



Remote Desktop Manager

USER MANUAL

Version 9.1

Table of Contents

Foreword	0
Part I Getting Started	14
1 What is Remote Desktop Manager?.....	14
2 System Requirements.....	14
3 Main Screen.....	15
4 Creating a New Entry.....	17
5 Configuring an Entry.....	19
6 Establishing a Connection.....	20
7 Security.....	21
Part II Installation	25
1 Client.....	25
Overview	25
Configuration File Location	25
Portable (USB)	26
Terminal Services	29
Custom Installer Service	30
Activate Custom Installer Subscription (Register)	30
Create an Installation Package.....	31
Installer File Generation.....	40
Registration	41
Register Enterprise Edition.....	41
Register Standard Edition.....	42
2 Database.....	43
Upgrade	43
3 Others.....	45
Add-ons	45
Configure SQL Server	45
Embedded Firefox	46
KeePass Plug-in	47
4 Uninstall.....	50
Part III Commands	52
1 File	52
Master Key	52
Go Offline/Online	52
My Data Source Information	53
Online Services	56
Backup	56
Serial Vault.....	60
Data Sources	63
Overview	63
Import	66

Overview	66
Import Sessions	68
Import Logins	69
Import Contacts	71
Export	72
Overview	72
Encrypted Html	74
Options	75
Overview	75
General	75
General	75
Application Start	77
Application Close	78
Notification	79
Proxy	80
Quick Connect	81
User Interface	82
User Interface	82
Dashboard	83
Filter	84
Keyboard	85
Navigation Pane	87
Trayicon/Taskbar	88
Tree View	89
Title Bar	91
Type	92
Type	92
RDP	93
SSH/Telnet	94
Web	95
Others	97
Custom Variables	98
Security	99
Tools	102
Path	104
Advanced	107
Export Options	109
Templates	111
Templates	111
My Personal Credentials	116
Default Settings	117
2 Home	120
Overview	120
Connect	121
Macros	122
Clipboard	122
VPN	124
View	124
Tools	126
Password History	128
Entry History	129
3 Actions	132
Overview	132

Connect	133
Actions	133
Commands	134
Overview	134
RDP	134
VNC	135
SSH Shell	136
Telnet	137
Layout	138
Settings	139
Edit	140
Screenshot	140
4 Edit	141
Batch Edit	141
Shortcut/Linked Entries	148
User Specific Settings	149
Credential Entry Overriding	154
Credentials	154
Display	156
Screen Size	157
Default Browser	158
Keyboard	159
Gateway	160
Local Machine Specific Settings	162
Settings	165
General	165
Display Mode	165
Security	170
Credentials	170
More	171
Description	171
Keywords/Tags	173
Alternate Host	174
Tab Page Category/Color	174
VPN	176
Overview	176
Link To Existing Session	179
Post/Pre VPN Commands	180
Sub Connections	184
Overview	184
Information	185
General	185
Hardware	187
Contact	188
Purchase	189
Notes	190
Custom Fields	191
Statistics	192
Events	193
Connection Events	193
Auto Typing Macro	195
Attachments	198
Overview	198
Logs	199

Options	199
View Logs	201
Log Details	202
Tools	205
Overview	205
Intel® AMT	207
Advanced.....	209
Overview	209
Variables	211
5 View.....	220
Panels	220
View	220
Logs	221
Usage Logs (Local).....	221
Usage Logs (Global).....	222
Layout	223
Footer	223
Play List	223
Actions	224
Management.....	229
Default at Startup.....	232
ToDo List	234
Actions	234
Search	236
Export	236
6 Administration.....	237
Data Source Settings	237
Security Providers	241
User Management	244
Integrated Security.....	247
Permissions.....	248
Security Group Management	250
Role Management	250
Deleted Entries	252
Reports	253
Credential Report.....	253
Entry Information Report.....	254
Entry List Report.....	256
Entry Status Report.....	257
Expired Entry List Report.....	258
Security Group Report.....	258
VPN Reference Report.....	259
Connecting External System	260
Refactoring	262
Extract	262
Convert To.....	263
Template	264
Sub Connection.....	265
Tools	265
Add-on Manager.....	265
Macro/Script/Tool Manager.....	268
Translation Manager	269
Localizer	270

Remote Desktop Manager Server Console.....	271
PowerShell CmdLets.....	272
Close-RDM-Session.....	273
Get-RDM-DataSource.....	274
Get-RDM-Domain.....	275
Get-RDM-Passw ord.....	275
Get-RDM-Property.....	276
Get-RDM-Session.....	277
Get-RDM-UserName.....	278
New -RDM-Session.....	279
Open-RDM-Session.....	280
Remove-RDM-Session.....	281
Set-RDM-DataSource.....	282
Set-RDM-Domain.....	282
Set-RDM-Passw ord.....	283
Set-RDM-Property.....	284
Set-RDM-Session.....	286
Set-RDM-UserName.....	287
Passw ord Generator.....	288
SSH Key Generator.....	291
Passw ord Analyzer.....	293
Local RDP/RemoteApp Manager.....	294
Macros/Scripts/Tools.....	300
Overview	300
Wake-on-LAN	301
Window	303
Overview	303
Header	304
Window s.....	305
Tree View	306
Help	306
Application Logs	306
Diagnostic.....	308

Part IV Data Sources

311

1 Overview.....	311
Data Source Types	313
Import/Export Data Source	316
Lock Data Source	317
Caching	318
Offline	319
Offline Read/Write.....	320
2 Types.....	322
Amazon S3	322
Settings	322
Dropbox	324
Settings	325
FTP	326
Settings	327
SFTP	331
Settings	332
Microsoft Access	335
Settings	336

SQLite	338
Settings	339
MariaDB	342
Settings	343
Web	345
Settings	346
XML	347
Settings	347
Advanced Data Sources	350
SQL Server/SQL Azure (MSSQL)	351
Settings	352
MySQL	355
Settings	356
Remote Desktop Manager Online (RDMO)	358
Activate Subscription (Register)	359
Activate Online Data Source Trial	360
Settings	363
Remote Desktop Manager Server (RDMS)	365
Remote Desktop Manager Server Installation	366
Security Checklist	374
Automatic User Account Creation	374
Settings	374

Part V Entry Types

378

1 Sessions	378
Overview	378
Types	378
Remote Connections	378
Citrix ICA/HDX	378
DameWare Mini Remote Control	379
FTP	380
Applications	381
Built-in FTP/FTPS	381
Built-in SFTP	383
Host	385
HP Remote Graphics Receiver	386
Intel® AMT (KVM)	387
LogMeIn	387
Desktop Shortcut	388
Portal (Host Url)	389
Microsoft Remote Desktop (RDP)	391
Normal	391
Azure RDP	400
Hyper-V RDP	401
NoMachine	403
PC Anywhere	404
Radmin	405
Remote Assistance	406
ScreenConnect	407
TeamViewer	408
Telnet, SSH, RAW, rLogin	409
Putty	410
Built-in Telnet	412

Built-in SSH	412
Built-in SSH Shell.....	413
SSH Private Keys.....	414
VNC	416
Applications	416
Embedded UltraVNC.....	417
VPN	418
Web Browser (HTTP/HTTPS).....	418
Auto Login	421
X Window	422
Virtualization.....	423
Amazon Web Services (AWS) Console.....	423
Citrix XenServer.....	424
Microsoft Azure Console.....	425
Microsoft Azure Table Storage Explorer.....	433
Microsoft Hyper-V.....	434
Microsoft Virtual PC.....	435
Microsoft Virtual Server.....	436
Microsoft Windows Virtual PC.....	437
Oracle VirtualBox.....	438
VMware (Player, Workstation, vSphere).....	439
VMware Console.....	441
VMware Remote Console.....	442
Cloud Explorer.....	443
Amazon S3	443
Dropbox	445
Microsoft Azure Storage Explorer.....	447
Others	449
Command Line	449
Data Report	449
Database	452
Inventory Report.....	456
PowerShell	456
SNMP Report	457
SQL Server Management Studio.....	461
Windows Explorer.....	462
2 Data Entries.....	463
Overview	464
Auto Fill	465
Chrome Extension.....	467
Firefox Extension.....	471
IE Extension.....	476
Types	478
Account	478
Alarm Codes	479
Bank Information.....	480
Credit Card.....	481
Email Account.....	482
Note/Secure Note.....	484
Other	485
Passport	486
Safety Deposit.....	486
Software/Serial.....	487
Web	488

3	Contact.....	490
4	Documents.....	492
	Certificate	492
	Default	493
	Image	493
	Microsoft Office (Word, Excel, PowerPoint, Visio and OneNote)	494
	PDF	495
	Phonebook	497
	Text	498
5	Groups.....	500
	Overview	500
	Types	504
	Company.....	504
	Customer.....	504
	Database.....	505
	Device	506
	Domain	507
	Group/Folder.....	507
	Identity	508
	Printer	509
	Server	510
	Site	511
	Workstation.....	511
6	Credentials.....	512
	Overview	512
	Dynamic Credential Linking	514
	Types	515
	Credential Redirection.....	515
	1Passw ord	520
	Firefox Passsw ord Manager.....	521
	Google Passsw ord Manager.....	521
	LastPass	522
	Connection String.....	523
	KeePass	524
	Passw ord Safe.....	525
	Passw ord Vault Manager.....	526
	Passw ordstate.....	527
	Pleasant Passw ord Server.....	528
	Private Key.....	529
	Secret Server.....	530
	Username/Passw ord.....	534
	Window s Credential Manager.....	534
7	VPN.....	535
	Overview	535
	Types	536
	Cisco VPN.....	536
	Microsoft VPN.....	537
	SonicWall VPN.....	539
	TheGreenBow	540
8	Macros/Scripts/Tools.....	541
	Overview	541
	Types	541

AutoHotKey.....	541
Autolt	543
Command Line.....	544
Database Query.....	545
Jitbit Macro Recorder.....	545
Macro	546
PowerShell (Local).....	547
PowerShell (Remote).....	547
PSEXec	548
Template	549
VBScript	549
WASP PowerShell.....	550
WMI	551

Part VI User Interface 553

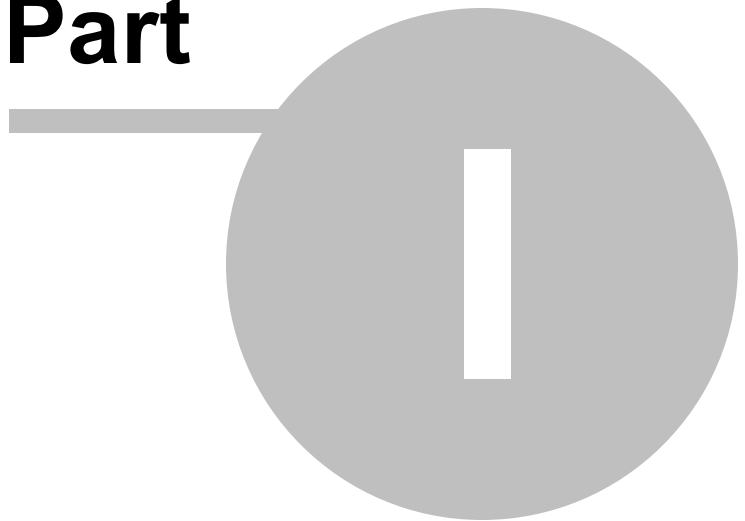
1 Style.....	553
2 Top Pane.....	557
Quick Access Toolbar	558
Quick Connect.....	559
Ribbon / Menu	560
3 Navigation Panels.....	561
All Entries	561
Private Vault	566
Opened Sessions	566
Favorite Entries	568
Most Recently Used Entries	570
Application Tools	570
4 Content Area.....	571
Dashboards	572
Sessions.....	572
Data Entries.....	572
Groups	573
Credentials.....	574
Macros/Scripts/Tools.....	574
5 Panes (Footer).....	575
Attachments	577
Description	578
Details	578
Hyper-V Console	579
Information	581
Logs	583
Sub Connections	584
Tab Groups	584
Terminal Services Console	584
VMware Console	586
XenServer Console	589
6 Status Bar.....	590
Search/Filter	591
Grab Input	594
7 Tray Icon.....	594

Part VII How-to	597
1 How-to understand Remote Desktop Manager licensing.....	597
2 How-to configure the Yubikey 2-Factor Authentication.....	597
3 How-to configure the Google Authenticator 2-Factor Authentication.....	599
Part VIII Support/Resources	603
1 Command Line Arguments.....	603
2 Follow Us.....	603
3 Keyboard Shortcuts.....	604
4 Lexicon.....	606
5 Technical Support.....	606
6 Add-on Documentation.....	607
Overview	607
SQL Server Management Studio Add-On	607
VPN Add-ons	608
Overview	608
Avaya (Nortel).....	609
Barracuda NG Network.....	609
Bitvise Tunnelier.....	609
Check Point Endpoint Security	609
Check Point VPN-1 SecureClient.....	610
Cisco AnyConnect.....	610
F5 Firepass SSL.....	610
FEC Secure IPSec.....	610
FortiClient.....	611
Generic VPN.....	611
Juniper Junos Pulse.....	611
Juniper Network Connect.....	611
Juniper WSAM.....	612
Juniper-Netscreen.....	612
NCP Secure Entry Client.....	612
OpenVPN.....	612
SecureCRT.....	612
Shrew Soft.....	613
SonicWall NetExtender.....	613
WatchGuard Mobile.....	613
WatchGuard SSL.....	613
7 Best Practices.....	614
Quick Start	614
Backups	615
Security	616
Use Credential Entries	618
Use VPN Entries	619
8 Tips And Tricks.....	619
Automation via Windows PowerShell	619
Creating Shortcuts	620
Data Migration	622

Data Report	625
Edit Hosts File	628
How to Backup	629
How to Reinstall	630
How to Subscribe to the Announcements Forums	630
HTML Export Using Symmetric Encryption	631
Identify Security Groups	632
Keep Tabs Opened	635
Passcode Prompt When Opening an Entry	637
Open RD Gateway Only when Unable to Ping Host	638
RDP Session Time Limits	638
Remote PowerShell	642
Remote Install with PSEXEC	642
Run as Another User	644
Built-in RunAs	645
Manual RunAs	649
Running Remote Desktop Manager as Another User	655
SQL Server Data Source with Integrated Security	657
SQL Server Maintenance Plans	661
Tab Groups	662
Team Tips	663
VPN	665
VPN Group	665
VPN Routing	666
9 Troubleshooting.....	667
Data Sources	667
MySQL	668
SQL Server	668
General	669
FIPS (Encryption)	670
Large Memory Aware Application	671
LogMeIn	672
Microsoft RDP	672
Automatic Logon	676
Logoff Access Denied	678
Protocol Error	680
Performance	681
Profiler	682
Putty	685
RPC	685
SSH	686
User Interface	686
VPN	688
Web Browsers	689
WMI	690
Index	0

Getting Started

Part



1 Getting Started

1.1 What is Remote Desktop Manager?

Description



Remote Desktop Manager is an application designed to manage all of your remote connections, passwords and credentials. With Remote Desktop Manager, you can quickly and easily organize, find and launch your remote connections.

Remote Desktop Manager acts like a wrapper and a manager around existing technologies, and uses no proprietary protocols. All communications are established using either an external library or third party software.

Remote Desktop Manager is compatible with many tools and technologies, including: **Citrix**, **Dameware**, **FTP**, **Hyper-V**, **LogMeIn**, **Microsoft Remote Assistance**, **Microsoft Remote Desktop**, **PC Anywhere**, **Radmin**, **SSH**, **Sun Virtual Box**, **Team Viewer**, **Telnet**, **Terminal Services**, **Virtual PC**, **VMware**, **VNC**, **X Windows**, and more!

Where Do I Start if I Don't Know Anything About Remote Connection Technologies?

If you've never used Remote Desktop Client (mstsc.exe), VNC or any other communication application or tool, and you simply want to connect to a remote machine, we recommend that you use [LogMeIn](#), which is a free web-based remote access application.

Remote Desktop Manager Supports the Following Protocols

- FTP ([File Transfer Protocol](#))
- HP RGS ([HP Remote Graphics Software](#))
- HTTP/S ([Hypertext Transfer Protocol](#))
- ICA ([Independent Computing Architecture](#))
- RAW ([Transmission Control Protocol](#))
- RDP ([Remote Desktop](#))
- rLogin ([rLogin](#))
- SSH ([Secure Shell](#))
- Telnet ([TELEcommunication NETwork](#))
- VNC ([Virtual Network Computing](#))
- And much more!

1.2 System Requirements

Minimum Requirements

- Windows XP (SP2 or later), 2003, Vista, 2008, 7, 8 and 2012
- [Microsoft .NET Framework 3.5](#)
- 800MHz processor
- 512MB RAM
- 1024 x 768 screen resolution

- 100+ MB hard drive space



.NET 4.0 does not contains the .NET Framework 3.5. You will need to install it separately.

64-bit Support

Remote Desktop Manager is compatible with all 64-bit versions of Windows, starting with Windows Vista SP1.

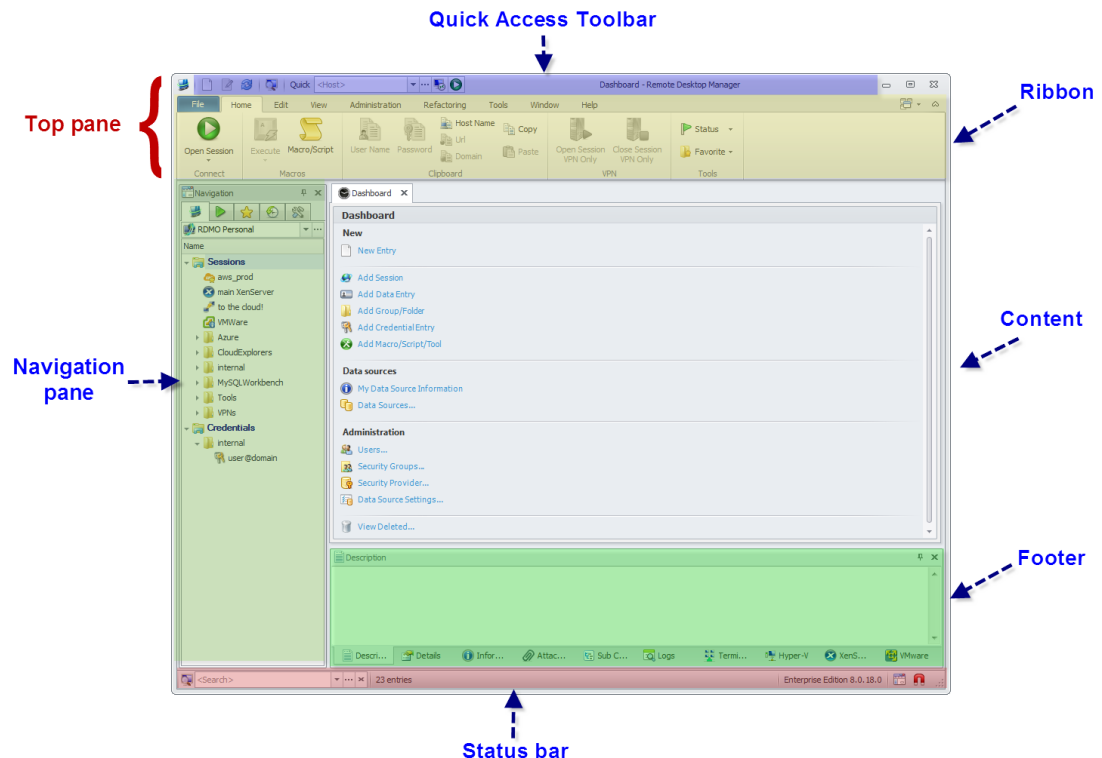
Terminal Services and Thin Client Support

Remote Desktop Manager can be installed on a Terminal Server machine, thin client and Windows XP Embedded as well.

1.3 Main Screen

Description

Here is Remote Desktop Manager's main screen when using the **Default (Ribbon)** style. Two other styles exist as can be seen below. See the [User Interface](#) topic for instructions on how to change the current style.

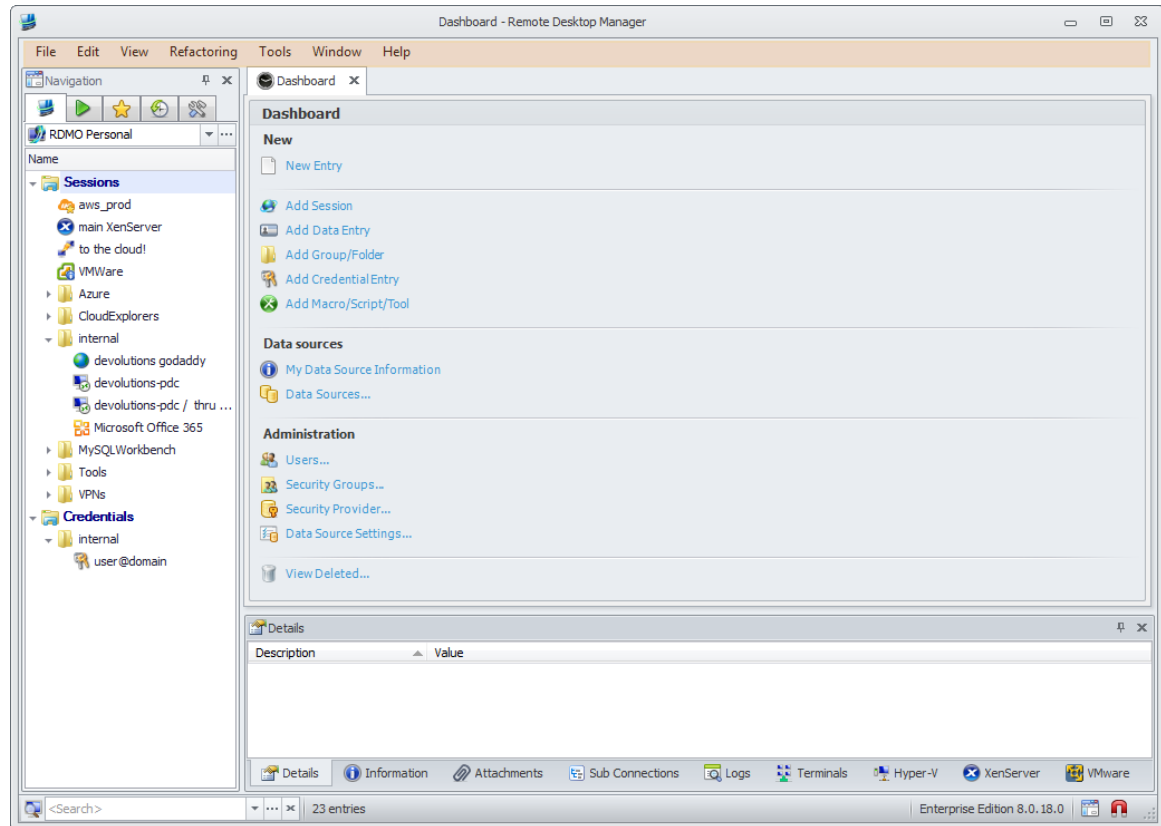


Default (Ribbon) User Interface Style

Read the following topics for more details on specific areas

[Quick Access Toolbar](#)[Ribbon / Menu](#)[Navigation Pane](#)[Content Area](#)[Panels \(Footer\)](#)[Status Bar](#)

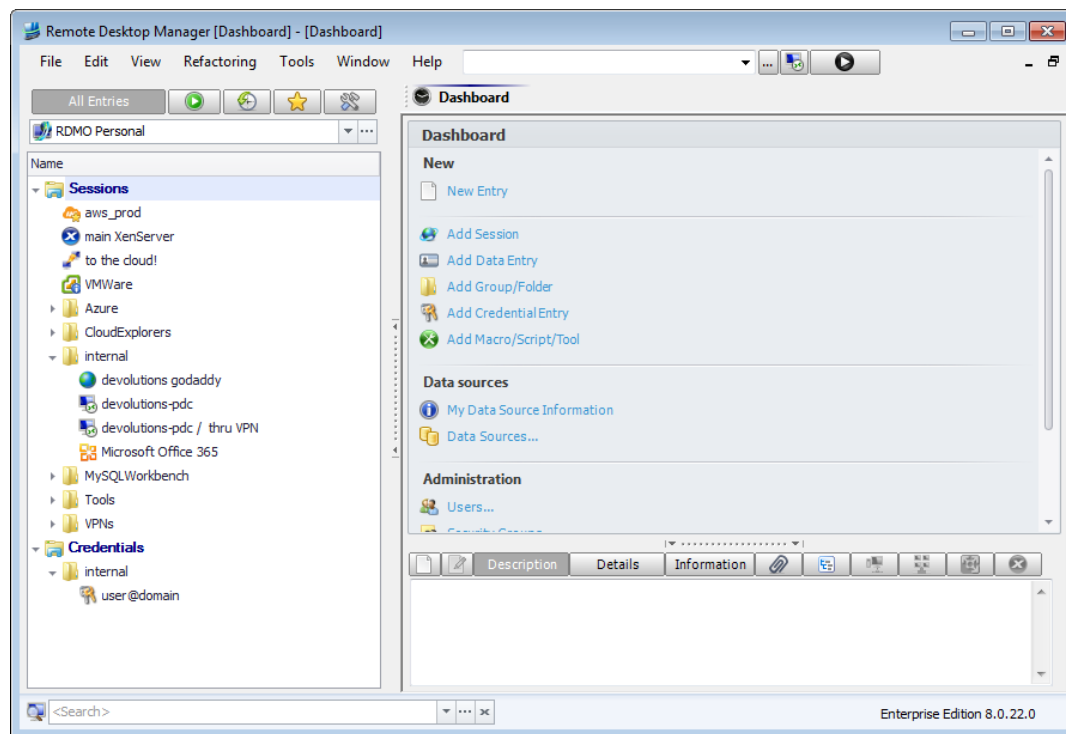
Default (menu) User Interface Style



Default (Menu) User Interface Style

As can be seen, the differences are only in the top pane area. The *Ribbon* has been replaced by a standard menu, and the *Quick Access toolbar* is not present.

Classic UI (v7.X) User Interface Style



Classic UI (v7.X) User Interface Style

The Classic UI is our previous version's default style. It uses no dockable panes and has a standard menu. Users that have been using Remote Desktop Manager for a long time may prefer this style for its minimalist interface that they are used to.

1.4 Creating a New Entry

Overview

To start using Remote Desktop Manager you must configure a session. There are many types of sessions; you should know what third party or technology you will use to connect remotely in order to choose the appropriate session type(s) that you plan on configuring.

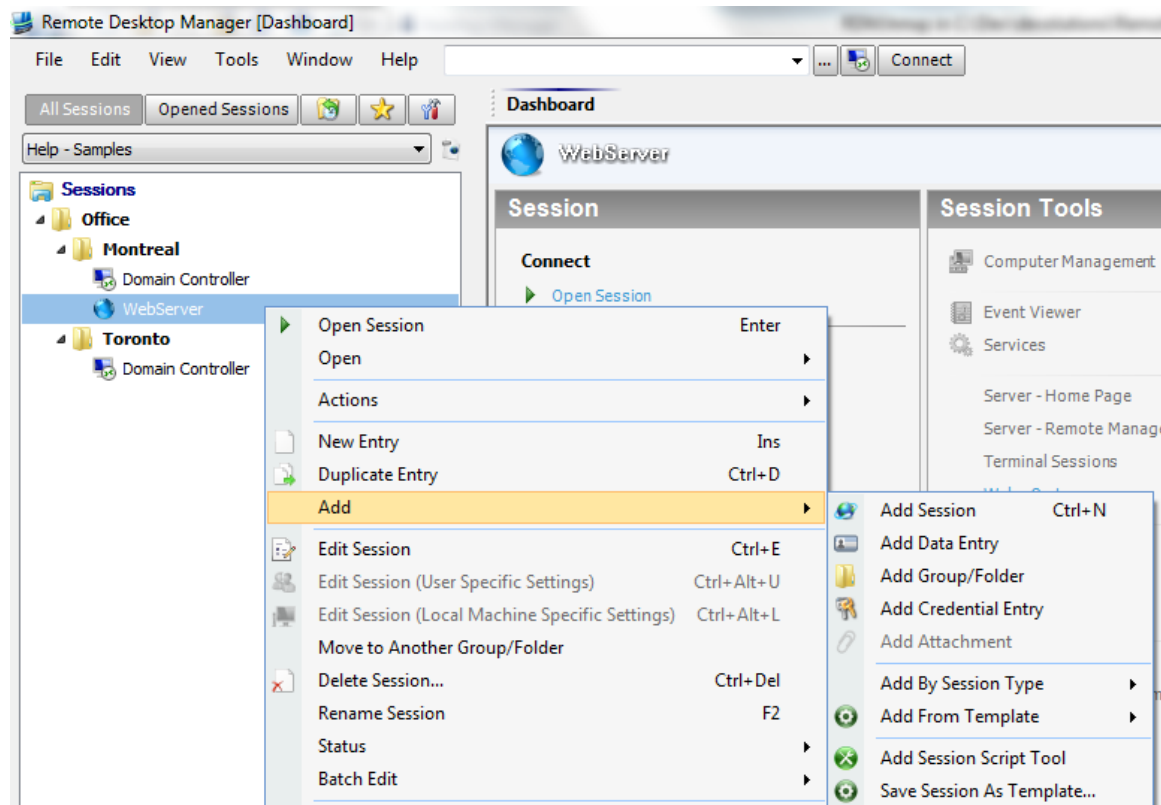
Remote Desktop Manager supports the following session types:

- Citrix XenApp (ICA)
- Dameware Mini Remote Control
- FTP (Explorer, Filezilla and WinSCP)
- LogMeIn
- Microsoft Hyper-V
- Microsoft Remote Assistance
- Microsoft Remote Desktop (RDP)
- Microsoft Virtual PC
- Microsoft Virtual Server
- Microsoft Windows Virtual PC
- Putty (SSH, Telnet, RAW and rLogin)
- Radmin Viewer
- Oracle VirtualBox
- Symantec PC Anywhere
- Team Viewer
- VMware (ESXi, Player, vSphere, Workstation)
- VNC (UltraVNC, TightVNC, RealVNC and embedded)
- VPN (Cisco, Microsoft, SonicWall, TheGreenBow...)
- X Windows
- And many more by installing other add-ons

Creating a Session from the Context Menu

The easiest way to create a new session is by using the **Insert** key or from the Context Menu. On the

main application window, simply right-click **Sessions** 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 session property window. If you are unsure of the type of session you need, simply create a blank section and specify the session type at a later time.



Adding a new session

Creating a Session with Drag & Drop

You can also create a session by dragging & dropping an .rdp file in the main application window. When you do this, 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's also possible to drag & drop the LogMeIn desktop shortcut to create a LogMeIn session.



It is possible that drag & 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.

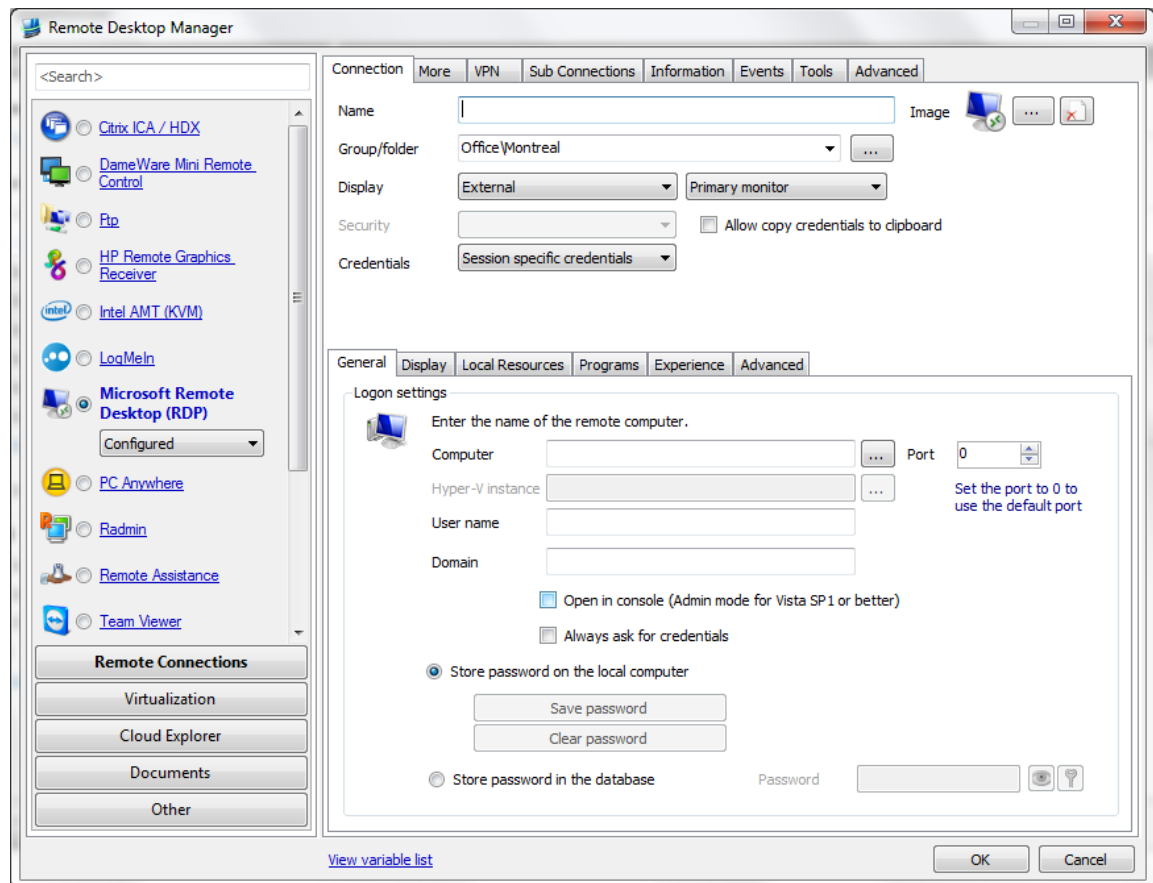
Creating a Session by Importing its Configuration

You can also import a session 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.

1.5 Configuring an Entry

Description

Each entry type has its own specific settings. However, some settings are shared.



Session editing dialog

Description	
Name	The name of the session that appears in the sessions list. This will be copied to the host field as it's initial value because many times the computer name is entered here and can be used directly.
Group/Folder	This is 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 and embedded in Remote Desktop Manager, or externally. In the case of the latter, and if the application allows it, you may select the monitor on allows it will be displayed.
Security Group	In the Enterprise edition, allows the Administrator to assign a security group to a session, and therefore limit a subset users to view this session.
Credentials	Used to define the credential source: <ul style="list-style-type: none"> Session-specific credentials: uses the username and password from the session type configuration. Credential repository: links this session to an existing credential

	<p>repository entry. This is the solution that allows for reuse and lets you maintain the minimum number of entries whenever the credentials need updating.</p> <ul style="list-style-type: none"> • Embedded credential entry: creates an embedded credential repository entry. It will be stored within this session's configuration
--	---

As well as the fields described above, additional tab pages contain many data fields and options for your sessions.

Description	
More (Tab Page)	Contains the following sections: Description , Keywords/Tags , Alternate Host , Tab Page Category/Color . The session description can be in plain text, in rich text format, or a website link.
VPN (Tab Page)	Used to optionally configure al VPN connection for use with the session. Please see VPN Overview for more details.
Sub Connections (Tab Page)	Contains the sub connections linked to this session. It's possible to use variables that refer to this session's fields, such as the host name, from within sub connections. This is useful for connecting to the same host with different protocols. Please see Sub Connections Overview for more details.
Information (Tab Page)	Contains different types of information related to the session, such as the Hardware , Contact and Custom Fields .
Events (Tab Page)	Contains a script or command line to be executed before or after establishing a connection. For example, this can be used to execute a batch file or an external application that prompts the user for more information, or to update a log on an external server. Please see Connection Events and Auto Typing Macro .
Logs (Tab Page)	Contains the session logs and other related options. For example, entering a comment when opening a session can be made mandatory. Please see Log Options
Attachments (Tab Page)	Manages the session attachments. Used to add, edit and delete the linked files. Please see Attachments Overview
Tools (Tab Page)	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. Please see Tools Overview
Advanced (Tab Page)	Contains advanced settings related to the session, such as the internal data source ID and session ID. These values can be used to invoke Remote Desktop Manager from a command line to open the session, or to run a batch modification. Please see Advanced settings

1.6 Establishing a Connection

Description

There are two possible modes for establishing a connection:

- From a configured connection in the connection list
- Using the quick connect feature, learn more about quick connect [here](#).

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

Configured Connection

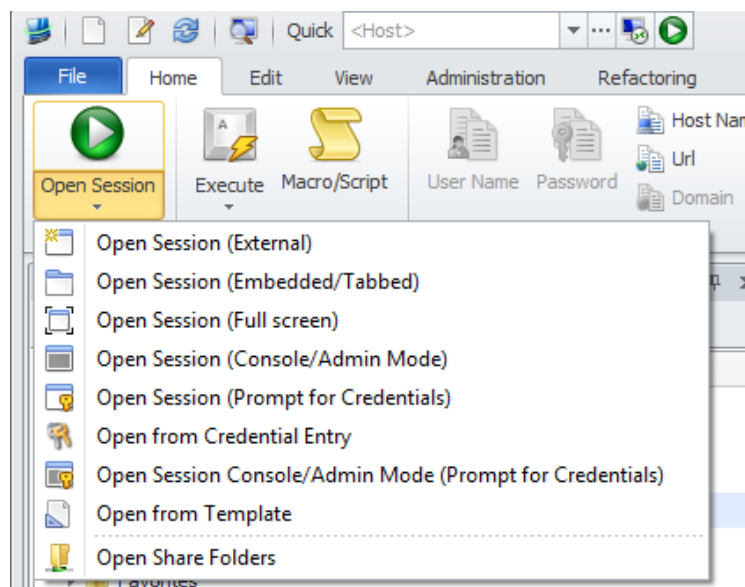
You may open a Connection by many means:

- by double clicking it in the sessions list
- by pressing enter while the entry is focused
- by using the contextual menu (right-click).
- by using the commands in the ribbon.

All entry types have a default action associated with them, this action is executed when you use any means described above. The default action is often "Open", but you can modify it for certain entry types.

Via the menus, you may specify different connection options, such as:

- 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



Opening an existing session

1.7 Security

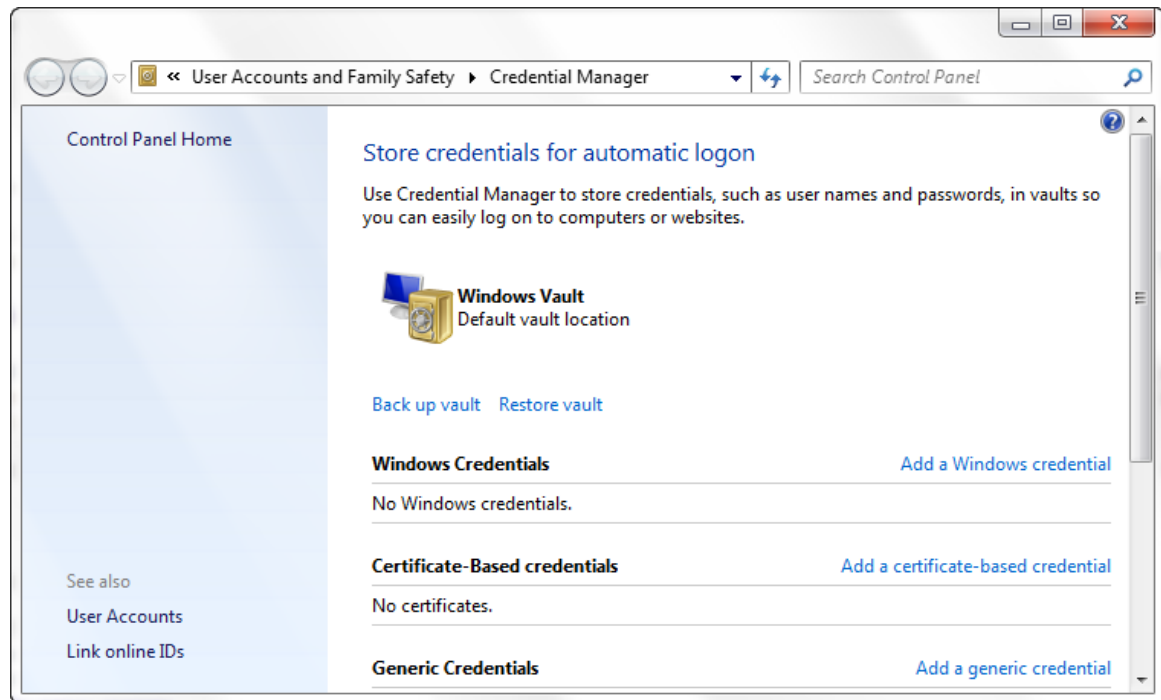
Description

All passwords stored in the application database, and are encrypted using a strong encryption algorithm. As such, even if a user accesses the data directly in the database, it will be unreadable.

If you choose to store passwords locally, Remote Desktop Manager will use the same mechanism used by mstsc.exe (Microsoft Remote Desktop client), and the passwords will be stored in the Windows Credential repository. You can access it from "User Account" in Windows. However, note that you will be unable to see the password because it has been encrypted by Windows.

What is the Windows Credential Manager?

The Windows Credential Manager allows you to store credentials, such as user names and passwords, which you use to log on to websites or other computers on a network. By storing your credentials, Windows can automatically log you on to websites or other computers. Credentials are saved in special folders on your computer called vaults. Windows and other programs (such as web browsers) can securely give the credentials in these vaults to other computers and websites.



Windows Credential Vault

For information about saving credentials in a vault, see [Credentials Overview](#). You can also learn more in the [Windows Credential Manager](#) section

U.S. Federal Government Approved Encryption

Our application integrates an Advanced Encryption Standard (AES) algorithm to protect your local files and your sensitive data in the database. A mix of our own private key and a master password (passphrase) is used to create a strong encryption key (256-bit key).

This cipher is regarded as being 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.

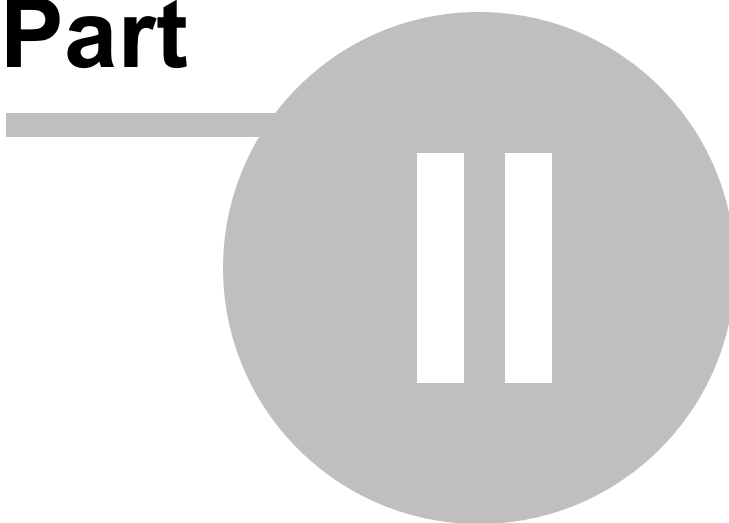
Tips

It's also possible to enforce the security by:

- Using and [Advanced Data Source](#) and give restricted user access
- Enabling the encryption of the session in the [Advanced Tab Page](#) (Encrypt configuration in the data source)
- Using the [Data Source Settings](#)
- Using the [Security Provider](#) with a passphrase
- Choosing not to save password in the data source, which will prompt for the credential on the first connection

Installation

Part



2 Installation

2.1 Client

2.1.1 Overview

Description

You can download Remote Desktop Manager either as a setup files or as a compressed (zip) file containing the binaries.

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 please consult [Portable \(USB\)](#).

Licence

You have a 30 day trial of the Enterprise edition. If you possess a purchased licence for the Enterprise Edition, please follow the instructions at [Register Enterprise Edition](#), if you want to disable the Enterprise Edition trial immediately please follow [Register Standard Edition](#)

Data Source

By default, a local data source has already been created using the SQLite format. You can add as many data sources as you require, please see [Data Source Overview](#) for more information.



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

External Applications

Configure your installation path for all the external applications you plan to use. For example RealVNC, Putty, Filezilla, etc. Please consult [Path](#) for more information.

Terminal Services

Please consult the [Terminal Services](#) topic for full details.



To install on Windows 2003, please read the [Microsoft RDP Troubleshooting](#) topic.

2.1.2 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.
An hyperlink will display the installation folder.

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

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



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

Override the Default Path

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

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

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

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

Default Configuration For Terminal Services Environment

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

2.1.3 Portable (USB)

Description

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



The portable installation mode allows you to run multiple installs of Remote Desktop Manager. You can have multiple versions using various licenses and different configurations.



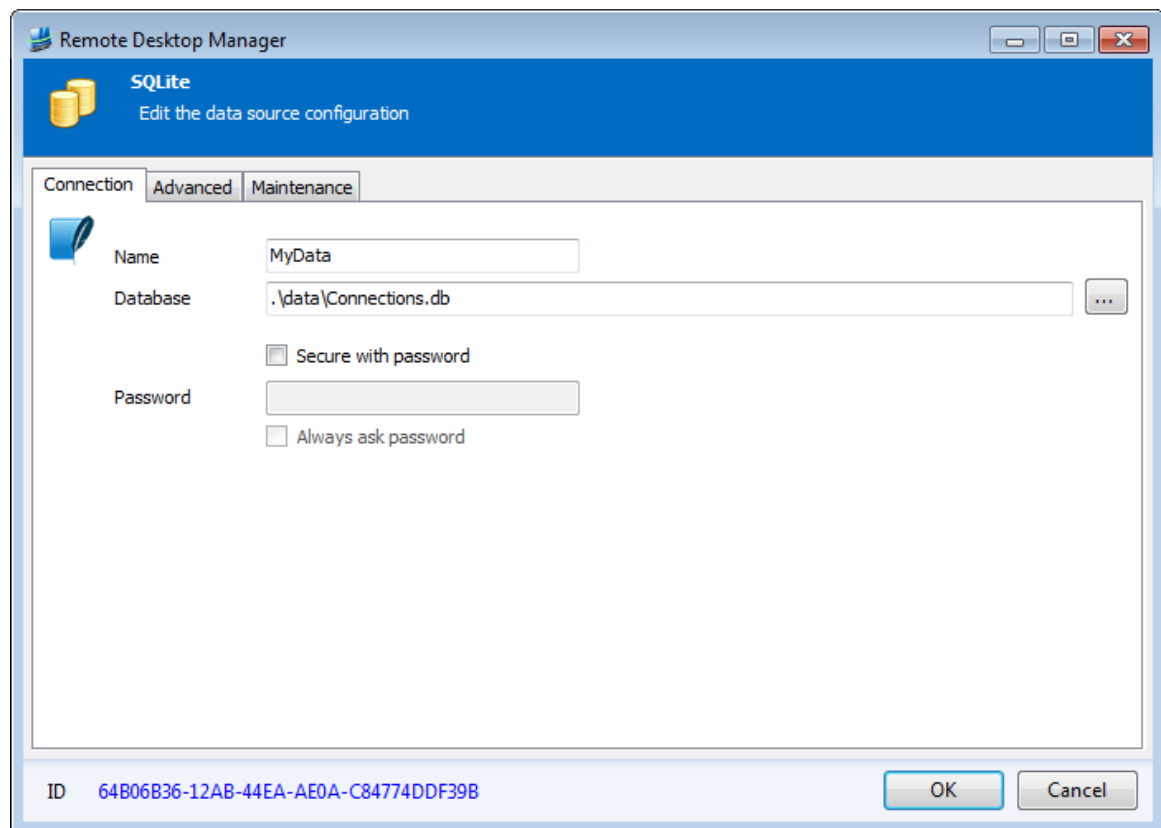
Remote Desktop Manager stores the offline cache in your Windows profile and this cannot be changed for security reasons. Therefore if you are using an advanced data source, the offline file and the cache will be unavailable.

Procedure



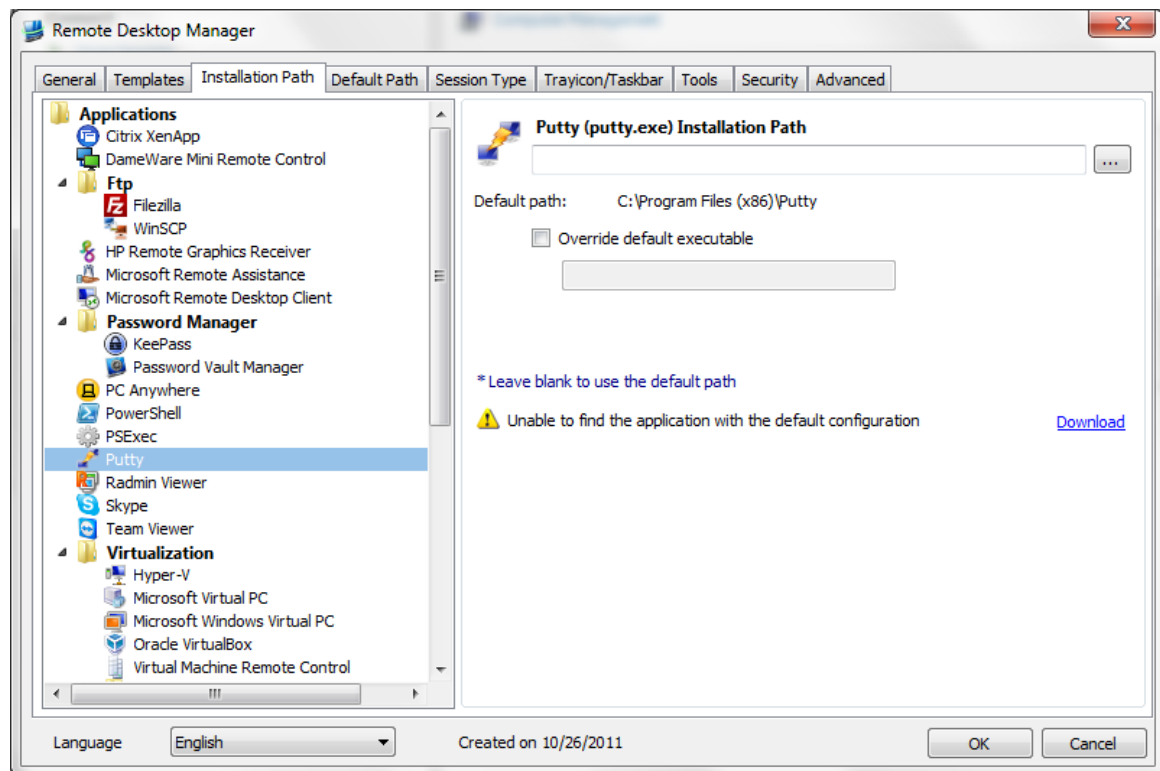
This is a "recipe" that ensures true portability and ease of maintenance. You can adapt it to your liking.

1. Download the "Binary Files" package of Remote Desktop Manager
2. Create a RemoteDesktopManager folder on your portable device.
3. In the installation folder created at step 2, create two folders
 - 3.1. a **config** folder
 - 3.2. a **data** folder
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. Delete the existing data source that was created automatically.
8. Create a new data source of a type that can be stored on your portable device: XML, SQLite
9. Configure the data source using a relative path so it is stored on the portable device: `.\Data\Connections.db`



Data source saved relative to the installation folder

11. Configure your portable applications (Filezilla, Putty, UltraVNC, etc.) in the same manner (relative to the installation folder).



Portable Putty installation path configuration

2.1.4 Terminal Services

Description

Remote Desktop Manager has 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.



Roaming user profiles must be used for this procedure to apply.

Procedure

1. After installing Remote Desktop Manager, configure it as you prefer. We really recommend going through all the configuration options and finding the set of options that you wish to distribute. The data sources are of special interest because it is much better if they are configured by an administrator. You can even take the opportunity of locking the data sources to protect against any modification by the users. Please refer to [Lock Data Source](#) for more information.
2. When Remote Desktop Manager is configured to your liking, locate the configuration file. A simple trick is to go in **File -> Options -> Advanced**, at the bottom of the form you will see a Hyperlink that will open the configuration folder. The file is RemoteDesktopManager.cfg
3. Make a copy of that file and rename it *default.cfg*

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.

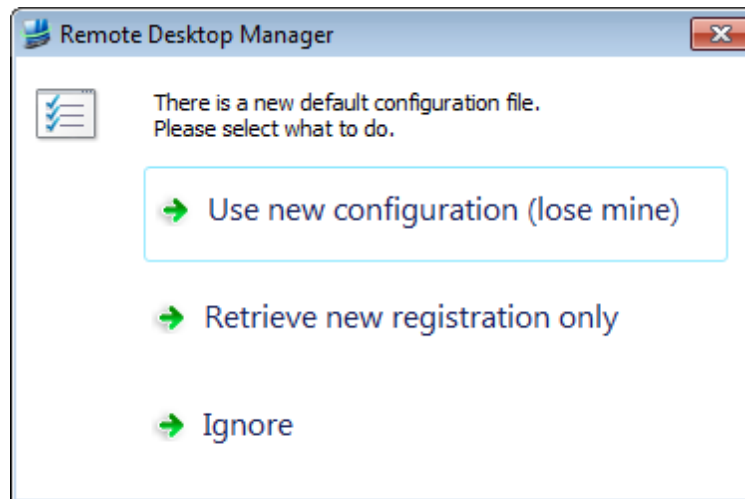
Workflow

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

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



New default.cfg detected

By selecting **Use new configuration (lose mine)**, the user's configuration is simply overwritten. If you only wish to update the Remote Desktop Manager licence key after a renewal, choose **Retrieve new registration only**.

2.1.5 Custom Installer Service

2.1.5.1 Activate Custom Installer Subscription (Register)

Description



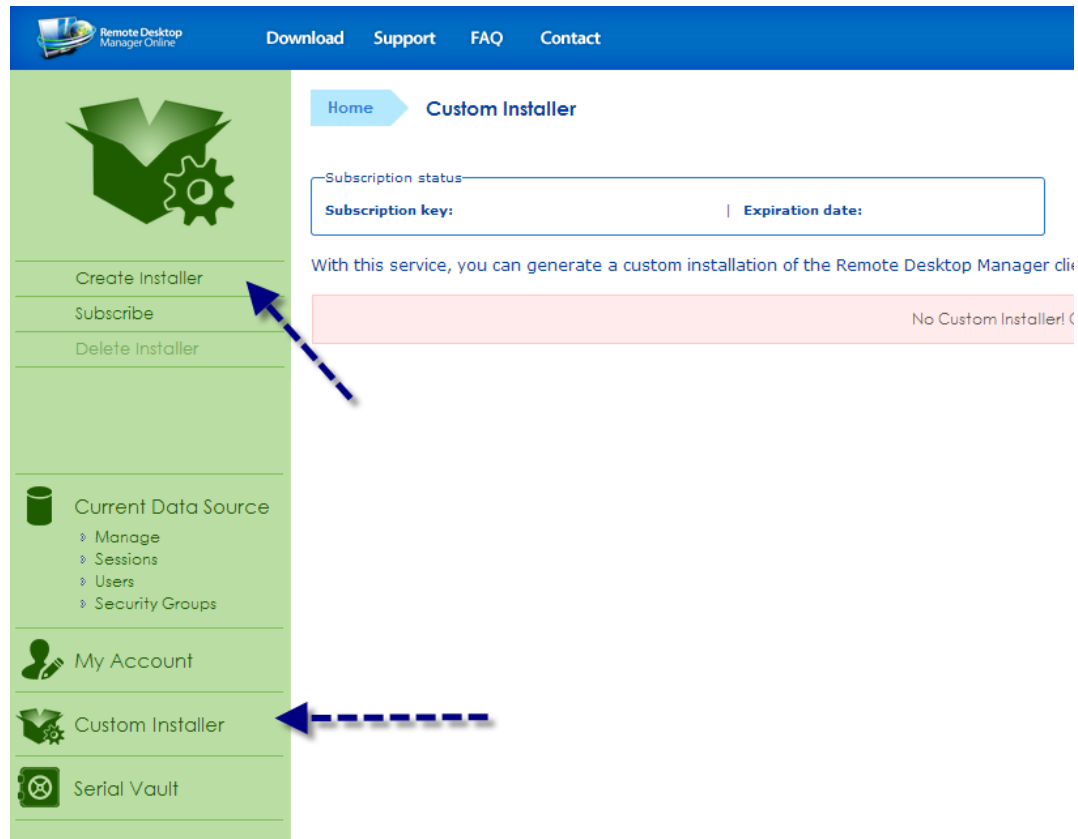
The Custom Installer Service of Remote Desktop Manager Online allows you to generate and download custom installations of Remote Desktop Manager with a choice of pre-configured settings like a data source or the registration key (serial number).

For more information regarding the custom installer service, consult the [web site](#).



You need to create a Remote Desktop Manager Online account (free) to activate your custom installer service serial number.

1. Please go to <https://online.remotedesktopmanager.com/>
2. Go to: Custom Installer > Subscribe and enter in your serial number.



Custom Installer Service registration

2.1.5.2 Create an Installation Package

Description



The Custom Installer Service of Remote Desktop Manager Online allows you to generate and download custom installations of Remote Desktop Manager with a choice of pre-configured settings like a data source or the registration key (serial number).

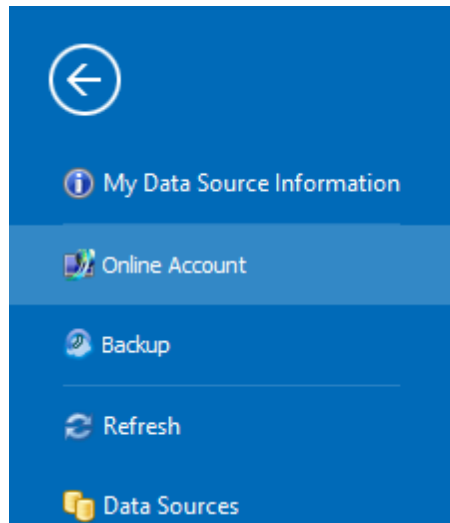
For more information regarding the custom installer service, consult our [website](#).



Remote Desktop Manager installs the required add-ons automatically when it detects that they are needed. If you need to customize an Add-on settings, you must perform the modifications on your machine then create the installer package. It's settings will be distributed automatically.

Settings

1. Click on **File -> Online Account -> Sign-in** to connect to your Remote Desktop Manager Online account.



RDMO account

Online account

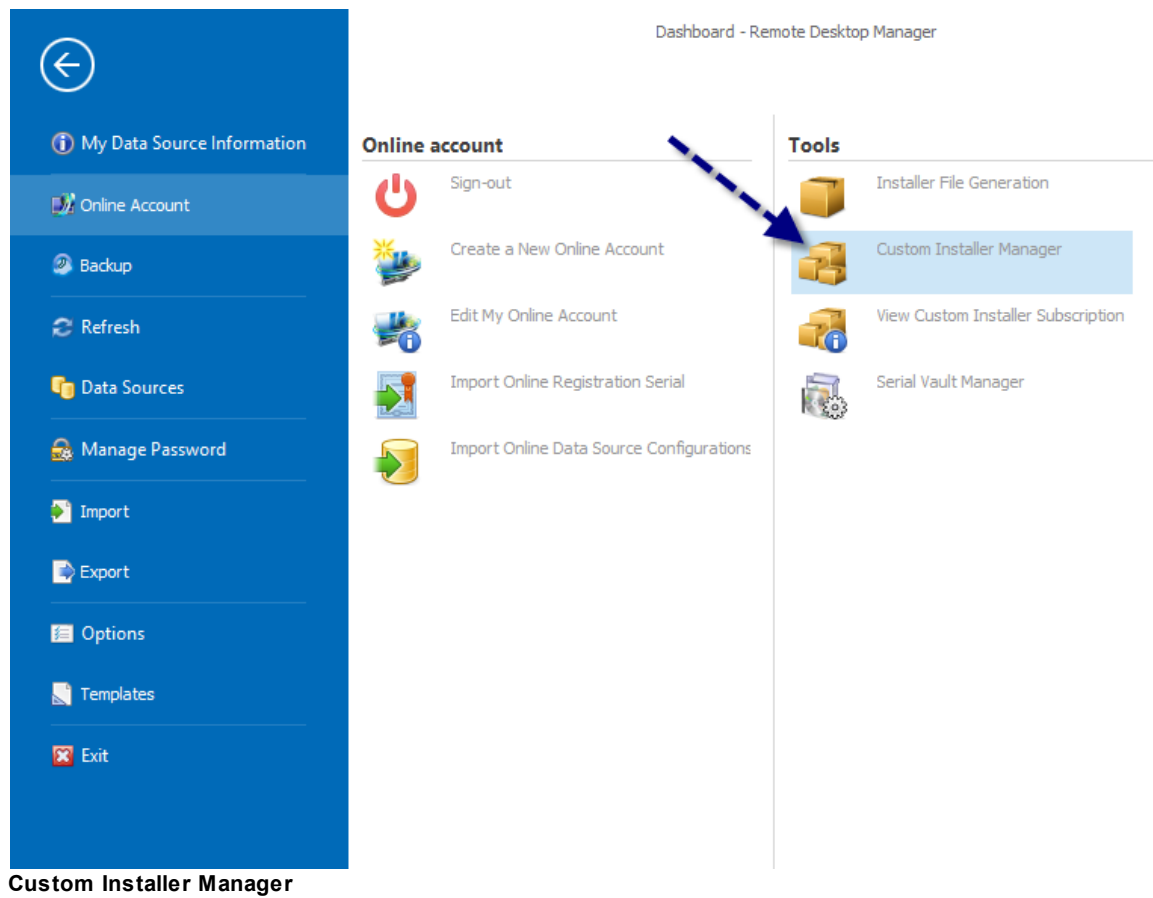


Sign-in

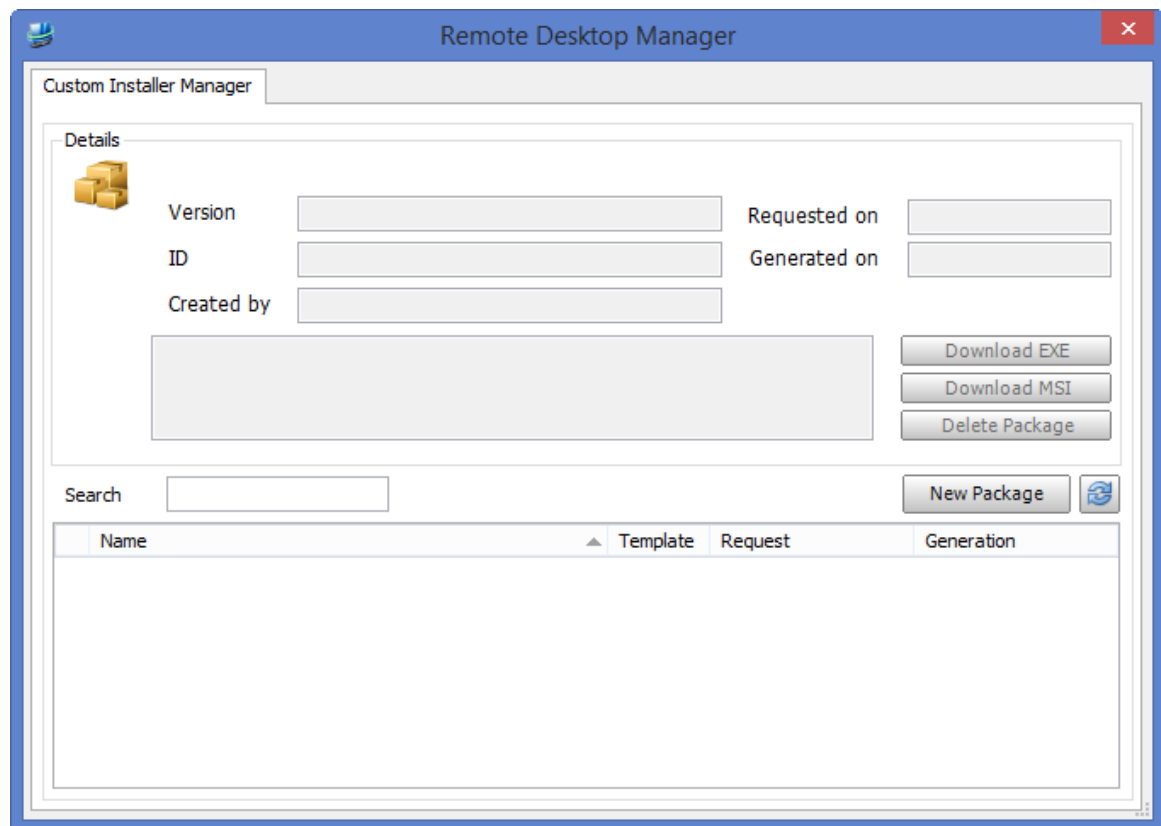


Create a New Online Account

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

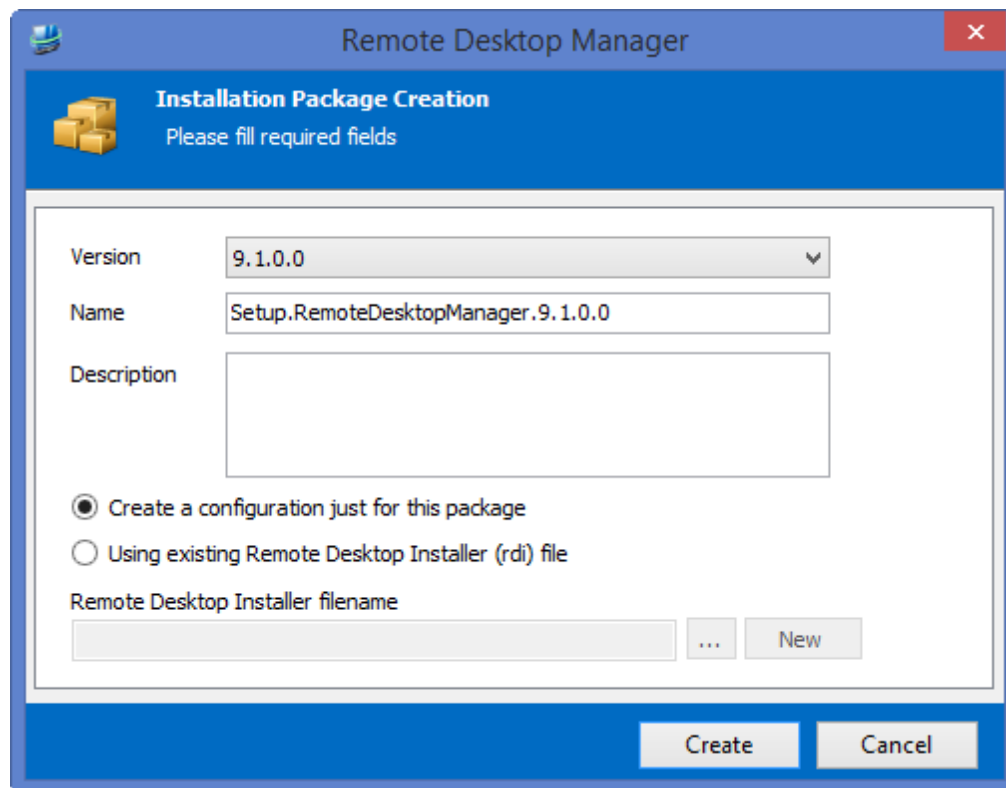


3. Click on the **New Package** button.



New Package

4. Select the application version and enter a name for your package. By default the data source and option selection is performed by the wizard, but you have the option of choosing an existing Remote Desktop Installer (rdi) file that was created as described in [Installer File Generation](#). The file selection controls will be enabled if you select "Using existing Remote Desktop Installer (rdi) file. When your choices are made, click on **Create**.



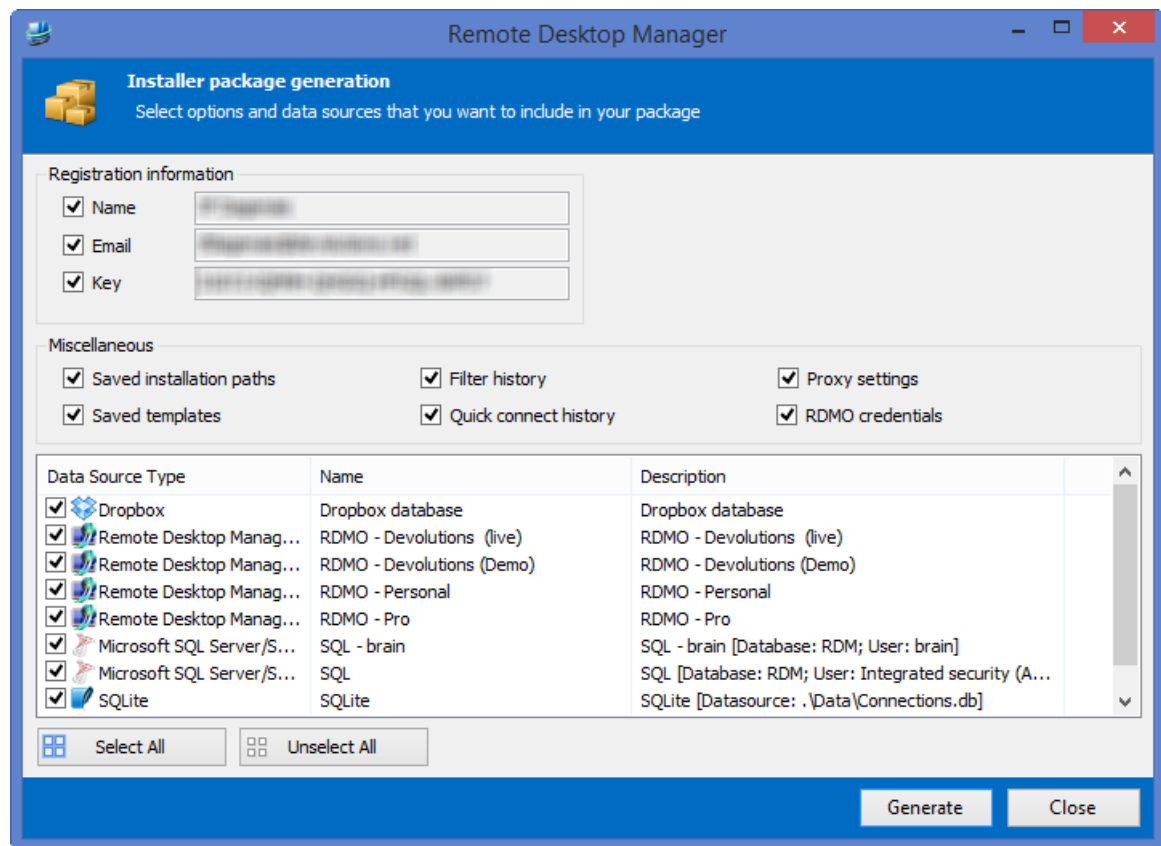
The screenshot shows a Windows-style dialog box titled "Remote Desktop Manager" with a close button (X) in the top right corner. The dialog has a blue header bar with the text "Installation Package Creation" and a sub-header "Please fill required fields" next to a yellow box icon. The main content area is white and contains the following fields and controls:

- Version:** A dropdown menu showing "9.1.0.0".
- Name:** A text box containing "Setup.RemoteDesktopManager.9.1.0.0".
- Description:** An empty text box.
- Radio buttons:** Two options are present:
 - ☒ Create a configuration just for this package
 - ☐ Using existing Remote Desktop Installer (rdi) file
- Remote Desktop Installer filename:** A text box followed by an ellipsis button (...) and a "New" button.

At the bottom right of the dialog, there are two buttons: "Create" and "Cancel".

Package Creation

5. If you create a new configuration, you can select what you want to include in your custom installer. After, click on **Generate**.



Package Generation

Registration information

Option	Description
Name	Company registration name
Email	Registration email
Key	Serial key

Miscellaneous

Option	Description
Saved installation paths	Preserve your installation paths configured for the external application
Saved templates	Includes your local templates in the export
Filter history	Preserve your filter history
Quick connect history	Preserve your Quick connect history
Proxy settings	Includes your proxy settings
RDMO Credentials	Includes your RDMO credentials

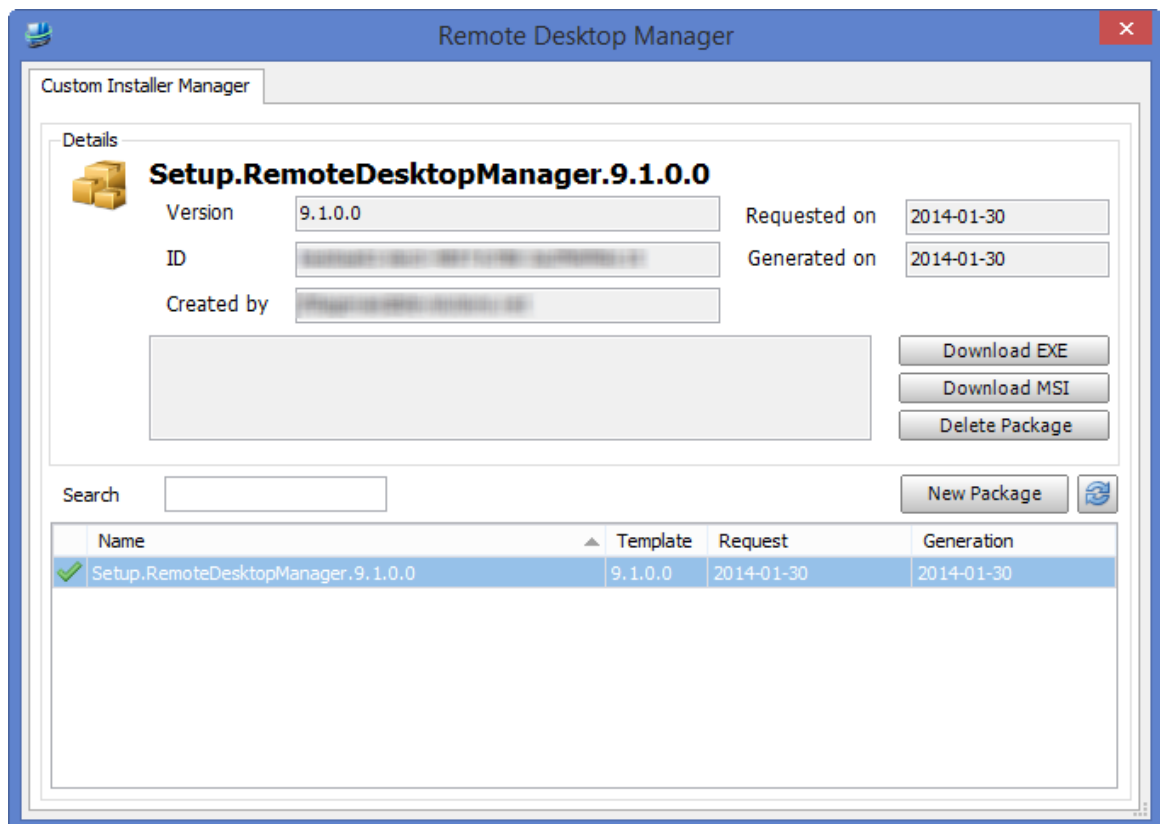
- The request is submitted to our online services and does take some time to complete. Upon completion you will receive a confirmation email.

7. You can choose to download the installer as a Windows Installer (MSI file) or as an executable (EXE file).



setup.exe is in fact what is called a bootstrapper that will ensure the installer runs with the required privileges.
Use the msi only if you know you are running with all rights and process elevation.

8. Download executable from **Custom Installer Manager** by clicking on **Download EXE** or **Download MSI**.




Download EXE or Download MSI

9. Select where you want to save the installer on your computer.
10. When the package is save on your computer, you can start the installation.

Download your custom installer from our website


You could also download your custom installer from our website. Open your **email confirmation** and click on **here**.

 Remote Desktop Manager Online

Custom Installer Request

Hi,

Your custom installer request was processed successfully.





Type: Remote Desktop Manager
Version: 9.1.0.0
Name: Setup.RemoteDesktopManager.9.1.0.0
Description:

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

Sincerely yours,


Devolutions inc.
support@devolutions.net

 Remote Desktop Manager Online




Email confirmation

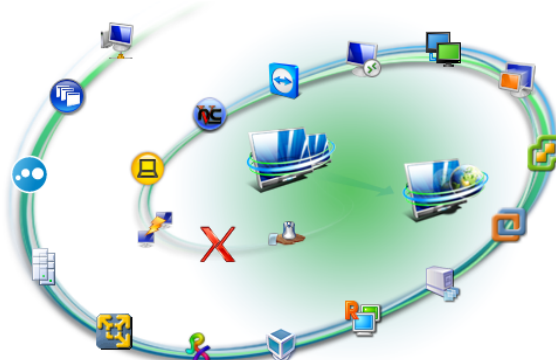
Enter your **register email address** and your **password** to login.

 Remote Desktop Manager Online

Download Support FAQ Contact

 Remote Desktop Manager Online

Store and share all your remote desktop connections online



Email Password

[Forgot your password?](#) [Log In](#)


Create an Account (Free)

Email *

First name *

Last name *

Company

Country * 

Password *

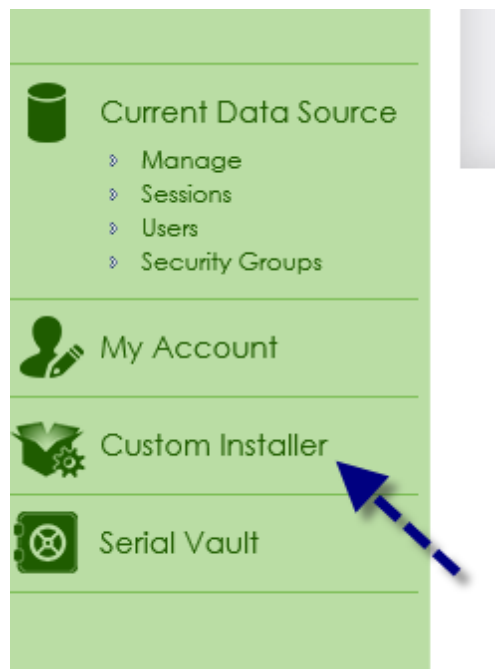
Confirm Password *

Keep me informed ☒

[Create Account](#)

RDMO credentials

Click on **Custom Installer**.



Custom Installer

Click on **EXE** or **MSI** in the download column to download the package on your computer.

Home Custom Installer

Subscription status

Subscription key: 0130C-5N0WJ-Q364E-SQWEG-K1532 | Expiration date: Feb 01, 2015

With this service, you can generate a custom installation of the Remote Desktop Manager or Password Vault Manager client with a data source of your choice pre-installed.

Output name	Description	Type	Version	Creation date	Status	Download
Setup.RemoteDesktopManager.9.1.0.0		RDM	9.1.0.0	Jan 30, 2014	✓	MSI EXE

Download EXE

When the package is downloaded, you can start the installation.

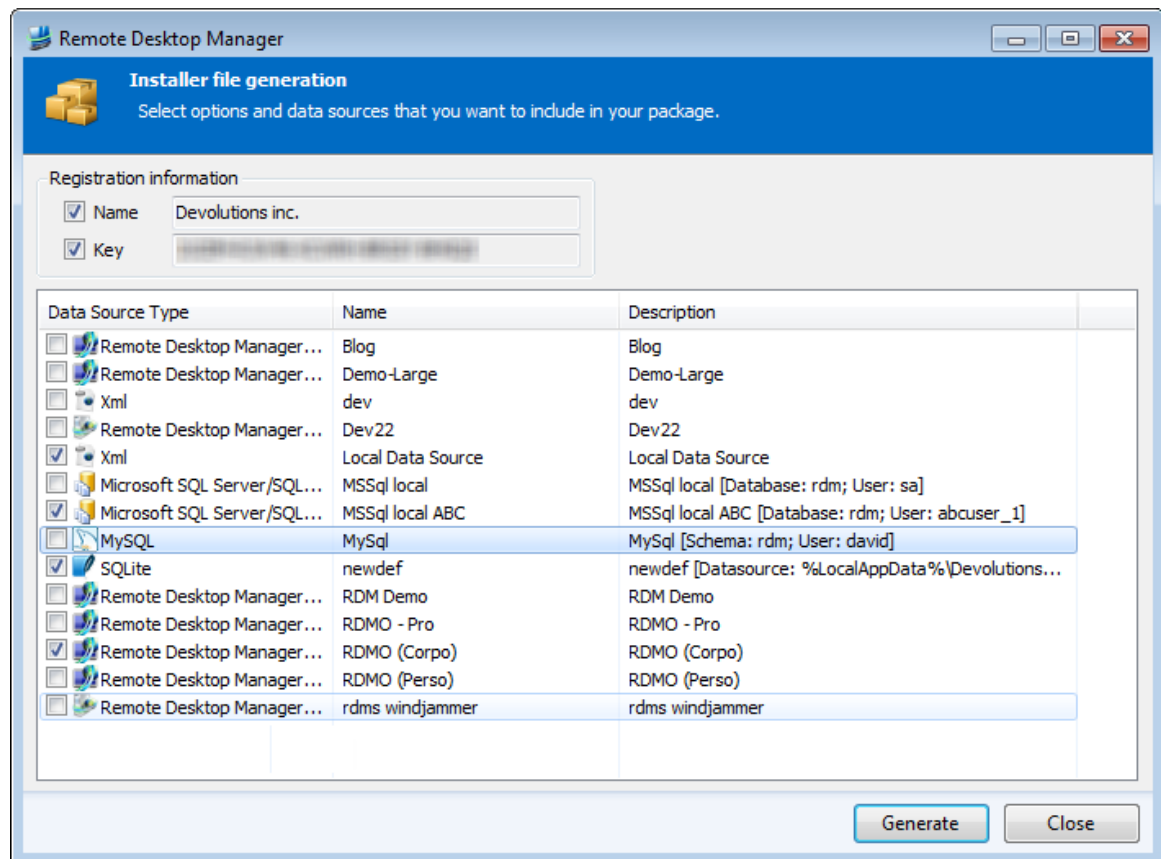
2.1.5.3 Installer File Generation

Description

When creating an installation package with the Custom Installer Manager, users have to choose what data sources to distribute. Instead of having to perform the same selections for all future updates, which can be a source of errors, you can instead perform the selection once, and reuse the resultant file.

Procedure

After launching the tool, you are presented with a form to select which data sources to include. You can also include the name and serial key for the registration.



Clicking on Generate will display a file save dialog for you to name the file.

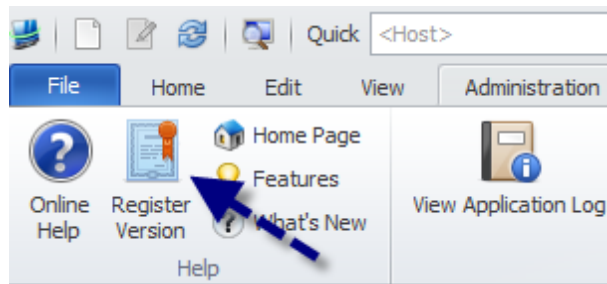
This file can be used in the Custom Installer Manager when creating an installation package. Please see [Create an Installation Package](#) for details.

2.1.6 Registration

2.1.6.1 Register Enterprise Edition

Instructions

To register or select a version, go in the menu **Help > Register Version**.

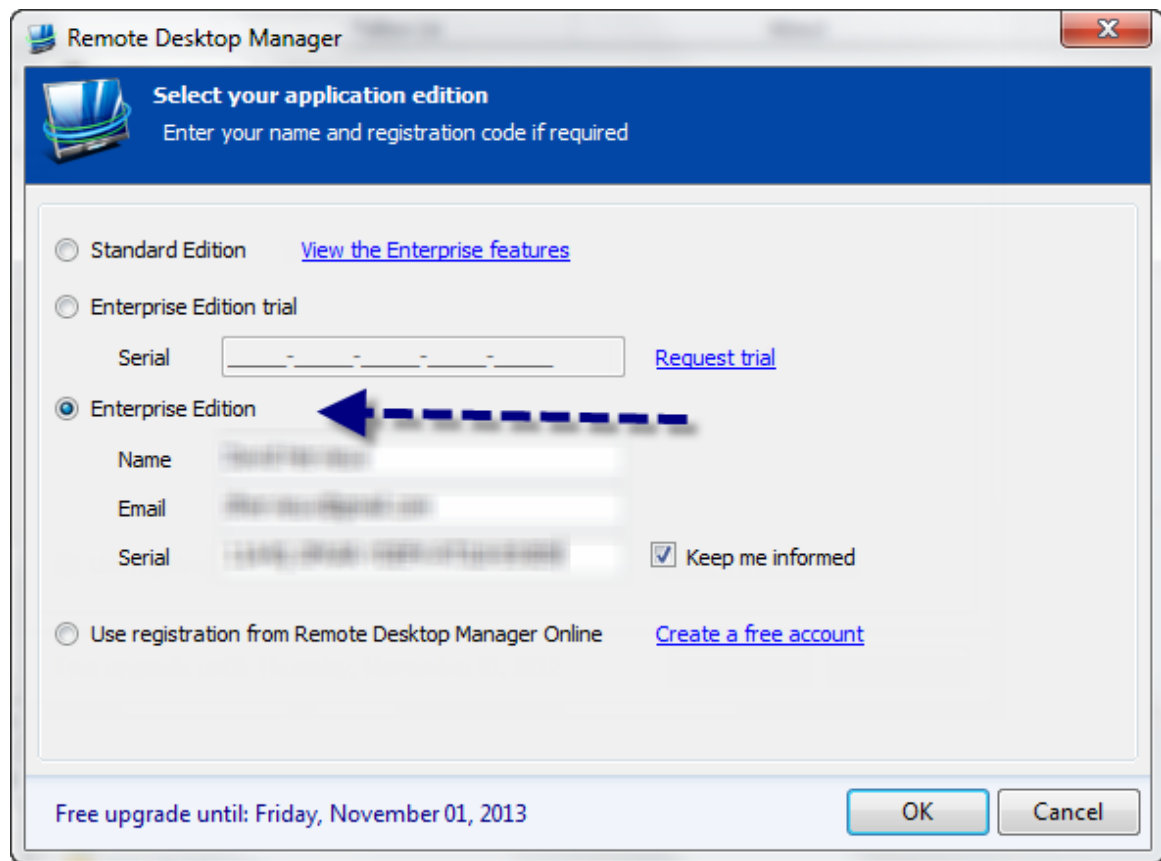


Register button

Enterprise Edition

After you receive our email with your serial number, you can register the application and unlock the Enterprise features.

Enter the user name and serial number exactly as noted in the email.

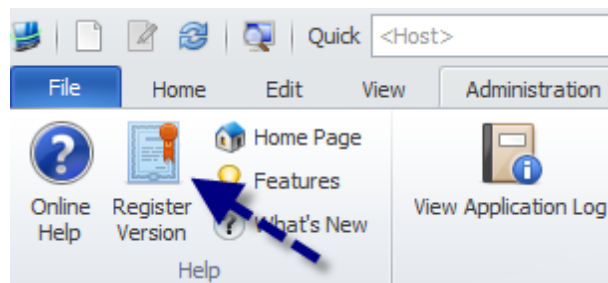


Registration Dialog

2.1.6.2 Register Standard Edition

Instructions

To register or select a version, go in the menu **Help > Register Version**.



Register button

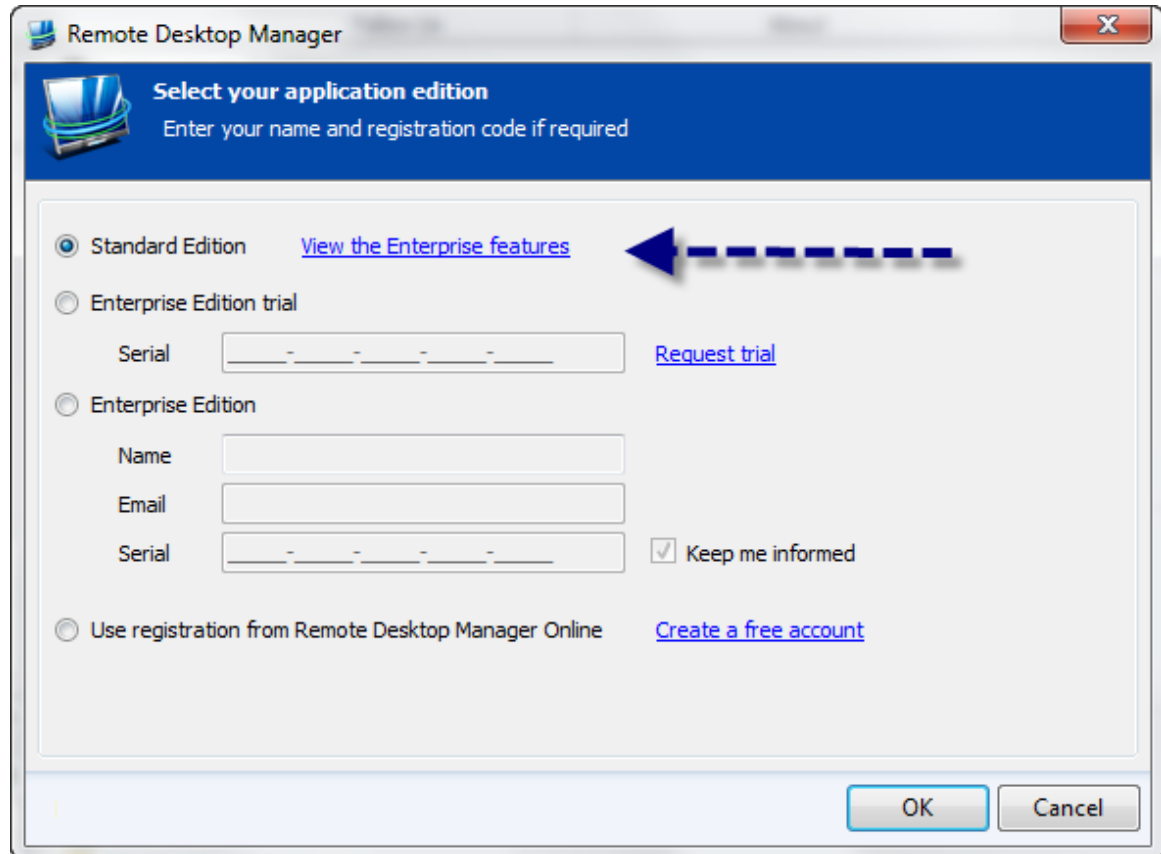
Standard Edition (Free Edition)

The standard edition is free for personal and commercial usage. The 30-day trial exists to allow you to test the application without having to register.



You can wait for the end of your 30-day trial to register. Alternatively you can switch immediately to the Standard edition by clicking on the Registration button. Registration is mandatory at the end of the 30-day trial.

Select Standard edition and close the dialog.



Registration dialog

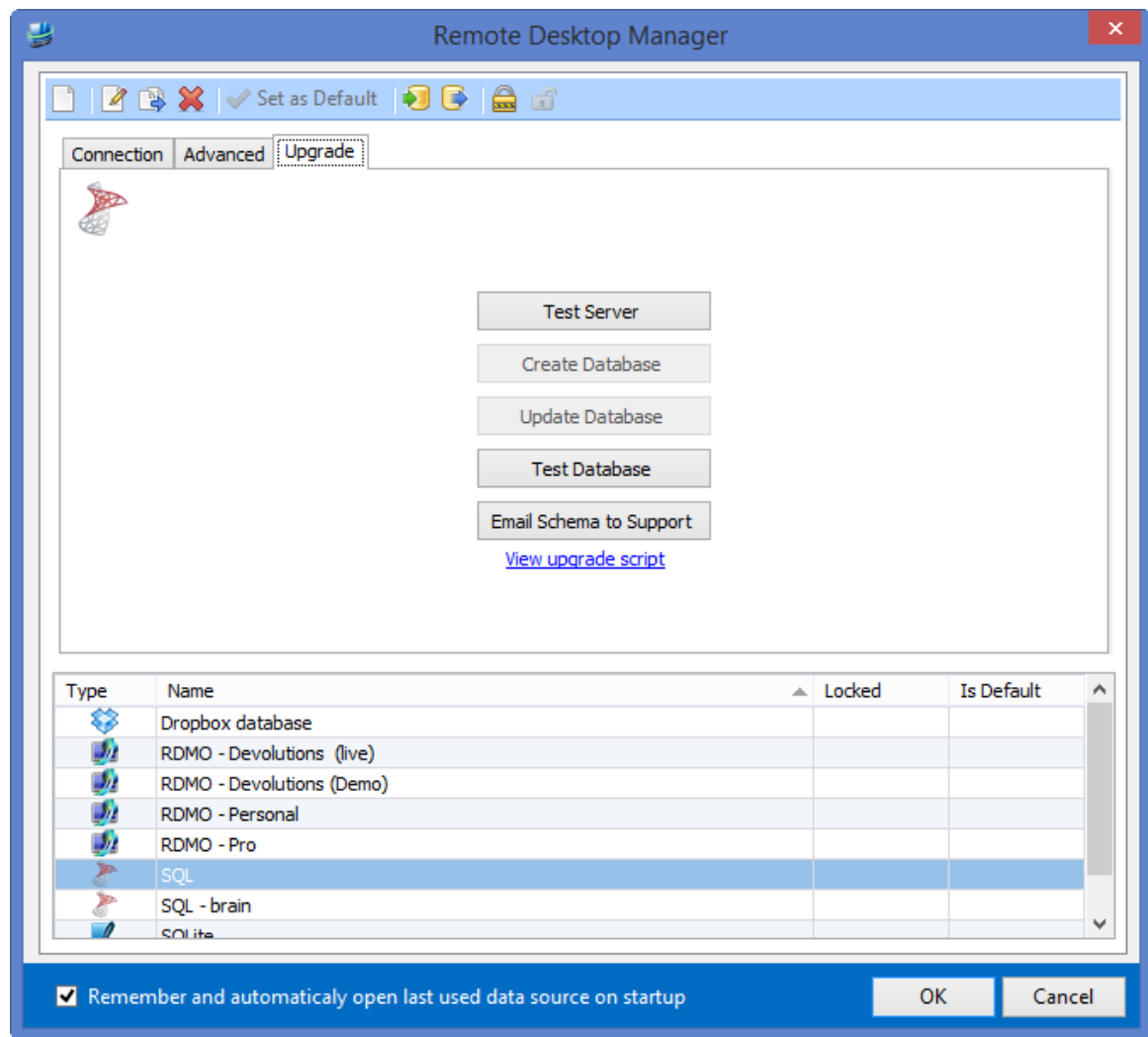
2.2 Database

2.2.1 Upgrade

Description

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

Settings



Data Sources Upgrade tab

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

Follow these steps for a successful version upgrade.

1. Ensure you are the sole user of the database during the upgrade process.
2. Backup your database using the DBMS tools.
3. Open Remote Desktop Manager while logged on as a user with administrative rights. You must also be **SYSDBA** or **DB_OWNER**.
4. You may be prompted with an upgrade message when your data source is accessed. If so accept the upgrade.
5. Update the client software on all workstations.

Please consult topic [Data Source Settings](#) for more information.

2.3 Others

2.3.1 Add-ons

Description

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

You can find the list [here](#) and download them directly from our website.

Add-on Manager

Consult the Add-on Manager [topic](#) for more details.

2.3.2 Configure SQL Server

Server Computer

1. Install Remote Desktop Manager Enterprise on the machine.
2. Install SQL Server or SQL Server Express (this version is free)

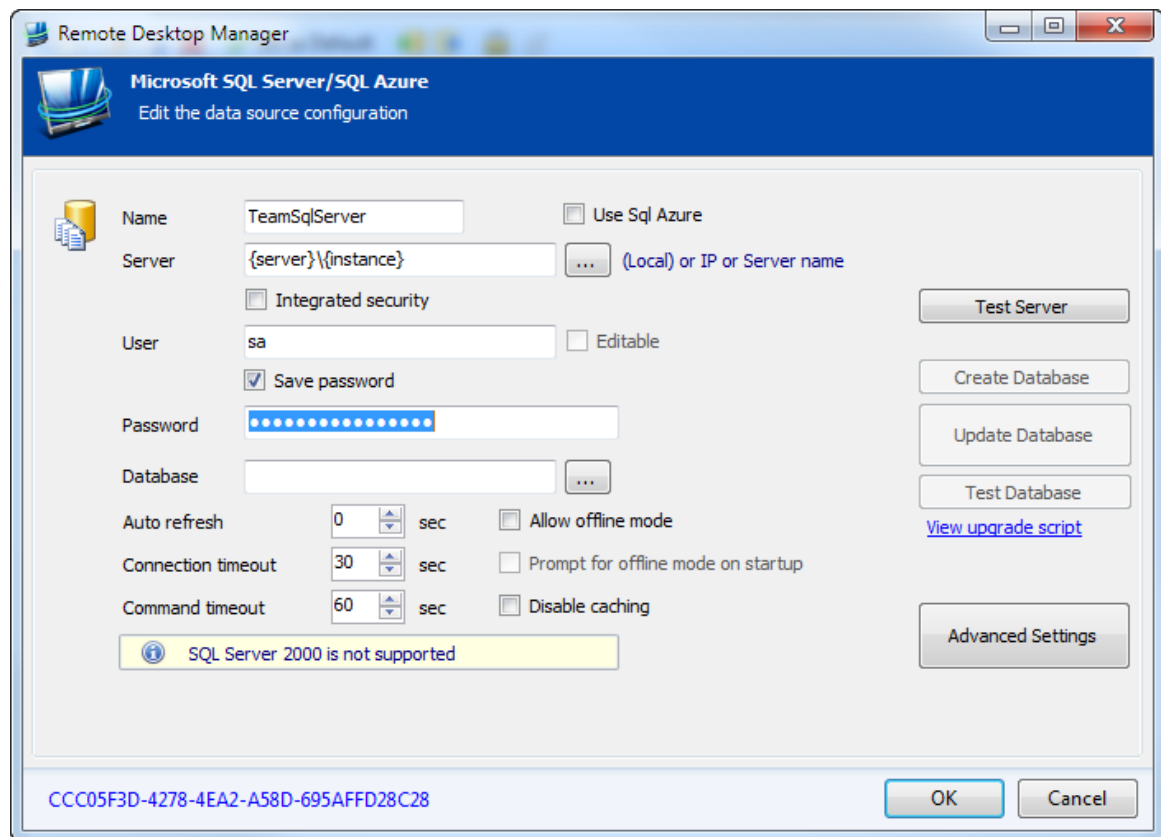


Newly installed SQL Server instances do not allow remote connections. Please follow the directions in [SQL Server](#).



If you wish you can enable SSL Encryption to communicate with your instance of SQL Server.
Please follow directions on <http://support.microsoft.com/kb/316898>

3. To create an empty database, select **File -> Data Sources**, select **New** then choose Microsoft SQL server in the list.
4. Configure the connection test using **Test server**.



SQL Server/SQL Azure data source configuration

5. Enter a name for the database and click **Create Database**.
6. Create and configure security access for any other user needed in Remote Desktop Manager **File** -> **Administration** -> **Users**

Client Computer

1. Install or unzip Remote Desktop Manager Enterprise on the machine.
2. Configure Remote Desktop Manager to connect directly to the SQL Server (use the machine name and SQL Server instance name).
3. You can configure the connection in the menu: **File** -> **Data Sources**.
4. Click on **Add SQL Server Data source**.
5. Configure the connection settings and test the connection.

2.3.3 Embedded Firefox

Description

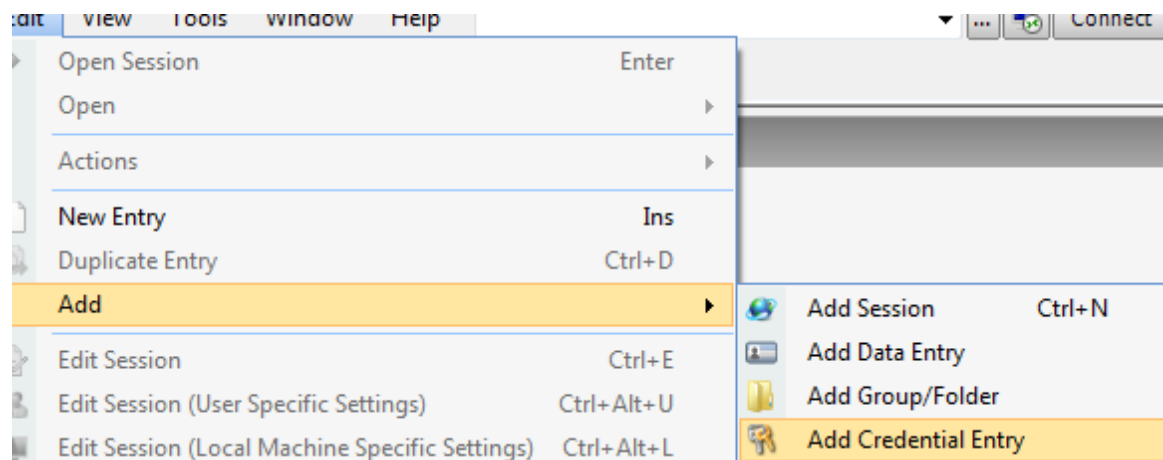
When running an embedded Firefox session, a third party is required to launch the browser. If its not installed you will be presented with a dialog to download a zip file. Unzip the content in a folder of your

choice and use the ellipsis button to select the executable from the folder where you've unzipped the archive.

2.3.4 KeePass Plug-in

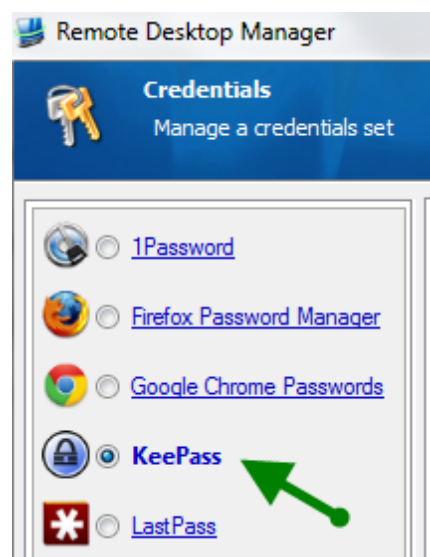
Preparing KeePass:

1. Make sure that KeePass is closed.
2. Open Remote Desktop Manager and add a new credential entry menu **Edit->Add->Add Credential Entry**.



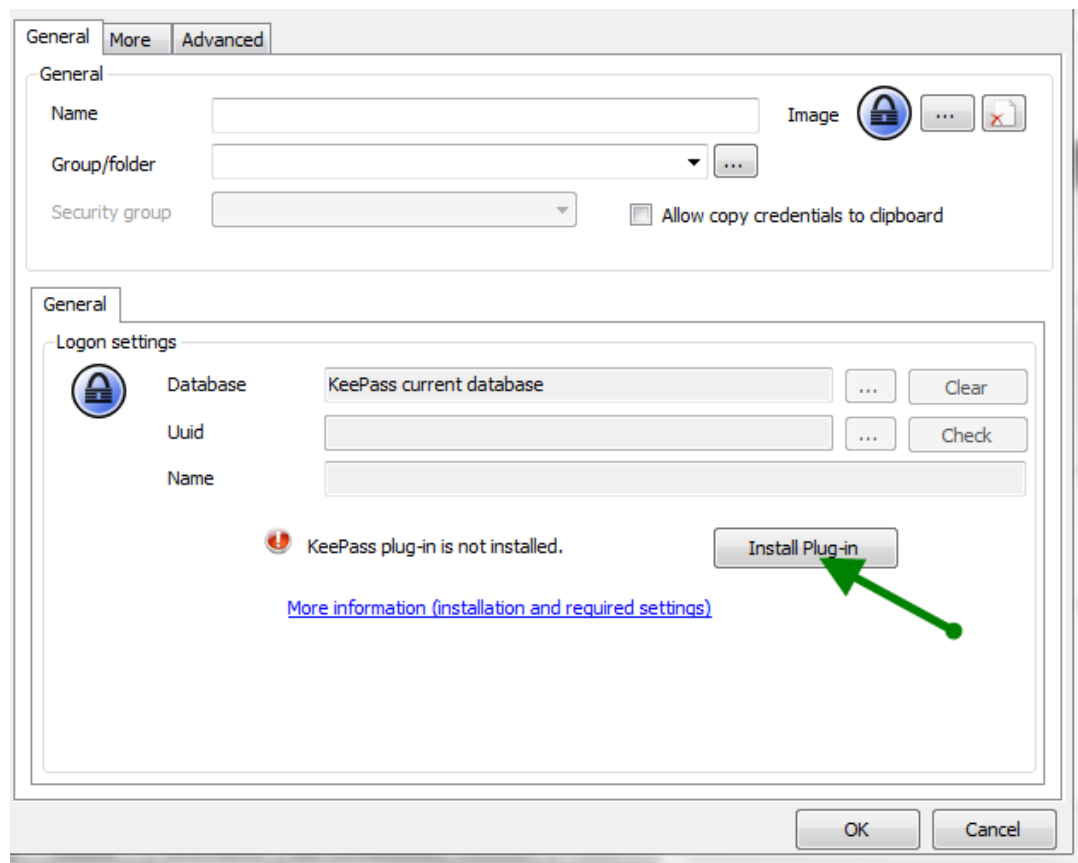
Add credential entry

3. From the list, select KeePass.



KeePass

4. Verify KeePass plug-in status. If installation is required, click the "Install Plug-In" button (For manual installation see next step).



Install the KeePass plug-in

4. If manual installation is required,
 - Browse to <http://remotedesktopmanager.com/Home/ExternalAddOns>.
 - Download the Remote Desktop Manager Plug-in for Keepass
 - Unzip in **KeePass** application folder

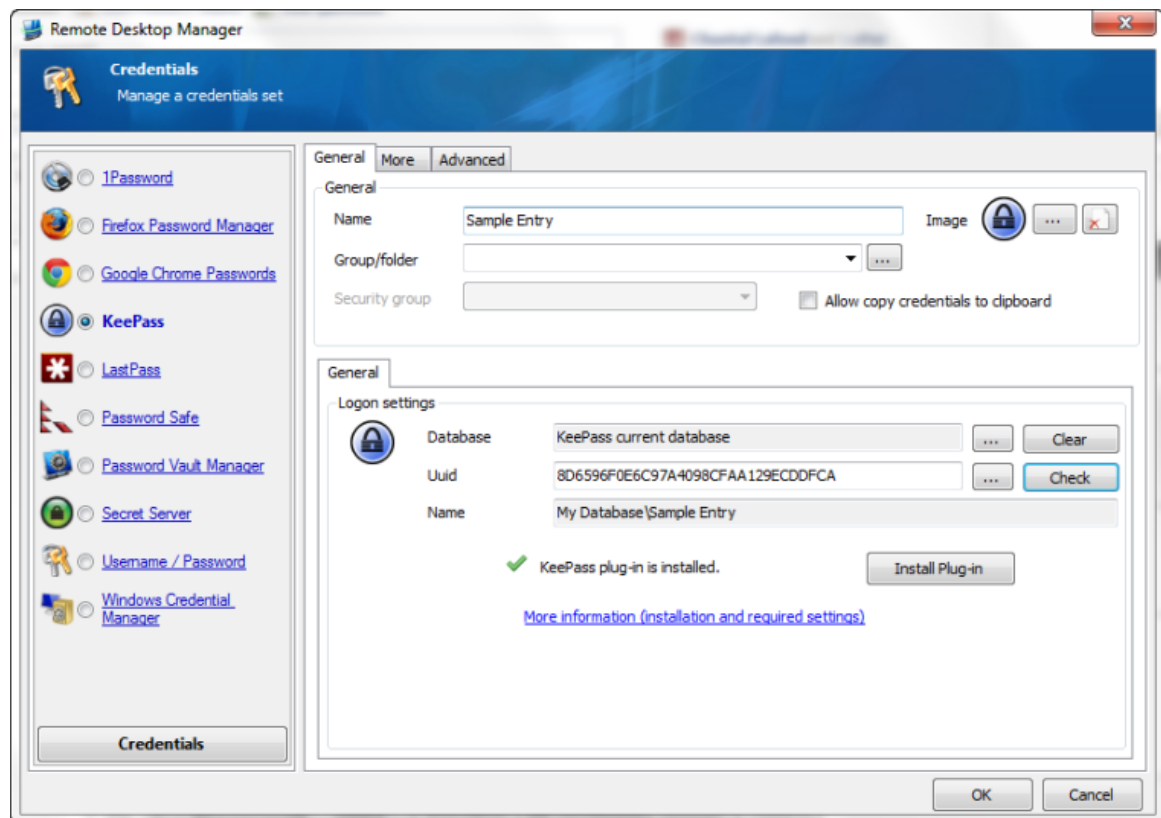


The plugin will not work if the KeePass is installed on a network drive.

5. Restart KeePass.

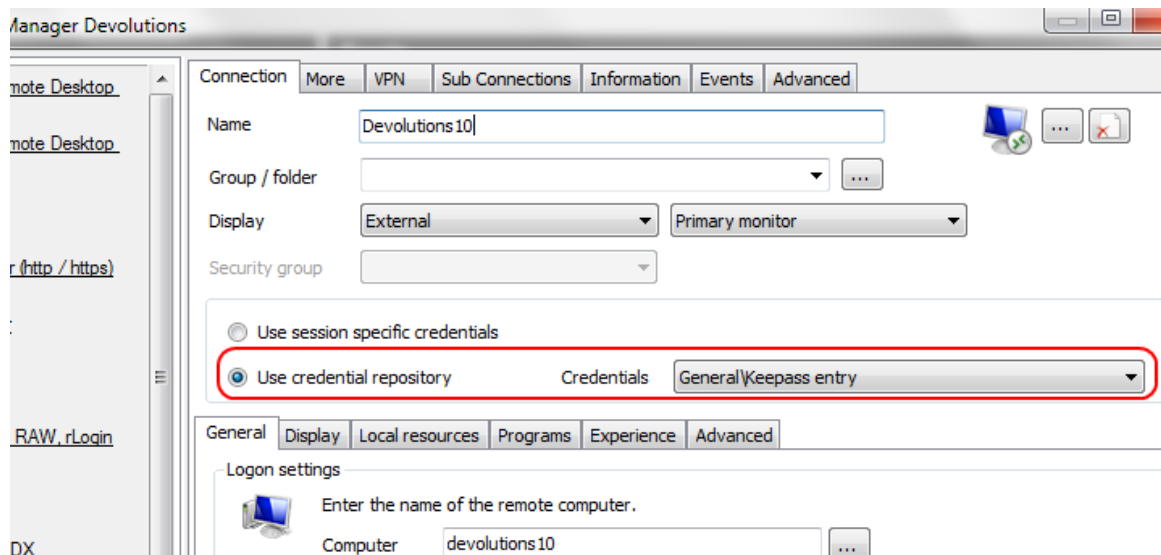
Configuring a session in Remote Desktop Manager:

1. Create a new credential session (Menu->Edit->Add->Credential Repository).



New credential session

2. Select KeePass, and enter the Uuid. Click the "Check" button to confirm.
3. Use the newly-created credential entry in an existing session.



Use credential repository

Integrating KeePass with Remote Desktop Manager:

We've created a brief video on integrating KeePass with Remote Desktop Manager. Learn how to easily and efficiently create automatic logins for a Remote Desktop connection or any supported connection type (e.g. LogMeIn, Telnet, Citrix, VNC, TeamViewer, FTP, VPN, and more).

http://www.youtube.com/watch?v=OE876qZv_UU

2.4 Uninstall

Instructions

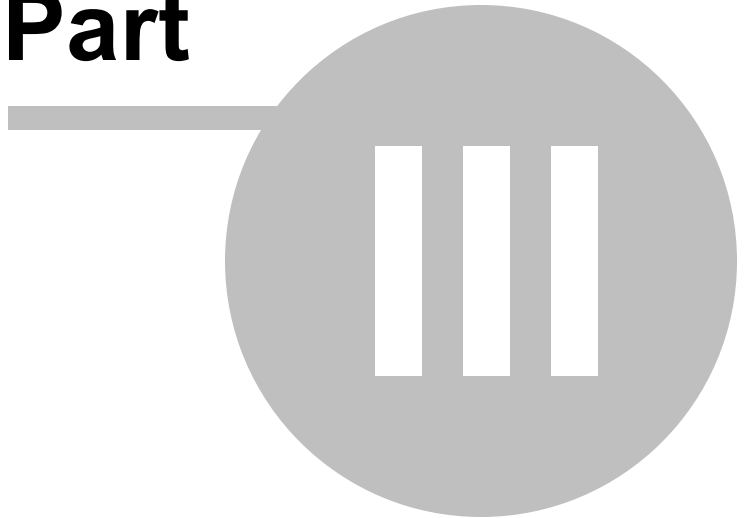
Remote Desktop Manager does not install anything in the Windows system directory, and the only registry settings created are for the auto run functionality and the installation path. As a result, Remote Desktop Manager can be uninstalled easily.

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.

You can also manually delete the content of **"%LocalAppData%\Devolutions\RemoteDesktopManager"** or **"%AppData%\Devolutions\RemoteDesktopManager"**

Commands

Part



3 Commands

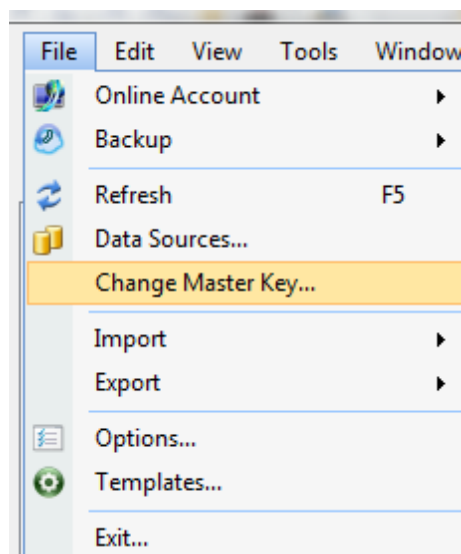
3.1 File

3.1.1 Master Key

Description

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

- Xml
- Dropbox



Change Master Key menu

It is generally a good idea to apply a Master Key to your XML or Dropbox Data Sources, as it adds another layer of security protecting your Remote Sessions. It is highly advisable to implement the Master Key functionality of Remote Desktop Manager if you're using Remote Desktop Manager in a portable environment (i.e. USB Flash Drive, USB Hard Drive), or if the Data Source is the portable portion of the application.

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

3.1.2 Go Offline/Online

Description

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



This feature is only available when using an [Advanced Data Source](#). There are also settings in both the data source and the user account that may prevent you from using the Offline Mode. Ask your administrator if the menu is not visible.



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

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

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

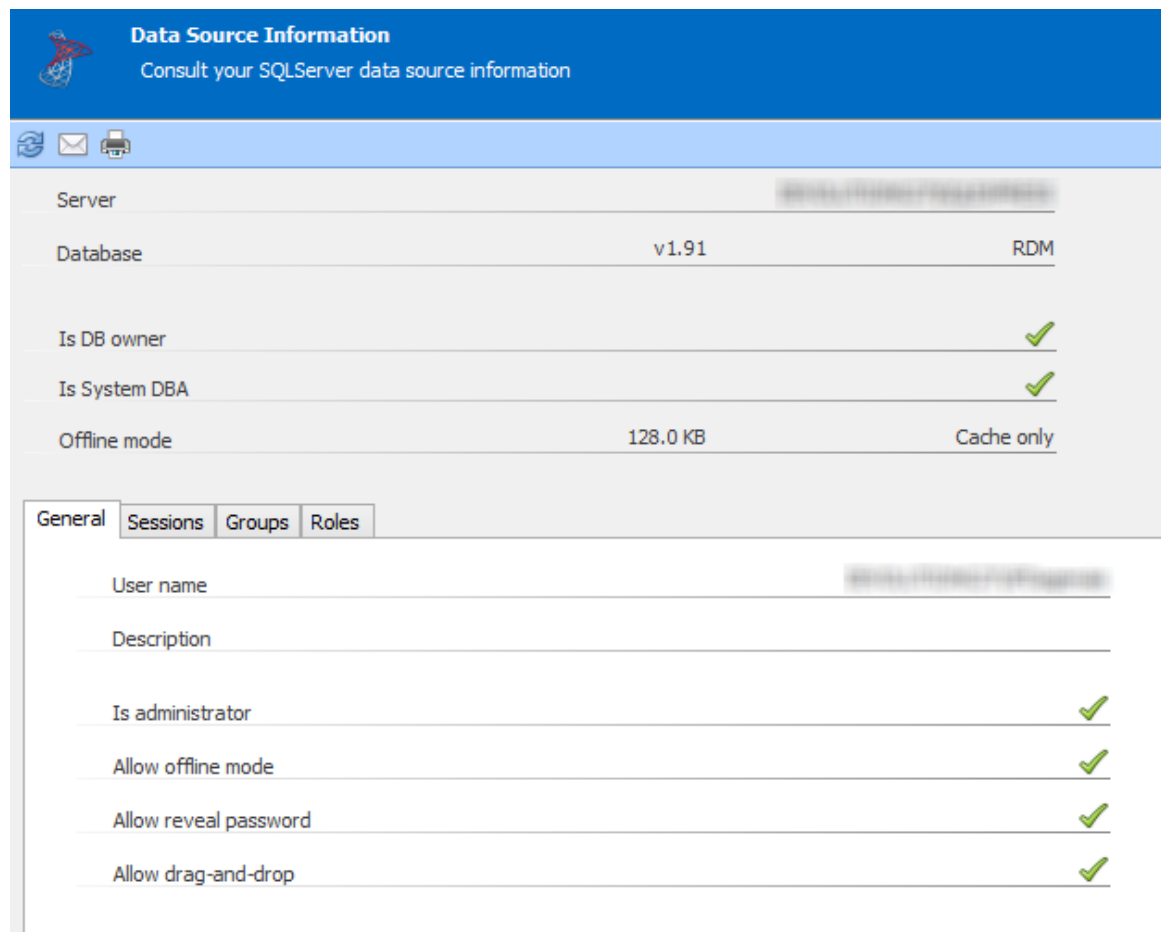
3.1.3 My Data Source Information

Description

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



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



Data Source Information
Consult your SQLServer data source information

Server [Blurred]

Database v1.91 RDM

Is DB owner ☒

Is System DBA ☒

Offline mode 128.0 KB Cache only

General Sessions Groups Roles

User name [Blurred]

Description

Is administrator ☒

Allow offline mode ☒

Allow reveal password ☒

Allow drag-and-drop ☒

My Data Source Information - SQL Server data source

Settings

General



General Sessions Groups Roles

User name [Blurred]

Description

Is administrator ☒

Allow offline mode ☒

Allow reveal password ☒

Allow drag-and-drop ☒

My Data Source Information - SQL Server General tab

The general tab will display information on the data source such as:

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

Sessions

General	Sessions	Groups	Roles
Add sessions			✓
Edit sessions			✓
Delete sessions			✓
View session details			✓
View session information			✓
Import sessions			✓
Export sessions			✓
Allow add entry in root folder			✓

My Data Source Information - SQL Server Sessions tab

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

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

Groups

General	Sessions	Groups	Roles
Group Name		Rights	
Helpdesk		View, Add, Edit, Delete	

My Data Source Information - SQL Server Groups tab

The groups tab will display the groups and the rights into those groups that a user have in the data source.

Roles

General Sessions Groups Roles		
Role Name	Rights	Helpdesk
Manager	View, Add, Edit, Del...	View, Add, Edit, Delete

My Data Source Information - SQL Server Roles tab

The roles tab will display the roles that the user is member of and the rights related to this role.

Offline Mode

The offline mode will display the size of the offline file along with the effective mode (disabled, read-only or writable). Hover the mouse over the offline mode to get the full offline mode display.

Data source settings: Read/write
User settings: Read/write
Data source config.: Read/write

Offline Mode - tool tip

For more information see [Offline Mode](#)

3.1.4 Online Services

3.1.4.1 Backup

Description

The Online Backup Service (available via subscription) allows you to automatically save your entries safely in an online storage space, and restore them in the event of problems.

The Online Backup Service is the simple, reliable and cost-effective way to avoid losing all of your valuable data and settings due to a human error or an equipment failure.



The Online Data is encrypted using a client key, therefore it is impossible for Devolutions to access your information.

Available for both the Standard and Enterprise edition, this affordable backup solution works with XML, Microsoft Access and SQLite data source in Remote Desktop Manager.



The PRO subscription adds event history to the BASIC subscription. For current pricing please visit

<http://remotedesktopmanager.com/remotedesktopmanager/Home/OnlineBackup>

Configuration Instruction

1. On Remote Desktop Manager's main screen, on the bottom right corner, click on the backup logo to configure the automatic backup. If the logo is not active, it means you are currently on an unsupported data source.

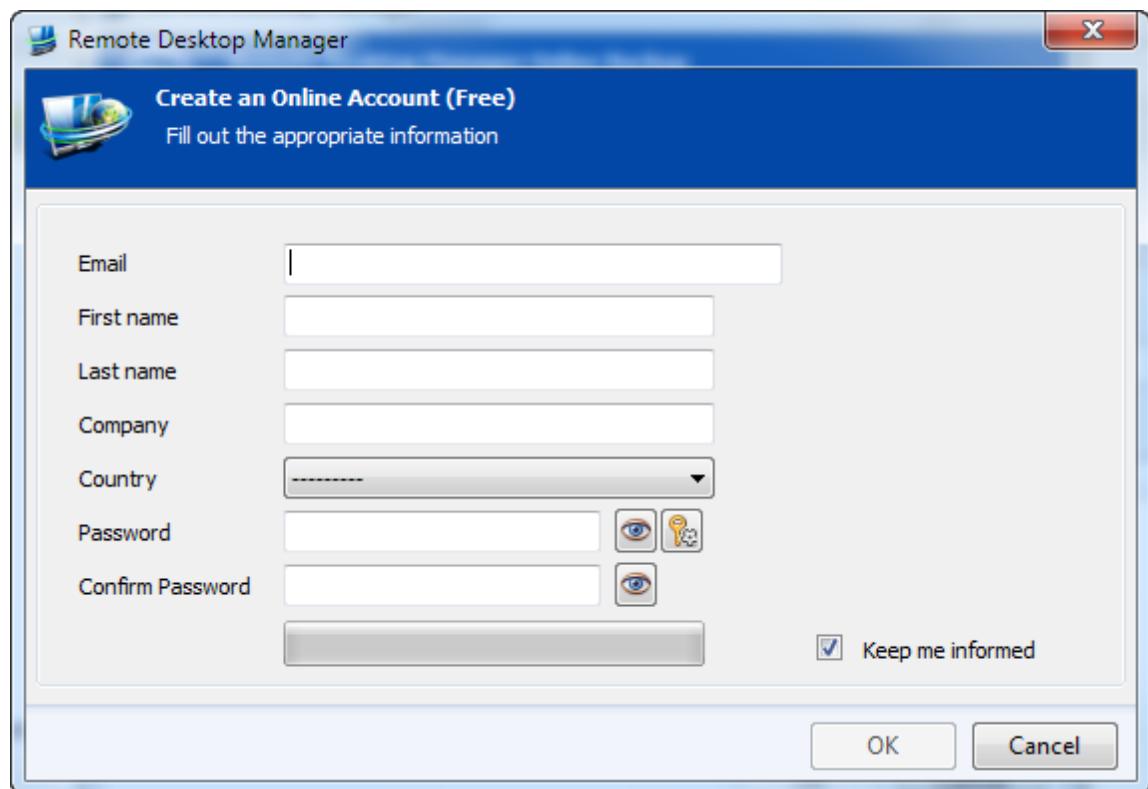


Backup logo

The following form will appear

Remote Desktop Manager Online (RDMO) information

2. If you don't have a Remote Desktop Manager Online account, select **Create a free account** and fill in the information.

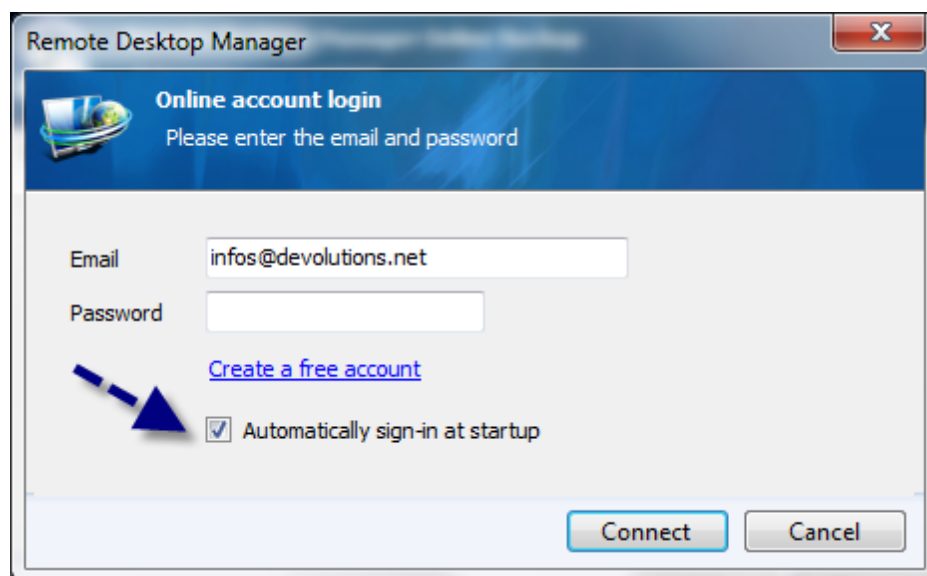


The screenshot shows the 'Remote Desktop Manager' window with the title 'Create an Online Account (Free)'. Below the title is the instruction 'Fill out the appropriate information'. The form contains the following fields and controls:

- Email: A text input field.
- First name: A text input field.
- Last name: A text input field.
- Company: A text input field.
- Country: A dropdown menu.
- Password: A text input field with an eye icon and a key icon to its right.
- Confirm Password: A text input field with an eye icon to its right.
- Keep me informed: A checked checkbox.
- OK and Cancel buttons at the bottom right.

RDMO Account creation

3. Login with your Remote Desktop Manager Online account and check "Automatically sign-in at startup" so that the backup will be automatically enabled at your next startup.



The screenshot shows the 'Remote Desktop Manager' window with the title 'Online account login'. Below the title is the instruction 'Please enter the email and password'. The form contains the following fields and controls:

- Email: A text input field containing 'infos@devolutions.net'.
- Password: A text input field.
- Create a free account: A blue hyperlink with a blue arrow pointing to it.
- Automatically sign-in at startup: A checked checkbox.
- Connect and Cancel buttons at the bottom right.

Account login



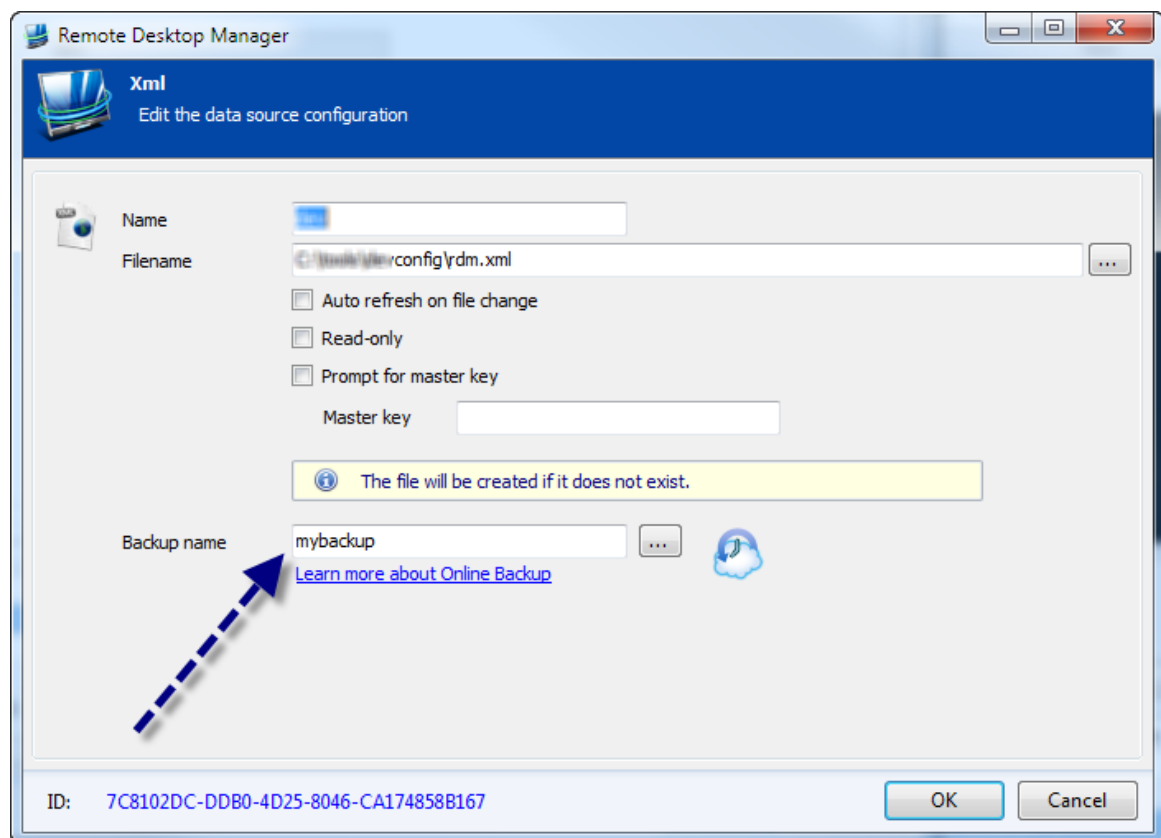
For forgotten passwords or locked accounts you must go online to use the forgot password feature. Please visit <https://online.remotedesktopmanager.com/> to proceed.

4. Enter the serial for your subscription. You can click on **Buy** in order to purchase or you can request a trial on <http://remotedesktopmanager.com/remotedesktopmanager/Home/OnlineBackup>.

5. You will need to specify a unique backup name, for each of your desired data sources, which will be used to backup and restore the data source. Edit your data source settings and fill-in the "Backup Name" field.



You must perform this for all your XML, MS Access and SQLite data sources in order to be fully protected!



Backup Name

6. Once the backup name has been set, the Online Backup logo will display a green check mark showing that the backup is now enabled.



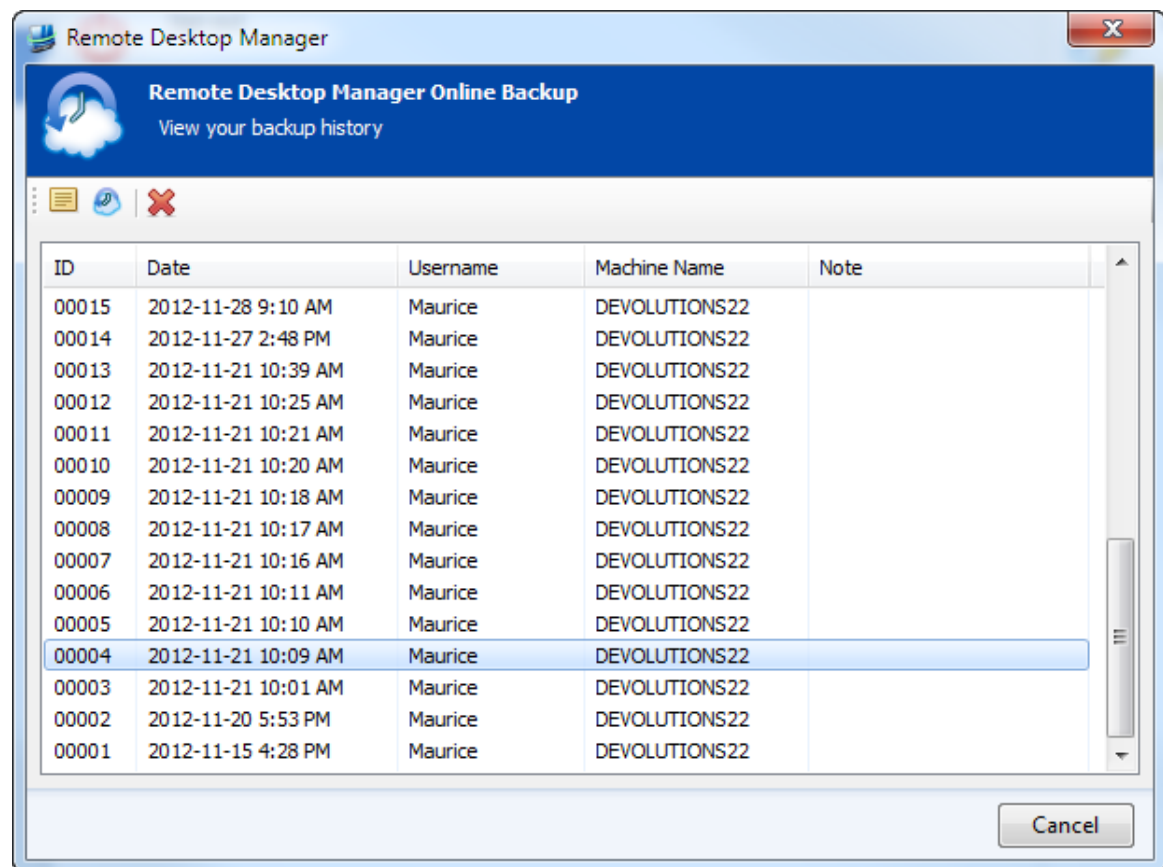
Online Backup logo



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

Restore Instruction

1. To restore a data source from a backup, select it as the current data source.
2. Go to File > Backup > View History to display the list of your backups.
3. Select one from all the available restore points, this will enable the action buttons at the top.
4. Press on the second button to restore. Alternatively Right-click on your chosen backup to display the restore popup menu.



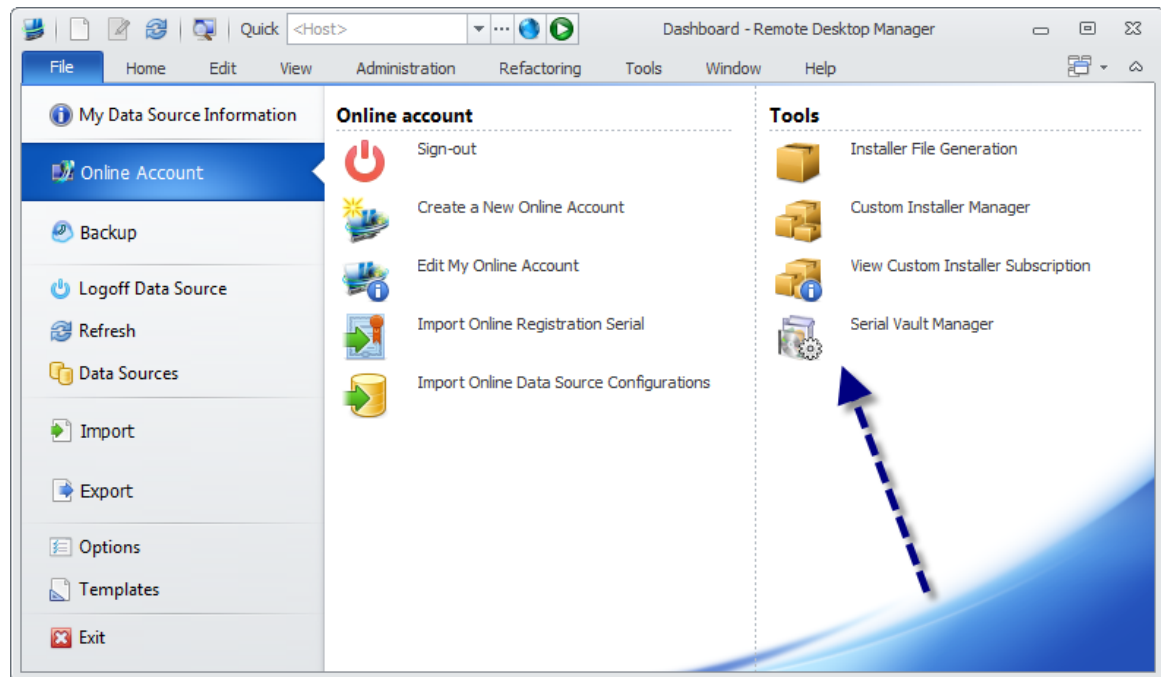
Backup history

3.1.4.2 Serial Vault

Description

The serial vault is part of the Remote Desktop Manager Online subscription. It allows you to store Serial numbers for software licenses that you own. The vault is also available when you log in the Remote Desktop Manager Online site.

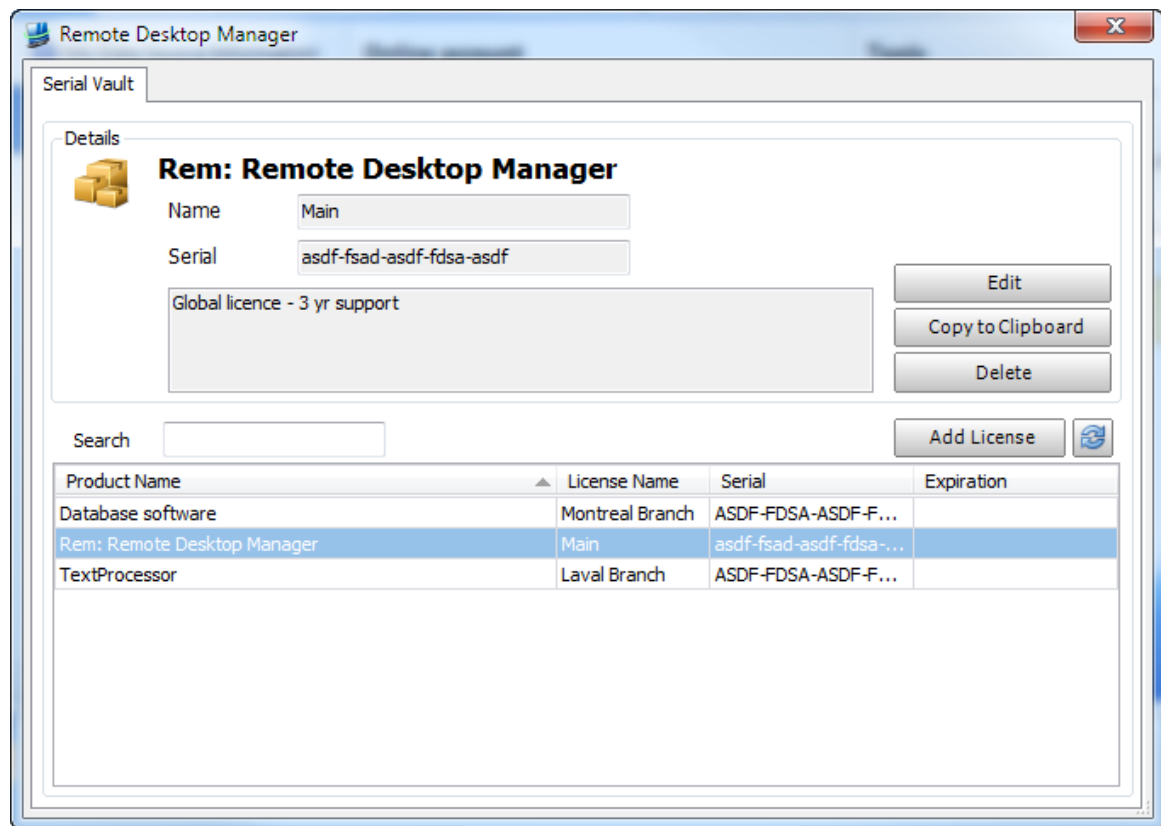
Select **File->Online account**, you will see the Serial Vault Manager link.



Online account access

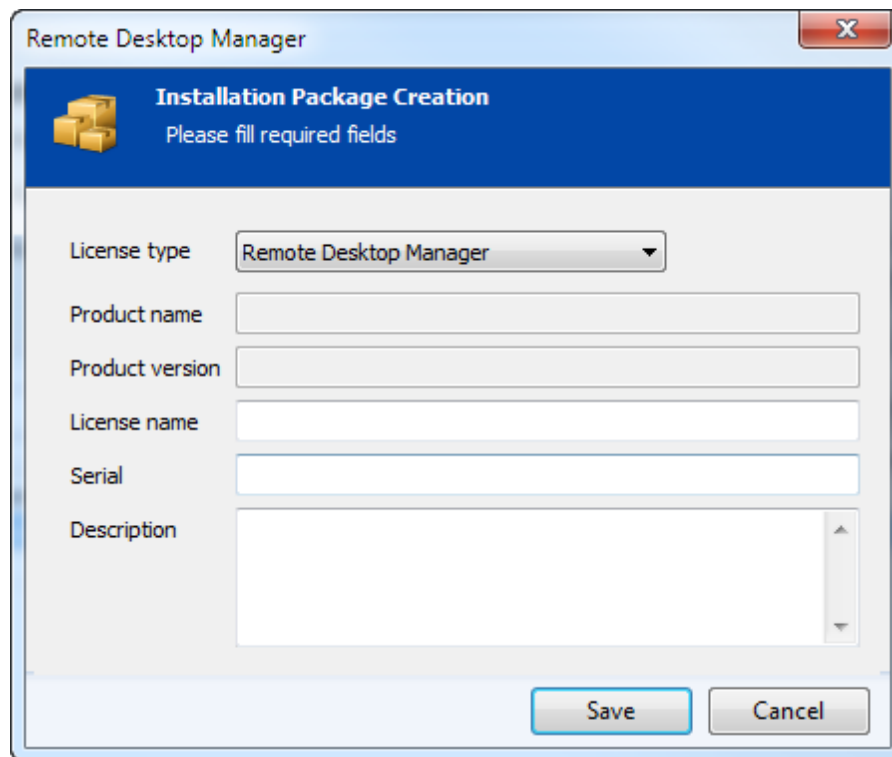
Workflow

Clicking on Serial Vault Manager will display this dialog



Serial Vault Manager

Edit will allow you to edit the serial entry. For your convenience, the copy to clipboard button can be used to quickly be able to paste the serial in a registration window. You can also delete entries or create new ones.

The image shows a Windows-style dialog box titled "Remote Desktop Manager". Inside the dialog, there is a blue header bar with a yellow cube icon and the text "Installation Package Creation" and "Please fill required fields". Below the header, there are several input fields: "License type" (a dropdown menu currently showing "Remote Desktop Manager"), "Product name", "Product version", "License name", "Serial", and "Description" (a text area). At the bottom right of the dialog are "Save" and "Cancel" buttons.

Add license dialog

Selecting "Other" as the License type will activate all controls so you can enter the information as you see fit.

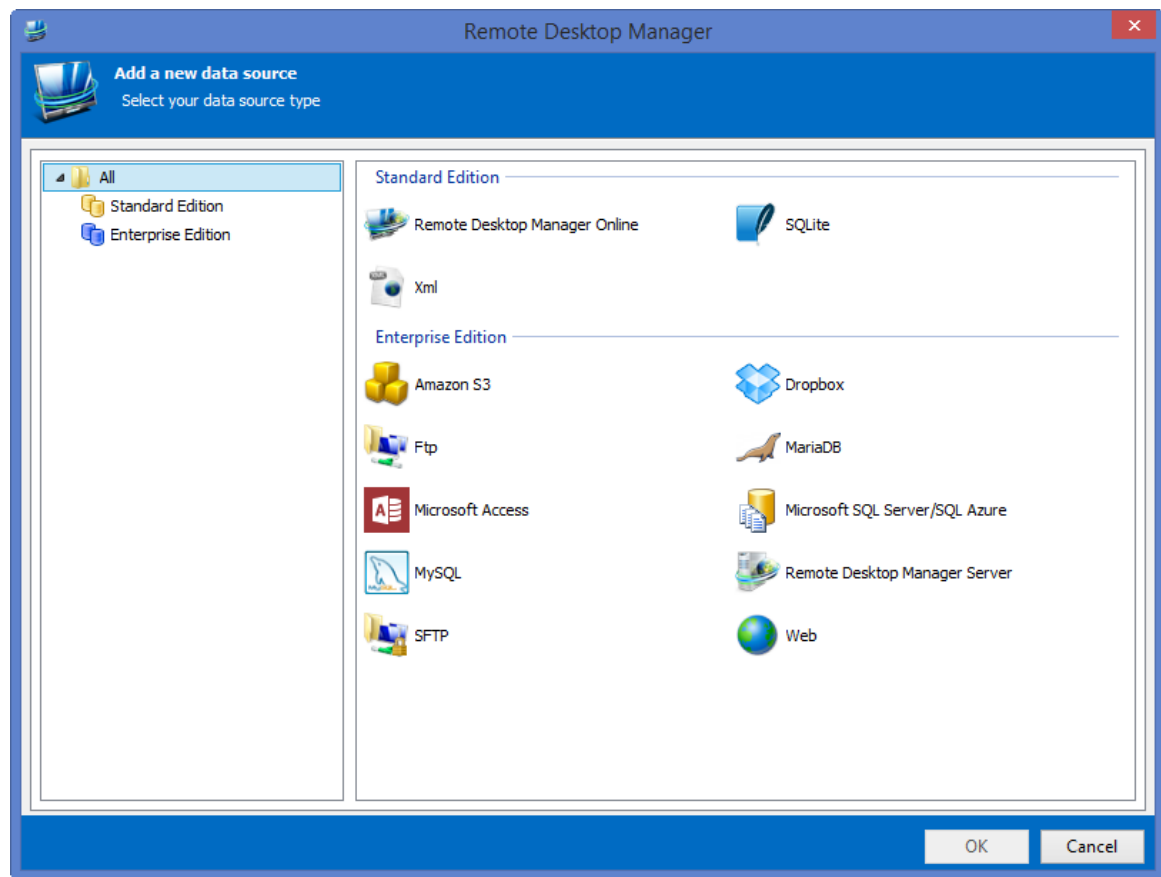
3.1.5 Data Sources

3.1.5.1 Overview

Description

Remote Desktop Manager supports multiple types of data sources. Some are only available with the Enterprise edition.

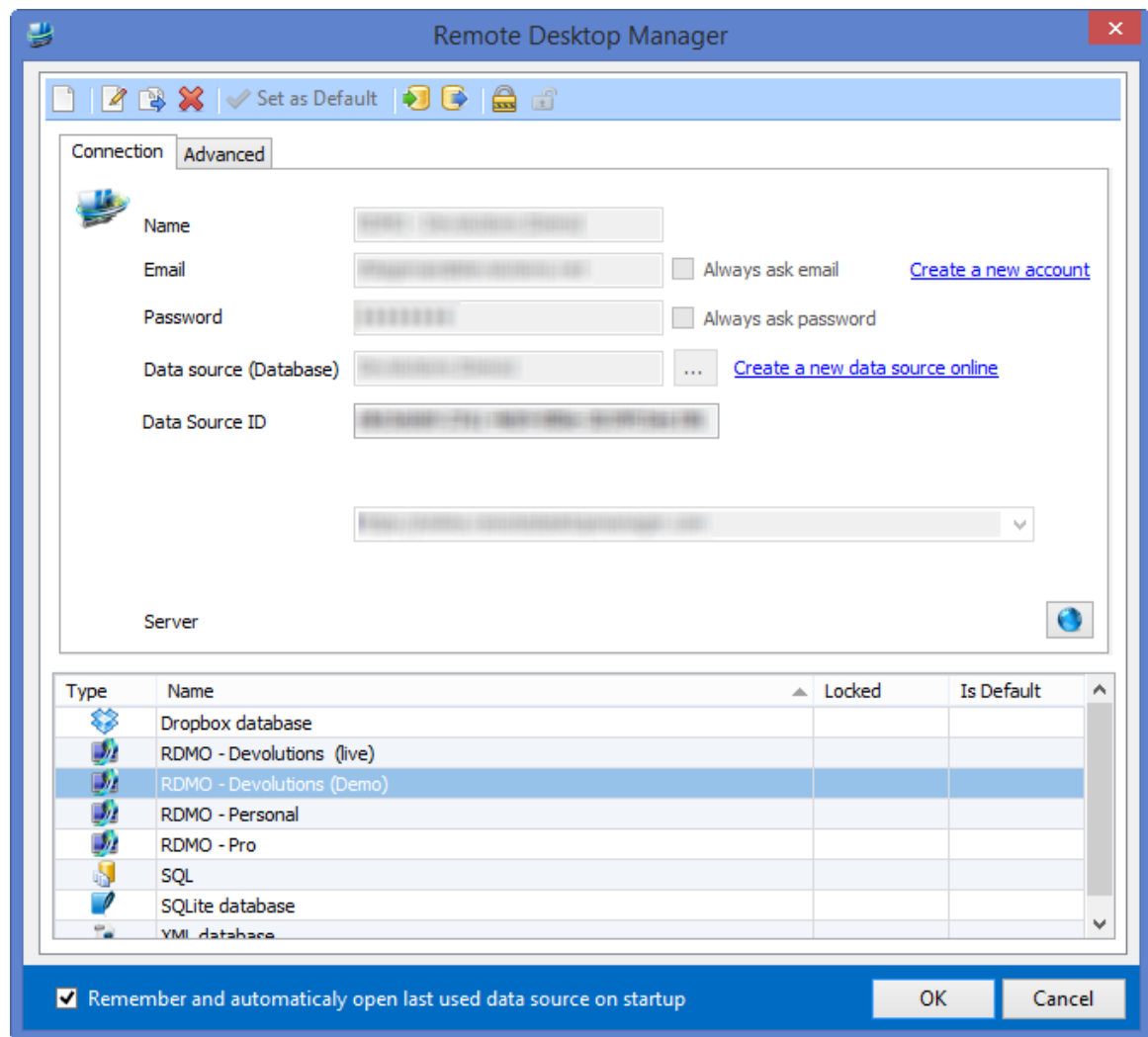
Please refer to the topic [Data Source Types](#) for more details on all types of data sources supported.



New data source

Settings

Use **File -> Data Sources** to manage your data sources.



Data Sources

Add a new data source

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

Edit/Duplicate/Delete data source

Use buttons below to edit, duplicate or delete a data source configuration.





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


Set as Default

Set as default button will set the selected data source to open at startup of Remote Desktop Manager. This feature is not available if *Remember and automatically open last used data source on startup* is enabled.


Import/Export data source configuration

Use buttons below   to import or export the data source configuration. The configuration will be exported in a .RDD file and you will be able to configure another workstation easily.

Lock data source

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

Unlock data source

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

Remember and automatically open last used data source on startup

Remote Desktop Manager will remember the last used data source and will open it on startup.

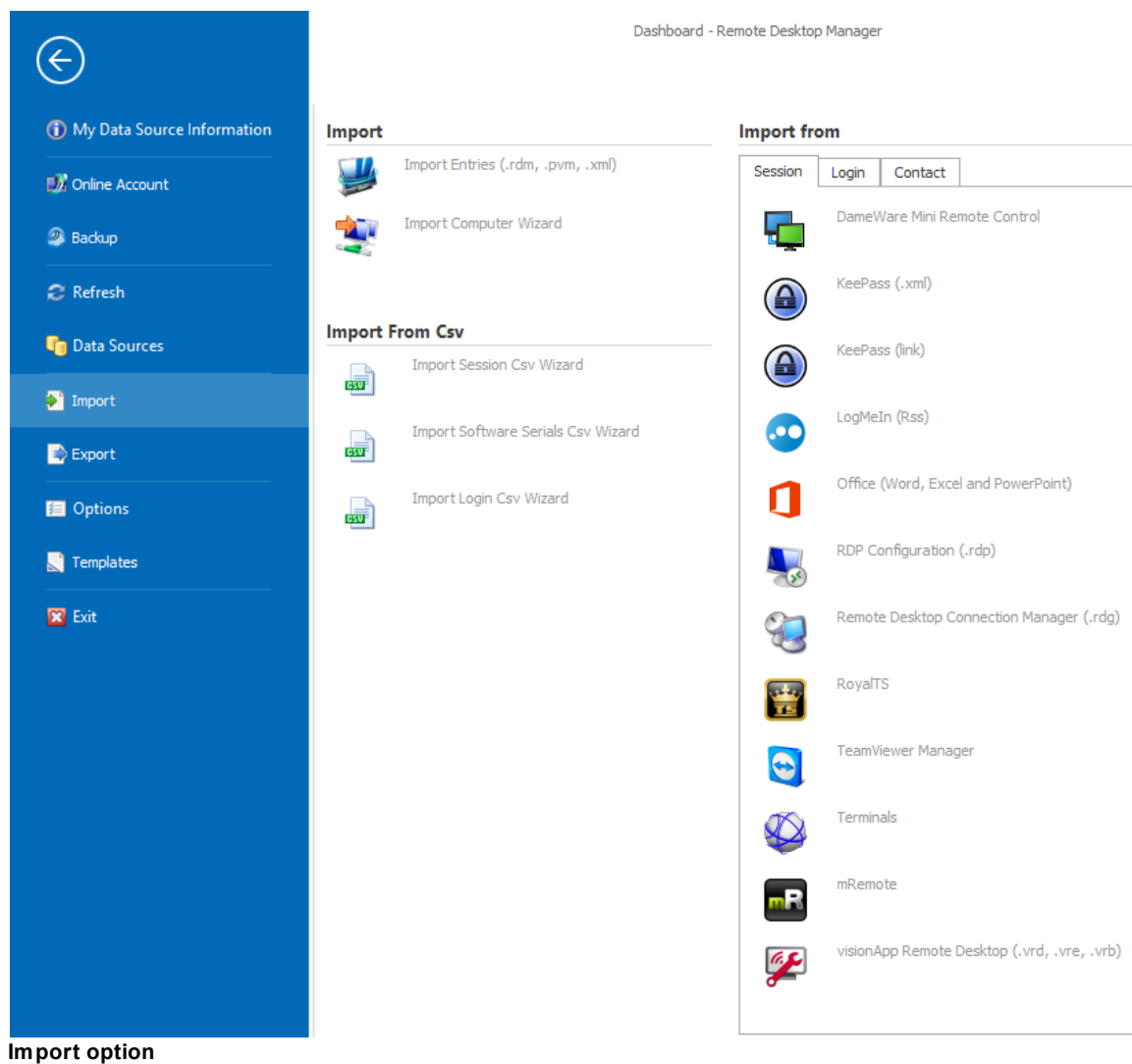
3.1.6 Import

3.1.6.1 Overview

Description

Use the **File -> Import** option to import entries in Remote Desktop Manager. You can import many entry types, and this from a multitude of sources.

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



Import option

Settings

Import Entries

Import Entries is use to import sessions store in file such like:

- .rdm (Remote Desktop Manager native export format)
- .pvm (Password Vault Manager native export format)
- .xml

Import Computer Wizard

You can import your computers list from different sources.

These sources include:

- Network neighborhood
- Your current domain or another domain on your network

- List of computers from a file



The wizard is available in the Enterprise edition.

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.



The entries are import in the current folder.

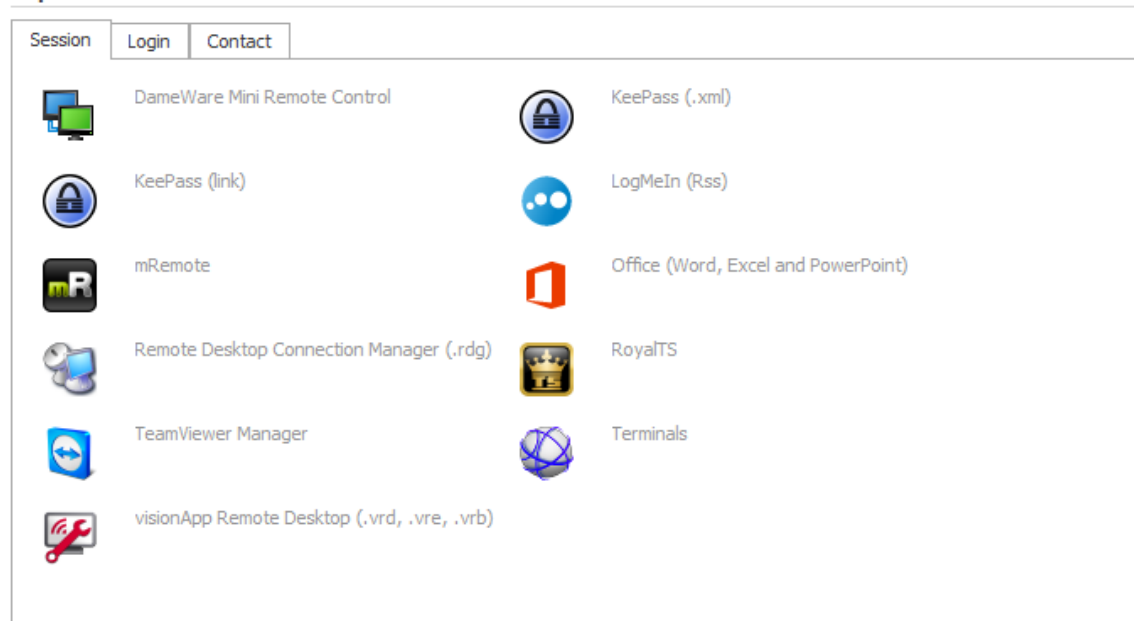
Consult topics below to import sessions, logins and contact from many tools:

- [Import Sessions](#)
- [Import Logins](#)
- [Import Contacts](#)

3.1.6.2 Import Sessions

Description

Use the **File -> Import -> Import from | Session** to import sessions into Remote Desktop Manager.

Import from**Import Session menu**

Settings

Import from Session

You can import sessions from an existing application. Your configuration must not be encrypted for Remote Desktop Manager to be able to parse the content.

The list of the supported applications includes:

- Dameware Mini Remote Control
- KeePass (.xml)
- KeePass (link)
- LogMeIn (Rss)
- Office (Word, Excel and Powerpoint)
- RDP Configuration (.rdp)
- Remote Desktop Manager Connection (.rdg)
- RoyalTS
- TeamViewer Manager
- Terminals
- mRemote
- visionApp Remote Desktop (.vrd, .vre, vrb)



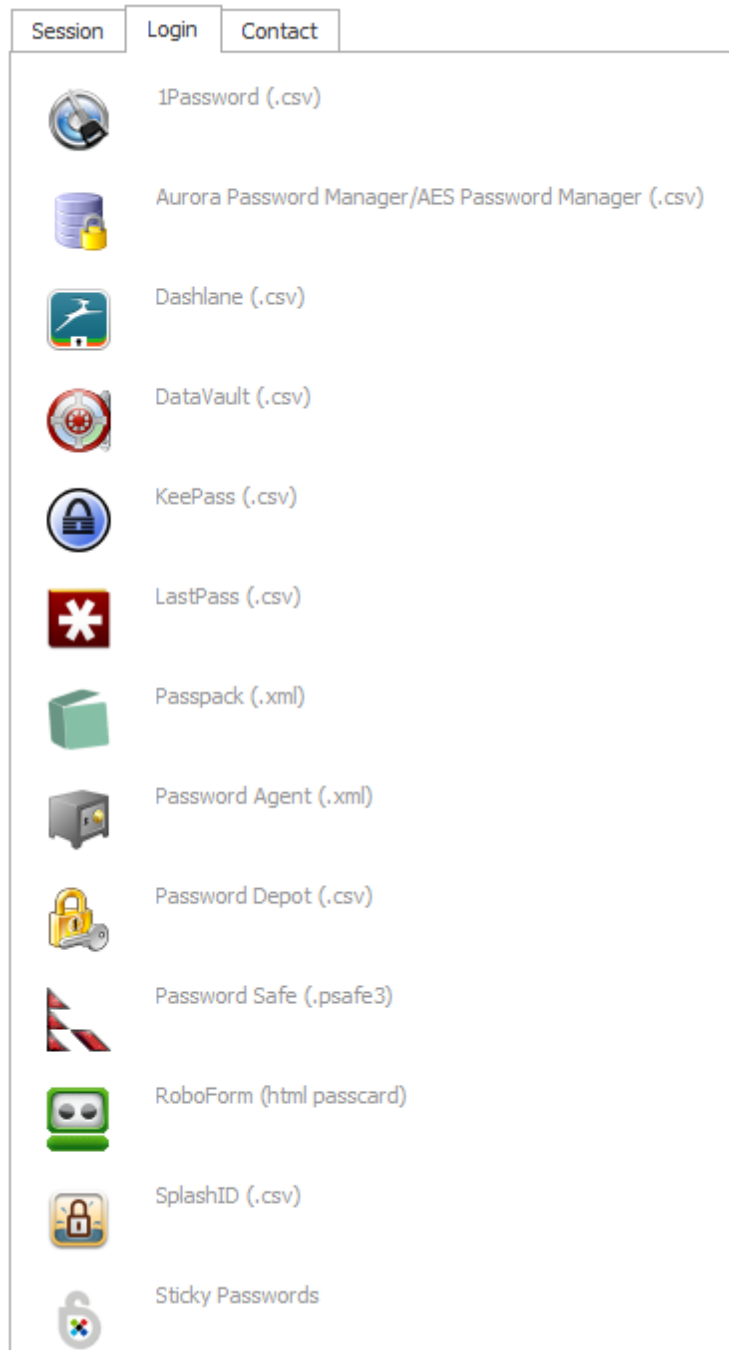
The entries are import in the current folder.

3.1.6.3 Import Logins

Description

Use the **File -> Import -> Import from | Login** to import login into Remote Desktop Manager.

Import from



Import Login menu

Settings

Import from Login

You can import credentials from a wide array of formats that are exported by various password management solutions. Your configuration must not be encrypted for Remote Desktop Manager to be able to parse the content.

The list of the supported applications includes:

- 1Password (.csv)
- Aurora Password Manager/AES Password Manager (.csv)
- Dashlane (.csv)
- DataVault (.csv)
- KeePass (.csv)
- LastPass (.csv)
- Passpack (.xml)
- Password Agent (.xml)
- Password Depot (.csv)
- Password Safe (.psafe3)
- RoboForm (html passcard)
- SplashID (.csv)
- Sticky Passwords (.csv)



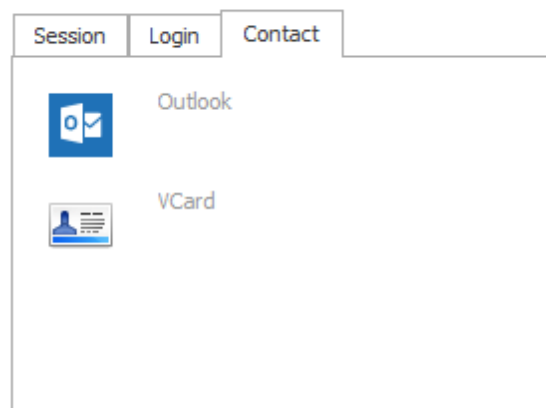
The entries are import in the current folder.

3.1.6.4 Import Contacts

Description

Use the **File -> Import -> Import from | Contact** to import contacts into Remote Desktop Manager.

Import from



Import Contact menu

Settings

Import from Contact

You can import contacts from Microsoft Outlook and from VCard.



Microsoft Outlook contacts sub folders import is supported.



The entries are import in the current folder.

3.1.7 Export

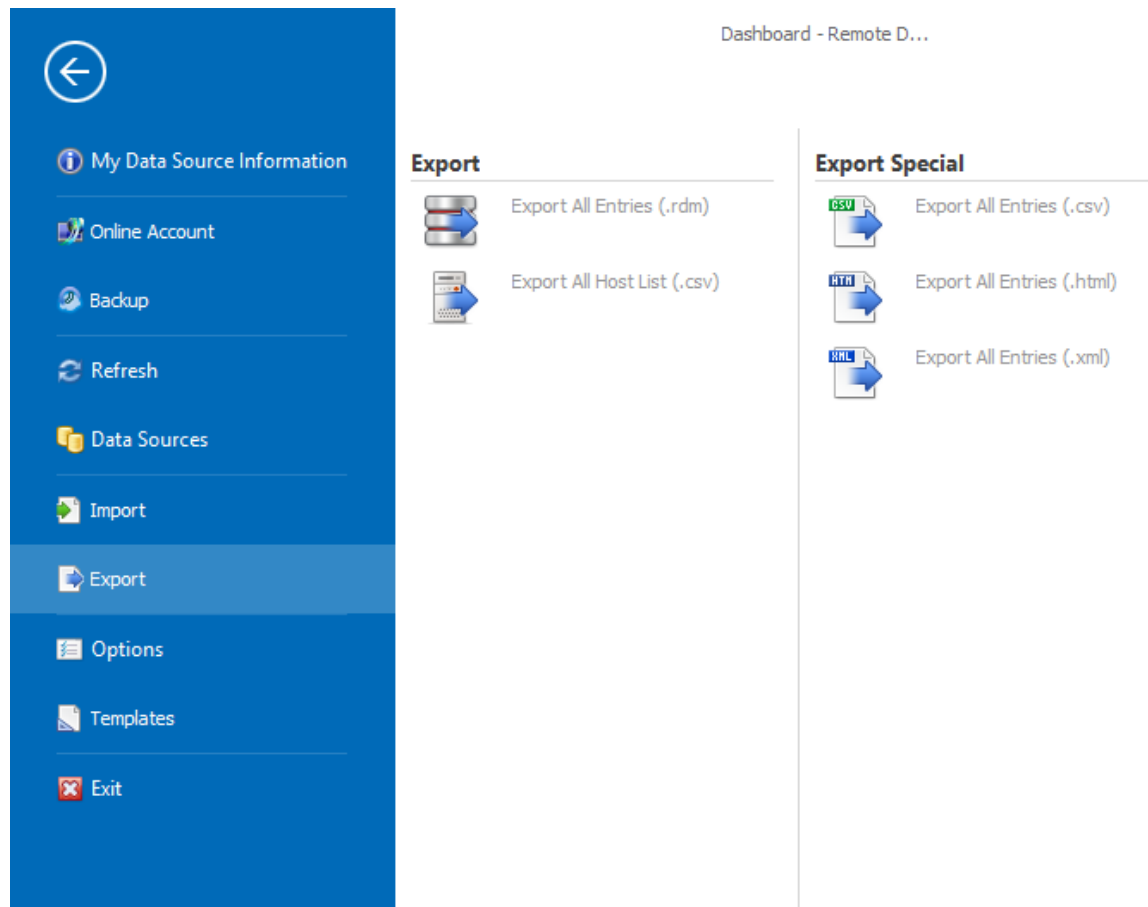
3.1.7.1 Overview

Description

Remote Desktop Manager supports many export options. 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.

Settings

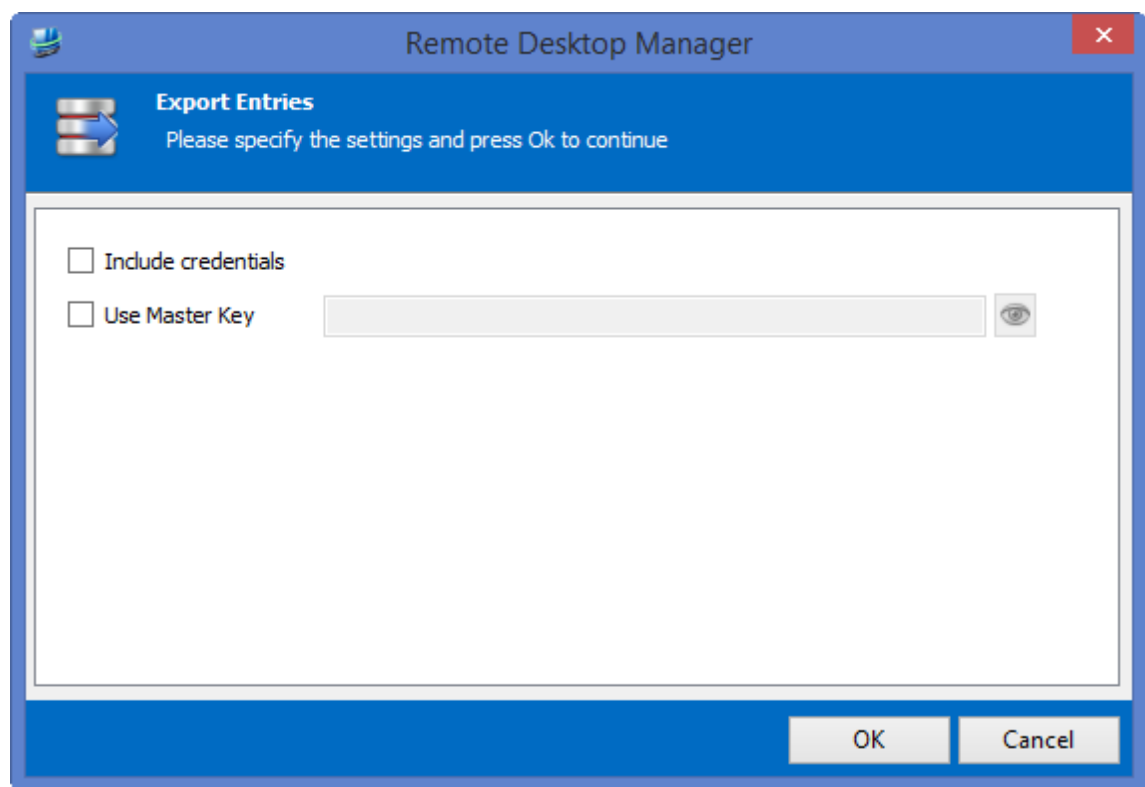


File -> Export

When using an [Advanced Data Source](#), export capabilities can be disabled via security policies at the data source level (no one can export) or at a user level (particular users can't export). See [Security Group Management](#) for more information.

Basic export***Export All Entries (.rdm)***

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



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 want the export a slightly more detailed list including the following information: Host, Description, Display Name, Group, Security Group.

Export special

The export special will display an additional dialog that allows you to select entries.

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 will be under your exclusive control.



Please note that the csv columns will vary depending on entry types being exported.

Export All Entries (.html)

Export all entries within a AES-256 to encrypt self contained html file. See [Export Html Encrypted](#) 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 it sets the file extension to .xml instead.

3.1.7.2 Encrypted Html

Description

The Html Encrypted export format was designed to allow for simple & 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 filename for the new document. Once the export completes the file will open in your default browser.



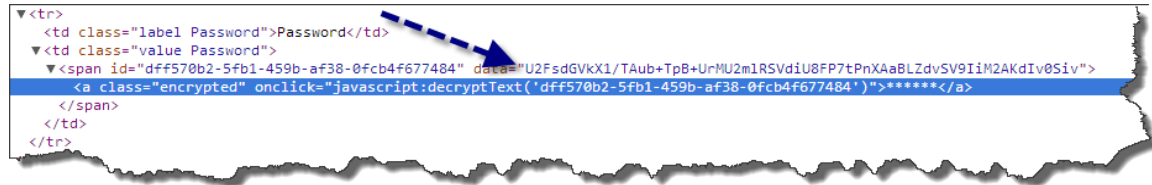
Ensure you do not forget the password as you will not be able to decrypt the data without it.

When exporting multiple entries all will contained within the same file. At decrypt time, each encrypted value must be decrypted individually for security reasons. Once you're done with the sensitive data simply hit **F5** to refresh the file or simply close it. Your data is now safe from prying eyes.

AES-256

We use AES-256 to encrypt/decrypt your sensitive data. Since the decryption is done entirely in the

browser, there's no need for external tools, downloads or installs.



Encrypted value

Safe & Smart Virtual Backup

In addition, HTML Export using symmetric encryption is a great way to securely backup your passwords and other sensitive information. It allows you to share information via email, or simply send the file to your personal email account as a backup.

3.1.8 Options

3.1.8.1 Overview

Description

Remote Desktop Manager has many options and they are available in the following topics:

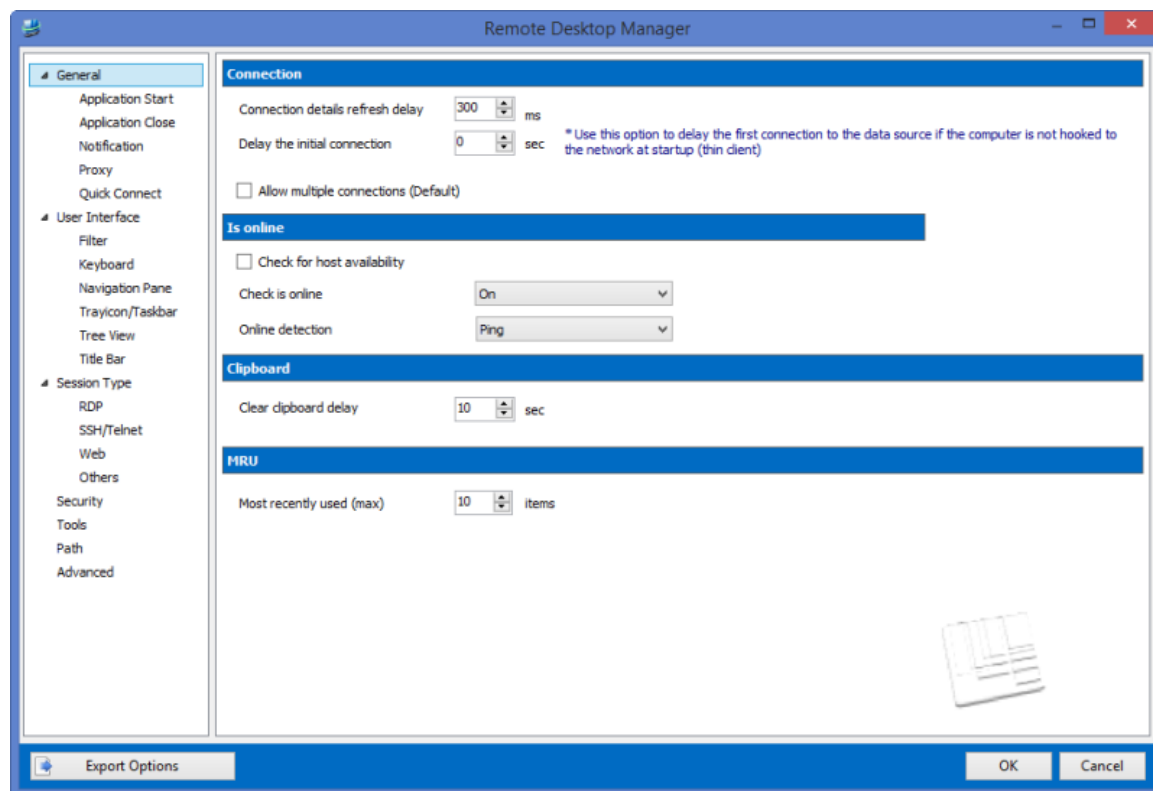
- [General](#)
- [Application Start](#)
- [Application Close](#)
- [Notification](#)
- [Proxy](#)
- [Quick Connect](#)
- [User Interface](#)
- [Filter](#)
- [Keyboard](#)
- [Navigation Pane](#)
- [Trayicon/Taskbar](#)
- [Tree View](#)
- [Title Bar](#)
- [Session Type](#)
- [RDP](#)
- [SSH/Telnet](#)
- [Web](#)
- [Others](#)
- [Security](#)
- [Tools](#)
- [Path](#)
- [Advanced](#)
- [Export Options](#)

3.1.8.2 General

3.1.8.2.1 General

Description

Use the **File -> Options -> General** to control application general settings.



General

Settings

Connection

Options	Description
Connection details refresh delay	Delay that occurs after pretty much every action in Remote Desktop Manager before the currently selected node is queried to display information in various tabs. Adjust this to adapt it to your environment.
Delay the initial connection	Use this option to delay the first connection to the data source if the computer is not hooked to the network at startup (thin client).
Allow multiple connections	Allows you to open multiple concurrent connections (tabs) to the same session. If not enabled, selecting "Open Session" will simply set the focus on the existing connection.

Is Online

Options	Description
Check for host availability	Hosts are pinged to determine if they are available. Host will be display in "red" in the tree view if not available.
Check is online	By default, the application checks if the host is online. Option can be turn on or off.
Online detection	Detection mode for the <i>is online</i> option, choose between ping or port scan.

Clipboard

Options	Description
Clear clipboard delay	Set the delay to empty the clipboard after a copy of an remote information.

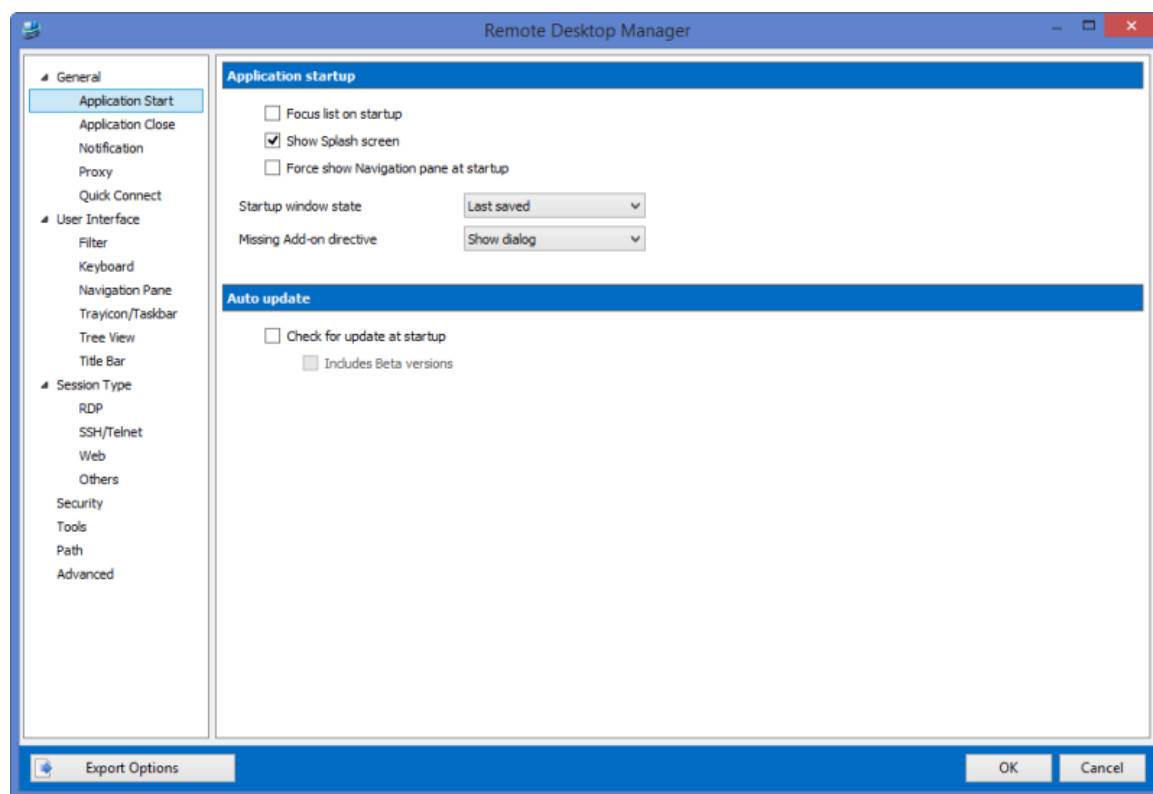
MRU

Options	Description
Most recently used (max)	Indicate the maximum number of items to display in the list view. See MRU topics for more information on Most Recently Used.

3.1.8.2.2 Application Start

Description

Use the **File -> Options -> General | Application Start** to control application startup settings.



Application Start

Settings

Application startup

Option	Description
Focus list on startup	The focus will be set on the entry list when application starts.

Show Splash screen	Application will display the splash screen on startup.
Force show Navigation pane list at startup	The Navigation pane list will be shown on start, even if it was hidden when the application was closed.
Startup window state	Indicate the display of the windows state at startup: <ul style="list-style-type: none"> • Last saved • Minimized • Maximized
Missing Add-on directive	Indicate the display of the missing Add-on directive window: <ul style="list-style-type: none"> • Show dialog • Auto Install • Do nothing

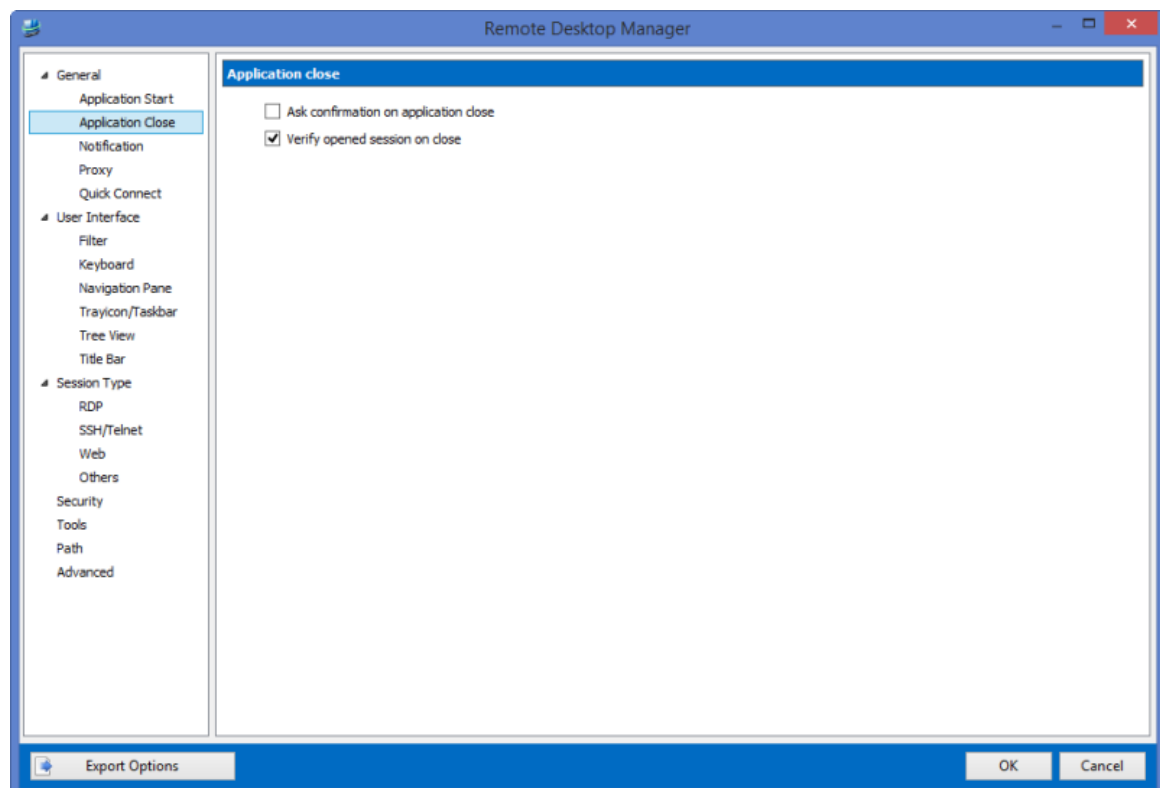
Auto update

Option	Description
Check for update at startup	Application will perform a verification for new releases availability.
Include Beta versions	Application will include beta version in the update verification.

3.1.8.2.3 Application Close

Description

Use the **File -> Options -> General | Application Close** to control application close settings.



Application Close

Settings

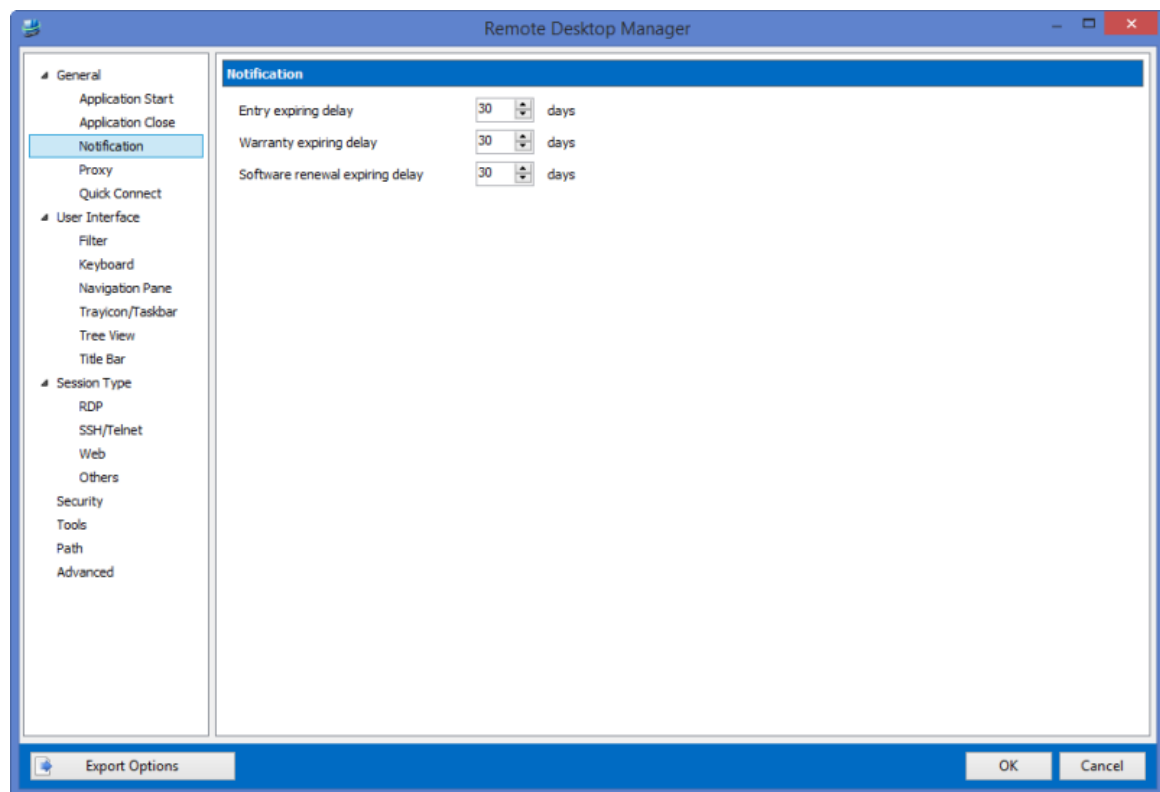
Application Close

Option	Description
Ask confirmation on application close	Application will prompt you for confirmation when you attempt to close it.
Verify opened session on close	Application will warn you about running sessions when you attempt to close it.

3.1.8.2.4 Notification

Description

Use the **File -> Options -> General | Notification** to control application notification settings.



Notification

Settings

Notification

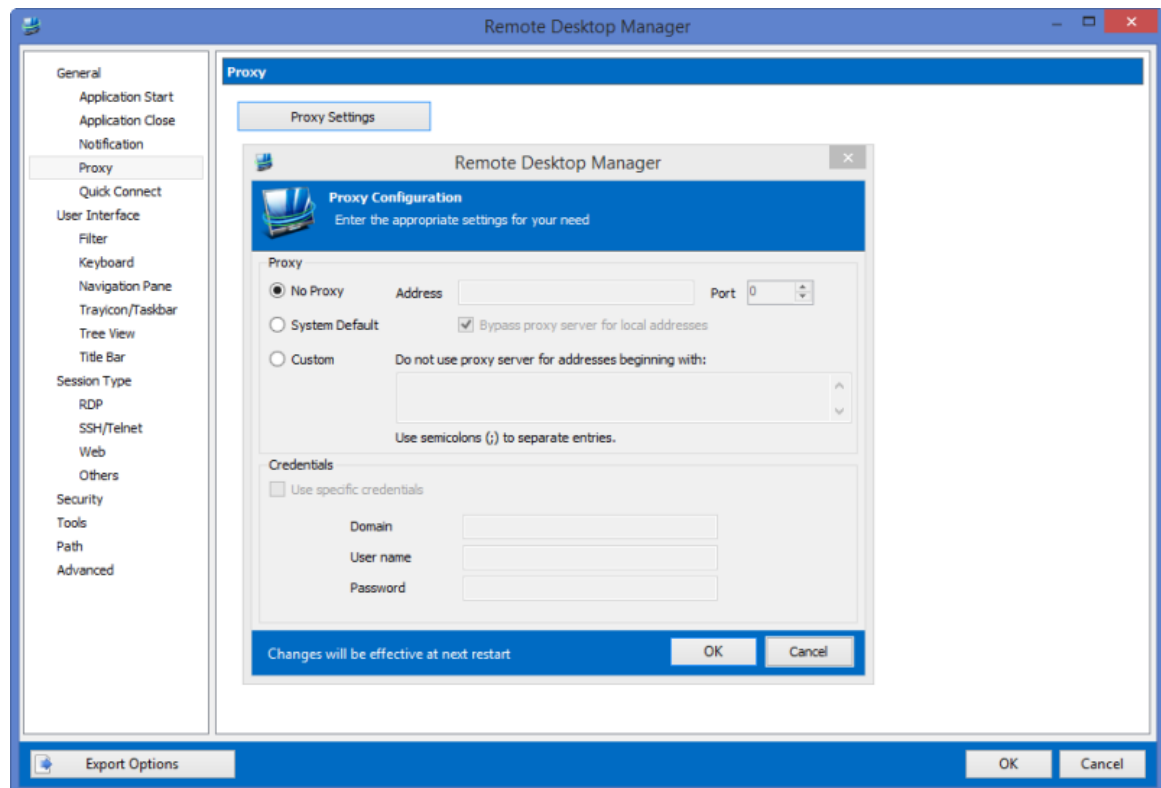
Option	Description
Entry expiring delay	Set the number of days to receive a notification before an entry expires.

Warranty expiring delay	Set the number of days to receive a notification before a warranty expires.
Software renewal expiring delay	Set the number of days to receive a notification to renew a software.

3.1.8.2.5 Proxy

Description

Use the **File -> Options -> General | Proxy** to control application proxy settings.



Proxy

Settings

Proxy

Option	Description
No Proxy	No proxy settings.
System Default	Use the system default proxy.
Custom	Use a custom proxy by selecting the address and port. It's possible to built a list of exceptions with this option.

Credentials

Option	Description
--------	-------------

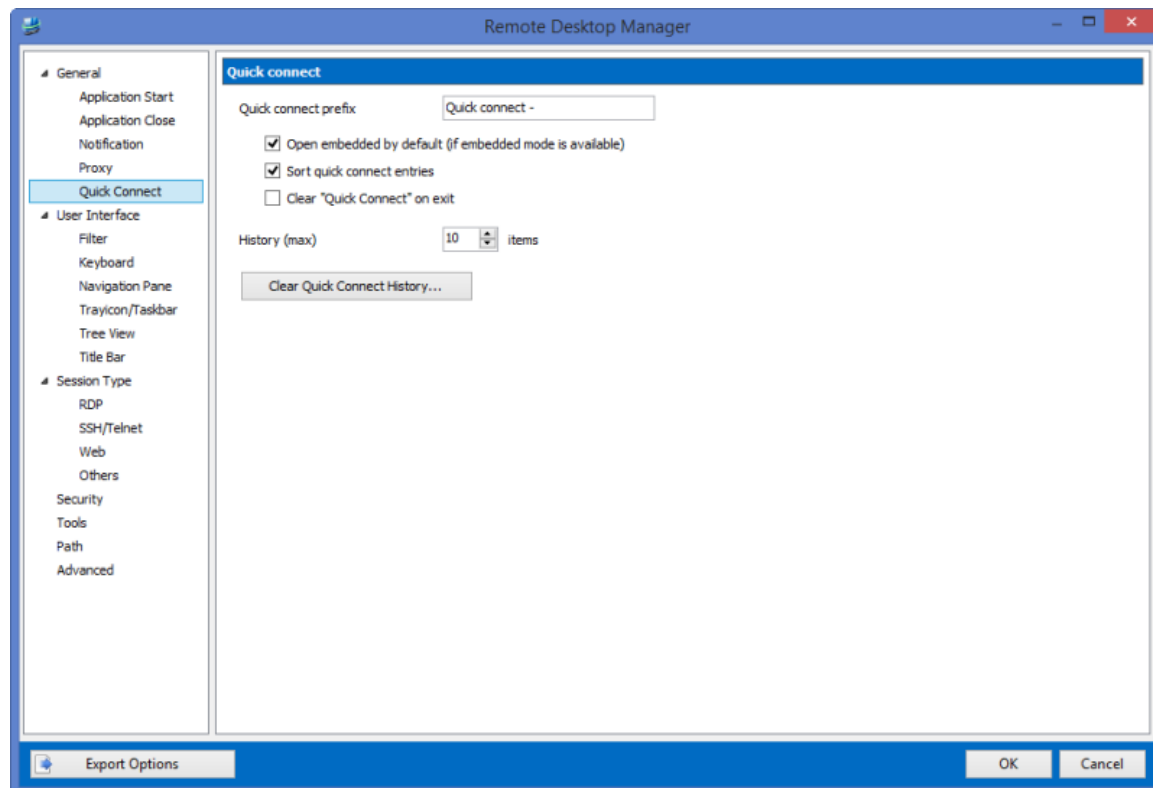
Use specific credentials

Use specific credentials when custom is selected.

3.1.8.2.6 Quick Connect

Description

Use the **File -> Options -> General | Quick Connect** to control application Quick Connect settings. Consult the following for more information on [Quick Connect](#).

**Quick Connect**

Settings

Quick Connect

Option	Description
Quick Connect prefix	Enter the prefix to add to the session name that is started in Quick Connect mode. This applies only to embedded sessions.
Open embedded by default (If embedded mode is available)	Quick connect sessions will be opened embedded if possible.
Sort quick connect entries	Organize the quick connect drop down items in alphabetic order.
Clear "Quick Connect" on exit	The application will not persist your quick connect information upon close.
History (max)	Indicates the maximum number of quick connect entries to maintain the history list displayed in the drop down.

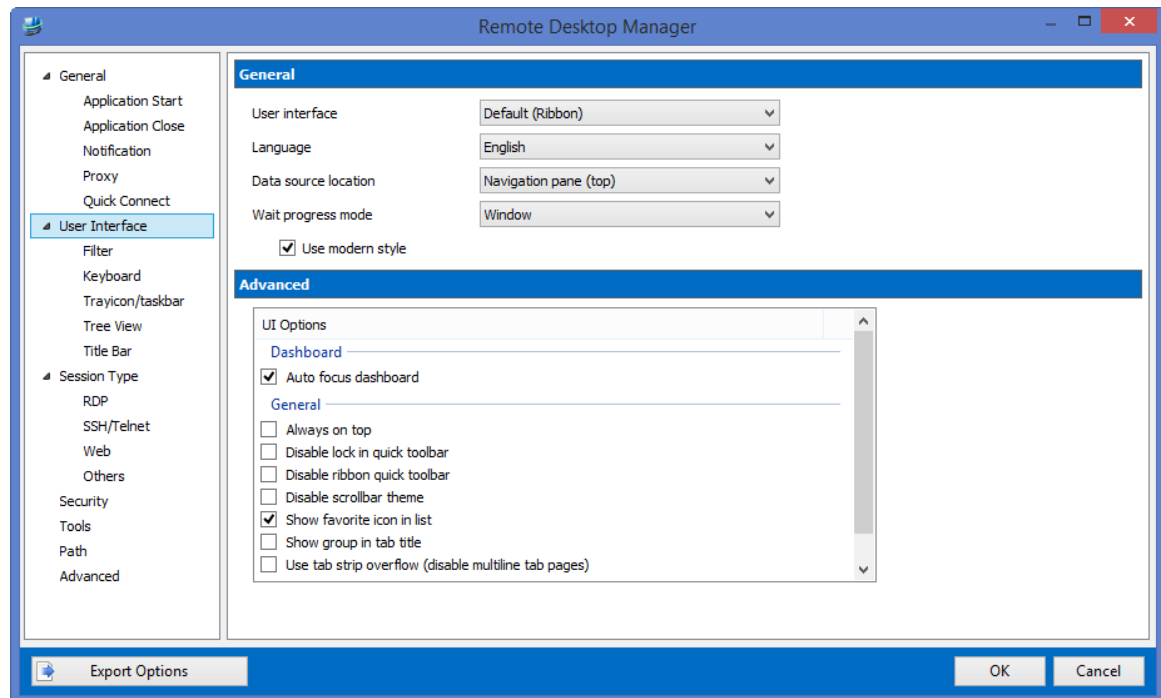
Clear Quick Connect History Use this button to clear the quick connect history drop down.

3.1.8.3 User Interface

3.1.8.3.1 User Interface

Description

Use the **File -> Options -> User Interface** to control what is displayed in Remote Desktop Manager's User Interface.



User Interface

Settings

General

Options	Description
User Interface	Indicate the user interface mode: <ul style="list-style-type: none"> • Default (Ribbon) • Default (Menu) • Classic UI (v7.X) For more information see User Interface Style topic.
Language	Select your preferred language for the user interface.
Data source location	Select the position of your data source selection drop down: <ul style="list-style-type: none"> • Status bar • Navigation Pane (top) • Navigation Pane (bottom)

	<ul style="list-style-type: none"> • None
Wait progress mode	Display your wait progress information in a Window or Status bar. You can disable the waitprogress by selecting None.
Use modern style	Remote Desktop Manager will display with the Microsoft modern style interface.



The Data Source Location **none** setting is not supported in the Classic UI mode.

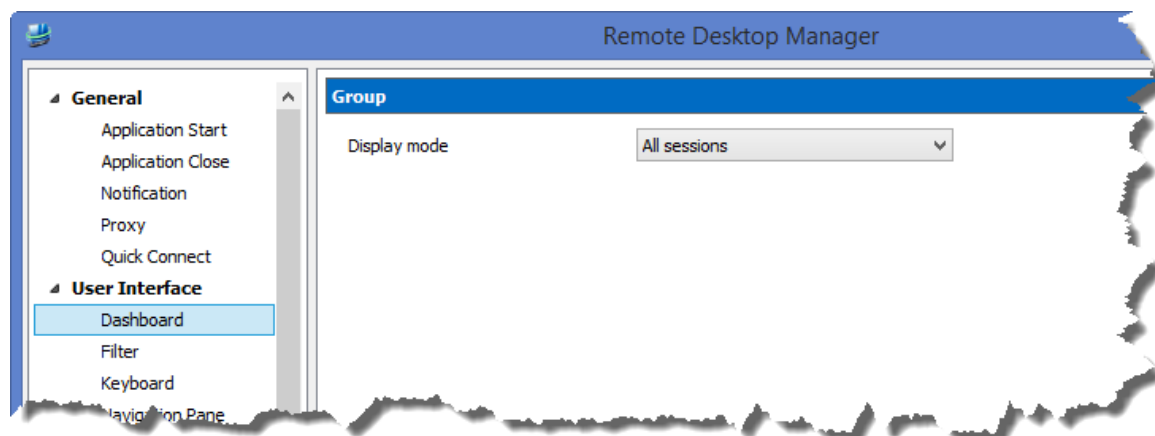
UI Options

Options	Description
Auto focus dashboard	When checked and an inactive entry is selected in the tree view, the corresponding dashboard is displayed and focus is immediately set on it.
Always on top	Keeps the application on top of all others.
Disable lock in quick toolbar	Disable the lock button in the quick access toolbar.
Disable ribbon quick toolbar	Disable the ribbon quick access toolbar.
Disable scrollbar theme	Disable scrollbar theme. This is useful if you have issue clicking on the toolbar.
Show favorite icon in list	Favorite icon is overlaid on your session icon.
Show group in tab title	Display group in opened tab title.
Use tab strip overflow (disable multiline tab pages)	When there are too many active tabs for the width of the application, having this option checked will result in a new line of tabs to appear. If unchecked then arrows will appear to indicate more tabs are present.

3.1.8.3.2 Dashboard

Description

Use the **File -> Options -> User Interface | Dashboard** to control how the application display the sessions in the Dashboard.



Dashboard

Settings

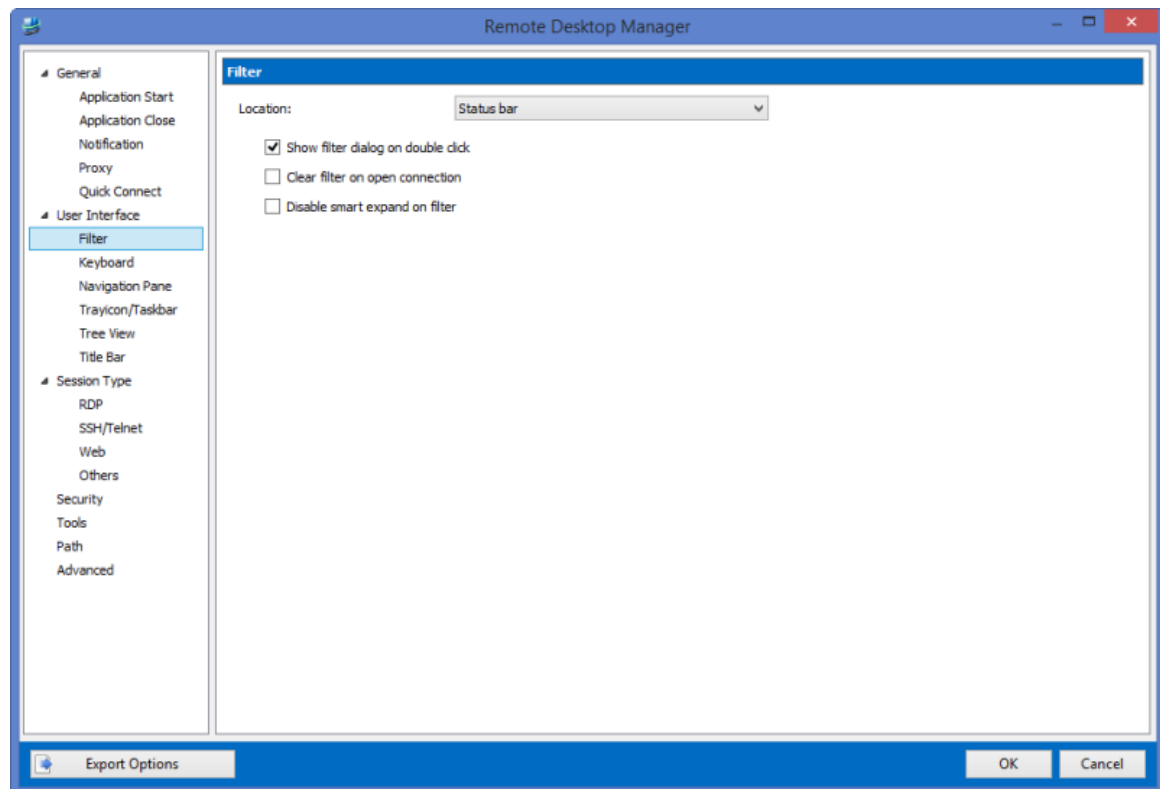
Group

Option	Description
Display mode	Determine how the entries are display in the group dashboard. Choose between: <ul style="list-style-type: none">• First level only: only the entries and the groups located directly in the selected group are listed.• All sessions: all the entries are listed including those contained in the sub-folders.• Default (all if not more than...): All entries will be display if not more than the select number when the Default option is active.

