

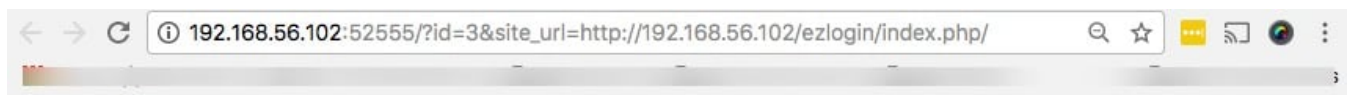
NODE_RDP_PROTOCOL_X224_NEG_FAILURE()

184 admin October 7, 2024 [Common Errors & Troubleshooting](#) 12793

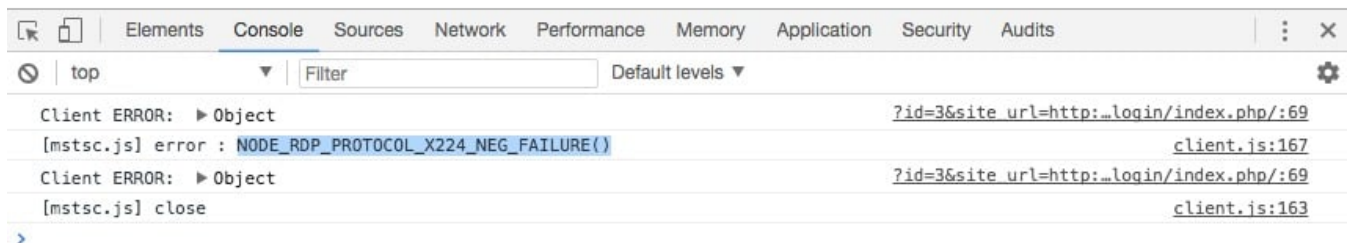
Troubleshooting "Connection has been closed" error in windows RDP

Overview: This article provides solutions for resolving the "Connection has been closed" error in Windows RDP. It advises using the web console to inspect error details and recommends disabling Network Level Authentication and enforcing TLS encryption through Group Policy Editor to mitigate issues like "NODE_RDP_PROTOCOL_X224_NEG_FAILURE()."

1. If you get the error " **Connection has been closed. Another user may have logged in on the remote Windows machine**" while doing RDP into the remote Windows server, then 'right click'->'inspect'-> click 'console' tab as shown in the image below.



Connection has been closed. Another user may have logged in on the remote windows machine.



Note:

To open the web console and gather information about the error, follow any of these steps.

1. Right-click on the RDP browser tab, select "Inspect", and then navigate to the "Console" tab on the opened page.

or

2. Press "F12" to access the console of the GUI.

Step 1: Check if the **username and password in Ezeelogin software are correct**. Refer to below example.

Ezeelogin Welcome, Administrator Logout

Servers

- Server Groups
- Super Groups
- Sub SSH Users
- Sub SSH User Maps
- mExec lists
- Import
- Global Key
- Key Management

Web Portals

Users

Access Control

Settings

Cluster

Command Guard

Account

Help

License

← Collapse

Add Server

Hostname: Windows_RDP

Remote SSH / RDP Login User: Administrator

SSH Private Key

SSH Port: 22

Password Management: keep server password

RDP Port: 3389

Windows Domain

Control Panel: -- None --

Description: RDP SERVER

IP Address(es): 192.168.1.10

SSH / RDP Password:

SSH Key Passphrase

SSH: disabled

Server Group: test

RDP

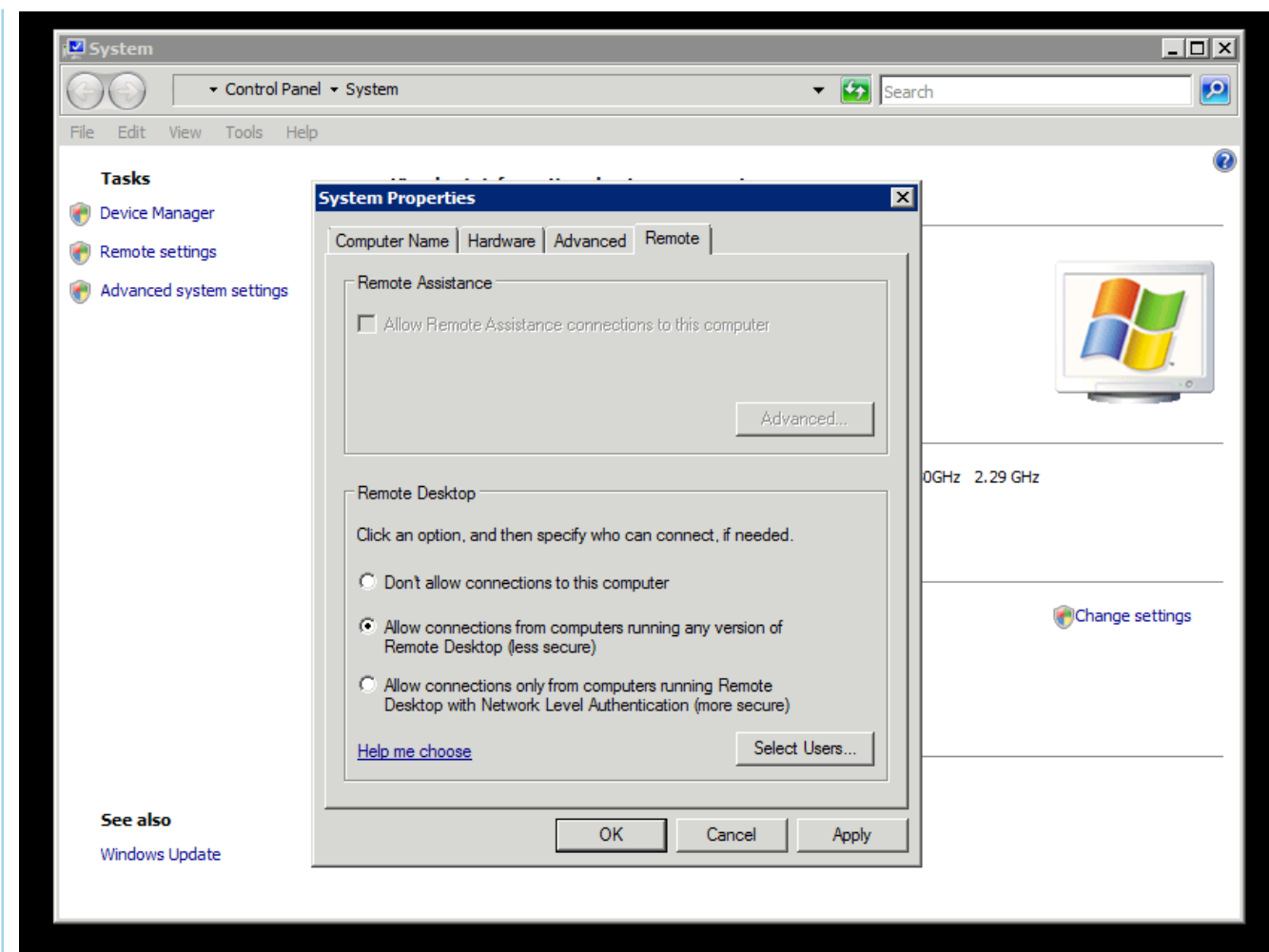
Datacenter: -- None --

First Prompt

Clone a server: -- None --

Cancel Save

Note: Confirm if RDP from Ezeelogin works when Network Level Authentication is disabled, check the settings under Control Panel -> System -> Remote settings.



Step 2: Also make sure to force TLS encryption on all RDP connections.

Step 2 (A): Run `mmc` in the Run application of your Windows server. In the console, open **File > Add/Remove Snap in > Select Global Policy Editor** and add the selected Snap in .

Step 2 (B): Select **Local Computer** and then select **Finish>OK**

Step 2 (C): In the sidebar Navigate to **Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Hosts > Security**. Then Edit the "Require use of specific security layer for remote (RDP) connections" policy as shown below.

You need to select the security layer as **SSL (TLS 1.0)**

windows [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Require use of specific security layer for remote (RDP) connections

Require use of specific security layer for remote (RDP) connections Previous Setting Next Setting

Not Configured Comment:

Enabled

Disabled

Supported on:

Options: Help:

Security Layer: Choose the security layer from the drop-down list.

This policy setting specifies whether to require the use of a specific security layer communications between clients and RD Session Host servers during Remote Desktop (RDP) connections.

If you enable this policy setting, all communications between clients and RD Session Host servers during remote connections must use the security method specified in this setting. The following security methods are available:

- * Negotiate: The Negotiate method enforces the most secure method that is supported. If Transport Layer Security (TLS) version 1.0 is supported, it is used to authenticate the client and RD Session Host server. If TLS is not supported, native Remote Desktop Protocol (RDP) encryption is used for secure communications, but the RD Session Host server is not authenticated.
- * RDP: The RDP method uses native RDP encryption to secure communications between the client and RD Session Host server. If you select this setting, the RD Session Host server is not authenticated.
- * SSL (TLS 1.0): The SSL method requires the use of TLS 1.0 to authenticate the RD Session Host server. If TLS is not supported, the connection fails.

If you disable or do not configure this policy setting, the security method to be used for communications to RD Session Host servers is not specified at the Group Policy level.

Related Articles:

[Add Windows server for RDP via browser](#)

[Could not Start Ezeelogin RDP proxy](#)

Online URL:

https://www.ezeelogin.com/kb/article/node_rdp_protocol_x224_neg_failure-40;-41;-184.html