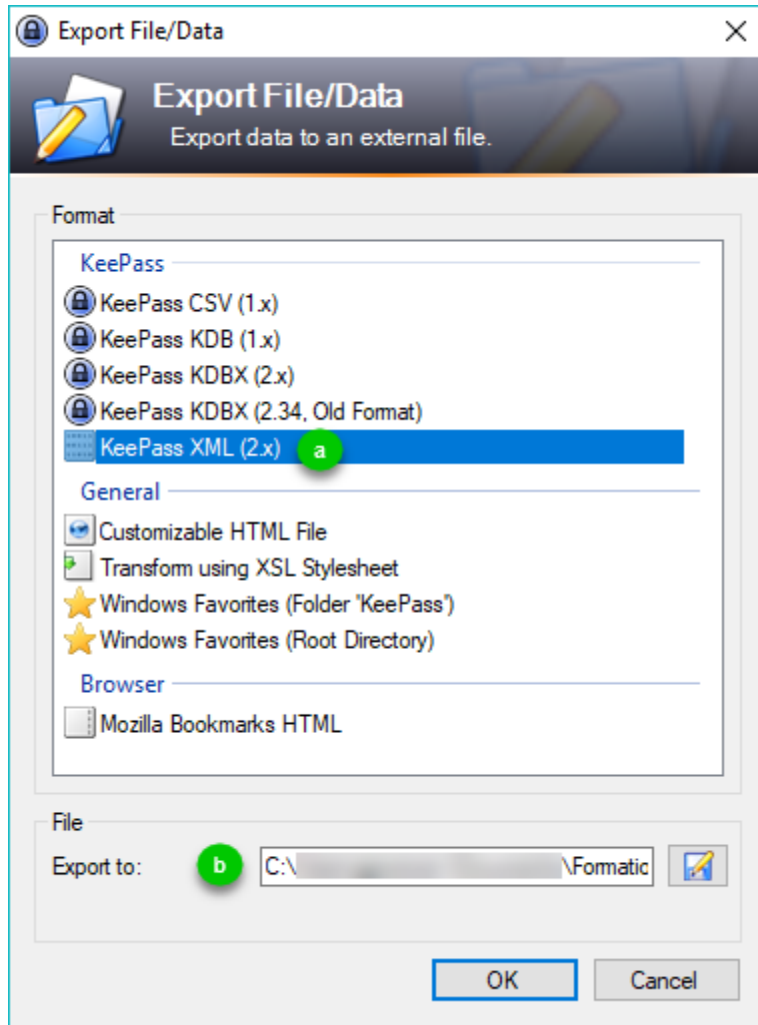
1. In the **File** menu, click **Export**.



*KeePass - File - Export*

2. Export Data to an external file. RDM supports two file types for KeePass: XML and CSV. An XML file will retain the folder structure from KeePass.

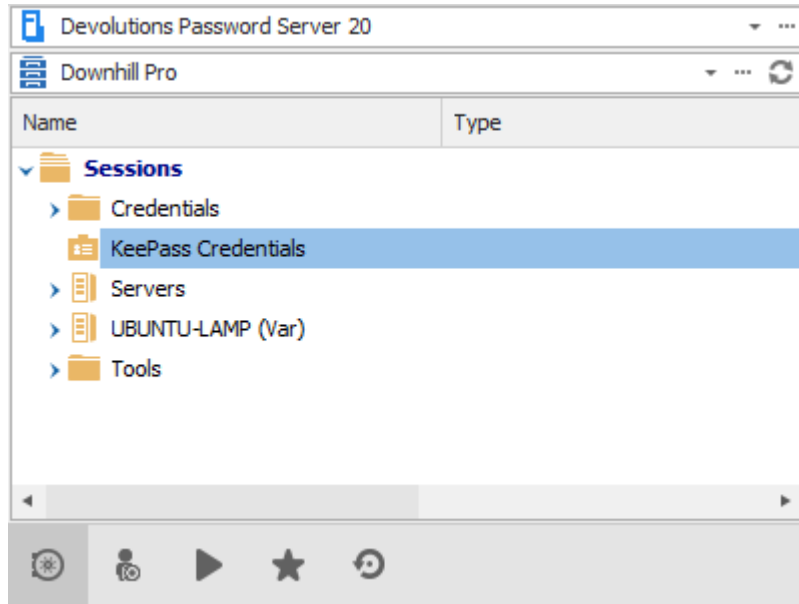
- a) Choose desired file type: **KeePass CSV (1.x)** or **KeePass XML (2.x)**
- b) Select path to save the exported file.



*KeePass - Export Data*

## IMPORT DATA INTO REMOTE DESKTOP MANAGER

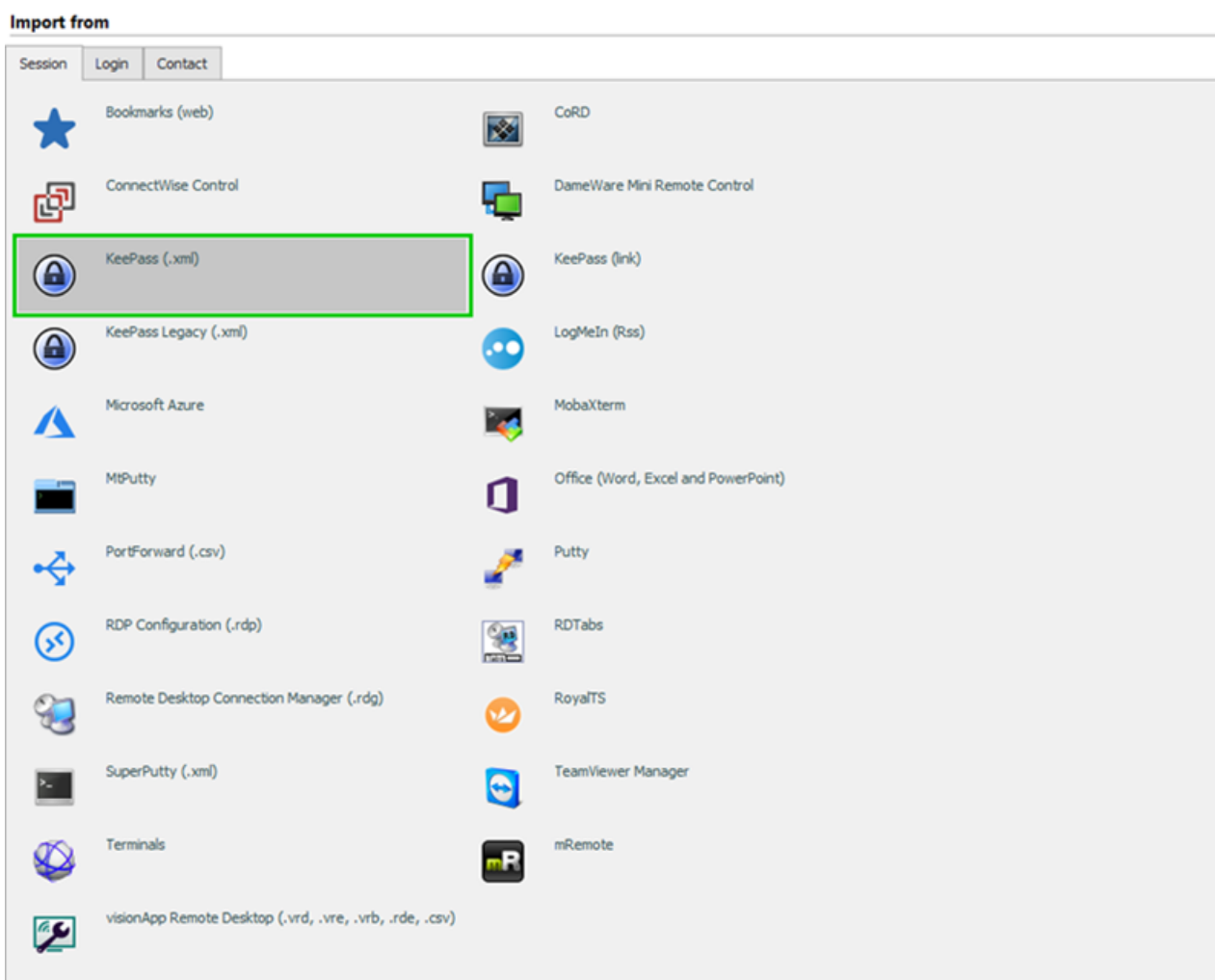
1. The data is imported into the currently selected folder.



2. Choose the file type to import in ***File – Import.***

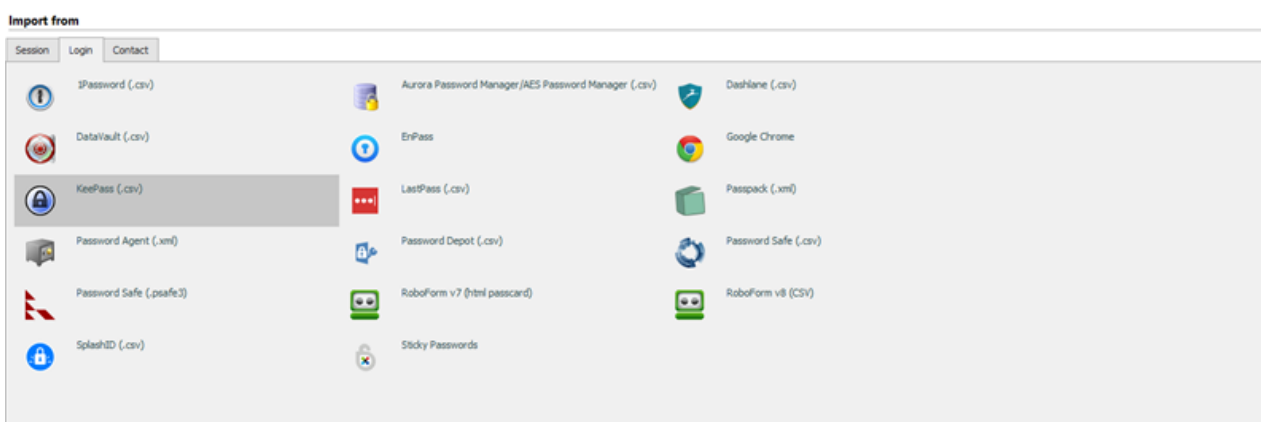
2.1 To import an xml file, choose **Import from Session.**





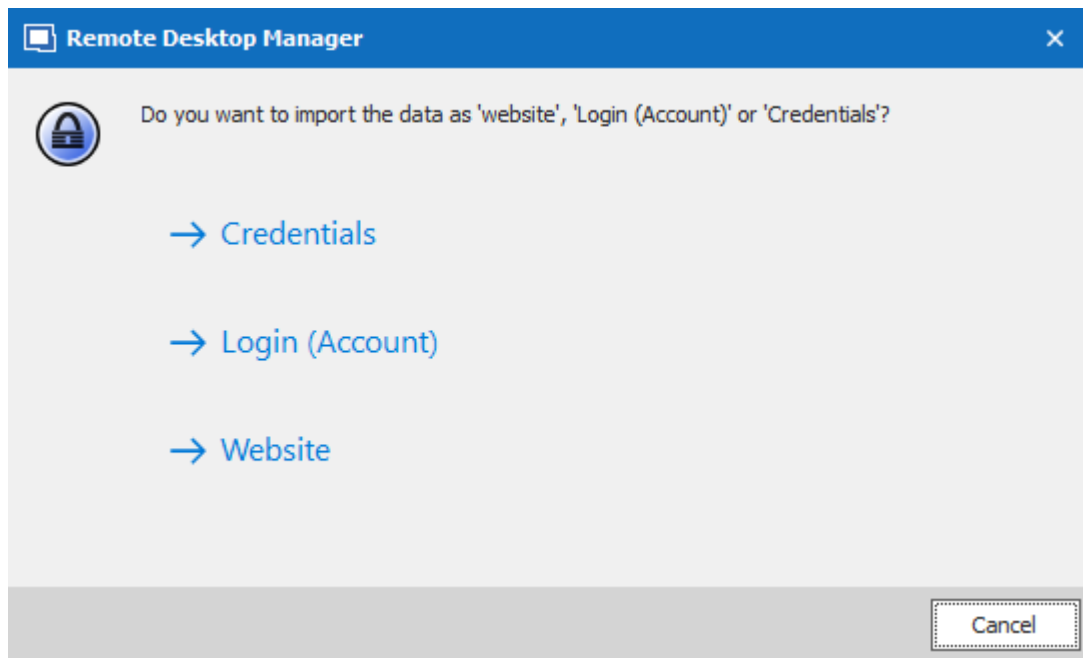
*File – Import from Session (XML)*

2.2 To import a csv file, choose **Import from Login**.



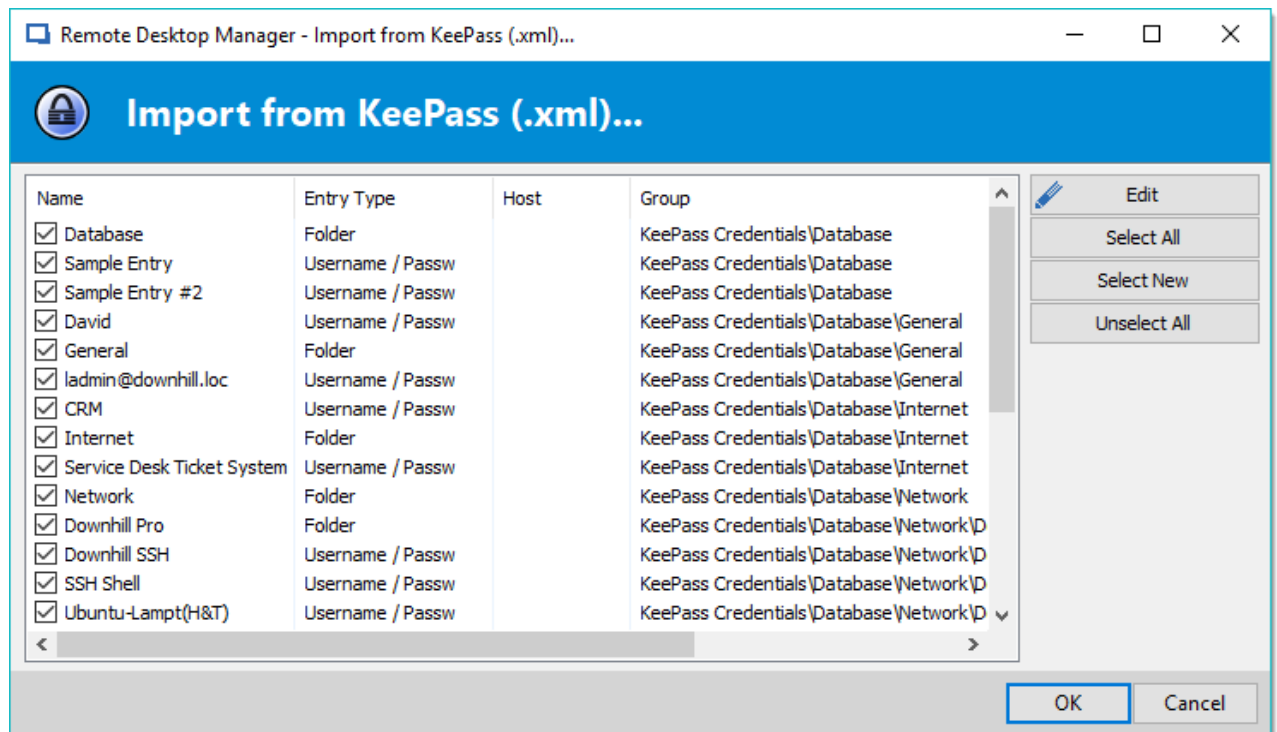
*File - Import from Login (CSV)*

3. Choose an entry type. All imported entries are converted to this type.

*Entry Type - Imported Data*

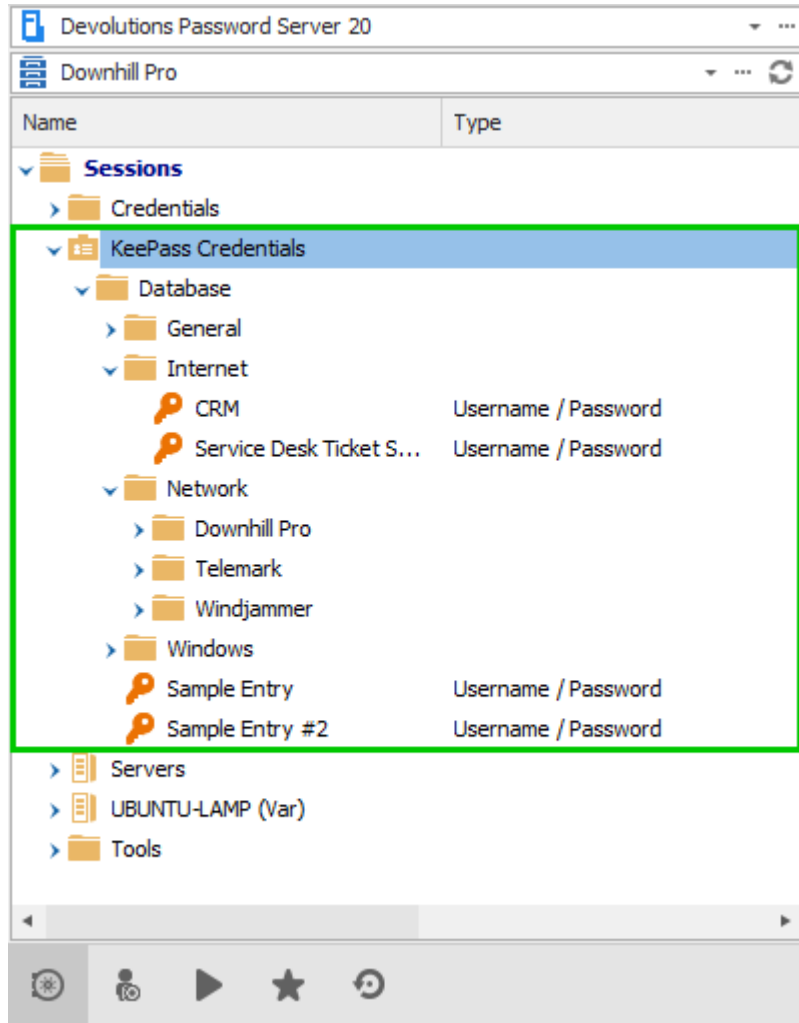
OPTION	DESCRIPTION
<b>Credentials</b>	Includes username, password and domain.
<b>Website</b>	Includes username, password, and website address. Good choice for website information and can be used with Devolutions Web Login. Has more settings for default web browser, display, credentials and security questions.

4. Select the KeePass exported file in the file explorer and click **Open**.
5. Choose the entries you want to import.



*Import entries from KeePass*

6. The imported entries are ready to use.



*Imported KeePass entries in Remote Desktop Manager*

#### 10.1.1.6 Import and Export

### DESCRIPTION

To simplify deployment for multiple users, it is possible to import and export data sources, entries, and even the application's configuration. Configure the application once, with data sources, entries, and options. Export any of these configurations, then import them in another Remote Desktop Manager instance.



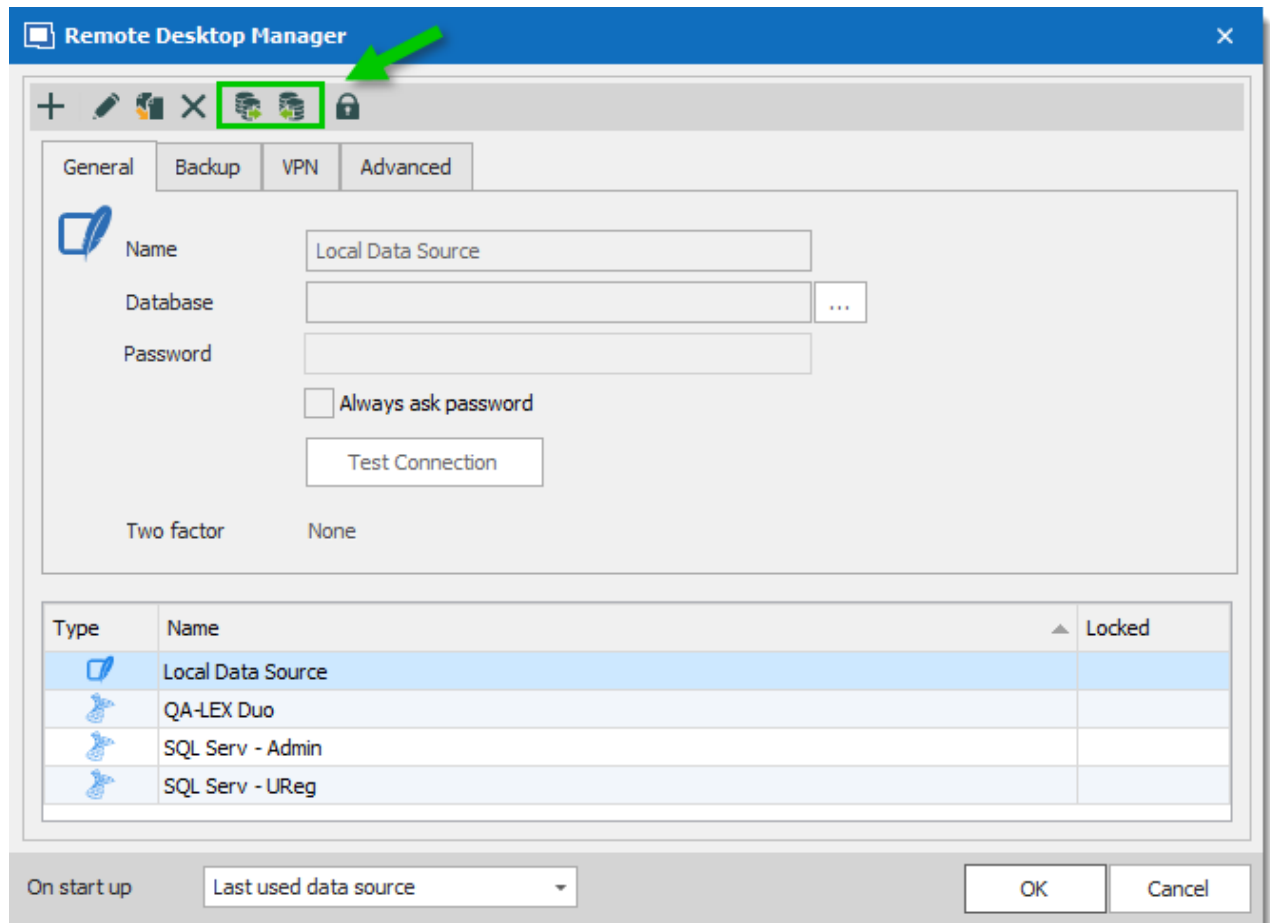
Instead of exporting/importing data sources and options separately, it is possible to create a custom installer. Our Custom Installer Service replicates the configuration of a Remote Desktop Manager instance.

## HOW TO EXPORT ENTRIES FROM RDM

*Export entries from RDM and into My Private Vault DPS*

### DATA SOURCES

Only the data source configuration is exported. The resulting .rdd file does not contain the database content. It contains only the configuration used to connect to the database. From **File – Data Sources**, click on the **Export Data Source Configuration...** button, then save the \*.rdd file on your computer.



*Data Sources - Import and Export*

To import the data source in another Remote Desktop Manager instance, use **File – Data Sources**, and click on the **Import Data Source Configuration** button.



A locked data source can be exported and imported, but the content will be locked unless a password is entered when the data source is selected. See [Lock Data Source](#) for more information.

## ENTRIES

Entries configuration can be exported to save the time of creating the same set of entries for multiple users. There are many ways of exporting entries. The only formats allowed to import entries previously exported from Remote Desktop Manager are .rdm, and .xml.

Export a set of entries:

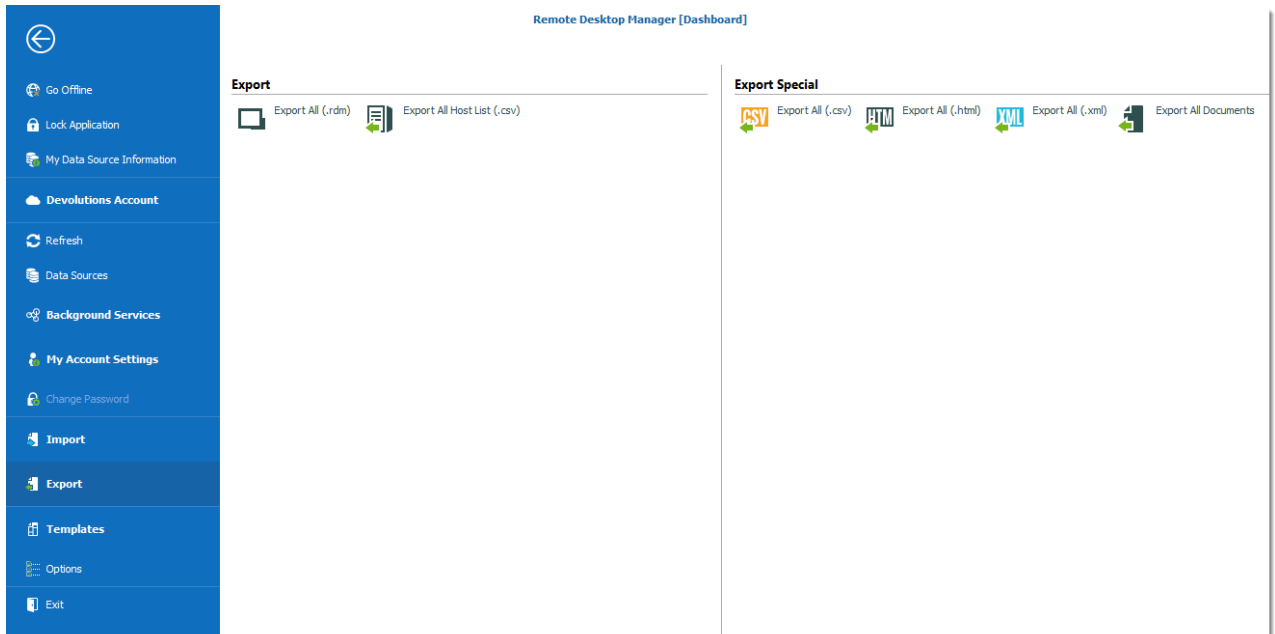
OPTION	DESCRIPTION
<b>Export Selection</b>	Select one entry or more, then right-click the selection. In the context menu, under <b>Export</b> , select <b>Export Selection (.rdm)...</b>
<b>Export Special</b>	Select one entry or more, then right-click the selection. In the context menu, under <b>Export – Export Special</b> , select the desired export format.
<b>Export as RDP</b>	Select one RDP entry, then right-click the selection. In the context menu, under <b>Export</b> , select <b>Export Entry as Remote Desktop File (.rdp)...</b>

Export all entries:

OPTION	DESCRIPTION
<b>Export All Entries</b>	Right-click an entry in the Navigation Pane. In the context menu, under <b>Export</b> , select <b>Export All Entries (.rdm)...</b>
<b>Export Special</b>	Right-click an entry in the Navigation Pane. In the context menu, under <b>Export – Export Special</b> , select the desired export format.
<b>Export All Host</b>	Right-click an entry in the Navigation Pane. In the context menu, under <b>Export</b> , select <b>Export All Hosts List (.csv)...</b>

OPTION	DESCRIPTION
<b>Export All Documents</b>	Right-click an entry in the Navigation Pane. In the context menu, under <b>Export – Export Special</b> , select <b>Export All Documents...</b>

The functionalities for exporting all entries are also available in the **File – Export** Menu.

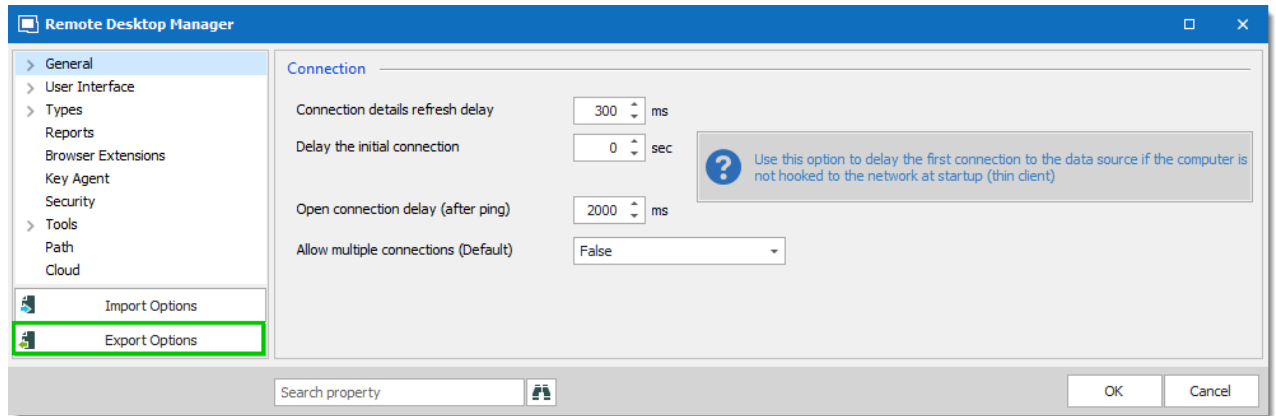


*File - Export*

## APPLICATION CONFIGURATION

The application's configuration can be exported to replicate the configuration in other Remote Desktop Manager instances.

Use **File – Options – Export Options**, and save the RemoteDesktopManager.cfg file on your computer.



*File - Options - Export Options*

To import the configuration, use File - Options - Import Options, and select the exported RemoteDesktopManager.cfg. You can also copy the file to the installation directory of another Remote Desktop Manager instance.

#### 10.1.1.7 Multiple Types of Connections to a single computer

## DESCRIPTION

You have hosts for which you need to use many different remote access technologies (ex: RDP, SSH, Web, etc).

There are three solutions to this scenario:

1. [Ad-hoc Launch with a Template](#)
2. [Folders and Dynamic Variables](#)
3. [Host with Templates](#)

##### 10.1.1.7.1 Ad-hoc Launch with a Template

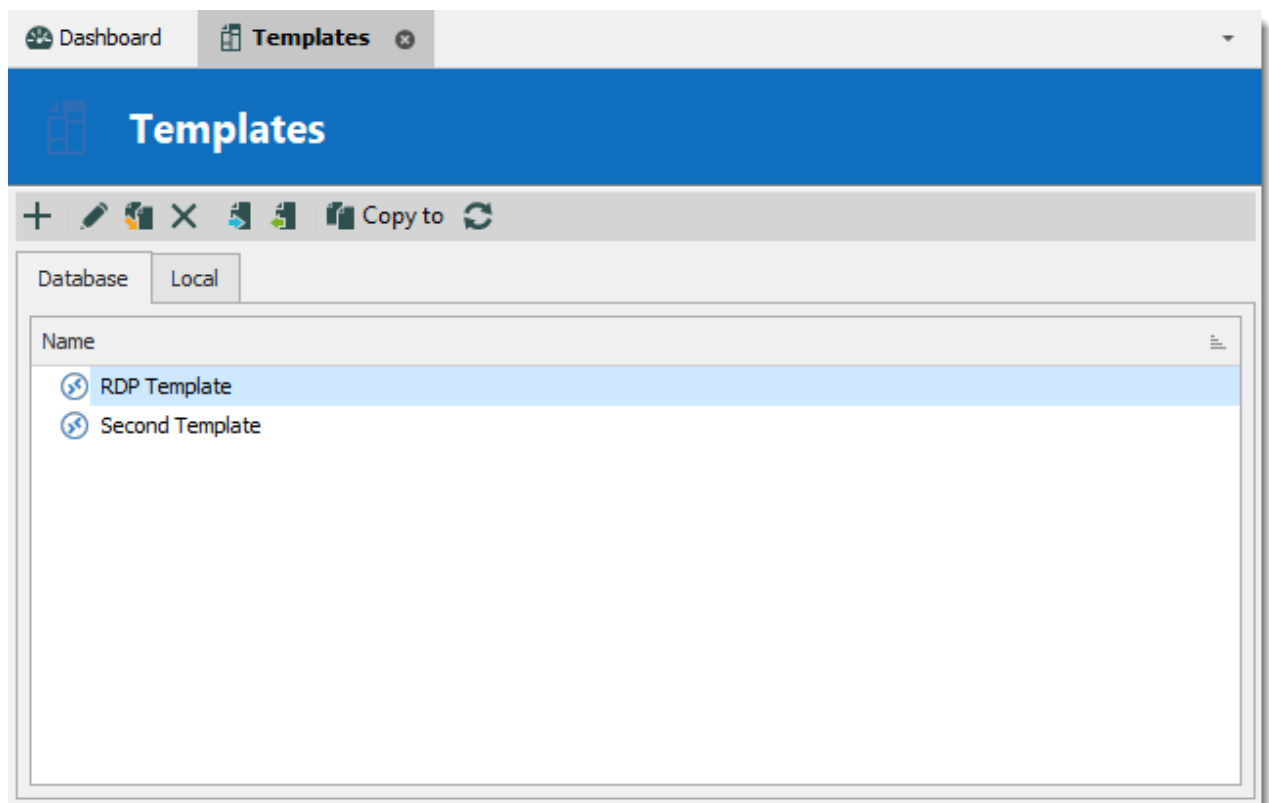
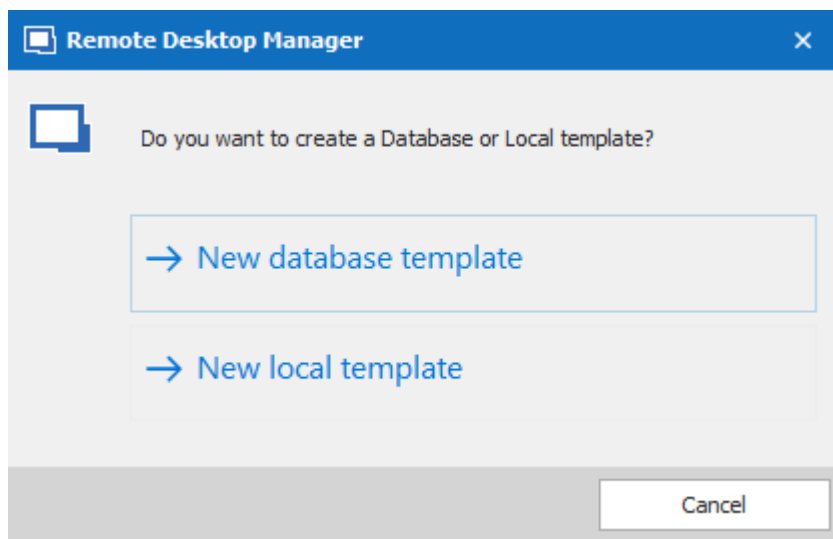
## DESCRIPTION

This method uses a dashboard command that is available on all sessions. It's a good fit for a scenario where you usually connect with a specific technology, but occasionally need to use another.

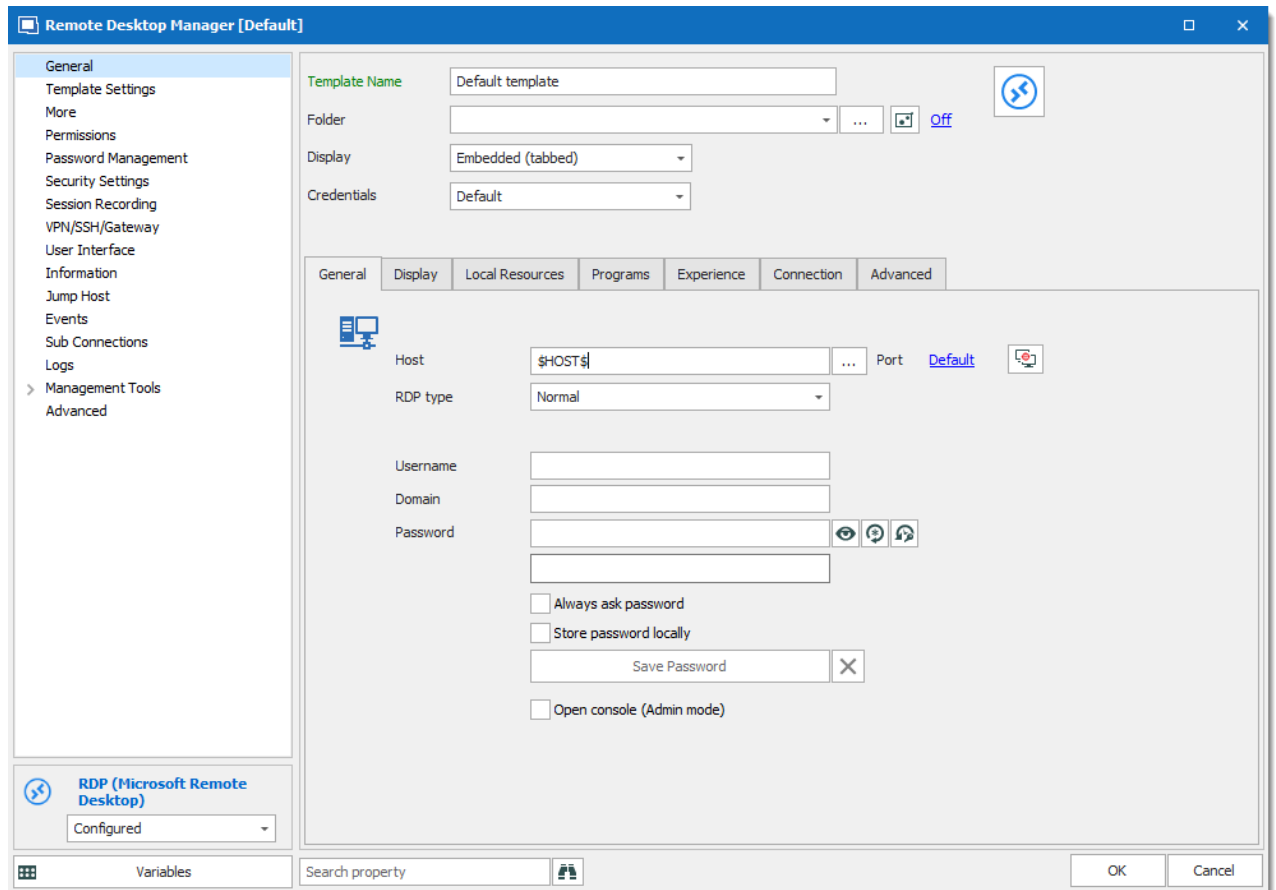
## SETTINGS

1. Create a local or database template in **File – Templates – Templates**.



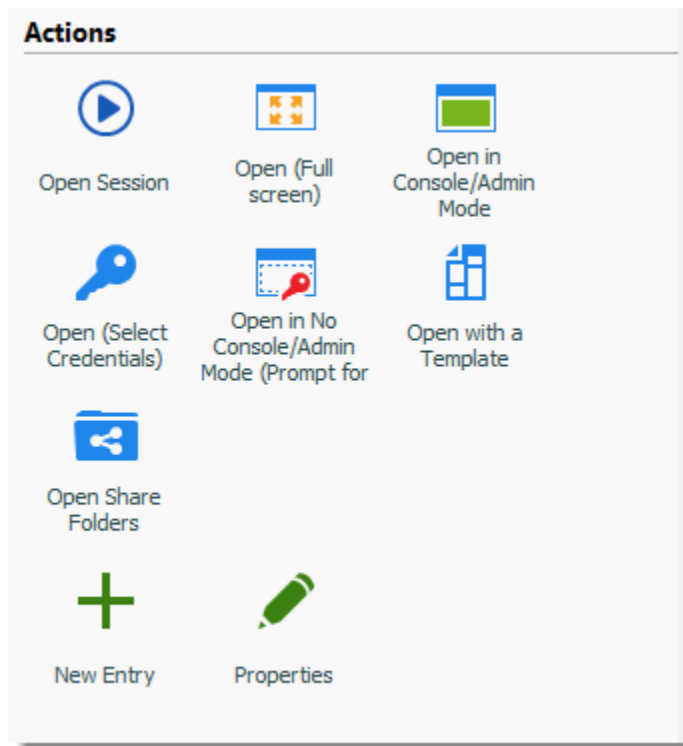
*Templates**Create Template*

2. In the computer field, use the **\$HOST\$** variable and click on **OK**.



*Default Template*

3. In the case that you need to launch a session using a template, click on **Open with a Template** in the **Dashboard** and select the appropriate template



*Open with a Template*

#### 10.1.1.7.2 Folders and Dynamic Variables

## DESCRIPTION

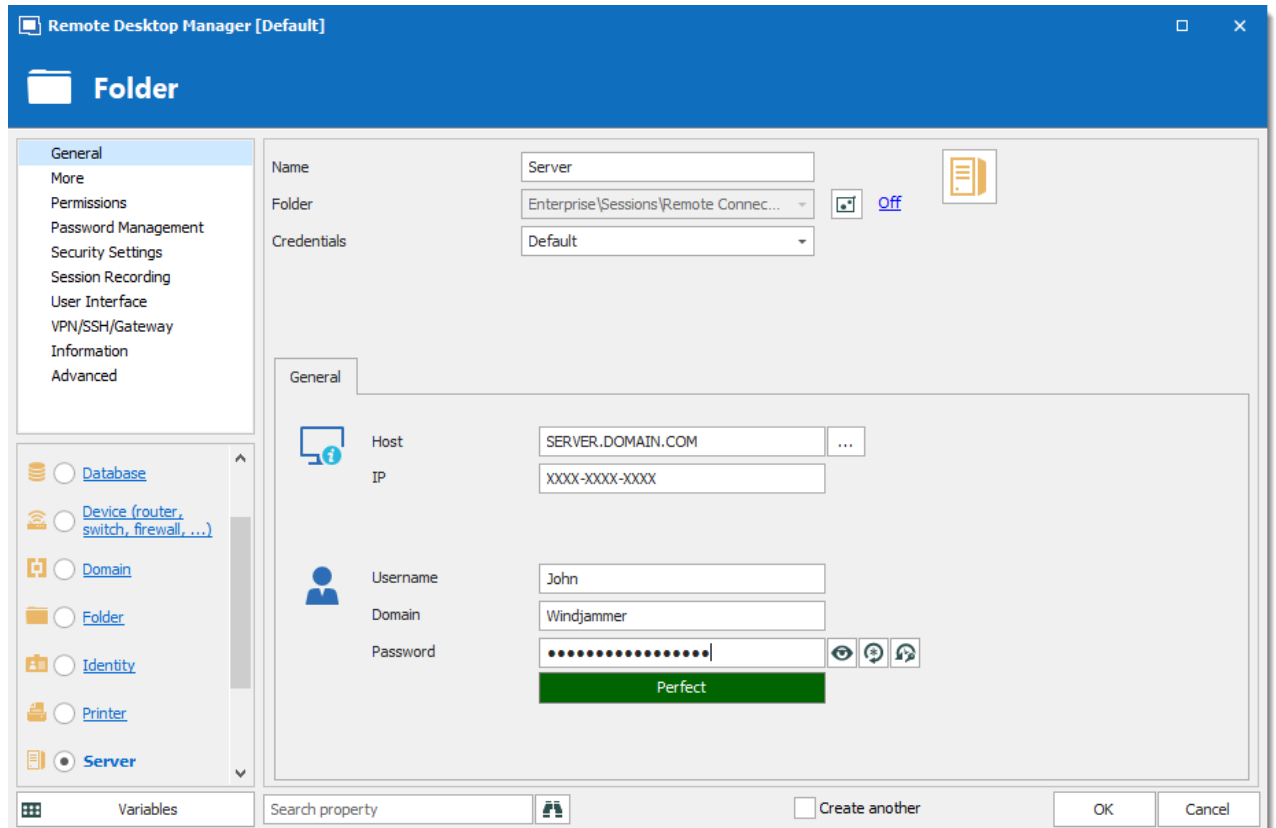
In Remote Desktop Manager, you can use Folder entries to organize your sessions in the application. It is possible to store information at the top level folder and use Variables in the child entries to resolve information that you have saved in the parent folder.



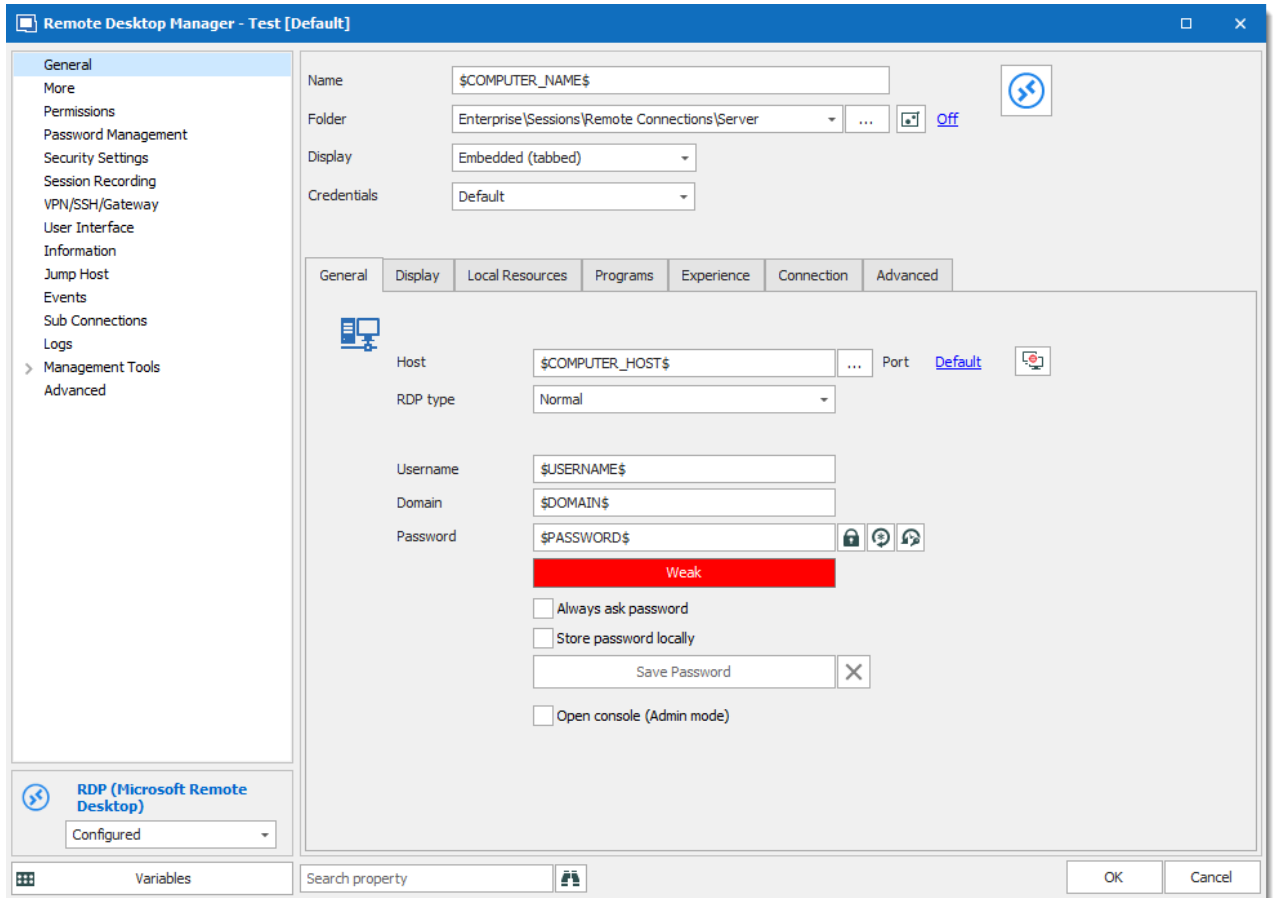
Variables are only supported for **Advanced Data Sources** like SQL Server, MySQL and <%DPS%>.

## SETTINGS

1. Create a Company, Database, Device, Domain, Identity, Printer, Server, Site, Software or Workstation folder in the Navigation Pane.
2. Enter information in Folder properties. Only include a password if you want to put password protection on the folder.

*Folder Properties*

3. In the child sessions, use the appropriate Variables to retrieve the information that is saved at the folder level



Variables

## 10.1.1.7.3 Host with Templates

## DESCRIPTION

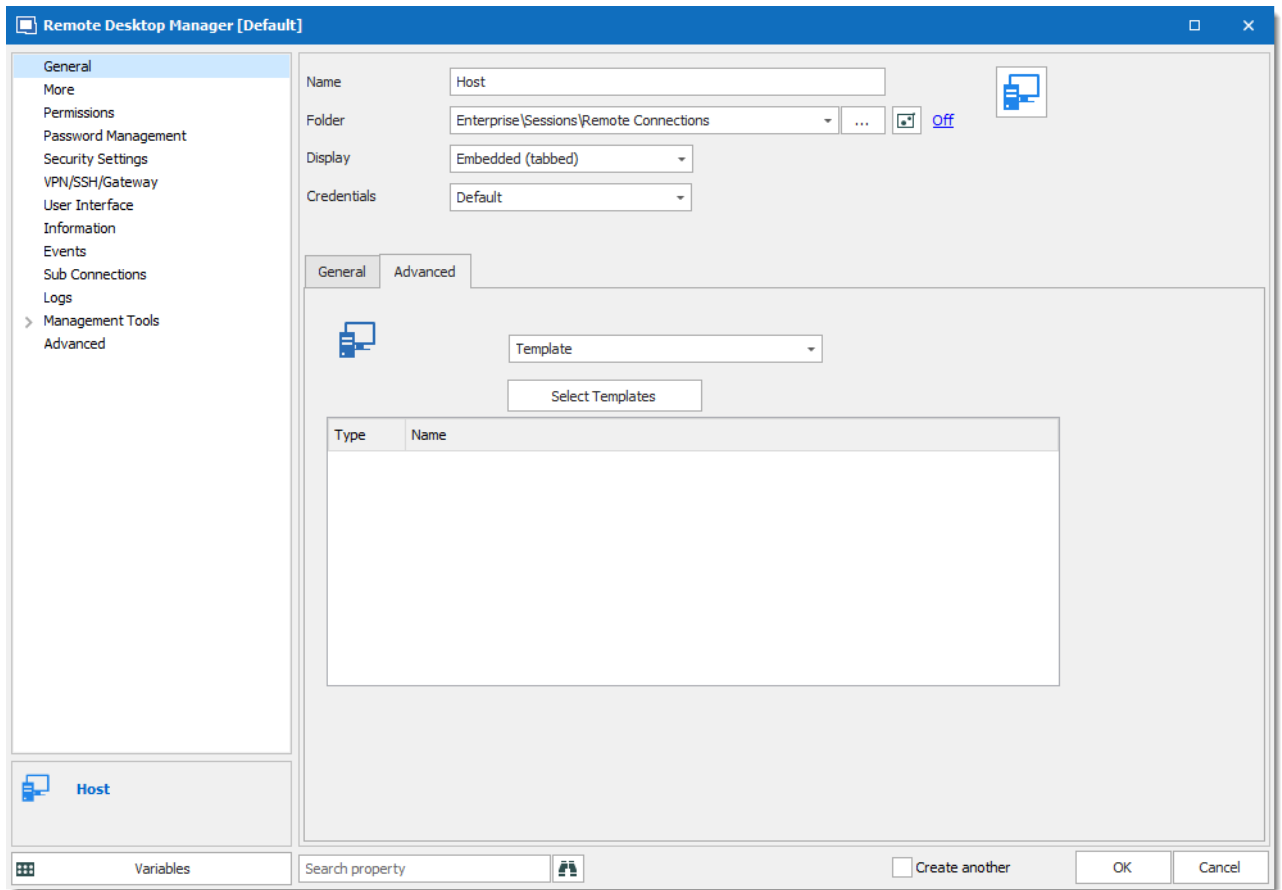
A Host entry will let you use templates in order to connect to the host. It will prompt you to choose which template to use to launch the host.

## SETTINGS



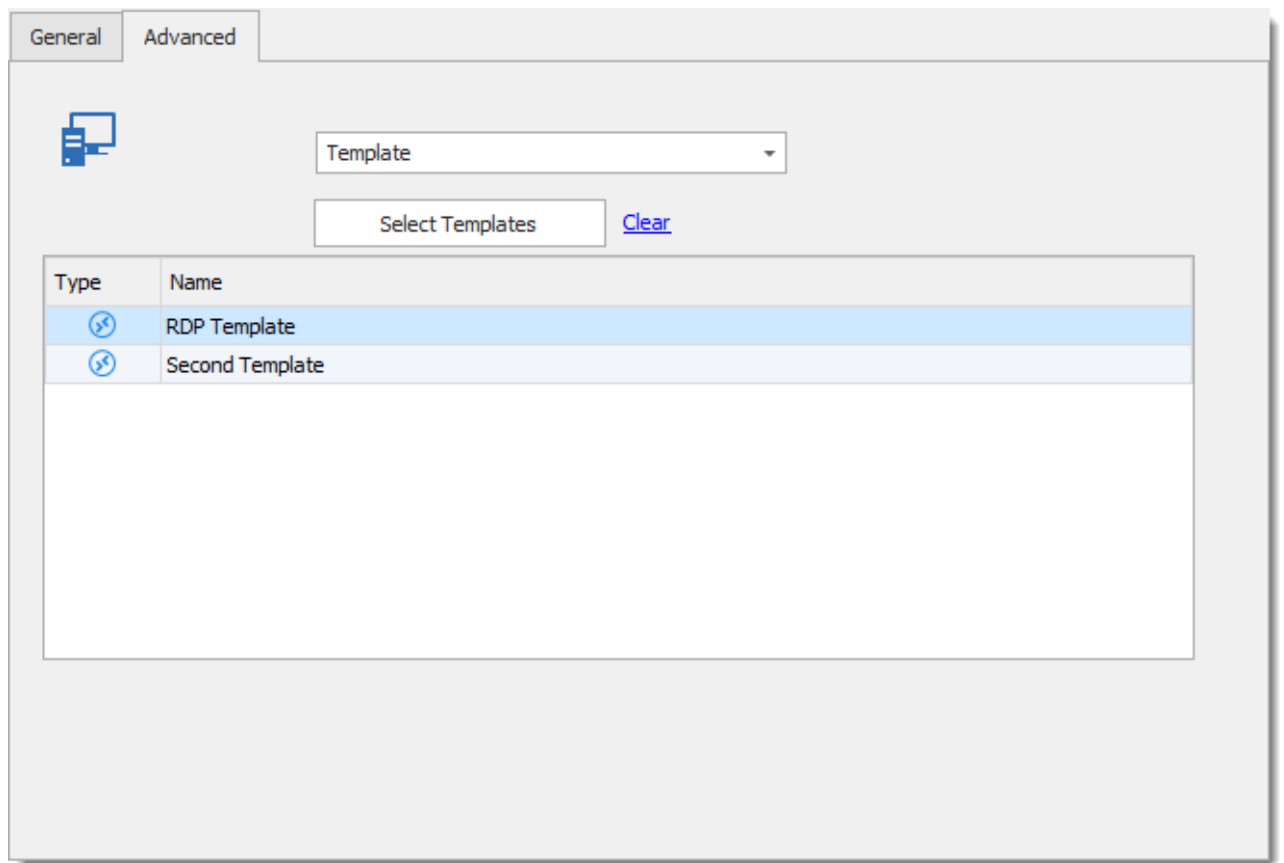
1. Create one or multiple [Templates](#) via the **File – Templates – Templates menu**. You may need to use Variables like **\$HOST\$** for the host name as well as **\$USERNAME\$** or **\$PASSWORD\$** for the username and password.

2. Create a host entry and click on the **Action** tab



*Host Entry*



3. Press the **Select Templates** button and select the templates that you would like to add to your Host session
4. The templates will now be added to your host session



General Advanced

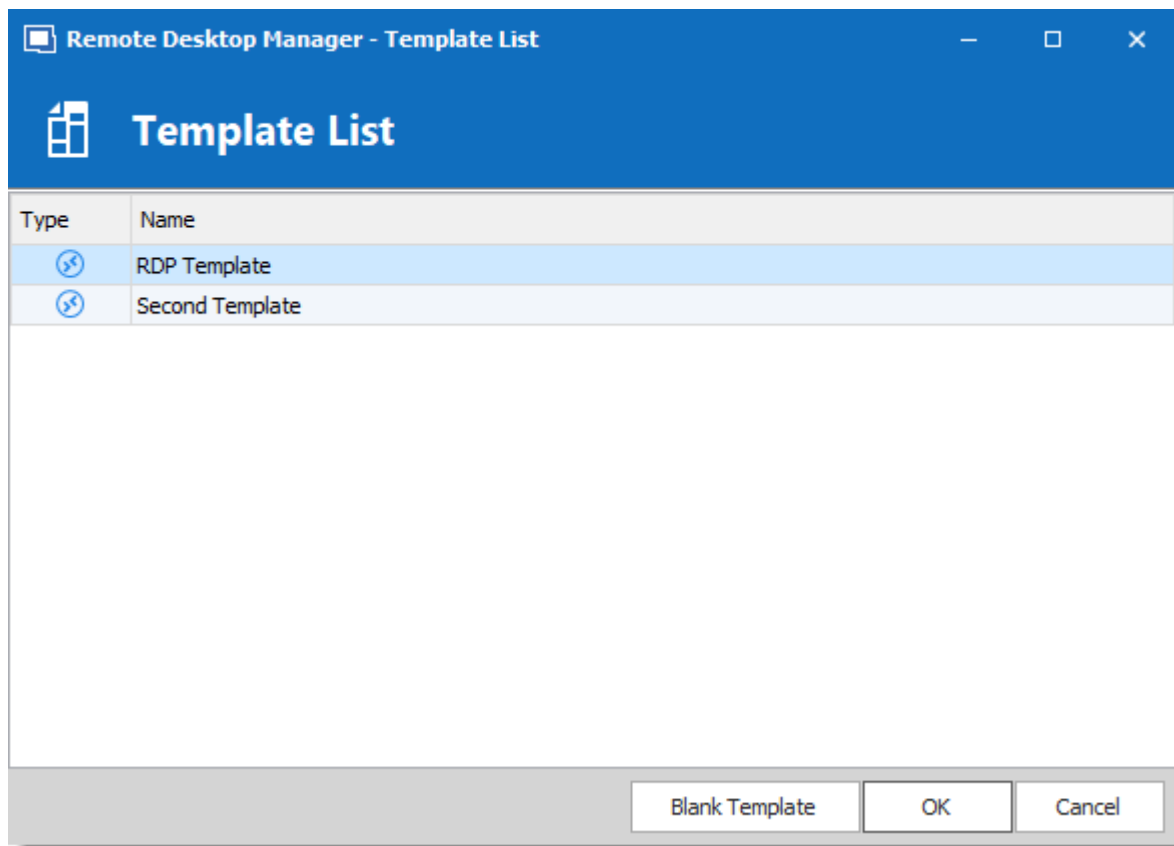
Template

Select Templates [Clear](#)

Type	Name
	RDP Template
	Second Template

*Select Templates*

5. Launch your **Host** session. You will be prompt to select the appropriate template to launch the session



*Open Host Session*

#### 10.1.1.8 Pwned Password Check

### DESCRIPTION

In the InfoSec world, a pwned password is a password that has been exposed in data breaches (i.e. they are owned/pwned by hackers).

Using a pwned password significantly increases the chances of being the victim of a data breach. **Pwned Check** leverages Troy Hunt's Pwned Passwords API and automatically checks to see if a password that you're using (or are thinking of using) has been pwned by hackers. If it has, you will be notified and can be proactive and choose something else to stay out of harm's way. There are over half a billion passwords in the Pwned Passwords database.

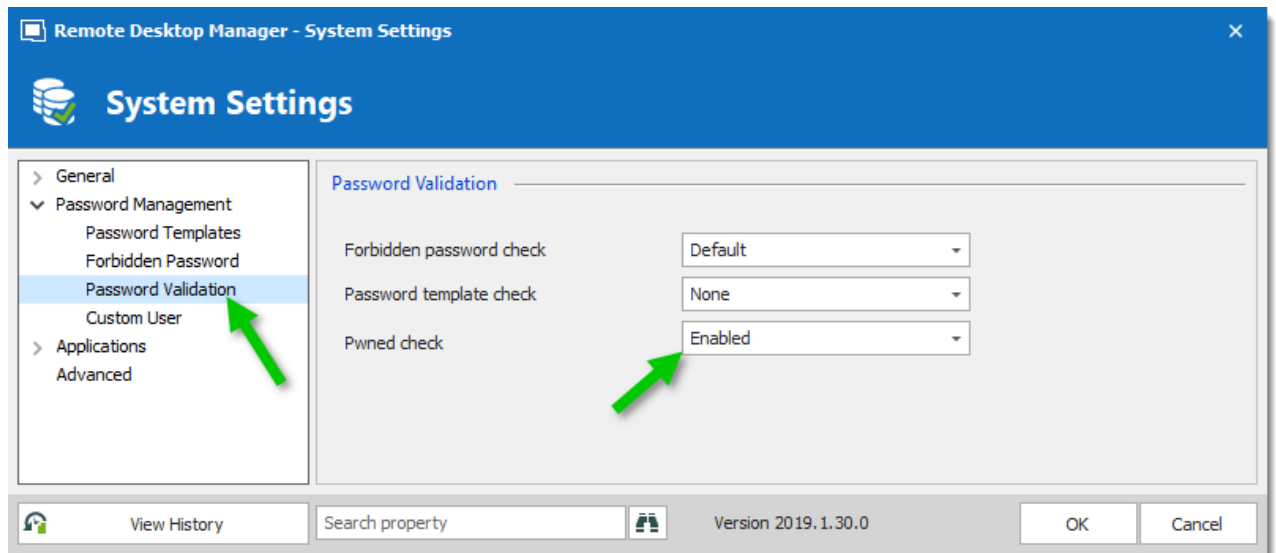
### PWNED PASSWORD CHECK EXPLAINER VIDEO



## HOW TO SET UP THE PWNEED PASSWORD CHECK

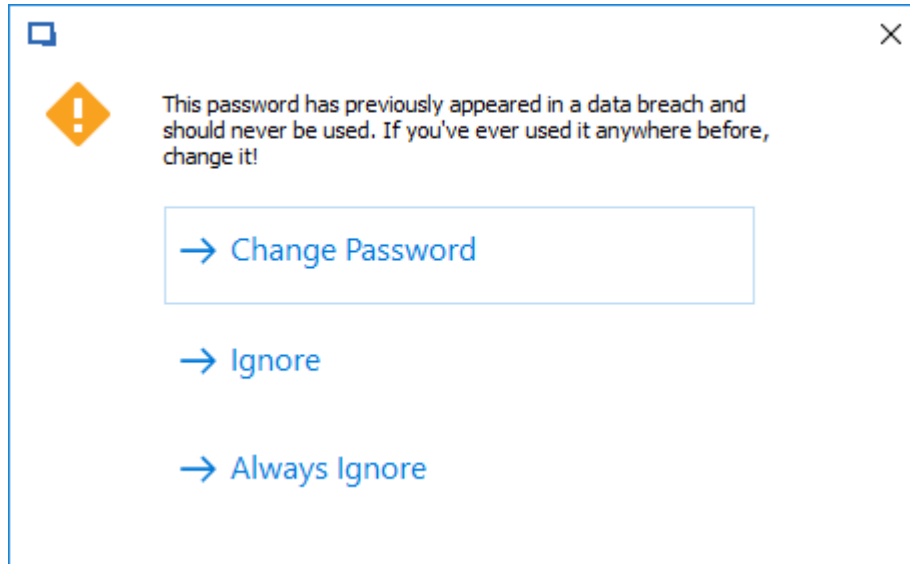
In existing databases, Pwned check is not turned on automatically.

1. On the Administration tab, open **Data Source Settings (System Settings) – Password Validation**.
2. Choose **Enabled** from the list.



*Administration - System Settings - Password Validation*

Remote Desktop Manager analyzes a password when you save an entry. A message is displayed when a password is found in the Pwned Passwords database. If you see this window you should change your password immediately. Remember to change it in Remote Desktop Manager and the actual account.



*Warning to change a password that was included in a data breach*

## THE BACK END

Rest assured Remote Desktop Manager does NOT send your passwords to Pwned Passwords.

Here is how it works:

Pwned Password Check uses k-Anonymity.

Remote Desktop Manager only sends the first five characters of the SHA-1 password hash to the API.

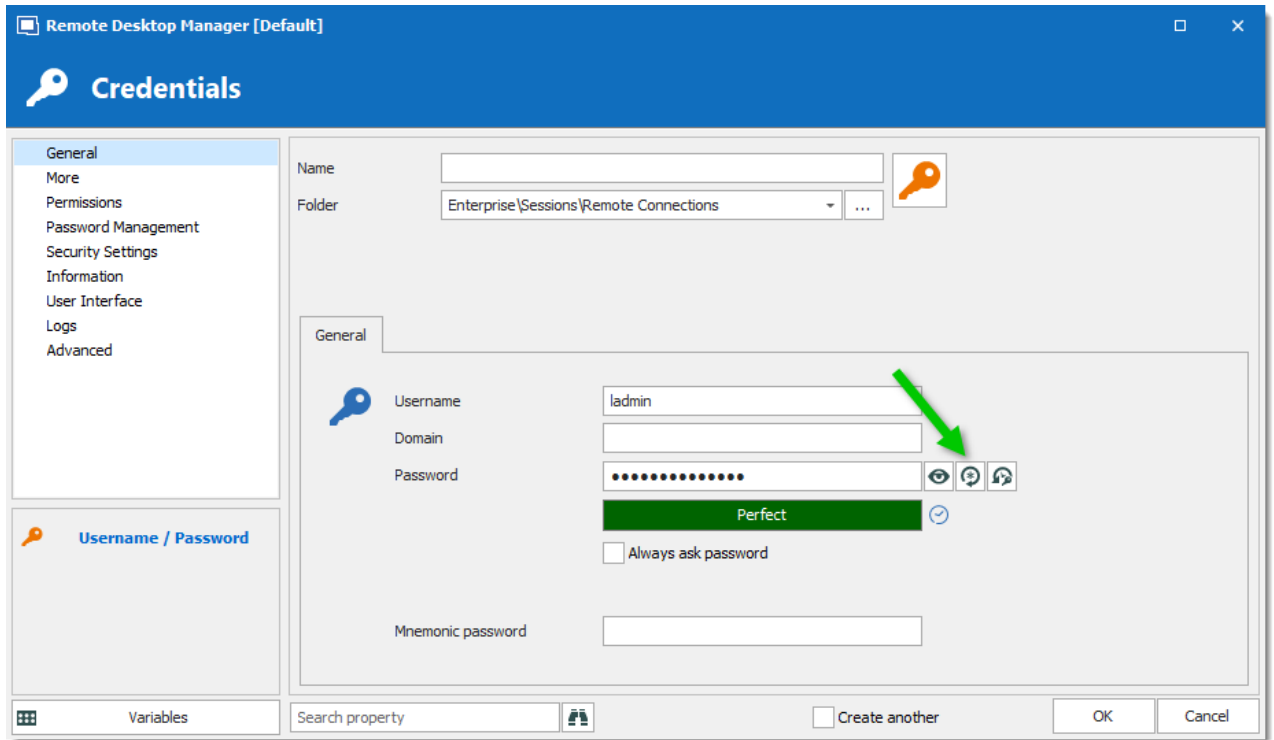
The API sends back a list of every password hash that matches the first five characters of the hash. The API only sends back the second part of the hash.

Remote Desktop Manager compares the hashes on the list to the password hash for the password you want to use.

If there is a match you receive a warning.

## CHOOSE STRONGER PASSWORDS

Remote Desktop Manager makes it easy to make strong passwords. The built-in [Password Generator](#) creates secure passwords, following your specifications for password length and complexity. The password generator is available on every entry beside the field where you enter a password.



*Password Generator is found on most entry where you include a password*

Remote Desktop Manager also has a [Password Analyzer](#) that provides feedback on all your passwords. A rating is included on the entry. It uses Zxcvbn to evaluate passwords.

You can also create a report of all your passwords by using the **Password Analyzer** in the **Tools** tab.

**Tools - Password Analyzer**

**Settings**

☐ Show all ☐ Show private vault

☐ Show VPN analysis ☐ Show pwned password analysis

**Analysis**

Name	Folder	Username	Date	Since	Occurrence	Password Strength
Active Directory	Enterprise\Synchroni...	administrator	1/14/2019 9:11 AM	6 months	2	Weak
Active Directory Console	Enterprise\Sessions\...	administrator	12/19/2018 6:49 AM	7 months	2	Weak
BasicCred	Enterprise\Credentials	David	11/13/2018 10:45 ...	8 months	4	Popular
CredPV		David	1/2/2019 11:16 AM	6 months	4	Popular
Email Account	Enterprise\InfoTypes	Email	11/13/2018 8:42 AM	8 months	1	Good
Login (Account)	Enterprise\InfoTypes	TestLaccount	11/13/2018 8:17 AM	8 months	2	Weak
Login (Web)	Enterprise\InfoTypes	TestLusername	11/13/2018 8:35 AM	8 months	2	Weak
RDPTest	Enterprise\Sessions\...		4/30/2019 9:17 AM	2 months	1	Weak
RDPTest - Copy	Enterprise\Sessions\...	test	1/18/2019 3:19 PM	6 months	4	Popular
TeamViewer	Enterprise\Sessions\...	845370611	12/19/2018 11:08 ...	7 months	1	Good
test	Enterprise\Sessions\...	test	2/5/2019 9:51 AM	5 months	1	Popular
Wi-Fi Router	Enterprise\InfoTypes		11/13/2018 8:45 AM	8 months	1	Good
Windows Admin Center	Enterprise\Sessions\...	david	2/5/2019 10:02 AM	5 months	1	Perfect

Tools - Password Analyzer

### 10.1.1.9 Vaults Overview

Vaults are containers that divide the data source into multiple compartments.

We recommend using Vaults for improved organization and security. Vaults also help performance as they limit the amount of entries that load at once.

Vaults are available with Advanced Data Sources: Devolutions Password Server, SQL Azure, Maria DB, MySQL and SQL server.



This feature underwent a change of name, as **Vaults** were called **Repositories** before **Remote Desktop Manager 2019**.

This article covers:

- [Create Vaults](#)
- [Move entries to different Vaults](#)
- [Navigate between Vaults](#)
- [Role-based security with Vaults](#)
- [Vaults shortcuts](#)

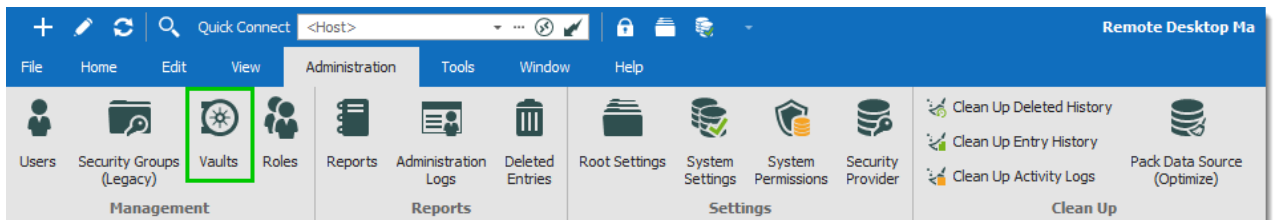
## SETUP AND USE VAULTS IN REMOTE DESKTOP MANAGER

*Get started with Vaults: create, manage, make shortcuts*

## CREATE A VAULT

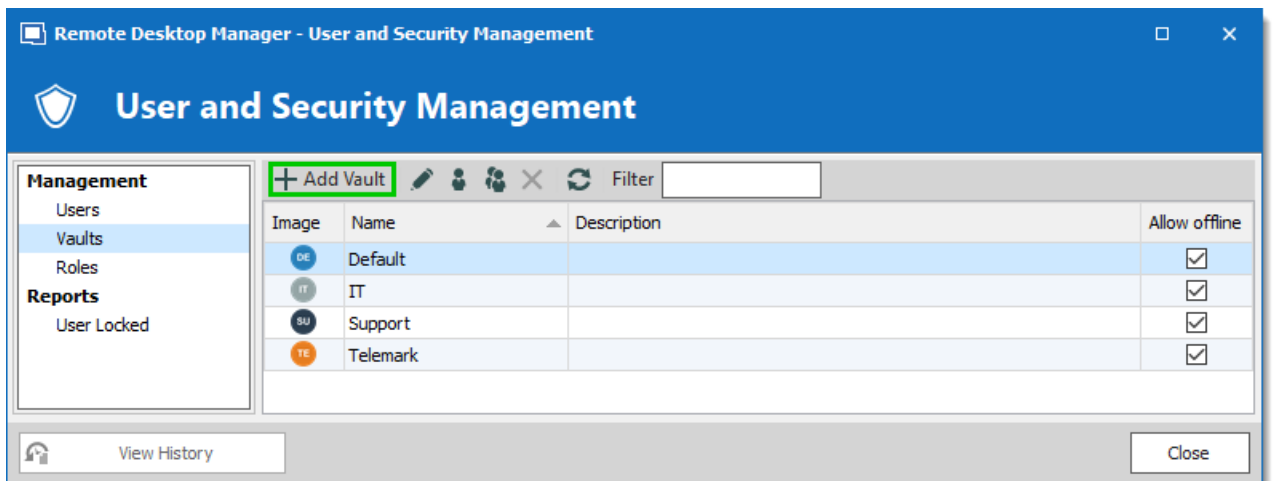
We recommend creating a different **Vault** for each customer or department.

1. On the **Administration** tab, click **Vaults**.



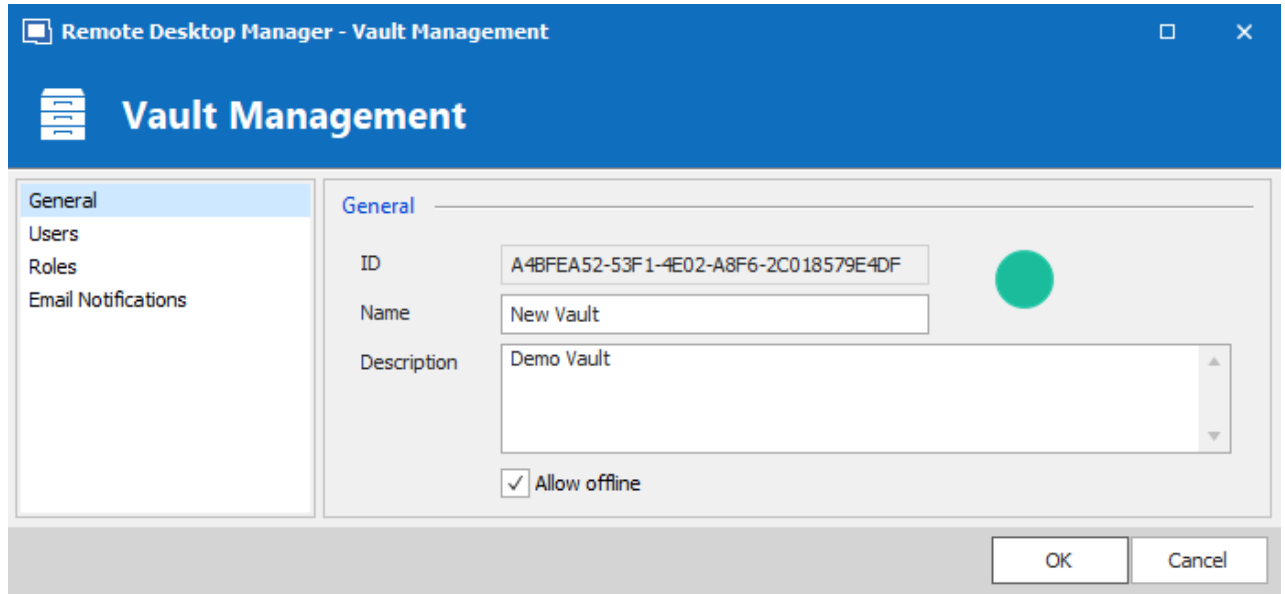
*Administration – Vaults*

2. Click **Add Vault**.



*Vaults – Add Vault*

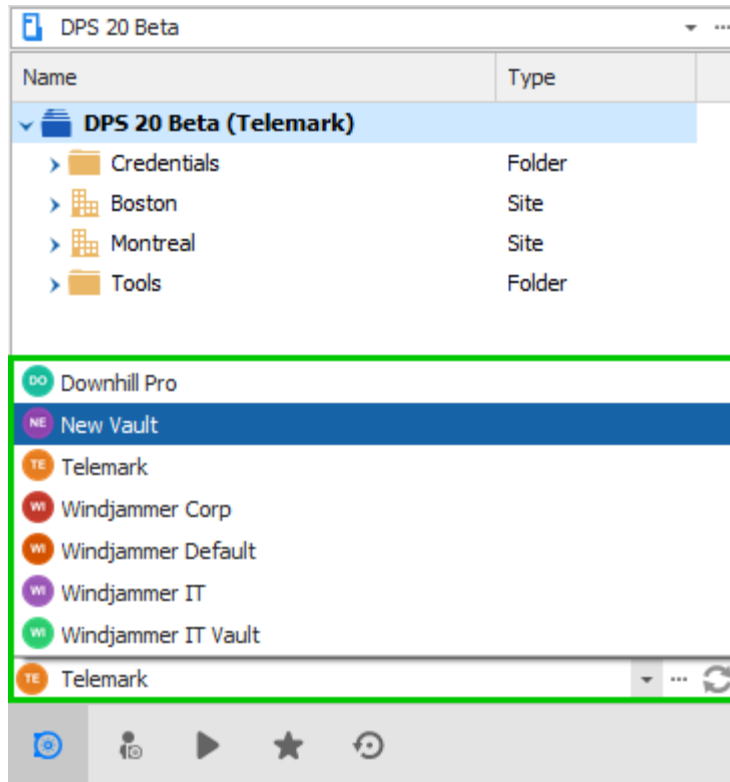
3. Enter a **Name** and **Description** (optional). The ID is generated automatically.

*Vault Management*

Navigate between Vaults

## MOVE BETWEEN VAULTS

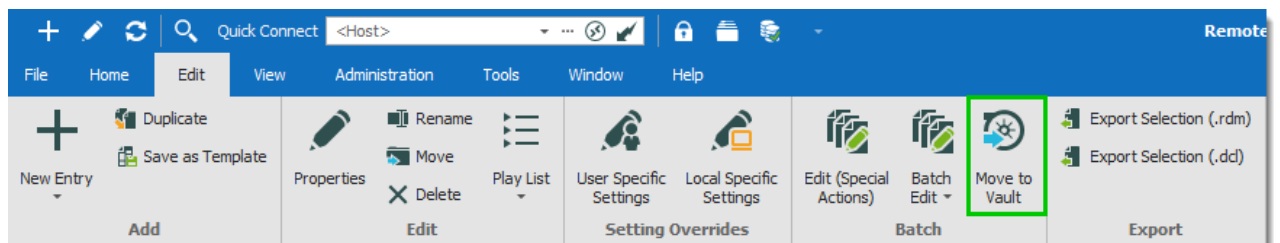
1. In the Navigation Pane, use the Vault list to move between Vaults. Change the location of the Vault list in [File – Options – User Interface – Vault Location](#).



*Navigation Pane – Vault selector*

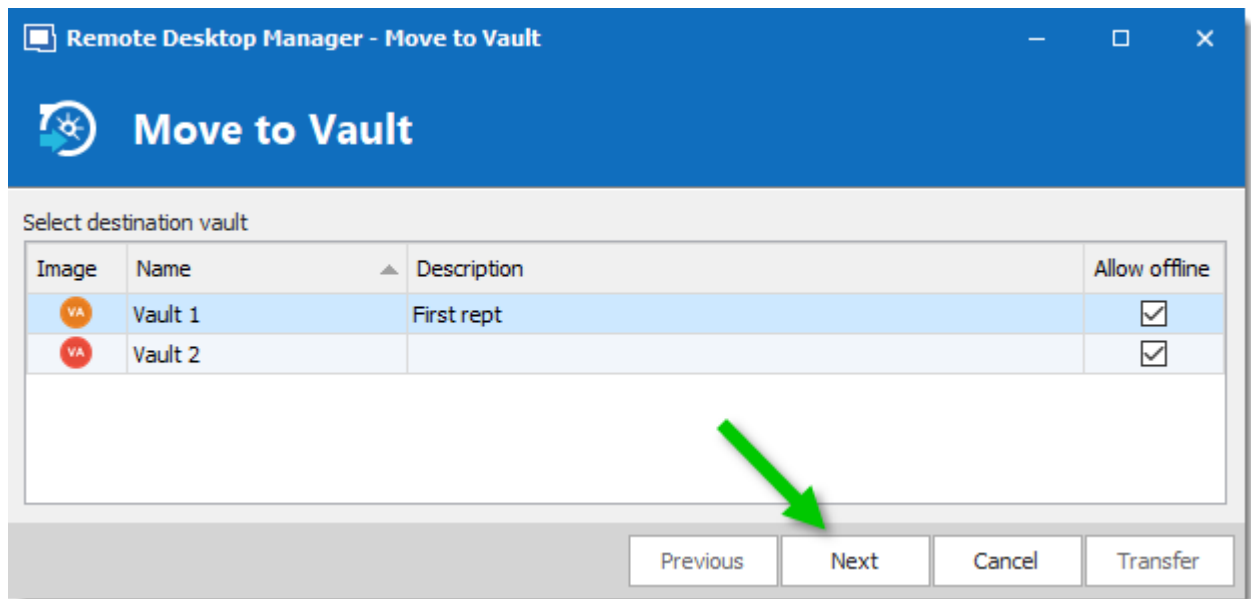
## MOVE ENTRIES TO A DIFFERENT VAULT

1. Start in the Vaults you want to transfer repositories out of.
2. On the **Edit** tab, click **Move to Vault**.

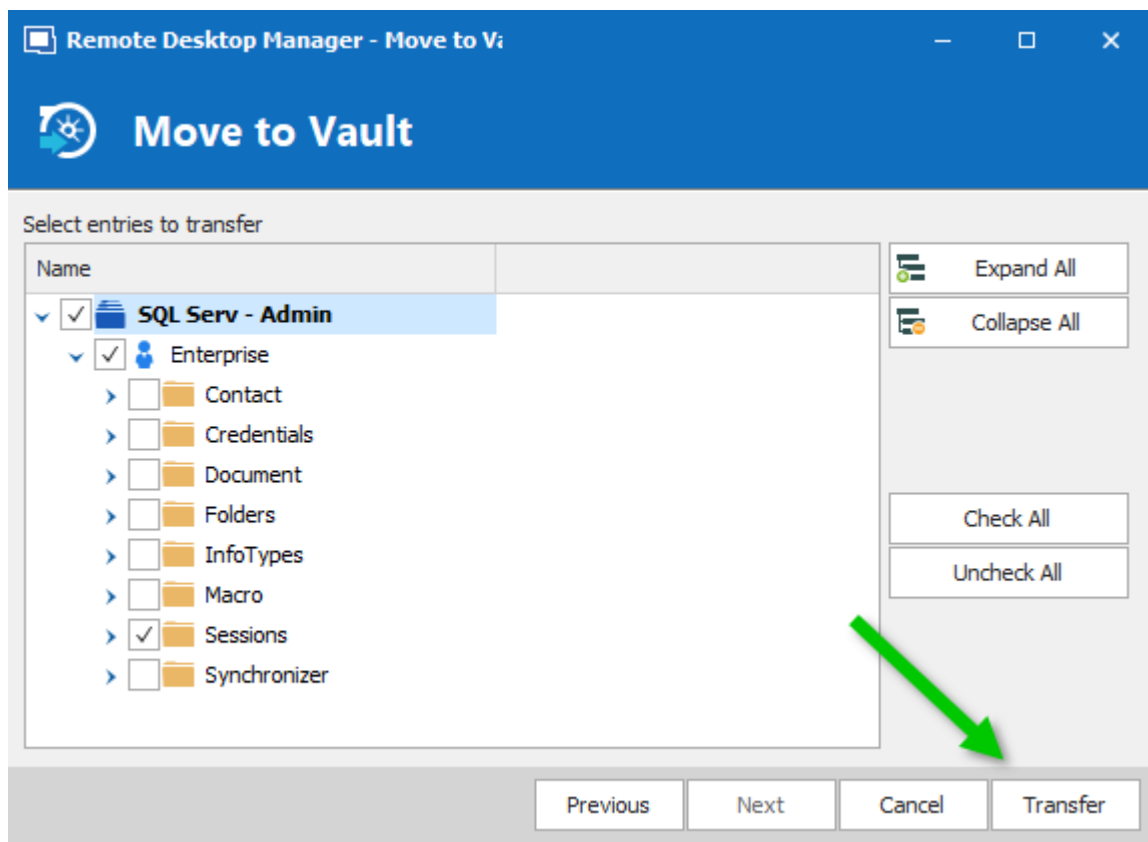


*Edit - Move to Vaults*

3. Select the repository you want to move the entries to, and click **Next**.

*Move to Vaults*

4. Choose the entries you want to transfer to the new repository, and click **Transfer**.

*Select the entries you want to transfer*



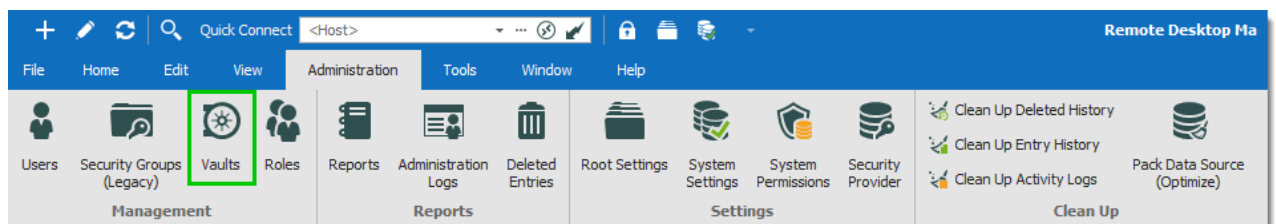
## MANAGE ROLE-BASED SECURITY BY VAULT

Vaults simplify user management because Active Directory groups define who has access to a Vaults. These Active Directory groups are known as **Roles** in Remote Desktop Manager. In general, most roles have access to a couple Vaults, while some groups will only have access to one Vaults. Limiting access to Vaults minimizes the need to set permissions on lower-level folders.

*How to assign roles to a Vault and the permissions you need to keep in mind*

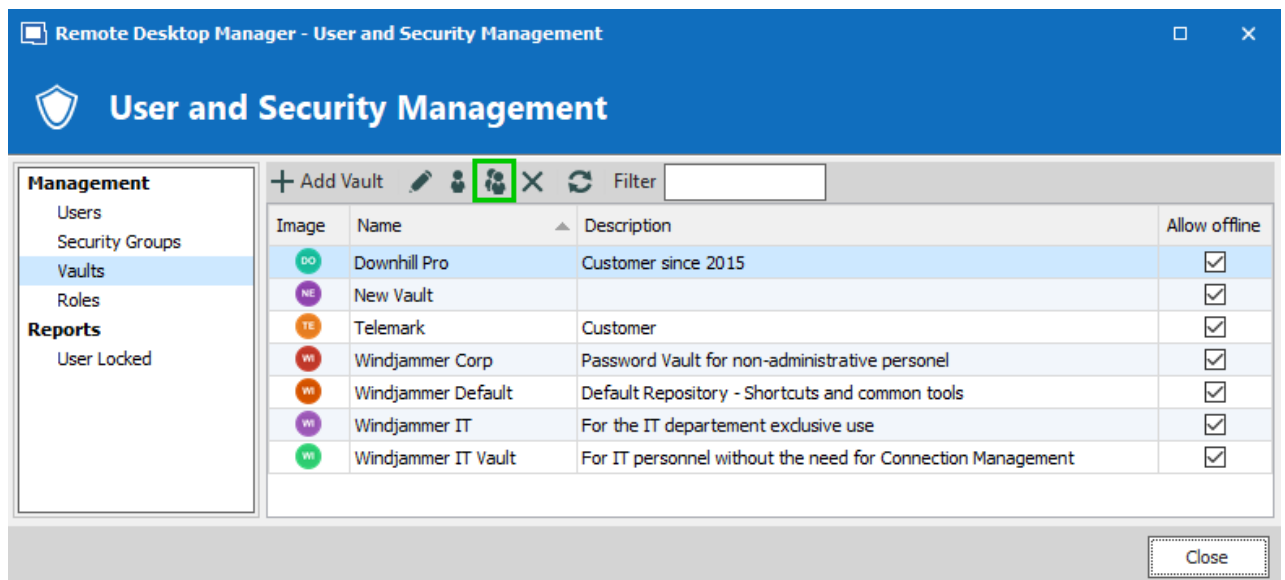
### GIVING ROLES ACCESS TO A VAULT

1. On the **Administration** tab, then click **Vaults**.



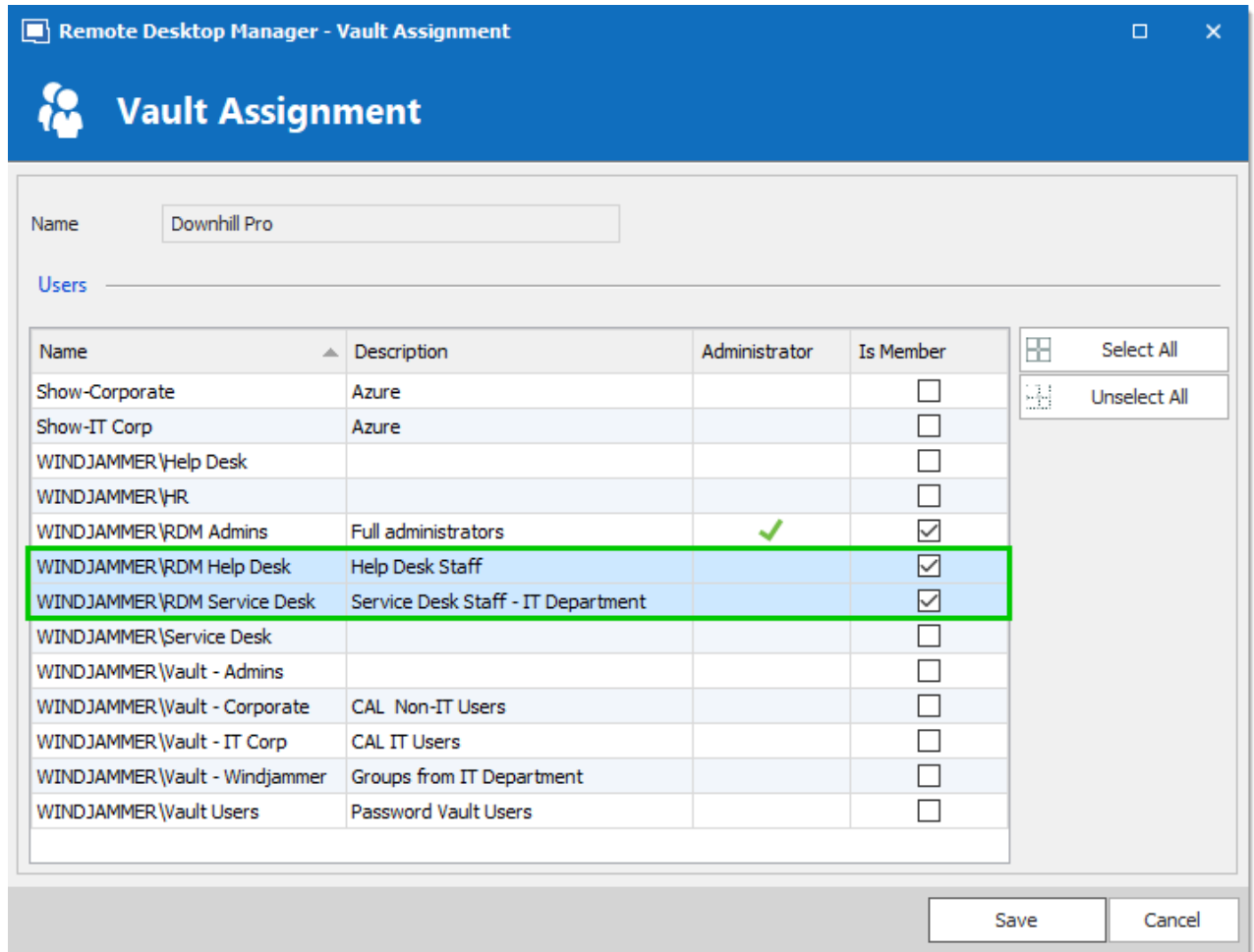
*Administration –Vaults*

2. On the **User and Security Management** window, choose the Vaults, then click **Assign Roles**.



*User and Security Management - Vaults - Assign Roles*

3. Choose which roles have access to the Vaults: select the **Is Member** box.



Repository Assignment

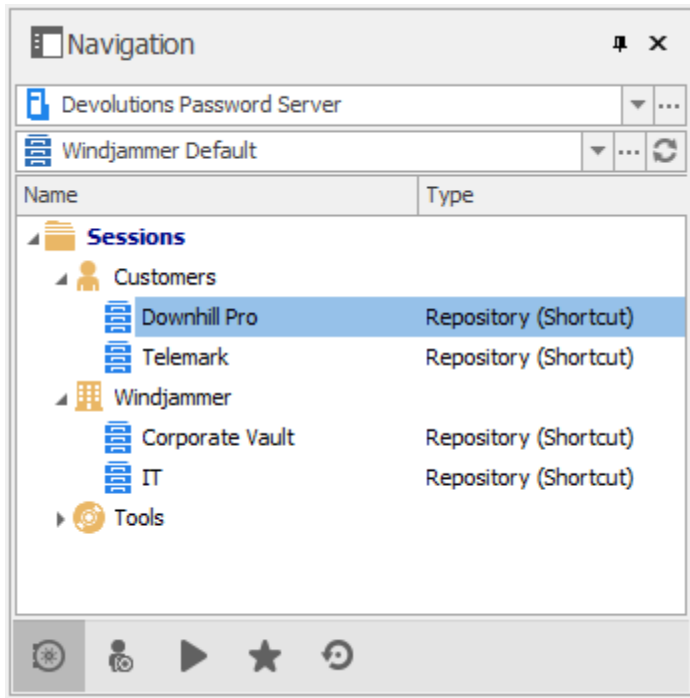
## VAULTS SHORTCUTS

Navigate between vaults with the [Vault List](#) or vaults shortcuts.

We recommend administrators and users who have access to multiple vaults create vaults shortcuts to navigate between vaults.

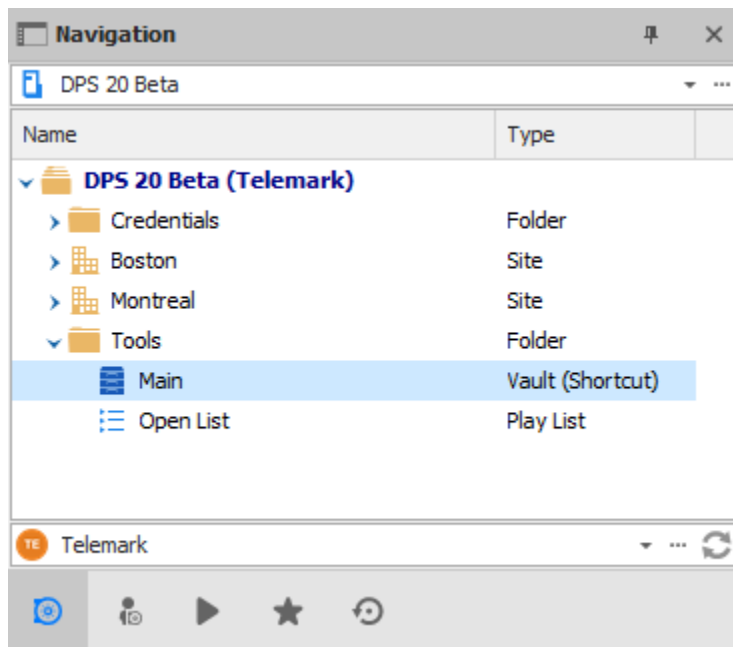
If you use vaults shortcuts, the vault root should only contain folders. Do not save entries at the vault root.

The main (default) vault contains shortcuts to other vaults.



*Main (Default) Vaults with Vaults Shortcuts*

Each Vault contains a shortcut that returns the user to the main Vault.

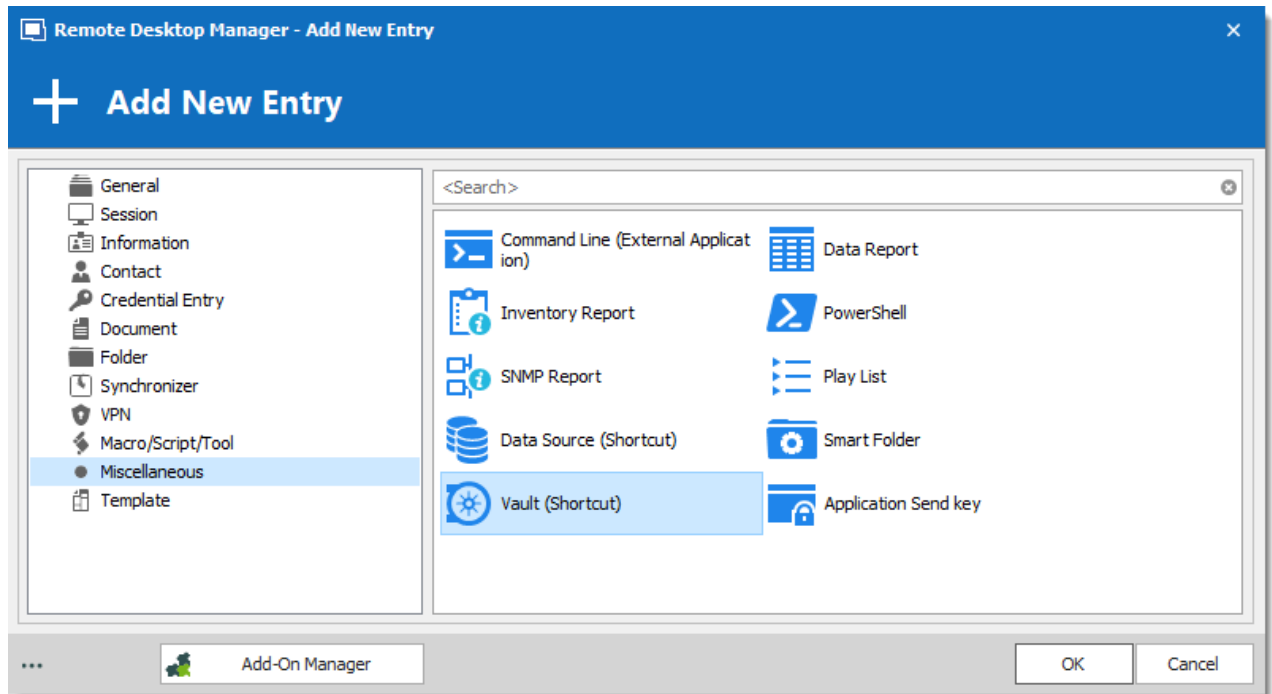


*Downhill Pro Vault with Shortcut Back to Main Vault*

## CREATE A VAULT SHORTCUT

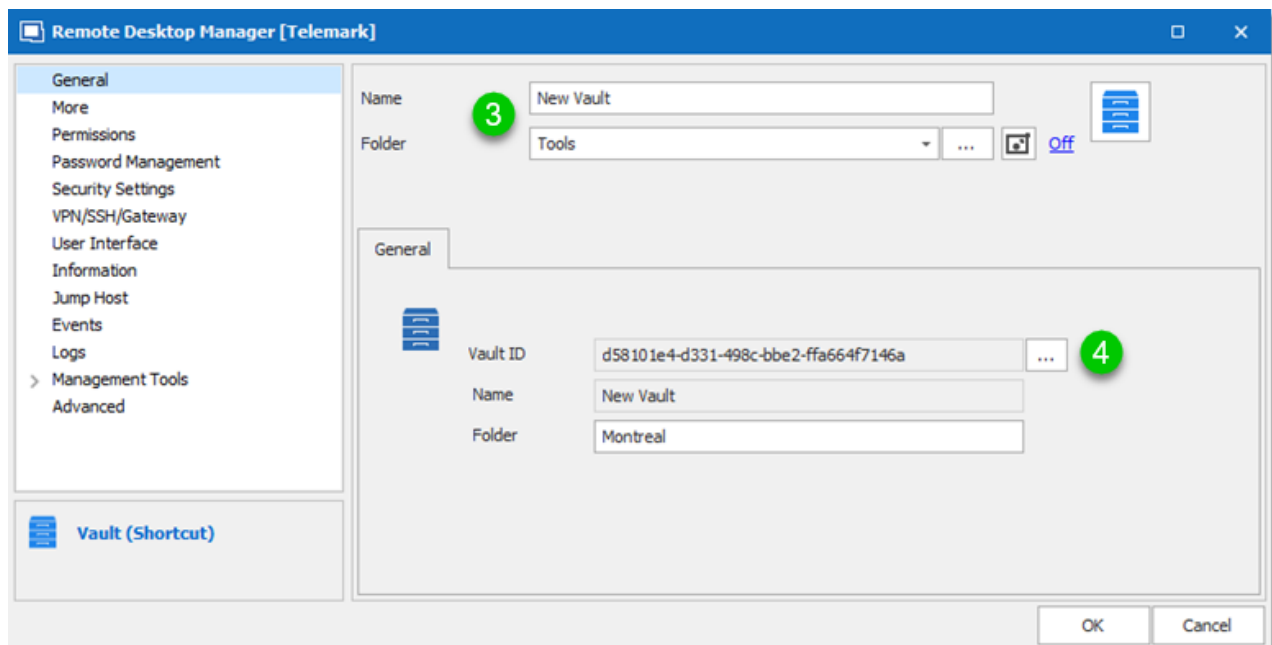
1. On the **Edit** tab, click **New Entry**.

- Click **Miscellaneous** and then select **Vault (Shortcut)**.



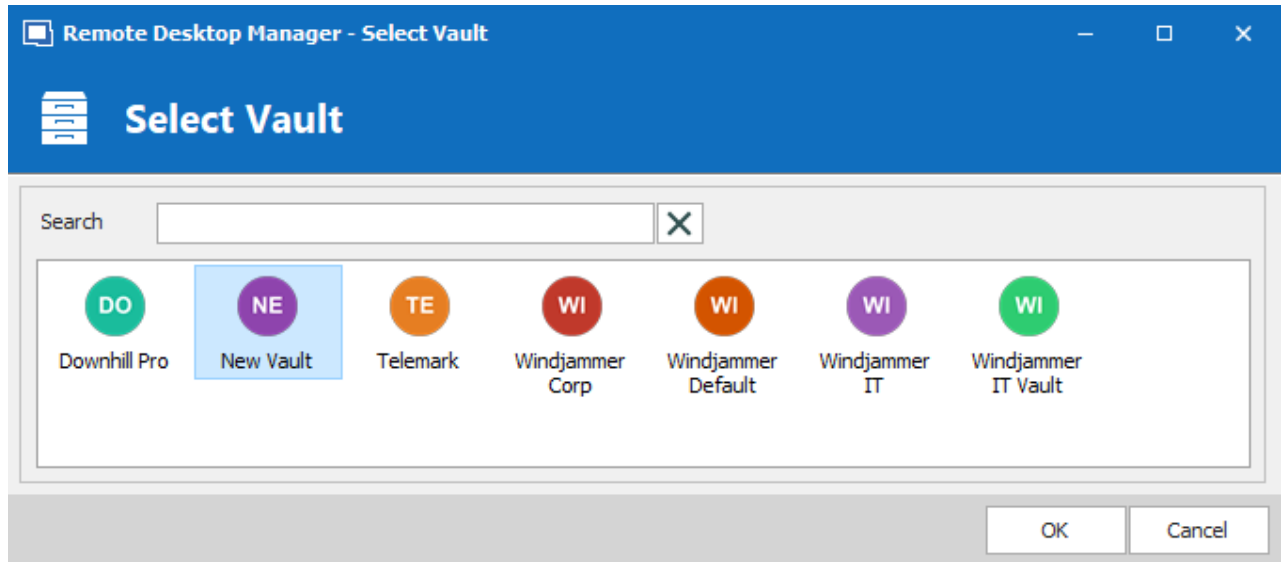
*Add New Entry - Miscellaneous - Vault (Shortcut)*

- In the **Name** box, enter the name of the Vault you are creating a shortcut to. Save the shortcut in a folder.
- To find the **Vaults ID**, click the ellipses button. Enter a folder name (case sensitive) to create a shortcut to a specific folder.



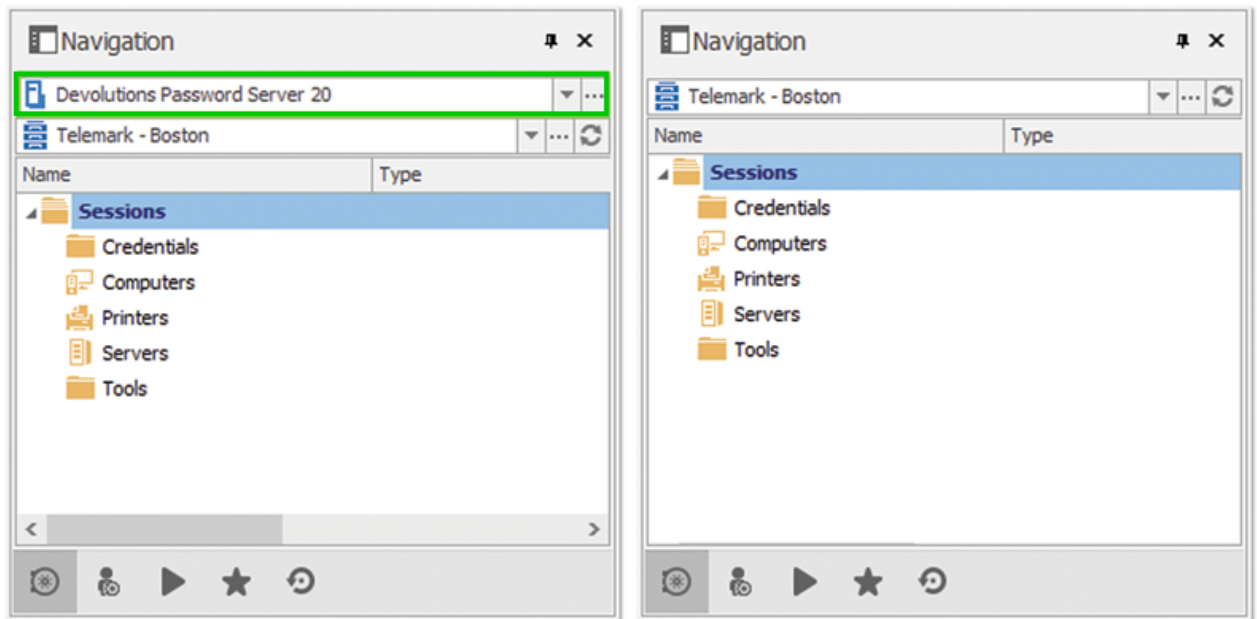
*Vault (Shortcut) - Properties*

5. Select the destination Vault.



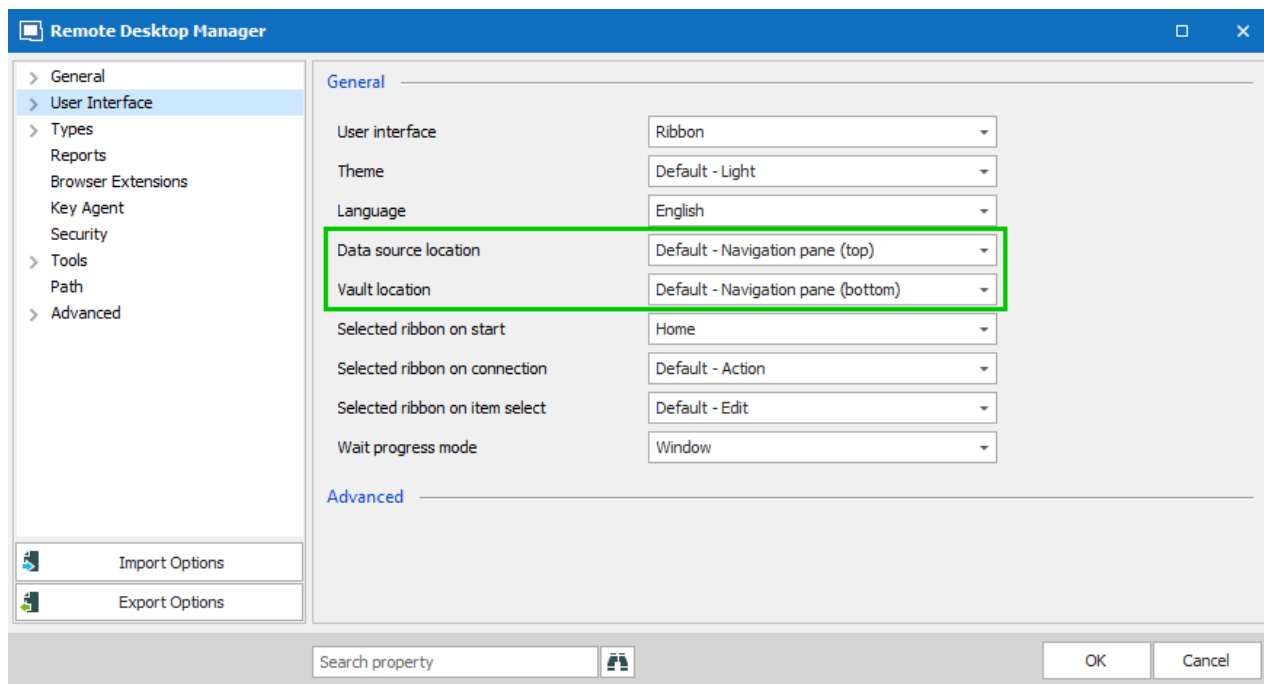
*Select Vault*

We recommend removing the data source drop-down list when using Vault shortcuts. Then the Vaults list can be moved above the Navigation Pane.



*Remove Data Source Box and Options*

Both options are configured in **File – Options – User Interface**.



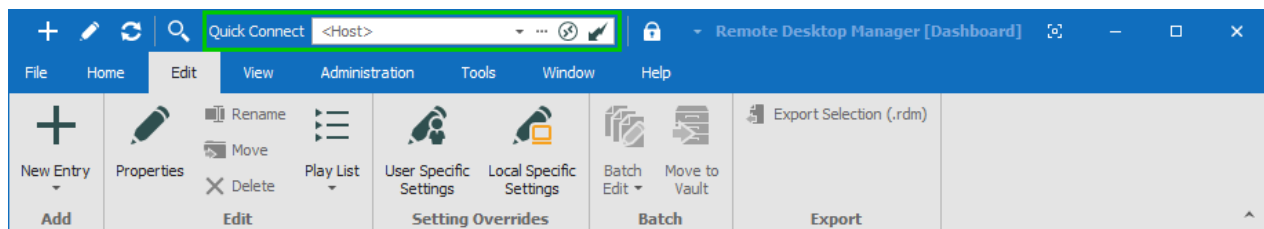
File - Options - User Interface

#### 10.1.1.10 Quick Connect

Via the quick connect toolbar, you can open an **ad-hoc** session by specifying the host and session type. It's also possible to create a template and establish the connection with your template. Configure the settings in the template, Remote Desktop Manager will apply them when connecting to the specified host.

## SETTINGS

The control is composed of multiple sub controls.



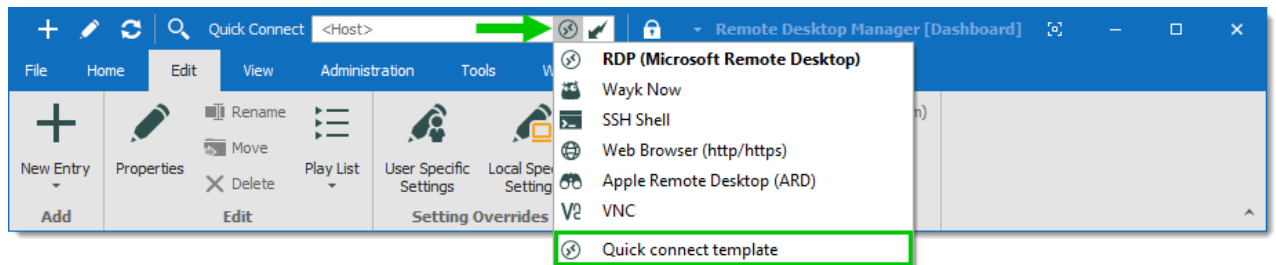
Quick Connect Toolbar



Listing network discoverable devices is a lengthy operation.

The ellipsis button will list network discoverable computer to allow you to select computer from the list.