3.1.8.3.3 Filter

Description

Use the **File -> Options -> User Interface | Filter** to control application filter box and settings. See topic [Search/Filter](#) for more information.



Filter

Settings

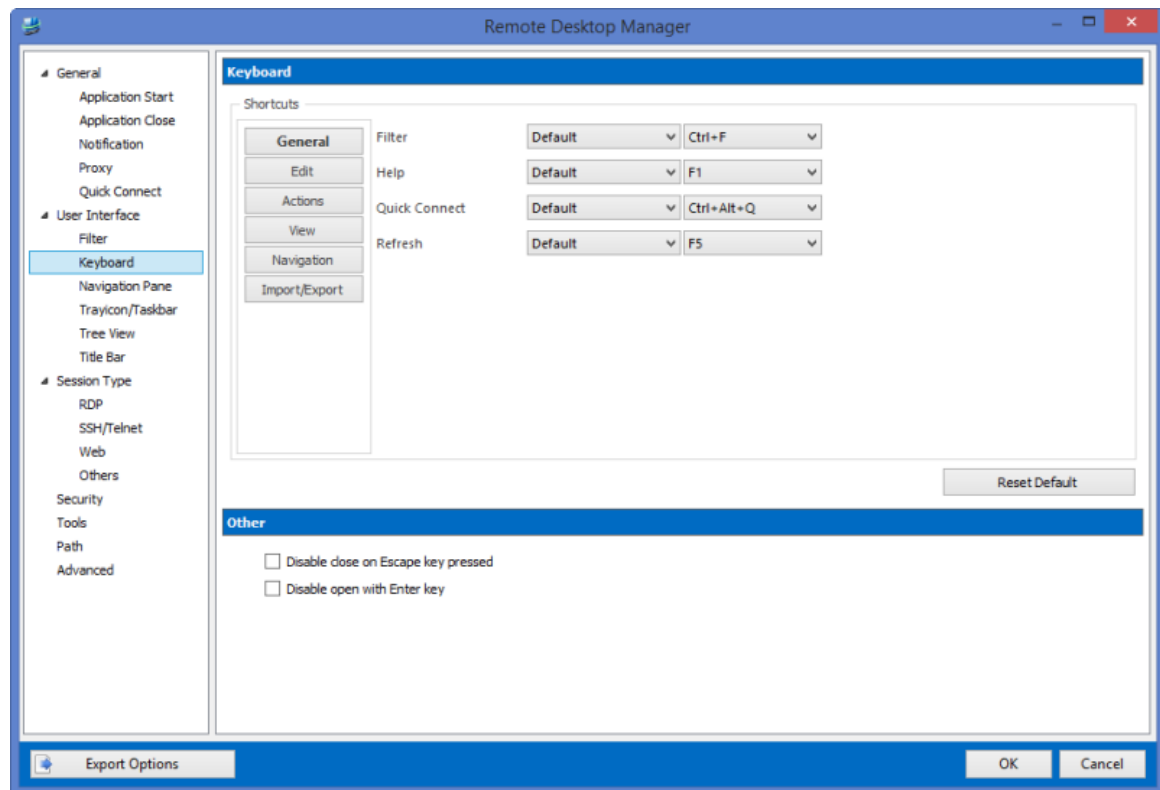
Filter

Option	Description
Location	<p>For the location of the filter box, you can choose between:</p> <ul style="list-style-type: none"> • Status bar • Navigation pane (bottom) • Navigation pane (top) • None <p>When None is select, a dialog will appear when the shortcut is press.</p>
Show filter dialog on double click	Double-click in the filter field to open the filter dialog box.
Clear filter on open connection	The filter is cleared each time a session is opened.
Disable smart expand on filter	When the smart expand is enabled, the application will remember on each keystroke which folders was opened, including the original state.

3.1.8.3.4 Keyboard

Description

Use the **File -> Options -> User Interface | Keyboard** to control how the application handles keyboard input.



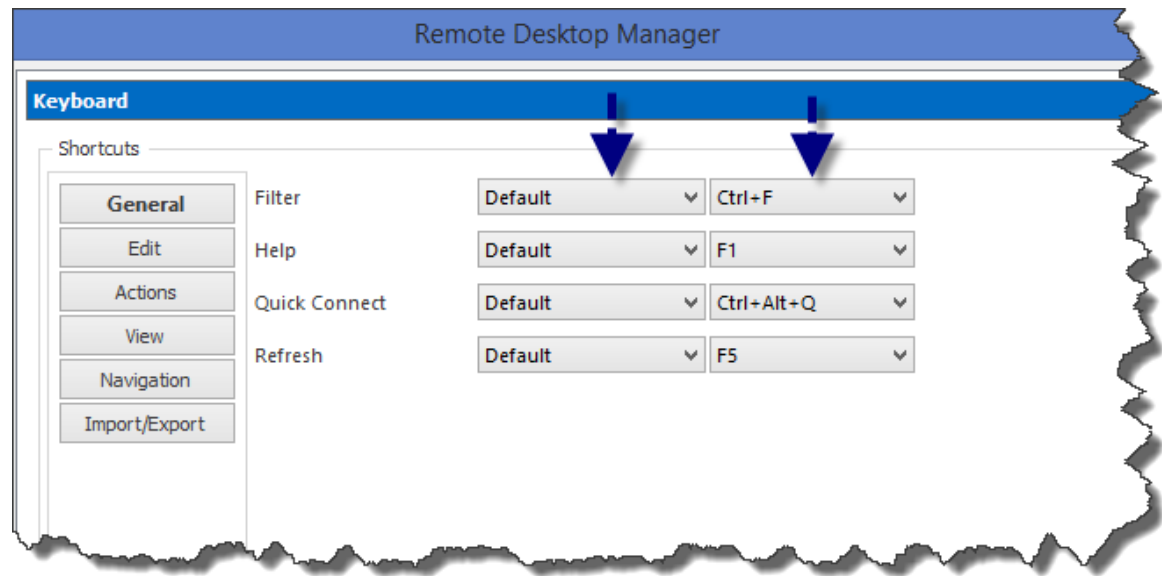
Keyboard

Settings

Keyboard

On the left there are different shortcuts categories. This lightens the screen and allows you to focus on less shortcuts at the same time.

To configure a keyboard shortcut for an action, two controls are provided.



Keyboard Shortcuts

Shortcuts

The first drop down is for the scope of the keyboard shortcut.

Option	Description
Default	Use default shortcut keys. Use the magnet in the status bar to disable the shortcut.
When not in session	Use the shortcut keys when the focus is not in a session.
Global hotkey	This create global window hot key. For example, you can use it to execute a macro when Remote Desktop Manager is not loaded.
None	Select the none item to remove any hot key for the corresponding action.



Currently no validation is performed as to your usage of the same key combination for two actions.

Other

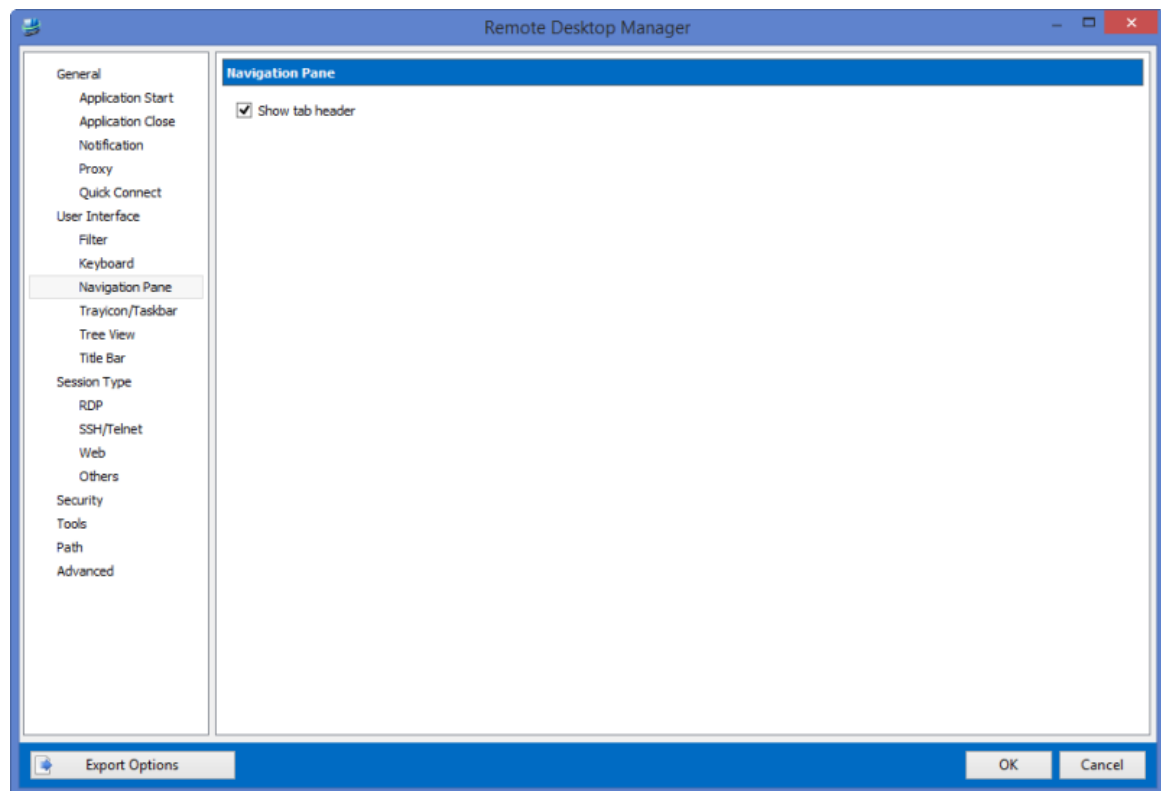
Option	Description
Disable open with Enter key	Pressing the Enter key while an entry is selected will not open it.

Disable close on Escape key pressed	Pressing the Escape key while in a running session will not close it.
-------------------------------------	---

3.1.8.3.5 Navigation Pane

Description

Use the **File -> Options -> User Interface | Navigation Pane** to control application Navigation Pane display.



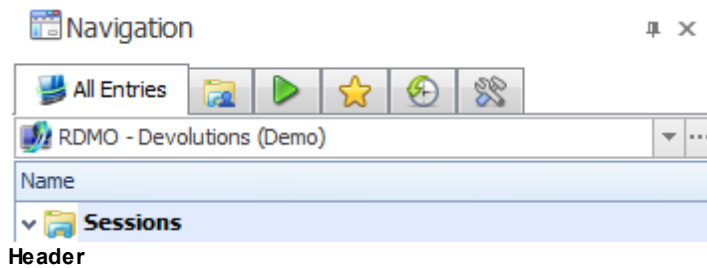
Navigation Pane

Settings

Navigation Pane

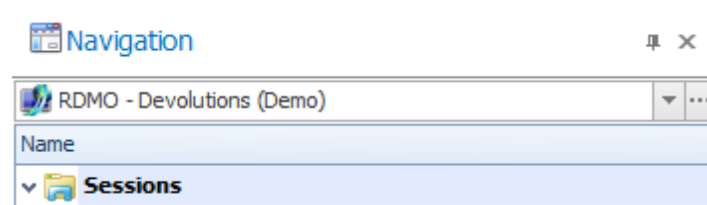
Option	Description
Show tab header	Display the header tab in the Navigation Pane.

With Header



Header

Without Header

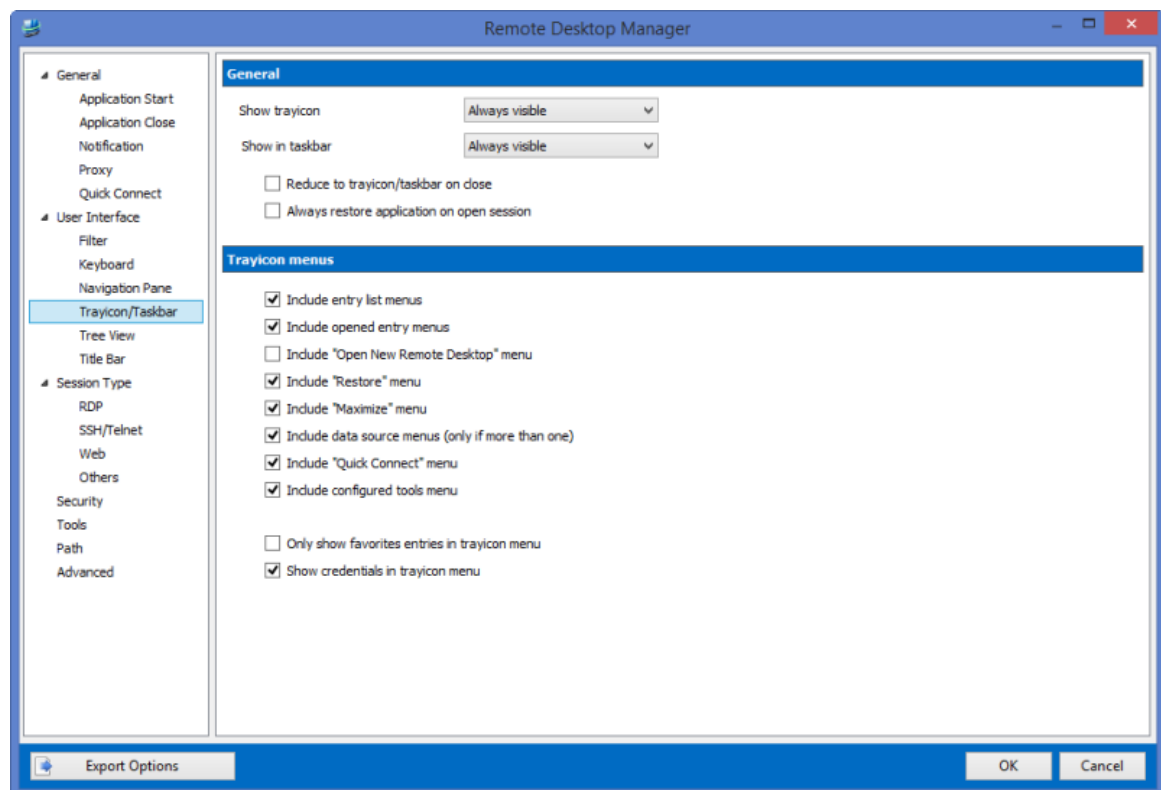


Without Header

3.1.8.3.6 Trayicon/Taskbar

Description

Use the **File -> Options -> User Interface | Trayicon/Taskbar** to control application tray icon and taskbar.



Trayicon/Taskbar

Settings

General

Option	Description
Show trayicon	Indicates if the trayicon is enabled.
Show in taskbar	Indicates if the application is visible in the Windows taskbar.
Reduce to trayicon/taskbar on close	Clicking on the X will minimize the application instead of closing it.
Always restore application on open session	When using the menu in the trayicon to launch a session and when application is minimized, enabling this option will restore application before launching the session.

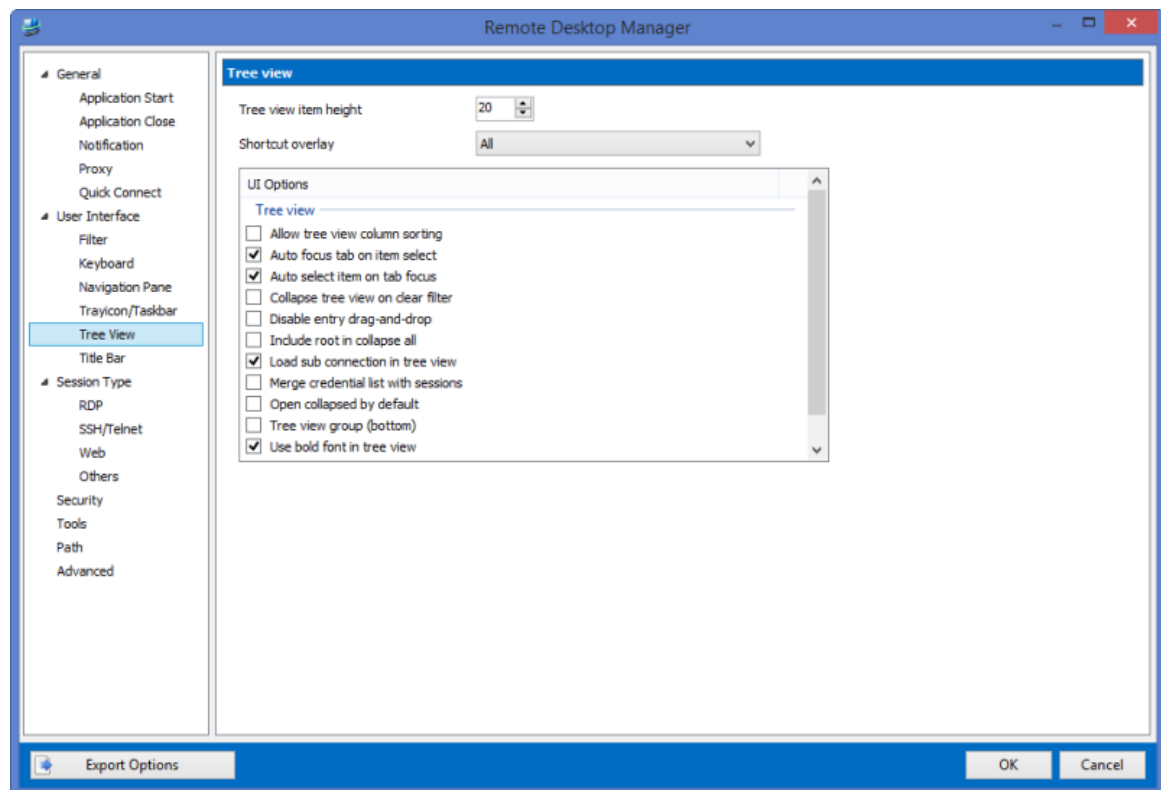
Trayicon menus

Option	Description
Include entry list menus	Includes the entries in the trayicon menu.
Included opened entry menus	Includes a sub-menu for opened sessions.
Include "Open New Remote Desktop" menu	Includes a menu to launch a new RDP session with mstsc.exe.
Include "Restore" menu	Includes a menu to restore application when it has been minimized.
Include "Maximize" menu	Includes a menu to maximize the application window to take the full area of the screen.
Include data source menus	Includes a sub-menu for the data sources. This requires more than one data source to function.
Include "Quick Connect" menu	Includes a menu to perform a quick connect to a host.
Include configured tools menu	Includes sub menu listing all configured tools.
Only show favorites entries in trayicon menu	Only the favorites entries will appear in the tray icon menu.
Show credentials in trayicon menu	Indicate if the credentials are listed in the tray icon menu.

3.1.8.3.7 Tree View

Description

Use the **File -> Options -> User Interface | Tree View** to control application tree view.



Tree View

Settings

Tree View

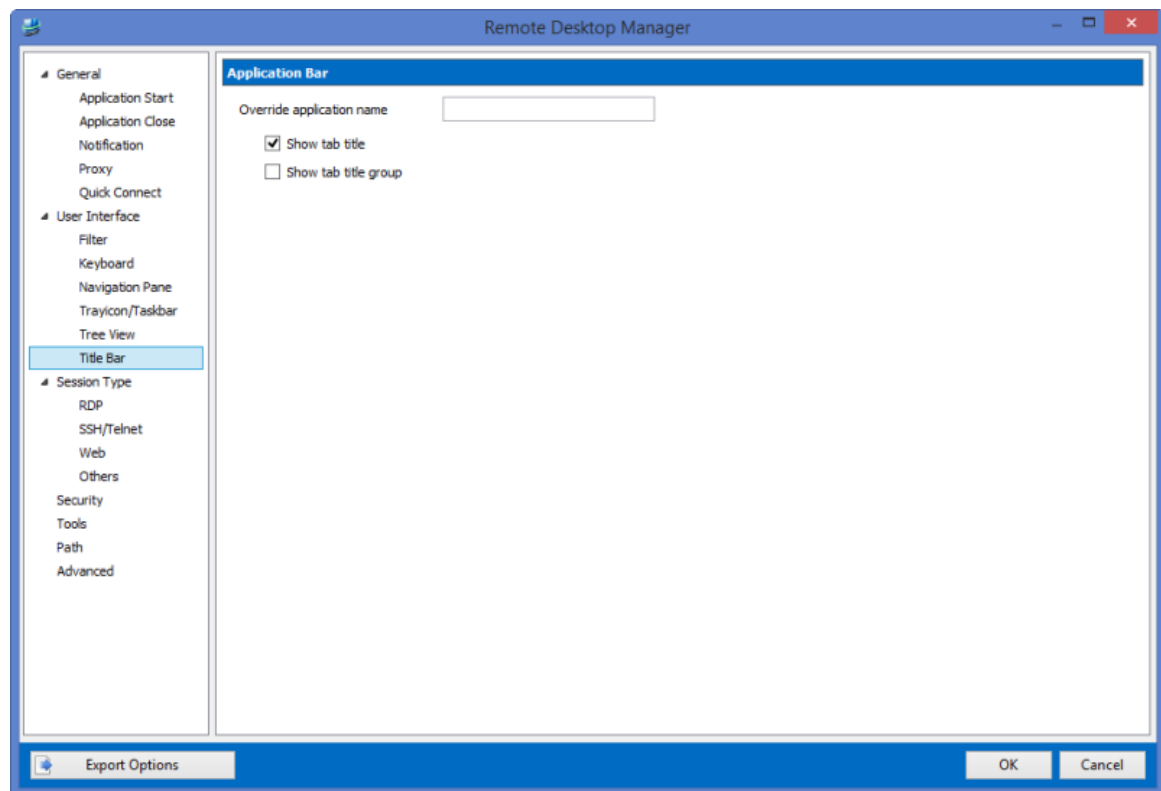
Option	Description
Tree view item height	Specify the height of individual items in the Tree view. Valid values are between 16 and 32.
Shortcut overlay	Determine if the shortcut icon is visible on all the items, all except the original one or not visible. Choose between: <ul style="list-style-type: none"> • All • None • All except original
Allow tree view column sorting	Allows tree view columns to be sorted.
Auto focus tab on item select	When you select an entry in the tree view, the auto focus will change for the related item tab page.
Collapse tree view clear filter	When you apply a filter and then clear it using the X button, having this option checked will automatically collapse the tree view.
Disable entry drag-and-drop	This setting disables moving entries with drag-and-drop. Use this option to avoid any unwanted session create by drag and drop by mistake.
Include root in collapse all	By default the application has many root nodes in the tree view. i.e. Sessions, Credentials, Macros/Scripts/Tools. Collapsing the tree view will also collapse every root nodes if this option is enabled. Only the children of the current root are affected by the command when this

	option is not enabled.
Load sub connection in tree view	Indicate if the sub connections appear under their parent in the tree view. You can use the sub-connection pane if you don't want them listed in the tree.
Merge credential list with sessions	Use this option if you want the credentials to appear within the list of Sessions instead of in their own root.
Open collapsed by default	The entry list will always be collapsed upon startup.
Tree view group (bottom)	This setting indicates if the Group/Folder entries are at bottom of the list instead of appearing first under their parent.
Use bold font in tree view	Indicate if the root level items are displayed using the bold attribute.

3.1.8.3.8 Title Bar

Description

Use the **File -> Options -> User Interface | Title bar** to control application title bar.



Title bar

Settings

Application bar

Option	Description
Override application name	Display a custom title for the application title bar. Use this setting to

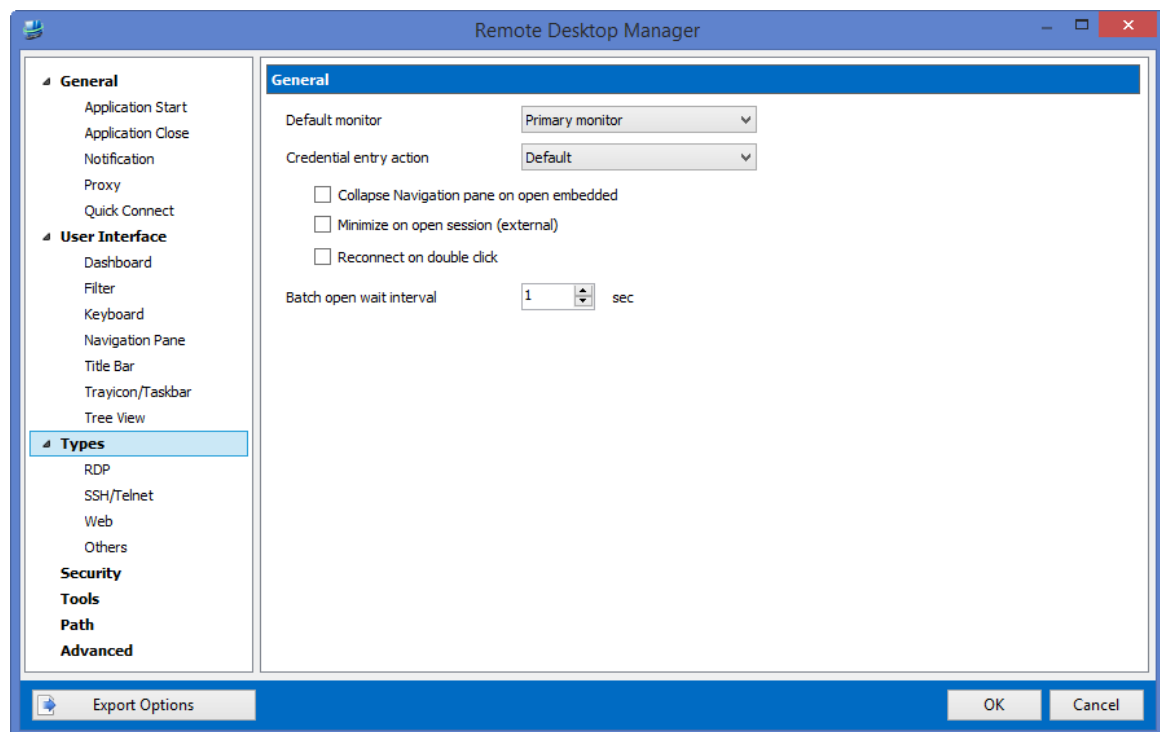
	get a unique identifier when you have multiple instances opened or when you use multiple versions side by side.
Show tab title	The application bar will append the caption of the current tab to the name to the title bar.
Show tab title group	This will prefix the tab title name with the session group name. It will also appear in the application title bar.

3.1.8.4 Type

3.1.8.4.1 Type

Description

Use the **File -> Options -> Type** to control settings applied to entries of the Session type.



Session Type

Settings

General

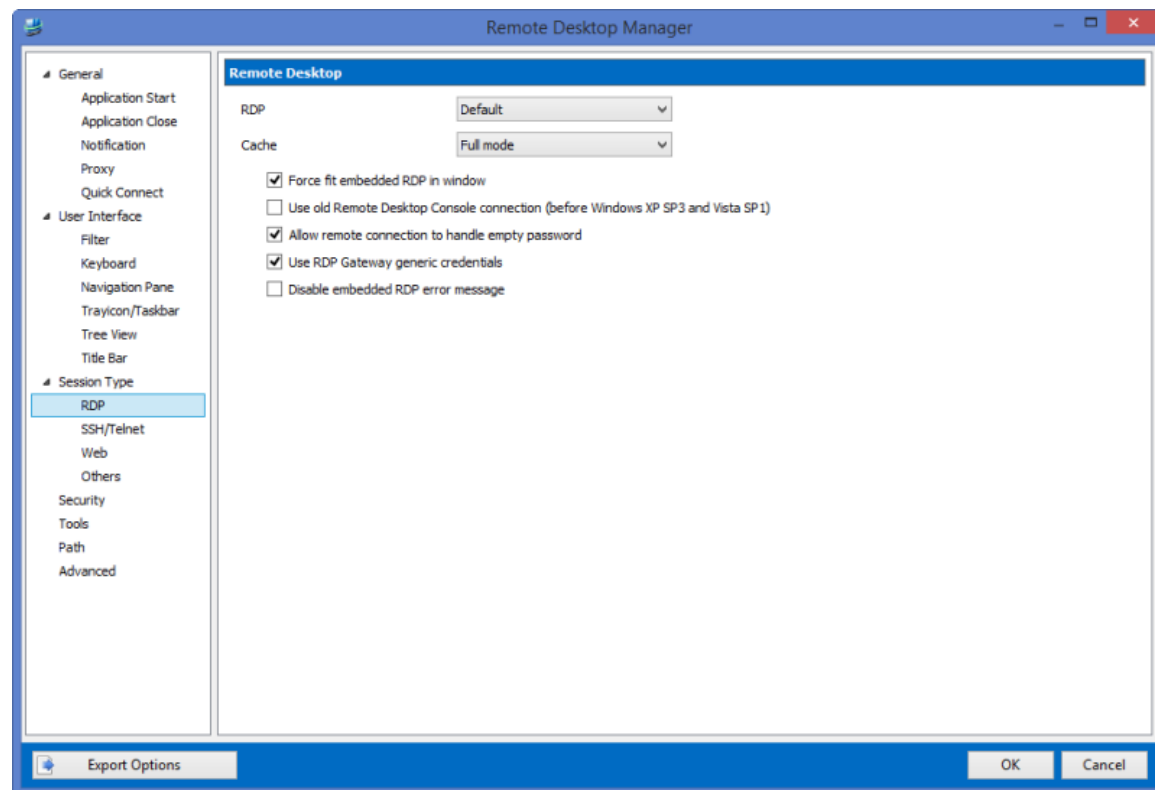
Option	Description
Default monitor	Choose your preferred monitor from the list.
Credential entry action	Allows you to change the Default action executed when you launch the entry. Each entry can override this setting but this is the default behavior when "Default" is specified in the configuration.

	<p>Allowed values are:</p> <ul style="list-style-type: none"> • Default: The system default is "View Dashboard" • View Entry: Opens the entry in view mode • Copy password: Copies the password to the clipboard. Note that there is a delay after which the clipboard is cleared for safety purposes. Please see Advanced • View dashboard: Displays the Credential Entry dashboard for the current entry • Edit: Opens the entry in edition mode.
Collapse Navigation pane on open embedded	This will perform an automatic hide the navigation pane when an embedded session is launched.
Minimize on open session (external)	This will automatically minimize of the application when an external session is launched.
Reconnect on double click	The application will reconnect remote host instead of focusing it when the node in the tree view is double clicked. It's only supported by the connections types.
Batch open wait interval	Specify the delay between each opening when multiple sessions are opened in batch.

3.1.8.4.2 RDP

Description

Use the **File -> Options -> Session Type | RDP** to control settings applied to a RDP session type.



RDP

Settings

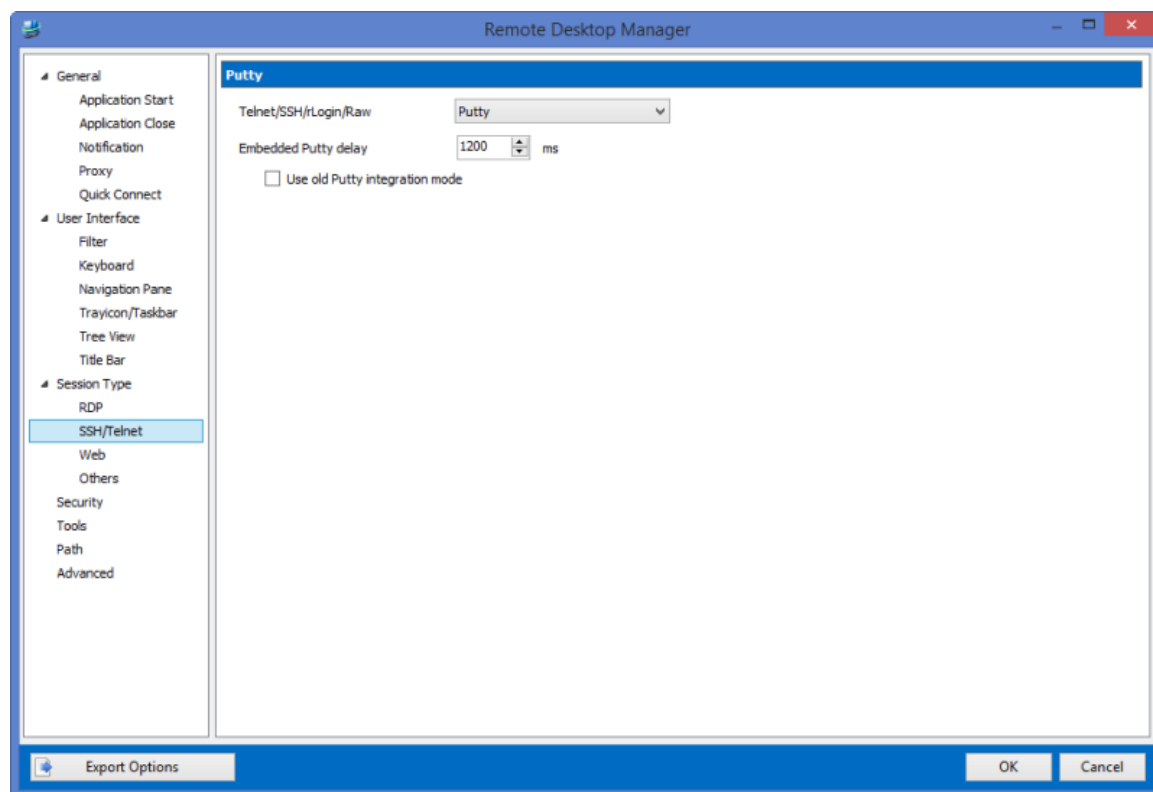
Remote Desktop

Option	Description
RDP	Select RDP version you want to use.
Cache	Select the default RDP cache mode used: <ul style="list-style-type: none">• Full mode• Thin client• Small cache Change this mode to reduce the memory usage when you have multiple connections opened at the same time.
Force fit embedded RDP in windows	The application will force the resolution to fit inside the available content space.
Use old Remote Desktop Console Connection(before Windows XP SP3 and Vista SP1)	Use the connection console mode in external as it existed before Windows XP SP3 and Vista SP1. The most mstsc.exe parameter is different between theses two versions.
Allow remote connection to handle empty password	This will allow the connection even if the password is empty and let the RDP connection to handle the prompt for password. The application automatically prompt for the credentials when it detect an empty password and when this option is disabled. It can then reuse those credentials for an automatic login.
Use RDP gateway generic credentials	This will impose the usage of the generic credentials in the Windows Credential Repository instead of the domain credentials. Use for backward compatibility only.
Disabled embedded RDP error message	This will prevent the error message from a lost RDP connections to be displayed to the user.

3.1.8.4.3 SSH/Telnet

Description

Use the **File -> Options -> Session Type | SSH/Telnet** to control settings applied to SSH/Telnet session type.



SSH/Telnet

Settings

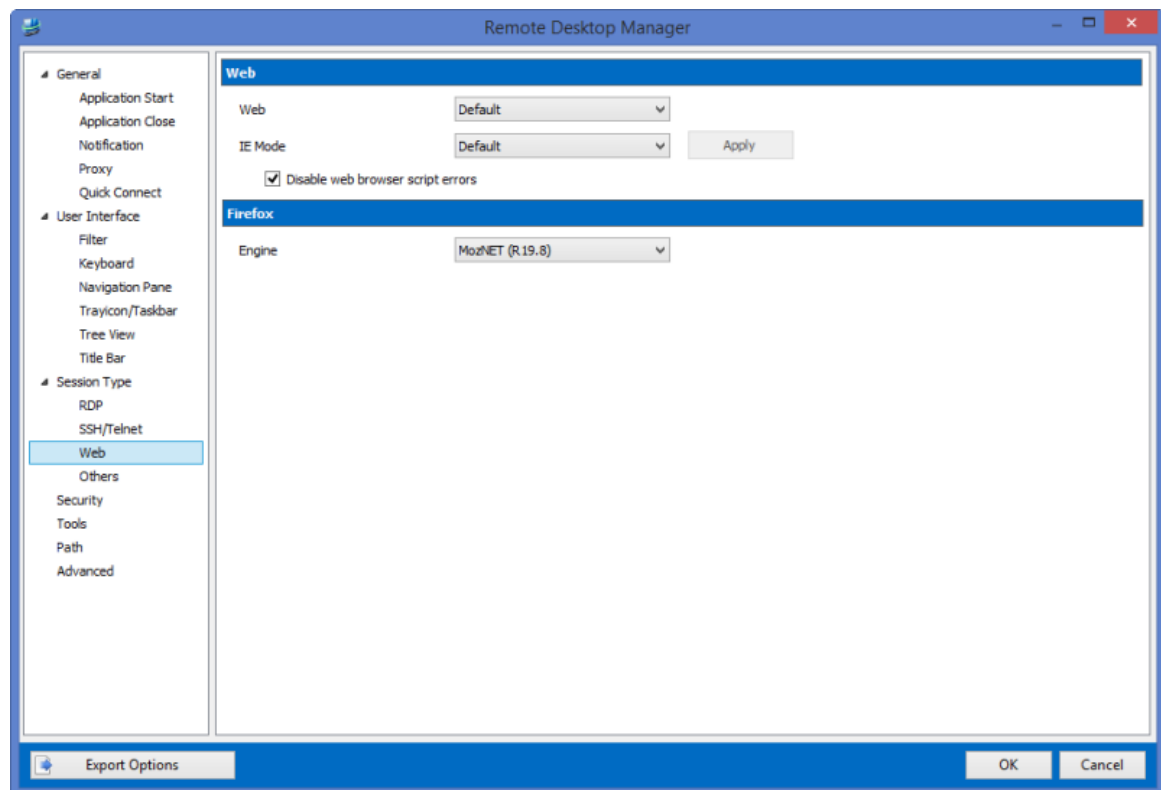
Putty

Option	Description
Telnet/SSH/rLogin/Raw	Used to select the default application: <ul style="list-style-type: none"> • Putty • Plink • Kitty
Embedded Putty delay	When using "Old putty integration mode", this is the delay of time Remote Desktop Manager will pause after establishing an embedded putty connection. Adjust this if more initialization time is required.
Use old Putty integration mode	Use the previous of integrating Putty which was using a basic delay to detect that the application was ready. Use this if putty connections fail.

3.1.8.4.4 Web

Description

Use the **File -> Options -> Session Type | Web** to control settings applied to web session type.



Web

Settings

Web

Option	Description
Web	Choose your preferred web browser from the list. The Default value indicates to use the default web browser set on the computer.
IE Mode	Choose the emulation mode for Internet Explorer. Some web sites don't work well with old or new versions of Internet Explorer.
Disable web browser script errors	This will prevent scripting errors to be displayed to the user.

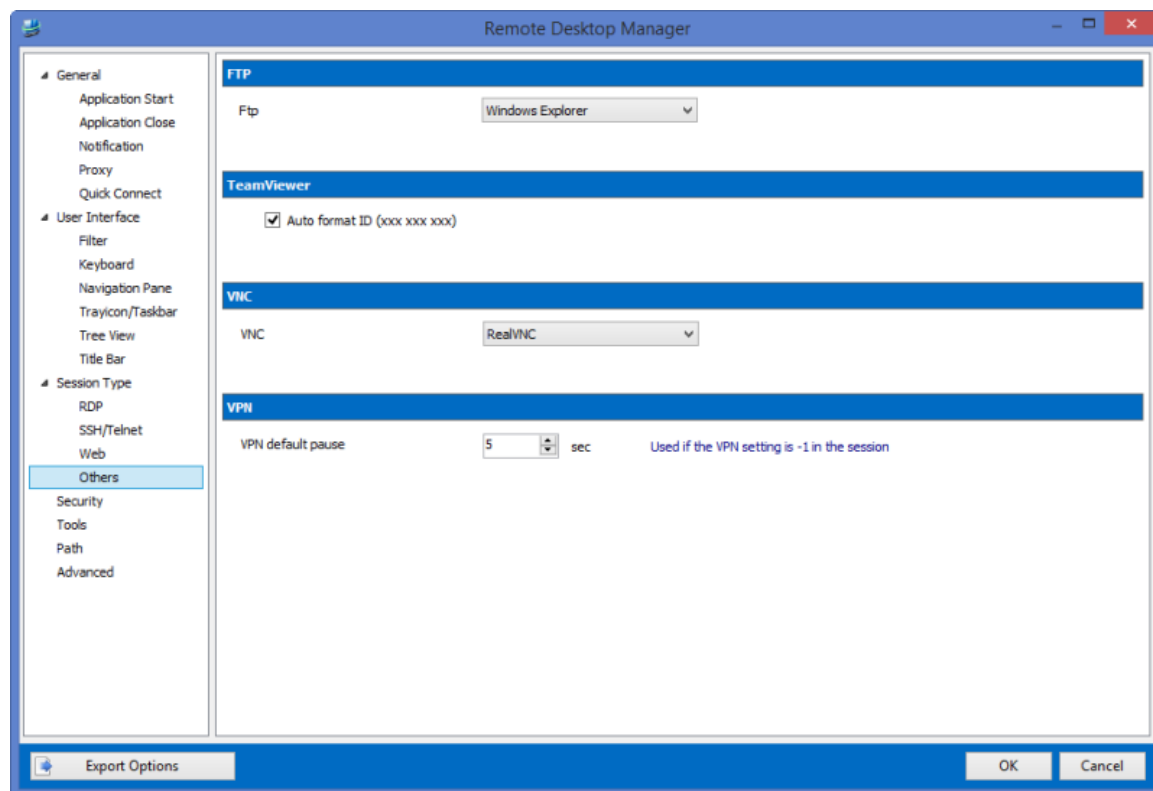
Firefox

Option	Description
Engine	Choose the default embedded Firefox engine used by the application. The possible values are: <ul style="list-style-type: none"> • MozNET (R19.8) • geckofx

3.1.8.4.5 Others

Description

Use the **File -> Options -> Session Type | Others** to control settings applied to FTP, Teamviewer, VNC and VPN.



Others

Settings

FTP

Theses settings are applied to all the FTP session types.

Option	Description
FTP	Choose your preferred FTP application from the list: <ul style="list-style-type: none"> • Windows Explorer • Filezilla • WinSCP

TeamViewer

Theses settings are applied to all the TeamViewer session types.

Option	Description
--------	-------------

Auto format the TeamViewer ID	Indication to the application to automatically format the TeamViewer ID before invoking the command line. Some version of TeamViewer require a special formatting.
-------------------------------	--

VNC

Theses settings are applied to all the VNC session types.

Option	Description
VNC	Choose your preferred VNC client from the list of supported clients: <ul style="list-style-type: none">• RealVNC• TightVNC• UltraVNC• VNCViewer Plus

VPN

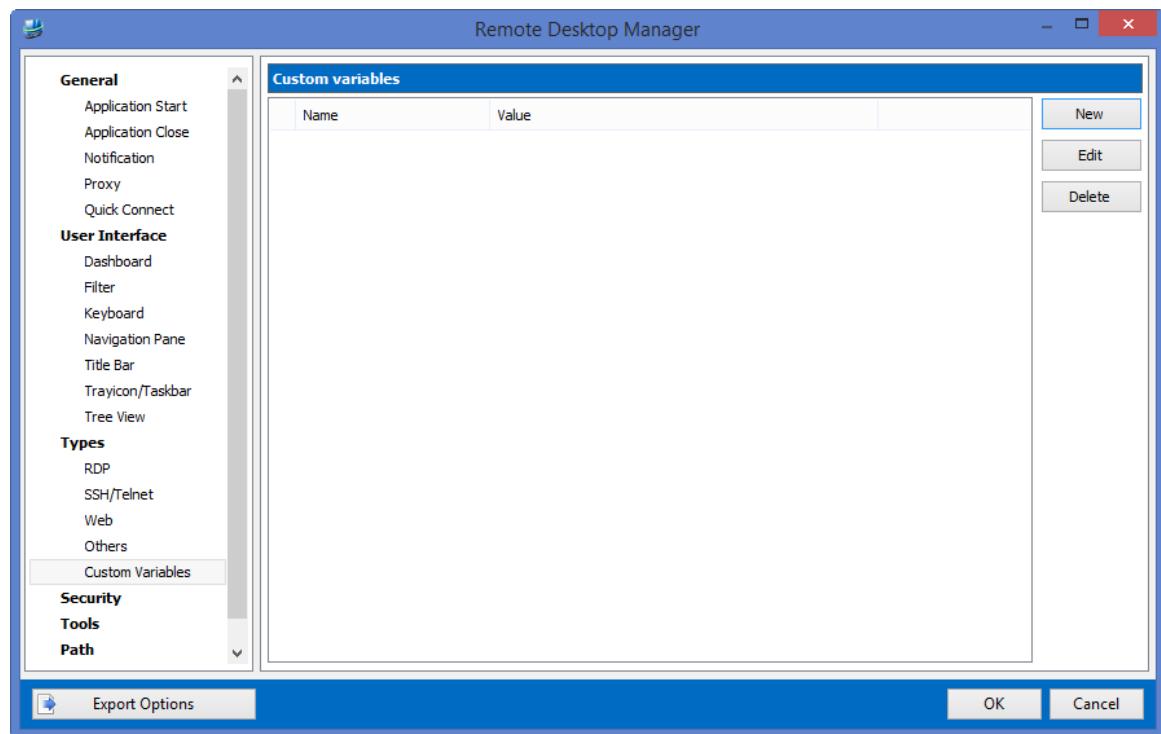
Theses settings are applied to all the VPN types.

Option	Description
VPN default pause	Indicate the default delay in seconds after a VPN connection is established. Adjust this value if your VPN client requires more time to perform the initial setup. The default value is only used when the setting is set to -1 in the session itself.

3.1.8.4.6 Custom Variables

Description

Use the **File -> Options -> Session Type | Custom Variables** to manage your own variable.



Custom Variables

Settings

Custom variables

The custom variables option has been implemented to customize your own variables in the application.

3.1.8.5 Security

Description

Use the **File -> Options -> Security** to control application behaviour as it pertains to system security.

Application security (local)

Application security (local)	
<input checked="" type="radio"/> No application password	
<input type="radio"/> Use application password	
New password	<input type="text"/>
Confirm Password	<input type="text"/>
<input type="radio"/> Use Windows credentials as application password	

Application security (local)

Option	Description
--------	-------------

No application password	The application will have any security enabled. However it's recommended to use the default Windows lock workstation feature.
Use application password	Enable the application level security and define a specific password to access the application.
Use Windows credentials as application password	Enable the application level security and requires the same password as your Windows password. The application needs an access to the domain to authenticate the user.

2-Factor authentication

2-Factor authentication

☐ Require Yubikey authentication
Yubikey

☐ Require Google Authenticator
Configure

2-factor authentication

Option	Description
Require Yubikey authentication	Use a Yubikey device to get access to the application when it starts or when it's locked.
Require Google Authenticator	Use a Google Autnenticator device to get access to the application when it starts or when it's locked.

Lock

Lock

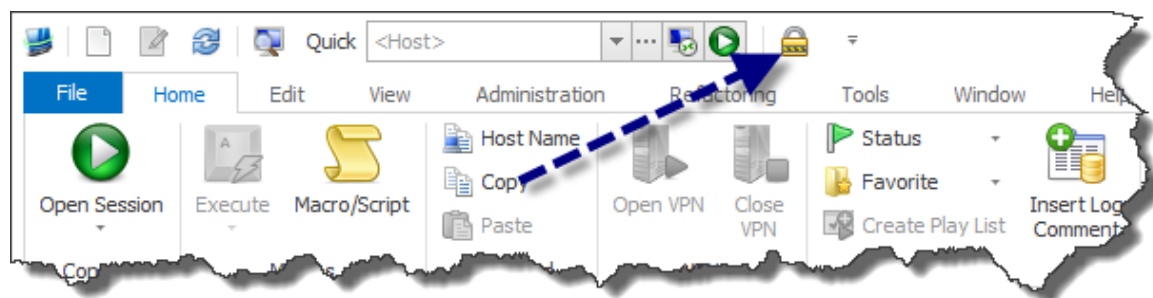
☐ Lock application when minimized
☐ Lock on idle
 minutes

Lock

Option	Description
Lock application when minimized	Lock application when minimized in the taskbar.
Lock on idle	Automatically lock the application when it's not used after a determined number of time. The value is in minute.

Locking the application

You can manually lock the application by clicking on **File -> Lock Application** or by pressing the Lock Application button in the Quick Toolbar.



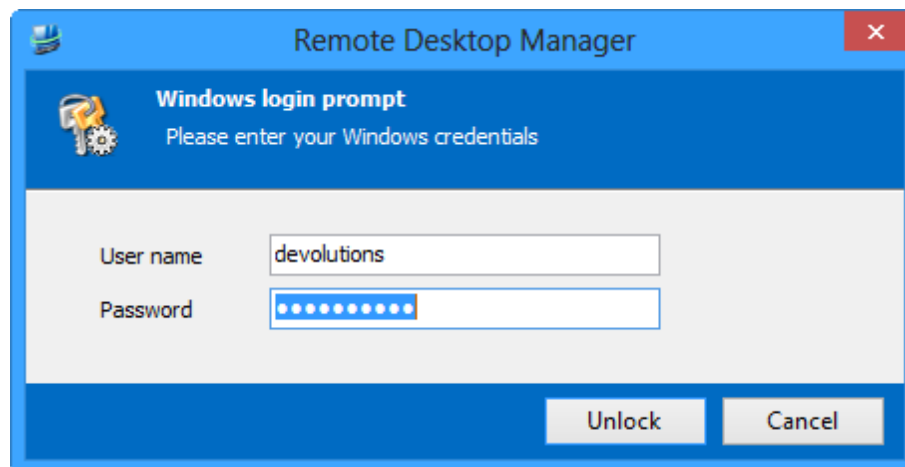
Lock Application button



The Lock Application button can be hidden by configuration. Check **Disable lock in quick toolbar** in **File -> Options -> User Interface -> Advanced**

Unlocking the application

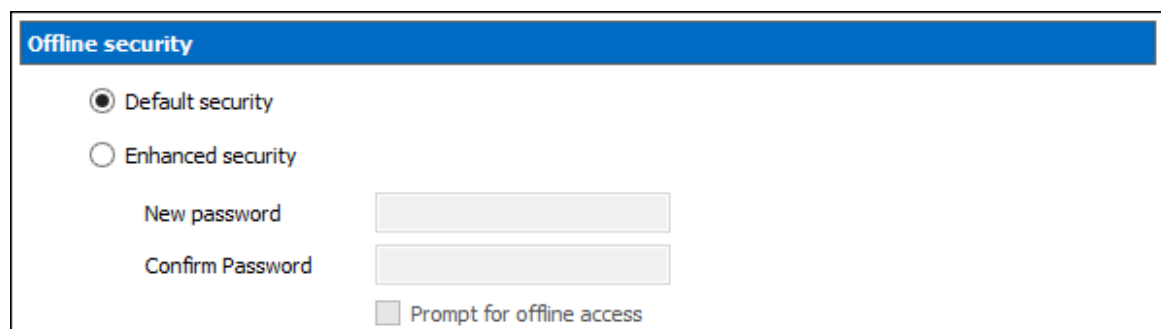
When you re-activate the application, you will be prompted with the application login screen and you might have to enter your password, use the Yubikey or the Google Authenticator to get access to the main screen.



Unlock the application

Offline security

This section contains the global offline security settings.

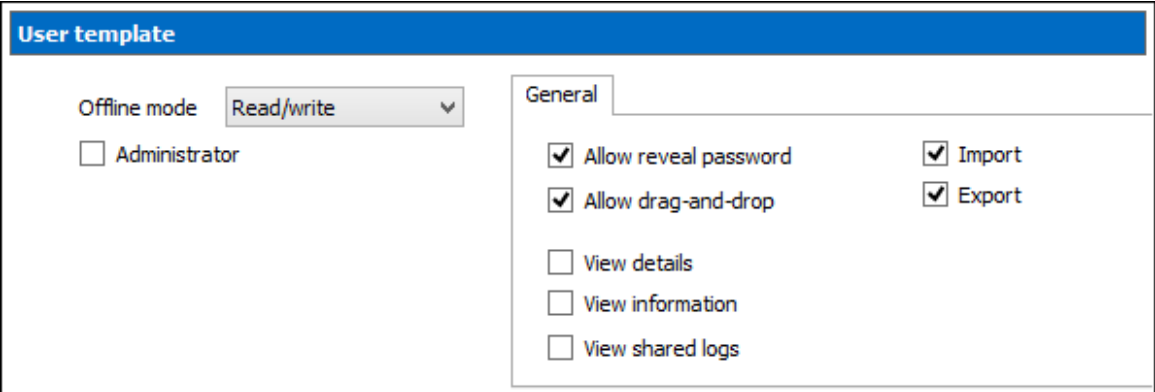


Offline security

Option	Description
Default security	The application uses an offline file is encrypted with a non-portable computed key hash.
Enhanced security	The application uses an offline file is encrypted with a hash of the non-portable computed key plus user specific password. This password is saved internally by default.
Prompt for offline access	This checkbox force the user to enter the password prior to accessing the offline data.

User template

This section contains the default values used when a new user is created in an data source. It's used as a template to simplify the batch creation process.



The screenshot shows a window titled "User template" with a blue header bar. Inside, there are two main sections. On the left, under "Offline mode", there is a dropdown menu set to "Read/write" and a checkbox labeled "Administrator" which is currently unchecked. On the right, there is a tabbed interface with the "General" tab selected. This tab contains several options: "Allow reveal password" (checked), "Allow drag-and-drop" (checked), "View details" (unchecked), "View information" (unchecked), "View shared logs" (unchecked), "Import" (checked), and "Export" (checked).

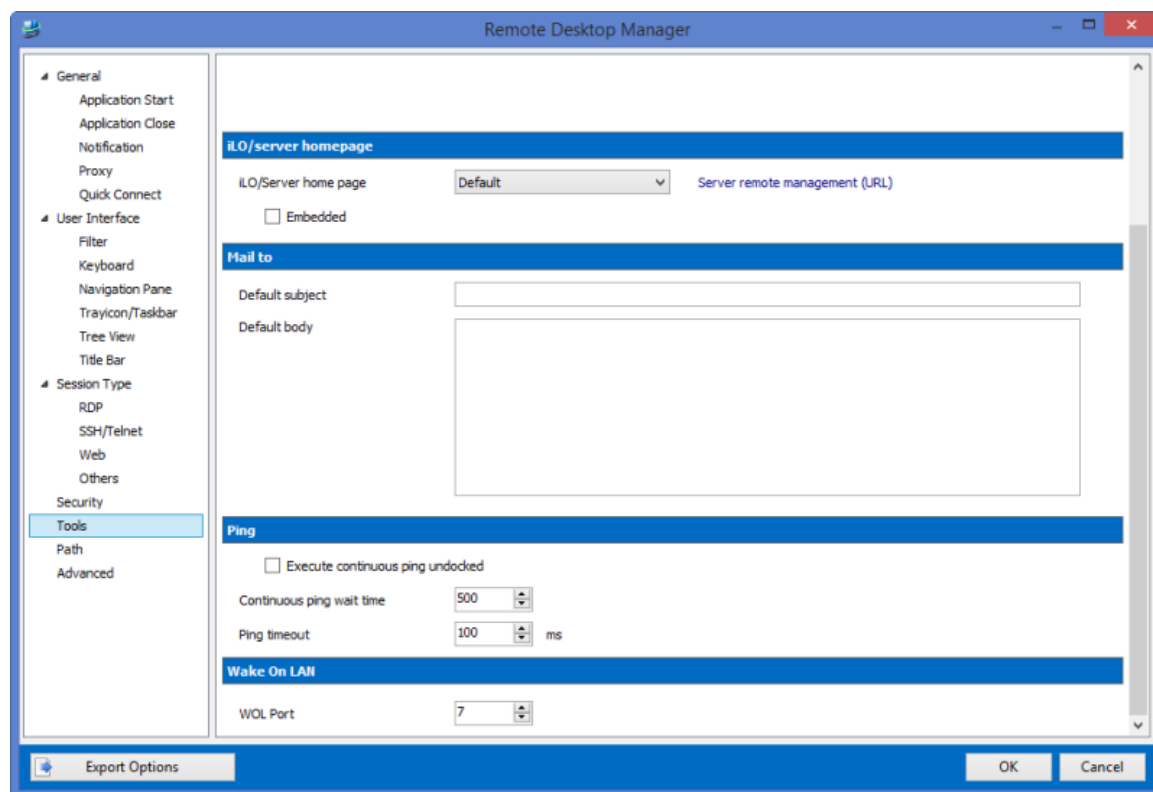
User template

See the [User Permissions](#) section for more details about the different fields.

3.1.8.6 Tools

Description

Use the **File -> Options -> Tools** to control application behaviour as it pertains to iLO, Mail to, Ping and Wake On Lan.



Tools

Settings

iLO/Server homepage

Option	Description
iLO/Server home page	Choose your preferred browser to connect to the iLO system.
Embedded	Indicate the default mode for opening the iLO or server home page. When checked, Please note the embedded will disable the browser selection drop down since only IE can be selected for now.

Mail To

The application allows you to send emails to various contacts as described in [Contact](#). This section serves as a template for emails sent through system.

All [variables](#) are supported in the subject and in the body. This enables rich context sensitive emails.

Option	Description
Default subject	Default subject of the email.
Default body	Default body of the email.

Mail to

Default subject: A quick note on the \$NAME\$ session in RDM

Default body: \$HOST\$
\$DOMAIN\$

Mail to options

Ping

Option	Description
Execute continuous ping undocked	Indicate to undock the continuous ping window when executed.
Continuous ping wait time	Set the interval between the ping sequences.
Ping timeout	Set the timeout for the default ping operation.

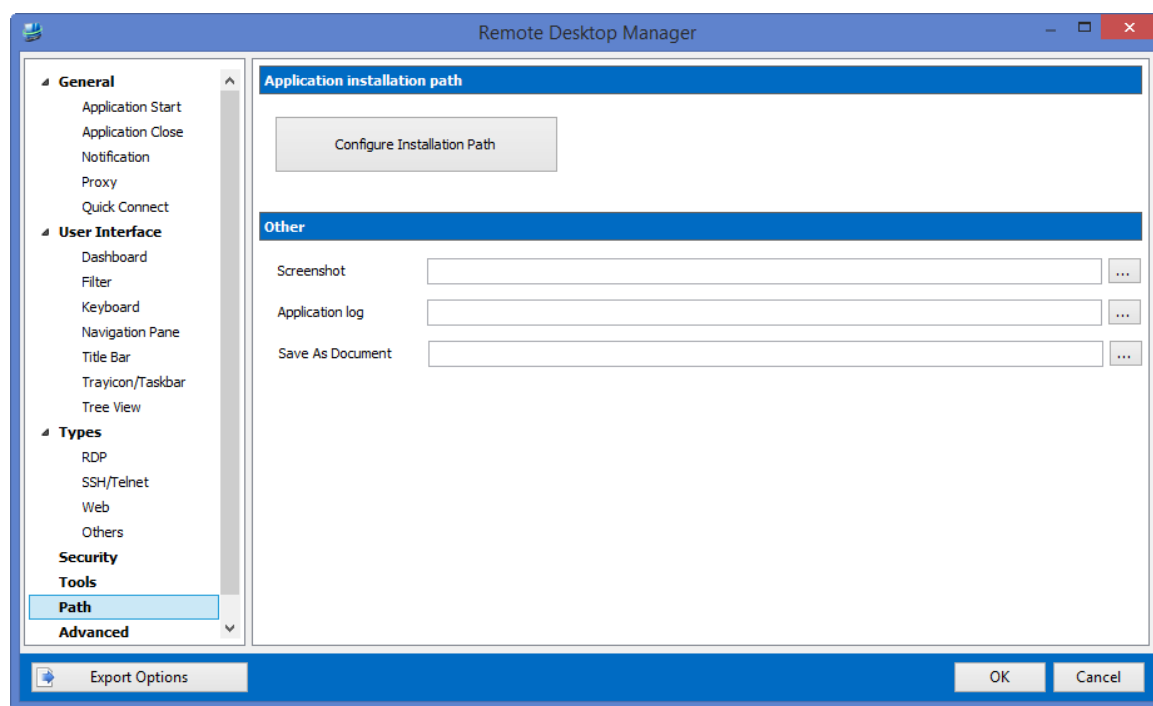
Wake On LAN

Option	Description
WOL Port	Specify the default port for the Wake On LAN.

3.1.8.7 Path

Description

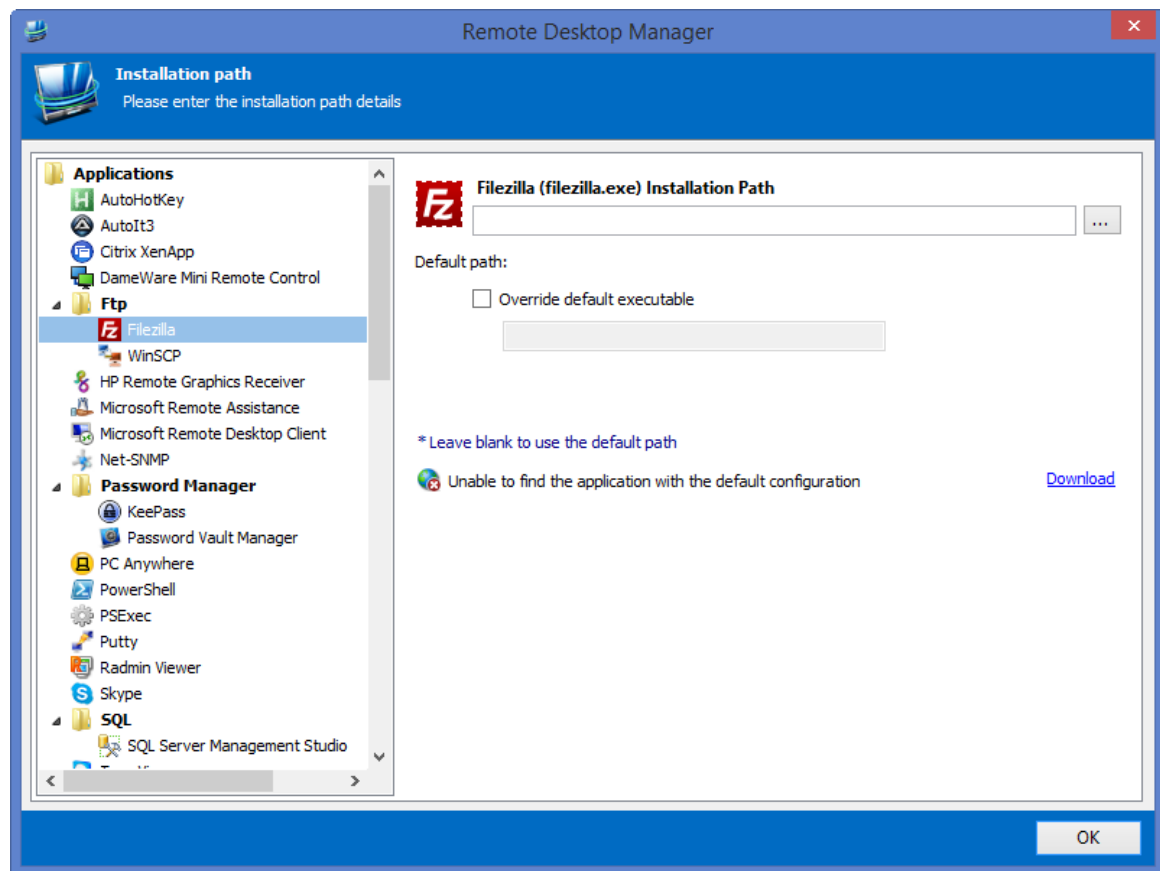
Use the **File -> Options -> Path** to control application behaviour as it pertains to the third party applications that Remote Desktop Manager is able to integrate with. It also contains the default destination path for the screenshots and logs.



Path

Settings

Configure installation path



Configure Installation Path

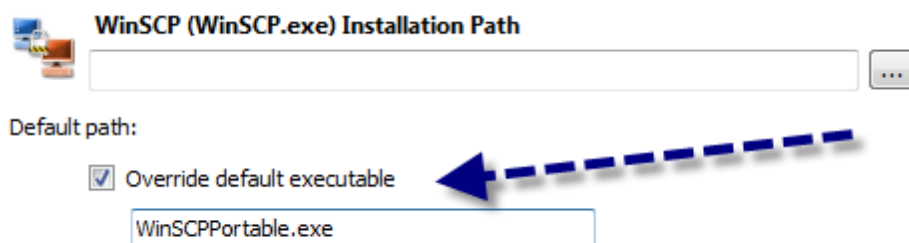
For each third party application, Remote Desktop Manager will attempt to locate it using default installation paths. Typically as soon as you have a third party application installed using the default settings you should see a message indicating the application is ready.



Application is ready label

Click on the ellipsis button to browse for the executable when you have a local installation that is not detected automatically. This will allow you to manually find and specify the installation path for the third party.

Some third party applications offer different executable names. For example this is true for a portable version or a customized distribution like portable Putty. You can specify this custom name by checking the Override default executable and specifying the new name with the file extension.



Override default executable check box and text area

We have added a download link for your convenience . Clicking on this link will bring you to the default site where you can locate and download the installer for the third party application.

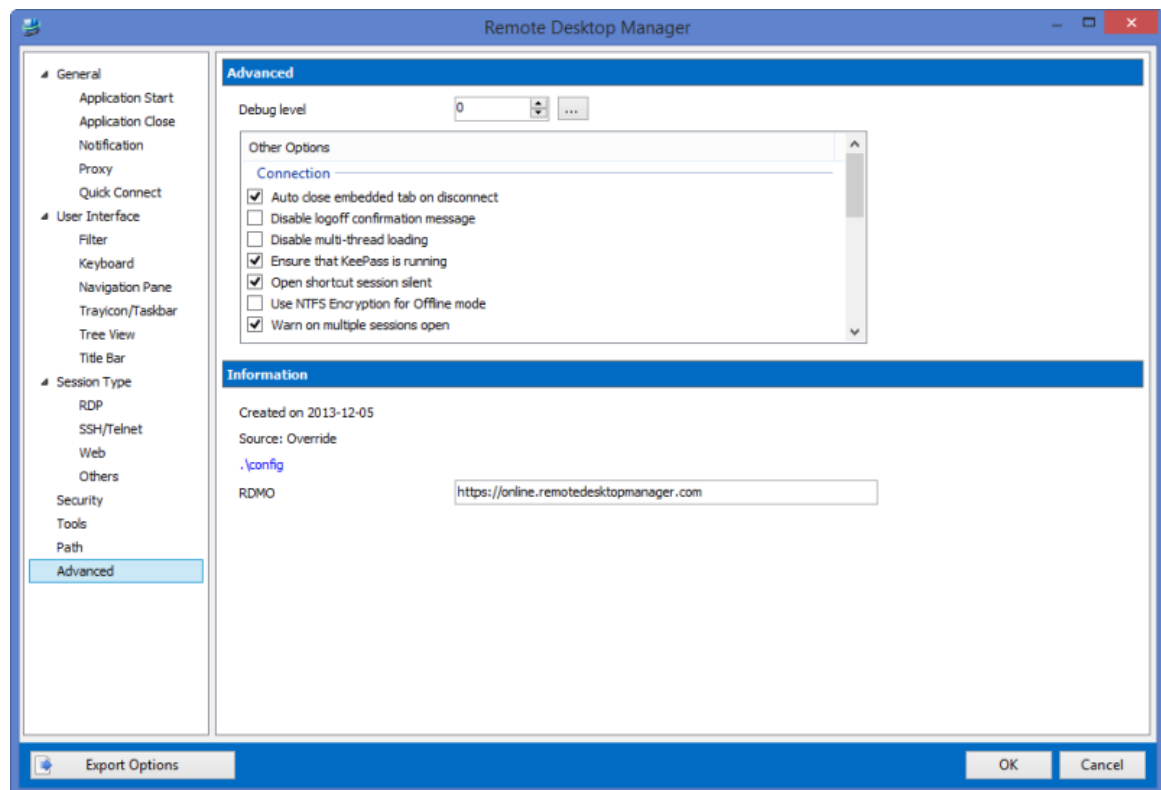
Other

Option	Description
Screenshot	Specify a path to store the application screenshots available at Action-> Screenshot .
Application log	Specify a path to store the application logs available at Help-> Application Logs .
Save As Document	Specify a path to open a default folder when a document need to be saved.

3.1.8.8 Advanced

Description

Use the **File -> Options -> Advanced** tab to control application behaviour as it pertains to low level settings.



Advanced

Settings

#

Advanced

Option	Description
Debug level	Set the level of debugging information that Remote Desktop Manager will capture. This should be modified only on request from a Devolutions support technician and it might slow down your system.

Other Options

Option	Description
Auto close embedded tab on disconnect	Automatically closes the tab for embedded sessions when they are disconnected.
Disable logoff confirmation message	When pressing the logoff button in a embedded RDP session, Remote Desktop Manager, will disconnect the session without the logoff confirmation message.
Disable multi-thread loading	This setting allow Remote Desktop Manager to use multiple thread to load the data. Disable this will decrease performance.
Ensure that KeePass is running	Validate that KeePass is running on your computer before accessing any KeePass data.
Open shortcut session silent	Disable the command line warning message when using a shortcut.
Use NTFS Encryption for Offline mode	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.
Warn on multiple sessions open	When opening more than one session you'll be presented with a confirmation dialog. This typically occurs when doing an Open session on a group/folder.
Allow multiple instances	Allows more than one instance of Remote Desktop Manager to run concurrently. This is not recommended.
Disable stack trace	Disable the stack trace details when an error happens in Remote Desktop Manager. This is a security feature.
Focus content on application activation	This will set focus on the last embedded session when the application is activated.
Force refresh before edit entry	This will perform a refresh of the entry just before entering in edit mode. This is useful in a multi-user environment with a shared data source. This ensures that you are editing the most recent version of the entry.
Always show "Go Offline" button	It will always display the "Go Offline" button in the status bar when Offline Mode is active.
Disable custom images	This will 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 are expanded automatically.
Hide last opened play list in play list management	This will not show the last opened play list at the startup in the play list dialog.
Hide version label	This will hide the version label from both the startup screen and from the main program window. Simply an option to lighten the interface.
Use old entry sort	Use the old entry sort from previous version of Remote Desktop Manager.

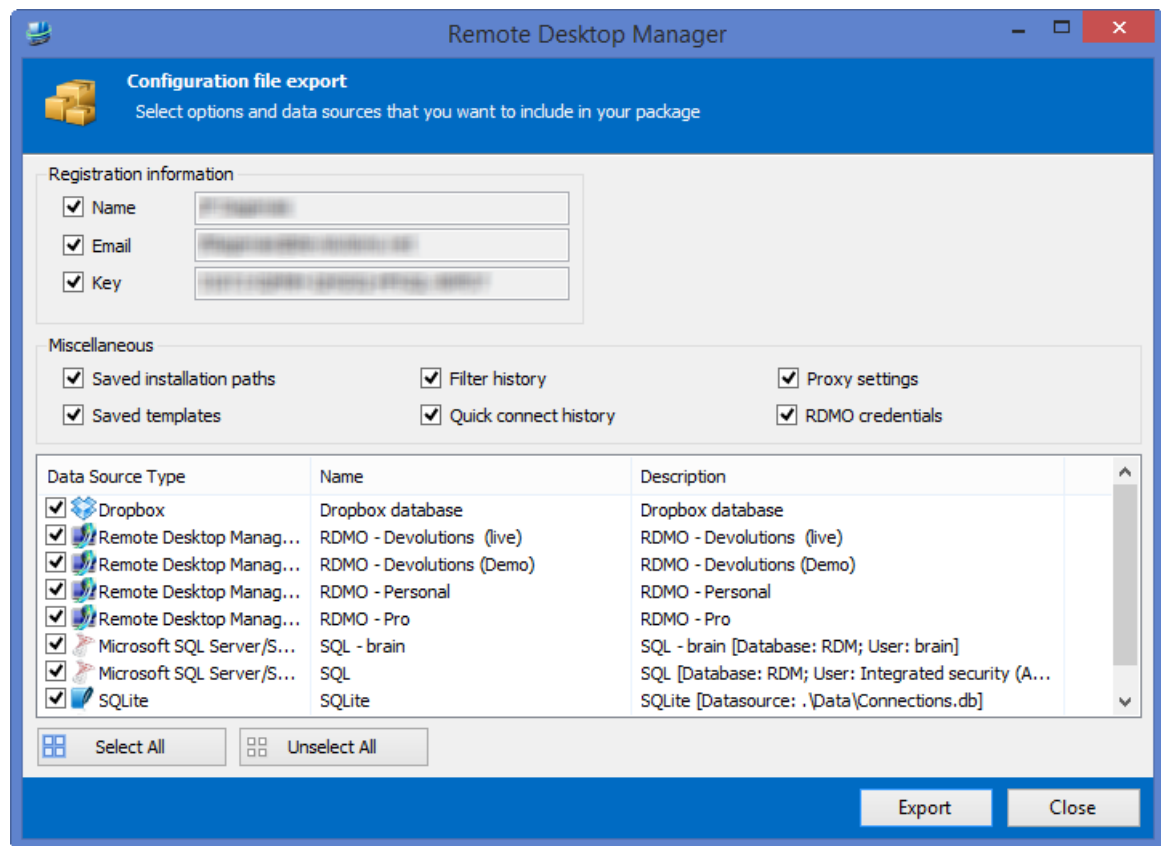
Information

Option	Description
Created on	Creation date of the Remote Desktop Manager configuration folder.
Source	Source of the Remote Desktop Manager configuration settings.
Path	Shortcut to access the configuration folder directly.
RDMO	RDMO Website address. Available in debug mode only.

3.1.8.9 Export Options

Description

Use **File -> Options -> Export Options** to control the options to export your application configuration. Use this to easily transfer settings to another machine or share them with a colleague.



Export Options

Settings

Registration information

Option	Description
Name	Company registration name
Email	Registration email
Key	Serial key

Miscellaneous

Option	Description
Saved installation paths	Preserve your installation paths configured for the external application
Saved templates	Includes your local templates in the export
Filter history	Preserve your filter history
Quick connect history	Preserve your Quick connect history
Proxy settings	Includes your proxy settings
RDMO Credentials	Includes your Remote Desktop Manager Online credentials

Data Sources



The data source configurations you select will be exported with the username/password as they are configured currently. If you are creating a file so you can quickly set up a new employee, you must take care of not giving away your credentials.

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.

How to restore the settings

See [Configuration File Location](#) topic

3.1.9 Templates

3.1.9.1 Templates

Description

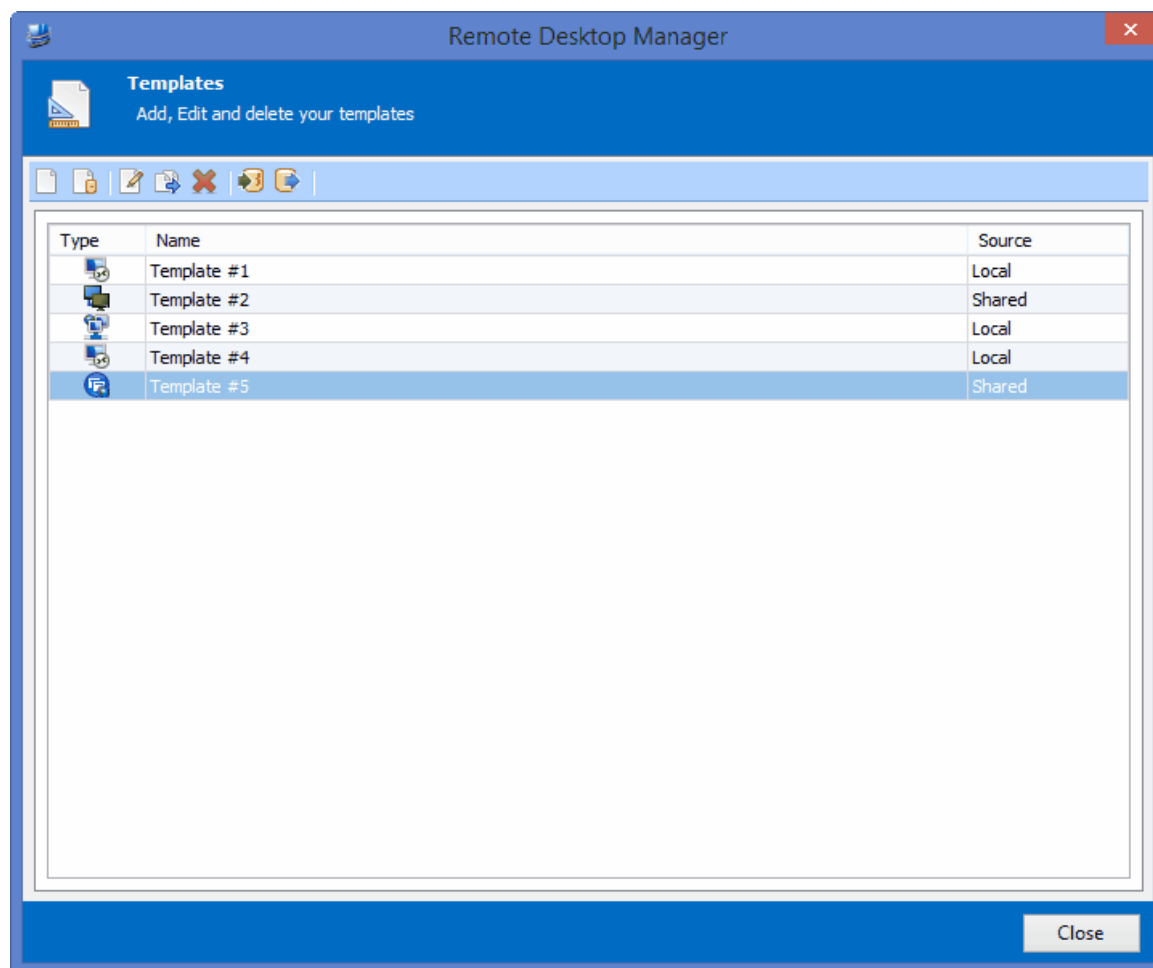
This allows you to create predefined configuration available such as:

- Create a new session
- Quickly connect
- Open as a template
- Create an import wizard

Templates can be useful if you want to have predefined values when you create a specific entry. It's possible to create Local templates and/or Shared Templates.

Templates are available in the options dialog or via the menu **File -> Templates -> Templates**

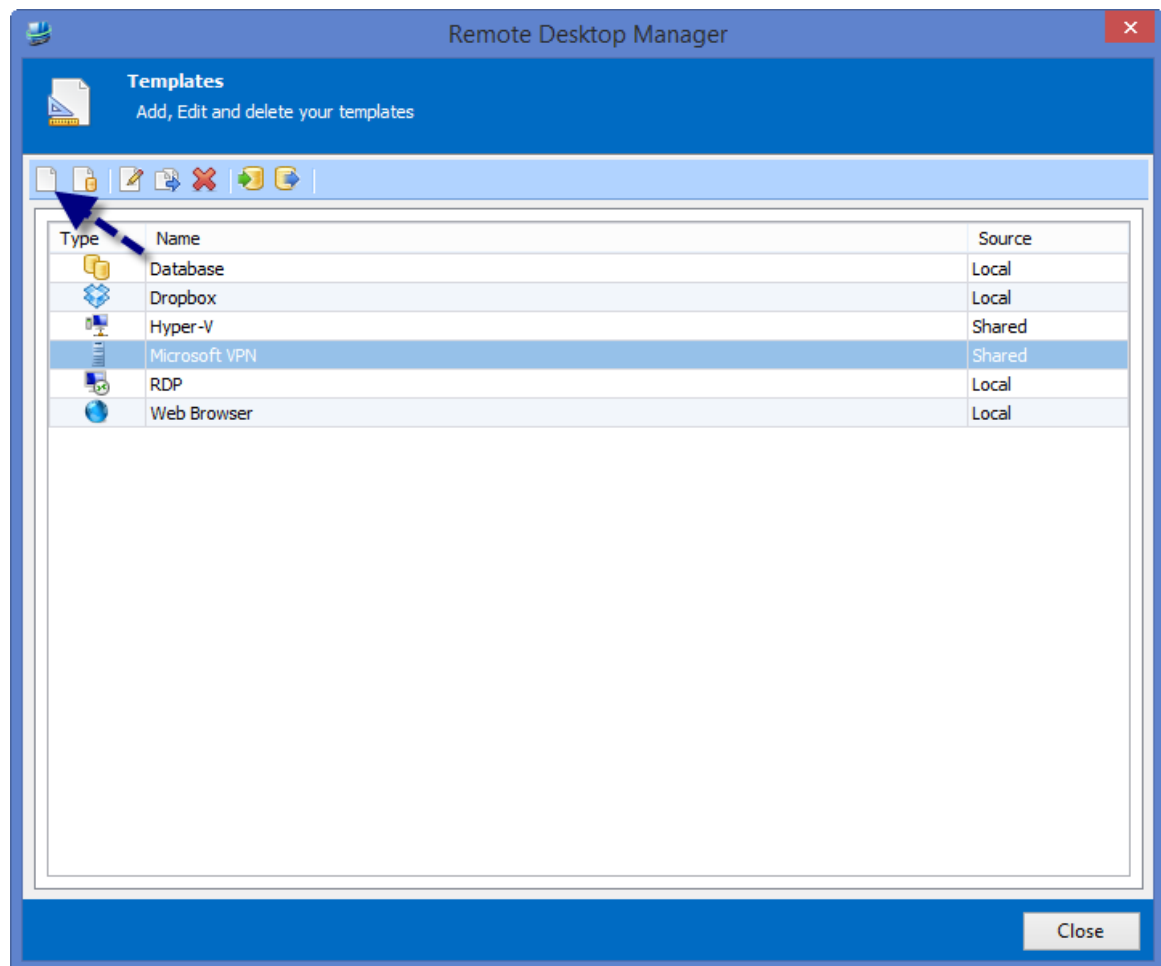
This allows you to create predefined templates that are available with the quick connect toolbar, or when you create or import a new session.



Templates

Local Template

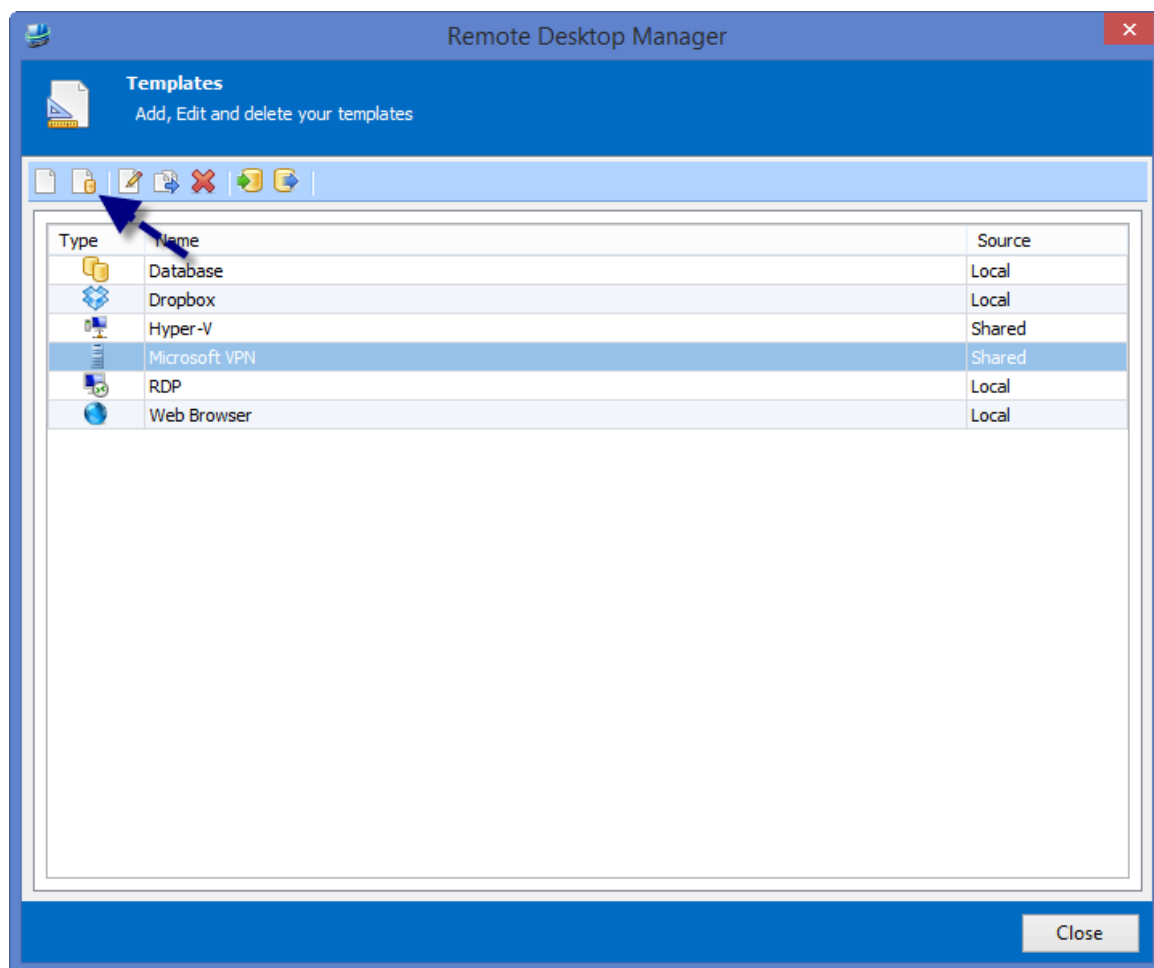
Local templates are saved on the local computer, and are not available to other users.



Local Template

Shared Template

Shared templates are saved in the database, and can be used by all the users.

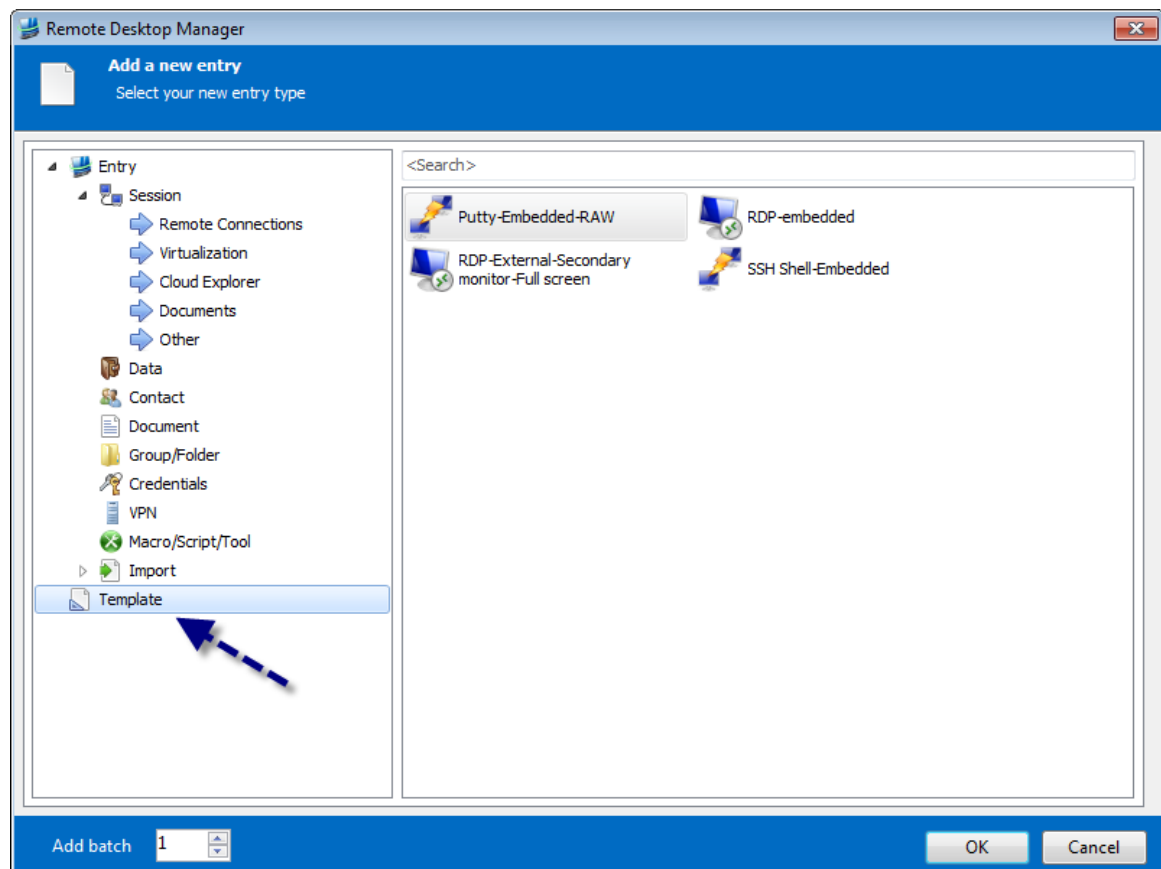


Shared Template

Usage

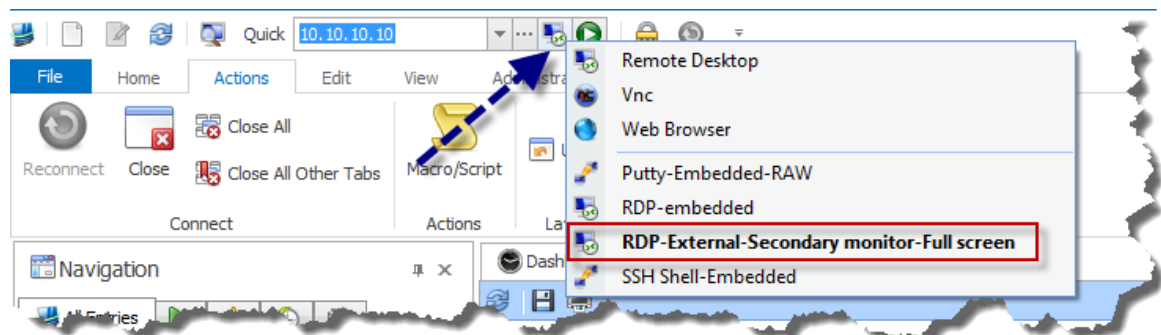
The template can be used in the following cases:

Creating a new session



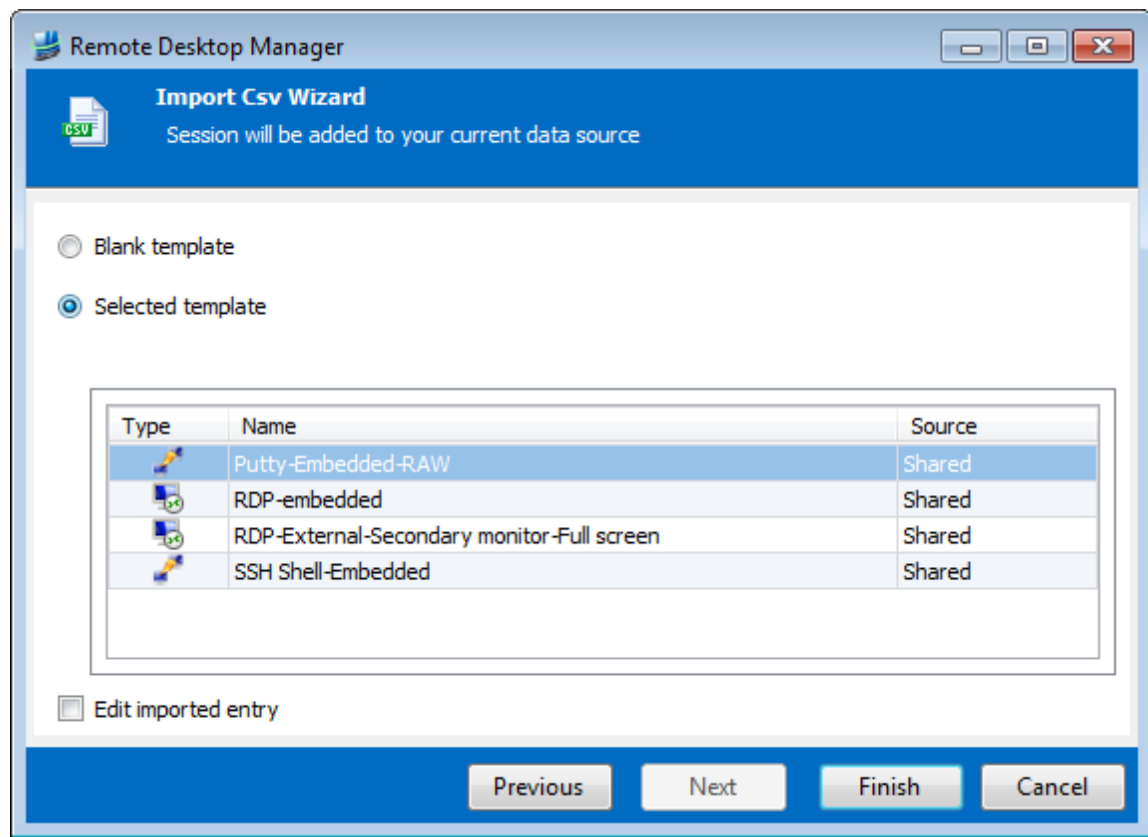
New Entry dialog - Template selected

Running a Quick connect session



Import session wizard

Using the import session wizard, the second step allows you to use a template for the imported sessions.



Import session wizard

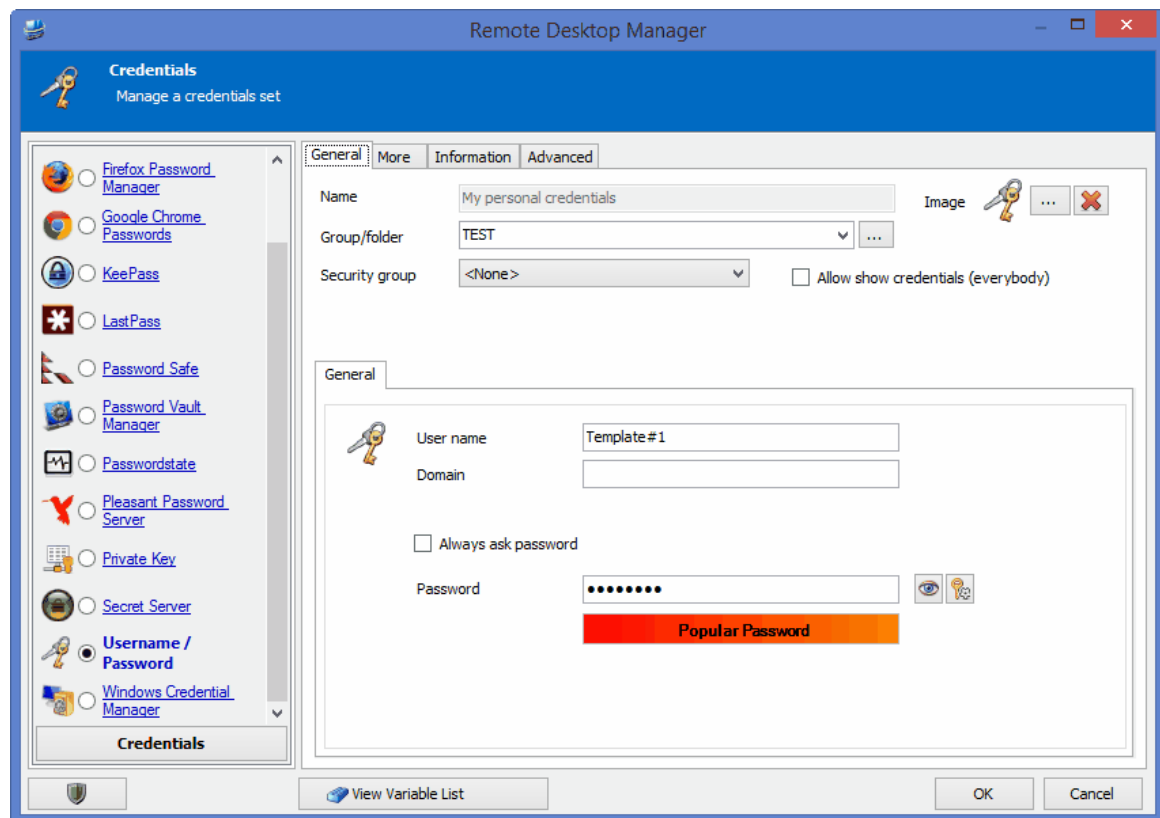
3.1.9.2 My Personal Credentials

Description

The *My Personal Credentials* feature is a single credential entry stored in your private area of the database.

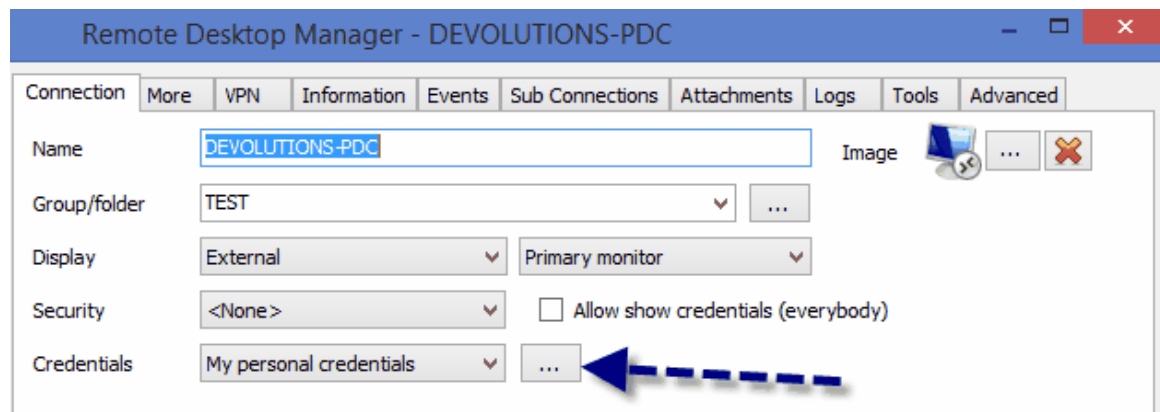
It is typically used to hold the Windows credentials for your running session because Remote Desktop Manager cannot access them. If you cannot use integrated security then you must store your credentials in *My Personal Credentials*.

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*.



Personal Credentials

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



My Personal Credentials

For more information on credentials, please refer to the [Credentials](#) topic.

3.1.9.3 Default Settings

Description

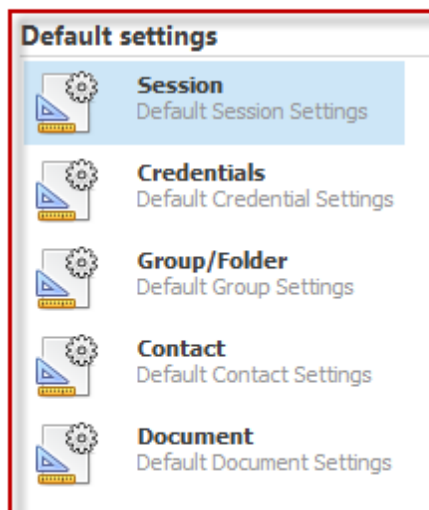
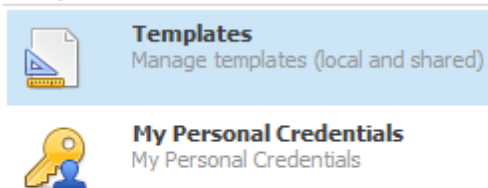
This allows you to create, edit or reset your default that are used whenever a new entry is created. Every entry type is supported and can have a default template defined.

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

All of the entry types are organized by category, as in the new entry dialog, in order to help you locate the entry type you want to customize.

- Session
- Credentials
- Group/Folder
- Contact
- Document

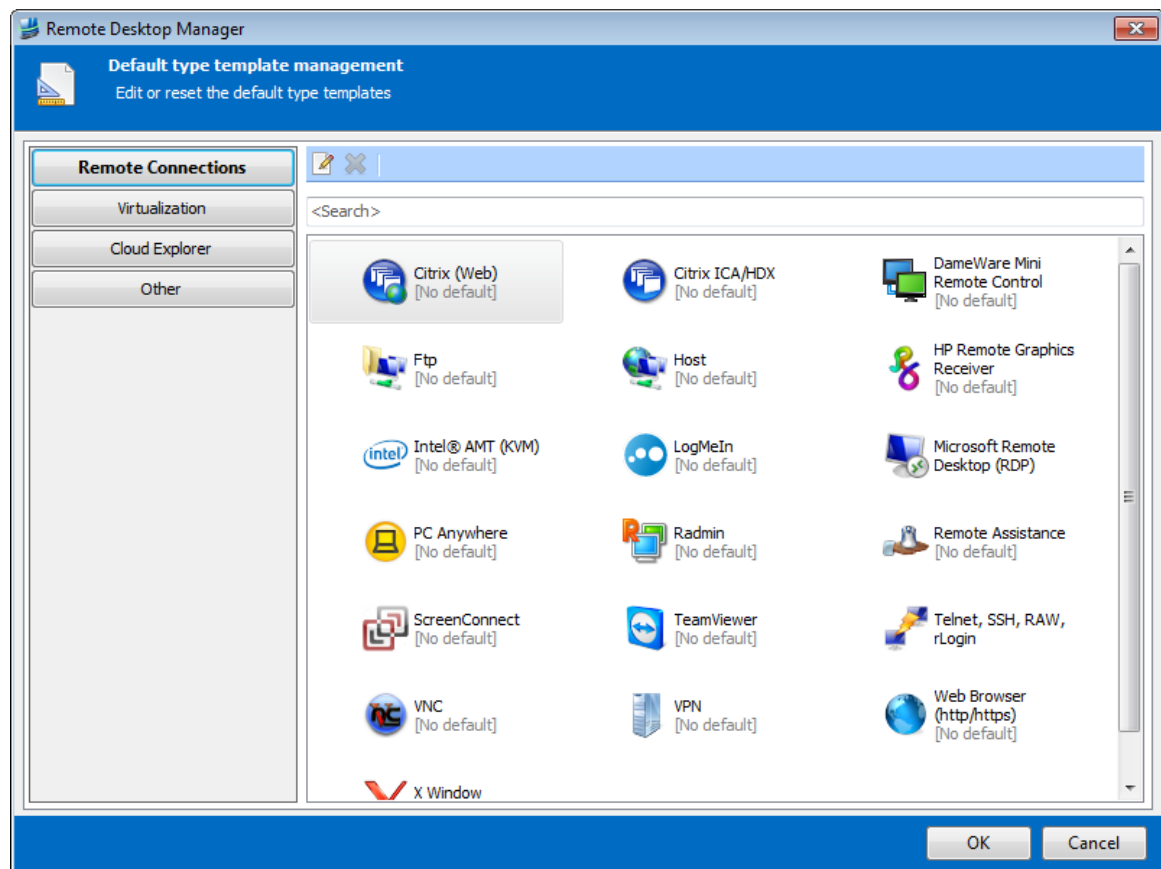
Templates



File - Templates

Workflow

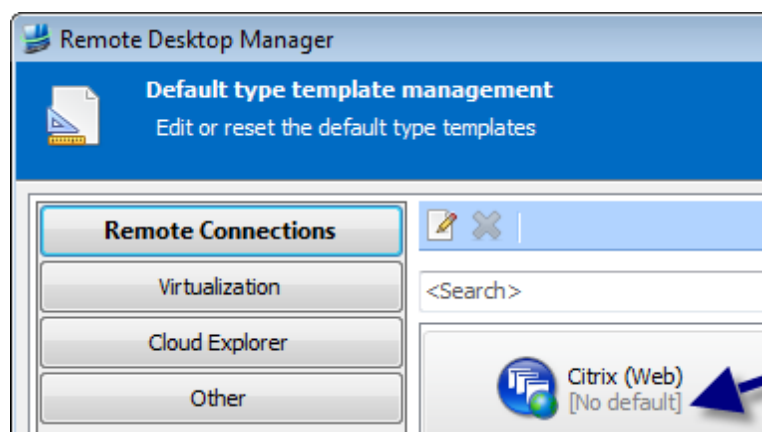
After selecting your category, a window will appear with all of the entry types for that category.



Template management

No template defined

Notice that a **[No default]** notice is displayed below each type that does not have a default template defined.

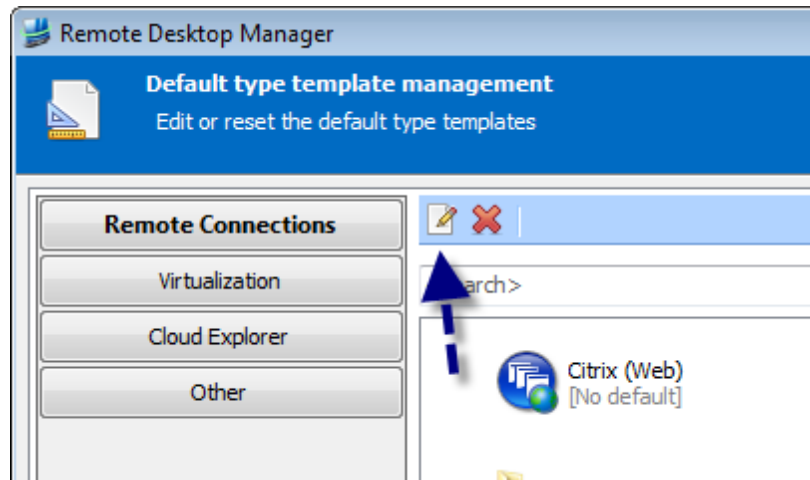


No Default highlight

Selecting a type without a default will allow you to create a new template.

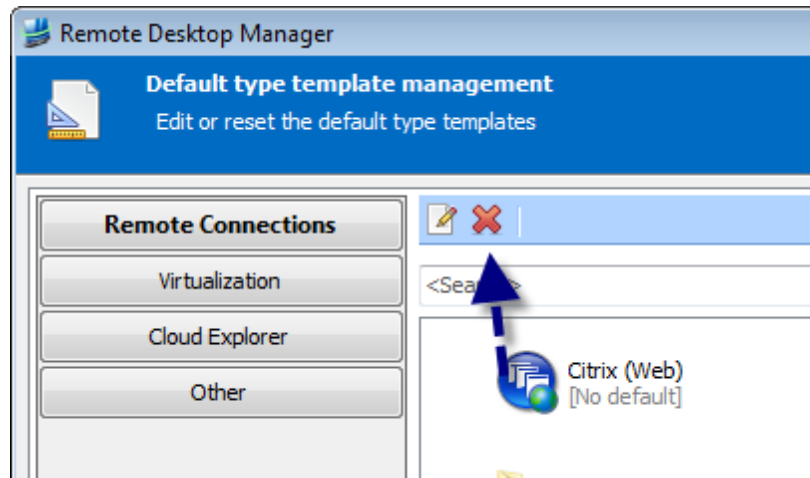
Template defined

All the 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



Edit button detail

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



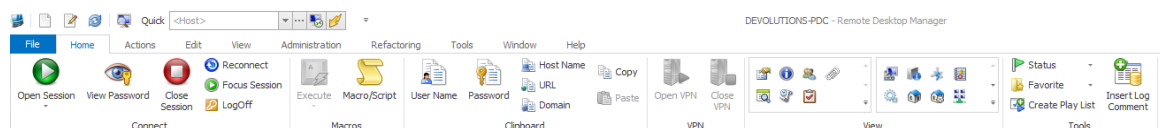
Delete button detail

3.2 Home

3.2.1 Overview

Description

The Home menu will allow you to do some actions on the current session. The ribbon will display the following tab when the session is embedded.



Home tab

Consult topics below for more information on each sections:

- [Connect](#)
- [Macros](#)
- [Clipboard](#)
- [VPN](#)
- [View](#)
- [Tools](#)

3.2.2 Connect

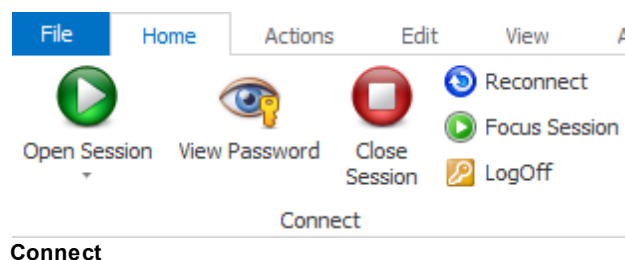
Description

The Connect section in Home tab allow you to open\close\reconnect your sessions.



Actions are different depending on your session type.

Settings



Open Session

Allow you to open your session. You can also select another mode to open your session with this option.

View Password

Allow you to see the session password

Close Session

Close the active session.

Reconnect

This perform a full reconnect on RDP session. This will completely close the session and reopen it.

Focus Session

Focus on the active session.

Logoff

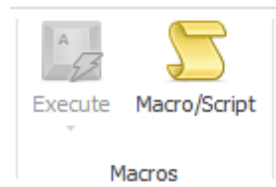
Logoff the RDP session. See [Logoff](#) topic if any problems.

3.2.3 Macros

Description

The Macros section in Home tab allow you to execute scripts or macros.

Settings



Macros

Execute

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

Macro/Script

Displays a window where you can Select a macro or script, as well as the execution options.

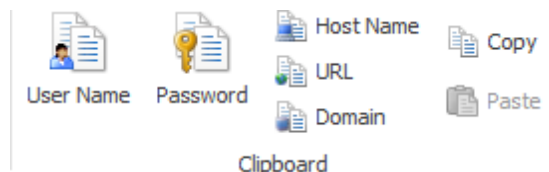
3.2.4 Clipboard

Description

The Clipboard section in Home tab allow to copy data entries values in your clipboard such as:

- Username
- Password
- Domain
- Host Name
- URL

Settings



Clipboard



When using an [Advanced Data Source](#), the administrator can control in the [Data Source Settings](#) if copy passwords are permitted or not.

Username

Copy the username define in your session to the clipboard.

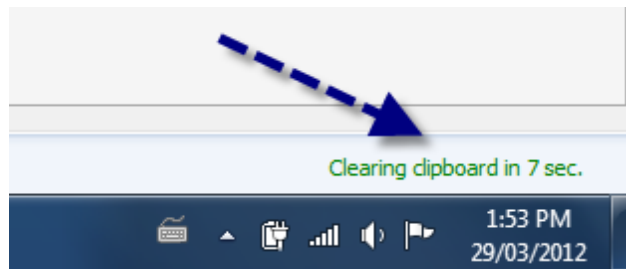
Password

Copy the password define in your session to the clipboard.

The password to clipboard most also be allowed for the feature to be available. Check "Allow copy credentials to clipboard" for the given session.



For security reasons, the clipboard will be cleared after **10** seconds when you copy a password. The delay can be configured via the system options, see [Options](#) for more information.



Clipboard clear notification

Domain

Copy the domain define in your session to the clipboard.

Host Name

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

URL

Copy the URL define in your session to the clipboard.

Copy/Paste

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



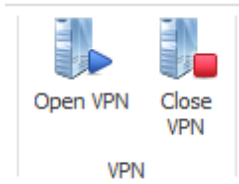
When using an [Advanced Data Source](#) the user must have Add Session rights to be able to copy/paste sessions.

3.2.5 VPN

Description

The VPN section in Home tab allow to open/close a VPN without connecting or disconnecting the session.

Settings



VPN



This feature is enable when a VPN his configure inside your session.

Open VPN

Open a VPN that is configure inside a session before your start the connection to the session.

Close VPN

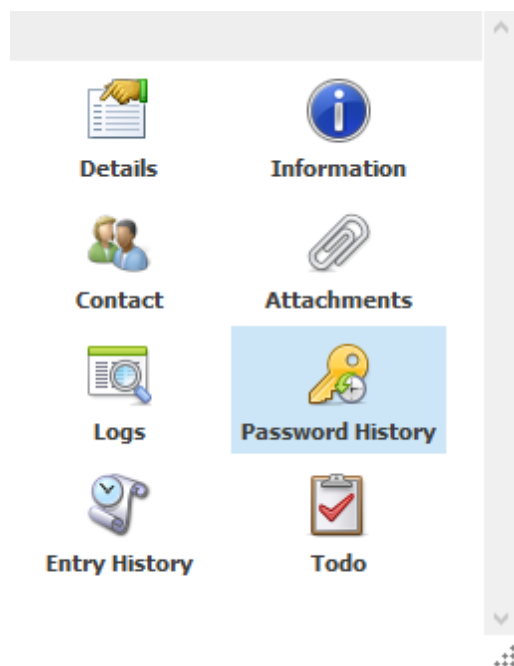
Close a VPN that is configure inside a session and leave the session open.

3.2.6 View

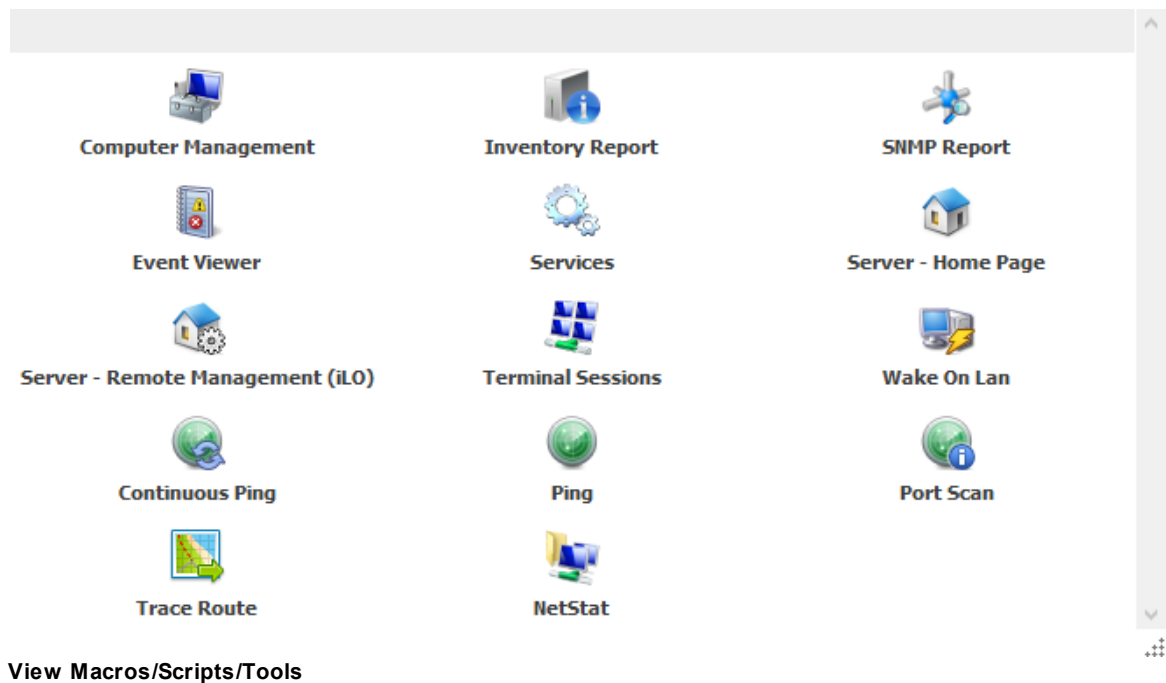
Description

The View section in Home tab will display multiple information on the remote session.

Settings



Option	Description
Details	Display the connection details. See Details topic for more information.
Information	Display several information on the entry. See Information topic for more information.
Contact	Display the contact information. See Contact topic for more information.
Attachments	Display the attachments file. See Attachments topics for more information.
Logs	Display remote computer logs. See Logs topic for more information.
Password History	Display the password history for a session. See Password History topic for more information.
Entry History	Allows you to compare two entries and manage history revisions. See Entry History topic for more information.
ToDo	Allow you to manage ToDo's related to the session. See ToDo Actions topic for more information.



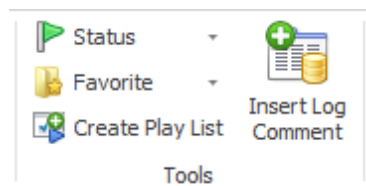
For more information, please consult the [Macros/Scripts/Tools Overview](#) topic.

3.2.7 Tools

Description

The Tools section in Home tab allow to change the status of a session, create/delete favorite, create a Play List and Insert Log Comment.

Settings



Tools

Status

Locked Status

This allow the user who has locked the session to use it and block the others.



The session will be locked for other users only. The holder of the lock can still use it. To prevent usage of a session by everybody you must disable it.

Disabled Status

A disabled session can't be opened. It's mostly used when you don't want to delete it but avoid any unattended connection. It's also useful to disable an account for one of your former customer.

Warning Status

This status allows the session to be used, but displays a message to the user before it is opened.

Expired Status

An expired session can't be opened. It can be set manually or automatically if the session expiration date is set in his property.

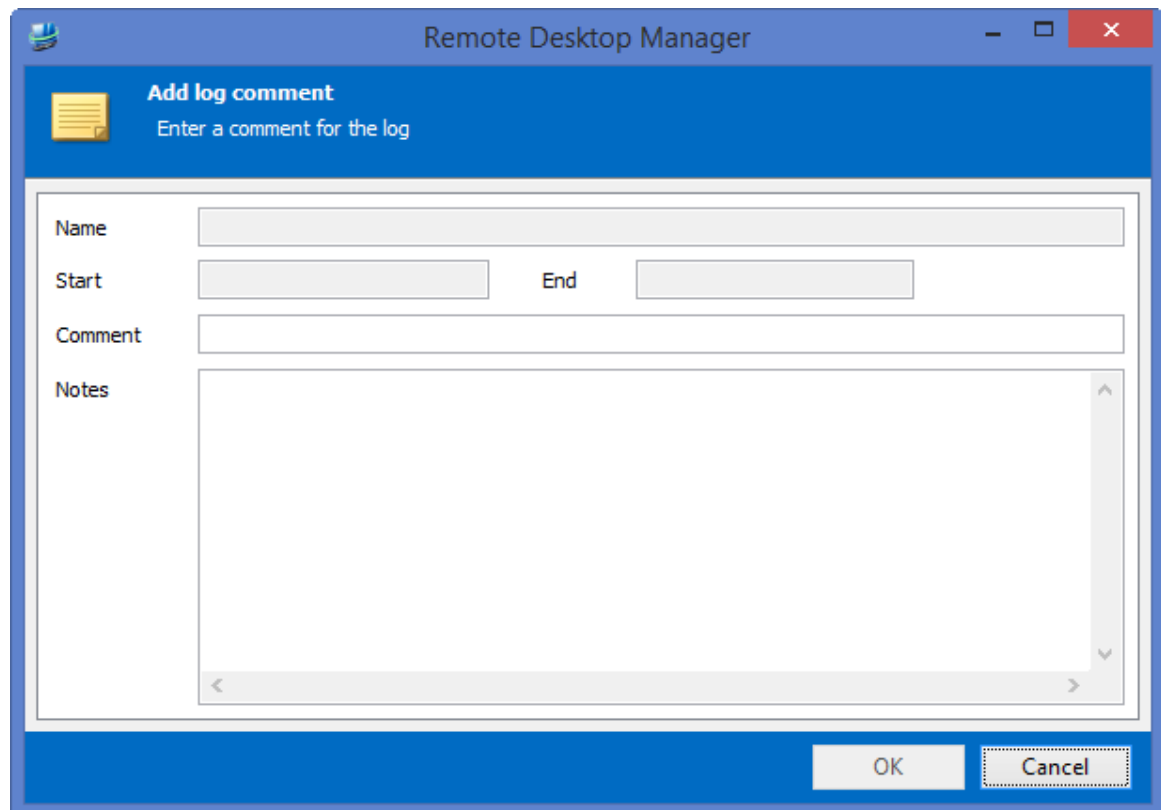
Favorite

Please consult [Favorite Entries](#) topic for more information.

Create Play List

Please consult [Play List](#) topic for more information.

Insert Log Comment

The image shows a screenshot of a software window titled "Remote Desktop Manager". Inside the window, there is a sub-dialog titled "Add log comment" with a yellow notepad icon. Below the title, it says "Enter a comment for the log". The dialog contains several input fields: a "Name" field, "Start" and "End" date/time fields, a "Comment" text field, and a "Notes" area with a large text box and a scrollbar. At the bottom right of the dialog are "OK" and "Cancel" buttons.

Log comment

Add a log comment to the session that will be saved in the session log. To consult the session logs,

right-click on the session and select **View -> Logs**.

3.2.8 Password History

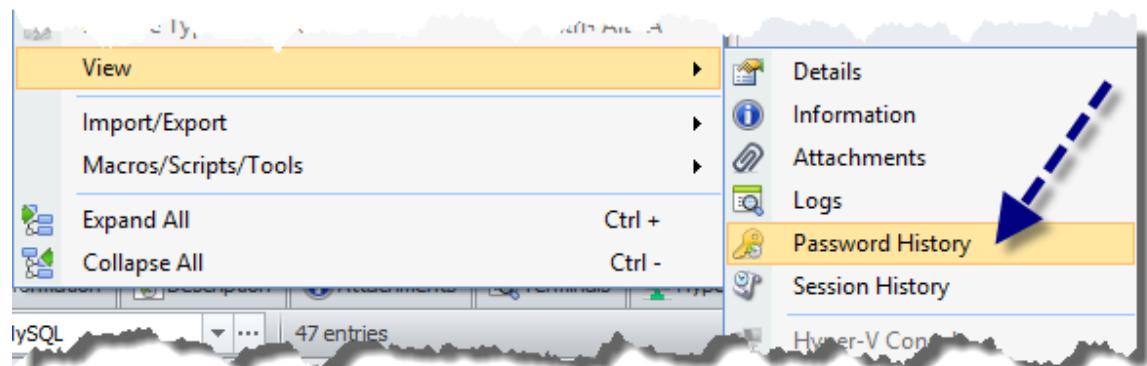
Description



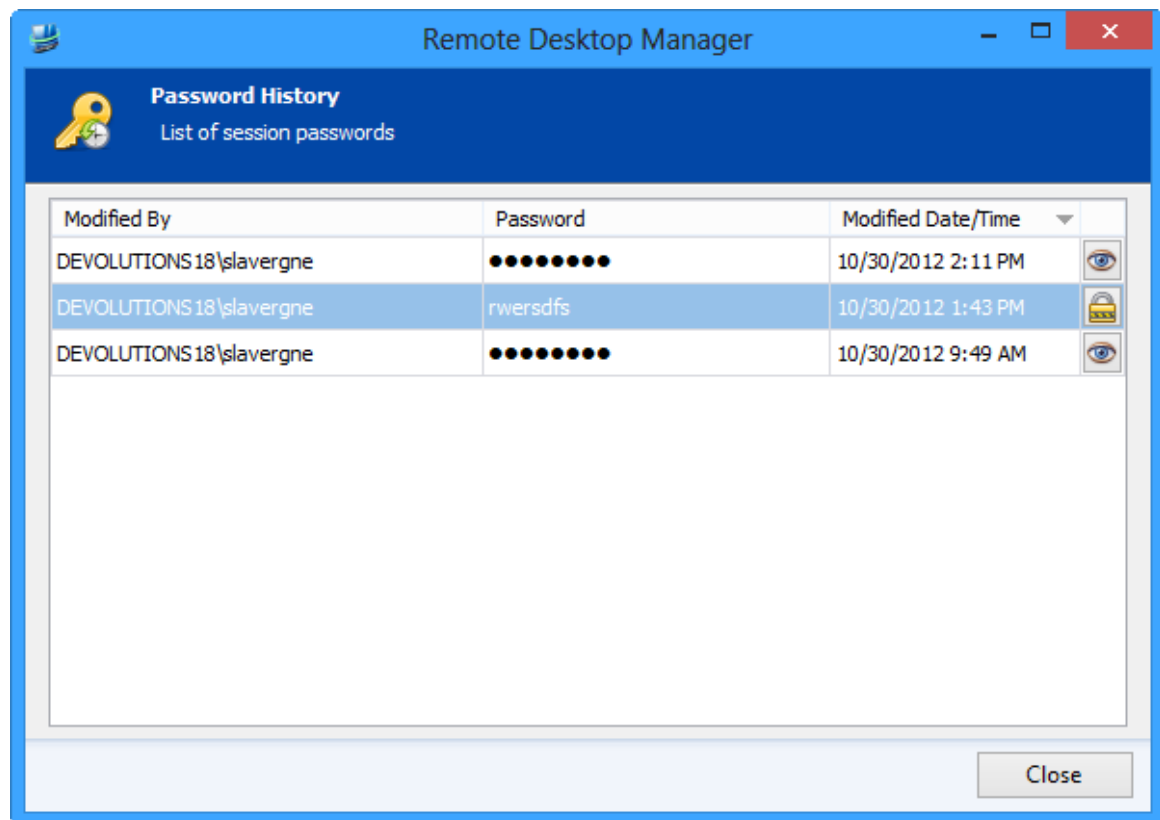
This feature is only available when using an [Advanced Data Source](#).

The Password History feature allows for viewing of the password history for a session. The number of historical passwords to save is set in the [Data Source Settings](#).

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



Right-click View -> Password History



Password History view

3.2.9 Entry History

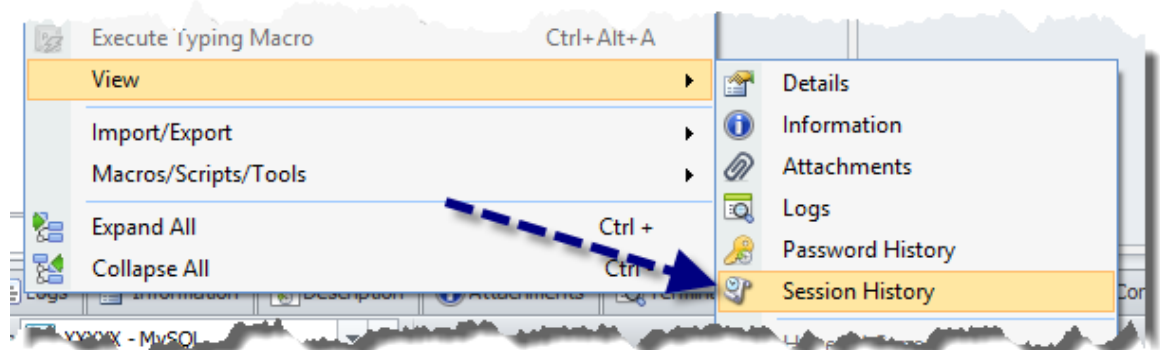
Description



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

Entry history allows for versioning of sessions while allowing for compares.

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



Right-click View -> Session History

Session history view

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

Remote Desktop Manager

Version history
View and compare entry versions

Name: Domian Controller Action: Update

Connection type: RDPCConfigured Group: Office\London

User name: DEVOLUTIONS18\slavergne Created on: 11/12/2012 10:16 AM

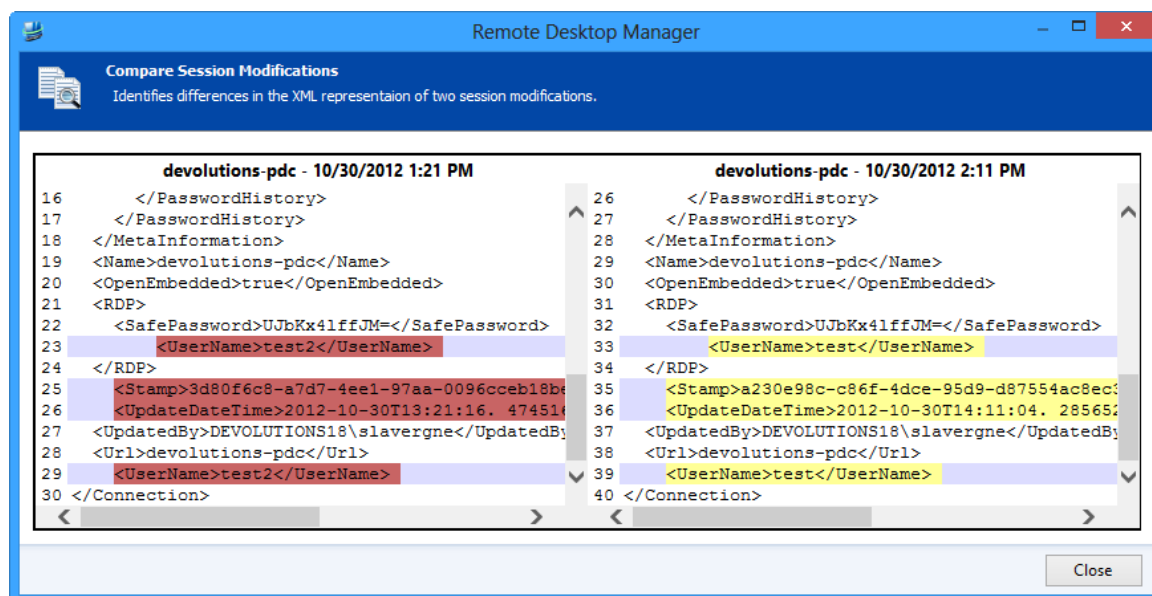
Data source user: root Modified on: 11/12/2012 3:16 PM

Action	Session Type	Name	Group	Created On	Modified On
Update	RDPCConfigured	Domian Controller	Office\London	11/12/2012 10:16 AM	11/12/2012 3:16 PM
Update	RDPCConfigured	Domian Controller	Office\London	11/12/2012 10:15 AM	11/12/2012 3:16 PM
Update	RDPCConfigured	Domian Controller	Office\London	11/12/2012 10:15 AM	11/12/2012 3:16 PM
Update	RDPCConfigured	Domian Controller	Office\London	11/12/2012 10:15 AM	11/12/2012 3:16 PM

< >

Compare Delete Delete All Close

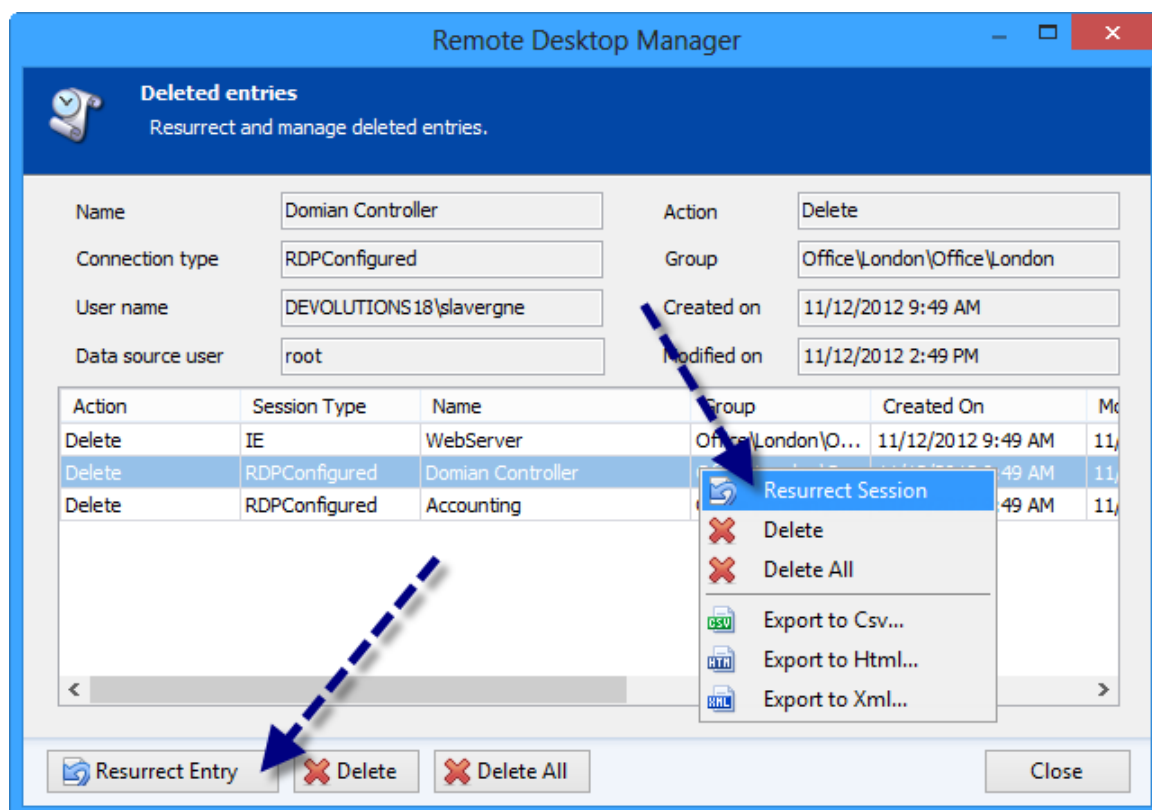
Entry history view



Compare session modifications

View Deleted Entries

Administration -> Management -> [View Deleted Entries](#) allows for the manage and resurrect of deleted entries.



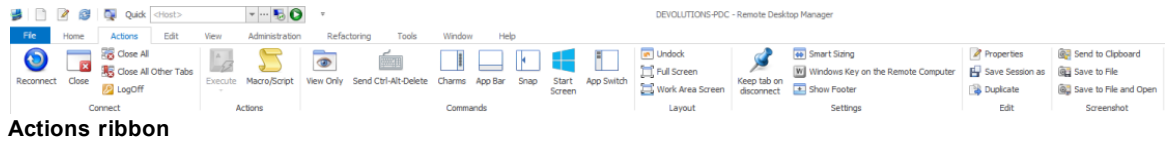
Resurrect entry

3.3 Actions

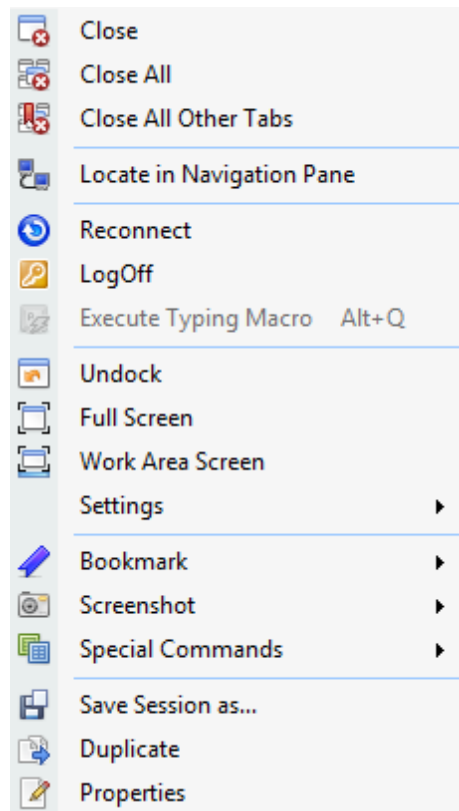
3.3.1 Overview

Description

Actions are operations that can be performed on running sessions. The Actions menus are visible only when the operation is possible. The ribbon will display the following tab when the session is embedded.



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



Right-click on the tab of an embedded session.

The sections are:

- [Connect](#)
- [Actions](#)
- [Commands](#)
- [Layout](#)
- [Settings](#)
- [Edit](#)
- [Screenshot](#)

3.3.2 Connect

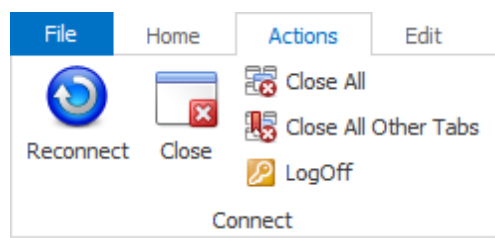
Description

The Connect actions allow you to reconnect\disconnect session(s).



Actions are different depending on your session type.

Settings



Connect Actions

Reconnect

Quickly close the session, then re-open it automatically. Use it to update the resolution of your embedded RDP connections when you resize the window.

Close

Close the active session.

Close All

Close all the opened sessions.

Close All Other Tabs

Close all the opened sessions except the active one.

LogOff

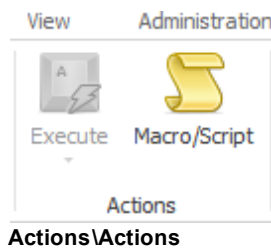
Logoff the RDP session. See [Logoff](#) topic if any problems.

3.3.3 Actions

Description

The Actions section in Actions tab allow you to execute scripts or macros.

Settings



Execute

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

Macro/Script

Displays a window where you can Select a macro or script, as well as the execution options.

3.3.4 Commands

3.3.4.1 Overview

Description

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

Please refer to the following topics for more details:

- [RDP](#)
- [VNC](#)
- [SSH Shell](#)
- [Telnet](#)



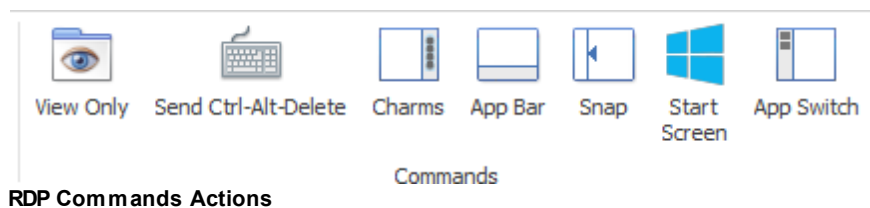
Session add-ons may add custom command in this section, they will not be documented in these topics, but rather in the add-on documentation.

3.3.4.2 RDP

Description

The commands for a RDP session allow you send remote commands to your host.

Settings



View Only

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.

Send Ctrl-Alt-Delete

Send the key combination CTRL+ALT+DELETE to the host.

Charms

On Windows 8 or Windows 2012 server, displays the Charms bar (Search, Share, Start, Devices, and Settings bar).

App Bar

On Windows 8 or Windows 2012 server, displays the App bar to show navigation, commands, and tools.

Snap

On Windows 8 or Windows 2012 server, allows you to run two applications side-by-side.

Start Screen

Open the Start menu on the host computer.

App Switch

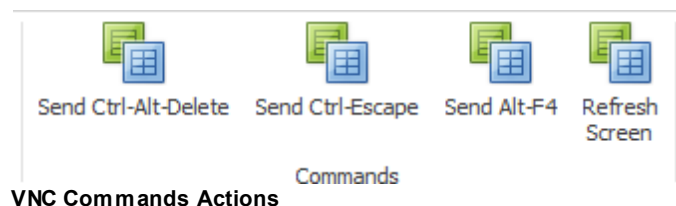
On Windows 8 or Windows 2012 server, switches from an application to another.

3.3.4.3 VNC

Description

The commands for a VNC session allow you send remote commands to your host.

Settings



Send Ctrl-Alt-Delete

Send the key combination CTRL+ALT+DELETE to the host.

Send Ctrl-Escape

Send the key combination CTRL+ESCAPE to the host to open the Start menu.

Send Alt-F4

Send the key combination ALT+F4 to the host to close an application.

Refresh Screen

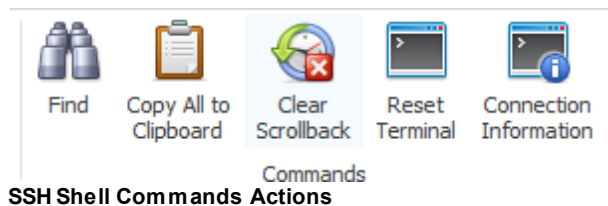
Refresh the host screen.

3.3.4.4 SSH Shell

Description

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

Settings



Find

Open a find window to search for specific words.

Copy All to Clipboard

Copy all selected text to the Clipboard.

Clear Scrollback

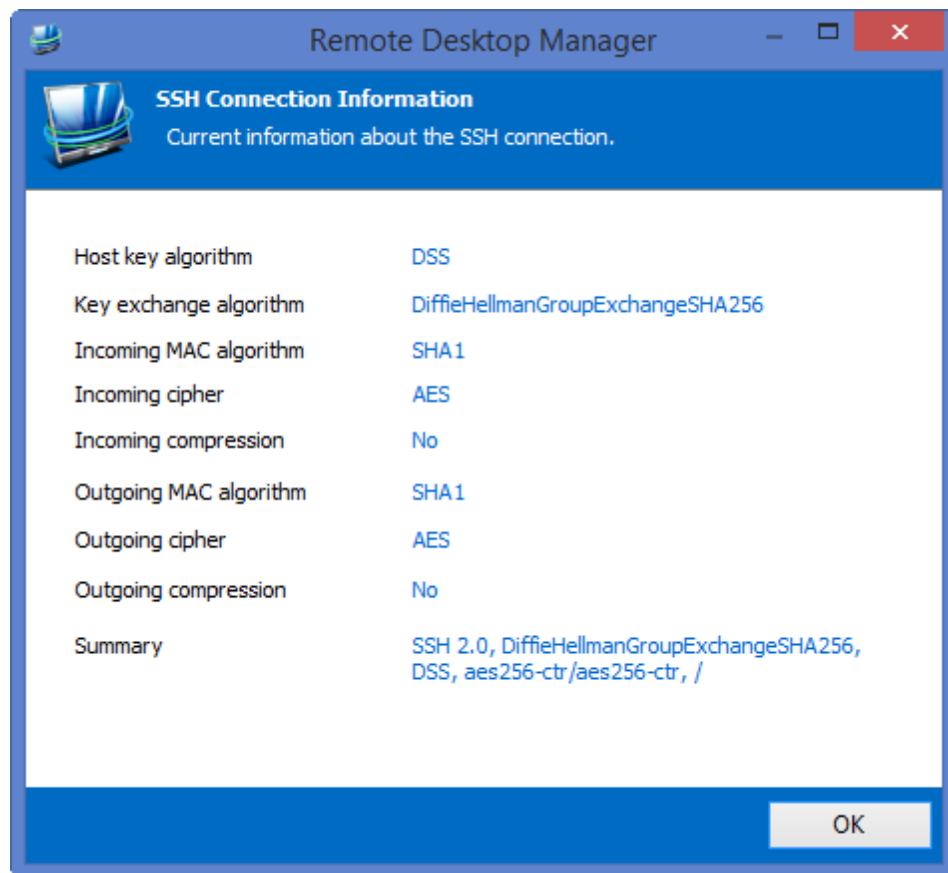
Clear the scrolling display that precedes the current line.

Reset Terminal

Reset host terminal connection.

Connection Information

Provides connection host information in a form as below.



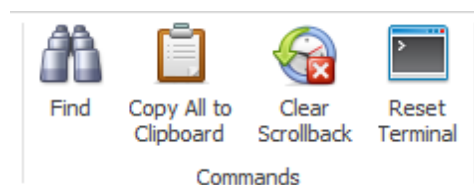
Connection Information

3.3.4.5 Telnet

Description

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

Settings



Telnet Commands Actions

Find

Open a find window to search for specific words.

Copy All to Clipboard

Copy all selected text to the Clipboard.

Clear Scrollback

Clear the scrolling display that precedes the current line.

Reset Terminal

Reset host terminal connection.

3.3.5 Layout

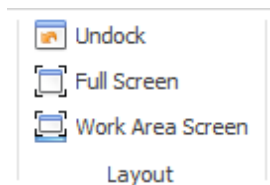
Description

The Layout actions allow you to view your session in various modes: *Undocked*, *Embedded*, view in *full screen* or in *work area screen*.



The Layout actions are only available in embedded mode. Actions may be different depending on your session type.

Settings



Layout Actions

Undock

Allow you undock your embedded session and move it anywhere outside Remote Desktop Manager or even on another monitor.

Embedded

Allow you to re-embed your session when your session is undocked.

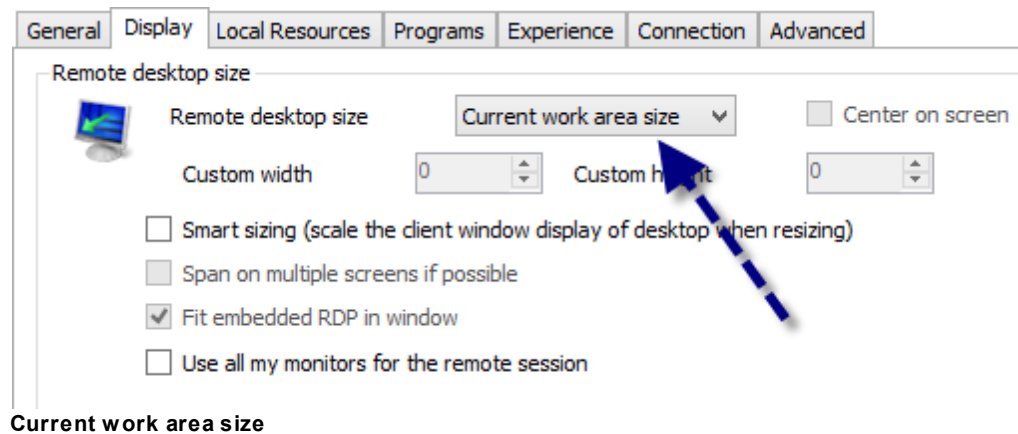
Full Screen

Display your session in full screen outside Remote Desktop Manager. Use this action if you want to open your session in external mode using the RDP client.

Work Area Screen

This mode allows you to open the connection in full screen but to have also access to your local taskbar.

You need to select *Current work area size* in your RDP entry first.



3.3.6 Settings

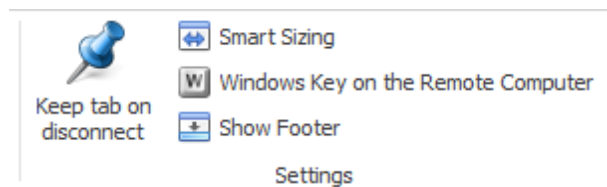
Description

The Settings actions allow you to apply settings such as smart sizing, Windows key on the remote computer and show footer.



The Settings actions are only available in embedded mode. Actions may be different depending on your session type.

Settings



Settings Actions

Keep tab on disconnect

Your session tab will stay after a session disconnect. For more information, see [Keep Tab Opened](#) topic.

Smart Sizing

Enable or disable the RDP smart sizing.

Windows Key on the Remote Computer

When pressing the Windows key, it will send the function to your host instead of running it on your computer.

Show Footer

Remote Desktop Manager footer will be displayed inside your remote session.

3.3.7 Edit

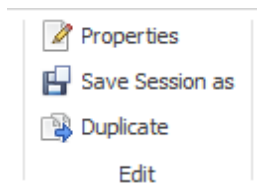
Description

The Edit actions allow you to create/edit/duplicate your active session.



The Edit actions are only available in embedded mode.

Settings



Edit Actions

Properties

Opens the properties window of your session entry.

Save Session as

Prompts you to save your session on the same or different name.

Duplicate

Duplicates your active session in a new embedded screen.

3.3.8 Screenshot

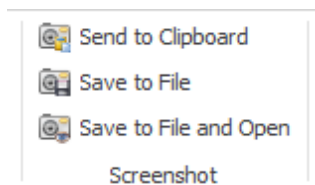
Description

The Screenshot actions allow you to capture a screenshot of a running session.



The Screenshot actions are only available in embedded mode.

Settings



Screenshot Actions

Send to Clipboard

Performs a typical capture to the clipboard.

Save to File

Prompts for a file name, and saves the capture to that file.

Save to File and Open

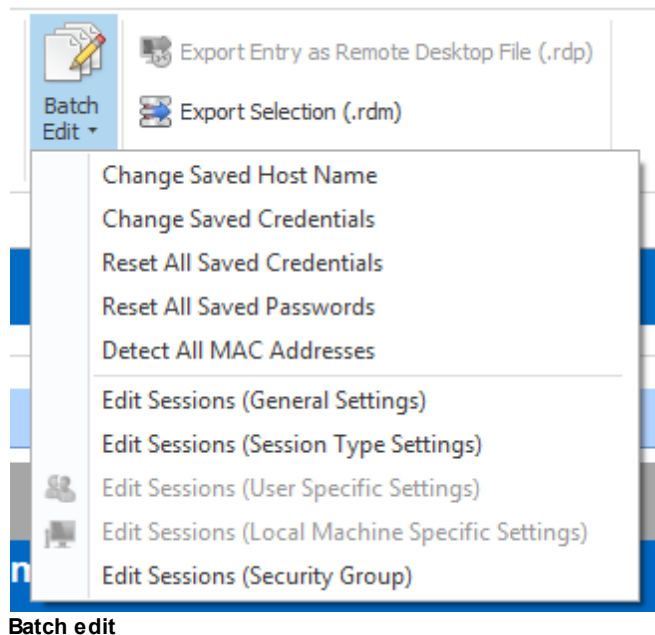
Prompts for a file name, saves the capture to that file and opens the file using your default editor.

3.4 Edit

3.4.1 Batch Edit

Description

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



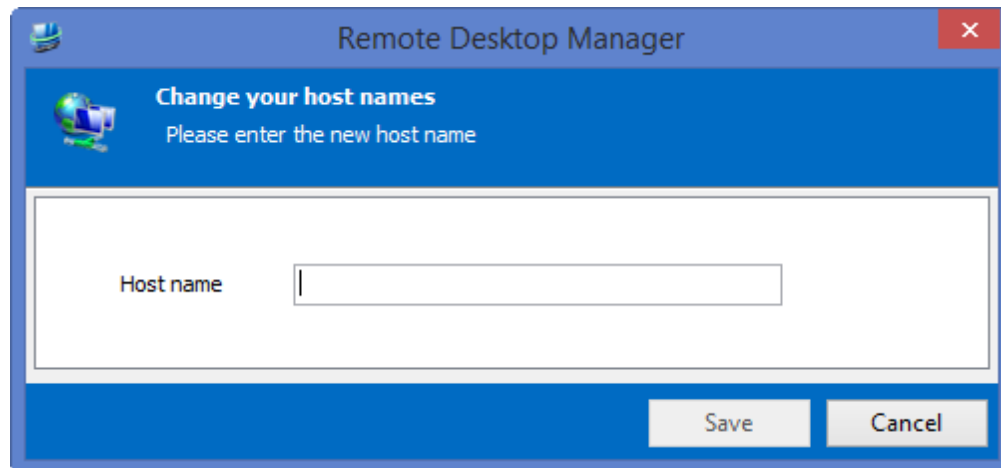
You can also change:

- Host Name
- Credentials
- General Settings
- Session Type Settings
- User Specific Settings
- Local Machine Specific Settings

- Security Group

Settings

Change Saved Host Name

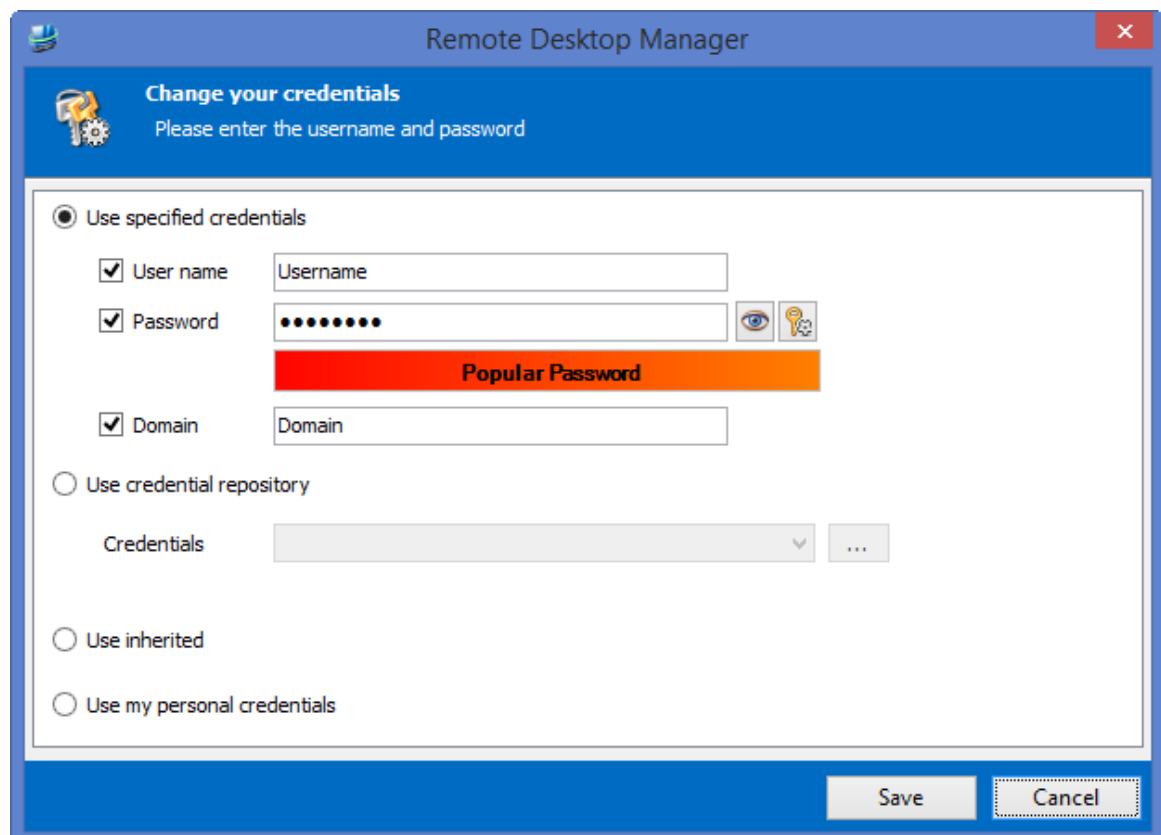


The screenshot shows a dialog box titled "Remote Desktop Manager" with a close button (X) in the top right corner. The main heading is "Change your host names" with a subtext "Please enter the new host name". Below this is a text input field labeled "Host name". At the bottom right are "Save" and "Cancel" buttons.

Change Saved Host name

You can change multiple host names at the same time.

Change Saved Credentials



The screenshot shows a dialog box titled "Remote Desktop Manager" with a close button (X) in the top right corner. The main heading is "Change your credentials" with a subtext "Please enter the username and password". Below this are three radio button options: "Use specified credentials" (selected), "Use credential repository", and "Use inherited". Under "Use specified credentials", there are three checked checkboxes: "User name" (with a text field containing "Username"), "Password" (with a masked password field and a "Popular Password" button), and "Domain" (with a text field containing "Domain"). Under "Use credential repository", there is a "Credentials" dropdown menu and a button with three dots. At the bottom right are "Save" and "Cancel" buttons.

Change Saved Credentials

You can change the configured credentials for multiple sessions in a batch. You can use the following options to change the credentials:

Option	Description
Use Specified credentials	Use a specific username, password and domain.
Use credential repository	Use a Credential entry linked entry which can be external credentials like KeePass for example. This is very useful for sharing or reusing existing credentials among entries.
Use Inherited	Use the credentials of it's parent entry or group.
Use my personal credentials	This allows you to use one set of credentials to replace or emulate the ones from your Windows session. See My Personal Credentials topic.

Reset All Saved Credentials

This will clear existing credentials for the selected sessions.

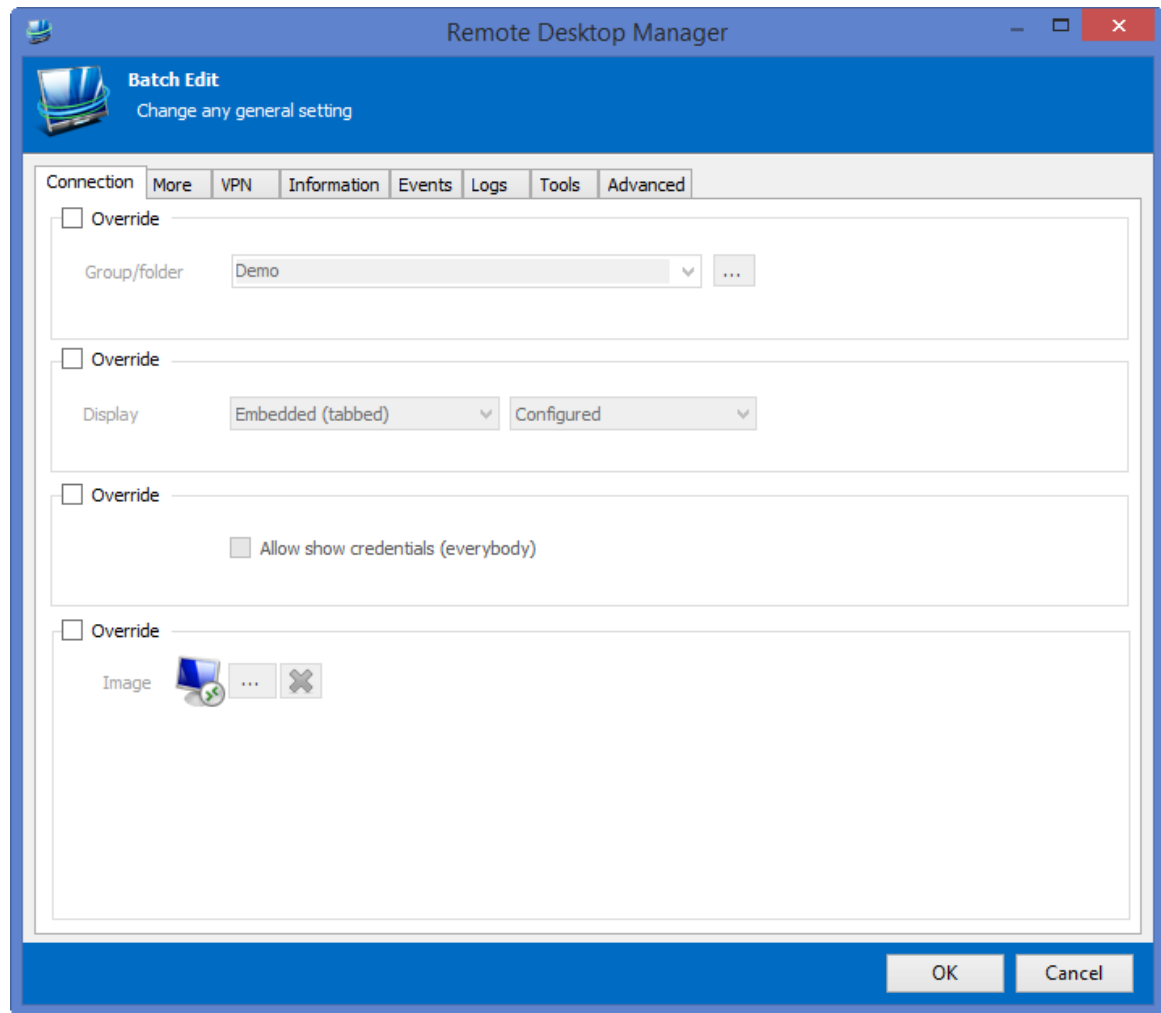
Reset All Saved Passwords

This will clear existing passwords for the selected sessions.

Detect All MAC addresses

This will detect all MAC addresses for the selected sessions.

Edit Sessions (General Settings)



General Settings

You can change common session settings. The session can be of any type, because a common set of options are shared among sessions. The following general settings can be changed:

- [Group/Folder](#)
- [Display](#)
- [Allow show credentials \(everybody\)](#)
- Image
- [Description](#)
- [Keywords/Tags](#)
- [Tab Page Category/Color](#)
- [VPN](#)
- Information ([General](#), [Hardware](#), [Purchase](#), [Notes](#), [Custom Fields](#))
- [Contact Information](#) (Base, Address, Communication)
- [Events](#)
- [Logs](#)
- [Tools](#)
- [Intel AMT](#)
- [Advanced Settings tab](#)

Edit Sessions (Session Type Settings)



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

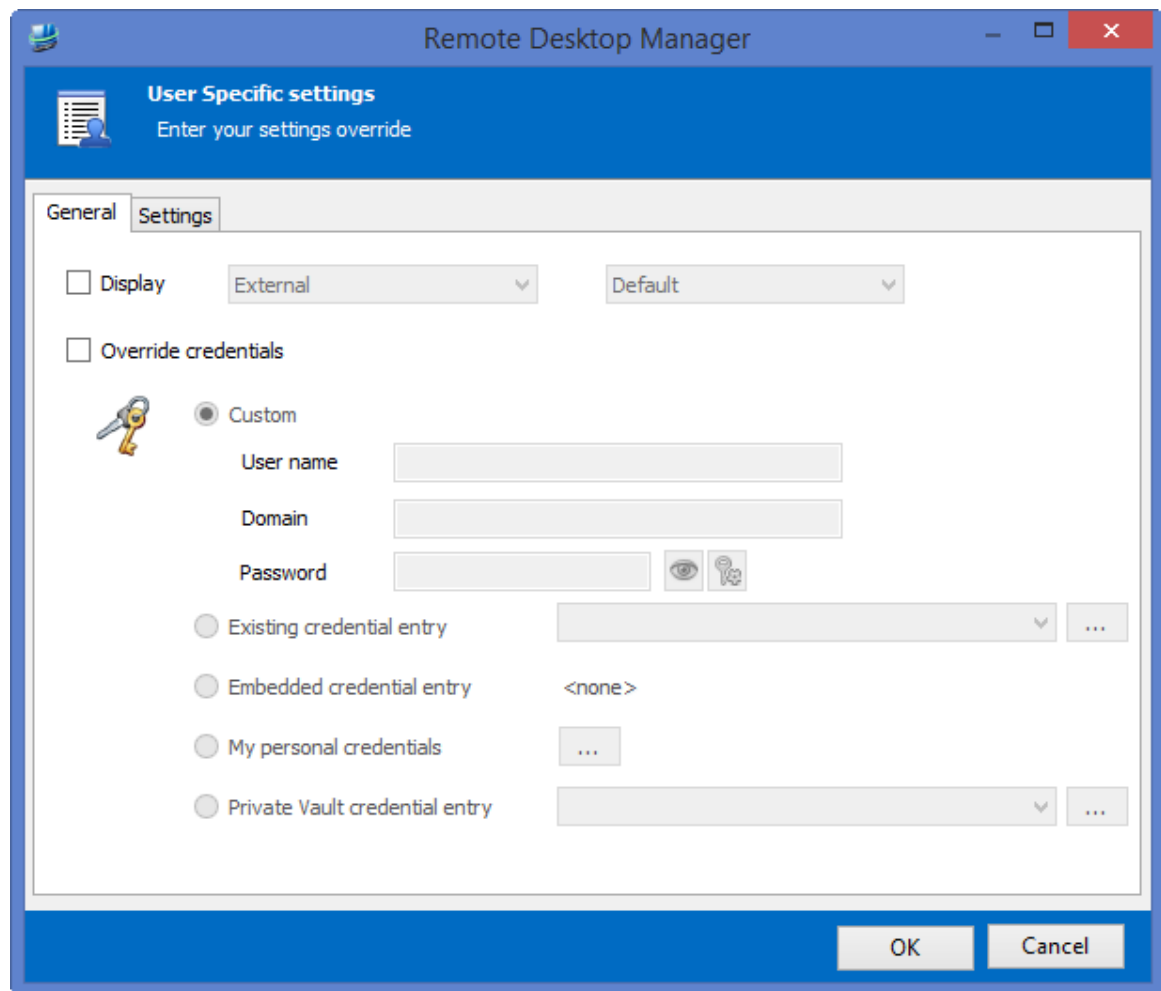
The screenshot shows the 'Remote Desktop Manager' window with the 'Batch Edit' dialog box open. The dialog has a blue header with the title 'Batch Edit' and the subtitle 'Change any connection specific setting'. Below the header are several tabs: 'General', 'Display', 'Local resources', 'Programs', 'Experience', 'Connection', and 'Advanced'. The 'General' tab is selected. Inside the 'General' tab, there is a section titled 'Logon settings'. It contains the following fields and options:

- A checkbox labeled 'Edit logon settings in batch'.
- A text box labeled 'Enter the name of the remote computer.' with a 'Computer' label and a 'Port' label.
- A dropdown menu labeled 'RDP type' with 'Normal' selected.
- A text box labeled 'User name'.
- A text box labeled 'Domain'.
- A checkbox labeled 'Open in console (Admin mode for Vista SP1 or better)'.
- A checkbox labeled 'Always ask for credentials'.
- A radio button labeled 'Store password on the local computer'.
- A radio button labeled 'Store password in the database'.
- A 'Save Password' button.
- A 'Clear password' button.
- A 'Password' text box with an eye icon and a key icon.

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

Session Type Settings

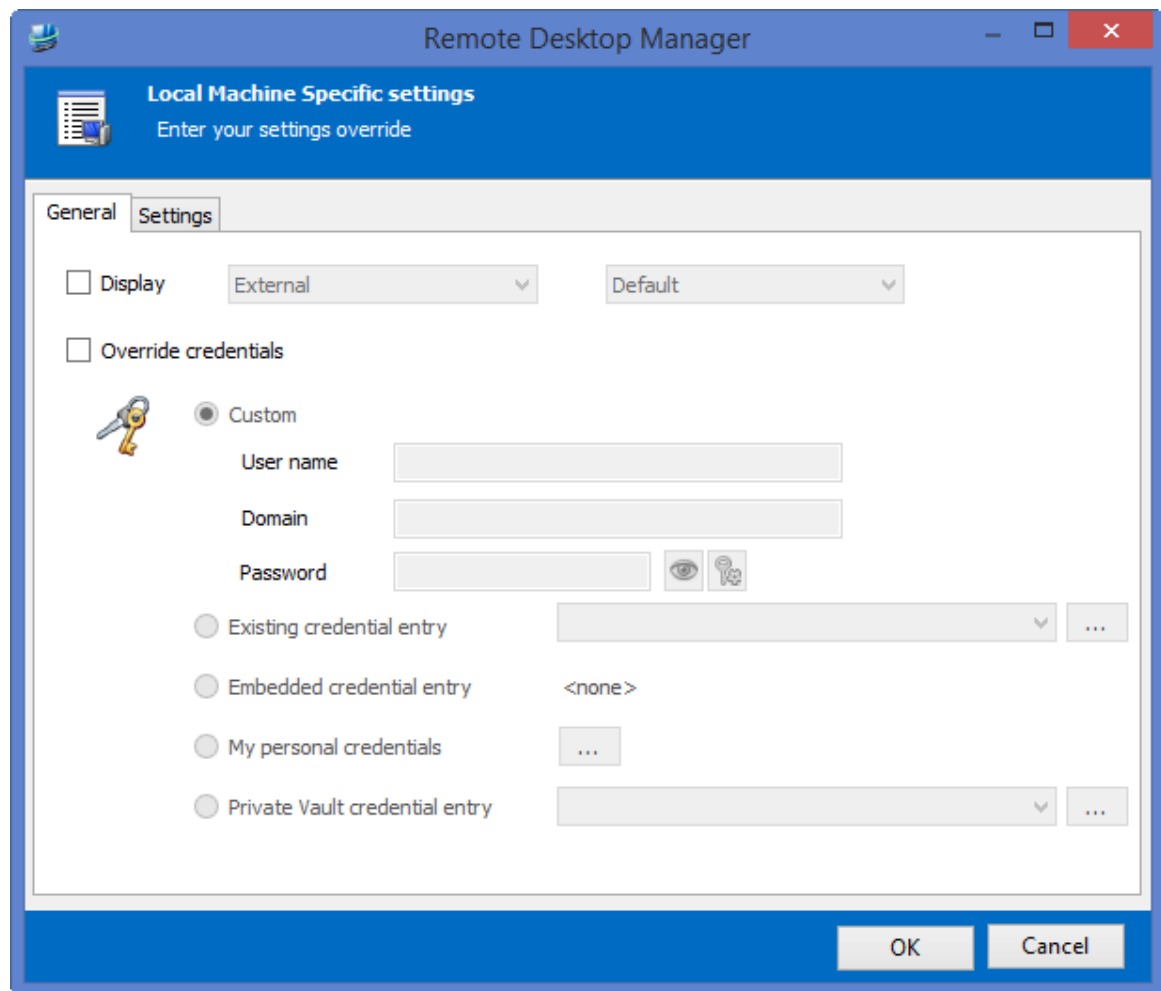
Edit Sessions (User Specific Settings)



User Specific Settings

[User Specific Settings](#) can be modified in a batch if they're supported by the session type.

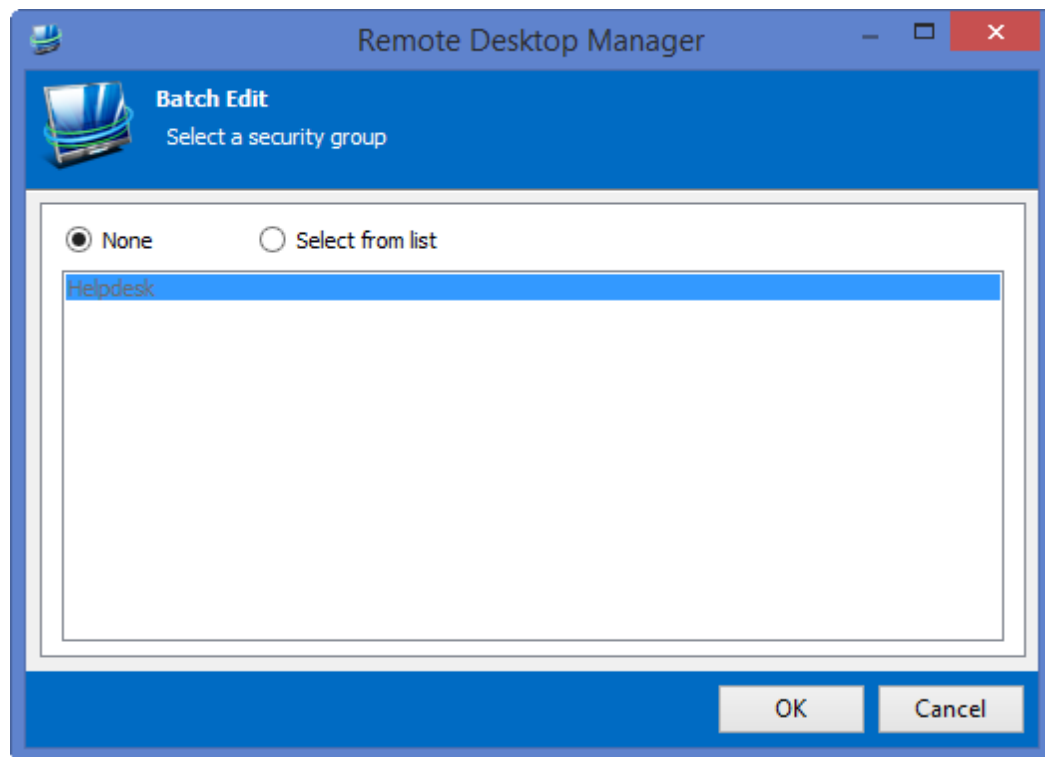
Edit Sessions (Local Machine Specific Settings)



Local Machine Specific Settings

[Local Machine Specific Settings](#) can be modified in a batch if they're supported by the session type.

Edit Sessions (Security Group)



Security Group

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

3.4.2 Shortcut/Linked Entries

Description

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

- assign different access to the folder
- create a favorite folder with everything centralized
- reuse a document for different scenario.

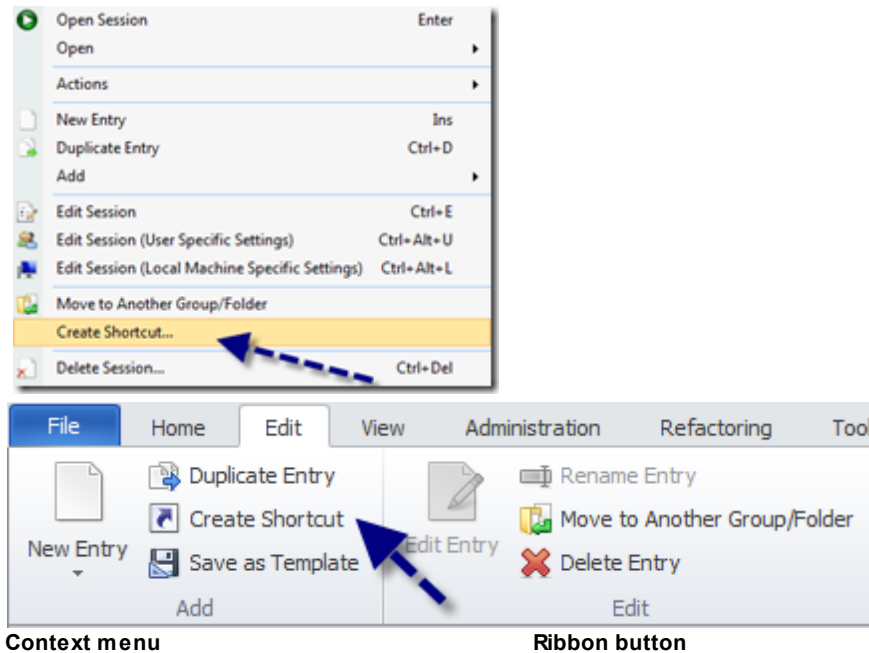


Two shortcuts selected

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

Creating a Shortcut: Option 1

One way to create a shortcut is by using the menu **Edit->Create Shortcut...** or with the ribbon button



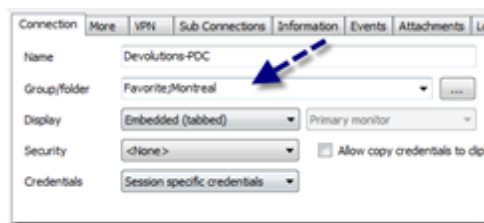
Simply choose the destination folder for the shortcut. The application will automatically refresh and display the new shortcut in the list.



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 “;”. You can also use the browse button (...) and select more than one group by holding the Ctrl key while clicking on the tree node.



3.4.3 User Specific Settings

Description

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

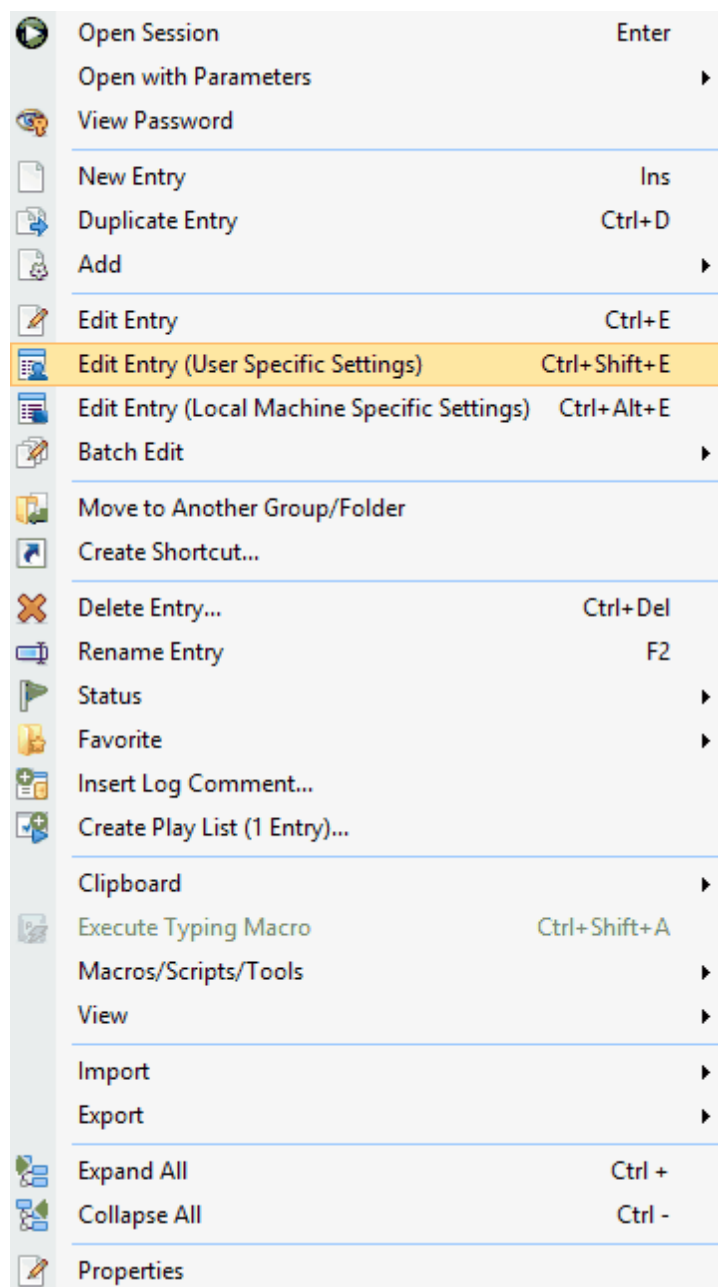
User Specific Settings



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



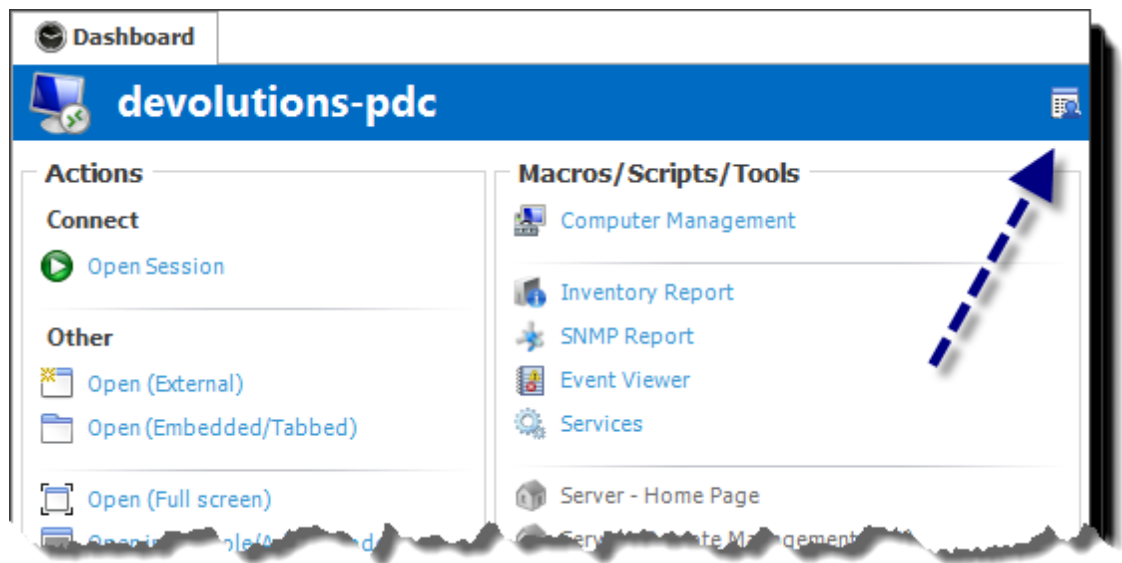
If both User Specific settings and [Local Machine Specific Settings](#) are defined on the same entry, [Local Machine Specific Settings](#) have dominance.



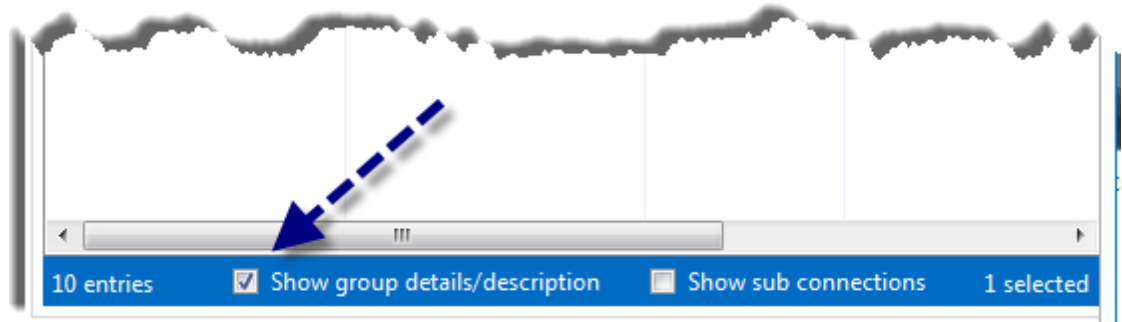
User Specific Settings menu

User Specific settings indicator

For entries with defined **User Specific Settings**, an indicator appears in the dashboard when you select the entry. You can simply click on the indicator to go to the Edit Entry (User specific settings) dialog.



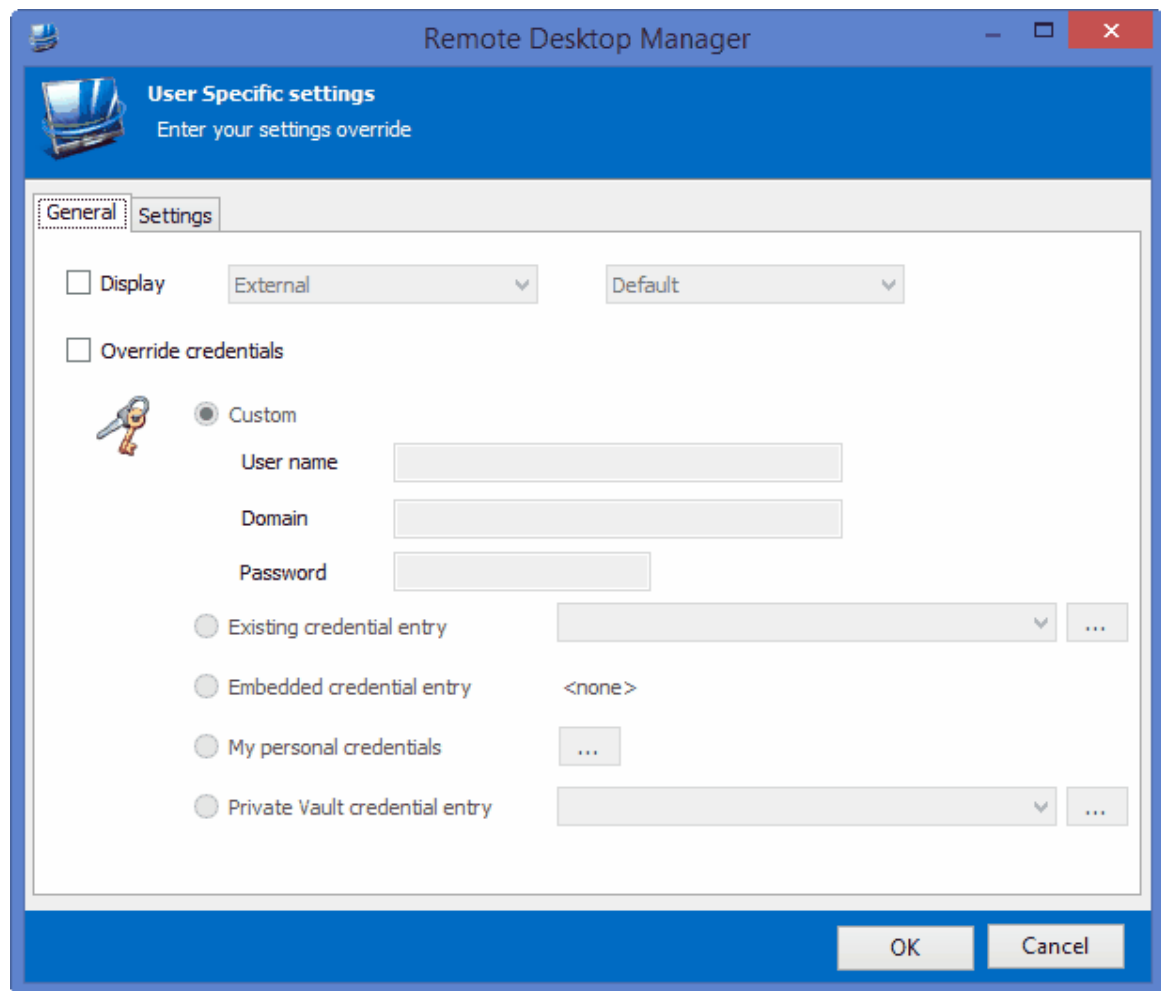
For Groups/Folders, you must have enabled the **Show group details/description** option to see the indicator.



Workflow

Sessions and Groups/Folders

In the majority of cases, this dialog will appear.



User Specific Settings

Please consult each specific override topics for more information:

- [Credential Entry Overriding](#)
- [Credentials](#)
- [Display](#)
- [Screen Size](#)
- [Default Browser](#)
- [Keyboard](#)
- [Gateway](#)

Credentials Entries

In the case of credential entries, please refer to [Credential Entry Overriding](#).

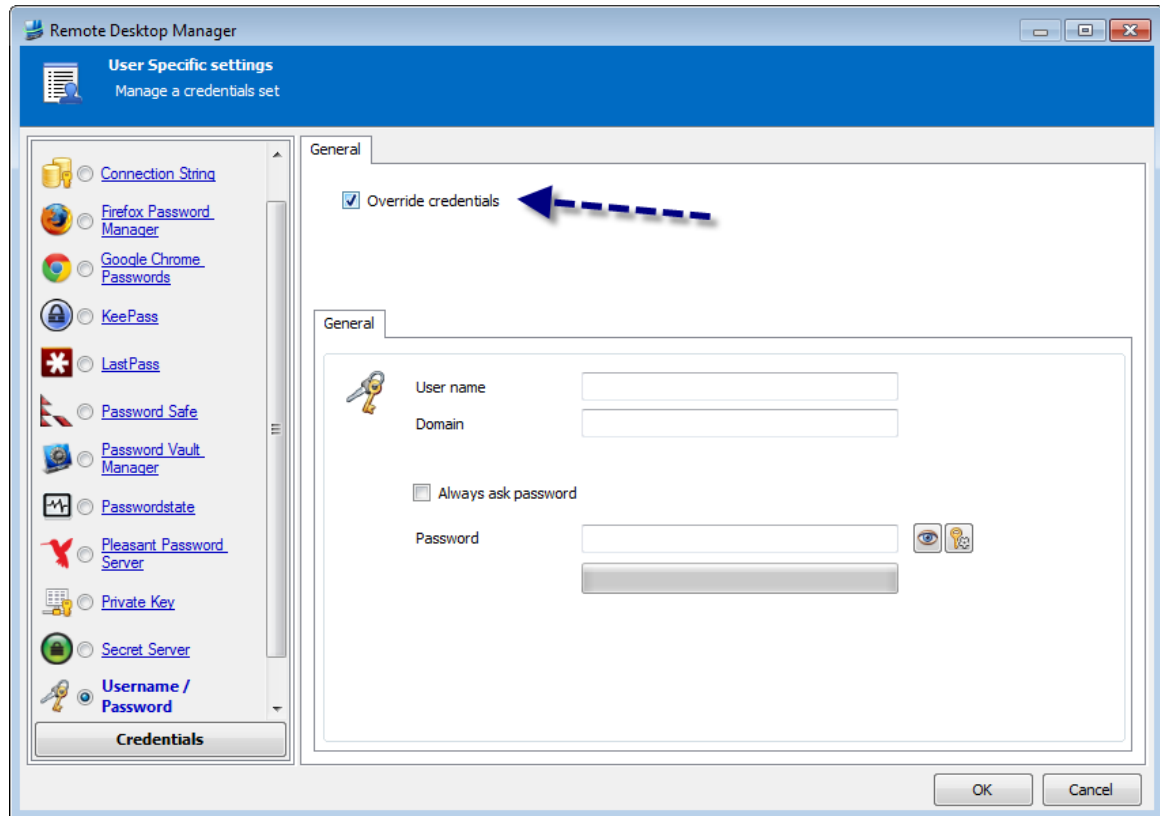
My Personal credentials

For more information please consult [My Personal Credentials](#)

3.4.3.1 Credential Entry Overriding

Description

The credential entry is a special case. When overriding using either [User Specific Settings](#) or [Local Machine Specific Settings](#), a specialized dialog appears to allow you to override the original credentials.



Override Credential Entry dialog

Settings

To override the credentials, you must first check the **Override credentials** option. Then you enter the new credentials in the area below.

To stop overriding credentials, uncheck the **Override credentials** option.

3.4.3.2 Credentials

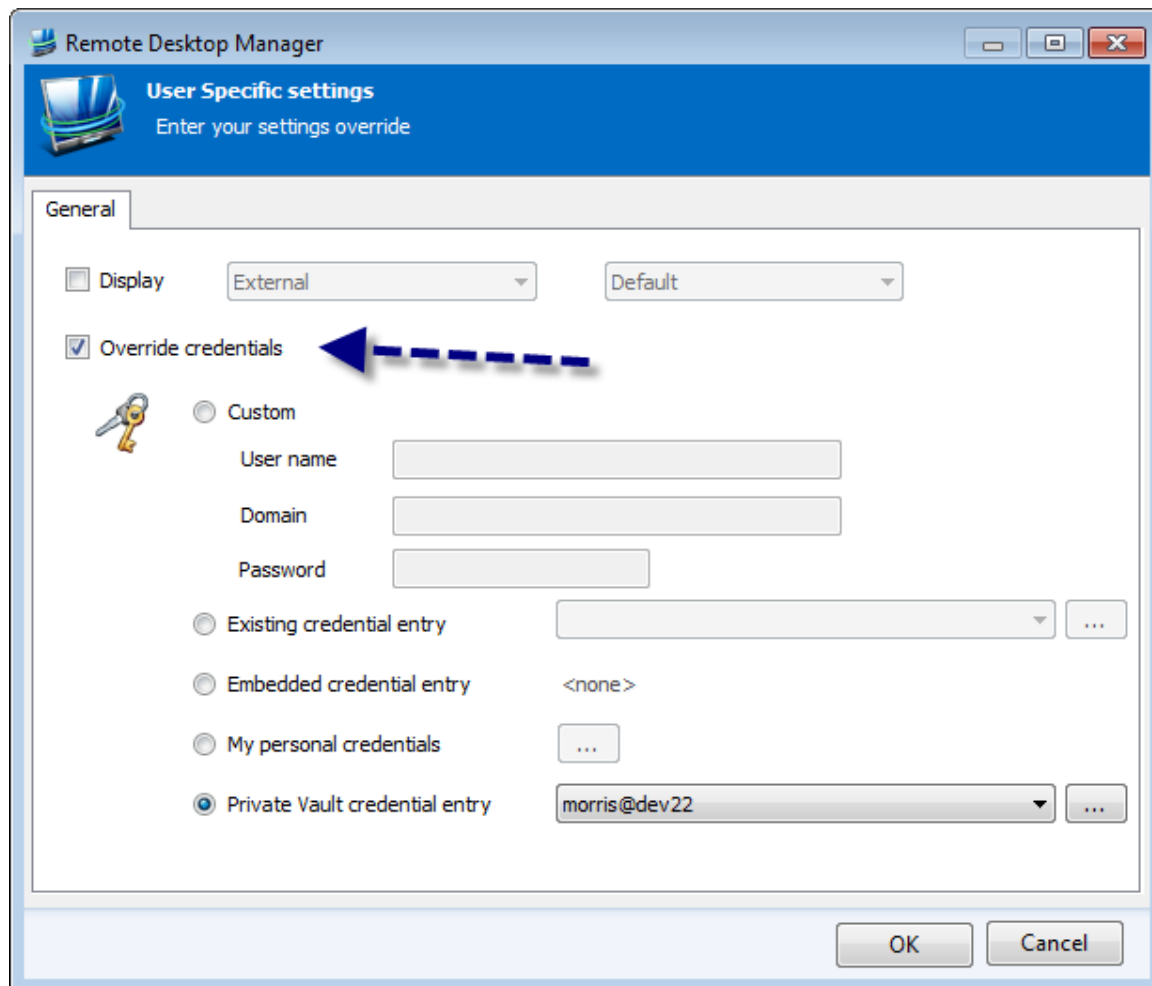
Description

Override Credentials will allow you to specify other credentials than the ones that are stored in an entry. You can choose from multiple sources according to your security practices and policies.



The Credentials override is available on all entry types.

Settings



Override Credentials

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

Option	Description
Custom Credentials	Use a specific User name, Domain and Password.
Existing credential entry	Use an existing credential entry.
Embedded credential entry	Use Embedded credentials.
My personal credentials	Use the credentials stored in My Personal Credentials (Note 1)
Private Vault credential entry	Use an entry from your Private Vault. (Note 2)

Notes

1. For more information please consult [My Personal Credentials](#)

2. The Private Vault credential entry is only available under the following conditions:

- 2.1. The Private Vault is available for your data source, please consult [Private Vault](#);
- 2.2. You are overriding at the folder level;
- 2.3. You are overriding a session that is itself in the Private Vault.

3.4.3.3 Display

Description

This allows you to select a different display mode for the session.



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

Settings

Remote Desktop Manager

User Specific settings
Enter your settings override

General Settings

☒ Display External Monitor #1

☐ Override credentials

Custom

User name

Domain

Password

☐ Existing credential entry

☐ Embedded credential entry <none>

☒ My personal credentials

☐ Private Vault credential entry

OK Cancel

Override Display

Please consult [Display Mode](#) for information on available settings and their usage.

3.4.3.4 Screen Size

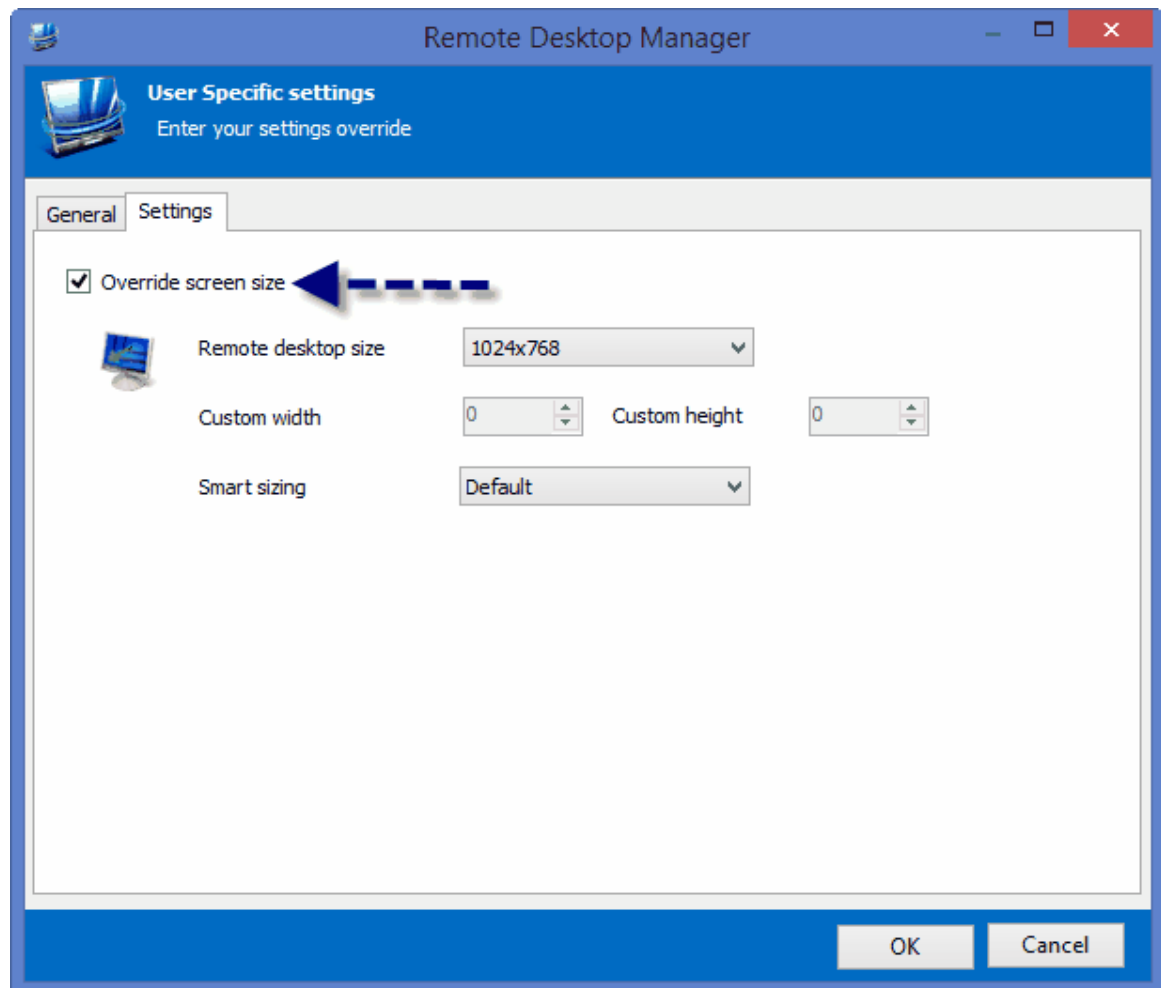
Description

Override Screen Size will allow you to customize the size of the local window that is hosting the remote session.



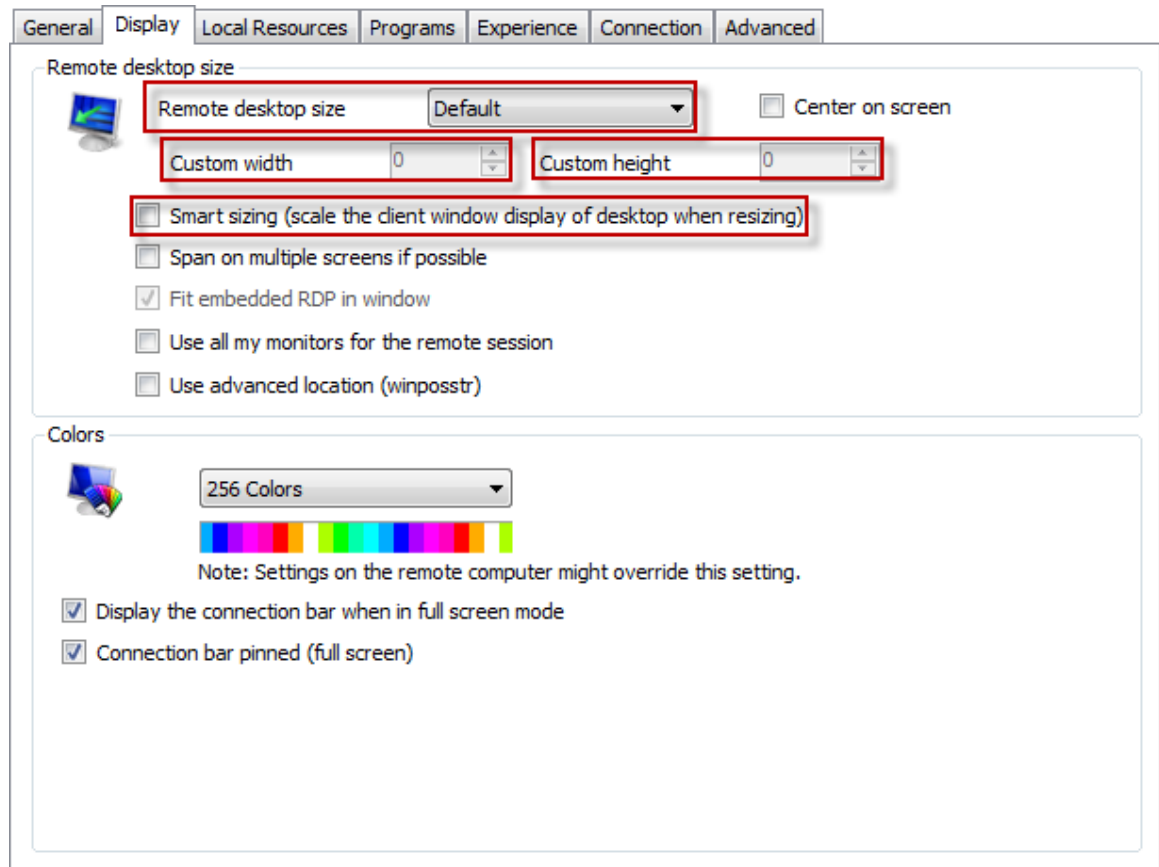
Screen Size is only visible for **RDP sessions**.

