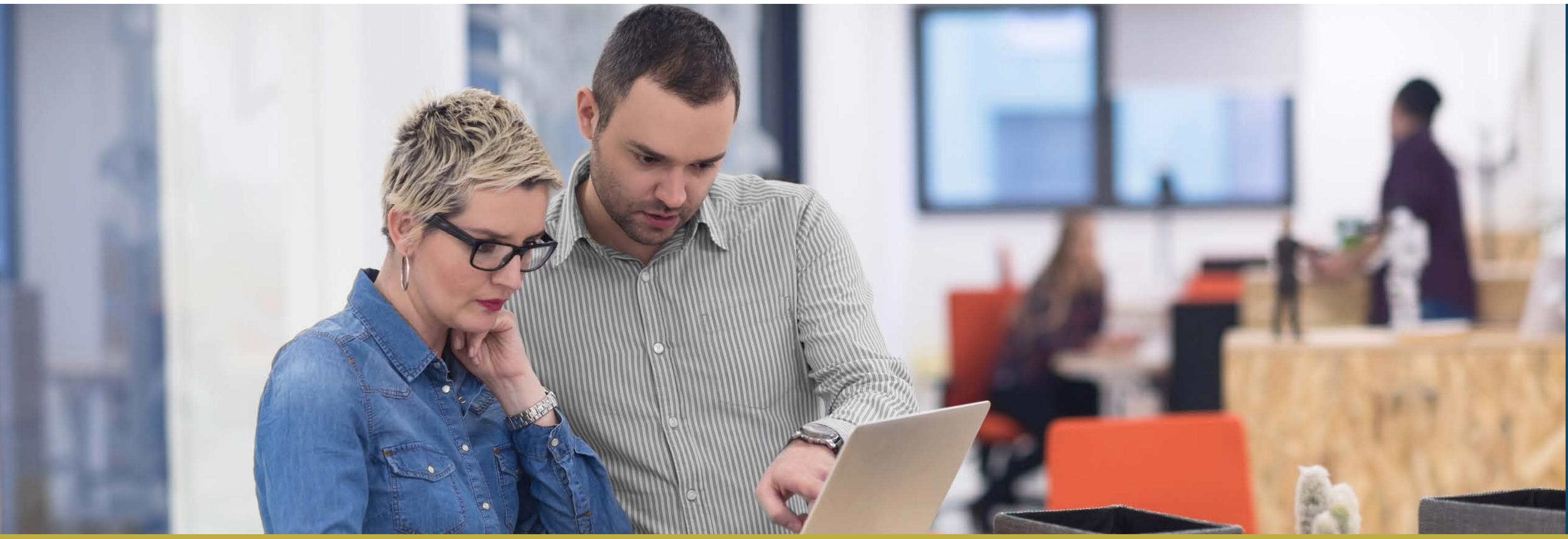
Petri IT Knowledgebase Resource
A BWW Media Group Brand



Petri Webinar Brief
October 5th, 2018

Remote Desktop Security for the SMB

Presenter: Michael Otey
Moderator: Brad Sams, Petri IT Knowledgebase, Executive Editor at Petri.com

There's no doubt that Remote Desktop is the SMB administrator's go-to remote administration tool. Remote Desktop is incredibly useful for remote administration as it enables you to have an interactive session with your remote systems – where the SMB administrator can work with them exactly as if they were local. There's no need to learn other remote management tools that can be difficult to setup and use or complicated scripting technologies.

Remote Desktop enables the SMB administrators to diagnose and resolve problems remotely. However, Remote Desktop is a powerful tool that often uses highly privileged access to the remote systems in your network. As such security for Remote Desktop is critically important. The Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) recommend that businesses review and understand their Remote Desktop usage and take steps to reduce the likelihood of compromise. They point out that failure to implement the proper security precautions can open the door to both malware and ransomware attacks and that Remote Desktop exploits can be difficult to spot because they have no user input. Let's take a closer look at understanding RDP and some of the main security concerns that the SMB administrator needs to be aware of with Remote Desktop.

Sponsored by
Devolutions

Understanding RDP

To properly secure Remote Desktop it's important to understand how it works. Remote Desktop uses the Microsoft's proprietary protocol Remote Desktop Protocol (RDP) to connect to remote systems.

By default, RDP uses TCP port 3389 and UDP port 3389. RDP is designed to support different types of network topologies and multiple LAN protocols. On the target server, RDP uses its own video driver to render display output into network packets and then uses the RDP network protocol to send them to the Remote Desktop client. The RDP client receives rendered display data and converts it into Microsoft Windows graphics device interface (GDI) API calls that are displayed by the Remote Desktop client.

Mouse and keyboard events are redirected from the client to the server. The RDP server uses its own keyboard and mouse driver to process these events. In addition, RDP has the ability to redirect other local client resources to the remote RDP target including the clipboard, printers, and local drives.

