**Zack Pelka**

Configure Windows Locally and in a GPO for NLA RDP / Network Level Authentication for Remote Desktop (RDP)

|  |  |
| --- | --- |
| Prepared By: | Zachary Pelka |
| Document Version: | 1.1 |
| Last Updated On: | 8JAN2021 |
| Document Classification: | Public Domain |

The information in the document may contain proprietary and confidential information that is intended for the employees of ZP Enterprises only. If you are not an employee of ZP Enterprises, you are hereby notified that any disclosure, copying, distribution, retention, or use of the contents of this information is prohibited in an altered form. This is for public use without modification.

## **Purpose**

This article gives the steps to lock down Remote Desktop Protocol (RDP) and to create an Active Directory Group Policy (GPO) to force the use of NTLM authentication. NLA was introduced first with RDP 6.0 in Windows Vista and later on Windows XP SP3.

One of the biggest advantages also is that since TLS is used it will warn us if it can not validate the identity of the host we are connecting to. For this, we will need a PKI infrastructure integrated with AD in our Windows environment. On a Windows 2008 environment, we can install on a server the role of Active Directory Certificate Service to install an Enterprise CA accepting all defaults so it can provide Computer Certificates to the machines in the domain in an automated way using Group Policy.

When you enable this option, users have to authenticate themselves to the network before they can connect to your PC. Allowing connections only from computers running Remote Desktop with NLA is a more secure authentication method that can help protect your computer from malicious users and software. To learn more about NLA and Remote Desktop, check out [Configure NLA for RDS Connections](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11)).

**Pay special attention to the impact of the changes in the “disadvantages” section.**

Exploits

The BlueKeep vulnerability ([**CVE-2019-0708**](https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708))

[CVE-2019-9510](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9510)

Advantages

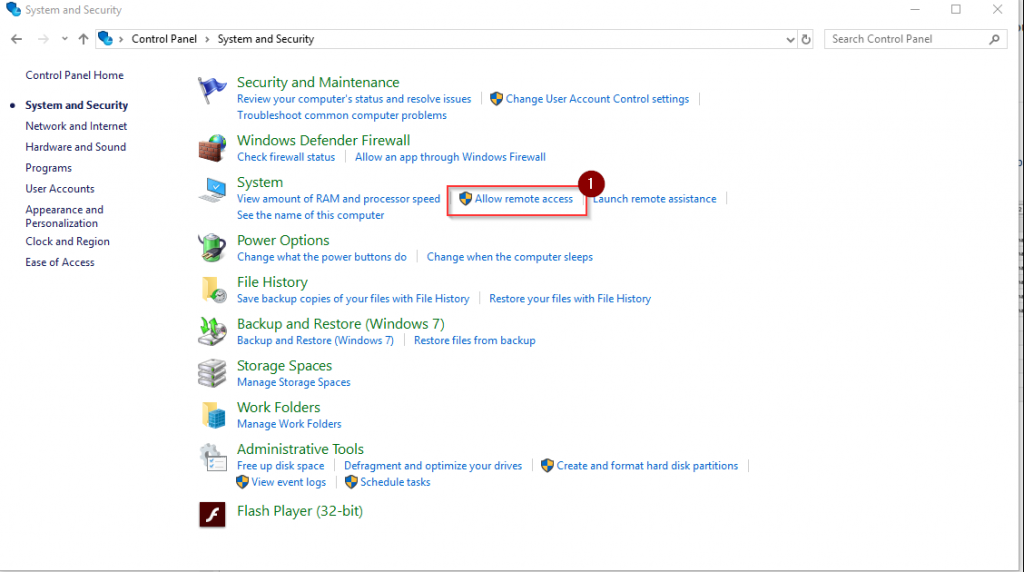
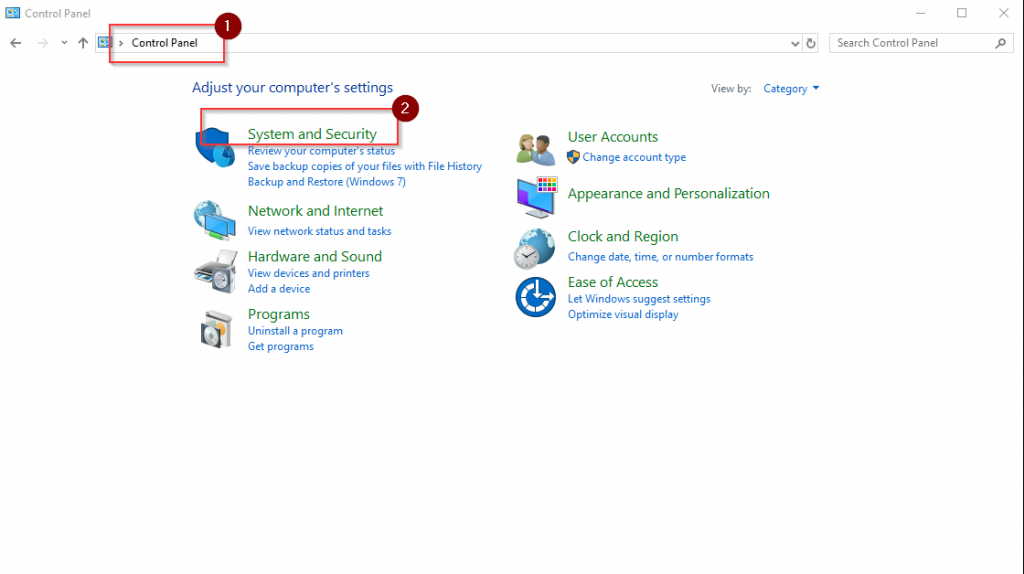
* It requires fewer [remote computer](https://en.wikipedia.org/wiki/Remote_computer) resources initially, by preventing the initiation of a full [remote desktop connection](https://en.wikipedia.org/wiki/Terminal_Services) until the user is authenticated, reducing the risk of denial-of-service attacks.
* It allows NT [Single sign-on](https://en.wikipedia.org/wiki/Single_sign-on) (SSO) to extend to [Remote Desktop Services](https://en.wikipedia.org/wiki/Remote_Desktop_Services).
* It can help mitigate Remote Desktop vulnerabilities that can only be exploited before authentication. [[3]](https://en.wikipedia.org/wiki/Network_Level_Authentication#cite_note-3)

