# Table of Contents

## Part I Overview
1. Remote Desktop Manager ................................................................. 16
2. Security ................................................................................. 17
3. System Requirements .................................................................. 17
   Prerequisite Software .................................................................. 18
4. The Devolutions Platform ............................................................ 18
   Remote Desktop Manager Agent .................................................... 19
   Remote Desktop Manager Jump ..................................................... 21

## Part II Getting Started
1. Using Remote Desktop Manager .................................................. 25
2. Checklist for Individuals .............................................................. 27
   Select the Data Source type - Individuals ....................................... 27
3. Checklist for Teams ..................................................................... 29
   Select the Data Source type - Teams ............................................. 29
   Set up a team folder for default settings ........................................ 31
4. Creating an Entry ....................................................................... 33
5. Managing Credentials ................................................................. 34

## Part III Installation
1. Client ....................................................................................... 37
   Ancillary Files ........................................................................ 37
   Configuration File Location .......................................................... 39
   Custom Installer Manager ............................................................ 40
   Installer File Generator .................................................................. 41
   Custom Installer Manager ............................................................ 46
   For All Users ........................................................................... 53
   Portable (USB) .......................................................................... 54
   Previous Version ....................................................................... 57
   Registration .............................................................................. 58
   Enterprise Edition ...................................................................... 59
   Free Edition ............................................................................. 63
   Register from Devolutions Cloud ................................................ 68
   Trial Request ............................................................................ 70
   Terminal Services / Remote Desktop Services ............................. 71
2. Database Upgrade ...................................................................... 74
3. Uninstall .................................................................................. 75
4. Update ..................................................................................... 75

## Part IV User Interface
1. Main Screen ............................................................................ 78

© 2019 Devolutions inc.
# Contents

| 3  | 2  | Style | 79 |
| 3  | 3  | Theme | 83 |
| 4  | 4  | Top Pane | 84 |
| 5  | 5  | Navigation Pane | 86 |
| 6  | 6  | Content Area | 95 |
| 7  | 7  | Panes (Footer) | 99 |
| 8  | 8  | Status Bar | 103 |
| 9  | 9  | Tray Icon | 106 |

## Part V  Data Sources  108

1 - 2-Factor Authentication | 111 |
| Google Authenticator | 115 |
| YubiKey | 117 |
| Duo | 118 |
| AuthAnvil | 122 |

2 - Caching | 123 |

3 - Create a data source | 125 |

4 - Data Source Types | 129 |
| Advanced Data Sources | 131 |
| Devolutions Online Database | 132 |
| Devolutions Password Server | 136 |
| MariaDB | 142 |
| Microsoft SQL Azure | 147 |
| Microsoft SQL Server | 168 |
| MySQL | 180 |
| Private vault | 186 |
| DropBox | 187 |
| Google Drive | 191 |
| Devolutions Online Drive | 193 |
| SQLite | 197 |
| WebDAV | 202 |
| XML | 205 |

5 - Import/Export Data Source | 209 |

6 - Lock Data Source | 210 |

7 - Offline mode | 211 |
| Offline Read/Write | 215 |

8 - Manage Cache | 218 |

9 - My Vault (Private) | 219 |
Part VI Entries

1 -Common Settings............................................................................................................................................................................................
  General ............................................................................................................................................................................................
  More ............................................................................................................................................................................................
  Permissions ................................................................................................................................................................................
  Password Management ......................................................................................................................................................................
  Security Settings ............................................................................................................................................................................
  Checkout system ..............................................................................................................................................................................
  Session Recording ........................................................................................................................................................................
  VPN/SSH/Gateway ........................................................................................................................................................................
  User Interface ................................................................................................................................................................................
  Information ......................................................................................................................................................................................
  Jump Host .....................................................................................................................................................................................
  Events ...........................................................................................................................................................................................
  Typing Macro ................................................................................................................................................................................
  Logs ................................................................................................................................................................................................
  Management Tools ........................................................................................................................................................................
  Wake-on-LAN ................................................................................................................................................................................
  Advanced ......................................................................................................................................................................................

2 -Sessions................................................................................................................................................................................................
  Open a Remote Connection ..............................................................................................................................................................
  Remote Connections ............................................................................................................................................................................
  Apple Remote Desktop ...................................................................................................................................................................
  BeyondTrust Password Safe Dashboard ........................................................................................................................................
  FTP ...............................................................................................................................................................................................
  Host ...............................................................................................................................................................................................
  LogMeIn ........................................................................................................................................................................................
  Microsoft Remote Desktop (RDP) ....................................................................................................................................................
  PowerShell Remote Console ..........................................................................................................................................................
  ScreenConnect ..............................................................................................................................................................................
  Spiceworks ....................................................................................................................................................................................
  Telnet ............................................................................................................................................................................................
  VNC ................................................................................................................................................................................................
  Wayk Now .....................................................................................................................................................................................
  Virtualization ..................................................................................................................................................................................
  Amazon Aws Dashboard ..............................................................................................................................................................
  Microsoft Hyper-V Dashboard ...................................................................................................................................................
  VMware Dashboard ......................................................................................................................................................................
  File Browser ...................................................................................................................................................................................
  Microsoft OneDrive Explorer ........................................................................................................................................................
  Others ................................................................................................................................................................................................
  Data Report ....................................................................................................................................................................................
  PowerShell ......................................................................................................................................................................................
  SNMP Report ................................................................................................................................................................................
  SQL Server Management Studio ....................................................................................................................................................

3 -Information................................................................................................................................................................................................

4 -Contact................................................................................................................................................................................................

5 -Credentials................................................................................................................................................................................................
  Credential Redirection .................................................................................................................................................................
  Dynamic Credential Linking ..........................................................................................................................................................
  Types ................................................................................................................................................................................................

© 2019 Devolutions inc.
Part VII Commands

1 - Context Menu ........................................................................................................................................................................ 413
   Open with Parameters .................................................................................................................................................................. 413
2 - File ......................................................................................................................................................................................... 415
   Go Offline/Online ........................................................................................................................................................................ 418
   My Data Source Information ....................................................................................................................................................... 419
   Devolutions Account .................................................................................................................................................................. 422
   Backup ..................................................................................................................................................................................... 424
   Settings .................................................................................................................................................................................... 424
   Restore .................................................................................................................................................................................... 426
   Refresh .................................................................................................................................................................................... 429
   Change Master Key ................................................................................................................................................................. 429
   Data Sources ........................................................................................................................................................................... 430
   Background Services ............................................................................................................................................................... 432
   Import ....................................................................................................................................................................................... 433
     Import Computer Wizard ...................................................................................................................................................... 435
     Import Session CSV Wizard ................................................................................................................................................... 440
     Import Network Scan .......................................................................................................................................................... 443
     Import Sessions ................................................................................................................................................................. 444
     Import Logins ................................................................................................................................................................. 445
     Import Contacts ............................................................................................................................................................... 446
   Export .................................................................................................................................................................................... 447
     Encrypted Html ................................................................................................................................................................. 450
   Options ................................................................................................................................................................................... 451
     Advanced ............................................................................................................................................................................. 452
     Import Options ................................................................................................................................................................. 455
     Export Options ................................................................................................................................................................. 458
   My Account Settings .............................................................................................................................................................. 460
     My Personal Credentials .................................................................................................................................................. 462
     User Specific Settings List ................................................................................................................................................ 464
### Remote Desktop Manager

<table>
<thead>
<tr>
<th>3 - Home</th>
<th>4 - Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Templates ............................................................................................................................................................................................................................................................</td>
<td>465</td>
</tr>
<tr>
<td>Creating Templates ..................................................................................................................................................................................................................................................</td>
<td>469</td>
</tr>
<tr>
<td>Default Settings ....................................................................................................................................................................................................................................................</td>
<td>474</td>
</tr>
<tr>
<td>Password Templates ...............................................................................................................................................................................................................................................</td>
<td>476</td>
</tr>
<tr>
<td>5 - Edit</td>
<td>6 - View</td>
</tr>
<tr>
<td>Edit ..................................................................................................................................................................................................................................................................................</td>
<td>481</td>
</tr>
<tr>
<td>Play List ........................................................................................................................................................................................................................................................................</td>
<td>481</td>
</tr>
<tr>
<td>Setting Overrides ...............................................................................................................................................................................................................................................</td>
<td>484</td>
</tr>
<tr>
<td>Specific Settings ...............................................................................................................................................................................................................................................</td>
<td>485</td>
</tr>
<tr>
<td>Batch ............................................................................................................................................................................................................................................................................</td>
<td>487</td>
</tr>
<tr>
<td>Batch Edit ......................................................................................................................................................................................................................................................</td>
<td>488</td>
</tr>
<tr>
<td>7 - Administration</td>
<td>8 - Tools</td>
</tr>
<tr>
<td>Management ..................................................................................................................................................................................................................................................................</td>
<td>489</td>
</tr>
<tr>
<td>User Management .........................................................................................................................................................................................................................................</td>
<td>492</td>
</tr>
<tr>
<td>Role Management ..........................................................................................................................................................................................................................................</td>
<td>492</td>
</tr>
<tr>
<td>Reports .....................................................................................................................................................................................................................................................................</td>
<td>498</td>
</tr>
<tr>
<td>Reports .....................................................................................................................................................................................................................................................................</td>
<td>499</td>
</tr>
<tr>
<td>Deleted Entries ..........................................................................................................................................................................................................................................</td>
<td>502</td>
</tr>
<tr>
<td>Settings ....................................................................................................................................................................................................................................................................</td>
<td>505</td>
</tr>
<tr>
<td>Root (Settings) .........................................................................................................................................................................................................................................</td>
<td>507</td>
</tr>
<tr>
<td>System Settings ........................................................................................................................................................................................................................................</td>
<td>507</td>
</tr>
<tr>
<td>System Permissions ...................................................................................................................................................................................................................................</td>
<td>508</td>
</tr>
<tr>
<td>Security Providers ..............................................................................................................................................................................................................................</td>
<td>509</td>
</tr>
<tr>
<td>Clean up ..................................................................................................................................................................................................................................................................</td>
<td>512</td>
</tr>
<tr>
<td>Clean Up Deleted History ........................................................................................................................................................................................................</td>
<td>512</td>
</tr>
<tr>
<td>Clean Up Entry History ...........................................................................................................................................................................................................</td>
<td>512</td>
</tr>
<tr>
<td>Clean Up Activity Logs ...........................................................................................................................................................................................................</td>
<td>512</td>
</tr>
<tr>
<td>Pack Data Source (Optimize) ........................................................................................................................................................................................................</td>
<td>512</td>
</tr>
<tr>
<td>8 - Tools</td>
<td>9 - Commands</td>
</tr>
<tr>
<td>Password Generator ...........................................................................................................................................................................................................................................</td>
<td>514</td>
</tr>
<tr>
<td>SSH Key Generator .......................................................................................................................................................................................................................................</td>
<td>516</td>
</tr>
<tr>
<td>Certificate Generator ..........................................................................................................................................................................................................................</td>
<td>516</td>
</tr>
<tr>
<td>Port Generator .........................................................................................................................................................................................................................................</td>
<td>520</td>
</tr>
<tr>
<td>Tools ......................................................................................................................................................................................................................................................................</td>
<td>524</td>
</tr>
<tr>
<td>Password Analyzer ......................................................................................................................................................................................................................................</td>
<td>524</td>
</tr>
<tr>
<td>Key Agent Manager ..........................................................................................................................................................................................................................</td>
<td>524</td>
</tr>
<tr>
<td>PowerShell (RDM CmdLet) ........................................................................................................................................................................................................</td>
<td>524</td>
</tr>
</tbody>
</table>

© 2019 Devolutions inc.
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get-RDMInstance</td>
<td>704</td>
</tr>
<tr>
<td>Get-RDMOpenedSession</td>
<td>704</td>
</tr>
<tr>
<td>Get-RDMPaylistLocal</td>
<td>705</td>
</tr>
<tr>
<td>Get-RDMPaylistShared</td>
<td>706</td>
</tr>
<tr>
<td>Get-RDMPaylistShared</td>
<td>706</td>
</tr>
<tr>
<td>Get-RDMPaylistPrivateSession</td>
<td>707</td>
</tr>
<tr>
<td>Get-RDMSecurityGroup</td>
<td>708</td>
</tr>
<tr>
<td>Get-RDMSession</td>
<td>709</td>
</tr>
<tr>
<td>Get-RDMSessionStatus</td>
<td>710</td>
</tr>
<tr>
<td>Get-RDMSessionCredentials</td>
<td>711</td>
</tr>
<tr>
<td>Get-RDMSessionDocumentStoredInDatabase</td>
<td>712</td>
</tr>
<tr>
<td>Get-RDMSessionDomain</td>
<td>712</td>
</tr>
<tr>
<td>Get-RDMSessionPassword</td>
<td>713</td>
</tr>
<tr>
<td>Get-RDMSessionProperty</td>
<td>714</td>
</tr>
<tr>
<td>Get-RDMSessionUserName</td>
<td>715</td>
</tr>
<tr>
<td>Get-RDMSessionUserName</td>
<td>716</td>
</tr>
<tr>
<td>Get-RDMSessionUserName</td>
<td>716</td>
</tr>
<tr>
<td>Get-RDMSessionDomain</td>
<td>717</td>
</tr>
<tr>
<td>Get-RDMSessionPassword</td>
<td>718</td>
</tr>
<tr>
<td>Get-RDMSessionProperty</td>
<td>719</td>
</tr>
<tr>
<td>Get-RDMSessionUserName</td>
<td>720</td>
</tr>
<tr>
<td>Get-RDMSessionUserName</td>
<td>720</td>
</tr>
<tr>
<td>Get-RDMSessionUserName</td>
<td>723</td>
</tr>
<tr>
<td>Get-RDMSessionUserName</td>
<td>723</td>
</tr>
<tr>
<td>Get-RDMSessionUserName</td>
<td>724</td>
</tr>
<tr>
<td>Get-RDMSessionUserName</td>
<td>724</td>
</tr>
<tr>
<td>Get-RDMSessionUserName</td>
<td>725</td>
</tr>
<tr>
<td>Get-RDMSessionUserName</td>
<td>726</td>
</tr>
<tr>
<td>Get-RDMSessionUserName</td>
<td>727</td>
</tr>
<tr>
<td>Get-RDMSessionUserName</td>
<td>728</td>
</tr>
<tr>
<td>Get-RDMSessionUserName</td>
<td>728</td>
</tr>
<tr>
<td>Get-RDMSessionUserName</td>
<td>729</td>
</tr>
<tr>
<td>Get-RDMSessionUserName</td>
<td>730</td>
</tr>
<tr>
<td>Get-RDMSessionUserName</td>
<td>731</td>
</tr>
<tr>
<td>Get-RDMSessionUserName</td>
<td>732</td>
</tr>
<tr>
<td>Get-RDMSessionUserName</td>
<td>732</td>
</tr>
<tr>
<td>Get-RDMSessionUserName</td>
<td>733</td>
</tr>
<tr>
<td>Get-RDMSessionUserName</td>
<td>734</td>
</tr>
<tr>
<td>Get-RDMSessionUserName</td>
<td>735</td>
</tr>
<tr>
<td>Get-RDMSessionUserName</td>
<td>736</td>
</tr>
<tr>
<td>Get-RDMSessionUserName</td>
<td>737</td>
</tr>
</tbody>
</table>
50  `Set-RDMCurrentDataSource` .......................................................................................................................... 738
51  `Set-RDMDataSource` ........................................................................................................................................... 739
52  `Set-RDMDataSourceProperty` ............................................................................................................................ 739
53  `Set-RDMPersonalCredentials` ............................................................................................................................ 740
54  `Set-RDMParseListLocal` ....................................................................................................................................... 741
55  `Set-RDMParseListShared` ...................................................................................................................................... 741
56  `Set-RDMParsePrivateSession` ............................................................................................................................. 742
57  `Set-RDMParse` ...................................................................................................................................................... 742
58  `Set-RDMParseGroupRights` ................................................................................................................................. 743
59  `Set-RDMParseProperty` .......................................................................................................................................... 744
60  `Set-RDMSecurityGroup` ........................................................................................................................................ 745
61  `Set-RDMSecurityGroupProperty` .......................................................................................................................... 746
62  `Set-RDMSession` .................................................................................................................................................... 747
63  `Set-RDMSessionStatus` .......................................................................................................................................... 748
64  `Set-RDMSessionCredentials` .................................................................................................................................. 749
65  `Set-RDMSessionDocument` ..................................................................................................................................... 749
66  `Set-RDMSessionDomain` ......................................................................................................................................... 750
67  `Set-RDMSessionPassword` ..................................................................................................................................... 751
68  `Set-RDMSessionProperty` ....................................................................................................................................... 752
69  `Set-RDMSessionUsername` ..................................................................................................................................... 753
70  `Set-RDMTemplate` .................................................................................................................................................. 754
71  `Set-RDMUser` .......................................................................................................................................................... 755
72  `Set-RDMUserGroupRights` ....................................................................................................................................... 755
73  `Set-RDMUserProperty` ............................................................................................................................................ 756
74  `Set-RDMUserSecurity` ............................................................................................................................................. 757
75  `Set-RDMUserSpecificSettings` ............................................................................................................................... 758
76  `Start-RDMinstance` .................................................................................................................................................. 759
77  `Update-RDMUI` ....................................................................................................................................................... 759
78  `New-RDMRandomPassword` .................................................................................................................................... 760
79  `Open-RDMSyncSession` .......................................................................................................................................... 761
80  `Set-RDMDatasourceMasterKey` ............................................................................................................................ 762
81  `Set-RDMSQLiteDatasourcePassword` .................................................................................................................... 762
82  `Invoke-RDMLoadFromInventorySession` ............................................................................................................. 763
83  `Add-RDMSessionAttachment` .................................................................................................................................. 764
84  `Get-RDMSRepository` ............................................................................................................................................. 765
85  `Get-RDMSessionAttachment` .................................................................................................................................. 765
86  `Invoke-RDMCreateDataSourceDatabase` ........................................................................................................... 766
87  `Invoke-RDMLoadDataSourceDatabase` .................................................................................................................. 767
88  `New-RDMSRepository` ............................................................................................................................................ 767
Part XI  Knowledge Base  773

1  -Protocols and application..................................................................................................................... 774
   Remote Desktop Manager .............................................................................................................................. 774
      Add a web link in Macros/Scripts/Tools Session ....................................................................................... 774
      Configure VPN for multiple sessions ....................................................................................................... 775
      Import Credentials From KeePass ........................................................................................................... 779
      Import and Export ...................................................................................................................................... 786
      Multiple Types of Connections to a single computer ............................................................................. 789
      Pwned Password Check .............................................................................................................................. 797
      Vaults Overview .......................................................................................................................................... 800
      Quick Connect ............................................................................................................................................. 809
      Send application logs ................................................................................................................................. 810
      Send error report ....................................................................................................................................... 812
      Upgrade from Free Edition to Enterprise Edition ...................................................................................... 814
      Understand Remote Desktop Manager licensing .................................................................................... 816
      Web protocol handler ................................................................................................................................. 817
      Get Started with Remote Desktop Manager .............................................................................................. 820
      Create a saved search with Smart Folders ................................................................................................. 847
      Add an RDP entry ....................................................................................................................................... 848
   Remote Desktop Manager Jump .................................................................................................................. 848
      Configure Remote Desktop Manager Jump ............................................................................................... 848
   RDP ................................................................................................................................................................. 853
      Restoring the rdp file association with mstsc.exe ..................................................................................... 853
   SSH ................................................................................................................................................................. 853
      Configure an SSH Tunnel ........................................................................................................................... 853
   VMware .......................................................................................................................................................... 854
      Configuring VMware’s PowerCLI for use by Remote Desktop Manager ................................................. 854
   Tips and tricks ................................................................................................................................................. 855
      Use Multiple Versions of a Third Party Application ................................................................................. 855
      Sending Windows Credentials inside TeamViewer .................................................................................... 855

2  -Performance................................................................................................................................................ 859
   Memory Tuning Of RDP Sessions ................................................................................................................ 859

3  -Security...................................................................................................................................................... 860
   Blocking MS RDP to Only Use Remote Desktop Manager ......................................................................... 860
   Certificate validation ..................................................................................................................................... 861
   Windows Credential Manager ....................................................................................................................... 866

Part XII  Support/Resources  868

1  -Keyboard Shortcuts ..................................................................................................................................... 869
2  -Command Line Arguments ....................................................................................................................... 871
3  -Lexicon ....................................................................................................................................................... 873
4  -Follow Us ................................................................................................................................................... 873

© 2019 Devolutions inc.
5 -Technical Support .................................................................................................................. 874

6 -Add-on Documentation ........................................................................................................... 874
   Bomgar Representative Console Add-on .................................................................................. 875
   DbVisualizer Add-on .............................................................................................................. 876
   NoMachine Add-on ................................................................................................................. 877
   PenguINet SSH Client Add-on ................................................................................................. 878
   SAP Frontend Server (SAP GUI) Add-on .................................................................................. 880
   Shutdown Application Tool Add-on ......................................................................................... 881
   SQL Server Management Studio Add-On .................................................................................. 883
   VPN Add-ons .......................................................................................................................... 885
      Cisco AnyConnect .................................................................................................................. 885
      Generic VPN .......................................................................................................................... 886
      OpenVPN .............................................................................................................................. 887

7 -Best Practices .......................................................................................................................... 888
   Data Backups ........................................................................................................................... 889
   Credential Management For Teams ......................................................................................... 890
   Use Credential Entries ............................................................................................................. 893
   Use VPN Entries ..................................................................................................................... 893

8 -How-To ................................................................................................................................... 893
   How to Add a Web Link in Macros/Scripts/Tools Session ......................................................... 893
   How to apply policies ............................................................................................................... 898
   How to Backup Remote Desktop Manager .............................................................................. 902
   How to Configure Password Manager Pro in Remote Desktop Manager .............................. 902
   How to Configure ConnectWise (ScreenConnect) 5 in Remote Desktop Manager .............. 907
   How to Configure the Google Authenticator 2-Factor Authentication ................................. 911
   How to Configure the Yubikey 2-Factor Authentication .......................................................... 912
   How to Disable Remote Desktop Manager Auto Update ....................................................... 914
   How to Reinstall Remote Desktop Manager ........................................................................... 914
   How to Send an Error Report ................................................................................................. 915
   How to Send a File Securely .................................................................................................... 917
   How to Send the Application Logs Report ............................................................................. 918
   How to Send your Configuration File ..................................................................................... 919
   How to Setup a SSH Tunnel .................................................................................................... 919
   How to Setup Remote Desktop Manager to Receive New Update ........................................ 925
   How to Setup the Usage of the Session Credentials to Launch a Tool .................................. 925
   How to Subscribe to the Announcements Forums ................................................................... 926
   How to Use a Typing Macro to Perform Authentication .......................................................... 927
   How to use the Theme system ................................................................................................. 930
   Image List ................................................................................................................................. 931
   PowerShell ............................................................................................................................... 938
      Extract TeamViewer ID ......................................................................................................... 939
      Custom Export to CSV .......................................................................................................... 939
      Remote Management ........................................................................................................... 940
      Script Execution Policy ....................................................................................................... 940
      Change your Synchronizer source ....................................................................................... 940

9 -Tips And Tricks ......................................................................................................................... 944
   Allow Open Multiple Connections ....................................................................................... 944
   Automating Remote Microsoft Management Console (MMC) ............................................. 945
   Create a list of credentials ...................................................................................................... 948
   Creating Shortcuts .................................................................................................................. 951
   Data Migration ....................................................................................................................... 953
   Data Report ............................................................................................................................. 959
## Troubleshooting

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit Hosts File</td>
<td>962</td>
</tr>
<tr>
<td>Handling RDP Connections</td>
<td>965</td>
</tr>
<tr>
<td>HTML Export Using Symmetric Encryption</td>
<td>966</td>
</tr>
<tr>
<td>Keep Tabs Opened</td>
<td>967</td>
</tr>
<tr>
<td>Open RD Gateway Only when Unable to Ping Host</td>
<td>969</td>
</tr>
<tr>
<td>Passcode Prompt When Opening an Entry</td>
<td>969</td>
</tr>
<tr>
<td>RDP Session Time Limits</td>
<td>970</td>
</tr>
<tr>
<td>Remote Install with PSEnc</td>
<td>974</td>
</tr>
<tr>
<td>Run as Another User</td>
<td>975</td>
</tr>
<tr>
<td>Built-in RunAs</td>
<td>976</td>
</tr>
<tr>
<td>Manual RunAs</td>
<td>981</td>
</tr>
<tr>
<td>Running Remote Desktop Manager as Another User</td>
<td>987</td>
</tr>
<tr>
<td>SQL Server Data Source with Integrated Security</td>
<td>988</td>
</tr>
<tr>
<td>SQL Server Maintenance Plans</td>
<td>994</td>
</tr>
<tr>
<td>Tab Groups</td>
<td>995</td>
</tr>
<tr>
<td>Team Tips</td>
<td>997</td>
</tr>
<tr>
<td>Testing variables</td>
<td>999</td>
</tr>
<tr>
<td>Use Different Versions of Same Application</td>
<td>1000</td>
</tr>
<tr>
<td>VPN</td>
<td>1000</td>
</tr>
<tr>
<td>VPN Group</td>
<td>1000</td>
</tr>
<tr>
<td>VPN Routing</td>
<td>1001</td>
</tr>
<tr>
<td>2-Factor Authentication</td>
<td>1005</td>
</tr>
<tr>
<td>1Password</td>
<td>1006</td>
</tr>
<tr>
<td>Apple Remote Desktop</td>
<td>1006</td>
</tr>
<tr>
<td>BeyondTrust</td>
<td>1006</td>
</tr>
<tr>
<td>Clipboard</td>
<td>1007</td>
</tr>
<tr>
<td>Corrupted System File</td>
<td>1008</td>
</tr>
<tr>
<td>Data Recovery</td>
<td>1008</td>
</tr>
<tr>
<td>Data Sources</td>
<td>1008</td>
</tr>
<tr>
<td>Database Schema</td>
<td>1010</td>
</tr>
<tr>
<td>Devolutions Online Database</td>
<td>1012</td>
</tr>
<tr>
<td>MySQL</td>
<td>1012</td>
</tr>
<tr>
<td>SQL Azure</td>
<td>1014</td>
</tr>
<tr>
<td>SQL Server</td>
<td>1015</td>
</tr>
<tr>
<td>DB Upgrades</td>
<td>1019</td>
</tr>
<tr>
<td>FIPS (Encryption)</td>
<td>1019</td>
</tr>
<tr>
<td>KeePass</td>
<td>1020</td>
</tr>
<tr>
<td>LogMeIn</td>
<td>1020</td>
</tr>
<tr>
<td>Microsoft Office</td>
<td>1021</td>
</tr>
<tr>
<td>Microsoft RDP</td>
<td>1022</td>
</tr>
<tr>
<td>Automatic Logon</td>
<td>1026</td>
</tr>
<tr>
<td>Cannot Store Password on Local Computer</td>
<td>1031</td>
</tr>
<tr>
<td>Display Issues</td>
<td>1032</td>
</tr>
<tr>
<td>Keyboard not working</td>
<td>1033</td>
</tr>
<tr>
<td>Licensing Protocol Error</td>
<td>1033</td>
</tr>
<tr>
<td>Logoff Access Denied</td>
<td>1034</td>
</tr>
<tr>
<td>Logoff Issue</td>
<td>1036</td>
</tr>
<tr>
<td>Memory and Performance Issues</td>
<td>1036</td>
</tr>
<tr>
<td>Missing mapped drives</td>
<td>1038</td>
</tr>
<tr>
<td>Printer Redirection</td>
<td>1040</td>
</tr>
</tbody>
</table>
Protocol Error .................................................................................................................. 1040
RDP Session Credentials ............................................................................................... 1042
Remote Computer Requires Authentication to be Enabled Error .............................. 1043
Reconnect ....................................................................................................................... 1043
RD Gateway Credentials Prompt When Trying To Reconnect .................................... 1044
RDM Hangs when logging off RDP sessions .................................................................. 1045
Sessions work using mstsc.exe but not in RDM ............................................................ 1047
Network Devices ........................................................................................................ 1048
Password Manager Pro ............................................................................................... 1048
Performance ................................................................................................................ 1051
Data sources ................................................................................................................ 1051
Diagnostic .................................................................................................................... 1053
Startup ........................................................................................................................ 1056
Powershell ................................................................................................................... 1056
Putty .............................................................................................................................. 1060
Remote Desktop Manager ............................................................................................ 1060
Caching ........................................................................................................................ 1062
Debugging .................................................................................................................... 1062
High CPU Usage ......................................................................................................... 1063
HDPI Scaling Issues .................................................................................................... 1064
Hung Remote Desktop Manager .................................................................................. 1067
Large Memory Aware Application ............................................................................... 1068
Missing Navigation Pane ............................................................................................ 1069
Missing Sessions ......................................................................................................... 1070
Offline Mode ............................................................................................................... 1071
Profiler ........................................................................................................................ 1072
Root Is Empty Error ..................................................................................................... 1072
Session Focus Issue ..................................................................................................... 1073
SQL Server Data Source Connection Refused ............................................................. 1073
Startup performance ................................................................................................... 1074
Unable to install or upgrade ......................................................................................... 1076
Unable to Uninstall ....................................................................................................... 1076
Upgrade ....................................................................................................................... 1077
User Interface .............................................................................................................. 1077
Unable to communicate with Password Vault Manager ............................................. 1079
Proxy Authentication Required Error ......................................................................... 1080
RPC ............................................................................................................................... 1080
Secret Server ............................................................................................................... 1081
Secure Note .................................................................................................................. 1082
Session Tools .............................................................................................................. 1082
SSH ............................................................................................................................. 1083
Synchronizers ............................................................................................................. 1084
Active Directory Synchronizer .................................................................................... 1084
VMWare ...................................................................................................................... 1085
Advanced Troubleshooting of the PowerCLI ............................................................... 1088
VPN .............................................................................................................................. 1090
Missing Opened VPN from List .................................................................................. 1090
FortiClient ................................................................................................................... 1090
Sonicwall Global VPN Client ...................................................................................... 1091
Microsoft VPN ............................................................................................................ 1091
Cisco AnyConnect ....................................................................................................... 1092
Web Browsers ............................................................................................................ 1093
Internet Explorer ........................................................................................................ 1093
Google Chrome .......................................................................................................... 1095

© 2019 Devolutions inc.
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, Terminal Services, VMware, VNC, SCP, Wayk Now, X Windows, and more!

The Remote Desktop Manager ecosystem

Remote Desktop Manager is available in two editions:

<table>
<thead>
<tr>
<th>Edition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free</td>
<td>For individuals only, no information can be shared with colleagues. The most popular remote access technologies are supported, and passwords can be stored securely.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>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 your security requirements. Devolutions also offers two specialized services for either Cloud-Based storage, or to get full Active Directory Integration.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Platform</th>
<th>Free Edition</th>
<th>Enterprise Edition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>macOS</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>iOS</td>
<td></td>
<td>✔ (Free App)</td>
</tr>
<tr>
<td>Android</td>
<td></td>
<td>✔ (Free App)</td>
</tr>
</tbody>
</table>

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.
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 7 SP1, Windows 8.1, and Windows 10.
- 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.

Terminal Services and Thin Client Support

Remote Desktop Manager can be installed on Terminal 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

<table>
<thead>
<tr>
<th>APPLICATIONS</th>
<th>DESCRIPTION</th>
<th>INSTALLATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Desktop Manager (RDM)</td>
<td>Application used to manage and centralize remote access technologies, passwords, documents and shared information.</td>
<td>Windows, macOS, iOS, Android</td>
</tr>
<tr>
<td>Remote Desktop Manager Agent</td>
<td>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 TrustedHosts.</td>
<td>Windows</td>
</tr>
<tr>
<td>Remote Desktop Manager Jump</td>
<td>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.</td>
<td>Windows</td>
</tr>
<tr>
<td>Devolutions Password Server (DPS)</td>
<td>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.</td>
<td>Windows</td>
</tr>
<tr>
<td>Devolutions Web Login (DWL)</td>
<td>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.</td>
<td>Windows, macOS</td>
</tr>
</tbody>
</table>

### 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.
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:

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](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](https://remotedesktopmanager.com/Home/Download) and deploy them on the remote host in the folder of your choice.
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?

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
2 Getting Started

2.1 Using Remote Desktop Manager

Steps to getting Remote Desktop Manager up and running.

Remote Desktop Manager is highly flexible and can work for both individuals and teams.

Since the concerns are quite different, please follow the checklist that applies to your environment.

Checklist for Individuals

This checklist is mostly for individuals but also for teams of three users or less that do not want to implement security.

<table>
<thead>
<tr>
<th>CHECKLIST FOR INDIVIDUALS (ENTERPRISE EDITION)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 - Register your license.</td>
</tr>
<tr>
<td>Step 2 - Choose your data source type (individuals).</td>
</tr>
<tr>
<td>Step 3 - Select your Security Provider.</td>
</tr>
<tr>
<td>Step 4 - Set up your Devolutions Online Backup.</td>
</tr>
<tr>
<td>Step 5 - Create your Default Settings.</td>
</tr>
<tr>
<td>Step 6 - Import your data.</td>
</tr>
</tbody>
</table>

For more details on the Checklist for Individuals, please follow this link.

Checklist for Teams

This checklist is useful when setting up Remote Desktop Manager for a team environment that wishes to implement security.

<table>
<thead>
<tr>
<th>CHECKLIST FOR TEAMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 - Register your license.</td>
</tr>
<tr>
<td>Step 2 - Add your Data Source (for teams).</td>
</tr>
<tr>
<td>Step 3 - Select your Security Provider.</td>
</tr>
<tr>
<td>Step 4 - Create your folder structure.</td>
</tr>
<tr>
<td>Step 5 - Create your Default Settings.</td>
</tr>
<tr>
<td>Step 6 - Create Users.</td>
</tr>
<tr>
<td>Step 7 - Create Roles.</td>
</tr>
<tr>
<td>Step 8 - Create Entries.</td>
</tr>
<tr>
<td>Step 9 - Grant Permissions.</td>
</tr>
<tr>
<td>Step 10 - Import your Data.</td>
</tr>
</tbody>
</table>

For more details on the Checklist for Teams, please follow this link.
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.

<table>
<thead>
<tr>
<th>CHECKLIST FOR INDIVIDUALS (ENTERPRISE EDITION)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 - <strong>Register your license serial.</strong></td>
</tr>
<tr>
<td>Step 2 - <strong>Choose a data source type (individuals).</strong></td>
</tr>
<tr>
<td>Step 3 - Set up your data source with a master key or encryption.</td>
</tr>
<tr>
<td>Step 4 - <strong>Set up your Devolutions Online Backup with Devolutions Cloud.</strong></td>
</tr>
<tr>
<td>Step 5 - <strong>Create your Default Settings.</strong></td>
</tr>
<tr>
<td>Step 6 - <strong>Import your data.</strong></td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>DATA SOURCE</th>
<th>LOCAL</th>
<th>SELF-HOSTED</th>
<th>CLOUD BASED</th>
<th>SHARED BETWEEN YOUR COMPUTER S</th>
<th>WORKS OFFLINE</th>
<th>MULTI-USER</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQLite</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>XML</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Devolutions Online Drive</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dropbox (Note )</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Note 1</td>
</tr>
<tr>
<td>Amazon S3,</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Note 1</td>
</tr>
<tr>
<td>FTP, SFTP</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Note 1</td>
</tr>
<tr>
<td>Web</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>Note 2</td>
</tr>
<tr>
<td>Devolutions Online Database - Basic</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>3 users</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Register your license.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Add your Data Source (for teams).</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select your Security Provider.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Create your folder structure.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Create your Default Settings.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Create Users.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Create Roles.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Create Entries.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Grant Permissions.</td>
</tr>
<tr>
<td>Step 10</td>
<td>Import your Data.</td>
</tr>
</tbody>
</table>

**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.
<table>
<thead>
<tr>
<th>CONCERN</th>
<th>DEVOLUTIONS PASSWORD SERVER</th>
<th>SQL SERVER</th>
<th>SQL AZURE</th>
<th>MYSQL/MARIADB</th>
<th>DODB PRO</th>
<th>DODB ENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>The database is not accessible to end users</td>
<td>X</td>
<td>Note 1 &amp; 2</td>
<td>Note 1</td>
<td>Note 1</td>
<td>Note 1</td>
<td>Note 1</td>
</tr>
<tr>
<td>AD accounts used for authentication</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AD group membership used to assign permissions</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The data is stored on-premises</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity Logs</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Data accessible globally</td>
<td>Note 3</td>
<td>Note 4</td>
<td>X</td>
<td>Note 4</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Optional local cache of connections</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

**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.

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.
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.
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.

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:

<table>
<thead>
<tr>
<th>Password visibility</th>
<th>You can store passwords in a Credential entry (Username / Password entry, which (by default) makes the password USABLE, but not VISIBLE, 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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credentials set on folders</td>
<td>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 Inherited Credentials.</td>
</tr>
<tr>
<td>Entry location</td>
<td>When storing entries in the tree view, users with the View 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 Private Vault 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 User Specific Settings feature described below.</td>
</tr>
<tr>
<td>User Specific Settings</td>
<td>User Specific Settings are partial overrides for settings of your entries, most notably the Credentials. When applying such an override, one can choose the type in the credentials directly in the override or one can choose to instead link to credentials stored elsewhere, such as the Private Vault.</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>SCENARIO</th>
<th>STRATEGY</th>
</tr>
</thead>
<tbody>
<tr>
<td>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).</td>
<td>Set the credentials on the <strong>Root Settings</strong>. All children use <strong>Inherited Credentials</strong>.</td>
</tr>
<tr>
<td>Each user has its own credentials for many different branches (often corresponds to customers/departments, etc).</td>
<td>Make use of the <strong>User Specific Settings</strong> on each branch. All children use <strong>Inherited Credentials</strong>.</td>
</tr>
<tr>
<td>Each user has its own credentials managed by an administrator.</td>
<td>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 <strong>User Specific Settings</strong> to specify that the credentials stored in that folder is used to override what is defined in the entries.</td>
</tr>
<tr>
<td>Each team uses the same credentials.</td>
<td>Much like directly above, but all the members of the team have access to the folder. All of them must use the <strong>User Specific Settings</strong>.</td>
</tr>
<tr>
<td>Each user uses their domain account.</td>
<td>Have the sessions configured to use <strong>My personal credentials</strong>. Each user will be prompted to define them once per workstation that they use.</td>
</tr>
</tbody>
</table>
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


### 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.

### Terminal Services

Please consult the Terminal 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

<table>
<thead>
<tr>
<th>FILE(S)</th>
<th>LOCATION</th>
<th>OVERRIDE SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration File(s) (*.cfg, *.ext)</td>
<td>[CONFIG]</td>
<td>None</td>
</tr>
<tr>
<td>Data File(s) (*.xml, *.db)</td>
<td>[CONFIG] or custom path.</td>
<td>None</td>
</tr>
<tr>
<td>Default Settings</td>
<td>[CONFIG]</td>
<td>Data source settings (System Settings)</td>
</tr>
<tr>
<td>Layout Files (*.lyt)</td>
<td>[CONFIG]</td>
<td>None</td>
</tr>
<tr>
<td>Log Files (*.log, *.debug)</td>
<td>[CONFIG]</td>
<td>None</td>
</tr>
<tr>
<td>Offline/Cache data (offline.db)</td>
<td>[PROFILE][Datasource]</td>
<td><strong>Use application directory for online cache</strong> will use instead [INSTALLDIR]</td>
</tr>
<tr>
<td>Local Play lists</td>
<td>[PROFILE][Datasource]\Playlists</td>
<td><strong>Use application directory for local playlist</strong> will use instead [INSTALLDIR]</td>
</tr>
<tr>
<td>Local Templates</td>
<td>They are serialized directly in the configuration file of the application.</td>
<td>None</td>
</tr>
<tr>
<td>Themes</td>
<td>[CONFIG]</td>
<td>None</td>
</tr>
</tbody>
</table>

### Offline and Local Play list option

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

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

<table>
<thead>
<tr>
<th>CASE</th>
<th>CONFIGURATION FILE LOCATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed under &quot;Program Files&quot; or &quot;Program Files (x86)&quot;</td>
<td><code>%LocalAppData%\Devolutions\RemoteDesktopManager</code></td>
</tr>
<tr>
<td>Application running on Terminal Server</td>
<td><code>%AppData%\Devolutions\RemoteDesktopManager</code>. This is the roaming profile and avoids multi-user conflicts.</td>
</tr>
<tr>
<td>Other</td>
<td>Installation folder</td>
</tr>
</tbody>
</table>

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:

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

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 Terminal Services Environment

Please refer to Terminal Services for details.

3.1.3 Custom Installer Manager

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 Cloud 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.

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

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

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

![Remote Desktop Manager]

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.

Registration information
### Registration Information

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Company registration name.</td>
</tr>
<tr>
<td><strong>Email</strong></td>
<td>Registration email if using a generic address.</td>
</tr>
<tr>
<td><strong>Key</strong></td>
<td>License serial.</td>
</tr>
</tbody>
</table>

### Installer File Generator - Miscellaneous

- **Do not redistribute the Devolutions Cloud 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.

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

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

### 3.1.3.2 Custom Installer Manager

#### Description

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

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

#### Create an Installation Package

1. Click on **File – Devolutions Account – Sign-in** to connect to your Devolutions Cloud account.
2. Click on **Custom Installer Manager** to create a new custom installer with specific settings.

![Custom Installer Manager](image1)

3. Click on **New Package**.

![Custom Installer Manager - New Package](image2)

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.
When choosing to create a new configuration, select what to include in the custom installer, then click on **Generate**.
5. Once the installation package has been created, the request is submitted to our online service. A confirmation dialog window appears if successful.

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

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

Best regards,

Devolutions Team  
support@devolutions.net

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 Cloud 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](image)

Download From The Devolutions Cloud

From the **Devolutions Cloud account** 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.
3.1.4 For All Users

Description

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

Procedure

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

1. Copy the installer to a folder available for all users of the workstation. e.g. c:\Deploy

2. Open an Elevated Command prompt (right click on the shortcut and select Run as administrator).

3. Run the following command, adapted for the version that you are installing

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

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

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

Notes

The Microsoft installer technology copies the installer package under a new randomized name as well as register it in a database. Our experience shows that this copy has a way of disappearing and that the database becomes corrupted. We often have to direct our community to use

https://support.microsoft.com/en-us/mats/program_install_and_uninstall
The *Quiet* and *Passive* parameters are just to ensure that you do not have to make a choice during the installation. We found that this reduces the risk of errors.

### 3.1.5 Portable (USB)

**Description**

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

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="icon_info.png" alt="Info" /></td>
<td>The portable installation mode allows you to run multiple versions of Remote Desktop Manager, using various license serials and configurations.</td>
</tr>
<tr>
<td><img src="icon_wrong.png" alt="Wrong" /></td>
<td>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.</td>
</tr>
<tr>
<td><img src="icon_tip.png" alt="Tip" /></td>
<td>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.</td>
</tr>
<tr>
<td><img src="icon_right.png" alt="Right" /></td>
<td>The following steps ensures true portability and ease of maintenance. It can easily be adapted to your liking.</td>
</tr>
</tbody>
</table>

**Procedure**

1. Download the "Zip" package of Remote Desktop Manager.
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`
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.
You can now delete the pre-existing Local data source that had been created automatically.

### 3.1.6 Previous Version

**Description**

Sometimes you may need an older version installer package. If the version wasn't an official release or had been replaced by an ulterior build, you may not always see it on your download page.

**Procedure**

All our builds are available and it's easy to recreate the download link by simply changing the version number from other download links.

For example, downloading Remote Desktop Manager 11.0.12.0 can be done using this hyperlink: [http://cdn.devolutions.net/download/Setup.RemoteDesktopManager.11.0.12.0.exe](http://cdn.devolutions.net/download/Setup.RemoteDesktopManager.11.0.12.0.exe)

You can simply copy the link to your address bar, and replace the version number by the one you are looking for. Ex: [http://cdn.devolutions.net/download/Setup.RemoteDesktopManager.11.0.8.0.exe](http://cdn.devolutions.net/download/Setup.RemoteDesktopManager.11.0.8.0.exe)

You can download the needed version from one of the links in the sections below as well.
Remote Desktop Manager Enterprise Edition .exe

Remote Desktop Manager Enterprise Edition msi package

Remote Desktop Manager Enterprise Edition zip file

Remote Desktop Manager Free Edition .exe

Remote Desktop Manager Free Edition .msi package

Remote Desktop Manager Free Edition zip file

3.1.7 Registration

Description

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

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

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

Devolutions Password Server
Consult Create Devolutions Server Instance to register a new Devolutions Server instance. If you want to activate your renewal license key, consult How To Activate Your Renewal Subscription for Devolutions Server.

Devolutions Online Database
Please consult Online Database Registration to register a new Devolutions Online Database.
3.1.7.1 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


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

Below, you will find your unique Remote Desktop Manager Enterprise license information.

User: Devolutions (global license)  
Serial: 119D2-747MA-__-__-__  
Renewal Date: July 1st 2023

Devolutions License Serial Email

Go to Help – Register Product. Enter the username, email, and serial number, then click OK.
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 – Data Source Settings (System Settings).

In the System Settings window, go in the Serial Number section. Enter the license serial and click OK.
For Users

Once the license serial is stored in the data source, launch the new installation of Remote Desktop Manager and click *Cancel* when prompted for a license serial.

When no serial is found, the application indicates *No Enterprise license found* in the Navigation Pane.
No Enterprise License Found

Navigate to **File – Data Sources**, and add the data source containing the license serial.

License Found - The Data Source is Connected

The application is now registered and the data source connected.

**3.1.7.2 Free Edition**

**Description**

Remote Desktop Manager Free Edition still requires (free) registration after 30 days to be able to use the application. To enable you to fully test the Free Edition prior to providing your email address, we have granted a 30-day grace period during which no registration is necessary.

Upon every application launch, the **Register the Application** window is displayed. It provides the number of remaining days in the grace period, and the source choices for the registration data.
Use registration from Devolutions Cloud

Every holder of a Devolutions Cloud account (also free of charge) is assigned a license serial for all our complementary products. By selecting *Use registration from Devolutions Cloud*, a credentials prompt is displayed upon clicking OK. The license serial will be retrieved automatically from the provided account. If you do not have a Devolutions Cloud account, create one by clicking the ***Create a Free Account*** link.

**Use an existing Devolutions Cloud account**

Enter the information of an existing Devolutions Cloud account to log in.
Create a new Devolutions Cloud account

Click on **Create a Free Account** link to display the following registration form in a web browser.

> The Devolutions Cloud account registration is not complete until you have received the activation email and clicked on the **Activate** link. Attempting to complete the Remote Desktop Manager Free registration process will fail unless you have confirmed the email address.
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 provided manually. You will need to obtain the serial registration key from your Devolutions Cloud account.

Simply log in to https://cloud.devolutions.net and click on My Serials in the navigation pane on the left. The serials for the Free Editions of both Remote Desktop Manager located on the top of the page.
Store these license serials in a safe place in case they are needed for an offline registration of the product.

Once the license serial is available offline, open Remote Desktop Manager - Free Edition. In the Register the Application window, select **Use serial** and enter a valid license serial, along with your email.
3.1.7.3 Register from Devolutions Cloud

Description

It is possible to register the product with a license serial stored in a Devolutions Cloud account.

When creating a Devolutions Cloud account a free license serial is provided for the free edition of our products. License serials purchased for the enterprise edition can be stored in the My Serials section of the Devolutions Cloud website.

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

2. In the Select your Application Edition window, select Use registration from Devolutions Cloud.
3. Enter the credentials of the Devolutions Cloud account, then click **Connect**.
3.1.7.4 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.
When the trial has been requested, an email containing the trial license serial is sent to the address provided in the form above.

### 3.1.8 Terminal Services / Remote Desktop Services

#### Description

Remote Desktop Manager has an excellent support for running under a Terminal Services environment. A master configuration file can be created to distribute settings for all new users of the system or even to update existing user's configuration.
Please ensure that you have followed Microsoft's recommendation on how to set up an RDS environment. It will severally impact the performance if default Windows installations are performed. [https://docs.microsoft.com/en-us/windows-server/administration/performance-tuning/role/remote-desktop/session-hosts](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 terminal 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.

**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 Cloud 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**

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄</td>
<td>A group policy exists to force the new configurations to be accepted automatically.</td>
</tr>
<tr>
<td>⚠️</td>
<td>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 <code>default.cfg</code> file has changed.</td>
</tr>
<tr>
<td>📦</td>
<td>If the main concern is deploying a new license key, and you are using one of the Advanced Data Sources, you should rather use the Data source settings (System Settings) - Serial feature.</td>
</tr>
</tbody>
</table>

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

![Remote Desktop Manager dialog](image)

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.

<table>
<thead>
<tr>
<th><strong>Warning</strong></th>
<th>The user performing the update must have administrative privileges on the underlying database. (SYSDBA or DB_OWNER).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Warning</strong></td>
<td>Perform a database backup and ensure that you can quickly perform a restore if required.</td>
</tr>
<tr>
<td><strong>Warning</strong></td>
<td>If your organization allows for a read/write offline cache, ensure that all of your users have merged their offline edits.</td>
</tr>
</tbody>
</table>

**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.
### Release Notes

**VERSION 2019.1.27.0 (June 5th 2019)**

**NEW FEATURES**
- Added support live display for FreeRDP/VNC/ARD
- Added thumbnail support for all the file explorer session type (FTP, SFTP, SSH Shell, S3...)

**IMPROVEMENTS**
- Added "Start all live displays" in thumbnails
- Added folder information in multiple reports
- Added setting to decide if you want to use the template's credentials in "Open with parameters -> Template"
- Added the possibility to filter the smart folder results

### Update Options

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

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

### 4.4 Top Pane

The **Top Pane** contains the Quick Access Toolbar and the Ribbon / Menu.

![Remote Desktop Manager top pane](image)

It can be hidden to maximize the work area.

![Hide the top pane completely](image)

![Hide the ribbon](image)

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.
4.4.1 Quick Access Toolbar

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

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

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 then select Add.

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>📝</td>
<td>Create a new entry in your current data source.</td>
</tr>
<tr>
<td>🕵️‍♂️</td>
<td>Open the properties window of your selected entry.</td>
</tr>
<tr>
<td>⌚️</td>
<td>Refresh your data source.</td>
</tr>
<tr>
<td>🔍</td>
<td>Open the filter dialog window to allow you to do a quick search.</td>
</tr>
</tbody>
</table>
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.
## Contents

<table>
<thead>
<tr>
<th>ELEMENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data source selector</td>
<td>Allows to switch to another configured data source.</td>
</tr>
<tr>
<td>Entry list</td>
<td>Displays the content of the current data source, depending on the selected tab. It allows to select entries and perform action on them.</td>
</tr>
<tr>
<td>Vault selector</td>
<td>Allows to switch to another configured Vault in the data source.</td>
</tr>
<tr>
<td>Tabs</td>
<td>Allows to switch to different views of the entry list, such as the Favorite entries or the Opened sessions.</td>
</tr>
</tbody>
</table>

### 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
- My Vault (Private)
- 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.
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.
**VPN Groups**

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

---

**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.

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.
The most recently used entries view can be personalized the same way as the tree view. Click on the *** button to select your preferred view.
To delete the most recently used entries history, select **Clear Most Recently Used Entries...**

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

### 4.6 Content Area

**Description**

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

The options change depending on the entry:

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

Description

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

<table>
<thead>
<tr>
<th>Display Mode Settings</th>
</tr>
</thead>
</table>

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.
The different tabs available in the dashboard:

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

The tabs can be hidden if they are not necessary for a user. Simply right-click any tab, then select an item to toggle the visibility of its relative tab.

### 4.7 Panes (Footer)

**Description**

Although the panes are by default in the footer, most tabbed windows can be moved around and docked to your liking. That applies to the Default (Ribbon) or Default (Menu) styles.
Use the **View – Footer** commands from the ribbon to control the visibility of individual panes.

### 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.

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.
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.

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.

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.
### 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.

#### 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.
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!

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
Remote Desktop Manager

- 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](image)

### 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

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

**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.*
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.
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.

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

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use default data source</td>
<td>Select the data source to connect to when the application starts.</td>
</tr>
<tr>
<td>Last used data source</td>
<td>Connect to the last used data source.</td>
</tr>
<tr>
<td>Prompt for data source</td>
<td>Prompt the user to for a data source to connect to.</td>
</tr>
</tbody>
</table>

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

3. In the next window, click **Change**.
3. Choose the type of 2-Factor Authentication you wish to use.

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**.

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

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

**Description**

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

**Settings**

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

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

5.1.3 **Duo**

**Description**

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

**Settings**

Before you start the configuration, make sure you have created yourself a Duo account and 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**.
2. In Remote Desktop Manager select Duo as your Two factor authentication and click on **Duo – General Settings**.

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

See the Duo Web SDK Documentation to integrate Duo into your custom web application.

Details

- Integration key: DJOLD
- Secret key: QwNZ
- API hostname: api-b8.duosecurity.com

Duo Account - Web SDK

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

5. Click on Save to authenticate yourself with your Duo account that has just been activated.
6. If you have more than one device connected to your Duo account, select the device you wish to use for your 2-Factor authentication.

7. Select the method by which you would like to receive your Duo Passcode.
   - **Duo Push**: The code is "pushed" to your Duo application.
   - **Send SMS**: You will receive the code by SMS on your registered phone number.
   - **Phone**: You will receive a phone call and a computer generated voice will dictate the code to you.
Once you have completed all the steps, you will be prompted with the Duo Authentication every time you connect to your secured data source.

5.1.4 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**.
2. Enter the information of your AuthAnvil account and click on Check to validate the entered information.

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 accessed via the *File – Data Sources – Edit Data Source – Advanced tab* of an **Advanced Data Source**.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>No client caching.</td>
</tr>
<tr>
<td>Intelligent</td>
<td>Intelligent cache has the ability to handle many more sessions without experiencing performance degradation.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>When first opening the data source Remote Desktop Manager will loaded the session from the offline file then refresh to get the up-to-date information.</td>
</tr>
</tbody>
</table>

**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.
3. Select the type of data source to create.
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).
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.
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

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
<th>PROS AND CONS</th>
</tr>
</thead>
</table>
| Devolutions Online Drive | Remote Desktop Manager uses Devolutions Online Drive to store and synchronize your sessions. Access your sessions from anywhere using a simple Internet connection. For more information, please consult our Online Drive topic. | Pros:  
  - Quick.  
  - Reliable.  
  - The service is free.  
Cons:  
  - No possibility for sharing.  
  - No security management. |
| Devolutions Password Server | Remote Desktop Manager uses Devolutions Password Server to store session information. For more information, please consult our Devolutions Password Server topic. | Pros:  
  - Quick.  
  - Reliable.  
  - Secure. |
<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
<th>PROS AND CONS</th>
</tr>
</thead>
</table>
| Dropbox        | Remote Desktop Manager uses the Dropbox API to retrieve the XML file from the configured repository. For more information, please consult our Dropbox topic. | Pros:  
• Can be shared in read-only mode.  
• Backups (by Dropbox) are automatic.  
• Storage infrastructure is free (if within your free storage quota).  
Cons:  
• No security management.  
• There is a possibility for conflict or data corruption to occur.  
• Doesn't support all features, such as attachments, connection logs and User Management. |
| MariaDB        | Remote Desktop Manager uses MariaDB as a drop-in replacement for MySQL. For more information, please consult our MariaDB topic. | Pros:  
• Quick.  
• Reliable.  
• The database is free and can be installed on Linux.  
• Supports all features, such as attachments, connection log, Offline mode and User Management.  
Cons:  
• MariaDB needs to be installed. |
| Microsoft SQL Azure | Remote Desktop Manager uses the Microsoft cloud platform to save and manage all sessions. For more information, please consult our SQL Azure topic. | Pros:  
• Quick.  
• Reliable.  
• Secure.  
• Supports all features, such as attachments, connection log, Offline mode and User Management.  
Cons:  
• Microsoft Azure needs to be configured. |
| Microsoft SQL Server | Remote Desktop Manager uses the power of SQL Server to save and manage all sessions. This is the recommended data source for a multi-user environment. For more information, please consult our SQL Server (MSSQL) topic. | Pros:  
• Quick.  
• Reliable.  
• Secure.  
• Supports all features, such as attachments, connection log, Offline mode and User Management.  
• SQL Server Express is free. |
<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
<th>PROS AND CONS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MySQL</strong></td>
<td>Remote Desktop Manager uses a MySQL database to store session information. For more information, please consult our MySQL topic.</td>
<td>Cons: SQL Server must be installed. Pros: Quick. Reliable. The database is free and can be installed on Linux. Supports all features, such as attachments, connection log, Offline mode and User Management.</td>
</tr>
<tr>
<td><strong>SQLite</strong></td>
<td>Remote Desktop Manager uses a SQLite database to store session information. For more information, please consult our SQLite topic.</td>
<td>Cons: MySQL needs to be installed. Pros: Quick. Reliable. The database is free. Supports all features, such as attachments &amp; connection logs.</td>
</tr>
<tr>
<td><strong>WebDAV</strong></td>
<td>Remote Desktop Manager uses an HTTP connection to retrieve the XML file on a WebDav server. For more information, please consult our WebDAV topic.</td>
<td>Cons: No possibility for sharing. No security management. Pros: Can be shared in read-only mode. Easy to deploy online.</td>
</tr>
<tr>
<td><strong>XML</strong></td>
<td>Remote Desktop Manager saves the settings directly in a file with the XML format. For more information, please consult our XML topic.</td>
<td>Cons: No possibility of sharing. No security management. There is a possibility for conflict or data corruption to occur. Doesn't support all features, such as attachments, connection logs and User Management. Pros: Easy backup. Can be edited manually or by an external system. Nothing to install.</td>
</tr>
</tbody>
</table>

### 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**
Devolutions Online Database - General Tab

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the data source.</td>
</tr>
<tr>
<td>Always ask password</td>
<td>Always ask password when connecting to the data source.</td>
</tr>
<tr>
<td>Create a Free account</td>
<td>Create a new Devolutions Cloud account.</td>
</tr>
<tr>
<td>Database</td>
<td>Name of the data base created online. You must use the ellipsis button to</td>
</tr>
<tr>
<td></td>
<td>select it from the list of online data sources available to the name.</td>
</tr>
<tr>
<td>Database ID</td>
<td>Unique Key to identify the data source.</td>
</tr>
<tr>
<td>Two factor</td>
<td>Enable the 2-Factor Authentication to access your data source.</td>
</tr>
<tr>
<td>Test Credentials</td>
<td>Test the credentials that you have configured to connect on Remote Desktop Manager Online.</td>
</tr>
</tbody>
</table>

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

Advanced
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caching mode</td>
<td>Determine how the entries will be loaded from the data source. See Caching topic for more information.</td>
</tr>
<tr>
<td>Ping online method</td>
<td>Indicate the prefer ping online. Select between:</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>• Web request</td>
</tr>
<tr>
<td>Auto refresh</td>
<td>Set the interval for the automatic refresh.</td>
</tr>
<tr>
<td>Prompt for offline mode on startup</td>
<td>Every time you will connect to your data source, you will be prompted to use the data source in offline mode.</td>
</tr>
<tr>
<td>Auto go offline</td>
<td>If the ping online method doesn't work it will automatically go offline.</td>
</tr>
<tr>
<td>Disable lock</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 website 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 Server installation instructions
- Devolutions Server Security Checklist
- Devolutions Server Automatic Account Creation

**Configure the server data source on all your client machines**

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

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

**Settings**

**General**
### Devolutions Password Server - General

**OPTION** | **DESCRIPTION**
--- | ---
Name | Enter a name for the data source.
Host | Enter the URL of the DVLS instance.  
Example: [http://<hostname or IP address>/<instance name>](http://<hostname or IP address>/<instance name>)
Use Windows authentication | Use the same credentials are your current Windows user.
Use Office365 authentication | Use the same credentials as your current Office365 user.
Always prompt for credentials | Always ask for the username and password when connecting to the data source.
Username | Enter the username to connect to the data source.
Password | Enter the password to connect to the data source.
Always ask password | Always ask for the password when connecting to the data source.
Test Connection | Test the connection with Devolutions Server to validate the credentials.
### Devolutions Password Server - Settings

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

### Private Vault

![Private Vault](image_url)
## OPTION

<table>
<thead>
<tr>
<th>TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| **Type** | Select the type of Private Vault to use. Select between:  

- **Default**: use the default Private Vault, which is stored in the database.  
- **None**: disable the Private Vault for all users.  
- **Online Drive**: use a Devolutions Online Drive file (*.dod) as a Private Vault.  |

## VPN

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

![Devolutions Password Server - VPN](image)

## Advanced
### Devolutions Password Server - Advanced

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Caching mode</strong></td>
<td>Determines how the entries will be reloaded in the data source. For more information, please consult the <a href="#">Caching</a> topic.</td>
</tr>
<tr>
<td><strong>Ping online method</strong></td>
<td>Indicate the preferred ping online method. Select between:</td>
</tr>
<tr>
<td></td>
<td>- None</td>
</tr>
<tr>
<td></td>
<td>- Web request</td>
</tr>
<tr>
<td><strong>Popup license expiration</strong></td>
<td>Determine how the application advises of the license expiration. Select between:</td>
</tr>
<tr>
<td></td>
<td>- All</td>
</tr>
<tr>
<td></td>
<td>- Only Administrator(s)</td>
</tr>
<tr>
<td></td>
<td>- Disabled</td>
</tr>
<tr>
<td><strong>Auto refresh</strong></td>
<td>Set the interval for the automatic refresh.</td>
</tr>
<tr>
<td><strong>Prompt for offline mode on startup</strong></td>
<td>Ask to use the data source in offline mode when the user connects to the data source.</td>
</tr>
<tr>
<td><strong>Auto go offline</strong></td>
<td>Use the data source in offline mode when the ping method does not respond.</td>
</tr>
<tr>
<td><strong>Disable lock</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
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.


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

![MariaDB General settings interface](image-url)
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the data source.</td>
</tr>
<tr>
<td>Host</td>
<td>Name of the host (server name) where the data source will be stored.</td>
</tr>
<tr>
<td>Username</td>
<td>Username used to access the host server.</td>
</tr>
<tr>
<td>Password</td>
<td>Password used to access the host server.</td>
</tr>
<tr>
<td>Always ask password</td>
<td>Always prompts for the user to input a password when connecting to the data source.</td>
</tr>
<tr>
<td>Allow change username</td>
<td>Allows the user to change the username. This specific setting will save the currently type username (unlike similar features such as &quot;Always prompt for credentials&quot;).</td>
</tr>
<tr>
<td>Schema</td>
<td>Name of the schema (database) on the MySQL server.</td>
</tr>
<tr>
<td>Two factor</td>
<td>Enable the 2-Factor Authentication to access your data source.</td>
</tr>
<tr>
<td>Test Host</td>
<td>Test the connection with the host (server name) to validate if the proper information has been provided.</td>
</tr>
<tr>
<td>Test Schema</td>
<td>Test the connection with the schema to validate if the proper information has been provided.</td>
</tr>
</tbody>
</table>

**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](image)

### Upgrade
**OPTION** | **DESCRIPTION**
--- | ---
Test Host | Test the connection with the Host (server name) to validate if the proper information has been provided.
Create Schema | Create the schema (database) on the MariaDB server to use Remote Desktop Manager.
Update Schema | Update the schema (database) on the MariaDB server, if required, to use Remote Desktop Manager.
Test Schema | Test the connection with the schema (database) to validate if the proper information has been provided.
Email Schema to Support | Send your schema (database) to the Devolutions Support team.
View Upgrade Script | Prompts a window to provide information about the Upgrade Script.

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

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Caching mode</strong></td>
<td>Determine how the entries will be reloaded in the data source. See <a href="#">Caching</a> topic for more information.</td>
</tr>
<tr>
<td><strong>Ping online method</strong></td>
<td>Indicate the preferred ping online. Select between:</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>• Port Scan</td>
</tr>
<tr>
<td><strong>Connection timeout</strong></td>
<td>Waiting time before a connection timeout.</td>
</tr>
<tr>
<td><strong>Command timeout</strong></td>
<td>Waiting time before a command timeout.</td>
</tr>
<tr>
<td><strong>Auto refresh</strong></td>
<td>Set the interval for the automatic refresh.</td>
</tr>
<tr>
<td><strong>Prompt for offline mode on startup</strong></td>
<td>Every time you will connect to your data source, you will be prompted to use the data source in offline mode.</td>
</tr>
<tr>
<td><strong>Auto go offline</strong></td>
<td>If the ping online method doesn't work it will automatically go offline.</td>
</tr>
<tr>
<td><strong>Disable lock</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>More Settings</strong></td>
<td>Directly edit the connection string values.</td>
</tr>
</tbody>
</table>
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

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".


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
## Microsoft SQL Azure - General

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the data source.</td>
</tr>
<tr>
<td>Host</td>
<td>Enter the server hostname or IP address.</td>
</tr>
<tr>
<td>Login mode</td>
<td>Specify the authentication mode to use. Select between:</td>
</tr>
<tr>
<td></td>
<td>- Database login</td>
</tr>
<tr>
<td></td>
<td>- Custom login</td>
</tr>
<tr>
<td></td>
<td>- Active Directory Password</td>
</tr>
<tr>
<td></td>
<td>- Active Directory Integrated</td>
</tr>
<tr>
<td></td>
<td>- Active Directory Interactive (with MFA support)</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username to access the SQL Azure database.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password to access the SQL Azure database.</td>
</tr>
<tr>
<td>Always ask password</td>
<td>Prompt for the password when a user connects to the data source.</td>
</tr>
<tr>
<td>Allow change username</td>
<td>Allow the username to be edited when connecting to the data source.</td>
</tr>
<tr>
<td>Database</td>
<td>Enter the name of the SQL Azure database.</td>
</tr>
<tr>
<td>Two factor</td>
<td>Enable the 2-Factor Authentication.</td>
</tr>
<tr>
<td>Test Database</td>
<td>Test the connection with the database to validate if the proper information has been provided.</td>
</tr>
</tbody>
</table>
### Settings

**Microsoft SQL Azure** - Settings Tab

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

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

**Upgrade**
Microsoft SQL Azure

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Database</td>
<td>Create the database on the SQL server to use Remote Desktop Manager.</td>
</tr>
<tr>
<td>Update Database</td>
<td>Update the database on the SQL server, if required to use Remote Desktop Manager.</td>
</tr>
<tr>
<td>Test Database</td>
<td>Test the connection with the database to validate if the proper information has been provided.</td>
</tr>
<tr>
<td>Email Schema to Support</td>
<td>Send your schema to the Devolutions Support team.</td>
</tr>
<tr>
<td>View Upgrade Script</td>
<td>Prompts a window to provide information about the Upgrade Script.</td>
</tr>
</tbody>
</table>

**VPN**

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

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

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

5. Connect on the Microsoft 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.
The Microsoft SQL Azure data source is now correctly configured.