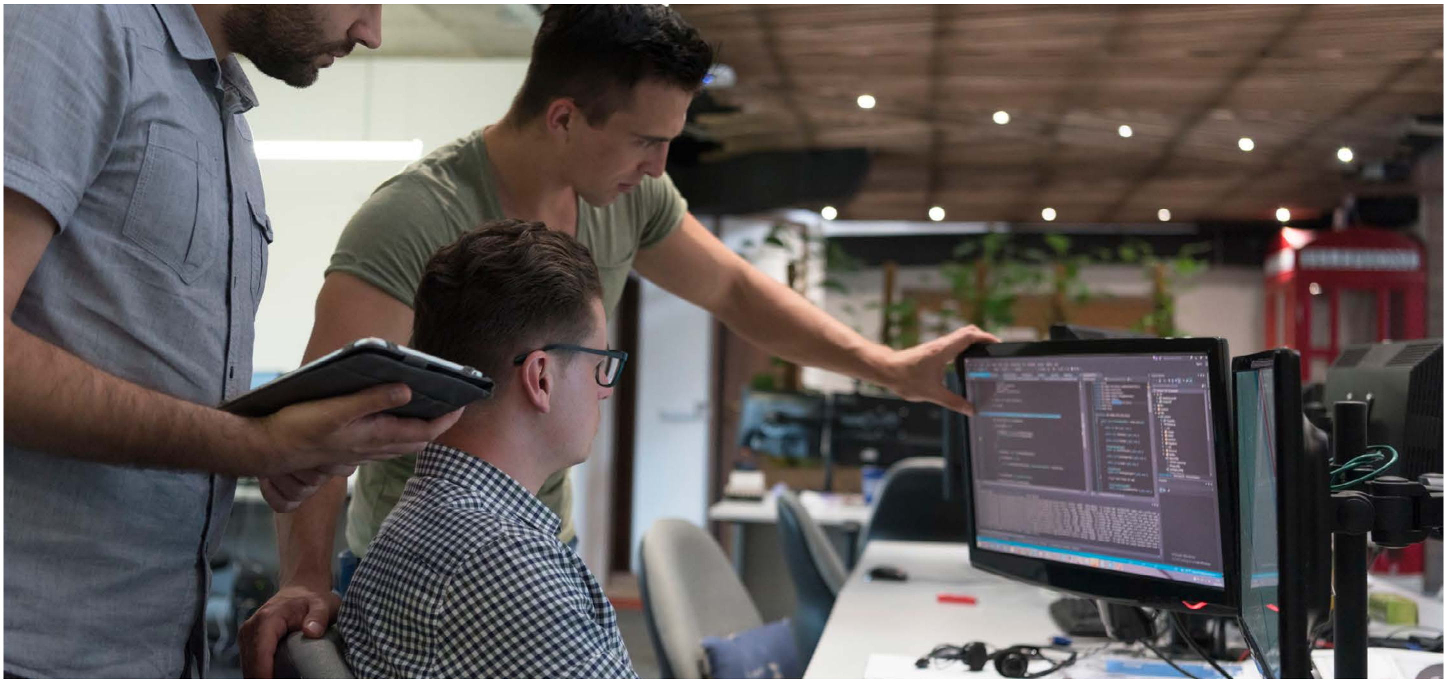
RDP Security Risks

Remote Desktop is a powerful tool and there are a number of possible RDP security risks – especially if your Remote Desktop servers are accessible from the Internet.

An Internet-wide scan carried out by security researchers from Rapid7 showed that there were over 11 million devices with 3389/TCP ports left open online. The number is up early 2016 when a previous scan found 9 million devices with port 3389 open. Many businesses – especially SMBs -- are unaware of the risks that come with potentially exposing RDP over the Internet.

RDP can be an attractive hacking target as the security is typically bound to an Active Directory (AD) domain for authentication. If AD or it's domain trusts are improperly configured hackers can obtain credentials for your organization's private internal resources.

For instance, even if you use a DMZ domain for Remote Desktops, improperly configured trusts within your corporate domains can lead to security breaches. RDP



is an important security vector and if hackers find a way into RDP they can validate user accounts, expose passwords, and infect your internal systems with malware and ransomware.

Brute force

One of the most common attacks to exposed RDP systems is brute force password hacking. With a brute force attack the attacker typically has a small list of user ids and then automated hacking software is used to quickly generate a large number of password guesses.

This past July 2018, LabCorp, one of the largest clinical labs in the U.S was hacked by the Samsam group using a brute force attack against RDP. They gained access through RDP and were able to further deploy ransomware on the LabCorp network. While the ransomware attack didn’t result in a data breech it was able to encrypt thousands of systems and hundreds of production servers were forced offline while their systems were restored.

This was basically the same ransomware that was used to attack the city of Atlanta in 2017. Protecting against brute force RDP attacks is vital for any exposed RDP systems.

