Windows RDP Lab
By Michael Ambeguia

Purpose: The purpose of this lab is to explore Windows Remote Desktop Protocol in detail and gain hands-on experience configuring it. RDP is widely used in Windows ecosystems for remote administration and technical support and is a vital tool to learn how to use. Understanding the security implications of running RDP is another important consideration as well since like all network services it requires.properly configuring its settings. In this lab I will go over how RDP works, how to configure RDP, and how to secure RDP using Group Policy.

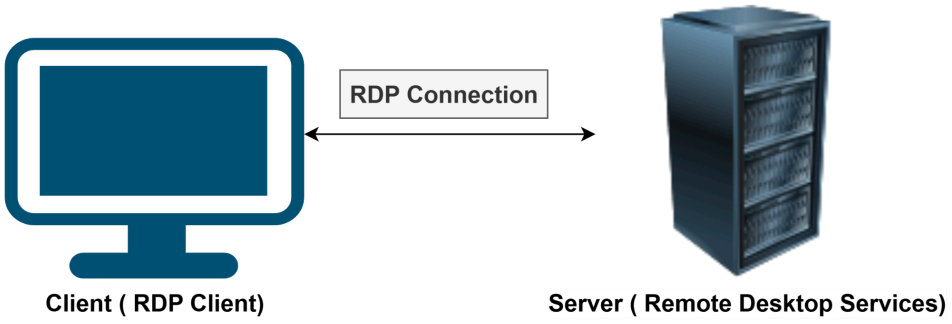
Sections:

1. Introduction to RDP
2. Enabling and Configuring RDP
3. Securing RDP
4. Use RDP

Section #1 Introduction to RDP:

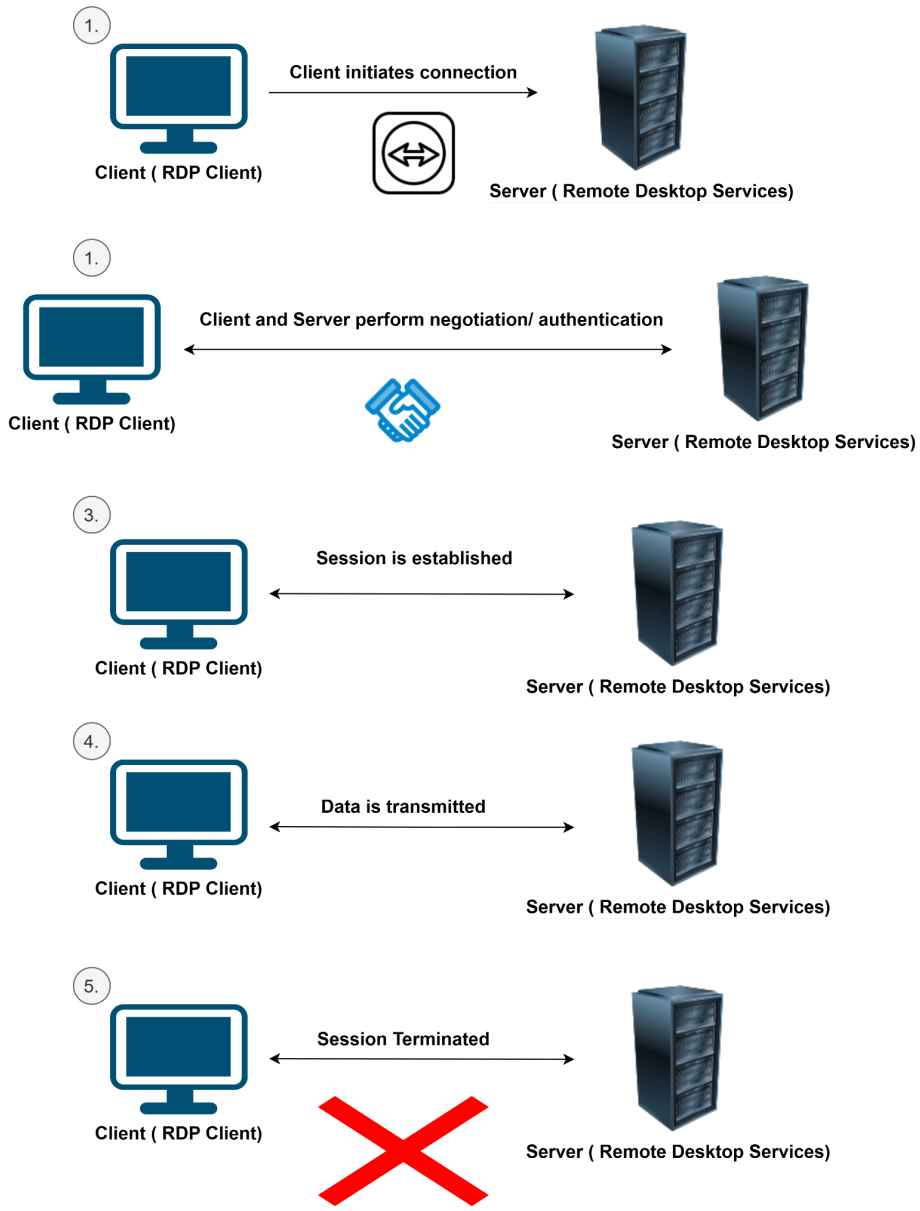
1.1 What is RDP? Why is it used?

RDP (Remote Desktop Protocol) is a network service that allows users to connect to a remote device. The remote connection allows users to get an actual GUI session on the device unlike SSH which mainly only grants a terminal. RDP uses a client/server model with the server being the device that is connected to and the client being the device initiating the connection. It also uses TCP as the layer 4 protocol since a session has to be established, the order of the data packets is vital for RDP functionality, and RDP requires all packets to reach the destination.



RDP is mainly used to administer remote Windows devices and to provide technical support remotely. By providing a GUI interface, administering remote Windows devices and providing technical support is simplified with RDP.

1.2 How does RDP work?



Step #1. The client initiates a connection to the RDP server. This connection typically occurs over TCP port 3389.

Step #2. The RDP client and server perform a negotiation for authentication methods and security settings. For instance, a common authentication negotiation would be if RDP should use network credentials (AD credentials) or local credentials for authentication. For security settings the client and server will need to establish which encryption algorithms will be used to secure the data in transit.