5.4.1.4.2 Configure Active Directory Password

**Description**

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


From the **Ribbon**, navigate to **Administration – Users**, and add a new user.

Select "Office365/Azure AD" as the authentication type;

![User Management](image)

**Set the Authentication type to Office365/Azure AD**

**Note:** 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 AD Admin to create your other users (to start). Once you've created other admin users, you can use them to create more users.
5.4.1.4.3  Configure Active Directory Interactive (with MFA Support)

Description

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

Settings
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.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default</strong></td>
<td>Prompt to authenticate on each data source.</td>
</tr>
<tr>
<td><strong>Shared</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

3. Enter the email address to authenticate in the **Username** field.

4. Click on **Configure** to set the **Azure App Settings**.
5. Configure the database to authenticate in the **Database** field.

5.4.1.4.3.1  Configure 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 needs to be registered in the Microsoft SQL Azure console with the appropriate API permissions.

**Settings**

1. Login on [Azure Portal](https://devolutions.net/).
2. In the Azure Active Directory section, select App registrations and then, New registration.
3. Configure the **Name**, **Supported account types** and **Redirect URL** as indicated below.

### Supported account types

**Who can use this application or access this API?**

- [ ] Accounts in this organizational directory only (Devolutions)
- [x] Accounts in any organizational directory
- [x] Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

### 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 (mobile & desktop)**: https://devolutions.net
4. Click on the **Authentication** section and configure it as indicated below.
5. Click on the **API Permissions** section and configure it as indicated below.

6. Select **Azure Active Directory Graph – Delegated Permissions – User – User.Read** and click on **Add Permissions**.
Request API permissions

Select an API

- Microsoft APIs
- APIs my organization uses
- My APIs

Commonly used Microsoft APIs

**Microsoft Graph**

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and move through a single endpoint.

- **Azure Batch**
  - Schedule large-scale parallel and HPC.

- **Azure Data Catalog**
  - Programmatic access to Data Catalog.

- **Azure Data Lake**
  - Access to storage and compute for big data.

**Supported legacy APIs**

- **Azure Active Directory Graph**
  - Programmatic access to directory data and objects.

- **Exchange**
  - A powerful, easy-to-use way to access and manipulate Exchange data.
7. We would need to add a second permission. To do so, select **APIs my organization uses**, then type **Azure** and select **Azure SQL Database**.
# Request API permissions

## Select an API

<table>
<thead>
<tr>
<th>Microsoft APIs</th>
<th>APIs my organization uses</th>
<th>My APIs</th>
</tr>
</thead>
</table>

Apps in your directory that expose APIs are shown below:

<table>
<thead>
<tr>
<th>NAME</th>
<th>APPLICATION (CLIENT) ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure Analysis Services</td>
<td>ac7d521-0382-477b-008f-7e1d95f85ca2</td>
</tr>
<tr>
<td>Azure Container Registry</td>
<td>6a0ec4d3-30cb-4a83-91d-ae58bc0de3d26</td>
</tr>
<tr>
<td>Azure Data Lake</td>
<td>e9f9c6b-5ce5-44c8-925d-01507e97e</td>
</tr>
<tr>
<td>Azure DevOps</td>
<td>499b84ac-1321-427f-a17-267ca697598</td>
</tr>
<tr>
<td>Azure Key Vault</td>
<td>cfa8b139-82a2-471a-a3c9-0f0be7a4093</td>
</tr>
<tr>
<td>Azure Media Services</td>
<td>374b2a64-3b6c-436b-934c-b220eacc870</td>
</tr>
<tr>
<td>Azure Pipelines Hub (Prod)</td>
<td>4a01d87e-8a5d-461d-b264-b79c3739a12</td>
</tr>
<tr>
<td>Azure Pipelines Hub (Staging)</td>
<td>602e6588-03e5-4c84-ad02-9552a6521637</td>
</tr>
<tr>
<td><strong>Azure SQL Database</strong></td>
<td><strong>022907d3-0f1b-48f7-badc-1ba6abab66</strong></td>
</tr>
<tr>
<td>Azure Storage</td>
<td>e406a68f-f3d4-42a8-90b6-2b2b9497a1f</td>
</tr>
<tr>
<td>AzureDatabricks</td>
<td>2f814a6-3304-4ab8-85cb-c0e6f879c1d</td>
</tr>
</tbody>
</table>

APIs my organization uses
8. Select **Delegated permissions – user_impersonation** and click **Add permissions**.

9. The **API permissions** should look like this.

10. Your **Azure Active Directory App Registration** is now completed.
11. Copy the App Registration's Application (client) ID.

12. Paste the Application ID inside Remote Desktop Manager, in the App Registration section.

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.

All editions of Microsoft SQL Server (including Express) starting with 2012 and above are supported.

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**
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the data source.</td>
</tr>
<tr>
<td>Host</td>
<td>Enter the server hostname or IP address.</td>
</tr>
<tr>
<td>Login mode</td>
<td>Specify the authentication mode to use. Select between:</td>
</tr>
<tr>
<td></td>
<td>· Database login</td>
</tr>
<tr>
<td></td>
<td>· Integrated Security (Active directory)</td>
</tr>
<tr>
<td></td>
<td>· Custom Login</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username to access the SQL Azure database.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password to access the SQL Azure database.</td>
</tr>
<tr>
<td>Always ask password</td>
<td>Prompt for the password when a user connects to the data source.</td>
</tr>
<tr>
<td>Allow change username</td>
<td>Allow the username to be edited when connecting to the data source. (Only with Always ask password enabled)</td>
</tr>
<tr>
<td>Database</td>
<td>Enter the name of the SQL Azure database.</td>
</tr>
<tr>
<td>Two factor</td>
<td>Enable the 2-Factor Authentication.</td>
</tr>
<tr>
<td>Test Server</td>
<td>Test the connection with the server to validate if the proper information has been provided.</td>
</tr>
<tr>
<td>Test Database</td>
<td>Test the connection with the database to validate if the proper information has been provided.</td>
</tr>
</tbody>
</table>

**Settings**

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

### Private Vault

**Microsoft SQL Server**

<table>
<thead>
<tr>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
</tr>
<tr>
<td>Default</td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td>Online Drive</td>
</tr>
</tbody>
</table>

**Microsoft SQL Server - Private Vault Tab**

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

### Upgrade
Microsoft SQL Server - Upgrade Tab

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Server</td>
<td>Test the connection with the server to validate if the proper information has been provided.</td>
</tr>
<tr>
<td>Create Database</td>
<td>Create the database on the SQL server.</td>
</tr>
<tr>
<td>Update Database</td>
<td>Update the database on the SQL server.</td>
</tr>
<tr>
<td>Test Database</td>
<td>Test the connection with the database to validate if the proper information has been provided.</td>
</tr>
<tr>
<td>Email Schema to Support</td>
<td>Send your schema to the Devolutions support team.</td>
</tr>
<tr>
<td>View Upgrade Script</td>
<td>Open the upgrade script in a new window.</td>
</tr>
</tbody>
</table>

VPN
Open a VPN to access your data prior to connecting to your Microsoft SQL Server.
Advanced
### Microsoft SQL Server - Advanced Tab

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caching mode</td>
<td>Determines how the entries will be reloaded in the data source. For more information, please consult the <a href="#">Caching</a> topic.</td>
</tr>
<tr>
<td>Connection timeout</td>
<td>Set the delay of the connection timeout.</td>
</tr>
<tr>
<td>Command timeout</td>
<td>Set the delay of the command timeout.</td>
</tr>
<tr>
<td>Auto refresh</td>
<td>Set the interval for the automatic refresh.</td>
</tr>
<tr>
<td>Prompt for offline mode on startup</td>
<td>Ask to use the data source in offline mode when the user connects to the data source.</td>
</tr>
<tr>
<td>Allow beta database upgrade</td>
<td>Allow beta upgrade of the database (when using a beta version of Remote Desktop Manager).</td>
</tr>
<tr>
<td>Manage Cache</td>
<td>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.</td>
</tr>
<tr>
<td>More Settings</td>
<td>Edit the connection string values directly.</td>
</tr>
</tbody>
</table>
5.4.1.5.1 Configure SQL Server

**Description**

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

   ![Info icon]
   Newly installed Microsoft SQL Server instances do not allow remote connections. Please follow the directions in [SQL Server](https://support.microsoft.com/en-us/kb/316898).

   ![Info icon]
   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](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.
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.

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.
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.

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)](https://technet.microsoft.com).

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.

   ![Remote Desktop Manager - Microsoft SQL Server](image)

   - Caching mode: Intelligent
   - Connection timeout: 30 sec
   - Command timeout: 60 sec
   - Auto refresh: 0 sec
   - Prompt for offline mode on startup
   - Allow beta database upgrade

   ![More Settings](image)

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

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**

![MySQL - General Tab](image-url)
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the data source.</td>
</tr>
<tr>
<td>Host</td>
<td>Name of the server where the data source will be store.</td>
</tr>
<tr>
<td>Port</td>
<td>If not using the default port, enter your Port number.</td>
</tr>
<tr>
<td>Integrated Security</td>
<td>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 Integrated Security for more information.</td>
</tr>
<tr>
<td>Username</td>
<td>Username to access the MySQL server.</td>
</tr>
<tr>
<td>Password</td>
<td>Password to access the MySQL server.</td>
</tr>
<tr>
<td>Always ask password</td>
<td>Prompt for the password when a user connects to the data source.</td>
</tr>
<tr>
<td>Allow change username</td>
<td>Allow the username to be edited when connecting to the data source.   (Only with Always ask password enabled)</td>
</tr>
<tr>
<td>Schema</td>
<td>Name of the schema on the MySQL server for the utilization of Remote Desktop Manager.</td>
</tr>
<tr>
<td>Two factor</td>
<td>Enable the 2-Factor Authentication to access your data source.</td>
</tr>
<tr>
<td>Test Host</td>
<td>Test the connection with the Host (server) to validate if the proper information has been provided.</td>
</tr>
<tr>
<td>Test Schema</td>
<td>Test the connection with the schema to validate if the proper information has been provided.</td>
</tr>
</tbody>
</table>

**Private Vault**

[Remote Desktop Manager - MySQL](image)

ID: 6E3B2993-33CE-4C8D-86D1-66452FAB2C2AA

[MySQL - Private Vault Tab](image)
### OPTION | DESCRIPTION
--- | ---
**Type** | Select the type of [Private Vault](#) to use. Select between:
- **Default**: use the default Private Vault, which is stored in the database.
- **None**: disable the Private Vault for all users.
- **Online Drive**: use a Devolutions Online Drive file (*.dod) as a Private Vault.

---

**Upgrade**

![MySQL - Upgrade Tab](image)

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Host</td>
<td>Test the connection with the host (server) to validate if the proper information has been provided.</td>
</tr>
<tr>
<td>Create Schema</td>
<td>Create the schema on the MySQL server to use Remote Desktop Manager.</td>
</tr>
<tr>
<td>Update Schema</td>
<td>Update the schema on the MySQL server, if required, to use Remote Desktop Manager.</td>
</tr>
<tr>
<td>Test Schema</td>
<td>Test the connection with the schema to validate if the proper information has been provided.</td>
</tr>
<tr>
<td>Email Schema to Support</td>
<td>Send your schema to the Devolutions Support team.</td>
</tr>
<tr>
<td>View Upgrade Script</td>
<td>Open the upgrade script in a new window.</td>
</tr>
</tbody>
</table>
**VPN**

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

---

**Advanced**
### MySQL - Advanced Tab

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Caching mode</strong></td>
<td>Determine how the entries will be reload in the data source. See Caching topic for more information.</td>
</tr>
</tbody>
</table>
| **Ping online method**        | Indicate the preferred ping online method. Select between:  
- None  
- Ping  
- Port Scan |
| **Connection timeout**        | Waiting time before a connection timeout. |
| **Command timeout**           | Waiting time before a command timeout. |
| **Auto refresh**              | Set the interval for the automatic refresh |
| **Prompt for offline mode on startup** | Every time you will connect to your data source, you will be prompted to use the data source in offline mode. |
| **Auto go offline**           | If the ping online method doesn’t work it will automatically go offline. |
| **Disable lock**              | Disable the option to lock the data source directly. You can still lock the application but you won't be prompted for the database password if this option is disabled. |
| **More Settings**             | 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.

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.
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.

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

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.
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the data source.</td>
</tr>
</tbody>
</table>
| Mode                           | Select the mode that is preferred to configure the data source. Select between:  
|                                | Account                                  |
|                                | Local                                    |
| Local path (Local Mode)        | Contains the local path where the Dropbox files are accessible.                  |
| Email (Account Mode)           | Contains the email address associated with the Dropbox account.                  |
| Validate with Dropbox (Account Mode) | Button to validate the email address with the Dropbox account.               |
| Master key                     | Add an additional layer of security to your data source by using master key.    |
| Always ask master key          | Connecting to the data source will always prompt for the master key.            |
| Dropbox directory              | Indicate the folder in Dropbox. It should not contain any drive since it's stored online. Leave it empty to use the default Dropbox root. |
| Filename                        | Indicate the filename used to store the data on the data source.                |
| Compress database file         | Activate this option if you wish to compress your database file.                |

**VPN**

Open a VPN to access your data prior to connecting to your Dropbox.
Remote Desktop Manager

Advanced
### Dropbox - Advanced Tab

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

#### 5.4.3 Google Drive

**Description**

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

**General**
**Google Drive**

**General Tab**

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

**VPN**

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

Description

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

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

Please consult 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**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the data source.</td>
</tr>
<tr>
<td>Create a free account</td>
<td>Create a new Devolutions Cloud account.</td>
</tr>
<tr>
<td>Always ask password</td>
<td>Prompts for the password every time a connection to the Online Drive is attempted.</td>
</tr>
<tr>
<td>Test Connection</td>
<td>Test the connection with Devolutions Online Drive to validate the provided credentials.</td>
</tr>
<tr>
<td>Filename</td>
<td>Indicate the filename used to store the data on the Online Drive.</td>
</tr>
<tr>
<td>Master key</td>
<td>Contains a master key to access the data source.</td>
</tr>
<tr>
<td>Always ask master key</td>
<td>Ask for the master key every time a connection to the Online Drive is attempted.</td>
</tr>
</tbody>
</table>

**Backup**

Please consult the Online Backup topic for information on this service.
Devolutions Online Drive - Backup Tab

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

**VPN**
Open a VPN to access your data prior to connecting to your Devolutions Online Drive.
Advanced
### Devolutions Online Drive - Advanced Tab

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

#### 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 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.

Settings

General
## SQLite - General Tab

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

### Backup

© 2019 Devolutions inc.
### SQLite - Backup Tab

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Backup</strong></td>
<td>Select between:</td>
</tr>
<tr>
<td></td>
<td><strong>None</strong>: No backup of your data source will be created.</td>
</tr>
<tr>
<td></td>
<td><strong>File backup</strong>: Your backup will be saved to a chosen file but will not automatically do backup every 30 seconds.</td>
</tr>
<tr>
<td></td>
<td><strong>Online Backup</strong>: An Online Backup (using Online Backup) will automatically be created.</td>
</tr>
</tbody>
</table>

**VPN**

Open a VPN to access your data prior to connecting to your **SQLite**.
Advanced
### SQLite - Advanced Tab

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

### 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
### WebDAV - General Tab

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

### VPN

Open a VPN to access your data prior to connecting to your WebDAV.
Advanced
WebDAV - Advanced Tab

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto refresh</td>
<td>Set the interval for the automatic refresh.</td>
</tr>
<tr>
<td>Log enabled</td>
<td>Enables logging and its features.</td>
</tr>
</tbody>
</table>

5.4.7 XML

Description

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

Highlights

- This is a very simple data source and it can be modified or generated by an external tool.
- It is possible to configure an auto refresh interval.
- The Online Backup is available for this data source.

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

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

Settings
### General

#### XML - General Tab

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

### Backup
## XML - Backup Tab

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

### Backup name
Specify the backup name that will allow you to automatically save your sessions in a safe online storage space and restore them in the event of problems.

## VPN
Open a VPN to access your data prior to connecting to your XML.
Advanced
### XML - Advanced Tab

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

#### 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.
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

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

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).
**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

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>Prevent an offline cache from being used.</td>
</tr>
<tr>
<td>Intelligent</td>
<td>Use the offline cache only for recent changes.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>Prevents an offline cache from being used.</td>
</tr>
<tr>
<td>Read-only</td>
<td>Allow to view and use entries only. The content of the data source cannot be modified.</td>
</tr>
<tr>
<td>Read/Write</td>
<td>Allow to view, use, and edit entries. Conflicts caused by offline modifications are managed when back online.</td>
</tr>
</tbody>
</table>
Beyond the group policies, the Offline mode is controlled at four levels:

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

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

<table>
<thead>
<tr>
<th>USER PERMISSIONS</th>
<th>DATA SOURCE SETTINGS (SYSTEM SETTINGS)</th>
<th>DATA SOURCE CONFIGURATION</th>
<th>Vault CONFIGURATION</th>
<th>EFFECTIVE ACCESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled or Read-only or Read/write</td>
<td>Disabled or Read-only or Read/write</td>
<td>Disabled or Read-only or Read/write</td>
<td>Allow offline disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Disabled or Read-only or Read/write</td>
<td>Disabled or Read-only or Read/write</td>
<td>Disabled</td>
<td>Allow offline enabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Disabled or Read-only or Read/write</td>
<td>Disabled</td>
<td>Disabled or Read-only or Read/write</td>
<td>Allow offline enabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Disabled</td>
<td>Disabled or Read-only or Read/write</td>
<td>Disabled or Read-only or Read/write</td>
<td>Allow offline enabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Read-only or Read/write</td>
<td>Read-only or Read/write</td>
<td>Read-only or Read/write</td>
<td>Allow offline disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Read-only or Read/write</td>
<td>Read-only or Read/write</td>
<td>Read-only</td>
<td>Allow offline enabled</td>
<td>Read-only</td>
</tr>
<tr>
<td>Read-only or Read/write</td>
<td>Read-only</td>
<td>Read-only or Read/write</td>
<td>Allow offline enabled</td>
<td>Read-only</td>
</tr>
<tr>
<td>Read-only</td>
<td>Read-only or Read/write</td>
<td>Read-only or Read/write</td>
<td>Allow offline enabled</td>
<td>Read-only</td>
</tr>
<tr>
<td>Read/write</td>
<td>Read/write</td>
<td>Read/write</td>
<td>Allow offline enabled</td>
<td>Read/write</td>
</tr>
</tbody>
</table>

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](image)

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.

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

---

### 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.

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

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear output</td>
<td>Clear the output window.</td>
</tr>
<tr>
<td>Analyze</td>
<td>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.</td>
</tr>
<tr>
<td>Vacuum</td>
<td>This will run an SQLite command to reduce your cache size. The Vacuum should only be used after trying to execute a Repair of your cache. If the repair hasn't solved your issue running a Vacuum will usually solve issues when dealing with a corrupted cache.</td>
</tr>
<tr>
<td>Repair</td>
<td>The repair will run four different SQLite commands to repair a corrupted cache:</td>
</tr>
<tr>
<td></td>
<td>PRAGMA integrity_check</td>
</tr>
<tr>
<td></td>
<td>REINDEX DatabaseInfo</td>
</tr>
<tr>
<td></td>
<td>REINDEX Connections</td>
</tr>
<tr>
<td></td>
<td>REINDEX Properties</td>
</tr>
</tbody>
</table>

5.9 My Vault (Private)

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.
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.
Entries

Part VI
6 Entries

Every item you see in the navigation pane is an Entry. Create a new Entry from the ribbon by using the New Entry button in the Edit tab or by right clicking in the navigation pane and clicking on New Entry.

Entries come in various types and are described in the following sections:

- Session
- Information
- Contact
- Credential Entry
- Document
- Folder
- Synchronizer
- VPN
- Macros/Scripts/Tools
- Miscellaneous
6.1 Common Settings

Some settings are common to most entry types, meaning that they are almost the same for every entry. These options are on the side menu of the properties of entries.
For more information, please consult:

- General
- More
- Permissions
- Password Management
- Security Settings
- Session Recording
- VPN/SSH/Gateway
- User Interface
- Information
- Jump Host
- Events
- Logs
- Management Tools
- Advanced

### 6.1.1 General

**Description**

The General side menu contains general information about your entry.
## Settings

### DESCRIPTION

**Name**

Enter the name of the session that will be displayed in your treeview. This will be copied to the host field as its initial value as often the computer name is entered here and can be used directly.

**Folder**

Used to organize the session in different folders, either in the tray icon context menu or in the tree view. Learn more [here](#).

**Display**

Allows the session to be opened embedded in Remote Desktop Manager or externally. In the latter case, you may select the monitor on which it will be displayed (if the application and work setup permits it).

**Credentials**

Used to define the credential source:

- **Default**: Uses the username and password from the session type configuration.
- **Credential repository**: Links this session to an existing Credential repository entry. This is the solution that allows for reuse and lets you maintain the minimum number of entries whenever the credentials need updating.
- **Embedded**: Creates an embedded Credential repository entry. It will be stored within this session’s configuration.
- **Inherited**: This will use the credentials of the parent of the entry.
- **My personal credentials**: This setting will use your account-specific personal credentials. These can be setup in File – My Account Settings.
- **None**: This will setup the entry without credentials.
- **Private Vault search**: This will allow you to use credential entries currently located in your Private Vault.

### 6.1.2 More

**Description**
Description
Remote Desktop Manager supports three ways of describing entries:

- Text
- RTF
- URL

The description is displayed in a tooltip when hovering the described entry with the mouse in the tree view.

Tags
Add tags to use smart folders and saved searches.

Alternate host
Alternate Host handles changes in network topology. For example when having a laptop that is being used at home and at the office you may need to connect differently for each location, in those circumstances you can let the system detect how to connect.

Expiration
Enter a date to automatically change your entry Status to Expired and to get it listed in the Expired Session Report.
6.1.3 Permissions

Description

Access to entries is managed by permissions set on those entries. Combined together, permissions create a strong layer of security to prevent unwanted access by users of the data source. This system provide a large collection of permissions to choose from, providing great flexibility in access management.

Security Groups have been deprecated, but are still available for reference purposes. Do not use security groups and role-based access control at the same time.

Permissions

Possible values

There are four possible values that define how permissions are granted:

- **Inherited**: Inherit the permission from parent folders.
- **Custom**: Specify which users/roles that have permission. Click Select roles or users to define who has permissions.
- **Everyone**: Grant the permission to every user.
- **Never**: Block the permission for every user, except administrators.

For examples on using permissions, please consult the Role Based Security System topics.
Security Groups

Security groups are a legacy method of controlling access. We strongly recommend using the role-based access control instead.

Security groups were used to protect sessions from a subset of system users. Assign your entry to a security group then control who has access to it and how much control they have on the entry.

For more information please consult the Security Group Management topic.

6.1.4 Password Management

Description

The Password Management tab is used to manage multiple settings affecting the passwords of the entry, such as its complexity or pre-determined templates.
Password Template

The Password Template section let you build or select your preferred password limitations or basic necessities.

The Template settings include:

- **Default**: Currently, the default setting functions as None.
- **None**: There will be no restriction on passwords.
- **Inherited**: This inherits the settings from the data source configuration.
- **Custom**: Customize your password requirements by choosing minimum lengths or a number of symbols.
- **List**: With this, you can select from your currently available password template list.

Password Validation

The Password Validation has two different settings, Complexity and Pwned check.

**Complexity**

The Complexity settings dictates whether or not the Password Templates will be enforced. Its settings include:

- **Default**: Currently, the default setting functions as None.
- **None**: There will be no restriction on passwords.
- **Required**: The requirements set for the password validity will need to be met to proceed.
- **Warning**: The password will be accepted even if it does not meet the set requirements, but users will receive a warning nonetheless.
- **Inherited**: The setting will be inherited from the data source configuration.
Pwned Check
This setting is used to search for your inputted passwords within the Have I Been Pwned? resources.

- **Default**: Currently, the default setting functions as None.
- **None**: There will be no verification.
- **Enabled**: The verification will be done.
- **Inherited**: The setting will be inherited from the data source configuration.

### 6.1.5 Security Settings

**Description**

The **Security Settings** section is used to manage various settings regarding the edited entry.

![Common settings – Security Settings](image)
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checkout mode</td>
<td>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. For more information, please consult the Checkout system topic.</td>
</tr>
<tr>
<td>Checkout prompt</td>
<td>Prompt for a comment.</td>
</tr>
<tr>
<td>Allow offline</td>
<td>Select if an entry can be used offline. Select between:</td>
</tr>
<tr>
<td></td>
<td>- Root (refers to the data source configuration)</td>
</tr>
<tr>
<td></td>
<td>- True</td>
</tr>
<tr>
<td></td>
<td>- False</td>
</tr>
<tr>
<td></td>
<td>- Inherited</td>
</tr>
<tr>
<td>Time Based Usage</td>
<td>The Time-based usage allows to limit the usage of resources to specific times. This feature is useful to prevent unattended use of entries. Works with Advanced Data Sources.</td>
</tr>
<tr>
<td>Allow password in variable</td>
<td>Enable this setting for the $PASSWORD$ variable to be available with the command line.</td>
</tr>
</tbody>
</table>

### 6.1.5.1 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.
Checkout mode

Checkout mode enables or disables the checkout system. It also decides how the checkout mode functions.
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root</td>
<td>Inherits the checkout mode setting from the root folder.</td>
</tr>
<tr>
<td>Not available</td>
<td>Disables the checkout system.</td>
</tr>
<tr>
<td>Automatic</td>
<td>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.</td>
</tr>
<tr>
<td>Manual</td>
<td>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.</td>
</tr>
<tr>
<td>Inherited</td>
<td>Inherits the check out mode from the parent folder.</td>
</tr>
<tr>
<td>Optional</td>
<td>Offers the option to check out an entry manually or use (open and edit) the entry without checking it out.</td>
</tr>
</tbody>
</table>

**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.

![Remote Desktop Manager (Default)](image)

Checkout required

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

**Root setting**

The checkout system Root refer to the settings in the root folder.
To set the checkout system root settings:

1. Select the root folder in the **Navigation Pane**.

2. Click on the **Root Settings** button in the **Dashboard**.

3. In the root settings, navigate to the **Security** section.

### 6.1.6 Session Recording

The session recording feature records videos of opened sessions for auditing purpose.
This feature generates two files when recording a session. A video file and an information file.

### Session Recording Settings

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| **Mode** | Select how the feature is applied to the session. Select between:  
- **Default**: inherits the values from the root settings.  
- **Optional**: ask the user if they want to record the session at opening.  
- **Required**: record the session each time it is used.  
- **Never**: disable session recording for the current session.  
- **Inherited**: Retrieve the settings from parent folders. |
| **Destination** | Select a location to save the recording. |
| **Filename** | Select which name is applied to the recorded file. |

**6.1.7 VPN/SSH/Gateway**

**Description**

A VPN connection can be configured in the session properties, in the **VPN/SSH/Gateway** section. The connection can be established automatically, manually or when a specific condition is met.

Although you can configure a VPN details in session properties, it is best practice to link a session entry to a separate **VPN entry**. Please see, **Configure a VPN for multiple sessions** to learn more.
Each VPN type has its own set of properties to configure and you must know them in order to properly configure them. For more information about settings see the VPN entry topic.

**VPN Group**

Please consult VPN Group topic for more information.

**VPN Type**

Select which type of VPN you wish to configure inside your session. There are multiple natively supported VPN connection types and many more are available through add-ons. Please consult VPN Add-ons for more information.

**Installation Path**

You can manually configure your VPN installation path. To use the default installation path, leave the field empty.
Define the VPN settings in this tab. Enter the VPN name and credentials to properly connect to your VPN.

**VPN with Phonebook**
You can configure a **Phone book** with a **VPN** for a **RDP Entry**. This VPN entry can use the default Phone book, a specific Phone book, an embedded Phone book or a reference to a type of Phone book document.

This is only supported by the Microsoft VPN.

### 6.1.8 User Interface

**Description**

This section controls how your entry is displayed and what information is contained in it.

![Entries properties – User Interface section](image)

**Content**

- **Tab page**
- **Color**
- **Other**

**Tab Page**

**Tab group**

Tab group group tabs by user-defined categories.
Tab Page Section

Tab groups are displayed above the sessions' tabs.

Tab group location

Click on a tab group to filter the opened sessions and display only sessions from that group.

Tab groups – Filter on the Contact category

Much like the Folder feature, a hierarchical structure can be defined by entering a backslash to indicate a sub-level.
Tab group structure

You can also use left click to drag out the tab groups as a separate window.

Tab Page Title

Indicate a tab title to display instead of the name of the session. You can use a variable to add a prefix or a suffix.
Visibility

This setting is useful for VPN connections and entries that don't necessarily need interaction when opened. If the value is set to **False**, the session's tab is hidden when the session is opened.

To view hidden sessions in the Navigation Pane, select the view **Opened Sessions** tab and then select **Hidden Sessions**.
Keep tab page opened on disconnect
Enable this setting to keep the tab page opened when the application detects a closed connection. For more information, please consult Keep Tabs Opened for more information.

This setting can be changed in multiple sessions at the same time using the Batch Edit feature.

Color
It is possible to change the default color of the tab page to easily identify it.
### OPTION | DESCRIPTION
--- | ---
**Color** | Set the entry's tab page color.
**Fore color** | Set the foreground color of the name of the entry in the navigation pane.

The application colors the border of the embedded window along with the tab.

![Screenshot of the application interface showing various options and entries with colored tabs and icons.]

### Other

#### Other

- **Sort priority**: 0
- **Show in trayicon**: ✔️
- **Embedded footer visible**: ✗

[Sort priority default is 0 (use a higher value to place this item before other entries)]
### OPTION | DESCRIPTION
---|---
Sort priority | Set the number to a higher number to increase the sorting priority in the navigation pane.
Show in tray icon | Allow access to the entry from the tray icon.
Embedded footer visible | Display a footer under the session.

#### 6.1.9 Information

**Description**

The **Information** side menu contains general information regarding your computer, software, hardware, expiration warranty, etc...

![Image of Information side menu]

The various sections of this feature are mostly for you to input information regarding the entry’s specifics (usually the target host). The sections are divided as follows:

- **General**: Enter specific information regarding the computer, such as operating system, MAC address and hardware description. This will also enable certain actions within the dashboard, for example the Wake-on-LAN.
- **Software**: Here you can input a list all software installed on the remote computer as well as indicate the server roles.
- **Hardware**: Specify the hardware information of the remote computer.
- **Contact**: Enter contact information or link to a contact entry. It can be useful when managing a third party server.
- **Purchase**: Enter information related to the invoice or the purchase of the equipment.
- **Custom Fields**: Define custom properties and values that can then be access via variables ($CUSTOM_FIELD1$, $CUSTOM_FIELD2$, etc.) in child connections or Macros/Scripts/Tools. You
must be an administrator or have additional privileges to reveal password in order to view the protected values.

- **Statistics**: View who created or update the entry, as well as the date.

### 6.1.10 Jump Host

**Description**

Indicates if the entry is a Jump Host. Please consult our [Jump Online Help](#) for more details on Remote Desktop Manager Jump.

![Remote Desktop Manager Jump Host settings](image)

### 6.1.11 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.
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.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No script, command line or message prompt is executed.</td>
</tr>
<tr>
<td>Script</td>
<td>Select a script file to execute. The VBScript (*.vbs) file is the only supported format.</td>
</tr>
<tr>
<td>Command Line</td>
<td>Enter a command line to execute.</td>
</tr>
<tr>
<td>Message Prompt</td>
<td>Enter a message to display.</td>
</tr>
<tr>
<td>Macros/Scripts/Tools</td>
<td>Select a Macros/Scripts/Tools entry from the data source.</td>
</tr>
<tr>
<td>PowerShell</td>
<td>Select a PowerShell script from a local drive.</td>
</tr>
<tr>
<td>Copy to clipboard</td>
<td>Provide text to copy to the clipboard.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power On Mode</td>
<td>Enable the Wake-on-LAN.</td>
</tr>
<tr>
<td>Wait timeout</td>
<td>Enter the delay before retrying the to wake the remote device.</td>
</tr>
<tr>
<td>Retry count</td>
<td>Enter the number of time to try to wake the remote device.</td>
</tr>
</tbody>
</table>

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 \textit{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.

\textit{Be advised that using this feature in an environment where passwords must be hidden from the user is highly discouraged.}

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute automatically</td>
<td>Execute the macro automatically when the session is opened.</td>
</tr>
<tr>
<td>Initial wait</td>
<td>Enter the delay before the macro is executed.</td>
</tr>
<tr>
<td>Type</td>
<td>Select how the macro is executed. Select between:</td>
</tr>
<tr>
<td></td>
<td>\textbf{Default}: enter a typing macro manually.</td>
</tr>
<tr>
<td></td>
<td>\textbf{Link}: select an existing Macros/Scripts/Tools from the data source.</td>
</tr>
<tr>
<td>Typing macro</td>
<td>Enter the typing macro to execute. For more information, please consult the \textit{Typing Macro} topic.</td>
</tr>
<tr>
<td>Macro password</td>
<td>Enter a password to prompt for before executing the macro.</td>
</tr>
<tr>
<td>Delay time</td>
<td>Enter the delay time for the {DELAY} instruction.</td>
</tr>
<tr>
<td>Command</td>
<td>Enter the delay time between each command.</td>
</tr>
</tbody>
</table>

\subsection*{6.1.11.1 Typing Macro

\textbf{Description}

The \textit{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 \textit{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.

\textit{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.
<table>
<thead>
<tr>
<th>KEY</th>
<th>CODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>BACKSPACE</td>
<td>{BACKSPACE}, (BS), or {BKSP}</td>
</tr>
<tr>
<td>BREAK</td>
<td>{BREAK}</td>
</tr>
<tr>
<td>CAPS LOCK</td>
<td>{CAPSLOCK}</td>
</tr>
<tr>
<td>CTRL + ALT + DELETE</td>
<td>{CTRL-ALT-DEL}</td>
</tr>
<tr>
<td>DEL or DELETE</td>
<td>{DELETE} or {DEL}</td>
</tr>
<tr>
<td>DOWN ARROW</td>
<td>{DOWN}</td>
</tr>
<tr>
<td>END</td>
<td>{END}</td>
</tr>
<tr>
<td>ENTER</td>
<td>{ENTER}</td>
</tr>
<tr>
<td>ESC</td>
<td>{ESC}</td>
</tr>
<tr>
<td>HELP</td>
<td>{HELP}</td>
</tr>
<tr>
<td>HOME</td>
<td>{HOME}</td>
</tr>
<tr>
<td>INS or INSERT</td>
<td>{INSERT} or {INS}</td>
</tr>
<tr>
<td>LEFT ARROW</td>
<td>{LEFT}</td>
</tr>
<tr>
<td>NUM LOCK</td>
<td>{NUMLOCK}</td>
</tr>
<tr>
<td>PAGE DOWN</td>
<td>{PGDN}</td>
</tr>
<tr>
<td>PAGE UP</td>
<td>{PGUP}</td>
</tr>
<tr>
<td>PRINT SCREEN</td>
<td>{PRTSC}</td>
</tr>
<tr>
<td>RIGHT ARROW</td>
<td>{RIGHT}</td>
</tr>
<tr>
<td>SCROLL LOCK</td>
<td>{SCROLLLOCK}</td>
</tr>
<tr>
<td>TAB</td>
<td>{TAB}</td>
</tr>
<tr>
<td>UP ARROW</td>
<td>{UP}</td>
</tr>
<tr>
<td>F1</td>
<td>{F1}</td>
</tr>
<tr>
<td>F2</td>
<td>{F2}</td>
</tr>
<tr>
<td>F3</td>
<td>{F3}</td>
</tr>
<tr>
<td>F4</td>
<td>{F4}</td>
</tr>
<tr>
<td>F5</td>
<td>{F5}</td>
</tr>
<tr>
<td>F6</td>
<td>{F6}</td>
</tr>
<tr>
<td>F7</td>
<td>{F7}</td>
</tr>
<tr>
<td>F8</td>
<td>{F8}</td>
</tr>
<tr>
<td>F9</td>
<td>{F9}</td>
</tr>
<tr>
<td>F10</td>
<td>{F10}</td>
</tr>
<tr>
<td>F11</td>
<td>{F11}</td>
</tr>
<tr>
<td>F12</td>
<td>{F12}</td>
</tr>
<tr>
<td>F13</td>
<td>{F13}</td>
</tr>
<tr>
<td>F14</td>
<td>{F14}</td>
</tr>
<tr>
<td>F15</td>
<td>{F15}</td>
</tr>
<tr>
<td>F16</td>
<td>{F16}</td>
</tr>
<tr>
<td>Keypad add</td>
<td>{ADD}</td>
</tr>
<tr>
<td>Keypad subtract</td>
<td>{SUBTRACT}</td>
</tr>
<tr>
<td>Keypad multiply</td>
<td>{MULTIPLY}</td>
</tr>
<tr>
<td>Keypad divide</td>
<td>{DIVIDE}</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>KEY</th>
<th>CODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHIFT</td>
<td>+</td>
</tr>
<tr>
<td>CTRL</td>
<td>^</td>
</tr>
<tr>
<td>ALT</td>
<td>%</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>COMMANDS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>{DELAY}</td>
<td>This command introduces a delay of 300 ms (default value) before the next command.</td>
</tr>
<tr>
<td>{WINDOW:??}</td>
<td>This command focus a window containing the specified name after the semi colon.</td>
</tr>
<tr>
<td>{PREV-WINDOW}</td>
<td>Select the previous window before executing the remaining commands.</td>
</tr>
</tbody>
</table>

**Macro Password**

You can define a password to be use within the typing macro exclusively. Use the variable $MACRO_PASSWORD$ to access the password.

### 6.1.12 Logs

**Description**

- This feature requires an Advanced Data Source.
- When using a Devolutions Online Database data source, an Enterprise Subscription is required to have access to logging features.

The Logs section controls settings related to the logs of entries.
It also has a feature to warn you if you attempt to open a session, from the same data source, as another user. The application uses the logs to detect an open connection. Note that applications closed while being Offline will not register in the logs as closed, and must be manually closed with a right click.

There are also options to prompt for a comment, optional or required, when a session is opened or closed. **Prompt for comment on open** will also prompt for comments when a password is viewed or copied.

The **Warn if already opened** option is supported in Embedded (tabbed) display mode only. Both prompt for comments are supported in embedded and external display mode.

**Settings**

**Settings**
### OPTION | DESCRIPTION
---|---
**Warn if already opened** | Monitors all users of the current data source to verify if the session is already opened. This prevents "stealing" sessions from other users.

**Prompt for comment on open** | Prompt the user for a comment when launching the session and when viewing or copying the password. These comments are logged in the entry's logs.

**Open comment is required** | Forces the user to enter an Open session comment.

**Prompt for comment on close** | Prompt the user for a comment when closing the session. Close comments are logged in the entry's logs.

**Close comment is required** | Force the user to enter a Close session comment.

Right click on the log entry to display the contextual menu to show the log details. You can export the log or view more information about users.

Right-click on a log entry to display the Log Details contextual menu.

#### Log details contextual menu

- **Focus Session**
- **View Details**
- **View On Open Comment**
- **View On Close Comment**
- **Edit Notes...**
- **Flag as Closed**
- **Refresh**
- **Export to Csv...**
- **Export to Html...**
- **Export to Xls...**
- **Export to Xml...**

#### View Details window

The View Details window has three tabs: **General**, **Details** and **Comments**.

#### General Tab

The **General** tab displays session information to identify the entry and also displays the session running time. Notes can be entered using the contextual menu in the log entry grid.

#### Details tab
The Details tab displays information on the user and computer from which the session was started and on the destination host. It also displays information if the session was forcibly closed using the Close menu.

**Comments tab**

The Comments tab displays the On Open comment and On Close comment.

### 6.1.13 Management Tools

#### Description

The Management Tools tab allows you to configure different settings used by the Macros/Scripts/Tools including credentials when the remote credentials are required. It contains all of the authentication settings related to the session tools (e.g. Services, Wake-on-LAN, Shutdown Remote Computer, etc.) available in the application. For example it is used to execute a remote WMI query or a remote PowerShell script.

The applications available are:

- ControlUp
- IntelAMT
- Is Online (Ping/Port scan)
- Remote Desktop Commander
- Remote Management
- Home Page
- Remote Tools
- Spiceworks
- Wake-on-LAN

#### Settings

The settings depend on the tool selected.
## Credentials

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use default credentials</td>
<td>Use the default credentials. Please note that the application does not set</td>
</tr>
<tr>
<td></td>
<td>anything and assume that the current Windows user has all the privileges</td>
</tr>
<tr>
<td></td>
<td>required to execute the tool.</td>
</tr>
<tr>
<td>Use session credentials</td>
<td>Use the same credentials defined in the session directly or in the linked</td>
</tr>
<tr>
<td></td>
<td>credential entry.</td>
</tr>
<tr>
<td>Custom credentials</td>
<td>Use a specific username, password and domain.</td>
</tr>
<tr>
<td>Credential repository</td>
<td>Uses a linked Credential Entry which can also be an external credential like</td>
</tr>
<tr>
<td></td>
<td>KeePass. It is very useful for sharing or reusing credential among entries.</td>
</tr>
<tr>
<td>My personal credentials</td>
<td>Use one set of credentials to replace or emulate the ones from your Windows</td>
</tr>
<tr>
<td></td>
<td>session. See My Personal Credentials topic.</td>
</tr>
<tr>
<td>Prompt for credentials</td>
<td>Specify the credentials every time.</td>
</tr>
</tbody>
</table>

## Settings

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open VPN before execution</td>
<td>Specifies that the session defined VPN should be activated prior to running</td>
</tr>
<tr>
<td></td>
<td>the Macros/Scripts/Tools. The application will open it if it's not already</td>
</tr>
<tr>
<td></td>
<td>opened.</td>
</tr>
</tbody>
</table>
## 6.1.13.1 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.
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.
6.1.14 Advanced

Description
The **Advanced** tab contains settings such as the internal data source ID and session ID. These values can be used to invoke Remote Desktop Manager from a command line or even a web protocol handler.

**Settings**

**Miscellaneous**
### OPTION

**Override domain**
Allow you to override the domain when the credential are sent to the remote session. Select between:
- **Default**: Use the domain from the domain field in the session.
- **Use Host Name**: Use the host name (computer name) as the domain.
- **Custom Domain**: Use the domain in the Domain field from the Information section (in entry overview).
- **Use Domain from UPN**: Use the UPN's domain.

**Allow open multiple connections**
When a connection is already open and you reopen it, create a new instance instead of focusing on the other session.

**Username format**
Determines the username's format. Useful when connecting to remote systems that have a single field for the username but where you still need to send the domain name in order to authenticate. The possible values are:
- **No Change**: Does not change the username.
- **{Domain}\{User}**: Formats the username by prefixing with the domain name.
- **{User}@\Domain**: Formats the username by appending the domain name.
- **{User}**: Trims the domain to keep only the username.

**Custom host port**
With this you can input a customizable port for the host.

**Undock maximized**
Display mode undocked will be maximized when launched.

**Automatically close session after**
Check if you want your session to automatically close after a given number of minutes.

### IDs (Used in a Command line or in PowerShell scripts)

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database ID</td>
<td>Internal RDM database ID. Used as a Command Line Arguments or when using RDM PowerShell module.</td>
</tr>
<tr>
<td>Data Source ID</td>
<td>Internal RDM data source ID. Used as a Command Line Arguments or when using RDM PowerShell module.</td>
</tr>
<tr>
<td>Session ID</td>
<td>Internal RDM session ID. Used as Command Line Arguments or when using RDM PowerShell module.</td>
</tr>
<tr>
<td>Command line</td>
<td>Fully defined command line to start this session via a command line. Hit the copy button to copy the entire command line.</td>
</tr>
<tr>
<td>Create Desktop Shortcut</td>
<td>Automatically create a Remote Desktop Manager shortcut on your desktop.</td>
</tr>
<tr>
<td>Create web URL</td>
<td>Automatically create a web URL. Requires that the protocol handler has been registered by our installer.</td>
</tr>
<tr>
<td>Creation source</td>
<td>The creation source is used when deleting and moving entries using the Synchronizer.</td>
</tr>
</tbody>
</table>

### 6.2 Sessions

#### Description

Remote Desktop Manager separates the connection types in four different categories:
• General
• Remote connections
• Virtualization
• File Browser
• Other

**General**

This category contains the more popular and frequently used sessions.

**Remote Connections**

This category contains all of the remote connections types that are used to connect to remote systems, including computers, switches, VPNs, printers, etc.

**Virtualization**

This category contains all of the virtualization connections, including the local virtual machines tools and server tools. Remote Desktop Manager supports tools from Microsoft, VMware, Oracle and more.

**File Browser**

This category contains all the cloud file browser integrated in Remote Desktop Manager.

**Other**

This category contains many useful session types that are not directly supported, or those that are neither a virtualization nor a remote connection. For example we find the Command Line (External Application), the Inventory Report and the Play List session types in this group.

### 6.2.1 Open a Remote Connection

There are two ways of establishing a connection. It is possible to either:

- Add entries in the connection list.
- Use the Quick Connect feature.

Depending on the method, Remote Desktop Manager can use a completely different application or library. For example, the external mode for Remote Desktop uses the Microsoft Remote Desktop's client (mstsc.exe), and the embedded mode uses the Remote Desktop ActiveX control.

**Configured Connection**

There are many ways to open a session:

- Double-click the entry in the connection list.
- Press enter while the entry is selected.
- Use the context menu (right-click).
- Click Open Session on the Home tab (ribbon).
- Use the commands in the dashboard.
All entry types have a default action associated with them (e.g. Open, Navigate URL). These actions are executed when you use any means described above. The default action is often "Open", but you can modify it for certain entry types.

Remote Desktop Manager provides three display modes:

- **External**
- **Embedded (tabbed)**
- **Undocked**

Please note that **not** all sessions support the three modes. It depends on the integration and the availability of the third party application.

**External Mode**

With the External mode, the session is opened as an external process with no direct link to Remote Desktop Manager.

This display mode usually launches the native application. For example the native application for RDP is mstsc.exe. The external mode will automatically run on the Primary monitor. Depending on the type of session, an external mode session view will be updated if Remote Desktop Manager can detect that its running.

**Embedded (tabbed) Mode**

An embedded session runs within Remote Desktop Manager window and displays tabs at the top of the Dashboard. This mode centralizes the opened session in the application which makes it easy to switch from one to another.

There are several session-specific actions available by right clicking (Contextual Menu) on a tab title.
Web session opened in Embedded mode

Undocked

While the embedded mode is useful in some cases, you may prefer to move the content in an external window. If so, this can be easily done using the contextual menu. Remote Desktop Manager will create a new window to contain the tabbed session allowing you to move it anywhere else (i.e. on another screen).

To dock the content back to its original place, use the context menu by right clicking on the window icon.
Undocked mode supports different configurations for multiple monitor setups.

**Open with parameters**
You may specify different connection options when opening an entry. Click the arrow below **Open Session** on the **Home** tab or use the right-click context menu.

Examples of special actions:

- Open Full Screen.
- Embedded/External Display Mode.
- Console or admin mode with the RDP protocol.
- Force prompt for credentials.
- Open with or without the configured **VPN**.
- Open from a template.

### 6.2.2 Remote Connections

**Description**

This category contains all of the connection types that are used to connect to a remote system, including computers, switches, VPNs, printers, etc.
We support a very wide range of connections, ranging from Apple Remote Desktop, Web Browser (http/https), LogMeIn and much more. Explore to your heart's content!

### 6.2.2.1 Apple Remote Desktop

**Description**

This entry is used to define and configure an Apple Remote Desktop session.

- Remote management of macOS devices
- Embedded Mode
- Undocked Mode
- Supports Credential repository
- Show Opened Session
- Supports Logging

**Apple Remote Desktop** is our integration of the remote connection protocol created by Apple. This session allows to remotely control or monitor macOS devices.

**Settings**
## General

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Enter the host name or IP address of the remote device.</td>
</tr>
<tr>
<td>Ellipsis button</td>
<td>Provides the list of computers discovered on your network. This can take a few moments to generate.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port to access the remote computer. Set the value to 0 to use the default port.</td>
</tr>
<tr>
<td>Port generator</td>
<td>Click the icon to display the Port Generator.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username to connect to the remote computer.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password to connect to the remote computer.</td>
</tr>
<tr>
<td>View / Hide Password</td>
<td>Click the view icon to view your password. Click the hide icon to hide your password.</td>
</tr>
<tr>
<td>Password History</td>
<td>Click the icon to display the Password History.</td>
</tr>
<tr>
<td>Password Analyzer</td>
<td>Indicates the strength of the password.</td>
</tr>
</tbody>
</table>

## Settings
Apple Remote Desktop - Settings

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scaled</td>
<td>Scale the remote display to fit the window.</td>
</tr>
<tr>
<td>Screen</td>
<td>Select the screen where you want to display the remote connection. Select between:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default</strong>: Use the setting in <em>File – Options – Types – Others – Apple Remote Desktop (ARD)</em>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Primary</strong>: Display the primary screen.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Custom</strong>: Select which screen to display.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Prompt</strong>: Prompt at opening to select the remote display if there is more than one.</td>
</tr>
<tr>
<td>View only (input ignored)</td>
<td>Connect in view only mode. This option disables the keyboard and mouse while in session.</td>
</tr>
<tr>
<td>Request shared session</td>
<td>The remote user will be prompted with a request to share his session.</td>
</tr>
<tr>
<td>Disable clipboard transfer</td>
<td>Disable the clipboard sharing.</td>
</tr>
<tr>
<td>Authentication type</td>
<td>Select the authentication mode for the connection. Select between:</td>
</tr>
<tr>
<td></td>
<td>- <strong>ARD</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>ARD ask observe</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>ARD ask control</strong></td>
</tr>
</tbody>
</table>
### Apple Remote Desktop - Advanced

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| **Mouse cursor**              | Select the way the mouse cursor is handled. Select between:  
  - Track remote cursor locally  
  - Let remote server deal with mouse cursor  
  - Don’t show remote cursor |
| **Emulate 3 buttons (with 2-button click)** | Emulate mouse **button 3** when clicking on both **button 1** and **button 2**. |
| **Swap mouse buttons 2 and 3** | Invert mouse buttons 2 and 3. |
| **Apply Windows key combinations** | Select where the key combinations are sent. Select between:  
  - On the local computer  
  - On the remote computer  
  - In full screen mode only |
| **Keyboard layout**           | Select the keyboard layout. Select between:  
  - Azerty  
  - Qwerty |
| **Preferred encoding**        | Change the encoding to use less bandwidth. From the least to the most bandwidth used, select between:  
  - Zlib 16 gray (black and white)  
  - Zlib halftone (black and white)  
  - Zlib thousands (in color)  
  - Zlib (you can choose your custom compression level)  
  - Default (color) |
| **Custom compression level**  | Available only with the **Preferred encoding - Zlib** encoding. |


### BeyondTrust Password Safe Dashboard

**Description**
BeyondTrust Password Safe Dashboard connects to your BeyondTrust Password Safe account. You need to include the BeyondTrust API key in the entry properties.

This entry is used to define and configure a BeyondTrust Password Safe Console session. It supports the following:

- Credential repository
- Support Host
- Copy Password
- Show Opened Session
- Support Logging

**Settings**

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Enter the server name and port (ex: <a href="https://yourserver:8080">https://yourserver:8080</a>)</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username to connect on the server</td>
</tr>
<tr>
<td>Domain</td>
<td>Enter the domain to connect on the server</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password to connect on the server</td>
</tr>
<tr>
<td>Application API key</td>
<td>Enter the Application API key. Consult the section <em>How to obtain the Application API key</em> below to retrieve the Application Key.</td>
</tr>
</tbody>
</table>

**How to obtain the Application API key**

Connect on BeyondInsight, go in the Password Safe section and then go in Application API Registration.
6.2.2.3 FTP

Description

Remote Desktop Manager includes built-in FTP and SFTP entries. We also support Filezilla and WinSCP.

To set the default application for FTP (Third Party), go to File – Options – FTP. The choices are Windows Explorer, Filezilla or WinSCP.
6.2.2.4 Host

**Description**

This entry 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.

This entry is used to define and configure a Host session. It supports the following:

- Auto Login (embedded mode only)
- Copy Password
- Credential repository
- Embedded Mode
- External Mode
- Show Opened Session

Since no session can be established with simply a Host entry, this is mostly useful to either apply templates, or to serve as a parent for sub-connections. Please see Templates for more details.

**Settings**

**General**

<table>
<thead>
<tr>
<th>General</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Host icon]</td>
<td>![Use host from template]</td>
</tr>
</tbody>
</table>
| ![Use host from template] | ![...]
| ![Always prompt for host] | ![Use credentials from template] |
| ![Username] | ![Domain] |
| ![Password] | ![Show Password] |

**Host - General**
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use host from template</td>
<td>Use the template host (if using a template).</td>
</tr>
<tr>
<td>Host</td>
<td>Enter the hostname or IP address of the remote device.</td>
</tr>
<tr>
<td>Elipsis button</td>
<td>Provides the list of computers discovered on your network. This can take a few moments to generate.</td>
</tr>
<tr>
<td>Always prompt for host</td>
<td>Prompt you every time for the hostname or IP address.</td>
</tr>
<tr>
<td>Use credentials from template</td>
<td>Use the template credentials (if using a template).</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username that applies to the host.</td>
</tr>
<tr>
<td>Domain</td>
<td>Enter the domain that applies to the host.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password that applies to the Host.</td>
</tr>
<tr>
<td>View / Hide Password</td>
<td>Click on the view icon to view your password. Click on the hide icon to hide your password.</td>
</tr>
<tr>
<td>Password History</td>
<td>Click the icon to display the Password History.</td>
</tr>
<tr>
<td>Password Analyzer</td>
<td>Indicates the strength of the password.</td>
</tr>
</tbody>
</table>

**Advanced**

The template selected is the one executed when either pressing enter, double-clicking or by using the Open Session command.
6.2.2.5 LogMeIn

**Description**

LogMeIn remote access products use a proprietary remote desktop protocol that is transmitted via SSL. An SSL certificate is created for each remote desktop, and is used to cryptographically secure communications between the remote desktop and the accessing computer. You can find more information [here](#).

This entry is used to define and configure a LogMeIn session. It supports the following:

- Auto Login
- Credential repository
- Show Opened Session
- Built in
- Embedded Mode
- Support Logging
- Copy Password
- External Mode
- Support Reconnect

Users access remote desktops using an Internet-based web portal and, optionally, the LogMeIn Ignition stand-alone application. The portal also provides status information for the remote computers and, optionally, remote computer management functions.

**Automatic Login**

You have two modes available to achieve the Auto Login in embedded view.

- [LogMeIn Desktop shortcut](#) (LogMeIn Pro only)
- [LogMeIn portal](#) with auto login (works with any LogMeIn account)

**Settings**

**General**
### LogMeIn - General

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hide navigation bar</td>
<td>Hide LogMeIn navigation bar.</td>
</tr>
<tr>
<td>Sandbox process</td>
<td>Enable the use of sandbox (computer security) process.</td>
</tr>
<tr>
<td>Auto submit</td>
<td>Enable the Auto-submit of the credentials.</td>
</tr>
<tr>
<td>Hide script errors</td>
<td>Hide script errors that can be present in some websites.</td>
</tr>
</tbody>
</table>

### Login

#### Host Login

- **Username**
- **Password**

#### Portal Login

- **Credentials**
- **Email**
- **Password**
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Login - Username</td>
<td>Enter your Host username.</td>
</tr>
<tr>
<td>Host Login - Password</td>
<td>Enter your Host password.</td>
</tr>
<tr>
<td>Portal Login - Credentials</td>
<td>Use the various credential features provided by RDM to set your credentials.</td>
</tr>
<tr>
<td>Portal Login - Email</td>
<td>Enter your LogMeIn account email address.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter your LogMeIn account password.</td>
</tr>
</tbody>
</table>

6.2.2.5.1 Desktop Shortcut

Description

Note: as stated on the LogMeIn web site (LogMeIn), Desktop Shortcut is a Pro Edition feature.

1. Log in to the LogMeIn website.
2. Select the desired computer.
3. Select the option Settings.
4. Select the tab "Desktop Shortcut".
5. Drag and drop the computer icon in Remote Desktop Manager.

6.2.2.5.2 Portal (Host Url)

Description

This connection method can be used with all versions of LogMeIn. This method requires the session to run Embedded and the use of Internet Explorer.
If you are using Internet Explorer 11, you need to change the IE emulation mode to Internet Explorer 10. Please consult the LogMeIn troubleshooting topic for more information on how to proceed.

**Settings**

1. Log in to the LogMeIn website.
2. Right-Click the URL shortcut of the computer and use the copy command.

3. Paste the information in the LogMeIn portal (host URL) field
4. In the **Login** tab populate both **Portal Login** and **Host Login** information
6.2.6  Microsoft Remote Desktop (RDP)

**Description**

This entry is used to define and configure a Microsoft Remote Desktop (RDP) session.

- Auto Login
- Credential repository
- Full Screen
- Show Opened Session
- Support Reconnect
- Built in
- Embedded Mode
- Support Host
- Support BeforeDisconnectEvent
- Support AfterDisconnectEvent
- Copy Password
- External Mode
- Multi Monitor Support
- Support Logging
- Batch Edit

**Settings**

**General**

![Microsoft Remote Desktop (RDP) - General](image)

Host

RDP type: Normal

Username

Domain

Password

Always ask password

Store password locally

Save Password

Open console (Admin mode)
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Enter the host name or IP address of the remote computer.</td>
</tr>
<tr>
<td>Ellipsis button</td>
<td>Provides the list of computers discovered on your network. This can take a few moments to generate.</td>
</tr>
<tr>
<td>Port</td>
<td>Click on the link to modify the port number. Set the port to 0 to use the default port.</td>
</tr>
<tr>
<td>Port generator</td>
<td>Click on the icon to display the Port Generator.</td>
</tr>
<tr>
<td>RDP Type</td>
<td>Select the RDP session type. Select between:</td>
</tr>
<tr>
<td></td>
<td>· Normal</td>
</tr>
<tr>
<td></td>
<td>· Azure</td>
</tr>
<tr>
<td></td>
<td>· Hyper-V (embedded only)</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username to connect to the remote computer.</td>
</tr>
<tr>
<td>Domain</td>
<td>Enter the domain to connect to the remote computer.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password to connect to the remote computer.</td>
</tr>
<tr>
<td>Password Analyzer</td>
<td>Indicates the strength of the password.</td>
</tr>
<tr>
<td>View / Hide Password</td>
<td>Click on the view icon to view your password. Click on the hide icon to hide your password.</td>
</tr>
<tr>
<td>Password Generator</td>
<td>Click on the icon to display the Password Generator.</td>
</tr>
<tr>
<td>Password History</td>
<td>Click on the icon to display the Password History.</td>
</tr>
<tr>
<td>Always ask password</td>
<td>Always ask password when connecting to the remote computer.</td>
</tr>
<tr>
<td>Store password locally</td>
<td>Use the Windows Credential Manager to store passwords. It is not the best option because it has the following limitations:</td>
</tr>
<tr>
<td></td>
<td>· The Credential Manager will hold only one entry per host, therefore if you have multiple sessions towards the same host, the last saved entry will overwrite whatever was stored.</td>
</tr>
<tr>
<td></td>
<td>· The one host limitation ignores the port, therefore multiple sessions towards the same host, but with different ports, will conflict as well. Last saved entry overrides whatever was stored.</td>
</tr>
<tr>
<td>Open console (Admin mode)</td>
<td>Connect to the console session of a server using Remote Desktop for Administration. Normally required for TS Session Hosts only, please consult <strong>Note 1</strong>.</td>
</tr>
</tbody>
</table>

**Display**
### Microsoft Remote Desktop (RDP) - Display

**OPTION** | **DESCRIPTION**
--- | ---
**Screen sizing mode** | Scale the client window display of the desktop when resizing between:
- Scrollbar.
- Smart reconnect (reconnect the session when the window size changes).
- Smart sizing (stretch the remote display to fit the window).
**Remote Desktop Size** | Select the screen size for the remote computer.
**Custom width** | Specify a custom width number for the screen size.
**Custom height** | Specify a custom height number for the screen size.
**Colors** | Select the color quality when connected on the remote computer.
**Display the connection bar when in full screen mode** | Display the connection bar at the top of your screen in full screen size mode.
**Connection bar pinned (full screen)** | Fix the connection bar at the top of the screen.

### Local Resources
Remote Computer Sound
- Bring to this computer
- Remote audio recording
- Do not record

Keyboard
- Apply Windows key combinations (for example ALT+TAB)
- On the local computer
- Keyboard layout: Default

Local Devices and Resources
- Select the devices and the resources you want to use in your remote session
- Printers
- Serial ports
- Hard drives
- Clipboard
- Prompt for selected resources
- Other supported Plug and Play (PnP) devices
- Smart cards
- All drives
- Specific drives
- More
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Remote computer sound       | Indicate what to do with the sound on the remote computer. Select between:  
  - Bring to this computer  
  - Do not play             
  - Leave at remote computer |
| Remote audio recording      | Indicate what to do with the audio recording on the remote computer. Select between:  
  - Do not record           
  - Record from this computer |
| Keyboard                    | Specify how key combination should be executed. Select between:  
  - On the local computer   
  - On the remote computer  
  - In full screen mode only |
| Local devices and resources | Select the devices and resources that you wish to use on the remote computer. Select between:  
  - Printers                
  - Serial Ports            
  - Hard drives             
  - Clipboard               
  - Prompt for selected resources (Only available in external mode)  
  - Other supported Plug and Play (PnP) devices  
  - Smart cards             |
| All drives                  | Select this option if you want all of your drives to be present on the remote computer. |
| Specific drives             | Select one or more specific drive that you want to be present on the remote computer. |

Programs
## Microsoft Remote Desktop (RDP) - Programs

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start the following program on connection (alternate shell)</td>
<td>Enable to specify a program to launch on the remote computer when the connection is established.</td>
</tr>
<tr>
<td>Program path and filename</td>
<td>Specify the program path and filename to start when the connection is established.</td>
</tr>
<tr>
<td>Start in the following folder</td>
<td>Specify the working folder used by the program in the previous step.</td>
</tr>
<tr>
<td>Use RemoteApp (seamless mode)</td>
<td>Open an rdp connection, starts a specified program, maximizes the application window and runs without the windows desktop.</td>
</tr>
<tr>
<td>Program</td>
<td>Specify the program for the RemoteApp.</td>
</tr>
<tr>
<td>Parameters</td>
<td>Specify the parameters for the RemoteApp.</td>
</tr>
<tr>
<td>Execute the following program after login</td>
<td>Enable if you wish to automatically run a program immediately after login.</td>
</tr>
</tbody>
</table>

### Experience
### Microsoft Remote Desktop (RDP) - Experience

<table>
<thead>
<tr>
<th>Performance Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Choose the connection speed to optimize performance</strong></td>
</tr>
<tr>
<td><strong>Default</strong></td>
</tr>
</tbody>
</table>

**Allow the following**

- Desktop background
- Redirect DirectX
- Font smoothing
- Redirect video playback
- Desktop composition
- Enable data compression
- Show window contents while dragging
- Menu and window animation
- Load plug-ins in embedded mode: Default
- Reconnect if connection is dropped
- Detect network automatically
- Cache: Default
- Persistent bitmap caching
- Keep alive: 0 sec
- Detect bandwidth automatically
- Visual styles
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose the connection speed to optimize performance</td>
<td>Specify the connection speed to use to optimize the remote session performance. Select between:</td>
</tr>
<tr>
<td></td>
<td>- Default</td>
</tr>
<tr>
<td></td>
<td>- Modem (56 kbps)</td>
</tr>
<tr>
<td></td>
<td>- Low-speed broadcast (256 kbps - 2 Mbps)</td>
</tr>
<tr>
<td></td>
<td>- Satellite (2-16 Mbps with high latency)</td>
</tr>
<tr>
<td></td>
<td>- High-speed broadcast (2-10 Mbps)</td>
</tr>
<tr>
<td></td>
<td>- WAN (&gt;10 Mbps with high latency)</td>
</tr>
<tr>
<td></td>
<td>- LAN (&gt;10 Mbps with low latency)</td>
</tr>
<tr>
<td>Allow the following</td>
<td>Enable the following features on the remote computer:</td>
</tr>
<tr>
<td></td>
<td>- Desktop background</td>
</tr>
<tr>
<td></td>
<td>- Font smoothing</td>
</tr>
<tr>
<td></td>
<td>- Desktop composition</td>
</tr>
<tr>
<td></td>
<td>- Show window contents while dragging</td>
</tr>
<tr>
<td></td>
<td>- Menu and window animation</td>
</tr>
<tr>
<td></td>
<td>- Visual styles</td>
</tr>
<tr>
<td></td>
<td>- Persistent bitmap caching</td>
</tr>
<tr>
<td></td>
<td>- Redirect DirectX</td>
</tr>
<tr>
<td></td>
<td>- Redirect video playback</td>
</tr>
<tr>
<td></td>
<td>- Load plug-ins in embedded mode</td>
</tr>
<tr>
<td></td>
<td>- Enable data compression</td>
</tr>
<tr>
<td></td>
<td>- Detect network automatically</td>
</tr>
<tr>
<td></td>
<td>- Detect bandwidth automatically</td>
</tr>
<tr>
<td></td>
<td>- Reconnect if connection is dropped</td>
</tr>
<tr>
<td>Cache</td>
<td>Select the type of cache that will be used for the remote session:</td>
</tr>
<tr>
<td></td>
<td>- Default: Use the value set in File → Options → Type → RDP → Cache.</td>
</tr>
<tr>
<td></td>
<td>- Full mode: This protocol is full Windows 8 Remote Desktop protocol.</td>
</tr>
<tr>
<td></td>
<td>- Thin client: This protocol is limited to using the Windows 7 with SP1 RemoteFX codec and a smaller cache. All other codecs are disabled. This protocol has the smallest memory footprint.</td>
</tr>
<tr>
<td></td>
<td>- Small cache: This protocol is the same as Full mode, except it uses a smaller cache.</td>
</tr>
<tr>
<td>Keep alive</td>
<td>Data will be sent to the remote computer to keep the session alive. You can determinate the time between that and when the data is send. This option is only available in embedded mode.</td>
</tr>
</tbody>
</table>
Microsoft Remote Desktop (RDP) - Connection

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

- Do not use RD Gateway server
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Server authentication verifies that you are connecting to the intended remote computer | If the actual verification does not meet minimum policy requirements, select what needs to be done by the remote computer between the following:  
- Connect and don't warn me  
- Do not connect  
- Warn me |
| Activate network level authentication (SingleSignOn) | Network Level Authentication completes user authentication before you establish a remote session and the logon screen appears. This is a more secure authentication method. |
| Automatically detect RD Gateway server settings | The RD Gateway server settings will be detected by the application automatically. |
| Use these RD Gateway server settings | Indicate the specific settings to connect on the RD Gateway server. |
| Host | Enter the RD Gateway server/host name. |
| Logon method | Select the logon method between:  
- Ask for password (NTLM)  
- Smart card  
- Allow me to select later  
- Use a gateway access token |
| Gateway access token | Provide the access token if the Logon method is set to Use a gateway access token. |
| Open gateway only when unable to ping host | Establish a connection with the RD Gateway server only when it is not possible to ping the remote computer. |
| Bypass RD Gateway server for local addresses | Bypass the RD Gateway server when connecting on a remote computer who has a local IP address. |
| Use same RD Gateway credentials as remote computer | Use your personal RD Gateway credentials to connect on the remote computer. |
| Credentials | See RDP Gateway credentials section below. |
| Do not use RD Gateway server | Don’t use any RD Gateway server to connect on the remote computer. |

**RDP Gateway credentials**
Microsoft Remote Desktop (RDP) - Gateway Credentials
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use custom credentials</td>
<td>Use a specific username, domain and store the password on the local computer or store the password in the database.</td>
</tr>
<tr>
<td>Store password on the local computer</td>
<td>This will use the Windows Credential Manager. It is not the best option because it has the following limitations:</td>
</tr>
<tr>
<td></td>
<td>• The Credential Manager will hold only one entry per host, therefore if you have multiple sessions towards the same host, the last saved entry will overwrite whatever was stored.</td>
</tr>
<tr>
<td></td>
<td>• The one host limitation ignores the port, therefore multiple sessions towards the same host, but with different ports, will conflict as well. Last saved entry overrides whatever was stored.</td>
</tr>
<tr>
<td>Store password in the database</td>
<td>The password will be store in the database.</td>
</tr>
<tr>
<td>Domain</td>
<td>Set the domain name.</td>
</tr>
<tr>
<td>Use Credential repository</td>
<td>Use a linked credential entry.</td>
</tr>
<tr>
<td>Inherited</td>
<td>Use inherited credentials.</td>
</tr>
<tr>
<td>Use my personal credentials</td>
<td>Use the credentials stored in My Personal Credentials.</td>
</tr>
<tr>
<td>Use Private Vault search</td>
<td>Use the Search string to search for credential entries in the Private Vault.</td>
</tr>
</tbody>
</table>

### Advanced

**Enable CredSSP support**
- Default

**Log off mode**
- Default

**Automatically logoff when disconnecting**
- Default

**Reconnect mode**
- Standard

**RDP Version**
- Latest

**Minimal input send interval**
- 100 ms

**Restricted admin mode**

**Background input**

**Enable super user**

**Public mode**

**Workspace ID**

**Alternate full address**

**Load balance info**

---

Microsoft Remote Desktop - (RDP) - Advanced
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable CredSSP support</td>
<td>RDP will use the Credential Security Support Provider (CredSSP) for the authentication on the remote computer. Select between:</td>
</tr>
<tr>
<td>Log off mode</td>
<td>Select the log off method between:</td>
</tr>
<tr>
<td></td>
<td>· Default</td>
</tr>
<tr>
<td></td>
<td>· Automatic</td>
</tr>
<tr>
<td></td>
<td>· RDM Agent</td>
</tr>
<tr>
<td></td>
<td>· Remote Desktop Services API</td>
</tr>
<tr>
<td></td>
<td>· Macro</td>
</tr>
<tr>
<td>Automatically logoff when disconnecting</td>
<td>Automatically log off your RDP session when disconnecting.</td>
</tr>
<tr>
<td>Reconnect mode</td>
<td>Select the reconnect behavior. Select between:</td>
</tr>
<tr>
<td></td>
<td>· Default</td>
</tr>
<tr>
<td></td>
<td>· Full</td>
</tr>
<tr>
<td></td>
<td>· Smart reconnect</td>
</tr>
<tr>
<td></td>
<td>· Legacy</td>
</tr>
<tr>
<td>Minimal input send interval</td>
<td>Set the minimum time in milliseconds between the input is send to the remote computer.</td>
</tr>
<tr>
<td>Background input</td>
<td>The remote computer can accept input even when the focus is not on the session.</td>
</tr>
<tr>
<td>Restriected admin mode</td>
<td>This enables the restricted admin mode.</td>
</tr>
<tr>
<td>Enable super pan</td>
<td>Enabling super pan will take the entirety of your screen for the RDM session.</td>
</tr>
<tr>
<td>Prompt for credentials on client</td>
<td>Always prompt for credentials when launching client.</td>
</tr>
<tr>
<td>Public mode</td>
<td>Public mode is a security feature that limits the security information stored on the remote station. It also limits the amount of time this information can be stored.</td>
</tr>
<tr>
<td>Workspace ID</td>
<td>Enter the Workspace ID that contain the setting associate to the RemoteApp and Desktop ID.</td>
</tr>
<tr>
<td>Use redirection server</td>
<td>Redirect a remote computer to the RDP session host.</td>
</tr>
<tr>
<td>Alternate full address</td>
<td>Indicate an alternate name of the remote computer that you want to connect on.</td>
</tr>
<tr>
<td>Load balance info</td>
<td>Indicate the load balance info when the load balancing feature is enable on the RD Connection Broker.</td>
</tr>
</tbody>
</table>

**Note 1**

As per knowledge base article 947723, since rdp 6.1 (Windows 2008), using the admin mode is not necessary except when the server itself is a RD Session Host.