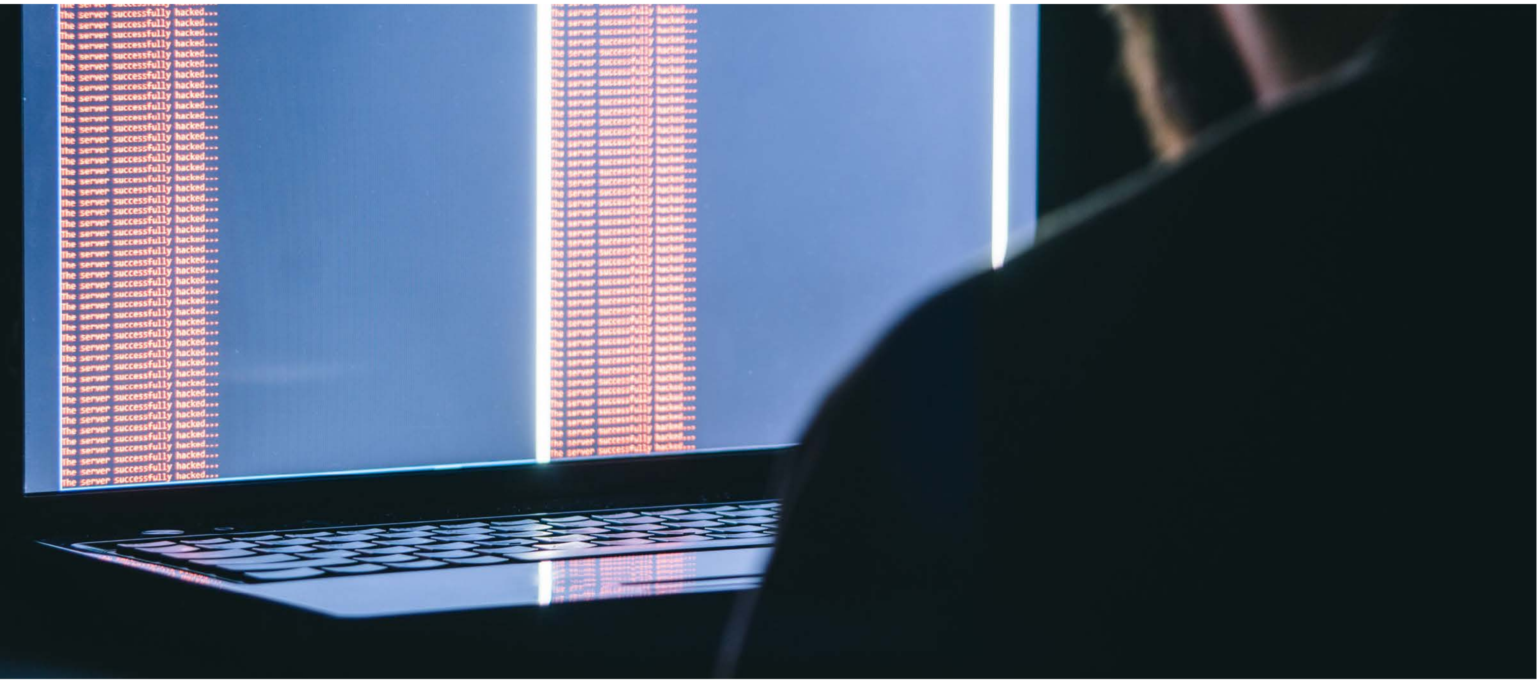
Password spraying

Another common RDP attack method is known as password spraying. With this type of attack there is typically a long list of users and a small list of strategically-chosen passwords that are used to attempt to login to the different accounts.

Password spraying allows hackers to attempt many logins usually without locking out users as it avoids repeated login attempts with the same user id so there is little notification. This technique can be effective because many employees use weak passwords. The list of potential attack accounts are often built by hackers by mining publicly available sources of information like Google, LinkedIn, and Facebook.

Man-in-the-Middle attacks

Older versions of RDP and misconfigured implementations can also be susceptible to man-in the middle attacks. Essentially, a man-in-the middle attack can cause RDP traffic to flow through a different host than the one the user intends. This man-in-the-middle host is then able to view the RDP network traffic and, in some cases, manipulate it and even possibly alter the security level negotiated between the server and client. This could possibly result in the user’s name and password being captured or other security exposures.

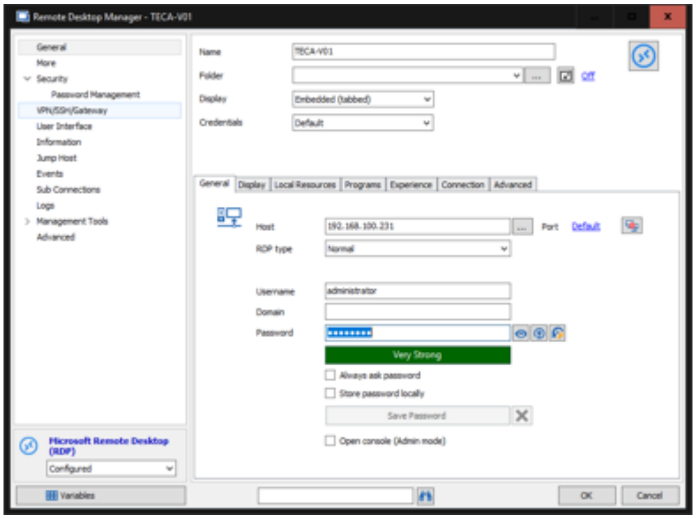


Securing RDP

There are a number of different options that SMBs can incorporate to lock down the security of their Remote Desktop connections. Taking advantage of some or all of these options can go a long way toward ensuring the safety and protection of the IT infrastructure.

Security starts with strong passwords

Security starts by making sure that all of your users are using strong passwords. Strong passwords that can't be easily guessed provide a core protection for your organization's sensitive data and can provide a strong layer of protection from brute force and password spraying attacks. Tools like Devolution Remote Desktop Manager (RDM) can ensure that your Remote Desktop passwords are strong by supporting password policies requiring, length, levels of complexity and enforcing password reuse history.