Settings



Override Screen Size

The settings being overridden by this are in the Display tab of the RDP sessions



Display tab

3.4.3.5 Default Browser

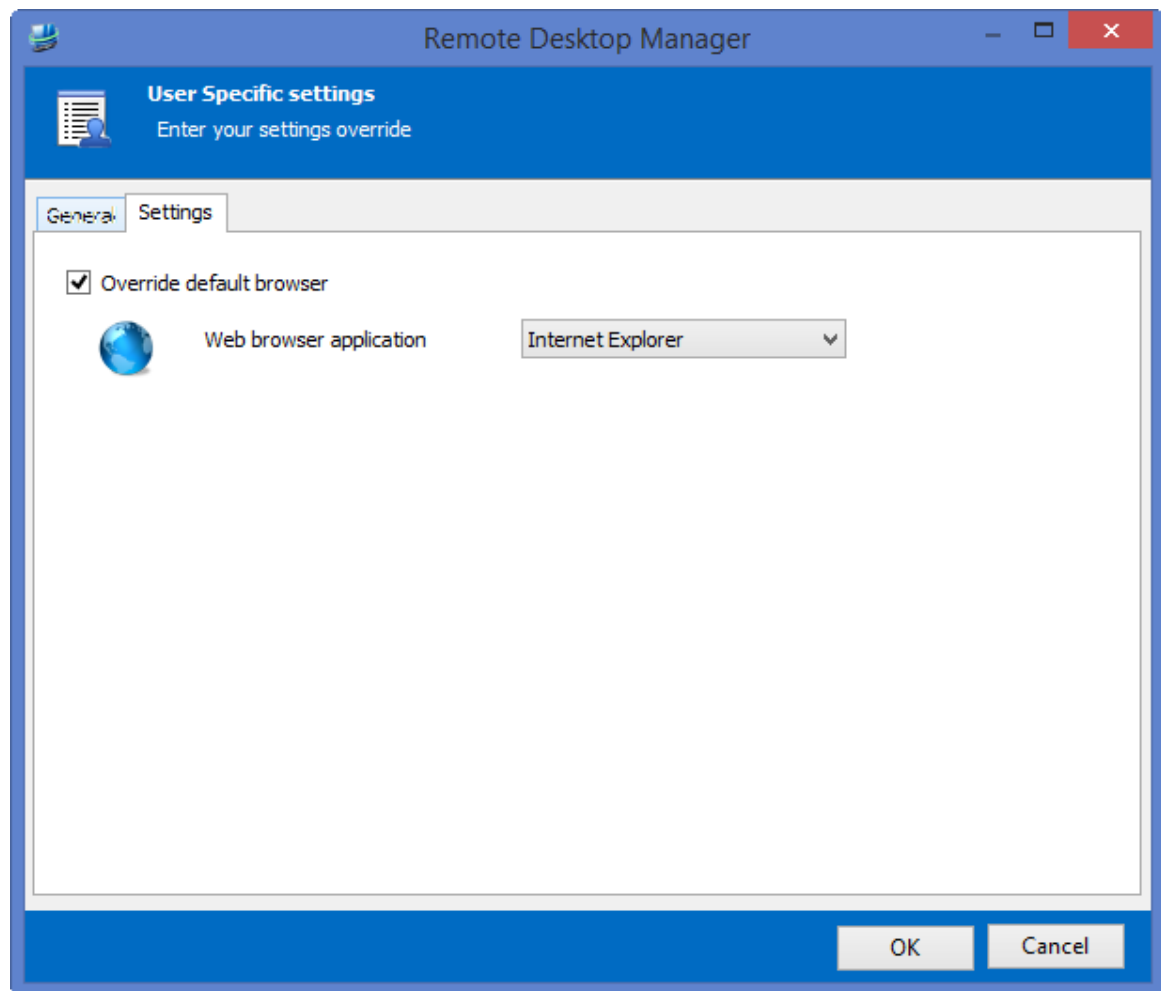
Description

Override default browser will allow you to customize the internet default browser for a web browser session.



Override default browser is only visible for **Web Browser sessions**.

Settings



Override default browser

Option	Description
Web browser application	Override the default web browser in the application. Select between: <ul style="list-style-type: none">• Internet Explorer• Firefox

3.4.3.6 Keyboard

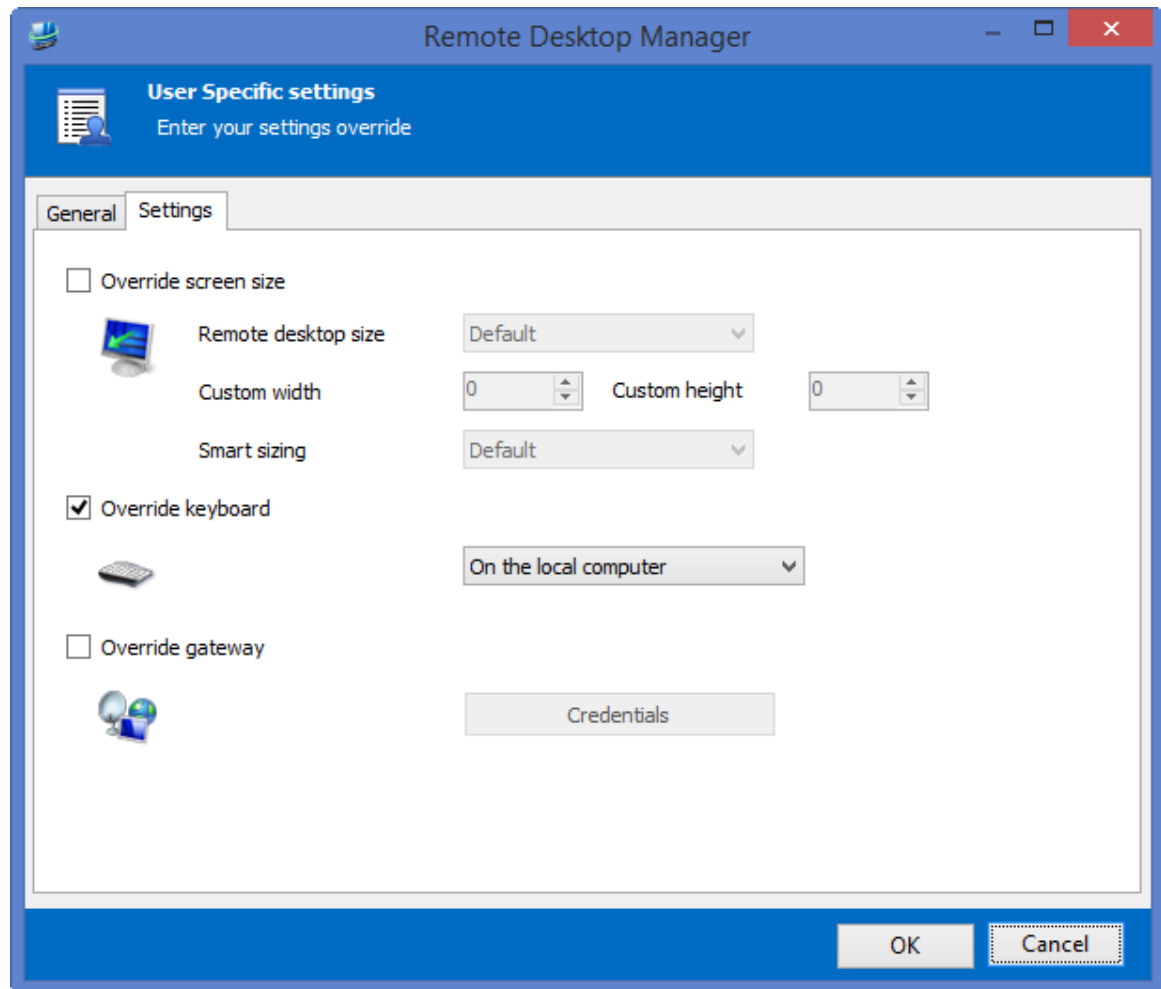
Description

Override keyboard will allow you to customize the keyboard redirection on the remote session.



Override keyboard is only visible for **RDP sessions**.

Settings



Override keyboard

Option	Description
On the local computer	Override the keyboard on the local computer.
On the remote computer	Override the keyboard on the remote computer.
In full screen mode only	Override the keyboard when remote session is in full screen mode only.

3.4.3.7 Gateway

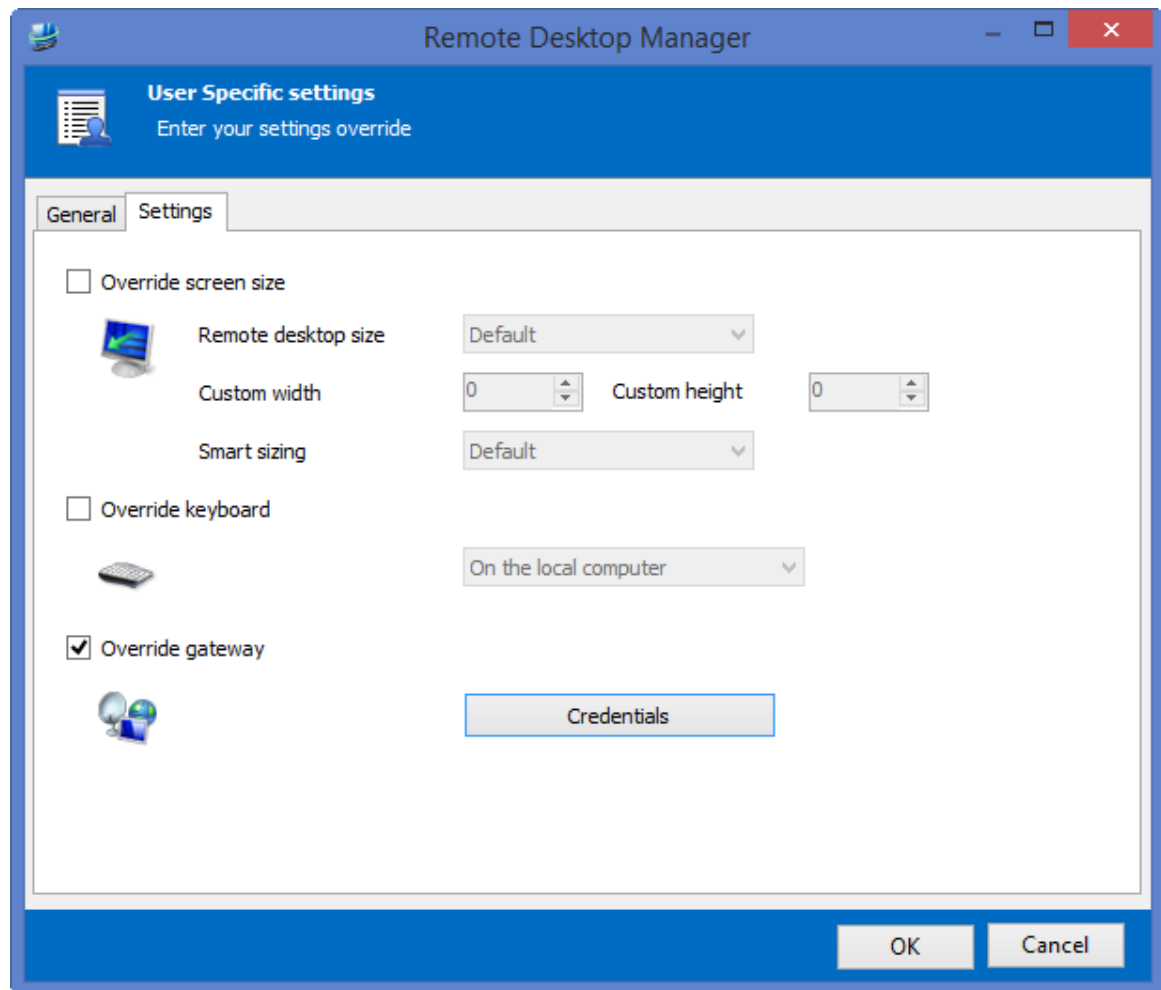
Description

Override gateway will allow you to customize the RDP Gateway credentials to use on the remote session.



Override gateway is only visible for **RDP sessions**.

Settings



Override gateway

RDP Gateway credentials

Option	Description
Use custom credentials	Use a specific User name, Domain and Password.
Use credential repository	Uses a linked Credential Entry. See topic Credentials for more information.
Use my personal credentials	Use the credentials stored in My Personal Credentials .
Private Vault credential entry	Use an entry from your Private Vault .

3.4.4 Local Machine Specific Settings

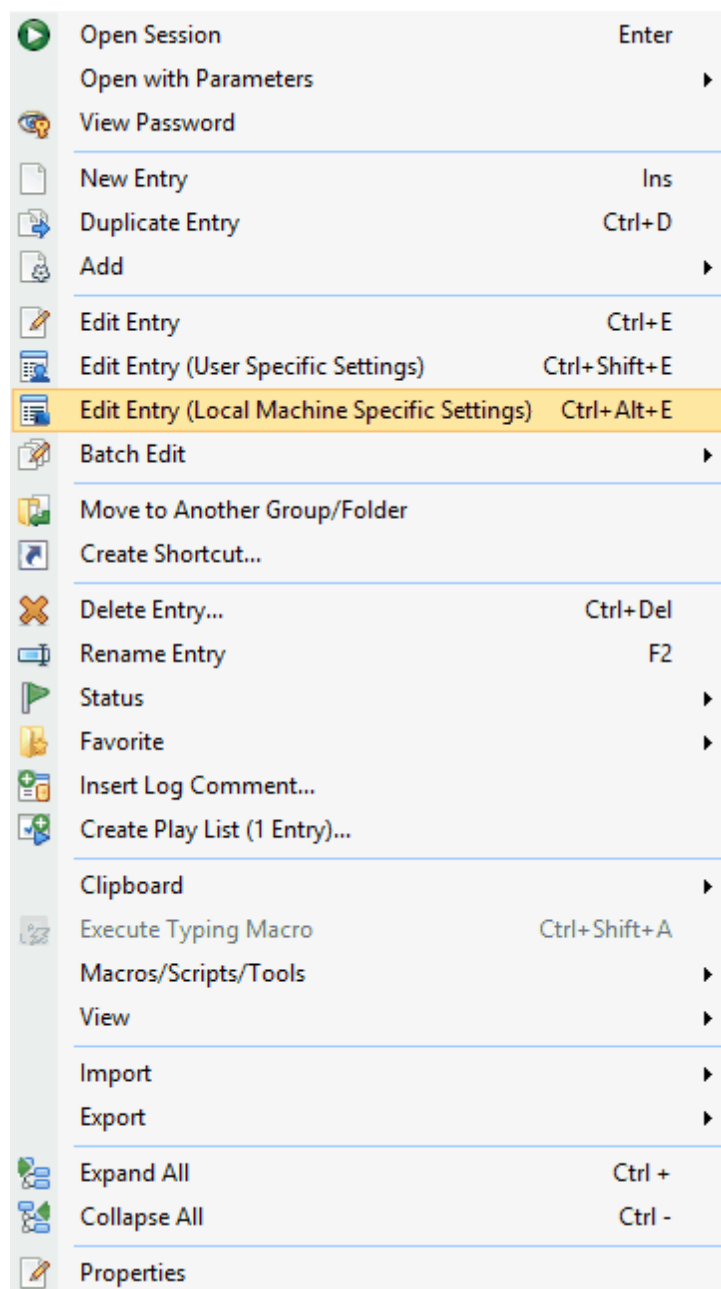
Description

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

Local Machine Specific Settings



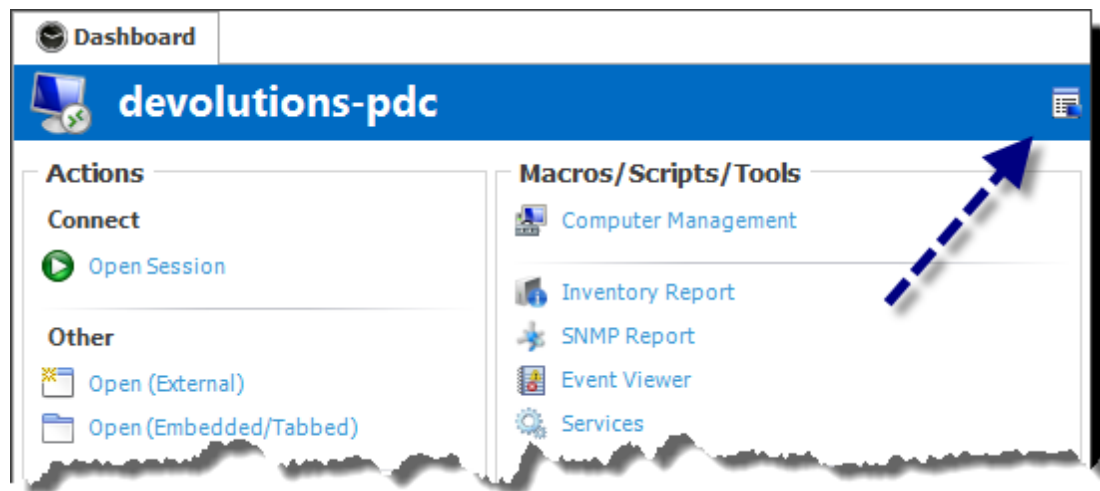
This feature is only available when using an [Advanced Data Source](#). A setting on the data source allows usage of Local Machine Specific Settings, Contact your administrator if the menu is grayed out.



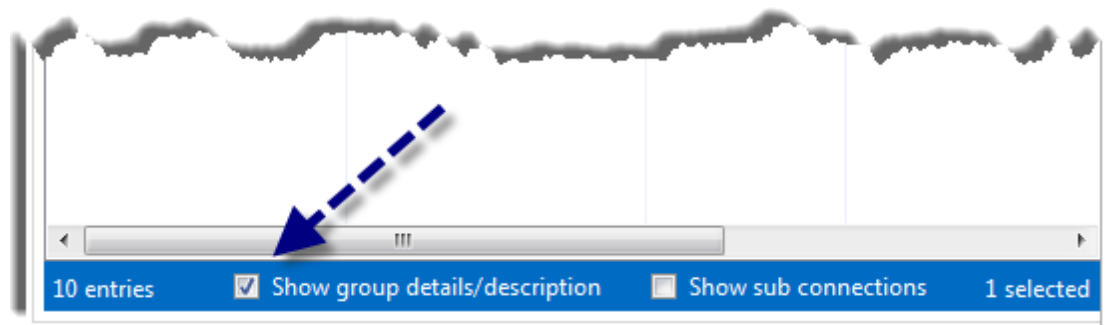
Local Machine Specific Settings menu

Local Machine Specific settings indicator

For entries with defined **Local Machine Specific Settings**, an indicator appears in the dashboard when you select the entry. You can simply click on the indicator to go to the Edit Entry (Local Machine specific settings) dialog.



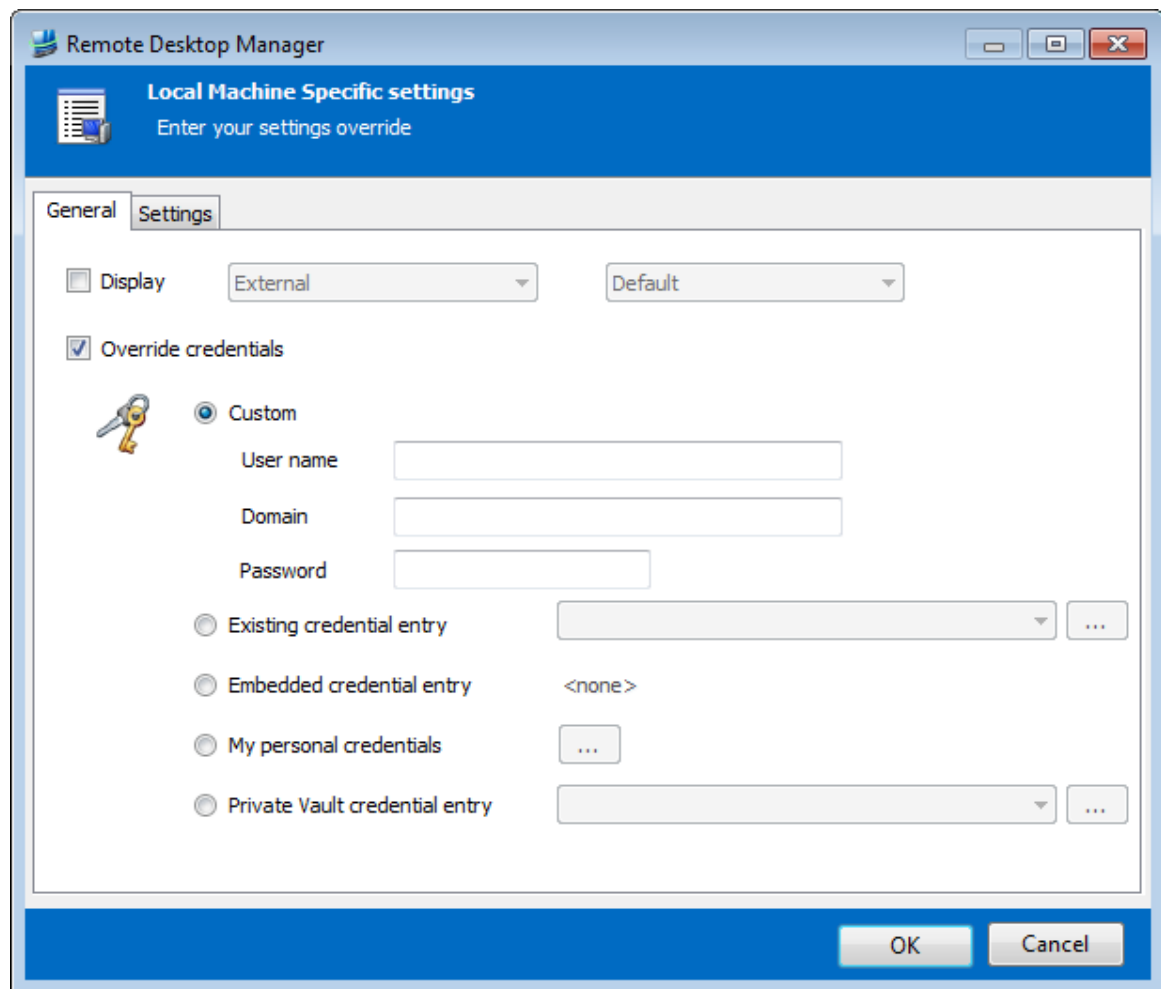
For Groups/Folders, you must have enabled the **Show group details/description** option to see the indicator.



Workflow

Sessions and Groups/Folders

In the majority of cases, this dialog will appear.



Local Machine Specific Settings

Please consult each specific override topic for more information.

[Credentials](#)

[Display](#)

[Screen Size](#)

Credentials Entries

In the case of credential entries, please refer to [Credential Entry Overriding](#).

3.4.5 Settings

3.4.5.1 General

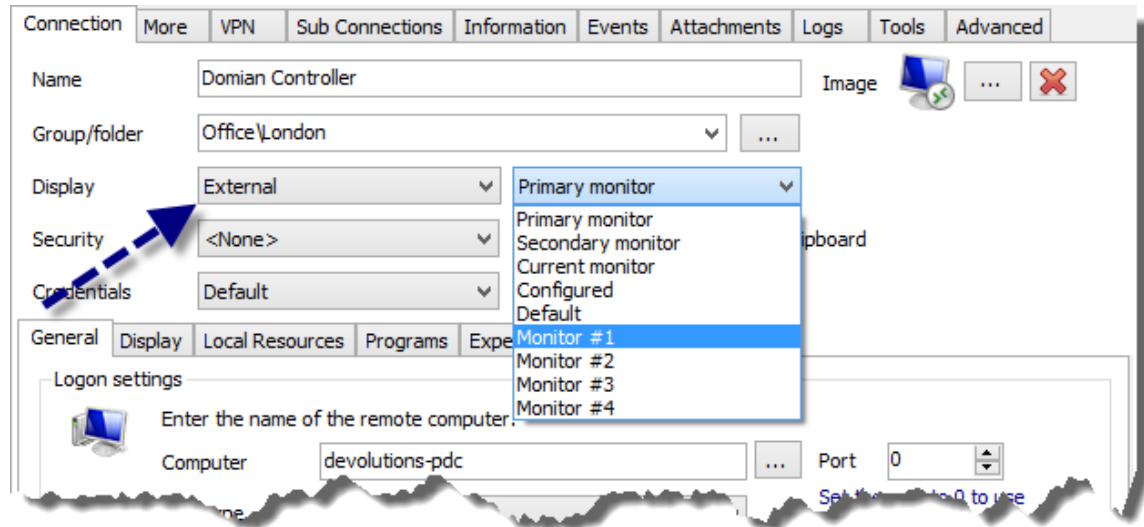
3.4.5.1.1 Display Mode

Description

Remote Desktop Manager provides two types of session:

- External
- Embedded/tabbed

Please note that some sessions will not support both modes. It depends on the integration and the availability of the third party application.



Display mode

External Mode

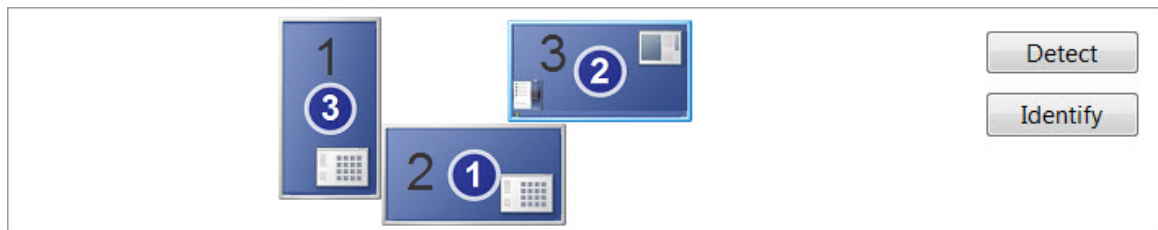
External mode session are opened as an external process, with no direct link to Remote Desktop Manager.

This mode usually launches the native application. For example, the native application for RDP is `mstsc.exe`. Typically, it's also possible to choose the destination monitor. Depending on the type of session, an external mode session view will be updated if Remote Desktop Manager can detect that its running.

External mode supports multiple monitor options

- Primary monitor
This is the monitor that has marked as "main display" in Windows
- Secondary monitor
The other non-primary monitor, obsolete, use Monitor #1,2,3,4 instead
- Current monitor
The monitor that RDM is running in
- Configured
see System Options
- Default
don't move the application, leave it where it starts, let Windows decide.
- Monitor #1
- Monitor #2
- Monitor #3
- Monitor #4

Monitor #1,2,3,4 are numbered from left to right, top to bottom and does not correspond to the numbers you see in Windows. See examples:



Example 1



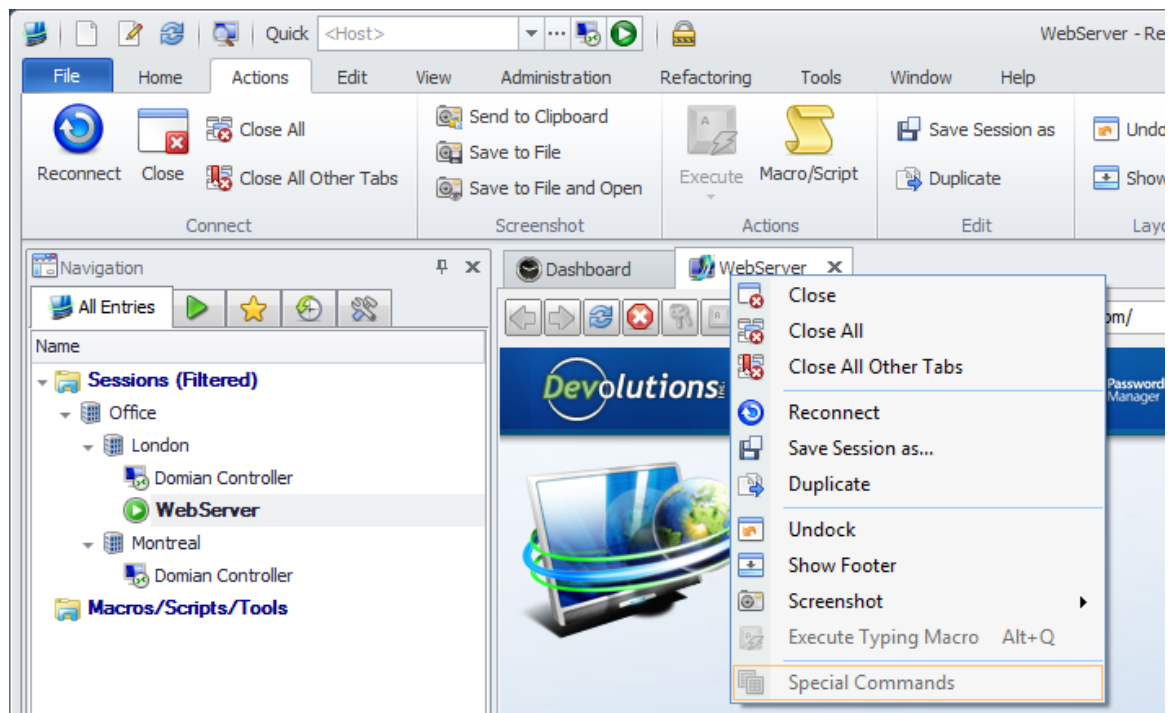
Example 2



Example 3

Embedded/Tabbed Mode

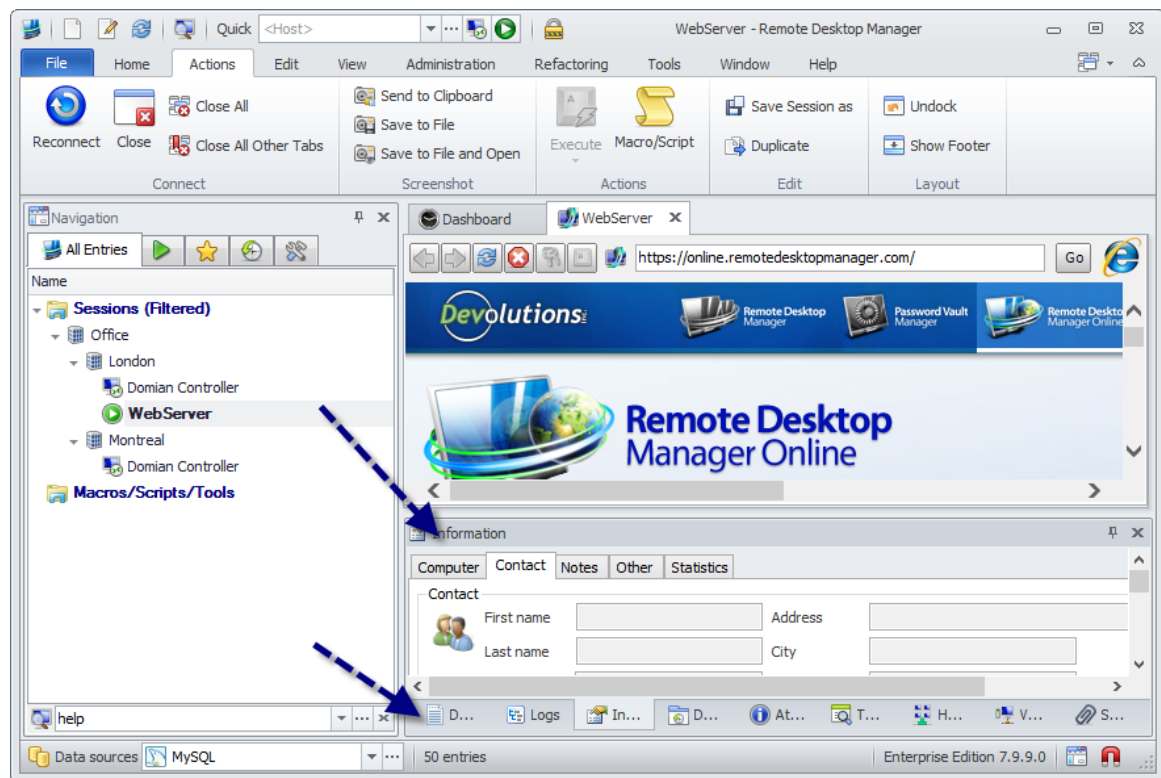
An embedded session runs within the confines of the Remote Desktop Manager window, and displays tabs at the top of the window. This mode centralizes the opened session in the application, which makes it easy to switch from one to another.



Web session opened in embedded mode

There are several session-specific actions available by right clicking (Context Menu) on the title of the tab.

You can also show the session footer (description, information, log, attachment, details, etc.) at the bottom of the screen, and capture a screenshot of the content.

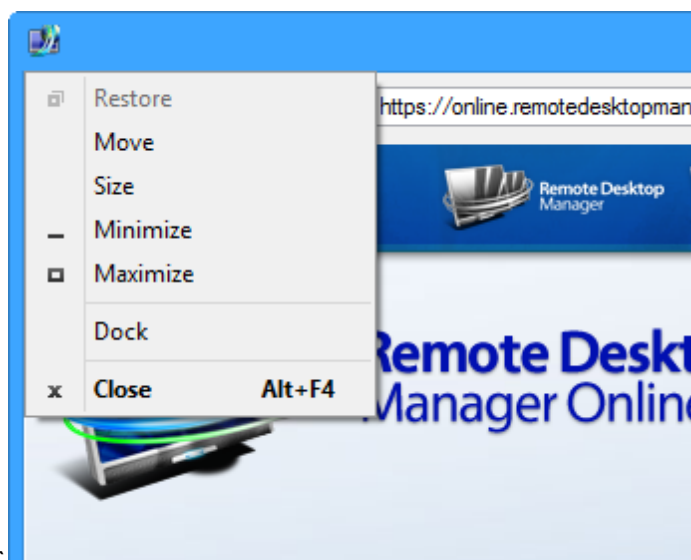


Embedded session with the footer visible

Embedded/Tabbed 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 context menu. Remote Desktop Manager will create a new window to contain the tabbed session, and will allow 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.

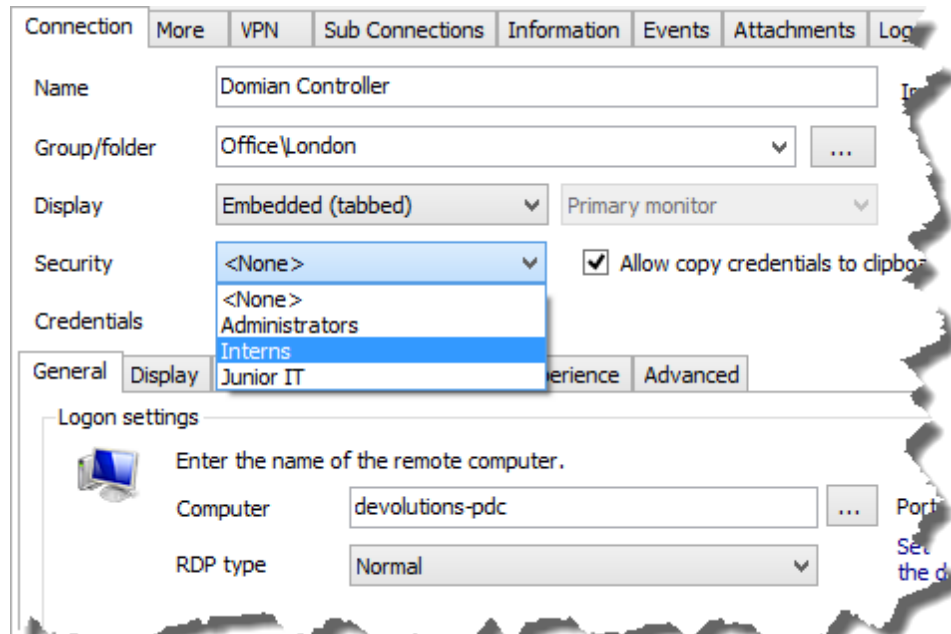


Undocked session window context menu

3.4.5.1.2 Security

Description

Assign a security group to the current entry.

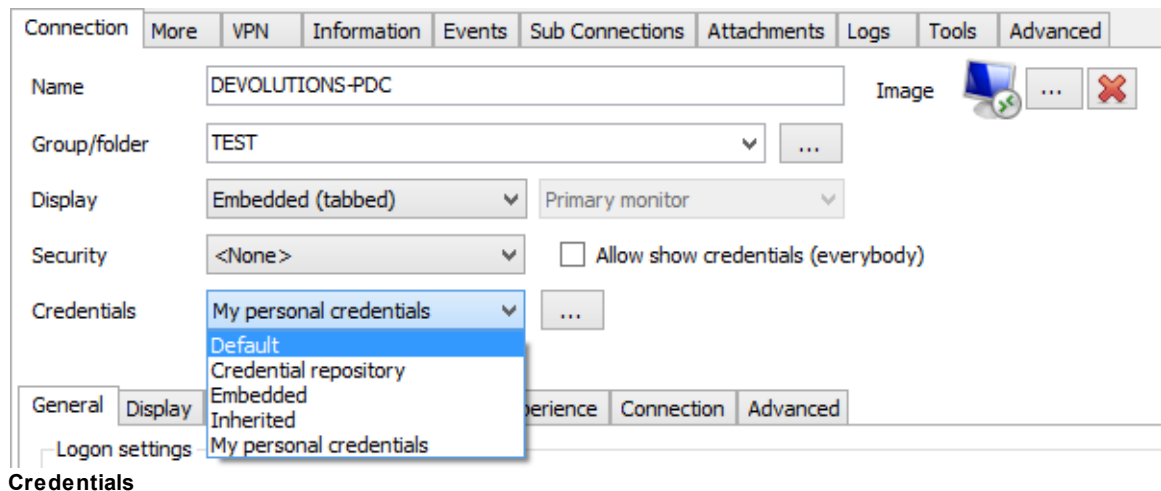


Security group

3.4.5.1.3 Credentials

Description

The **Credentials** drop down defines where/how the entry will fetch its credentials.



The values are:

Setting	Description
Default	Credentials are saved within the entry
Credential repository	Uses a linked Credential Entry in Remote Desktop Manager, which can be external credentials like KeePass for example. Very useful for sharing or reusing credentials among entries.
Embedded	The session has its own credential entry embedded within it, which can be external like KeePass for example. The embedded credential can't be shared among other entries.
Inherited	The entry uses the credentials of it's parent entry or group.
My Personal Credentials	This allows you to use one set of credentials to replace or emulate the ones from your Windows session.



There is another possibility when using [User Specific Settings](#) or [Local Machine Specific Settings](#). Please consult [Credentials](#) on how to use an entry from the [Private Vault](#)

3.4.5.2 More

3.4.5.2.1 Description

Description

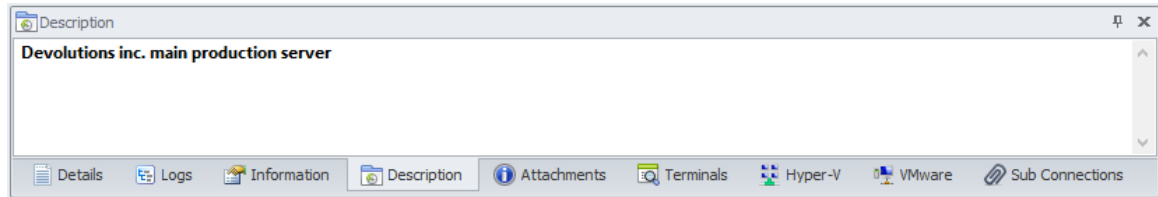
Remote Desktop Manager supports three description types:

- Plain text description
- Note
- External URL description

The description is displayed in **bold** on the dashboard

Plain Text Description (Basic)

This is the most basic description, and is simply a text without formatting.



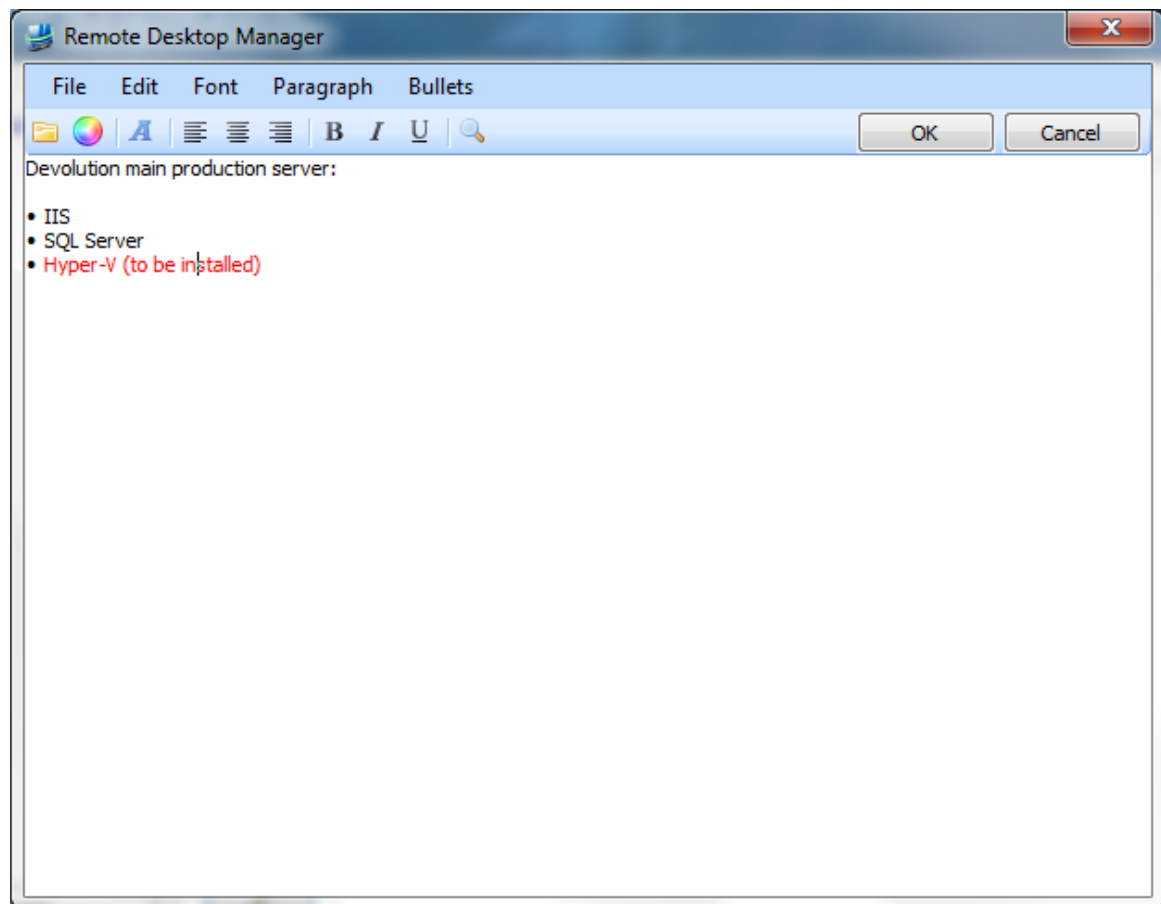
Plain text description

Note

The RTF (Rich Text Format) description offers more formatting options, and allows you to change:

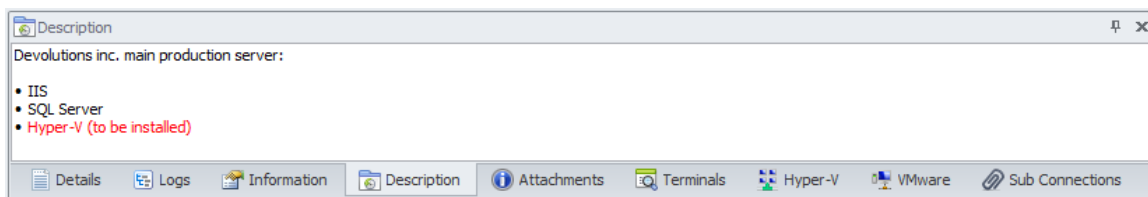
- Text color
- Font size
- Font style
- Text alignment

You can also create lists (numbered and bullets).



RTF description editor

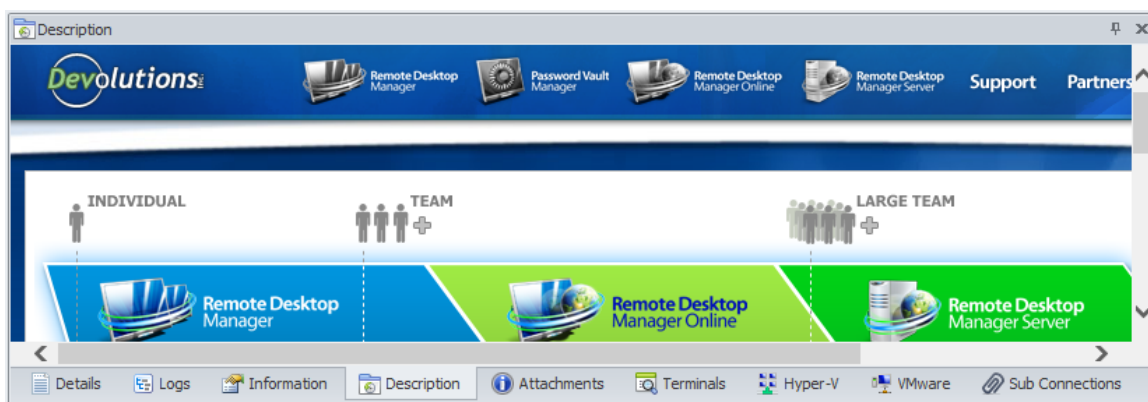
Remote Desktop Manager will display the description exactly the way it was formatted in the editor.



RTF text description

External URL Description

The description may also be a link to a URL (e.g. on a server in the Intranet). By using session variables (\$SESSION_ID\$, \$SESSION_NAME\$, etc.), the web site can generate a HTML page dynamically. This lets you integrate an external system or a custom application.

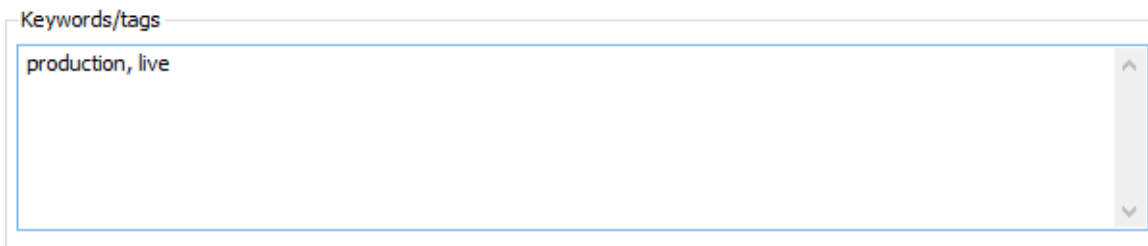


External URL description

3.4.5.2.2 Keywords/Tags

Description

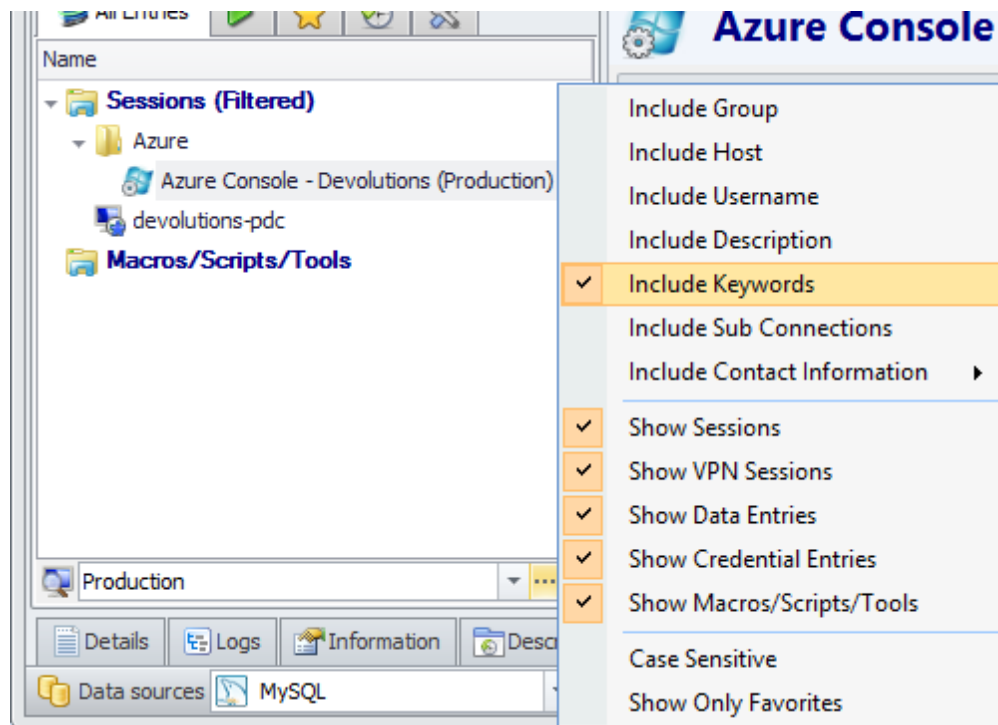
Add keywords or tags to allow searching.



Keywords/tags

Searching

Keywords searching must be enabled.

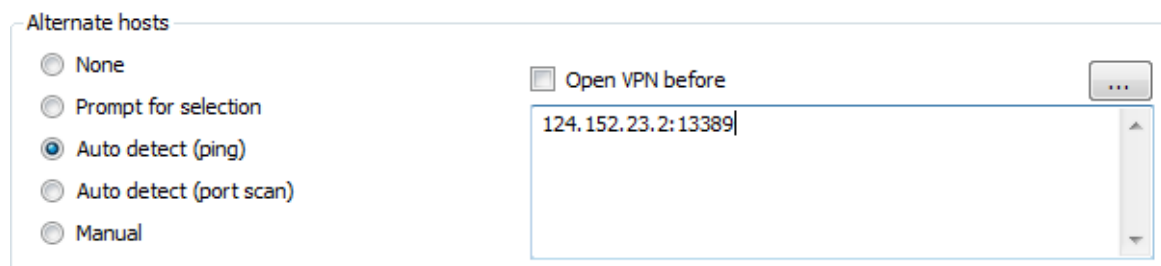


Enable keyword search

3.4.5.2.3 Alternate Host

Description

Alternate host feature allows for easy handling of changes in network topology. For example when you have a laptop that is being used at home & at the office. You may need to connect differently for each location. No worries, let the system detect how to connect.



Alternate hosts

3.4.5.2.4 Tab Page Category/Color

Description

Tab page category allows for easy grouping of tabs while the color feature allows to visually identify session groups. For example we could use red to identify production servers and green for test servers.

Settings

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

User interface

Tab page category Color

Tab title ☐ Keep tab page opened on disconnect

☒ Show in trayicon ☐ Include in shared favorites

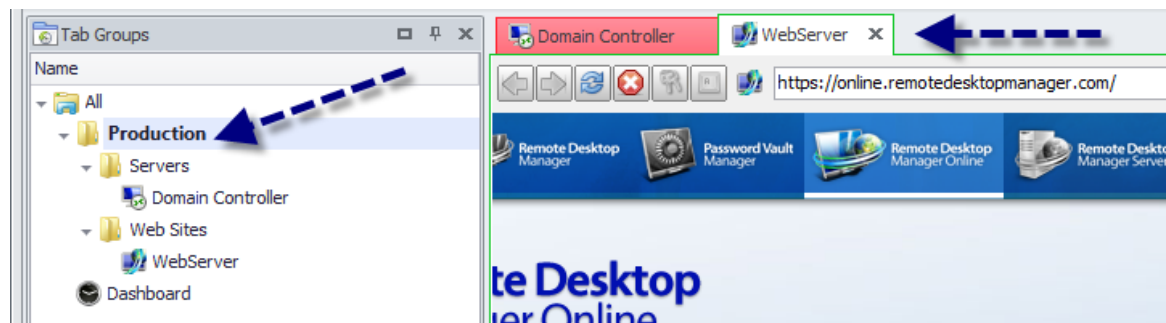
☐ Expire

Options

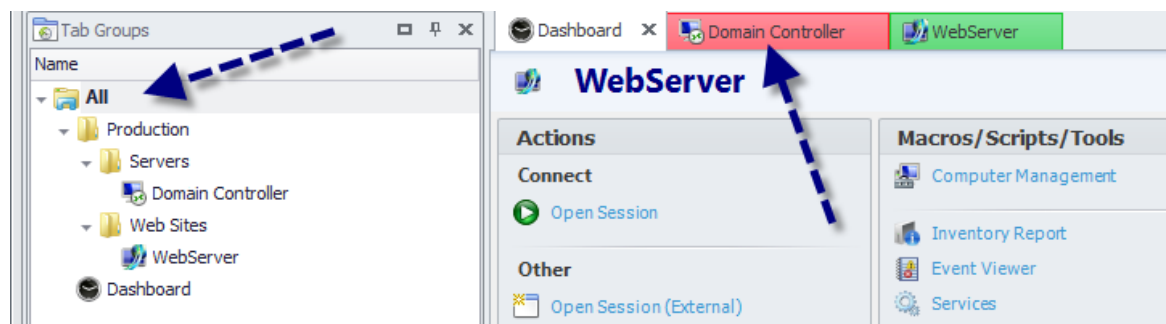
Tab Page Category

Once tab page categories have been assigned opened connections will be displayed grouped by category/subcategory within the Tab Groups window. Clicking on a session will activate it. Clicking on a category will filter the opened sessions to only display session from that category/subcategory.

See samples below:



Tab Groups - Filter on the Production category



All Tab Groups - no filter

Tab Color

When assigned the tab color will color the border of the embedded window along with the actual tab when it's not selected.

Tab Title

Indicate a tab title to display this title instead of the name of the session.

Keep tab page opened on disconnect

See topic [Keep Tabs Opened](#) for more information

This option can be change in multiple sessions at the same time using the [Batch Edit](#) feature.

Show in trayicon

You sessions will be available from the [trayicon](#).

Include in shared favorites

The session will be added to the shared [favorite](#).

Expire

Enter a date to change the [status](#) of the session to "Expired".

3.4.5.3 VPN**3.4.5.3.1 Overview****Description**

A VPN connection can be configured in the session properties, in the VPN tab. The connection can be established automatically, manually or when a particular condition is met.

There are multiple natively supported VPN connection types, and many more are available through add-ons, please consult [VPN Add-ons](#) for more information.

Although you can define your VPN details in the session, it's a best practice to link to an existing VPN session. Please refer to [Link To Existing Session](#) for more information.

VPN Opening mode

Option	Description
Always connect	Opens the VPN each time the session is launched.
Manual	The VPN is configured, but it must be opened manually from the session context menu or the dashboard.
Connect if unable to ping/ port scan	The application will try to ping the host or a configured address. If unable to reach the host, the VPN will be opened before launching the session.
Inherited	Will connect using VPN configured in the parent entry.
Ask for confirmation	Ask for a confirmation before opening the VPN.

VPN Closing mode

Option	Description
On session close	Closes the VPN as soon as it detects that the session is closed. However, some session types' close events cannot be detected, and as such the VPN must be closed manually.

Manually later	The VPN must be closed manually from either the session context menu or the dashboard.
Confirm disconnect	The application will ask for a confirmation before closing the VPN when it detects that the current session is terminated.

VPN Group

A VPN Group will regroup the entries which share the same VPN connection.

When multiple entries are members of the same VPN group and 2 or more of them are connected, the VPN connection will stay active until the last session disconnects.

The VPN group name needs to be exactly the same to ensure that Remote Desktop Manager increments the usage counter.

The VPN close mode need to be set to **On sessions close** to use this feature.

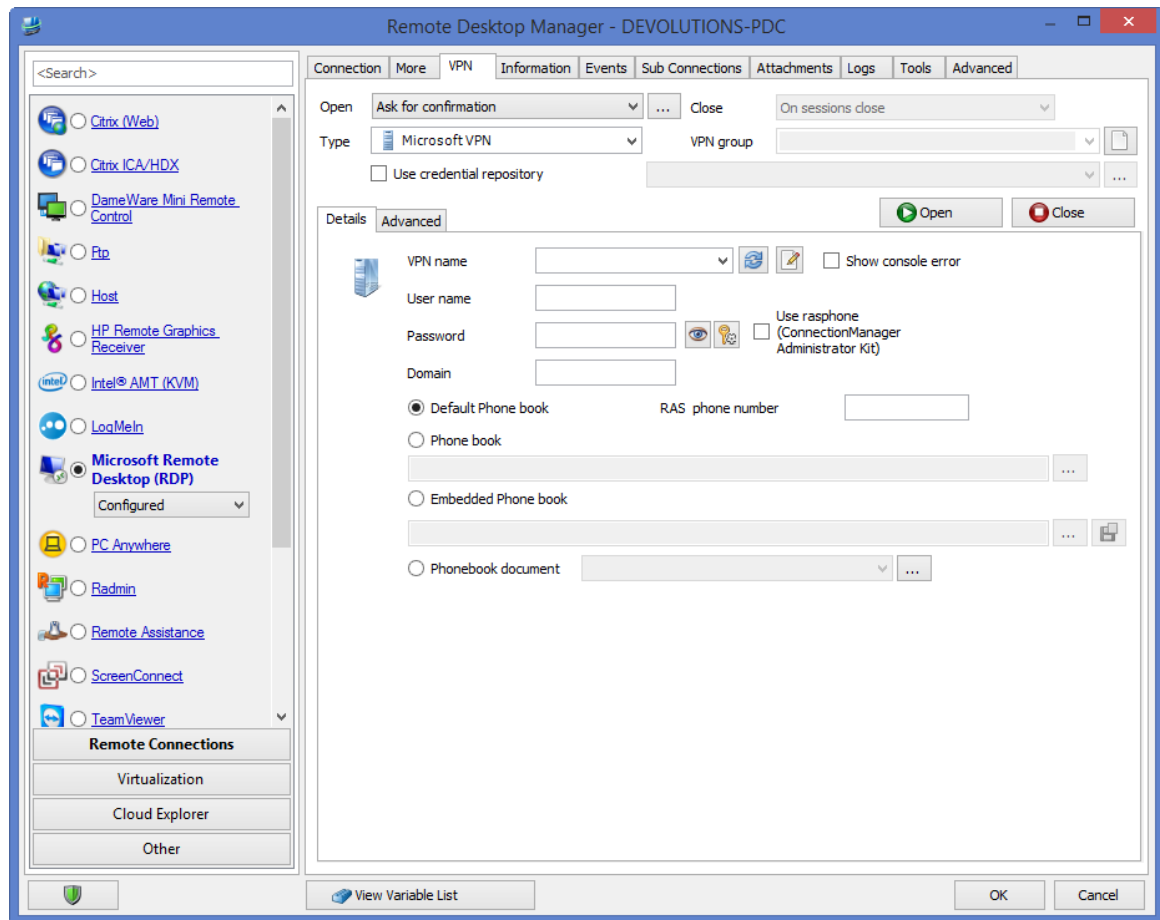
VPN Group



VPN groups are defined inside each individual entries under the VPN tab.

Settings

Each VPN type has its own set of properties to configure, and you must know them in order to properly configure them.



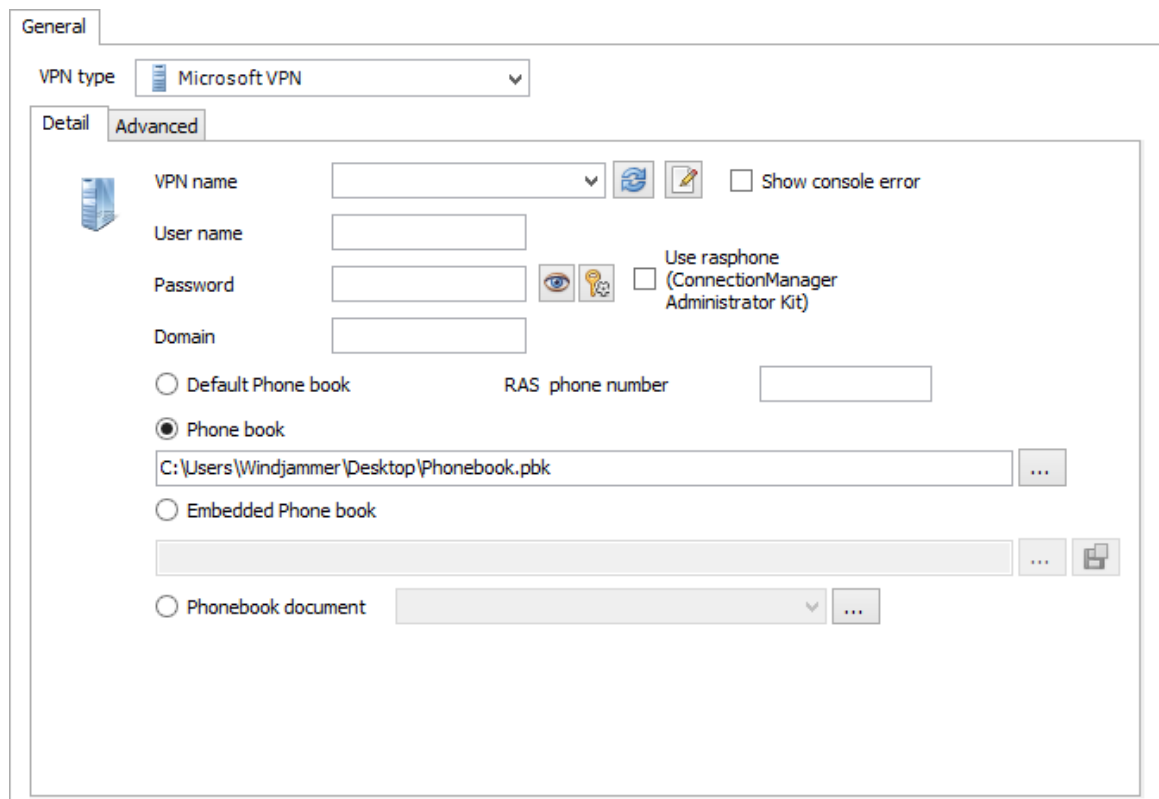
VPN session configuration

VPN with Phonebook

You can configure a Phonebook inside a VPN entry. This VPN entry can use the Default Phonebook; a specific Phonebook; an embedded Phonebook; or a reference to a document of type Phonebook.



This is only supported by the Microsoft VPN.



Phonebook inside VPN

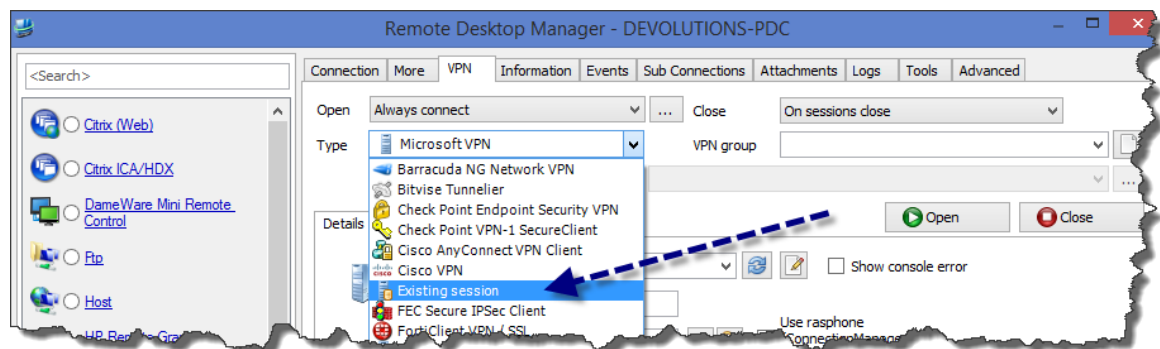
Please refer to [Phonebook](#) for more information on phonebook.

3.4.5.3.2 Link To Existing Session

Description

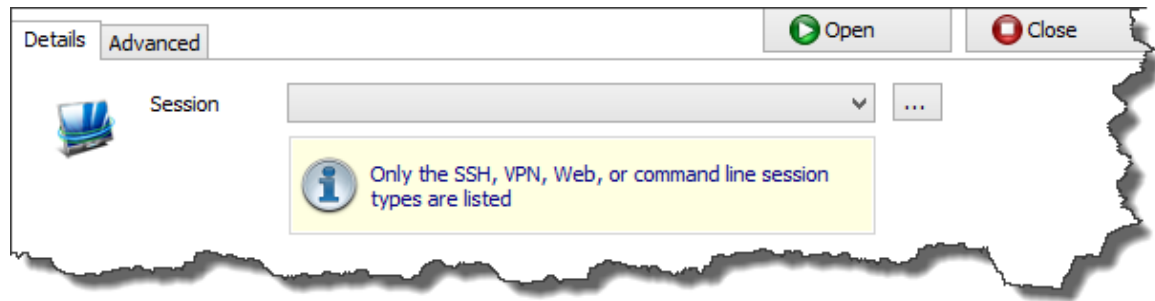
Any session can be set up to use entries of various types as its VPN definition. The benefit of doing this is that you can share your VPN settings with multiple sessions, and manage them in one place.

After selecting your desired option from the **Open** drop-down, simply select the value **Existing Session** in the VPN type combo box.



VPN configuration tab

The settings tab will now allow you to select an existing entry from the Session drop-down.



Details tab



Only SSH, VPN, Web or command line session type can be selected in the drop-down.

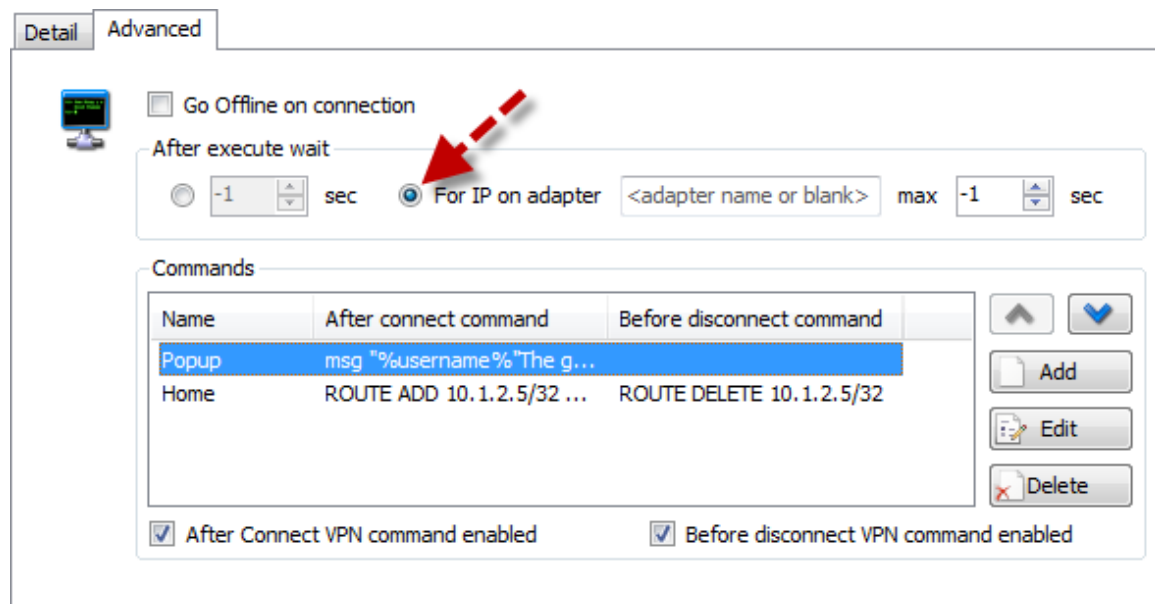
3.4.5.3.3 Post/Pre VPN Commands

Description

Post/Pre VPN Commands allows you to specify commands to be run after the VPN connection has been established and/or before the VPN connection is closed. You can specify custom commands or use the simple UI for defining route commands.

Enable

Enable the Post/Pre VPN Commands by selecting "After execute wait" - "For IP on adapter". This specifies that RDM will wait until the given adapter has acquired a valid IP.



VPN Advanced Tab

RDM will wait for the adapter named **<adapter name or blank>**. In most cases leave this field blank. Blank specifies that RDM will use the VPN name as the adapter name, works with most VPNs

(Microsoft for example) where the VPN is the adapter. In cases of a SonicWALL VPN where the adapter is only created once the VPN has been enabled/connected. In this case enter (part of) the adapter name, you can use the command line "route print" to quickly find the adapter name. Example:
SonicWall Virtual

```
C:\Windows\system32>route print
=====
Interface List
30...00 60 73 13 5a da .....SonicWALL Virtual NIC
33...00 ff e9 85 c0 a4 .....TAP-Win32 Adapter V9
15...74 e5 0b 30 00 a7 .....Microsoft Virtual WiFi Miniport Adapter #2
14...74 e5 0b 30 00 a7 .....Microsoft Virtual WiFi Miniport Adapter
13...74 e5 0b 30 00 a6 .....Intel(R) WiFi Link 1000 BGN
11...84 8f 69 b7 6a 11 .....Realtek PCIe GBE Family Controller
20...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
21...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
1.....Software Loopback Interface 1
```

Route Print Output - Interface List

The "max -1 sec" specifies the time out in seconds that RDM will wait for the adapter. -1 is wait forever, if ever you have specified the wrong adapter name, the -1 option may hang the system.

Define Custom Command

With custom commands you can execute any command after the VPN connect or/and before VPN disconnect. The possibilities are endless. Below is an example that displays a message specifying that the gateway is up and specifies the IP. Simple but effective.

Remote Desktop Manager

Custom Pre/Post Connect VPN Commands

Please enter required information.

Name: Ready to use

☒ After Connect VPN command enabled ☐ Before disconnect VPN command enabled

☒ Run in 64 Bits mode ☐ Run as Administrator

☒ Custom \$GATEWAY\$: VPN IP

After VPN connect run the following

msg "%username%"The gateway with IP \$GATEWAY\$ is now ready to use.

Before VPN disconnect run the following

☐ Route (Add/Remove)

IP: Metric:

Mask: Interface:

Gateway

☒ Use VPN IP

OK Cancel

Custom Command Example

Define Route Command

Define a route to be added/remove along with this VPN connection. The option to use or not the VPN's IP as the gateway allows you to direct a route away from the gateway to any IP. If you don't specify the "Use VPN IP" check box then the gateway must be manually specified.

Remote Desktop Manager

Custom Pre/Post Connect VPN Commands
Please enter required information.

Name:

☒ After Connect VPN command enabled ☒ Before disconnect VPN command enabled

☒ Run in 64 Bits mode ☒ Run as Administrator

☐ Custom \$GATEWAY\$: VPN IP

After VPN connect run the following

Before VPN disconnect run the following

☒ **Route (Add/Remove)**

IP: Metric:

Mask: Interface:

Gateway: ☒ Use VPN IP

OK Cancel

Route Command Example

Command Management

Add, edit or delete commands. Specify the order of the command execution. Disable all After Connect or Before Disconnect commands.

Commands

Name	After connect command	Before disconnect command
Popup	msg "%username%" "The g..."	
Home	ROUTE ADD 10.1.2.5/32 ...	ROUTE DELETE 10.1.2.5/32

☒ After Connect VPN command enabled ☒ Before disconnect VPN command enabled

Buttons: Add, Edit, Delete

Route Command Example



The order of commands are reversed for the **Before disconnect** step. Example:

- connect
- execute command A before action
- execute command B before action
- use vpn
- execute command B after action
- execute command A after action
- disconnect

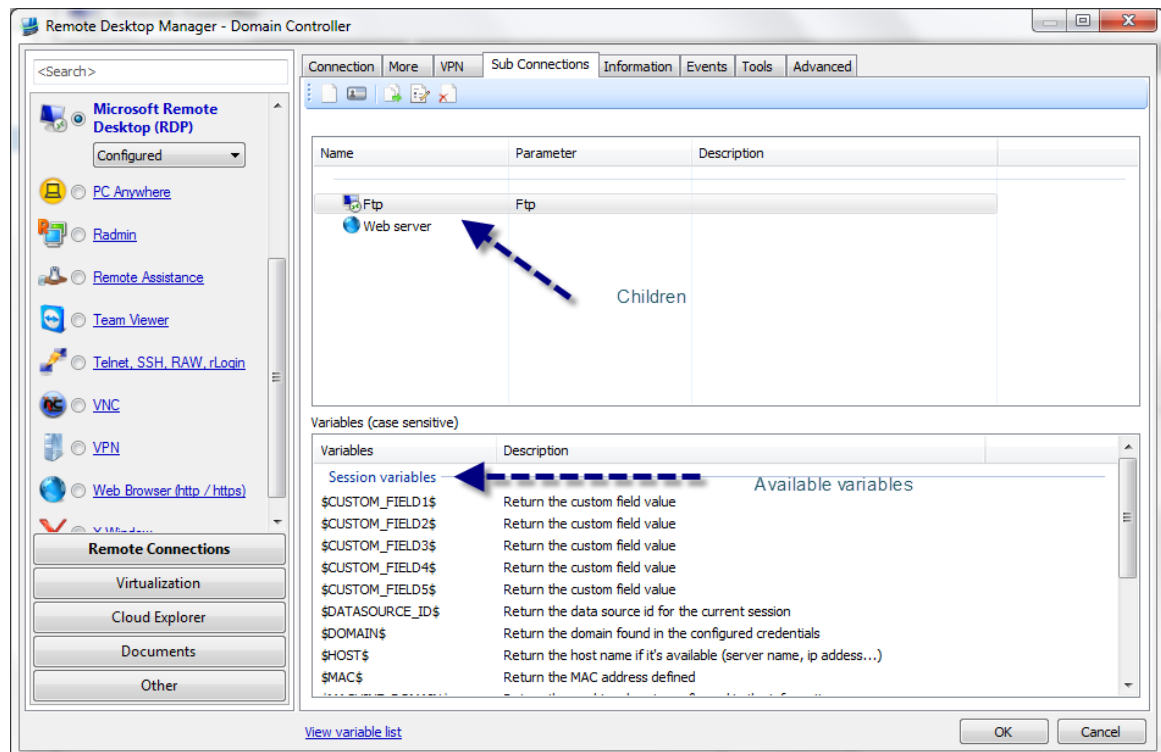
3.4.5.4 Sub Connections

3.4.5.4.1 Overview

Description

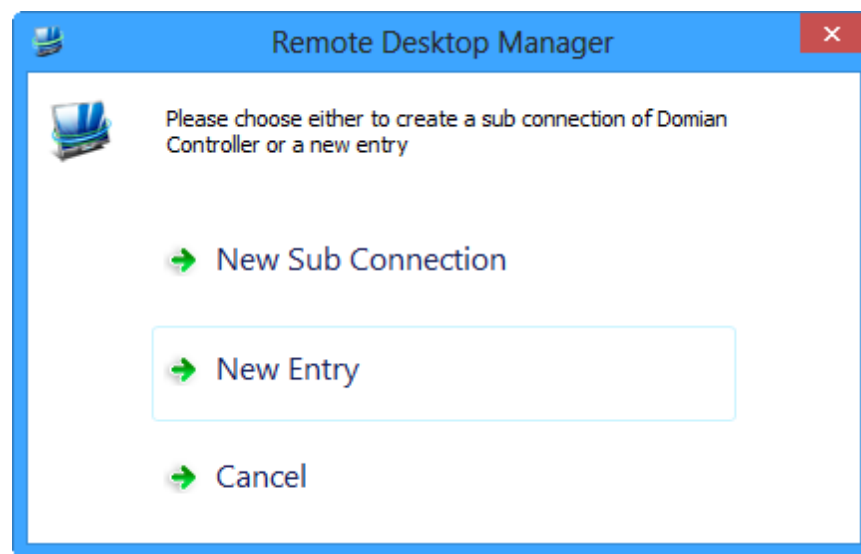
Sub connections are used to share properties between groups of sessions (e.g. the host name). They're also used to regroup many connection types for a computer (e.g. the RDP/FTP/HTTP connection).

Sub connections are configured in the parent connection in the **Sub Connections** tab page. Use the predefined variables in the child session to get access to the parent settings. The most common usage is to reuse the host name and credentials from the parent within the sub connection.



Sub connections tab page

Sub connections can also be added/created by first selecting a parent connection then with a simple right-click **Add** -> **Add...** or **Edit** -> **New Entry**. You will be prompted with the following dialog:



New connection dialog.

Sub-connections of Host entry types

Host entry types are very useful in serving as parents for sub-connections. Please see [Host](#) for details.

3.4.5.5 Information



3.4.5.5.1 General

Description

The general tab allows you to specify computer specific information such as operating system & MAC address. This will control/enable certain actions within the dashboard.

Settings

General Hardware Contact Purchase Notes Custom Fields Statistics


 Domain MAC 

OS Architecture

Site Blade

Rack Details

Software

☐ Is virtual machine
 ☐ Is Terminal server
 ☐ Is Hyper-V server
 ☐ Is VMware server
 ☐ Is XenServer server

General tab

Option	Description
Domain	Specify remote computer Domain.
MAC	Retrieve remote computer MAC address and enable Wake On Lan functionality.
OS	Specify remote computer Operating System.
Architecture	Select between 32-bit or 64-bit.
Site	Indicate the site where his locate the remote computer.
Blade	Indicate if the remote computer his a blade PC.
Rack	Indicate in which rack the device is located.
Details	Indicate any important details on the remote computer.
Software	List the softwares install on a remote computer.
Is virtual machine	Allows to specify the virtual machine name.
Is Terminal server	Enable Terminal console in dashboard.
Is Hyper-V server	Enable Hyper-V console in dashboard.
Is VMware server	Enable VMware console in dashboard.
Is XenServer server	Enable XenServer console in dashboard.

3.4.5.5.2 Hardware

Description

The hardware tab allows you to specify the hardware information of a remote computer.

Settings

General

Hardware


Contact

Purchase

Notes

Custom Fields

Statistics

 CPU

Memory

Monitors

Asset Tag

Details

Hardware tab

Option	Description
CPU	Indicate remote computer CPU model.
Memory	Indicate remote computer memory amount and memory model.
Monitors	Indicate the number of monitors and the monitor model.
Asset Tag	Enter remote computer Asset Tag.
Details	Indicate any details on the remote computer.

3.4.5.5.3 Contact

Description

The contact tab allows you to enter contact information for a given session. Very useful when you are managing third party servers.

Settings

The screenshot shows the 'Contact' tab in the Remote Desktop Manager application. At the top, there is a tab bar with 'General', 'Hardware', 'Contact', 'Purchase', 'Notes', 'Custom Fields', and 'Statistics'. The 'Contact' tab is selected. Below the tab bar, there is a 'Contact' section with a 'Default' dropdown menu. The main area contains a form with various fields for contact information, organized into two columns. On the left, there is a small icon of two people. The fields include: First name, Last name, Company, Gender (with a dropdown menu showing 'Unspecified'), Customer #, Address, Prefix (with a dropdown menu), City, Title, State, Zip code, Email, Country (with a dropdown menu), Home phone, Work phone, Fax, Cell, Skype, and Website. On the right side of the form, there are four buttons: 'View Map', 'Email Contact', 'Call (Skype)', and 'Open website'.

Contact tab

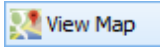
Default Contact

Enter the **contact information** to enter contact information related to a remote session.

Reference Contact

Use **reference contact** to associate a contact to a credentials entry.

View Map

Enter a complete address for a contact and the  button will show you his location in Google Maps.

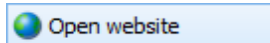
Email Contact

Enter a email address for a contact and click the  button to send him directly a email.

Call (Skype)

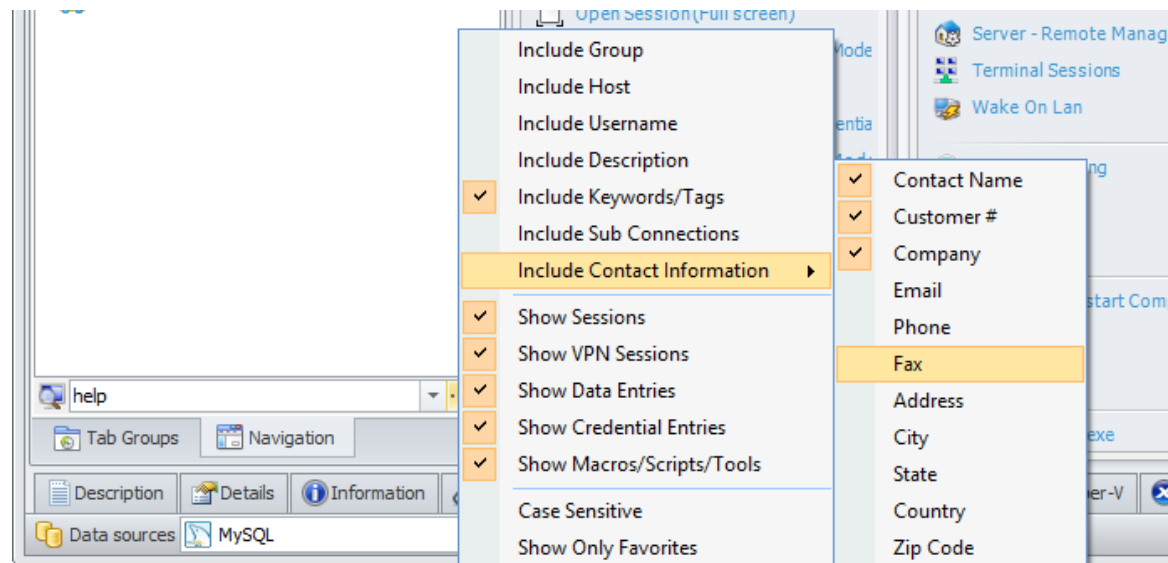
Enter Skype username for a contact and click  button to contact him via Skype directly.

Open website

Enter a website for a contact and click the  button to go directly on his website.

Searching

Most information on this tab can enabled for searching. Please refer to [Search/Filter](#)



Search options menu, click on ... button.

Please refer to [Contact](#) for more information.

3.4.5.5.4 Purchase

Description

The purchase tab allows you to enter information of a specific equipment.

Settings

General	Hardware	Contact	Purchase	Notes	Custom Fields	Statistics
Purchase						
Date	<input type="checkbox"/>	2014-01-20		Age		
Vendor		<input type="text"/>				
Serial number		<input type="text"/>				
Warranty						
Expiration	<input type="checkbox"/>	2014-01-20		Remaining		
Service tag		<input type="text"/>				
Service level		<input type="text"/>				

Purchase tab

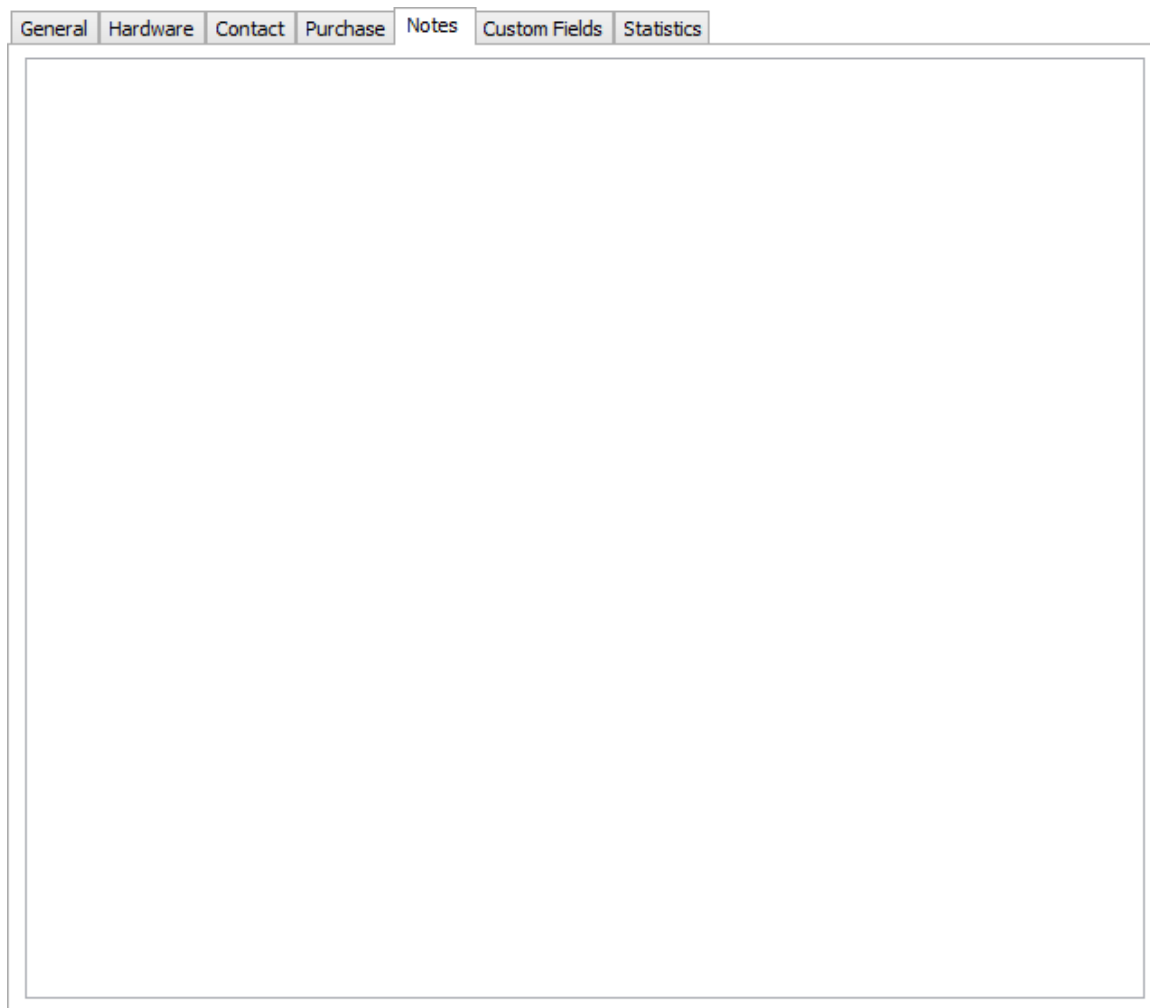
Option	Description
Date	Indicate the date that the purchase of the equipment has been made.
Vendor	Specify the name of the vendor who sold the equipment.
Serial number	Enter the serial number of the equipment.
Expiration	Enter the expiration date of the warranty.
Service tag	Indicate the equipment service tag.
Service level	Indicate the technical service level that was purchase for this equipment.

3.4.5.5.5 Notes

Description

The notes tab allows you to enter any notes related to a remote computer.

Settings



Notes tab

3.4.5.5.6 Custom Fields

Description

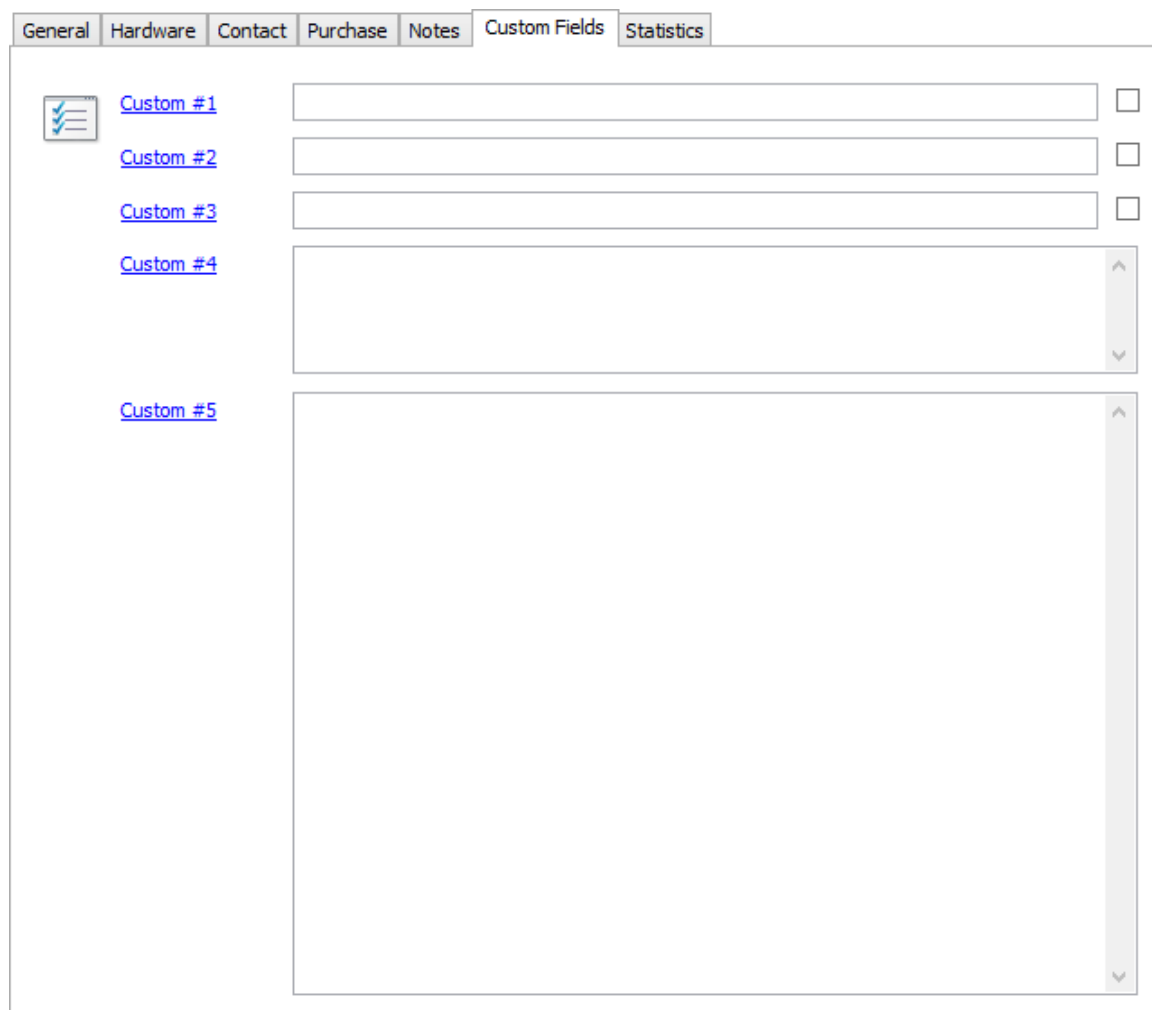
The custom fields tab allows you to define custom properties and values that can then be access via variables (\$CUSTOM_FIELD1\$, \$CUSTOM_FIELD2\$, etc.) in child connections or Macros/Scripts/Tools.




Custom field 1, 2 & 3 can be encrypted for enhanced security.
When used with an [Advanced Data Source](#) users must have reveal password capabilities to be able to decrypt and view the value.



Must be an administrator or have reveal password privileges to see protected values.



General Hardware Contact Purchase Notes Custom Fields Statistics

 Custom #1 ☐

Custom #2 ☐

Custom #3 ☐

Custom #4

Custom #5

Custom Fields tab


3.4.5.5.7 Statistics

Description

The statistics tab provide information on the entry like:

- The user who create the entry
- The entry creation date
- The user who perform the last update on the entry
- The last date when the entry was updated

Settings

General	Hardware	Contact	Purchase	Notes	Custom Fields	Statistics
Information						
 <div> <p>Created by</p> <p>Creation date</p> <p>Last update by</p> <p>Last update date</p> </div>						

Statistics tab

3.4.5.6 Events

3.4.5.6.1 Connection Events

Description

Remote Desktop Manager gives you the flexibility to run operations before or after establishing a connection.

The operations are defined via the **Events** tab of the session properties window. Define a script or a command line to be executed. Remote Desktop Manager will execute the command at the appropriate time. You may also pass parameters, such as the session ID, the session name, or the configured username.

In addition, you can adjust the settings to run a script for an executable in a 64-bit context, or as an administrator. It's also possible to specify a timeout or pause a process currently running. This is sometimes necessary in order to allow the process to complete a task.

With **Before connection & After disconnection** events the only scripting file formate is VBScript (.

vbs).

Connection More VPN Sub Connections Information **Events** Attachments Logs Tools Advanced

Before connection

☒ None

☐ Script

☐ Command line

☐ Prompt message

☐ Wait for exit ☒ Use default working directory Wait timeout 60

☐ Run as Administrator ☐ Run in 64 bits mode Post execution pause 0

After connection

☒ Execute automatically Initial wait 0 sec

Default

Typing macro

Macro password Delay time {Delay} 300 ms

After disconnection (only supported by RDP and embedded)

☒ None

☐ Script

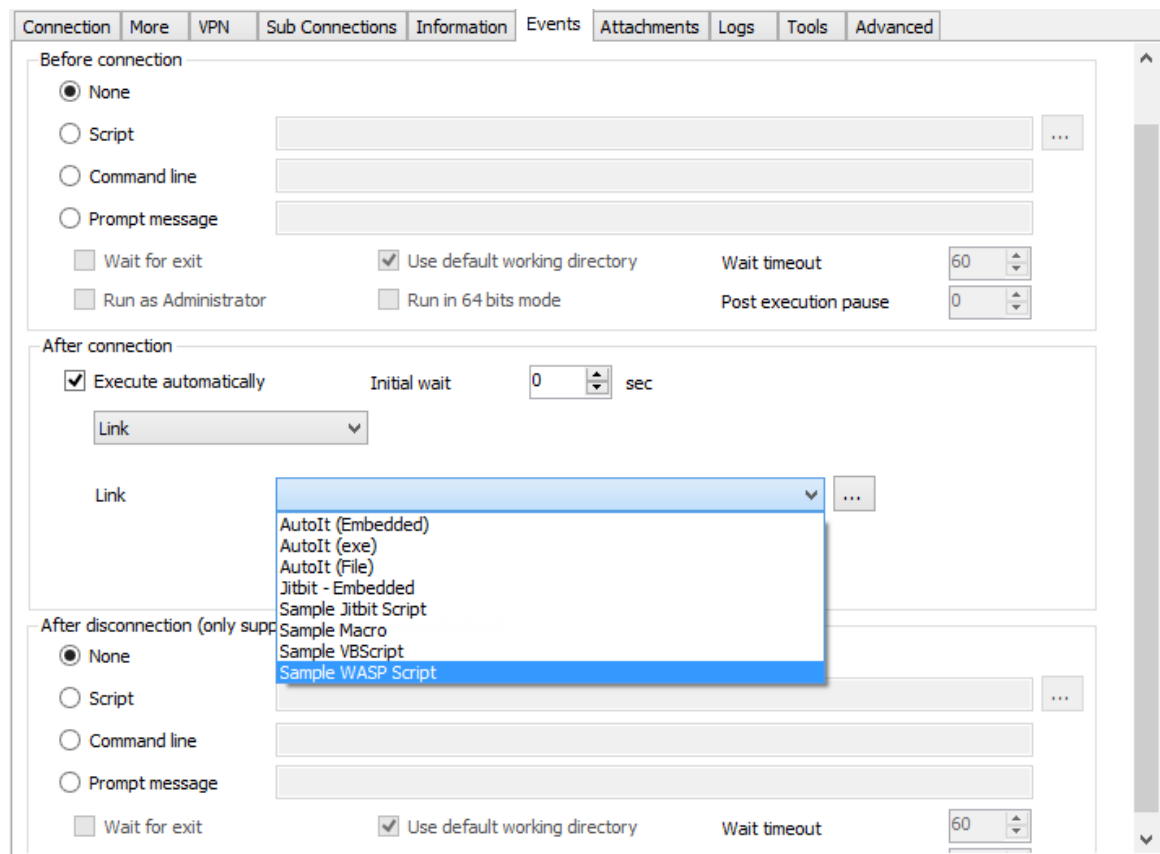
☐ Command line

☐ Prompt message

☐ Wait for exit ☒ Use default working directory Wait timeout 60

Session events tab page

After connection action may be a typing macro or link any predefined session Macro/Script/Tool.



Session events tab page - linked macro drop down

3.4.5.6.2 Auto Typing Macro

Description

The Auto Typing Macro allows you to execute automatically a typing macro once a session has been established.

The screenshot shows the 'Advanced' tab in the Remote Desktop Manager interface. The 'After connection' section is active, showing options for executing a script or command line. The 'Script' option is selected. The 'Execute automatically' checkbox is checked. The 'Typing macro' field contains the text 'hello{Delay}world{Delay}\$MACRO_PASSWORD\$'. The 'Macro password' field is masked with dots. The 'Delay time {Delay}' is set to 300 ms. The 'Wait timeout' is set to 60 seconds. The 'Post execution pause' is set to 0 seconds. The 'Use default working directory' checkbox is checked. The 'Run in 64 bits mode' checkbox is unchecked. The 'Wait for exit' checkbox is unchecked. The 'Run as Administrator' checkbox is unchecked. The 'Before connection' section is also visible, with the 'Script' option selected. The 'After disconnection' section is also visible, with the 'Script' option selected.

Auto typing macro

Typing Macro

Each key is represented by one or more characters. To specify a single keyboard character, use the character itself. For example, to represent the letter A, pass in the string "A" to the method. To represent more than one character, append each additional character to the one preceding it. To represent the letters A, B, and C, specify the parameter as "ABC".

Special keys

To specify characters that aren't displayed when you press a key, such as ENTER or TAB, and keys that represent actions rather than characters, use the codes in the following table.

Key	Code
BACKSPACE	{BACKSPACE}, {BS}, or {BKSP}
BREAK	{BREAK}
CAPS LOCK	{CAPSLOCK}
DEL or DELETE	{DELETE} or {DEL}
DOWN ARROW	{DOWN}
END	{END}
ENTER	{ENTER}

ESC	{ESC}
HELP	{HELP}
HOME	{HOME}
INS or INSERT	{INSERT} or {INS}
LEFT ARROW	{LEFT}
NUM LOCK	{NUMLOCK}
PAGE DOWN	{PGDN}
PAGE UP	{PGUP}
PRINT SCREEN	{PRTSC}
RIGHT ARROW	{RIGHT}
SCROLL LOCK	{SCROLLLOCK}
TAB	{TAB}
UP ARROW	{UP}
F1	{F1}
F2	{F2}
F3	{F3}
F4	{F4}
F5	{F5}
F6	{F6}
F7	{F7}
F8	{F8}
F9	{F9}
F10	{F10}
F11	{F11}
F12	{F12}
F13	{F13}
F14	{F14}
F15	{F15}
F16	{F16}
Keypad add	{ADD}
Keypad subtract	{SUBTRACT}
Keypad multiply	{MULTIPLY}
Keypad divide	{DIVIDE}

To specify keys combined with any combination of the SHIFT, CTRL, and ALT keys, precede the key code with one or more of the following codes.

Key	Code
SHIFT	+
CTRL	^
ALT	%

To specify that any combination of SHIFT, CTRL, and ALT should be held down while several other keys are pressed, enclose the code for those keys in parentheses. For example, to specify to hold down SHIFT while E and C are pressed, use "+(EC)". To specify to hold down SHIFT while E is pressed, followed by C without SHIFT, use "+EC".

Special commands

Commands	Description
{DELAY}	This command introduces a small delay of 300 ms (default value) before the next command.
{WINDOW:???	This command focus a window containing the specified name after the semi colon.
{PREV-WINDOW}	Select the previous window before executing the remaining commands.

Macro Password

You can define a password that is to be used within the typing macro exclusively. Use the variable **\$MACRO_PASSWORD\$** to access the password.

3.4.5.7 Attachments

3.4.5.7.1 Overview


Description

With the Enterprise edition and an [Advanced Data Source](#), you can add an attachment to an entry. The file is stored directly in the database. Please note that the file will not be available in Offline Mode.



Attachment list

The attachment can be any type and any size, depending on your bandwidth and database. You can also view a saved attachment from: the session context menu, the session properties, or directly on the dashboard.

The update button  will allow you to update directly your selected document instead of deleting it. Use it to save your local modification after an edit.

3.4.5.8 Logs

3.4.5.8.1 Options

Description



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

The Logs tab displays the usage/edition logs for the session.

It also has a feature to warn you if you attempt to open a session that is currently in use by another user of the **same** data source. The application uses the log to detect a opened connection.

There are also options to prompt for a comment, required or not, when a session is opened/closed.



The warn if already opened option is supported in embedded mode.
The open and close comments are supported in embedded and in external mode.

Connection More VPN Information Events Sub Connections Attachments **Logs** Tools Advanced

Settings

☐ Warn if already opened

☐ Prompt for comment on open

☐ Open comment is required

☐ Prompt for comment on close

☐ Close comment is required

Logs

Date Last 7 Days 2013-12-03 To 2013-12-10

☐ Show live session only (auto refresh) Client time

Message	On Open Comment	Log Date	End Date/Time	Acti
Open session		2013-12-10 1:06 PM	2013-12-10 1:48 PM	
Open session		2013-12-10 10:56 AM	2013-12-10 11:09 AM	
Open session		2013-12-10 9:53 AM	2013-12-10 10:31 AM	
Open session		2013-12-10 8:52 AM	2013-12-10 8:58 AM	
Open session		2013-12-09 2:37 PM	2013-12-09 2:50 PM	
Open session		2013-12-09 2:35 PM	2013-12-09 2:37 PM	
Open session		2013-12-09 1:56 PM	2013-12-09 2:35 PM	
Entry edited		2013-12-09 1:56 PM		
Open session		2013-12-09 1:52 PM	2013-12-09 1:56 PM	
Open session		2013-12-09 1:45 PM	2013-12-09 1:51 PM	
Open session		2013-12-09 1:44 PM	2013-12-09 1:45 PM	
Open session		2013-12-09 1:44 PM	2013-12-09 1:44 PM	
Open session		2013-12-09 1:24 PM	2013-12-09 1:29 PM	
Open session		2013-12-09 1:14 PM	2013-12-09 1:24 PM	

Logs tab

Settings

Settings

Option	Description
Warn if already opened	This setting will monitor all users of the current data source to verify if the session is already opened. This is to prevent "stealing" the session from this user. Most useful when using the administrative remote desktop licenses that allow only two connections at a time.
Prompt for comment on open	The program will prompt you for a comment when you open the session. The comment will appear in the log.
Open comment is required	Will force the user to enter an Open session comment.
Prompt for comment on close	The program will prompt you for a comment when you close the session. The comment will appear in the log.
Close comment is required	Will force the user to enter a Close session comment.

Logs

Option	Description
Date drop down	Choose the period of interest to you. You can select custom in order to enter specific dates.
Date time edit controls	Enabled when the date drop down is at Custom . Enter the start date and end date in the controls.
Show Live session only (auto refresh)	This will hide the inactive sessions from the list. It will start a timer to auto-refresh the list periodically.
Time	Choose between Client Time, Local Time and UTC Time. Useful for distributed systems.
Refresh	Perform a manual refresh using this button.

Right click on the log entry to display the contextual menu to show the log details form, refer to [Log Details](#) for information on that form.

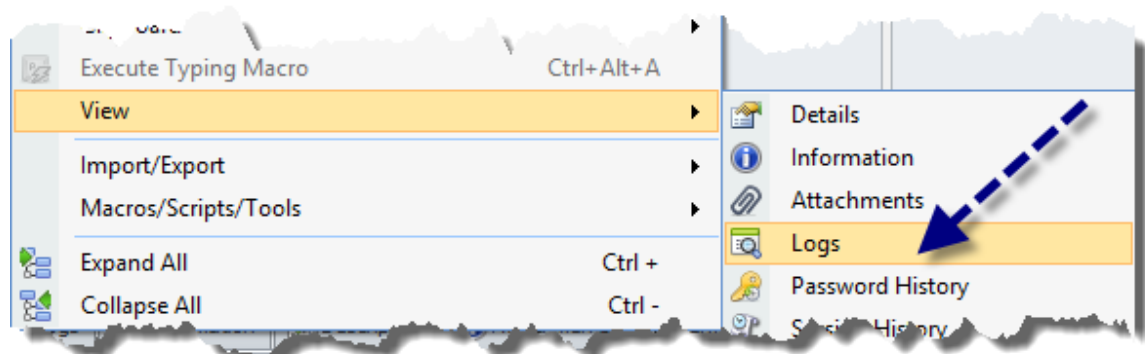
3.4.5.8.2 View Logs

Description



This feature requires an [Advanced Data Source](#) such as [MSSQL](#) and [MySQL](#).

Allows for viewing session activity logs. The log viewer displays information about session activity. Things like open session durations, open/close comments, user who performed the action & action time.



Right-click View -> Logs

Message	On Open Comment	Log Date	End Date/Time	Active Time	Duration	On Close Comment
Open session		10/30/2012 2:11 PM	10/30/2012 2:11 PM	3 sec	9 sec	
Open session		10/30/2012 2:11 PM	10/30/2012 2:11 PM	13 sec	26 sec	
Entry edited		10/30/2012 2:11 PM				
Open session		10/30/2012 2:10 PM	10/30/2012 2:10 PM	9 sec	8 sec	
Password history was revealed		10/30/2012 1:44 PM				
Password history was revealed		10/30/2012 1:43 PM				
Password history was revealed		10/30/2012 1:43 PM				
Entry edited		10/30/2012 1:43 PM				
Entry edited		10/30/2012 1:21 PM				
New entry added		10/30/2012 1:20 PM				
Entry deleted		10/30/2012 1:20 PM				
Entry edited		10/30/2012 1:20 PM				
Entry edited		10/30/2012 1:19 PM				
New entry added		10/30/2012 9:49 AM				

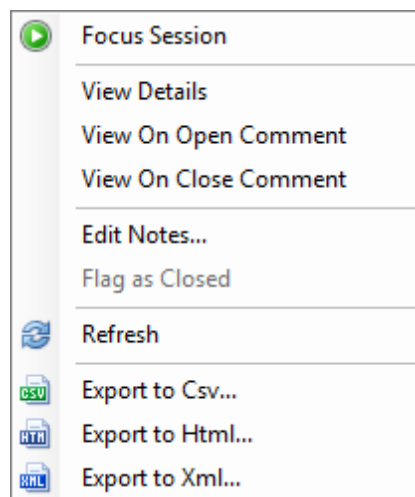
Log viewer

Right click on the log entry to display the contextual menu. It is described in [Log Details](#)

3.4.5.8.3 Log Details

Description

When you are viewing a entry usage log, either in the entry [Options](#), or in [View Logs](#) (Accessible via **View -> View Usage Log (Database)**), you are presented with a contextual menu.



Log Entry Contextual Menu

Menu Items

- **Focus Session:** Set the focus on the corresponding entry in the navigation tree view.
- **View Details:** Display the information window for the log entry. see below for details.
- **View On Open Comment:** Displays the Open comment in a simplified window.
- **View On Close Comment:** Displays the Close comment in a simplified window.
- **Edit Notes...:** Edit the log entry note in a simplified window

- **Flag as Closed:** Enabled only for open entries, will force the status to Closed
- **Refresh:** Performs a refresh of the log entry.
- **Export to Csv...:** Opens a dialog to export the content of the grid to a Csv file.
- **Export to Html...:** Opens a dialog to export the content of the grid to a Html file.
- **Export to Xml...:** Opens a dialog to export the content of the grid to a Xml file.

Details window

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

General Tab

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

The screenshot shows a window titled 'Remote Desktop Manager' with a sub-header 'Log entry' and a button 'View the current log entry'. Below this is a tabbed interface with three tabs: 'General', 'Details', and 'Comments'. The 'General' tab is active and displays the following fields:

Connection	test	Connection type	Microsoft Remote Desktop (RDP)
Group			
Message	Open session		
Start	2013-02-01 - 2:58 PM	End	2013-02-01 - 2:58 PM 20 sec
Notes	<div></div>		

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

General Tab

Details tab

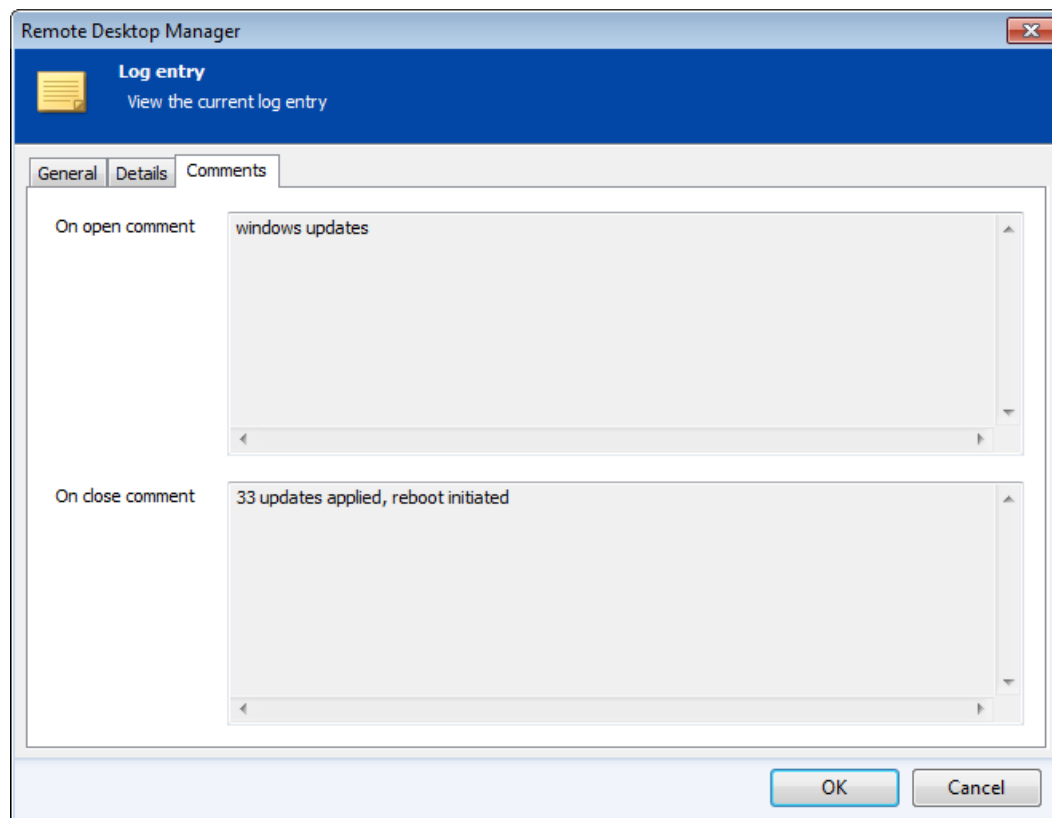
The details tab displays information on the User and computer from which the session was started, and on the destination host. It also displays information if the session was forcibly closed using the Close menu.

The screenshot shows a window titled "Remote Desktop Manager" with a sub-header "Log entry" and the text "View the current log entry". Below this is a tabbed interface with three tabs: "General", "Details", and "Comments". The "Details" tab is currently selected. It contains several input fields: "User name" with the value "DEVOLUTIONS22\Maurice", "Database user name" with "sa", "Machine name" with "DEVOLUTIONS22", "Message type" with "Open Connection", and "Host" with "test". To the right of these fields is a checkbox labeled "Open embedded/tab" which is unchecked. Below these fields is a section titled "Manual close information" containing two more input fields: "Closed by" and "Close time". At the bottom right of the dialog are "OK" and "Cancel" buttons.

Details tab

Comments tab

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



Comments tab

3.4.5.9 Tools

3.4.5.9.1 Overview

Description


The tools tab allows you to define the credentials used by the Macros/Scripts/Tools when remote credentials are required. For example: execute a remote WMI query or remote PowerShell script.

Settings

Connection More VPN Information Events Sub Connections Attachments Logs Tools Advanced

Credentials

☒ Use default credentials
☐ Use session credentials
☐ Use custom credentials

User name
 Domain
 Password  ☐ Always ask credentials



☐ Use credential repository
 Credentials

☐ Use my personal credentials

Settings

☐ Open VPN before execution

Management Tools

iLO 
 Home page 

Intel® AMT

☐ Intel® AMT

Management

Tools tab

Credentials

Option	Description
Use default credentials	Use the default credentials.
Use session credentials	Use the same credentials as defined in the session.
Use custom credentials	Use a specific username, password or domain.
Use credentials repository	Uses a credential entry linked entry which can be external credentials like KeePass for example. Very useful for sharing or reusing credentials among entries.
Use my personal credentials	This allows you to use one set of credentials to replace or emulate the ones from your Windows session. See My Personal Credentials topic

Settings

Option	Description
--------	-------------

Open VPN before execution	Specifies that the session defined VPN should be activated prior to running of the Macros/Scripts/Tools.
---------------------------	--

Management Tools

Option	Description
iLO	Indicate the link to access iLO remote management system.
Home page	Indicate the link to access the home page.

Intel® AMT

Consult [Intel® AMT](#) topic for more information.

3.4.5.9.2 Intel® AMT

Description

Remote Desktop Manager has built-in Intel® AMT support. You can perform actions like reboot, power up/down or open KVM directly in Remote Desktop Manager.



Since Remote Desktop Manager integrates Intel® AMT using Ultra VNC, functionality will be accessible depending on how you've configured Intel® AMT. For example the SMB mode is not supported in the Enterprise mode.

Settings

Select the Tools tab of a session and activate Intel® AMT support.

Management

Intel® AMT

☒ Intel® AMT

Management **KVM**

☒ Prompt for credentials
☐ Use custom credentials
 User name
 Password ☐ Prompt for password
☐ Use credential repository
 Credentials

Management

Option	Description
Prompt for credentials	Intel AMT will prompt for a username and password on every connection.
Use custom	Enter a custom username and password to connect on Intel AMT.

credentials	
Use credential repository	Select a credential from the repository.

KVM

Intel® AMT

☒ Intel® AMT

Management KVM

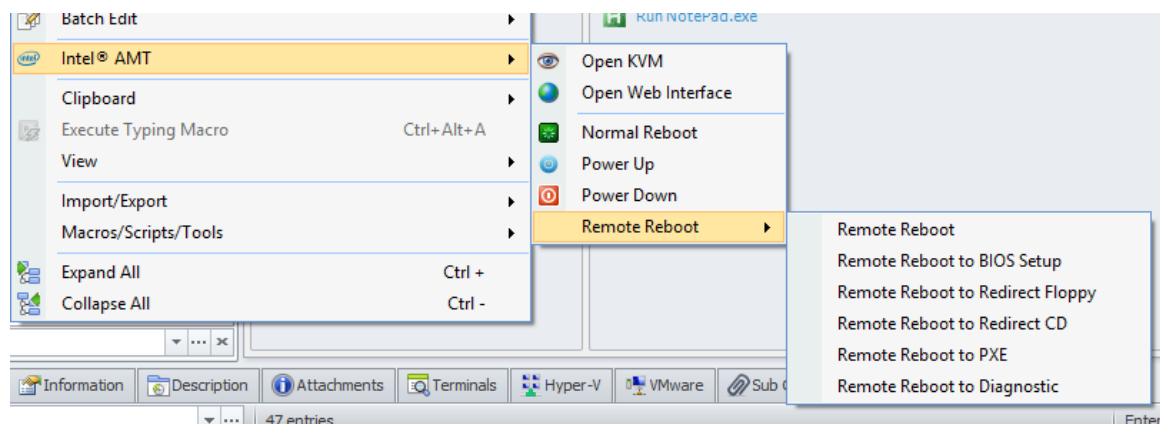
☒ Same as AMT Management
☐ Prompt for credentials
☐ Use custom credentials
 Password ☐ Prompt for password
☐ Use credential repository
 Credentials

KVM

Option	Description
Same as AMT Management	The same credentials to connect on AMT will be use to connect on KVM.
Prompt for credentials	KVM will prompt for a username and password on every connection.
Use custom credentials	Enter a custom username and password to connect on KVM.
Use credential repository	Select a credential from the repository.

Actions

Right-click on the session and select **Intel® AMT -> ...**



Intel® AMT menu

3.4.5.10 Advanced

3.4.5.10.1 Overview

Description

The advanced tab holds the advanced session options.

Advanced tab

Settings

Miscellaneous

Feature	Description
Sort priority	Controls where the session will reside within the sorted list/tree view. Descending order is used to display, therefore give a higher rating to

	have the session appear before.
Encrypt configuration in data source	By default only passwords are encrypted. When you enable this option the entire session configuration is also encrypted.
Allow password in variable	The default functionality of the \$PASSWORD\$ variable is only available when used via command line. This option will enable the \$PASSWORD\$ variable in all situations. This has major security repercussions if you have a system where not all users are allowed see the session password, therefore use with caution.
Force machine name as domain name	Send machine name as domain when supplying credentials. This is useful when the credentials you use are for the local machine only.
Embedded footer visible	On open session footer will be visible
Allow open multiple connections	When a connection is already open and you open it again, create a new instance instead of focusing the other session
User name format	<p>Determines the username 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:</p> <p>Default: does not change the user name.</p> <p>Domain\Username: formats the username by prefixing with the domain name.</p> <p>Username@Domain: formats the username by appending the domain name.</p>

Is Online

Feature	Description
Check is Online	Check if the host is online and display host availability in tree view
Online Detection	Validate if host is available with a ping or port scan



Enabling this option can cause performance degradation on your system due to the continuous pinging. Use this feature accordingly.

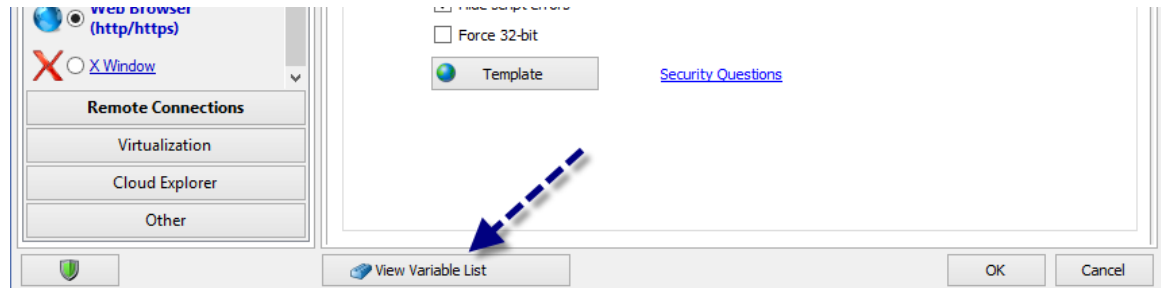
IDs (Used on the Command line or in PowerShell scripts)

Feature	Description
Data Source ID	Internal RDM data source ID. Used as a Command Line Arguments or when using RDM PowerShell extensions.
Session ID	Internal RDM session ID. Used as Command Line Arguments or when using RDM PowerShell extensions.
Command line	Fully defined command line to start this session via command line. Hit the copy button to copy the entire command line.
Create Desktop Shortcut	Automatically create a desktop shortcut.

3.4.6 Variables

Description

Session variables can be used in any session configuration, or with any templates. They will be replaced by their corresponding values just prior to a connection.



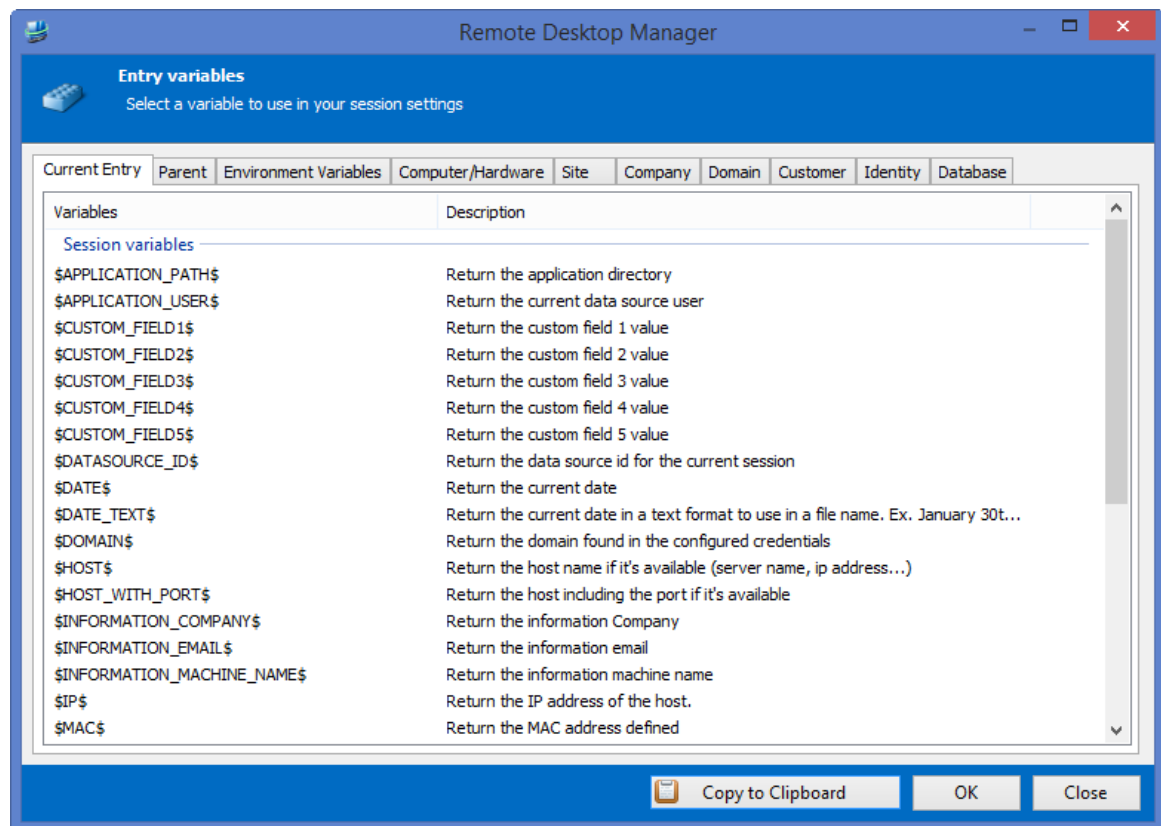
View Variable List

You can select a variable by double clicking on it directly in the dialog. For ease of use there is an hyperlink 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



Entry variables

The variables are classified 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.

Current Entry



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

For an [Advanced Data Source](#), the administrator can disable usage of this variable for the whole data source.

Session variables

Option	Description
\$CUSTOM_FIELD1\$	Return the custom field field 1 value
\$CUSTOM_FIELD2\$	Return the custom field field 2 value
\$CUSTOM_FIELD3\$	Return the custom field field 3 value
\$CUSTOM_FIELD4\$	Return the custom field field 4 value
\$CUSTOM_FIELD5\$	Return the custom field field 5 value
\$DATASOURCE_ID\$	Return the data source id for the current session

\$DOMAIN\$	Return the domain found in the configured credentials
\$HOST\$	Return the host name if it's available (server name, ip address...)
\$HOST_WITH_PORT\$	Return the host including the port if it's available
\$INFORMATION_COMPANY\$	Return the information Company
\$INFORMATION_EMAIL\$	Return the information email
\$INFORMATION_MACHINE_NAME\$	Return the information machine name
\$IP\$	Return the host name if it's available (server name, ip address...)
\$MAC\$	Return the MAC address defined
\$MACHINE_DOMAIN\$	Return the machine domain configured in the information
\$MACRO_PASSWORD\$	Return the typing macro password
\$NAME\$	Return the session name
\$PASSWORD\$	This variable is replaced by the password. It's only available when enabled in the advanced options
\$PORT\$	Return the host port if it's available (server name, ip address...)
\$QUICK_CONNECT\$	This variable is replaced by the quick connect value Note 2
\$SERIAL\$	Return the serial number in the invoice tab
\$SERVICE_TAGS\$	Return the service tag field located in the information tab
\$SESSION_ID\$	Return the current session id (guid)
\$USERNAME\$	Return the user name found in the configured credentials
\$VIRTUAL_MACHINE_ID\$	Return the virtual machine ID

Global variables

Option	Description
\$APPLICATION_PATH\$	Return the application path
\$APPLICATION_USER\$	Return the current data source user
\$DATE\$	Return the current date
\$DATE_TEXT\$	Return the current date in a text format to use in a file name. Ex: January 30th 2013 -> 20130130
\$LOCAL_IP\$	Return the local IP v4 address
\$MY_MACHINE_NAME\$	Return the current machine name
\$PUBLIC_IP\$	Return the public IP exposed on the internet
\$TIME\$	Return the current time
\$TIME_TEXT\$	Return the current time in a text format to use in a file name. EX: 8h15 30 -> 081530

Parent

This context exists only when in a sub-connection. It returns the corresponding value taken from the parent entry.



\$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 of the general tab.

Option	Description
\$PARENT_CUSTOM_FIELD1\$	Return the custom field field 1 value
\$PARENT_CUSTOM_FIELD2\$	Return the custom field field 2 value
\$PARENT_CUSTOM_FIELD3\$	Return the custom field field 3 value
\$PARENT_CUSTOM_FIELD4\$	Return the custom field field 4 value
\$PARENT_CUSTOM_FIELD5\$	Return the custom field field 5 value
\$PARENT_DOMAIN\$	Return the domain found in the parent configured credentials
\$PARENT_HOST\$	Return the host name if it's available (server name, ip address...)
\$PARENT_HOST_WITH_PORT\$	Return the host including the port if it's available
\$PARENT_INFORMATION_COMPANY\$	Return the information Company
\$PARENT_INFORMATION_EMAIL\$	Return the information email
\$PARENT_INFORMATION_MACHINE_NAME\$	Return the information machine name
\$PARENT_IP\$	Return the IP address.
\$PARENT_MAC\$	Return the MAC address defined
\$PARENT_MACRO_PASSWORD\$	Return the typing macro password
\$PARENT_NAME\$	Return the session name
\$PARENT_PASSWORD\$	Return the password from the parent configured credentials. It's only available when enabled in the parent advanced options
\$PARENT_PORT\$	Return the host port if it's available (server name, ip address...)
\$PARENT_SERIAL\$	Return the serial number in the invoice tab
\$PARENT_SERVICE_TAG\$	Return the service tag field located in the information tab
\$PARENT_SESSION_ID\$	Return the parent session id (guid)
\$PARENT_USERNAME\$	Return the user name from the parent configured credentials
\$PARENT_VIRTUAL_MACHINE_ID\$	Return the virtual machine ID

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.

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

Computer/Hardware

The following context will find any entry of the corresponding type, as long as it's in the hierarchy above you current entry. If there are multiple matches it takes the entry closest to the current entry.

Option	Description
\$COMPUTER_CUSTOM_FIELD1\$	Return the custom field field 1 value
\$COMPUTER_CUSTOM_FIELD2\$	Return the custom field field 2 value
\$COMPUTER_CUSTOM_FIELD3\$	Return the custom field field 3 value
\$COMPUTER_CUSTOM_FIELD4\$	Return the custom field field 4 value
\$COMPUTER_CUSTOM_FIELD5\$	Return the custom field field 5 value
\$COMPUTER_DOMAIN\$	Return the domain found in the configured credentials
\$COMPUTER_HOST\$	Return the host name if it's available (server name, ip address...)
\$COMPUTER_INFORMATION_COMPANY\$	Return the information Company
\$COMPUTER_INFORMATION_EMAIL\$	Return the information email
\$COMPUTER_INFORMATION_MACHINE_NAME\$	Return the information machine name
\$COMPUTER_IP\$	Return the IP Address
\$COMPUTER_MAC\$	Return the MAC address defined
\$COMPUTER_NAME\$	Return the session name
\$COMPUTER_SERIAL\$	Return the serial number in the invoice tab
\$COMPUTER_SERVICE_TAG\$	Return the service tag field located in the information tab
\$COMPUTER_VIRTUAL_MACHINE_ID\$	Return the virtual machine ID

Site

The following context will find any entry of the corresponding type, as long as it's in the hierarchy above you current entry. If there are multiple matches it takes the entry closest to the current entry.

Option	Description
\$SITE_CUSTOM_FIELD1\$	Return the custom field field 1 value
\$SITE_CUSTOM_FIELD2\$	Return the custom field field 2 value
\$SITE_CUSTOM_FIELD3\$	Return the custom field field 3 value
\$SITE_CUSTOM_FIELD4\$	Return the custom field field 4 value
\$SITE_CUSTOM_FIELD5\$	Return the custom field field 5 value
\$SITE_DOMAIN\$	Return the domain found in the configured credentials
\$SITE_INFORMATION_COMPANY\$	Return the information Company
\$SITE_INFORMATION_EMAIL\$	Return the information email
\$SITE_INFORMATION_MACHINE_NAME\$	Return the information machine name
\$SITE_NAME\$	Return the session name
\$SITE_SERIAL\$	Return the serial number in the invoice tab
\$SITE_SERVICE_TAG\$	Return the service tag field located in the information tab

\$SITE_VIRTUAL_MACHINE_ID\$	Return the virtual machine ID
-----------------------------	-------------------------------

Company

The following context will find any entry of the corresponding type, as long as it's in the hierarchy above you current entry. If there are multiple matches it takes the entry closest to the current entry.

Option	Description
\$COMPANY_CUSTOM_FIELD1\$	Return the custom field field 1 value
\$COMPANY_CUSTOM_FIELD2\$	Return the custom field field 2 value
\$COMPANY_CUSTOM_FIELD3\$	Return the custom field field 3 value
\$COMPANY_CUSTOM_FIELD4\$	Return the custom field field 4 value
\$COMPANY_CUSTOM_FIELD5\$	Return the custom field field 5 value
\$COMPANY_DOMAIN\$	Return the domain found in the configured credentials
\$COMPANY_INFORMATION_Company\$	Return the information Company
\$COMPANY_INFORMATION_EMAIL\$	Return the information email
\$COMPANY_INFORMATION_MACHINE_NAME\$	Return the information machine name
\$COMPANY_NAME\$	Return the session name
\$COMPANY_SERIAL\$	Return the serial number in the invoice tab
\$COMPANY_SERVICE_TAG\$	Return the service tag field located in the information tab
\$COMPANY_VIRTUAL_MACHINE_ID\$	Return the virtual machine ID

Domain

The following context will find any entry of the corresponding type, as long as it's in the hierarchy above you current entry. If there are multiple matches it takes the entry closest to the current entry.

Option	Description
\$DOMAIN_CUSTOM_FIELD1\$	Return the custom field field 1 value
\$DOMAIN_CUSTOM_FIELD2\$	Return the custom field field 2 value
\$DOMAIN_CUSTOM_FIELD3\$	Return the custom field field 3 value
\$DOMAIN_CUSTOM_FIELD4\$	Return the custom field field 4 value
\$DOMAIN_CUSTOM_FIELD5\$	Return the custom field field 5 value
\$DOMAIN_DOMAIN\$	Return the domain found in the configured credentials
\$DOMAIN_INFORMATION_COMPANY\$	Return the information Company
\$DOMAIN_INFORMATION_EMAIL\$	Return the information email
\$DOMAIN_INFORMATION_MACHINE_NAME\$	Return the information machine name
\$DOMAIN_NAME\$	Return the session name

\$DOMAIN_SERIAL\$	Return the serial number in the invoice tab
\$DOMAIN_SERVICE_TAG\$	Return the service tag field located in the information tab
\$DOMAIN_VIRTUAL_MACHINE_ID\$	Return the virtual machine ID

Customer

The following context will find any entry of the corresponding type, as long as it's in the hierarchy above you current entry. If there are multiple matches it takes the entry closest to the current entry.

Option	Description
\$CUSTOMER_CUSTOM_FIELD1\$	Return the custom field field 1 value
\$CUSTOMER_CUSTOM_FIELD2\$	Return the custom field field 2 value
\$CUSTOMER_CUSTOM_FIELD3\$	Return the custom field field 3 value
\$CUSTOMER_CUSTOM_FIELD4\$	Return the custom field field 4 value
\$CUSTOMER_CUSTOM_FIELD5\$	Return the custom field field 5 value
\$CUSTOMER_DOMAIN\$	Return the domain found in the configured credentials
\$CUSTOMER_INFORMATION_COMPANY\$	Return the information Company
\$CUSTOMER_INFORMATION_EMAIL\$	Return the information email
\$CUSTOMER_INFORMATION_MACHINE_NAME\$	Return the information machine name
\$CUSTOMER_NAME\$	Return the session name
\$CUSTOMER_SERIAL\$	Return the serial number in the invoice tab
\$CUSTOMER_SERVICE_TAG\$	Return the service tag field located in the information tab
\$CUSTOMER_VIRTUAL_MACHINE_ID\$	Return the virtual machine ID

Identity

The following context will find any entry of the corresponding type, as long as it's in the hierarchy above you current entry. If there are multiple matches it takes the entry closest to the current entry.

Option	Description
\$IDENTITY_CUSTOM_FIELD1\$	Return the custom field field 1 value
\$IDENTITY_CUSTOM_FIELD2\$	Return the custom field field 2 value
\$IDENTITY_CUSTOM_FIELD3\$	Return the custom field field 3 value
\$IDENTITY_CUSTOM_FIELD4\$	Return the custom field field 4 value
\$IDENTITY_CUSTOM_FIELD5\$	Return the custom field field 5 value
\$IDENTITY_DOMAIN\$	Return the domain found in the configured credentials
\$IDENTITY_INFORMATION_COMPANY\$	Return the information Company
\$IDENTITY_INFORMATION_EMAIL\$	Return the information email

\$IDENTITY_INFORMATION_MACHINE_NAME\$	Return the information machine name
\$IDENTITY_NAME\$	Return the session name
\$IDENTITY_SERIAL\$	Return the serial number in the invoice tab
\$IDENTITY_SERVICE_TAG\$	Return the service tag field located in the information tab
\$IDENTITY_VIRTUAL_MACHINE_ID\$	Return the virtual machine ID

Database

The following context will find any entry of the corresponding type, as long as it's in the hierarchy above you current entry. If there are multiple matches it takes the entry closest to the current entry.

Option	Description
\$DB_CUSTOM_FIELD1\$	Return the custom field field 1 value
\$DB_CUSTOM_FIELD2\$	Return the custom field field 2 value
\$DB_CUSTOM_FIELD3\$	Return the custom field field 3 value
\$DB_CUSTOM_FIELD4\$	Return the custom field field 4 value
\$DB_CUSTOM_FIELD5\$	Return the custom field field 5 value
\$DB_DOMAIN\$	Return the domain found in the configured credentials
\$DB_INFORMATION_COMPANY\$	Return the information Company
\$DB_INFORMATION_EMAIL\$	Return the information email
\$DB_INFORMATION_MACHINE_NAME\$	Return the information machine name
\$DB_NAME\$	Return the session name
\$DB_SERIAL\$	Return the serial number in the invoice tab
\$DB_SERVICE_TAG\$	Return the service tag field located in the information tab
\$DB_VIRTUAL_MACHINE_ID\$	Return the virtual machine ID

Custom fields

Custom fields can contain any data you require and can be accessed using the `*_CUSTOM_FIELD*` variables. Please refer to [Custom Fields](#) for details.

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 in templates.

3.5 View

3.5.1 Panels

Description

That section of the ribbon controls the state of the Navigation pane.



Panels section of the View tab

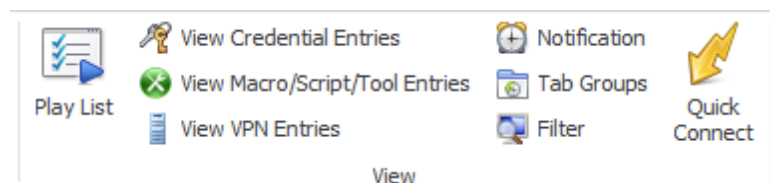
Refer to the following topics for more information:

- [All Entries](#)
- [Private Vault](#)
- [Opened Sessions](#)
- [Favorite Entries](#)
- [Most Recently Used Entries](#)
- [Application Tools](#)
- [ToDo List](#)

3.5.2 View

Description

The view section allows access to specialized screens that show only a subset of your entries. These are useful mainly for installations with a great number of entries.



View section of the View tab

Refer to the following topics for more information:

- [Play List](#)
- [Use Credential Entries](#)
- [Use VPN Entries](#)
- [Tab Groups](#)
- [Search/Filter](#)
- [Quick Access Toolbar](#)

3.5.3 Logs

3.5.3.1 Usage Logs (Local)

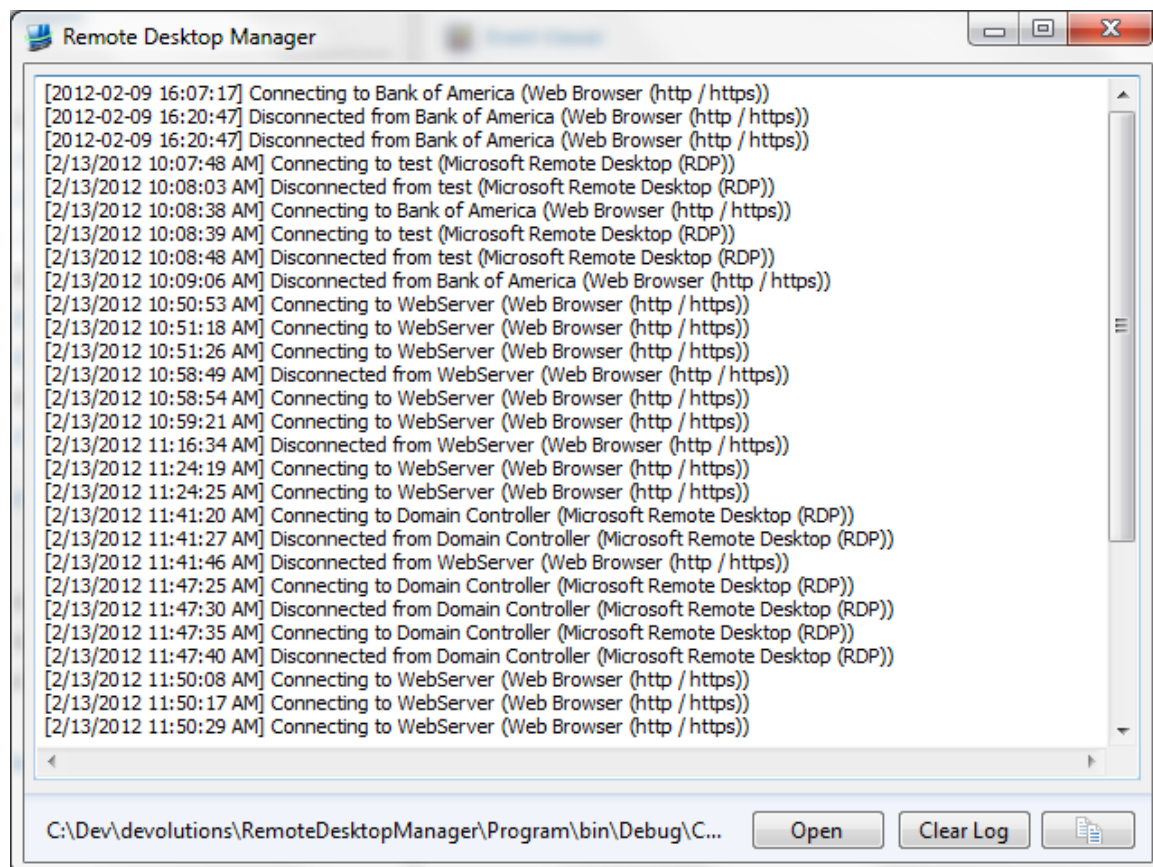
Description

Remote Desktop Manager supports two types of logs:

- Local usage log, which is file based
- [Global usage log](#), in a database

Local Session Log

A basic local logging system is automatically available by default. This allows the system administrator to view the log file for all session activities on the current machine. It's available on the local machine only via the menu **View Local Connection Log**.



Local connection log

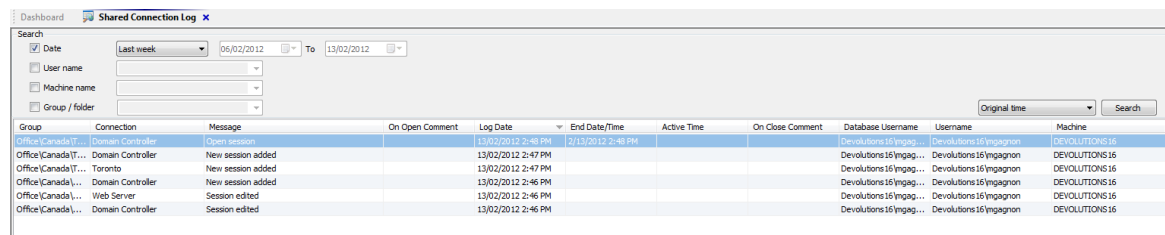
The log is written directly to a file in the settings folder.

3.5.3.2 Usage Logs (Global)

Description

The shared session log offers a more robust solution. Through it, it's possible to monitor an opened session for all users by using the SQL Server, or the Remote Desktop Manager Online data source. The log is available for a specific session in the context menu **View->Logs**, in the session configuration (Log tab page), and in the dashboard.

The log contains all the CRUD (add, edit and delete) operations, including the time and the username. It also contains all the details about the open/closed sessions, including those from the VPN.



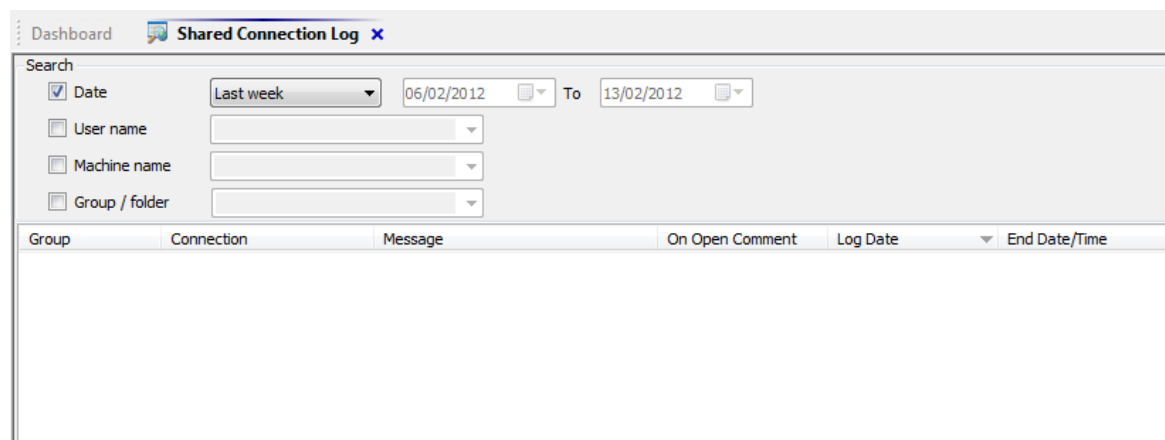
Group	Connection	Message	On Open Comment	Log Date	End Date/Time	Active Time	On Close Comment	Database Username	Username	Machine
Office/Canada(T...	Domain Controller	Open session		13/02/2012 2:46 PM	2/13/2012 2:46 PM			Devolutions 16/ingag...	Devolutions 16/ingagnon	DEVOLUTIONS 16
Office/Canada(T...	Domain Controller	New session added		13/02/2012 2:47 PM				Devolutions 16/ingag...	Devolutions 16/ingagnon	DEVOLUTIONS 16
Office/Canada(T...	Toronto	New session added		13/02/2012 2:47 PM				Devolutions 16/ingag...	Devolutions 16/ingagnon	DEVOLUTIONS 16
Office/Canada(T...	Domain Controller	New session added		13/02/2012 2:46 PM				Devolutions 16/ingag...	Devolutions 16/ingagnon	DEVOLUTIONS 16
Office/Canada(T...	Web Server	Session edited		13/02/2012 2:46 PM				Devolutions 16/ingag...	Devolutions 16/ingagnon	DEVOLUTIONS 16
Office/Canada(T...	Domain Controller	Session edited		13/02/2012 2:46 PM				Devolutions 16/ingag...	Devolutions 16/ingagnon	DEVOLUTIONS 16

Session logs

It's also possible to view in real time who is connected by ticking the checkbox "Show live session only." This will filter the list to display only the opened sessions in the grid.

The session log can be visualized in a global view by using the shared connection log (**View Shared Connection Log**). Use this view to find information for multiple sessions for a specific time, or for a specific user. The window is similar to a search tool and it offers multiple filter types, including:

- User name
- Machine name
- Time period



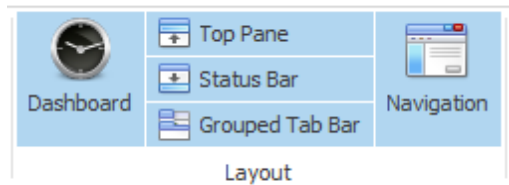
Group	Connection	Message	On Open Comment	Log Date	End Date/Time	Active Time	On Close Comment	Database Username	Username	Machine
Office/Canada(T...	Domain Controller	Open session		13/02/2012 2:46 PM	2/13/2012 2:46 PM			Devolutions 16/ingag...	Devolutions 16/ingagnon	DEVOLUTIONS 16
Office/Canada(T...	Domain Controller	New session added		13/02/2012 2:47 PM				Devolutions 16/ingag...	Devolutions 16/ingagnon	DEVOLUTIONS 16
Office/Canada(T...	Toronto	New session added		13/02/2012 2:47 PM				Devolutions 16/ingag...	Devolutions 16/ingagnon	DEVOLUTIONS 16
Office/Canada(T...	Domain Controller	New session added		13/02/2012 2:46 PM				Devolutions 16/ingag...	Devolutions 16/ingagnon	DEVOLUTIONS 16
Office/Canada(T...	Web Server	Session edited		13/02/2012 2:46 PM				Devolutions 16/ingag...	Devolutions 16/ingagnon	DEVOLUTIONS 16
Office/Canada(T...	Domain Controller	Session edited		13/02/2012 2:46 PM				Devolutions 16/ingag...	Devolutions 16/ingagnon	DEVOLUTIONS 16

Shared connection log panel

3.5.4 Layout

Description

The Layout section holds commands to control the layout of various Remote Desktop Manager components.



Layout section of the View tab

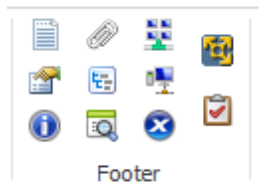


If you hide the Top Pane, you have two ways of restoring it. Either in the system menu (see [Top Pane](#)) or by using the keyboard shortcut for toggling its visibility. ALT-F11 by default.

3.5.5 Footer

Description

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



Footer Section of the View Tab



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

3.5.6 Play List

Description

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

The Play List can be used to create groups of sessions for a specific tasks or for security reasons.

You can build your own Play Lists and start all entries from a Play List at the same time.

For more information, please consult topics:

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

3.5.6.1 Actions

Description

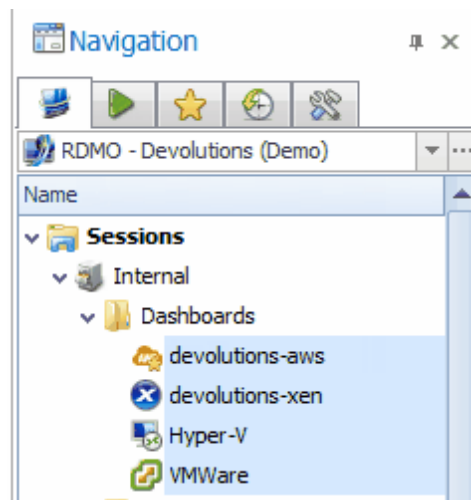
Here are the 4 methods to create or edit a Play List:

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

Settings

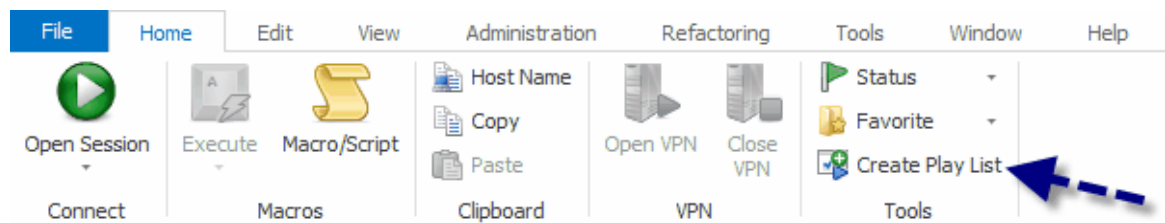
Create Play List by selecting entries in the Navigation Pane

Select the entries in the Navigation Pane.



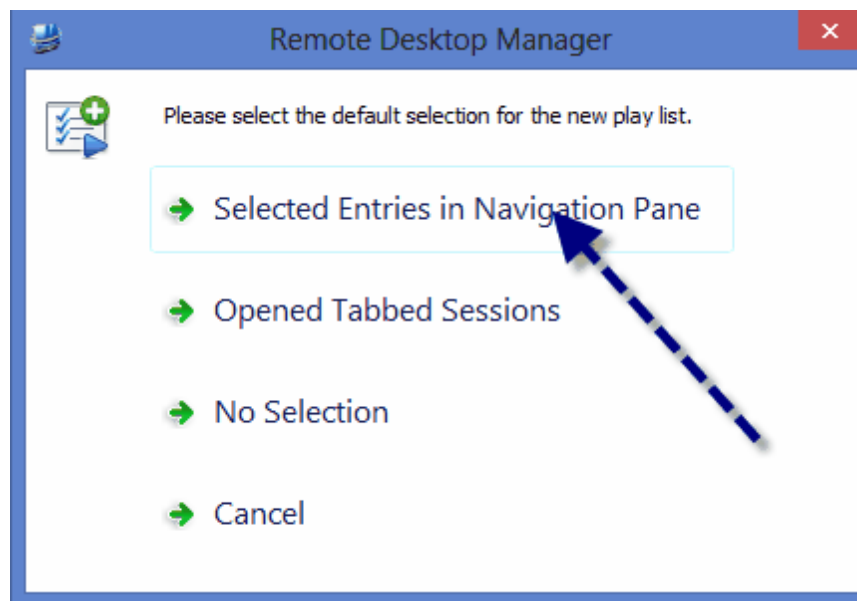
Selected Entries

Click **Create Play List** in the Ribbon Menu.



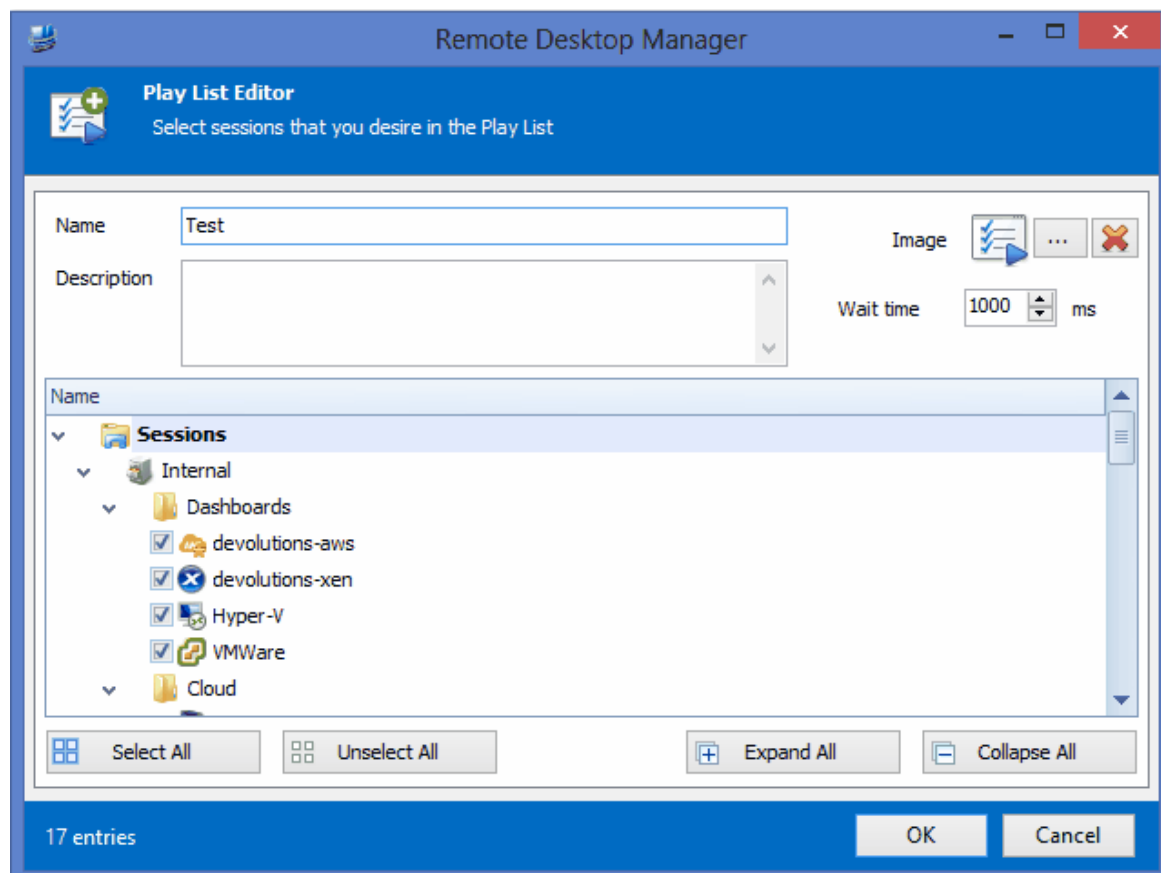
Ribbon Menu

Click **Select Entries in Navigation Pane**.



Selected Entries in Navigation Pane

Provide a name to your Play List and click **OK**.



Play List Editor



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

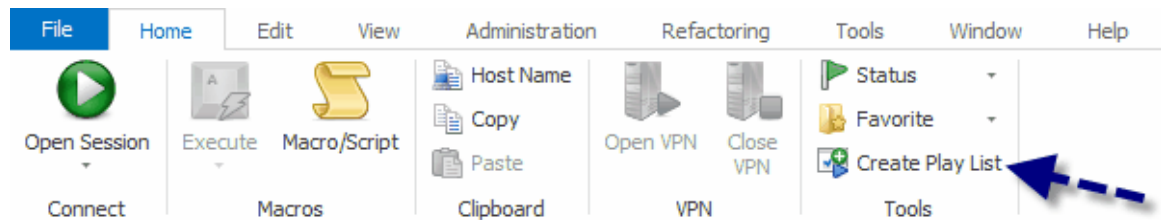


The wait time is used to set the delay between opening of the different entries.

Create Play List with Opened Tabbed Sessions

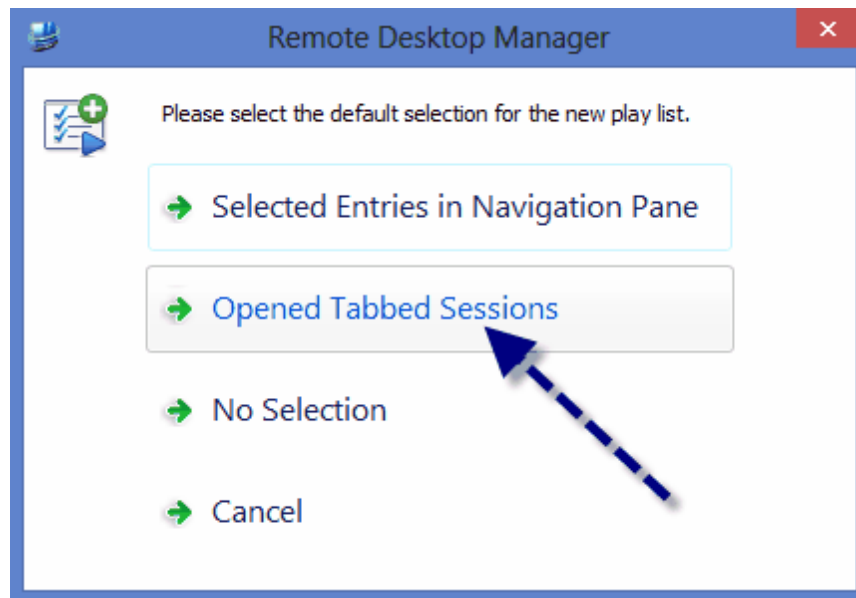
Open all the sessions that you want in your Play List in Embedded/Tabbed mode.

Click **Create Play List** in the Ribbon Menu.



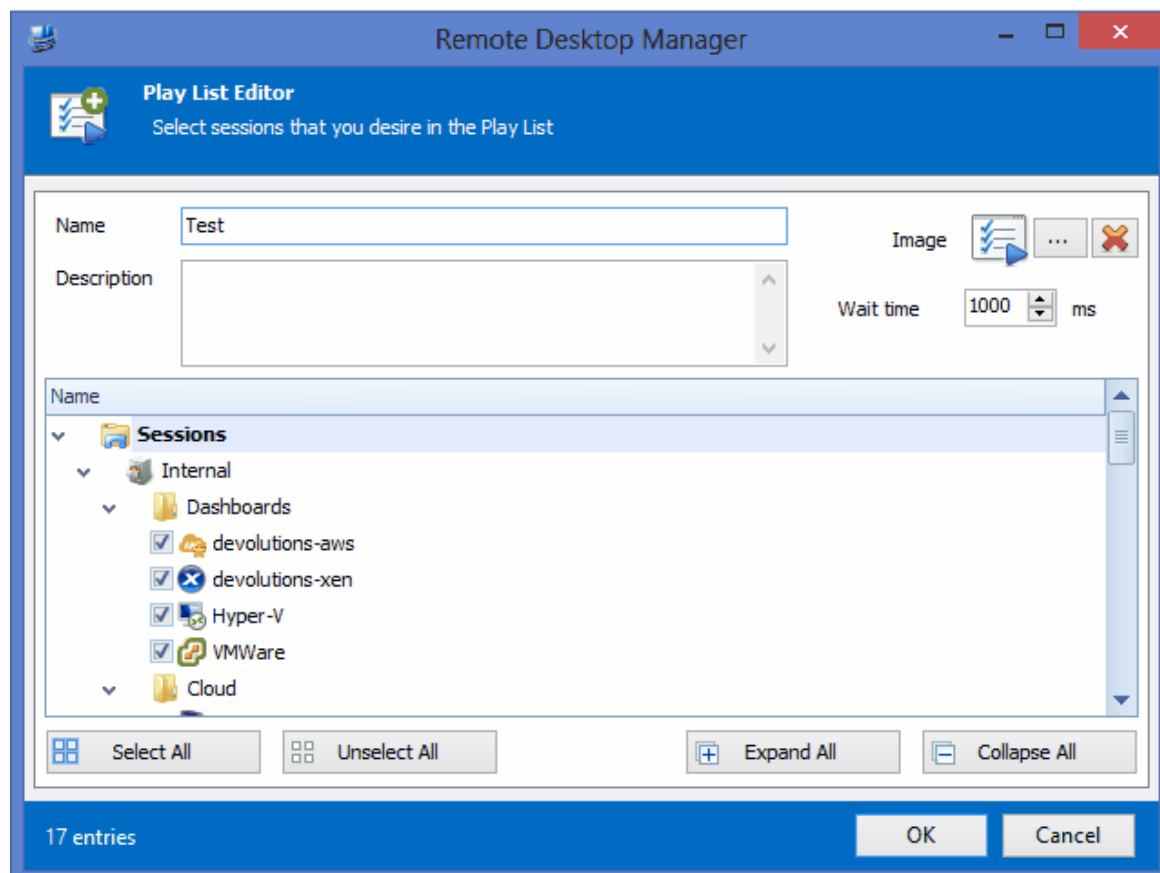
Ribbon Menu

Click **Opened Tabbed Sessions**.



Opened Tabbed Sessions

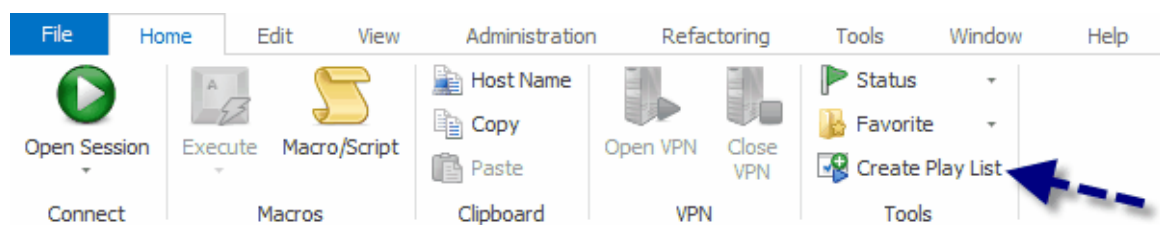
Provide a name to your Play List and click **OK**.



Play List Editor

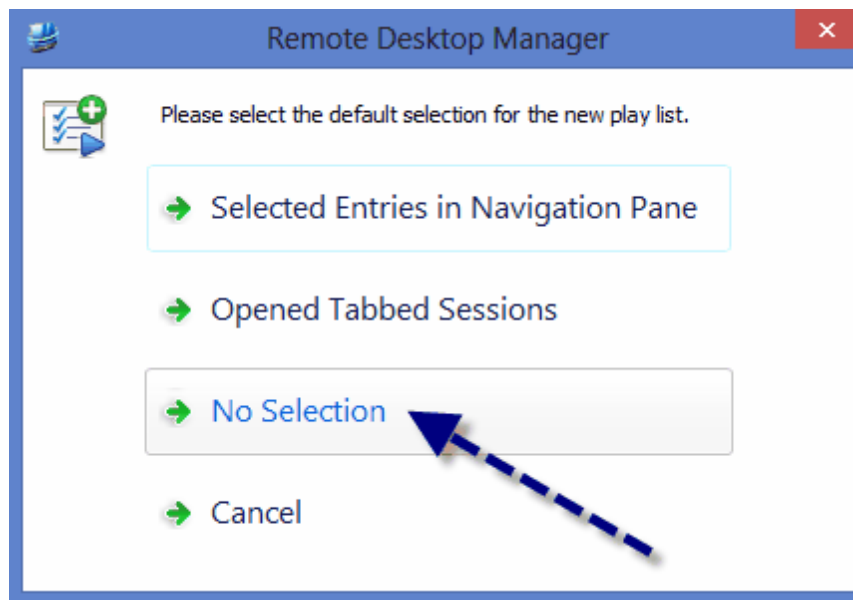
Create Play List with No Selection

Click **Create Play List** in the Ribbon Menu.



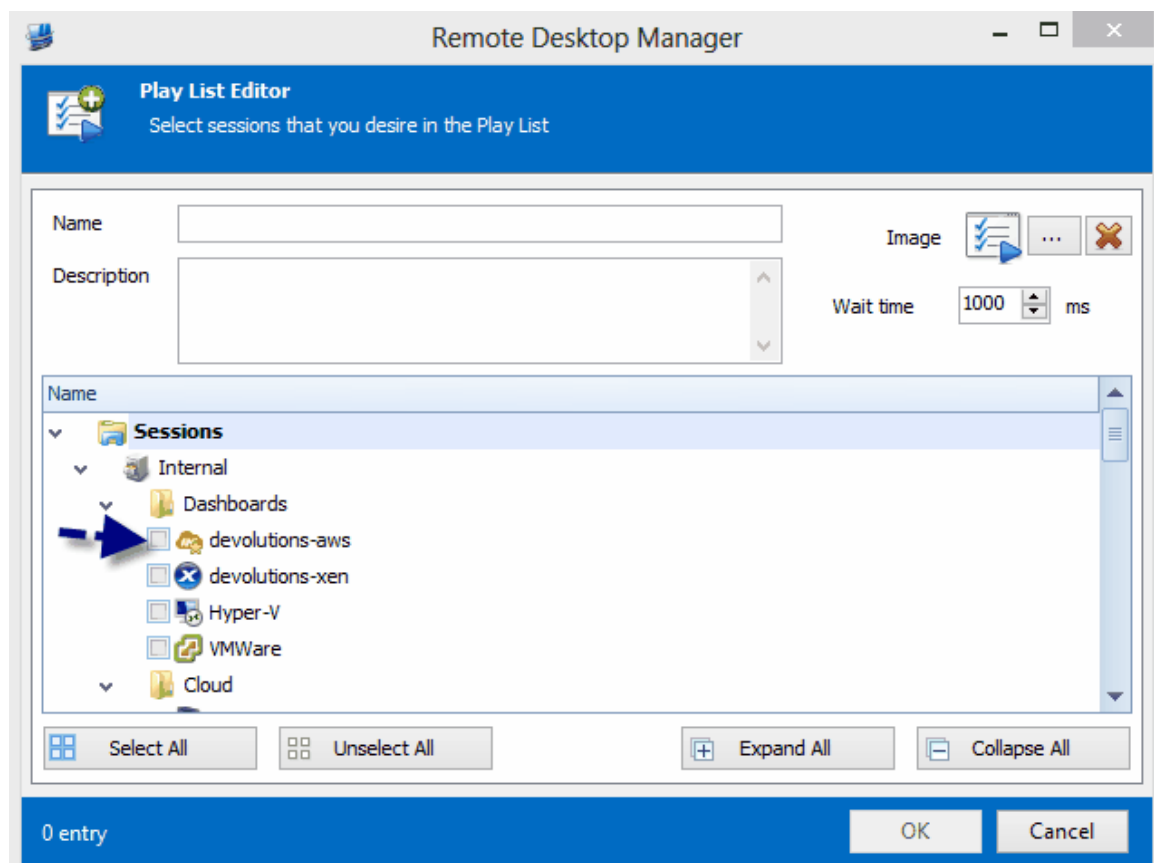
Ribbon Menu

Click **No Selection**.



No Selection

Select the entries wanted in your Play List by checking the box beside the entry name.

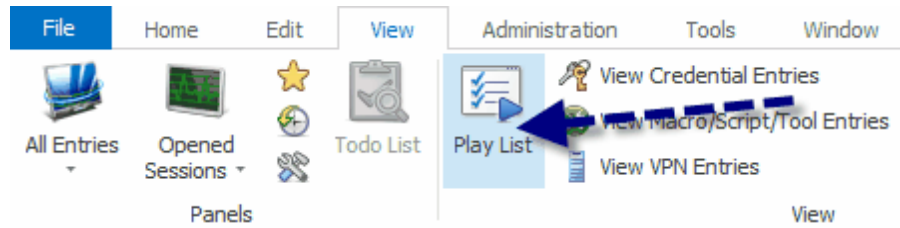


Play List Editor

Provide a name to your Play List and click **OK**.

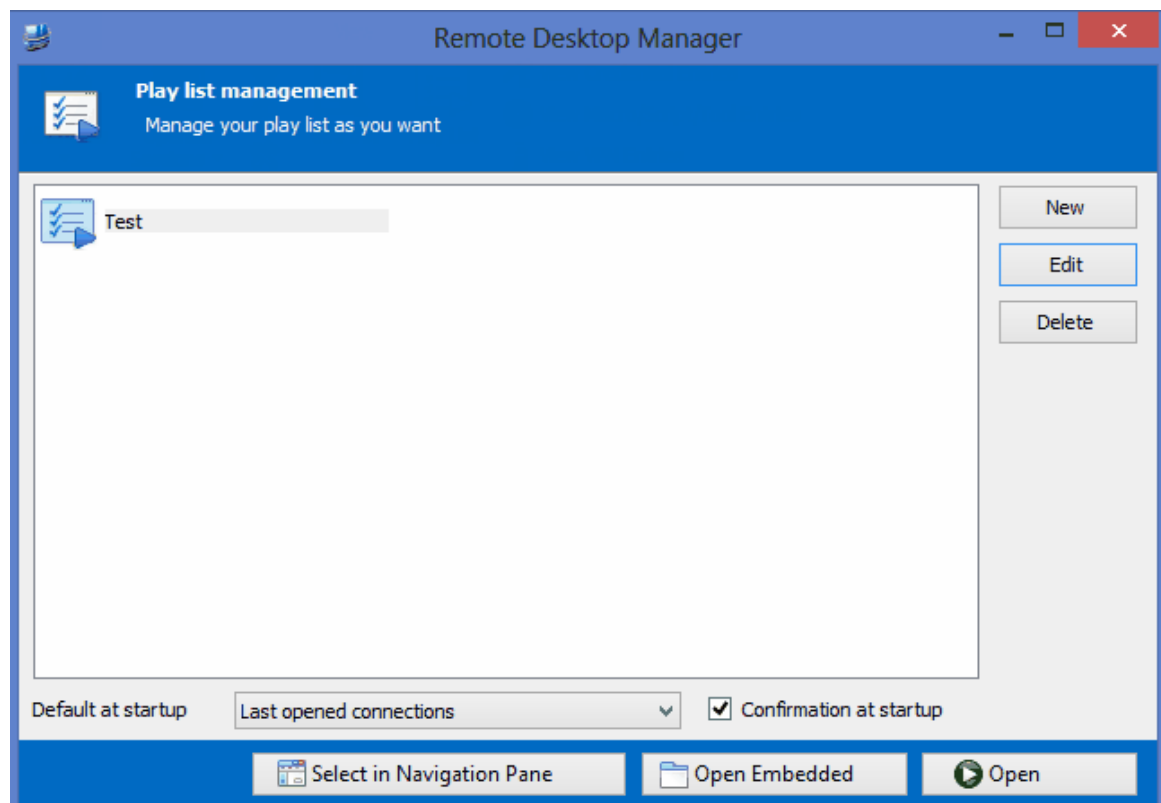
Edit a existing Play List

You can edit a Play List by clicking **View -> Play List**.



View - Play List

You will now be able to edit a Play List.



Play List Management



You can also use the context menu to add an entry to an existing **Play List**. When your entry is selected, **right-click** on it in the Navigation Pane and select **Play List -> Add to Play List**.

3.5.6.2 Management

Description

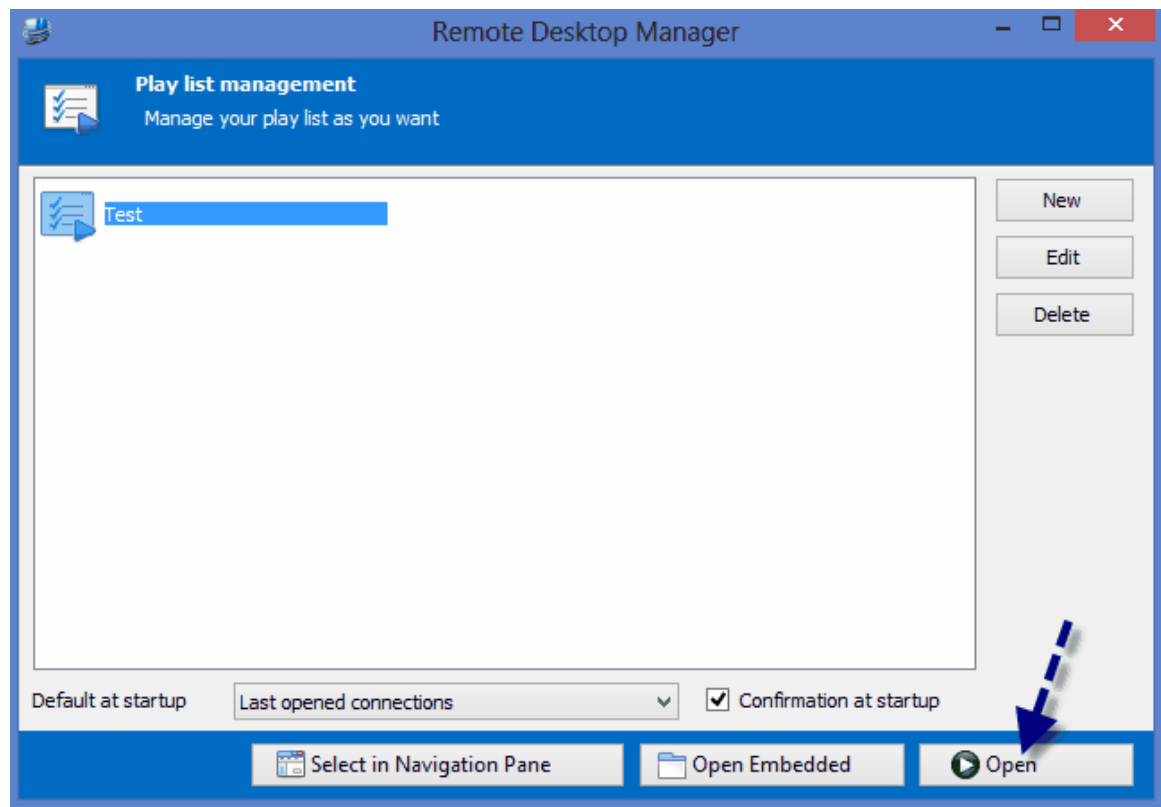
There's 3 methods to use a Play List:

Option	Description
Open	Items will open using the mode defined in each session.
Open Embedded	Items will be all opened using the embedded mode
Select in Navigation Pane	Items will be selected in the Navigation Pane, this allows you to choose another command to run on the section as a second step.

Settings

Open items in default mode

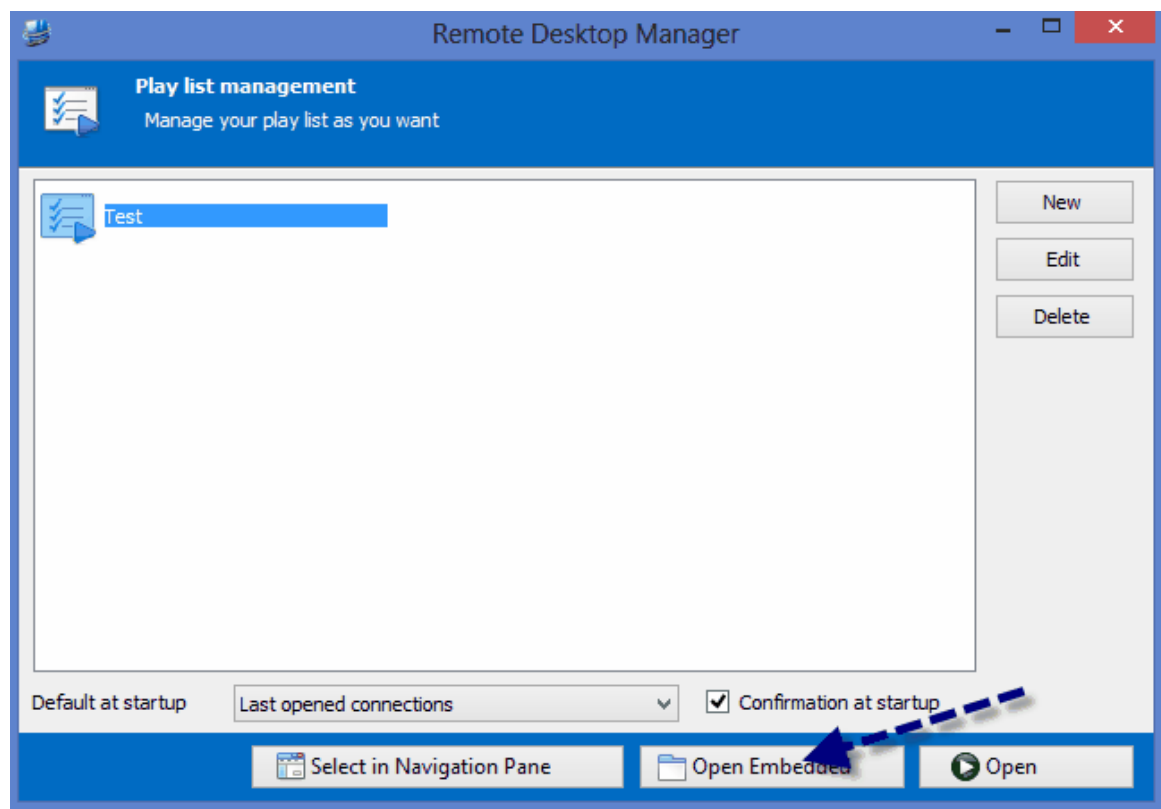
Click **View -> Play List -> Select your Play List -> Open**



Default Mode

Open items in Embedded mode

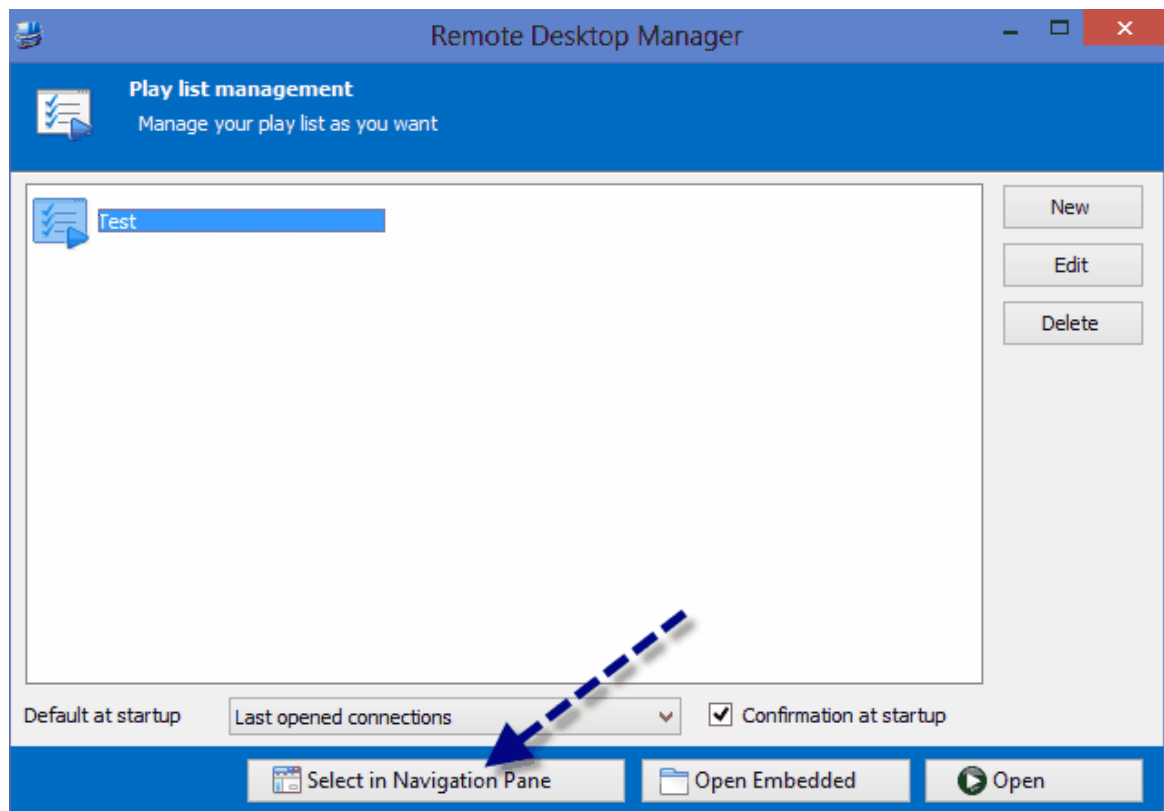
Click **View -> Play List -> Select your Play List -> Open Embedded**



Open Embedded

Open items with Select in Navigation Pane

Click **View -> Play List -> Select your Play List -> Select in Navigation Pane**



Select in Navigation Pane

Then press **Enter** to select the entries.

3.5.6.3 Default at Startup

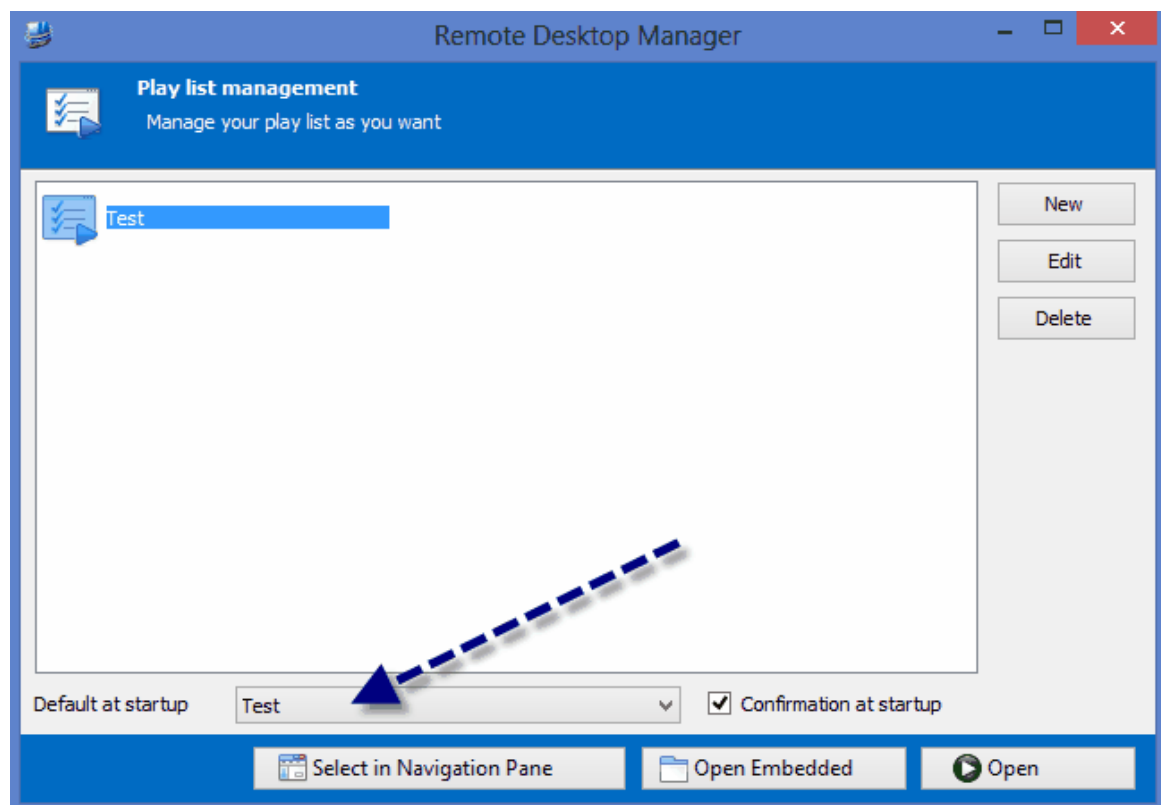
Description

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

Settings

Default Play List at startup

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



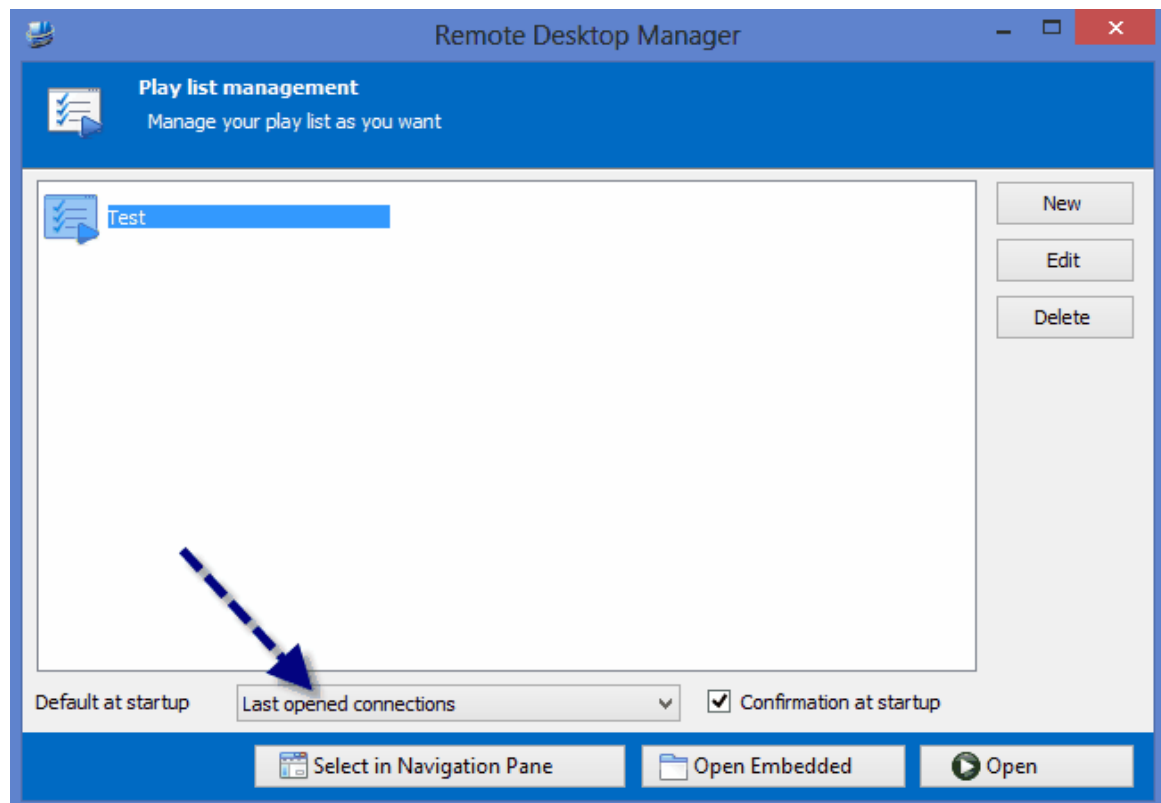
Default at startup



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

Last opened connections at startup

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



Last opened connections

3.5.7 ToDo List

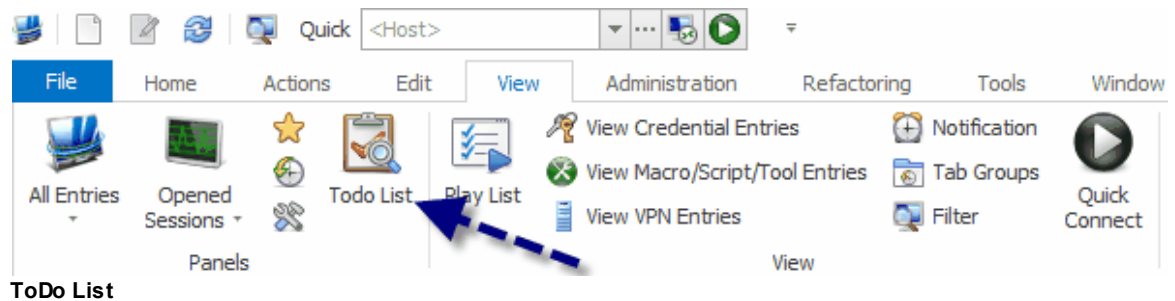
3.5.7.1 Actions

Description

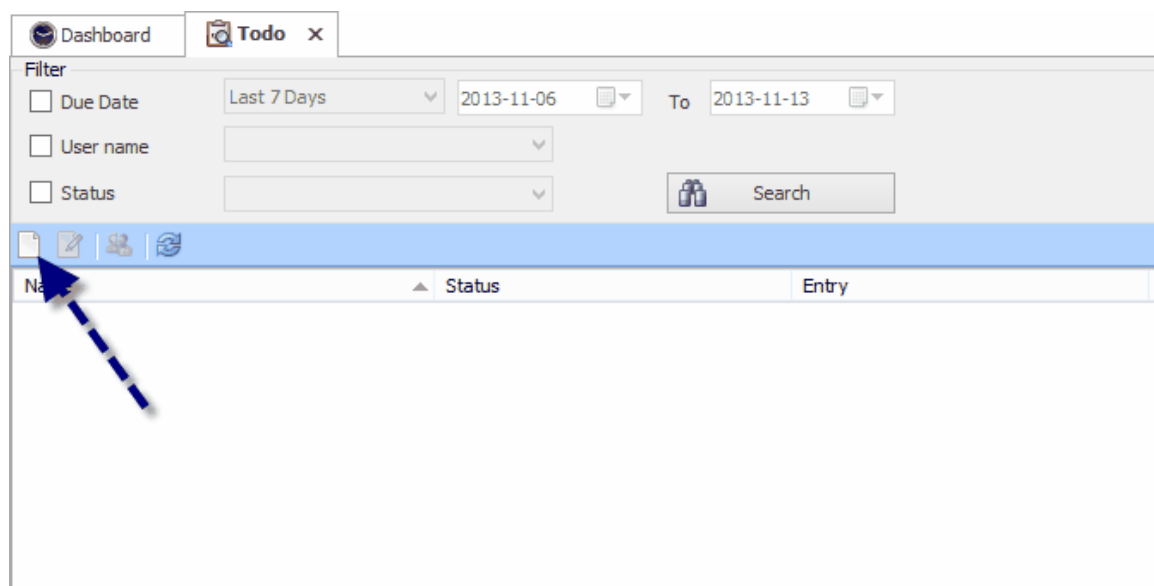
Create tasks in the ToDo List to help you follow what work needs to be performed by your staff.

Creation of a task

Click **ToDo List** in the View menu of the ribbon

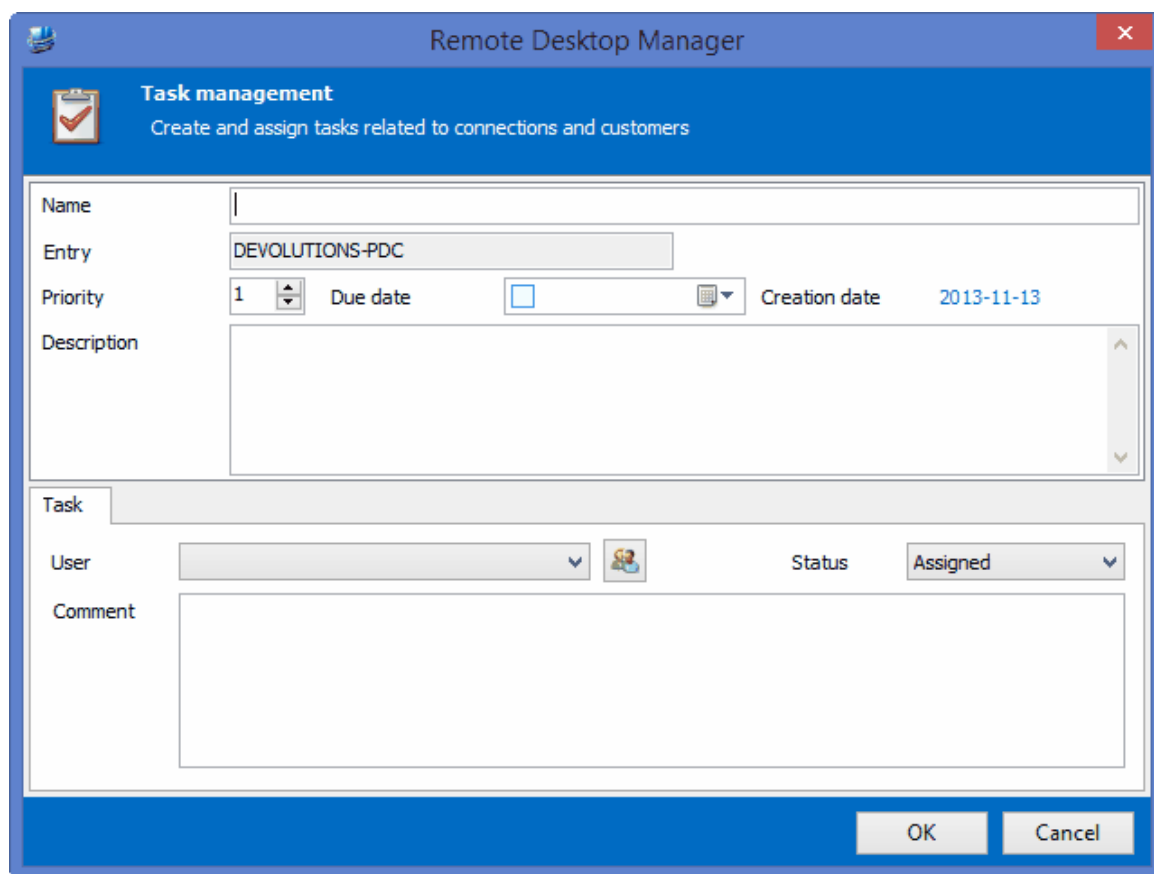


Click **Add new Todo**



Add new todo

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



Task Management



Tasks can be assigned to a user.

Assign Me

You can use the Assign to Me button , to set your identity instantly.

Status

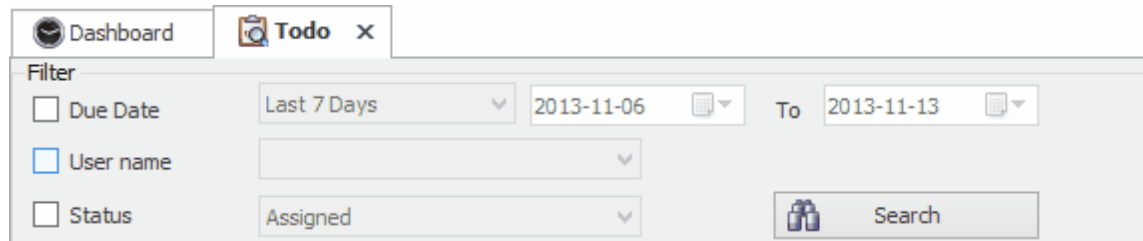
Different statuses can be applied to a task:

- Assigned
- Canceled
- Closed
- Done
- In progress
- Open
- Postponed

3.5.7.2 Search

Description

When many tasks are created in Remote Desktop Manager, perform a search to filter our the list of displayed tasks. You can search by Due Date, User name or by Status



Search Filter

3.5.7.3 Export

Description

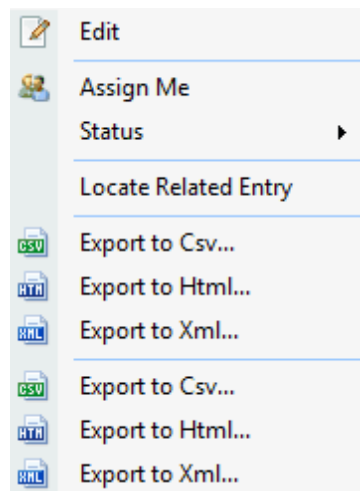
Tasks can be exported in different types of files for print or only for review.

How to export tasks



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

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



Export options

Export file type

You can export tasks in these file formats

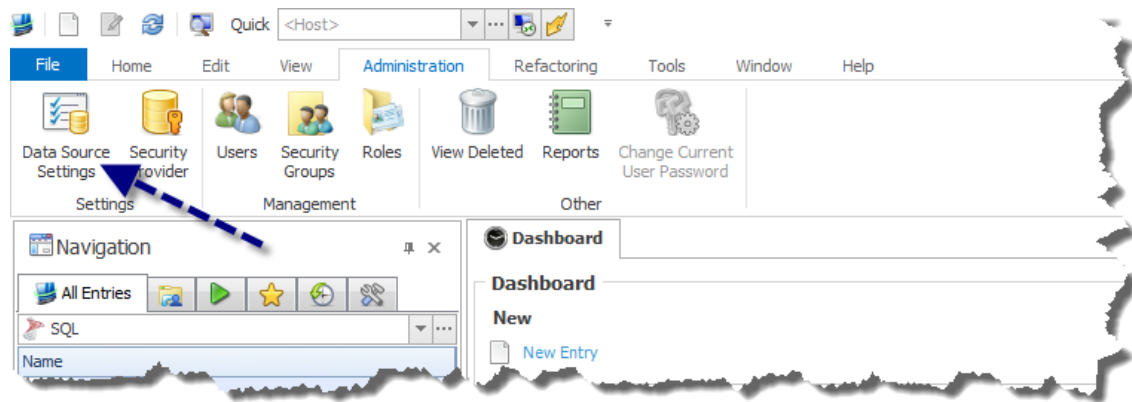
- CSV
- HTML
- XML

3.6 Administration

3.6.1 Data Source Settings

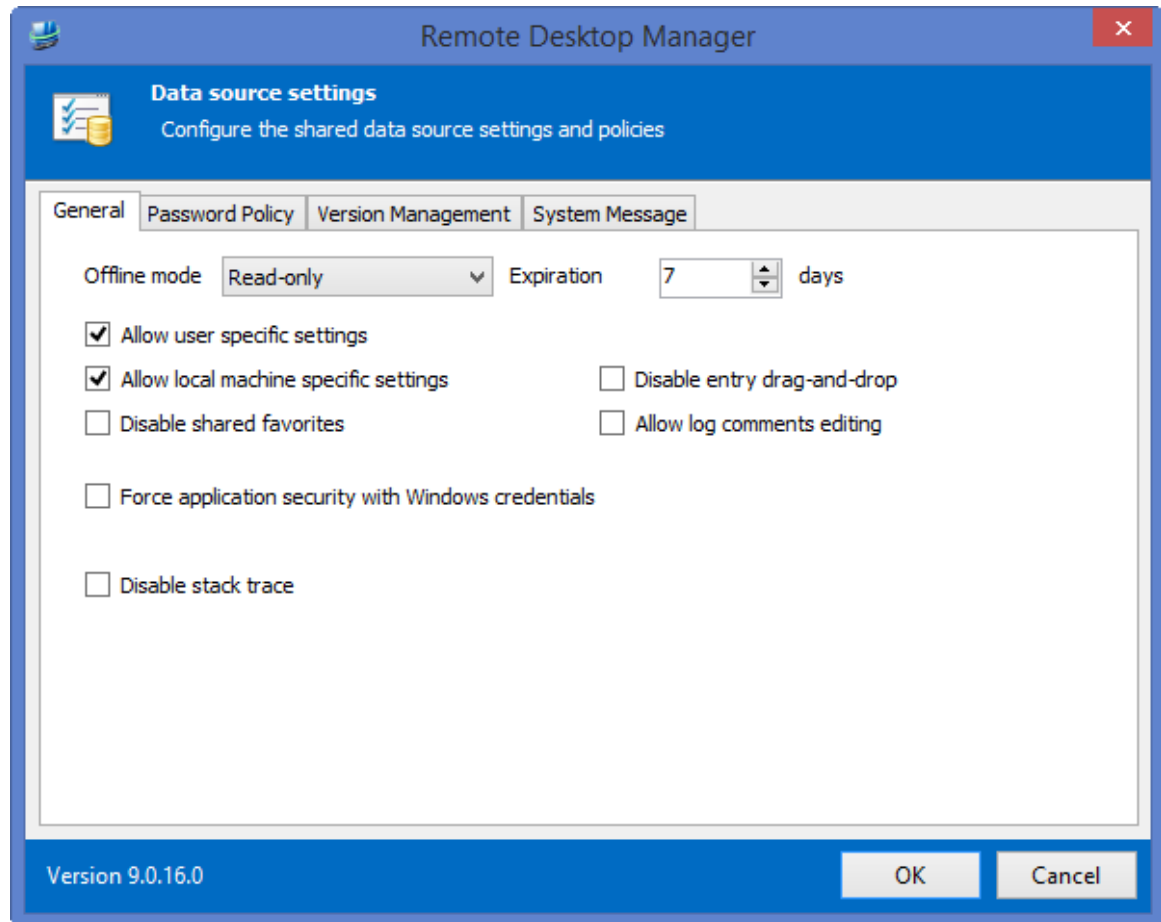
Description

Data source settings allows you to control many global aspects of the data source. Settings like Offline Mode, password policies & version management are available. You define general policies applicable for the whole data source. This feature is accessible from **Administration -> Data Source Settings**.



Data Source Settings

General

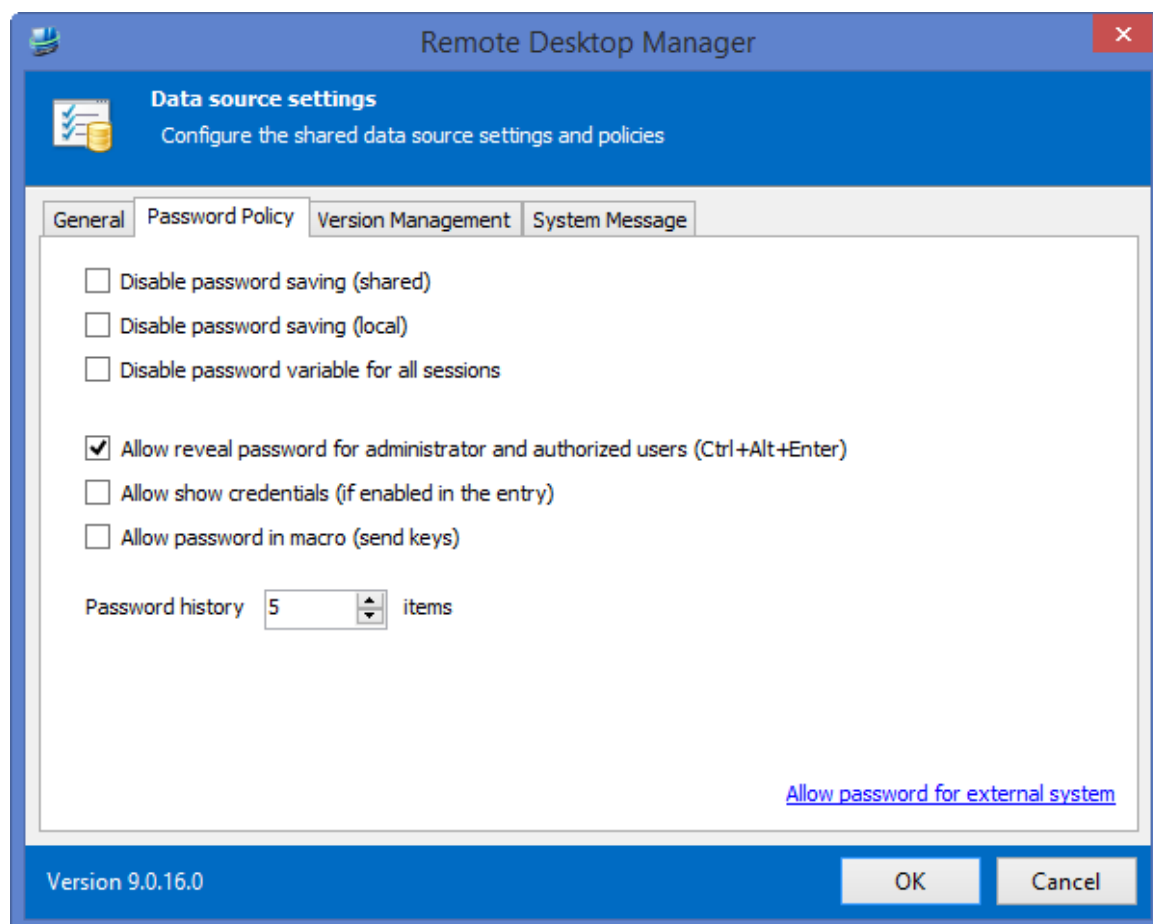


General tab

Option	Description
Offline mode	Set the global data source support for Offline Mode. Useful when using a VPN connection that makes using local network impossible.
Expiration	Number of days that the local copy will be considered valid for the offline cache. You should go online prior to the end of that period to revalidate the data.
Allow user specific settings	Enables the use of user specific settings. See User Specific Settings for more information.
Allow local machine specific settings	Enables the use of local machine specific settings. See Local Machine Specific Settings for more information.
Disable shared favorites	Disable the shared favorites and make them invisible for all users of the data source.
Force application security with Windows credentials	Require the users to authenticate with their Windows credentials at application startup.
Disable stack trace	Disable the stack trace details when an error appears during the execution of the application.

