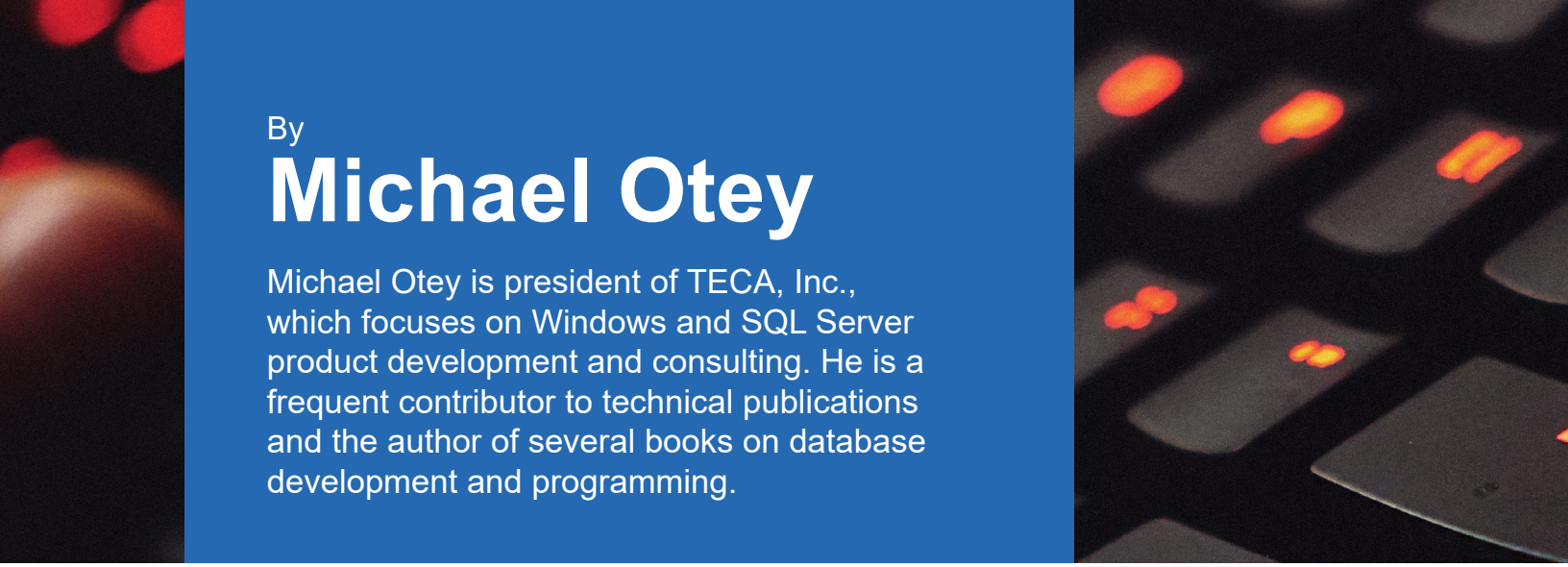
Remote Desktop Security & Password Management

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.

Remote administration is one of the core activities for IT administrators today and Remote Desktop is the administrator's go to tool. Remote Desktop enables you to start an interactive session with a remote system and to control that system just as if it were your local system. Remote Desktop connections are essential for efficient remote management and troubleshooting. While Remote Desktop is an essential tool, it's vital to remember that it is also a very powerful application that that needs to be secured.