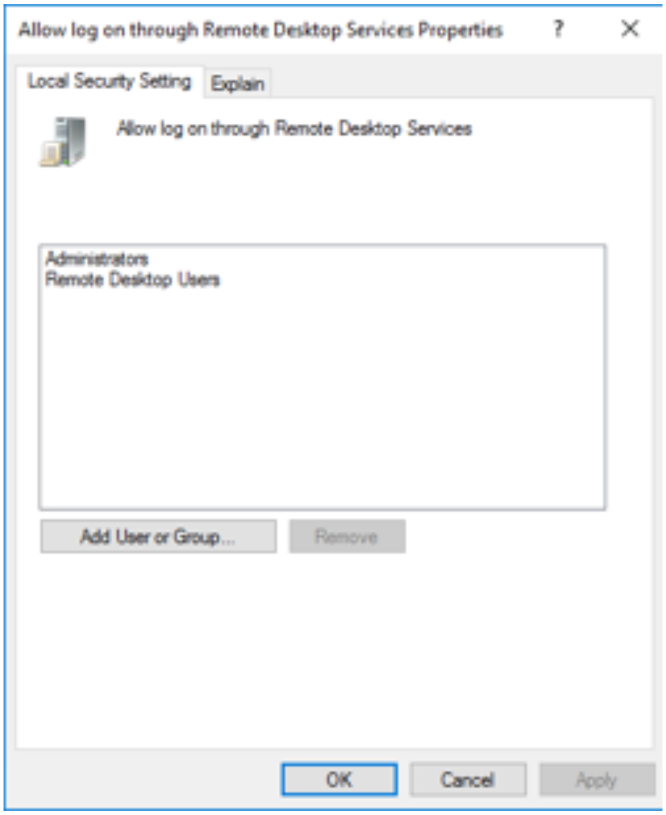


Name: TECA-V01
Folder:
Off
Display: Embedded (tabbed)
Credentials: Default
Host: 192.168.100.231
Port: Default
RDP type: Normal
Username: administrator
Domain:
Password: ••••••••
Very Strong
□ Always ask password
□ Store password locally
□ Open console (Admin mode)
Configured

Figure 1 - Using Strong Passwords with Remote Desktop Manager

RDM also provides a useful gauge of password strength when you create a new RDP session. You can see RDM's password strength gauge in Figure 1.

Locking Down RDP accounts with Security Policies



Allow log on through Remote Desktop Services

Administrators
Remote Desktop Users

Figure 2 – Locking down RDP users
You can optionally remove both of the groups listed by default in the Allow log on through Remote Desktop Services Property and then select Add User or Group to add the users or groups you want to have explicitly authorized to use Remote Desktop Services.

Changing the default users that are authorized to use Remote Desktop Services can also enhance your RDP security. By default, Windows Local Security Policies enables the Administrator's group and the Remote Desktop Users group to login with Remote Desktop.

If you want to change this you can open Local Security Policy using Server Manager then selecting Tools and Local Security Policy or by entering secpol.msc on the command prompt. From the Local Security Policy dialog expand Local Policies, then User Rights Assignment and double-click on the Allow log on through Remote Desktop Services. This will display the dialog you can see in Figure 2.

Using Account Lockout Policies

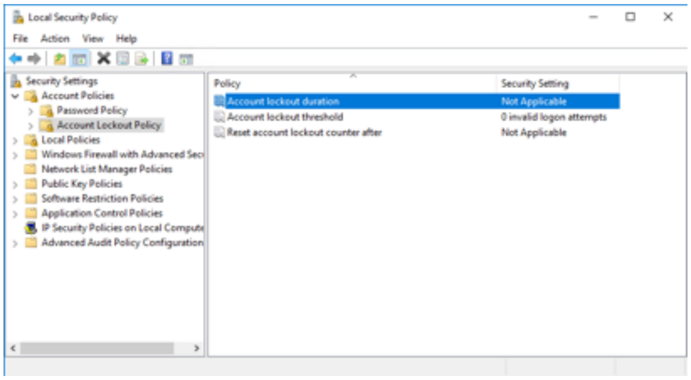
Account lockout policies can also help strengthen your Remote Desktop security. Account lockout policies can make it much more difficult for hackers and other unauthorized personnel from guessing your passwords manually or by using automated password cracking tools. Account lockout policies will lock out the RDP session from being used for a specified period of time after a number of incorrect login attempts. You can setup an account lockout policy by using Server Manager selecting Tools, then Local Security Policy or by typing secpol.msc into a command prompt. Expand Account Policies and then select Account Lockout Policies like you can see in Figure 3.

The Account lockout duration controls the amount of time an account will be locked out. While the specific lock out duration depend on the needs of the business a general recommended starting place is three minutes. The Account lockout threshold specifies the number of failed logins that will cause a user account to be locked out. Generally setting this between 4 and 10 is a good starting point. Reset account lockout counter after sets the time frame for counting invalid login attempts. This value is recommended to be less than or equal to the account lockout duration.