**6.2.2.6.1 Azure RDP**

**Overview**

**Azure RDP** is a Windows Remote Desktop session directly into an Azure role instance without having to use the Azure Management Console ([https://azure.microsoft.com/en-us/](https://azure.microsoft.com/en-us/)).
Settings

1. Enable Azure RDP access by following these instructions:

2. Open the Azure Portal ([https://portal.azure.com](https://portal.azure.com)) and select the deployment you would like to connect to. You’ll need the DNS name (Computer), Role Name & Role IDs.

![Azure Portal](image)

3. Create a new RDP session with the following values:

   **Host:** Azure DNS  
   **Role Name:** Azure role name  
   **ID:** The azure role ID (if you have 8 instances running, then 0 - 7 are the IDs)
6.2.2.6.2 Hyper-V RDP

Description

You can connect to a Hyper-V instance using RDP through the Hyper-V server. There is no need to enable RDP on the Hyper-V instance, because Remote Desktop Manager features two levels of authentication.

- Auto login to the Hyper-V instance is not supported.
- The credentials provided are for the Hyper-V server (not the instance).

Settings
Create a new RDP session on the Hyper-V server. Input your login credentials prior to selecting the Hyper-V instance.

The Hyper-V enhanced sessions mode is supported in Remote Desktop Manager.

The Hyper-V session support the Hyper-V v2 with a Windows Server 2012 R2 destination.

**Enhanced Session mode**

Enhanced session mode allows redirection of local devices and resources from computers running Virtual Machine Connection.

Enhanced session mode provides the following capabilities:

- Display Configuration
- Audio redirection
- Printer redirection
- Full clipboard support (improved over limited prior-generation clipboard support)
- Smart Card support
- USB Device redirection
- Drive redirection
Remote Desktop Manager

- Redirection for supported Plug and Play devices

You don’t need a network connection to the Virtual Machine session like you would with RDP.

**Troubleshooting**


### 6.2.2.7 PowerShell Remote Console

**Description**

This entry is used to define and configure a *PowerShell Remote Console* session.

The *PowerShell Remote Console* performs PowerShell operations on a remote device.

**Settings**


**General**

![PowerShell Remote Console - General](image)

Type: Computer name

Host

Port: Default

Configuration

Username

Domain

Password

© 2019 Devolutions inc.
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Type       | Select the type of connection. Select between:  
  · Computer name  
  · Connection uri  
  · VM name  
  · VM Id |
| Host       | Enter the host name or IP address of the remote device. |
| Ellipsis button | Provides the list of computers discovered on your network. This can take a few moments to generate. |
| Port       | Enter the port to access the remote computer. Set the port to 0 to use the default port. |
| Port generator | Clicking on the icon to display the Port Generator. |
| Use SSL    | Secure the connection with SSL encryption (https). |
| Configuration | Enter the PowerShell session configuration name. |
| Username   | Enter the username of the remote device. |
| Domain     | Enter the domain of the remote device. |
| Password   | Enter the password of the remote device. |
| View / Hide Password | Click on the view icon to view your password. Click on the hide icon to hide your password. |
| Password Generator | Click on the icon to display the Password Generator. |
| Password History | Click on the icon to display the Password History. |
| Password Analyzer | Indicates the strength of the password. |

**Run As**

![PowerShell Remote Console - Run As](image-url)
### OPTION | DESCRIPTION
--- | ---
None | Turns off the Run As function.
Current session | Use the credential provided under the General tab.
Custom | Use custom Username, Password and Domain.
Credential repository | Select an existing credential entry with the combo box or the ellipsis button.
My personal credentials | Retrieve the credentials from My Personal Credentials. Click on the ellipsis button to edit your personal credentials.

**Advanced**

![PowerShell Remote Console - Advanced](image)

### OPTION | DESCRIPTION
--- | ---
Other parameters | Enter additional parameters you wish to use.
PowerShell version | Select the PowerShell version to use. Select between:
- Default (Current Version)
- Version 2
Resize window | Force window resize (buffer & window).
Run as Administrator | Run PowerShell command as an administrator.
Run in 64-bit mode | Run RDM CmdLet in 64 bits version.
Single thread apartment | Starts Windows PowerShell using a single-threaded apartment.

#### 6.2.2.8 ScreenConnect

**Description**

ScreenConnect offers lightning-fast remote support and remote access to connect and solve problems faster.
This entry is used to define and configure a ScreenConnect session.

- Auto Login
- Copy Password
- Show Opened Session
- External Mode
- Show Opened Session
- Support Logging

Consult the How-to Configure ScreenConnect 5 in Remote Desktop Manager topic if you want to configure a ScreenConnect 5 session.

To use version 2.3 of the ScreenConnect extension, you must have Remote Desktop Manager version 13.5.5.0 or above.

Settings

General
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Enter the name or IP address of the ScreenConnect server. You also need to specify the port.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username of the ScreenConnect server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password of the ScreenConnect server.</td>
</tr>
<tr>
<td>Password Analyzer</td>
<td>Indicates the strength of the password.</td>
</tr>
<tr>
<td>Always ask password</td>
<td>Always ask password when connecting to ScreenConnect server.</td>
</tr>
<tr>
<td>Use One Time Password</td>
<td>Uses the OTP setting.</td>
</tr>
<tr>
<td>Session name</td>
<td>Select or enter the machine name or session name to connect.</td>
</tr>
<tr>
<td>Always prompt for session name</td>
<td>With this option the system will ask you which session you wish to start each time you open the session.</td>
</tr>
<tr>
<td>Use session name as filter</td>
<td>Use the session name as a filter to reduce choices.</td>
</tr>
</tbody>
</table>
| Connection type     | Specify the connection type. Select between:  
  - Guest  
  - Host |
| Auto create         | If the sessions doesn’t exist it will be created with these settings. |
| Session group       | Specify the session group. Select between:  
  - User Sessions  
  - Meetings |
| Session type        | Specify the session type. Select between:  
  - Published  
  - Secure Code  
  - On invitation only |
| Secure code         | Specify the secure code to use. Only available when the Session Code session type is selected. |

**Invitation Emails**
Screenconnect - Invitation emails

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invitation Emails</td>
<td>An invitation email will be sent at the session opening for each email in the list. One email per line needs to be enter.</td>
</tr>
</tbody>
</table>

**Advanced**

Screenconnect - Advanced

User display name change is only available starting from ScreenConnect 6.6 using the V2.2 extension
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Select the version of ScreenConnect that you want to use in the application.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: Use the default version of ScreenConnect that you have set in <em>File - Options - Types - ScreenConnect</em>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Version 4.x and lower</strong>: Use the version 4 and lower of ScreenConnect.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Extension (Version 5 or higher)</strong>: You need to install the extension from the ScreenConnect browser extension to use this version of ScreenConnect.</td>
</tr>
<tr>
<td>User display name</td>
<td>With this setting you can decide whether you want to display your windows username or data source username.</td>
</tr>
</tbody>
</table>

### 6.2.2.9 Spiceworks

**Description**

This entry is used to define and configure a _Spiceworks_ session. At this time, it is simply a wrapper to open the dashboard, submit your credentials, and optionally focus to a group or a device.

**Settings**

![Spiceworks General Tab](spiceworks_general_tab.png)

*Spiceworks - General Tab*
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spiceworks host</td>
<td>Enter the URL of the Spiceworks server. Ensure that the protocol and port are specified. i.e. <a href="http://spiceworks:9675">http://spiceworks:9675</a></td>
</tr>
<tr>
<td>Email</td>
<td>Email address used as account identifier on Spiceworks services.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password to access the Spicework Host.</td>
</tr>
<tr>
<td>Web browser</td>
<td>Select the web browser to use.</td>
</tr>
</tbody>
</table>
| Mode              | Select between the following modes:  
  - Dashboard  
  - Group  
  - Help Desk |

**Usage**

Specify the server URL and enter valid credentials. By default, the dashboard view will be shown after the credentials have been submitted and accepted.

You can elect to show directly a specific group by choosing the **group** option, then using the ellipsis to select the specific group to display.

You must have the required permissions to view groups to use the **group** link feature.

You can alternatively elect to display a specific device by choosing the **device** option, then using the ellipsis to select the specific device to display.

You must have the required permissions to view the devices to use the **device** link feature.

**6.2.2.10 Telnet**

**Description**

**Telnet** is a network protocol used to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection.

This entry is used to define and configure a **Telnet** session.

- Embedded Mode  
- Show Opened Session  
- External Mode  
- Support Logging  
- Credential repository
### Telnet - General

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Enter your Telnet remote host name to connect.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port to connect to the remote host.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter your account username.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter your account password.</td>
</tr>
<tr>
<td>Always ask password</td>
<td>Always ask password when connecting to the session.</td>
</tr>
<tr>
<td>User prompt string</td>
<td>Type down a string for user prompt.</td>
</tr>
<tr>
<td>Password prompt string</td>
<td>Type down a string for password prompt.</td>
</tr>
<tr>
<td>Delay</td>
<td>Set active delay between actions on connection.</td>
</tr>
</tbody>
</table>

### Post Login
### Telnet - Post Login

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automatic (ENTER) after command</strong></td>
<td>Emulates the keystroke (ENTER) automatically between commands, use with delay for best result.</td>
</tr>
<tr>
<td><strong>Delay</strong></td>
<td>Delay between commands.</td>
</tr>
<tr>
<td><strong>Commands</strong></td>
<td>Set up commands to send.</td>
</tr>
</tbody>
</table>

#### Proxy
Proxy type: Socks4

Credential repository

Host

Username

Password

Excluded hosts

Consider proxying local host connections

DNS name lookup at proxy end: Automatic

Telnet / local proxy command

Leave the field blank to use the default

Telnet - Proxy
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy type</td>
<td>Select your Proxy type between:</td>
</tr>
<tr>
<td></td>
<td>- None</td>
</tr>
<tr>
<td></td>
<td>- Socks4</td>
</tr>
<tr>
<td></td>
<td>- Socks5</td>
</tr>
<tr>
<td></td>
<td>- HTTP</td>
</tr>
<tr>
<td></td>
<td>- Telnet</td>
</tr>
<tr>
<td></td>
<td>- Local</td>
</tr>
<tr>
<td>Credential repository</td>
<td>Use the Credential repository of RDM for your proxy connection.</td>
</tr>
<tr>
<td>Host</td>
<td>Enter the proxy host address.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the proxy port.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username of the proxy host.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password of the proxy host.</td>
</tr>
<tr>
<td>Excluded hosts</td>
<td>The Excluded hosts box may contain more than one exclusion range, separated by commas. Enter hosts that would automatically be excluded.</td>
</tr>
<tr>
<td>Consider proxying local host connections</td>
<td>Connections to the local host are never proxied, even if the proxy exclude list does not explicitly contain them. It is very unlikely that this behaviour would ever cause problems, but if it does you can change it by enabling this option Consider proxying local host connections.</td>
</tr>
<tr>
<td>DNS name lookup at proxy end</td>
<td>If you are using a proxy to access a private network, it can make a difference whether DNS name resolution is performed by WinSCP itself (on the client machine) or performed by the proxy. The Do DNS name lookup at proxy end configuration option allows you to control this, select between:</td>
</tr>
<tr>
<td></td>
<td>- Automatic: WinSCP will do something it considers appropriate for each type of proxy. Telnet, HTTP and SOCKS5 proxies will have host names passed straight to them; SOCKS4 proxies will not.</td>
</tr>
<tr>
<td></td>
<td>- No: WinSCP will always do its own DNS, and will always pass an IP address to the proxy.</td>
</tr>
<tr>
<td></td>
<td>- Yes: WinSCP will always pass host names straight to the proxy without trying to look them up first.</td>
</tr>
<tr>
<td>Telnet/local proxy command</td>
<td>If you are using the Telnet proxy type, the usual command required by the firewall’s Telnet server is connect, followed by a host name and a port number. If your proxy needs a different command, you can enter an alternative here.</td>
</tr>
</tbody>
</table>
### Telnet - Advanced

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Internet protocol            | This option allows the user to select between the old and new Internet protocols and addressing schemes, choose between:  
  - Default (WinSCP)  
  - IPv4  
  - IPv6 |
| Initial keypad mode          | This option sets the initial status of the keypad  
  - Default  
  - Application  
  - Normal |
| Close on disconnect or error | Close the session when disconnecting or when an error occur. |

#### 6.2.2.11 VNC

**Description**

This entry is used to define and configure a **VNC** session.

- Auto Login  
- Credential repository  
- Full Screen  
- Show Opened Session  
- Built in  
- Embedded Mode  
- Support Host  
- Support AfterDisconnectEvent  
- Copy Password  
- External Mode  
- Multi Monitor Support  
- Support Logging
Only Ultra VNC and our Default VNC is supported in Embedded mode. All other VNC applications supported by Remote Desktop Manager are available only in External mode.

Providing the password in external mode is only supported by UltraVNC.

**Settings**

Embedded UltraVNC is the recommended mode for maximum compatibility. It also supports chats and files transfer while connected.

**General**

- **VNC application**: UltraVNC
- **Host**: ...
- **Port**: Default
- **FullScreen**: unchecked
- **Arguments**: 

![VNC - General](image)
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| VNC application       | Select your VNC application. The drop-down menu will have different option depending if you wish to run your session in Embedded or External mode. Embedded mode:  
  - Default  
  - VNC  
  External mode:  
  - RealVNC  
  - TightVNC  
  - UltraVNC  
  - VNC Viewer plus |
| Custom configuration  | By selecting **Custom configuration** you will have to enter all required information regarding the remote computer in the **Settings** and **Advanced** tabs. The screen size, color depth and the encryption level can only be customized when selecting the Custom configuration option. |
| Config filename       | Enter the path of your configuration file.                                                                                                 |
| Host                  | The host supports a distinct syntax to specify the port and display number. They must be set as the server requires. This syntax has been proven to work:  
  \{HOSTNAME\}::{PORT}:{DISPLAY}.  
  i.e. \$HOST\$::5902:2 |
| Port                  | Enter the port number if not using the default port.                                                                                         |
| Arguments             | Fully define a command line argument to start the session with.                                                                            |

**Settings**
VNC - Settings
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>VNC Password</td>
<td>Enter the password for the VNC server</td>
</tr>
<tr>
<td>Windows NTLM authentication</td>
<td>Enter your NTLM credentials (username, password and domain) to be authenticated.</td>
</tr>
<tr>
<td>View / Hide Password</td>
<td>Click on the view icon to view your password. Click on the hide icon to hide your password.</td>
</tr>
<tr>
<td>Password Generator</td>
<td>Click on the icon to display the Password Generator.</td>
</tr>
<tr>
<td>Password History</td>
<td>Click on the icon to display the Password History.</td>
</tr>
<tr>
<td>Password Analyzer</td>
<td>Indicates the strength of the password.</td>
</tr>
<tr>
<td>Color depth</td>
<td>Select the display color depth for the remote computer between:</td>
</tr>
<tr>
<td></td>
<td>· True color</td>
</tr>
<tr>
<td></td>
<td>· 256 colors</td>
</tr>
<tr>
<td></td>
<td>· 64 colors</td>
</tr>
<tr>
<td></td>
<td>· 8 colors</td>
</tr>
<tr>
<td></td>
<td>· 8 bit color</td>
</tr>
<tr>
<td></td>
<td>· 8 grey color (32 bits color screen resolution)</td>
</tr>
<tr>
<td></td>
<td>· 4 grey color (32 bits color screen resolution)</td>
</tr>
<tr>
<td></td>
<td>· 2 grey color (32 bits color screen resolution)</td>
</tr>
<tr>
<td>Scaled</td>
<td>The remote display is automatically scaled to fit the size of the window.</td>
</tr>
<tr>
<td>Other parameters</td>
<td>Enter any other parameters you wish to use.</td>
</tr>
<tr>
<td>Embedded delay (x64 only)</td>
<td>Adjust this value if more initialization time is required.</td>
</tr>
<tr>
<td>Request shared session</td>
<td>Allows several clients to share the same VNC session. If this option isn't set, only one client can be connected to the same Server. If a new &quot;non-shared&quot; client is connected, existing clients are disconnected, or new connection is dropped, depending on the server's configuration.</td>
</tr>
<tr>
<td>View only (input ignored)</td>
<td>Disable the session's input. No keyboard or mouse events are sent from the viewer to the server.</td>
</tr>
<tr>
<td>Hide toolstrip</td>
<td>Hide the toolstrip.</td>
</tr>
<tr>
<td>Show status window</td>
<td>Enables you to view the status window.</td>
</tr>
<tr>
<td>Disable clipboard transfer</td>
<td>Disable the clipboard synchronization (used for the copy-paste).</td>
</tr>
</tbody>
</table>

**Advanced**
VNC - Advanced

- Mouse:
  - Mouse cursor: Track remote cursor locally
  - Emulate 3 buttons (with 2-button click)
  - Swap mouse buttons 2 and 3
  - Track mouse movement

- Encoding:
  - Preferred encoding: Default
  - Custom compression level: 6
  - JPEG compression level: 6

- DSM Plugin:
  - DSM filename

- Proxy:
  - Proxy host:port

- Keyboard:
  - Apply Windows key combinations (for example ALT+TAB)
    - On the local computer
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mouse cursor</td>
<td>Select the mouse cursor behavior. Select between:</td>
</tr>
<tr>
<td></td>
<td>· Track remote cursor locally</td>
</tr>
<tr>
<td></td>
<td>· Let remote server deal with mouse cursor</td>
</tr>
<tr>
<td></td>
<td>· Don't show remote cursor</td>
</tr>
<tr>
<td>Emulate 3 buttons (with 2-button click)</td>
<td>Emulate mouse button 3 when clicking on both button 1 and button 2.</td>
</tr>
<tr>
<td>Swap mouse buttons 2 and 3</td>
<td>Switch your mouse buttons 2 and 3.</td>
</tr>
<tr>
<td>Track mouse movement</td>
<td>Track the mouse movement in real-time.</td>
</tr>
<tr>
<td>Preferred encoding</td>
<td>Change the encoding to use less bandwidth. From the least to the most bandwidth, select between:</td>
</tr>
<tr>
<td></td>
<td>· Default</td>
</tr>
<tr>
<td></td>
<td>· Auto</td>
</tr>
<tr>
<td></td>
<td>· CoRRE</td>
</tr>
<tr>
<td></td>
<td>· Hextile</td>
</tr>
<tr>
<td></td>
<td>· Raw</td>
</tr>
<tr>
<td></td>
<td>· RRE</td>
</tr>
<tr>
<td></td>
<td>· Tight</td>
</tr>
<tr>
<td></td>
<td>· Ultra</td>
</tr>
<tr>
<td></td>
<td>· Zlib</td>
</tr>
<tr>
<td></td>
<td>· ZlibHEX</td>
</tr>
<tr>
<td></td>
<td>· ZRLE</td>
</tr>
<tr>
<td>Custom compression level</td>
<td>Option available only when choosing the Preferred encoding Zlib.</td>
</tr>
<tr>
<td>JPEG compression level</td>
<td>For information value only.</td>
</tr>
<tr>
<td>DSM filename</td>
<td>If you choose to use a DSM plug-in for your connection, you can choose between:</td>
</tr>
<tr>
<td></td>
<td>· MSRC4 plugin</td>
</tr>
<tr>
<td></td>
<td>· SecureVNCPlugin</td>
</tr>
<tr>
<td></td>
<td>· SecureVNCPluginARC4</td>
</tr>
<tr>
<td>Proxy</td>
<td>If using a proxy server enter the host and port to connect.</td>
</tr>
</tbody>
</table>

**6.2.2.12 Wayk Now**

**Description**

This entry is used to define and configure a **Wayk Now** session.

- Embedded Mode
- External Mode
- Full Screen
- Support Host
- Show Opened Session

**Wayk Now** allows to take control of a remote computer to offer assistance. For more information about this product, please consult the **Wayk Now Online Help**.

**How to use Wayk Now**

A brief demonstration of how to use Devolutions remote access protocol, Wayk Now.
To use Wayk Now from Remote Desktop Manager, Wayk Now must be installed on the remote computer.

Settings

General

Wayk Now - General
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Wayk Den source | Select the Wayk Den source: Select between:  
  - Default (Cloud)  
  - Cloud  
  - Local |
| Host           | Enter the remote computer's **Source ID** (6-digit identification number) or IP address. |
| Preferred authentication | Select the authentication mode to use. Select between:  
  - Default  
  - Prompt For Permission  
  - Secure Remote Password  
  - Secure Remote Delegation |
| Username       | Enter the username of the remote computer. Only if using the secure remote delegation authentication mode. |
| Password        | Enter the password of the remote computer. |
| View / Hide password | Click on the view icon to view the password.  
  Click on the hide icon to hide the password. |
| Password generator | Click on the icon to display the [Password Generator](#). |
| Password history | Click on the icon to display the password history for this session. |
| Password Analyzer | Indicates the strength of the password. |
| Friendly name   | Enter a custom name for the remote user to recognize you in the chat window. |

**Advanced**

<table>
<thead>
<tr>
<th>General</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Keyboard</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

WaykNow - Advanced
### Quality Mode

Select the quality of the remote session. Select between:
- Default
- Low
- Medium
- High

### Scaled

Automatically scale the remote session to fit the window.

### Apply Windows key combinations

Select where the Windows key combinations are applied. Select between:
- On the local computer
- On the remote computer
- In full screen mode only

### Unique ID

Set up the unique ID from the target Wayk Now Host.

---

**Wayk Now Session in Remote Desktop Manager**

![Example of Wayk Now Session in Remote Desktop Manager](image)

For more information about available settings during an active session, please see the [Wayk Now online help](https://www.wayknow.com/help).

### 6.2.3 Virtualization

#### Description

This category contains all of the virtualization session types that are used to connect to a virtual remote system.
Here is a list of our Virtualization remote session:

- VMware (Player, Workstation, vSphere)
- Microsoft Hyper-V Dashboard
- XenServer Dashboard
- VMWare Dashboard
- Oracle VirtualBox
- Amazon Aws Dashboard
- Microsoft RDS Dashboard (Terminal Server)
- VMware Remote Console

### 6.2.3.1 Amazon Aws Dashboard

**Description**

The **Amazon Web Services (AWS) Dashboard** allows you to perform operations against the different AWS services.

**Prerequisites**
Existing AWS account for the services supported by the console and currently valid access keys.

Workflow

General

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friendly name</td>
<td>Enter the host name or IP address of the remote device.</td>
</tr>
<tr>
<td>Access key ID</td>
<td>Provides the list of computers discovered on your network. This can take a few moments to generate.</td>
</tr>
<tr>
<td>Secret access key</td>
<td>Enter the port to access the remote computer. Set the value to 0 to use the default port.</td>
</tr>
<tr>
<td>View / Hide Password</td>
<td>Click the view icon to view your password. Click the hide icon to hide your password.</td>
</tr>
<tr>
<td>Password History</td>
<td>Click on the icon to display the Password History.</td>
</tr>
<tr>
<td>Region</td>
<td>Select the appropriate region for best results.</td>
</tr>
</tbody>
</table>

Credentials

This tab supports a variety of RDM's credential feature to best suit your needs.

6.2.3.2 Microsoft Hyper-V Dashboard

Description

This entry is used to define and configure a Hyper-V session.

Settings
The Microsoft Hyper-V Dashboard is illustrated below, and provides a platform to configure your Hyper-V session.

Hyper-V Console

**General**

The following connection type uses vmconnect.exe. Please refer to [Hyper-V RDP](#) for further details.

Hyper-V - General Tab

We recommend using a Hyper-V RDP for a built-in and embedded view support.
Advanced

The Resources monitoring tab is only available in the console mode. The costly columns will appear only when the corresponding option is selected.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM processor usage</td>
<td>Monitor the processor usage of the virtual machine</td>
</tr>
<tr>
<td>VM Memory Demand</td>
<td>Monitor the memory demand of the virtual machine.</td>
</tr>
</tbody>
</table>
6.2.3.3 VMware Dashboard

Description

This entry is used to define and configure a VMware Dashboard session. The VMWare Console allows for basic administrative tasks of a VMWare host.

There are multiple steps to properly configure the PowerCLI on client workstations. Please follow the instructions thoroughly.

Some operations are not allowed on the Free edition of VMware Esxi.

Settings

Simply enter the host name or IP, the username and the password of a user with administrative rights on the host.
## VMware Dashboard - General Tab

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Host name of the vSphere server.</td>
</tr>
<tr>
<td>Ellipsis button</td>
<td>Performs network discovery to offer a list of servers.</td>
</tr>
<tr>
<td>Username</td>
<td>Username used to connect to the server.</td>
</tr>
<tr>
<td>Password</td>
<td>Password used to connect to the server.</td>
</tr>
</tbody>
</table>
| Hide/Reveal password | Shows or hides the clear text password. Available for:  
|                    | • Administrators.                                                          |
|                    | • Users that have the Allow Reveal Password privilege.                      |
| Generate password  | Displays the [Password Generator](#).                                       |
| Always ask password| Select to force entry of the password upon every use. Disables the Password entry control. |
| Console connection mode | Choose between:  
|                    | • Default: Uses the VMware remote console.       |
|                    | • VMware Player: Uses the VMware player.          |
|                    | • VMware remote console: Uses the VMware remote console.                  |

## Actions
### Action Description

<table>
<thead>
<tr>
<th>ACTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power on</td>
<td>Powers on the virtual machine</td>
</tr>
<tr>
<td>Power off</td>
<td>Powers off the virtual machine</td>
</tr>
<tr>
<td>Suspend</td>
<td>Suspends the virtual machine</td>
</tr>
<tr>
<td>Shut down guest</td>
<td>Shuts down the virtual machine. Only available when the VMware guest tools are running.</td>
</tr>
<tr>
<td>Restart guest</td>
<td>Restarts the virtual machine. Only available when the VMware guest tools are running.</td>
</tr>
<tr>
<td>Connect</td>
<td>Connect with the technology specified in the <strong>Console Connection mode</strong> setting of the console</td>
</tr>
<tr>
<td>New</td>
<td>Creates a persistent entry for the selected virtual machine.</td>
</tr>
<tr>
<td>Host</td>
<td>Name of the VMware Dashboard entry</td>
</tr>
<tr>
<td>Refresh</td>
<td>Refreshes the list of virtual machines</td>
</tr>
<tr>
<td>Auto refresh</td>
<td>Select to enable automatic refreshing of the content at a regular interval.</td>
</tr>
</tbody>
</table>

### 6.2.4 File Browser

**Description**

This category contains all of the File Browser session types that are used to connect to cloud remote system.
6.2.4.1 Microsoft OneDrive Explorer

Settings

This entry is used to define and configure a **Microsoft OneDrive Explorer** session. Microsoft OneDrive Explorer allows to perform everyday operations with documents stored in Microsoft OneDrive using the Windows Explorer, as if the files were on the local computer.

To configure an OneDrive for Business session, please consult the [OneDrive for Business] topic.

Settings
### General

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Account</td>
<td>Enter the email of the Microsoft Account used to access OneDrive.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password of the Microsoft account used to access OneDrive.</td>
</tr>
<tr>
<td>Password Analyzer</td>
<td>Indicates the strength of the password.</td>
</tr>
<tr>
<td>Always ask password</td>
<td>Always prompt for the password when the session is launched.</td>
</tr>
</tbody>
</table>
| OneDrive type           | Select your OneDrive type. Select between:  
  * Consumer  
  * Business |
| Account Status          | This label will tell you whether or not the entry is validated and ready for use. |
| Validate OneDrive       | You can use this toggle on and off the validation of the entry. |
| Default Directory       | Enter the default directory to access OneDrive. |
| Auto accept API permissions | Automatically accept the API permission. If not enabled you will have to accept the API permission manually when asked to. |
| Show files in tree view | Display the storage files in the session tree view (display using hierarchy). |

### Advanced
### OneDrive Explorer - Advanced Tab

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show local files</td>
<td>Show local files in the left pane of the session.</td>
</tr>
<tr>
<td>Local path</td>
<td>Enter the default local file path to open in the local file pane.</td>
</tr>
</tbody>
</table>

#### 6.2.4.1.1 OneDrive for Business

**Description**

An Office 365 subscription and an Azure subscription are required to get started. Remote Desktop Manager must be registered in Azure Active Directory and then request permissions for OneDrive for Business.

In the properties of a OneDrive Explorer session, select Business as the OneDrive type.
Register Remote Desktop Manager with the Azure Management Portal

To authenticate with OneDrive in Remote Desktop Manager, the application must be registered with the Microsoft Azure Management Portal.

For step-by-step information on how to register your application with OneDrive Business and how to specify the Office 365 permissions please follow this link.

1. In the Azure Active Directory section, select App registrations, then click on New application registration.
2. Name the application, specify that it is a **Web application**, and also enter [https://login.live.com/oauth20_desktop.srf](https://login.live.com/oauth20_desktop.srf) as the **Sign-on URL (Reply URL)** as below.

![Microsoft Azure Management - Single Sign-on](image)

3. Two alphanumeric keys must be retrieved from the Azure Portal to authenticate Remote Desktop Manager.

   3.1. The **Application ID**. Find it in the properties of the registered application.
3.2. The Secret key. Find it in the Keys blade of the registered application settings. Note that this key is visible only at the time it is generated. Leaving the blade will hide the key indefinitely.

Office 365 API permissions
You will need to specify permissions for Office 365 SharePoint Online that Remote Desktop Manager requires. In your permissions to other applications select the Delegated Permission drop down list of your Office 365 SharePoint Online and add the Read and write user files and Read user files.

6.2.5 Others
Description
This category contains other kind of session types that can be used.
6.2.5.1 Data Report

Description

This entry is used to define and configure a Data Report session. A Data Report is composed of a database connection string and a database query to be executed. The result is displayed in a read only grid with export capabilities. It is useful to quickly integrate data into the application.

- Auto Login
- Copy Password
- Embedded Mode
- Show Opened Session
- Credential repository
- Support Logging

Workflow

You must configure your connection string and your SQL query. You will also need to know how to write an SQL statement as this is database dependent.

Settings

General
### Data Report - General Tab

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Source</strong></td>
<td>Select your source between:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default:</strong> The connection string is defined directly within the session.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Credential repository:</strong> Use a linked <a href="#">Connection String</a> credential entry as the connection string.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Inherited:</strong> Navigate down the inheritance graph of the object to find the connection string.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Prompt:</strong> At open connection time, the system will prompt the user to select the desired <a href="#">Connection String</a> from credential entry list.</td>
</tr>
<tr>
<td><strong>Data source</strong></td>
<td>Contains the data source type like ODBC, OLEDB or native. This value is read only and is automatically extracted from the connection string.</td>
</tr>
<tr>
<td><strong>Data provider</strong></td>
<td>Specify the provider used for the database access. This value is read only and is automatically extracted from the connection string.</td>
</tr>
<tr>
<td><strong>Connection string</strong></td>
<td>This value contains the database connection string and can be hidden/encrypted for a better security.</td>
</tr>
<tr>
<td><strong>Host</strong></td>
<td>Contains the connection server name. This value is read only and is automatically extracted from the connection string.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>Contains the username used to access the database. This value is read only and is automatically extracted from the connection string. If using Windows Authentication the field will be empty.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Contains the username used to access the database. This value is read only and is automatically extracted from the connection string. If using Windows Authentication the field will be empty.</td>
</tr>
</tbody>
</table>
When the source is set to Prompt you will see a dialog box prior to opening the connection. Only the Connection String credential entries from your data source are listed. Select the entry to use and the report will be executed.

**Parameters**

Using parameters is quite simple. Write your query with parameter place holders (@Param1 or ? depending of the data provider you use). On the Parameters tab define the parameter type and default value. When opening the session, you will be prompted for the parameter values.

**Example of Query fields:**

```sql
SELECT FieldA, FieldB From Table1 Where FieldC = @Param1 or FieldD = @Param2
```

Parameter placeholders syntax depends on the chosen data provider:

- **.NET Framework Data Provider for SQL Server**: Uses named parameters in the format `@paramname`
- **.NET Framework Data Provider for OLE DB**: Uses positional parameter markers indicated by a question mark (`?`).
- **.NET Framework Data Provider for ODBC**: Uses positional parameter markers indicated by a question mark (`?`)
- **.NET Framework Data Provider for Oracle**: Uses named parameters in the format: `parmname`
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select between 3 types:</td>
</tr>
<tr>
<td></td>
<td>· Unused</td>
</tr>
<tr>
<td></td>
<td>· Text</td>
</tr>
<tr>
<td></td>
<td>· Secured</td>
</tr>
<tr>
<td></td>
<td>· Integer</td>
</tr>
<tr>
<td></td>
<td>· Numeric</td>
</tr>
<tr>
<td></td>
<td>· Date</td>
</tr>
<tr>
<td></td>
<td>· DateTime</td>
</tr>
<tr>
<td></td>
<td>· GUID</td>
</tr>
<tr>
<td>Default value</td>
<td>Enter the default value.</td>
</tr>
<tr>
<td>Exec Query</td>
<td>Once your have set the default value of your parameter you can execute your query fields.</td>
</tr>
<tr>
<td>Show parameters in report header</td>
<td>Show the parameter name in the report header. You can change the parameter name by clicking on Parameter.</td>
</tr>
</tbody>
</table>

### Query

Enter the query in the **Query** tab, which features an SQL syntax-highlighted text box with line numbers which must be compatible with the data provider.

This supports multiple queries in the statement and will display the results in different tab pages. Most native drivers support it. For ODBC, you must locate an advanced setting named *MultipleActiveResultSets* or *MARS_Connection* and turn it on. If you do not see such a property, then it is not supported by your driver.
**Troubleshooting**

While setting up the connection use the **Test Connection** button of the **Connection Properties Window** to ensure the connection is configured properly.

Use the **Exec Query** button on the **Parameters** tab to preview the query result.

More information is available in the **Tips and Tricks Data Report** topic.

### 6.2.5.2 PowerShell

**Description**

This entry is used to define and configure a **PowerShell** session.

- Auto Login
- Credential repository
- Multi Monitor Support
- Built in
- Embedded Mode
- Show Opened Session
- Copy Password
- External Mode
- Support Logging

**Settings**

The remote system must be configured to allow remote commands. Please consult **Enable and Use Remote Commands in Windows PowerShell**.

**General**
PowerShell - General Tab

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>Enter the PowerShell command.</td>
</tr>
<tr>
<td>Filename</td>
<td>Select a PowerShell file on the network or on the computer.</td>
</tr>
<tr>
<td>Arguments</td>
<td>Arguments that are appended to the Command.</td>
</tr>
<tr>
<td>Execution mode</td>
<td>Select your execution mode between:</td>
</tr>
<tr>
<td></td>
<td>• Default</td>
</tr>
<tr>
<td></td>
<td>• Command</td>
</tr>
<tr>
<td></td>
<td>• Encoded command</td>
</tr>
<tr>
<td>PowerShell version</td>
<td>Select your PowerShell version between:</td>
</tr>
<tr>
<td></td>
<td>• Default (current version)</td>
</tr>
<tr>
<td></td>
<td>• Version 2</td>
</tr>
<tr>
<td>No exit</td>
<td>Does not exit after running startup commands</td>
</tr>
<tr>
<td>No profile</td>
<td>Does not load the Windows PowerShell profile.</td>
</tr>
<tr>
<td>Resize window</td>
<td>Force window resize (buffer &amp; window).</td>
</tr>
<tr>
<td>Single thread apartment</td>
<td>Starts Windows PowerShell using a single-threaded apartment</td>
</tr>
<tr>
<td>Run as administrator</td>
<td>Run PowerShell command as a administrator.</td>
</tr>
<tr>
<td>Debug</td>
<td>Show debug</td>
</tr>
<tr>
<td>No Logo</td>
<td>Hides the copyright banner at startup.</td>
</tr>
<tr>
<td>Load RDM CmdLet</td>
<td>Load RDM CmdLet Snap-in in the PowerShell session.</td>
</tr>
<tr>
<td>Run in 64-bit mode</td>
<td>Run RDM CmdLet in 64 bits version.</td>
</tr>
<tr>
<td>Non interactive (suppress error message)</td>
<td>Does not present an interactive prompt to the user.</td>
</tr>
</tbody>
</table>
Host and Credentials

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Select the host computer to execute the Powershell command.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username to access the host computer.</td>
</tr>
<tr>
<td>Domain</td>
<td>Enter the domain to access the host computer.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password to access the host computer.</td>
</tr>
</tbody>
</table>

Run As

Use the variables in your parameters:
- $USERNAME$
- $DOMAIN$
- $HOST$
- $PASSWORD$
Remote Desktop Manager

6.2.5.3 SNMP Report

Description

This entry is used to define and configure a **SNMP Report** session. SNMP Reports will provide you information from devices on your network such as routers, switches, servers, workstations, printers and more.

Remote Desktop Manager uses a specific tool (NET-SNMP) for the SNMP Report. You will be prompted to download the tool if it wasn’t already installed on your computer.

You can use the following SNMP versions to run your SNMP reports entries:

- SNMP Version 1
- SNMP Version 2c
- SNMP Version 3

Settings
### SNMP Report - General Tab

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Host name / IP address of host.</td>
</tr>
<tr>
<td>SNMP version</td>
<td>Select your SNMP version between:</td>
</tr>
<tr>
<td></td>
<td>• SNMP Version 1</td>
</tr>
<tr>
<td></td>
<td>• SNMP Version 2c</td>
</tr>
<tr>
<td></td>
<td>• SNMP Version 3</td>
</tr>
<tr>
<td>Command</td>
<td>Determine the content of the report between:</td>
</tr>
<tr>
<td></td>
<td>• List available OIDs and values</td>
</tr>
<tr>
<td></td>
<td>• Get specific OIDs values</td>
</tr>
<tr>
<td></td>
<td>• Status of the host</td>
</tr>
<tr>
<td>Community</td>
<td>Community equal to the password. By default, the password is the word public.</td>
</tr>
<tr>
<td>MIB Directory</td>
<td>Location of the MIB database.</td>
</tr>
<tr>
<td>OIDs</td>
<td>Object identifier for an object in the MIB. This help you reduce the items in the report.</td>
</tr>
<tr>
<td>Trim MIB names</td>
<td>Remove MIB names.</td>
</tr>
<tr>
<td>Prompt for options</td>
<td>Options to change the command or to specify an OIDs before the report execution.</td>
</tr>
</tbody>
</table>
More commands can be added to Remote Desktop Manager upon request, please post a feature request on our forum.

**OIDs examples**
- sysDescr.0
- sysObjectID.0
- sysUpTimeInstance
- sysContact.0
- sysName.0

**V3 Specific**

If your network uses the SNMP V3, you will also need to enter information in the V3 Specific tab.

![SNMP Report - V3 Specific Tab](image-url)
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Authentication protocol | Select your authentication protocol between:  
  - None  
  - MD5  
  - SHA |
| Authentication passphrase| Enter your authentication protocol password. |
| Privacy protocol        | Choose between None or DES |
| Privacy passphrase       | Enter your privacy protocol password. |
| Security engine ID      | Enter your security engine ID which is part of the target host configuration |
| Security name           | Enter your security name which is part of the target host configuration |
| Context engine ID       | Scanning engine to retrieve context-sensitive information from the target host. |
| Context name            | Scanning engine to retrieve context-sensitive information from the target host. |
| Destination engine      | Select your destination engine between:  
  - Not specified  
  - Boots  
  - Time |

**Functions**

**Execution Logs**

When a SNMP Report is open, at any time you can look at the bottom in the execution log window to see if the report has encountered a problem.

**Save**

You can save the report or the execution log in a Text document to keep your information or to print it.

![Save button](image)

**Refresh**

The refresh button can be used to refresh your report or to generate a different report from the current one. You can change the Command and/or specify some OIDs.
6.2.5.4 SQL Server Management Studio

Description

This entry is used to define and configure a SQL Server Management Studio session.

- Auto Login
- Built in
- Credential repository
- Embedded Mode
- Copy Password
- Support Logging
- Show Opened Session

If you are sending a command line from a computer that is not on the domain to a computer that is on the domain, check **Net Only** when using **Run As different user**.

Settings
### SQL Server Management Studio - General Tab

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Enter the full Host name. If a default instance has been used, you could just enter the server name.</td>
</tr>
<tr>
<td>Database</td>
<td>Enter the SQL database you wish to connect upon login (optional).</td>
</tr>
<tr>
<td>Integrated security (Active Directory)</td>
<td>Enable this option if you wish to use Active Directory.</td>
</tr>
<tr>
<td>Run as different user (Active Directory only)</td>
<td>If using Integrated security you have the option of running your session as a different user.</td>
</tr>
<tr>
<td>Net Only (Active Directory only)</td>
<td>If you are sending a command line from a computer that is not on the domain to a computer that is on the domain, enable the Net Only setting for credentials of the Running As.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username for the SQL Server Authentication.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the SQL Server Authentication.</td>
</tr>
<tr>
<td>Default query file</td>
<td>Specify the file to be opened in the editor. Please see Add-On documentation for more information.</td>
</tr>
<tr>
<td>Show splash screen</td>
<td>Enable SQL Server Management Studio to display its splash screen.</td>
</tr>
</tbody>
</table>

If choosing Run as different user you will have to specify which credentials to use when starting with Run As.
### 6.3 Information

Information entries are used to store information that is meant to be shared with other users of the data source, such as websites, alarm codes, serial numbers, etc.
Websites

The **Website** entry is for online accounts. It can store a website url address and a set of credentials. The website can be opened in Remote Desktop Manager or externally. The entry can be linked with our Devolutions Web Login browser extension. When opening a website externally our browser extension Devolutions Web Login fills the username and password for you.
6.4 Contact

Description

Contact entry types are used to manage your contacts in Remote Desktop Manager.

Settings

You can choose between 7 different types of contacts

Example of Devolutions Web Login injecting a password for an online log-in form
## Contents

**Contact Type**  | **Description**  
--- | ---
Company | Used to define and configure a “Company” contact.  
Customer | Used to define and configure a “Customer” contact.  
Default | Used to define and configure a contact with no defined type. Use this type of entry if your contact does not fit in any other category.  
Employee | Used to define and configure a “Employee” contact.  
Family | Used to define and configure a “Family” contact.  
Supplier | Used to define and configure a “Supplier” contact.  
Support | Used to define and configure a “Support” contact.  

Enter all the information related to a contact to create your entry.

### Contact Entry

**General**
Use this subsection to enter basic information about the contact, such as their name, gender and job title.

The **Credentials** link allows to embed a set of credentials in the entry.

Click on the **Customer #** link to change the name of the field.

### Address
Use the middle-left subsection to enter information about the contact's company and address.

Use the **View Map** button to open Google Maps with your default web browser.

### Communication
Use the middle-right subsection to enter the contact's communication information, such as their email address or phone number.

Click on the **Email Contact** button to send an email to the specified email address with your default email application.

Click on the **Call (Skype)** button to call the specified number with Skype. A Skype username can also be specified in the Skype field.

Click on the **Open Website** button to navigate to the specified website with your default web browser.

## 6.5 Credentials

### Description

Credential entries store account information, such as usernames, passwords, domains, etc. Credentials entries are grouped in a Credential repository, a collection of all the credentials stored in the data source.

Credential entries offer flexibility in *Remote Desktop Manager*.

- Set multiple sessions to use a specific credential entry in the data source. Choose **Credential repository** from the **Credentials** list in the entry properties. One benefit is you only need to change information in one entry, when required. See **Credential repository** below.
- Use **Dynamic Credential Linking** and **Credential Redirection** with third-party password managers.
- Configure **User Specific Settings** or a Private Vault Search in entry properties to link credentials stored in a Private Vault with entries in shared Vaults.

To create a credential entry, use the **New Entry** button and select the **Credentials** section.
The credential branch

By default, credentials are stored in the same list as other entries are. This behavior can be changed so credentials are stored in a separated list.

To separate credentials from other entries, navigate to File – Options – User Interface – Tree View. Under UI Options, disable the Merge credential list with sessions option. You must also disable this option in the Data Source Settings (System Settings) – Applications – Type Settings.
The Credential repository

The Credential repository is the collection of all the credentials stored in the data source. The Credential repository allows you to use the same credential entry for multiple session.

The Credential repository is available almost anywhere in RDM, including Folders, Sessions, Synchronizers, VPN and Website entry types.

When configuring a session select Credential repository from the Credential drop down list, then select the desired credential entry from the credentials list.
Select a credential entry

To configure the Credential repository to prompt you to select a set of credentials, which allows for using multiple credentials for the same host, select **Prompt on connection** from the credential list.

### Available credential entries

We support a multitude of credential entry types, both integrated and external! Explore to your heart's content.

#### 6.5.1 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.

![LastPass credential]

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**. 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.
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.
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

![Remote Desktop Manager](image1)

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

![Remote Desktop Manager](image2)

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](image)

**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

![Remote Desktop Manager](image)

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.

![Credential Name](image)

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**
6.5.2 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 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.*
2. When creating an 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.

3. Select a credential from the 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".

6.5.3 Types

6.5.3.1 AuthAnvil Password Server

**Description**

This entry is used to define and configure a **AuthAnvil Password Server** credential entry.

**Settings**

**General**
### AuthAnvil Password Server – General

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service URL</td>
<td>Enter the AuthAnvil Password Server URL to connect. <strong>Example:</strong> https://&lt;ServerHostname&gt;/AAPS/AAPS.svc</td>
</tr>
<tr>
<td>Certificate</td>
<td>Select a specific certificate to connect to your AuthAnvil Password Server. For more information, please consult the Certificate section below.</td>
</tr>
<tr>
<td>Use &quot;My Account Settings&quot;</td>
<td>Use the information configured in <a href="#">My Account Settings</a> to connect.</td>
</tr>
<tr>
<td>Organization ID</td>
<td>Indicate your password Vault Organization ID.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username to connect to your AuthAnvil Password Server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password to connect to your AuthAnvil Password Server.</td>
</tr>
<tr>
<td>Credentials list mode</td>
<td>Indicate the credential list that you want to display. Select between:</td>
</tr>
<tr>
<td></td>
<td>- <strong>All credentials</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Public credentials only</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Private credentials only</strong></td>
</tr>
<tr>
<td>Private Vault key</td>
<td>Indicate the Private Vault key.</td>
</tr>
</tbody>
</table>

**Advanced**
### OPTION

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always prompt with list</td>
<td>Always prompt with the list of credentials when connecting.</td>
</tr>
<tr>
<td>Credentials</td>
<td>Select a specific credential on your AuthAnvil Password Server.</td>
</tr>
<tr>
<td>Validate</td>
<td>Validate the connection to the server to confirm that the credentials are working.</td>
</tr>
</tbody>
</table>

### Certificate

The certificate for the AuthAnvil entry can be downloaded from the AuthAnvil server web interface. Navigate to **Admin – External Settings – Third Party Certificates**, and download the **SSO certificate**.
6.5.3.2 Connection String

Description

This entry is used to define and configure a Connection String credential entry. Connection string credential entries are exactly the same as a Database Folder with the exception that they are not limited by the inheritance hierarchy of folders and sessions.

Settings

General

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data source</td>
<td>Contains data source types like ODBC, OLEDB or native. This value is read only and is extracted from the connection string.</td>
</tr>
<tr>
<td>Data provider</td>
<td>Specify the provider used for the database access. This value is read only and is extracted from the connection string.</td>
</tr>
<tr>
<td>Connection string</td>
<td>This value contains the database connection string and it can be hidden/encrypted for higher security.</td>
</tr>
<tr>
<td>Eye/Lock button</td>
<td>Reveals or hides the connection string</td>
</tr>
<tr>
<td>Ellipsis button</td>
<td>Displays the standard Windows Connection string builder dialog.</td>
</tr>
<tr>
<td>Host</td>
<td>Connection server name.</td>
</tr>
<tr>
<td>Username</td>
<td>Username to connect on the server.</td>
</tr>
<tr>
<td>Password</td>
<td>Password to connect on the server.</td>
</tr>
</tbody>
</table>
### 6.5.3.3 Custom

#### Description

This entry is used to define and configure a **Custom** credential entry.

#### Settings

**General**

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| **Powershell** | Select between:  
  - **PowerShell**: Type your PowerShell command in the Command field  
  - **Linked PowerShell**: Link your credential entry to a pre-existing PowerShell command |

#### Parameters
You can use parameters in your PowerShell script, just type \$PARAMETER1\$ for the first parameter, \$PARAMETER2\$ for the second parameter, etc...

**6.5.3.4 CyberArk**

**Description**

This entry is used to define and configure a CyberArk credential entry. Retrieve credentials directly from a CyberArk Vault using their REST APIs.

A Remote Desktop Manager Site License is necessary to use the CyberArk integration.

As per this initial implementation, you must create a credential entry **FOR EACH** credential that you want to access from Remote Desktop Manager. A feature to list accounts is being implemented at this time. You can alternatively use the PACLI to generate a CSV file that can be paired with a **CSV Synchronizer** to have entries generated automatically at a regular frequency.

**Settings**

To retrieve the information easily, match the numbers from the credential entry picture below in Remote Desktop Manager with the same numbers from the CyberArk portal.

The images from the CyberArk portal are below as well.
CyberArk - General Tab

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web services URL</td>
<td>Enter the Privileged Account Security (PAS) URL. (It typically ends by PasswordVault although just the root is need in this field.) e.g. if accessing the PAS using <a href="https://server.domain.com/PasswordVault">https://server.domain.com/PasswordVault</a>, you would simply specify <a href="https://server.domain.com">https://server.domain.com</a> in this field.</td>
</tr>
<tr>
<td>Virtual Directory</td>
<td>Used to specify when the PAS solution is not deployed at the root of a web site. It would be the case when there is an extra folder between the root of the address (.com) and the PasswordVault string.</td>
</tr>
<tr>
<td>Version</td>
<td>Select which version you wish to use.</td>
</tr>
<tr>
<td>Use &quot;My Account Settings&quot;</td>
<td>Use the username/password combination stored in File – My Account Settings – CyberArk.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username to connect on Cyberark's PAS solution.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password to connect on Cyberark's PAS solution.</td>
</tr>
<tr>
<td>Safe name</td>
<td>Enter the name of the safe where the entries are stored. Provided by your CyberArk administrator. The default value is &quot;root&quot;</td>
</tr>
<tr>
<td>Folder</td>
<td>Enter the folder name where the entries have been stored. Provided by your CyberArk administrator. The default value is &quot;root&quot;</td>
</tr>
<tr>
<td>Keywords</td>
<td>Enter the keywords that will help locate the entry. Their API will perform a partial match in their Name field. Note that if the keywords match with multiple results, an error will be displayed.</td>
</tr>
</tbody>
</table>

Advanced
## CyberArk - Advanced Tab

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain search method</td>
<td>Specify how you wish to search for the Domain.</td>
</tr>
<tr>
<td>Domain field</td>
<td>Specify the field (and possibly content) of the Domain field.</td>
</tr>
</tbody>
</table>

### Cyberak PAS screen
6.5.3.5 CyberArk AIM

Description

This entry is used to define and configure a CyberArk AIM credential entry. Retrieve credentials from CyberArk AIM server and improve credentials security.

- A Remote Desktop Manager Site License is necessary to use the CyberArk AIM entry.
- As per this initial implementation, you must create a credential entry FOR EACH credential that you want to access from Remote Desktop Manager. A second phase is planned where the REST API will be used rather than AIM.

Settings

All the needed information's to create a CyberArk credential entry in Remote Desktop Manager is provided below. To retrieve the information easily, match the numbers from the credential entry picture below in Remote Desktop Manager with the same numbers from the CyberArk portal.
The images from the CyberArk portal are below as well.

CyberArk AIM Credential Entry

Privileged Account Security Portal
CyberArk Applications Tab

3. Application Details: Devolutions_RDM

4. Account Details

5. Location: \n
6. Last verified: N/A
Last modified: Administrator (12/11/2017 7:00:32 AM)
Last used: Administrator (12/11/2017 7:00:32 AM)
Username: downhill\admin
Address: VDOWSRSV-DC
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web services URL</td>
<td>Enter the Privileged Account Security URL.</td>
</tr>
<tr>
<td>Use &quot;My Account Settings&quot;</td>
<td>Use the username stored in File – My Account Settings – CyberArk AIM.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username to connect on Cyberark.</td>
</tr>
<tr>
<td>Application server URL</td>
<td>Enter the URL to the CyberArk AIM web server. Example: https://&lt;host.domain&gt;/AIMWebService/v1.1/AIM.asmx</td>
</tr>
<tr>
<td>Application ID</td>
<td>Enter the name of the application ID for the CyberArk Central Credential Provider web services. This information will be provided by your CyberArk administrator.</td>
</tr>
<tr>
<td>Show / Hide Application ID</td>
<td>Click to view the Application ID. Click to hide the Application ID.</td>
</tr>
<tr>
<td>Safe name</td>
<td>Enter the name of the safe where the entries are created.</td>
</tr>
<tr>
<td>Folder</td>
<td>Enter the folder name where the entries have been created. Provided by your CyberArk administrator. The default value is &quot;root&quot;</td>
</tr>
<tr>
<td>Object</td>
<td>Enter the object name of the entry.</td>
</tr>
</tbody>
</table>

### 6.5.3.6 KeePass

**Description**

This entry is used to define and configure a **KeePass** credential entry. Use a KeePass plugin to send the credential to Remote Desktop Manager. The KeePass application must be running and the database must be opened.

- **KeePass 1.X is not supported.**

- This type has recently been improved to support linking to multiple KeePass databases simultaneously. Simply add all the paths separated by semi-colons in the **Database** control.

**Settings**

**General**
KeePass - General Tab

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Database</strong></td>
<td>The default KeePass database is selected by Remote Desktop Manager.</td>
</tr>
<tr>
<td><strong>Set database path manually</strong></td>
<td>This option needs to be checked if you wish to manually indicate the location of your database. If you wish to use multiple databases at once, simply list their respective paths separated by semi-colons.</td>
</tr>
<tr>
<td><strong>Install Plug-in</strong></td>
<td>Install the KeePass Plug-In on your computer.</td>
</tr>
<tr>
<td><strong>More information (installation and required settings)</strong></td>
<td>Provide information on the KeePass Plug-In.</td>
</tr>
</tbody>
</table>

Advanced

KeePass - Advanced Tab
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uuid</td>
<td>Universal Unique Identifier of the entry in the database.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the entry in the database.</td>
</tr>
<tr>
<td>Always prompt with list</td>
<td>Always prompt with the list of credentials when connecting.</td>
</tr>
<tr>
<td>Allow view credentials action</td>
<td>Enables the View credentials command.</td>
</tr>
</tbody>
</table>

See [Dynamic Credential](#) topic for more information on Dynamic Credential Linking.

### 6.5.3.7 LastPass

#### Description

This entry is used to define and configure a **LastPass** credential entry.

LastPass offers different features per subscription plans. Remote Desktop Manager supports certain features of each plan:

- **Standard:** 2-Factor Authentication (Google Authenticator) and Secure Notes. The ones that contain both a Username and Password are displayed in Remote Desktop Manager (Server, Email account, Database, Instant Messenger).

- **Premium:** 2-Factor Authentication (YubiKey), please see LastPass, Yubikey and mobile access section below.

- **Enterprise:** Shared Folders.

#### Settings

- **Watch Video**

#### General
### LastPass - General Tab

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mode</strong></td>
<td>Select between:</td>
</tr>
<tr>
<td></td>
<td>• Credential Redirection</td>
</tr>
<tr>
<td></td>
<td>• Integrated</td>
</tr>
<tr>
<td><strong>Account name</strong></td>
<td>LastPass account name (Email address).</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Password to access the LastPass account.</td>
</tr>
<tr>
<td><strong>Always ask password</strong></td>
<td>Always ask password when connecting to LastPass.</td>
</tr>
<tr>
<td><strong>Title</strong></td>
<td>Use the ellipsis to select the credential in your LastPass database, its title will be displayed when there is a selection.</td>
</tr>
<tr>
<td><strong>Uuid</strong></td>
<td>Universal Unique Identifier of the entry in the database.</td>
</tr>
<tr>
<td><strong>Always prompt with list</strong></td>
<td>Always prompt with the list of credentials accessible from LastPass.</td>
</tr>
</tbody>
</table>
Credential Redirection Mode

Please refer to Credential Redirection for full instructions.

Dynamic Credential Linking

Please refer to Dynamic Credential for more information.

6.5.3.8 Mateso Password Safe

Description

This entry is used to define and configure a Mateso Password Safe credential entry. The integration with Mateso Password Safe requires a Mateso Enterprise Plus subscription.

Make sure web services is installed on the Mateso Password Safe server. You also need a certificate from a trusted Certification Authority installed in the Trusted Root Certification Authorities.

Settings
### 6.5.3.9 One Time Password

#### Description

This entry is used to define and configure a **One Time Password** credential entry.

The **One Time Password** credential type is used as a second authentication factor that allows a user to secure its account with a generated verification code changing over time.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Enter the Mateso Password Safe server address. Example: mateso.yourcorporatedomain.com</td>
</tr>
<tr>
<td>Database</td>
<td>Select the database which the passwords are retrieved from.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter a Mateso account username.</td>
</tr>
<tr>
<td>Password (1)</td>
<td>Enter a Mateso account password.</td>
</tr>
<tr>
<td>Password (2)</td>
<td>Use the ellipsis button to select a password from the Mateso database.</td>
</tr>
<tr>
<td>Always prompt with list</td>
<td>Always prompt with a list of available credentials in the Mateso database when using the entry. Useful to create a Credential repository to link with other entries in Remote Desktop Manager.</td>
</tr>
</tbody>
</table>
Enabling Multifactor Authentication

To use the multifactor authentication, this feature must be enabled from the user's account of a service or website that supports multifactor authentication. Usually, you can find the multifactor authentication settings in the security preferences of a user's account. The name of the feature should be similar to **two-factor authentication**, **two-step verification**, or **multifactor authentication**.

When enabling multifactor authentication, a list of recovery codes might be generated as well by the website or application. Carefully store these in a safe place. These recovery codes will be useful if the user happens to lose the **One Time Password** entry.
Website security preferences - Two-step verification

The website or application could ask if you want to receive verification codes by text messages or generate them by an application. Choose to generate the codes by an application. This will generate a secret key to enter in Remote Desktop Manager.

Choose to receive verification codes by an authenticator application

Copy the key to the clipboard and paste its content in the Key field of the One Time Password entry. If there are spaces in the key, remove them.
Enable two-step verification

An authenticator app lets you generate security codes on your phone without needing to receive text messages. If you don’t already have one, we support any of these apps.

To configure your authenticator app:

- Add a new time-based token.
- Enter the secret key below, or scan a barcode instead.

wff 25p3 pr21

Accept the changes in the website or application, and in Remote Desktop Manager. When connecting to the account, click on the View Password button to display the generated verification code. Enter the verification code when prompted by the website or application.

One Time Password Entry - View Password

6.5.3.10 Password List

Description
This entry is used to define and configure a **Password List** credential entry.

The Password List credential type allows for storing multiple credentials in one entry. These credentials can then be used in sessions. Each entry within the password list entry contains a username, a domain, a password, and a description. An expiration date can also be set on each credential entry in the password list.

A great advantage of the password list is that it contains multiple credentials in a single entry.
**Remote Desktop Manager**

**Settings**

Password List - General Tab

<table>
<thead>
<tr>
<th>ACTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Add credentials to the list.</td>
</tr>
<tr>
<td>Edit</td>
<td>Edit the selected credentials.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete the selected credentials.</td>
</tr>
</tbody>
</table>

**Add Credentials**

From the password list entry properties, click on Add ➕.
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Enter the username to which the password is associated.</td>
</tr>
<tr>
<td>Domain</td>
<td>Enter the domain of the user.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password of the user.</td>
</tr>
<tr>
<td>View / Hide</td>
<td>Click on the view icon to view the password.</td>
</tr>
<tr>
<td>password</td>
<td>Click on the hide icon to hide the password.</td>
</tr>
<tr>
<td>Password</td>
<td>Click on the icon to display the Password Generator.</td>
</tr>
<tr>
<td>generator</td>
<td></td>
</tr>
<tr>
<td>Expiration</td>
<td>Set an expiration date for the password.</td>
</tr>
<tr>
<td>Custom Tab</td>
<td>Here you can add custom information to your Password lists.</td>
</tr>
<tr>
<td>Roles Tab</td>
<td>You can Assign roles or Users directly to your credentials.</td>
</tr>
</tbody>
</table>

6.5.3.11 Secret Server

Description

This entry is used to define and configure a Secret Server credential entry.
The Secret Server integration requires its Web Services feature to be enabled. For more information, please refer to the Secret Server documentation.

Currently, the Remote Desktop Manager integration of Secret Server supports **Radius** and **Duo Pin** as a second authentication factor. **Duo Push** is not supported.

**Settings**

**General**

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service URL</strong></td>
<td>Enter the URL of the Secret Server web services endpoint. Please see note below.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>Enter the Domain. Required when Secret Server is configured with domain authentication.</td>
</tr>
<tr>
<td><strong>Use &quot;My Account Settings&quot;</strong></td>
<td>Use the credentials configured in My Account Settings to connect.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>Enter a Secret Server username. The password is prompted upon validating the settings or when selecting a secret.</td>
</tr>
</tbody>
</table>

**Credential Selection**
### Secret Server – Credential Selection Tab

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| **Look up** | Select how the secret is retrieved from Secret Server. Select between:  
  - **Default**: select from the available secrets.  
  - **By Name**: provide a name that matches a secret.  
  - **Prompt For List** |
| **Mode**  | Select the secret mode. Select between:  
  - **As Credential**  
  - **As Private Key** |

**Default**

![Default Secret Server – Credential Selection – Default](image)
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Click on the ellipsis button to display a list of available secrets. This control displays the name of the template for the selected secret.</td>
</tr>
<tr>
<td>Name</td>
<td>Displays the name of the selected secret.</td>
</tr>
<tr>
<td>Test Settings</td>
<td>Click to be prompted for the password and validate the credentials.</td>
</tr>
</tbody>
</table>

### Name

<table>
<thead>
<tr>
<th>General</th>
<th>Credential Selection</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lookup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secret name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>As Credential</td>
<td></td>
</tr>
</tbody>
</table>

**Secret Server – Credential Selection – By Name**

### Secret name

Enter the partial or full name of the secret to use. Variables can be used, which means you could set up a naming structure for your secrets that would match the structure you are using for your sessions.