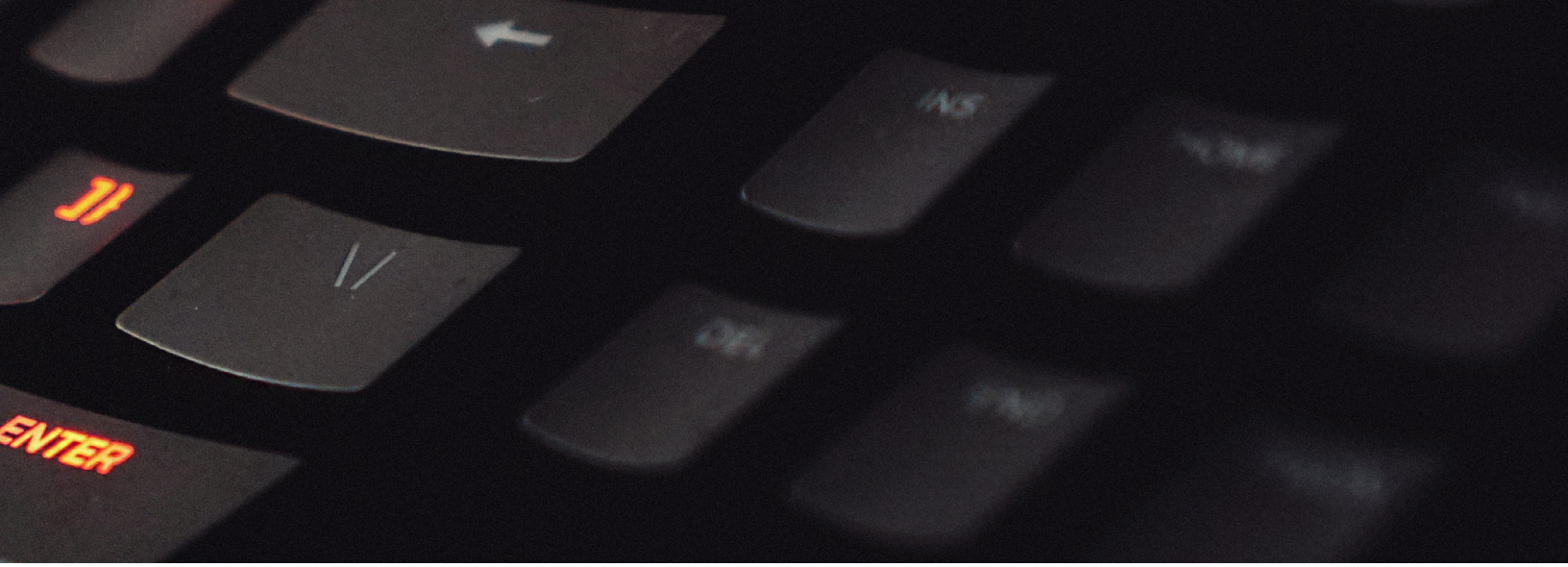
Remote Desktop connections often have elevated privileges because they need to perform different administrative tasks. This means that is absolutely essential that your Remote Desktop administration platform is secured. In addition, both administrators and users frequently use various web browsers for a variety of daily tasks and many web sites require credentials that need to be secured as well.

In this whitepaper you'll learn about some of the challenges in password management for remote administration then you'll see how you can use Devolution's **Remote Desktop Manager (RDM)** to centrally and securely manage your remote passwords for both privileged administrative users and business users with the same platform.

Challenges in Password Management

Managing passwords is a difficult security challenge for all IT departments and organizations worldwide. Properly securing your passwords – especially administrative passwords – is vital for enterprise security. Passwords are your first line of defense for keeping your company's assets secure as well as enabling your users to be productive. Exposed passwords can result in data breaches, external hacks, insider threats and even exposing your critical business data and processes to malware and ransomware attacks. Some of the main challenges to password management include:

- Keeping employee passwords confidential – The first challenge with password management is making sure they are actually a secret. Users have been known to be quite lax with the security of passwords. They have been known to share their passwords, use yellow sticky notes to post them on their monitors and use very weak passwords such as "password".
- Sharing privileged accounts – Users aren't alone in creating password security risks. Administrators have also been known to share privileged administrative accounts for convenience. This can make some administrative tasks easier but it also eliminates the ability to log and audit changes.



- Reusing common account names and passwords – Another security challenge is preventing users from reusing common user account names and passwords. If you visit a lot of different websites or have a large number of remote systems it can be tempting to reuse the same login information. However, that practice is not secure and if one of the sites becomes compromised then any other site that shares that authentication information could potentially be compromised as well.
- Not changing default passwords – Another potential problem is neglecting to change the default passwords that are supplied with some applications and devices. These default passwords are typically not very strong and they are usually well-known. Overlooking changing these default password can introduce a potential security exposure.
- Social engineering password attacks – Another challenge for password management is social media and email phishing attacks that are designed to trick users into providing login information that can be used to gain access to your company's resources.
- Protection against password cracking – Another challenge is to prevent passwords from being stolen by password cracking programs. Passwords are typically stored in a cryptographic hash on the systems that you access. If the attacker can gain access to the hash file, for instance by getting a copy of a VM's VHD files they could use a variety of different password cracking programs to attempt to extract your organization's security information. Storing passwords in secured locations, using strong passwords and keeping separate passwords for different systems can help mitigate this threat.
- Lack of auditability for privileged accounts – The ability to be able to log and track the actions of your administrators can be especially important for auditing remote access and being able to identify the person responsible for a given set of changes.
- Lack of centralized management – Without centralized password management important passwords can be distributed in many places across your organization -- weakening network security and increasing management and support efforts. Centralized password management reduces the points of password exposure and provides a more easily managed central repository for your remote credentials.

