



CONTROL THE **IT** CHAOS

3 Remote Desktop Factors That Contribute to System Administration Chaos



IT DOESN'T TAKE LONG BEFORE THE NUMBER OF PASSWORDS AND CONFIGURATION SETTINGS FOSTERS CHAOS

System administrators live and die by remote connections in order to quickly help users with their problems no matter where they are in the world. On a one-off basis, remote desktop mechanisms seem simple enough to deal with. For a single session, it is just a matter of using the

right protocol and having access to appropriate credentials to make a connection and gain access to the system. But as sysadmins scale their efforts across different types of IT assets, various connection protocols, numerous users, and different business groups or customer environments, the difficulty of securely managing credentials and configuring connections for each user situation starts to rear its head.

When IT groups manually manage connections, it doesn't take long before the number of passwords and configuration settings fosters chaos that quickly overwhelms teams. Problems typically crop up on three major fronts.

FACTOR 1 | FRAGMENTATION ADDS COMPLEXITY

Every user system has its own unique set of configuration requirements based on network policies, remote access tools, system protocols and credential information. At scale, **it becomes very difficult for the IT group to manage and share all of that connection and credential information.**

Ideally, when IT admins need to complete a task, they should be able to quickly access each system involved without jumping through a lot of hoops. However, as things stand, many organizations rely on a complex mishmash of Excel spreadsheets and Word documents to keep track of relevant connection information. With manual approaches like this, administrators struggle to keep track of new machines and establish a single source of truth for up-to-date server, connection and credential information. This means that every time they touch a new system remotely, sysadmins must do the legwork to look up credential information and take multiple steps to log in.

FACTOR 2 | LACK OF USER MANAGEMENT HEIGHTENS RISKS

Not only does this kind of manual tracking introduce complexity to a sysadmin's job, it also brings a lot of risk to the table. **The lack of automated controls over passwords, credentials and system privileges adds needless risk to the remote connection process.**

From both a regulatory and risk management perspective, IT groups need a way to give admins access without ever exposing user credentials during the process. What's more, organizations need to be able to manage privileges so not every sysadmin can necessarily access every single system in the environment. This requires security controls that can limit a sysadmin group's privileges based on the sensitivity of the system in question.

A manual process doesn't give the control necessary to manage risk across a large inventory of systems or a varied customer base. Additionally, configuring sessions on an ad hoc basis establishes a lack of reproducibility in configuration standards. This adds a greater probability of misconfigurations appearing in an environment that could potentially be leveraged by attackers.

FACTOR 3 | MANUAL CONFIGURATION KILLS PRODUCTIVITY

At the end of the day, the complexity of manually managing so many different connection variables eats into a sysadmin's daily working hours. Sysadmins and other IT pros need to establish remote connections over and over again throughout the day. If they need to enter an IP address, retrieve connection settings, start an instance of Remote Desktop Protocol or otherwise configure a session every time they work on a new task, the administrative overhead stacks up quickly. This poses a

This poses a huge drain on productivity that can ultimately impact a department's bottom line.

Controlling the chaos with Remote Desktop Manager

IT teams need a way to control the chaos on all of these fronts. They need a system that can help centralize configuration and connection information, manage user credentials without exposing passwords and 3 Remote Desktop Factors That Contribute to System Administration Chaos provide a single pane of glass that doesn't require a ton of rote administrative tasks just to establish a connection. Administrators need it to scale across hundreds of different types of connections, with wide scale interoperability and technology agnosticism. And they need a clear audit trail to prove the security of connections to customers and regulators.

Devolutions Remote Desktop Manager (RDM) does all of these things. It's an elegant and efficient system that saves remote connections, passwords and related documents in a single, secure platform.

The centralization of data makes it easy to add, edit, delete, share, organize and find remote connections and credentials. It's paired with an intuitive interface that can serve as an admin's Swiss Army knife for remote access. It offers more than 160 integrated technologies and protocols, including add-ons that support more than 25 types of virtual private networks (VPNs).

Most important, the connectivity is managed securely. IT teams can easily integrate existing password managers directly into RDM. The platform is designed so sysadmins are never given access directly to users' credential information. What's more, privileges are managed through permissions rules and security groups for ultimate flexibility. This creates the necessary separation of duties to protect sensitive data and comply with data security regulations.

Devolutions helps customers defeat the three factors

Devolutions helps a wide range of organizations control IT chaos by beating the major remote connection factors that contribute to it. Here's how RDM has helped IT professionals at **GolfNow, Siemens Building Technologies, and EchoStar, in their own words:**

ON COMPLEXITY:

"I AM ROUTINELY GOING INTO 20 TO 30 MACHINES PER DAY AT A MINIMUM. IF I HAD TO STOP AND LOOK UP THE SERVER ADDRESS, MY CREDENTIAL INFORMATION, MY VPN INFORMATION, OPEN THE VPN, OPEN THE MACHINE AND TYPE IN MY CREDENTIALS, I WOULDN'T BE ABLE TO FUNCTION OR PRODUCE THE LEVEL OF WORK I AM TODAY."

– Justin Azevedo, data services manager, GolfNow

ON SECURITY:

"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."

– Eric Olmstead, building automation senior programmer, Siemens Building Technologies

ON PRODUCTIVITY:

"IN MY 20 YEARS AS AN ADMIN, I'VE WORKED ACROSS MULTIPLE TYPES OF NETWORK HARDWARE INTERFACES, AS WELL AS OPERATING SYSTEMS. EACH OF THEM NEEDS TO BE ACCESSED BY ONE TOOL OR ANOTHER. BUT WITH RDM, I CAN GET MY WORK DONE BY USING JUST ONE TOOL! RDM TRULY IS ONE CONSOLE FOR ALL OF MY REMOTE ADMINISTRATIVE NEEDS."

– David Sechler, staff specialist, systems/network, EchoStar