Disable entry drag-and-drop	Entry group modification using the drag and drop will be disabled. Use this setting to avoid accidental drag and drop.
Allow log comments editing	Enable the log comment editing for all the users.

Password Policy

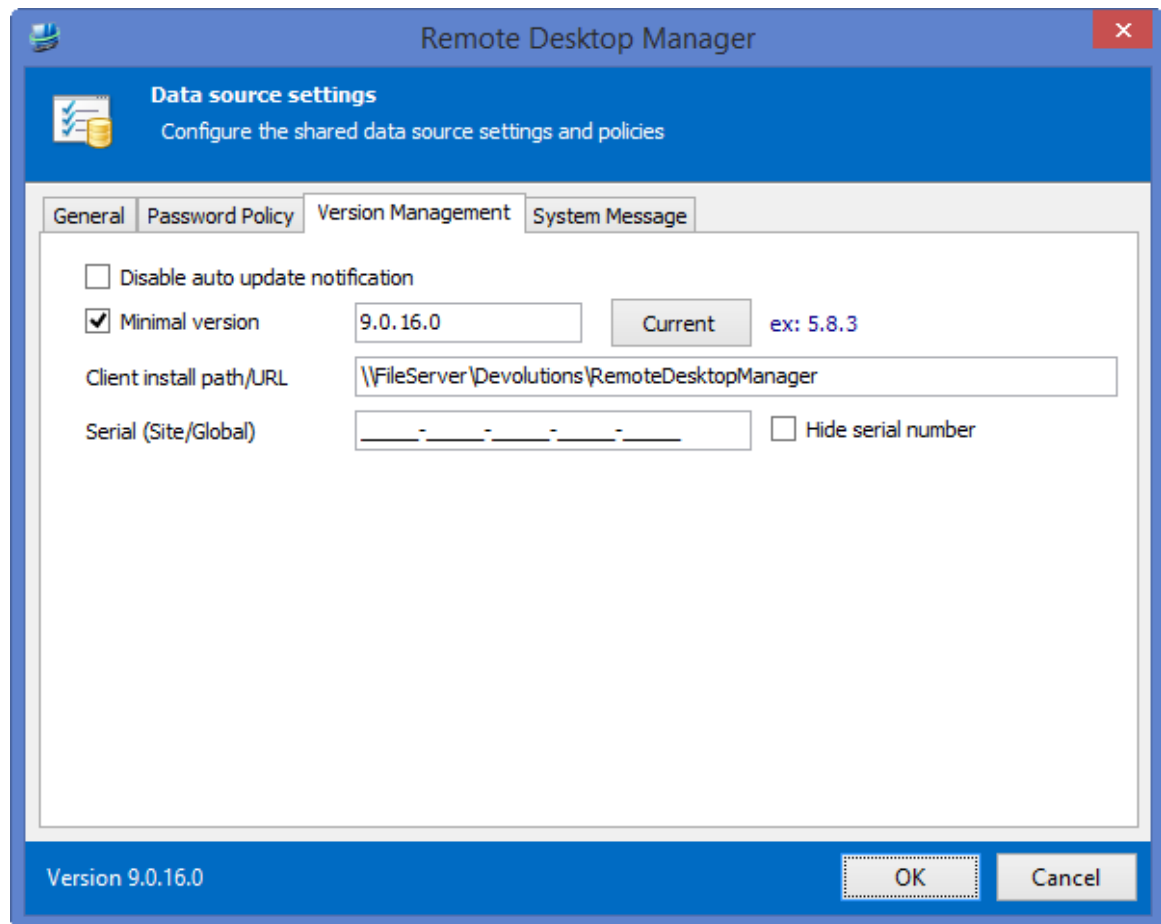


Password Policy tab

Option	Description
Disable password saving (shared)	Users will not be able to save passwords within session.
Disable password saving (local)	Users will not be able to save passwords using Windows credential vault. This is mostly used for the RDP sessions.
Disable password variable for all sessions	Renders \$PASSWORD\$ variable unusable for this data source.
Allow reveal password for administrator and authorized users (Ctrl+Alt+Enter)	Controls if reveal password is enabled for authorized users.
Allow copy password in clipboard (if enabled in the session)	Enables copy password when it's enabled in the session.
Allow password in macro (send keys)	Renders \$MACRO_PASSWORD\$ variable useless for this data source.

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

Version Management

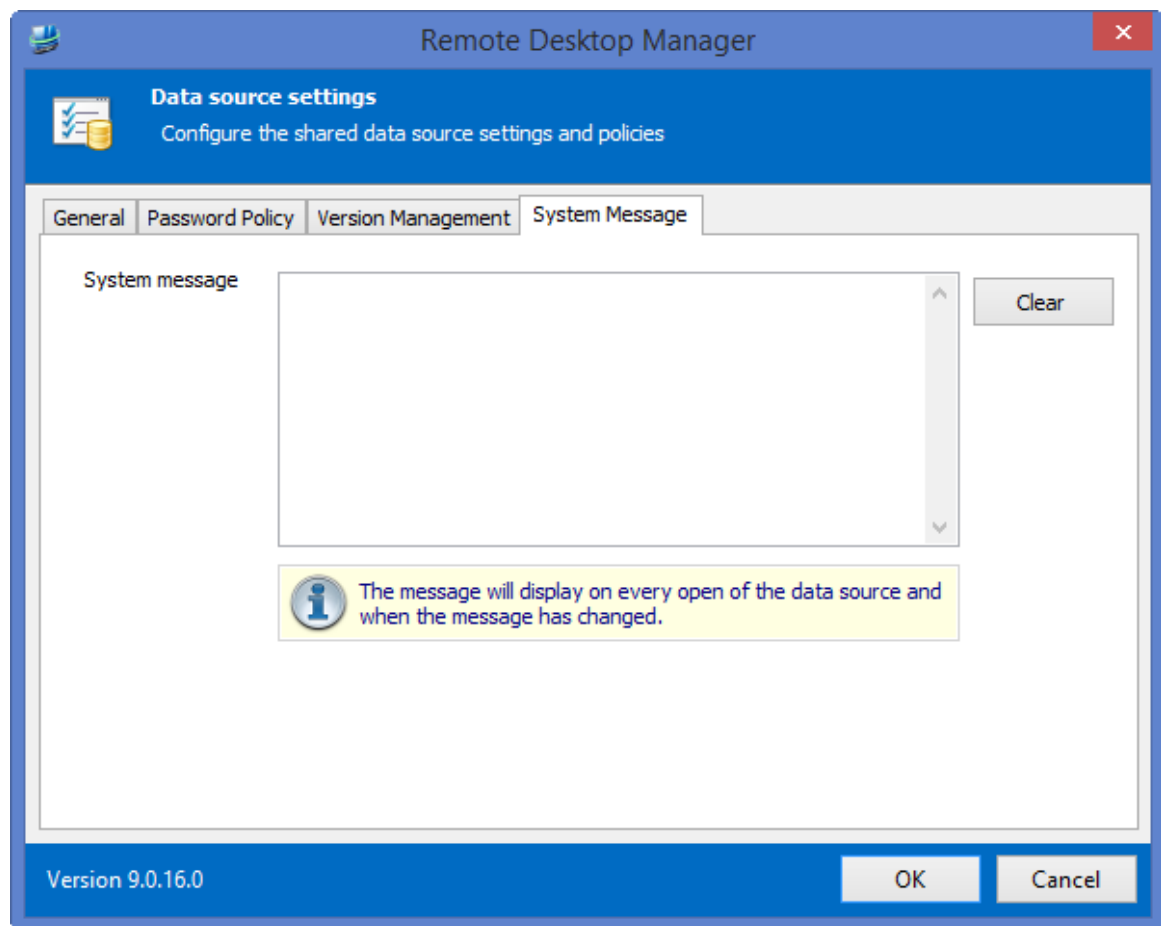


Version Management tab

Option	Description
Disable auto update notification	Disable the auto update notification message. Use this when you want to manually update the application.
Minimal version	Force users of the data source to use a minimal version. Enter the entire version number (7.9.10.0) to force a specific version or use partial number for force a subset version (7.9). Use this to disable connecting to the data source with an older version.
Client install path/URL	Used in conjunction with the minimal version, once a minimal version requirement is not met the system will prompt the user that the version is not valid and it will open the link (path/URL) to download the new version.
Serial (Site/Global)	Easily distribute Site/Global serials to the entire organization. The application is updated with the license if it's newer then the registered one.

Hide serial number	The serial number will be hidden by default for all users connected to the data source.
--------------------	---

System Message



System Message tab

Option	Description
System message	The message will be displayed every time the data source is opened or when the message changes. Use Ctrl+ENTER to create a new line.

3.6.2 Security Providers

Description

The security provider is responsible for encrypting the data in the database. It's available with an [Advanced Data Source](#) only.

Select the provider you wish, and configure it by using the menu **Administration -> Security Provider**.



Regardless of the security provider you select, the password is encrypted at least once in the database. There is no password stored in clear text at any time.

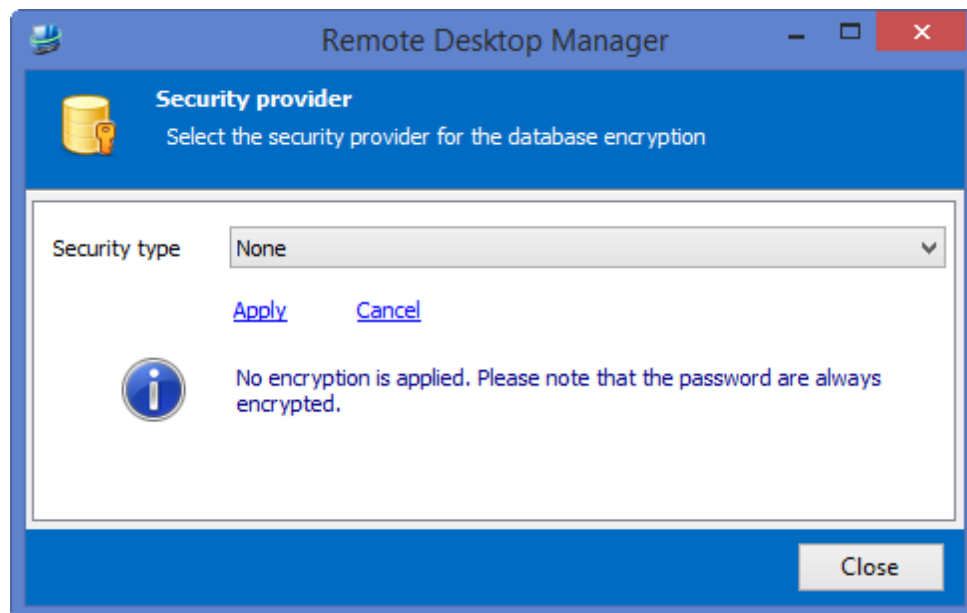
Settings



Please note that changing a security provider when many sessions have previously been configured may take a bit of time.



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



Security provider dialog

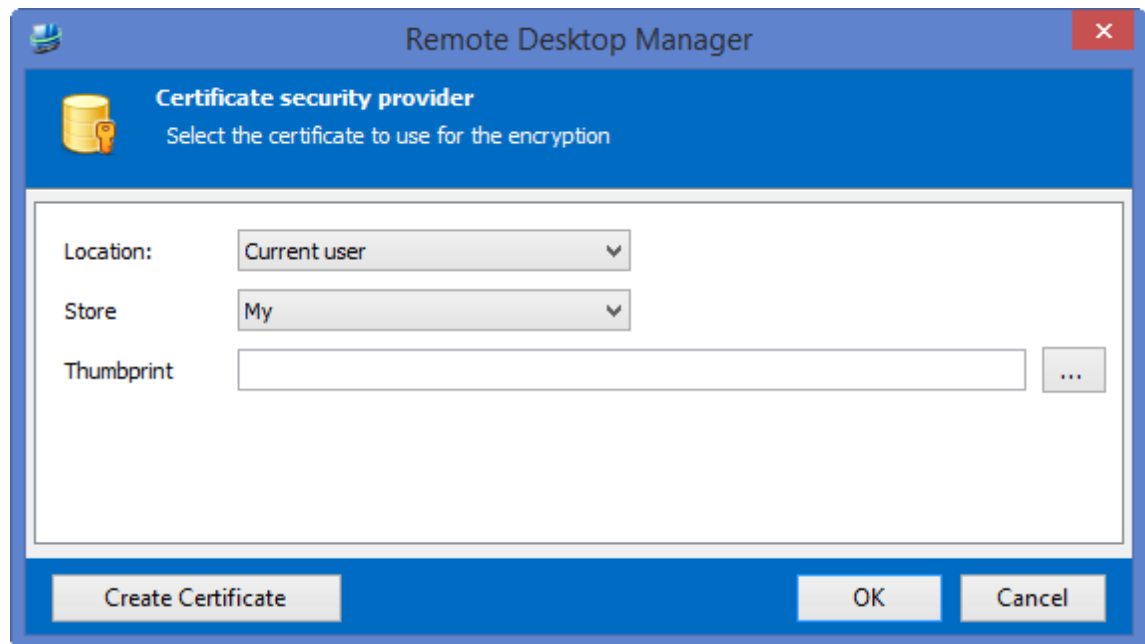
Option	Description
None	The session data is not encrypted at all except for the passwords.
Basic	All of the data is encrypted in the database with our own private key and it's impossible for an external system to access it.
Default	This is the legacy security provider. The data is encrypted if the session configuration is set accordingly to the advanced settings.
Shared passphrase	All of the data is encrypted with a mix of our key, a salt and the pass phrase you've entered. This is the most secure encryption, but if the pass phrase is lost, there is nothing that can do to recover the data.
Certificate	All data is encrypted using a certificate installed. See Certificate section for more details.



By using your own passphrase with any of the [Advanced Data Sources](#), you ensure that nobody can read your session, even when people have a direct access to your database(s) or even a backup. You should always use this when you use SQL Azure or Remote Desktop Manager Online.

Certificate

The certificate security provider encrypts the whole XML structure using AES with your certificate mixed with our own private key.



Certificate security provider

Option	Description
Location	Indicate the location of the certificate. Select between: <ul style="list-style-type: none">• Current user• Local machine
Store	Indicate the store location of the certificate. Select between: <ul style="list-style-type: none">• Address book• Authorization root• Certificate authority• Disallowed• My• Root• Trusted people• Trusted publisher
Thumbprint	Select a certificate that already exist to use it for the encryption.

Create Certificate

Self Signed Certificate

Option	Description
Common name	Name of the certificate.
Key size (bits)	Indicates the key size (bits) of the certificate. Select between: <ul style="list-style-type: none"> • 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 into a pfx file and secure this certificate with a password.
Save to certificate store	Indicate the location and the store to save the certificate.

3.6.3 User Management

Description

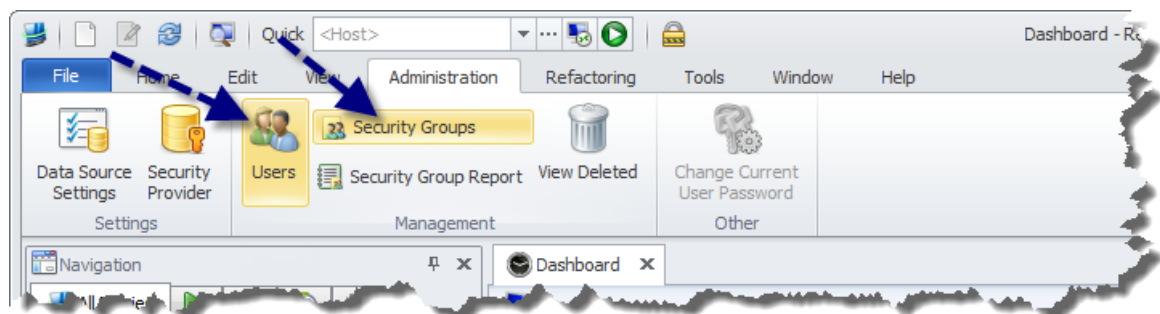


This feature requires an [Advanced Data Source](#) such as [MSSQL](#) and [MySQL](#).

User management allows for creating & managing users & security access rights. The user/group administration is available from the menu bar **Administration -> Users or Security Group**.



In order to create users and assign rights, you must be administrator of not only Remote Desktop Manager, but also of the underlying database (such as [MSSQL](#) and [MySQL](#))



Administration tab - Users & Security Groups

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



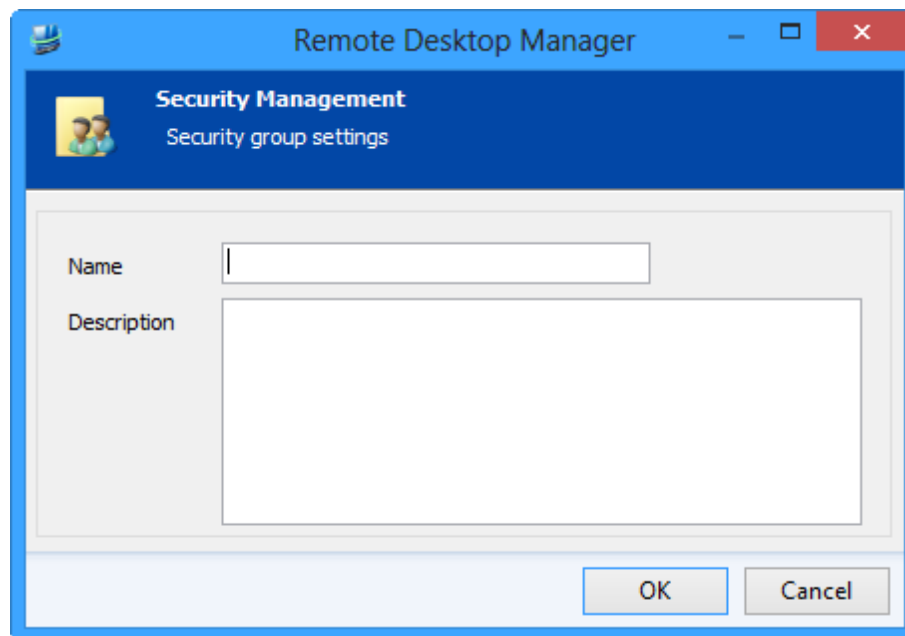
All sessions without security groups are considered public!

Steps

1. [Create a security group](#)
2. [Create a user](#)
3. Assign [Permissions](#) to the user
4. [Assign the security group to the session](#)

Create a security group

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



Security group dialog

Create users

Create the user using default security (specify the password) or integrated security (for more information please see [Integrated Security](#)).

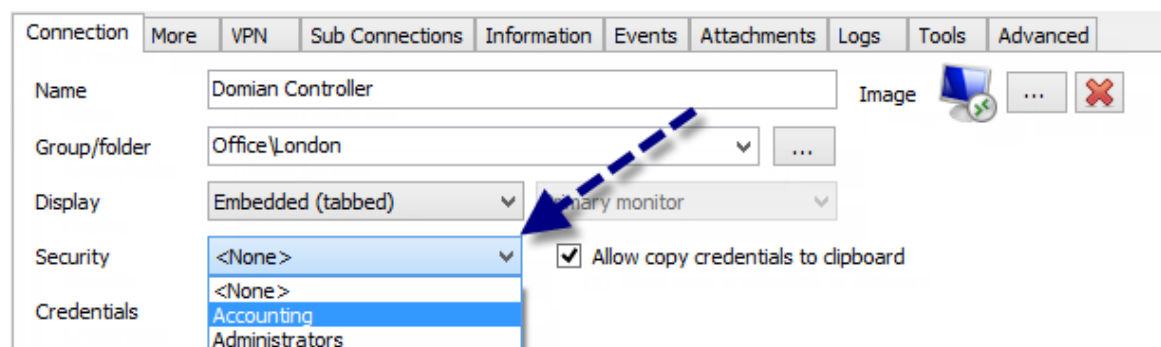


Not all [Advanced Data Sources](#) support the use of integrated security. SQL Server supports it natively. [MySQL](#) supports integrated security via [Windows Authentication Plugin](#) which is a commercial extension of MySQL.

You can assign different security options to the user, such as the allow Offline Mode, a read-only mode, and more. However, there is currently no way to inherit security rights from a group. They must be assigned individually for each user. For detailed information please refer to [Permissions](#)

Assign the security group to the session

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

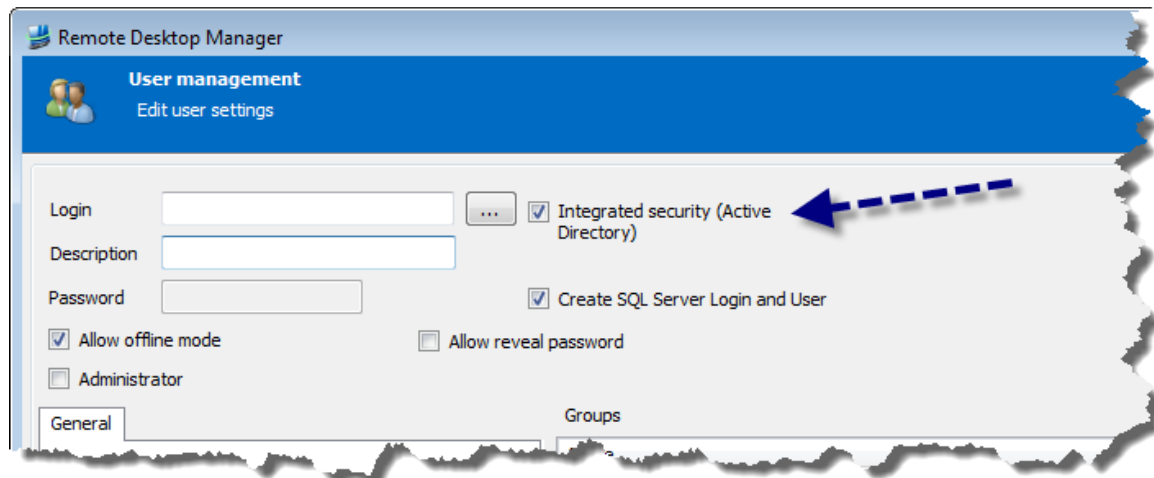


Session configuration - security group

3.6.3.1 Integrated Security

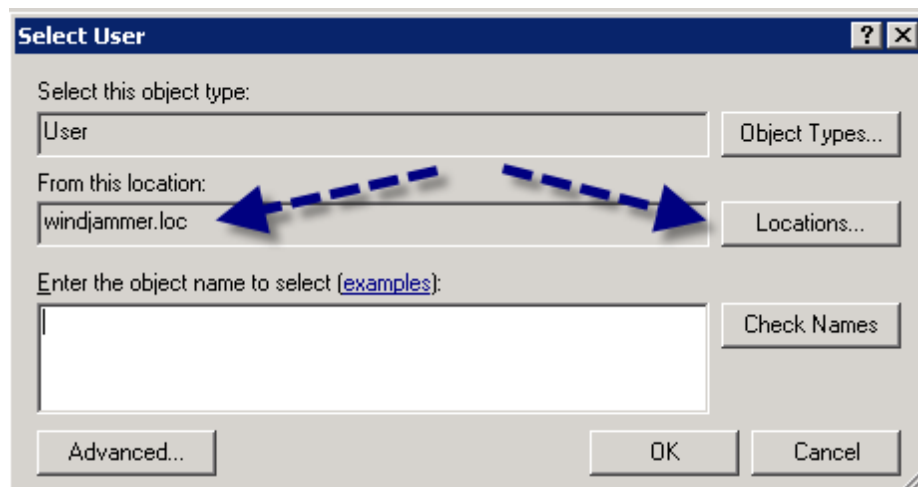
Description

Integrated Security is the name Microsoft gives to the technology that uses your currently running session credentials and passes them automatically to the remote resources for authentication. In our case this is used for [Advanced Data Sources](#) like SQL Server and MySQL. When in a Remote Desktop Manager dialog you check an "Integrated Security" checkbox, the password field will be disabled because the operating system will provide a cached copy automatically.



User Management form

When the option is enabled, an ellipsis button will either appear or be enabled. Clicking this button will display the Windows "Select User" dialog.



Select user dialog

Ensure the appropriate domain is displayed because sometime the location defaults to the local computer. Click the Locations button to be able to browse for the domain instead.

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

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](#)

3.6.3.2 Permissions

Description

Remote Desktop Manager allows for advanced user rights management that allow you to control how a session is used. Note that some control's visibility depends on the active data source.

Add/Edit user dialog

Settings

General settings

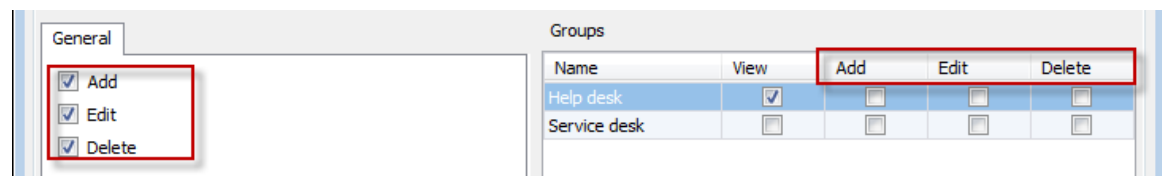
Option	Description
Login	Login name for the user. When using Integrated security you must select the user in the directory.
Full name	Full name of the user, for display purposes only
password	Password for the user. Disabled when using Integrated security
Integrated security	Specify to use Windows Integrated Authentication for authenticating to the data source. Applies only to SQL Server and RDMS, depending on

	their configuration. When checked, an ellipsis button appears to allow you to browse for the user account in the directory.
Create SQL login and user	The system will create the login and user in SQL server. Disable this if you don't have sufficient privileges on the server to create them. Your organization's DBA will have to perform these steps manually.
Enabled	Appears only when editing an existing user. You can disable the user account using this option.
Allow offline mode	Allows the user to enable the Offline Mode on the data sources. This also depends on the data source being configured to allow it.
Allow reveal password	Allows this user to use the Reveal Password command.
Administrator	Grants full administrative rights to the user. This is for the system as a whole.
Offline mode	Choose between: <ul style="list-style-type: none"> • Disabled: no offline cache allowed for that user • Read-only: a read-only cache is allowed for Advanced Data Sources. • Read-Write: an advanced cache, with change synchronization, is allowed for Advanced Data Sources.

Session settings

Option	Description
Add	When checked, will grant the Add privilege for public groups. Also controls the visibility of the Add column in the Groups grid
Edit	When checked, will grant the Add privilege for public groups. Also controls the visibility of the Edit column in the Groups grid
Delete	When checked, will grant the Add privilege for public groups. Also controls the visibility of the Delete column in the Groups grid
View session details	Allows this user to see the content of the Details tab. Applies to all sessions.
View session information	Allows this user to see the content of the Information tab. Applies to all sessions.
View shared logs	Allows this user to see the content of the logs that apply to a session. Applies to all sessions.
Import sessions	Allows the user to import sessions.
Export sessions	Allows the user to export sessions.
Allow drag-and-drop	Allows the user to move the sessions using drag-and-drop

Groups



The Add, Edit and Delete columns are visible only after you have checked the corresponding option boxes.



Enabling the option in the general tab grants the corresponding privilege for all public groups (groups that have no security group assigned)

The options in the grid apply for the security group in the first column

Option	Description
View	Allows the user to View AND USE the entries for that security group.
Add	Allows the user to add entries in groups/folders for that security group
Edit	Allows the user to Edit the entries for that security group.
Delete	Allows the user to Delete the entries for that security group.

3.6.4 Security Group Management

Description



This feature requires an [Advanced Data Source](#) such as [MSSQL](#) and [MySQL](#).

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

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

For more information on how to create security groups see [here](#).

3.6.5 Role Management

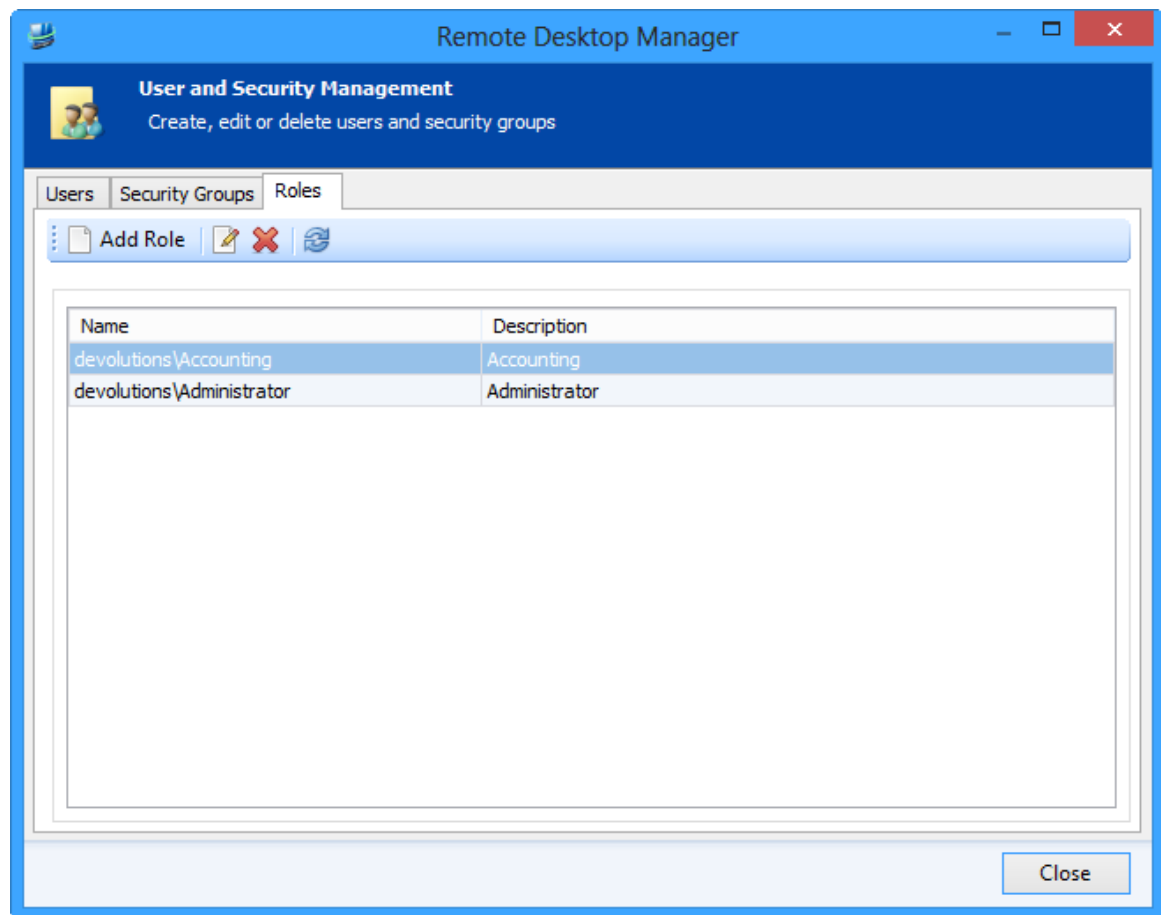
Description

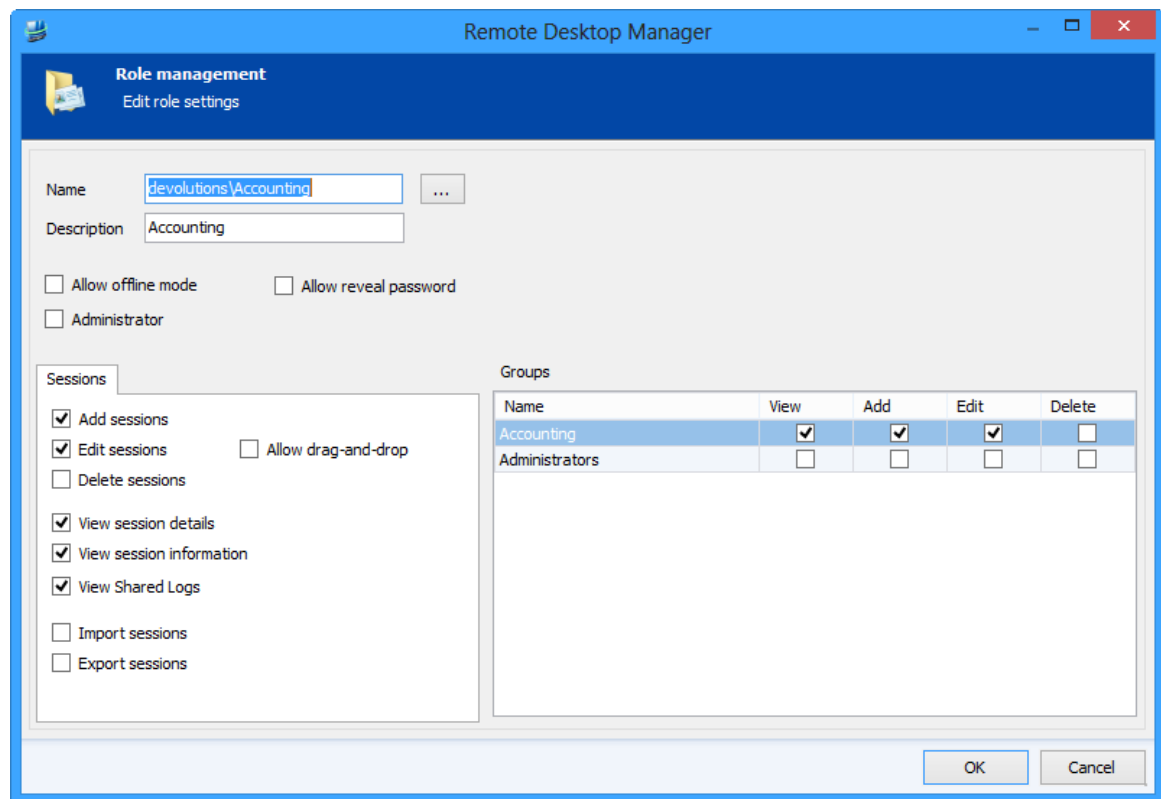


This feature requires [Remote Desktop Manager Server](#) (RDMS).

Roles in Remote Desktop Manager are directly related to Active Directory groups. The interface and management of roles are quite similar as the corresponding notions for users, but instead of a single Remote Desktop Manager user, they apply to an Active Directory group.

By leveraging active directory integration you can easily define access rights for all domain users in your organization. No need to configure each user individually, simply add or remove users in the linked group and let the system take care of the rest. Once a domain user logon onto the RDMS data source, they will be created if need be and users rights will be controlled by the defined groups.

**Role Management**



Editing roles

3.6.6 Deleted Entries

Description

The **View deleted** command allows you to view the deleted entries, as well as restoring them.

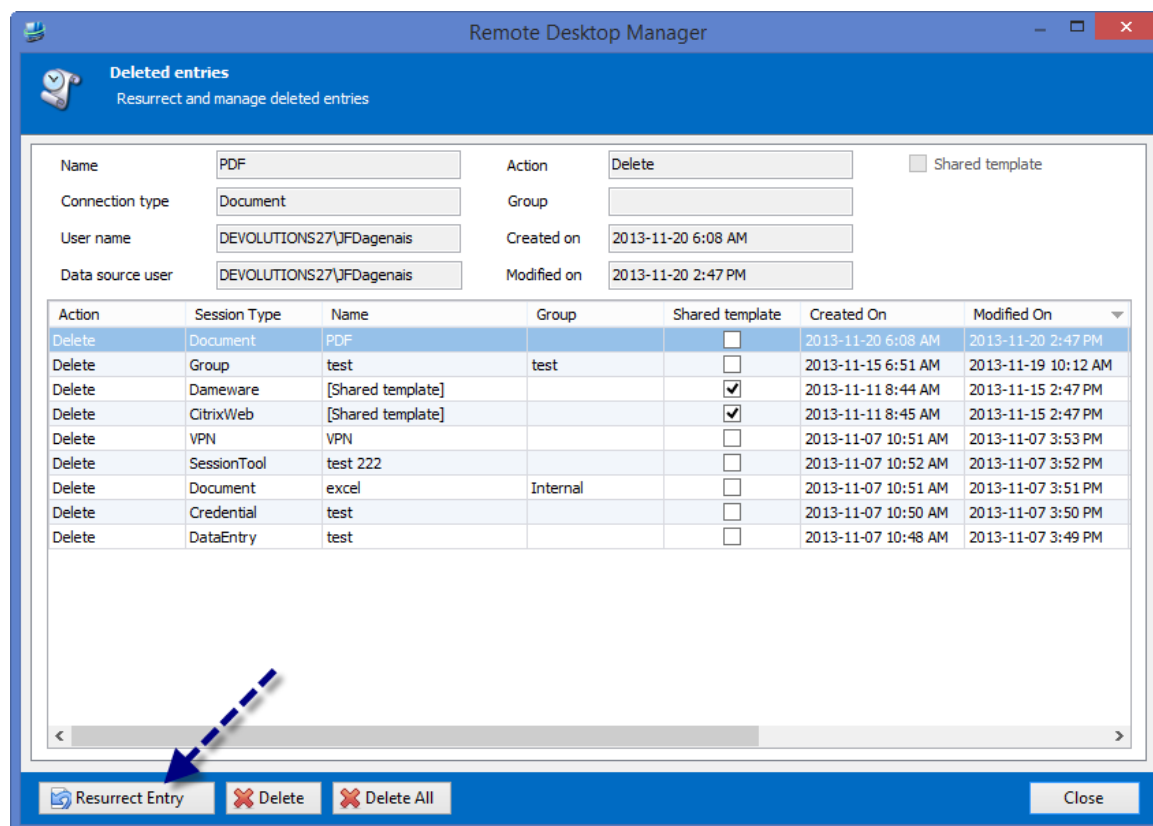


This feature requires an [Advanced Data Source](#).

Manage Deleted Entries

If an entry is deleted and needs to be restored, use **Resurrect Entry** at the bottom of the window.

You can also permanently delete your deleted entries.



View Deleted

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.



Deleted entries can be resurrected as long as the [Security Provider](#) has not been changed since the delete action.



Administrators can permanently delete some or all deleted entries.

3.6.7 Reports

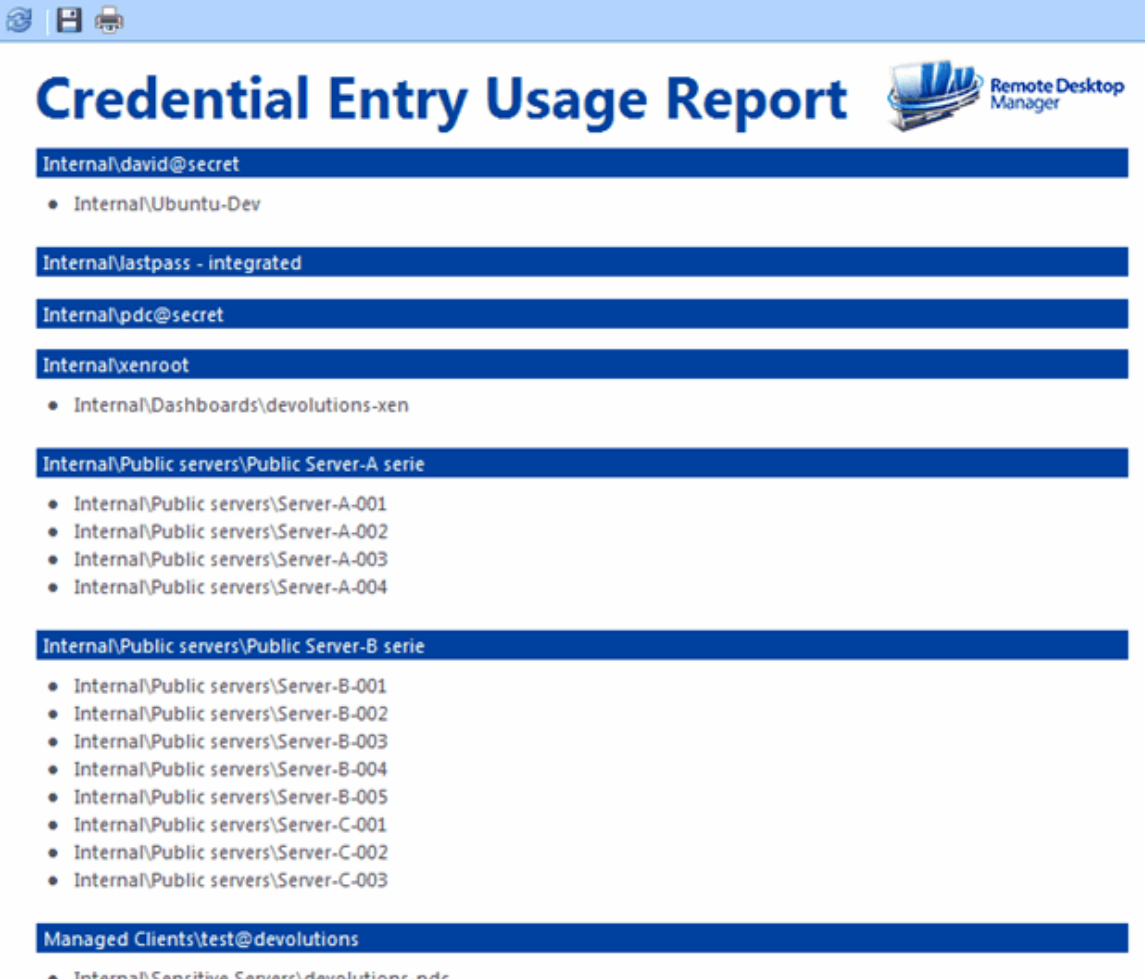
3.6.7.1 Credential Report

Description

This report shows where credentials are used.



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



The screenshot shows the 'Credential Entry Usage Report' interface. At the top, there are icons for settings, save, and print. The title 'Credential Entry Usage Report' is prominently displayed next to the 'Remote Desktop Manager' logo. Below the title, the report is organized into sections, each with a blue header bar:

- Internal\David@secret**
 - Internal\Ubuntu-Dev
- Internal\lastpass - integrated**
- Internal\pdc@secret**
- Internal\xenroot**
 - Internal\Dashboards\devolutions-xen
- Internal\Public servers\Public Server-A serie**
 - Internal\Public servers\Server-A-001
 - Internal\Public servers\Server-A-002
 - Internal\Public servers\Server-A-003
 - Internal\Public servers\Server-A-004
- Internal\Public servers\Public Server-B serie**
 - Internal\Public servers\Server-B-001
 - Internal\Public servers\Server-B-002
 - Internal\Public servers\Server-B-003
 - Internal\Public servers\Server-B-004
 - Internal\Public servers\Server-B-005
 - Internal\Public servers\Server-C-001
 - Internal\Public servers\Server-C-002
 - Internal\Public servers\Server-C-003
- Managed Clients\test@devolutions**
 - Internal\Sensitive Servers\devolutions-pdc

Credential Entry Usage Report

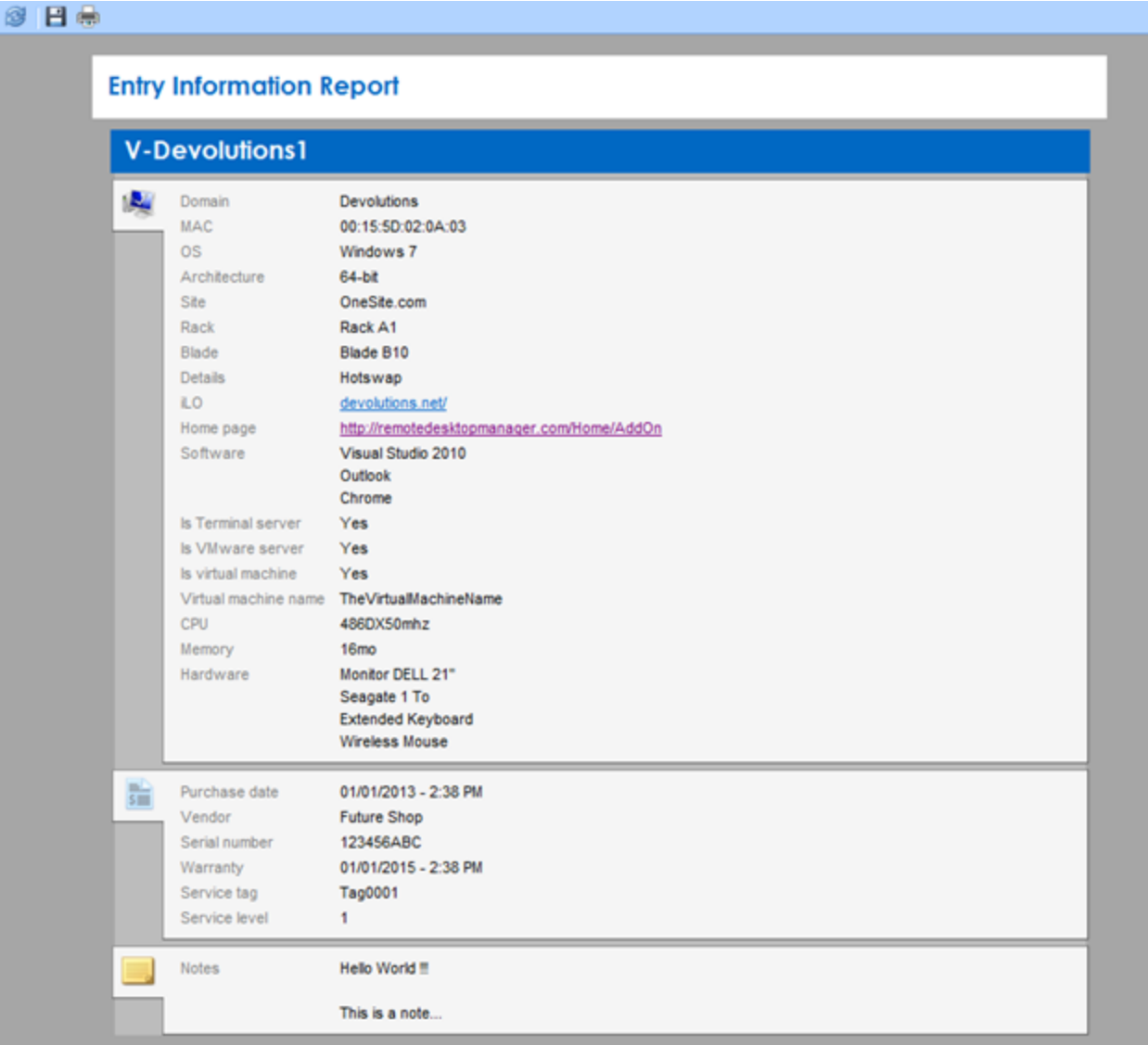
3.6.7.2 Entry Information Report

Description

This report displays the fields of the Information pane for entries.



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



Entry Information Report

V-Devolutions1

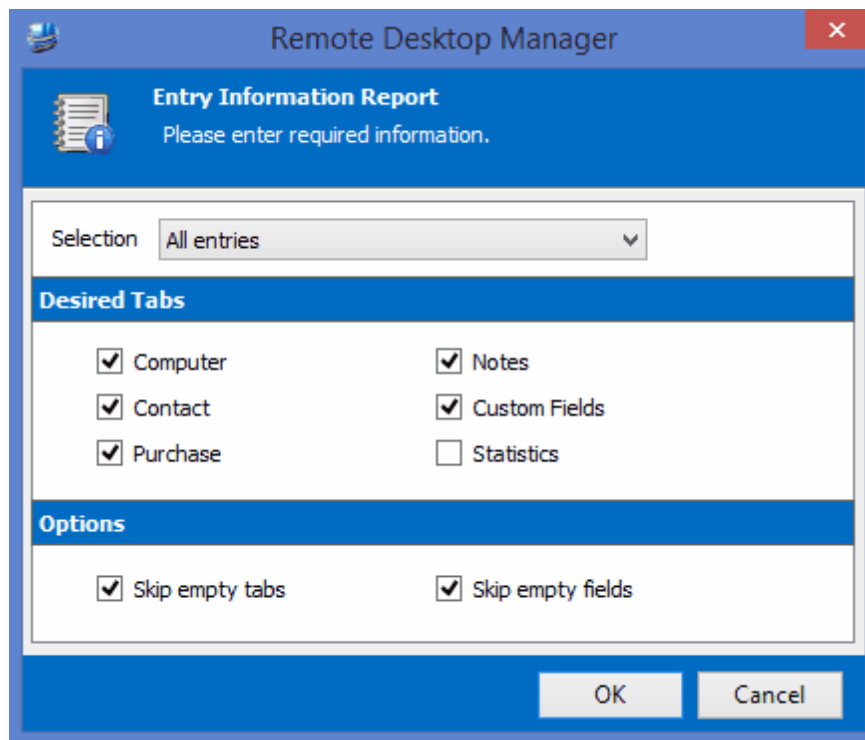
Domain	Devolutions
MAC	00:15:5D:02:0A:03
OS	Windows 7
Architecture	64-bit
Site	OneSite.com
Rack	Rack A1
Blade	Blade B10
Details	Hotswap
ILO	devolutions.net/
Home page	http://remotedesktopmanager.com/Home/AddOn
Software	Visual Studio 2010 Outlook Chrome
Is Terminal server	Yes
Is VMware server	Yes
Is virtual machine	Yes
Virtual machine name	TheVirtualMachineName
CPU	486DX50mhz
Memory	16mo
Hardware	Monitor DELL 21" Seagate 1 To Extended Keyboard Wireless Mouse

Purchase date	01/01/2013 - 2:38 PM
Vendor	Future Shop
Serial number	123456ABC
Warranty	01/01/2015 - 2:38 PM
Service tag	Tag0001
Service level	1

Notes	Hello World !!! This is a note...
-------	--

Entry Information Report

Settings



Report settings

Selection

It is possible to run the report on all entries, or on currently selected entries in the navigation pane.

Desired tabs

You can choose which sub-tabs are selected for the report.

Options

- Skip empty tabs: empty tabs do not appear in the report.
- Skip empty fields: empty fields do not appear in the report.


3.6.7.3 Entry List Report

Description

This report shows a simplified list of all your entries. Entry names are in fact hyperlinks to drill down directly to the entry.



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



Entry List Report

Group/folder	Name	Description
Internal	david@secret	
Internal	Devolutions - VPN	
Internal	lastpass - integrated	
Internal	pdc@secret	
Internal	Ubuntu-Dev	
Internal	V-Devolutions1	
Internal	xenroot	
Internal\Cloud\AWS	S3 Devolutions	
Internal\Cloud\AWS	staging	CRON jobs and SYSLOG.
Internal\Cloud\Azure	staging	CRON jobs and SYSLOG.
Internal\Cloud\OpenStack	staging	CRON jobs and SYSLOG.
Internal\Dashboards	devolutions-aws	
Internal\Dashboards	devolutions-xen	
Internal\Dashboards	Hyper-V	
Internal\Dashboards	VMWare	
Internal\Public servers	Public Server-A serie	Same credential for all A-serie servers
Internal\Public servers	Public Server-B serie	Same credential for all B-serie servers
Internal\Public servers	Server-A-001	Movie server A thru E
Internal\Public servers	Server-A-002	Movie server F thru J
Internal\Public servers	Server-A-003	Movie server K thru O
Internal\Public servers	Server-A-004	Movie server P thru Z
Internal\Public servers	Server-B-001	Audio server Classical
Internal\Public servers	Server-B-002	Audio server Rock
Internal\Public servers	Server-B-003	Audio server Hits
Internal\Public servers	Server-B-004	Audio server Metal
Internal\Public servers	Server-B-005	Audio server Dance
Internal\Public servers	Server-C-001	Audio server Dance
Internal\Public servers	Server-C-002	Audio server Dance
Internal\Public servers	Server-C-003	Audio server Dance

Entry List Report

3.6.7.4 Entry Status Report

Description

This report show the lists of any entries with an assigned status.



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



Group/folder	Name	Status
Internal\Public servers	Server-B-001	Warning
Internal\Public servers	Server-B-002	Warning
Internal\Public servers	Server-B-003	Warning
Internal\Public servers	Server-B-004	Warning
Internal\Public servers	Server-B-005	Warning
Internal\Public servers	Server-C-001	Expired
Internal\Public servers	Server-C-002	Expired
Internal\Public servers	Server-C-003	Expired

Entry Status Report

3.6.7.5 Expired Entry List Report

Description

This report list all the expired entries with an expiration date. Before running the report, you need to select one of the following:

- Expired connections and warranties
- Expired connections
- Expired warranties



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

The report will display with the proper information depending of the selection.



Group/folder	Name	Expiration	Status
Internal\Public servers	Server-C-001	01/10/2013	Expired
Internal\Public servers	Server-C-002	01/10/2013	Expired
Internal\Public servers	Server-C-003	01/10/2013	Expired

Expired Entry List Report

3.6.7.6 Security Group Report

Description

This report displays the assigned security groups for all the entries. It's not an HTML report like the other reports.



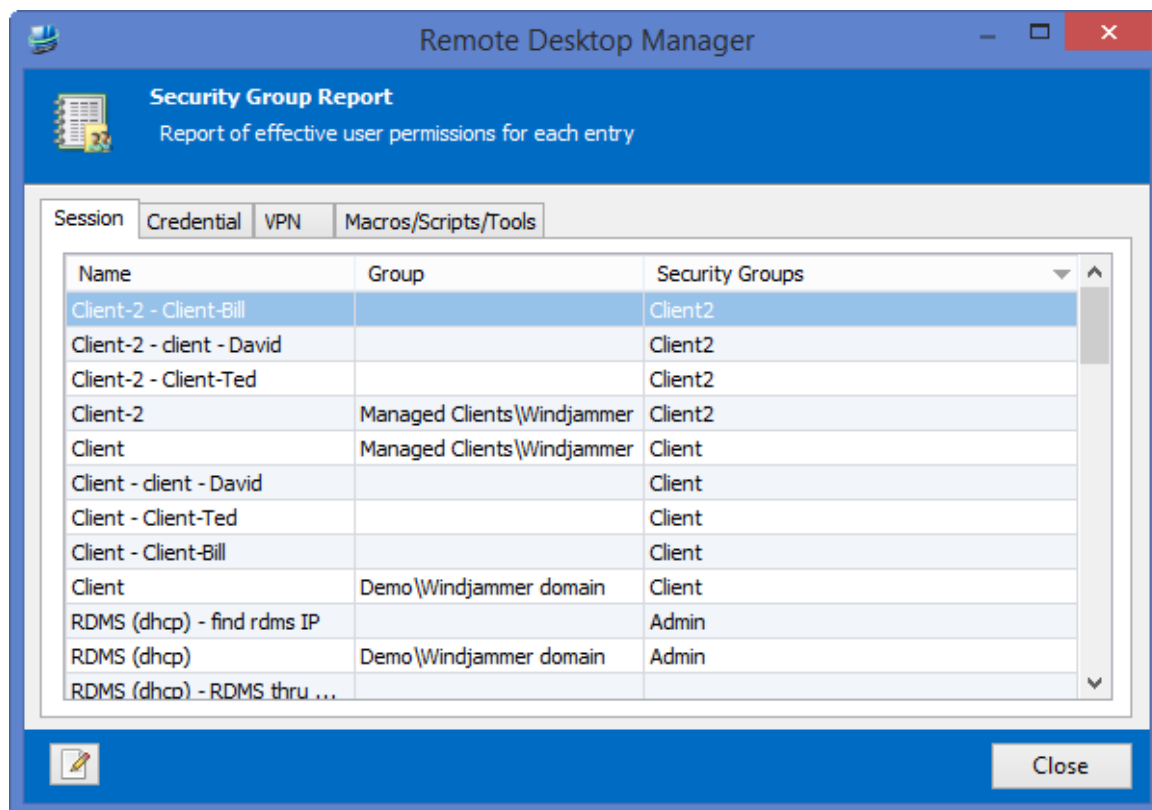
This feature requires an [Advanced Data Source](#).




It is a recommended practice to run this report every time you change a security group or assign any user permissions.



Any entry without a security group is public, any user can use/edit/delete public sessions. In a typical team environment there should be no entries without a security group.



Security group report

The dialog has tabs that organizes the entries by types. Sub-connections are also included in this report and are prefixed with their parent name. You can use the edit button  to quickly edit the selected entry.

3.6.7.7 VPN Reference Report

Description

This report shows the entries that are using VPN entries. Use this report to view all VPN entries, and the sessions that use them in their VPN tab.



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

VPN Reference Report

Internal\Devolutions - VPN

- Internal\Sensitive Servers\devolutions-pdc

Internal\Public servers\VPN Public Servers A serie

- Internal\Public servers\Server-A-001
- Internal\Public servers\Server-A-002
- Internal\Public servers\Server-A-003
- Internal\Public servers\Server-A-004

Internal\Public servers\VPN Public Servers B serie

- Internal\Public servers\Server-B-001
- Internal\Public servers\Server-B-002
- Internal\Public servers\Server-B-003
- Internal\Public servers\Server-B-004
- Internal\Public servers\Server-B-005

Internal\Public servers\VPN Public Servers C serie

- Internal\Public servers\Server-C-001
- Internal\Public servers\Server-C-002
- Internal\Public servers\Server-C-003

VPN Reference Report

3.6.8 Connecting External System

Description

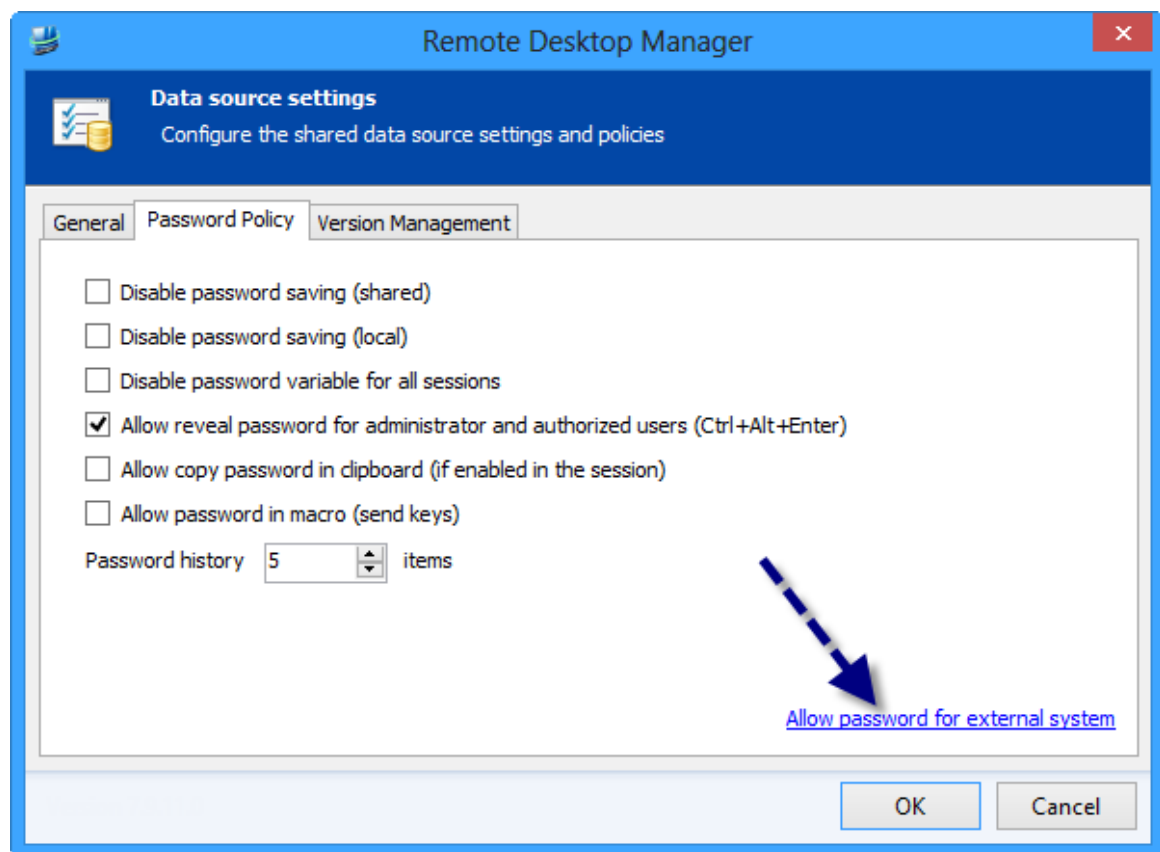


This feature requires an [Advanced Data Source](#) such as [MSSQL](#) and [MySQL](#).

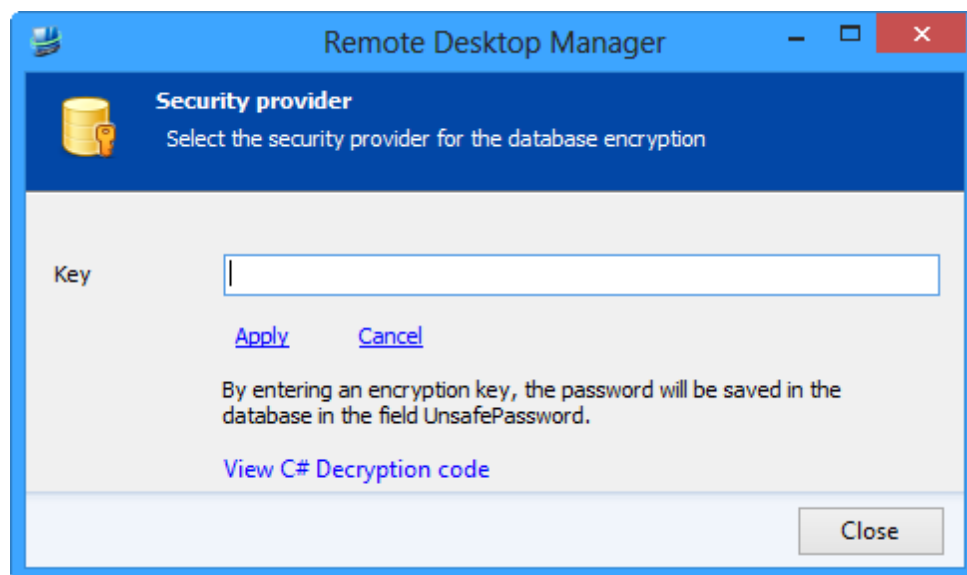
Connecting with external systems is possible via the underlying data source. Very useful when you want to sync your RDM data with an external system like a CRM.

The session information is stored in the Data field of the Connections table for the underlying data store.

However getting the password encrypted password from the data source requires that the allow password for external systems be enabled.



Enable allow password for external system



Enter pass phrase & hit apply

Once enable this will cause the system to extract a copy of the password the will then be re-encrypted using the pass phrase and stored back into the SafePassword field of the Connections table.

Decryption Code

Use the following .Net decryption code to decrypt your passwords.

```
public static string Decrypt(string encryptedString, string key)
{
    if (string.IsNullOrEmpty(encryptedString))
    {
        return encryptedString;
    }

    try
    {
        TripleDESCryptoServiceProvider tripleDesCryptoServiceProvider = new TripleDESCryptoServiceProvider();
        MD5CryptoServiceProvider cryptoServiceProvider = new MD5CryptoServiceProvider();

        string strTempKey = key;

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

        tripleDesCryptoServiceProvider.Key = byteHash;

        tripleDesCryptoServiceProvider.Mode = CipherMode.ECB;

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

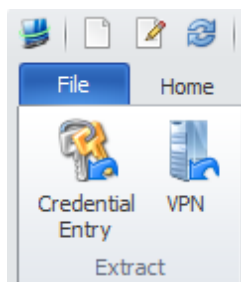
        string strDecrypted =
            Encoding.UTF8.GetString(
                tripleDesCryptoServiceProvider.CreateDecryptor().TransformFinalBlock(
                    byteBuff, 0, byteBuff.Length));

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

3.6.9 Refactoring

3.6.9.1 Extract

Description



The extract actions are available in the Refactoring tab. Remote Desktop Manager currently supports two types of extraction refactoring:

- Extract VPN: used to create a new VPN entry and link it to the current session

- Extract Credentials: used to create a credential entry and link it to the current session

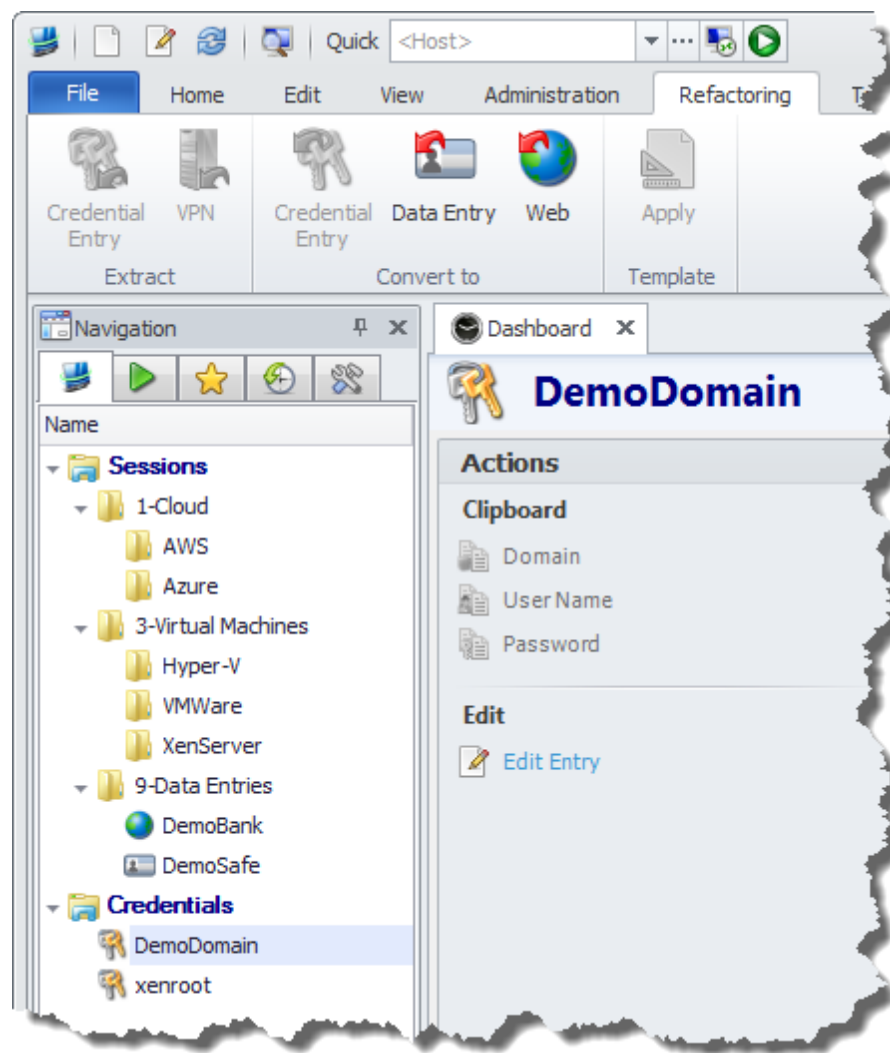
As described, this doesn't modify the source session in any way.

3.6.9.2 Convert To

Description

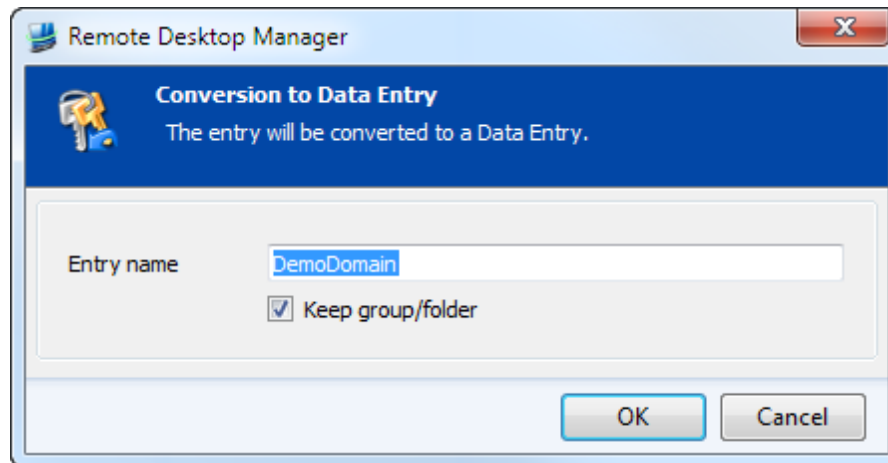
Conversion actions are available in the refactoring tab page. They convert the current entry into another entry type. There are currently 3 kinds and their actions are enabled only when the source entry is compatible with the destination.

- Credential Entry: Converts the source entry to a credential entry.
- Data Entry: Converts the source entry to a data entry
- Web: Converts the source entry to a web entry.



Refactoring tab

When you select the refactoring you are presented with a dialog to enter a name for the new entry. You can also specify to keep the same folder. The dialogs are mostly the same for all three refactorings.

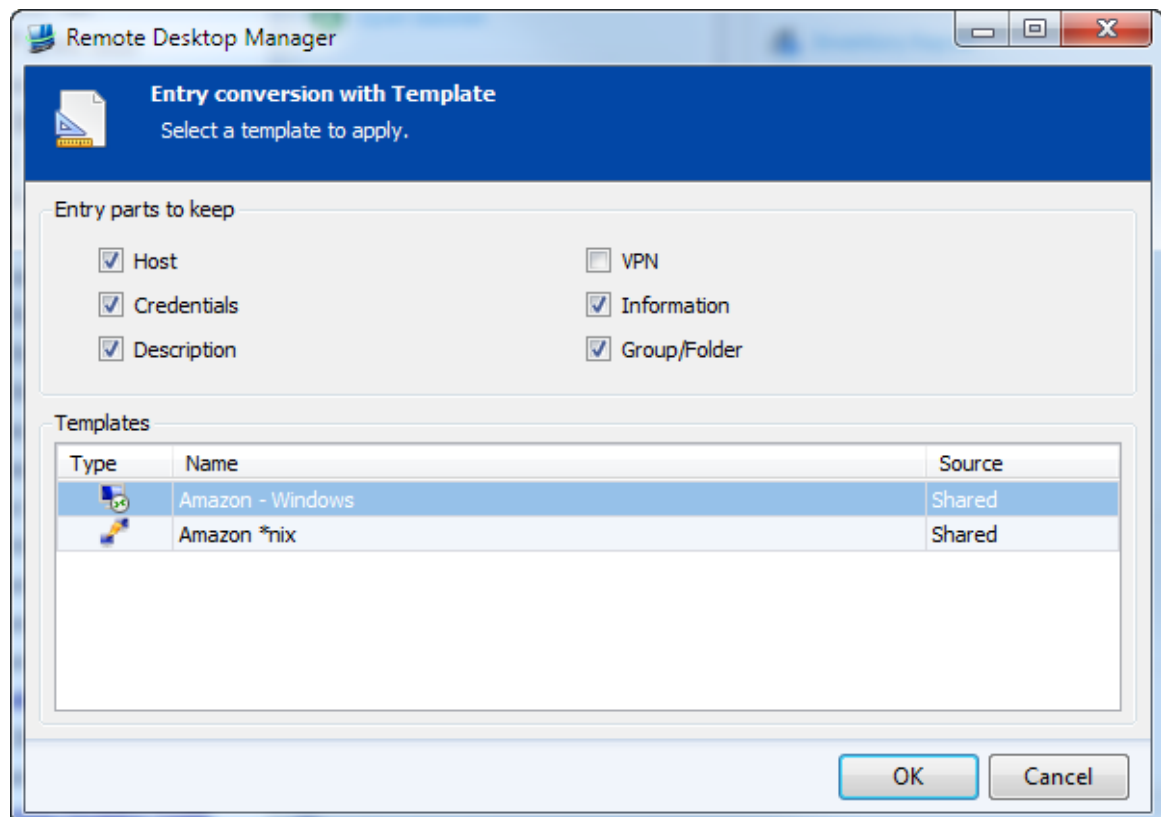


Conversion form

3.6.9.3 Template

Description

The template refactoring is used to apply massive changes from a template, while offering to preserve a few of the existing field values. Whereas the batch update allows you to perform discrete changes, this is more of a bulk changes tool. It even allows to change the type of the entry, for example you could change multiple SSH Shell entries to PUTTY entries in one fell swoop.



Template conversion form

Settings

The check boxes are used to preserve the corresponding part of the original entry.

Host	Preserves the host name.
Credentials	Preserves the credentials as defined in the General tab AND in the Options group of the Tools tab.
Description	Preserves all of the information on the More tab.
VPN	Preserves all of the information on the VPN tab.
Information	Preserves all of the information on the Information tab.
Group/Folder	Preserves the group/folder.

3.6.9.4 Sub Connection

Description

Sub Connection refactorings allows you to set a connection under a parent connection, or to reverse the process. Please see Sub Connections [Overview](#) for more information on their utility.

Parent

Available for connections that are not parents themselves, this allows you to move a connection under a parent connection.

Un-parent

Available only for sub connections, this allows you to move a connection out from under a parent connection.



If you want to move a sub connection under a new parent, it cannot be performed in a single action. You must first **Un-parent** it to be a standalone connection, then use the **Parent** command.

3.6.10 Tools

3.6.10.1 Add-on Manager

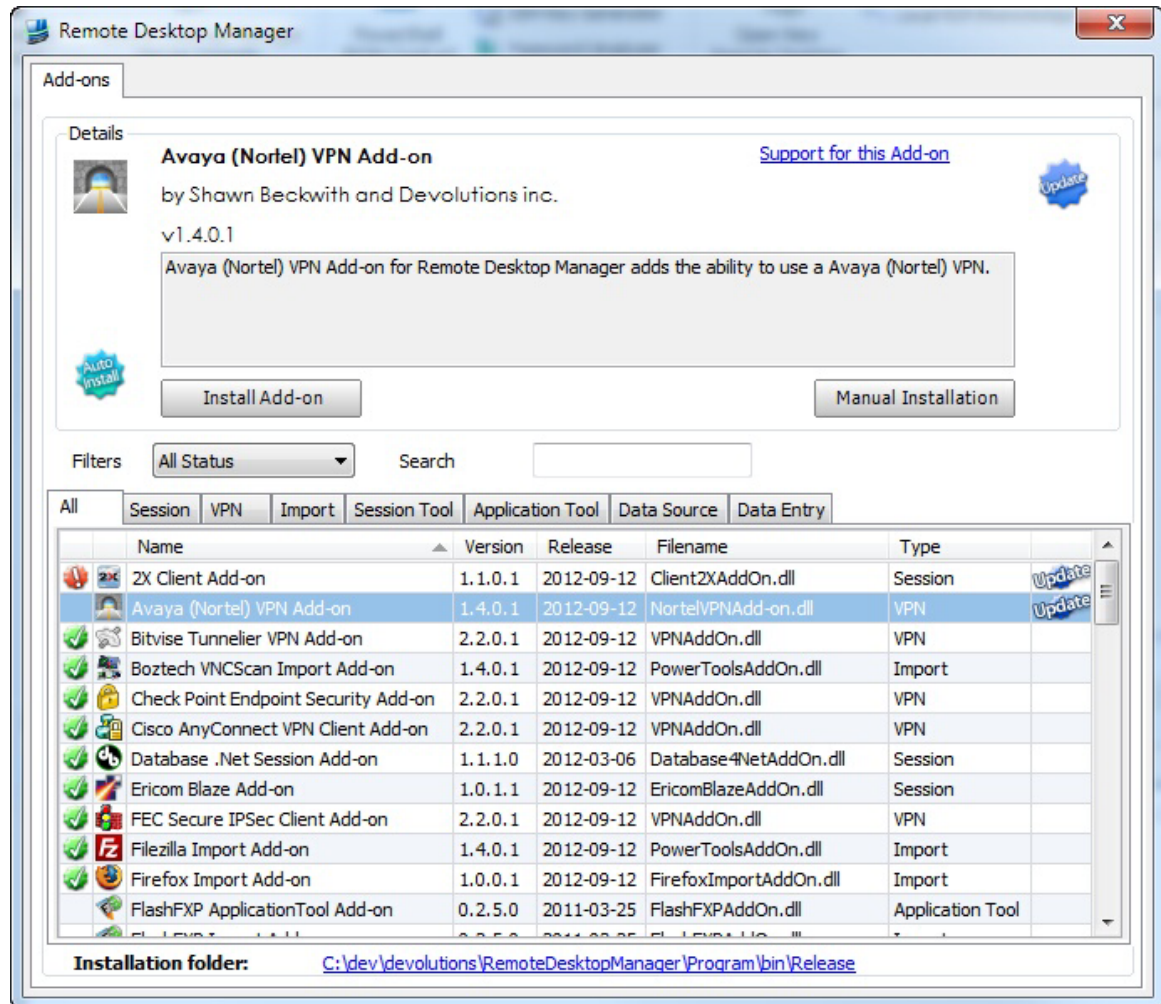
Description

The Add-on Manager is available in the **Tools->Add-on Manager** menu. It is used to simplify the management and the installation of different add-ons. It lists all of the add-ons that are supported by the current version of the application.

The add-ons are classified by category (*session, import, data source*, etc.), and can be sorted according to their current status (*available, outdated, uninstalled*). Add-ons that can be updated will be displayed with a special and clearly visible icon as seen below.

If the add-on does not require any special third party library, the manager will deploy it automatically

after clicking the install button. A restart of the application will be required. The same procedure and limitation applies when uninstalling an add-on.



Add-on manager dialog

Icon Legend

The first column of the grid contains an icon indicating the state of the add-on.

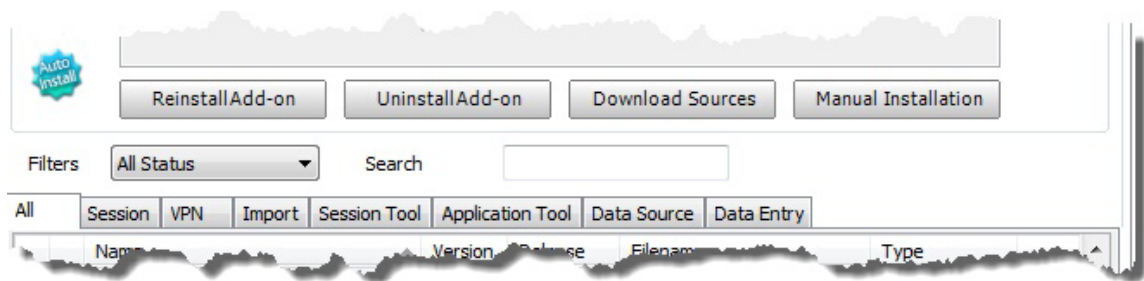
Blank: Add-on not installed locally.

: Add-on installed and up to date.

: Add-on installed but not at the latest version.

Workflow

The visibility of the action buttons available on the form is toggled depending on the context. There are four buttons as follows.



Button highlight

Reinstall Add-On

Reinstalls the add-on after getting a confirmation from the user. An application restart will be required.

Uninstall Add-On

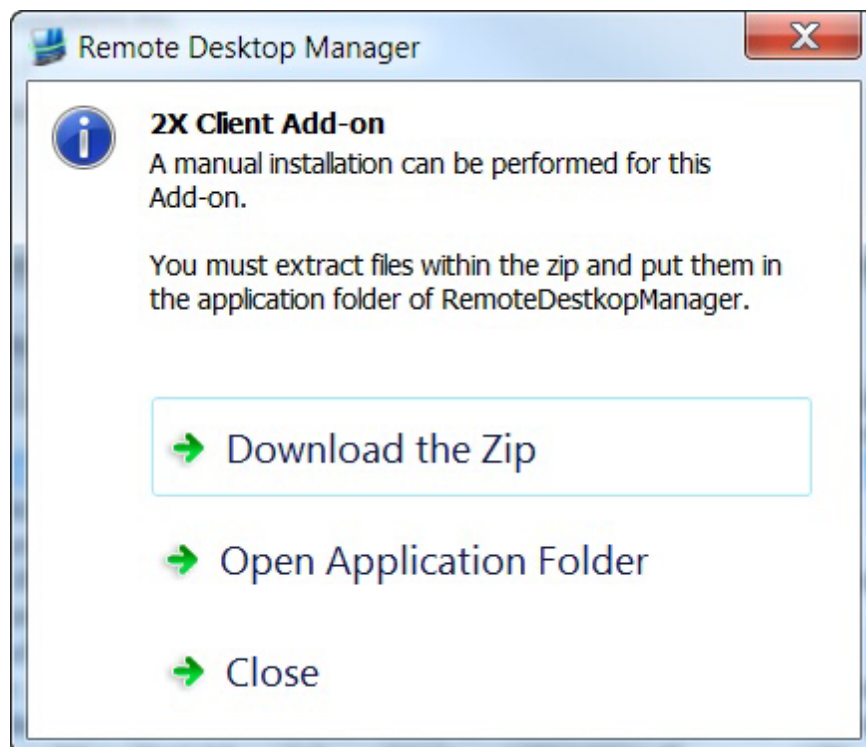
Uninstalls the add-on after getting a confirmation from the user. An application restart will be required.

Download Sources

Launches the download of an archive containing the source code for the add-on.

Manual Installation

1. Click on the Manual Installation button, the following dialog will appear



Manual Installation Dialog

2. Click on the **Open Application Folder** button, a Windows explorer will open in the proper folder

for your installation.

3. Click on **Download the Zip** button, this will launch the download of the zip archive.
4. Unzip all files in the installation folder opened at step 2.
5. Restart Remote Desktop Manager
6. Create a new session with the newly installed add-on type, or use it if it's a custom tool or an import dialog

Troubleshooting

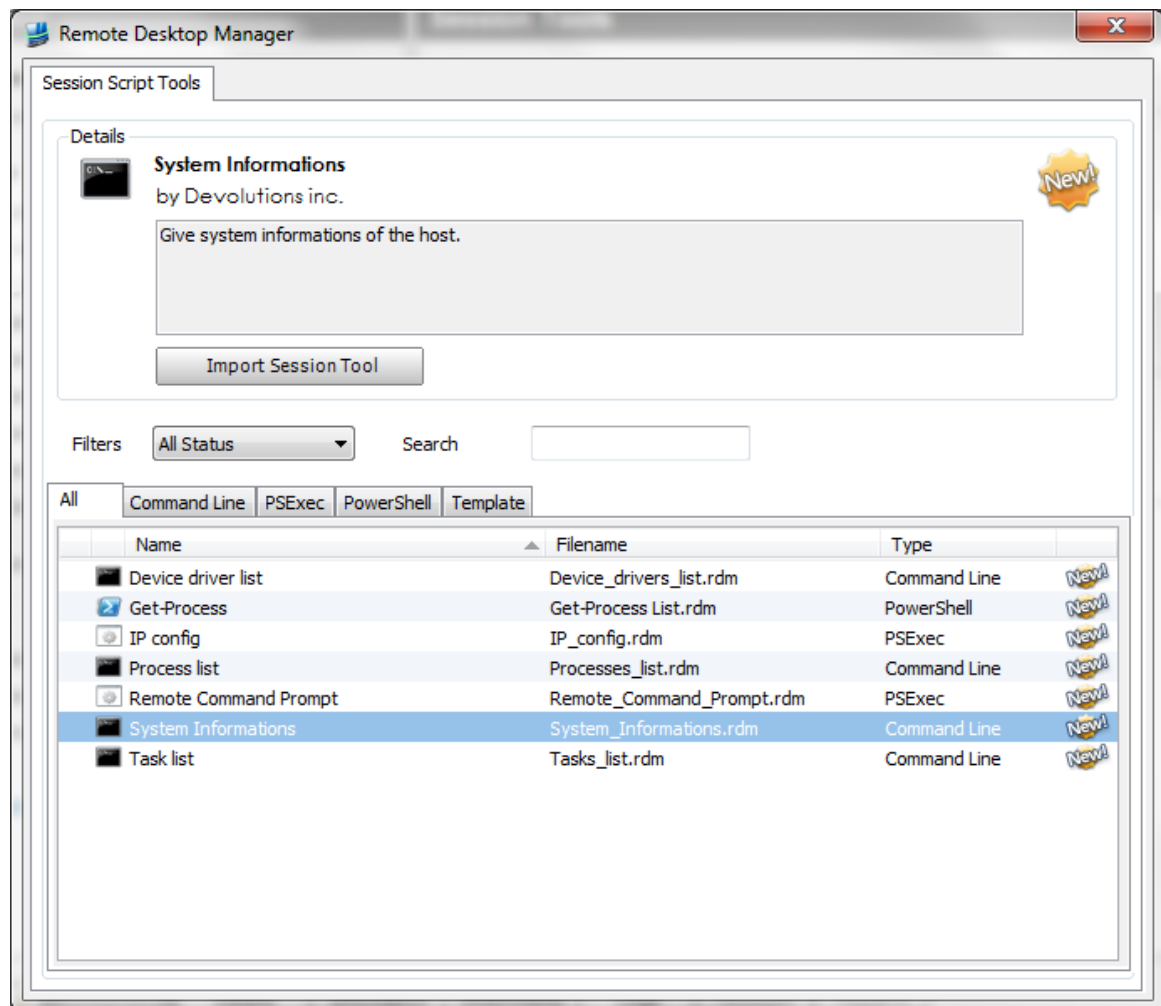
If you cannot see the add-on in the session type list, verify that it is loaded in the About box, which is available from **Help > About** menu. Also verify that the .dll file is in the Remote Desktop Manager folder.

Some add-ons are supported directly by Devolutions, and some others are developed by third parties. More information can be found in the [Add-On forum](#).

3.6.10.2 Macro/Script/Tool Manager

Description

The manager simplifies the installation of any session script tool provided by the community. You can import an existing tool directly in the current data source by clicking the Import button, and submit any interesting session script tools to us at support@devolutions.net.

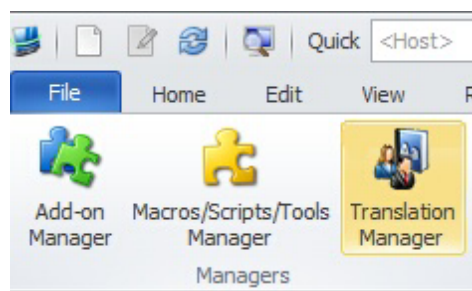


Macros/Scripts/Tools Manager

3.6.10.3 Translation Manager

Description

The translation manager is in fact a cloud based translation repository, managed by an external application named the *Devolutions Localizer*, developed by our team at Devolutions. It allows for easy translation of resources used by our products.



Ribbon button

It is launched from **Tools -> Translation Manager**.

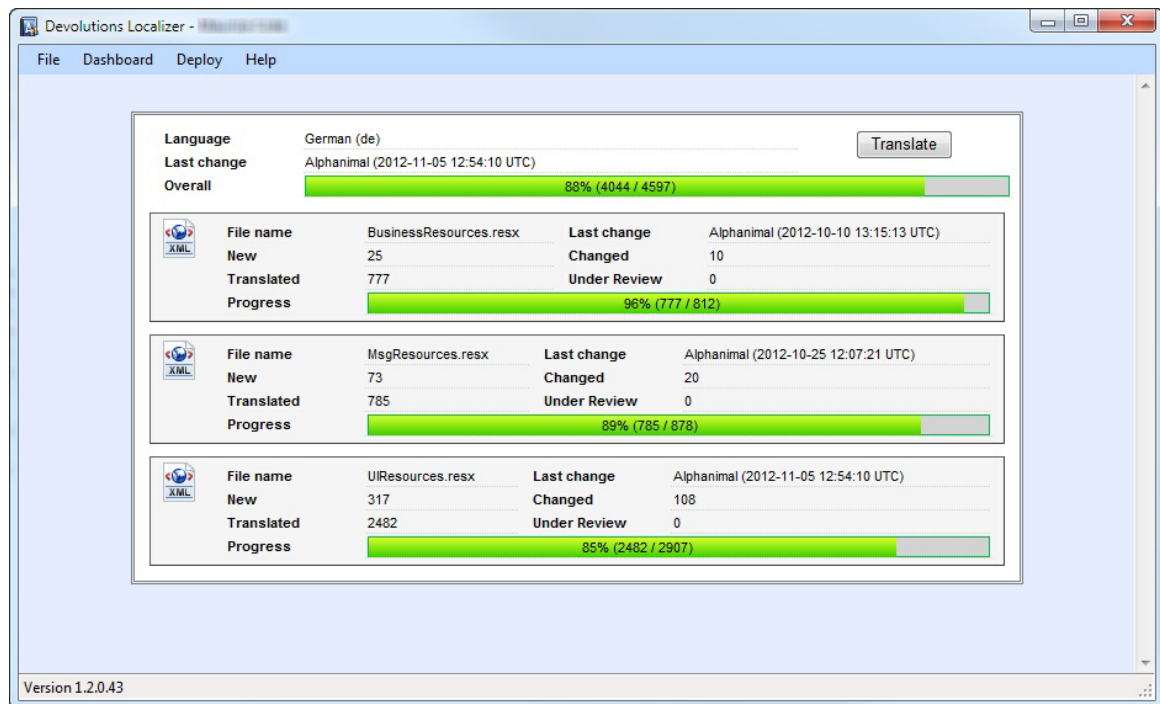
It requires an account that you can create at [here](#). Enter the requested information and submit the form. You will receive a confirmation email within 24 hours.

For more information on the localization process, read the [Localizer](#) topic

3.6.10.3.1 Localizer

Description

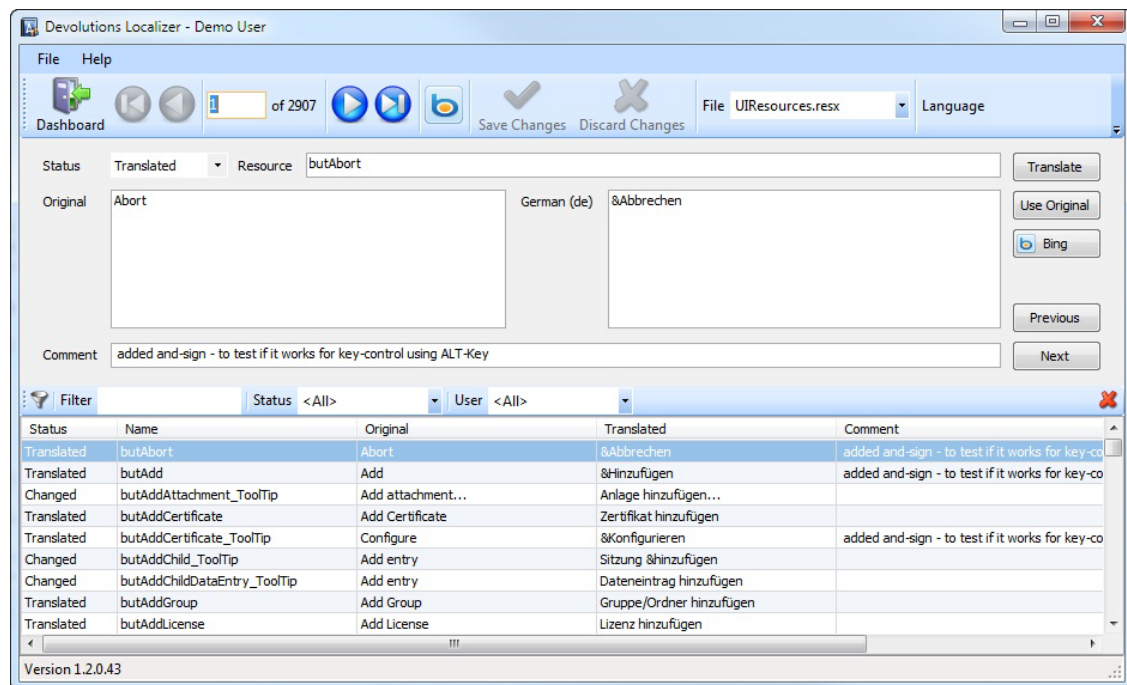
The Devolutions Localizer is a ClickOnce application what will be installed in your application data folders and will check for updates automatically. It is used to manipulate the cloud based translation repository.



Devolutions Localizer

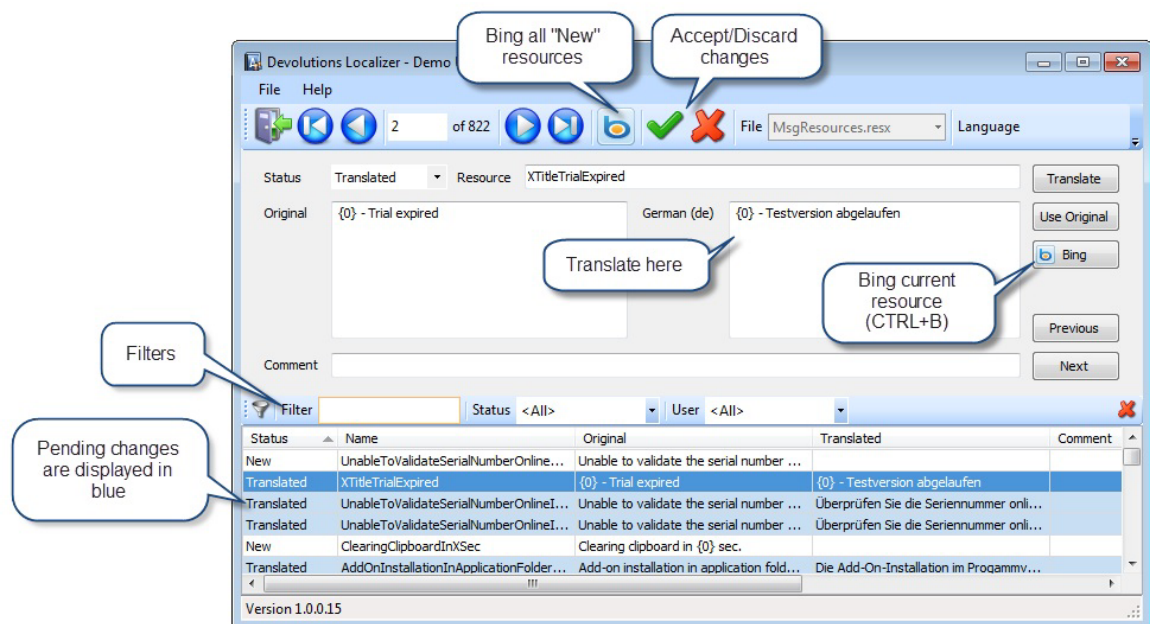
Workflow

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.



Localizer translation form

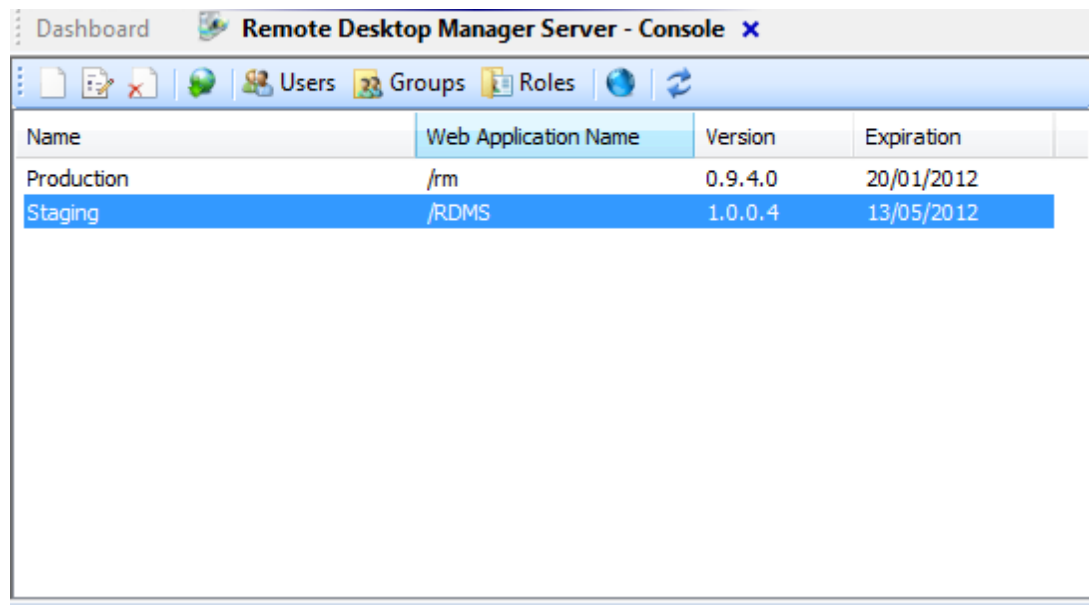
Here is a visual overview of the main features.



3.6.10.4 Remote Desktop Manager Server Console

Description

Accessible from the menu **Tools->Remote Desktop Manager Server Console**



The screenshot shows the 'Remote Desktop Manager Server - Console' window. It has a menu bar with 'Dashboard', 'Users', 'Groups', and 'Roles'. Below the menu is a table with the following data:

Name	Web Application Name	Version	Expiration
Production	/rm	0.9.4.0	20/01/2012
Staging	/RDMS	1.0.0.4	13/05/2012

Remote Desktop Manager Server

Requirements:

- You need to execute the Remote Desktop Manager client with "Run As Administrator".
- IIS needs to be installed as well.

3.6.10.5 PowerShell CmdLets

Description

Remote Desktop Manager supports Windows PowerShell. PowerShell is a powerful scripting shell that lets administrators automate Remote Desktop Manager.

Installing RDM PowerShell Cmdlet snapin

You have two ways of installing the RDM PowerShell Cmdlet snapin. The simplest, start PowerShell using the menu Tools -> PowerShell (RDM Cmdlet) from within RDM. This will automatically register the Cmdlet and load the snapin ready for use. The second is using a script similar to this:

```
set-alias installutil $env:windir\Microsoft.NET\Framework\v2.0.50727\installutil;installutil 'InstallPath
\RemoteDesktopManager.PowerShell.dll';Get-PSSnapin -Name *Remote.Desktop* -Registered | %
{ Write-Host "$_" -NoNewLine; if ( (Get-PSSnapin -Name $_ -ErrorAction SilentlyContinue) -eq $null )
{ Write-Host "installing" -ForegroundColor Yellow; Add-PsSnapin $_ } else { Write-Host "already
installed" -ForegroundColor Green; } }
Install & load snapin (you must change the installpath)
```

Registration must only be done the first time. From now on running the following script will suffice. Adding the following to your [PowerShell profile](#) will make things much simpler.

```
Get-PSSnapin -Name *Remote.Desktop* -Registered | % { Write-Host "$_" -NoNewLine; if ( (Get-
PSSnapin -Name $_ -ErrorAction SilentlyContinue) -eq $null ) { Write-Host "installing" -ForegroundColor
Yellow; Add-PsSnapin $_ } else { Write-Host "already installed" -ForegroundColor Green; } }
Load snapin
```

Note

RDM PowerShell Cmdlet snapin must run under the x86 architecture. Make sure you run the PowerShell (x86) version of PowerShell.

CmdLets

- [Close-RDM-Session](#)
- [Get-RDM-DataSource](#)
- [Get-RDM-Domain](#)
- [Get-RDM-Password](#)
- [Get-RDM-Property](#)
- [Get-RDM-Session](#)
- [Get-RDM-UserName](#)
- [New-RDM-Session](#)
- [Open-RDM-Session](#)
- [Remove-RDM-Session](#)
- [Set-RDM-DataSource](#)
- [Set-RDM-Domain](#)
- [Set-RDM-Password](#)
- [Set-RDM-Property](#)
- [Set-RDM-Session](#)
- [Set-RDM-UserName](#)

3.6.10.5.1 Close-RDM-Session

SYNOPSIS

Close an open session.

SYNTAX

Close-RDM-session [-ID] <Guid> [<CommonParameters>]

DESCRIPTION

You will be prompted to confirm the close session.

PARAMETERS

-ID <Guid>

(Required) Specifies the GUID of the session to be closed.

Must be a valid GUID, in the form {00000000-0000-0000-0000-000000000000}.

-Force

Forces the close session 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 Close-RDM-session -detailed". For technical information, type "Get-Help Close-RDM-session -full".

EXAMPLE 1

```
PS C:\> $list = Get-RDM-Session; Close-RDM-Session $list[1].ID
```

Retrieves the list of available sessions, closes the session at index 1.

EXAMPLE 2

```
PS C:\> Close-RDM-Session "{00000000-0000-0000-0000-000000000000}"
```

Closes session with ID = "{00000000-0000-0000-0000-000000000000}".

EXAMPLE 3

```
PS C:\> Close-RDM-Session -ID "{00000000-0000-0000-0000-000000000000}" -Force
```

Force close of the session with ID = "{00000000-0000-0000-0000-000000000000}".

RELATED LINKS

[Get-RDM-Session](#)

[Open-RDM-Session](#)

3.6.10.5.2 Get-RDM-DataSource**SYNOPSIS**

Retrieve the list of available data sources.

SYNTAX

```
Get-RDM-DataSource [<CommonParameters>]
```

DESCRIPTION

Retrieve the list of available data sources. The current selected data source is marked with an "X".

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-RDM-DataSource -detailed". For technical information, type "Get-Help Get-RDM-DataSource -full".

EXAMPLE 1

```
PS C:\> $list = Get-RDM-DataSource
```

Retrieves the list of available data sources.

EXAMPLE 2

```
PS C:\> $list = Get-RDM-DataSource; $list[0]
```

Retrieves the list of available data sources and displays the first item.

EXAMPLE 3

```
PS C:\> $list = Get-RDM-DataSource; Set-RDM-DataSource $list[1].ID
```

Retrieves the list of available data sources and sets the current data source the the second element

in the list.

RELATED LINKS

[Set-RDM-DataSource](#)

3.6.10.5.3 Get-RDM-Domain

SYNOPSIS

Get the domain from the specified session.

SYNTAX

Get-RDM-Domain [-ID] <Guid> [<CommonParameters>]

DESCRIPTION

Get the domain from the specified session.

PARAMETERS

-ID <Guid>

(Required) Specifies the GUID of the session to get the domain 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 Get-RDM-Domain -detailed". For technical information, type "Get-Help Get-RDM-Domain -full".

EXAMPLE 1

```
PS C:\> $list = Get-RDM-Session; Get-RDM-Domain $list[1].ID
```

Retrieves the list of available sessions and gets the domain from the the second element in the list.

EXAMPLE 2

```
PS C:\> Get-RDM-Domain "{00000000-0000-0000-0000-000000000000}"
```

Get the domain from the session with ID = "{00000000-0000-0000-0000-000000000000}".

RELATED LINKS

[Get-RDM-Session](#)

[Set-RDM-Domain](#)

[Get-RDM-Username](#)

[Set-RDM-Username](#)

[Get-RDM-Password](#)

[Set-RDM-Password](#)

3.6.10.5.4 Get-RDM-Password

SYNOPSIS

Get the password from the specified session.

SYNTAX

Get-RDM-Password [-ID] <Guid> [<CommonParameters>]

DESCRIPTION

Get the password from the specified session. Session must be marked as "Allow copy credentials to clipboard" if not null is returned.

PARAMETERS

-ID <Guid>

(Required) Specifies the GUID of the session to get the password 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 Get-RDM-Password -detailed". For technical information, type "Get-Help Get-RDM-Password -full".

EXAMPLE 1

```
PS C:\> Get-RDM-Password "{00000000-0000-0000-0000-000000000000}"
```

Get the password from the session with ID = "{00000000-0000-0000-0000-000000000000}".

EXAMPLE 2

```
PS C:\> $list = Get-RDM-Session; Get-RDM-Password $list[1].ID
```

Retrieves the list of available sessions and gets the password from the the second element in the list.

RELATED LINKS

[Get-RDM-Session](#)

[Get-RDM-Domain](#)

[Set-RDM-Domain](#)

[Get-RDM-Username](#)

[Set-RDM-Username](#)

[Set-RDM-Password](#)

3.6.10.5.5 Get-RDM-Property

SYNOPSIS

Get the value of property given a session ID and path.

SYNTAX

Get-RDM-Property [-ID] <Guid> [[-Path] <String>] [-Property] <String> [<CommonParameters>]

DESCRIPTION

Protected values will always return null.

Non value types will always return ".ToString()".

PARAMETERS

-ID <Guid>

(Required) Specifies the GUID 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>

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-RDM-Property -detailed". For technical information, type "Get-Help Get-RDM-Property -full".

EXAMPLE 1

```
PS C:\> Get-RDM-Property -ID "{00000000-0000-0000-0000-000000000000}" -Property "Group"
```

Get the Group value from the session with ID = "{00000000-0000-0000-0000-000000000000}".

EXAMPLE 2

```
PS C:\> Get-RDM-Property "{00000000-0000-0000-0000-000000000000}" "MetaInformation" "OS"
```

Get the MetaInformation.OS value from the session with ID = "{00000000-0000-0000-0000-000000000000}".

EXAMPLE 3

```
PS C:\> $list = Get-RDM-Session; Get-RDM-Property -ID $list[1].ID -Path "MetaInformation" -Property "OS"
```

Retrieves the list of available sessions and then returns MetaInformation.OS value of the the second element in the list.

RELATED LINKS

[Get-RDM-Session](#)

[Set-RDM-Property](#)

3.6.10.5.6 Get-RDM-Session

SYNOPSIS

Retrieve the list of available sessions.

SYNTAX

```
Get-RDM-Session [<CommonParameters>]
```

DESCRIPTION

Retrieve the list of available sessions for the current selected data source. Session list contains a column "Session" that can be directly manipulated then updated. (see SetRDMSessionCommand for more detail).

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-RDM-Session -detailed". For technical information, type "Get-Help Get-RDM-Session -full".

EXAMPLE 1

```
PS C:\> $list = Get-RDM-Session; $list[1].Session.Name = "New Name"; Set-RDM-Session $list[1].Session
```

Retrieves the list of available sessions, modify the name of the second session, update the session.

EXAMPLE 2

```
PS C:\> $list = Get-RDM-Session; $list[0]
```

Retrieves the list of available sessions and displays the first item.

EXAMPLE 3

```
PS C:\> Get-RDM-Session
```

Retrieves the list of available sessions.

RELATED LINKS

[Get-RDM-DataSource](#)

[Set-RDM-DataSource](#)

[Set-RDM-Session](#)

3.6.10.5.7 Get-RDM-UserName**SYNOPSIS**

Get the username from the specified session.

SYNTAX

```
Get-RDM-Username [-ID] <Guid> [<CommonParameters>]
```

DESCRIPTION

Get the username from the specified session.

PARAMETERS

-ID <Guid>

(Required) Specifies the GUID of the session to get the password 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 Get-RDM-Username -detailed". For technical information, type "Get-Help Get-RDM-Username -full".

EXAMPLE 1

```
PS C:\> $list = Get-RDM-Session; Get-RDM-Password $list[1].ID
```

Retrieves the list of available sessions and gets the password from the the second element in the list.

EXAMPLE 2

```
PS C:\> Get-RDM-Username "{00000000-0000-0000-0000-000000000000}"
```

Get the username from the session with ID = "{00000000-0000-0000-0000-000000000000}".

RELATED LINKS

[Get-RDM-Session](#)
[Get-RDM-Domain](#)
[Set-RDM-Domain](#)
[Set-RDM-Username](#)
[Get-RDM-Password](#)
[Set-RDM-Password](#)

3.6.10.5.8 New -RDM-Session

SYNOPSIS

Create a new session instance.

SYNTAX

```
New-RDM-session [-Name] <String> [-Host] <String> [-Kind] <String> [<CommonParameters>]
```

DESCRIPTION

Create a new session instance. The instance has not yet been saved. Assign the result to a variable then call "Set-RDM-Session \$s" to save the session.

PARAMETERS

-Name <String>
 (Required) New session name.

-Host <String>
 (Required) New session host.

-Kind <String>
 (Required) New session kind. Must be on of the following:

"Undefined", "RDPConfigured", "RDPFilename", "CommandLine", "VNC", "WebBrowser",
 "LogMeIn", "TeamViewer", "Putty", "Ftp", "VirtualPC", "Radmin", "Dameware", "VMWare",
 "PCAnywhere", "ICA", "XWindow", "HyperV", "AddOn", "RemoteAssistance", "VPN", "VirtualBox",
 "VMRC", "XenCenter", "WindowsVirtualPC", "Group", "Credential", "HpRgs", "DeskTone",
 "ApplicationTool", "SessionTool", "Customer", "DataEntry"

<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-RDM-session -detailed". For technical information, type "Get-Help New-RDM-session -full".

EXAMPLE

```
PS C:\> $session = New-RDM-Session -Name "New Sesion" -Host "myServer" -Kind  
"RDPConfigured";Set-RDM-Session $session
```

Create & save new session.

RELATED LINKS

[Get-RDM-DataSource](#)

[Set-RDM-DataSource](#)

[Set-RDM-Session](#)

[Remove-RDM-session](#)

3.6.10.5.9 Open-RDM-Session

SYNOPSIS

Open the specified session.

SYNTAX

```
Open-RDM-session [-ID] <Guid> [<CommonParameters>]
```

DESCRIPTION

Open the specified session.

PARAMETERS

-ID <Guid>

(Required) Specifies the GUID of the session to get the domain 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 Open-RDM-session -detailed". For technical information, type "Get-Help Open-RDM-session -full".

EXAMPLE 1

```
PS C:\> Open-RDM-Session -ID \"{00000000-0000-0000-0000-000000000000}\"
```

Open the session with ID = \"{00000000-0000-0000-0000-000000000000}\".

EXAMPLE 2

```
PS C:\> $list = Get-RDM-Session; Open-RDM-Session -ID $list[1].ID
```

Retrieves the list of available sessions and opens the second element in the list.

RELATED LINKS

[Close-RDM-Session](#)
[Get-RDM-Session](#)

3.6.10.5.10 Remove-RDM-Session

SYNOPSIS

Delete an existing session.

SYNTAX

Remove-RDM-session [-ID] <Guid> [-NoRefresh] [<CommonParameters>]

DESCRIPTION

You will be prompted to confirm the delete.

PARAMETERS

-ID <Guid>

(Required) Specifies the GUID of the session to be removed.

Must be a valid GUID, in the form {00000000-0000-0000-0000-000000000000}.

-NoRefresh

Do not send refresh notification back to Remote Desktop Manager. This should be used when loop through sessions (for optimization).

-Force

Forces removal of the session 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-RDM-session -detailed". For technical information, type "Get-Help Remove-RDM-session -full".

EXAMPLE 1

```
PS C:\> $list = Get-RDM-Session; Remove-RDM-Session $list[1].ID
```

Retrieves the list of available sessions, deletes session at index 1.

EXAMPLE 2

```
PS C:\> Remove-RDM-Session "{00000000-0000-0000-0000-000000000000}"
```

Delete session with ID = "{00000000-0000-0000-0000-000000000000}".

EXAMPLE 3

```
PS C:\> Remove-RDM-Session -ID "{00000000-0000-0000-0000-000000000000}" -Force
```

Force delete of the session with ID = "{00000000-0000-0000-0000-000000000000}".

RELATED LINKS

[Get-RDM-DataSource](#)
[Set-RDM-DataSource](#)

[Get-RDM-Session](#)

3.6.10.5.11 Set-RDM-DataSource

SYNOPSIS

Set current active data source.

SYNTAX

```
Set-RDM-DataSource [-ID] <Guid> [<CommonParameters>]
```

DESCRIPTION

Set current active data source.

PARAMETERS

-ID <Guid>

Specifies the GUID of the data source to set as the current. (Required)

The value 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 Set-RDM-DataSource -detailed". For technical information, type "Get-Help Set-RDM-DataSource -full".

EXAMPLE 1

```
PS C:\> Set-RDM-DataSource "{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-RDM-DataSource; Set-RDM-DataSource $list[1].ID
```

Retrieves the list of available data sources and sets the current data source the the second element in the list.

RELATED LINKS

[Get-RDM-DataSource](#)

3.6.10.5.12 Set-RDM-Domain

SYNOPSIS

Set the domain from the specified session.

SYNTAX

```
Set-RDM-Domain [-ID] <Guid> [-Domain] <String> [-NoRefresh] [<CommonParameters>]
```

DESCRIPTION

Set the domain from the specified session.

PARAMETERS

-ID <Guid>

(Required) Specifies the GUID of the session to get the domain from.

Must be a valid GUID, in the form {00000000-0000-0000-0000-000000000000}.

-Domain <String>

(Required) New domain name

-NoRefresh

Do not send refresh notification back to Remote Desktop Manager. This should be used when loop through sessions (for optimization).

<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-RDM-Domain -detailed". For technical information, type "Get-Help Set-RDM-Domain -full".

EXAMPLE 1

```
PS C:\> $list = Get-RDM-Session; Set-RDM-Domain -ID $list[1].ID -Domain "MyOtherDomain.com" -NoRefresh
```

Retrieves the list of available sessions and sets the domain from the the second element in the list with no UI refresh.

EXAMPLE 2

```
PS C:\> Set-RDM-Domain "{00000000-0000-0000-0000-000000000000}" "MyOtherDomain.com"
```

Set the domain from the session with ID = "{00000000-0000-0000-0000-000000000000}".

RELATED LINKS

[Get-RDM-Session](#)
[Get-RDM-Domain](#)
[Get-RDM-Username](#)
[Set-RDM-Username](#)
[Get-RDM-Password](#)
[Set-RDM-Password](#)

3.6.10.5.13 Set-RDM-Password

SYNOPSIS

Set the password from the specified session.

SYNTAX

```
Set-RDM-Password [-ID] <Guid> [-Password] <SecureString> [-NoRefresh] [<CommonParameters>]
```

DESCRIPTION

Set the password from the specified session. Session must be marked as "Allow copy credentials to clipboard" if not null is returned.

PARAMETERS

-ID <Guid>

(Required) Specifies the GUID 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 SecurString.

Note: Use either "Read-Host -AsSecureString" or "ConvertTo-SecureString"

-NoRefresh

Do not send refresh notification back to Remote Desktop Manager. This should be used when loop through sessions (for optimization).

<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-RDM-Password -detailed". For technical information, type "Get-Help Set-RDM-Password -full".

EXAMPLE 1

```
PS C:\> Set-RDM-Password -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-RDM-Session; Set-RDM-Password -ID $list[1].ID -Password (Read-Host -AsSecureString "Password")
```

Retrieves the list of available sessions and sets the password from the the second element in the list.

RELATED LINKS

[Get-RDM-Session](#)

[Get-RDM-Domain](#)

[Set-RDM-Domain](#)

[Get-RDM-Username](#)

[Set-RDM-Username](#)

[Get-RDM-Password](#)

3.6.10.5.14 Set-RDM-Property

SYNOPSIS

Set the value of property given a session ID and path.

SYNTAX

```
Set-RDM-Property [-ID] <Guid> [[-Path] <String>] [-Property] <String> [-Value] <Object> [-NoRefresh] [<CommonParameters>]
```



Do not use Set-RDM-Property to change the **username**, **password**, or **domain** properties. Instead use [Set-RDM-UserName](#), [Set-RDM-Password](#) or [Set-RDM-Domain](#)



Do not use Set-RDM-Property to change the **Host** field. There are too many side effects at this time because add-ons perform code whenever the host is changed, this will not occur when going through PowerShell. You should create new sessions when you need to change the host.

DESCRIPTION

Protected values will always return null.

Non value types will always return ".ToString()".

PARAMETERS

-ID <Guid>

(Required) Specifies the GUID of the session to get the password from.

Must be a valid GUID, in the form {00000000-0000-0000-0000-000000000000}.

-NoRefresh

Do not send refresh notification back to Remote Desktop Manager. This should be used when loop through sessions (for optimization).

-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 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-RDM-Property -detailed". For technical information, type "Get-Help Set-RDM-Property -full".

EXAMPLE 1

```
PS C:\> $list = Get-RDM-Session; Set-RDM-Property -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 the second element in the list.

EXAMPLE 2

```
PS C:\> Set-RDM-Property "{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:\> Set-RDM-Property -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}".

RELATED LINKS

[Get-RDM-Session](#)

[Get-RDM-Property](#)

3.6.10.5.15 Set-RDM-Session

SYNOPSIS

Save/set the session.

SYNTAX

```
Set-RDM-Session [-Session] <Session> [-NoRefresh] [<CommonParameters>]
```

DESCRIPTION

Save/set the session. Session must be first fetch via Session property of the Get-RDM-Session cmdlet or via the New-RDM-Session result.

PARAMETERS

-Session <Session>

(Required) Session object, must be retrieved from Get-RDM-Session or created via New-RDM-Session

-NoRefresh

Do not send refresh notification back to Remote Desktop Manager. This should be used when loop through sessions (for optimization).

<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-RDM-Session -detailed". For technical information, type "Get-Help Set-RDM-Session -full".

EXAMPLE 1

```
PS C:\> $list = Get-RDM-Session; $list[1].Session.Name = "New Name"; Set-RDM-Session $list[1].Session
```

Retrieves the list of available sessions, modify the name of the second session, update the session.

EXAMPLE 2

```
PS C:\> $session = New-RDM-Session -Name "New Session" -Host "myServer" -Kind "RDPConfigured"; Set-RDM-Session $session
```

Create & save new session.

RELATED LINKS[Get-RDM-DataSource](#)[Set-RDM-DataSource](#)[Get-RDM-Session](#)[New-RDM-session](#)[Remove-RDM-session](#)

3.6.10.5.16 Set-RDM-UserName

SYNOPSIS

Set the username from the specified session.

SYNTAX

Set-RDM-Username [-ID] <Guid> [-UserName] <String> [-NoRefresh] [<CommonParameters>]

DESCRIPTION

Set the username from the specified session.

PARAMETERS

-ID <Guid>

(Required) Specifies the GUID of the session to get the password from.

Must be a valid GUID, in the form {00000000-0000-0000-0000-000000000000}.

-UserName <String>

(Required)

-NoRefresh

Do not send refresh notification back to Remote Desktop Manager. This should be used when loop through sessions (for optimization).

<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-RDM-Username -detailed". For technical information, type "Get-Help Set-RDM-Username -full".

EXAMPLE 1