Encrypting RDP Connections

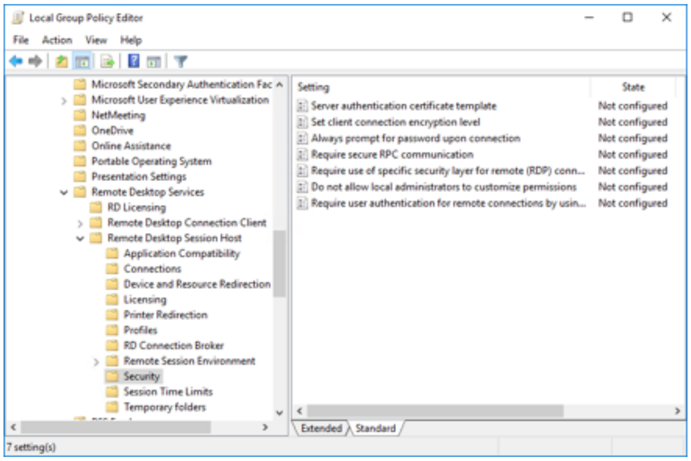
Many SMB assume that RDP is always secured with the highest encryption available by default. However, client RDP connections actually negotiate with the host for the level of encryption that will be used. RDP uses RSA Security's RC4 encryption which is designed to efficiently encrypt small amounts of data for secure communications over networks. Administrators can select to encrypt RDP data by using a 56 or 128-bit key.

To set the level of RDP encryption on the Windows Server 2016 RDP target system you can start the Local Group Policy Editor from Server Manager or by typing gpedit.msc into a command prompt. From the Local Group Policy Editor expand Computer Configuration, then Administrative Templates, Windows Components, Remote Desktop Services, Remote Desktop Session Host, and then click on Security. This will display the server's RDP security policies that you can see in Figure 4. To make sure that the RDP sessions to this system are encrypted at the highest levels select the Set client connection encryption level policy. This will display the dialog that you can see in Figure 5.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Sec
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

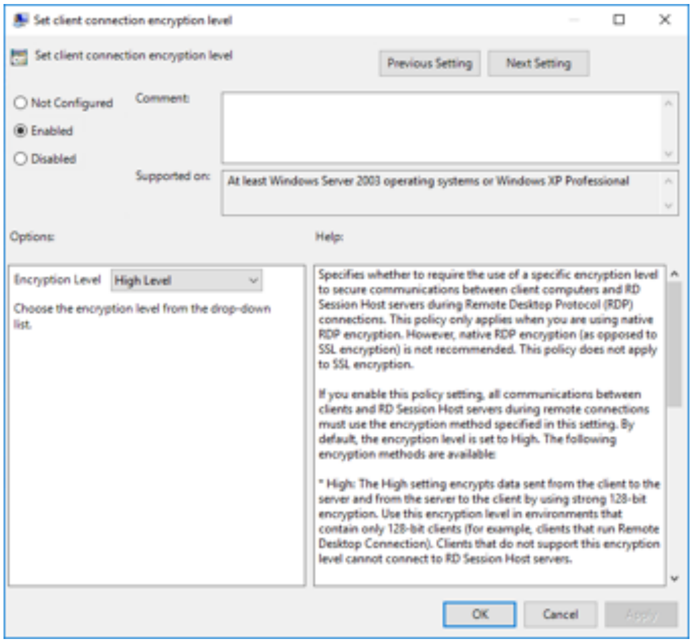
Policy	Security Setting
Account lockout duration	Not Applicable
Account lockout threshold	0 invalid logon attempts
Reset account lockout counter after	Not Applicable

Figure 3 – Setting Account Lockout Policies


Local Group Policy Editor
File
Action
View
Help
Microsoft Secondary Authentication Fac
Microsoft User Experience Virtualization
NetMeeting
OneDrive
Online Assistance
Portable Operating System
Presentation Settings
Remote Desktop Services
RD Licensing
Remote Desktop Connection Client
Remote Desktop Session Host
Application Compatibility
Connections
Device and Resource Redirection
Licensing
Printer Redirection
Profiles
RD Connection Broker
Remote Session Environment
Security
Session Time Limits
Temporary folders
Extended
Standard
7 setting(s)

Setting	State
Server authentication certificate template	Not configured
Set client connection encryption level	Not configured
Always prompt for password upon connection	Not configured
Require secure RPC communication	Not configured
Require use of specific security layer for remote (RDP) conn...	Not configured
Do not allow local administrators to customize permissions	Not configured
Require user authentication for remote connections by usin...	Not configured

Figure 4 – Setting Windows Server 2016 host RDP security policies
To make sure that the RDP sessions to this system are encrypted at the highest levels select the Set client connection encryption level policy. This will display the dialog that you can see in Figure 5.


Set client connection encryption level
Set client connection encryption level
Previous Setting
Next Setting
OK
Cancel
Apply

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2003 operating systems or Windows XP Professional

Options:

Encryption Level: High Level

Choose the encryption level from the drop-down list.

Help:

Specifies whether to require the use of a specific encryption level to secure communications between client computers and RD Session Host servers during Remote Desktop Protocol (RDP) connections. This policy only applies when you are using native RDP encryption. However, native RDP encryption (as opposed to SSL encryption) is not recommended. This policy does not apply to SSL encryption.

If you enable this policy setting, all communications between clients and RD Session Host servers during remote connections must use the encryption method specified in this setting. By default, the encryption level is set to High. The following encryption methods are available:

* High: The High setting encrypts data sent from the client to the server and from the server to the client by using strong 128-bit encryption. Use this encryption level in environments that contain only 128-bit clients (for example, clients that run Remote Desktop Connection). Clients that do not support this encryption level cannot connect to RD Session Host servers.