### Prompt For List

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always prompt with list</td>
<td>Select the secret from a list upon every use.</td>
</tr>
</tbody>
</table>

### Authentication

There is no field to hold the Secret Server password in the entry's properties. When it is required to connect to Secret Server, the following dialog is prompted.
The password is cached in memory for the current session only.

Notes

Secret Server Service URL

Secret server supports Windows Authentication depending on the version being used and the web server that hosts the application. The Service URL in that case would use the following form: `<Secret Server URL>/winauthwebservice/sswinauthwebservice.asmx`. Please refer to the Secret Server documentation to see if it is supported for your edition, and for how to enable it. As soon as we detect that the endpoint being used is for Windows Authentication, it will be used seamlessly.

Follow this procedure to obtain the proper service URL:

1. Log in to the Secret Server web application.
2. Go in the administration - Configuration section.
3. Locate the View Webservices hyperlink.
4. Right-click and copy the hyperlink.
5. Paste the value in the Service URL field.
Username
Variables are supported in the username field. If the names are similar across your domain and Secret Server, you could do one of the following:

- `%username%@%userdomain%`, this uses windows environment variables that hold your identity.
- `%username%@somedomain.com`, mix of environment and plain text.

Dynamic Credential Linking
Please refer to Dynamic Credential for more information.

6.5.3.12 Sticky Password

Description

This entry is used to define and configure a Sticky Password credential entry.

Settings

General
### Sticky Password - General Tab

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Enter the Sticky Password account's email.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the Sticky Password account's password.</td>
</tr>
<tr>
<td>Always ask password</td>
<td>Check this option to be prompted for the password upon every usage of this entry. It also has the effect of preventing the password from being specified.</td>
</tr>
<tr>
<td>Credentials</td>
<td>Displays the currently selected credentials. Select the credential with the ellipsis button.</td>
</tr>
<tr>
<td>Always prompt with list</td>
<td>Displays a list of the available credentials when the Sticky Password entry is used.</td>
</tr>
</tbody>
</table>

**Cloud sync**

To use Sticky Password in Remote Desktop Manager, the Cloud Sync option must be activated in Sticky Password. Note that this feature is available only with Sticky Password Premium.
6.6 Documents

**Description**

Document entry types are used to store any type of document directly in the data source.

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.
Document types

In most cases, updating a document saves the new file name. Exceptions are: Email and HTML.

The different document types include settings to access the document:

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link to file</td>
<td>Enter the path to a file located on your PC or on your network.</td>
</tr>
<tr>
<td>Url</td>
<td>Open a file using a URL. You can also use your default Windows Credentials to open the file.</td>
</tr>
<tr>
<td>Stored in database</td>
<td>Select a file that will be stored in the database. Some data sources do not support this mode.</td>
</tr>
</tbody>
</table>

6.7 Folder

Description
Folders are used to organize your entries. You can set permission on folders to limit who can access the folder and what those users can do.

You can also set properties (e.g. Session Recording or Checkout mode) on the folder and then set child entries to inherit folder settings.

You can assign a folder type (e.g. Server) or use variables as a folder name (for more information, please consult the Variables topic).

Folder Properties

To decide how to access folder settings through properties or a specific folder properties button, the Show folder details/description option is available in the dashboard when a folder is selected.

1. Disable Show folder details/description: Use Folder Properties to edit folder settings and Properties to modify a selected entry.
2. Enable Show folder details/description: Use Properties to edit folder settings (The Folder Properties button is unavailable).

If the option Show folder details/description is unchecked (default setting), click Folder Properties to edit or view folder settings. Click Properties to edit the selected entry settings.
When the option *Show folder details/description* is checked, the *Folder Properties* button is unavailable. Click *Properties* to edit the selected folder instead of the entry.

**Folder settings**

Much of the information in folder properties is optional. Only include *Credentials*, *Username* or *Password* on the folder if you want to protect it. In most cases, leave the information blank (a).
You can set other settings on the folder. After set the entries within the folder to *inherit* the permissions.

Below is an example of a folder where the VPN is set at the folder level. All session entries within the folder inherit the VPN settings. The folder is also a *Server* type.
Example of VPN settings in Folder properties and an excerpt of the navigation pane to show the folder structure.

Another example is setting **Permissions** at the folder level to restrict access to sensitive information.
Folder Types

Multiple folder types are available. They have special icons to represent the type. You can access information from special entry types through variables: $FOLDERTYPE_variables$. For example, $COMPANY_variables$.

- Company
- Customer
- Database
- Device (router, switch firewall)
- Domain
- Folder
- Identity
- Printer
- Server
- Site
- Software
- Workstation

Database Folder

The Database folder provides some of the functionality of the Database session. In properties, press the ellipsis button to select the data source and data provider. This will generate the connection string with the information you enter in the dialog.
6.8 Synchronizer

Description

The Synchronizer family is a category of entries that can maintain Remote Desktop Manager in sync with an external data source. It will create sessions from information obtained from the source.

You should use security to prevent non-privileged users from using them.

Our recommendations are:

1. Disable the "Synchronize automatically" setting. If enabled, it runs after every data source refresh.

2. Use our "command line" feature and schedule a task to run it at the frequency of your choice. You can get the proper command line in the advanced properties of the synchronizer itself.

3. If the synchronizer changes a lot of sessions, it may be best to use a "RDM service account", meaning an account not used by one of your users. It will help clear our historical data from our logs.

Remote Desktop Manager has the following synchronizers:

- **Active Directory**: Creates session entries for each computer in Active Directory.
- **Comma Separated Values (CSV)**: Create entries for devices. See [Import Strategies and File Format](#) for more information about using the wizard and entry templates.
- **Spiceworks**
- **ConnectWise Control (ScreenConnect)**
- **Hyper-V**: Creates sessions for virtual machines on a Hyper-V server.
- **Device (router, switch firewall)**
- **VMWare**
- **Entries (.RDM, .PVM)**: Synchronize entries from a Remote Desktop Manager file.
- **Amazon EC2**: Create session entries for virtual machines on the web service.
- **KeePass Xml Synchronizer**: Create credential or website entries.

Duplicate entries

If running the synchronizer results in duplicate entries or other things you did not expect with entries, configure **Action on entry mismatch**. The option is on the [Advanced tab](#) in the Synchronizer entry properties.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action on entry mismatch</td>
<td>Choose the action to be executed when there is a mismatch between the entries:</td>
</tr>
<tr>
<td></td>
<td>- <strong>None</strong>: No action will be taken on the mismatch entry.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Delete</strong>: The mismatch entry will be deleted.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Move to</strong>: Move the mismatch entry to a designated folder.</td>
</tr>
</tbody>
</table>
**6.9 VPN**

**Description**

**VPN Entry** is used to configure a VPN. One VPN entry can be linked to multiple sessions. See [Configuring a VPN for multiple sessions](#) to see the step-by-step guide.

**VPNs and access to your data source**

Many organizations configure their devices to channel ALL traffic through the VPN. This may break the connection to your data source. When you are subject to this constraint, it is best to enable the **Offline Mode** in **Data Source Settings (System Settings)**, then configure the VPN options to automatically **Go offline on connection**.

For more information on how to manage VPN, please consult [VPN Management](#) topic.

**Supported VPNs**

There are multiple VPN entries already included in Remote Desktop Manager and many more are available through add-ons. Please consult [VPN Add-ons](#) for more information.

Supported VPNs include:

- Apple VPN
- CISCO VPN
- Microsoft VPN
- Sonicwall VPN
- OpenVPN
- And more!
Options

Go Offline on connection and Go Online on disconnect

The Go Offline on connection and Go Online on disconnect options are essential when all traffic is tunneled through the VPN and you lose connection to the data source. The data source must be configured to allow for Offline availability.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Go Offline on connection</td>
<td>The session goes offline once connected to the VPN.</td>
</tr>
<tr>
<td>Go Online on disconnect</td>
<td>The session goes back online once disconnected from the VPN.</td>
</tr>
<tr>
<td>Use adapter to detect</td>
<td>Use the adapter to detect the VPN connection.</td>
</tr>
<tr>
<td>connection</td>
<td></td>
</tr>
<tr>
<td>Close connection after</td>
<td>Close the VPN connection after the number of minutes indicated.</td>
</tr>
<tr>
<td>Detect reachable host in</td>
<td>Automatically close the VPN wait dialog when the host is reachable.</td>
</tr>
<tr>
<td>wait</td>
<td></td>
</tr>
</tbody>
</table>
After Execute Wait

You can adjust the time Remote Desktop Manager waits for the VPN to open. In the sec box, enter the 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.

Commands

In VPN properties – Advanced Tab, you can add commands. With custom commands you can execute any command after the VPN connects and/or before VPN disconnect.

6.10 Macros/Scripts/Tools

Description

The session script tools can be either a script, a command line, or a helper applicable to a selected session. Each can be configured and shared in the data source.

They are listed in the dashboard under the Macros/Scripts/Tools section or in the context menu under Macros/Scripts/Tools.

Session tools are commonly used to retrieve information, perform an action, change an item, or change a configuration on the session host. It can also be used to share properties between groups of sessions using PowerShell, PSEexec or keyboard macros.

Macros/Scripts/Tools can be used to run against a host as well as run your macro through the RDM Agent.

Session Variables can be used as parameters for the Macros/Scripts/Tools.

Macros/Scripts/Tools Manager
Entry - Macros/Scripts/Tools

General Settings

Those settings will be identical for every Macro/Scrip/Tools entry.
### Macros/Scripts/Tools - More Settings

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow run via agent</td>
<td>Allows you to launch a script through an Agent.</td>
</tr>
<tr>
<td>Automatically open target</td>
<td>Force the opening of a connection before executing the Macros/Scripts/Tools.</td>
</tr>
<tr>
<td>connection</td>
<td></td>
</tr>
<tr>
<td>Close target connection</td>
<td>Automatically close the connection after executing the Macros/Scripts/Tools.</td>
</tr>
<tr>
<td>connection after execution</td>
<td></td>
</tr>
<tr>
<td>Allow batch execute</td>
<td>Allows you to execute the macro on multiple machines at the same time.</td>
</tr>
<tr>
<td>Prompt for host</td>
<td>Automatically prompt for the host on every use.</td>
</tr>
<tr>
<td>Prompt for confirmation</td>
<td>Always prompts for a confirmation on use.</td>
</tr>
</tbody>
</table>

#### 6.10.1 PowerShell (Local)

**Description**

This entry is used to integrate a **PowerShell (Local)** session/script/tool.
We suggest to use either relative paths or in general paths **without spaces** or use the PowerShell Session to execute a script with parameters. Here some examples:

- Macro that can use Session Variables:
  `.\Data\ConnectAfterReboot.ps1 -strHost $HOST$ -OpenRDMSession`

- Session that can specify a filename and arguments:
  `.\data\New-RDM-Data.ps1
  -AddNewOnly`

### Settings

#### General

[Image of PowerShell (Local) - General Tab]
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>Enter the PowerShell command.</td>
</tr>
<tr>
<td>Assign file icon to session</td>
<td>Assign the file icon in the address bar of the session.</td>
</tr>
<tr>
<td>Arguments</td>
<td>Enter your command line argument. For more information please see Command Line Arguments.</td>
</tr>
<tr>
<td>Working directory</td>
<td>Working directory to set for the script execution.</td>
</tr>
<tr>
<td>PowerShell version</td>
<td>Select your PowerShell version between:</td>
</tr>
<tr>
<td></td>
<td>• Default</td>
</tr>
<tr>
<td></td>
<td>• Version 2</td>
</tr>
<tr>
<td>Wait for application to exit</td>
<td>Executes the script while the application waits for completion. Is it a</td>
</tr>
<tr>
<td>(Remote Desktop Manager will be synchronous operation therefore it will be unavailable)</td>
<td>unresponsive while the script runs.</td>
</tr>
<tr>
<td>Open embedded/tabbed</td>
<td>Open the PowerShell macro embedded.</td>
</tr>
<tr>
<td>Run as administrator</td>
<td>Run PowerShell macro as a administrator.</td>
</tr>
<tr>
<td>Resize window</td>
<td>Force window resize (buffer &amp; window).</td>
</tr>
<tr>
<td>Run in 64-bits mode</td>
<td>Run CmdLet in 64 bits version.</td>
</tr>
<tr>
<td>Run as different user</td>
<td>Run the PowerShell macro as a different user.</td>
</tr>
<tr>
<td>Load RDM CmdLet</td>
<td>Load CmdLet Snap-in in the PowerShell session.</td>
</tr>
<tr>
<td>No exit</td>
<td>Leaves the PowerShell window open after the script has completed.</td>
</tr>
<tr>
<td>Debug</td>
<td>Show debug</td>
</tr>
</tbody>
</table>

**Advanced**

- No exit
- Use SSL
- Resize window
- Run as Administrator
- Open embedded/tabbed
- Wait for application to exit (Remote Desktop Manager will be unavailable)
- Debug
- Load RDM CmdLet
- Run in 64-bit mode
- Run as different user
- Use session credentials
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>No exit</td>
<td>Leaves the PowerShell window open after the script has completed.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Use the SSL setting.</td>
</tr>
<tr>
<td>Resize window</td>
<td>Force window resize (buffer &amp; window).</td>
</tr>
<tr>
<td>Run as Administrator</td>
<td>Run PowerShell macro as an administrator.</td>
</tr>
<tr>
<td>Open embedded/tabbed</td>
<td>Open the PowerShell macro embedded.</td>
</tr>
<tr>
<td>Debug</td>
<td>Show debug</td>
</tr>
<tr>
<td>Load RDM CmdLet</td>
<td>Load CmdLet Snap-in in the PowerShell session.</td>
</tr>
<tr>
<td>Run in 64-bit mode</td>
<td>Run CmdLet in 64 bits version.</td>
</tr>
<tr>
<td>Run as different user</td>
<td>Run the PowerShell macro as a different user.</td>
</tr>
<tr>
<td>Use session credentials</td>
<td>Use the current session credentials.</td>
</tr>
<tr>
<td>Wait for application to exit (Remote Desktop Manager will be unavailable)</td>
<td>Executes the script while the application waits for completion. Is it a synchronous operation therefore it will be unresponsive while the script runs.</td>
</tr>
</tbody>
</table>

### 6.10.2 Template

#### Description

This entry is used to apply an existing Template to an entry. By configuring a specific template, it's possible to open a session with a completely different connection type. The original parameters will be merged with the one from the specified template.

#### Settings

![Template - General Tab](image)
For more information regarding using a template with an existing connection, please consult the link below:
https://help.remotedesktopmanager.com/tipsandtricks_typesconnections.htm

6.11 Variables

Description

Variables can be used in any entry’s configuration or with any templates. The variables will be replaced by their corresponding values just prior to establishing a connection.

You can select a variable by double clicking on it directly in the dialog. For ease of use there is a button at the bottom of the edition screen that allows you to select a variable to insert in the currently focused field.

Variables are case-sensitive and must be typed in UPPERCASE.

Settings
The variables are classify under multiple tabs. Not all contexts are available depending on the entry being edited, for example the Parent tab is present only when editing a sub connection.

**General**

$\text{$\text{PASSWORD}$}$: For security reason, this is only available with the command line session type and some specific types. You must enable it in the Security Settings of the entry with "Allow password in variable" option.

For an Advanced Data Source, the administrator can disable usage of this variable for the whole data source in Data Source Settings (System Settings), at the bottom of the Password Management tab.
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>$APPLICATION_NAME$</td>
<td>Returns the application name.</td>
</tr>
<tr>
<td>$CONTACT_DOMAIN$</td>
<td>Returns the contact's domain.</td>
</tr>
<tr>
<td>$CONTACT_PASSWORD$</td>
<td>Returns the contact's password.</td>
</tr>
<tr>
<td>$CONTACT_USERNAME$</td>
<td>Returns the contact's username.</td>
</tr>
<tr>
<td>$CURRENT_CLIPBOARD$</td>
<td>Returns the current clipboard content.</td>
</tr>
<tr>
<td>$CUSTOM_FIELD1$</td>
<td>Returns the custom field field 1 value.</td>
</tr>
<tr>
<td>$CUSTOM_FIELD2$</td>
<td>Returns the custom field field 2 value.</td>
</tr>
<tr>
<td>$CUSTOM_FIELD3$</td>
<td>Returns the custom field field 3 value.</td>
</tr>
<tr>
<td>$CUSTOM_FIELD4$</td>
<td>Returns the custom field field 4 value.</td>
</tr>
<tr>
<td>$CUSTOM_FIELD5$</td>
<td>Returns the custom field field 5 value.</td>
</tr>
<tr>
<td>$DATA_SOURCE_ID$</td>
<td>Returns the data source id for the current session.</td>
</tr>
<tr>
<td>$DOMAIN$</td>
<td>Returns the domain found in the configured credentials.</td>
</tr>
<tr>
<td>$DYNAMIC_PORTS$</td>
<td>Returns the dynamic port used when the entry uses an SSH VPN with a dynamic port set up.</td>
</tr>
<tr>
<td>$HOST$</td>
<td>Returns the host name if it's available (server name or IP address...).</td>
</tr>
<tr>
<td>$HOST_WITH_PORT$</td>
<td>Returns the host including the port if it is available.</td>
</tr>
<tr>
<td>$HOST_WITHOUT_DOMAIN$</td>
<td>Returns the host name without the domain if it is available.</td>
</tr>
<tr>
<td>$INFORMATION_COMPANY$</td>
<td>Returns the company specified in information.</td>
</tr>
<tr>
<td>$INFORMATION_EMAIL$</td>
<td>Returns the email specified in information.</td>
</tr>
<tr>
<td>$INFORMATION_IP$</td>
<td>Returns the information IP.</td>
</tr>
<tr>
<td>$INFORMATION_MACHINE_NAME$</td>
<td>Returns the machine name specified in information.</td>
</tr>
<tr>
<td>$IP$</td>
<td>Returns the IP specified in information.</td>
</tr>
<tr>
<td>$KEYWORDS$</td>
<td>Returns the keywords/tags.</td>
</tr>
<tr>
<td>$MAC$</td>
<td>Returns the MAC address specified in information.</td>
</tr>
<tr>
<td>$MACHINE_DOMAIN$</td>
<td>Returns the machine domain specified in information.</td>
</tr>
<tr>
<td>$MACRO_PASSWORD$</td>
<td>Returns the typing macro password.</td>
</tr>
<tr>
<td>$NAME$</td>
<td>Returns the entry name.</td>
</tr>
<tr>
<td>$ONE_TIME_PASSWORD$</td>
<td>Returns a timed one time password.</td>
</tr>
<tr>
<td>$PASSWORD$</td>
<td>This variable is replaced by the password. It's only available when enabled in the advanced options.</td>
</tr>
<tr>
<td>$PORT$</td>
<td>Returns the host port if it's available and when it's not the default.</td>
</tr>
<tr>
<td>$QUICK_CONNECT$</td>
<td>This variable is replaced by the quick connect value (Note). Use this variable when you create a template used specifically for the quick connect.</td>
</tr>
<tr>
<td>$REMOTE_MANAGEMENT_SERVER$</td>
<td>Returns the Remote Management Server url (if configured).</td>
</tr>
<tr>
<td>$REMOTE_MANAGEMENT_SERVER_HOST$</td>
<td>Returns the host part of the Remote Management Server url (if configured).</td>
</tr>
<tr>
<td>$SERIAL$</td>
<td>Returns the serial number from invoice tab.</td>
</tr>
<tr>
<td>$SERVICE_TAG$</td>
<td>Returns the service tag field specified in information.</td>
</tr>
<tr>
<td>$SESSION_ID$</td>
<td>Returns the current session id (guid).</td>
</tr>
<tr>
<td>$TAGS$</td>
<td>Returns the tags.</td>
</tr>
<tr>
<td>$TOOL_DOMAIN$</td>
<td>Returns the tool domain.</td>
</tr>
<tr>
<td>$TOOL_PASSWORD$</td>
<td>Returns the tool password.</td>
</tr>
</tbody>
</table>
### Global variables

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>$APPLICATION_PATH$</td>
<td>Returns the application path.</td>
</tr>
<tr>
<td>$APPLICATION_USER$</td>
<td>Returns the current data source logged user.</td>
</tr>
<tr>
<td>$DATE$</td>
<td>Returns the current date.</td>
</tr>
<tr>
<td>$DATE_TEXT$</td>
<td>Returns the current date in a text format to use in a file name. Ex: January 30th 2013 - 20130130.</td>
</tr>
<tr>
<td>$DATE_TEXT_ISO$</td>
<td>Returns the current date in a basic ISO 8601 format. EX: January 30th 2013 - 20130130.</td>
</tr>
<tr>
<td>$FULLSCREEN_HEIGHT$</td>
<td>Returns the screen full screen height.</td>
</tr>
<tr>
<td>$FULLSCREEN_WIDTH$</td>
<td>Returns the screen full screen width.</td>
</tr>
<tr>
<td>$LOCAL_IP$</td>
<td>Returns the local IP v4 address.</td>
</tr>
<tr>
<td>$MY_MACHINE_NAME$</td>
<td>Returns the current machine name.</td>
</tr>
<tr>
<td>$PUBLIC_IP$</td>
<td>Returns the public IP exposed on the internet.</td>
</tr>
<tr>
<td>$TIME$</td>
<td>Returns the current time.</td>
</tr>
<tr>
<td>$TIME_TEXT$</td>
<td>Returns the current time in a text format to use in a file name. Ex: 8h15 30 - 081530</td>
</tr>
<tr>
<td>$TIME_TEXT_ISO$</td>
<td>Returns the text of the current time in the basic ISO 8601 format. Ex: 8h15 30 - 081530</td>
</tr>
<tr>
<td>$WORKAREA_HEIGHT$</td>
<td>Returns the screen work area height.</td>
</tr>
<tr>
<td>$WORKAREA_WIDTH$</td>
<td>Returns the screen work area width.</td>
</tr>
</tbody>
</table>

### Global - Data Source variables

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>$DATA_SOURCE_DOMAIN$</td>
<td>Returns the current data source domain.</td>
</tr>
<tr>
<td>$DATA_SOURCE_NAME$</td>
<td>Returns the current data source name.</td>
</tr>
<tr>
<td>$DATA_SOURCE_PASSWORD$</td>
<td>Returns the current data source password.</td>
</tr>
<tr>
<td>$DATA_SOURCE_USERNAME$</td>
<td>Returns the current data source username.</td>
</tr>
<tr>
<td>$DATA_SOURCE_USERPROFILE_EMAIL$</td>
<td>Returns the current data source user's email.</td>
</tr>
<tr>
<td>$DATA_SOURCE_USERPROFILE_FIRSTNAME$</td>
<td>Returns the current data source user's firstname.</td>
</tr>
<tr>
<td>$DATA_SOURCE_USERPROFILE_LASTNAME$</td>
<td>Returns the current data source user's lastname.</td>
</tr>
<tr>
<td>$DATA_SOURCE_USERPROFILE_PHONE$</td>
<td>Returns the current data source user's phone number.</td>
</tr>
</tbody>
</table>

### Environment Variables

This context allows you to access ANY environment variable defined in your system. The ones available in the form are the standard ones, but any value enclosed by the percent sign will be expanded using the
Windows environment. You could use this to set a custom security token in your user profile and use it from within Remote Desktop Manager.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>%ALLUSERSPROFILE%</td>
<td>C:\ProgramData</td>
</tr>
<tr>
<td>%APPDATA%</td>
<td>C:\Users{username}\AppData\Roaming</td>
</tr>
<tr>
<td>%COMMONPROGRAMFILES%</td>
<td>C:\Program Files\Common Files</td>
</tr>
<tr>
<td>%COMMONPROGRAMFILES(x86)%</td>
<td>C:\Program Files (x86)\Common Files</td>
</tr>
<tr>
<td>%COMPUTERNAME%</td>
<td>{computername}</td>
</tr>
<tr>
<td>%COMSPEC%</td>
<td>C:\Windows\System32\cmd.exe</td>
</tr>
<tr>
<td>%HOMEDRIVE%</td>
<td>C:</td>
</tr>
<tr>
<td>%HOMEPATH%</td>
<td>\Users{username}</td>
</tr>
<tr>
<td>%LOCALAPPDATA%</td>
<td>C:\Users{username}\AppData\Local</td>
</tr>
<tr>
<td>%LOGONSERVER%</td>
<td>\{domain_logon_server}</td>
</tr>
<tr>
<td>%PATH%</td>
<td>C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;{plus program paths}</td>
</tr>
<tr>
<td>%PATHEXT%</td>
<td>.com;.exe;.bat;.cmd;.vbs;.vbe;.js;.jse;.wsf;.wsh;.msc</td>
</tr>
<tr>
<td>%PROGRAMDATA%</td>
<td>%SystemDrive%\ProgramData</td>
</tr>
<tr>
<td>%PROGRAMFILES%</td>
<td>%SystemDrive%\Program Files</td>
</tr>
<tr>
<td>%PROGRAMFILES(X86)%</td>
<td>%SystemDrive%\Program Files (x86) (only in 64-bit version)</td>
</tr>
<tr>
<td>%PROMPT%</td>
<td>Code for current command prompt format. Code is usually $P$G {Drive}:</td>
</tr>
<tr>
<td>%PSModulePath%</td>
<td>%SystemRoot%\system32\WindowsPowerShell\v1.0\Modules\</td>
</tr>
<tr>
<td>%PUBLIC%</td>
<td>%SystemDrive%\Users\Public</td>
</tr>
<tr>
<td>%SystemDrive%</td>
<td>C:</td>
</tr>
<tr>
<td>%SystemRoot%</td>
<td>%SystemDrive%\Windows</td>
</tr>
<tr>
<td>%TEMP%</td>
<td>%SystemDrive%\Users{username}\AppData\Local\Temp</td>
</tr>
<tr>
<td>%TMP%</td>
<td>%SystemDrive%\Users{username}\AppData\Local\Temp</td>
</tr>
<tr>
<td>%USERDOMAIN%</td>
<td>{userdomain}</td>
</tr>
<tr>
<td>%USERNAME%</td>
<td>{username}</td>
</tr>
<tr>
<td>%USERPROFILE%</td>
<td>%SystemDrive%\Users{username}</td>
</tr>
<tr>
<td>%WINDIR%</td>
<td>C:Windows</td>
</tr>
</tbody>
</table>

**Group**

**Parent**

This context exists only when in a sub-connection. It returns the corresponding value taken from the parent entry.
$\text{PARENT_PASSWORD}$: For security reason, this is only available for use in the keyboard macro. If you must use the credentials stored in the parent to connect, you must choose Parent in the credentials drop down list of the general tab.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{PARENT_APPLICATION_NAME}$</td>
<td>Returns the application name.</td>
</tr>
<tr>
<td>$\text{PARENT_CURRENT_CLIPBOARD}$</td>
<td>Returns the current clipboard content.</td>
</tr>
<tr>
<td>$\text{PARENT_CUSTOM_FIELD1}$</td>
<td>Returns the parent custom field field 1 value.</td>
</tr>
<tr>
<td>$\text{PARENT_CUSTOM_FIELD2}$</td>
<td>Returns the parent custom field field 2 value.</td>
</tr>
<tr>
<td>$\text{PARENT_CUSTOM_FIELD3}$</td>
<td>Returns the parent custom field field 3 value.</td>
</tr>
<tr>
<td>$\text{PARENT_CUSTOM_FIELD4}$</td>
<td>Returns the parent custom field field 4 value.</td>
</tr>
<tr>
<td>$\text{PARENT_CUSTOM_FIELD5}$</td>
<td>Returns the parent custom field field 5 value.</td>
</tr>
<tr>
<td>$\text{PARENT_DOMAIN}$</td>
<td>Returns the parent domain found in the parent configured credentials.</td>
</tr>
<tr>
<td>$\text{PARENT_HOST}$</td>
<td>Returns the parent host name if it's available (server name or IP address...).</td>
</tr>
<tr>
<td>$\text{PARENT_HOST_WITH_PORT}$</td>
<td>Returns the parent host including the port if it's specified.</td>
</tr>
<tr>
<td>$\text{PARENT_HOST_WITHOUT_DOMAIN}$</td>
<td>Returns the host name without the domain if it's available.</td>
</tr>
<tr>
<td>$\text{PARENT_INFORMATION_COMPANY}$</td>
<td>Returns the company specified in the parent information.</td>
</tr>
<tr>
<td>$\text{PARENT_INFORMATION_EMAIL}$</td>
<td>Returns the email specified in information.</td>
</tr>
<tr>
<td>$\text{PARENT_INFORMATION_MACHINE_NAME}$</td>
<td>Returns the machine name specified in information.</td>
</tr>
<tr>
<td>$\text{PARENT_IP}$</td>
<td>Returns the IP address specified in parent information.</td>
</tr>
<tr>
<td>$\text{PARENT_MAC}$</td>
<td>Returns the MAC address defined.</td>
</tr>
<tr>
<td>$\text{PARENT_MACRO_PASSWORD}$</td>
<td>Returns the typing macro password.</td>
</tr>
<tr>
<td>$\text{PARENT_NAME}$</td>
<td>Returns the session name.</td>
</tr>
<tr>
<td>$\text{PARENT_PASSWORD}$</td>
<td>Returns the password from the parent configured credentials. It's only available when enabled in the parent advanced options.</td>
</tr>
<tr>
<td>$\text{PARENT_PORT}$</td>
<td>Returns the host port if it's available (server name, IP address...).</td>
</tr>
<tr>
<td>$\text{PARENT_SERIAL}$</td>
<td>Returns the serial number in the invoice tab.</td>
</tr>
<tr>
<td>$\text{PARENT_SERVICE_TAGS}$</td>
<td>Returns the service tag field located in the information tab.</td>
</tr>
<tr>
<td>$\text{PARENT_SESSION_ID}$</td>
<td>Returns the parent session id (guid).</td>
</tr>
<tr>
<td>$\text{PARENT_TOOL_DOMAIN}$</td>
<td>Returns the tool domain.</td>
</tr>
<tr>
<td>$\text{PARENT_TOOL_PASSWORD}$</td>
<td>Returns the tool password.</td>
</tr>
<tr>
<td>$\text{PARENT_TOOL_USERNAME}$</td>
<td>Returns the tool username.</td>
</tr>
<tr>
<td>$\text{PARENT_USERNAME}$</td>
<td>Returns the username from the parent configured credentials.</td>
</tr>
<tr>
<td>$\text{PARENT_VIRTUAL_MACHINE_ID}$</td>
<td>Returns the virtual machine ID specified in information.</td>
</tr>
</tbody>
</table>
The following context will find any Folder Database entry type as long as it is in the hierarchy above your current entry. If there is multiple matches it will take the entry closest in the hierarchy to the current entry.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>$DB_APPLICATION_NAME$</td>
<td>Returns the application name.</td>
</tr>
<tr>
<td>$DB_CURRENT_CLIPBOARD$</td>
<td>Returns the current clipboard content.</td>
</tr>
<tr>
<td>$DB_CUSTOM_FIELD1$</td>
<td>Returns the database custom field field 1 value.</td>
</tr>
<tr>
<td>$DB_CUSTOM_FIELD2$</td>
<td>Returns the database custom field field 2 value.</td>
</tr>
<tr>
<td>$DB_CUSTOM_FIELD3$</td>
<td>Returns the database custom field field 3 value.</td>
</tr>
<tr>
<td>$DB_CUSTOM_FIELD4$</td>
<td>Returns the database custom field field 4 value.</td>
</tr>
<tr>
<td>$DB_CUSTOM_FIELD5$</td>
<td>Returns the database custom field field 5 value.</td>
</tr>
<tr>
<td>$DB_DOMAIN$</td>
<td>Returns the domain found in the configured credentials.</td>
</tr>
<tr>
<td>$DB_INFORMATION_COMPANY$</td>
<td>Returns the company specified in the database information.</td>
</tr>
<tr>
<td>$DB_INFORMATION_EMAIL$</td>
<td>Returns the information email.</td>
</tr>
<tr>
<td>$DB_INFORMATION_MACHINE_NAME$</td>
<td>Returns the information machine name.</td>
</tr>
<tr>
<td>$DB_NAME$</td>
<td>Returns the session name.</td>
</tr>
<tr>
<td>$DB_SERIAL$</td>
<td>Returns the serial number in the invoice tab.</td>
</tr>
<tr>
<td>$DB_SERVICE_TAG$</td>
<td>Returns the service tag field located in the information tab.</td>
</tr>
<tr>
<td>$DB_VIRTUAL_MACHINE_ID$</td>
<td>Returns the virtual machine ID.</td>
</tr>
</tbody>
</table>

Domain

The following context will find any Folder Domain entry type as long as it is in the hierarchy above your current entry. If there is multiple matches it will take the entry closest in the hierarchy to the current entry.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>$DOMAIN_APPLICATION_NAME$</td>
<td>Returns the application name.</td>
</tr>
<tr>
<td>$DOMAIN_CURRENT_CLIPBOARD$</td>
<td>Returns the current clipboard content.</td>
</tr>
<tr>
<td>$DOMAIN_CUSTOM_FIELD1$</td>
<td>Returns the domain custom field field 1 value.</td>
</tr>
<tr>
<td>$DOMAIN_CUSTOM_FIELD2$</td>
<td>Returns the domain custom field field 2 value.</td>
</tr>
<tr>
<td>$DOMAIN_CUSTOM_FIELD3$</td>
<td>Returns the domain custom field field 3 value.</td>
</tr>
<tr>
<td>$DOMAIN_CUSTOM_FIELD4$</td>
<td>Returns the domain custom field field 4 value.</td>
</tr>
<tr>
<td>$DOMAIN_CUSTOM_FIELD5$</td>
<td>Returns the domain custom field field 5 value.</td>
</tr>
<tr>
<td>$DOMAIN_DOMAIN$</td>
<td>Returns the domain found in the configured credentials.</td>
</tr>
<tr>
<td>$DOMAIN_INFORMATION_COMPANY$</td>
<td>Returns the company specified in the domain information.</td>
</tr>
<tr>
<td>$DOMAIN_INFORMATION_EMAIL$</td>
<td>Returns the information email.</td>
</tr>
<tr>
<td>$DOMAIN_INFORMATION_MACHINE_NAME$</td>
<td>Returns the information machine name.</td>
</tr>
<tr>
<td>$DOMAIN_NAME$</td>
<td>Returns the session name.</td>
</tr>
<tr>
<td>$DOMAIN_SERIAL$</td>
<td>Returns the serial number in the invoice tab.</td>
</tr>
<tr>
<td>$DOMAIN_SERVICE_TAG$</td>
<td>Returns the service tag field located in the information tab.</td>
</tr>
<tr>
<td>$DOMAIN_VIRTUAL_MACHINE_ID$</td>
<td>Returns the virtual machine ID.</td>
</tr>
</tbody>
</table>
**Company**

The following context will find any Folder Company entry type as long as it is in the hierarchy above your current entry. If there is multiple matches it will take the entry closest in the hierarchy to the current entry.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>$COMPANY_APPLICATION_NAME$</td>
<td>Returns the application name.</td>
</tr>
<tr>
<td>$COMPANY_CURRENT_CLIPBOARD$</td>
<td>Returns the current clipboard content.</td>
</tr>
<tr>
<td>$COMPANY_CUSTOM_FIELD1$</td>
<td>Returns the company custom field field 1 value.</td>
</tr>
<tr>
<td>$COMPANY_CUSTOM_FIELD2$</td>
<td>Returns the company custom field field 2 value.</td>
</tr>
<tr>
<td>$COMPANY_CUSTOM_FIELD3$</td>
<td>Returns the company custom field field 3 value.</td>
</tr>
<tr>
<td>$COMPANY_CUSTOM_FIELD4$</td>
<td>Returns the company custom field field 4 value.</td>
</tr>
<tr>
<td>$COMPANY_CUSTOM_FIELD5$</td>
<td>Returns the company custom field field 5 value.</td>
</tr>
<tr>
<td>$COMPANY_DOMAIN$</td>
<td>Returns the domain found in the configured credentials.</td>
</tr>
<tr>
<td>$COMPANY_INFORMATION_COMPANY$</td>
<td>Returns the company specified in the company information.</td>
</tr>
<tr>
<td>$COMPANY_INFORMATION_EMAIL$</td>
<td>Returns the information email.</td>
</tr>
<tr>
<td>$COMPANY_INFORMATION_MACHINE_NAME$</td>
<td>Returns the information machine name.</td>
</tr>
<tr>
<td>$COMPANY_NAME$</td>
<td>Returns the session name.</td>
</tr>
<tr>
<td>$COMPANY_SERIAL$</td>
<td>Returns the serial number in the invoice tab.</td>
</tr>
<tr>
<td>$COMPANY_SERVICE_TAG$</td>
<td>Returns the service tag field located in the information tab.</td>
</tr>
<tr>
<td>$COMPANY_VIRTUAL_MACHINE_ID$</td>
<td>Returns the virtual machine ID.</td>
</tr>
</tbody>
</table>

**Software**

The following context will find any Folder Software entry type as long as it is in the hierarchy above your current entry. If there is multiple matches it will take the entry closest in the hierarchy to the current entry.
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>$SOFTWARE_APPLICATION_NAME$</td>
<td>Returns the application name.</td>
</tr>
<tr>
<td>$SOFTWARE_CURRENT_CLIPBOARD$</td>
<td>Returns the current clipboard content.</td>
</tr>
<tr>
<td>$SOFTWARE_CUSTOM_FIELD1$</td>
<td>Returns the custom field field 1 value.</td>
</tr>
<tr>
<td>$SOFTWARE_CUSTOM_FIELD2$</td>
<td>Returns the custom field field 2 value.</td>
</tr>
<tr>
<td>$SOFTWARE_CUSTOM_FIELD3$</td>
<td>Returns the custom field field 3 value.</td>
</tr>
<tr>
<td>$SOFTWARE_CUSTOM_FIELD4$</td>
<td>Returns the custom field field 4 value.</td>
</tr>
<tr>
<td>$SOFTWARE_CUSTOM_FIELD5$</td>
<td>Returns the custom field field 5 value.</td>
</tr>
<tr>
<td>$SOFTWARE_DOMAIN$</td>
<td>Returns the domain found in the configured credentials.</td>
</tr>
<tr>
<td>$SOFTWARE_INFORMATION_COMPANY$</td>
<td>Returns the information Company.</td>
</tr>
<tr>
<td>$SOFTWARE_INFORMATION_EMAIL$</td>
<td>Returns the information email.</td>
</tr>
<tr>
<td>$SOFTWARE_INFORMATION_MACHINE_NAME$</td>
<td>Returns the information machine name.</td>
</tr>
<tr>
<td>$SOFTWARE_NAME$</td>
<td>Returns the session name.</td>
</tr>
<tr>
<td>$SOFTWARE_SERIAL$</td>
<td>Returns the serial number in the invoice tab.</td>
</tr>
<tr>
<td>$SOFTWARE_SERVICE_TAG$</td>
<td>Returns the service tag field located in the information tab.</td>
</tr>
<tr>
<td>$SOFTWARE_VIRTUAL_MACHINE_ID$</td>
<td>Returns the virtual machine ID.</td>
</tr>
</tbody>
</table>

**Site**

The following context will find any Folder Site entry type as long as it is in the hierarchy above your current entry. If there is multiple matches it will take the entry closest in the hierarchy to the current entry.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>$SITE_APPLICATION_NAME$</td>
<td>Returns the application name.</td>
</tr>
<tr>
<td>$SITE_CURRENT_CLIPBOARD$</td>
<td>Returns the current clipboard content.</td>
</tr>
<tr>
<td>$SITE_CUSTOM_FIELD1$</td>
<td>Returns the site custom field field 1 value.</td>
</tr>
<tr>
<td>$SITE_CUSTOM_FIELD2$</td>
<td>Returns the site custom field field 2 value.</td>
</tr>
<tr>
<td>$SITE_CUSTOM_FIELD3$</td>
<td>Returns the site custom field field 3 value.</td>
</tr>
<tr>
<td>$SITE_CUSTOM_FIELD4$</td>
<td>Returns the site custom field field 4 value.</td>
</tr>
<tr>
<td>$SITE_CUSTOM_FIELD5$</td>
<td>Returns the site custom field field 5 value.</td>
</tr>
<tr>
<td>$SITE_DOMAIN$</td>
<td>Returns the domain found in the configured credentials.</td>
</tr>
<tr>
<td>$SITE_INFORMATION_COMPANY$</td>
<td>Returns the company specified in the site information.</td>
</tr>
<tr>
<td>$SITE_INFORMATION_EMAIL$</td>
<td>Returns the information email.</td>
</tr>
<tr>
<td>$SITE_INFORMATION_MACHINE_NAME$</td>
<td>Returns the information machine name.</td>
</tr>
<tr>
<td>$SITE_NAME$</td>
<td>Returns the session name.</td>
</tr>
<tr>
<td>$SITE_SERIAL$</td>
<td>Returns the serial number in the invoice tab.</td>
</tr>
<tr>
<td>$SITE_SERVICE_TAG$</td>
<td>Returns the service tag field located in the information tab.</td>
</tr>
<tr>
<td>$SITE_VIRTUAL_MACHINE_ID$</td>
<td>Returns the virtual machine ID.</td>
</tr>
</tbody>
</table>
## Computer/Hardware

The following context will find any Folder Device, Printer and Workstation entry type as long as it is in the hierarchy above your current entry. If there is multiple matches it will take the entry closest in the hierarchy to the current entry.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{COMPUTER_APPLICATION_NAME}$</td>
<td>Returns the application name.</td>
</tr>
<tr>
<td>$\text{COMPUTER_CURRENT_CLIPBOARD}$</td>
<td>Returns the current clipboard content.</td>
</tr>
<tr>
<td>$\text{COMPUTER_CUSTOM_FIELD1}$</td>
<td>Returns the computer custom field field 1 value.</td>
</tr>
<tr>
<td>$\text{COMPUTER_CUSTOM_FIELD2}$</td>
<td>Returns the computer custom field field 2 value.</td>
</tr>
<tr>
<td>$\text{COMPUTER_CUSTOM_FIELD3}$</td>
<td>Returns the computer custom field field 3 value.</td>
</tr>
<tr>
<td>$\text{COMPUTER_CUSTOM_FIELD4}$</td>
<td>Returns the computer custom field field 4 value.</td>
</tr>
<tr>
<td>$\text{COMPUTER_CUSTOM_FIELD5}$</td>
<td>Returns the computer custom field field 5 value.</td>
</tr>
<tr>
<td>$\text{COMPUTER_DOMAIN}$</td>
<td>Returns the computer domain found in the configured credentials.</td>
</tr>
<tr>
<td>$\text{COMPUTER_HOST}$</td>
<td>Returns the host name if it's available (server name, IP address...).</td>
</tr>
<tr>
<td>$\text{COMPUTER_HOST_WITHOUT_DOMAIN}$</td>
<td>Returns the host name without the domain if it's available.</td>
</tr>
<tr>
<td>$\text{COMPUTER_INFORMATION_COMPANY}$</td>
<td>Returns the company specified in the computer information.</td>
</tr>
<tr>
<td>$\text{COMPUTER_INFORMATION_EMAIL}$</td>
<td>Returns the information email.</td>
</tr>
<tr>
<td>$\text{COMPUTER_INFORMATION_MACHINE_NAME}$</td>
<td>Returns the information machine name.</td>
</tr>
<tr>
<td>$\text{COMPUTER_IP}$</td>
<td>Returns the IP Address.</td>
</tr>
<tr>
<td>$\text{COMPUTER_MAC}$</td>
<td>Returns the MAC address defined.</td>
</tr>
<tr>
<td>$\text{COMPUTER_NAME}$</td>
<td>Returns the session name.</td>
</tr>
<tr>
<td>$\text{COMPUTER_SERIAL}$</td>
<td>Returns the serial number in the invoice tab.</td>
</tr>
<tr>
<td>$\text{COMPUTER_SERVICE_TAG}$</td>
<td>Returns the service tag field located in the information tab.</td>
</tr>
<tr>
<td>$\text{COMPUTER_VIRTUAL_MACHINE_ID}$</td>
<td>Returns the virtual machine ID.</td>
</tr>
</tbody>
</table>

## Identity

The following context will find any Folder Identity entry type as long as it is in the hierarchy above you current entry. If there is multiple matches it will take the entry closest in the hierarchy to the current entry.
## IDENTITY

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$IDENTITY_APPLICATION_NAME$</td>
<td>Returns the application name.</td>
</tr>
<tr>
<td>$IDENTITY_CURRENT_CLIPBOARD$</td>
<td>Returns the current clipboard content.</td>
</tr>
<tr>
<td>$IDENTITY_CUSTOM_FIELD1$</td>
<td>Returns the identity custom field field 1 value.</td>
</tr>
<tr>
<td>$IDENTITY_CUSTOM_FIELD2$</td>
<td>Returns the identity custom field field 2 value.</td>
</tr>
<tr>
<td>$IDENTITY_CUSTOM_FIELD3$</td>
<td>Returns the identity custom field field 3 value.</td>
</tr>
<tr>
<td>$IDENTITY_CUSTOM_FIELD4$</td>
<td>Returns the identity custom field field 4 value.</td>
</tr>
<tr>
<td>$IDENTITY_CUSTOM_FIELD5$</td>
<td>Returns the identity custom field field 5 value.</td>
</tr>
<tr>
<td>$IDENTITY_DOMAIN$</td>
<td>Returns the domain found in the configured credentials.</td>
</tr>
<tr>
<td>$IDENTITY_INFORMATION_COMPANY$</td>
<td>Returns the company specified in the identity information.</td>
</tr>
<tr>
<td>$IDENTITY_INFORMATION_EMAIL$</td>
<td>Returns the information email.</td>
</tr>
<tr>
<td>$IDENTITY_INFORMATION_MACHINE_NAME$</td>
<td>Returns the information machine name.</td>
</tr>
<tr>
<td>$IDENTITY_NAME$</td>
<td>Returns the session name.</td>
</tr>
<tr>
<td>$IDENTITY_SERIAL$</td>
<td>Returns the serial number in the invoice tab.</td>
</tr>
<tr>
<td>$IDENTITY_SERVICE_TAG$</td>
<td>Returns the service tag field located in the information tab.</td>
</tr>
<tr>
<td>$IDENTITY_VIRTUAL_MACHINE_ID$</td>
<td>Returns the virtual machine ID.</td>
</tr>
</tbody>
</table>

## CUSTOMER

The following context will find any Folder Customer entry type as long as it is in the hierarchy above your current entry. If there is multiple matches it will take the entry closest in the hierarchy to the current entry.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$CUSTOMER_APPLICATION_NAME$</td>
<td>Returns the application name.</td>
</tr>
<tr>
<td>$CUSTOMER_CURRENT_CLIPBOARD$</td>
<td>Returns the current clipboard content.</td>
</tr>
<tr>
<td>$CUSTOMER_CUSTOM_FIELD1$</td>
<td>Returns the customer custom field field 1 value.</td>
</tr>
<tr>
<td>$CUSTOMER_CUSTOM_FIELD2$</td>
<td>Returns the customer custom field field 2 value.</td>
</tr>
<tr>
<td>$CUSTOMER_CUSTOM_FIELD3$</td>
<td>Returns the customer custom field field 3 value.</td>
</tr>
<tr>
<td>$CUSTOMER_CUSTOM_FIELD4$</td>
<td>Returns the customer custom field field 4 value.</td>
</tr>
<tr>
<td>$CUSTOMER_CUSTOM_FIELD5$</td>
<td>Returns the customer custom field field 5 value.</td>
</tr>
<tr>
<td>$CUSTOMER_DOMAIN$</td>
<td>Returns the domain found in the configured credentials.</td>
</tr>
<tr>
<td>$CUSTOMER_INFORMATION_COMPANY$</td>
<td>Returns the company specified in the customer information.</td>
</tr>
<tr>
<td>$CUSTOMER_INFORMATION_EMAIL$</td>
<td>Returns the information email.</td>
</tr>
<tr>
<td>$CUSTOMER_INFORMATION_MACHINE_NAME$</td>
<td>Returns the information machine name.</td>
</tr>
<tr>
<td>$CUSTOMER_NAME$</td>
<td>Returns the session name.</td>
</tr>
<tr>
<td>$CUSTOMER_SERIAL$</td>
<td>Returns the serial number in the invoice tab.</td>
</tr>
<tr>
<td>$CUSTOMER_SERVICE_TAG$</td>
<td>Returns the service tag field located in the information tab.</td>
</tr>
<tr>
<td>$CUSTOMER_VIRTUAL_MACHINE_ID$</td>
<td>Returns the virtual machine ID.</td>
</tr>
</tbody>
</table>
Custom fields

Custom fields can contain any required data and can be accessed using the "_CUSTOM_FIELD" variables. To access custom fields, select an entry, then click Information in the entry overview in the dashboard. Finally, choose the Custom Fields tab.

Quick Connect

The $QUICK_CONNECT$ variable will be replaced by the value in the Quick Connect control as described in Quick Connect. It is only useful when a template connection is selected.
Part VII

Commands
7 Commands

7.1 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.

- Open Session
- Check Out
  - Open with Parameters
- View Password
- Copy Username and Password
- Copy Username
- Copy Password
- Execute Script Via Agent
- New Entry
- Duplicate Ctrl+D
  - Add
  - Edit
- Move...
- Delete... Ctrl+Del
- Favorite
- Play List
  - Clipboard
  - Macros/Scripts/Tools
  - View
  - Import
  - Export
  - Expand All Ctrl +
  - Collapse All Ctrl -
  - Properties

7.1.1 Open with Parameters

Description

The Open with Parameters menu all options available to open a session.
## 7.2 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.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open (External)</td>
<td>Open a session as an external process, with no direct link to Remote Desktop Manager.</td>
</tr>
<tr>
<td>Open (Embedded/Tabbed)</td>
<td>Open the session within the confines of the Remote Desktop Manager dashboard and display tabs at the top of the window.</td>
</tr>
<tr>
<td>Open via Jump...</td>
<td>Open the session through a <a href="#">Jump</a> host.</td>
</tr>
<tr>
<td>Open (Full Screen)</td>
<td>Open the session with the full screen display mode.</td>
</tr>
<tr>
<td>Open in Console/Admin Mode</td>
<td>Connect to the console session of a server using Remote Desktop for Administration.</td>
</tr>
<tr>
<td>Open (Select Credentials)...</td>
<td>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.</td>
</tr>
<tr>
<td>Open in No Console/Admin Mode (Prompt for Credentials)</td>
<td>Open your session normally and prompt your for your credentials to connect.</td>
</tr>
<tr>
<td>Open Share Folders</td>
<td>Open the shared folders of the remote computer.</td>
</tr>
<tr>
<td>Open with a Template...</td>
<td>Open from a template that you have already created.</td>
</tr>
<tr>
<td>VPN</td>
<td>Select between:</td>
</tr>
<tr>
<td></td>
<td>- Open (Without VPN).</td>
</tr>
<tr>
<td></td>
<td>- Open VPN Only.</td>
</tr>
<tr>
<td></td>
<td>- Close VPN Only.</td>
</tr>
</tbody>
</table>
**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 Cloud 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.

7.2.1 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).
Several features are not available in offline mode, such as:

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

### 7.2.2 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

<table>
<thead>
<tr>
<th>ID</th>
<th>Server</th>
<th>Database</th>
<th>TCP</th>
<th>v1.523</th>
<th>JaqJaDen</th>
</tr>
</thead>
</table>

| 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
<table>
<thead>
<tr>
<th>Entries</th>
<th>Security Groups (Legacy)</th>
<th>Roles</th>
</tr>
</thead>
</table>

| 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 | ☑ |

---

### User and security

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

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database user</td>
<td>The name of the user currently logged to the database.</td>
</tr>
<tr>
<td>User</td>
<td>The actual windows user.</td>
</tr>
<tr>
<td>Description</td>
<td>Display the description of the user connected to the data source.</td>
</tr>
<tr>
<td>Is administrator</td>
<td>Indicates if the user is an administrator.</td>
</tr>
<tr>
<td>Allow offline mode</td>
<td>Indicates if the user can use the data source in offline mode.</td>
</tr>
<tr>
<td>Allow drag-and-drop</td>
<td>Indicates if the user can drag-and-drop entries in the data source.</td>
</tr>
<tr>
<td>Is Auto Refresh</td>
<td>Indicates if the data source auto refreshes.</td>
</tr>
<tr>
<td>Auto refresh interval</td>
<td>Indicates the delay for the auto refresh to occur.</td>
</tr>
<tr>
<td>Is Two Factor Configuration</td>
<td>Indicates if the data source is configured with a second factor of authentication.</td>
</tr>
</tbody>
</table>

Entries
### 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.

### 7.2.3 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

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sign-in or Sign-out</td>
<td>Sign-in with your <a href="https://www.devolutions.com/products/password-manager/oddb">Devolutions Online Database (DODB)</a> account that has already been created. Sign-out of your Devolutions Online Database (DODB) account.</td>
</tr>
<tr>
<td>Create a New Devolutions Account</td>
<td>Create a new <a href="https://www.devolutions.com/products/password-manager/oddb">Devolutions Online Database (DODB)</a> account.</td>
</tr>
</tbody>
</table>

## Settings

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically sign-in at startup</td>
<td>Automatically sign-in to your <a href="https://www.devolutions.com/products/password-manager/oddb">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="https://www.devolutions.com/products/password-manager/oddb">Devolutions Online Database data source</a> or our <a href="https://www.devolutions.com/products/password-manager/oddb">Online Backup</a> service.</td>
</tr>
</tbody>
</table>

## Tools

- Installer File Generator
- Custom Installer Manager
- Import Online Database Configurations
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Installer Manager</td>
<td>Consult topic Custom Installer Manager.</td>
</tr>
<tr>
<td>Import Online Database Configurations</td>
<td>Import Online database configuration in the application.</td>
</tr>
</tbody>
</table>

### 7.2.4 Backup

**Description**

Please consult topic Online Backup for information on this service.

### 7.2.4.1 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 Cloud account.
2. Click on **View Subscription**.
3. Click on the ellipsis to enter your **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.

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.
7.2.4.2 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](image)

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

![Select your Backup](image)

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

6. Click on **Finish** to perform your backup restore.
7.2.5 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.

**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.

7.2.6 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).

7.2.7 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.


**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.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use default data source</td>
<td>Set the data source that you always want to open at start up.</td>
</tr>
<tr>
<td>Last used data source</td>
<td>Open with the last used data source.</td>
</tr>
<tr>
<td>Prompt for data source</td>
<td>A message box will open on startup for the data source selection.</td>
</tr>
</tbody>
</table>

7.2.8 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.
Is Online

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

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable check for server availability</td>
<td>Server is ping to determine if they are available. Server will be displayed in &quot;red&quot; in the tree view if not available.</td>
</tr>
<tr>
<td>Execute automatic check every</td>
<td>Execute the online check automatically each determined amount of minutes.</td>
</tr>
<tr>
<td>Check is online</td>
<td>If the option is On the application will verify if the server is online.</td>
</tr>
<tr>
<td>Online detection</td>
<td>If Check is online option is enable, select the detection method between:</td>
</tr>
<tr>
<td></td>
<td>• Ping</td>
</tr>
<tr>
<td></td>
<td>• Port scan</td>
</tr>
</tbody>
</table>

7.2.9 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
**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

### 7.2.9.1 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.

Refer to the sections below depending on the chosen source.

**Network Neighborhood**

The next screen will immediately be populated with the result of the network discovery.
If you prefer your sessions to use the IP address instead of the Host name to connect to the devices, check the "select by IP address" option. This requires that the "Resolve by IP address" was selected in the first screen of the wizard. Select the computers for which you want to create session and proceed to Template Selection below. Multi-select is allowed by using CTRL-click and SHIFT-click.
Active directory
The following screen allows you to select the domain to interrogate after which you must press refresh to load the list of computers that are available.

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

**Host list**

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

**Template selection**

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

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

### 7.2.9.2 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**
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.

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.

### 7.2.9.2.1 Import Strategies and file format

#### Description

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

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

If you need finer control, you can specify the template to use in a Template column of the CSV file. But since you're able to specify the entry type from within the CSV file it may not be necessary. 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: "Meta\Information\OS" or "Meta\Information\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.
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Host name of the device, this is the only mandatory field.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the entry</td>
</tr>
<tr>
<td>ConnectionType</td>
<td>Token representing the connection type. It is best to use the <strong>Clipboard-Copy</strong> method to obtain the acceptable values.</td>
</tr>
<tr>
<td>Folder</td>
<td>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.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the entry.</td>
</tr>
<tr>
<td>Open (Embedded)</td>
<td>Boolean value <em>(true or false)</em> 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.</td>
</tr>
<tr>
<td>Username</td>
<td>Username used to open a session to the device.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain used to open a session to the device.</td>
</tr>
<tr>
<td>Password</td>
<td>Password used to open a session to the device. Please note that this field is encrypted and stored into another field upon being imported.</td>
</tr>
<tr>
<td>MetaInformation\SerialNumber</td>
<td>Serial Number of the device.</td>
</tr>
<tr>
<td>MetaInformation\ServiceTag</td>
<td>Service Tag of the device.</td>
</tr>
<tr>
<td>MetaInformation\PurchaseDate</td>
<td>Purchase date in a ISO8601 format, i.e. yyyy-mm-dd</td>
</tr>
</tbody>
</table>

**CSV samples**

**With specified session types**

```
Host,Name,Template,ConnectionType,ConnectionSubType,SubMode,Group,Username,Domain,Password,Description,URL
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,,,,
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) sub-type"
192.168.10.006,six,"Telnet, SSH, RAW, rLogin",,2,QA Lab,,,"This is the SSH Shell (Rebex) sub-type"
192.168.10.007,seven,"Telnet, SSH, RAW, rLogin",,3,QA Lab,,,"This is the SSH (Rebex) sub-type"
192.168.10.008,eight,,VNC,,,QA Lab,,,,Description008,
192.168.10.009,nine,,Citrix,,,QA Lab,,,,Description009,
```

### 7.2.9.3 Import Network Scan

**Description**

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

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

If you wish to review each and every session as they are imported you can check the **Edit imported entry**, however we do not recommend this for large number of sessions.
7.2.9.4 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

You can import your sessions from an existing application or an existing file format. Some applications 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!

7.2.9.5 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.
**7.2.9.6 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.

### 7.2.10 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**

- Export
  - Export All (.rdm)
  - Export All Host List (.csv)

**Export Special**

- Export All (.csv)
- Export All (.html)
- Export All (.xml)
- Export All Documents

**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.

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.
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 all attachments or all document entries that are linked to your data source.

**7.2.10.1 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.

**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.

### 7.2.11 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.
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**

### 7.2.11.1 Advanced

**Description**
Use the **File – Options – Advanced** tab to control the application behavior as it pertains to low level settings.

---

**Settings**

**Advanced**
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debug level</td>
<td>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.</td>
</tr>
</tbody>
</table>
| Logs                          | The logs can be saved in a file or in a database file. Select between:  
• **Both**: Logs will be saved in a text file and in a database file.  
• **Database**: Logs will be saved in a file named RemoteDesktopManager.log.db. The file is located in the installation folder of the application.  
• **File**: Logs will be saved in a file named RemoteDesktopManager.log. The file is located in the installation folder of the application. |
| Connection constructor        | The connection constructor is used for memory optimization when using legacy. We strongly recommend to leave this option at Default. **Only change this option upon request from a Devolutions support technician.** |
| Offline engine                | You can choose your Offline engine between the SQLite or OpenMCDF. **Only change this option upon request from a Devolutions support technician.** |
| Force "localhost" when using VPN dynamic port | Forces the use of "localhost" when using the VPN dynamic port. |
| Confirm on multiple session open if open count greater than | Select a target number where mass opening sessions will demand confirmation. |

**Other Options - Connections**
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto close embedded tab on disconnect</td>
<td>Automatically closes all tabs for embedded sessions when they are disconnected.</td>
</tr>
<tr>
<td>Confirm on multiple sessions open</td>
<td>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.</td>
</tr>
<tr>
<td>Disable embedded 32 shell execute</td>
<td>Disable the shell embedded 32 execute in Windows for embedded sessions.</td>
</tr>
<tr>
<td>Disable logoff confirmation message</td>
<td>When pressing the logoff button in an embedded RDP session, Remote Desktop Manager, will disconnect the session without the logoff confirmation message.</td>
</tr>
<tr>
<td>Disable multi-thread loading</td>
<td>This setting allows Remote Desktop Manager to use multiple threads to load the data. Disabling this option will decrease the performance.</td>
</tr>
<tr>
<td>Disable multi-thread offline file</td>
<td>This setting allows Remote Desktop Manager to use multiple threads in offline file. Disabling this option will decrease the performance.</td>
</tr>
<tr>
<td>Disable RDP virtual channel</td>
<td>Turning off virtual channel disables some Remote Desktop Services features such as clipboard and printer redirection.</td>
</tr>
<tr>
<td>Enable advanced Logging for Telnet and SSH (AdvancedTelnetSSH.log)</td>
<td>This option creates an AdvancedTelnetSSH.log file in %LocalAppData% \Devolutions\RemoteDesktopManager. This file can be helpful when retrieving logs for Telnet/SSH connections.</td>
</tr>
<tr>
<td>Enable offline read/write locks</td>
<td>Activate locks for the Offline read/write rights.</td>
</tr>
<tr>
<td>Ensure that KeePass is running</td>
<td>Validate that KeePass is running on your computer before accessing any KeePass data.</td>
</tr>
<tr>
<td>Force refresh before edit entry</td>
<td>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.</td>
</tr>
<tr>
<td>Force restore application with desktop shortcut</td>
<td>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.</td>
</tr>
<tr>
<td>Open shortcut session silent</td>
<td>Disable the command line warning message when using a shortcut.</td>
</tr>
<tr>
<td>Use connection loader optimization</td>
<td>Only enable this option upon request from our Support team.</td>
</tr>
<tr>
<td>Use DirectX rendering in VNC</td>
<td>By default this option is enabled to use DirectX rendering when available for VNC connection.</td>
</tr>
<tr>
<td>Use NTFS Encryption for Offline mode</td>
<td>When using Offline Mode, 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.</td>
</tr>
<tr>
<td>Use Secret Server Legacy Interface</td>
<td>Enable to use the Secret Server Legacy interface.</td>
</tr>
</tbody>
</table>

**Other Options - General**
### Remote Desktop Manager

#### OPTION | DESCRIPTION
--- | ---
Allow multiple instances | Allows more than one instance of Remote Desktop Manager to run concurrently. This is not a recommended practice.
Allow non upgraded data source | Allow Remote Desktop Manager to work on an older data source that has not being upgraded.
Confirm on drag and drop move | When session(s) are moved by drag and drop, a confirmation message will appear to confirm the move.
Disable stack trace | Disable the stack trace details when an error occurs in Remote Desktop Manager. This is a security feature.
Focus content on application activation | Set focus on the last embedded session when the application is activated.
Use application directory for local play list | Use the installation folder to save the local play list that has been created.
Use application directory for offline cache | Use the installation folder to save the offline cache file.

### Other Options - UI Options

#### OPTION | DESCRIPTION
--- | ---
Always show "Go Offline" button | Always display the "Go Offline" button in the status bar when Offline Mode is active.
Disable custom images | Disable the loading of any custom images in the tree view. Too many custom images could dramatically increase the size of the data source and increase the load time at the same time.
Expand all tree nodes on select credential entry | After creating a new credential entry, the tree nodes expands automatically.
Hide last opened play list in play list management | Hide the last opened play list at startup in the play list dialog.
Use old entry sort | Use the old entry sort from previous version of Remote Desktop Manager.

### Information

#### OPTION | DESCRIPTION
--- | ---
Created on | Creation date of Remote Desktop Manager configuration folder.
Source | Source of Remote Desktop Manager configuration settings.
Path | Shortcut to access the configuration folder directly.

---

#### 7.2.11.2 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**

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the selected configuration file as the new one</td>
</tr>
<tr>
<td>Choose options to replace</td>
</tr>
<tr>
<td>Create a backup (.old)</td>
</tr>
</tbody>
</table>

**Choose options to replace**

- **Use the selected configuration file as the new one**
  - Use the RemoteDesktopManager.cfg file as a new configuration file for your application.

- **Choose options to replace**
  - Select which options to replace in your actual RemoteDesktopManager.cfg file. See below for more information.

- **Create a backup (.old)**
  - Create a backup of your old RemoteDesktopManager.cfg file.
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.

### 7.2.11.3 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.
Configuration file export dialog

Settings

Registration information

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Company registration name.</td>
</tr>
<tr>
<td>Email</td>
<td>Registration email.</td>
</tr>
<tr>
<td>Key</td>
<td>Serial key.</td>
</tr>
</tbody>
</table>

Miscellaneous

The local templates may contain credentials, ensure you do not share the exported file.
## 7.2.12 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 times as required. This section also allows to manage Personal Credentials, Personal Private Key and Specific Settings lists.

### Settings

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

### 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.
My Account Settings

Information

Database user
User
Administrator

My Personal Credentials
My Personal Private Key
User Specific Settings List
Local Specific Settings List

Settings

AuthAnvil Password Server
Box
CyberArk
CyberArk AIM
CyberArk PSM Server
Dashlane
Devolutions Hub
Devolutions Password Server

My Account Settings
### OPTION  DESCRIPTION

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

**Settings**

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

#### 7.2.12.1 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% (Terminal Services)\Devolutions\RemoteDesktopManager` and delete the `Credentials.rdt` file to reset it.
**My Personal Credentials** can be selected in your entries under **Credentials**.
7.2.12.2 User Specific Settings List

Description

The User Specific Settings List feature will provide all entries that are overridden with user Specific Settings.
### 7.2.13 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.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>Edit the selected User Specific Settings.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete the selected User Specific Settings.</td>
</tr>
<tr>
<td>Import</td>
<td>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.</td>
</tr>
<tr>
<td>Export</td>
<td>Export a list of user Specific Settings into a .rds file. A password is required to encrypt the .rds file.</td>
</tr>
</tbody>
</table>
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).

**Availability**

When creating a template, its availability can be specified in the properties.
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).
The template can be selected before creating the entry as well. Simply use the Template section of the Add New Entry window.

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

Import wizard
The import session wizard uses a template for the imported sessions.
7.2.13.1 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.
2. In the **Templates** window, click the **Add template** button.
3. Select an entry to create the template for.
4. Enter a name for the template, and configure the properties as necessary.

**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...**
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.
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**...

### 7.2.13.2 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
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.

7.2.13.3 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.
2. The **Password Templates** window provides an overview of current templates, as well as add, edit and delete commands.
3. To add a new template click **Add** (plus sign).