Step #3. Once the negotiation is over and the client user is authenticated a session is started so a connection to the remote device is established.

Step #4. In this step the client will have access to GUI for the remote system. The client user can manipulate the GUI. The cursor movements, clicks, and keyboard input is sent to the RDP server over the network and performed on the remote system.

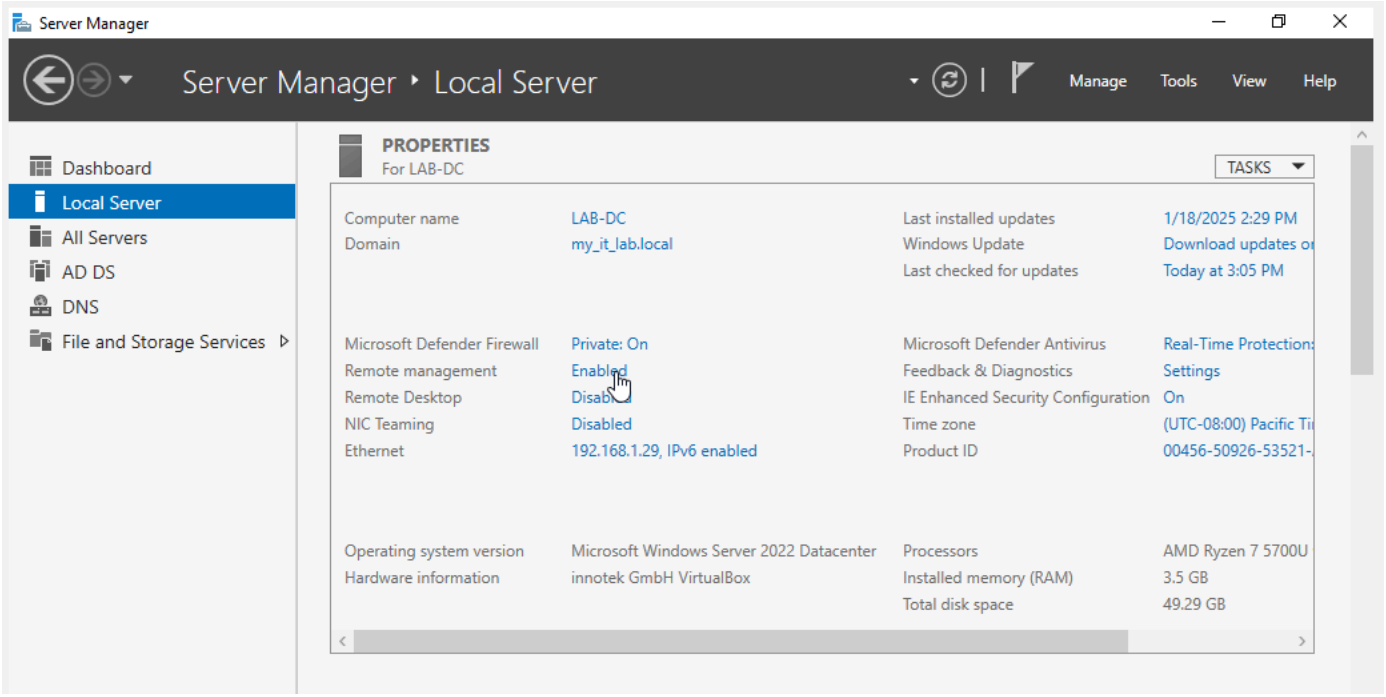
Step #5. Once the client user performs their tasks on the remote system they can end the session.

Section #2 Enabling and Configuring RDP:

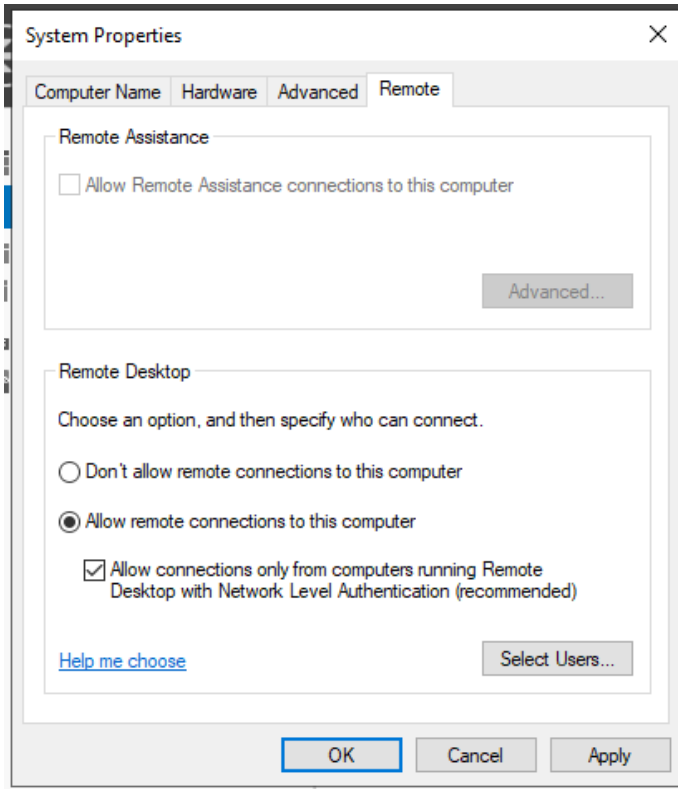
Note: ***RDP configurations happen on the device you want to connect to (server-side) and not the client you are using RDP client on!*** For this lab I will be setting up RDP on a Windows Server 2022 system.

2.1 Verify that RDP is enabled:

On a Windows Server system you can check if RDP is enabled via the Server Manager utility.