## USING TEMPLATES



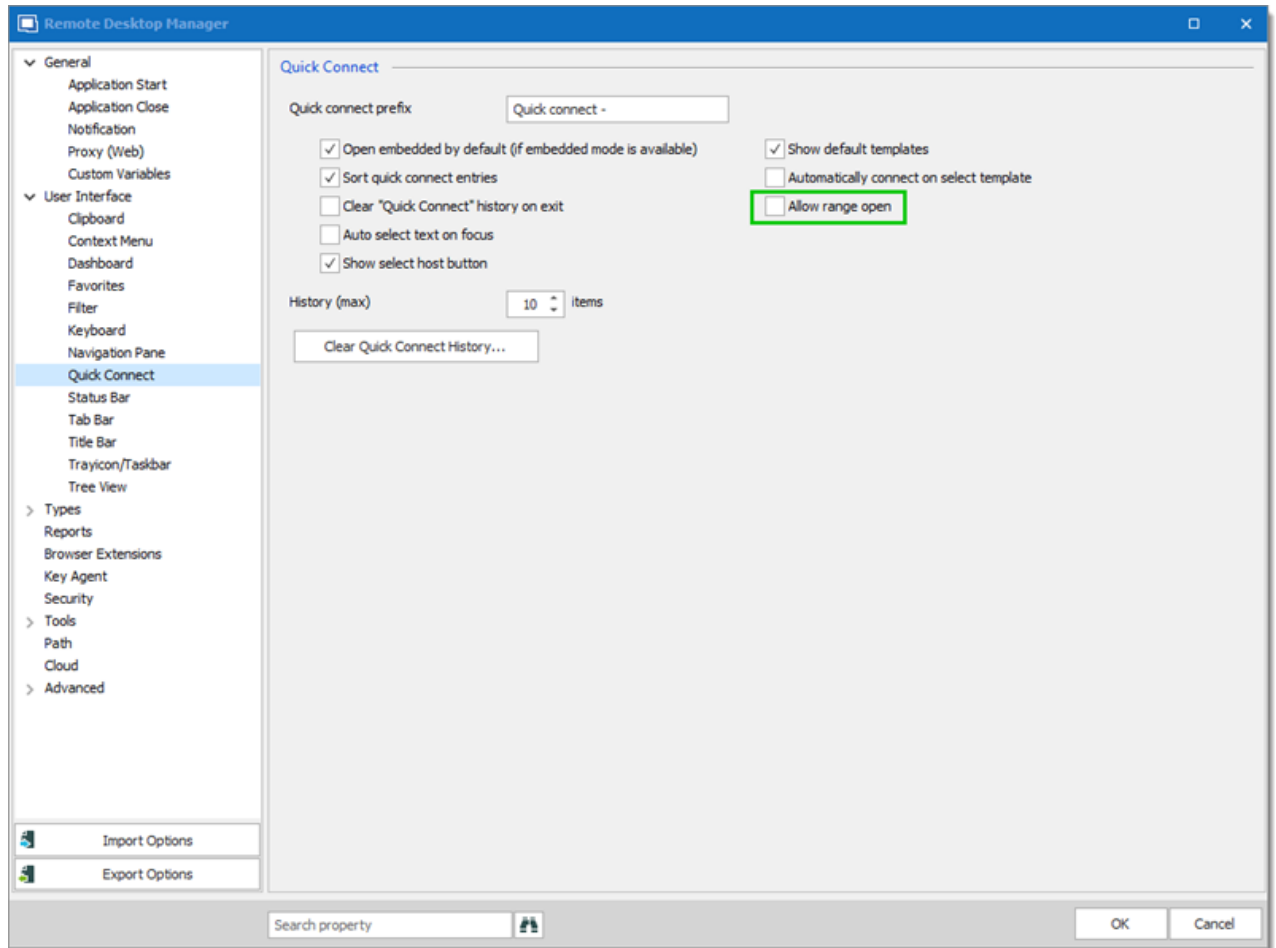
*Quick Connect Type Selection*

Remote Desktop Manager offers default templates to connect with the Quick Connect feature, but it is possible to use [custom templates](#). In that case, the **host** field in the template must be set to the **\$QUICK\_CONNECT\$** variable. When they are created, custom templates are automatically added at the bottom of the type list.

### 10.1.1.10.1 Allow Range Open

This feature allows to open multiple machine with the quick connect in Remote Desktop Manager

Check the option Allow range open in ***File-Options-User Interface-Quick Connect***

*Allow Range Open*

This range function requires that a sequenced number is at the end of the same name for all the machine like this list: devolutions08, devolutions09, devolutions10.

Use this syntax in Quick Connect: **MachineNameX~Y**

For example: to open the machines devolutions3, devolutions4 and devolutions5 you would write **devolutions3~5**.

#### 10.1.1.11 Send application logs

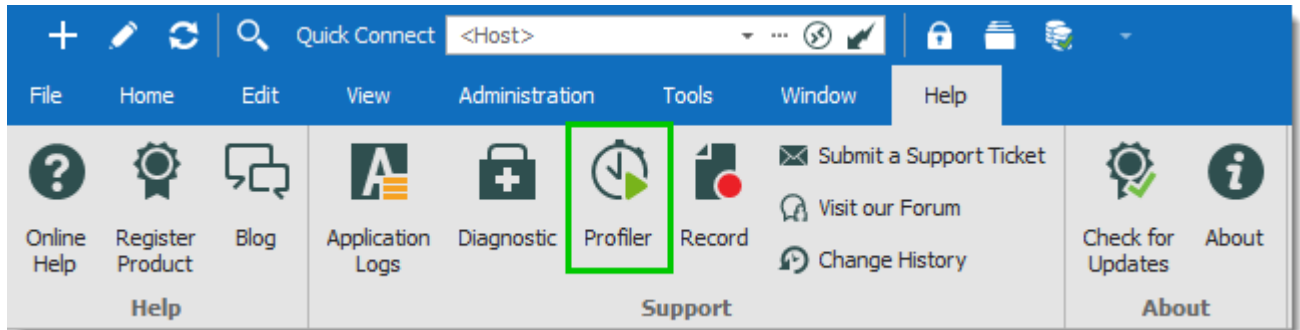
## DESCRIPTION

The Devolutions team will need your application logs in some cases to help recreate a specific issue.

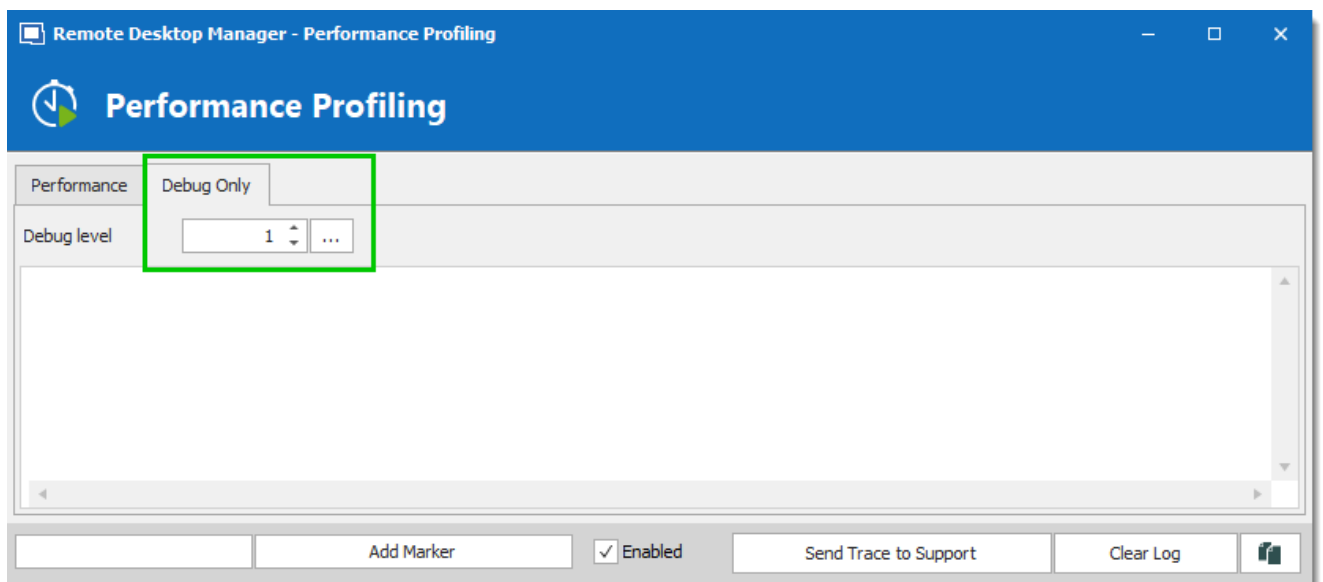


## SENDING YOUR APPLICATION LOGS

1. Before sending them, please set the **Debug Level to 1** by clicking on the **Profiler** in the **Help** tab.

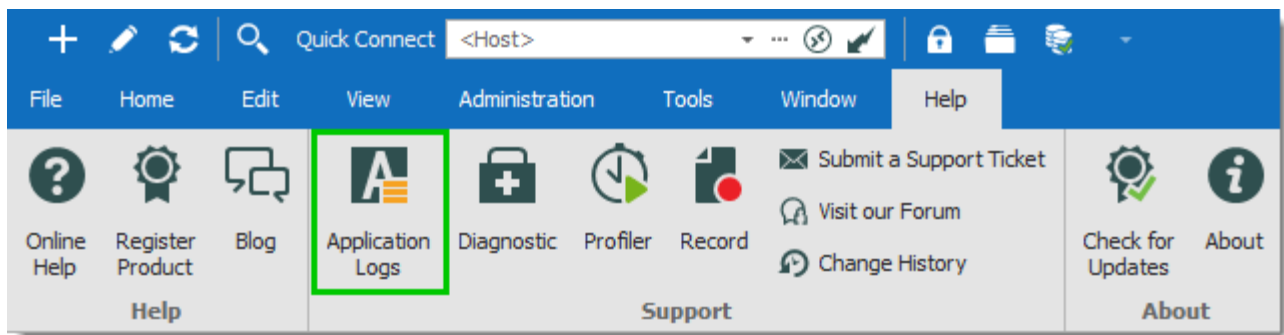


*Profiler*

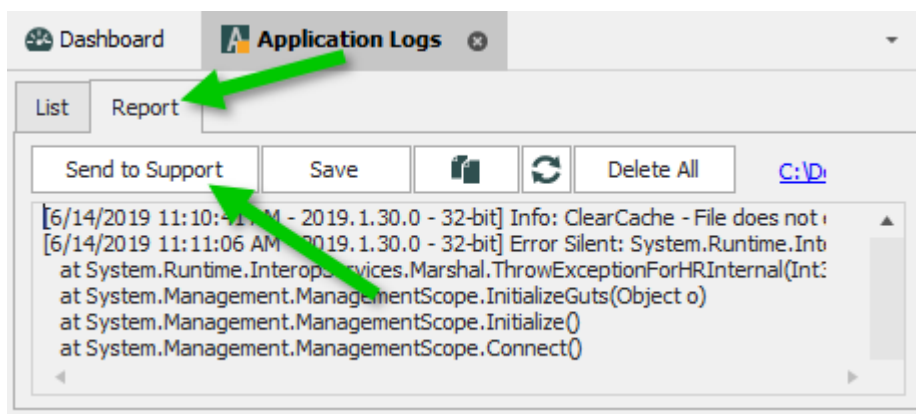


*Profiler- Debug Only*

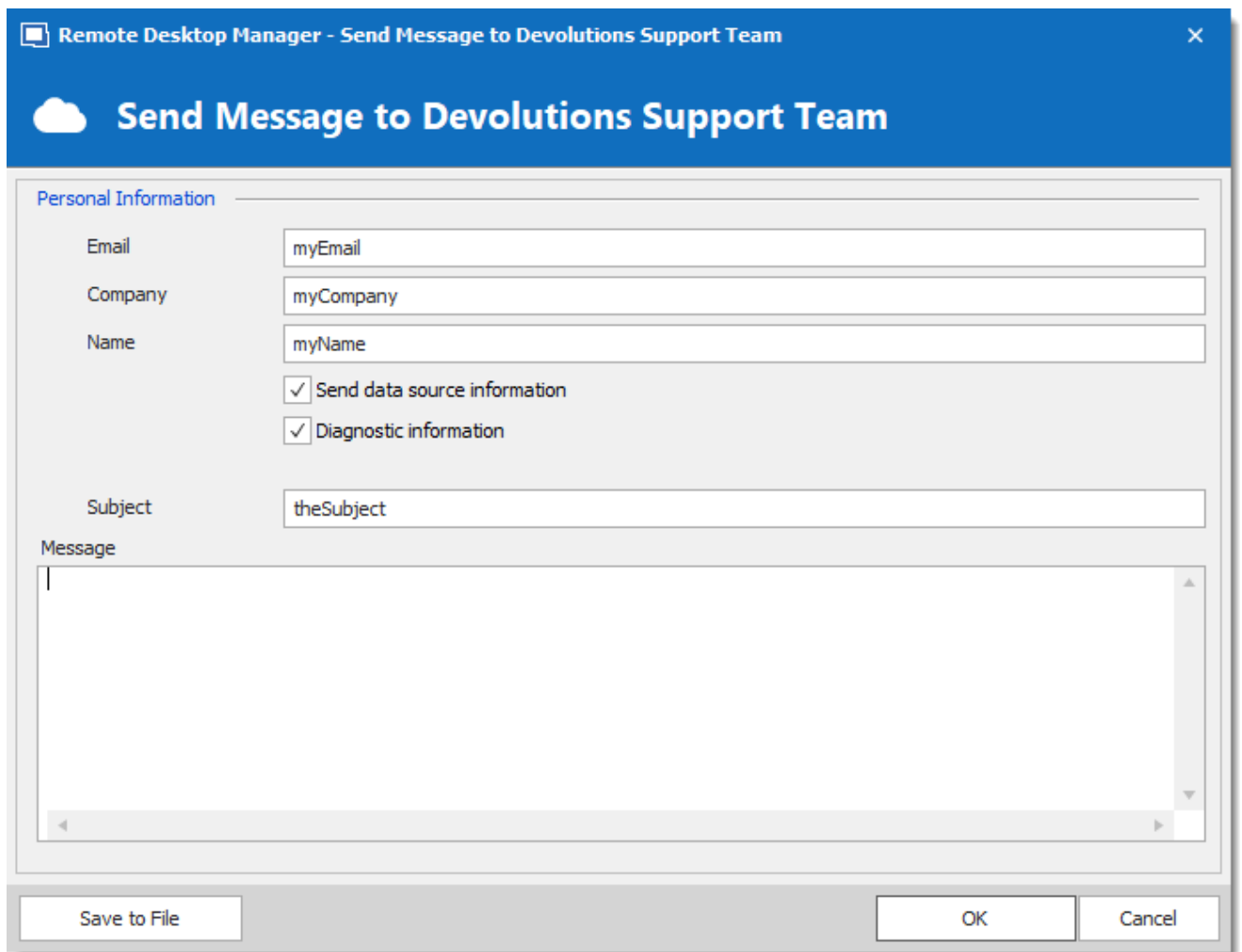
2. After, click on **Application Logs**.
- 3.



3. Go to the Report tab, and click on Send to Support.



4. Fill your contact information along with a complete explanation on the issue and press **OK**.



The screenshot shows a Windows-style dialog box titled "Remote Desktop Manager - Send Message to Devolutions Support Team". The dialog has a blue header bar with a cloud icon and the title "Send Message to Devolutions Support Team". Below the header, there is a section titled "Personal Information" with a tabbed interface. The "Personal Information" tab is active, showing fields for "Email" (myEmail), "Company" (myCompany), and "Name" (myName). Below these fields are two checked checkboxes: "Send data source information" and "Diagnostic information". There is also a "Subject" field containing "theSubject". At the bottom of the "Personal Information" section is a large text area labeled "Message" with a vertical scrollbar. At the very bottom of the dialog are three buttons: "Save to File", "OK", and "Cancel".

#### 10.1.1.12 Send error report

### DESCRIPTION

An error report is created when an application error occurs in Remote Desktop Manager. You can send that error report to the Devolutions support team to help reproduce the issue more easily.

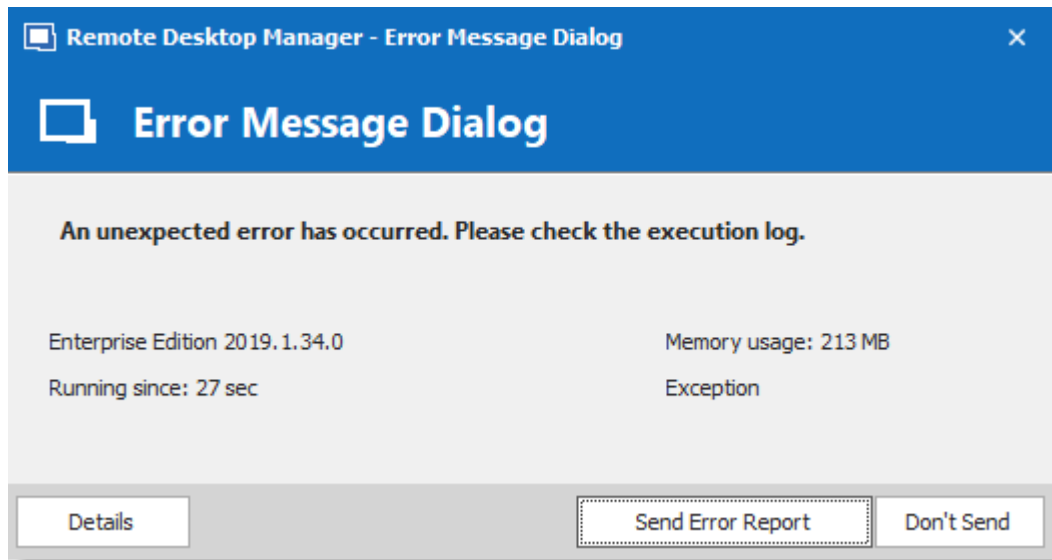


When sending your error report please make sure to include as many details as possible in the message section to ensure that our support team reproduces the issue with ease.

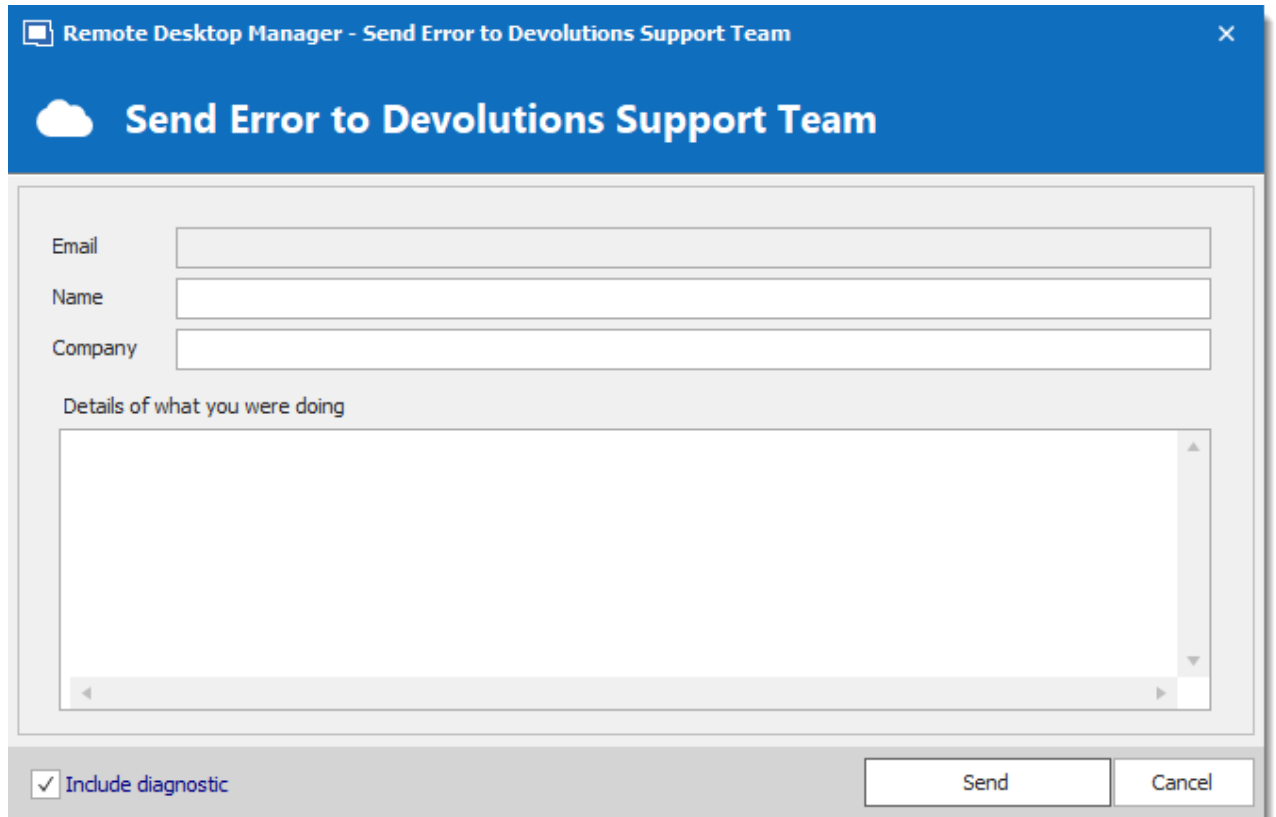
## SEND AN ERROR REPORT

When an error dialog appear in Remote Desktop Manager follow these steps to send it to the support team.

1. Press the **Send Error Report** button.



2. Fill in your contact information along with a detailed explanation on the issue and press OK.



Remote Desktop Manager - Send Error to Devolutions Support Team

Send Error to Devolutions Support Team

Email

Name

Company

Details of what you were doing

☒ Include diagnostic

Send Cancel

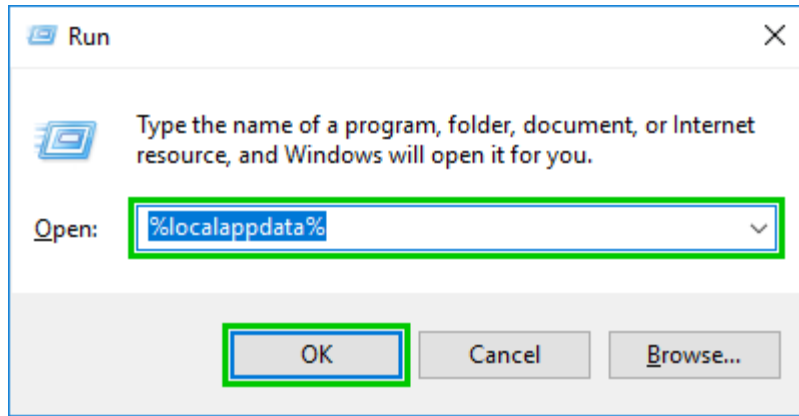
#### 10.1.1.12.1 Send configuration file

## DESCRIPTION

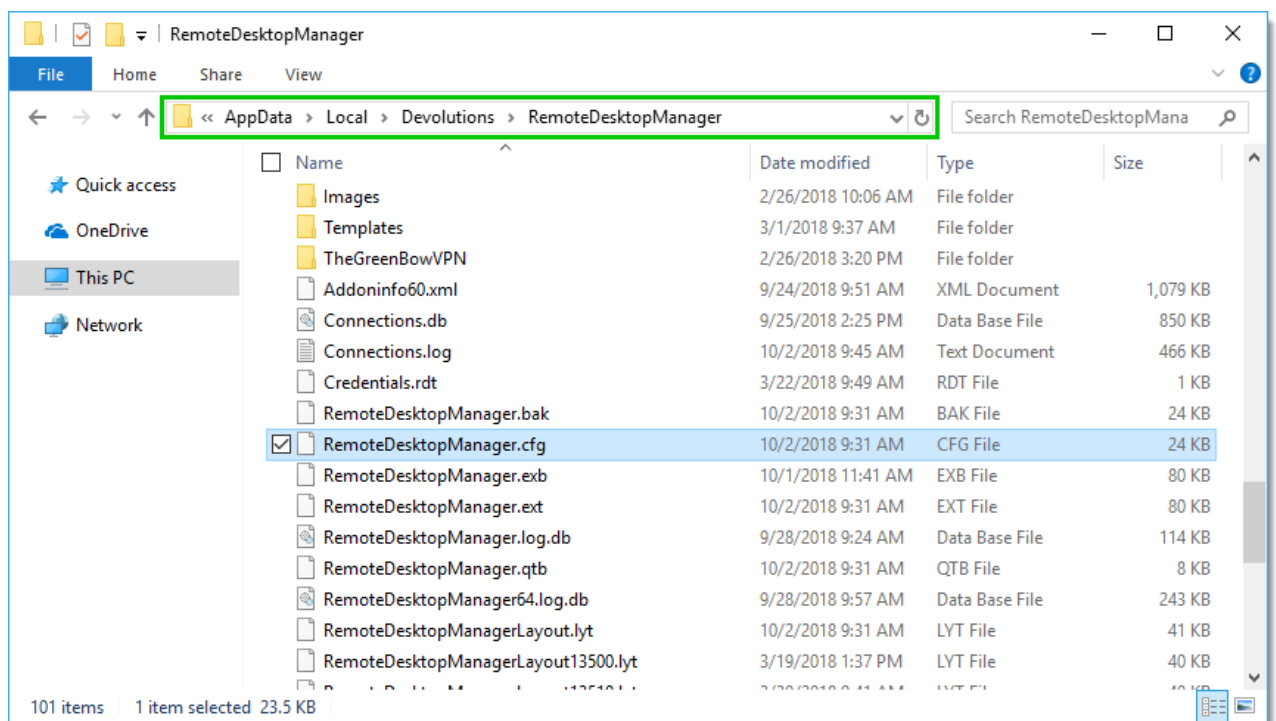
In some cases, the Devolutions team will need your configuration file to help reproduce a particular issue.

## SEND YOUR CONFIGURATION FILE

1. Press the **Windows key + R**.
2. Type **"%localappdata%"** in the **Run** window and press **OK**.



3. In the folder, locate the *RemoteDesktopManager.cfg* file.



4. Please send us the file securely via ShareFile.

#### 10.1.1.13 Upgrade from Free Edition to Enterprise Edition

## DESCRIPTION

These steps will help you get through the process of upgrading from the Free Edition of Remote Desktop Manager to the Enterprise Edition.

## STEPS



The Enterprise edition allows for a 30-day trial. Since both editions are **totally independent** from each other and can be operated side-by-side, this means that you can perform this procedure and still benefit of a trial for the Enterprise Edition features prior to making your decision.



File based data sources (XML, SQLite, etc) are by default stored in the configuration folder. As a precaution, go through each data source in **File - Data sources** and have a look at the local path (if any). Any file that is in the configuration folder must be copied manually.



The paths mentioned in this topic are for those that have installed using the default settings. The best way to locate your configuration folder is to use **File - Options - Advanced**, in this form you will find an hyperlink near the bottom. This opens your configuration folder. Please ensure you close the application before going further.

1. Install Remote Desktop Manager Enterprise edition. The download location is <http://remotedesktopmanager.com/Home/Download>.
2. Launch the Enterprise Edition once to have its own configuration folder initialized, then close it.
3. Open **%localappdata%\Devolutions\RemoteDesktopManagerFree**. You will copy files to **%localappdata%\Devolutions\RemoteDesktopManager** so you may wish to open another explorer window to that location.
4. Copy the following files to the RemoteDesktopManager folder:

**RemoteDesktopManagerFree.cfg**

**RemoteDesktopManagerFree.ext**

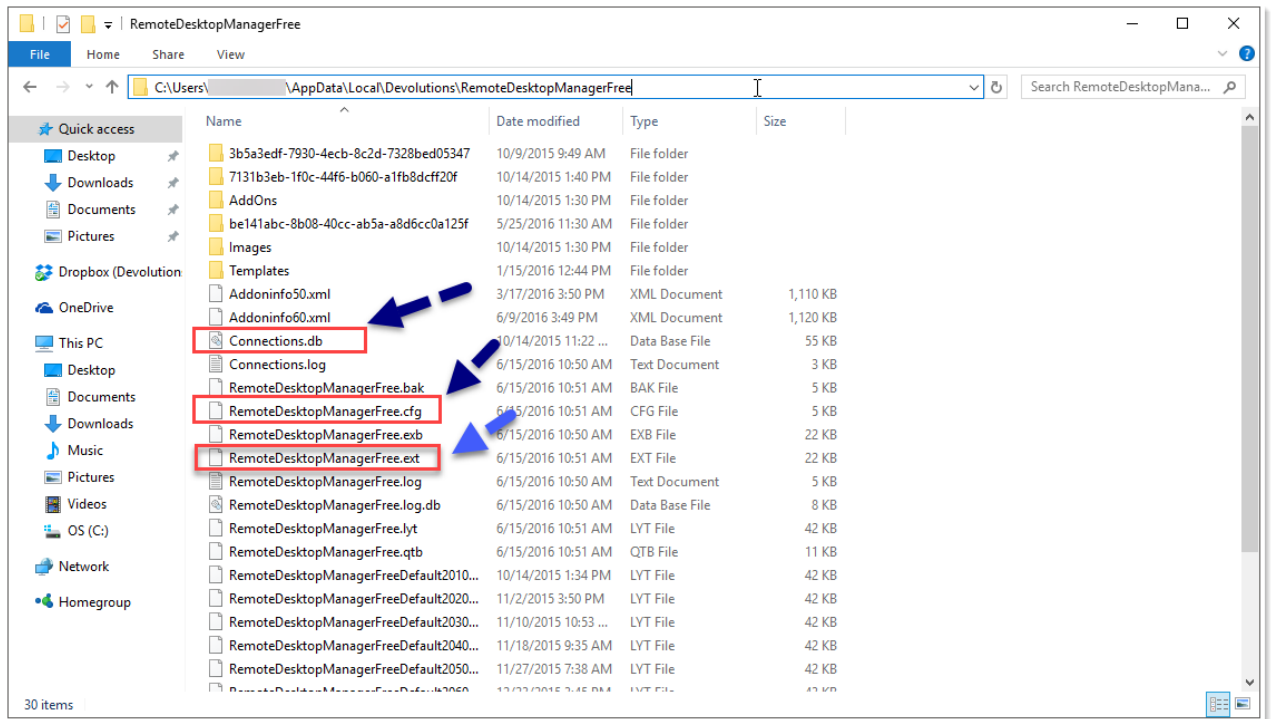
**Connections.db**. (default name of the Local Data Source)

Any and ALL other data source files identified in the Data sources list

5. Rename the copied file to remove the **Free** suffix.:

**RemoteDesktopManagerFree.cfg** to **RemoteDesktopManager.cfg**

**RemoteDesktopManagerFree.ext** to **RemoteDesktopManager.ext**



AppData Folder

Run the Enterprise edition and ensure all of your data sources are available.

Uninstall the Free edition **when you are sure** that everything is working as expected.

#### 10.1.1.14 Understand Remote Desktop Manager licensing

### DESCRIPTION



In the context of licensing, a user is an individual that uses Remote Desktop Manager. Credentials that are stored within Remote Desktop Manager have no impact on licensing.



Licenses are calculated **per user**, not per installation. There is no limitation on installing Remote Desktop Manager (laptop, desktop, home computer, etc), as long as you hold the proper number of licenses for each individual that connect to your system.





The licenses are for use by the customer that appears on the invoice. You cannot share your license with a sub-contractor or, in the case of a service provider, to one's customers. This applies even if you grant them access to a shared data source.

Four types of licenses are available to purchase, depending on the number of users:

- User license
- Site license
- Country license
- Global license

## USER LICENSE

These licenses are purchased individually. There must be a separate license for each individual who will have access to the software. This is akin to a **named user license**.

## SITE LICENSE

This license offers unlimited users on the same site (location). Remote workers who are based in another office are NOT included. A location is a workplace. If a user must work from another address, they need another license. Please contact [sales@devolutions.net](mailto:sales@devolutions.net) to describe your scenario and get help on which license to purchase.

## COUNTRY LICENSE

This license offers unlimited uses within a specified country. One license serial is delivered, which allows unlimited users at unlimited locations within the same country. Please contact [sales@devolutions.net](mailto:sales@devolutions.net) to get a quote.

## GLOBAL LICENSE

This license offers unlimited uses, worldwide. One license is delivered, which can be used for an unlimited amount of users at unlimited location around the world. Please contact [sales@devolutions.net](mailto:sales@devolutions.net) to get a quote.

### 10.1.1.15 Web protocol handler

## DESCRIPTION

A **Web Protocol Handler** (also called **URL Protocol Handler**) has been implemented in Remote Desktop Manager to be able to launch a session directly from HTML content. This can be very useful to call Remote Desktop Manager from a Configuration Management Database (CMDB) or even a Document Management System (DMS).



Internet Explorer and Mozilla Firefox execute the URL by clicking on it or by pressing Enter. However, with some other web browser such as Google Chrome, executing the URL normally results in a web search. These browsers may require to do **Ctrl + Click** or **Ctrl + Enter** to execute the URL.

## SCENARIOS

There are two ways of using the handler:

1. Generate a URL for a session (basically every entry type that connects to a remote device using a protocol).
2. Generate a URL for a template, this will allow you to specify the host name of the device you wish to connect to, but it will take the settings of the template.

## PARAMETERS

Here are the parameters used to build a protocol handler URL. These are for advanced scenarios. Only the **DataSource** and **Session** IDs are enough to open a connection.



Please note that the **DataSource** parameter overrides the data source which the application connects to at start-up. This applies even if the user is prompted for a data source to connect to when the application starts.

PARAMETER	DESCRIPTION
<b>DataSource</b>	Indicate the data source or the database ID.  Find them in the <b>IDs</b> section of the <b>Advanced properties</b> of an entry.

PARAMETER	DESCRIPTION
	A data source ID is unique per installation, which makes the URL usable only by the workstation where the data source has been created. By default Remote Desktop Manager generates the URL with the database ID.
<b>Session</b>	Indicate the ID of a session. Find it in the <b>Session ID</b> field in the <b>Advanced properties</b> of a session.
<b>Template</b>	Indicate the ID of the template of an entry. The <b>template</b> parameter retrieves some properties of a template and uses them against the <b>session</b> parameter. The <b>host</b> parameter is required when using the <b>template</b> parameter.
<b>Host</b>	Indicate the hostname or IP address of the remote device. Used along with the <b>template</b> parameter, or to override the <b>host</b> property of the <b>session</b> parameter.
<b>Port</b>	Indicate the port to use. Used to override the <b>port</b> property of the <b>session</b> or <b>template</b> parameter.
<b>Username</b>	Indicate the username to use. Used to override the <b>username</b> property of the <b>session</b> or <b>template</b> parameter.
<b>Password</b>	Indicate the password to use. Used to override the <b>password</b> property of the <b>session</b> or <b>template</b> parameter.
<b>Domain</b>	Indicate the domain to use. Used to override the <b>domain</b> property of the <b>session</b> or <b>template</b> parameter.
<b>Title</b>	Indicate the title of the tab when a session is launched using the Embedded (tabbed) display mode. This can be very useful when several sessions are launched at the same time.
<b>Filter</b>	Populate the Search field.

PARAMETER	DESCRIPTION
<b>Tabpage</b>	<p>Give the focus to a tab in the dashboard after the application has completed the startup procedure. Available only with the <b>Select</b> action. The possible tabs are:</p> <ul style="list-style-type: none"> <li>• <b>Overview</b></li> <li>• <b>Documentation</b></li> <li>• <b>Macros/Scripts/Tools</b></li> <li>• <b>Management Tools</b></li> <li>• <b>Information</b></li> <li>• <b>Attachments</b></li> <li>• <b>Logs</b></li> <li>• <b>Recordings</b></li> </ul>

## ACTIONS

- **Open**: open the specified connection.
- **Find**: find sessions by host.
- **Edit**: edit the specified connection.
- **View**: view the password of the specified entry.
- **OpenWithMacro**: open the specified with a macro.
- **Select**: select a connection in the Navigation Pane (allows to select a tab in the dashboard as well).

## SYNTAX

Syntax:

```
rdm://<action>?<parameter1>=<value>[&<parameter2>=<value>]
```

The base syntax of the protocol handler requires the **application protocol**, an **action** and **at least one parameter** to work with.

There are three rules to follow when constructing an URL for the protocol handler:

- The action is separated from the parameters with a question mark (?).
- Each parameter is assigned a value by using an equal sign (=).
- Parameter/Value pairs are separated with an ampersand (&).

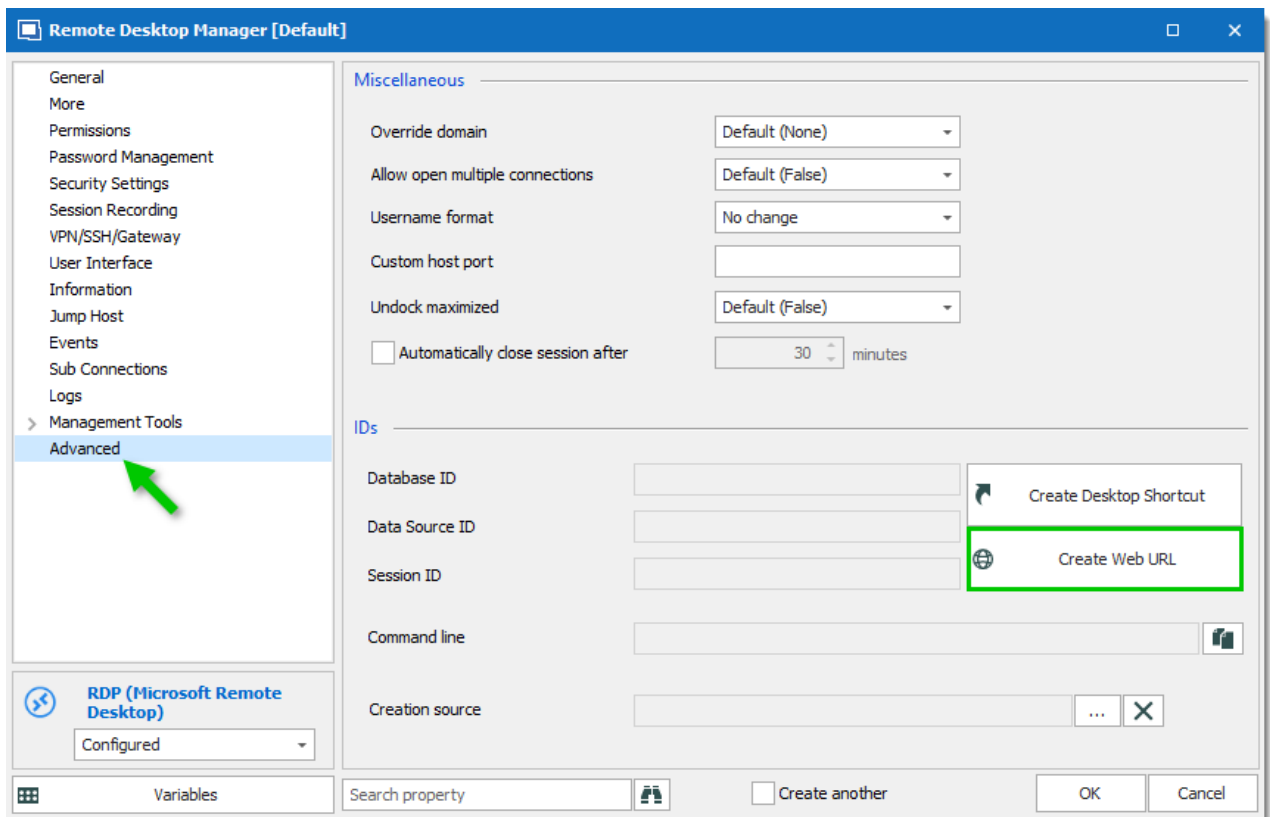
## EXAMPLES

### OPEN REMOTE DESKTOP MANAGER WITH THE SEARCH/FILTER FIELD POPULATED AND THE FOCUS ON THE DASHBOARD

```
rdm://open?Filter=RDP&TabPage=Dashboard
```

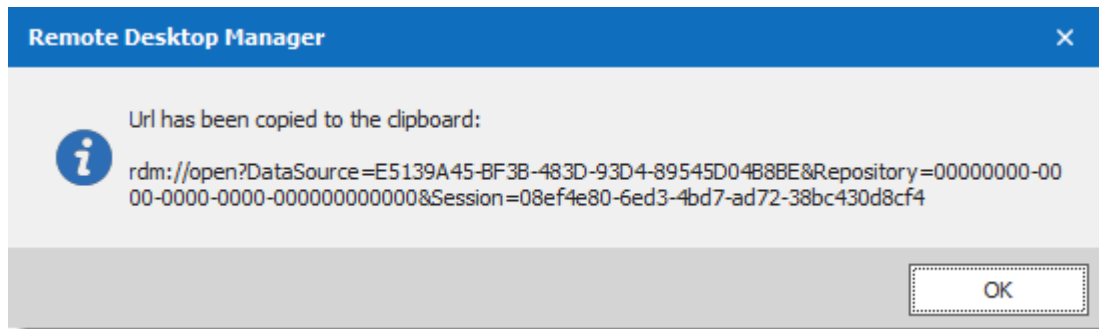
### OPEN AN RDP SESSION

1. In the **Advanced** section of an entry properties, click on the **Create Web Url** button.



Create Web Url

2. The Url is stored in the clipboard.



*Url copied to clipboard*

3. Paste (**Ctrl+V**) this Url in any application able to handle application protocols. It can be in a web page, a web browser address bar, or even a supported chat application. The protocol handler launches Remote Desktop Manager if it is closed, then perform the requested action with the provided parameters.

#### 10.1.1.16 Create a saved search with Smart Folders

## DESCRIPTION

Smart folders are saved searches. You can search by entry name and/or tag. The smart folder lists search results in the dashboard. You can open and edit entries directly from the smart folder. The folder updates dynamically; each time you open the folder it searches.

## ADD A SMART FOLDER

1. Click **New Entry**.
2. Click **Miscellaneous**, then select **Smart Folder**.
3. Enter the name for the smart folder. This is how the smart folder name will appear in the Navigation Pane. It is not for the search terms.
4. Choose the location.
5. Enter a search term and/or a tag.

To search for multiple terms, use:

"&&" for "and"

"||" for "or"

To select tags, click more options and a tag.

## USE A SMART FOLDER

1. Select the folder in the Navigation Pane.
2. You can work with an entry directly from the search results.  
Double-click to open an entry.  
Right-click to access actions in the context menu (e.g. View password or Select in dashboard).

The smart folder can be edited. It has the same settings as other entries.

### 10.1.1.17 Add an RDP entry

## DESCRIPTION

**RDP (Microsoft Remote Desktop)** and other tools that open remote connections are saved as **Session** entries Remote Desktop Manager. The entries store information about the host, credentials, local resources, and VPN, so users can open a session with one click. You can also set permissions, configure security settings and customize logs.

Here are the basics to get you started.

1. On the **Edit** tab, click **New Entry**.
2. Choose **RDP (Microsoft Remote Desktop)**.
3. Enter a **Name** for the session.
4. Choose a **Display** mode, the most common are:
  - **Embedded (tabbed)** opens a new tab in Remote Desktop Manager.
  - **External** opens in the external application.
5. Choose the credentials to use.  
To use credentials you have saved as a separate entry, choose **Credential repository** and select the entry from the list.  
Select **Default** if you want to enter the credentials directly in the entry.
6. Enter the **Host** address.

## OPEN A RDP SESSION

Click **Open Session** on the **Home tab** or **Dashboard**

You can open more than one session at once. With embedded sessions you can switch between the tabs or monitor connections simultaneously: use thumbnail view or [rearrange open sessions with split screen](#).

### 10.1.1.18 Quick Start

## DESCRIPTION

Welcome to Remote Desktop Manager! Here are three steps to quickly set up Remote Desktop Manager and start testing the features.

- [About the data source](#)
- [Import credentials from Keepass \(or other sources\)](#)
- [Save a RDP session](#)

If you want to learn more, see [our online help](#).

#### 10.1.1.18.1 About the data source

## DESCRIPTION

Remote Desktop Manager comes with a local SQL Lite data source. It is enough to quickly test out remote connections (e.g. SSH or Microsoft Remote Desktop) and other types of entries.

To try role-based access control, you need to add an advanced source.

To add a new data source, click **File – Data Sources**.

## LEARN MORE

[Choose a data source](#)

#### 10.1.1.18.2 Import credentials

## DESCRIPTION

Remote Desktop Manager imports credentials from 16 third-party applications. It is an efficient way to build your data. The imported information can be converted into different types of entry (e.g. username/password, Login (account), and Website).

You can use credential entries to open remote connections, saved as sessions in Remote Desktop Manager. Credential repositories link one credential or a list of credentials with a session.



To see the types of information you can import, go to **File – Import**.

## LEARN MORE

Watch this video for step-by-step instructions: [Import credentials from KeePass](#).

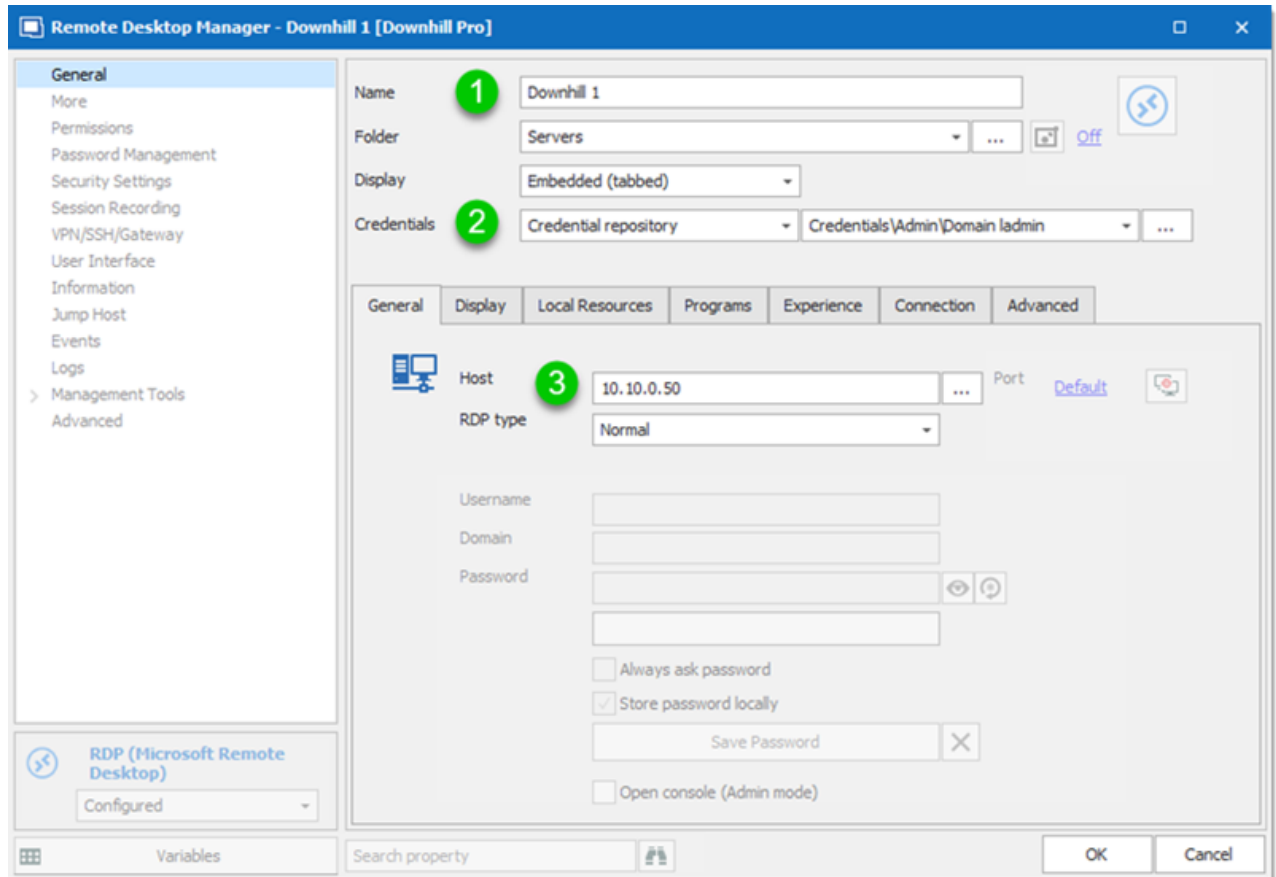
Read [how to import credentials in the online help](#).

10.1.1.18.3 Create a RDP session

## DESCRIPTION

When it comes to entries, there are a lot of different options. Here's a quick way to set up an **RDP (Microsoft Remote Desktop)** entry:

1. Name the entry
2. Enter the **Host** address
3. Choose **Credential repository** and link a credential entry with this session. You can also enter the username and password directly in the entry by choosing **Default**.



*RDP (Microsoft Remote Desktop) Entry Properties*

Then, you can open the session with one click.

Click **Open Session** on the Home tab.

## LEARN MORE

[More information about RDP entries](#)

[How to set up a VPN with a session](#)

### 10.1.1.19 SQL Server Always On Availability Groups

## DESCRIPTION

Main RDM clients and DPS are written using the .net platform, which means that the capabilities are often derived from .net libraries themselves.

As such, supported availability groups are a feature of the database driver used. All types are therefore supported:

- Multi-Subnet Failover
- Application Intent
- Read-Only Routing
- Multi-Subnet Failover: Faster Single Subnet Endpoint Failover
- Multi-Subnet Failover: Named Instance Resolution For SQL Clustered Instances

## 10.1.2 Remote Desktop Manager Jump

### 10.1.2.1 Configure Remote Desktop Manager Jump

#### DESCRIPTION



Please note that if your windows profile is corrupted Remote Desktop Manager Agent and Remote Desktop Manager Jump might not work.

Remote Desktop Manager Jump is built in Remote Desktop Manager desktop application (Windows only). This feature relies on the **Remote Desktop Manager Agent** and a full installation of Remote Desktop Manager on the local machine and the jump host.

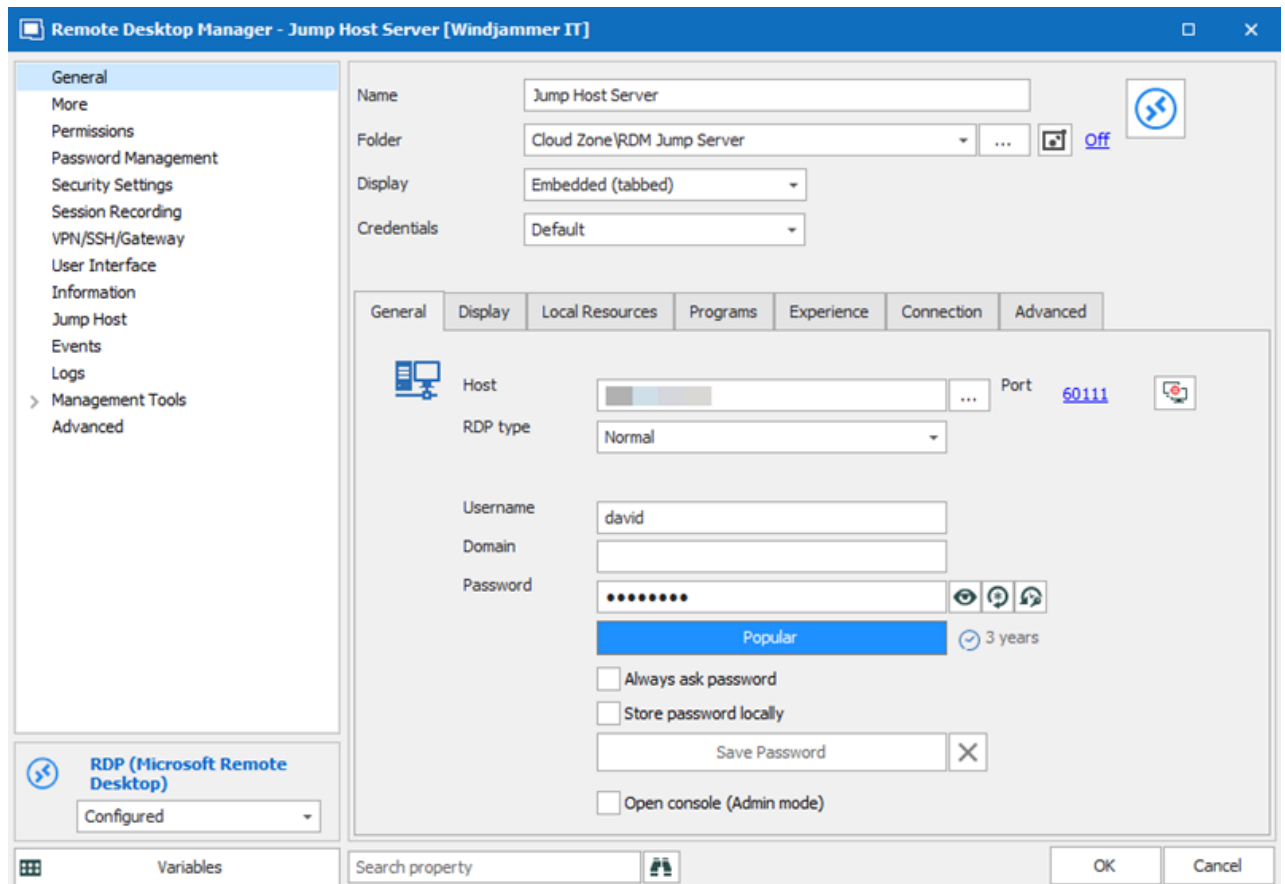
For an introduction on Remote Desktop Manager Jump, please consult the [Remote Desktop Manager Jump](#) topic.

#### GETTING STARTED WITH REMOTE DESKTOP MANAGER JUMP

#### PROCEDURE

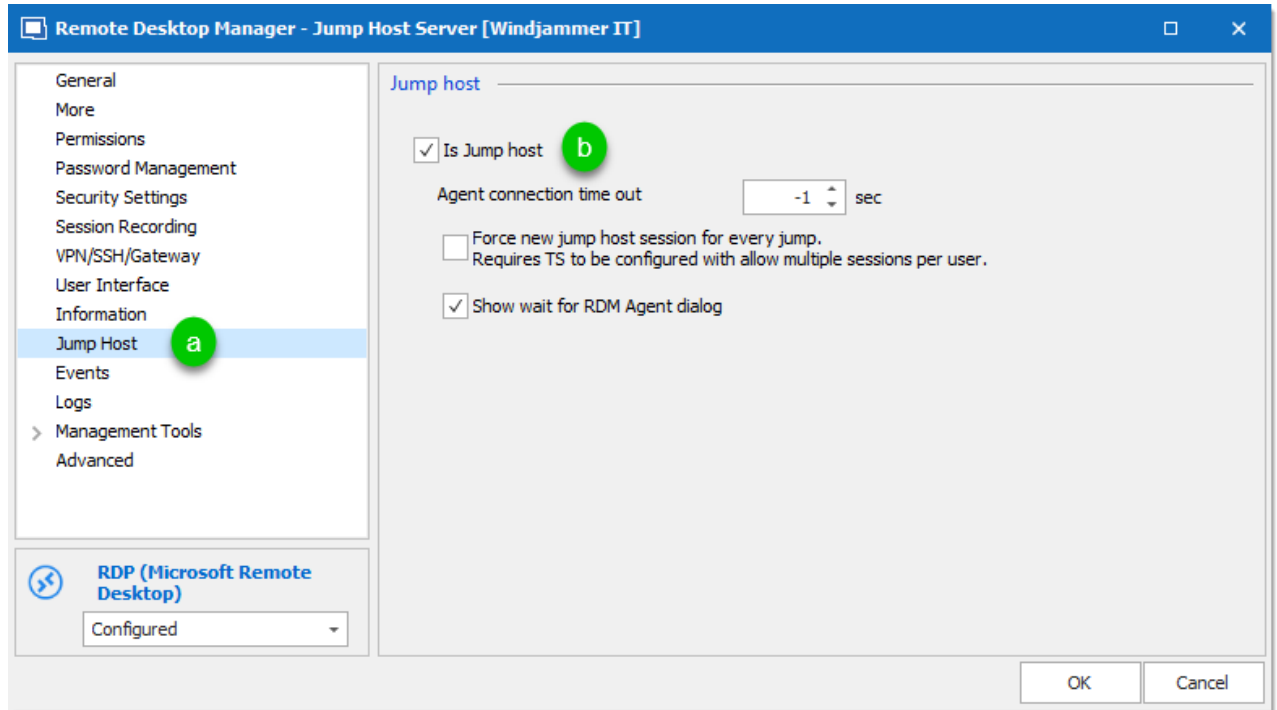
##### SET UP THE JUMP HOST

1. Add an RDP entry for the jump host. Enter a **name** for the session, **host** name and include **credentials**.



*Jump Host RDP entry properties*

2. Click **Jump Host** and check **Is Jump Host**.



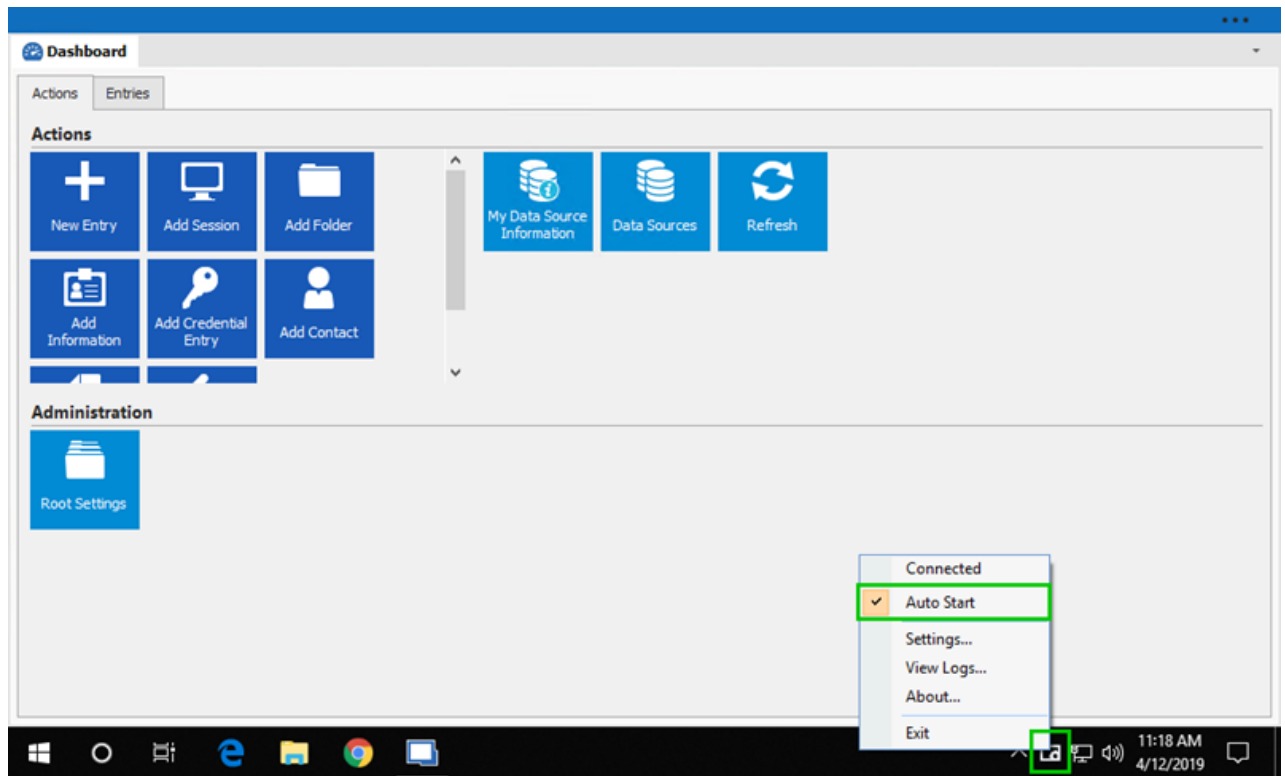
*Check Is Jump Host – Jump Host properties*

### 3. Open the Jump Host session.

- Install Remote Desktop Manager on the jump host. You can use the same license as your local instance.
- The application is installed with a local data source (SQL Lite). There is no need to add a data source because the jump host is only an intermediary between the local and remote hosts.

### 4. Confirm Remote Desktop Manager Agent is set to **auto-start**. Go to **Tools – More Tools** and select Remote Desktop Manager Agent. Click **Yes** to start the agent.

### 5. Right-click the Remote Desktop Manager Agent in the taskbar. Check **Auto Start**.



*Confirm Auto Start for Remote Desktop Manager Agent*

6. Adjust the user interface on the jump host to maximize the area to display remote sessions.
  - Make the application full screen.
  - Remove the Navigation Pane. Go to **View** and click **Navigation**.
  - Hide the ribbon. On the **View** tab, click **Top Pane**.

To show the ribbon again, click the blue bar at the top of the jump host instance of Remote Desktop Manager. To reset the layout, on the **Window** tab, click **Reset Layout**.

The jump host is ready to use.

### THREE THINGS TO REMEMBER:



Hide the **Ribbon** and **Navigation Pane**; it will make it easier to work. The menus are not needed. Hiding them provides more space in the dashboard.



Use the same **Remote Desktop Manager license** on the local and remote instances.

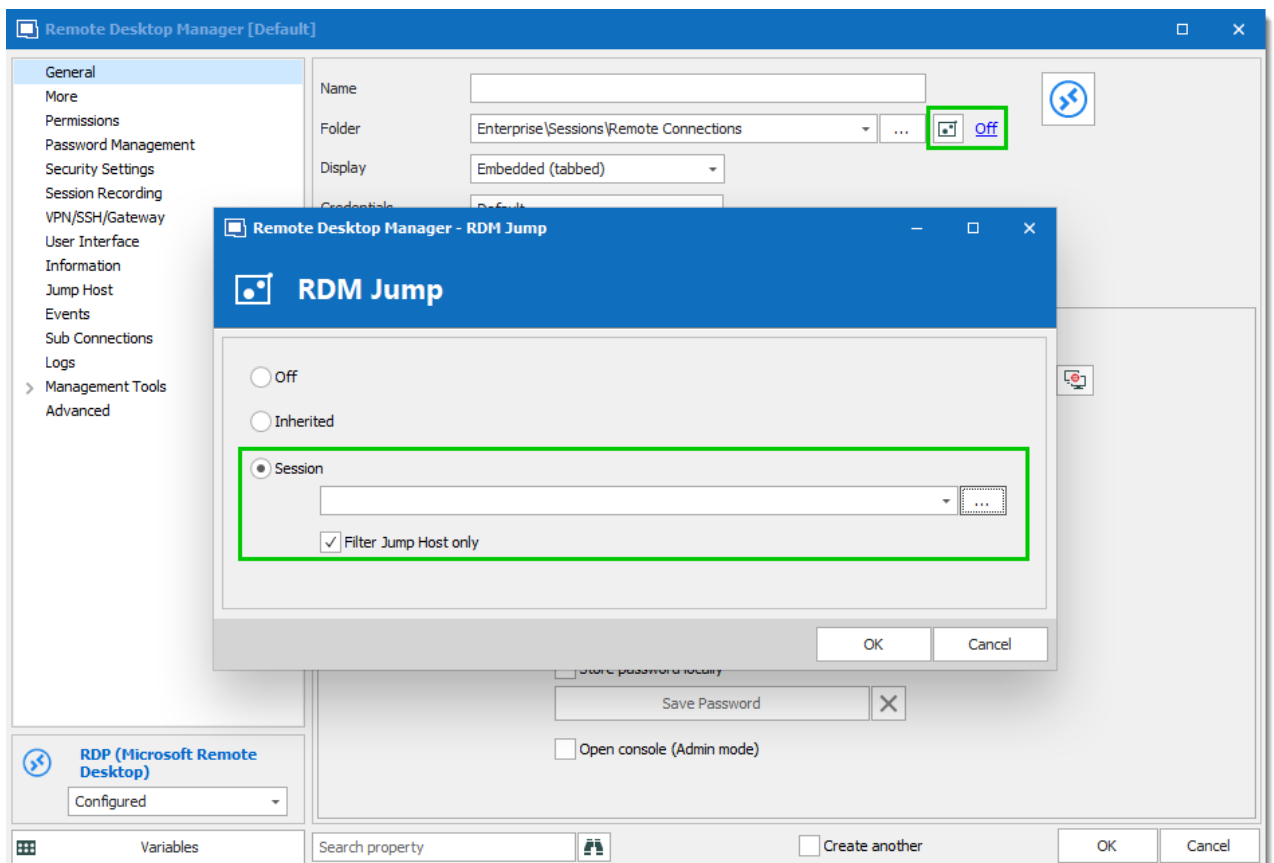
The jump host acts as a relay between the local and the remote systems, it is possible to use the Remote Desktop Manager license serial that has been used on the local workstation to register the application on the jump host.



There is no need to add a data source on the jump host. Remote Desktop Manager opens for first time with a default **Local Data Source**. This is sufficient because the application on the jump host only acts as an intermediate between the local and the remote hosts.

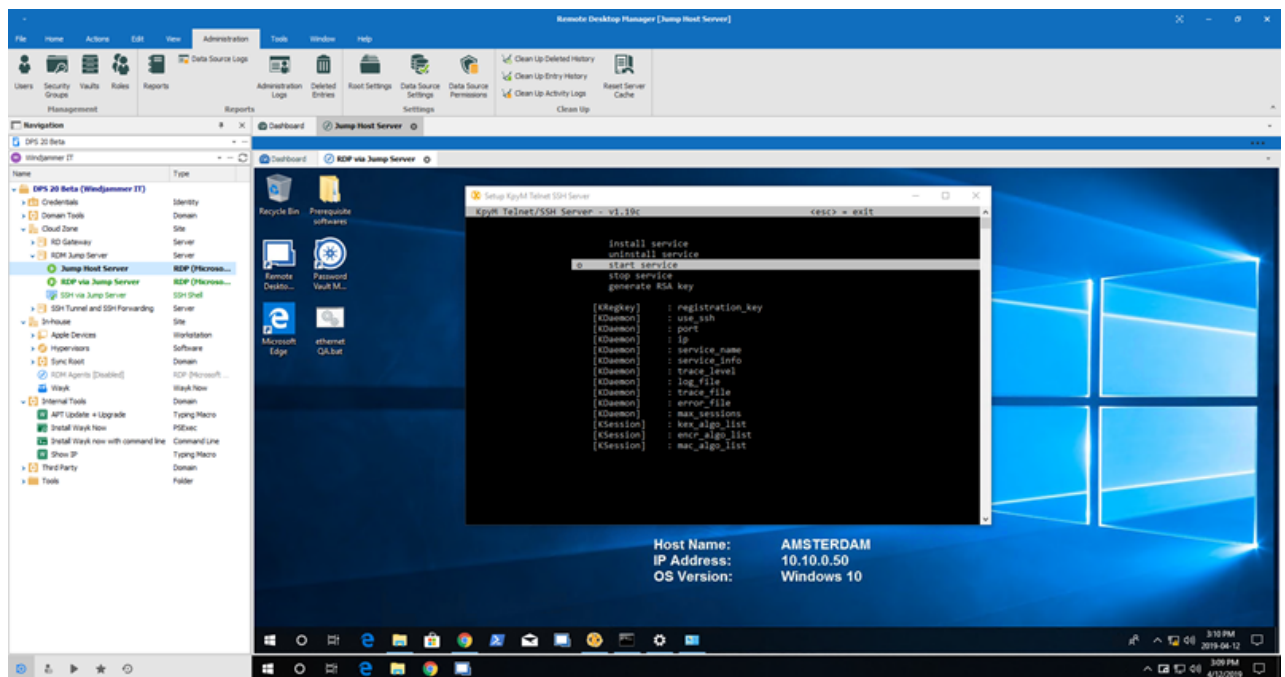
## CONFIGURE A SESSION TO USE THE JUMP HOST

1. On the local Remote Desktop Manager instance, create a session entry as usual. Set the jump host by clicking on the **RDM Jump settings** button. The jump host can be **Inherited** if the jump host is defined in the parent folder, or choose a specific **Session**.



*Jump host selection*

2. Click **Open Session**. The Remote Desktop Manager Jump opens automatically. It looks like a session in a session.



*RDP Session open with Jump Host*

## 10.1.3 RDP

### 10.1.3.1 Restoring the rdp file association with mstsc.exe

## DESCRIPTION

If you have elected to do so during the installation, the **\*.rdp** file extension has been associated with Remote Desktop Manager, this means that it does not use the **mstsc.exe** client from Microsoft anymore.

## SOLUTION

From an elevated command prompt (run as administrator), run the following command:

```
ftype RDP.File="%systemroot%\system32\mstsc.exe" "%1"
```

## TIP

Add the command above to the domain logon script to fix all of your users at once.



## 10.1.4 SSH

### 10.1.4.1 Configure an SSH Tunnel

#### DESCRIPTION

SSH tunneling is used to establish an encrypted connection over an untrusted network. It consists of an encrypted tunnel created through the SSH protocol, between an SSH client and an SSH server, providing a secure connection for data transfer. The SSH Tunnel can also be used to establish sort of a virtual private network (VPN) to access services across firewalls.

## 10.1.5 VMware

### 10.1.5.1 Configuring VMware's PowerCLI for use by Remote Desktop Manager

#### DESCRIPTION

The [VMware PowerCLI](#) is used by Remote Desktop Manager to interact with vSphere/vCenter in three distinct cases:

1. Getting the list of virtual machines from a vSphere/vCenter;
2. Performing operations on these virtual machines (start, stop, etc); and
3. Launching a VMware Remote Console.



Some operations are not allowed on the Free edition of VMware Esxi. All operations acting on the state of the virtual machine need the vSphere API license.

As a service to our community, we will provide the procedure to get the PowerCLI up and running. Please remember that this is not a product of Devolutions and that we have no control over breaking changes that may occur between versions of the PowerCLI. You should always refer to the manufacturer's documentation.

#### PROCEDURE



This procedure is valid for version 6.5 of VMware's PowerCLI.



The [bitness](#) of both Remote Desktop Manager and the PowerCLI must be taken into account for this procedure. Since these steps are performed only once, we would recommend that you follow the procedure for BOTH the 32 bit and 64 bit editions of the PowerCLI.

1. Ensure that PowerShell's script execution policy is configured. Please refer to Script Execution Policy.
2. Launch VMware vSphere PowerCLI using the shortcut on your system, this is the 64 bit version (using **Run As Administrator**).
3. Launch VMware vSphere PowerCLI (32-Bit), adjust both windows side by side (using **Run As Administrator**).
4. In both windows, set the SSL certificate setting of your choice. Obviously deploying a valid certificate on the vSphere server and trusting the Certification Authority is the most secure route. In secure environments or in a low-risk setting, we simply set to ignore.

```
set-PowerCLIConfiguration -invalidCertificateAction "ignore" -confirm:$false
```

5. Connect to a vSphere/vCenter server. If there are prompts by the PowerCLI, respond accordingly.

```
Connect-VIServer {your server}
```

6. Run the following command to see if there are error messages:

```
Get-View -ViewType VirtualMachine | select -Property Name, {$_ .Moref.Value};
```

If you see no error messages, you can close both PowerCLIs and you are now ready to test it using Remote Desktop Manager.

## 10.1.6 Tips and tricks

### 10.1.6.1 Use Multiple Versions of a Third Party Application

## DESCRIPTION

You have 2 different versions of an application installed on your workstation and you want to be able to use both versions within Remote Desktop Manager.

## SETTINGS

When you configure your **Application Installation Path** in **File – Options – Path**, separate the 2 paths by a semi-colon (;).

Remote Desktop Manager will prompt you with the selection list and you will be able to pick the one that you want to use.

### EXAMPLE

`C:\Program Files\Appsv1;D:\Program Files\Appsv2`

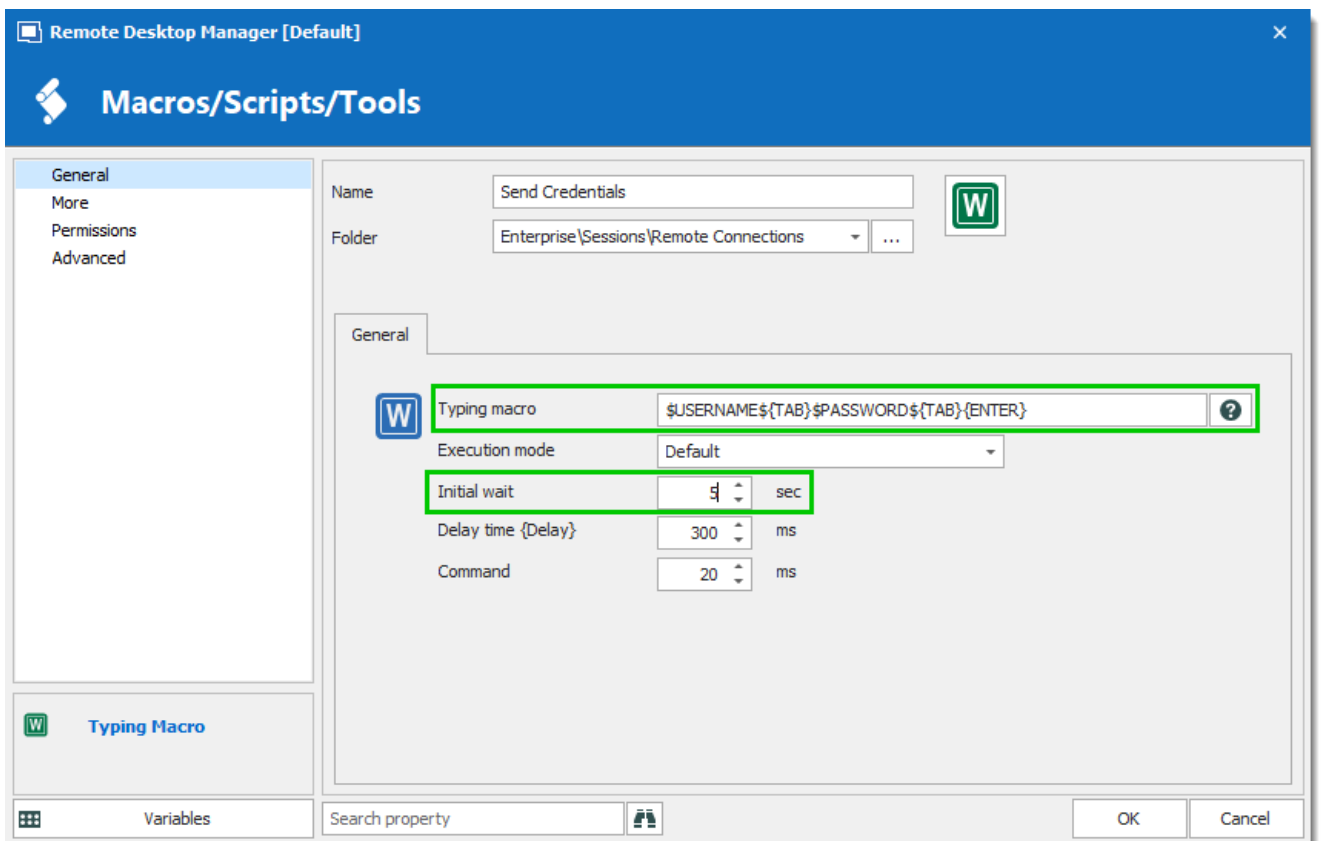
#### 10.1.6.2 Sending Windows Credentials inside TeamViewer

### DESCRIPTION

Many users have requested the ability to automate the login process on a Windows system through TeamViewer.

Since we are not able to send the password automatically inside the TeamViewer session, you would need to accomplish this with a typing macro.

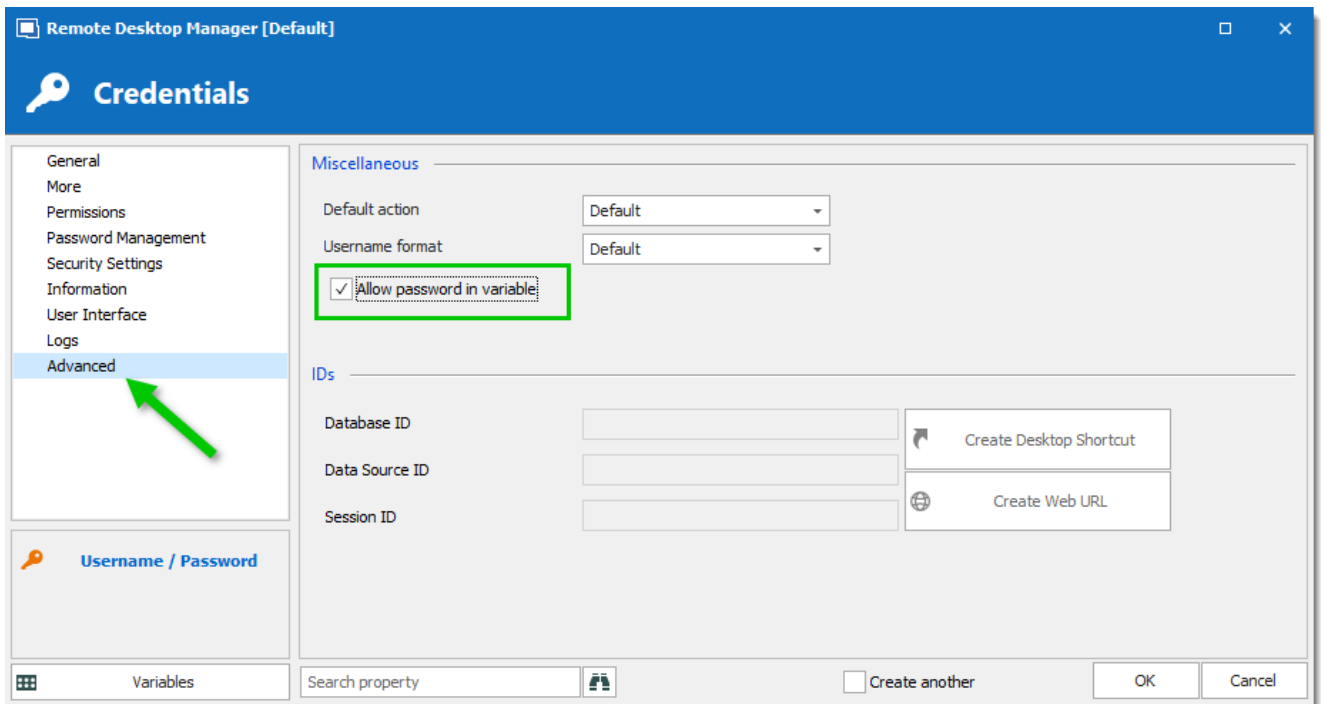
First, the typing macro session should look like the following;



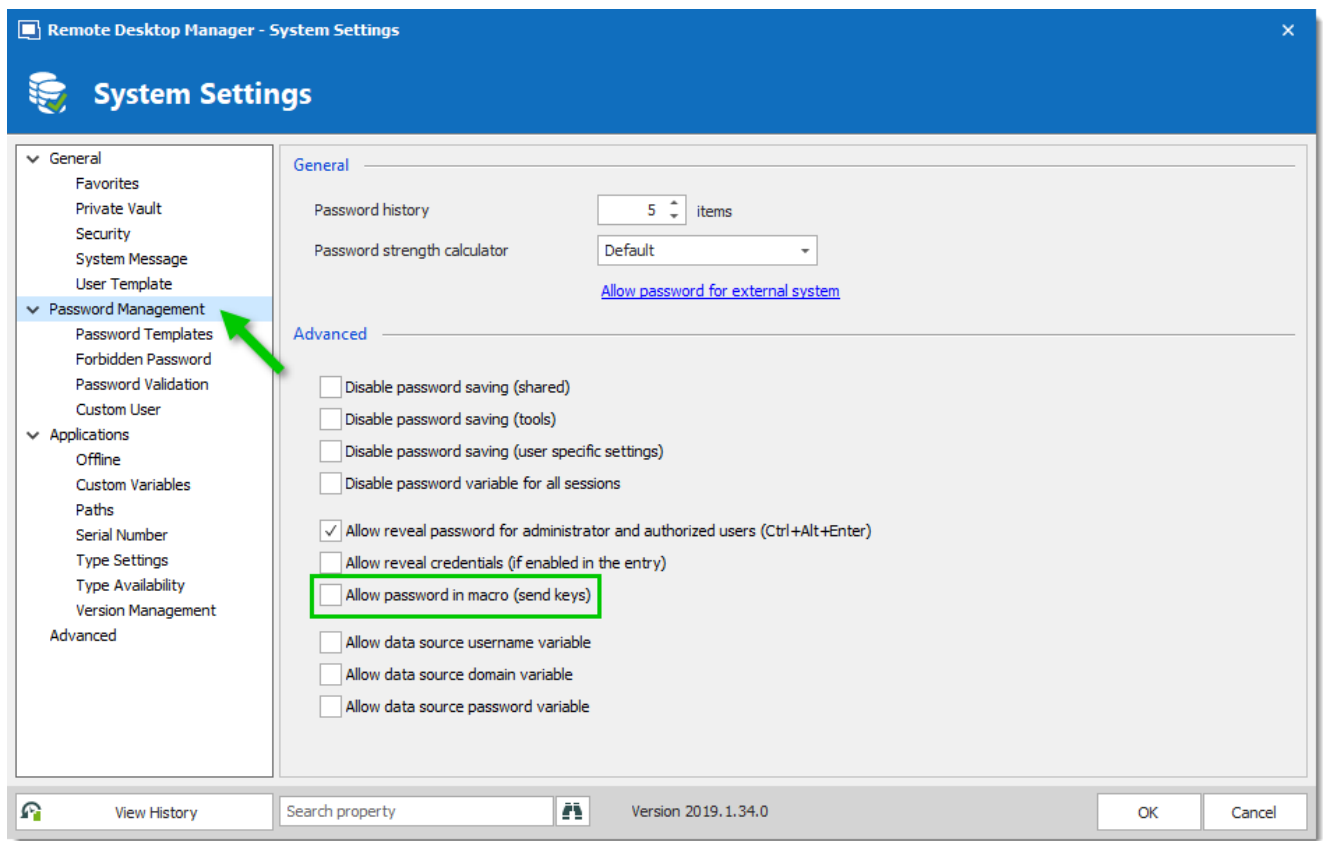
*Macro Entry Details*

Please note that the initial wait has been configured to 5 seconds, this varies depending on each user system.

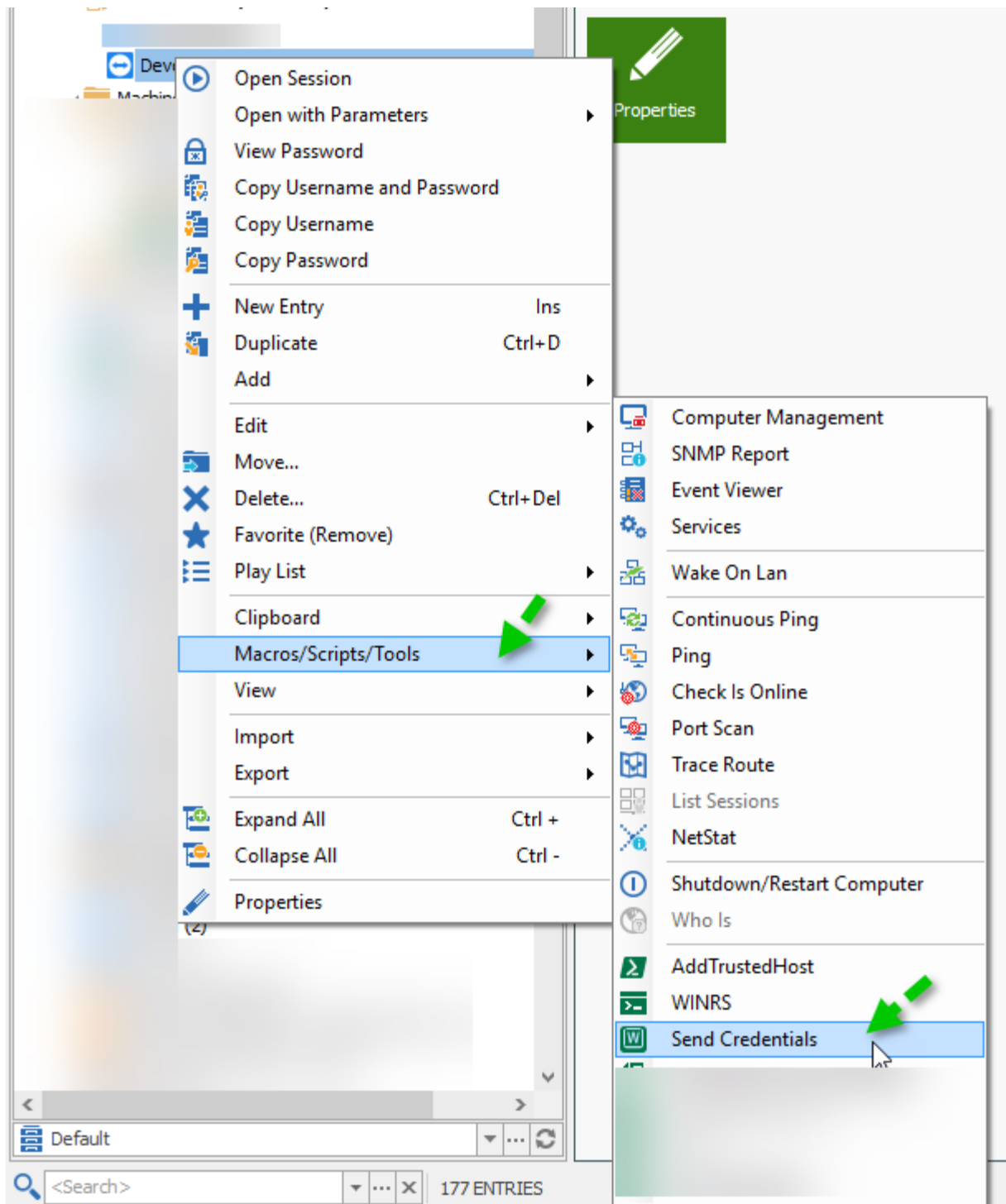
Now, in the properties of your Credential entry, you will enable the **Allow password in variable** in the **Advanced** section.



If you have an Advanced Data Source, in **Administration – Data Sources Settings (System Settings) – Password Management**, you will need to enable the **Allow password in macro (send keys)** option.



The next step happens when the TeamViewer session is opened and credentials are ready to be entered. Right-click on your credential entry and select **Macros/Scripts/Tools -> Send Credentials** (or whatever name you gave your entry).



In conclusion, put the mouse cursor in the appropriate login field and the typing macro will do the rest.

## 10.2 Performance

### 10.2.1 Memory Tuning Of RDP Sessions

#### DESCRIPTION

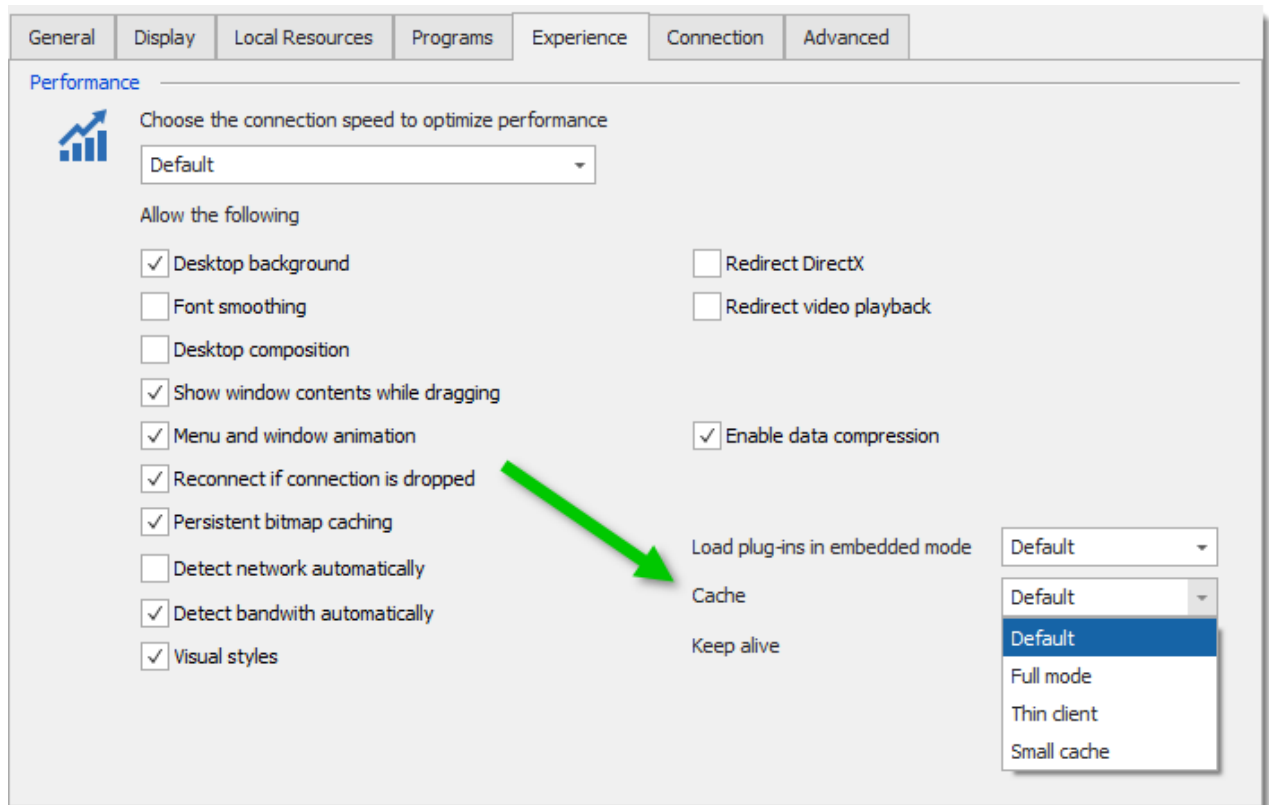
RDP sessions using version 8 of the protocol, namely Windows 8 and Windows 2012, consume more memory than previous versions of the protocol. For those of you that open many sessions concurrently, this sometimes forced you into using the 64 bit version of Remote Desktop Manager.

By default, the RDP protocol will reserve a sizable chunk of memory right from the start of a session for caching purposes, but we have some level of control over that. In the **Experience** tab of the RDP session, there is a **Cache** setting that you can use to control the behavior. It's values are as follows:

VALUE	DESCRIPTION
<b>Default</b>	Uses the value set in <i><b>File – Options – Types – RDP – Cache.</b></i>
<b>Full Mode</b>	The protocol is full Windows 8 Remote Desktop Protocol cache.
<b>Thin client</b>	The protocol is limited to using the Windows 7 with SP1 RemoteFX codec and a smaller cache. All other codecs are disabled. <b>This protocol has the smallest memory footprint.</b>
<b>Small cache</b>	The protocol is the same as <b>Full mode</b> , except it uses a smaller cache.

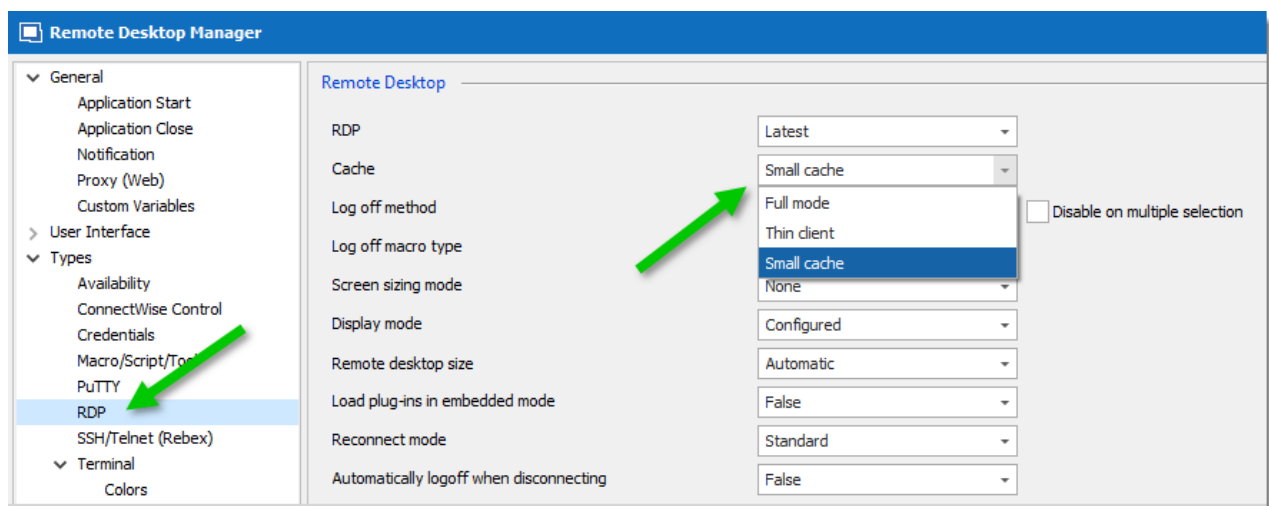
Choosing **Thin client** is therefore the choice that limits memory consumption the most, but will downgrade to the previous version of the protocol. The **Small Cache** mode may be sufficient for your needs if you need the newer features of the RDP protocol.





*RDP Type cache settings*

You might wish to set this for all sessions. In this case, go to **File – Options – Types – RDP** to assign the default value, then in all of your sessions use **Default**.



*Details of the RDP global options*

## 10.3 Security

### 10.3.1 Blocking MS RDP to Only Use Remote Desktop Manager

#### DESCRIPTION

Some organizations want to centralize their Remote Desktop connections to be established from Remote Desktop Manager only. A few things need to be considered to implement this in your organization.

#### SOLUTION

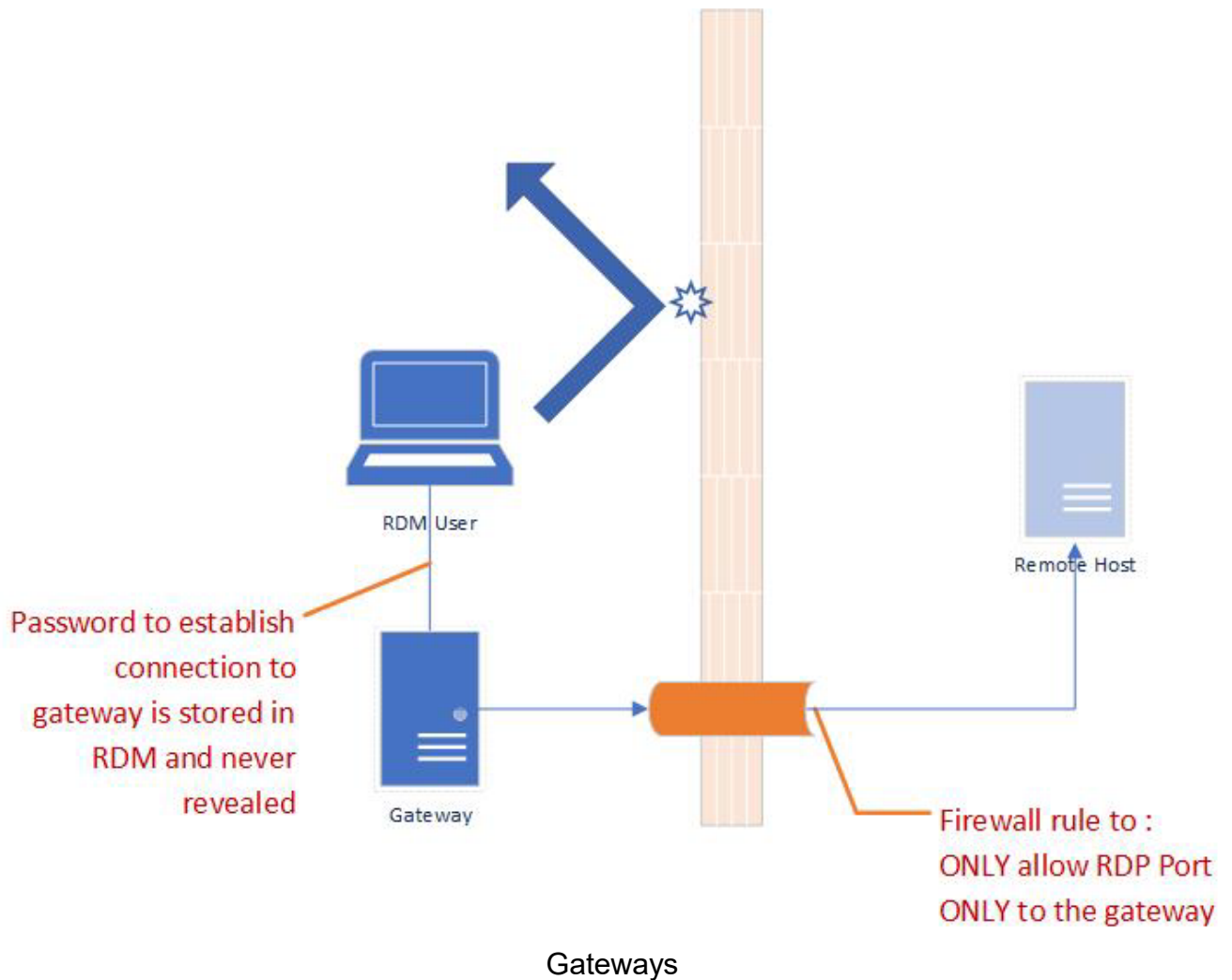
Just blocking Microsoft RDP (**mstsc.exe**) is still leaving other “surfaces” open for getting access. One could imagine installing Microsoft RDC Manager or even another copy of Remote Desktop Manager which would connect with settings that you do not approve.

Indeed, you can force your users to use Remote Desktop Manager by hiding the session credentials in the application. This will results in the users able to establish the remote connection without knowing the credentials.

If you feel that disabling Microsoft RDP (**mstsc.exe**) is sufficient for your needs, it is documented on

<https://social.technet.microsoft.com/wiki/contents/articles/4980.how-to-enable-or-disable-remote-desktop-via-group-policy-windows-2008.aspx>

Our best solution involves going through a gateway that is protected by a password unknown from the end user. One can achieve this by using a SSH Tunnel or our own Jump feature. The second step is to adjust the firewalls on the remote hosts to disable connections from IP addresses other than those use by your approved gateways.



SSH tunnels are a very good approach since they can run on a VM using any \*nix distribution and require limited ram and hdd space.

This will also force your user to use Remote Desktop Manager because the credentials to use a SSH Tunnel cannot be a domain credential and the information to authenticate will be saved in Remote Desktop Manager.

For more information, please consult [How to Setup a SSH Tunnel](#)

### 10.3.2 Certificate validation

#### DESCRIPTION

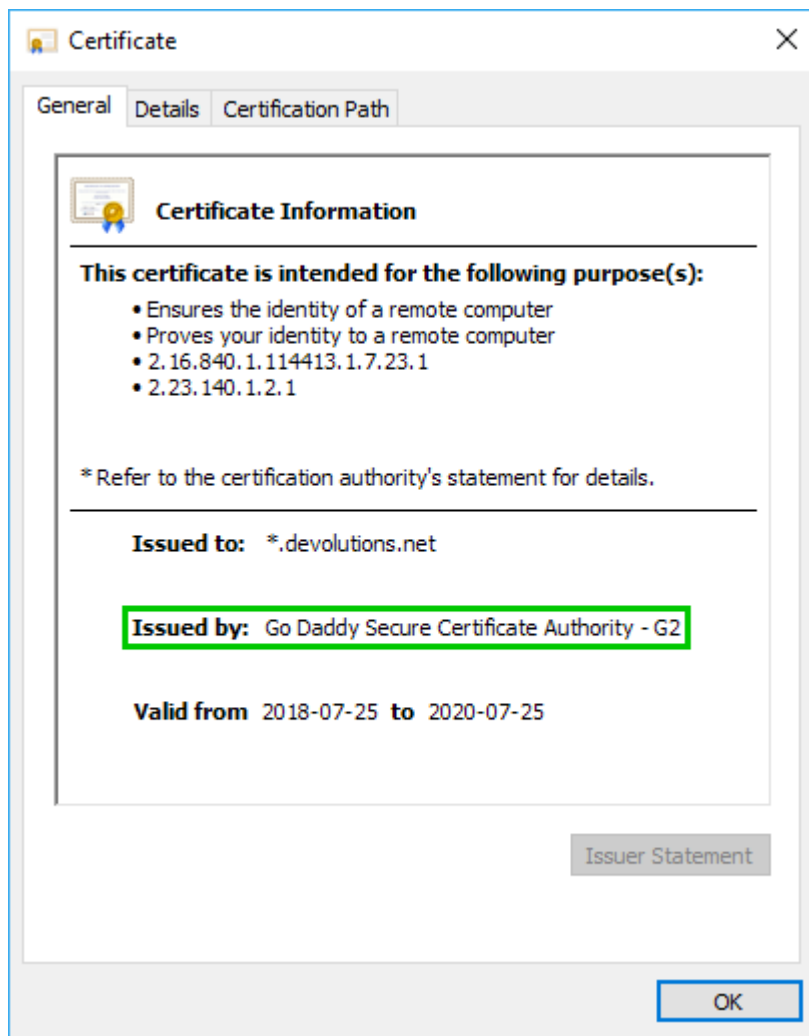
Remote Desktop Manager can validate certificates against the certificate store. However, ensure to only validate certificates from a trusted certification authority.

This topic covers:

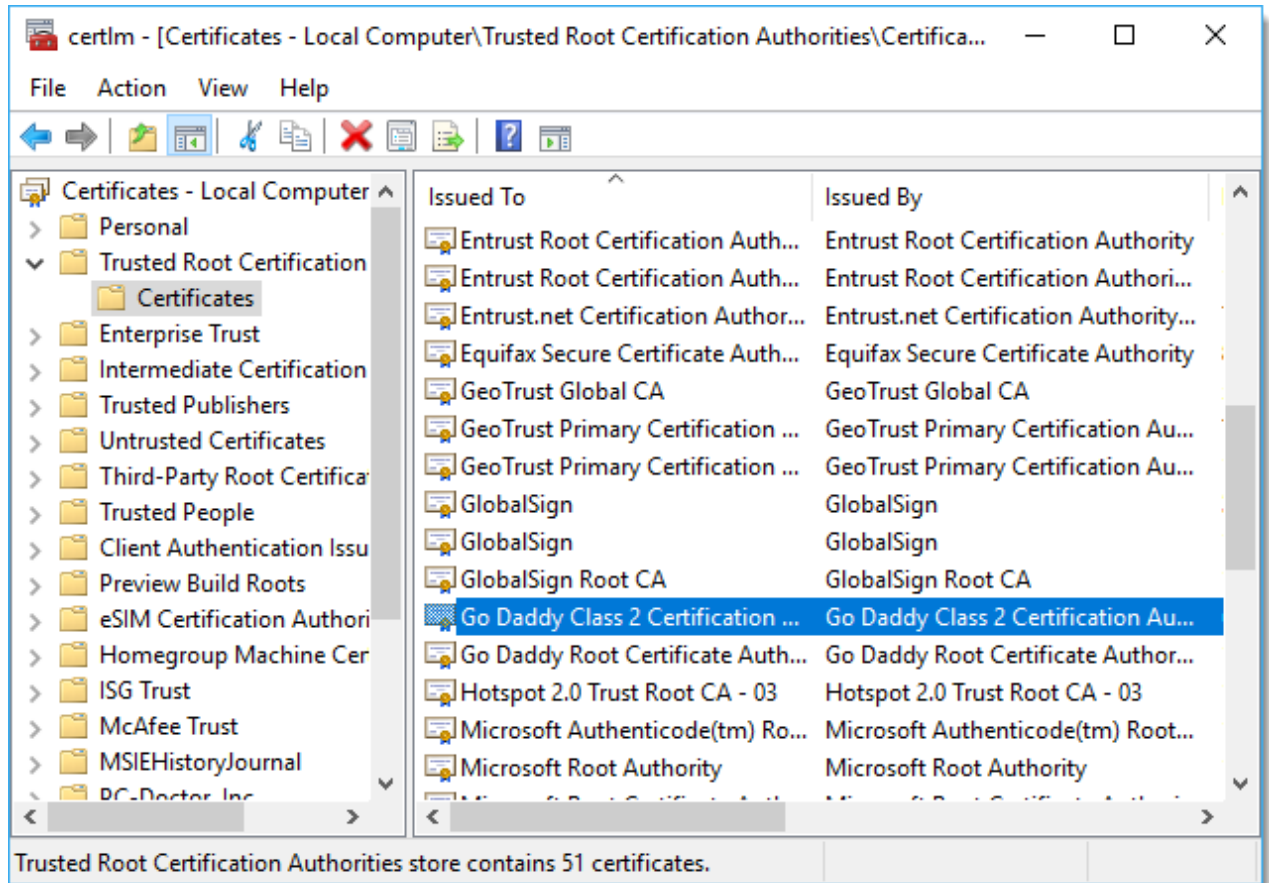
- Verifying the Certification Authority (CA).
- Remember a certificate.
- Certificate options.
- Troubleshooting steps for certificate errors.

## VERIFY THE CERTIFICATION AUTHORITY (CA)

1. Open the certificate, then verify by which Certification Authority the certificate has been **issued by**, in the **General** tab.

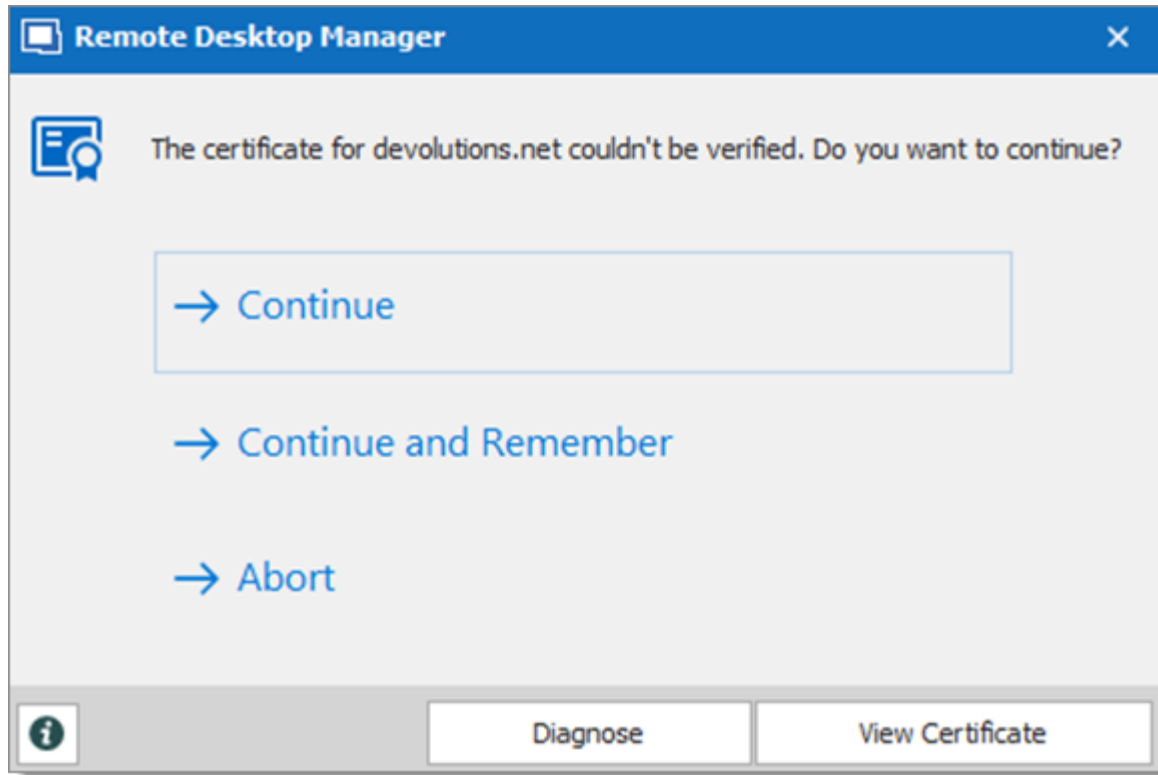


2. Verify that the Certification Authority is properly installed in the certificate store.



## REMEMBER A CERTIFICATE

It is possible for Remote Desktop Manager to remember a certificate when prompted to verify it.

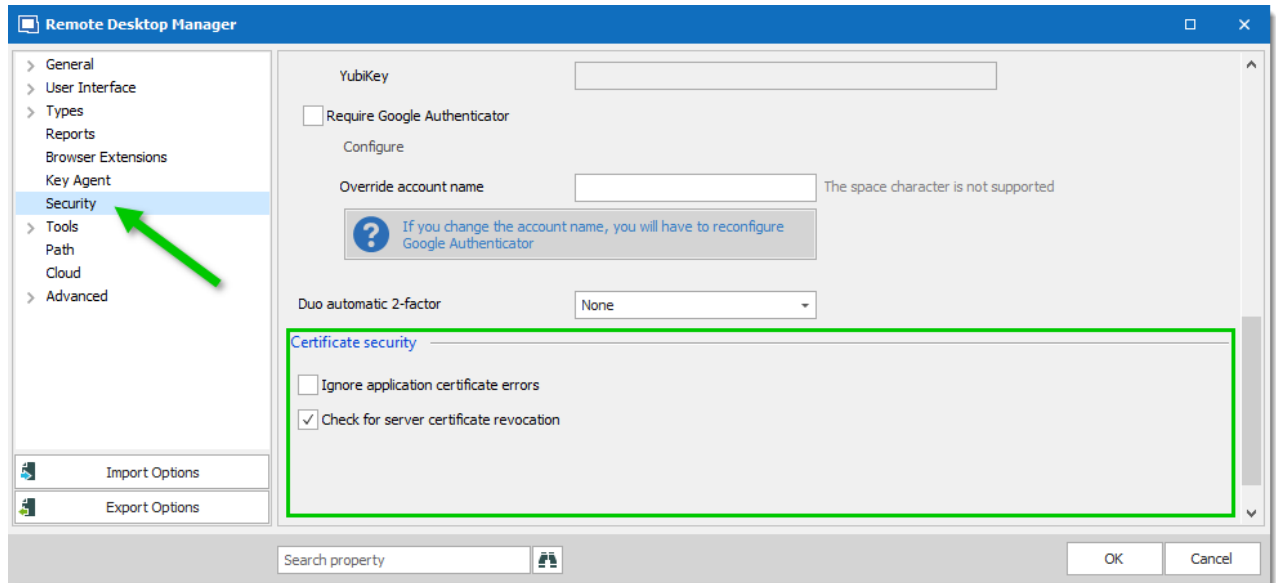


- For the current session only: click **Continue**.
- Until the cache is cleared: click **Continue and Remember**.

Always make sure that the certificate is valid before clicking on any of those choices. Verify the certificate by clicking **View Certificate**.

## CERTIFICATE OPTIONS

Navigate to **File – Options – Security – Certificate security** to manage options related to certificates.



## IGNORE APPLICATION CERTIFICATE ERRORS

Enable this option to disable the application certificate validation. This is not recommended, as it would compromise confidentiality and integrity of communications between the client and the server and could expose the application to potential threats.

## RESET KNOWN CERTIFICATES

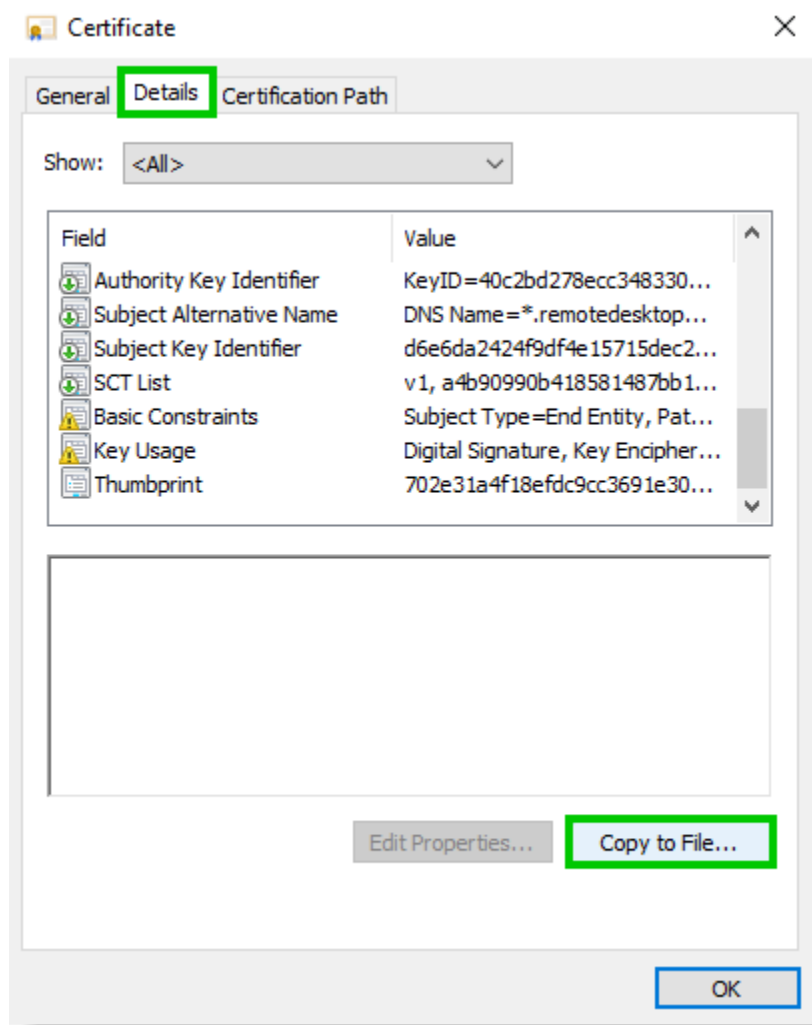
Use this option to clear the cached certificates. All certificates would need to be validated again.

## TROUBLESHOOTING

To find out more about why the certificate validation failed, you can use some tools, but you need to export the certificate first.

To export the certificate, follow these steps:

1. Click **View certificate** in the Remote Desktop Manager prompt.
2. Click on the **Details** tab of the Windows certificate prompt.
3. Click **Copy to File...** and proceed to export the certificate as a \*.cer file.