Figure 5 – Setting the client connection encryption level
To set the encryption level click the Enabled radio button near the top of the dialog and then use the Encryption Level dropdown to select High Level. This will ensure that Remote Desktop sessions are secured with 128-bit encryption.

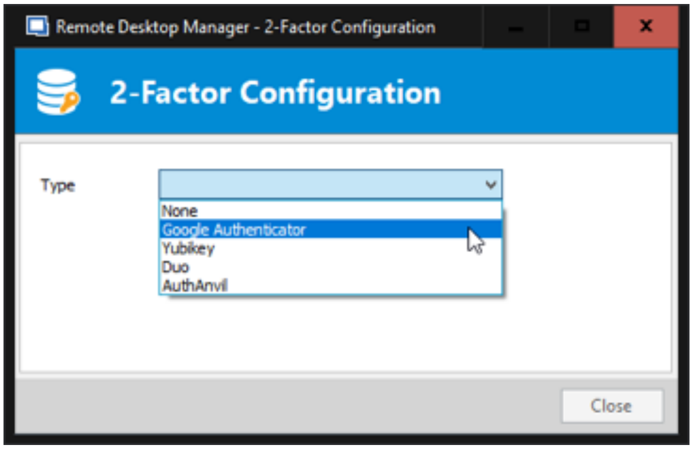


Figure 6 – Setting up Two-Factor Authentication with RDM

Using Two-Factor Authentication

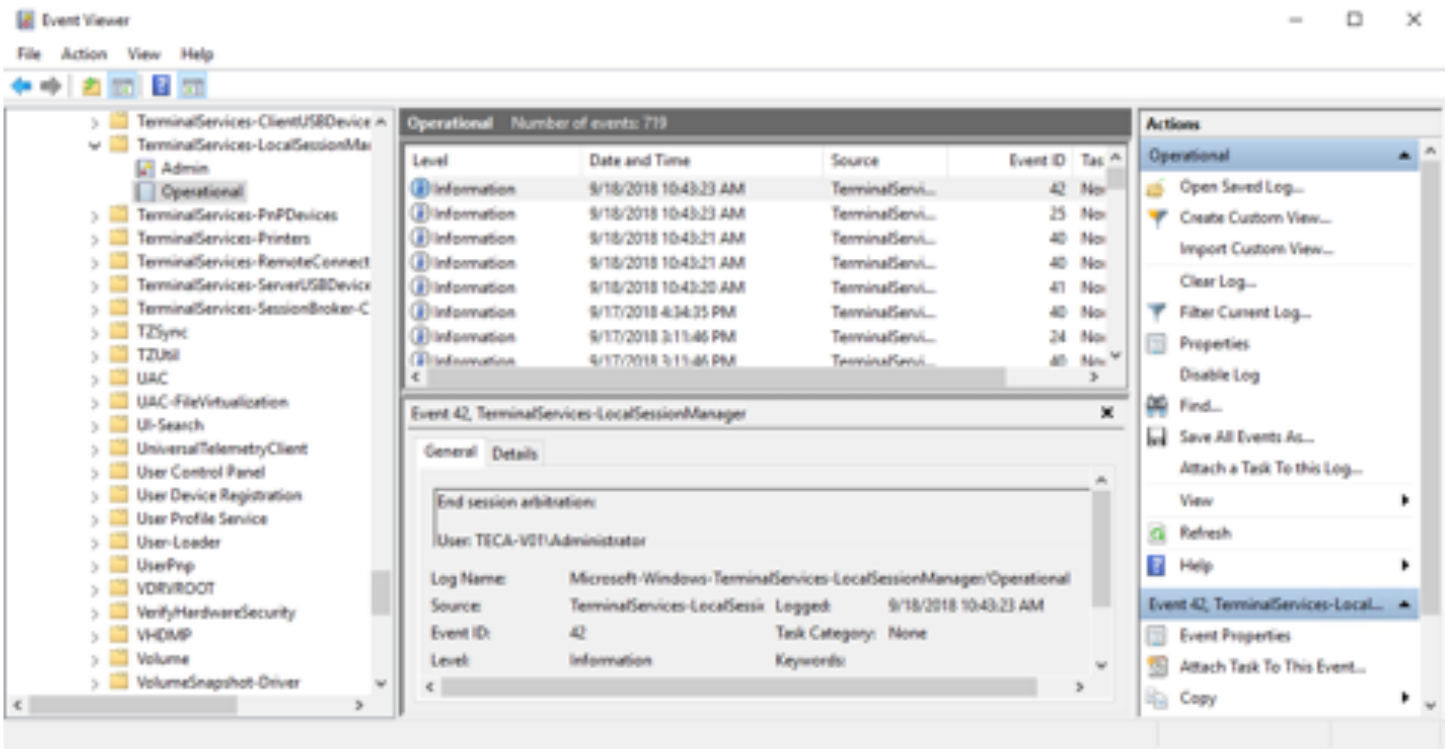
Two-Factory Authentication (TFA) can be another tool that can help you to secure RDP connections. Two-factor authentication provides stronger user identification by combing two different login components. These components are typically something the user knows like a password and something the user possesses like a key Fob or smartcard. TFA is provides a stronger level of security as an unauthorized user is less likely to be able to supply both of the factors required for authentication. To implement TFA with RDP you typically need to incorporate third-party products.

