REPORT
Troubleshooting Remote Access and Network Isolation

v1.0.0

Author:

Eldon Gabriel

January 16, 2026

TABLE OF CONTENTS

REVISION HISTORY

Version	Date	Author	Description of Changes
v1.0.0	01/16/2026	Eldon G.	Initial draft.

EXECUTIVE SUMMARY

Project Description

This report explains how I resolved ongoing issues with the Remote Desktop Protocol (RDP) between a macOS computer and a Windows virtual machine (VM). I switched from an unstable network setup to a more reliable one. I also resolved issues with login and Group Policy settings to create a working system with Internet access.

SECTION 1.0: PHASE I – NETWORK INFRASTRUCTURE STABILIZATION

1.1 Initial State

The VM is configured with a **Bridged Adapter**. Connection attempts failed because of VPN interference and Wi-Fi signal drops on the host machine.

1.2 Action Taken

I pivoted the network architecture to a **Host-Only Adapter.** Then I configured a static IP range on the virtual interface of the host.

1.3 Results

A consistent, low-latency "Ping" was achieved between the Mac host and the Windows VM (`172.16.20.3`), removing the network layer as a point of failure.

SECTION 2.0: PHASE II – SECURITY POLICY AND AUTHENTICATION REMEDIATION

2.1 Obstacle

After establishing connectivity, the RDP client displayed a "black screen" followed by the error message: *"The user has not been granted the requested logon type at this computer."*

2.2 Troubleshooting Steps

2.2.1 Registry Modification

Network Level Authentication (NLA) was disabled via `PowerShell` by setting `UserAuthentication` to `0`, which accommodates the macOS RDP handshake.

2.2.2 User Rights Assignment

The verified user, `John`, was confirmed as a member of the local **Remote Desktop Users** group. The `gpedit.msc` tool was used to update the **Allow log on through Remote Desktop Services** policy.

2.2.3 Conflict Resolution (Breakthrough)

The root cause was identified when the **Administrators** group was found under the **"Deny log on through Remote Desktop Services"** policy. In Windows, a “Deny” rule overrides all “Allow” permissions.
The **Administrators** group was removed from the Deny policy, and the `gpupdate /force` command was executed to apply the changes.

SECTION 3.0: PHASE III – CONNECTIVITY AND INTERNET RESTORATION

3.1 Final Obstacle

After Remote Desktop access was restored, the Windows virtual machine did not have internet access due to the isolated nature of the Host-Only network configuration.

3.2 Solution Implemented

A dual-homed network configuration was implemented to restore internet access while maintaining secure RDP connectivity.

Adapter 1: Host-Only adapter used for management and Remote Desktop traffic between the host and the virtual machine.

Adapter 2: NAT adapter used to provide outbound internet access for the virtual machine.

3.3 Results

The virtual machine maintained a stable Remote Desktop session while also allowing access to the internet for browser-based research and tool updates.

SECTION 4.0: TECHNICAL FINDINGS AND SKILLS DEMONSTRATED

4.1 Identity and Access Management

Understanding the hierarchy of local groups and user rights assignments, including how explicit "Deny" permissions override "Allow" permissions in Remote Desktop Services.

4.2 Group Policy Management

Using `gpedit.msc` to identify and remediate authentication failures related to Remote Desktop logon policies.

4.3 Network Design

Designing a virtual network architecture that balances isolation and functionality using multiple network adapters.

4.4 Troubleshooting Methodology

Applying a structured troubleshooting approach by progressing from network connectivity issues to application-level authentication problems.

SECTION 5.0: CONCLUSION

5.1 Key Takeaways

The exercise resolved issues with connection, login, and internet access between the macOS host and Windows VM. A secure Remote Desktop Protocol (RDP) setup enabled reliable management and research. The investigation revealed that administrators were incorrectly listed under **"Deny log on through Remote Desktop Services."**

5.2 Security Implications and Recommendations

The identified Group Policy conflict represents a potential security risk, as improper "Deny" and "Allow" rules can prevent legitimate access or expose misconfigurations.

5.2.1 Recommendations

1. Regularly review and audit Group Policy settings to prevent conflicts that block authorized users.
2. Document and version control security policies to track changes and avoid misconfigurations.
3. Maintain dual-homed network designs with a clear separation of management and Internet traffic to reduce network risk.
4. Map these findings to **NIST CSF** best practices for **Access Control (PR.AC)** and **System Configuration (PR.IP)**.
5. Ensure compliance with relevant frameworks, such as **ISO 27001**, for secure system administration and access management.