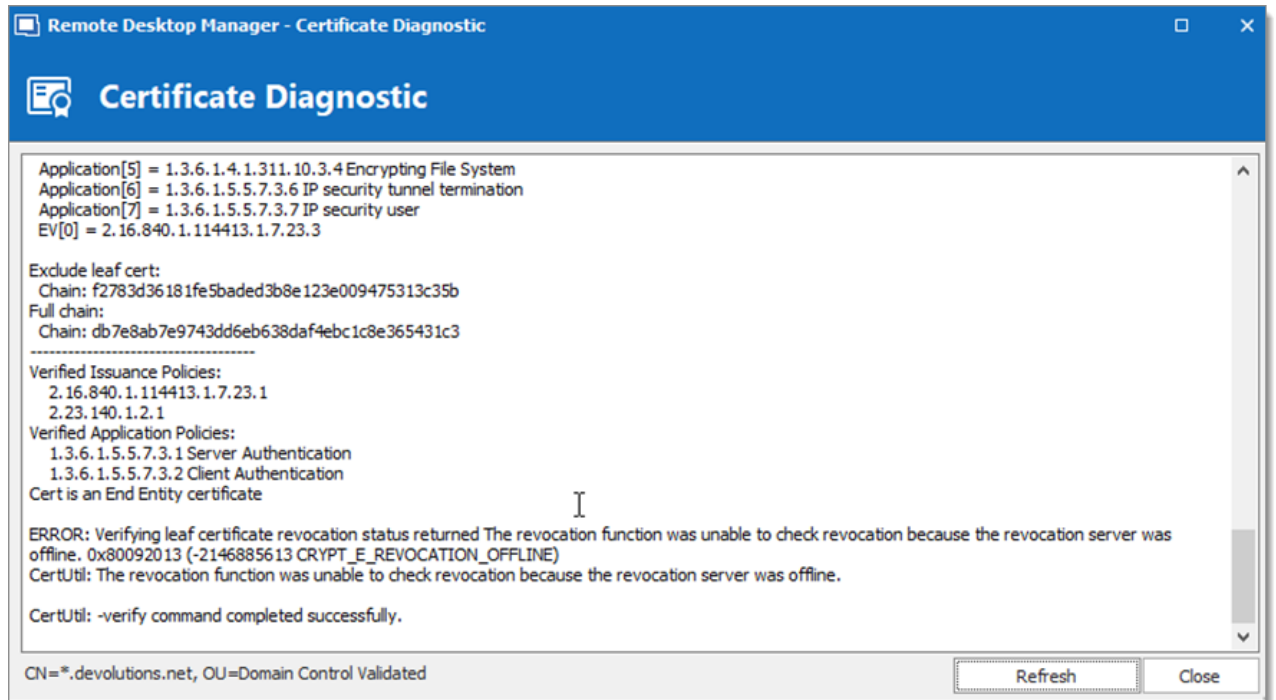
*Certificate Window*

## TOOLS

Here are some tools that can be used to verify the newly exported certificate:

1. Using the **Diagnose** button to get the certificate diagnostic.





## 2. Using PowerShell (requires PowerShell v4):

1.1 In a PowerShell console, replace the path below with the path of your certificate, then run:

```
$cert=New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("C:\
```

1.2 Then, run the following command:

```
Test-Certificate -Cert $cert
```

## 3. Using CMD:

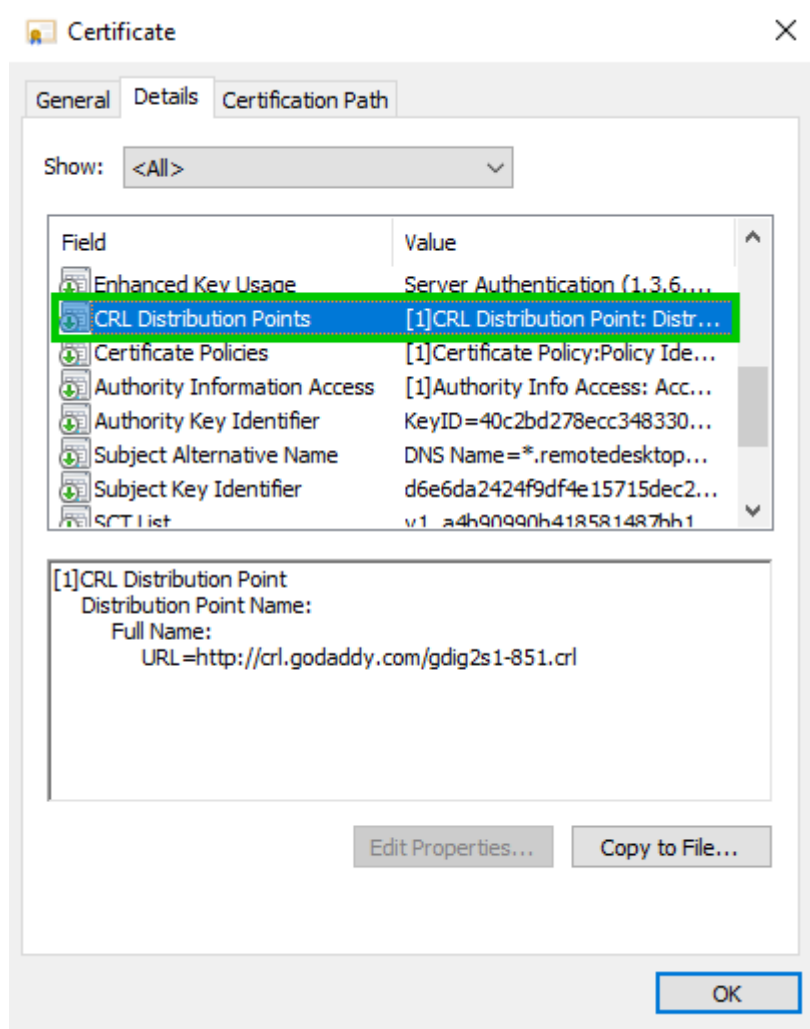
Run the following command (replace the path below with the path of your certificate):

```
certutil -verify "C:\Users\mmorrisette\Desktop\cert.cer"
```

The resulting output from those tools can be used to obtain more information about the encountered issue.

## COMMON ISSUES

- Root and Intermediate certificate authority are not properly installed in the Windows certificate store.
- Ensure that the proxy server blocks do not block the CRL (Certificate Revocation List) server as it is required to validate a certificate.

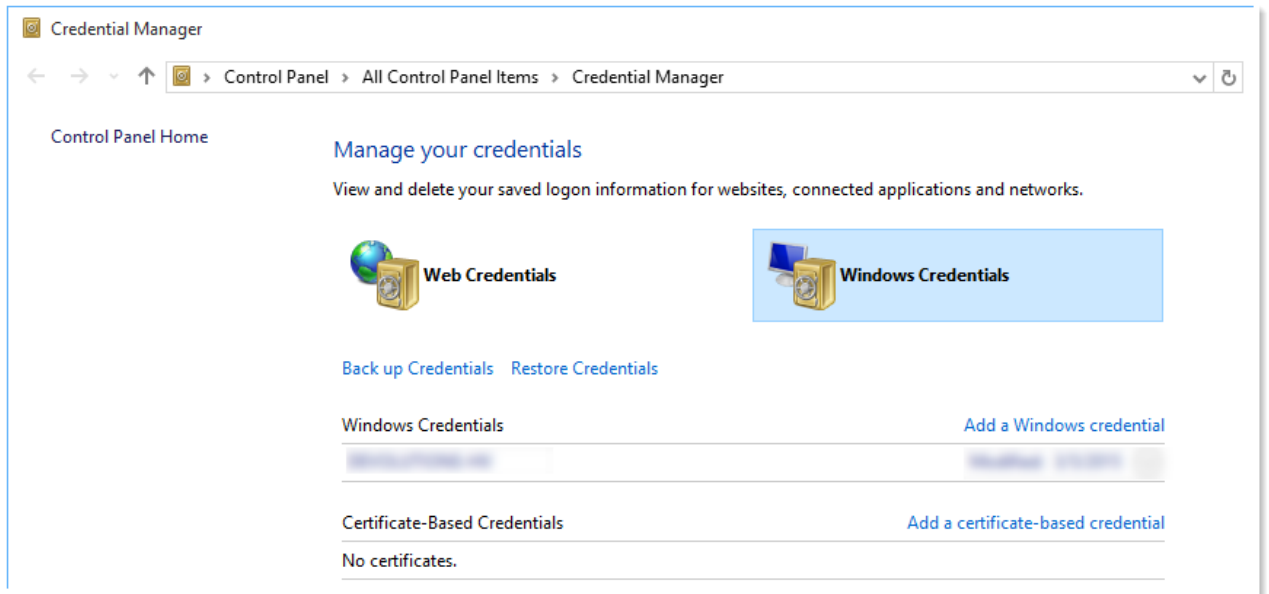


Certificate - CRL server

### 10.3.3 Windows Credential Manager

#### DESCRIPTION

The Windows Credential Manager allows you to store credentials, such as usernames and passwords, which you can use to log on to websites or other computers on a network. By storing your credentials, Windows can automatically log you on to websites or other computers. Credentials are saved in special folders on your computer called Vaults. Windows and other programs (such as web browsers) can securely give the credentials in these Vaults to other computers and websites.



### *Windows Credentials*

For information about saving credentials in Windows, see [Credentials Overview](#). You can also learn more in the [Windows Credential Manager](#) section.

# Technical Support

---

Part XI

## 11 Technical Support

**Hours:** Monday to Friday 7:30 a.m. to 6:00 p.m. EST

**Knowledge Base:** Find helpful information's and procedures regarding our [products](#).

**Email:** [ticket@devolutions.net](mailto:ticket@devolutions.net)

**Forum:** <https://forum.devolutions.net/>

**Language:** English-Français-Deutsch

**Phone:** +1 844 463.0419

### EXTENDED AND PREMIUM SUPPORT PLANS

Subscribers of a paid support plan receive an email address and a plan ID. You should send your support requests to the appropriate email address and provide your plan ID in the subject line.

Please consult our [Support Policy](#) for more information.



# Support/Resources

---

Part XII

## 12 Support/Resources

### 12.1 Keyboard Shortcuts

#### DESCRIPTION

Here are the default keyboard shortcuts for various commands. These can be modified in ***File – Options – User Interface – Keyboard***.

#### GENERAL

ACTION	SHORTCUT
Filter	Ctrl+F
Force Refresh	Ctrl+F5
Online Help	F1
Quick Connect	Ctrl+Alt+Q
Refresh	F5

#### EDIT

ACTION	SHORTCUT
Add Credential Entry	Alt+Shift+N
Add Folder	Ctrl+Shift+N
Add Information	Ctrl+Alt+N

ACTION	SHORTCUT
<b>Add Session</b>	Ctrl+N
<b>Delete</b>	Ctrl+Del
<b>Duplicate</b>	Ctrl+D
<b>Edit Entry</b>	Ctrl+E
<b>Local Specific Settings</b>	Ctrl+Alt+E
<b>New Entry</b>	Ins
<b>Rename Entry</b>	F2
<b>User Specific Settings</b>	Ctrl+Shift+E

## ACTIONS

ACTION	SHORTCUT
<b>Clipboard - Copy Connection String</b>	Ctrl+Alt+H
<b>Clipboard - Copy Domain</b>	Ctrl+Alt+B
<b>Clipboard - Copy Host Name</b>	Ctrl+H
<b>Clipboard - Copy Password</b>	Ctrl+Shift+B
<b>Clipboard - Copy Url</b>	Ctrl+Shift+H



ACTION	SHORTCUT
<b>Clipboard - Copy Username</b>	Ctrl+B
<b>Execute Typing Macro</b>	Ctrl+Shift+A
<b>Navigate URL</b>	Enter
<b>Open (Embedded/Tabbed)</b>	Ctrl+Enter
<b>Open (External)</b>	Shift+Enter
<b>Open (Full screen)</b>	Alt+Enter
<b>View Password</b>	Ctrl+P

## VIEW

ACTION	SHORTCUT
<b>Dashboard</b>	Alt+F6
<b>Details</b>	F12
<b>Favorites</b>	F10
<b>Grouped Tab Pane</b>	Ctrl+Alt+F9
<b>Header Pane</b>	Alt+Shift+F6
<b>Large Icons</b>	F6

ACTION	SHORTCUT
<b>Navigation Pane</b>	Alt+F8
<b>Opened Sessions</b>	F8
<b>Play List Management</b>	Ctrl+G
<b>RDP Toggle View Only</b>	Shift+F3
<b>Recent (Recent Used Entries)</b>	F9
<b>Status Bar</b>	Alt+F7
<b>Tabbed Entries Pane</b>	Alt+F9
<b>Tiles</b>	F3
<b>Top Pane</b>	Alt+F11
<b>Tree View</b>	F7

## NAVIGATION

ACTION	SHORTCUT
<b>Change Data Source</b>	Ctrl+Shift+D
<b>File</b>	Ctrl+Shift+F
<b>Focus Dashboard</b>	Ctrl+Shift+L

ACTION	SHORTCUT
<b>Focus Tab</b>	Ctrl+Shift+Up
<b>Focus Tree/List</b>	Ctrl+L
<b>Goto Bookmark 1</b>	Ctrl+1
<b>Goto Bookmark 2</b>	Ctrl+2
<b>Goto Bookmark 3</b>	Ctrl+3
<b>Goto Bookmark 4</b>	Ctrl+4
<b>Goto Bookmark 5</b>	Ctrl+5
<b>Goto Bookmark 6</b>	Ctrl+6
<b>Goto Bookmark 7</b>	Ctrl+7
<b>Goto Bookmark 8</b>	Ctrl+8
<b>Goto Bookmark 9</b>	Ctrl+9
<b>Select Next Tab</b>	Ctrl+Shift+Right
<b>Select Previous Tab</b>	Ctrl+Shift+Left
<b>Set Bookmark 1</b>	Ctrl+Shift+1
<b>Set Bookmark 2</b>	Ctrl+Shift+2
<b>Set Bookmark 3</b>	Ctrl+Shift+3
<b>Set Bookmark 4</b>	Ctrl+Shift+4

ACTION	SHORTCUT
<b>Set Bookmark 5</b>	Ctrl+Shift+5
<b>Set Bookmark 6</b>	Ctrl+Shift+6
<b>Set Bookmark 7</b>	Ctrl+Shift+7
<b>Set Bookmark 8</b>	Ctrl+Shift+8
<b>Set Bookmark 9</b>	Ctrl+Shift+9
<b>Switch Vault</b>	Ctrl+Shift+R

## IMPORT/EXPORT

ACTION	SHORTCUT
<b>Import Entries (.rdm, .pvm, .vnc, .rdp)</b>	Ctrl+Shift+I

## 12.2 Command Line Arguments

### DESCRIPTION

Remote Desktop Manager can be launched using a command line.



Some features are only available in the Enterprise edition.



Remote Desktop Manager also offers a Web Protocol Handler.

### Usage: RemoteDesktopManager.exe [parameters]

PARAMETERS	DESCRIPTION
<b>{filename [* .rdm]}</b>	Open in embedded or external mode the connection from file name.
<b>/Silent</b>	Execute the application minimized in a system tray icon. This option cannot be combined with other parameters.
<b>/Datasource:{datasource id}</b>	Specify the data source ID (available in the Advanced Tab of the session).
<b>/Session:{session ID}; {session ID}...</b> <b>/UserName:{username}</b> <b>/Domain:{domain}</b> <b>/Password:{password}</b>	Specify one or more session IDs (available in the Advanced Tab of the session).
<b>/ChangePassword:{new password}</b>	Change the session password. Only available for Remote Desktop sessions and embedded passwords. The data source ID and the session ID are required.
<b>/RegisterUser:"{registration user}"</b>	Change the Remote Desktop Manager registration name. The value must be in double quotes.
<b>/RegisterSerial:"{serial number}"</b>	Change the Remote Desktop Manager serial number. The value must be in double quotes.
<b>/Template:{template ID}</b> <b>/Host:{host name}</b>	Open the template ID with the specified host name and an optional username/password.

PARAMETERS	DESCRIPTION
<b>/UserName:{username}</b> <b>/Domain:{domain}</b> <b>/Password:{password}</b>	The template ID is the <b>Session ID</b> of the template (available in the Advanced Tab of the template).
<b>/Profiler</b>	Starts the profiler at start of application. Good for profiling the start process.
<b>/Title:"{title}"</b>	Specify a tab title when using an embedded session.
<b>/Filter:{filter}</b>	Execute the application with the filter filled with a parameter.
<b>/TabPage: Dashboard</b>	The Dashboard is selected at startup of the application.

## USAGE

### EXAMPLE #1 - OPEN A TEMPLATE AND CONNECT TO A HOST

```
RemoteDesktopManager.exe /DataSource:178c2fda-dab4-4f41-98df-6e3205c0a011 /Template:a666b
```

### EXAMPLE #2 - OPEN A SESSION

```
RemoteDesktopManager.exe /DataSource:178c2fda-dab4-4f41-98df-6e3205c0a011 /Session:474bcb
```

### EXAMPLE #3 - REGISTER THE APPLICATION

```
RemoteDesktopManager.exe /RegisterUser:"First name, Last name" /RegisterSerial:"xxxxx-xxx
```

## 12.3 Lexicon

## DESCRIPTION

Remote Desktop Manager is a feature-rich software that has an extensive set of functionality. Here are the major concepts that are important to understand in order to use the program to its full potential.

## DATA SOURCE

A container for entries. It can be a local file or a database (either local or shared). You can use multiple distinct data sources in the application, although only one is considered active at one point in time. See data source [Overview](#) for more information.

## ENTRY

All items in your data source are entries. There are multiple types. The entry is an abstract concept that serves as a container for all specific types.

## CREDENTIAL ENTRY

A credential is used to control access to a resource by identifying the user. It can be a classic username/password pair held by the application or even by an external source.

## INFORMATION ENTRY

An information entry can contain various information like account information, emails, serial numbers. Unlike credential entries, information entries are meant to be shared. Therefore, the data in the information entries is not encrypted. It's principal use in Remote Desktop Manager is to hold Web site information, from the URL to the credentials. This allows auto log in on the specified web site.

## CONNECTION

Any type of entry that allows you to connect to a remote host, service or device is a connection. An IP address or host name is normally used, as well as credentials.

## SESSION

In Remote Desktop Manager infancy, it was mainly aimed at managing Microsoft Remote Desktop. A **Session** was a term that was in use back then to describe a connection to









Microsoft Remote Desktop Services. It appears widely in our documentation. Any technology that connects to something and that needs to use authentication is a **Session**.

## 12.4 Follow Us



### OVERVIEW

Get the hottest information about our products - tips and tricks, case studies and new release announcements!

This is not a marketing newsletter. We focus on the issues that matter to you, whether you're looking for up-to-the-minute software tutorials, additional outside resources or a peek at how others are using our products.

Links	
	<a href="#">Facebook</a>
	<a href="#">LinkedIn</a>
	<a href="#">RSS feeds</a>
	<a href="#">Twitter</a>
	<a href="#">YouTube</a>
	<a href="#">Blog</a>
	<a href="#">Forum</a>
	<a href="#">Spiceworks</a>



	<a href="#">Reddit</a>
	<a href="#">Instagram</a>

## 12.5 Best Practices

### DESCRIPTION

The following recommendations are provided for new and experienced users alike. Remote Desktop Manager has a lot of flexibility and sometimes we are faced with so many choices that we aren't sure of the proper decision to make or its impacts. Read below to find out what our own AND the community's experience has shown is the preferred way of operating Remote Desktop Manager in various scenarios.

Most of these recommendations apply to the Enterprise Edition because the range of options is so much greater than the Free Edition.

### 12.5.1 Credential Management For Teams

### DESCRIPTION

Remote Desktop Manager allows to handle credentials in multiple ways for a team environment. This brings flexibility, but at the cost of creating difficulty when you need to choose an implementation for a particular requirement.

Below are multiple methods to handle credentials. You may choose one or many depending on your requirements. We often see scenarios where our clients manage their own infrastructure, as well as their customers. Group entries in folders depending on the kind of credential management that you must use. Each of these folders could use a different scheme.

### PREAMBLE

Here are a few notions to know prior to getting to the scenarios, as they are at the core of the usage of Remote Desktop Manager:

## INHERITED CREDENTIALS

Credentials can be set at different levels, such on the entries themselves or on their parent folders. The latter enables entries to inherit credentials from a parent folder. Whenever using inherited credentials, the credential resolver will go up a level and use the credentials set on the parent folder. If the inheritance is set on a folder, the resolver simply continues up to the next parent.

## PRIVATE VAULT

The [Private Vault](#), available for [Advanced Data Sources](#), allows to create entries available only to their owner. In the cases where a user must use a credential that is exclusive to them, using the Private Vault is the logical choice.

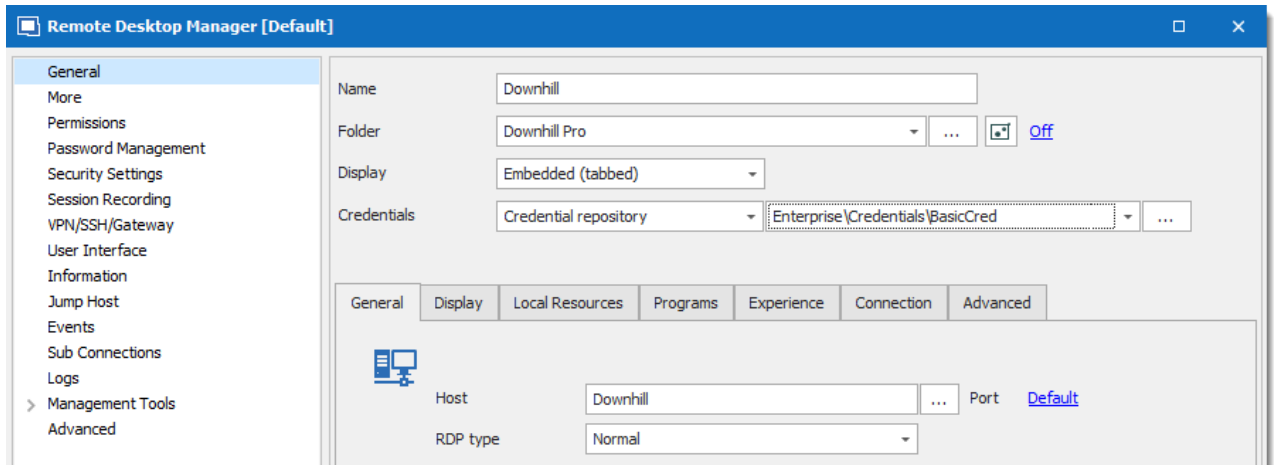
## SPECIFIC SETTINGS

[Specific Settings](#) allow you to override some settings of the entries in the data source. One of the most typical use for this is to override the credentials of the entry for a specific user. Specific settings can override credentials, session types, folders, etc.

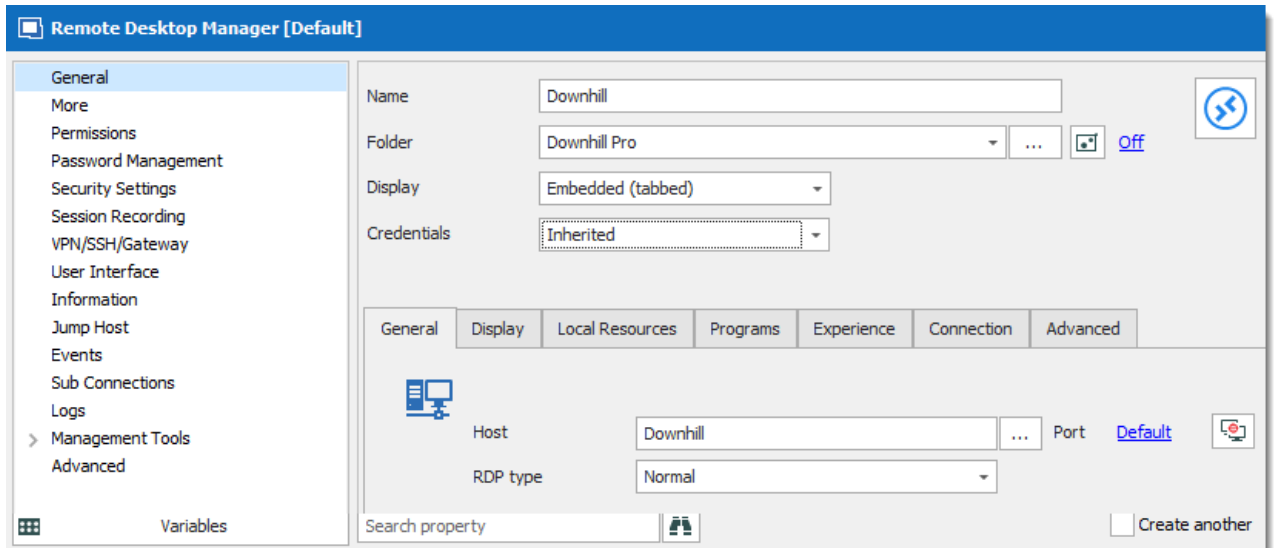
## SCENARIOS

### ALL USERS SHARE THE SAME SET OF CREDENTIALS

The credential entries are referenced directly in the properties of sessions. Select **Credential repository**, then select the existing credential entry from the data source.

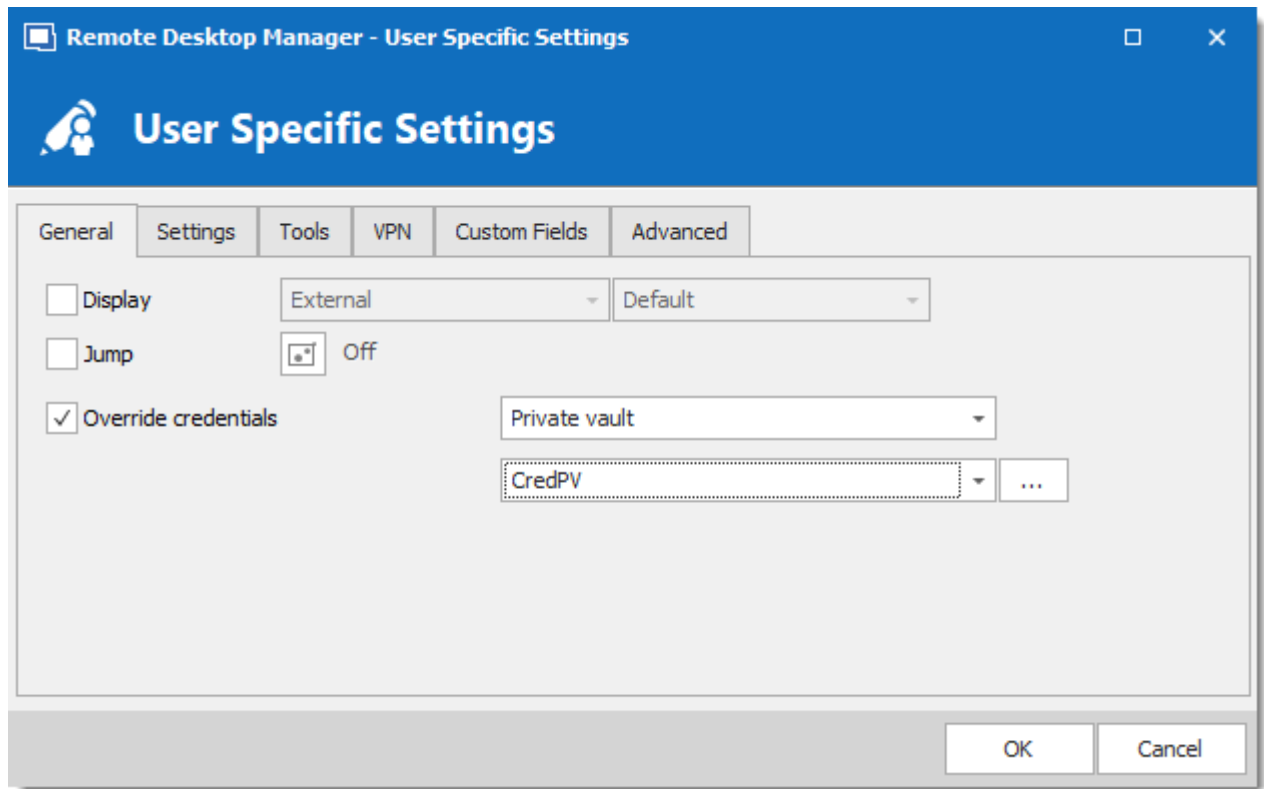


If the credentials are the same for more than one device, store the sessions in a folder which the credential entry is assigned to, and set the sessions to use the **inherited** credential mode.



## EVERY USER HAVE THEIR OWN SET OF CREDENTIALS

Use the **User Specific Settings**. Type the credentials directly or refer a credential entry in the Private Vault (recommended).



## USERS SHARE A SET OF CREDENTIALS WHILE ADMINS USE DIFFERENT CREDENTIALS

The shared credential entries are referenced directly in the properties of sessions. Admins use **User Specific Settings** to override the credentials, usually to refer a credential entry in the Private Vault.

## REFACTOR MULTIPLE ENTRIES AT ONCE

To change the credentials of multiple entries at once, the following features might help you out:

### BATCH EDIT

The [Batch Edit](#) feature allows to modify multiple entries at once. This feature can be used to apply a set of credentials on multiple entries.

### POWERSHELL

The [PowerShell CmdLet](#) of Remote Desktop Manager allows to massively update entries. The script below will set all folders to use the **inherited** credential mode.



**Always** have a backup of the data source before running a PowerShell script.

```
cls
Write-Host "Fixing Groups...\`n"
$entries = Get-RDMSession | where {$_.Kind -eq "Group"}

foreach ($entry in $entries)
{
    Write-Host ("    Processing : " + $entry.Name)
    $entry.CredentialConnectionId = "<Credential entry ID>"
    Set-RDMSession $entry
}

Write-Host "`nDONE!"
```

## 12.5.2 Use Credential Entries

### DESCRIPTION

Credentials management is one of the main strengths of Remote Desktop Manager. Although you can specify the credentials directly in the properties of entries, we recommend linking credentials to entries. This has the following advantages:

- Credential entries can be linked to multiple entries.
- The linked credential entry is the only one requiring modifications if necessary, rather than change every entry affected by it.
- When necessary, Permissions can be customized for an entry to better suit your needs (when an [Advanced Data Source](#) is used).

## 12.5.3 Use VPN Entries

### DESCRIPTION

Although you can specify VPN details directly in the entry's settings, using a VPN entry should provide better results. This has the following advantages.

- VPN entries can be used in multiple sessions.
- Only that specific VPN entry requires maintenance when modifications are necessary.
- When necessary, Permissions can be customized for an entry to better suit your needs (when an [Advanced Data Source](#) is used).

## 12.6 How-To

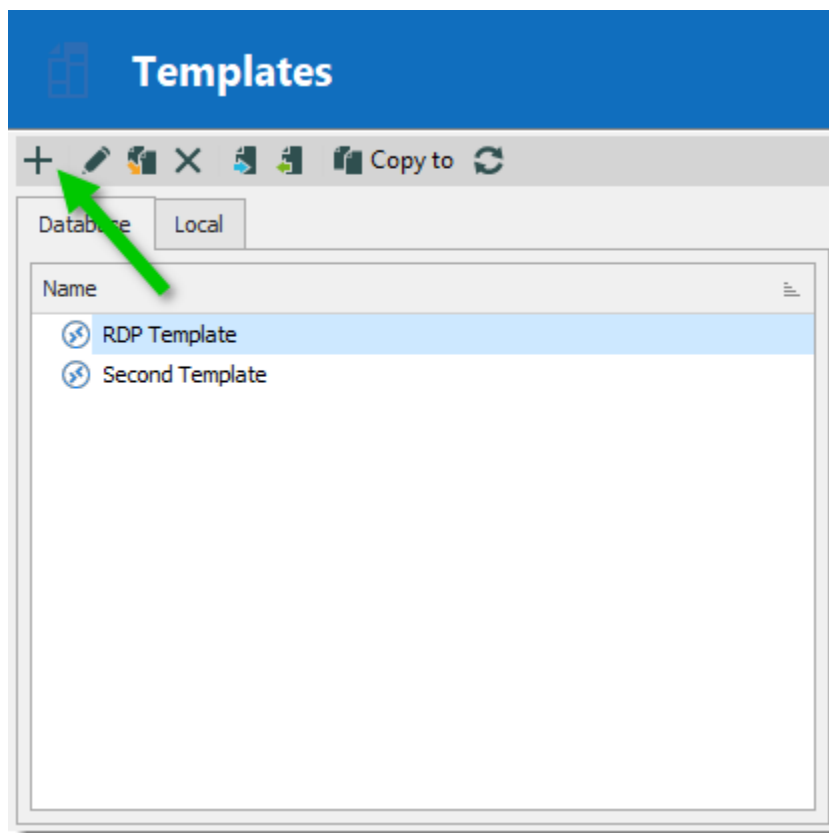
### 12.6.1 How to Add a Web Link in Macros/Scripts/Tools Session

#### DESCRIPTION

It's possible to create a **Macros/Scripts/Tools** session that contain a web link. This **Macros/Scripts/Tools** can be launched from the dashboard.

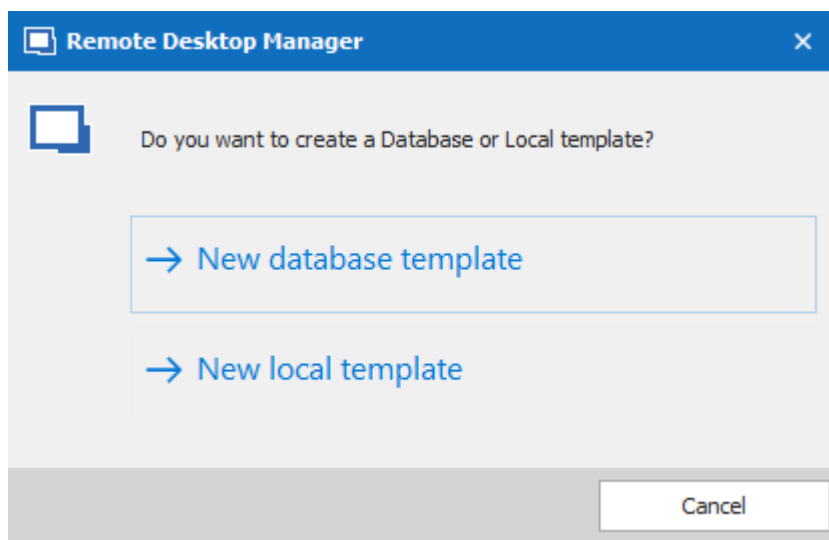
#### SETTINGS

1. Create a database [Template](#) by clicking on **File – Templates – Templates – Add template**.



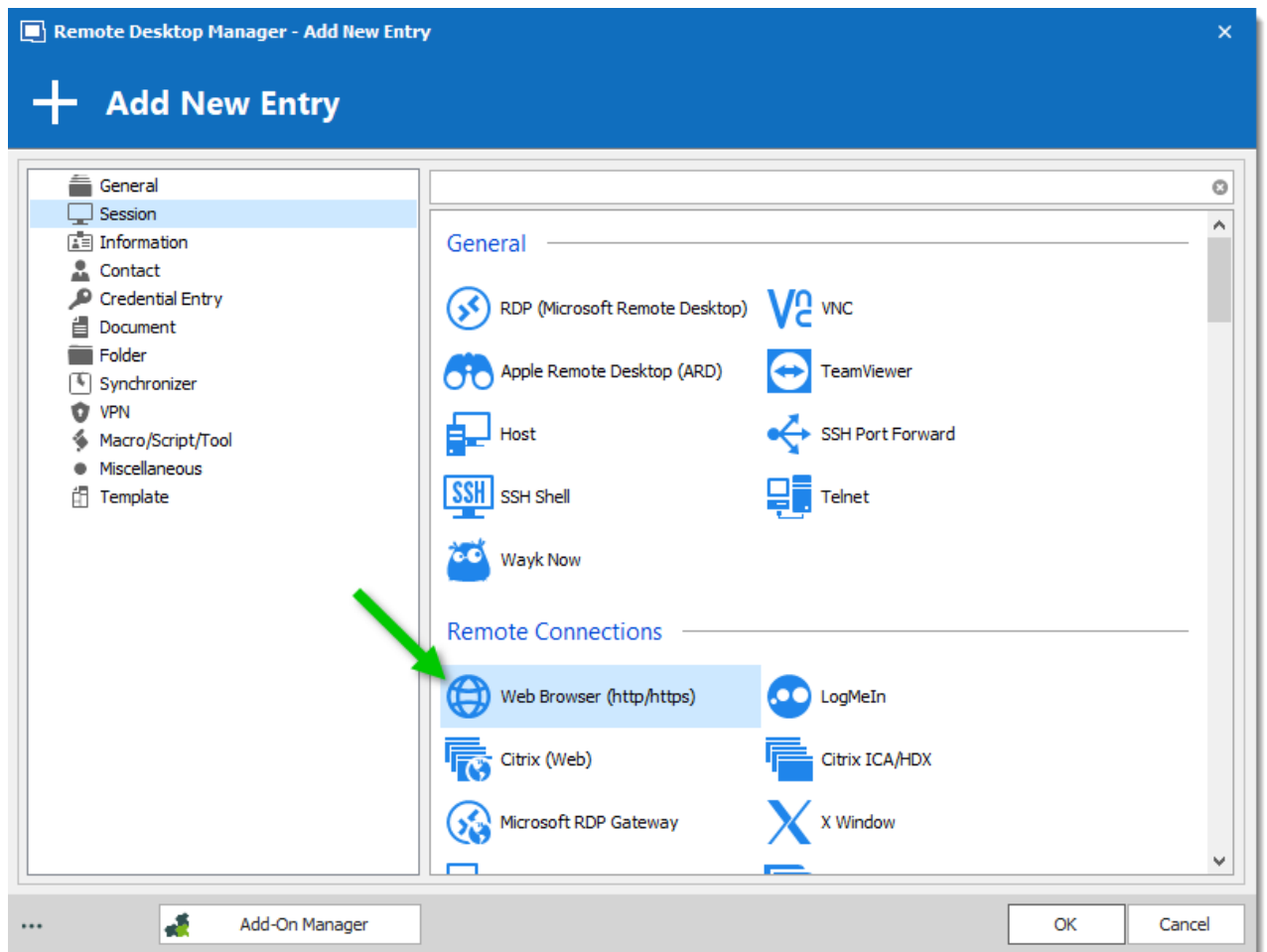
Add a Template

2. Select **Create a database template**



Create a shared template

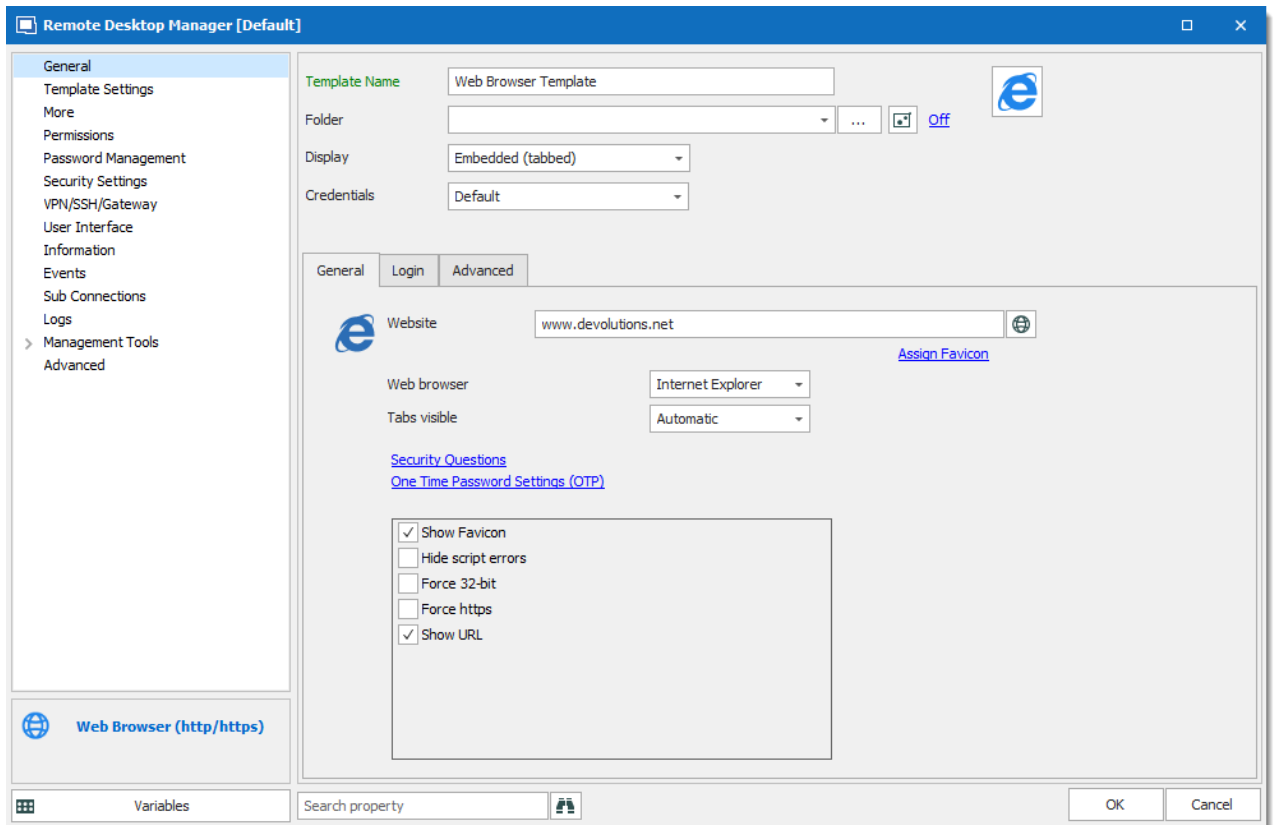
3. Select the **Web Browser (http/https)** session type.



*Web Browser session*

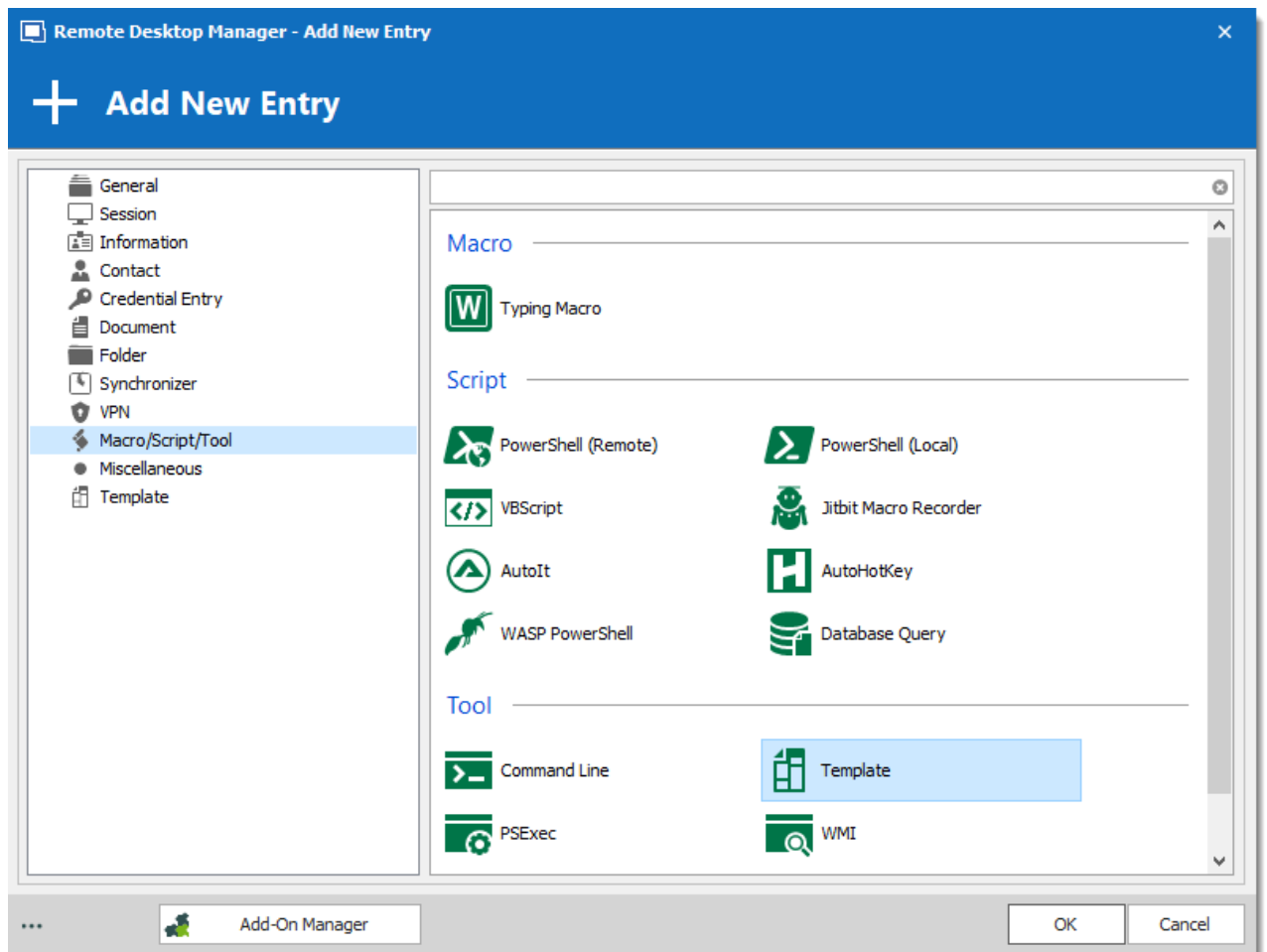
4. Indicate the proper information in the template and click on **OK**.





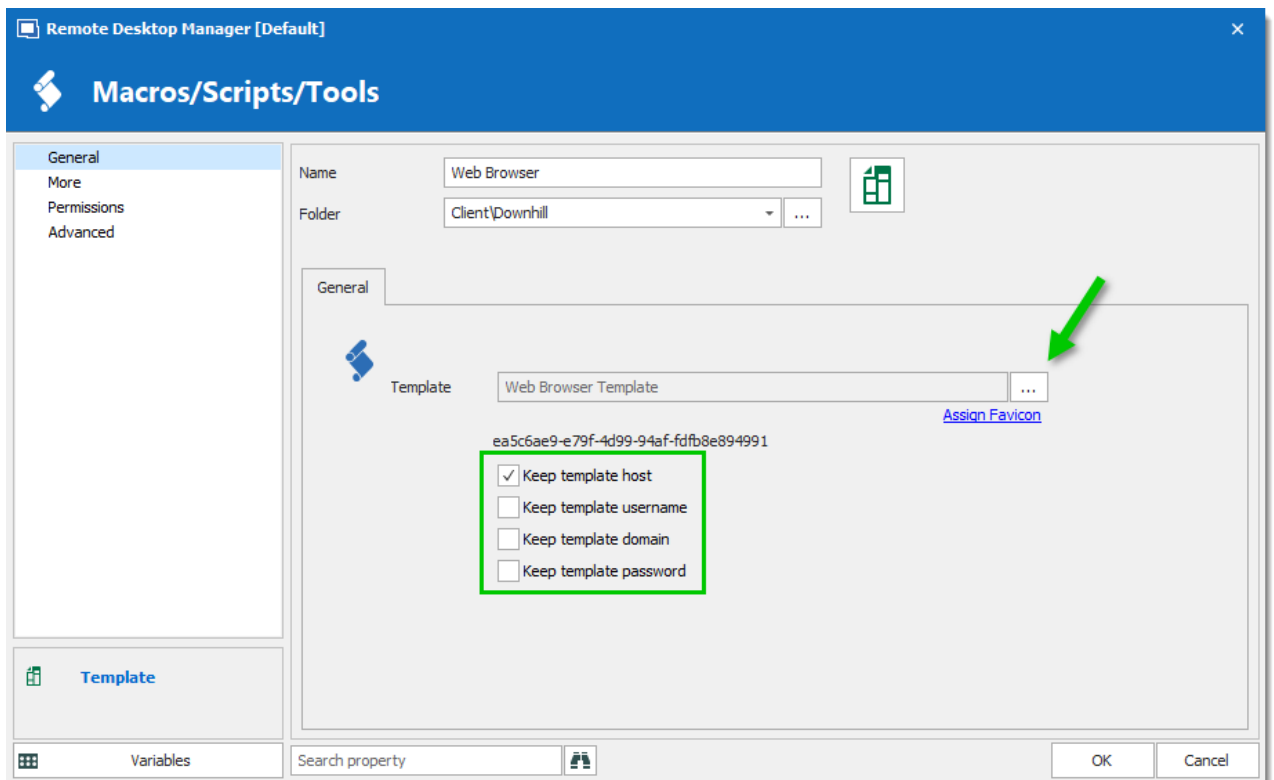
*Template Creation*

5. After the creation of the template, create a new entry **Macros/Scripts/Tools - Template**. This isn't done through the Template menu from step 1 - 4, use the **Add Entry** feature to locate a **Template** in the **Macros/Scripts/Tools**.



*Macro/Script Tool - Template*

6. Click on the ellipsis to select your newly created template and check the box **Keep template host**. You can also opt to keep whichever part of the credentials you would want.



*Macros/Scripts/Tools template creation*

7. You can now launch the web link (website) from the Tree View.

## 12.6.2 How to apply policies

### DESCRIPTION

Administrative Templates facilitates the management of registry-based policy settings that can be applied on the computer and/or the user configuration. Group policy (GPO) is a tool for organizations to enforce settings on their computers and allows to harden Remote Desktop Manager security.



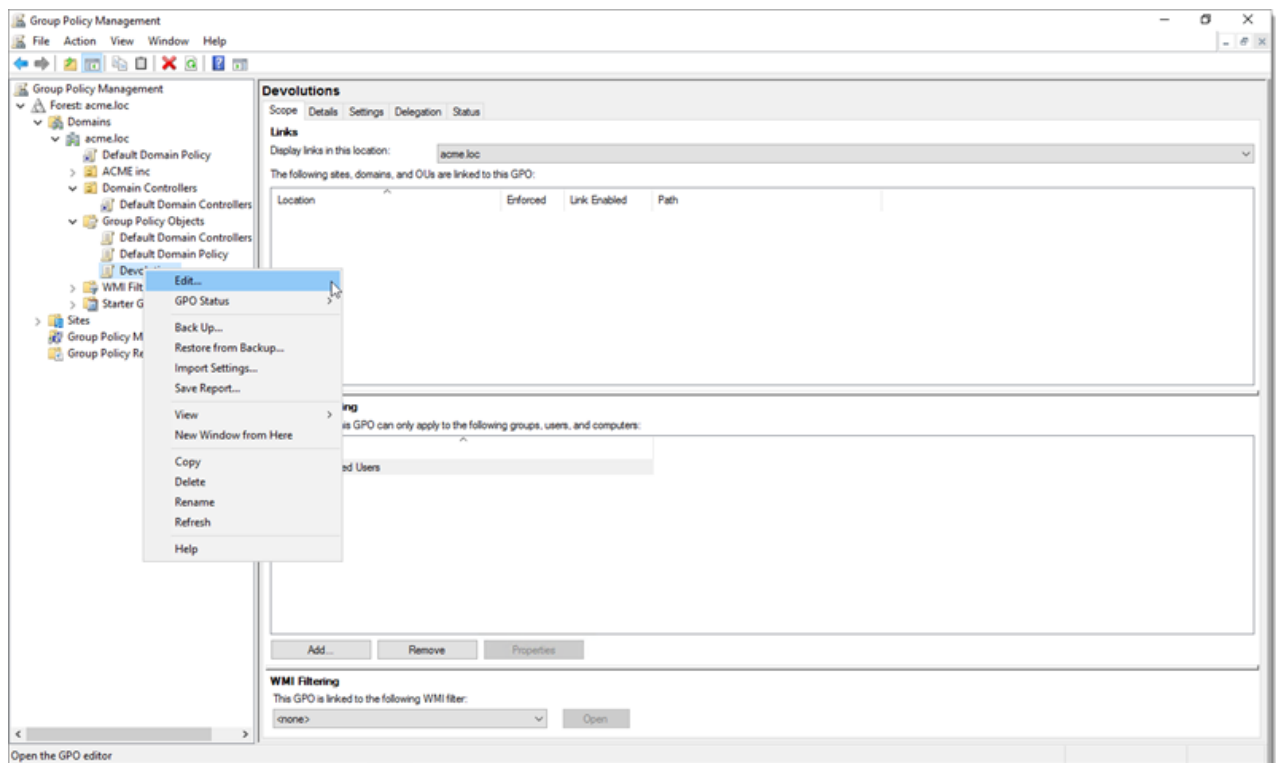
The Administrative Templates are simply registry settings that are enforced by domains. They contain registry keys that can also be set on computers that are not joined to domains. Proper Access Control Lists (ACL) must be put in place to prevent users from modifying registry settings in this case. Refer to the tables below to find the registry key for each policy setting.

To learn more on how to deploy the Remote Desktop Manager Administrative Templates on your domain please refer to the Microsoft Online Help.

The admx file is distributed with Remote Desktop Manager, you will find it in a **Policies** sub-folder. By default the path is **C:\Program Files (x86)\Devolutions\Remote Desktop Manager\Policies**.

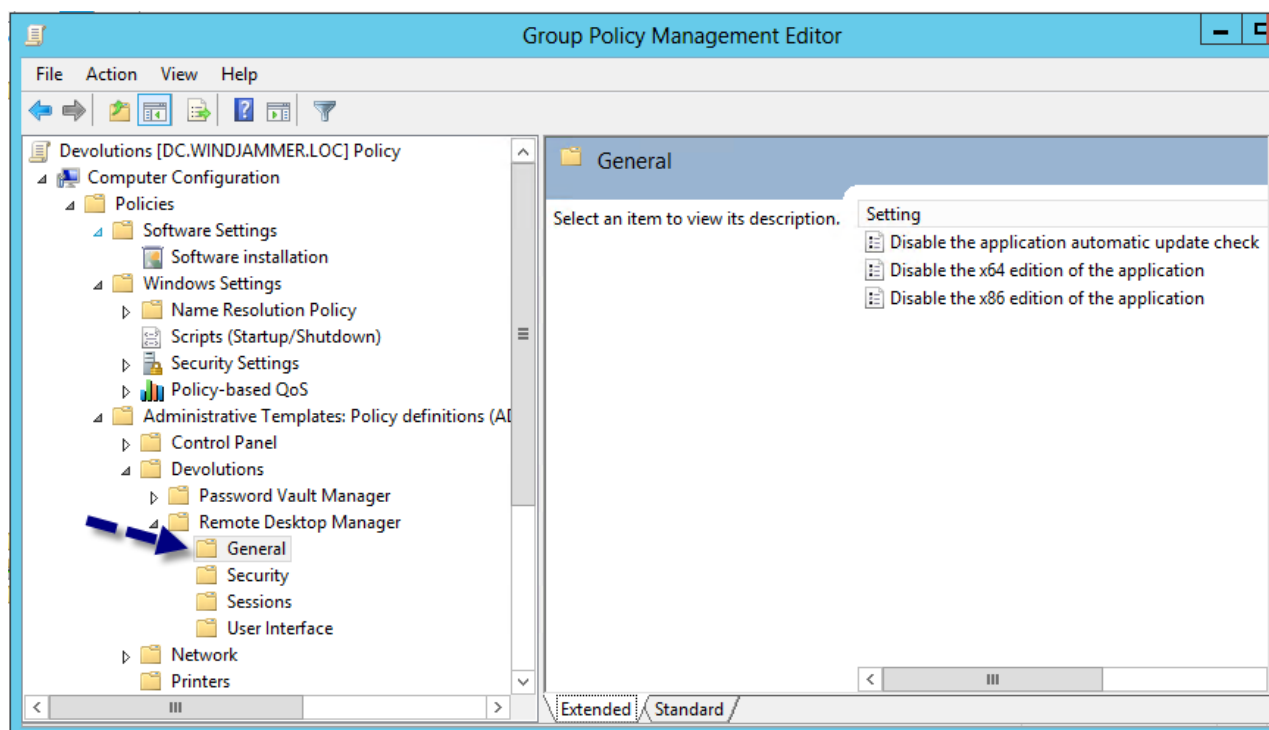
## SETTINGS

RemoteDesktopManager includes an Administrative templates file (.admx), which describes the policies that are offered.



Group Policy Management Folder

In the console tree, click the folder under Administrative Templates that contains the policy settings you want to configure.



## GENERAL

POLICY NAME	REGISTRY KEY (PLEASE SEE <a href="#">NOTE 1</a> )
<b>Disable the telemetry data collection</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableAnalytics
<b>Disable the application automatic update check</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableAutoUpdate
<b>Disable the Help - Check Version button</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableUpdate
<b>Disable the Register Product in the Help menu</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableRegisterProduct

POLICY NAME	REGISTRY KEY (PLEASE SEE <a href="#">NOTE 1</a> )
<b>Disable the x64 edition of the application</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableX64
<b>Disable the x86 of the application</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableX86
<b>Force refresh before edit entry</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\ForceRefreshBeforeEditEntry
<b>Force the loading of the default.cfg file</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\ForceDefaultConfigurationLoading
<b>Force updating all major update</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\ForceUpdatingMajorUpdate
<b>Force updating all update</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\ForceUpdatingAllUpdate
<b>Force updating all update and beta</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\ForceUpdatingAllUpdateAndBeta
<b>Force updating once a month</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\ForceUpdatingOnceAMonth

## SECURITY

POLICY NAME	REGISTRY KEY (PLEASE SEE <a href="#">NOTE 1</a> )
<b>Force the user to always be prompted for the passphrase while connecting to a data source that is protected by a Passphrase Security Provider</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\AlwaysPromptForPassphrase
<b>Apply forced password template in Password Generator tool</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\ApplyForcedPasswordTemplateInPasswordGeneratorTool
<b>Check for server certificate revocation</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\CheckForServerCertificateRevocation
<b>Disable execute scripts via terminal</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableExecuteScriptsViaTerminal
<b>Disable local drive sharing of RDP entries</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableLocalDriveSharing
<b>Disable My Account Settings</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableMyAccountSettings
<b>Disable my personal private key</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableMyPersonalPrivatekey
<b>Disable the caching mode</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableCaching

POLICY NAME	REGISTRY KEY (PLEASE SEE <a href="#">NOTE 1</a> )
<b>Disable the offline mode</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableOffline
<b>Disable the tools of the password generator</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisablePasswordGenerator
<b>Disable the override hard drive specific settings for the RDP entries</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableRDPHardDrivesSpecificSettings
<b>Disable the read/write in offline mode</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableReadWriteOffline
<b>Force the user to always be prompted for his credentials when opening the application</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\ForceLogin
<b>Force multiple factor authentication on the application login</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\ForceApplicationMFA
<b>Use Windows credentials as application password and force the currently logged on username and domain</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\ForceWindowsCredentialsAndCurrentlyLoggedInUsernameAndDomain
<b>Ignore application certification errors</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\IgnoreApplicationCertificateErrors

## SESSIONS



POLICY NAME	REGISTRY KEY (PLEASE SEE <a href="#">NOTE 1</a> )
<b>Disable the add-on creation and the Add-on Manager</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableAddOn
<b>Disable all session events</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\ForceDisableAllSessionEvents
<b>Disable the Add-on creation of entries</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableAddOnEntries
<b>Disable the Add-on Manager</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableAddOnManager
<b>Disable the custom image edition in the session configuration</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableCustomImage
<b>Disable import in private vault</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableImportInPrivateVault
<b>Disable the reveal password command</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableRevealPassword
<b>Allow the user to connect even after the entry has expired</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\EnableConnectionAfterExpiration
<b>Inside the private vault, allows only credentials entries</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\OnlyAllowCredentialsInPrivateVault

## USER INTERFACE

POLICY NAME	REGISTRY KEY (PLEASE SEE <a href="#">NOTE 1</a> )
<b>Disable the menu Help - About</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableAbout
<b>Disable the Help menu</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableHelp
<b>Disable quick connect</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableQuickConnect
<b>Disable all the local application tools like the Event Viewer or IIS</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableApplicationTools
<b>Disable the possibility to drag and drop sessions</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableDragAndDrop
<b>Disable the menu File - Data Sources</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableFileDataSources
<b>Disable the menu File - Options</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableFileOptions
<b>Disable the import and the export of the <a href="#">Configuration File</a> in File - Options</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableImportExportOptions
<b>Disable the My Personal Credential feature</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableMyPersonalCredential

POLICY NAME	REGISTRY KEY (PLEASE SEE <a href="#">NOTE 1</a> )
	ktopManager\DisableMyPersonalCredentials
<b>Disable the Devolutions Account usage</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableOnlineAccount
<b>Disable the option to open with parameter</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableOpenWithParameters
<b>Disable the error report prompt</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableSendErrorReportDialog
<b>Disable the Add-On Manager in the Tools menu</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableToolsAddOnManager
<b>Disable the Chocolatey Console in the Tools menu</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableToolsChocolateyConsole
<b>Disable the Devolutions Password Server Console in the Tools menu (Deprecated 12.6.8)</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableToolsDevolutionsServerConsole
<b>Disable the Extension Manager in the Tools menu</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableToolsExtensionManager
<b>Disable the Local RDP/RemoteApp Manager in the Tools menu</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableToolsLocalRDPRemoteAppManager

POLICY NAME	REGISTRY KEY (PLEASE SEE <a href="#">NOTE 1</a> )
<b>Disable the Macro/Script/Tool Manager in the Tools menu</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableToolsMacroScriptToolManager
<b>Disable the Tools ribbon tab and menu</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableToolsMenu
<b>Disable the Open New Remote Desktop option in the Tools menu</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableToolsOpenNewRemoteDesktop
<b>Disable the Powershell RDM Cmdlet in the Tools menu</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableToolsPowershellRDMCmdlet
<b>Disable the RDM Agent in the Tools menu</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableToolsRDMAgent
<b>Disable the Translation Manager in the Tools menu</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableToolsTranslationManager
<b>Disable the Top Pane (Ribbon/Menubar)</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableTopPane
<b>Force the Merge credential list with sessions option</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\EnableMergeCredentialListWithSessions
<b>Force the merging of the session toll list with sessions</b>	%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\EnableMergeSessionListWithSessions

POLICY NAME	REGISTRY KEY (PLEASE SEE <a href="#">NOTE 1</a> )
	ktopManager\EnableMergeSessionToolListWithSessions

## NOTES

%Root% can either be HKEY\_LOCAL\_MACHINE or HKEY\_CURRENT\_USER depending on how you want to enforce the policy. Please refer to Microsoft's documentation to make the best choice for your situation.

### 12.6.3 How to Backup Remote Desktop Manager

#### DESCRIPTION

Backups are important in case of hardware failure.

A proper backup will cover both your **data** and your **settings**.

#### BACKUP

#### DATA

Your data is stored in your data source. Please consult Data Source Backups for more details.

#### SETTINGS

You can export your settings via the [Export Options](#) wizard of Remote Desktop Manager.

### 12.6.4 How to Configure Password Manager Pro in Remote Desktop Manager

#### DESCRIPTION

You can create Password Manager Pro credential entries in Remote Desktop Manager, however a Password Manager Pro account needs to be created and configured in the application prior to the utilization.

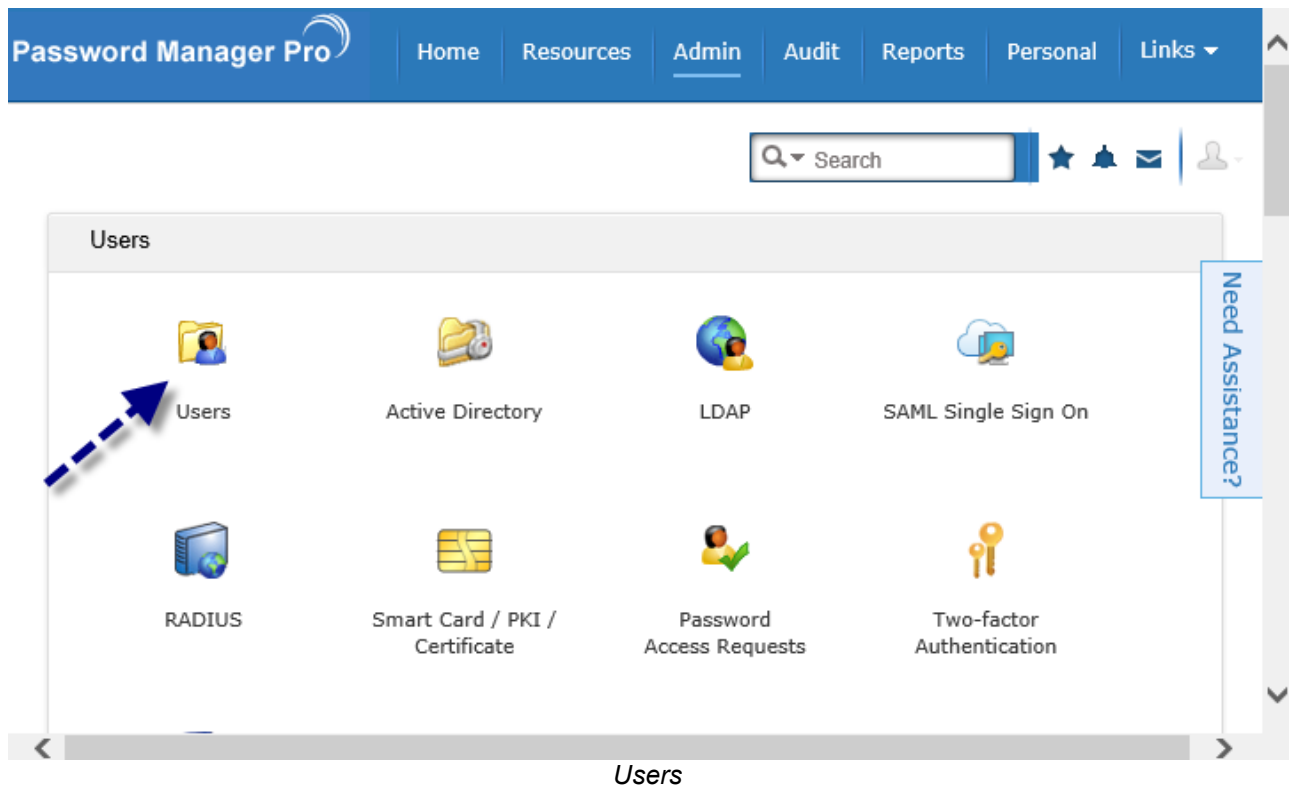
## SETTINGS

1. Connect to your Password Manager Pro server (<https://localhost:7272>) using your admin account.

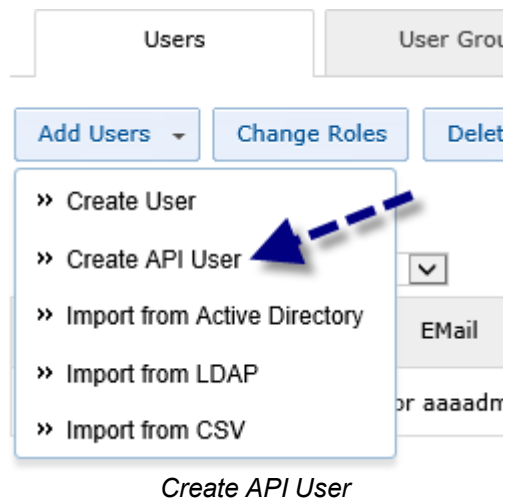


*Password Manager Pro*

2. Inside Password Manager Pro, click on Admin and select Users.



3. Create a new API user.



4. In the Host Name field, enter the name of the computer where the API user will be use.

Add API User ?

User Name : jeff ?

Host Name : devolutions1 ?

Full Name : ?

Email :

Access Level : Password User v

Access Scope : ☒ Passwords owned and shared  
☐ All passwords in the system (this will make this user the super administrator)

Add API User

5. Enable the REST API to have a API Auth Token key generated

XML-RPC API : Browse...

access :

REST API : ☒ Enable ☐ Disable

AUTH Token : [Reg]

(Copy the generated API Auth Token)

AUTH Token validity : ☒ Never Expires ☐ Expires On 1

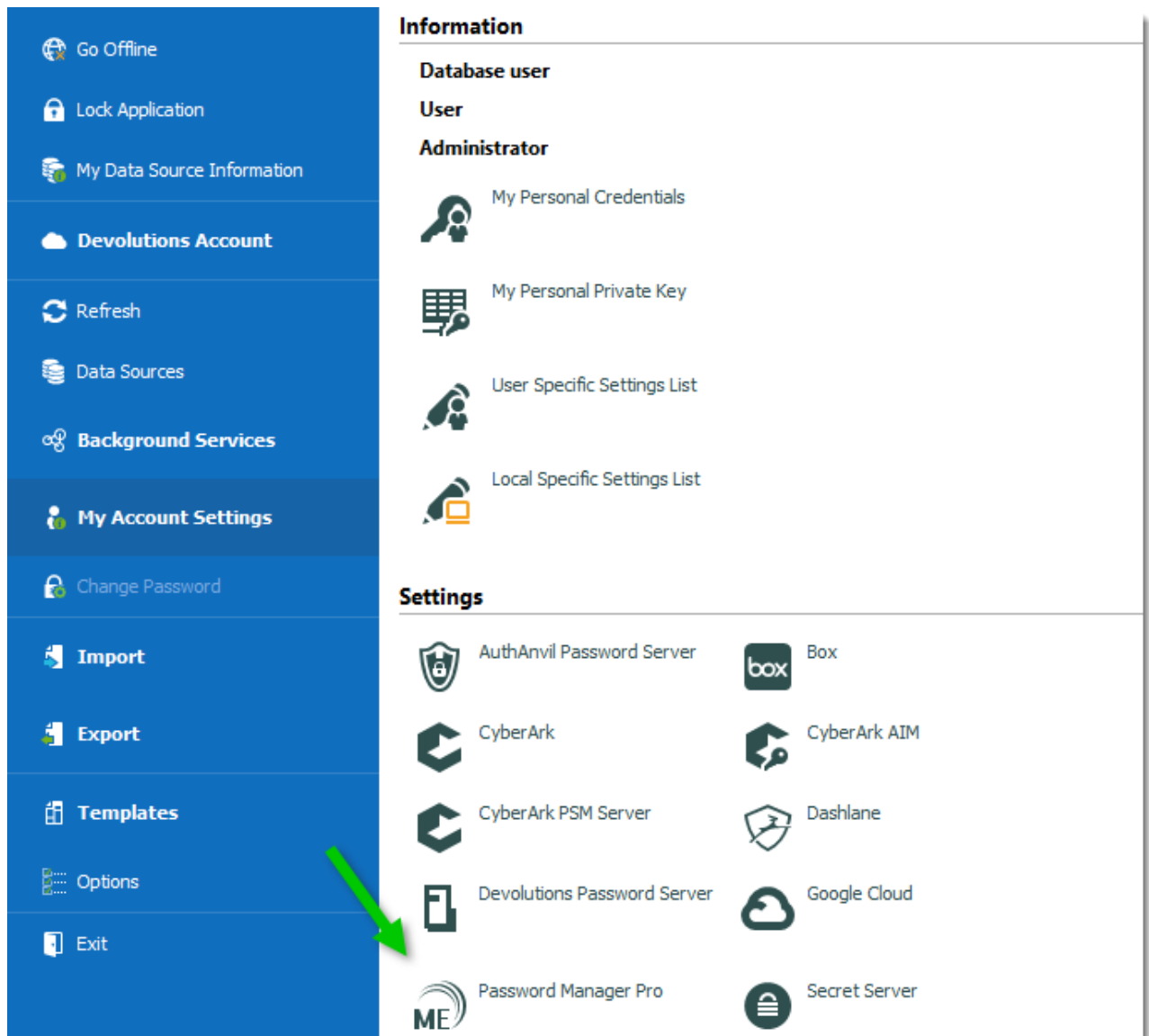
Auth Token



Copy the Auth token key in your clipboard. You will need it to configure Password Manager Pro in Remote Desktop Manager.

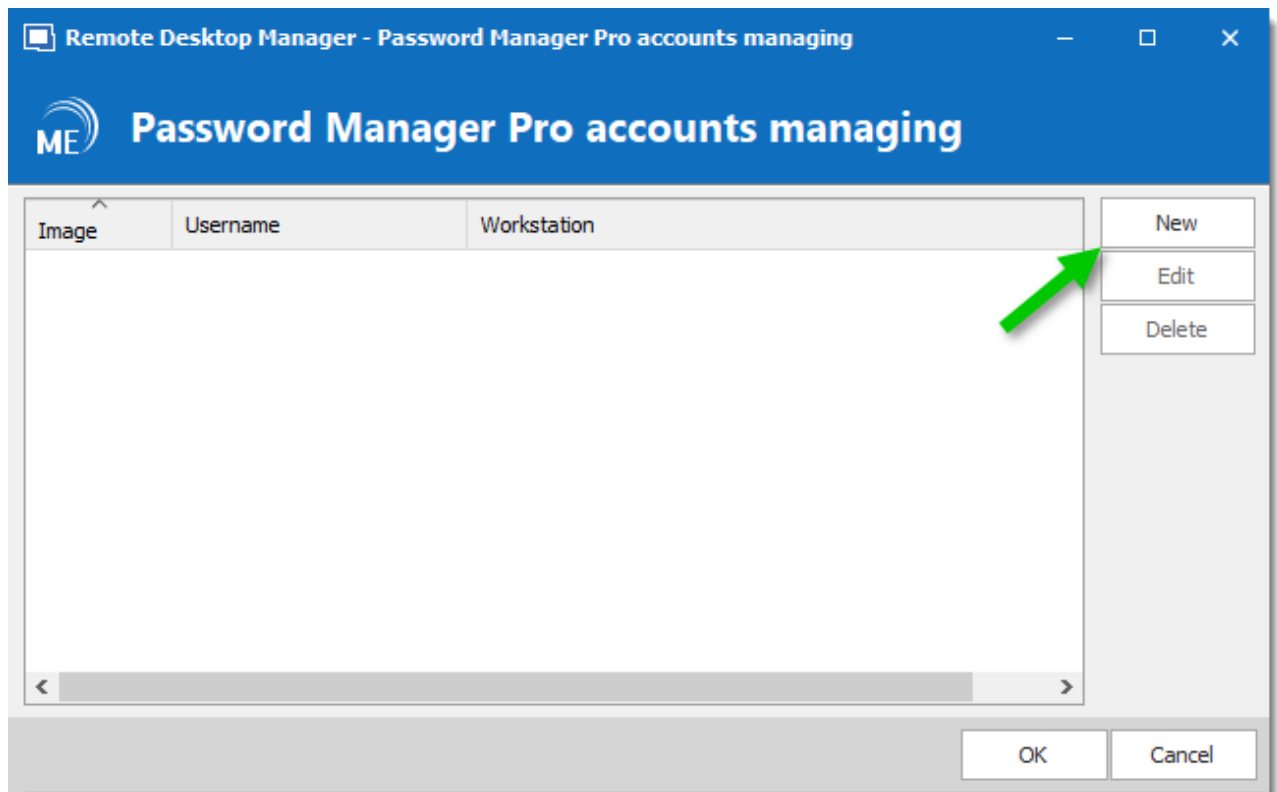
6. Now, go inside Remote Desktop Manager and click on **File – My Account Settings – Password Manager Pro.**



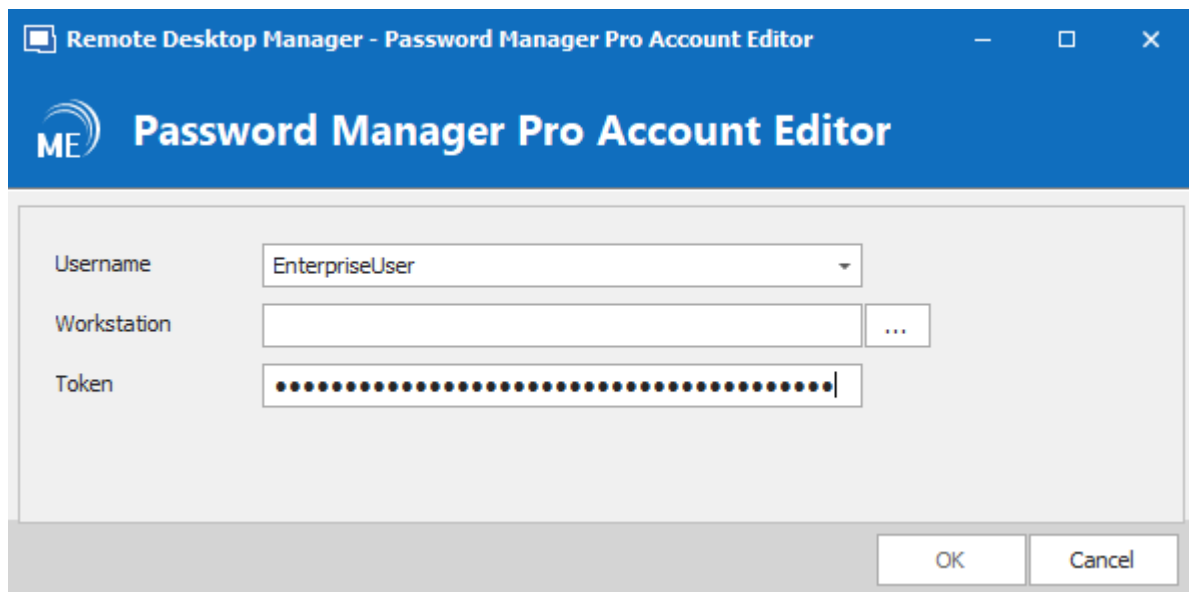


*Password Manager Pro Account Settings*

7. Click on **New** to create a Password Manager Pro account

*New User*

8. Enter the username of the API User that you have created in Password Manager Pro in the **Username** field, enter the appropriate computer name in the **Workstation** field and paste the Auth Token key that you have copied on step 5 in the **Token** field and click on **OK**.

*New User*

9. You can now create a Password Manager Pro credential entry in Remote Desktop Manager

The screenshot shows the 'General' tab of a credential entry configuration window. On the left is the 'ME' logo. The configuration fields are as follows:

- Service URL:** A text box containing 'https://vdownsrv-pmp' with a globe icon to its right.
- Port:** A spinner box set to '7272'.
- Use My Account Settings:** A checked checkbox.
- Username:** A text box with a dropdown arrow.
- Resource:** A text box with an ellipsis button and a refresh icon.
- Account:** A text box.
- Always prompt with list:** A checked checkbox.
- Domain override:** A text box.

*Credential Entry*

## 12.6.5 How to Configure ConnectWise (ScreenConnect) 5 in Remote Desktop Manager

### DESCRIPTION

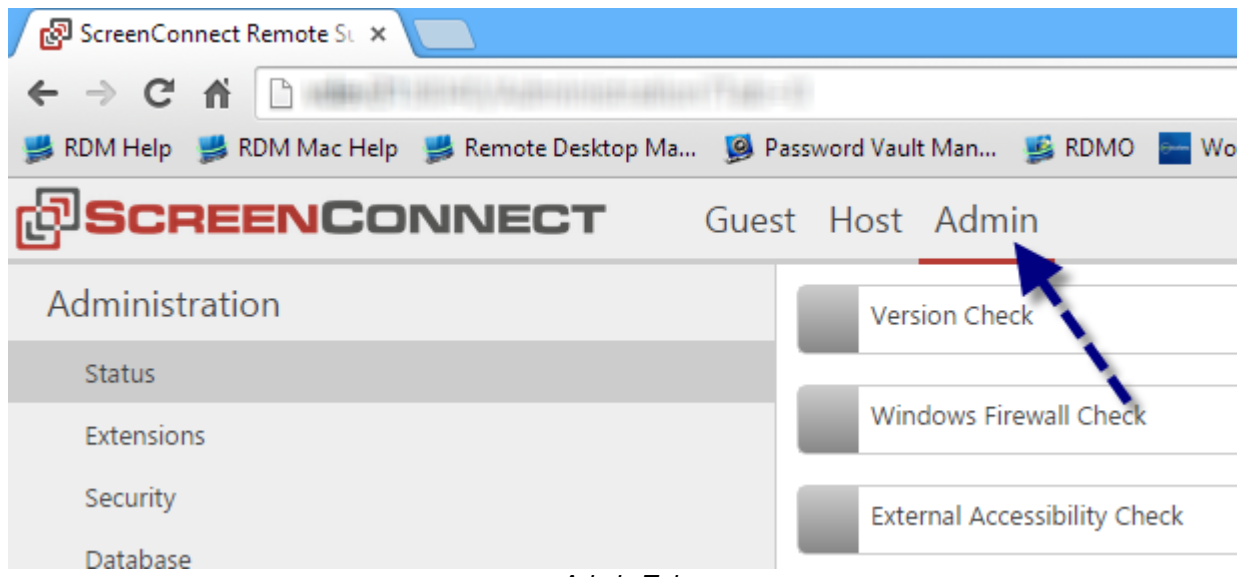
It's possible to use ConnectWise (ScreenConnect) in Remote Desktop Manager, however a ConnectWise (ScreenConnect) extension needs to be installed prior to the utilization. After the extension installation, you can configure ConnectWise (ScreenConnect) 5 in Remote Desktop Manager.



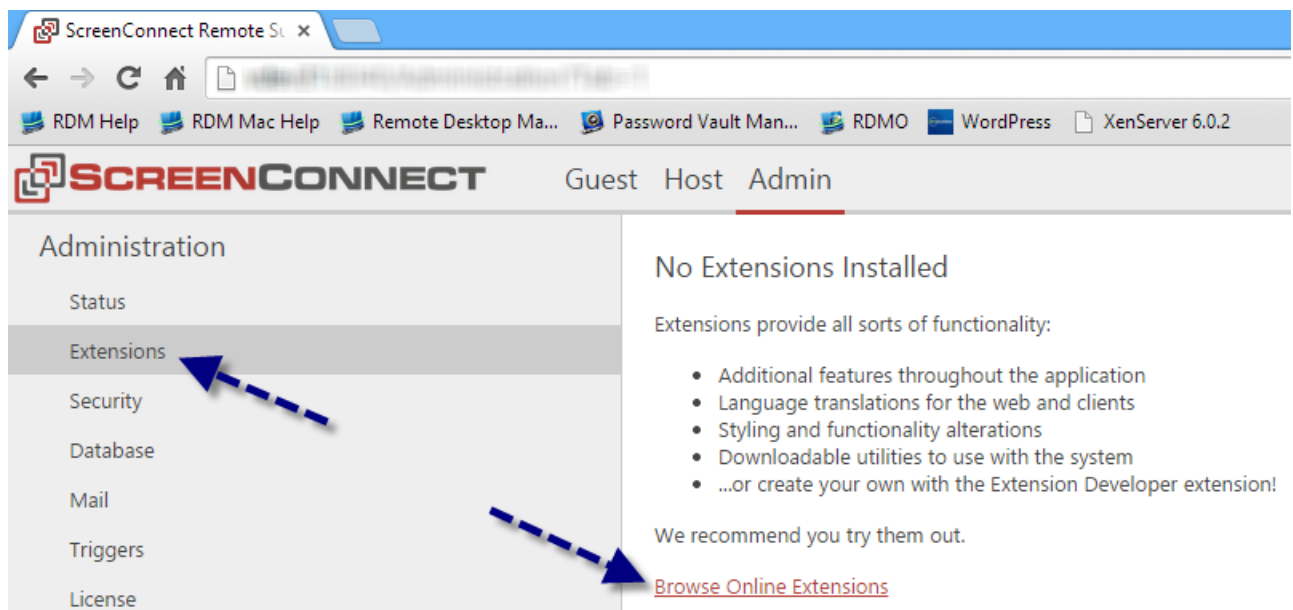
The Remote Desktop Manager extension needs to be installed on your ConnectWise (ScreenConnect) server.

### SETTINGS

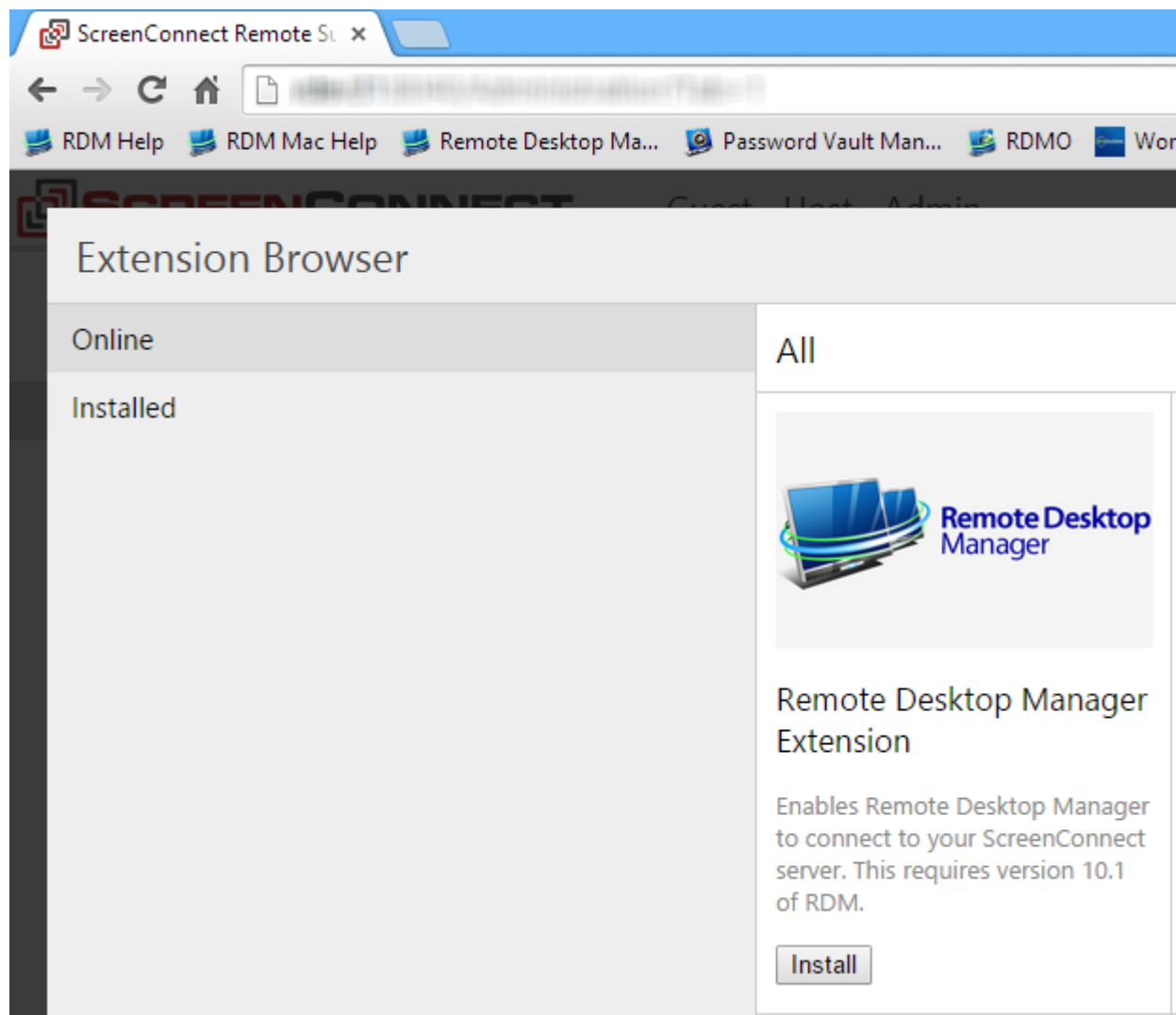
1. Connect on ConnectWise (ScreenConnect) server and click on **Admin**.

*Admin Tab*

2. Click on **Extensions** in the Administration section and select **Browse Online Extensions**.

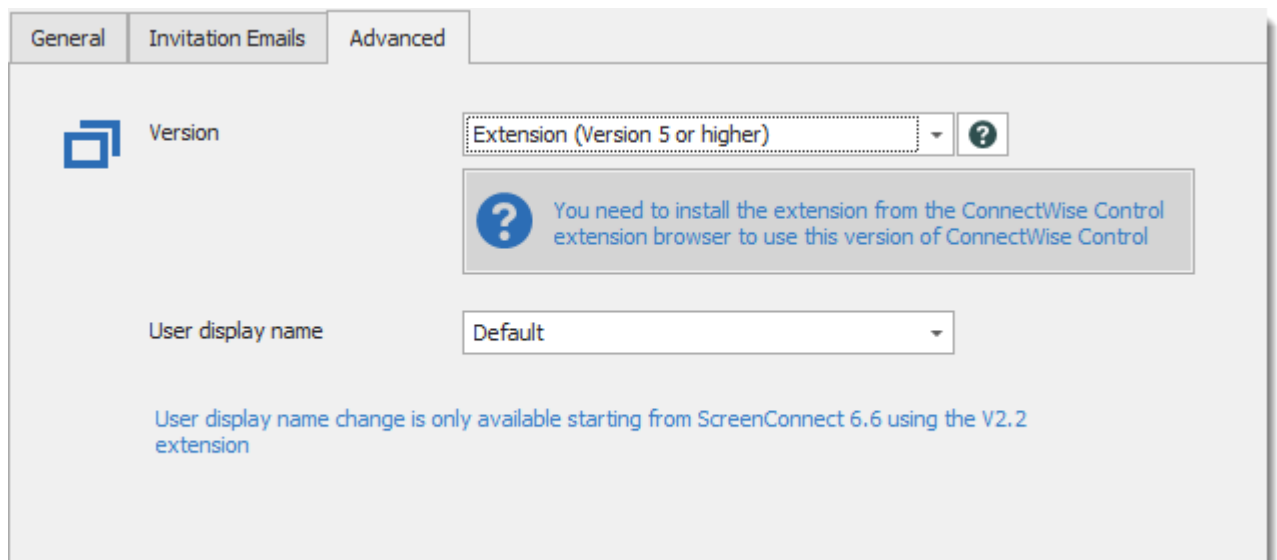
*Extensions*

3. Install Remote Desktop Manager Extension.



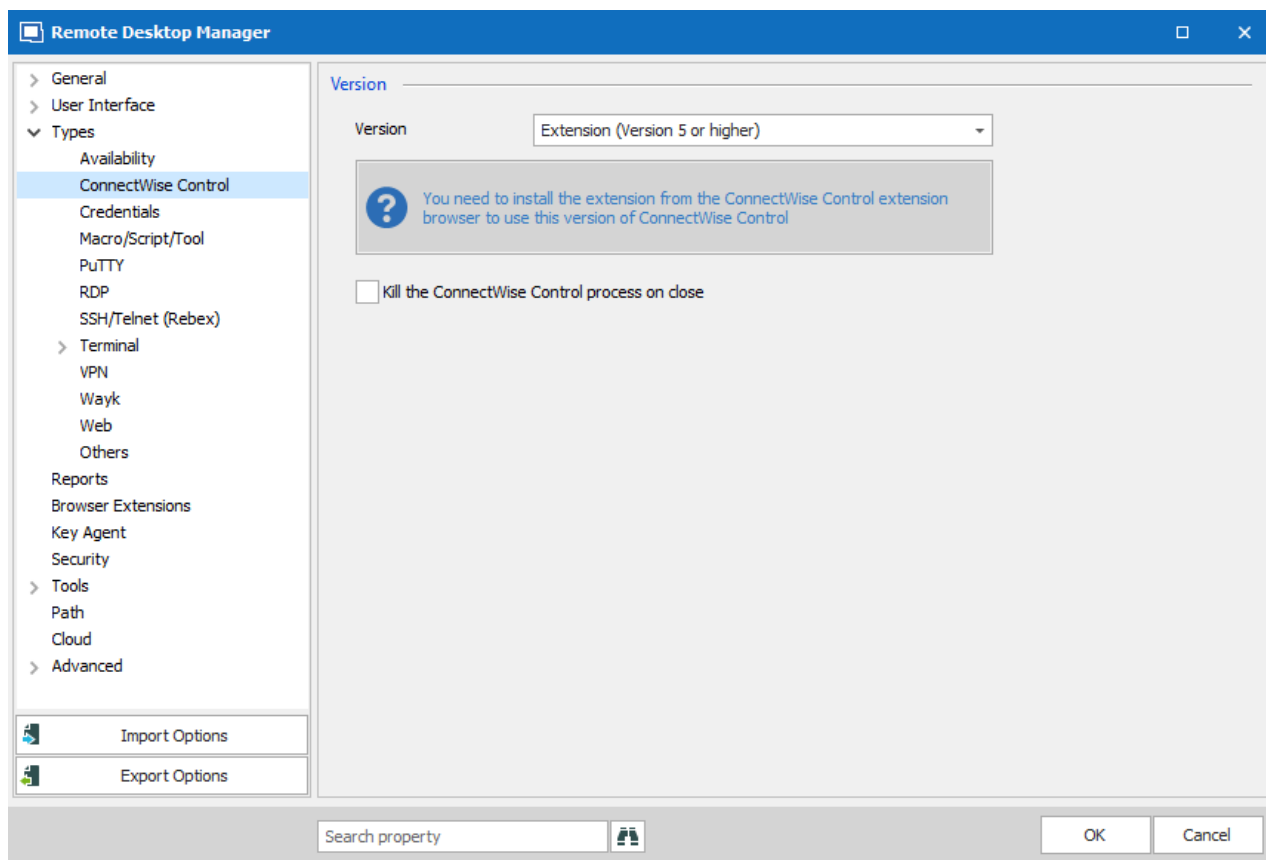
*Remote Desktop Manager Extension*

4. Now that the extension is installed, you can create your ScreenConnect session. In the **Advanced** tab, change the version for **Extension (Version 5 or higher)**.



*ConnectWise Control (ScreenConnect) - Advanced*

5. You can also select **Default** in the drop down list instead of **Extension (Version 5 or higher)**. If you select **Default**, you'll need to configure the ScreenConnect version that you wish to use in **File – Options – Types – ConnectWise Control**.



*File - Options - Types - ConnectWise (ScreenConnect)*

## 12.6.6 How to Configure the Google Authenticator 2-Factor Authentication

### DESCRIPTION

Remote Desktop Manager has the option to use Google Authenticator to provide an additional security layer when the application starts.

### 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.

1. Click on **File – Options – Security** and select **Require Google Authenticator** in the 2-Factor Authentication section. Then click on **Configure** to set up your Google Authentication.

Remote Desktop Manager

- > General
- > User Interface
- > Types
- Reports
- Browser Extensions
- Key Agent
- Security**
- > Tools
- Path
- Cloud
- > Advanced

**Application Security (Local)**

☒ No application password

☐ Use application password

New password

Confirm Password

☒ Encrypt local files using the application password

☐ Use this computer's credentials as application password

☐ Force currently logged on username and domain

**2-Factor Authentication**

☐ Require Yubikey authentication

YubiKey

☒ **Require Google Authenticator**

[Configure](#)

Override account name  The space character is not supported

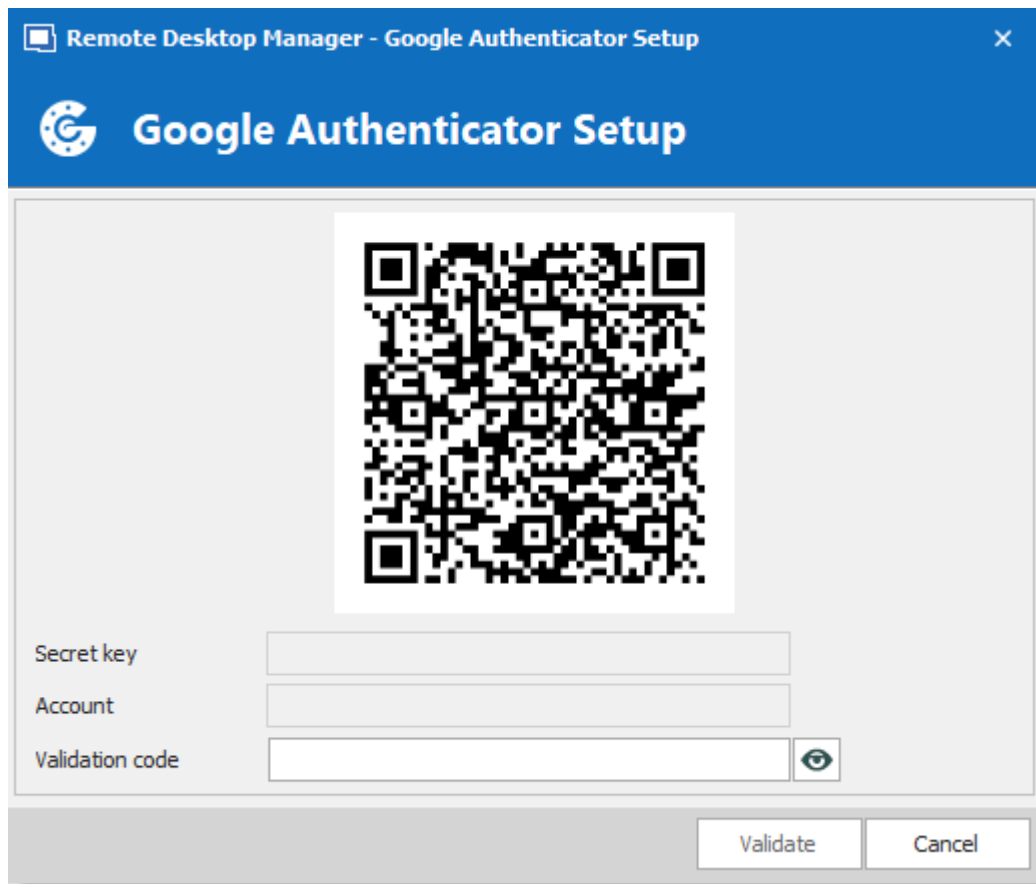
If you change the account name, you will have to reconfigure Google Authenticator

Duo automatic 2-factor

*Google Authenticator*

2. Scan the QR code on your screen with the Google Authenticator application to setup Remote Desktop Manager in Google Authenticator.  
When Remote Desktop Manager is configured in Google Authenticator, enter the Validation code provided by Google Authenticator in Remote Desktop Manager.





*Google Authenticator Setup*

3. When the Validation code is entered, click on **Validate**, then **OK**.
4. Relaunch Remote Desktop Manager to be prompted for the Google Authenticator code.



Google Authenticator generates a new validation code every 30 seconds. There will be a color indicating the end of the time window is approaching, please consult the application documentation of your device for complete information.

## 12.6.7 How to Configure the Yubikey 2-Factor Authentication

### DESCRIPTION

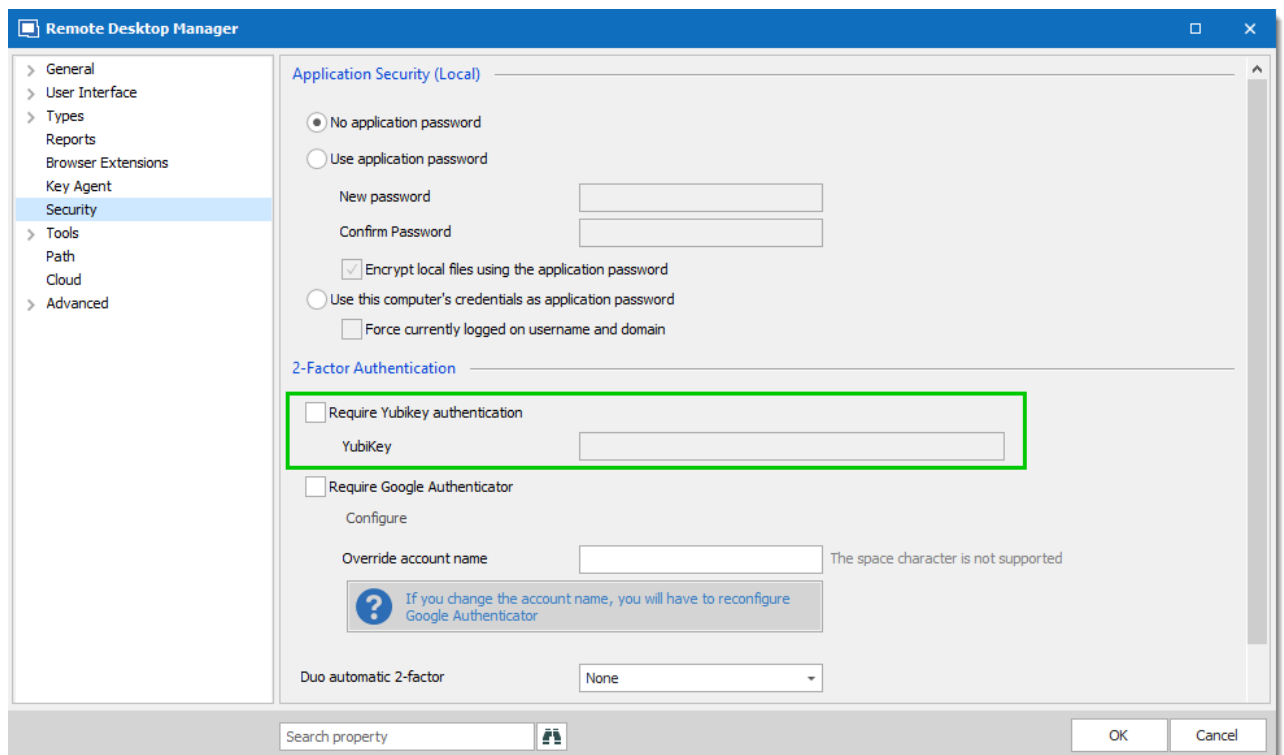
Remote Desktop Manager allows you to configure a Yubikey to provide an additional security layer when the application starts.

## SETTINGS



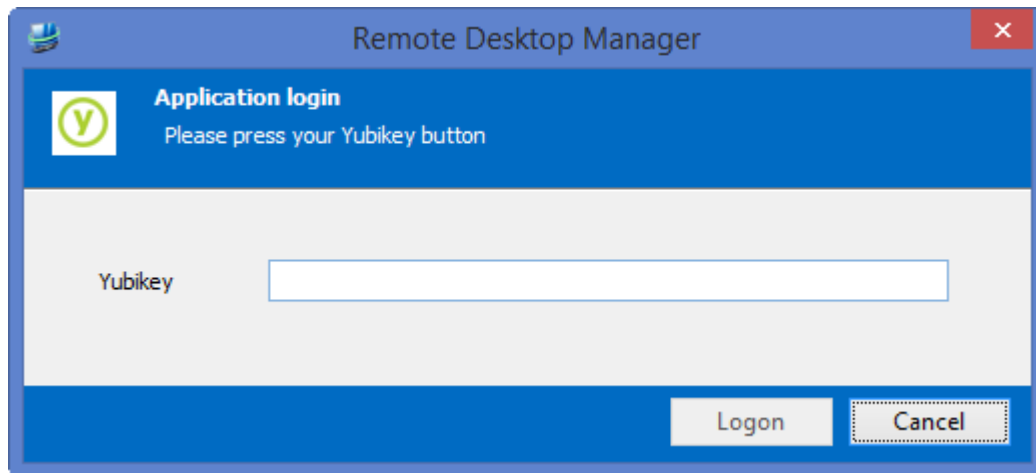
Before starting the configuration, make sure you have a [Yubikey](#) in your possession.

1. Insert the Yubikey into a USB port of your computer.
2. Click on **File – Options – Security** and select **Require Yubikey authentication** in the 2-Factor authentication section. Press and hold the gold button on the Yubikey to have the code in Remote Desktop Manager and click **OK**.



*Yubikey Authentication*

3. Relaunch Remote Desktop Manager to be prompted for a Yubikey code.



*Yubikey Authentication request*

4. Press and hold the gold button on the Yubikey and access will be granted.

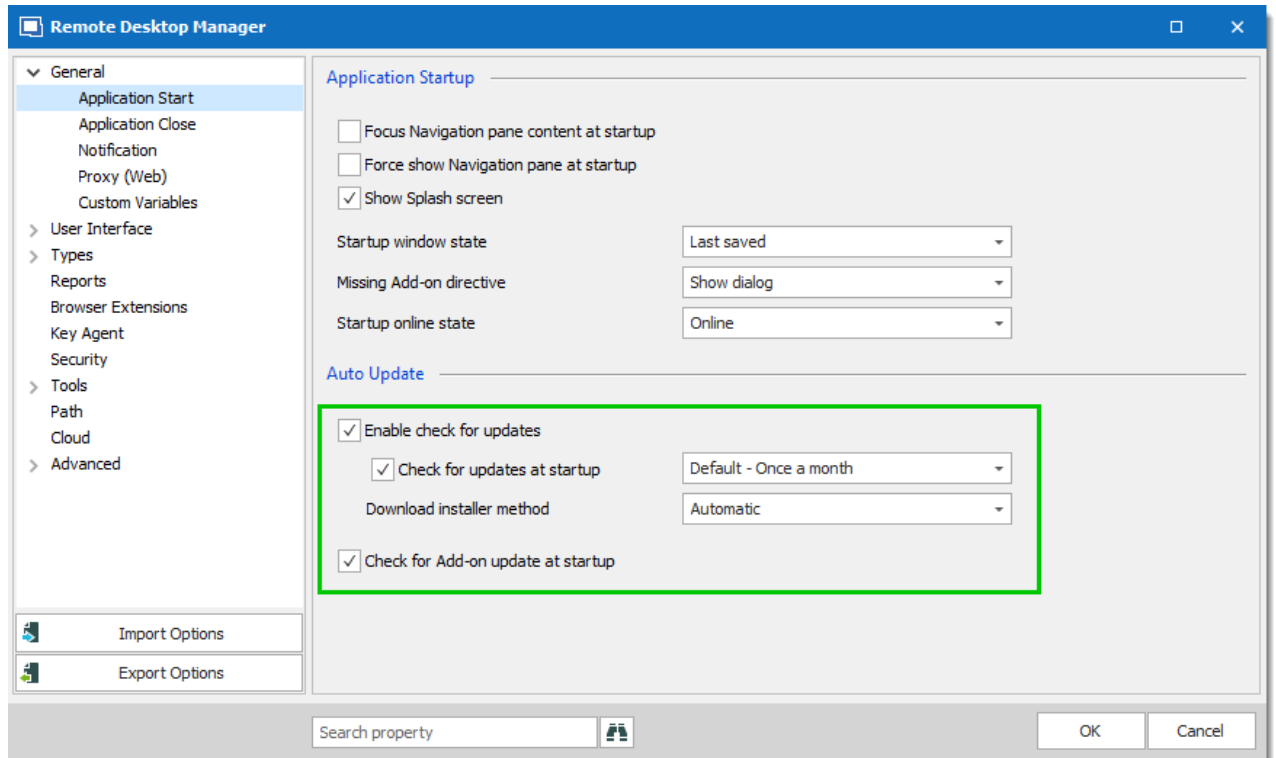
## 12.6.8 How to Disable Remote Desktop Manager Auto Update

### DESCRIPTION

Remote Desktop Manager frequently offers new updates to release new features, improvements as well as fixes. If you don't want to receive the update notifications, you can disable it in the options.

### SETTINGS

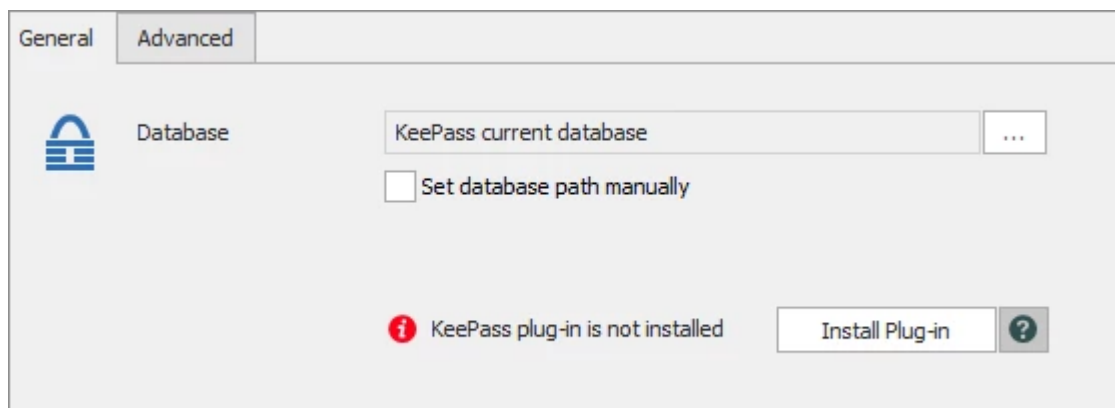
In Remote Desktop Manager, uncheck both options “**Check for update at startup**” and “**Includes Beta versions**” in **File – Options – General – Application Start**.

*Application Start - Auto Update*

## 12.6.9 How to Download the KeePass Plugin

### DESCRIPTION

You need the KeePass plug-in to send the credential to Remote Desktop Manager (RDM).





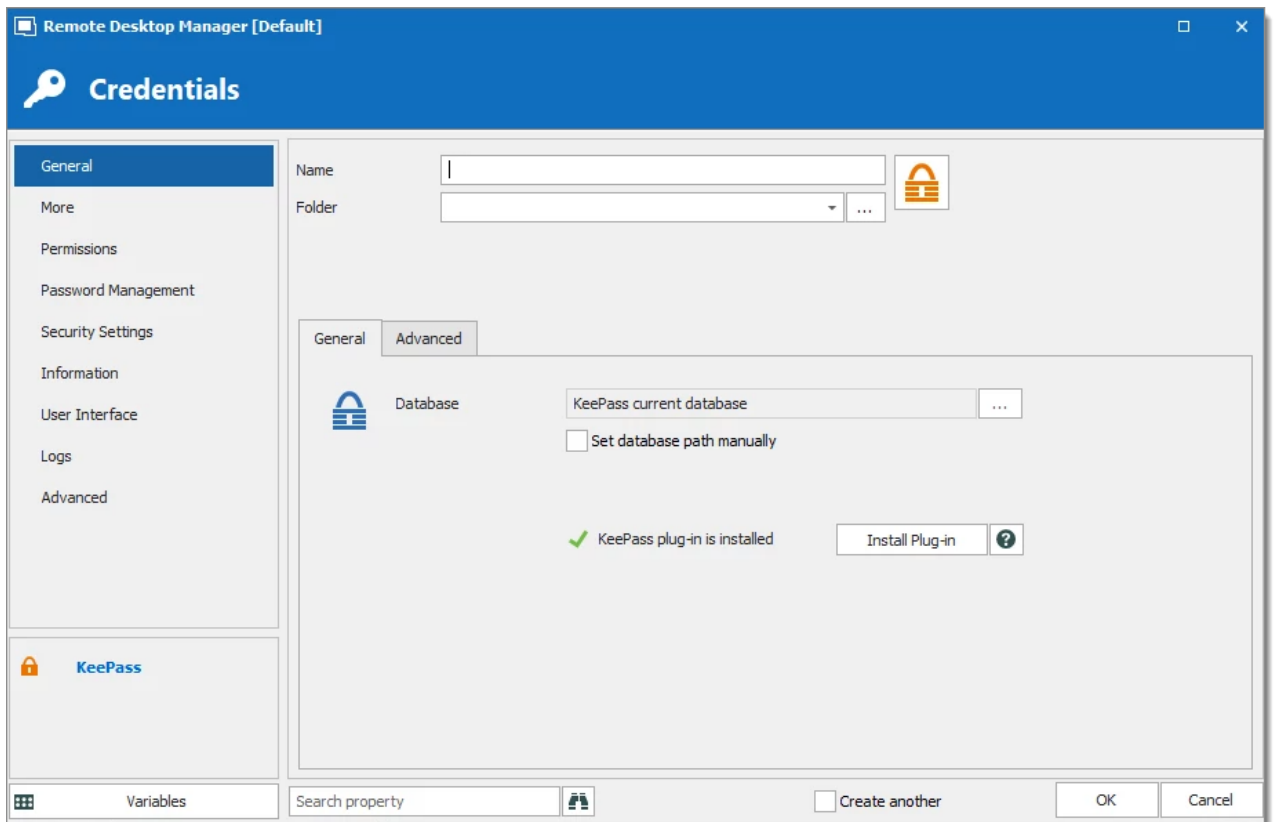
KeePass 1.X is not supported.

1. Due to the changes made in RDM with add-on, you will need to download the KeePass plugin manually using this link :  
<https://remotedesktopmanager.com/download/Devolutions.RemoteDesktopManager.KeePassPlugin.2.1.2.0.zip>.
2. When the download is finished, copy the .dll files in the KeePass installation folder (you can locate your KeePass installation folder with the help of the KeePass Help Center).



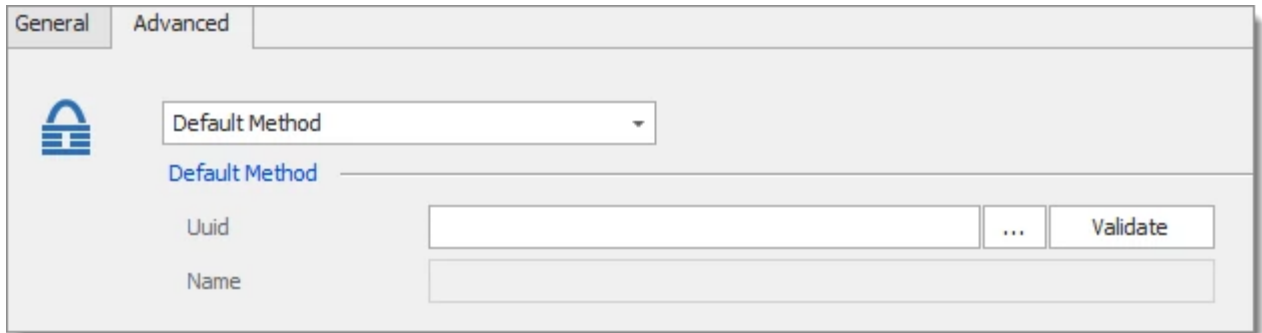
The KeePass application must be running and the database must be opened

3. In RDM create a KeePass entry. You can validate that the KeePass plug-in is now installed.



Remote Desktop Manager will by default select the database; this option can be overridden by manually entering the path. RDM also can support linking to multiple KeePass databases simultaneously. Add all the paths separated by semicolons.