Devolutions RDM's data sources support multiple two-factor authentication options, including: Duo, Google Authenticator, Yubikey and AuthAnvil.
You can see an It's important that you don't make the mistake of thinking that TFA alone is a complete solution for RDP security. To be truly effective TFA must be uniformly applied to the organization's perimeter.

For instance, if you have a VPN using TFA but other services behind the VPN do not have TFA it might be possible for a hacker to exploit them to gain access to your infrasture. For maximum protection TFA it should be setup for all exposed assets that have access to sensitive information. example of using TFA with RDM in Figure 6.

Tracking Remote Logon Activity

Regular monitoring your Remote Desktop activity is



Operational Number of events: 719

Level	Date and Time	Source	Event ID	Tas
Information	9/18/2018 10:43:23 AM	TerminalServi...	42	No
Information	9/18/2018 10:43:23 AM	TerminalServi...	25	No
Information	9/18/2018 10:43:21 AM	TerminalServi...	40	No
Information	9/18/2018 10:43:21 AM	TerminalServi...	40	No
Information	9/18/2018 10:43:20 AM	TerminalServi...	41	No
Information	9/17/2018 4:34:35 PM	TerminalServi...	40	No
Information	9/17/2018 3:11:46 PM	TerminalServi...	24	No
Information	9/17/2018 3:11:46 PM	TerminalServi...	40	No

Event 42, TerminalServices-LocalSessionManager

General Details

End session arbitration:

User: TECA-V01\Administrator

Log Name: Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
Source: TerminalServices-LocalSessi Logged: 9/18/2018 10:43:23 AM
Event ID: 42 Task Category: None
Level: Information Keywords:

Figure 6 – Using the Remote Desktop Activity Log

another important factor for ensuring the security of your IT infrastructure. Regular monitoring can help you to detect if there are any regular unauthorized failed login attempts.

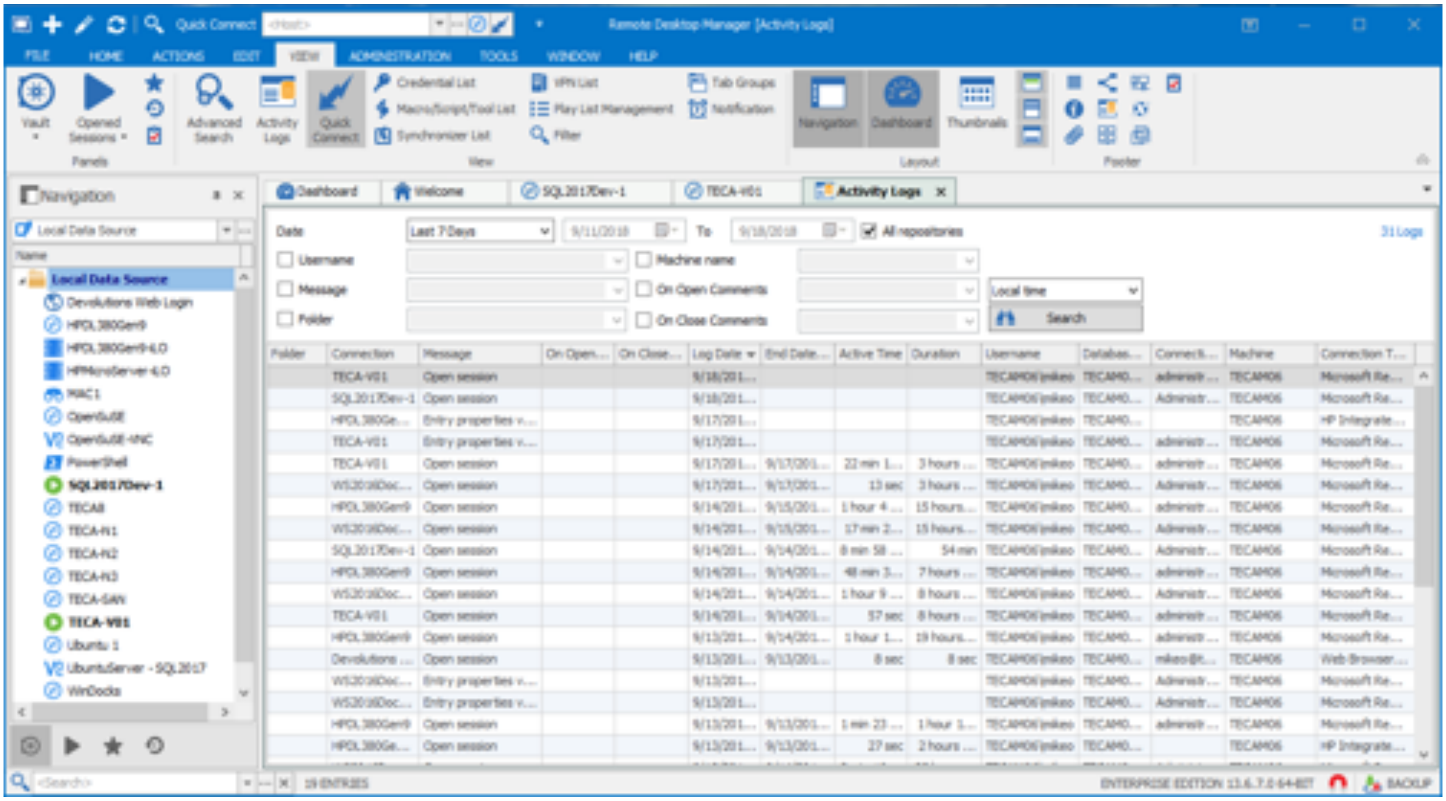
You can use Windows Server Event Viewer to track your Remote Desktop login activity by going to Server Manager then selecting Tools and Event Viewer. Expand Applications and Services Logs, then Microsoft, Windows, TerminalServices-LocalSessionManger and then select Operational. Using a centrally managed like Devolutions RDM can provide an even greater level of level of detail and information into your organization's Remote Desktop activity.