Properly securing your remote connections is essential because they can potentially expose your business to security breaches. Devolutions RDM provides a number of core enterprise-level security features that can enable you to centrally secure and manage access to all the different remote servers in your organization.

Remote Desktop Manager's Secure Password Management

Passwords provide the foundation your remote security strategies and RDM provides several core capabilities that enable you to better control and secure the passwords used by RDM users. RDM provides support for password policies, password generation and enforcement as well as centralized remote password management.

RDM Password Policies

Strong password policies are your first line of defense against security breaches. While most users and administrators realize strong passwords are important it's easy to become lax or frustrated by them when you have lots of different remote sites to work with. Centrally managed password policies can prevent users from implementing weak passwords. RDM supports all of the essential password policies required to enforce strong passwords including:

- **Minimum password length** – Requires a minimum number of characters in 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
- **Password history** – Prevents old password from being reused for a specified period
- **Password age** – Requires that a user must change their password in a specified time period

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. It is recommended that you implement a password age policy that requires users to change their passwords every 90 days for a strong password and every 180 days for a passphrase. In addition, RDM enables you to create a list of forbidden passwords which can stop users from attempting to create easily guessable passwords like 'password'.

Password Generator

Creating strong password can be a frustrating task for some users. To make this task easier and more secure RDM provides a Password Generator that's integrated with each session entry. RDM's Password Generator is able to create complex random passwords that are highly secure. You can create the passwords using the default password creation template or you can make your own custom password generation templates. You can see RDMs Password Generator in Figure 1.The bottom portion of the window shows the list of generated passwords. Each generated password can potentially have a different level of strength ranging from Very Strong to Perfect. Clicking on a password and then clicking on the Select button will insert the generated password into your remote session entry.