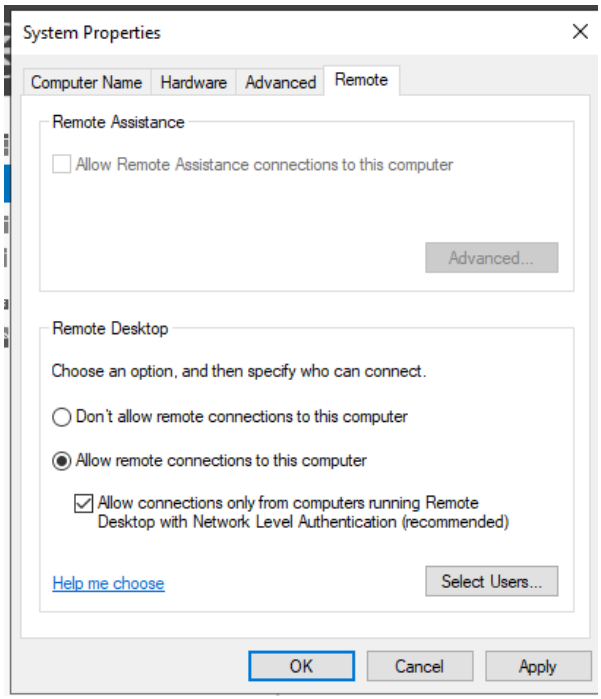
RDP is disabled currently so I need to enable it. I clicked on the allow button and also chose to only allow Network Level Authentication (Kerberos) for RDP connections.



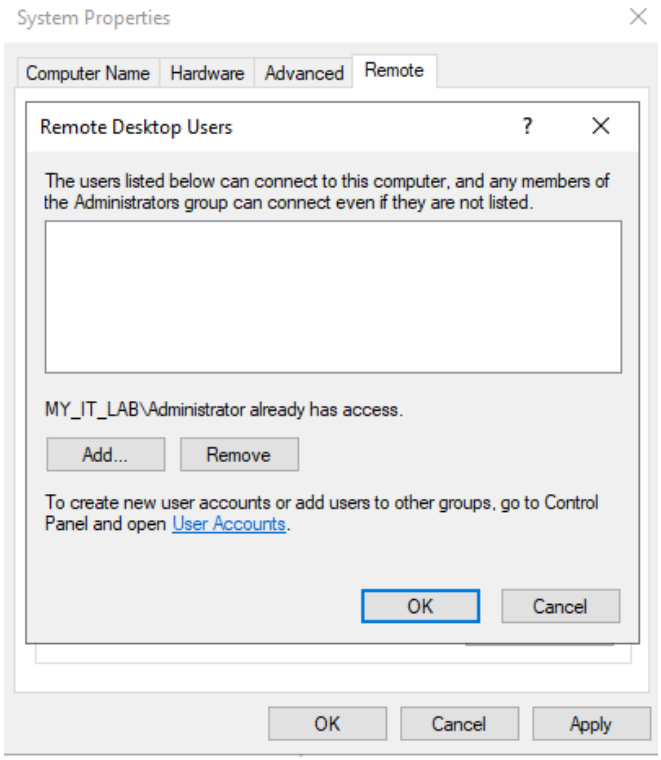
2.2 Allow a specific user to use RDP:

RDP permissions are linked to a user's security group membership. Mainly users in the Administrator group can perform RDP connections.

1. Go to the Remote section

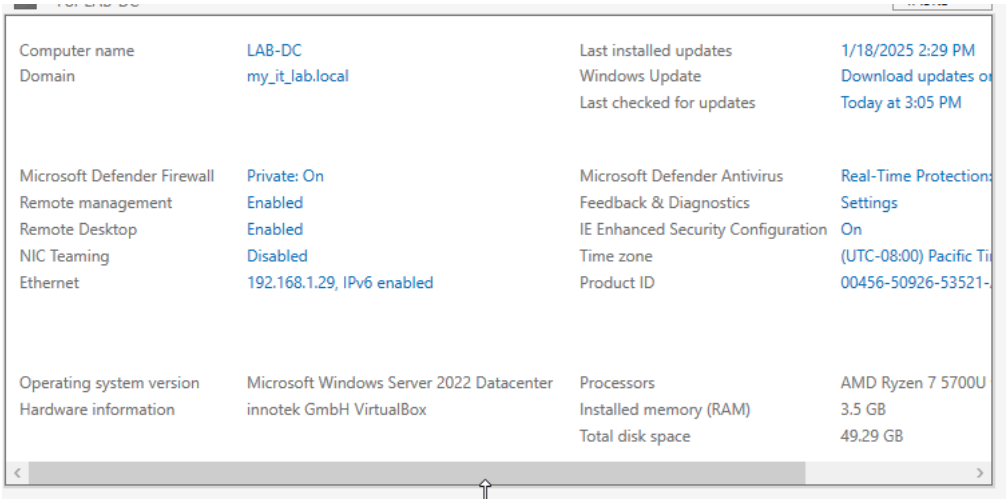


2. Now click select users



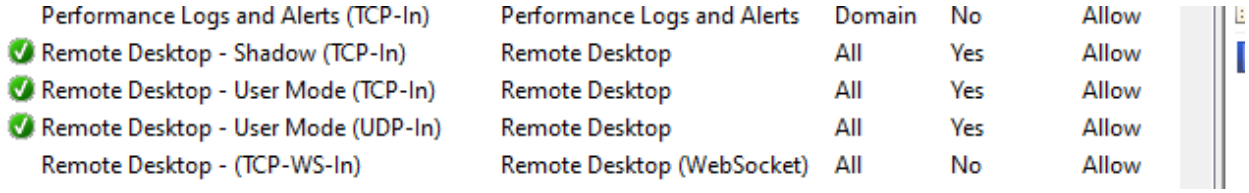
The Administrator account (the domain admin account) has permissions to connect to the server via RDP since it is in the Administrators group. I will just use this account for the purposes of the lab. If I wanted another user to use RDP they would need to be a member of the Administrators group and added to the list shown above.