4. a) Enter a template name.
   
   b) Choose a **Mode** and configure the settings.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default</strong></td>
<td>General settings about length and minimum amounts for characters and symbols.</td>
</tr>
<tr>
<td><strong>Advanced settings</strong></td>
<td>Granular character settings (e.g. special characters and symbols, inclusions, exclusions).</td>
</tr>
<tr>
<td><strong>Readable password</strong></td>
<td>Settings for syllables, numbers and symbols.</td>
</tr>
<tr>
<td><strong>Use a pattern</strong></td>
<td>Set a pattern for the passwords using the key.</td>
</tr>
<tr>
<td><strong>Pronounceable password</strong></td>
<td>Settings for length, case, digits and characters.</td>
</tr>
</tbody>
</table>

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

### Use a Password Template with Password Generator

1. On the **Tools** tab, click **Password Generator**. Or open the password generator from an entry.
2. To choose a password template, select the title from the list. **Default** is equivalent to no template, until it is configured by an administrator. When you select a template the options are unavailable because they were saved in the template.
3. Click **Generate** to list possible passwords.
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.
7.3 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.

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

7.4 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.
Connection

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconnect</td>
<td>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.</td>
</tr>
<tr>
<td>Close</td>
<td>Close the active session.</td>
</tr>
<tr>
<td>LogOff</td>
<td>Logoff the RDP session. See Logoff topic for more information.</td>
</tr>
</tbody>
</table>

Actions

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute</td>
<td>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.</td>
</tr>
<tr>
<td>Macro/Script</td>
<td>Displays a window where you can select a macro or script, as well as the execution options.</td>
</tr>
<tr>
<td>Type Clipboard</td>
<td>Send the content of the clipboard over to the opened session.</td>
</tr>
</tbody>
</table>

Display

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

Settings

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep tab on disconnect</td>
<td>Your session tab will stay after a session disconnect. For more information, see Keep Tab Opened topic.</td>
</tr>
<tr>
<td>Smart Sizing</td>
<td>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.</td>
</tr>
<tr>
<td>Smart Reconnect</td>
<td>Automatically reconnect your session with the most appropriate band.</td>
</tr>
<tr>
<td>Windows Key on the Remote Computer</td>
<td>When enabling Windows key, it will send the function to your host instead of running it on your computer.</td>
</tr>
</tbody>
</table>

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

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

### Video

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record</td>
<td>Record your screen in an MP4 format. We recommend the use of a VLC player to view the recorded video.</td>
</tr>
</tbody>
</table>

Alternatively, these actions are also available by right-clicking on the tab of an embedded session.
7.4.1 Commands

7.4.1.1 RDP

Description

The commands for an RDP session allows you to send remote commands to your host.

Settings
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Only</td>
<td>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.</td>
</tr>
<tr>
<td>Send Ctrl+Alt+Delete</td>
<td>Send the key combination CTRL+ALT+DELETE to the host.</td>
</tr>
<tr>
<td>Charms</td>
<td>On Windows 8 or Windows 2012 server, displays the Charms bar (Search, Share, Start, Devices, and Settings bar).</td>
</tr>
<tr>
<td>App Bar</td>
<td>On Windows 8 or Windows 2012 server, displays the App bar to show navigation, commands, and tools.</td>
</tr>
<tr>
<td>Snap</td>
<td>On Windows 8 or Windows 2012 server, allows you to run two applications side-by-side.</td>
</tr>
<tr>
<td>Start Screen</td>
<td>Open the Start menu on the host computer.</td>
</tr>
<tr>
<td>App Switch</td>
<td>On Windows 8 or Windows 2012 server, switches from an application to another.</td>
</tr>
</tbody>
</table>

7.4.1.2 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](image)
Remote Desktop Manager

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh Screen</td>
<td>Refresh the host screen.</td>
</tr>
<tr>
<td>Window Start Menu</td>
<td>Open the Start menu on the host computer.</td>
</tr>
<tr>
<td>Send Ctrl-Alt-Delete</td>
<td>Send the key combination CTRL+ALT+DELETE to the host.</td>
</tr>
<tr>
<td>Send Custom Keys</td>
<td>Send custom keys combination to the host.</td>
</tr>
<tr>
<td>Alt</td>
<td>Send ALT to the host.</td>
</tr>
<tr>
<td>Ctrl</td>
<td>Send CTRL to the host.</td>
</tr>
<tr>
<td>View only mode</td>
<td>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.</td>
</tr>
<tr>
<td>Remote input</td>
<td>Keyboard and pointer events will be sent to the server and the local and remote clipboard will be synchronized.</td>
</tr>
<tr>
<td>Open file transfer</td>
<td>Open the file transfer with the host computer.</td>
</tr>
<tr>
<td>Open chat dialog</td>
<td>Open a chat dialog with the host computer.</td>
</tr>
<tr>
<td>Options</td>
<td>Open the Connection Options window.</td>
</tr>
<tr>
<td>Information</td>
<td>Open the window containing information regarding your VNC connection status and traffic.</td>
</tr>
</tbody>
</table>

7.4.1.3 SSH Shell (Rebex)

Description

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

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

Start Recording
Recording type

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

**Connection Information**

Provides connection host information in a form as shown below.
7.4.1.4 Telnet

Description

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

Settings

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

Start Recording

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

Description

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

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Entry</td>
<td>Create a new entry (session, folder, information entry, credentials, etc.).</td>
</tr>
<tr>
<td>Duplicate</td>
<td>Create a duplicate of your entry.</td>
</tr>
<tr>
<td>Create Shortcut</td>
<td>Link your entry to more than one group. For more information, consult the text below.</td>
</tr>
<tr>
<td>Save as Template</td>
<td>Save the selected entry as a local or database template.</td>
</tr>
</tbody>
</table>

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.
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**

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Properties</td>
<td>Edit the properties of the selected entry.</td>
</tr>
<tr>
<td>Rename</td>
<td>Rename the selected entry.</td>
</tr>
<tr>
<td>Move</td>
<td>Move the selected entry to another folder.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete the selected entry. A confirmation dialog is displayed to confirm the action.</td>
</tr>
<tr>
<td>Play List</td>
<td>Use the various play list features.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Specific Settings</td>
<td>Override properties of the selected entry with settings specific to the current user. For more information, please consult the Specific Settings topic.</td>
</tr>
<tr>
<td>Local Specific Settings</td>
<td>Override properties of the selected entry with settings specific to the local machine. For more information, please consult the Specific Settings topic.</td>
</tr>
</tbody>
</table>

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](image)

Batch

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit (Special Actions)</td>
<td>Perform special actions on the selected entries, such as change the type, run a script, and more. For more information, please consult the Batch Actions Samples.</td>
</tr>
<tr>
<td>Batch Edit</td>
<td>Perform an action on multiple entries at once. This is particularly useful for doing mass modifications of entries (such as changing the display mode after modifying the workspace or their credential entries when changing your passwords). Multiple entries must be selected for this feature to be visible. For more information, please consult the Batch Edit topic.</td>
</tr>
<tr>
<td>Move to Vault</td>
<td>Transfer the selected entries to another Vault in the database.</td>
</tr>
</tbody>
</table>
### Export

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export Entry as Remote Desktop File (.rdp)</td>
<td>Export the selected entries in a Remote Desktop File (.rdp) format.</td>
</tr>
<tr>
<td>Export Selection (.rdm)</td>
<td>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.</td>
</tr>
</tbody>
</table>

### 7.5.1 Edit

#### 7.5.1.1 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.
Play lists can be saved three different ways:

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>The Play List is saved locally and can only be accessed as such. These can only be launched through the Play List Management.</td>
</tr>
<tr>
<td>Shared</td>
<td>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.</td>
</tr>
<tr>
<td>Private Vault</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.
2. On the **Edit** ribbon menu, click **Play List**, then select whichever setting you prefer.
OPTION | DESCRIPTION
---|---
New | Creates a new Play List directly, a window prompt will ask you where you wish to save it and which selection you would like to highlight.
Create from Opened Sessions | Brings up the window for creating a new Play List with all currently opened session already selected for the Play List. You can select and remove additional entries if desired.
Add Selection to Existing Play List (X Entry) | Prompts a window where you can select currently accessible Play Lists and adds the selection in the Navigation Pane to the Play List.

3. Choose if you wish to save your Play List locally, in a shared Vault or in your Private Vault. Saving it locally will prompt a different window. This window will contain everything needed for a local Play List.
4. The next window lets you choose how you want your current selection or opened sessions to affect your playlist.

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

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

**Edit Existing Play List**

1. On Edit, click **Play List Management**.

2. Select the Play List you wish to modify and click **Edit**.
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.

7.5.1.1.2 Using a Play List

**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

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

7.5.2 Setting Overrides

7.5.2.1 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**.

**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.

**Workflow**

In the majority of cases, editing the **Specific Settings** displays the following dialog:
Specific settings are context sensitive, and several settings might not be available for some entry types.

7.5.3  Batch

7.5.3.1  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.

**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](#).
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.
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.
Edit Sessions (User/Local Specific Settings)

Specific Settings can be modified in a batch if supported by the type of the edited entries.

7.6 View

Description

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

Refer to the following topics for more information:
### Panels

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vault</td>
<td>Access the view mode for your Navigation Pane for the current Vault.</td>
</tr>
<tr>
<td>Opened Sessions</td>
<td>Display the currently Opened Sessions in your Navigation Pane.</td>
</tr>
<tr>
<td>Favorites</td>
<td>Display your Favorite entries and folder in your Navigation Pane.</td>
</tr>
<tr>
<td>Recent</td>
<td>Display your Recently Opened Sessions in your Navigation Pane.</td>
</tr>
<tr>
<td>Task List</td>
<td>Display your current Task List.</td>
</tr>
</tbody>
</table>

### View

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

### Layout

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

### 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.

7.6.1 Panels

7.6.1.1 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.

Creating a task

1. Click on Add new task.
Add a task

2. Enter your task information, like the name of the task, the priority, the due date, the description, etc.
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a custom name for the task</td>
</tr>
<tr>
<td>Entry</td>
<td>Displays the entry currently selected in the navigation pane. The task is assigned to this entry. Read-only field.</td>
</tr>
<tr>
<td>Priority</td>
<td>Set the priority of the task.</td>
</tr>
<tr>
<td>Due date</td>
<td>Set a deadline for the task.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the task for the assigned user.</td>
</tr>
<tr>
<td>User</td>
<td>Assign a user to the task.</td>
</tr>
<tr>
<td>Assign to me</td>
<td>Click this button to assign the task to yourself.</td>
</tr>
<tr>
<td>Clear assigned user</td>
<td>Clear the assigned user.</td>
</tr>
<tr>
<td>Status</td>
<td>Set a status for the task. Select between:</td>
</tr>
<tr>
<td></td>
<td>• Open</td>
</tr>
<tr>
<td></td>
<td>• Assigned</td>
</tr>
<tr>
<td></td>
<td>• In progress</td>
</tr>
<tr>
<td></td>
<td>• Closed</td>
</tr>
<tr>
<td></td>
<td>• Done</td>
</tr>
<tr>
<td></td>
<td>• Canceled</td>
</tr>
<tr>
<td></td>
<td>• Postponed</td>
</tr>
<tr>
<td>Comment</td>
<td>Enter a comment for the task.</td>
</tr>
</tbody>
</table>

7.6.2 View

7.6.2.1 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...
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder</td>
<td>The Folder where your entry is situated.</td>
</tr>
<tr>
<td>Connection</td>
<td>The connection being used to open your entry.</td>
</tr>
<tr>
<td>Message</td>
<td>Indicate the action that was done on your entry or session.</td>
</tr>
<tr>
<td>On Open Comment</td>
<td>The Open Comment is defined in the Log tab of your session, to learn more please see <a href="#">Logs Options</a>.</td>
</tr>
<tr>
<td>On Close Comment</td>
<td>The Close Comment is defined in the Log tab of your session, to learn more please see <a href="#">Logs Options</a>.</td>
</tr>
<tr>
<td>Log Date</td>
<td>Indicate the date and time your session was opened or your entry was edited.</td>
</tr>
<tr>
<td>End Date/Time</td>
<td>Indicate the date and time when the session or entry was closed.</td>
</tr>
<tr>
<td>Active Time</td>
<td>Only available for sessions in embedded mode. It will record your session active time, meaning the time your session was opened in embedded mode and you were active in your session. If your session is opened but your view is on your Dashboard tab and not on your session tab, no Active Time will be recorded.</td>
</tr>
<tr>
<td>Database username</td>
<td>Indicate the database username.</td>
</tr>
<tr>
<td>Connection user</td>
<td>Indicate the Connection user.</td>
</tr>
<tr>
<td>Machine</td>
<td>Indicate the machine name.</td>
</tr>
<tr>
<td>Connection Type</td>
<td>Indicate the connection type that was used.</td>
</tr>
</tbody>
</table>
7.6.2.2 Advanced Search

**Description**

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

![Advanced Search Window](image)

**Settings**
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You can select between different criteria to tweak your search:</td>
</tr>
<tr>
<td></td>
<td>- Name</td>
</tr>
<tr>
<td></td>
<td>- Connection type</td>
</tr>
<tr>
<td></td>
<td>- Contact Reference</td>
</tr>
<tr>
<td></td>
<td>- Creation date</td>
</tr>
<tr>
<td></td>
<td>- Custom field</td>
</tr>
<tr>
<td></td>
<td>- Description</td>
</tr>
<tr>
<td></td>
<td>- Domain</td>
</tr>
<tr>
<td></td>
<td>- Group</td>
</tr>
<tr>
<td></td>
<td>- Host</td>
</tr>
<tr>
<td></td>
<td>- Is favourite</td>
</tr>
<tr>
<td></td>
<td>- Keywords/tags</td>
</tr>
<tr>
<td></td>
<td>- Last update date</td>
</tr>
<tr>
<td></td>
<td>- Name</td>
</tr>
<tr>
<td></td>
<td>- OS</td>
</tr>
<tr>
<td></td>
<td>- Password strength</td>
</tr>
<tr>
<td></td>
<td>- Security group</td>
</tr>
<tr>
<td></td>
<td>- Status</td>
</tr>
<tr>
<td></td>
<td>- Username</td>
</tr>
<tr>
<td>Load</td>
<td>Load searches that has been previously saved.</td>
</tr>
<tr>
<td>Save</td>
<td>Allows you to save your search locally and reuse it.</td>
</tr>
<tr>
<td>Save as</td>
<td>Use to save a previously saved search but under another name.</td>
</tr>
<tr>
<td>Export</td>
<td>Export the entries of your search result as a Csv, Html, Xls or Xml file.</td>
</tr>
<tr>
<td></td>
<td>Sensitive information will be encrypted using AES.</td>
</tr>
<tr>
<td>Search</td>
<td>Once you have selected your search criteria click on Search to display the</td>
</tr>
<tr>
<td></td>
<td>search result.</td>
</tr>
<tr>
<td>Reset</td>
<td>Reset all your fields to proceed with a new Search.</td>
</tr>
<tr>
<td>Select in Navigation</td>
<td>Select your search result in your Navigation Pane. This option can be used in</td>
</tr>
<tr>
<td>Pane</td>
<td>combination with a Batch Edit.</td>
</tr>
</tbody>
</table>

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.

### 7.6.2.3 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
**User Interface**

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

**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.

### 7.7 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.

### Management

These feature requires an Advanced Data Source.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>Opens the User Management.</td>
</tr>
<tr>
<td>Security Groups (Legacy)</td>
<td>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.</td>
</tr>
<tr>
<td>Vaults</td>
<td>Opens the Vault Management tab of User Management.</td>
</tr>
<tr>
<td>Roles</td>
<td>Opens the Role Management tab of User Management.</td>
</tr>
</tbody>
</table>

### Reports

The logs feature requires an Advanced Data Source.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reports</td>
<td>Open the Reports section to select which type of report best suit your current needs.</td>
</tr>
<tr>
<td>Administration Logs</td>
<td>Opens the Administration Logs.</td>
</tr>
<tr>
<td>Deleted Entries</td>
<td>Open a log of all Deleted Entries (since last clean up).</td>
</tr>
</tbody>
</table>

### Settings

These feature requires an Advanced Data Source.
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root Settings</td>
<td>Opens the Root Settings. The 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 root. Therefore, using permissions on the root folder allows to secure all entries below the root level. Refer to Default security for entries for more information.</td>
</tr>
<tr>
<td>System Settings (Data Source Settings)</td>
<td>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.</td>
</tr>
<tr>
<td>System Permissions</td>
<td>Modify System Permissions.</td>
</tr>
<tr>
<td>Security Provider</td>
<td>Set up a Security Provider for an additional layer of security.</td>
</tr>
</tbody>
</table>

**Clean Up**

This feature requires an Advanced Data Source.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clean Up Deleted History</td>
<td>Perform a partial or full clean up of the Deleted History.</td>
</tr>
<tr>
<td>Clean Up Entry History</td>
<td>Perform a partial or full clean up of the Entry History.</td>
</tr>
<tr>
<td>Clean Up Activity Logs</td>
<td>Perform a partial or full clean up of the Activity Logs. You also have the option to clean up the Administration Logs if desired.</td>
</tr>
<tr>
<td>Pack Data Source (Optimize)</td>
<td>The Pack Data Source (Optimize) feature analyzes all entries, compress and save them, thus saving space in your data source.</td>
</tr>
</tbody>
</table>

### 7.7.1 Management

#### 7.7.1.1 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 Management settings**

**General**
## User Management - General

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication type</td>
<td>Select the user's authentication type:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Custom (Devolutions)</strong>: create a user specific to Remote Desktop Manager without creating an SQL login.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Database (SQL Server)</strong>: authenticate using the SQL login from your SQL Server.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username for the user. When using <strong>Integrated Security</strong> the user must be selected from the directory.</td>
</tr>
<tr>
<td>Integrated security (Active Directory)</td>
<td>Specify to use Active Directory to authenticate to the data source. Applies only to SQL Server and Devolutions Server, depending on their configuration. For more information, please consult the <strong>Integrated Security</strong> topic.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the user's Password. This field is disabled when using <strong>Integrated Security</strong>.</td>
</tr>
<tr>
<td>User type</td>
<td>Select the type of user to create, select between:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Administrator</strong>: Grant full administrative rights to the user.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Read only user</strong>: Grant only the view access to the user.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Restricted user</strong>: Select which rights to grant to the user.</td>
</tr>
<tr>
<td></td>
<td>- <strong>User</strong>: Grant all basic rights to the user (Add, Edit, Delete). For more information, please consult the <strong>User Types</strong> topic.</td>
</tr>
<tr>
<td>User license type</td>
<td>Select the license type of the user. Select between:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Connection Management</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Password Management</strong></td>
</tr>
<tr>
<td>Full name</td>
<td>Enter the First name and Last name of the user.</td>
</tr>
<tr>
<td>Email</td>
<td>Insert the user's email address.</td>
</tr>
</tbody>
</table>
**Information**

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

![User Management - Information - Details](Image)

**Roles**

Select roles to assign to the user.

![User Management - Roles](Image)
## Roles

Check the Is Member box to assign the role to the user. Consult Role Management topic for more information.

---

### Privileges

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>View information section</td>
<td>Allow the user to view the information section.</td>
</tr>
<tr>
<td>Activity logs</td>
<td>Allow the user to view the Activity logs.</td>
</tr>
<tr>
<td>Import</td>
<td>Allows the user to Import sessions (Clipboard - Paste as well). The import menu (File – Import) and the import feature in the context menu will be grayed out if the option is not active.</td>
</tr>
<tr>
<td>Export</td>
<td>Allows the user to Export sessions (Clipboard - Copy as well). The export menu (File – Export) and the export feature in the context menu will be grayed out if the option is not active.</td>
</tr>
</tbody>
</table>

---

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

**OPTION**

**DESCRIPTION**

<table>
<thead>
<tr>
<th>Remote Desktop Manager</th>
<th>Select if the user can access to the data source from Remote Desktop Manager.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devolutions Web Login</td>
<td>Select if the user can access to the data source form Devolutions Web Login.</td>
</tr>
</tbody>
</table>

### Settings

**User Management**

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:

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>No offline cache allowed for the user.</td>
</tr>
<tr>
<td>Cache only</td>
<td>Allow to save a cache of the data source but not the offline mode.</td>
</tr>
<tr>
<td>Read-only</td>
<td>A read-only cache. The user will not be able to edit data in the data source. This mode is allowed for <strong>Advanced Data Sources</strong> only.</td>
</tr>
<tr>
<td>Read/Write</td>
<td>An advanced cache, with change synchronization. This mode is allowed for <strong>Advanced Data Sources</strong> only.</td>
</tr>
</tbody>
</table>

### 7.7.1.1 User Types

**Description**

When creating users in Remote Desktop Manager, four types of user are available. Basic rights are granted to the created users depending on their type.
User Management - User Type

<table>
<thead>
<tr>
<th>TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Grant all rights and permissions to the user.</td>
</tr>
<tr>
<td>User</td>
<td>Grant all the basic rights to the user (Add, Edit, Delete).</td>
</tr>
<tr>
<td></td>
<td>For more information, please consult the Rights section below in this topic.</td>
</tr>
<tr>
<td>Restricted user</td>
<td>Personalize the rights to grant to the user.</td>
</tr>
<tr>
<td>Read only user</td>
<td>Grant only the view access to the user.</td>
</tr>
</tbody>
</table>

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 root folder of the data source.
7.7.1.2 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.

Ensure the appropriate domain is displayed in the From this location field. Sometimes 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.
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:

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not specified</td>
<td>Do not specify any TLS option.</td>
</tr>
<tr>
<td>REQUIRE NONE</td>
<td>Allow the connection without any certificate.</td>
</tr>
<tr>
<td>REQUIRE SSL</td>
<td>Allow the connection only with SSL encryption.</td>
</tr>
<tr>
<td>REQUIRE X509</td>
<td>Allow the connection only with valid X509 certificate.</td>
</tr>
</tbody>
</table>
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 Server**

Roles in Devolutions Server are in fact links to Active Directory groups. By leveraging Active Directory integration you can easily define access rights for all domain users in your organization. Once a domain user log in the Devolutions Server data source, their user account will be created if needed and users rights will be controlled by the defined groups.

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

For more information please see [Devolutions Server 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.

![Remote Desktop Manager - User and Security Management](#)

![Roles - Add Role](#)
7.7.2 Reports

7.7.2.1 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.

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.
7.7.2.1.1 Export Reports

**Description**

The Export Reports is a way to execute and export reports through a command line. You can use this feature in a shortcut or in a batch file and use the Windows task scheduler to execute it.

You will be able to export Data Report, Inventory report as well as most of the reports found in our Generate Report list except for the Password Usage and Security Group.

You must have the rights to run report in Remote Desktop Manager to use this feature.

**Settings**

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

```
C:\*** /DataSource:*** /report:***/reportoutput:***/reportsettings:***/closeapp
```

<table>
<thead>
<tr>
<th>PARAMETERS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\</td>
<td>Enter the path used to start your Remote Desktop Manager application (path of the RemoteDesktopManager.exe file)</td>
</tr>
<tr>
<td>/DataSource</td>
<td>Specify the data source ID.</td>
</tr>
<tr>
<td>/report</td>
<td>Specify the type of report to generate or the report ID.</td>
</tr>
<tr>
<td>/reportoutput</td>
<td>Specify the path to save your report and the name for the newly generated report.</td>
</tr>
<tr>
<td>/reportsettings</td>
<td>Specify the path of your report settings file (.rdr).</td>
</tr>
<tr>
<td>/closeapp</td>
<td>This command will close the Remote Desktop Manager if the application was started from a command line. If Remote Desktop Manager was already open before launching the command it won't close the application.</td>
</tr>
</tbody>
</table>

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.
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:

<table>
<thead>
<tr>
<th>REPORT TYPE IN Remote Desktop Manager</th>
<th>REPORT NAME (TYPE) TO INSERT IN THE COMMAND LINE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usage Log</td>
<td>SharedConnectionLog</td>
</tr>
<tr>
<td>Entry Information</td>
<td>EntryInformation</td>
</tr>
<tr>
<td>Expiration Schedule</td>
<td>CalendarExpiredEntry</td>
</tr>
<tr>
<td>Expired Entry List</td>
<td>ConnectionExpiredEntry</td>
</tr>
<tr>
<td>Expired Passports</td>
<td>ConnectionExpiredPassports</td>
</tr>
<tr>
<td>Expired Softwares</td>
<td>ConnectionExpiredSoftwares</td>
</tr>
<tr>
<td>Expired Warranties</td>
<td>ConnectionExpiredWarranties</td>
</tr>
<tr>
<td>Entry Status</td>
<td>ConnectionStatus</td>
</tr>
<tr>
<td>Credential Entry References</td>
<td>CredentialEntryUsage</td>
</tr>
<tr>
<td>Entry Validity Report</td>
<td>EntryValidity</td>
</tr>
<tr>
<td>VPN References</td>
<td>VPNEntryUsage</td>
</tr>
<tr>
<td>Entry List</td>
<td>Connection</td>
</tr>
<tr>
<td>Duplicate Entries</td>
<td>DuplicateEntry</td>
</tr>
<tr>
<td>Password Complexity</td>
<td>PasswordComplexity</td>
</tr>
<tr>
<td>Password Analyzer</td>
<td>PasswordAnalyzer</td>
</tr>
</tbody>
</table>
Here is an example of a command line for an Entry Information Report:

C:\Program Files (x86)\Devolutions\Remote Desktop Manager\RemoteDesktopManager.exe /DataSources /reportoutput:C:\dev\devolutions\Rapport\rapportEntry.csv /reportsettings:C:\dev\devolutions\Rapport\SettingsEntryInformation.rdr /closeapp

### 7.7.2.2 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 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.

7.7.3 Settings
7.7.3.1 Root (Settings)
7.7.3.1.1 Default security for entries

Description
In the root 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.
To confirm the change, edit an entry below the 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.

### 7.7.3.2 System Settings

#### 7.7.3.2.1 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.
<table>
<thead>
<tr>
<th>GENERAL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow user Specific Settings</td>
<td>Allow users to save <a href="#">User Specific Settings</a>.</td>
</tr>
<tr>
<td>Allow database clean up</td>
<td>Allows logs and deleted history to be cleaned up. For more information, please consult the <a href="#">Clean up</a> topic.</td>
</tr>
<tr>
<td>Allow shortcuts</td>
<td>Allow the reiteration of entries through the shortcut feature.</td>
</tr>
<tr>
<td>Allow entry states (Lock, Running, Checkout)</td>
<td>Allow entries to be locked when used or edited.</td>
</tr>
<tr>
<td>Allow virtual folders</td>
<td>Allow to store entries in virtual folders. (Not supported with Devolutions Password Server.)</td>
</tr>
<tr>
<td>Automatic check in after</td>
<td>Forces checked out entries to check in automatically after a set delay.</td>
</tr>
<tr>
<td>Allow sub connections</td>
<td>Allow users to create sub connections.</td>
</tr>
<tr>
<td>Add entry mode</td>
<td>Select if users are prompted to choose a template when creating a new entry. Select between:</td>
</tr>
<tr>
<td></td>
<td>• Default</td>
</tr>
<tr>
<td></td>
<td>• Template list (include default)</td>
</tr>
<tr>
<td></td>
<td>• Template list only</td>
</tr>
<tr>
<td></td>
<td>• No template selection</td>
</tr>
</tbody>
</table>
### COMMENTS

<table>
<thead>
<tr>
<th>Allow log comments editing</th>
<th>Enable the log comment editing for all users.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum length (char)</td>
<td>Set the minimum length (in characters) allowed for comments.</td>
</tr>
</tbody>
</table>

### FILE SIZE

| Maximum file size (MB) | Limit the size of attachments and document entries to avoid to over load the data source. |

7.7.3.2.1.1 Security

#### Settings

**System Settings - General - Security**

**DATA SOURCE SECURITY**

<table>
<thead>
<tr>
<th>Create Vault with restricted access by default</th>
<th>Automatically secure the root settings when creating a repository. Therefore, the permissions settings are set to <strong>Never</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force data source 2-factor configuration</td>
<td>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.</td>
</tr>
<tr>
<td>Resolve credentials in overview</td>
<td>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.</td>
</tr>
<tr>
<td>Use legacy security</td>
<td>Use the old system of managing privileges: security groups.</td>
</tr>
</tbody>
</table>
### TIME-BASED USAGE

<table>
<thead>
<tr>
<th>TIME-BASED USAGE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time of day</td>
<td>Select the hours which the data source is limited to. Select between:&lt;br&gt;• <strong>Any time</strong>: the session can be used at any hour.&lt;br&gt;• <strong>Custom</strong>: manually select the time frame the session is available for.</td>
</tr>
<tr>
<td>Time of week</td>
<td>Select which days the data source is available for. Select between:&lt;br&gt;• <strong>Any day</strong>: the session can be used any day of the week or week-end.&lt;br&gt;• <strong>Week days</strong>: the session can be used only the week days.&lt;br&gt;• <strong>Week ends</strong>: the session can be used only the week ends.&lt;br&gt;• <strong>Custom</strong>: manually select each day the session is available for.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Select the time zone you are currently in.</td>
</tr>
</tbody>
</table>

#### 7.7.3.2.1.2 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.
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.
Use the following .net code to decrypt your passwords:

```csharp
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;
    }
}
```

7.7.3.2.2 Application

**Description**

The Applications section manages the availability of different features related to Remote Desktop Manager application.
### Allow Access

**Operating systems**
Enable access to the data source from the selected operating systems.

### General

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow local Specific Settings</td>
<td>Allow users to save <a href="#">Local Specific Settings</a>.</td>
</tr>
<tr>
<td>Allow templates (local)</td>
<td>Allows to locally save entry's templates.</td>
</tr>
<tr>
<td>Disable entry drag-and-drop</td>
<td>Disable entries drag and drop from one folder to another. This setting is useful for avoiding accidental drag and drop.</td>
</tr>
<tr>
<td>Disable quick connect</td>
<td>Disable the <a href="#">Quick Connect</a> feature for all users of the data source.</td>
</tr>
<tr>
<td>Disable RDM Agent and Jump</td>
<td>Disable the option to activate a session as an RDM Agent or Jump.</td>
</tr>
<tr>
<td>Disable stack trace</td>
<td>Disable the stack trace details when an error occurs in Remote Desktop Manager. This is a security feature.</td>
</tr>
<tr>
<td>PASSWORD</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow local password templates</td>
<td>Allows password templates to be saved locally.</td>
</tr>
<tr>
<td>Disable password saving for data source access</td>
<td>Prevent users to save or change the passwords stored in the data source configurations.</td>
</tr>
<tr>
<td>Disable password saving (local)</td>
<td>Prevent users from saving passwords in the properties of entries.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WELCOME PAGE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use web or html welcome page</td>
<td>Enter an URL to use as the application’s welcome page.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SECURITY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force application security with Windows credentials</td>
<td>Require the users to authenticate with their Windows credentials at application startup.</td>
</tr>
<tr>
<td>Force application security with Google Authenticator</td>
<td>Require the users to authenticate with <a href="#">Google Authenticator</a> at application startup.</td>
</tr>
<tr>
<td>Lock application</td>
<td>Set the application to lock:</td>
</tr>
<tr>
<td></td>
<td>• On Minimize: lock application when minimized in the taskbar for all users of the data source.</td>
</tr>
<tr>
<td></td>
<td>• On Idle: automatically lock the application when it is not used after a determined amount of time.</td>
</tr>
<tr>
<td></td>
<td>• On Windows lock: lock the application on Windows lock.</td>
</tr>
<tr>
<td></td>
<td>• On standby: lock the application when on standby.</td>
</tr>
</tbody>
</table>

7.7.3.2.2.1 Offline

**Description**

![Remote Desktop Manager - System Settings](image-url)
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offline mode</td>
<td>Set the global data source <strong>Offline Mode</strong> availability. The offline mode is useful when using a VPN connection that makes using local network impossible.</td>
</tr>
<tr>
<td>Expiration</td>
<td>Number of days before the offline cache expires. You must go online prior to the end of that period to re-validate the data.</td>
</tr>
<tr>
<td>Prompt for credentials before going offline</td>
<td>Force the user to provide their credentials before going offline.</td>
</tr>
<tr>
<td>Prompt for 2FA before going offline</td>
<td>Force the user to provide their 2FA before going offline.</td>
</tr>
</tbody>
</table>

It is not recommended to set the **Expiration** to 0, as this will disable the expiration of the offline cache.

7.7.3.2.2.2 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**

System Settings - Serial Number
## 7.7.3.2.2.3 Type availability

### Settings

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial (Site/Global)</td>
<td>Enter a Site/Global license serial to share with the data source. The application is updated with this license serial if it is newer than the one already registered.</td>
</tr>
<tr>
<td>Hide serial number</td>
<td>The license serial will be hidden for all users when accessing the Register Product window.</td>
</tr>
</tbody>
</table>

### Option availability

**Type Availability**

Select entry types to exclude. Excluded entries will not be in the Add New Entry window.

### Version Management

**Description**

The Version Management allows the administrators to manage the data source availability in other versions of Remote Desktop Manager.

**Windows and macOS**
## Version Management

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimal version</td>
<td>Forcates 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.</td>
</tr>
<tr>
<td>Minimal version custom message</td>
<td>Enter a custom message for the minimal version notification.</td>
</tr>
<tr>
<td>Maximal version</td>
<td>Forcates users of the data source to use a maximal version. Enter the entire version number (2019.1.0.0) to force a specific version. Use this to disable connecting to the data source with a newer version.</td>
</tr>
<tr>
<td>Maximal version custom message</td>
<td>Enter a custom message for the maximal version notification.</td>
</tr>
<tr>
<td>Disable auto update notification</td>
<td>Disable the auto update notification message. Use this to manually update the application and prevent from getting notified when new versions are available.</td>
</tr>
<tr>
<td>Download URL</td>
<td>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.</td>
</tr>
</tbody>
</table>
## 7.7.3.3 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](image)

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import</td>
<td>Allow users/roles to import entries in the data source.</td>
</tr>
<tr>
<td>Export</td>
<td>Allow users/roles to export from the data source.</td>
</tr>
<tr>
<td>Add in root</td>
<td>Allow users/roles to create entries in the root folder.</td>
</tr>
<tr>
<td>Root properties</td>
<td>Allow users/roles to access the root properties.</td>
</tr>
</tbody>
</table>

### Miscellaneous
### System Permissions - Miscellaneous

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity logs</td>
<td>Allow users/roles to view the activity logs.</td>
</tr>
<tr>
<td>Reports</td>
<td>Allow users/roles to generate and view reports.</td>
</tr>
<tr>
<td>View deleted entries</td>
<td>Allow users/roles to view and restore deleted entries.</td>
</tr>
<tr>
<td>View administration logs</td>
<td>Allow users/roles to view the administration logs.</td>
</tr>
<tr>
<td>Check in (force)</td>
<td>Allow users/roles to check in entries with the checked out state.</td>
</tr>
</tbody>
</table>

**Tools**
### System Permissions - Tools

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console management tools</td>
<td>Allow users/roles to use console management tools.</td>
</tr>
<tr>
<td>Buit-in tools (Wake-on-LAN, NetStat, Ping, ...)</td>
<td>Allow users/roles to use session related tools.</td>
</tr>
<tr>
<td>Macros/Scripts/Tools entry</td>
<td>Allow users/roles to use Macros/Scripts/Tools entries.</td>
</tr>
<tr>
<td>Management Tools</td>
<td>Allow users/roles to use Management Tools.</td>
</tr>
<tr>
<td>Web management tools</td>
<td>Allow users/roles to use web management tools.</td>
</tr>
</tbody>
</table>

### Management

The **Default** value in **Tools** is equivalent to **Never**.
### System Permissions - Management

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Allow users/roles to access the user management.</td>
</tr>
<tr>
<td>Security Group</td>
<td>Allow users/roles to access the security groups management.</td>
</tr>
<tr>
<td>Role</td>
<td>Allow users/roles to access the roles management.</td>
</tr>
<tr>
<td>Vault</td>
<td>Allow users/roles to manage Vaults.</td>
</tr>
<tr>
<td>Data source settings</td>
<td>Allow users/roles to access data source settings.</td>
</tr>
<tr>
<td>(System Settings)</td>
<td></td>
</tr>
<tr>
<td>Template</td>
<td>Allow users/roles to create and manage templates.</td>
</tr>
<tr>
<td>Password template</td>
<td>Allow users/roles to create and manage password templates.</td>
</tr>
</tbody>
</table>

### 7.7.3.4 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.

2. Select a security type from the drop down list.
Security Type

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>This is the legacy security provider. The data is encrypted if the entry configuration is set accordingly in the advanced settings of the entries.</td>
</tr>
<tr>
<td>Shared passphrase</td>
<td>Set up a shared passphrase for the Security Provider.</td>
</tr>
</tbody>
</table>

Shared Passphrase

If the passphrase is lost, **nothing** that can be done to recover the data. When using a passphrase, always copy it to a secure location.
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.
Certificate Security Provider

**OPTION** | **DESCRIPTION**
--- | ---
**Location** | Indicate the certificate location. Select between:  
- Current user  
- Local machine

**Store** | Indicate the store location of the certificate. Select between:  
- Address book  
- Authorization root  
- Certificate authority  
- Disallowed  
- My  
- Root  
- Trusted people  
- Trusted publisher

**Thumbprint** | Select an existing certificate.

**Create Certificate**

It is possible to create a Self Signed certificate by clicking on Create Certificate.
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common name</td>
<td>Name of the certificate.</td>
</tr>
</tbody>
</table>
| Key size (bits) | Indicate the key size (bits) of the certificate. Select between:  
  - 384  
  - 512  
  - 1024  
  - 2048  
  - 4096  
  - 8192  
  - 16384 |
| Valid from | Start date of the certificate. |
| Valid to | End date of the certificate. |
| Save to file (pfx) | Save the certificate as a pfx file and secure this certificate with a password. |
| Save to certificate store | Indicate the location and the store to save the certificate. |
7.7.4 Clean up

7.7.4.1 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.

2. Confirm your choice prior to permanently delete your deleted entries.
There will be no backup of your History. We strongly recommend to do a Backup before proceeding.

### 7.7.4.2 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.
2. Another window will appear to confirm your choice of deleting all the history prior to the chosen date.

No History backup is created. We strongly recommend to do a Backup before proceeding.

7.7.4.3 Clean Up Activity Logs

**Description**

The **Clean Up Activity Logs** will delete your data source’s Activity Logs, you also have the option to clean up the **Administration logs** and set up a back up if desired.
This feature requires an Advanced Data Source.

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

**Settings**

1. You must confirm your choice prior to permanently deleting your data source logs.

   **Clean Up 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

   ![Clean up data source logs](image)

2. Once you have entered your Backup file name and proceeded with the clean up a delete log result window will appear.

   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.
7.7.4.4 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.
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**.

### 7.8 Tools

#### Description

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

#### Generators
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Generator</td>
<td>Opens the Password Generator window. You can use this to generate passwords according to pre-determined criteria for better security.</td>
</tr>
<tr>
<td>SSH Key Generator</td>
<td>Launches the SSH Key Generator. SSH keys provide a secure way of logging into a virtual private server with SSH than using a password alone.</td>
</tr>
<tr>
<td>Certificate Generator</td>
<td>Launches the Certificate Generator. With this you can create a self-signed certificate, which is an identity certificate that is signed by the same entity whose identity is certified.</td>
</tr>
<tr>
<td>Port Generator</td>
<td>Launches the Port Generator. With this you can generate ports for your connections.</td>
</tr>
</tbody>
</table>

### Tools

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Analyzer</td>
<td>Opens the Password Analyzer. This is used to evaluate the strength of passwords stored in the data source. This feature is restricted to Administrators only.</td>
</tr>
<tr>
<td>My Inventory</td>
<td>Set up a My Inventory report.</td>
</tr>
<tr>
<td>Key Agent Manager</td>
<td>Opens the Key Agent Manager. This is used to hold all your SSH Keys in memory, already decoded and ready for them to be used.</td>
</tr>
<tr>
<td>PowerShell (RDM CmdLet)</td>
<td>Opens the PowerShell (RDM CmdLet).</td>
</tr>
<tr>
<td>Wayk Now</td>
<td>Launches the Wayk Now application.</td>
</tr>
<tr>
<td>More Tools</td>
<td>The More Tools window contains a variety of application tools such as: Chocolatey Console, Local RDP/RemoteApp Manager, Playback (Ansi), RDM Agent and more.</td>
</tr>
</tbody>
</table>

### Managers

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

### 7.8.1 Generators

#### 7.8.1.1 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.

**Advanced settings**
Select the type and amount of characters to include in the password.
**Readable password**

Generate passwords that are readable but are not actual words.
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.
The following are supported patterns:
<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>KEY</th>
<th>SAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lower-Case Alphanumeric</td>
<td>a</td>
<td>abcdefghijklmnopqrstuvwxyz 0123456789</td>
</tr>
<tr>
<td>Mixed-Case Alphanumeric</td>
<td>A</td>
<td>ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789</td>
</tr>
<tr>
<td>Bracket</td>
<td>b</td>
<td>(][{}&lt;&gt;</td>
</tr>
<tr>
<td>Lower-Case Consonant</td>
<td>c</td>
<td>bcdghijklmnopqrstuvwxyz</td>
</tr>
<tr>
<td>Mixed-Case Consonant</td>
<td>C</td>
<td>BCDFGHJKLMNPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz</td>
</tr>
<tr>
<td>Digit</td>
<td>d</td>
<td>123456789</td>
</tr>
<tr>
<td>Lower-Case Hex Character</td>
<td>h</td>
<td>0123456789 abcdef</td>
</tr>
<tr>
<td>Upper-Case Hex Character</td>
<td>H</td>
<td>0123456789 ABCDEF</td>
</tr>
<tr>
<td>Lower-Case Letter</td>
<td>l</td>
<td>abcdefghijklmnopqrstuvwxyz</td>
</tr>
<tr>
<td>Mixed-Case Letter</td>
<td>L</td>
<td>ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz</td>
</tr>
<tr>
<td>Punctuation</td>
<td>p</td>
<td>.-;</td>
</tr>
<tr>
<td>Printable 7-Bit Special Character</td>
<td>s</td>
<td>!*$%^&amp;'(+,-:.;&lt;=&lt;&gt;?[]^{}~</td>
</tr>
<tr>
<td>Printable 7-Bit ASCII</td>
<td>S</td>
<td>A-Z, a-z, 0-9, !*$%^&amp;'(+,-:.;&lt;=&lt;&gt;?[]^{}~</td>
</tr>
<tr>
<td>Upper-Case Letter</td>
<td>u</td>
<td>ABCDEFGHIJKLMNOPQRSTUVWXYZ</td>
</tr>
<tr>
<td>Upper-Case Alphanumeric</td>
<td>U</td>
<td>ABCDEFGHIJKLMNOPQRSTUVWXYZ 0123456789</td>
</tr>
<tr>
<td>Lower-Case Vowel</td>
<td>v</td>
<td>aeiou</td>
</tr>
<tr>
<td>Mixed-Case Vowel</td>
<td>V</td>
<td>AEIOU aeiou</td>
</tr>
<tr>
<td>High ANSI</td>
<td>x</td>
<td>From ‘~’ to U255 (excluding U255)</td>
</tr>
<tr>
<td>Upper-Case Consonant</td>
<td>Z</td>
<td>BCDFGHJKLMNPQRSTUVWXYZ</td>
</tr>
<tr>
<td>Upper-Case Vowel</td>
<td>Z</td>
<td>AEIOU</td>
</tr>
<tr>
<td>Escape (Fixed Char)</td>
<td>\</td>
<td>Use following character as is</td>
</tr>
<tr>
<td>Escape (Repeat)</td>
<td>{n}</td>
<td>Repeats the previous character n times</td>
</tr>
<tr>
<td>Custom character</td>
<td>[x]</td>
<td>Define a custom character sequence</td>
</tr>
</tbody>
</table>

**Pronounceable password**

Generate passwords that are pronounceable, but are not actual words.
**Strong password**

Generate an 8 character passwords with alphanumeric and special characters.
7.8.1.2 SSH Key Generator

Description

SSH keys provide a secure way of logging into a virtual private server with SSH than using a password alone. While a password can eventually be cracked with a brute force attack, SSH keys are nearly impossible to decipher by brute force alone.

Settings
SSH Key Generator

Key algorithm: RSA
Key size: 1024
Comment: username@hostname

You can add this into OpenSSH's authorized keys file:

```
ssh-rsa
AAAAAB3NzaC1yc2EAAAADAQABAAABAAGQjQ+4r/4b2D/aajQvYv8+ZujG4J8F7QZt3Fv69T
vU77Rl77/W0k5+s5+6P2D58lRT1JcZ5ZJtL7hF1f5z/FQXH/7Nl68FfF35W84eC3Thw
U7Mo7y1/4owFH1x/4uJp6j2h667k/LKr4G/U0H1/1Ggt57JXZzn6+Jw1jQy5s9l/y/0
+kb+/KcZ/eCw9/4w7RZ6z/6WZ97Z4v/a7y0+57Clgk/nOGs+Fh685b/Ay3N73w
```


Passphrase:
Confirm passphrase:

Load Private Key...  Save Public Key...  Save Private Key...

Close
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key algorithm</td>
<td>You can choose between: <strong>RSA</strong>: 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. <strong>DSA</strong>: It is faster in signing but slower in verifying. It can only be used for signing/verification it <strong>does not encrypt/decrypt</strong>. When using DSA it is a recommended to use a 1024 bits key size.</td>
</tr>
<tr>
<td>Key size</td>
<td>You can choose your SSH Key size between: <strong>1024 bits</strong>: Minimum key size <strong>2048 bits</strong>: Default and recommended key size <strong>4096 bits</strong>: Maximum key size</td>
</tr>
<tr>
<td>Comment</td>
<td>Enter your username and the name of the computer you're transferring your key to.</td>
</tr>
<tr>
<td>Load Private Key</td>
<td>This feature will allow you to import a previously saved SSH Key.</td>
</tr>
<tr>
<td>Save Public Key</td>
<td>Saving the public key will generate a *.pub file. Simply enter a file name when prompted.</td>
</tr>
</tbody>
</table>
| Save Private Key | You will have the option of saving your Private Key in different format, choose between:  
• PKCS #8 Private Key (*.pri)  
• PuTTY Private Key (*.ppk)  
• OpenSSH Private Key (*.pri) |

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

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

7.8.1.3 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**
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common name</td>
<td>Name of the certificate.</td>
</tr>
<tr>
<td>Key size (bits)</td>
<td>Indicates the key size (bits) of the certificate. Select between:</td>
</tr>
<tr>
<td></td>
<td>- 1024</td>
</tr>
<tr>
<td></td>
<td>- 2048</td>
</tr>
<tr>
<td></td>
<td>- 4096</td>
</tr>
<tr>
<td></td>
<td>- 8192</td>
</tr>
<tr>
<td></td>
<td>- 16384</td>
</tr>
<tr>
<td>Valid from</td>
<td>Starting date of the certificate.</td>
</tr>
<tr>
<td>Valid to</td>
<td>Expiration date of the certificate.</td>
</tr>
<tr>
<td>Save to file (pfx)</td>
<td>Save the certificate into a *.pfx file and secure this certificate with a password.</td>
</tr>
<tr>
<td>Save to certificate store</td>
<td>Indicate the location and the store to save the certificate.</td>
</tr>
<tr>
<td>Location</td>
<td>Indicate the location of the certificate. Select between:</td>
</tr>
<tr>
<td></td>
<td>- Current user</td>
</tr>
<tr>
<td></td>
<td>- Local machine</td>
</tr>
<tr>
<td>Store</td>
<td>Indicate the store location of the certificate. Select between:</td>
</tr>
<tr>
<td></td>
<td>- Address book</td>
</tr>
<tr>
<td></td>
<td>- Authorization root</td>
</tr>
<tr>
<td></td>
<td>- Certificate authority</td>
</tr>
<tr>
<td></td>
<td>- Disallowed</td>
</tr>
<tr>
<td></td>
<td>- My</td>
</tr>
<tr>
<td></td>
<td>- Root</td>
</tr>
<tr>
<td></td>
<td>- Trusted people</td>
</tr>
<tr>
<td></td>
<td>- Trusted publisher</td>
</tr>
</tbody>
</table>

![Remote Desktop Manager - Self Signed Certificate](image)

**Self Signed Certificate**

- Store
- Thumbprint
- Private key

Browse Store
View Certificate
View Private Key

Close
### 7.8.1.4 Port Generator

**Description**

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

**Settings**

- **Boundaries**
- **Include well known ports**
- **Include registered ports**
- **Include ports used by others sessions**

Port Generator:

<table>
<thead>
<tr>
<th>Port Numbers</th>
<th>1152</th>
<th>22961</th>
<th>36353</th>
<th>49608</th>
<th>62283</th>
</tr>
</thead>
<tbody>
<tr>
<td>1286</td>
<td>25033</td>
<td>38512</td>
<td>49617</td>
<td>62632</td>
<td></td>
</tr>
<tr>
<td>6302</td>
<td>25893</td>
<td>39234</td>
<td>49954</td>
<td>64116</td>
<td></td>
</tr>
<tr>
<td>10842</td>
<td>29762</td>
<td>44634</td>
<td>55373</td>
<td>64878</td>
<td></td>
</tr>
<tr>
<td>14378</td>
<td>34577</td>
<td>45921</td>
<td>57001</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16419</td>
<td>35026</td>
<td>46515</td>
<td>58310</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20926</td>
<td>36136</td>
<td>49088</td>
<td>58744</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2019 Devolutions inc.
7.8.2 Tools
7.8.2.1 Password Analyzer

Description

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.

![Entry Properties - Password Field With Password Analyzer](image)

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 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)
## 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**.
2. Click on **Add key** and select the file to open your SSH 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.
5. In the **Private Key** tab of your SSH Shell session leave the option for the Private Key to **No Private Key**.
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](image)

**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.
2. In the **Advanced** tab of your Private Key entry activate the option **Automatically load to key agent.**
7.8.2.3 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.
7.8.2.4 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.

For more information about using Wayk Now consult the Wayk Now Online Help.
7.8.2.5 More Tools

7.8.2.5.1 Chocolatey Console

Description

Chocolatey need to be installed on your computer to use the Chocolatey Console.

The Chocolatey Console is available in the Tools – More Tools - Chocolatey Console menu. It allows you to install all the supported applications from Chocolatey directly from Remote Desktop Manager.

Settings

![Chocolatey Console]

<table>
<thead>
<tr>
<th>Name</th>
<th>Installed Version</th>
<th>Latest Version</th>
<th>Installed</th>
</tr>
</thead>
<tbody>
<tr>
<td>autohotkey</td>
<td>1.1.23.01</td>
<td></td>
<td></td>
</tr>
<tr>
<td>autot</td>
<td>3.3.14.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>breeze</td>
<td>3.15.0.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firefox</td>
<td>44.0.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GoogleChrome</td>
<td>48.0.2664.109</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HeidiSQL</td>
<td>8.3.0.1694</td>
<td></td>
<td></td>
</tr>
<tr>
<td>java</td>
<td>8.0.66</td>
<td></td>
<td></td>
</tr>
<tr>
<td>keepass</td>
<td>2.31</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mvsd.workbench</td>
<td>6.3.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>powershell</td>
<td>4.0.20141001</td>
<td></td>
<td></td>
</tr>
<tr>
<td>putty.install</td>
<td>0.66</td>
<td>0.66</td>
<td></td>
</tr>
<tr>
<td>putty</td>
<td>7.1.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Redmine.Viewer</td>
<td>3.4.0.2012928</td>
<td></td>
<td></td>
</tr>
<tr>
<td>safari</td>
<td>7.18.0.112</td>
<td></td>
<td></td>
</tr>
<tr>
<td>skype</td>
<td>2016.03.02</td>
<td></td>
<td></td>
</tr>
<tr>
<td>teamviewer</td>
<td>11.0.53254</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tightvnc</td>
<td>2.7.10.20148503</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Chocolatey Console
### Usage

During the installation, you will see the following window.

![Installation window](image)

When the installation is completed you will see a check mark in the **Installed** column.
7.8.2.5.2 Local RDP/RemoteApp Manager

Description


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
Remote Desktop Manager

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.

**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.
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).

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

![New RemoteApp Settings](image1.png)

2. Configure the RemoteApp

![Remote Desktop Manager](image2.png)

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.
7.8.2.5.3 Playback (Ansi)

**Description**

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

**Settings**
## More Tools - Playback (Ansi)

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Open]</td>
<td>Select the ansi file you wish to open in the Terminal Playback.</td>
</tr>
<tr>
<td>![Font]</td>
<td>Select the font for the Terminal Playback.</td>
</tr>
<tr>
<td>![Options]</td>
<td>See <strong>Options</strong> section.</td>
</tr>
<tr>
<td>![Clear screen]</td>
<td>Clear the screen to play another ansi file.</td>
</tr>
</tbody>
</table>

### Options
Remote Desktop Manager

**Ansi Player Options**

- **Terminal name**: xterm
- **Encoding**: iso-8859-1 Western European (ISO)
- **Auto wrap**: On
- **Backspace wrap**: On

- **Force Non-destructive backspace**
- **Ignore Substitute character**
- **Implicit Carriage return in Linefeed**

Buttons: OK, Cancel
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal name</td>
<td>Indicate the terminal name.</td>
</tr>
<tr>
<td>Encoding</td>
<td>Indicate the encoding you wish to use.</td>
</tr>
<tr>
<td>Auto wrap</td>
<td>Indicate what happen when text reaches the right-hand edge of the window. Select between:</td>
</tr>
<tr>
<td></td>
<td>· On</td>
</tr>
<tr>
<td></td>
<td>· Off</td>
</tr>
<tr>
<td></td>
<td>· Dos</td>
</tr>
<tr>
<td>Backspace wrap</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>· On</td>
</tr>
<tr>
<td></td>
<td>· Off</td>
</tr>
<tr>
<td></td>
<td>· Dos</td>
</tr>
<tr>
<td>Force Non-destructive backspace</td>
<td>Allow to perform a normal backspace without deleting a character.</td>
</tr>
<tr>
<td>Ignore Substitute character</td>
<td>Ignore the substitute character that can be use in Putty.</td>
</tr>
<tr>
<td>Implicit Carriage return in Linefeed</td>
<td>Most servers send two control characters, CR and LF, to start a new line on the screen. The CR character makes the cursor return to the left-hand side of the screen. The LF character makes the cursor move one line down (and might make the screen scroll). Some servers only send LF, and expect the terminal to move the cursor over to the left automatically. If you come across a server that does this, you will see a stepped effect on the screen. If this happens to you, try enabling the option and things might go back to normal.</td>
</tr>
</tbody>
</table>

7.8.2.5.4 RDM Agent

Description

The **Remote Desktop Manager Agent** is a very powerful tool that allows commands to be run on multiple machines.
**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**.
Quick Script - Message
OPTION | DESCRIPTION
---|---
Message | Send a message to all targets.

Quick Script - Command Line (cmd.exe)
## Quick Script - Command Line

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

## Quick Script - PowerShell
### Quick Script - PowerShell

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

### Quick Script - Run
**Quick Script - Run**

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

**Quick Script - Scripts/Tools**
## OPTION

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scripts/Tools</strong></td>
<td>Select a script or a tool session that you have already created in Remote Desktop Manager.</td>
</tr>
</tbody>
</table>
Search for a script or a tool you wish to execute through the RDM Agent.

**Settings**
Remote Desktop Manager

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open all connections</td>
<td>When multiple sessions are selected to <strong>Execute Script Via Agent</strong>, it will open all the selected connections.</td>
</tr>
<tr>
<td>Delay</td>
<td>Enter the time delay between opening each selected session.</td>
</tr>
</tbody>
</table>

**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.

**7.8.3 Managers**

**7.8.3.1 Add-on Manager**

**Description**

The Add-on Manager is available in the **Tools – Add-on Manager** menu. It is used to simplify the management of different add-ons. It lists all of the add-ons that are supported by the current version of the application.

Add-ons are used to extend the application. They are developed by using the Remote Desktop Manager SDK. There are multiple types of add-ons:

- Application tool add-ons.
- Data source add-ons.
- Import add-ons (Filezilla, SecureCRT, etc.).
- Session tools add-ons (remote shutdown, whois...).
- Session type add-ons (Java Web Start, SQL Management Studio, etc.).
- VPN add-ons (OpenVPN, Nortel VPN, etc.).
- Data entry add-ons.
- And more.
**Settings**

The add-ons are classified by category (session, import, data source, etc.) and can be sorted according to their current status (available, outdated, uninstalled).

If the add-on doesn't require any special third party library, the manager will deploy it automatically after clicking on the install button. The same procedure applies when uninstalling an add-on.

If you're adding or removing multiple Add-ons, you can use the spacebar keystroke to quickly add and remove Add-ons.

![Add-On Manager](image)

The first column of the grid contains an icon indicating the state of the add-on. A ✔️ means the Add-on is now functional.

### 7.8.3.2 Translation Manager

**Description**

Use the *Tools – Translation Manager* to easily translate resources used by our products.

The translation manager is in fact a cloud based translation repository that is managed by an external application named Devolutions Localizer, developed by our team at Devolutions.
**Settings**

The Devolutions Localizer requires an account that you can create [here](#). Enter the requested information, submit the form and you will receive a confirmation email within 24 hours.

![Devolutions Localizer](image)

For more information on the localization process, read the [Localizer](#) topic.

### 7.8.3.2.1 Localizer

**Description**

The **Devolutions Localizer** is a "click once" application that will be installed within your application data folder and will verify automatically for updates. It is used to manipulate the cloud based translation repository.
Workflow

From the dashboard view you get a quick progress overview for each Resource file used by the application, simply choose the file you plan to work on and click the **Translate** button. You'll be presented with the following screen.
Here is a visual overview of the main features.

**Help**

**Description**
The **Help** tab contains links to the Devolutions forum and Online Help, and many support-related features, such as the **Application Logs**, the **Profiler**, and the **Recorder**.

### Help

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Help</td>
<td>Launches the Online Help you are currently browsing!</td>
</tr>
<tr>
<td>Register Product</td>
<td>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.</td>
</tr>
<tr>
<td>Blog</td>
<td>Visit our <a href="#">Blog</a>. Learn about the Devolutions Team, as well as our Goals, Products and more.</td>
</tr>
</tbody>
</table>

### Support

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications Logs</td>
<td>Opens the <strong>Application Logs</strong>. This is useful for understanding encountered errors.</td>
</tr>
<tr>
<td>Diagnostic</td>
<td>Launches the <strong>Diagnostic</strong> feature.</td>
</tr>
<tr>
<td>Profiler</td>
<td>Use the <strong>Profiler</strong> to acquire specific information. Used to diagnose connectivity issues with a data source.</td>
</tr>
<tr>
<td>Record</td>
<td>Use the <strong>Recorder</strong>. Used to help our Devolutions Support team troubleshoot the problem</td>
</tr>
<tr>
<td>Submit a Support Ticket</td>
<td>Submit a Support Ticket. Help us make your experience better by reporting experience issues or by asking for new features.</td>
</tr>
<tr>
<td>Visit our Forum</td>
<td>Visit our <a href="#">Forum</a>. You can create an account and experience the bleeding edge of our customer support.</td>
</tr>
<tr>
<td>Change History</td>
<td>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.</td>
</tr>
</tbody>
</table>

### About

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check for Updates</td>
<td>Launch the Update Manager.</td>
</tr>
<tr>
<td>About</td>
<td>Learn about Remote Desktop Manager.</td>
</tr>
</tbody>
</table>
7.9.1 Support
7.9.1.1 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.

![Remote Desktop Manager - Delete History Logs](image)

**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**.
7.9.1.2 Diagnostic

Description

If you encounter a problem with Remote Desktop Manager, you can run a system diagnostic, which is available in Help – Diagnostic. This could help diagnose or give a pointer to what kind of issues you might be experiencing.

System

The administrator item could be the possible source for security problem. This happen often when a user has the SYSDBA or is DB_OWNER of the SQL Server database. Some other issues could be related to the fact that the application is running in Terminal Services. However Remote Desktop Manager is fully compatible with Terminal Services.

FIPS related issues and solutions can be found in the specific FIPS (Encryption) troubleshooting section. If you have a Remote Desktop Manager Jump configured you can run a test of your Jump host by clicking on Jump Test.
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.

**Policy**

The Policy tab displays the list of [Group Policy Templates](#) to see if any of them has been applied.
7.9.1.3 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.

2. The Profiler data will appear in the **Performance Profiling** window.
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.
## 7.9.1.4 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.
Devolutions Web Login
8  Devolutions Web Login

Overview

Devolutions Web Login is a web browser extension used to retrieve credentials from a client application or a remote server, such as Remote Desktop Manager or Devolutions Password Server respectively. Once properly installed and connected to a source of data, Devolutions Web Login will automatically obtain credentials to log you in to any website.

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 weighted against your security requirements.

The 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.

Here is a quick overview of the Devolutions Web Login.

Store Credentials

Credentials are stored in entries, which are contained in external data sources used by a local client application such as Remote Desktop Manager, or a remote server using Devolutions Password Server. These entries usually are Website information entries. Fill in the Website and Credential fields and enable the web browser extension link.
Retrieve Credentials

Once **Devolutions Web Login is installed** and entries have the **web browser extension link enabled**, these entries are automatically retrieved from the client application or the remote server when you navigate to the website provided in the entry.
Log in to a Website

Select an entry from the list in Devolutions Web Login to fill in the login information and connect to the website.
8.1 Installation

Description

This guide will show you how to install the Devolutions Web Login. This web browser extension can be installed in the following browsers:

- Chrome
- Firefox
- Microsoft Edge
- Safari (TBD)
- Opera

8.1.1 Chrome

Description

The installation of the Devolutions Web Login in the Google Chrome web browser is fast and simple.

1. Start Google Chrome.
2. Navigate to the Devolutions Web Login download page.
3. Click the Add To Chrome button.
4. Click Add Extension in the confirmation dialog.

Once installed, access the extension by clicking ✴ in the top-right corner of the Google Chrome web browser.
8.1.2 Firefox

Description

The installation of the Devolutions Web Login in the Firefox web browser is fast and simple.

1. Start Firefox.
2. Download the extension from the Devolutions Web Login download page.
3. Click Allow in the confirmation dialog.
4. Click Add, when prompted to add Devolutions Web Login to the extension.
5. Once installed, access the extension by clicking ✳ in the top-right corner of Firefox.

8.1.3 Microsoft Edge

Description

Devolutions Web Login for Microsoft Edge extension requires several steps to complete the installation.

You must have the Windows 10 Anniversary Update to be able to install the Edge Extension.

1. Start Microsoft Edge.

2. Download the Edge extension with the Extension Manager.
   To access the Extensions Manager, navigate to Tools – Extensions Manager. Click the Install button under the Edge Extension.
   A .zip file will be downloaded. Unzip the file in the desired folder.
3. Open a command prompt and enter the following line to disable the loopback:
   `CheckNetIsolation.exe LoopbackExempt -a -n="Microsoft.MicrosoftEdge_8wekyb3d8bbwe"`

   ![Disable loopback](image)

4. In Microsoft Edge, type `about:flags` in the address bar. Under Developer Settings, enable the **Enable extension developer features** option.
5. Open the Settings and More ( ⋮ ⋮ ⋮ ) menu, and select Extensions.

6. Click the Load extension button and select the folder unzipped at step 1.
7. Devolutions Web Login is added to the Microsoft Edge web browser. Click it to open the Microsoft Edge extension settings.

8. In the Microsoft Edge extension settings, enable the Show button next to the address bar option.
Devolutions Web Login

About
Devolutions Web Login For Edge is a free form filler extension that obtains credentials from Remote Desktop Manager, Password Vault Manager and Devolutions Server.

Devolutions Web Login

- On

ID: DevolutionsWebLogin_47189BCE7CC141B6980C2F1C52BE1257
Location: \Mac\Home\Documents\DWL
Inspect: Background page

Show button next to the address bar

- On

Options
Reload extension
Remove

Microsoft Edge extension settings

The extension is now correctly installed. Access it by clicking ⭐ in the top-right corner of the Microsoft Edge web browser.

Microsoft Edge toolbar – Remote Desktop Manager

8.1.4 Safari

Description
TBD
8.1.5 Opera

Description

The installation of the Devolutions Web Login in the Opera web browser is fast and simple.

1. Start Opera.

2. Download the extension from the Devolutions Web Login download page.

3. In the Opera menu, select Extension, then Manage extensions.

4. Drag and drop the .nex file downloaded at step 2 from your download folder to the Opera web browser.
6. Click Install in the confirmation dialog.

6. Once installed, access the extension by clicking ✭ in the top-right corner of Opera.
8.2 Settings

Description

Devolutions Web Login preferences are separated in five categories.

General

The General settings allow to control the default behavior of Devolutions Web Login.
### General

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Remote Desktop Manager app</td>
<td>Used to retrieve entries from Remote Desktop Manager. The application must be opened.</td>
</tr>
<tr>
<td>Enable Password Vault Manager app (Not recommended)</td>
<td>Used to retrieve credentials from Password Vault Manager. The application must be opened.</td>
</tr>
<tr>
<td>Enable Devolutions Password Server</td>
<td>Used to retrieve credentials from Devolutions Password Server. Further configuration is necessary in the DLVS settings of Devolutions Web Login and a user must be logged in.</td>
</tr>
<tr>
<td>Destination folder</td>
<td>Choose the folder where the credentials are stored in the data source.</td>
</tr>
</tbody>
</table>

### Action options
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Automatically retrieve credentials on page  | Devolutions Web Login automatically search for credentials in the data source when connecting to a website.  
If disabled, click on the Devolutions Web Login extension icon to retrieve credential once connected to a website.  
This process can cause performance issues if there is a large amount of entries in the data source. |
| load                                        |                                                                                                                                              |
| Automatically fill in credentials on load   | Automatically try filling in the credentials when loading a web page.                                                                        |
| Automatically submit the form after filling | Automatically try submitting the credentials once the field are filled.                                                                        |

**Appearance**

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show icon in fields</td>
<td>Show the Devolutions Web Login extension icon in the credential fields.</td>
</tr>
<tr>
<td>Show save site dialog</td>
<td>Prompt to save the provided credentials when logging in to a website.</td>
</tr>
<tr>
<td>Color the filled fields</td>
<td>Color the fields filled by Devolutions Web Login.</td>
</tr>
<tr>
<td>Select your favorite color</td>
<td>Select the color to use for the colored fields.</td>
</tr>
</tbody>
</table>

**RDM (and PVM)**

**General**
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use default port</td>
<td>Use the port 19443 to communicate with the application.</td>
</tr>
<tr>
<td>Port to use</td>
<td>Specify the port to use to establish the connection between the application and the extension. Only if the default port if disabled.</td>
</tr>
<tr>
<td>RDM application key</td>
<td>Secure the port with an application key. Use the same code here and in the client application. In Remote Desktop Manager, navigate to File – Options – Browser Extensions to set the application key.</td>
</tr>
</tbody>
</table>

**Advanced**

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable native messaging</td>
<td>TBD</td>
</tr>
<tr>
<td>Use legacy API</td>
<td>Use the old browser extension API for compatibility with older versions of Remote Desktop Manager.</td>
</tr>
</tbody>
</table>

**DPS**

**General**

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server url</td>
<td>Enter the URL of the Devolutions Password Server instance to connect to.</td>
</tr>
</tbody>
</table>

**Never list**

The Never list displays the list of websites which will never prompt to save credentials. Click the trashcan icon to remove the site from the list.
8.3 Using Devolutions Web Login
8.3.1 Store Credentials

**Description**

Devolutions Web Login credentials can be retrieved from three different sources: **Remote Desktop Manager**, **Password Vault Manager** and **Devolutions Password Server**. These credentials are stored in entries, generally **Website** information type entries.

