Overcoming Remote Desktop Challenges with

Remote Desktop Manager

Petri IT Knowledgebase
A BWW Media Group Brand

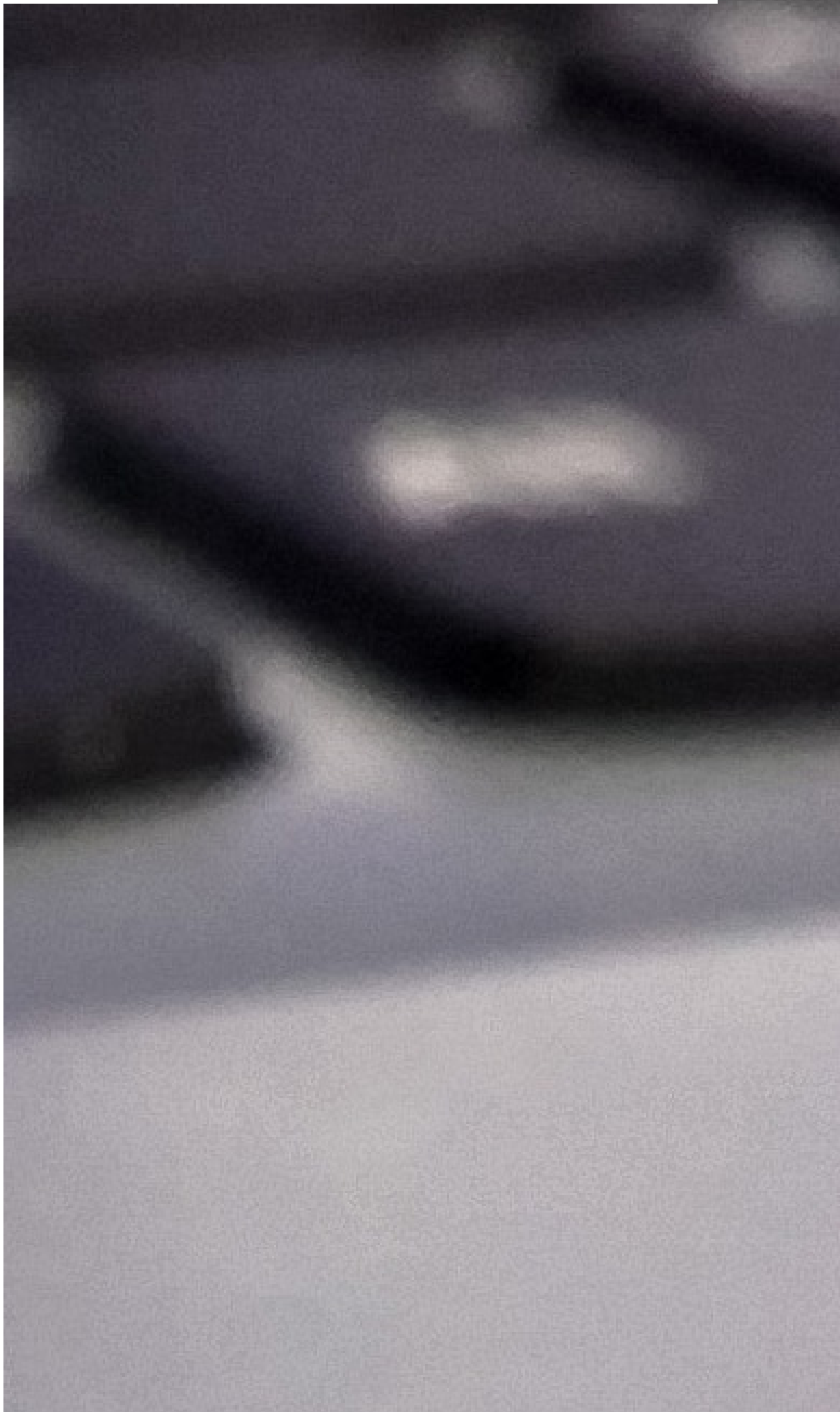
SPONSORED BY
Devolutions

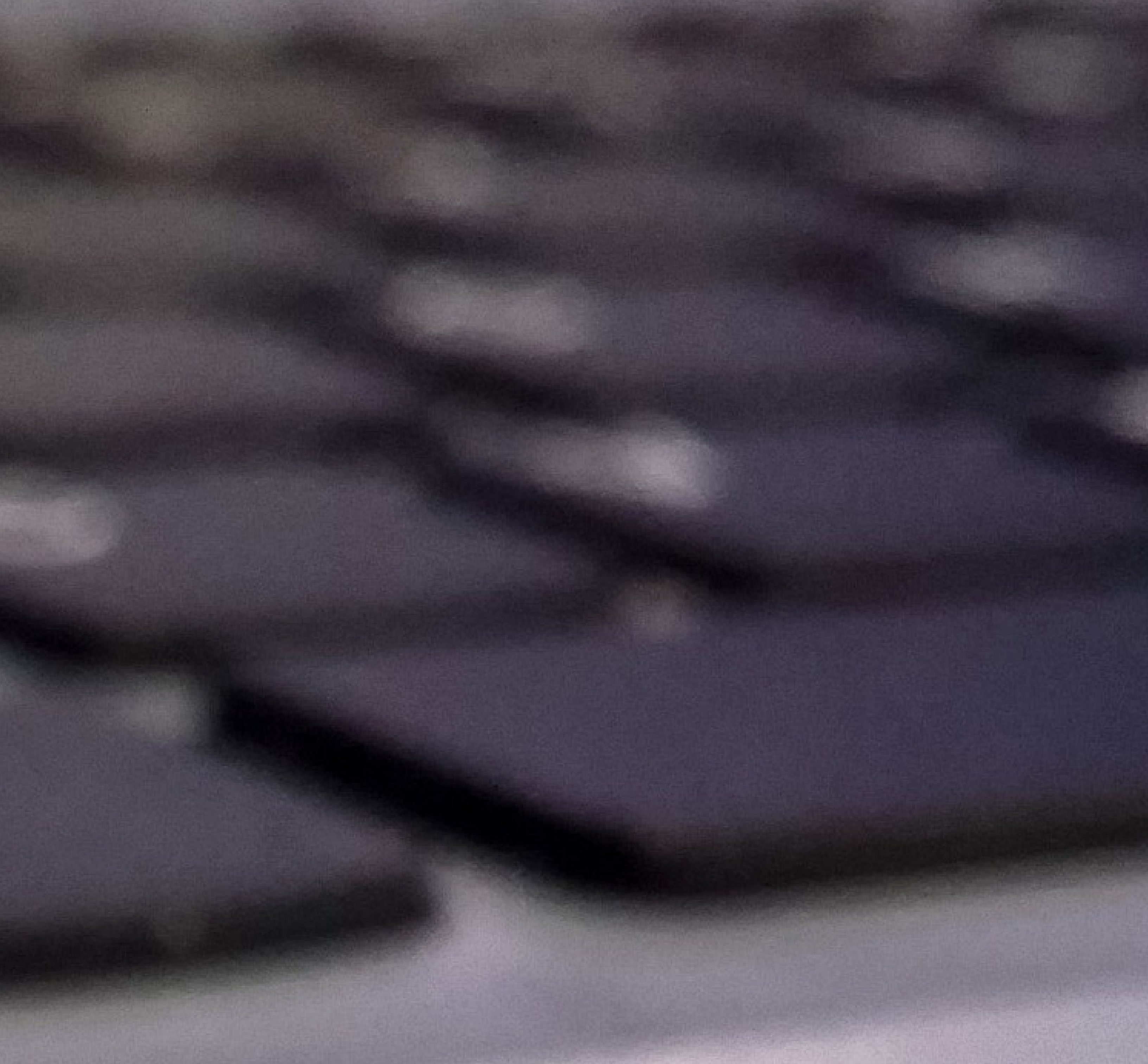
By

Michael Otey

Michael Otey is president of TECA, Inc., which focuses on Windows and SQL Server product development and consulting. He is a frequent contributor to technical publications and the author of several books on database development and programming.

In today's corporate environment IT administrators typically need to manage many different remote systems. These systems can be physical systems or they might be VMs. Many times, these systems reside locally as well as in remote locations and in the cloud. For Windows IT administrators the Remote Desktop is the primary tool that the vast majority of IT administrators use every day for these necessary remote management tasks. Remote Desktop enables you to start an interactive session with a remote system that has been configured to allow Remote Desktop access. Remote Desktop opens a window on your local system that contains the desktop of the remote system that you connect to. Your mouse and keyboard actions are sent to the remote system and the interactive session allows you to operate and troubleshoot the remote system very much like you are sitting at a local display. This kind of control and interactive display is essential when you're trying to troubleshoot problems or configure systems remotely.