As you can see in Figure 7, RDM's Activity Log provides a centralized consolidated view of all of your organization Remote Desktop activity. For RDP connections RDM tracks the connection system, date, time, user and machine for all RDP sessions. In addition, RDM can also provide management and tracking for the vast majority of remote connection in use by most businesses including VNC, FTP Telnet, SSH, VPN and web browser connections.

Protect RDP using a Defense in Depth Strategy

Securing RDP for SMBs is every bit as important as it is in the enterprise – perhaps even more so as security breaches for the SMB can have a bigger overall impact on the business. Defense in depth is the best approach for securing RDP. In addition to securing RDP using the strategies that are outlining in this paper its vital that you keep your client and server operating systems patched with the current updates. Critical services should be behind a VPN and not directly exposed on the Internet.

VPNs are designed to separate and secure your private resources for external attacks. They are hardened and designed to prohibit unauthorized access to your systems and services like RDP. Even if the VPN is breeched there is still separation from your corporate infrastructure.



Date: Last 7 Days, 9/11/2018 To 9/18/2018 ☑ All repositories 31 Logs

□ Username □ Machine name

□ Message □ On Open Comments Local time

□ Folder □ On Close Comments Search

Folder	Connection	Message	On Open...	On Close...	Log Date	End Date...	Active Time	Duration	Username	Databas...	Connecti...	Machine	Connection T...
	TECA-V01	Open session			9/18/201...				TECAM06\mikeo	TECAM0...	administr...	TECAM06	Microsoft Re...
	SQL2017Dev-1	Open session			9/18/201...				TECAM06\mikeo	TECAM0...	Administr...	TECAM06	Microsoft Re...
	HPDL380Ge...	Entry properties v...			9/17/201...				TECAM06\mikeo	TECAM0...		TECAM06	HP Integrate...
	TECA-V01	Entry properties v...			9/17/201...				TECAM06\mikeo	TECAM0...	administr...	TECAM06	Microsoft Re...
	TECA-V01	Open session			9/17/201...	9/17/201...	22 min 1...	3 hours ...	TECAM06\mikeo	TECAM0...	administr...	TECAM06	Microsoft Re...
	WS2016Doc...	Open session			9/17/201...	9/17/201...	13 sec	3 hours ...	TECAM06\mikeo	TECAM0...	Administr...	TECAM06	Microsoft Re...
	HPDL380Gen9	Open session			9/14/201...	9/15/201...	1 hour 4 ...	15 hours...	TECAM06\mikeo	TECAM0...	administr...	TECAM06	Microsoft Re...
	WS2016Doc...	Open session			9/14/201...	9/15/201...	17 min 2...	15 hours...	TECAM06\mikeo	TECAM0...	Administr...	TECAM06	Microsoft Re...
	SQL2017Dev-1	Open session			9/14/201...	9/14/201...	8 min 58 ...	54 min	TECAM06\mikeo	TECAM0...	Administr...	TECAM06	Microsoft Re...
	HPDL380Gen9	Open session			9/14/201...	9/14/201...	48 min 3...	7 hours ...	TECAM06\mikeo	TECAM0...	administr...	TECAM06	Microsoft Re...
	WS2016Doc...	Open session			9/14/201...	9/14/201...	1 hour 9 ...	8 hours ...	TECAM06\mikeo	TECAM0...	Administr...	TECAM06	Microsoft Re...
	TECA-V01	Open session			9/14/201...	9/14/201...	57 sec	8 hours ...	TECAM06\mikeo	TECAM0...	administr...	TECAM06	Microsoft Re...
	HPDL380Gen9	Open session			9/13/201...	9/14/201...	1 hour 1...	19 hours...	TECAM06\mikeo	TECAM0...	administr...	TECAM06	Microsoft Re...
	Devolutions ...	Open session			9/13/201...	9/13/201...	8 sec	8 sec	TECAM06\mikeo	TECAM0...	mikeo@t...	TECAM06	Web Browser...
	WS2016Doc...	Entry properties v...			9/13/201...				TECAM06\mikeo	TECAM0...	Administr...	TECAM06	Microsoft Re...
	WS2016Doc...	Entry properties v...			9/13/201...				TECAM06\mikeo	TECAM0...	Administr...	TECAM06	Microsoft Re...
	HPDL380Gen9	Open session			9/13/201...	9/13/201...	1 min 23 ...	1 hour 1...	TECAM06\mikeo	TECAM0...	administr...	TECAM06	Microsoft Re...
	HPDL380Ge...	Open session			9/13/201...	9/13/201...	27 sec	2 hours ...	TECAM06\mikeo	TECAM0...		TECAM06	HP Integrate...

19 ENTRIES ENTERPRISE EDITION 13.6.7.0 64-BIT BACKUP

Figure 7 – Tracking Remote Desktop usage with RDM's Activity Log