**Manually create entries**

This example show how to store credentials for Devolutions Web Login with a **Website** information entry created in Remote Desktop Manager.

1. In Remote Desktop Manager, using any data source, create an information entry of type **Website**.
Create an entry

2. Provide the following properties to the entry:

2.1. Enter a custom Name for the entry.
2.2. Set the Display mode to External.
2.3. Enter the login page URL of the desired website in the Website field.
2.4. Enter the Credentials of an account to connect to the website.
2.5. Check the Enable web browser extension link box. This allows Devolutions Web Login extension to retrieve the entry when connecting to its respective website.
Automatically create entries

When connecting to a website using a web browser with Devolutions Web Login installed, use the **Save** button in the dialog to have Devolutions Web Login create a **Website** entry in the selected application. This dialog prompts automatically when connecting to a website that does not have any credentials detected.

By default, the entry is saved in a folder named Devolutions Web Login, which will be created if it does not exists. This behavior can be changed from the **Devolutions Web Login settings**.
### 8.3.2 Retrieve Credentials

**Description**

Once properly configured, credentials are detected automatically when connecting to their respective URL.

Credentials can be retrieved from three different sources:
- Remote Desktop Manager
- Password Vault Manager
- Devolutions Password Server

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications icons</td>
<td>Select which application the credential entry should be created with.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a custom name for the entry.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username to store in the entry.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password to store in the entry.</td>
</tr>
<tr>
<td>Folder</td>
<td>Choose the folder where the entry should be saved in.</td>
</tr>
<tr>
<td>Never</td>
<td>Add the site or domain to the never list. Click the [X] to dismiss the dialog and be prompted at the next connection.</td>
</tr>
<tr>
<td>Repository</td>
<td>Select the repository where the credentials are saved in (Remote Desktop Manager only).</td>
</tr>
<tr>
<td>Save in My Vault</td>
<td>Save the credentials in the private vault of the selected application.</td>
</tr>
<tr>
<td>Save in Vault</td>
<td>Save the credentials in the vault of the selected application.</td>
</tr>
</tbody>
</table>
Entries are retrieved automatically

From Remote Desktop Manager

From the Devolutions Web Login General Settings, make sure to enable the application.
Open Remote Desktop Manager and connect to the data source holding the credentials linked to Devolutions Web Login.
Navigate to the URL of an entry linked with the browser extension. The credentials are automatically detected by Devolutions Web Login.

Click Devolutions Web Login icon in the web browser. Select the Remote Desktop Manager icon to display the list of all available credentials in the data source.
Remote Desktop Manager – Credentials retrieved from Remote Desktop Manager

Click on the credential entry, the username and password fields are then filled automatically.
8.3.2.1 From Devolutions Password Server

**Configure DWL with DPS**

In the Devolutions Web Login General settings, make sure the Devolutions Password Server is enabled.

![Remote Desktop Manager - Enable link to Devolutions Server](image)

Click the Devolutions Password Server icon and enter the URL of an instance to connect to.
Click the Login button, then enter the credentials to log in to the server.

Navigate to the URL of an entry linked with the browser extension. The credentials are automatically detected by Devolutions Web Login.
Click the Devolutions Web Login icon in the web browser. Select Devolutions Password Server to display a list of available credentials.
Devolutions Web Login - Credentials retrieved from Devolutions Password Server

Click on the credential entry, the username and password fields are then filled automatically.
8.3.3 Secure Remote Desktop Manager

Description

As mentioned in the Devolutions Web Login Overview, installing this extension in a Terminal Services environment can introduce security risks. In such environments, each user must have a distinct and secret port assigned, as well as an application passcode to prevent any other Devolutions Web Login from listening in on that port.

The application passcode is displayed in clear text, but must be kept secret by the user.

To enable this security layer, follow these steps:

1. In Remote Desktop Manager, navigate to File – Options – Browser Extensions.

2. In the browser extensions options:
   - Uncheck Use default port.
   - Enter a custom port.
   - Enter a passcode in Application key.

3. In the web browser, click the Devolutions Web Login icon, and select the Remote Desktop Manager Options.
   - Disable Use default port.
   - Enter a custom port.
   - Enter the same passcode as in the Application key field in Remote Desktop Manager.
Settings > RDM

- General
  - Use default port
  - Port to use: 4100
  - RDM application key: XXXX

- Advanced
  - Enable native messaging
  - Use legacy API
Role Based Security System
Role Based Security System

Description

Remote Desktop Manager role-based security system 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 security system efficiently.

Here are the main key points of the role based security 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 security system 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 security system, 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.

Configure a Role

To assign users to the role, click , then check the Is Member box of the respective user.
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.
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**.

**Administrators**

**Administrators** can do everything, regardless of the security. These users are usually the chief officers and senior management.

**Restricted users**
Restricted users have limited access to resources. They usually have the Add and Edit rights only. These users can be mid or first level executives, such as service desk and help desk.

Users

Users also have limited access to resources much like Restricted users. However, Users have by default the Add, Edit and Delete rights and can perform these actions on all unsecured entries.

Read only users

Read only users can only view and use resources, but cannot edit them. These users are usually external consultants.

Select the appropriate user type

When creating users, some key points must be taken into consideration. Ask yourself the following questions while configuring a new user:

- Should they be able to access any resource without restriction? These are your Administrators.
- Should they be able to add, edit, or delete entries? A User would have all of these. Alternatively, you can select specific rights with Restricted User.
- Should they be able to see sensitive information, or import and export entries? Read-Only users are best used for those who should very limited access. You can also use the privilege tab for additional control over users.

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.

Permissions are usually set on folders, and apply to all child entries. A best practice is to set all the permissions of the root folder to Never. As a result, all permissions of all entries are denied by default.
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 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.

9.1 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 Security System 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:
9.2 Scenarios

9.2.1 Simplified Security

**Description**

This feature is only available when using an Advanced Data Source.
While the following scenario is relevant for small to medium enterprises, it is not recommended for a larger business. For a scenario more suited for large enterprises, please consult the Advanced Security scenario.

Our fictional company, Windjammer, has four 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.

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.
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
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 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.
· **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.
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 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.
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.
We want the ServiceDesk to be able to use the Domain Admin credential entry as well but not the HelpDesk. For this we must grant the **View** permission to the ServiceDesk. The ServiceDesk will still be able to edit the credential entry but will never see the password. The delete permission is set to **Never**.

The last step for the Telemark child items is to set the **View** permission to the ServiceDesk and the HelpDesk on the Boston folder and leave every other permission of this folder to **Default**. This denies the Consultants to view the Boston folder. Now, the Consultants will be able to view and open entries only in the Montreal folder.
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 Settings](image)

**Telemark\Montreal - Permissions**

**In Conclusion**

The permissions are now correctly set. Note that every entry added at 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:
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.

### 9.2.2 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.

**HelpDesk** users are **Restricted Users** as well. They only have the Add right. However, they cannot add entries into the root folder.
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 user, 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.
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.
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.

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.

We grant the following permissions to the Users, ServiceDesk and HelpDesk:

- **View:** Custom; Consultants, HelpDesk, ServiceDesk.
- **Add:** Custom; ServiceDesk.
- **Edit:** Custom; ServiceDesk.
- **Delete:** Inherited; Never inherited from Root. Only the administrator can delete entries.

### Telemark - Permissions

![Telemark - Permissions](image)

- **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.
We want the ServiceDesk to be able to use the **Domain ladmin** credential entry, but not the HelpDesk. For this, we must grant the View permission to the ServiceDesk. The ServiceDesk is still able to use the credential entry but will never see the password.

- **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 ladmin** credential entry, but not the HelpDesk. For this, we must grant the View permission to the ServiceDesk. The ServiceDesk is still able to use the credential entry but will never see the password.

- **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.

- **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.
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 (its permissions have been changed to Everyone. Here is what each user should see in the 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.

9.3 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.

9.3.1 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 following rights are to be enabled in the Permissions section when creating a user:
The administrator:
- When creating the user, check the **Administrator** box to give it access to everything.

The **ServiceDesk**:
- **Add**
- **Edit**
- **Deny add entry in root folder**
The HelpDesk:
- **Add**
- **Deny add entry in root folder**

The MontrealConsultant has read-only access. He cannot see any password or entry detail.
- Leave everything disable for this user
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

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.
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.

- **View**: HelpDesk, MontrealConsultant, ServiceDesk
- **Add**: ServiceDesk
- **Edit**: ServiceDesk
- **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.

![Telemark\Credentials\Admin - Permissions](image)

- **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.
No need to set any permissions on the Montreal folder, since they are inherited from the parent folders.

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 \textit{Add} and \textit{Edit} permissions to the Administrator user/role.
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:
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 X
10  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.

PowerShell snapin
The Snapin is still delivered with Remote Desktop Manager, but not maintained. If instructions are needed on that deprecated technology, please refer to the manual of our previous version. It can be downloaded from here.

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\RemoteDesktopManager.PowerShellModule.psd1"`  

If the sample above does not work due to a different Remote Desktop Manager installation directory, simply change `$\{env:ProgramFiles(x86)\}\Devolutions\Remote Desktop Manager\RemoteDesktopManager` for the correct application path.

CmdLets
- Add-RDMRoleToUser
- Add-RDMSessionAttachment
- Close-RDMSession
- Copy-RDMSession
- Export-RDMSession
- Get-RDMCurrentDataSource
- Get-RDMDataSource
- Get-RDMDatasourceProperty
- Get-RDMInstance
- Get-RDMOpenedSession
- Get-RDMP playlistLocal
- Get-RDMP playlistShared
- Get-RDMPrivateSession
- Get-RDMRepository
- Get-RDMRole
- Get-RDMSecurityGroup
- Get-RDMSession
- Get-RDMSessionAttachment
- Get-RDMSessionCredentials
- Get-RDMSessionDocumentStoredInDatabase
- Get-RDMSessionDomain
- Get-RDMSessionPassword
- Get-RDMSessionProperty
- Get-RDMSessionStatus
- Get-RDMSessionUserName
Contents

- Get-RDMTemplate
- Get-RDMUser
- Get-RDMUserSpecificSettings
- Import-RDMSession
- Invoke-RDMCreateDataSourceDatabase
- Invoke-RDLDMFromInventorySession
- Invoke-RDMParentSession
- Invoke-RDMUnparentSession
- Invoke-RDMUpdateDataSourceDatabase
- New-RDMDataSource
- New-RDMLogComment
- New-RDMPlistLocal
- New-RDMPlistShared
- New-RDMRandomPassword
- New-RDMRepository
- New-RDMRole
- New-RDMSecurityGroup
- New-RDMSession
- New-RDMUser
- Open-RDMQuickConnect
- Open-RDMSession
- Open-RDMSyncSession
- Read-RDMSession
- Remove-RDMDataSource
- Remove-RDMRepository
- Remove-RDMRole
- Remove-RDMRoleToUser
- Remove-RDMSecurityGroup
- Remove-RDMSession
- Remove-RDMSessionAttachment
- Remove-RDMUser
- Rename-RDMGroup
- Set-RDMCurrentDataSource
- Set-RDMDatasource
- Set-RDMDataSourceMasterKey
- Set-RDMDataSourceProperty
- Set-RDMDataSourceRepository
- Set-RDMPersonalCredentials
- Set-RDMPlistLocal
- Set-RDMPlistShared
- Set-RDMPprivateSession
- Set-RDMRepository
- Set-RDMRole
- Set-RDMRoleGroupRights
- Set-RDMRoleProperty
- Set-RDMSecurityGroup
- Set-RDMSecurityGroupProperty
- Set-RDMSession
- Set-RDMSessionAttachment
- Set-RDMSessionCredentials
- Set-RDMSessionDocument
- Set-RDMSessionDomain
- Set-RDMSessionPassword
- Set-RDMSessionProperty
10.1 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.
<table>
<thead>
<tr>
<th>SETTING</th>
<th>WELL KNOWN GUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td>Credential repository --- Prompt on connection ---</td>
<td>&quot;45479560-173E-435D-8848-C22F863FDC96&quot;</td>
</tr>
<tr>
<td>Embedded</td>
<td>should be used for backwards compatibility only, we prefer not to list it here.</td>
</tr>
<tr>
<td>Parent (only for sub-connections)</td>
<td>&quot;E2CC9029-CA3A-4308-BA54-16D5029BC8ED&quot;</td>
</tr>
<tr>
<td>Inherited</td>
<td>&quot;1310CF82-6FAB-4B7A-9EEA-3E2E451CA2CF&quot;</td>
</tr>
<tr>
<td>My personal credentials</td>
<td>&quot;9F3C3BCF-068A-4927-B996-CA52154CAE3B&quot;</td>
</tr>
<tr>
<td>None</td>
<td>&quot;B87B29D9-9239-4D7B-86D8-9B53DCD3BA9F&quot;</td>
</tr>
<tr>
<td>Private Vault, paired with</td>
<td>&quot;245A4245-48E7-4DF5-9C4C-11861D8E1F81&quot;</td>
</tr>
<tr>
<td>PersonalConnectionID</td>
<td></td>
</tr>
<tr>
<td>Private Vault Search, paired with</td>
<td>&quot;88E4BE76-4C5B-4694-AA9C-D53B7E0FE0DC&quot;</td>
</tr>
<tr>
<td>CredentialPrivateVaultsearchString</td>
<td></td>
</tr>
</tbody>
</table>

**Tips and tricks**

- Use the Set-RDMProperty 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!

**10.2 PowerShell Samples**

**Description**

These are the recipes to perform various tasks using our PowerShell cmdlets.

**10.2.1 Creating an entry**

**Description**

This sample creates an entry.

**Sample**

```powershell
$computerName = "wind10";
$theusername = "david";
$thedomain = "windjammer";
$thepassword = "123456";
$session = New-RDMSession -Host $computerName -Type "RDPQualified" -Name $computerName;
Set-RDMSession -Session $session -Refresh;
Update-RDmui;
Set-RDMSessionUsername -ID $session.ID $theusername;
Set-RDMSessionDomain -ID $session.ID $thedomain;
$pass = ConvertTo-SecureString $thepassword -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

10.2.2 Creating Group Folder Structure from CSV file

Description

Please note that the CSV file must be encoded in UTF-8 to support special characters.

This sample creates a Group Folder structure from a CSV file.

Sample

$csv = Import-Csv "c:\YourFolder\GroupFolder.csv"
foreach ($csvEntry in $csv) {
    $groupName = $csvEntry.Name
    # Extract the group folder name
    if ($groupName.Contains("\") { }
        $groupName = $groupName.Substring($groupName.LastIndexOf("\"), $groupName.Length -
    $groupName = $groupName.TrimStart("\")
    
    # Create the group folder if it is not null, empty or fill in with space characters
    if (![string]:IsNullOrWhiteSpace($groupName)) { 
        $session = New-RDMSession -Type "Group" -Name $groupName
        $session.Group = $csvEntry.Name
        Set-RDMSession $session
        Write-Host "Group Folder $groupName created" -f Yellow
    }
}

Update-RDMUI

Notes

The CSV file must have only one column with the title set as Name.
The full path must be specified for each sub folder.

Here is an example of this CSV file:
10.3 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 provide 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

```powershell
$connection.Web.OnlySendPasswordInPasswordField = $false;
$RDM.Save ();
```

Enable View Url Embedded (Information Entries)
Remote Desktop Manager

```csharp
$connection.DataEntry.ViewUrlDisplayMode = "Default";
$RDM.Save();

ViewUrlDisplayMode: "Default" = embedded, "External" = external.

Open URL (external) for Web Login (Information Entries)

```csharp
$connection.DataEntry.DefaultAction = "OpenUrlExternal";
$RDM.Save();

SSH Shell Batch Edit (Session Type Settings)

```csharp
$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

```csharp
$connection.ConnectionType = 'LogMeIn';
$connection.ConnectionSubType = '' ;
$connection.LogMeIn.Url = $connection.WebBrowserUrl;
$RDM.Save();

Enable the "Hide script errors in all your LogMeIn sessions."

```csharp
$connection.LogMeIn.ScriptErrorsSuppressed = $true;
$RDM.Save();

Hide navigation bar.

```csharp
$connection.LogMeIn.ShowUrl = $false;
$RDM.Save();

Change the Web Browser Application.
Enable the Sandbox Process.

```powershell
$connection.LogMeIn.SandboxProcess = $true;
$RDM.Save();
```

Change the URL.

```powershell
$connection.LogMeIn.Url = " ";
$RDM.Save();
```

Change the Portal Login field.

```powershell
$connection.LogMeIn.DashboardHostUrl = " ";
$RDM.Save();
```

Change Username & Password.

Please run these two one at a time

**Host:**

```powershell
$connection.LogMeIn.UserName = " ";
$RDM.Save();
```

```powershell
$connection.LogMeIn.SafePassword = " ";
$RDM.Save();
```

**Portal:**

```powershell
$connection.LogMeIn.DashboardEmail = " ";
$RDM.Save();
```

```powershell
$connection.LogMeIn.SafePasswordDashboard = " ";
$RDM.Save();
```

Change a custom field value without changing the data

```powershell
$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.**

```powershell
$connection.host = $Connection.name + ".mydomain.com"
$RDM.Save();
```
**Bulk Change Recording Field for Putty sessions**

```powershell
$connection.Putty.RecordingMode = 1;
$connection.Putty.RecordingFileName = "C:\path\to\your\file.log"
$RDM.Save();
```

**Change the computer field of an RDP session**

```powershell
$connection.Url = "";
$RDM.Save();
```

**Encoding**

```powershell
$connection.Putty.TelnetEncoding = "UTF-8";
$RDM.Save();
```

**Change the expiration date of an RDP session**

The date must be specified using the ISO8601 format.

```powershell
$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.

```powershell
$connection.MetaInformation.Expiration = (Get-Date).AddMonths(6);
$RDM.Save();
```

**Modify Page Tab Title in UI**

```powershell
$connection.TabTitle = '$COMPANY_NAME$ - $NAME$';
$RDM.Save();
```

**Clear Keywords in Session**

```powershell
$connection.MetaInformation.Keywords = "";
$RDM.Save();
```

**Change History Max lines for SSH Shell (Rebex)**

```powershell
$connection.Putty.HistoryMaxLength = 2000;
$RDM.Save();
```
Convert Command Line tool to a Command Line session

```powershell
$connection.ConnectionType = 3;
$RDM.Save();
```

Change Keyboard Hook for an RDP session

```powershell
$connection.KeyboardHook = "OnTheRemoteComputer";
$RDM.Save();
```

### 10.4 Add-RDMRoleToUser

**SYNOPSIS**

Add role to an user

**SYNTAX**

```
Add-RDMRoleToUser -RoleName [RoleName] <String> -RoleObject [RoleObject] <PSRoleInfo> -UserName [UserName] <String> -UserObject [UserObject] <PSUserInfo> [CommonParameters]
```

**DESCRIPTION**

Add role to an user

**PARAMETERS**

- `-RoleName <String>` (Required) Role name

- `-RoleObject <PSRoleInfo>` (Required) Role object, must be retrieved from Get-RDMRole or created via New-RDMRole.

- `-UserName <String>` (Required) username

- `-UserObject <PSUserInfo>` (Required) User object, must be retrieved from Get-RDMSecurityGroup or created via New-RDMUser.

<CommonParameters>

This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

**NOTES**

For more information, type "Get-Help Add-RDMRoleToUser -detailed". For technical information, type "Get-Help Add-RDMRoleToUser -full".

**EXAMPLE 1**

```
PS C:\> Add-RDMRoleToUser -RoleObject $role -UserObject $user
```

Add role to an user.

**RELATED LINKS**
10.5 Close-RDMSession

SYNOPSIS
Close a session

SYNTAX

DESCRIPTION
Close a session

PARAMETERS
-Force <SwitchParameter>
Forces close of the Session without confirmation by the user. Optional.

-ID <Guid>
(Required) Specifies the ID of the session to be closed.
Must be a valid GUID, in the form {00000000-0000-0000-0000-000000000000}.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Close-RDMSession -detailed". For technical information, type "Get-Help Close-RDMSession -full".

EXAMPLE 1
PS C:\> Close-RDMSession -ID 00000000-0000-0000-0000-000000000000

Close a session.

RELATED LINKS

10.6 Copy-RDMSession

SYNOPSIS
Copy a session.

SYNTAX
Copy-RDMSession -DontChangeID [DontChangeID] <SwitchParameter> -IncludePasswordHistory
[IncludePasswordHistory] <SwitchParameter> -IncludeSubConnections [IncludeSubConnections]
<SwitchParameter> -PSConnection [PSConnection] <PSConnection[]] -ResolveVariables
[ResolveVariables] <SwitchParameter> [CommonParameters>

DESCRIPTION
Copy a session.

PARAMETERS
-DontChangeID <SwitchParameter>
Copy the session without changing the ID
-IncludePasswordHistory <SwitchParameter>
  Include password history in the session copy

-IncludeSubConnections <SwitchParameter>
  Include sub connections in the session copy

-PSConnection <PSConnection[]>
  (Required) Session to copy

-ResolveVariables <SwitchParameter>
  Resolve variables in the session copy

<CommonParameters>
  This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable,
  WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help
  about_commonparameters".

NOTES
  For more information, type "Get-Help Copy-RDMSession -detailed". For technical information, type "Get-
  Help Copy-RDMSession -full".

RELATED LINKS

10.7 Export-RDMSession

SYNOPSIS
  Export a list of sessions to a file

SYNTAX
  Export-RDMSession -CSV [CSV] <SwitchParameter> -ExcludeSessionPassword [ExcludeSessionPassword]
  <SwitchParameter> -HTML [HTML] <SwitchParameter> -IncludeCredentials [IncludeCredentials]
  <SwitchParameter> -IncludeSecurityGroups [IncludeSecurityGroups] <SwitchParameter> -Password
  <SwitchParameter> [<CommonParameters>]

DESCRIPTION
  Export a list of sessions to a file

PARAMETERS
  -CSV <SwitchParameter>
  (Required) Export the sessions into a CSV file

  -ExcludeSessionPassword <SwitchParameter>
  Don't export the password in the connections exported

  -HTML <SwitchParameter>
  (Required) Export the sessions into a HTML file

  -IncludeCredentials <SwitchParameter>
  Include credentials in the export (Only available for the XML type).

  -IncludeSecurityGroups <SwitchParameter>
  Include Security Groups in the export (Only available for the XML type).
-Password <SecureString>
  Password.

-Path <String>
  (Required) Path where the file will be the saved. Must end with:


-Sessions <PSConnection[]>
  (Required) Sessions.

-XML <SwitchParameter>
  (Required) Export the sessions into a XML file

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable,OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Export-RDMSession -detailed". For technical information, type "Get-Help Export-RDMSession -full".

EXAMPLE 1
PS C:\> $sessions = get-rdmsession; $password = read-host -assecurestring "Password"; Export-RDMSession -XML -Path C:\MyPath\MyFilename.xml -Sessions $sessions -Password $password

Retrieves the list of available sessions and export them to a xml file at C:\MyPath\Filename.xml.

RELATED LINKS

10.8 Get-RDMCurrentDataSource

SYNOPSIS
Retrieve the active data source.

SYNTAX
Get-RDMCurrentDataSource [<CommonParameters>]

DESCRIPTION
Retrieve the active data source.

PARAMETERS
<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable,OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Get-RDMCurrentDataSource -detailed". For technical information, type "Get-Help Get-RDMCurrentDataSource -full".

EXAMPLE 1
PS C:\> $list = Get-RDMCurrentDataSource
The current active data sources.

RELATED LINKS

10.9 Get-RDMDataSource

SYNOPSIS
Retrieve the list of available data sources.

SYNTAX
Get-RDMDataSource -Name [Name] <String> [<CommonParameters>]

DESCRIPTION
Retrieve the list of available data sources.

PARAMETERS
-Name <String>
Data source name

<CommonParameters>
This cmdlet supports the common parameters:Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Get-RDMDataSource -detailed". For technical information, type "Get-Help Get-RDMDataSource -full".

EXAMPLE 1
PS C:\> $list = Get-RDMDataSource

Retrieves the list of available data sources.

EXAMPLE 2
PS C:\> $list = Get-RDMDataSource; $list[0]

Retrieves the list of available data sources and displays the first item.

EXAMPLE 3
PS C:\> $list = Get-RDMDataSource; Set-RDMDataSource $list[1].ID

Retrieves the list of available data sources and sets the current data source the second element in the list.

RELATED LINKS
Set-RDMDataSource

10.10 Get-RDMDatasourceProperty

SYNOPSIS
Get the value of property given for a dataSource.

SYNTAX
Get-RDMDataSourceProperty -DataSource [DataSource] <PSDataSource> -Property [Property] <String> [<CommonParameters>]

DESCRIPTION
Protected values will always return null.

PARAMETERS
-DataSource <PSDataSource> (Required) Specifies the datasource
-Property <String> (Required) Property to set.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Get-RDMDataSourceProperty -detailed". For technical information, type "Get-Help Get-RDMDataSourceProperty -full".

RELATED LINKS

10.11 Get-RDMInstance

SYNOPSIS
Get the instance info

SYNTAX
Get-RDMInstance [<CommonParameters>]

DESCRIPTION
Get the instance info

PARAMETERS
<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Get-RDMInstance -detailed". For technical information, type "Get-Help Get-RDMInstance -full".

RELATED LINKS

10.12 Get-RDMOpenedSession

SYNOPSIS
Retrieve the list of opened sessions of the current data source.

SYNTAX
Get-RDMOpenedSession [<CommonParameters>]
**DESCRIPTION**
Retrieve the list of opened sessions of the current data source.

**PARAMETERS**
<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

**NOTES**
For more information, type "Get-Help Get-RDMOpenedSession -detailed". For technical information, type "Get-Help Get-RDMOpenedSession -full".

**EXAMPLE 1**
PS C:\> $list = Get-RDMOpenedSession
Retrieves the list of available data sources of the current data source.

**EXAMPLE 2**
PS C:\> $list = Get-RDMOpenedSession; $list[0]
Retrieves the list of the opened sessions and displays the first item.

**RELATED LINKS**

### 10.13 Get-RDMPlaylistLocal

**SYNOPSIS**
Get the local playlists of the current data source

**SYNTAX**
Get-RDMPlaylistLocal -ExportConnection [ExportConnection] <SwitchParameter> [<CommonParameters>]

**DESCRIPTION**
Get the local playlists of the current data source

**PARAMETERS**
-ExportConnection <SwitchParameter>
Export the playlist connections.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

**NOTES**
For more information, type "Get-Help Get-RDMPlaylistLocal -detailed". For technical information, type "Get-Help Get-RDMPlaylistLocal -full".

**EXAMPLE 1**
PS C:\> $playlists = Get-RDMPlaylistLocal
Get the local playlists of the current data source.

RELATED LINKS

10.14 Get-RDMPlaylistShared

SYNOPSIS
Get the shared playlists of the current data source

SYNTAX
Get-RDMPlaylistShared -ExportConnections [ExportConnections] <SwitchParameter> [<CommonParameters>]

DESCRIPTION
Get the shared playlists of the current data source

PARAMETERS
-ExportConnections <SwitchParameter>
Export the playlist connections.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Get-RDMPlaylistShared -detailed". For technical information, type "Get-Help Get-RDMPlaylistShared -full".

EXAMPLE 1
PS C:\> $playlists = Get-RDMPlaylistShared

Get the shared playlists of the current data source.

RELATED LINKS

10.15 Get-RDMPrivateSession

SYNOPSIS
Retrieve the list of available sessions from the user Private Vault.

SYNTAX
Get-RDMPrivateSession -GroupName [GroupName] <String> [-IncludeDocumentsStoredInDatabase [IncludeDocumentsStoredInDatabase] <SwitchParameter> -IncludeLocalPlaylists [IncludeLocalPlaylists] <SwitchParameter> -IncludeSubFolders [IncludeSubFolders] <SwitchParameter> -IncludeUserSpecificSettings [IncludeUserSpecificSettings] <SwitchParameter> -Name [Name] <String> [<CommonParameters>]

DESCRIPTION
Retrieve the list of available sessions from the user Private Vault for the current selected data source.

PARAMETERS
-GroupName <String>
GroupName
-IncludeDocumentsStoredInDatabase <SwitchParameter>
Include attachment from documents

-IncludeLocalPlaylists <SwitchParameter>
Include dependable connections and local playlists from playlist connection

-IncludeSubFolders <SwitchParameter>
Include subfolders from the group name

-IncludeUserSpecificSettings <SwitchParameter>
Include user Specific Settings

-Name <String>
Session name

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Get-RDMPrivateSession -detailed". For technical information, type "Get-Help Get-RDMPrivateSession -full".

RELATED LINKS
Get-RDMDataSource
Set-RDMDataSource
Set-RDMPrivateSession

10.16 Get-RDMRole

SYNOPSIS
Retrieve the list of available roles.

SYNTAX
Get-RDMRole -Name [Name] <String> [<CommonParameters>]

DESCRIPTION
Retrieve the list of available roles for the current selected data source.

PARAMETERS
-Name <String>
Role name

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Get-RDMRole -detailed". For technical information, type "Get-Help Get-RDMRole -full".
EXAMPLE 1
PS C:\> Get-RDMRole

Retrieves the list of available role.

EXAMPLE 2
PS C:\> $list = Get-RDMRole; $list[0]

Retrieves the list of available roles and displays the first item.

EXAMPLE 3
PS C:\> $list = Get-RDMRole; $list[1].Name = "New Name";Set-RDMRole $list[1]

Retrieves the list of available roles, modify the name of the second role, update the role.

RELATED LINKS
New-RDMRole
Remove-RDMRole
Set-RDMRole
Set-RDMRoleProperty

10.17 Get-RDMSecurityGroup

SYNOPSIS
Retrieve the list of available security groups.

SYNTAX
Get-RDMSecurityGroup -Name [Name] <String> [<CommonParameters>]

DESCRIPTION
Retrieve the list of available security groups for the current selected data source. Security group list contains a column "Session" that can be directly manipulated then updated. (see Set-RDMSessionCommand for more detail).

PARAMETERS
-Name <String>
Security group name

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES

EXAMPLE 1
PS C:\> Get-RDMSecurityGroup

Retrieves the list of available security groups.

EXAMPLE 2
PS C:\> $list = Get-RDMSecurityGroup; $list[0]
Retrieves the list of available security groups and displays the first item.

EXAMPLE 3
PS C:\> $list = Get-RDMSecurityGroup; $list[1].Name = "New Name"; Set-RDMSecurityGroup $list[1]

Retrieves the list of available security groups, modify the name of the second security group, update the security group.

RELATED LINKS
New-RDMSecurityGroup
Remove-RDMSecurityGroup
Set-RDMSecurityGroup
Set-RDMSecurityGroupProperty

10.18 Get-RDMSession

SYNOPSIS
Retrieve the list of available sessions.

SYNTAX

DESCRIPTION
Retrieve the list of available sessions for the current selected data source.

PARAMETERS
-CaseSensitive <SwitchParameter>
Case sensitive

-GroupName <String>
GroupName

-IncludeDocumentsStoredInDatabase <SwitchParameter>
Include attachment from documents

-IncludeLocalPlaylists <SwitchParameter>
Include dependable connections and local playlists from playlist connection

-IncludeSubFolders <SwitchParameter>
Include subfolders from the group name

-IncludeUserSpecificSettings <SwitchParameter>
Include user Specific Settings

-Name <String>
Session name

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Get-RDMSession -detailed". For technical information, type "Get-Help Get-RDMSession -full".

EXAMPLE 1
PS C:\> Get-RDMSession

Retrieves the list of available sessions.

EXAMPLE 2
PS C:\> $list = Get-RDMSession; $list[0]

Retrieves the list of available sessions and displays the first item.

EXAMPLE 3
PS C:\> $list = Get-RDMSession; $list[1].Name = "New Name"; Set-RDMSession $list[1]

Retrieves the list of available sessions, modify the name of the second session, update the session.

RELATED LINKS
Get-RDMDataSource
Set-RDMDataSource
Set-RDMSession

10.19 Get-RDMSessionStatus

SYNOPSIS
Get the status from the specified session.

SYNTAX

DESCRIPTION
Get the status from the specified session.

PARAMETERS
-ID <Guid>
(Required) Specifies the ID of the session to get the status from.

Must be a valid GUID, in the form {00000000-0000-0000-0000-000000000000}.

-Session <PSConnection>
(Required) Specifies the session to set the status to

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Get-RDMSessionStatus -detailed". For technical information, type "Get-Help Get-RDMSessionStatus -full".

**EXAMPLE 1**
PS C:\> Get-RDMSessionStatus "{00000000-0000-0000-0000-000000000000}"  
Get the status from the session with ID = "{00000000-0000-0000-0000-000000000000}".

**EXAMPLE 2**
PS C:\> $list = Get-RDMSession; Get-RDMSessionStatus $list[1]  
Retrieves the list of available sessions and gets the status from the second element in the list.

**RELATED LINKS**
Get-RDMSession  
Get-RDMSessionPassword  
Get-RDMSessionUserName  
Set-RDMSessionDomain  
Set-RDMSessionPassword  
Set-RDMSessionStatus  
Set-RDMSessionUsername

## 10.20 Get-RDMSessionCredentials

**SYNOPSIS**
Returns the session credentials

**SYNTAX**
Get-RDMSessionCredentials -GetID [GetID] <SwitchParameter> -PSConnection [PSConnection]  
<PSConnection> [<<CommonParameters>>]

**DESCRIPTION**
Returns the session credentials

**PARAMETERS**
-GetID <SwitchParameter>
  Get the credential ID.

-PSConnection <PSConnection>  
  (Required) Specifies the connection to get credentials from.

<CommonParameters>
  This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable,  
  WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help  
  about_commonparameters".

**NOTES**
For more information, type "Get-Help Get-RDMSessionCredentials -detailed". For technical information,  
type "Get-Help Get-RDMSessionCredentials -full".

**RELATED LINKS**
10.21 Get-RDMSessionDocumentStoredInDatabase

SYNOPSIS
Get documents stored in database

SYNTAX
Get-RDMSessionDocumentStoredInDatabase [CommonParameters]

DESCRIPTION
Get documents stored in database

PARAMETERS
CommonParameters
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Get-RDMSessionDocumentStoredInDatabase -detailed". For technical information, type "Get-Help Get-RDMSessionDocumentStoredInDatabase -full".

RELATED LINKS

10.22 Get-RDMSessionDomain

SYNOPSIS
Get the domain from the specified session.

SYNTAX

DESCRIPTION
Get the domain from the specified session.

PARAMETERS
-ID <Guid>
(Required) Specifies the ID of the session to get the domain from.

Must be a valid GUID, in the form (00000000-0000-0000-0000-000000000000).

-Session <PSConnection>
(Required) Specifies the session to set the domain to

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Get-RDMSessionDomain -detailed". For technical information, type "Get-Help Get-RDMSessionDomain -full".

EXAMPLE 1
PS C:\> Get-RDMSessionDomain "{00000000-0000-0000-0000-000000000000}"
Get the domain from the session with ID = "{00000000-0000-0000-0000-000000000000}".

**EXAMPLE 2**

PS C:\> $list = Get-RDMSession; Get-RDMSessionDomain $list[1].ID

Retrieves the list of available sessions and gets the domain from the second element in the list.

**RELATED LINKS**

Get-RDMSession
Get-RDMSessionPassword
Get-RDMSessionUserName
Set-RDMSessionDomain
Set-RDMSessionPassword
Set-RDMSessionUsername

### 10.23 Get-RDMSessionPassword

**SYNOPSIS**

Get the password from the specified session.

**SYNTAX**


**DESCRIPTION**

Get the password from the specified session. Session must be marked as "Allow show credentials" if not null is returned.

**PARAMETERS**

- **-AsPlainText** <SwitchParameter>
  
  Returns the password as plain text.

- **-ID** <Guid>
  
  (Required) Specifies the ID of the session to get the password from.

  Must be a valid GUID, in the form {00000000-0000-0000-0000-000000000000}.

- **-Session** <PSConnection>
  
  (Required) Specifies the session to get the password from.

  <CommonParameters>

  This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

**NOTES**

For more information, type "Get-Help Get-RDMSessionPassword -detailed". For technical information, type "Get-Help Get-RDMSessionPassword -full".

**EXAMPLE 1**

PS C:\> Get-RDMSessionPassword "{00000000-0000-0000-0000-000000000000}"

Get the password from the session with ID = "{00000000-0000-0000-0000-000000000000}".
EXAMPLE 2
PS C:\> $list = Get-RDMSession; Get-RDMSessionPassword $list[1].ID

Retrieves the list of available sessions and gets the password from the second element in the list.

RELATED LINKS
Get-RDMSession
Get-RDMSessionDomain
Get-RDMSessionUserName
Set-RDMSessionDomain
Set-RDMSessionPassword
Set-RDMSessionUsername

10.24 Get-RDMSessionProperty

SYNOPSIS
Get the value of property given a session ID and path.

SYNTAX

DESCRIPTION
Protected values will always return null.

PARAMETERS
-ID <Guid>(Required) Specifies the ID of the session to get the password from.
Must be a valid GUID, in the form {00000000-0000-0000-0000-000000000000}.

-Path <String>
The path to the property being read (reference RDM export xml). If top level property do not specify parameter or pass empty string ["""] or $null

-Property <String>(Required) Property to read(get).

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Get-RDMSessionProperty -detailed". For technical information, type "Get-Help Get-RDMSessionProperty -full".

EXAMPLE 1
PS C:\> Get-RDMSessionProperty -ID "{00000000-0000-0000-0000-000000000000}" -Property "Group"

Get the Group value from the session with ID = "{00000000-0000-0000-0000-000000000000}".

EXAMPLE 2
Get the MetaInformation.OS value from the session with ID = "(00000000-0000-0000-0000-000000000000)".

EXAMPLE 3
PS C:\> $list = Get-RDMSession; Get-RDMSessionProperty -ID $list[1].ID -Path "MetaInformation" -Property "OS"
Retrieves the list of available sessions and then returns MetaInformation.OS value of the second element in the list.

RELATED LINKS
Get-RDMSession
Set-RDMSessionProperty

10.25 Get-RDMSessionUserName
SYNOPSIS
Get the username from the specified session.

SYNTAX

DESCRIPTION
Get the username from the specified session.

PARAMETERS
-ID <Guid>(Required) Specifies the ID of the session to get the username from.
Must be a valid GUID, in the form {00000000-0000-0000-0000-000000000000}.

-Session <PSConnection>(Required) Specifies the session to set the username to.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable,OutBuffer and OutVariable.For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Get-RDMSessionUserName -detailed”. For technical information, type "Get-Help Get-RDMSessionUserName -full”.

EXAMPLE 1
PS C:\> Get-RDMSessionUserName "(00000000-0000-0000-0000-000000000000)"
Get the username from the session with ID = "(00000000-0000-0000-0000-000000000000)".

EXAMPLE 2
PS C:\> $list = Get-RDMSession; Get-RDM-Password $list[1].ID
Retrieves the list of available sessions and gets the password from the second element in the list.
10.26 Get-RDMTemplate

SYNOPSIS
Retrieve the list of available templates.

SYNTAX
Get-RDMTemplate -Type [Type] <String> [CommonParameters]

DESCRIPTION
Retrieve the list of available templates. The current selected template is marked with an "X".

PARAMETERS
-Type <String>
Type of templates

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Get-RDMTemplate -detailed". For technical information, type "Get-Help Get-RDMTemplate -full".

EXAMPLE 1
PS C:\> $list = Get-RDMTemplate
Retrieves the list of available templates.

EXAMPLE 2
PS C:\> $list = Get-RDMTemplate; $list[0]
Retrieves the list of available templates and displays the first item.

RELATED LINKS
Set-RDMDataSource

10.27 Get-RDMUser

SYNOPSIS
Retrieve the list of available users.

SYNTAX
Get-RDMUser -Name [Name] <String> [CommonParameters]

DESCRIPTION
Retrieve the list of available users for the current selected data source.

PARAMETERS
-Name <String>
  username

<CommonParameters>
  This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
  For more information, type "Get-Help Get-RDMUser -detailed". For technical information, type "Get-Help Get-RDMUser -full".

EXAMPLE 1
  PS C:\> Get-RDMUser

  Retrieves the list of available user.

EXAMPLE 2
  PS C:\> $list = Get-RDMUser; $list[0]

  Retrieves the list of available users and displays the first item.

EXAMPLE 3
  PS C:\> $list = Get-RDMUser; $list[1].Description = "New Description"; Set-RDMUser $list[1]

  Retrieves the list of available users, modify the name of the second user, update the user.

RELATED LINKS
  New-RDMUser
  Remove-RDMUser
  Set-RDMUser
  Set-RDMUserProperty

10.28 Get-RDMUserSpecificSettings

SYNOPSIS
Get the session user Specific Settings

SYNTAX
Get-RDMUserSpecificSettings -Session [Session] <PSConnection> [<CommonParameters>]

DESCRIPTION
Get the session user Specific Settings

PARAMETERS
  -Session <PSConnection>
  (Required) PSSession object, must be retrieved from Get-RDMSession or created via New-RDMSession.

  <CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Get-RDMUserSpecificSettings -detailed". For technical information, type "Get-Help Get-RDMUserSpecificSettings -full".

RELATED LINKS

10.29 Import-RDMSession

SYNOPSIS
Import RDM session from a file

SYNTAX

DESCRIPTION
Import RDM session from a file

PARAMETERS
-DuplicateAction <String>
Action when a duplicate is found. Must be one of the following:

"Add", "Overwrite", "Ignore"

-Group <String>
The group where the sessions will be saved.

-Path <String>
(Required) Path where the file is loaded. Must be finish:

"RDM: .rdm", "XML: .xml"

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Import-RDMSession -detailed". For technical information, type "Get-Help Import-RDMSession -full".

EXAMPLE 1
PS C:\> Import-RDMSession -Path "C:\MyFile.rdm" -Group "DestinationGroup" -DuplicateAction "Add"

RELATED LINKS
10.30 Invoke-RDMParentSession

SYNOPSIS
Invoke a refactoring action to move a connection under a parent connection.

SYNTAX

DESCRIPTION
Move a session under a parent session.

PARAMETERS
-ParentSession <PSConnection> (Required) PSCConnection object, must be retrieved from Get-RDMSession or created via New-RDMSession that you will become the parent of the sessions.

-Refresh <SwitchParameter>
Send refresh notification to Remote Desktop Manager application.

-Session <PSConnection[]>
(Required) PSCConnection object, must be retrieved from Get-RDMSession or created via New-RDMSession that will become a subconnection of the parent session.

-UseInheritedVPN <SwitchParameter>
Use inherited VPN.

-UseParentCredentials <SwitchParameter>
Use parent credentials.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Invoke-RDMParentSession -detailed". For technical information, type "Get-Help Invoke-RDMParentSession -full".

EXAMPLE 1
PS C:\> $list = Get-RDMSession; $parent = $list[0]; $child = $list[1]; Invoke-RDMParentSession -ParentSession $parent -Session $child -Refresh

Session in the variable $child becomes a subconnection of the session in the variable $parent and refresh the sessions.

RELATED LINKS
Invoke-RDMUnparentSession
10.31 Invoke-RDMUnparentSession

SYNOPSIS
Invoke a refactoring action to move out a connection under a parent connection.

SYNTAX
Invoke-RDMUnparentSession -Refresh [Refresh] <SwitchParameter> -Session [Session] <PSConnection[]> [CommonParameters>

DESCRIPTION
Move out a session under a parent session.

PARAMETERS
-Refresh <SwitchParameter>
Send refresh notification to Remote Desktop Manager application.

-Session <PSConnection[]>
(Required) PSSession object, must be retrieved from Get-RDMSession or created via New-RDMSession that you want to unparented.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Invoke-RDMUnparentSession -detailed". For technical information, type "Get-Help Invoke-RDMUnparentSession -full".

EXAMPLE 1
PS C:\> $list = Get-RDMSession; $parent = $list[0]; Invoke-RDMUnparentSession -Session $parent.SubConnections -Refresh
The subconnections in the session in the variable $parent are unparented.

RELATED LINKS
Invoke-RDMParentSession

10.32 New-RDMDDataSource

SYNOPSIS
Create a new datasource instance.

SYNTAX

DESCRIPTION
Create a new datasource instance. The instance has not yet been saved. Assign the result to a variable then call "Set-RDMDatasource $s" to save the datasource.

PARAMETERS
-Access <SwitchParameter>
  (Required) Create a Microsoft Access data source

-AccessKeyID <String>
  (Required) Enter the Amazon S3 Access Key ID.

-BucketName <String>
  (Required) Enter the bucket's name created on Amazon S3 website and used by the application

-Database <String>
  (Required) Indicates the filename of the SQLite database (.db).

-DatabaseID <String>
  (Required) Unique Key to identify the data source.

-DODB <SwitchParameter>
  (Required) Create a Devolutions Online Database data source

-DontSavePassword <SwitchParameter>
  Don't save the password in the SQL Server data source settings

-Dropbox <SwitchParameter>
  (Required) Create a Dropbox data source

-DVLS <SwitchParameter>
  (Required) Create a DVLS data source

-Filename <String>
  (Required) XML Filename

-FTP <SwitchParameter>
  (Required) Create a FTP data source

-FTPHost <String>
  (Required) FTP server name to access the XML file.

-FTPPath <String>
  (Required) FTP server name to access the XML file.

-Hostname <String>
  (Required) Name of the server where the data source will be store.

-IntegratedSecurity <SwitchParameter>
  Specify to use Windows Integrated Authentication for authenticating to the data source
KeyName <String>
   Name of the file that will be used to store the data on Amazon S3.

MySQL <SwitchParameter>
   (Required) Create a MySQL data source

Name <String>
   (Required) Name of the data source.

Password <SecureString>
   (Required) Password used to access the FTP server.

S3 <SwitchParameter>
   (Required) Create an Amazon S3 data source

Schema <String>
   (Required) Name of the schema on the MySQL server for the utilization of Remote Desktop Manager.

SecretAccessKey <SecureString>
   (Required) Enter the Amazon S3 Access Key ID.

Server <String>
   (Required) Name of Devolutions Server instance.

SetDatasource <SwitchParameter>
   Save the data source.

SFTP <SwitchParameter>
   (Required) Create an SFTP data source

SQLite <SwitchParameter>
   (Required) Create a SQLite data source

SQLServer <SwitchParameter>
   (Required) Create a SQL Server data source

URLFilename <String>
   (Required) Indicate the web location of the data source and the name of data source file.

UserEditable <SwitchParameter>
   Editable username

Username <String>
   (Required) Username used to access the FTP server.

Web <SwitchParameter>
   (Required) Create a Web data source

XML <SwitchParameter>
   (Required) Create an XML data source

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help New-RDMDDataSource -detailed". For technical information, type "Get-Help New-RDMDDataSource -full".

RELATED LINKS
Set-RDMDDataSource

10.33 New-RDMLLogComment

SYNOPSIS
Create a log comment.

SYNTAX

DESCRIPTION
Create and insert a new log comment.

PARAMETERS
-Comment <String>
Log comment.

-EndDateTime <Boolean>
End date.

-Notes <String>
(Required) Log notes.

-Session <PSConnection>
(Required) Session object, must be retrieved from Get-RDMSession or created via New-RDMSession.

-StartDateTime <DateTime>
(Required) Start date.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help New-RDMLLogComment -detailed". For technical information, type "Get-Help New-RDMLLogComment -full".

EXAMPLE 1
PS C:\> $sessions = Get-RDMSession;$date = Get-Date;New-RDMLLogComment -Comment "MyComment" -Notes "MyNotes" -Session $sessions[2] -StartDateTime $date -EndDateTime $date.AddDays(3)
Create & save a new log comment.

RELATED LINKS

10.34 New-RDMPlaylistLocal

SYNOPSIS
Create a new local playlist

SYNTAX

DESCRIPTION
Create a new local playlist

PARAMETERS
-Connections <Connection[]> (Required) Connections in the new playlist.

-Description <String> (Required) New local playlist description.

-Name <String> (Required) New local playlist name.

-WaitTime <Int32> (Required) New local playlist wait time.

-ExportConnection <SwitchParameter> Export the playlist connections.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help New-RDMPlaylistLocal -detailed". For technical information, type "Get-Help New-RDMPlaylistLocal -full".

RELATED LINKS

10.35 New-RDMPlaylistShared

SYNOPSIS
Create a new shared playlist

SYNTAX

© 2019 Devolutions inc.
DESCRIPTION
Create a new shared playlist

PARAMETERS
-ConnectionPlayList <ConnectionPlayList>
  (Required) Connections in the new playlist.

-ExportConnections <SwitchParameter>
  Export the playlist connections.

-Name <String>
  (Required) New shared playlist name.

<CommonParameters>
  This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable,
  WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help
  about_commonparameters".

NOTES
For more information, type "Get-Help New-RDMPlaylistShared -detailed". For technical information, type
"Get-Help New-RDMPlaylistShared -full".

RELATED LINKS

10.36 New-RDMRole

SYNOPSIS
Create a new role instance.

SYNTAX
New-RDMRole -SetRole [SetRole] <SwitchParameter> -Description [Description] <String> -Name [Name]
  <String> [<CommonParameters>]

DESCRIPTION
Create a role instance. The instance has not yet been saved. Assign the result to a variable then call
"Set-RDMRole $s" to save the role.

PARAMETERS
-SetRole <SwitchParameter>
  Save the new role.

-Description <String>
  Role description.

-Name <String>
  (Required) New role name.

<CommonParameters>
  This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable,
  WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help
  about_commonparameters".

NOTES
For more information, type "Get-Help New-RDMRole -detailed". For technical information, type "Get-Help New-RDMRole -full".

**EXAMPLE 1**

PS C:\> $role = New-RDMRole -Name "New Role" ; Set-RDMRole $role

Create & save new role.

**RELATED LINKS**

Get-RDMRole
Remove-RDMRole
Set-RDMRole
Set-RDMRoleProperty

### 10.37 New-RDMSecurityGroup

**SYNOPSIS**
Create a new security group instance.

**SYNTAX**


**DESCRIPTION**
Create a security group instance. The instance has not yet been saved. Assign the result to a variable then call "Set-RDMSecurityGroup $s" to save the security group.

**PARAMETERS**

- **-SetSecurityGroup** <SwitchParameter>
  Save the new security group.

  - **-Description** <String>
    Security group description.

  - **-Name** <String>
    (Required) New security group name.

    <CommonParameters>
    This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

**NOTES**

**EXAMPLE 1**

PS C:\> $securityGroup = New-RDMSecurityGroup -Name "New SecurityGroup" ; Set-RDMSecurityGroup $securityGroup

Create & save new security group.

**RELATED LINKS**

Get-RDMSecurityGroup
10.38 New-RDMSession

SYNOPSIS
Create a new session instance.

SYNTAX

DESCRIPTION
Create a new session instance. The instance has not yet been saved. Assign the result to a variable then call "Set-RDMSession $s" to save the session.

PARAMETERS
-Group <String>
Session group.

-Host <String>
New Session host.

-Name <String>
(Required) New PSSession name.

-SetSession <SwitchParameter>
Save the session in the current data source

-TemplateID <Guid>
Create PSSession from template.

-Type <String>
(Required) New session kind. Must be one of the following:

"AzureQueueStorage", "AzureStorage", "BeyondTrustPasswordSafeConsole",
"Customer", "Dameware", "Database", "DataEntry", "DataReport", "DataSource", "DeskRoll",
"Deskton", "DevolutionsProxy", "Document", "DropBox", "Ftp", "Gateway", "Group", "Host", "HpRgs",
"Radmin", "RDCommander", "RDPConfigured", "RDPFilename", "RemoteAssistance", "ResetPassword",
"TeamViewerConsole", "Telnet", "TemplateGroup", "TerminalConsole", "VirtualBox", "VirtualPC",
"VMRC", "VMWare", "VMWareConsole", "VNC", "VPN", "Wayk", "WebBrowser", "WebDav",
"WindowsVirtualPC", "XenServer", "XWindow"

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help New-RDMSession -detailed". For technical information, type "Get-Help New-RDMSession -full".

EXAMPLE 1
PS C:\> $session = New-RDMSession -Name "New Session" -Host "myServer" -Type "RDPConfigured"; Set-RDMSession $session

Create & save new session.

RELATED LINKS
Get-RDMDataSource
Remove-RDMSession
Set-RDMDataSource
Set-RDMSession

10.39 New-RDMUser

SYNOPSIS
Create a new user instance.

SYNTAX

DESCRIPTION
Create a user instance. The instance has not yet been saved. Assign the result to a variable then call "Set-RDMUser $s" to save the user.

PARAMETERS
-Administrator <SwitchParameter>
  Gives the user administrator rights

-Login <String>
  Login.

-SetUser <SwitchParameter>
  Set the user in the data source

-AuthentificationType <String>
  Authentification type. Available in some data sources

-Disable <SwitchParameter>
  Disables the user. Available in some data sources

-Email <String>
  User email. Available when using a all data source except DODB
-IntegratedSecurity <SwitchParameter>
  Integrated security. Only available in SQL Server and DVLS data sources

-LoginEmail <String>
  Login email. Available in some data sources

-Password <SecureString>
  User password. Available when using a SQL Server data source and integrated security is not used

-SkipCreateSQLServerLogin <SwitchParameter>
  Skip to create the SQL Server login. Available in SQL Server data source

<CommonParameters>
  This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable,
  WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
  For more information, type "Get-Help New-RDMUser -detailed". For technical information, type "Get-Help New-RDMUser -full".

EXAMPLE 1
  PS C:\> $user = New-RDMUser -Name "New SecurityGroup" ;Set-RDMUser $user
  Create & save new user.

RELATED LINKS
  Get-RDMUser
  Remove-RDMUser
  Set-RDMUser
  Set-RDMUserProperty

10.40 Open-RDMQuickConnect

SYNOPSIS
  Open a session by specifying the host.

SYNTAX

DESCRIPTION
  Open an ad-hoc session by specifying the host.

PARAMETERS
  -Connection <PSCollection>
    Specifies a connection template

  -Domain <String>
    Specifies the domain of the host to open.

  -Host <String>
(Required) Specifies the host of the host to open.

-Password <SecureString>
  Specifies the password of the host to open

-TemplateID <Guid>
  Specifies a template ID

-Username <String>
  Specifies the username of the host to open.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Open-RDMQuickConnect -detailed". For technical information, type "Get-Help Open-RDMQuickConnect -full".

EXAMPLE 1
PS C:\> Open-RDMQuickConnect -Host "MyHost" -Connection connection"

Open the host MyHost.

RELATED LINKS
Get-RDMSession

10.41 Open-RDMSession

SYNOPSIS
Open the specified session.

SYNTAX

DESCRIPTION
Open the specified session.

PARAMETERS
-ID <Guid>
  (Required) Specifies the ID of the session to open.
  Must be a valid GUID, in the form {00000000-0000-0000-0000-000000000000}.

-Silent <SwitchParameter>
  Silent

-ForceExternal <SwitchParameter>
  Open the session external

<CommonParameters>
This cmdlet supports the common parameters:Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Open-RDMSession -detailed". For technical information, type "Get-Help Open-RDMSession -full".

EXAMPLE 1
PS C:\> Open-RDMSession -ID "{00000000-0000-0000-0000-000000000000}"

Open the session with ID = "{00000000-0000-0000-0000-000000000000}".

EXAMPLE 2
PS C:\> $list = Get-RDMSession; Open-RDMSession -ID $list[1].ID

Retrieves the list of available sessions and opens the second element in the list.

RELATED LINKS
Get-RDMSession

10.42 Read-RDMSession

SYNOPSIS
Read RDM session from a file

SYNTAX

DESCRIPTION
Read RDM session from a file

PARAMETERS
-DuplicateAction <String>
Action when a duplicate is found. Must be one of the following:

"Add", "Overwrite", "Ignore"

-Group <String>
The group where the sessions will be saved.

-Path <String>
(Required) Path where the file is loaded. Must be finish:

"RDM: .rdm", "XML: .xml"

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Read-RDMSession -detailed". For technical information, type "Get-Help Read-RDMSession -full".

EXAMPLE 1
PS C:\> $session = Read-RDMSession -Filename "C:\MyFile.rdm" -DuplicateAction "Add"; Set-RDMSession $session[0]

RELATED LINKS

10.43 Remove-RDMDataSource

SYNOPSIS
Remove data source.

SYNTAX
Remove-RDMDataSource -DataSource [DataSource] <PSDataSource> [<CommonParameters>]

DESCRIPTION
Remove data source.

PARAMETERS
-DataSource <PSDataSource>
  (Required) Specifies the data source to remove.

<CommonParameters>
  This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Remove-RDMDataSource -detailed". For technical information, type "Get-Help Remove-RDMDataSource -full".

RELATED LINKS

10.44 Remove-RDMRole

SYNOPSIS
Delete an existing role.

SYNTAX

DESCRIPTION
You will be prompted to confirm the delete.

PARAMETERS
-Force <SwitchParameter>
  Forces removal of the role without confirmation by the user. Optional.

-ID <Guid>
  (Required) Specifies the GUID of the role to be deleted from.
Must be a valid GUID, in the form {00000000-0000-0000-0000-000000000000}.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Remove-RDMRole -detailed". For technical information, type "Get-Help Remove-RDMRole -full".

EXAMPLE 1
PS C:\> $list = Get-RDMRole; Remove-RDMRole $list[1].ID
Retrieves the list of available sessions, deletes role at index 1.

EXAMPLE 2
PS C:\> Remove-RDMRole "{00000000-0000-0000-0000-000000000000}"
Delete session with ID = "{00000000-0000-0000-0000-000000000000}".

EXAMPLE 3
PS C:\> Remove-RDMRole -ID "{00000000-0000-0000-0000-000000000000}" -Force
Force delete of the role with ID = "{00000000-0000-0000-0000-000000000000}".

RELATED LINKS
Get-RDMRole
New-RDMRole
Set-RDMRole
Set-RDMRoleProperty

10.45 Remove-RDMRoleToUser

SYNOPSIS
Remove a role to an user.

SYNTAX
Remove-RDMRoleToUser -Role [Role] <PSRoleInfo> -User [User] <PSUserInfo>
[<CommonParameters>]

DESCRIPTION
Remove a role to an user.

PARAMETERS
-Role <PSRoleInfo>
  (Required) Role object, must be retrieved from Get-RDMRole or created via New-RDMRole.

-User <PSUserInfo>
  (Required) User object, must be retrieved from Get-RDMUser or created via New-RDMUser.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Remove-RDMRoleToUser -detailed". For technical information, type "Get-Help Remove-RDMRoleToUser -full".

EXAMPLE 1
PS C:\> Remove-RDMRoleToUser -Role $role -User $user

Remove role to an user.

RELATED LINKS
Add-RDMRoleToUser
Get-RDMRole
Get-RDMUser
New-RDMRole
New-RDMUser
Set-RDMUser

10.46 Remove-RDMSecurityGroup

SYNOPSIS
Delete an existing security group.

SYNTAX

DESCRIPTION
You will be prompted to confirm the delete.

PARAMETERS
-Force <SwitchParameter>
Forces removal of the security group without confirmation by the user. Optional.

-ID <Guid>
(Required) Specifies the GUID of the security group to be deleted from.

Must be a valid GUID, in the form {00000000-0000-0000-0000-000000000000}.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Remove-RDMSecurityGroup -detailed". For technical information, type "Get-Help Remove-RDMSecurityGroup -full".

EXAMPLE 1
PS C:\> $list = Get-RDMSecurityGroup; Remove-RDMSecurityGroup $list[1].ID

Retrieves the list of available security groups, deletes security group at index 1.
EXAMPLE 2
PS C:\> Remove-RDMSecurityGroup "{00000000-0000-0000-0000-000000000000}"
Delete security group with ID = "{00000000-0000-0000-0000-000000000000}".

EXAMPLE 3
PS C:\> Remove-RDMSecurityGroup -ID "{00000000-0000-0000-0000-000000000000}" -Force
Force delete of the security group with ID = "{00000000-0000-0000-0000-000000000000}".

RELATED LINKS
Get-RDMSecurityGroup
New-RDMSecurityGroup
Set-RDMSecurityGroup
Set-RDMSecurityGroupProperty

10.47 Remove-RDMSession

SYNOPSIS
Delete an existing session.

SYNTAX

DESCRIPTION
You will be prompted to confirm the delete.

PARAMETERS
-Force <SwitchParameter>
  Forces removal of the session without confirmation by the user. Optional.

-ID <Guid>
  (Required) Specifies the ID of the session to be deleted.

  Must be a valid GUID, in the form {00000000-0000-0000-0000-000000000000}.

-Refresh <SwitchParameter>
  Send refresh notification to Remote Desktop Manager application.

-Session <PSConnection[]>
  (Required) Specifies the sessions to remove

  <CommonParameters>
  This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Remove-RDMSession -detailed". For technical information, type "Get-Help Remove-RDMSession -full".

EXAMPLE 1
PS C:\> $list = Get-RDMSession; Remove-RDMSession $list[1].ID

Retrieves the list of available sessions, deletes session at index 1.

EXAMPLE 2
PS C:\> Remove-RDMSession "(00000000-0000-0000-0000-000000000000)"

Delete session with ID = "(00000000-0000-0000-0000-000000000000)".

EXAMPLE 3
PS C:\> Remove-RDMSession -ID "(00000000-0000-0000-0000-000000000000)" -Force

Force delete of the session with ID = "(00000000-0000-0000-0000-000000000000)".

EXAMPLE 4
PS C:\> $sessions = Get-RDMSession -Name 'My Session'; Remove-RDMSession -Session $session -Force

Force delete of the session MySession

RELATED LINKS
Get-RDMDDataSource
Get-RDMSession
Set-RDMDDataSource

10.48 Remove-RDMUser

SYNOPSIS
Delete an existing user.

SYNTAX

DESCRIPTION
You will be prompted to confirm the delete.

PARAMETERS
-DeleteSQLLogin <SwitchParameter>
Forces removal of the SQL Login without confirmation by the user. Optional.

-Force <SwitchParameter>
Forces removal of the user without confirmation by the user. Optional.

-ID <Guid>
(Required) Specifies the GUID of the user to be deleted from.

Must be a valid GUID, in the form {00000000-0000-0000-0000-000000000000}.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".
NOTES
For more information, type "Get-Help Remove-RDMUser -detailed". For technical information, type "Get-Help Remove-RDMUser -full".

EXAMPLE 1
PS C:\> $list = Get-User; Remove-RDMUser $list[1].ID
Retrieves the list of available users, deletes user at index 1.

EXAMPLE 2
PS C:\> Remove-RDMUser "{00000000-0000-0000-0000-000000000000}"
Delete security group with ID = "{00000000-0000-0000-0000-000000000000}".

EXAMPLE 3
PS C:\> Remove-RDMUser -ID "{00000000-0000-0000-0000-000000000000}" -Force
Force delete of the user with ID = "{00000000-0000-0000-0000-000000000000}".

RELATED LINKS
Get-RDMUser
New-RDMUser
New-RDMUser

10.49 Rename-RDMGroup

SYNOPSIS
Rename the group in a connection

SYNTAX

DESCRIPTION
Rename the group in a connection

PARAMETERS
-ID <Guid> (Required) Specifies the ID of the session to be deleted.
   Must be a valid GUID, in the form (00000000-0000-0000-0000-000000000000).

-NewGroupName <String> (Required) New group name.

-Session <PSConnection> (Required) Specifies the session object to modify

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Rename-RDMGroup -detailed". For technical information, type "Get-Help Rename-RDMGroup -full".

RELATED LINKS

10.50 Set-RDMCurrentDataSource

SYNOPSIS
Set current active data source.

SYNTAX

DESCRIPTION
Set current active data source.

PARAMETERS
-DataSource <PSDataSource>
  Specifies the datasource to set current

  -ID <Guid>
  (Required) Specifies the GUID of the data source to set as the current.

  The value must be a valid GUID, in the form {00000000-0000-0000-0000-000000000000}

  -Password <SecureString>
  Data source password

  -Username <String>
  Data source username

  <CommonParameters>
  This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Set-RDMCurrentDataSource -detailed". For technical information, type "Get-Help Set-RDMCurrentDataSource -full".

EXAMPLE 1
PS C:\> Set-RDMCurrentDataSource "{00000000-0000-0000-0000-000000000000}"
Set active data source to the data source with ID = "{00000000-0000-0000-0000-000000000000}".

EXAMPLE 2
PS C:\> $list = Get-RDMDataSource; Set-RDMCurrentDataSource $list[1].ID
Retrieves the list of available data sources and sets the current data source the second element in the list.

RELATED LINKS
Get-RDMDataSource
10.51 Set-RDMDataSource

SYNOPSIS
Save/set the datasource.

SYNTAX
Set-RDMDataSource -DataSource [DataSource] <PSDataSource> [CommonParameters>

DESCRIPTION
Save/set the datasource. Datasource must be first fetch via Data source property of the Get-RDMDataSource cmdlet or via the New-RDMDataSource result.

PARAMETERS
-DataSource <PSDataSource>(Required) Specifies the datasource to set/save.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Set-RDMDataSource -detailed". For technical information, type "Get-Help Set-RDMDataSource -full".

EXAMPLE 1
PS C:\> $list = Get-RDMDataSource; Set-RDMDataSourceProperty -DataSource $list[0] -Property "Name" -Value "MyNewDataSourceName"; Set-RDMDataSource $list[0]

Change the name of the first data source

RELATED LINKS
Get-RDMDataSource

10.52 Set-RDMDataSourceProperty

SYNOPSIS
Save/set the datasource.

SYNTAX
Set-RDMDataSourceProperty -DataSource [DataSource] <PSDataSource> -Property [Property] <String> -Value [Value] <Object> [CommonParameters>

DESCRIPTION
Save/set the datasource. Datasource must be first fetch via Data source property of the Get-RDMDataSource cmdlet or via the New-RDMDataSource result.

PARAMETERS
-DataSource <PSDataSource>
(Required) Specifies the datasource

-Property <String>
(Required) Property to set.
-Value <Object>
   (Required) New value.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Set-RDMDataSourceProperty -detailed". For technical information, type "Get-Help Set-RDMDataSourceProperty -full".

EXAMPLE 1
PS C:\> $list = Get-RDMDataSource; Set-RDMDataSourceProperty -DataSource $list[0] -Property "Name" -Value "MyNewDataSourceName"; Set-RDMDataSource $list[0]
Change the name of the first data source

RELATED LINKS
Get-RDMDataSource

10.53 Set-RDMPersonalCredentials

SYNOPSIS
Set RDM personal credentials. (Username/Password type only)

SYNTAX

DESCRIPTION
Set RDM personal credentials. (Username/Password type only)

PARAMETERS
-AlwaysAskPassword <Boolean>
Set Always ask password option in personal credentials

-Domain <String>
Set domain in personal credentials

-Password <SecureString>
Set password in personal credentials

-Username <String>
Set username in personal credentials

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Set-RDMPersonalCredentials -detailed". For technical information, type "Get-Help Set-RDMPersonalCredentials -full".

EXAMPLE 1
PS C:\> Set-RDMPersonalCredentials

Set RDM personal credentials. (Username/Password type only)

RELATED LINKS

10.54 Set-RDMPlaylistLocal

SYNOPSIS
Save a local playlist

SYNTAX
Set-RDMPlaylistLocal -ImportConnection [ImportConnection] <SwitchParameter> -Playlist [Playlist] <PSPlaylistLocal> [<CommonParameters>]

DESCRIPTION
Save a local playlist

PARAMETERS
-ImportConnection <SwitchParameter>
Import the playlist connections to the data source.

-Playlist <PSPlaylistLocal>
(Required) Specifies the local playlist to set/save.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Set-RDMPlaylistLocal -detailed". For technical information, type "Get-Help Set-RDMPlaylistLocal -full".

RELATED LINKS

10.55 Set-RDMPlaylistShared

SYNOPSIS
Save a shared playlist in the current data source

SYNTAX

DESCRIPTION
Save a shared playlist in the current data source

PARAMETERS
-ImportConnection <SwitchParameter>
Import the playlist connections to the data source.

-Playlist <PSPlaylistShared>
  (Required) Specifies the shared playlist to set/save.

-PrivateVault <SwitchParameter>
Save the shared playlist in the Private Vault.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Set-RDMPlaylistShared -detailed". For technical information, type "Get-Help Set-RDMPlaylistShared -full".

RELATED LINKS

10.56 Set-RDMPrivateSession

SYNOPSIS
Save the session in the user Private Vault

SYNTAX
Set-RDMPrivateSession -Refresh [Refresh] <SwitchParameter> -Session [Session] <PSConnection[]> [CommonParameters>

DESCRIPTION
Save the session in the user Private Vault

PARAMETERS
-Refresh <SwitchParameter>
  Send refresh notification to Remote Desktop Manager application.

-Session <PSConnection[]>
  (Required) PSSession object, must be retrieved from Get-RDMSession or Get-RDMPrivateSession or created via New-RDMSession.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Set-RDMPrivateSession -detailed". For technical information, type "Get-Help Set-RDMPrivateSession -full".

RELATED LINKS

10.57 Set-RDMRole

SYNOPSIS
Save/set the role.
SYNTAX
Set-RDMRole -Role [Role] <PSRoleInfo> [CommonParameters>

DESCRIPTION
Save/set the role. Role must be first fetch via role property of the Get-RDMRole cmdlet or via the New-RDMRole result.

PARAMETERS
-Role <PSRoleInfo>
  (Required) Role object, must be retrieved from Get-RDMRoleSecurityGroup or created via New-RDMRole.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Set-RDMRole -detailed". For technical information, type "Get-Help Set-RDMRole -full".

EXAMPLE 1
PS C:\> $role = New-RDMRole -Name "New Role" ; Set-RDMRole $role
Create & save new role.

RELATED LINKS
Get-RDMRole
New-RDMRole
Remove-RDMRole
Set-RDMRoleProperty

10.58 Set-RDMRoleGroupRights

SYNOPSIS
Assign/set role permissions.

SYNTAX
[View] <Nullable’1> [CommonParameters>

DESCRIPTION
Assign/set role permissions.

PARAMETERS
-Add <Boolean>
  Allows the role to add entries in groups/folders for that security group.

-Delete <Boolean>
  Allows the role to Delete the entries for that security group.

-Edit <Boolean>
Allows the role to Edit the entries for that security group.

-Role <PSRoleInfo>
  (Required) role object, must be retrieved from Get-RDMRole or created via New-RDMRole.

-SecurityGroup <PSSecurityGroupInfo>
  (Required) Security group object, must be retrieved from Get-RDMSecurityGroup or created via New-RDMSecurityGroup.

-View <Boolean>
  Allows the role to View AND USE the entries for that security group.

<CommonParameters>
  This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
  For more information, type "Get-Help Set-RDMRoleGroupRights -detailed". For technical information, type "Get-Help Set-RDMRoleGroupRights -full".

EXAMPLE 1
  PS C:\> $roles = Get-RDMRole; $groups = Get-RDMSecurityGroup; Set-RDMRoleGroupRights -role $roles[1] -SecurityGroup $groups[0] -Add $true -Delete $true

  Retrieves the list of available roles and groups. Set permission add and delete to the second role of the list on the first group of the list

RELATED LINKS
  Get-RDMRole
  New-RDMRole
  New-RDMSecurityGroup
  Remove-RDMRole

10.59 Set-RDMRoleProperty

SYNOPSIS
  Set the value of property given to a role.

SYNTAX
  Set-RDMRoleProperty -Property [Property] <String> -Role [Role] <PSRoleInfo> -Value [Value] <Object> 
  [<CommonParameters>]

DESCRIPTION
  Set the value of property given to a role.

PARAMETERS
  -Property <String>
    (Required) Property to set.

  -Role <PSRoleInfo>
    (Required) Specifies the ID of the session to get the password from.

    Must be a valid GUID, in the form {00000000-0000-0000-0000-000000000000}. 
-Value <Object>
(Required) New value.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Set-RDMRoleProperty -detailed". For technical information, type "Get-Help Set-RDMRoleProperty -full".

EXAMPLE 1
PS C:\> Set-RDMRoleProperty -Role "$role" -Property "Description" -Value "My New Description"
Set the description value for the role given.

EXAMPLE 2
PS C:\> $list = Get-RDMRole; Set-RDMRoleProperty -Role $list[1] -Property "Description" -Value "My description"
Retrieves the list of available role and then sets the description value of the second element in the list.

RELATED LINKS
Get-RDMRole
New-RDMRole
New-RDMRole
Remove-RDMRole

10.60 Set-RDMSecurityGroup

SYNOPSIS
Save/set the security group.

SYNTAX

DESCRIPTION

PARAMETERS
-SecurityGroup <PSSecurityGroupInfo>
(Required) Security group object, must be retrieved from Get-RDMSecurityGroup or created via New-RDMSecurityGroup.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Set-RDMSecurityGroup -detailed". For technical information, type "Get-Help Set-RDMSecurityGroup -full".

**EXAMPLE 1**