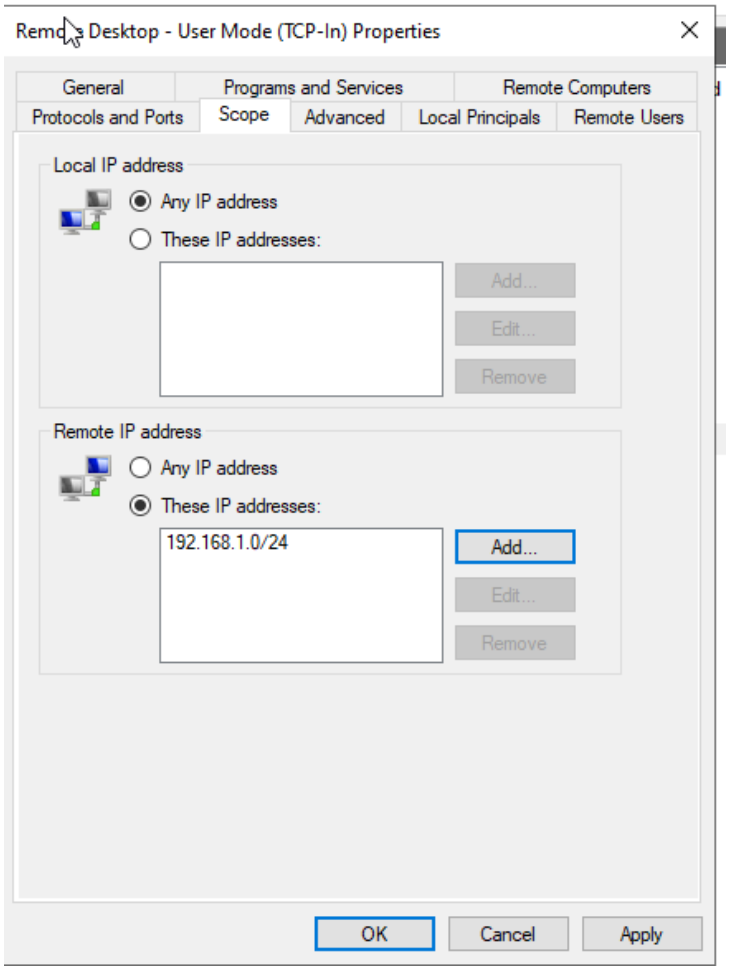
Now just click ok a couple of times then apply. RDP is now enabled on the Windows Server system:



Section #3 Securing RDP:

3.1 Configure the firewall on the device to only allow access to RDP from the local network:



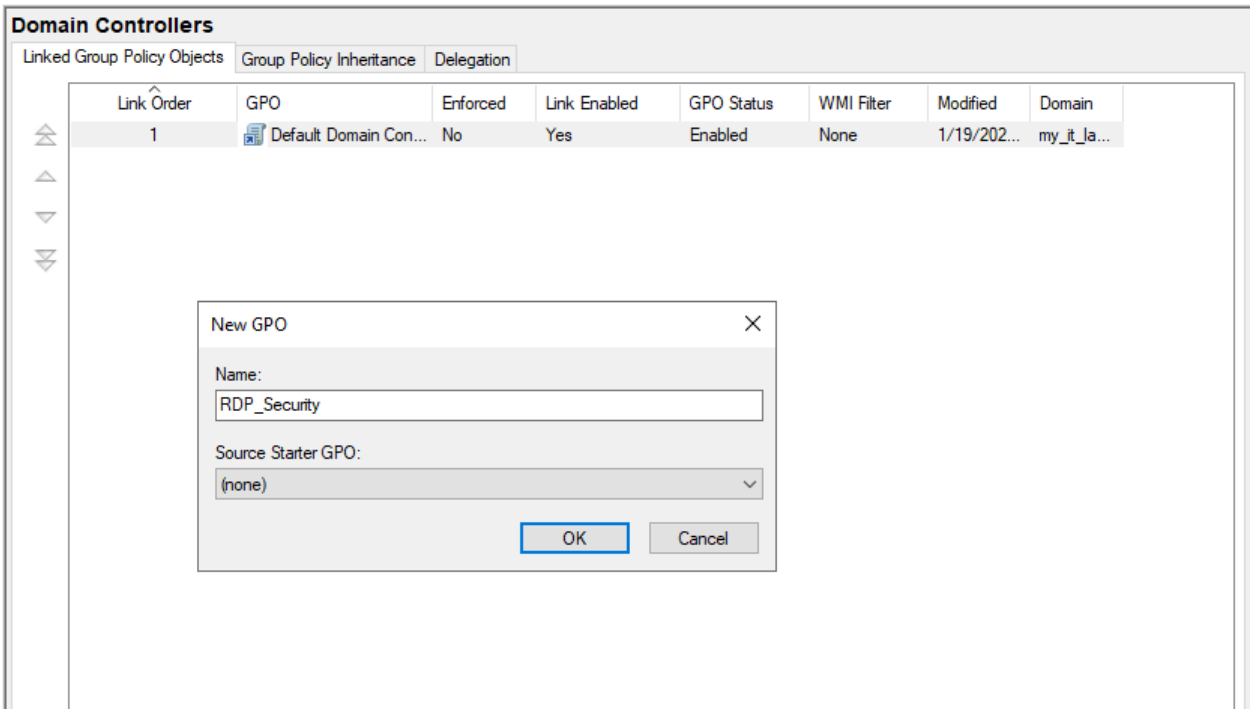


Now only devices on my local network can attempt to connect to the Server via RDP. It is a smart idea to limit the possible network traffic that can reach the server by using firewall rules. I don't want devices on a remote network to have the ability to attempt to connect to the Windows Server via RDP.

3.2 Create a GPO for the Domain Controllers OU:
The Windows Server I am using in this lab is a DC so it is in the DC OU. I will apply a RDP_Security GPO to the OU to harden RDP.

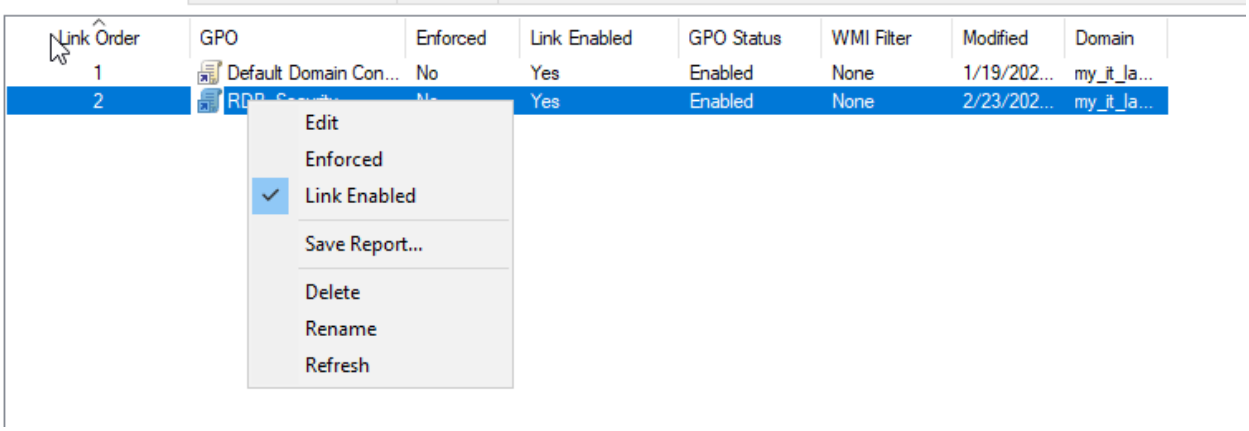
1. Create the RDP_Security GPO

New Group Policy Objects can be created with the GPO management console.



