## Forcing RDP to use TLS Encryption

427 Krishnaja August 2, 2024 Common Errors & Troubleshooting, General 11561

## How to force RDP to use TLS Encryption?

**Overview:** This article provides instructions on how to force Remote Desktop Protocol (RDP) to use TLS encryption.



Windows Remote Desktop Protocol (RDP) is widely used by system administrators to provide remote operators access to internal systems and servers. In a shocking oversight, this connection does not use strong encryption by default. To force RDP to use TLS Encryption follow below steps

Step 1: Open the Root console

Open the search bar and type "**mmc**" or run **mmc.exe** from the Run application. Select the top application, which will open the system console.

All Apps	Documents	Web More 🔻		<i>₽</i> …
Best match				
Run comm	and			
Search the web			mmc	
🔎 mmc - See v	veb results	>	Run command	
, P mmc colleg	e	>		
, P mmc login		>	🖵 Open	
		>	C Run as administrator	
𝒫 mmcc		>	D Open file location	
, мтс <b>ое ри</b>	ne	>		
, P mmc cme I	ist	>		
, ∕⊂ mmc da2 a	lpha	>		
,				

Step 2: Open the Group Policy Editor Snap-in

Open File -> Add/Remove Snap-in and select Global Policy Editor.

			<u>^</u>
File Action View Favorites Window Help			- 8 ×
New Ctrl+N			
Open Ctrl+O		Actions	
Save Ctrl+S	These set is the state of a line for the	Console Root	
Save As	There are no items to show in this view.	More Actions	• •
Add/Remove Snap-in Ctrl+M			
Options			1000
1 compmgmt			and the second second
E-a			
LAR			
Enables you to add shap jus to or remove them from the shap	n-in contole		

Step 3: Select "Group Policy Editor" and click on "Add" the selected snap-in.

<b>a</b>	Console1 - [Console Root]	
🚟 File Action View Fi	Add or Remove Snap-ins	
🜩 📄 🔐 🔒 🔽 📷	You can select snap-ins for this console from those available on your computer and configue extensible snap-ins; Selected snap-ins; Selected snap-ins; Selected snap-ins; Selected snap-ins; Selected snap-ins; Selected snap-ins; Console Root By Microsoft Cor Folder Microsoft Cor Folder Microsoft Cor	re the selected set of snap-ins. For Edit Extensions Remove Move Up
	■ Group Policy Manag       Microsoft Cor         ■ Group Policy Object       Microsoft Cor         ■ Group Policy Starter       Microsoft Cor         ■ JP Security Monitor       Microsoft Cor         ■ Link to Web Address       Microsoft Cor         ■ Link to Web Address       Microsoft Cor         ■ Local Backup       Microsoft Cor         ■ Local Users and Gro       Microsoft Cor         ■ NAP Client Configur       Microsoft Cor         ■ NAP Client Configur       Microsoft Cor         ■ NAP Client Configur       Microsoft Cor	Move Down Advanced
	Description: This snap-in allows you to edit the local Group Policy Objects stored on a computer.	OK Cancel

Step 4: Select the "Local Computer", this should be the default and select "Finish" > "Ok"



Step 5: Navigate to the RDP Session Security Policies

In the sidebar Navigate to Local Computer Policy -> Computer Configuration -> Administrative Templates -> Windows Components -> Remote Desktop Services --> Remote Desktop Session Hosts -> Security. Then select "Set client encryption level" and edit that policy.

File Action View Favorites	Window Help		
	🚊 Security		Actions
Connections Connections Connections Connections Profiles RD Connection Bro Conne	Set client connection encryption level Edit <u>policy setting</u> Requirements: At least Windows Server 2003 operating systems or Windows XP Professional Description: This policy setting specifies whether to require the use of a specific encryption level to secure communications between client computerss and RD Session Host servers during Remote Desktop Protocol (RDP) connections.	Setting       Image: Server authentication certificate template       N         Set Client connection encryption level       Image: Set Client connection       N         Always prompt for password upon connection       N       Image: Set Client connection       N         Require secure RPC communication       N       Image: Set Client connection       N         Image: Require use of specific security layer for remote (RDP) conn       Image: Do not allow local administrators to customize permissions       N         Image: Require user authentication for remote connections by usin       N	Security More Actions Set client connection en More Actions
	If you enable this policy setting, all communications between clients and RD Session Host servers	×	5

**Step 6:** Require the Highest native Encryption possible

Edit the "Set client encryption level policy".

Set client connect	tion encryption le	Set client cor vel	Previous Setting Next Setting		x	nplates\Windows Con	npor	nents\Remote 💻 🗖 🔅	×
O Not Configured	Comment:			[	^			Actions	_
Enabled								Security	•
O Disabled					~	nplate	No	More Actions	►
	Supported on:	At least Window	vs Server 2003 operating systems or Windows XP Profes	sional	^	/el		Set client connection en	•
					~	connection	No	More Actions	►
Options:			Help:			n r for remote (RDP) conn customize permissions	No		
Encryption Level Hi Choose the encryp list. Lo	igh Level ient Compatible igh Level ww Level	n	This policy setting specifies whether to require the us specific encryption level to secure communications to client computerss and RD Session Host servers during Desktop Protocol (RDP) connections. If you enable this policy setting, all communications clients and RD Session Host servers during remote co must use the encryption method specified in this set default, the encryption nethod specified in this set default, the encryption level is set to High. The follow encryption methods are available: * High: The High setting encrypts data sent from the server and from the server to the client by using stror encryption. Use this encryption level in environments contain only 128-bit clients (for example, clients that Desktop Connection). Clients that do not support thi level cannot connect to RD Session Host servers. * Client Compatible: The Client Compatible setting e	e of a etween Remote between nnections ing. By ing client to the g 128-bit that run Remote encryption		ote connections by usin	No		

Step 7: A better idea -> Force TLS instead

Edit the "Require use of specific security layer for remote (RDP) connections" policy.



Online URL: https://www.ezeelogin.com/kb/article/forcing-rdp-to-use-tls-encryption-427.html