4. In the Advanced tab choose your preferred method. It is where you can enter your Universal Unique Identifier (Uuid) and the name of the entry in the database, or to always be prompt with a list.



General Advanced

Default Method

Default Method

Uuid

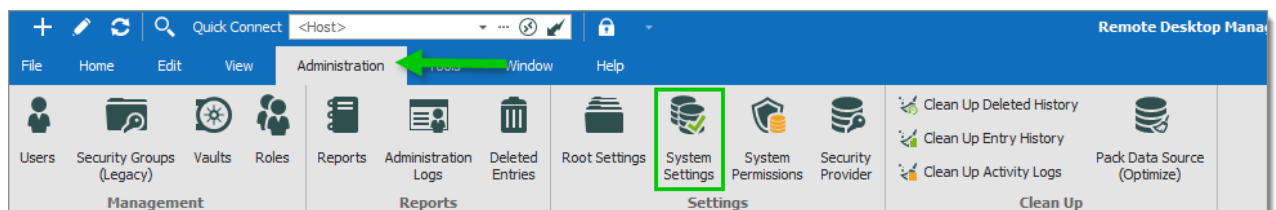
Validate

Name

## 12.6.10 How to Register Licenses in Older Version

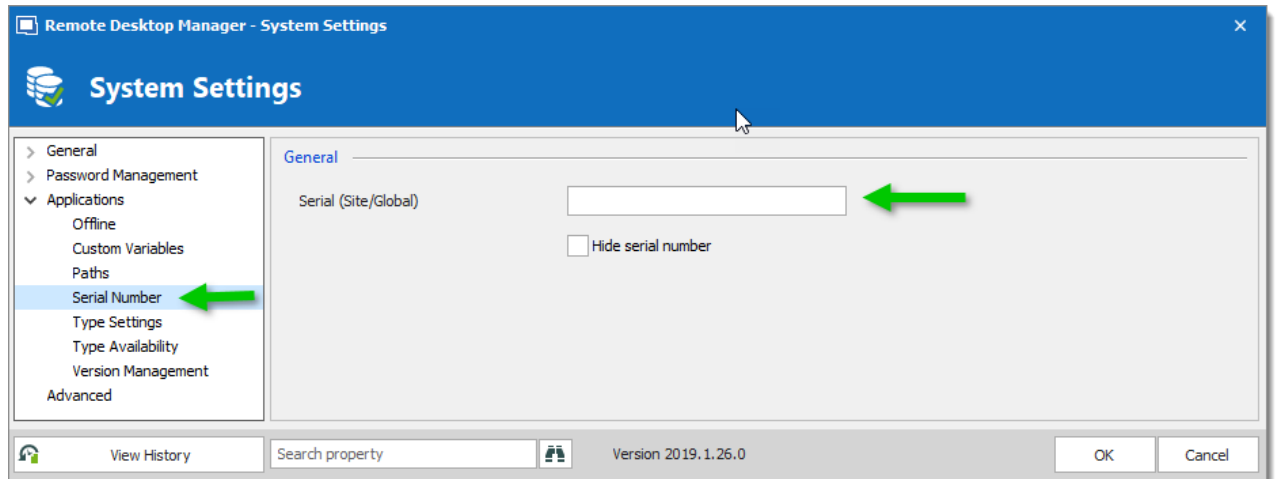
### DESCRIPTION

To register the license serial of Remote Desktop Manager in the data source in a version prior to 2019.2.24, go to **Administration - System Settings**.



*Administration - System Settings*

In the System Settings window, go in the **Serial Number** section. Enter the license serial and click **OK**.



*System Settings - Serial Number*

## 12.6.11 How to Reinstall Remote Desktop Manager

### DESCRIPTION



Before reinstalling Remote Desktop Manager, a backup will be required. Please consult [How-to Backup](#) topic.

Refer to the [Installation Overview](#) topic for details on the installation of Remote Desktop Manager.

### SETTINGS

After Remote Desktop Manager has been reinstalled on your computer, you need to copy your RemoteDesktopManager.cfg (that you had backed up) to the **%LocalAppData%\Devolutions\RemoteDesktopManager folder. This is the default path.** If you have not installed with the default settings, please consult [Configuration File Location](#) for instructions on locating your configuration folder.

### DATA

If you have moved the file based data source to another relative path, you will have to edit the data source definitions to fix the paths.

## 12.6.12 How to Send an Error Report

### DESCRIPTION

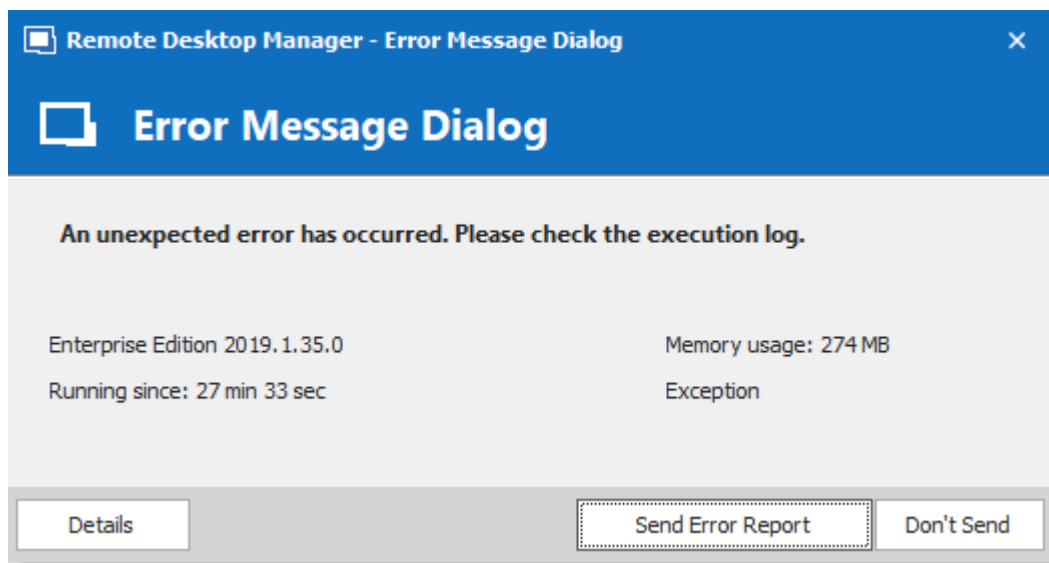
When an application error occurs in Remote Desktop Manager, you can send the error report to the Devolutions' support team.



The strength of Remote Desktop Manager comes in great part from its community of users and we depend on you to not only send in those reports, but to do it with as much information as possible. We often already have the solution, so please use your real email address.

### WORKFLOW

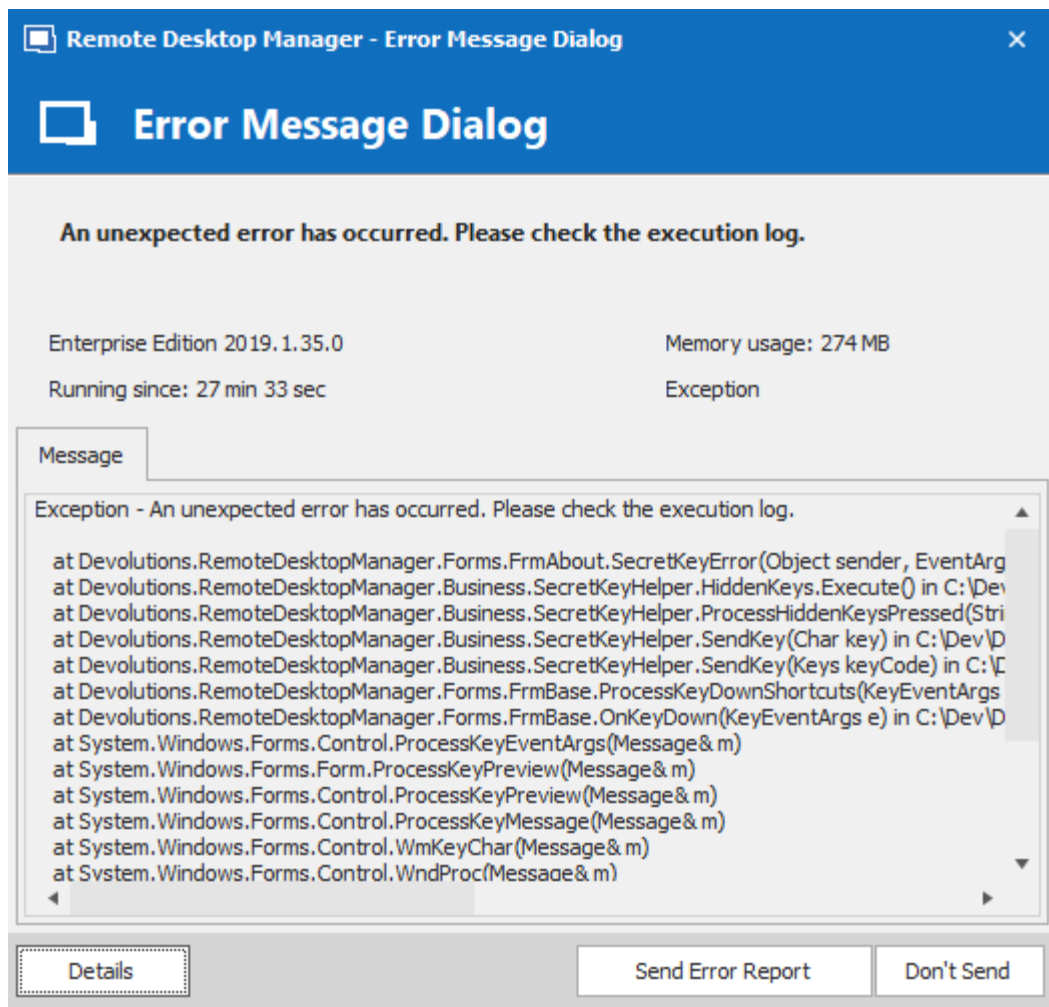
1. An error dialog appears in Remote Desktop Manager.



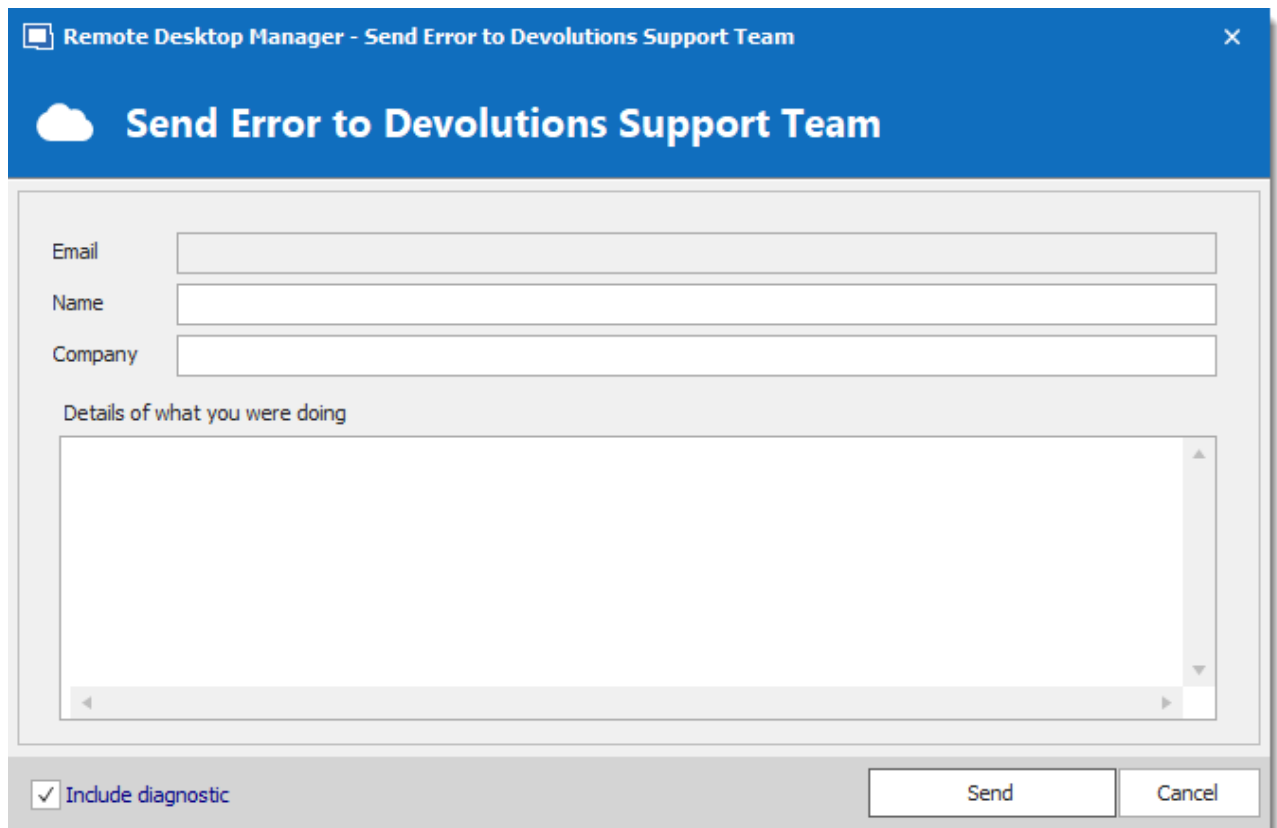
*Error Message dialog*

2. To see more information regarding the error click on **Details**.



*Details*

3. To send in the report, press **Send Error Report**



Remote Desktop Manager - Send Error to Devolutions Support Team

**Send Error to Devolutions Support Team**

Email

Name

Company

Details of what you were doing

☒ Include diagnostic

Send Cancel

*Send Error Report*

4. Fill in your information and add as many details as you can before pressing **Send** such as:



It's really important that you enter your email address, name and company name before you send the report, so that the Devolutions support team can contact you.

- The feature that you were using;
- The steps that you performed to get the error;
- Has this error occurred more than once;
- Are you the only one in your team to have the error; etc.

### 12.6.13 How to Send a File Securely

#### DESCRIPTION

The Support team, QA department or engineering department may request some file(s) for investigation on a specific scenario or to troubleshoot a certain issue.

## SOLUTION

Devolutions has a secure way to transfer file(s) between a customer and us. We use ShareFile to transfer the data securely.

The file(s) can be sent to us securely via this link <https://devolutions.sharefile.com/filedrop>.

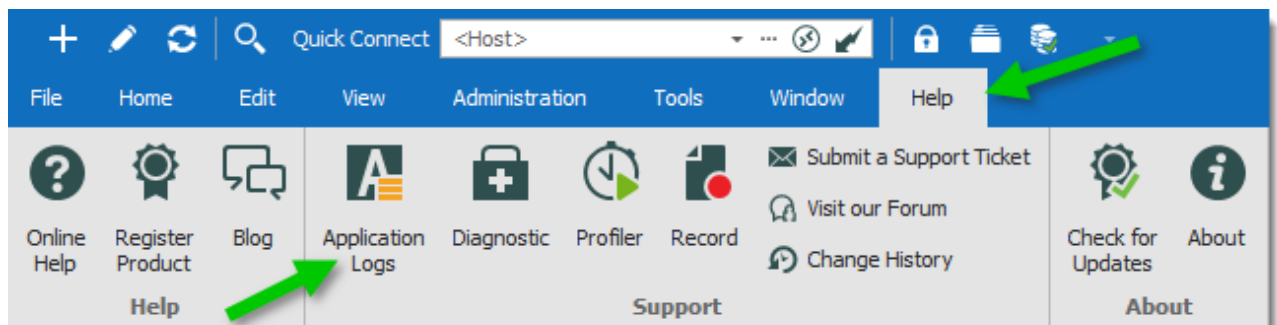
### 12.6.14 How to Send the Application Logs Report

## DESCRIPTION

The Devolutions support team may ask for the application logs to help you in certain situation. Here is how to send it to the support team.

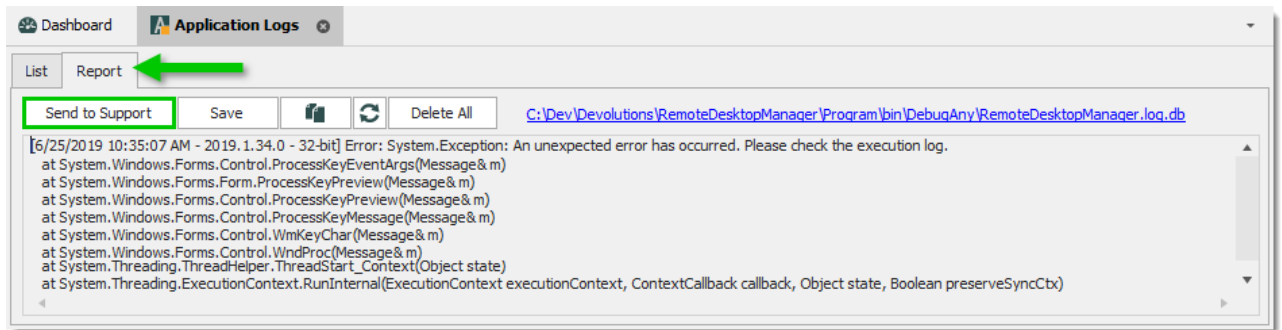
## WORKFLOW

1. Click on **Help – Application Logs**.



*View Application Log*

2. Select the **Report** tab. Then click on the **Send to Support** button.

*Report Tab*

3. Fill the **Email**, **Company** and **Name** field with your information (your email address, your Company name and your name) and click on **OK** to send the report.

Remote Desktop Manager - Send Message to Devolutions Support Team

## Send Message to Devolutions Support Team

Personal Information

Email

Company

Name

☒ Send data source information

☒ Diagnostic information

Subject

Message

Save to File OK Cancel

*Send message to Support*

### 12.6.15 How to Send your Configuration File

The Devolutions support team may ask for your configuration file to help you in certain situations. Here's how to send a clean configuration file to the support team.

1. Go in **File – Options** and press the **Export Options** button.
2. Remove any sensitive information's and **save** the file on your computer. The file name will be RemoteDesktopManager.cfg.
3. In order for us to provide you a secure link to share your file, send an email to [ticket@devolutions.net](mailto:ticket@devolutions.net).

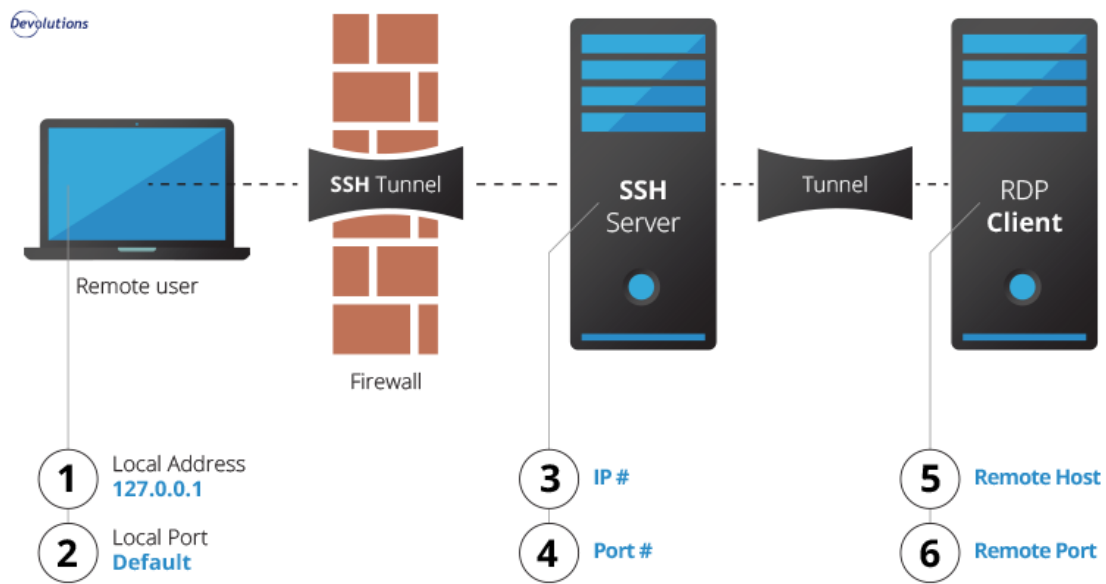


### 12.6.16 How to Setup a SSH Tunnel

#### DESCRIPTION

SSH tunneling is used to create an encrypted connection over an untrusted network. It consists of an encrypted tunnel created through an SSH protocol, providing secure connections for data transfer. The SSH Tunnel can be used to establish sort of a virtual private network (VPN) to access services across firewalls.

This is the procedure to establish a basic SSH Tunnel to reach a remote machine.



SSH Tunnel Diagram

## CREATE AN SSH TUNNEL

To create an SSH tunnel, local connections through a specified port must be forwarded to an SSH server.

To create an SSH tunnel a given port of one machine needs to be forwarded to a port on the other machine which will be the other end of the tunnel. Once the SSH tunnel has been established, the user can connect to earlier specified port at first machine to access the network service.

1. Create an **SSH Tunnel** entry.

The screenshot shows the 'SSH Tunnel entry' configuration window. It has three tabs: 'General', 'Private Key', and 'Advanced'. The 'General' tab is selected. Under the 'General' section, there are fields for 'Host', 'Username', 'Password', and 'Password prompt string'. There is also a 'Set public key' button. Under the 'Outgoing Tunnel Settings' section, there are fields for 'Mode' (set to 'Local'), 'Local address' (set to '127.0.0.1'), 'Local port' (set to 'Default'), 'Remote host', and 'Remote port' (set to 'Default').

SSH Tunnel entry

Set up the properties as follows:

## SSH SERVER SETTINGS

OPTION	DESCRIPTION
<b>Host</b>	Set the IP address of the SSH Server. (please refer to <b>1</b> in the Tunnel diagram)
<b>Port</b>	Set the port of the SSH Server. The default port is 22. (please refer to in the Tunnel diagram)
<b>Set public key</b>	Setup the public key
<b>Username</b>	Enter the SSH server username to connect.
<b>Password</b>	Enter the SSH server password to connect.

## OUTGOING TUNNEL SETTINGS

OPTION	DESCRIPTION
<b>Mode</b>	Select between: <b>Local</b> , <b>Remote</b> or <b>Dynamic</b> .
<b>Local address</b>	The local address must be left to 127.0.0.1. (please refer to ① in the Tunnel diagram)
<b>Local port</b>	In most cases leave the local port to its default value 3390. (please refer to ② in the Tunnel diagram)
<b>Remote host</b>	Enter the host or IP address of your remote client. (please refer to ⑤ in the Tunnel diagram)
<b>Remote port</b>	Set the final port that you must reach, in most cases leave it to it's default value 3389. (please refer to ⑥ in the Tunnel diagram)

At this time, you can launch your entry to see if indeed the tunnel has been opened successfully. Close the session.

## CREATE YOUR REMOTE SESSION

Create an RDP session.



The screenshot shows the 'Remote Desktop Manager [Default]' window. The left sidebar contains a tree view with categories like General, More, Permissions, Password Management, Security Settings, Session Recording, VPN/SSH/Gateway, User Interface, Information, Jump Host, Events, Sub Connections, Logs, Management Tools, and Advanced. The main pane is titled 'General' and shows the following fields:

- Name:** RDP through SSH Tunnel
- Folder:** Enterprise\Sessions\Remote Connections
- Display:** Embedded (tabbed)
- Credentials:** Default

Below these fields are tabs for General, Display, Local Resources, Programs, Experience, Connection, and Advanced. The 'General' tab is active, showing:

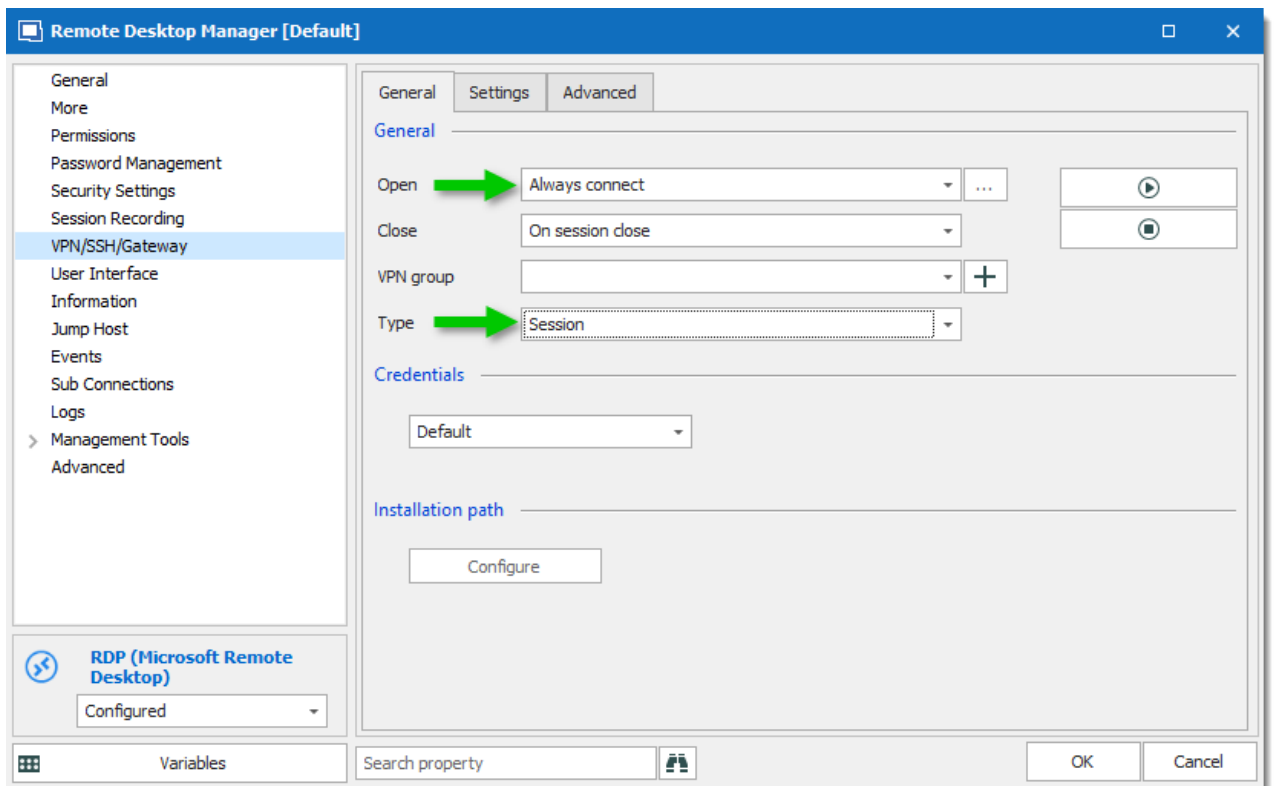
- Host:** 127.0.0.1
- RDP type:** Normal
- Username:** XXXXXX
- Domain:** XXXXXX
- Password:** A masked password field with a strength indicator showing 'Very Strong'.
- ☐ Always ask password
- ☐ Store password locally
- ☐ Open console (Admin mode)

At the bottom, there is a 'Variables' section, a 'Search property' field, and buttons for 'Create another', 'OK', and 'Cancel'.

RDP entry

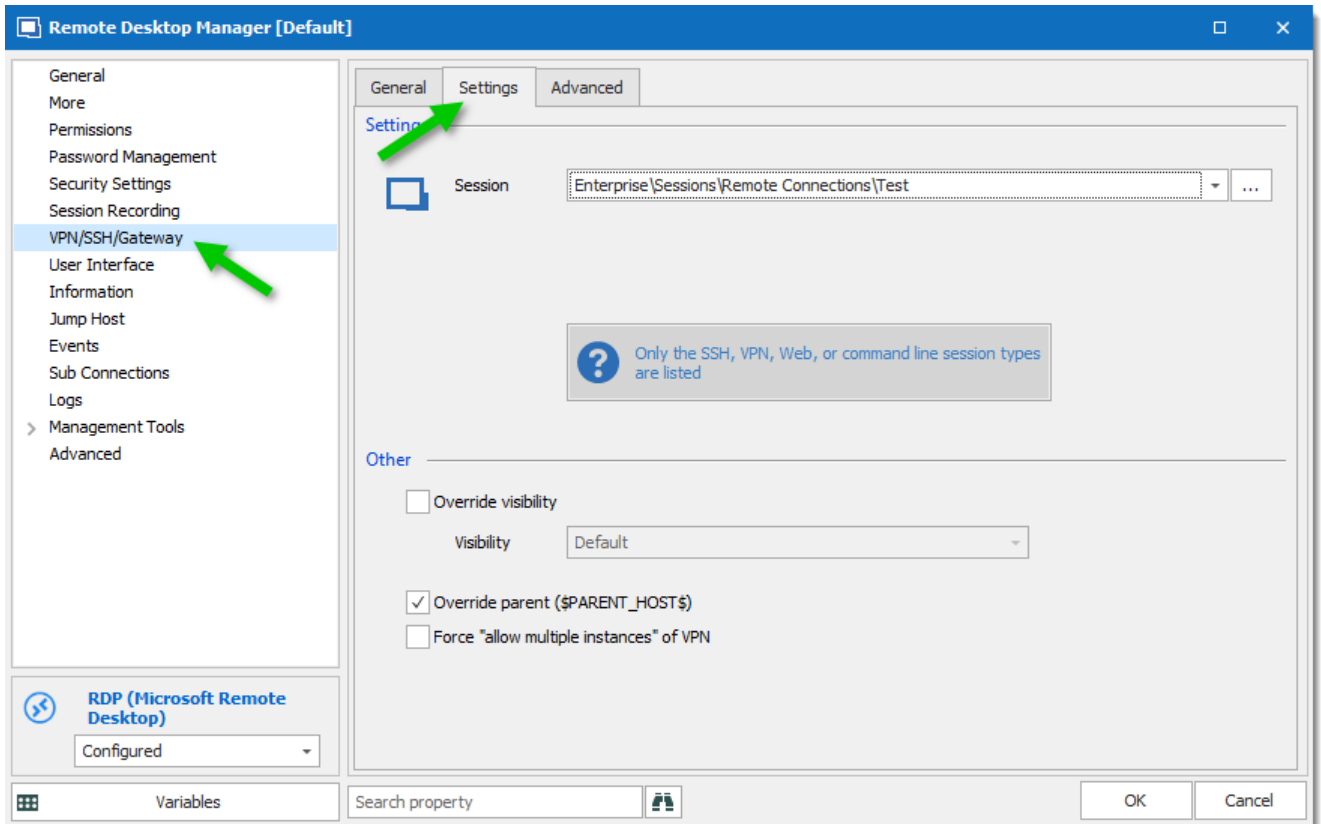
OPTION	DESCRIPTION
<b>Host</b>	Enter your <b>Local address</b> which is 127.0.0.1. (please refer to ① in the Tunnel diagram)
<b>Port</b>	Enter your <b>Local port</b> which is 3390. (please refer to ② in the Tunnel diagram)
<b>RDP type</b>	Leave the RDP type to Normal.
<b>Username</b>	Enter the username of your Remote Host.
<b>Domain</b>	Enter the domain of your Remote Host.
<b>Password</b>	Enter the password of your Remote Host.

In the **VPN/SSH/Gateway** side menu of your RDP session select **Always connect** in the **Open** field and **Session** in the **Type** field.



*RDP session - VPN side menu*

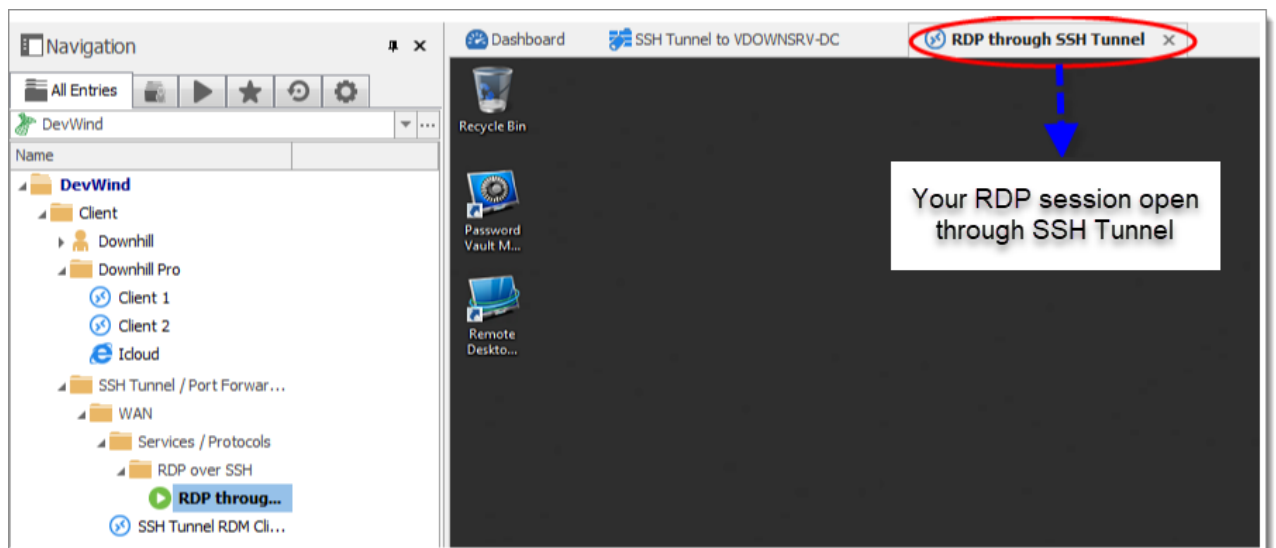
In the **VPN – Settings** tab, click on the drop down list next to **Session** and select your **SSH Tunnel** entry previously created.



*RDP session - VPN - Settings*

You now have configured your session with the following rule: for each connection that comes on interface 127.0.0.1 and port 3390, forward that connection to the SSH server and request the server to forward that connection to your Remote host.

You can now launch your RDP session, your SSH Tunnel will open, establish the connection and then launch and open your RDP session.



*RDP session open through an SSH Tunnel*

### 12.6.16.1 How to Broadcast Action in SSH

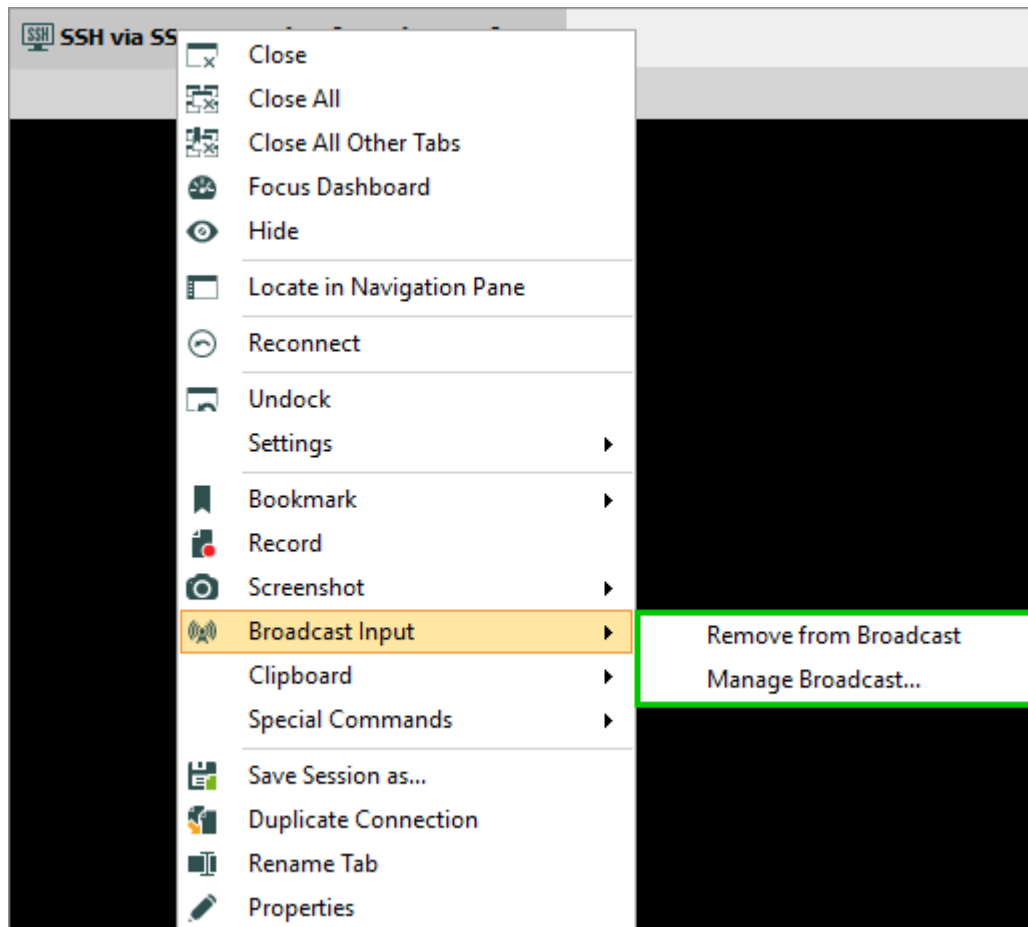
## DESCRIPTION

In Remote Desktop Manager you can manage two or more active SSH session with Broadcast actions.



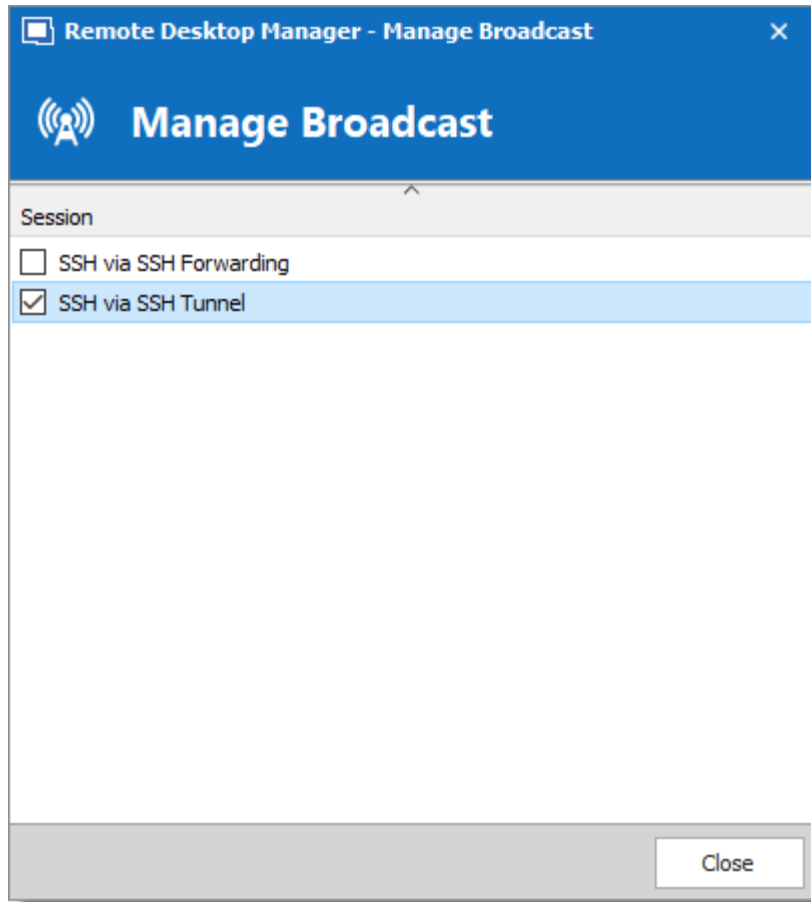
An upgraded database, by an administrator, might be required.

1. Open at least two SSH sessions.
2. Right-click on an SSH tab, click **Broadcast Input**, then **Manage Broadcast**.



*Broadcast Input Menu*

3. Select all the required session in the list and close the window.



*Manage Broadcast List*

You can now broadcast commands on all the sessions at the same time.

To remove a session from the broadcast, you can either bring the **Manage Broadcast** window to uncheck the session, or on the specific SSH tab, right-click to bring the menu, click **Broadcast Input**, then **Remove from Broadcast**.

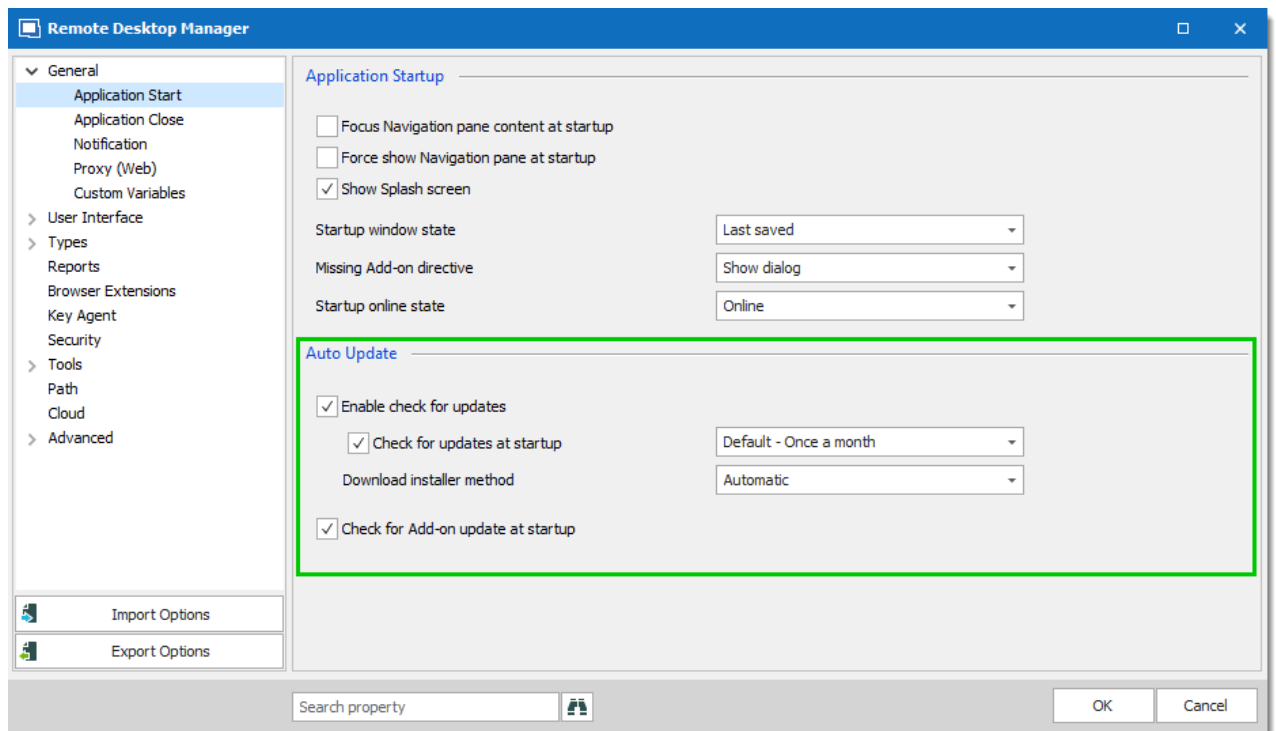
### 12.6.17 How to Setup Remote Desktop Manager to Receive New Update

#### DESCRIPTION

Remote Desktop Manager frequently offers new updates to release new features, improvements, as well as fixes. If you always want to use the latest version of Remote Desktop Manager, follow the steps below.

#### SETTINGS

1. In the application, check both options “**Check for update at startup**” and “**All updates including beta**” in **File – Options – General – Application Start**.



General - Application Start - Auto Update

2. Subscribe to the [Announcements Forums](#) to be aware of all the latest announcements on our products.

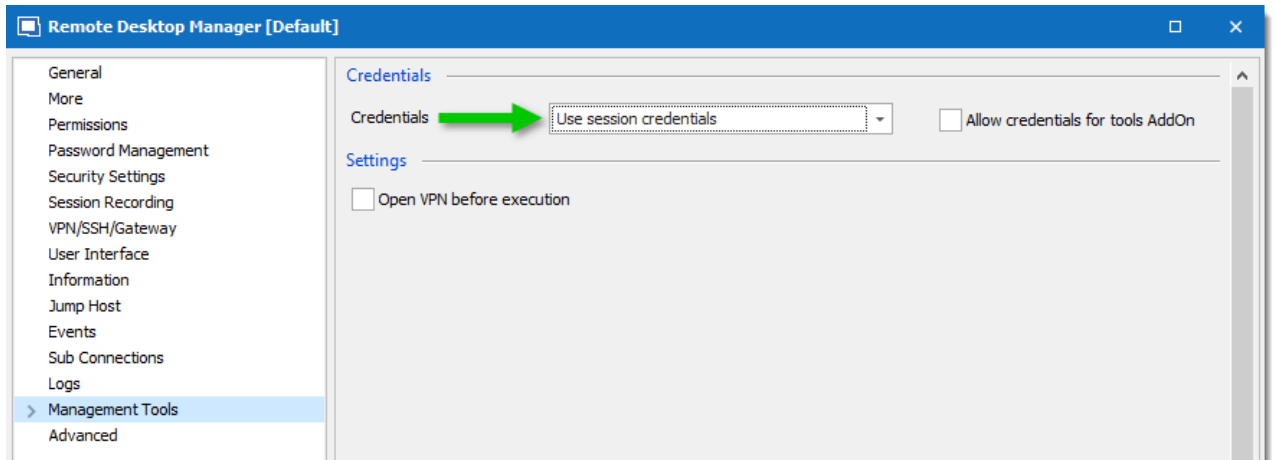
## 12.6.18 Setup the Usage of the Session Credentials to Launch a Tool

### DESCRIPTION

To run some tools, specific credentials needs to be sent through the remote session. By default, the credential used by a tool are the one from the Windows session. Sometime with those credentials you will not have enough privileges to run the tool. This is why you need to use the credential of the session instead.

### SETTINGS

You can specify the usage of the session credentials for a session in **Management Tools – Credentials – Use session credentials**.



*Use session credentials*

We also recommend that you configure your [Default Settings](#) of the entry type that need this setting by default.

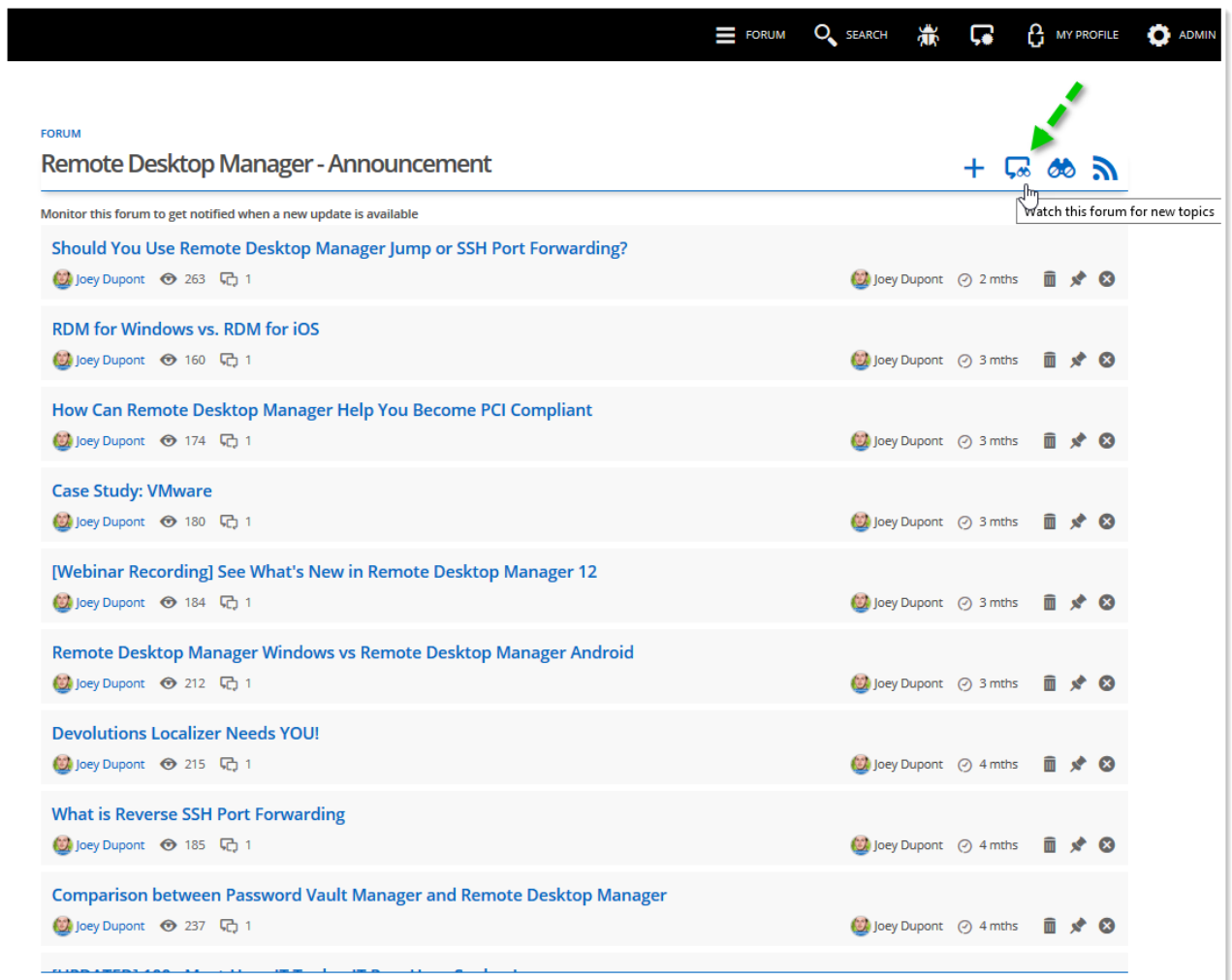
## 12.6.19 How to Subscribe to the Announcements Forums

### DESCRIPTION

You can be notified when new product updates are available by subscribing to announcements on our forum at <https://forum.devolutions.net/>

If you wish to subscribe to the announcements for Remote Desktop Manager, click on the following link : <https://forum.devolutions.net/forum20-remote-desktop-manager--announcements.aspx>

After, click on **Watch this forum for new topics**.



Devolutions Forum

The procedure is the same for all forums.

## 12.6.20 How to Use a Typing Macro to Perform Authentication

### DESCRIPTION

Sometimes it can be difficult to perform authentication on certain websites. With Remote Desktop Manager, it's possible to send the credential through a typing macro using variables.





This feature simply uses a basic mechanism offered by the .net framework of sending keystrokes, much like if a person was using the keyboard. It sends the keystrokes to the operating system itself, they will be handled by WHATEVER application has the focus at the time that the message is received. If the focus is switched to another window, the credentials will most likely be revealed by being typed in a text area.

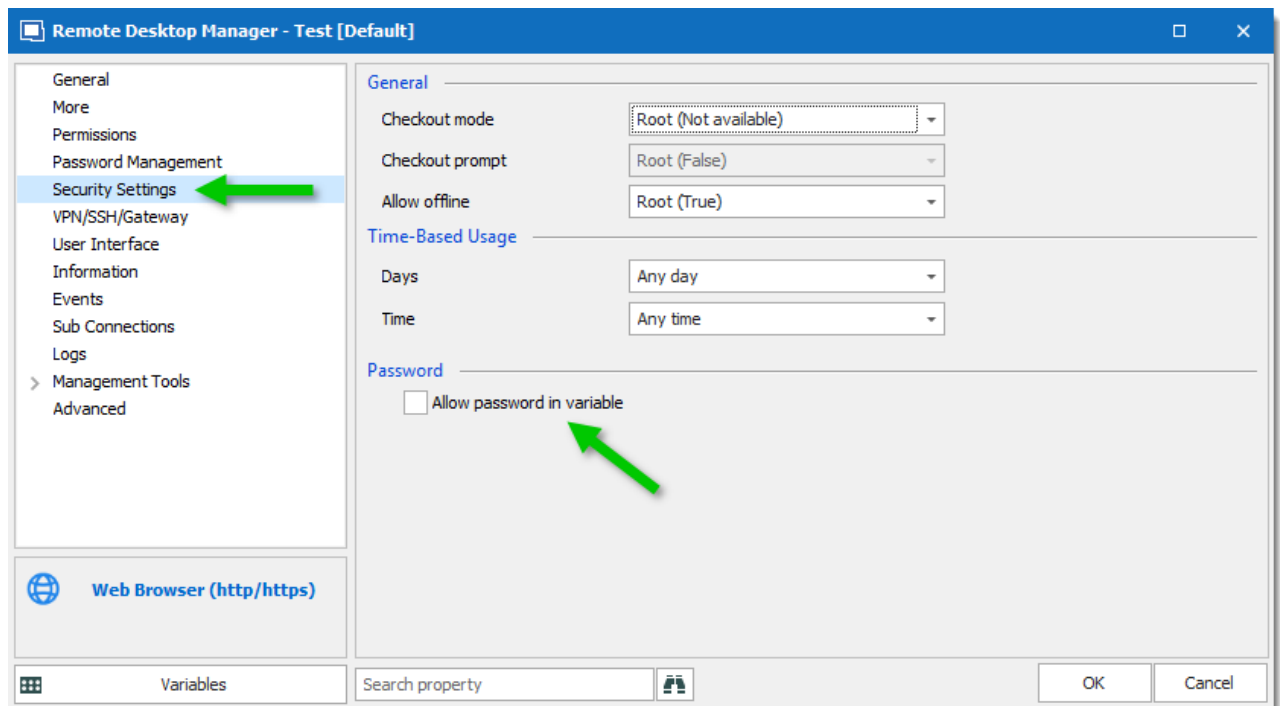
DO NOT USE THIS FEATURE in an environment where passwords MUST be hidden from the user.

## SETTINGS

1. Edit your **Web Browser (http/https)** entry, click on the **Login** tab, and unchecked the **Auto submit** and **Auto fill login** option.

Autofill

2. In the **Security Settings** section, check the **Allow password in variable** option. This option need to be checked so that the typing macro can send the password to the remote session.

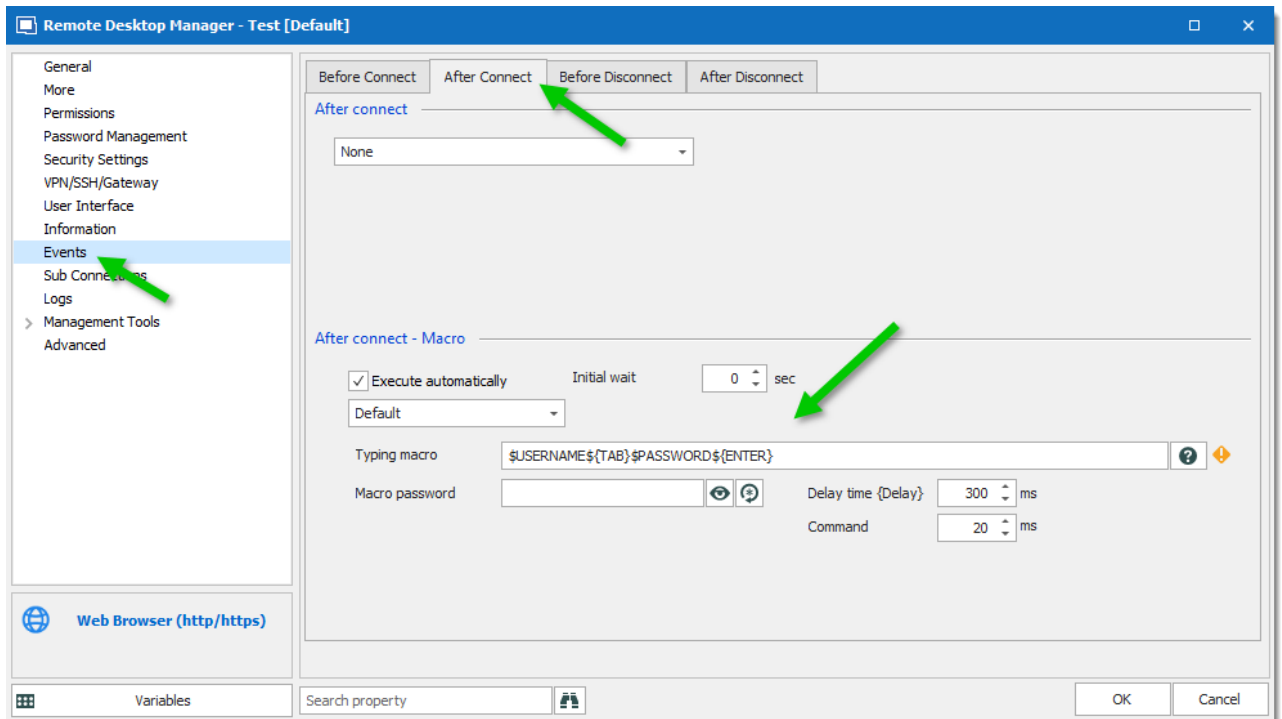


Allow password in variable



Using an [Advanced Data Sources](#), the option **Allow password in macro (send keys)** in [Administration - Data Source Settings \(System Settings\) - Password Management](#) also needs to be enabled.

3. In the **Events** section, click on the **After Connect** tab and add the following macro in the **Typing Macro** section: \$USERNAME\${TAB}\$PASSWORD\${ENTER}. You may have to adjust the **Initial wait** to leave time for the page to load.



Typing macro



Make sure that the cursor is in the appropriate field prior to the macro execution so that the username and password can be sent properly to the website.

## 12.6.21 How to use the Theme system

### DESCRIPTION

The "Theme system" of Remote Desktop Manager is still in its infancy and will evolve in future releases. You can override most images used by Remote Desktop Manager simply by providing an image in the Theme folder, the only requirement is that the file uses a specific name. Most images come in pair, a small one and a large one. You must override both in order to be consistent.

### FOLDER LOCATION

The **Theme** folder can be found in your local [configuration folder](#), under the **Images** folder.

## IMAGE FILE SPECIFICATIONS

### TRAY ICON

It must be a standard [\\*.ico](#) file containing at least a 16\*16 image. The name must be **Trayicon.ico**.

### SMALL IMAGES

Png file, 16\*16 pixels.

### LARGE IMAGES

Png file, 32\*32 pixels.

## IMAGE FILE NAMES

The file name is standardized as: {EntryType}{Size}.png

For instance for the Folder type, the image names are: **GroupFolderLarge.png** and **GroupFolderSmall.png**. Another example is for RDP sessions, their name is RDPConfigured, resulting in **SessionRDPConfiguredLarge.png** and **SessionRDPConfiguredSmall.png**.

Please consult [Image List](#) to see a list of most images.

#### 12.6.21.1 Image List

## DESCRIPTION

Here is a partial list of images that are possible to override using the theme folder.

## IMAGES

Trayicon.ico

2XClientLarge.png  
2XClientSmall.png  
AmmyyAdminLarge.png  
AmmyyAdminSmall.png  
AnydeskLarge.png  
AnydeskSmall.png  
AnyplaceControlLarge.png  
AnyplaceControlSmall.png  
AwrcProLarge.png  
AwrcProSmall.png  
AxelViewerLarge.png  
AxelViewerSmall.png  
AzureStorageExplorerLarge.png  
AzureStorageExplorerSmall.png  
BarracudaNgFirewallLarge.png  
BarracudaNgFirewallSmall.png  
BitviseSshClientLarge.png  
BitviseSshClientSmall.png  
BomgarRepresentativeConsoleLarge.png  
BomgarRepresentativeConsoleSmall.png  
CiscoAsdmLarge.png  
CiscoAsdmSmall.png  
CitrixNetscalerLarge.png  
CitrixNetscalerSmall.png  
ContactCompanyLarge.png

ContactCompanySmall.png  
ContactCustomerLarge.png  
ContactCustomerSmall.png  
ContactDefaultLarge.png  
ContactDefaultSmall.png  
ContactEmployeeLarge.png  
ContactEmployeeSmall.png  
ContactFamilyLarge.png  
ContactFamilySmall.png  
ContactSupplierLarge.png  
ContactSupplierSmall.png  
ContactSupportLarge.png  
ContactSupportSmall.png  
CredentialAppleKeychainLarge.png  
CredentialAppleKeychainSmall.png  
CredentialAuthAnvilPasswordServerLarge.png  
CredentialAuthAnvilPasswordServerSmall.png  
CredentialChromePasswordManagerLarge.png  
CredentialChromePasswordManagerSmall.png  
CredentialConnectionStringLarge.png  
CredentialConnectionStringSmall.png  
CredentialDefaultLarge.png  
CredentialDefaultSmall.png  
CredentialFirefoxPasswordManagerLarge.png  
CredentialFirefoxPasswordManagerSmall.png

CredentialKeePassLarge.png  
CredentialKeePassSmall.png  
CredentialLastPassLarge.png  
CredentialLastPassSmall.png  
CredentialOnePasswordLarge.png  
CredentialOnePasswordSmall.png  
CredentialPMProLarge.png  
CredentialPMProSmall.png  
CredentialPasswordBoxLarge.png  
CredentialPasswordBoxSmall.png  
CredentialPasswordSafeLarge.png  
CredentialPasswordSafeSmall.png  
CredentialPasswordVaultManagerLarge.png  
CredentialPasswordVaultManagerSmall.png  
CredentialPasswordstateLarge.png  
CredentialPasswordstateSmall.png  
CredentialPleasantPasswordServerLarge.png  
CredentialPleasantPasswordServerSmall.png  
CredentialPrivateKeyLarge.png  
CredentialPrivateKeySmall.png  
CredentialSecretServerLarge.png  
CredentialSecretServerSmall.png  
CredentialWindowsVaultLarge.png  
CredentialWindowsVaultsmall.png  
DataEntryAlarmLarge.png

DataEntryAlarmSmall.png  
DataEntryBankInfoLarge.png  
DataEntryBankInfoSmall.png  
DataEntryCredentialLarge.png  
DataEntryCredentialSmall.png  
DataEntryCreditCardLarge.png  
DataEntryCreditCardSmall.png  
DataEntryCustomLarge.png  
DataEntryCustomSmall.png  
DataEntryEmailAccountLarge.png  
DataEntryEmailAccountSmall.png  
DataEntryPassportLarge.png  
DataEntryPassportSmall.png  
DataEntrySafetyDepositLarge.png  
DataEntrySafetyDepositSmall.png  
DataEntrySecureNoteLarge.png  
DataEntrySecureNoteSmall.png  
DataEntrySerialLarge.png  
DataEntrySerialSmall.png  
DataEntryWalletLarge.png  
DataEntryWalletSmall.png  
DataEntryWebLarge.png  
DataEntryWebSmall.png  
Database.NetLarge.png  
Database.NetSmall.png



DbVisualizerLarge.png  
DbVisualizerSmall.png  
DocumentCertificateLarge.png  
DocumentCertificateSmall.png  
DocumentDefaultLarge.png  
DocumentDefaultSmall.png  
DocumentExcelLarge.png  
DocumentExcelSmall.png  
DocumentImageLarge.png  
DocumentImageSmall.png  
DocumentOneNoteLarge.png  
DocumentOneNoteSmall.png  
DocumentPDFLarge.png  
DocumentPDFSmall.png  
DocumentPhoneBookLarge.png  
DocumentPhoneBookSmall.png  
DocumentPowerPointLarge.png  
DocumentPowerPointSmall.png  
DocumentTextLarge.png  
DocumentTextSmall.png  
DocumentVisioLarge.png  
DocumentVisioSmall.png  
DocumentWordLarge.png  
DocumentWordSmall.png  
EricomBlazeClientLarge.png

EricomBlazeClientSmall.png  
FileExplorerLarge.png  
FileExplorerSmall.png  
FlashfxpLarge.png  
FlashfxpSmall.png  
GateprotectFirewallAdministrationClientLarge.png  
GateprotectFirewallAdministrationClientSmall.png  
GroupCompanyLarge.png  
GroupCompanySmall.png  
GroupCustomerLarge.png  
GroupCustomerSmall.png  
GroupDatabaseLarge.png  
GroupDatabaseSmall.png  
GroupDeviceLarge.png  
GroupDeviceSmall.png  
GroupDomainLarge.png  
GroupDomainSmall.png  
GroupFolderLarge.png  
GroupFolderSmall.png  
GroupIdentityLarge.png  
GroupIdentitySmall.png  
GroupPrinterLarge.png  
GroupPrinterSmall.png  
GroupRootLarge.png  
GroupRootSmall.png

GroupServerLarge.png  
GroupServerSmall.png  
GroupSiteLarge.png  
GroupSiteSmall.png  
GroupSoftwareLarge.png  
GroupSoftwareSmall.png  
GroupWorkstationLarge.png  
GroupWorkstationSmall.png  
HeidisqlLarge.png  
HeidisqlSmall.png  
HpIntegratedLightsOutLarge.png  
HpIntegratedLightsOutSmall.png  
IbmPersonalCommunicationsLarge.png  
IbmPersonalCommunicationsSmall.png  
IsiLightDeskLarge.png  
IsiLightDeskSmall.png  
JavaWebStartLarge.png  
JavaWebStartSmall.png  
MacroScriptAppleScriptLarge.png  
MacroScriptAppleScriptSmall.png  
MacroScriptAutoHotKeyLarge.png  
MacroScriptAutoHotKeySmall.png  
MacroScriptAutoITLarge.png  
MacroScriptAutoITSmall.png  
MacroScriptCommandLineLarge.png

MacroScriptCommandLineSmall.png  
MacroScriptDatabaseQueryLarge.png  
MacroScriptDatabaseQuerySmall.png  
MacroScriptJitBitLarge.png  
MacroScriptJitBitSmall.png  
MacroScriptMacroLarge.png  
MacroScriptMacroSmall.png  
MacroScriptPSExecLarge.png  
MacroScriptPSExecSmall.png  
MacroScriptPowerShellLarge.png  
MacroScriptPowerShellLocalLarge.png  
MacroScriptPowerShellLocalSmall.png  
MacroScriptPowerShellSmall.png  
MacroScriptTemplateLarge.png  
MacroScriptTemplateSmall.png  
MacroScriptVBScriptLarge.png  
MacroScriptVBScriptSmall.png  
MacroScriptWASPPowerShellLarge.png  
MacroScriptWASPPowerShellSmall.png  
MacroScriptWMILarge.png  
MacroScriptWMISmall.png  
MobaxtermLarge.png  
MobaxtermSmall.png  
MysqlGuiToolsLarge.png  
MysqlGuiToolsSmall.png

MysqlworkbenchLarge.png  
MysqlworkbenchSmall.png  
NavicatPremiumLarge.png  
NavicatPremiumSmall.png  
NetopGuestLarge.png  
NetopGuestSmall.png  
NetsupportManagerLarge.png  
NetsupportManagerSmall.png  
NomachineLarge.png  
NomachineSmall.png  
NxClientLarge.png  
NxClientSmall.png  
OfficeWord,ExcelAndPowerPointLarge.png  
OfficeWord,ExcelAndPowerPointSmall.png  
PdfLarge.png  
PdfSmall.png  
PenguinetSshClientLarge.png  
PenguinetSshClientSmall.png  
PgadminliiLarge.png  
PgadminliiSmall.png  
PowertermProLarge.png  
PowertermProSmall.png  
ProxyNetworks-ProxyMasterLarge.png  
ProxyNetworks-ProxyMasterSmall.png  
RemoteUtilities-ViewerLarge.png

RemoteUtilities-ViewerSmall.png

Remoteassistant365Large.png

Remoteassistant365Small.png

RoyalTsLarge.png

RoyalTsSmall.png

RvtoolsLarge.png

RvtoolsSmall.png

SapGuiLarge.png

SapGuiSmall.png

SapNetweaverLarge.png

SapNetweaverSmall.png

Sccm2012RemoteControlLarge.png

Sccm2012RemoteControlSmall.png

SecurecrtLarge.png

SecurecrtSmall.png

SecurefxLarge.png

SecurefxSmall.png

SessionADConsoleLarge.png

SessionADConsoleSmall.png

SessionAddOnLarge.png

SessionAddOnSmall.png

SessionAppleRemoteDesktopLarge.png

SessionAppleRemoteDesktopSmall.png

SessionAwsLarge.png

SessionAwsSmall.png

SessionAzureLarge.png  
SessionAzureSmall.png  
SessionAzureTableStorageLarge.png  
SessionAzureTableStorageSmall.png  
SessionCitrixWebLarge.png  
SessionCitrixWebSmall.png  
SessionCommandLineLarge.png  
SessionCommandLineSmall.png  
SessionComputerLarge.png  
SessionComputerSmall.png  
SessionContactLarge.png  
SessionContactSmall.png  
SessionCredentialLarge.png  
SessionCredentialSmall.png  
SessionDamewareLarge.png  
SessionDamewareSmall.png  
SessionDataEntryLarge.png  
SessionDataEntrySmall.png  
SessionDataReportLarge.png  
SessionDataReportSmall.png  
SessionDatabaseLarge.png  
SessionDatabaseSmall.png  
SessionDeskRollLarge.png  
SessionDeskRollSmall.png  
SessionDocumentLarge.png

SessionDocumentSmall.png  
SessionDropBoxLarge.png  
SessionDropBoxSmall.png  
SessionFtpLarge.png  
SessionFtpSmall.png  
SessionGatewayLarge.png  
SessionGatewaySmall.png  
SessionGroupLarge.png  
SessionGroupSmall.png  
SessionHostLarge.png  
SessionHostSmall.png  
SessionHpRgsLarge.png  
SessionHpRgsSmall.png  
SessionHyperVLarge.png  
SessionHyperVSmall.png  
SessionICALarge.png  
SessionICASmall.png  
SessionInventoryReportLarge.png  
SessionInventoryReportSmall.png  
SessionItermLarge.png  
SessionItermSmall.png  
SessionLogMeInLarge.png  
SessionLogMeInSmall.png  
SessionPCAnywhereLarge.png  
SessionPCAnywhereSmall.png



SessionPlayListLarge.png  
SessionPlayListSmall.png  
SessionPowerShellLarge.png  
SessionPowerShellSmall.png  
SessionPuttyLarge.png  
SessionPuttySmall.png  
SessionRDPConfiguredLarge.png  
SessionRDPConfiguredSmall.png  
SessionRadminLarge.png  
SessionRadminSmall.png  
SessionRemoteAssistanceLarge.png  
SessionRemoteAssistanceSmall.png  
SessionS3Large.png  
SessionS3Small.png  
SessionSNMPReportLarge.png  
SessionSNMPReportSmall.png  
SessionScreenConnectLarge.png  
SessionScreenConnectSmall.png  
SessionSessionToolLarge.png  
SessionSessionToolSmall.png  
SessionSkyDriveLarge.png  
SessionSkyDriveSmall.png  
SessionSpiceworksLarge.png  
SessionSpiceworksSmall.png  
SessionSyncLarge.png

SessionSyncSmall.png  
SessionTeamViewerLarge.png  
SessionTeamViewerSmall.png  
SessionTerminalConsoleLarge.png  
SessionTerminalConsoleSmall.png  
SessionVMRCLarge.png  
SessionVMRCSmall.png  
SessionVMWareConsoleLarge.png  
SessionVMWareConsoleSmall.png  
SessionVMWareLarge.png  
SessionVMWareSmall.png  
SessionVNCLarge.png  
SessionVNCSmall.png  
SessionVPNLarge.png  
SessionVPNSmall.png  
SessionVirtualBoxLarge.png  
SessionVirtualBoxSmall.png  
SessionVirtualPCLarge.png  
SessionVirtualPCSmall.png  
SessionWebBrowserLarge.png  
SessionWebBrowserSmall.png  
SessionWindowsVirtualPCLarge.png  
SessionWindowsVirtualPCSmall.png  
SessionXWindowLarge.png  
SessionXWindowSmall.png

SessionXenServerLarge.png  
SessionXenServerSmall.png  
SmartftpLarge.png  
SmartftpSmall.png  
SqlServerManagementStudioLarge.png  
SqlServerManagementStudioSmall.png  
StatusAddOnMissingLarge.png  
StatusAddOnMissingSmall.png  
StatusConnectedLarge.png  
StatusConnectedSmall.png  
SupermicroIpmiUtilitiesLarge.png  
SupermicroIpmiUtilitiesSmall.png  
SyncActiveDirectoryLarge.png  
SyncActiveDirectorySmall.png  
SyncCSVLarge.png  
SyncCSVSmall.png  
TeraTermProLarge.png  
TeraTermProSmall.png  
TextLarge.png  
TextSmall.png  
ToadLarge.png  
ToadSmall.png  
VisioLarge.png  
VisioSmall.png  
VmwareHorizonViewClientLarge.png

VmwareHorizonViewClientSmall.png

VmwareRemoteConsoleLarge.png

VmwareRemoteConsoleSmall.png

WinboxLarge.png

WinboxSmall.png

XmailManagerLarge.png

XmailManagerSmall.png

XmanagerLarge.png

XmanagerSmall.png

XshellLarge.png

XshellSmall.png

ZocLarge.png

ZocSmall.png

## SPLASHSCREEN

It is possible to personalize the splashscreen by adding a splashscreen.png file in ***Images\Themes***. The recommended size is 520 by 320 but the window will automatically adapt to the image.

## 12.7 Tips And Tricks

### DESCRIPTION

Our favorite tips and tricks are in this section.

If you have a suggestion for improving an existing tip or even to suggest a new one, please send a note to [ticket@devolutions.net](mailto:ticket@devolutions.net).

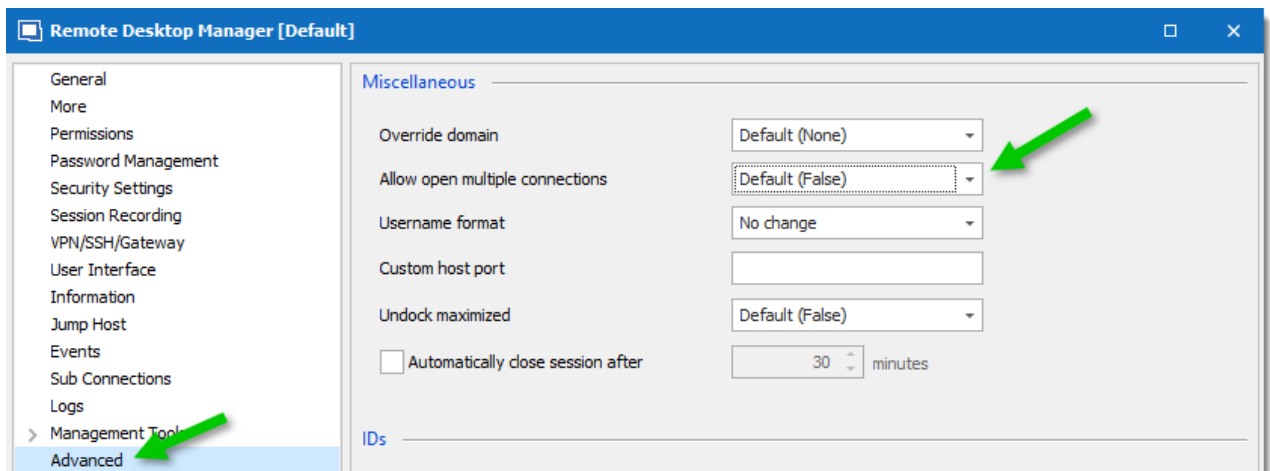
## 12.7.1 Allow Open Multiple Connections

### DESCRIPTION

Remote Desktop Manager allows you to open multiple connections on the same host.

### SOLUTION

You can enable the "Allow open multiple connections" option in the **Advanced Tab** of an entry.



*Advanced Tab*

OPTION	DESCRIPTION
True	<b>Allow open multiple connections</b> will be active for this entry only.
False	<b>Allow open multiple connections</b> will be disabled for this entry only.

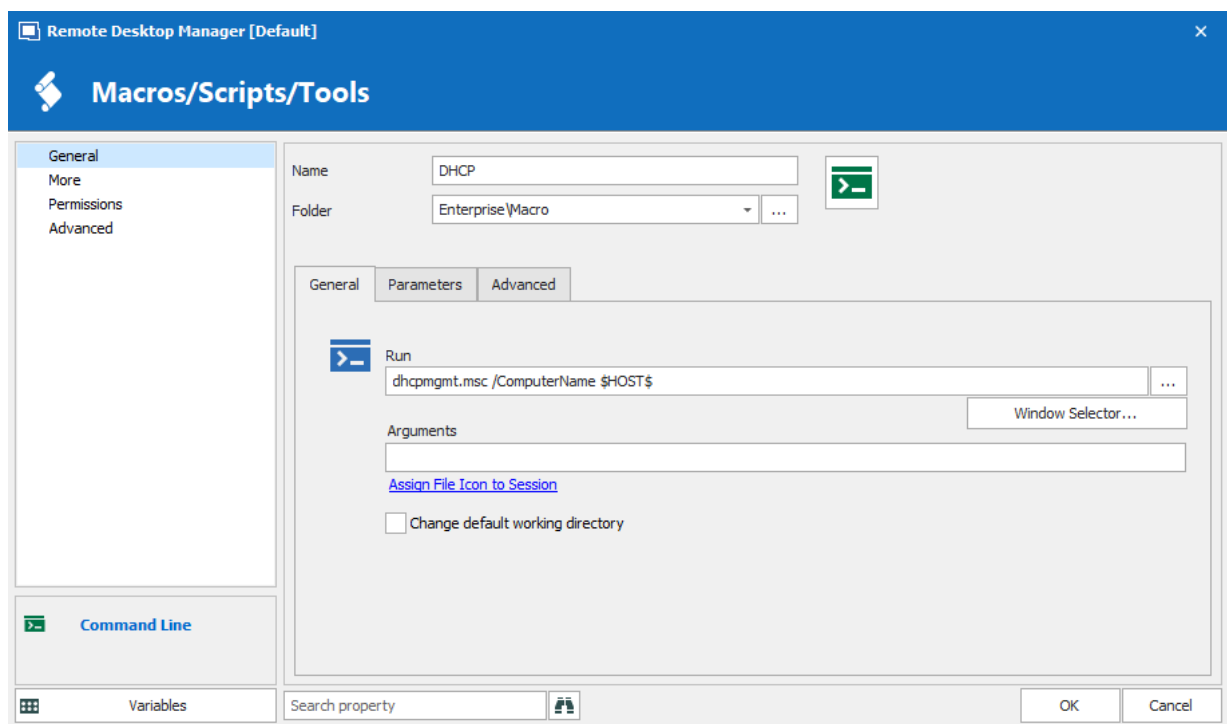
## 12.7.2 Automating Remote Microsoft Management Console (MMC)

### DESCRIPTION

You can configure a MMC Snap-In console to run on any of your servers. The Snap-In need to support remote access.

## SETTINGS

1. Create the session tool via **New Entry – Add Macros/Scripts/Tools**.
2. Select **Command Line**.
3. Name the session DHCP.
4. Type the following in the Run field: **dhcpgmt.msc /ComputerName \$HOST\$** (\$HOST\$ is the variable that will be replaced by the server name or IP address).



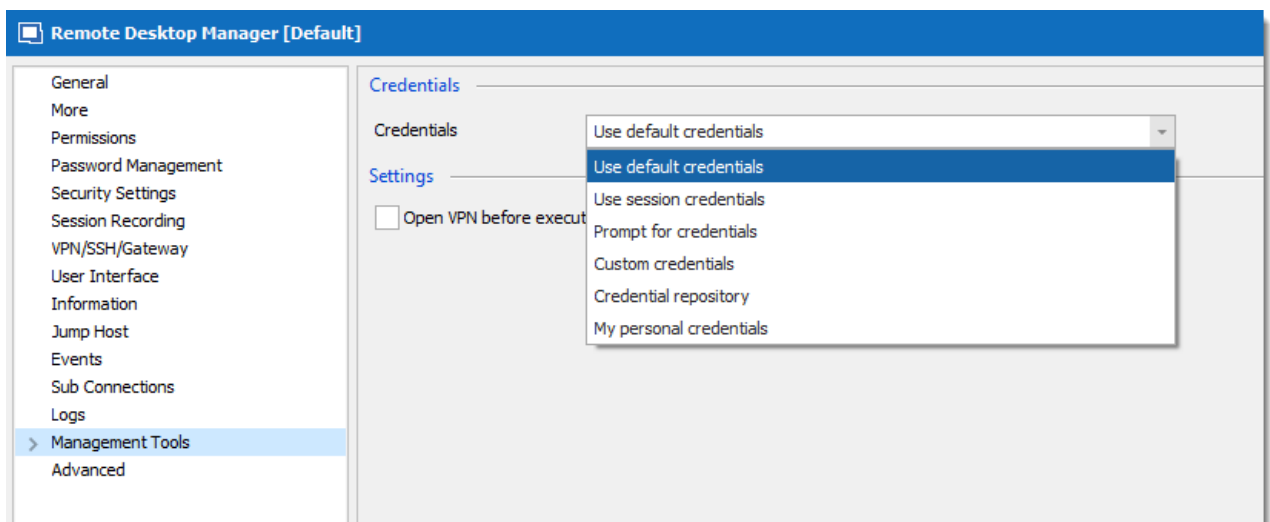
*DHCP Macros/Scripts/Tools*

5. Select **Run as Administrator** in the **Execution Mode** tab.



If you are running a Windows 64bit edition, you would need to enable the **Run in 64-bit mode** option in the **Execution Mode** tab.

6. Click **OK** to save your entry.
7. Now, you would need to verify that your sessions use the appropriate credential to run the tool. In the **Management Tools** section of each sessions, make sure you've selected the proper credentials to be supplied:

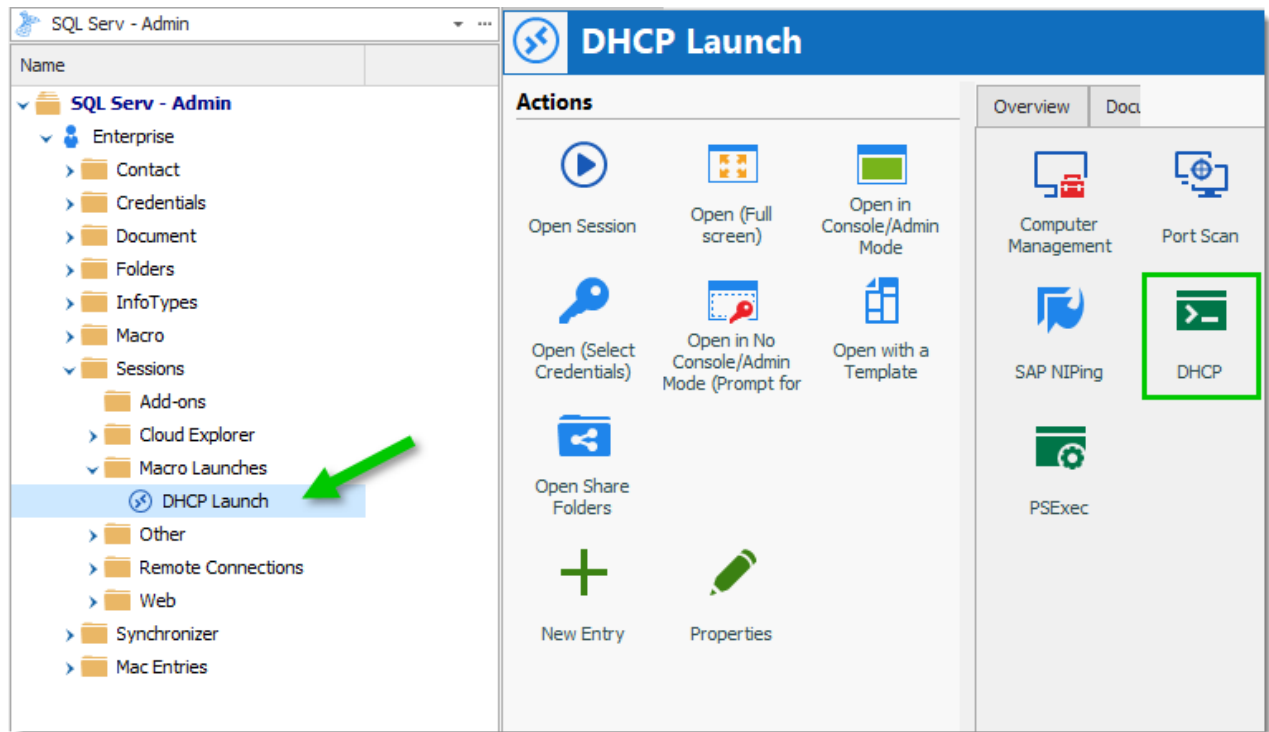


*Tools section*

OPTION	DESCRIPTION
<b>Use default credentials</b>	Use the credentials from the Windows session
<b>Use session credentials</b>	Use the same credentials as the session
<b>Prompt for credentials</b>	Prompts for the credentials on use.
<b>Custom credentials</b>	Use the Username, Password and Domain specify
<b>Credential repository</b>	Specify a set of credentials from the repository

OPTION	DESCRIPTION
<b>Use my personal credentials</b>	Use <a href="#">My Personal Credentials</a>

To run the Snap-In, select your session and execute the tool from the dashboard.



Dashboard

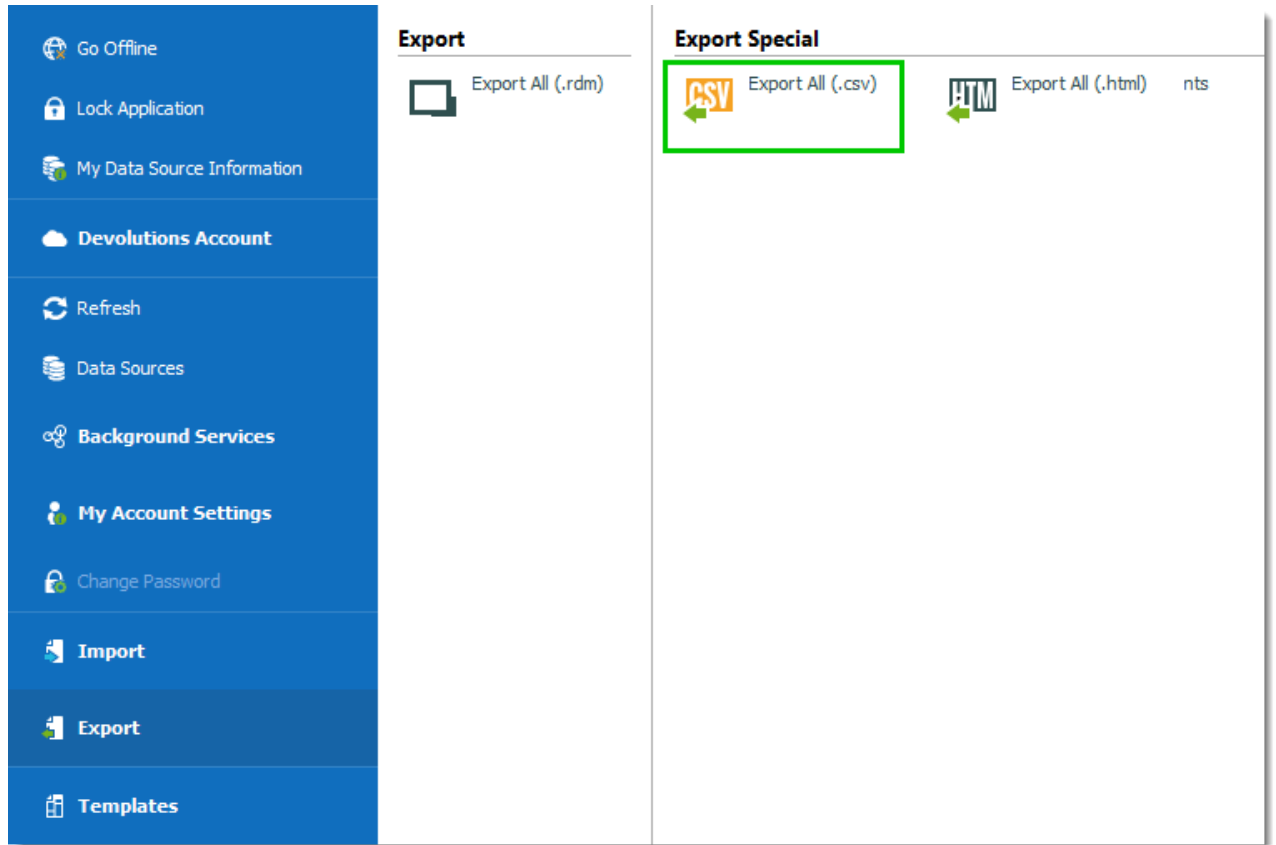
### 12.7.3 Create a list of credentials

#### DESCRIPTION

If you wish to create a report containing a full list of all your credentials here are the steps to follow:

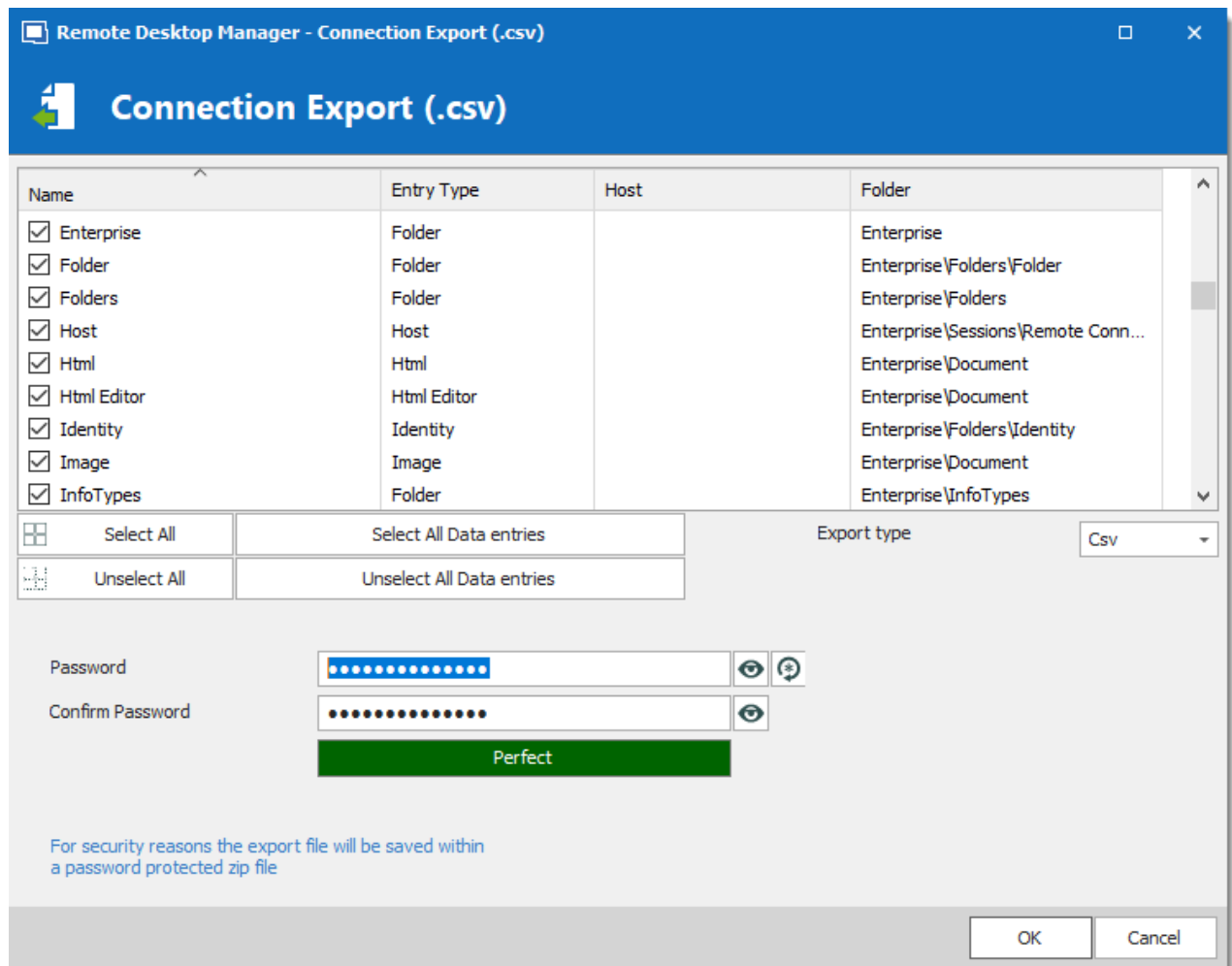
1. In the menu **File – Export – Export Special**, select the option **Export All (.csv)**.





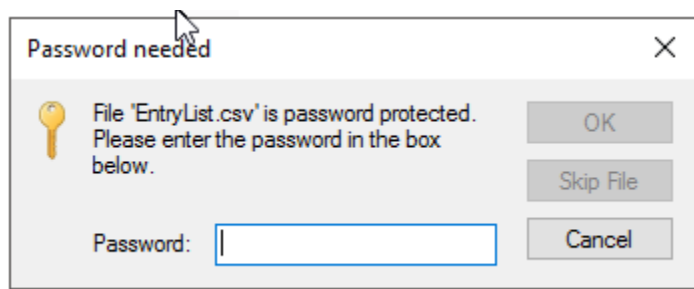
*File - Export*

2. Enter a password to create a password protected zip file.



Connection Export

3. When you try to open your Zip file, it will prompt you for your password.



Password

4. Once your password entered and your file unzipped, you will have your full list of credentials with all your information in a **\*.csv** file format.

A	B	C	D	E
ConnectionType	ConnectionSubType	SubMode	Name	Group
Web Browser (http/htt	FireFox		0 Forum test	Mark\Sessions_Test
OneDrive Explorer			0 OneDrive_Test	Mark\Sessions_Test
Putty (Telnet, SSH, RAW, rLogin)			0 Putty	Mark\Sessions_Test
Microsoft Remote Desktop (RDP)			0 QA machine W10	Mark\Sessions_Test
Microsoft Remote Desktop (RDP)			0 QA-W81	Mark\Sessions_Test
FTP/FTPS/SFTP/SCP			0 SFTP_1	Mark\Sessions_Test
Microsoft Remote Desktop (RDP)			0 SPICEWORKS-V	Mark\Sessions_Test
VMware (Player, Work: VMInfra			0 SRV-VMW	Mark\Sessions_Test
SSH Shell			0 SSH Connect.	Mark\Sessions_Test
Group/Folder			0 Sessions_Test	Mark\Sessions_Test
Microsoft Remote Desktop (RDP)			0 Telemark11	Mark\Sessions_Test

Excel Sheet

## 12.7.4 Creating Shortcuts

### OVERVIEW

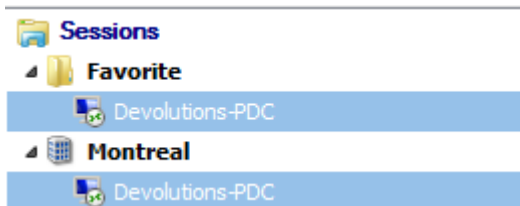
There are a many scenarios where it makes sense for an entry to appear more than once in the UI. For example, you might want to:

- Assign different access rights to the folder.
- Create a favorite folder with everything centralized.
- Reuse a document for different scenarios.

However, doing this manually is time consuming, tedious and prone to error. But no longer!

### SOLUTION

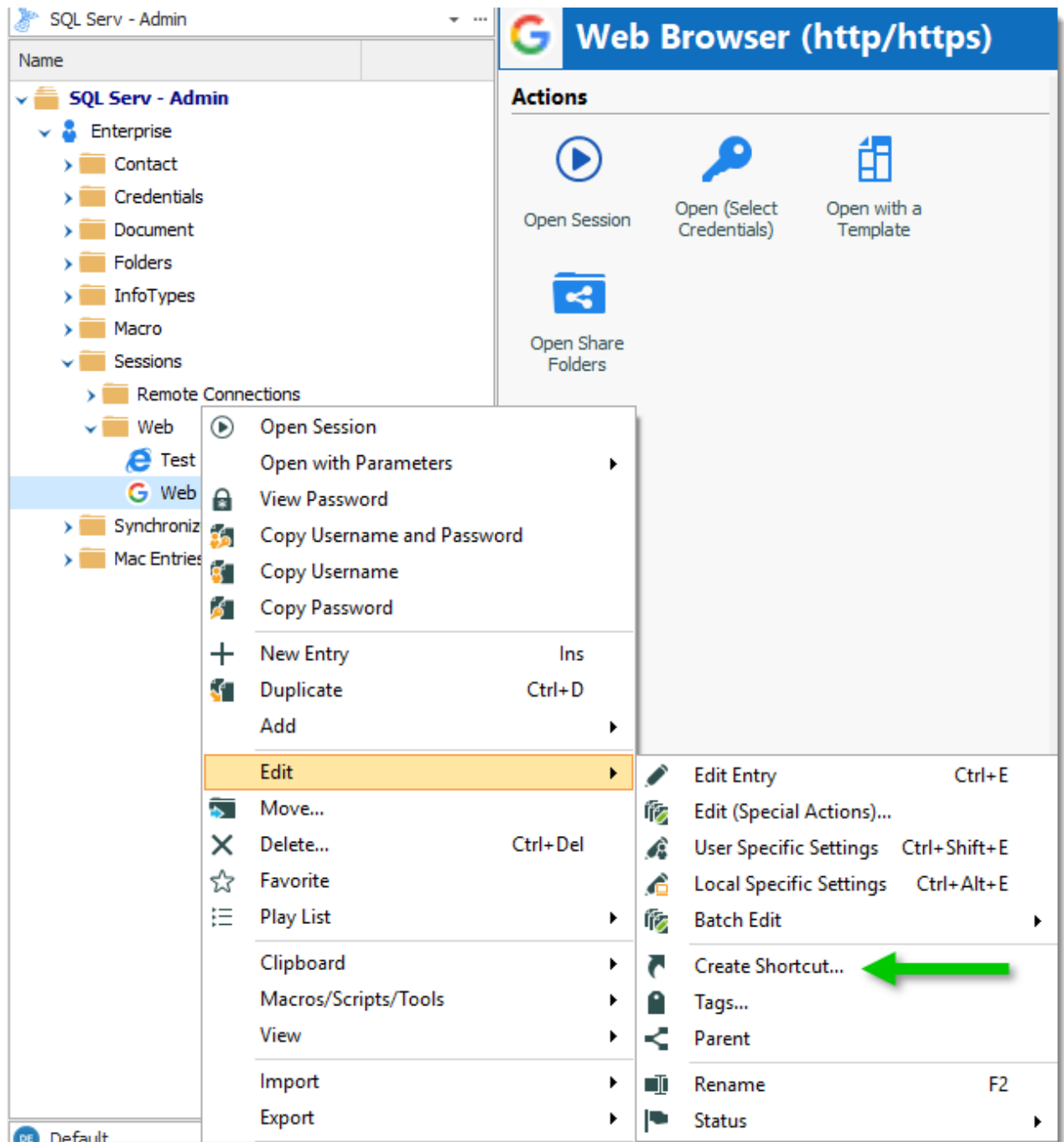
Fortunately, Remote Desktop Manager makes creating shortcuts simple and quick! It works by saving the entry once in the database, while linking it to more than one group. So when Remote Desktop Manager loads the data, it automatically creates a link to the original entry. You don't have to lift a finger – everything is done for you, to save your time and simplify your life.



Same Entry in Two Groups

## CREATING A SHORTCUT: OPTION 1

One way to create a shortcut is by using the menu **Edit -> Create Shortcut...**



*Create Shortcut Command*

Simply choose the destination folder for the shortcut. Remote Desktop Manager will automatically refresh and display the new shortcut in the list.



There is no visual difference 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, which are separated by semicolons “;”. You can also use the browse button (...) and select more than one group by holding the Ctrl key while clicking on the tree node.

*Folder Example*

### 12.7.5 Data Migration

## DESCRIPTION

Here are the steps to follow when copying data from one data source to another.



If you have used the **Document** entries in the **Stored in database** mode or used **attachments**, the binary content of the documents is NOT exported in any of our export formats. These documents/attachments **MUST** be handled manually.



If you are using a self-managed RDBMS (SQL Server, MySQL, MariaDB), you can use their management tools to move the database to another server. Please follow their respective documentation on how to successfully transfer not only that data, but also the user accounts.

SQL Server: [MSDN Article on how to move databases](#)

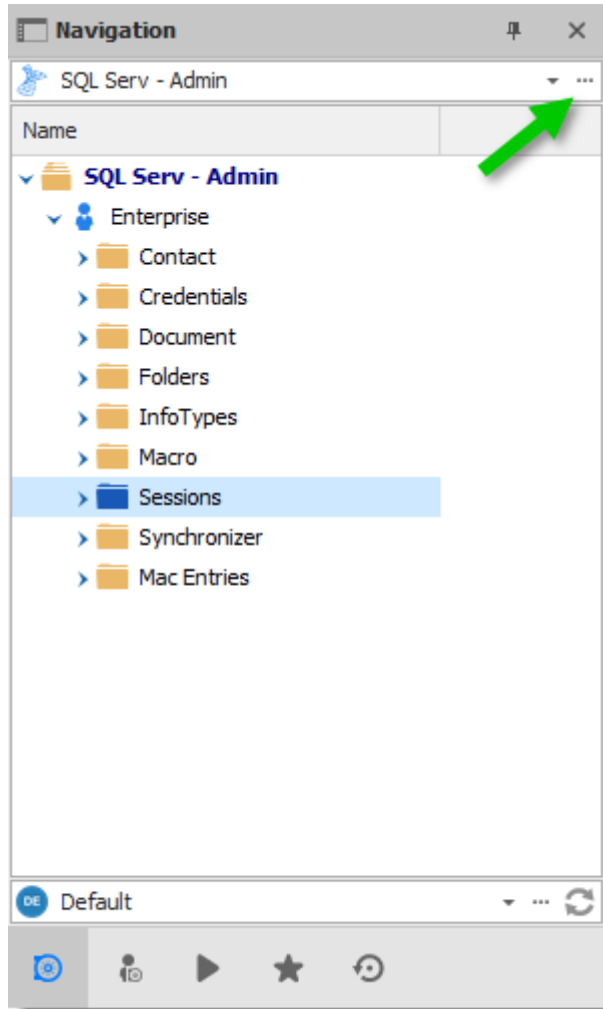
MySQL: [MySQL Copying databases](#)

MariaDB: [MySQLDump](#)

The migration is simply an export of your original data source followed by an import in the new destination data source.

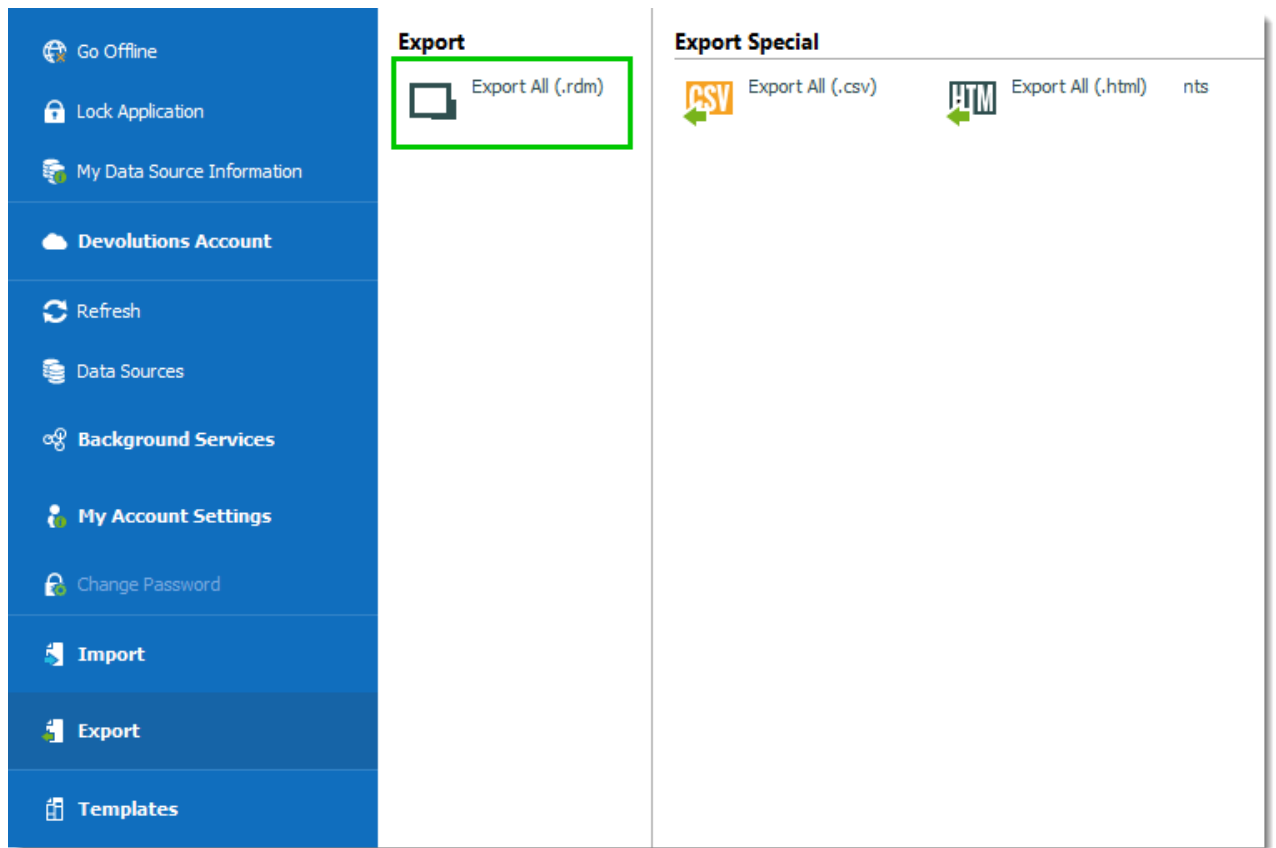
## EXPORT

1. Select your data source in the data source selection drop down list.



*Data Source drop down menu*

2. Select **File – Export – Export All (.rdm)**.



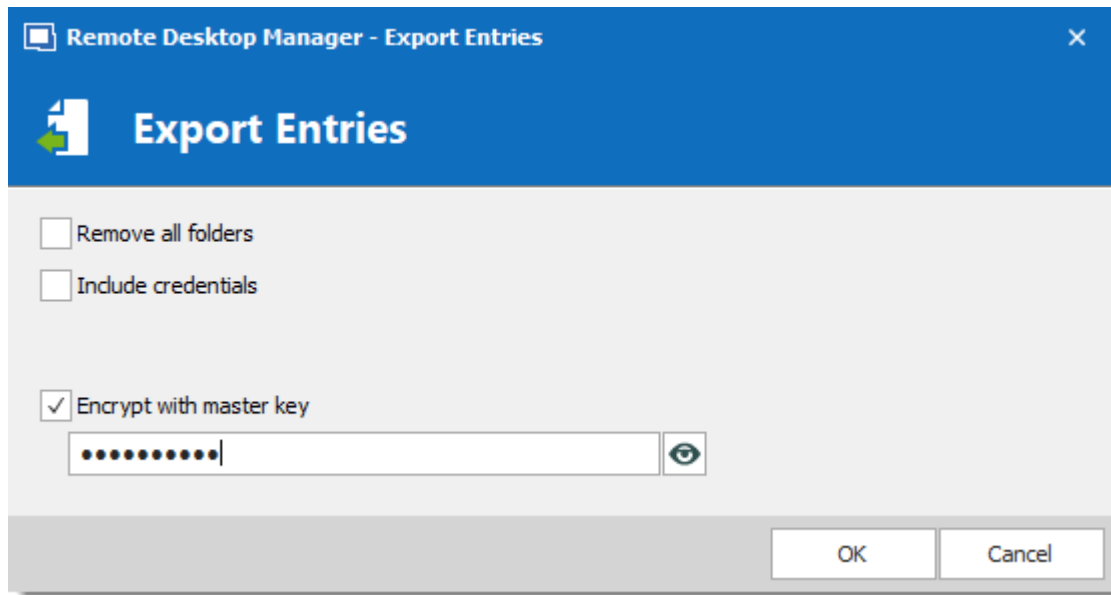
*Export menu*

3. Select your export entries options. You can choose to export your credentials and may also choose to use a Master Key as an added security layer. For a typical migration you would check those options.



Ensure that you do not forget the Master Key as you will not be able to decrypt the data without it.



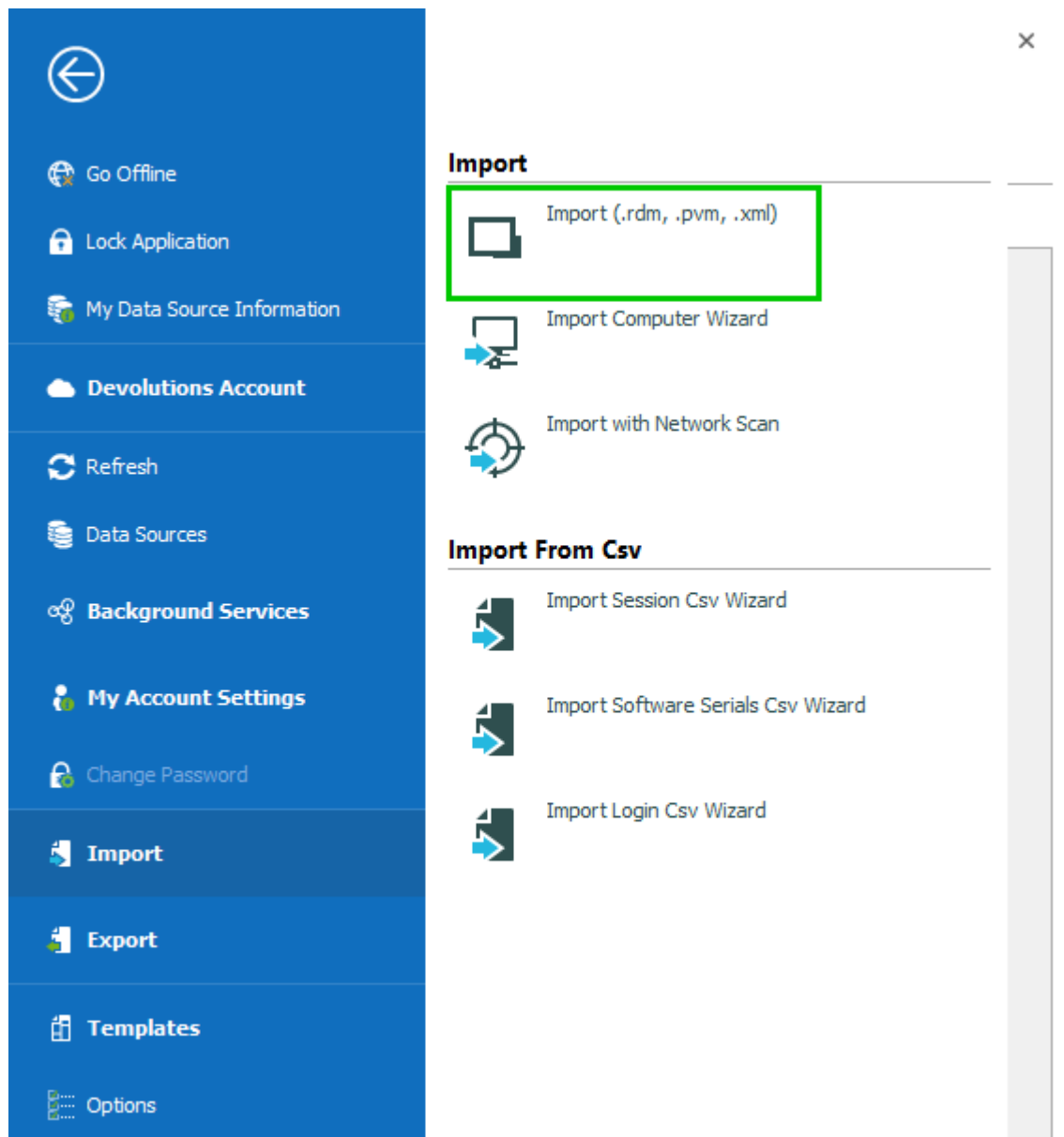


*Export Entries Option*

4. Save the file with the name and location of your choice.

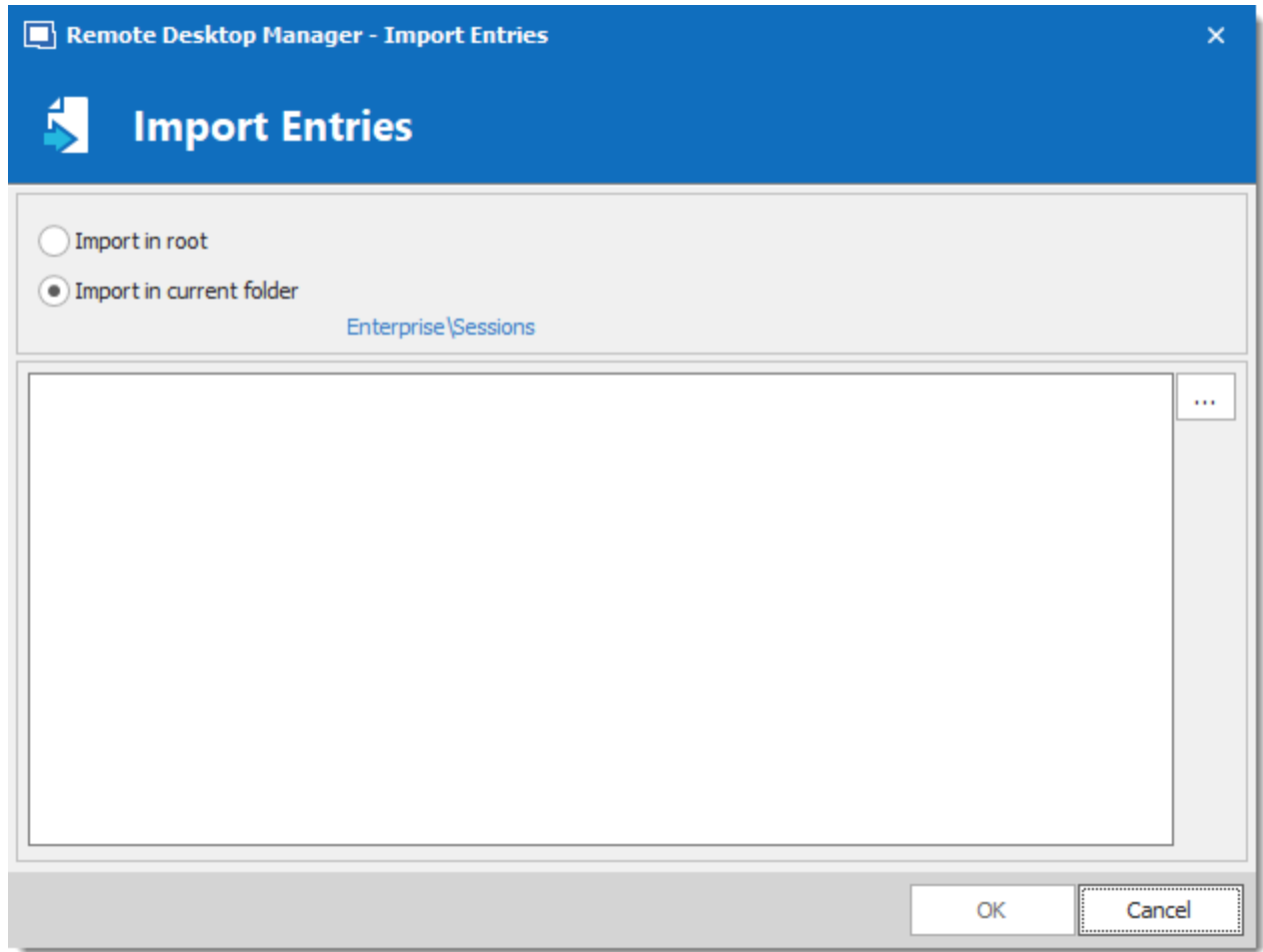
## IMPORT

1. Select the destination data source in the data source selection drop down list.
2. Select **File – Import – Import (\*.rdm, \*.pvm, \*.xml)**.