In this whitepaper you'll learn about some of the challenges of using Remote Desktop to manage your enterprise servers and then see some of the best ways that you can address these issues. Many companies use Microsoft's Remote Desktop Connection Manager for their remote Windows management requirements. However, Remote Desktop Connection Manager has several critical limitations in an enterprise desktop environment. You'll see how you can address these limitations as well as how **Devolutions Remote Desktop Manager** provides an enterprise-ready feature set to address your remote management requirements.

Remote Desktop Management Challenges

While managing remote desktops is an essential daily task for most IT administrators it also presents some difficult challenges. Let’s take a closer look at the some of the three main remote desktop management challenges.

- **Managing multiple connections** - One of the biggest challenges with Remote Desktop is managing and organizing multiple remote connections. Most administrators in medium and larger companies need to connect to dozens if not hundreds of remote systems which can be very difficult to manage. Using RDP files enables you to save your connection settings and optionally your authentication information. This works great for a few systems but it quickly gets very messy and potentially confusing when the number of remote connections grow into dozens or more. Attempting to manually manage connections can result in a lack of standardization, confusion and potential errors.

- **Securing your remote connections** – The next biggest remote desktop management challenge is properly securing the remote connections. Just like a traditional desktop environment, passwords are your first line of defense in securing your corporate infrastructure. All accounts with access to Remote Desktop Connections need to require strong passwords. To simplify management, some companies attempt to use the same passwords for multiple accounts – or worse resort to yellow sticky notes -- which can create a huge security exposure. You need to ensure that your remote management network connections, passwords, and credentials are all secure. In addition, when you’re dealing with multiple remote systems and access by many different IT personal you need a way of logging access to those systems for auditing and troubleshooting.

- **Connecting to Linux and other heterogeneous hosts** - One of the other challenges with remote desktop management is connecting to heterogeneous host systems. Today very few companies only have Windows systems to manage. Instead, most business are using a mix of Windows, Linux, Mac and other non-Windows systems. For most Windows administrators this means they need to use multiple remote management tools. Remote Desktop is limited to the RDP protocol which for the most part restricts its use to Windows systems. While some Linux distributions can be managed with RDP most cannot. This often requires that the administrator has to incorporate multiple tools like VNC, Putty and Apple Remote Desktop in addition to Windows Remote Desktop.

There are several different paths that you can take to clear these hurdles in remote desktop management. You can try to manually organization multiple .rdp files into separate folders with different permission but this can be extremely cumbersome and difficult for large numbers of connections. Instead, many businesses opt to use Microsoft’s Remote Desktop Connection Manager or a third party remote desktop manger like Devolutions Remote Desktop Manager to more effectively manage their remote desktop connections. Let’s take a closer look at using Microsoft’s Remote Desktop Connection Manager and Devolutions Remote Desktop Manager to handle your remote connection requirements.

Microsoft Remote Desktop Connection Manager

One tool that many IT administrators use to help manage their remote desktop management needs is Microsoft's Remote Desktop Connection Manager. Microsoft's Remote Desktop Connection Manager (RDCMan) is a free download and it can help you to manage multiple remote desktop connections by centralizing all of your remote desktop connections under a single management console. RDCMan is supported on Windows 10 Tech Preview (Windows 10), Windows 7, Windows 8, Windows 8.1, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server Tech Preview (Windows Server 2016). RDCMan is a basic tool whose main purpose is to help you to organize remote connections under a single console. You can see an example of Microsoft's Remote Desktop Connection Manager in Figure 1.