```
PS C:\> Set-RDM-Username "{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-RDM-Session; Get-RDM-Password -ID $list[1].ID -Username
```

Retrieves the list of available sessions and gets the password from the the second element in the list.

RELATED LINKS[Get-RDM-Session](#)[Get-RDM-Domain](#)

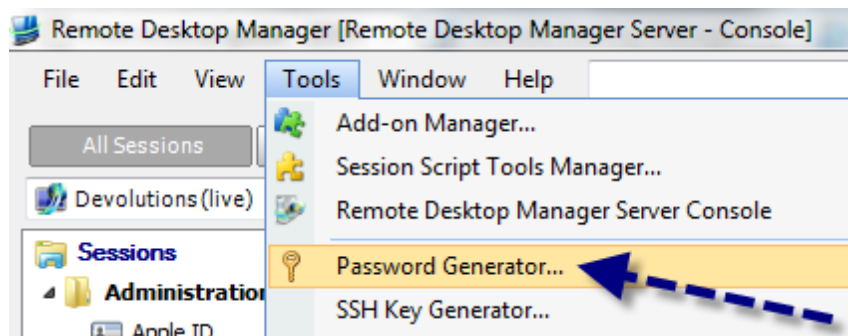
[Set-RDM-Domain](#)
[Get-RDM-Username](#)
[Get-RDM-Password](#)
[Set-RDM-Password](#)

3.6.10.6 Password Generator

Description

The Password Generator enables you to create random passwords that are secure and difficult to interpret or predict, due to a mix of uppercase and lowercase letters, numbers and punctuation symbols.

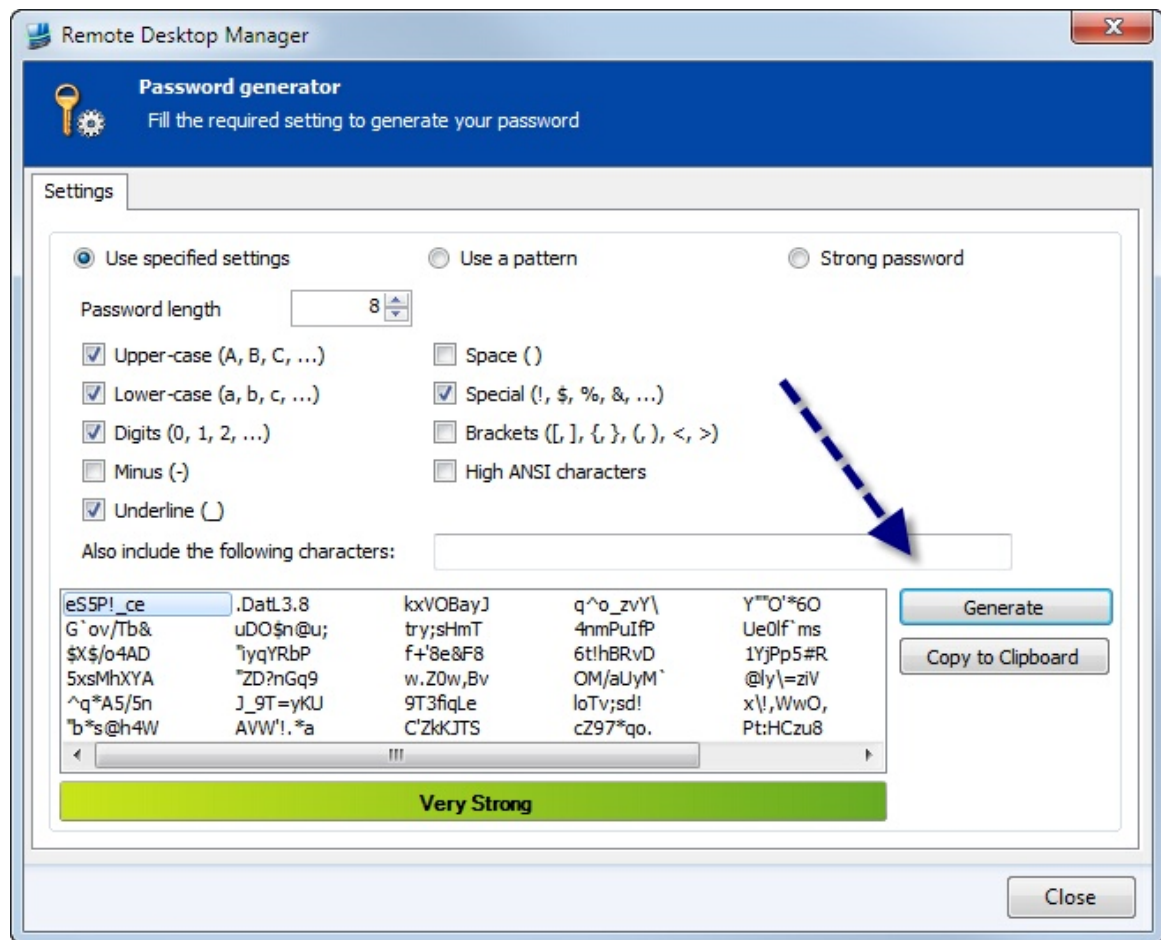
Password Generator is available in **Tools -> Password Generator....**



There are three types of settings:

1. Use the specified settings

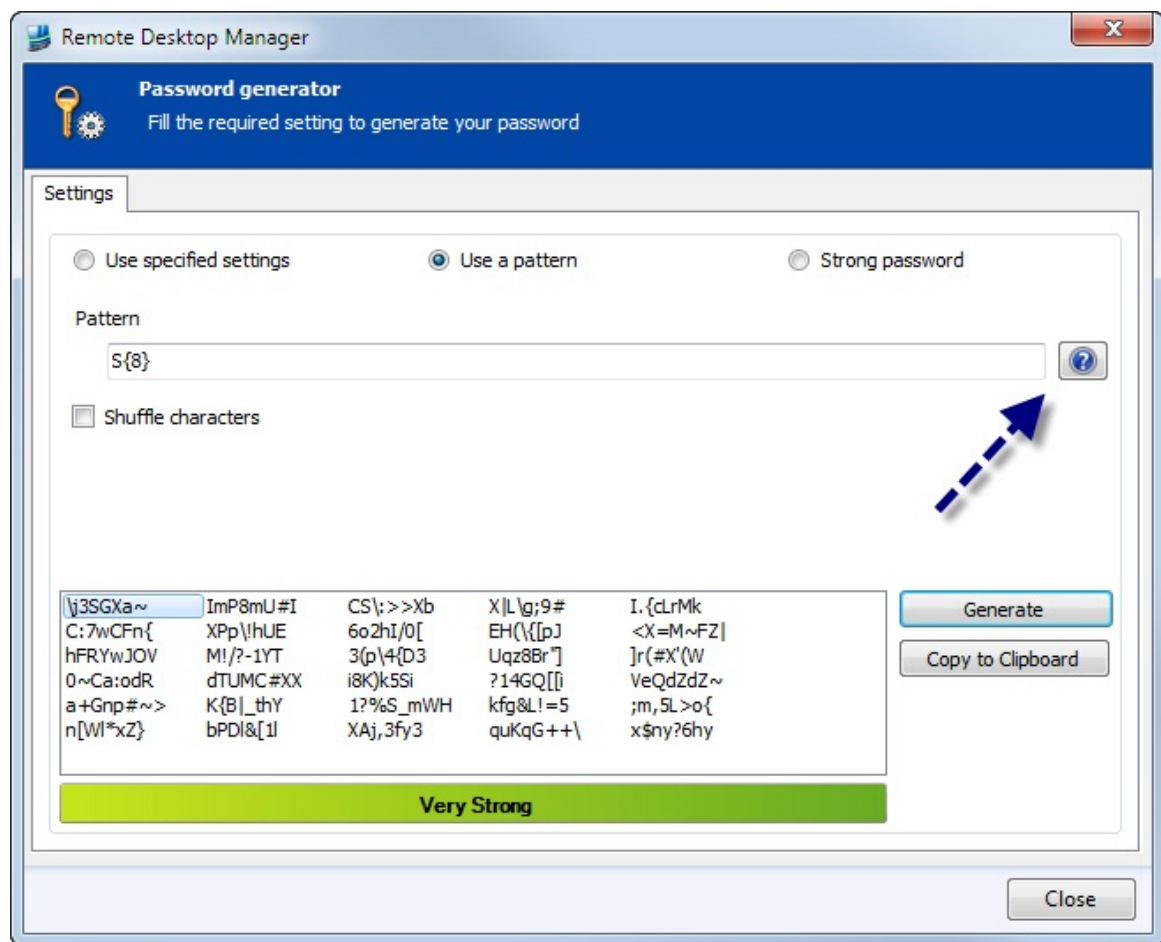
Choose all the character types you desire and generate passwords.



Specified settings

2. Use a pattern

Press the question mark button and select any pattern you need to create your passwords.



Pattern

The following are the supported patterns.

Key	Description	Sample
a	Lower-Case Alphanumeric	abcdefghijklmnopqrstuvwxyz 0123456789
A	Mixed-Case Alphanumeric	ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789
b	Bracket	()[]{}<>
c	Lower-Case Consonant	bcdfghjklmnpqrstvwxyz
C	Mixed-Case Consonant	BCDFGHJKLMNPQRSTUVWXYZ bcdfghjklmnpqrstvwxyz
d	Digit	123456789
h	Lower-Case Hex Character	0123456789 abcdef
H	Upper-Case Hex Character	0123456789 ABCDEF
l	Lower-Case Letter	abcdefghijklmnopqrstuvwxyz
L	Mixed-Case Letter	ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz
p	Punctuation	,.:/;

s	Printable 7-Bit Special Character	!"#\$%&'()*+,-./:;<=>?[\]^_{}~
S	Printable 7-Bit ASCII	A-Z, a-z, 0-9, !"#%&'()*+,-./:;<=>?[\]^_{}~
u	Upper-Case Letter	ABCDEFGHIJKLMNOPQRSTUVWXYZ
U	Upper-Case Alphanumeric	ABCDEFGHIJKLMNOPQRSTUVWXYZ 0123456789
v	Lower-Case Vowel	aeiou
V	Mixed-Case Vowel	AEIOU aeiou
x	High ANSI	From '~' to U255 (excluding U255)
z	Upper-Case Consonant	BCDFGHJKLMNPQRSTVWXYZ
Z	Upper-Case Vowel	AEIOU
\	Escape (Fixed Char)	Use following character as is
{n}	Escape (Repeat)	Repeats the previous character <i>n</i> times
[x]	Custom character	Define a custom character sequence

3. Strong password

Remote Desktop Manager will generate an 8 character password with mixed case alphanumerics and special characters.

The screenshot shows the 'Settings' dialog box for Remote Desktop Manager. The 'Strong password' option is selected. Below the options, there is a grid of generated password candidates. The first candidate, '19YczEQ[', is highlighted. To the right of the grid are 'Generate' and 'Copy to Clipboard' buttons. At the bottom, a green bar indicates the password strength as 'Very Strong'.

19YczEQ[0MgFI95_	eL6MI+2K	BJ8I939\$	Y29s<5W9
a_2L2Id6	y5ap3^Nj	sC85 7vN	BY4#q08E	61=hcF7J
>UZ4c3uP	0Lgd3N1^	~M06LE43	Y5Ih7~3u	0~4o3wBA
Y:uA73h1	HU50~suF	T)9Fc2Qv	7hLA%dJ6	h22nYY1&
7Ep>Sn34	(jS30nxP	V)sPb03U	X5,TCj5g	7Fi9]Q0y
	T6Gh"sL1	rA69=YrQ	6FQzsR9	G+76bS40

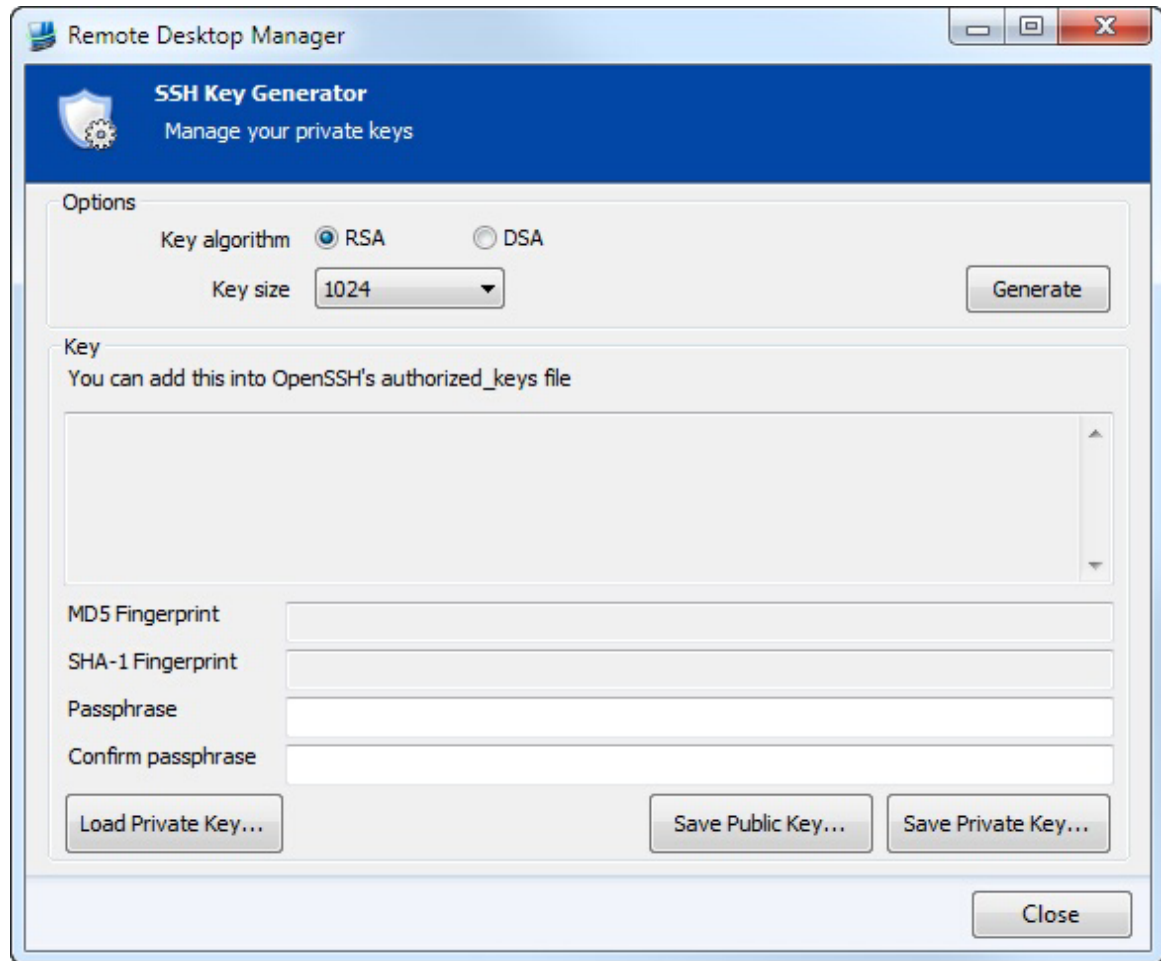
Very Strong

Strong password

3.6.10.7 SSH Key Generator

Description

This tool allows the creation of key files.



SSH Key Generator dialog

Workflow

Generating a key

1. Choose your type of key: RSA or DSA.
2. Choose the desired key size. The available list is different for each key type.
3. Click on **generate**, you will see a popup message informing you that the newly generated key has been copied to the clipboard. The key will also be displayed in the central area.

Loading a private key

This feature will allow you import a key, in order to export in various formats.

Saving the public key

Saving the public key will generate a *.pub file. Simply enter a file name when prompted.

Saving the private key

Saving the private key will generate your choice of:

- PKCS #8 Private Key (*.pri)
- PuTTY Private Key (*.ppk)
- OpenSSH Private Key (*.pri)

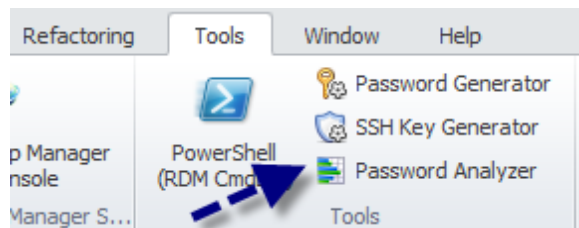
If you did not specify a passphrase you will have to confirm that this is what you desire.

3.6.10.8 Password Analyzer

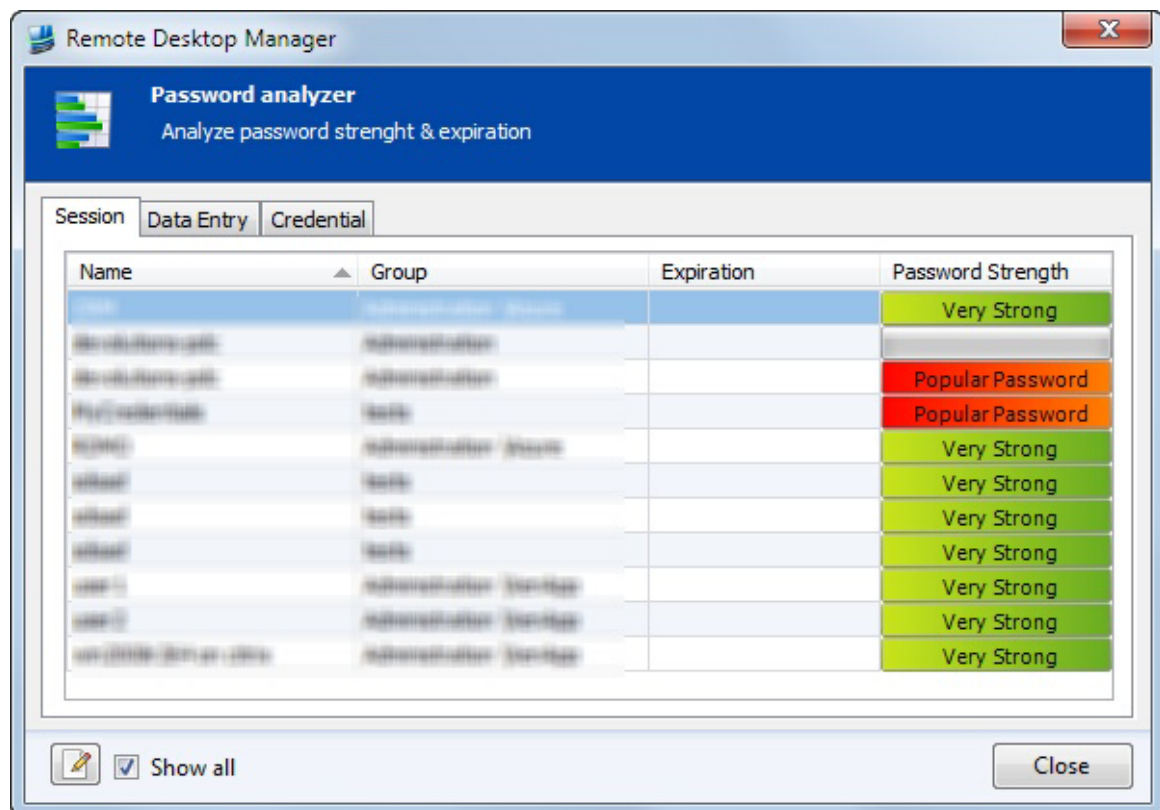
Description

The password Analyzer will display a strength indicator for all passwords that are stored with your various entries.

It is accessible from from the **Tools->Password Analyzer...** menu



Password Analyzer button in the ribbon



Password Analyzer

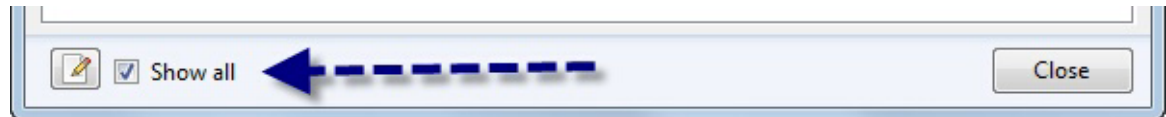
Settings

The dialog displays three tabs:

- *Sessions*
- *Data Entry*
- *Credential*

In a single glance you can see the strength ratings of your stored passwords.

Two controls can be seen at the bottom left.



Control highlight

The button is to open the current entry so you can edit it. The checkbox, when unchecked, will display only entries with actual passwords stored in them.

3.6.10.9 Local RDP/RemoteApp Manager

Description

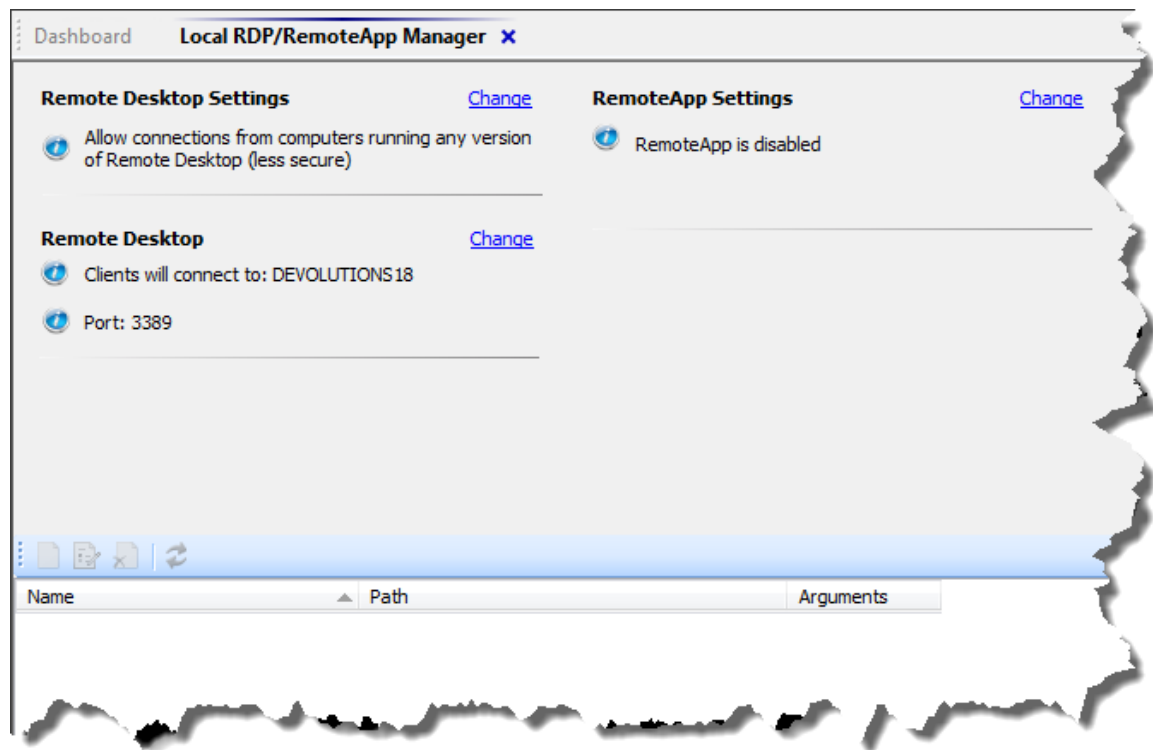
Easily manage local RDP settings and configure RemoteApp.

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. Why? 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.

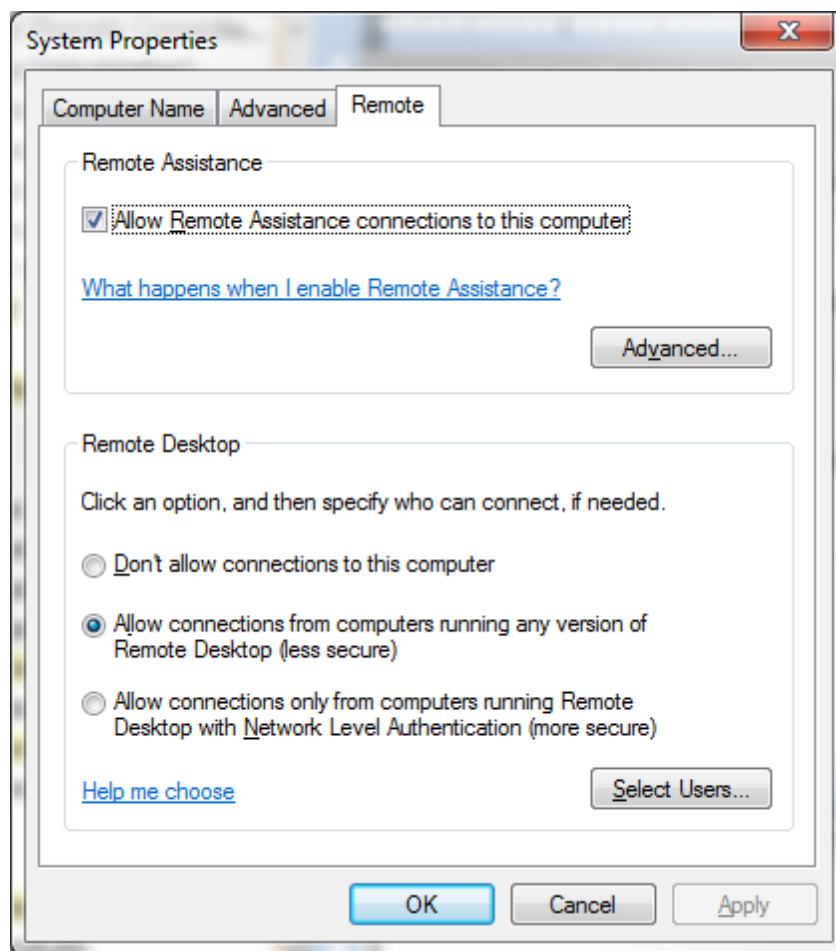
Console

Tools -> Local RDP/RemoteApp Manager menu



Local RDP/RemoteApp Manager console

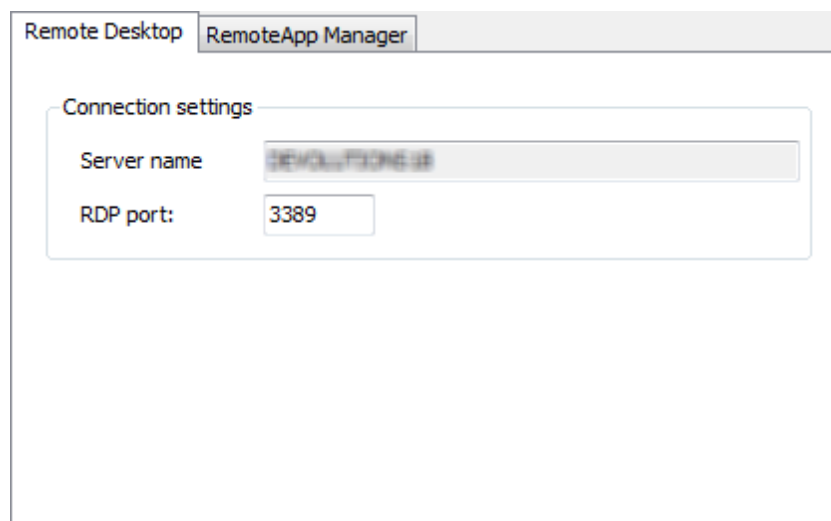
Remote Desktop Settings



Remote Assistance/Desktop System Properties

Remote Desktop

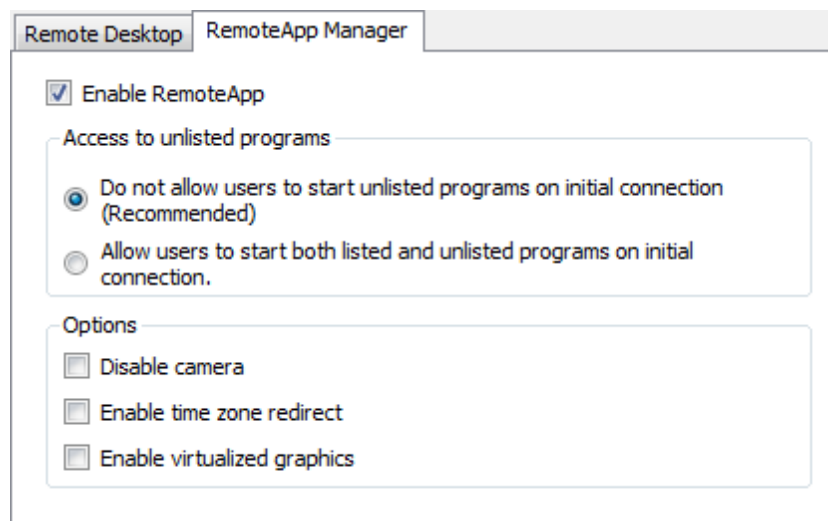
Allows you to modify the local RDP port.



Local RDP

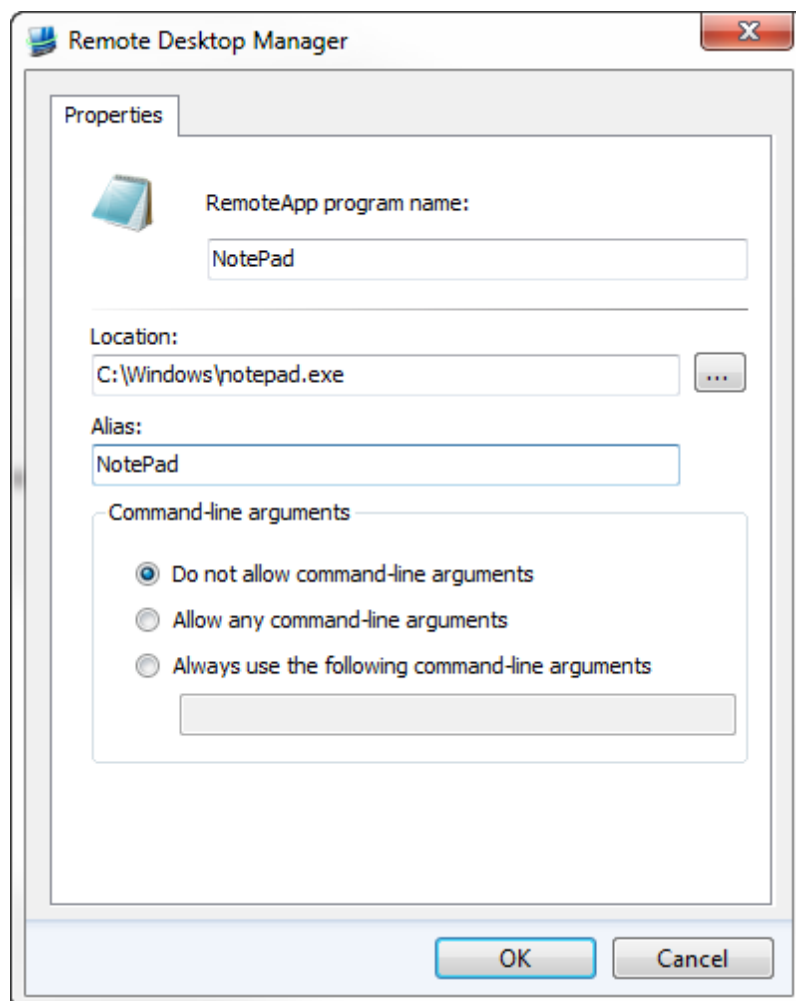
Enable RemoteApp

- Start Remote Desktop Manager using Run as Administrator on the machine that you want to enable RemoteApp functionality
- Start RemoteApp Manager Console (Tools -> Local RDP/RemoteApp Manager)
- Enable RemoteApp on the machine.



RemoteApp settings

- Add a new RemoteApp

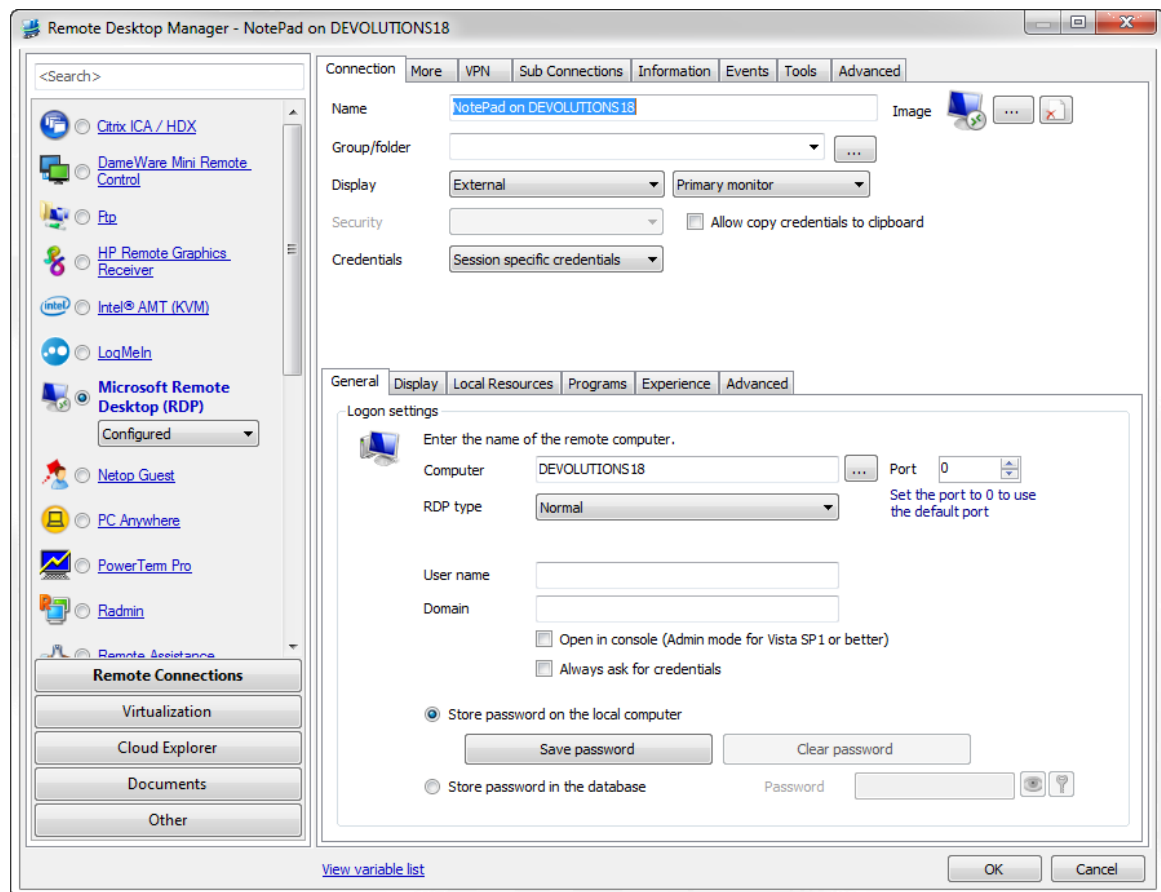


NotePadd RemoteApp settings

- Configure a client RDP session to launch the NotePad RemoteApp

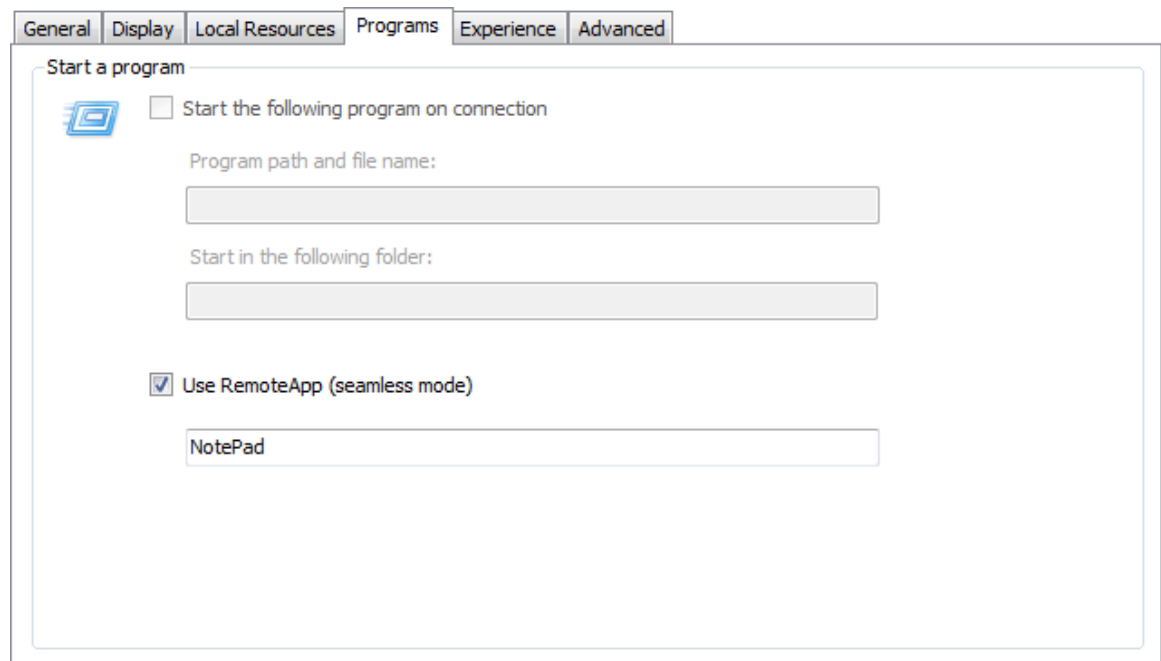
Create a RemoteApp Session

- Start Remote Desktop Manager
- Create new RDP Session



New RDP Session

- Select the Programs tab



Programs Tab

- Enter name of the RemoteApp
- Save & launch the session, you will have the RemoteApp running locally.

3.6.10.10 Macros/Scripts/Tools

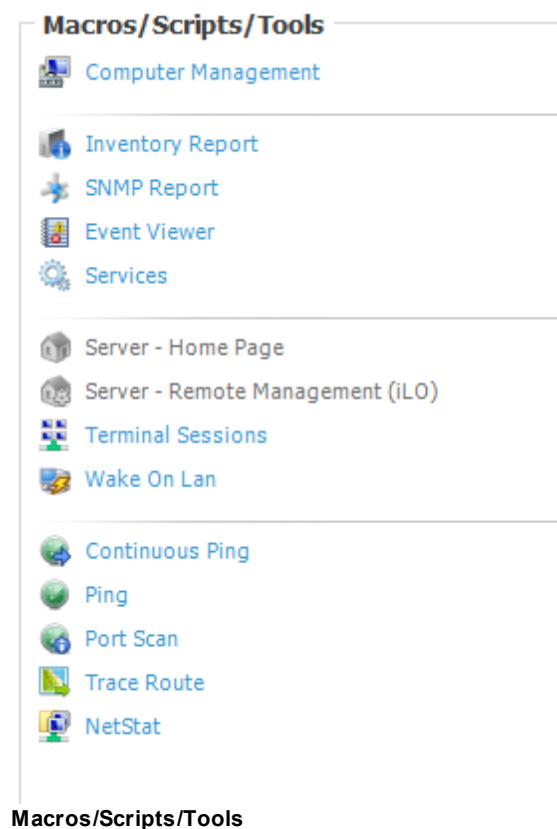
3.6.10.10.1 Overview

Description

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

There are three types of tools:

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



Built-in Tools

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

Option	Description
--------	-------------

Computer Management	Opens the Computer Management snap-in for a remote machine.
Inventory Report	Open a Inventory Report for a remote machine.
SNMP Report	Open the SNMP Report for a device on the network.
Event Viewer	Open the Event Viewer for a remote machine.
Services	Open the Windows Services manager for a remote machine.
Server - Home Page	Opens a web page if a home page is configured in the Information tab of the session configuration.
Server - Remote Management (iLO)	Opens a web page, if a remote management link (e.g. iLo) is configured in the Information Tab of the session configuration.
Terminal Sessions	Opens the Remote Desktop Manager Terminal Services dashboard for the selected session, so that you can: <ul style="list-style-type: none"> • View opened sessions • View the running processes • Send a message • Restart the machine • Logoff the selected user • Shutdown the machine
Wake On Lan	Sends a command for the Wake-on-Lan .
Continuous Ping	Opens the ping of Remote Desktop Manager and perform a continuous ping.
Ping	Opens the ping of Remote Desktop Manager and returns the result.
Port Scan	Opens the port scan of Remote Desktop Manager and returns the result.
Trace Route	Display the route and measuring transit delays of packets across an network.
NetStat	Display network statistics to find problems on the network.

Add-on Session Tool

You can extend the built-in list using the SDK and installing the compiled add-on. The new tools will be displayed below the built-in tool list in the menu and the dashboard. By creating your own add-ons, you gain more control on the implementation including execution, configuration and monitoring.

You can use the [Add-on Manager](#), or download them directly from our [website](#).

Macros/Scripts/Tools

The session script tool can be a script, a command line, or an helper applicable to a selected session. They can be configured and shared in the data source. They are listed in the dashboard under the session tool section.

For more information, see topic [Macros/Script/Tools](#).

3.6.10.10.2 Wake-on-LAN

Description

Wake-on-LAN is an Ethernet computer networking standard, which allows a computer to be turned on or

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

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

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

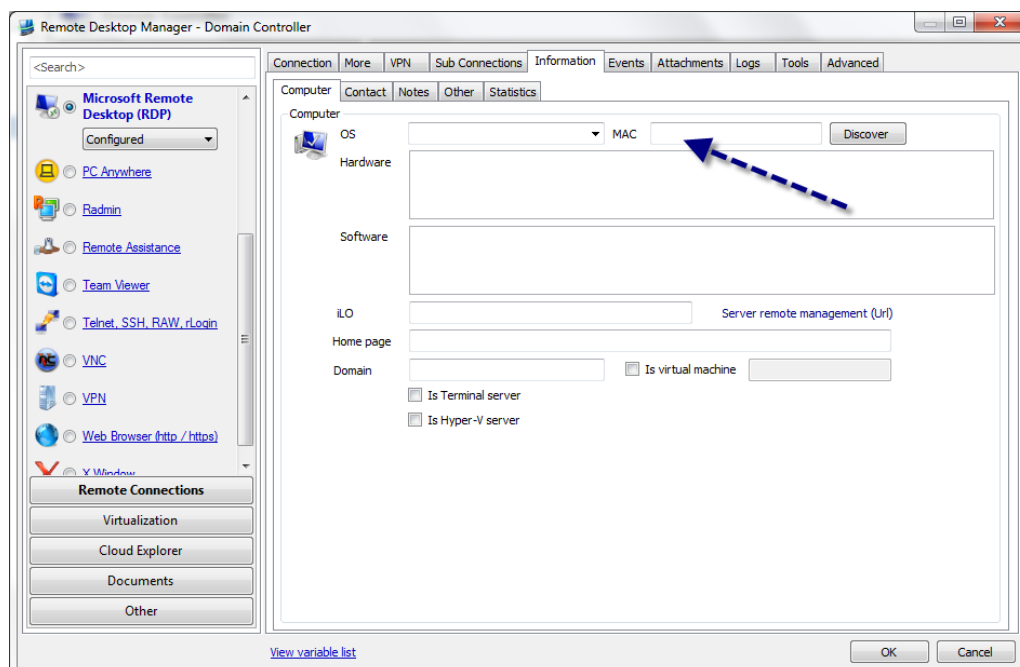
Enabling Wake-on-LAN

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

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

Configure Remote Desktop Manager

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



Session configuration - Wake-on-LAN

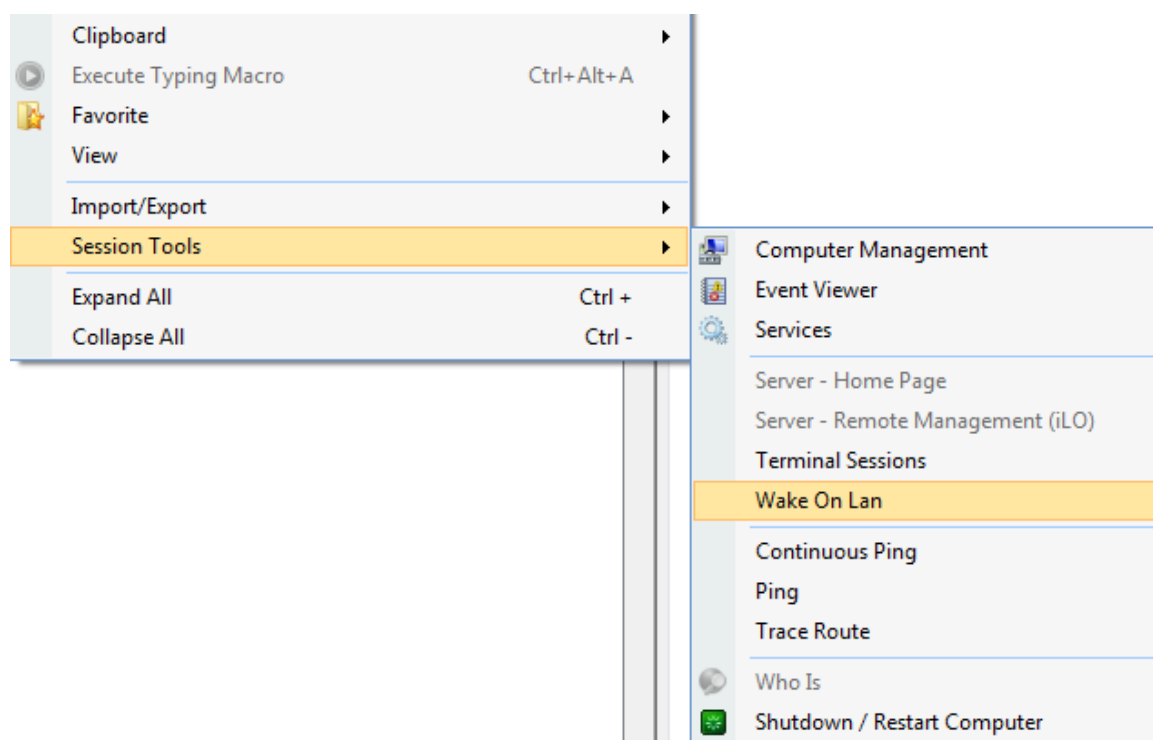
You can use the Discover button to automatically determine the MAC address. If this is unsuccessful, you will need to enter it manually.

About the MAC address discovery

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

Use Wake-on-LAN

If the settings are correctly configured, you can invoke the Wake-on-LAN from the session's context menu, which can be found in the **Session Tools > Wake On Lan** menu.



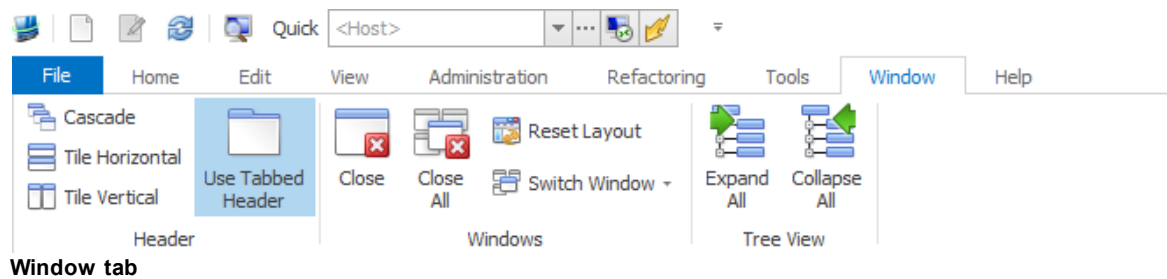
Session tools - Wake-on-LAN

3.6.11 Window

3.6.11.1 Overview

Description

The Window tab manages the different window layouts in Remote Desktop Manager.



The sections are:

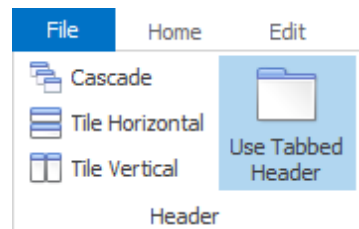
- [Header](#)
- [Windows](#)
- [Tree View](#)

3.6.11.2 Header

Description

The Header section allows you to display your windows in different mode.

Settings



Cascade

Displays the sessions in cascade mode.

Tile Horizontal

All the sessions will be displayed one under an other.

Tile Vertical

All the sessions will be displayed side by side.

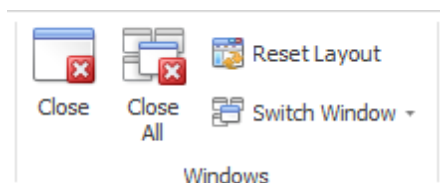
Use Tabbed Header

Sessions are displayed in separate tabs instead of MDI windows.

3.6.11.3 Windows

Description

The Windows section allows you to close your sessions, switch between them or reset the application layout.



Windows section

Close

Close the active session tab.

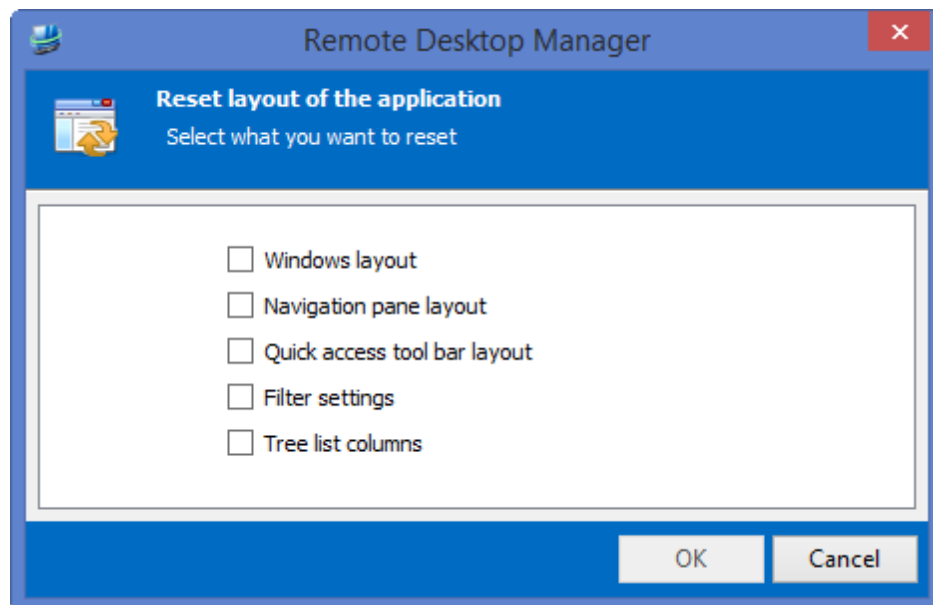
Close All

Close all the opened session tabs.

Switch Window

Used to easily switch between the different opened sessions when you have multiple connections opened. All the tab pages including the dashboard will be listed in the drop down.

Reset Layout



Reset Layout

Option	Description
Windows layout	Resets window layout to the original state.

Navigation pane layout	Reset the Navigation pane layout and automatically switch to the tree view mode.
Quick access tool bar layout	Reset the Quick access tool bar buttons.
Filter settings	Reset the filter/search field.
Tree list columns	Remove all columns in the Navigation Pane except the name column.

3.6.11.4 Tree View

Description

The Tree View section allows you to expand or collapse your entry groups in the navigation panel.



Expand All

Expand all the groups in the Navigation pane when the Tree view mode is used.

Collapse All

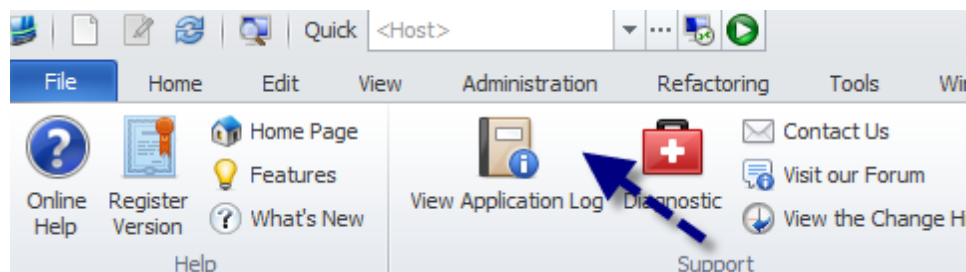
Collapse all the groups in the Navigation pane when the Tree view mode is used.

3.6.12 Help

3.6.12.1 Application Logs

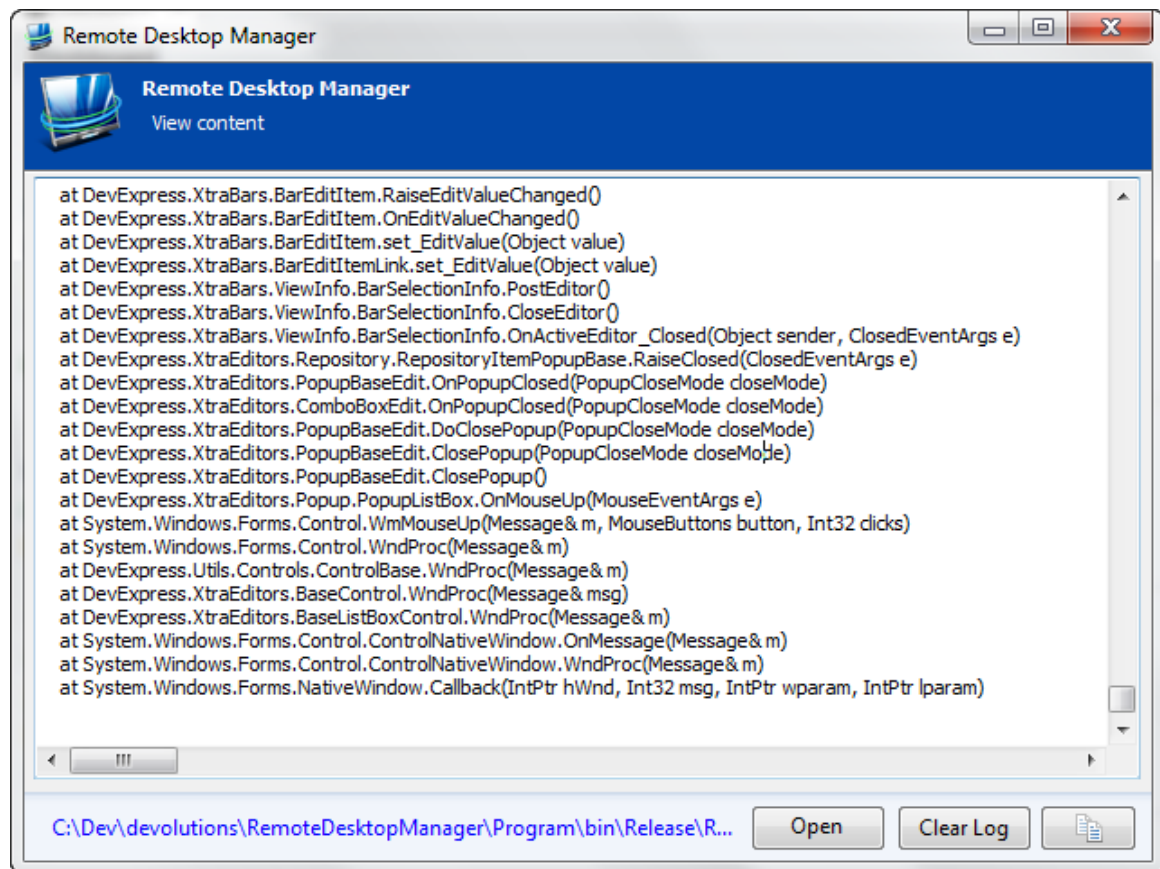
Description

In case of error, you can verify the local application log, which is available from the menu in **Help > View Application Log...**



View Application Log button

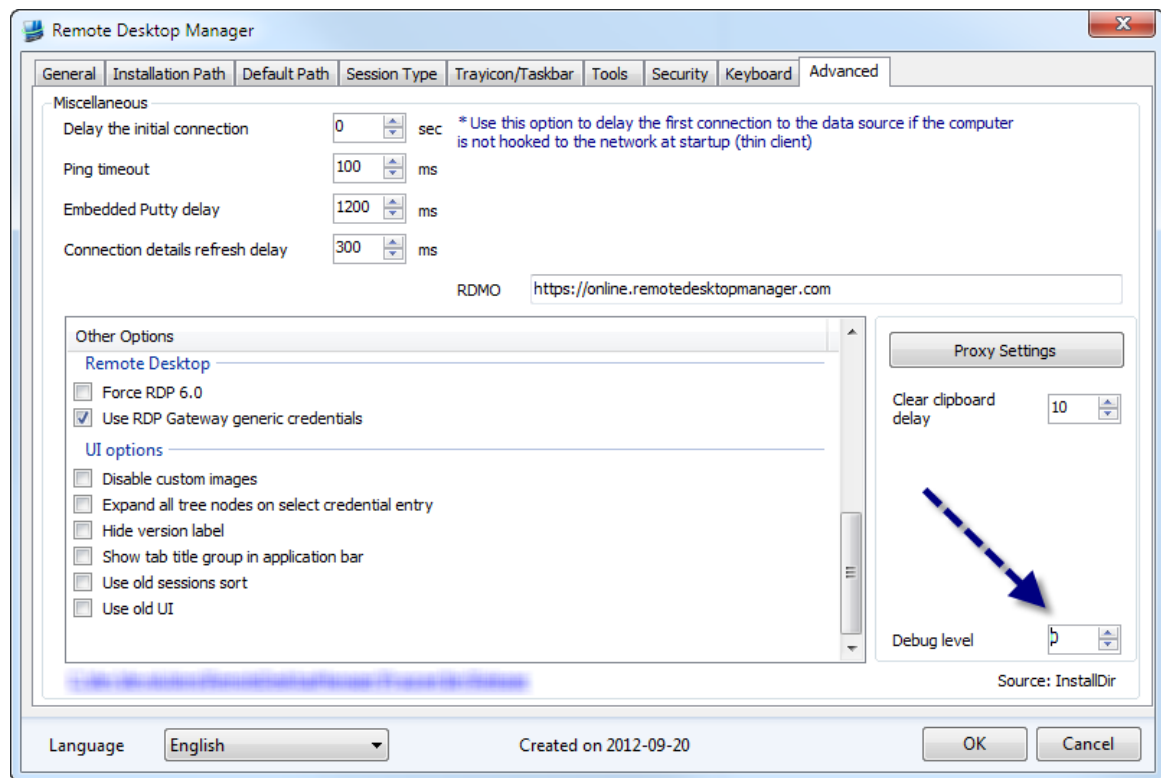
Those logs are saved in in %LocalAppData%\Devolutions\RemoteDesktopManager\RemoteDesktopManager.cfg



View Application Logs dialog

Increasing the log level

When requested by a Devolutions employee during a support process, you may be asked to increase the log level of the application to a higher level.

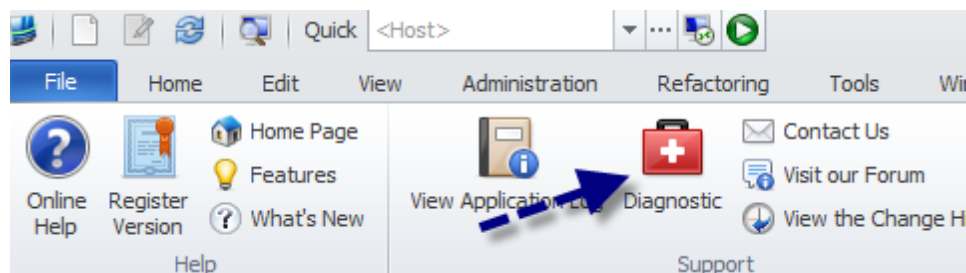


Advanced options tab

3.6.12.2 Diagnostic

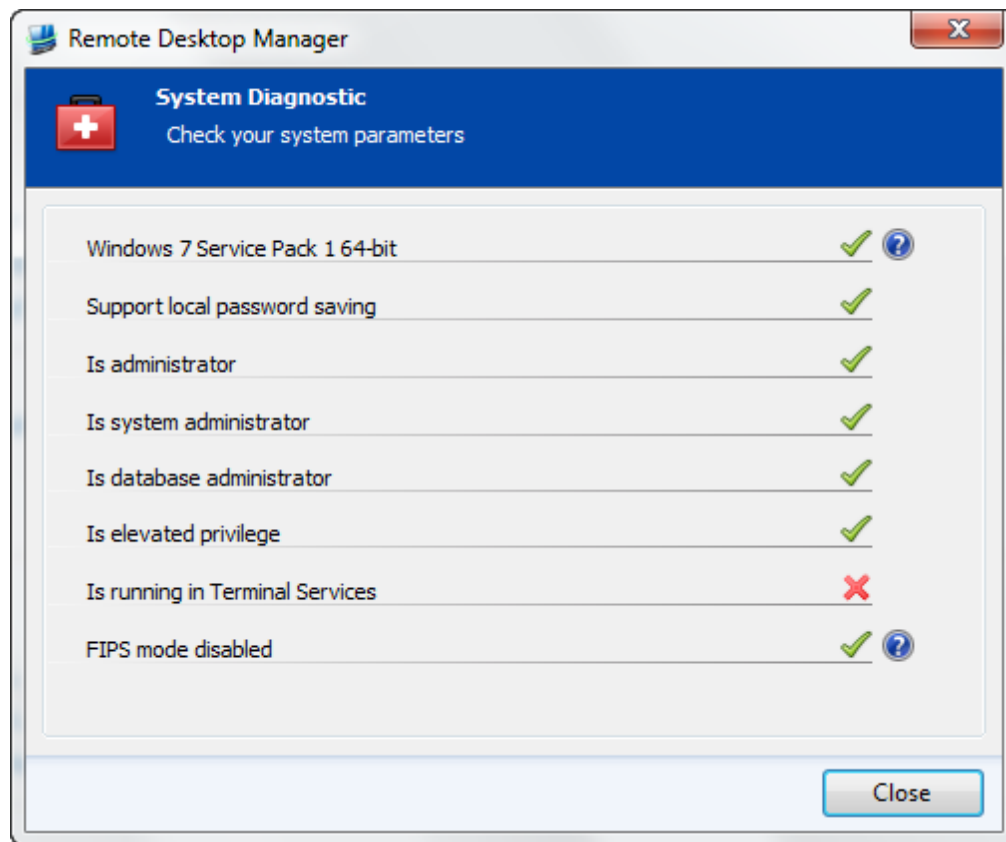
Description

If you encounter a problem, you can run the system diagnostic available from the menu in **Help > Diagnostic...**



System Diagnostic button

This will help us find diagnose the problem that you might have.



System Diagnostic dialog

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.

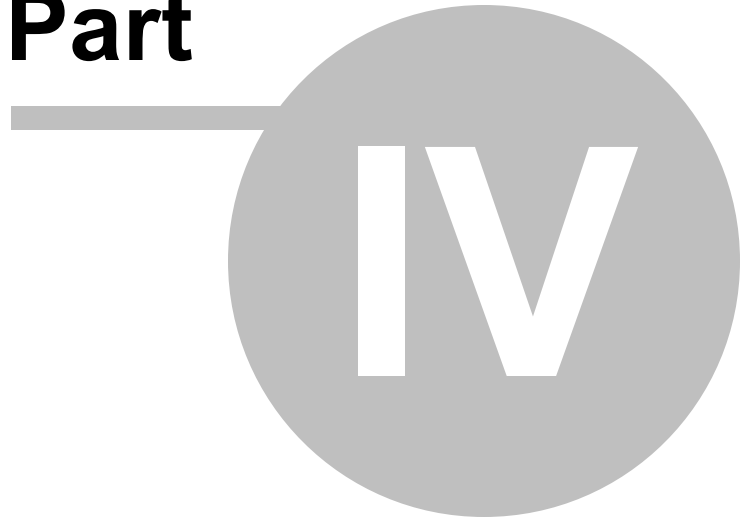
FIPS related issue and solutions can be found in the specific [FIPS \(Encryption\)](#) trouble shooting section.



Please read the [Troubleshooting](#) topic, it lists error messages and could contain the fix/workaround for your problem.

Data Sources

Part



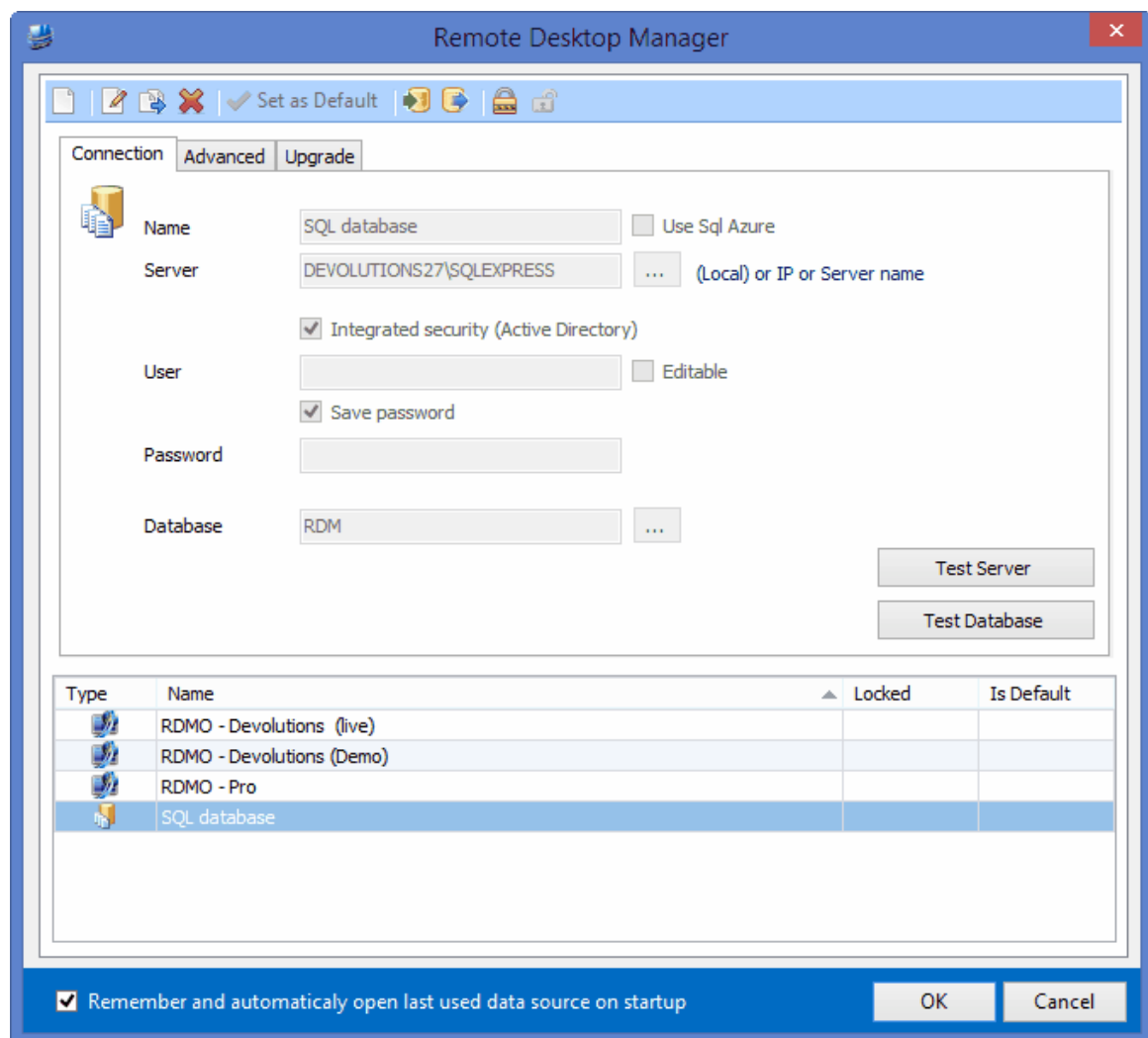
4 Data Sources

4.1 Overview

Description

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

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

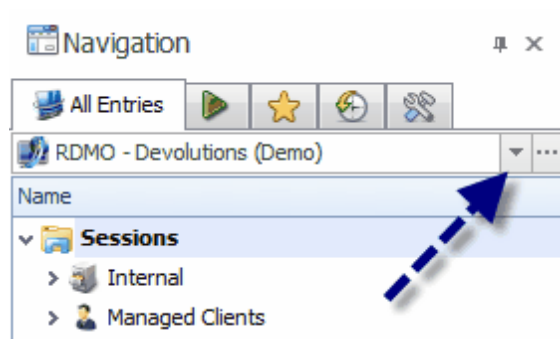


Data source configurations

Multiple Data Sources

You can configure multiple data sources within the application. These data sources can be of mixed types but there is only one active at a time.

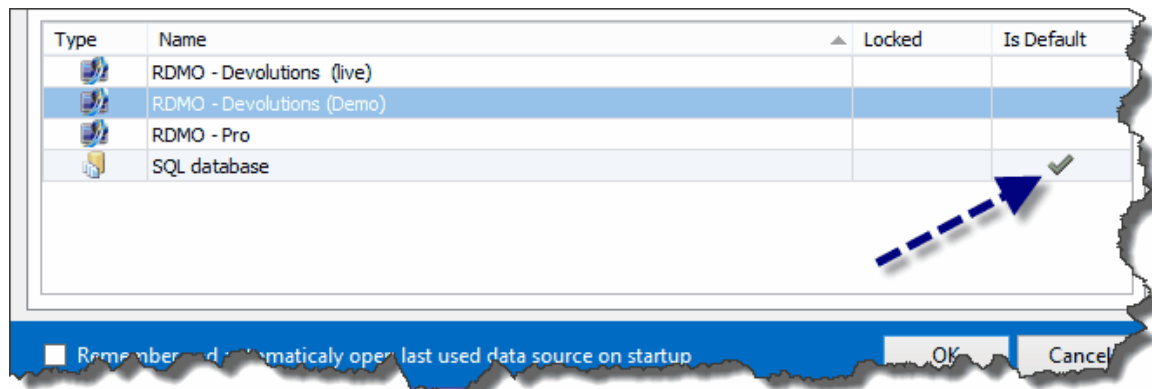
It is possible to switch from one data source to another via the data source combo box.



Choose your current data source

Default Data Source

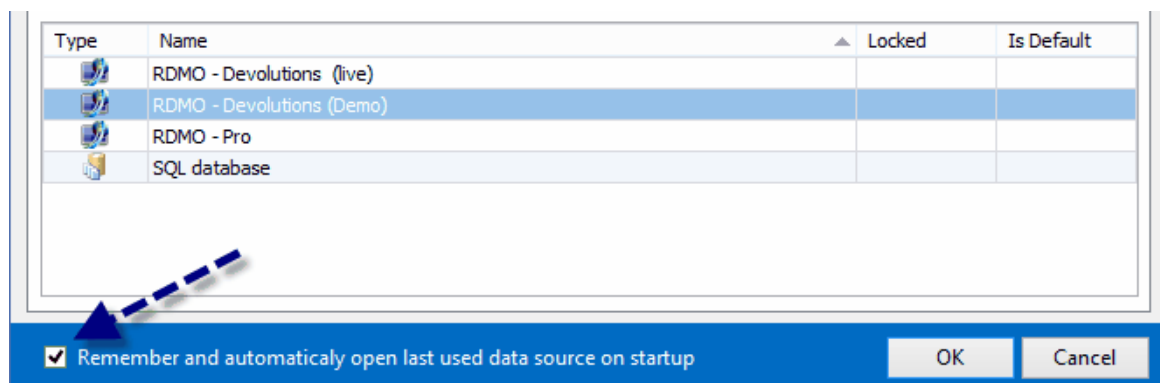
You may assign a default data source in the data source dialog. The default data source will be open when Remote Desktop Manager starts. This option is disabled if you activate the remember last data source settings. See the other section for more details.



Default data source

Re-open Last Data Source at Startup

Instead of selecting a default data source, you can check ***Remember and automatically open last used data source on startup*** and the last data source you used will open at startup. This is the default setting for the new application installation.



Remember and automatically open last used data source on startup

Data Source Settings

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




4.1.1 Data Source Types




Description






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



If you're running the Standard edition, you'll be running from the local data source which is a SQLite database by default.

Data Source Types

Name	Description	Pros and cons
Remote Desktop Manager Online 	Remote Desktop Manager connects to Devolutions' online repository. For more information, please consult Remote Desktop Manager Online (RDMO) topic.	Pros: <ul style="list-style-type: none"> • Quick • Reliable • Secure • Supports all features, such as attachments, connection log, Offline Mode and security management • SQL Server Express is free Cons: <ul style="list-style-type: none"> • Not hosted internally • This will not be free permanently
SQLite 	Remote Desktop Manager uses a SQLite database to store session information. For more information, please consult SQLite topic.	Pros: <ul style="list-style-type: none"> • Quick • Reliable • The database is free • Supports all features, such as attachments, connection log, Offline Mode and security management Cons: <ul style="list-style-type: none"> • SQLite needs to be installed
XML file storage 	Remote Desktop Manager saves the settings directly in a file with the XML format. For more information, please consult XML topic.	Pros: <ul style="list-style-type: none"> • Easy backup • Can be edited manually or by an external system • Nothing to install Cons: <ul style="list-style-type: none"> • No possibility of sharing • No security management • There is a possibility for conflict or data corruption to occur

		<ul style="list-style-type: none"> Doesn't support all features, such as attachments, connection logs and security access
<p>Amazon S3 storage</p> 	<p>Remote Desktop Manager saves the settings in a file located in an Amazon S3 bucket.</p> <p>Amazon S3 is a storage service for the Internet. It's designed to make cloud computing accessible to everyone.</p> <p>Amazon S3 provides a simple web services interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the web. Remote Desktop Manager uses its API to persist your session settings.</p> <p>More details on cloud computing and Amazon S3 can be found at: http://aws.amazon.com/s3/</p> <p>For more information, please consult Amazon S3 topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> Can be shared in read-only mode Backups (by Amazon) are automatic <p>Cons:</p> <ul style="list-style-type: none"> You must have an Amazon account and pay storage and transfer fees, although most would agree they are minimal. No security management There is a possibility of conflicts or data corruption to occur Doesn't support all features, such as attachments, connection logs and security access
<p>Dropbox</p> 	<p>Remote Desktop Manager uses the Dropbox API to retrieve the XML file from the configured repository.</p> <p>For more information, please consult Dropbox topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> Can be shared in read-only mode Backups (by Dropbox) are automatic Storage infrastructure is free (if within your free storage quota) <p>Cons:</p> <ul style="list-style-type: none"> No security management There is a possibility for conflict or data corruption to occur Doesn't support all features, such as attachments, connection logs and security access
<p>FTP</p> 	<p>Remote Desktop Manager uses an FTP connection to retrieve the XML file.</p> <p>For more information, please consult FTP topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> Can be shared in read-only mode Easy to deploy online <p>Cons:</p> <ul style="list-style-type: none"> 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 security access
<p>MariaDB</p>	<p>Remote Desktop Manager uses MariaDB as a drop-in replacement for MySQL.</p>	<p>Pros:</p> <ul style="list-style-type: none"> Quick Reliable

	<p>For more information, please consult MariaDB topic.</p>	<ul style="list-style-type: none"> • The database is free and can be installed on Linux • Supports all features, such as attachments, connection log, Offline Mode and security management <p>Cons:</p> <ul style="list-style-type: none"> • MySQL needs to be installed
<p>Microsoft Access</p> 	<p>Remote Desktop Manager saves the settings in a Microsoft Access database on the local machine, or on a network share.</p> <p>Microsoft Access is a pseudo relational database management system from Microsoft, which combines the relational Microsoft Jet Database Engine with a graphical user interface and software development tools.</p> <p>For more information, please consult Microsoft Access topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Easy setup • Can be shared • Easy backup <p>Cons:</p> <ul style="list-style-type: none"> • Slower than SQL Server • 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 security access
<p>Microsoft SQL Server/ SQL Azure</p> 	<p>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.</p> <p>For more information, please consult SQL Server/SQL Azure (MSSQL) topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Quick • Reliable • Secure • Supports all features, such as attachments, connection log, Offline Mode and security management • SQL Server Express is free <p>Cons:</p> <ul style="list-style-type: none"> • SQL Server must be installed
<p>MySQL</p> 	<p>Remote Desktop Manager uses a MySQL database to store session information.</p> <p>For more information, please consult MySQL topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Quick • Reliable • The database is free and can be installed on Linux • Supports all features, such as attachments, connection log, Offline Mode and security management <p>Cons:</p> <ul style="list-style-type: none"> • MySQL needs to be installed
<p>Remote Desktop Manager Server</p> 	<p>Remote Desktop Manager uses Remote Desktop Manager Server to store session information.</p> <p>For more information, please consult Remote Desktop Manager Server (RDMS) topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Quick • Reliable • Secure • Supports all features, such as attachments, connection log, Offline Mode and security management

		<ul style="list-style-type: none"> • SQL Server Express is free • Active Directory integration <p>Cons:</p> <ul style="list-style-type: none"> •
SFTP 	<p>Remote Desktop Manager uses a Secure FTP connection to retrieve the XML file.</p> <p>For more information, please consult SFTP topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Can be shared in read-only mode • Easy to deploy online <p>Cons:</p> <ul style="list-style-type: none"> • 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 security access
Web 	<p>Remote Desktop Manager uses a Web connection to retrieve the XML file.</p> <p>For more information, please consult Web topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Easy backup • Can be edited manually or by an external system • Nothing to install <p>Cons:</p> <ul style="list-style-type: none"> • No possibility for sharing • Read-only • Doesn't support all features, such as attachments, connection logs and security access

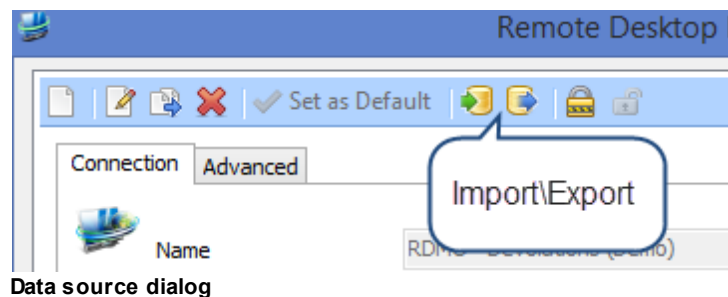
Data Source Types

4.1.2 Import/Export Data Source

Description

You can simplify the deployment for multiple users by exporting and importing the data source configuration. The generated file will have a .rdd extension and will 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 other [Export](#) functionalities to [Backup](#) or copy the database content.

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



Data source dialog

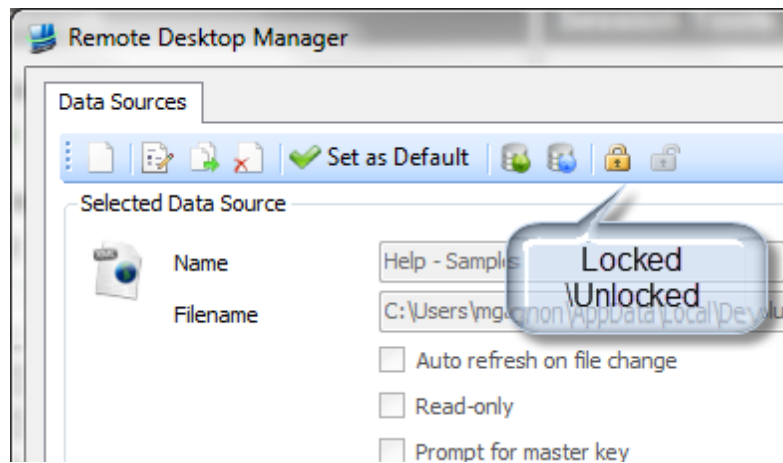


A locked data source can be exported and imported, but its content will not be accessible for use unless a password is entered when the data source is selected. See [Lock Data Source](#) for more information.

4.1.3 Lock Data Source

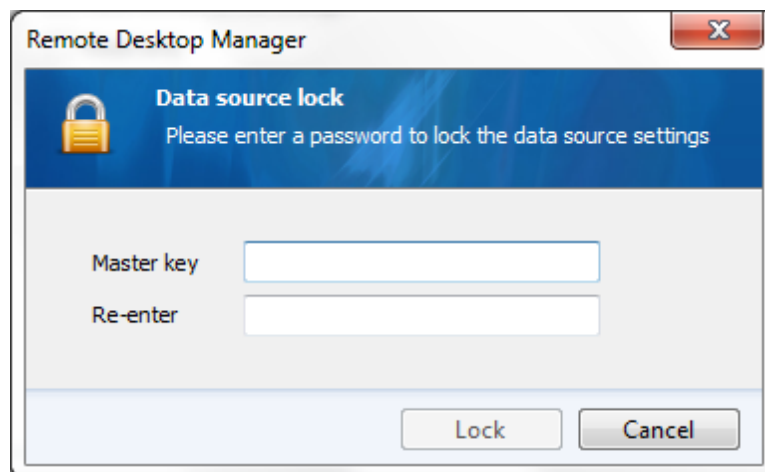
Lock Data Source

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



Lock data source toolbar

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.



Lock data source dialog



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

4.1.4 Caching

Description

The caching mode will determine how the client will re-load entries when changes are detected. On large data sources caching is a must and will increase performance significantly.



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



If you feel the cache is outdated, press CTRL while you click on refresh, this will force reading from the database to recreate the cache.

Settings

Modes

Offline mode	Read/write	<input type="checkbox"/> Prompt for offline mode on startup
Caching mode	Intelligent	
Auto refresh	Intelligent	
Connection timeout	30 sec	
Command timeout	60 sec	

Data source configuration - Caching mode

Option	Description
Disabled	No client caching.
Simple	Simple caching is the legacy caching mode. Performance may suffer when connected to data sources containing many sessions. On a modification of data within a data source the server cache token is changed. When Remote Desktop Manager performs a refresh it will compare it's local cache token with the data source token. In the case where has changed the entire data source is reloaded.
Intelligent	Intelligent cache has the ability to handle many more sessions without experiencing performance degradation. In the case of intelligent cache each modification performs a token update on the server. When Remote Desktop Manager performs a refresh action it will query the data source for any changes (delta) of changes to be applied client side since it last checked the data source. The delta of the changes is then sent to the application and applied locally. When first opening the data source Remote Desktop Manager will loaded the session from the offline file then refresh to get the up-to date information.

Storage

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

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



You can enhance the security of the offline file by setting the Enhanced security in the options. See topic [Offline Security](#)



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

4.1.5 Offline

Description

The offline mode enables users to see/manipulate their sessions while disconnected from the data source. This is extremely useful for offsite personnel or when working in environments that have sporadic network availability.

- When connected via VPN to clients network
- Working from home
- Working offsite



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

Settings

Offline Modes

Offline mode	Read/write	<input type="checkbox"/> Prompt for offline mode on startup
Caching mode	Disabled	
Auto refresh	Read-only	
	Read/write	
	0	sec
Connection timeout	5	sec
Command timeout	60	sec
	<input type="checkbox"/> Disable lock	

Data source configuration - Offline mode

Option	Description
--------	-------------

Disabled	No offline use of the data.
Read-only	Session data can be browsed and launched while not communicating back to the data source.
Read/Write	Session data can be browsed/launched/modified.



[Read/Write](#) is not available with the Free and Basic subscription of [Remote Desktop Manager Online \(RDMO\)](#)



Not all functionality of Remote Desktop Manager is enabled while offline. Even when in read/write access mode you may not be able to perform all actions. Note that the [Private Vault](#) feature is available in offline mode.

[Grant/Remove Offline](#)

The offline mode is controlled at three levels:

- User permissions.
- Data source settings (server config)
- Data source configuration (local config)

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

User permissions	Data Source Settings	Data Source Configuration	Effective Access
Disabled or Read-only or Read/write	Disabled or Read-only or Read/write	Disabled	Disabled
Disabled or Read-only or Read/write	Disabled	Disabled or Read-only or Read/write	Disabled
Disabled	Disabled or Read-only or Read/write	Disabled or Read-only or Read/write	Disabled
Read-only or Read/write	Read-only or Read/write	Read-only	Read-only
Read-only or Read/write	Read-only	Read-only or Read/write	Read-only
Read-only	Read-only or Read/write	Read-only or Read/write	Read-only
Read/write	Read/write	Read/write	Read/write



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

4.1.5.1 Offline Read/Write

Description

Offline read/write enables the user to perform add, updates & deletes while the data source is offline. Those changes are saved locally and synced back to the data source once the data source becomes

available.



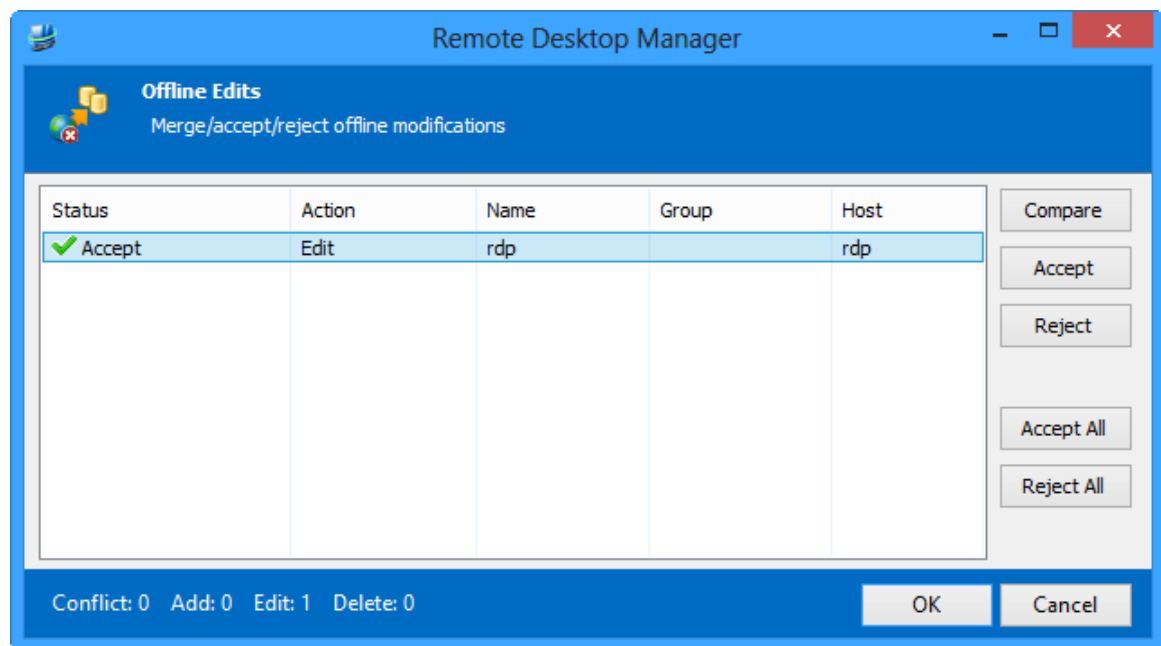
Not all functionality of Remote Desktop Manager is enabled while offline. Even when in read/write access mode, you may not be able to perform all actions. Note that the [Private Vault](#) feature is available in offline mode.

Once offline, the users security still apply. Add/Edit/Delete privileges granted by the system admin are respected. See [User Management](#).

Workflow

- Connect to the data source.
- Go offline (disconnect network, shutdown service...)
- Edit any connection
- Connect your network or restart your service...
- Refresh or Go Online

You will be prompted with:



Offline Edits - sync changes

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 changes have been detected
- Conflict - when changes have been detected

4.2 Types

4.2.1 Amazon S3

Description



Remote Desktop Manager saves the settings in a file located in an Amazon S3 bucket. Amazon S3 is storage for the Internet. It is designed to make web-scale computing easier for everyone.

Amazon S3 provides a simple web services interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the web and Remote Desktop Manager uses this API to persist your session settings.

More details on cloud computing and Amazon S3 can be found at: <http://aws.amazon.com/s3/>

Highlights

- This data source can be shared over the Internet between multiple locations
- This is a file-based data source, based on the XML data source



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

Settings

Consult [Amazon S3 settings](#) for more information on the configuration.

4.2.1.1 Settings

Settings

Connection

Remote Desktop Manager

Amazon S3
Edit the data source configuration

Connection Advanced

Name Amazon S3

Access key ID

Secret access key

Bucket name

Key name (filename) connections.xml

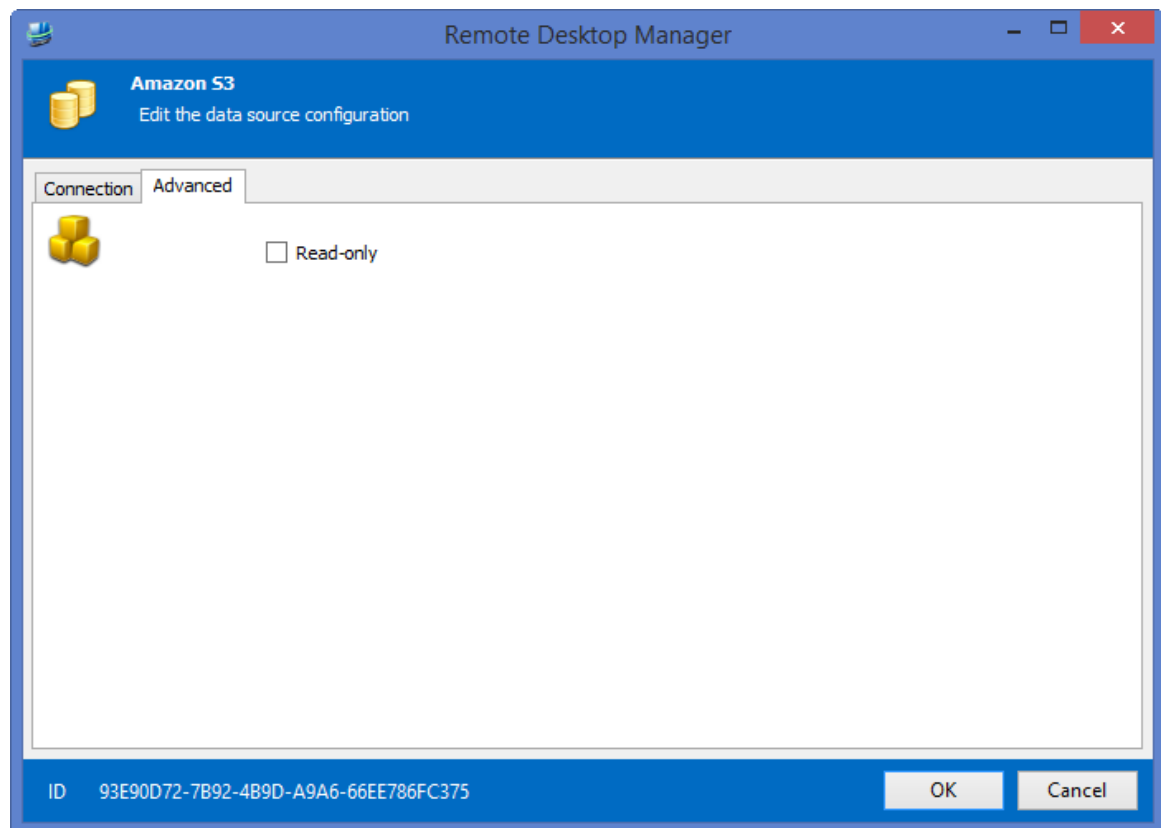
The file will be created if it does not exist

ID 93E90D72-7B92-4B9D-A9A6-66EE786FC375 OK Cancel

Amazon S3 Connection tab

Option	Description
Name	Name of the data source.
Access key ID	Contains the Amazon S3 Access Key ID.
Secret access key	Contains the Amazon S3 Secret access ID.
Bucket name	Name of the bucket created on Amazon S3 website and used by the application.
Key name (filename)	Name of the file that will be used to store the data on Amazon S3.

Advanced



Amazon S3 Advanced tab

Option	Description
Read-only	Set the data source in read only. No new entry can be created and the existing data cannot be edit.

4.2.2 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

Consult [Dropbox settings](#) for more information on the configuration.

4.2.2.1 Settings

Settings

Connection

Dropbox Connection tab

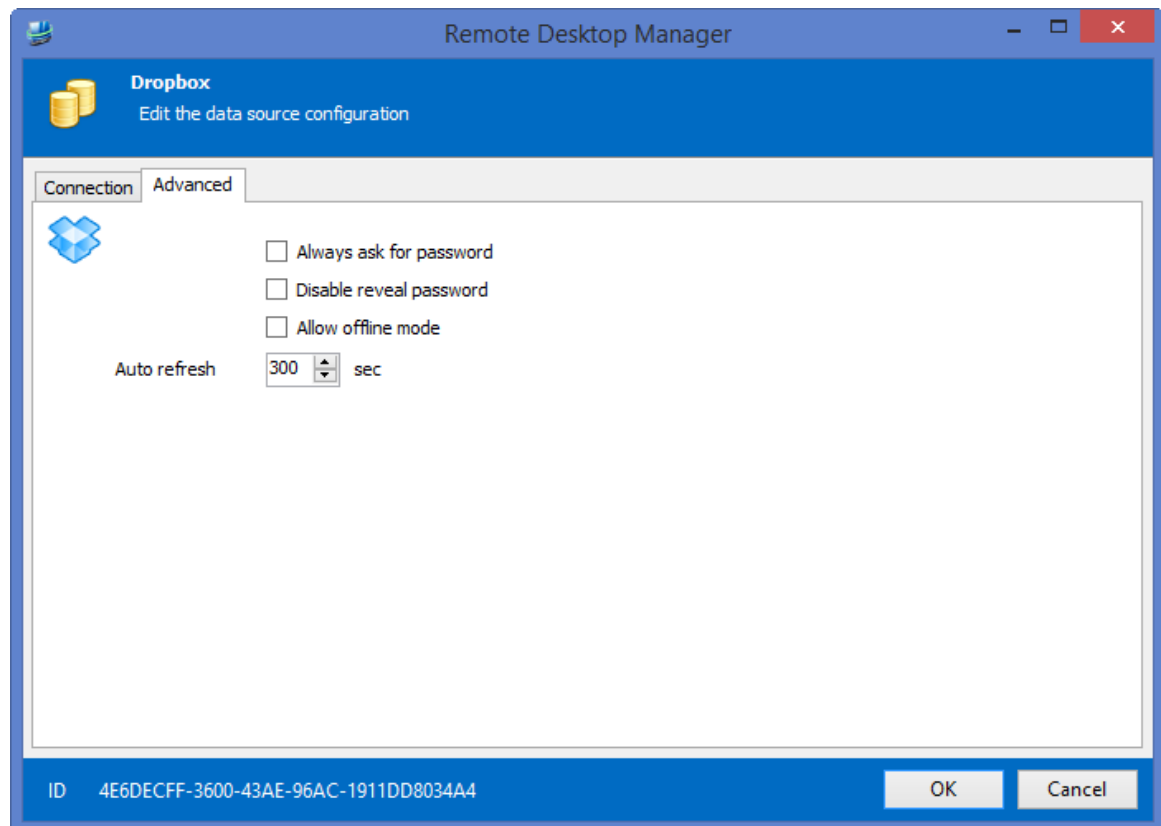
Option	Description
Name	Name of the data source.
Email	Contains the email address associated with the Dropbox account.
Validate with Dropbox	Button to validate the email address with the Dropbox account.
Dropbox directory	Indicate the folder in Dropbox. It should not contains any drive since it's stored online. Leave it empty to use the default Dropbox root.

Filename	Indicate the filename used to store the data on the data source.
----------	--



Remote Desktop Manager doesn't support the 2-Factor Authentication of Dropbox. To make it work, you need to disable the 2-Factor Authentication in Dropbox, create your Dropbox data source and click validate with Dropbox to complete the configuration. When everything is functional, you can turn on again the 2-Factor Authentication in Dropbox.

Advanced



Dropbox Advanced tab

Option	Description
Always ask for password	Force the password prompt before the initial connection on Dropbox.
Disable reveal password	Disable the reveal password feature when a user access this data source.
Allow offline mode	Allow the data source to be used in Offline Mode.
Auto refresh	Set the interval to use between each automatic refresh.

4.2.3 FTP

Description



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

Highlights

- This data source can be shared over the Internet between multiple locations
- This is a file-based data source, based on the XML data source



Although it can be shared between multiple locations, there is no conflict management for the configuration. If you share with other users you may get update conflicts and run into issues.

Settings

Consult [FTP settings](#) for more information on the configuration.

4.2.3.1 Settings

Settings

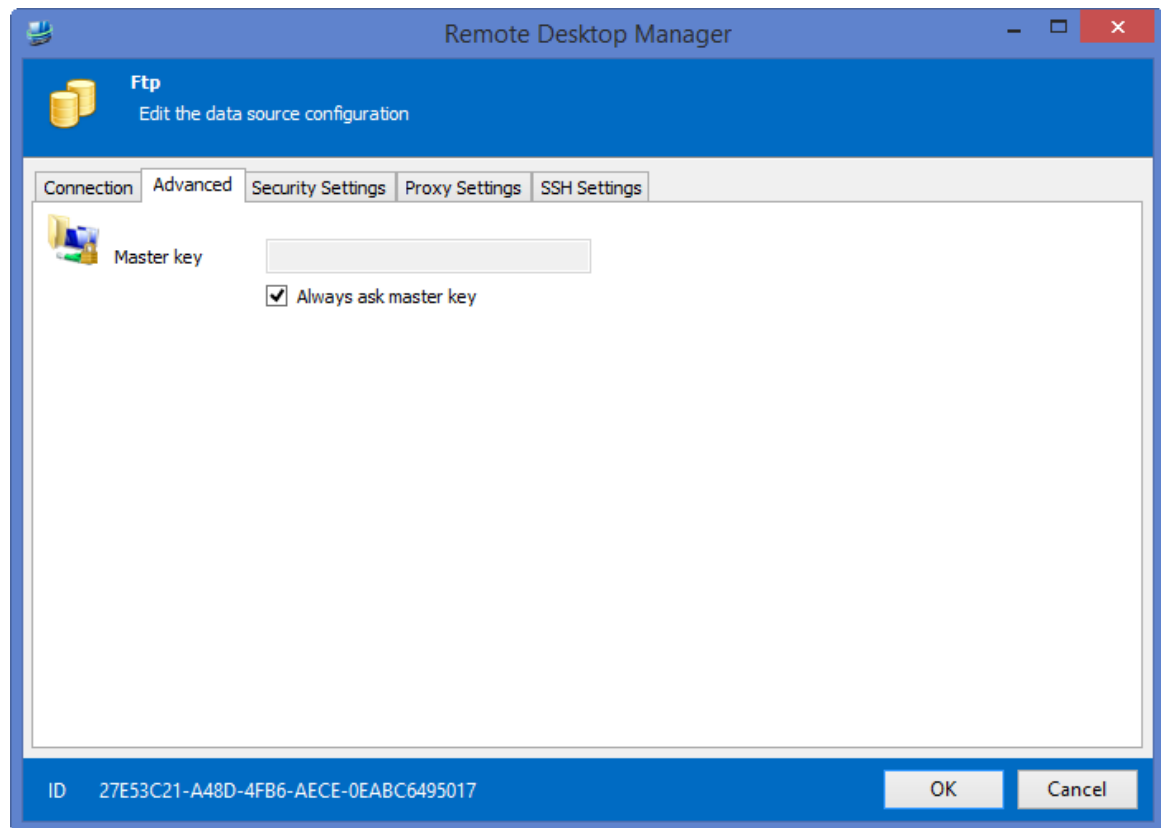
Connection

The screenshot shows the 'Remote Desktop Manager' application window with the 'Ftp' tab selected. The title bar reads 'Remote Desktop Manager'. Below the title bar, there's a blue header with 'Ftp' and 'Edit the data source configuration'. The main area has tabs for 'Connection', 'Advanced', 'Security Settings', 'Proxy Settings', and 'SSH Settings'. The 'Connection' tab is active, showing fields for 'Name' (FTP), 'Ftp path' (ftp://server.domain.com/RDM), 'Port' (21), 'User name' (user@domain.com), 'Password' (masked with dots), 'Filename' (RDM.xml), and a 'Passive mode' checkbox which is checked. There are also icons for 'Show password' and 'Remember password'. A yellow information box at the bottom states 'The file will be created if it does not exist'. The bottom of the window shows an ID '0BB12F8D-9263-46BB-B729-BA5DFC7C6660' and 'OK' and 'Cancel' buttons.

FTP Connection tab

Option	Description
Name	Name of the data source.
FTP Path	FTP server name to access the XML file.
Passive mode	Set the FTP mode to passive.
Username	Username used to access the FTP server.
Password	Password used to access the FTP server.
Filename	Indicate the remote folder and filename for data source XML.

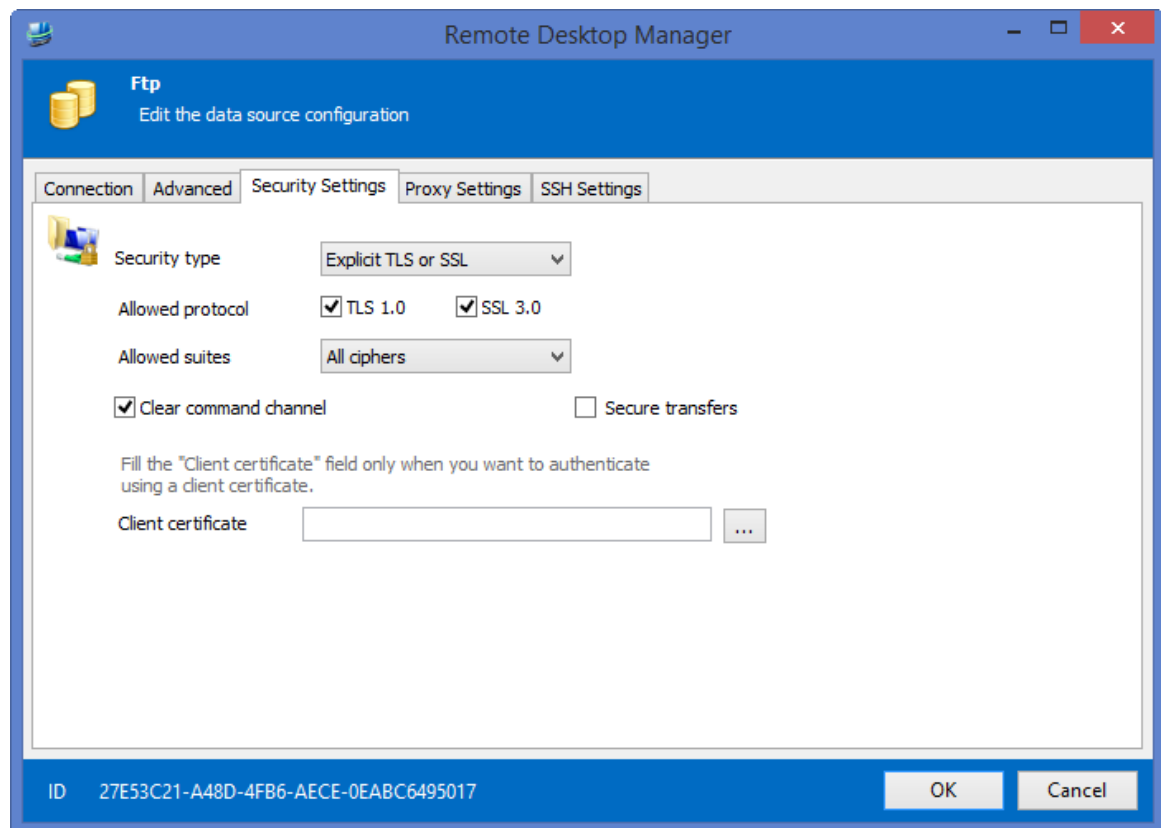
Advanced



FTP Advanced tab

Option	Description
Always ask master key	Always ask the master key to connect to the data source. The application will not store any password.

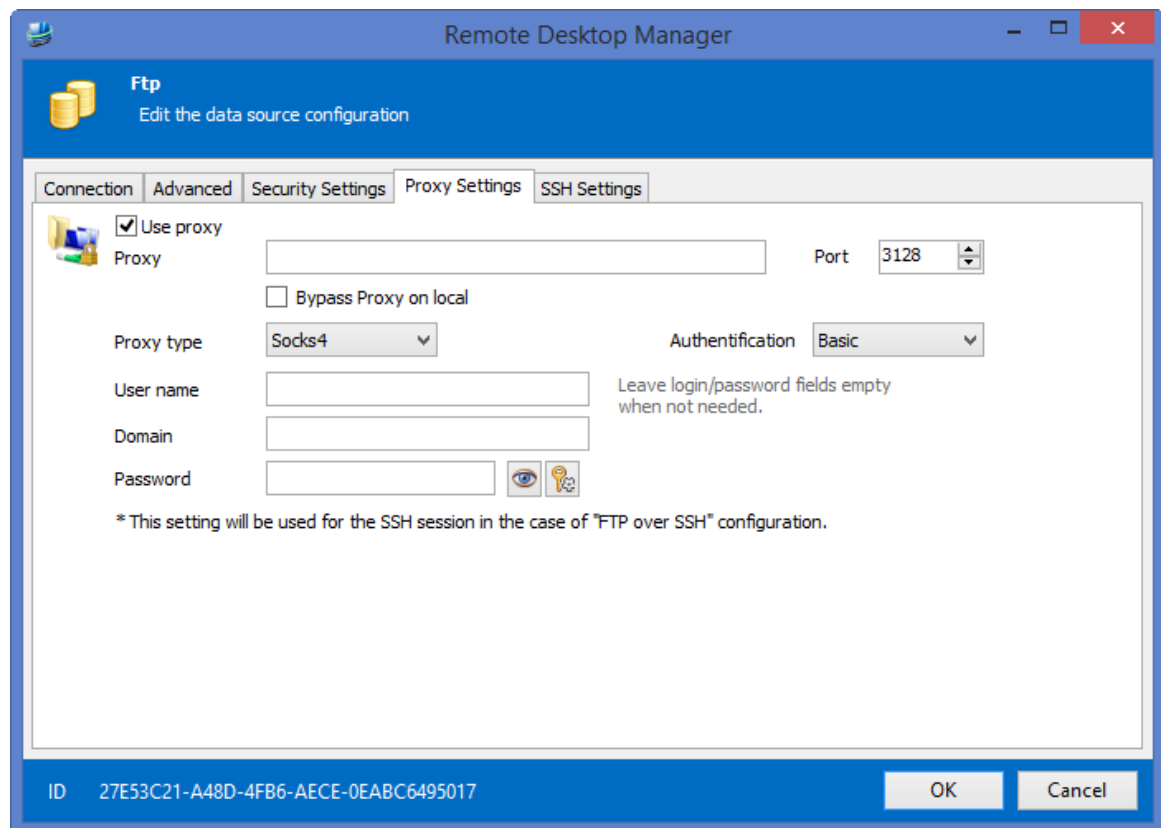
Security Settings



FTP Security Settings tab

Option	Description
Security type	Specify the security type used for the FTP connection.
Allowed protocol	Indicate the allowed FTP protocol.
Allowed suites	Indicate the allowed cipher suites.
Clear command channel	If the Clear Control Connection (CCC) setting is enabled, the FTP client connects to the server, negotiates a secure connection, authenticates (sends user and password) and reverts back to plaintext.
Secure transfers	Enable the secure transfers.
Client certificate	Specify the client certificate used for the authentication.

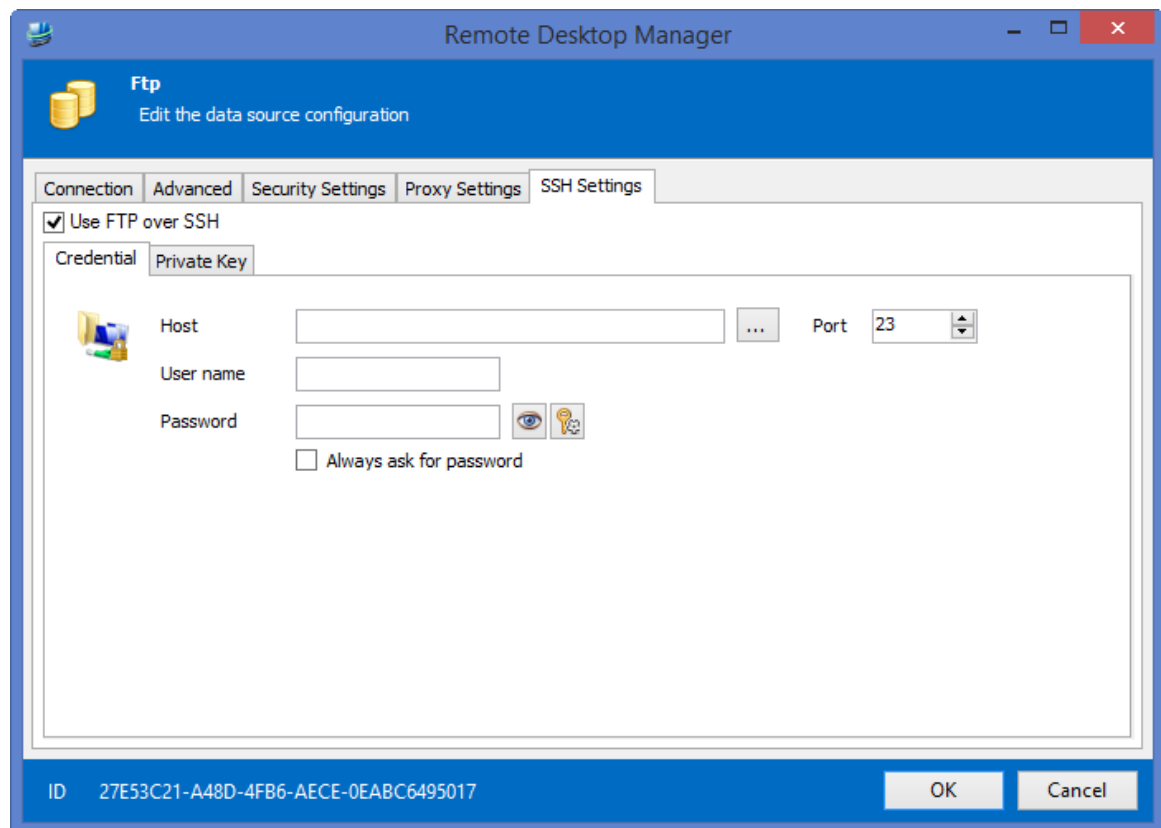
Proxy Settings



FTP Proxy Settings tab

Option	Description
Proxy	Enter the name of the Proxy Server.
Proxy type	Specify the proxy type to use.
Authentication	Select the type of authentication mode used to connect on the proxy server such as Basic or NTLM.
Username	Username to access the Proxy server.
Domain	Domain to access the Proxy server.
Password	Password to access the Proxy server.

SSH Settings



FTP SSH Settings tab

Option	Description
Use FTP over SSH	Use FTP over SSH connection.
Host	Name of the host to access the FTP over SSH.
Username	Username to access the FTP Server over SSH.
Password	Password to access the FTP Server over SSH.
No private Key	Indicate that no private key is used.
Private key file	Specify the private key filename located on the local disk.
Private key data	Specify the private key data instead of the filename.

4.2.4 SFTP

Description



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

Highlights

- This data source can be shared over the Internet between multiple users
- This is a file-based data source, based on the XML data source



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

Settings

Consult [SFTP settings](#) for more information on the configuration.

4.2.4.1 Settings

Settings

Connection

The screenshot shows the 'Remote Desktop Manager' window with the 'SFTP' tab selected. The title bar says 'Remote Desktop Manager'. The main area is titled 'SFTP' and 'Edit the data source configuration'. There are four tabs: 'Connection' (selected), 'Advanced', 'Proxy Settings', and 'Private Key'. The 'Connection' tab contains the following fields:

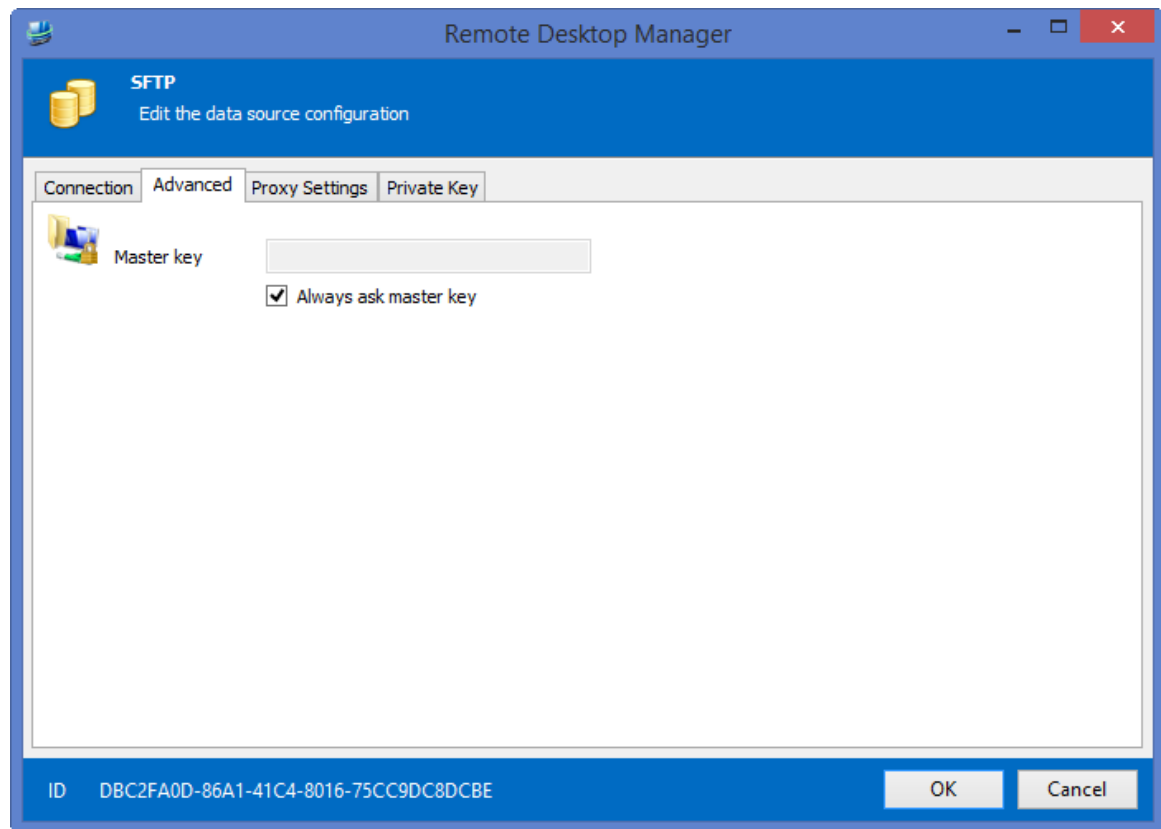
- Name:** SFTP
- Ftp host:** ftp://server.domain.com/RDM
- Port:** 22
- User name:** user@domain.com
- Password:** masked with dots, with icons for showing/hiding and a key icon.
- Filename:** rdm.xml

Below the fields is a yellow information box that says: 'The file will be created if it does not exist'. At the bottom, there is an 'ID' field with the value 'DBC2FA0D-86A1-41C4-8016-75CC9DC8DCBE', and 'OK' and 'Cancel' buttons.

SFTP Connection tab

Option	Description
Name	Name of the data source.
FTP Host	FTP server name to access the XML file.
Username	Username used to access the FTP server.
Password	Password used to access the FTP server.
Filename	Indicate the remote folder and filename for data source XML.

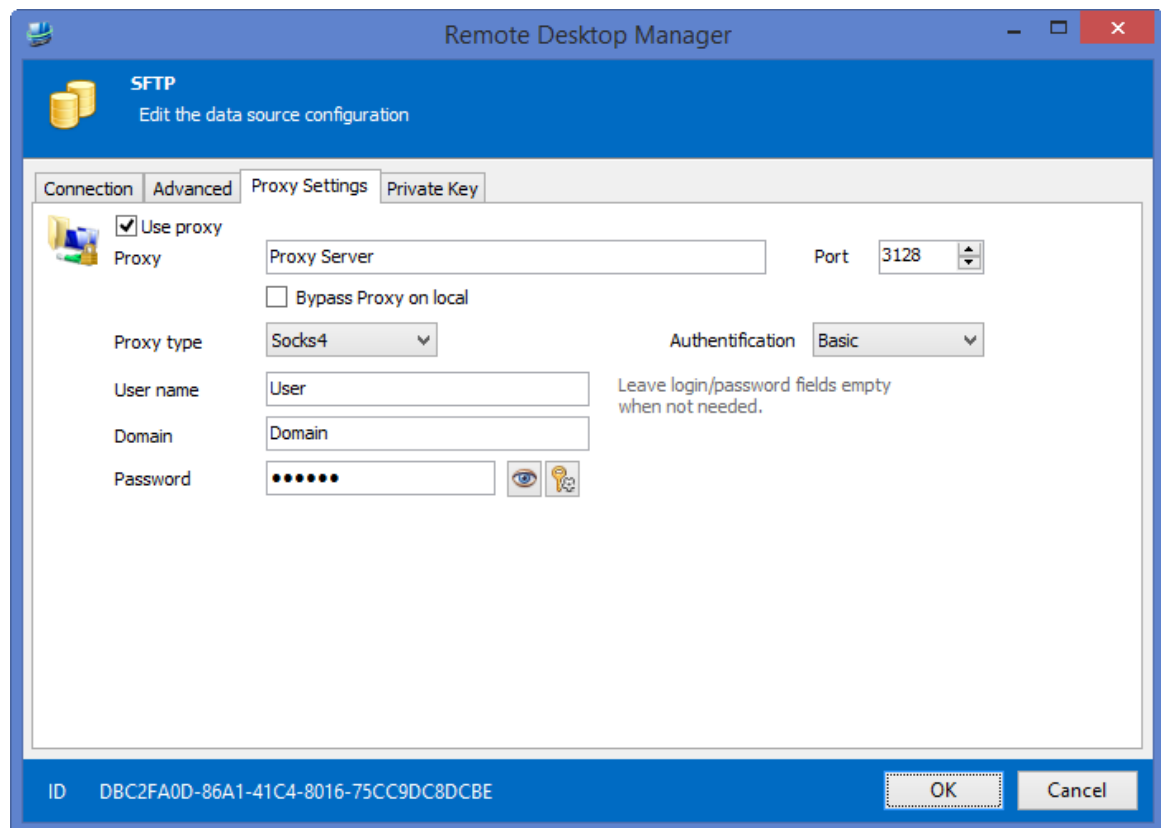
Advanced



SFTP Advanced tab

Option	Description
Always ask master key	Always ask the Master key when connecting to the data source.

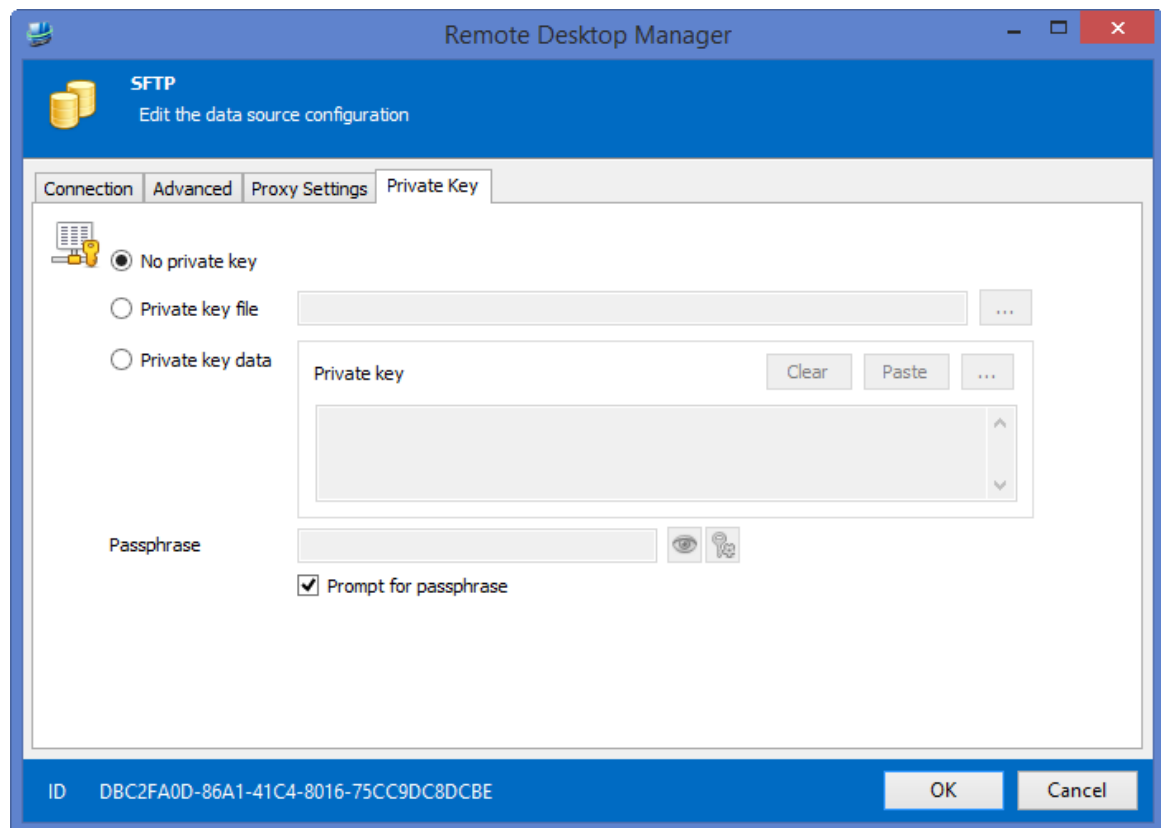
Proxy Settings



SFTP Proxy Settings tab

Option	Description
Proxy	Enter the name of the Proxy Server.
Proxy type	Specify the proxy type to use.
Authentication	Select the type of authentication mode used to connect on the proxy server such as Basic or NTLM.
Username	Username to access the Proxy server.
Domain	Domain to access the Proxy server.
Password	Password to access the Proxy server.

Private Key



SFTP Private Key tab

Option	Description
No private Key	Indicate that no private key is used.
Private key file	Specify the private key filename located on the local disk.
Private key data	Specify the private key data instead of the filename.

4.2.5 Microsoft Access

Description



Remote Desktop Manager saves the settings in a Microsoft Access database, located on the local machine or on a network share.

Microsoft Access is a pseudo relational database management system from Microsoft, which combines the relational Microsoft Jet Database Engine with a graphical user interface and software development tools.

Highlights

- This data source supports the native Access database password (Note that the password must be set using Microsoft Access directly – Remote Desktop Manager does not allow you to set or change the database, because it requires an exclusive connection to it)
- The Offline Mode is supported by this data source

- The database can be shared by multiple users on a network drive, but the performance and the data integrity can't be guaranteed
- The [Online Backup Service](#) is available for this data source



This data source is **not recommended** since Microsoft has stopped providing support in the newest Windows version.



Entering a database password when creating the physical file has no effect. You must use Microsoft Access to set the password in the database file.

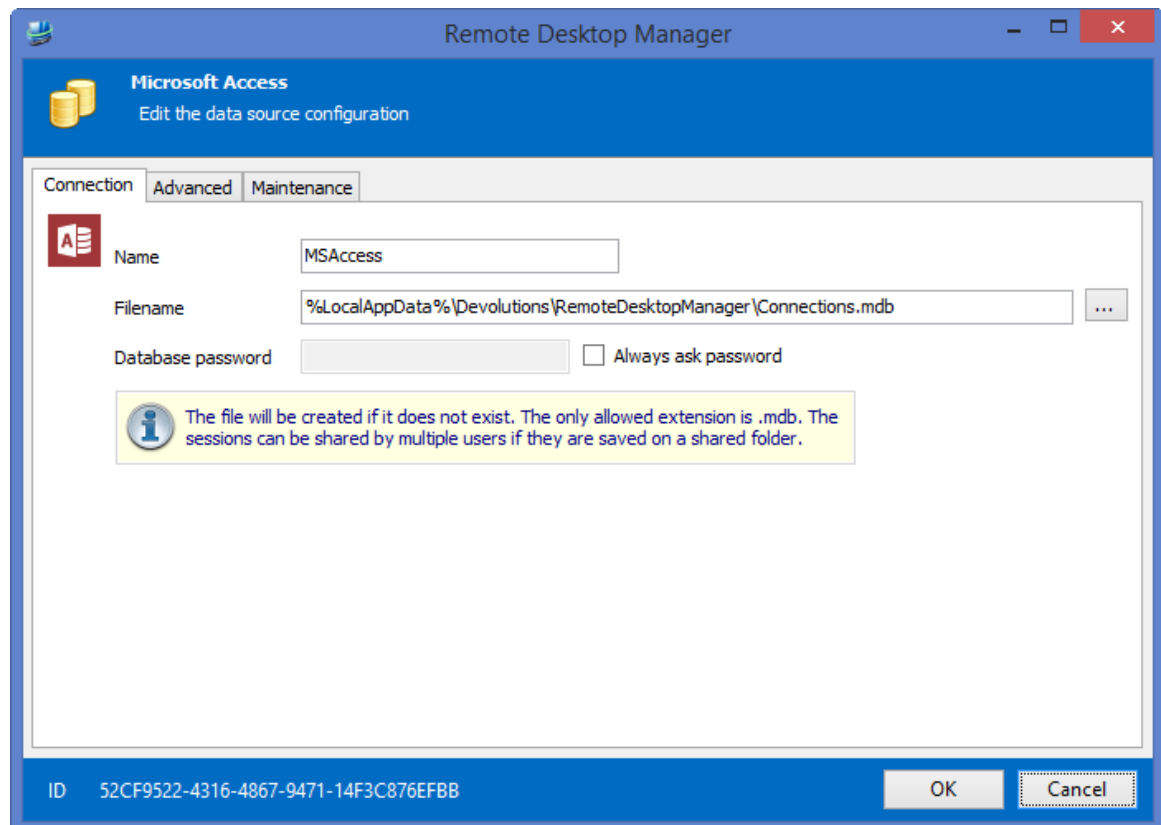
Settings

Consult [Microsoft Access settings](#) topic for more information on the configuration.

4.2.5.1 Settings

Settings

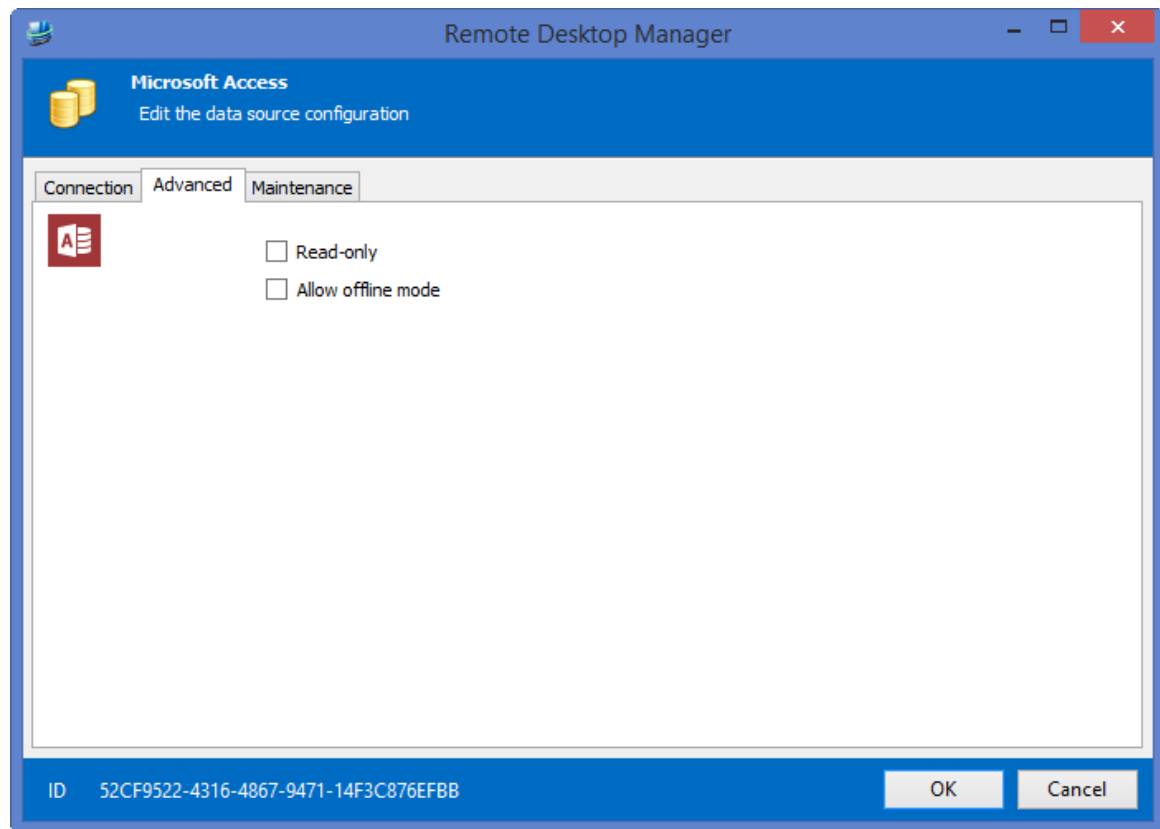
Connection



MS Access Connection tab

Option	Description
Name	Name of the data source.
Filename	Indicate the destination folder including data source file name. This needs to be an .mdb file extension.
Database password	Password to open the database. The application will not set the password. It needs to be applied with another tool like Microsoft Access directly.
Always ask password	Always ask for password when connecting to the data source.

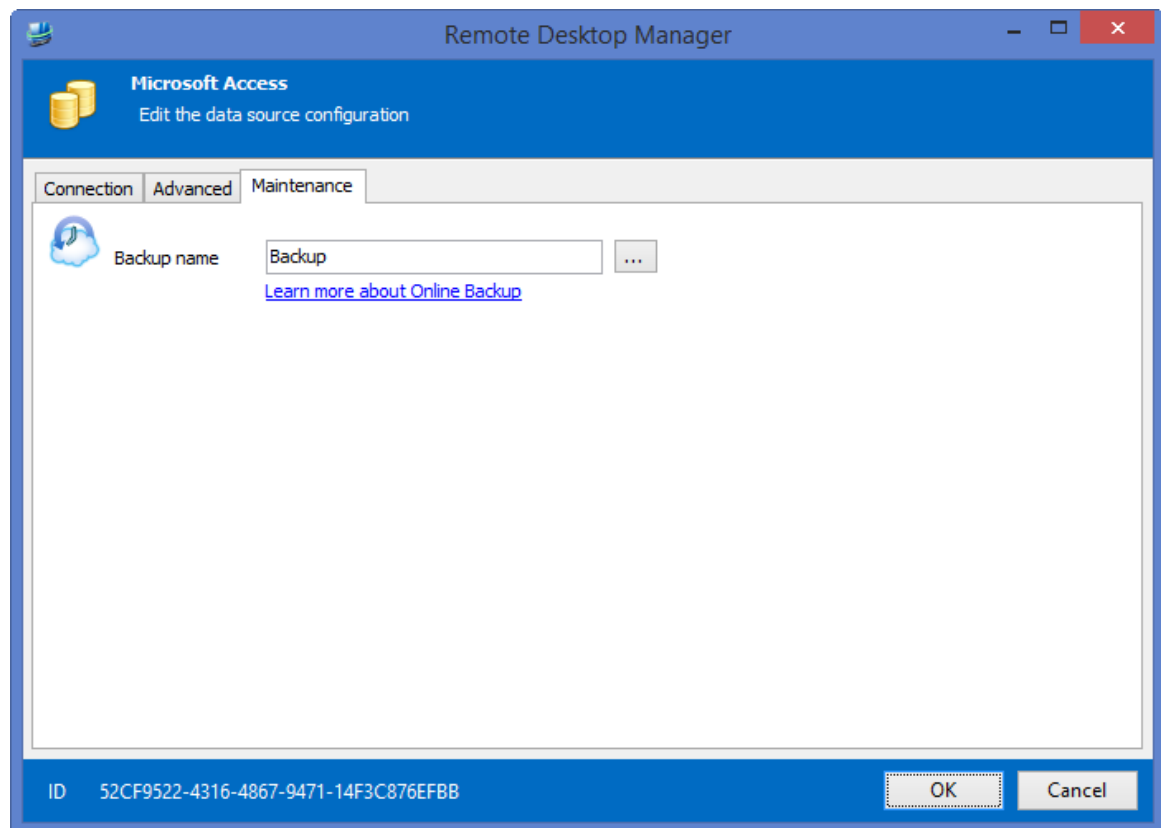
Advanced



MS Access Advanced tab

Option	Description
Read-only	Set the data source in read only. No new entry can be created and the existing data cannot be edit.
Allow offline mode	Allow the data source to be use in Offline Mode.

Maintenance



MS Access Maintenance tab

Option	Description
Backup name	Specify the backup name used by the Online Backup Service (available via subscription). It allows you to automatically save your sessions in a safe online storage space, and restore them in the event of problems.

4.2.6 SQLite

Description



Remote Desktop Manager's SQLite data source is ideal for single user 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.

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

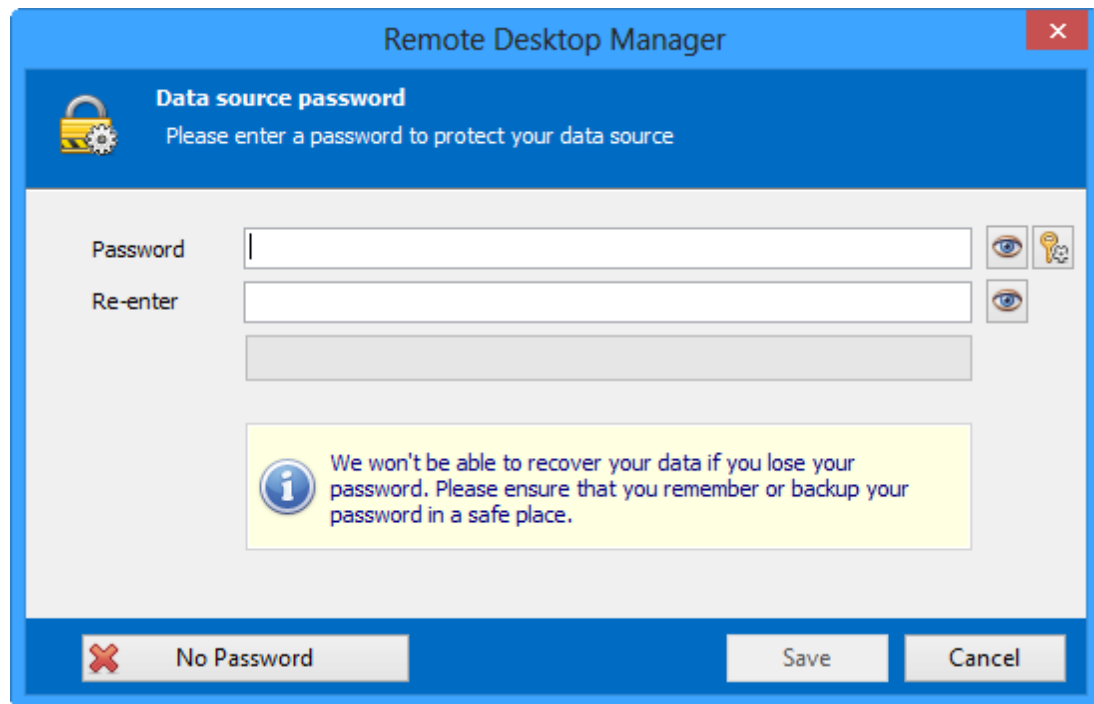
Settings

Consult [SQLite settings](#) topic for more information on the configuration.

Password management

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

Change or clear the password of a SQLite data source.

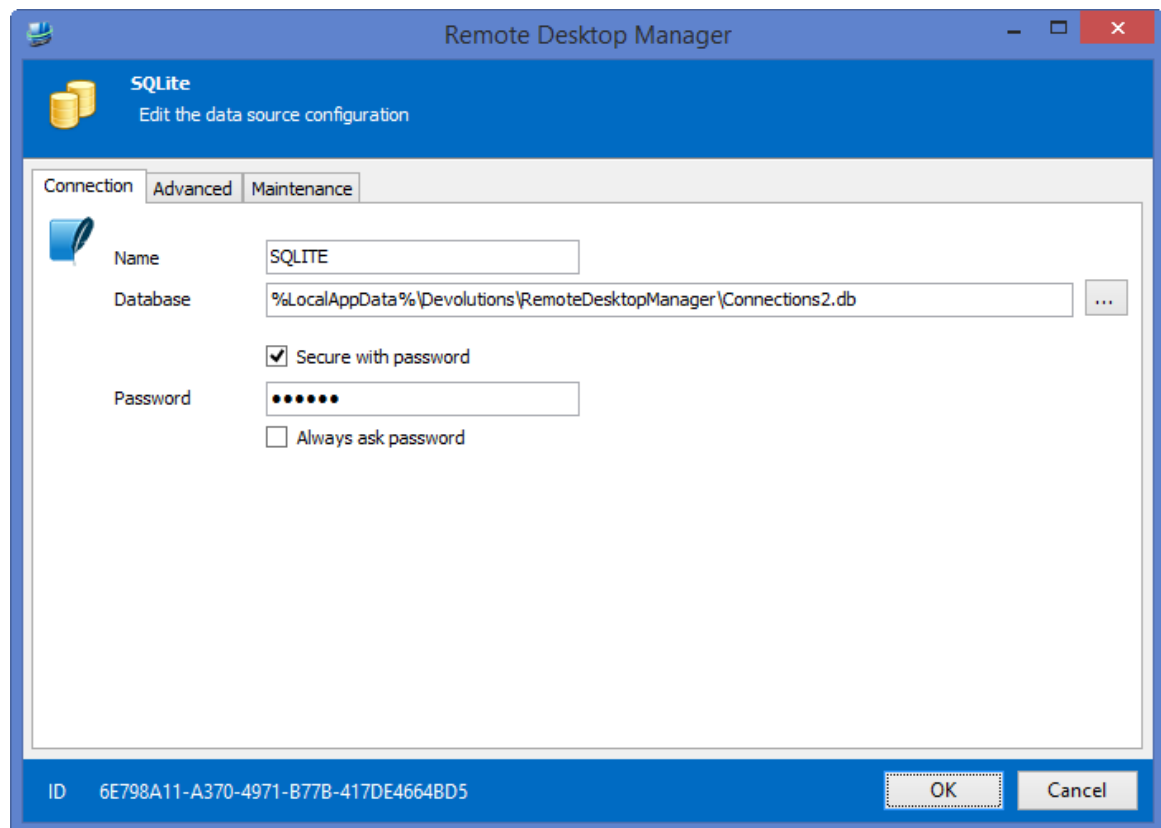


Manage password dialog

4.2.6.1 Settings

Settings

Connection



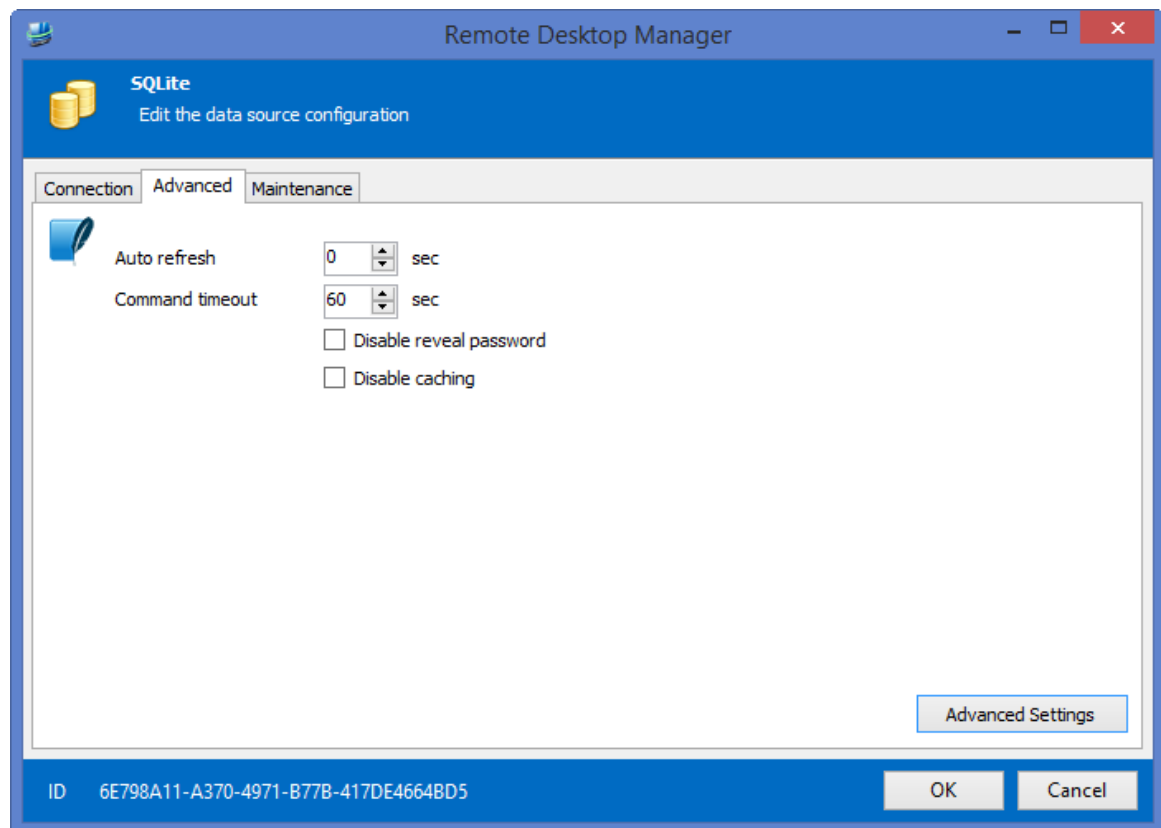
SQLite Connection tab



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

Option	Description
Name	Name of the data source.
Database	Indicates the filename of the SQLite database (.db).
Password	Password used to access the data source.
Secure with password	Secure the data source with a password. This is used to encrypt the database content and it cannot be recovered if lost.
Always ask password	Always ask for the password when connecting to the data source.

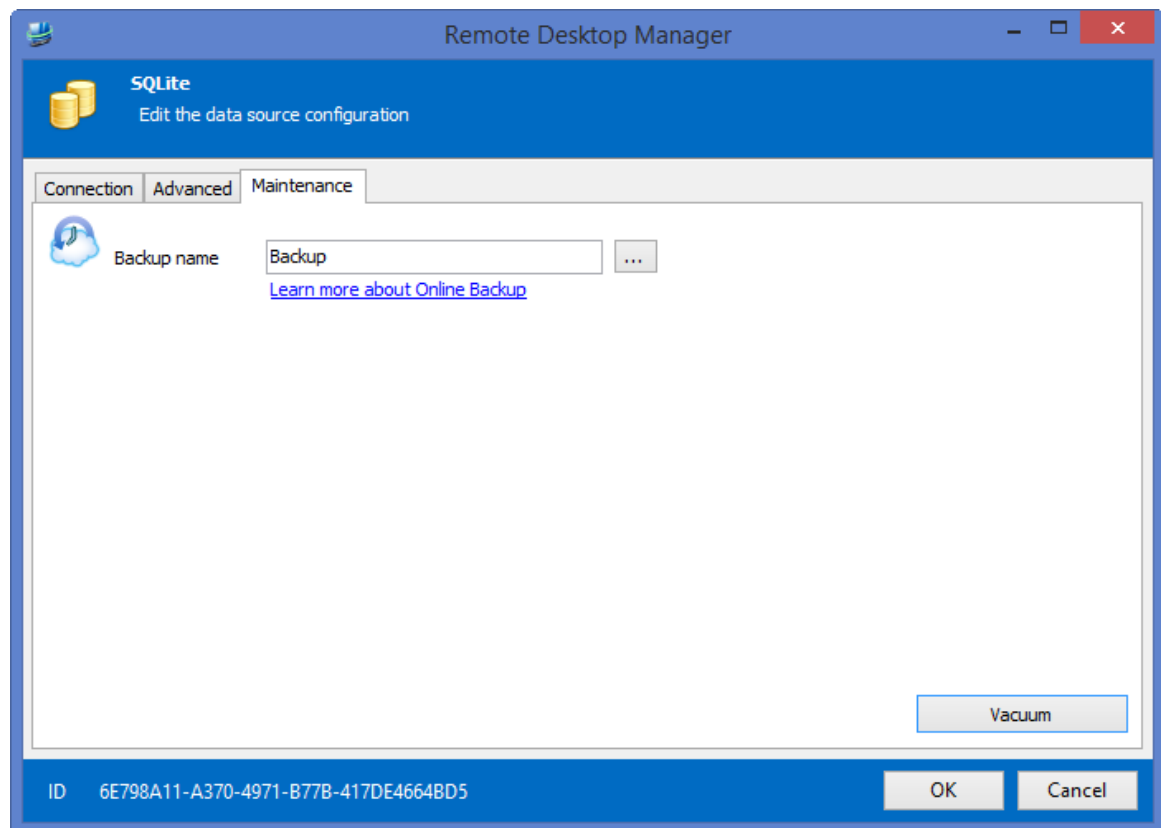
Advanced



SQLite Advanced tab

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

Maintenance



SQLite Maintenance tab

Option	Description
Backup name	Specify the backup name used by the Online Backup Service (available via subscription). It allows you to automatically save your sessions in a safe online storage space, and restore them in the event of problems.
Vacuum	Used to compress and clean up the current database file.

4.2.7 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
- Integrated Security support.

Settings

Consult [MariaDB settings](#) topic for more information on the configuration.

4.2.7.1 Settings

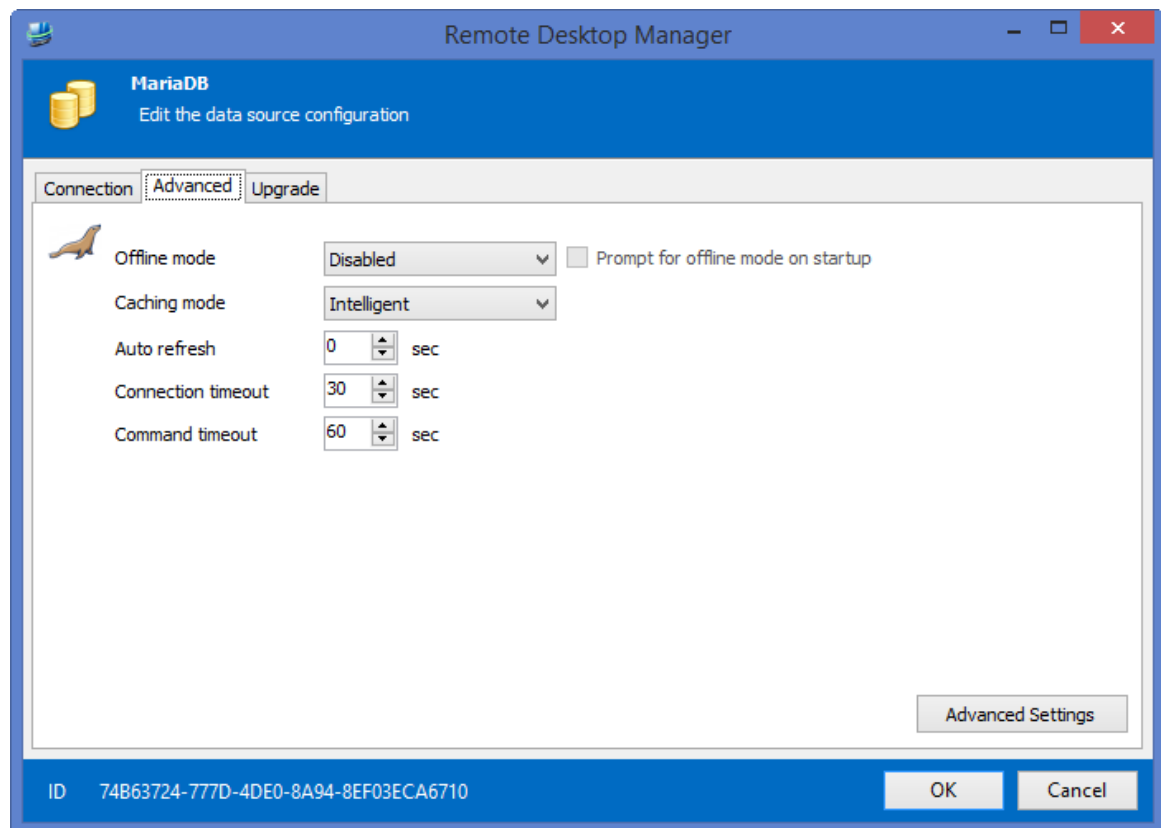
Settings

Connection

MariaDB Connection tab

Option	Description
Name	Name of the data source.
Host name	Name of the host (server name) where the data source will be store.
User	Username used to access the host server.
Password	Password used to access the host server.
Schema	Name of the schema (database) on the MySQL server.
Test Host	Test the connection with the host (server name) to validate if the proper information has been provided.
Test Schema	Test the connection with the schema to validate if the proper information has been provided.

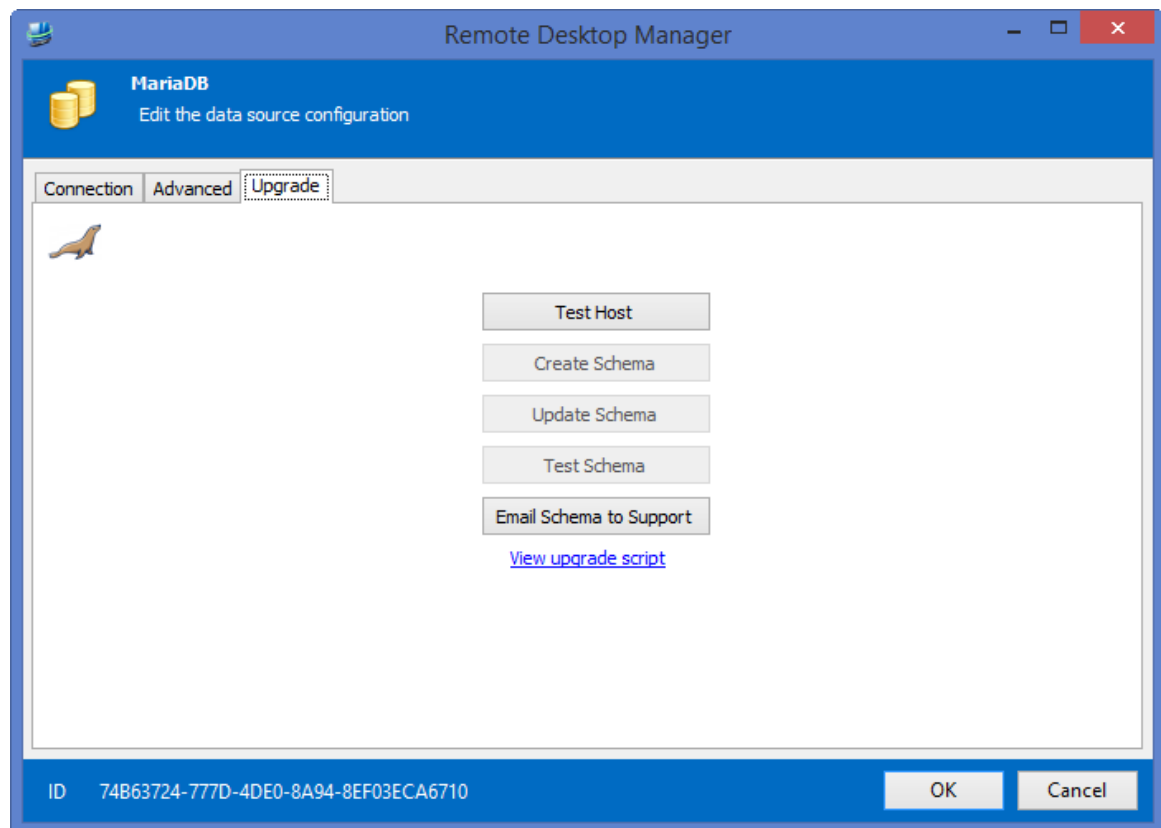
Advanced



MariaDB Advanced tab

Option	Description
Offline mode	Determine if you want to use this data source in Offline Mode. With this mode, the data source can be available in Read Only or in Read/Write mode.
Caching mode	Determine how the entries will be reloaded in the data source. See Caching Mode topic for more information.
Auto refresh	Set the interval for the automatic refresh
Connection timeout	Waiting time before a connection timeout.
Command timeout	Waiting time before a command timeout.
Advanced Settings	Directly edit the connection string values.

Upgrade



MariaDB Upgrade tab

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.

4.2.8 Web

Description



Remote Desktop Manager reads the session settings directly from a file located on a web site.

Highlights

- This read-only data source can be shared over the Internet between multiple users

- This is a file-based data source, based on the XML data source
- Supports Windows authentication in IIS

Settings

Consult [Web settings](#) for more information on the configuration.

4.2.8.1 Settings

Settings

Connection

The screenshot shows a window titled 'Remote Desktop Manager' with a blue header bar. Below the header, there's a section titled 'Web' with a subtitle 'Edit the data source configuration'. The main area is a tabbed interface with the 'Connection' tab selected. It contains four input fields: 'Name' (Web datasource), 'URL filename' (http://webdatasource.com/RDM.xml), 'User name' (user@domain.com), and 'Password' (masked with dots). At the bottom, there's an 'ID' field with the value 'BEFFCF5E-F686-4C9D-9E96-718069BE84FB' and two buttons: 'OK' and 'Cancel'.

Web Connection tab

Option	Description
Name	Name of the data source.
URL filename	Indicate the web location of the data source and the name of data source file.
Username	Username used to access the data source.
Password	Password used to access the data source.

4.2.9 XML

Description



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

Highlights

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



There is no conflict management for the configuration file. If you share with other users you may get update conflicts and run into issues. This data source type is meant for a single user using multiple computers, not multiple users.



All passwords are encrypted by default. You can specify a custom password (master key) to fully encrypt the content of the file.

It's impossible to recover the data if the master key is lost. Please make sure to remember or backup the master key in a safe place.

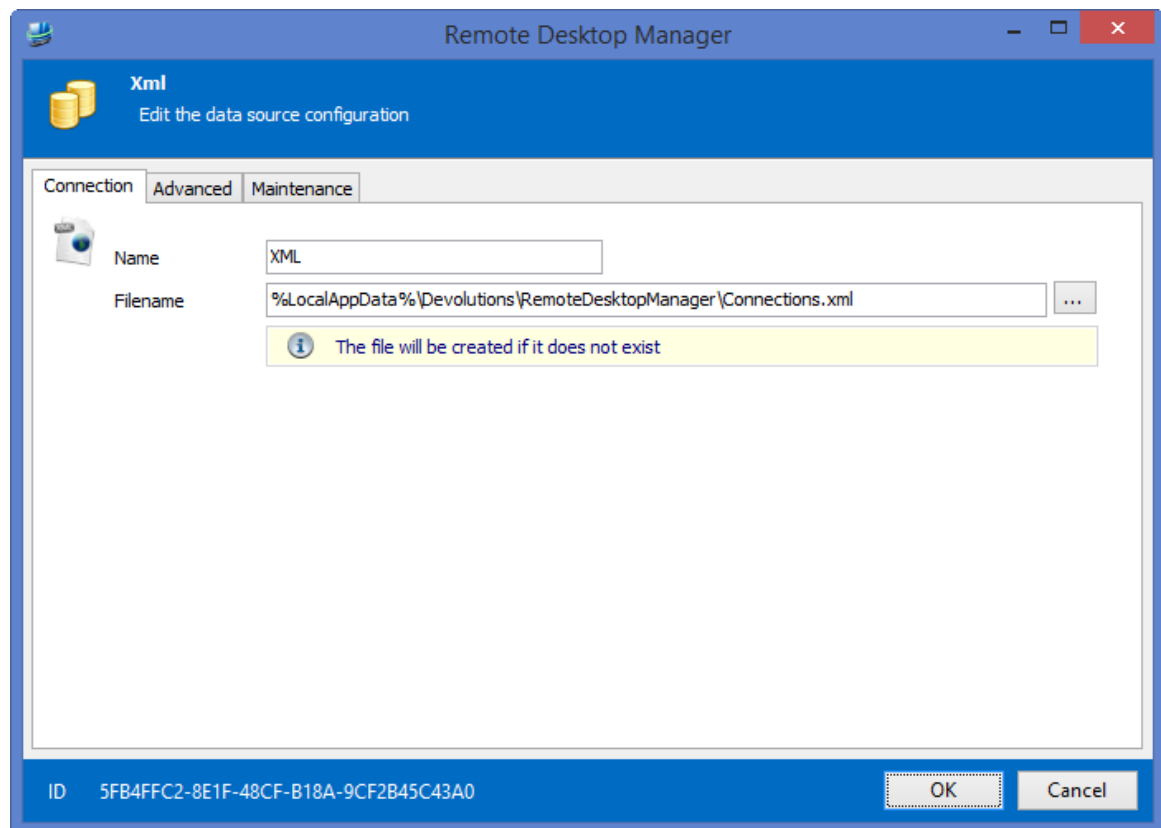
Settings

Consult [XML settings](#) for more information on the configuration.

4.2.9.1 Settings

Settings

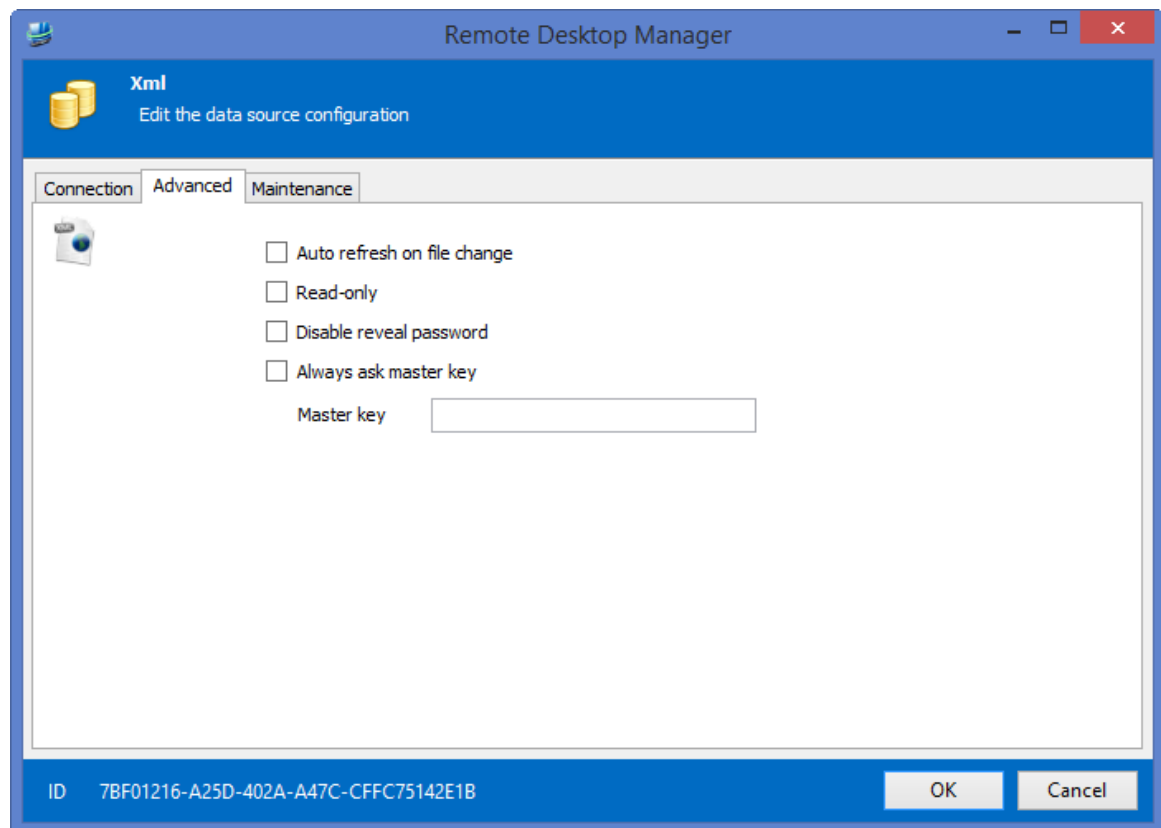
Connection



XML Connection tab

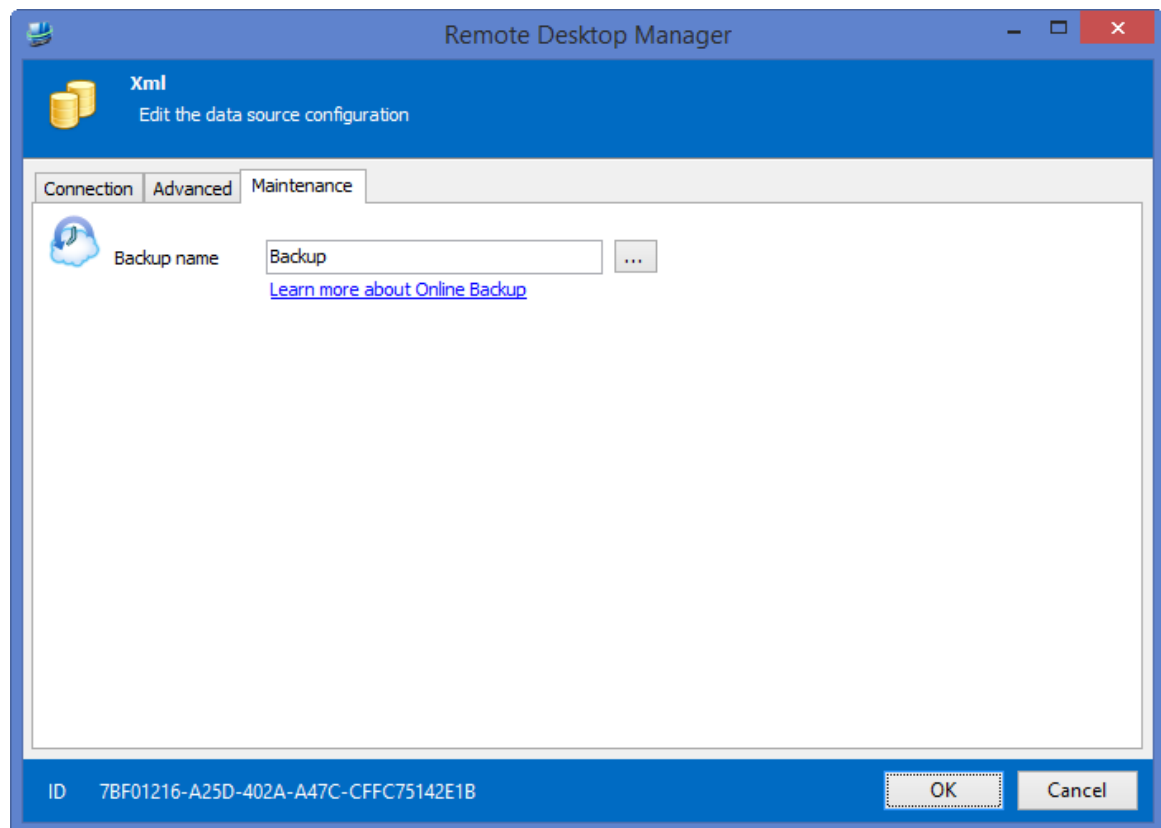
Option	Description
Name	Name of the data source.
Filename	Specify the full path of the XML file used to save the data. Relative paths and environment variables can be used as well.

Advanced

**XML Advanced tab**

Option	Description
Auto refresh on file change	Indicate if the application monitor the file changes to automatically refresh the data source.
Read-only	Set the data source in read only. No new entry can be created and the existing data cannot be edit.
Disable reveal password	Disable the reveal password feature when a user accesses this data source.
Always ask master key	Always ask the Master key before opening the data source. This is used to encrypt the XML content and it could not be recovered if lost.

Maintenance



XML Maintenance tab

Option	Description
Backup name	Specify the backup name used by the Online Backup Service (available via subscription). It allows you to automatically save your sessions in a safe online storage space, and restore them in the event of problems.

4.2.10 Advanced Data Sources

Description

Advanced Data Sources are typically running on an advanced management system, either a Database Management System or our own Online Services.

This allows Remote Desktop Manager to support these features:

- Entry Attachments
- Audit and logging
- Advanced security with user and security group management
- Offline Mode (please see below for more details)

Currently the Advanced Data Sources are:

- [SQL Server/SQL Azure \(MSSQL\)](#)
- [MySQL](#)

- [Remote Desktop Manager Online \(RDMO\)](#)
- [Remote Desktop Manager Server \(RDMS\)](#)

Common settings

Offline mode

The Offline Mode allows you to connect to a read-only 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.



The offline mode file 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 this case, there is no key saved anywhere.

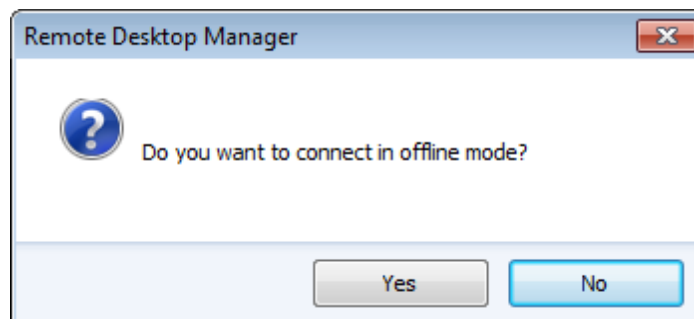
For added security, offline files are set to expire after a delay, the default expiry is set to 7 days but can be modified via the **Administration -> Data Source Settings**.



We want to highlight that the offline cache is read only. For mobile workers we recommend creating a local data source. This allows you to create new entries, or, by using **Clipboard -> Copy** and **Clipboard -> Paste**, to copy entries between data sources and modify them as needed. When reconnecting to the data source you can use copy/paste again to update the online copy.

Prompt for offline mode on startup

Remote Desktop Manager will display a confirmation dialog when opening a data source for the first time. You can select to work offline or not.



Offline mode confirmation dialog

4.2.10.1 SQL Server/SQL Azure (MSSQL)

Description



Remote Desktop Manager uses the power of Microsoft SQL Server to save and manage all sessions. This is the recommended data source type for a multi-user environment. Microsoft SQL Server 2005, 2008 and 2012 are supported (All editions except the compact). See this [Configure SQL Server](#) topic for more details about how to configure SQL Server.

Highlights

- This data source allows user management with a superior security model
- The Offline Mode can be used when the server is unavailable, or when the user is on the road
- Full connection log and attachment support
- The data source supports an auto refresh at your preferred interval
- Microsoft SQL Azure can be used to create an online database. Get more detail on SQL Azure [here](#)



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



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

Settings

Consult [SQL Server/SQL Azure \(MSSQL\) settings](#) topic for more information on the configuration.

4.2.10.1.1 Settings

Settings

Connection

Remote Desktop Manager

Microsoft SQL Server/SQL Azure
Edit the data source configuration

Connection Advanced Upgrade

Name SQL data source ☐ Use Sql Azure

Server SQL Server ... (Local) or IP or Server name

☐ Integrated security (Active Directory)

User user@domain.com ☐ Editable

☒ Save password

Password

Database RDM ...

Test Server

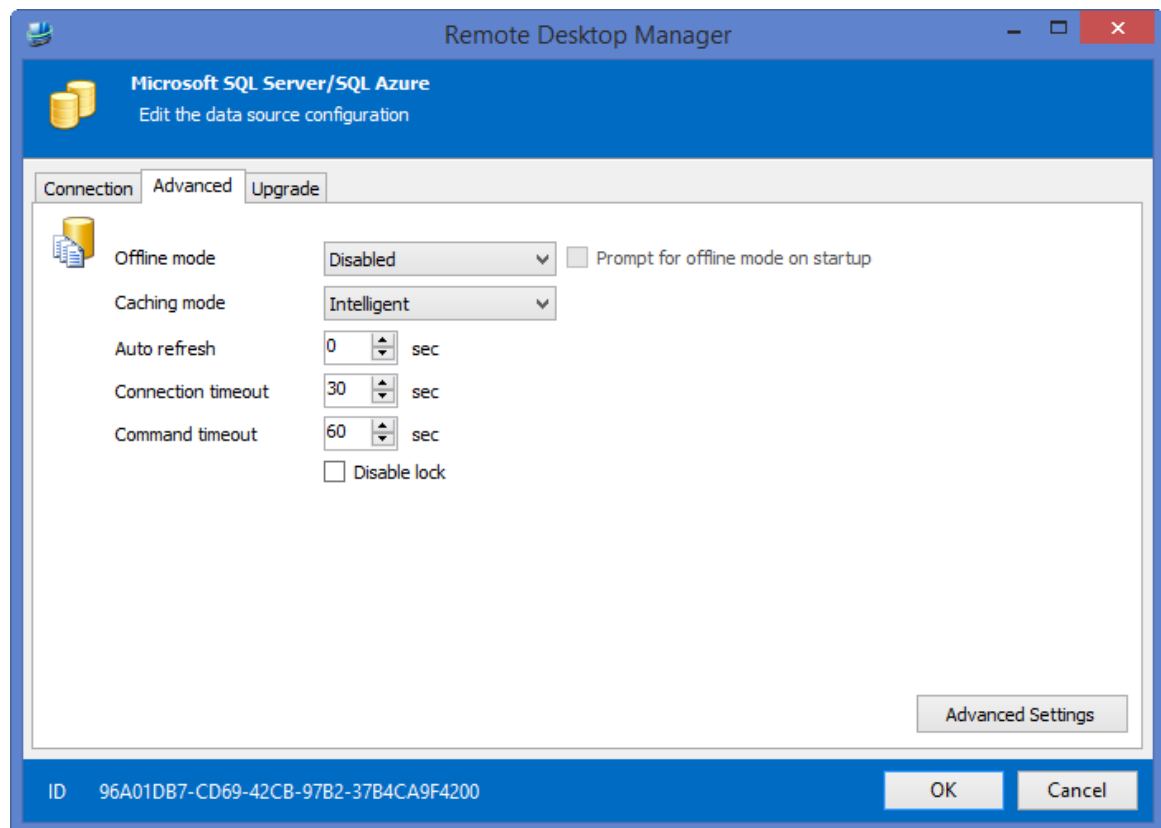
Test Database

ID 96A01DB7-CD69-42CB-97B2-37B4CA9F4200 OK Cancel

SQL Connection tab

Option	Description
Name	Name of the data source.
Server	Name of the server where the data source will be store.
User	Username to access the SQL server.
Password	Password used to access the SQL server.
Database	Name of the database on the SQL server for the utilization of Remote Desktop Manager.
Test Server	Test the connection with the server to validate if the proper information has been provided.
Test Database	Test the connection with the database to validate if the proper information has been provided.

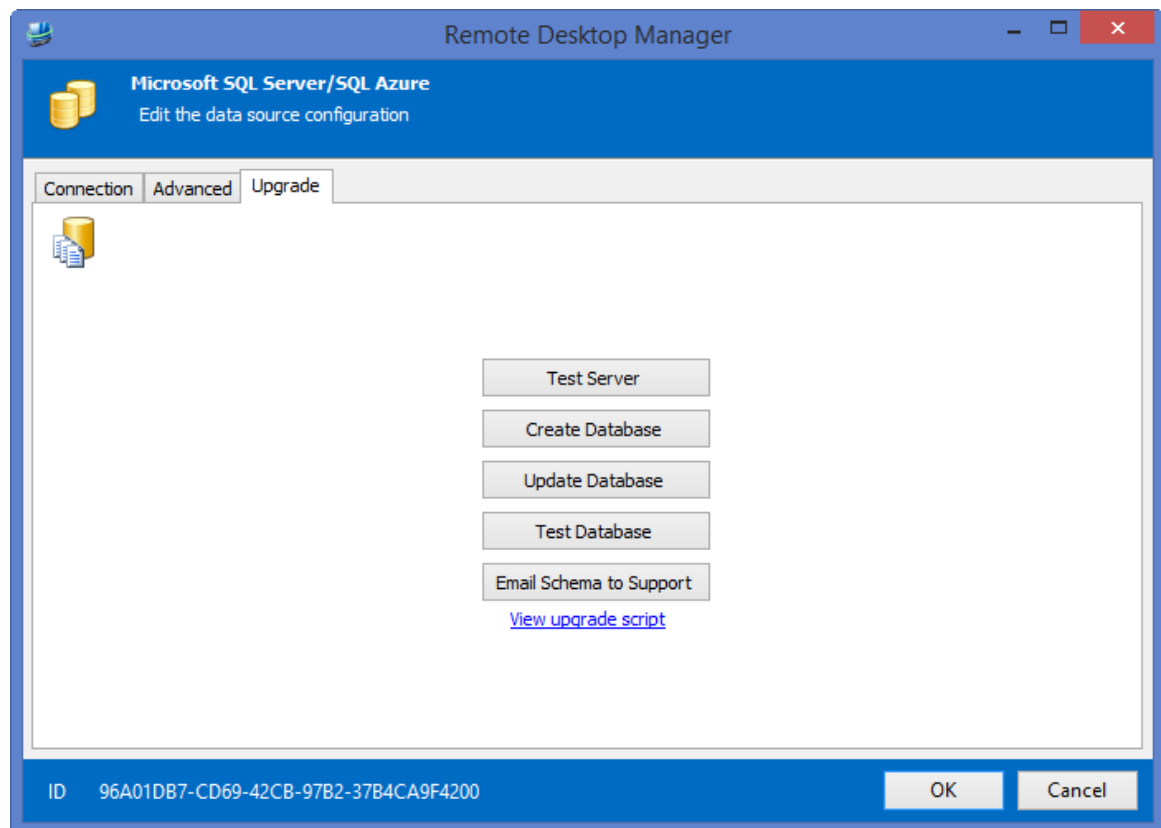
Advanced



SQL Advanced tab

Option	Description
Offline mode	Determine if you want to use this data source in Offline Mode. With this mode, the data source can be available in Read Only or in Read/Write mode
Caching mode	Determine how the entries will be reload in the data source. See Caching Mode topic for more information.
Auto refresh	Set the interval for the automatic refresh
Connection timeout	Waiting time before a connection timeout.
Command timeout	Waiting time before a command timeout.
Disable lock	Disable the option to lock the data source directly. You can still lock the application but you won't be prompted for the database password if this option is disabled.
Advanced Settings	Edit of the connection string values directly.

Upgrade



SQL Upgrade tab

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

4.2.10.2 MySQL

Description



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

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

Consult [MySQL settings](#) for more information on the configuration.

Troubleshooting

Consult [MySQL troubleshooting](#) for more information.

4.2.10.2.1 Settings

Settings

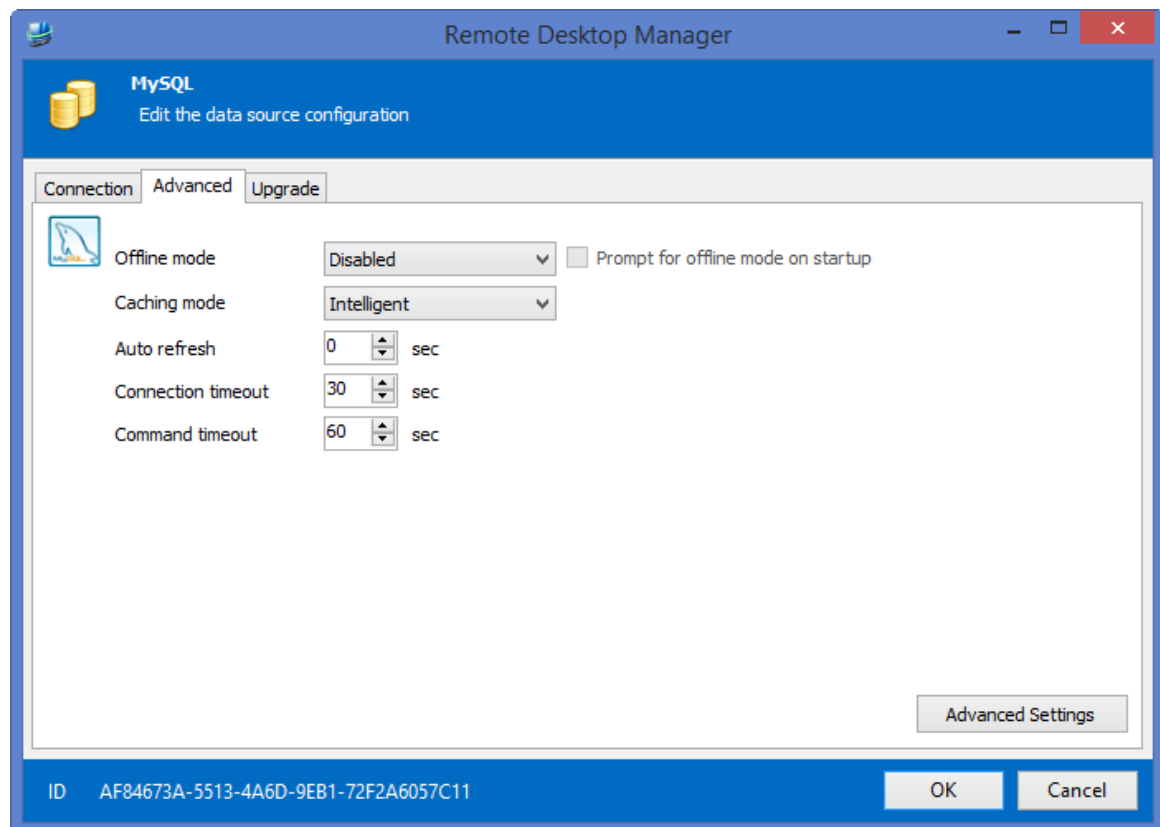
Connection

MySQL Connection tab

Option	Description
Name	Name of the data source.
Host name	Name of the server where the data source will be store.
User	Username to access the MySQL server.
Password	Password to access the MySQL server.
Schema	Name of the schema on the MySQL server for the utilization of Remote Desktop

	Manager.
Test Host	Test the connection with the Host (server) to validate if the proper information has been provided.
Test Schema	Test the connection with the schema to validate if the proper information has been provided

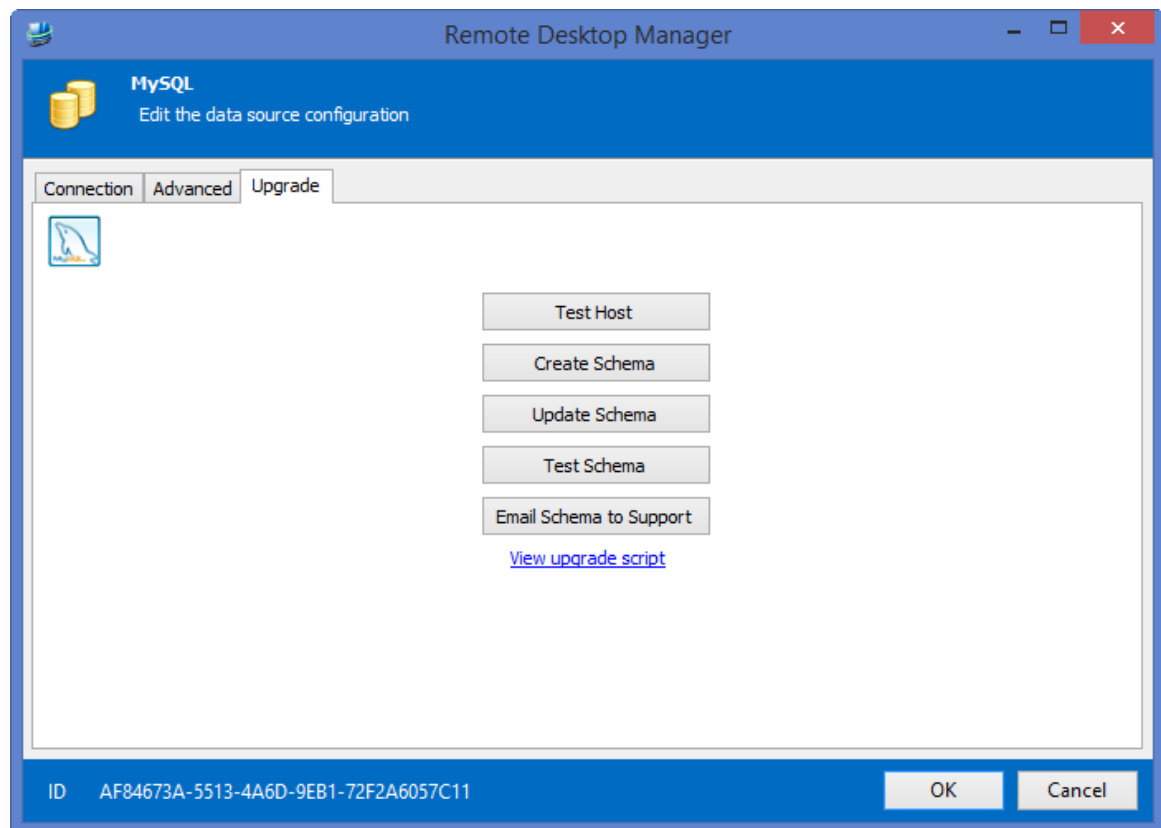
Advanced



MySQL Advanced tab

Option	Description
Offline mode	Determine if you want to use this data source in Offline Mode. In this mode, the data source can be available in Read Only or in Read/Write mode
Caching mode	Determine how the entries will be reload in the data source. See Caching Mode topic for more information.
Auto refresh	Set the interval for the automatic refresh
Connection timeout	Waiting time before a connection timeout.
Command timeout	Waiting time before a command timeout.
Advanced Settings	Edit the connection string values directly.

Upgrade



MySQL Upgrade tab

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

4.2.10.3 Remote Desktop Manager Online (RDMO)

Description



Remote Desktop Manager Online is a hosted repository managed by Devolutions. Remote Desktop Manager connects directly to the data source over the Internet. For details on this service, please visit <https://online.remotedesktopmanager.com>.

Highlights

- No VPN required to access the data

- Full connection logs
- Hosted by Devolutions on Microsoft Windows Azure and Microsoft SQL Azure
- This data source allows user and security groups management
- The offline mode can be used when the Internet is unavailable, or when the user is on the road and disconnected

For information on how to obtain a trial subscription, please consult [RDMO Trial](#). However if you have subscribed to our service and need to register, please consult [RDMO Registration](#).

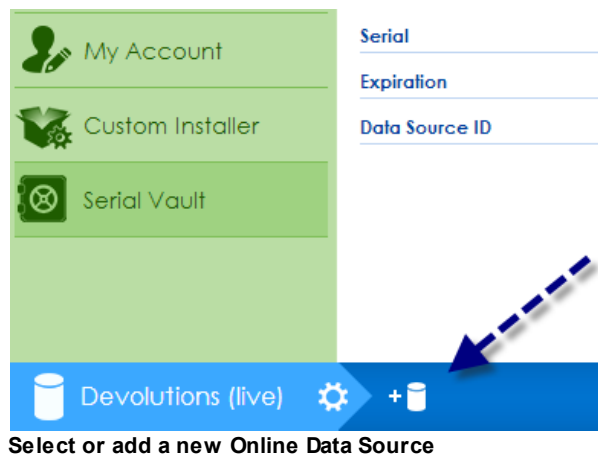
Settings

Refer to [Remote Desktop Manager Online settings](#) for more information on the configuration.

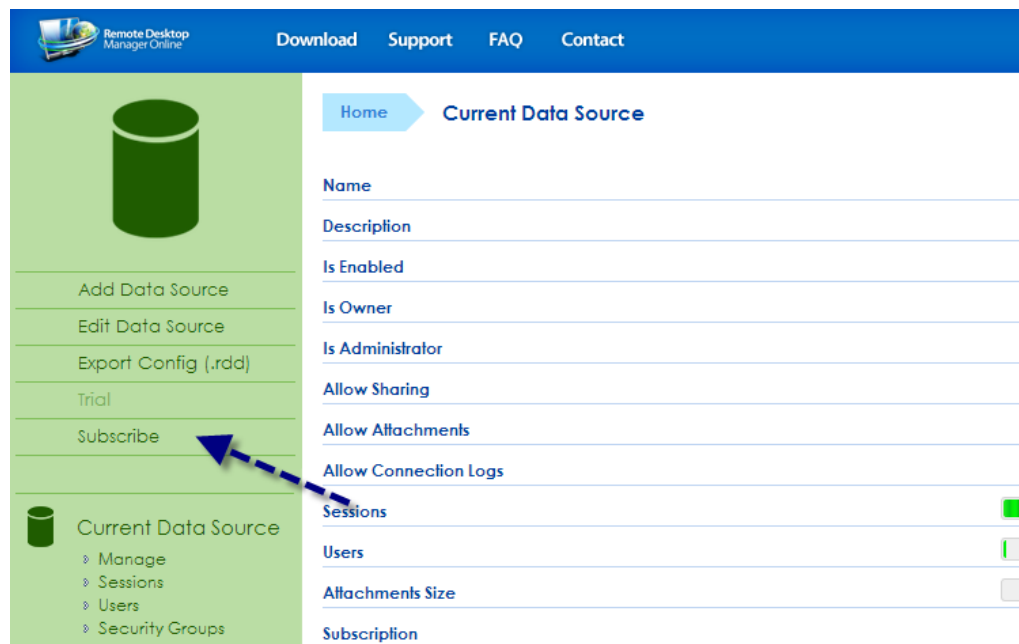
4.2.10.3.1 Activate Subscription (Register)

Description

1. Please go to <https://online.remotedesktopmanager.com> and make sure to have a valid account (free)
2. Go to: Current Data Source or create a new one with Add Data Source

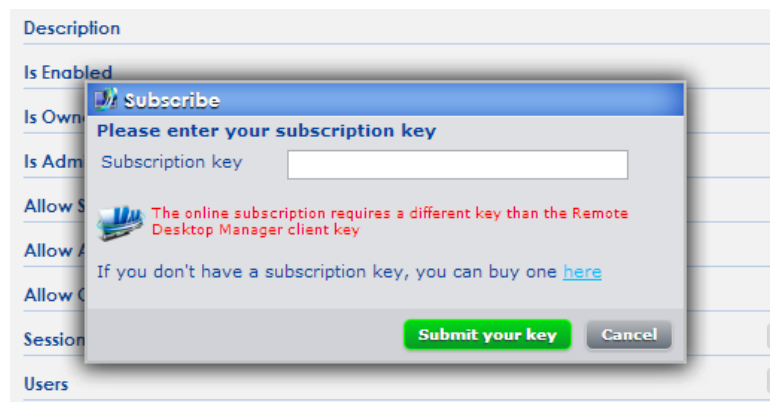


3. Click on the Subscribe button



Subscribe button

4. Enter your serial number



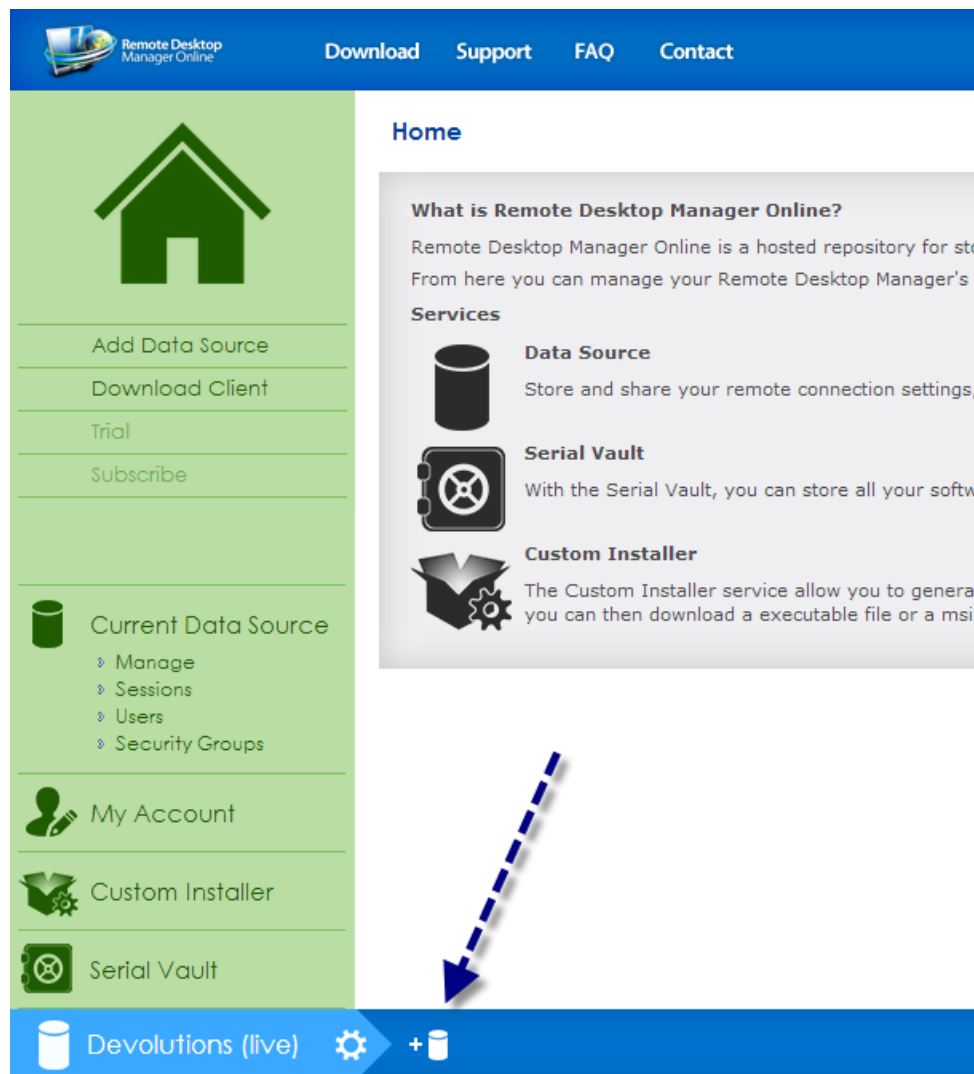
5. Use the Remote Desktop Manager client to add/edit/delete your entries

4.2.10.3.2 Activate Online Data Source Trial

Description

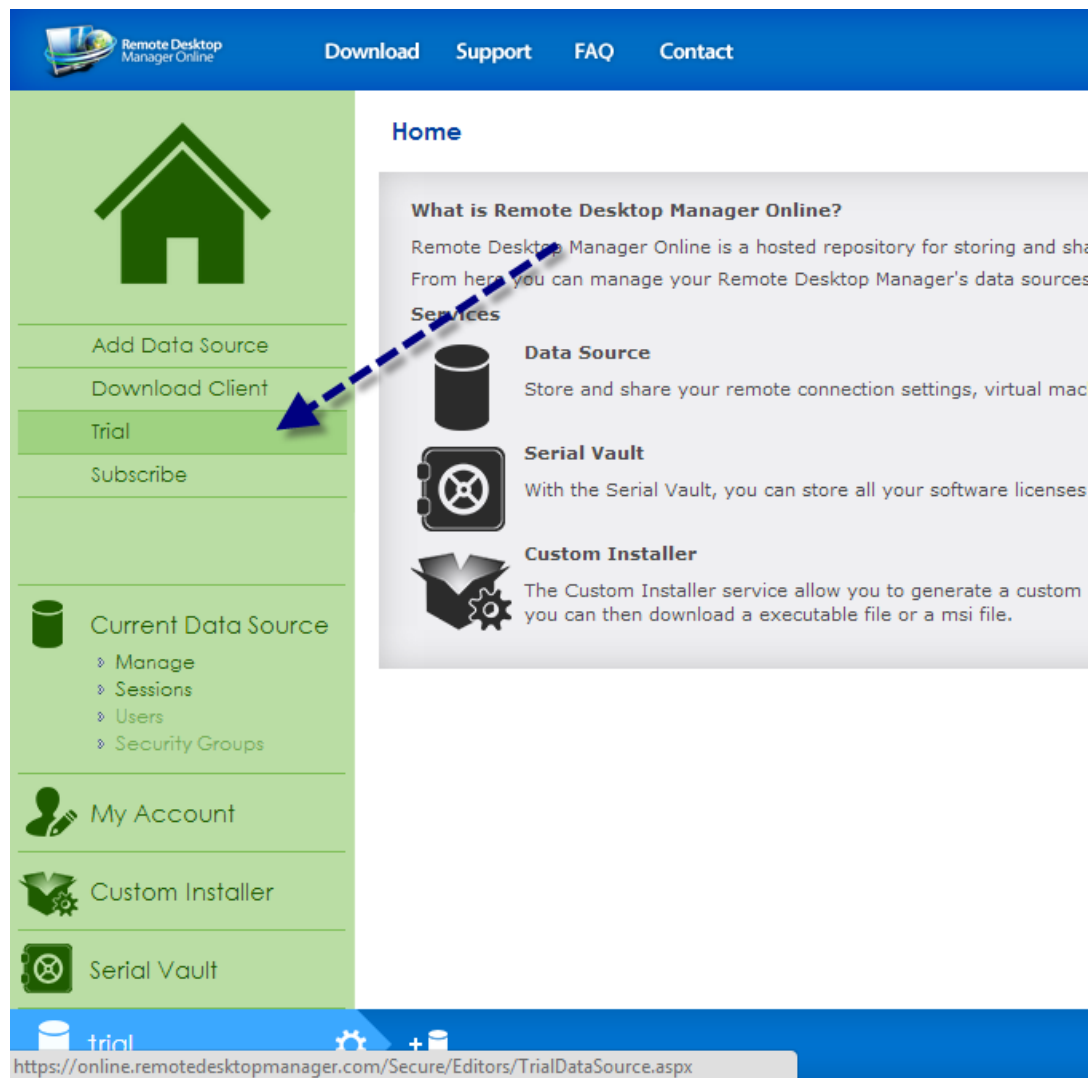
Requesting a trial for the Remote Desktop Manager Online (RDMO) service is quite easy.

1. Go online at <https://online.remotedesktopmanager.com>
2. Create a new data source

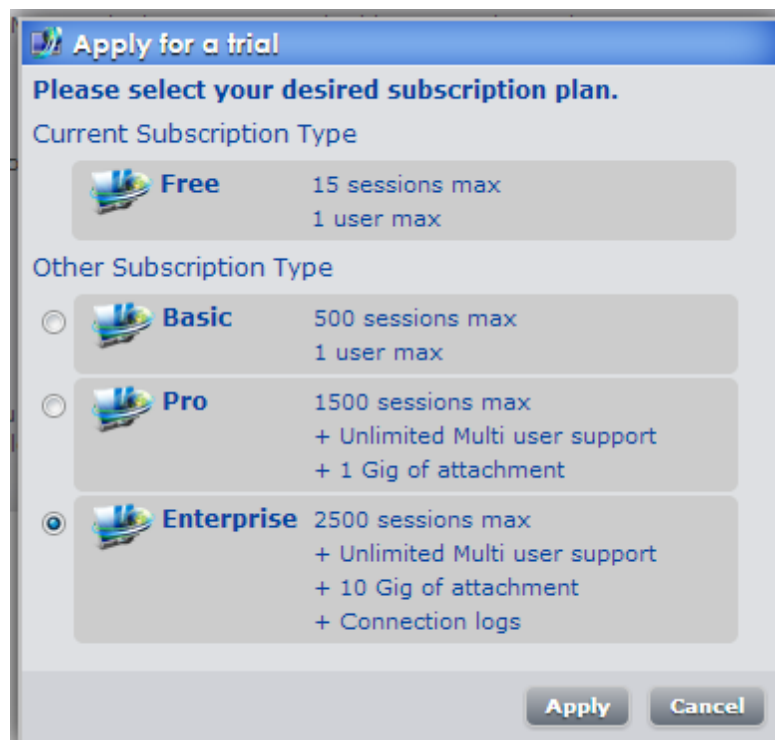


3. Enter the data source details

4. Click on the trial link



5. Choose the edition and press Apply



6. Open Remote Desktop Manager client and add the data source, more details in [Remote Desktop Manager Online \(RDMO\)](#)
7. Add/Edit/Remove users and security access, please see [User Management](#)

4.2.10.3.3 Settings

Settings

Connection

The screenshot shows the 'Remote Desktop Manager Online' window with the 'Advanced' tab selected. The window title is 'Remote Desktop Manager'. The subtitle is 'Remote Desktop Manager Online' and the instruction is 'Edit the data source configuration'. The 'Connection' tab is also visible. The 'Advanced' tab contains the following fields and options:

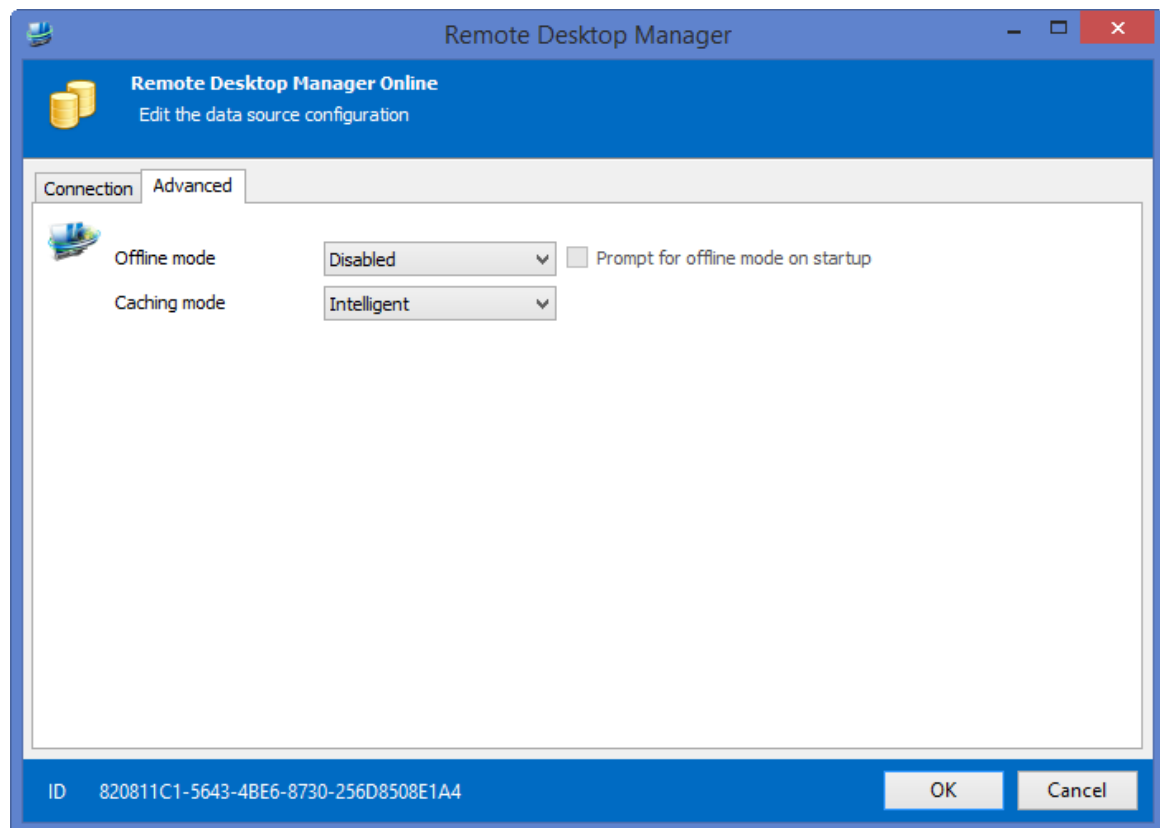
- Name:** RDMO - Online
- Email:** email@domain.com
- Always ask email:** ☐
- Password:** (masked with dots)
- Always ask password:** ☐
- Data source (Database):** (empty field with an ellipsis button)
- Data Source ID:** (empty field)

Links for creating new accounts and data sources are provided on the right. The 'Server' section at the bottom shows the ID: B5443D48-7798-421E-B447-EAA301FEC15C. 'OK' and 'Cancel' buttons are at the bottom right.

RDMO Connection tab

Option	Description
Name	Name of the data source.
Email	Email address used to connect online.
Always ask email	Always ask for email when connecting to the data source.
Password	Password to connect to the data source.
Always ask password	Always ask for password when connecting to the data source.
Data source (Database)	Name of the data source created online. You must use the ellipsis button to select it from the list of online data sources available to the entered email.
Data Source ID	Unique Key to identify the data source.

Advanced



RDMO Advanced tab

Option	Description
Offline mode	Determine if you want to use this data source in offline mode. In offline mode, the data source can be available in Read Only or in Read/Write mode. See Offline mode topic for more information.
Caching mode	Determine how the entries will be loaded from the data source. See Caching Mode topic for more information.

4.2.10.4 Remote Desktop Manager Server (RDMS)

Description



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

Highlights

- High-end security server for your company
- Share your sessions with multiple users
- Can be deployed online
- Support Windows authentication and Active Directory group integration
- Client and server side caching optimization
- Requires the Remote Desktop Manager Enterprise client (included with the server license)



Remote Desktop Manager Server supports only SQL Server as a data store at this time.

For more information please consult these topics

- [Remote Desktop Manager Server Installation](#)
- [Security Checklist](#)
- [Automatic User Account Creation](#)

Configure the server data source on all your client machines.

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

Consult [Remote Desktop Manager Server settings](#) topic for more information on the configuration.

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

4.2.10.4.1 Remote Desktop Manager Server Installation

Topology

Remote Desktop Manager Server is in fact a Web application. This allows for exposing its services on the Internet or simply an Intranet.

The recommended topology is to use two servers: a Database server and a Web server. Obviously, for small installations, a single server can be used, but resources will be shared between the two roles thereby lowering performance.



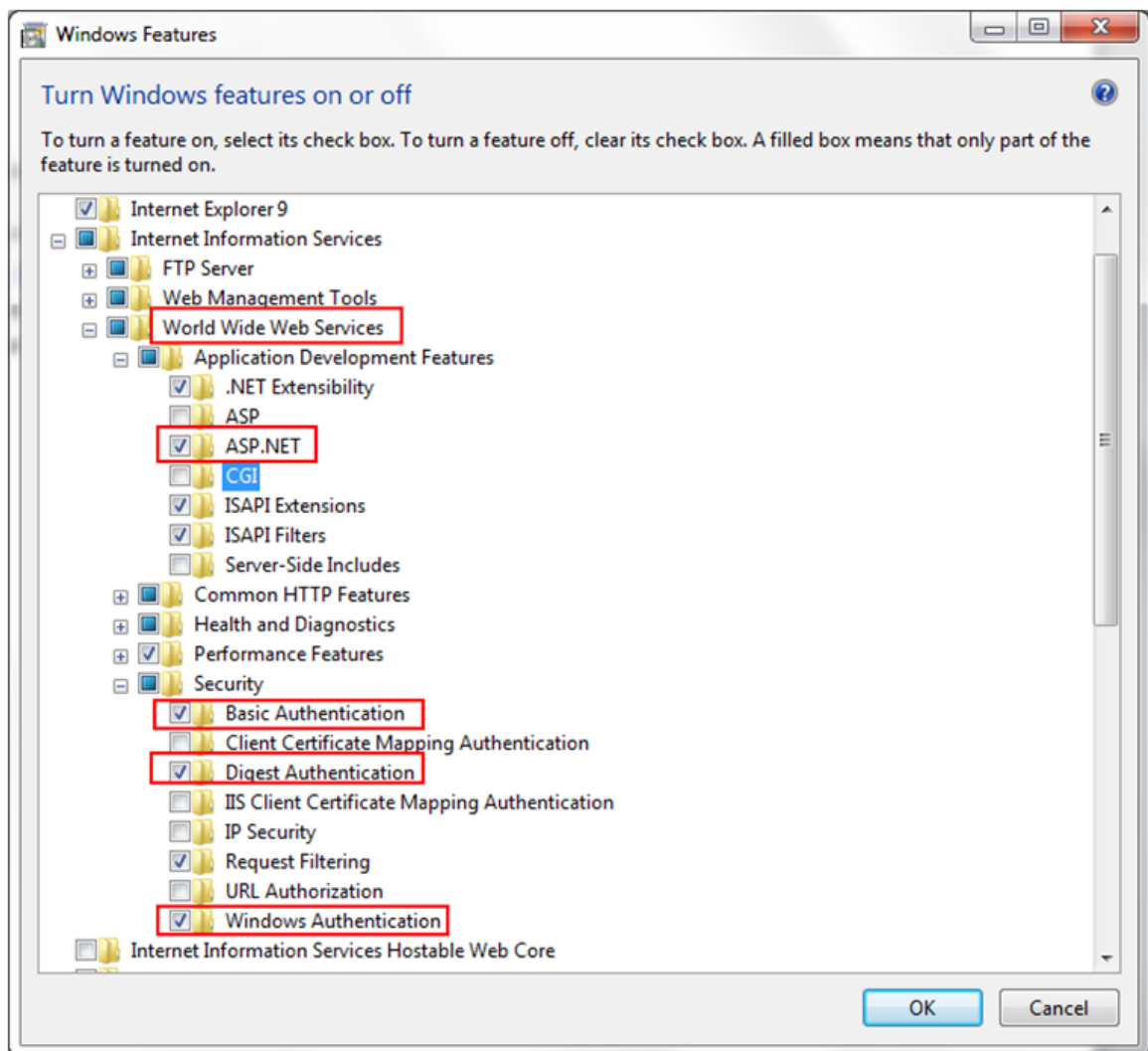
Remote Desktop Manager Enterprise Edition must be installed on the web server in order to manage the Remote Desktop Manager Server application.

For active directory integration, you should join both servers to the domain.

How to install the server

Web Server Pre-requisites

Make sure Internet Information Services is installed with all the ASP.NET requirements.



Windows features

Database server pre-requisites

Install SQL Server Express or Standard. [Download SQL Server 2012 Express from Microsoft's site](#)

Remote Desktop Manager has no requirements that would dictate what communication protocol is used, as well as many of the options offered to you by SQL Server. As long as the client workstation can connect to the SQL Server, Remote Desktop Manager will work. Also note that Microsoft has upped the default security in the 2012 version of SQL Server. The SA user is now initially disabled and you must understand each option when installing.

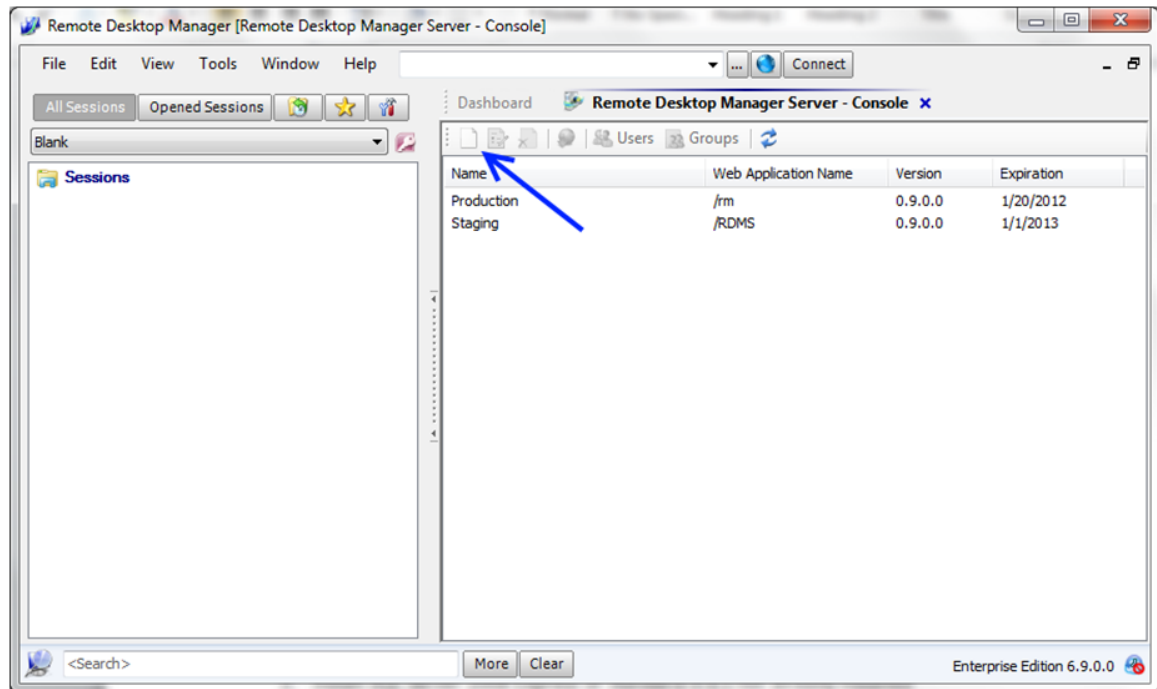
Remote Desktop Manager

1. Download and install Remote Desktop Manager on the web server. [Download](#)
2. Execute Remote Desktop Manager with elevated privileges (run as administrator).
3. From the menu **Tools > Remote Desktop Manager Server Console**, open the Remote Desktop Manager Server console.



All operations done through the console are done with the credentials used to launch Remote Desktop Manager. If you must use other credentials you must launch another window session. The RunAs command does not offer the option of starting a process with elevated privileges.

4. Deploy a new server instance.



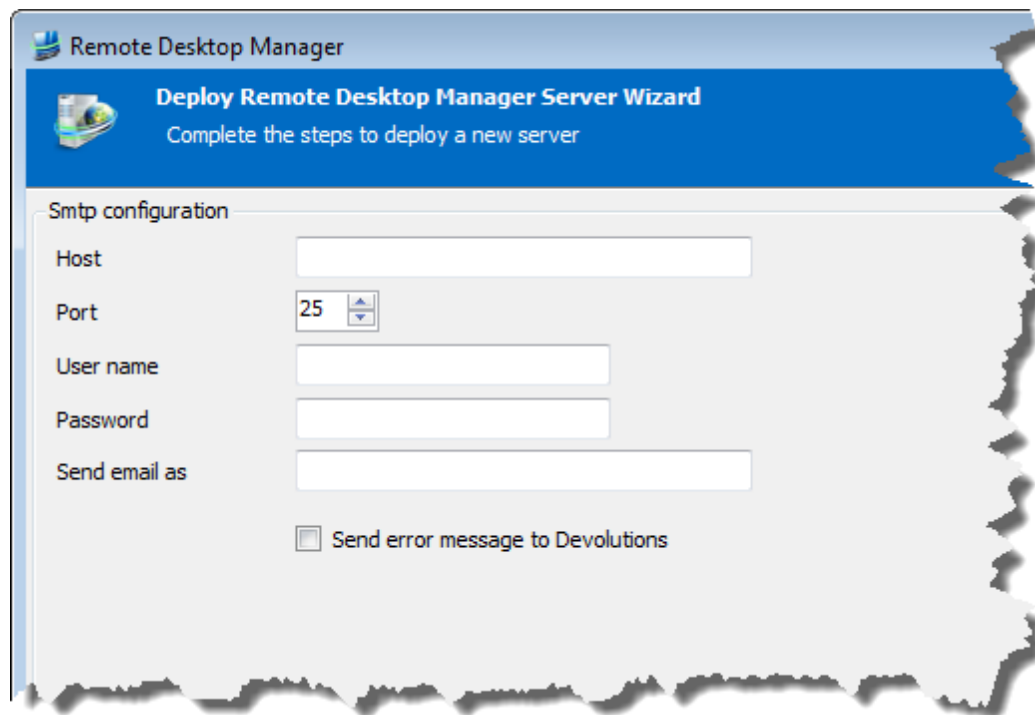
Remote Desktop Manager Server - Console

5. Configure the server with the name settings and authentication mode.

Remote Desktop Manager Server settings

Authenticate mode	Description
Built-in user	The RDMS is used to authenticate the user. You must create the initial user through the console
Domain user	The domain is used to authenticate the user.
Local machine user	The application allows a local user to be authenticated unto the server.
Database user	The database is used to authenticate the user

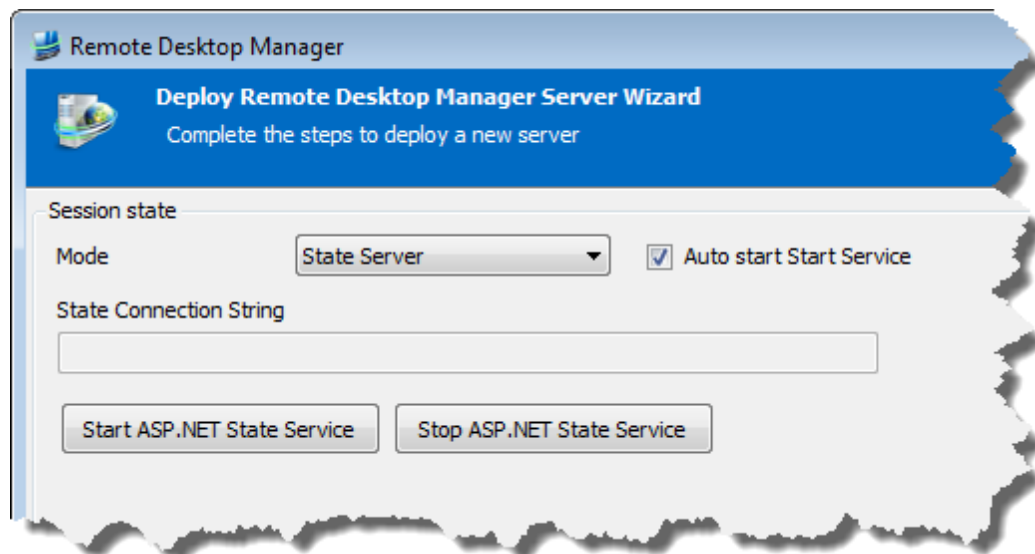
6. Enter a serial, alternatively you can [Request a trial](#)
7. Optionally configure the email setting



The screenshot shows the 'SMTP configuration' step of the 'Deploy Remote Desktop Manager Server Wizard'. The window title is 'Remote Desktop Manager'. The wizard title is 'Deploy Remote Desktop Manager Server Wizard' with the subtitle 'Complete the steps to deploy a new server'. The configuration fields include: 'Host' (text box), 'Port' (spinner box set to 25), 'User name' (text box), 'Password' (text box), and 'Send email as' (text box). There is an unchecked checkbox labeled 'Send error message to Devolutions'.

SMTP Configuration page

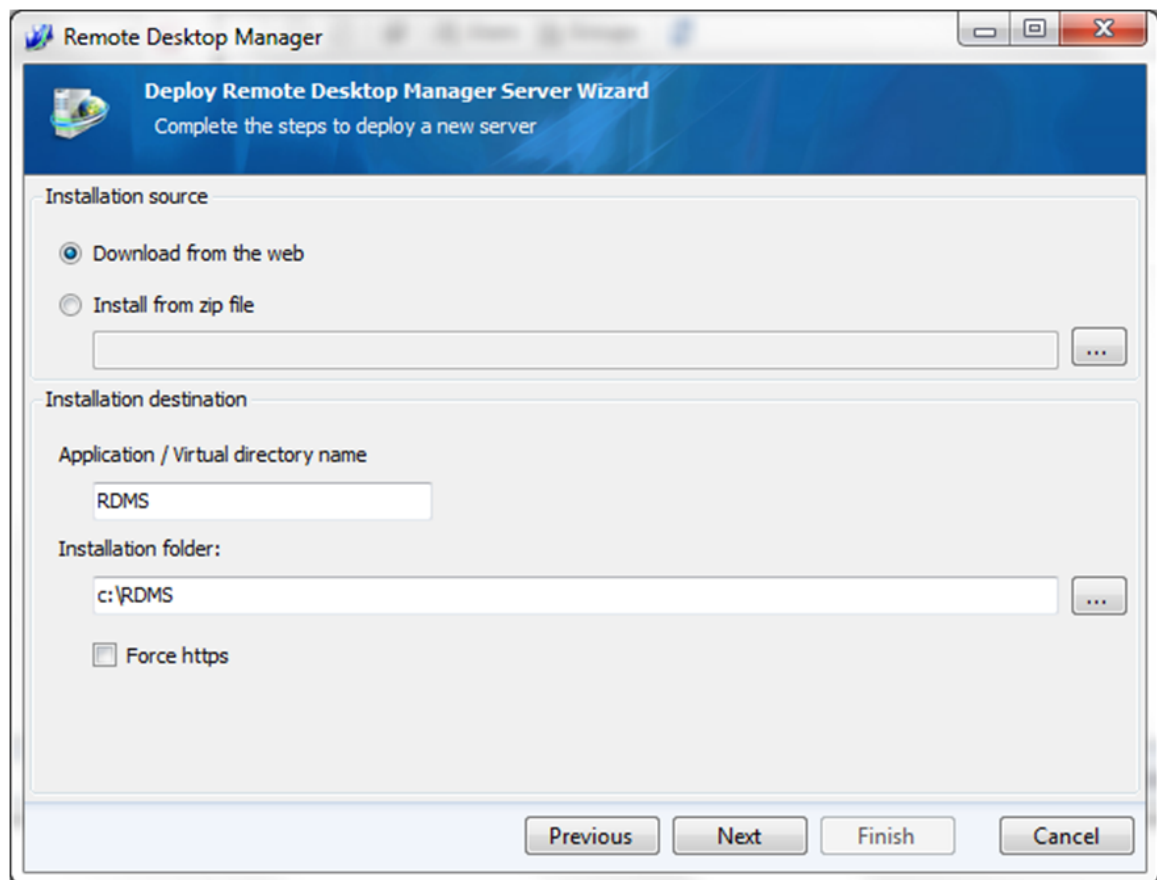
8. Ensure the ASP.NET State service is started or set to automatically start. The State Service is require to maintain web session information between each call.



The screenshot shows the 'Session state' step of the 'Deploy Remote Desktop Manager Server Wizard'. The window title is 'Remote Desktop Manager'. The wizard title is 'Deploy Remote Desktop Manager Server Wizard' with the subtitle 'Complete the steps to deploy a new server'. The configuration includes: 'Mode' (dropdown menu set to 'State Server'), 'Auto start Start Service' (checked checkbox), 'State Connection String' (text box), and two buttons: 'Start ASP.NET State Service' and 'Stop ASP.NET State Service'.

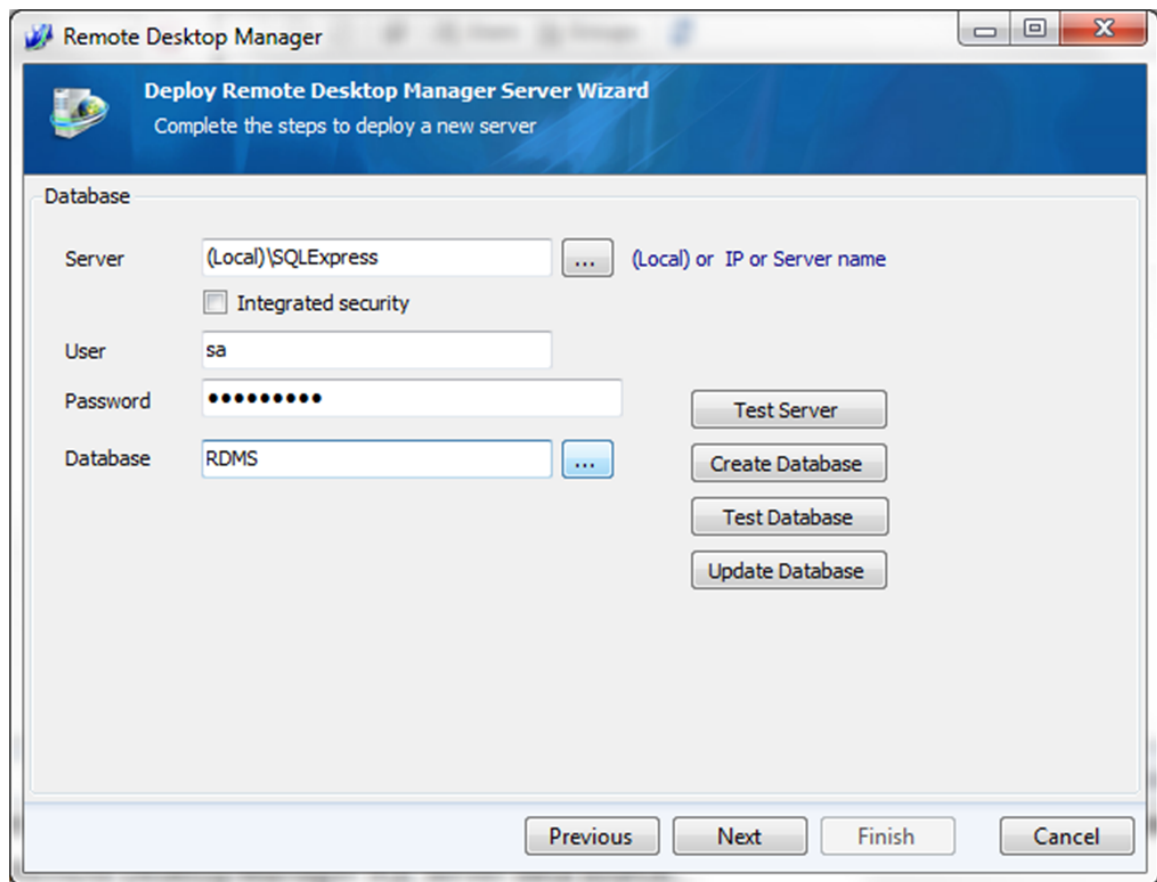
Auto Start Service

9. Select a zip file or use the automatic download. Choose a destination folder and an IIS virtual directory name.



Source/Destination

10. Enter the database settings and create the database. You can reuse an existing database from a Remote Desktop Manager SQL Server data source and just upgrade it. It's 100% compatible.

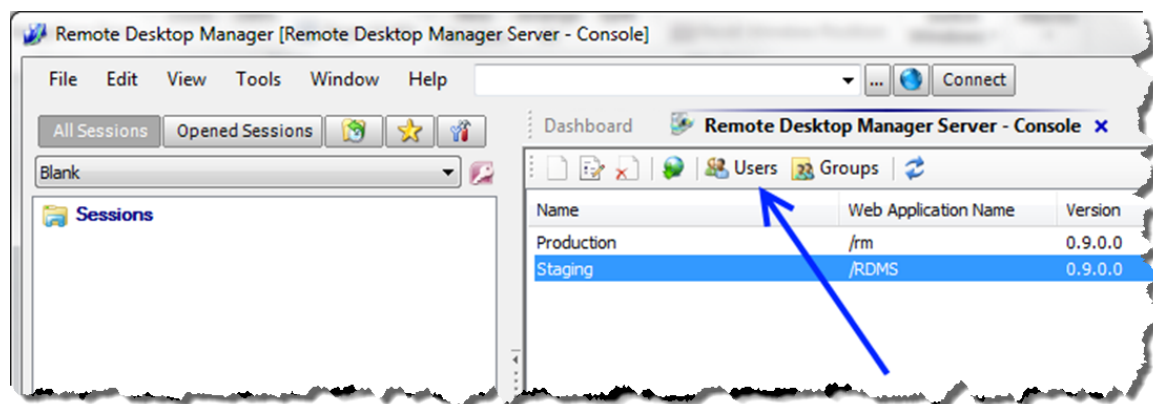
**Create a database**

11. Execute the final step and deploy the server.
12. You can test the server installation by opening the URL. e.g.: <http://localhost/RDMS>.
13. Configure users and security groups and add at least one administrator user account.

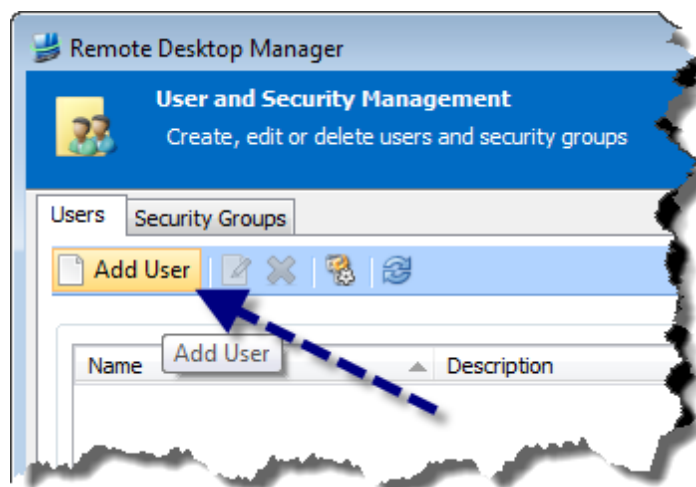


You must create an administrator account if you've enabled the RDMS Authentication model. In other cases, the account name must match with the chosen authentication model. If you are unsure of the result, also enable RDMS authentication, create an administrator account and grant the Administration privilege to the account.

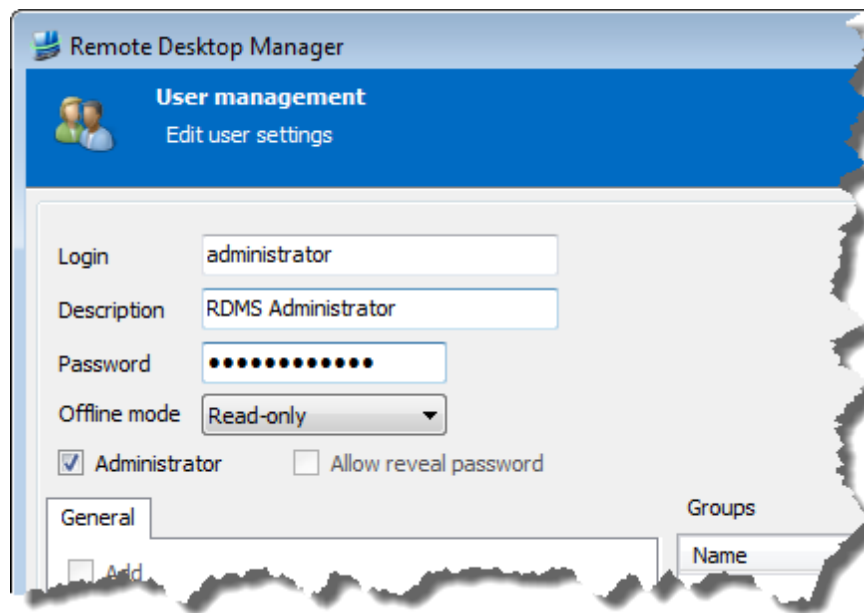
After the successful authentication with the other model, the RDMS user account will have been created and you will be able to see how to format your account names. You can then disable the RDMS authentication model. Please see [Automatic User Account Creation](#)



Configure users and security groups



User and Security Management



User management form

14. Configure the data source on all the client machines that run Remote Desktop Manager

4.2.10.4.2 Security Checklist

Description

To reach the highest possible level of security you should adhere to the following guidelines.

General

- Use Windows Authentication exclusively

SQL Server

- Enable only the **Windows Authentication Mode**
- Communicate through an encrypted connection, this will require a certificate to be installed.

Web Server

- Configure the application pool to use domain credentials. This account will need to be added to SQL Server as a login.
- Serve content only through SSL (https).

4.2.10.4.3 Automatic User Account Creation

Description

When using Remote Desktop Manager Server authentication, obviously the user account need to be created beforehand in order to authenticate to the system. In all other cases (Domain user, Local machine user or Database user), there is not match found in RDMS with the user which is authenticating.

You can create the user beforehand and assign rights as you choose, but in the event that a user logs in while there is no account for him, RDMS will create the user account.



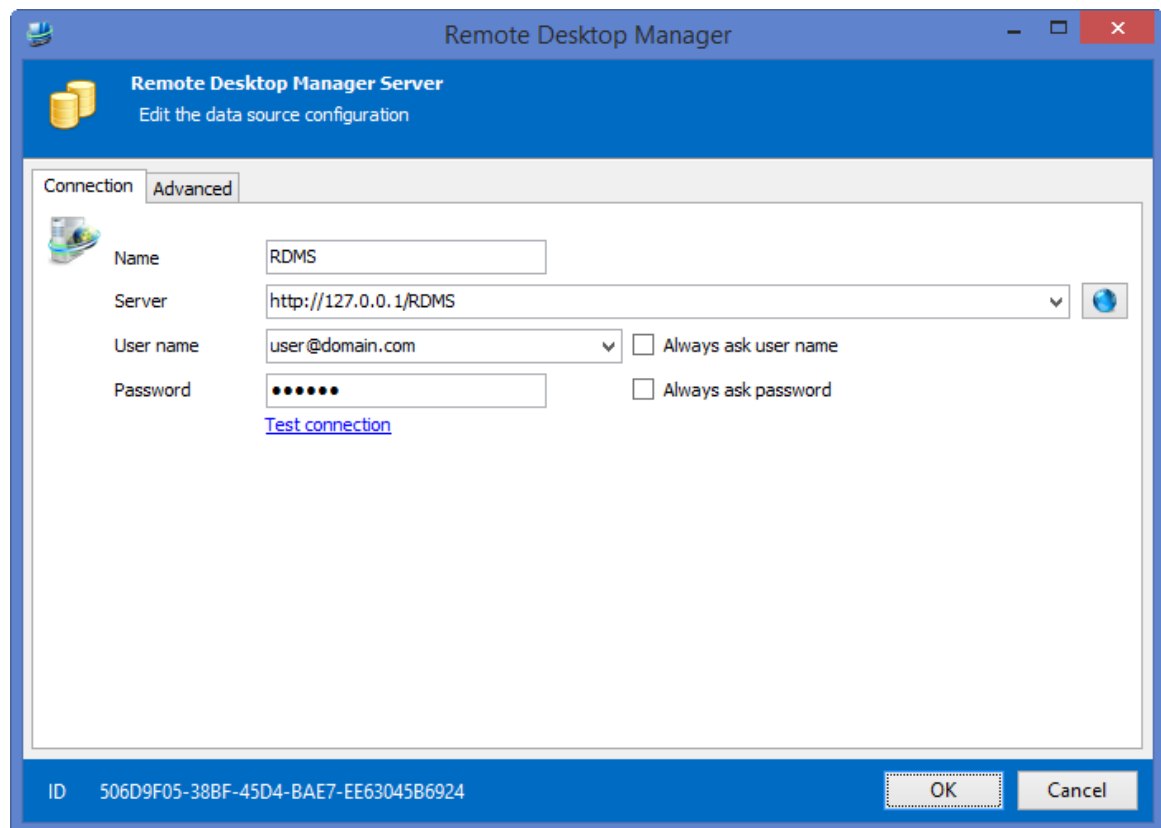
User accounts created by the server have no rights other than logging on the system. They will be able to see and edit the objects that have no security defined.

After their first login, their account is created but you must assign them the rights you see fit. Depending on the authentication mode used, the user name may be prefixed by the domain name.

4.2.10.4.4 Settings

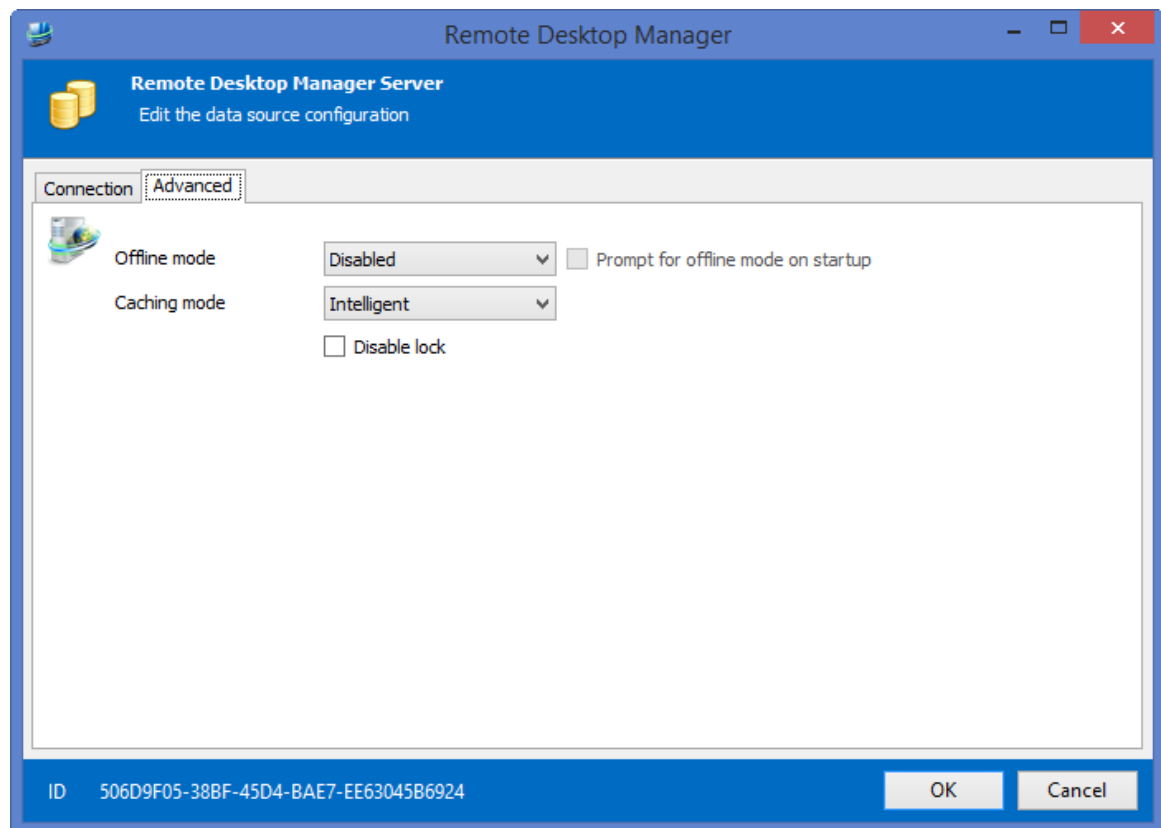
Settings

Connection

**RDMS Connection tab**

Option	Description
Name	Name of the data source.
Server	Name of Remote Desktop Manager Server instance.
Username	Username to connect to the data source.
Password	Password to connect to the data source.
Test connection	Test the connection with Remote Desktop Manager Server to validate if the proper information has been provided.
Always ask username	Always ask for the username when connecting to the data source.
Always ask password	Always ask for the password when connecting to the data source.

Advanced



RDMS Advanced tab

Option	Description
Offline mode	Determine if you want to use this data source in offline mode. In offline mode, the data source can be available in Read Only or in Read/Write mode.
Prompt for offline mode on startup	Every time you will connect on your data source, you will be prompt to use the data source in offline mode.
Caching mode	Determine how the entries will be reload in the data source. See Caching Mode topic for more information.
Disable lock	Disable the option to lock the data source.

Entry Types

Part



5 Entry Types

5.1 Sessions

5.1.1 Overview

Description

Remote Desktop Manager separates the connection types in four different categories:

- Remote connections
- Virtualization
- Cloud Explorer
- Others

Remote Connections

This category contains all of the connection types that are used to connect to a remote system, including computers, switches, VPNs or printers.

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.

Cloud Explorer

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, the text and the Windows Explorer session types in this group.

5.1.2 Types

5.1.2.1 Remote Connections

5.1.2.1.1 Citrix ICA/HDX

Description



This entry is used to define and configure a 'Citrix ICA/HDX' session.

- | | | |
|----------------------------------|-----------------------|-------------------------|
| • Auto Login (embedde mode only) | • Copy Password | • Credential Repository |
| • Embedded Mode | • External Mode | • Full Screen |
| • Support Host | • Show Opened Session | • Support Logging |

Settings

Citrix connection type support two modes:

- Config file (ICA configuration file)
- Custom configuration

The custom configuration require the XenApp Client to be installed and the session to be in embedded mode. It uses the Citrix ActiveX to open the connection. The screen size, color depth and the encryption level can be customized.

The screenshot shows a configuration dialog box with four tabs: General, Display, Programs, and Advanced. The General tab is active. It features a folder icon and two radio buttons: 'Config file name' (unselected) and 'Custom configuration (embedded mode only)' (selected). Below these are input fields for 'Computer', 'User name', 'Domain', and 'Password'. The 'Computer' field has a browse button (...). The 'Port' field is set to '0' with a dropdown arrow, and a note says 'Set the port to 0 to use the default port'. The 'Password' field has an eye icon and a key icon.

5.1.2.1.2 DameWare Mini Remote Control

Description



This entry is used to define and configure a 'DameWare Mini Remote Control' session.



- | | | |
|-----------------|-----------------|-------------------------|
| • Auto Login | • Copy Password | • Credential Repository |
| • Embedded Mode | • External Mode | • Show Opened Session |

Settings

General

Host ... Port

User ID

Password  

Shared secret

Domain

Authentication mode

☐ Auto close on disconnect

☐ Use RDP protocol

☐ Use mirror driver

☒ Bypass DMRC saved host settings

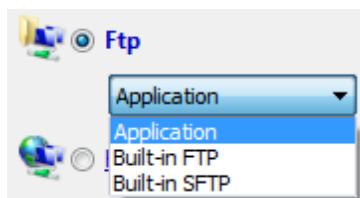
5.1.2.1.3 FTP

Description

This entry is used to define and configure a 'Ftp' session.

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

The Ftp connection type support many external applications. Moreover it's also possible to use the built-in Ftp/SFTP/FTPS

**See also**

- [Supported applications](#)
- [Built-in FTP/FTPS](#)
- [Built-in SFTP](#)

5.1.2.1.3.1 Applications

Description

The FTP-Applications mode allows you to configure an external application to perform FTP operations.

The screenshot shows the 'General' tab of a configuration window. It includes a 'Host' field with a browse button, an 'Application' dropdown set to 'Filezilla', an 'Anonymous' checkbox, 'User name' and 'Password' fields, a 'Directory' field, a 'Session' dropdown, and an 'Other parameters' field. On the right side, there are radio buttons for 'FTP' (selected), 'SFTP', 'SCP', 'FTPS', and 'Session'. Below the 'FTP' radio button is a dropdown menu for encryption, currently set to 'No encryption'. A 'Passive mode' checkbox is also checked.

General Tab

Settings

Supported applications:

Windows Explorer	Windows built-in FTP client.
Filezilla	Free cross platform FTP software (See FileZilla on Wikipedia)
WinSCP	Free open source client (See WinSCP on Wikipedia)
Default Configured	Uses the application that is configured in the RDM Default application settings.

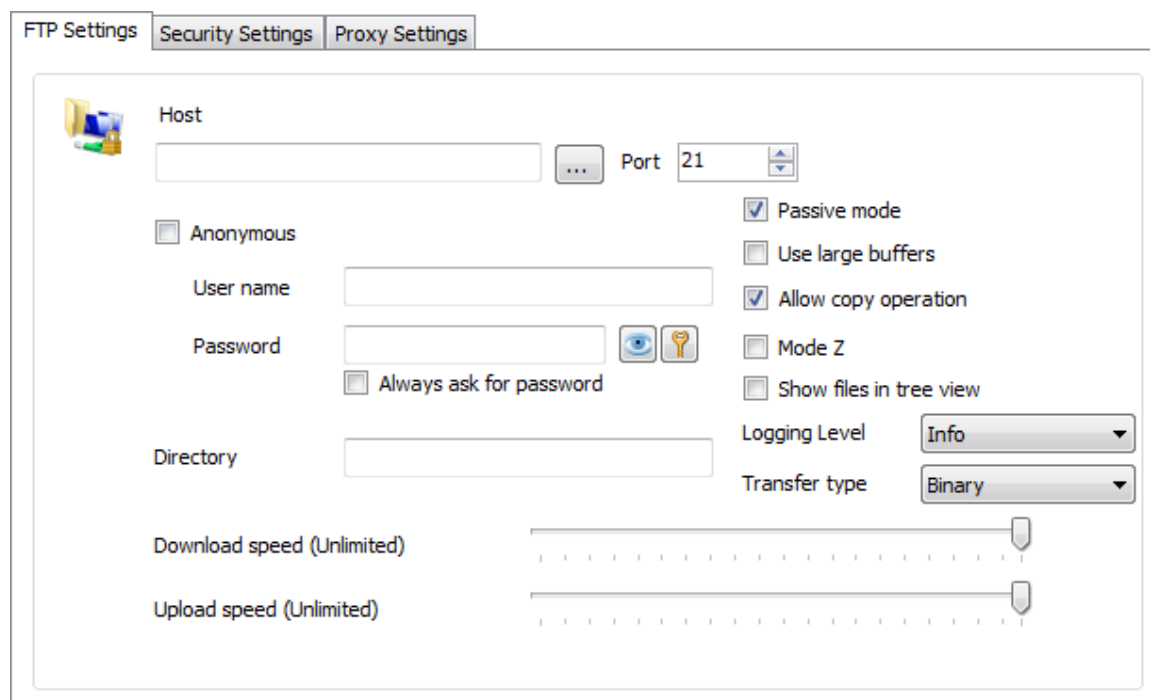
Protocol

The choice of protocols depend on the selected application. Please refer to the selected application's documentation.

5.1.2.1.3.2 Built-in FTP/FTPS

Description

This entry type allows for plain FTP or FTP Secure (also known as FTP over SSL)





FTP Settings | Security Settings | Proxy Settings

Host: Port: 21

☐ Anonymous

User name:

Password:  

☐ Always ask for password

Directory:

☒ Passive mode

☐ Use large buffers

☒ Allow copy operation

☐ Mode Z

☐ Show files in tree view

Logging Level: Info

Transfer type: Binary

Download speed (Unlimited):

Upload speed (Unlimited):

FTP/FTPS Entry

FTP Settings

Host	Host name / IP address of host
Port	Port number to use
Anonymous	Either check anonymous or enter credentials.
User name	
Password	
Always ask for password	Check in order to always prompt for the password when connecting
Directory	Set the initial directory to this value upon connection
Passive mode	Uses the FTP passive mode. By default it is ON, but you may have to turn it off depending on server options.
Use large buffers	This sets the communication library to attempt to optimize the transfer by adjusting network options. In many case you should see a performance improvement.
Allow copy operation	This option will enable the "Copy" menu to appear. The copy operation is in fact a download followed by an upload. Therefore is the remote content is highly sensitive for security reasons, or the operation can be detrimental to performance, it is best to disable the operation.
Mode Z	Activates ad-hoc compression if the server support its.
Show files in tree view	This enables showing the files in the left hand tree view instead of only in the file list.
Logging Level	Sets the level of information that is displayed in the logging window. Useful to diagnose problems.
Transfer type	Choose between ASCII or Binary.
Download speed	Specify a maximum download speed if desired. Useful to preserve network

	bandwidth for other applications
Upload speed	Specify a maximum upload speed if desired. Useful to preserve network bandwidth for other applications

Security Settings

Security type	Choose between No Security , explicit or implicit TLS/SSL.
Allowed protocol	When explicit or implicit TLS/SSL is chosen, you can specify the protocol to use.
Allowed suites	Choose between all ciphers or secure only .
Clear command channel	Credentials are encrypted, but not FTP commands themselves. This is only for the command channel.
Secure transfers	Indicates if encryption of the data itself is performed. Often the administrators need to protect only the credentials.
Client certificate	Browse for the file containing a certificate only if you want to authenticate using the certificate.

Proxy Settings

When the use of a proxy is required, enter your proxy information in this tab.

SSH Settings

When tunneling the ftp thru SSH, check Use FTP over SSH and enter the information on your SSH host.

5.1.2.1.3.3 Built-in SFTP

Description

Built-in SFTP allows the use of SSH File Transfer Protocol. (read more on [Wikipedia](#))



Only SSH v2 is supported. SSH v1 has inherent design flaws which make it vulnerable and it has been generally considered obsolete

The screenshot shows the 'SFTP Settings' tab of the Remote Desktop Manager configuration window. The settings are as follows:

- Host:** 10.10.10.10
- Port:** 21
- User name:** ftuser
- Password:** [masked]
- Directory:** [empty]
- Logging Level:** Info
- Transfer type:** Binary
- Download speed (Unlimited):** [slider at maximum]
- Upload speed (Unlimited):** [slider at maximum]
- Options:**
 - ☐ Use large buffers
 - ☒ Allow copy operation
 - ☐ Show files in tree view
 - ☐ Always ask for password

Built-in SFTP Tab

FTP Settings

Host	Host name / IP address of host
Port	Port number to use
User name Password	Enter credentials.
Always ask for password	Check in order to always prompt for the password when connecting
Directory	Set the initial directory to this value upon connection
Use large buffers	This sets the communication library to attempt to optimize the transfer by adjusting network options. In many case you should see a performance improvement.
Allow copy operation	This option will enable the "Copy" menu to appear. The copy operation is in fact a download followed by an upload. Therefore is the remote content is highly sensitive for security reasons, or the operation can be detrimental to performance, it is best to disable the operation.
Show files in tree view	This enables showing the files in the left hand tree view instead of only in the file list.
Logging Level	Sets the level of information that is displayed in the logging window. Useful to diagnose problems.
Transfer type	Choose between ASCII or Binary.
Download speed	Specify a maximum download speed if desired. Useful to preserve network bandwidth for other applications
Upload speed	Specify a maximum upload speed if desired. Useful to preserve network bandwidth for other applications

Proxy Settings

When the use of a proxy is required, enter your proxy information in this tab.

Private Key

When authenticating using a certificate, enter the key information in this tab. You can specify a filename or paste the content of the key directly. The latter is extremely useful when using a shared data source.

5.1.2.1.4 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.

- Auto Login
- 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 Overview](#) for more details.



Settings

General


Host
192.168.1.229
...

User name
david

Domain

Password
••••••••



Default Action

☐ Choose template

There is no template selected from this host.

Select templates

☒ Choose sub-connection to launch

General

Enter the Host name or IP address and credentials that apply to the Host.

Default Action

The Default Action is the one executed when either pressing enter, double-clicking or by using the Open Session command.

- **Choose template:** Will display a dialog allowing you to choose which template to apply.
 - **Select templates:** You can filter the list of templates by using this command. Using click and ctrl-click to make your selection.
- **Choose sub-connection to launch:** Will display a dialog allowing you to choose which sub-connection to launch. If only one sub-connection exists, it will be launched automatically.

5.1.2.1.5 HP Remote Graphics Receiver

Description



This entry is used to define and configure a 'HP Remote Graphics Receiver' session.

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

Settings

The screenshot shows the 'General' tab of the configuration window. It includes a 'Server' field with a browse button, a 'Port' field set to 42966, and checkboxes for 'Show login screen' and 'Show Splash screen'. There are also fields for 'User name' and 'Password' with visibility and key icons. A 'Properties' section at the bottom contains a text area with an example property: 'Ex: Rgreceiver.Network.Timeout.Warning=10000'.

General	
	Server <input type="text"/> ... Port <input type="text" value="42966"/>
<input type="checkbox"/>	Show login screen
	User name <input type="text"/>
	Password <input type="password"/>
<input type="checkbox"/>	Show Splash screen
Properties	<div><div></div></div>
Ex: Rgreceiver.Network.Timeout.Warning=10000	

5.1.2.1.6 Intel® AMT (KVM)

Description



This entry is used to define and configure a 'Intel® AMT (KVM)' session.

- Auto Login
- Built in
- Copy Password
- Credential Repository
- Embedded Mode
- Support Host
- Multi Monitor Support
- Show Opened Session
- Support AfterDisconnectEvent

Settings

The screenshot shows a settings window with three tabs: 'General', 'Settings', and 'Advanced'. The 'Settings' tab is active. Inside the 'Settings' tab, there is an Intel logo on the left, followed by the text 'Host'. To the right of 'Host' is a text input field and a button with three dots (a menu button).

5.1.2.1.7 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](#).

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.

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

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

LogMeIn general tab

5.1.2.1.7.1 Desktop Shortcut

Description

Note: As stated on the LogMeIn web site ([Comparison Chart](#)) Desktop Shortcut is a Pro Edition feature.

1. Logon onto the LogMeIn website
2. Select the desired computer
3. Edit the computer settings in LogMeIn
4. Select the tab "Desktop Shortcut"
5. Drag and drop the computer icon in Remote Desktop Manager

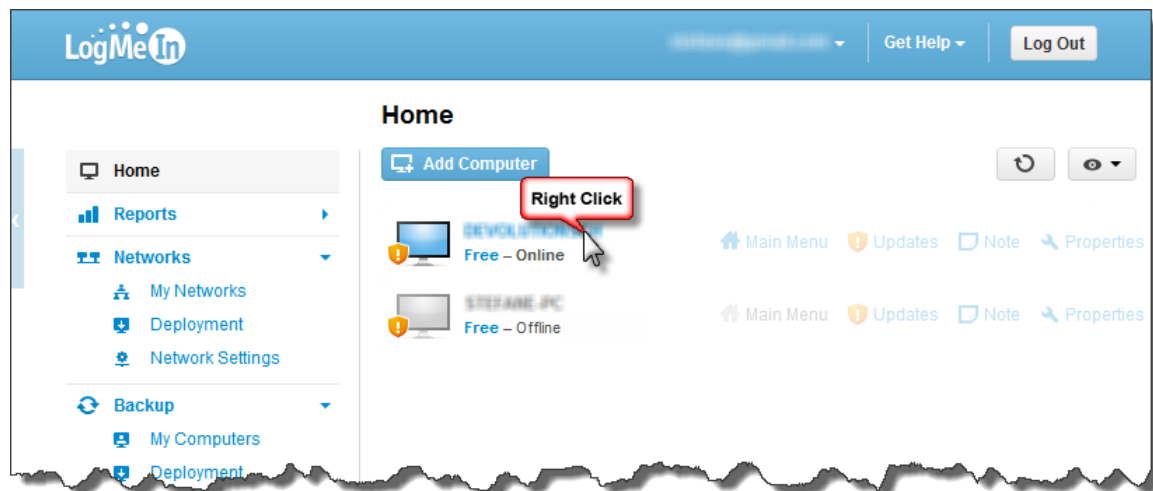


5.1.2.1.7.2 Portal (Host Url)

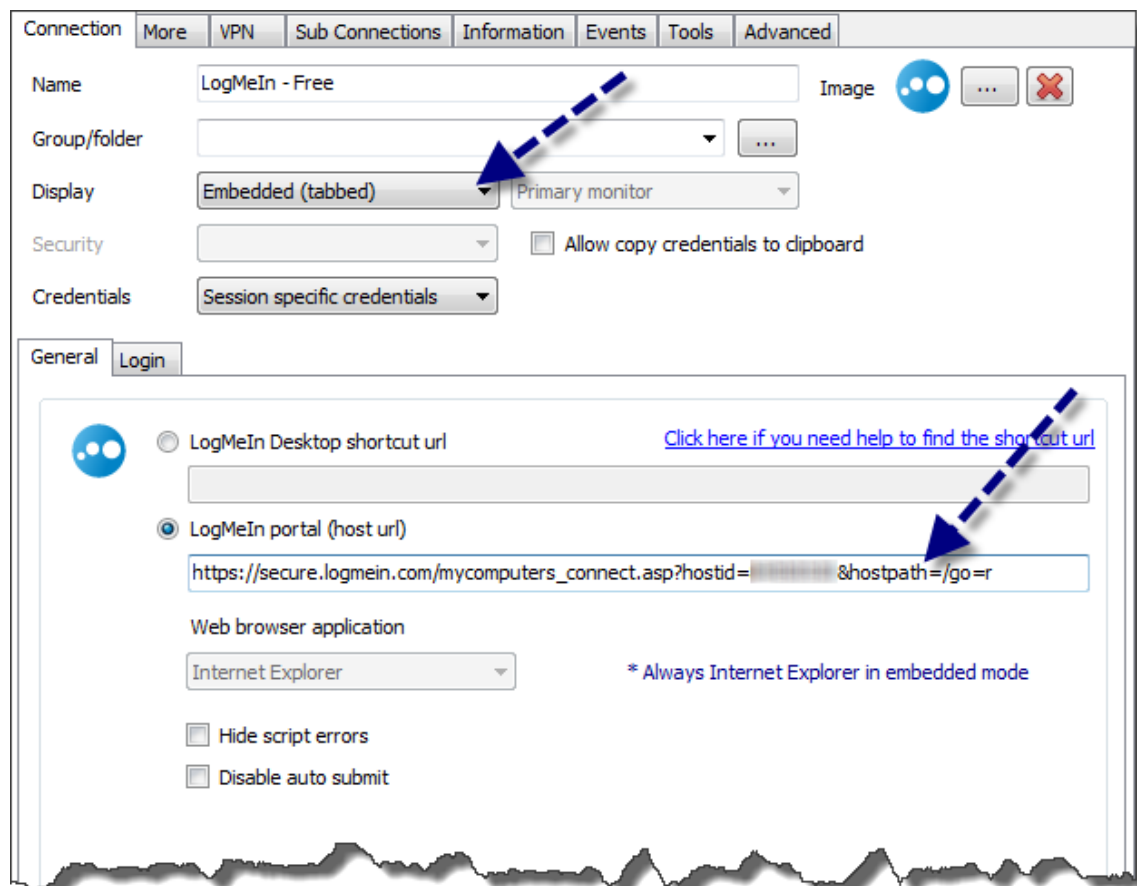
Description

Note: 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.

1. Logon onto the LogMeIn website
2. Right-Click the URL shortcut of a computer and use the copy command.
3. Paste in "LogMeIn portal (host URL)" field



LogMeIn - Home screen



LogMeIn Session - Settings

- On the "Login" tab populate both "Portal Login" & "Host Login" information

The screenshot shows the 'Login' tab of the 'LogMeIn Session' configuration window. It contains two main sections: 'Portal Login' and 'Host Login'.

Portal Login: Includes a blue circular icon with two white dots. It has input fields for 'Email' and 'Password'. To the right of the password field are two icons: an eye (toggle visibility) and a key (toggle password saving).

Host Login: Includes a gear icon with an orange keyhole. It has input fields for 'User name' and 'Password'. To the right of the password field are the same eye and key icons. A checkbox labeled 'Auto fill login' is checked and located to the right of the 'User name' field.

LogMeIn Session - Login tab

5.1.2.1.8 Microsoft Remote Desktop (RDP)

5.1.2.1.8.1 Normal

Description



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

- | | | |
|-------------------------|-----------------------------------|-------------------------|
| • Auto Login | • Built in | • Copy Password |
| • Credential Repository | • Embedded Mode | • External Mode |
| • Full Screen | • Support Host | • Multi Monitor Support |
| • Show Opened Session | • Support AfterDisconnectEvent | • Support Logging |
| • Support Reconnect | • User Settings Can Be Overridden | • Batch Edit |

Settings

General

The screenshot shows the 'General' tab of the Remote Desktop Manager interface. At the top, there are tabs for 'General', 'Display', 'Local Resources', 'Programs', 'Experience', 'Connection', and 'Advanced'. The 'General' tab is active, displaying 'Logon settings'. A computer icon is next to the 'Computer' field, which contains 'DEVOLUTIONS-PDC'. To its right is a 'Port' field with '0' and a note: 'Set the port to 0 to use the default port'. Below these is an 'RDP type' dropdown menu set to 'Normal'. Further down are 'User name' and 'Domain' text boxes. There are two checkboxes: 'Open console (Admin mode)' and 'Always ask for credentials', both currently unchecked. Two radio buttons are present: 'Store password on the local computer' (selected) and 'Store password in the database'. Below the first radio button are 'Save Password' and 'Clear Password' buttons. Below the second radio button is a 'Password' text box with eye and key icons to its right.

General tab

Option	Description
Computer	Enter the name of the remote computer.
Port	Enter the port to access the remote computer. Set the port to 0 to use the default port.
RDP Type	Select the RDP session type. Select between: <ul style="list-style-type: none"> • Normal • Azure • Hyper-V (embedded only)
Username	Enter the username to connect on the remote computer.
Domain	Enter the domain to connect on the remote computer.
Open console (Admin mode)	Connect to the console session of a server using Remote Desktop for Administration.
Always ask for credentials	Always ask for credentials when connecting to the remote computer.
Store password on the local computer	This will use the Windows Credential Manager. It is not the best option because it has the following limitations: <ul style="list-style-type: none"> • 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. • 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.
Store password in the database	The password will be store in the database.



With the Standard Edition, you can now save your credentials as long as you use an [XML](#) or a [SQLite](#) data source.

Display

General Display Local Resources Programs Experience Connection Advanced

Remote desktop size

Remote desktop size Default ☐ Center on screen

Custom width 0 Custom height 0

☐ Smart sizing (scale the client window display of desktop when resizing)

☐ Span on multiple screens if possible

☒ Fit embedded RDP in window

☐ Use all my monitors for the remote session

Colors

Highest Quality (32 bits)

Note: Settings on the remote computer might override this setting.

☒ Display the connection bar when in full screen mode

☒ Connection bar pinned (full screen)

Display tab

Option	Description
Remote Desktop Size	Select the prefer screen size on the remote computer.
Center on screen	Remote computer screen will be center in the middle of the screen.
Custom width	Specify a custom width number for the screen size.
Custom height	Specify a custom height number for the screen size.
Smart sizing	Scale the client window display of desktop when resizing.
Span on multiple screens if possible	Extend the remote computer screen on multiple screens when possible.
Fit embedded RDP window	The embedded display mode need to be select to be able to check "Fit embedded RDP window".
Use all my monitors for the remote session	Use all the monitors when connected on the remote computer.
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)

The connection bar can be pinned or unpinned when screen is in full size.

Local Resources

Local Resources tab


Option	Description
Remote computer sound	Indicate what to do with the sound on the remote computer. Select between: <ul style="list-style-type: none"> • Bring it 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: <ul style="list-style-type: none"> • Do not record • Record from this computer
Keyboard	Windows key combination will be execute: <ul style="list-style-type: none"> • On the local computer • On the remote computer • In full screen mode only
Local devices and resources	Select the devices and resources that you want to use on the remote computer. Select between: <ul style="list-style-type: none"> • Printers • Serial Ports • Hard drives • Clipboard

	<ul style="list-style-type: none"> • Prompt for selected resources • 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

General Display Local Resources **Programs** Experience Connection Advanced

Start a program

 ☐ Start the following program on connection

Program path and filename:

Start in the following folder:

☐ Use RemoteApp (seamless mode)

Program

Parameters

Programs tab


Option	Description
Start the following program on connection	Select if a specific program need to be start at the opening of a session on the remote computer.
Program path and filename	Specify the program path and filename to start the application at the opening of a session on the remote computer.
Start in the following folder	Specify a folder to open at the startup of a session on the remote computer.
Use RemoteApp (seamless mode)	Open an rdp connection, starts a specified program, maximizes the application window and runs without the windows desktop.
Program	Specify the program for the RemoteApp.
Parameters	Specify the parameters for the RemoteApp.

Experience

General Display Local Resources Programs **Experience** Connection Advanced

Performance

Choose the connection speed to optimize performance

 Default

Allow the following:

☒ Desktop background ☐ Redirect DirectX

☐ Font smoothing ☐ Redirect video playback

☐ Desktop composition ☒ Load plug-ins in embedded mode

☒ Show contents of window while dragging ☒ Enable data compression

☒ Menu and window animation

☒ Themes

☒ Bitmap caching

☐ Detect network automatically

Cache Default

☒ Detect bandwidth automatically

Keep alive 0 sec

☒ Reconnect if connection is dropped

Experience tab


Option	Description
Choose the connection speed to optimize performance	Specify the connection speed to use to optimize the remote session performance. Select between: <ul style="list-style-type: none"> • Default • Modem (56 kbps) • Low-speed broadcast (256 kbps - 2 Mbps) • Satellite (2-16 Mbps with high latency) • High-speed broadcast (2-10 Mbps) • WAN (>10 Mbps with high latency) • LAN (> 10 Mbps with low latency)
Allow the following	The following options can be enable to be available on the remote computer: <ul style="list-style-type: none"> • Desktop background • Font smoothing • Desktop composition • Show contents of window while dragging • Menu and window animation • Themes • Bitmap caching • Redirect DirectX • Redirect video playback • Load plug-ins in embedded mode

	<ul style="list-style-type: none"> • Enable data compression • Detect network automatically • Detect bandwidth automatically • Reconnect if connection is dropped
Cache	Select the type of cache that will be use for the remote session: <ul style="list-style-type: none"> • Default • Full mode • Thin client • Small cache
Keep alive	Data will be sent to the remote computer to keep the session alive. You can determinate the time between that the data is send.

Connection


General Display Local Resources Programs Experience **Connection** Advanced

Authentication

 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 (SingleSignOn)

 ☐ Automatically detect RD Gateway server settings

☒ Use these RD Gateway server settings:

Server name

Logon method

☐ Open gateway only when unable to ping host

☐ Bypass RD Gateway server for local addresses

☐ Use my RD Gateway credentials for remote computer

☐ Do not use RD Gateway server

Connection tab

Option	Description
Server authentication verifies that you are connecting to the intended remote computer	If the actual verification does not meet minimum policy requirements, select what need to be done by the remote computer between the following: <ul style="list-style-type: none"> • 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.
Server name	Enter the RD Gateway server name.
Logon method	Select the logon method between: <ul style="list-style-type: none"> • Ask for password (NTLM) • Smart card • Allow me to select later
Open gateway only when unable to ping host	Establish a connection with the RD Gateway server only when it's 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 my RD Gateway credentials for remote computer	Use your personal RD Gateway credentials to connect on the remote computer.
Credentials	See RDP Gateway credentials section.
Do not use RD Gateway server	Don't use any RD Gateway server to connect on the remote computer.

RDP Gateway credentials

Remote Desktop Manager

RDP Gateway credentials
Please enter your gateway credentials

☒ Use custom credentials

User name

Domain

☒ Store password on the local computer

Save Password

Clear Password

☐ Store password in the database Password

☐ Use credential repository

☐ Use my personal credentials


OK Cancel

RDP Gateway Credentials

Option	Description
Use custom credentials	Use a specific User name, Domain and store the password on the local computer or store the password in the database.
Use credential repository	Uses a linked Credential Entry. See topic Credentials for more information.
Use my personal credentials	Use the credentials stored in My Personal Credentials .

Advanced

General Display Local Resources Programs Experience Connection **Advanced**



 Enable CredSSP support Default

Keyboard layout [Default](#)

Minimal input send interval 100 ms ☐ Background input

☐ Full reconnect

Connection Broker - High Availability


 Workspace ID ☐ Use redirection server

Alternate full adress

Load balance info

Advanced tab

Option	Description
Enable CredSSP support	RDP will use the Credential Security Support Provider (CredSSP) for the authentication on the remote computer. Select between: <ul style="list-style-type: none"> • Default • True • False
Keyboard layout	Indicate the Remote Desktop keyboard layout that you want to use on the remote computer.
Minimal input send interval	Set the minimum time in milliseconds between the input is send to the remote computer.
Background input	The remote computer can accept input even when the focus is not on the session.
Full reconnect	Will perform a full reconnect on the remote computer if the

	connection has been lost because of a network disconnection.
Workspace ID	Enter the Workspace ID that contains the settings associated to the RemoteApp and Desktop ID.
Use redirection server	Redirect a remote computer to the RDP session host.
Alternate full address	Indicate an alternate name of the remote computer that you want to connect on.
Load balance info	Indicate the load balance info when the load balancing feature is enabled on the RD Connection Broker.

5.1.2.1.8.2 Azure RDP

Overview

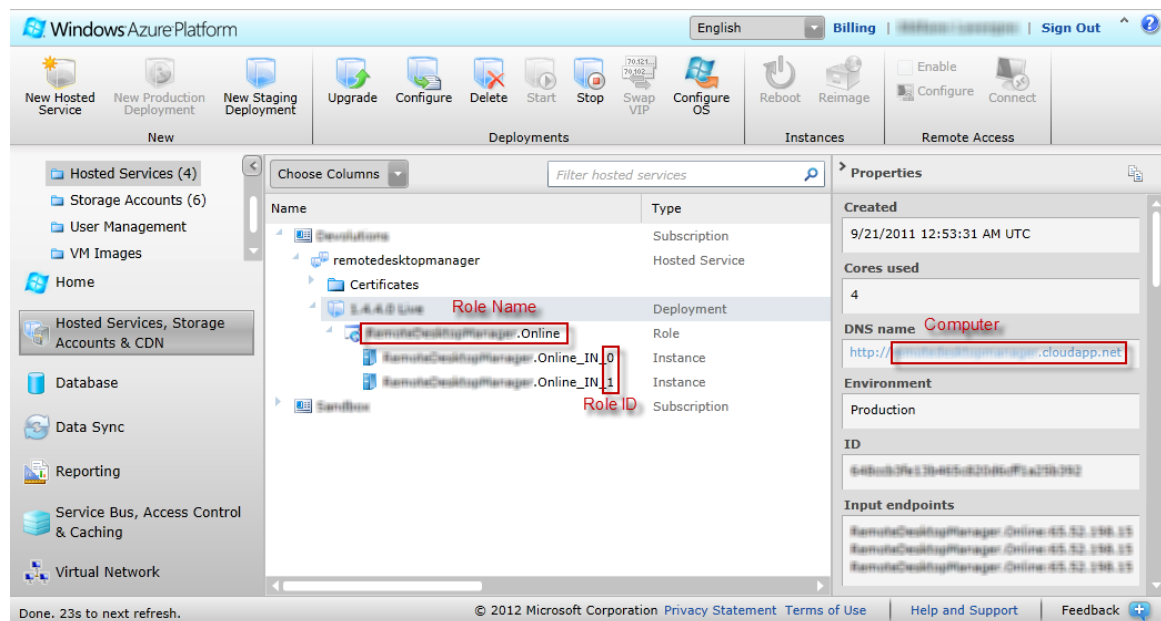
RDP directly into an Azure role instance without having to use the Azure Management Console (<https://windows.azure.com>).

Settings

First, enable Azure RDP access by following these instructions:

<http://msdn.microsoft.com/en-us/library/windowsazure/gg443832.aspx>

Second, open the Azure Management Console (<https://windows.azure.com>) and select the deployment you would like to connect to. You'll need the DNS name (Computer), Role Name & Role IDs.



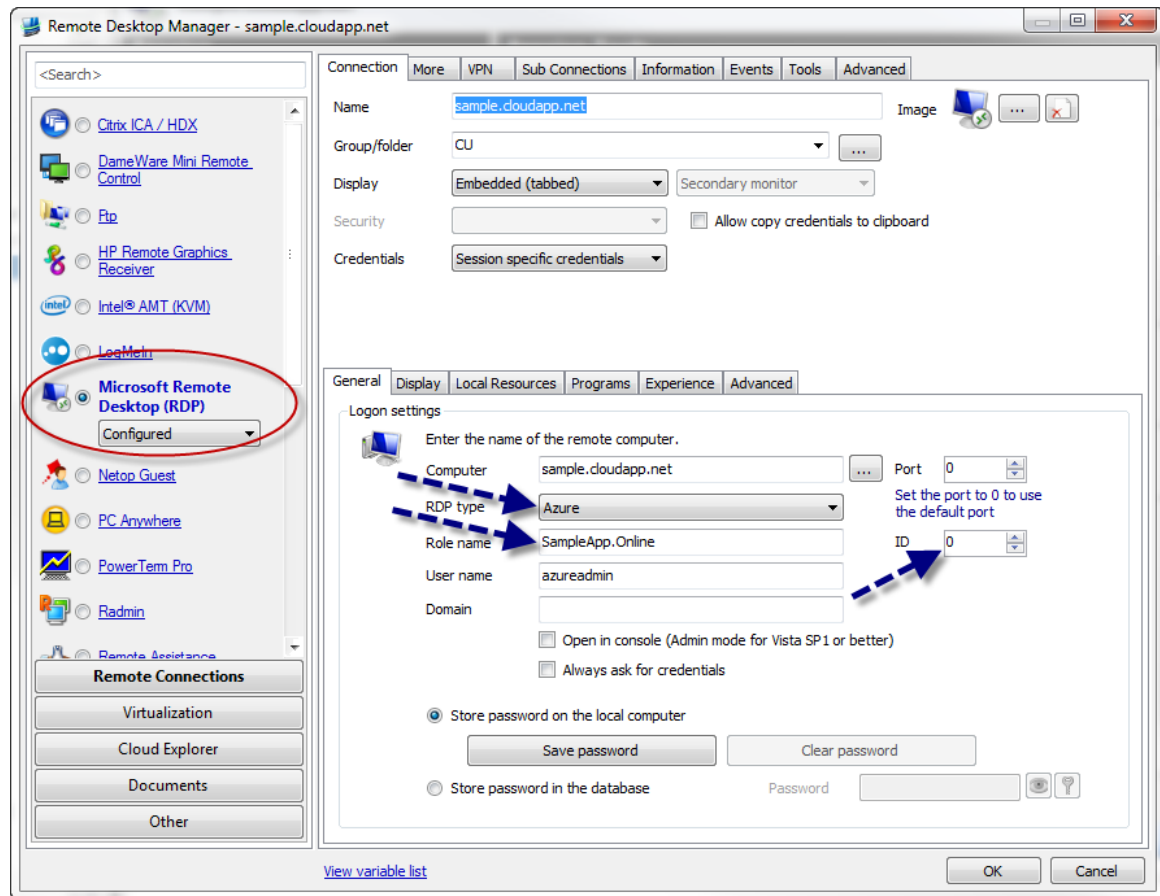
Azure Management Console

Third, create a new RDP session with the following values:

Computer: Azure DNS (the name of the Azure Role deployment)

Role Name: Azure role name

ID: The azure role ID (if you have 8 instances running, then 0 - 7 are the IDs)



Create Azure RDP session

Troubleshooting

Is RDP access configured in your Azure account?

<http://msdn.microsoft.com/en-us/library/windowsazure/gg443832.aspx>

5.1.2.1.8.3 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.

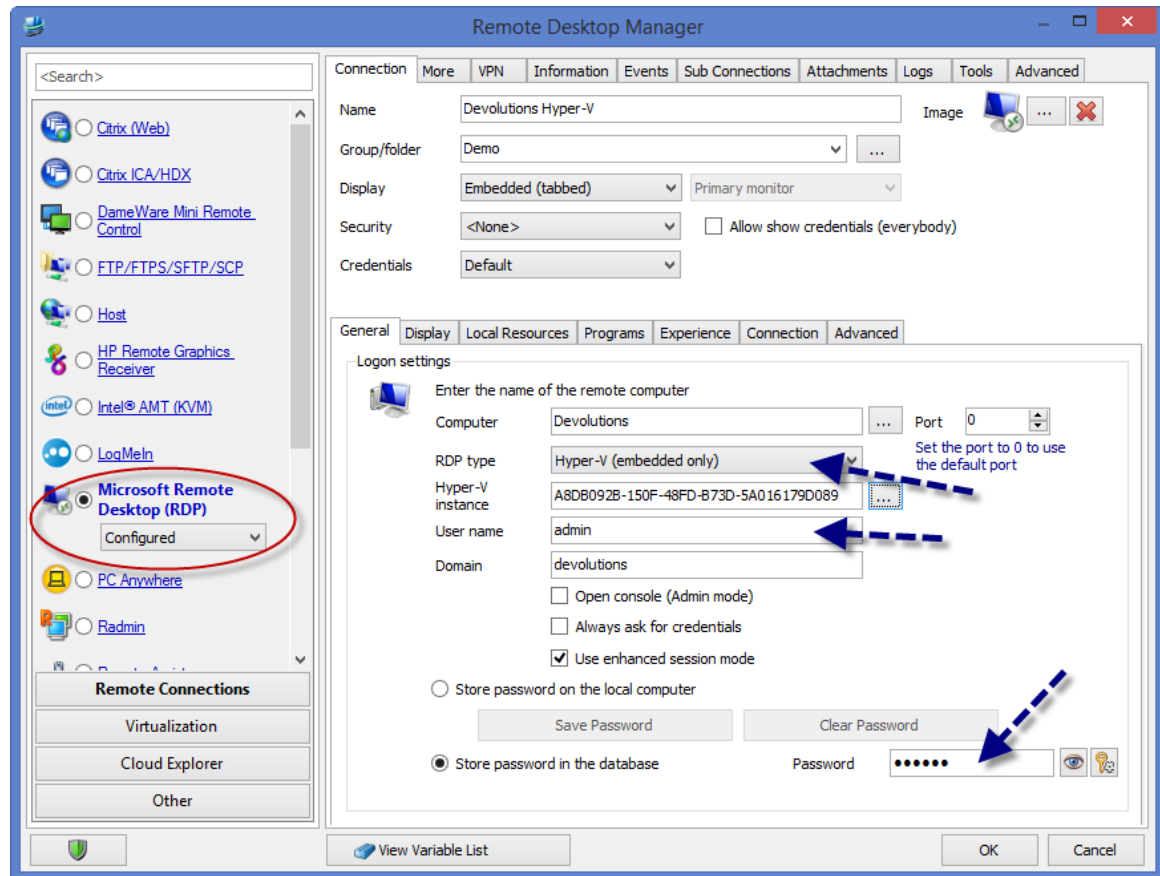


Auto login to the Hyper-V instance is not supported.



The credentials provided are for the Hyper-V server (not the instance).

Settings



Create Hyper-V RDP session

Create a new RDP session to 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.

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

- 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

Ensure that your credentials include admin rights on the Hyper-V server. Also ensure that WMI ports are open, and that no firewalls are blocking connections.

<http://blog.mpecsinc.ca/2009/06/hyper-v-error-access-denied-unable-to.html>

Check to see whether Hyper-V Tools for Remote Administration are working: <http://technet.microsoft.com/en-us/library/cc794756.aspx>

Links

[Hyper-V Dashboard](#)

5.1.2.1.9 NoMachine

Description

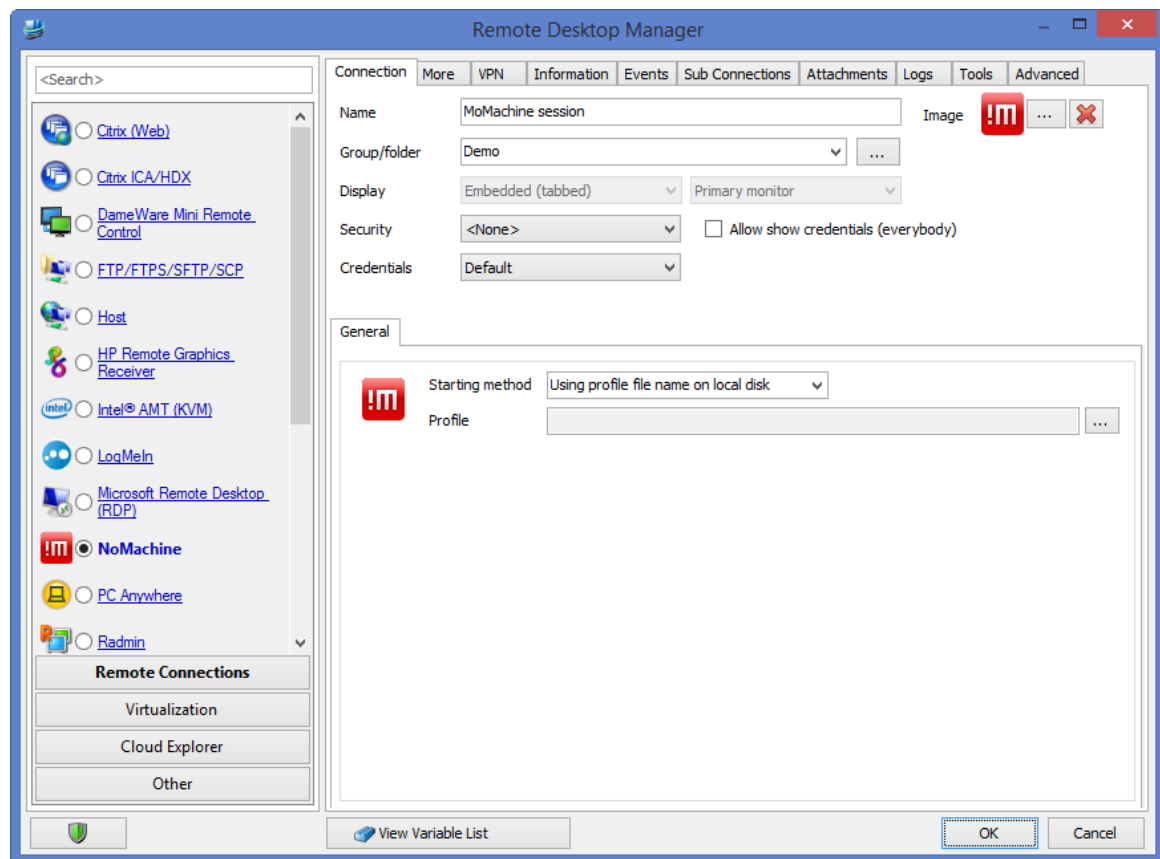


This entry is used to define and configure a 'NoMachine' session. This allows you to store in Remote Desktop Manager each NoMachine profile as a distinct session, so that you can connect automatically to different computers (exactly like RDP session).



The NoMachine entry type is available when the NoMachine [Add-on](#) is installed.

Settings



NoMachine entry

Option	Description
Starting method	<p>Using profile file name on local disk: The session will be linked to an existing profile (file) on a computer and it will be dependent on it.</p> <p>Using stored profile in session: 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.</p>
Profile	Select the NoMachine profile to use for the connection.

5.1.2.1.10 PC Anywhere

Description




Allow for a PC Anywhere connection via a .chf file.

- External mode
- Show opened session

Settings

General

 PC Anywhere config file name (*.chf)

Host override

PC Anywhere configuration

5.1.2.1.11 Radmin

Description




This entry is used to define and configure a 'Radmin' session.



Since the Radmin command line does not support the password parameter, the application is unable to do an auto login. The only known workaround available is by using the [auto typing macro](#) feature.

Settings

General

 ☒ Configuration

Host
 ... <address>:<port>

Color ☐ Full screen

Mode

Through

☐ Config file name

...

5.1.2.1.12 Remote Assistance


Description



This entry is used to define and configure a 'Remote Assistance' session.

Settings

General

 Connection mode

☒ Expert (Opening an invitation)

☐ Novice (ask for assistance)

☐ Offer assistance

Computer or IP address

5.1.2.1.13 ScreenConnect

Description




This entry is used to define and configure a 'ScreenConnect' session.

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

Settings

General



Host
User name
Password
☐ Always ask for password
Session name
☐ Always ask for session name.

Auto create session
☐ Create session if doesn't exists.
Session type

Connection type

5.1.2.1.14 TeamViewer


Description

This entry is used to define and configure a 'TeamViewer' session.



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

Settings

General

 ID

Password



☐ Prompt for password

☒ Remote support
☐ Presentation
☐ File transfer
☐ VPN
☐ Choose on connection

Wait time ms

5.1.2.1.15 Telnet, SSH, RAW, rLogin

Description

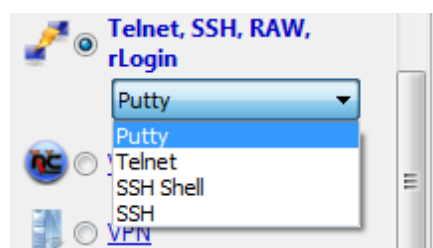


This entry is used to define and configure a 'Telnet, SSH, RAW, rLogin' session.

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

Settings

It's possible to use this connection with Putty or directly built-in:



Sub-types

See also

- [Built-in Telnet](#)
- [Built-in SSH](#)
- [Built-in SSH Shell](#)

5.1.2.1.15.1 Putty

Description

The Putty integration allows to re-use an existing session saved locally or a custom configuration. It also support the tabbed environment.

Settings

General

The screenshot shows the 'General' tab of the Putty settings dialog. It features three tabs: 'General', 'After Login Commands', and 'Advanced'. The 'General' tab is active. It contains a 'Session' dropdown menu with a search icon and a 'Host and credentials are optional' note. Below this are fields for 'Host', 'User name', and 'Password'. A radio button labeled 'Use these settings' is selected. Under this, there are fields for 'Protocol' (set to 'Default'), 'Port' (set to '22'), 'Host' (set to '\$COMPUTER_IP\$'), 'User name', and 'Password'. A 'Port forwarding' section includes a large text area and '+' and '-' buttons. A 'Verbose' checkbox is also present. At the bottom, there is a 'Show debug information (embedded)' checkbox.

General Tab

You can either choose an existing session definition from Putty or specify the settings here.

After Login Commands

After Login Commands Tab

Much like keyboard macros, these commands are simply sent to the remote host after the configurable delay. If the first 5 commands are not sufficient, simply use the More Commands text area and enter as many commands as needed and separate each one by a carriage return.

Advanced

Advanced Tab

Option	Description
Application	Allows you to choose a different command line client. Choose between Putty, PLink, Default or Kitty. Default simply indicates to use whatever was defined in File -> Options -> Session Type for the Telnet/SSH/rLogin/Raw option.
Internet protocol	You can choose to use either IPv4 or IPv6
Other parameters	any parameter listed here will simply be appended to the command line used to launch the program.

5.1.2.1.15.2 Built-in Telnet

Description

Telnet

5.1.2.1.15.3 Built-in SSH

Description



Only SSH v2 is supported. SSH v1 has inherent design flaws which make it vulnerable and it has been generally considered obsolete

The screenshot shows a configuration window for SSH with two tabs: 'General' and 'Private Key'. The 'General' tab is active. It contains two main sections: 'Outgoing tunnel settings' and 'Proxy settings'. In the 'Outgoing tunnel settings' section, there is an 'SSH' icon, a 'Host' field, a 'Port' dropdown set to '22', a 'User name' field, a 'Password' field with an eye icon, an 'Always ask for password' checkbox, a 'Local IP' dropdown set to '127.0.0.1', a 'Port' dropdown set to '3390', and a 'Remote port' dropdown set to '3389'. The 'Proxy settings' section has a 'Use proxy' checkbox, a 'Proxy' field, a 'Port' dropdown set to '3128', a 'Proxy type' dropdown set to 'Socks4', a 'User name' field, and a 'Password' field. A note on the right says 'Leave login/password fields empty when not needed.'

SSH

Settings

General

TBD

Private Key

Please consult [SSH Private Keys](#)

5.1.2.1.15.4 Built-in SSH Shell

Description



Only SSH v2 is supported. SSH v1 has inherent design flaws which make it vulnerable and it has been generally considered obsolete

General Terminal Keyboard Private Key

SSH settings

Host Port

User name

Password

☐ Always ask for password

Proxy settings

☐ Use proxy

Proxy Port

Proxy type

User name

Password

Leave login/password fields empty when not needed.

SSH Shell

Settings

General

TBD

Terminal

TBD

Keyboard

TBD

Private Key

Please consult [SSH Private Keys](#)

5.1.2.1.15.5 SSH Private Keys

Description

The private key settings apply to [Built-in SSH](#) and [Built-in SSH Shell](#). They allow you to provide a key file instead of a password for SSH connections.

The screenshot shows a settings window with five tabs: General, Terminal, Keyboard, Private Key (selected), and Recording. The Private Key tab contains two main sections. The first section, 'Private key file', has a radio button selected and a text field for 'Filename' containing the path '%USERPROFILE%\mykey.ppk'. The second section, 'Private key data', has an unselected radio button and a large text area for entering key data. Above the text area are three buttons: 'Clear', 'Paste', and an ellipsis button.

Private Key tab

Settings

Settings	Description
No private key	No private key will be sent
Private key file	Allows you to select a key file to submit as credentials
Filename	Name of the file containing the key. You can use environment variables as in the screen capture above.
Private key data	Allows you to specify the textual data of the key. This results in the key being stored within the entry itself and eases distribution.

Private key data controls

Settings	Description
Clear	Will clear the content of the field.
Paste	Allows you to paste the content of the clipboard in the text area.
Ellipsis button	Allows you to select a file which will be read in the text area.

5.1.2.1.16 VNC

Description



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

- Auto Login
- Built in
- Copy Password
- Credential Repository
- Embedded Mode
- External Mode
- Full Screen
- Support Host
- Multi Monitor Support
- Show Opened Session
- Support AfterDisconnectEvent
- Support Logging

Settings

General Settings Advanced

VNC application
RealVNC

Host
Full screen

Command line arguments

Custom configuration
Config file name

5.1.2.1.16.1 Applications

Description

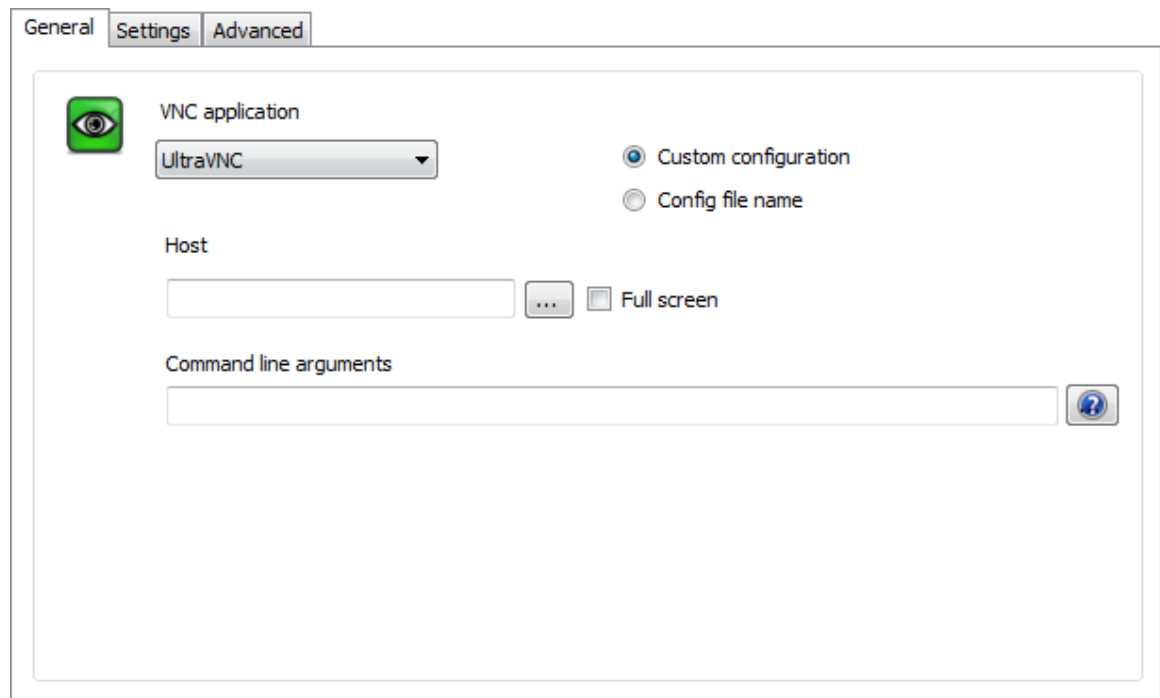
Supported applications in external mode are:

- RealVNC
- TightVNC
- UltraVNC



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

Settings



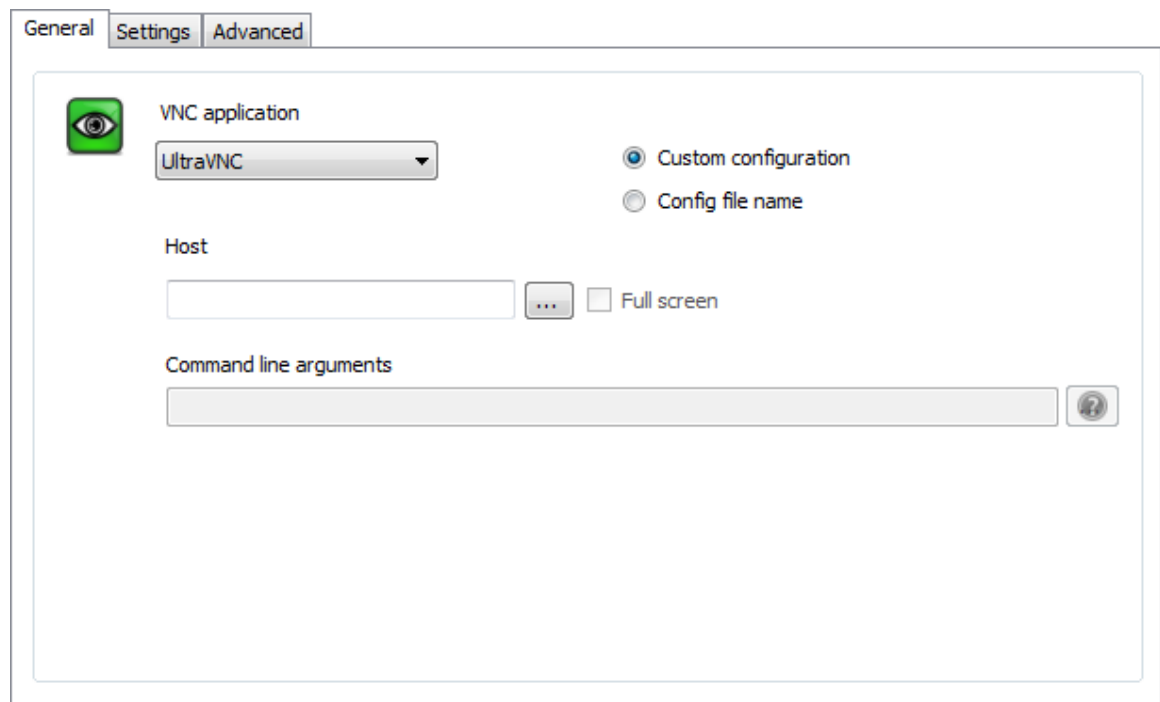
The screenshot shows a settings window with three tabs: "General", "Settings", and "Advanced". The "Settings" tab is selected. Inside the settings area, there is a green eye icon next to the "VNC application" label. Below this is a dropdown menu currently set to "UltraVNC". To the right of the dropdown are two radio buttons: "Custom configuration" (which is selected) and "Config file name". Below these is a "Host" label followed by a text input field and a button with three dots. To the right of the input field is a checkbox labeled "Full screen". At the bottom, there is a "Command line arguments" label followed by a long text input field and a help icon (a blue circle with a question mark).

5.1.2.1.16.2 Embedded UltraVNC

Description

Embedded UltraVNC is the recommended mode for the maximum of compatibility. It also support chat and file transfer while connected.

Settings



Settings

Host

The host support 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`

5.1.2.1.17 VPN

Description

Consult this [topic](#) for more information about the VPN management.

5.1.2.1.18 Web Browser (HTTP/HTTPS)

Description



This entry is used to define and configure a 'Web Browser (http/https)' session. It allows you to open a browser, either external or embedded, to a site of your choice. More importantly, it can perform automatic login of most web sites.

Supported features

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

Settings

The screenshot shows the 'Connection' settings window for 'Devolutions Forums'. The 'Connection' tab is active, and the 'General' sub-tab is selected. The 'Name' field is 'Devolutions Forums'. The 'Group/folder' is empty. The 'Display' is set to 'External' and the 'Primary monitor' is selected. The 'Security' is set to 'Default'. The 'Credentials' are set to 'Default'. The 'Allow copy credentials to clipboard' checkbox is unchecked. The 'Web browser url' is 'http://forum.devolutions.net'. The 'Web browser application' is 'Internet Explorer'. The 'Enable web browser extension link' checkbox is checked. The 'Open new browser session (no merge)' checkbox is unchecked. There is a 'Template' button at the bottom.

General tab

The Display setting affects the content of the tabs below because it changes the manner in which the browser is launched. Its two possible values are External or Embedded.

1. External: Launches the browser as you would do normally, meaning the browser application is launched.
2. Embedded: The browser window is embedded in Remote Desktop Manager. Content is displayed in a tab like an embedded session would be. Only two browsers can be embedded in this manner, namely Internet Explorer and Firefox.

Common Settings

Setting	Description
Web browser URL	Url for the site to open
Assign Favicon to session	Helper utility to extract the favicon from the web site and assign it to the session. This helps you recognizing the proper entry in a large list.

Enable web browser extension link

This is used in conjunction with the web browser extensions. Please consult [Auto Fill](#)

External Settings

General Tab - External Display

Setting	Description
Web browser application	Allows you to choose you preferred application. The Default setting means that the default browser of the machine is used.
Open new browser session (no merge)	IE ONLY, this will launch a new application even if one is already running.

Embedded settings

General Tab - Embedded Display

Setting	Description
Web browser application	Allows you to choose between Internet Explorer or Firefox. Certain features are available only for Internet Explorer.

Tabs visible	You can choose to display tabs within the embedded browser. Valid sessions are Automatic, never and always.
Show Favicon	When running, the icon for the web page is fetched and put on the tab.
Hide script errors	Script errors will not be displayed if you check this.



Running an embedded Firefox requires a third party that is available freely from our site. Upon first usage you will be presented with a dialog requesting the installation path of the third party. Please consult [Embedded Firefox](#) for more information.

5.1.2.1.18.1 Auto Login



Form Authentication

General Login

Authentication mode: Form

User name:

Domain:

Password:  

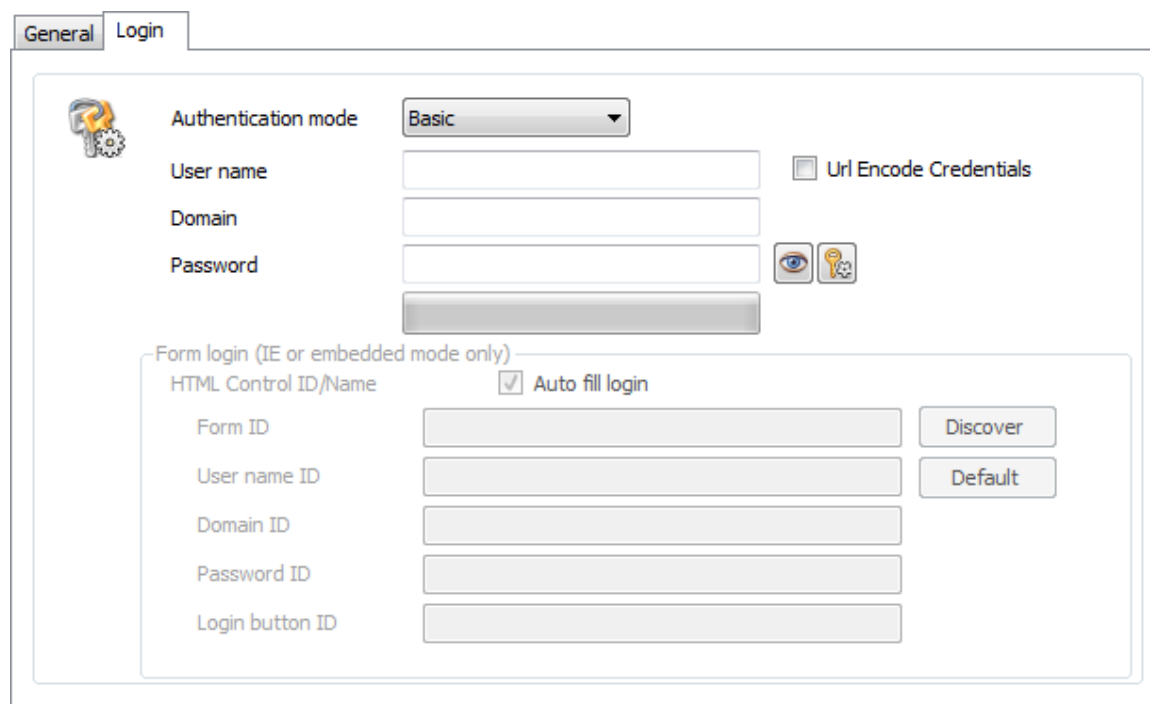
Form login (IE or embedded mode only)

☒ Auto fill login

HTML Control ID/Name		
Form ID	<input type="text"/>	Discover
User name ID	<input type="text"/>	Default
Domain ID	<input type="text"/>	
Password ID	<input type="text"/>	
Login button ID	<input type="text"/>	

Login tab - Form authentication mode

Basic Authentication



The screenshot shows the 'Login' tab of the Remote Desktop Manager interface. It features a 'General' tab and a 'Login' tab. The 'Login' tab is active, displaying a settings panel with a gear icon. The 'Authentication mode' is set to 'Basic'. Below this, there are input fields for 'User name', 'Domain', and 'Password'. To the right of the 'User name' field is a checkbox labeled 'Url Encode Credentials'. To the right of the 'Password' field are icons for an eye (toggle visibility) and a key (toggle password saving). Below these fields is a large grey button. A section titled 'Form login (IE or embedded mode only)' contains a checkbox for 'Auto fill login' which is checked. Below this are five input fields labeled 'Form ID', 'User name ID', 'Domain ID', 'Password ID', and 'Login button ID'. To the right of these fields are two buttons: 'Discover' and 'Default'.

Login tab - Basic authentication mode

5.1.2.1.19 X Window


Description



This entry is used to define and configure a 'X Window' session.

Settings

General


 XLaunch (Xming) file name

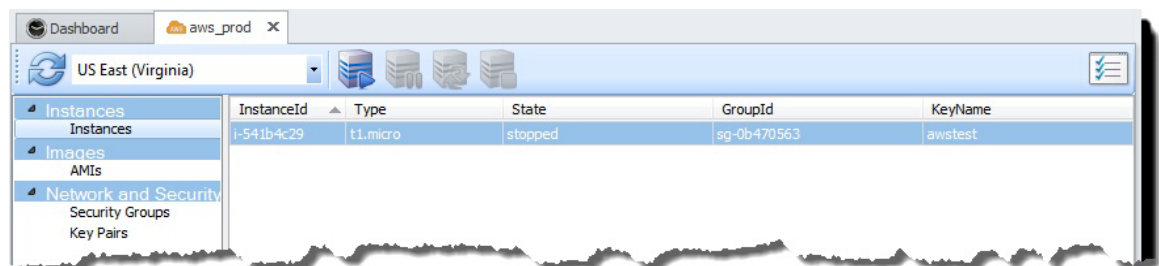
5.1.2.2 Virtualization

5.1.2.2.1 Amazon Web Services (AWS) Console

Description



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



AWS EC2 console



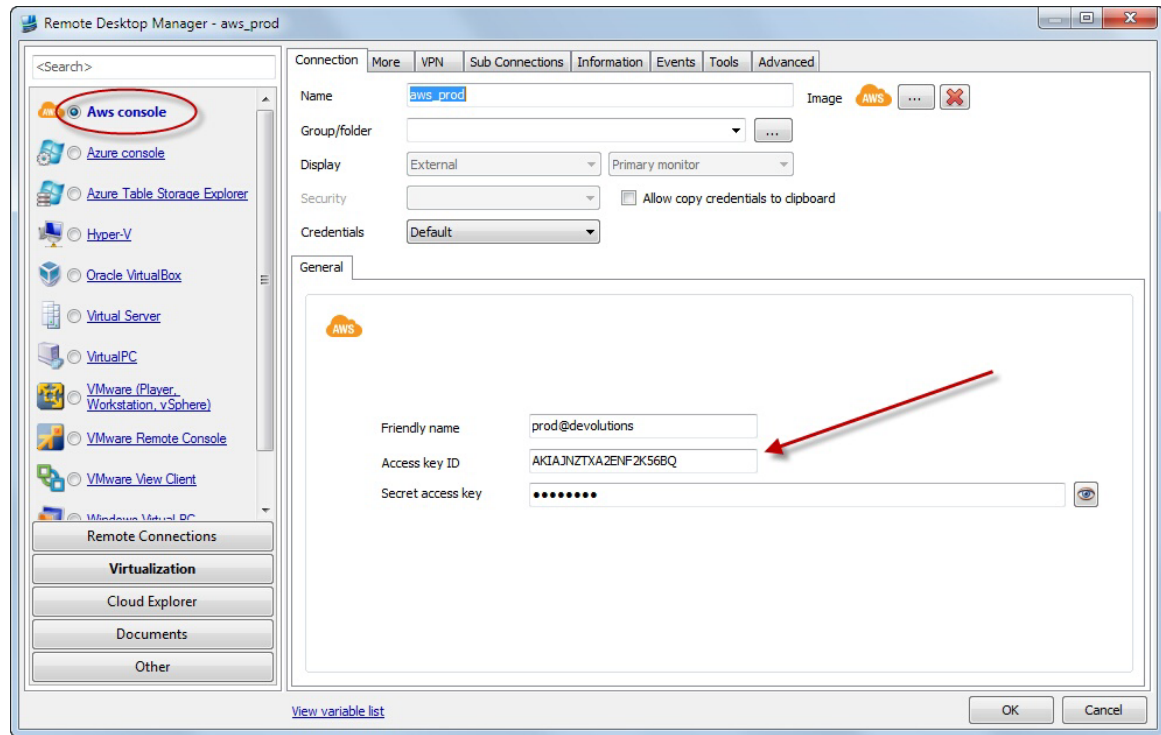
Although multiple services will be supported in the long run, currently only Amazon EC2 is implemented.

Prerequisites

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

Settings

Enter a friendly name for the account and its access keys.



AWS console - general settings

Workflow

EC2

The EC2 tab displays information about your instances, images, security groups and key pairs. The currently supported operations are against instances only.

- Start: start a stopped instance
- Stop: stop a running instance.
- Reboot: reboots a running instance
- Terminate: terminate a running instance.



Performing a *Stop* followed by a *Start* will cause two hours of billing being charged to your account. One for the fraction you consumed before the *Stop*, and one for the part after the *Start*. A reboot on the other hand is seamless in that for the AWS infrastructure, the same machine was kept running. This is why we currently do not display a *Rebooting* state.

5.1.2.2.2 Citrix XenServer

Description



This entry is used to define and configure a 'XenServer' session.

- Auto Login
- Built in
- Copy Password
- Credential Repository
- External Mode
- Show Opened Session

Name	Description	Uptime
Another win2008	windows 2008 R2 64 bits	2012-09-25 10:37 PM
NetScaler Virtual Appliance	NetScaler Virtual Appliance	2012-10-04 9:10 PM
Win2012	File server	2012-10-04 9:10 PM
Windows 2008 R2 64 p2 zenapp	DNS, BDC	2012-10-10 7:05 AM
Windows 2008 template	XenApp is for sharing APPS!	2012-09-26 5:34 PM

XenServer Console

Settings

Fill in the connection details

General

Host

192.168.1.231 ... Port 80

Simply type in the name / IP address of the host, and the desired port.

Workflow

The currently supported actions operate on existing Virtual Machines. They correspond exactly to the action available thru Citrix® XenCenter.

Troubleshooting

Before attempting connection from RDM, ensure connectivity is achieved using Citrix® XenCenter.

5.1.2.2.3 Microsoft Azure Console

Description

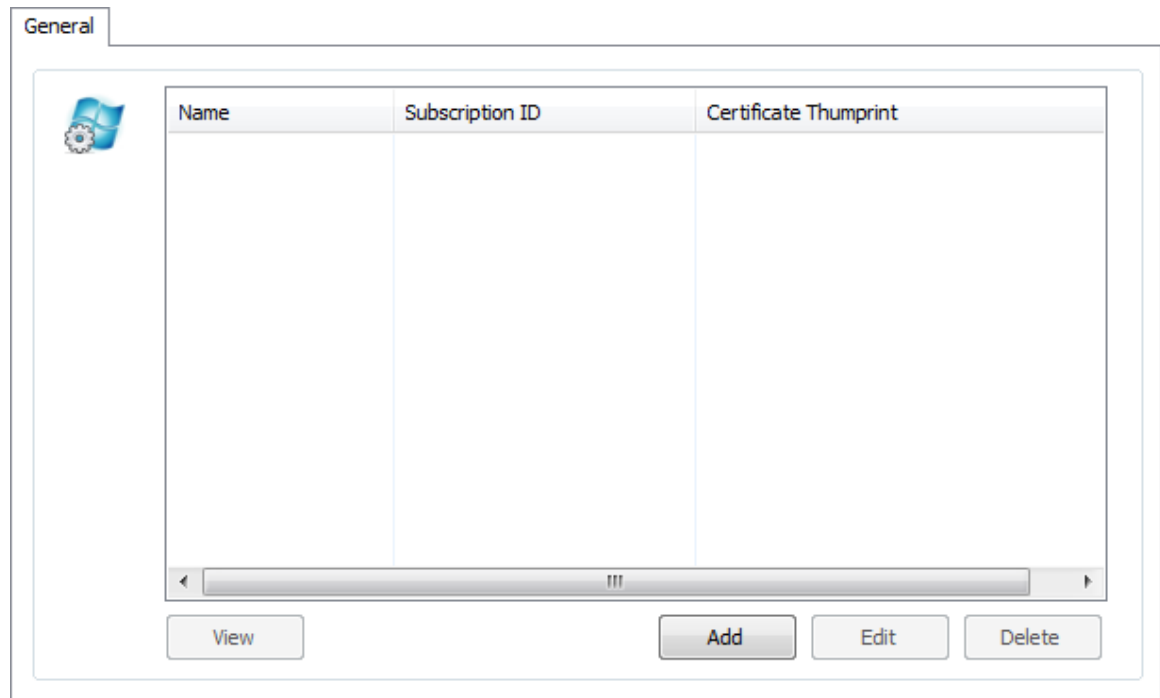


This allows for the management of Azure subscriptions within the Remote Desktop Manager application. Replicating most of the functionality available in the Silverlight application available from Microsoft ([here](#)).

Please note that at the moment only Cloud Services are supported.

This session uses the Windows Azure Service Management REST API to communicate with the Azure instances. Setup via the Microsoft Silverlight application is required prior to using the API. More information on the Management API is available [here](#).

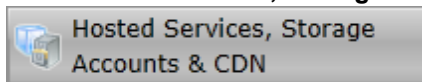
Settings



Setup - Upload Certificate to Azure Subscription

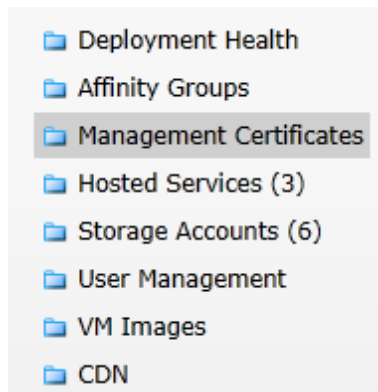
First we must configure the Azure subscription to allow the use of the Azure Service Management REST API.

1. Logon <https://windows.azure.com> using your Live account
2. Select **Hosted Services, Storage Accounts & CDN**



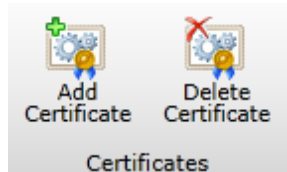
Hosted services, storage accounts & CDN

3. Select **Manage Certificates**



Manage certificates

4. Add a certificate for all subscriptions you want to manage. Any certificate will do. You can create one, if need be, with IIS or using the MakeCert tool.



Add certificate

5. Please note the thumbprint of the certificate(s) uploaded, they will be required when registering the subscription.

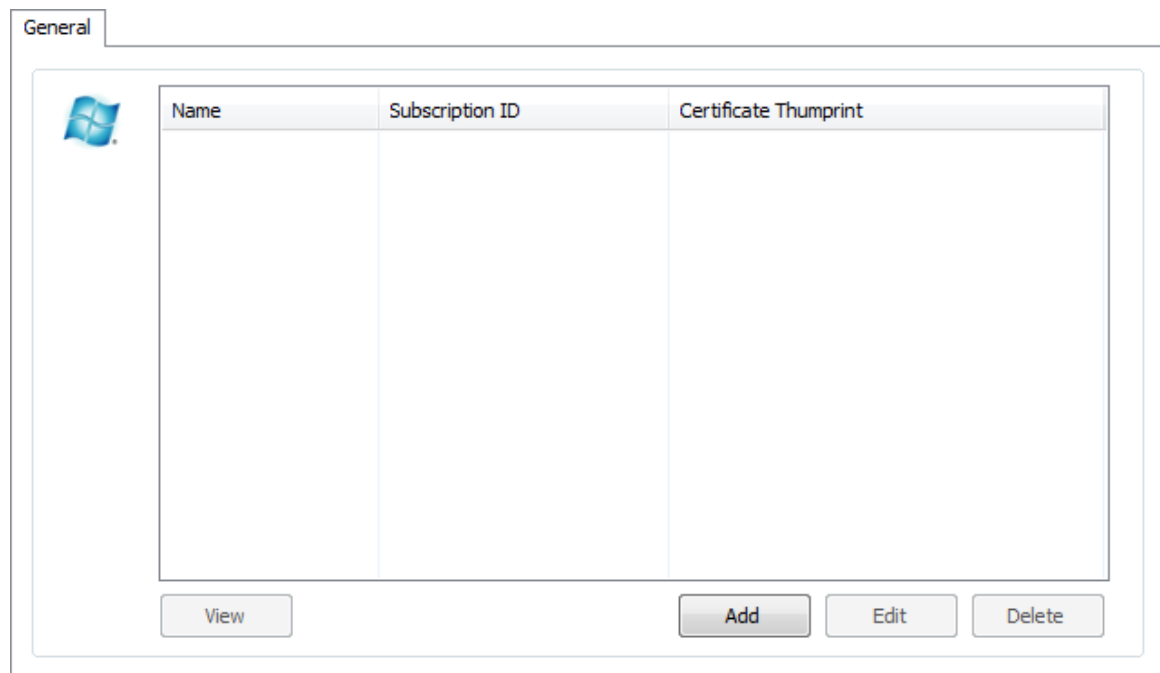
Specifications

Features	Availability
External mode	
Embedded mode	X
Show opened session	Embedded only
Batch edit	
User settings can be overridden	
Auto login	
Full screen	
Multi-monitor support	

Configuring Azure Subscription

Multiple Azure subscriptions can be managed within the same Azure Session. Simply add all subscription you wish to manage.

General



Name	Subscription ID	Certificate Thumbprint
------	-----------------	------------------------

View Add Edit Delete

Data entry Account settings

Remote Desktop Manager

Azure Subscription
Manage Azure Subscription

Name

Subscription ID

Certificate thumbprint

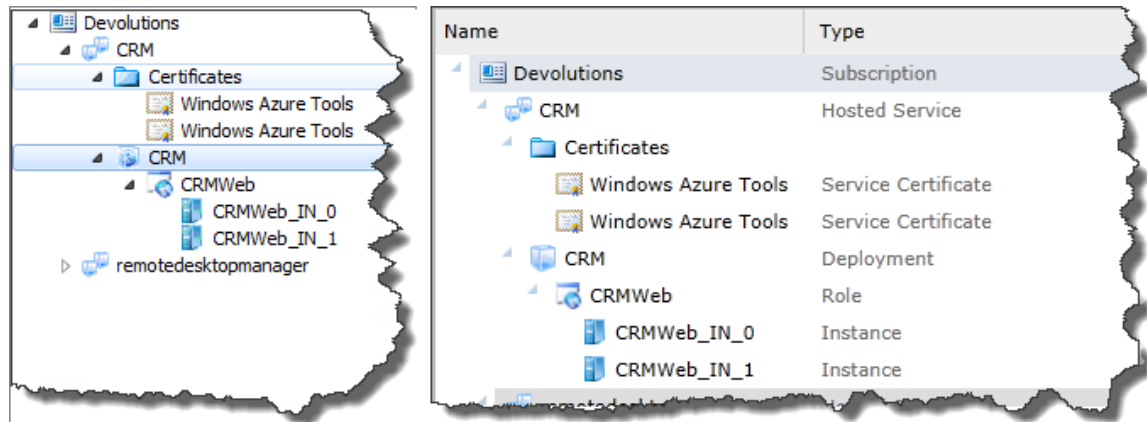
Test

OK Cancel

Add Subscription

[Role]

[Role Instance]



Left (Azure session) - Right (Azure console)

	Account administrator
	<input type="text" value="dherve@20101@hotmail.com"/>
Created	<input type="text" value="n/a"/>
Name	<input type="text" value="Devolutions"/>
Quota	<input type="text" value="Cores: 6/20
Hosted Services: 2/6
Storage: 5/5"/>
Service administrator	<input type="text" value="dherve@20101@hotmail.com"/>
Subscription ID	<input type="text" value="1-111-11111-11111-11111-11111-11111"/>
Type	<input type="text" value="Subscription"/>
Status	<input type="text" value="Active"/>

Subscription detail



DNS Name
[http://\[redacted\].cloudapp.net/](http://[redacted].cloudapp.net/)

Cores used
1 (\$28.80/month approx.)

Name
[redacted]

Environment
Production

VIP
[redacted]

Status
Running

Type
Deployment

Input endpoints
[redacted] : [redacted] :80
[redacted] : [redacted] :3389

Os Version
WA-GUEST-OS-1.18_201202-01

Deployment detail

Count
2

Cores used
1 (\$28.80/month approx.)

Name
CRMWeb

Environment
Production

Os Version
WA-GUEST-OS-1.18_201202-01

Status
Running

Type
Role

Role detail

	Size
	ExtraSmall
	Cores used
	1 (\$28.80/month approx.)
	Name
	CRMWeb_IN_0
	Environment
	Production
	Os Version
	WA-GUEST-OS-1.18_201202-01
	Status
	Running
	Type
	Instance
	Update domain
	0
	Start time
	n/a

Role instance detail

Notes

All referenced certificates must be installed on the machine where you want to open the Azure session. Not having the certificate installed will cause the Azure session to fail while establishing the connection.



The certificate must be installed in Personal (Current User) not Computer.



If a user has access to Azure Management REST API certificate then that user could use the certificate to control, via Azure PowerShell management cmdlets or code, all (almost) aspects of the subscription.

5.1.2.2.4 Microsoft Azure Table Storage Explorer


Description



This entry is used to define and configure a 'Azure Table Storage Explorer' session.

Settings

General



Account name

Account shared key

☒ Use SSL

☐ Use development storage

Test connection

5.1.2.2.5 Microsoft Hyper-V


Description



This entry is used to define and configure a 'Hyper-V' session. This connection type uses vmconnect.exe. We recommend to use the [Hyper-V RDP](#) for a built-in and embedded view support.

Settings

General

 Host

... Instance count

☒ By name

Virtual machine name

☐ By ID (guid)

Virtual machine ID

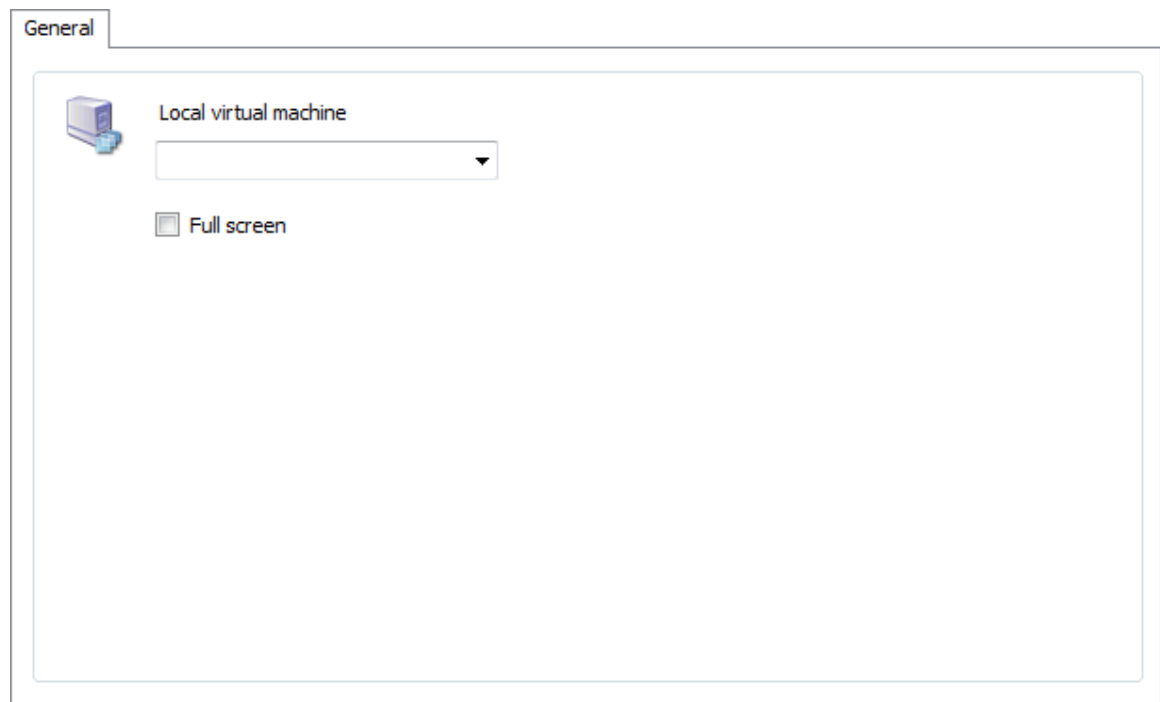
5.1.2.2.6 Microsoft Virtual PC

Description



This entry is used to define and configure a 'VirtualPC' session.

Settings



5.1.2.2.7 Microsoft Virtual Server

Description






This entry is used to define and configure a 'Virtual Server' session.

- Embedded Mode
- External Mode
- Support Host
- Show Opened Session
- Support Logging
- User Settings Can Be Overridden



Settings

General

 Url  Port  Set the port to 0 to use the default port

User name

Domain

Password  

☐ Reduced color mode

☐ Administrator mode

☐ View only mode

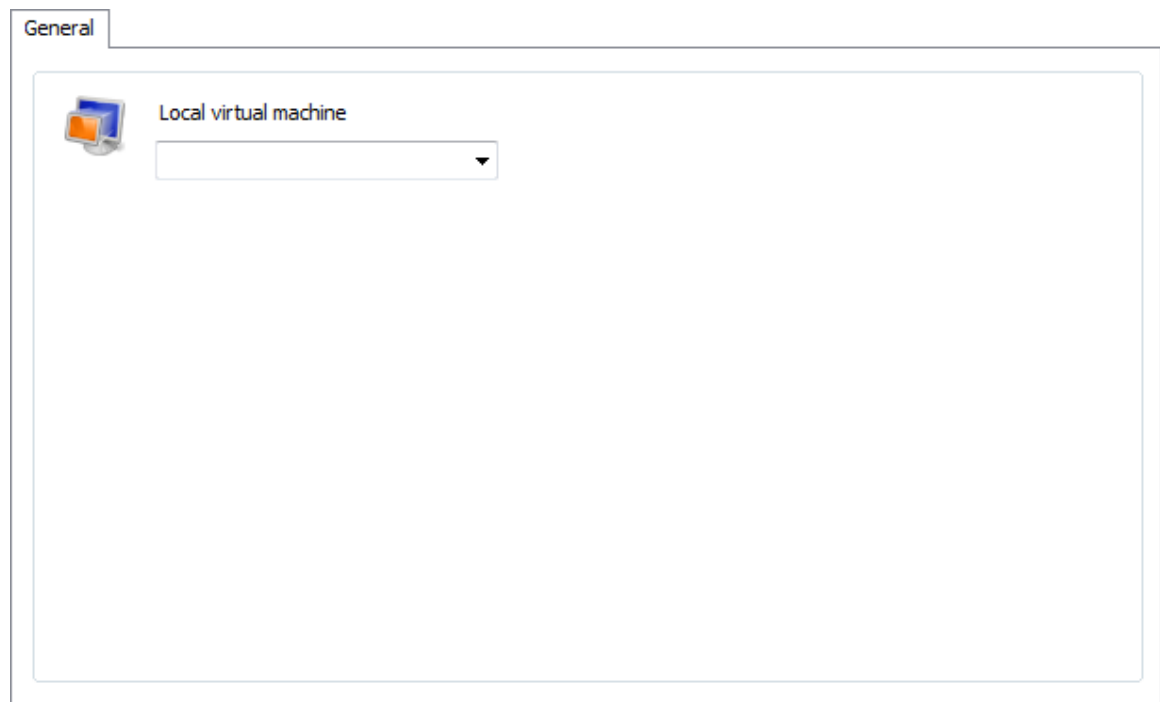
5.1.2.2.8 Microsoft Windows Virtual PC

Description



This entry is used to define and configure a 'Windows Virtual PC' session.

Settings



5.1.2.2.9 Oracle VirtualBox


Description



This entry is used to define and configure a 'Oracle VirtualBox' session.

Settings

General

 Virtual machine

5.1.2.2.10 VMware (Player, Workstation, vSphere)

Description




This entry is used to define and configure a 'VMware (Player, Workstation, vSphere)' session.

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

VMware Player

General

 Application VMware Player

Virtual machine file name
 ...

☐ Full screen

Server ... ☐ Use Windows credentials


User name

Password 👁️ 🔑

Other parameters

VMware Workstation

General

 Application VMware Workstation

Virtual machine file name
 ...

☐ Full screen

Server ... ☐ Use Windows credentials


User name

Password 👁️ 🔑

Other parameters

VMware Infrastructure and vSphere

General



 Application VMware Infrastructure Client / vSphere Client

Virtual machine file name

☐ Full screen

Server ... ☐ Use Windows credentials

User name

Password  

Other parameters

5.1.2.2.11 VMWare Console

Description

The VMWare Console allows basic administrative tasks of a VMWare host.

Dashboard Virtual machines - VMWare x


Power on Power off Suspend Shut down guest Restart guest Connect New Host VMWare Auto refresh

Name	State	Host CPU - MHz	Host Mem - MB	Guest Mem - %	Note
Windjammer SQL	Powered On	35	796	11	
Windjammer RDMS	Powered On	13	796	2	
Windjammer DC	Powered On	45	2080	13	
Ubuntu	Powered On	5	1044	0	



VMWare Console

Settings

General

 Host ...

User name

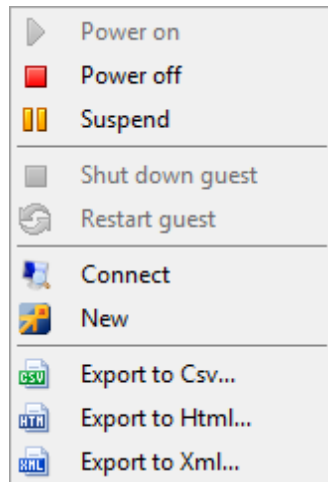
Password  

General tab of the VMWare Console entry

Simply enter the host name or IP, the user name and the password of a user with administrative rights on the host.

Workflow

Using the toolbar at the top, or the contextual menu of the grid you can perform operations on Guests:



Contextual menu

Operations depend on the configuration of the host, please refer the VMWare's documentation on the meaning of each command.

On the toolbar, there is a Refresh button that will query the Host to display it's current state. You can also enable an Automatic refresh that will perform it periodically.

5.1.2.2.12 VMware Remote Console


Description

This entry is used to define and configure a 'VMware Remote Console' session.

- Auto Login
- Copy Password
- Credential Repository
- External Mode
- Multi Monitor Support
- Show Opened Session

Settings

General





Virtual Center/ESX(i) Server

Server IP/DNS

☐ Passthrough Authentication

User name

Password  

VM Name/Configuration

.vmx filename

or

VM Id

☐ Full screen

5.1.2.3 Cloud Explorer

5.1.2.3.1 Amazon S3

Description




This entry is used to define and configure a 'Amazon S3' session.

- Auto Login
- Built in
- Copy Password
- Credential Repository
- Embedded Mode
- Show Opened Session


Settings

General Local

 ☒ Show all buckets
☐ Show a specific bucket

Bucket

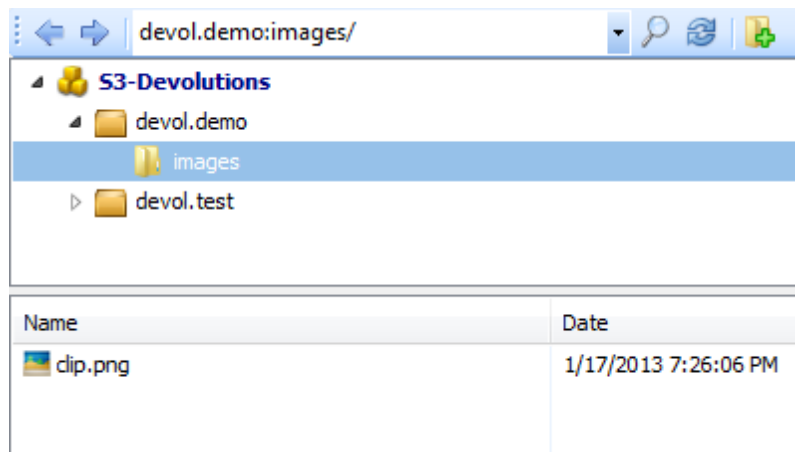
Access key ID

Secret access key 

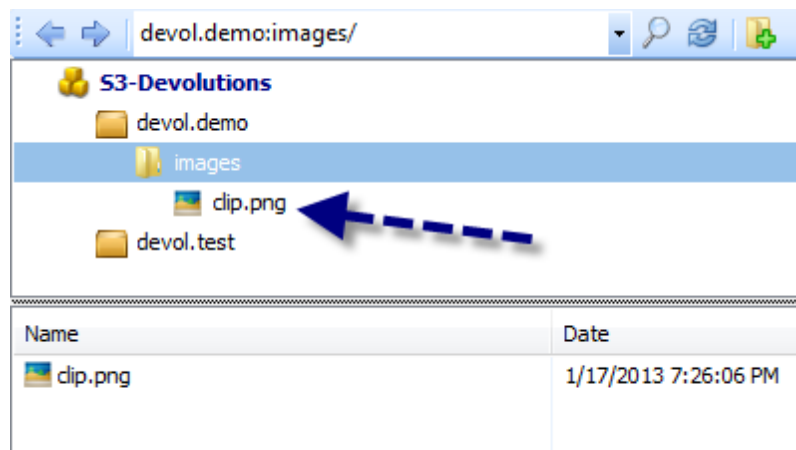
☒ Show files in tree view
☐ Large icons for root

Choose between showing all buckets or a specific one. Enter the Bucket name carefully as it is case sensitive. Also enter the Access key ID and the Secret access key.

The **Show files in tree view** setting will include the files in the top-most tree view.

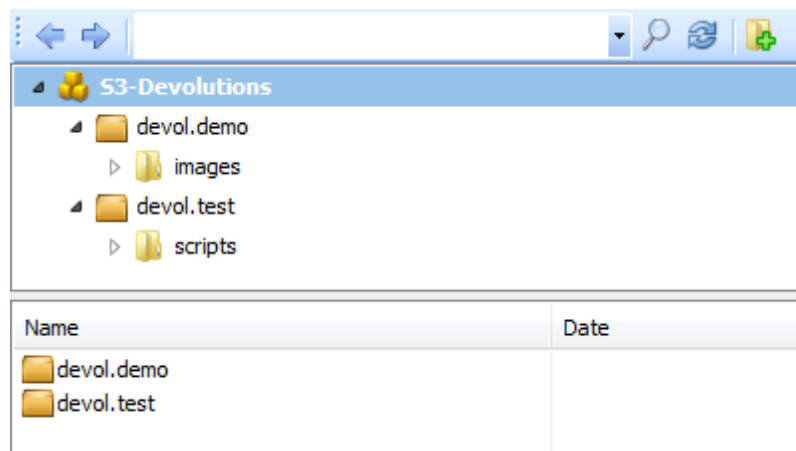


Show Files - OFF

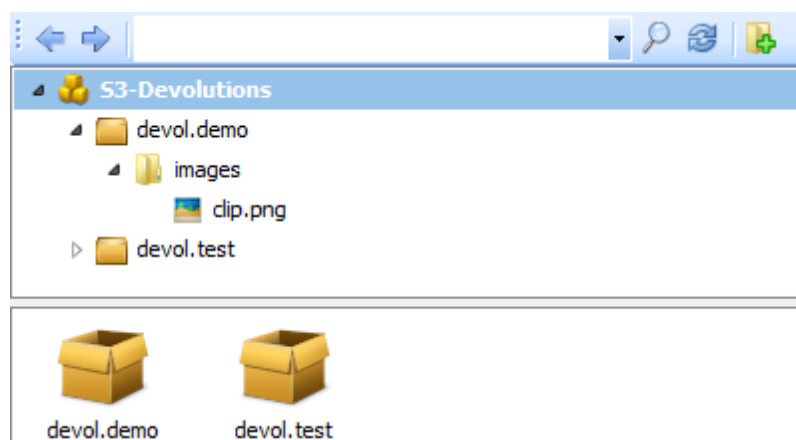


Show Files - ON

The **Large icons for root** setting will change the appearance of the S3 buckets in the detail view.



Large icons - OFF



Large icons - ON

5.1.2.3.2 Dropbox

Description



This entry is used to define and configure a 'Dropbox' session.

- Auto Login
- Built in
- Copy Password
- Credential Repository
- Embedded Mode
- Show Opened Session

Settings

General

Default directory

Email

☐ Show files in tree view

Account status The account is not validated yet.

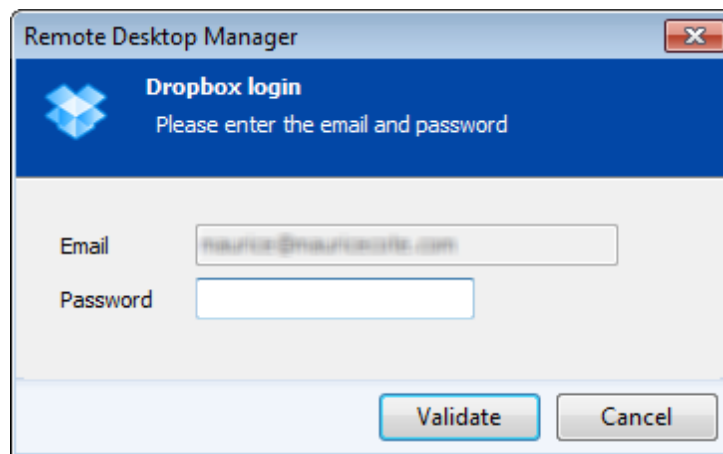
Validate with Dropbox

Settings Tab for Dropbox

Setting	Description
Default directory	Optional - the directory to display by default.
Email	Email address for the Dropbox account.
Show files in tree view	This will display the files in the left-hand tree view instead of just in the right-hand list.

Workflow

After at least you email is entered, press **Validate with Dropbox**. The following dialog will appear.



Dropbox login

Enter your password and press Validate.

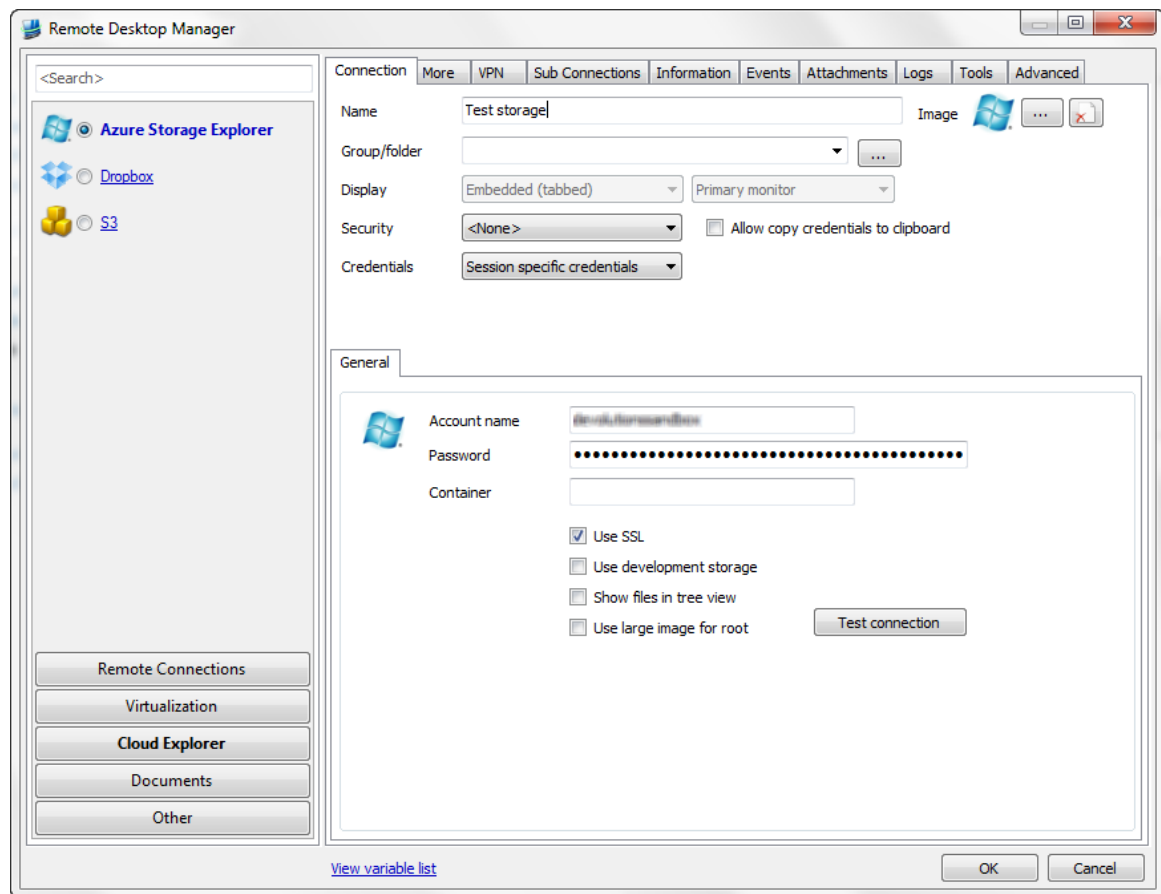
5.1.2.3.3 Microsoft Azure Storage Explorer

Settings



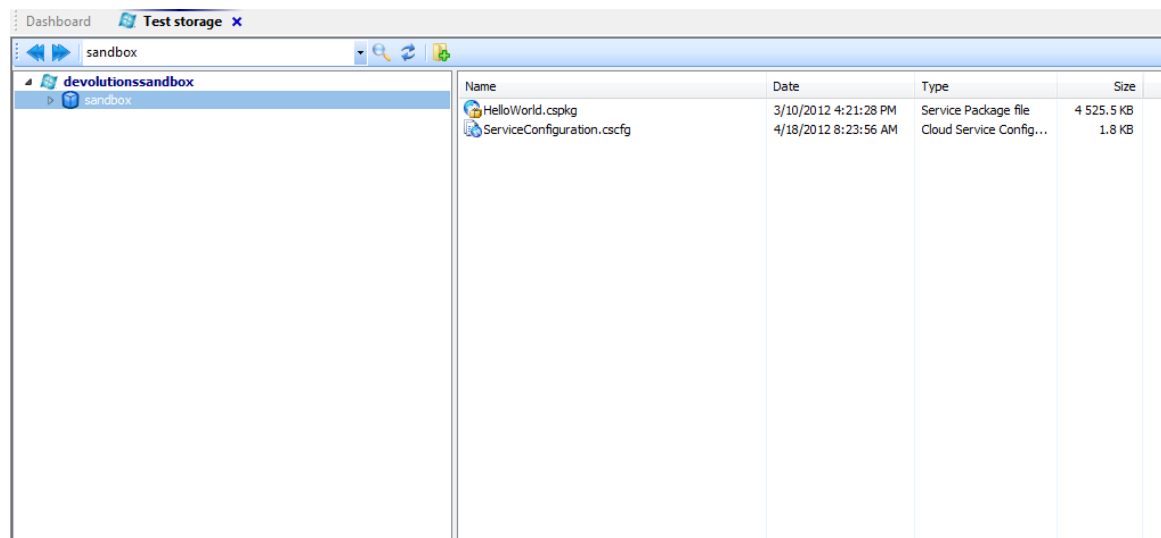
This entry is used to define and configure a 'Azure Storage Explorer' session.

Settings



Azure Storage Explorer

Explorer



Azure dashboard

5.1.2.4 Others

5.1.2.4.1 Command Line

Description



This entry is used to define and configure a 'Command Line' session. The host and credentials can be used as parameters by using the related variables.

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

Settings

General Host and Credentials

Run

[Assign file icon to session](#)

☒ Use Default Working directory

☐ Wait for application to exit (Remote Desktop Manager will be unavailable)

☐ Run as Administrator ☐ Run in 64 Bits mode ☒ Use Shell Execute

Process name [Set default process name](#)

TIP: Use default process name if you want your application to be listed in the opened sessions

5.1.2.4.2 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's useful to quickly integrate data into the application.

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

Workflow

Configure your connection string and the SQL query. You need to know how to write a SQL statement and this is database dependent.

Settings

General

The screenshot shows the 'General' tab of a settings dialog. It includes a tab bar at the top with 'General', 'Parameters', and 'Query'. Below the tab bar, there is a grid of settings. The 'Source' is set to 'Default'. 'Data source' is 'Microsoft SQL Server'. 'Data provider' is '.NET Framework Data Provider for SQL Server'. 'Connection string' is masked with dots and has an eye icon and a dropdown arrow. 'Host', 'User name', and 'Password' are also masked with dots and have eye icons.

General tab

Option	Description
Source	<ul style="list-style-type: none"> • Default: The connection string is defined directly within the session. • Credential Entry: Use a linked Connection String credential entry as the connection string. • Inherited: Navigate down the inheritance graph of the object to find the connection string. • Prompt: At open connection time, the system will prompt the user to select the desired Connection String from credential entry list.
Data source	Contains the data source type like ODBC, OLEDB or native. This value is read only and it's extracted from the connection string.
Data provider	Specify the provider used for the database access. This value is read only and it's extracted from the connection string.
Connection string	This value contains the database connection string and it can be hidden/encrypted for a better security.
Host	Contains the connection server name. This value is read only and it's extracted from the connection string.
User name	Contains the username used to access the database. This value is read only and it's extracted from the connection string. It is blank if you use Windows Authentication.

Password	Contains the username used to access the database. This value is read only and it's extracted from the connection string. It is blank if you use Windows Authentication.
----------	--



When the source is set to Prompt you will see a dialog box prior when you open the connection.
Only the [Connection String](#) credential entries from your data source are listed. Select the entry to use and the report will execute.

Parameters

General Parameters Query

Custom parameters

Parameter description	Type	Default value
Parameter #1	@Param1 Integer	10
Parameter #2	@Param2 Unused	
Parameter #3	@Param3 Unused	
Parameter #4	@Param4 Unused	
Parameter #5	@Param5 Unused	

Example of Query fields:

Exec Query

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

Parameters tab

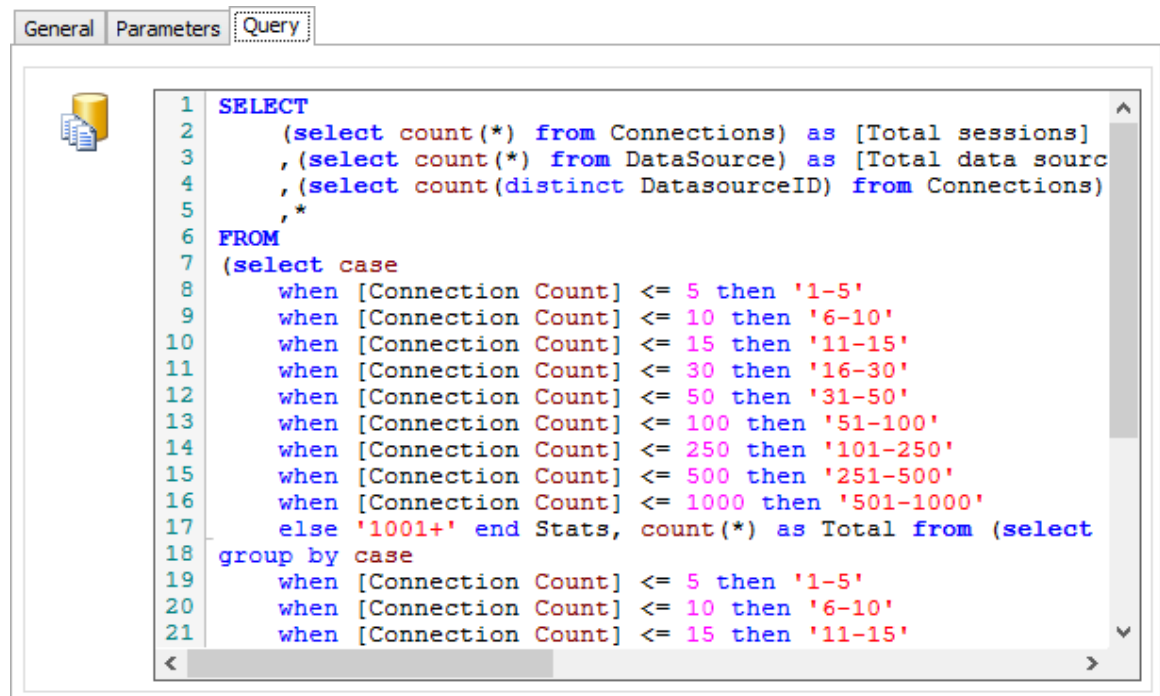
Using parameters is simple. Write your query with parameter place holders (@Param1 or ? depending of the data provider you use). On the **Parameters** tab define the parameter type and default value. On open of the session, you will be prompted you for the parameter values.



Parameter placeholders syntax depends on the data provider.

Parameter	Description
.NET Framework Data Provider for SQL Server	Uses named parameters in the format @parametername.
.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 (or parmname).

Query



Query tab

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



Data Report support the multi query report and it will display the results in different tab pages.

Troubleshooting

While setting up the connection use the **Test Connection** button of the [Connection Properties Window](#) to make sure connection is configured properly.

Once your query has been written you can use the **Exec Query** button on the **Parameters** tab to preview the result of the query.

More information is available in the [Tips and Tricks Data Report](#) topic.

5.1.2.4.3 Database

Description



This entry is used to define and configure a 'Database' session. Database sessions don't do much on their own. They only serve as a holder for a connection string. Add Data Report session to unlock its full potential.

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

Settings

General

Source: Default

Data source: Microsoft SQL Server

Data provider: .NET Framework Data Provider for SQL Server

Connection string: [Redacted] [Eye icon] [More icon]

Host: DEVOLUTIONS18\SQLE2012

User name: [Redacted]

Password: [Redacted] [Eye icon]

Database settings

Properties	
Source	Default, Credential entry or Inherited
Data source	Read only, extracted from the connection string.
Data provider	Read only, extracted from the connection string.
Connection string	The database connection string, can be hidden/encrypted for better security
Host	Connection server name. Read only, extracted from the connection string.
User name	Read only, extracted from the connection string. It is blank if you are use Windows Authentication.
Password	Read only, extracted from the connection string. It is blank if you are use Windows Authentication

Source	
Default	The connection string is defined within the session.
Credential Entry	Use a linked Connection String credential entry for the connection string.
Inherited	Navigate down the inheritance graph of the object to find the connection string.

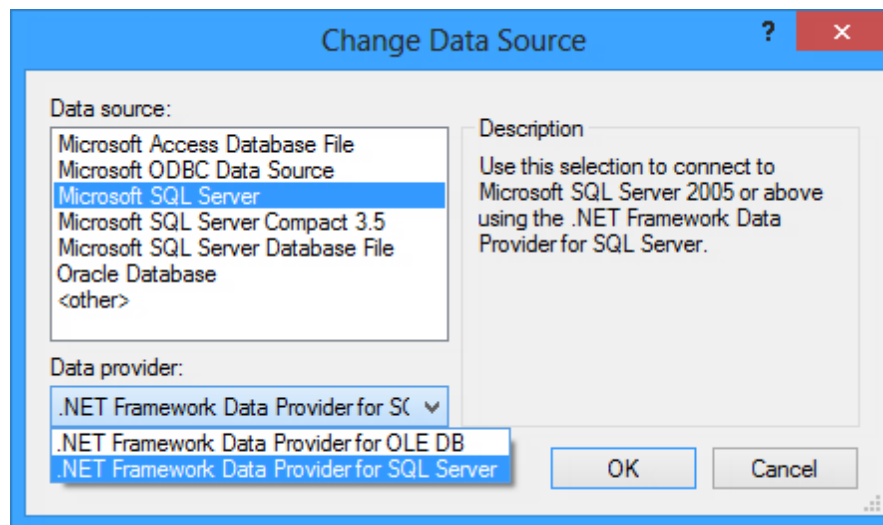
Prompt	At open connection time, the system will prompt the user to select the desired Connection String credential entry.
--------	--

Workflow

To create a Database session using a default data source, click on the ... button to define your connection string.

Connection properties

Make sure you select the appropriate data provider for the database you want to connect to. Hit the **Change...** button.



Select Data source & Data provider

Example:

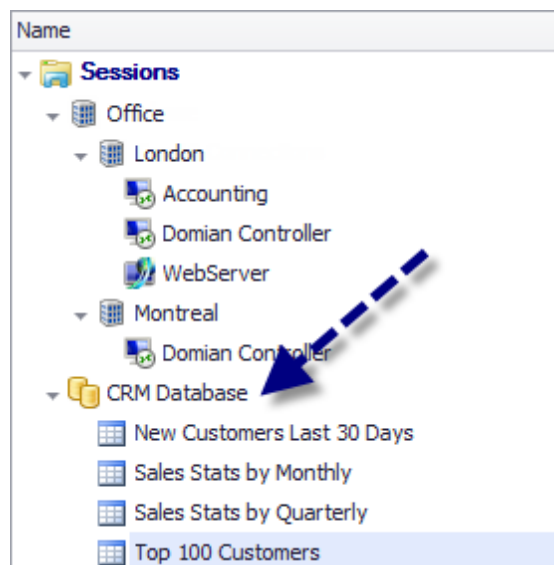
SQL Server - **Microsoft SQL Server**, **.NET Framework Data Provider for SQL Server**

Oracle - **Oracle Database**, **.NET Framework Data Provider for Oracle**

Specify sever name, database name and all other required information for the chosen data provider.

Once you have a Database session you can add child Data Report sessions, set data source as Inherited.

The tree view should look something like this:



Sample Database session with child Data Report sessions.

Troubleshooting

While setting up the connection use the **Test Connection** button of the [connection properties window](#) to make sure connection is configure properly.

5.1.2.4.4 Inventory Report

Description



This entry is used to define and configure a 'Inventory Report' session.

- Auto Login
- Built in
- Copy Password
- Credential Repository
- Embedded Mode
- Show Opened Session

Settings

5.1.2.4.5 PowerShell

Description




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

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

Settings

General Host and Credentials

 ☒ Command

☐ File name

Arguments

☒ No exit

☐ No profile

☐ Non interactive (suppress error message)

☐ Single thread apartment

☐ No logo

☐ Run as Administrator

☐ Run in 64 Bits mode

PowerShell settings

Notes

The remote system must be configured to allow remote commands. Please consult [Enable and Use Remote Commands in Windows PowerShell](#)

5.1.2.4.6 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.

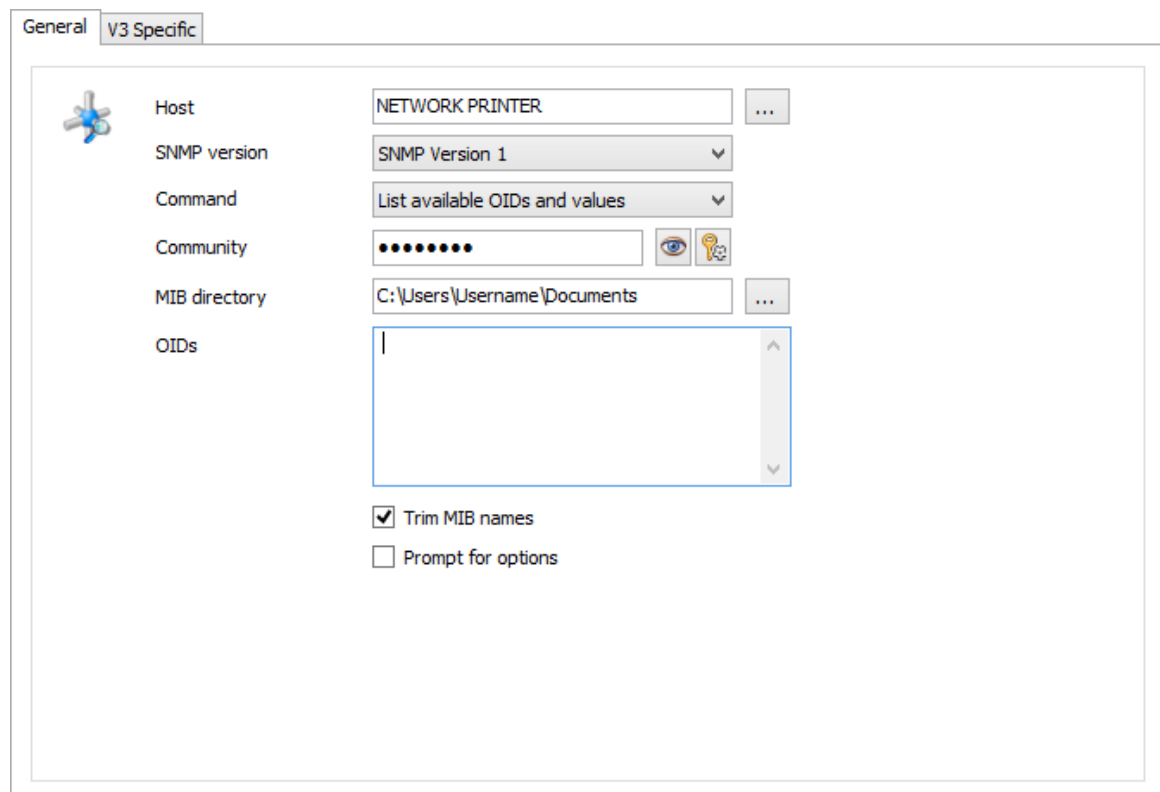


Remote Desktop Manager uses a specific tool (NET-SNMP) for the SNMP Report. You will be prompted to download it if it's not already installed on your computer.

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

Parameters	Description
Host	Host name / IP address of host
SNMP version	Version of your SNMP (V1, V2c or V3)
Command	Determine the content of the report
Community	Community equal to the password. By default, the password is the word public
MIB Directory	Location of the directory for the MIB database
OIDs	Object identifier for an object in the MIB. This help you reduce the items in the report
Trim MIB names	Remove MIB names
Prompt for options	Options to change the command or to specify a OIDs before the report execution

Available Command

- List available OIDs and values
- Get specific OIDs values
- Status of the host



More commands can be added to Remote Desktop Manager upon request, please post a feature request on our forums.

OIDs examples


- sysDescr.0
- sysObjectID.0
- sysUpTimeInstance
- sysContact.0
- sysName.0



V3 Specific





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

General V3 Specific

 Authentication protocol

Authentication passphrase  

Privacy protocol

Privacy passphrase  

Security engine ID

Security name

Context engine ID

Context name

Destination engine

SNMP Report V3 Specific Tab

Parameters	Description
Authentication protocol	Choose between None, MD5 or SHA
Authentication passphrase	Authentication protocol password
Privacy protocol	Choose between None or DES
Privacy passphrase	Privacy protocol password
Security engine ID	Part of the target host configuration
Security name	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	Choose between Not specified, Boots and 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.