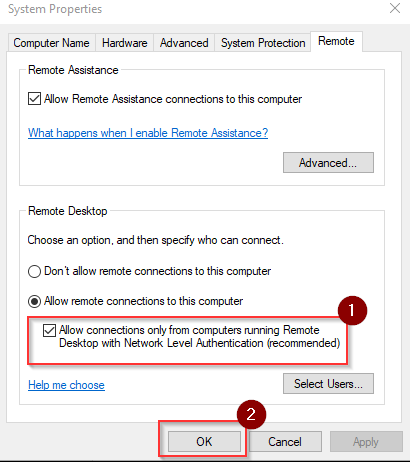
Disadvantages

* No support for other credential providers
* To use Network Level Authentication in Remote Desktop Services, the client must be running Windows XP SP3 or later, and the host must be running Windows Vista or later [[4]](https://en.wikipedia.org/wiki/Network_Level_Authentication#cite_note-4) or Windows Server 2008 or later.
* Support for RDP Servers requiring Network Level Authentication needs to be configured via registry keys for use on Windows XP SP3.
* Not possible to change a password via CredSSP. This is a problem when "User must change password at next logon" is enabled or if an account's password expires.
* Requires "Access this computer from the network" privilege, which may be restricted for other reasons.
* The IP addresses of the clients trying to log in will not be stored in the security audit logs, making it harder to block brute force or dictionary attacks employing a firewall.
* Smart card authentication from one domain to another using a remote desktop gateway is not supported with NLA enabled on the end client.