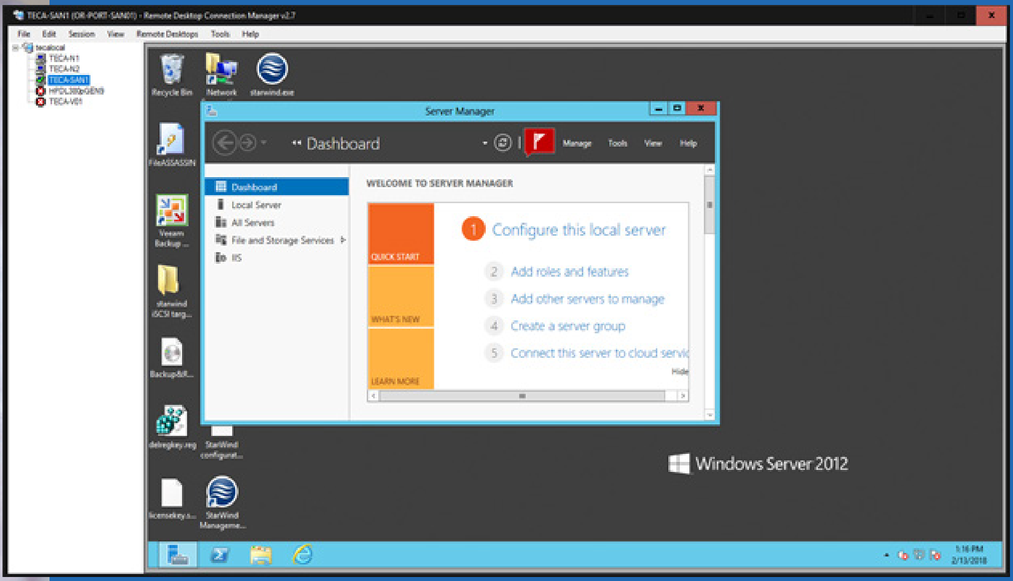


Figure 1 – Microsoft Remote Desktop Connection Manager

As you can see in Figure 1 RDCMan allows you to create groups of different remote systems that you can connect to. Each group is stored in a separate .rdg file which can be exported and shared by other users. It's important to realize that these are all separate files which can make implementing batch changes and sharing them with multiple users very cumbersome. RDCMan also offers the ability to encrypt your stored credentials using certificates. Remote connections have the ability to inherit settings from the group they are part of or you can customize each remote session. By default, the remote display is rendered in the main frame of the RCDMan console but you also have the option of undocking the remote session. RCDMan is primarily a Windows management tool. It can use RDP to connect to remote Windows sessions and it can also connect to Hyper-V VM console sessions using VMConnect.

RDCMan is adequate for a managing a small number of systems. Unfortunately, it has a number of significant limitations when used in a medium, large business and enterprise scenarios. Some of the main limitations for RCDMan include:

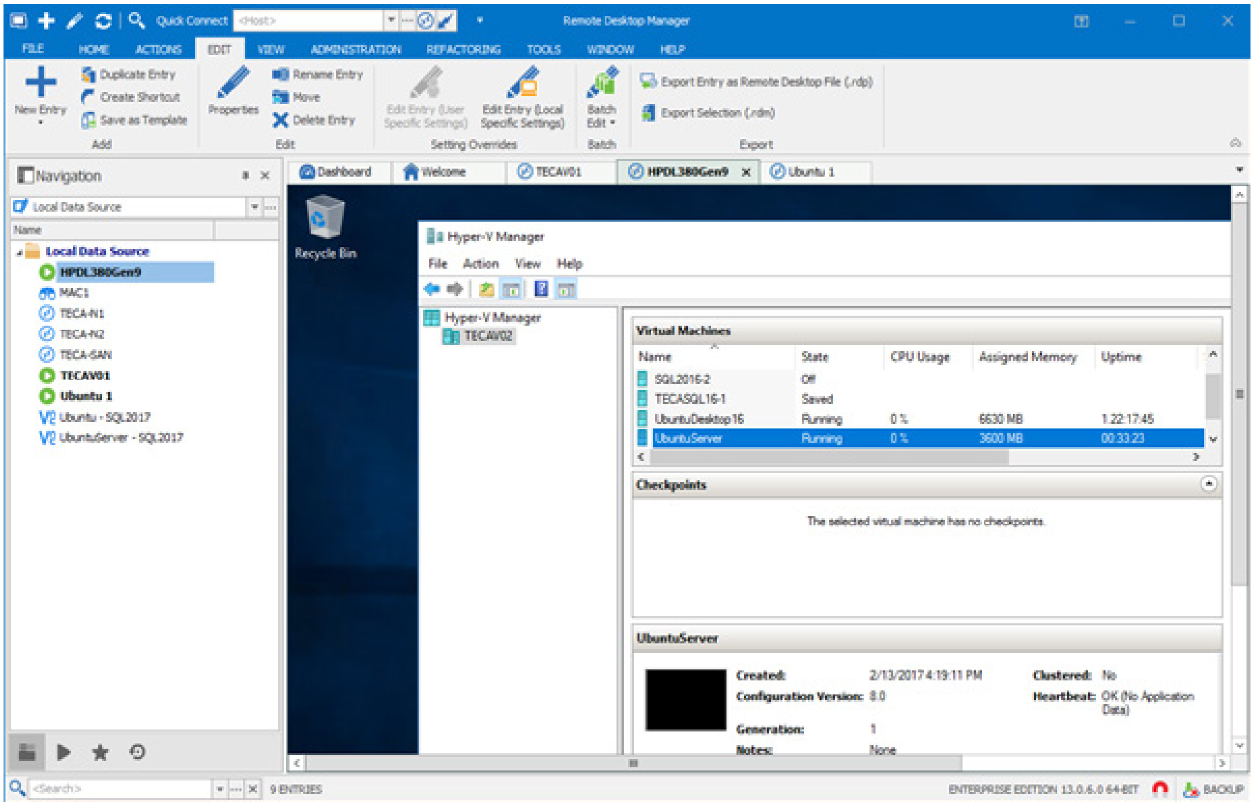
- No support for Linux and Mac desktops - RDC is primarily designed to be a Windows-only management tool and it doesn't support the full range of heterogenous servers that are in most businesses today.
- It is not officially supported by Microsoft – One important thing than many administrators don't realize is that RDCMan is not an official Microsoft product and it is not supported by Microsoft nor is it kept current. The last update for RDCMan was in 2014.
- Manual credential entry – RDCMan requires you to manually enter the credential data for your remote sessions. This can be time consuming and can result in errors.
- Remote Desktop only – RDCMan does not provide any other additional networking tools or capabilities.