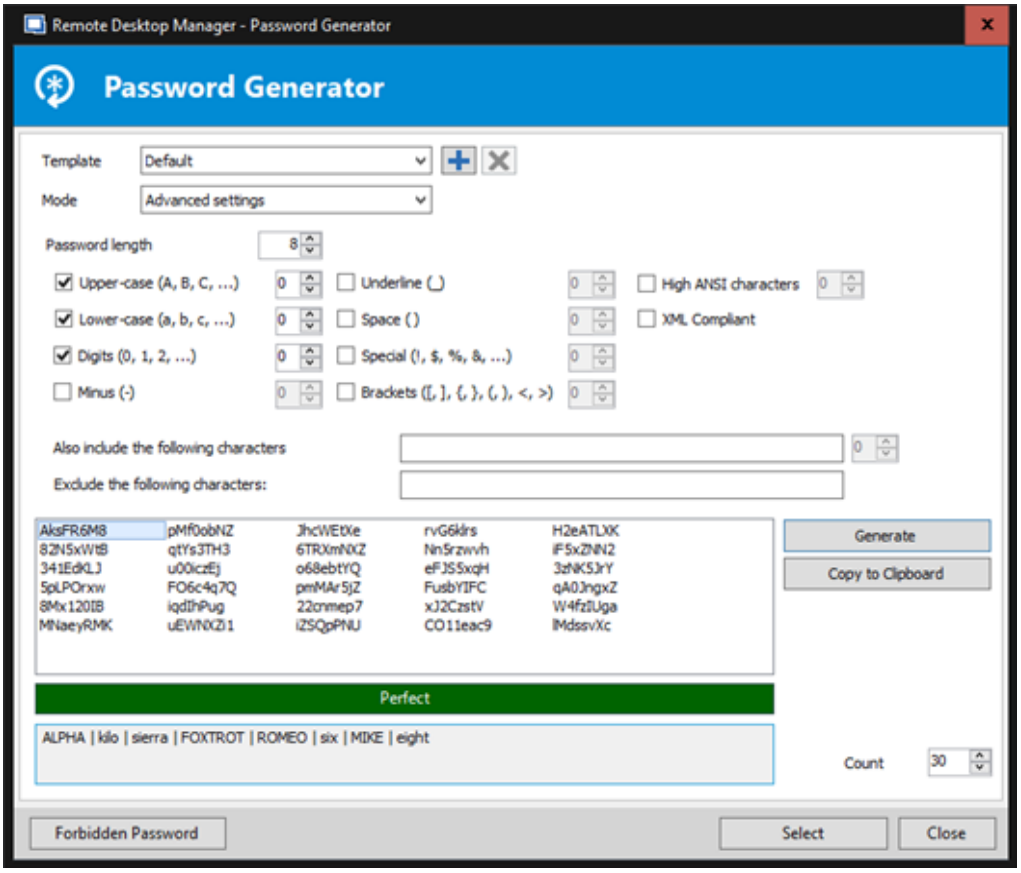


Figure 1 – Automatically creating strong passwords with RDM's Password Generator

Password Analyzer

To enable administrators to periodically check the strength of the passwords that are in use RDM provides a built-in password analyzer that can evaluate the passwords used by all the users of each remote session. You can see an example of RDM's Password Analyzer in Figure 2. In Figure 2 you can see that the passwords for each session and user are ranked as Weak, Strong, Perfect and Very Strong. Double clicking on any of the entries will bring up the session configuration dialog enabling you to change the password for those sessions that have weak passwords.