I created a new RDP_Security GPO that will be applied to the Domain Controllers OU.

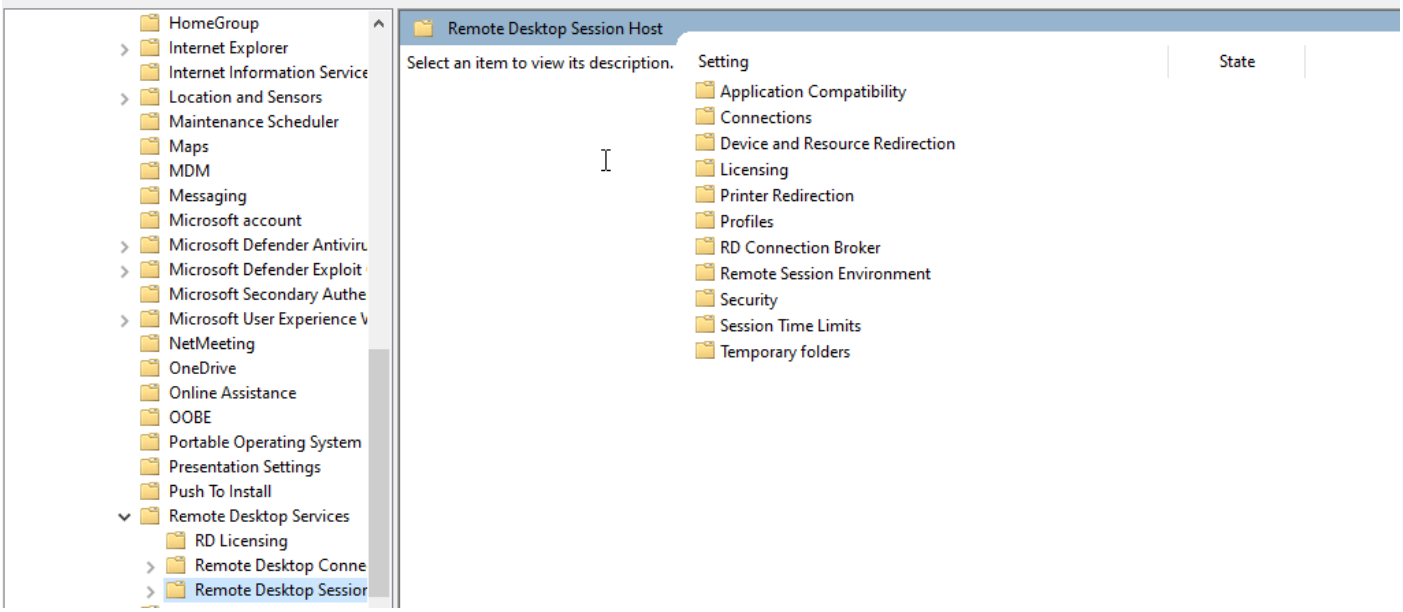
2. Edit the RDP_Security GPO



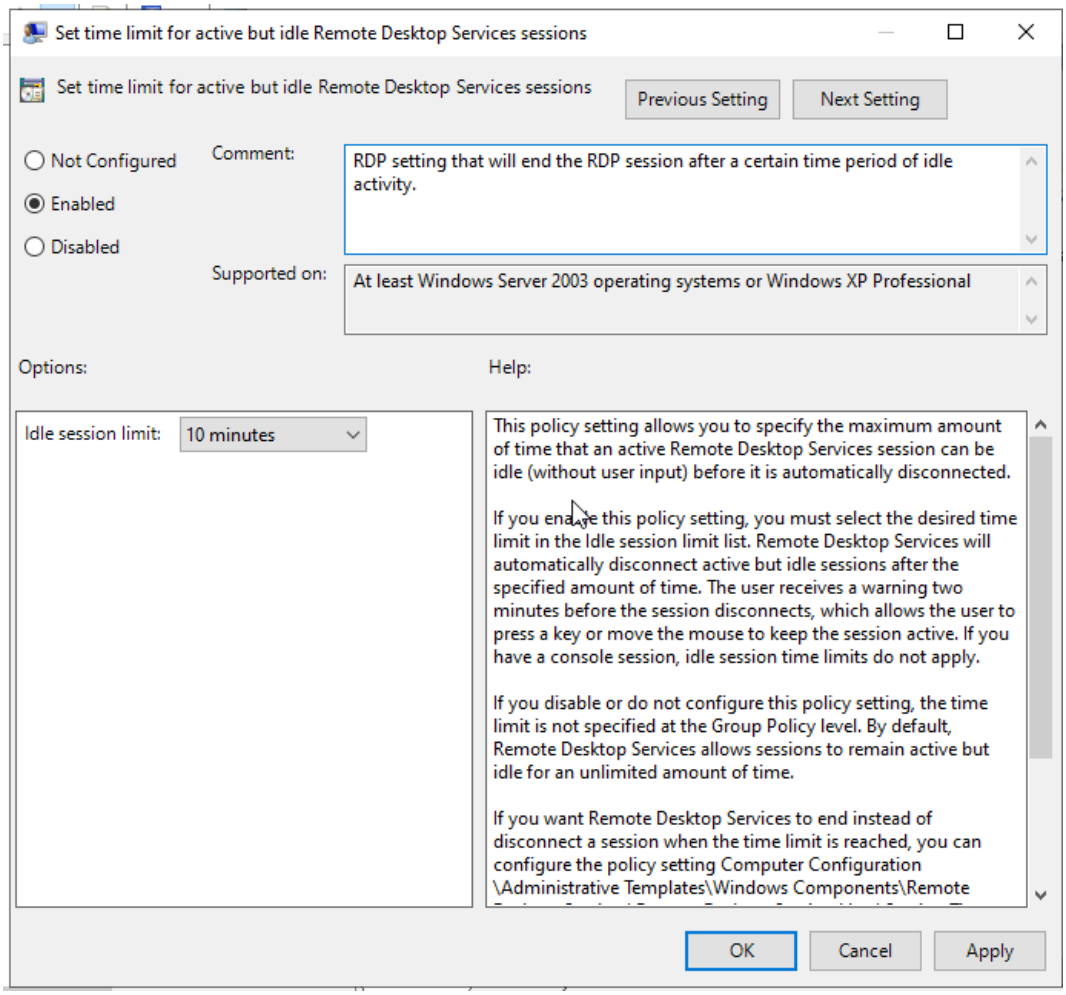
Once a GPO is created you can configure its settings by editing it.