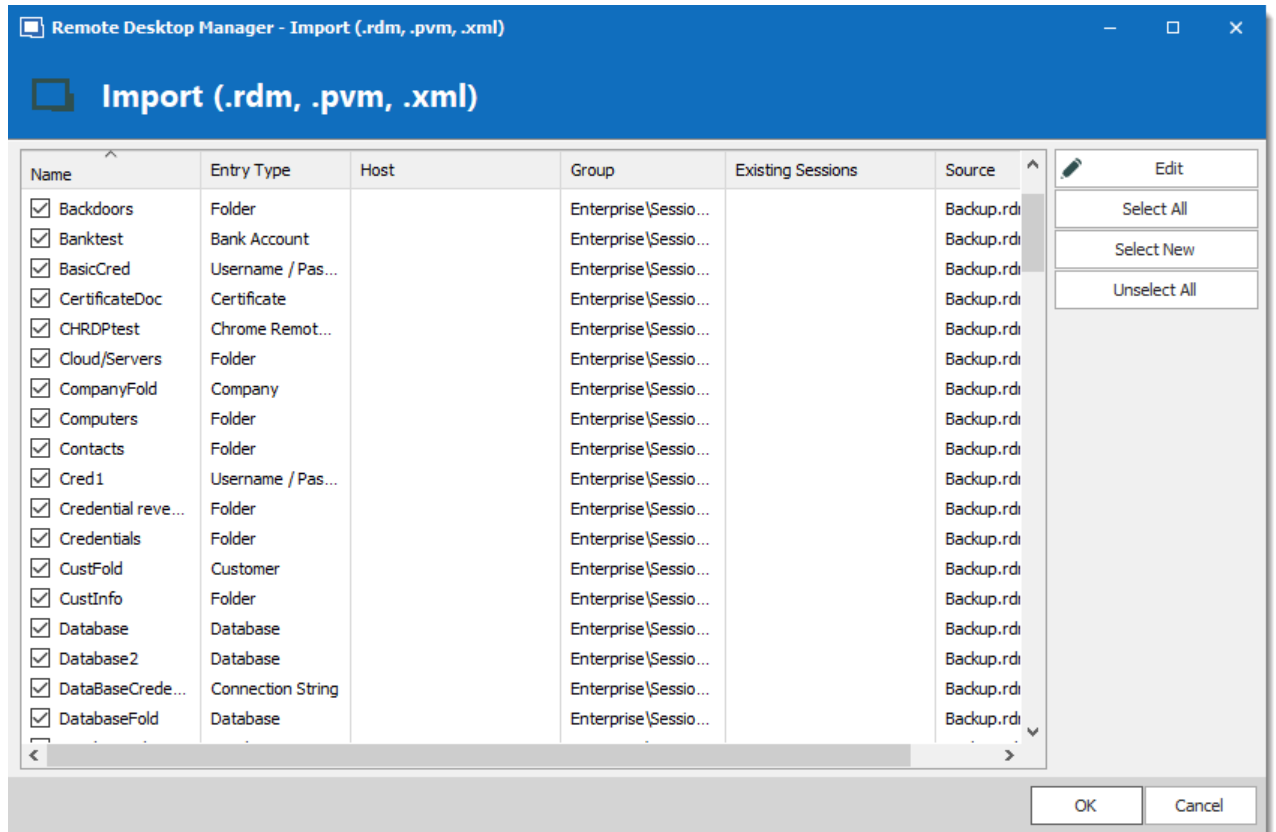
*Import menu*

3. In the **Import Entries** dialog use the ellipsis button to browse for the data file exported in the previous section.

*Import Entries*

OPTION	DESCRIPTION
<b>Import in root</b>	Import your entries in the root of your data source, meaning it will keep the exact same structure (group, folder, credentials) as the one you've exported. It is the suggested method of import.
<b>Import in current folder</b>	Import all your entries under the selected folder of the data source.

4. In the next dialog you'll be presented with a list of all entries that are in the data file. You can select which entry you wish to import or you can **Select All** to import all of your entries. Simply press **OK** to complete the process

*Import Entries - Session selection*

## 12.7.6 Data Report

### DESCRIPTION

The Data Report session type can be use to empower any/all users to generate reports, without having to grant them access to the actual server.

### SETTINGS

#### GENERAL

The screenshot shows a configuration window titled 'Data Report Session' with three tabs: 'General', 'Parameters', and 'Query'. The 'General' tab is active. On the left, there is a blue icon representing a data table. The main area contains the following fields and controls:

- Source:** A dropdown menu with 'Default' selected.
- Data source:** A dropdown menu with 'Microsoft SQL Server' selected.
- Data provider:** A dropdown menu with '.NET Framework Data Provider for SQL Server' selected.
- Connection string:** A text input field with an eye icon and a three-dot menu icon to its right.
- Host:** A text input field.
- Username:** A text input field.
- Password:** A text input field with an eye icon to its right.
- Fit columns to content:** A checkbox that is currently unchecked.

*Data Report Session*

Create a Data Report entry and define the connection string by either:

- Specify the connection in the entry itself.
- Use a credential entry.
- Inherited from a parent.
- Prompt for credentials.

## PARAMETERS

Parameter description	Type	Default value
<a href="#">Parameter #1</a>	@Param1	Unused
<a href="#">Parameter #2</a>	@Param2	Unused
<a href="#">Parameter #3</a>	@Param3	Unused
<a href="#">Parameter #4</a>	@Param4	Unused
<a href="#">Parameter #5</a>	@Param5	Unused

Exemple of Query fields:

```
SELECT FieldA, FieldB From Table1 Where FieldC=@Param1 or FieldD=@Param2
```

☐ Show parameters in report header

Execute Query

*Data Report Session - Parameters Tab*

Specify the parameters by setting the name, type and default value of all parameters.

## QUERY

1

*Data Report Session - Query Tab*

Enter the query in the Query tab, which features a SQL syntax-highlighted text box with line numbers.



Ensure that your DBA sets the proper security groups, and that each specific user(s) has access to it.

### 12.7.7 Edit Hosts File

## DESCRIPTION

IT technicians, as well as web developers, often need to edit the Windows hosts file. This requires starting your favorite editor using elevated privileges (obviously only if UAC is active), browsing for the hosts file which is deep in the windows folder and enclosed in a hidden folder on top of that.

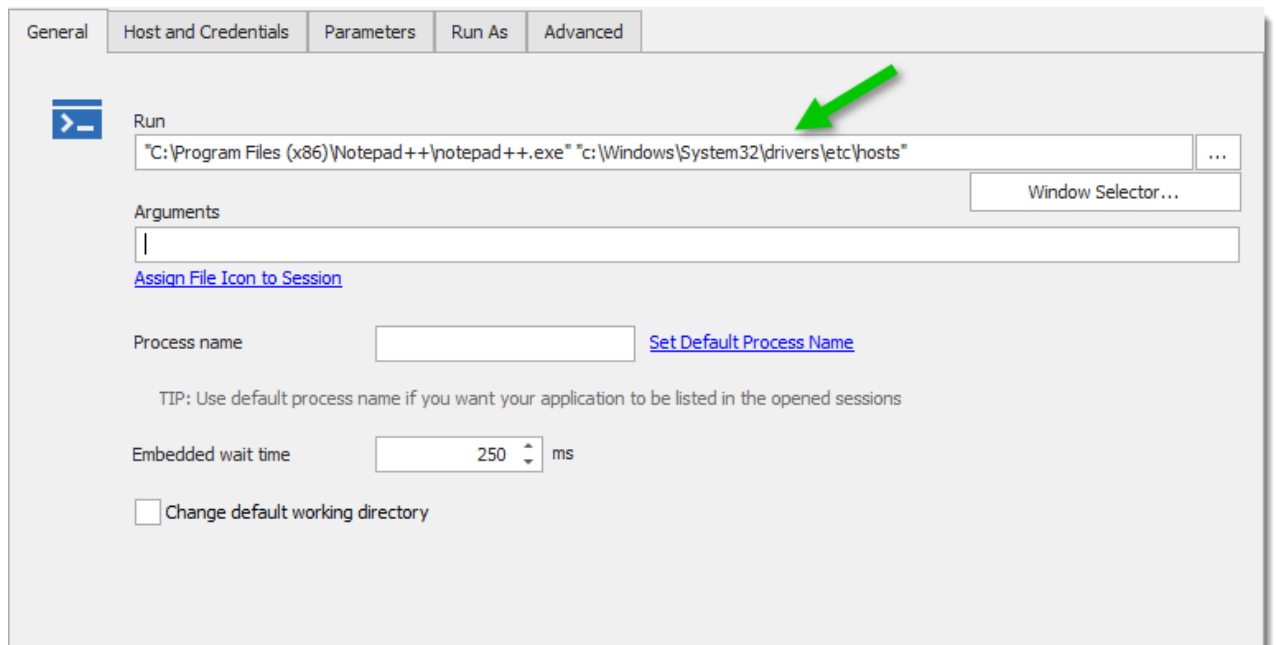
For your own machine you can create a shortcut to achieve this goal, but experience tells us that most people don't bother with it, ending up losing precious time when they must modify the hosts file.

What better tool than one that you use every day, which is already running in the notification area, to implement a solution with. If the machines you work on have the same setup, this will work for all of them.

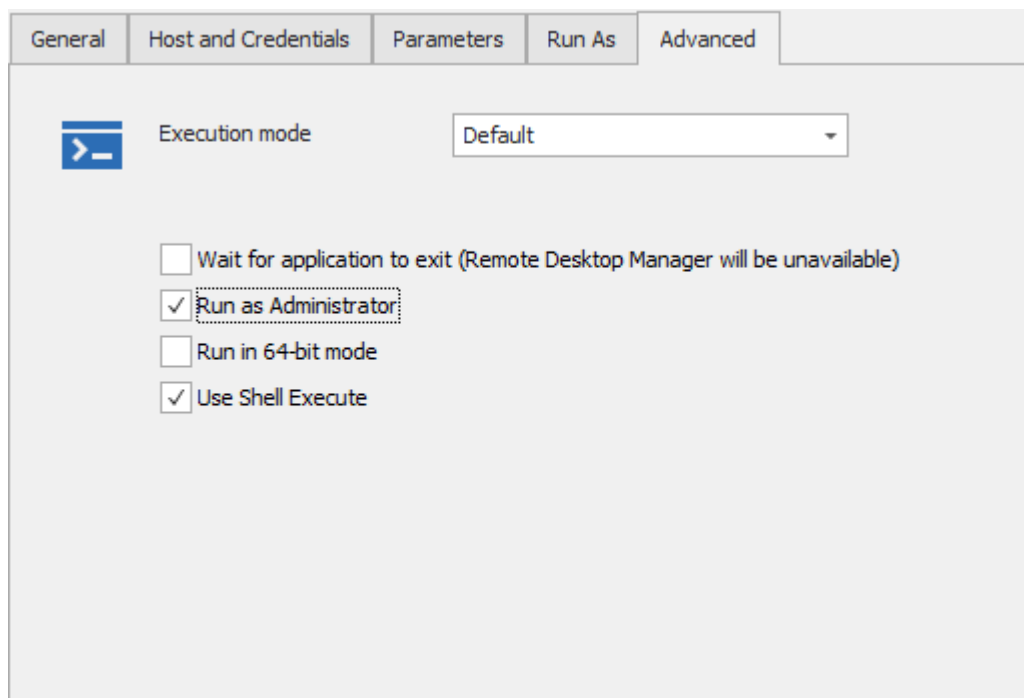
Simply create a session with the proper settings.

## STEPS

1. Create a new **Command Line (External Application)** session and enter a session name. In the **General** tab, click on the ellipsis button and select your editor of choice in the **Run** text box. Then, paste the following after the name of the program: "c:\Windows\System32\drivers\etc\hosts". Ensure a blank space separates the two and include the double quotes.

*Command Line (External Application) - General Tab*

2. In the **Advanced** tab, check the **Run as Administrator** option.

*Command Line (External Application) - Advanced Tab*





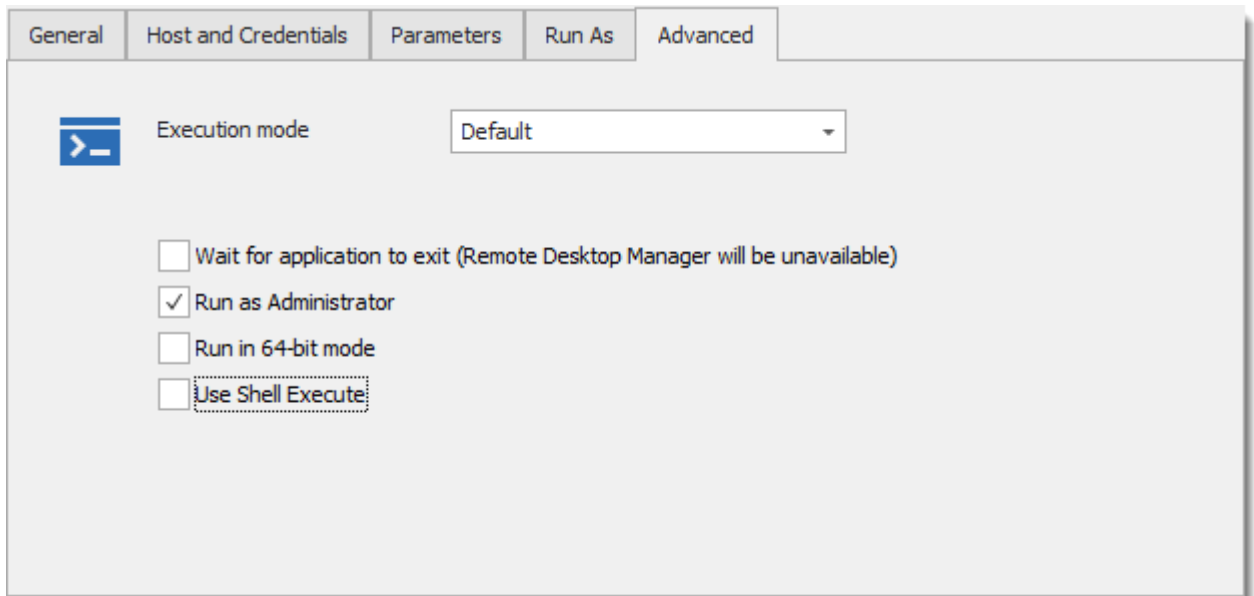
Close your editor before proceeding with those steps. If your editor is already running, it will not elevate the privileges. We have implemented an AutoHotKey script that closes the editor of choice, but being that it shuts off without saving pending changes, it is not a risk-free solution. It will all depend on your chosen editor's reaction to the WM\_QUIT message.

It is a simple and efficient solution. You can use this for any tool you use regularly. Paired with shared data source it makes for a powerful library of tools for your team.

## ALTERNATIVE IF YOU WANT TO USE THE PARAMETERS TAB

Some people wish to use the parameters tab because, upon launching, it will display a dialog where you can confirm the value of the parameters and even allows you to change them for whole new values.

1. Create a new Command Line session and in the **Advanced** tab, check the **Run as Administrator** and disable the **Use Shell Execute** option.



*Command Line (External Application) - Advanced Tab*

2. In the **General** tab, click on the ellipsis button and select your editor of choice in the **Run** text box. Then enter "{1}" after the name of the executable, keeping a space between the two values and including the quotes.

General Host and Credentials Parameters Run As Advanced

Run

"C:\Program Files (x86)\Notepad++\notepad++.exe"

Arguments

Window Selector...

[Assign File Icon to Session](#)

Process name

[Set Default Process Name](#)

TIP: Use default process name if you want your application to be listed in the opened sessions

Embedded wait time 250 ms

☐ Change default working directory

*Command Line (External Application) - General Tab*

3. In the **Parameters** tab, set Parameter # 1 type to **Text** and then enter the following in the Default Value: **c:\Windows\System32\drivers\etc\hosts**

General Host and Credentials Parameters Run As Advanced

Parameter name	#	Type	Default value
<a href="#">Parameter #1</a>	{1}	Text	c:\Windows\System32\drivers\etc\hosts
<a href="#">Parameter #2</a>	{2}	Unused	
<a href="#">Parameter #3</a>	{3}	Unused	
<a href="#">Parameter #4</a>	{4}	Unused	
<a href="#">Parameter #5</a>	{5}	Unused	

Example in Run field:

c:\My folder\mypgm.exe -u="{1}" -p="{2}"

[View Command](#)

*Command Line (External Application) - Parameters Tab*

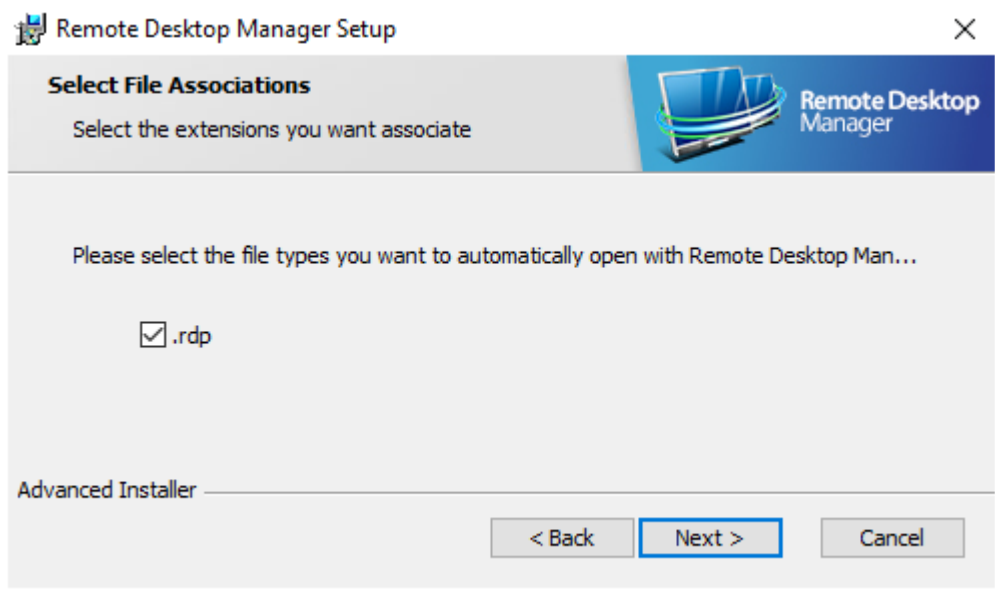
This is helpful when mostly using the tool with a certain file, but occasionally need to edit another file. You could have separate entry for each file you commonly edit, but this shows how flexible Remote Desktop Manager can be.

## 12.7.8 Handling RDP Connections

### DESCRIPTION

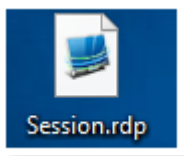
Remote Desktop Manager can manage **\*.rdp** file to open and connect sessions immediately. Even if your application is closed, you can open a **\*.rdp** file. The application will open and start your connection.

### SETTINGS



*Remote Desktop Manager installation wizard*

When deploying an installation of Remote Desktop Manager, you will be able to associate your **\*.rdp** file to the application, allowing you to start an **\*.rdp** file from your computer to be opened inside Remote Desktop Manager.



*.rdp File*

If an **\*.rdp** file is launched, the session will start in Remote Desktop Manager. You can then create a new entry with this session by simply clicking on **save session as** from the edit section of the Actions tab.

## 12.7.9 HTML Export Using Symmetric Encryption

### OVERVIEW

As we all know, email isn't secure. But it's convenient, fast and free – and so many of us ignore the security risks.

Yet when you step back and think about it, ask yourself: Would you ever think of sending cash through the regular mail? Even sending it through a courier is risky! But if you send sensitive information via email, that's pretty much what you're doing.

Fortunately, there's a solution!

We've developed a feature that allows for symmetric encryption of sensitive information, so that it can then be securely sent via email (or any other protocol) while keeping the data safe.

This feature can also be used to save/export/backup sensitive information to disk.

### HOW IT WORKS

The feature is simple and easy to use:

- Select one or multiple data entries.
- Right-click **Import/Export – Export Data Entry – Export Data Entry (.html)**.
- When prompted, enter a password.
- Save the file to disk.

And that's it! Your document is ready to be securely sent via email or any other protocol.

### EXPORT MULTIPLE ENTRIES

And what if you're exporting multiple data entries? To prevent prying eyes from seeing more than they should, each secured string must be individually decrypted. Someone is walking by your desk, simply hit F5 or close the file, and the information is secure again.

### A WORD ABOUT 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. Here's a snapshot of the encrypted values:

```
<tr>...</tr>
<tr>
  <td class="label EmailPOP3Password">Password</td>
  <td class="value EmailPOP3Password" colspan="3">
    <span id="a2da6626-a620-49da-8aaf-85495af294cb" data="U2FsdGVkX18jCcpyAqqnT1gi1+Y03TvMM6kex1tpFUA=">
      <a class="encrypted" onclick="javascript:decryptText('a2da6626-a620-49da-8aaf-85495af294cb')">*****
    </span>
  </td>
```

*Html File Content*

## SAFE & SMART VIRTUAL BACKUP

In addition, HTML Export using symmetric encryption is a great way to securely – and virtually – 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. The possibilities are endless, and it's just another way that we're working hard to help you centralize it, secure it and simplify IT!

## PRINTING

Sorry, decryption of the printed document isn't supported. We have yet to figure out a way to do this. If someone ever does please let us know.

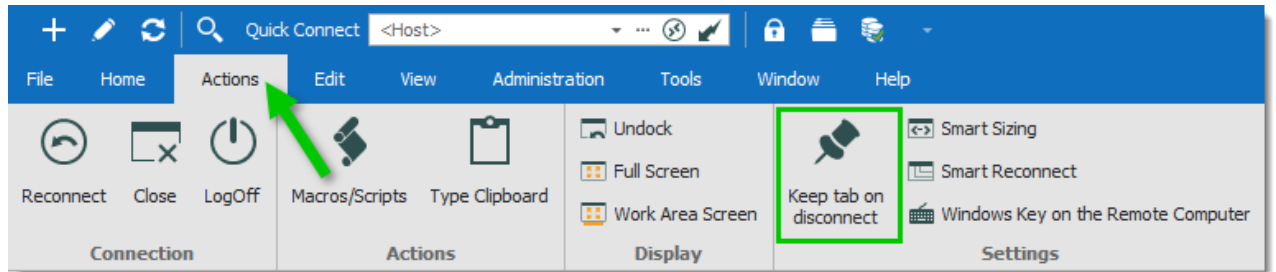
### 12.7.10 Keep Tabs Opened

## DESCRIPTION

Remote Desktop Manager offers you the possibility of keeping a tab open even when disconnected, thus allowing you to restart a remote device or simply keep your work area set up to quickly resume after a work interruption.

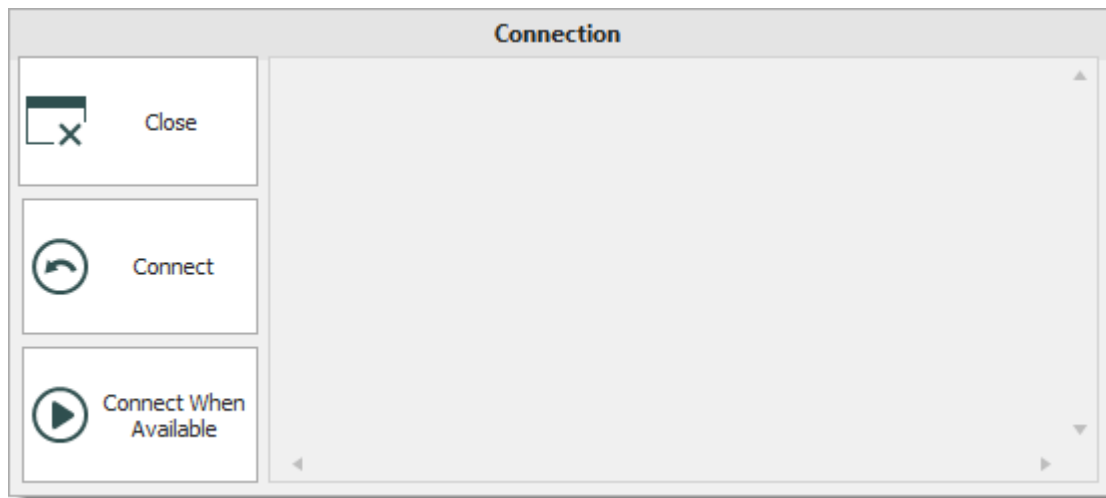
## WORKFLOW

Your session must be running in embedded mode. Once your session is open, you'll notice the **Keep tab on disconnect** option in your **Action** ribbon.



*Actions Ribbon*

Enable the **Keep tab on disconnect** to be able to perform a logoff or restart while keeping the tab present. A panel will replace the content of the session.

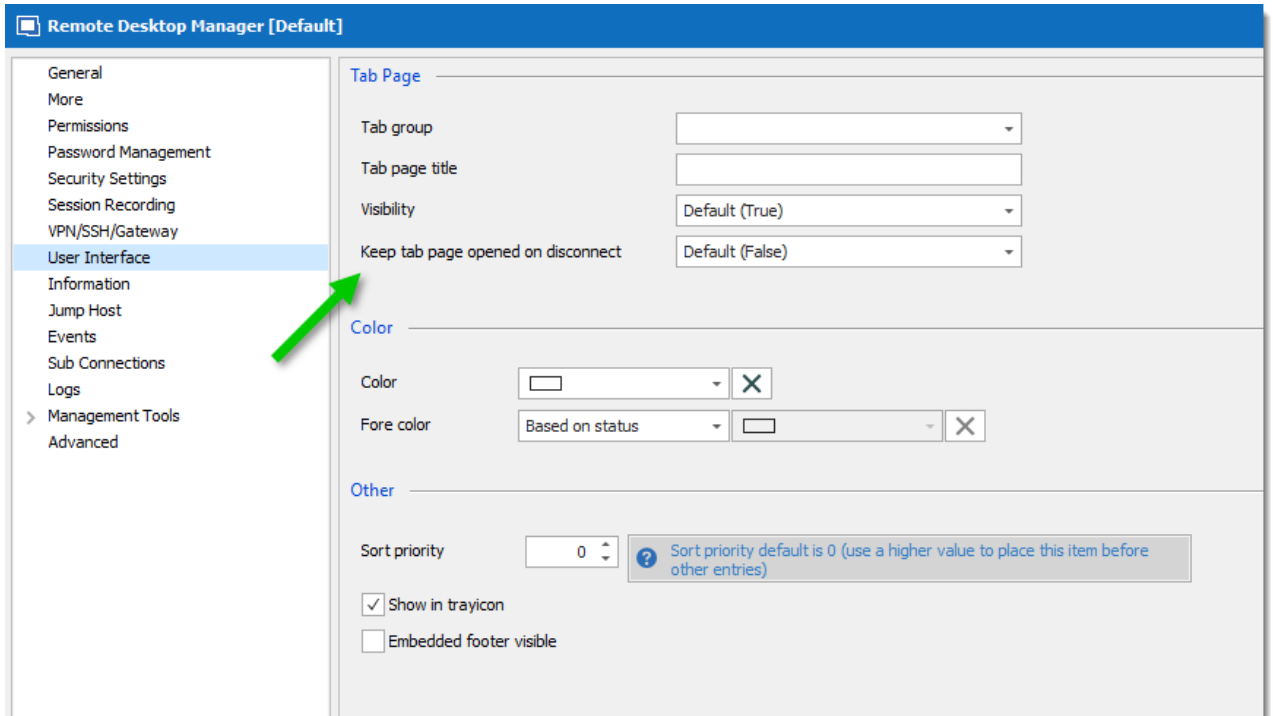


*Connection panel*

This panel offers three actions:

- **Close:** You changed your mind and want to close the tab
- **Connect:** Connect the session
- **Connect When Available:** Pings the host until it becomes available, then connects the session.

If you wish to have the option enabled by default, edit your session and in the User Interface tab enabled the **Keep tab page opened on disconnect** option.



RDP session - User Interface

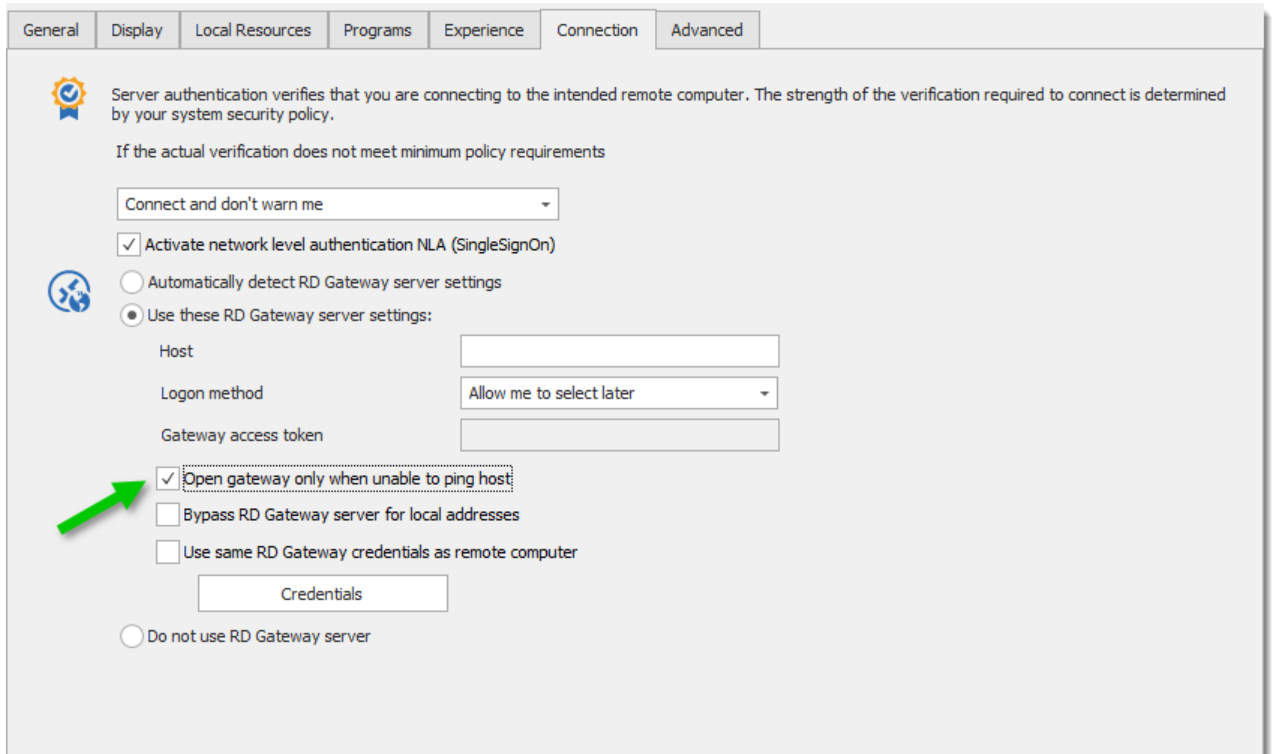
### 12.7.11 Open RD Gateway Only when Unable to Ping Host

## DESCRIPTION


Use your RD Gateway only when your host is unreachable.

## SETTINGS

In your Microsoft Remote Desktop (RDP) entry, under Connection, you can enable **Open gateway only when unable to ping host**, connectivity with the remote host will be tested to see if its reachable, if not, the RD Gateway will be used.




General Display Local Resources Programs Experience **Connection** Advanced

 Server authentication verifies that you are connecting to the intended remote computer. The strength of the verification required to connect is determined by your system security policy.

If the actual verification does not meet minimum policy requirements

Connect and don't warn me

☒ Activate network level authentication NLA (SingleSignOn)

 ☐ Automatically detect RD Gateway server settings

☒ Use these RD Gateway server settings:

Host

Logon method: Allow me to select later

Gateway access token

☒ Open gateway only when unable to ping host

☐ Bypass RD Gateway server for local addresses

☐ Use same RD Gateway credentials as remote computer

Credentials

☐ Do not use RD Gateway server

Connection Tab

## 12.7.12 Passcode Prompt When Opening an Entry

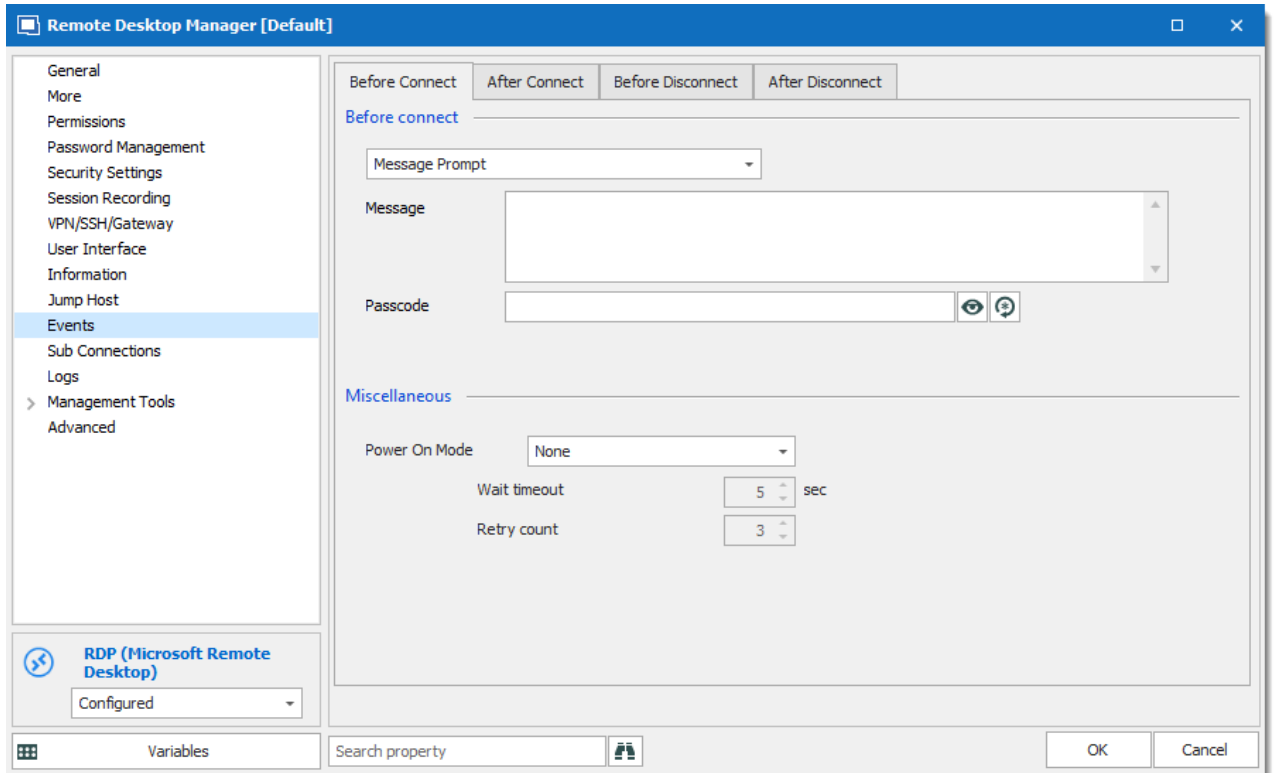
### DESCRIPTION

Sometimes you want to ensure that your users are really opening the right session.

### WORKFLOW

In the Events tab, in the Before Connection section, when you select **Message Prompt**, you will notice a Passcode field.

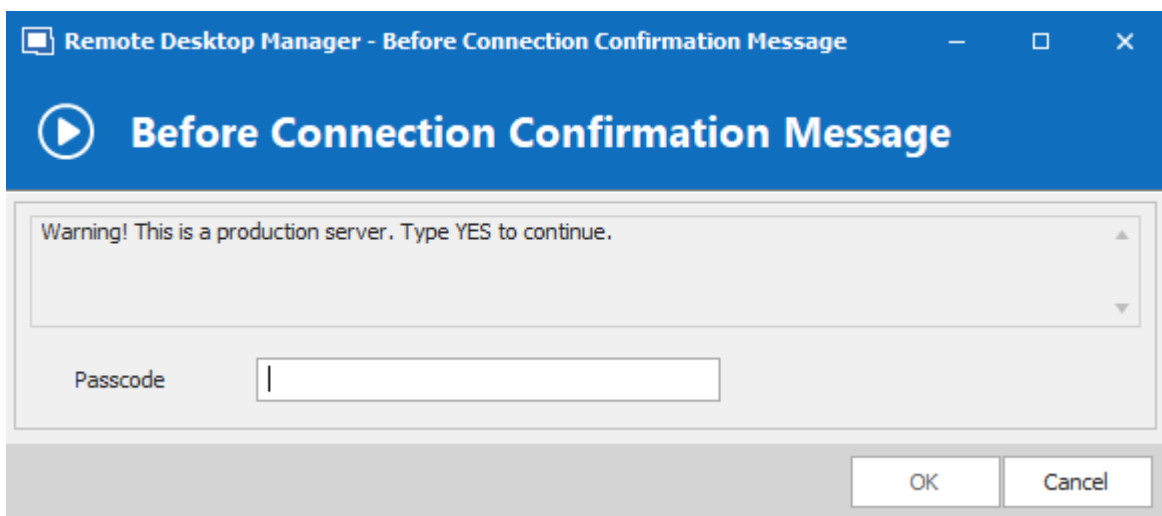




Events Tab

There is a field to enter a **Message** and another one for a **Passcode**. The idea is not to add another password to launch the session, but rather to act as a safeguard. For example, you could set the message to “Warning! This is a production server. Type YES to continue.” and set the Passcode to YES.

This allows you to give just a little jolt when you attempt to launch the session!



Passcode In Action

## 12.7.13 RDP Session Time Limits

### DESCRIPTION

When you close your RDP sessions, you may inadvertently (or willfully) leave your session running on the remote host. Depending on the programs you have left running, this can consume excessive resources and can be even interpreted as a security risk.

Windows allows you to control how **Remote Desktop Services** handle sessions through Group Policies. This can be administered on the host computer itself, or be pushed at the domain level for multiple hosts.

What follows is the procedure to perform on a single host computer.

### PROCEDURE

1. Launch **Edit group policy**. (Press the windows key, and type "edit group policy", for Windows 8 it is in the **Settings** category).

2. Browse to:

Computer Configuration  
    Administrative Templates  
        Windows Components  
            Remote Desktop Services  
                Remote Desktop Session Host  
                    Session Time limits

The settings are described as follows (when you alter the setting using the Group Policy Editor, you will see a detailed description).

<b>Set time limit for disconnected sessions</b>	This policy setting allows you to configure a time limit for disconnected Remote Desktop Services sessions. By default, Remote Desktop Services allows users to disconnect from a Remote Desktop Services session without logging off and ending the session.
<b>Set time limit for active but idle Remote Desktop Services sessions</b>	This policy setting allows you to specify the maximum amount of time that an active Remote Desktop Services

	session can be idle (without user input) before it is automatically disconnected.
<b>Set time limit for active Remote Desktop Services sessions</b>	This policy setting allows you to specify the maximum amount of time that a Remote Desktop Services session can be active before it is automatically disconnected.
<b>End session when time limits are reached</b>	This policy setting specifies whether to end a Remote Desktop Services session that has timed out instead of disconnecting it.

3. Double click on the setting (or right-click, **Edit**), an edition form will appear.

Set time limit for disconnected sessions

Set time limit for disconnected sessions

Previous Setting Next Setting

☒ Not Configured Comment:

☐ Enabled

☐ Disabled

Supported on: At least Windows Server 2003 operating systems or Windows XP Professional

Options: End a disconnected session

Help: This policy setting allows you to configure a time limit for disconnected Remote Desktop Services sessions.

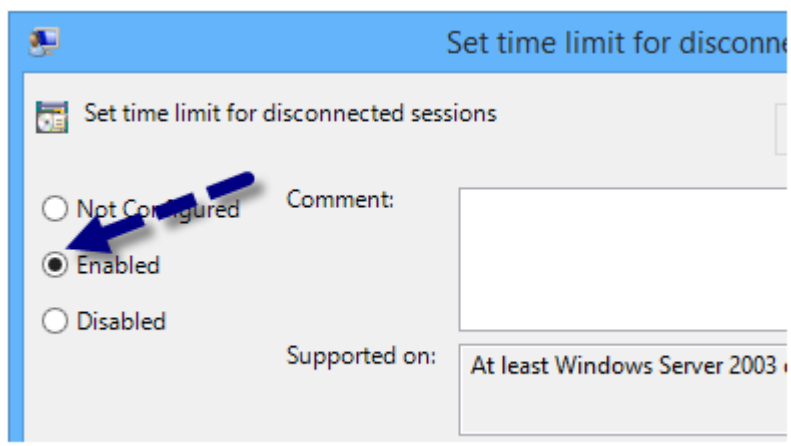
You can use this policy setting to specify the maximum amount of time that a disconnected session remains active on the server. By default, Remote Desktop Services allows users to disconnect from a Remote Desktop Services session without logging off and ending the session.

When a session is in a disconnected state, running programs are kept active even though the user is no longer actively connected. By default, these disconnected sessions are maintained for an unlimited time on the server.

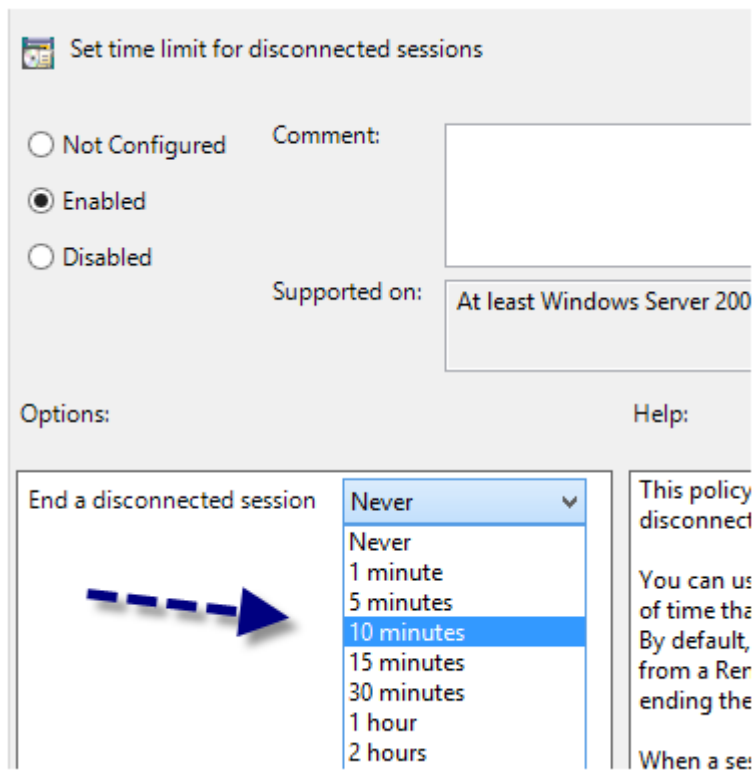
If you enable this policy setting, disconnected sessions are deleted from the server after the specified amount of time. To enforce the default behavior that disconnected sessions are maintained for an unlimited time, select Never. If you have a console session, disconnected session time limits do not apply.

OK Cancel Apply

4. Select **Enabled**, this will enable the control in the lower section.



5. Choose your desired value from the list.



6. Press Apply.

7. Repeat for other settings as desired. Note that for true/false settings there is no control in the Options area. Just enabling the policy will activate the setting.

From then on, all future sessions established on that host will follow these policy settings.

You may want to explore all the policies below Remote Desktop Services, you may find hidden gems that would help your organization.

## 12.7.14 Remote Install with PSEXec

### DESCRIPTION

When you need to perform a remote installation, you have multiple options. Such as a domain policy, a logon script or PSEXec.

Depending on the way the security is configured on the remote computer, you may run into issues where even an administrator cannot install an application properly. For these cases, you need to run PSEXec in the context of the system account.

First of all, you will need to install the Sysinternals tools from Microsoft, because you will need the help of PSEXec.exe in the execution of this script. (<https://technet.microsoft.com/en-us/sysinternals/bb842062>)

Then, download the **\*.msi** or the **\*.exe** of the application you wish to install and save the file on a shared drive that is accessible from the remote computer.



Options exist to copy files remotely, please refer to PSEXec documentation for further details.

### SETTINGS

1. Create a **Macros/Scripts/Tools** entry, use the **PSEXec** type. In the Command line section, add the following (long) line:

```
C:\Tools\Sysinternals\psexec.exe \\$HOST$ -i -u $TOOL_DOMAIN\$ $TOOL_USERNAME$ -p $TOOL_PASSWORD$
k "msiexec /i \\SRV-DEPLOY\msi\Setup.RemoteDesktopManager.10.9.0.0.msi /quiet /passive /n
```



The full path to the **\*.msi** must be entered. A shared network is recommended in this case.

A few notes on that command line:

1. Replace the path to launch PSEXec.

2. Add the appropriate credentials in the **Tools** section of your session, if left blank it will use your current Windows session credentials.
3. Indicate the appropriate server shared to get the **\*.msi** or **\*.exe**.
4. When you are ready to deploy your application on the remote computer, you just need to select the appropriate session in the Navigation Pane and launch the **Macros/Scripts/Tools** from the Dashboard. The **Macros/Scripts/Tools** entry can also be launch via the RDM Agent.

## USAGE

The Macros/Scripts/Tools type are always run in the context of a session. In fact they use the information in the session to identify what host to run the tool against, that is why we used the \$HOST\$ variable.

For this reason, the first step is to select a session, any type of session will do (RDP, SSH, etc). After selecting the session, the dashboard will display the **Macros/Scripts/Tools**. Simply clicking on the tool will therefore launch it against the host linked to the currently selected session. You can select hosts and install in sequence.

### 12.7.15 Run as Another User

## DESCRIPTION

There are many different type of credentials and they are used by a multitude of users. Be it a mobile warrior, a sysadmin that follows best practices and doesn't log on to his computer using his domain admin account or even a safety conscious parent that creates limited accounts for the kids on the family computer. This requires the capability to start an application under a different set of credentials while we are already logged on using our main credentials.

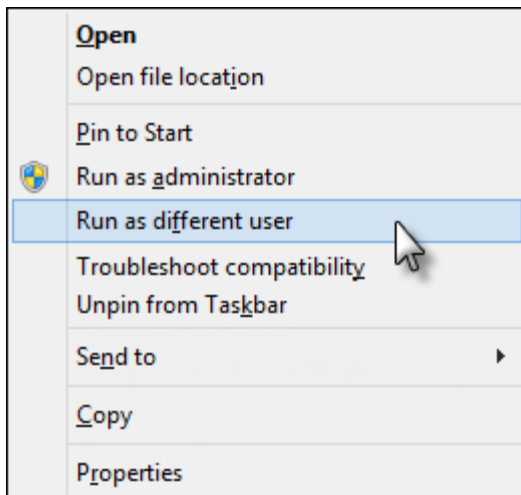
The problem is solved by using the Windows **Run As** command.



The **Run As** command requires that the **Secondary Logon** service be running.

## SETTINGS

In Windows you can manually start any process as a different user using **SHIFT + right-click** to get the context menu.



*SHIFT + right-click popup menu*

The **Run As** command has many parameters to change its behaviour, we won't cover them all here, but if you have an advanced scenario we suggest you consult the Windows help.

## OPTIONS

You have two options when it comes to **Run As**:

### BUILT-IN RUN AS

In Remote Desktop Manager, some sessions/tools types support the **Run As** functionality. For a complete list and configuration information see the [Built-In Run As](#) help topic.

### MANUAL RUN AS

Your session type is not supported and needs help to manually configure Run As? See the [Manual Run As](#) help topic.

#### 12.7.15.1 Built-in RunAs

## DESCRIPTION



This article describes the built-in method of using **Run As**. For session types that don't yet support the built-in method you can follow the manual steps outlined [here](#).

## SETTINGS

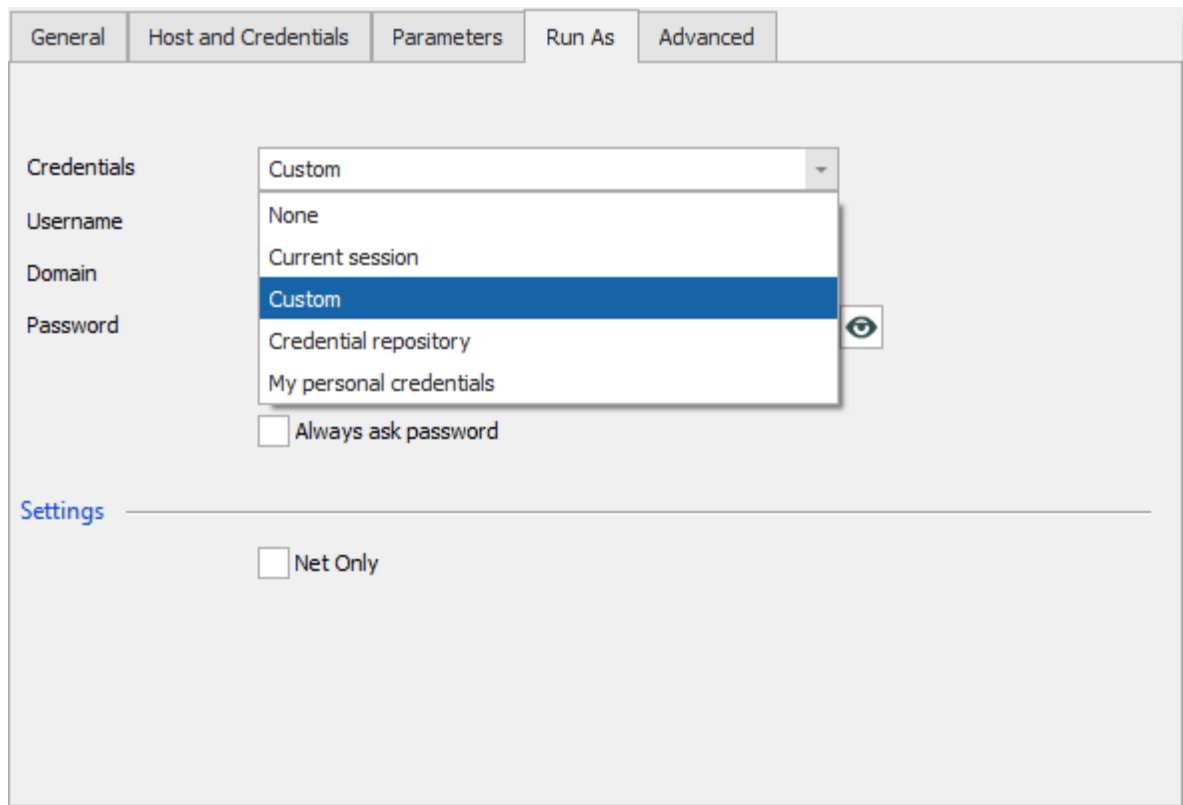


## SUPPORTED TYPES

The following types currently support **Run As**.

OPTION	DESCRIPTION
<b>Session</b>	<ul style="list-style-type: none"><li>• Command Line</li><li>• PowerShell</li></ul>
<b>Macros/Scripts/Tools</b>	<ul style="list-style-type: none"><li>• Command Line</li><li>• PowerShell Local</li><li>• PowerShell Remote</li><li>• PSEXec</li></ul>
<b>Session Add-on</b>	<ul style="list-style-type: none"><li>• SQL Server Management Studio</li></ul>

## SESSION



*Command Line (External Application) - Run As Tab*

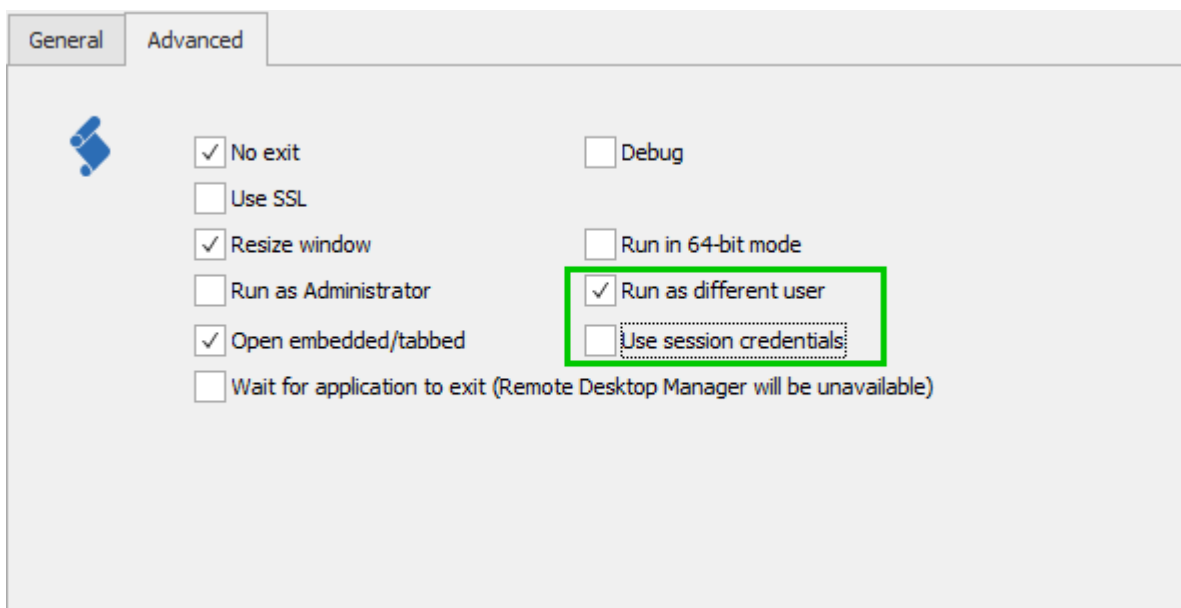
Sessions that support Run As will have a Run As tab where you specify which credentials to use when starting with Run As.

OPTION	DESCRIPTION
<b>None</b>	No Run As is performed.
<b>Current session</b>	Use the same credentials as defined in the session.
<b>Custom credentials</b>	Use specified custom credentials.
<b>Credential repository</b>	Use a link credential entry.

OPTION	DESCRIPTION
Use my personal credentials	Use a link private credential entry.

## MACROS/SCRIPTS/TOOLS

With tools session types you only need to specify **Run as different user** in **Advanced** tab. At execution time the credentials will be resolved and used to start the Windows Credentials unless you select Use session credentials, in which case it will use those active for the session.

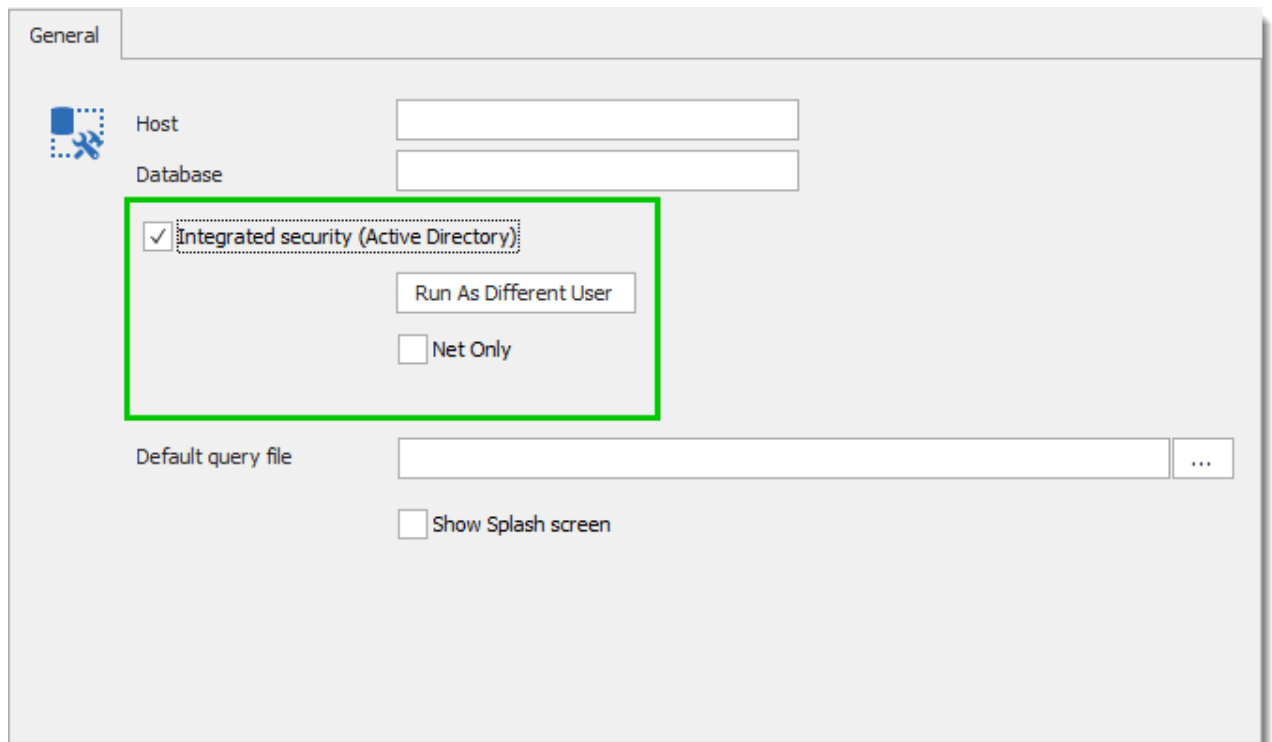


*PowerShell (Remote) - Advanced Tab*

With tools session types you only need to specify **Run as different user**. At execution time the credentials will be resolved and used to start the Run As process.

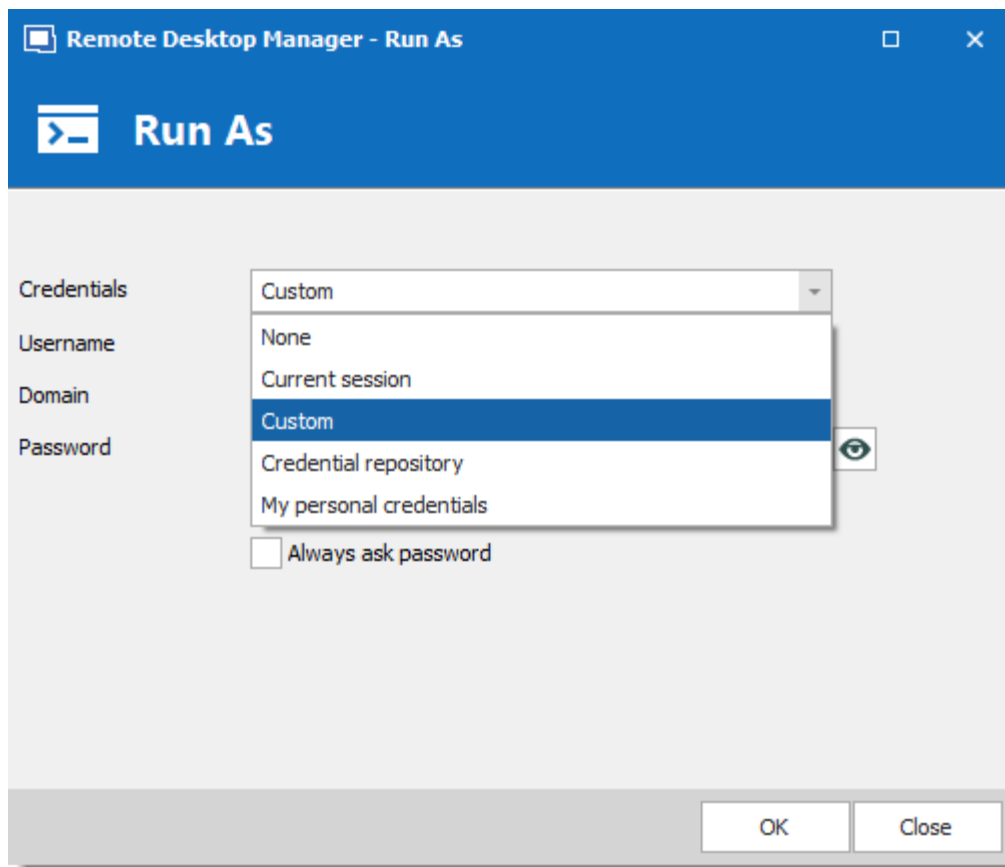
## SESSION ADD-ON

**SQL Server Management Studio** supports Run As. Configure it like you would configure a normal session.



*SQL Server Management Studio - General*

Click on **Run as different user** to modify the **Run As** settings.



*Run As Different User*

## NOTES

**Run as Different User** and **Run As Administrator** are mutually exclusive.

**Run as Different User** doesn't allow for **Shell Execute**.

### EXAMPLE: COMMAND LINE SESSION WITH RUN AS DIFFERENT USER ON THE SAME WORKGROUP/DOMAIN

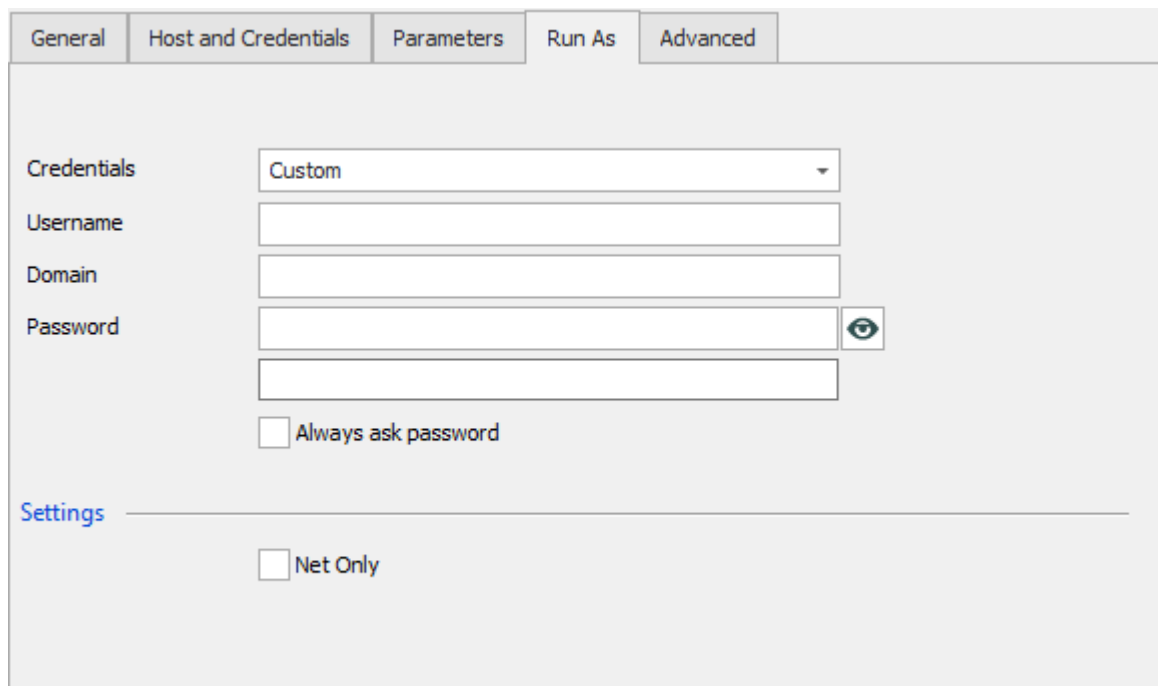
1. Create a new Command Line session.
2. Set the command to **CMD**.



The screenshot shows the 'General' tab of a dialog box with five tabs: 'General', 'Host and Credentials', 'Parameters', 'Run As', and 'Advanced'. The 'General' tab is active. It features a blue icon with a right arrow and a minus sign. Below the icon, there is a 'Run' label and a text input field containing 'cmd'. Underneath, there is an 'Arguments' label and an empty text input field. At the bottom, there is a blue hyperlink that reads 'Assign File Icon to Session'.

*Command Line (External Application) - General Tab*

3. Specify the **Run As** credentials.

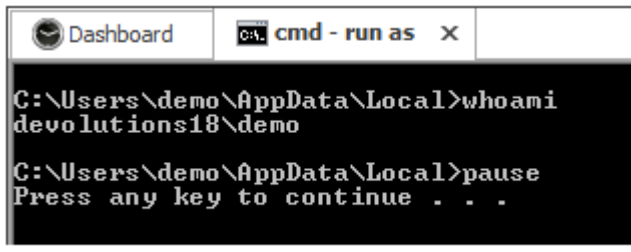


The screenshot shows the 'Run As' tab of the same dialog box. It has five tabs: 'General', 'Host and Credentials', 'Parameters', 'Run As', and 'Advanced'. The 'Run As' tab is active. It contains a 'Credentials' section with a dropdown menu set to 'Custom'. Below this are three text input fields for 'Username', 'Domain', and 'Password'. The 'Password' field has a small eye icon to its right. Below the 'Password' field is a checkbox labeled 'Always ask password'. At the bottom, there is a section labeled 'Settings' with a checkbox labeled 'Net Only'.

*Command Line (External Application) - Run As Tab*

4. Save your session.

5. Run your Command Line session.



### 12.7.15.2 Manual RunAs

## DESCRIPTION



This article describes the manual method of using RunAs. Some types support built-in RunAs details are available [here](#).

## SETTINGS

## SCENARIOS

There are two major scenarios when using RunAs: the authentication server is accessible directly from your machine or you need delayed authentication.

- **AUTHENTICATION SERVER IS LOCALLY ACCESSIBLE**

This scenario is for when you are already authenticated on a domain/workgroup and you need to switch to another account of the same domain/workgroup.

- **DELAYED AUTHENTICATION**

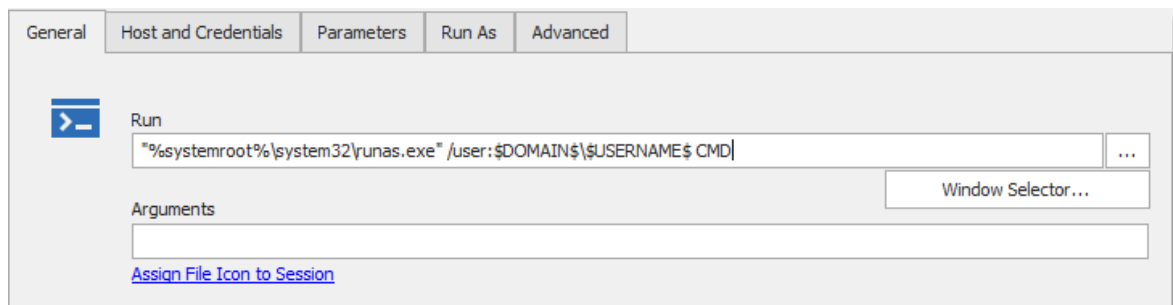
This scenario is for when it is impossible to log on your machine using the other set of credentials. For example you need to connect to a client's domain using your laptop that is on your company's domain. This will require using the **/NETONLY** parameter of RunAs.

## EXAMPLES

The RunAs command is invoked from an entry of the "Command line" type. Create the entry either by pressing the Insert key or by using the menus. Select the "Command line" type and enter a name for it.

### EXAMPLE 1: RUNNING A COMMAND PROMPT AS ANOTHER USER OF THE SAME WORKGROUP/DOMAIN

1. You can use the ellipsis button to browse for the **runas.exe** command, but if you are in a shared data source and the session is used on various operating systems, it's better to type in **"%systemroot%\system32\runas.exe"** because it will work on all of them.
2. Append **/user:\$DOMAIN\$\\$USERNAME\$**, keeping it outside of the quotes. Note the use of two variables that will pull the appropriate value from other fields of the same session. For more information please consult the Variables topic.
3. Append the name of the executable you want to run. Enclose it in quotes if the full path contains spaces. In our case we can simply add **CMD**,



Command Line (External Application) - General Tab

4. Specify your credentials in the **Host and Credential** tab. Note that when you are not part of a domain, you should enter the computer name in the domain field.



General Host and Credentials Parameters Run As Advanced

Host

Username david

Domain windjammer

Password

Perfect

Use the variables in your parameters:

- \$USERNAME\$
- \$DOMAIN\$
- \$HOST\$
- \$PASSWORD\$

5. In the **Events** tab you must define a typing macro

5.1. Set the Initial Delay to the lowest value that will allow the initial prompt to appear. On most systems 1 second is sufficient

5.2. In the Typing macro field, enter the following: **\$PASSWORD\${ENTER}**. For more information please consult Auto Typing Macro.

After connect - Macro

☒ Execute automatically Initial wait 1 sec

Default

Typing macro \$PASSWORD\${ENTER}

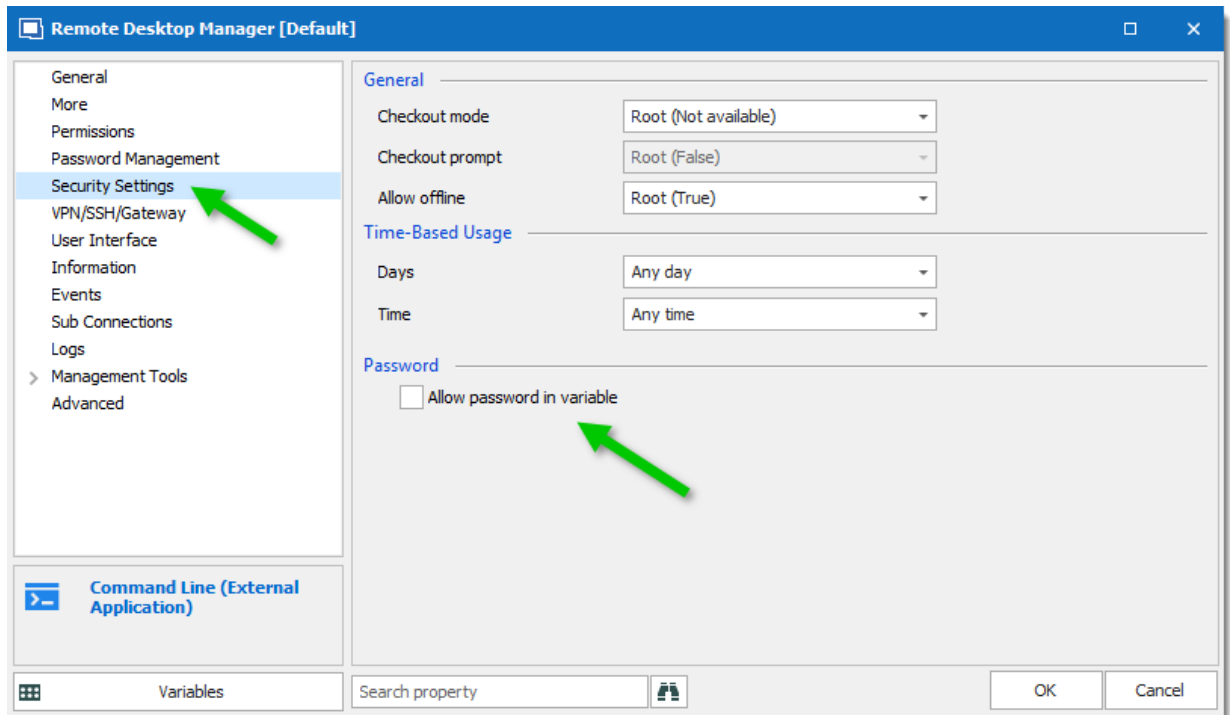
Macro password

Delay time {Delay} 300 ms

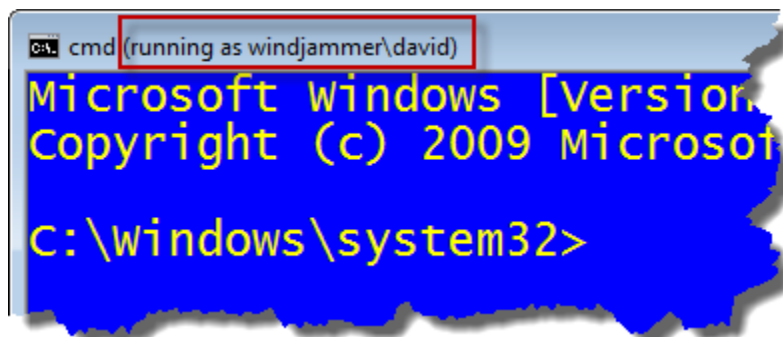
Command 20 ms

*Events - After Connect Tab*

6. In the **Security Settings** tab, you must check **"Allow password in variable"**.



When you run your session, a command prompt window appears requesting the password for the user. The Typing Macro will fill it in after the 1 second delay. After this, the command window that is running under the different credentials appears. Note that the title indicates the other identity.



## EXAMPLE 2: RUNNING SQL SERVER MANAGEMENT STUDIO AS A USER OF A DIFFERENT DOMAIN/WORKGROUP FOR USING WINDOWS AUTHENTICATION

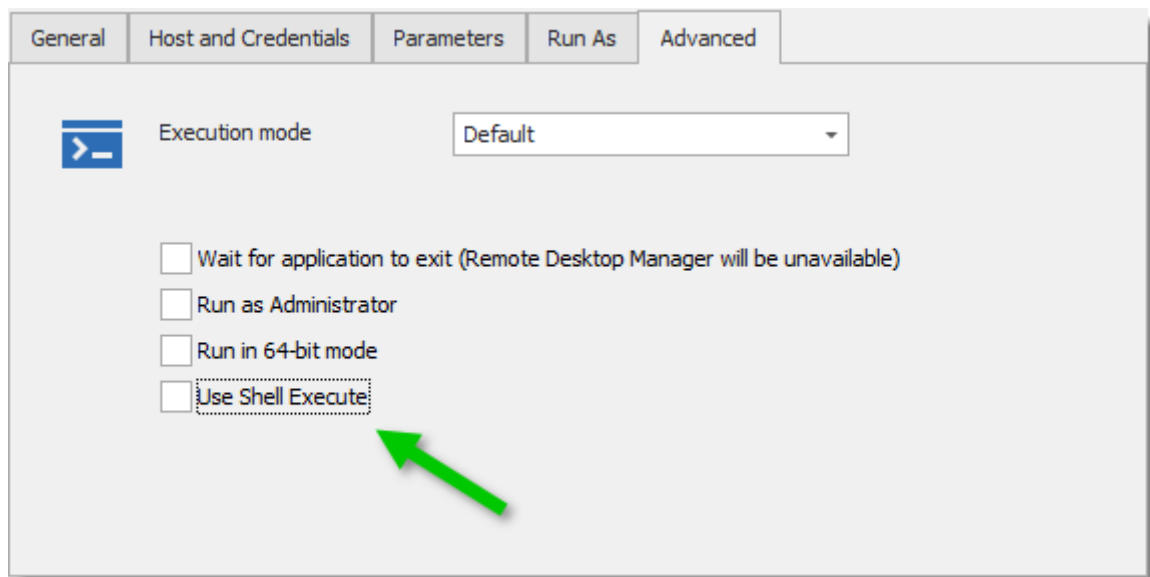
There are minor differences with Example 1, but here is the full procedure to make it easy to read



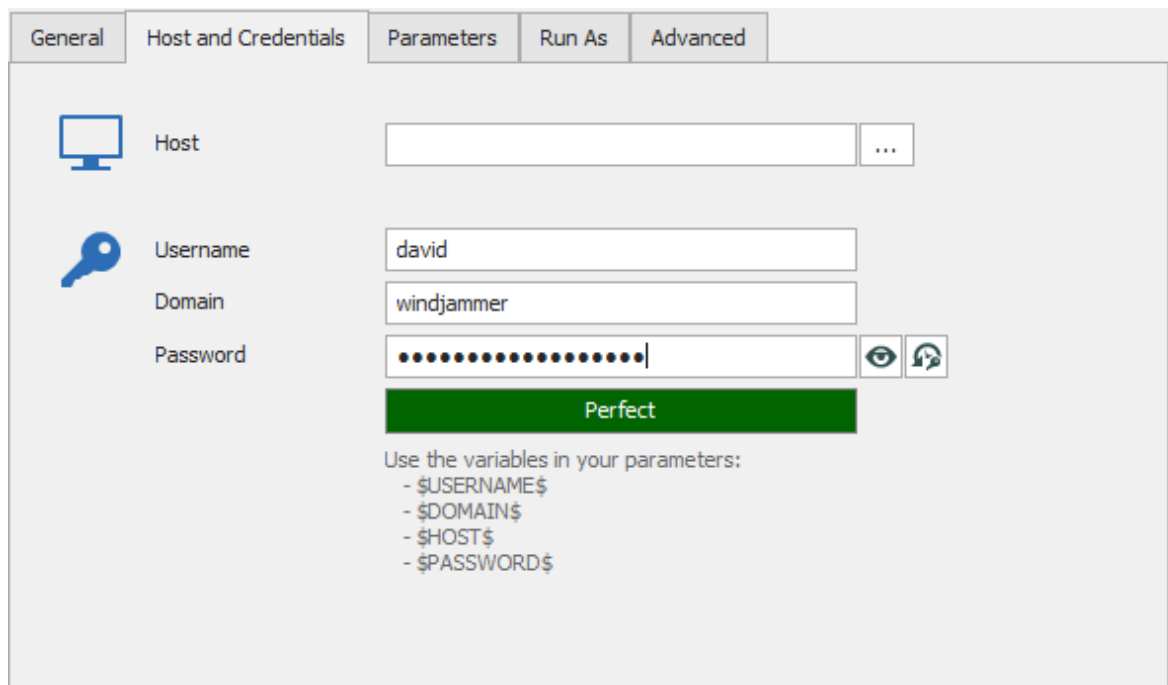
Note that most of our entries now support **NetOnly** as a built in feature.

1. You can use the ellipsis button to browse for the runas.exe command, but if you are in a shared data source and the session will be used on various operating systems, it's better to type in **"%systemroot%\system32\runas.exe"** because it will work on all of them.
2. Append **/netonly /user:\$DOMAIN\$\\$USERNAME\$**, keeping it outside of the quotes. Note the use of two variables that will pull the appropriate value from other fields of the same session. For more information please consult the Variables topic. Also note the use of the **NetOnly** parameter, it signals that the credentials will be used for network access only.
3. Append the name of the Management Studio executable and its parameters. All this needs to be within the same double quotes
  - 3.1. SQL Server Management studio is located at "C:\Program Files (x86)\Microsoft SQL Server\110\Tools\Binn\ManagementStudio\Ssms.exe" on most machines, adapt to your situation if it's not the same.
  - 3.2. My parameters look like this: **-S sql.windjammer.loc -E**. -S is for the server name, -E is to use windows authentication, you can even specify the database using -d \_\_DB\_NAME\_\_ (i.e. -d rdm)

The result is: "C:\Program Files (x86)\Microsoft SQL Server\110\Tools\Binn\ManagementStudio\Ssms.exe -S sql.windjammer.loc -E"
4. Uncheck **"Use Shell Execute"** (this must be done for most Windows Applications)



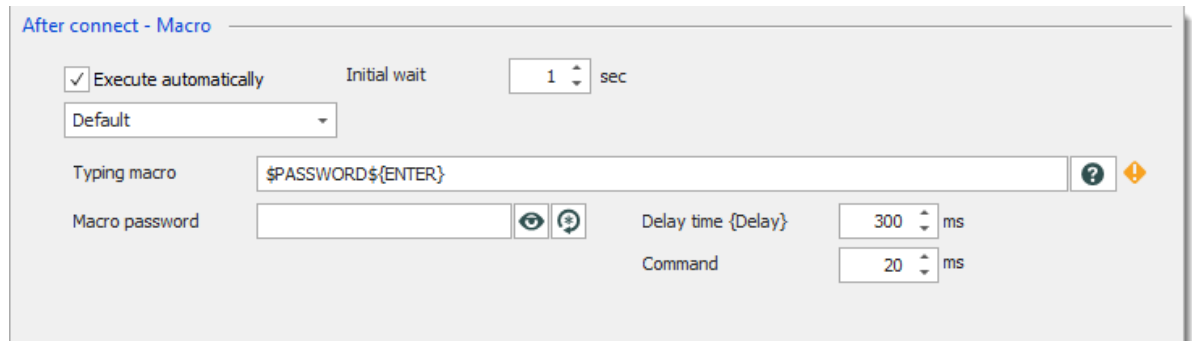
7. Specify your credentials in the **Host and Credential** tab. Note that when you are not part of a domain, you should enter the computer name in the domain field.



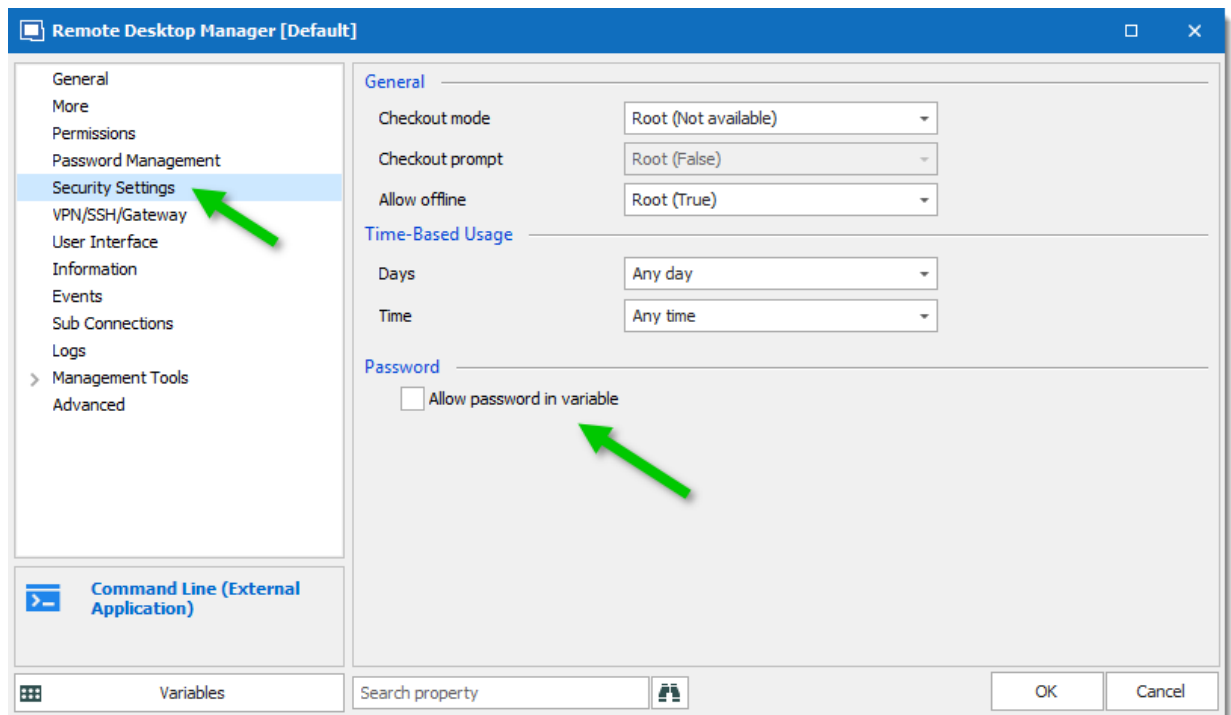
8. In the Events tab you must define a typing macro

8.1. Set the Initial Delay to the lowest value that will allow the initial prompt to appear. On most systems 1 second is sufficient

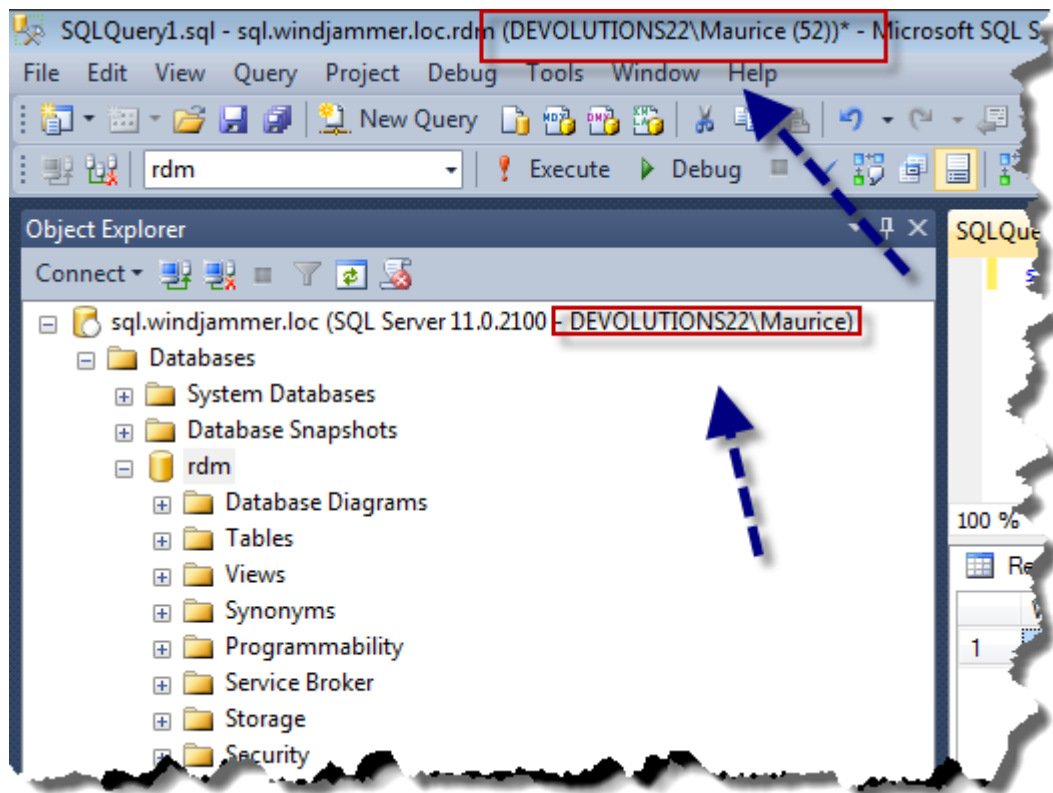
8.2. In the Typing macro field, enter the following: **`$PASSWORD${ENTER}`**. For more information please consult Auto Typing Macro.



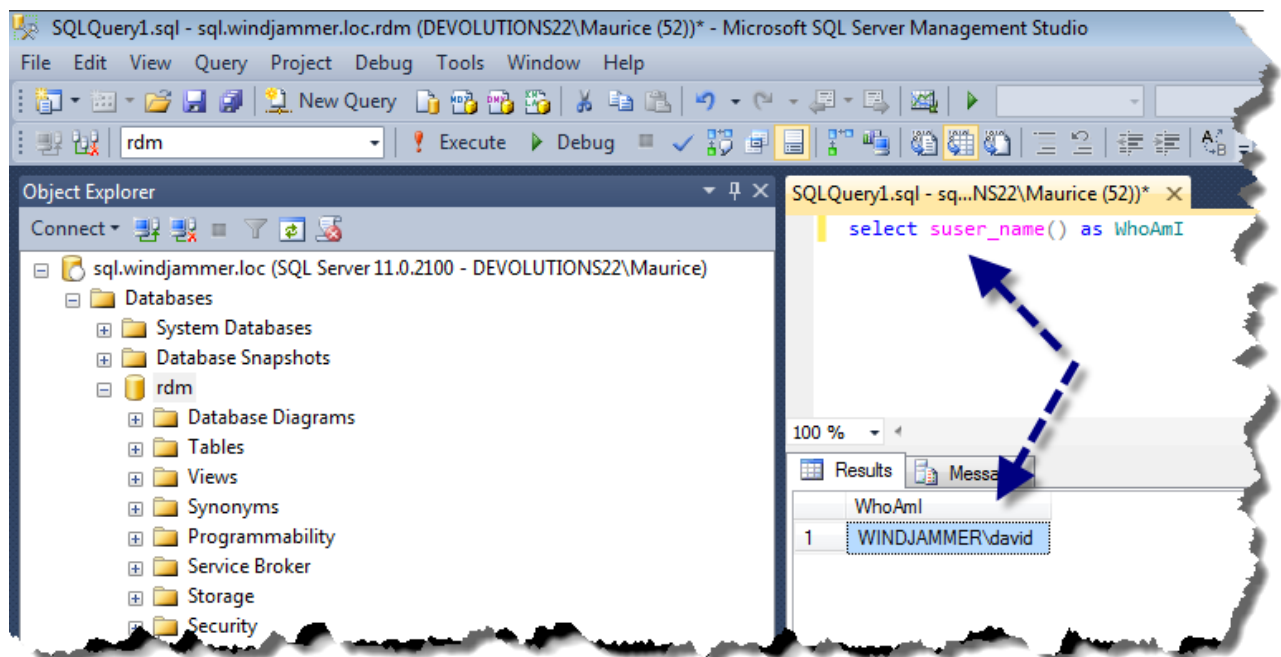
9. In the advanced tab, you must check "***Enable password in variable***".



Run the session and wait for Management studio to appear, attentive users will notice that it looks like you are running under your local credentials because of these...



A simple query will prove that it worked, perform a ***SELECT SUSER\_NAME()*** query.



## 12.7.16 Running Remote Desktop Manager as Another User

### DESCRIPTION

There are many different type of credentials and they are used by a multitude of users. On Windows systems, having multiple user accounts enables the ability to launch Remote Desktop Manager under a different set of credentials while we are already logged on using main credentials. This allows for using Integrated security to connect to an [Advanced Data Source](#).



These solutions require the "Secondary Log-on" service to be running.



If the other account belongs to a domain different than the one from your workstation, solution A must be used.

### SOLUTION A - RUNAS COMMAND

This solution is ideal if you do this often, you can create a batch file with the command and simply type in your password when prompted.

The RunAs command has many parameters to change its behaviour, we wont cover them all here, but if you have an advanced scenario we suggest you consult the Windows help.

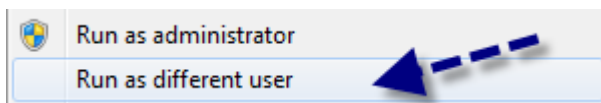
1. Open a command prompt.
2. Type ***runas /netonly /user:{your username here}***. Usage of the **NetOnly** parameter signals that the credentials will be used for network access only. Ensure you username is entered as your infrastructure requires. Typically its ***{domain}\{user}***, i.e. ***windjammer\david***
3. Append the full path to Remote Desktop Manager, typically ***%ProgramFiles(x86)%\Devolutions\Remote Desktop Manager\RemoteDesktopManager.exe***, but you must ensure this is correct for your machine.
4. When you press enter, you are prompted for the password, then the application will launch.

```
C:\tools>runas /netonly /user:windjammer\david "%ProgramFiles(x86)%\Devolutions\
Remote Desktop Manager\RemoteDesktopManager.exe"
Enter the password for windjammer\david:
```

*RunAs command example*

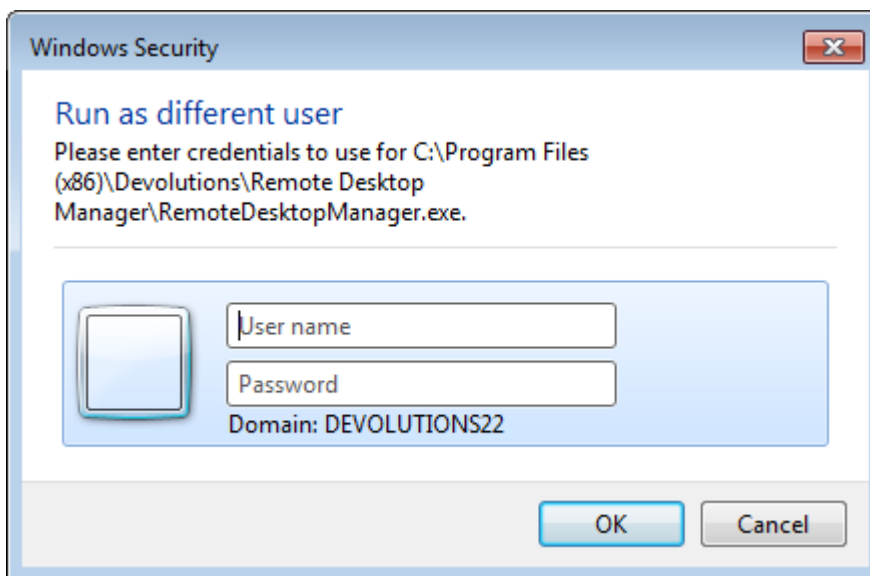
## SOLUTION B - SHIFT+RIGHT CLICK ON THE SHORTCUT OR EXECUTABLE TO REMOTE DESKTOP MANAGER

When you press **Shift + Right Click** on an executable, you'll notice an additional menu item for **Run as different user**.



*Shift + Right click contextual menu*

You are presented with a logon form in which you must specify the username and password.



### 12.7.17 SQL Server Data Source with Integrated Security

## OVERVIEW



We will take you through a step by step guide to configure and test a Remote Desktop Manager deployment against an SQL Server data source using Integrated Security.

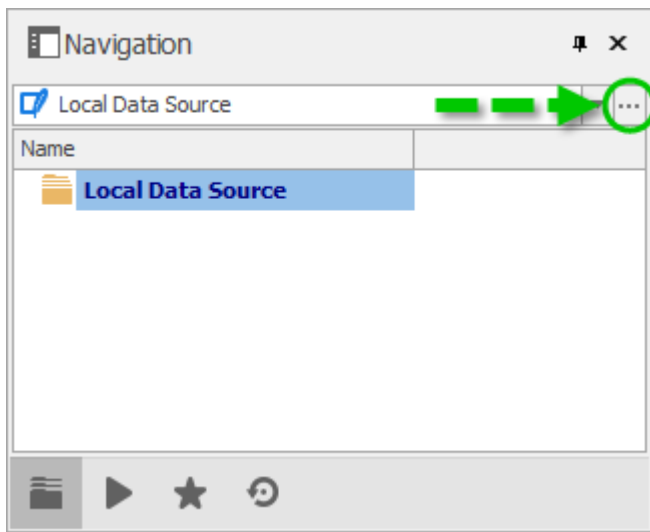


Any user (domain, local machine or SQL user) that has a server role of `sysadmin` is automatically an administrator of Remote Desktop Manager.

## CREATE THE DATABASE

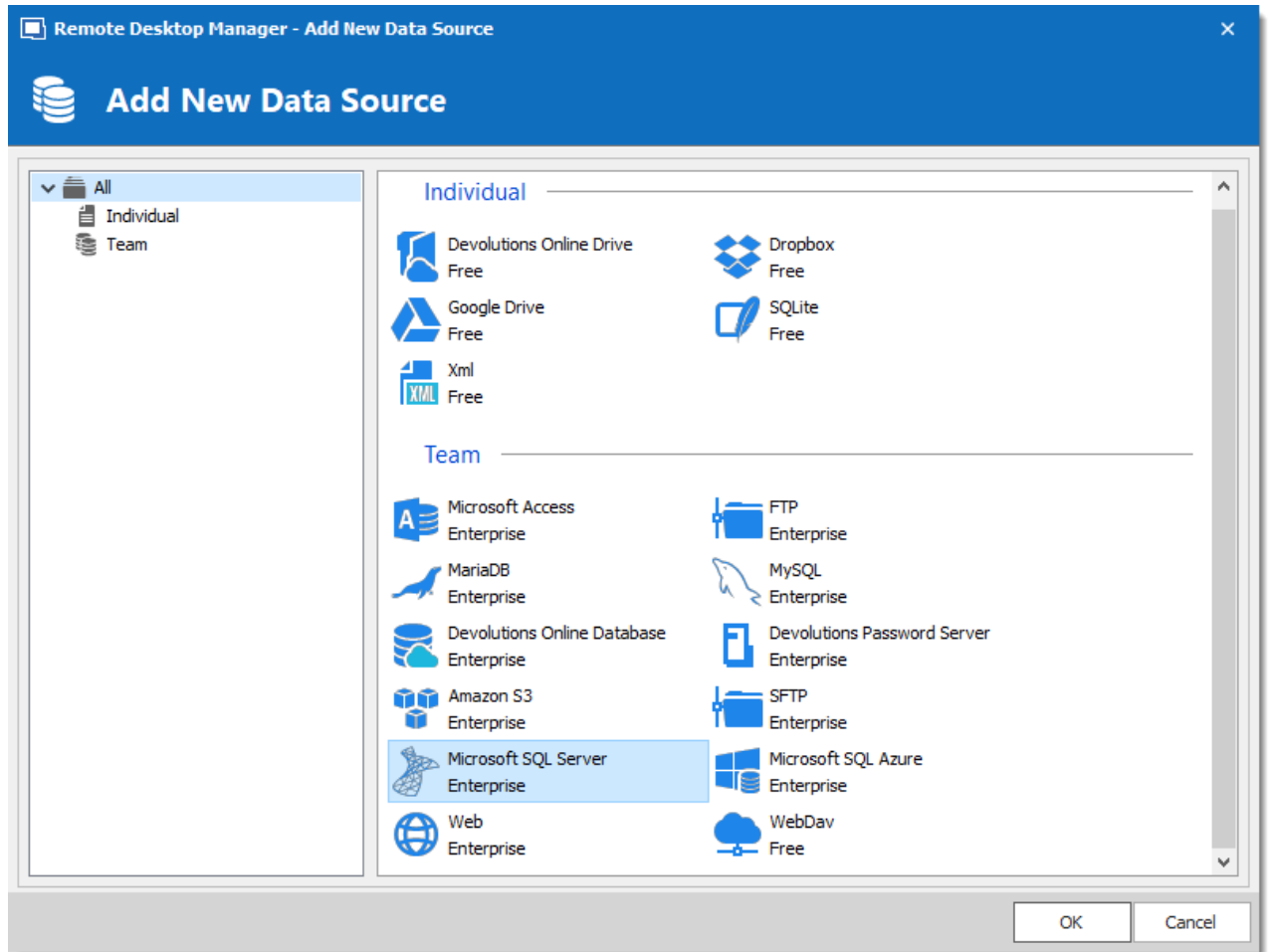
The first step is to create the database that will store all your entries.

Click on the **ellipsis** button in the Navigation Pane, then click on **+ Add a new data source**.



*Navigation Pane - Data Sources*

Select the **Microsoft SQL Server** data source and click **OK**.



*Microsoft SQL Server Data Source*

- Specify the **Name**, **Server** and **Database**
- Authenticate with a user that is part of the `sysadmin` role.

The screenshot shows a configuration window with the 'Upgrade' tab selected. The 'General' sub-tab is active. The configuration fields are as follows:

Field	Value
Name	SQL Server
Host	localhost
Login mode	Database login
Username	sa
Password	.....
Always ask password	<input type="checkbox"/>
Allow change username	<input type="checkbox"/>
Database	Windjammer
Two factor	<a href="#">None</a>

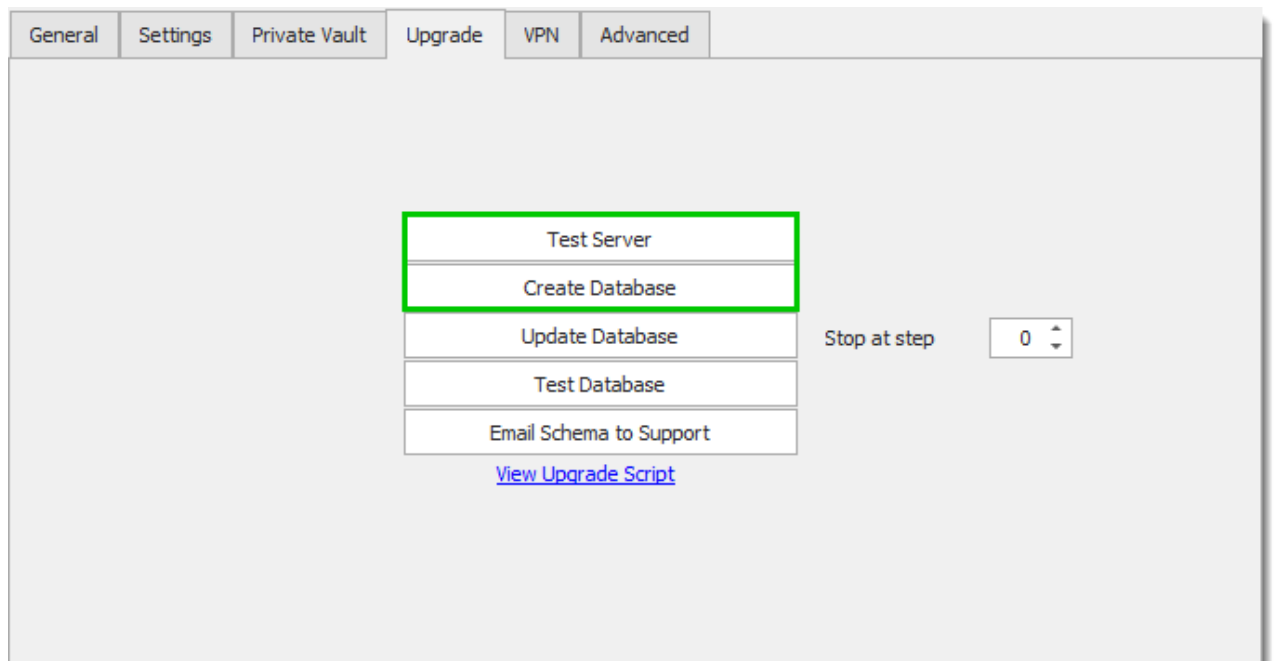
Buttons: Test Server, Test Database

*Create the SQL Server Data Source*



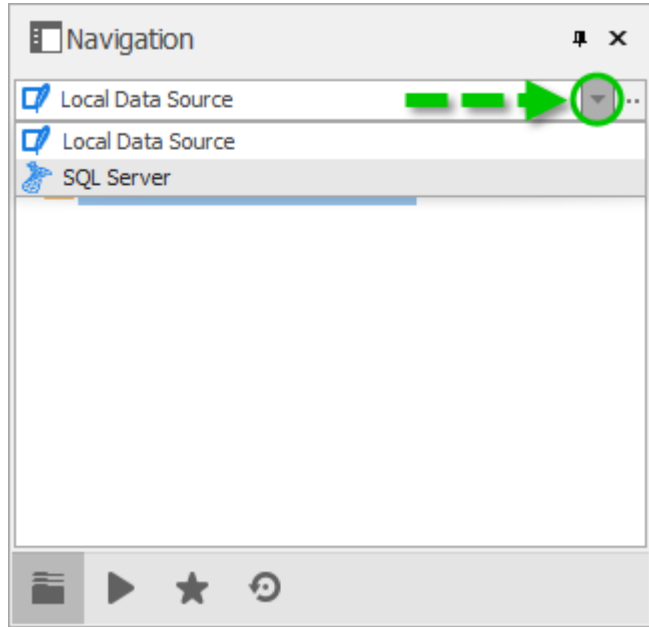
If the logged-on Windows User is not part of the SQL Server **sysadmin** role and you've configured the server to use SQL Server and Windows Authentication Mode, then use a SQL Server user (SA for example) that has the appropriate role assigned. You can then add yourself as a Remote Desktop Manager user later and change the data source to use **Integrated security**.

- From the upgrade tab, click **Test Server** then **Create Database** to create the SQL Server database.



*Test the server and create the database*

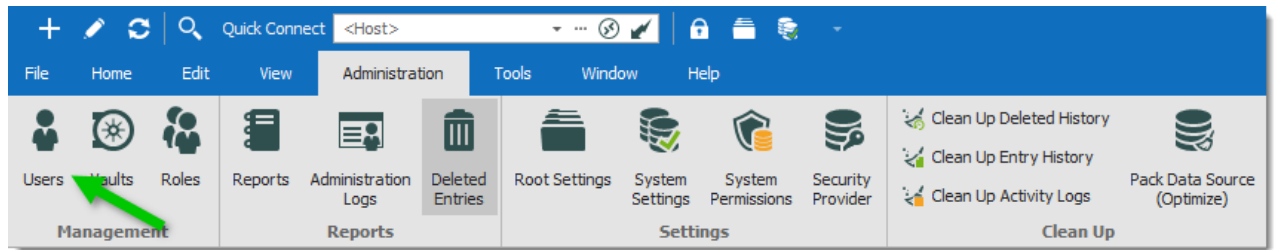
Press **OK** to close the dialogs. In the Navigation Pane, select the newly created data source from the data source drop down list.



*Select the Data Source*

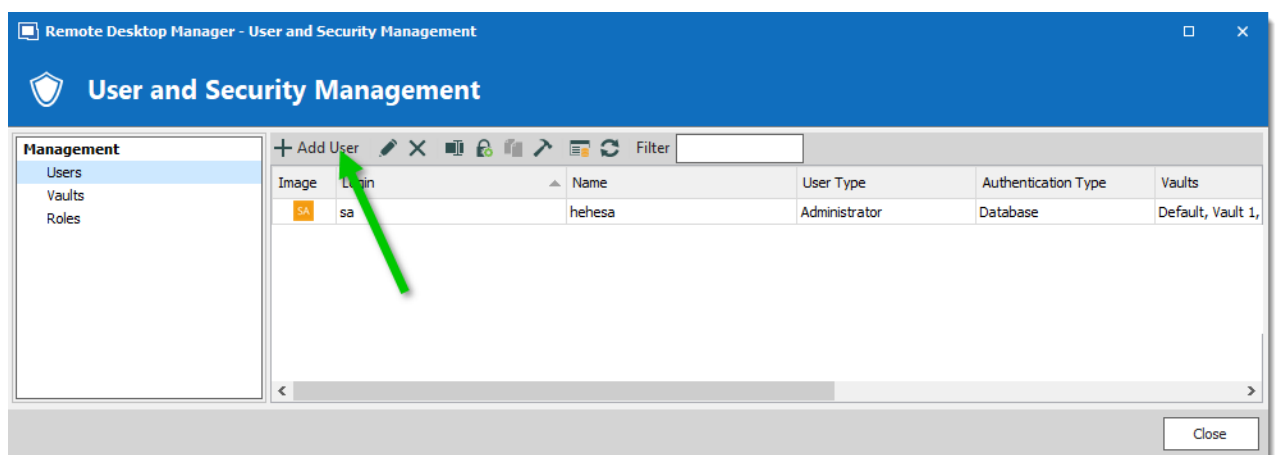
## CREATE USERS

To create users, navigate to **Administration – Users**.



*Administration - Users*

Click **+ Add Users**.



*User and security management*

Check the **Integrated security (Active Directory)** box and click the ellipsis button to select the domain user to add.

Remote Desktop Manager - User Management

**User Management**

General

ID: 519EEAB3-2479-49D6-B562-23430A6B2F1D

Authentication type: Database

Username: VDEVOLUTIONSXXX\username ☒ Integrated security (Active Directory)

Password:  ☒ Create SQL Server Login and User

User type: User

User license type: Default

Information

First name:  Last name:

Email:

OK Cancel

*User Management – Integrated Security*

Select the **User type**. Grant the **Add**, **Edit**, and **Delete** rights (optional, restricted user only). For more information on user types and rights, please consult the [Administration – Users](#) topic.



Keep the **Create SQL Server Login and User** box checked. This will in effect cause Remote Desktop Manager to map a new login to the domain account and link it to a user.

You can uncheck this in the case where your DBA has created your login already on the SQL Server.

Repeat these steps for each user that needs access to this data source in Remote Desktop Manager.

## CONFIGURE REMOTE DESKTOP MANAGER FOR OTHER WORKSTATIONS

To configure the data source on other workstations, three methods are available:

- Create the data source as done previously, making sure to check the **Integrated Security (Active Directory)** box.
- Export the data source from the initial workstation and import it into Remote Desktop Manager on all client workstations.
- Use our [Custom Installer Manager](#) service to help distribute the application and personalize the installation process.

## TEST THE CONFIGURATION

If you have a second set of domain credentials, you could use this trick to test locally. [Running Remote Desktop Manager as Another User](#)

Now in your Remote Desktop Manager with admin rights, create a few roles (Admin, Production, Staging) and assign them users.

### 12.7.18 SQL Server Maintenance Plans

## DESCRIPTION

Sadly, a SQL Server Instance is not something you can simply install and run without proper care. Keeping the default values for new databases will almost certainly cause issues in the long run.

If maintenance is not performed regularly, the database files will grow and grow until the mere size of the files will decrease performance and finally reach a point where the client application appears unusable.

We are **NOT** a DBA shop. Asking the question "[What is the best maintenance plan I can implement?](#)" to seasoned DBAs will invariably result in an answer similar to "[It depends](#)".



These "pointers" are provided as is and we cannot be held responsible if they don't meet your requirements. You must consult a qualified database administrator to confirm your needs and how to meet them.

The backup strategy really depends on the amount of data you are comfortable with **losing** in the event of failure, yes... expect to lose data, the cost of a system that does NOT lose **any** data is **quite high** and is not in the scope of this topic.

If you are comfortable with only being able to revert to last night's backup, you can set the DB to simple recovery model, and take a nightly full backup.

If you want something a little more robust we have seen the following:

- A daily full backup of the DB.
- More frequent backup of the transaction log, lets say every 4 hours starting at 06:00 and ending at 18:01 or 22:01
- A cleanup task to remove older backups.

If you need to be able to recover data that is minutes in the past, then you really need a qualified DBA to help you.

Again, these are examples of how we've seen backups planned for non-critical systems. If it does **not** meet **your** specific requirements. You **must** monitor: the time the backups take to complete; the free space left on the backup device; **and so on and so on!**

Also, a backup strategy involves actually going through the recovery process regularly to prove that it works. Backups usually work fine, it is the restoring process that is difficult, imagine having a boss breathing down your neck while you are searching for the proper sequence of actions because you've never done this before...

If you look at our first ever sysadminotaur, (at <http://blog.devolutions.net/2012/08/sysadminotaur.html>) you can guess that we've heard of bad backup plans before...



Backup plans must be monitored and Recovery plans must be **enacted** to confirm they actually work!

## 12.7.19 Tab Groups

### DESCRIPTION

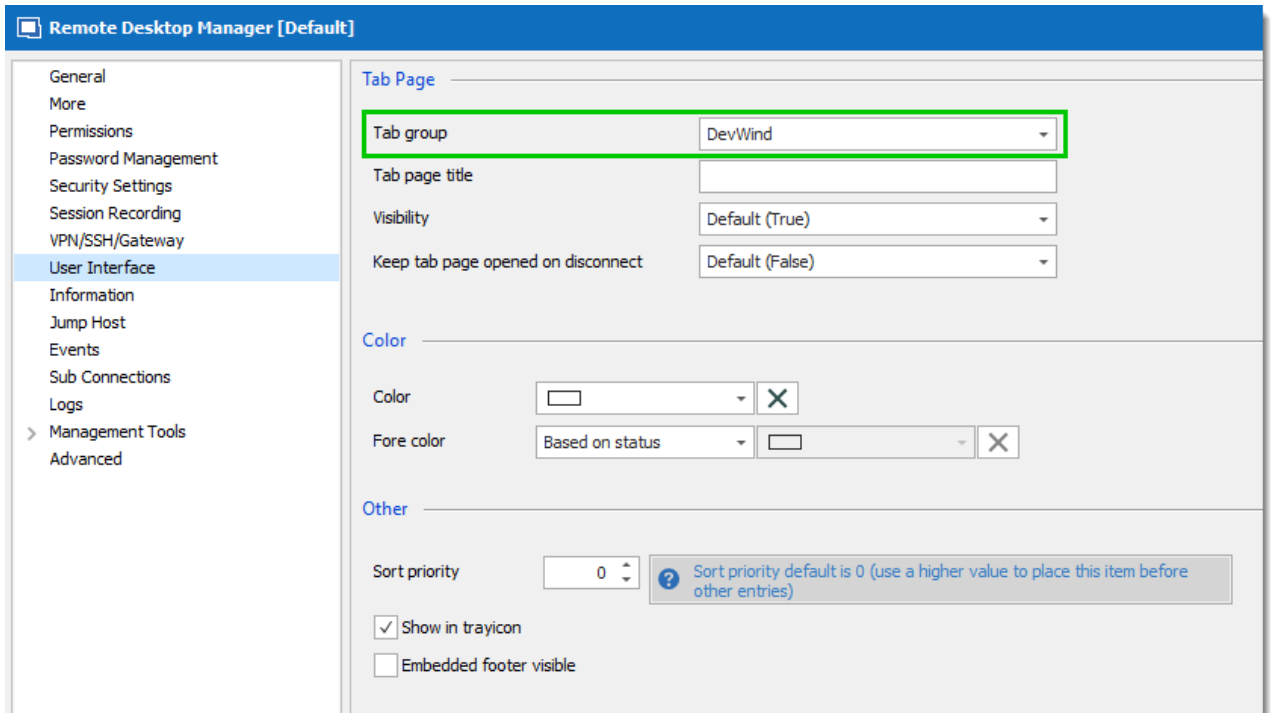
Remote Desktop Manager is great for running many sessions at once by using its **Embedded/Tabbed** display mode. It's especially true when using multiple remote control technologies at the same time. No longer will you have to dig in your task bar to locate the session of interest, you have them all running in tabs within the same tool used to launch them.