```
ifAdminStatus.1 = up  
ifAdminStatus.2 = down  
ifAdminStatus.3 = up  
ifOperStatus.1 = up  
ifOperStatus.2 = down
```

Execution Log

Execution Logs


Save

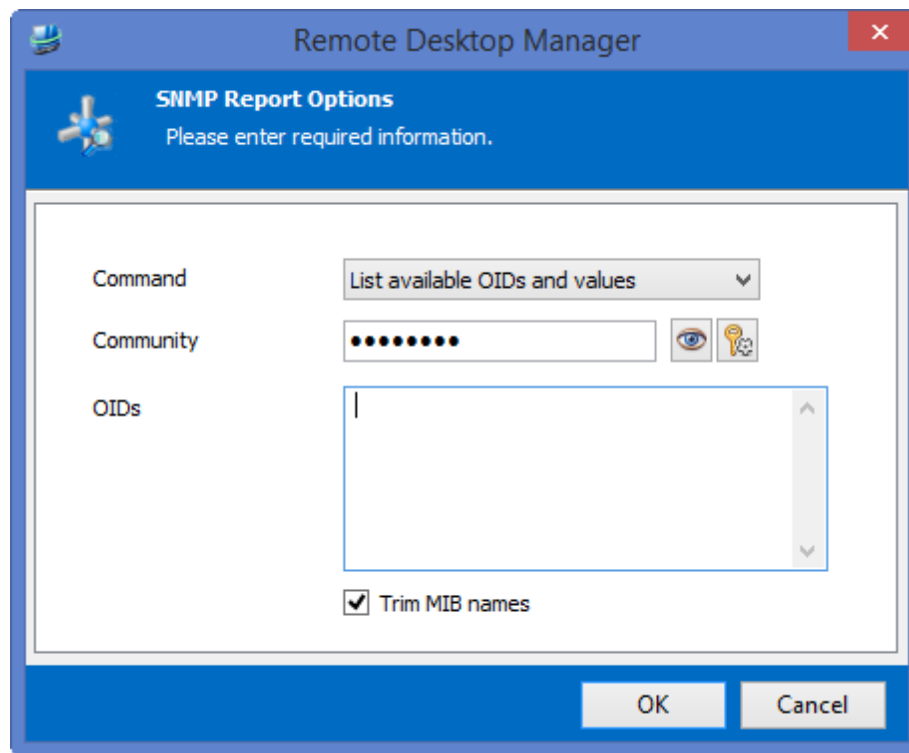
You can save the report or the execution log in a Text document to keep your information or to print it.



Save button

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.



Refresh window

5.1.2.4.7 SQL Server Management Studio

Description




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

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

Settings


General

 Server/Instance

Database

☐ Integrated security (Active Directory) Run as different user

User name

Password 

Default query file ...

☐ Show Splash screen

SQL Server Management Studio

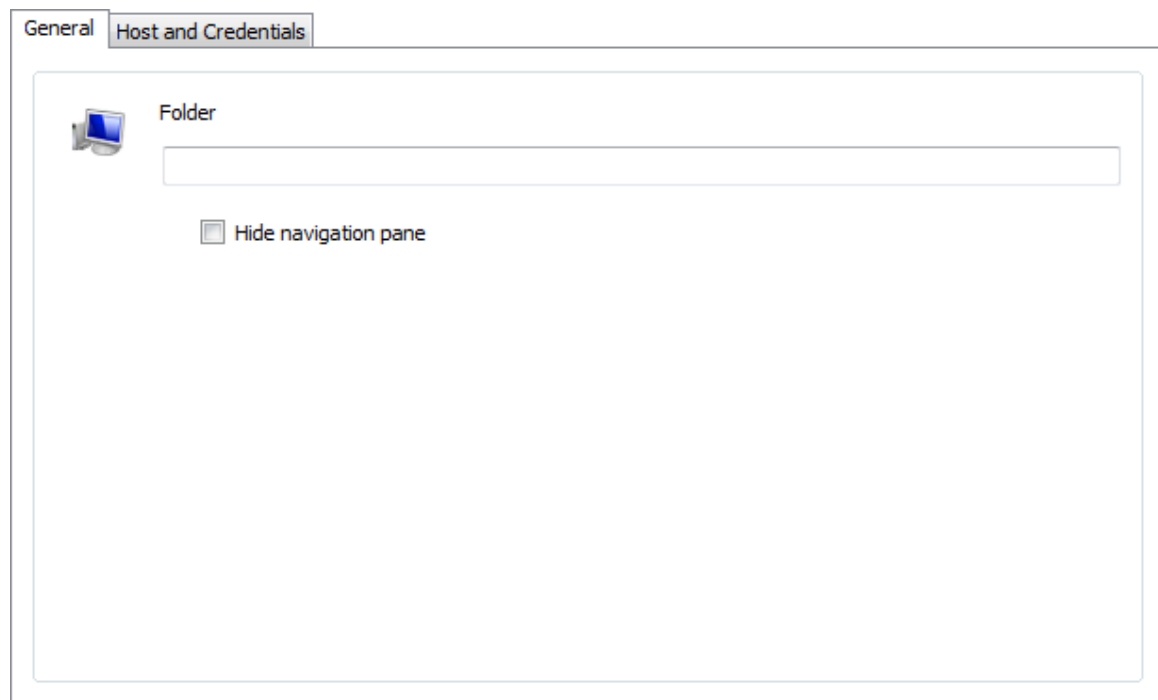
5.1.2.4.8 Windows Explorer

Description

This entry is used to define and configure a 'Windows Explorer' session.

- Auto Login
- Copy Password
- Credential Repository
- Embedded Mode
- External Mode
- Multi Monitor Support

Settings

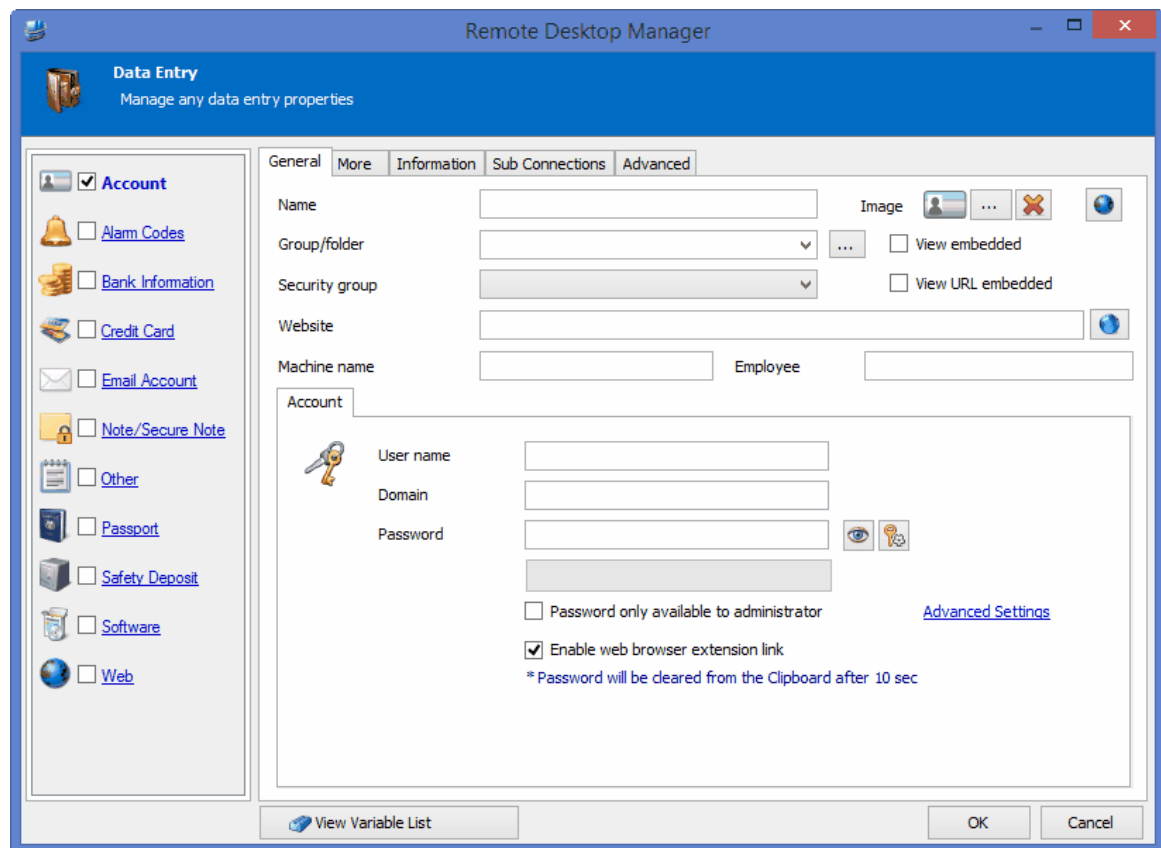


The screenshot shows a software window with two tabs: 'General' and 'Host and Credentials'. The 'Host and Credentials' tab is active. Inside this tab, there is a section labeled 'Folder' with a computer icon. Below this label is a text input field. Further down, there is a checkbox labeled 'Hide navigation pane'.

5.2 Data Entries

Description

Title	Description
Name	The name of the data entry that appears in the data entries list.
Group / folder	This is used to organize the data entry in different folders, either in the context menu or in the tree view. Learn more here .
Security Group	In the Professional edition, allows the Administrator to assign a security group to a data entry, and permit a subset of selected users to see this data entry.
Website	Url of the web page for this entry. Url will be used to navigate to the web site.
Machine name	Machine name
Employee	Employee name
More tab page	Contains the data entry description, the keyword entries and typing macro information. The data entry description can be in plain text, in rich text format, or a website link.
Information tab page	Contains different types of information related to the data entry, such as the machine specifications or some useful notes. Custom information can also be added.
Sub Connections tab page	Contains different types of entries or sessions that can be added to the data entry.
Advanced tab page	Contains more advanced settings related to the data entry.

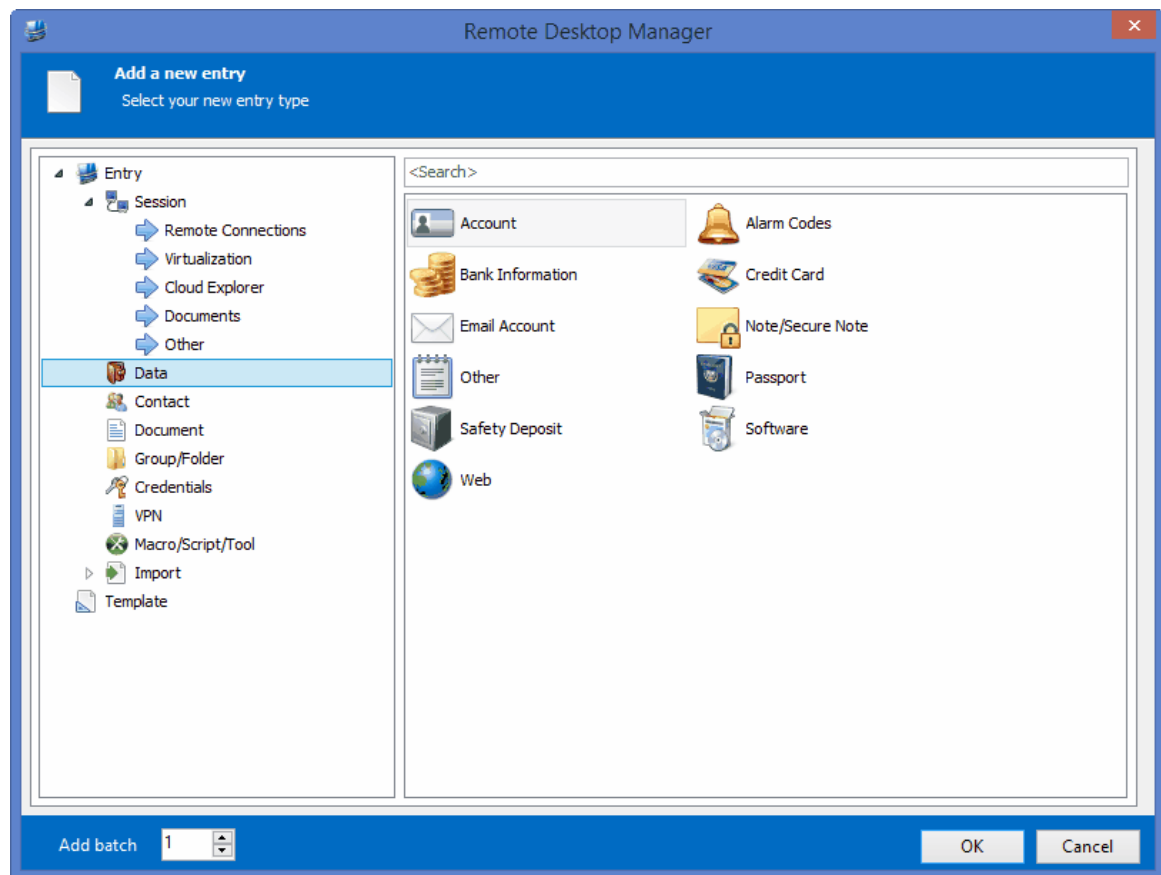


Data entry common settings

5.2.1 Overview

Description

Data entry types are used to store sensitive information like account information, serial numbers, credit card information into the data source.



New data entry dialog

Refer to these topics for more information

- [Account](#)
- [Alarm Codes](#)
- [Bank Information](#)
- [Credit Card](#)
- [Email Account](#)
- [Note/Secure Note](#)
- [Other](#)
- [Passport](#)
- [Safety Deposit](#)
- [Software/Serial](#)
- [Web](#)

5.2.2 Auto Fill

Description

Web browser auto fill via browser extension is available for Chrome, Firefox and Internet Explorer.

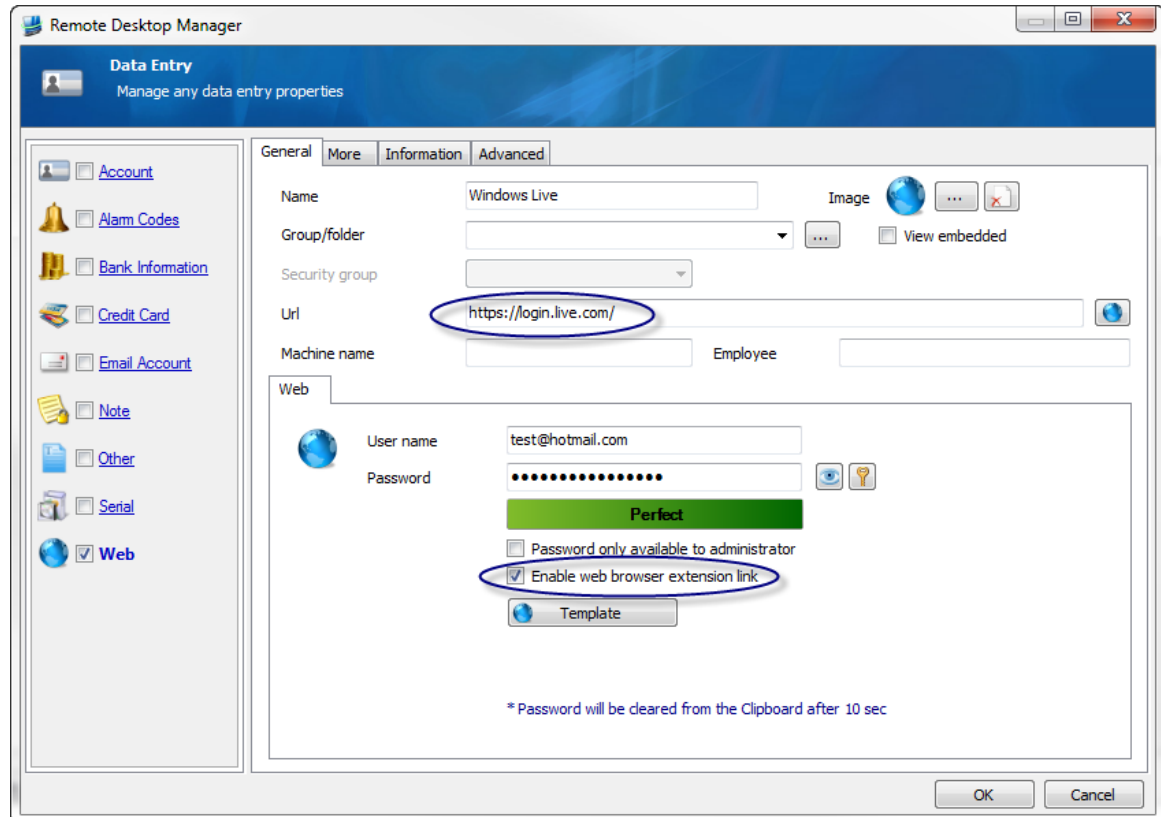
Installation

- [Chrome Extension](#)

- [Firefox Extension](#)
- [IE Extension](#)

Creating Data Entries/Sessions

Web & Account data entry types & [Web Browser](#) sessions support Auto Fill. They must however be configured to allow web browser extension links. The Url field must be the URL of the login page for the given page (Ex. <http://login.live.com>). You must also enable the **Enable web browser extension link** option.



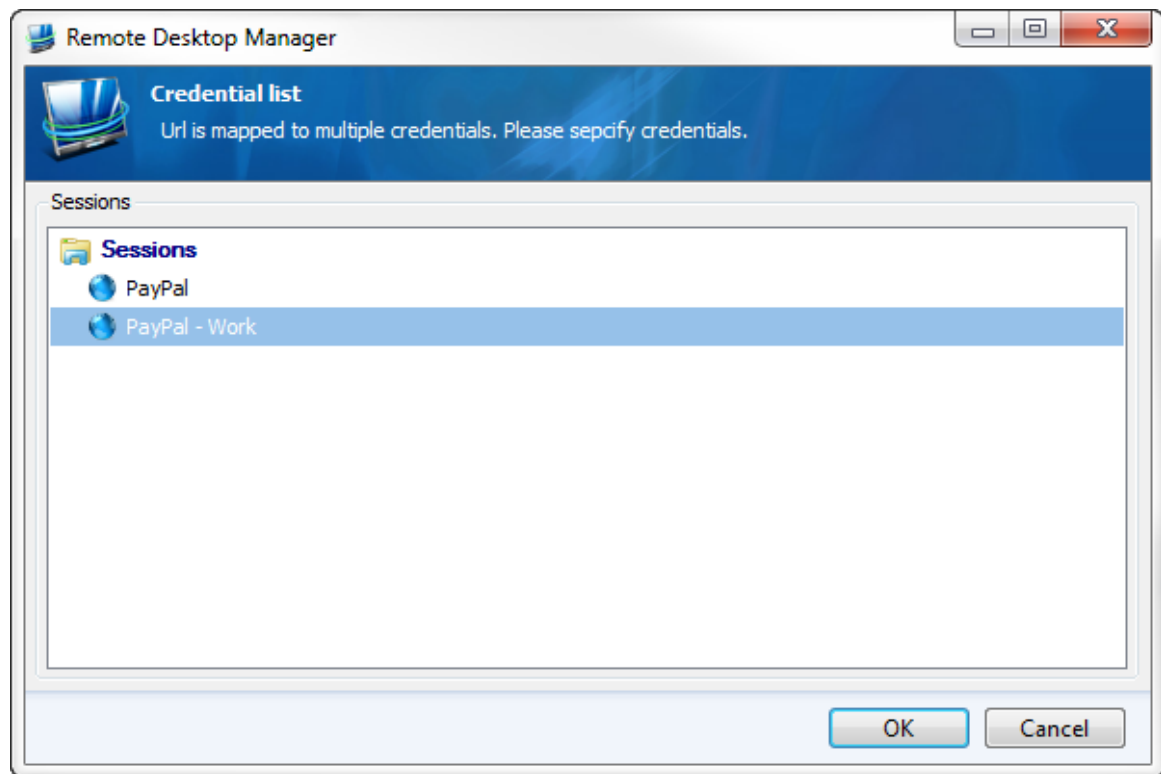
Auto fill support

Troubleshoot

Data entries must be marked (checked) as "Enable web browser extension link" for auto fill feature to work.

If Remote Desktop Manager is configured with multiple data sources only the currently active data source will be queried.

When multiple data entries match the web site Remote Desktop Manager will prompt for you to select a specific data entry.



Select specific data entry

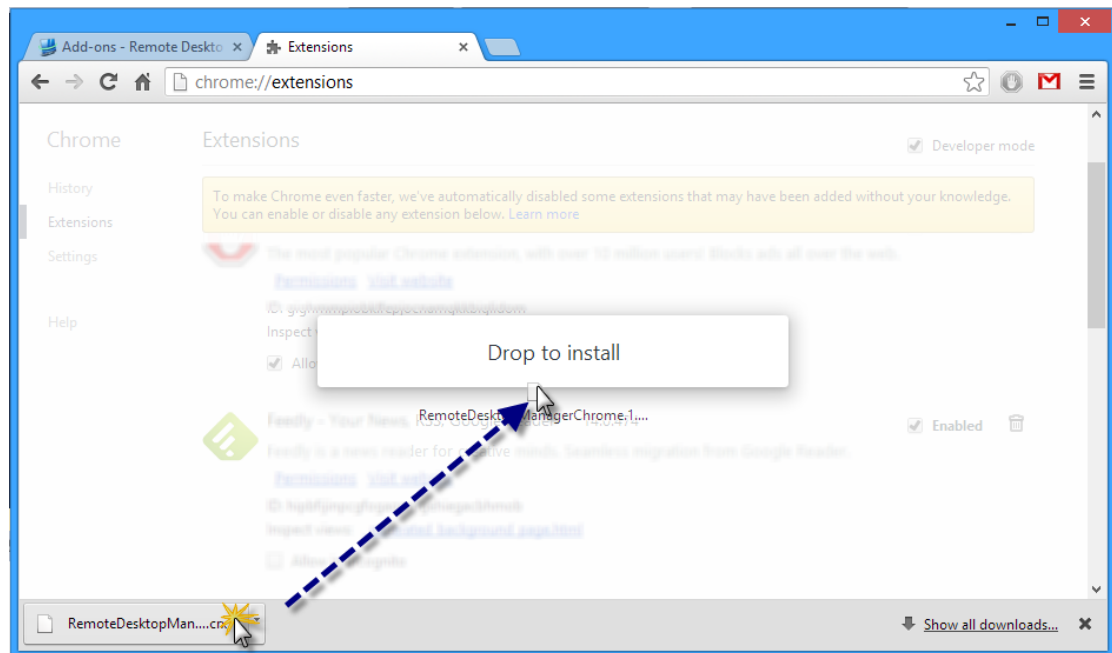
5.2.2.1 Chrome Extension

Description

Remote Desktop Manager - Chrome Extension

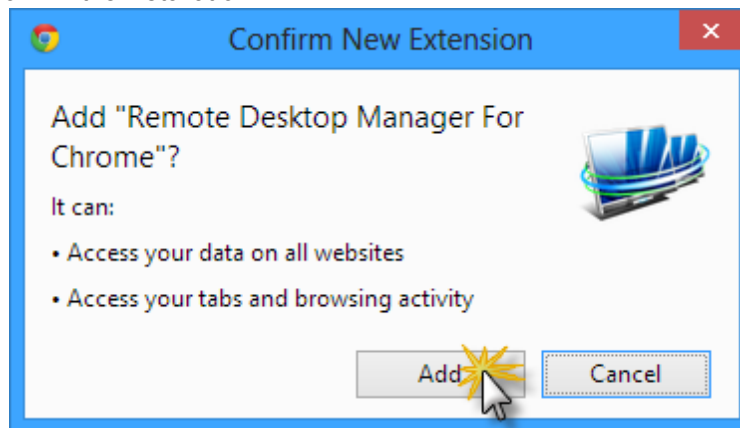
Installation

- Start Chrome
- Go [here](#) & download (right click -> Save link as...) the .crx file Remote Desktop Manager for Chrome Extension
- Open the Chrome Extensions window (Tools -> Extensions)
- Drag-drop the extension from the download bar to the extension window



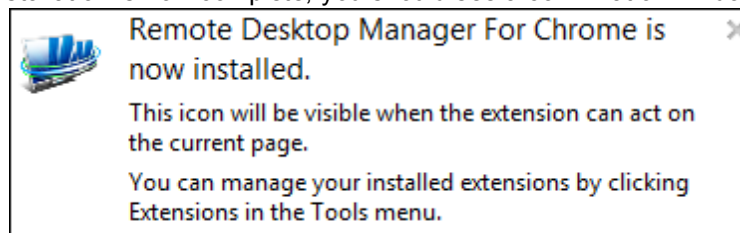
Drag-drop the .crx file onto the Extension window.

- Confirm the installation



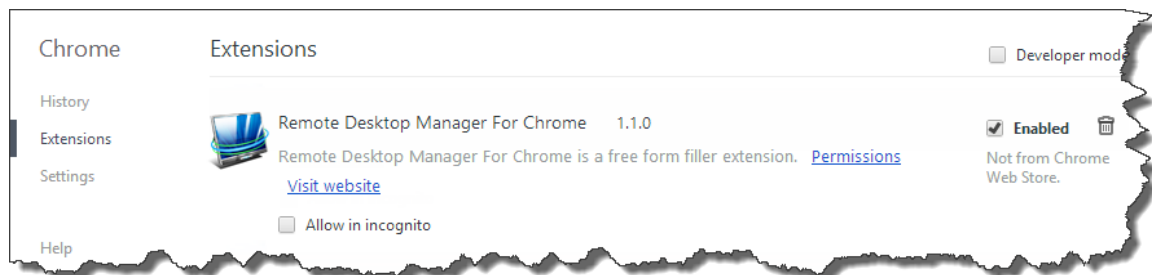
Confirm Chrome Extension Installation

- Installation is now complete, you should see a confirmation window (top right of Chrome)



Remote Desktop Manager For Chrome is now installed

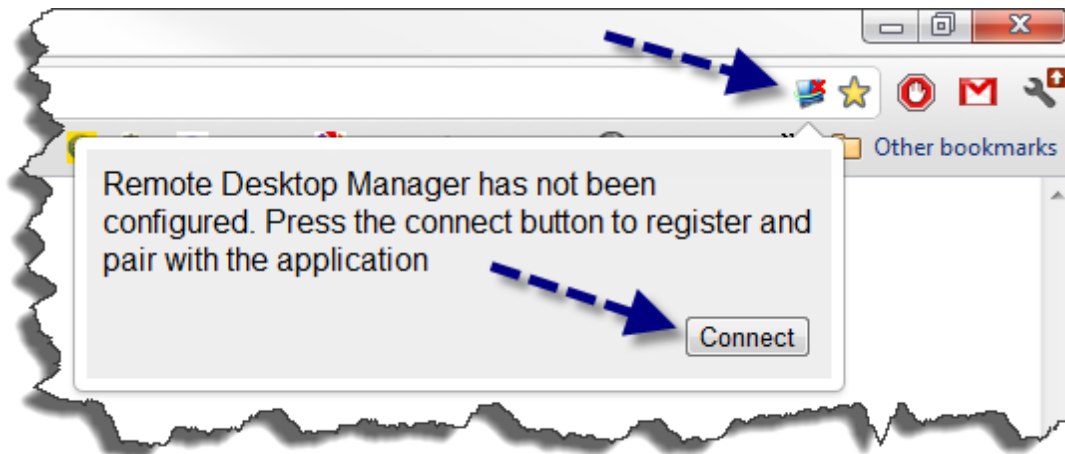
- To view/manager all installed Chrome extensions Tools -> Extensions



Remote Desktop Manager For Chrome is now installed

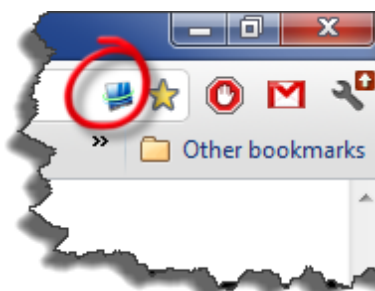
Using

- Open Remote Desktop Manager if not already started
- You will need to configure the Remote Desktop Manager for Chrome extension of first use



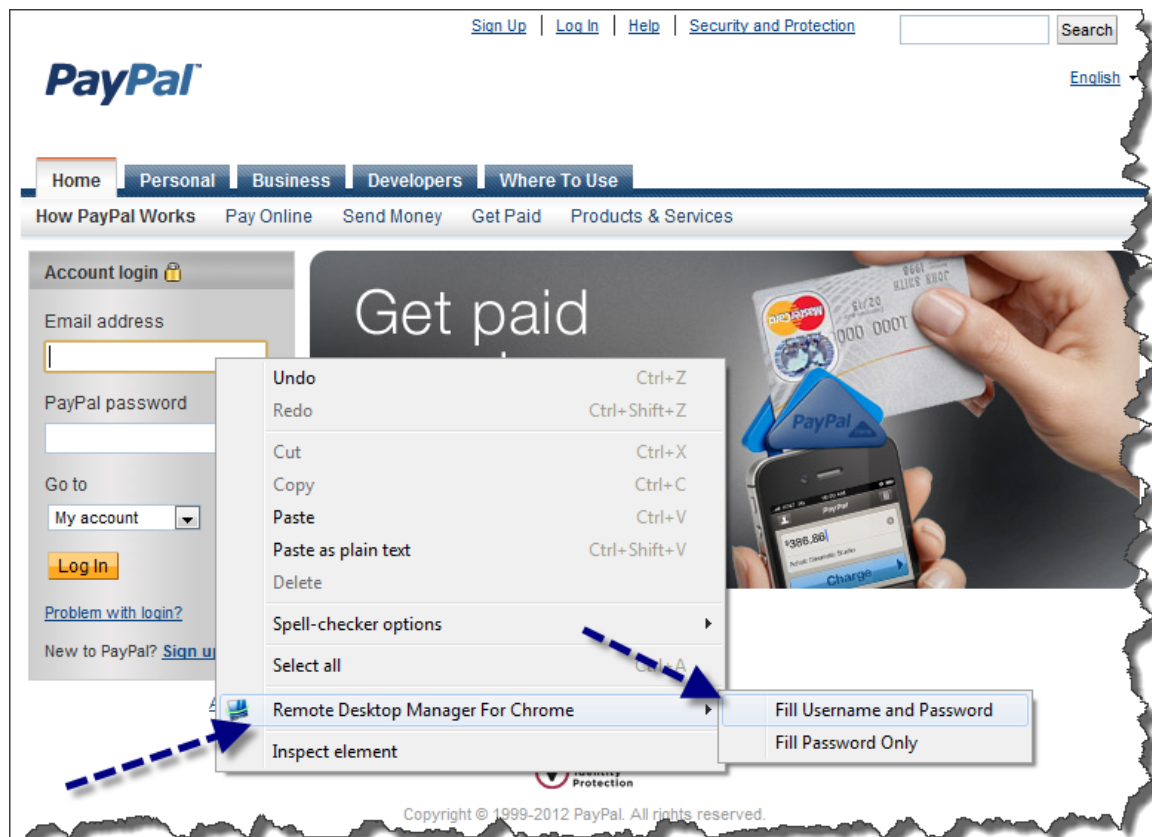
Connect Extension to RDM

- Open a web site that has been configured in Remote Desktop Manager
- Check the status of the extension



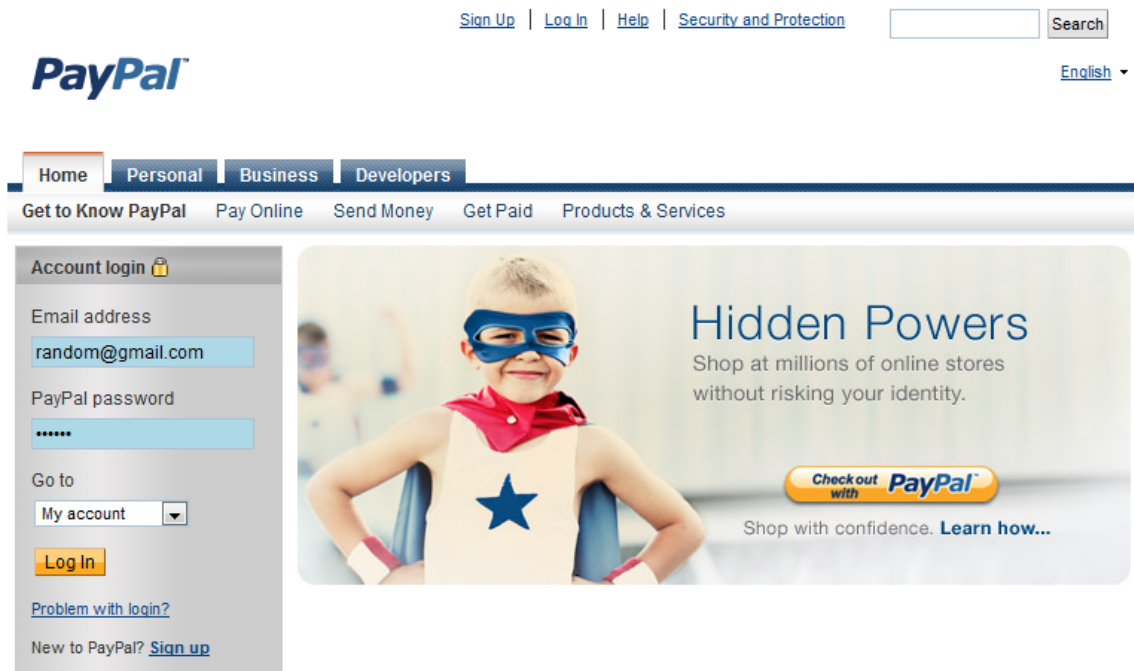
Connect Extension to RDM

- Right click in either the username or password field and select the fill option



Select Fill Option

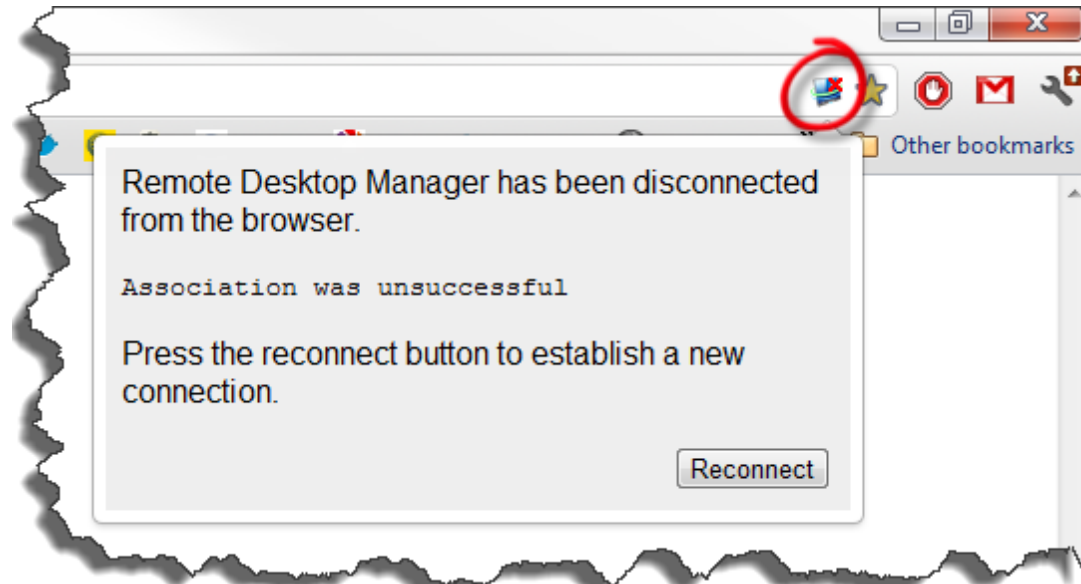
- Result



Sample web site populated with Remote Desktop Manager auto fill feature

Troubleshoot

If an error occurs the extension icon will show the error icon. Simply click on the icon for further information.



Sample Extension Error

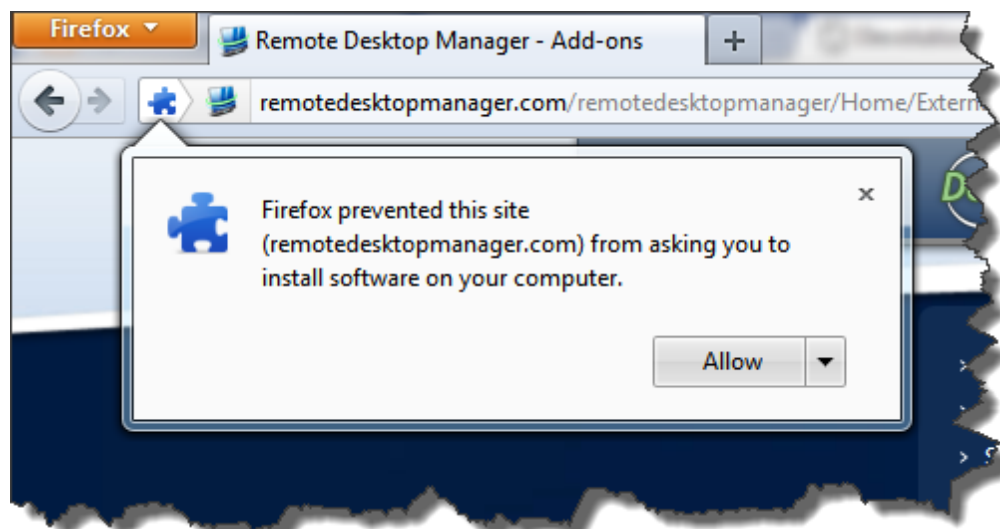
5.2.2.2 Firefox Extension

Description

Remote Desktop Manager - Chrome Extension

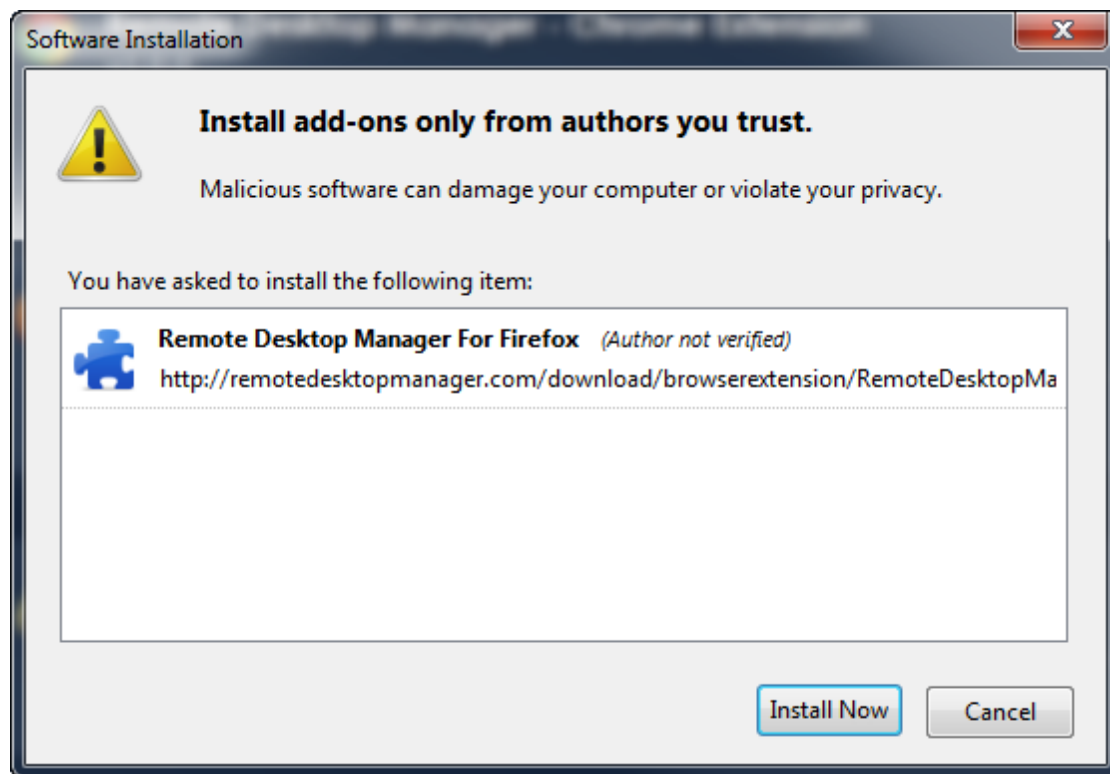
Installation

- Start Firefox
- Go [here](#) & download the .xpi file Remote Desktop Manager - Firefox Extension



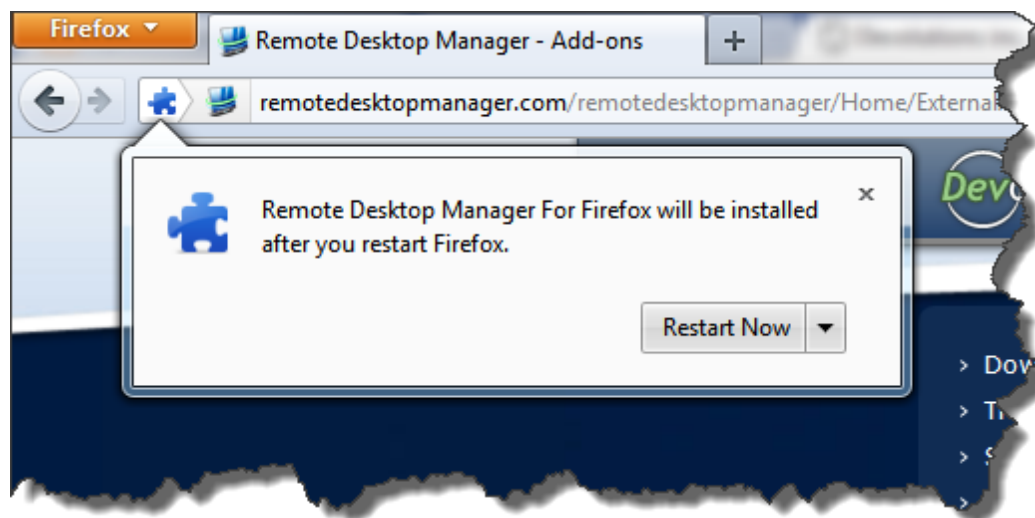
Allow Remote Desktop Manager Firefox Extension

- Confirm the installation



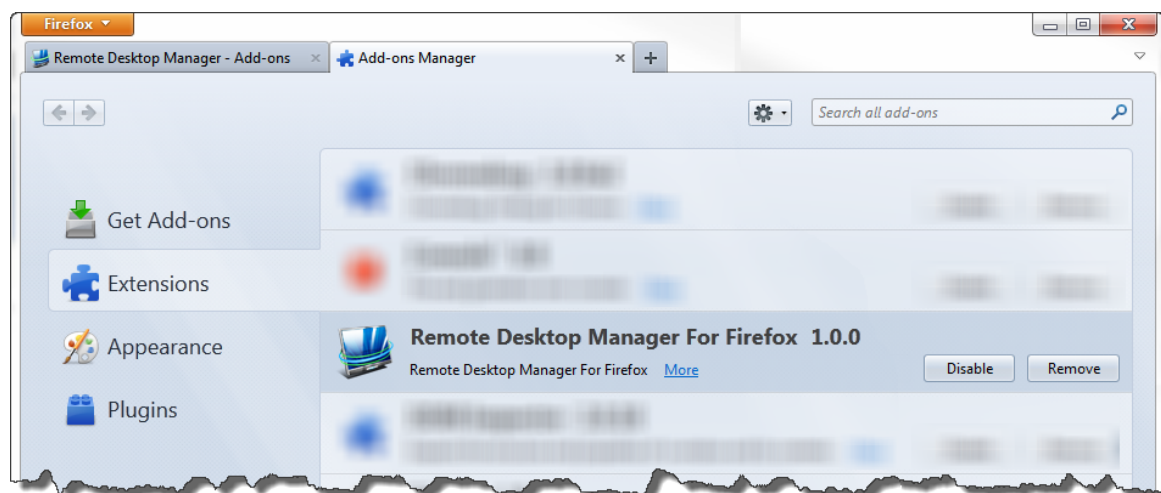
Confirm Remote Desktop Manager Firefox Extension Installation

- Restart Firefox



Restart Firefox

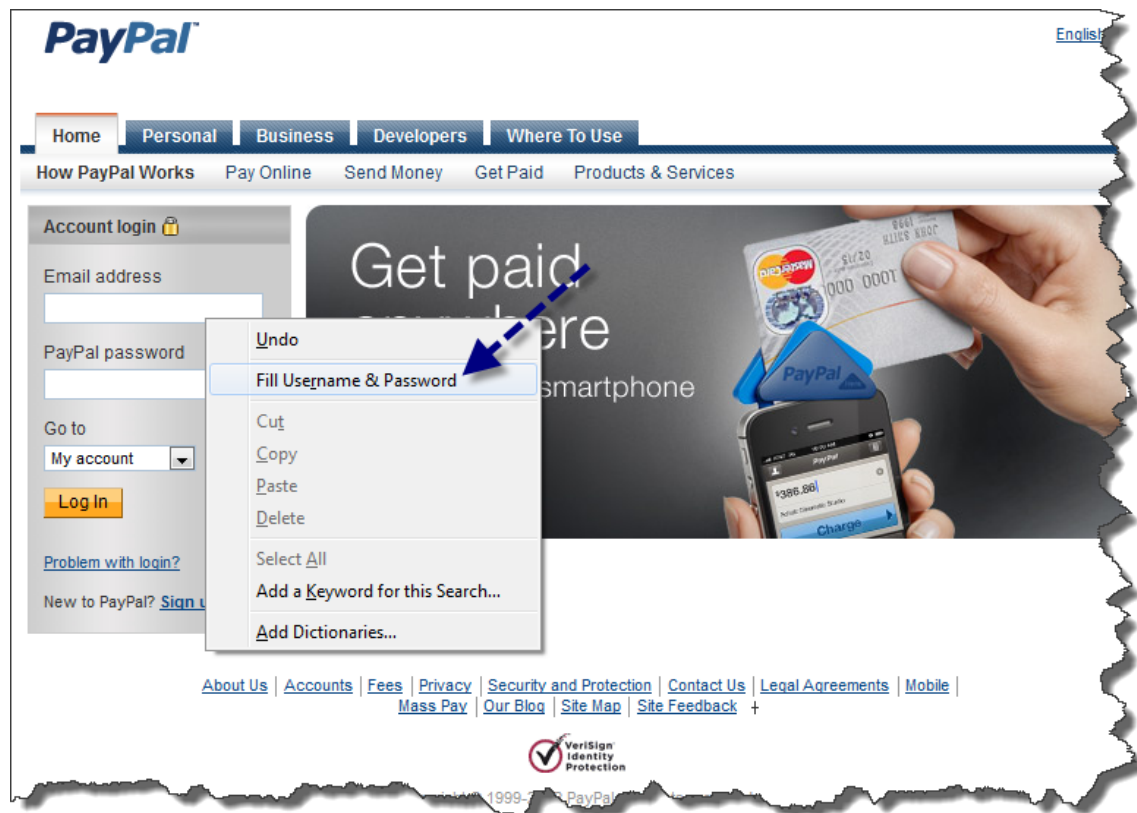
- To view/manager all installed Firefox extensions see Odd-ons menu



Remote Desktop Manager For Firefox is now installed

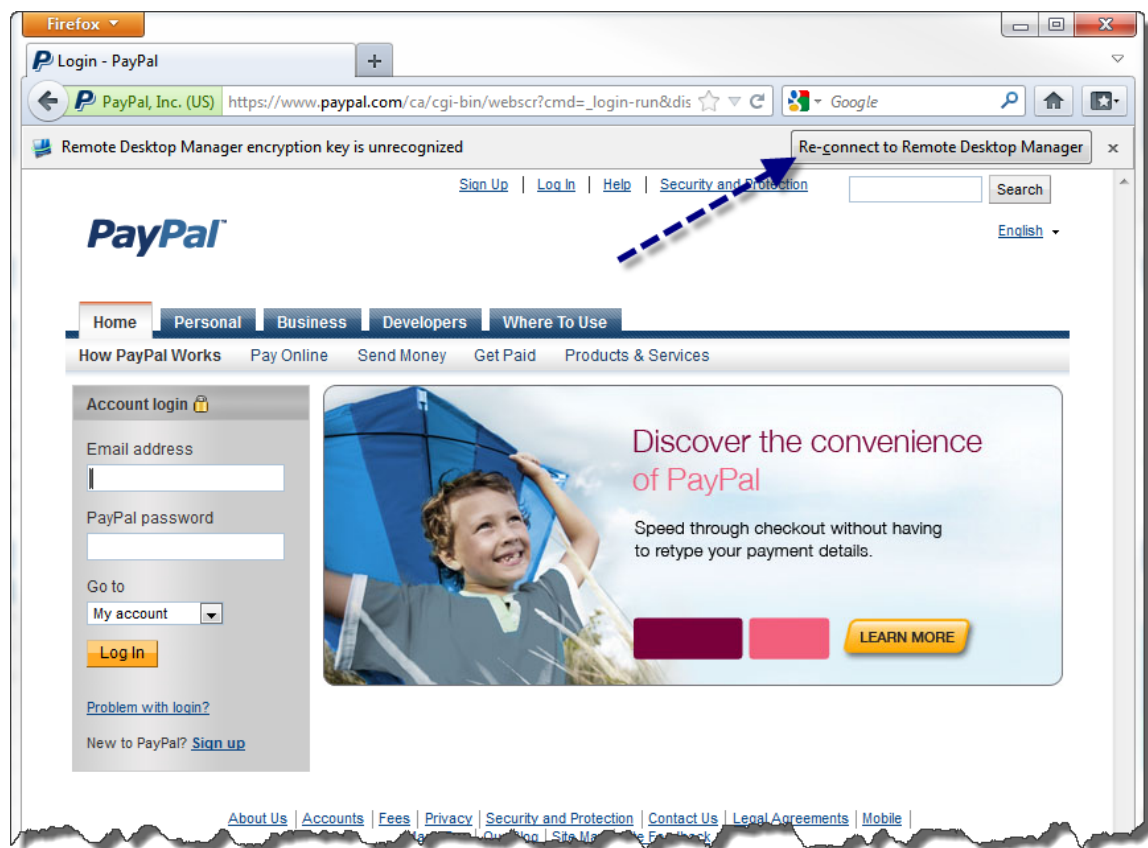
Using

- Open Remote Desktop Manager if not already started
- Open a web site that has been configured in Remote Desktop Manager
- Right click in either the username or password field and select the fill option



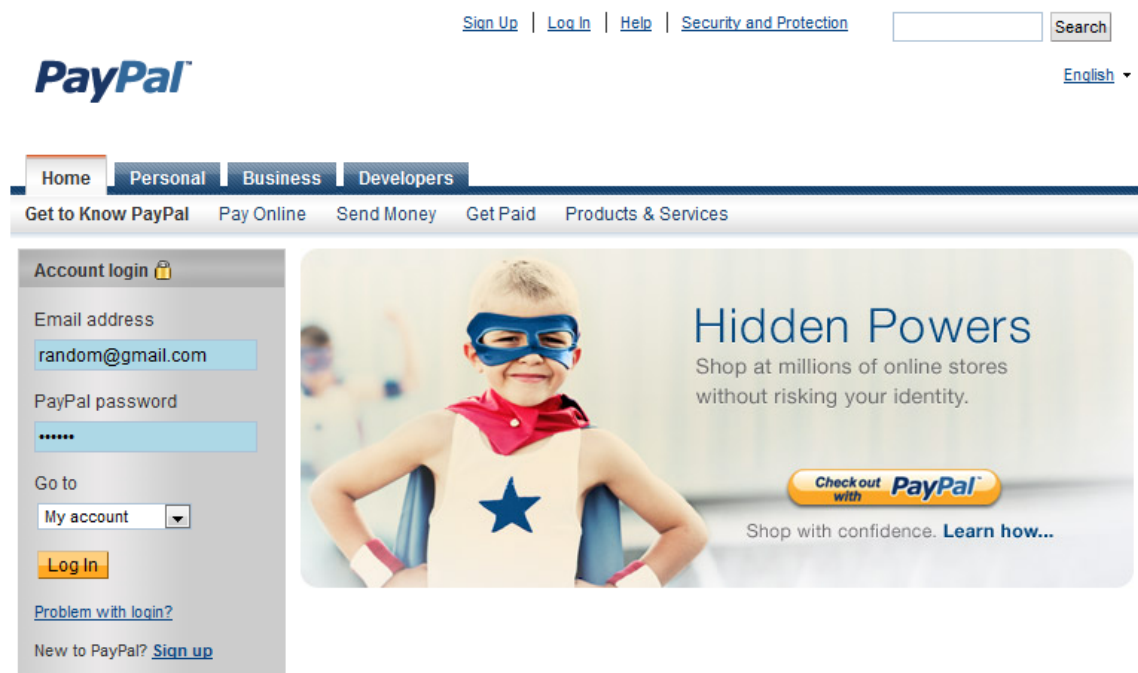
Select Fill Option

- You will need to configure the Remote Desktop Manager for Firefox extension on first use



Connect Extension to RDM

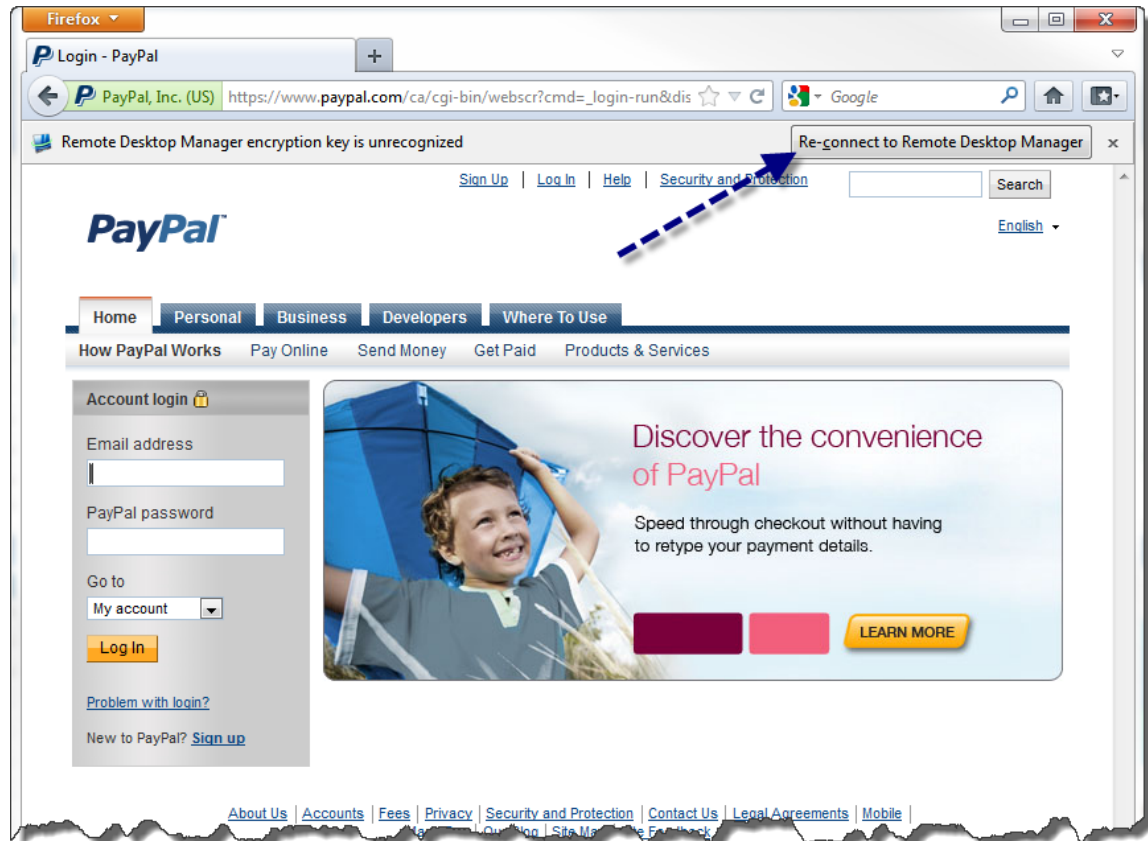
- Right click again
- Result



Sample web site populated with Remote Desktop Manager auto fill feature

Troubleshoot

You may need to re-configure the Remote Desktop Manager for Firefox extension once in a while



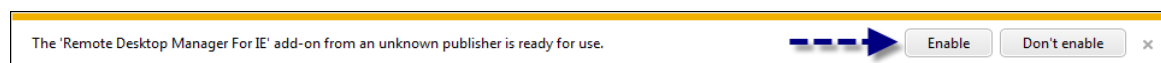
5.2.2.3 IE Extension

Description

Web browser auto fill is only available for Internet Explorer 8 or better.

Installation

- Download ([here](#)) & install the Internet Explorer Extension
- Start Internet Explorer
- If prompted to enable, make sure to enable

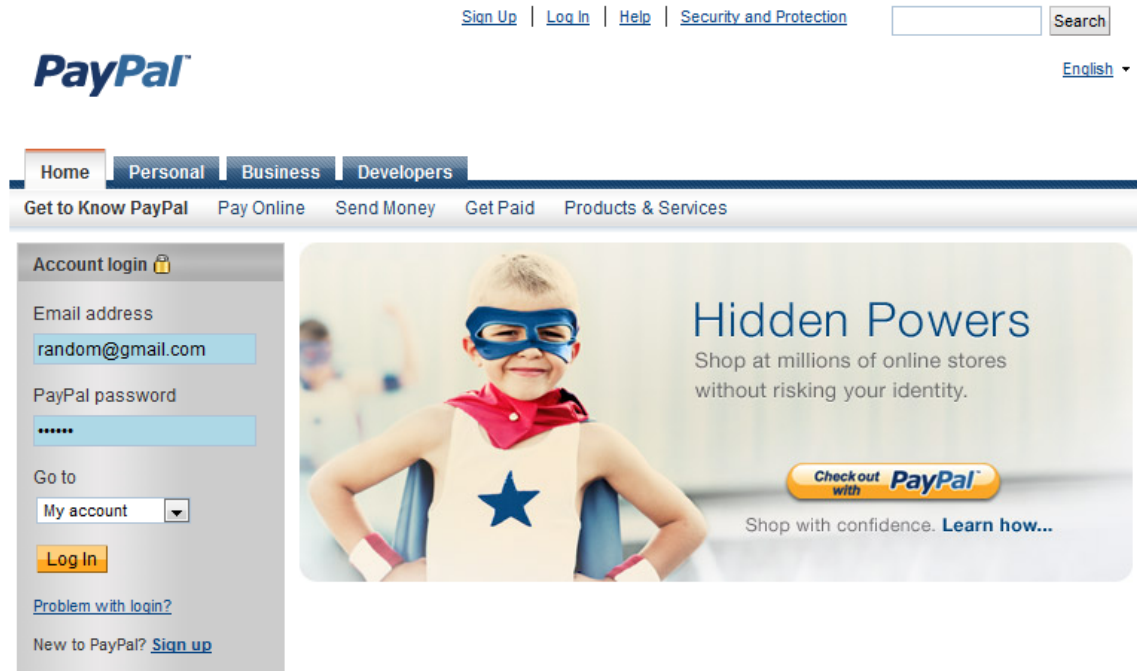


Enable Remote Desktop Manager For IE add-on

- Restart Internet Explorer

Using

- Open Remote Desktop Manager if not already started
- Open a web site that has been configured in Remote Desktop Manager, you should have the username & password automatically populated and both text boxes should now be light-blue

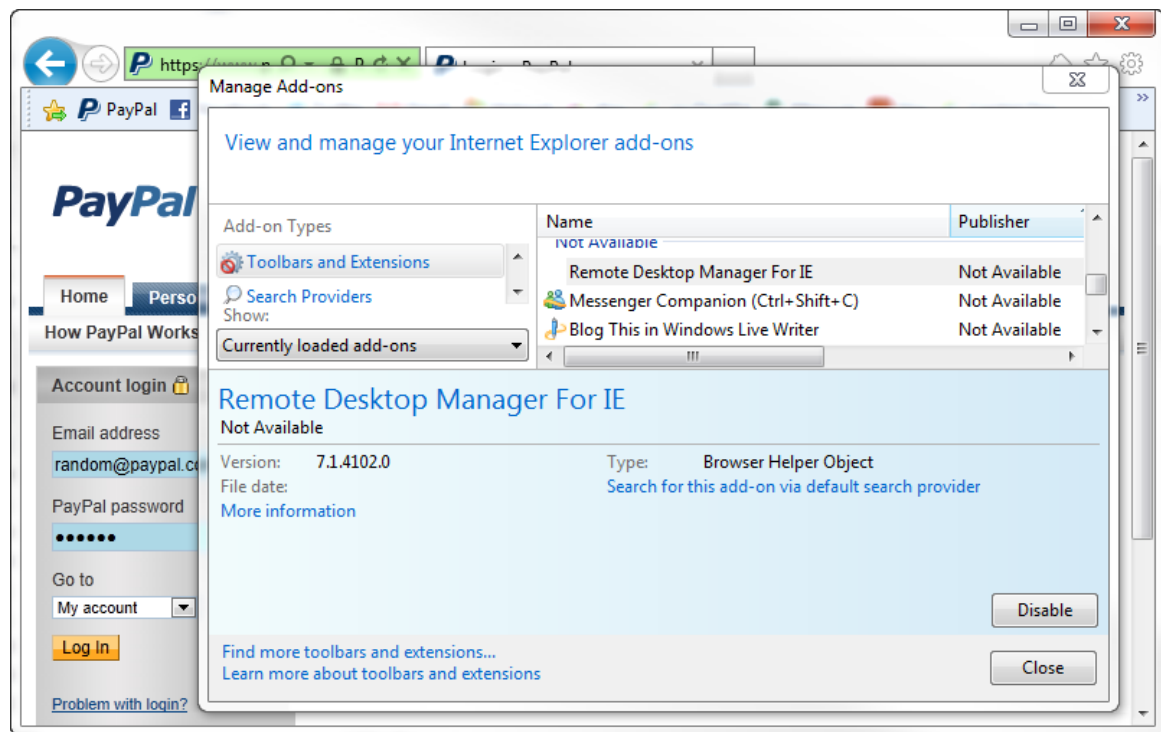


The screenshot shows the PayPal homepage. At the top right, there are links for [Sign Up](#), [Log In](#), [Help](#), and [Security and Protection](#), followed by a search bar and a language dropdown set to [English](#). The PayPal logo is on the left. Below the logo is a navigation bar with tabs for **Home**, **Personal**, **Business**, and **Developers**. Underneath this are links for [Get to Know PayPal](#), [Pay Online](#), [Send Money](#), [Get Paid](#), and [Products & Services](#). On the left side, there is a 'Account login' section with a lock icon. It contains fields for 'Email address' (populated with 'random@gmail.com') and 'PayPal password' (masked with dots). Below these is a 'Go to' dropdown menu set to 'My account', a 'Log In' button, and links for [Problem with login?](#) and 'New to PayPal? [Sign up](#)'. To the right of the login form is a large promotional banner for 'Hidden Powers' featuring a child in a superhero costume. The banner text says 'Shop at millions of online stores without risking your identity.' and includes a 'Checkout with PayPal' button and the text 'Shop with confidence. [Learn how...](#)'.

Sample web site populated with Remote Desktop Manager auto fill feature

Troubleshoot

Double check that the add-on is in fact enabled. In Internet Explorer on the Manage add-ons window.



Enable/Disable Remote Desktop Manager for IE

5.2.3 Types


5.2.3.1 Account

Description



The Account data entry type is used for storing account information including user name, domain & password.

Settings

Account

 User name

Domain

Password  

☐ Password only available to administrator [Advanced Settings](#)

☐ Enable web browser extension link

*Password will be cleared from the Clipboard after 10 sec


5.2.3.3 Bank Information

Description

The Bank Information data entry is useful for storing sensitive banking information such as account number & PIN.

Settings

Bank Information



Bank name

Bank branch

Account type

Account owner

Account number

Routing number

PIN

SWIFT

Phone

Address

Bank Information settings

Option	Secured	Description
Bank name		Enter bank name.
Bank branch		Enter bank branch name.
Account type		Indicate the account type.
Account owner		Indicate the owner of the account.
Account number		Enter bank account number.
Routing number		Enter bank code.
PIN	✓	Enter bank account PIN number.
SWIFT		Enter SWIFT code if the bank is member of the SWIFT network.
Phone		Enter bank phone number.
Address		Enter bank address.


5.2.3.4 Credit Card

Description

The Credit Card data entry is useful for storing sensitive credit card information such as card number, PIN or CVC.

Settings

Credit Card



Card owner

Card type

Card number ☐ Is hidden

Valid from

Expiration

Validation (CVC)

PIN

Password

Verified by

Secure code

Issuing bank

Customer service phone

Credit Card settings

Option	Secured	Description
Card owner		Credit card owner as it appears on the actual card.
Card type		Card type, choose from the list or type in the card type if it is not available in the list.
Card number	✓	Credit card number as it appears on the actual card.
Expiration	✓	Expiration date as it appears on the actual card.
Validation (CVC)	✓	The 3 or 4 digit security code as it appears on the back of the card.
PIN	✓	The PIN number for the card.
Password		Password associate with credit card.
Verified by		Online security requiring a password before every online purchase.
Secure code		3 digit security code as it appears on the back of the card.
Is hidden		Controls the security information for this card. If hidden is set all secured fields will be encrypted on export and hidden in view mode.

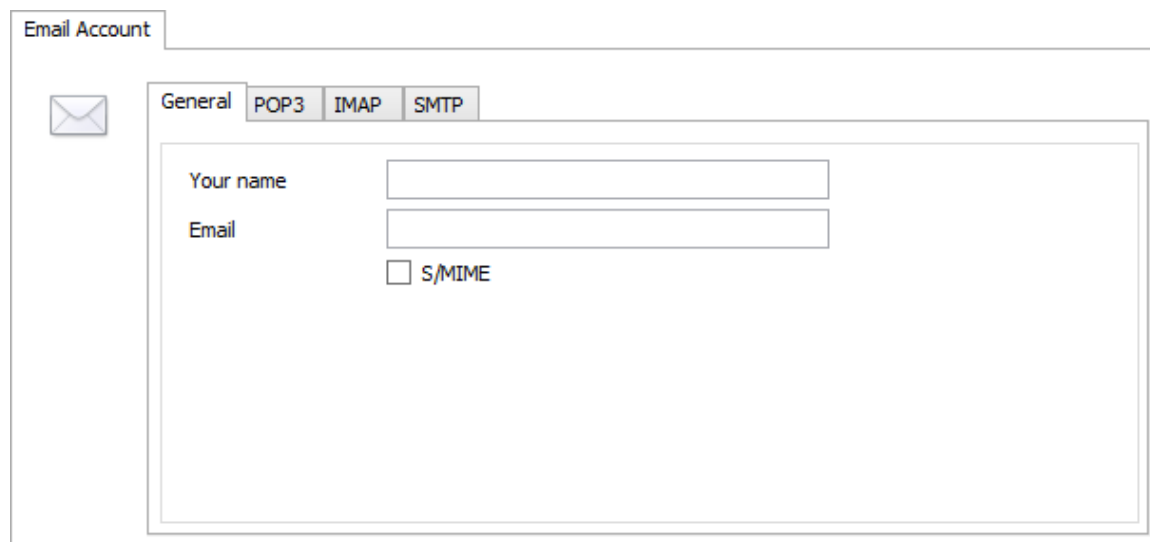
5.2.3.5 Email Account

Description

Securely store email account settings including POP3/IMAP/SMTP servers, user name & passwords.

Settings

General

The screenshot shows a dialog box titled 'Email Account'. It has a tabbed interface with 'General', 'POP3', 'IMAP', and 'SMTP' tabs. The 'General' tab is selected. On the left, there is an envelope icon. The main area contains three input fields: 'Your name', 'Email', and a checkbox labeled 'S/MIME'.

Email General settings

Option	Secured	Description
Your name		Account name
Email		Email address
S/MIME		Does this email account require/use Secure/Multipurpose Internet Mail Extensions


POP3

Email Account

General POP3 IMAP SMTP

Host name Port 110

User name

Password 

☐ SSL

Authentication Password

Email POP3 settings

Option	Secured	Description
Host name		POP3 host name
Port		POP3 port, default 110
User name		POP3 user name
Password	✓	POP3 password
SSL		POP3 requires SSL connection
Authentication		POP3 authentication mode


IMAP

Email Account

General POP3 IMAP SMTP

Host name Port 143

User name

Password 

☐ SSL

Authentication Password

Email IMAP settings

Option	Secured	Description
--------	---------	-------------

Host name		IMAP host name
Port		IMAP port, default 110
User name		IMAP user name
Password	✓	IMAP password
SSL		IMAP requires SSL connection
Authentication		IMAP authentication mode

SMTP

The screenshot shows the 'Email Account' settings window with the 'SMTP' tab selected. The fields are as follows:

- Host name: [Text Field]
- Port: 25 (Spinner)
- ☐ My outgoing server (SMTP) requires authentication
- ☐ Use same settings as my incoming mail server
- User name: [Text Field]
- Password: [Text Field] (with eye icon for visibility toggle)
- ☐ SSL
- Authentication: Password (Dropdown)

Email SMTP settings

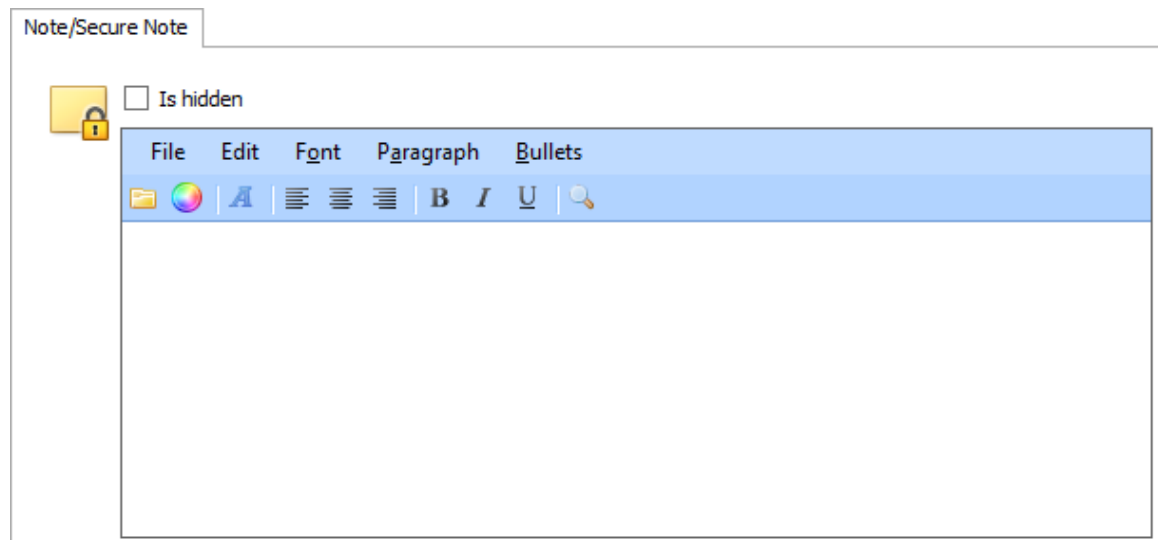
Option	Secured	Description
Host name		SMTP host name
Port		SMTP port, default 110
My outgoing server (SMTP) requires authentication		Does the SMTP server require authentication
Use same settings as my incoming mail server		Use POP3 or IMAP settings for the outgoing server authentication
User name		SMTP user name
Password	✓	SMTP password
SSL		SMTP requires SSL connection
Authentication		SMTP authentication mode

5.2.3.6 Note/Secure Note

Description

Note data entry is a simple free form note allowing you to securely store any type of free from information.

Settings



Note/Secure note settings

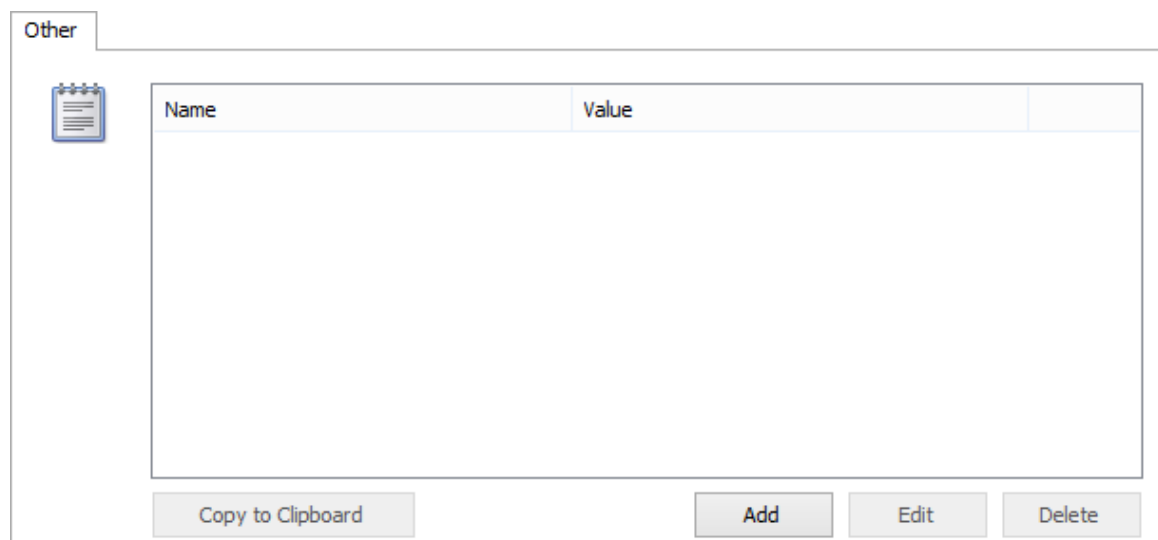
Option	Secured	Description
Note	✓	Any free form RTF text
Is hidden		Controls the encryption of the note on export and view

5.2.3.7 Other

Description

The Other data entry type is used for securely storing name/value pairs of information.

Settings



Other settings

Option	Secured	Description
Name		Name of the settings
Value	✓	Value of the settings
Is hidden		Is the value hidden (secured). On export a hidden value will be encrypted


5.2.3.8 Passport

Description

The Passport data entry is useful for storing your passport information such as your passport number and its expiration date.

Settings

Passport




Last name

First / middle name

Gender


☒ Male
 ☐ Female

Passport number



Expiration

2013-11-13



Country of issue

Passport Settings

Option	Secured	Description
Last name		Last name on the passport
First / middle name		First / middle name on the passport
Gender		Male or Female
Passport number	✓	Passport number
Expiration		Expiration date on the passport
Country of issue		Country who issue the passport


5.2.3.9 Safety Deposit


Description

The Safety Deposit data entry is used to store your safety deposit information.


Settings

Safety Deposit



Institution
Address
Customer service number
Box number 
Passcode

Safety Deposit Settings

Option	Secured	Description
Institution		Name of the institution
Address		Address of the institution
Customer Service Number		Customer service number
Box number		Personal Box number
Passcode		Personal Passcode


5.2.3.10 Software/Serial

Description




Software/Serial is a data entry that provides the ability to store software serial number information. Including version, expiry date, name and license key.

Settings

Software



Software
Version
Licensed to
Associated email
Purchase date
Renewal date
Licenses

☐ 2013-11-25 
☐ 2013-11-25 
 

Software serial settings

Option	Secured	Description
Software		Software name
Version		Software version number
Licensed to		Name of person who register the license
Associated email		Email associate to the license
Purchase date		Purchase date of the license
Renewal date		Date to renew the license
Licenses		Single key or list of keys


5.2.3.11 Web

Description

The Web data entry type is used for storing web site credential information including user name, domain and password.



Settings

Web



User name


Domain

Password  

☐ Use credential repository

☐ Password only available to administrator

☐ Enable web browser extension link

 Template

[Security Questions](#)

[Advanced Settings](#)

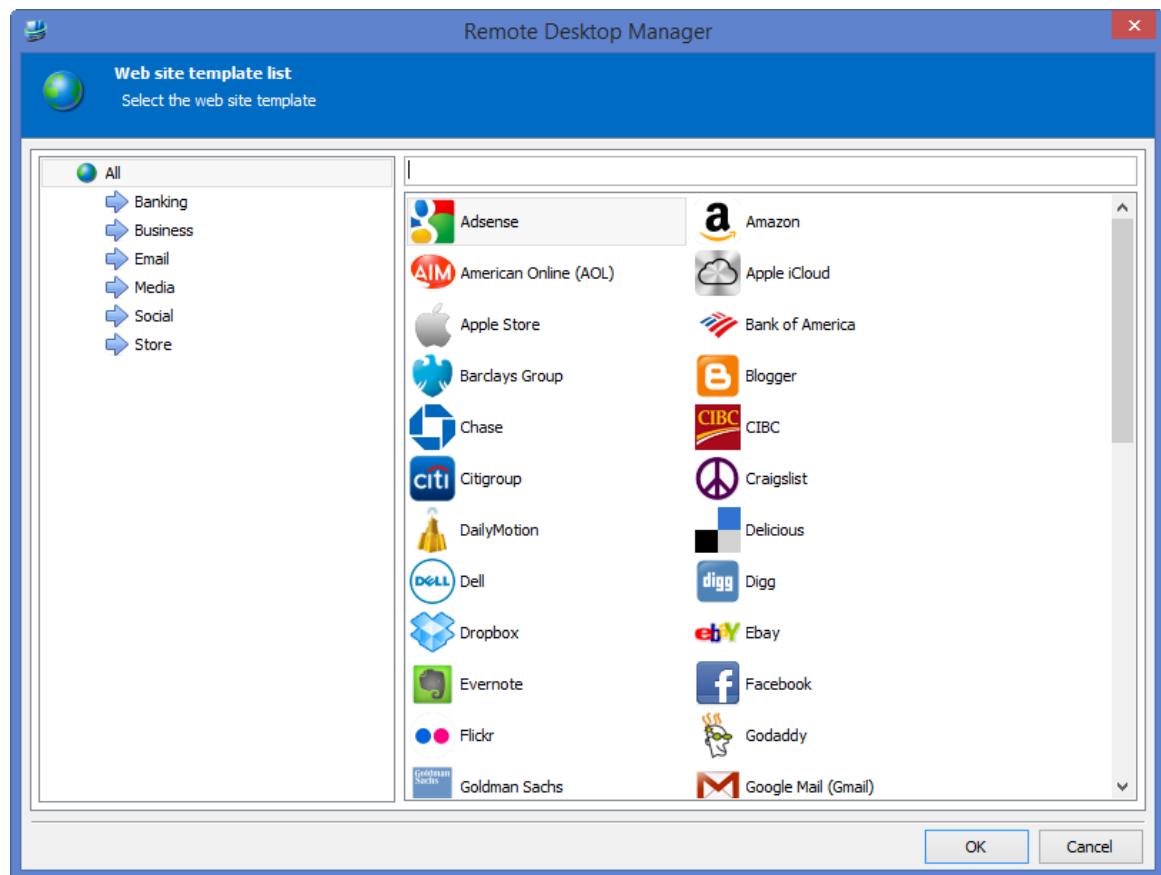
Web settings

Option	Secured	Description
User name		The user name associated to the account
Domain		The domain associated to the account
Password	✓	The password associated to the account
Use credential repository		Use a credential repository to login
Password only available to administrator		Must be administrator to be able to view/reveal password the password
Enable web browser extension link		Data entry will be available for the auto fill feature

Templates

You can chose from over 55 pre-built templates to help eliminate guess work. For example:

- Facebook
- Hotmail
- LogMeIn
- Paypal
- Twitter



Web site template list





5.3 Contact



Description

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

Settings

You can choose between 6 different types of contacts

	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.

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

General
More
Information
Sub Connections
Attachments
Logs
Advanced

General

First name
Last name

Middle name
Prefix

Gender
Unspecified
Job title

Company
Email

Address
Home phone

City
Work phone

State
Cell

Zip code
Fax

Country
Skype

Website


Group/folder
Demo
Image

Display
Embedded (tabbed)
Security group
<None>


Customer #

Contact entry

View Map

Enter a complete address for a contact and the  button will show you his location in Google Maps.

Email Contact

Enter a email address for a contact and click the  button to send him directly a email.

Call (Skype)

Enter Skype username for a contact and click  button to contact him via Skype directly.

Website

Enter a website for a contact and click  button to open the contact website.

5.4 Documents

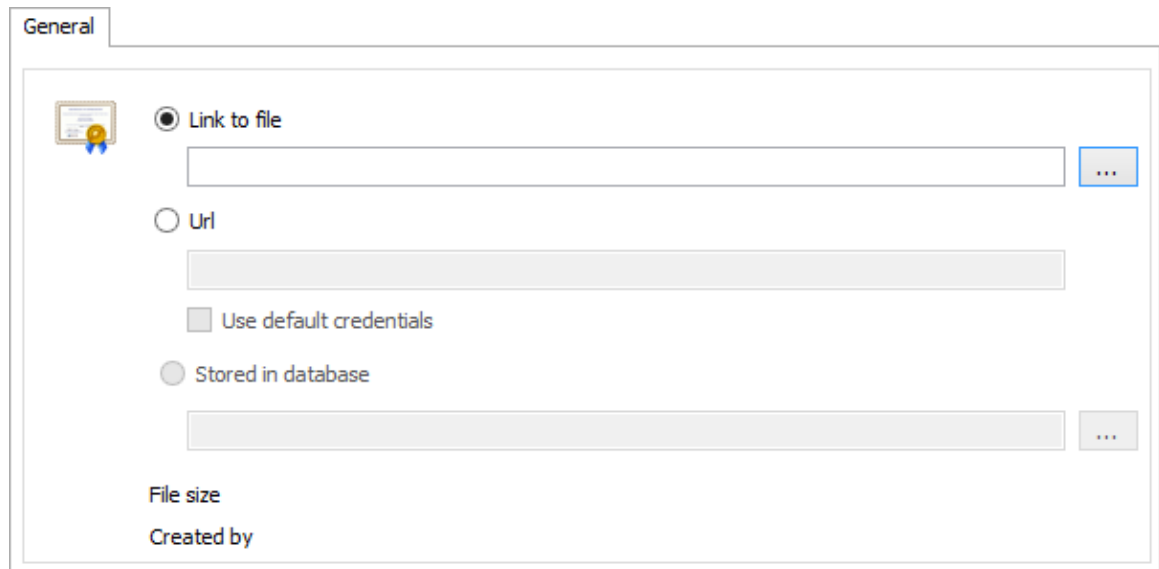
5.4.1 Certificate

Description



This entry is used to define and configure a 'Certificate' document entry.

Settings



The image shows a 'General' tab in a settings dialog for a 'Certificate' document type. It features three radio buttons: 'Link to file' (selected), 'Url', and 'Stored in database'. The 'Link to file' option has a text input field and a blue button with three dots. The 'Url' option has a text input field. The 'Stored in database' option has a text input field and a grey button with three dots. There is also a checkbox for 'Use default credentials'. At the bottom, there are labels for 'File size' and 'Created by'.

Certificate document type

Link to file

Links to a file located on your PC or on your network.

Url

Open a file using a URL. You can also use your default Windows Credentials to open the file.

Stored in database

Select a file that will be stored in the database. Some data sources do not support this mode.



If you update a document this will also save the new filename.

5.4.2 Default

Description



This entry is used to define and configure a 'Default' document entry. Use this type whenever Remote Desktop Manager does not support specific support for your file type.

Settings

General

☒ Link to file
 ...

☐ Url

☐ Use default credentials

☐ Stored in database
 ...

File size

Created by

Default document type

Link to file

Links to a file located on your PC or on your network.

Url

Open a file using a URL. You can also use your default Windows Credentials to open the file.

Stored in database

Select a file that will be stored in the database. Some data sources do not support this mode.



If you update a document this will also save the new filename.

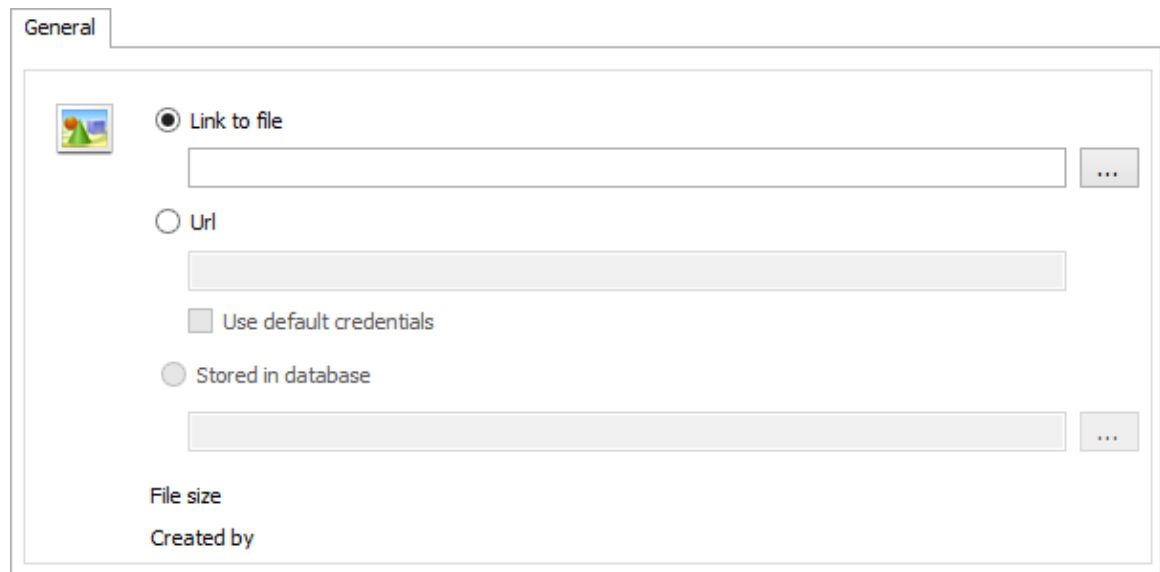
5.4.3 Image

Description




This entry is used to define and configure a 'Image' document entry. Image entry support the embedded mode.

Settings



General

 ☒ Link to file

☐ Use default credentials

☐ Stored in database

File size

Created by

Image document type

Link to file

Links to a file located on your PC or on your network.

Url

Open a file using a URL. You can also use your default Windows Credentials to open the file.

Stored in database

Select a file that will be stored in the database. Some data sources do not support this mode.



If you update a document this will also save the new filename.

5.4.4 Microsoft Office (Word, Excel, PowerPoint, Visio and OneNote)

Description



This entry is used to define and configure a 'Microsoft Office' document entry. Word, Excel and PowerPoint support the embedded mode when both Remote Desktop Manager and MS Office are running using the 32 bit architecture.

Microsoft Office document types

- Word
- Excel
- PowerPoint

- Visio
- OneNote'

Settings

Microsoft Office document type

Link to file

Links to a file located on your PC or on your network.

Url

Open a file using a URL. You can also use your default Windows Credentials to open the file.

Stored in database

Select a file that will be stored in the database. Some data sources do not support this mode.



If you update a document this will also save the new filename.

5.4.5 PDF

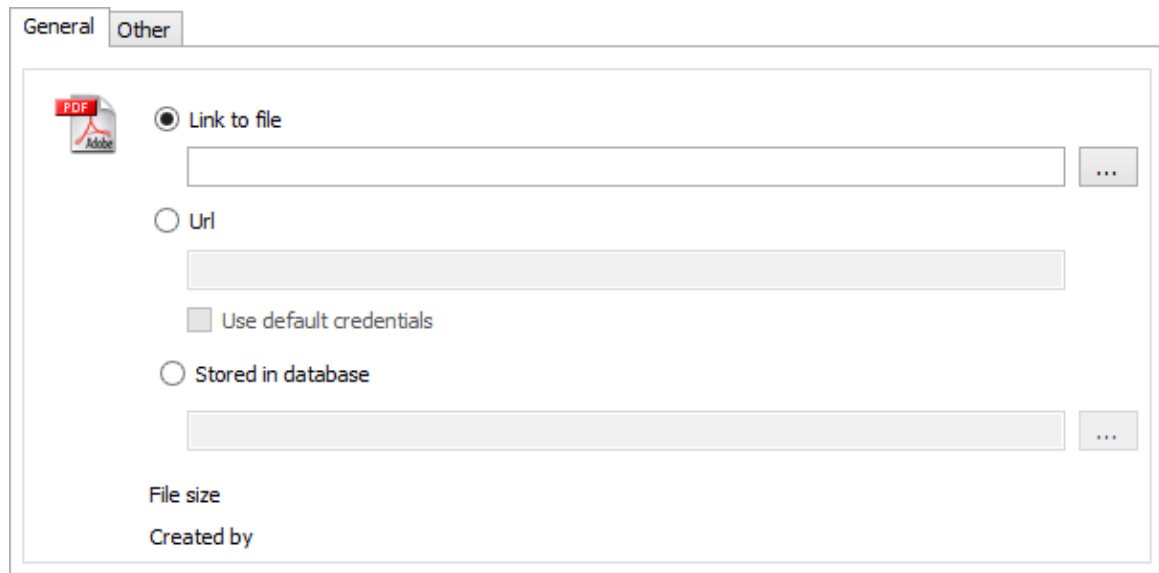
Description



This entry is used to define and configure a 'PDF' document entry. PDF entries support the embedded mode.

Settings

General



PDF General tab

Link to file

Links to a file located on your PC or on your network.

Url

Open a file using a URL. You can also use your default Windows Credentials to open the file.

Stored in database

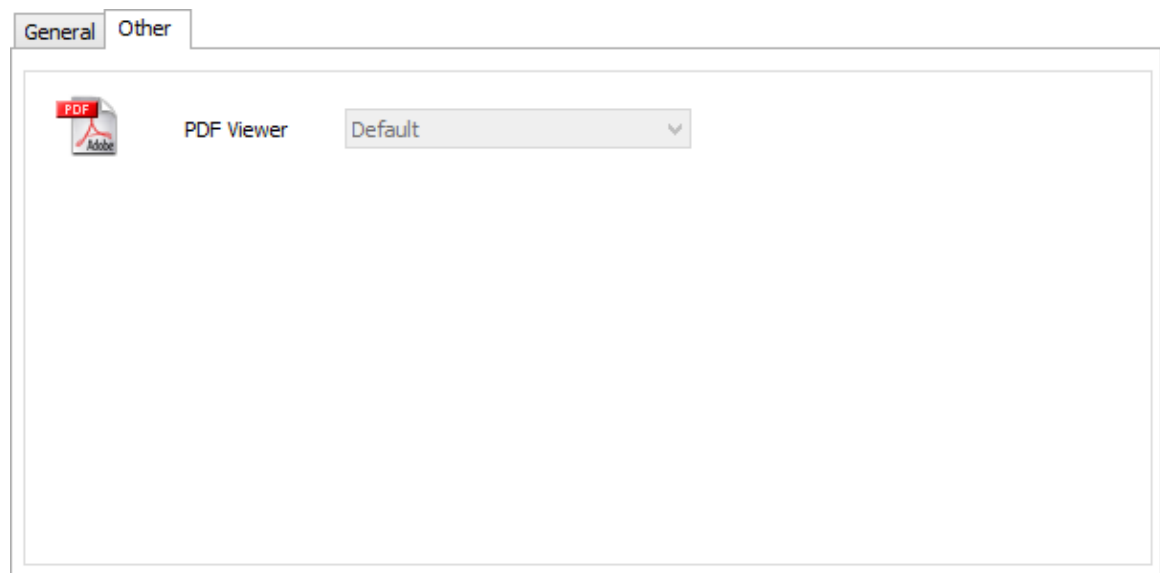
Select a file that will be stored in the database. Some data sources do not support this mode.



If you update a document this will also save the new filename.

Other

Allows you to choose the PDF Viewer you want to use.



PDF Other tab

Supported PDF Viewer

- Acrobat Reader
- PDF-XChange Viewer
- PDF-XChange Viewer Pro

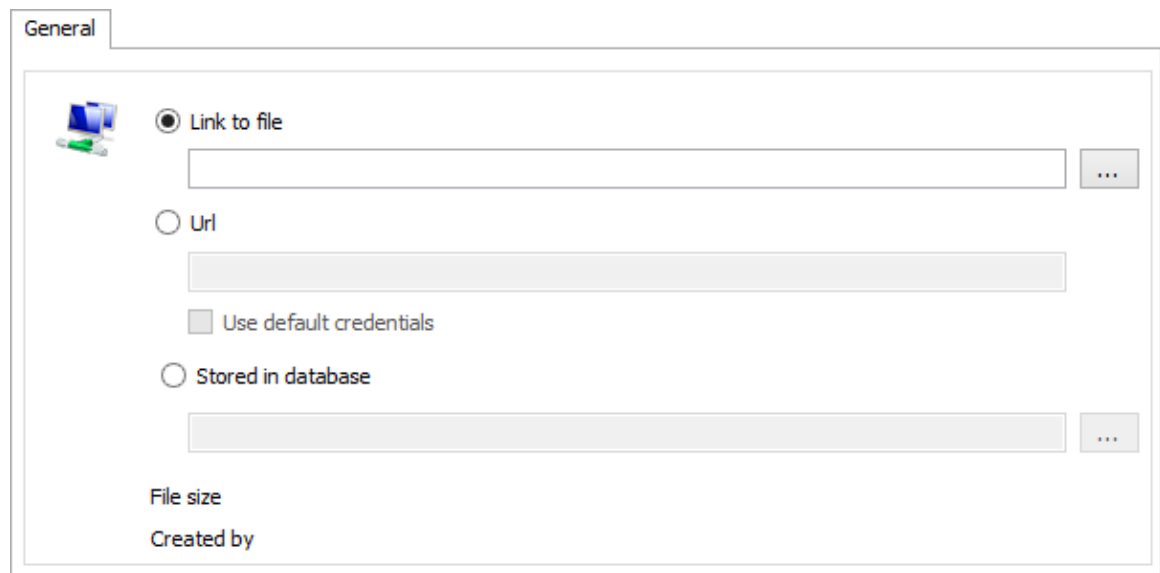
5.4.6 Phonebook

Description



This entry is used to define and configure a 'Phonebook' document entry. It can be used for a VPN configuration.

Settings



Phonebook document type

Link to file

Links to a file located on your PC or on your network.

Url

Open a file using a URL. You can also use your default Windows Credentials to open the file.

Stored in database

Select a file that will be stored in the database. Some data sources do not support this mode.



If you update a document this will also save the new filename.

VPN with Phonebook

For more information on VPNs, refer to the [VPN Overview](#) topic.

5.4.7 Text

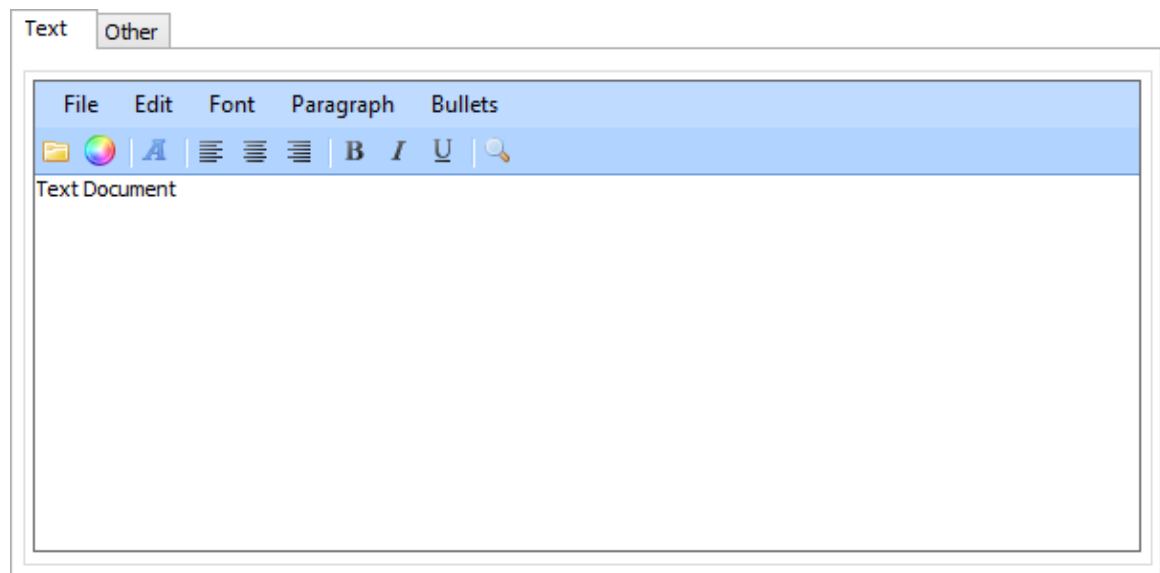
Description



This entry is used to define and configure a 'Text' document entry. We support the Rich Text format (RTF).

Settings

To configure a Text entry, you just need to type your text in the blank section.



Text document type

Preview text in description

Check this box if you want to display your text in the description field before opening your text file.

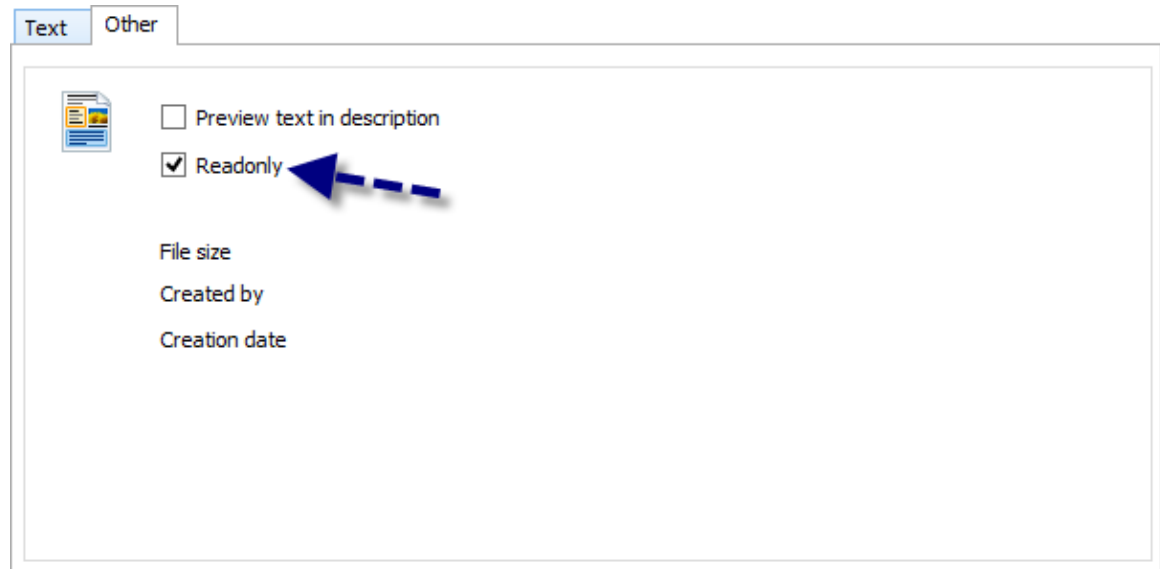


Preview text in description



Description Field***Read Only***

Check this box if you want to disallow the permission to edit your entry.



The screenshot shows a dialog box with two tabs: 'Text' and 'Other'. The 'Text' tab is active. Inside the dialog, there is a document icon on the left. To its right, there are two checkboxes: 'Preview text in description' (unchecked) and 'Readonly' (checked). A blue dashed arrow points to the 'Readonly' checkbox. Below these checkboxes, there are three labels: 'File size', 'Created by', and 'Creation date'.

Read Only

5.5 Groups

5.5.1 Overview

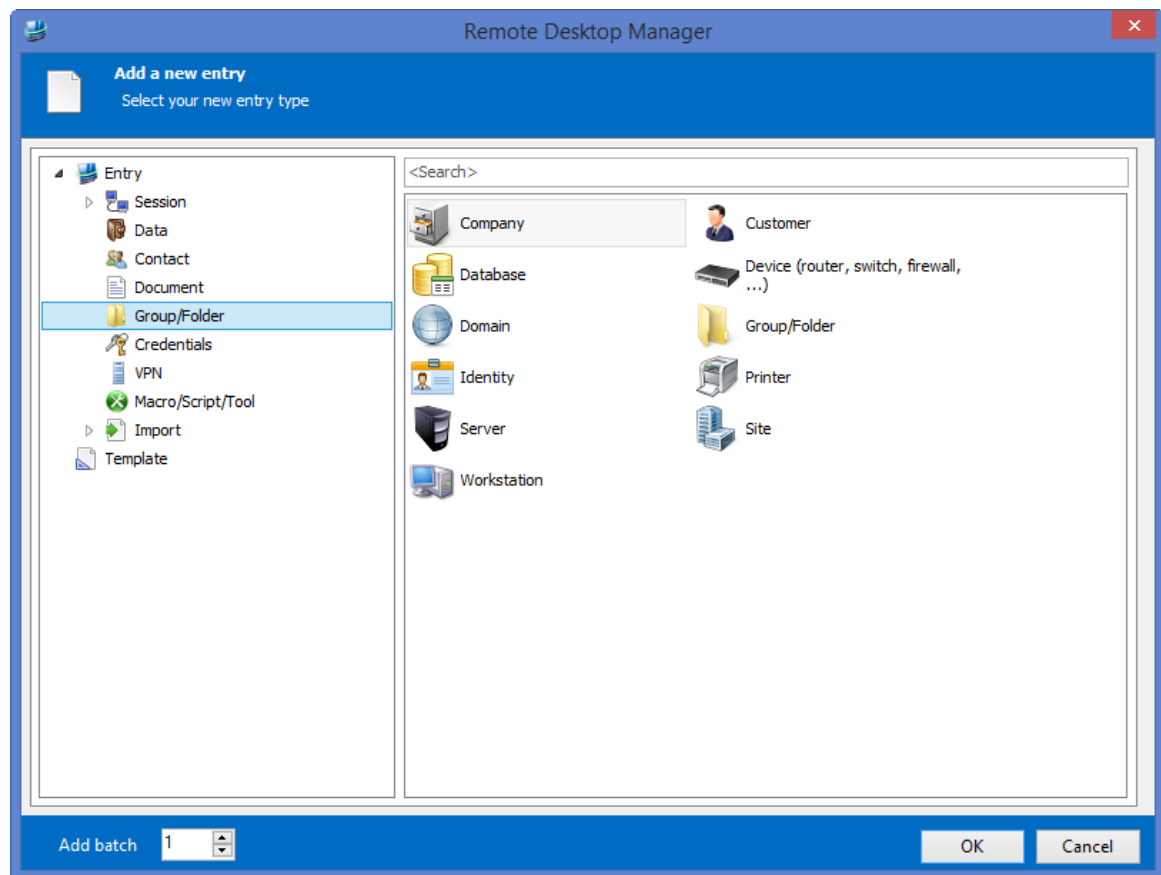
Description

Groups or folders are used to organize your entries in a logical way. It's possible to create an extensive hierarchy groups and sub groups, which Remote Desktop Manager will automatically sort alphabetically.

Groups can be created in two different ways:

- Via the session properties
- From the session tree view

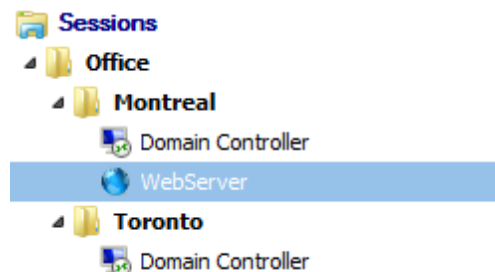
You can assign a group type to simplify the organization or use variables (refer to the [Variables](#) topic for more info):



Group types

Creating Groups via the Entry Settings

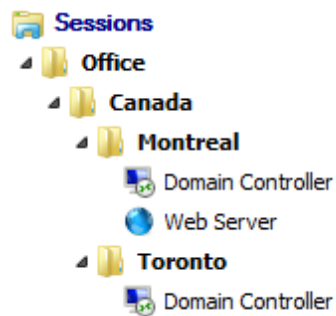
Groups can be specified in the session properties. Simply fill this field with your desired group name, and Remote Desktop Manager will generate the corresponding tree structure. Use the backslash (\) to create a sub group.



Basic group structure

For example, "Office\Canada\Montreal" will create three nodes in the tree:

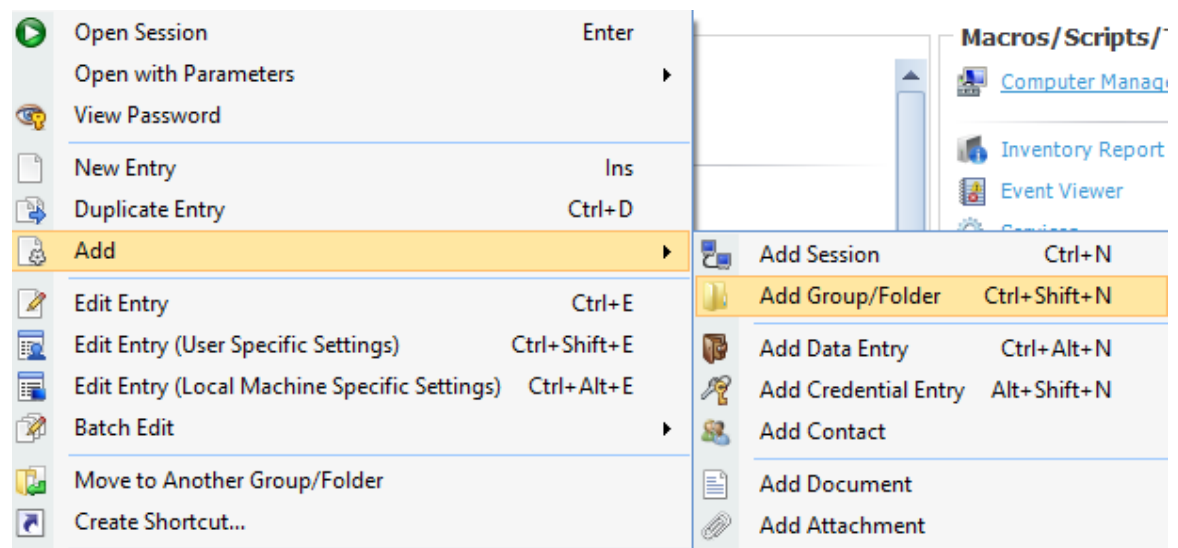
- Office
- Canada
- Montreal



Modified group structure with a new node

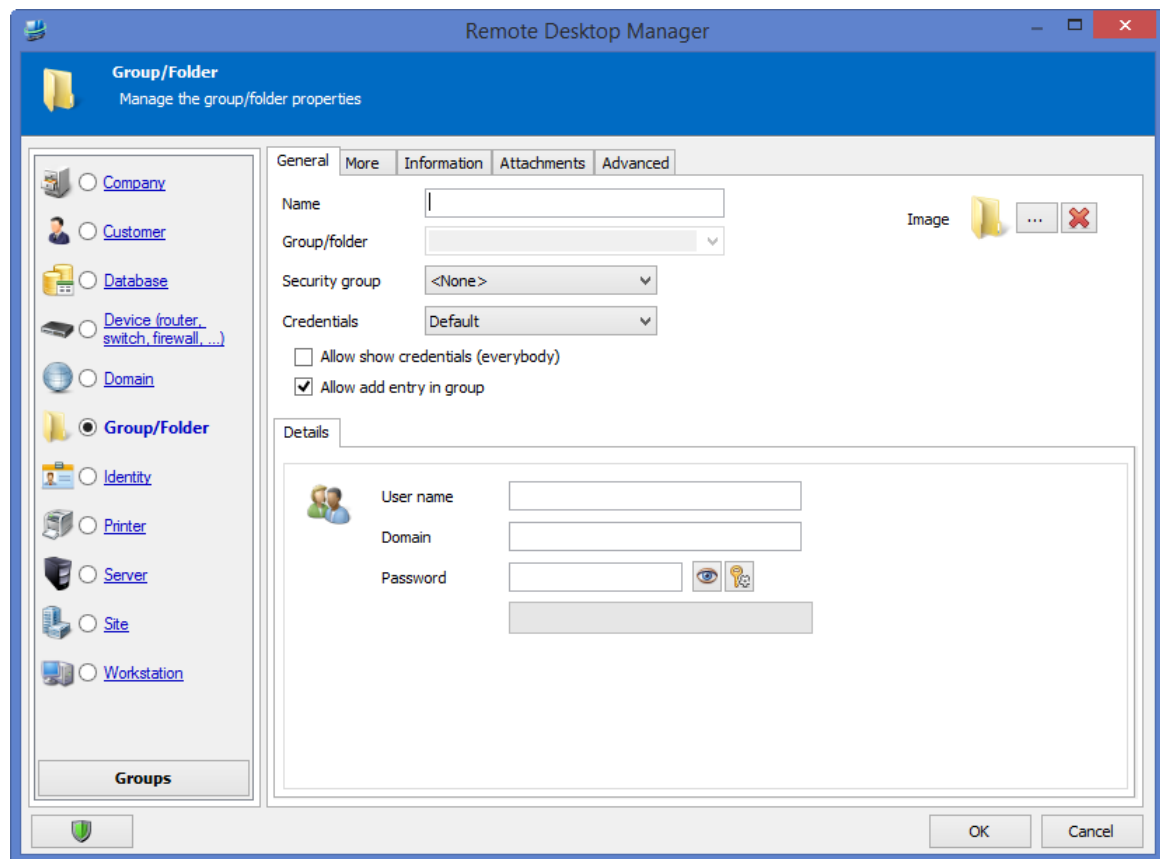
Creating Groups from the Tree View

By right clicking the root node of a group or an existing session, a context menu appears allowing you to create a new group.



Add group from the session context menu

The "Add Group" dialog box will then prompt you to enter the name of the group, and choose its parent group.

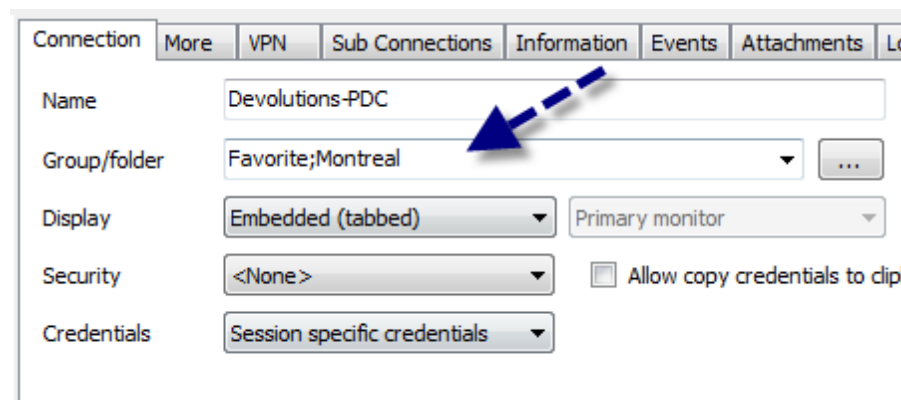


Group edition dialog

Once a group is created, you can add a session by using the menu, or by dragging its node directly to the content of the group.

Multiple Groups

Add a entry 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.



Group/Folder Example

Shortcuts

To access your folder rapidly, you can create shortcuts on them. Please refer you to the [Creating Shortcuts](#) topic.

5.5.2 Types

5.5.2.1 Company

Description





This entry is used to organize a 'Company' group.

Settings

Details

User name

Domain

Password  

Company group tab

Enter the user name, domain and password.

If you wish for children entries to inherit them, you need to specify the ***inherited*** credentials setting in the session.



To access field from this group entry, you should use \$COMPANY_ variables.
For more information, please consult the [Variables](#) topic.

5.5.2.2 Customer


Description



This entry is used to organize a 'Customer' group. Customer represent your client.



Settings

Details



User name

Domain

Password  

Customer group tab

Enter the user name, domain and password.

If you wish for children entries to inherit them, you need to specify the ***inherited*** credentials setting in the session.



To access field from this group entry, you should use \$CUSTOMER_ variables. For more information, please consult the [Variables](#) topic.

5.5.2.3 Database


Description





This entry is used to organize a 'Database' group. The Database group provides a subset of the functionality offered by the Database session. See [Database](#) session for more information.

Settings

General


 Data source

Data provider

Connection string  

Host

User name

Password 

Database group tab

Enter the connection information if you wish the child entries to inherit from it. Press the ellipsis button to be able to select the data source and data provider. This will generate the connection string with the information you enter in the dialog.



To access field from this group entry, you should use \$DB_ variables.
For more information, please consult the [Variables](#) topic.

5.5.2.4 Device



Description




This entry is used to organize a 'Device' group. A device group can be used for any types of devices such as a router, a switch or a firewall as example.

Settings



Details

 Computer 

IP

 User name

Domain

Password  

Device group tab

Use the ellipsis button to select from a list of discoverable computers or enter the name or IP address manually.

Enter the user name, domain and password.

If you wish for children entries to inherit them, you need to specify the *inherited* credentials setting in the session.



To access field from this group entry, you should use \$COMPUTER_ variables. For more information, please consult the [Variables](#) topic.

5.5.2.5 Domain

Description



This entry is used to organize a 'Domain' group.

Settings

Details

 Domain

Domain Group Tab

Enter the domain name.



To access field from this group entry, you should use \$DOMAIN_ variables. For more information, please consult the [Variables](#) topic.

5.5.2.6 Group/Folder



Description



This entry is used to organize the entries in a folder structure.

Settings

Details

	User name	<input type="text"/>
	Domain	<input type="text"/>
	Password	<input type="password"/>  
		<input type="text"/>

Group/Folder group tab

Enter the user name, domain and password for credentials that you wish to associate with that group.

If you wish for children entries to use the specified credentials, you need to set the *Credentials* setting to ***inherited*** in the session.



No variables can grant access to fields of this entry for this group type.

5.5.2.7 Identity


Description



This entry is used to organize a 'Identity' group. Identity group is like a customer account that a customer gave you to access a certain session.



Settings

Details



User name

Domain

Password  

Identity group tab

Enter the user name, domain and password.

If you wish for children entries to inherit them, you need to specify the ***inherited*** credentials setting in the session.



To access field from this group entry, you should use \$IDENTITY_ variables.
For more information, please consult the [Variables](#) topic.

5.5.2.8 Printer


Description




This entry is used to organize a 'Printer' group.

Settings

Details





Computer 

IP



User name

Domain

Password  

Device group tab

Use the ellipsis button to select from a list of discoverable computers or enter the name or IP address manually.

Enter the user name, domain and password.

If you wish for children entries to inherit them, you need to specify the ***inherited*** credentials setting in the session.




To access field from this group entry, you should use \$COMPUTER_ variables. For more information, please consult the [Variables](#) topic.


5.5.2.9 Server**Description**

This entry is used to organize a 'Server' group.


Settings

Details

**Computer**





IP

**User name**

Domain

Password



Server group tab

Use the ellipsis button to select from a list of discoverable computers or enter the name or IP address manually.

Enter the user name, domain and password.

If you wish for children entries to inherit them, you need to specify the ***inherited*** credentials setting in the session.



To access field from this group entry, you should use \$COMPUTER_ variables. For more information, please consult the [Variables](#) topic.

5.5.2.10 Site




Description



This entry is used to organize a 'Site' group. Site can be used to specify a building, floor or department.

Settings

Details

	User name	<input type="text"/>
	Domain	<input type="text"/>
	Password	<input type="password"/>  
<input type="button" value="OK"/>		

Site group tab

Enter the user name, domain and password.

If you wish for children entries to inherit them, you need to specify the ***inherited*** credentials setting in the session.



To access field from this group entry, you should use \$SITE_ variables.
For more information, please consult the [Variables](#) topic.

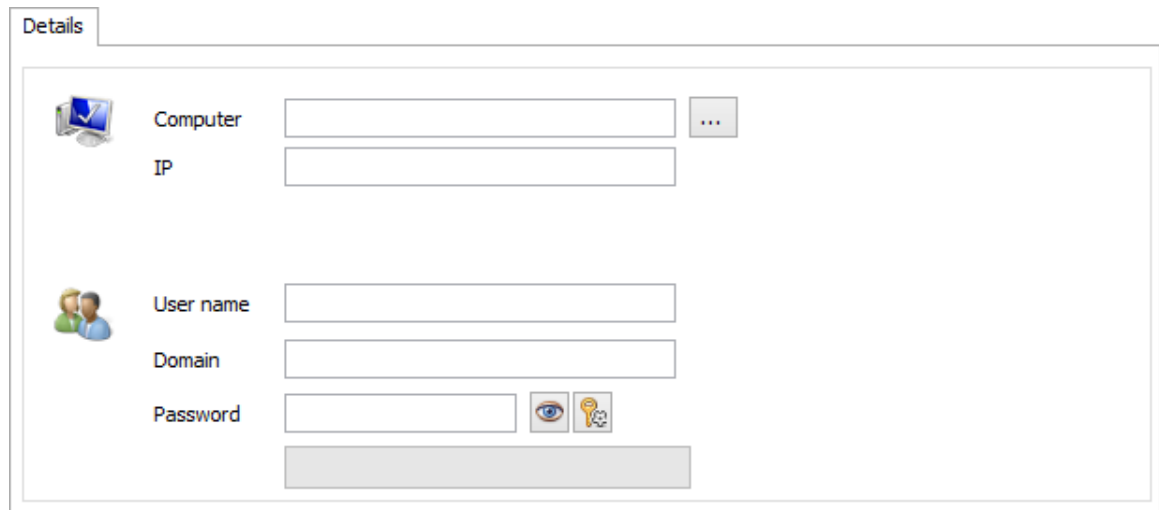
5.5.2.11 Workstation

Description



This entry is used to organize a 'Workstation' group.

Settings



The screenshot shows the 'Details' tab of the Remote Desktop Manager interface. It contains several input fields for configuring a remote session:

- Computer:** A text field with a computer icon to its left and an ellipsis button to its right.
- IP:** A text field located below the Computer field.
- User name:** A text field with a user icon to its left.
- Domain:** A text field located below the User name field.
- Password:** A text field with a key icon to its right. Below the password field is a grey rectangular button.

Workstation group tab

Use the ellipsis button to select from a list of discoverable computers or enter the name or IP address manually.

Enter the user name, domain and password.

If you wish for children entries to inherit them, you need to specify the ***inherited*** credentials setting in the session.



To access field from this group entry, you should use \$COMPUTER_ variables. For more information, please consult the [Variables](#) topic.

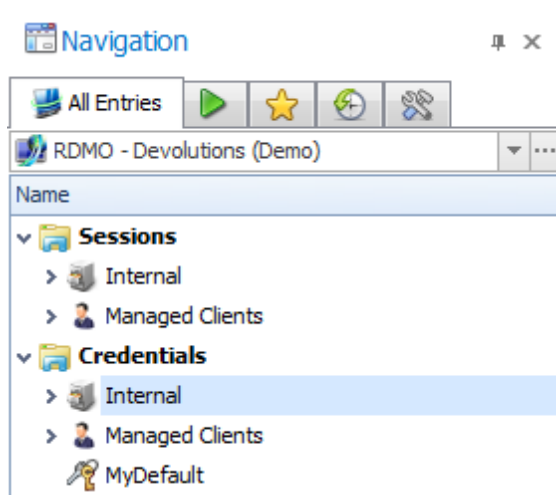
5.6 Credentials

5.6.1 Overview

Description

The credential repository is available in the Enterprise edition and allows you to set multiple sessions to use a specific set of credentials. This simplifies management by allowing you to maintain a single entry.

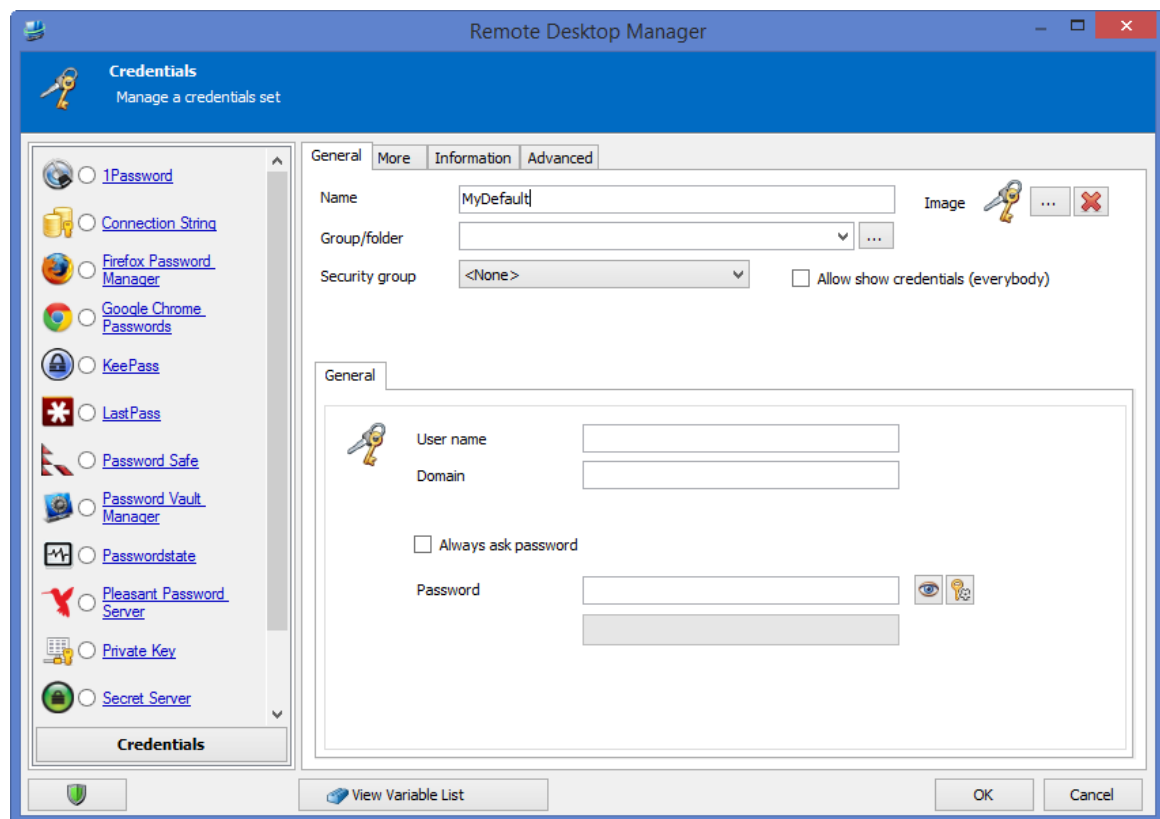
The ***Credentials*** branch is visible in the tree view under the session list by default (if the ***merge credentials with sessions*** option is not enabled).



Credentials node from the tree view

Currently, the credential repository is available for the **Sessions** and **VPN** entry types. You can configure it to prompt you to select a set of credentials, which allows you to use multiple credentials for the same host.

To create a credential entry, use the session's context menu and select **Add -> Add Credential Entry**.



Credential Entry dialog

There are multiple types of credentials, some of which require an external application. See the next section for more details.

5.6.2 Dynamic Credential Linking

Description

You can create a single credential entry for each external system below and use this credential in any entry type.

External Credentials System

- [1Password](#)
- [KeePass](#)
- [LastPass](#)
- [Password Safe](#)
- [PasswordState](#)
- [Secret Server](#)
- [Password Vault Manager](#)

1. Create a credential entry and check "Always prompt with list"

General

Logon settings

Mode ☒ Integrated ☐ Credential redirection

Integrated

Database ...

Password ☐ Always prompt for password

☒ Always prompt with list

Title ...

Uuid Check

1Password settings

2. In a session definition, you must choose "Credential Repository" and then your credential entry created in the previous step. Notice that a new action appears just below the credential selection drop down.

Connection More VPN Information Events Sub Connections Attachments Logs Tools Advanced

Name: Devolutions-PDC

Group/folder:

Display: External Primary monitor

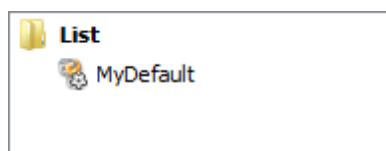
Security: <None> ☐ Allow show credentials (everybody)

Credentials: Credential repository Internal\MyDefault

[Select from list](#)

Select from list

3. Select a credential in our standard dialog box



Credential Selection Dialog box

4. The link will change to the name of the credential

Connection More VPN Information Events Sub Connections Attachments Logs Tools Advanced

Name: dc1

Group/folder: Managed Clients\Downhill pro

Display: External Primary monitor

Security: <None> ☐ Allow show credentials (everybody)

Credentials: Credential repository MyDefault

MyDefault

Name of the credential

5.6.3 Types

5.6.3.1 Credential Redirection

Description

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

In order to be able to leave all credentials in your platform of choice, and yet be able to use Remote Desktop Manager for your day to day operations, we've implemented a mechanism to request the credentials from your chosen credential repository, then redirect them to the resource you want to connect to.

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 will act to

redirect the credentials from your chosen repository to the remote resource.

Pre-requisites

- Your tool of choice must be installed and work properly with the related browser 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 sections. First you create the credential entry in your repository, second you use a link to these credentials in a Remote Desktop Manager entry, and last you launch the session and use your provider to fill in the credentials.

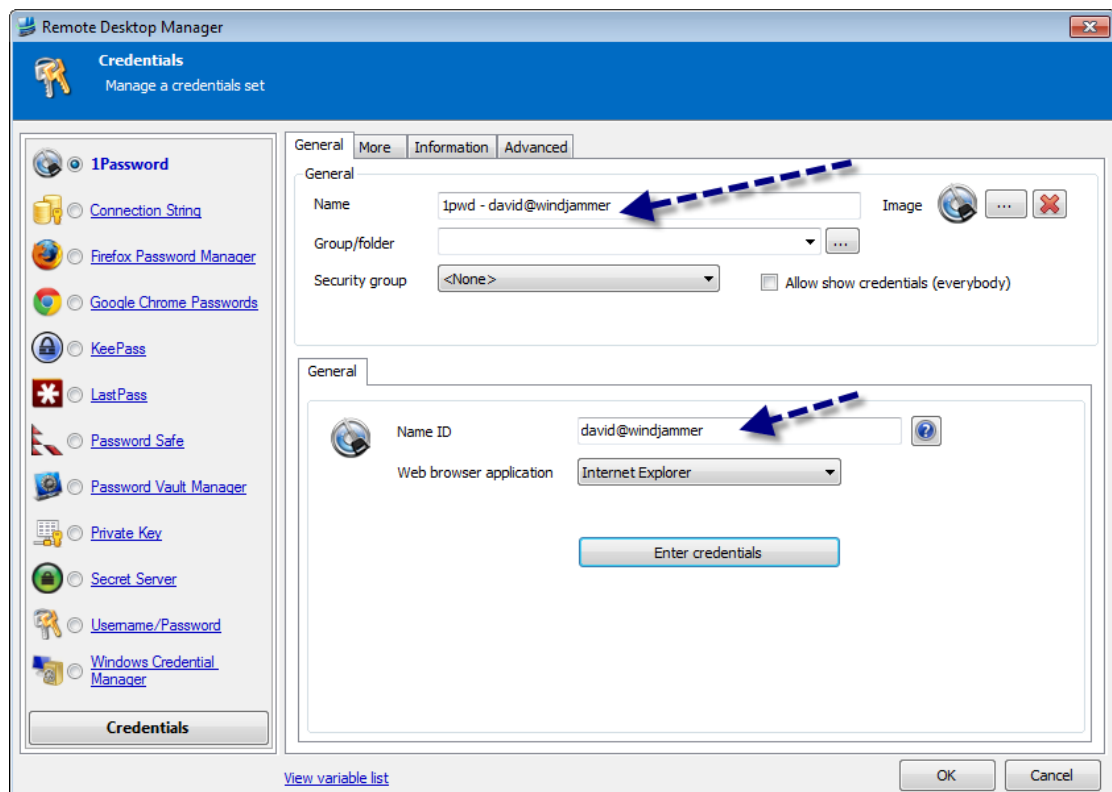
We will use 1Password in our example, but the steps are the same for Lastpass.



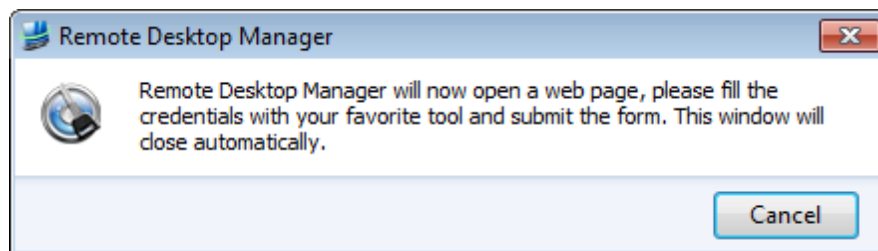
Your chosen tool may require to be unlocked once or multiple times depending on your configuration. These steps are not covered by this guide as it may change for each installation.

Creating the credential entry

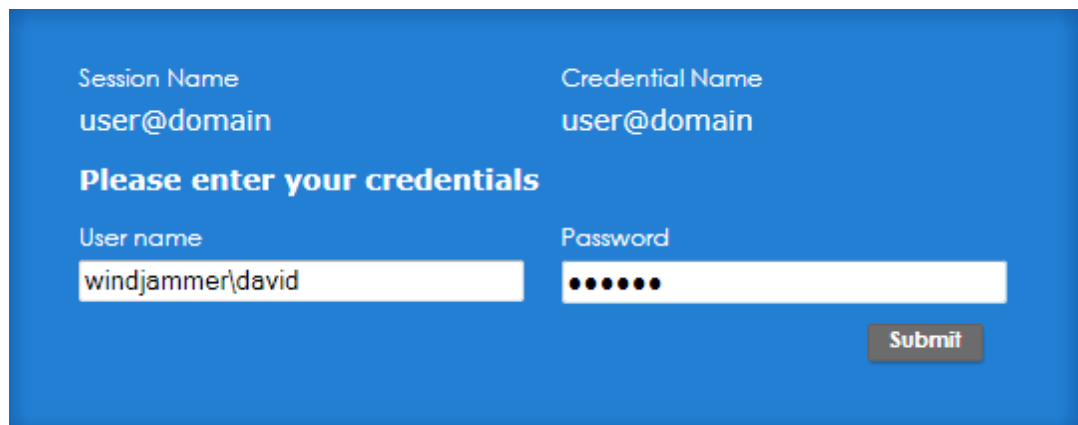
- Create a new entry of the *1Password (Credentials)* type.
- Give it a name.
- Enter a label in the *Name ID* field. This must be unique within your 1Password repository. It will be used to identify the credentials and will be exposed as a subdirectory of the URL used to intercept the credentials.



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



- The chosen browser is launched for a URL that looks like <http://127.0.0.1:9999/david@windjammer/login.aspx>. Notice the middle part is the *Name ID* entered previously
- Enter your credentials to save in the browser



Session Name
user@domain

Credential Name
user@domain

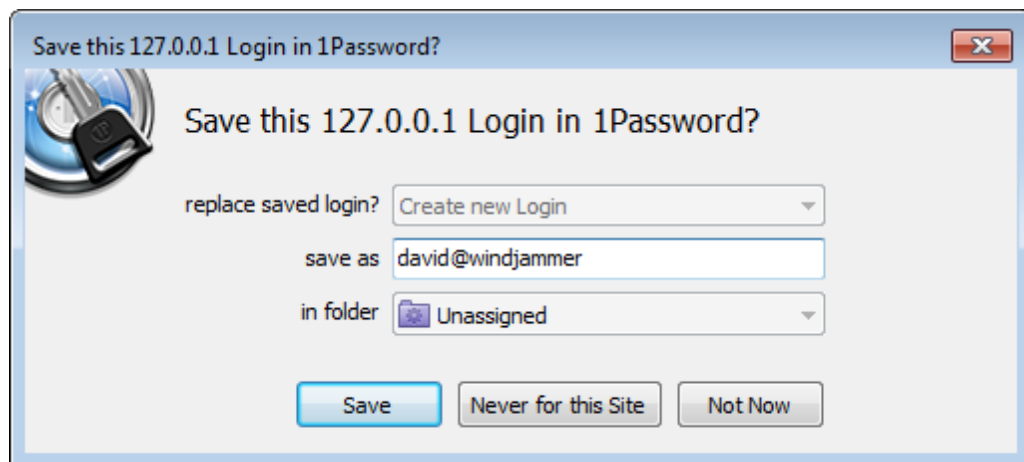
Please enter your credentials

User name
windjammer\david

Password
●●●●●●

Submit

- 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.
- In your tool Save dialog, we recommend you give it the same name as the *Name ID* you entered previously



Save this 127.0.0.1 Login in 1Password?

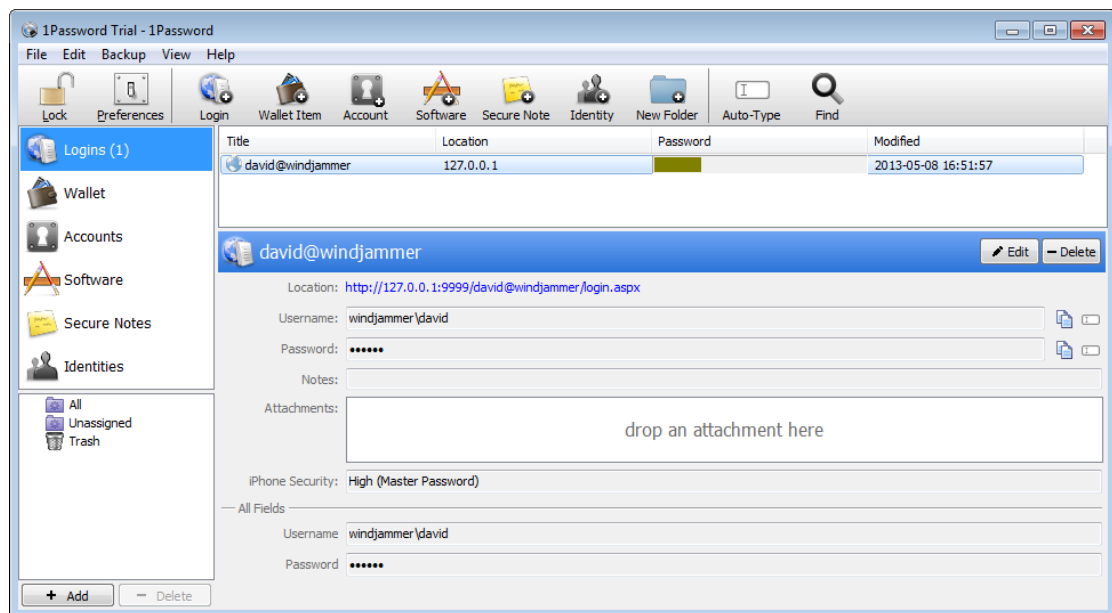
replace saved login? Create new Login

save as david@windjammer

in folder Unassigned

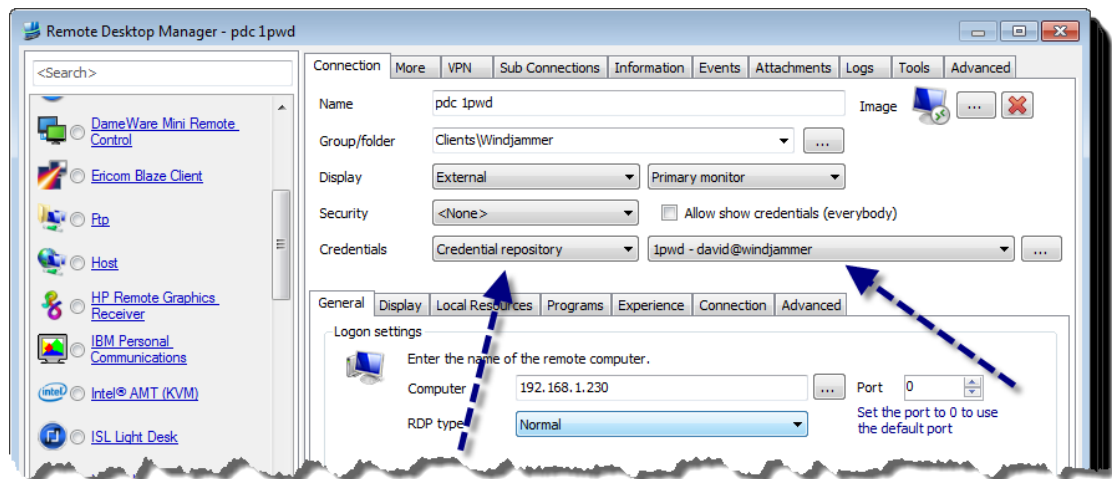
Save Never for this Site Not Now

- In the web browser, press the submit button. This will close the browser after a delay.
- In Remote Desktop Manager, save your credential entry
- Using your password provider, confirm that the credentials are saved.



Creating a session using the credential entry

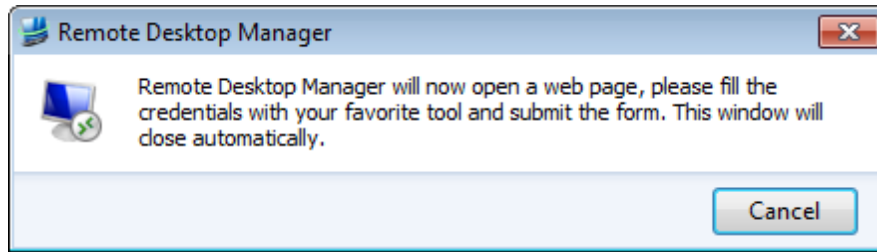
- Create a new entry, we will use a RDP session for the example.
- Give it a name
- For *Credentials*, select *Credential repository*, then your newly created credential entry



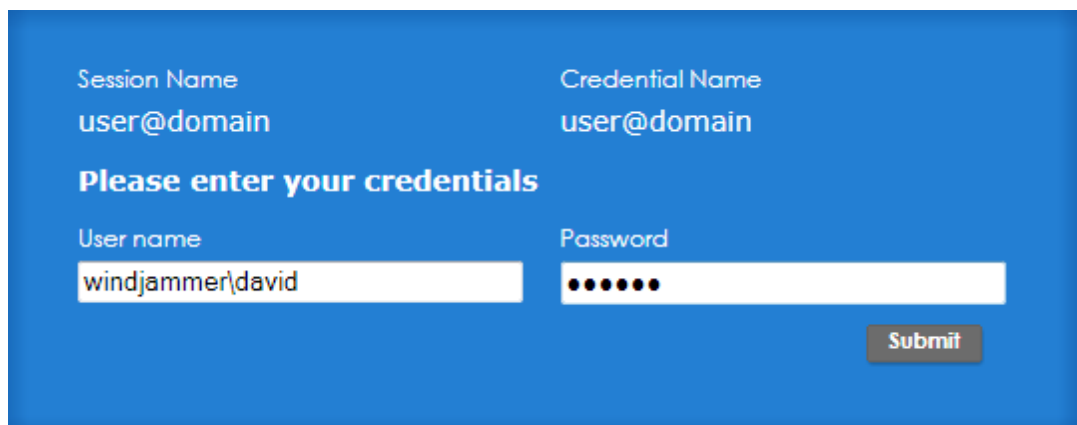
- Specify the computer name or IP
- Save your session

Using the session

- Select your session then launch it. This will initiate the following sequence of events
 - Remote Desktop Manager will display this informative dialog



- The chosen browser is launched for the URL associated to the session
- 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.



- In the web browser, press submit. The page will be closed after a delay
- The RDP session is launched and authentication is successful

See also

Lastpass downloads: https://lastpass.com/misc_download.php

1Password instructions: <http://support.agilebits.com/kb/browser-extensions/how-to-install-and-update-the-browser-extensions>

5.6.3.1.1 1Password

Description



This entry is used to define and configure a '1Password' credential entry.

Integrated Mode

The integrated mode allows you to determine which database, password and credential you want to use in your 1Password entry.

Settings

Parameters	Description
Database	Folder containing your database
Password	Password to access your database
Title	Credential selected in your database
Uuid	Universal Unique Identifier



General

Logon settings

Mode ☒ Integrated ☐ Credential redirection

Integrated

Database C:\Users\Username\Documents\1Password\1Password.agilekeychain ...

Password   ☐ Always prompt for password

☐ Always prompt with list

Title \1password ...

Uuid 4FDA52693DB0456EBD950F658D1830AE Check

Integrated Mode

Credential Redirection Mode

Please refer to [Credential Redirection](#) for full instructions.

Dynamic Credential Linking

Please refer to [Dynamic Credential](#) for more information.

5.6.3.1.2 Firefox Password Manager

Description



This entry is used to define and configure a 'Firefox Password Manager' credential entry. Use the credential from Firefox by creating an internal web server in Remote Desktop Manager to retrieve the information.

Settings

Please refer to [Credential Redirection](#) for full instructions.

5.6.3.1.3 Google Password Manager

Description



This entry is used to define and configure a 'Google Chrome Passwords' credential entry. Use the credential from Google Chrome by creating an internal web server in Remote Desktop Manager to retrieve the information.

Settings

Please refer to [Credential Redirection](#) for full instructions.

5.6.3.1.4 LastPass

Description



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



LastPass enterprise features aren't supported.

Integrated Mode


The integrated mode allows you to determine which Account name, password and credential you want to use in your LastPass entry.

Settings

Parameters	Description
Account name	LastPass account name (Email address)
Password	Password to access your database
Two factor	Choose between None, Yubikey or Google Authenticator
Title	Credential selected in your database
Uuid	Universal Unique Identifier



General


Logon settings

 Mode ☒ Integrated ☐ Credential redirection


Integrated


Account name

Password   ☐ Always prompt for password

Two factor 

☐ Always prompt with list

Title 

Uuid 

Integrated Mode

Credential Redirection Mode

Please refer to [Credential Redirection](#) for full instructions.

Dynamic Credential Linking

Please refer to [Dynamic Credential](#) for more information.

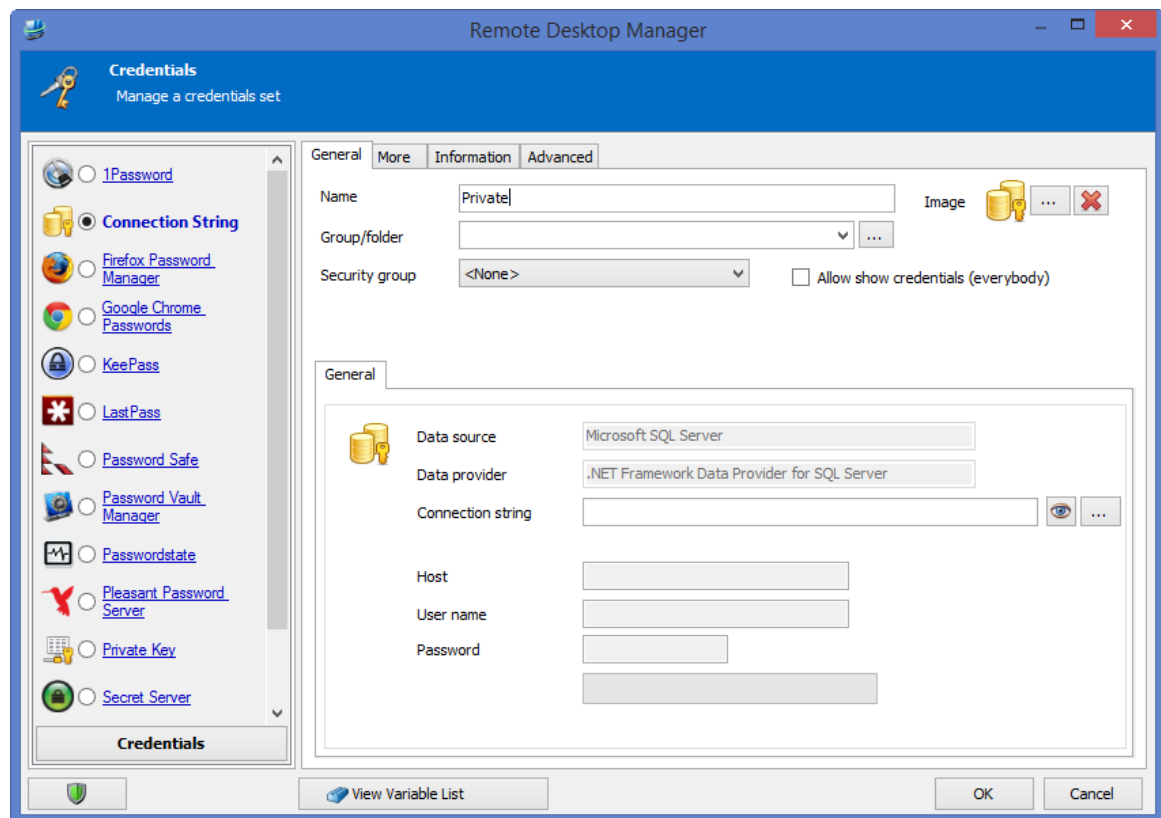
5.6.3.2 Connection String

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 Group](#) with the exception that they are not limited by the inheritance hierarchy of groups & sessions. See [Database](#) session for more information.

Settings



Connection String credential entry

5.6.3.3 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.

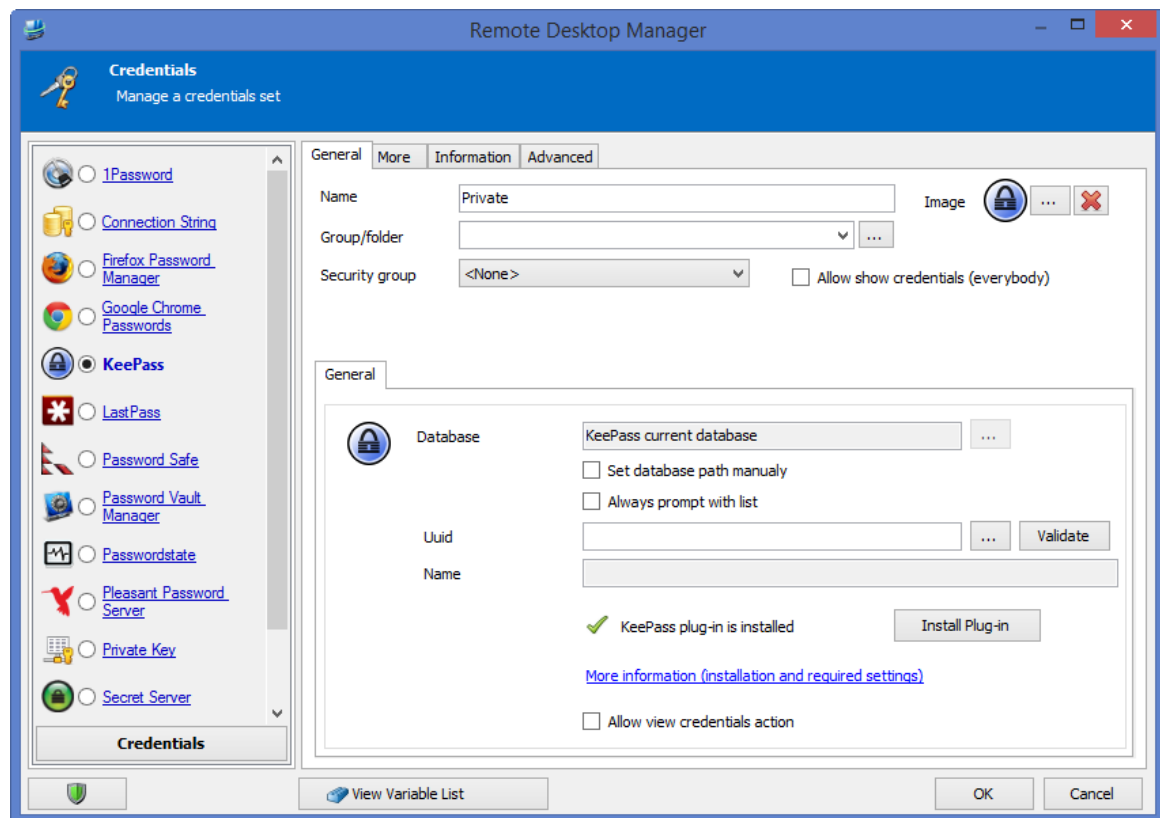


You can get find the installation instruction [here](#).



KeePass 1.X is not supported

Settings



KeePass credential entry

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

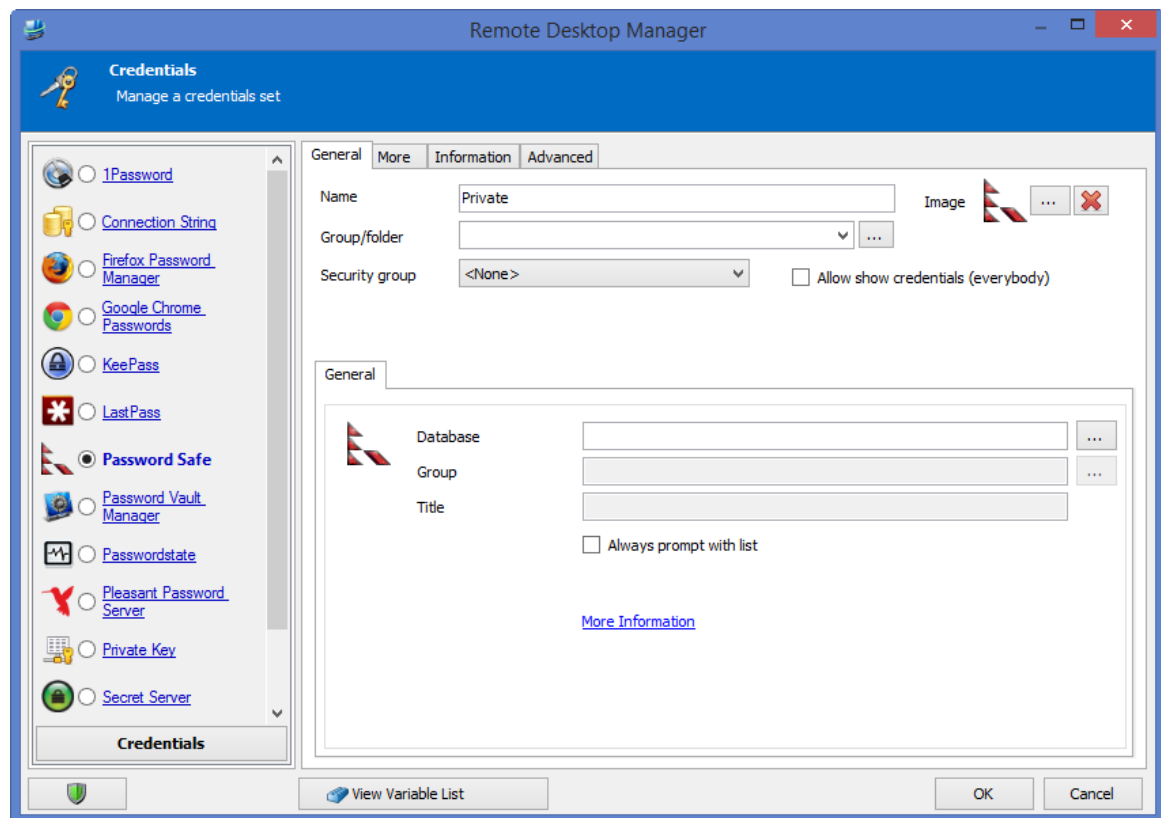
5.6.3.4 Password Safe

Description



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

Settings



Password Safe credential entry

Dynamic Credential Linking

Please refer to [Dynamic Credential](#) for more information.

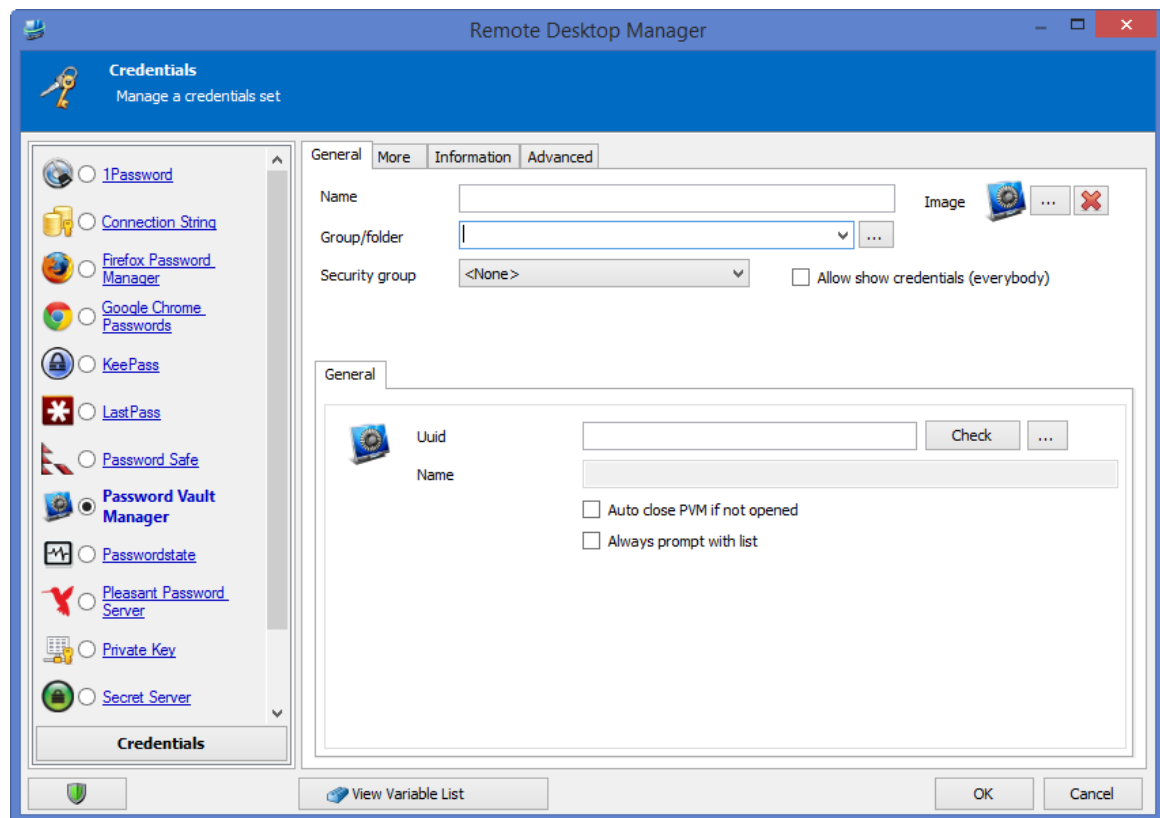
5.6.3.5 Password Vault Manager

Description



This entry is used to define and configure a 'Password Vault Manager' credential entry.

Settings



Password Vault Manager credential entry

Dynamic Credential Linking

Please refer to [Dynamic Credential](#) for more information.

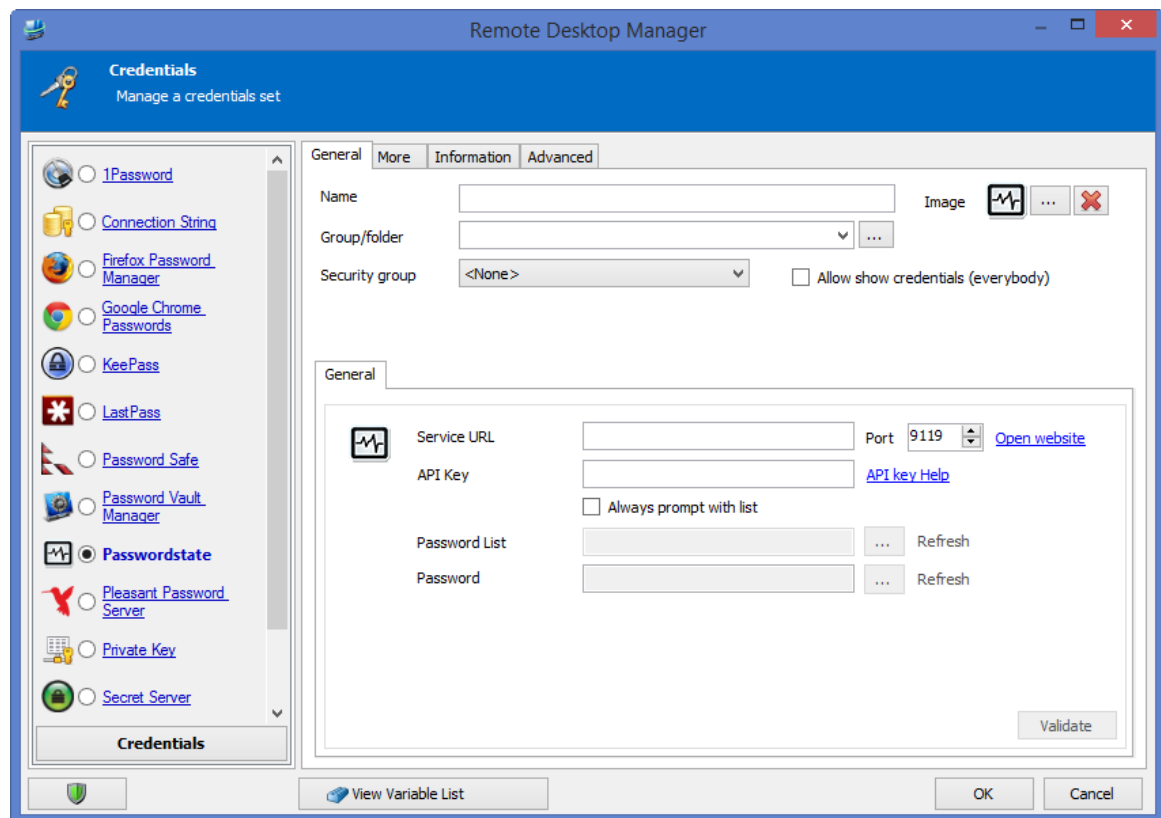
5.6.3.6 Passwordstate

Description



This entry is used to define and configure a 'Passwordstate' credential entry.

Settings



Passwordstate credential entry

Dynamic Credential Linking

Please refer to [Dynamic Credential](#) for more information.

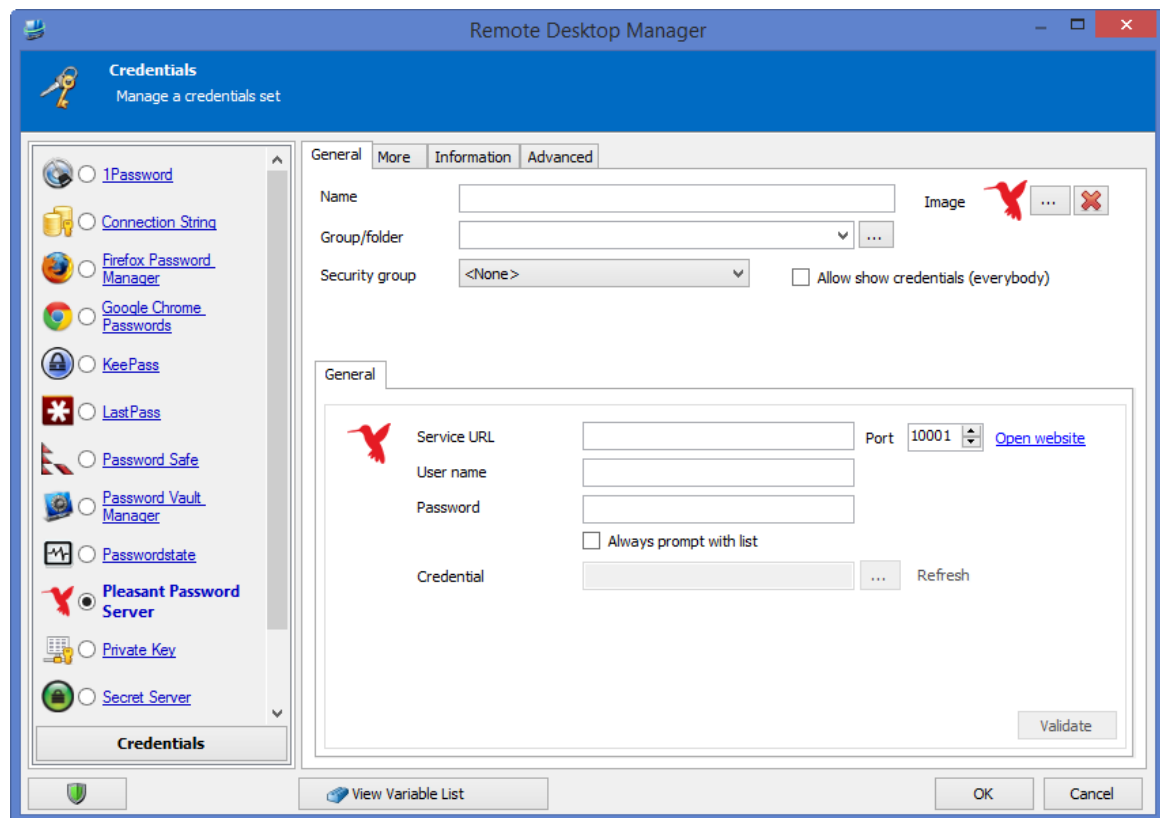
5.6.3.7 Pleasant Password Server

Description



This entry is used to define and configure a 'Pleasant Password Server' credential entry.

Settings



Pleasant Password Server credential entry

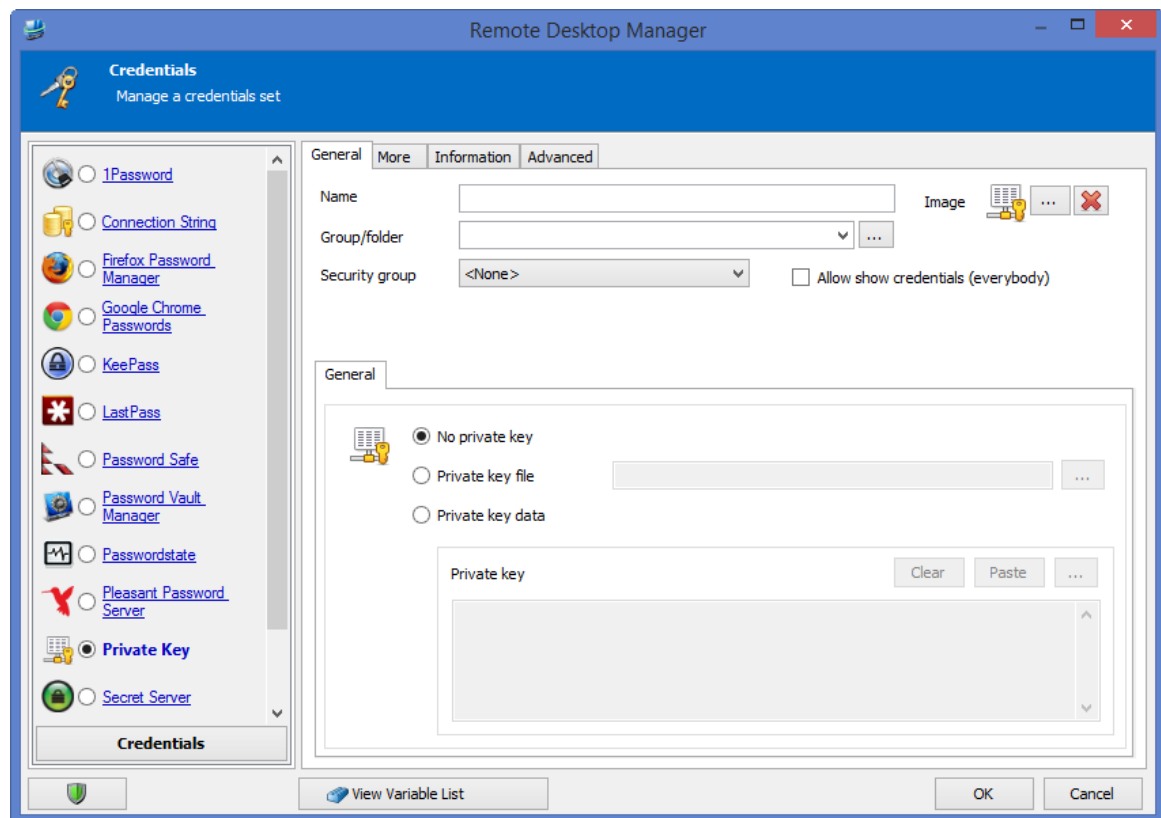
5.6.3.8 Private Key

Description



This entry is used to define and configure a 'PasswordState' credential entry.

Settings



Private Key credential entry

5.6.3.9 Secret Server

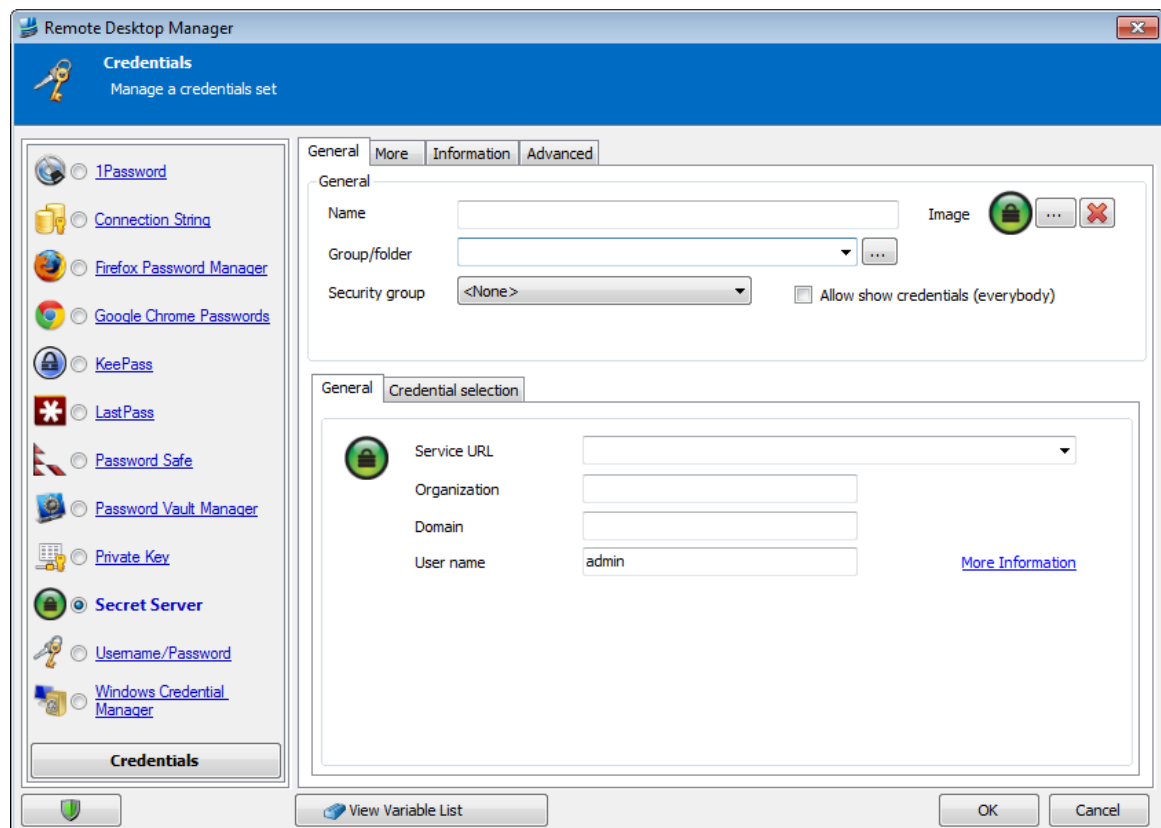
Description



This entry is used to define and configure a 'Secret Server' credential entry.

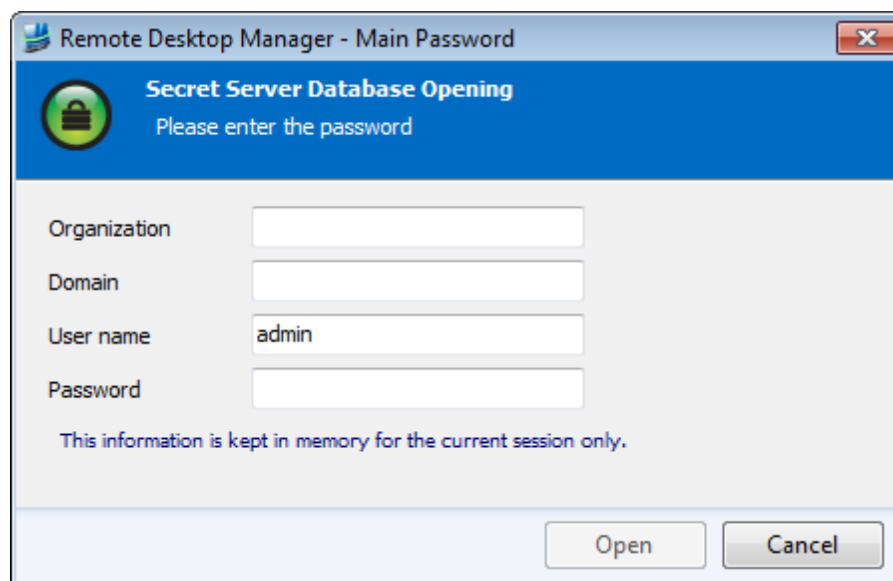


Integration with Secret Server requires its Web Services feature to be enabled. Please refer to the Secret Server documentation for details.



Authentication

As can be seen in the settings screen, there is no field to hold the password to Secret Server. When it is required to connect to Secret Server, the following dialog will appear to prompt you for the credentials





The password is cached in memory for the current session only.

Settings

General

Name	Description
Service URL	The URL of the Secret Server web services endpoint. Please see note below
Organization	Required by Secret Server when using the online edition
Domain	Required when Secret Server is configured for domain authentication.
User name	User name for Secret Server, you will be prompted for the password when it is required.

Credential Selection

General

Credential Selection

☐ Standard method

Template

Name

Test Settings

☐ By secret name method

Secret name

Variables are allowed. The first match (full or partial) is automatically chosen.

☒ Always prompt with list

Name	Description
Standard Method	Allows you to select a secret from Secret Server that will be obtained dynamically upon usage.
Template	Clicking on the ellipsis button will display a list of secrets that you have access to. This control displays the name of the template for the selected secret.
Name	Clicking on the ellipsis button will display a list of secrets that you have access to. This control displays the name of the selected secret.
Test Settings	Allows you to test if the selected secret is accessible with your credentials
By secret name method	Allows you to select the secret to use by using its name.
Secret name	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 used for your sessions.
Always prompt with list	Will prompt you with the secret list upon every use.

Notes

Secret Server Service URL

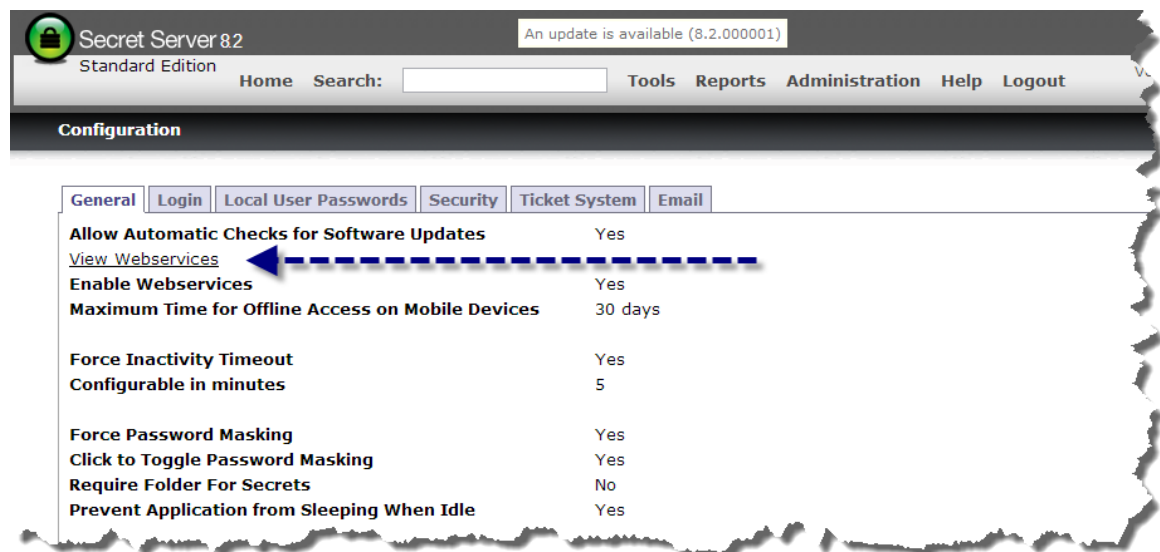


Secret server supports Windows Authentication depending on the version being used and the web server that hosts the application. The Service URL in that case would use the following form: <Secret Server URL>/winauthwebservice/sswinauthwebservice.asmx, please refer to the documentation of your edition of Secret Server to see if it is supported, 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

Here is a procedure to obtain the proper service URL

1. Log on the Secret Server web site of your local installation
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



Secret Server General Configuration tab

Username

Variables are supported in the user name 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.

5.6.3.10 Username/Password

Description



This entry is used to define and configure a 'Username/Password' credential entry. Provide the username, domain and password to save the credential. This is the default credential type.

Settings

The screenshot shows the 'Remote Desktop Manager' window with the 'Credentials' tab selected. The left sidebar lists various credential types, with 'Username / Password' highlighted. The main area shows the configuration for this type. The 'General' tab is active, displaying fields for 'Name', 'Group/folder', and 'Security group'. Below these, there is a section for 'User name', 'Domain', and 'Password'. The 'Always ask password' checkbox is unchecked. The 'Image' field shows a key icon. The 'Allow show credentials (everybody)' checkbox is also unchecked. The 'View Variable List' button is at the bottom left, and 'OK' and 'Cancel' buttons are at the bottom right.

Username/Password credential entry

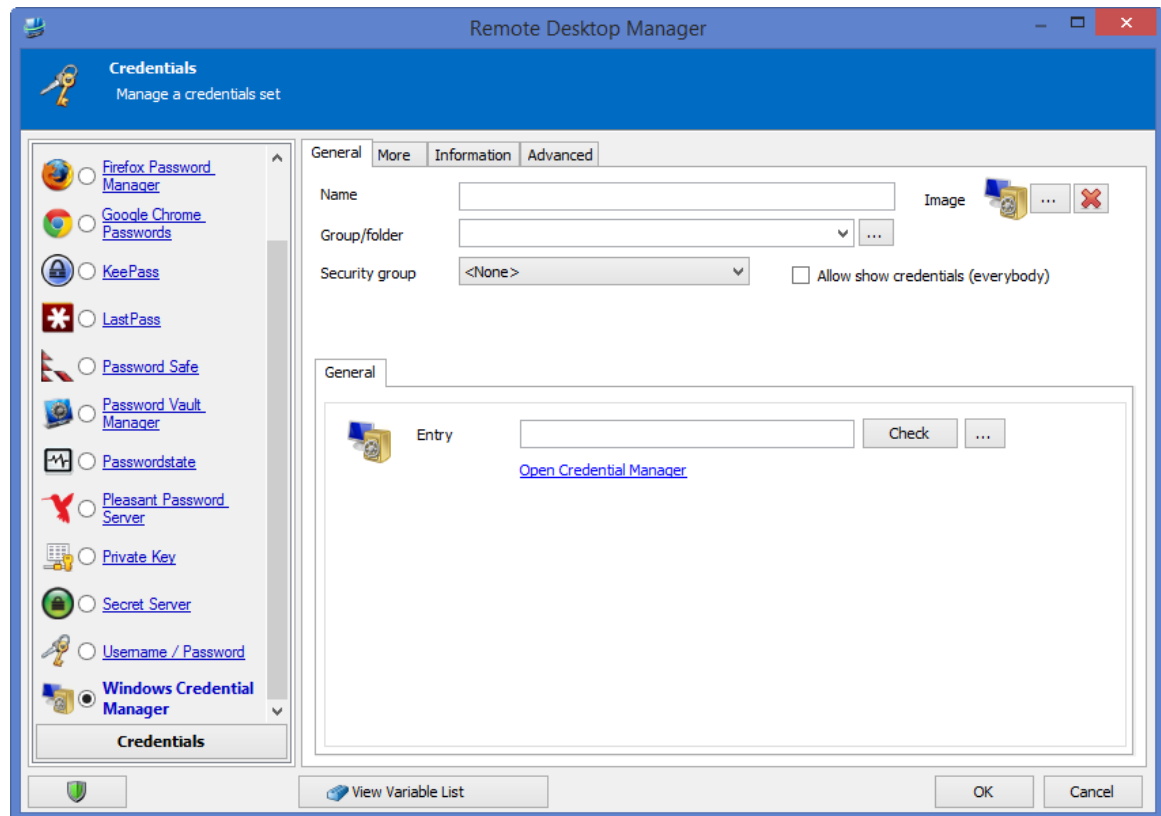
5.6.3.11 Windows Credential Manager

Description



This entry is used to define and configure a 'Windows Credential Manager' credential entry. Use an existing credential entry from the Windows Credential Manager (also called Windows vault).

Settings



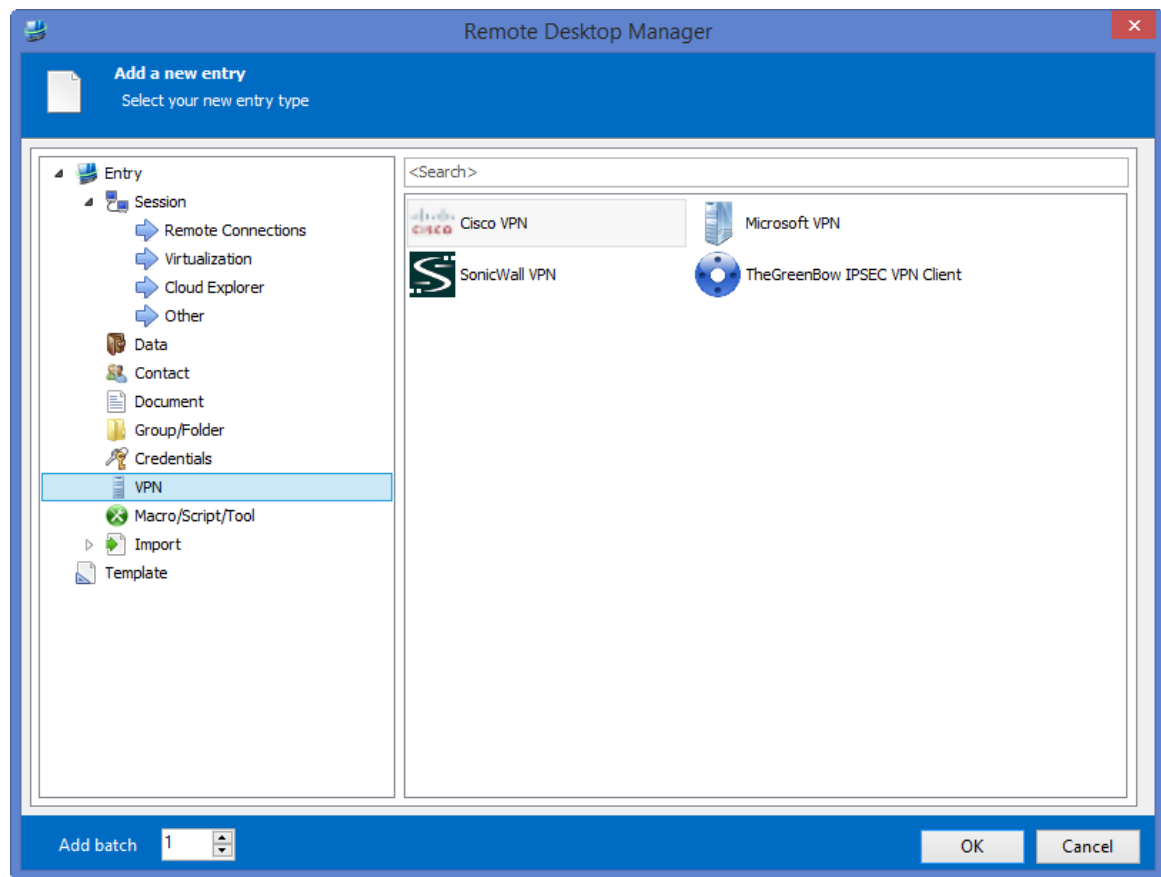
Windows Credential Manager credential entry

5.7 VPN

5.7.1 Overview

Description

VPN entry is used to configure a VPN session who can be share through multiple entries.



New VPN entry dialog

Consult topics below for more information on Remote Desktop Manager native VPN.

- [Cisco VPN](#)
- [Microsoft VPN](#)
- [SonicWall VPN](#)
- [TheGreenBow](#)

Multiple [VPN Add-ons](#) can be install in Remote Desktop Manager through the [Add-on Manager](#).

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

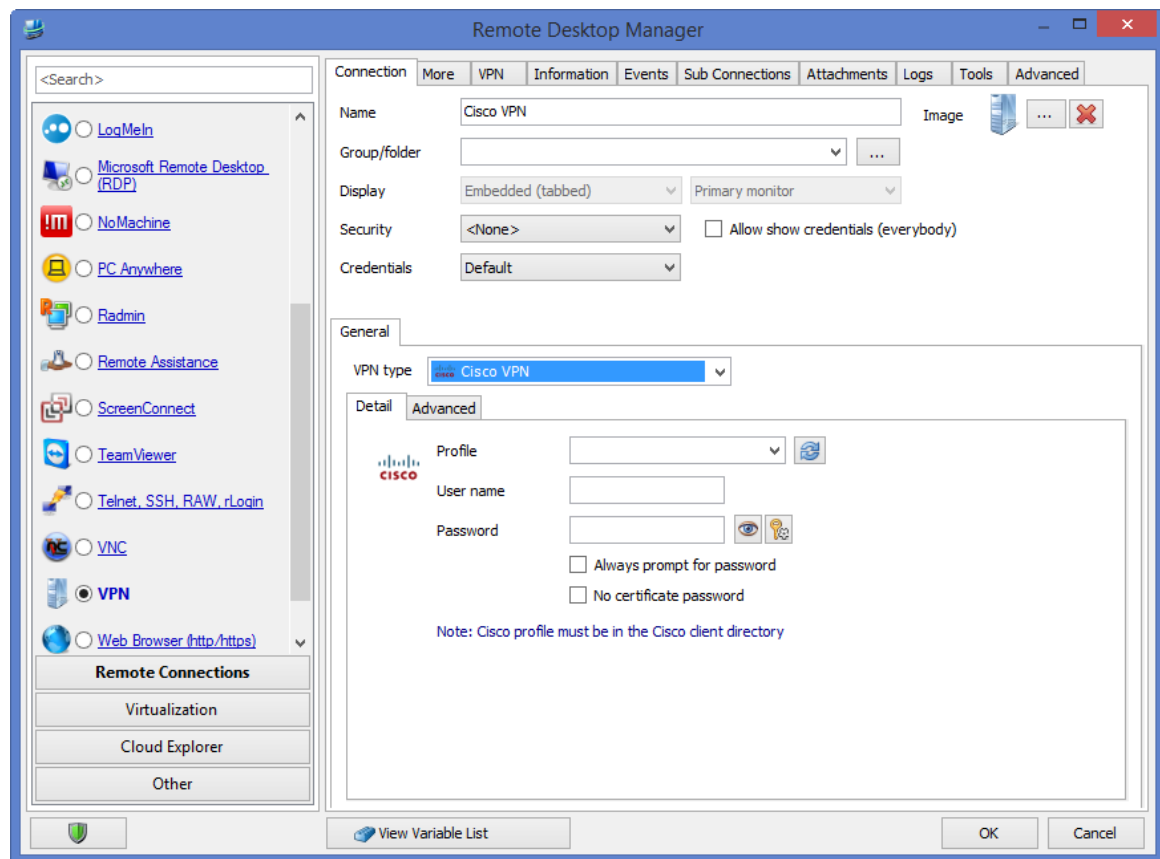
5.7.2 Types

5.7.2.1 Cisco VPN

Description

This entry is used to define and configure a "Cisco VPN" session. Use the Cisco AnyConnect add-on to configure a Cisco AnyConnect VPN.

Settings



Cisco VPN

Option	Description
Profile	Select a Cisco profile from in the Cisco client directory. Only the profiles available in the Cisco folder can be used.
User name	Username to connect on the Cisco VPN.
Password	Password to connect on the Cisco VPN.
Always prompt for password	Indicate to not store the password and always prompt for it when connecting to the VPN.
No certificate password	Indicate the there is not certificate password.

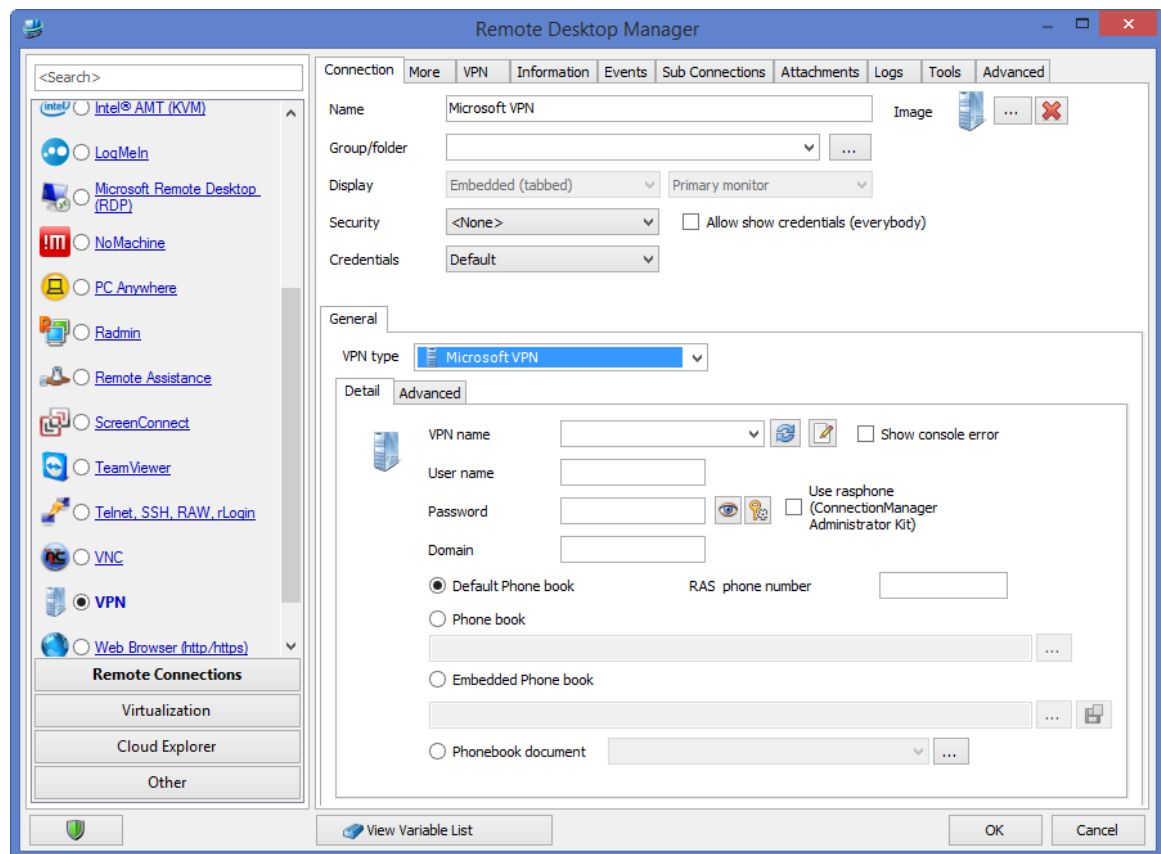
Consult topic [VPN Overview](#) for more information on VPN Management.

5.7.2.2 Microsoft VPN

Description

This entry is used to define and configure a "Microsoft VPN" session. It integrates rasdial.exe and rasphone.exe

Settings



Microsoft VPN

Option	Description
VPN name	Name of the VPN.
Show console error	Display the console errors or messages during the connection. Use this setting to diagnose if any connection problem appears. The application will capture the command line trace and it will display the result.
User name	Username to connect on the Microsoft VPN.
Password	Password to connect on the Microsoft VPN.
Domain	Domain to connect on the Microsoft VPN.
Use rasphone (Connection Manager Administration Kit)	Used to open a VPN created with the Connection Manager Administration Kit or when you need to force the rasphone usage.
Default Phonebook	Use the default Phonebook on the computer usually located in %userprofile%\AppData\Roaming\Microsoft\Network\Connections\Pbk\rasphone.pbk
RAS phone number	Enter the remote access service phone number
Phone book	Select a phone book file to use for the connection. Specify a local file or network file to share it.
Embedded Phone book	Embed the phonebook directly in the session to make it more portable. Please note that if you use the same

	phonebook for multiple VPN it's better to create a Phone Book Document to reduce the size of the database.
Phonebook document	Select a Phone Book Document entry from the list populated by the application.

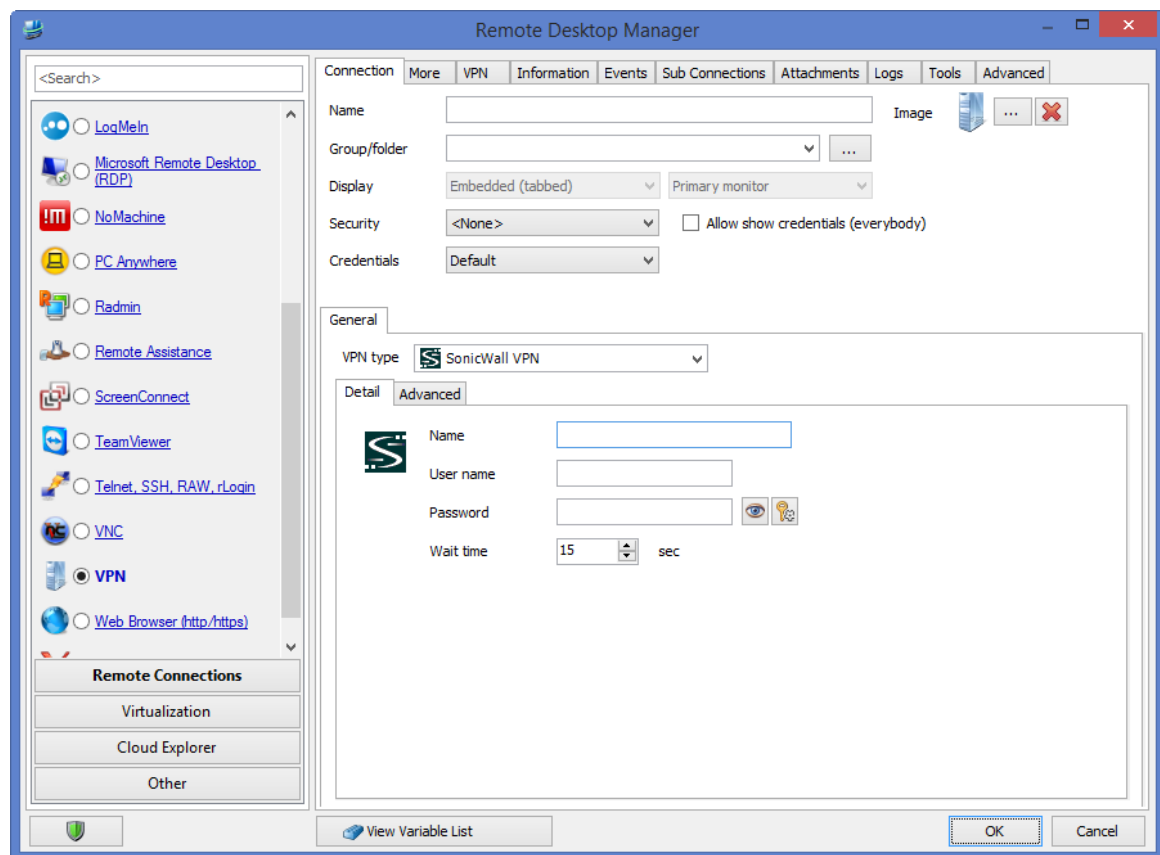
Consult topic [VPN Overview](#) for more information on VPN Management.

5.7.2.3 SonicWall VPN

Description

This entry is used to define and configure a "SonicWall VPN" session with the SonicWall Global client. Use the SonicWall NetExtender add-on to use if with a SonicWall NetExtender VPN.

Settings



SonicWall VPN

Option	Description
Name	Enter the name of the connection. This must match an existing SonicWall profile.
User name	User name to connect on the SonicWall VPN.
Password	Password to connect on the SonicWall VPN.
Wait time	Enter a wait time between the attempt to open the VPN and the attempt to

perform further action. Increase it if your VPN takes a long time to complete the connection process.

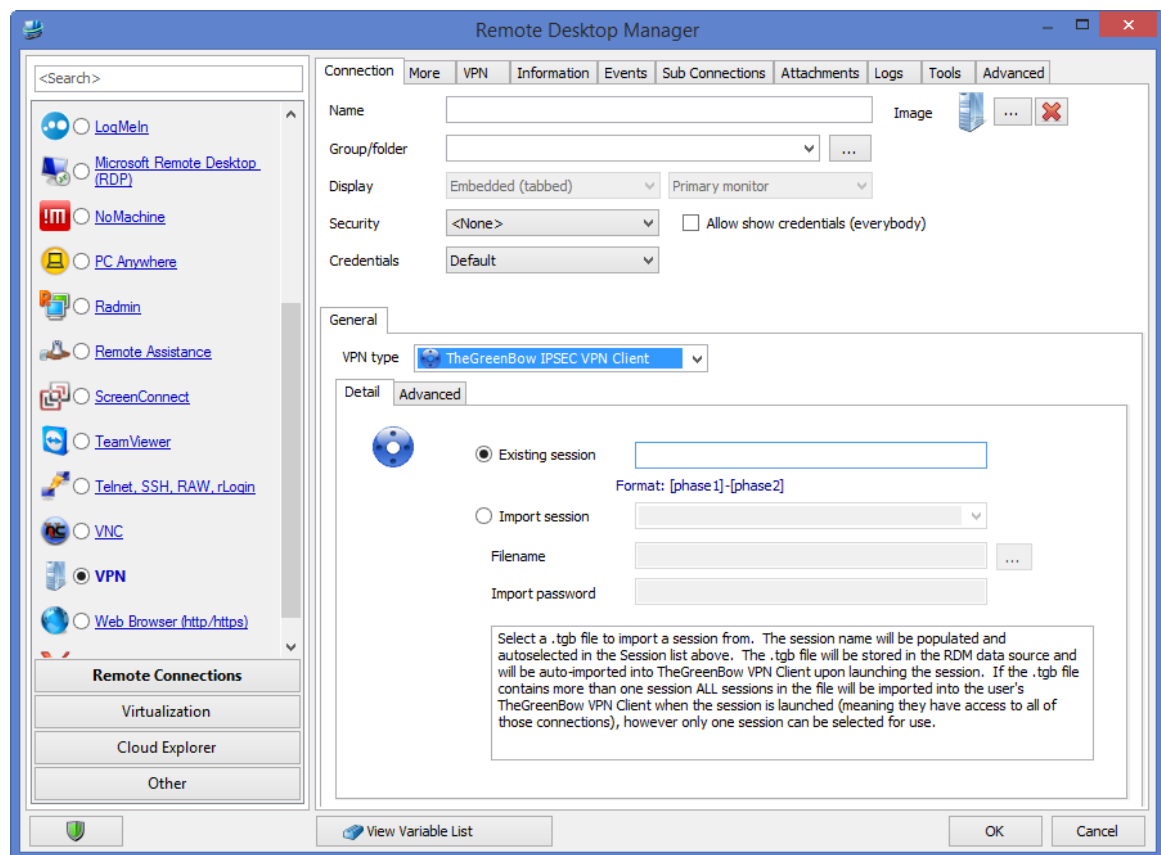
Consult topic [VPN Overview](#) for more information on VPN Management.

5.7.2.4 TheGreenBow

Description

This entry is used to define and configure a "TheGreenBow IPSEC VPN Client" session.

Settings



TheGreenBow

Option	Description
Existing session	Use a existing The Green Bow VPN Session.
Import session	Select the session to import inside the .tgb file.
Filename	Select the .tgb file to import in the application.
Import password	Enter the password that was set in your export file from The Green Bow VPN Client.

Consult topic [VPN Overview](#) for more information on VPN Management.

5.8 Macros/Scripts/Tools

5.8.1 Overview

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, and are listed in the dashboard under the "Macros/Scripts/Tools" section.

Session tools are commonly used to retrieve an information, perform some action, change an item, or change a configuration on the session host. There are three types of tools currently supported:



The [Session Variables](#) can be used as parameters for the macro/script/tool.

Macro/Script/Tool Manager

Consult this [topic](#) for more details about the Macro/Script/Tool Manager.

See Also

- [AutoHotKey](#)
- [Autolt](#)
- [Command Line](#)
- [Database Query](#)
- [Jitbit Macro Recorder](#)
- [Macro](#)
- [PowerShell \(Local\)](#)
- [PowerShell \(Remote\)](#)
- [PSEXec](#)
- [Template](#)
- [VBScript](#)
- [WASP PowerShell](#)
- [WMI](#)

5.8.2 Types

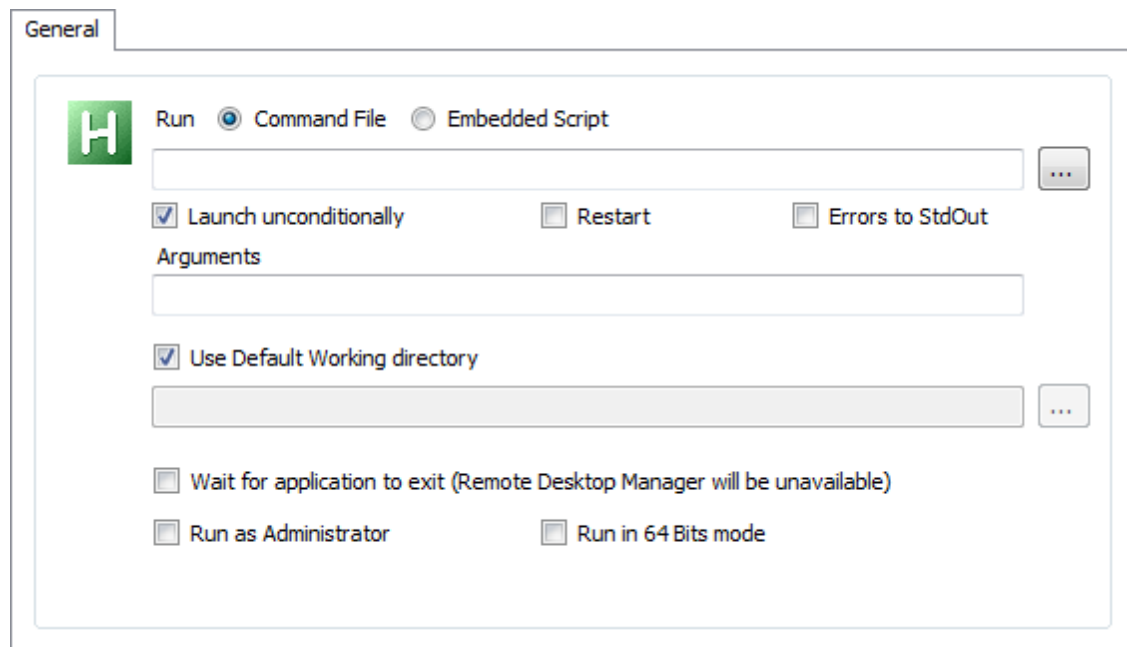
5.8.2.1 AutoHotKey

Description



This entry is used to integrate AutoHotKey freeware tool. It is used for automation, Hotkeys and scripting.

Settings



AutoHotKey entry configuration

Command file mode

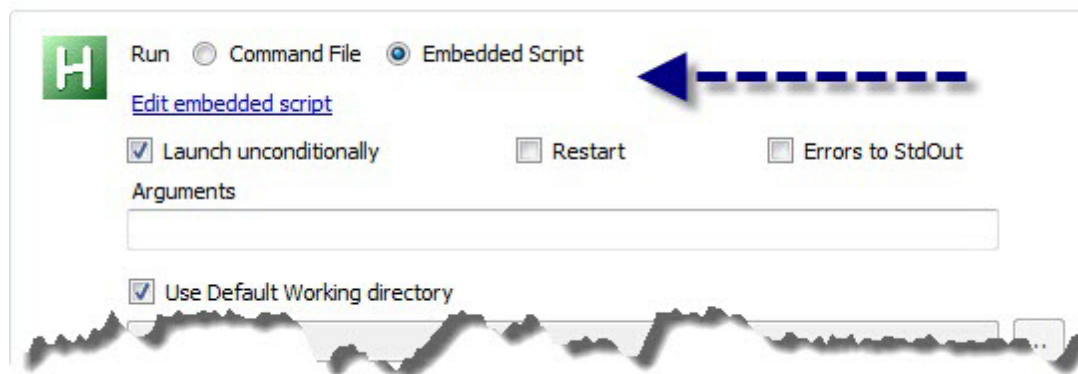
The default mode is to run command files. Simply press the button to select your file.

The rest of the settings are as follows:

Properties	
Launch unconditionally	This is sometimes required because some hooks are not installed to preserve memory. Please consult the AutoHotKey manual.
Restart	Restarts the script if it is currently running.
Errors to StdOut	Errors messages are redirected to the standard output instead of displaying dialog.
Arguments	Parameters to send to your AutoHotKey script.
Working directory	Choose to run from the default working directory of AutoHotKey, or specify the working directory.
Wait for application to exit	Runs the script synchronously, this means that the RDM process will wait for the script to return before resuming execution. This will cause RDM to be unresponsive while the script runs.
Run as administrator	Elevates the process to run as an administrator.
Run in 64 Bits mode	Runs by using the 64 bit architecture.

Embedded script mode

Choosing the Embedded Script radio button toggles the interface as follows.



Embedded script mode

Prerequisites

Local installation of AutoHotKey.

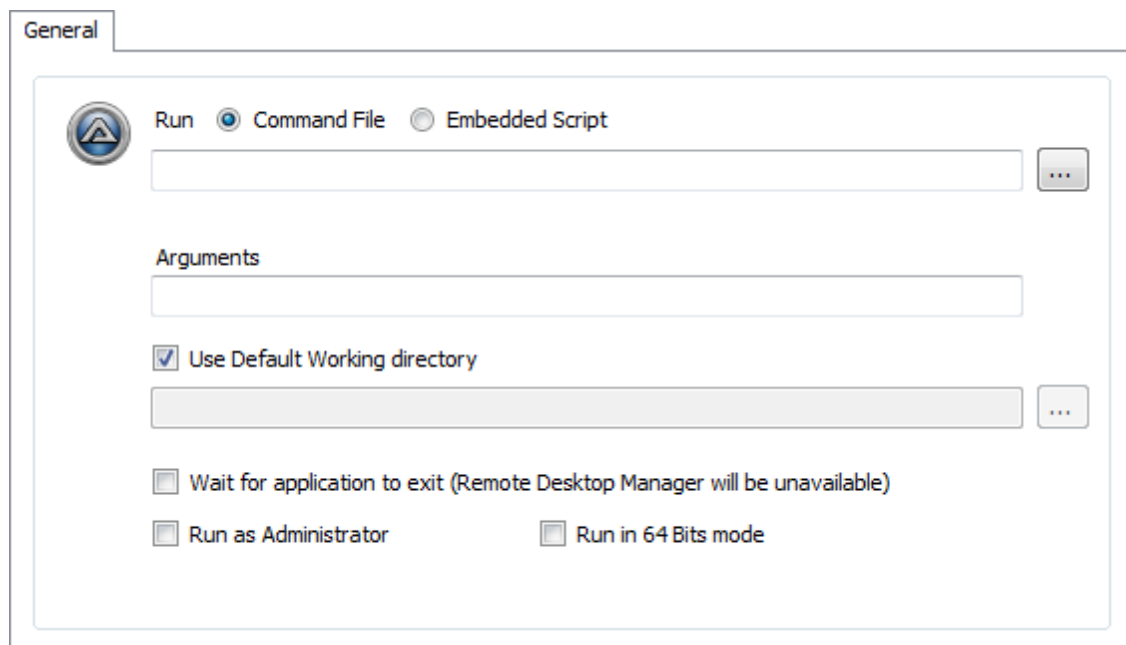
5.8.2.2 Autolt

Description



This entry is used to integrate a 'Autolt' macro/script/tool.

Settings



5.8.2.3 Command Line

Description



This entry is used to integrate the Windows command line. It will execute a command on the local machine.

Settings

Command line entry configuration

Click on the ellipsis button to select the command to run. Additionally you can assign another icon to the entry.

The remainder of the settings are as follows:

Properties	
Working directory	Choose to run from the system default working directory, or specify the working directory.