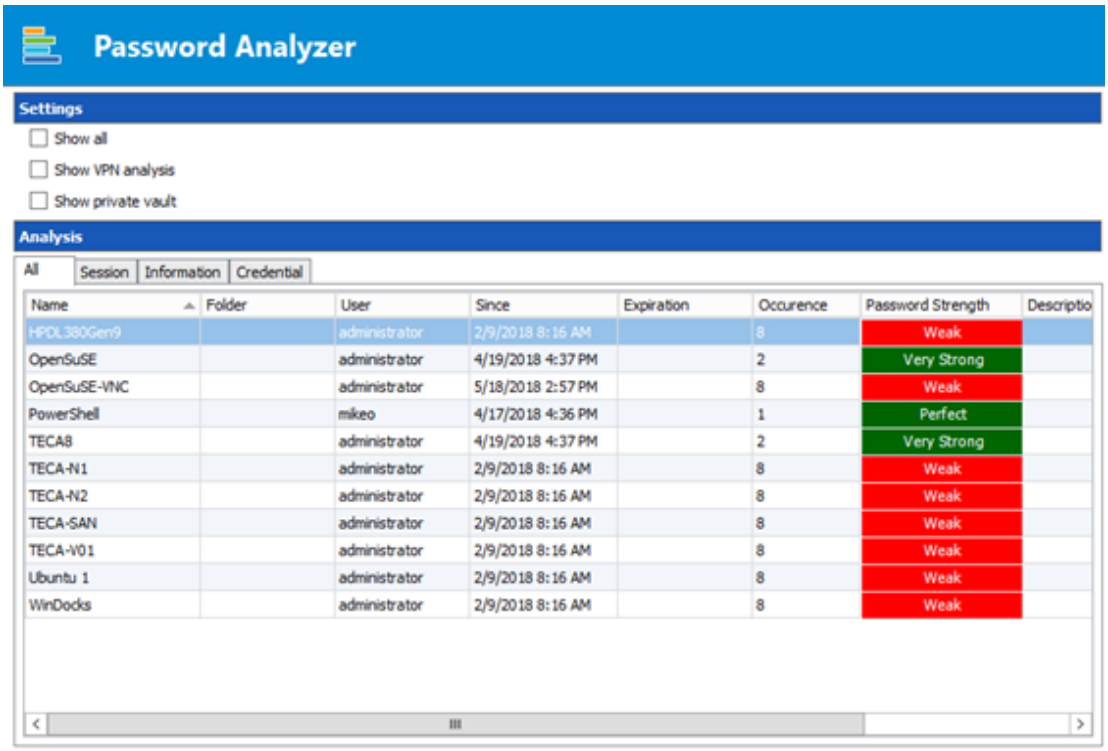


Figure 2 – RDMs Password Analyzer can report weak passwords

Centralized Password Management

IT administrators are responsible for managing and controlling access to the variety of different on-site and off-site servers. However, remote access for many businesses is typically inefficient and insecure because rely on multiple remote connection tools and often many different password managers. RDM can solve the problem of secure remote access by providing the ability to centrally and securely manage all of your remote connection passwords in one secure location. RDM can store company-wide passwords in an on-premise encrypted database helping users to quickly access the connection information and to share it between users and across teams. You can configure multiple remote connections that are shared from a centralized repository providing secure connections to remote servers, virtual machines, websites and applications. RDM supports a wide choice of remote connections, including web sites, Remote Desktop Protocol, RemoteFX, RealVNC, TightVNC, UltraVNC, Citrix ICA, LogMeIn, TeamViewer, RGS, DameWare, Radmin, pcAnywhere, Telnet, VMware vSphere, Hyper-V and more. RDM simplifies remote access by consolidating multiple different types of connections into a single window reducing desktop clutter and providing a single remote access portal.

In addition to managing Remote Desktop connections, RDM also provides centralized secure access to web sites through its web browser extension. Devolutions Web Login connection entry can store and retrieve the credentials required to log you in to any website. RDM's web browser extension technology works with RDM to obtain credentials and automatically fill in any authentication fields shown in the web browser. The authentication information is automatically when you use RDM to navigate to a website identified in a Web Login entry. You can see an

example of creating a new Web Login in Figure 3.

In Figure 3 you can see how the Web Login entry stores the URL and then login information for a remote website that requires authentication. Like remote desktop connections, the web site can be displayed either docked within the main RDM window or it can be displayed undocked on the desktop. Checking the Enable web browser extension link enables RDM to pass the browser the login information.