But when you reach a certain number of running sessions, it may become difficult to identify them using only their name. To improve user experience for those of us that love embedded sessions, we created a feature to filter the tab pages, it is called the **Tab group**.



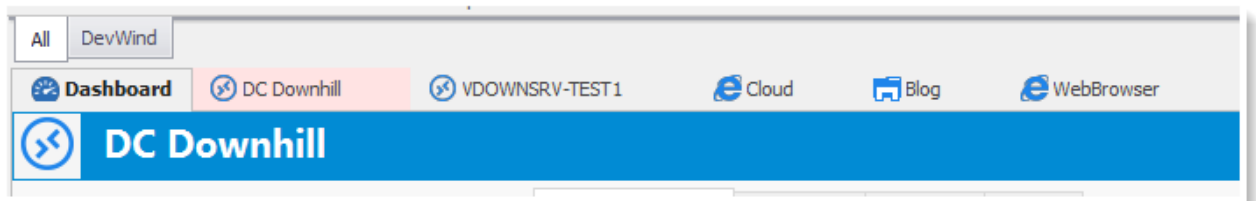
## SETTINGS

The tab settings are found in the **User Interface** side menu of your session properties.



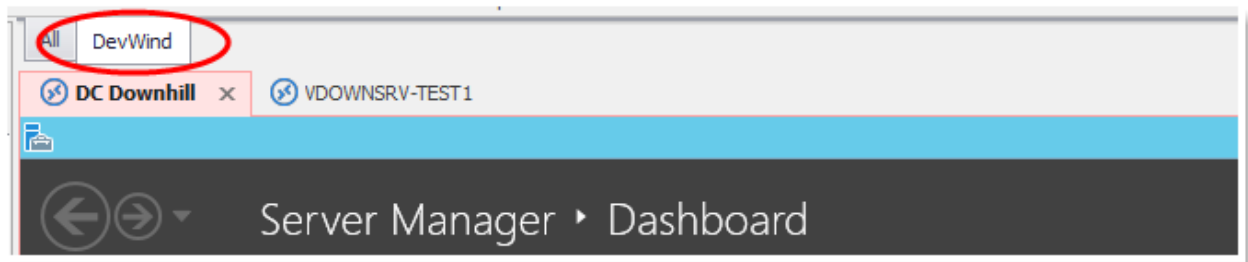
*RDP session - User Interface*

Simply type a name in the **Tab group** to create a tab group when launching an instance. You can see it in action in the image below



*Tab groups displayed - All selected*

When the **All** group is selected, it performs no filtering. When you select another group, it hides all the sessions that do not match with the filter. In the example below, I've adjusted two sessions to have the same category.



*Specific Tab group selected*

## 12.7.20 Team Tips

### OVERVIEW

Here are five RDM team tips.

### SECURITY, USERS & ROLES

Sharing session information is great -- but controlling access is bliss.

Through Remote Desktop Manager's Role system, you can control access and user rights for specific sessions and actions.

Start by creating roles and naming them accordingly to what you expect them to be able to view and use. Then assign users to them. Now all you have to do is assign roles to entries and folders according to your wishes.

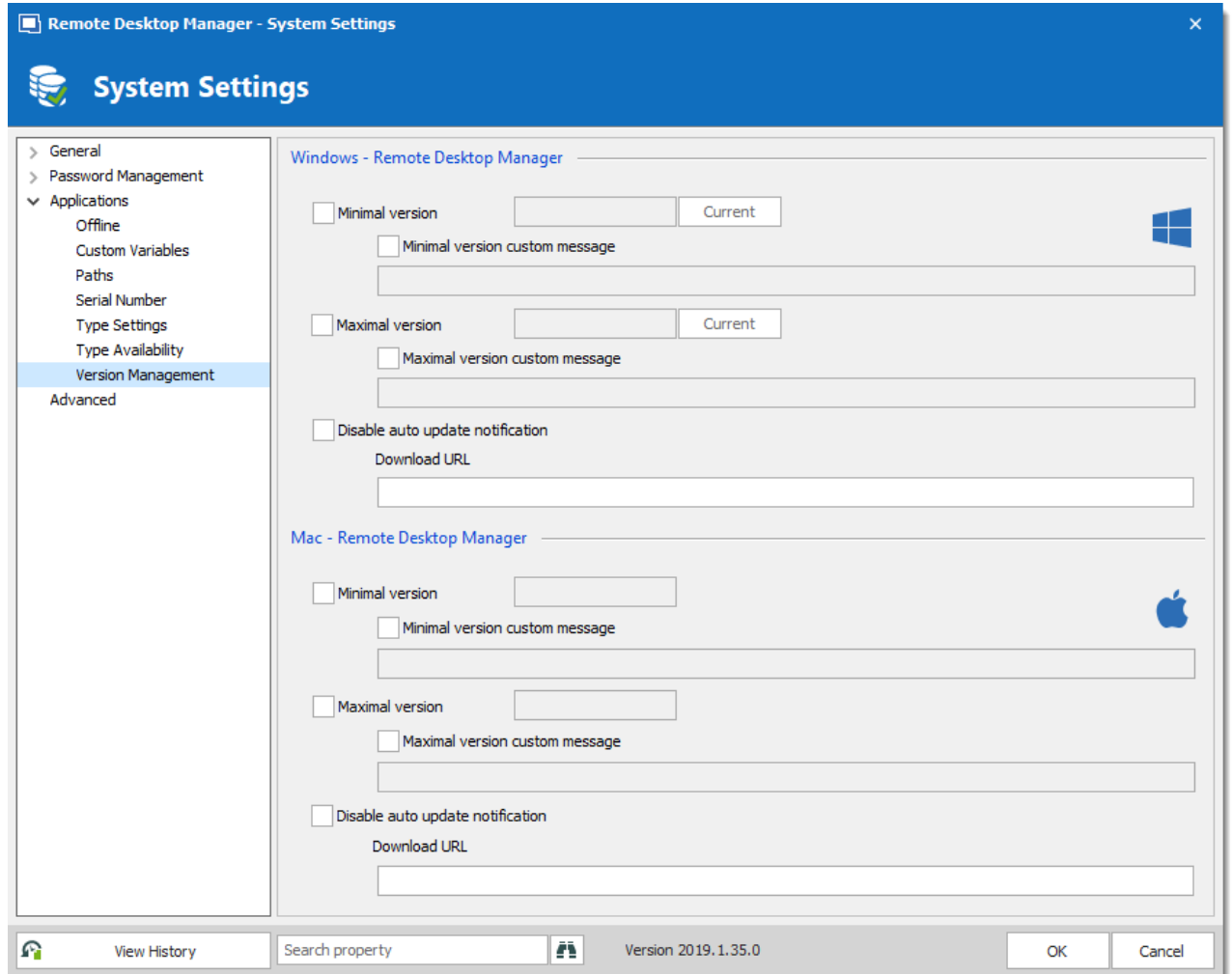
### STREAMLINED DEPLOYMENT WITH CUSTOM INSTALLER

Okay: you're ready to deploy Remote Desktop Manager and make everyone see you as the company hero. You've manually configured your data sources, specified your site license, and defined system options. You can feel the excitement coursing through your veins. You are on a mission!

But wait – before you go live, why not have us create a [Custom Installer](#) for you? Once we do that, your grateful team will only need to install the resulting MSI file to access their ready-to-use pre-configured Remote Desktop Manager installation. You will be loved by one and all, perhaps with a parade, a state, or an award named after you.

## VERSION MANAGEMENT

Here's a familiar scenario: your team has been using Remote Desktop Manager for months or even years, and all is well. Then along comes a new version full of cool new features, and you think that everyone in your company should upgrade. This window below depicts the different options at your disposal to control client versions.



Version Management

We've made this extremely easy. Simply open **Administration – Data Source Settings (System Settings) – Version Management**. Below, a description of some of the settings;

- **Disable auto update notification** – This will disable the "New version is available" message. (You're welcome!)
- **Minimal version** – This specifies the minimal acceptable version. If a member of your team runs an RDM version below this level, they'll be prompted to upgrade.

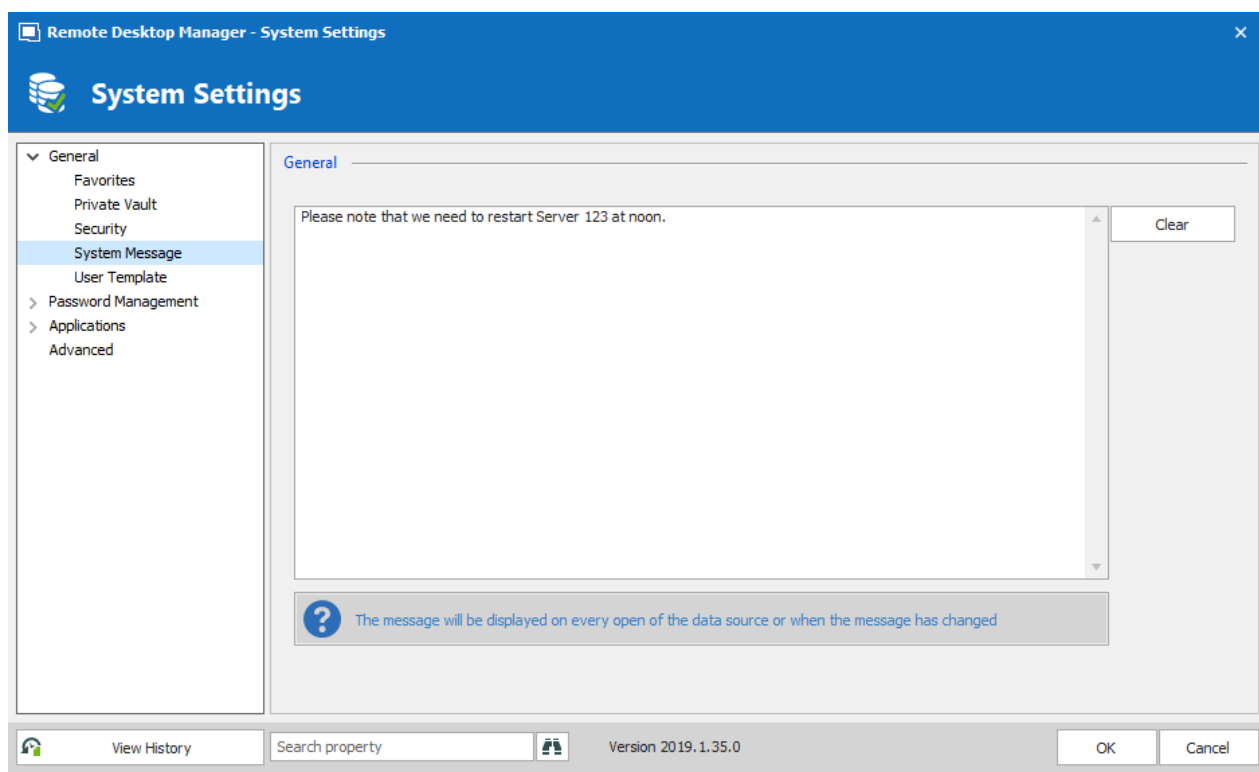
- **Download URL** – This improves install speed by downloading the MSI onto your local network, and lets all of your team members easily upgrade from this path. In short, this saves time and avoids installing the wrong version.

The **Administration – Data Source Settings (System Settings) – Serial Number** section is useful if you have a Site or Global License, and keeps you from having to manually set the key on every client.

## DATA SOURCE SETTINGS (SYSTEM SETTINGS)

The general tab of the **Administration – Data Source Settings (System Settings)** form allows you to easily control security aspects.

A great team feature here is the **System Message**, which allows an administrator to inform users of upcoming system downtime, policy change or anything else. Each user will get the message when they perform the next action (open, edit, refresh...) of the data source. Use it to display company confidentiality clauses or, if you wish, create chaos with a message like the one below. A little bit of chaos is good for the soul.



*System Message*

## DEVOLUTIONS PASSWORD SERVER

Do you need Active Directory integration? Or perhaps you have off site users who need to access the shared data source, but don't want to use a VPN connection? Maybe you want more security and caching? Devolutions Password Server delivers all that and much more!

You deploy **Devolutions Password Server** on-premises and can decide to publish the instance only on your intranet; or go all the way and offer it online. This allows you to create an enterprise wide high-end data store. Find out more about **Devolutions Password Server** at <http://server.devolutions.net/>

### 12.7.21 Testing variables

#### DESCRIPTION



Variables are only supported for **Advanced Data Sources** like SQL Server, mySQL and <%DPS%>.

Remote Desktop Manager's Auto Typing Macro is really helpful to simulate user interaction. It's mostly used to perform automatic logon on web pages, but you can run advanced shell commands on various operating systems.

Sometimes you need to confirm exactly what will be sent when using our Variables.

A simple trick is to create a batch file that just types out whatever is sent on the command line.

Just copy the following in your favorite editor and save it as a command file, I named mine **parrot.bat**

```
@echo off
echo.
echo.
echo %*
echo.
echo.
pause
```

Now its a simple matter of creating a **Command Line (External Application)** session and set the command line to the path of the **parrot.bat** file and add the variables right after.

```
"C:\tools\parrot.bat" %DOMAIN% %IP% %USERNAME%
```

Now when you run the entry, you will see exactly what values are sent.

A reminder that for the password to be available as a variable, you must go in the **Security Settings** of the entry and check **Allow password in variable**.

## 12.7.22 Use Different Versions of Same Application

### DESCRIPTION

You have 2 different versions of an application installed on your workstation and you want to be able to use both versions inside Remote Desktop Manager.

### SETTINGS

When you configure your application installation path in **File – Options – Path**, separate the paths by a ;

Remote Desktop Manager will prompt you with the selection list and you will be able to pick the one that you want to use.

### EXAMPLE

***C:\Program Files\Appsv1;D:\Program Files\Appsv2***

## 12.7.23 VPN

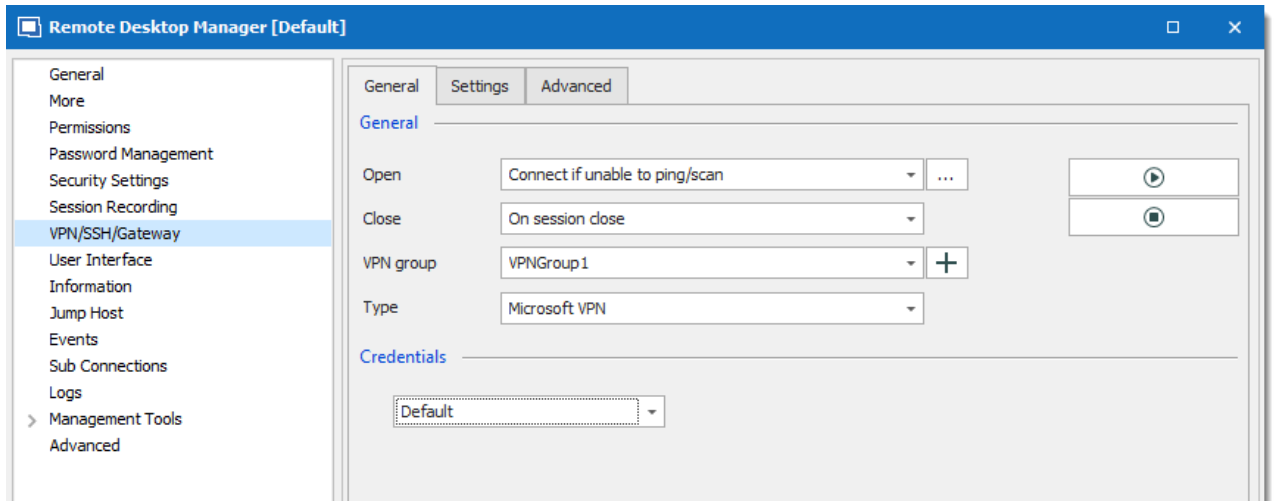
### 12.7.23.1 VPN Group

### OVERVIEW



VPN groups are defined inside each individual entry in the VPN/SSH/Gateway section.

When multiple entries are configured to use the same VPN group, the VPN connection will stay active until the last session disconnects.



VPN Group

The VPN close mode need to be set to **On sessions close** to use this feature.

The VPN group name needs to be exactly the same to ensure that Remote Desktop Manager increments the usage counter.

### 12.7.23.2 VPN Routing

## OVERVIEW

Establishing a VPN connection using Remote Desktop Manager is easy. Unfortunately, adding routes has to be done manually. Wait for the adapter to connect, find the IP and add the desired routes. Even if you use a script (such as a Power Shell script), it's still a redundant time consuming task – and one you can certainly live without.

```
C:\Windows\system32>ROUTE ADD 10.1.2.5/32 100.77.183.56
OK!

C:\Windows\system32>ROUTE PRINT
=====
IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway
0.0.0.0                    0.0.0.0          192.168.1.1
10.1.2.5                    255.255.255.255  100.77.183.56
127.0.0.0                  255.0.0.0        On-link
127.0.0.1                  255.255.255.255 On-link
127.255.255.255            255.255.255.255 On-link
192.168.1.0                255.255.255.0   On-link
```

## SOLUTION

This feature is part of a larger concept called VPN Commands, and allows you to run any type of script or executable post-VPN-connect and pre-VPN-disconnect.

**Advanced**

☐ Go Offline on connection
 ☐ Go Online on disconnect

☐ Close connection after 0 min
 ☐ Use adapter to detect connection

☐ Detect reachable host in wait

VPN reconnect mode: Default

**After Execute Wait**

☐ -1 sec
 ☒ For IP on adapter

Wait maximum of -1 sec Then delay -1 ms

**Commands**

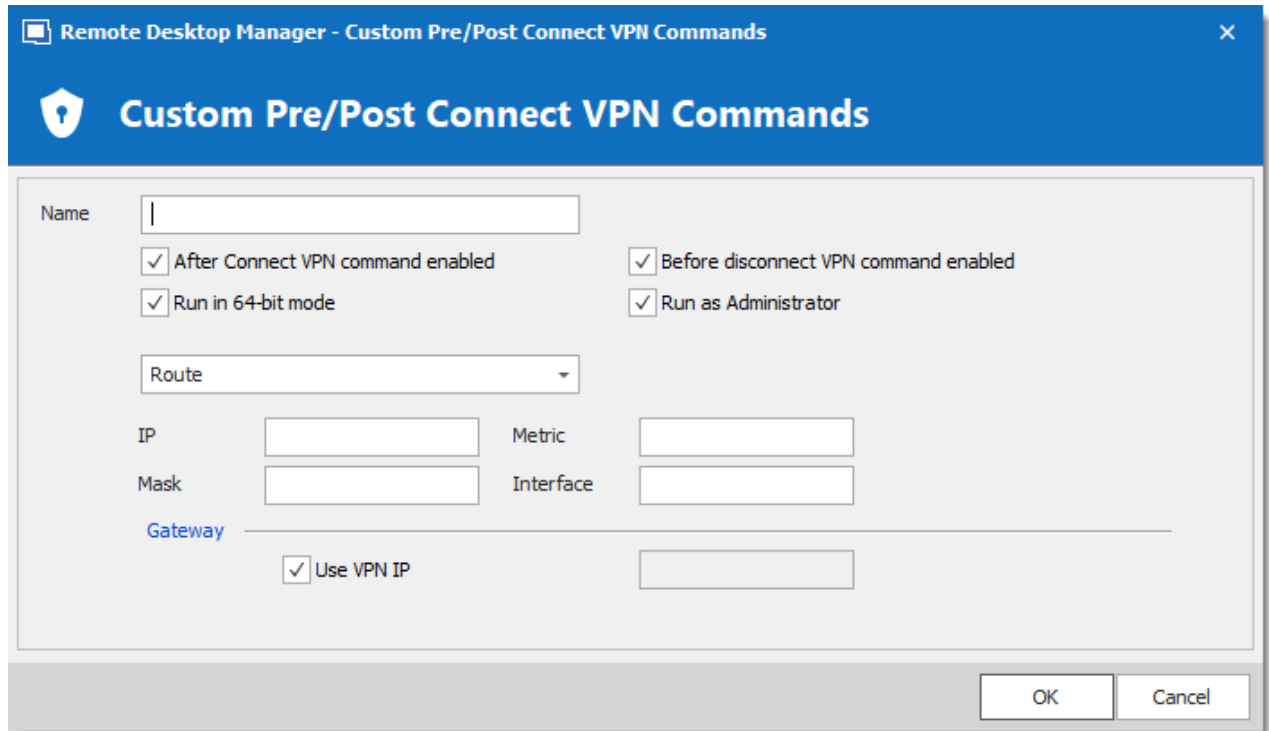
Name	After Connect Command	Before Disconnect Command
Home	ROUTE ADD 10.1.2.5 \$GA...	ROUTE DELETE 10.1.2.5

☒ After Connect VPN command enabled
 ☒ Before disconnect VPN command enabled

## WORKFLOW

1. Configure the VPN to wait until the adapter connects and gets assigned an IP (we'll be using the adapter's IP to define the routes).
2. Click on **Add** to display the **Commands** dialog.
3. Create a route definition by selecting **"Route (Add/Remove)"** radio item. Finally, set the IP and any other required information.





## 12.8 Troubleshooting

### 12.8.1 1Password

#### ERROR

**WHEN YOU CREATE A NEW 1PASSWORD CREDENTIAL ENTRY, ONLY THE LATEST ENTRIES ADDED TO 1PASSWORD ARE DISPLAYED.**

In 1Password, click on **File – Repair 1Password Vault**. This should fix the issue.

### 12.8.2 2-Factor Authentication

#### ERRORS

## WITH GOOGLE AUTHENTICATOR, YOU ARE GETTING AN INVALID PASSWORD ERROR EVEN THOUGH YOU ARE SURE OF ENTERING THE PROPER ONE.

The computer clock must be within a small error margin in order to generate the proper authenticator code. We recommend using a NNTP server in order to keep your computer clock synchronized.

## YOU HAVE LOST THE DEVICE

Your Remote Desktop Manager is set to authenticate with Yubikey or Google Authenticator. You no longer have the Yubikey key or the Google Authenticator and you want to turn off this option to connect on Remote Desktop Manager.

If you had installed using the default settings, the configuration file is **%localappdata%\Devolutions\RemoteDesktopManager\RemoteDesktopManager.cfg**

You can choose to simply delete it, obviously all of your settings will be lost, alternatively you can open it and remove everything between the ***EncryptedDataSources*** tags. You will have to re-register all of your data sources and point to either the file or database that you were using.

```

22 <EncryptedDataSources>
23 <string>GNvexSxqRcw+2rlkvSWJfGggayCDY2NjIp+4uXfMpsrV0Ue4U2me6vXQOumLkcy5w6FlfLzI2ri2+QQwvRZX7kzKOyQJVI
24 <string>GNvexSxqRcw+2rlkvSWJfGggayCDY2NjIp+4uXfMpsrV0Ue4U2me6vXQOumLkcy5w6FlfLzI2ri2+QQwvRZX7kzKOyQJVI
25 <string>GNvexSxqRcw+2rlkvSWJfGggayCDY2NjIp+4uXfMpsrV0Ue4U2me6vXQOumLkcy5w6FlfLzI2ri2+QQwvRZX7kzKOyQJVI
26 <string>xhgm0NzbYbv8pgihFZIScZje/0IydutVHGAusA7q/zLBRebYqC0ZRT5nP4+ldbHSj5Qhexz3GzI9E3EXraeAfo8NE5syVI
27 <string>xhgm0NzbYbv8pgihFZIScZje/0IydutVHGAusA7q/zLBRebYqC0ZRT5nP4+ldbHSj5Qhexz3GzI9E3EXraeAfo8NE5syVI
28 <string>xhgm0NzbYbv8pgihFZIScZje/0IydutVHGAusA7q/zLBRebYqC0ZRT5nP4+ldbHSj5Qhexz3GzI9E3EXraeAfo8NE5syVI
29 <string>xhgm0NzbYbv8pgihFZIScZje/0IydutVHGAusA7q/zLBRebYqC0ZRT5nP4+ldbHSj5Qhexz3GzI9E3EXraeAfo8NE5syVI
30 <string>xhgm0NzbYbv8pgihFZIScZje/0IydutVHGAusA7q/zLBRebYqC0ZRT5nP4+ldbHSj5Qhexz3GzI9E3EXraeAfo8NE5syVI
31 <string>xhgm0NzbYbv8pgihFZIScZje/0IydutVHGAusA7q/zLBRebYqC0ZRT5nP4+ldbHSj5Qhexz3GzI9E3EXraeAfo8NE5syVI
32 <string>xhgm0NzbYbv8pgihFZIScZje/0IydutVHGAusA7q/zLBRebYqC0ZRT5nP4+ldbHSj5Qhexz3GzI9E3EXraeAfo8NE5syVI
33 <string>xhgm0NzbYbv8pgihFZIScZje/0IydutVHGAusA7q/zLBRebYqC0ZRT5nP4+ldbHSj5Qhexz3GzI9E3EXraeAfo8NE5syVI
34 <string>xhgm0NzbYbv8pgihFZIScZje/0IydutVHGAusA7q/zLBRebYqC0ZRT5nP4+ldbHSj5Qhexz3GzI9E3EXraeAfo8NE5syVI
35 <string>gvnPAj/pQgv8pgihFZIScZje/0IydutVHGAusA7q/zLBRebYqC0ZRT5nP4+ldbHS2MuYa8tdu5E9E3EXraeAfo8NE5syVI
36 <string>GNvexSxqRcw+2rlkvSWJfGggayCDY2NjIp+4uXfMpsrV0Ue4U2me6vXQOumLkcy5w6FlfLzI2ri2+QQwvRZX7kzKOyQJVI
37 <string>gvnPAj/pQgv8pgihFZIScZje/0IydutVHGAusA7q/zLBRebYqC0ZRT5nP4+ldbHS2MuYa8tdu5E9E3EXraeAfo8NE5syVI
38 <string>GNvexSxqRcw+2rlkvSWJfGggayCDY2NjIp+4uXfMpsrV0Ue4U2me6vXQOumLkcy5w6FlfLzI2ri2+QQwvRZX7kzKOyQJVI
39 <string>GNvexSxqRcw+2rlkvSWJfGggayCDY2NjIp+4uXfMpsrV0Ue4U2me6vXQOumLkcy5w6FlfLzI2ri2+QQwvRZX7kzKOyQJVI
40 <string>xhgm0NzbYbv8pgihFZIScZje/0IydutVHGAusA7q/zLBRebYqC0ZRT5nP4+ldbHSj5Qhexz3GzI9E3EXraeAfo8NE5syVI
41 <string>SB8ec+PVfiJSolmw93nSZ7a13imoRySDVs3PF1X9E182J2DBQ2L0BCGRLg7IjEZUANmAYoUYI4DRLO5/ZhTx4GggayCDY;
42 <string>xhgm0NzbYbv8pgihFZIScZje/0IydutVHGAusA7q/zLBRebYqC0ZRT5nP4+ldbHSj5Qhexz3GzI9E3EXraeAfo8NE5syVI
43 </EncryptedDataSources>

```

*Encrypted DataSources*

```

22 <EncryptedDataSources>
23 </EncryptedDataSources>

```

*Empty Encrypted DataSources*

## 12.8.3 Apple Remote Desktop

### ERRORS

#### NOT ABLE TO ESTABLISH A REMOTE CONNECTION TO A MAC COMPUTER USING APPLE REMOTE DESKTOP (ARD) ENTRY TYPE

Try to restart the Remote Management service on the mac computer. On the mac, go in **System Preferences – Sharing** and uncheck/check the Remote Management service.

#### BLACK SCREEN APPEARS AFTER CONNECTING WITH APPLE REMOTE DESKTOP

Activating the logging on the mac may help the Devolutions support team resolving the issue. In order to activate the logging server side, execute the following command in Terminal:

**sudo defaults write /Library/Preferences/com.apple.RemoteManagement ARDCollectLogs -bool YES**

Once this is done, you can try to connect normally using Remote Desktop Manager. The log will then be located in the **/tmp** folder of the Mac computer.

To turn off logging, execute this command:

```
sudo defaults write /Library/Preferences/com.apple.RemoteManagement ARDCollectLogs -bool NO
```

## 12.8.4 BeyondTrust

### ERRORS

#### **SYSTEM.URIFORMATEXCEPTION: INVALID URI: THE FORMAT OF THE URI COULD NOT BE DETERMINED**

In the **Host** field of the BeyondTrust Password Safe Console entry, make sure to enter the server name like `https://beyondtserver`.

Do not enter the IP address of the server. Entering the IP address instead of the server name will return this error.

#### **SYSTEM.NET.WEBEXCEPTION: THE REMOTE SERVER RETURNED AN ERROR: (404)**

In the **Host** field of the BeyondTrust Password Safe Console entry, make sure to enter the server name like `https://beyondtserver`.

Do not enter the web URL to access the console from a web browser, example

`https://beyondtserver/eEye.RetinaCS.Server/PasswordSafe`.

#### **NOT FOUND SYSTEM.NET.WEBEXCEPTION: THE REMOTE SERVER RETURNED AN ERROR: (500) INTERNAL SERVER ERROR**

In the **Host** field of the BeyondTrust Password Safe Console entry, make sure to enter the server name like `https://beyondtserver`.

Do not enter the web URL to access the console from a web browser, example

`https://beyondtserver/eEye.RetinaCS.Server/PasswordSafe`.

#### **SYSTEM.NET.WEBEXCEPTION: THE REMOTE SERVER RETURNED AN ERROR: (401) UNAUTHORIZED**

In the **Application API key** field of the BeyondTrust Password Safe Console entry, make sure that you have entered the appropriate key. Please refer to the BeyondTrust Password Safe Console entry to learn how to obtain the application API key.

#### **BEYOND TRUST PASSWORD SAFE OR BEYOND TRUST PASSWORD SAFE CONSOLE IS EMPTY AND NO ERROR IS RETURNED**

Make sure that the **Enable for API access** option is checked for your privileged account in BeyondTrust.

## 12.8.5 Clipboard

### DESCRIPTION

#### THIRD PARTY APPLICATIONS INTERFERE WITH THE DATA IN THE CLIPBOARD, PREVENTING YOU FROM COPY/PASTING INFORMATION.

Some applications can affect the clipboard. Below is a list of applications that are known to interfere with the clipboard. Please keep in mind that other applications might affect the clipboard.

- Citrix GoToAssist
- Microsoft Garage Mouse without Borders
- TeamViewer 12

An option allows to revert to the legacy copy/paste method.

Navigate to **File – Options – General**, in the **Clipboard** section and set the **Clipboard copy method option** to **Legacy**. This should resolve the issue.

**Remote Desktop Manager**

- General
  - Application Start
  - Application Close
  - Notification
  - Proxy (Web)
  - Custom Variables
- User Interface
- Types
- Reports
- Browser Extensions
- Key Agent
- Security
- Tools
- Path
- Cloud
- Advanced

**Connection**

Connection details refresh delay: 300 ms

Delay the initial connection: 0 sec

Open connection delay (after ping): 2000 ms

Allow multiple connections (Default): False

**Is online**

☐ Check if host is online

☐ Execute automatic check every: 10 minutes

Check is online: Off

Online detection: Ping

**Clipboard**

Clear clipboard delay: 10 sec

Clipboard secure copy delay: 100 ms

Clipboard copy method: Legacy

Credential copy options: All buttons

*Clipboard Options*

## 12.8.6 Corrupted System File

### DESCRIPTION

The components of the .Net Framework are considered a core Windows feature, therefore there are no facilities to reinstall them. However, there are tools to verify and repair system files.



Running those tools may take a long time.

1. Run SFC Scannow - <https://support.microsoft.com/en-us/kb/929833>
2. Run .Net Framework repair tool - <https://www.microsoft.com/en-ca/download/details.aspx?id=30135>

## 12.8.7 Data Recovery

### DESCRIPTION

In the event of data loss due to hardware failure, it is still possible to recover data from your storage device if it is still useable.

1. On the storage device that failed, navigate to **C:\Users\%USERNAME%\AppData\Local\Devolutions** and copy the entire **RemoteDesktopManager** or **RemoteDesktopManagerFree** folder.
2. This folder will contain the local data source (SQLite or XML) as well as your configuration file.
3. Copy/Paste this folder at the same place on your new computer and you should retrieve your data.



The path mentioned in this topic are for those that have installed using the default settings. The best way to locate your configuration folder is to use **File – Options – Advanced**, in this form you will find an hyperlink near the bottom. This opens your configuration folder.



File based data sources (XML, SQLite, etc) are by default stored in that configuration folder. As a precaution, go through each data source in **File – Data sources** and have a look at the local path (if any). Any file that is in the configuration folder should be copied to ensure full data recovery.

## 12.8.8 Data Sources

### DESCRIPTION

This chapter contains data source related troubleshooting. Since Remote Desktop Manager supports such a wide array of data sources, there can be multiple causes for connectivity issues.

### INITIAL TROUBLESHOOTING

#### THE NAME OF THE DATA SOURCE IS ENTERED INCORRECTLY

For those data source types that need a host name, please ensure it is typed correctly.

#### THE MACHINE IS UNABLE TO RESOLVE THE NAME OF THE DATA SOURCE HOST USING DNS

For data source types that need a host name, please ensure that the name you have provided does resolve by the DNS server which it is linked to, not only your current network connection, but all connections that you will use Remote Desktop Manager over.

In general, PING is a poor testing tool because the server may have been configured to ignore PING requests. Use NSLOOKUP to help identify the issue.

A common issue in a multi-domain environment is that you must use the Fully Qualified Domain Name (FQDN) of a server in order to reach it. (e.g. **srvname.domain.loc** instead of **srvname**)

Another common issue is that your DNS cache is corrupted, in that case you can open an elevated command prompt and use the following commands.

```
ipconfig /flushdns
ipconfig /registerdns
```

## OPENING A VPN HAS DISCONNECTED THE LOCAL LAN OR RENDERED THE DATA SOURCE UNREACHABLE

If the network administrator has deemed necessary to tunnel ALL traffic through the connection when a VPN is active, you will have to resort to using our [Offline](#) capabilities, ideally paired with our options to automatically Go offline on connection as can be seen in the Advanced section of the VPN entry type.

For a Web based VPN, ensure the routes are all valid, i.e. the path followed to reach the remote host is indeed going through the proper interface.

## AN ANTI-VIRUS OR FIREWALL IS BLOCKING THE APPLICATION

This may be hard to diagnose but sadly the support department can attest that it occurs quite often. Here are some items to monitor.



If you are in a position to do so, it may help to TEMPORARILY disable the AV and the Firewall. You must make an informed decision as to the risk that is involved in your situation. Always enable all security features as soon as you have ascertained if that component was causing the issue.

ISSUE	RESOLUTION
<b>Anti-Virus</b>	Set the AV to ignore Remote Desktop Manager, you could also exclude our local configuration folder.
<b>Firewall blocks RDM - all the time</b>	Create a rule to allow RDM to communicate with at the very least your data source host. Keep in mind that, if you use embedded browser sessions, Remote Desktop Manager must have access to the remote hosts on which you open pages.



ISSUE	RESOLUTION
<b>Firewall blocks RDM - specific network</b>	The firewall rules are tied to the category of the network profile ( <b>Public/Private/DomainAuthenticated</b> ), ensure that all your network profiles allow for connectivity. Use <b>netsh interface ip show interfaces</b> and <b>Set-NetConnectionProfile</b> for resolution.

#### 12.8.8.1 Database Schema

### DESCRIPTION

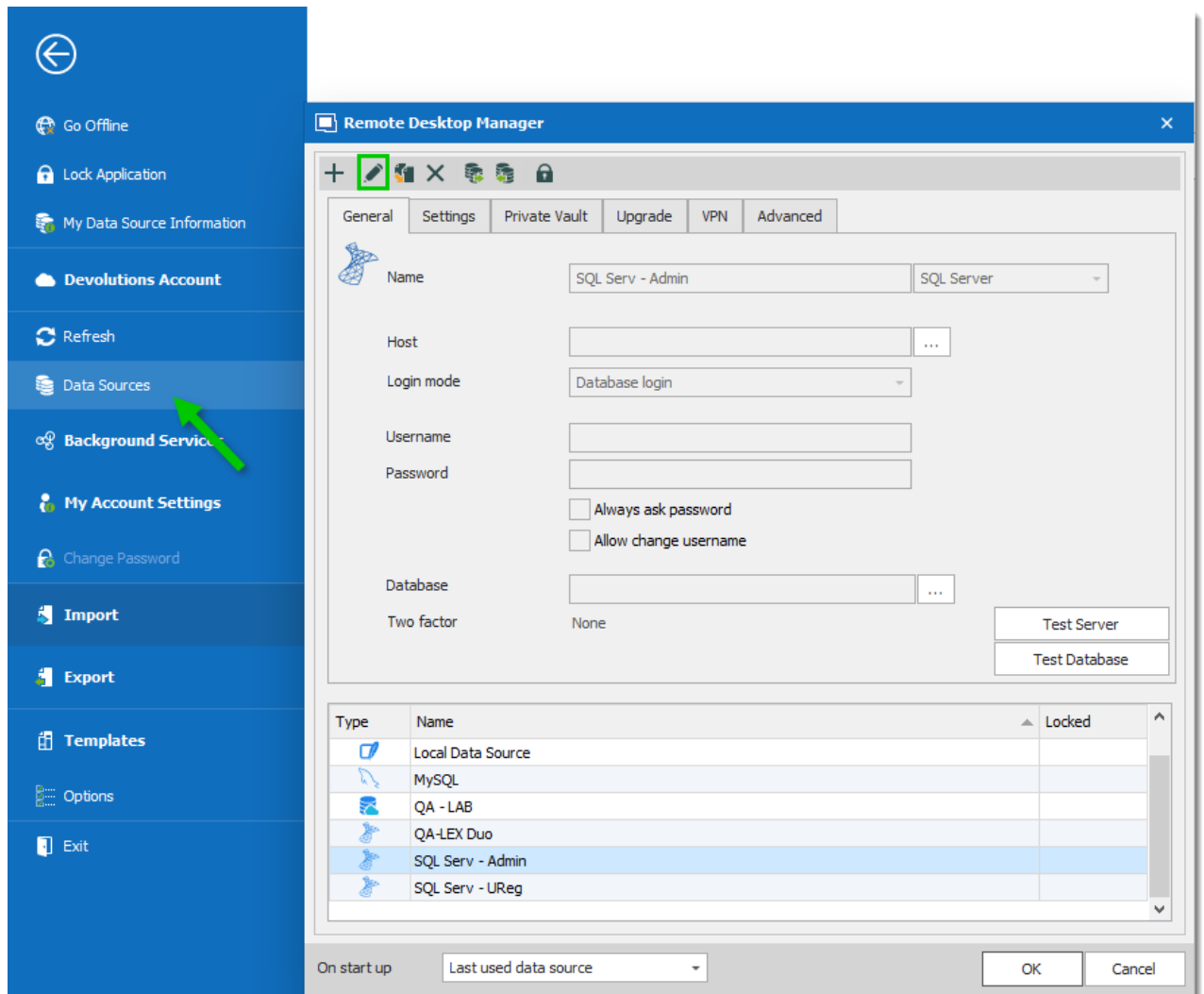
Sometimes the support staff will ask that the database schema.



This feature is only available for data sources that are backed by a database management system: [MariaDB](#), [SQL Azure](#), [SQL Server](#) and [MySQL](#).

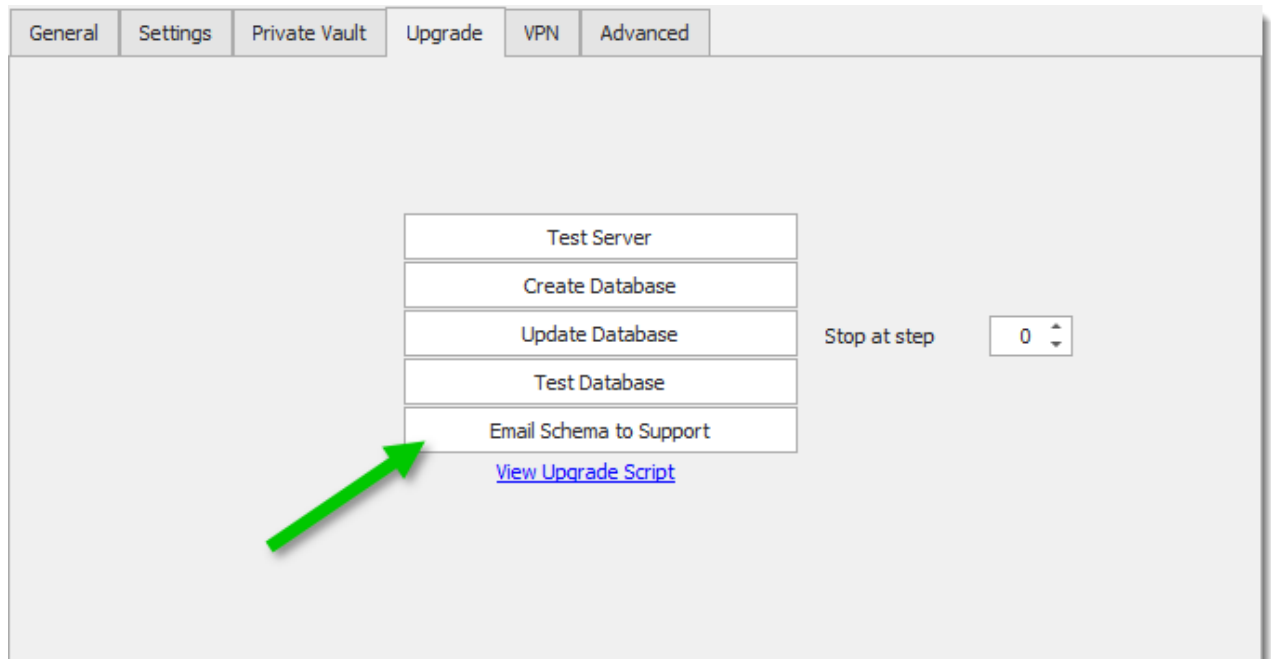
When requested by the Devolutions Support team during a support process, you may be asked to send us your database schema for thorough analysis of your issue.

1. Go in **File – Data Sources – Edit Data Source**.



### *Data Sources*

2. In the tab **Upgrade** click on **Email Schema to Support**.



*Email Schema To Support*

3. Fill in all the requested information and click on **OK**.

The image shows a dialog box titled 'Remote Desktop Manager - Send Database Schema Diagnostic to Support'. The main heading is 'Send Database Schema Diagnostic to Support'. Below the heading are three input fields: 'Email' with the value 'myaddress@myemail.com', 'Company' with the value 'MyCompany', and 'Name' with the value 'MyName'. Below these is a 'Message' label and a large text area for input. At the bottom right are 'OK' and 'Cancel' buttons.

*Database Schema*

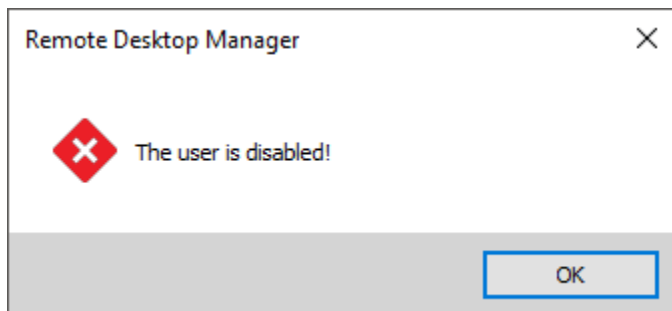
OPTION	DESCRIPTION
Email	Enter <b>your email address</b> so that the support team can contact you
Company	Enter your Company name
Name	Use the same title as the one first used to report the issue
Message	If you haven't described your issue before, enter a short description of it

#### 12.8.8.2 Devolutions Online Database

### DESCRIPTION

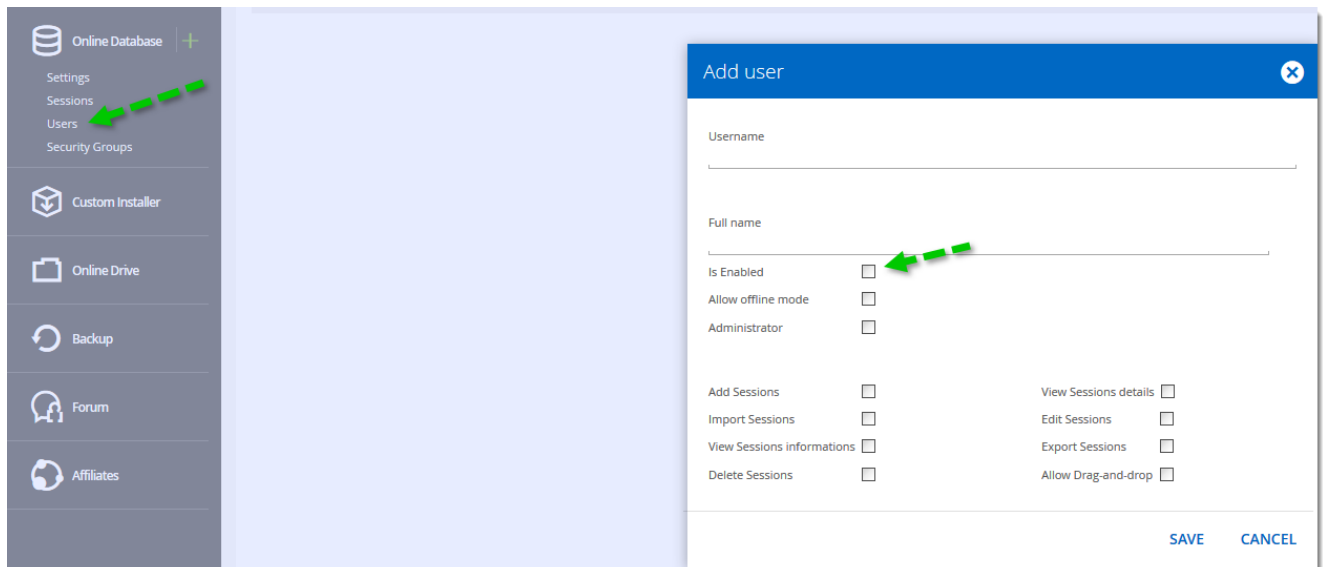
#### THE USER IS DISABLED!

When attempting to connect to the data source, you receive the error message below;



***DODB User Disabled***

On [Devolutions Customer Portal](#) in the User section, please ensure that the User is indeed Enabled.



*Devolutions Customer Portal - Users*

### 12.8.8.3 MySQL

## ERRORS

### CONNECTING TO MYSQL USING A PRIVATE CERTIFICATE

1. Create SSL keys as described in [Creating SSL Certs](#).
2. Create a client certificate.
  - 2.1. `openssl pkcs12 -export -in client-cert.pem -inkey client-key.pem -certfile cacert.pem -out client.pfx`
3. Grant privileges to the user as described in [Grant Syntax](#).
  - 3.1. `GRANT ALL PRIVILEGES ON test.* TO 'root'@'localhost' IDENTIFIED BY 'goodsecret' REQUIRE SSL;`
4. Run `certmgr.msc` and import the client certificate in the user store.
5. In the **Advanced** settings of your MySQL data source set the following values:

5.1. Certificate Store Location: CurrentUser

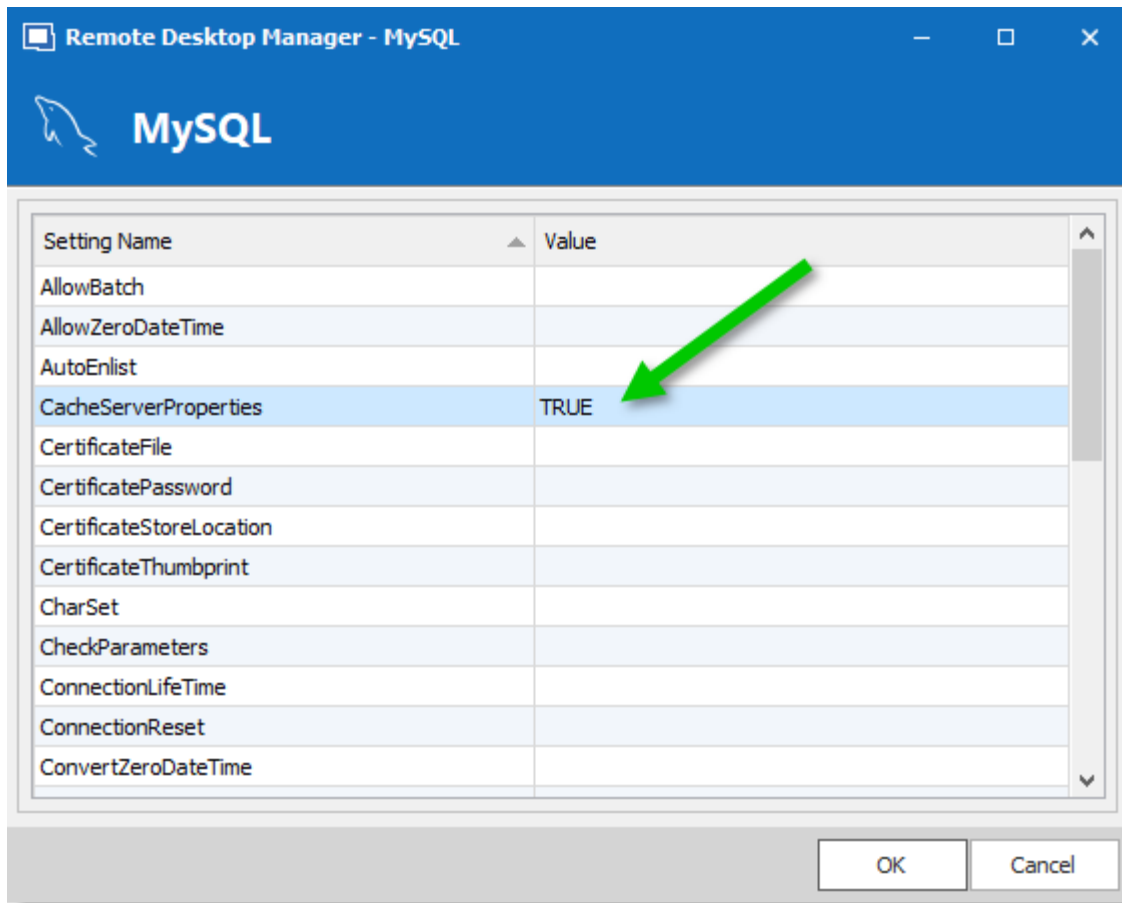
5.2. SSL Mode: Required

### **ERROR WHEN EDITING ENTRY**

**"MYSQL.DATA.MYSQLCLIENT.MYSQLEXCEPTION (0X80004005): PACKETS LARGER THAN MAX\_ALLOWED\_PACKET ARE NOT ALLOWED."**

When you have that type of error while attempting to edit or add a new entry on a MySQL database the problem is because your **Advanced** settings have been modified.

The resolution is to **Edit** your database, Select the **Advanced** tab and go to **More Settings**.



*CacherServerProperties Default Value*

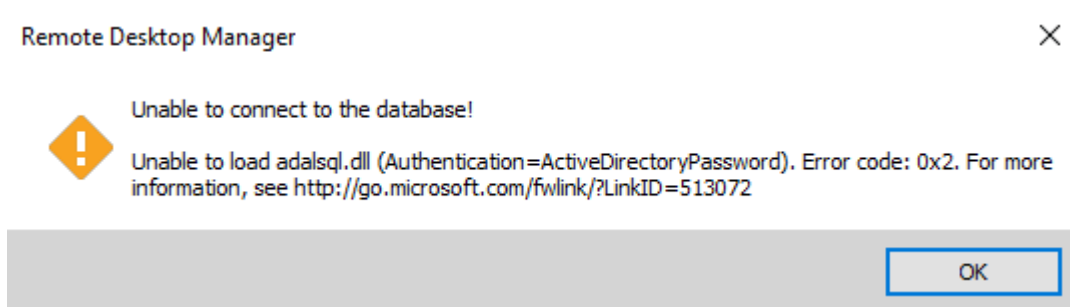
Erase the **Value** of the **CacheServerProperties** field.

#### 12.8.8.4 SQL Azure

## ISSUES

**"UNABLE TO LOAD ADALSQL.DLL  
(AUTHENTICATION=ACTIVEDIRECTORYPASSWORD). ERROR CODE: 0X2. FOR  
MORE INFORMATION, SEE [HTTP://GO.MICROSOFT.COM/FWLINK/?  
LINKID=513072](http://go.microsoft.com/fwlink/?linkid=513072)"**

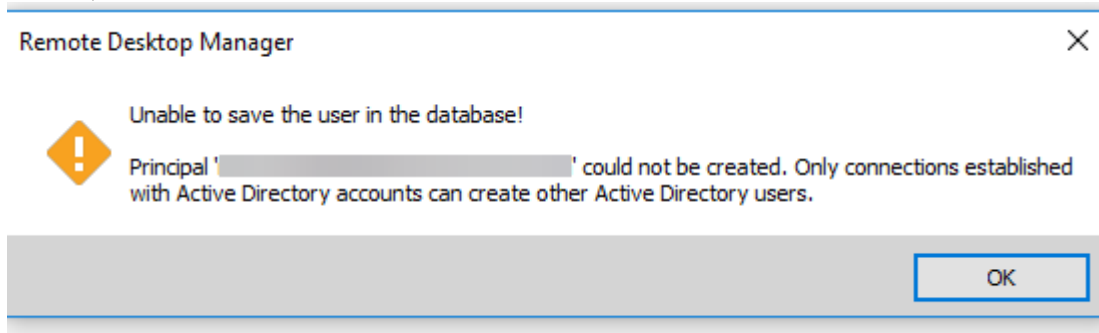
When attempting to use a SQL Azure data source, you receive the error message below;

*SQL Azure Error*

To resolve this issue, please have a look at the topic on [SQL Azure](#).

## **"PRINCIPAL ' ' COULD NOT BE CREATED. ONLY CONNECTIONS ESTABLISHED WITH ACTIVE DIRECTORY ACCOUNTS CAN CREATE OTHER ACTIVE DIRECTORY USERS."**

When creating a user with azure active directory account authentication, you see the error below;

*Azure AD Error*

You must first define your SQL Server Azure AD Admin via the Azure Portal, then login into Remote Desktop Manager using that Azure AD account, from there you will be able to create new Azure AD accounts (admin and non-admin). Those new admins will also be able to do the same.

For more information, please have a look at the topic [Configure SQL Azure AD Authentication](#).

12.8.8.4.1 SQL Azure: One or More Errors Occurred

## **DESCRIPTION**

## **PROBLEM**



After following the steps in [Configure Azure Active Directory App Registration](#), you receive the error message below:

**System.AggregateException: One or more errors occurred. --->**  
**System.AggregateException: One or more errors occurred.**

## SOLUTION

If you get this error, please send us your [Azure Active Directory app manifest](#) at [ticket@devolutions.net](mailto:ticket@devolutions.net) so that we can validate your configuration.

### 12.8.8.5 SQL Server

## DESCRIPTION

SQL Server is surely the most used repository within our community. Even though it is extremely easy to put in place, some decisions have a huge impact on its operation.

We have separated the concerns in two categories:

[SQL Server Connectivity](#)

[SQL Server Performance](#)

#### 12.8.8.5.1 SQL Server Connectivity

## CONTENT

- [New SQL Server installation](#)
- [Unable to connect to SQL Server](#)
- [A network-related or instance-specific error occurred...](#)
- [Universal Data Link \(.udl\) file](#)
- [Login failed for user Reason: Token-based server access validation failed](#)
- [Login failed. The login is from an untrusted domain and cannot be used with windows authentication](#)

## ISSUES

### NEW SQL SERVER INSTALLATION

SQL Server installs with limited network connectivity. Therefore, when initially installed, the Database Engine cannot be accessed from another device.

#### **Allow Remote Access**

On older versions of SQL Server, remote connections must be allowed manually. Follow these [instructions](#) to enable connectivity.

#### **Enable protocols**

To connect to the Database Engine from another device, a protocol, such as TCP/IP, must be enabled.

1. In the **SQL Server Configuration Manager**, expand **SQL Server Network Configuration**.
2. Select an instance.
3. Right-click the desired protocol, then select **Enable**.

#### **Open a communication port in the firewall**

To connect to an SQL Server from another device, a communication port must be opened in the firewall.

1. In the **Start** menu, type **WF.msc** and press **Enter** to open the **Windows Firewall with Advanced Security**.
2. Select **Inbound Rules** in the left pane.
3. Right-click **Inbound Rules**, then select **New Rule....**
4. In the **Rule Type** page, select **Port**, then click **Next**.
5. In the **Protocol and Ports** page, select **TCP**. Select **Specific local ports**, then type the port number of the instance of the Database Engine. The SQL Server default instance listens on port **1433**. Click **Next**.
6. In the **Action** page, select **Allow the connection**, then click **Next**.
7. In the **Profile** page, select the profiles that describe the computer connection environment, then click **Next**.
8. In the **Name** page, enter a **Name** and **Description** for the rule, then click **Finish**.

### UNABLE TO CONNECT TO SQL SERVER

1. Go in **Help – Application Logs** to see if relevant error messages are present. There's a good chance that you will see [A network-related or instance-specific error occurred...](#)
2. Create a Universal Data Link (\*.udl) file to test your SQL Connection (see [Universal Data Link \(.udl\) file](#)).
3. Anti-virus or Firewall is blocking the application.

## TEST THE CONNECTION WITH A UNIVERSAL DATA LINK (\*.UDL) FILE

This will test that the instance is allowing your **workstation** to connect. **Firewalls and anti-virus** software may still **prevent** Remote Desktop Manager from accessing the network even though the Universal Data Link test is conclusive.

1. Open the **Windows File Explorer**.
2. Navigate to the folder in which the \*.udl file will be stored.
3. Select the **Home** tab. Using the **New item** menu, create a **Text Document**.
4. Rename this file and change its file extension to \*.udl.  
File name extensions might be hidden by the **Windows File Explorer**.  
To show the file name extensions, in the **View** tab of the **File Explorer**, enable the **File name extensions** option.



Do not include the space characters in the name of the file.



A warning that changing file extensions can cause files to become unusable might be displayed. Disregard it.

5. Double-click the \*.udl file to open the **Data Link Properties** dialog box.
6. In the **Provider** tab, select the **Microsoft OLE DB Provider for ODBC Drivers** provider.
7. In the **Connection** tab, select Use connection string, and enter a custom connection string.  
Example of valid connection string:  
`Driver={SQL Server};Server=myServerAddress;Database=myDataBase;Uid=myUsername;`
8. Use the **Advanced** tab to view and set other initialization properties for your data.
9. Use the **All** tab to review and edit all OLE DB initialization properties available for your OLE DB provider.
10. In the **Connection** tab, use the **Test connection** button to test the SQL Server connectivity.

11. Click **OK** to save the connection string to the Universal Data Link (.udl) file.

## LOGIN FAILED FOR USER – REASON: TOKEN-BASED SERVER ACCESS VALIDATION FAILED

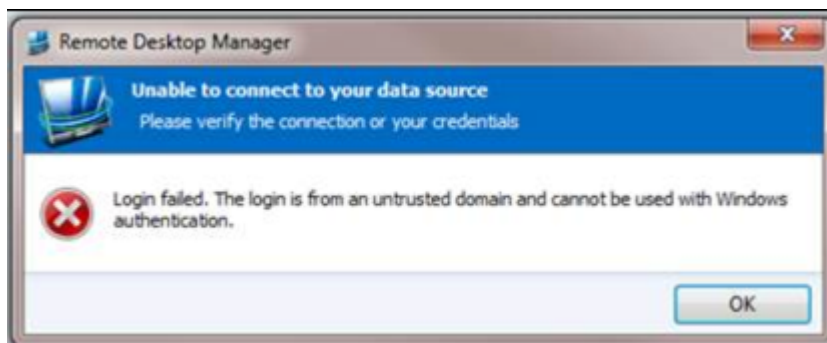
Finding the true reason for this is quite a process. A web search reveals so many solutions to attempt, and it is easy to get lost in all those steps. The thing to keep in mind is that the error message is misleading and the cause is often a simple thing.

The first step is to ensure that the issue is not unique to Remote Desktop Manager. Testing with a [Universal Data Link file](#) as shown above will prove that the workstation configuration is not the issue.

When granting rights to the DB using AD group membership and one of your users has that error message, you must check privileges for ALL the AD groups that he belongs to. Anything with an explicit DENY must be evaluated carefully. The query below will help identify these occurrences.

```
select princ.*, perm.* from sys.server_principals princ, sys.server_permissions perm
where perm.grantee_principal_id = princ.principal_id
AND state_desc = 'DENY'
```

## LOGIN FAILED. THE LOGIN IS FROM AN UNTRUSTED DOMAIN AND CANNOT BE USED WITH WINDOWS AUTHENTICATION.



*Error Message*

The following error message appear when you can't access Remote Desktop Manager data source with Integrated Authentication when connected to a Dialup VPN.

## SOLUTION

1. Locate your VPN connections (\*.pbk) file.
2. You can find it here: **%APPDATA%\Microsoft\Network\Connections\Pbk** or if you have it set to allow all users to use the connection, you can find it here: **C:\ProgramData\Microsoft\Network\Connections\Pbk**
3. Edit the \*.pbk file with a text editor and find the line UseRasCredentials=1
4. Disable this setting by changing the 1 to 0: UseRasCredentials=0

## A NETWORK-RELATED OR INSTANCE-SPECIFIC ERROR OCCURRED...

This error message means that the server could not be reached, the possible causes are numerous.



These steps are for Client side troubleshooting exclusively. For full guidance on this issue please consult [this article on Technet](#)



If the error message indicates that the Named Pipes are in use and you are accessing a remote server, ensure that the TCP IP protocol is used simply by adding **tcp:** in front of the instance name, i.e. **tcp:vmtxg.database.windows.net**

CAUSE	DIAGNOSTIC
Server name mistyped (Known as the Instance name).	<a href="#">Universal Data Link (.udl) file</a>

CAUSE	DIAGNOSTIC
<b>Only server name is specified when there is no Default instance on that server.</b>	<a href="#">Universal Data Link (.udl) file</a>
<b>Is the SQL Server up and running.</b>	<a href="#">Universal Data Link (.udl) file</a>
<b>SQL Server is listening on a non-standard port.</b>	<a href="#">Universal Data Link (.udl) file</a>
<b>Anti-Virus blocking Remote Desktop Manager.</b>	Check in the Anti-Virus logs to see blocked threats.
<b>Firewall is preventing Remote Desktop Manager to connect.</b>	Adjust your firewall to allow RemoteDesktopManager.exe and RemoteDesktopManager64.exe to communicate with external services.

## 12.8.8.5.2 SQL Server Performance

## DESCRIPTION

Whenever the performance of queries against SQL Server decreases, check on the following:

### SIZE OF DATABASE FILES

If you transaction log file is enormous, it may be that the recovery model of the database is set to FULL, which means that it requires regular backups in order to clean up past transactions.

You can confirm this is in the properties of the DB itself.

The most urgent step is to perform a full Backup of the DB.

Run the following statement against the database.

```
exec sp_spaceused
```

## 12.8.9 DB Upgrades

### ERROR

**SQLLEXCEPTION - TIMEOUT EXPIRED. THE TIMEOUT PERIOD ELAPSED PRIOR TO COMPLETION OF THE OPERATION OR THE SERVER IS NOT RESPONDING.**

Presence of sizable **historical** or **log** data in the DB can cause this error to be triggered. Please consult [Clean up](#) and prune data as you see fit.

## 12.8.10 FIPS (Encryption)

### ERROR

**“SYSTEM.INVALIDOPERATIONEXCEPTION: THIS IMPLEMENTATION IS NOT PART OF THE WINDOWS PLATFORM FIPS VALIDATED CRYPTOGRAPHIC ALGORITHMS”:**

The problem could be related to the FIPS mode enabled.

Remote Desktop Manager uses the AES/Rijndael encryption and SHA-256 hashing algorithms, which are implemented by the Microsoft .NET Framework. If the local security policy on your system enforces FIPS compliant implementations, Remote Desktop Manager cannot run. As a result, you will receive this error message.

### SOLUTION 1

To fix this error, configure the Local Security Policy on your system to allow FIPS non-compliant algorithm implementations. Here are the steps:

1. Go to **Control Panel > Administrative Tools > Local Security Policy > Open Local Policies > Security Options**

2. Disable the option "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing."



Some software (i.e. Cisco VPN Anyconnect) requires the use of FIPS. If this is your case, you must implement the alternative solution described below.

## SOLUTION 2

Inside Remote Desktop Manager's installation folder, create a text file named ***RemoteDesktopManager.exe.config*** containing the following:

```
<configuration>
  <runtime>
    <enforceFIPSPolicy enabled="false"/>
  </runtime>
</configuration>
```

### 12.8.11 KeePass

## ERRORS

### YOU ARE PROMPTED TWICE TO OPEN KEEPASS WHEN CONNECTING TO A SESSION

In KeePass, click on ***Tools -> Options***, go in the Advanced tab and uncheck **Remember and automatically open last used database on startup**.

### THE FOLLOWING PLUGIN IS INCOMPATIBLE WITH THE CURRENT KEEPASS VERSION

- Make sure that the installation of KeePass was successful.



- Delete all the ***RemoteDesktopManager.Connector.dll*** and ***RemoteDesktopManagerPlugin.dll*** files that you may have in the installation folder of KeePass. (We have since then modified how Plug In functions, and these files should no longer exist).

## 12.8.12 LogMeIn

### ERRORS

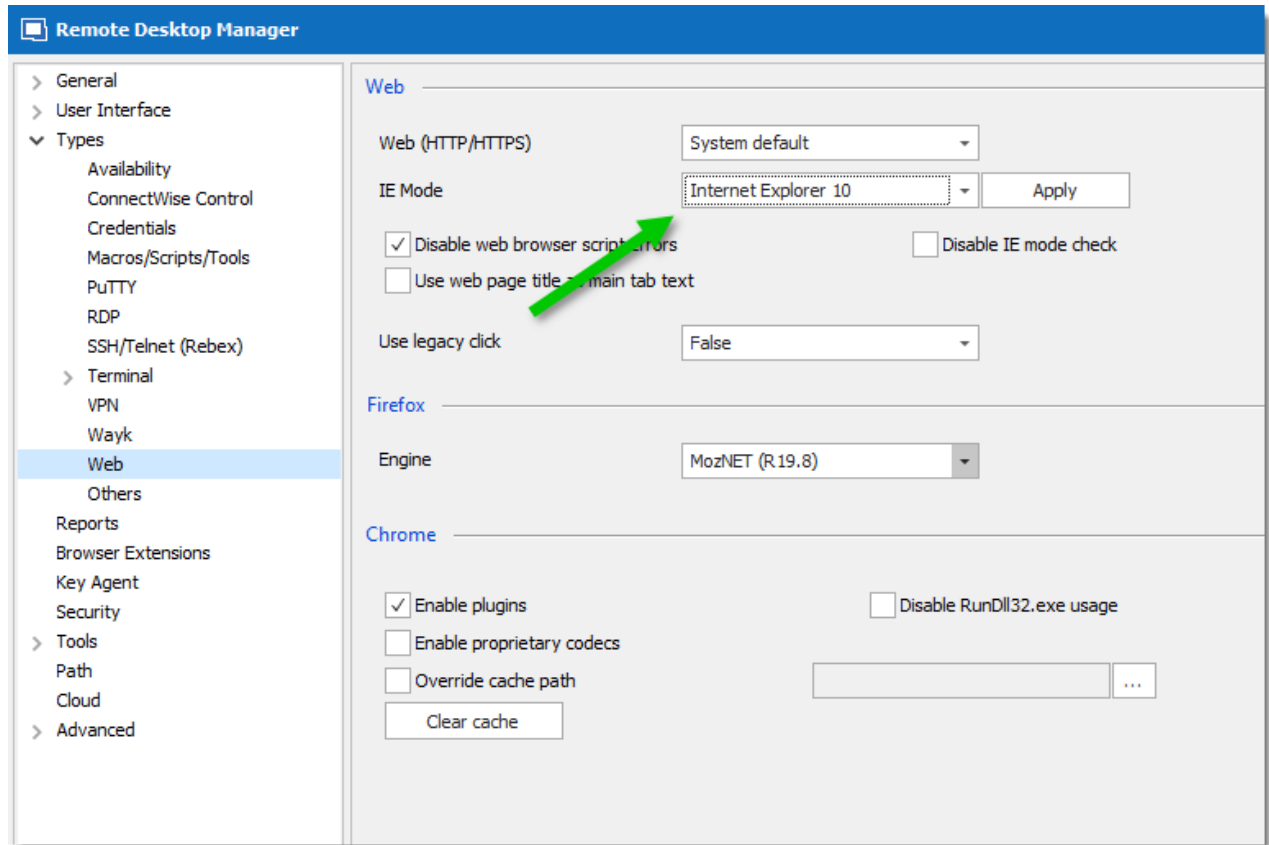
#### A LOGMEIN PLUGIN MAY BE REQUIRED WHEN LAUNCHING LOGMEIN IN EMBEDDED MODE.

1. Copy the **LogMeIn** portal URL from your **LogMeIn** session.
2. Close Remote Desktop Manager.
3. Open Internet Explorer as an administrator.
4. Paste the LogMeIn portal URL in Internet Explorer and launch it.
5. Internet Explorer should prompt to install the LogMeIn ActiveX.
6. Install the LogMeIn ActiveX.
7. Access the LogMeIn portal URL from your Internet Explorer window to be sure that the ActiveX as been installed properly.
8. Close Internet Explorer.
9. Open Remote Desktop Manager and launch your LogMeIn session.

You should not be prompted for the LogMeIn ActiveX anymore.

#### COMEXCEPTION - REQUESTED RESOURCE IN USE. (EXCEPTION FROM HRESULT: 0X800700AA)

Change the IE emulation mode in **File – Options – Types – Web** to use **Internet Explorer 10**.



IE Mode

### 12.8.13 Microsoft Office

## ERROR

### WHEN THE EMBEDDED MODE IS USED, AN ERROR IS DISPLAYED THAT OFFICE HAS TO BE INSTALLED, YET IT ALREADY IS.

Under certain conditions which we cannot identify, an **Office 2013 32 bit Edition** installation on a **64 bit system** may miss registry keys to allow for hosting Office Documents in ActiveX controls. This can be confirmed by going in **Help – Application Logs** to view the full error message. It should be something like `System.Runtime.InteropServices.COMException: The associated COM server does not support ActiveX Document embedding.`

To resolve this, you have to create a reg file with the content below and merge it in your registry. A restart may be required. As a preliminary step you could open the registry to confirm that the **DocObject** keys are indeed missing. The keys below are respectively for : Word, Excel, PowerPoint, Visio, and Project.

Windows Registry Editor Version 5.00

```
[HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{F4754C9B-64F5-4B40-8AF4-679732AC0607}\DocObject]
```

[HKEY\_CLASSES\_ROOT\Wow6432Node\CLSID\{00020830-0000-0000-C000-000000000046}\DocObj

[HKEY\_CLASSES\_ROOT\Wow6432Node\CLSID\{CF4F55F4-8F87-4D47-80BB-5808164BB3F8}\DocObj

[HKEY\_CLASSES\_ROOT\Wow6432Node\CLSID\{00021A15-0000-0000-C000-000000000046}\DocObj

[HKEY\_CLASSES\_ROOT\Wow6432Node\CLSID\{74B78F3A-C8C8-11D1-BE11-00C04FB6FAF1}\DocObj

## 12.8.14 Microsoft RDP

### THE MICROSOFT RDP CLIENT IS NOT WORKING PROPERLY

Please consult our [Corrupted System File](#) topic.

### AUTOMATIC LOGON

Automatic logon troubleshooting is in the [Automatic Logon](#) topic.

### SESSIONS WORK USING MSTSC.EXE BUT NOT IN REMOTE DESKTOP MANAGER

Please consult [Sessions work using mstsc.exe but not in RDM](#).

### ERRORS

**“CANNOT COPY <FILENAME>: WINDOWS CANNOT FIND ‘%1!|S!’. CHECK THE SPELLING AND TRY AGAIN, OR TRY SEARCHING FOR THE ITEM BY CLICKING THE START BUTTON AND CLICKING SEARCH”**

This is a bug in the Microsoft Remote Desktop Client. The workaround is to enable the Smart Card even if it's not required for the connection.

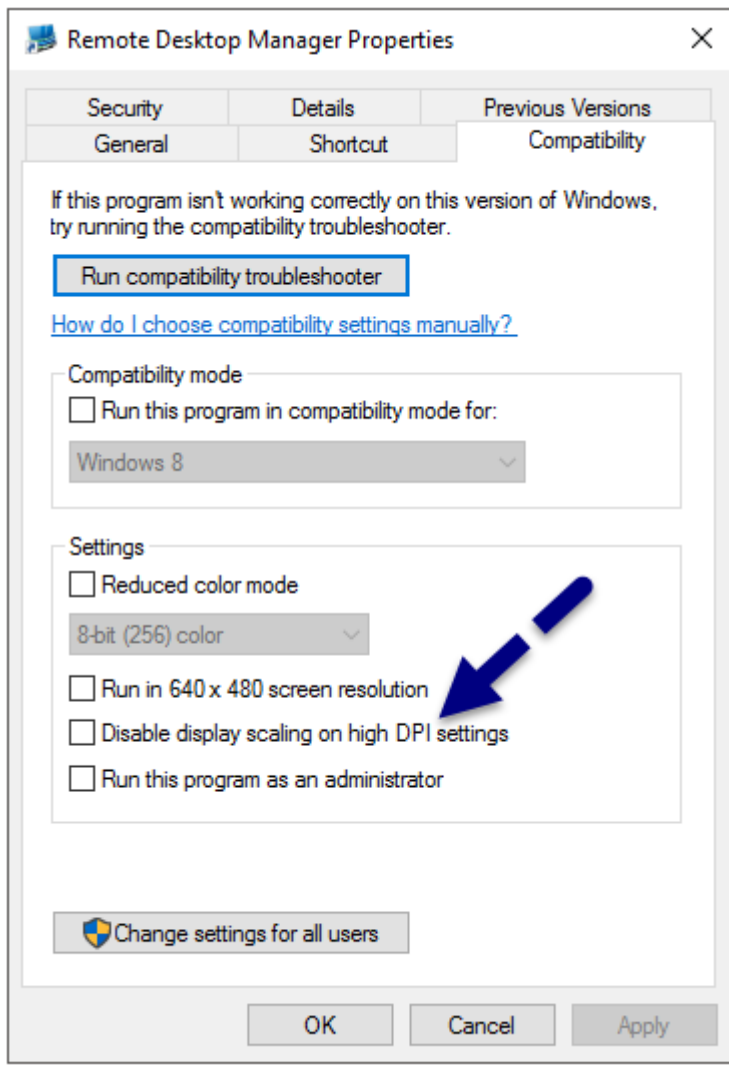
**I RECEIVE AN ERROR WHEN I TRY AND GET SESSION DETAILS, OR WHEN I EXECUTE A LOGOFF WITH AN RDP SESSION. HOW DO I FIX THIS?**

Please read the information [Logoff Access Denied](#).

## **SCREEN AREAS UNRESPONSIVE IN EMBEDDED SESSIONS.**

This most often occurs on systems that use a DPI setting of more than 100%. To disable scaling in RDM you must adjust the compatibility settings on the Windows shortcut for RDM.

1. Right-click on the shortcut to RDM.
2. Select Properties.
3. Go to the "Compatibility" tab.
4. Check "Disable display scaling on high DPI settings".



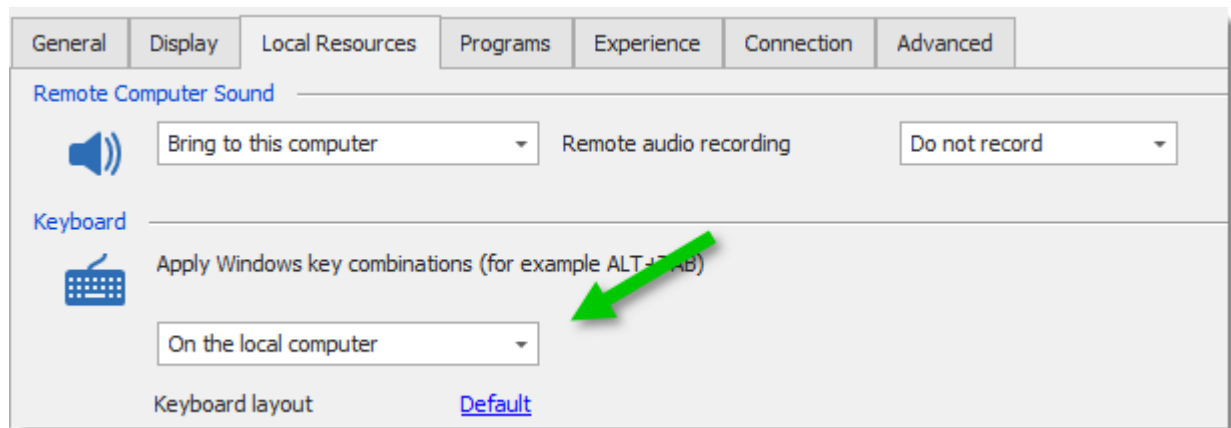
Compatibility Tab

## I HAVE MULTIPLE SESSIONS TO THE SAME COMPUTER WITH DIFFERENT CREDENTIALS, BUT IT ALWAYS USES THE LAST ONE I ENTERED.

This issue stems from the fact that the Windows Credential repository holds only one entry per Windows user for a remote computer. If you use the **Embedded (tabbed)** display mode and store the password in the database, you'll be able to work around that limitation.

## THE WINDOWS SHORTCUTS ARE BEING PERFORMED IN THE SESSION BUT ALWAYS ON MY COMPUTER.

You must configure the Keyboard setting in the **Local Resources** tab of the session settings. You can select "On the remote computer" or "In full screen only" according to your personal preferences.



*Local Resources Tab*

## **COPY/PASTE BETWEEN A REMOTE SESSION AND MY LOCAL COMPUTER STOPPED WORKING**

This issue arises when a program called RDPCLIP becomes unstable. You can kill its process and launch a new instance.

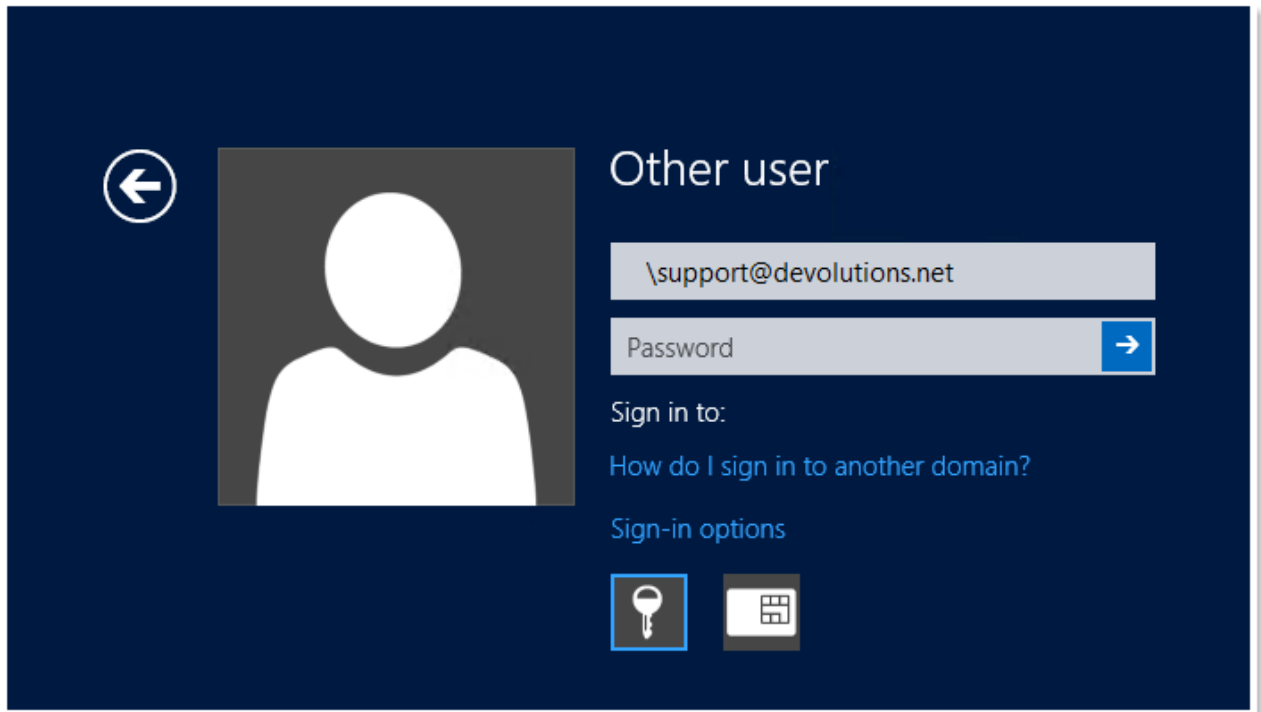
1. On the affected system, load up task manager (right click in taskbar and select Task Manager).
2. Go to the **Processes Tab**.
3. Select **rdpclip.exe**.
4. Click **End Process**.
5. Go to the **Application Tab**.
6. Click **New Process**.
7. Type **rdpclip**.
8. Click **Ok**.

## **COPY/PASTE OPERATION WITHIN THE REMOTE HOST ARE EXTREMELY SLOW**

As strange as it may seem, we've isolated the issue to "Serial Ports" being enabled. Turn off Serial port sharing and see if the performance is improved.

## **LOG ON USERNAME ON WINDOWS SERVER 2012 IS SENT INCORRECTLY**

When you try to connect to a Windows Server 2012, you see the following result below. There are several spaces that shouldn't be there.



*Windows Server 2012 Log In*

To fix this issue, go in **Properties – General – Advanced** and change the option **Enable CredSSP support** to **True**.

The screenshot shows the 'Advanced' tab of the RDP Session configuration window. The 'Enable CredSSP support' dropdown is highlighted with a green box and set to 'True'. Other settings include Log off mode (Default), Automatically logoff when disconnecting (Default), Reconnect mode (Standard), RDP Version (Latest), Minimal input send interval (100 ms), and checkboxes for Restricted admin mode, Prompt for credentials on client, Background input, Enable super pan, and Public mode. The Connection Broker - High Availability section includes fields for Workspace ID, Alternate full address, Load balance info, and a checkbox for Use redirection server.

RDP Session Advanced Tab

#### 12.8.14.1 Automatic Logon

### DESCRIPTION

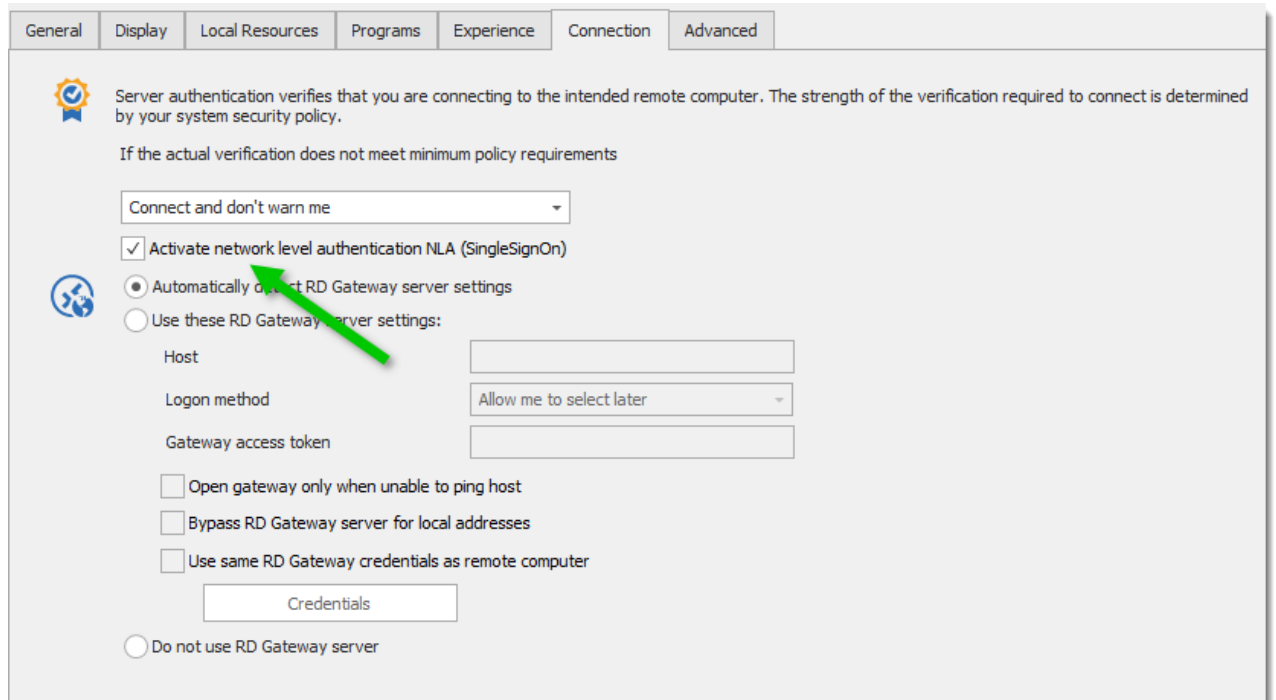
Sometimes the automatic logon does not function and your credentials are requested by the remote system. Here are some steps to help identify the issue. Support for automatic logon was introduced on Windows 2003/XP, so ensure you are trying to connect to these or later versions. Windows 2000 does not support the automatic logon.

### RDP SESSIONS CONNECT SUCCESSFULLY WHEN IN EXTERNAL MODE, BUT NOT IN EMBEDDED MODE

This issue may be caused by a bad authentication negotiation because in some cases **Single Sign On (SSO)** requires **Network Level Authentication (NLA)**. It can happen when prompting for credentials and when using automatic logon. Please activate **Network Level**



**Authentication** in the **Connection** tab of your session. You might also have to check the **Public Mode** option in the **Advanced** tab to make it work.



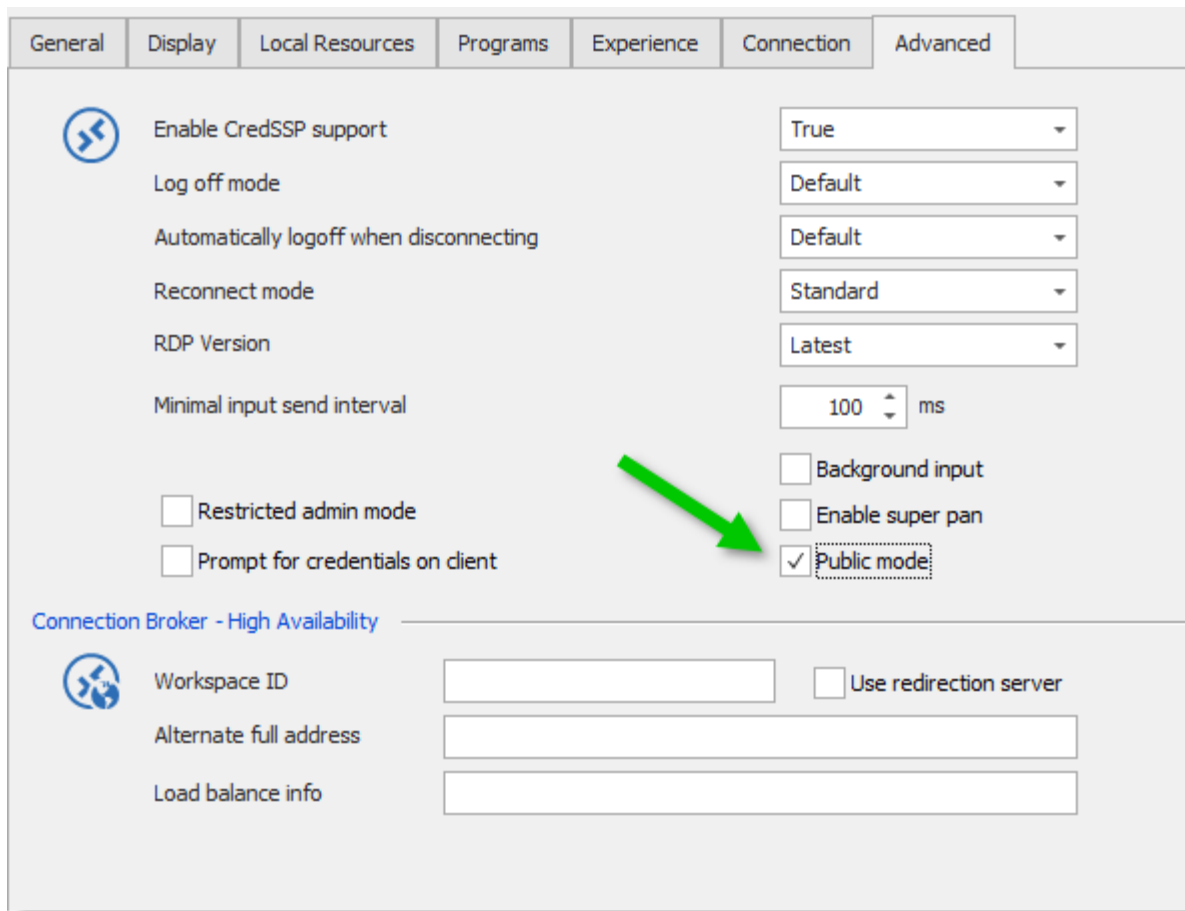
The screenshot shows the 'Connection' tab of a Remote Desktop Connection window. At the top, there are tabs for General, Display, Local Resources, Programs, Experience, Connection, and Advanced. The 'Connection' tab is active. It features a gear icon and text explaining server authentication. Below this, a dropdown menu is set to 'Connect and don't warn me'. A checkbox labeled 'Activate network level authentication NLA (SingleSignOn)' is checked. To the left of this checkbox is a blue globe icon. Below the checkbox, there are two radio button options: 'Automatically connect RD Gateway server settings' (which is selected) and 'Use these RD Gateway server settings:'. The second option has fields for 'Host', 'Logon method' (set to 'Allow me to select later'), and 'Gateway access token'. Below these fields are three unchecked checkboxes: 'Open gateway only when unable to ping host', 'Bypass RD Gateway server for local addresses', and 'Use same RD Gateway credentials as remote computer'. A 'Credentials' button is located below the third checkbox. At the bottom, there is a radio button option 'Do not use RD Gateway server'.

*Network Level Authentication*



See also : [Network Level Authentication](#), [Configure NLA for Remote Desktop Services Connections](#).

## THE CONNECTION WAS DENIED BECAUSE THE USER ACCOUNT IS NOT AUTHORIZED FOR REMOTE LOGIN

We have discovered that enabling the **Public Mode** option in the **Advanced** tab resolves the issue.



The screenshot shows the 'Advanced' tab of the 'RDP Session' configuration window. The 'Public mode' checkbox is checked and highlighted with a green arrow. The 'Connection Broker - High Availability' section is also visible.

General	Display	Local Resources	Programs	Experience	Connection	Advanced
<p> Enable CredSSP support <span>True</span></p> <p>Log off mode <span>Default</span></p> <p>Automatically logoff when disconnecting <span>Default</span></p> <p>Reconnect mode <span>Standard</span></p> <p>RDP Version <span>Latest</span></p> <p>Minimal input send interval <span>100</span> ms</p> <p><input type="checkbox"/> Restricted admin mode</p> <p><input type="checkbox"/> Prompt for credentials on client</p> <p><input type="checkbox"/> Background input</p> <p><input type="checkbox"/> Enable super pan</p> <p><input checked="" type="checkbox"/> <b>Public mode</b></p> <p><b>Connection Broker - High Availability</b></p> <p> Workspace ID <span></span> <input type="checkbox"/> Use redirection server</p> <p>Alternate full address <span></span></p> <p>Load balance info <span></span></p>						

*RDP Session - Advanced Tab*

## ENSURE CREDENTIALS ARE ENTERED PROPERLY.

RDM allows for advanced credential management. Depending on your choice of: **Default**, **Credential repository**, **Embedded** or **Inherited** ensure the credentials are properly entered.

General | Display | Local Resources | Programs | Experience | Connection | Advanced

Host: vwindsrv-sql ... Port: [Default](#)

RDP type: Normal

Username: Test

Domain:

Password:

☐ Always ask password

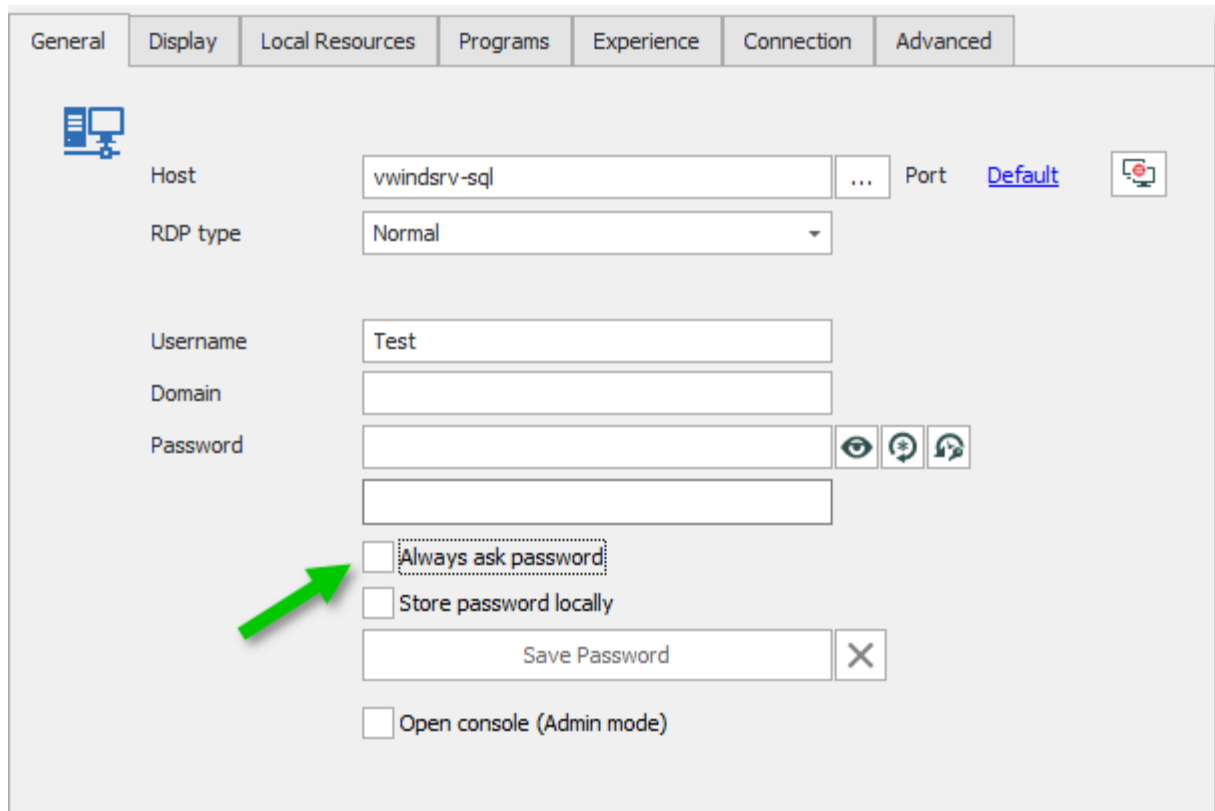
☒ Store password locally

Save Password X

☐ Open console (Admin mode)

*Storing your Password*

**ENSURE THAT "ALWAYS ASK PASSWORD" IS NOT CHECKED.**



Microsoft Remote Desktop - General Tab

## ENSURE A SYSTEM POLICY DEFINED ON THE HOST IS NOT REQUIRING EXPLICIT CREDENTIAL ENTRY

The host server can be configured to always require the credentials to be entered in an interactive manner by the user. Ask your system administrator to confirm if this is the case.

Choose the instructions depending on the server operating system. Note that there are often multiple ways to configure the host (WMI, Scripting, etc), but the group policies are the preferred method. Therefore the links are for the articles describing group policy solutions when they are available.

APPLIES TO	LINK
<b>Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 with SP1, Windows Server 2003 with SP2</b>	Microsoft ended support for Windows Server 2003 on July 14, 2015. This change has affected your software updates and security options.
<b>Windows Server 2008</b>	<a href="#">Group Policy Settings for Remote Desktop Services in Windows Server 2008</a>
<b>Windows Server 2008 R2</b>	<a href="#">Group Policy Settings for Remote Desktop Services in Windows Server 2008 R2</a>
<b>Windows 2012</b>	<p>The settings are on the Session Collection Properties.</p> <p>More info on the new Remote Desktop Services:</p> <p>Guide to configure the <a href="#">Quick Deployment</a>:</p> <p><a href="#">Test Lab Guide: Remote Desktop Services Session Virtualization Quick Start</a></p>

## **SINGLE SIGN ON WORKS FOR TS WEB ACCESS, HOWEVER, THEY CANNOT BE SHARED ACROSS TS WEB ACCESS AND TS OR TS GATEWAY.**

You must adjust a group policy to allow that. Please follow the directions in <http://blogs.msdn.com/b/rds/archive/2007/04/19/how-to-enable-single-sign-on-for-my-terminal-server-connections.aspx>

## **REMOTE DESKTOP MANAGER HANGS WHEN PROMPTED TO ENTER CREDENTIALS.**

When you are prompted with this credential box, Remote Desktop Manager hangs.



*Windows Security*

## PROBABLE CAUSE

The issue seems to occur with users using a Wacom Bamboo Fun Pen & Touch tablet. Latest drivers are installed.

When users with a Wacom tablet click on a session with an expired password in the Private Vault or a non domain joint server, forcing Remote Desktop Manager (or in fact RDP) displaying a credential popup, Remote Desktop Manager freezes.

When the user does the very same action with a regular mouse, everything goes fine.

The problem appears to be in the Wacom settings along with some windows settings to use Windows Ink as handwriting.

When Use Windows Ink was disabled, Remote Desktop Manager didn't freeze anymore when displaying a credential box.

It did also solve problems with the focus of other applications.

### 12.8.14.2 Cannot Store Password on Local Computer

## DESCRIPTION

**IN A MICROSOFT RDP SESSION, YOU WANT TO STORE THE PASSWORD ON THE LOCAL COMPUTER, HOWEVER THE "SAVE PASSWORD" BUTTON IS GRAYED OUT.**



Please note that this setting may have been set by a group policy. If you find the value but do not know the reason why it is set, a Domain Administrator may have set it. We do not condone bypassing corporate policies.

Click on Start \ Run and type regedit to open the registry editor. Navigate to HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows NT\Terminal Services\DisablePasswordSaving key and change the value to 0.

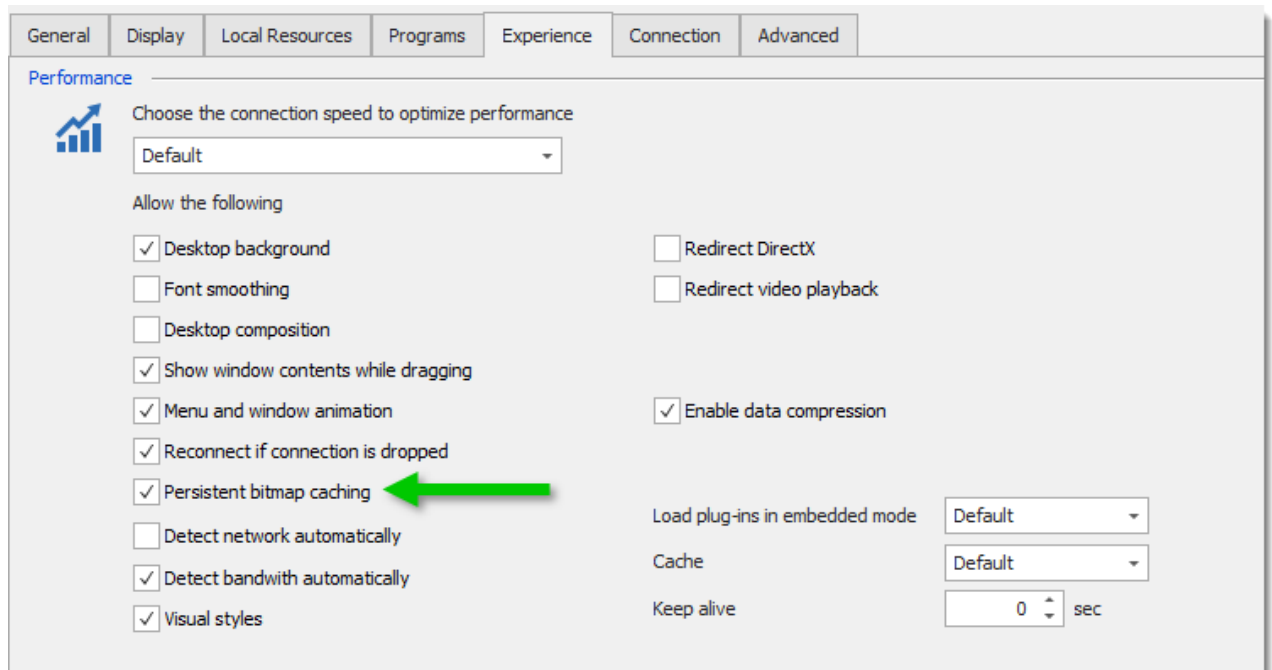
Make sure you've checked the **Store password locally** feature and that you have text in the **Host** field.

#### 12.8.14.3 Display Issues

## DESCRIPTION

### THE REMOTE SESSION'S CONTENT IS BLURRY

Uncheck **Persistent bitmap caching** under the **Experience** tab in the properties of your RDP session.

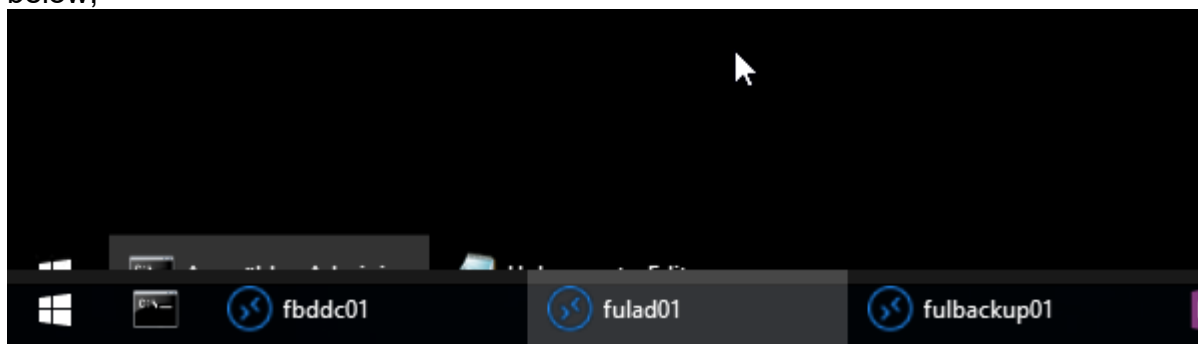
*Bitmap Caching*

## SESSIONS ARE FLICKERING, TURNING BLACK OR RANDOMLY SHUFFLES WHILE WORKING

We have identified the CA DSM Agent Suite for desktop management as being the culprit for those who use this product. The remote control agent from this product seems to interfere with the modern GUI of Remote Desktop Manager. If you stop the agent, the problem should go away.

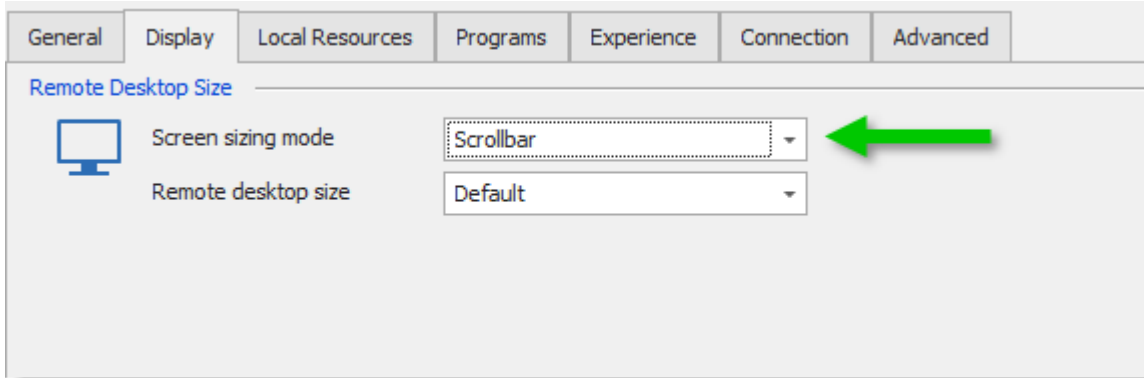
## REMOTE TASKBAR IS HIDDEN BY THE ONE OF YOUR LOCAL MACHINE

The taskbar on your remote system is hidden by the one from your local machine as shown below;

*Windows Taskbar*



Simply set this option as shown below in the properties of your RDP session under the **Display** tab.



*RDP Properties*

#### 12.8.14.4 Keyboard not working

### DESCRIPTION

#### KEYBOARD NOT WORKING ON A WINDOWS 7 COMPUTER

Some users have experienced issues where their keyboard would not work on the Windows 7 system.

The solution is to update the RDP client on Windows 7.

KB's must be installed in the following order: KB2574819, KB2830477, KB2857650, KB2913751, KB2923545

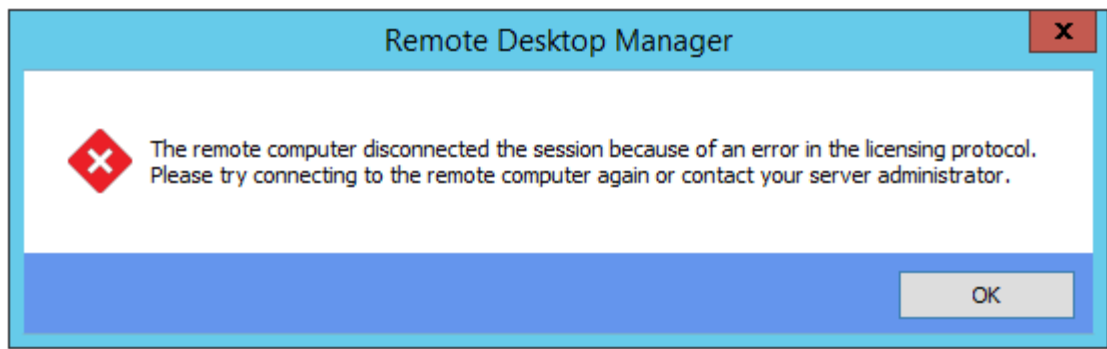
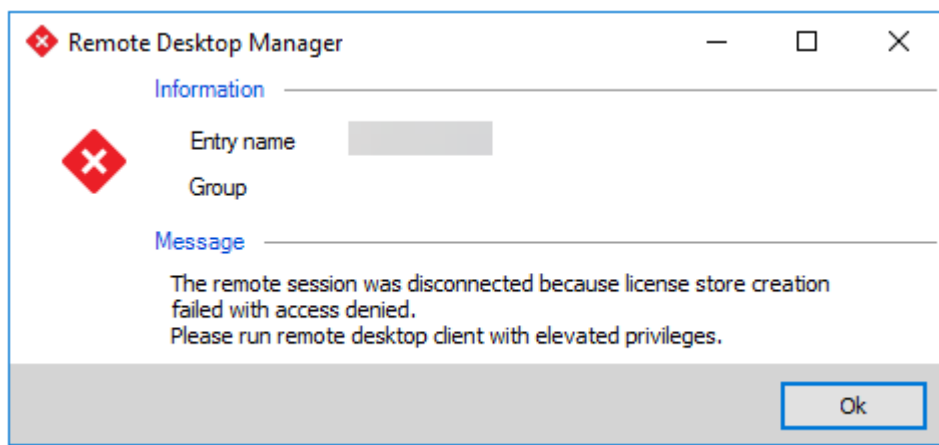
Here's a link to get you there quickly;

<https://support.microsoft.com/en-us/help/2923545/update-for-rdp-8-1-is-available-for-windows-7-sp1>

#### 12.8.14.5 Licensing Protocol Error

### DESCRIPTION

When you connect to a remote workstation, you receive one of the errors below.

*Licensing Protocol Error**License Store Creation*

## SOLUTION

1. Close Remote Desktop Manager.
2. Depending on your Windows architecture (32-bit or 64-bit) delete the specified registry key(s);

WINDOWS	REGISTRY KEY(S)
32-bit	<b><i>HKLM\SOFTWARE\Microsoft\MSLicensing</i></b>
64-bit	<b><i>HKLM\SOFTWARE\Microsoft\MSLicensing</i></b> <b><i>HKLM\SOFTWARE\Wow6432Node\Microsoft\MSLicensing</i></b>

3. Run Microsoft RDP (mstsc.exe) as an administrator to recreate the registry key (just once).
4. Restart Remote Desktop Manager.

#### 12.8.14.6 Logoff Access Denied

### LOGOFF ACCESS DENIED ERROR OR "UNABLE TO ENUMERATE REMOTE SESSIONS"

This section describes the solution for the "access denied" error which occurs when using **qwinsta.exe/rwinsta.exe** or WTSOpenServer Windows API function to access to a Windows XP SP2 PC.

The same thing happens when trying to connect to a Windows XP SP2 using Remote Desktop Services Manager from a Windows 2003 Server. This is because **qwinsta.exe** command calls WTS functions (WTSOpenServer, WTSEnumerateSessions, ...), you will encounter the same error when using either the command or the API.

#### VERIFY THE FOLLOWING:

1. Ensure you have the correct credential.

Although you do not need to provide a username and a password when executing **qwinsta.exe** or WTSOpenServer, Windows uses its stored credentials automatically, just like accessing a shared folder.

The easiest way to confirm the credential is to use Explorer to access remote server's C\$ share. Also, you can use "net use" command.

For those who want to connect to a remote server programmatically using WTSOpenServer API, WNetAddConnection2 function should be enough to make sure you got a piece of credential before calling WTSOpenServer function.

It goes without saying that the user in the credentials needs to have enough privilege on the remote server to carry out the operation.

2. Open RPC ports on firewall.

An API call involves connecting to a remote machine using RPC. In most cases, the RPC service is running and you can confirm that from the service management interface. To open RPC ports, simply enable "File and Printer Sharing" in the Windows Firewall setting.

(Generally, if the RPC is blocked by the firewall on the remote machine, the error should be "1722 RPC server is unavailable" rather than "5 Access denied")

### 3. Disable "Force Guest" log on.

You can change this option from either local security policy or registry.

Local security policy: run **secpol.msc > Security Settings > Local Policies > Security Options > Network access:** Sharing and security model for local accounts, and set to "Classic".

Registry: find "forceguest" item in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`, and set it to 0.

Both methods are equivalent. If this option is set to 1, remote logging in user will be impersonated as Guest account (and if Guest account is disabled, login fails). Set it to 0 enables user logging in as themselves.

### 4. If you still receive "access denied" and it only happens when the remote OS is Windows XP SP2, it is very likely akin to the following case:

To confirm, you need a packet sniffer such as Wireshark (a great freeware).

When you use a sniffer to capture the SMB packets, you can see the authentication is OK (NTLM if workstation, Kerberos if Windows 2003 domain), but the RPC gets `nca_s_fault_access_denied (0x00000005)` as error code.

This means the remote RPC component failed to execute the requested operation. It is because in Windows XP SP2, it is not allowed to operate on remote desktop service (RDS) through RPC by default. To modify this setting to enable Remote Desktop API through RPC, you need to find the following registry key:

```
HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server
```

Then add a DWORD value named "AllowRemoteRPC" and change its value to 1.