Devolutions Remote Desktop Manager

Most businesses have remote desktop management needs that go beyond the basic capabilities provided by Microsoft's free offering. Devolutions Remote Desktop Manager (RDM) provides the ability to manage multiple remote desktop connections. In addition, RDM offers a far more extensive set of tools and enterprise-level management capabilities then Microsoft's RDCMan. Let's take a closer look at some of the main remote management capabilities and tools offered by RDM.

First, RDM is supported on almost all of today's popular Windows desktop and server platforms including: Windows Vista SP2, Windows 7 SP1, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 SP2, Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016. The latest version also requires the Microsoft .NET Framework 4.6. There are both 32-bit and 64-bit versions of RDM.

RDM provides a modern interface that makes use of a ribbon menu and a tabbed interface for each open remote session. You can see Devolutions Remote Desktop Manager in Figure 2.



Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime
SQL2016-2	Off			
TECASQL16-1	Saved			
UbuntuDesktop16	Running	0 %	6630 MB	1.22:17:45
UbuntuServer	Running	0 %	3600 MB	00:33:23

The selected virtual machine has no checkpoints.

UbuntuServer

Created: 2/13/2017 4:19:11 PM
Configuration Version: 8.0
Generation: 1
Notes: None
Clustered: No
Heartbeat: OK (No Application Data)

Figure 2 – Devolutions Remote Desktop Manager

for each remote location or business unit that you manage. RDM provides granular control over each connection, each group of connections, or each data source. By default, all of the open sessions appear in their own tabs in the Context Area. You can work with each data source and session by right clicking on it in the Navigation pane. If you are using the tabbed display you can quickly switch between sessions by clicking the desired tab. RDM gives you the option of making your connections appear in tabbed interface or enabling them to be undocked like a standard Remote Desktop connection. For multiple monitor support RDM enables you to create a container window that is separate from the main window and you can drag and drop open tabs onto the container window.

Group Management

Almost all medium businesses up through the enterprise have multiple people using remote desktop connections and these users are often separated into different locations or application management teams. To facilitate team access RDM's session connection information can be stored in a number of different types of shared data sources. These data sources and their sessions can be shared by multiple team members. RDM supports the following shared data sources:

- **Amazon S3** - Can be shared in read-only mode. Basic support.
- **Devolutions Online Database** - Basic support for micro teams (up to 3 users), Professional and Enterprise editions support larger teams.
- **Devolutions Server** – Shared. Supports all features, such as attachments, connection log, Offline Mode and Security Management.
- **Dropbox** - Can be shared in read-only mode.
- **FTP** – Uses an XML file that can be shared in read-only mode.
- **Google Drive** -- Shared. Supports all features, such as attachments, connection log, Offline Mode and Security Management.
- **MariaDB** -- Shared. Supports all features, such as attachments, connection log, Offline Mode and Security Management.
- **Microsoft Access** – Shared but not recommended as Microsoft doesn't support it in the newest versions on Windows.
- **Microsoft SQL Azure** -- Shared. Supports all features, such as attachments, connection log, Offline Mode and Security Management.
- **Microsoft SQL Server** – The recommended data source for multiple users. Shared. Supports all features, such as attachments, connection log, Offline Mode and Security Management.
- **MySQL** -- Shared. Supports all features, such as attachments, connection log, Offline Mode and Security Management
- **SFTP** – Can be shared in read-only mode. Basic support.
- **SQLLite** -- Shared. Supports all features, such as attachments, connection log, Offline Mode and Security Management
- **WebDav** -- Can be shared in read-only mode. Basic support.