Wait for application to exit	Runs the script synchronously, this means that the RDM process will wait for the script to return before resuming execution. This will cause RDM to be unresponsive while the script runs.
Run as administrator	Elevates the process to run as an administrator.
Run in 64 Bits mode	Runs by using the 64 bit architecture.
Open embedded/tabbed	Displays the command window in a tab within RDM.
Shell execute	Uses the shell execute mode. Please refer to the Windows documentation.

5.8.2.4 Database Query

Description



This entry is used to integrate a 'Database Query' macro/script/tool.

Settings

A screenshot of the 'Database Query' settings dialog. It has a 'General' tab. Inside, there is a 'Query type' dropdown menu set to 'DataReport'. Below it is a large text area labeled 'Query' with a vertical scrollbar on the right and a small button with three dots in the top right corner.

5.8.2.5 Jitbit Macro Recorder


Description



This entry is used to integrate a 'Jitbit Macro Recorder' macro/script/tool.

Settings

General

 Run ☒ Command File ☐ Embedded Script

☐ Wait for application to exit (Remote Desktop Manager will be unavailable)

☒ Shell Execute

5.8.2.6 Macro


Description



This entry is used to integrate a built-in macro. It uses the same keys/commands supported in [Auto Typing Macro](#)

Settings

General

 Typing macro

Initial wait sec

Delay time {Delay} ms

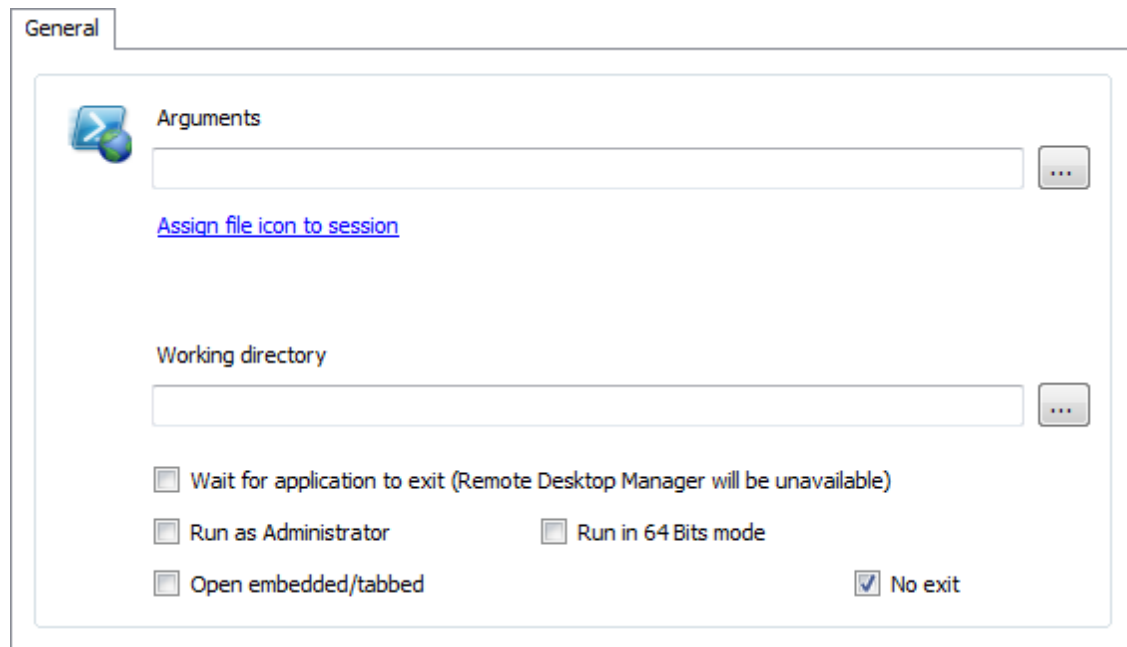
5.8.2.7 PowerShell (Local)

Description



This entry is used to integrate a 'PowerShell (Local)' session/script/tool.

Settings

A screenshot of the 'General' tab in a settings dialog for PowerShell (Local). The dialog has a title bar with 'General' selected. Inside, there's a section titled 'Arguments' with a text box and a button with three dots. Below that is a link 'Assign file icon to session'. Then a section titled 'Working directory' with another text box and a button with three dots. At the bottom, there are four checkboxes: 'Wait for application to exit (Remote Desktop Manager will be unavailable)', 'Run as Administrator', 'Run in 64 Bits mode', and 'Open embedded/tabbed'. The 'No exit' checkbox is checked.

5.8.2.8 PowerShell (Remote)


Description




This entry is used to integrate a 'PowerShell (Remote)' session/script/tool. It will execute a PowerShell command on the remote machine.

Settings


General

 Arguments



[Assign file icon to session](#)

Working directory



☐ Wait for application to exit (Remote Desktop Manager will be unavailable)

☐ Run as Administrator ☐ Run in 64 Bits mode

☐ Open embedded/tabbed ☒ No exit

5.8.2.9 PSEXec


Description




This entry is used to integrate a 'PSEXec' macro/script/tool. A PS Exec command is sent to the remote machine. You can get more information from the Microsoft website [here](#).

Settings

General

 Remote command (absolute path of the application on the remote computer)

Local working directory



☐ Wait for application to exit (Remote Desktop Manager will be unavailable)

☐ Run as Administrator ☐ Run in 64 Bits mode

☐ Open embedded/tabbed

5.8.2.10 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

The screenshot shows a settings window with a tab labeled 'General'. Inside the window, there is a section titled 'Template' with a file icon to its left. Below the title is a large, empty text input field. To the right of the input field is a small button with three dots, indicating a file selection dialog.

5.8.2.11 VBScript

Description




This entry is used to integrate a 'VBScript' macro/script/tool.

Settings

General

Run ☒ Command File ☐ Embedded Script

 ...

Arguments

☒ Use Default Working directory

...

☐ Wait for application to exit (Remote Desktop Manager will be unavailable)

☐ Run as Administrator ☐ Run in 64 Bits mode

☐ Open embedded/tabbed ☒ Shell Execute

5.8.2.12 WASP PowerShell

Description





This entry is used to integrate a 'WASP PowerShell' macro/script/tool.

Settings

General

Run ☒ Command File ☐ Embedded Script

 ... 

Arguments

☒ Use Default Working directory

...

☐ Wait for application to exit (Remote Desktop Manager will be unavailable)

☐ Run as Administrator ☐ Run in 64 Bits mode

☐ Open embedded/tabbed ☒ Shell Execute ☒ No exit

5.8.2.13 WMI


Description



This entry is used to integrate a 'WMI' session/script/tool.

Settings

General



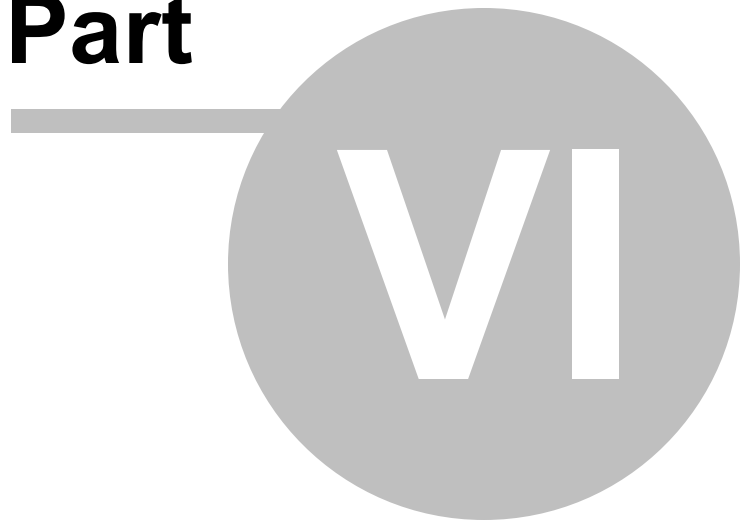
Namespace

WMI query

Test on Localhost

User Interface

Part



6 User Interface

6.1 Style

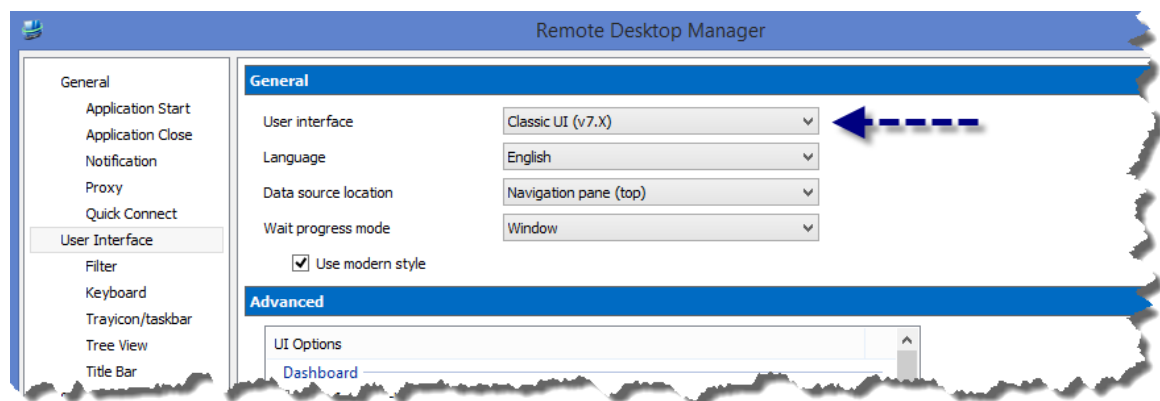
Description

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

- [Default \(Ribbon\)](#)
- [Default \(Menu\)](#)
- [Classic UI \(v7.X\)](#)

Configuration

To select the UI style you must go in **File -> Options -> User Interface**.

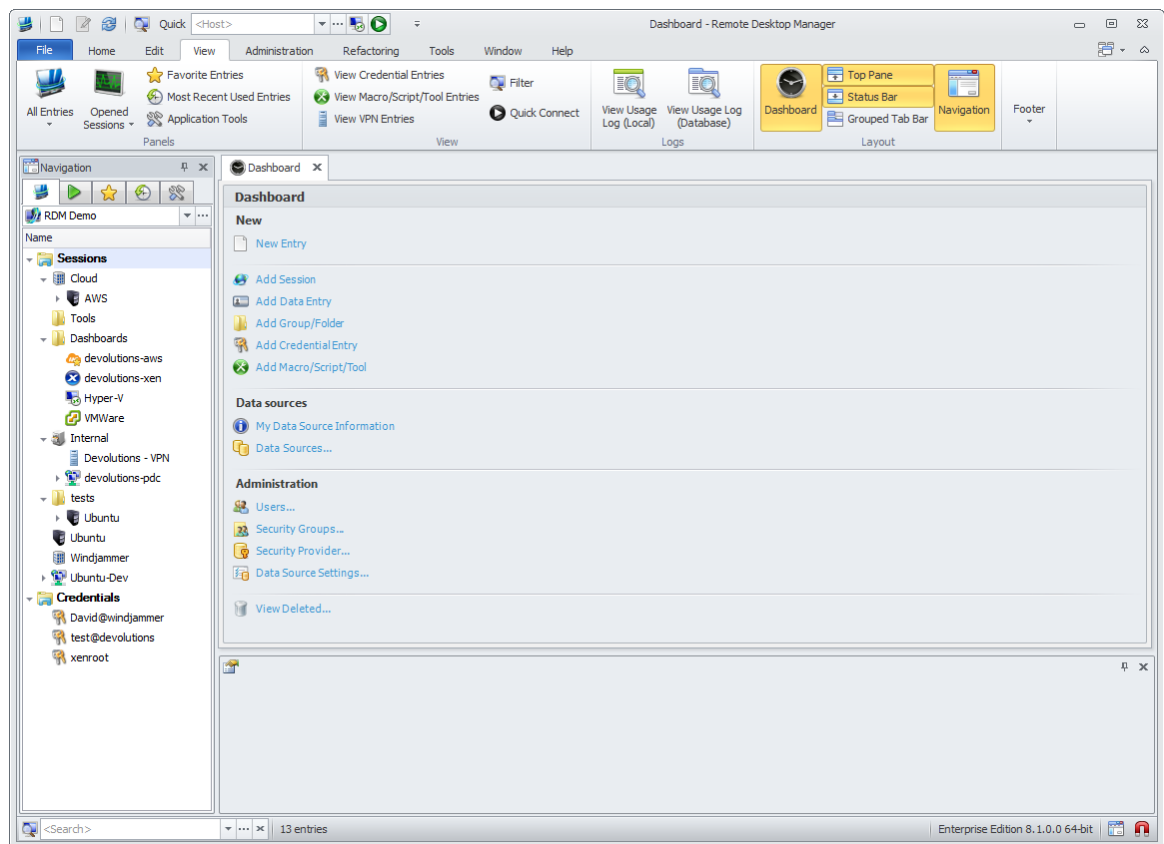


User Interface

Existing styles

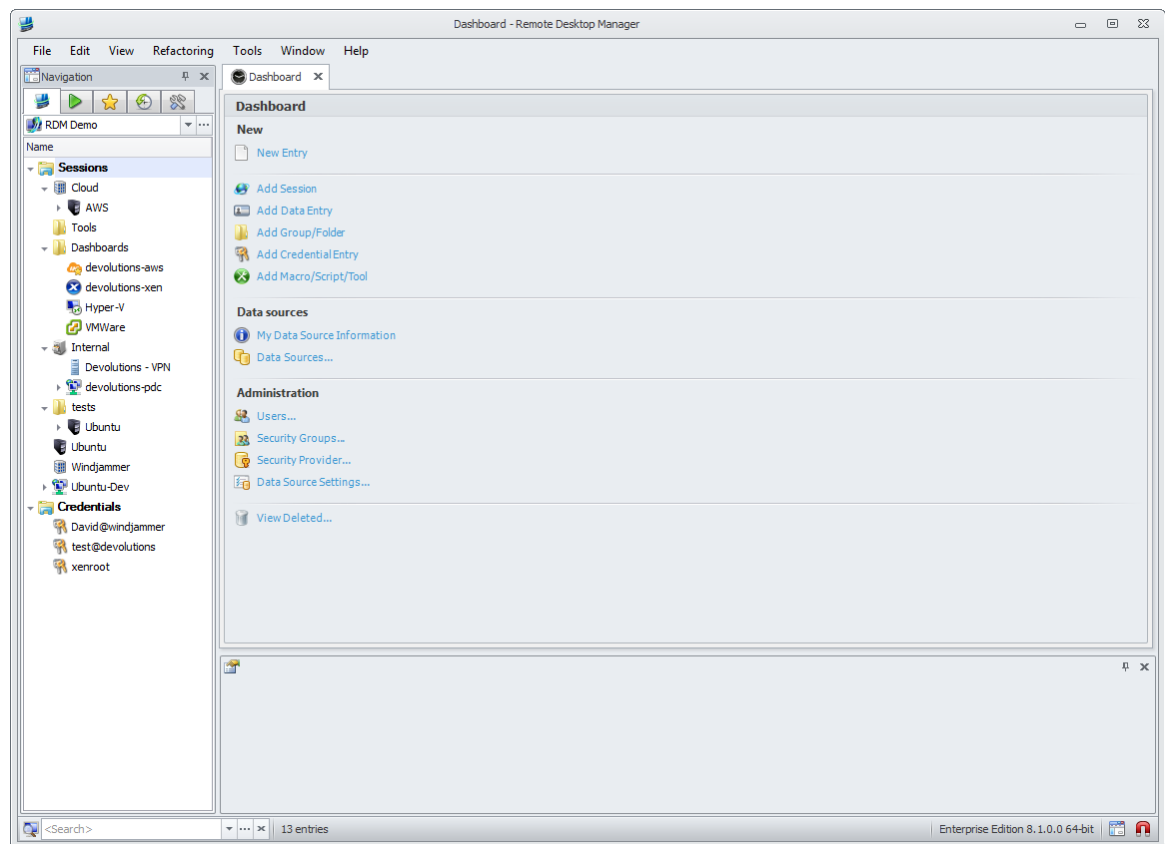
Default (Ribbon)

The latest style sports an advanced control called the ribbon. Icons and text make it easy to learn what features exist.



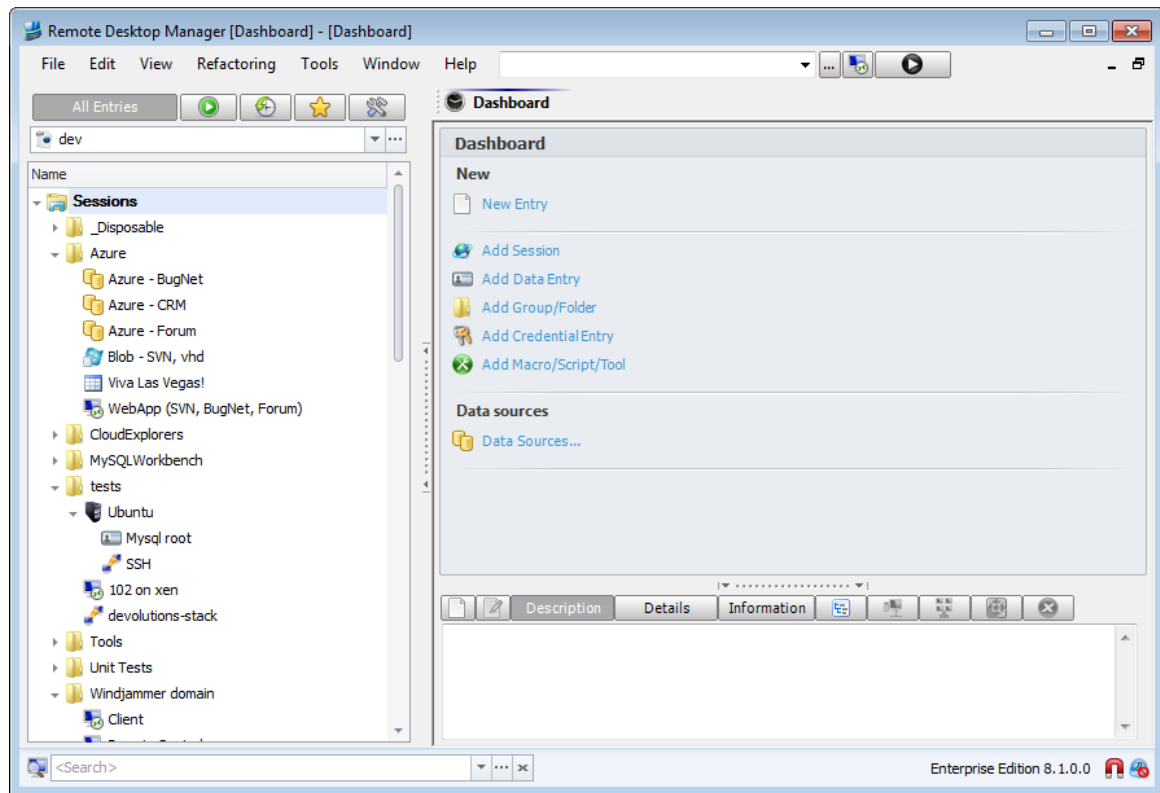
Default (Menu)

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



Classic UI (v7.X)

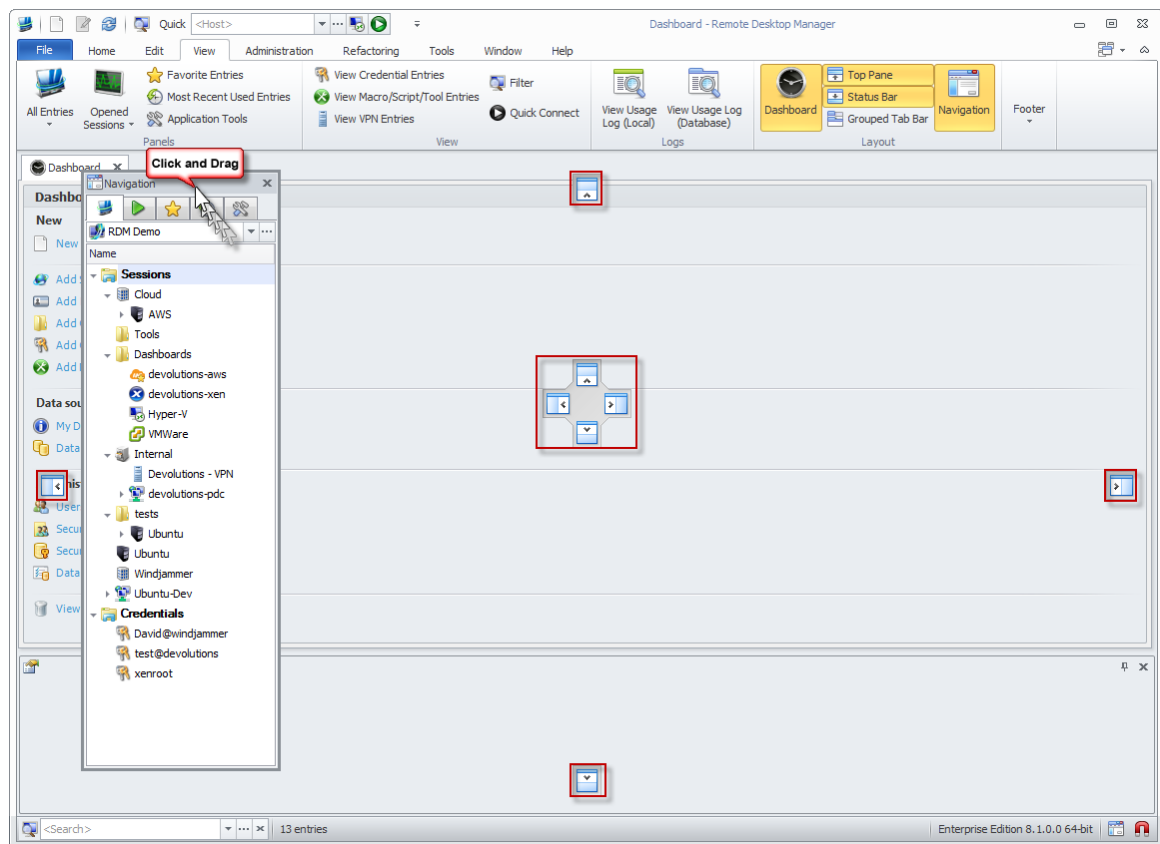
This style support minimal customization but requires minimal system resources to operate.



The Data Source Location set to none in File - > Options -> User Interface is not supported in Classic UI.

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.

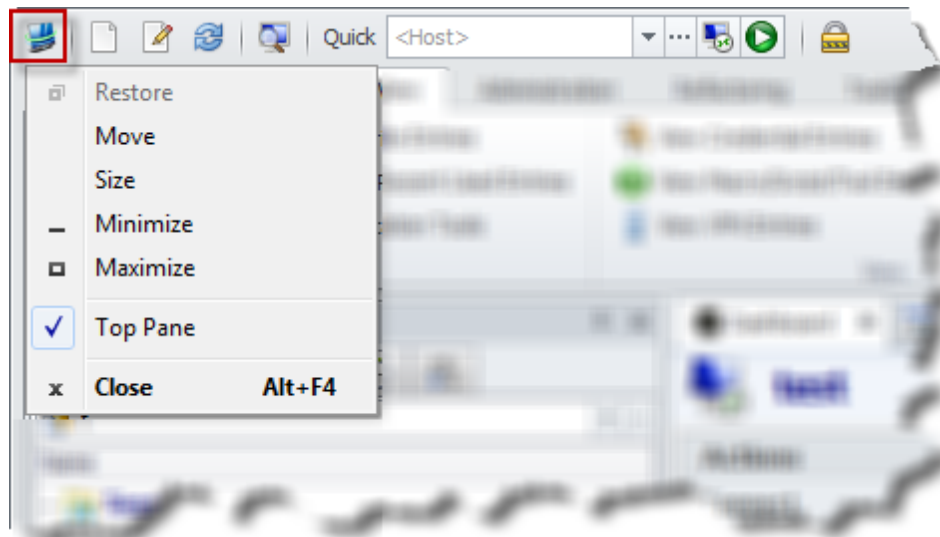


6.2 Top Pane

Description

The Top Pane is a container for the [Quick Access Toolbar](#) and the [Ribbon / Menu](#). It's usefulness arises of the fact that it can be hidden to maximize the client area of the main form.

System menu icon



System menu

Click on this icon to display the system menu. Almost the same as any other Windows Application, but with the addition of the Top Pane toggle. This toggle will hide the Quick Access Toolbar and the Ribbon. This offers more display area for embedded sessions. If you hide the Top Pane using this toggle, or with the **View -> Layout -> Top Pane** command, this is one of the way to restore it. The other being the keyboard shortcut assigned to this command, namely Alt-F11.

6.2.1 Quick Access Toolbar

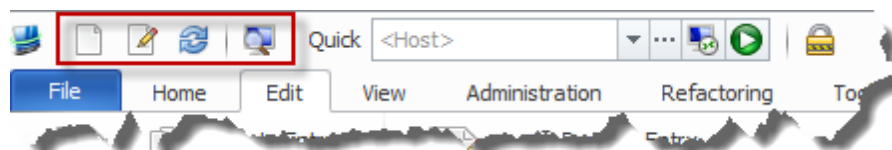
Description

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

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



Favorite commands



Favorite commands

Right-Clicking on any command will display a contextual menu. If you perform this on a command in the Quick Access Toolbar, the caption will be **Remove from Quick Access Toolbar**. If you perform this on a command in the ribbon, the caption will be **Add to Quick Access Toolbar**. Use this at your leisure to add or remove commands from this area.

Quick Connect control

Please refer to [Quick Connect](#) for a detailed description.

Lock Command

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

6.2.1.1 Quick Connect

Description

Via the quick connect button, you can open an *ad-hoc* session by specifying the host and session type. It's also possible to create a template and use it. In the template you specify the desired default settings, and Remote Desktop Manager will apply them with the specified host.



Quick Connect Control

Settings

The control is composed of multiple sub controls.

Combo Box

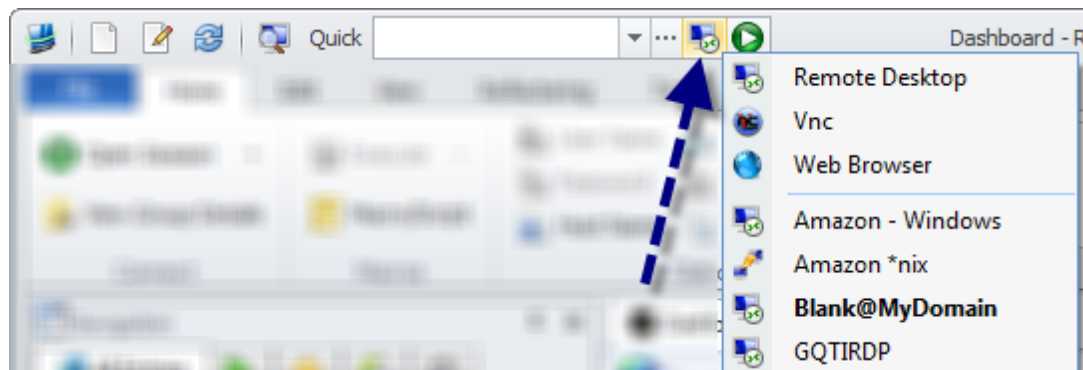
This area is used either to type in the host information, or by using the drop down and selecting a host from your Quick Connect history.

Please consult the [Quick Connect](#) topic for settings that apply to the Quick connect history feature.

Host Selection

The ellipsis button will list network discoverable computer to allow you to select computer from the list. Please note that It takes some time to perform the discovery.

Type Selection



Quick connect - connection type selection

Clicking on this button will allow you to choose either a connection type or an existing template. Selecting a type from the top area of the menu will simply launch the appropriate client and connect to the host. Selecting a template is quite powerful because you can specify all options: Credential, display mode, typing macros, etc. This template will be used to connect to the host using its settings.

Connect button

Click on the Connect button (green arrow) to launch the connection with your chosen configuration.

Quick Connect Variable

The **\$QUICK_CONNECT\$** variable can be used in a template to specify a replaceable value. It will be assigned at runtime with the content of the Quick Connect combo box. It is normally set in the Host field of a template, but it is also commonly used in the typing macro.

6.2.2 Ribbon / Menu

Description

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

Ribbon



Ribbon

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

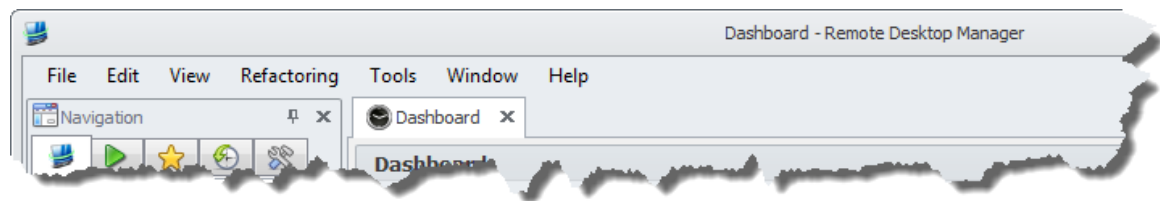
There are two interesting commands at the top right area:

- Content selector: Allows you to choose the active tab in the dashboard area
- Minimize ribbon: Collapses the ribbon so it appears as a menu. Useful when trying to maximize the content area.



Collapsed ribbon

Menu



Classic menu

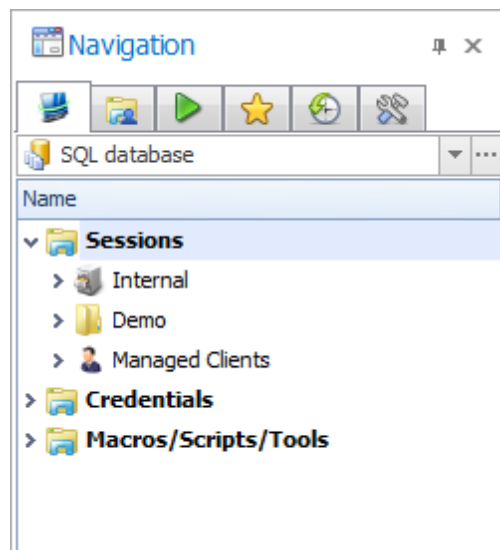
The classic menu is exactly that: classic. It contains the same commands but presented in a menu fashion.

6.3 Navigation Panels

Description

The Navigation Pane is the core of Remote Desktop Manager's user interface.

The All Entries tab lists all the various entries (sessions, data entries, credentials entries, etc) and is the principal manner of launching sessions.



Navigation Pane

More details on each tab can be found below:

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

6.3.1 All Entries

Description

The All Entries tab lists all existing entries. The view selection can be done in **View -> All Entries**.

The visual structure can be:

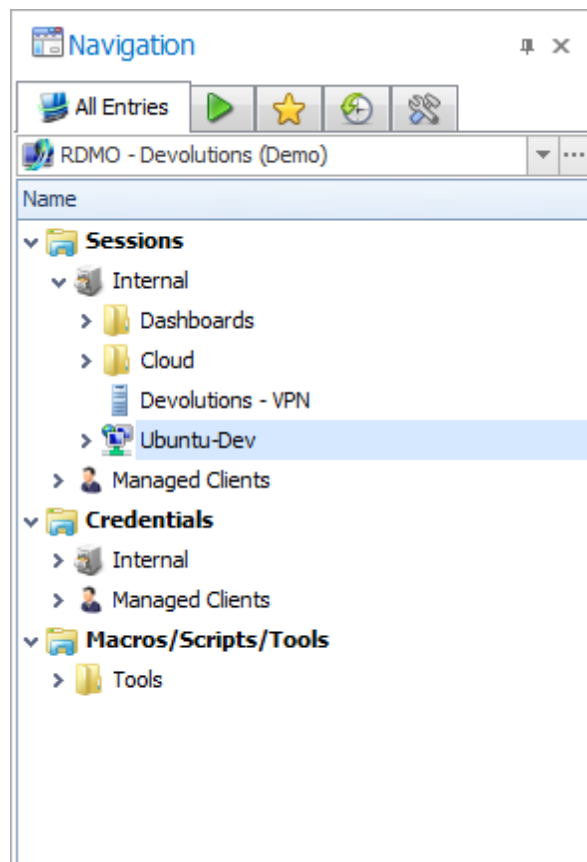
- Tree View
- Tiles View
- List View
- Details View
- Large Icons View

Tree View



Use the F7 shortcut (default shortcut) to change the entry view to tree view.

The tree view offers the most flexible display mode. By focusing the control, you can activate the incremental search by typing letters and numbers. Use Ctrl+Up/Down to move to the next or previous matching entry and Backspace to delete the current incremental search.

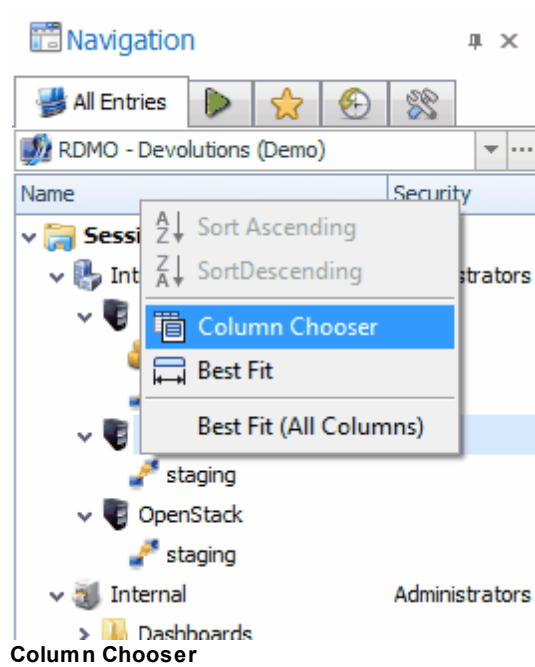


Tree view

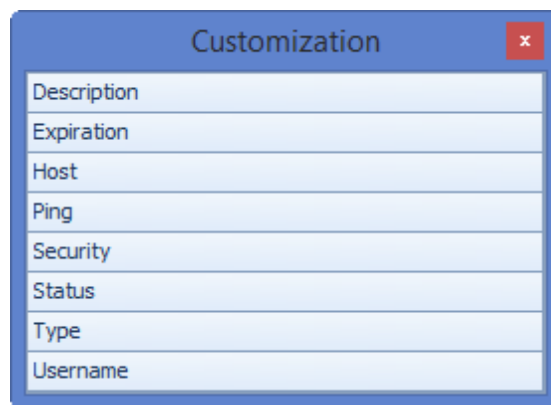
Column Chooser

It's possible to specify the visible columns in the tree list view. Columns can be added in the Navigation

Pane by right-clicking on the column Name in the Navigation Pane and selecting Column Chooser.



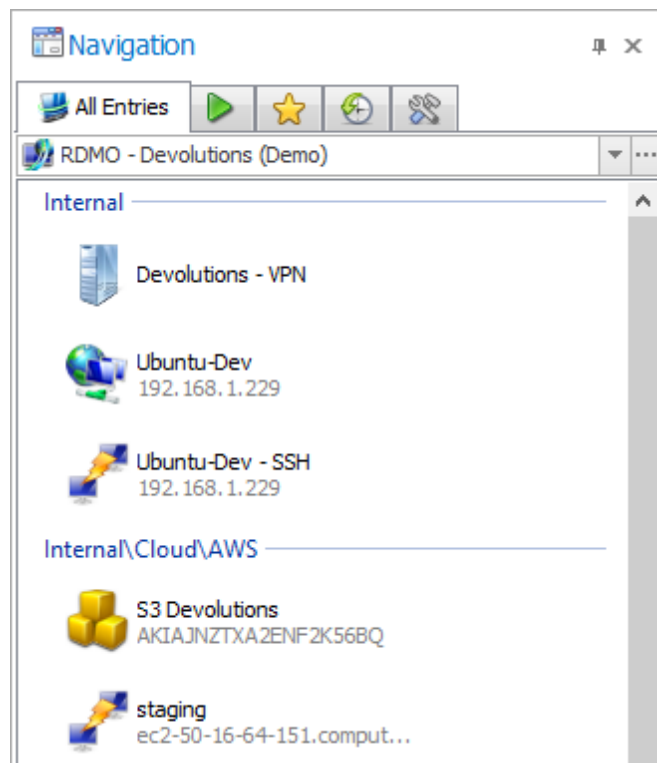
The following columns can be added:



Customization

Tiles View

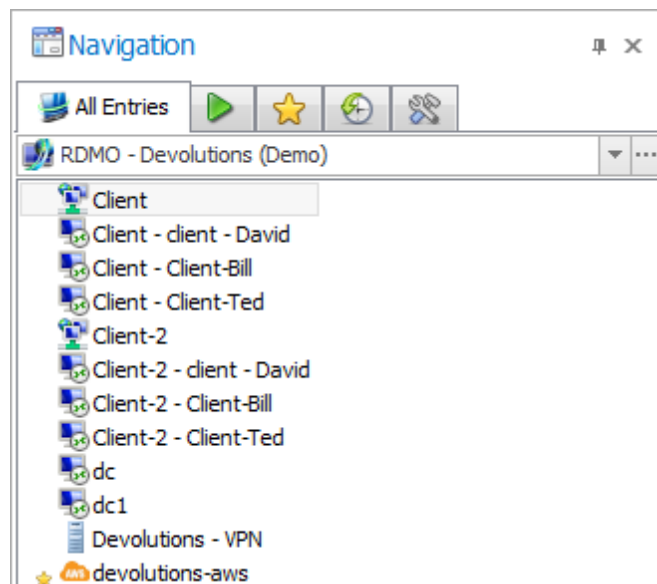
The Tiles view displays the sessions to see all of them next to one another.



Tiles view

List View

The list view displays the sessions as a list.

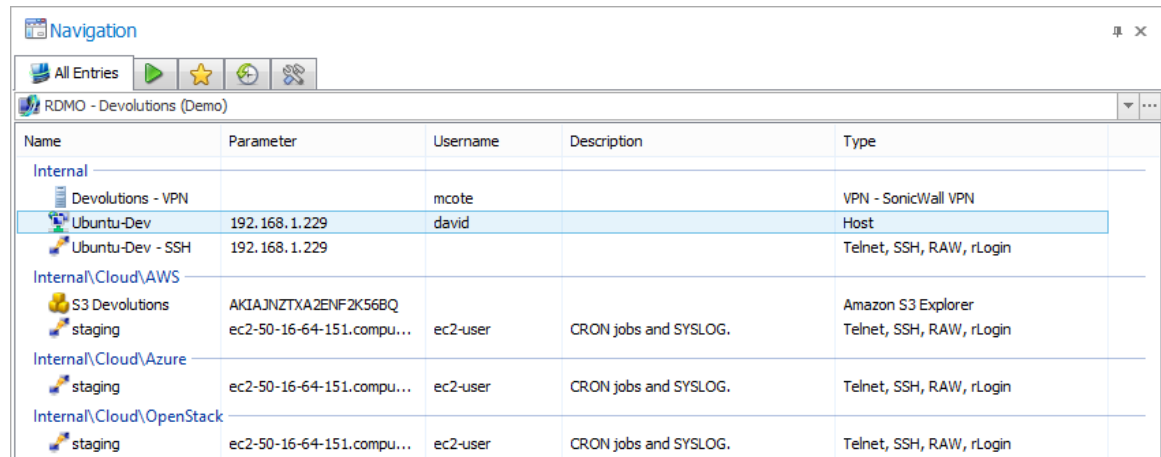


List view

The list view can contain a large number of session configurations. Use the filter box at the bottom of the screen to help you find what you need. Learn more about this feature [here](#).

Details View

The Details view displays multiple details on each sessions.

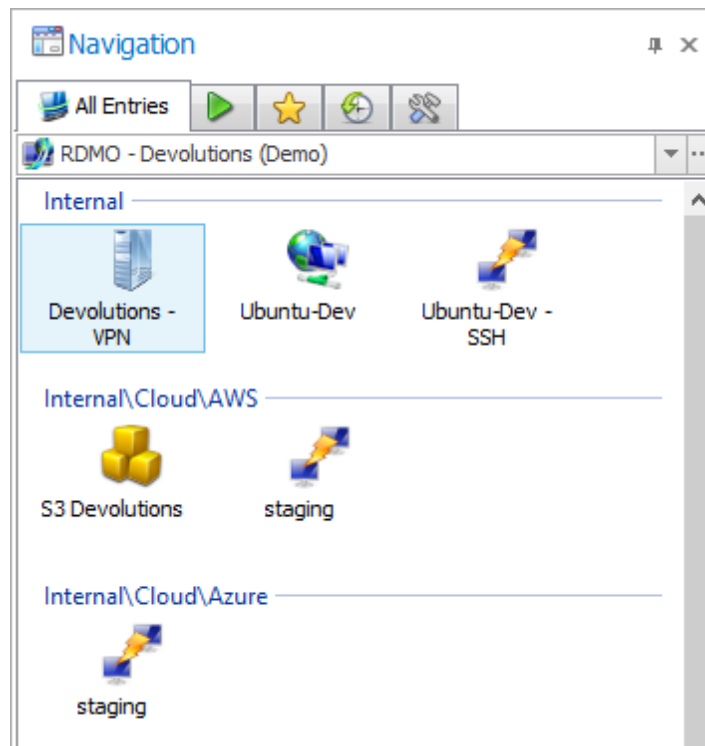


Name	Parameter	Username	Description	Type
Internal				
Devolutions - VPN		mcote		VPN - SonicWall VPN
Ubuntu-Dev	192.168.1.229	david		Host
Ubuntu-Dev - SSH	192.168.1.229			Telnet, SSH, RAW, rLogin
Internal\Cloud\AWS				
S3 Devolutions	AKIAJNZTXA2ENF2K56BQ			Amazon S3 Explorer
staging	ec2-50-16-64-151.compu...	ec2-user	CRON jobs and SYSLOG.	Telnet, SSH, RAW, rLogin
Internal\Cloud\Azure				
staging	ec2-50-16-64-151.compu...	ec2-user	CRON jobs and SYSLOG.	Telnet, SSH, RAW, rLogin
Internal\Cloud\OpenStack				
staging	ec2-50-16-64-151.compu...	ec2-user	CRON jobs and SYSLOG.	Telnet, SSH, RAW, rLogin

Detail view

Large Icons View

The Large Icon view displays sessions with large icons.



Large Icons view

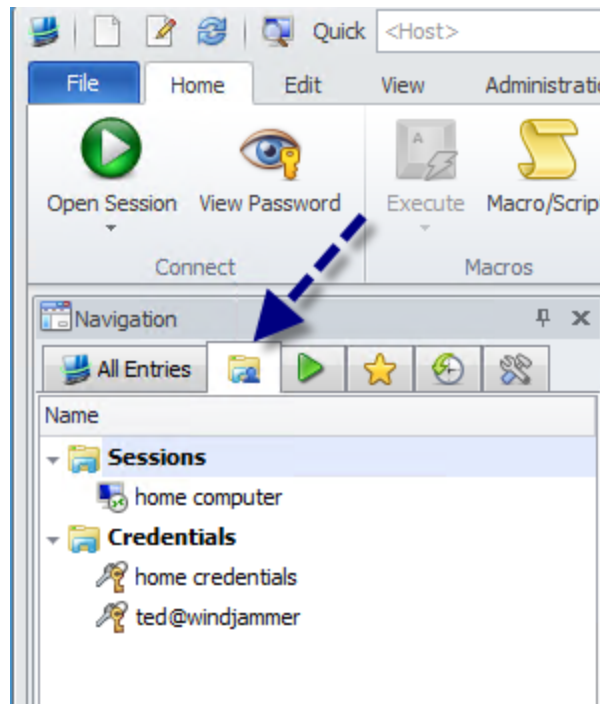
6.3.2 Private Vault

Description

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



The Private Vault is currently only available for [MSSQL](#), [MySQL](#), and [Remote Desktop Manager Server](#) data sources.



Private Vault tab

A note on Credentials

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

1. From a session in the Private Vault
2. When using the Edit Entry ([User Specific Settings](#)).

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 itself, or by using our extension mechanism that is user specific.

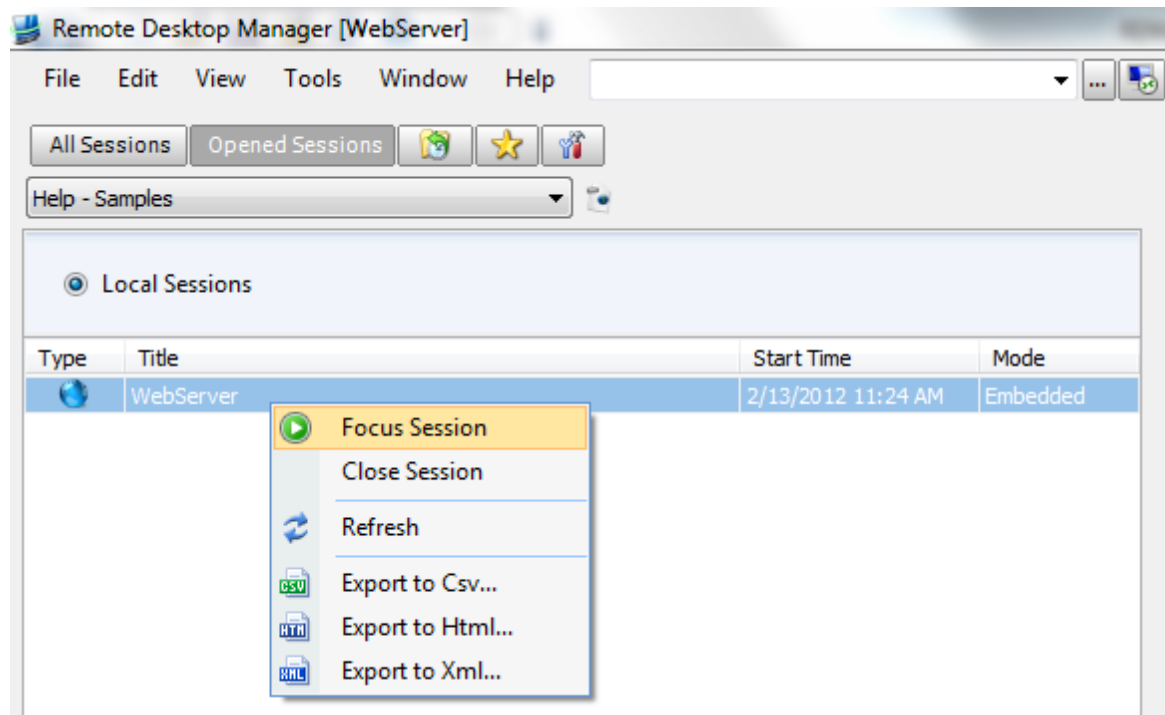
6.3.3 Opened Sessions

Description

The opened view shows currently opened sessions by type, and for the local machine only. You can

focus and bring to front/close an opened session by double clicking it from the list. All of the embedded sessions are listed, and the external session will appear if Remote Desktop Manager is able to discover the specific type of session.

Local Opened Sessions



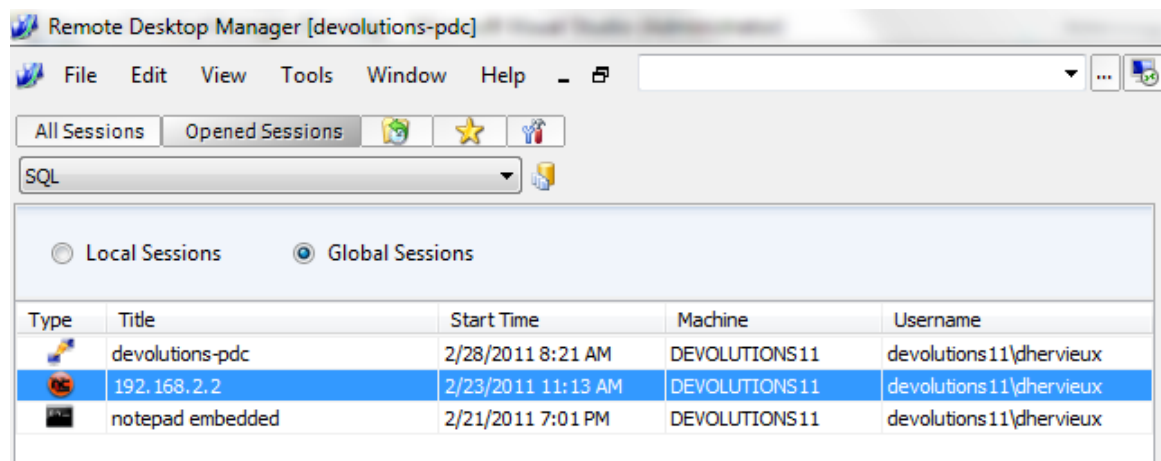
Local opened session view

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.

Global Opened Sessions

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



Global opened session view

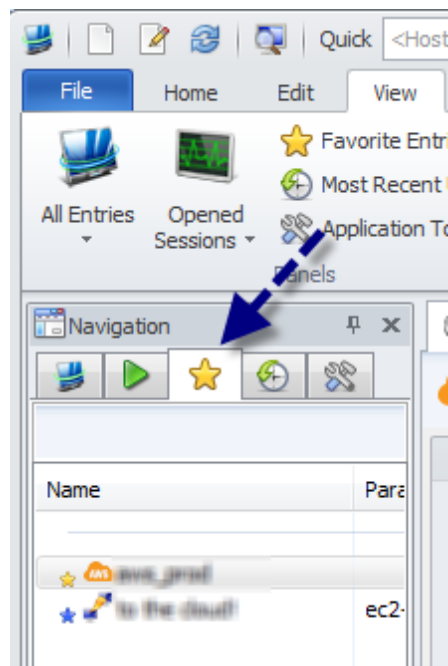
For many reasons beyond our control, it's possible for a session to be terminated without Remote Desktop Manager knowing that this has taken place. This can happen, for example, if Remote Desktop Manager isn't running when another application ends. As a result, any terminated session will remain listed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

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

6.3.4 Favorite Entries

Description



This view contains all of your favorite sessions that have been configured in the current data source. This is useful when the number of managed entries becomes too great or if you must maintain a strict directory structure to hold your entries.



Favorites Tab

Settings

There are two types of favorite sessions:

- Shared favorites 
- Local favorites 

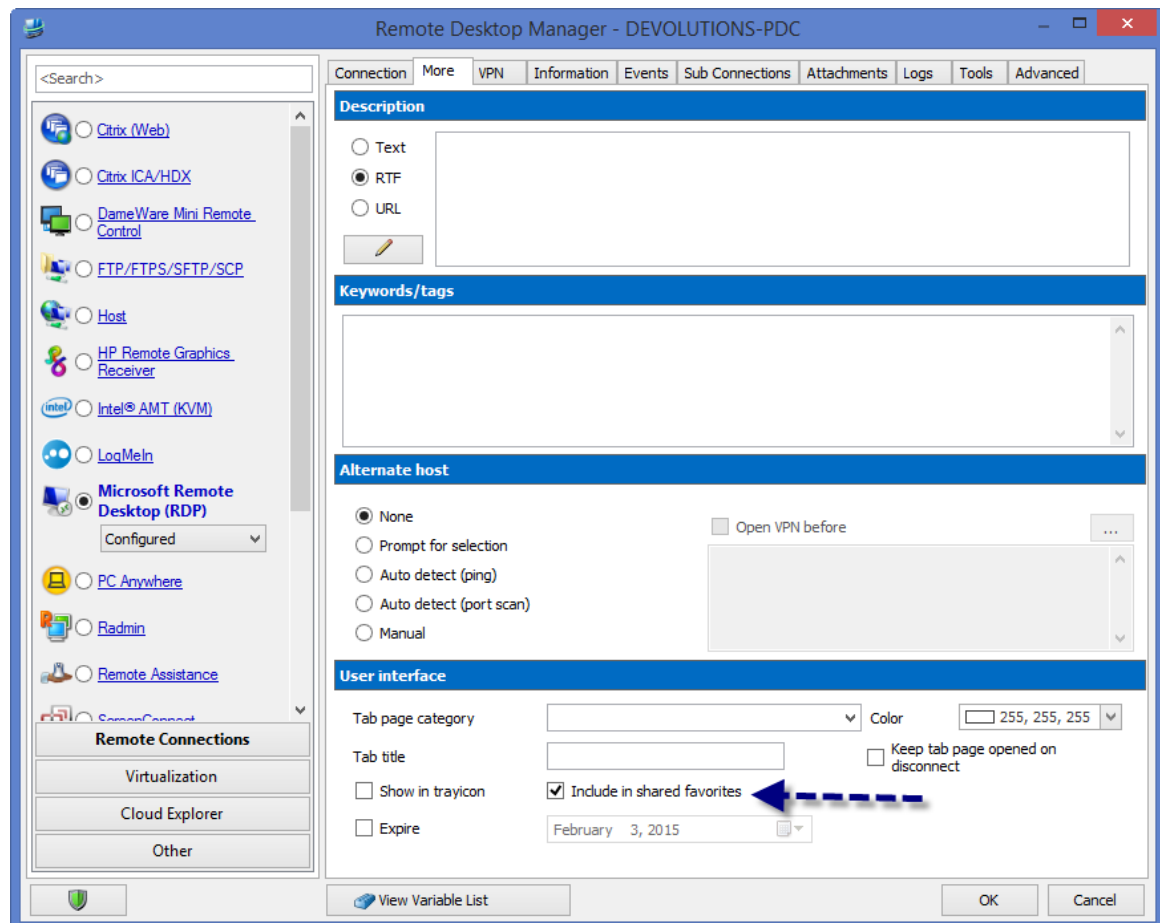


The yellow star is for a shared favorite and the blue star is for a local favorite.

Shared favorites are shared by all users who are connected to the data source, and are directly configured from the session.

Local favorites are flagged locally on the current machine by the current user. The settings are saved in the application settings.

Adding a Session to the Shared Favorites



Session settings dialog

You may add or remove a session from the shared favorites by editing its properties.

You can also use the context menu to include or remove a session from your favorites by **right-clicking** on the session and select **Favorites** or you can do it by clicking on **Home** and select **Favorite** in the [Tools](#) section.

Adding a Session to the Local Favorites

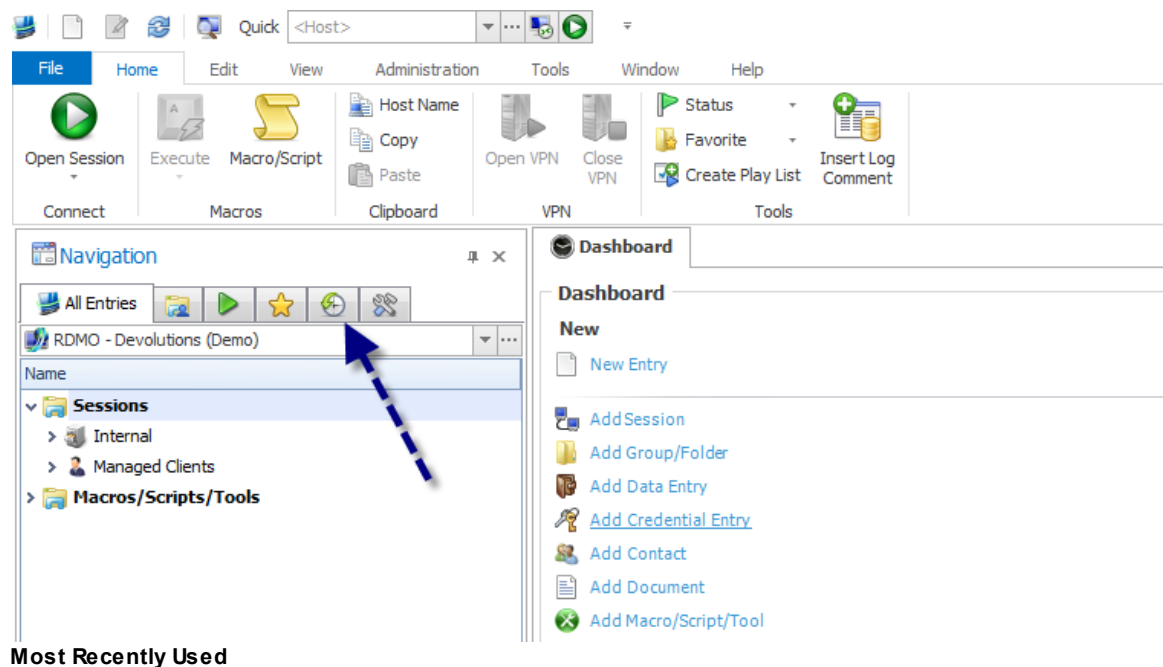
A local favorite can be added through the favorite.

You can also use the context menu to include or remove a session from your favorites by **right-clicking** on the session and select **Favorites** or you can do it by clicking on **Home** and select **Favorite** in the [Tools](#) section.

6.3.5 Most Recently Used Entries

Description

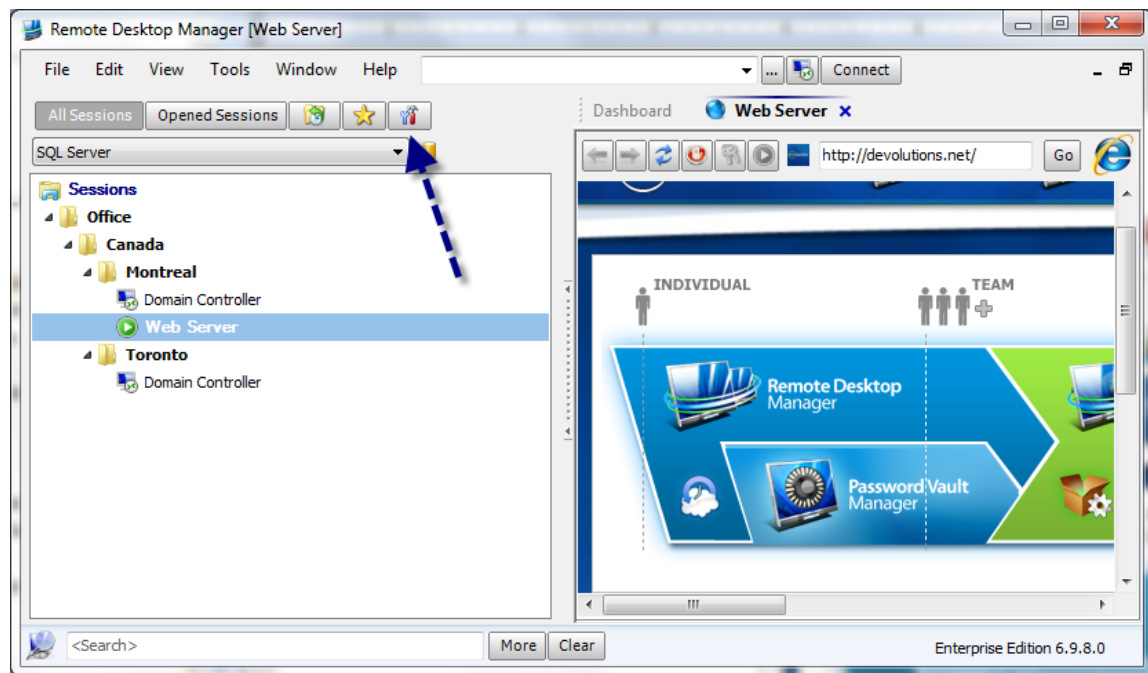
This view show the most recently used sessions for a specific data source on the local computer.



6.3.6 Application Tools

Description

This view shows all pre-configured tools. These tools are not specific to a session, and each is executed on the local computer. For specific session tools, see the session tools available in the context menu.



Application tools button

Available Tools

- Command Prompt
- Computer Management
- Control Panel
- Event Viewer
- Internet Information Services (IIS) Manager
- IP Config
- Open Network Connections
- Registry Editor
- Services

Application Tools Add-Ons

You may add more application tools by using the SDK. These tools will be loaded when Remote Desktop Manager starts.

6.4 Content Area

Description

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

Existing dashboards are described further in their own help topics

[Sessions](#)
[Data Entries](#)

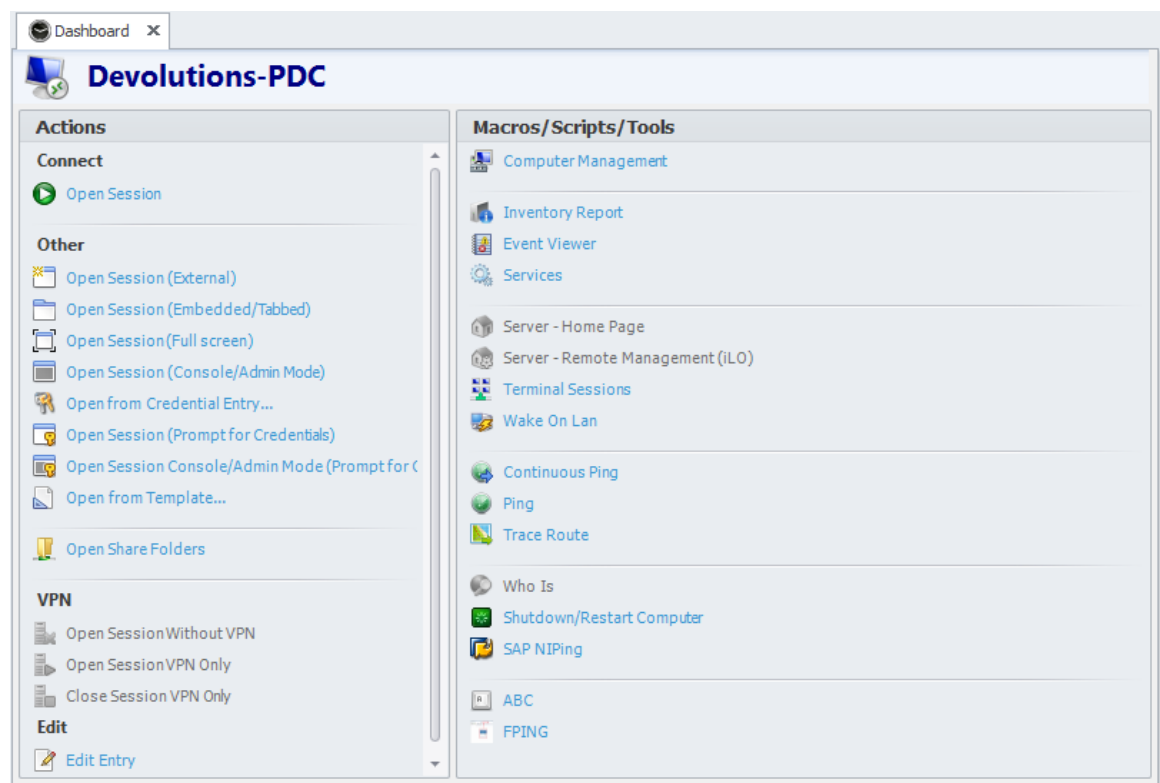
[Groups](#)
[Credentials](#)
[Macros/Scripts/Tools](#)

6.4.1 Dashboards

6.4.1.1 Sessions

Description

The dashboard displays a quick view showing possible actions, or information for the current entry. It contains the same actions that are found in the context menu and the ribbon. It's also possible to access the Macros/Scripts/Tools available for the current selection.

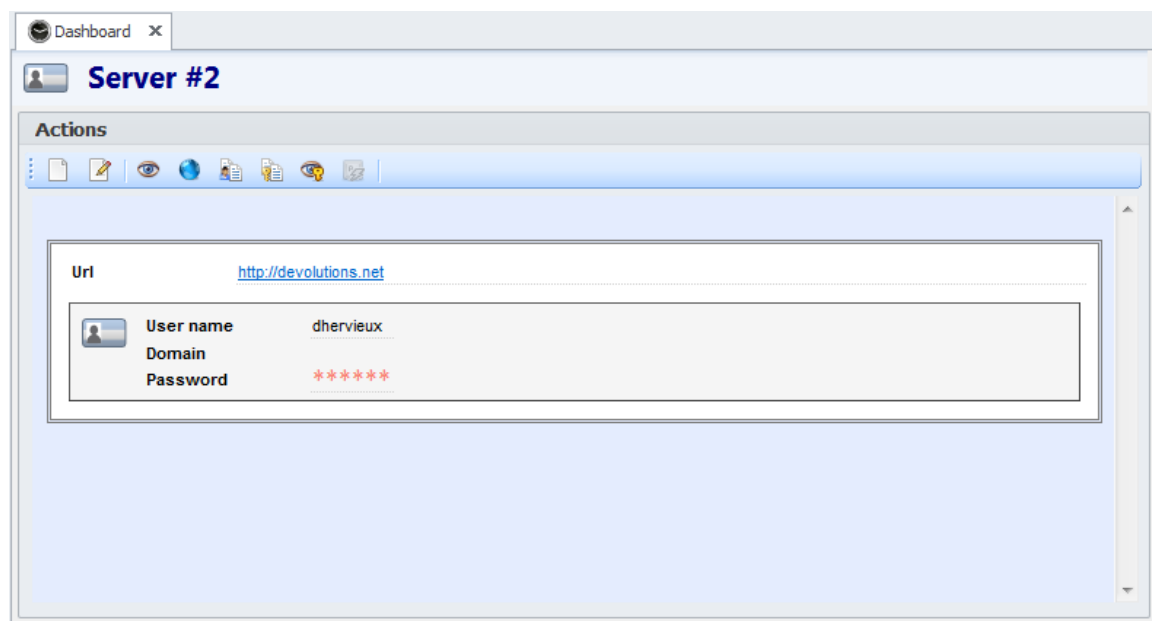


Dashboard for a specific session

6.4.1.2 Data Entries

Description

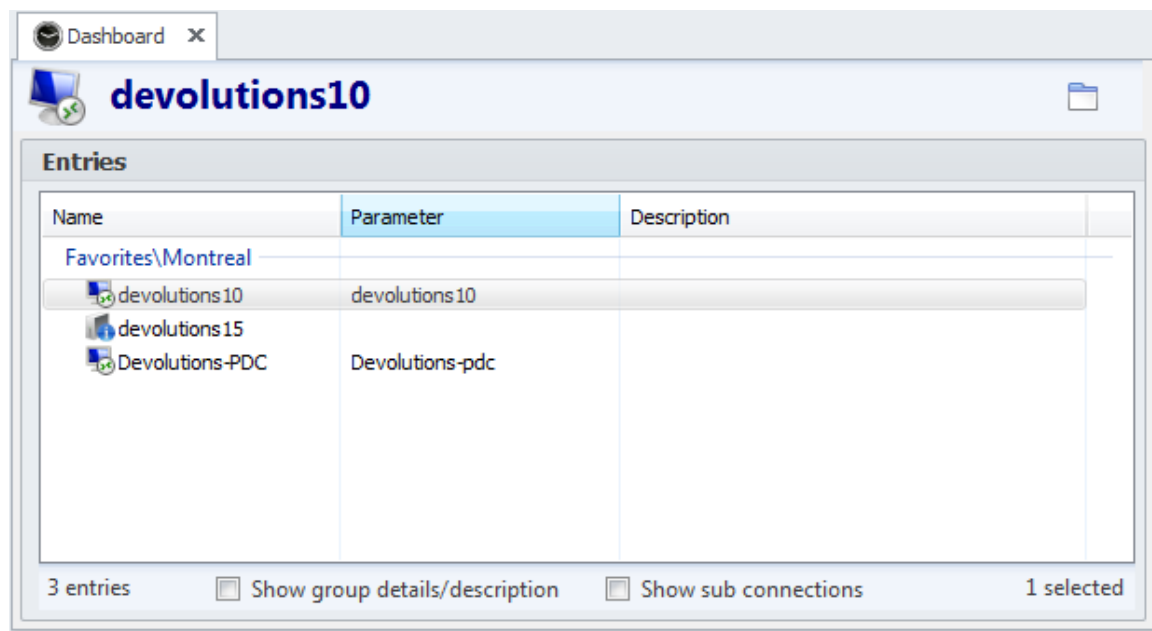
The dashboard displays a quick view showing possible actions, or information for the current data entry. It contains the same actions that are found in the context menu and the ribbon.



6.4.1.3 Groups

Description

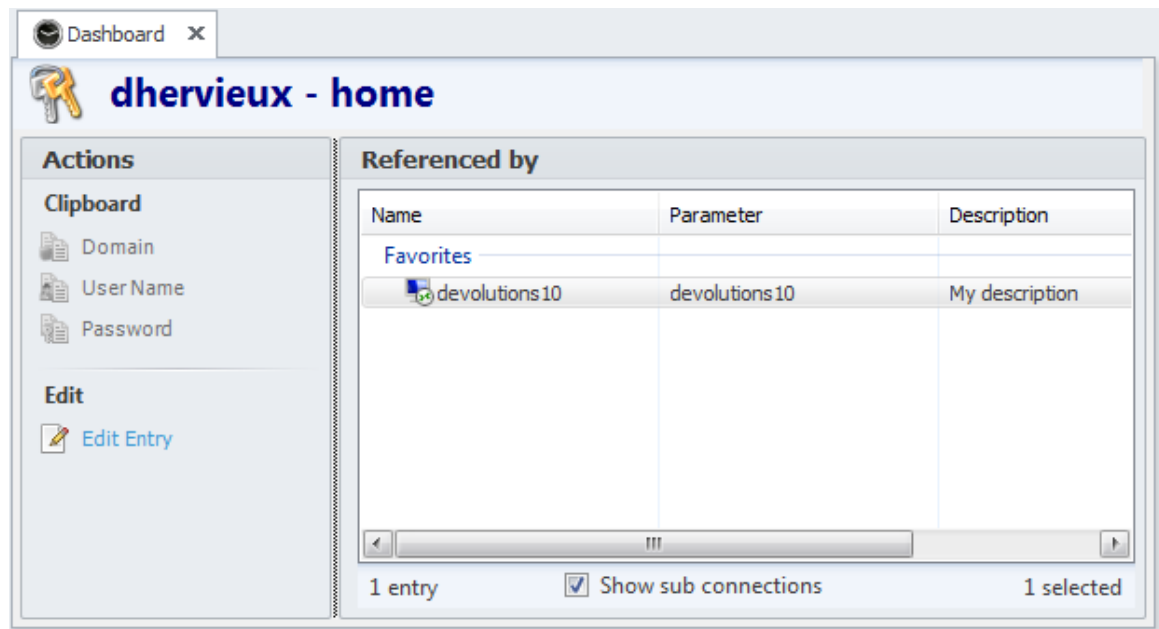
The dashboard displays the group entries. It's possible to display the group details directly or display only the information regarding the selected item.



6.4.1.4 Credentials

Description

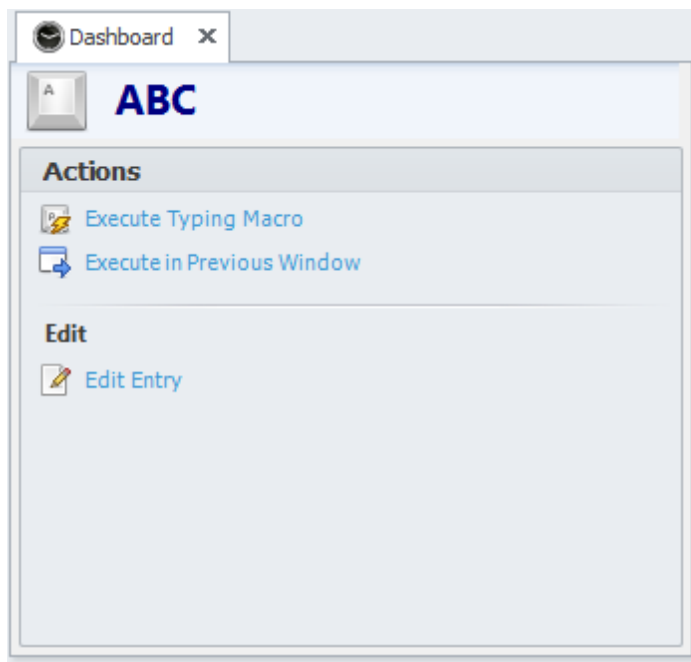
The dashboard displays a quick view showing possible actions, or information for the current credential entry. It possible to easily view which other entry use the current credential entry.



6.4.1.5 Macros/Scripts/Tools

Description

The dashboard displays a quick view showing possible actions for the current macro/script/tool. It contains the same actions that are found in the context menu and the ribbon.

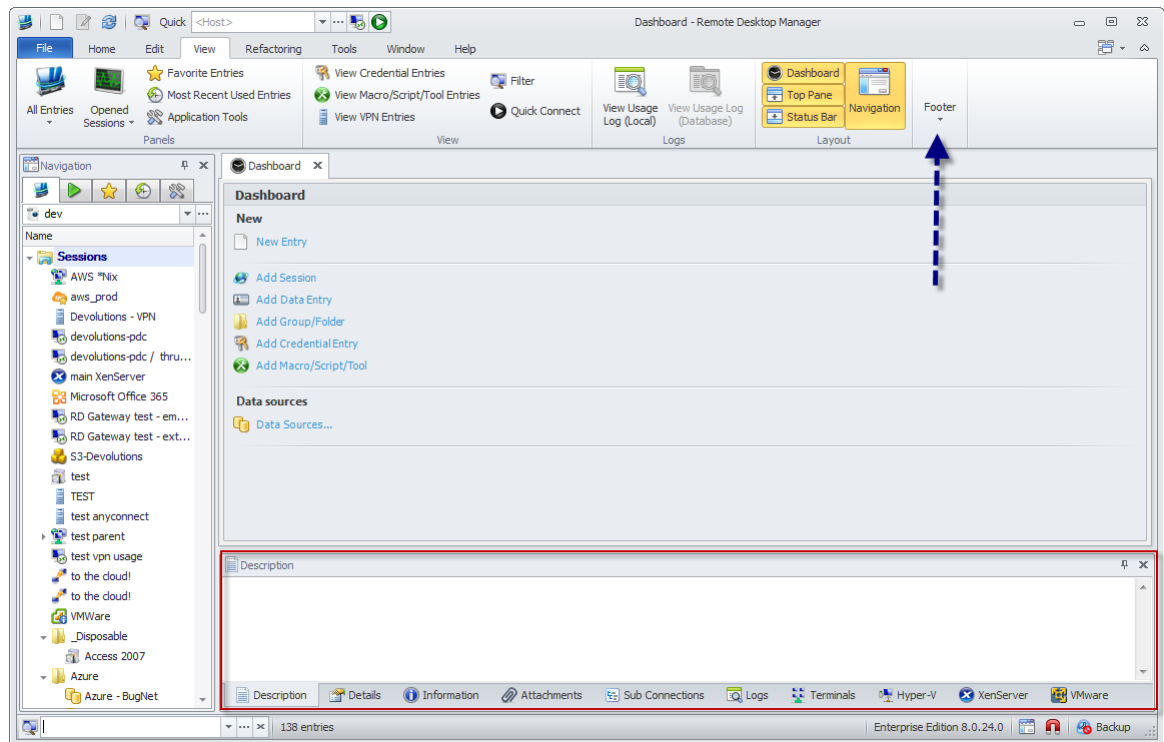


6.5 Panes (Footer)

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.

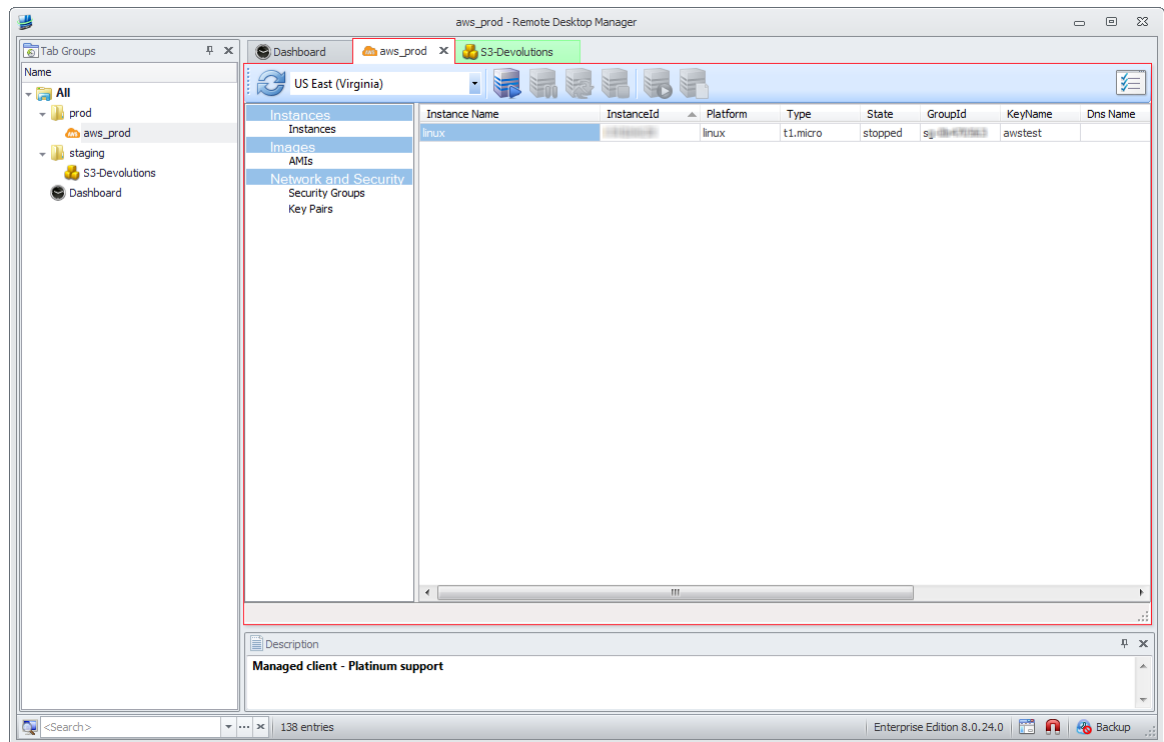
Use the View -> Footer commands to control the visibility of individual panes.



Footer area

Docked example

Here is a personalized setup, for the keyboard shortcut enthusiast and that manages a great number of session using tab groups.



Personalized setup

6.5.1 Attachments

Description

Allows you to add an attachment to an entry. The file is stored directly in the database.



The file will not be available in the offline mode.




Only available with an [Advanced Data Source](#)



Attachment list

The attachment can be any type and size, depending on your bandwidth and on the data source. You can also view a saved attachment from:

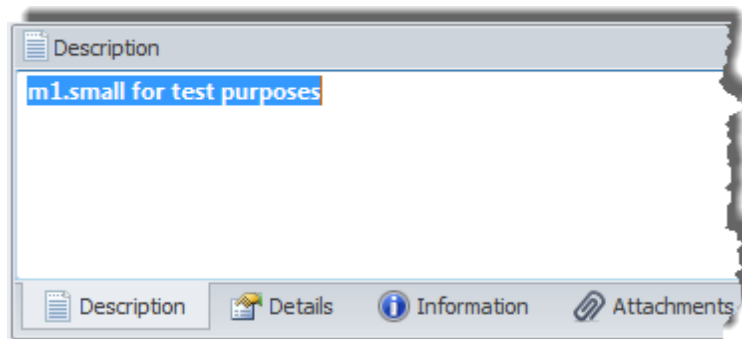
- the session context menu;
- the session properties; or
- directly on the dashboard.

The update button  will allow you to update directly your selected document. Use it to save your local modifications after an edit.

6.5.2 Description

Description

The Description pane displays the content of the Description field of the entry.



6.5.3 Details

Description

The connection details can be found on the dashboard, and is a simple grid that lists complete session information. The grid supports the copy/paste feature. Exporting is not available.

Dashboard		Details - DEVOLUTIONS-PDC x	
Description		Value	
Always Ask for Resources		False	
Authentication Level		ConnectDontWarnMe	
Auto Reconnection		False	
Connection Type		RDPConfigured	
Console / Admin Mode		False	
Data Source ID		a350631f-4368-4642-bb8e-76a5c2637ff1	
Description			
Desktop Composition		False	
Disable Bitmap Cache		False	
Disable Cursor Setting		False	
Disable Full Window Drag		False	
Disable Menu Animations		False	
Disable Themes		False	
Disable Wallpaper		False	
Display Monitor		Configured	
Domain			
Font Smoothing		False	
Group		Demo	

Connection detail grid from the dashboard

6.5.4 Hyper-V Console

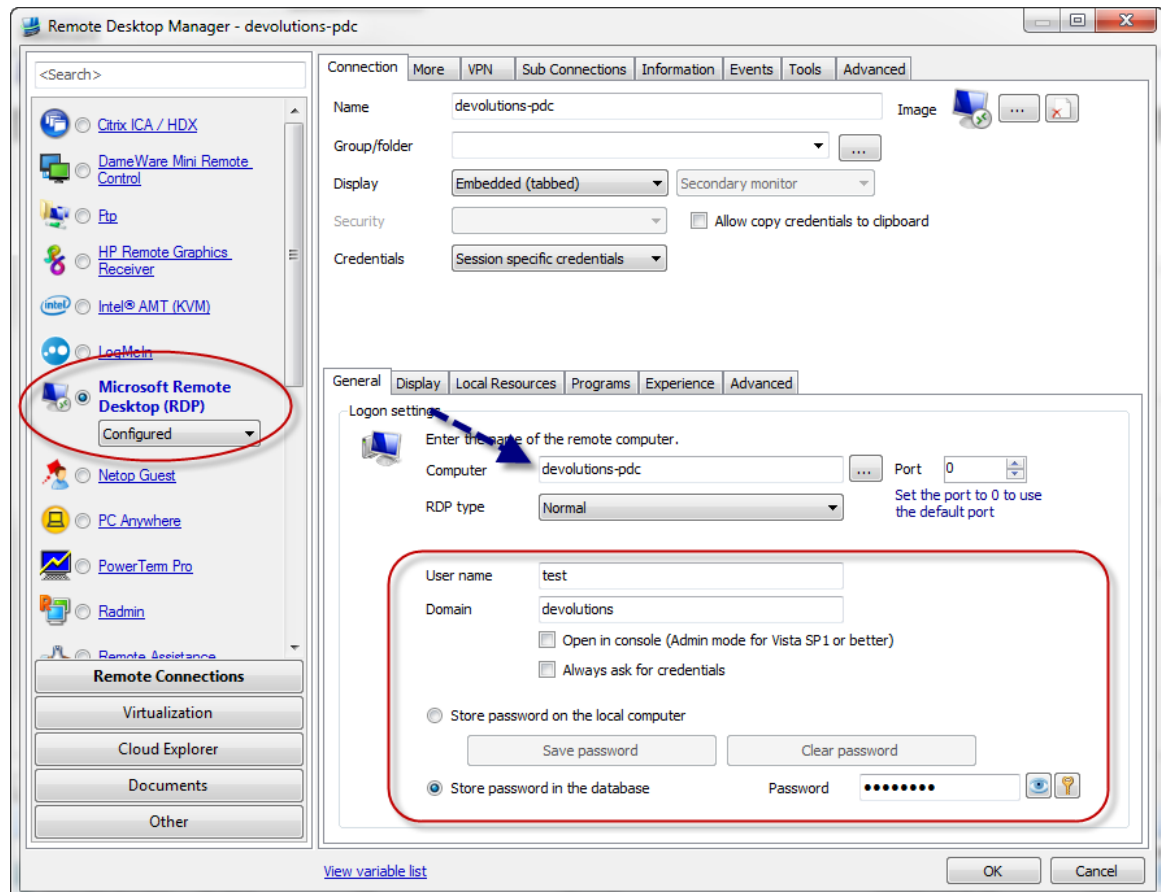
Dashboard

Remote Desktop Manager's Hyper-V Dashboard allows you to have quick glance at the Hyper-V instances running on the given Hyper-V server. Also allowing you to perform a few Hyper-V actions:

- Start
- Shutdown
- Save
- Pause
- Preview

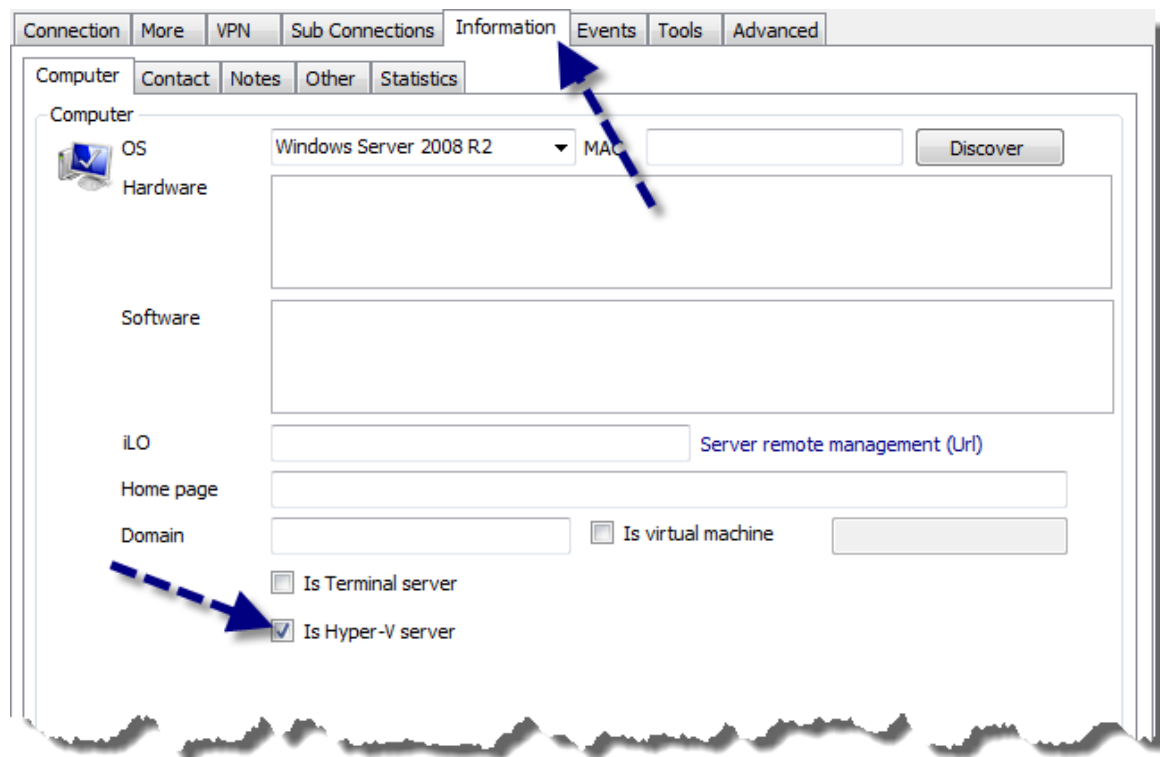
Setup

Create a new RDP session to the Hyper-V server making sure you specify the proper login credentials.



Create RDP session

On the Information tab, select "Is Hyper-V Server"



Enable Hyper-V

Hyper-V Console View

Description Details Information Terminals Hyper-V						
<div> Start Shutdown Save Pause Preview Host devolutions-gdt Auto refresh </div>						
Name	State	Health	Operational Status	Uptime	Last	
DEVOLUTIONS-PC	Enabled	OK	OK			
Win7 32bit Template	Disabled	OK	Stopped		3/22,	
Win7x32_320_2008R2	Enabled	OK	OK	2.05:32:26.8320000	3/20,	
Win7x32_VMG	Disabled	OK	Stopped		3/22,	
Win7x32_VMG	Disabled	OK	Stopped		3/22,	
Win7x32_VMGtemplate...	Enabled	OK	OK	2.05:32:11.4970000	3/20,	

Troubleshooting

Make sure you have specified credentials that have admin rights on the Hyper-V server, WMI ports are open and no firewalls are blocking the connections.

<http://blog.mpecsinc.ca/2009/06/hyper-v-error-access-denied-unable-to.html>

Does it work using Hyper-V Tools for Remote Administration? Try it.

<http://technet.microsoft.com/en-us/library/cc794756.aspx>

Links

[Hyper-V RDP](#)

6.5.5 Information

Description

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

Computer

The computer tab displays information that is mostly informative, as well as settings that indicate the entry is a dashboard that can be displayed in a separate pane.

The screenshot shows a web-based interface with a top navigation bar containing tabs: Connection, More, VPN, Sub Connections, Information (selected), Events, Attachments, Logs, Tools, and Advanced. Below this, a sub-navigation bar for the 'Computer' section includes tabs: Computer (selected), Contact, Notes, Other, and Statistics. The main content area is titled 'Computer' and features a left sidebar with icons and labels for OS, Hardware, Software, iLO, Home page, and Domain. The main panel contains several input fields and checkboxes. At the top, there is a dropdown menu, a 'MAC' label, an empty text field, and a 'Discover' button. Below this are three large empty rectangular boxes for OS, Hardware, and Software. Further down, there is an 'iLO' label, a text field, and a link 'Server remote management (Url)'. Below that is a 'Home page' label and a text field. At the bottom, there is a 'Domain' label, a text field, and a group of checkboxes: 'Is virtual machine', 'Is Terminal server', 'Is Hyper-V server', 'Is VMware server', and 'Is XenServer'. A large grey button is positioned to the right of the 'Is virtual machine' checkbox.

Computer tab

Contact

The contact tab displays information on a person that has a link to the entry. It could be the technician managing a remote machine.

The screenshot shows the 'Sub Connections' tab in the Remote Desktop Manager application. Under the 'Sub Connections' tab, there is a 'Contact' sub-tab. The 'Contact' sub-tab contains a form with the following fields:

- First name
- Last name
- Company
- Customer #
- Prefix
- Title
- Email
- Phone
- Fax
- Address
- City
- State
- Zip code
- Country
- Skype

At the bottom right of the form, there are two buttons: 'Email Contact' and 'Call (Skype)'.

Contact Tab

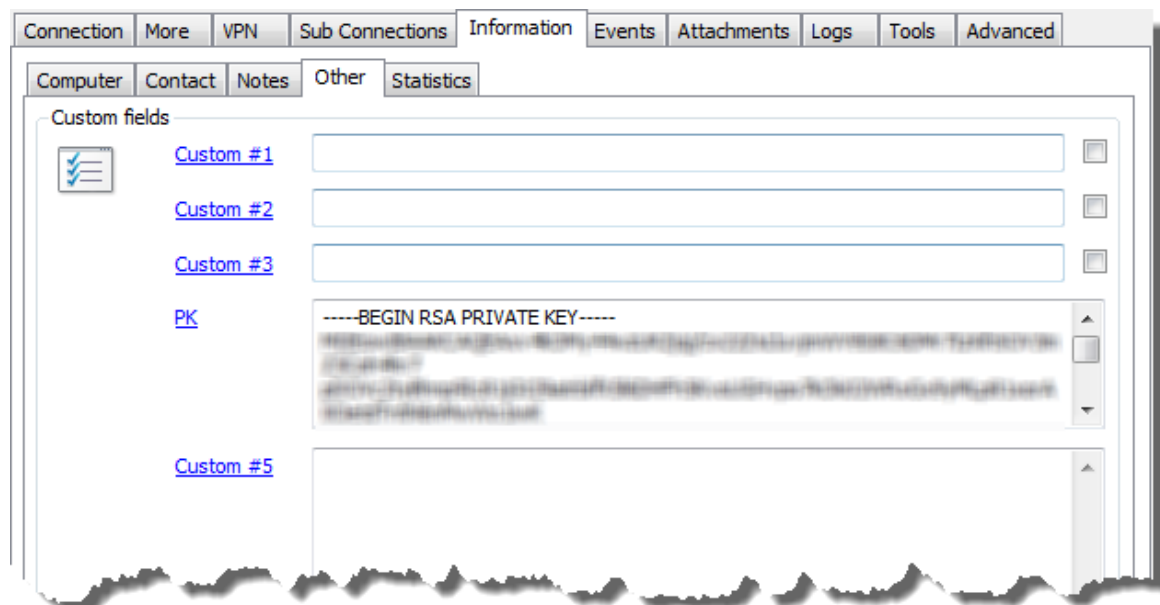
Notes

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

Others

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

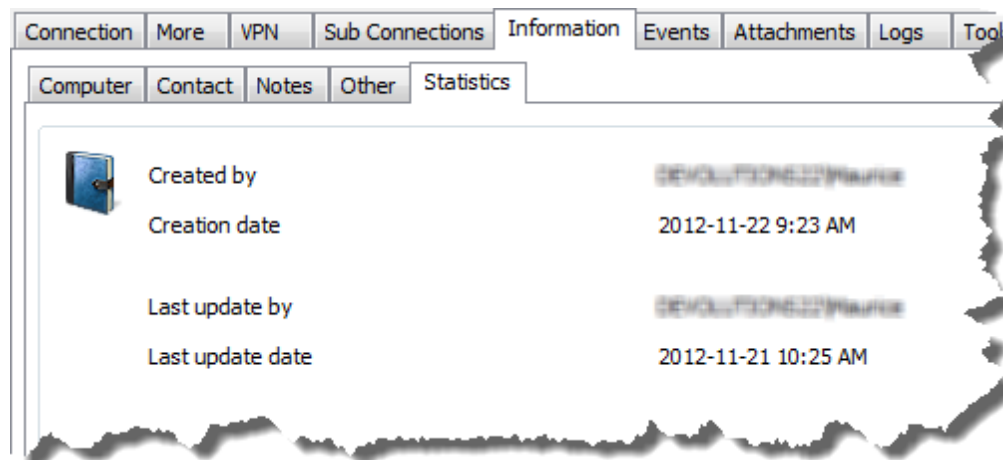
For ease of use, the labels can be modified to reflect the data you intend to store in them. Clicking on the label allows you to enter any caption you desire, as you can see in this screen capture where the custom field has been re-labeled PK as it is meant to contain a private key.



Other Tab

Statistics

The statistics tab simply displays some information on the creation and last modification of the entry.



Statistics Tab

6.5.6 Logs

Description

This pane displays the [Usage Logs \(Global\)](#) saved in the database.

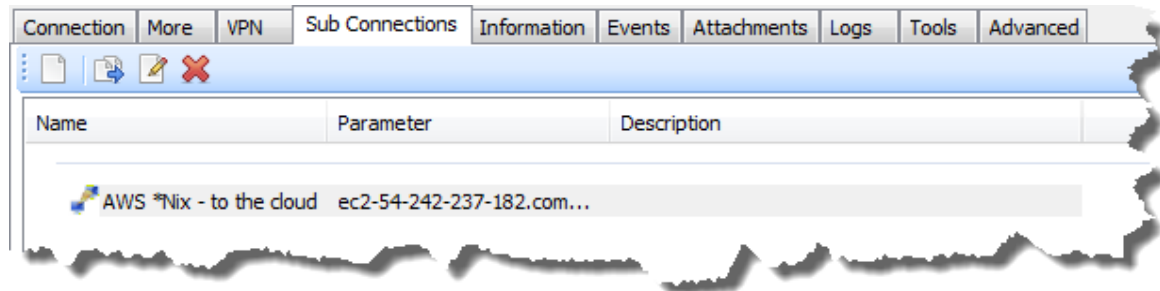


Only available with an [Advanced Data Source](#)

6.5.7 Sub Connections

Description

The Sub Connections tab is only visible when you have defined sub connections for the current entry.



Sub Connections Tab

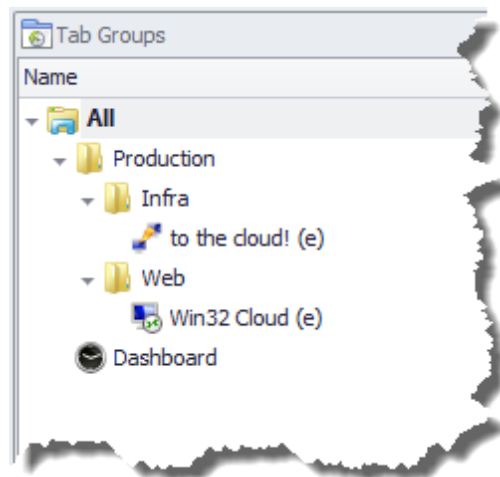
Please refer to the Sub Connections [Overview](#) topic for more information.

6.5.8 Tab Groups

Description

Tab Groups are a functionality to help organize the running sessions. Evidently it is of use for those who run a lot of sessions concurrently.

Much like the Group/Folder feature that helps organize your sessions, a hierarchical structure can be easily implemented.



Tab groups in action

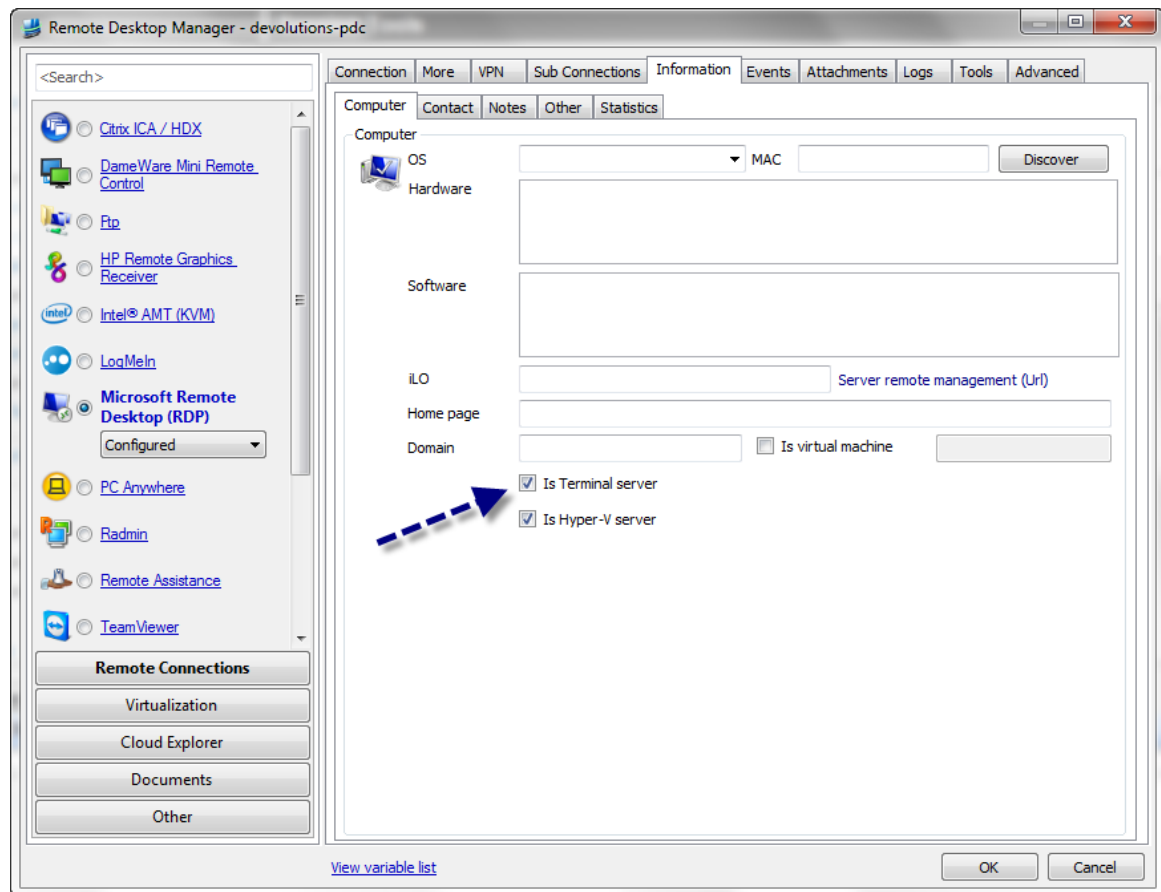
Please refer to the [Tab Page Category/Color](#) topic for full details on this feature.

6.5.9 Terminal Services Console

Description

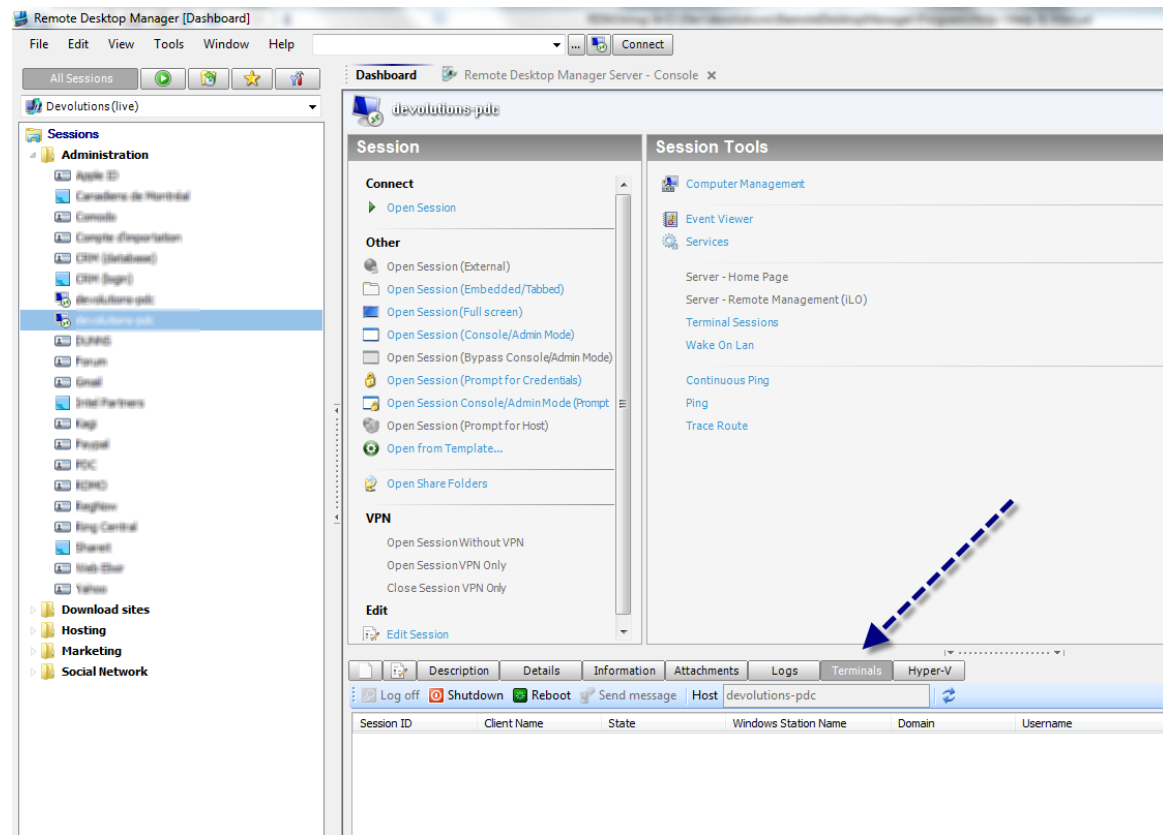
You need to check the "Is Terminal server" box to see the Terminal Service Dashboard by editing your

session in the tab pages **Information->Computer**



Terminal Server Console

Pane



Dashboard

6.5.10 VMware Console

Dashboard

Remote Desktop Manager's VMware Dashboard allows you to have quick glance at VMware instances. Allowing you to perform many actions:

- Power on
- Power off
- Suspend
- Shut down guest
- Restart guest
- Connect
- Create new connection

Prerequisites

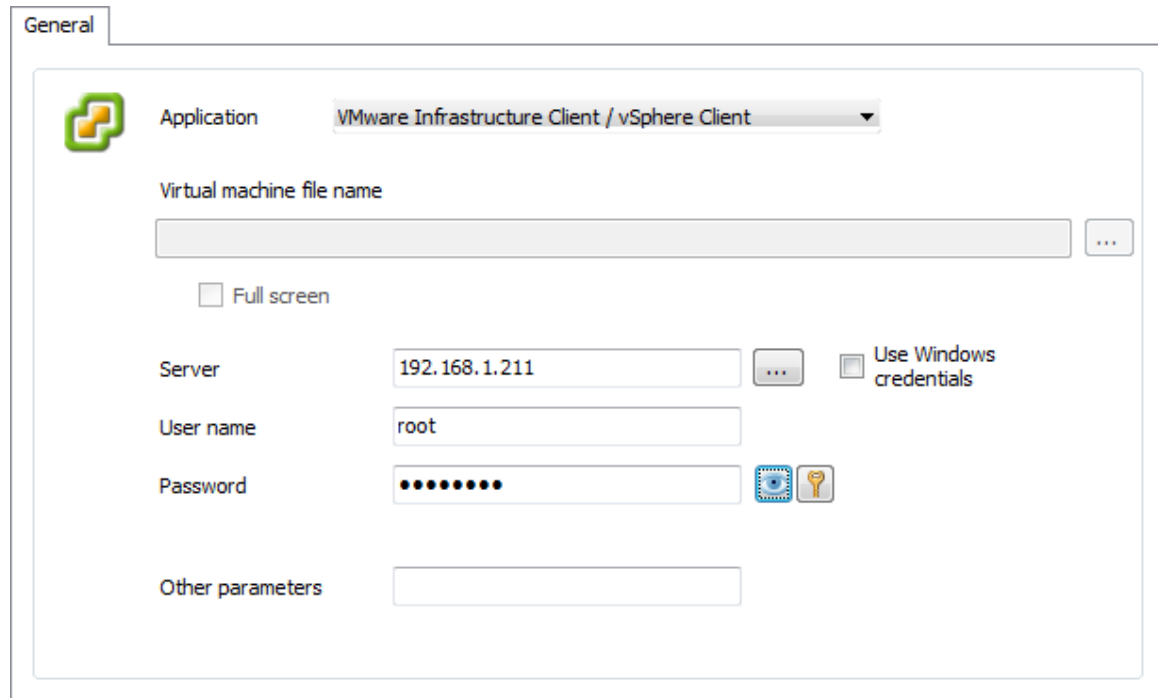
If you don't yet have the file VMware.Vim.dll & its associated dll files installed & registered on your system please download and install [vSphere PowerCLI](#)

Using any web browser navigate to your VMware server and install the associated SSL certificate.

Setup

Create a VMware vSphere Client or VMware Remote Console session (other session types will also work).

Set the host, username and password of the VMware server you want to connect.

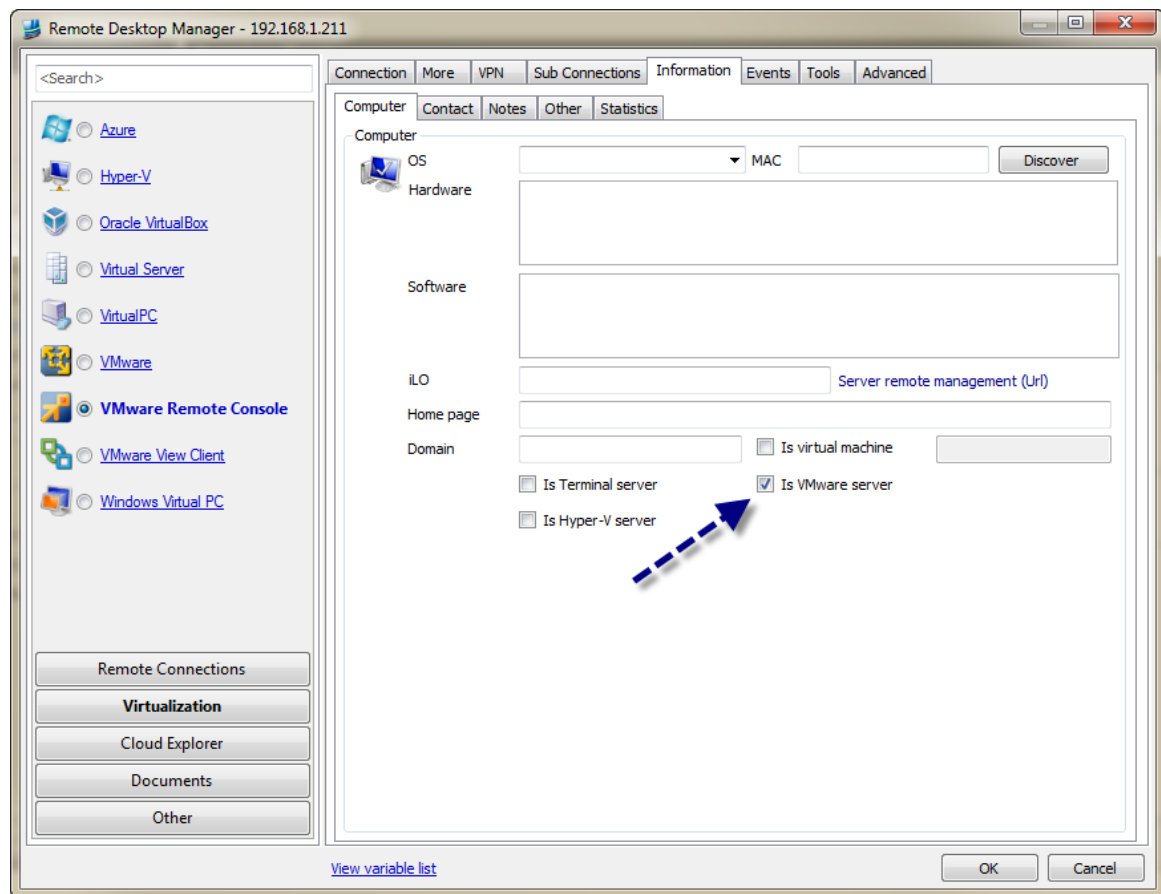


The screenshot shows a window titled "General" with a VMware logo icon. It contains the following fields and options:

- Application:** A dropdown menu set to "VMware Infrastructure Client / vSphere Client".
- Virtual machine file name:** A text input field with a browse button (three dots) to its right.
- Full screen:** An unchecked checkbox.
- Server:** A text input field containing "192.168.1.211" and a browse button (three dots) to its right.
- User name:** A text input field containing "root".
- Password:** A text input field with masked characters (dots), a "Show/Hide" eye icon, and a "Use Windows credentials" checkbox.
- Other parameters:** A text input field.

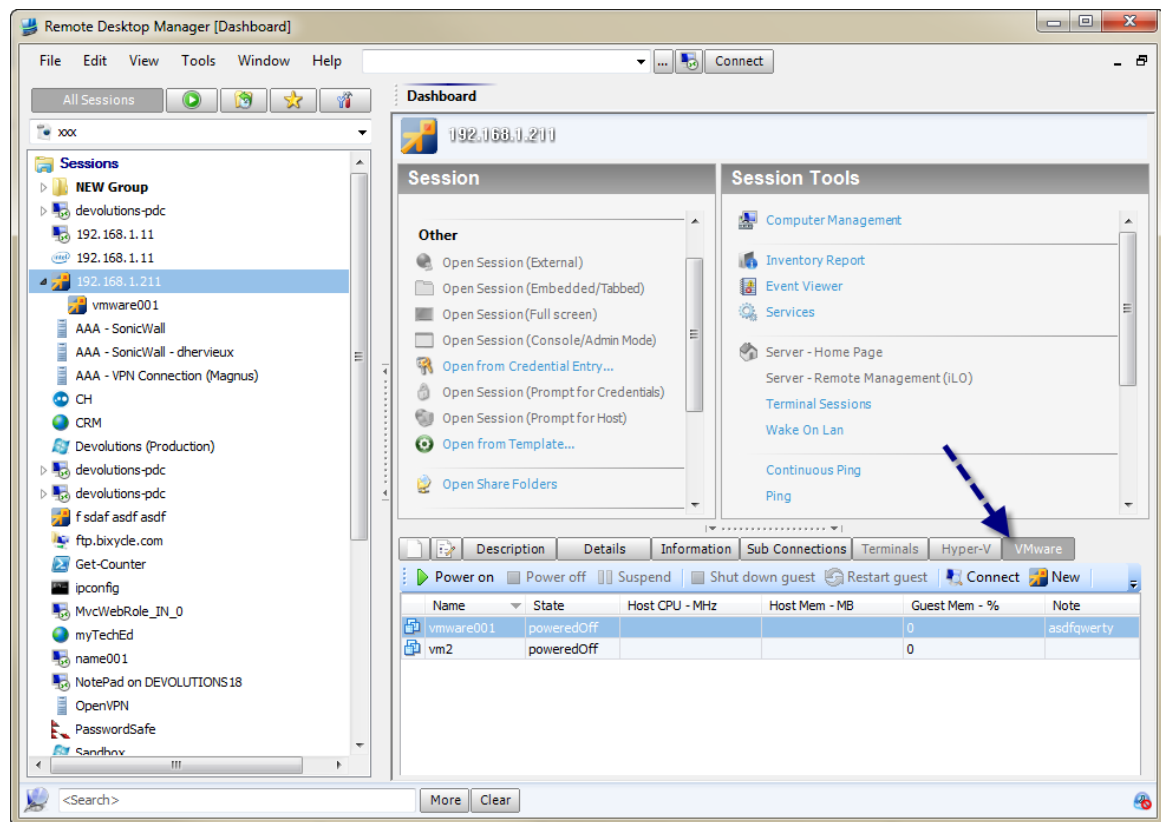
VMware session information

Next, you need to check the "Is VMware server" box to activate the VMware dashboard by editing your session in the tab pages **Information** -> **Computer**.



Enable VMware dashboard

VMware Console View



VMware Dashboard

Troubleshooting

If you get "ERROR System.IO.FileNotFoundException: Could not load file or Assembly "VMware.Vim, Version=5.0.0.0, Culture=neutral, PublicKeyToken=10980b081e887e9f"..."

Install [vSphere PowerCLI](#)

See also

[VMware](#)

6.5.11 XenServer Console

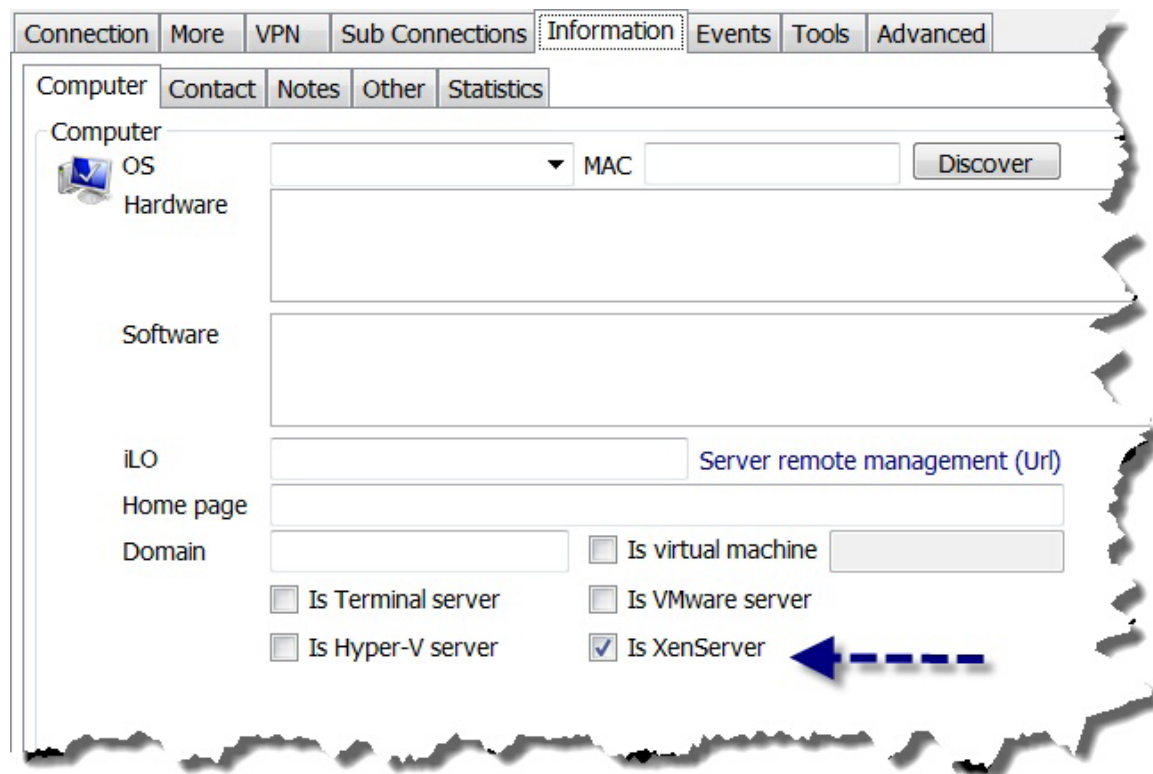
Description

Remote Desktop Manager's XenServer Dashboard allows you to have quick glance at XenServer instances.

Prerequisites

Nothing is required apart from your credentials to access a XenServer.

Settings



Information | Computer tab.

Create an RDP connection to your XenServer server, in addition check the "Is XenServer" checkbox on the **Information | Computer** tab.

Workflow

The console is essentially the same as the dashboard. Please refer to [XenServer](#).

6.6 Status Bar

Description

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

- Search/Filter Area
- Remote Desktop Manager version label
- Navigation pane toggle
- Grab input toggle



Status bar

Search/Filter Area

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

Remote Desktop Manager version label

This displays the Edition and Version information for Remote Desktop Manager. Double click on the label to display the registration form.

Navigation pane toggle

This button toggles the visibility of the Navigation Pane. Much like the Top Pane of the [Quick Access Toolbar](#), this allows more display area for embedded sessions. Its associated keyboard shortcut is Alt+F8

Grab input toggle

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

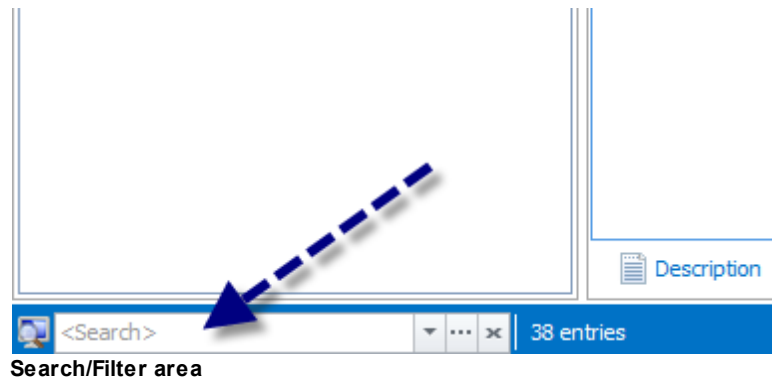
6.6.1 Search/Filter

Description

It is possible to apply a filter in the Navigation Pane tree view by typing some characters in the filter box. The filter is applied using the specified settings in the application options.

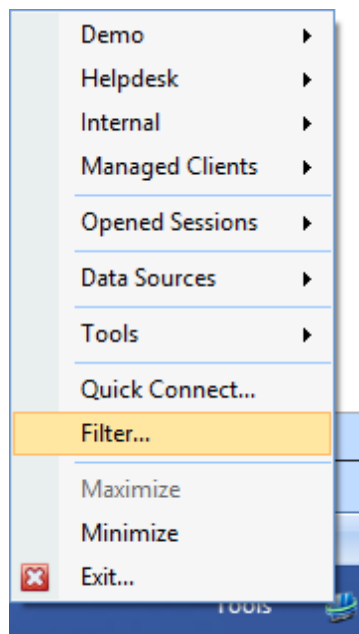
Settings

Status bar



The search/filter is in the Status Bar, select the ellipsis button to display the options.

Trayicon



Filter in trayicon

The search/filter is also available from the trayicon. Right-click on the Remote Desktop Manager [trayicon](#) and select Filter.

Keyboard Shortcut

Use the keyboard shortcut CTRL+F to quickly set focus in the Search/Filter control. This can be disabled in [File -> Options -> Keyboard](#).

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

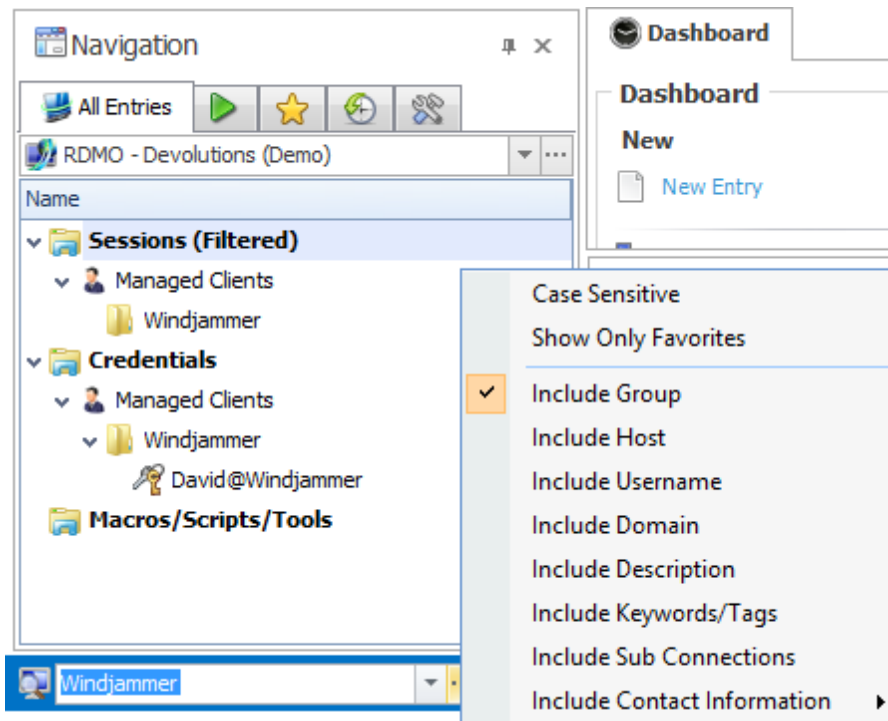
Filter Expression

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

- Session name
- Group name
- Host
- Description
- Keywords
- Sub Connections
- Various Contact information fields (choose them in the sub menu)

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



Filter box and menus

If the Navigation Pane tree view is hidden, a dialog will appear with the filtered content.

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, don't use unless you are looking for (")
- Token leading/trailing white-spaces are trimmed

Examples (this will work)

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

Examples (this will not work as expected)

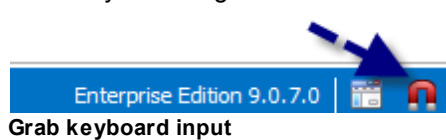
- Laptop && "Baton Rouge"
 - Will work but filter for the string "Baton Rouge" and not the string Baton Rouge
- Laptop && (Baton Rouge || Boise)
 - Will work but filter for Laptop and the string (Baton Rouge || Boise)

6.6.2 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.



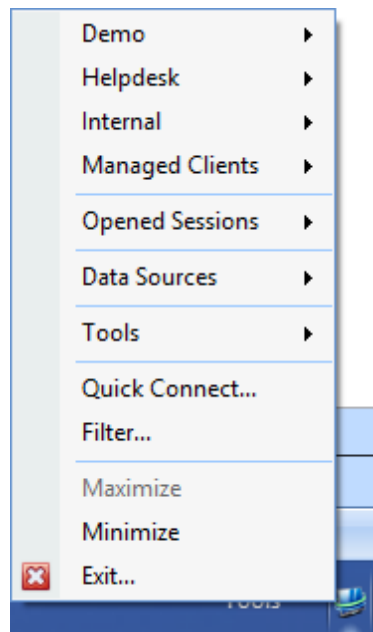
6.7 Tray Icon

Description

Remote Desktop Manager also lets you show the sessions list and other useful information in the Windows system tray.

You can also customize the content. To open a session, click on it or use the context menu by right-clicking on the icon to access more options.

The application's options window contains many settings that enable you to customize the system tray icon settings. You can also disable it from here, or change its default behavior.



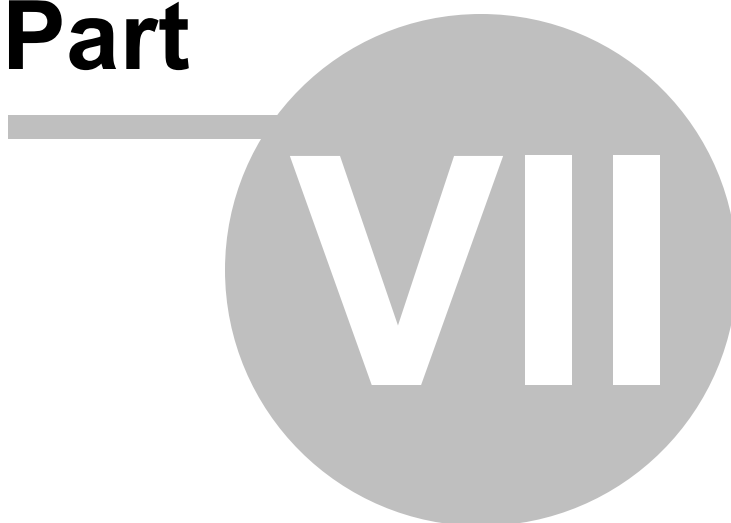
Trayicon view

Option	Description
--------	-------------

Sessions List	Shows the sessions from the current data source. Sessions are listed by default, you it's also possible to include only those who are marked as favorites.
Opened Sessions	Lists all the opened sessions exactly like the opened sessions view.
Data Sources	Lists the available data sources and allows the user to switch dynamically from one to another. This section only appears if it's enabled and more than one data source is configured.
Tools	Lists all the configured tools like the configured tools View .
Quick Connect	Prompts for the Quick Connect dialog to open an add-hoc connection with a specific type or a selected template.
Filter	Launch the Search/Filter to make research inside the application.
Maximize	Display the application in full screen.
Minimize	Minimize the application in the task bar.
Exit	Close the application

How-to

Part



7 How-to

7.1 How-to understand Remote Desktop Manager licensing

Description



Licenses are calculated per user, not per installation. There is no limitation on installing Remote Desktop Manager, as long as you have the proper number of licenses for the users of your system.

Depending on how many licenses are needed, there's 3 license packs available:

- User
- Site
- Global

User

With a User license, each user requires a license. You will receive 1 license key per user license.

Site

With a Site license, you can have unlimited users in the same site (location). You will receive 1 license key and this key will grant a license for every users in the same location.

Global

With a global license, you can have unlimited users in unlimited locations. You will receive 1 license key and this key will grant a license for every users in every locations.

7.2 How-to configure the Yubikey 2-Factor Authentication

Description

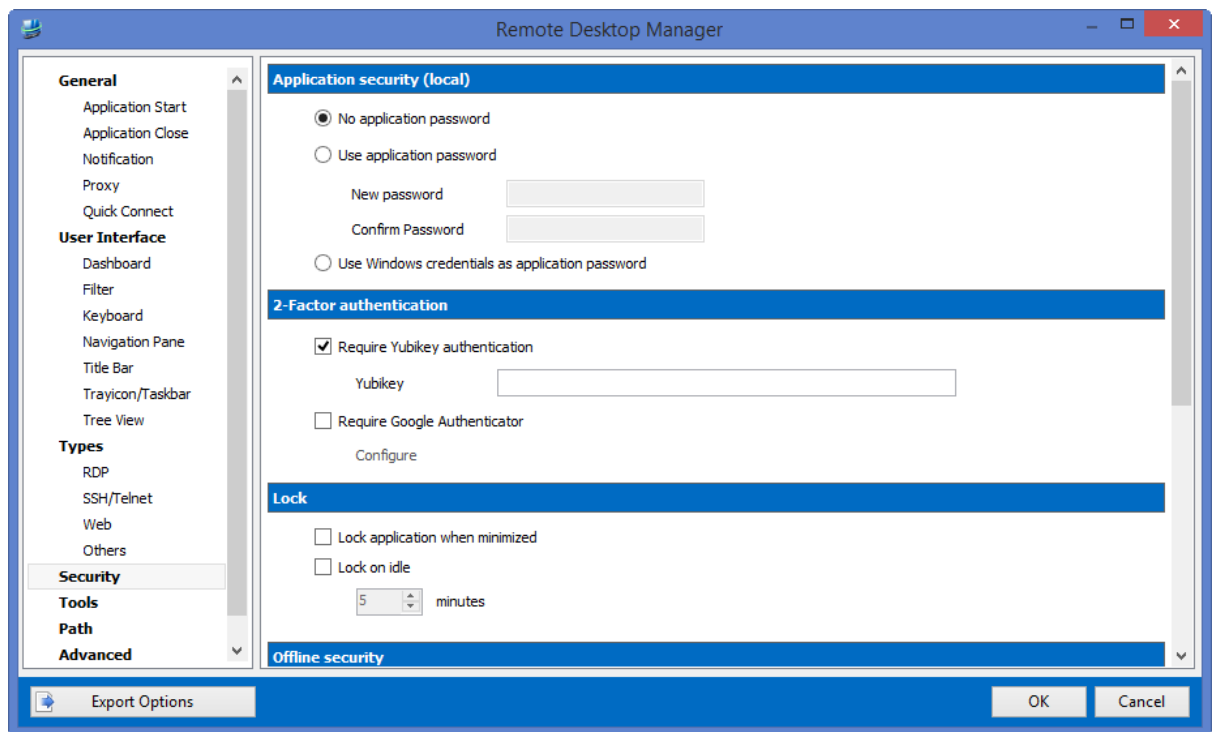
Remote Desktop Manager allow you to configure a Yubikey to provide an additional layer of security when the application opened.

Settings



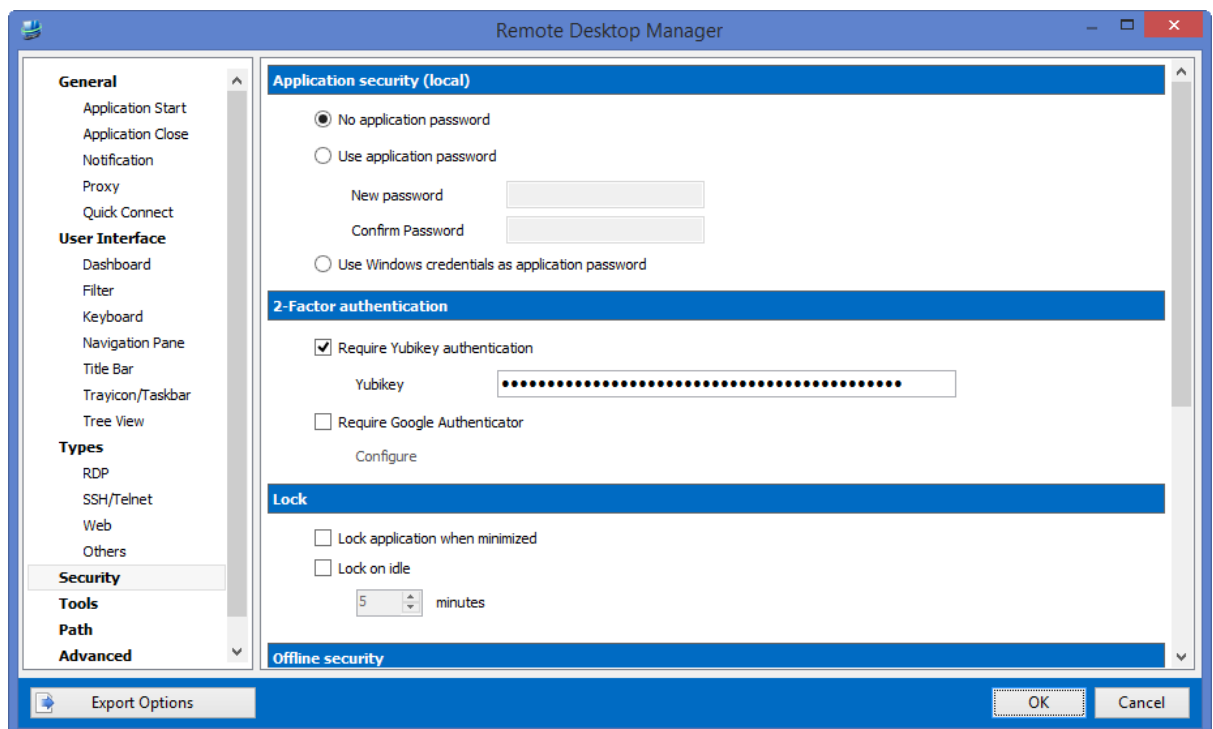
Before you start the configuration, make sure you have in your possession a [Yubikey](#).

1. Insert the Yubikey into a USB port on your computer.
2. Click on **File -> Options -> Security** and select **Require Yubikey authentication** in the 2-Factor authentication section.



Yubikey authentication

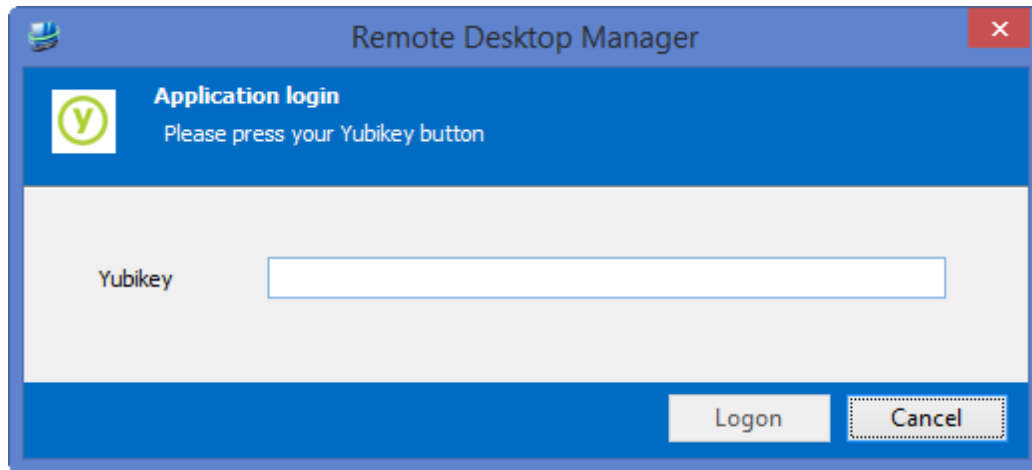
3. Press and hold the gold button on the Yubikey to have a Yubikey code generate in Remote Desktop Manager and click **OK**.



Yubikey Password

4. Close and reopen Remote Desktop Manager to be prompt to enter the Yubikey code to access the

application.



Yubikey code

5. Press and hold the gold button on the Yubikey and access will be granted without pressing anything else.

7.3 How-to configure the Google Authenticator 2-Factor Authentication

Description

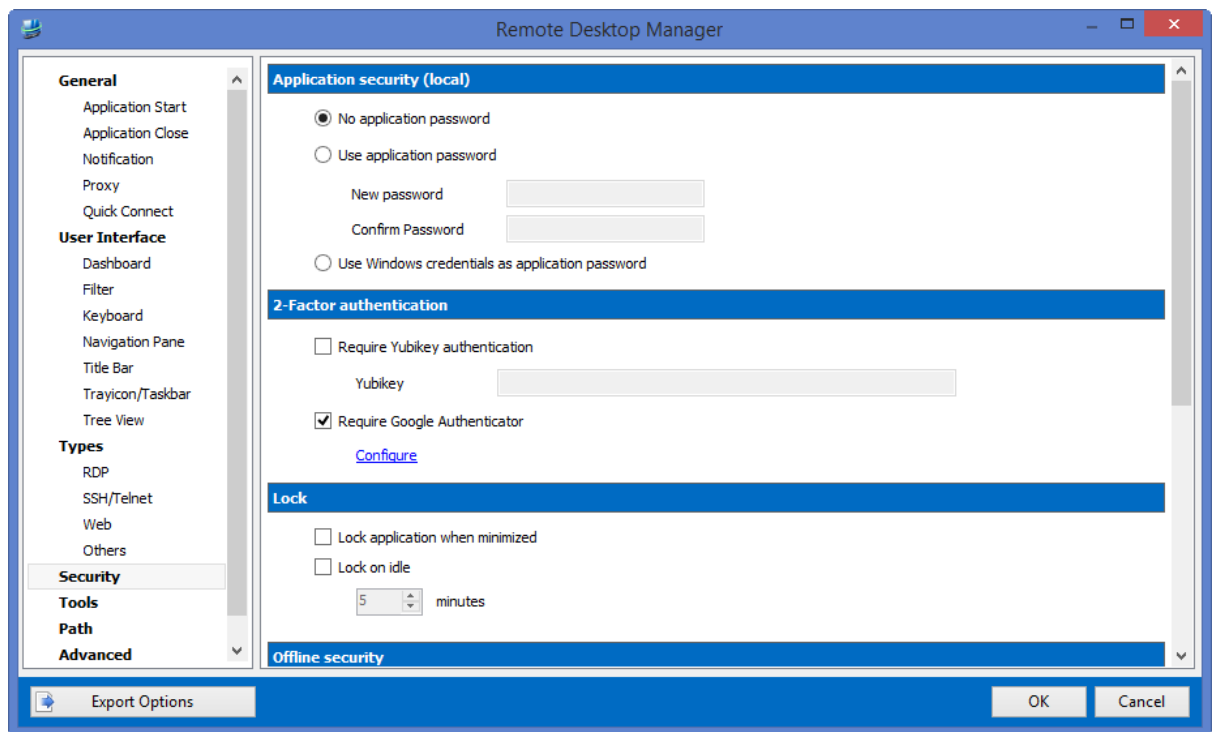
Remote Desktop Manager allow you to use Google Authenticator to provide an additional layer of security when the application opened.

Settings



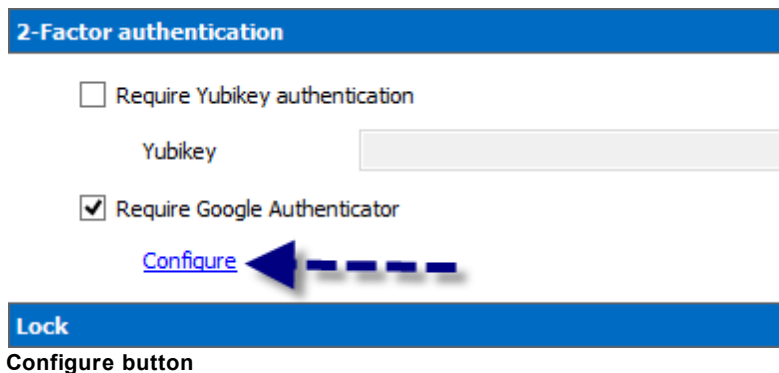
Before you start the configuration, make sure you have installed the [Google Authenticator](#) application on your Android device, Blackberry or on your Apple product (iPhone, iPad or iPod Touch).

1. Click on **File -> Options -> Security** and select **Require Google Authenticator** in the 2-Factor authentication section.



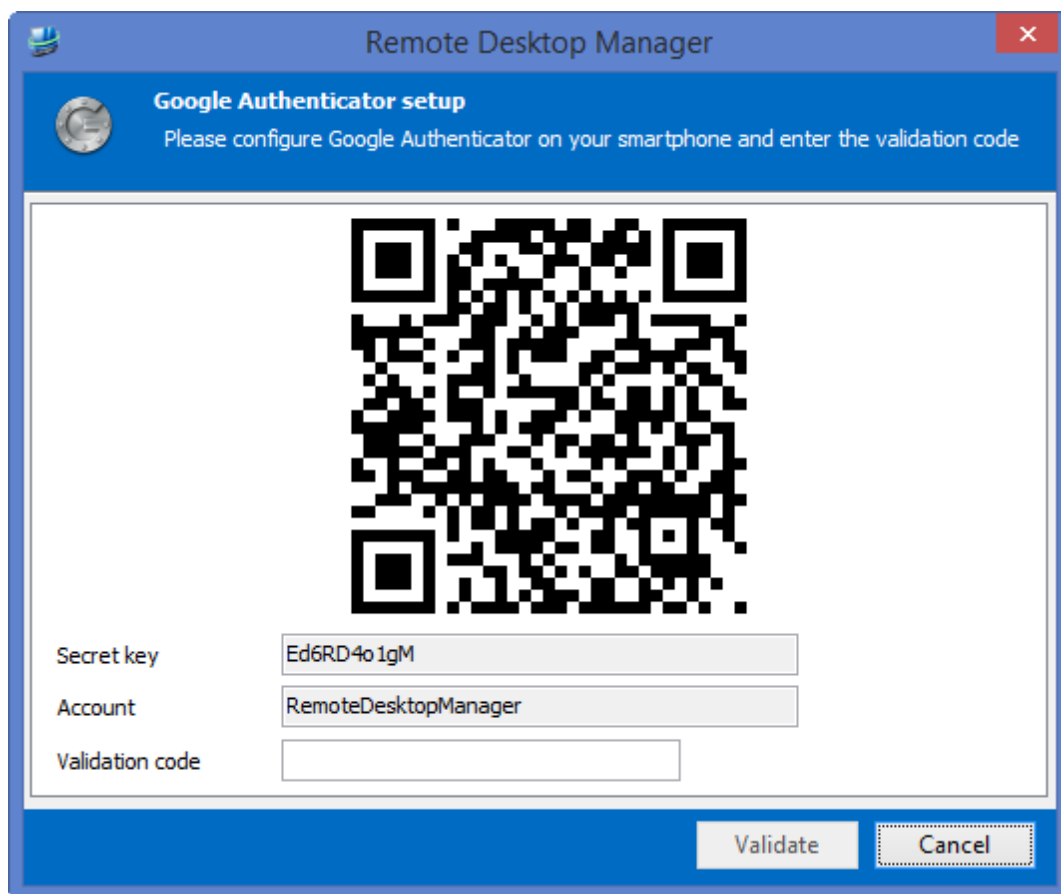
Google Authenticator

- Click on **Configure**.



Configure button

- Scan the barcode on your screen with the Google Authenticator application to setup Remote Desktop Manager in Google Authenticator.
When Remote Desktop Manager is configure in Google Authenticator, enter the Validation code provided by Google Authenticator in Remote Desktop Manager.



Scan barcode

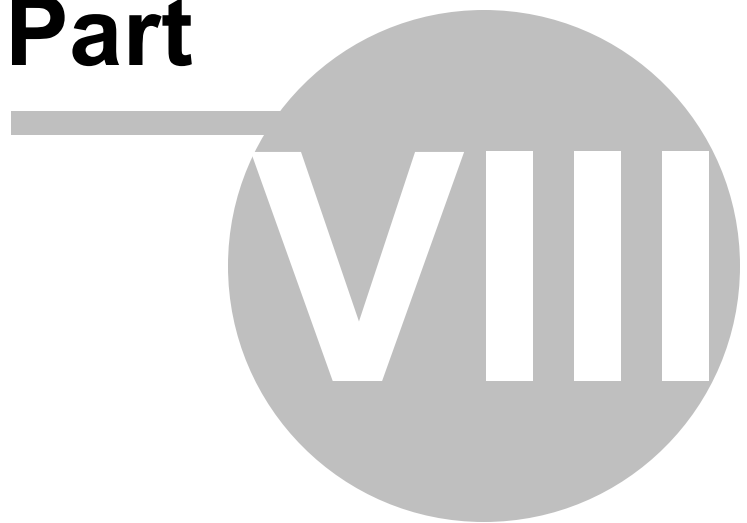
4. When the Validation code is enter, click on **Validate** and **OK**.
5. Close and reopen Remote Desktop Manager to be prompt to enter the Google Authenticator code to access the application.



Google Authenticator generate a new validation code every 30 seconds.

Support/Resources

Part



8 Support/Resources

8.1 Command Line Arguments

Usage

Remote Desktop Manager can be executed in a command line. However, some features are only available in the Enterprise edition.

usage: RemoteDesktopManager.exe [parameters]

Parameters	
{filename [* .rdm]}	Open in embedded or external mode the connection from file name.
/Silent	Execute the application minimized in a system tray icon. This option cannot be combined with other parameters.
/Datasource:{datasource id}	Specify the data source id (available in the Advanced Tab of the session).
/Session:{session ID};{session ID} /UserName:{username} /Password:{password}	Specify one or more session IDs (available in the Advanced Tab of the session)
/ChangePassword:{new password}	Change the session password. Only available for Remote Desktop sessions and embedded passwords. The data source ID and the session ID are required.
/RegisterUser:"{registration user}"	Change the Remote Desktop Manager registration name. The value must be in double quotes.
/RegisterSerial:"{serial number}"	Change the Remote Desktop Manager serial number. The value must be in double quotes.
/Template:{local template ID} /Host:{host name} /UserName:{username} /Password:{password}	Open the template with the specified host name and an optional username/password.
/Profiler	Starts the profiler at start of application. Good for profiling the start process.






8.2 Follow Us

Overview

Get the hottest information about our products - tips and tricks, case studies and new release announcements!

This is not a marketing newsletter. We focus on the issues that matter to you, whether you're looking for up-to-the-minute software tutorials, additional outside resources, or a peek at how others are using our products.

Links

	Facebook	http://facebook.remotedesktopmanager.com
	LinkedIn	http://linkedin.remotedesktopmanager.com
	RSS feeds	http://rss.remotedesktopmanager.com
	Twitter	http://twitter.remotedesktopmanager.com
	YouTube	http://youtube.remotedesktopmanager.com
	Blog	http://blog.remotedesktopmanager.com
	Google+	http://plus.remotedesktopmanager.com/
	Spicework	http://spice.devolutions.net
	Forum	http://forum.devolutions.net

8.3 Keyboard Shortcuts

Description

Here are the default keyboard shortcuts for various commands. These can be modified in **File -> Options -> Keyboard**. For more information please consult [Keyboard](#)

Actions

Action	Shortcut
Clipboard - Connection String	Ctrl+Alt+H
Clipboard - Domain	Ctrl+Alt+B
Clipboard - Host Name	Ctrl+H
Clipboard - Password	Ctrl+Shift+B
Clipboard - Url	Ctrl+Shift+H
Clipboard - User Name	Ctrl+B
Execute Typing Macro	Ctrl+Shift+A

Edit

Action	Shortcut
Add Credential Entry	Alt+Shift+N
Add Data Entry	Ctrl+Alt+N
Add Group/Folder	Ctrl+Shift+N
Add Session	Ctrl+N
Delete Entry	Ctrl+Del
Duplicate Entry	Ctrl+D
Edit Entry	Ctrl+E
Edit Entry (Local Machine Specific Settings)	Ctrl+Alt+E

Edit Entry (User Specific Settings)	Ctrl+Shift+E
New Entry	Ins
Rename Entry	F2

General

Action	Shortcut
Filter	Ctrl+F
Focus Dashboard	Ctrl+Shift+L
Focus Tree/List	Ctrl+L
Help	F1
Quick Connect	Ctrl+Alt+Q
Refresh	F5

ImportExport

Action	Shortcut
Export Entry as Remote Desktop File (.rdp)	Ctrl+Shift+E
Export Selection (.rdm)	Ctrl+Alt+E
Import Entries (.rdm, .pvm, .vnc, .rdp)	Ctrl+Shift+I

View

Action	Shortcut
Dashboard	Alt+F6
Details	F12
Entry List Pane	Alt+F8
Favorite Entries	F10
Footer Pane	Alt+Shift+F7
Grouped Tab Pane	Ctrl+Alt+F9
Header Pane	Alt+Shift+F6
Large Icons	F6
List	F4
Most Recent Used Entries	F9
Opened Sessions	F8
Status Bar	Alt+F7
Tabbed Entries Pane	Alt+F9
Tiles	F3
Top Pane	Alt+F11
Tree View	F7
View Usage Log (Local)	F11

8.4 Lexicon

Description

Remote Desktop Manager is a feature rich program 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, a database (either local or shared), or our own *Remote Desktop Manager Online* service. You can use multiple distinct data sources in the program, 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 and sometimes even sub-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 program, or even by an external source.

Data entry

A data entry is meant to contains various information like account information, emails, serial numbers. It's principal use in Remote Desktop Manager is to hold Web site information, from the URL to the credentials. This allows auto login 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 address or 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, but the term **Connection** is broader in scope and is now our preferred term.

8.5 Technical Support

Standard Edition (Free)

Support is solely through our online forums at <http://forum.devolutions.net/>.

Enterprise Edition

Holders of a valid license can obtain free support for Remote Desktop Manager. Please email any

questions or suggestions to support@devolutions.net.

You are also encouraged to find information and ask questions in our forums at <http://forum.devolutions.net/>. They contain years of relevant information and have the benefit of being enriched for the whole community when we post an answer.

8.6 Add-on Documentation

8.6.1 Overview

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](#) for more details on how to install or manage Add-ons.

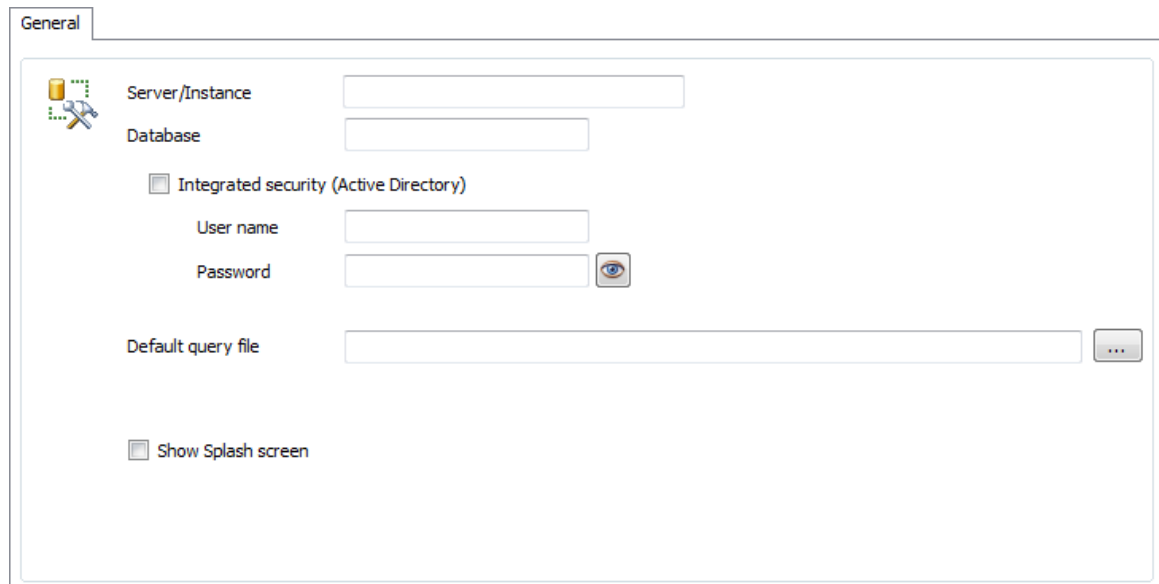
8.6.2 SQL Server Management Studio Add-On

Description

This add-on allows you to launch Sql Server Management Studio 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.

Settings



The screenshot shows the 'General' settings tab for the SQL Server Management Studio Add-on. It includes the following fields and options:

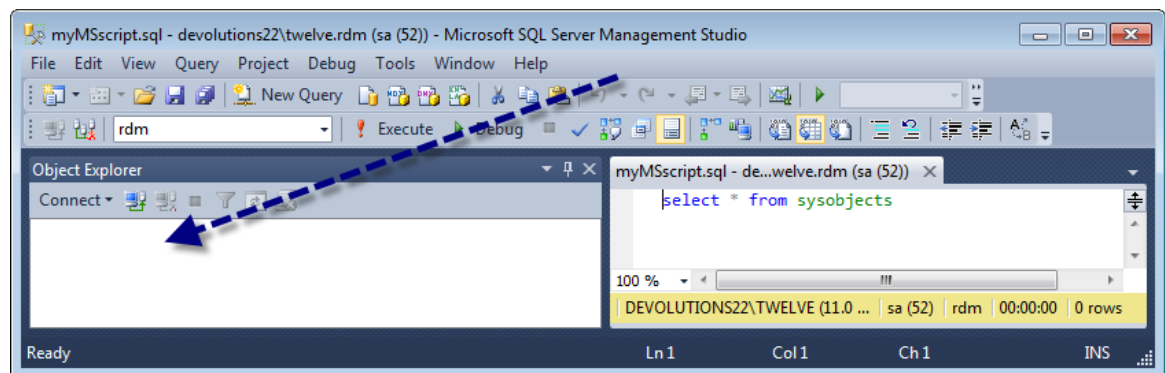
- Server/Instance**: A text input field.
- Database**: A text input field.
- Integrated security (Active Directory)**: A checkbox.
- User name**: A text input field.
- Password**: A text input field with a toggle icon (eye) to the right.
- Default query file**: A text input field with a browse button (three dots) to the right.
- Show Splash screen**: A checkbox.

General Settings Tab of the add-on

Setting	Description
Server/Instance	Indicate the full instance name. When a default instance as been used, normally you can put only the server name here
Database (Optional)	Used to indicate to select a database upon login.
Integrated Security	Indicates to use your windows credentials to authenticate on the server.
User name	When using Sql Server authentication, user name to use.
Password	When using Sql Server authentication, password to use.
Default query file (Optional)	Specifies a file that will be opened in the editor. Please see note below
Show splash screen	Indicates to let Sql Server Management Studio display its splash screen.

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.



8.6.3 VPN Add-ons

8.6.3.1 Overview

Description

Multiple VPN Add-ons can be installed using Remote Desktop Manager [Add-on Manager](#).

Consult topics below for more details on each VPN Add-ons:

- [Avaya \(Nortel\)](#)
- [Barracuda NG Network](#)
- [Bitwise Tunnelier](#)
- [Check Point Endpoint Security](#)
- [Check Point VPN-1 SecureClient](#)
- [Cisco AnyConnect](#)
- [F5 Firepass SSL](#)
- [FEC Secure IPSec](#)
- [FortiClient](#)
- [Generic VPN](#)
- [Juniper Junos Pulse](#)

- [Juniper Network Connect](#)
- [Juniper WSAM](#)
- [Juniper-Netscreen](#)
- [NCP Secure Entry Client](#)
- [OpenVPN](#)
- [SecureCRT](#)
- [Shrew Soft](#)
- [SonicWall NetExtender](#)
- [WatchGuard Mobile](#)
- [WatchGuard SSL](#)

8.6.3.2 Avaya (Nortel)

Description



Avaya (Nortel) VPN Add-on can be used to connect to your Avaya (Nortel) VPN session.

This Add-on can be installed using the [Add-on Manager](#).

For more information please consult [VPN Overview](#).

8.6.3.3 Barracuda NG Network

Description



Barracuda NG Network VPN Add-on can be used to connect to your Barracuda NG Network VPN session.

This Add-on can be installed using the [Add-on Manager](#).

For more information please consult [VPN Overview](#).

8.6.3.4 Bitwise Tunnelier

Description



Bitwise Tunnelier VPN Add-on can be used to connect to your Bitwise Tunnelier VPN session.

This Add-on can be installed using the [Add-on Manager](#).

For more information please consult [VPN Overview](#).

8.6.3.5 Check Point Endpoint Security

Description



Check Point Endpoint Security Add-on can be used to connect to your Check Point Endpoint Security VPN session.

This Add-on can be installed using the [Add-on Manager](#).

For more information please consult [VPN Overview](#).

8.6.3.6 Check Point VPN-1 SecureClient

Description



Check Point VPN-1 SecureClient Add-on can be used to connect to your Check Point VPN-1 SecureClient VPN session.

This Add-on can be installed using the [Add-on Manager](#).

For more information please consult [VPN Overview](#).

8.6.3.7 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](#).

For more information please consult [VPN Overview](#).

8.6.3.8 F5 Firepass SSL

Description



F5 Firepass SSL VPN Client Add-on can be used to connect to your F5 Firepass SSL VPN session.

This Add-on can be installed using the [Add-on Manager](#).

For more information please consult [VPN Overview](#).

8.6.3.9 FEC Secure IPSec

Description



FEC Secure IPSec Client Add-on can be used to connect to your FEC Secure IPSec VPN session.

This Add-on can be installed using the [Add-on Manager](#).

For more information please consult [VPN Overview](#).

8.6.3.10 FortiClient

Description



FortiClient VPN/SSL Add-on can be used to connect to your FortiClient VPN session.

This Add-on can be installed using the [Add-on Manager](#).

For more information please consult [VPN Overview](#).

8.6.3.11 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](#).

For more information please consult [VPN Overview](#).

8.6.3.12 Juniper Junos Pulse

Description



Juniper Junos Pulse VPN Add-on can be used to connect to your Juniper Junos Pulse VPN session.

This Add-on can be installed using the [Add-on Manager](#).

For more information please consult [VPN Overview](#).

8.6.3.13 Juniper Network Connect

Description



Juniper Network Connect Add-on can be used to connect to your Juniper Network Connect VPN session.

This Add-on can be installed using the [Add-on Manager](#).

For more information please consult [VPN Overview](#).

8.6.3.14 Juniper WSAM

Description



Juniper WSAM Add-on can be used to connect to your Juniper WSAM VPN session.

This Add-on can be installed using the [Add-on Manager](#).

For more information please consult [VPN Overview](#).

8.6.3.15 Juniper-Netscreen

Description



Juniper-Netscreen Add-on can be used to connect to your Juniper-Netscreen VPN session.

This Add-on can be installed using the [Add-on Manager](#).

For more information please consult [VPN Overview](#).

8.6.3.16 NCP Secure Entry Client

Description



NCP Secure Entry Client Add-on can be used to connect to your NCP Secure Entry Client VPN session.

This Add-on can be installed using the [Add-on Manager](#).

For more information please consult [VPN Overview](#).

8.6.3.17 OpenVPN

Description



OpenVPN Add-on can be used to connect to your OpenVPN VPN session.

This Add-on can be installed using the [Add-on Manager](#).

For more information please consult [VPN Overview](#).

8.6.3.18 SecureCRT

Description



SecureCRT VPN Add-on can be used to connect to your SecureCRT VPN session.

This Add-on can be installed using the [Add-on Manager](#).

For more information please consult [VPN Overview](#).

8.6.3.19 Shrew Soft

Description



Shrew Soft VPN Client Add-on can be used to connect to your Shrew Soft VPN session.

This Add-on can be installed using the [Add-on Manager](#).

For more information please consult [VPN Overview](#).

8.6.3.20 SonicWall NetExtender

Description



SonicWall NetExtender Add-on can be used to connect to your SonicWall NetExtender VPN session.

This Add-on can be installed using the [Add-on Manager](#).

For more information please consult [VPN Overview](#).

8.6.3.21 WatchGuard Mobile

Description



WatchGuard Mobile VPN Add-on can be used to connect to your WatchGuard Mobile VPN session.

This Add-on can be installed using the [Add-on Manager](#).

For more information please consult [VPN Overview](#).

8.6.3.22 WatchGuard SSL

Description



WatchGuard SSL VPN Add-on can be used to connect to your WatchGuard SSL VPN session.

This Add-on can be installed using the [Add-on Manager](#).

For more information please consult [VPN Overview](#).

8.7 Best Practices

8.7.1 Quick Start

Description

The following recommendations are provided for new and experienced users alike. Remote Desktop Manager has a lot of flexibility and sometimes we are faced with so many choices that we aren't sure of the proper decision to make or its impacts. Read below to find out what our own AND the community's experience has shown is the preferred way of operating Remote Desktop Manager in various scenarios.

Most of these recommendations apply to the Enterprise Edition because the range of options is so much greater than the Standards.

Basic recommendations

Data sources

An [Advanced Data Source](#) is best for the capabilities it allows (i.e. logging, attachments). For mobile workers they can even allow offline mode.

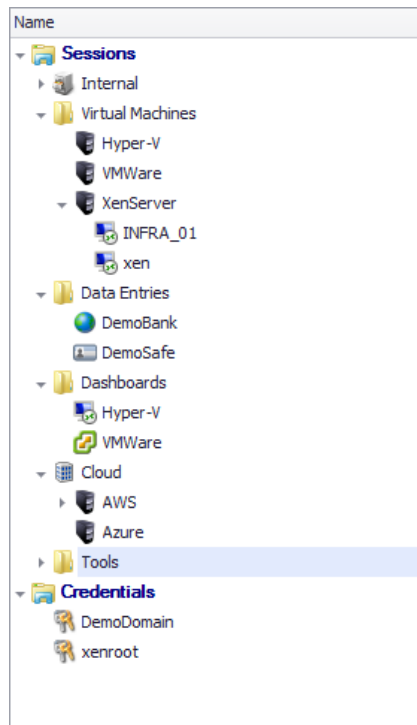
Use multiple data sources if you need to separate a client's session from your own, or if you have different security requirements for a subset of sessions.

Reusable entries

Credential entries, VPN entries and Macros can be used by multiple sessions. Define them once and reuse them rather than entering the details in all the sessions.

Organize your entries

The Group/Folder entry type exists to create a structure much like folders. Multiple sub-types exist to further refine the organization of your entries. See Group [Overview](#) for more details.



Multiple user considerations

Coming soon...

8.7.2 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.



SQLite

Our recommended backup solution is to subscribe to our [Online Backup Service](#)



Xml

Our recommended backup solution is to subscribe to our [Online Backup Service](#)



Microsoft Access

Our recommended backup solution is to subscribe to our [Online Backup Service](#)



Microsoft Sql Server

We recommend creating a maintenance plan to perform automatic backups regularly. This video is a good start on the subject: [Setting up a Maintenance Plan to Backup Databases](#)

8.7.3 Security

Description

Remote Desktop Manager's security allows you to create a granular protection system that is quite flexible. With the flexibility comes at the price or sometimes making the wrong choices that increase the time involved in managing the system.

What follows are recommendations from our use of the system, as well as from users that have shared their ideas with us.

Vocabulary

Your staff is organized in "teams", but to use a generic concept we'll use Tiers in our examples. Small organizations often have two tiers, but larger ones may have four.

- Tier 1 is often the top level system administrators. They have full control of everything.
- Tier 2 is for the staff that can see everything, but can edit only a subset of entries. They usually correspond to Service Desks, the senior staff, etc
- Tier 3 is for the staff that has limited visibility over the infrastructure. They have mostly read only rights, but may be able to edit sessions for certain groups. Help desks typically fall in that category, as well a junior staff members.
- Tier 4 is for read only access. Often for external consultants that come in for a mandate. They cannot see any passwords or entry details.

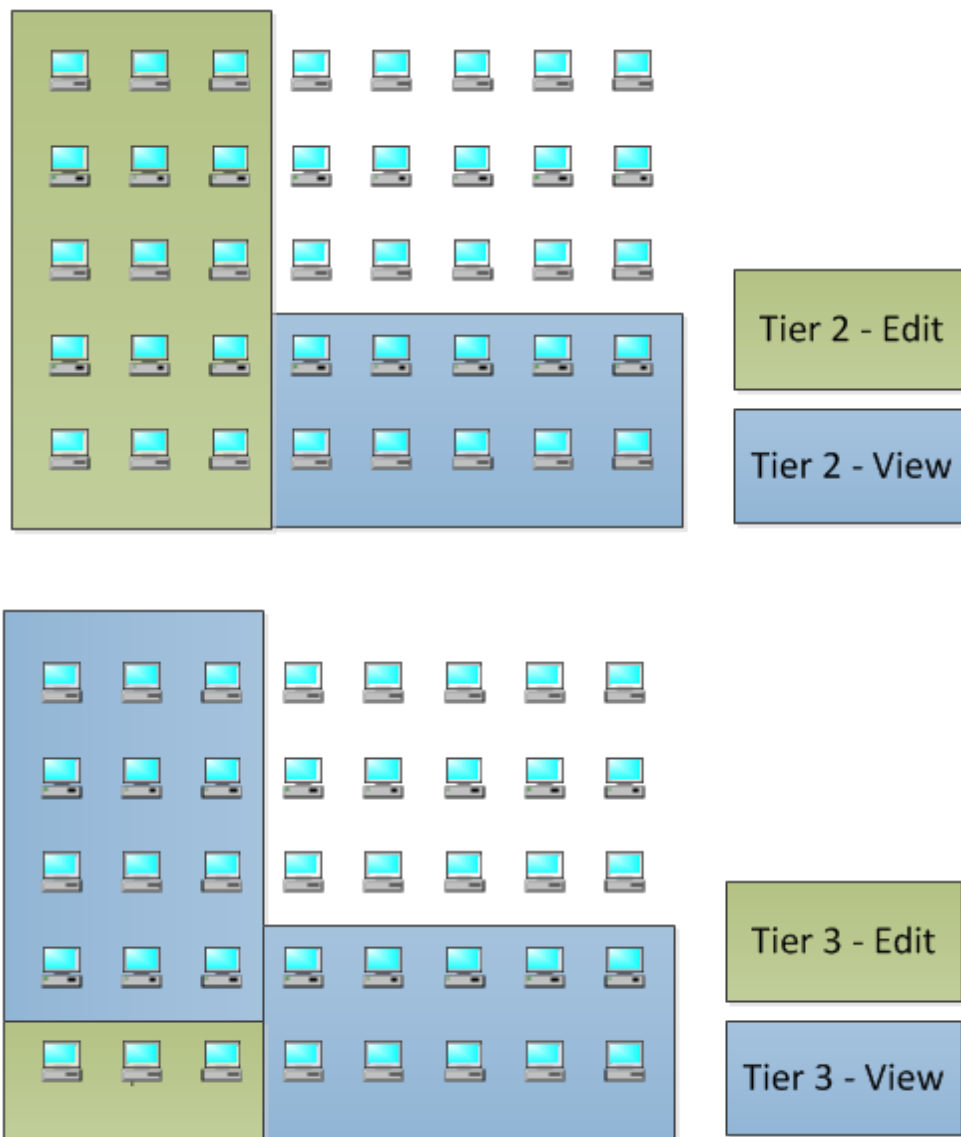
Recommendations

Do not replicate your AD groups.

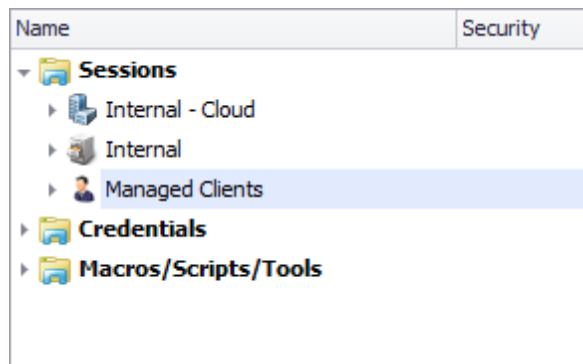
Remote Desktop Manager groups are to separate entries (sessions, credentials, etc), not users. Tier 3 personnel may have access to Group A in read only, Group B in read/write and not even see Group C, but Tier 2 personnel may have to edit everything. You will grant users the appropriate rights for each entry group.

Create a folder structure much like your organization is managing its operations

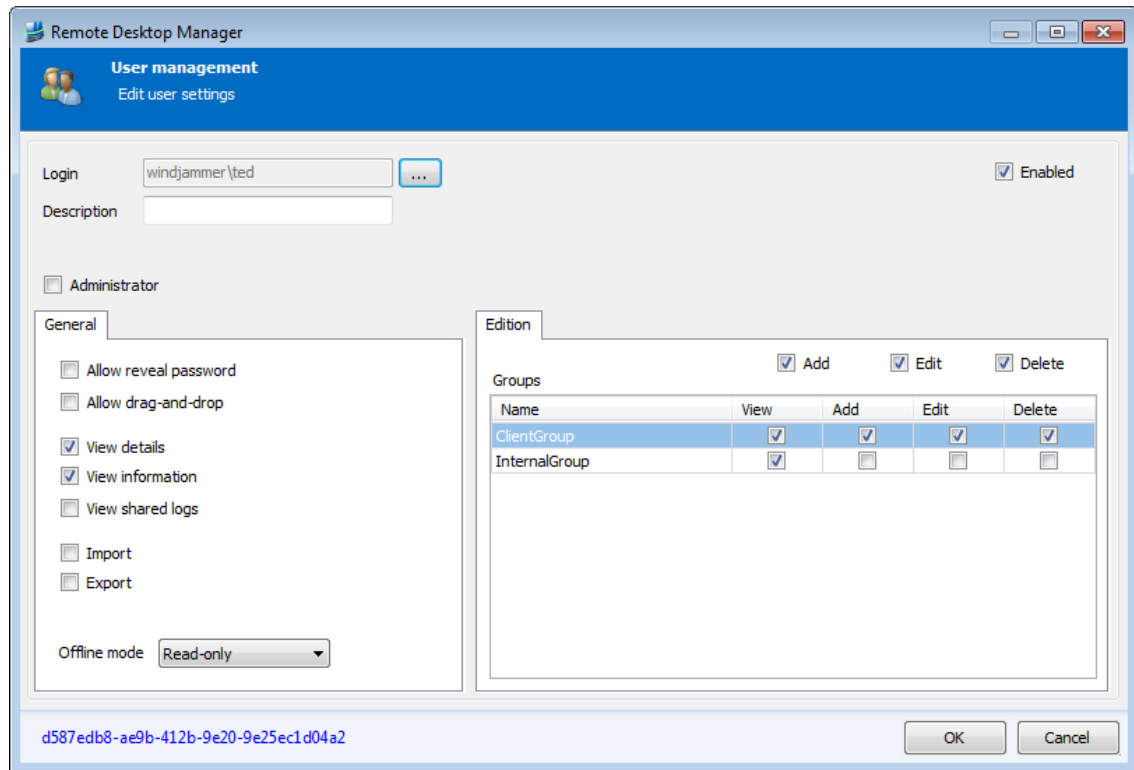
Its best to separate by area of concerns. Think of your sessions and credentials and separate them by your wish to make them A - visible and B - editable to each of your tiers. Each "intersection" of privilege by a subset of your team means another root level folder.



Once you have separated sessions into groups, create a root level folder for each group and give it a meaningful name. After that assign a security group the the root level folder.



After that, open the user to assign his rights for the group as described in [Permissions](#)



Assign security groups to high level folders

If you need to assign security groups to a deep folder, or to a specific entry, then you are creating an exception. It may end up consuming a disproportionate amount of time to manage these exceptions. You should look at the possibility of creating a new folder to make things clear for everyone in your organization.

Use the shortcut feature to give different permissions for an entry.

As can be seen in [Creating Shortcuts](#), an entry can appear under more than one folder. This is our recommended practice whenever you need to assign multiple permission sets to the same entry and you run into issues because it doesn't fit your security scheme.

8.7.4 Use Credential Entries

Description

One of Remote Desktop Manager's strengths is certainly its management of credentials. Although you can specify the credentials directly in the entry settings, you should rather use a credential entry. This has the following advantages.

- Credential entries can be used in multiple sessions
- Only that single credential entry must be maintained when modifications are required
- Permissions can be set on the use of the entry (when an [Advanced Data Source](#) is used)

8.7.5 Use VPN Entries

Description

Although you can specify the VPN details directly in the entry settings, you should rather use a VPN entry. This has the following advantages.

- VPN entries can be used in multiple sessions
- Only that single VPN entry must be maintained when modifications are required
- Permissions can be set on the use of the entry (when an [Advanced Data Source](#) is used)

For more information, please consult [VPN Overview](#).

8.8 Tips And Tricks

Description

Our favorite tips and tricks are under this topic. If you have a suggestion for improving an existing tip or even to suggest a new one, please send a note to infos@devolutions.net.

8.8.1 Automation via Windows PowerShell

Overview

The RDM snap-in allows for quick and robust automation of actions, such as add/edit/open of sessions. The possibilities are endless, and are limited only by your imagination – and, of course, the tool's functionality.

Since its release, this highly-requested feature has become a very useful in solving user requests. A quick search through our forum reveals many ingenious usages of the cmdlets, such as automating the creation of Windows Start Menu shortcuts for every RDM session ([link](#)).

To learn more, you can find full RDM cmdlet documentation available via [online help](#), or directly in PowerShell using the Get-Help cmdlet.

Example: Create Web Data Entry

Here's a simple example of the RDM PowerShell snap-in at work. We'll be covering how I imported all blog URLs from Google Reader.

- 1) I started by exporting my Google Reader subscriptions (via Google Takeaway).
- 2) Next, I loaded the file into an XmlDocument using Get-Content.
- 3) Finally, I created an RDM session for each node, and assigned the appropriate properties:

```
[xml]$rss = Get-Content C:\rss.xml;

foreach ($site in $rss.opml.body.outline)
{
    $session = New-RDM-Session -Name $site.Text -Kind "DataEntry"
    $session.Group = "RSS"
    $session.AddDataEntryKind(11 <# Web #>);
    Set-RDM-Session $session -NoRefresh;
    Set-RDM-Property -ID $session.ID -Path "DataEntry" -Property "Url" -Value $site.htmlUrl
}
```

```
}
```

Example: Reflect the group name as the company name

```
foreach ($list in Get-RDM-Session)
{
    $group = Get-RDM-Property -id $list.id -Property "Group";
    Set-RDM-Property -ID $list.ID -Path "MetaInformation" -Property "Company" -value $group -NoRefresh
}
```

Now, for you IT pros out there, this is a pretty simple example that you could do in your sleep! However, I merely wanted to illustrate how robust the feature is, and how you can use it to make your life easier and more productive.

Additional tips

Here are some additional tips to help you get the most out of the PowerShell snap-in:

- Use the `-NoRefresh` flag for faster script execution, especially in loops, since the UI isn't refreshed during the action.
- Use the `Set-RDM-Property` 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!

So, how would you find more helpful tips like these? Simply visit our forum and ask! Plus, if the tool can't do what you need it to, we'll see what we can do to add it to a future release. In fact, most of the features we've built so far are a result of user requests for help and guidance.

8.8.2 Creating Shortcuts

Overview

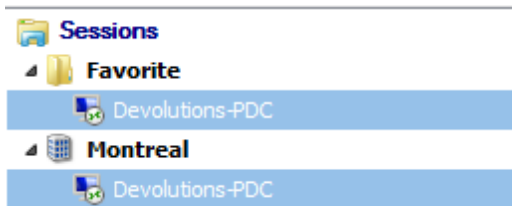
There are a many scenarios where it makes sense for an entry to appear more than once in the UI. For example, you might want to:

- assign different access rights to the folder
- create a favorite folder with everything centralized
- reuse a document for different scenarios

However, doing this manually is time consuming, tedious and prone to error. But no longer!

Solution

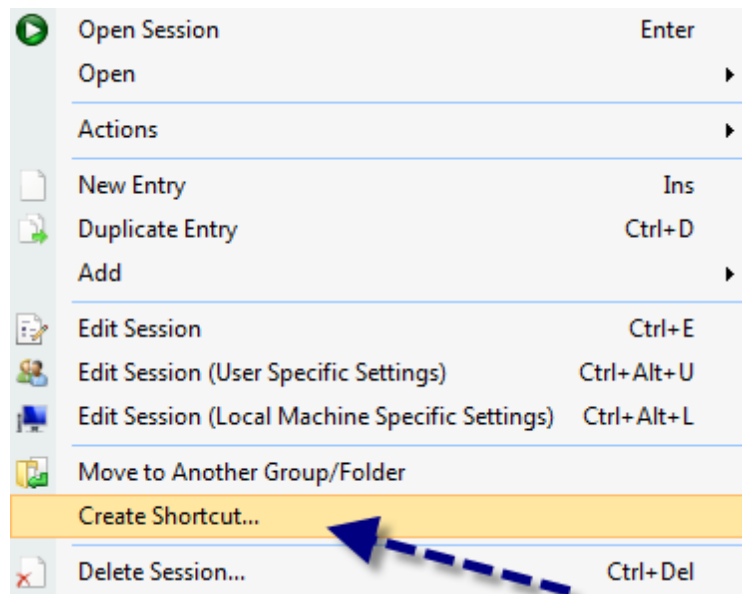
Fortunately, Remote Desktop Manager makes creating shortcuts easy, simple and quick! It works by saving the entry once in the database, while linking it to more than one group. So when Remote Desktop Manager loads the data, it automatically creates a link to the original entry. You don't have to lift a finger – everything is done for you, to save your time and simplify your life.



Same Entry in Two Groups

Creating a Shortcut: Option 1

One way to create a shortcut is by using the menu **Edit->Create Shortcut...**



Create Shortcut Command

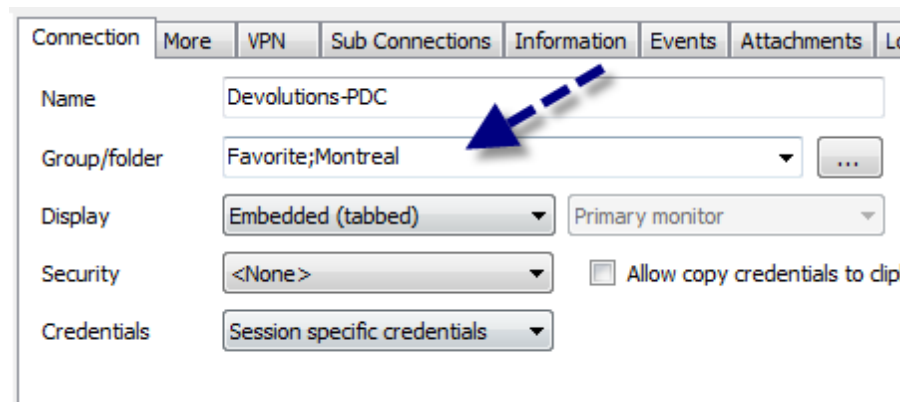
Simply choose the destination folder for the shortcut. Remote Desktop Manager will automatically refresh and display the new shortcut in the list.



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

Creating a Shortcut: Option 2

A second way to create a shortcut is via the session properties. Since the shortcut is based on a group list, simply add a session in multiple groups by setting two or more destinations, which are separated by semicolons “;”. You can also use the browse button (...) and select more than one group by holding the Ctrl key while clicking on the tree node.



Group/Folder Example

8.8.3 Data Migration

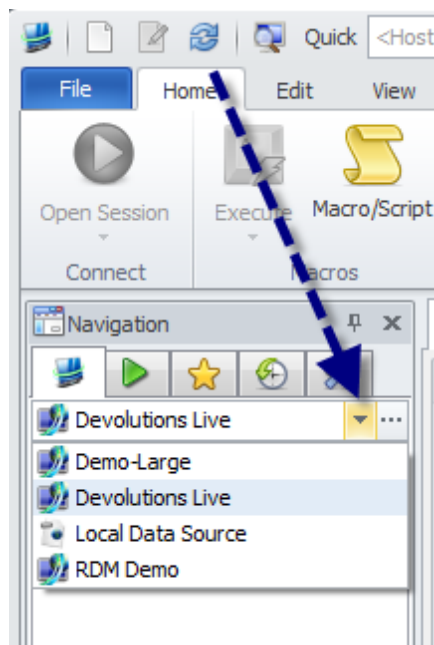
Description

Many users start with the standard edition but end up migrating to the Enterprise edition. Here is the procedure to migrate the data between data sources.

The migration is simply an export from the origin data source, followed by an import in the destination data source.

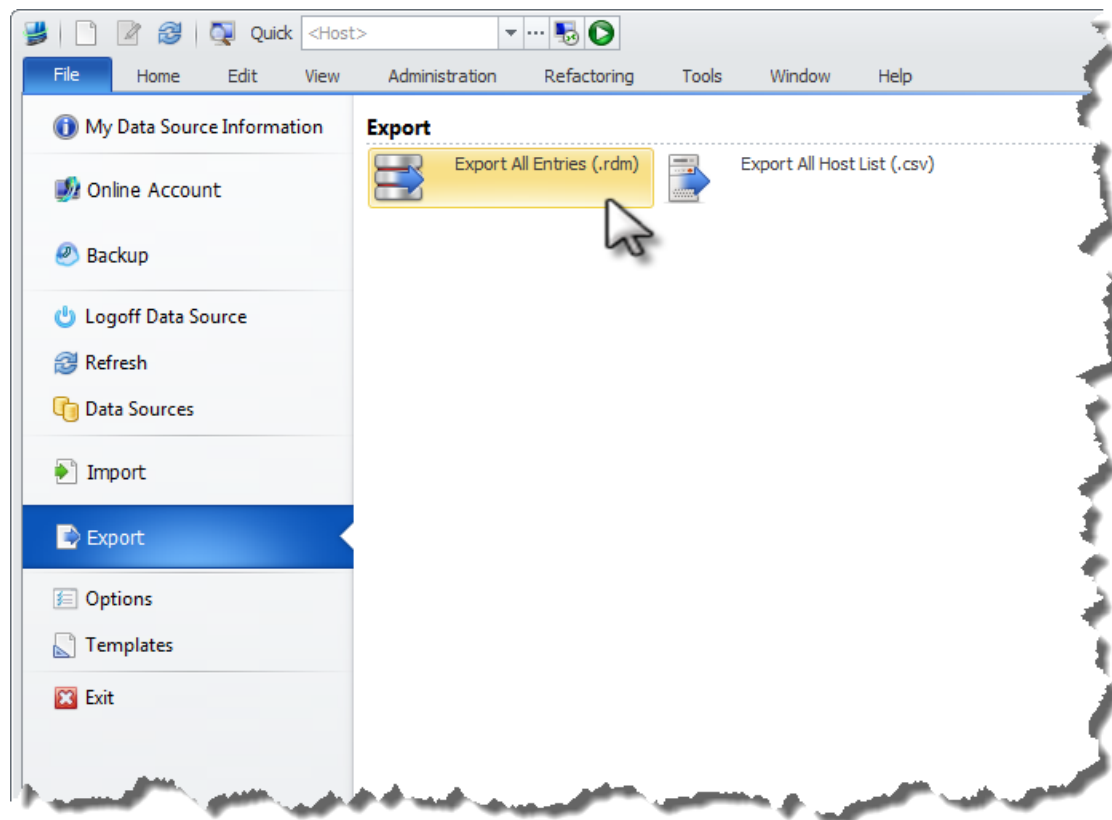
Export

- Select the origin data source in the data source selection drop down.



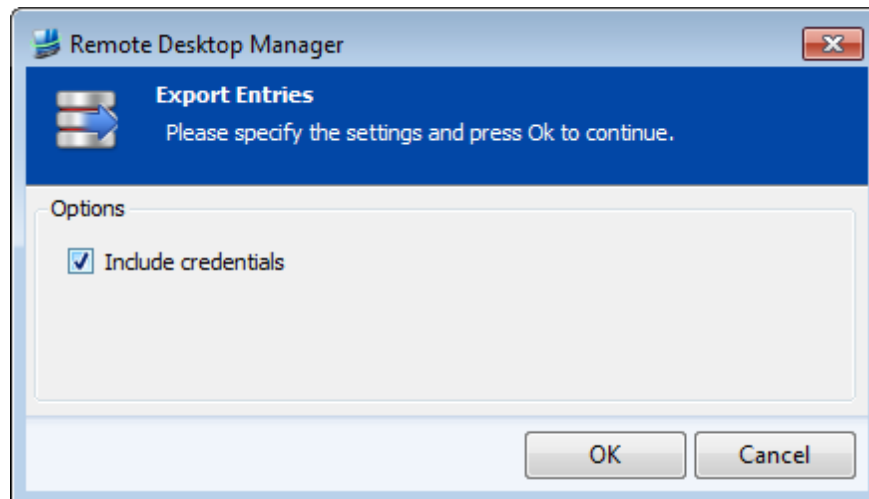
Data source selection drop down

- Select **File -> Export -> Export All Entries (.rdm)**.



Export sub menu

- Decide if you want to export credentials or not. For a typical migration you would check the option.

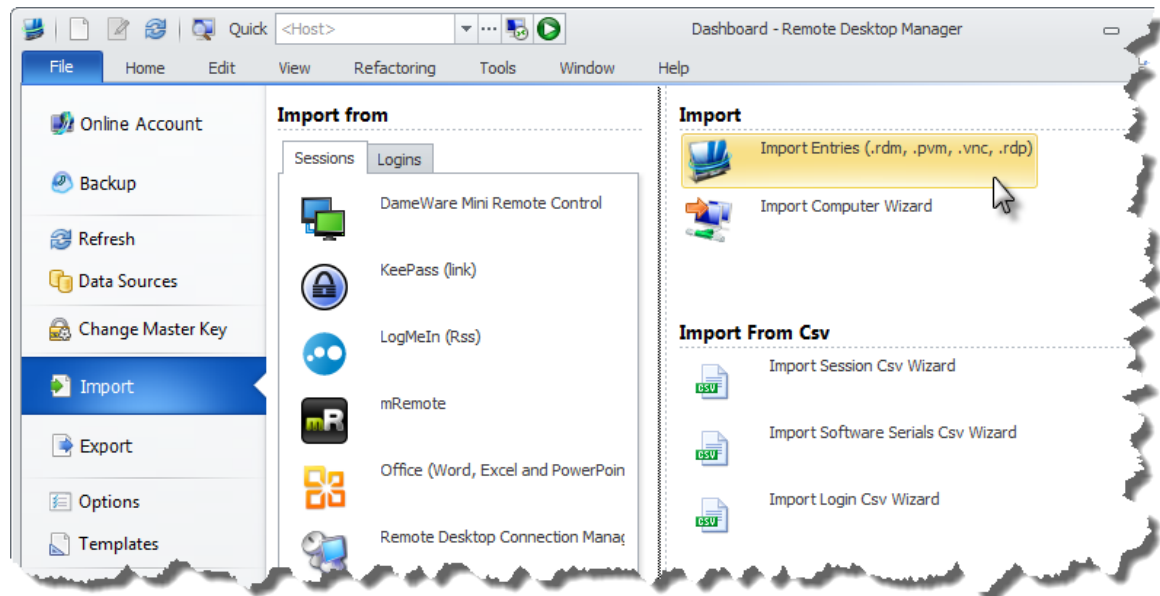


Export entries option dialog

- Save the file with the name and location of your choice.

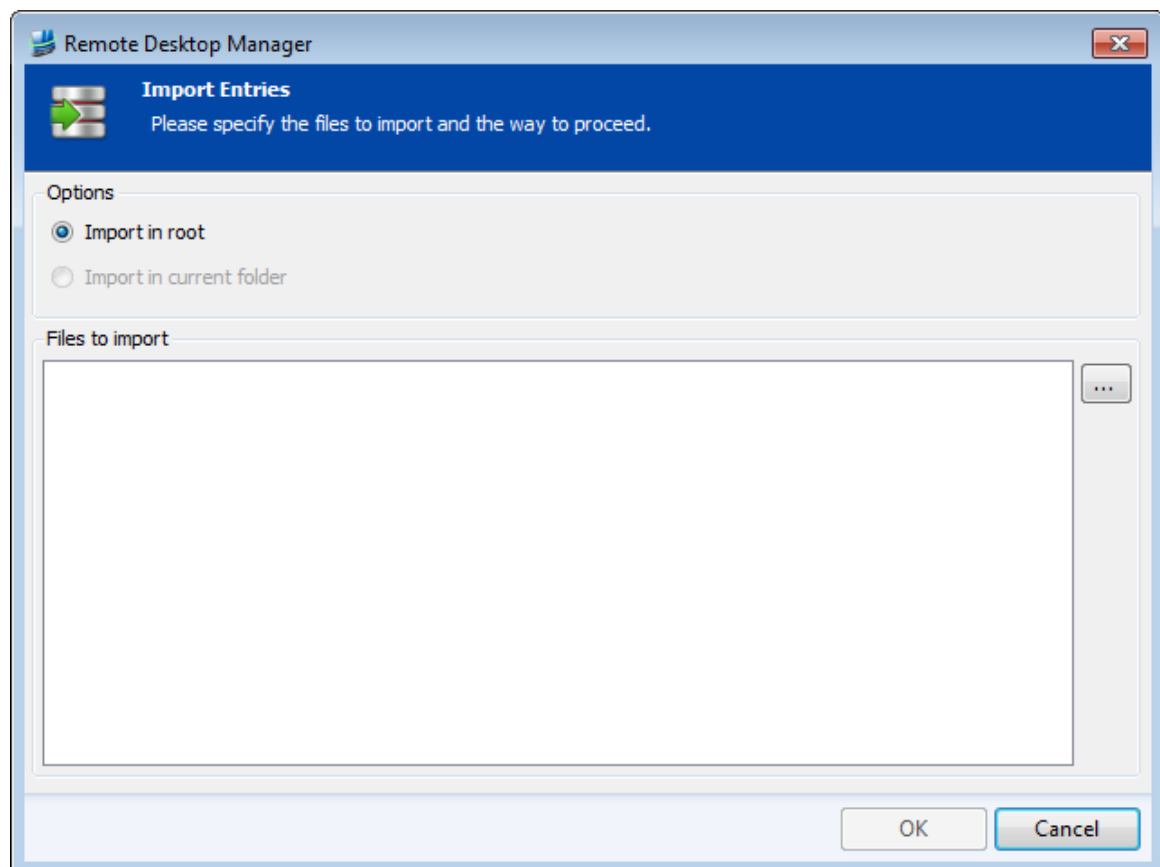
Import

- Select the destination data source in the data source selection drop down.
- Select **File -> Import -> Import Entries (.rdm, *.pvm, .vnc, .rdp)**.



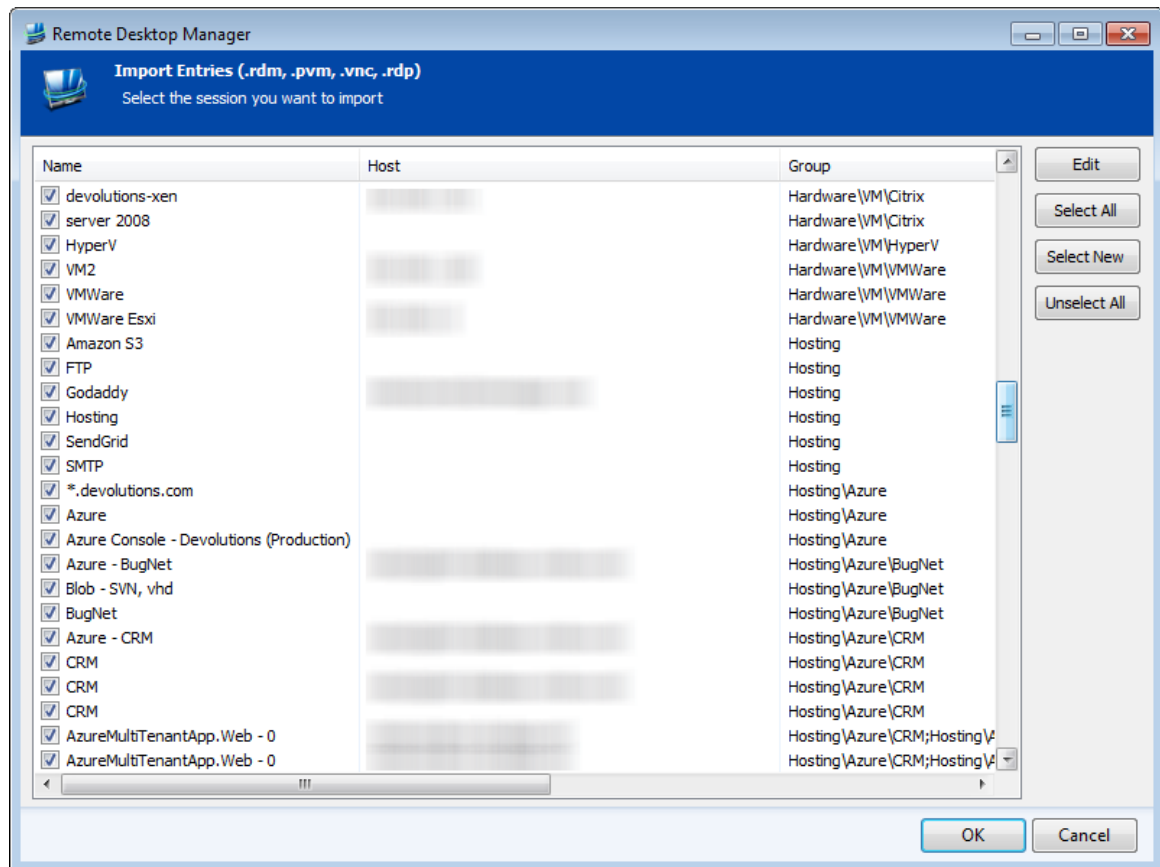
Import sub menu

- In the Import Entries dialog, use the ellipsis button to browse for the data file exported in the previous section.



Import Entries dialog

- In the next dialog, you are presented with a list of all entries that are in the data file. Simply press ok to complete the process



Import Entries - session selection dialog.

8.8.4 Data Report

Description

The Data Report session type can be use to empower any/all users to generate reports, without having to grant them access to the actual server.

Settings

General

The screenshot shows the 'General' tab of a configuration window. It features a tabbed interface with 'General', 'Parameters', and 'Query' tabs. The 'General' tab is active and contains a list of configuration fields on the left and their corresponding input controls on the right. The fields are: 'Source' (a dropdown menu set to 'Default'), 'Data source' (a text box containing 'Microsoft SQL Server'), 'Data provider' (a text box containing '.NET Framework Data Provider for SQL Server'), 'Connection string' (a text box filled with dots, with an eye icon and an ellipsis button to its right), 'Host' (a text box with a blurred value), 'User name' (a text box with a blurred value), and 'Password' (a text box filled with dots, with an eye icon to its right). A small grid icon is located to the left of the 'Source' field.

General Tab

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

General Parameters Query

Custom parameters

Parameter description	Type	Default value
Parameter #1	@Param1 Unused	
Parameter #2	@Param2 Unused	
Parameter #3	@Param3 Unused	
Parameter #4	@Param4 Unused	
Parameter #5	@Param5 Unused	

Exemple of Query fields: Exec Query

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

Parameters Tab

Specify the parameters by setting the name, type and default value of all parameters.

Query

General Parameters Query

```

1  with cteCountry as
2  (
3      SELECT
4          UPPER(c.Code) as Code,
5          c.Country,
6          i.InvoiceID
7      FROM Invoice AS i
8      LEFT OUTER JOIN Counti
9      WHERE i.IsQuote = 0 AND i.
10         and i.CreationDate betwe
11  ),
12  cteTotal as (select count(*) as To
13  select top (@Param1) c.Code, c.Cou
14  from cteCountry c, cteTotal t
15  group by c.Country, c.Code, t.Tota
16  order by count(*) / (t.Total * 1.0
  
```

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.

8.8.5 Edit Hosts File

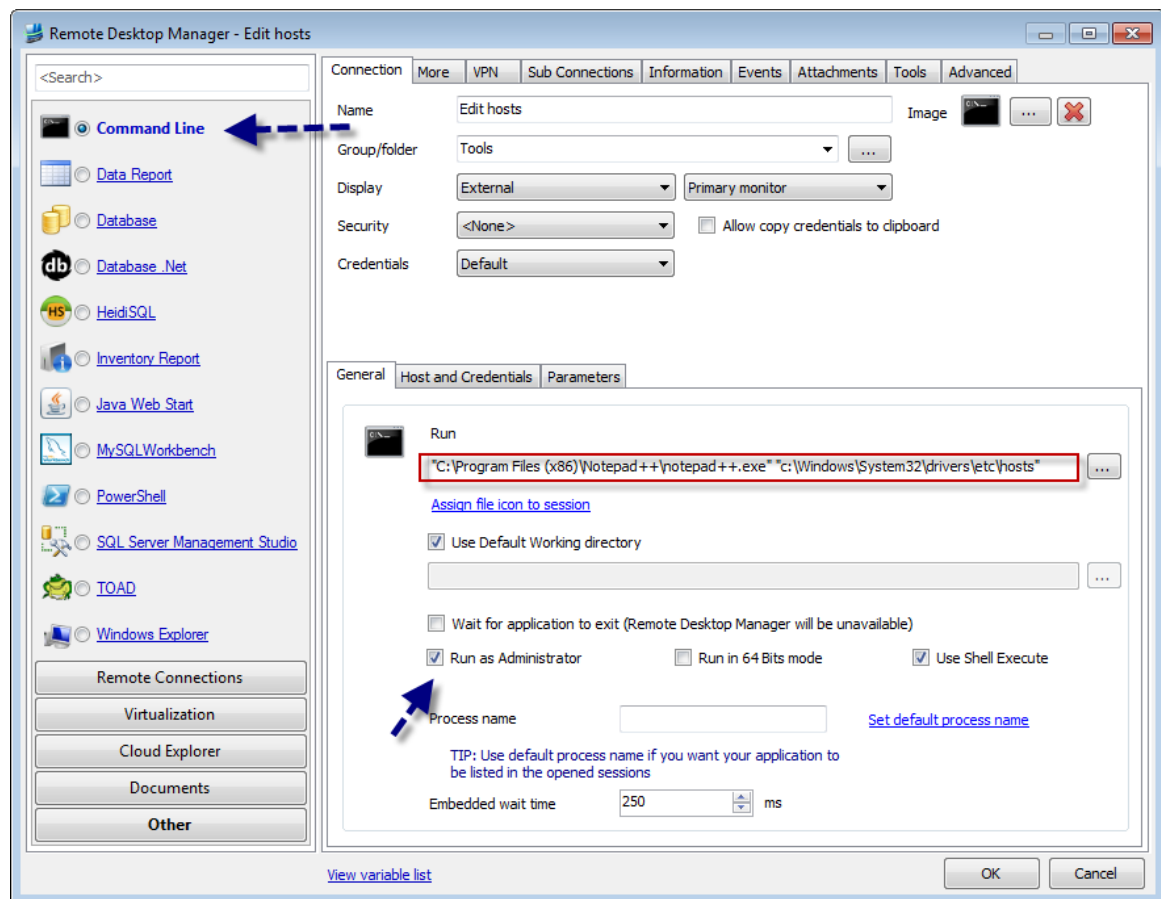
Description

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 you goal, but our experience tells us that most people don't bother with it, ending up losing precious seconds every time 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 on all of them.

Simply create a session with the proper settings.



Edit Hosts session configuration

Steps

1. Create a new **Command Line** session.
2. Enter a session name
3. Check the **Run as Administrator** check box.

4. Using the ellipsis button, select your editor of choice in the **Run** text box.
5. Paste the following after the name of the program, ensure a blank space separates the two and include the double quotes. **"c:\Windows\System32\drivers\etc\hosts"**



If your editor is already running, it will not elevate the privileges. You should close it beforehand. I've implemented a AutoHotKey script that closes my editor of choice, but being that it shuts off without saving pending changes, its not a solution for the faint hearted. It depends on your chosen editor's reaction to the WM_QUIT message.

That's it. Simple and efficient. 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 want 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.

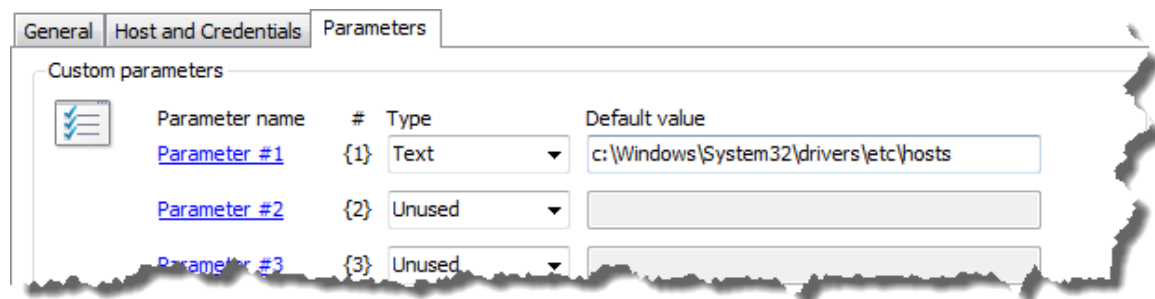
Steps 1-4 are the same

Step 5 - Enter **"{1}"** after the name of the executable, keeping a space between the two values and including the quotes.

Step 6 - Uncheck **"Use Shell Execute"**

Step 7 - In the parameters tab, set parameter # 1 type to **"Text"**

Step 8 - Enter the following in the Default Value: **c:\Windows\System32\drivers\etc\hosts**



Parameters tab

This is helpful if you mostly use the tool with a certain file, but occasionally need to edit another file. I'd rather have a separate entry for each file I commonly edit, but this shows how flexible Remote Desktop Manager really is.

8.8.6 How to Backup

Description

Backups are important in case of hardware failure.

A proper backup will cover both your **data** and your **settings**.

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.

8.8.7 How to Reinstall

Description



Before reinstalling Remote Desktop Manager, you need to do a backup. Please refer to [How to Backup](#).

A proper backup will consist of the application settings, and of the data sources.

Refer to the [Installation Overview](#) topic for details on the installation of Remote Desktop Manager.

Settings

When Remote Desktop Manager has been reinstalled on your computer, ***before you open it***, you need to copy your RemoteDesktopManager.cfg inside the folder ***%LocalAppData%\Devolutions\RemoteDesktopManager***. ***This is the default path***

This config file contain all your settings.

Please refer to the [Configuration File Location](#) for more details on RemoteDesktopManager.cfg.

Data

If you have moved the file based data sources to another relative path, you will have to edit the data source definitions to fix the paths.

8.8.8 How to Subscribe to the Announcements Forums

You can be notified when new updates are available on our products by subscribing to the announcements forums on <http://forum.devolutions.net>

If you want to subscribe to the announcements for Remote Desktop Manager, click on the link below:

<http://forum.devolutions.net/forum20-remote-desktop-manager--announcements.aspx>

After, click on watch this forum for new topics.

Forum **Remote Desktop Manager - Announcements**

Monitor this forum to get notified when a new update is available

new topic | 1 | 2 | 3 | watch this forum for new topics | watch this forum for new posts

		Latest Post	Views	Posts
	Remote Desktop Manager 9.0.4.0 from Maxime Trottier	1 days ago - Maxime Trottier	44	1
	What's new in Remote Desktop Manager 9! from Maxime Trottier	14 days ago - Maxime Trottier	1108	1
	October Poll: Mac vs. PC // Let the Battle Begin! from Maxime Trottier	24 days ago - Maxime Trottier	118	1
	Remote Desktop Manager 9 now available! from Maxime Trottier	27 days ago - Maxime Trottier	146	1

Devolutions Forum

The procedure is the same for all forums, below are the Announcement forums that exist at this time

Remote Desktop Manager MAC:

<http://forum.devolutions.net/forum43-remote-desktop-manager-mac--announcements.aspx>

Password Vault Manager:

<http://forum.devolutions.net/forum27-password-vault-manager--announcements.aspx>

Password Vault Manager MAC:

<http://forum.devolutions.net/forum47-password-vault-manager-mac--announcements.aspx>

Remote Desktop Manager Online:

<http://forum.devolutions.net/forum31-remote-desktop-manager-online--announcements.aspx>

Remote Desktop Manager Server:

<http://forum.devolutions.net/forum32-remote-desktop-manager-server--announcements.aspx>

8.8.9 HTML Export Using Symmetric Encryption

Overview

As we all know, email isn't secure. But it's convenient, fast and free – and so many of us ignore the security risks.

Yet when you step back and think about it, ask yourself: Would you ever think of sending cash through the regular mail? Even sending it through a courier is risky! But if you send sensitive information via email, that's pretty much what you're doing.

Fortunately, there's a solution!

We've developed a feature that allows for symmetric encryption of sensitive information, so that it can then be securely sent via email (or any other protocol) while keeping the data safe.

This feature can also be used to save/export/backup sensitive information to disk.

How it works

The feature is simple and easy to use:

- Select one or multiple data entries
- Right-click Import/Export -> Export Data Entry -> Export Data Entry (.html)
- When prompted, enter a password
- Save the file to disk

And that's it! Your document is ready to be securely sent via email or any other protocol.

Export Multiple Entries

And what if you're exporting multiple data entries? To prevent prying eyes from seeing more than they should, each secured string must be individually decrypted. Someone is walking by your desk, simply hit F5 or close the file, and the information is secure again.

A Word about AES-256

We use AES-256 to encrypt/decrypt your sensitive data. Since the decryption is done entirely in the browser, there's no need for external tools, downloads or installs. Here's a snapshot of the encrypted values:



```

<tr>...</tr>
<tr>
  <td class="label EmailPOP3Password">Password</td>
  <td class="value EmailPOP3Password" colspan="3">
    <span id="a2da6626-a620-49da-8aaf-85495af294cb" data="U2FsdGVkX18jCcpyAqqnT1gi1+Y03TvMM6kex1tpFUA=">
      <a class="encrypted" onclick="javascript:decryptText('a2da6626-a620-49da-8aaf-85495af294cb')">*****
    </span>
  </td>
</tr>
<tr>...</tr>

```

Html File Content

Safe & Smart Virtual Backup

In addition, HTML Export using symmetric encryption is a great way to securely – and virtually – backup your passwords and other sensitive information. It allows you to share information via email, or simply send the file to your personal email account as a backup. The possibilities are endless, and it's just another way that we're working hard to help you centralize it, secure it and simplify IT!

Printing

Sorry, decryption of the printed document isn't supported. We have yet to figure out a way to do this. If someone ever does please let us know.

8.8.10 Identify Security Groups

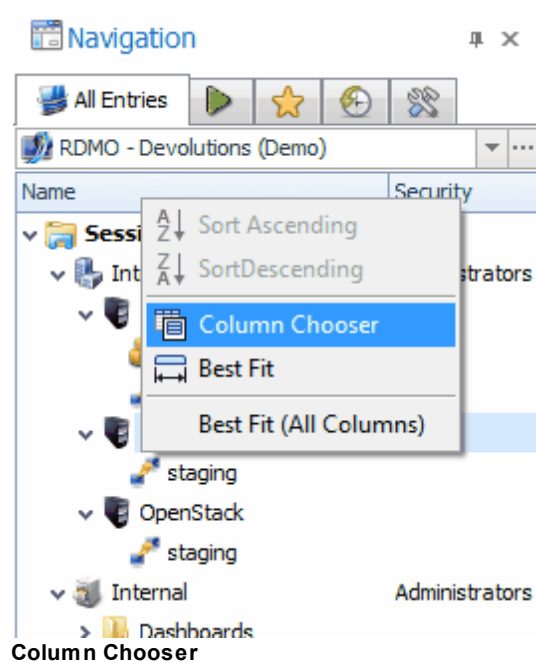
Description

There are 3 methods to identify which security groups are associated to an entry.

Navigation tree view column

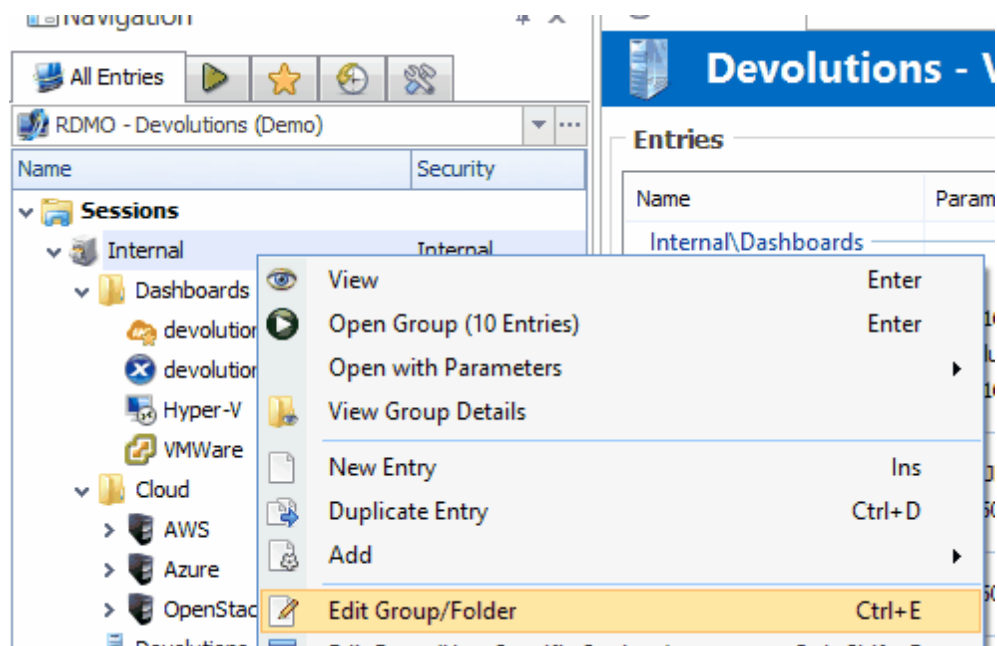
A **Security** column can be added in the Navigation Pane by right-clicking on the column Name in the Navigation Pane and selecting Column Chooser.

Double-Click on Security and the column Security will now be added and you would be able to see what security groups are apply to your entry.



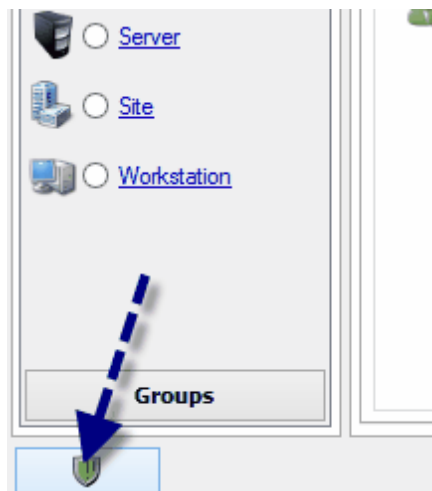
Security shield in entry properties

By Right-Clicking on your entry and select Edit Properties

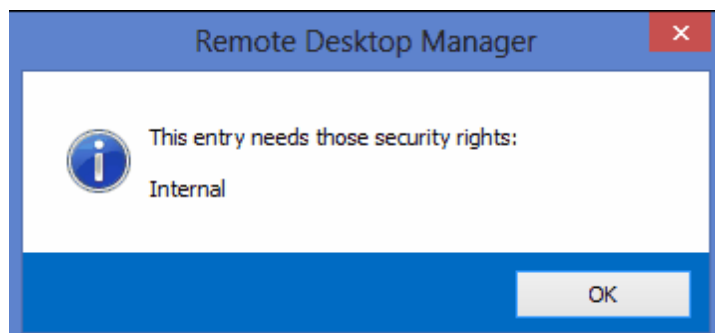


Edit entry for security group

Click on the green Shield at the bottom of the screen and the security right for your entry will appear



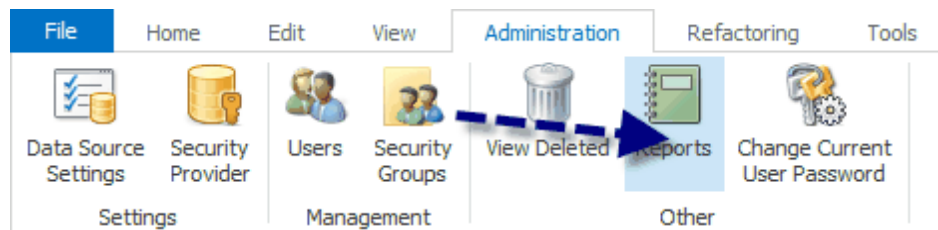
Green Shield



Security rights

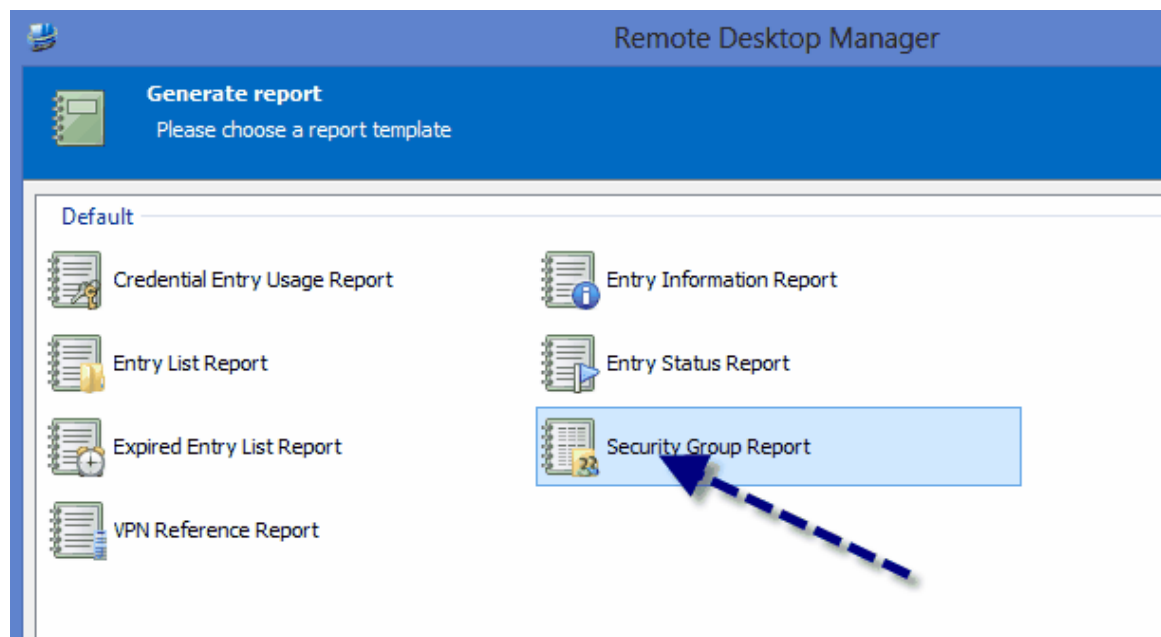
Security group report

By selecting the **Administration -> Reports**



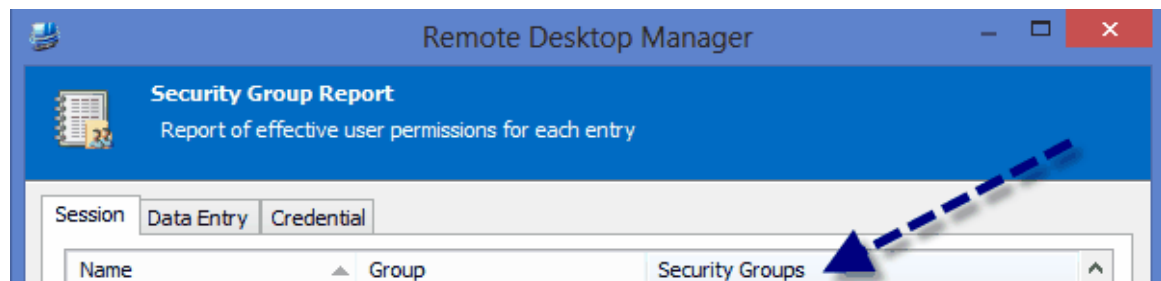
Reports in Administration tab

After, double-click on Security Groups Report



Security Groups Report

In the Security Group Report window, you will see a column for the Security Groups



Security Groups column

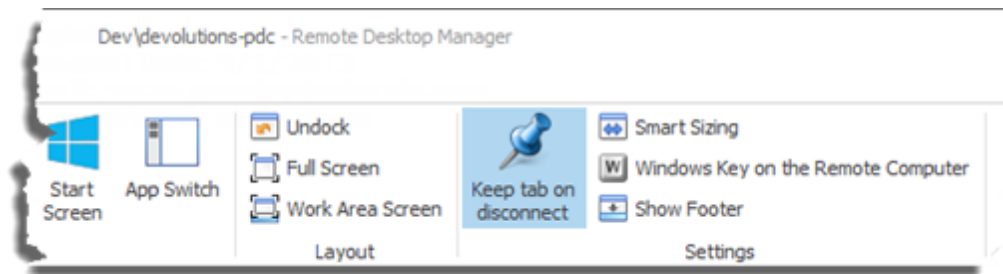
8.8.11 Keep Tabs Opened

Description

There is the possibility of keeping a tab open during a disconnect. This allows you to restart a remote device or simply keep your work area set up to resume quickly after a work interruption.

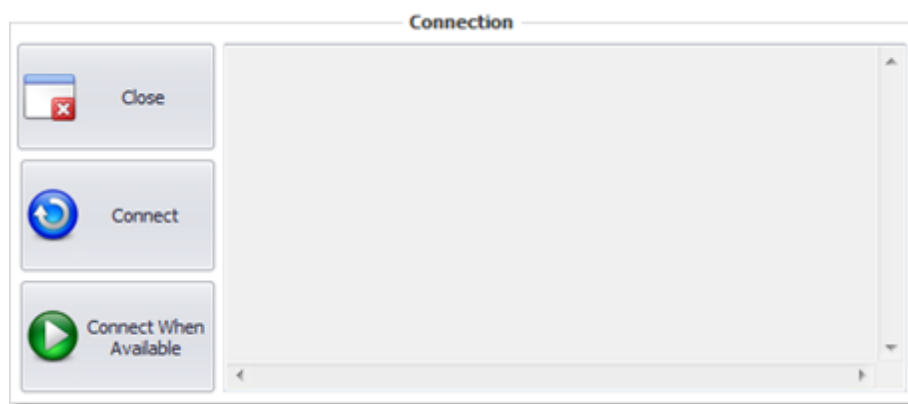
Workflow

Since this is for tabs, the session must be running embedded. You'll notice a new action in the settings section: "Keep tab on disconnect"



Ribbon

Simply enabling this action will allow you to perform a logoff or restart while keeping the tab present. A panel will replace the content of the session.

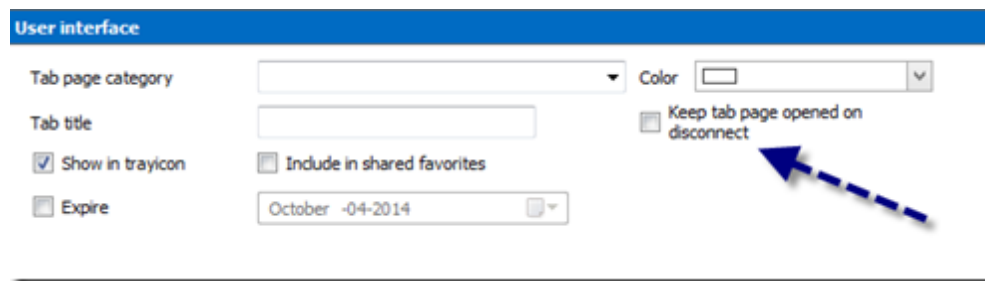


Connection Panel

This panel offers three actions:

- Close: You changed your mind and want to close the tab
- Connect: Connect the session
- Connect When Available: Pings the host until it becomes available, then connects the session.

You can even edit the session settings so the option is always enabled, you simple need to visit the More Tab and scroll down to the User Interface section



More -> User interface

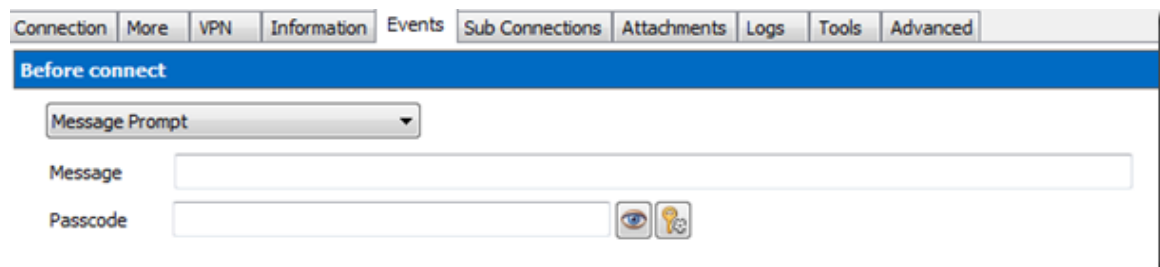
8.8.12 Passcode Prompt When Opening an Entry

Description

Sometimes you want to ensure that your users are really opening the right session.

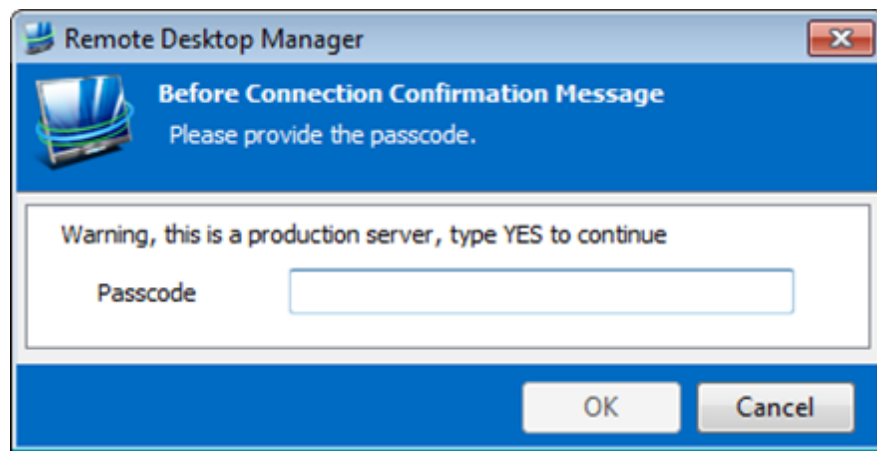
Workflow

In the Events tab, in the Before Connection section, when you select “Message Prompt”, you will notice a Passcode field.



Events tab

There is a field to enter a Message and another one for a Passcode. The idea is not to have another password to launch the session, but rather to act as a safeguard. For example, you could set the message to “Warning, this is a production server, type YES to continue” and set the Passcode to YES. This allows you to give just a little jolt when you attempt to launch the session!



Passcode in action

8.8.13 Open RD Gateway Only when Unable to Ping Host

Description

Use your RD Gateway only when your host is unreachable.

Settings

In your Microsoft Remote Desktop (RDP) entry, under Connection, you can enable **Open gateway only when unable to ping host**, connectivity with the remote host will be tested to see if its reachable, if not, the RD Gateway will be used.

General Display Local Resources Programs Experience **Connection** Advanced

Authentication

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 (SingleSignOn)

☐ Automatically detect RD Gateway server settings

☒ Use these RD Gateway server settings:

Server name: gateway.windjammer.com

Logon method: Allow me to select later

☒ Open gateway only when unable to ping host

☐ Bypass RD Gateway server for local addresses

☐ Use my RD Gateway credentials for remote computer

☐ Do not use RD Gateway server

Credentials

Connection tab



The method used to test connectivity will be the one set in the **Advanced** tab of the entry, **Is Online** section, **Online Detection** setting. Please see [Advanced Settings Overview](#) for more details.

8.8.14 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
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)

Set time limit for disconnected sessions	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.
Set time limit for active but idle Remote Desktop Services sessions	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.
Set time limit for active Remote Desktop Services sessions	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.
End session when time limits are reached	This policy setting specifies whether to end a Remote Desktop Services session that has timed out instead of disconnecting it.

3. Double click on the setting (or right-click -> Edit), an edition form will appear

The screenshot shows a Windows-style dialog box titled "Set time limit for disconnected sessions". At the top, there are "Previous Setting" and "Next Setting" buttons. Below the title bar, there are three radio buttons: "Not Configured" (selected), "Enabled", and "Disabled". To the right of these is a "Comment:" text box. Below the radio buttons is a "Supported on:" section with a dropdown menu showing "At least Windows Server 2003 operating systems or Windows XP Professional". Under the "Options:" label, there is a dropdown menu currently set to "End a disconnected session". To the right of this is a "Help:" section containing three paragraphs of text explaining the policy setting. At the bottom right, there are "OK", "Cancel", and "Apply" buttons.

Set time limit for disconnected sessions

Previous Setting Next Setting

☒ Not Configured Comment:

☐ Enabled

☐ Disabled

Supported on: At least Windows Server 2003 operating systems or Windows XP Professional

Options: End a disconnected session

Help:

This policy setting allows you to configure a time limit for disconnected Remote Desktop Services sessions.

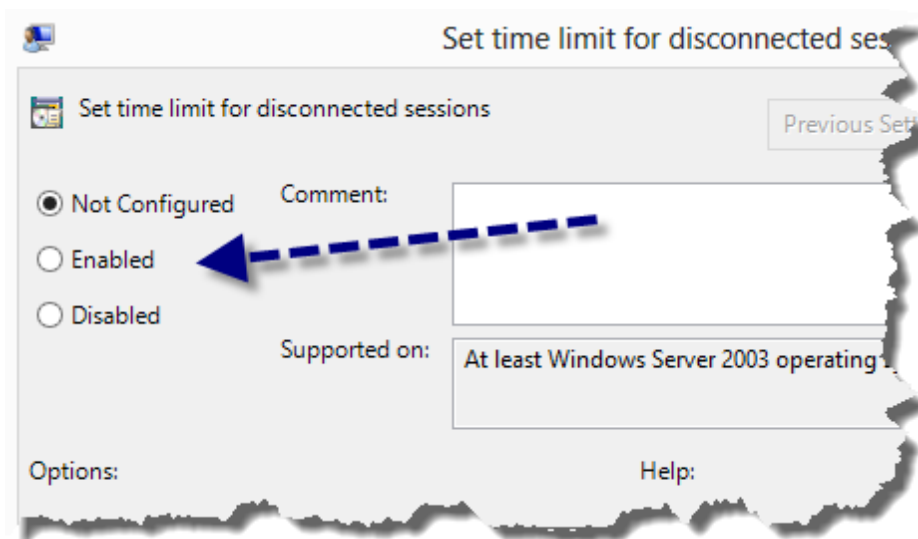
You can use this policy setting to specify the maximum amount of time that a disconnected session remains active on the server. By default, Remote Desktop Services allows users to disconnect from a Remote Desktop Services session without logging off and ending the session.

When a session is in a disconnected state, running programs are kept active even though the user is no longer actively connected. By default, these disconnected sessions are maintained for an unlimited time on the server.

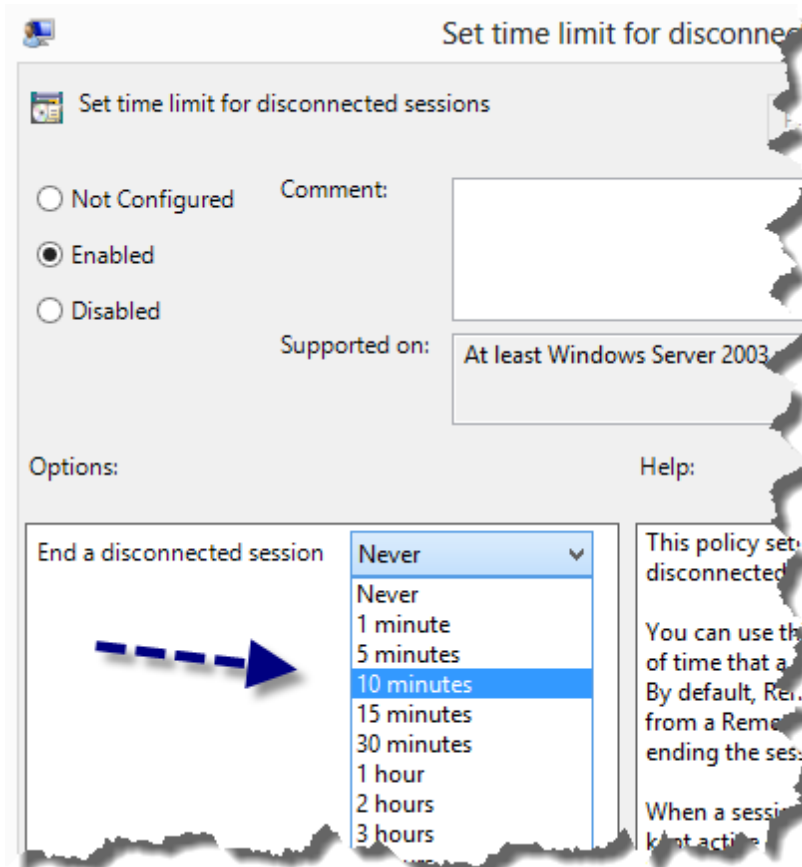
If you enable this policy setting, disconnected sessions are deleted from the server after the specified amount of time. To enforce the default behavior that disconnected sessions are maintained for an unlimited time, select Never. If you have a console session, disconnected session time limits do not apply.

OK Cancel Apply

4. Select **Enabled**, this will enable the control in the lower section



5. Choose your desired value from the list



6. Press Apply

7. Repeat for other settings as desired. Note that for true/false settings there is no control in the Options area. Just enabling the policy will activate the setting.

From then on, all future sessions established on that host will follow these policy settings.

You may want to explore all the policies below Remote Desktop Services, you may find hidden gems that would help your organization.

8.8.15 Remote 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.

Pre-requisites

Script Execution Policy

By default, no scripts can be run a new installations. No only must you enable script execution, but you must choose if you require scripts to have a digital signature.

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 se

Remote Management

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. In an elevated privileges PowerShell session, run the `Enable-PSRemoting -Force` command.

References

<http://technet.microsoft.com/en-us/library/ee176949.aspx>

<http://www.howtogeek.com/117192/how-to-run-powershell-commands-on-remote-computers/>

8.8.16 Remote Install with PSEXec

Description

When you need to perform a remote installation, you have multiple options. You could use a domain policy, a logon script or PSEXec.

Depending on the way the security is configured on the remote computer, you may run into issues that even an administrator cannot install an application properly. For these cases, you need to run PSEXec in the context of the system account. This option is not available (yet) in our PSEXec wrapper, but you can easily use a Command Line (Macro/Script/Tool) instead.



PSEXec is a tool provided by Sysinternals. You must have it installed locally and available in your System Path for it to run successfully with our PSEXec type. For the Command Line tool, you can specify the full path manually.

Options exist to copy files remotely, please refer to PSEXec documentation for further details.

Settings

1. Create the command line (Macro/Script/Tool) and give it a meaningful name.
2. Enter the PSEXec command line as:
`PSEXec \\$HOST$ -s -e msiexec /i {path to msi}`

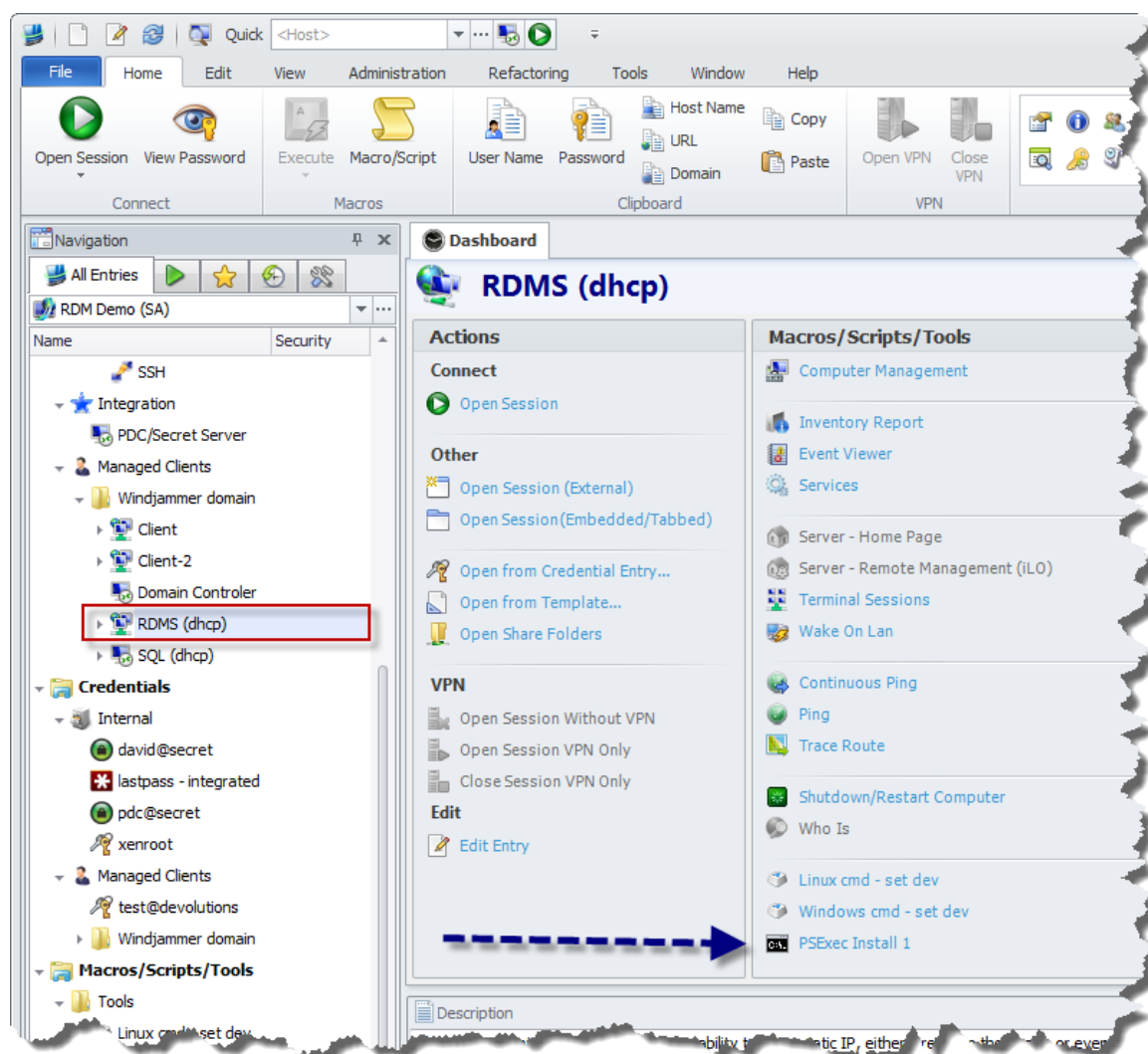


The full path to the msi must be entered. A network share is recommended in this case.

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.

8.8.17 Run as Another User

Description

Most of us use many different credentials. 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 of starting an application under a different set of credentials while we are already logged on using our main credentials.

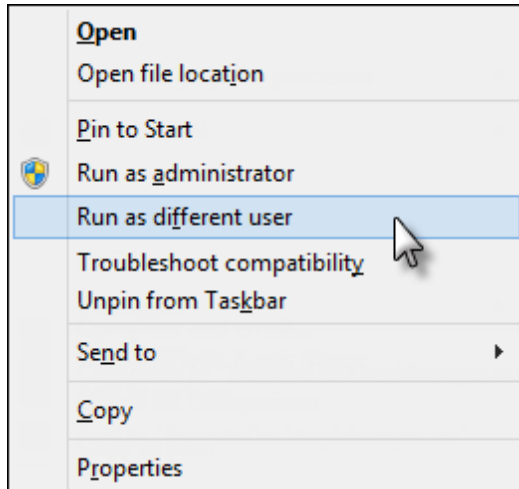
The problem is solved by using the Windows RunAs command.



The RunAs command requires that the "Secondary Logon" service be running.

Settings

In Windows you can manually start any process as a different user using SHIFT + right-click to get the context menu.



SHIFT + right-click popup menu

The RunAs command has many parameters to change its behaviour, we won't cover them all here, but if you have an advanced scenario we suggest you consult the Windows help.

Options

You have two options when it comes to Run As:

- **Built-In Run As**

In Remote Desktop Manager, some sessions/tools types support the Run As functionality. For a complete list and configuration information see the [Built-In Run As](#) help topic.

- **Manual Run As**

Your session type is not supported and needs help to manually configure Run As? See the [Manual Run As](#) help topic.

8.8.17.1 Built-in RunAs

Description



This article describes the built-in method of using Run As. For session types that don't yet support the built-in method you can follow the manual steps outlined [here](#).

Settings

Supported Types

The following types currently support Run As

Option	Description
Session	<ul style="list-style-type: none"> • Command Line • PowerShell
Session Tool	<ul style="list-style-type: none"> • Command Line • PowerShell Local • PowerShell Remote • PSEXec
Session Add-on	<ul style="list-style-type: none"> • SQL Server Management Studio

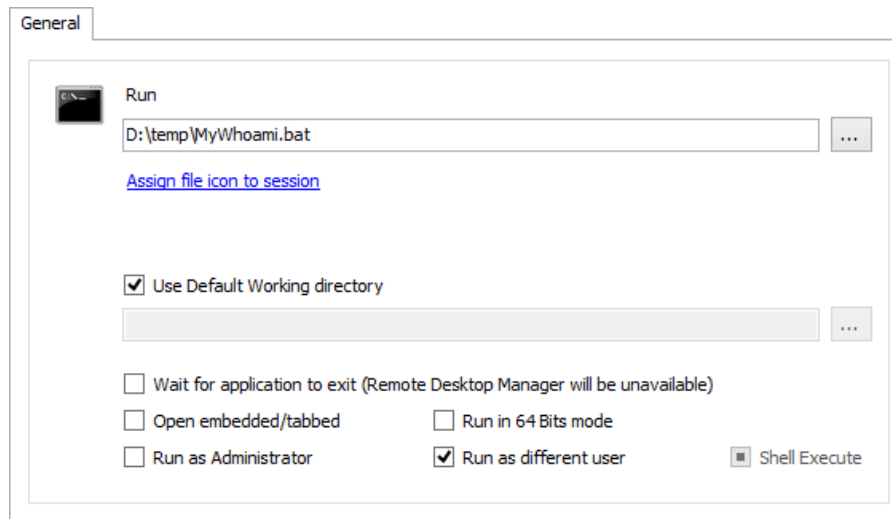
Session

PowerShell session - Run As tab

Sessions that support Run As will have a Run As tab where you specify which credentials to use when starting with Run As.

Option	Description
Disabled	no Run As is performed
Use session credentials	use the same credentials as defined in the session
Use custom credentials	use specified custom credentials
Use credential repository	use a link credential entry
Use my personal credentials	use a link private credential entry

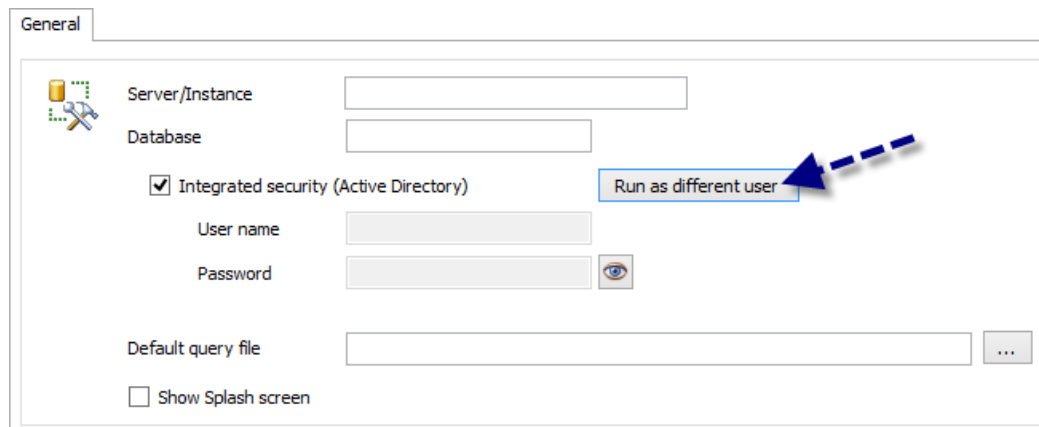
Session Tool

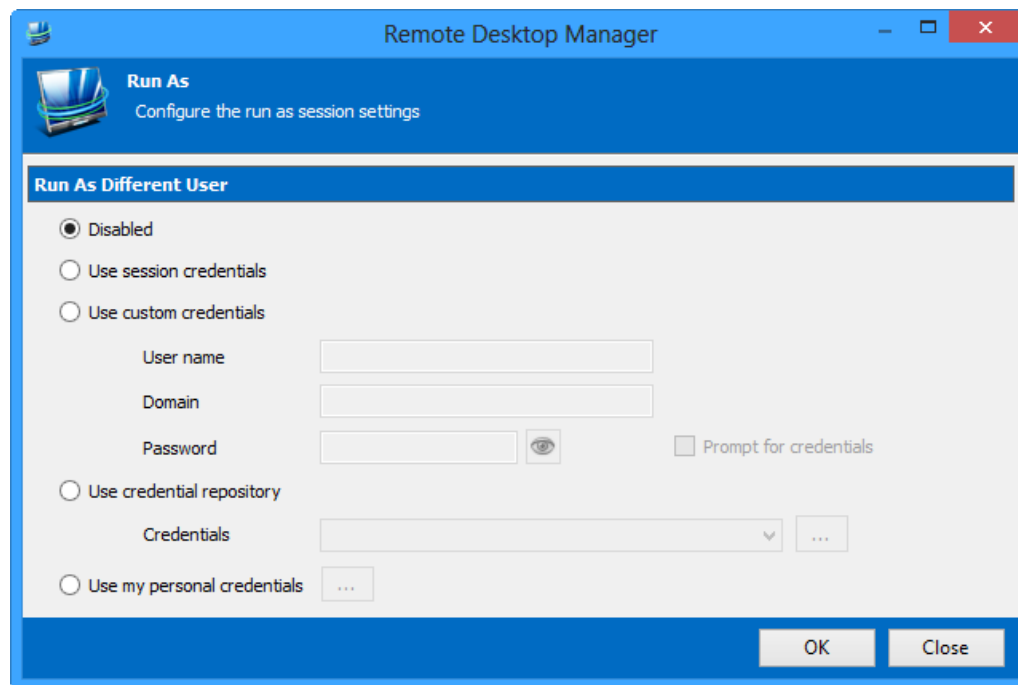
**Command line tools**

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 is the only Add-on that supports Run As. Configure it much you would a normal session.

**SQL Server Management Studio - settings**



Run As - configuration

Notes

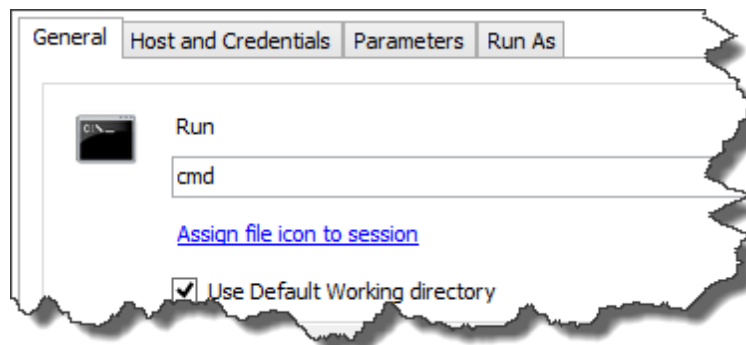
Run as Different User and **Run As Administrator** are mutually exclusive.

Run as Different User doesn't allow for **Shell Execute**.

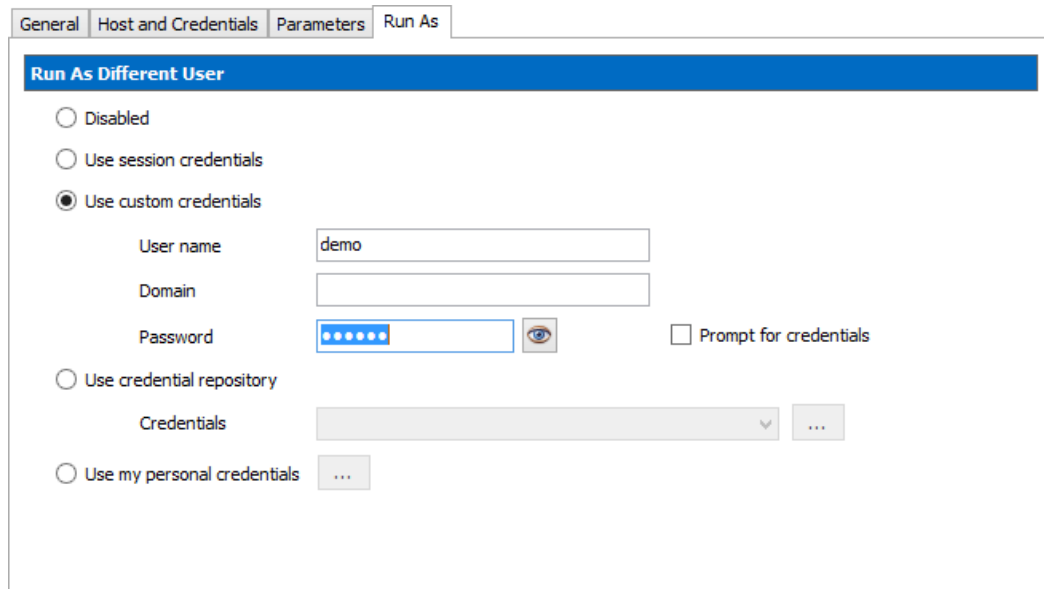
The **NetOnly** parameter is not supported in the built-in Run As support. If you must use the **NetOnly** parameter you must revert to the [Manual Run As](#) method.

Example: Command line session with Run as different user on the same workgroup/domain

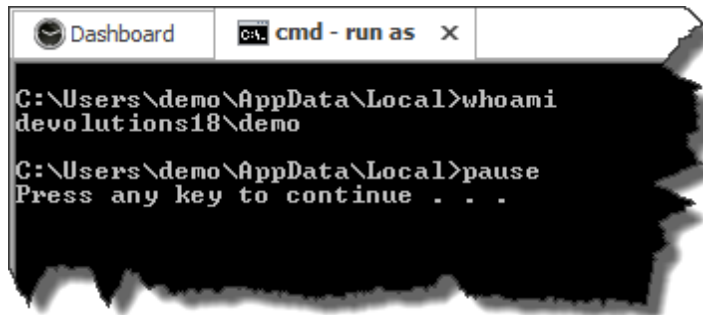
1. Create a new Command Line session.
2. Set the command to **CMD**.



3. Specify the Run As credentials.



4. Save the session.
5. Run the session.



8.8.17.2 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.

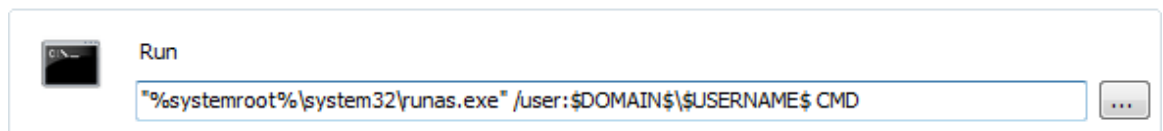
For example you need to connect to a client's domain using your laptop that is on your company's domain. This will require using the **/NETONLY** parameter of RunAs.

Examples

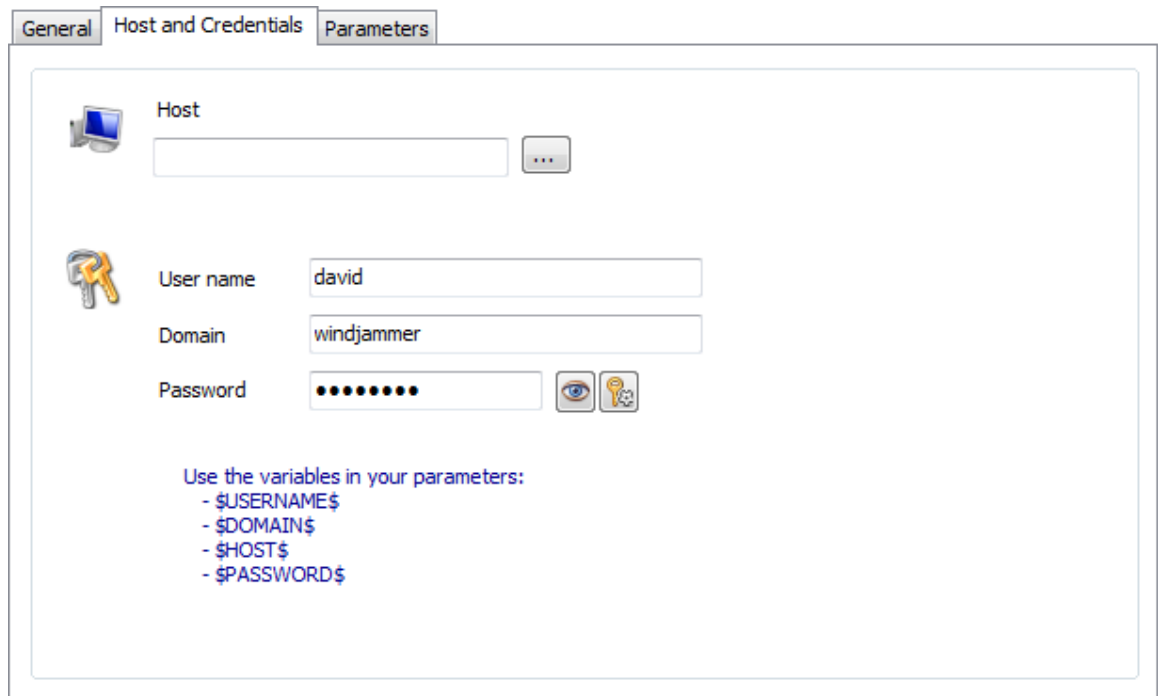
The RunAs command is invoked from an entry of the "Command line" type. Create the entry either by pressing the Insert key or by using the menus. Select the "Command line" type and enter a name for it.

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 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 **/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.



5. In the Events tab you must define a typing macro

- 5.1. Set the Initial Delay to the lowest value that will allow the initial prompt to appear. On most

systems 1 second is sufficient

- 5.2. In the Typing macro field, enter the following: **\$PASSWORD\${ENTER}**. For more information please consult [Auto Typing Macro](#).

After connection

☒ Execute automatically Initial wait 1 sec

Default

Typing macro \$PASSWORD\${ENTER}

Macro password Delay time {Delay} 300 ms

6. In the advanced tab, you must check "**Enable password in variable**".

Connection More VPN Sub Connections Information Events Tools Advanced

Ping

☒ Check host availability
☐ Don't check host availability

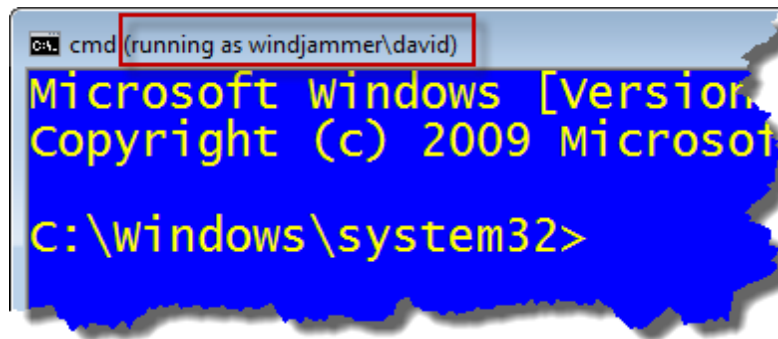
Miscellaneous

Sort priority 0 Sort priority default is 0. Use a higher value to place this item before other entries.

☒ Allow password in variable
☐ Embedded footer visible
☐ Open undocked
☐ Force machine name as domain name (override the credentials)
☐ Allow open multiple connections

Internal information

When you run your session, a command prompt window appears requesting the password for the user. The Typing Macro will fill it in after the 1 second delay. After this, the command window that is running under the different credentials appears. Note that the title indicates the other identity.



Example 2: Running SQL Server Management Studio as a user of a different domain/workgroup for using Windows Authentication

There are minor differences with Example 1, but here is the full procedure to make it easy to read

1. You can use the ellipsis button to browse for the `runas.exe` command, but if you are in a shared data source and the session will be used on various operating systems, it's better to type in `"%systemroot%\system32\runas.exe"` because it will work on all of them.
2. Append `/netonly /user:$DOMAIN\$USERNAME$`, keeping it outside of the quotes. Note the use of two variables that will pull the appropriate value from other fields of the same session. For more information please consult the [Variables](#) topic. Also note the use of the **NetOnly** parameter, it signals that the credentials will be used for network access only.
3. Append the name of the Management Studio executable and its parameters. All this needs to be within the same double quotes
- 3.1. SQL Server Management studio is located at "C:\Program Files (x86)\Microsoft SQL Server\110\Tools\Binn\ManagementStudio\Ssms.exe" on most machines, adapt to your situation if it's not the same.
- 3.2. My parameters look like this: **-S sql.windjammer.loc -E**. -S is for the server name, -E is to use windows authentication, you can even specify the database using -d __DB_NAME__ (i.e. -d rdm)

The result is: "C:\Program Files (x86)\Microsoft SQL Server\110\Tools\Binn\ManagementStudio\Ssms.exe -S sql.windjammer.loc -E"

4. Uncheck **"Use Shell Execute"** (this must be done for most Windows Applications)

General Host and Credentials Parameters

Run

`"%systemroot%\system32\runas.exe" /netonly /user:$DOMAIN\$USERNAME$ "C:\Program Files (x86)\Internet Explorer\iexplore.exe"` ...

[Assign file icon to session](#)

☒ Use Default Working directory

...

☐ Wait for application to exit (Remote Desktop Manager will be unavailable)

☐ Run as Administrator ☐ Run in 64 Bits mode ☐ Use Shell Execute

Process name

[Set default process name](#)

TIP: Use default process name if you want your application to be listed in the opened sessions

Embedded wait time 250 ms

7. Specify your credentials in the **Host and Credential** tab. Note that when you are not part of a domain, you should enter the computer name in the domain field.

General Host and Credentials Parameters

Host

...

User name david

Domain windjammer

Password

Use the variables in your parameters:

- \$USERNAME\$
- \$DOMAIN\$
- \$HOST\$
- \$PASSWORD\$

8. In the Events tab you must define a typing macro

- 8.1. Set the Initial Delay to the lowest value that will allow the initial prompt to appear. On most

systems 1 second is sufficient

- 8.2. In the Typing macro field, enter the following: **\$PASSWORD\${ENTER}**. For more information please consult [Auto Typing Macro](#).

After connection

☒ Execute automatically Initial wait 1 sec

Default

Typing macro **\$PASSWORD\${ENTER}**

Macro password Delay time {Delay} 300 ms

9. In the advanced tab, you must check "**Enable password in variable**".

Connection More VPN Sub Connections Information Events Tools Advanced

Ping

☒ Check host availability
☐ Don't check host availability

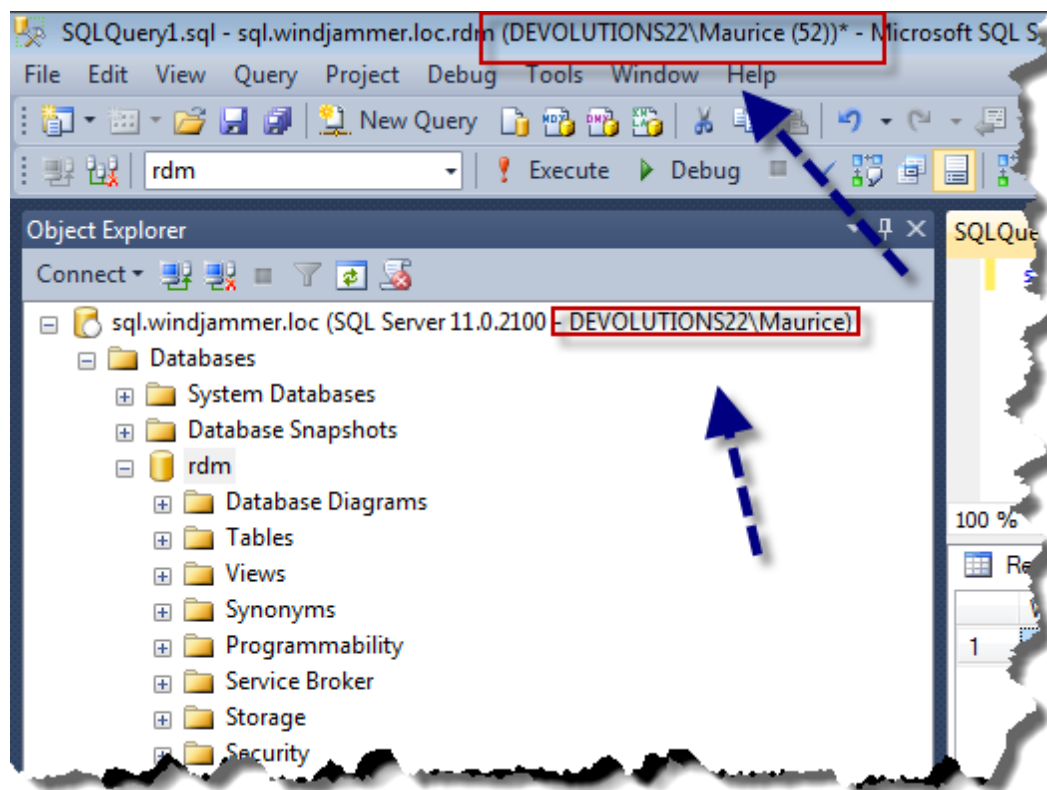
Miscellaneous

Sort priority 0 Sort priority default is 0. Use a higher value to place this item before other entries.

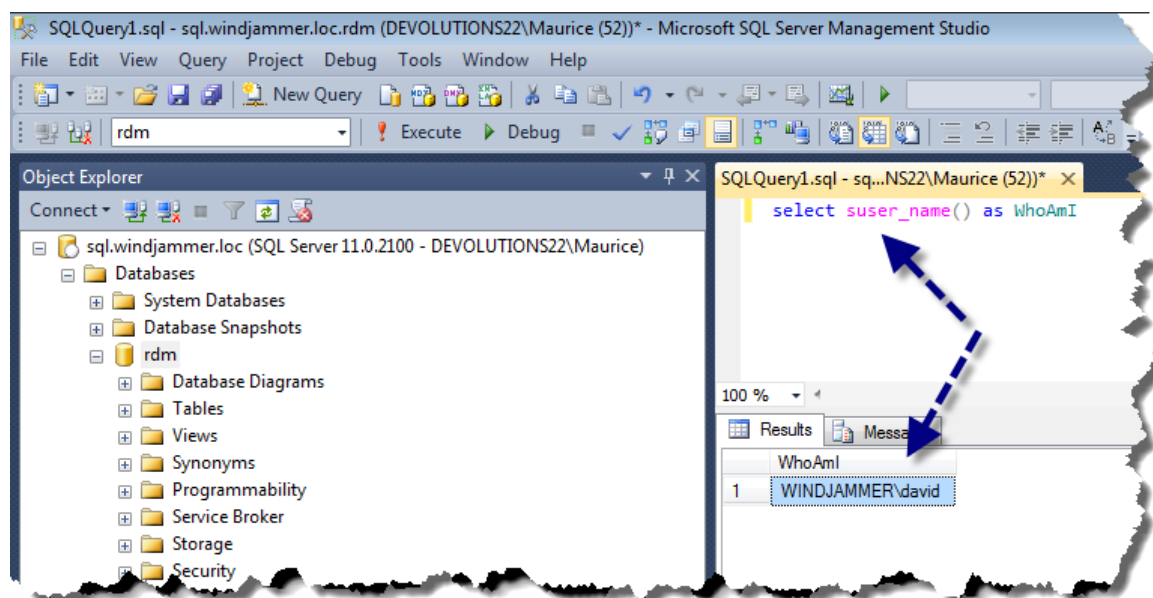
☒ Allow password in variable
☐ Embedded footer visible
☐ Open undocked
☐ Force machine name as domain name (override the credentials)
☐ Allow open multiple connections

Internal information

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 USER_NAME()*** query.



8.8.18 Running Remote Desktop Manager as Another User

Description

Most of us use many different credentials. 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 of starting Remote Desktop Manager under a different set of credentials while we are already logged on using our main credentials. This will allow you to use Integrated security to connect to an [Advanced Data Source](#).



These solutions require that the "Secondary Logon" service be running.

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 won't cover them all here, but if you have an advanced scenario we suggest you consult the Windows help.

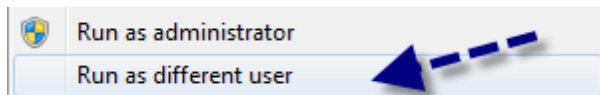
1. Open a command prompt
2. Type ***runas /netonly /user:{your user name here}***. Usage of the ***NetOnly*** parameter signals that the credentials will be used for network access only. Ensure your user name is entered as your infrastructure requires. Typically it's {domain}\{user}, i.e. windjammer\david
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

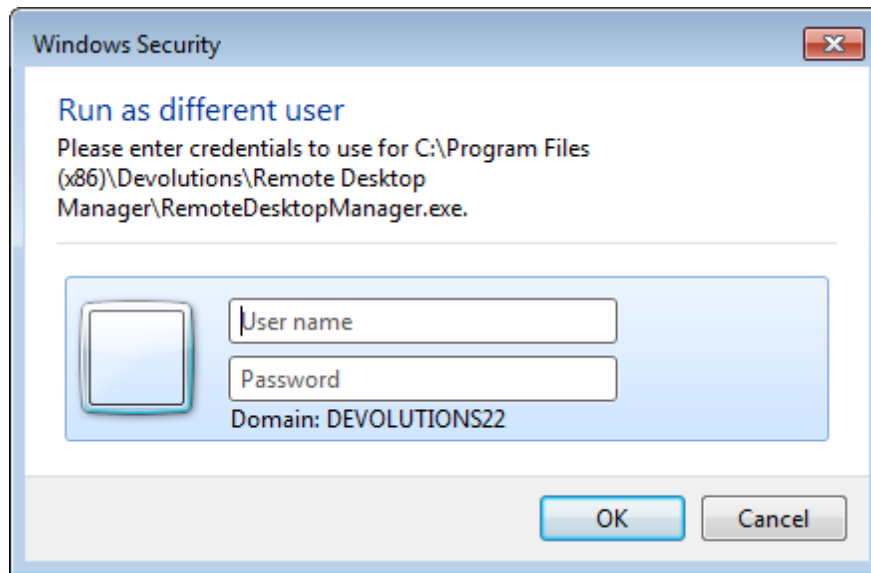
Solution B - Shift+Right Click on the shortcut or executable to Remote Desktop Manager

When you press Shift + Right Click on an executable, you'll notice an additional menu item for **Run as different user**.



Advanced contextual menu

You are presented with a logon form in which you must specify the username and password.



8.8.19 SQL Server Data Source with Integrated Security

Overview

We will take you through a step by step guide on configuring and testing a Remote Desktop Manager deployment against a 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.

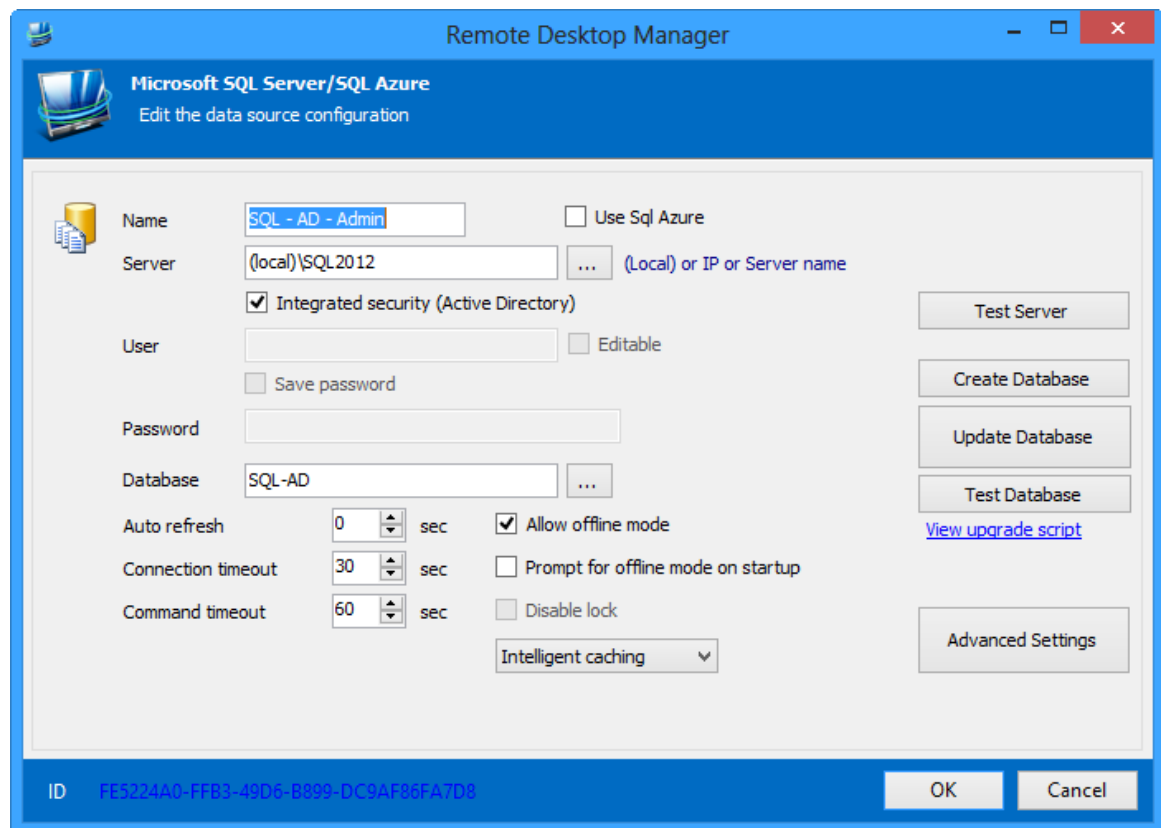
File -> Data Sources -> Add a new Data Source

- Specify the Name, Server & Database
- Make sure you authenticate with a user that is part of the **sysadmin** role.



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 after the fact and change the data source to use **Integrated security**.

- Press **Test Server** to test the connection to the server.
- Press **Create Database** to actually create the Remote Desktop Manager database.



Create new data source

Press ok to close the dialog. In the navigation pane, select your newly created data source from the data source drop down.

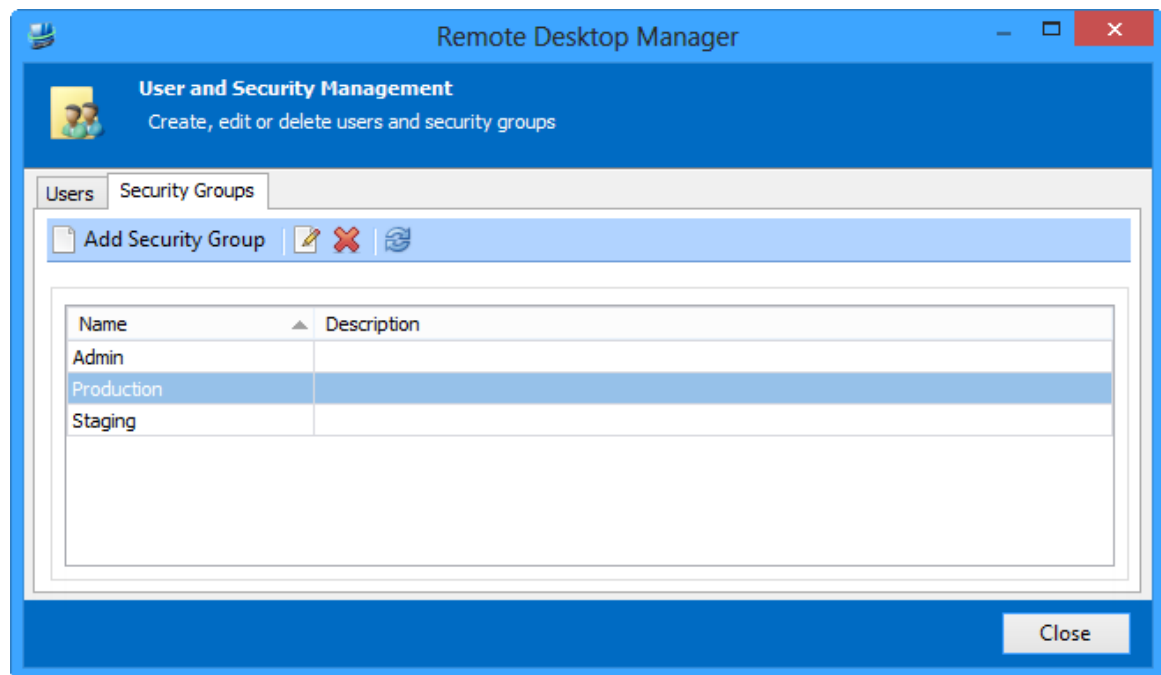
Create the security groups and users

Administration -> Security Groups

Add some security groups. In the case I've added Admin, Production & Staging security groups. This will allow me to limit access to sessions to a subset of users.

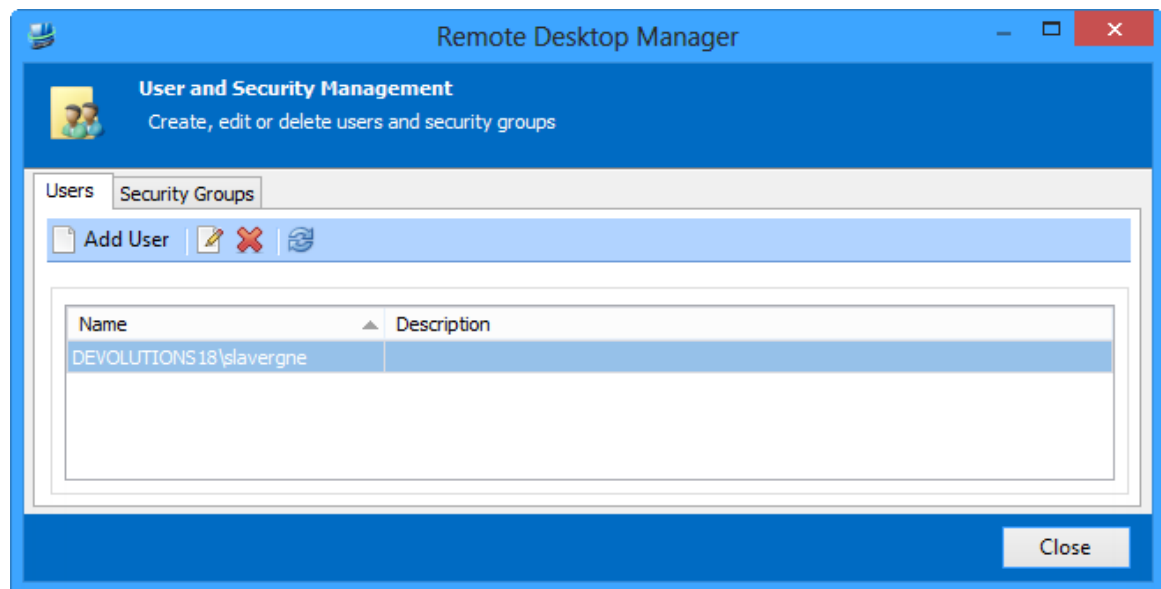


For more information on [Security Groups & User management](#).



Security groups management

The next step is to add the other users.



User management

Administration -> Users -> Add User

- First check **Integrated security (Active Directory)** - this will enable the ... button, click it & select the domain user you would like to add.
- In the General tab, check **Add, Edit & Delete**
- In the Groups check **View, Add, Edit & Delete** of the **Staging** security group.

User management
Edit user settings

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

Description:

Password: ☒ Create SQL Server Login and User

☒ Allow offline mode ☐ Allow reveal password

☐ Administrator

General

☒ Add
☒ Edit
☒ Delete

☒ View details ☒ Allow drag-and-drop
☒ View information
☒ View shared logs

☐ Import
☐ Export

Groups

Name	View	Add	Edit	Delete
Admin	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Production	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Staging	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

2774dd27-c75b-44ed-8ad5-6db25042df06

OK Cancel

Add new domain user



Keep **Create SQL Server Login and User** 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 you've already added a login for the domain group for example. Since the user is part of the group in question they would be granted login privileges through the groups access, not through a user specific account. This would help minimize support tasks in SQL Server.

So now we've created a non-admin user that only has access rights to the Staging security group. Repeat for each user that needs access to this data source in Remote Desktop Manager.

Remote Desktop Manager for Client Workstations

Now we need to configure Remote Desktop Manager on other client workstations. You have a few options here:

- Create the data source just like you did the first time, making sure you've set **Integrated Security (Active Directory)**
- Export the data source from the initial workstation and import into Remote Desktop Manager on all client workstations.

- Use our [Custom Installer](#) service to help you distribute the application and personalize the installation process.

Testing

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 that has admin rights, create a few sessions and assign them a security group (Admin, Production or Staging). Leave the security group blank for some sessions.

Now in Remote Desktop Manager running under a limited account, refresh the data source, you will only see the sessions that are part of the security group for which you've granted rights to this user.

8.8.20 SQL Server Maintenance Plans

Description

A Sql Server Instance is, sadly, 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.

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. It does not meet your specific requirements and 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 thru the recovery process regularly to prove that it works.

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...



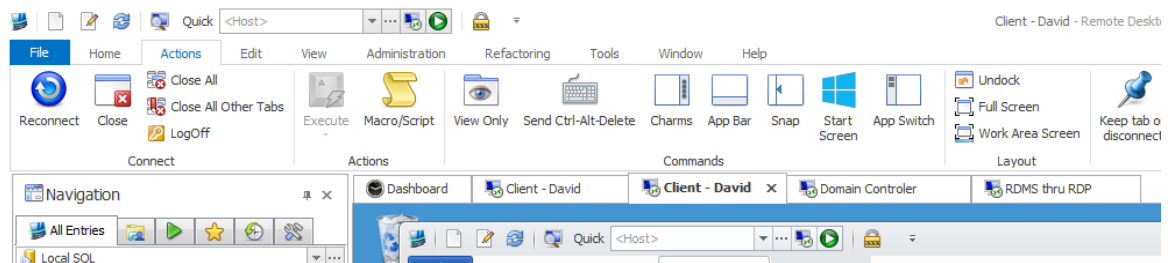
Backup plans must be monitored and Recovery plans must be enacted to confirm they actually work!

8.8.21 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 remoting technologies at the same time. No longer you have to dig in your task bar to locate the session of interest, you have all of them running in tabs in the same tool that you use to launch them.

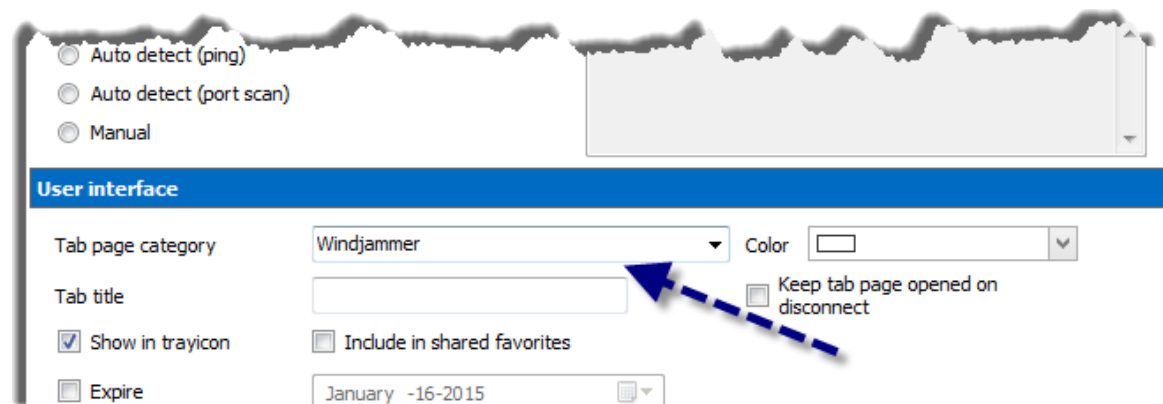
But when you reach a certain number of running sessions, it may become difficult to identify them using only their name. To improve on the user experience for those of us that love embedded sessions, we created a feature to Filter the tab pages, it is called the *Tab Page Category*.



Embedded/Tabbed sessions

Settings

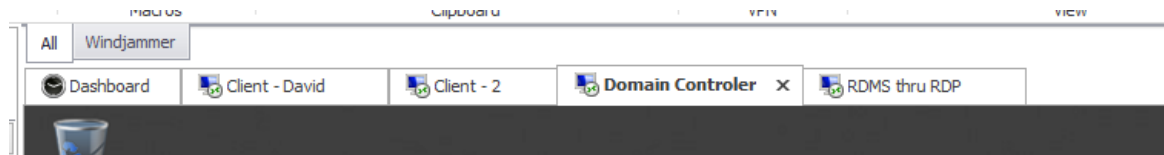
The setting is in the *More* tab of the session settings.



User Interface section of the More tab

Simply typing in a name will create a tab group when you launch the instance. You can see it in action

in the image below



Tab groups displayed - All selected

When the All group is selected, it performs no filtering. When you select another group, it hides all the sessions that do not match with the filter. In the example below, I've adjusted two sessions to have the same category.



Specific tab group selected

8.8.22 Team Tips

Overview

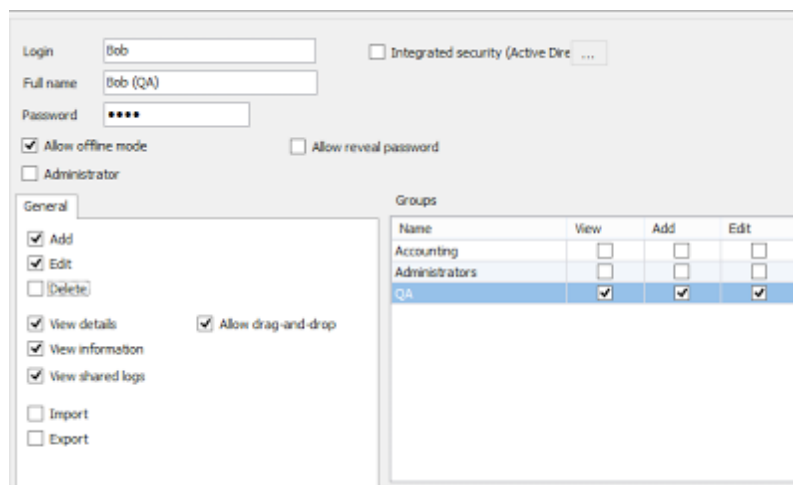
Here are 5 RDM team tips.

Security, Users & Groups

Sharing session information is great -- but controlling access is bliss.

Through RDM's Groups & Security settings, you can control access and user rights for specific sessions and actions.

Start by defining the groups, and assign users rights for each appropriate user. Keep in mind that once sessions are assigned to a security group, users must have access rights to them. Sessions without a security group are considered public.



Streamlined Deployment With Custom Installer

Okay: you're ready to deploy RDM 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 preconfigured RDM 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 RDM 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. Is this going to cause misery and perhaps rioting? No!

We've made it extremely easy. Simply open Administration -> Data Source Settings -> Version Management tab. Let me explain some of the settings.

- **Disable auto update** – 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.
- **Client install path/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.
- **Serial (Site/Global)** – This 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

The general tab of the Data Source Settings form allows you to easily control security aspects, such as allowing offline mode and specifying the expiration policy of offline data. 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 above. A little bit of chaos is good for the soul.

Remote Desktop Manager Server (RDMS)

Do you need Active Directory group or role management? Or perhaps you have offsite 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? RDMS delivers all that and much more!

You can deploy RDMS internally or online to create an enterprise wide high-end data store. And RDMS comes with a complete Remote Desktop Manager client Global License, which means an unlimited amount of users can use it worldwide. Find out more about RDMS at <http://remotedesktopmanagerserver.com/>.

8.8.23 VPN

8.8.23.1 VPN Group

Overview

A VPN Group will regroup the entries which share the same VPN connection.

When multiple entries are members of the same VPN group and 2 or more of them are connected, the VPN connection will stay active until the last session disconnects.

The VPN group name needs to be exactly the same to ensure that Remote Desktop Manager increments the usage counter.

The VPN close mode need to be set to **On sessions close** to use this feature.



VPN groups are defined inside each individual entries under the VPN tab.

8.8.23.2 VPN Routing

Overview

Establishing a VPN connection using Remote Desktop Manager is easy. Unfortunately, adding routes has to be done manually. Wait for the adapter to connect, find the IP and add the desired routes. Even if you use a script (such as a Power Shell script), it's still a redundant time consuming task – and one you can certainly live without.

```
C:\Windows\system32>ROUTE ADD 10.1.2.5/32 100.77.183.56
OK!

C:\Windows\system32>ROUTE PRINT
=====
IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway
0.0.0.0                    0.0.0.0          192.168.1.1
10.1.2.5                    255.255.255.255  100.77.183.56
127.0.0.0                  255.0.0.0        On-link
127.0.0.1                  255.255.255.255  On-link
127.255.255.255            255.255.255.255  On-link
192.168.1.0                255.255.255.0    On-link
```

Solution

This feature is part of a larger concept called Post/Pre VPN Commands, and allows you to run any type of script or executable post-VPN-connect and pre-VPN-disconnect.

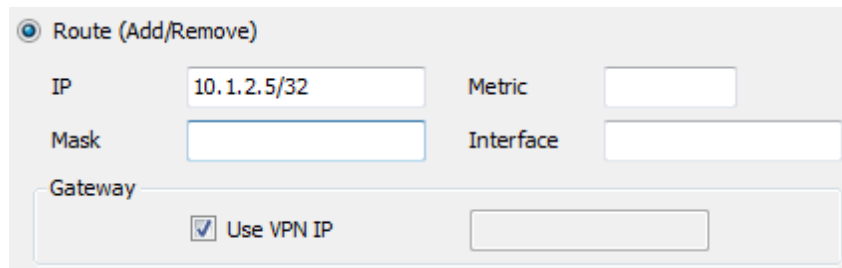
The screenshot shows the 'Advanced' tab of the VPN configuration window. Under the 'After execute wait' section, the 'For IP on adapter' radio button is selected. Below this, the 'Commands' section contains a table with two columns: 'After connect command' and 'Before disconnect command'. The 'Home' entry is highlighted in the table. At the bottom, there are checkboxes for 'After Connect VPN command enabled' and 'Before disconnect VPN command enabled', both of which are checked.

Name	After connect command	Before disconnect command
Home	ROUTE ADD 10.1.2.5/32 \$GATEWAY\$	ROUTE DELETE 10.1.2.5/32

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 **Custom Pre/Post Connect VPN Commands** dialog.
3. Create a route definition by selecting “**Route (Add/Remove)**” radio item. Finally, set the IP and any other required information.



8.9 Troubleshooting

Description

Consult sections below to get more information about:

- [Data Sources](#)
- [MySQL Data Source](#)
- [SQL Server Data Source](#)
- [General Troubleshooting](#)
- [FIPS \(Encryption\)](#)
- [Large Memory Aware Application](#)
- [LogMeIn](#)
- [Microsoft RDP](#)
- [Automatic Logon](#)
- [Logoff Access Denied](#)
- [Performance](#)
- [Profiler](#)
- [Putty](#)
- [RPC](#)
- [SSH](#)
- [User Interface](#)
- [VPN](#)
- [Web Browsers](#)
- [WMI](#)

8.9.1 Data Sources

Errors

Unable to connect to a Data Source

1. The name of the data source is entered incorrectly.
2. The machine is unable to resolve the name of the data source host using DNS.
3. opening a VPN had disconnected the local LAN or rendered the data source unreachable.
4. An Anti-virus or Firewall is blocking the application.

8.9.1.1 MySQL

Errors

Connecting to MySQL using a private certificate

1. Create SSL keys as described in [Creating SSL Certs](#)
2. Create a client certificate as described in [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

8.9.1.2 SQL Server

Errors

New SQL Server installation

On a new SQL Server installation, remote connections must be allowed manually. Follow these [Directions](#) to enable connectivity.

Unable to connect to SQL Server

1. Go in Help -> View Application Logs to see if relevant error messages are present.
2. The name of the data source is wrong.
3. Is the SQL Server is up and running. (Are you able to ping the server ?)
4. Create a Universal Data Link (.udl) file to test your SQL Connection (see sections below).
5. Anti-virus or Firewall blocking the application.

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.

Create a Universal Data Link (.udl) file

1. Open **Windows Explorer**
2. Select the folder in which you want to store the **.udl** file
3. If you are running Windows 2000 or later, select **New** on the **File** menu, and choose **Text Document**. A new file named **New Text Document.txt** appears in the directory. Rename this file, removing all spaces and changing its file extension to **.udl**.



A warning that changing file extensions can cause files to become unusable might appear. Disregard it.

If you are running Windows 98 and Windows NT systems with Microsoft Data Access Components (MDAC) installed, right-click the right pane, or results pane, select **New**, and choose **Microsoft Data Link**. A new file named **New Microsoft Data Link.udl** appears in the directory. You can rename this file.

Configure a universal data link (.udl) file

1. Double-click the universal data link (**.udl**) file. The **Data Link Properties** dialog box opens, displaying the following tabs: **Provider**, **Connection**, **Advanced**, and **All**. Choose **Next** to navigate from tab to tab.
2. On the **Provider** tab, select a database provider.
3. On the **Connection** tab, either select the data source name (DSN) of an available Provider, or enter a custom connection string. Valid DSNs for providers that are pre-defined on your system are displayed in the **Use Data Source** drop-down list.
4. Use the **Advanced** tab to view and set other initialization properties for your data.
5. Use the **All** tab to review and edit all OLE DB initialization properties available for your OLE DB provider.
6. Choose **OK** to save the connection string to the Universal Data Link (**.udl**) file.

8.9.2 General

Errors

"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 2.0 installation. We recommend that you try and repair the .NET Framework, or follow the instructions in the Microsoft Knowledge base article "[How to repair an existing installation of the .NET Framework](#)".

My mapped network drive(s) are not available when using Run As Administrator to launch RDM

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 <http://support.microsoft.com/kb/937624>.

8.9.3 FIPS (Encryption)

Errors

“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

In the RDM installation folder, create a text file named ***RemoteDesktopManager.exe.config*** containing the following:

```
<configuration>
  <runtime>
    <enforceFIPSPolicy enabled="false"/>
  </runtime>
</configuration>
```

8.9.4 Large Memory Aware Application

Description

Remote Desktop Manager is currently a 32 bit application, this impacts the limits the amount of memory it can use to 2 Gb. This didn't cause issues until the coming 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.

We are currently in the process of publishing a 64 bit version that will allow the application to use as much memory as is available, in the mean time, we've modified Remote Desktop Manager to allow it to access more memory, but this must be paired with a modification to your operating system.



You can perform this only if you have more then 2 Gb of RAM

Instructions

Windows XP/Server 2003

1. Right-click My Computer and select Properties. The System Properties dialog box will appear.
2. Click the Advanced tab.
3. In the Startup and Recovery area, click Settings. The Startup and Recovery dialog box will appear.
4. In the System startup area, click Edit. This will open the Windows boot.ini file in Notepad.
5. In the [Operating Systems] section, add the following switches to the end of the startup line that includes the /fastdetect switch: /3GB
6. Save the changes and close Notepad.
7. Click OK two times to close the open dialog boxes, and then restart the computer for the change to take effect.

Windows Vista, Windows 7, Server 2008



The memory parameter can be any value between 2048 (2 GB) and 3072 (3 GB). If you have 3Gb of RAM you must reserve some for your system. If you have 3 Gb of ram, allocate 2560 Mb, for 4 Gb systems use 3072.

1. Open command prompt with Administrator rights. To do this, go to Programs, Accessories, right-click on Command Prompt and select "Run as Administrator."
2. Enter the following at the prompt and press enter:

```
bcdedit /set IncreaseUserVA 2560
```

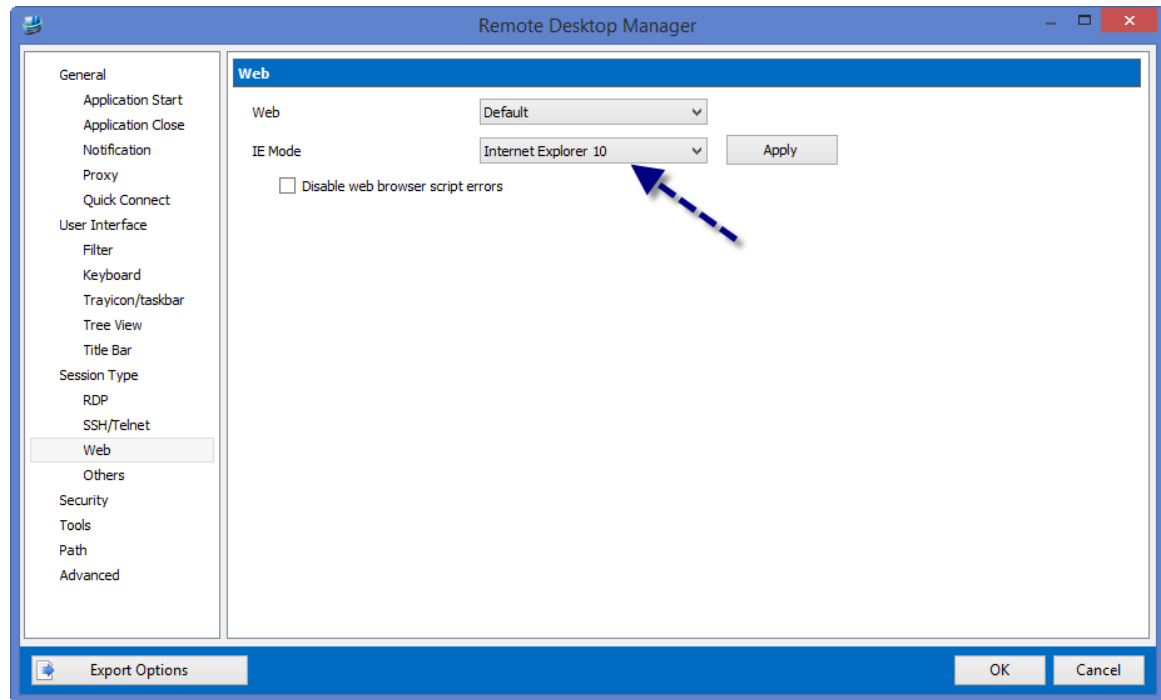
3. Close the prompt and restart the computer.

8.9.5 LogMeIn

Errors

COMException - Requested resource in use. (Exception from HRESULT: 0x800700AA)

Change the IE emulation mode in File -> Options | Session Types -> Web to use IE10



IE Mode

8.9.6 Microsoft RDP

The Microsoft RDP client is not working properly

The components of the Remote Desktop client are considered a core Windows feature, therefore there are no facilities to reinstall them. However, there is a tool to verify and repair system files.



Running the SFC command takes a long time.

1. Open an elevated command prompt (right click on command prompt, and select Run As Administrator)
2. Run the command `SFC /VERIFYONLY` to verify the system files or `SFC /SCANNOW` to verify them and attempt a repair

Automatic Logon

Automatic logon troubleshooting is in the [Automatic Logon](#) topic.

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.

Unable to find mstsc.exe in Windows Vista

Vista 64-bit edition requires Service Pack 1

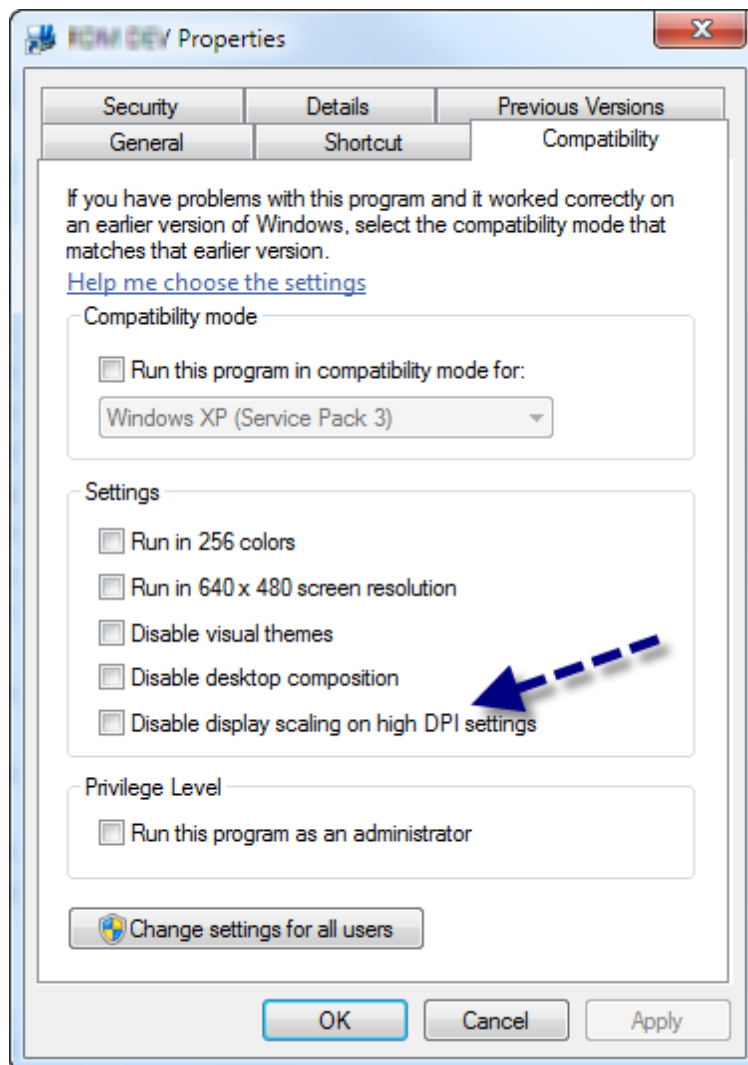
I receive an error when I try and get session details, or when I execute a logoff with an RDP session. How do I fix this?

Please read the information [Logoff Access Denied](#).

Screen areas unresponsive in embedded sessions.

This most often occurs on systems that use a DPI setting of more than 100%. To disable scaling in RDM you must adjust the compatibility settings on the Windows shortcut for RDM.

1. Right-click on the shortcut to RDM
2. Select Properties
3. Go to the "Compatibility" tab
4. Check "Disable display scaling on high DPI settings"



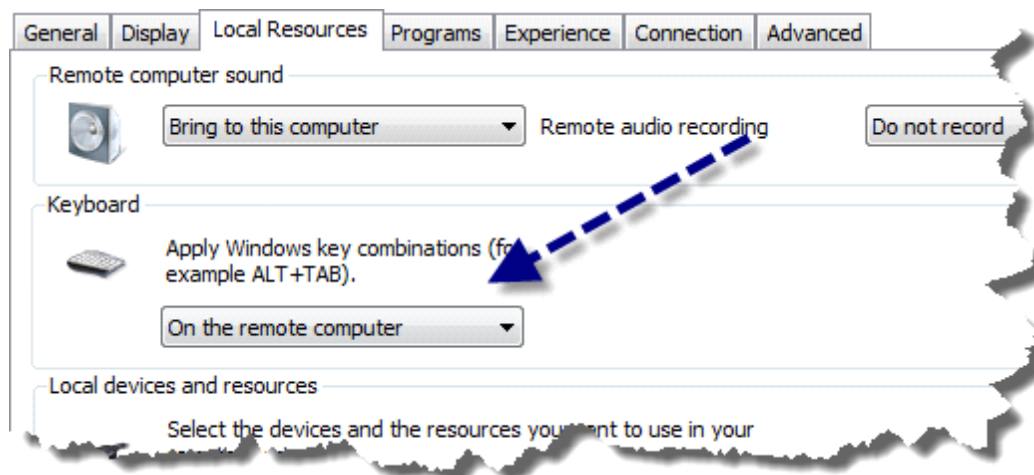
Compatibility tab

I have multiple sessions to the same computer with different credentials, but it always uses the last one I entered.

This issue stems from the fact that the Windows credential repository holds only one entry per Windows user for a remote computer. If you use the Embedded 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.

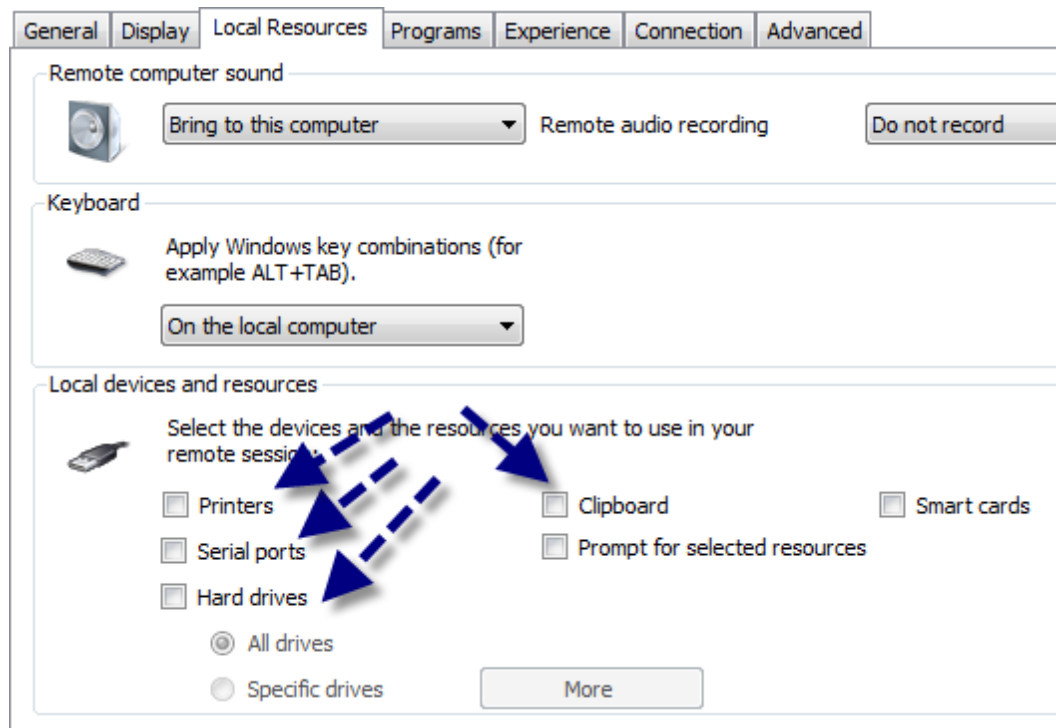
You must configure the Keyboard setting in the Local Resources tab of the session settings. You can select "On the remote computer" or "In full screen only" according to your personal preferences.



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 always up to date then it should be something else.

Sometimes the mapping of local devices will cause issues. Try to disable all device sharing to see if connectivity is restored.



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. Load up task manager (right click taskbar and select Task Manager)
2. Go to the Processes Tab
3. Select rdpclip.exe
4. Click End Process
5. Go to the Application Tab
6. Click New Process
7. Type rdpclip
8. Click Ok

Copy/paste operation WITHIN THE REMOTE HOST are extremely slow

As strange as it may seem, we've isolated the issue to "Serial Ports" being

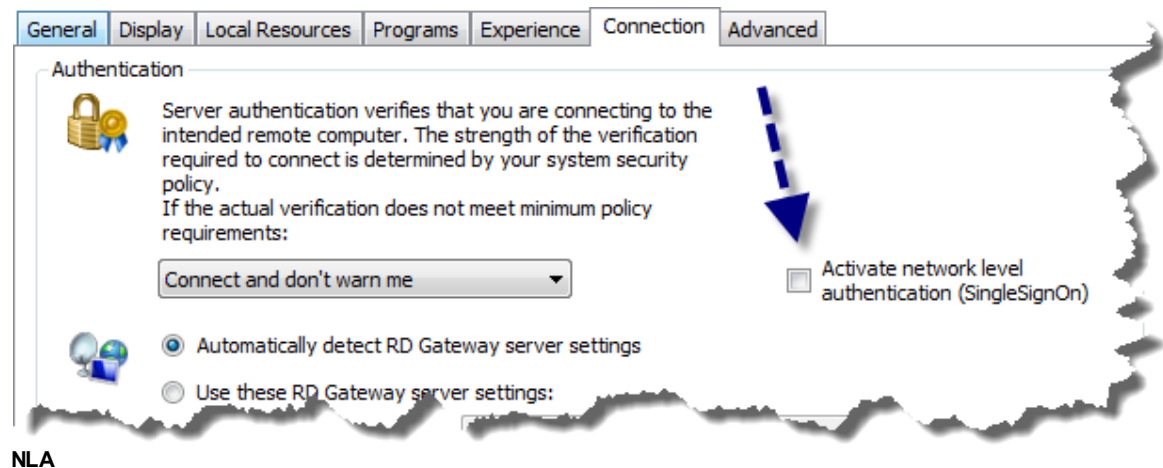
8.9.6.1 Automatic Logon

Description

Sometimes the automatic logon does not function and your credentials are requested by the remote system. Here are some steps to help identify the issue. Support for automatic logon was introduced on Windows 2003/XP, so ensure you are trying to connect to these or later versions. Windows 2000 does not support the automatic login.

RDP Sessions connect successfully when in external mode, but not in embedded mode.

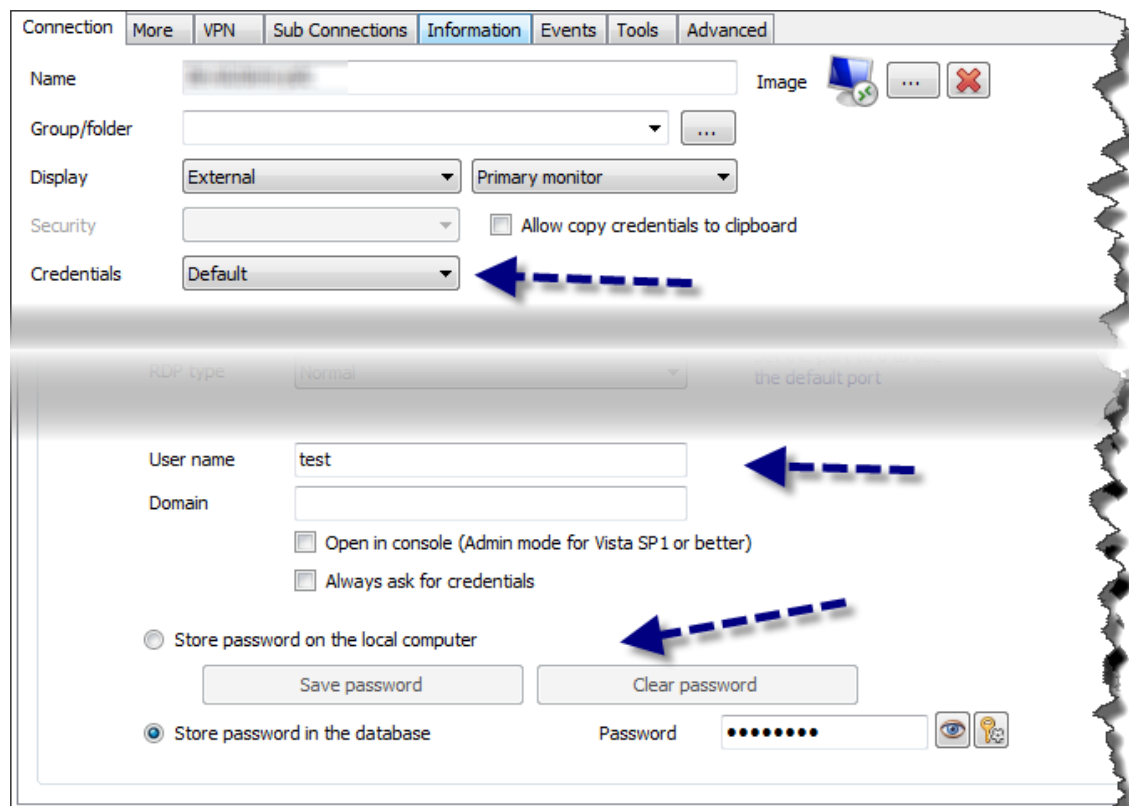
This issue may be caused by a bad authentication negotiation because in some cases **Single Sign On** (SSO) requires **Network Level Authentication** (NLA). It can happen when prompting for credentials and when using automatic logon. Please activate "Network Level Authentication" in the Connection tab of your session.



See also : [Network Level Authentication](#), [Configure NLA for Remote Desktop Services Connections](#)

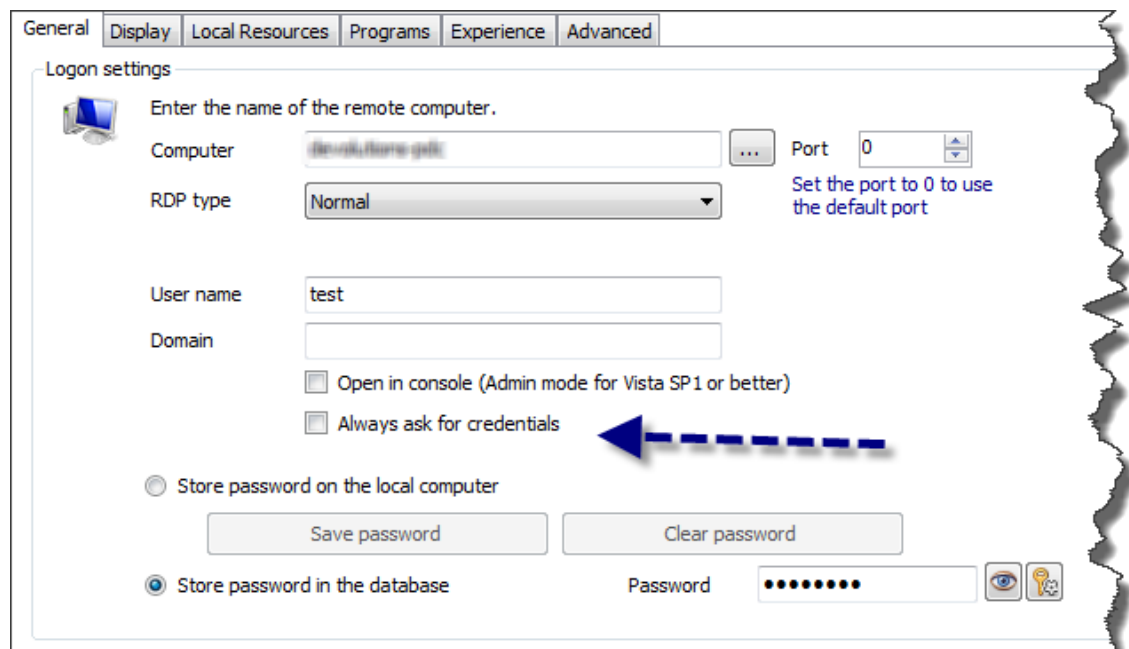
Ensure credentials are entered properly.

RDM allows for advanced credential management. Depending on your choice of: *Default*, *Credential Repository*, *Embedded* or *Inherited*, ensure the credentials are properly entered. Please see [Credentials](#)



Credential types

Ensure that "Always ask for credentials" is not checked.



Always ask for credentials

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 this is the case.

Choose the instructions depending on the server operating system. Note that there are often multiple ways to configure the host (WMI, Scripting, etc), but the group policies are the preferred method. Therefore the links are for the articles describing group policy solutions when they are available.

Applies To	Link
Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 with SP1, Windows Server 2003 with SP2	Configuring Terminal Services with Group Policy
Windows Server 2008	Group Policy Settings for Terminal Services in Windows Server 2008
Windows Server 2008 R2	Group Policy Settings for Remote Desktop Services in Windows Server 2008 R2
Windows 2012	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

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>

8.9.6.2 Logoff Access Denied

Logoff Access Denied Error or "Unable to enumerate remote sessions"

This section describes the solution for the "access denied" error 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 you are 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 use 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.

Of course the user in the credential should be a user on the remote server who has enough privilege to carry out the operation.

2. Open RPC ports on firewall

An API call involves connecting to a remote machine use 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 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.

The two ways are equivalent. If this option is set to 1, remote logged 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 probably 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 get 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:

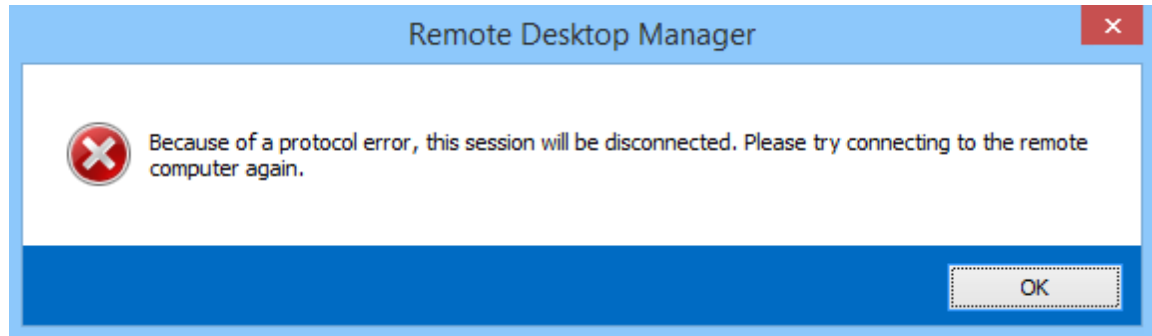
HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server

Then add a DWORD value named "AllowRemoteRPC" and change its value to 1.

8.9.6.3 Protocol Error

Errors

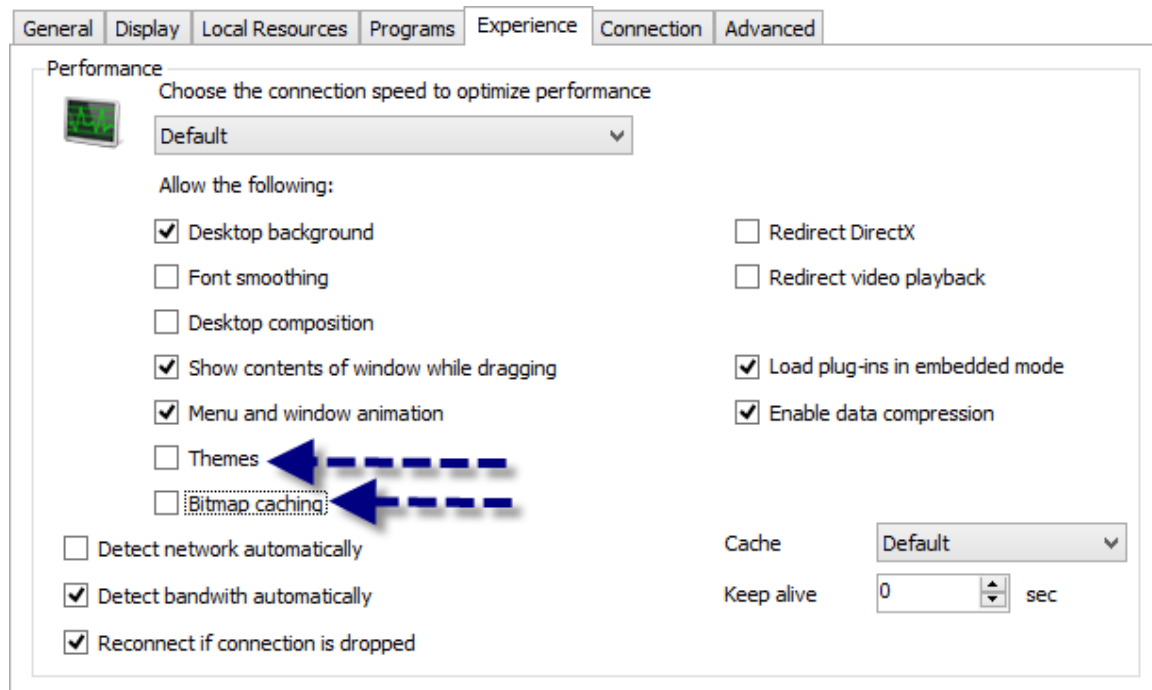
Because of a protocol error, this session will be disconnected. Please try connection to the remote computer again.



Error message

Solution 1

Uncheck Bitmap Caching and Themes under Experience tab



Uncheck Themes and Bitmap caching

Solution 2

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 3

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.

8.9.7 Performance

Startup

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. Please note that this is exceptional and occurs when your data source contains a great number of connections.

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](#)
- <http://blogs.technet.com/b/markrussinovich/archive/2009/05/26/3244913.aspx>

The workaround is to create a text file in Remote Desktop Manager installation folder, named **RemoteDesktopManager.exe.config** and containing the following:

```
<configuration>
  <runtime>
    <generatePublisherEvidence enabled="false"/>
  </runtime>
</configuration>
```

Refresh

This category affects all data source refreshes, therefore also the initial load at program startup.

Heavy usage of custom images

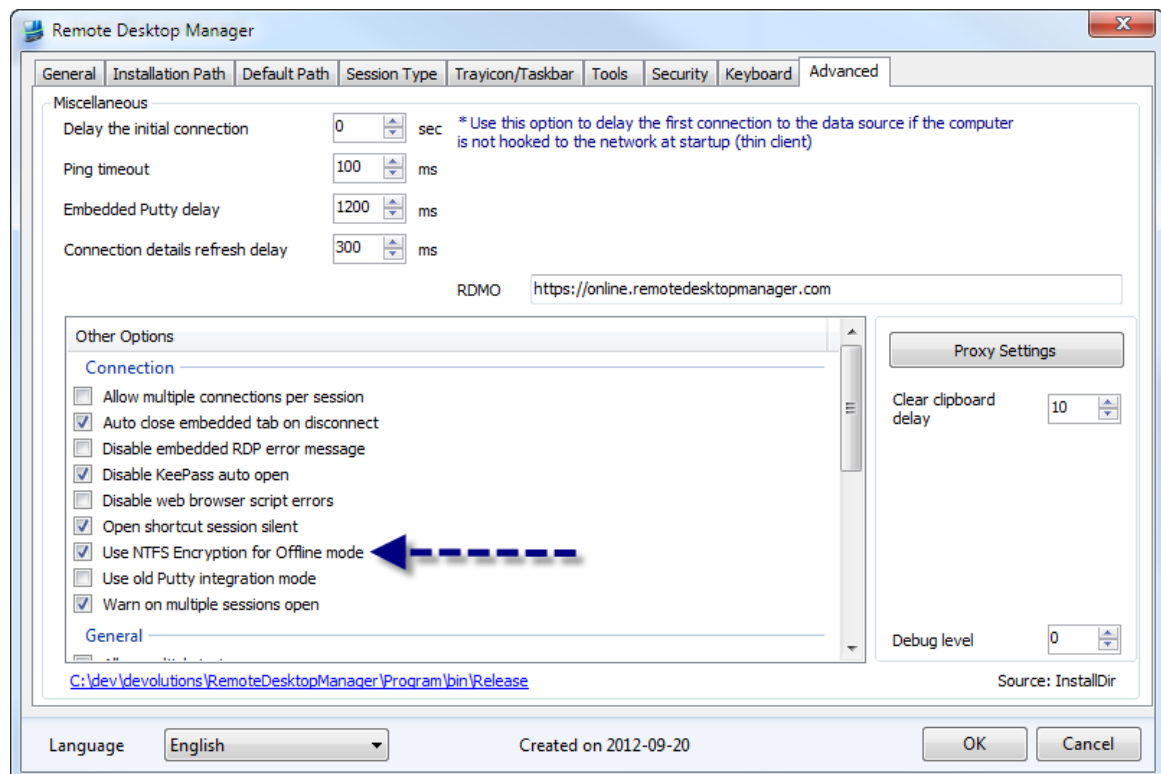
Custom images need to be stored in the data source, this results in the size of the configuration becoming problematic if there are too many entries using them. If that becomes the case it would be better to revert to built-in images.

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 Offline mode ([Data Source Settings](#) or [Overview](#)), 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 on a domain which has been hardened by the network administrator. You can turn off usage of NTFS encryption in the application options



Advanced application options

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.

8.9.8 Profiler

Description

Remote Desktop Manager has a built-in profiler to diagnose connectivity issues with a data source.



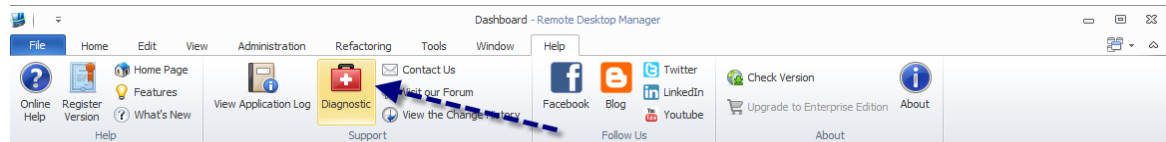
Displaying the profiler window might slow down the operations on the data source. Proceed with care.



To diagnose startup issues, you can enable the profiler from the command line as described in [Command Line Arguments](#)

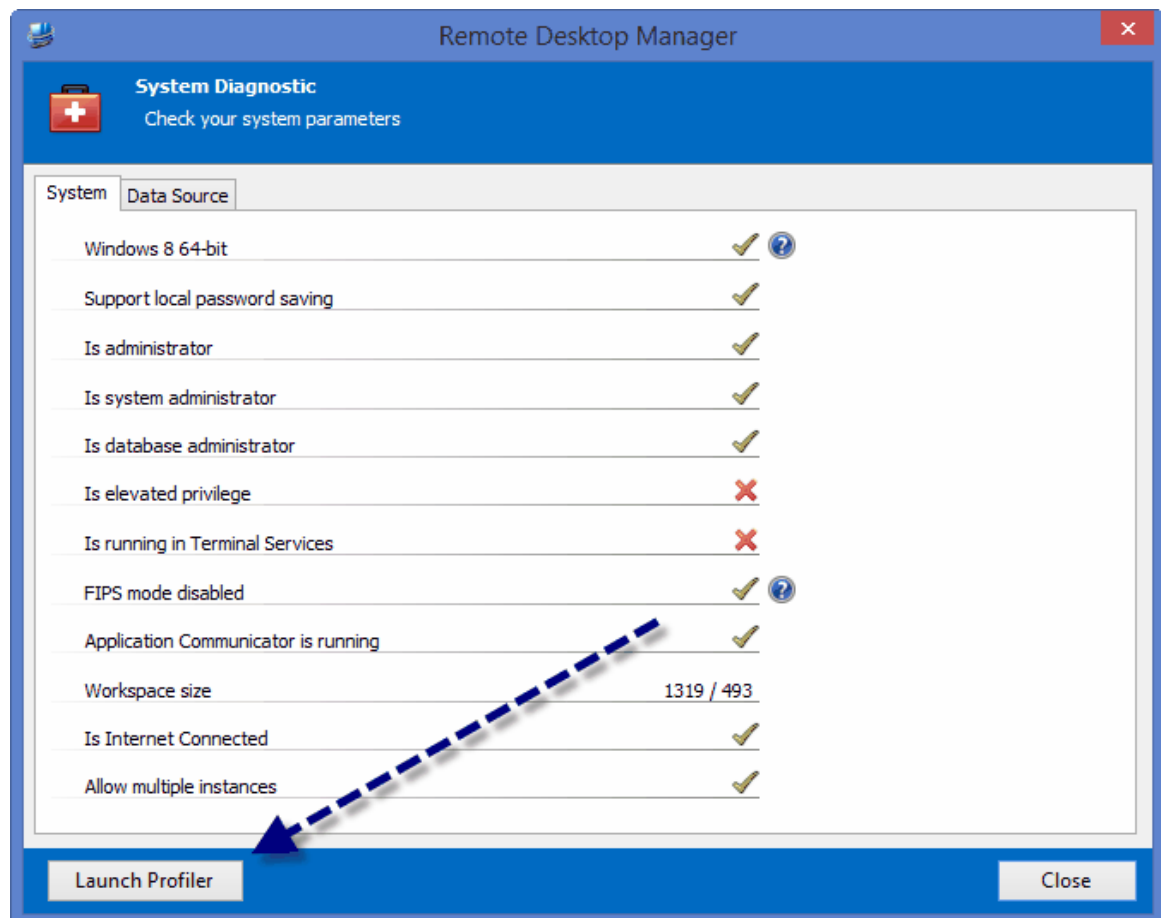
Procedure

1. Select **Help -> Diagnostic**




Diagnostic button

2. Click on **Launch Profiler**



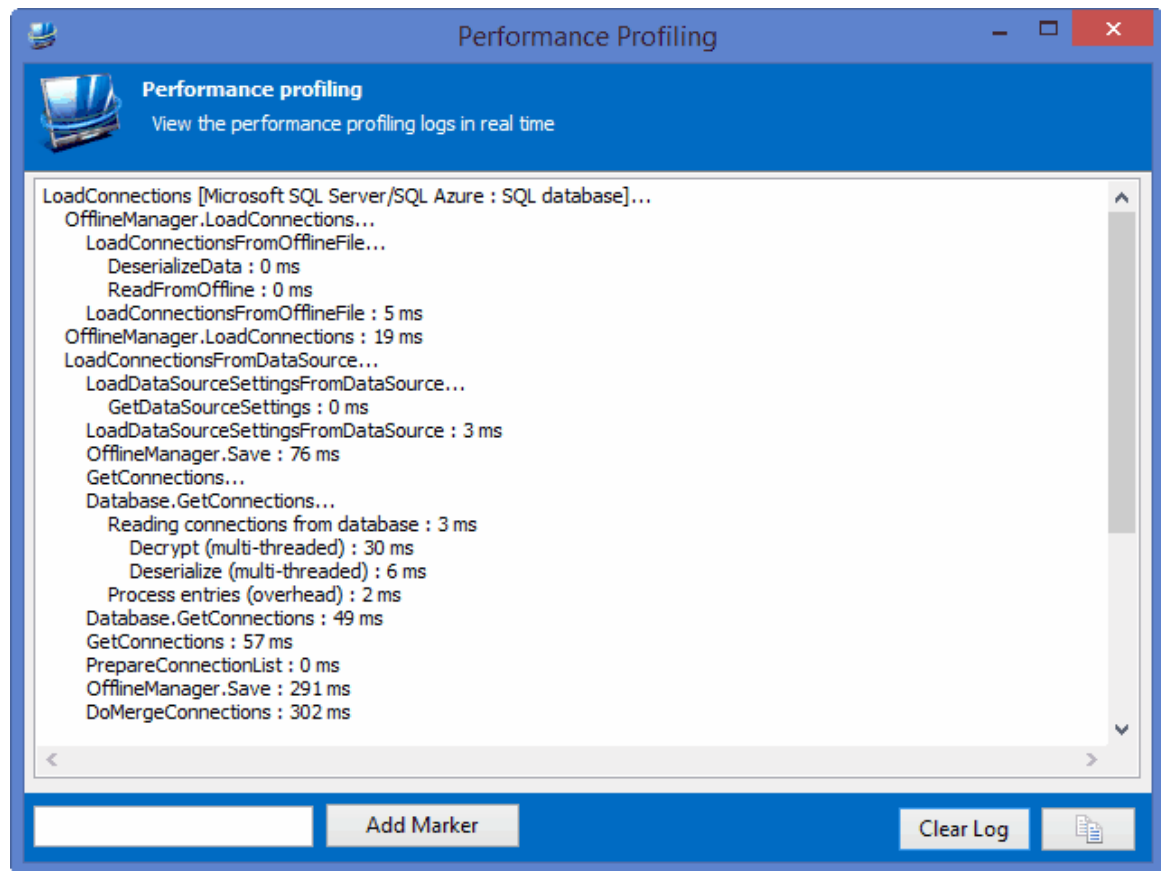
Launch Profiler

3. Move the window to the side in order to display the Remote Desktop Manager main window.

4. Refresh the data source by using the refresh button  or by using **File -> Refresh**. The Profiler data will appear in the Profiler window.

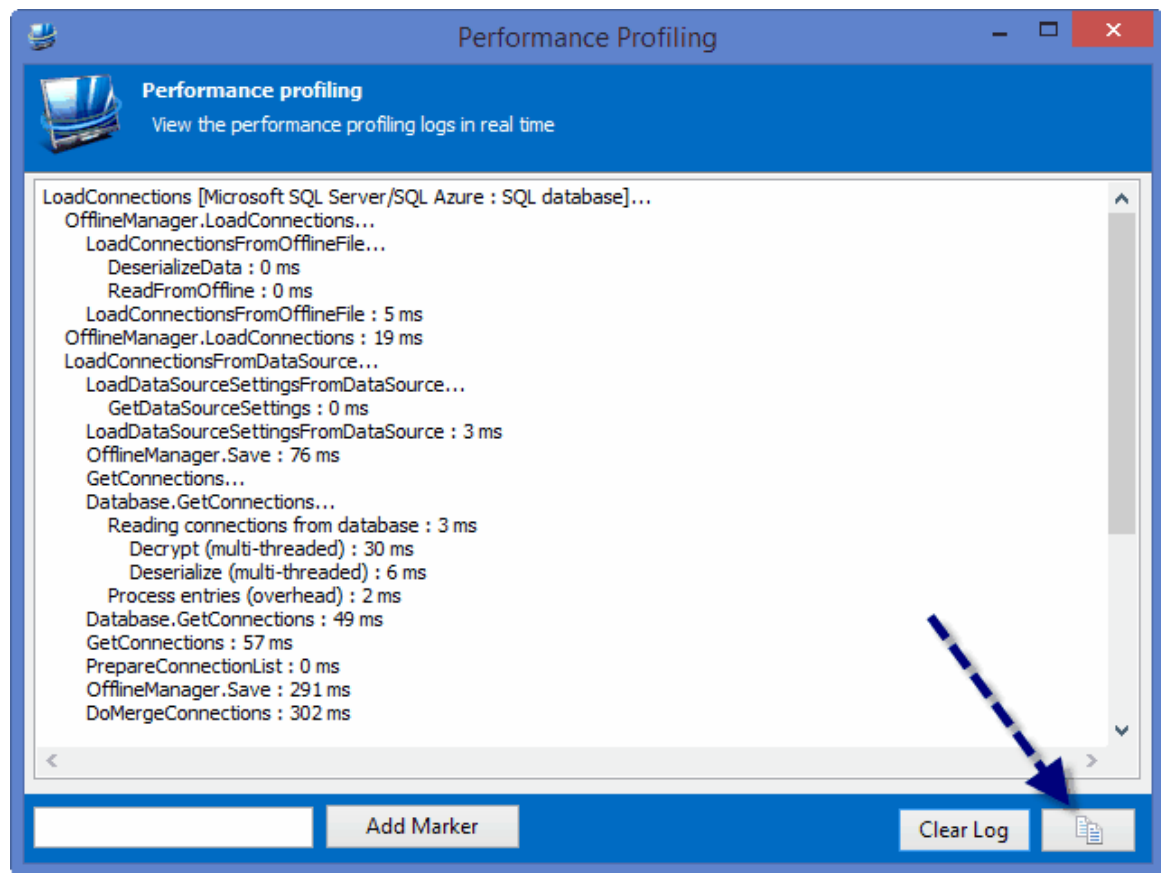


Holding the **CTRL** key while performing the refresh will force a full reload of the data source, thereby ignoring the cache.



Performance Profiling

5. Click on  to copy the Profiler data logs into your clipboard.




Copy to clipboard

6. Send the Profiler data logs to your support technician, or at the support email address relevant to your support contract.

8.9.9 Putty

Errors

Putty in embedded mode does not work when using Team Viewer .

Remote Desktop Manager is not able to execute Putty in embedded mode when 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 *Extra -> Options -> Advanced -> Show advanced options -> QuickConnect button -> Configure -> Show Quick Connect button* option.

8.9.10 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

8.9.11 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 those situations where SSH v1 is required.

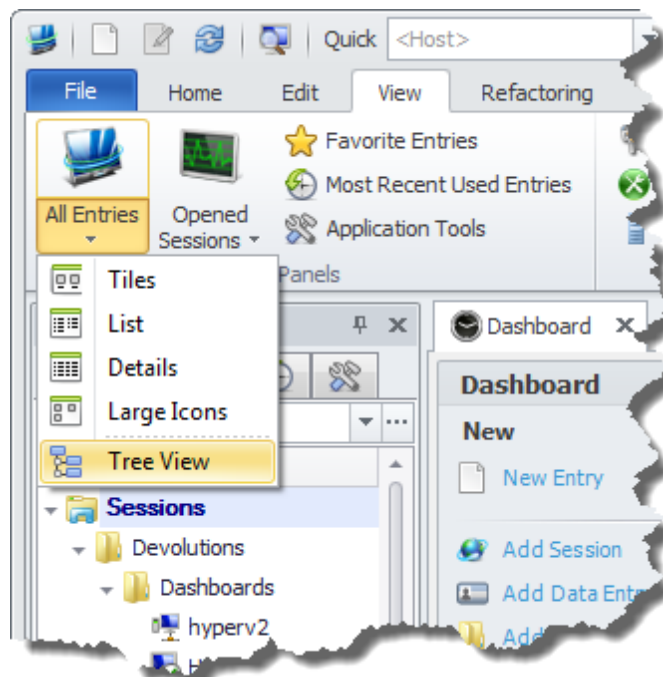
8.9.12 User Interface

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

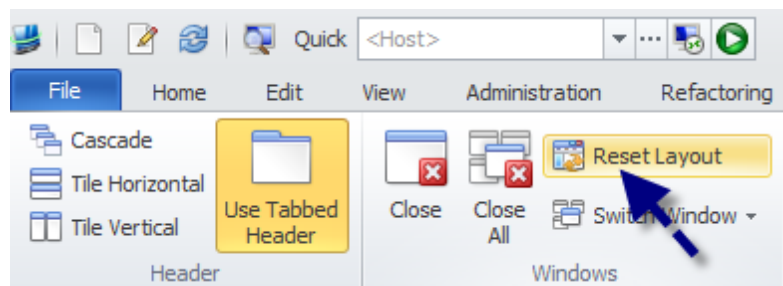
The navigation pane can be displayed in many modes. You can select the tree view with **View -> All Entries -> Tree View** or use the default shortcut **F7**



View -> All Entries menu

The main form layout is broken

Use the Reset Layout to apply the default layout from the **Window** menu:

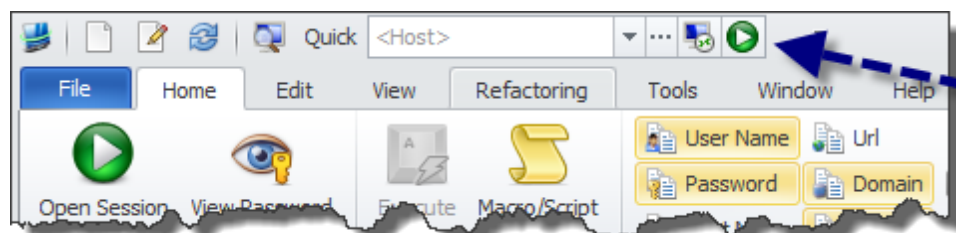


Reset Layout button



The reset layout might not resolve all the issues. Close the application and delete the layout files (*.lyt) in %LocalAppData%\Devolutions\RemoteDesktopManager to completely restore the layout.

The quick access toolbar needs to be reset

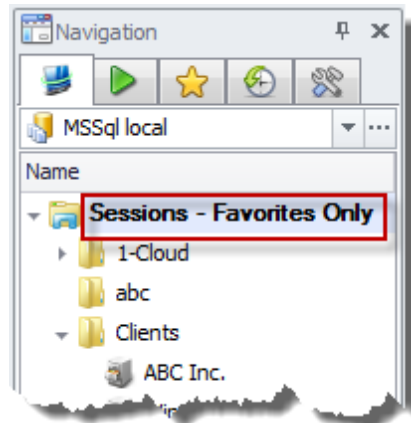


Quick Access Toolbar

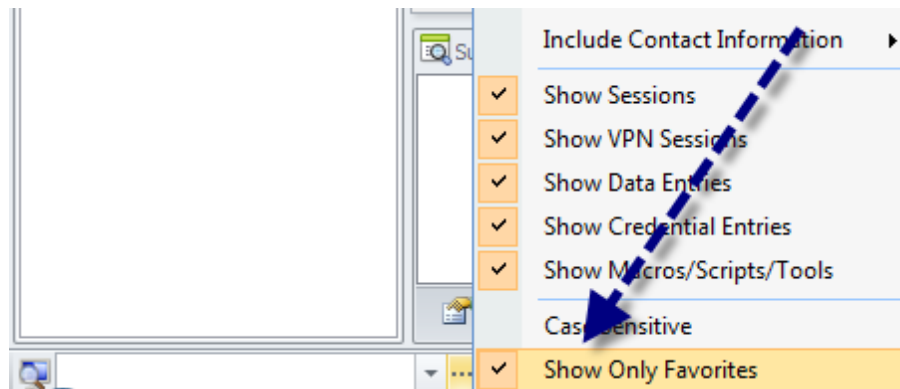
To reset the quick access toolbar, close the application and delete the file **remotedesktopmanager.qtb** in **%LocalAppData%\Devolutions\RemoteDesktopManager**

The navigation pane displays only my favorites

Only your favorites are displayed even though you are in the **"All Entries"** tab, the root node is also entitled **"Sessions - Favorites Only"**



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.



8.9.13 VPN

Errors

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.

8.9.14 Web Browsers

Errors

“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:

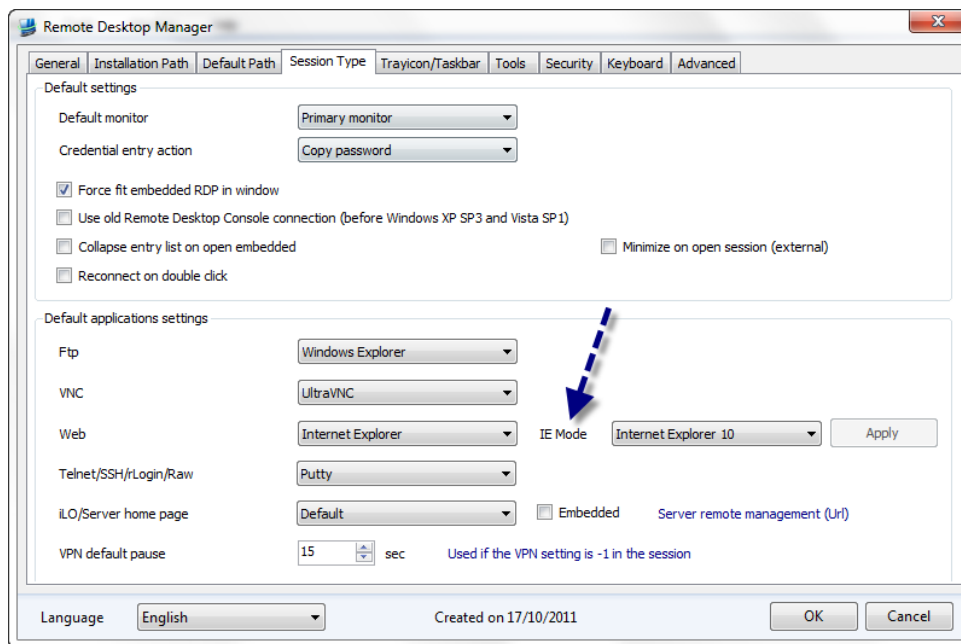
```
[HKEY_CURRENT_USER\Control Panel\Desktop]
"ForegroundLockTimeout"=dword:00000000
```

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.

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 the application options: **File->Options -> (Session Type)**



8.9.15 WMI

Access Denied Errors

Ensure the user account has the permissions necessary to access a computer remotely. [Securing a Remote WMI Connection \(Windows\)](#)

You can also find troubleshoot tips in [WMI Troubleshooting \(Windows\)](#).