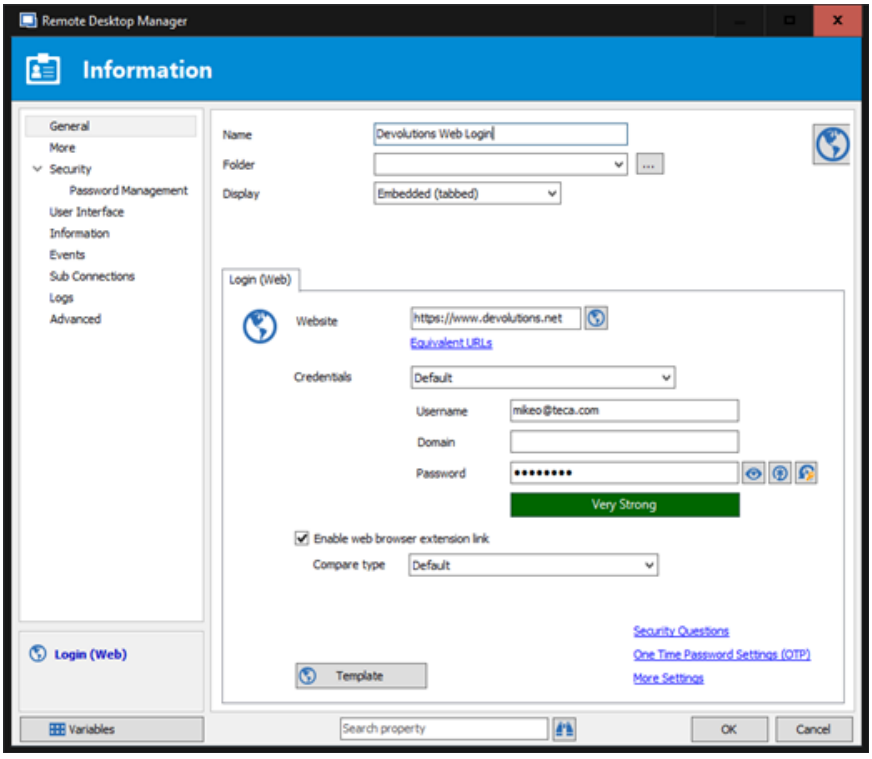
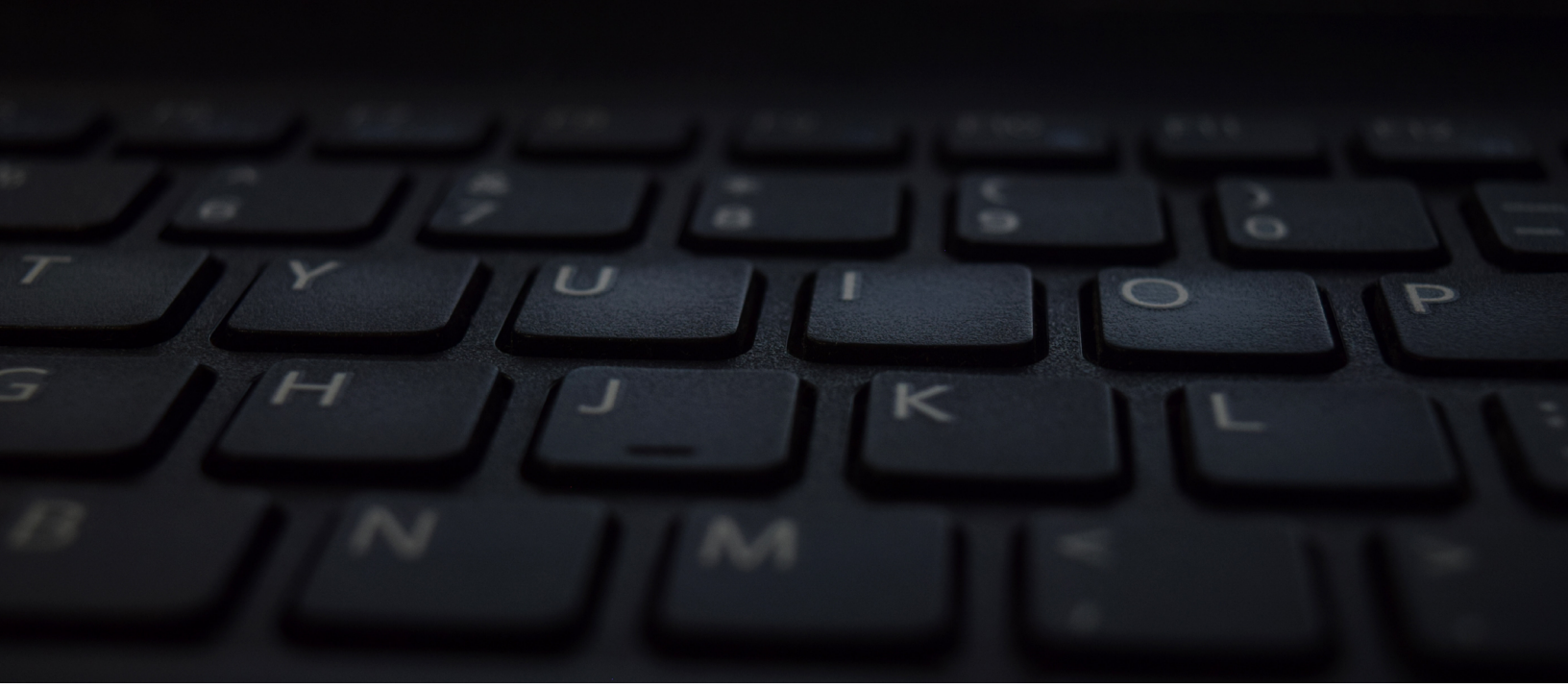


Figure 3 – Creating Web Login entries

Role Based Security

To facilitate and control remote access for multiple users RDM provides a role-based management capability that enables the administrator to control, delegate and filter different users access to privileged accounts. RDM's role-based management is often used to assign different security roles for different types of users like administrators, help desk personnel and consultants. Only authorized users can get access to view, edit or manage permitted privileged accounts. Restrictions are enforced based on the predefined user roles. Like you might expect, in order to use role-based security you need to use one of the shared team data sources like Microsoft SQL Server, SQL Azure or Devolutions Server.

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. All permissions are granular allowing multiple permissions can be set on multiple entries all at once. RDM's role-base security has the following attributes:



- Security is inherited -- Child items and folders are covered by the parent folder's security
- Permissions can be overridden -- Permission set on a sub folder will override the parent item's permissions
- Permissions are granular -- Multiple permissions can be set on entries at once

To ensure that remote connections are highly secured role-based security takes advantage of credential injection when sharing sessions. This credential injection works from all of RDM's connection types including remote desktop connections and different web site connections. RDM automatically brokers the role's credentials to the users. The users never have any access or knowledge of the actual credentials and are not able to compromise any security information. You can create new roles using the Roles option off RDM's Administrative menu. You can see an example of creating a new role with RDM in Figure 4.