Data sources that are stored in the cloud are typically automatically backed up by the cloud provider. To protect sensitive data in your data sources you can lock the data source configuration before you deploy it. The offline mode allows you to connect to a local 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. RDM's batch edit feature enables you to easily change the settings of multiple sessions in one operation. For instance, many companies have a 90-day password change cycle which can become a problem when you need to regularly change my passwords for multiple connections. RDM also allows you to associate keywords/tags for your entries facilitating easier searches for related entries.

Multiple Remote Host and Connection Types

Today's IT infrastructures are typically anything but homogenous. In addition to managing Windows Servers most businesses also need to manage Linux servers and sometimes Mac systems as well. Plus, administrators often need to connect directly to Hyper-V or VMware VMs as well as use other services like FTP or VPNs. Microsoft's RDCMan is essentially limited to RDP and cannot connect to a good portion of the systems that today's IT administrators need to manage. The remote connectivity capabilities provided by Devolutions RDM address the full range of connectivity required by today's businesses. In addition to Windows and RDP, RDM support multiple remote protocols like VNC for Linux connectivity, Apple Remote Desktop, Citrix ICA as, Hyper-V and VMware VMs as well as other remote control/management products like HP Integrated Lights Out (iLO) and LogMeIn. RDM enables you to consolidate your remote management using a single tool to connect to Windows, Linux and other heterogeneous remote systems. You can see the variety of RDM's support remote connections in Figure 3.