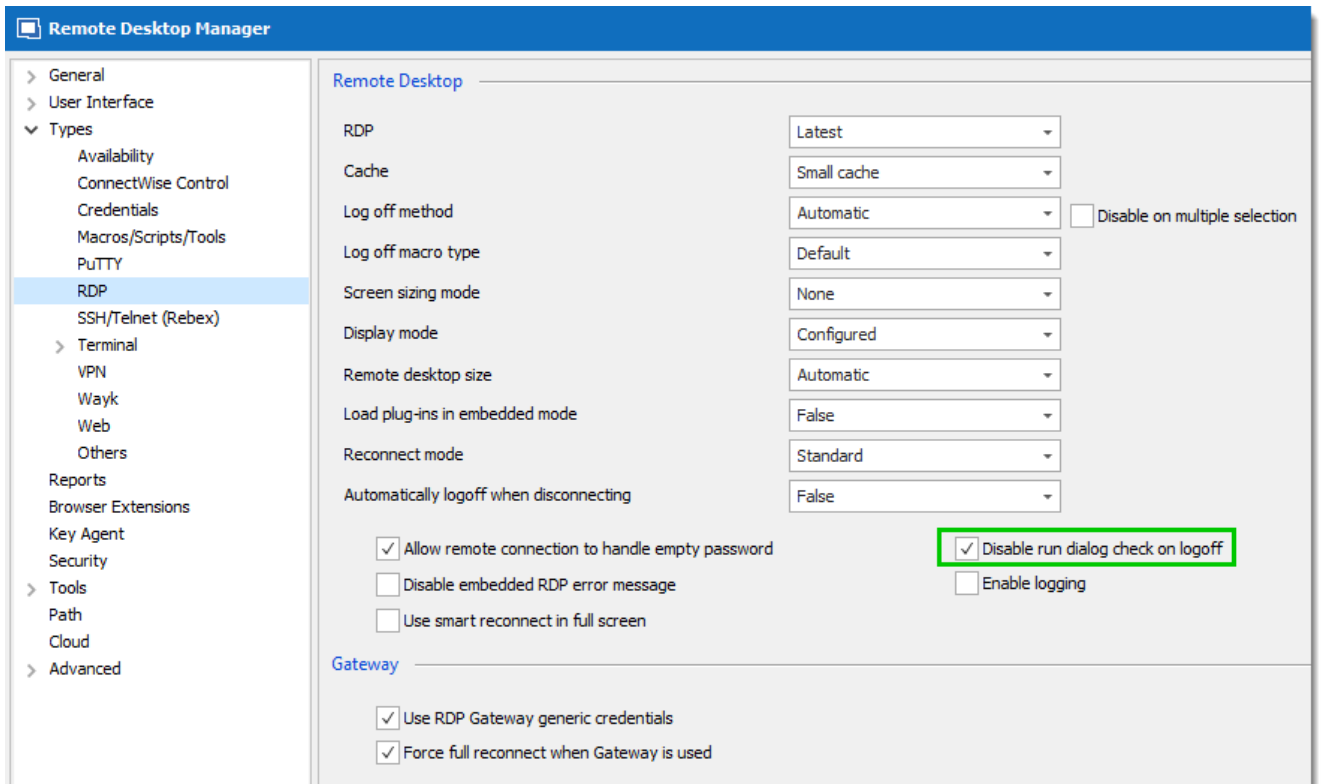
## 12.8.14.7 Logoff Issue

### DESCRIPTION

After creating and connecting to an RDP session, if you hit the 'LogOff' button in the Remote Desktop Manager ribbon, it appears to be sending the wrong command to the RDP session. It's sending 'shutdown /l' instead of 'shutdown /f'. It does this in both the Free and Enterprise version.

## SOLUTION

Simply check this option in **File -> Options -> Types -> RDP**.



*Disable run dialog check*

### 12.8.14.8 Memory and Performance issues

## DESCRIPTION

**YOU CAN ONLY RUN A FEW RDP SESSIONS AT THE SAME TIME IN REMOTE DESKTOP MANAGER AND YOU WANT TO KNOW HOW TO BE ABLE TO OPEN MORE SESSIONS.**

The amount of consumed memory is dictated by the remote technology, and in the case of RDP, by the Operating System of the remote host. Windows 8 / 2012 sessions do take upwards of 150Mb, whereas the previous versions would consume around half of that.

This is something that we have no control over. You can look at [Large Memory Aware Application](#) or use the 64bit edition of Remote Desktop Manager.

## RDP SESSION INITIATION IS SLOW, WHEN USING REMOTE DESKTOP MANAGER IN A VIRTUAL ENVIRONMENT

This situation is something that we also experience under those conditions (our testing environment is virtualized and has minimal memory for each guests).

In the **Experience** tab of your RDP session, you need to disable everything that is not used. A good method is to select the **Modem** connection speed, this will disable all settings that are related to appearance. You can then turn on a single setting to see if it affects the performance negatively. Repeat until you find the combination that works best for you.

## YOU USE RDP IN EMBEDDED MODE AND THE REMOTE SESSION IS EXTREMELY SLOW TO RESPOND. THE SESSION LOADS FINE, BUT WHEN YOU GET LOGGED-IN THE REMOTE COMPUTER, IT BECOMES UNRESPONSIVE. MOUSE CLICKS, KEYBOARD PRESSES AND APPLICATION LOADING ARE EXTREMELY SLOW. IN EXTERNAL MODE, EVERYTHING IS RUNNING FINE.

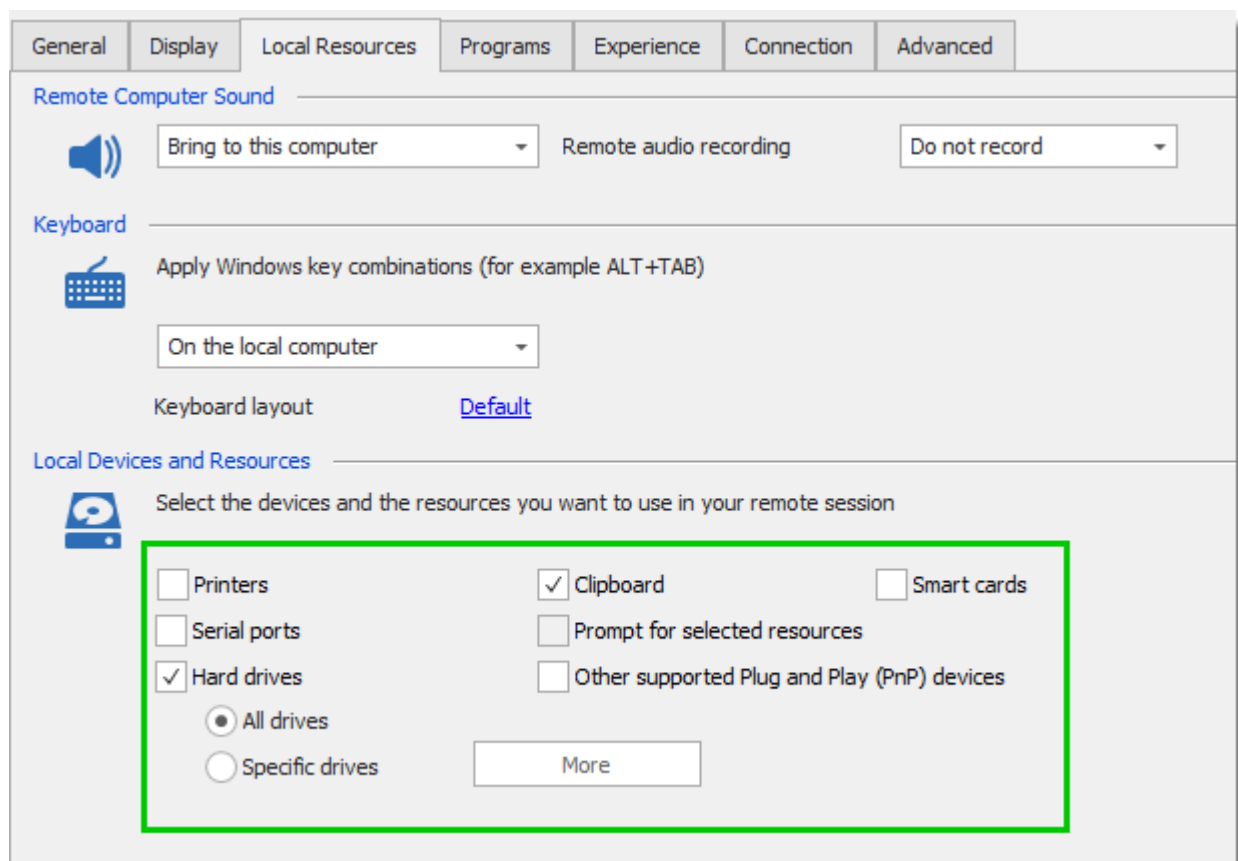
1. Disable your Anti-virus and test the connection to see if this make a difference. If you use Trend Micro Business Security, add **RemoteDesktopManager.exe**, **RemoteDesktopManager64.exe**, and **Embedded32.exe** to the Process Exception List under **Preferences – Global Settings** and update the Trend client. If you use Symantec Norton Internet Security, ensure you allow Remote Desktop Manager to access the internet in the Program Rules.
2. Uncheck all settings in the **Local Resources** tab.
3. Check **Disable display scaling on high DPI settings** in the options. Consult topic [Microsoft RDP](#) for more information.

4. Download and install Microsoft RDCMan to see if it's related to the RDP ActiveX. Remote Desktop Manager uses the same technology and this will ensure that your workstation doesn't have configuration issues.

## CONNECTIONS FAIL FOR SOME HOSTS

There are known security updates that have broken connectivity to a host, but they have been fixed in ulterior patches. If you keep the hosts updated then it should be something else.

Sometimes the mapping of local devices will cause issues. Uncheck all settings in the **Local Resources** tab.

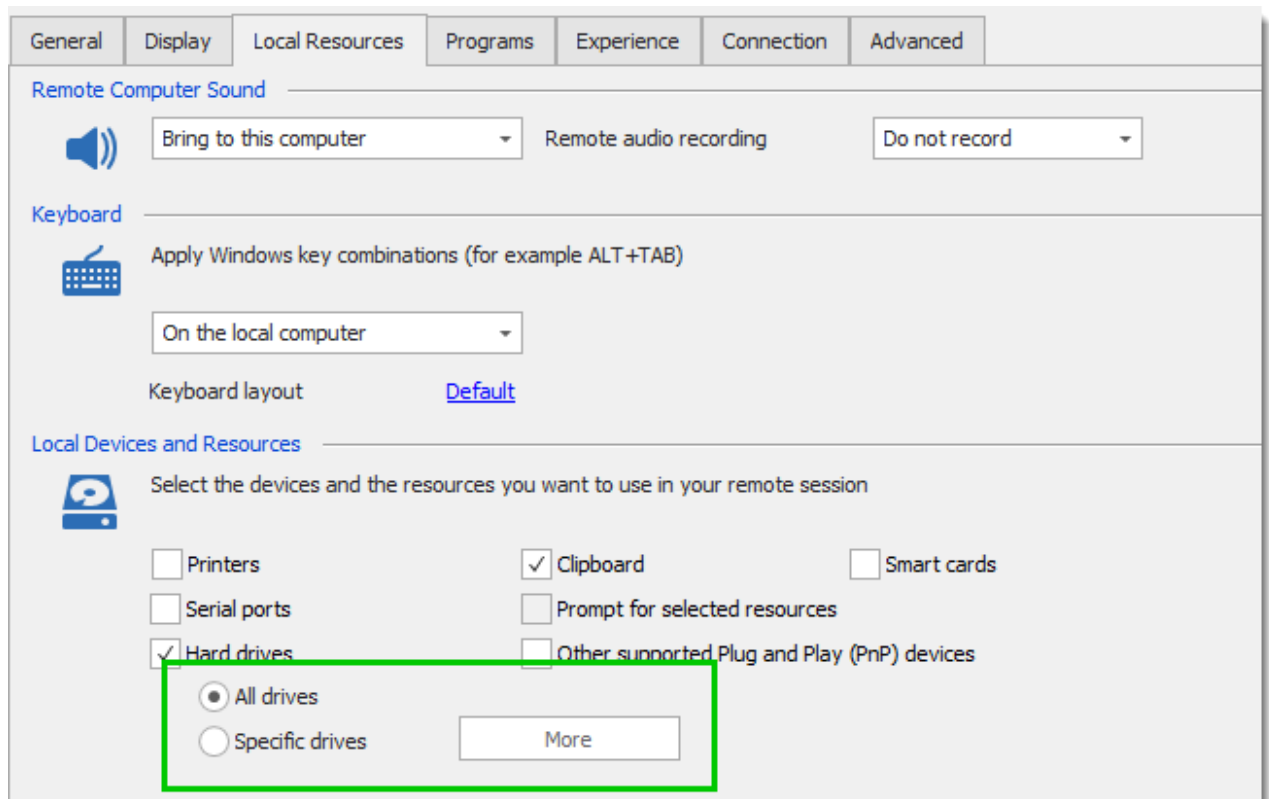


*Microsoft Remote Desktop (RDP) - Local Resources*

### 12.8.14.9 Missing mapped drives

## ERROR

Mapped network drives are not available in RDP sessions even though you have selected All drives; or are not displayed in the dialog when attempting to add **Specific Drives** using the **More** button.



*RDP Local Devices and Resources details*

## CAUSE

This problem happens when you start Remote Desktop Manager with elevated privileges (Run as administrator). Mapped drives are not available from an elevated prompt when UAC is configured to "Prompt for credentials" in Windows.

This issue is not caused by Remote Desktop Manager, you will need to apply a fix on all workstations from which you must launch Remote Desktop Manager with elevated privileges.

Please follow the steps in one of the following methods:



## METHOD 1

Using the Local Group Policy Editor, locate the following Group Policy path:

***Local Computer Policy\Windows Settings\Security Settings\Local Policies\Security Options***

Configure the following policy to **Prompt for consent**:

**User Account Control: Behaviour of the elevation prompt for administrators in Admin Approval Mode**

## METHOD 2

Map the required drives again in the elevated session. A good solution would be to create a batch/command file that starts by mapping the drives again, then launches Remote Desktop Manager.

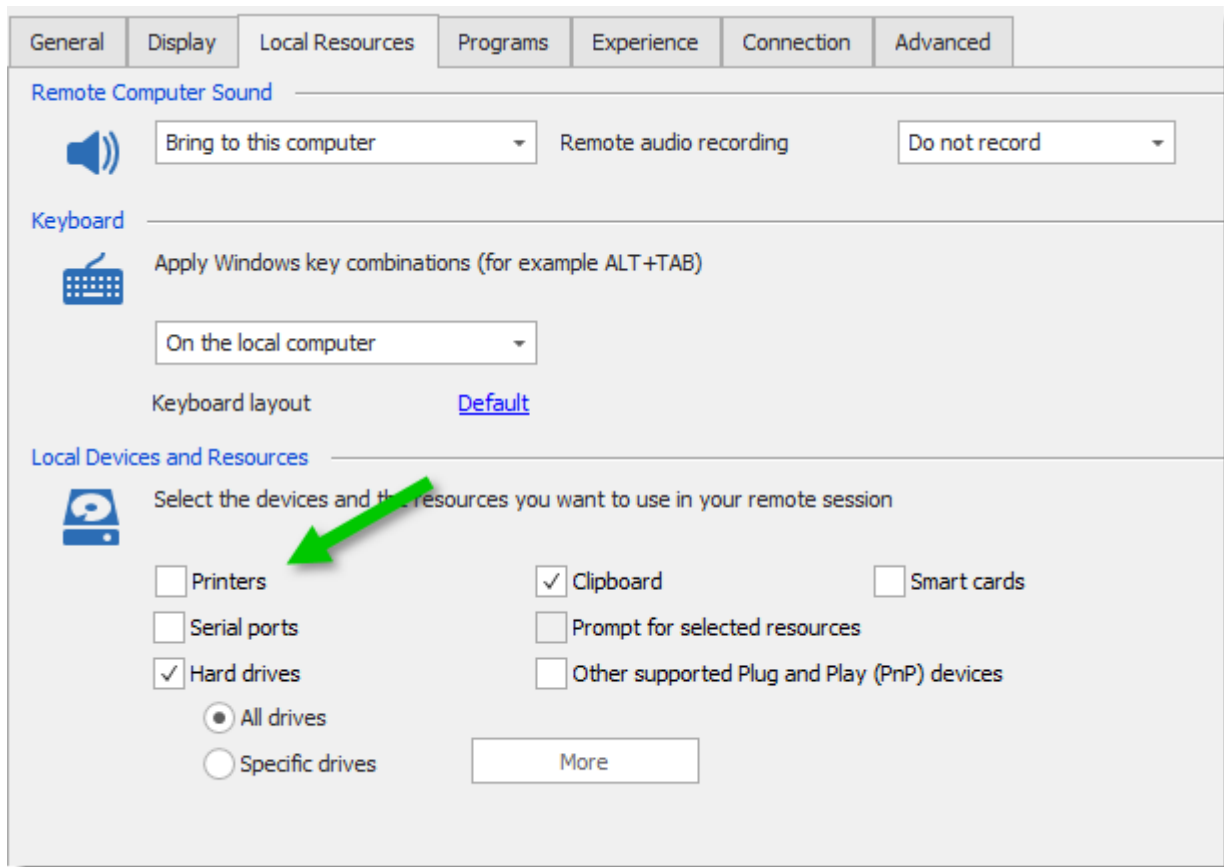
### 12.8.14.1(Printer Redirection)

## DESCRIPTION

You are attempting to use printers inside your remote sessions but they seem to be missing.

## SOLUTIONS

1. Ensure that the option for **Printers** in the **Local Resources** tab is enabled.



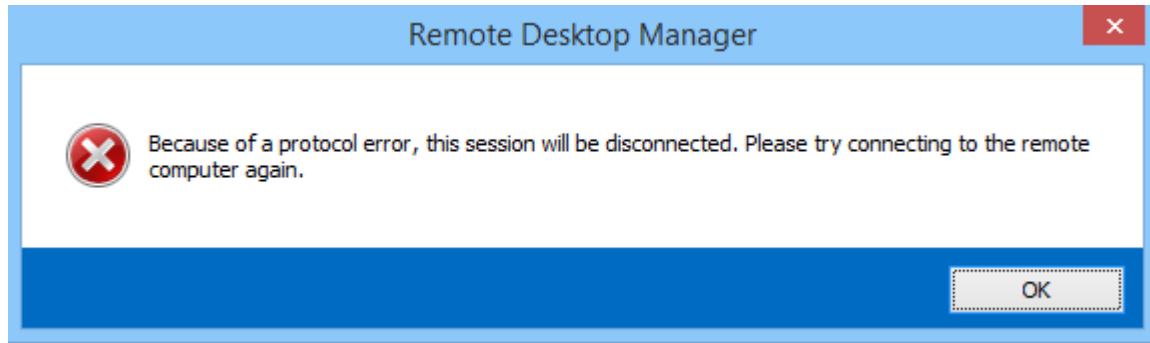
Printers

2. If you have a 64-bit Windows, you must start the Remote Desktop Manager 64-bit launcher. By default, this launcher is located in **C:\Program Files (x86)\Devolutions\Remote Desktop Manager** under the name **remotedesktopmanager64.exe**.

#### 12.8.14.1 Protocol Error

## ERRORS

**BECAUSE OF A PROTOCOL ERROR, THIS SESSION WILL BE DISCONNECTED. PLEASE TRY CONNECTING TO THE REMOTE COMPUTER AGAIN.**



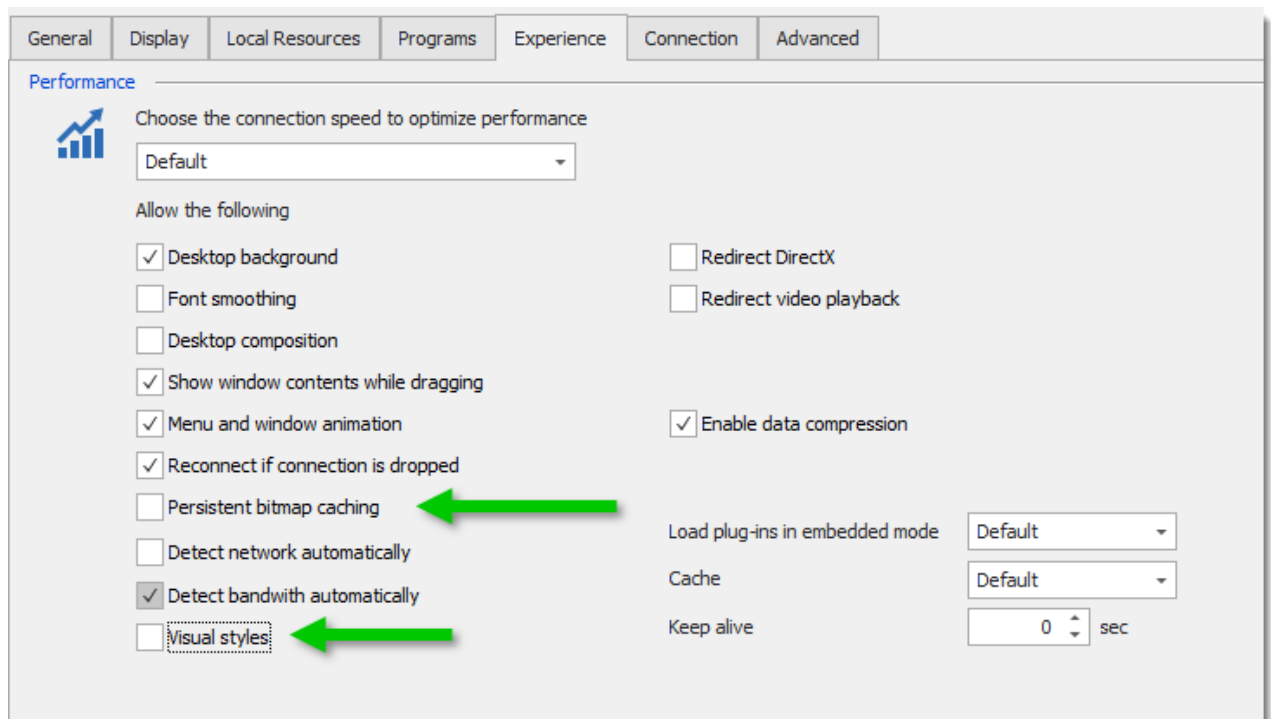
*Error message*

## SOLUTION 1

Try to use Remote Desktop Manager 64bit. To do so, launch Remote Desktop Manager64.exe from the installation folder instead of Remote Desktop Manager.exe.

## SOLUTION 2

Uncheck **Persistent bitmap caching** and **Visual styles** under the **Experience** tab in the properties of the RDP session.



*Uncheck Visual styles and Persistent bitmap caching*

## SOLUTION 3

Close Remote Desktop Manager, rename **default.rdp** file in My Documents to **default.old**, restart Remote Desktop Manager and try to connect with RDP.

## SOLUTIONS 4

Login in to the target machine by directly going to the console of that server or by any tool like VNC so that we can get access to that machine.

After connecting:

1. Right Click on the Desktop.
2. Select the Properties.
3. There DropDown the Themes and select the theme other than the current one.
4. Click on Apply, OK.

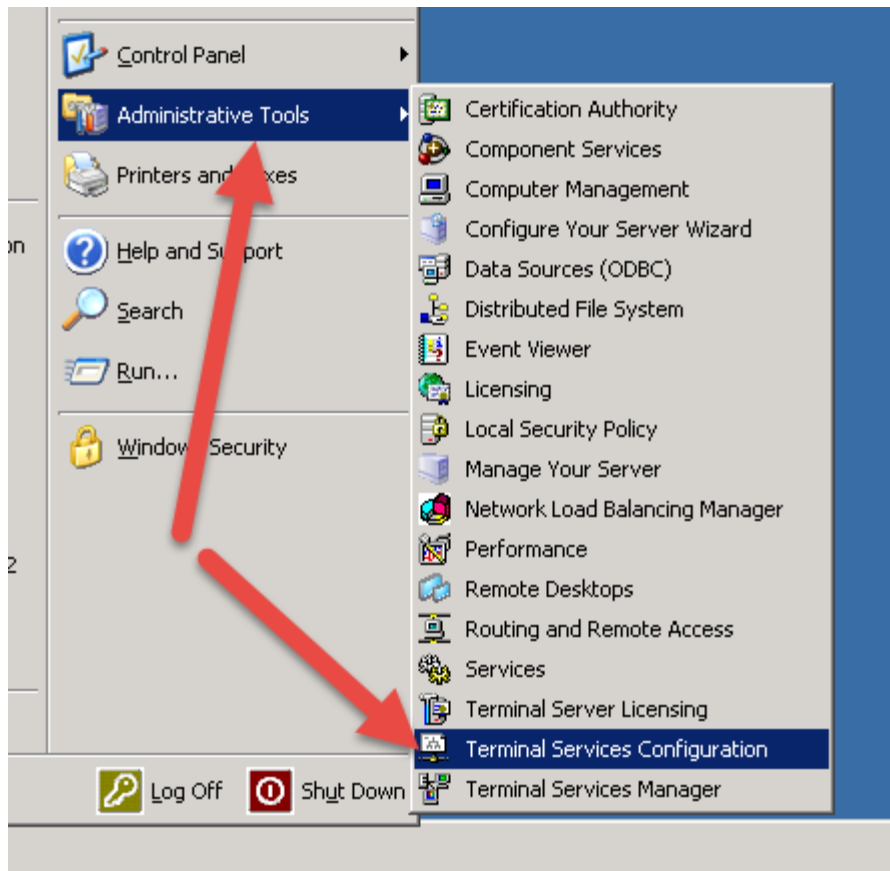
Now try to connect that machine remotely.

### 12.8.14.1 RDP Session Credentials

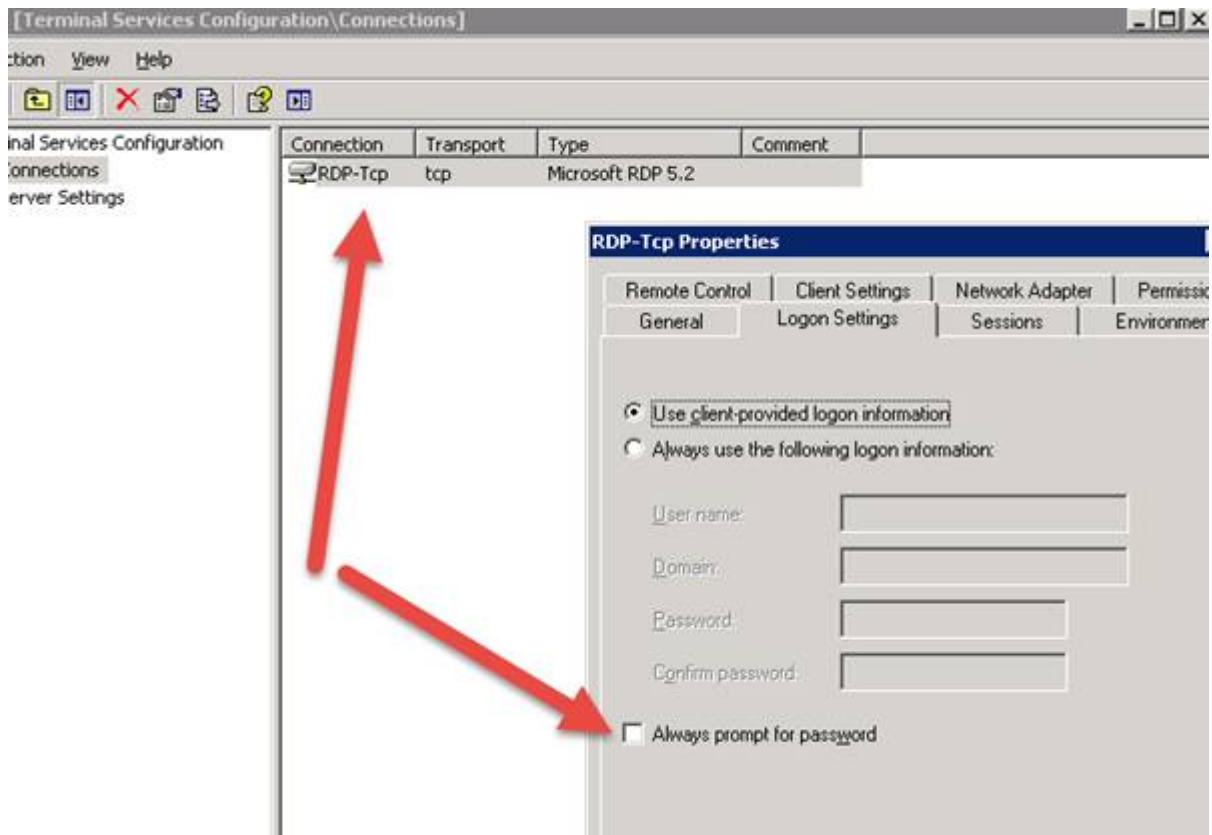
## ISSUES

### UNABLE TO PASS CREDENTIALS TO A WINDOWS SERVER 2003

The issue resides on the server itself. You simply have to disable the option **Always ask password** and enable the option **Use client-provided logon information** as shown below;



Windows Server 2003



Windows Server 2003

#### 12.8.14.1 Remote Computer Requires Authentication to be Enabled Error

### ERROR

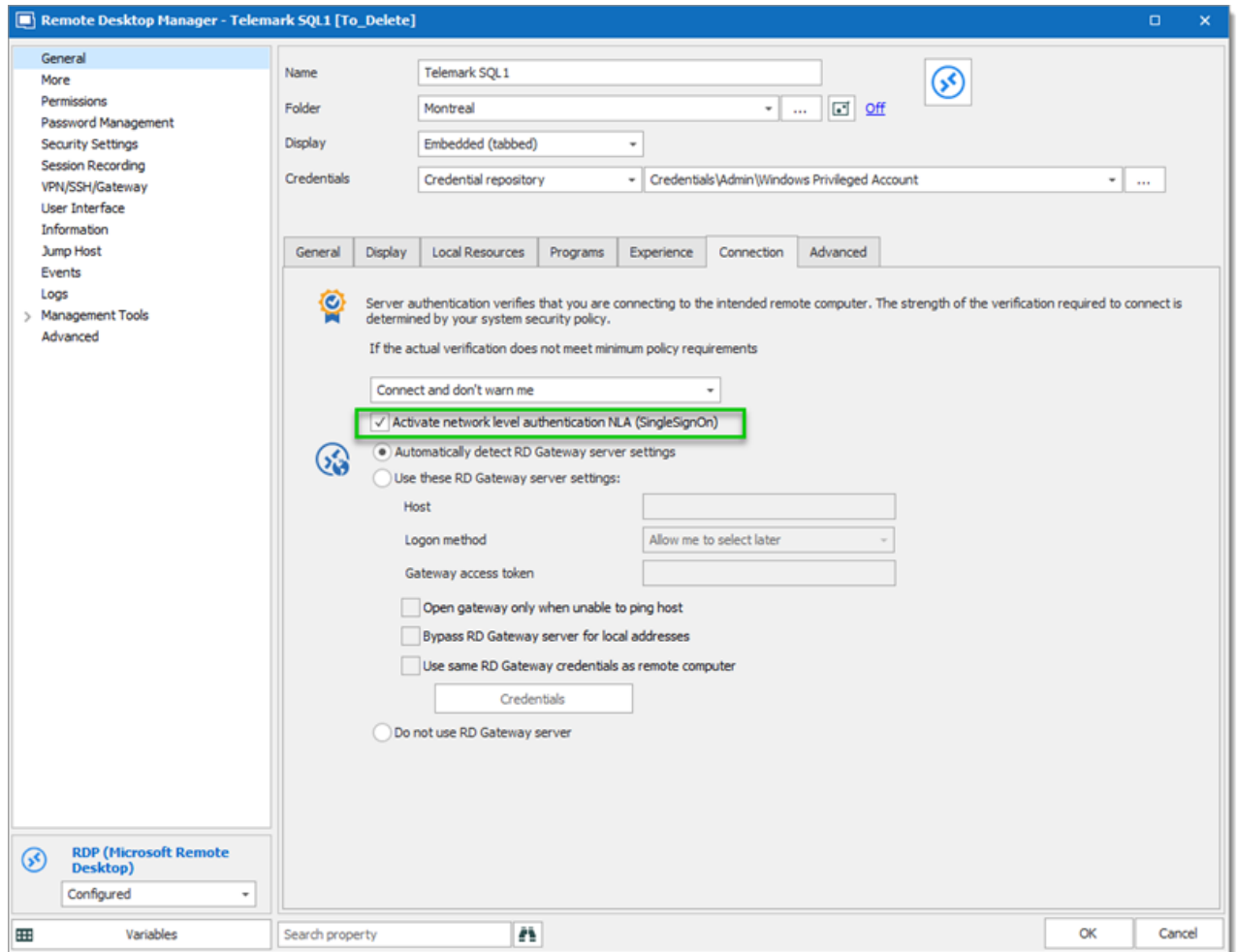
The connection cannot proceed because authentication is not enabled and the remote computer requires that authentication be enabled to connect.

### SOLUTION

This error occurs when you try to establish a remote connection from a Windows Server 2008R1 to a Windows Server 2016. In modern versions of Windows, like Windows 10 or Windows Server 2016, the RDP defaults have changed. The default for the Security Layer has changed from 0 to 2.

#### OPTION 1

In the RDP session check mark **Activate network level authentication** than **OK**.



*Remote Desktop Manager Activate network level authentication*

## OPTION 2

To resolve this issue, on the Windows Server 2016, open the registry (regedit.exe) and navigate to:  
 HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp. Then, change the SecurityLayer to 0.

### 12.8.14.1 Reconnect

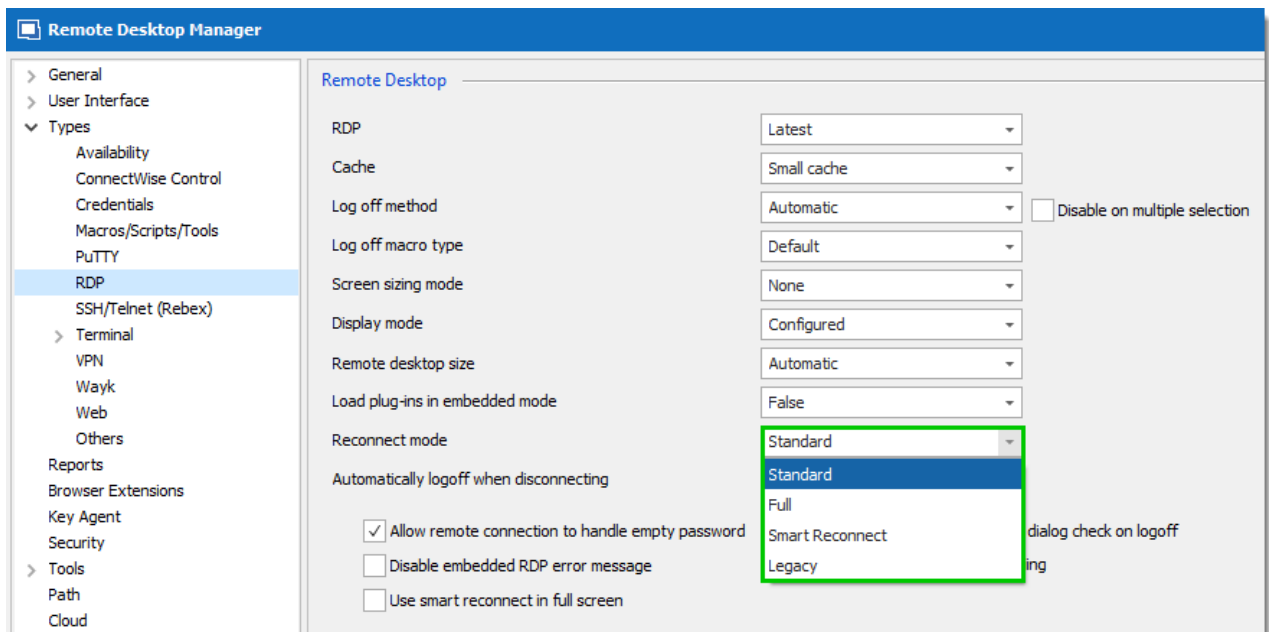
## DESCRIPTION

When a remote connection is locked and asks for the username and password to reconnect, instead of closing and relaunching the connection you would typically use the **Reconnect** feature. However, the session doesn't reconnect properly, because the credentials are not sent to the remote session.

This is an old issue and shouldn't happen unless your selection is currently legacy or your RDM requires updating, however if it happens nonetheless the fix remains the same.

## SOLUTION

In **File -> Options -> Types -> RDP** in the **Reconnect Mode** dropdown menu, adjust the setting and try again, we recommend trying to set it to **Full**.



*Reconnect Mode*

### 12.8.14.1 RD Gateway Credentials Prompt When Trying To Reconnect

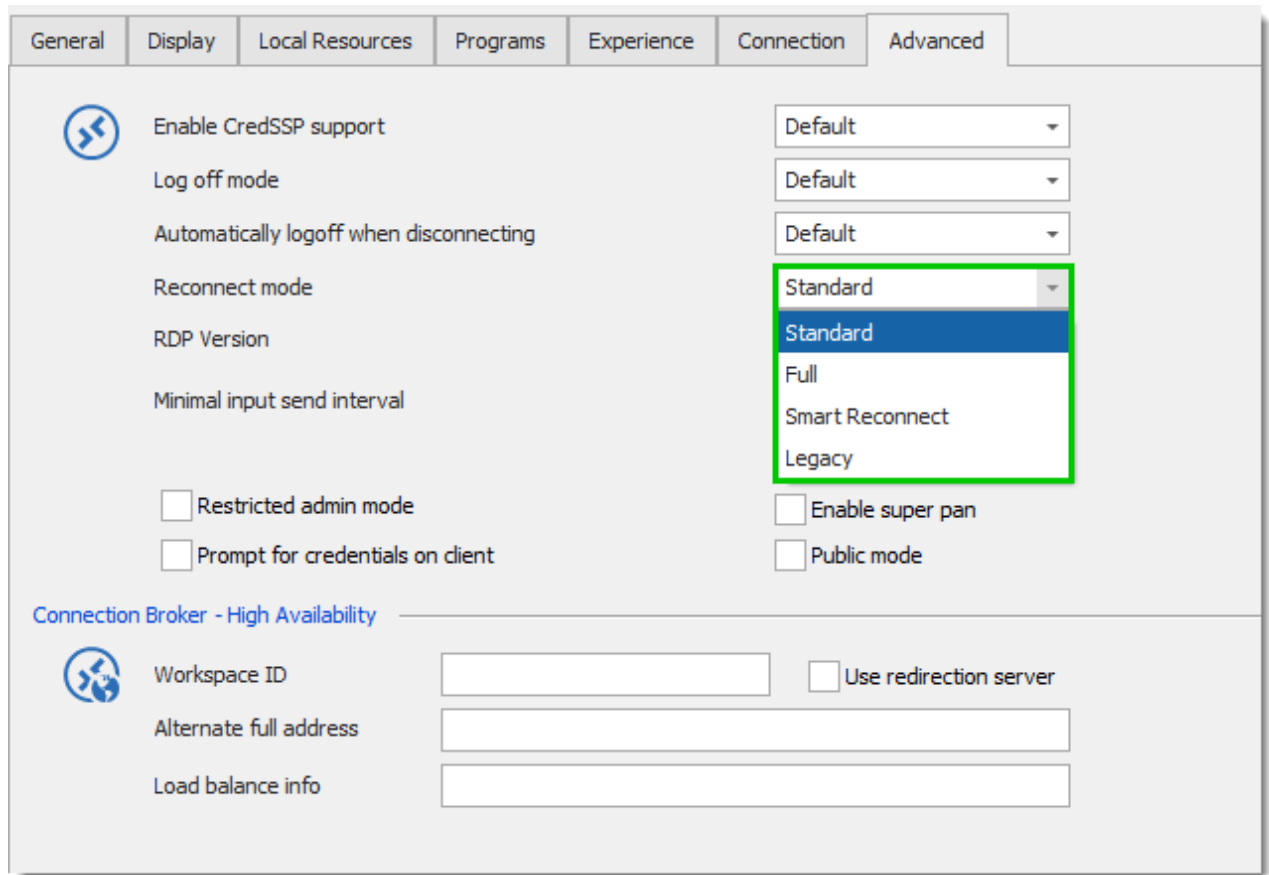
## DESCRIPTION

This problem happens when you have RD Gateway configured with some credentials and you use the reconnect action. You get prompted for the RD Gateway credentials and the application does not reuse the existing settings.

## SOLUTION

To fix this issue, set the **Reconnect mode** to **Full** in the RDP session **Advanced** settings. This will force the complete disconnect/reconnect and it will resolve the issue.





*Full Reconnect In Advanced Tab*

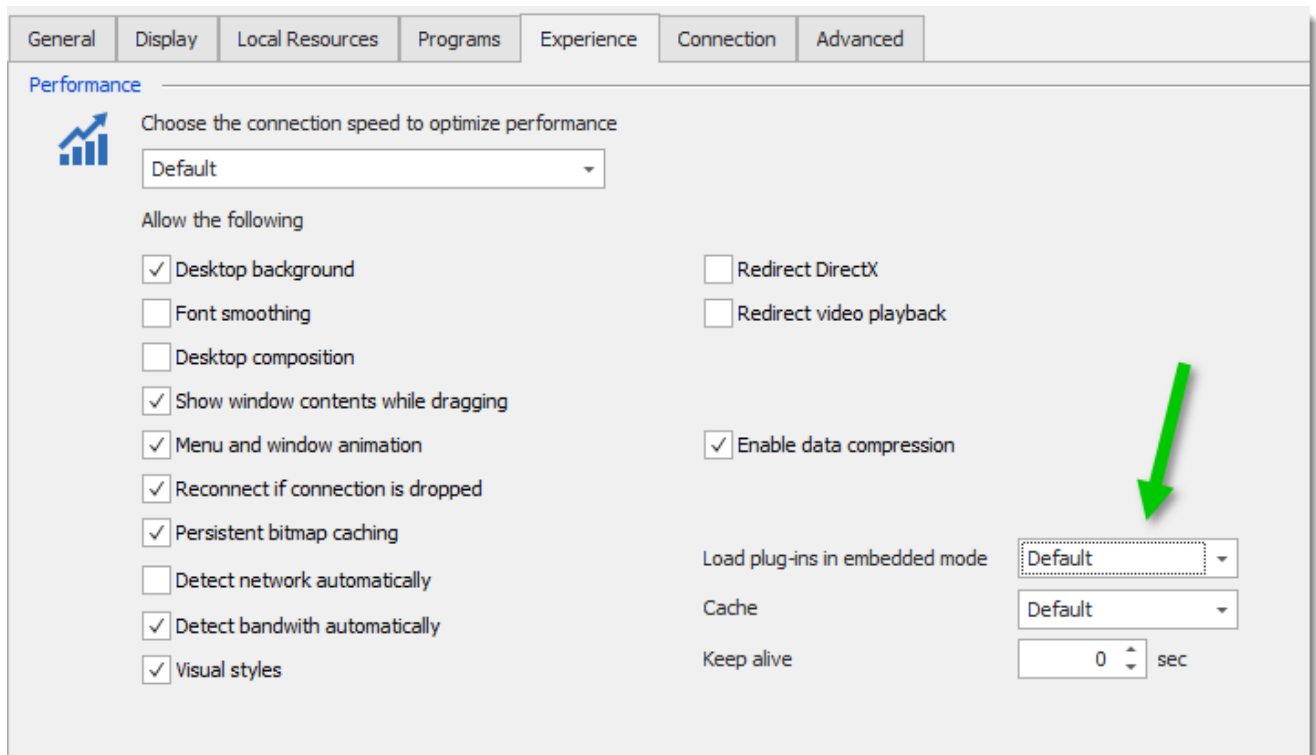
#### 12.8.14.1 RDM Hangs when logging off RDP sessions

### CAUSES

The two causes are RDP plug-ins and UDP usage under certain conditions.

### RDP PLUG-INS

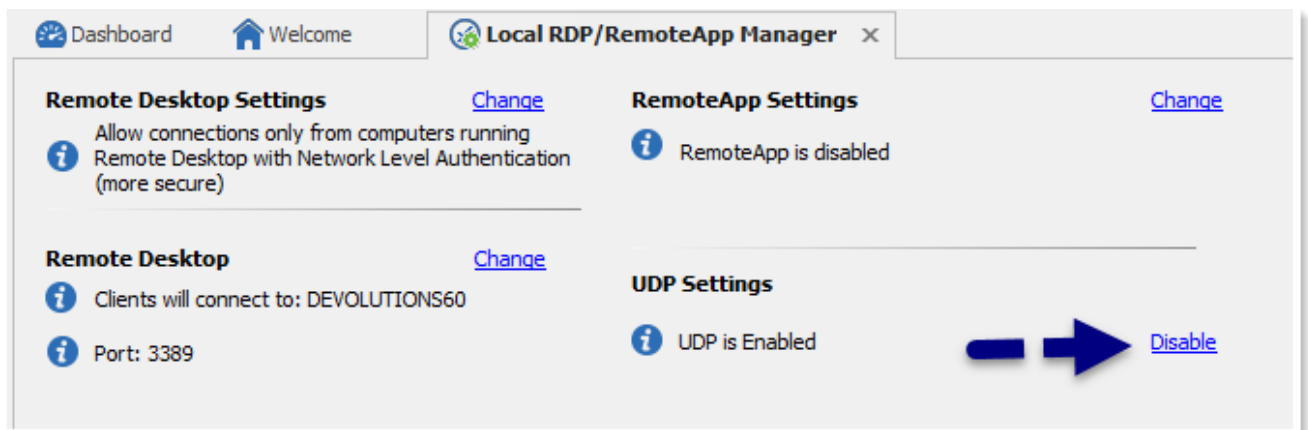
This one is quite easy to test out. You simply go in the **Experience** tab of your RDP sessions and set **Load plug-ins in embedded mode** to **False**. Do this first as it has a really low impact.



RDP Experience Tab

## UDP USAGE

There's an option in RDM to disable UDP usage. To do so, open Remote Desktop Manager as an administrator and click on **Tools -> Local RDP/RemoteApp Manager** and click on **Disable** to disable the **UDP settings**.



UDP Settings

This one is a bit trickier, some search results hint that this is caused only when going through a VPN, others mention that it occurs only on Windows 8 paired with a Gateway server, but this solution has worked for many of our users, so we suggest you try it.

It requires a registry change, so all the usual warnings and caveats apply here, ***back it up first!*** Consult this [Microsoft support article](#) for more information

The fix is to disable UDP on the client workstation using these simple steps:

1. Navigate to HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\Client.
2. Create a DWORD named fClientDisableUDP and assign it a value of 1.

#### 12.8.14.1 Sessions work using mstsc.exe but not in RDM

## DESCRIPTION

This topic describes the troubleshooting steps for when establishing a session to a remote host reacts differently in Remote Desktop Manager than when you are using **mstsc.exe**.

## EMBEDDED MODE ISSUES

Our **Embedded (tabbed) display mode** uses the Microsoft ActiveX and offers the most customization options, but is inherently different than using **mstsc.exe**. When wanting to ensure the issue is really in Remote Desktop Manager vs being an issue with the ActiveX, the procedure is to try to replicate the scenario with Microsoft's RDCMan. You can obtain that tool from <http://www.microsoft.com/en-ca/download/details.aspx?id=44989>. Simply install it, create sessions like you have in Remote Desktop Manager, then open them concurrently or in repetition to replicate the issue you think lies in Remote Desktop Manager.

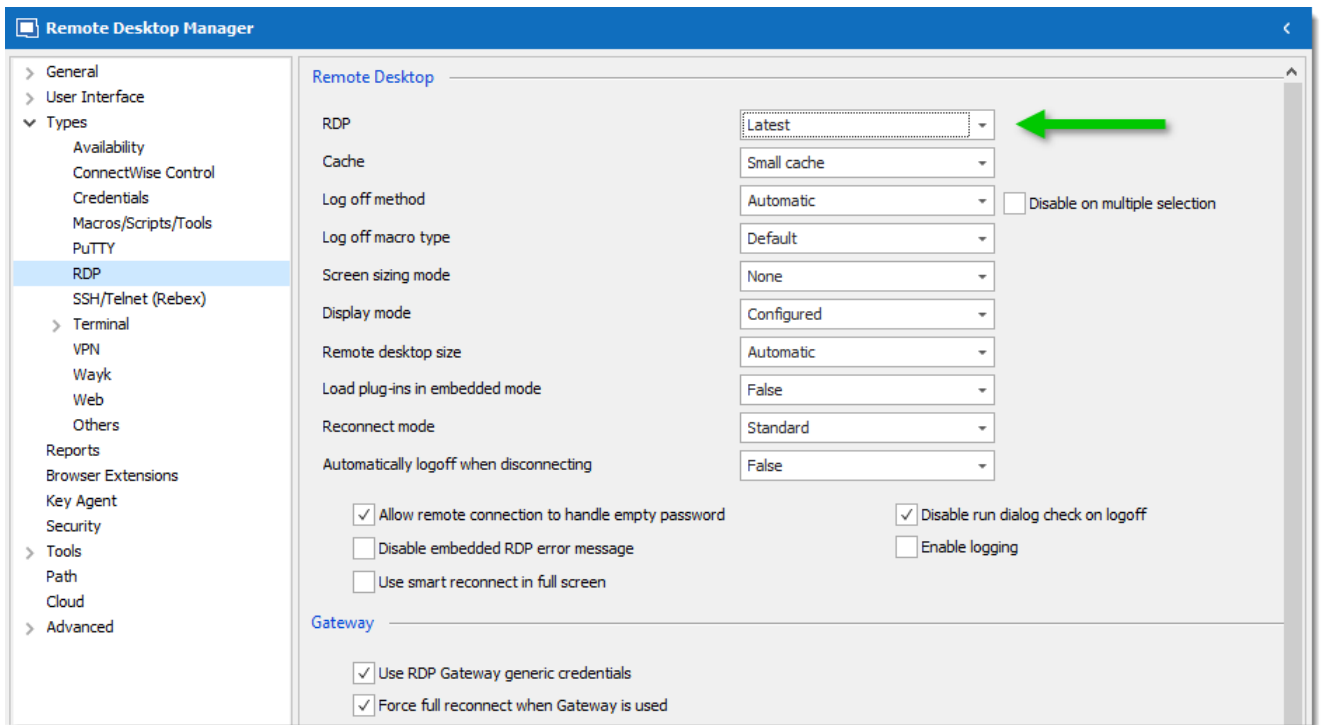
## COMPARING OUR SETTINGS TO A NATIVE RDP FILE

When you choose to use the **External display mode**, Remote Desktop Manager will in fact create a temporary RDP file and call **mstsc.exe** with the file as a parameter. It can be beneficial to grab that file while it exists and to compare it with one created using **mstsc.exe**.

1. Create or duplicate a session that you want to diagnose, set the **display mode** to **External**.
2. Launch that session.
3. The file will be deleted when you close Remote Desktop Manager, you need to copy it before then.
4. Open **%TMP%\RDM**, copy your file in another folder.
5. Open the file in your editor of choice and compare it to a file created using **mstsc.exe**

## STARTING RDP SESSIONS IS SLOW COMPARED TO THE NATIVE RDP

We have isolated the issue and we fixed it by changing your RDP engine version to **RDP 6.0** or **7.0** in **File -> Options -> Types -> RDP**

*RDP Engine*

## 12.8.15 Network Devices

### DESCRIPTION

It's possible to manage different devices via a web interface. However, you may have some issues to connect to the web interface using our **Web Browser** in the **Embedded (tabbed)** display mode.

For example, you may encounter issues with the following devices:

- Nagios
- Cisco
- Dell SonicWall

### SOLUTION

We use third party libraries for the integration of Firefox and Google Chrome in the **Embedded (tabbed)** display Mode. For Internet Explorer, we use the Microsoft ActiveX that is installed at the same time as the browser.

If none of the web browsers work in **Embedded (tabbed)** display Mode, you would need to launch the website using the **External** display mode and use our Devolutions Web Login to handle the credentials.

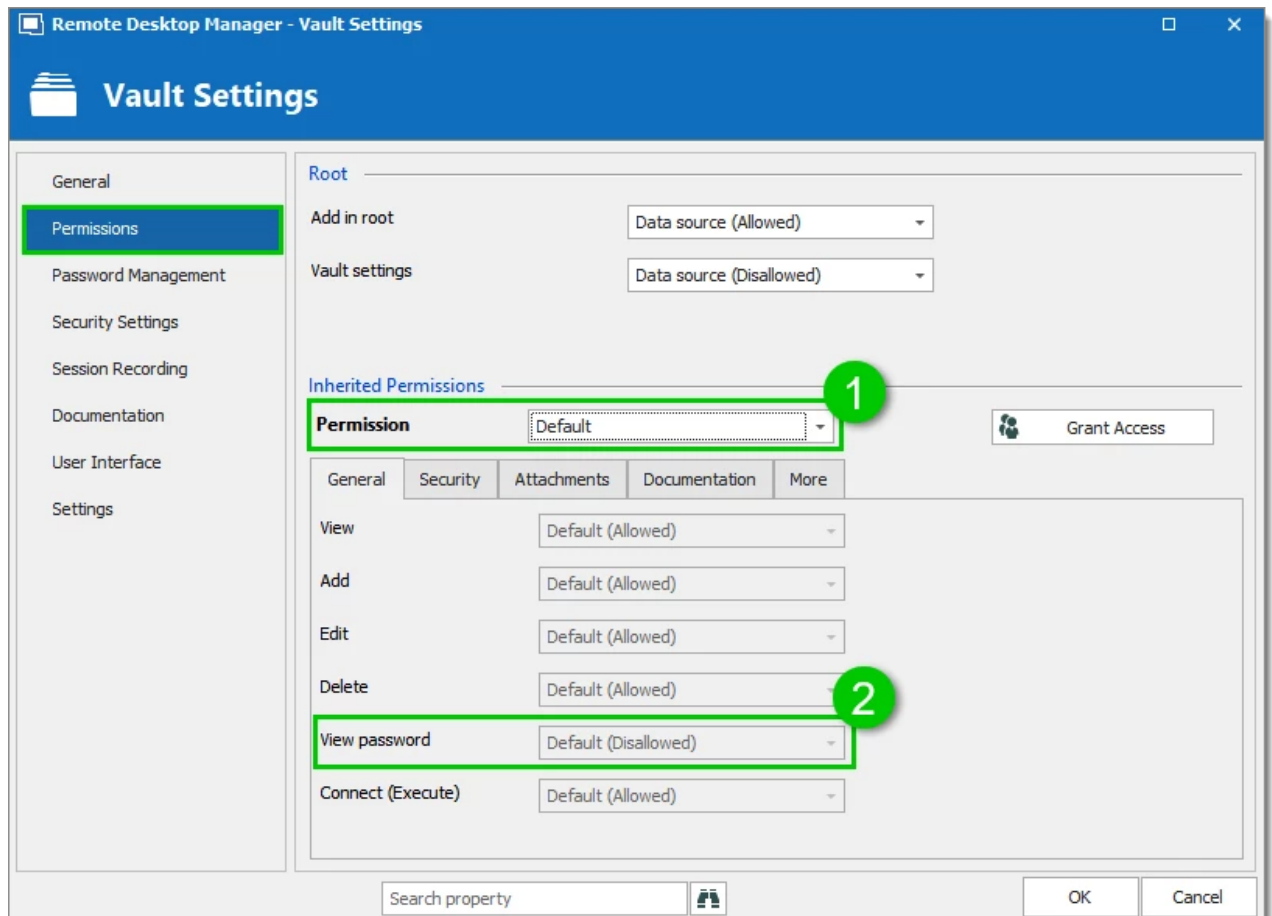
## 12.8.16 Non-Admin Users Cannot View Passwords

### DESCRIPTION

Normal users are no longer able to view or copy password after updating to Remote Desktop Manager 2019+

### SOLUTION

If you want to allow Users or specific Roles to be able to view the password from all your sessions, you must configure the **View Password** setting found in **Administration - Vault Settings - Permissions - View Password**.



*Vault Settings - Permission*

This setting was changed because of security purposes.

Here the associated line from the Release Notes : [https://remotedesktopmanager.com/release-notes#\\_gac=1.51723355.1554296008.Cj0KCQjws5HIBRDIARIsAOomqA3ywMlfEkq4pM\\_uVsDLut1r\\_Ow7RRZKo1D9MrqBBjzyShNd4AoQGBQaAhSiEALw\\_wcB](https://remotedesktopmanager.com/release-notes#_gac=1.51723355.1554296008.Cj0KCQjws5HIBRDIARIsAOomqA3ywMlfEkq4pM_uVsDLut1r_Ow7RRZKo1D9MrqBBjzyShNd4AoQGBQaAhSiEALw_wcB)

"Changed the View Password to not allowed by default for non administrator"

## 12.8.17 Password Manager Pro

### ERRORS

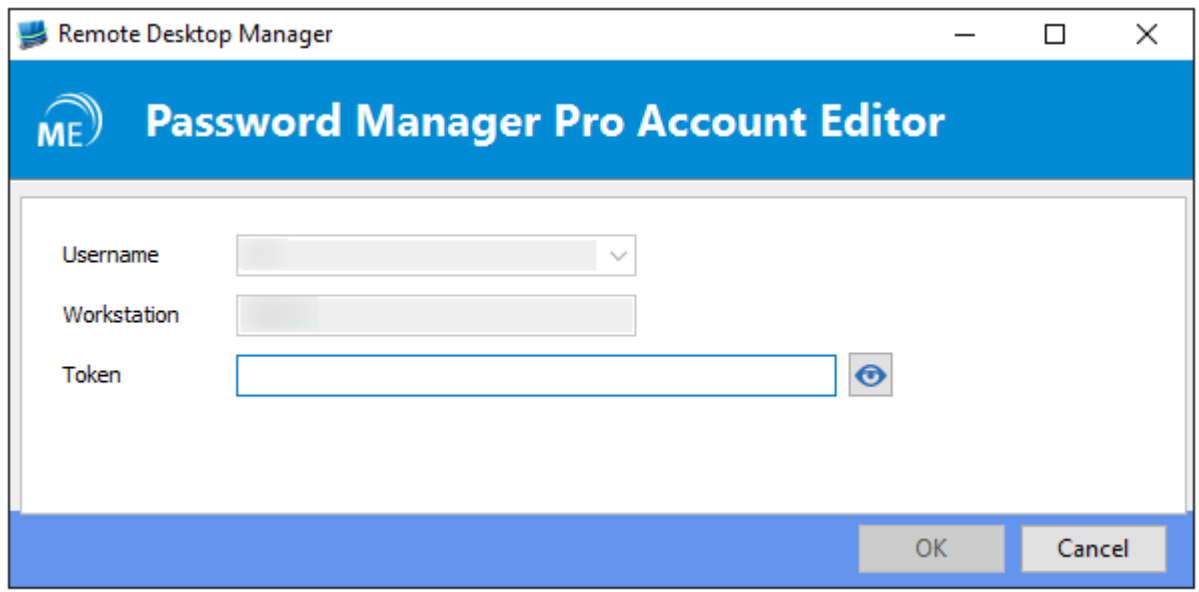
#### SYSTEM.NET.WEBEXCEPTION: THE SERVER COMMITTED A PROTOCOL VIOLATION. SECTION=RESPONSESTATUSLINE

During the configuration of your **Password Manager Pro** credential entry, make sure that the **URL** of your server contain **https://** and not **http://**. You absolutely need an **https://** at the beginning of the address to communicate properly with the server.

The screenshot shows the 'General' tab of the Password Manager Pro configuration window. The 'Service URL' field contains 'https://vdownsrv-pmp'. The 'Port' field is set to '7272'. The 'Use "My Account Settings"' checkbox is unchecked. The 'Username' field is empty. The 'Resource' field is empty. The 'Account' field is empty. The 'Always prompt with list' checkbox is checked. The 'Domain override' field is empty.

*Service URL*

**WHEN YOU TRY TO CONNECT ON A REMOTE COMPUTER OR GET THE CREDENTIAL LIST, A WINDOW APPEAR WITH AN EMPTY TOKEN FIELD AND THE USERNAME AND WORKSTATION FIELD GREYED OUT.**



*PMP Account Editor*

The Host Name configured in your API user in **Password Manager Pro** is not the same that you have configured in Remote Desktop Manager in **File – My Account Settings – Password Manager Pro**. Please consult the How to Configure Password Manager Pro in Remote Desktop Manager topic for more information on the configuration.

## SYSTEM.NET.WEBEXCEPTION: THE REQUEST WAS ABORTED: COULD NOT CREATE SSL/TLS SECURE CHANNEL.

**Password Manager Pro** can be configured to use SSLv3, TLSv1.0, TLSv1.1 and TLSv1.2. If you have configured your **Password Manager Pro** server to use TLSv1.2 only, you will encounter this error message. You need to configure your **Password Manager Pro** to accept TLSv1.0, TLSv1.1 and TLSv1.2.

## API KEY RECEIVED IS NOT ASSOCIATED TO ANY USER. AUTHENTICATION FAILED.

Edit your API user in **Password Manager Pro** and generate a new **Authentication Token**, save your API user and save this new token in Remote Desktop Manager in **File – My Account Settings – Password Manager Pro**.

## USER IS NOT ALLOWED TO ACCESS FROM THIS HOST

During the creation of an API User in **Password Manager Pro**, a **Host** (Computer name) is necessary to create the user. In **Password Manager Pro** it may be registered using the **Fully Qualified Domain Name (FQDN)** of the computer. In Remote Desktop Manager on the other hand, you must set it exactly the same as the %COMPUTERNAME% environment variable.

Another reason for this error we have seen is that the DNS name of the server was specified, but it would work perfectly fine if you were using the IP address instead. Please test it with the procedure described below.

## TESTING PROCEDURE WITH POWERSHELL

Here is a script that you can use to test your access from a client workstation. Save the following code in a file called **PMPTest.ps1**. The technology used in the script is the same as is used from within Remote Desktop Manager, therefore its the most conclusive test. If you contact **Password Manager Pro** support, they can provide a Java based test fixture. It is not as useful except to prove that the server basically responds to your queries.

```
[CmdletBinding()]
Param(
    [Parameter(Mandatory=$True, Position=1)]
    [string]$PMPServer,

    [Parameter(Mandatory=$True, Position=2)]
    [string]$AuthToken
)

add-type @"
    using System.Net;
    using System.Security.Cryptography.X509Certificates;
    public class TrustAllCertsPolicy : ICertificatePolicy {
        public bool CheckValidationResult(
            ServicePoint srvPoint, X509Certificate certificate,
            WebRequest request, int certificateProblem) {
            return true;
        }
    }
"@

[System.Net.ServicePointManager]::CertificatePolicy = New-Object TrustAllCertsPolicy
cls
$connect = "https://" + $PMPServer + ":7272/restapi/json/v1/resources?AUTHTOKEN=$Aut
$result = Invoke-WebRequest -Uri $connect
$form = $result.Content
$content = ConvertFrom-Json $form

$status = $content.operation.result.status

if ($status -eq "Success") {
    $content.operation.Details
}

if ($status -eq "Failed") {
    $status
    $content.operation.result.Message
}

Pause
```

Please note that the port is hard-coded in the script to 7272, which is the default value for **Password Manager Pro**. Adapt to your environment.

From within **Powershell**, type the following.

```
.\PMPTest.ps1 {YOUR_PMP_SERVER} {YOUR_PMP_TOKEN}
```

Test with both the DNS name of the server and the IP address and observe the results.



## REMOTE DESKTOP MANAGER IS RETURNING THE IP ADDRESS OF THE SERVER INSTEAD OF THE FQDN

In some organization, IP addresses are blocked and the host name of the **Password Manager Pro** server needs to be returned. In that case, the [Configuration File](#) of the application would need to be modified.

1. Close Remote Desktop Manager.
2. Find the Remote Desktop Manager [Configuration File](#).
3. Edit the configuration file and add the line  
`<ResolvePMProURLIntoIPAddress>false</ResolvePMProURLIntoIPAddress>`.
4. Save the modification and restart the application.

### 12.8.18 Performance

#### 12.8.18.1 Data sources

## REFRESH

This category affects all data source refreshes, therefore:

1. **Initial load at program startup.**
2. **Prior to an Edit operation:** by default, we reload the entry to ensure that we are working on the current version.
3. **Prior to establishing a connection:** we need to insert in the activity in our Logs.
4. **Whenever you use Refresh:** Depending on your cache settings, we typically just get the changes that occurred since your last refresh
5. **Whenever you use the Tree View.**

SQL Server has certain particularities that, if the default configuration is used, will cause performance degradation as time goes by. Please consult [SQL Server Performance](#).

## HEAVY USAGE OF CUSTOM IMAGES

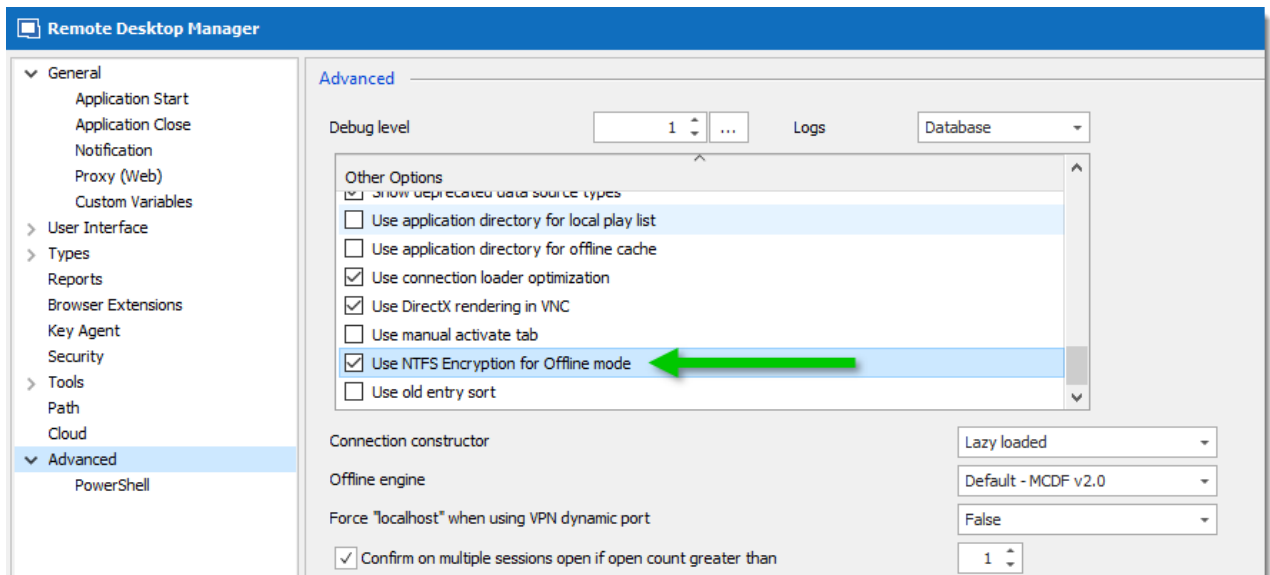
Custom images need to be stored in the data source, this results in the size of the configuration becoming problematic if there are too many entries using them. If that becomes the case it would be better to revert to built-in images.

## HEAVY USAGE OF RTF DESCRIPTION

RTF in itself is not a real issue until you decide to embed images in the description. This results in the same problem as using custom images, namely the size of the configuration becoming too large. If that becomes the case, reduce the size of your descriptions.

## OFFLINE MODE ACTIVATED FOR DATA SOURCE

When you enable the [Offline Mode](#), a local file is created and is kept in sync with the data source. This file is encrypted using the Windows built-in NTFS encryption which can cause delays in refreshing the local data file. This is rarely the case but seems to happen on computers within a domain which has been hardened by the network administrator. You can turn off this option by unchecking **Use NTFS Encryption for offline mode** in **File – Options – Advanced**.



NTFS Encryption

## CLASSIC UI

The new Ribbon UI is modern and allows for infinite variations of panel organization, but it does take more calculations by the UI layer. On most system this is not a cause for noticeable performance slowdown, but on others setting the User Interface to Classic UI (v7.x) in the general options tab will definitely help.




### 12.8.18.2 Diagnostic

## DESCRIPTION

Sometimes when a performance issue occurs while using Remote Desktop Manager, the support personnel may ask you to send information. Here are three sources of information that the support team requires to help diagnose your issue.

## PROCEDURES

### MY DATA SOURCE INFORMATION

## Data Source Information

ID			
Server			
Database	TCP	v1.523	JafJafDen
Is DB owner	✓		
Is System DBA	✓		
Offline mode	64.0 KB	Read/write	
Group Policy settings	Read/write		
System settings	Read/write		
User settings	Read/write		
Data source config	Intelligent		
Vault	Allow offline		
Vault	Default		

General
Entries
Security Groups (Legacy)
Roles

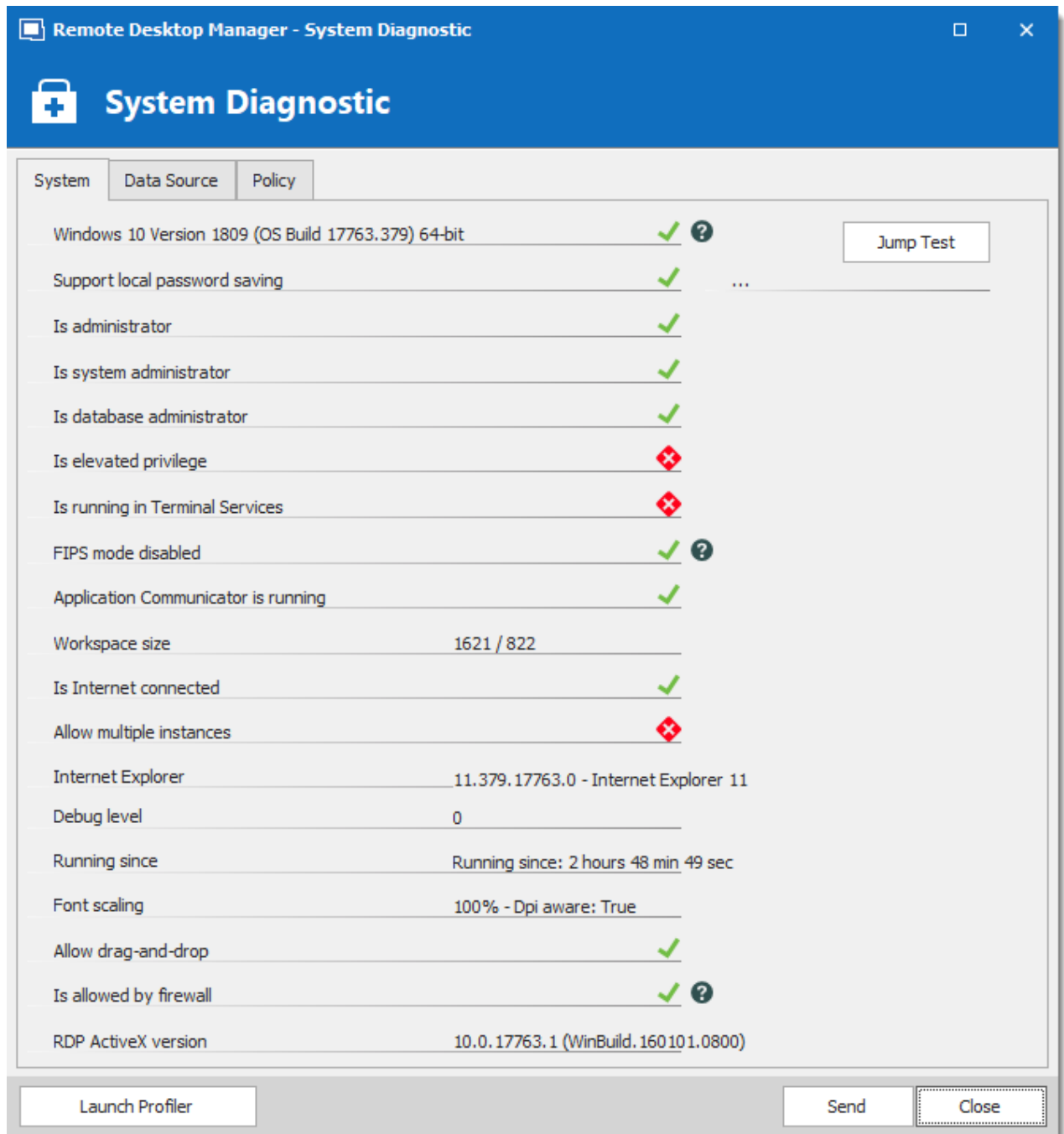
Database user			
User			
Description	hehesa		
Is administrator	✓		
Allow offline mode	✓		
Allow drag-and-drop	✓		
Is Auto Refresh	✗		
Auto refresh interval	0	sec	
Is Two Factor Configuration	✗		

My Data Source Information

1. Open **File – My Data Source Information**.

- Click on the envelope button to send the information to our support team. 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 username.

## DIAGNOSTIC

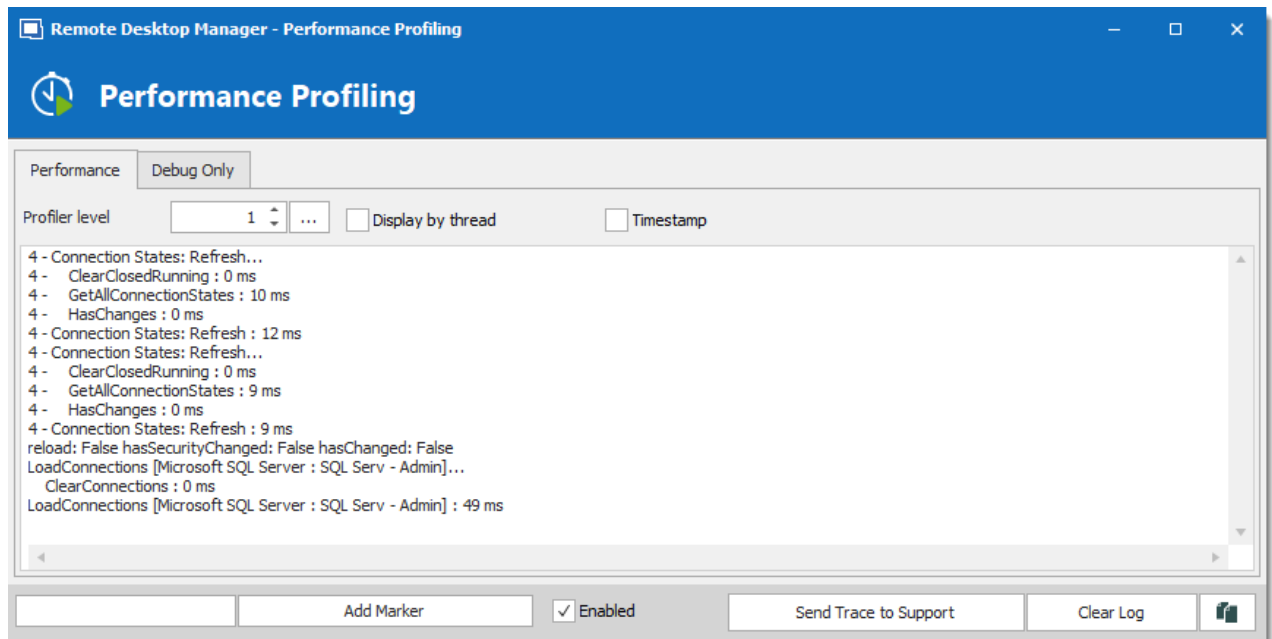


*Diagnostic Window*

- Open **Help – Diagnostic**.

- Click on the **Send** button. 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, please include your forum username.

## PROFILER



*Profiler*

- Open **Help – Profiler**, move the window aside to clear the main window of Remote Desktop Manager.
- Select the **Performance** tab.
- In Remote Desktop Manager, hold the CTRL key and press the refresh button.
- Information will be added in the **Performance** tab.
- Click on the **Send Trace to Support** button. 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, please include your forum username.

### 12.8.18.3 Startup

## DESCRIPTION

The start-up performance of the application can be affected by two main events:

- Launching the "Shell".
- Obtaining the content of the data source.

Since getting the data involves an additional layer that may be the cause of a perceived slowness for the application to be ready, we require that you create a new empty XML data

source to measure the application start-up time. This will in help determine if the issue lies with the shell or with the data source.

Please consult [Remote Desktop Manager Startup performance](#) for the first step. You can then consult [Performance - Data sources](#) if you feel that there is an issue in that area.

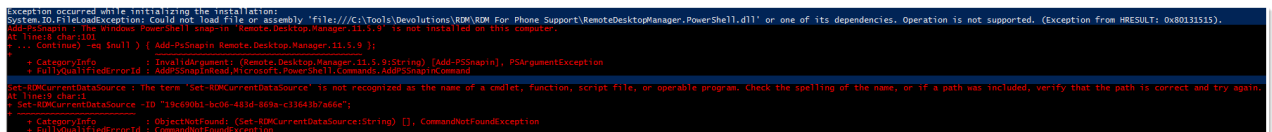
## 12.8.19 Powershell

### ERROR

When running **PowerShell (RDM CmdLet)** after deploying Remote Desktop Manager from the **\*.zip** file, you might see an error message like the following:

Exception occurred while initializing the installation:

System.IO.FileLoadException: Could not load file or assembly 'file:///C:\Tools\Devolutions\RDM\RDM For Phone Support\RemoteDesktopManager.PowerShell.dll' or one of its dependencies. Operation is not supported. (Exception from HRESULT: 0x80131515).



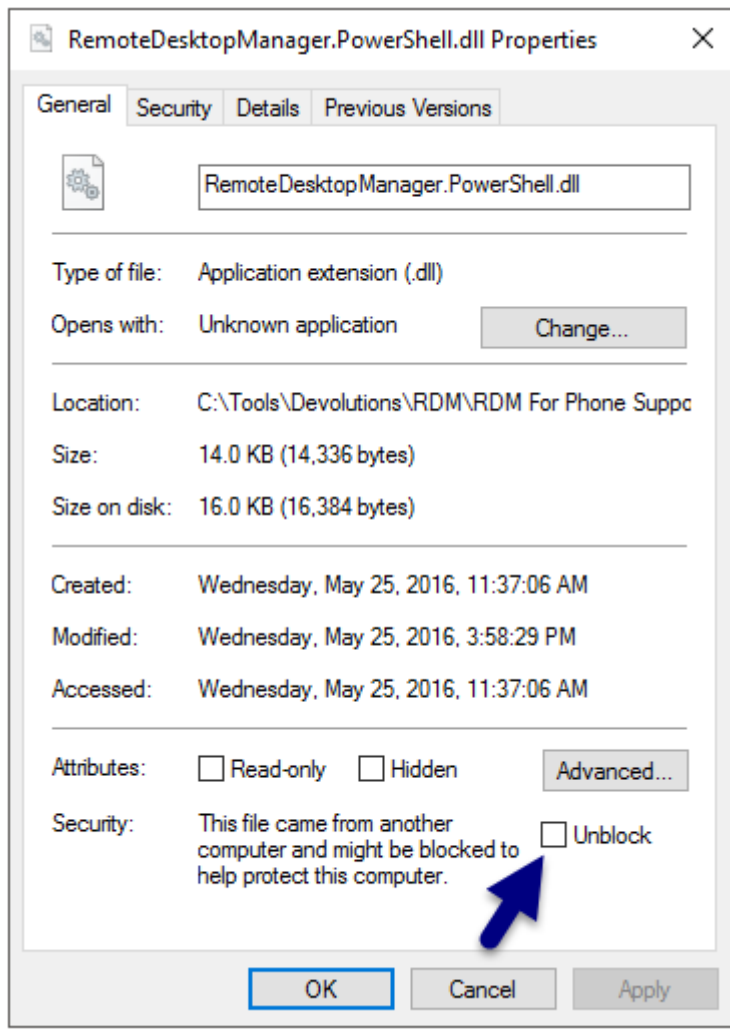
```
Exception occurred while initializing the installation:
System.IO.FileLoadException: Could not load file or assembly 'file:///C:\Tools\Devolutions\RDM\RDM For Phone Support\RemoteDesktopManager.PowerShell.dll' or one of its dependencies. Operation is not supported. (Exception from HRESULT: 0x80131515).
The Windows PowerShell snap-in 'RemoteDesktopManager.11.5.9' is not installed on this computer.
At line:1 char:10
+ ... Continue) -eq $null) { Add-PSSnapin RemoteDesktopManager.11.5.9 };
+ ~~~~~
+ CategoryInfo          : InvalidArgument. (RemoteDesktopManager.11.5.9:String) [Add-PSSnapin], PSArgumentException
+ FullyQualifiedErrorId : AddPSSnapinFailed,PowerShell.Commands.AddPSSnapinCommand

Set-RDMCurrentDataSource : The term 'Set-RDMCurrentDataSource' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:2 char:11
+ Set-RDMCurrentDataSource -ID "13c690b1-bc06-463d-803e-c1364b7a66e";
+ ~~~~~
+ CategoryInfo          : ObjectNotFound. (Set-RDMCurrentDataSource:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
```

Error Message

### SOLUTION

You must unblock **RemoteDesktopManager.PowerShell.dll** & **RemoteDesktopManager.Core.XmlSerializers.dll**. The 2 files are located in the installation folder of Remote Desktop Manager. **Right-click** on **RemoteDesktopManager.PowerShell.dll** & **RemoteDesktopManager.Core.XmlSerializers.dll** and select **Properties**. In the **Properties windows**, click on **Unblock**.



*Properties Of RemoteDesktopManager.PowerShell.dll*

## ERROR

Cannot load Windows PowerShell snap-in Remote.Desktop.Manager.10.0.4 because of the following error: Could not load file or assembly 'file:///C:\Program Files (x86)\Devolutions\Remote Desktop Manager\RemoteDesktopManager.PowerShell.dll' or one of its dependencies. This assembly is built by a runtime newer than the currently loaded runtime and cannot be loaded.

## SOLUTION

PowerShell v.4.0 need to be installed.





To get your PowerShell version, execute the following command:  
`$PSVersionTable`.

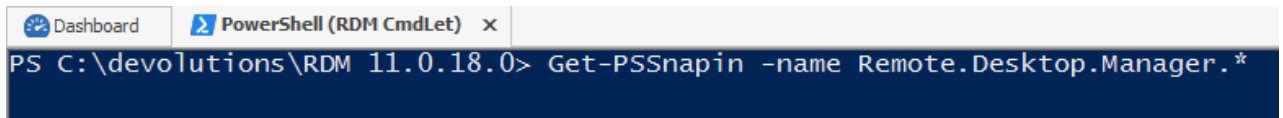
## ERROR

None of the Powershell cmdlets in Remote Desktop Manager work after an update, even if they were running correctly prior to the update.

## SOLUTION

The first step is to check how many versions of the RDM snap-in are currently installed on the computer. Just type this command in Powershell (RDM CmdLet) :

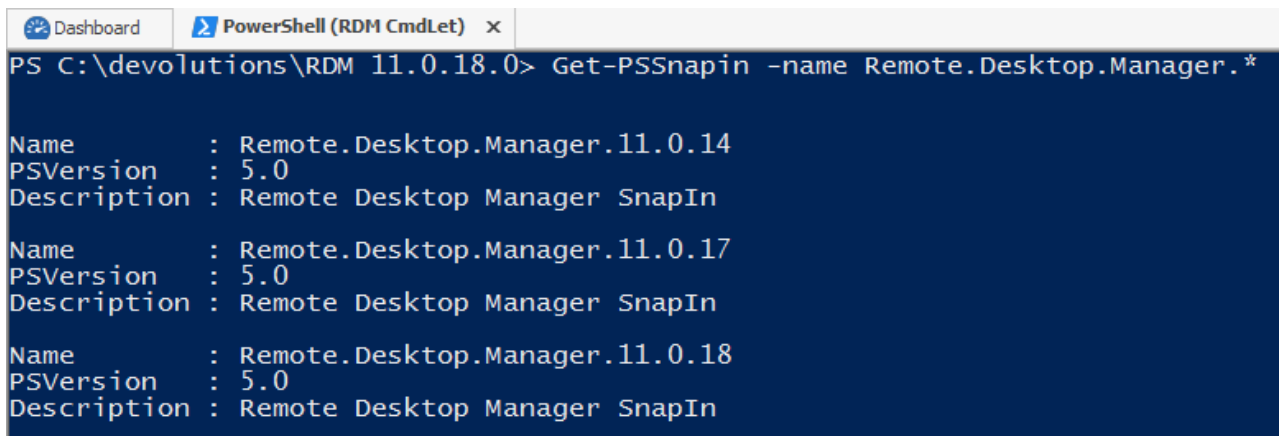
`Get-PSSnapin -name Remote.Desktop.Manager.*`



```
Dashboard PowerShell (RDM CmdLet) x
PS C:\devolutions\RDM 11.0.18.0> Get-PSSnapin -name Remote.Desktop.Manager.*
```

*Get-PSSnapin commandlet*

If there are more than one version of the snap-in installed, the result of the command will list them like this :



```
Dashboard PowerShell (RDM CmdLet) x
PS C:\devolutions\RDM 11.0.18.0> Get-PSSnapin -name Remote.Desktop.Manager.*

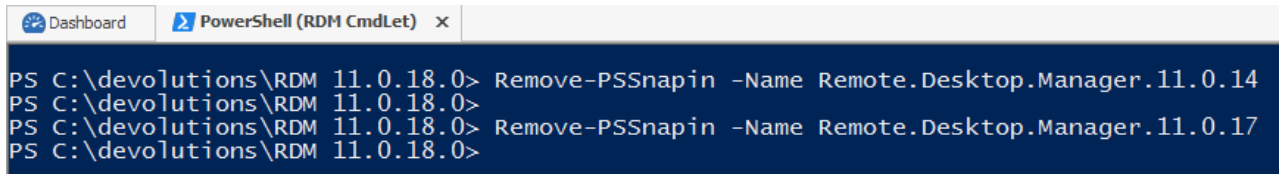
Name       : Remote.Desktop.Manager.11.0.14
PSVersion  : 5.0
Description : Remote Desktop Manager SnapIn

Name       : Remote.Desktop.Manager.11.0.17
PSVersion  : 5.0
Description : Remote Desktop Manager SnapIn

Name       : Remote.Desktop.Manager.11.0.18
PSVersion  : 5.0
Description : Remote Desktop Manager SnapIn
```

*List of all versions of the RDM snap-in*

To remove snap-ins that do not match with the actual version of Remote Desktop Manager installed on the computer, use the **Remove-PSSnapin** cmdlet, ensure you specify the specific version to remove.



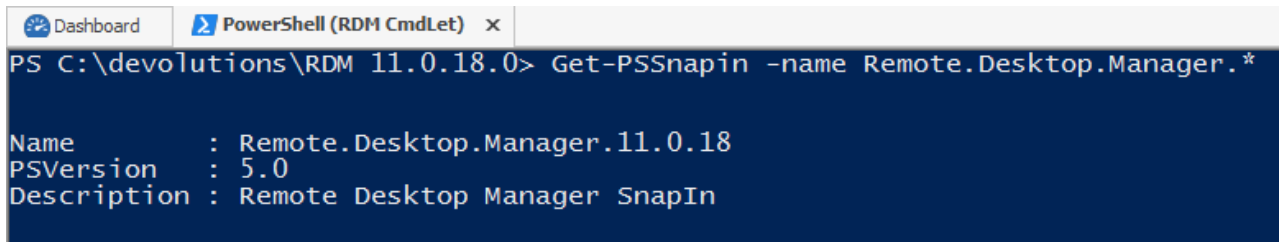
```

PS C:\devolutions\RDM 11.0.18.0> Remove-PSSnapin -Name Remote.Desktop.Manager.11.0.14
PS C:\devolutions\RDM 11.0.18.0>
PS C:\devolutions\RDM 11.0.18.0> Remove-PSSnapin -Name Remote.Desktop.Manager.11.0.17
PS C:\devolutions\RDM 11.0.18.0>

```

*Removing the undesired RDM snap-in*

Finally, verify if only the snap-in of the current version of RDM is installed with the Get-PSSnapin command.



```

PS C:\devolutions\RDM 11.0.18.0> Get-PSSnapin -name Remote.Desktop.Manager.*

Name          : Remote.Desktop.Manager.11.0.18
PSVersion     : 5.0
Description    : Remote Desktop Manager SnapIn

```

*List of all versions of the RDM snap-in*

## "CANNOT BE LOADED BECAUSE RUNNING SCRIPTS IS DISABLED ON THIS SYSTEM."

There are 2 probable causes.

1. This is a Windows Security Policy.

You must run the command below (Run as Administrator first);

```
Set-ExecutionPolicy
```

More Information can be found here;

<https://technet.microsoft.com/en-us/library/ee176961.aspx>


2. Open Remote Desktop Manager as Administrator and open the Powershell module and run;

```
Set-ExecutionPolicy
```

### 12.8.20 Putty

## ERROR

## PUTTY IN EMBEDDED MODE DOES NOT WORK IN THE APPLICATION

Remote Desktop Manager is not able to execute Putty in embedded mode when Team Viewer's QuickConnect button  is present in the title bar.

To resolve this issue, you need to disable the QuickConnect button in Team Viewer by unchecking the option **Extra – Options – Advanced – Show advanced options – QuickConnect button – Configure – Show QuickConnect button**.

This solution can also be applied to other applications such as Filezilla or Firefox.

## 12.8.21 Remote Desktop Manager

### ERRORS

#### MY MAPPED NETWORK DRIVE(S) ARE NOT AVAILABLE WHEN USING RUN AS ADMINISTRATOR TO LAUNCH REMOTE DESKTOP MANAGER

This is because of User Access Control (UAC), a built-in security layer of Windows. Effectively you are considered a different user with different preferences, the Mapped network drives being one such preference. In order to have the same mapped drives you have a few options:

1. Using an elevated command prompt, recreate the same mapped drive(s) using the `NET USE {DRIVENAME} {SHARENAME} /PERSISTENT:YES` command
2. Modifying the registry to link connections between the accounts, see <https://support.microsoft.com/en-us/kb/937624>.

#### "COULD NOT LOAD FILE OR ASSEMBLY "SYSTEM.ENTERPRISESERVICES.WRAPPER.DLL OR ONE OF ITS DEPENDENCIES. THE SYSTEM CANNOT FIND THE PATH SPECIFIED."

This error is due to a corrupted Microsoft's .NET Framework installation. Please consult the [Corrupted System File](#) topic for more information on how to resolve this issue.

#### "MIXED MODE ASSEMBLY IS BUILD AGAINST VERSION 2.0.50727 OF THE RUNTIME"

This should occur only on machines with development environments or when the .net framework have undergone multiple installs/uninstalls.

In RemoteDesktopManager.exe.cfg, which is located in the installation folder, locate the **startup** element and add the **useLegacyV2RuntimeActivationPolicy** attribute. The end result should look like:

```
<startup useLegacyV2RuntimeActivationPolicy="true">
```

## CAN'T PASTE IN ANY FIELDS OF REMOTE DESKTOP MANAGER

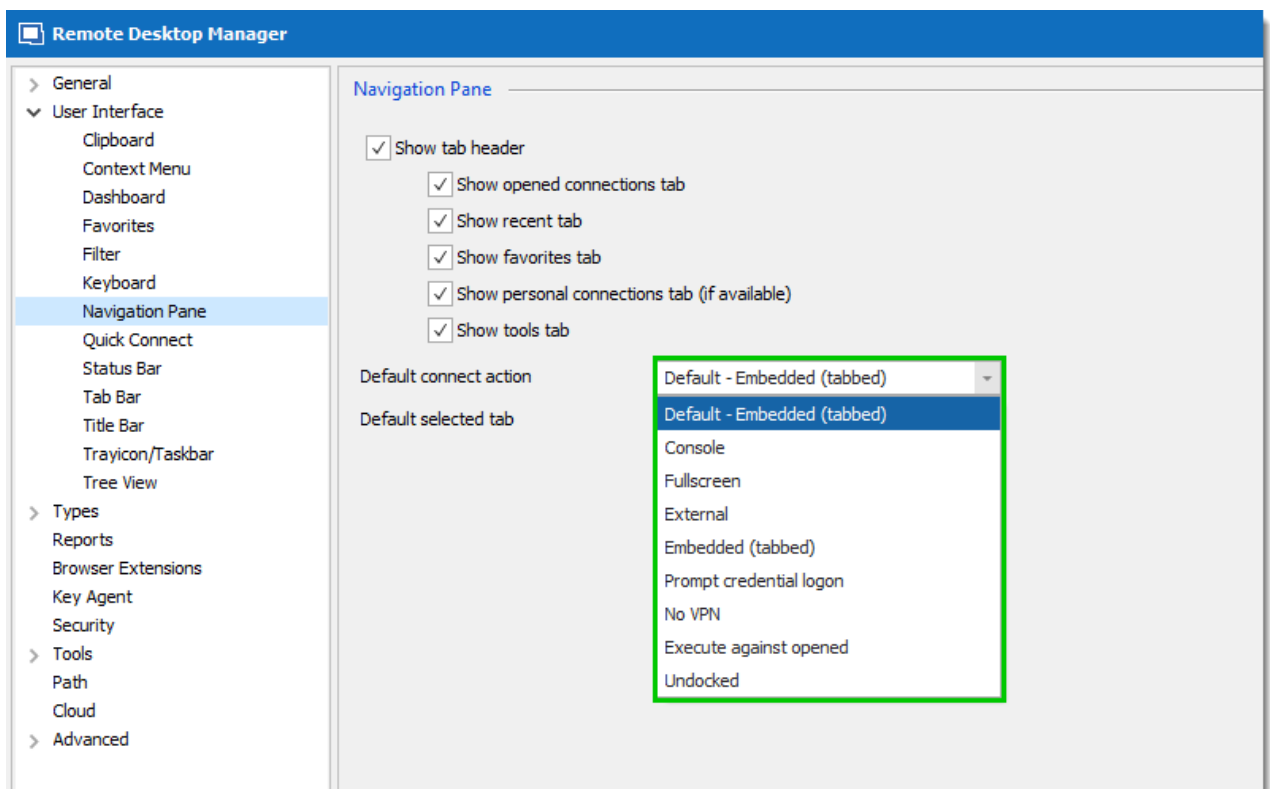
Webroot SecureAnywhere AntiVirus may cause the issue because of the Identity Protection module. Set **remotedesktopmanager.exe** to Allow and it will let you paste again in the application.

## REMOTE DESKTOP MANAGER HANGS

Please consult topic [Hung Remote Desktop Manager troubleshooting](#) for more information.

## ALL OF MY SESSIONS OPEN IN EMBEDDED AND/OR EXTERNAL MODE

All your sessions open in a display mode that is undesirable and you can't seem to set it the way you want by default. This can be changed by going in **File -> Options -> User Interface -> Navigation Pane**

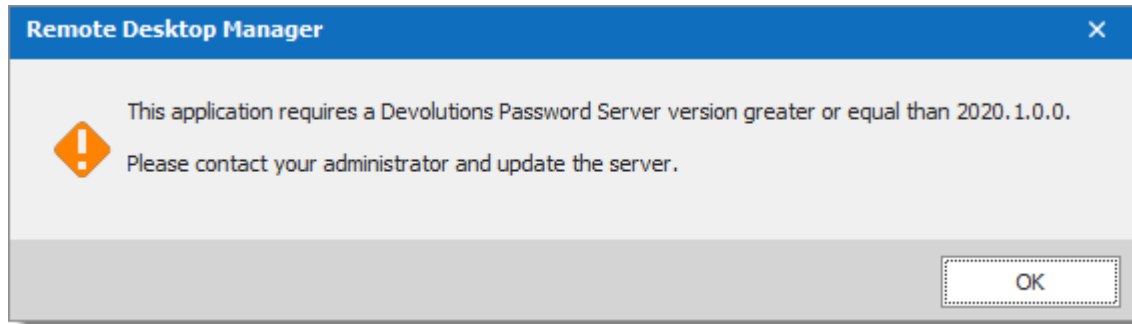


*Default Display Mode Action*

### 12.8.21.1 Application Requires DPS Version Greater or Equal

## DESCRIPTION

This application requires a <%DPS%> version greater or equal than...



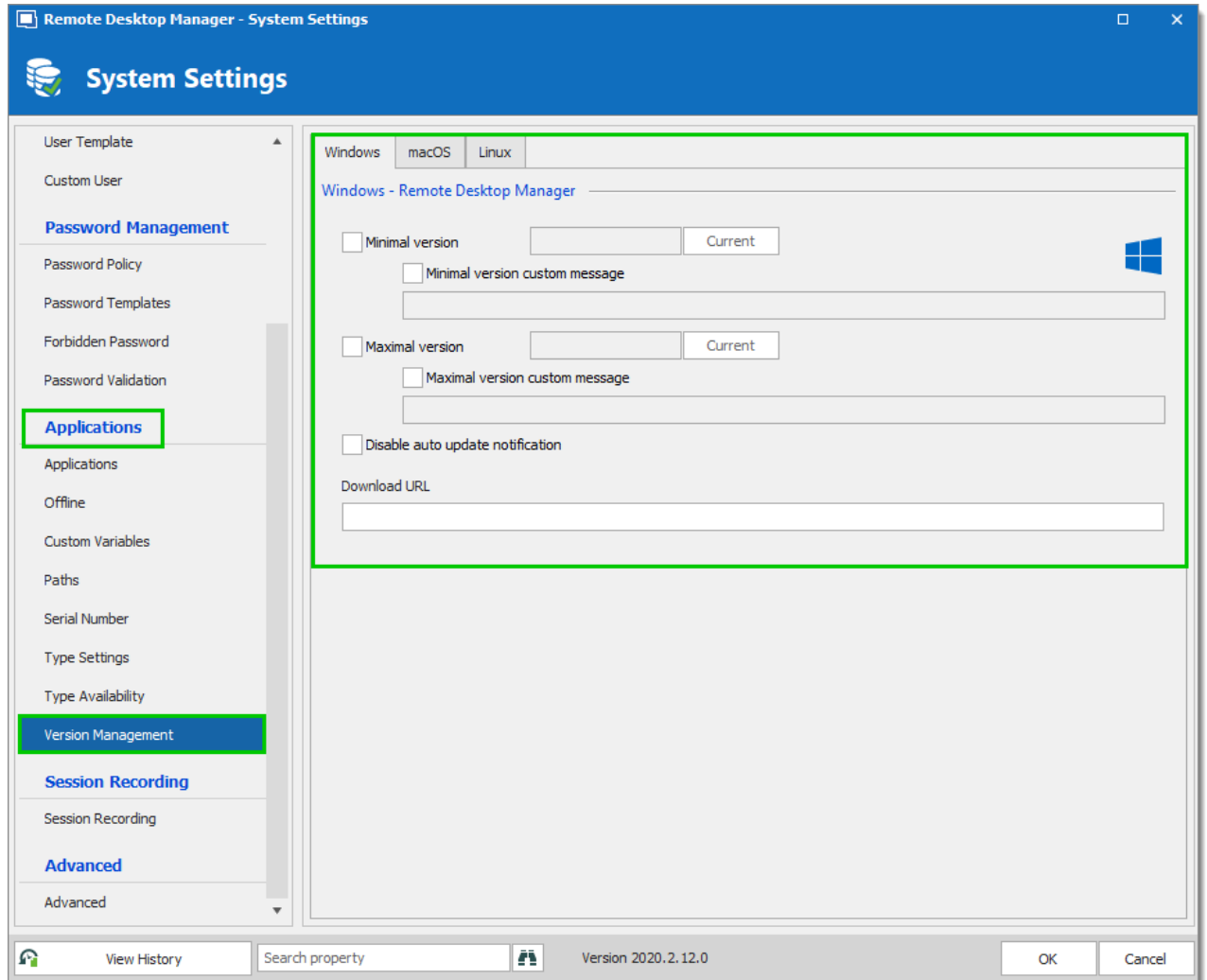
When Remote Desktop Manager is connected to a <%DPS%> data source, it will validate at start up the compatibility of both applications version. If an incompatibility occurs, the warning message above will appear in Remote Desktop Manager.

## SOLUTION

Firstly, we recommend a Devolutions Password Server upgrade. This link will provide instructions about how to perform the upgrade: [Upgrading Password Server](#). If you require assistance to perform the upgrade please contact us at [ticket@devolutions.net](mailto:ticket@devolutions.net).

## RECOMMENDATION

1. We strongly advise to deactivate the [auto-update](#) feature to avoid any unwanted update. Follow this link for more information about how to [apply policies](#) on Remote Desktop Manager group policies (GPO).
2. We recommend the use of the **Version Management** tool in **Administration - System Settings - Applications** of Remote Desktop Manager. This feature will prevent any unwanted upgrade unless approved by the administrator. Using this feature allows the administrator to control the Remote Desktop Manager versions available inside the organization.



*System Settings - Applications - Version Management*

### 12.8.21.2 Caching

## DESCRIPTION

You are not seeing the content that you're expecting to see in the [Navigation Pane](#).

## SOLUTION

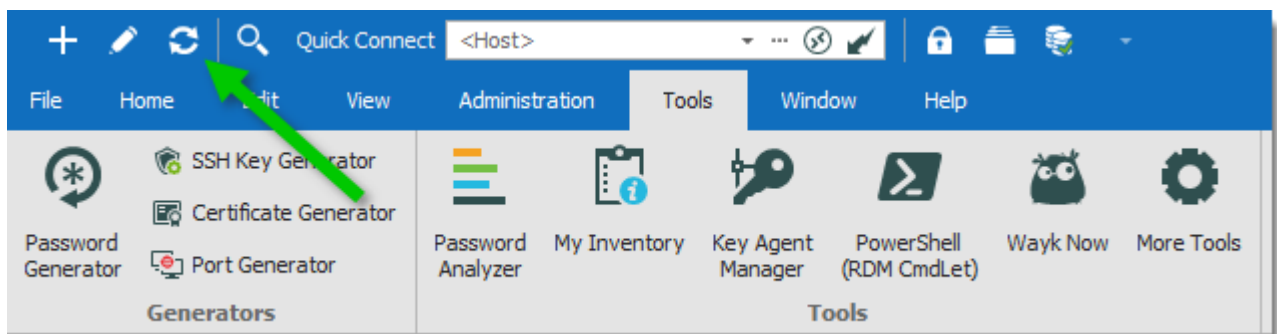
This issue can be caused by a corruption of the local cache. There's several methods to refresh the local cache in Remote Desktop Manager.

## METHOD 1

Press CTRL + F5 on your keyboard.

## METHOD 2

Hold the CTRL key on your keyboard and click on the **refresh** button in the [Quick Access Toolbar](#).



*Quick Access Toolbar*

## METHOD 3

You can manage the local cache by doing a **Vaccum**, a **Repair** or a **Delete**. Please consult [Manage Cache](#) topic for more information.

### 12.8.21.3 Debugging

## DESCRIPTION

Sometimes when an issue occurs while using Remote Desktop Manager, the support personnel may ask you to turn on debugging and send the information back. Here are two procedures that you can follow.

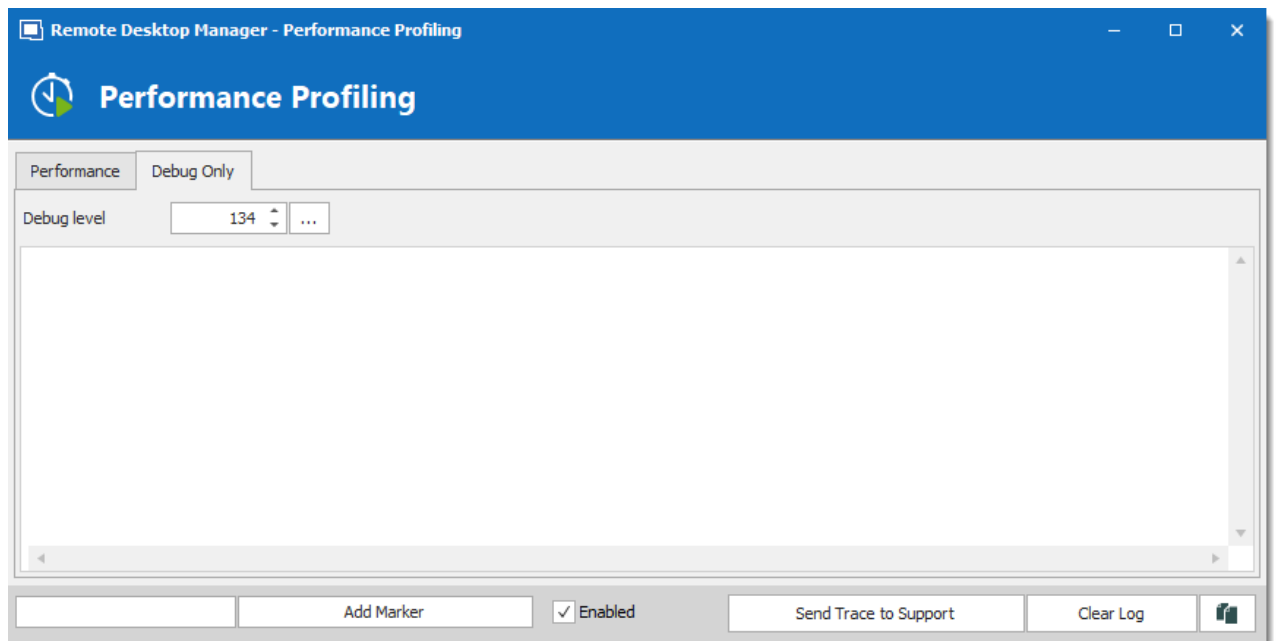


Any debug level other than zero will slow down the application and write a lot of information in the application logs. As soon as you have completed the diagnostics you should revert back the debug level to zero.

## PROCEDURES

Use the in-depth debugging method whenever you need to diagnose the startup or initial connection. The Ad-hoc debugging method is much easier to follow and is sufficient in most cases.

### AD-HOC DEBUGGING



*Debug only tab of the profiler window*

1. Open **Help – Profiler**, move the window aside to clear the main window of Remote Desktop Manager.
2. In the **Debug only** tab, click on the ellipsis button and activate the proper debug categories.
3. In Remote Desktop Manager, perform the action that is under investigation. For timing session load times, please press CTRL-F5 to invalidate the cache and perform a full refresh. You should see debug information appear in the profiler window.
4. 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 username.

### IN-DEPTH DEBUGGING



1. Open **File – Options – Advanced**, click on the **Debug level** ellipsis button and activate the proper debug categories.
2. In the Information section below, you will see a hyperlink to your configuration folder, press on it to have an explorer window opened in that folder.
3. Close Remote Desktop Manager.
4. As a preparatory phase, it would be best to clear existing logs to limit the scope of what will need to be analyzed. Delete or rename files named RemoteDesktopManager.log, RemoteDesktopManager.log.db and RemoteDesktopManager.debug from your configuration folder.
5. Start Remote Desktop Manager.
6. Perform the action that is under investigation.
7. Open **File – Options – Advanced**, set the **Debug level** to zero.
8. Close Remote Desktop Manager.
9. Package the **\*.log**, **\*.log.db** and **\*.debug** files from your configuration folder and send them to us.

#### 12.8.21.4 High CPU Usage

### DESCRIPTION

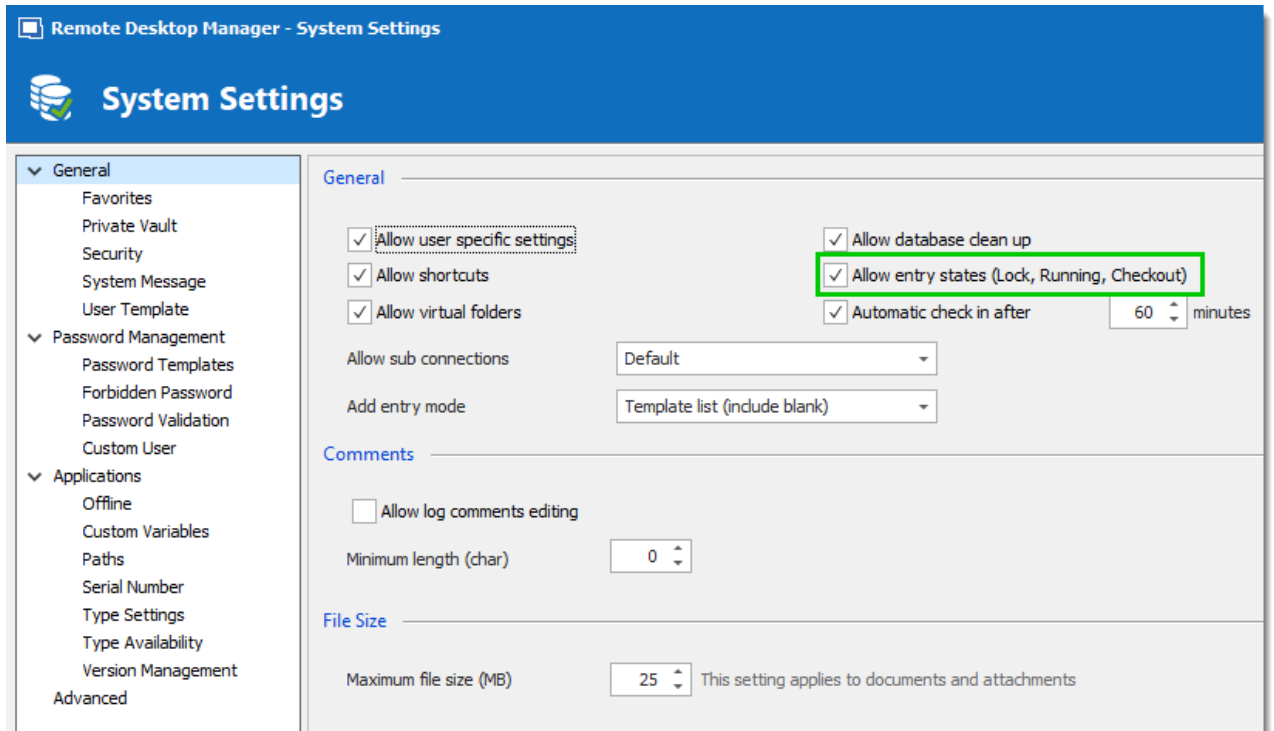
Since the release of Remote Desktop Manager 13, some users have experienced high CPU usage on their systems, especially in [Remote Desktop Services \(RDS\) environment](#). This is caused by the entry state verification feature.

### SOLUTION



This option is available with version 13.0.13.0 and above.

Disable the option **Allow entry states (Lock, Running, Checkout)** in **Administration – Data Source Settings (System Settings) – General** to improve performance on your servers and your workstations.



System Settings

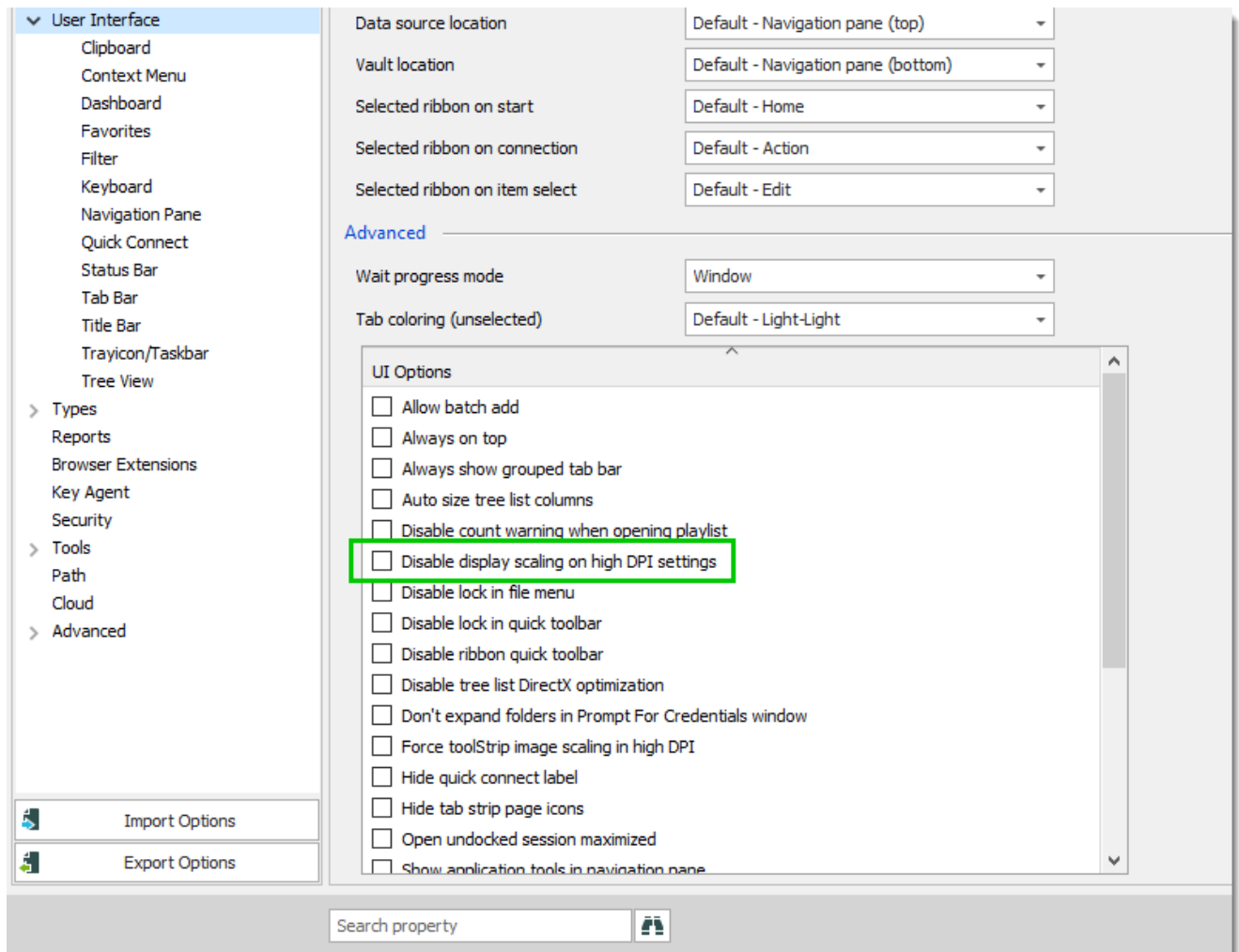
### 12.8.21.5 HDPI Scaling Issues

#### 4K SCREENS MAKE REMOTE DESKTOP MANAGER UNUSABLE

To resolve these issues, we will elaborate on two methods. One in Remote Desktop Manager and another using a built-in Windows functionality.