```powershell
PS C:\> $securityGroup = New-RDMSecurityGroup -Name "New SecurityGroup" ; Set-RDMSecurityGroup $securityGroup
```

Create & save new security group.

**RELATED LINKS**
- Get-RDMSecurityGroup
- New-RDMSecurityGroup
- Remove-RDMSecurityGroup
- Set-RDMSecurityGroupProperty

### 10.61 Set-RDMSecurityGroupProperty

**SYNOPSIS**
Set the value of property given to a security group.

**SYNTAX**

```powershell
```

**DESCRIPTION**
Protected values will always return null.

**PARAMETERS**

- **-SecurityGroup [PSSecurityGroupInfo]**
  (Required) Specifies the security group.

  - **-Property [String]**
    (Required) Property to set.

  - **-Value [Object]**
    (Required) New value.

- `<CommonParameters>`
  This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

**NOTES**
For more information, type "Get-Help Set-RDMSecurityGroupProperty -detailed". For technical information, type "Get-Help Set-RDMSecurityGroupProperty -full".

**EXAMPLE 1**

```powershell
PS C:\> Set-RDMSecurityGroupProperty -SecurityGroup "$securityGroup" -Property "Description" -Value "My New Description"
```

Set the description value for the security group given.

**EXAMPLE 2**
PS C:\> $list = Get-RDMSecurityGroup; Set-RDMSecurityGroupProperty -Group $list[1] -Property "Description" -Value "My description"

Retrieves the list of available security groups and then sets the description value of the second element in the list.

RELATED LINKS
Get-RDMSecurityGroup
New-RDMSecurityGroup
Remove-RDMSecurityGroup
Set-RDMSecurityGroup

10.62 Set-RDMSession

SYNOPSIS
Save/set the session.

SYNTAX
Set-RDMSession -Refresh [Refresh] <SwitchParameter> -Session [Session] <PSConnection[]>
[<CommonParameters>]

DESCRIPTION
Save/set the session. Session must be first fetch via Session property of the Get-RDM-Session cmdlet or via the New-RDMSession result.

PARAMETERS
-Refresh <SwitchParameter>
Send refresh notification to Remote Desktop Manager application.

-Session <PSConnection[]>
(Required) PSSession object, must be retrieved from Get-RDMSession or created via New-RDMSession.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable,OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Set-RDMSession -detailed". For technical information, type "Get-Help Set-RDMSession -full".

EXAMPLE 1
PS C:\> $list = Get-RDMSession; $list[1].Name = "New Name";Set-RDMSession $list[1]

Retrieves the list of available sessions, modify the name of the second session, update the session.

EXAMPLE 2
PS C:\> $session = New-RDMSession -Name "New Session" -Host "myServer" -Kind "RDPConfigured"; Set-RDMSession $session

Create & save new session.

RELATED LINKS
Get-RDMDDataSource
10.63 **Set-RDMSessionStatus**

**SYNOPSIS**
Set a status to a given session.

**SYNTAX**

**DESCRIPTION**
Set a status to a given session.

**PARAMETERS**
-ID <Guid>
(Required) Specifies the ID of the session to set the status to.

Must be a valid GUID, in the form {00000000-0000-0000-0000-000000000000}.

-Message <String>
Status message

-Session <PSConnection[]>
(Required) Specifies the session to set the status to

-Status <String>
(Required) Status type

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

**NOTES**
For more information, type "Get-Help Set-RDMSessionStatus -detailed". For technical information, type "Get-Help Set-RDMSessionStatus -full".

**EXAMPLE 1**
PS C:\> $list = Get-RDMSession; Set-RDMSessionStatus -Session $list[1] -Status Locked -Message 'Locked Message'

Set the status locked to the second element in the list.

**RELATED LINKS**
Get-RDMSession
Get-RDMSessionPassword
Get-RDMSessionStatus
Get-RDMSessionUserName
Set-RDMSessionDomain
Set-RDMSessionPassword
Set-RDMSessionUsername

10.64  Set-RDMSessionCredentials

SYNOPSIS
Save credentials in a session

SYNTAX
Set-RDMSessionCredentials -CredentialEntryID [CredentialEntryID] <String> -CredentialsType [CredentialsType] <String> -PSConnection [PSConnection] <PSConnection> -SetSession [SetSession] <SwitchParameter> [<CommonParameters>]

DESCRIPTION
Save credentials in a session

PARAMETERS
-CredentialEntryID <String>(Required) Specifies the credentials type.
-CredentialsType <String>(Required) Specifies the credentials type.
-PSConnection <PSConnection>(Required) Specifies the connection to set credentials to.
-SetSession <SwitchParameter> Specifies the credentials type.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Set-RDMSessionCredentials -detailed". For technical information, type "Get-Help Set-RDMSessionCredentials -full".

RELATED LINKS

10.65  Set-RDMSessionDocument

SYNOPSIS
Save a document in the current data source

SYNTAX

DESCRIPTION
Save a document in the current data source

PARAMETERS
-Document <PSConnectionDocument> (Required) Specifies the document to set/save.
Set the domain from the specified session.

SYNOPSIS
Set the domain from the specified session.

SYNTAX

DESCRIPTION
Set the domain from the specified session.

PARAMETERS
- Domain <String>
(Required) New domain name.

- ID <Guid>
(Required) Specifies the ID of the session to get the domain from.

Must be a valid GUID, in the form {00000000-0000-0000-0000-000000000000}.

- Refresh <SwitchParameter>
Send refresh notification to Remote Desktop Manager application.

- Session <PSConnection>
(Required) Specifies the session to set the Domain to.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Set-RDMSessionDomain -detailed". For technical information, type "Get-Help Set-RDMSessionDomain -full".

EXAMPLE 1
PS C:\> Set-RDMSessionDomain "{00000000-0000-0000-0000-000000000000}" "MyOtherDomain.com"
Set the domain from the session with ID = "{00000000-0000-0000-0000-000000000000}".

EXAMPLE 2
Set-RDMSessionPassword

SYNOPSIS
Set the password from the specified session.

SYNTAX

DESCRIPTION
Set the password from the specified session. Session must be marked as "Allow show credentials" if not null is returned.

PARAMETERS
-ID <Guid>(Required)
(Required) Specifies the ID of the session to get the password from.

-Must be a valid GUID, in the form {00000000-0000-0000-0000-000000000000}.

-Password <SecureString>
(Required) Password as SecureString.

-Refresh <SwitchParameter>
Send refresh notification to Remote Desktop Manager application.

-Session <PSConnection>
(Required) Specifies the session to set the password to.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Set-RDMSessionPassword -detailed". For technical information, type "Get-Help Set-RDMSessionPassword -full".

EXAMPLE 1
Set-RDMSessionPassword -ID "{00000000-0000-0000-0000-000000000000}" -Password (Read-Host -AsSecureString "Password")

Set the password from the session with ID = "{00000000-0000-0000-0000-000000000000}".

EXAMPLE 2
PS C:\> $list = Get-RDMSession; Set-RDMSessionPassword -ID $list[1].ID -Password (Read-Host -AsSecureString "Password")

Retrieves the list of available sessions and sets the password from the second element in the list.

RELATED LINKS
Get-RDMSession
Get-RDMSessionDomain
Get-RDMSessionPassword
Get-RDMSessionUserName
Set-RDMSessionDomain
Set-RDMSessionUsername

10.68 Set-RDMSessionProperty

SYNOPSIS
Set the value of property given a session ID and path.

SYNTAX

DESCRIPTION
Protected values will always return null.

PARAMETERS
-ID <Guid>(Required) Specifies the ID of the session to get the password from.

Must be a valid GUID, in the form {00000000-0000-0000-0000-000000000000}.

-Refresh <SwitchParameter>
Send refresh notification to Remote Desktop Manager application.

-Path <String>
The path to the property being read (reference RDM export xml). In the case of top level property do not specify parameter or pass empty string ["] or $null.

-Property <String>(Required) Property to set.

-Value <Object>(Required) New value.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".
NOTES
For more information, type "Get-Help Set-RDMSessionProperty -detailed". For technical information, type "Get-Help Set-RDMSessionProperty -full".

EXAMPLE 1
PS C:\> Set-RDMSessionProperty -ID "{00000000-0000-0000-0000-000000000000}" -Property "Group" -Value "My New Group Name"

Set the Group value from the session with ID = "{00000000-0000-0000-0000-000000000000}".

EXAMPLE 2
PS C:\> Set-RDMSessionProperty "{00000000-0000-0000-0000-000000000000}" "MetaInformation" "OS" "Windows Server 2008 R2"

Set the MetaInformation.OS value from the session with ID = "{00000000-0000-0000-0000-000000000000}".

EXAMPLE 3
PS C:\> $list = Get-RDMSession; Set-RDMSessionProperty -ID $list[1].ID -Path "MetaInformation" -Property "OS" -Value "Windows Server 2008 R2"

Retrieves the list of available sessions and then sets the MetaInformation.OS value of the second element in the list.

RELATED LINKS
Get-RDMSession
Get-RDMSessionProperty

10.69 Set-RDMSessionUsername

SYNOPSIS
Set the username on the specified session.

SYNTAX

DESCRIPTION
Set the username on the specified session.

PARAMETERS
-ID <Guid>
(Required) Specifies the ID of the session to set the password from.

Must be a valid GUID, in the form {00000000-0000-0000-0000-000000000000}.

-Refresh <SwitchParameter>
Send refresh notification to Remote Desktop Manager application.

-Session <PSConnection>
(Required) Specifies the session to set the username to

-UserName <String>
<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Set-RDMSessionUsername -detailed". For technical information, type "Get-Help Set-RDMSessionUsername -full".

EXAMPLE 1
PS C:\> Set-RDMSessionUsername "{00000000-0000-0000-0000-000000000000}" "localadmin"
Set the username from the session with ID = "{00000000-0000-0000-0000-000000000000}".

EXAMPLE 2
PS C:\> $list = Get-RDMSession; Get-RDMSessionPassword -ID $list[1].ID -Username
Retrieves the list of available sessions and gets the password from the second element in the list.

RELATED LINKS
Get-RDMSession
Get-RDMSessionDomain
Get-RDMSessionPassword
Get-RDMSessionUserName
Set-RDMSessionDomain
Set-RDMSessionPassword

10.70 Set-RDMTemplate

SYNOPSIS
Save templates in the current data sources

SYNTAX
Set-RDMTemplate -Template [Template] <PSTemplate[]> [CommonParameters]>

DESCRIPTION
Save templates in the current data sources

PARAMETERS
-Template <PSTemplate[]>
(Required) Template must be retrieved from Get-RDMTemplate

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Set-RDMTemplate -detailed". For technical information, type "Get-Help Set-RDMTemplate -full".

RELATED LINKS
10.71 Set-RDMUser

SYNOPSIS

SYNTAX

Set-RDMUser -User [User] <PSUserInfo> [<CommonParameters>]

DESCRIPTION

PARAMETERS
-User <PSUserInfo>
  (Required) User object, must be retrieved from Get-RDMUser or created via New-RDMUser.

<CommonParameters>
  This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable,
  WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help
  about_commonparameters".

NOTES
  For more information, type "Get-Help Set-RDMUser -detailed". For technical information, type "Get-Help
  Set-RDMUser -full".

RELATED LINKS

10.72 Set-RDMUserGroupRights

SYNOPSIS

Assign/set user permissions.

SYNTAX

  <SwitchParameter> -User [User] <PSUserInfo> -View [View] <Nullable`1> [<CommonParameters>]

DESCRIPTION

Assign/set user permissions.

PARAMETERS
-Add <Boolean>
  Allows the user to add entries in groups/folders for that security group.

-Delete <Boolean>
  Allows the user to Delete the entries for that security group.

-Edit <Boolean>
  Allows the user to Edit the entries for that security group.

-SecurityGroup <PSSecurityGroupInfo>
  (Required) Security group object, must be retrieved from Get-RDMSecurityGroup or created via New-
  RDMSecurityGroup.

-SetUser <SwitchParameter>
Set the user in the data source

-User <PSUserInfo> (Required) User object, must be retrieved from Get-RDMUser or created via New-RDMUser.

-View <Boolean>
   Allows the user to View AND USE the entries for that security group.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Set-RDMUserGroupRights -detailed". For technical information, type "Get-Help Set-RDMUserGroupRights -full".

EXAMPLE 1

Retrieves the list of available users and groups. Set permission add and delete to the second user of the list on the first group of the list.

RELATED LINKS
Get-RDMUser
New-RDMUser
Remove-RDMUser

10.73 Set-RDMUserProperty

SYNOPSIS
Set the value of property given to a user.

SYNTAX

DESCRIPTION
Set the value of property given to a user.

PARAMETERS
-Property <String>
(Required) Property to set.

-User <PSUserInfo>
(Required) Specifies the GUID of the user to get the password from.

Must be a valid GUID, in the form {00000000-0000-0000-0000-000000000000}.

-Value <Object>
(Required) New value.
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Set-RDMUserProperty -detailed". For technical information, type "Get-Help Set-RDMUserProperty -full".

EXAMPLE 1
PS C:\> Set-RDMUserProperty -User "$user" -Property "Description" -Value "My New Description"
Set the description value for the user given.

EXAMPLE 2
PS C:\> $list = Get-RDMUser; Set-RDMUserProperty -User $list[1] -Property "Description" -Value "My description"
Retrieves the list of available users and then sets the description value of the second element in the list.

RELATED LINKS
Get-RDMUser
New-RDMUser
Remove-RDMUser

10.74 Set-RDMUserSecurity

SYNOPSIS
Assign/set user security settings.

SYNTAX

DESCRIPTION
Assign/set user security settings.

PARAMETERS
-AllowDragAndDrop <Boolean>
Allows the user to move the sessions using drag-and-drop from other applications.

-AllowRevealPassword <Boolean>
Allows the user to use the Reveal Password command.

-CanExport <Boolean>
Allows the user to Export sessions.

-CanImport <Boolean>
Allows the user to Import sessions.
-CanViewDetails <Boolean>
  Allows the user to see the content of the Details tab for all sessions.

-CanViewGlobalLogs <Boolean>
  Allows the user to see the content of the Logs that apply to a session.

-CanViewInformations <Boolean>
  Allows the user to see the content of the Information tab for all sessions.

-DenyAddInRoot <Boolean>
  Denies the user the rights to add in the root.

-OfflineMode <String>
  Allows the user to enable the Offline Mode on the data sources. Choose between:
  
  Disabled : no offline cache allowed for that user
  
  ReadOnly : a read-only cache is allowed for Advanced Data Sources.
  
  ReadWrite : an advanced cache, with change synchronization, is allowed for Advanced Data Sources.

-SetUser <SwitchParameter>
  Set user

-User <PSUserInfo>
  (Required) User object, must be retrieved from Get-RDMUser or created via New-RDMUser.

<CommonParameters>
  This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
  For more information, type "Get-Help Set-RDMUserSecurity -detailed". For technical information, type "Get-Help Set-RDMUserSecurity -full".

EXAMPLE 1
PS C:\> Set-RDMUserSecurity -user $user -CanImport $true -CanExport $true -AllowRevealPassword $false -OfflineMode "Read/Write"

Set user to allow it to import, export, not allow to reveal password and set offline mode to read/write and

RELATED LINKS
Get-RDMUser
New-RDMUser
Remove-RDMUser

10.75 Set-RDMUserSpecificSettings

SYNOPSIS
Save user Specific Settings in a session
### Set-RDMUserSpecificSettings

**SYNTAX**

Set-RDMUserSpecificSettings -UserSpecificSettings [UserSpecificSettings] <BaseConnectionOverride> -
Connection [Connection] <PSConnection> [<CommonParameters>]

**DESCRIPTION**

Save user Specific Settings in a session

**PARAMETERS**

- **-UserSpecificSettings** <BaseConnectionOverride>
  (Required) User Specific Settings, must be retrieved from Get-RDMUserSpecificSettings.

- **-Connection** <PSConnection>
  (Required) Connection.

  <CommonParameters>
  This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction,
  WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

**NOTES**

For more information, type "Get-Help Set-RDMUserSpecificSettings -detailed". For technical information, type
"Get-Help Set-RDMUserSpecificSettings -full".

### RELATED LINKS

10.76 **Start-RDMInstance**

**SYNOPSIS**

Start a Remote Desktop Manager PowerShell instance

**SYNTAX**

Start-RDMInstance [<CommonParameters>]

**DESCRIPTION**

Start a Remote Desktop Manager PowerShell instance

**PARAMETERS**

  <CommonParameters>
  This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction,
  WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

**NOTES**

For more information, type "Get-Help Start-RDMInstance -detailed". For technical information, type "Get-
Help Start-RDMInstance -full".

### RELATED LINKS

10.77 **Update-RDMUI**

**SYNOPSIS**

Update RDM user interface.

**SYNTAX**
Update-RDMUI [<CommonParameters>]

DESCRIPTION
Update RDM user interface.

PARAMETERS
<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Update-RDMUI -detailed". For technical information, type "Get-Help Update-RDMUI -full".

EXAMPLE 1
PS C:\> Update-RDMUI

Update RDM user interface.

RELATED LINKS
10.78 New-RDMRandomPassword

SYNOPSIS
Create a new random password

SYNTAX
New-RDMRandomPassword -Session [Session] <PSConnection> -TemplateName [TemplateName] <String> [<CommonParameters>]

DESCRIPTION
Create a new random password

PARAMETERS
-Session <PSConnection>
Generate a random password with the password complexity of that session

-TemplateName <String>
Generate a random password with the template settings.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help New-RDMRandomPassword -detailed". For technical information, type "Get-Help New-RDMRandomPassword -full".

EXAMPLE 1
PS C:\> $randomPassword = New-RDMRandomPassword

Generate a random password with the default settings
EXAMPLE 2
PS C:\> $randomPassword = New-RDMRandomPassword -TemplateName $templateName

Generate a random password with the template settings

EXAMPLE 3
PS C:\> $session = Get-RDMSession -Name MySession; $randomPassword = New-RDMRandomPassword -Session $session

Generate a random password with the password complexity of the session

RELATED LINKS

10.79 Open-RDMSyncSession

SYNOPSIS
Open the specified sync session.

SYNTAX

DESCRIPTION
Open the specified sync session.

PARAMETERS
- -DontSetSessions <SwitchParameter>
Don't save the sessions into the data source

-ID <Guid>
(Required) Specifies the ID of the session to open.

Must be a valid GUID, in the form {00000000-0000-0000-0000-000000000000}.

-Session <PSConnection>
(Required) Specifies the PSCConnection to open

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Open-RDMSyncSession -detailed". For technical information, type "Get-Help Open-RDMSyncSession -full".

EXAMPLE 1
PS C:\> $result = Open-RDMSyncSession -ID "{00000000-0000-0000-0000-000000000000}" Open the sync session with ID = "{00000000-0000-0000-0000-000000000000}".

RELATED LINKS
Open-RDMSession
10.80 Set-RDMDatasourceMasterKey

SYNOPSIS
Modify or clear your data source master key

SYNTAX
Set-RDMDatasourceMasterKey -DataSource [DataSource] <PSDataSource> -NewMasterKey [NewMasterKey] <SecureString> -NoMasterKey [NoMasterKey] <SwitchParameter> [<CommonParameters>]

DESCRIPTION

PARAMETERS
-DataSource <PSDataSource> (Required) Specifies the data source to change the master key

-NewMasterKey <SecureString> (Required) New data source master key.

-NoMasterKey <SwitchParameter> (Required) Set no master key.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Set-RDMDatasourceMasterKey -detailed". For technical information, type "Get-Help Set-RDMDatasourceMasterKey -full".

EXAMPLE 1
PS C:\> $dataSource = Get-RDMDatasource -Name MyDataSource; Set-RDMDatasourceMasterKey -DataSource $dataSource -NewMaster (ConvertTo-SecureString -AsPlainText "MyMasterKey" -Force)
Modify the master key of the data source named MyDataSource to MyMasterKey

RELATED LINKS

10.81 Set-RDMSQLiteDatasourcePassword

SYNOPSIS
Modify or clear your data source password

SYNTAX

DESCRIPTION

PARAMETERS
- **DataSource** `<PSDataSource>`
  (Required) Specifies the SQLite data source

- **NewPassword** `<SecureString>`
  (Required) New data source password.

- **NoPassword** `<SwitchParameter>`
  (Required) Set no password.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Set-RDMSQLiteDatasourcePassword -detailed". For technical information, type "Get-Help Set-RDMSQLiteDatasourcePassword -full".

EXAMPLE 1
PS C:\> $dataSource = Get-RDMDataSource -Name MySqliteDataSource; Set-RDMSQLiteDatasourcePassword -DataSource $dataSource -NewPassword (ConvertTo-SecureString -AsPlainText "MyPassword" -Force)

Modify the password of the data source named MySqliteDataSource to MyPassword

RELATED LINKS
10.82 **Invoke-RDMLoadFromInventorySession**

SYNOPSIS
Invoke a Load from inventory action.

SYNTAX
Invoke-RDMLoadFromInventorySession -Credential [Credential] <PSCredential> -Session [Session] <PSConnection[]> [<CommonParameters>]

DESCRIPTION

PARAMETERS
- **Credential** <PSCredential>
  PSCredential object.

- **Session** <PSConnection[]>
  (Required) PSConnection object, must be retrieved from Get-RDMSession or created via New-RDMSession.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Invoke-RDMLoadFromInventorySession -detailed". For technical information, type "Get-Help Invoke-RDMLoadFromInventorySession -full".

EXAMPLE 1
PS C:\> $list = Get-RDMSession; Invoke-RDMLoadFromInventorySession -Session $list[0]; Set-RDMSession -Session $list[0] -Refresh

Invoke a Load from inventory on the first session in the list.

RELATED LINKS
Invoke-RDMUnparentSession

10.83 Add-RDMSessionAttachment

SYNOPSIS
Add a new attachment to a session

SYNTAX

DESCRIPTION
Add a new attachment to a session

PARAMETERS
-Description <String>
Attachment description.

-Filename <String>
(Required) Attachment filename.

-Password <SecureString>
Attachment password.

-Refresh <SwitchParameter>
Send refresh notification to Remote Desktop Manager application.

-SecurityGroup <PSSecurityGroupInfo>
Attachment security group.

-Session <PSConnection>
(Required) Session to add the attachment to.

-Title <String>
Attachment title.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Add-RDMSessionAttachment -detailed". For technical information, type "Get-Help Add-RDMSessionAttachment -full".

RELATED LINKS

10.84 Get-RDMRepository

SYNOPSIS
Retrieve the list of available repositories.

SYNTAX
Get-RDMRepository -Name [Name] <String> [<CommonParameters>]

DESCRIPTION
Retrieve the list of available repositories for the current selected data source.

PARAMETERS
-Name <String>
    Repository name

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Get-RDMRepository -detailed". For technical information, type "Get-Help Get-RDMRepository -full".

EXAMPLE 1
PS C:\> Get-RDMRepository

Retrieves the list of available repository.

EXAMPLE 2
PS C:\> $list = Get-RDMRepository; $list[0]

Retrieves the list of available repositories and displays the first item.

EXAMPLE 3
PS C:\> $list = Get-RDMRepository; $list[1].Name = "New Name"; Set-RDMRepository $list[1]

Retrieves the list of available repositories, modify the name of the second role, update the repository.

RELATED LINKS

10.85 Get-RDMSessionAttachment

SYNOPSIS
Get session attachments

SYNTAX
Get-RDMSessionAttachment -Session [Session] <PSConnection> [<CommonParameters>]
DESCRIPTION
Get session attachments

PARAMETERS
-Session <PSConnection>
  (Required) Specifies the connection to get the attachments from.

<CommonParameters>
  This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable,
  WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help
  about_commonparameters".

NOTES
For more information, type "Get-Help Get-RDMSessionAttachment -detailed". For technical
information, type "Get-Help Get-RDMSessionAttachment -full".

RELATED LINKS

10.86 Invoke-RDMCreateDataSourceDatabase

SYNOPSIS
Create a new Database

SYNTAX
-DataSource [DataSource] <PSDataSource> [<CommonParameters>]

DESCRIPTION

PARAMETERS
  Azure database edition.

-AzureDatabaseMaxSize <AzureDatabaseMaxSize>
  Azure database maximum size.

-AzureDatabaseServiceObjective <AzureDatabaseServiceObjective>
  Azure database service objective.

-DataSource <PSDataSource>
  (Required) PSSession object, must be retrieved from Get-RDMSession or created via New-RDMSession
  that you want to unparented.

<CommonParameters>
  This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable,
  WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help
  about_commonparameters".

NOTES
For more information, type "Get-Help Invoke-RDMCreateDataSourceDatabase -detailed". For technical
information, type "Get-Help Invoke-RDMCreateDataSourceDatabase -full".
EXAMPLE 1
PS C:\> $ds = New-RDMDataSource -SQLServer -Database 'PSTestCreation5' -Name 'PSSQLServerCreation' -Server 'localhost' -Username 'sa' -Password (ConvertTo-SecureString 'masterkey' –asplaintext –force); Invoke-RDMCreateDataSourceDatabase -DataSource $ds

Create a SQL Server data source and create the database

RELATED LINKS

10.87 Invoke-RDMUpdateDataSourceDatabase

SYNOPSIS
Upgrade a Database

SYNTAX
Invoke-RDMUpdateDataSourceDatabase -DataSource [DataSource] <PSDataSource> [<CommonParameters>]

DESCRIPTION

PARAMETERS
-DataSource <PSDataSource> (Required) PSDataSource object, must be retrieved from Get-RDMDataSource.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Invoke-RDMUpdateDataSourceDatabase -detailed". For technical information, type "Get-Help Invoke-RDMUpdateDataSourceDatabase -full".

EXAMPLE 1
PS C:\> $ds = Get-RDMDataSource -Name SQLServerDataSourceName; Invoke-RDMUpdateDataSourceDatabase -DataSource $ds

Get a SQL Server data source and upgrade the database

RELATED LINKS

10.88 New-RDMRepository

SYNOPSIS
Create a new repository instance.

SYNTAX
New-RDMRepository -Description [Description] <String> -Name [Name] <String> -SetRepository [SetRepository] <SwitchParameter> [<CommonParameters>]

DESCRIPTION
Create a repository instance. The instance has not yet been saved. Assign the result to a variable then call "Set-RDMRepository $s" to save the repository.

PARAMETERS
-Description <String>
  Role description.

-Name <String>
  (Required) New repository name.

-SetRepository <SwitchParameter>
  Save the new repository.

<CommonParameters>
  This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
  For more information, type "Get-Help New-RDMRepository -detailed". For technical information, type "Get-Help New-RDMRepository -full".

EXAMPLE 1
  PS C:\> $role = New-RDMRepository -Name "New Repository" ; Set-RDMRepository $role

  Create & save new repository.

RELATED LINKS

10.89 Remove-RDMRepository

SYNOPSIS
Delete an existing repository.

SYNTAX

DESCRIPTION
You will be prompted to confirm the delete.

PARAMETERS
-Force <SwitchParameter>
  Forces removal of the repository without confirmation by the user. Optional.

-ID <Guid>
  (Required) Specifies the GUID of the repository to be deleted from.

  Must be a valid GUID, in the form (00000000-0000-0000-0000-000000000000).

-RepositoryDestination <PSRepositoryInfo>
  Specifies the new repository to move the sessions from the deleted repository to.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Remove-RDMRepository -detailed". For technical information, type "Get-Help Remove-RDMRepository -full".

EXAMPLE 1
PS C:\> $list = Get-RDMRepository; Remove-RDMRepository $list[1].ID
Retrieves the list of available repositories, deletes repository at index 1.

EXAMPLE 2
PS C:\> Remove-RDMRepository '{00000000-0000-0000-0000-000000000000}'
Delete repository with ID = '{00000000-0000-0000-0000-000000000000}'.

EXAMPLE 3
PS C:\> Remove-RDMRepository-ID '{00000000-0000-0000-0000-000000000000}' -Force
Force delete of the repository with ID = '{00000000-0000-0000-0000-000000000000}'.

RELATED LINKS
Get-RDMRepository
New-RDMRepository
Set-RDMRepository

10.90 Remove-RDMSessionAttachment

SYNOPSIS
Remove session attachment.

SYNTAX
Remove-RDMSessionAttachment -Attachment [Attachment] <PSConnectionAttachment> -Force [Force]
<SwitchParameter> [<CommonParameters>]

DESCRIPTION
Remove session attachment.

PARAMETERS
-Attachment <PSConnectionAttachment>
  (Required) Connection.

-Force <SwitchParameter>
  Forces removal of the attachment without confirmation by the user. Optional.

<CommonParameters>
  This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Remove-RDMSessionAttachment -detailed". For technical information, type "Get-Help Remove-RDMSessionAttachment -full".

EXAMPLE 1
PS C:\> $session = Get-RDMSession -Name MySession; $attachments = Get-RDMSessionAttachment -Session $session; Update-RDMSessionAttachment -Attachment $attachments[0]

Remove the first attachment in the session.

RELATED LINKS
10.91 Set-RDMDatasourceRepository

SYNOPSIS
Modify data source repository

SYNTAX
Set-RDMDatasourceRepository -DataSource [DataSource] <PSDataSource> -Repository [Repository] <PSRepositoryInfo> [CommonParameters>

DESCRIPTION

PARAMETERS
-DataSource <PSDataSource> (Required) Specifies the data source to change the current repository

-Repository <PSRepositoryInfo> (Required) New data source current repository.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Set-RDMDatasourceRepository -detailed". For technical information, type "Get-Help Set-RDMDatasourceRepository -full".

EXAMPLE 1
PS C:\> $dataSource = Get-RDMDataSource -Name MyDataSource; $repository = Get-RDMRepository -Name MyRepository ;Set-RDMDatasourceRepository -DataSource $dataSource -Repository $repository

Modify the data source repository to

RELATED LINKS
10.92 Set-RDMRepository

SYNOPSIS
Save/set the repository.

SYNTAX
Set-RDMRepository -Repository [Repository] <PSRepositoryInfo> [CommonParameters>]


DESCRIPTION
Save/set the repository. Repository must be first fetch via repository property of the Get-RDMRepository cmdlet or via the New-RDMRepository result.

PARAMETERS
-Repository <PSRepositoryInfo>
  (Required) repository object, must be retrieved from Get-RDMRepository or created via New-RDMRepository.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Set-RDMRepository -detailed". For technical information, type "Get-Help Set-RDMRepository -full".

EXAMPLE 1
PS C:\> $repository = New-RDMRepository -Name "New Repository" ; Set-RDMRepository repository

Create & save new repository.

RELATED LINKS
10.93 Set-RDMSessionAttachment

SYNOPSIS
Save/set the session.

SYNTAX
Set-RDMSessionAttachment -Attachment [Attachment] <PSConnectionAttachment[]> -Refresh [Refresh] [SwitchParameter] [CommonParameters]

DESCRIPTION
Save/set the session. Session must be first fetch via Session property of the Get-RDM-Session cmdlet or via the New-RDMSession result.

PARAMETERS
-Attachment <PSConnectionAttachment[]>
  (Required) PSSession object, must be retrieved from Get-RDMSession or created via New-RDMSession.

-Refresh <SwitchParameter>
  Send refresh notification to Remote Desktop Manager application.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Set-RDMSessionAttachment -detailed". For technical information, type "Get-Help Set-RDMSessionAttachment -full".
EXAMPLE 1
PS C:\> $list = Get-RDMSession; $list[1].Name = "New Name"; Set-RDMSession $list[1]

Retrieves the list of available sessions, modify the name of the second session, update the session.

RELATED LINKS

10.94 Update-RDMSessionAttachment

SYNOPSIS
Update attachment document.

SYNTAX

DESCRIPTION
Update attachment document.

PARAMETERS
-Attachment <PSConnectionAttachment> (Required) Attachment to update the document to.

-Filename <String> (Required) New document filename

-Refresh <SwitchParameter>
Send refresh notification to Remote Desktop Manager application.

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer and OutVariable. For more information, type, "get-help about_commonparameters".

NOTES
For more information, type "Get-Help Update-RDMSessionAttachment -detailed". For technical information, type "Get-Help Update-RDMSessionAttachment -full".

EXAMPLE 1
PS C:\> $session = Get-RDMSession -Name MySession; $attachments = Get-RDMSessionAttachment -Session $session; Update-RDMSessionAttachment -Attachment $attachments[0] -Filename 'C:\Mytestfile.txt'

Update the first attachment to the document at 'C:\Mytestfile.txt'.

RELATED LINKS
11 Knowledge Base

11.1 Protocols and application

11.1.1 Remote Desktop Manager

11.1.1.1 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.
11.1.1.2 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.

Make sure to check the Keep template host option.
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.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>VPN does not open when the session is opened.</td>
</tr>
<tr>
<td>Always connect</td>
<td>VPN opens when the session is opened.</td>
</tr>
<tr>
<td>Manual</td>
<td>VPN requires user to manually activate the VPN before opening the session.</td>
</tr>
<tr>
<td>Connect if unable to ping/scan</td>
<td>Remote Desktop Manager tests if the host responds, if not the VPN opens.</td>
</tr>
<tr>
<td>Inherited</td>
<td>VPN inherits the settings.</td>
</tr>
<tr>
<td>Ask for confirmation</td>
<td>VPN prompts for confirmation before opening.</td>
</tr>
<tr>
<td>Connect if network adapter not found</td>
<td>Remote Desktop Manager tests if network adapter is installed and active, if not the VPN opens.</td>
</tr>
<tr>
<td>Prompt if unable to ping/scan</td>
<td>Tests if the host responds, if not VPN prompts for confirmation before opening.</td>
</tr>
</tbody>
</table>

3. In the **Close** list, select how the VPN closes at the end of a remote session. We recommend **On session close**.
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>On session close</td>
<td>VPN closes automatically when the session is closed.</td>
</tr>
<tr>
<td>Manually Later</td>
<td>VPN requires user to manually close the VPN entry when finished.</td>
</tr>
<tr>
<td>Confirm disconnect</td>
<td>VPN prompts to close the VPN when session is closed.</td>
</tr>
</tbody>
</table>

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.

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.
3. **On** VPN/SSH/Gateway, select **Override VPN** box.

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.

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**.

### 11.1.1.3 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**.

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.
**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**.
2.2 To import a csv file, choose **Import from Login**.

3. Choose an entry type. All imported entries are converted to this type.
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.
11.1.1.4 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.

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:
### Remote Desktop Manager

**Export Selection**
Select one entry or more, then right-click the selection. In the context menu, under **Export**, select **Export Selection (.rdm)**.

**Export Special**
Select one entry or more, then right-click the selection. In the context menu, under **Export – Export Special**, select the desired export format.

**Export as RDP**
Select one RDP entry, then right-click the selection. In the context menu, under **Export**, select **Export Entry as Remote Desktop File (.rdp)**.

### Export all entries:

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export All Entries</td>
<td>Right-click an entry in the navigation pane. In the context menu, under <strong>Export</strong>, select <strong>Export All Entries (.rdm)</strong>.</td>
</tr>
<tr>
<td>Export Special</td>
<td>Right-click an entry in the navigation pane. In the context menu, under <strong>Export – Export Special</strong>, select the desired export format.</td>
</tr>
<tr>
<td>Export All Host</td>
<td>Right-click an entry in the navigation pane. In the context menu, under <strong>Export</strong>, select <strong>Export All Host List (.csv)</strong>.</td>
</tr>
<tr>
<td>Export All Documents</td>
<td>Right-click an entry in the navigation pane. In the context menu, under <strong>Export – Export Special</strong>, select <strong>Export All Documents</strong>.</td>
</tr>
</tbody>
</table>

The functionalities for exporting all entries are also available in the **File – Export** Menu.

**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.
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.

11.1.1.5 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

11.1.1.5.1 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.
2. In the computer field, use the $HOST$ variable and click on OK.
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.
11.1.1.5.2 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.

**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.
3. In the child sessions, use the appropriate Variables to retrieve the information that is saved at the folder level
11.1.1.5.3 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
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
### Select Templates

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑</td>
<td>RDP Template</td>
</tr>
<tr>
<td>☑</td>
<td>Second Template</td>
</tr>
</tbody>
</table>
5. Launch your **Host** session. You will be prompted to select the appropriate template to launch the session.

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>😃</td>
<td>RDP Template</td>
</tr>
<tr>
<td>😍</td>
<td>Second Template</td>
</tr>
</tbody>
</table>

### 11.1.1.6 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 Pwned 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.
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 hast 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.
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](image1)

2. Click **Add Vault**.

![Vaults – Add Vault](image2)

3. Enter a **Name** and **Description** (optional). The ID is generated automatically.

![Vault Management](image3)

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](image)

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**.

3. Select the repository you want to move the entries to, and click **Next**.
4. Choose the entries you want to transfer to the new repository, and click **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.

2. On the User and Security Management window, choose the Vaults, then click Assign Roles.

3. Choose which roles have access to the Vaults: select the Is Member box.
**Vaults shortcuts**

Navigate between Vaults with the [Vault List](#) or Vaults shortcuts.

We recommend administrators and users who have access to multiple Vaults create Vaults shortcuts to navigate between Vaults.

If you use Vaults shortcuts, the root should only contain folders. Do not save entries at the root.

The main (default) Vault contains shortcuts to other Vaults.
Remote Desktop Manager

Each Vault contains a shortcut that returns the user to the main Vault.

Create a Vault shortcut

1. On the Edit tab, click New Entry.

2. Click Miscellaneous and then select Vault (Shortcut).
3. In the **Name** box, enter the name of the Vault you are creating a shortcut to. Save the shortcut in a folder.

4. To find the **Vaults ID**, click the ellipses button. Enter a folder name (case sensitive) to create a shortcut to a specific folder.

5. Select the destination Vault.
We recommend removing the data source drop-down list when using Vault shortcuts. Then the Vaults list can be moved above the navigation pane.

Both options are configured in **File – Options – User Interface**.
11.1.1.8 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.

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
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.

11.1.1.9 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.
2. After, click on Application Logs.

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.
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.

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.

11.1.1.11 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.

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`
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.

### 11.1.1.12 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 another license. Please contact 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 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 to get a quote.

### 11.1.13 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.

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DataSource</strong></td>
<td>Indicate the data source or the database ID. Find them in the <strong>IDs</strong> section of the Advanced properties of an entry. 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.</td>
</tr>
<tr>
<td><strong>Session</strong></td>
<td>Indicate the ID of a session. Find it in the <strong>Session ID</strong> field in the Advanced properties of a session.</td>
</tr>
<tr>
<td><strong>Template</strong></td>
<td>Indicate the ID of the template of an entry. The template parameter retrieves some properties of a template and uses them against the session parameter. The host parameter is required when using the template parameter.</td>
</tr>
<tr>
<td><strong>Host</strong></td>
<td>Indicate the hostname or IP address of the remote device. Used along with the template parameter, or to override the host property of the session parameter.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Indicate the port to use. Used to override the port property of the session or template parameter.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>Indicate the username to use. Used to override the username property of the session or template parameter.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Indicate the password to use. Used to override the password property of the session or template parameter.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>Indicate the domain to use. Used to override the domain property of the session or template parameter.</td>
</tr>
<tr>
<td><strong>Title</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Filter</strong></td>
<td>Populate the Search field.</td>
</tr>
<tr>
<td><strong>Tabpage</strong></td>
<td>Give the focus to a tab in the dashboard after the application has completed the startup procedure. Available only with the Select action. The possible tabs are:</td>
</tr>
<tr>
<td></td>
<td>• Overview</td>
</tr>
<tr>
<td></td>
<td>• Documentation</td>
</tr>
<tr>
<td></td>
<td>• Macros/Scripts/Tools</td>
</tr>
<tr>
<td></td>
<td>• Management Tools</td>
</tr>
<tr>
<td></td>
<td>• Information</td>
</tr>
<tr>
<td></td>
<td>• Attachments</td>
</tr>
<tr>
<td></td>
<td>• Logs</td>
</tr>
<tr>
<td></td>
<td>• Recordings</td>
</tr>
</tbody>
</table>

**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**

```plaintext
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**

```plaintext
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.
2. The URL is stored in the clipboard.

![Remote Desktop Manager](image)

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.

### 11.1.1.14 Get Started with Remote Desktop Manager

**Description**

Here’s a checklist to help you and your team get started with Remote Desktop Manager.

Steps 1-5 configure the foundations of Remote Desktop Manager. Next, make a custom installation package with these settings (Step 6) and share the *.msi or *.exe with the rest of your team. Administrators: follow steps 7-10 to manage security and create entries.

<table>
<thead>
<tr>
<th>CHECKLIST FOR TEAMS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> - Register your license</td>
</tr>
<tr>
<td><strong>Step 2</strong> - Add your Data Source (for teams)</td>
</tr>
<tr>
<td><strong>Step 3</strong> - Select your Security Provider</td>
</tr>
<tr>
<td><strong>Step 4</strong> - Configure Application Options &amp; Default Settings</td>
</tr>
<tr>
<td><strong>Step 5</strong> - Create a Custom Installation Package</td>
</tr>
<tr>
<td><strong>Step 6</strong> - Data Source Settings (System Settings)</td>
</tr>
<tr>
<td><strong>Step 7</strong> - Organize Your Information: Vaults and Folders</td>
</tr>
<tr>
<td><strong>Step 8</strong> - Fill Your Vaults: Add Entries and Import Data</td>
</tr>
<tr>
<td><strong>Step 9</strong> - Add Roles</td>
</tr>
<tr>
<td><strong>Step 10</strong> - Add Users and Assign Them to Roles</td>
</tr>
<tr>
<td><strong>Step 11</strong> - Manage Access and Permissions</td>
</tr>
</tbody>
</table>
When adding a Data Source (on Step 2), pay close attention to your choice of settings, as these cannot be modified remotely once you've shared your installation package. For instance, the Caching mode is relevant to using the Offline mode. You should take a moment and think about the needs of your data source and select what is appropriate before moving on to exporting.

11.1.1.14.1 Register your license

You must save your license to use Remote Desktop Manager Enterprise.

How to save your license serial number:
- After installation (in the application).
- Save the serial number for the entire team (in Data Source Settings (System Settings)).
- Save the serial number for an individual (in the application).

After Installation

Immediately following installation, you will be prompted to enter a Trial license or purchased license serial number.

1. Copy the serial number from the email.

2. Enter the trial license serial number or your purchased license serial number.

If you are using Remote Desktop Manager with a team, we suggest saving the serial number in Data Source Settings (System Settings) as well. Everyone will have access to the license and you will only need to update it here.

After your 30-day trial expires you need to update your license. You will receive a new serial number when you buy or renew your Remote Desktop Manager license. You can register your license two ways:

**Good for teams:** Save the serial number in Data Source Settings (System Settings) so the license applies to all the team members.

**Suitable for individuals:** Save the registration key manually in application.

If you are using a trial license, use the instructions for individuals.

**Good for teams:** Save the serial number in Data Source Settings (System Settings)

1. Copy the serial number from the email.
2. On **Administration** tab, click **Data Source Settings (System Settings)**.

3. Select **Serial Number**.
4. Paste the serial number in **Serial (Site/Global)**.
5. Check **Hide serial number** so members of your team can't view the serial number in **Data Source Settings (System Settings)** or the **Register Product** dialog on the **Help** tab.
Your Remote Desktop Manager is now active for all the members of your team.

The first time other users log in a Register the Application window will appear. Users should click Cancel. The serial number has been saved in the data source and no further action is required.

Good for individuals: Save the serial number in Register Product
1. Copy the serial number from the email.
2. On Help tab, click Register Product.

4. Enter your Name and Email. Then paste the serial number in Serial.
5. Sign up for the newsletter (or opt-out).
The license is only saved in your individual application.

11.1.14.2 Add a data source

Entries and other information (e.g. roles and permissions) are saved in Vaults in the data source. If you aren't sure what type of data source to use, see choosing a data source. Remote Desktop Manager comes with a local data source installed. We suggest that you delete the local data source after you add your own.

Add a host and name

1. Click File – Data Sources.
2. Click Add a new data source.
Choose the data source
3. Choose the type of data source you want to use.

Data Source Configuration
1. Enter a data source Name.
2. Enter a Host.
3. Select the Login mode to choose the type of credentials people use to connect to the data source. If you are not using Integrated Security with Active Directory, we recommend Custom Login. A custom login creates a separate login for Remote Desktop Manager, preventing users from connecting directly to the database.
4. To enter the credentials for a database administrator account, click Settings. We recommend that you do not use an SA account.
5. Enter your Username and Password.
6. Create a database or use an existing database (see below for instructions).
Configure the database

New database
a. Enter a name for the database.
b. Click Upgrade and then Create Database.

Existing database
a. Click more options to browse for the database. Select the database.
b. Click Upgrade and then Update Database.
We suggest that you delete the local data source after you add your own.
Other users could add information to the local data source if it is available.

Learn more
Configure data source options, see Data Source Settings (System Settings).
Block user access to data source configuration with group policies.
Give users a private space to keep entries they do not want to save in the shared Vaults, see My Vault (Private).

11.1.1.14.3 Add a security provider

We recommend adding a security provider to encrypt other information (e.g. entry configuration, host names etc).

Procedure
1. Make sure no one else is connected to the data source.
2. Create a backup if you have already added entries.
3. Go to Administration – Security Provider. If you are using Devolutions Password Server the security provider is configured in the console, see XXX.
4. Click Change Security Settings.
5. Select the Security type: Shared passphrase or Certificate.
   Default is encryption for passwords only.

**Add a passphrase**

1. Select Shared Passphrase.
2. To set the passphrase, click Apply.
3. Enter the passphrase or use the password generator.
4. Re-enter the passphrase in Confirm.
5. Save or print the passphrase and keep it somewhere safe.

Users need to enter the passphrase when they configure the data source. If you would like them to enter the passphrase each time they connect to the data source, see group policies. Save passphrase in registry is only used with terminal services when multiple people access the passphrase from the same machine.

Learn more about security providers.
If you lose the passphrase, you will lose your information. There will be no way to get the information back. Keep the passphrase in a safe place.

**Add a certificate**

1. Select **Certificate**.
2. To configure the certificate, click **Apply**.
3. Choose the location: Current **User** or Local **machine**.
4. Choose the store.
5. To select an existing certificate for **Thumbprint**, click more options.
6. If you want to create your own self-signed certificate, click **Create Certificate**.

![Certificate Security Provider](image)

**Configure Certificate for Security Provider**

**11.1.1.14.4 Configure Remote Desktop Manager Options and Default Settings**

Create a uniform Remote Desktop Manager experience for your users by configuring options and creating default settings.

The options in **File – Options** configure application settings (e.g. updates, User Interface, installation paths).

Configure these options before making a custom installation package so Remote Desktop Manager is consistent across the team.

There is a [group policy](#) to block user access to **File – Options**.

**Options**

There are many options but we've highlighted two that might interest you: disabling auto-updates and configuring the installation path.

**Auto Update**
Remote Desktop Manager automatically prompts to install updates by default. If you do not want users to receive notifications, turn off this option.

1. Go to **File – Options**.
2. In **General**, select **Application Start**.
3. In the **Auto Update** section, uncheck **Enable check for updates**.

**Installation Path**
Customize this path if the third-party applications you use with Remote Desktop Manager are installed on a centralized path, for example on a shared network or drive. You can also set customized paths for templates, add-ons, screenshots, documents and logs.

1. Go to **File – Options**.
2. Click **Path**.
3. Click **Configure Installation Path**.
4. Select the application and enter the custom path.

**Default Settings**
Create default settings for specific types of entries. When a user creates a new entry the settings you configured will be set by default. It does not force the options.

The default settings are saved locally. To ensure everyone on the team has access to the same settings, configure the default settings before making the custom installation package.
1. Click **File – Templates**.
2. In the **Default settings** section, select the category of entry you want to configure. In this example we choose, **Session** for remote connections and **RDP (Microsoft Remote Desktop)**.

![Default Settings in File - Templates](image)

3. There are many options you can configure. Some popular options for RDP entries include:

   a) **Display**: Choose how the session opens (e.g. embedded).
   b) **Credential**: Choose which credentials to use (e.g. Credential repository, inherited).

   **Local resources**:
   c) **Keyboard**: Choose how to use window-key combinations.
   d) **Hard drive**: Share your hard drive during sessions.
Let's save the configurations we've completed so far (license, data source, security provider, and settings) and create a custom installation package. The advantage of custom installer package is that when other team members install Remote Desktop Manager, you can be sure everyone has the right configuration.

Make sure to configure custom installation paths and to have verified if your data source supports Offline mode (if desired) before you create the package.

Do not to share your personal credentials or credentials for the data source when making the installation file. Make sure you uncheck the options in the Installer File Generator.

Devolutions Account
You need a Devolutions Account to use the Custom Installer Service. The account is free and available to all Devolutions clients.

How it works
A. Save the installation file (*.rdi).
B. Create the package.
C. Download the installation package (*.exe or *.msi) from Devolutions Cloud.
D. Share the custom installation package with your team.

A. Save the installation file

This installation file includes the data source configuration as well as other options you have configured. Save the file as a base configuration so it’s available for custom installations in the future. You can use this file to create custom installation packages with newer versions of the application.

1. To export the installation package, click **File – Devolutions Account**.
2. Click **Installer File Generator**.
3. Uncheck the options in **Registration Information**: Name, Email, Key. This information will not be shared in the installation file. Make sure the license serial key is saved in **Data Source Settings (System Settings)**.
4. Do not share your personal credentials or the administrator credentials for the data source. Make sure both **Devolutions Cloud credentials** and **Include data source credentials** are unchecked. **Saved templates** are locally stored templates, the option is unchecked by default because they may contain credentials.
5. Click **Generate** to save the file, It saves as an *.rdi file.

B. Create the package

1. In **File – Devolutions Account**, click **Custom Installer Manager**.
2. Click **New Package**.
3. Choose the version of <%TITLE>.
4. Enter a package name and description, the latter being optional.
5. Choose **Using existing Remote Desktop Installer (*.rdi) file**.
6. Browse for the *.rdi file we saved before.
7. Click Create.
C. Download the installation package

It's almost ready. The custom installation package can take some time to create. You'll receive an email with the download link once the package is available on Devolutions Cloud. Download the package from the website and deploy it to your users.

D. Install the custom package

If a user installs a custom package and they already had an older version of RDM installed, they will see the message below.

This message appears because Remote Desktop Manager creates a new default configuration file during the custom installation.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use New Configuration (Lose Mine)</td>
<td>The new configuration is used. The old configuration is lost.</td>
</tr>
<tr>
<td>Retrieve New Registration Only</td>
<td>RDM uses the new serial key in the new configuration file, but retains the other options from the old configuration.</td>
</tr>
<tr>
<td>Ignore</td>
<td>The old configuration is used.</td>
</tr>
</tbody>
</table>

11.1.1.14.6 Organize your information: Vaults and Folders

We recommend using Vaults and Folders to organize information, manage access and simplify security.

Vaults are containers that divide the data source into smaller containers. Folders organize entries in a Vault.

Here is an example of Vaults in Remote Desktop Manager. It includes Vaults for different departments at "Windjammer Inc" and two Vaults for customers: Downhill Pro and Telemark.

<table>
<thead>
<tr>
<th>Image</th>
<th>Name</th>
<th>Description</th>
<th>Allow offline</th>
</tr>
</thead>
<tbody>
<tr>
<td>DO</td>
<td>Downhill Pro</td>
<td>Customer since 2015</td>
<td></td>
</tr>
<tr>
<td>TE</td>
<td>Telemark</td>
<td>Customer</td>
<td></td>
</tr>
<tr>
<td>WC</td>
<td>Windjammer Corp</td>
<td>Password Vault for non-administrative personnel</td>
<td></td>
</tr>
<tr>
<td>WK</td>
<td>Windjammer Default</td>
<td>Default Repository - Shortcuts and common tools</td>
<td></td>
</tr>
<tr>
<td>WI</td>
<td>Windjammer IT</td>
<td>For the IT department exclusive use</td>
<td></td>
</tr>
<tr>
<td>WM</td>
<td>Windjammer IT Vault</td>
<td>For IT personnel without the need for Connection Management</td>
<td></td>
</tr>
</tbody>
</table>

Example of Vaults

Here is an example of the folders in the Downhill Pro Vault. The folders Servers and UBNTU-LAMP are customized.
Example of folder structure in a Vault

**Vaults**

Vaults simplify user management because a role (Active Directory group) can be given access to particular Vaults. It reduces the need for permissions on lower level folders.

A good practice is to use one Vault per department or client.

**Add a Vault**

1. Go to *Administration – Vaults.*

3. Enter a **Name** and optional **Description**.
4. To configure security, offline mode, permissions, and other options on the Vault, see [Root Settings](#).

Learn more about [Vaults](#).

### Folders

Folders are used to organize entries inside the Vault.

We recommend you save all your entries inside folders (i.e. no individual entries should be saved at the root level).

#### Add a folder

1. Go to **Edit – New Entry**.

2. Choose **Folder**.
3. Select the folder and click Properties on the Edit tab to configure options (e.g. VPNs, Permissions). Entries can inherit settings from the folder.
It's time to fill the Vaults with entries. Remote Desktop Manager includes over 150 types of entry. Entries include information for different uses: remote connections, credentials, VPNs, Documents, Scripts and more.

**Add an entry**

1. On the **Edit** tab, click **New Entry**.

2. Choose an entry type.

3. You can sort through the entry list with the filtering field.
4. Enter information about the entry. Not all the information is required. Common configurations are:
   a) **Folder**: Choose where the entry is saved. This default setting is your current selection in the Tree view.
   b) **Display**: Choose how an entry opens (e.g. Embedded (tabbed), Undocked or External)
   c) **Credentials**:
      - **Default**: Enter the username and password on the entry
      - **Inherited**: Inherits credentials from a higher folder.
      - **Credential repository**: choose from credentials in the Vault or prompt on connection with a list.
        A good option if you save shared credentials in specific folders.

5. There are common settings for every entry (e.g. permissions, VPN, logs) that customize entries.

**Import information**
Remote Desktop Manager imports from third-party applications, including RDP configurations, KeePass, LogMeIn and many more.

1. To import, click **File – Import**.
2. Choose the application you are importing information from.
3. The import wizard guiding you through the rest of the process varies depending on the source application. The entries are imported into the current Vault.

**Learn More**
Here is an example step-by-step guide and video: [Import accounts from KeePass](#).
Remote Desktop Manager has role-based access control. Roles provide granular control over what users in that role can see and do. All restrictions are enforced through permissions attributed to a specific role.

If you are using Devolutions Password Server, you can synchronize roles with Active Directory groups.

**Add Roles**
1. On the **Administration** tab, click **Roles**.
2. Click **Add Role**.
3. Enter a role **Name** and an optional **Description**.

**Give roles access to Vaults**
Use roles to manage who can see the Vault. Only members of the role will see the Vault, it will not be revealed to other users. You can use permissions to manage what the roles can do in the Vault.

1. On the **Administration** tab, click **Vaults**.
2. To edit a Vault's properties, click the properties button (pencil icon).
3. Click **Roles**.
4. Check **Is Member**.

Assign roles and users to Vaults in Vault Management
Why can’t members of the role see the Vault?

New databases have restricted access turned on by default. It means that all permissions are set to never. You need to give users permission to view the Vault. Learn more in Manage Access and Permissions.

Learn more
Create users and assign them to the roles
Give roles permissions

Add Users and Assign Them to Roles

The instructions below are to manually add users. If you are using Devolutions Password Server, you can synchronize users with Active Directory.

Add Users
1. In the Administration tab, under the Management section, click Users.
2. Click Add User.
3. Select the Authentication type to choose the type of credentials people use to connect to the data source. If you are not using Integrated Security with Active Directory, we recommend Custom Login. A custom login creates a separate login for Remote Desktop Manager, preventing users from connecting directly to the database.
4. Enter a Username.
5. Enter a password (if not using Integrated Security). It can be a temporary password: Check User must change password at next logon.
6. Select a User Type: Administrator, User, Restricted user, Read-only user. With Restricted User you can give permissions to add, edit, delete, etc.
7. Select a User license type. Default is Connection Management is for users who open remote connections (e.g. RDP or SSH sessions).
Assign Users to Roles

You only need to assign users to custom roles. If you are using Devolutions Password Server and Active Directory Groups you do not need to manually assign users to roles.

1. On the Administration tab, click Roles.
2. Click Assign Users to Roles.
3. Select users and check the user Is Member of the role.
Administrators give roles and users permissions to perform different actions.

Permissions are set at various levels:
- Data Source Permissions (System Permissions)
- Vaults (Root Settings)
- Folders
- Entries

Data Source Permissions
Permissions apply to the entire data source. Permissions are related to:
- Entries (e.g. import/export).
- Vaults.
- Templates.
- Logs and reports.
- Tools.
- Add in Root.
1. On the **Administration** tab, click **Data Source Permissions (System Permissions)**. The current default setting is in brackets.

**Vaults (Root Settings)**

The permissions in **Root Settings** apply to all the entries in the Vault. To set the permissions for the Vault, on the **Administration** tab, click **Root Settings**, then click **Permissions**.

There are many options. We want to draw your attention to two settings:

**View Password**: Change password visibility. A user can still open a remote connection in embedded mode without seeing the password.

**Execute**: Controls whether a user can use an entry (e.g., open a remote connection).

**Restricted Access**

Restricted access sets all permissions to **never**. An administrator then gives rights to view items and perform actions, as needed.

The option **Create Vault with restricted access by default** is enabled.

With restricted access, when you assign users to a Vault you must give them permission to view the contents of the Vault.

**Restricted Access: Allow members of a role to see contents of Vault**

1. On the **Administration** tab, click **Root Settings**.
2. Click **Permissions**.
3. Set **Permission** to **Custom**.
4. Set **View** to **Custom**.
5. Click **Select roles or users**. Choose the roles you want to view the Vault contents.
When restricted access is turned off, the permissions are set to default (everyone) at the root and permissions are inherited from the user (e.g. permissions set with restricted users).

You can change restricted access in **Data Source Settings (System Settings) – Security**.

**Folders**

Assign permissions to high level folders when permissions set at the Vault level are not sufficient. When configuring access and permissions on folders you are creating an exception to the general permissions for the Vault.

To edit permissions on a folder, select the folder and click **Properties**. Then click **Permissions**. On a folder, **Default** refers to the Vault permissions (root settings) or a higher level folder. The settings that are used are displayed beside the drop down lists.
Lower level folders can inherit permissions from parent folders.

**Entries**

You can set permissions on individual entries too. Select the entry, click **Properties**. Then click **Permissions**. Default refers to a parent folder. When the higher level folder is set to **Default** or **Inherited**, the entry will follow the permissions set at root. The settings that are used are displayed beside the dropdown lists.

### 11.1.15 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.

### 11.1.1.16 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.

### 11.1.2 Remote Desktop Manager Jump

#### 11.1.2.1 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](image)

2. Click **Jump Host** and check **Is Jump Host**.
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**.
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**.

2. Click **Open Session**. The Remote Desktop Manager Jump opens automatically. It looks like a session in a session.
11.1.3 RDP

11.1.3.1 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 is 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.

11.1.4 SSH

Description

TBD

11.1.4.1 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.

11.1.5 VMware

11.1.5.1 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**

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.

11.1.6  Tips and tricks

11.1.6.1  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

11.1.6.2  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.
11.2 Performance

11.2.1 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:

<table>
<thead>
<tr>
<th>VALUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Uses the value set in File – Options – Types – RDP – Cache.</td>
</tr>
<tr>
<td>Full Mode</td>
<td>The protocol is full Windows 8 Remote Desktop Protocol cache.</td>
</tr>
<tr>
<td>Thin client</td>
<td>The protocol is limited to using the Windows 7 with SP1 RemoteFX codec and a smaller cache. All other codecs are disabled. This protocol has the smallest memory footprint.</td>
</tr>
<tr>
<td>Small cache</td>
<td>The protocol is the same as Full mode, except it uses a smaller cache.</td>
</tr>
</tbody>
</table>

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.
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.

![Remote Desktop Manager](Image)

Details of the RDP global options

11.3 Security

11.3.1 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 result 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](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 approaches 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](#).

### 11.3.2 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.

   ![Certificate Information]

   - **Issued to:** *.devolutions.net
   - **Issued by:** Go Daddy Secure Certificate Authority - G2
   - **Valid from** 2018-07-25 to 2020-07-25

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.

![Certificate options screenshot]

#### 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.
Tools

Here are some tools that can be used to verify the newly exported certificate:

1. Using PowerShell (requires PowerShell v4):
   
   1.1 In a PowerShell console, replace the path below with the path of your certificate, then run:

   ```powershell
   $cert=New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("C:\path\to\certificate\cert.cer")
   ```

   1.2 Then, run the following command:

   ```powershell
   Test-Certificate -Cert $cert
   ```

2. Using CMD:

   Run the following command (replace the path below with the path of your certificate):

   ```cmd
   ```
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.

11.3.3 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.

For information about saving credentials in Windows, see Credentials Overview. You can also learn more in the Windows Credential Manager section.
Support/Resources
# 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

<table>
<thead>
<tr>
<th>ACTION</th>
<th>SHORTCUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Ctrl+F</td>
</tr>
<tr>
<td>Force Refresh</td>
<td>Ctrl+F5</td>
</tr>
<tr>
<td>Online Help</td>
<td>F1</td>
</tr>
<tr>
<td>Quick Connect</td>
<td>Ctrl+Alt+Q</td>
</tr>
<tr>
<td>Refresh</td>
<td>F5</td>
</tr>
</tbody>
</table>

### Edit

<table>
<thead>
<tr>
<th>ACTION</th>
<th>SHORTCUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Credential Entry</td>
<td>Alt+Shift+N</td>
</tr>
<tr>
<td>Add Folder</td>
<td>Ctrl+Shift+N</td>
</tr>
<tr>
<td>Add Information</td>
<td>Ctrl+Alt+N</td>
</tr>
<tr>
<td>Add Session</td>
<td>Ctrl+N</td>
</tr>
<tr>
<td>Delete</td>
<td>Ctrl+Del</td>
</tr>
<tr>
<td>Duplicate</td>
<td>Ctrl+D</td>
</tr>
<tr>
<td>Edit Entry</td>
<td>Ctrl+E</td>
</tr>
<tr>
<td>Local Specific Settings</td>
<td>Ctrl+Alt+E</td>
</tr>
<tr>
<td>New Entry</td>
<td>Ins</td>
</tr>
<tr>
<td>Rename Entry</td>
<td>F2</td>
</tr>
<tr>
<td>User Specific Settings</td>
<td>Ctrl+Shift+E</td>
</tr>
</tbody>
</table>

### Actions
### Action

<table>
<thead>
<tr>
<th>ACTION</th>
<th>SHORTCUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clipboard - Copy Connection String</td>
<td>Ctrl+Alt+H</td>
</tr>
<tr>
<td>Clipboard - Copy Domain</td>
<td>Ctrl+Alt+B</td>
</tr>
<tr>
<td>Clipboard - Copy Host Name</td>
<td>Ctrl+H</td>
</tr>
<tr>
<td>Clipboard - Copy Password</td>
<td>Ctrl+Shift+B</td>
</tr>
<tr>
<td>Clipboard - Copy Url</td>
<td>Ctrl+Shift+H</td>
</tr>
<tr>
<td>Clipboard - Copy Username</td>
<td>Ctrl+B</td>
</tr>
<tr>
<td>Execute Typing Macro</td>
<td>Ctrl+Shift+A</td>
</tr>
<tr>
<td>Navigate URL</td>
<td>Enter</td>
</tr>
<tr>
<td>Open (Embedded/Tabbed)</td>
<td>Ctrl+Enter</td>
</tr>
<tr>
<td>Open (External)</td>
<td>Shift+Enter</td>
</tr>
<tr>
<td>Open (Full screen)</td>
<td>Alt+Enter</td>
</tr>
<tr>
<td>View Password</td>
<td>Ctrl+P</td>
</tr>
</tbody>
</table>

### View

<table>
<thead>
<tr>
<th>ACTION</th>
<th>SHORTCUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>Alt+F6</td>
</tr>
<tr>
<td>Details</td>
<td>F12</td>
</tr>
<tr>
<td>Favorites</td>
<td>F10</td>
</tr>
<tr>
<td>Grouped Tab Pane</td>
<td>Ctrl+Alt+F9</td>
</tr>
<tr>
<td>Header Pane</td>
<td>Alt+Shift+F6</td>
</tr>
<tr>
<td>Large Icons</td>
<td>F6</td>
</tr>
<tr>
<td>Navigation Pane</td>
<td>Alt+F8</td>
</tr>
<tr>
<td>Opened Sessions</td>
<td>F8</td>
</tr>
<tr>
<td>Play List Management</td>
<td>Ctrl+G</td>
</tr>
<tr>
<td>RDP Toggle View Only</td>
<td>Shift+F3</td>
</tr>
<tr>
<td>Recent (Recent Used Entries)</td>
<td>F9</td>
</tr>
<tr>
<td>Status Bar</td>
<td>Alt+F7</td>
</tr>
<tr>
<td>Tabbed Entries Pane</td>
<td>Alt+F9</td>
</tr>
<tr>
<td>Tiles</td>
<td>F3</td>
</tr>
<tr>
<td>Top Pane</td>
<td>Alt+F11</td>
</tr>
<tr>
<td>Tree View</td>
<td>F7</td>
</tr>
</tbody>
</table>

### Navigation
### ACTION  | SHORTCUT
---  | ---
Change Data Source  | Ctrl+Shift+D
File  | Ctrl+Shift+F
Focus Dashboard  | Ctrl+Shift+L
Focus Tab  | Ctrl+Shift+Up
Focus Tree/List  | Ctrl+L
Goto Bookmark 1  | Ctrl+1
Goto Bookmark 2  | Ctrl+2
Goto Bookmark 3  | Ctrl+3
Goto Bookmark 4  | Ctrl+4
Goto Bookmark 5  | Ctrl+5
Goto Bookmark 6  | Ctrl+6
Goto Bookmark 7  | Ctrl+7
Goto Bookmark 8  | Ctrl+8
Goto Bookmark 9  | Ctrl+9
Select Next Tab  | Ctrl+Shift+Right
Select Previous Tab  | Ctrl+Shift+Left
Set Bookmark 1  | Ctrl+Shift+1
Set Bookmark 2  | Ctrl+Shift+2
Set Bookmark 3  | Ctrl+Shift+3
Set Bookmark 4  | Ctrl+Shift+4
Set Bookmark 5  | Ctrl+Shift+5
Set Bookmark 6  | Ctrl+Shift+6
Set Bookmark 7  | Ctrl+Shift+7
Set Bookmark 8  | Ctrl+Shift+8
Set Bookmark 9  | Ctrl+Shift+9
Switch Vault  | Ctrl+Shift+R

### Import/Export

| ACTION  | SHORTCUT
---  | ---
Import Entries (.rdm, .pvm, .vnc, .rdp)  | 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]

<table>
<thead>
<tr>
<th>PARAMETERS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>{filename [<em>.rdm,</em>.rdp]}</td>
<td>Open in embedded or external mode the connection from file name.</td>
</tr>
<tr>
<td>/Silent</td>
<td>Execute the application minimized in a system tray icon. This option cannot be combined with other parameters.</td>
</tr>
<tr>
<td>/Datasource:{datasource id}</td>
<td>Specify the data source ID (available in the Advanced Tab of the session).</td>
</tr>
<tr>
<td>/Session:{session ID};</td>
<td>Specify one or more session IDs (available in the Advanced Tab of the session).</td>
</tr>
<tr>
<td>{session ID}...</td>
<td>/UserName:{username}</td>
</tr>
<tr>
<td>/Domain:{domain}</td>
<td>/Password:{password}</td>
</tr>
<tr>
<td>/ChangePassword:{new password}</td>
<td>Change the session password. Only available for Remote Desktop sessions and embedded passwords. The data source ID and the session ID are required.</td>
</tr>
<tr>
<td>/RegisterUser:&quot;{registration user}&quot;</td>
<td>Change the Remote Desktop Manager registration name. The value must be in double quotes.</td>
</tr>
<tr>
<td>/RegisterSerial:&quot;{serial number}&quot;</td>
<td>Change the Remote Desktop Manager serial number. The value must be in double quotes.</td>
</tr>
<tr>
<td>/Template:{template ID}</td>
<td>Open the template ID with the specified host name and an optional username/password.</td>
</tr>
<tr>
<td>/Host:{host name}</td>
<td>/UserName:{username}</td>
</tr>
<tr>
<td>/Domain:{domain}</td>
<td>/Password:{password}</td>
</tr>
<tr>
<td>/Profiler</td>
<td>Starts the profiler at start of application. Good for profiling the start process.</td>
</tr>
<tr>
<td>/Title:&quot;{title}&quot;</td>
<td>Specify a tab title when using an embedded session.</td>
</tr>
<tr>
<td>/Filter:{filter}</td>
<td>Execute the application with the filter filled with a parameter.</td>
</tr>
<tr>
<td>/TabPage: Dashboard</td>
<td>The Dashboard is selected at startup of the application.</td>
</tr>
</tbody>
</table>

Usage

Example #1 - Open a template and connect to a host
RemoteDesktopManager.exe /DataSource:178c2fda-dab4-4f41-98df-6e3205c0a011 /Template:a666b21b-1479-4eee-b482-0a3d561d2411 /Host:Windjammer-PC1

Example #2 - Open a session
RemoteDesktopManager.exe /DataSource:178c2fda-dab4-4f41-98df-6e3205c0a011 /Session:474bcbcf-d507-435b-8c0a-a9e868781910

Example #3 - Register the application
RemoteDesktopManager.exe /RegisterUser:"First name, Last name" /RegisterSerial:"xxxxx-xxxxx-xxxxx-xxxxx-xxxxx"
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.
12.5 **Technical Support**

**Standard Support plan**

Support is solely through our online forums at [https://forum.devolutions.net/](https://forum.devolutions.net/).

**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.

You are also encouraged to find information and ask questions on our forum at [https://forum.devolutions.net/](https://forum.devolutions.net/). It contains years of relevant information and have the benefit of being enriched for the whole community when we post an answer.

Please consult our [Support Policy](https://forum.devolutions.net/) for more information.

12.6 **Add-on Documentation**

**Description**

This section contains the documentation of the Add-ons for Remote Desktop Manager. Not all Add-ons are provided by Devolutions but we'll do our best to cover what we host in our add-on repository.

See [Add-on Manager](https://forum.devolutions.net/) for more details on how to install or manage Add-ons.

See topics below for more information about more complex Add-ons:

- [Bomgar Representative Console Add-on](https://forum.devolutions.net/)
- [DbVisualizer Add-on](https://forum.devolutions.net/)
12.6.1 Bomgar Representative Console Add-on

Description

This entry is used to define and configure a "Bomgar Representative Console" session.

With this Add-on you will be able to define a session that will can automatically:

- Login
- Start a session with a search string (host/description)
- Start a script from disk
- Save a script within the session data to be able to start it on another workstation.

The Bomgar Representative Console entry type is available when the Bomgar Representative Console Add-on is installed.

Make sure that you have a bomgar-rep.exe file in the installation folder of Bomgar. You need the same file to be present in each site that you will create. Then, go in File – Options – Path – Bomgar Representative and configure Remote Desktop Manager to point on the appropriate installation folder.

Settings

Bomgar Representative Console
### OPTION

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
</table>
| Bomgar site | Select the Bomgar site to login. To create the Bomgar site properly, you need to create a folder for each of your sites. In each folder, make sure that bomgar-rep.exe is also present. Example:  
- C:\Program Files\Bomgar\Representative\Site1  
- C:\Program Files\Bomgar\Representative\Site2 |
| Username    | Enter the username to access the Bomgar site. |
| Password    | Enter the password to access the Bomgar site. |
| Starting method | Start a pinned client session with a search string: Start a client session with a search string. Indicate the Host/Description in the appropriate field.  
Start a script file name on local disk: Start a script from disk. Indicate the script in the Script Filename field.  
Start a stored script in session: Save a script within the session data to be able to start it on another workstation. Indicate the script in the Script Filename field. |
| Host/Description or Script Filename | See Starting method option. |

### 12.6.2 DbVisualizer Add-on

#### Description

This entry is used to define and configure a "DbVisualizer" session. DbVisualizer is a universal database tool used by developers, DBAs and analysts. It can be used on all major operating systems to access a wide range of databases.

The DbVisualizer entry type is available when the DbVisualizer Add-on is installed.
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection name</td>
<td>Enter the name of the connection.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username to connect on the database.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password to connect on the database.</td>
</tr>
<tr>
<td>SQL script file</td>
<td>Select the SQL script file (*.sql).</td>
</tr>
<tr>
<td>Preferences directory</td>
<td>Select the preferences directory on the computer.</td>
</tr>
<tr>
<td>Database encoding</td>
<td>Select the prefer database encoding.</td>
</tr>
<tr>
<td>Custom window title</td>
<td>Indicate the window title that you want to be display.</td>
</tr>
</tbody>
</table>

12.6.3 NoMachine Add-on

Description

This entry is used to define and configure a "NoMachine" session. This allows you to store in Remote Desktop Manager each NoMachine profile as a distinct session, so that you can connect automatically to different computers (exactly like RDP sessions).
The NoMachine entry type is available when the NoMachine Add-on is installed.

Settings

NoMachine entry

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting method</td>
<td><strong>Using profile file name on local disk</strong>: The session will be linked to an existing profile (file) on a computer and it will be dependent on it.</td>
</tr>
<tr>
<td></td>
<td><strong>Using stored profile in session</strong>: The data of an existing profile (file) will be stored directly in the session and it will be usable on any other computer that shares the data source.</td>
</tr>
<tr>
<td>Profile</td>
<td>Select the NoMachine profile to use for the connection.</td>
</tr>
</tbody>
</table>

12.6.4 PenguiNet SSH Client Add-on

Description

This entry is used to define and configure a "PenguiNet SSH Client" session. PenguiNet is a simple all-in-one SSH client for Windows. It also includes an SCP browser so that you can easily transfer files with just a few mouse clicks.

The PenguiNet SSH Client entry type is available when the PenguiNet SSH Client Add-on is installed.
**PeguiNet SSH Client - Profile name**

**Start method - Profile name**

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>Enter the profile name to connect on PenguiNet.</td>
</tr>
<tr>
<td>Start a Secure CoPy session (SCP)</td>
<td>Allow to start a Secure CoPy session (SCP). Secure CoPy or SCP is a means of securely transferring computer files between a local host and a remote host or between two remote hosts.</td>
</tr>
</tbody>
</table>

**PeguiNet SSH Client - Parameters**

**Start method - Parameters**
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Indicate the name of the host to connect.</td>
</tr>
<tr>
<td>Port</td>
<td>Indicate the port that you may use to connect.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username to connect with Penguinet.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password to connect with Penguinet.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Indeterminate the protocol that you want to use. Select between: Telnet, SSH, SCP</td>
</tr>
<tr>
<td>Terminal type</td>
<td>Indeterminate the terminal type that you want to use. Select between: Linux, VT100, Xterm</td>
</tr>
<tr>
<td>UTF-8</td>
<td>Allow you to use the UTF-8. The UTF-8 is a variable-width encoding that can represent every character in the Unicode character set.</td>
</tr>
<tr>
<td>Don't use SOCKS Server</td>
<td>Disallow the use of a SOCKS Server to connect with Penguinet.</td>
</tr>
</tbody>
</table>

### 12.6.5 SAP Frontend Server (SAP GUI) Add-on

**Description**

This entry is used to define and configure an "SAP Frontend Server (SAP GUI)" session. This allows you to start sessions selected from your saplogon.ini files located anywhere on your computer.

The SAP GUI entry type is available when the SAP Frontend Server (SAP GUI) [Add-on](#) is installed.
The SAP Frontend Server (SAP GUI) add-on does not allow you to insert connection information manually without selecting a saplogon.ini file first.

**Features**

- Possibility to copy/create saplogon.ini independent sessions. If you’re working in a not editable saplogon.ini environment (or daily refreshed due GroupPolicies from your Client-Team).
- Automatic logon and execute Transaction/Reports.
- Support for Secure Network Connect (SNC).
- Connections over saprouter(s), handles Loadbalancing (Logongroups), etc.

**Requirements**

Installation of SAP Frontend Server (SAP GUI) on Client required.

**Limitations**

Only external Sessions are possible.

### 12.6.6 Shutdown Application Tool Add-on

**Description**

The Shutdown Application Tool allows you to shutdown or restart one or many computers at the same time.

The Shutdown Application Tool is available when the Shutdown Application Tool Add-on is installed.

**Settings**

The Shutdown Application Tool is accessible from the Dashboard under the Macros/Scripts/Tools section.
**Shutdown/Restart Computer in Dashboard**

**Usage**

Select one or several computers that you want to restart or shutdown in the Navigation Pane and click on **Shutdown/Restart Computer** in the Dashboard.

Select the option that want those computer(s) to do, enter a comment and click on **Execute**.
12.6.7 SQL Server Management Studio Add-On

Description

This entry is used to define and configure an "SQL Server Management Studio" session. This allows you to launch and perform authentication to an instance. Optionally you can select a database, as well as open a script in the editor. SQL Server Management Studio is primarily a GUI tool, if you need to run commands and exit automatically, you should look at the SQLCMD tool that comes with the Sql Server utilities.

The SQL Server Management Studio entry type is available when the SQL Server Management Studio Add-on is installed.

Settings
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Indicate the full instance name. When a default instance as been used, normally you can put only the server name here</td>
</tr>
<tr>
<td>Database</td>
<td>Used to indicate to select a database upon login.</td>
</tr>
<tr>
<td>Integrated Security (Active Directory)</td>
<td>Indicates to use your windows credentials to authenticate on the server.</td>
</tr>
<tr>
<td>Run as different user (Integrated security only)</td>
<td>Use a different user to authenticate on the server.</td>
</tr>
<tr>
<td>Net Only (Integrated security only)</td>
<td>Use to make connections that are made from computers that are not on the customer's domain.</td>
</tr>
<tr>
<td>Username</td>
<td>When using Sql Server authentication, username to use.</td>
</tr>
<tr>
<td>Password</td>
<td>When using Sql Server authentication, password to use.</td>
</tr>
<tr>
<td>Default query file (Optional)</td>
<td>Specifies a file that will be opened in the editor. Please see note below</td>
</tr>
<tr>
<td>Show splash screen</td>
<td>Indicates to let Sql Server Management Studio display its splash screen.</td>
</tr>
</tbody>
</table>

**Note**

On some systems, specifying a file to open in the editor has the side effect of preventing the Object Explorer from being connected. This renders the add-on useful only for when you want to run the script and exit soon after. If you need to use the Object Explorer do not specify a script file.
12.6.8 VPN Add-ons

Description

Multiple VPN Add-ons can be installed using Remote Desktop Manager Add-on Manager.

We support a very wide variety of VPN Add-ons, explore them to your heart's content. Consult the three topics below for examples on what our VPN Add-ons look like:

- Cisco AnyConnect
- Generic VPN
- OpenVPN

12.6.8.1 Cisco AnyConnect

Description

Cisco AnyConnect VPN Client Add-on can be used to connect to your Cisco AnyConnect VPN session.

This Add-on can be installed using the Add-on Manager.

The Cisco AnyConnect will not be able to see if the VPN is already open on its own.
12.6.8.2 Generic VPN

Description

Generic VPN Add-on can be used to connect to your Generic VPN session.

This Add-on can be installed using the Add-on Manager.
12.6.8.3 OpenVPN

**Description**

OpenVPN Add-on can be used to connect to your OpenVPN VPN session.

This add-on requires Remote Desktop Manager to be runned with elevated privileges (run as administrator).

This Add-on can be installed using the Add-on Manager.
Information

For the Certificate and Key fields it's important that your files are into the same folder as the *.ovpn files.

You cannot use a configuration as below.