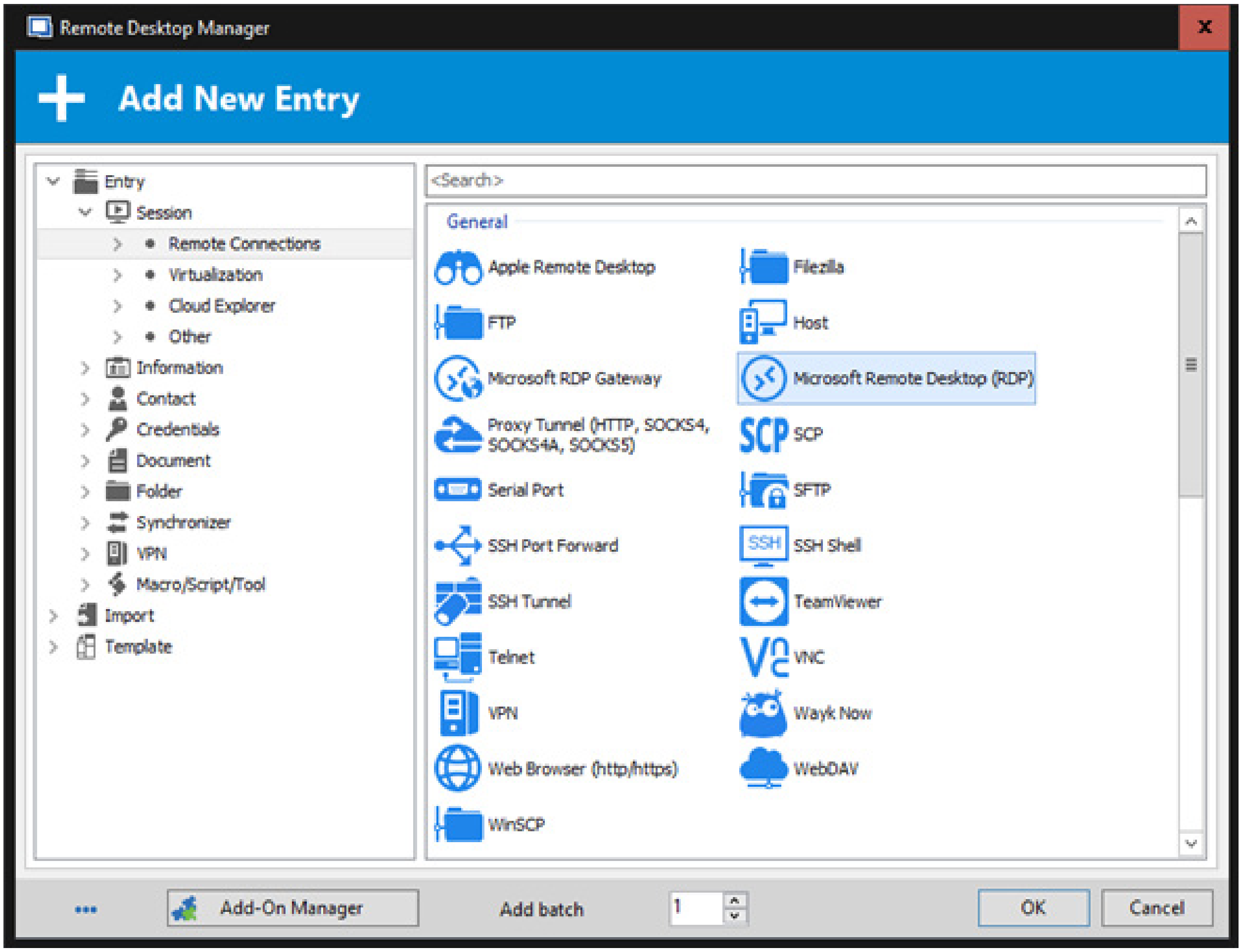


Figure 3 – Remote Desktop Manager’s supported remote connection

To create a new remote session select the desired session type and then RDM will prompt you for that sessions specific configuration properties. As you can see in Figure 3, RDM’s wide array of supported remote sessions enables you address the full range of remote management needs for the enterprise. Some of the most commonly needed remote session types the RDM supports include:

- Microsoft Remote Desktop (RDP) – For connections to Windows systems
- VNC – For connections to Linux systems
- Apple Remote Desktop – For connections to Apple systems
- Telnet – For connections to various Windows and Linux Telnet hosts
- FTP, SFTP, SCP & WinSCP – For connections to FTP hosts

Enterprise-level Security

Properly securing your remote desktop connections is essential because of the far-reaching access and administrative capabilities that they provide. RDM provides a number of enterprise-level security features that can enable you secure access to your remote sessions. Passwords are the first level of all security strategies and RDM provides a number of capabilities that can help you to manage remote session passwords. RDM provides centralized remote password management as well as password generation and enforcement of password policies. Centralizing all passwords and enterprise data in one secure location both helps administrators quickly access the information they need as well as enabling it to be kept in one secure location. RDM is able to enforce all of the essential password policies for remote sessions including:

- Password history - Determines when an old password can be reused
- Password age – Determines when a user must change their password
- Minimum password length - Determines the minimum number of characters required for a password
- Complexity requirements – Ensures that the password can’t contain the user name and that it must use at least three of the four possible character types: lowercase letters, uppercase letters, numbers, and symbols.

Another important security features that RDM provides is the built-in password analyzer. When you supply passwords for your remote sessions RDM's password analyzer will automatically evaluate the passwords and notify you if they are strong or weak. RDM is also able to automatically generate strong secure passwords. Enabling the Password Audit policy allows you to track all password changes

To handle the remote access security for users with different job responsibilities and remote access requirements RDM provides a role-based security system that enables flexible granular protection. For instance, you might want to create different roles and security settings for your administrators, help desk personal or consultants. RDM's role-based security enables security settings to be inherited. Child items and folders are automatically covered by a parent folder's security settings. The specific permissions for a given item can be overridden. You can set permissions on a sub folder or item to override the parent item's permissions.

RDM also provides several other important remote access security features. First, it has a check-in and check-out feature that enables an administrator to lock down access for a remote session. For instance, if you were performing a long lasting maintenance routine and you didn't want to allow any other access to the system you could check out the session and other users couldn't access it until it is checked back in. You can also restrict access to remote sessions based on time. For instance, you might only allow access to some remote sessions during business hours. RDM also supports two-factor authentication provides unambiguous identification. This feature is only available for the following data sources: SQLite, Online Database, Devolutions Server, MariaDB, Microsoft Access, SQL Azure, SQL Server and MySQL.

Logs are another important security feature that RDM provides. RDM logs the usage for all of your different remote sessions and actions. The logs record when sessions are opened and closed along with the duration of the session. They also record when entries are viewed or changed as well as who performed the action.