3. Go to the Computer Configurations/Admin Templates/Windows Components/Remote Desktop Services/Remote Desktop Session Host:

RDP GPOs are found under the Remote Desktop Session Host folder.

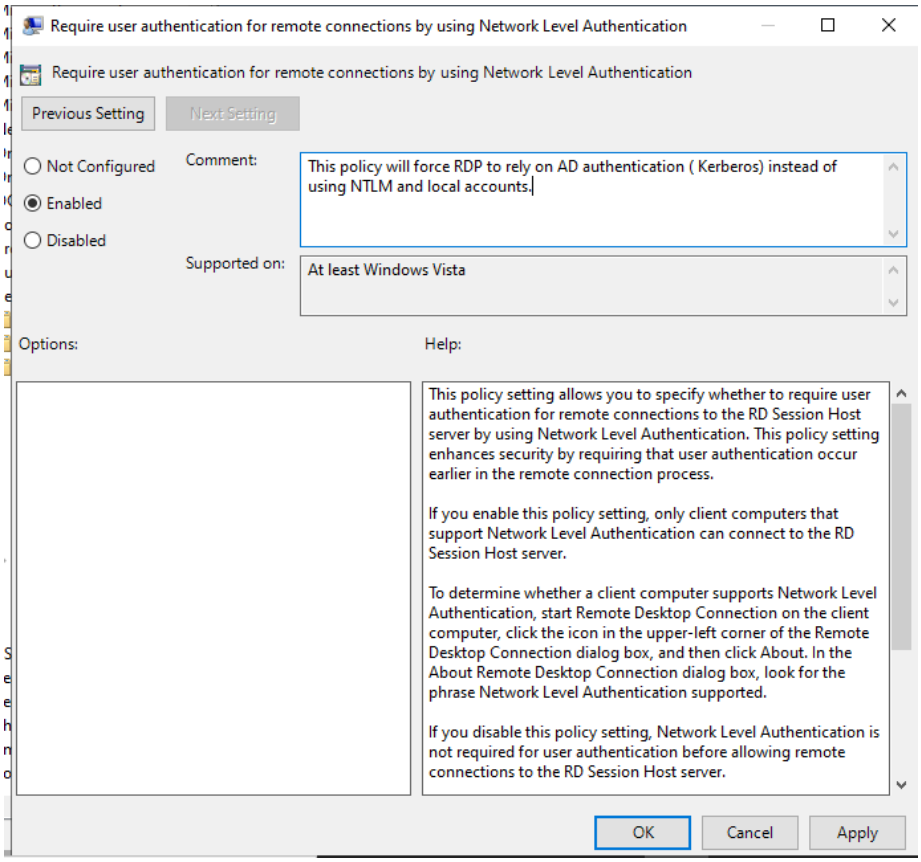


4. Configure the Session Time Limits:



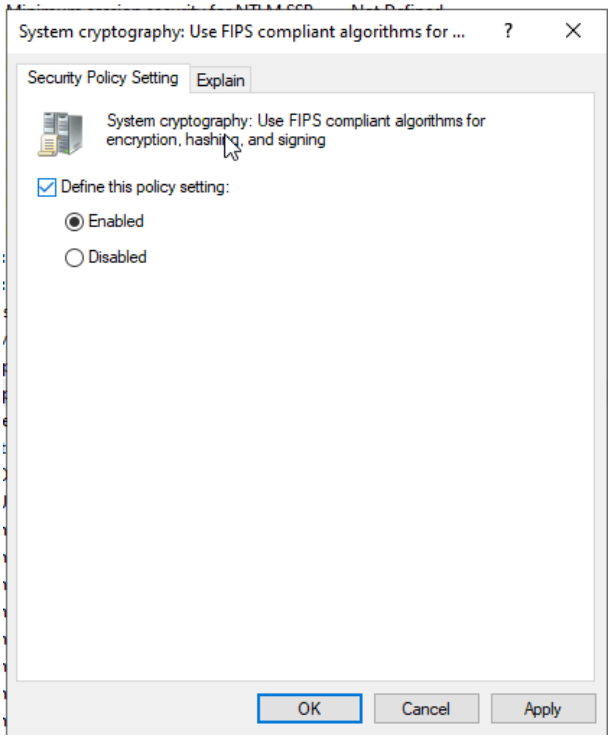
Limiting the session times for idle RDP sessions can reduce the risks of an open session being hijacked or someone gaining access to the physical client device and connecting to the server via an open session. This setting is similar to locking a PC or smartphone screen in that no random attackers can access the session if the actual user steps away for a moment. So by setting the idle session time to 10 minutes, after 10 minutes of idle time the RDP session will end.