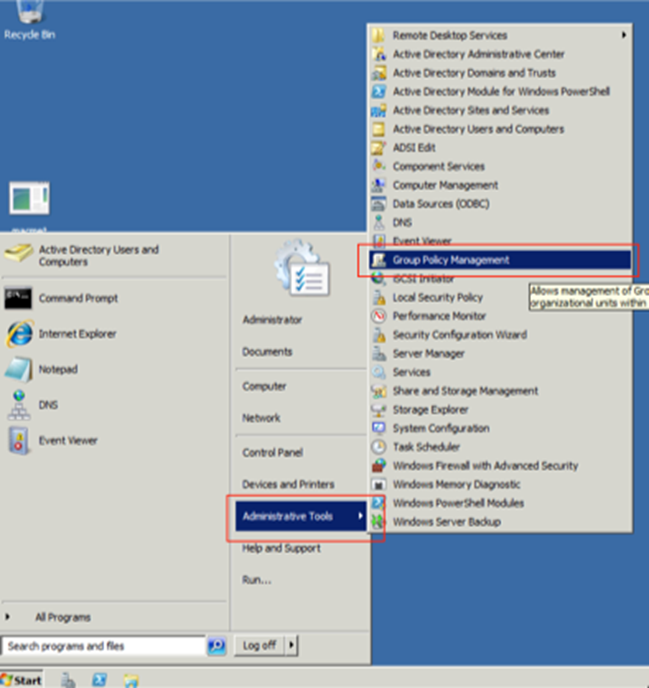
## **Local / Manual Configuration**

**To configure locally, navigate to:**



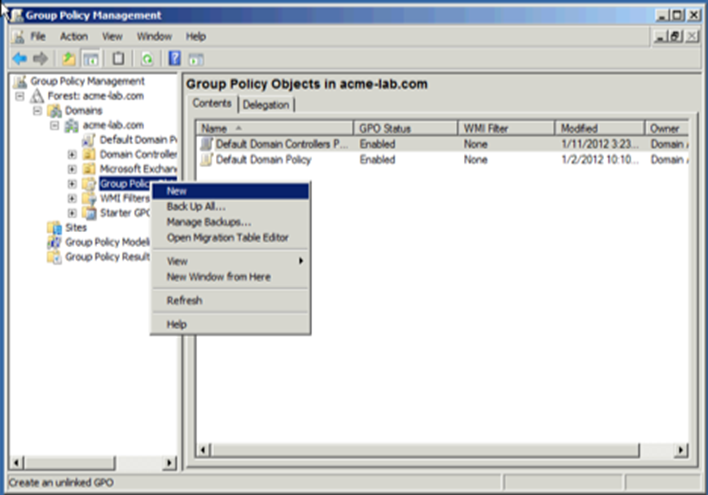


**To configure in the group policy editor:**



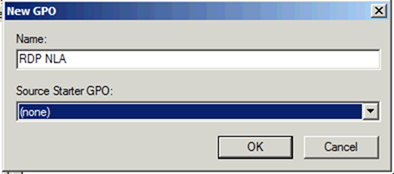
## **Create the GPO and its location**

Before you begin, create a new GPO at the Domain level:

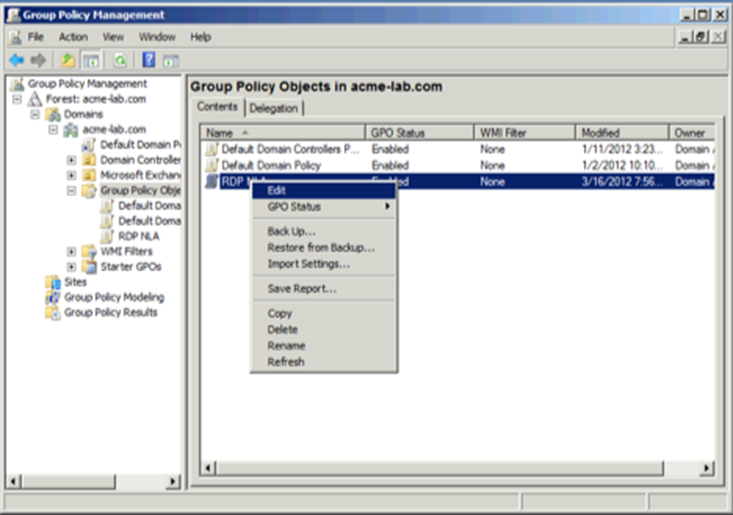


**Now create the new GPO:**

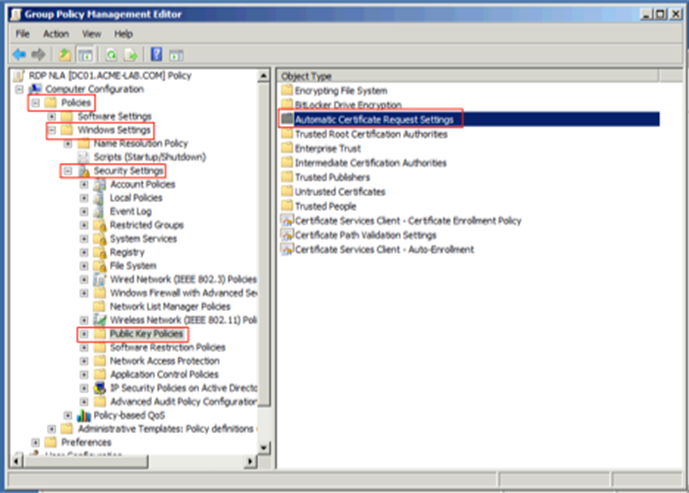
We give this policy a Name:

[](https://static.squarespace.com/static/52ad1d91e4b00a98a27ba20e/52ae5168e4b0988b43f4361f/52ae5169e4b0988b43f43abe/1331998090903/Windows-Live-Writer-Configuring-y_948B-)

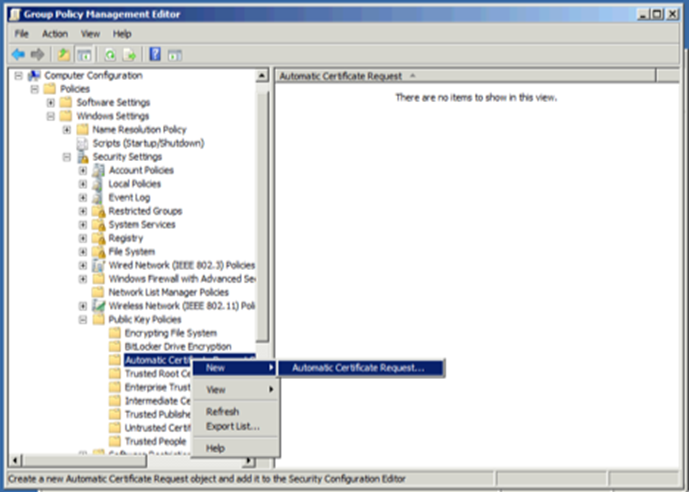
Once created we edit this policy by right-clicking on it and selecting Edit:

[](https://static.squarespace.com/static/52ad1d91e4b00a98a27ba20e/52ae5168e4b0988b43f4361f/52ae5169e4b0988b43f43ac0/1331998094707/Windows-Live-Writer-Configuring-y_948B-)

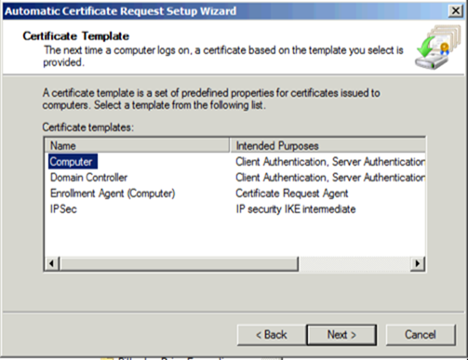
Now we select **Computer Configuration/Policies/Windows Settings/Public Key Policies/Automatic Certificate Request Settings**:

[](https://static.squarespace.com/static/52ad1d91e4b00a98a27ba20e/52ae5168e4b0988b43f4361f/52ae5169e4b0988b43f43ac2/1331998104437/Windows-Live-Writer-Configuring-y_948B-)

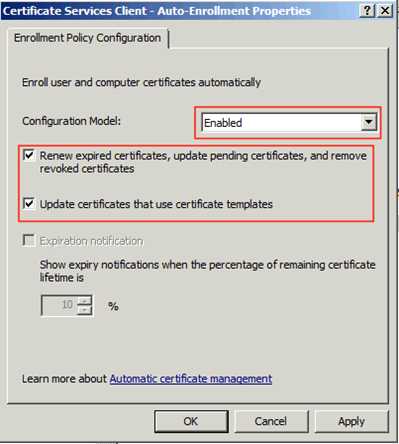
We now right-click on **Automatic Certificate Request Setting** and select to create a new **Automatic Certificate Request**, this will request to the CA a new Computer Certificate and renew the certificate when it expires automatically.

[](https://static.squarespace.com/static/52ad1d91e4b00a98a27ba20e/52ae5168e4b0988b43f4361f/52ae5169e4b0988b43f43ac4/1331998114187/Windows-Live-Writer-Configuring-y_948B-)

When the wizard starts we click **Next** then we select **Computer** Certificate Template:

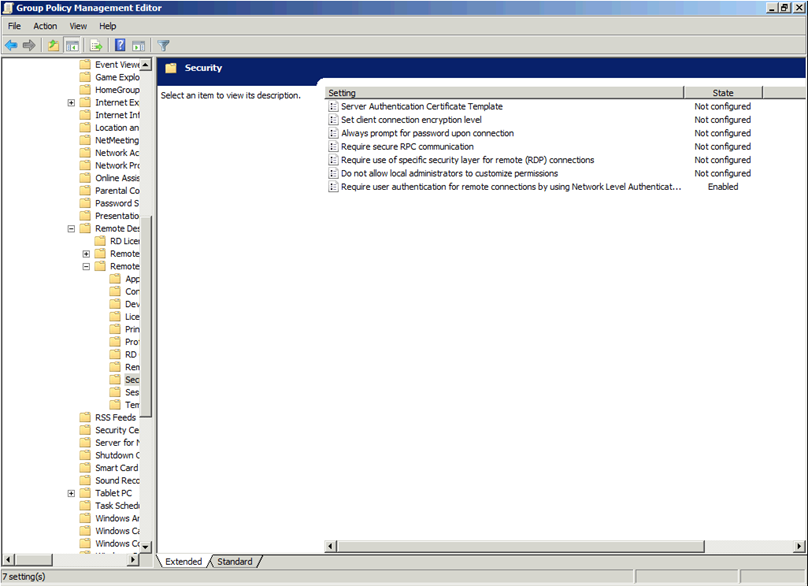
[](https://static.squarespace.com/static/52ad1d91e4b00a98a27ba20e/52ae5168e4b0988b43f4361f/52ae5169e4b0988b43f43ac6/1331998123008/Windows-Live-Writer-Configuring-y_948B-)

We click on **Next** and then on **Finish**. Now we select **Computer Configuration/Policies/Windows Settings/Public Key Policies**under that node we double click on **Certificate Services Client – Auto-Enrollment** we now select on the properties under Configuration Model we select Enable and make sure that the boxes for managing certificates in the store and for updating the certificate if the template is modified.

[](https://static.squarespace.com/static/52ad1d91e4b00a98a27ba20e/52ae5168e4b0988b43f4361f/52ae5169e4b0988b43f43ac8/1331998127035/Windows-Live-Writer-Configuring-y_948B-)

Now we have finished the section that will cover the certificate assignment for computers that get this GPO applied to.

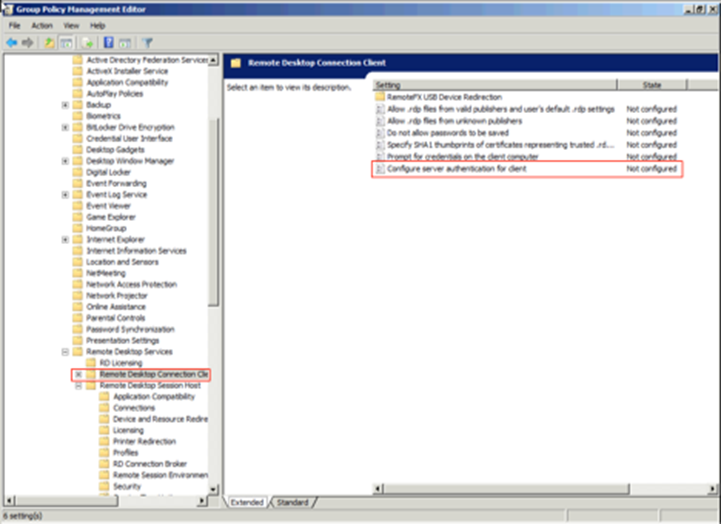
For configuring RDP to use NLA we now go to **Computer Configuration/Policies/Administrative Templates/Windows Components/Remote Desktop Settings/Remote Desktop Session Host/Security.** This GPO Tree Expansion is too large to include a screenshot, so please follow the navigation in bold just above.

[](https://static.squarespace.com/static/52ad1d91e4b00a98a27ba20e/52ae5168e4b0988b43f4361f/52ae5169e4b0988b43f43aca/1331998136047/Windows-Live-Writer-Configuring-y_948B-)

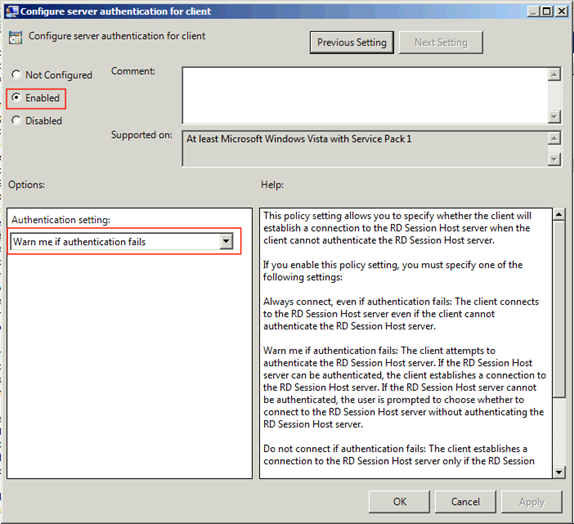
Select **Require user authentication for remote connections by using Network Level Authentication** and double click on it. On the properties screen select **Enable**and click on**OK.**

Now let's configure the client settings to make sure that we always select to warn in the case the host certificate can not be authenticated. We select **Computer Configuration/Policies/Administrative Templates/Windows Components/Remote Desktop Settings/Remote Desktop Connection Client.** This is just above the branch we just navigated to.