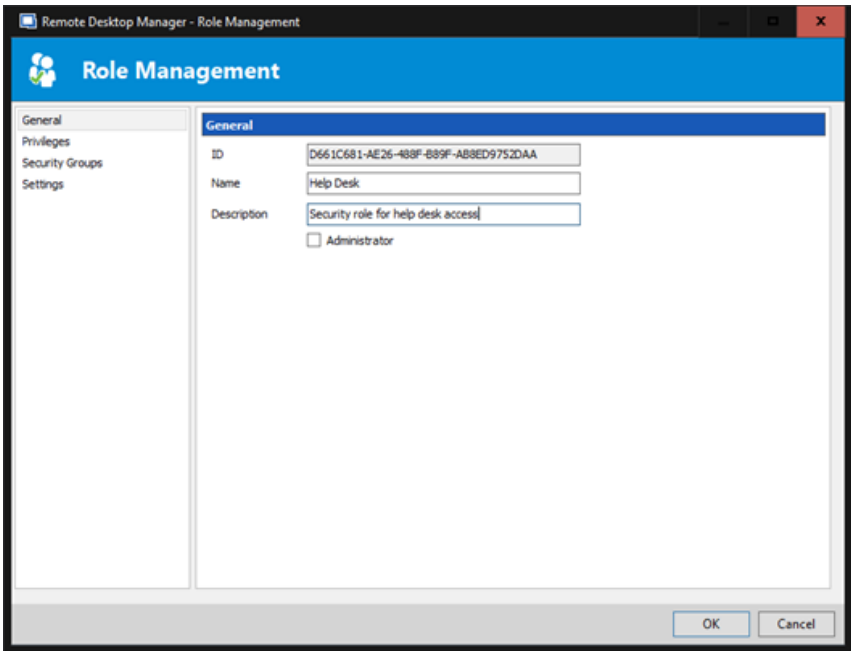


Figure 4 – Creating an RDM user role

To create role simply enter a name for the role; all the other settings can be left to default unless the role contains administrators. If the role is to be used by administrators then check the Administrator box when you create the role.

Next, after creating the roles you need, you can assign different users to the roles by clicking the Roles icon on the initial Security and User Management dialog. This will display the Security Role Assignment dialog that you can see in Figure 5. To assign users to a role you simply check the Is Member box for the respective user.

