Top 5 Features to Look for in a Remote Desktop Management Solution

Devolutions

THIS ARTICLE WAS WRITTEN BY THE TECH TARGET TEAM IN PARTNERSHIP WITH DEVOLUTIONS.

How remote desktop management can help sysadmins do their jobs more easily

System administrators are ready for a revolution in the way they do their jobs. On a typical workday, sysadmins might connect to remote systems using Remote Desktop Protocol (RDP), PuTTY, browser-based tools, proprietary software, virtual private networks (VPNs) and many more remote connection technologies. These tools are indispensable — no one wants to go back to the days of trying to talk users through a problem over the phone.

But the same tools can also inhibit productivity. Sysadmins use multiple remote connection technologies, each of which supports specific protocols and has its own tools and unique user interface. Adding to the complexity of their jobs, sysadmins often have dozens, or even hundreds, of credentials sets to store and protect. Some resort to insecure methods of password management such as spreadsheets and plain text in script files. Of course, some manage user access through Microsoft Active Directory, but even so, users could be required to enter their credentials dozens of times in a day. These realities sap productivity and make sysadmins' jobs more difficult.

A remote desktop management solution that addresses these challenges can be truly transformational—if it has the five essential features described in this paper.

LOOK FOR A REMOTE DESKTOP MANAGEMENT SOLUTION WITH THESE CORE FEATURES

A remote desktop management solution should have five core features if it is to transform the way sysadmins do their jobs. The solution should be able to:

1. **Manage a wide range of remote connection technologies and protocols**

2. **Vault and store account passwords and other sensitive information**

3. **Securely share session settings between users**

4. **Manage roles, permissions and user security rights**

5. **Easily organize and retrieve sessions with an intuitive user interface**

FEATURE 1 | MANAGE A WIDE RANGE OF REMOTE CONNECTION TECHNOLOGIES AND PROTOCOLS

On any given day, sysadmins' screens are littered with windows. Sysadmins might have to use SSH, FTP, Telnet, RDP, VNC, HTTPS, TeamViewer, LogMeIn and many other tools to access remote computers—and that's before lunch. Each tool has its own interface, licensing costs and requirements. This large number of remote session protocols and tools adds complexity to the job and can kill productivity as sysadmins juggle windows to switch between different remote desktop sessions.

An ideal solution should support, in a single pane of glass, the full range of protocols and tools sysadmins work with, including VPNs. This solution would replace many open windows with a single interface that holds all sessions—no more time-consuming switching between sessions and no more overloaded and confusing taskbars.

FEATURE 2 | VAULT AND STORE ACCOUNT PASSWORDS, CREDENTIALS AND OTHER SENSITIVE INFORMATION

Sysadmins often have from dozens to hundreds of credentials to manage, not to mention account numbers, credit card information, software licensing codes and many other types of information. This sensitive data is regularly stored in multiple locations, such as password management applications, saved RDP sessions, and even spreadsheets, making it difficult to follow security and compliance best practices.

A comprehensive remote desktop management solution will include a secure, centralized vault for credentials and other sensitive data. It should allow sysadmins to access this information from anywhere and support automatic filling of login forms. Additionally, sysadmins who use a credential management application such as KeePass will want to ensure that the remote desktop management solution integrates with, or supports export from, their credential-management application.

A solution that features a secure vault strengthens security and supports compliance because information is stored in a centralized database protected by AES (Advanced Encryption Standard) encryption. It also simplifies sysadmins' jobs by eliminating multiple stores and locations for data that sysadmins need to do their jobs.

FEATURE 3 | SECURELY SHARE SESSION SETTINGS BETWEEN USERS

When a sysadmin is stumped by a remote desktop issue, it can be helpful to share the session with a colleague. But doing so securely and efficiently is a challenge. Sysadmins often resort to sharing connection settings and credentials in time-consuming and insecure ways, such as email, instant messaging apps, or even writing them down. This approach saps productivity and can weaken security and compliance.

A powerful remote desktop management solution should store connection settings and credentials in an encrypted, centralized database so users don't have to manually share sensitive information. With the right solution, team members who have the appropriate permissions can access the same session, and the system can even show or hide certain information based on user rights. These features save time and can enhance security and compliance.

FEATURE 4 | MANAGE ROLES, PERMISSIONS AND USER SECURITY RIGHTS

Role-based access control is critical in team environments. Without it, administrators struggle to enforce separation of duties and other controls that are meant to ensure team members see only what they're entitled to see—and nothing else. To strengthen security and compliance, administrators need to be able to manage roles, permissions and user rights so that users only have access to credentials and connections to which they are authorized.

The right desktop management solution should allow administrators to easily manage user access by setting specific rights for one or multiple users. Look for a solution that allows fine-grained control through creation of specific roles and groups with corresponding permissions that regulate access to sessions. The solution should be able to integrate with existing user access control tools, such as Active Directory. Active Directory group policy changes should automatically propagate to the remote desktop management solution when adding new users or changing users' roles. Another important feature in a multiuser environment is monitoring and tracking. The solution should have comprehensive logging capability so that organizations can track who has opened, closed or made changes to sessions.

FEATURE 5 | EASILY ORGANIZE AND RETRIEVE SESSIONS WITH AN INTUITIVE USER INTERFACE

Because sysadmins have hundreds of connections to manage, powerful organizational capabilities and an intuitive user interface can make the difference between productivity and frustration.

The solution should allow sysadmins to easily organize remote connections in an intuitive manner. For example, sysadmins might want to create one folder to hold the organization's connections to cloud servers and another for on-premises connections. A powerful solution will give sysadmins multiple viewing options through a familiar tree list structure. The solution should also allow sysadmins to flag their most frequently accessed sessions and include a search function so that sysadmins can find sessions quickly and easily. Additionally, the solution should provide templates that save sysadmins time when creating new connections.

LET REMOTE DESKTOP MANAGEMENT TRANSFORM YOUR JOB

A remote desktop management solution that delivers the five features described in this paper can transform sysadmins' jobs. Devolutions Remote Desktop Manager includes these features and more. It supports more than 60 different add-ons, and admins can customize it to make it work with the organization's existing technologies—from VPNs to password management tools to remote connection clients.

Remote Desktop Manager has helped sysadmins at thousands of companies transform the way they work. According to Eric Olmstead, building automation senior programmer at Siemens Building Technologies:

> A big win is that we can now securely manage our connections and credentials in a way that is easy to update, easy to share and easy to protect. It is also incredibly easy now to add access for a new technician to a certain scope of connections and/or credentials, just by proper placement in AD groups. No more emailing connections or storing them in a network location, no more texting credentials, and so on.

More than 300,000 users all over the world are achieving similar benefits with Remote Desktop Manager. Ready to see it in action for yourself?

Contact Devolutions for a live demo at
https://remotedesktopmanager.com/Home/RequestDemo.