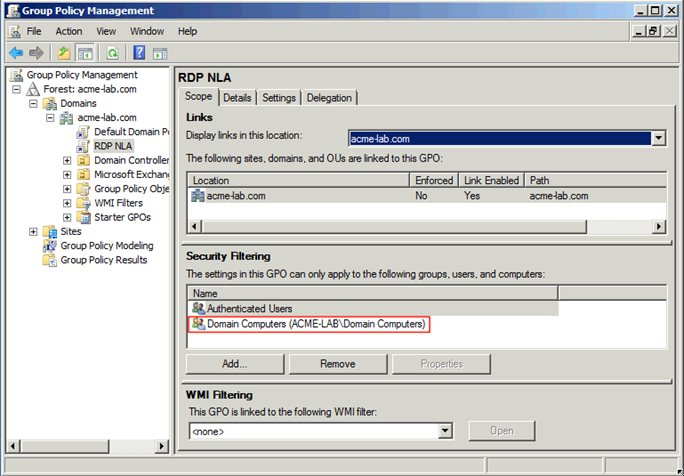
We double click on **Configure Authentication for Client**

[](https://static.squarespace.com/static/52ad1d91e4b00a98a27ba20e/52ae5168e4b0988b43f4361f/52ae5169e4b0988b43f43acc/1331998143893/Windows-Live-Writer-Configuring-y_948B-)

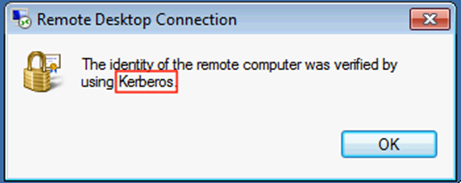
Select **Enable** and set the Option to **Warn me if authentication fails**

[](https://static.squarespace.com/static/52ad1d91e4b00a98a27ba20e/52ae5168e4b0988b43f4361f/52ae5169e4b0988b43f43ace/1331998151707/Windows-Live-Writer-Configuring-y_948B-)

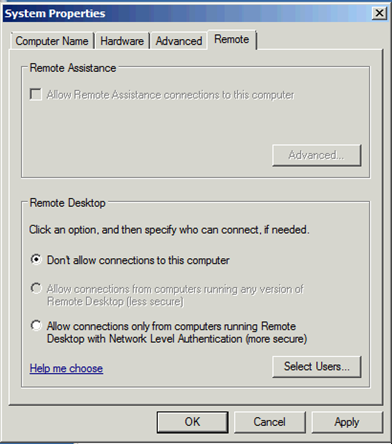
Click on **OK** and close the screen. Know you should have a proper policy that can be applied, but before we apply the policy we have to permit the **Domain Computers** group in the domain the permission to apply it:

[](https://static.squarespace.com/static/52ad1d91e4b00a98a27ba20e/52ae5168e4b0988b43f4361f/52ae5169e4b0988b43f43ad0/1331998158263/Windows-Live-Writer-Configuring-y_948B-)

And now we have a GPO that can be linked to any Domain in the forest or Organization Unit. Once applied when a connection is made, we can see the security in use by clicking on the lock on the top of a Remote Desktop Session in Windows and it will tell us how we were authenticated:

[](https://static.squarespace.com/static/52ad1d91e4b00a98a27ba20e/52ae5168e4b0988b43f4361f/52ae5169e4b0988b43f43ad2/1331998163677/Windows-Live-Writer-Configuring-y_948B-)

On those hosts that do not have RDP enabled you will see that the only option available is to use NLA

[](https://static.squarespace.com/static/52ad1d91e4b00a98a27ba20e/52ae5168e4b0988b43f4361f/52ae5169e4b0988b43f43ad4/1331998166113/Windows-Live-Writer-Configuring-y_948B-)

 As always, I hope you find this blog post informative and useful.

## **Sources**

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **By** | **Changes** |
| **1.0** | 7DEC2020 | Zachary Pelka | Initial Draft |
| **1.1** | 8JAN2021 | Zachary Pelka | Updated Document to include local configurations |
|  |  |  |  |