Remote Management Tools

Effective remote management requires more than just an interactive login to the remote system. In many cases you need to troubleshoot the network connectivity, check the configuration of a remote server or perform a variety of other management and troubleshooting tasks. In addition to remote desktop management, RDM provides a number of handy network management tools that you can use to manage your remote systems. You can see the collection of remote system management tools provided by RDM in Figure 4.

Effective remote management requires more than just an interactive login to the remote system. In many cases you need to troubleshoot the network connectivity, check the configuration of a remote server or perform a variety of other management and troubleshooting tasks. In addition to remote desktop management, RDM provides a number of handy network management tools that you can use to manage your remote systems. You can see the collection of remote system management tools provided by RDM in Figure 4.

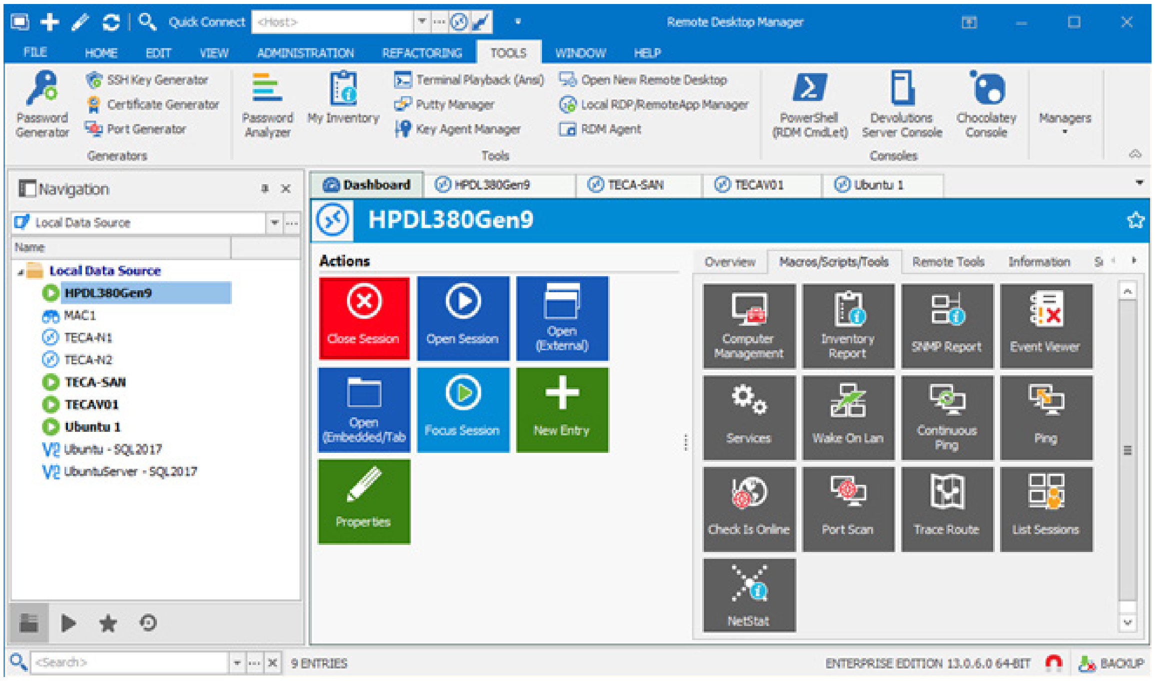


Figure 4- Remote Desktop Manager's remote management toolset

PowerShell Scripting

RDM also supports Windows PowerShell scripting which enables administrators to automate RDM management. RDM supplies a PowerShell Module called RemoteDesktopManager.PowerShellModule.dll which is located in the Remote Desktop Manager installation directory. You can use the Import-Module cmdlet to load the module into your PowerShell sessions. The RDM PowerShell module can be used to automate a wide variety of tasks including:

- Connecting to data sources
- Creating databases
- Loading configurations files
- Assigning credentials to entries
- Retrieving session properties
- Changing group folder and session properties
- Setting customer roles
- Importing and exporting CSVs

Enabling Enterprise-Level Remote Desktop Management

Remote desktop management is one of the most important tools used by today's IT administrators. RDM from Devolutions goes far beyond the basic Windows connectivity offered by Microsoft's RDCMan. RDM brings enterprise grade features like connectivity to all the popular server platforms, group management, security and scripting to remote management. RDM lets you centralize all your remote connections, credentials and tools into a single remote management platform that can be securely shared by your administrators and other remote desktop users.

SPONSORED BY

Devolutions