5. Requiring authentication to use Network Level Authentication



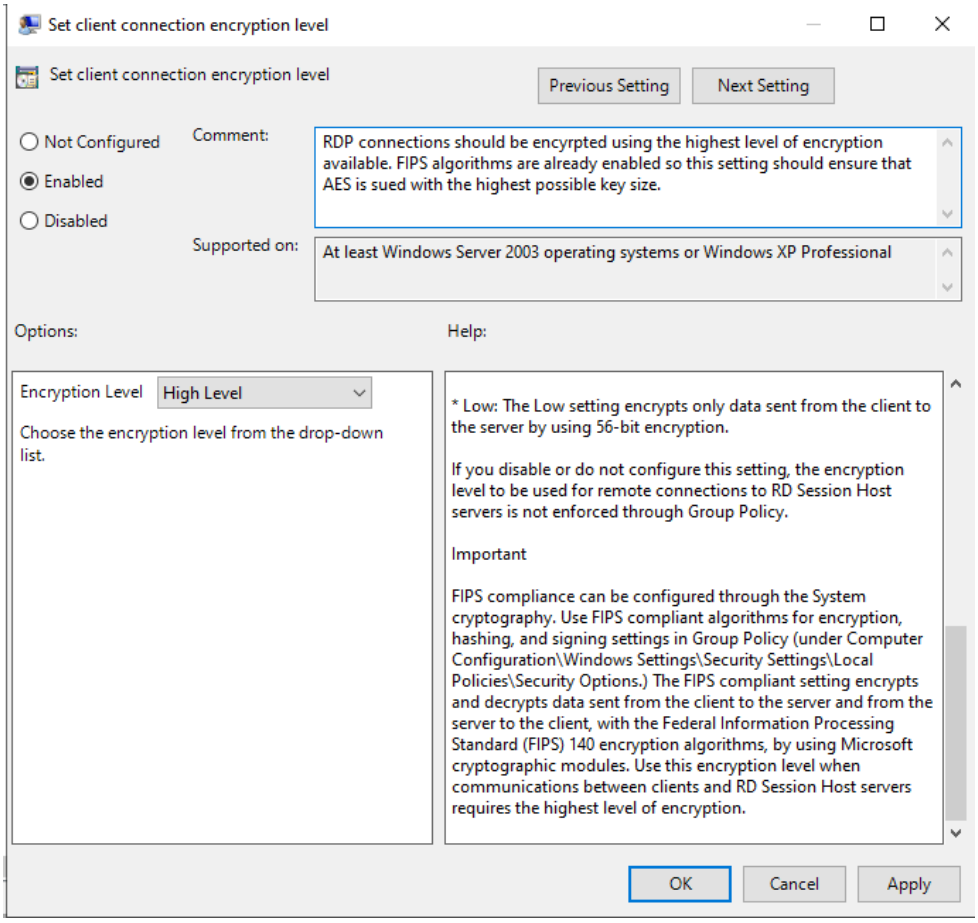
By forcing RDP connections to the RDP server to use NLA (Kerberos) the authentication process can be secured. Unlike regular NTLM authentication which actually sends the password across the network risking man in the middle, relay, and brute force attacks, Kerberos never sends a users' credentials across the network making such attacks ineffective. Even if Kerberos is used, passwords should still be long, random, and complex.

6. Enable fips compliant cryptography algorithms:



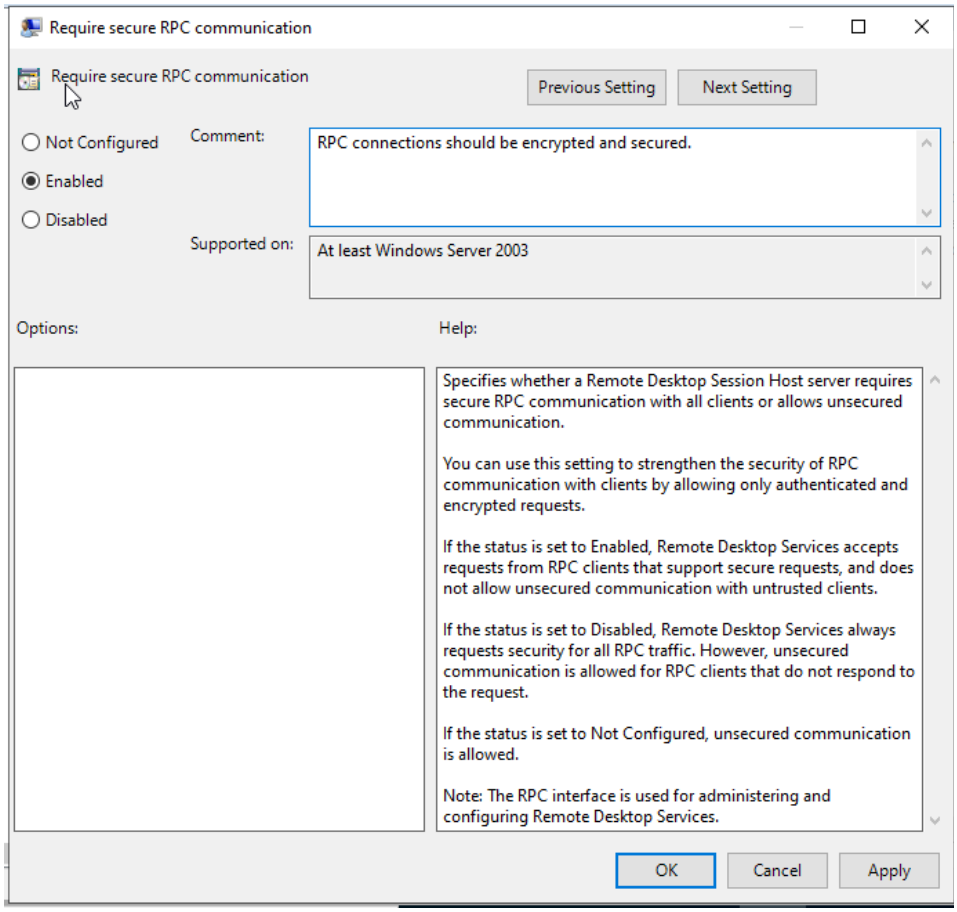
Enabling FIPS compliant algorithms will allow the device to use the strongest federal government validated and approved cryptographic algorithms. Using the strongest cryptographic algorithms ensures that data will be protected on the system and attackers won't be able to find weaknesses in the algorithms to exploit.

7. Configure RDP to use the highest level of encryption:



Now that FIPS algorithms are enabled, I forced RDP to use the highest level of encryption available on the system (FIPS). This will make the data in transit for RDP more secure. The strongest FIPS algorithm used is AES 128.

8. Configure RDP to only allow secure RPC:



Securing RDP to only allow RPC communications that are authenticated and encrypted is another hardening method. This technique is mainly used to prevent man in the middle attacks and the manipulation of RDP traffic.