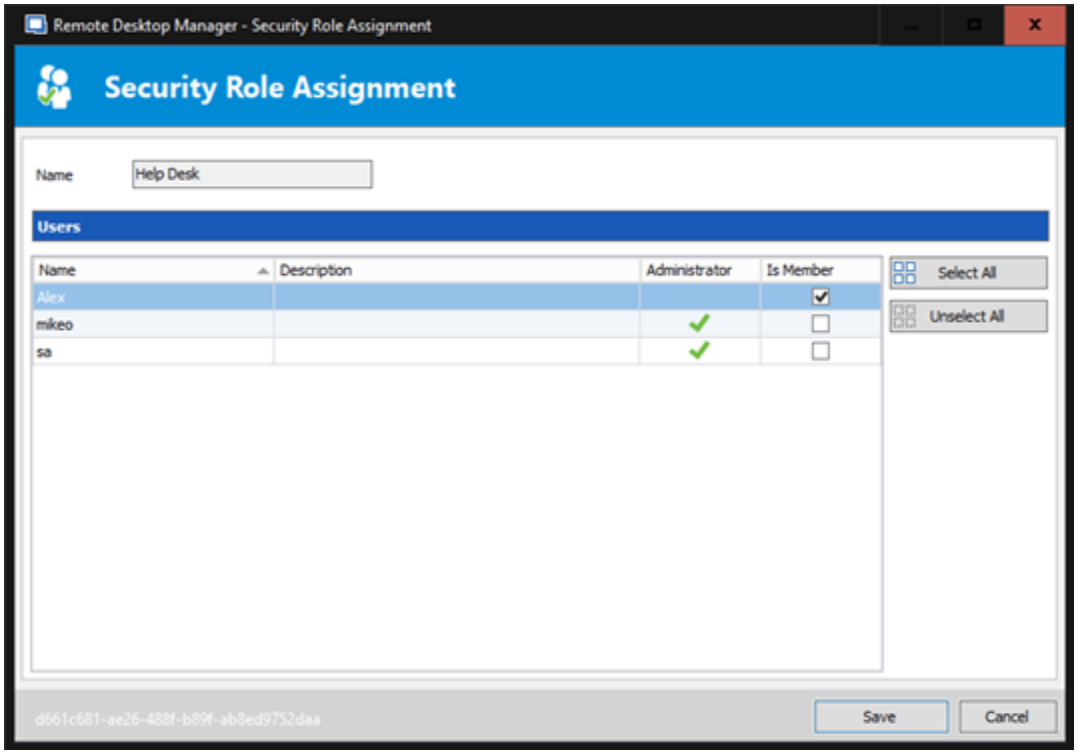


Figure 5 -- Assigning users to a role

Logging and Auditing

Logs and audit reports can enable you to evaluate your organization's security and help control access from privileged accounts. RDM logs all actions for each session and user and provides a complete audit trail for compliance and reporting. The logs record when sessions are opened and closed, the user who performed the action and with the duration of the session. RDM captures all privileged account operations including login attempts and history. RDM logs when session entries are viewed and changed as well as who performed the action. You can display a report of failed login attempts to a server. You can see an example RDM's remote connection Activity Logs in Figure 6.

Figure 6 shows the activity of each session entry, the session date and duration as well as the session user and session type. The advanced search capability enables you to filter the log for specific users, events and actions. The Activity Log can also be exported to a CSV file for further analysis.

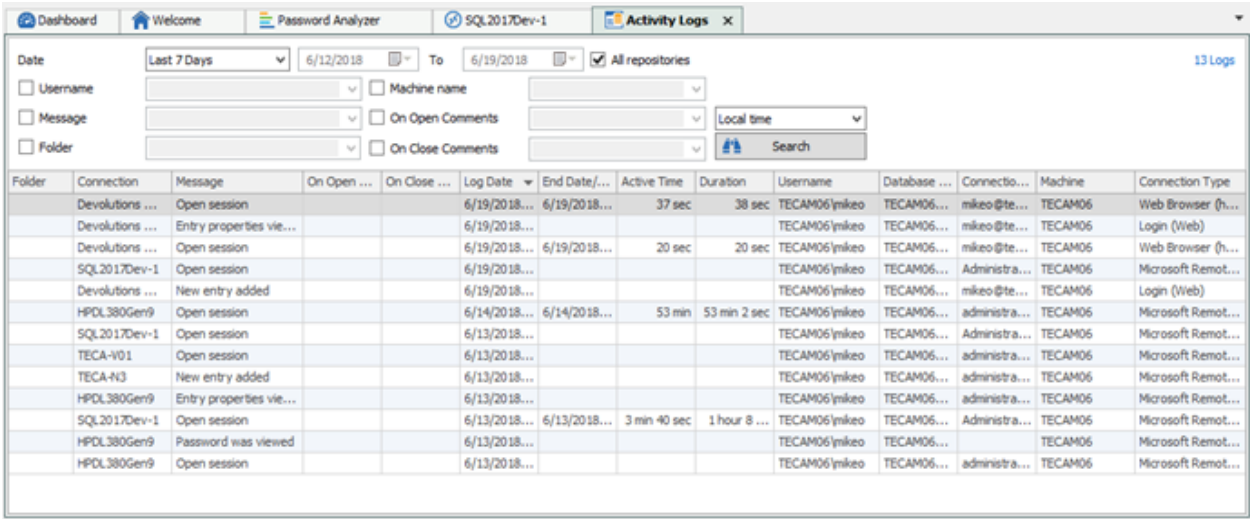


Figure 6 - Displaying RDM's security audit log

Additional Enterprise Security Consideration

RDM also provides several other important enterprise-level 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 example, 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 of the session and other users couldn't open the session 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 certain remote sessions during business hours. For more advanced security requirements RDM also supports two-factor authentication. Two-factor authentication is available for the following data sources: SQLite, Online Database, Devolution Server, MariaDB, Microsoft Access, SQL Azure, SQL Server and MySQL.

Additional Enterprise Security Consideration

Securely managing the remote connection requirements for your business is a difficult task that can easily create unintended security exposures through the use of multiple tools and multiple password repositories. RDM's centralized security and strong password protection can answer the challenges of enterprise password management and can strengthen your business's security as well as increase productivity for both users and administrators. Centralized role-based security facilitates secure team access for your remote desktop connections and your remote web connections. Enterprise-level logging and auditing provide visibility into your administrators and users remote session activity.