#### METHOD 1

First, in Remote Desktop Manager, go in **File – Options – User Interface** and please uncheck “**Disable display scaling on high DPI settings.**”



HDPI Scaling

If you cannot see the setting because of display issues, you can add the line in your config files directly. To locate your config file please refer to [Configuration File Location](#). Once you have found the right folder, please open **RemoteDesktopManager.cfg** with your preferred text editor. Under the line “<CreationDate>2016-11-14T00:00:00-05:00</CreationDate>” please add, “

```
<DisableHDPIAutoScaling>false</DisableHDPIAutoScaling>
```

Restart Remote Desktop Manager and the problem should be resolved.

## METHOD 2

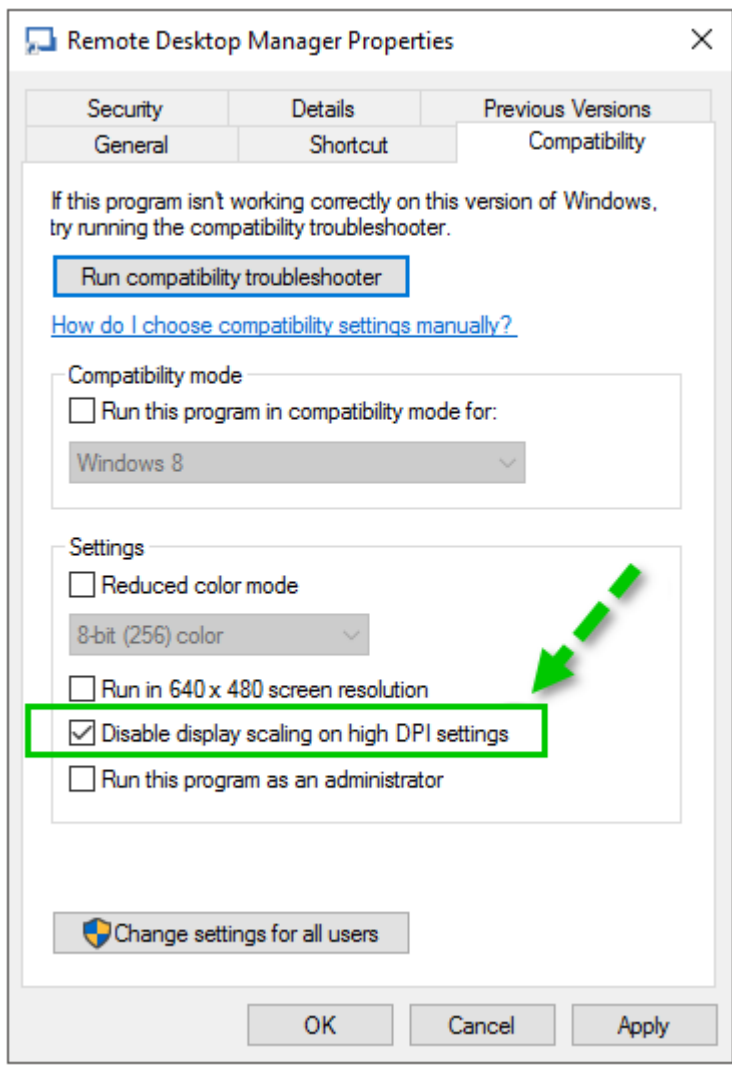
The second is directly with windows options.

Right-click on your Remote Desktop Manager icon. Go to **Properties** and in the **Compatibility** tab check **Disable display scaling on high DPI settings**.



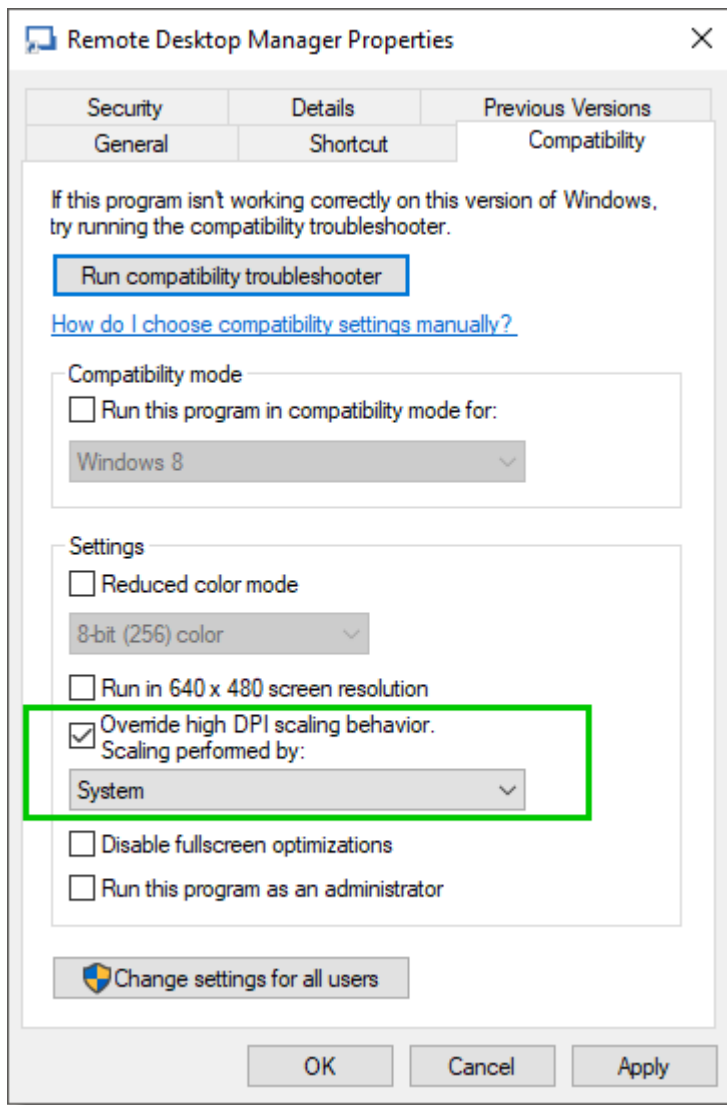
When applying this change, you must log off and log back in with your user for changes to take effect.

### Windows 10 Anniversary Update (Build 14393)



*DPI Settings*

### Windows 10 Creators Update (Build 15063 and above)



*DPI Settings*

#### 12.8.21.6 Hung Remote Desktop Manager

## DESCRIPTION

Remote Desktop Manager integrates with many different technologies and we do our best to isolate our main process from others, but it is not always possible.

## SYMPTOMS

## REMOTE DESKTOP MANAGER HANGS WHEN LOGGING OFF A RDP SESSION

Please refer to [RDM Hangs when logging off RDP sessions](#).

## REMOTE DESKTOP MANAGER HANGS FOR NO APPARENT REASON

Remote Desktop Manager hangs while you were not even using it or you were not using any other technology from within it. This makes it hard to identify the culprit. Advanced users can follow [Hung Remote Desktop Manager Dump file creation](#).

### 12.8.21.6.1 Hung Remote Desktop Manager Dump file creation

## DESCRIPTION



Follow this procedure **ONLY** when guided by a Devolutions support specialist.

There are no guarantees the we can identify the issue, but following this procedure may guide Devolutions towards identifying the root cause.



Please refrain from sending more than two dump files. We will simply not be able to analyze all of them.

## PROCEDURES

### AD-HOC METHOD

Perform this only when the application becomes unresponsive, meaning that it stops refreshing its screen and that the operating system adds the Unresponsive label in its title bar.

1. Launch the Task Manager.
2. Identify Remote Desktop Manager in the Apps list.
3. Right-click and choose **Create dump file**.
4. This will generate a file that cannot be transferred by email. There are multiple free online services to send large files, please [contact us](#) if you need a suggestion for such a service.

## USING THE PROCDUMP UTILITY

The following procedure makes use of a tool offered by Microsoft's Technet, namely the [Sysinternals](#) suite. The tool that we need is **procdump**. It is easier because the tool will monitor the application and create a dump file automatically.

Create a batch file containing a command such as:

```
{TOOLS_PATH}\procdump.exe -e -h -ma -g -x {DUMP_PATH} "{INSTALL_PATH}\RemoteDesktopManager
```

If the application becomes unresponsive, the tool will handle everything. Simply locate the dump file and send it to us.

### 12.8.21.7 Large Memory Aware Application

## DESCRIPTION

Remote Desktop Manager 32 bit version is limited in the amount of memory it can use. This is limited to 2 GB. This didn't cause issues until the release of Window 8 and Windows Server 2012, RDP connections to these OS's consume a large amount of memory, typically 140-160 Mb per connection.

Remote Desktop Manager 64 bit version allow the application to use as much memory as is available, in the mean time, we've modified Remote Desktop Manager to allow it to access more memory, but this must be paired with a modification to your operating system.



You can perform this only if you have more then 2 GB of RAM.

## INSTRUCTIONS

### WINDOWS XP/SERVER 2003

1. Right-click **My Computer** and select **Properties**. The System Properties dialog box will appear.
2. Click the **Advanced** tab.

3. In the **Startup and Recovery** area, click **Settings**. The **Startup and Recovery** dialog box will appear.
4. In the **System startup** area, click **Edit**. This will open the Windows *boot.ini* file in **Notepad**.
5. In the **[Operating Systems]** section, add the following switches to the end of the startup line that includes the `/fastdetect` switch: `/3GB`
6. Save the changes and close Notepad.
7. Click **OK** two times to close the open dialog boxes, and then restart the computer for the change to take effect.

## WINDOWS VISTA, WINDOWS 7, SERVER 2008



The memory parameter can be any value between 2048 (2 GB) and 3072 (3 GB). If you have 3GB of RAM you must reserve some for your system. If you have 3 GB of ram, allocate 2560 Mb, for 4 GB systems use 3072.

1. Open command prompt with Administrator rights. To do this, go to **Programs, Accessories**, right-click on **Command Prompt** and select "**Run as Administrator**".
2. Enter the following at the prompt and press enter:

```
bcdedit /set IncreaseUserVA 2560
```

3. Close the prompt and restart the computer.



## 12.8.21.8 Missing Navigation Pane

### DESCRIPTION

Several panes are missing in Remote Desktop Manager and you seem unable to bring them back.

### REMOTE DESKTOP MANAGER ENTERPRISE

Execute the following steps below:

- Close Remote Desktop Manager.
- Navigate to **%localappdata%\Devolutions**
- Copy the **RemoteDesktopManager** folder on your desktop.
- Delete the **RemoteDesktopManager** folder in **%localappdata%\Devolutions**
- Restart Remote Desktop Manager.

This will create a new **RemoteDesktopManager** folder in **%localappdata%\Devolutions**. If everything is back to normal, close Remote Desktop Manager again and copy the 3 files below from the folder **RemoteDesktopManager** on your desktop in **%localappdata%\Devolutions\RemoteDesktopManager** to restore your configuration and your local data source.

- **RemoteDesktopManager.cfg**
- **RemoteDesktopManager.ext**
- **Connections.db**

### REMOTE DESKTOP MANAGER FREE

Execute the following steps below:

- Close Remote Desktop Manager.
- Navigate to **%localappdata%\Devolutions**
- Copy the **RemoteDesktopManagerFree** folder on your desktop
- Delete the **RemoteDesktopManagerFree** folder in **%localappdata%\Devolutions**
- Restart Remote Desktop Manager.

This will recreate a new **RemoteDesktopManagerFree** folder in **%localappdata%\Devolutions**. If everything is back to normal, close Remote Desktop Manager again and copy the 3 files below from the folder **RemoteDesktopManagerFree** on your desktop in **%localappdata%\Devolutions\RemoteDesktopManagerFree** to restore your configuration and your local data source.

- **RemoteDesktopManagerFree.cfg**
- **RemoteDesktopManagerFree.ext**
- **Connections.db**

#### 12.8.21.9 Missing Sessions

## DESCRIPTION

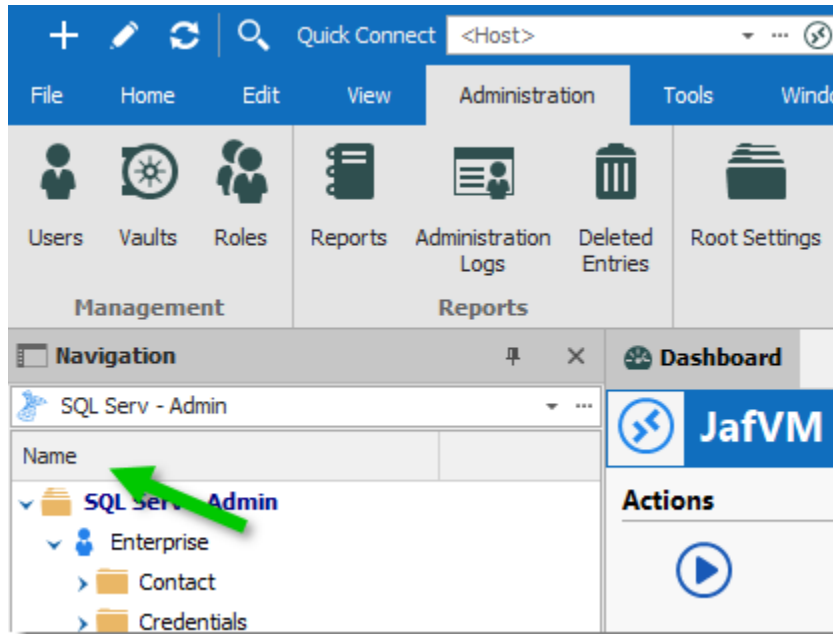
All entries are missing from the [Navigation Pane](#).

### SOLUTION 1

Refresh the local cache. Please consult the [Caching](#) topic for more information.

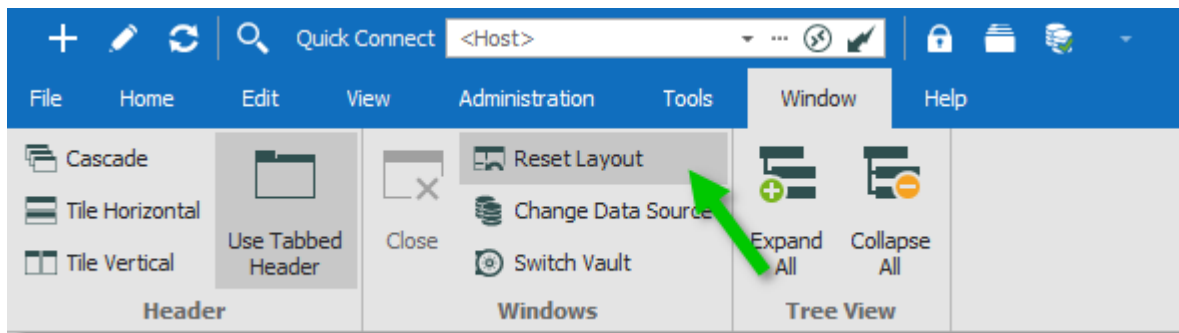
### SOLUTION 2

The **Name** column may be missing.



*Name Column Missing*

Click on **Window -> Reset Layout** to bring back the **Name** column.



*Reset Layout*

#### 12.8.21.1(Offline Mode

## ERRORS

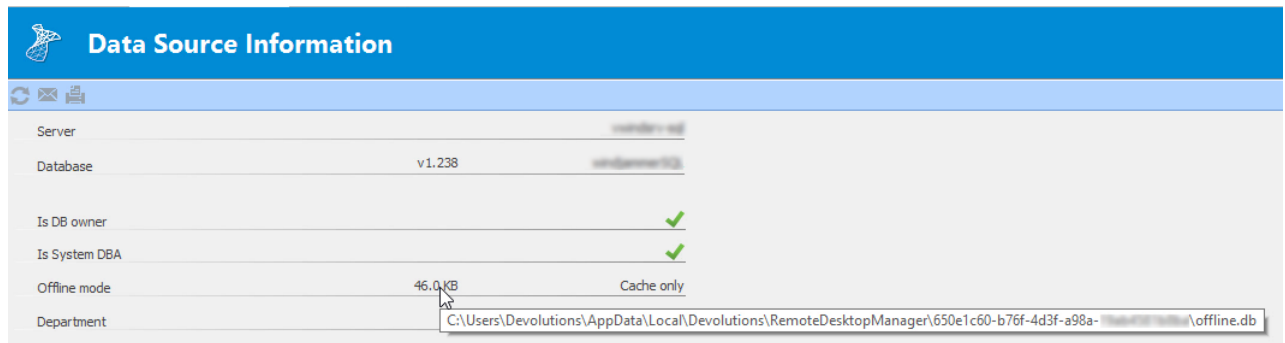
### MISSING ENTRIES OR DELETED ENTRIES STILL SHOWING

Your offline cache may be out of sync with the content of the data source. Press CTRL + F5 to refresh the local cache.

## SYSTEM.DATA.SQLite.SQLiteEXCEPTION (0X80004005): FILE IS ENCRYPTED OR IS NOT A DATABASE

The offline file (**offline.db**) needs to be deleted manually.

Click on **File – My Data Source Information** and now hover over the file size. This will give you the full file path, something like `%LocalAppData%\Devolutions\RemoteDesktopManager\GUID-DatasourceID\offline.db`.



*My Data Source Information*

Close Remote Desktop Manager, delete the **offline.db** file and restart Remote Desktop Manager. This will force the application to recreate the offline file.

### 12.8.21.11 Profiler

## DESCRIPTION

Please consult the [Profiler](#) topic for more information.

### 12.8.21.12 Proxy Authentication Required Error

## DESCRIPTION

When opening Remote Desktop Manager, you receive the following error message;

The remote server returned an error. (407) Proxy Authentication Required.

## SOLUTION 1

Please configure your proxy in **File -> Options -> Proxy**.

## SOLUTION 2

Please add the ***devolutions.net*** in your Proxy's exception list.

For those using our cloud solutions, please also add <https://cloud.devolutions.net>.

#### 12.8.21.13Red X in Navigation Pane or Credential List

### DESCRIPTION

There is a huge Red "X" in the Navigation Pane or in the Credential List

### SOLUTION

There are a few things you can try to get rid of the red X.

First, try going to the Window tab and click Reset Layout

Sometimes that can fix some Red X issues.

If that doesn't work, you can try to close RDM, then navigate to %localappdata% -> Devolutions -> RemoteDesktopManager and delete every file with the .lyt extension.

If neither of those methods does the trick, you will have to move the RemoteDesktopManager folder from localappdata to your desktop, then uninstall RDM, reboot your computer and reinstall RDM. Once you reopen RDM, the red X should be gone.

#### 12.8.21.14Root Is Empty Error

### DESCRIPTION

After upgrading to Remote Desktop Manager 13.5.x, you may receive the error below;

RootException - Root is empty!

```
at
Devolutions.RemoteDesktopManager.Managers.RootConnectionManager.get_RootConnectio
n()

at
Devolutions.RemoteDesktopManager.Frames.ConnectionViews.FreConnectionTreeListView.c
e5f4c5875531b613e87da05d31efd852(ConnectionViewMode
cfa8984eaceb595fb57911c4e0ee96824)

at
Devolutions.RemoteDesktopManager.Frames.ConnectionViews.FreConnectionTreeListView.L
oadConnectionList(Connection[] connections, ConnectionViewMode viewMode)

at
Devolutions.RemoteDesktopManager.Forms.FrmMainRibbonBase.LoadAllConnectionView(Bo
olean saveState)

at
Devolutions.RemoteDesktopManager.Forms.FrmMainRibbonBase.RefreshAllConnectionView(
Boolean saveState, Boolean checkOnline)

at Devolutions.RemoteDesktopManager.Managers.MainFormManager.DoFirstLoad(IMainForm
mainform)

at
Devolutions.RemoteDesktopManager.Forms.FrmMainDocumentManager.cae3b4c7c167cf0d9
747ac4fee11ac00a(Object c19f185fd70cefc696ba148af1c4faf54, EventArgs
cf1018bb83ec7debd818319fd3cb4844e)

at System.Windows.Forms.Timer.OnTick(EventArgs e)

at System.Windows.Forms.Timer.TimerNativeWindow.WndProc(Message& m)

at System.Windows.Forms.NativeWindow.Callback(IntPtr hWnd, Int32 msg, IntPtr wparam,
IntPtr lparam)
```

## SOLUTION 1

Many issues related to it have been addressed in the latest version which you can download here;

<https://remotedesktopmanager.com/home/download>

## SOLUTION 2

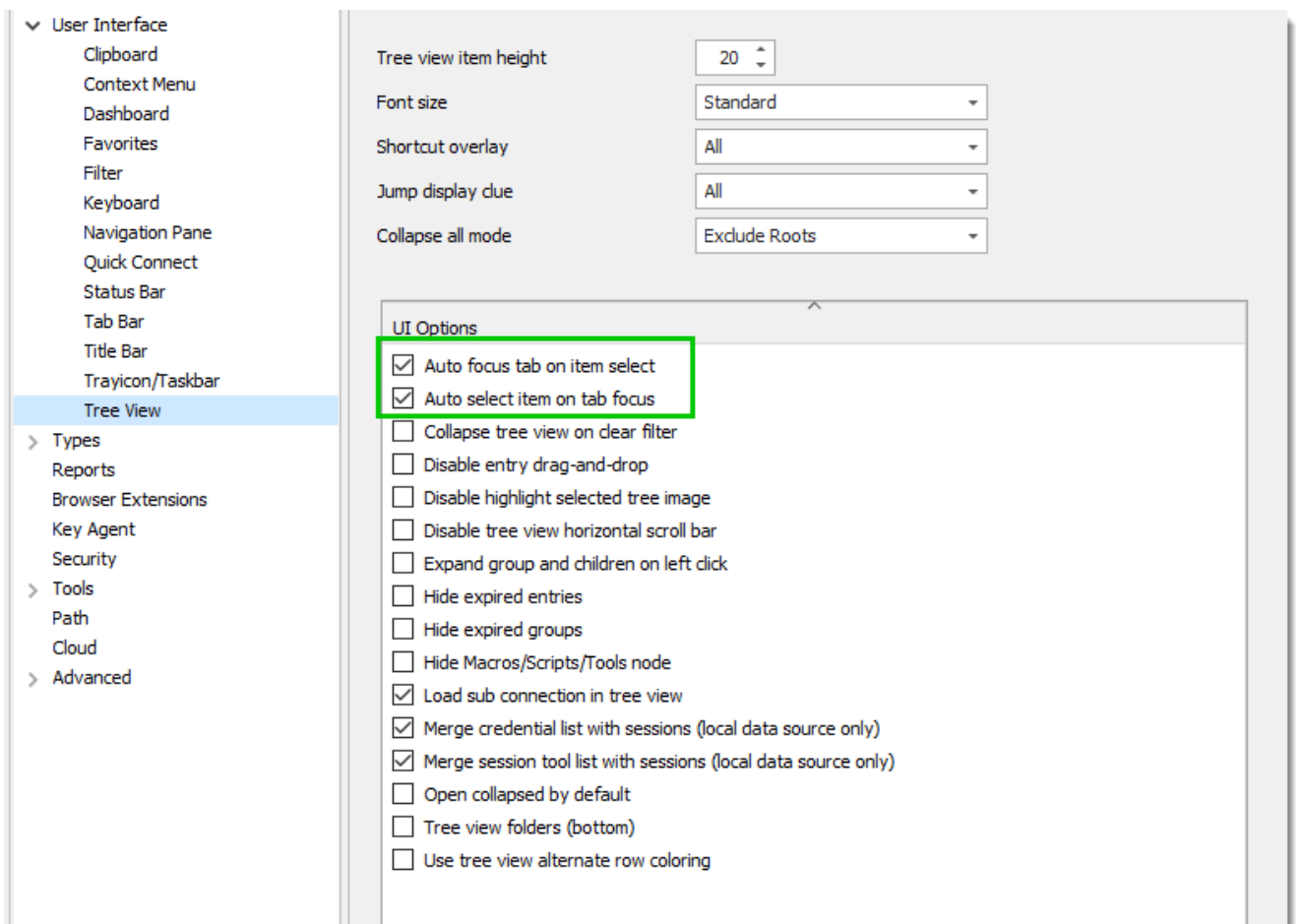
The other solution is to simply switch between data sources or delete and recreate the data source in **File -> Data Sources**.

### 12.8.21.1!Session Focus Issue

## DESCRIPTION

### AFTER CLOSING A SESSION, THE FOCUS IS SET TO THE LAST OPENED CONNECTION.

There are two settings in **File -> Options -> User Interface -> Tree View** that you can enable/disable to resolve this issue. Those are **Auto focus tab on item select** and **Auto select item on tab focus**.



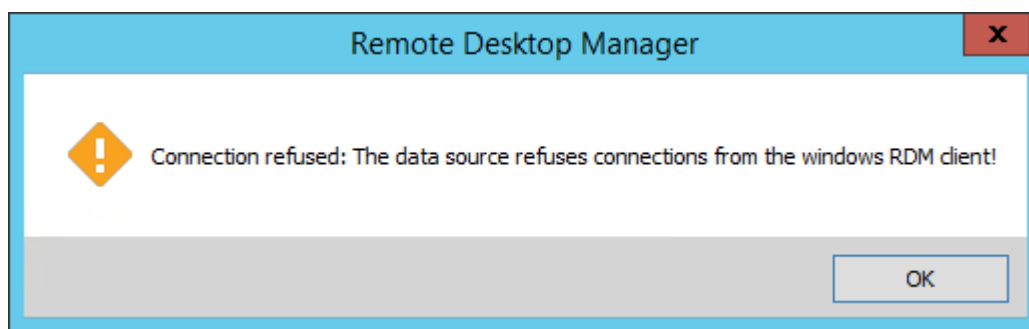
**Tree View Options**

### 12.8.21.1 SQL Server Data Source Connection Refused

## DESCRIPTION

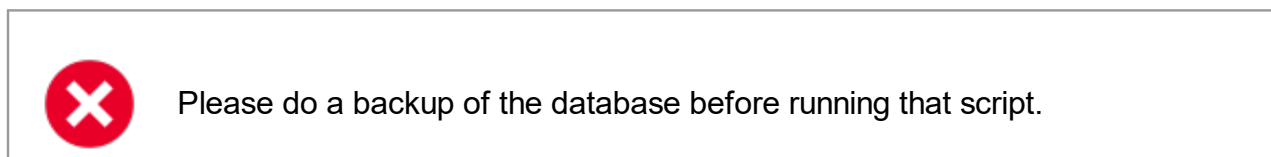
### UNABLE TO CONNECT FROM RDM OR PVM. CONNECTION REFUSED.

When you try to connect from either Remote Desktop Manager and/or Password Vault Manager, you receive the following message;



*Data Source Connection Error*

You will need to access the database via **SQL Server Management Studio** and execute the following statement on the database;



```
UPDATE dbo.DatabaseInfo
```

```
SET Settings = REPLACE(Settings,  
'<AllowAccessWindowsPVM>false</AllowAccessWindowsPVM>', '')
```

```
UPDATE dbo.DatabaseInfo
```

```
SET Settings = REPLACE(Settings,  
'<AllowAccessWindowsRDM>false</AllowAccessWindowsRDM>', '')
```

### 12.8.21.1 Startup performance

## DESCRIPTION





As described in the [Performance](#) chapter, the application performance must be validated with an empty data source. Please create a new empty XML data source and select it as being the current data source.

If you experience slow startup times, there are a few things to try in order to reduce the time before the application is available for use.

## SLOW STARTUP ON MACHINES THAT ARE NOT CONNECTED TO THE INTERNET.

For your security, we "sign" our program with a code signature. This results in the validity of the signature being checked at application startup. If the machine is not connected to the internet the application will wait for a response until a timeout occurs. For detailed explanations please read the following:

- [Improving Application Start Up Time](#)
- <https://blogs.technet.microsoft.com/markrussinovich/2009/05/23/the-case-of-the-slow-keynote-demo/>

The workaround is to create a text file in Remote Desktop Manager installation folder, named ***RemoteDesktopManager.exe.config*** that must contain the following:

```
<configuration>
  <runtime>
    <generatePublisherEvidence enabled="false"/>
  </runtime>
</configuration>
```

## PREVENT INTERNET ACCESS

Every time you start Remote Desktop Manager, the application will try to connect on <https://remotedesktopmanager.com/clientinternal/enterpriseneeds>. You should prevent all internet access from the application.

Add the line **<DisableAnalytics>true</DisableAnalytics>** to your [RemoteDesktopManager.cfg](#) file. You can place it above the last line, which should contain

**</Option>**. You can find the configuration file using **File – Options – Advanced** and click on the blue hyperlink at the bottom.

```

100 <TodoFilterOption />
101 <UserTemplatesArray>
102   <UserInfoTemplate>
103     <CustomSecurity>
104       <AllowDragAndDrop>>false</AllowDragAndDrop>
105     </CustomSecurity>
106   </UserInfoTemplate>
107 </UserTemplatesArray>
108 <VideoRecorderFrameRate>5</VideoRecorderFrameRate>
109 <WebBrowserScriptErrorsSuppressed>>true</WebBrowserScriptErrorsSuppressed>
110 <DisableAnalytics>>true</DisableAnalytics>
111 </Option>

```

*RemoteDesktopManager.cfg*

## NATIVE IMAGE GENERATION

Remote Desktop Manager is a .NET application. This means that the code is delivered in an intermediate format. It is then processed on your local machine in order to generate what is called a **Native Image**. Sometimes, this process can be slow. It can also reoccur after certain conditions are met. For these reasons, we deliver a batch file to process all of our files at once. You will find this file in the installation folder of Remote Desktop Manager. It is called *OptimizeRDM.bat*. Please open a Command Window using Run As Administrator and launch that script.

## ANTIVIRUS

It is possible that an antivirus application is causing slowdowns.



We do not recommend turning off the antivirus protection in risky conditions. You should close all browsers and ensure that only essential applications are running. We also suggest this step only for a short duration in order to see the startup time of the application change significantly.

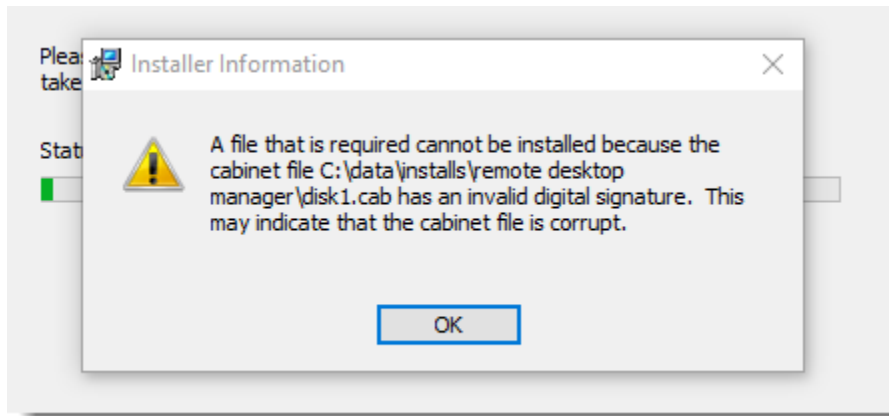
If your antivirus application allows it, simply turn off monitoring of Remote Desktop Manager's installation folder. If you are comfortable with turning off the whole antivirus protection, do this to test the startup time.

There is sadly nothing we can do in this case. It is only a step that helps in isolating the cause.

## 12.8.21.1 Unable to install or upgrade

### DESCRIPTION

When you install or upgrade Remote Desktop Manager, you receive this error message below;



*Installation Error Message*

You simply have to deploy the **\*.zip** file of Remote Desktop Manager in Remote Desktop Manager's installation folder.

By default, Remote Desktop Manager is installed in **C:\Program Files (x86)\Devolutions\Remote Desktop Manager**.

When the **\*.zip** file is downloaded, extract or copy/paste the content of the **\*.zip** file in the **C:\Program Files (x86)\Devolutions\Remote Desktop Manager** folder. When you restart Remote Desktop Manager, the latest version will be installed.

You can download the zip here; <https://remotedesktopmanager.com/Home/Download>.

## 12.8.21.1 Unable to Uninstall

### ERROR

#### UNABLE TO UNINSTALL REMOTE DESKTOP MANAGER FROM YOUR COMPUTER BECAUSE OF A MISSING MSI FILE

To fix issues that you may encounter with the installation, removal of the application or missing MSI file, please run the Microsoft Troubleshooting tool on your computer.

[https://support.microsoft.com/en-us/mats/program\\_install\\_and\\_uninstall](https://support.microsoft.com/en-us/mats/program_install_and_uninstall)

If the installer still reports an error, please run the installer from the command line using these parameters:

```
msiexec /i "{Name of msi package}" /L*V "Name of log file"
```

Please adapt to your environment and the folders that you use. Here is an example:

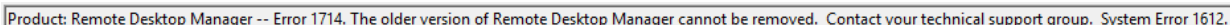
```
msiexec /i "Setup.RemoteDesktopManager.11.7.6.0.msi" /L*V "C:\log\RdmInstall.log"
```

Send the resulting log file to [ticket@devolutions.net](mailto:ticket@devolutions.net).

#### 12.8.21.2 Upgrade

## DESCRIPTION

You seem unable to uninstall Remote Desktop Manager from Programs and Features in Windows. In the Event log; you see the following error message;

A screenshot of an event log message box. The text inside the box reads: "Product: Remote Desktop Manager -- Error 1714. The older version of Remote Desktop Manager cannot be removed. Contact your technical support group. System Error 1612." The box has a light gray background and a thin border.

Product: Remote Desktop Manager -- Error 1714. The older version of Remote Desktop Manager cannot be removed. Contact your technical support group. System Error 1612.

*Event Log Message*

## STEP1

Please try the suggested fix by Microsoft here; <https://support.microsoft.com/en-us/help/17588/fix-problems-that-block-programs-from-being-installed-or-removed>.

Your settings and local data for RDM are by default under **%LOCALAPPDATA%\Devolutions\RemoteDesktopManager**, our installer doesn't touch this at all. You must preserve this folder in its current state.

## STEP 2

Once this is done, please contact [ticket@devolutions.net](mailto:ticket@devolutions.net) for further assistance.

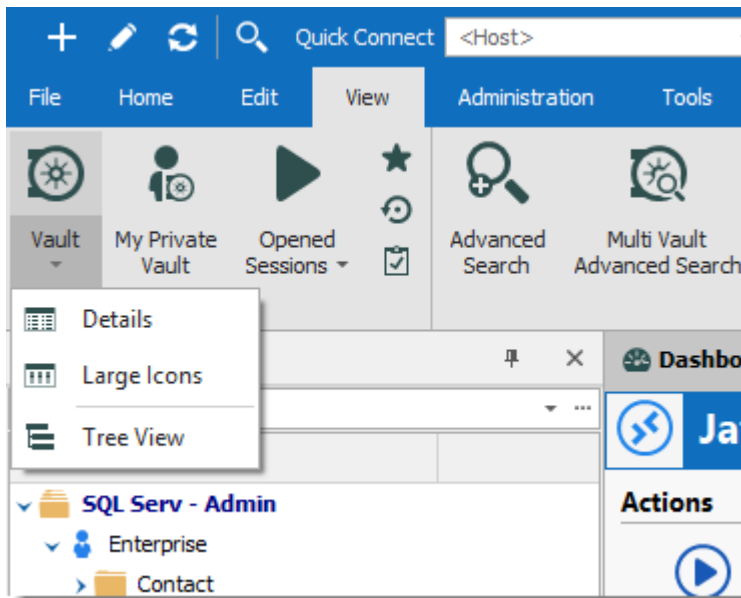
#### 12.8.21.2 User Interface

## THE RIBBON HAS BEEN HIDDEN AND I DON'T KNOW HOW TO MAKE IT VISIBLE

You have two options: Use the **Alt + F11** shortcut or using the system menu of the application you can check the "Top Pane" command. Please see [Top Pane](#) for more information.

## THE TREE VIEW HAS DISAPPEARED FROM THE NAVIGATION PANE

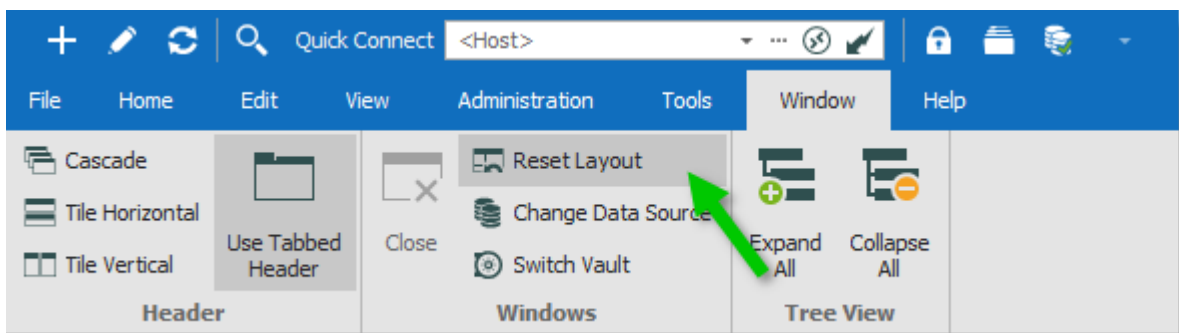
The Navigation Pane can be displayed in many modes. You can select the tree view with **View – Vault – Tree View** or use the default shortcut **F7**.



*View - Vault Menu*

## THE MAIN FORM LAYOUT IS BROKEN

Use the **Reset Layout** option to revert back to the default UI layout in the **Window** tab.



*Reset Layout Button*



The reset layout might not resolve all the issues. Close the application and delete the layout files (\*.lyt) in %LocalAppData%\Devolutions\RemoteDesktopManager to completely restore the layout.

## THE QUICK ACCESS TOOLBAR NEEDS TO BE RESET

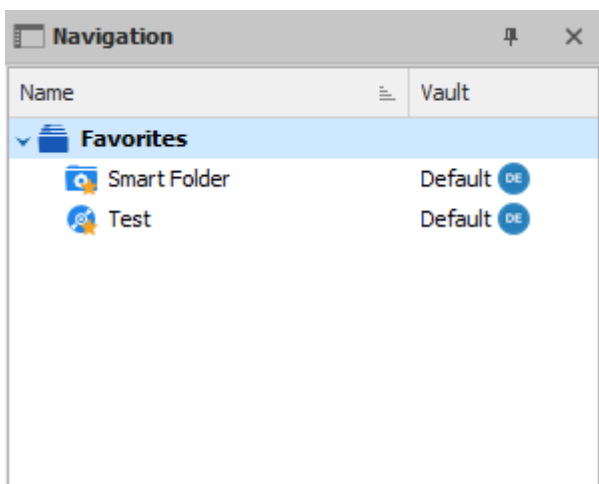


Quick Access Toolbar

To reset the quick access toolbar, close the application and delete the file **remotedesktopmanager.qtb** in %LocalAppData%\Devolutions\RemoteDesktopManager

## THE NAVIGATION PANE DISPLAYS ONLY MY FAVORITES

Only your favorites are displayed, the root node is also entitled "**Favorites**".



You may have inadvertently enabled a filter. Click on the ellipsis button of the search filter box and deselect the **Show Only Favorites** menu item. Simply **Vault** or whichever view you expected at the bottom of the pane.

### 12.8.21.2 Version Compatibility for RDM and DPS

## DESCRIPTION

Here a compatibility board explaining which version of Remote Desktop Manager should be used with Password Server and vice-versa.

Remote Desktop Manager Version	Devolutions Password Server Version
2020.1.20.0	2020.1.13.0
2019.2.24.0	2019.2.12.0
2019.1.41.0	2019.1.20.0
14.1.3.0	6.1.3.0
13.6.7.0	5.1.4.0
13.0.6.0	5.0.2.0
12.6.8.0	4.7.0.0

## 12.8.22 RPC

### ERRORS

#### THE RPC SERVER IS UNAVAILABLE (EXCEPTION FROM HRESULT: 0X800706BA)

This error may occur in the normal operation of RDM. The root causes are network connectivity or stopped Windows services.

- 1) Ensure the host is properly identified (**Name** or **IP address**) and it is indeed running and accepting network traffic.
- 2) Ensure the host firewall allows inbound traffic for Windows Management Instrumentation.
- 3) Ensure the following services are started and are set to automatic startup type.
  - **TCP/IP NetBIOS Helper**
  - **Remote Procedure Call (RPC)**
  - **Windows Management Instrumentation**

## 12.8.23 Secret Server

### DESCRIPTION

#### TESTING PROCEDURE WITH POWERSHELL

Here is a script that you can use to test your access from a client workstation.

Save the following code in a file called ***searchsecret.ps1***.

Change the script as needed to match your Secret Server and username/password/domain.

Change the \$searchterm to match your search.

This will allow you to test the connectivity between your workstation and your Secret Server server.

```
$url = 'http://mysecretserver/webservices/sswebservice.asmx'
$username = 'myusername'
$password = 'mypassword'
$domain = 'mydomain'    # leave blank for local users

$searchterm = 'VPN'
$proxy = New-WebServiceProxy -uri $url -UseDefaultCredential

# get a token for further use by authenticating using username/password
$result1 = $proxy.Authenticate($username, $password, '', $domain)
if ($result1.Errors.length -gt 0){
    $result1.Errors[0]
    exit
}
else
{
    $token = $result1.Token
}

# search secrets with our searchterm (authenticate by passing in our token)
Write-Host 'Searching for: ' $searchterm
$result2 = $proxy.SearchSecrets($token, $searchterm,$null,$null)
if ($result2.Errors.length -gt 0){
    $result2.Errors[0]
}
else
{
    Write-Host 'Got search results: ' $result2.SecretSummaries.length

    # If you want the data as XML
    # $xml = convertto-xml $result2.SecretSummaries -As string -Depth 20
    # $xml

    $result2.SecretSummaries | ForEach-Object { Write-Host 'SecretId:' $_.SecretId ' Name:'
```

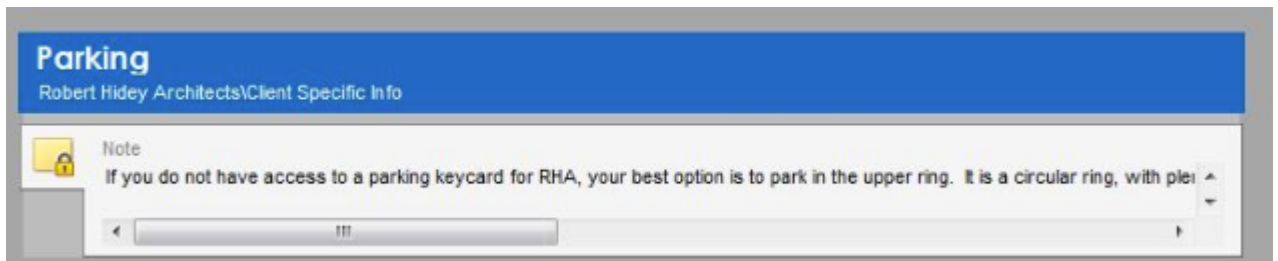


```
# if ($result2.SecretSummaries.length -gt 0) {  
# $result2.SecretSummaries[0]  
# }  
  
}
```

## 12.8.24 Secure Note

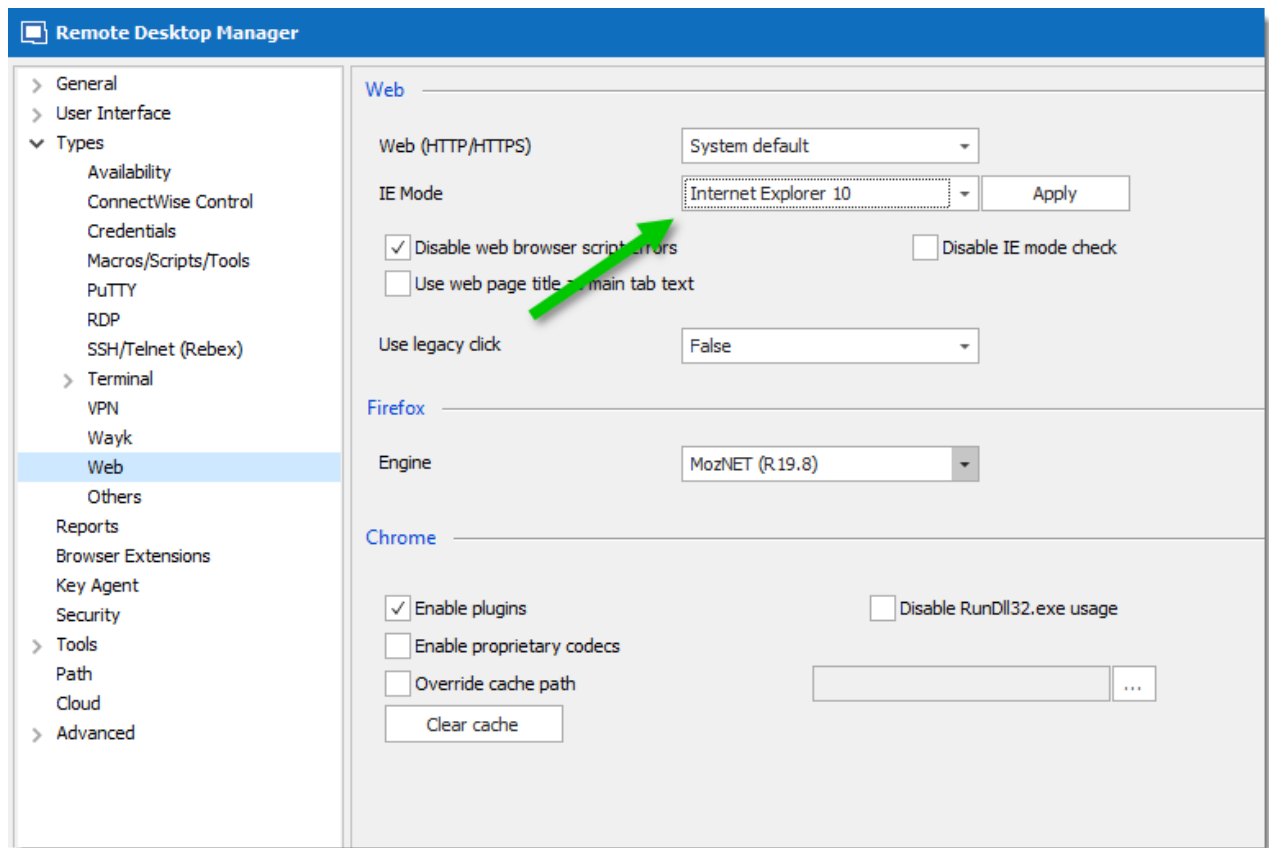
### ERROR

THE TEXT IN A SECURENOTE IS NOT DISPLAYED PROPERLY.



SecureNote

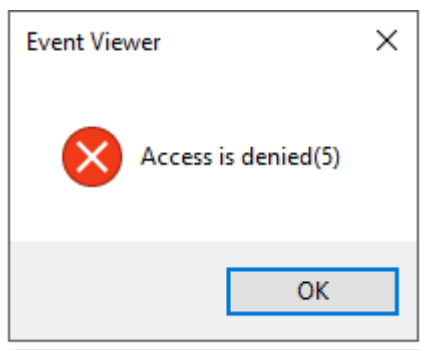
Change the IE emulation mode in **File – Options – Types – Web**, set the **IE Mode** to use **Internet Explorer 10**.

*IE Mode*

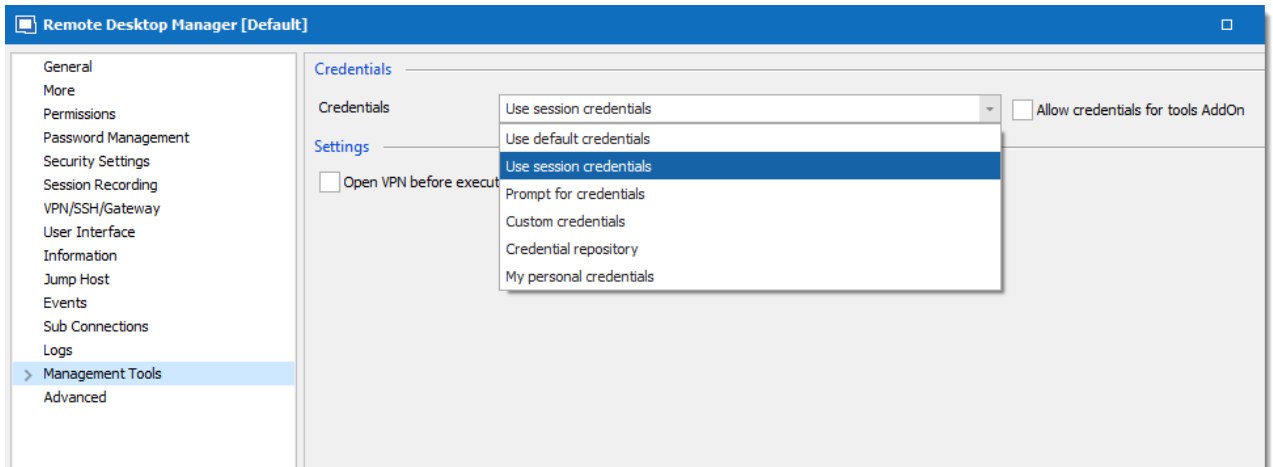
### 12.8.25 Session Tools

## COMPUTER MANAGEMENT GENERATES AN "ACCESS IS DENIED(5)" ERROR MESSAGE

When you attempt to use **Computer Management**, you receive the error below.



To get this working, you need to check this option in the **Tools** tab of the RDP session.



*RDP Session Properties*

If this doesn't solve your issue, it is likely that your session has **User Specific Settings** enabled. Please check your session for these settings.

This can be useful when you are using tools such as:

- **Hyper-V**
- **Event Viewer**
- **Computer Management**
- **Windows Services**

If this is often needed, we recommend you to change the [Default Settings](#) of the entry type. With this modification, all your new sessions will use the specified credentials when a tool is launched!

## 12.8.26 SSH

### REBEX.NET.SSHEXCEPTION: UNSUPPORTED PROTOCOL VERSION.

Only SSH v2 is supported. SSH v1 has inherent design flaws which make it vulnerable and it has been generally considered obsolete. Putty can be used for situations where SSH v1 is required.

### APPLICATION KEYPAD NOT WORKING CORRECTLY.

When trying to use the keypad in SSH, it does not send the correct characters when you type.

In the **Terminal** tab, please set the Disable application keypad mode to True so that the option works globally on all your sessions;

The screenshot shows the 'Advanced' tab of the SSH configuration window. The 'SSH Keypad mode' dropdown menu is highlighted with a green arrow pointing to it from the right. The other settings in the 'Advanced' tab are as follows:

Setting	Value
Override terminal type	
Encoding	Default
Auto wrap	Default
Local echo	Default
Initial keypad mode	Default
Disable application keypad mode	Default
Cursor type	Default
Cursor blink	Default
Reset scroll on display	Default
Force Non-destructive backspace	<input type="checkbox"/>
Implicit Carriage return in Linefeed	<input type="checkbox"/>
Implicit linefeed in carriage return	<input type="checkbox"/>
Max scrollbar lines	2000
Double-click delimiters	

SSH Keypad mode

## 12.8.27 Synchronizers

### 12.8.27.1 Active Directory Synchronizer

## GENERAL

### ENTRIES ARE CREATED WITH A \*CNF:{GUID} SUFFIX

This is a problem caused by Multimaster replication of directory objects. When there are name collisions, the system automatically renames one of the accounts by appending CNF to indicate conflict resolution and a GUID which is guaranteed to be unique.

There is a command to run to remove these objects, namely ***repadmin /removelingerobject***, please consult these references for the recipe to follow.

REF : <http://technet.microsoft.com/en-us/library/bb727059.aspx> and  
<https://social.technet.microsoft.com/Forums/windowsserver/en-US/e9327be6-922c-4b9f-8357-417c3ab6a1af/cnf-remove-from-ad?forum=winserverDS>

## DUPLICATE ENTRIES CREATED

### HOST NAME IS APPENDED WITH CNF, AND THE ENTRY NAME ALSO CONTAINS A GUID SUFFIX

Please refer to [Entries created with a CNF:{GUID} suffix](#) above.

#### 12.8.28 VMWare

## ERRORS



VMware tools make assumptions that their scripts are run in an interactive session and also present warnings the first time that they are run. As it stands today, you have to run commands interactively after you've installed or upgraded their tools.



The PowerCLI configuration has multiple scopes: **Session**, **User**, and **AllUsers**. Please refer to their documentation for details and on how to properly configure as per your requirements.

## CONNECTION TO THE SERVER FAILED!

This error message is displayed for various reasons. For a quick diagnostic, launch the VMware vSphere PowerCLI shortcut of the same bitness (32/64 bit) as your Remote Desktop Manager. Some commands will be listed in the table below to diagnose issues in sequence

STEP	COMMAND
Have you specified the Execution Policy of scripts?	Get-ExecutionPolicy
Have you configured the PowerCLI's InvalidCertificateAction?	Get-PowerCLIConfiguration
Have you configured the PowerCLI's DefaultVIMode?	Get-PowerCLIConfiguration

## IN THE POWERSHELL WINDOW : ERROR MESSAGE APPEAR BUT IT IS IMPOSSIBLE TO READ THEM BEFORE THE WINDOW CLOSES

Remote Desktop Manager ultimately sends a few commands in an encoded script, you can open a PowerShell window and type the following commands sequentially. This way you will have time to see the error messages.

The first command connects with the server, a password prompt will appear:

```
Connect-VIServer {server ip or name};
```

The second command lists the virtual machines present on the server. It displays the Name and the ID.

```
Get-View -ViewType VirtualMachine | select -Property Name, {$_.Moref.Value};
```

## IN THE POWERSHELL WINDOW : THERE WERE ONE OR MANY PROBLEM WITH THE SERVER CERTIFICATES

You also see a message related to **Set-PowerCLIConfiguration**. Please consult <https://www.vmware.com/support/developer/PowerCLI/PowerCLI51/html/Set-PowerCLIConfiguration.html> and make an informed decision as what is the best course of action when you take your security concerns into account. For users that are comfortable in

leaving the default certificate on the VMware server, you can launch a PowerShell command window and run the following:

```
set-PowerCLIConfiguration -invalidCertificateAction "ignore" -confirm:$false
```

## IN THE POWERSHELL WINDOW : THERE IS A QUESTION ABOUT MULTIPLE SERVER SUPPORT

As described in their message, it will be the default value in a coming release. Please consult their documentation and make an informed decision, but most users should accept the Multiple option.

## ISSUES WITH VMWARE POWERCLI

**THE TERM 'CONNECT-VISERVER' IS NOT RECOGNIZED AS THE NAME OF A CMDLET, FUNCTION, SCRIPT FILE, OR OPERABLE PROGRAM. CHECK THE SPELLING OF THE NAME, OR IF A PATH WAS INCLUDED, VERIFY THAT THE PATH IS CORRECT AND TRY AGAIN**

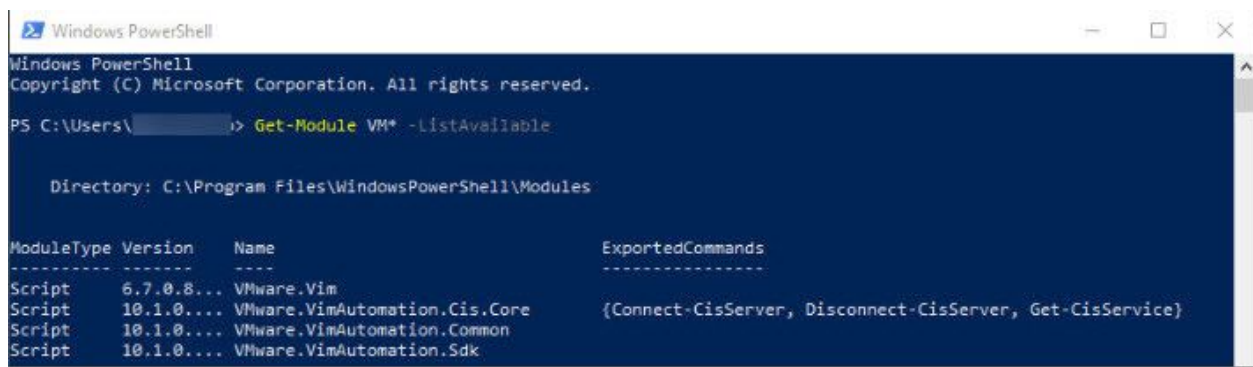
### CAUSE

This error occurs because the PowerCLI modules are not linked with PowerShell or the PowerCLI Module for the Connect-ViServer command is missing.

### SOLUTION

Check if VMware PowerCLI is installed.

Running '**Get-Module VM\* -ListAvailable**' in PowerShell shows the list of VMware modules installed.



```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\[user]> Get-Module VM* -ListAvailable

Directory: C:\Program Files\WindowsPowerShell\Modules

ModuleType Version      Name                                ExportedCommands
-----
Script      6.7.0.8... VMware.Vim                          {Connect-CisServer, Disconnect-CisServer, Get-CisService}
Script      10.1.0... VMware.VimAutomation.Cis.Core
Script      10.1.0... VMware.VimAutomation.Common
Script      10.1.0... VMware.VimAutomation.Sdk

```

VMware PowerCLI

You should see 4 VMware modules listed in PowerShell as shown in the image above.

You can test to see if PowerShell recognizes the '**Connect-ViServer**' command.



```

PS C:\Users\[user]> connect-viserver
connect-viserver : The term 'connect-viserver' is not recognized as the name of a cmdlet, function, script file, or
operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try
again.
At line:1 char:1
+ connect-viserver
~ ~~~~~
+ CategoryInfo          : ObjectNotFound: (connect-viserver:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

```

VMware PowerCLI

By typing the command, we see that PowerShell doesn't have the proper module installed.

In the PowerShell Window, install the PowerCLI modules by using the '**Install-Module**' command. Many step by step instructions can be found on Google.

Then type the '**Get-Module VM\* -ListAvailable**' command again, we can see that the PowerCLI modules are now listed.



```
PS C:\Users\> Get-Module VM* -ListAvailable

Directory: C:\Program Files\WindowsPowerShell\Modules

ModuleType Version      Name                                ExportedCommands
-----
Binary      6.5.1.5... VMware.DeployAutomation             {Add-DeployRule, Add-ProxyServer, Add-ScriptBundle, Copy-D...
Binary      6.5.1.5... VMware.ImageBuilder                 {Add-EsxSoftwareDepot, Add-EsxSoftwarePackage, Compare-Esx...
Manifest    6.5.2.6... VMware.PowerCLI                     {Add-ESXSoftwareDepot, Add-EsxSoftwarePackage, Compare-Esx...
Script      6.7.0.8... VMware.Vim                           {Connect-CisServer, Disconnect-CisServer, Get-CisService}
Script      10.1.0... VMware.VimAutomation.Cis.Core       {Connect-CisServer, Disconnect-CisServer, Get-CisService}
Binary      6.5.1.5... VMware.VimAutomation.Cloud          {Add-CIDatastore, Connect-CIServer, Disconnect-CIServer, G...
Script      10.1.0... VMware.VimAutomation.Common         {Connect-CisServer, Disconnect-CisServer, Get-CisService}
Binary      6.5.2.6... VMware.VimAutomation.Core           {Add-PassthroughDevice, Add-VirtualSwitchPhysicalNetworkAd...
Binary      6.0.0.5... VMware.VimAutomation.HA             Get-DrmInfo
Binary      7.1.0.5... VMware.VimAutomation.HorizonView    {Connect-HVServer, Disconnect-HVServer}
Binary      6.5.1.5... VMware.VimAutomation.License        Get-LicenseDataManager
Binary      6.5.1.5... VMware.VimAutomation.PCloud         {Connect-PIServer, Disconnect-PIServer, Get-PIComputeInsta...
Script      10.1.0... VMware.VimAutomation.Sdk            {Connect-PIServer, Disconnect-PIServer, Get-PIComputeInsta...
Binary      6.5.1.5... VMware.VimAutomation.Srm            {Connect-SrmServer, Disconnect-SrmServer}
Binary      6.5.1.5... VMware.VimAutomation.Storage        {Copy-VDisk, Export-SpbmStoragePolicy, Get-NfsUser, Get-Sp...
Script      1.0      VMware.VimAutomation.StorageUtility Update-VmfsDatastore
Binary      6.5.1.5... VMware.VimAutomation.Vds            {Add-VDSwitchPhysicalNetworkAdapter, Add-VDSwitchVMHost, E...
Binary      6.5.1.5... VMware.VimAutomation.vROps          {Connect-OMServer, Disconnect-OMServer, Get-OMAlert, Get-O...
Binary      6.5.1.5... VMware.VumAutomation               {Add-EntityBaseline, Copy-Patch, Get-Baseline, Get-Complia...
```

VMware PowerCLI

A Final test with the '**Connect-ViServer**' command, by typing it in PowerShell, the connection is established and the issue should be resolved.

```
PS C:\Users\> connect-viserver

cmdlet Connect-ViServer at command pipeline position 1
Supply values for the following parameters:
Server[0]:
PS C:\Users\>
```

VMware PowerCLI

## ADDITIONAL TROUBLESHOOTING

If try on a new computer and have an issue with VimAutomation.Core, you can install it with the command:

```
Install-Module -Name VMware.VimAutomation.Core -AllowClobber -Scope CurrentUser
```

After the installation, if you run the command:

```
Get-Module VM* -ListAvailable
```

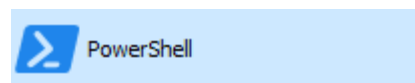
You should get the output below:

ModuleType	Version	Name	ExportedCommands
Script	6.7.0.1...	VMware.DeployAutomation	{Add-DeployRule, Add-ProxyServer, Add-ScriptBundle, Copy-D...
Script	6.7.0.1...	VMware.ImageBuilder	{Add-EsxSoftwareDepot, Add-EsxSoftwarePackage, Compare-Esx...
Manifest	11.1.0...	VMware.PowerCLI	
Script	6.7.0.1...	VMware.Vim	
Script	11.0.0...	VMware.VimAutomation.Cis.Core	{Connect-CisServer, Disconnect-CisServer, Get-CisService}
Script	11.0.0...	VMware.VimAutomation.Cloud	{Add-CIDatastore, Connect-CIServer, Disconnect-CIServer, G...
Script	11.0.0...	VMware.VimAutomation.Common	
Script	11.0.0...	VMware.VimAutomation.Core	{Add-PassthroughDevice, Add-VirtualSwitchPhysicalNetworkAd...
Script	7.6.0.1...	VMware.VimAutomation.HorizonView	{Connect-HVServer, Disconnect-HVServer}
Script	10.0.0...	VMware.VimAutomation.License	Get-LicenseDataManager
Script	11.0.0...	VMware.VimAutomation.Nsxt	{Connect-NsxtServer, Disconnect-NsxtServer, Get-NsxtService}
Script	11.0.0...	VMware.VimAutomation.Sdk	
Script	11.0.0...	VMware.VimAutomation.Security	{Get-SecurityInfo, Get-VTpm, Get-VTpmCertificate, Get-VTpm...
Script	11.1.0...	VMware.VimAutomation.Srm	{Connect-SrmServer, Disconnect-SrmServer}
Script	11.1.0...	VMware.VimAutomation.Storage	{Add-KeyManagementServer, Copy-VDisk, Export-SpbmStoragePo...
Script	1.3.0.0...	VMware.VimAutomation.StorageUtility	Update-VmfsDatastore
Script	11.0.0...	VMware.VimAutomation.Vds	{Add-VDSwitchPhysicalNetworkAdapter, Add-VDSwitchVMHost, E...
Script	11.0.0...	VMware.VimAutomation.Vmc	{Connect-Vmc, Disconnect-Vmc, Get-VmcSddcNetworkService, G...
Script	10.0.0...	VMware.VimAutomation.vROps	{Connect-OMServer, Disconnect-OMServer, Get-OMAlert, Get-O...
Script	6.5.1.7...	VMware.VumAutomation	{Add-EntityBaseline, Copy-Patch, Get-Baseline, Get-Complia...

PS C:\Windows\system32>

### VMware PowerCLI

If you restart RDM with the current user (not running as admin) and open the VMware Dashboard entry, after 30 seconds, you should see all your servers.



If this does not work, create a PowerShell entry, the blue one, select **Embedded Script** and type the script below:

```
Import-Module VMware.PowerCLI;
Connect-ViServer "SERVER_IP";
Get-View -ViewType VirtualMachine | select -Property Name, {$_.Moref.Value};
```

Click **OK** twice and try to start the Powershell entry.

If you get an error about execution policies, please refer to [https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about\\_execution\\_policies?view=powershell-5.1](https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_execution_policies?view=powershell-5.1)

But you can resolve the issue with the following command:

```
Set-ExecutionPolicy Unrestricted -Scope CurrentUser
```

Please refer to your administrator to ensure this command is allowed to be used within your infrastructure.

#### 12.8.28.1 Advanced Troubleshooting of the PowerCLI

## DESCRIPTION

Remote Desktop Manager calls PowerCLI's cmdlets and presents the results in its user interface. Here are steps to help isolate issues when the integration is not working as expected.

## SCRIPT A GET THE LIST OF VIRTUAL MACHINES

### GETVMS.PS1

```
Param(
    [Parameter(Mandatory=$true)]
    [string]$viServer,
    [Parameter(Mandatory=$true)]
    [string]$userName,
    [Parameter(Mandatory=$true)]
    [string]$password
) #end param

$VMHost = Connect-VIServer $($viServer) -User $userName -Password $password
if ($VMHost -eq $null ) { throw "Connection to server failed!";}
try
{
    Get-View -ViewType VirtualMachine | select -Property Name, {$_.Moref.Value};
}
catch
{
    write-host $ErrorMessage
}
Disconnect-VIServer $VMHost -Force -Confirm:$false
```

### EXAMPLE USE

```
.\GetVms.ps1 [SERVER_NAME] [USER_NAME] [PASSWORD]
```

Name	\$_Moref.Value
----	-----
MACHINE1	18
MACHINE2	19

## SCRIPT B - :LAUNCHING THE VMRC

### CONNECTVMRCFROMPOWERCLI.PS1

```

Param(
    [Parameter(Mandatory=$true)]
    [string]$viServer,
    [Parameter(Mandatory=$true)]
    [string]$userName,
    [Parameter(Mandatory=$true)]
    [string]$password,
    [Parameter(Mandatory=$true)]
    [string]$morefId = ""
) #end param

$VMHost = Connect-VIServer $($viServer) -User $userName -Password $password

if ($VMHost -eq $null) { throw "Connection to server failed!";}
$si = Get-View ServiceInstance
$sm = Get-View $si.Content.SessionManager
$ticket = $sm.AcquireCloneTicket()
try
{
    Start-Process -FilePath "C:\Program Files (x86)\VMware\VMware Remote Console\vmr
}
catch
{
    write-host $ErrorMessage
}
#must wait to allow for the process to be started BEFORE we disconnect from the serv
Start-Sleep -s 10
Disconnect-VIServer $VMHost -Force -Confirm:$false

```

## EXAMPLE USE

You must send the **MoRef.Value** which was obtained using Script A, in our example, let's start MACHINE2 which has 19 for ID.

```
.\ConnectVMRCFromPowerCLI.ps1 [SERVER_NAME] [USER_NAME] [PASSWORD] 19
```

The VMRC should appear and allow you to interact with it.

### 12.8.29 VPN

#### 12.8.29.1 Missing Opened VPN from List

## MISSING OPENED VPN FROM LIST:

The opened VPN is not listed in Remote Desktop Manager. Unfortunately, there is no way for us to detect an already opened VPN session.

#### 12.8.29.2 FortiClient

## DESCRIPTION



Fortinet removed the feature to inject credentials in FortiClient 5.4 and above. However, they still left the feature with FortiSSL

Company terminology:

- Fortinet is the name of the company
- Fortigate is the router of Fortinet
- Forticlient and FortiSSL are VPN of Fortinet

## SOLUTION

The CLI for FortiSSL is not included anymore with the download of FortiClient. You need to download the tools related to the current version of FortiClient [here](#).



You need to have a support plan with Fortinet to download the tools. If you don't have a support plan, try to contact Fortinet directly and ask them to send you the file.

The file FortiSSLVPNClient.exe needs to be saved in the installation folder of FortiClient.

### 12.8.29.3 Sonicwall Global VPN Client

## ERRORS

### THE CONNECTION IS NOT ESTABLISHED

Remote Desktop Manager simply calls the command line interface (CLI) with supported parameters. At this time (v4.9), the executable can be found in:

```
C:\Program Files\Dell SonicWALL\Global VPN Client\SWGVC.exe
```

Simply call it as follows:

```
SWGVC.exe /E connection_name /U username /P password
```

The CLI must be able to connect, Remote Desktop Manager doesn't perform anything additional to make it work.

#### 12.8.29.4 Microsoft VPN

## DESCRIPTION



These types of VPNs can use either the RASDIAL or RASPHONE applications for establishing the connection. Please consult Microsoft's article on their differences and usage.



You can refer to this Microsoft TechNet article for more information on RASDIAL: <https://technet.microsoft.com/en-us/library/bb490979.aspx>.

For specific errors, consult the ISSUES section below.

## GENERAL

Sometimes you need to accept a message or make a choice upon first use, but that typically occurs only the first time. Sadly this makes running the command manually once mandatory on all machines.

If you have elected to store the PBK in Remote Desktop Manager, we simply extract it to %**TMP%\RDM** upon usage. After trying to establish a connection once, you should see your phonebook in that folder, is it present?

By default, it uses RASDIAL, what happens if you run the following at the command prompt?

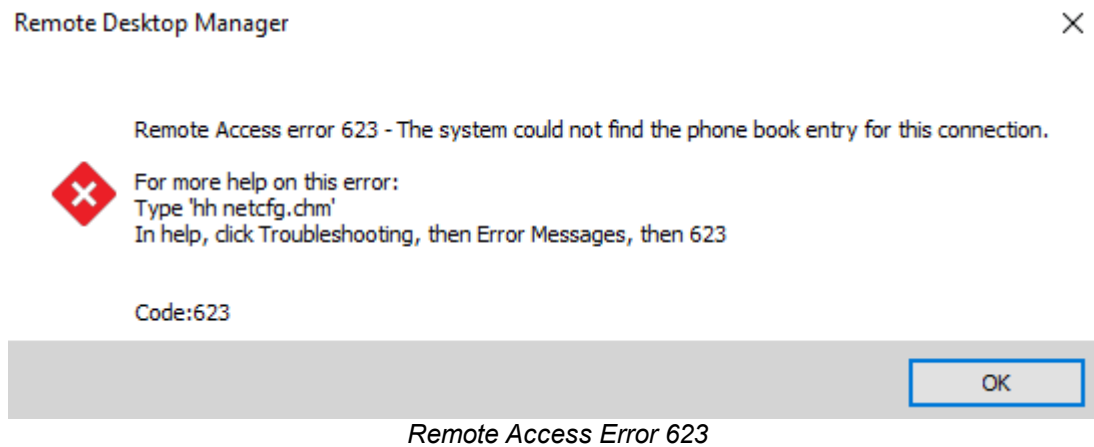
```
rasdial <connectionname> <username> <password> /phonebook:<phonebookpath>
```

or if the **Use rasphone (ConnectionManager Administrator Kit)** option is checked, it will use RASPHONE. What happens if you run the following at the command prompt?

```
rasphone -d <connectionname> -f <phonebookpath>
```

## ISSUES

## REMOTE ACCESS ERROR 623



Ensure that within the phonebook, the vpn definition name does contain a space character.

## PASSWORD WITH QUOTATION MARKS

Quotation mark (") is not a valid character and should not be used in the password of a Microsoft VPN entry.

### 12.8.29.5 Cisco AnyConnect

## DESCRIPTION

The Cisco AnyConnect add-on doesn't send the proper information like the password or the group number to the **vpncli.exe** DOS window to establish the VPN connection.

For example, only the half of the password is sent to the Cisco AnyConnect window.

## SOLUTION

The Cisco AnyConnect add-on use sendkeys to send information to the **vpncli.exe** window. The issue that we encounter is caused by the Windows UAC feature. Enabling/Disabling UAC on your computer should resolved the issue.

On your computer, go in **Control Panel – User Account – User Account Control Settings**:

- Select **Never Notify** to turn off the option.
- Select **Notify me or Always notify** to turn on the option.

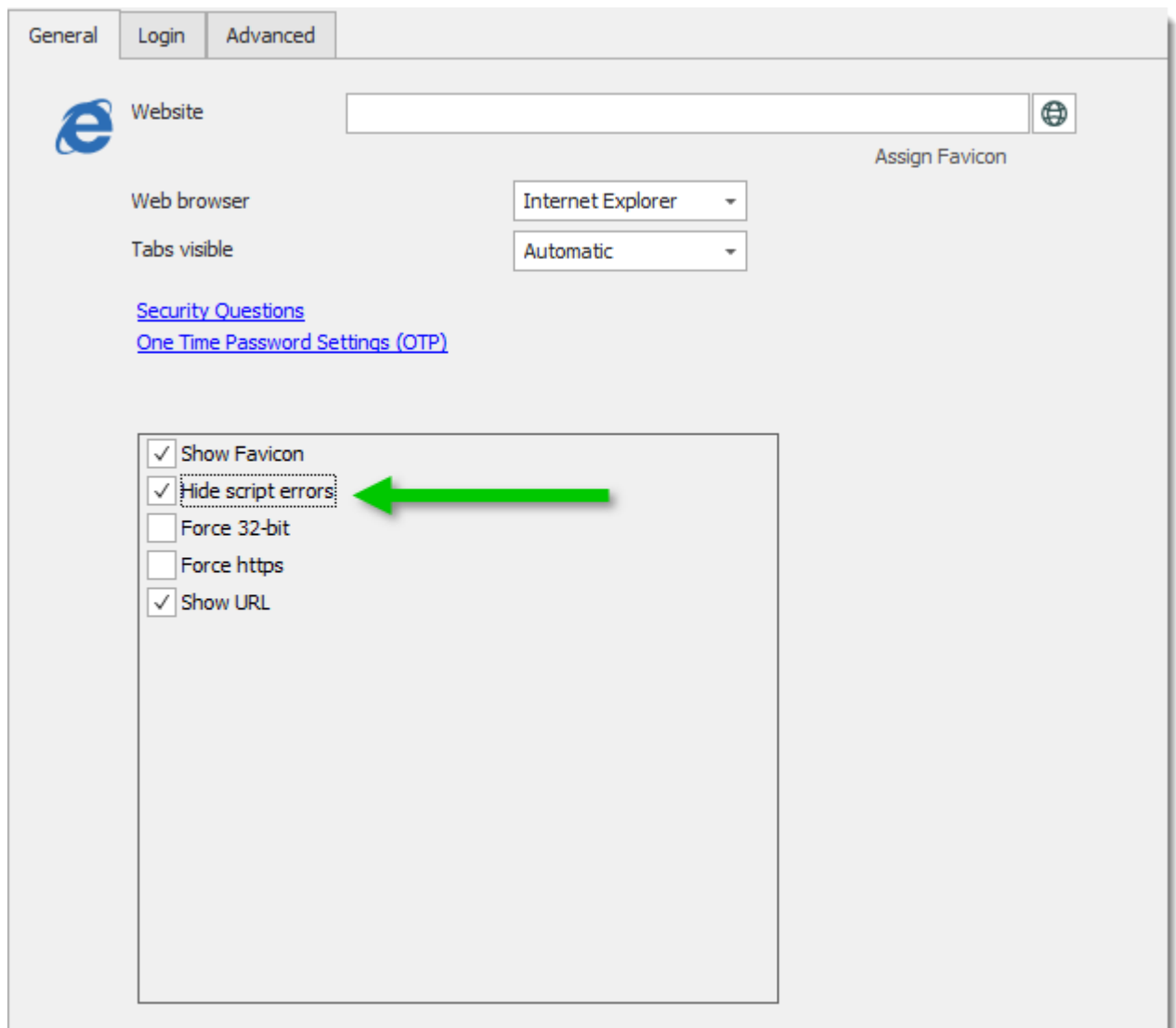
## 12.8.30 Web Browsers

### 12.8.30.1 Internet Explorer

## SCRIPT ERROR WITH IE EMBEDDED

### AN ERROR HAS OCCURRED IN THE SCRIPT ON THIS PAGE

When you launch a **Web Browser (http/https)** in Internet Explorer directly (**external mode**), the script errors are handled by the browser, so they are not displayed. In embedded mode, you need to enable the **Hide script error** in the properties of your session.



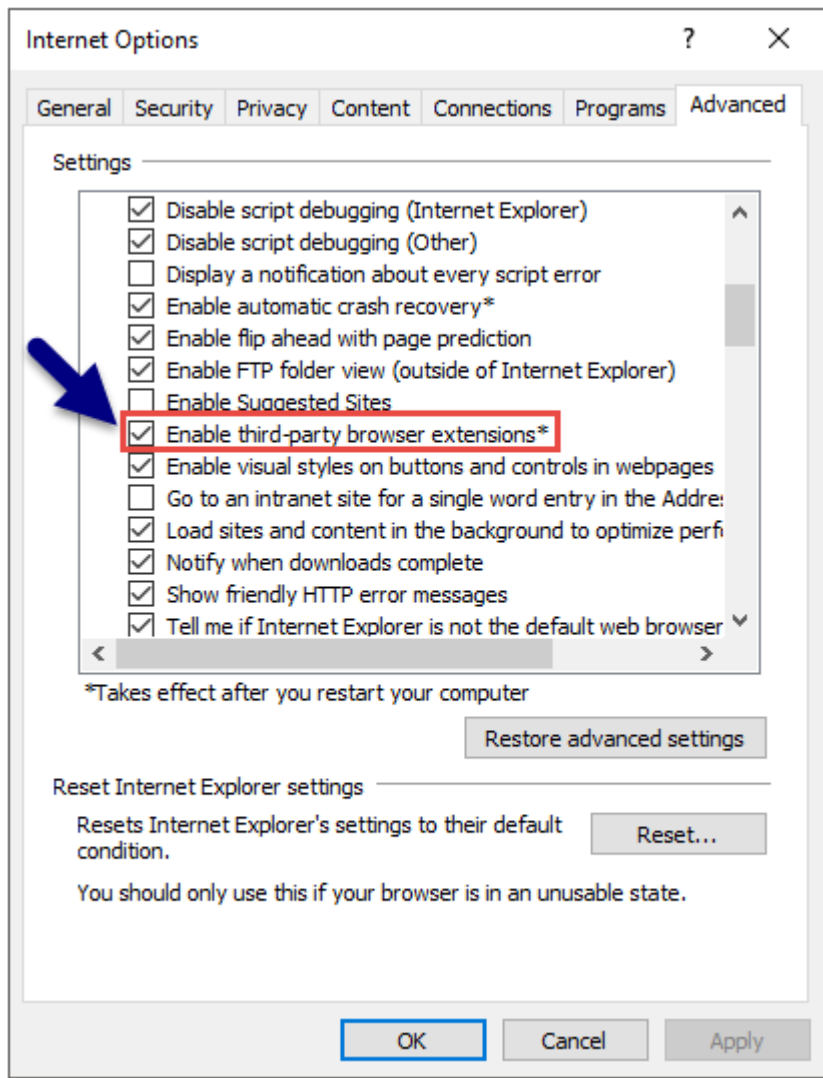
IE Embedded



## BROWSER EXTENSION DOESN'T APPEAR IN THE TOOLBAR BUT IT IS INSTALLED

This issue occurs when a specific option is unchecked for IE in **Tools -> Internet Options -> Advanced**

The option is called **Enable third-party browser extensions**. After enabling this option, IE must be restarted.



IE Advanced Options

## RENDERING

### EMBEDDED HTML CONTENT IS NOT RENDERED WITH THE LATEST INTERNET EXPLORER VERSION

By default Remote Desktop Manager does not use the latest IE version (emulation mode). This can be changed in **File – Options – Type – Web, IE Mode**.

### ACCESSVIOLATIONEXCEPTION - ATTEMPTED TO READ OR WRITE PROTECTED MEMORY

When a crash occurs in Remote Desktop Manager while using some ActiveX in IE, it's often caused by Data Execution Prevention (DEP). DEP is a security feature included in Windows. It is used to prevent an application or service from executing code from a non-executable memory region.

To fix this, simply change the DEP settings for the application as follows:

1. Right Click **My Computer – Properties**.
2. Choose **Advanced System Settings**.
3. Click the **Advanced** Tab.
4. Click **Settings** under **Performance**.
5. Select the tab **Data Execution Prevention**.
6. Add **RDM** to the list.

### LAUNCHED EXTERNAL WINDOWS (SUCH AS IE) POPUP IN THE BACKGROUND

You may have noticed that when you launch items such as IE windows from within RDM, they pop-up in the background.

The **ForegroundLockTimeout** registry value for the User's Profile has to be modified from the default of 200000 down to 0:

```
[HKEY_CURRENT_USER\Control Panel\Desktop]
"ForegroundLockTimeout"=dword:00000000
```

Please note that some programs that have an extensive library of add-ons (Like MS Word) may take the focus every time the add-on performs an action. You have to observe the reaction of your most used programs and judge what is the setup that works best for you.

#### 12.8.30.2 Google Chrome

## ISSUES

### ADOBE FLASH PLAYER NEEDS YOUR PERMISSION TO RUN

You need to install Adobe Flash Player with PPAPI.

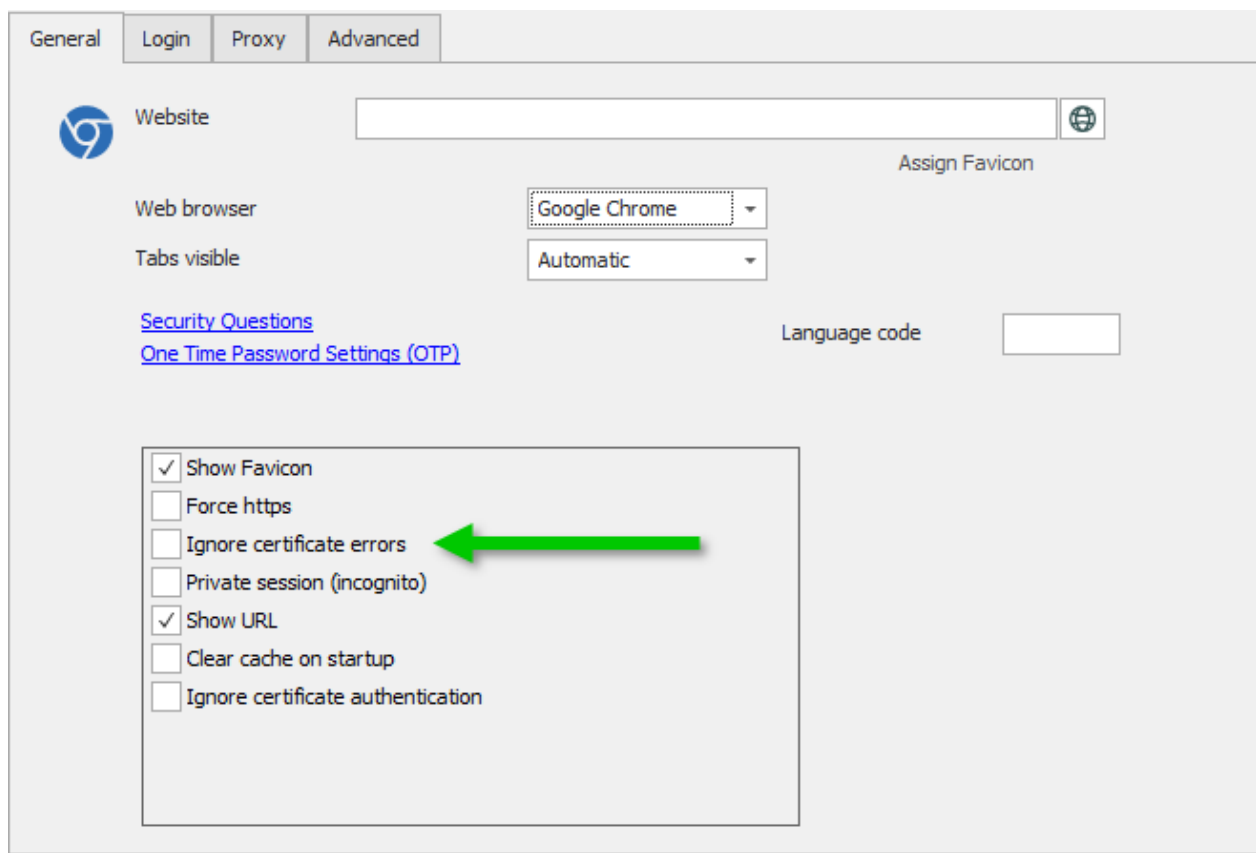
To do so, please follow the steps below:

- 1- Visit <https://get.adobe.com/flashplayer/> with **Google Chrome browser**;
- 2- Download **Adobe Flash Player**.
- 3- Launch the installer from your download folder.
- 4- After the installation, close and restart Remote Desktop Manager.
- 5- Create an embedded Chrome web session and use the following link <https://get.adobe.com/flashplayer/about/> to verify that it works.

### CERTIFICATE ERRORS IN EMBEDDED MODE

Remote Desktop Manager starts Google Chrome in a separate application (Embedded32.exe) and then re-parents the application inside Remote Desktop Manager.

To resolve this issue, you need to check the option **Ignore certificate errors** in the properties of the **Web Browser (http/https)** session.



*Google Chrome Session Properties*

### 12.8.30.3 Firefox

## ISSUES

### FIREFOX IN EMBEDDED MODE DOESN'T WORK IN THE APPLICATION

Remote Desktop Manager starts Firefox in a separate application (Embedded32.exe) and then re-parents the application inside Remote Desktop Manager.

Firefox does not work when the Team Viewer QuickConnect button  is present in the title bar.

To resolve this issue, you need to disable the QuickConnect button in Team Viewer by unchecking the option in **Extra – Options – Advanced – Show advanced options – QuickConnect button – Configure – Show QuickConnect button**.

#### 12.8.30.4 Web Authentication

## DESCRIPTION

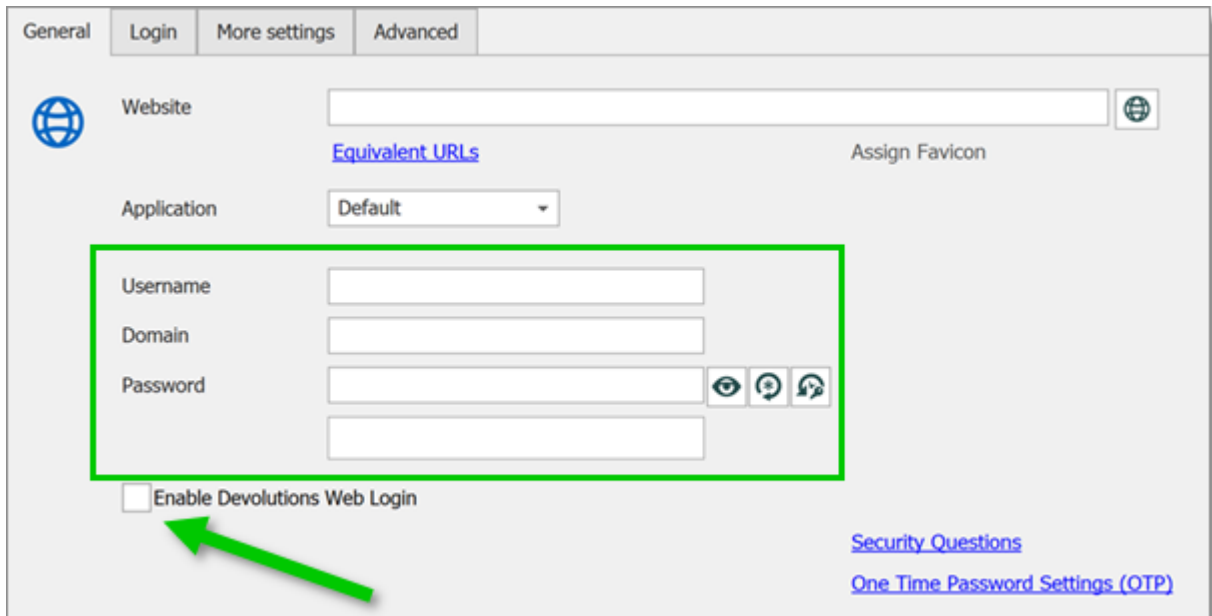
For some websites, the auto fill function does not work automatically. It is important to note that some website will prevent you from autofilling your credentials.

It requires some steps in order to properly send the username and password. Depending on the website, the process can be automatic or may require additional steps.

## METHOD 1

### AUTOMATICALLY LOG INTO A WEBSITE

1. In the **General** tab of the Web Browser entry, enter the credentials. This is also here that you can activate the Devolutions Web Login extension.



The screenshot shows the 'General' tab of the Web Browser settings. The 'Website' field is empty, and the 'Application' dropdown is set to 'Default'. The 'Username', 'Domain', and 'Password' fields are highlighted with a green box. Below these fields, there is a checkbox labeled 'Enable Devolutions Web Login' which is currently unchecked. A green arrow points to this checkbox. To the right of the password field, there are three icons: an eye, a key, and a lock. At the bottom right, there are links for 'Security Questions' and 'One Time Password Settings (OTP)'.

Web Browser - General

2. In the **Login - Settings** tab, set the **Authentication** to **Form**. Then, verify that the **Autofill login** and **Auto submit** options are enabled.

The screenshot shows the 'Web Browser - Login - Settings' dialog box. It has four tabs: 'General', 'Login', 'More settings', and 'Advanced'. The 'Login' tab is active. Under the 'Authentication' section, a dropdown menu is set to 'Form'. Below this, there are three sub-tabs: 'Settings', 'Html Control ID', and 'Custom'. The 'Settings' sub-tab is active. It contains three checkboxes: 'Autofill login' (checked), 'Autofill delay' (unchecked), and 'Auto submit' (checked). To the right of the 'Autofill delay' checkbox is a numeric input field set to '100' and a unit selector set to 'ms'.

Web Browser - Login - Settings

OPTION	DESCRIPTION
<b>Username</b>	Enter the username to connect on the website.
<b>Domain</b>	Enter the domain to connect on the website.
<b>Password</b>	Enter the password to connect on the website.
<b>Autofill login</b>	Automatically fills in the credential fields when opening the web page.
<b>Autofill delay</b>	Set a delay between opening the web page and attempting the auto fill feature.
<b>Auto submit</b>	Automatically submit the credentials and try connecting to the website.

3. In the **Html Control ID** tab, click the **Discover** button to define the appropriate fields.

The **Discover** command searches the web page to find the fields that correspond to those in the entry. This allows the application to find the appropriate fields to fill when connecting to the website.

General Login More settings Advanced

Authentication Form

Settings Html Control ID Custom

Profile Default

Form ID

Username ID

Domain ID

Password ID

One time password ID

Login button ID

Automatic

Discover

*Login - Html Control ID - Discover*

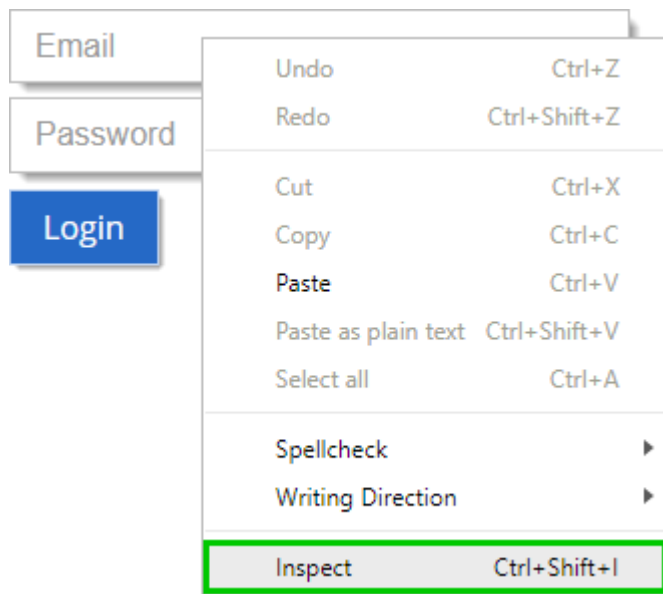
Once all the necessary steps have been completed, upon launching the session, the credentials will automatically be entered and logged into the site.

## METHOD 2

The second method requires to manually identify the IDs corresponding to the logon fields on the login web page.

For this example, we will be using Google Chrome to inspect the logon fields.

For both the Username & Password fields, you will be required to do a right-click inside each field and click on ***Inspect***;



*Login fields – Inspect*

You will see the corresponding IDs to be used in the HTML Control ID tab of the Web session in Remote Desktop Manager;

Below is an example of the inspection for the **Username** field. From it you can see that the Username ID is username.



```


<div style="position: absolute; top: 65px; left: 65px;">...</div>
<form name="loginForm" ng-submit="login(credentials)" novalidate class="ng-pristine ng-valid">
  <div id="loginForm">
    <p class="loginRow ng-hide" ng-show="devmode || electron">...</p>
    <p class="loginRow">
      <label id="username-label" class="loginLabel">
        "User name
        "
        <input id="username" aria-labelledby="username-label" tabindex="2" focus-me="true" ng-disabled="loggingIn" ng-class="{loginFailed: loginFailed}" class="margeTextInput ng-pristine ng-valid ng-touched" type="text" ng-model="credentials.username"> == $0
      </label>
    </p>
    <p class="loginRow">...</p>
    <p>&nbsp;</p>
    <p id="loginButtonRow">...</p>
  </div>
  <div id="productName">...</div>
</form>
<div id="footer" class="footer">...</div>
</div>
</div>

```

... p > #username-label > input#username.margeTextInput.ng-pristine.ng-valid.ng-touched

*Logon Fields Inspect*

### 12.8.31 WebDav

## ERRORS

### UNABLE TO CONNECT TO WEBDAV

Make sure that the appropriate domain is configured in the **Host** field (ex: domain.com) and that you have **"/remote.php/dav/files/USERNAME/"** in **Start location**.

If you have a HTTPS website, check the **Use SSL** checkbox and configure the port to be 443.



You can always refer you to the [ownCloud](#) documentation for more details on WebDav.

## 12.8.32 Web traffic

### DESCRIPTION



Do not use this without a specific request from Devolution's support personnel.



The trace file must NOT have a path specified, this requires that RDM be installed in a folder other than Program Files. (Running with elevated privileges doesn't circumvent the UAC.)

### PROCEDURE

```
<system.diagnostics>
  <trace autoflush="true" />
  <sources>
    <source name="System.Net" tracemode="protocolonly" maxdatasize="1024">
      <listeners>
        <add name="MyTraceFile"/>
      </listeners>
    </source>
  </sources>

  <sharedListeners>
    <add
      name="MyTraceFile"
      type="System.Diagnostics.TextWriterTraceListener"
      initializeData="System.Net.trace.log"
    />
  </sharedListeners>

  <switches>
    <add name="System.Net" value="Verbose" />
  </switches>
</system.diagnostics>
```

### ADVANCED MODE

To use with **SvcTraceViewer.exe**

```
<sharedListeners>
```

```
<add
  name="MyTraceFile"
  type="System.Diagnostics.XmlWriterTraceListener"
  initializeData="System.Net.trace.svclog"
/>
</sharedListeners>
```

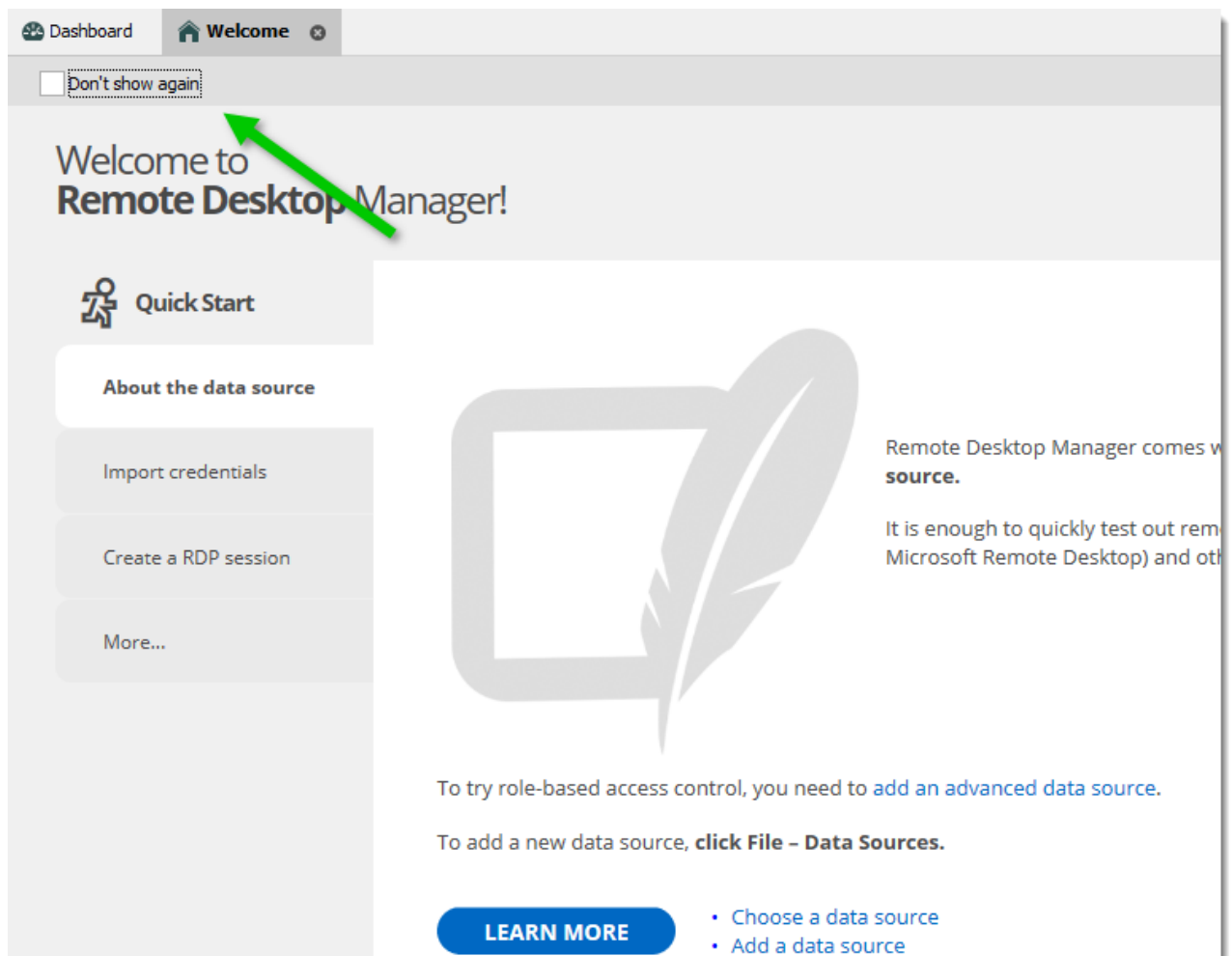
### 12.8.33 Welcome Page

## DESCRIPTION

We added a new **Getting Started** page at the opening of Remote Desktop Manager but you don't want to see it every time you open our application.

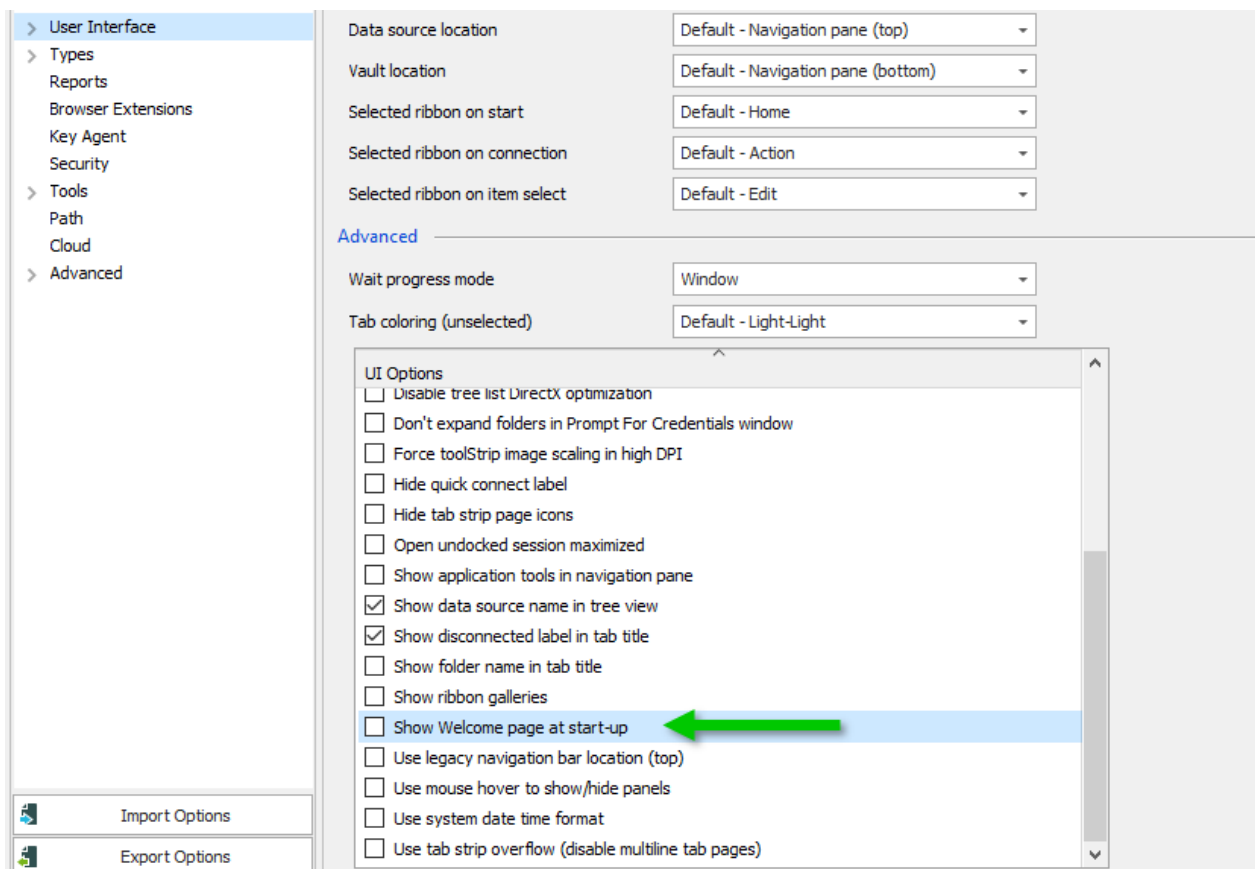
There are 2 ways of removing that page:

1. If you haven't closed it yet, simply click on **Don't show again** in the upper left corner.



*Hide Welcome Page*

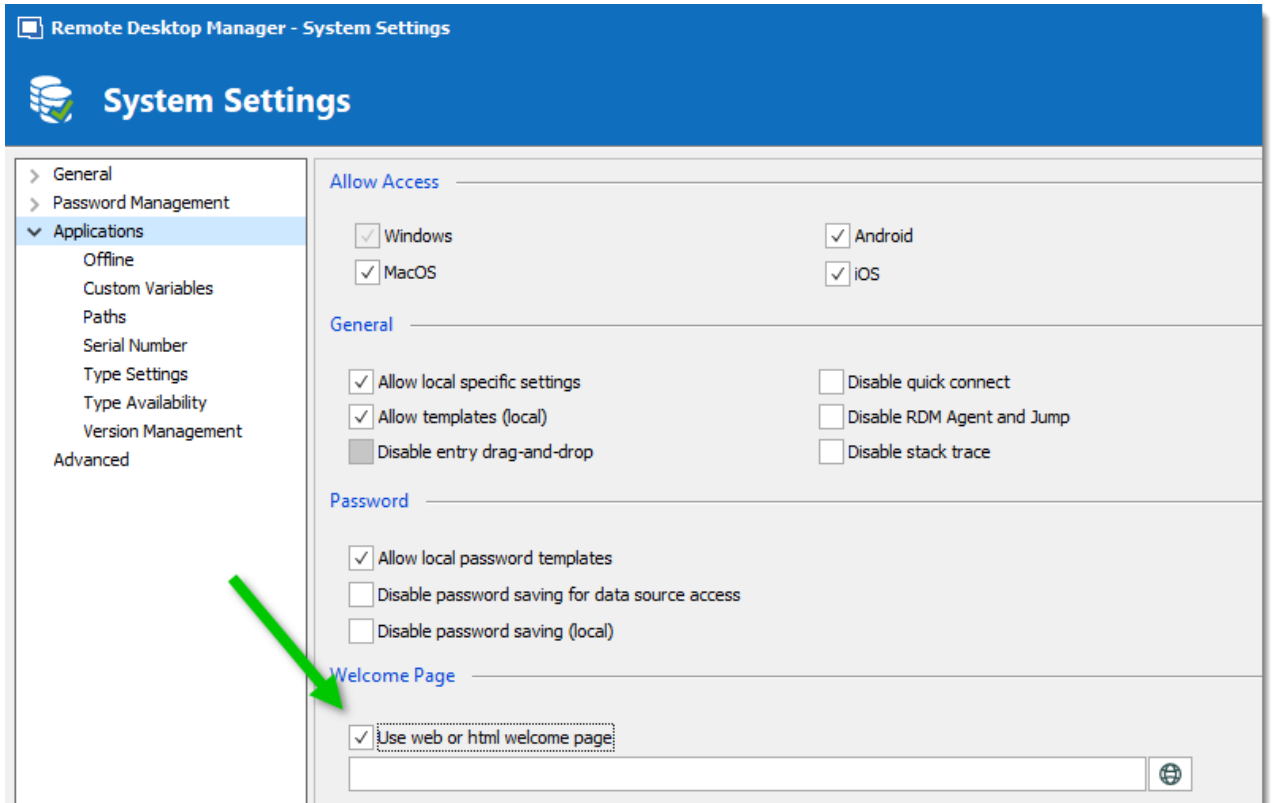
2. Go in **File -> Options -> User Interface** and uncheck **Show Welcome page at start-up**.



*Hide Welcome Page*

## CUSTOM WELCOME PAGE

It is possible to display your own welcome page at startup. Under **Administration** in the ribbon, choose **Data Source Settings (System Settings)**. Then, in **Applications**, under the **Welcome Page** section, enter the URL that points to your custom welcome page.



Welcome Page URL

## 12.8.34 WMI

### DESCRIPTION

Here's a primer on remote WMI:

<https://msdn.microsoft.com/en-us/library/aa389290.aspx>

In our environment, we basically run winrm quickconfig on all our machines, for those not joined to a domain we also add them to the TrustedHosts list. For machines not joined to a domain, there's an added difficulty if you are using the IP address instead of the **Host** name, it definitely offers a few challenges.

A good strategy is to get remoteWMI to work, then we integrate it in RDM. We like to use WMIC.

[https://msdn.microsoft.com/en-us/library/aa394531\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/aa394531(v=vs.85).aspx)

This is a lot of information to go over, please contact us at [ticket@devolutions.net](mailto:ticket@devolutions.net) if you hit a hurdle.

## ACCESS DENIED ERRORS

Ensure the user account has the necessary permissions to access a computer remotely [Securing a Remote WMI Connection \(Windows\)](#).

You can also find troubleshoot tips in [WMI Troubleshooting \(Windows\)](#).

## ERROR GETTING PRODUCTS INFORMATIONS

Invalid Class WMI or WMI class not found on Windows Server 2003. On Windows Server 2003, Win32\_Product is not enabled by default. You can enable it by following the steps provided in the link below:

<https://social.msdn.microsoft.com/Forums/vstudio/en-US/6fb0d3ea-1ccf-4554-bdf1-79c9e24388af/invalid-class-wmi-windows-2003-server>

## TESTING FROM A REMOTE COMPUTER

The WMIC command is used to test if you have access to the machine through WMI. You need to enter the following command below;

```
wmic /NODE:"ComputerName" bios get serialnumber
```

Below, an example with other credentials;

```
wmic /NODE:"ComputerName" /user:"username" /password:"password" bios get serialnumber
```

## 12.9 Tutorials

### DESCRIPTION

Our tutorials are published on [Devolutions YouTube channel](#). We have three main categories of tutorials:

- [Overview](#): Brief presentation of a product.
- [Getting Started](#): Procedure to get up and running in a quick fashion.
- [Spotlight On...](#): Detailed presentation of a specific aspect of our products.







Obviously some tutorials will not fit in one of these categories, but 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.

## 12.9.1 Overview

### DESCRIPTION

Overview videos present a brief presentation of a product, there is no step-by-step but only explanation of a certain part of our product.





OVERVIEW	DESCRIPTION	LINK
<b>Register your Remote Desktop Manager license</b>	<p>A quick look at how to register your license in Remote Desktop Manager.</p> <p>The data sources are the heart of Remote Desktop Manager. Here is a quick overview of the most popular data sources that we support.</p>	 Watch Video
<b>Register Remote Desktop Manager</b>	A quick look at how to download Remote Desktop Manager and register your license key.	 Watch Video
<b>Remote Desktop Manager</b>	A quick overview of Remote Desktop Manager. See how you can easily and securely centralize and consolidate all your remote connections, credentials and passwords.	 Watch Video
<b>Create Templates and Default Settings</b>	A quick overview at how to execute and export multiple reports with the option of exporting reports through a command line.	 Watch Video
<b>Create Users and Assign Permission</b>	Take a quick look at how to create users for your data base and how to assign specific permission to each user.	 Watch Video
<b>Create a folder structure that reflects your</b>	An overview at how to create a folder structure that will reflect your organizations.	 Watch Video

OVERVIEW	DESCRIPTION	LINK
<b>organization</b>		
<b>Simplified Security</b>	Learn how to create roles and permissions for a granular protection system using our Role Based Security System.	 Watch Video
<b>Choose your data source</b>	An overview at our multiple data sources and how to select the proper one for you and your enterprise.	 Watch Video








## 12.9.2 Getting Started

### DESCRIPTION

Getting Started videos present a step-by-step sequence to start using a product. They differ from our "Spotlight On..." series in that they are targeted on significant feature of the product, rather than on a piece of a whole.

GETTING STARTED	DESCRIPTION	LINK
<b>KeePass</b>	Learn how to perform the setup for the integration of KeePass with Remote Desktop Manager	 Watch Video
<b>LastPass</b>	Learn how to use your own LastPass account to manage passwords in Remote Desktop Manager.	 Watch Video
<b>Remote Desktop Manager Jump</b>	Learn how to perform the initial setup for allowing usage of Remote Desktop Manager Jump to connect to remote devices through a jump host.	 Watch Video
<b>Simplified Security</b>	Learn how to create roles and permissions for a granular protection system using our Role Based Security System.	 Watch Video



GETTING STARTED	DESCRIPTION	LINK
<b>Remote Desktop Manager Step 1: Register your Data Source</b>	Upon first launch learn how to create your first data source and your first database.	 Watch Video
<b>Remote Desktop Manager Step 2 Options for Team Environment</b>	Learn how to set up your options to make your environment more fitting for teams.	 Watch Video
<b>Remote Desktop Manager Step 3: Default Settings</b>	Taking a quick look at our options and what are the best default settings for your team environment before creating your entries.	 Watch Video
<b>Remote Desktop Manager Step 4: Getting Set Up</b>	Learn how to create a folder structure that reflects your organization using Remote Desktop Manager best practices.	 Watch Video
<b>Remote Desktop Manager Step 5: How to create your entries</b>	Learn how to create and manage your entries and also taking a quick look at Security Group Management.	 Watch Video
<b>Devolutions Password Server</b>	Learn how to create and set up your Devolutions Password Server.	 Watch Video
<b>Devolutions Online Database</b>	Learn how to can create your Devolutions Account and get started setting up your Online Database.	 Watch Video







### 12.9.3 Spotlight On...

## DESCRIPTION

This video category is destined to contain a number of short tutorials that provide information on more specific aspects or features of Remote Desktop Manager.

Ultimately, all longer videos will be replaced by a series of **Spotlight on...** tutorials.

Our [Getting Started](#) topic contains a sequence of steps to follow to go through the initial setup under various conditions. Please refer to it for the best sequence for your environment.

SPOTLIGHT ON...	DESCRIPTION	LINK
<b>Batch Edit</b>	Change the settings of multiple sessions in one operation. For example, it can be used to remove or update all of the credentials of a group of sessions.	 Watch Video
<b>Host and Templates</b>	A host is used to define and configure a generic host session that could be used as the parent for others. You can define a subset of templates to apply at the execution.	 Watch Video
<b>Offline Mode</b>	The offline mode allows you to connect to a read/write copy of the data source when the live database is unavailable. It can be used when a user is working from a disconnected network or when there is any kind of connectivity issue to the data source.	 Watch Video
<b>Simplified Security</b>	Learn how to create roles and permissions for a granular protection system using our Role Based Security System.	 Watch Video
<b>User Interface</b>	Learn how to manipulate the user interface elements of Remote Desktop Manager and adapt it according to your preferences.	 Watch Video
<b>Execute Report through Command Line</b>	Learn how to execute and export same reports multiple times by exporting reports through a command line.	 Watch Video

# Index

## - 2 -

2FA 125, 128, 131, 133, 137, 905

## - A -

Active Directory admin 187

## - B -

Bastion server 19

## - C -

Citrix 76

## - J -

Jump box 19

Jump server 19

## - M -

MFA 905

MSSQL 199

## - P -

parameters 756

Password analyzer 502

Password strength 502

## - R -

RDS 76

Remote Desktop Services 76

RemoteApp 76

## - S -

Service host 19

Silent install 43

## - T -

Terminal service 15, 38, 41, 76, 344, 540, 936, 947, 985

TS 76

two-factor 905

## - U -

Unattended 43

update 80



Control the IT Chaos

## Contact Us

For any questions, feel free to contact us:

Support: [support@devolutions.net](mailto:support@devolutions.net)

Skype: [support.devolutions](https://www.skype.com/en/contacts/devolutions)

Phone: +1 844 463.0419

Monday to Friday 8 a.m. to 4 p.m. EST

## Head Office

**Devolutions inc.**

1000 Notre-Dame

Lavaltrie, QC J5T 1M1

Canada