```
CA Certificate
Client Certificate\client_svpn\client1.crt
Client Key\client_svpn\client1.key
TLS Key
```

12.7 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 then the Free Edition.
12.7.1 Data Backups

Description

It is recommended to always have a current backup of your data source. Since we support a wide range of data stores, you should use the best solution for your chosen data source.

- **Amazon S3**
  Please consult Amazon website for their backup policy.

- **Devolutions Password Server**
  Devolutions Password Server use a SQL Server database to store the data. We recommend creating a maintenance plan to perform automatic backups regularly. This topic is a good start on the subject: [Setting up a Maintenance Plan to Backup Databases](#).

- **Dropbox**
  Please consult Dropbox website for their backup policy.

- **FTP**
  We recommend creating a maintenance plan to perform automatic backups regularly.

- **MariaDB**
  We recommend creating a maintenance plan to perform automatic backups regularly.

- **Microsoft Access**
  Our recommended backup solution is to use our free [Online Backup Service](#).

- **Microsoft SQL azure**
  We recommend creating a maintenance plan to perform automatic backups regularly.

- **Microsoft SQL Server**
  We recommend creating a maintenance plan to perform automatic backups regularly. This topic is a good start on the subject: [Setting up a Maintenance Plan to Backup Databases](#).

- **MySQL**
  We recommend creating a maintenance plan to perform automatic backups regularly. The following link is a good start on the subject: [http://dev.mysql.com/doc/refman/5.7/en/backup-methods.html](http://dev.mysql.com/doc/refman/5.7/en/backup-methods.html).

- **Online Database**
  The protection offered by Online Database is for Disaster recovery only, for instance a hardware failure. Note that we cannot restore a backup of a single database. Using our Entry History and our [View Deleted](#) features, you can revert any change on specific sessions.
Online Drive
Our recommended backup solution is to use our free Online Backup Service.

SFTP
We recommend creating a maintenance plan to perform automatic backups regularly.

SQLite
Our recommended backup solution is to use our free Online Backup Service.

Web
We recommend creating a maintenance plan to perform automatic backups regularly.

XML
Our recommended backup solution is to use our free Online Backup Service.

12.7.2 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.
```powershell
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!
```

### 12.7.3 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).

### 12.7.4 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).

For more information, please consult [VPN Overview](#).

### 12.8 How-To

#### 12.8.1 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**

2. Select Create a database template

3. Select the Web Browser (http/https) session type.
4. Indicate the proper information in the template and click on **OK**.
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**.
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.
7. You can now launch the web link (website) from the Tree View.

12.8.2 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.
In the console tree, click the folder under Administrative Templates that contains the policy settings you want to configure.
### General

<table>
<thead>
<tr>
<th>POLICY NAME</th>
<th>REGISTRY KEY (PLEASE SEE NOTE 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable the application automatic update check</td>
<td><code>%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableAutoUpdate</code></td>
</tr>
<tr>
<td>Disable the Help - Check Version button</td>
<td><code>%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableUpdate</code></td>
</tr>
<tr>
<td>Disable the x64 edition of the application</td>
<td><code>%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableX64</code></td>
</tr>
<tr>
<td>Disable the x86 of the application</td>
<td><code>%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableX86</code></td>
</tr>
</tbody>
</table>

### Security

<table>
<thead>
<tr>
<th>POLICY NAME</th>
<th>REGISTRY KEY (PLEASE SEE NOTE 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force the user to always be prompted for the passphrase while connecting to</td>
<td><code>%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\AlwaysPromptForPassphrase</code></td>
</tr>
<tr>
<td>a data source that is protected by a Passphrase Security Provider</td>
<td></td>
</tr>
<tr>
<td>Force the user to always be prompted for his credentials when opening the</td>
<td><code>%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\ForceLogin</code></td>
</tr>
<tr>
<td>application</td>
<td></td>
</tr>
</tbody>
</table>
## Sessions

<table>
<thead>
<tr>
<th>POLICY NAME</th>
<th>REGISTRY KEY (PLEASE SEE NOTE 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable the add-on creation and the Add-on Manager</td>
<td>%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableAddOn</td>
</tr>
<tr>
<td>Disable the custom image edition in the session configuration</td>
<td>%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableCustomImage</td>
</tr>
<tr>
<td>Disable the reveal password command</td>
<td>%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableRevealPassword</td>
</tr>
</tbody>
</table>

## User Interface

<table>
<thead>
<tr>
<th>POLICY NAME</th>
<th>REGISTRY KEY (PLEASE SEE NOTE 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable all the local application tools like the Event Viewer or IIS</td>
<td>%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableApplicationTools</td>
</tr>
<tr>
<td>Disable the Devolutions Cloud usage</td>
<td>%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableOnlineAccount</td>
</tr>
<tr>
<td>Disable the menu File - Data Sources</td>
<td>%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableFileDataSources</td>
</tr>
<tr>
<td>Disable the menu File - Options</td>
<td>%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableFileOptions</td>
</tr>
<tr>
<td>Disable the My Personal Credential feature</td>
<td>%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableMyPersonalCredentials</td>
</tr>
<tr>
<td>Disable the menu Help - About</td>
<td>%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableAbout</td>
</tr>
<tr>
<td>Disable the import and the export of the Configuration File in File - Options</td>
<td>%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableImportExportOptions</td>
</tr>
<tr>
<td>Disable the possibility to drag and drop sessions</td>
<td>%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\DisableDragAndDrop</td>
</tr>
<tr>
<td>Force the Merge credential list with sessions option</td>
<td>%Root%\SOFTWARE\Policies\Devolutions\RemoteDesktopManager\EnableMergeCredentialListWithSessions</td>
</tr>
</tbody>
</table>

## 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.
12.8.3 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.

12.8.4 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.

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 used.
5. Enable the REST API to have a API Auth Token key generated

XML-RPC API access:
- REST API: Enable

AUTH Token: [Reg]

(Copy the generated API Auth Token)

Token validity:
- Never Expires

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.**
7. Click on **New** to create a Password Manager Pro account
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**.

9. You can now create a Password Manager Pro credential entry in Remote Desktop Manager
12.8.5 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.
2. Click on Extensions in the Administration section and select **Browse Online Extensions**.

3. Install 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)**.
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.
12.8.6 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.

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.
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.

12.8.7 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.

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

4. Press and hold the gold button on the Yubikey and access will be granted.
12.8.8 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](image)

12.8.9 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.

### 12.8.10 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](image)

   **Error Message dialog**

   An unexpected error has occurred. Please check the execution log.

   - Enterprise Edition 2019.1.35.0
   - Running since: 27 min 33 sec
   - Memory usage: 274 MB
   - Exception

2. To see more information regarding the error click on Details.
An unexpected error has occurred. Please check the execution log.

Enterprise Edition 2019.1.35.0
Running since: 27 min 33 sec
Exception

Exception - An unexpected error has occurred. Please check the execution log.

3. To send in the report, press **Send Error Report**
4. Fill in your information and add as many details as you can before pressing Send such as:

- 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.

### 12.8.11 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](https://devolutions.sharefile.com/filedrop).
12.8.12 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.

2. Select the Report tab. Then click on the Send to Support button.

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.
12.8.13 How to Send your Configuration File

Description

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.

Workflow

1. Go in File – Options and press the Export Options button. Remove any sensitive information's and save the file on your computer. The file name will be RemoteDesktopManager.cfg.

2. Please send us the file securely via https://devolutions.sharefile.com/filedrop

12.8.14 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.

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.
Set up the properties as follows:

### SSH Server Settings

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Set the IP address of the SSH Server. (please refer to 1 in the Tunnel diagram)</td>
</tr>
<tr>
<td>Port</td>
<td>Set the port of the SSH Server. The default port is 22. (please refer to in the Tunnel diagram)</td>
</tr>
<tr>
<td>Set public key</td>
<td>Setup the public key</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the SSH server username to connect.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the SSH server password to connect.</td>
</tr>
</tbody>
</table>

### Outgoing Tunnel Settings

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Select between: Local, Remote or Dynamic.</td>
</tr>
<tr>
<td>Local address</td>
<td>The local address must be left to 127.0.0.1. (please refer to ① in the Tunnel diagram)</td>
</tr>
<tr>
<td>Local port</td>
<td>In most cases leave the local port to its default value 3390. (please refer to ② in the Tunnel diagram)</td>
</tr>
<tr>
<td>Remote host</td>
<td>Enter the host or IP address of your remote client. (please refer to ③ in the Tunnel diagram)</td>
</tr>
<tr>
<td>Remote port</td>
<td>Set the final port that you must reach, in most cases leave it to it's default value 3389. (please refer to ④ in the Tunnel diagram)</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Enter your <strong>Local address</strong> which is 127.0.0.1. (please refer to ① in the Tunnel diagram)</td>
</tr>
<tr>
<td>Port</td>
<td>Enter your <strong>Local port</strong> which is 3390. (please refer to ② in the Tunnel diagram)</td>
</tr>
<tr>
<td>RDP type</td>
<td>Leave the RDP type to Normal.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username of your Remote Host.</td>
</tr>
<tr>
<td>Domain</td>
<td>Enter the domain of your Remote Host.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password of your Remote Host.</td>
</tr>
</tbody>
</table>

In the **VPN/SSH/Gateway** side menu of your RDP session select **Always connect** in the **Open** field and **Session** in the **Type** field.
In the **VPN – Settings** tab, click on the drop down list next to **Session** and select your **SSH Tunnel** entry previously created.
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.
12.8.15 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.

![Remote Desktop Manager Application Start Settings](image)

2. Subscribe to the Announcements Forums to be aware of all the latest announcements on our products.

12.8.16 How to 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.
We also recommend that you configure your Default Settings of the entry type that need this setting by default.

### 12.8.17 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/](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](https://forum.devolutions.net/forum20-remote-desktop-manager--announcements.aspx)

After, click on **Watch this forum for new topics**.
The procedure is the same for all forums, below are the Announcement forums that exist at this time for our various products.

- Remote Desktop Manager MAC: https://forum.devolutions.net/forum43-remote-desktop-manager-mac--announcements.aspx
- Devolutions Cloud: https://forum.devolutions.net/forum31-remote-desktop-manager-online--announcements.aspx
- Devolutions Password Server: https://forum.devolutions.net/forum32-remote-desktop-manager-server--announcements.aspx
- Wayk Now: https://forum.devolutions.net/forum68-wayk-now--announcement.aspx

12.8.18 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.

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.
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.

12.8.19 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.

12.8.19.1 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
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
SessionIntelAMTLarge.png
SessionIntelAMTSmall.png
SessionInventoryReportLarge.png
SessionInventoryReportSmall.png
SessionItermLarge.png
SessionItermSmall.png
<table>
<thead>
<tr>
<th>SessionLogMeInLarge.png</th>
</tr>
</thead>
<tbody>
<tr>
<td>SessionLogMeInSmall.png</td>
</tr>
<tr>
<td>SessionPCAnywhereLarge.png</td>
</tr>
<tr>
<td>SessionPCAnywhereSmall.png</td>
</tr>
<tr>
<td>SessionPlayListLarge.png</td>
</tr>
<tr>
<td>SessionPlayListSmall.png</td>
</tr>
<tr>
<td>SessionPowerShellLarge.png</td>
</tr>
<tr>
<td>SessionPowerShellSmall.png</td>
</tr>
<tr>
<td>SessionPuttyLarge.png</td>
</tr>
<tr>
<td>SessionPuttySmall.png</td>
</tr>
<tr>
<td>SessionRDPConfiguredLarge.png</td>
</tr>
<tr>
<td>SessionRDPConfiguredSmall.png</td>
</tr>
<tr>
<td>SessionRadminLarge.png</td>
</tr>
<tr>
<td>SessionRadminSmall.png</td>
</tr>
<tr>
<td>SessionRemoteAssistanceLarge.png</td>
</tr>
<tr>
<td>SessionRemoteAssistanceSmall.png</td>
</tr>
<tr>
<td>SessionS3Large.png</td>
</tr>
<tr>
<td>SessionS3Small.png</td>
</tr>
<tr>
<td>SessionSNMPReportLarge.png</td>
</tr>
<tr>
<td>SessionSNMPReportSmall.png</td>
</tr>
<tr>
<td>SessionScreenConnectLarge.png</td>
</tr>
<tr>
<td>SessionScreenConnectSmall.png</td>
</tr>
<tr>
<td>SessionSessionToolLarge.png</td>
</tr>
<tr>
<td>SessionSessionToolSmall.png</td>
</tr>
<tr>
<td>SessionSkyDriveLarge.png</td>
</tr>
<tr>
<td>SessionSkyDriveSmall.png</td>
</tr>
<tr>
<td>SessionSpiceworksLarge.png</td>
</tr>
<tr>
<td>SessionSpiceworksSmall.png</td>
</tr>
<tr>
<td>SessionSyncLarge.png</td>
</tr>
<tr>
<td>SessionSyncSmall.png</td>
</tr>
<tr>
<td>SessionTeamViewerLarge.png</td>
</tr>
<tr>
<td>SessionTeamViewerSmall.png</td>
</tr>
<tr>
<td>SessionTerminalConsoleLarge.png</td>
</tr>
<tr>
<td>SessionTerminalConsoleSmall.png</td>
</tr>
<tr>
<td>SessionVMRCLarge.png</td>
</tr>
<tr>
<td>SessionVMRCSmall.png</td>
</tr>
<tr>
<td>SessionVMWareConsoleLarge.png</td>
</tr>
<tr>
<td>SessionVMWareConsoleSmall.png</td>
</tr>
<tr>
<td>SessionVMWareLarge.png</td>
</tr>
<tr>
<td>SessionVMWareSmall.png</td>
</tr>
<tr>
<td>SessionVNCLarge.png</td>
</tr>
<tr>
<td>SessionVNCSmall.png</td>
</tr>
<tr>
<td>SessionVPNLarge.png</td>
</tr>
<tr>
<td>SessionVPNSmall.png</td>
</tr>
<tr>
<td>SessionVirtualBoxLarge.png</td>
</tr>
<tr>
<td>SessionVirtualBoxSmall.png</td>
</tr>
<tr>
<td>SessionVirtualPCLarge.png</td>
</tr>
<tr>
<td>SessionVirtualPCSsmall.png</td>
</tr>
<tr>
<td>SessionWebBrowserLarge.png</td>
</tr>
<tr>
<td>SessionWebBrowserSmall.png</td>
</tr>
<tr>
<td>SessionWindowsVirtualPCLarge.png</td>
</tr>
<tr>
<td>SessionWindowsVirtualPCSsmall.png</td>
</tr>
<tr>
<td>SessionXWindowLarge.png</td>
</tr>
<tr>
<td>SessionXWindowSmall.png</td>
</tr>
</tbody>
</table>
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.

### 12.8.20 PowerShell

**Description**

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:
12.8.2.1 Extract TeamViewer ID

**Description**

You can use Powershell to extract the TeamViewer ID from a session.

**Settings**

Here a script to extract the TeamViewer ID from a session:

```powershell
$sessions = Get-RDM-Session | where {$_._Session.Kind -eq "TeamViewer"}
$sessions[0].Session.GetProperty("TeamViewer", "ID")
```

12.8.2.2 Custom Export to CSV

**Description**

Many customers ask for a special export that would contain specific fields.

**Settings**

Here is a small script that can be used to generate URLs for our new web protocol handler. We generate a csv file that contains the name and the URL.

```powershell
## 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 "RDPConfigured"} |
   foreach {
       new-Object Object |
       Add-Member NoteProperty Name $_._Name -PassThru |
       Add-Member NoteProperty URL "rdm://open?DataSource=$dsid&Session=$($_._ID)" -PassThru
   };
## save to csv, the field names are used as column headers.
$s | export-csv c:\temp\sessions.csv -notypeinformation;
```
12.8.20.3 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

12.8.20.4 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 session that is running with elevated privileges (using Run As Administrator).

12.8.20.5 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).
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)*.
4. Select the **Custom Powershell Command**.
5. Write the following line for your Powershell Command:

```powershell
$connection.CreationSource = "enter synchronizer ID number"
$RDM.Save();
```
12.9 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.

12.9.1 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.
### 12.9.2 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: `dhcpmgmt.msc /ComputerName $HOST$` ($HOST$ is the variable that will be replaced by the server name or IP address).
5. Select **Run as Administrator** in the **Execution Mode** tab.

   ![DHCP Macros/Scripts/Tools](image)

   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

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use default credentials</td>
<td>Use the credentials from the Windows session</td>
</tr>
<tr>
<td>Use session credentials</td>
<td>Use the same credentials as the session</td>
</tr>
<tr>
<td>Prompt for credentials</td>
<td>Prompts for the credentials on use.</td>
</tr>
<tr>
<td>Custom credentials</td>
<td>Use the Username, Password and Domain specify</td>
</tr>
<tr>
<td>Credential repository</td>
<td>Specify a set of credentials from the repository</td>
</tr>
<tr>
<td>Use my personal credentials</td>
<td>Use <a href="#">My Personal Credentials</a></td>
</tr>
</tbody>
</table>

To run the Snap-In, select your session and execute the tool from the dashboard.
12.9.3 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)**.
2. Enter a password to create a password protected zip file.
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.
12.9.4 Creating Shortcuts

Overview

There are 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.

Creating a Shortcut: Option 1

One way to create a shortcut is by using the menu Edit -> Create Shortcut...
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.

12.9.5 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.
2. Select **File – Export – Export All (.rdm)**.
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.
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.

3. In the **Import Entries** dialog use the ellipsis button to browse for the data file exported in the previous section.
Remote Desktop Manager

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import in root</td>
<td>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.</td>
</tr>
<tr>
<td>Import in current folder</td>
<td>Import all your entries under the selected folder of the data source.</td>
</tr>
</tbody>
</table>

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.
12.9.6 Data Report

Description

The Data Report session type can be used to empower any/all users to generate reports, without having to grant them access to the actual server.

Settings

General
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**
Data Report Session - Parameters Tab

Specify the parameters by setting the name, type and default value of all parameters.

Query

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.

12.9.7 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 then 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](image)

2. In the **Advanced** tab, check the **Run as Administrator** option.
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.
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.

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
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.

### 12.9.8 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.

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.

12.9.9 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:

| 967 |

**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.

**12.9.10 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.

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.
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.
12.9.11 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.

![Connection Tab](image)

12.9.12 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.
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!

---

### 12.9.13 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).

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set time limit for disconnected sessions</td>
<td>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.</td>
</tr>
<tr>
<td>Set time limit for active but idle Remote Desktop Services sessions</td>
<td>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.</td>
</tr>
<tr>
<td>Set time limit for active Remote Desktop Services sessions</td>
<td>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.</td>
</tr>
<tr>
<td>End session when time limits are reached</td>
<td>This policy setting specifies whether to end a Remote Desktop Services session that has timed out instead of disconnecting it.</td>
</tr>
</tbody>
</table>

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.
**12.9.14 Remote Install with PSEexec**

**Description**

When you need to perform a remote installation, you have multiple options. Such as a domain policy, a logon script or PSEexec.

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 PSEexec 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 PSEexec.exe in the execution of this script. ([https://technet.microsoft.com/en-us/sysinternals/bb842062](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 PSEexec documentation for further details.

**Settings**

1. Create a **Macros/Scripts/Tools** entry, use the **PSEexec** type. In the Command line section, add the following (long) line:

   C:\Tools\Sysinternals\psexec.exe \\$HOST\$ -i -u $TOOL_DOMAIN\$TOOL_USERNAME$ -p $TOOL_PASSWORD$ cmd /k "msiexec /i \SRV-DEPLOY\msi\Setup.RemoteDesktopManager.10.9.0.0.msi /quiet /passive /norestart"

   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 PSEexec.

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.

12.9.15 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.

---

**Settings**

In Windows you can manually start any process as a different user using **SHIFT + right-click** to get the context 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 need help to manually configure Run As? See the [Manual Run As](#) help topic.

### 12.9.15.1 Built-in RunAs

#### Description

This article describes the built in method of using Run As. For sessions 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.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session</td>
<td>· Command Line&lt;br&gt;· PowerShell</td>
</tr>
<tr>
<td>Macros/Script s/Tools</td>
<td>· Command Line&lt;br&gt;· PowerShell Local&lt;br&gt;· PowerShell Remote&lt;br&gt;· PSEexec</td>
</tr>
<tr>
<td>Session Add- on</td>
<td>· SQL Server Management Studio</td>
</tr>
</tbody>
</table>

**Session**
Sessions that support Run As will have a Run As tab where you specify which credentials to use when starting with Run As.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No Run As is performed.</td>
</tr>
<tr>
<td>Current session</td>
<td>Use the same credentials as defined in the session.</td>
</tr>
<tr>
<td>Custom credentials</td>
<td>Use specified custom credentials.</td>
</tr>
<tr>
<td>Credential repository</td>
<td>Use a link credential entry.</td>
</tr>
<tr>
<td>Use my personal credentials</td>
<td>Use a link private credential entry.</td>
</tr>
</tbody>
</table>

**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.
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.
Click on **Run as different user** to modify the **Run As** settings.

**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**.
3. Specify the **Run As** credentials.

4. Save your session.

5. Run your Command Line session.

```
C:\Users\deno\AppData\Local\whoami\devolutions18\demo
C:\Users\deno\AppData\Local\pause
Press any key to continue . . .
```
12.9.15.2 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,
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.

![Remote Desktop Manager](image)

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](#).

![Remote Desktop Manager](image)
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**

The 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\$USERNAMES`, 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)

5. 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: \texttt{\$PASSWORD\$\{ENTER\}}. For more information please consult \texttt{Auto Typing Macro}.  

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{image}
\caption{Typing macro settings in the Events tab.}
\end{figure}
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.

12.9.16 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 your username is entered as your 
infrastucture 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**.

You are presented with a logon form in which you must specify the username and password.

![Run as different user](image)

**12.9.17 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`.

Select the `Microsoft SQL Server` data source and click `OK`. 
- Specify the **Name**, **Server** and **Database**
- Authenticate with a user that is part of the **sysadmin** role.
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.
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](image)

**Create users**

To create users, navigate to *Administration – Users*.

![Administration - Users](image)

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.

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.

12.9.18 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!

12.9.19 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.
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.

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.
12.9.20 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.
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 confidentially 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](image)

**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 Server delivers all that and much more!

You deploy **Devolutions 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/](http://server.devolutions.net/)

**12.9.21 Testing variables**

**Description**

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`

```bash
@echo off
echo.
echo.
echo %*
echo.
echo.
pause
```

Now it's 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.**

### 12.9.22 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`

### 12.9.23 VPN

#### 12.9.23.1 VPN Group

**Overview**

VPN groups are defined inside each individual entries 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.
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.

### 12.9.23.2 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.

```plaintext
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       Use Interface
 0.0.0.0              0.0.0.0      192.168.1.1   192.168.1.1
10.1.2.5 255.255.255.255 0.0.0.0      100.77.183.56 On-link
127.0.0.0 127.0.0.1 255.255.255.255 0.0.0.0      On-link
127.255.255.255 255.255.255.255 0.0.0.0      On-link
10.1.168.1 255.255.255.0 0.0.0.0      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.
**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.
12.10 Tools

12.10.1 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](image)

**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.

**12.11 Troubleshooting**

**12.11.1 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.

### 12.11.2 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.
12.11.3 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 -boolYES
```

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 -boolNO
```

12.11.4 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](https://www.beyondtrust.com) entry, make sure that you have entered the appropriate key. Please refer to the [BeyondTrust Password Safe Console](https://www.beyondtrust.com) 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.

### 12.11.5 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.
12.11.6 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.

![Warning]

Running those tools may take a long time.


12.11.7 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.

![Error]

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.

![Error]

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.

12.11.8 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.

<table>
<thead>
<tr>
<th>ISSUE</th>
<th>RESOLUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Virus</td>
<td>Set the AV to ignore Remote Desktop Manager, you could also exclude our local configuration folder.</td>
</tr>
<tr>
<td>Firewall blocks RDM - all the time</td>
<td>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.</td>
</tr>
<tr>
<td>Firewall blocks RDM - specific network</td>
<td>The firewall rules are tied to the category of the network profile (Public/Private/DomainAuthenticated), ensure that all your network profiles allow for connectivity. Use netsh interface ip show interfaces and Set-NetConnectionProfile for resolution.</td>
</tr>
</tbody>
</table>
12.11.8.1 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.**

2. In the tab **Upgrade** click on **Email Schema to Support.**
3. Fill in all the requested information and click on OK.
### OPTION | DESCRIPTION
--- | ---
Email | Enter your email address 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

---

### 12.11.8.2 Devolutions Online Database

**Description**

**The user is disabled!**

When attempting to connect to the data source, you receive the error message below;

![Remote Desktop Manager](image)

**DODB User Disabled**

On [https://cloud.devolutions.net](https://cloud.devolutions.net) in the User section, please ensure that the User is indeed Enabled.

![Cloud Portal - Users](image)

---

### 12.11.8.3 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.
Erase the Value of the CacheServerProperties field.

12.11.8.4 SQL Azure

Issues

"Unable to load adalsql.dll (Authentication=ActiveDirectoryPassword). Error code: 0x2. For more information, see http://go.microsoft.com/fwlink/?LinkID=513072"

When attempting to use a SQL Azure data source, you receive the error message below:

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;

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.

12.11.8.5 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

12.11.8.5.1 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.


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 is 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 user has that error message, you must check privileges for ALL the AD groups that he belongs too. Anything with an explicit DENY must be evaluated carefully. The query below will help identify these occurrences.

```sql
select princ.*, perm.* from sys.server_principals princ, sys.server_permissions perm
where perm.grantee_principal_id = princ.principal_id
```
Login failed. The login is from an untrusted domain and cannot be used with windows authentication.

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 *.pkb 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.

![Error Message](image)

These steps are for Client side troubleshooting exclusively. For full guidance on this issue please consult [this article on Technet](https://technet.microsoft.com).

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). | Universal Data Link (.udl) file
Only server name is specified when there is no Default instance on that server. | Universal Data Link (.udl) file
Is the SQL Server up and running. | Universal Data Link (.udl) file
SQL Server is listening on a non-standard port. | Universal Data Link (.udl) file
Anti-Virus blocking Remote Desktop Manager. | Check in the Anti-Virus logs to see blocked threats.
Firewall is preventing Remote Desktop Manager to connect. | Adjust your firewall to allow RemoteDesktopManager.exe and RemoteDesktopManager64.exe to communicate with external services.

### 12.11.8.5.2 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.

```sql
exec sp_spaceused
```

### 12.11.9 DB Upgrades

**Error**

`SqlException - 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.

### 12.11.10(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:

```xml
<configuration>
  <runtime>
    <enforceFIPSPolicy enabled="false"/>
  </runtime>
</configuration>
```

### 12.11.1 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).

### 12.11.12 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.

12.11.13 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}\DocObject]

[HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{CF4F55F4-8F87-4D47-80BB-5808164BB3F8}\DocObject]

[HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{00021A15-0000-0000-C000-000000000046}\DocObject]

[HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{74B78F3A-C8C8-11D1-BE11-00C04FB6FAF1}\DocObject]

12.11.14 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".

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.

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.
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.
To fix this issue, go in **Properties – General – Advanced** and change the option **Enable CredSSP support** to **True**.

**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 login.

**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.
Network Level Authentication

We have discovered that enabling the **Public Mode** option in the **Advanced** tab resolves the issue.

**The connection was denied because the user account is not authorized for remote login**

See also: [Network Level Authentication](#), [Configure NLA for Remote Desktop Services Connections](#).
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.
Storing your Password

Ensure that "Always ask password" is not checked.
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.

<table>
<thead>
<tr>
<th>APPLIES TO</th>
<th>LINK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2012</td>
<td>The settings are on the Session Collection Properties. More info on the new Remote Desktop Services: Guide to configure the Quick Deployment; Test Lab Guide: Remote Desktop Services Session Virtualization Quick Start</td>
</tr>
</tbody>
</table>
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](image)

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.

12.11.14. 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.

12.11.14. 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.

**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;

Simply set this option as shown below in the properties of your RDP session under the **Display** tab.

### 12.11.14. 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](https://support.microsoft.com/en-us/help/2923545/update-for-rdp-8-1-is-available-for-windows-7-sp1)

### 12.11.14. Licensing Protocol Error

**Description**

When you connect to a remote workstation, you receive one of the errors below.
Solution


2. Depending on your Windows architecture (32-bit or 64-bit) delete the specified registry key(s):

<table>
<thead>
<tr>
<th>WINDOWS</th>
<th>REGISTRY KEY(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>32-bit</td>
<td>HKLM\SOFTWARE\Microsoft\MSLicensing</td>
</tr>
<tr>
<td>64-bit</td>
<td>HKLM\SOFTWARE\Microsoft\MSLicensing</td>
</tr>
<tr>
<td></td>
<td>HKLM\SOFTWARE\Wow6432Node\Microsoft\MSLicensing</td>
</tr>
</tbody>
</table>

3. Run Microsoft RDP (mstsc.exe) as an administrator to recreate the registry key (just once).

4. Restart Remote Desktop Manager.

12.11.14. 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 Terminal 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 terminal service (Remote Desktop) 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.

12.11.14. 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 'ashutdown /l' instead of 'shutdown /l'. It does this in both the Free and Enterprise version.

Solution

Simply check this option in File -> Options -> Types -> RDP.

12.11.14. 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.
12.11.14. 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.
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.
12.11.14.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.

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.


Errors
Because of a protocol error, this session will be disconnected. Please try connecting to the remote computer again.

**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.

**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.

12.11.14. 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;
12.11.14. 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.

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.

12.11.14. 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](image)

12.11.14.RD Gateway Credentials Prompt When Trying To Reconnect

Description

This problem happen 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.
12.11.14. 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.
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.

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](https://docs.microsoft.com/en-us/windows-server网球 Anna/s/remote-desktop/servers/remote-desktop-firewall-udp-settings) 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.

12.11.14. 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
12.11.1 | 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.
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.

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.

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.

```powershell
[CmdletBinding()]
Param(
    [Parameter(Mandatory=$True,Position=1)]
    [string]$PMPServer,
    [Parameter(Mandatory=$True,Position=2)]
    [string]$AuthToken
)

add-type @"using System.Net;
public class TrustAllCertsPolicy : ICertificatePolicy {
    public bool CheckValidationResult(
        ServicePoint srvPoint, X509Certificate certificate,
        WebRequest request, int certificateProblem) {
        return true;
    }
}
"
```

© 2019 Devolutions inc.
"@hotmail.com",
$connect = "https://" + $PMPServer + ":7272/restapi/json/v1/resources?AUTHTOKEN=$AuthToken
$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.

```powershell
.\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.

2. Find the Remote Desktop Manager **Configuration File**.
3. Edit the configuration file and add the line
   ```xml<br>     <ResolvePMProURLIntoIPAddress>false</ResolvePMProURLIntoIPAddress><br>   </xml>
```
4. Save the modification and restart the application.

### 12.11.17 Performance

#### 12.11.17.1 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**.

**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.
12.11.17. 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 or information that the support team requires to help diagnose your issue.

Procedures

My Data Source Information
1. Open **File – My Data Source Information**.
2. 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.

---

<table>
<thead>
<tr>
<th>ID</th>
<th>Server</th>
<th>Database</th>
<th>TCP</th>
<th>v1.523</th>
<th>JaJafDen</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is DB owner</td>
<td>✓</td>
<td>Is System DBA</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Offline mode</td>
<td>64.0 KB</td>
<td>Read/write</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group Policy settings</td>
<td>Read/write</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System settings</td>
<td>Read/write</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User settings</td>
<td>Read/write</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data source config</td>
<td>Intelligent</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vault</td>
<td>Allow offline</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vault</th>
<th>Default</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>General</th>
<th>Entries</th>
<th>Security Groups (Legacy)</th>
<th>Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database user</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>hehesa</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Is administrator | ✓ |
| Allow offline mode | ✓ |
| Allow drag-and-drop | ✓ |
| Is Auto Refresh | ![Alert] |
| Auto refresh interval | 0 sec |
| Is Two Factor Configuration | ![Alert] |
# Diagnostic

Open **Help – Diagnostic**.

2. 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**

1. Open **Help – Profiler**, move the window aside to clear the main window of Remote Desktop Manager.
2. Select the **Performance** tab.
3. In Remote Desktop Manager, hold the CTRL key and press the refresh button.
4. Information will be added in the **Performance** tab.
5. 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.

**12.11.17. Startup**

**Description**

The start-up performance of the application can be affected by two main events:

1. launching the "shell"
2. 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.

**12.11.18. 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).

**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**.
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.
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):

```powershell
```

If there are more than one version of the snap-in installed, the result of the command will list them like this:

```powershell
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
```

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.

```powershell
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> Remove-PSSnapin -Name Remote.Desktop.Manager.11.0.17
PS C:\devolutions\RDM 11.0.18.0> Remove-PSSnapin -Name Remote.Desktop.Manager.11.0.18
```

Finally, verify if only the snap-in of the current version of RDM is installed with the `Get-PSSnapin` command.

```powershell
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);

```bash
Set-ExecutionPolicy
```


2. Open Remote Desktop Manager as Administrator and open the Powershell module and run;

```bash
Set-ExecutionPolicy
```

**12.11.1 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.

**12.11.2 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`
12.11.20. 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.

Method 3
You can manage the local cache by doing a Vacuum, a Repair or a Delete. Please consult Manage Cache topic for more information.

12.11.20. 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.

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

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.
9. Package the *.log, *.log.db and *.debug files from your configuration folder and send them to us.

12.11.20. High CPU Usage

Description
Since the release of Remote Desktop Manager 13, some users have experienced high CPU usage on their systems, especially in Terminal Services / 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]

**12.11.20. 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.”
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, "

```xml
<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)

Remote Desktop Manager Properties

- Run compatibility troubleshooter
- How do I choose compatibility settings manually?
  - Compatibility mode:
    - Run this program in compatibility mode for:
      - Windows 8

Settings:
- Reduced color mode
- 8-bit (256) color
- Run in 640 x 480 screen resolution
- Disable display scaling on high DPI settings
- Run this program as an administrator

Change settings for all users

DPI Settings

Windows 10 Creators Update (Build 15063 and above)
12.11.20. 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.

12.11.20.5.1 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.exe"
```

If the application becomes unresponsive, the tool will handle everything. Simply locate the dump file and send it to us.

**12.11.20.6 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.

Instructions

**Windows XP/Server 2003**

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.

**12.11.20.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

### 12.11.20.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

12.11.20. 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`. 
Close Remote Desktop Manager, delete the `offline.db` file and restart Remote Desktop Manager. This will force the application to recreate the offline file.

### 12.11.20. Profiler

#### Description

Please consult the [Profiler](#) topic for more information.

### 12.11.20. Root Is Empty Error

#### Description

After upgrading to Remote Desktop Manager 13.5.x, you may receive the error below;

```csharp
RootException - Root is empty!
at Devolutions.RemoteDesktopManager.Managers.RootConnectionManager.get_RootConnection()
at Devolutions.RemoteDesktopManager.Frames.ConnectionViews.FreConnectionTreeListTreeView.ce5f4c5875531b613e87da05d31ef0d852(ConnectionViewMode cfa8984eaceb595fb57911c4e0ee96824)
at Devolutions.RemoteDesktopManager.Frames.ConnectionViews.FreConnectionTreeListTreeView.LoadConnectionList(Connection[] connections, ConnectionViewMode viewMode)
at Devolutions.RemoteDesktopManager.Forms.FrmMainRibbonBase.LoadAllConnectionView(Boolean saveState)
at Devolutions.RemoteDesktopManager.Forms.FrmMainRibbonBase.RefreshAllConnectionView(Boolean saveState, Boolean checkOnline)
at Devolutions.RemoteDesktopManager.Managers.MainFormManager.DoFirstLoad(IMainForm mainform)
at Devolutions.RemoteDesktopManager.Forms.FrmMainDocumentManager.cae3b4c7c167cf0d97474c4feee11ac00a(Object c19f1856d70c3e696ba148af1c4af54, EventArgs cf10188337debd818319fd3cb48a4e)
at System.Windows.Forms.Timer.OnTick(EventArgs e)
```

#### 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.

12.11.20. 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](image)

12.11.20. 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:

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>', '')
```

**12.11.20. 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:

```xml
<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/enterprisenews`. 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.

```
<WebBrowserScriptErrorsSuppressed>true</WebBrowserScriptErrorsSuppressed>
<DisableAnalytics>true</DisableAnalytics>
```

**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.

### 12.11.20. 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](https://remotedesktopmanager.com/Home/Download).

### 12.11.20. 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.

12.11.20.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:

![Event Log Message]

#### Step 1


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 for further assistance.

12.11.20.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.
The main form layout is broken

Use the Reset Layout option to revert back to the default UI layout in the Window tab.

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

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.

### 12.11.20. Unable to communicate with Password Vault Manager

#### Error

**Unable to communicate with Password Vault Manager, please verify it's started and that the database is opened!**:

When trying to retrieve a credential using your Password Vault Manager credential entry in Remote Desktop Manager, the loading times out and you receive the following error message;

![Error Dialog](image)

#### Solution

Please follow the steps below to resolve this.

2. Navigate to \%LOCALAPPDATA%\Devolutions\RemoteDesktopManager

3. Edit the file RemoteDesktopManager.cfg with a file editor.

3. Add the following line in the Configuration File:

   <EnsurePasswordVaultManagerPresent>false</EnsurePasswordVaultManagerPresent>

4. Save the file & restart Remote Desktop Manager. You should now be able to successfully communicate with Password Vault Manager.

**12.11.20 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.

**12.11.21 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
12.11.2 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
    $result2.SecretSummaries | ForEach-Object { Write-Host 'SecretId:' $_.SecretId '  Name:' $_.SecretName  ' FolderId:' $_.FolderId }
    # If you want the data as XML
    # $xml = convertto-xml $result2.SecretSummaries -As string -Depth 20
    # $xml
}
```
12.11.2 Secure Note

**Error**

The text in a SecureNote is not displayed properly.

Change the IE emulation mode in **File – Options – Types – Web**, set the IE Mode to use Internet Explorer 10.

---

### 12.11.2 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.

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!

### 12.11.2 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;

![SSH Keypad mode]

### 12.11.26 Synchronizers

#### 12.11.26.1 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.


**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.

12.11.2 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

<table>
<thead>
<tr>
<th>STEP</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have you specified the Execution Policy of scripts?</td>
<td>Get-ExecutionPolicy</td>
</tr>
<tr>
<td>Have you configured the PowerCLI's InvalidCertificateAction?</td>
<td>Get-PowerCLIConfiguration</td>
</tr>
<tr>
<td>Have you configured the PowerCLI's DefaultVIServerMode?</td>
<td>Get-PowerCLIConfiguration</td>
</tr>
</tbody>
</table>

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:
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.

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.

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.

A Final test with the `Connect-ViServer` command, by typing it in PowerShell, the connection is established and the issue should be resolved.

**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:
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

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.

**12.11.27 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]

<table>
<thead>
<tr>
<th>Name</th>
<th>$<em>.</em>.Moref.Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MACHINE1</td>
<td>18</td>
</tr>
<tr>
<td>MACHINE2</td>
<td>19</td>
</tr>
</tbody>
</table>

Script B - :Launching the VMRC

ConnectVMRCFromPowerCLI.ps1
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.

```powershell
.\ConnectVMRCFromPowerCLI.ps1 [SERVER_NAME] [USER_NAME] [PASSWORD] 19
```

The VMRC should appear and allow you to interact with it.

**12.11.2 VPN**

**12.11.28. 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.

**12.11.28. FortiClient**

**Error**

The plugin of FortiClient is asking for the **FortiSSLVPNClien.exe** file, however with FortiClient 5.2.1 or higher, the file is not present in the installation folder.

**Solution 1**
Duplicate the Forticlient.exe file in the installation folder of Forticlient and rename it to FortiSSLVPNClient.exe. In Remote Desktop Manager, click on File – Options – Path to configure the appropriate folder path to retrieve FortiSSLVPNClient.exe.

**Solution 2**

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](#).

However, 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 need to be saved in the installation folder of FortiClient.

### 12.11.28.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.

### 12.11.28.Microsoft VPN

#### Description

These types of VPNs can use either the RASDIAL or RASPHONE applications for establishing the connection. Please consult [Microsoft's article](https://technet.microsoft.com/en-us/library/bb490979.aspx) on their differences and usage.

You can refer to this Microsoft TechNet article for more information on RASDIAL:


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**

Remote Access error 623 - The system could not find the phone book entry for this connection.

For more help on this error:
Type `\help\netcfg.chm` in help, click Troubleshooting, then Error Messages, then 623

Code:623

Ensure that within the phonebook, the vpn definition name does not 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.

**12.11.28.** Cisco AnyConnect

**Description**

The [Cisco AnyConnect](https://www.cisco.com) add-on doesn't send the proper information like the password or the group number to the `vpncil.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 `vpncil.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.

12.11.2 Web Browsers

12.11.29 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](image-url)
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](image)

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.

**12.11.29.** **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/](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/](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.
12.11.29 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.

12.11.29. Web Authentication

Description

For some websites, the auto fill function does not work out of the box. It requires some steps in order to properly send the username and password. Depending on the website, the process can be simple or may require additional tweaks.

Method 1
Automatically log in to a website

1. In the Login tab of the Web Browser entry, select the Form Authentication mode, and enter the credentials. Then, verify that the Autofill login and Auto submit options are enabled.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter the username to connect on the website.</td>
</tr>
<tr>
<td>Domain</td>
<td>Enter the domain to connect on the website.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password to connect on the website.</td>
</tr>
<tr>
<td>Autofill login</td>
<td>Automatically fills in the credential fields when opening the web page.</td>
</tr>
<tr>
<td>Autofill delay</td>
<td>Set a delay between opening the credential fields and attempting the auto submit feature.</td>
</tr>
<tr>
<td>Auto submit</td>
<td>Automatically submit the credentials and try connecting to the website.</td>
</tr>
</tbody>
</table>

2. 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.
3. 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, do a right-click inside the field and click on 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, an example of the inspection for the Username field;
12.11.3 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.

12.11.3 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**

```xml
<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*

```xml
<sharedListeners>
  <add
    name="MyTraceFile"
    type="System.Diagnostics.XmlWriterTraceListener"
    initializeData="System.Net.trace.svclog"
  />
</sharedListeners>
```

**12.11.3 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.
2. Go in **File -> Options -> User Interface** and uncheck **Show Welcome page at start-up**.
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.
12.11.3 WMI

Description

Here’s a primer on remote WMI:

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.


This is a lot of information to go over, please contact us at 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:
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
```

### 12.12 Tutorials

#### Description

Our tutorials are published on [Devolutions YouTube channel](https://devolutions.net). 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.

#### 12.12.1 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.
<table>
<thead>
<tr>
<th>OVERVIEW</th>
<th>DESCRIPTION</th>
<th>LINK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Register your Remote Desktop Manager license</td>
<td>A quick look at how to register your license in Remote Desktop Manager. The data sources are the heart of Remote Desktop Manager. Here is a quick overview of the most popular data sources that we support.</td>
<td></td>
</tr>
<tr>
<td>Register Remote Desktop Manager</td>
<td>A quick look at how to download Remote Desktop Manager and register your license key.</td>
<td></td>
</tr>
<tr>
<td>Remote Desktop Manager</td>
<td>A quick overview of Remote Desktop Manager. See how you can easily and securely centralize and consolidate all your remote connections, credentials and passwords.</td>
<td></td>
</tr>
<tr>
<td>Create Templates and Default Settings</td>
<td>A quick overview at how to execute and export multiple reports with the option of exporting reports through a command line.</td>
<td></td>
</tr>
<tr>
<td>Create Users and Assign Permission</td>
<td>Take a quick look at how to create users for your database and how to assign specific permission to each user.</td>
<td></td>
</tr>
<tr>
<td>Create a folder structure that reflects your organization</td>
<td>An overview at how to create a folder structure that will reflect your organizations.</td>
<td></td>
</tr>
<tr>
<td>Simplified Security</td>
<td>Learn how to create roles and permissions for a granular protection system using our Role Based Security System.</td>
<td></td>
</tr>
<tr>
<td>Choose your data source</td>
<td>An overview at our multiple data sources and how to select the proper one for you and your enterprise.</td>
<td></td>
</tr>
</tbody>
</table>

**12.12.2 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.
## Contents

<table>
<thead>
<tr>
<th>GETTING STARTED</th>
<th>DESCRIPTION</th>
<th>LINK</th>
</tr>
</thead>
<tbody>
<tr>
<td>KeePass</td>
<td>Learn how to perform the setup for the integration of KeePass with Remote Desktop Manager</td>
<td>![Watch Video](Watch Video)</td>
</tr>
<tr>
<td>LastPass</td>
<td>Learn how to use your own LastPass account to manage passwords in Remote Desktop Manager.</td>
<td>![Watch Video](Watch Video)</td>
</tr>
<tr>
<td>Remote Desktop Manager Jump</td>
<td>Learn how to perform the initial setup for allowing usage of Remote Desktop Manager Jump to connect to remote devices through a jump host.</td>
<td>![Watch Video](Watch Video)</td>
</tr>
<tr>
<td>Simplified Security</td>
<td>Learn how to create roles and permissions for a granular protection system using our Role Based Security System.</td>
<td>![Watch Video](Watch Video)</td>
</tr>
<tr>
<td>Remote Desktop Manager Step 1: Register your Data Source</td>
<td>Upon first launch learn how to create your first data source and your first database.</td>
<td>![Watch Video](Watch Video)</td>
</tr>
<tr>
<td>Remote Desktop Manager Step 2 Options for Team Environment</td>
<td>Learn how to set up your options to make your environment more fitting for teams.</td>
<td>![Watch Video](Watch Video)</td>
</tr>
<tr>
<td>Remote Desktop Manager Step 3: Default Settings</td>
<td>Taking a quick look at our options and what are the best default settings for your team environment before creating your entries.</td>
<td>![Watch Video](Watch Video)</td>
</tr>
<tr>
<td>Remote Desktop Manager Step 4: Getting Set Up</td>
<td>Learn how to create a folder structure that reflects your organization using Remote Desktop Manager best practices.</td>
<td>![Watch Video](Watch Video)</td>
</tr>
<tr>
<td>Remote Desktop Manager Step 5: How to create your entries</td>
<td>Learn how to create and manage your entries and also taking a quick look at Security Group Management.</td>
<td>![Watch Video](Watch Video)</td>
</tr>
<tr>
<td>Devolutions Server</td>
<td>Learn how to create and set up your Devolutions Server.</td>
<td>![Watch Video](Watch Video)</td>
</tr>
<tr>
<td>Devolutions Online Database</td>
<td>Learn how to can create your Devolutions Cloud account and get started setting up your Online Database.</td>
<td>![Watch Video](Watch Video)</td>
</tr>
</tbody>
</table>

### 12.12.3 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.
<table>
<thead>
<tr>
<th>SPOTLIGHT ON...</th>
<th>DESCRIPTION</th>
<th>LINK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Batch Edit</td>
<td>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.</td>
<td><img src="#" alt="Watch Video" /></td>
</tr>
<tr>
<td>Host and Templates</td>
<td>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.</td>
<td><img src="#" alt="Watch Video" /></td>
</tr>
<tr>
<td>Offline Mode</td>
<td>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.</td>
<td><img src="#" alt="Watch Video" /></td>
</tr>
<tr>
<td>Simplified Security</td>
<td>Learn how to create roles and permissions for a granular protection system using our Role Based Security System.</td>
<td><img src="#" alt="Watch Video" /></td>
</tr>
<tr>
<td>User Interface</td>
<td>Learn how to manipulate the user interface elements of Remote Desktop Manager and adapt it according to your preferences.</td>
<td><img src="#" alt="Watch Video" /></td>
</tr>
<tr>
<td>Execute Report through Command Line</td>
<td>Learn how to execute and export same reports multiple times by exporting reports through a command line.</td>
<td><img src="#" alt="Watch Video" /></td>
</tr>
</tbody>
</table>
Index

- 2 -
2FA  111, 115, 117, 118, 122, 1005

- B -
Bastion server  21

- C -
Citrix  71

- J -
Jump box  21
Jump server  21

- M -
MFA  1005
MSSQL  168

- P -
parameters  871
Password analyzer  573
Password strength  573

- R -
Remote Desktop Services
  RDS  71
RemoteApp  71

- S -
Service host  21
Silent install  40

- T -
two-factor  1005

- U -
Unattended  40
update  74
Contact Us
For any questions, feel free to contact us:
Support: support@devolutions.net
Skype: support.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