Now that the GPO has been edited with the settings I want I can now verify that the GPO is applied:

```
C:\Users\Administrator>GPRESULT /R /SCOPE COMPUTER

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© Microsoft Corporation. All rights reserved.

Created on  2/ 23/ 2025 at 4:25:20 PM


RSOP data for  on LAB-DC : Logging Mode
---------------------------------------

OS Configuration:            Primary Domain Controller
OS Version:                  10.0.20348
Site Name:                   Default-First-Site-Name
Roaming Profile:
Local Profile:
Connected over a slow link?: No


COMPUTER SETTINGS
------------------
    CN=LAB-DC,OU=Domain Controllers,DC=my_it_lab,DC=local
    Last time Group Policy was applied: 2/23/2025 at 4:24:48 PM
    Group Policy was applied from:      LAB-DC.my_it_lab.local
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        MY_IT_LAB
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    -----------------------------
        Default Domain Controllers Policy
        RDP_Security
        Default Domain Policy

    The following GPOs were not applied because they were filtered out
    -------------------------------------------------------------------
        Local Group Policy
```

The LAB-DC server has the RDP_Security GPO applied. I used the GPRESULT commandlet to verify this.

Section #4 Use RDP:

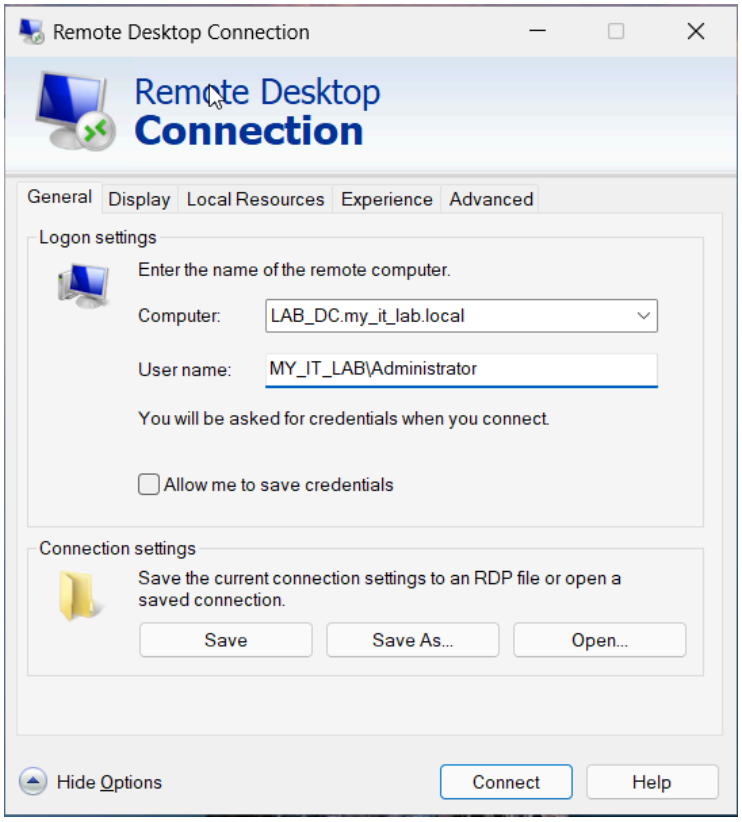
4.1 Sign in using the account with RDP permissions on the client device:

I signed into the client PC using the domain admin user account. This user has permissions to connect via RDP to the server.

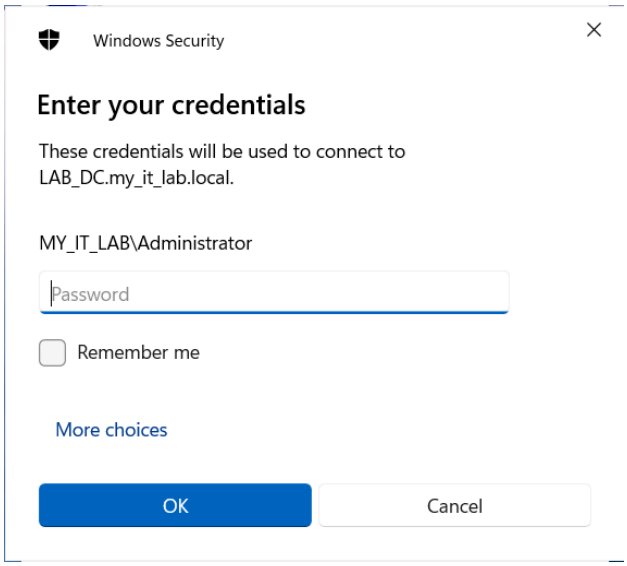
```
Microsoft Windows [Version 10.0.26100.1742]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>whoami
my_it_lab\administrator

C:\Users\Administrator>
```

4.2 Use the RDP client software to connect to the server:

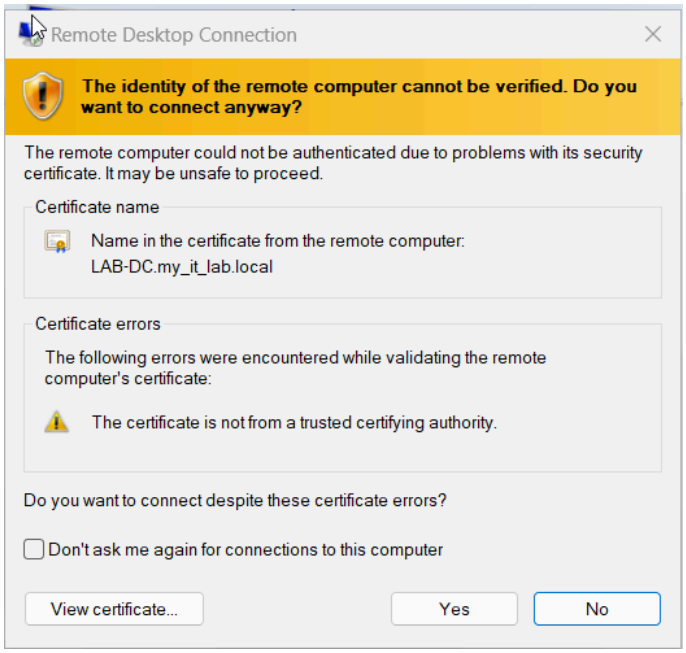
Enter the full AD username for the user.



The user is then prompted to enter their AD credentials.



There is a warning about the identity of the remote computer. This is because my client and server devices don't have any PKI certificates to establish a trust relationship. I won't worry about configuring this right now since it is not required and only adds a layer of integrity and authenticity to the RDP connection. I am confident that the device I am connecting to is legitimate.



I am in! I have access to the Domain Controller remotely! I can administer it remotely now.