Turning Off Network Level Authentication (NLA)

- Parallels Remote Application Server

This guide describes how to disable **Network Level Authentication** on various versions Windows Server with or without RD Session Host Role.

Windows 10 or Windows Server 2016 and Windows 8 or Windows Server 2012 without RD Session Host Role

Note: These steps do not apply to Windows Server 2012 and 2016 with the RD Session host role.

1. Open the **Control Panel**. Ensure that the control panel is showing items by **Category**. Click on **System and Security** and under System click on **Allow remote access**.

2. Under the **Remote Desktop** group un-tick the checkbox **Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)**.

3. Click **OK**.

Windows Vista or **Windows 7** and **Windows Server 2008** or **Windows Server 2008 R2** without RD Session Host Role.

Note: These steps do not apply to Windows 2008 and Windows 2008 R2 with the RD Session host role.

1. Open the **Control Panel**. Ensure that the Control Panel is showing items by **Category** (i.e. not in Classic View). Click on **System and Security** and under System click on **Allow remote access**

2. Under the **Remote Desktop** group choose **Allow connections from computers running any version of Remote Desktop (less secure)**.

3. Click **OK**.

Windows Server 2016 and Windows Server 2012 with RD Session Host role

1. On the **RD Session Host** server, open the **Server Manager**.
2. Click on **Remote Desktop Services**, then under **Collections** click on the name of the session collection name that you want to modify. Click on **Tasks** and select **Edit Properties**.

3. Under the **Security** tab un-tick the option **Allow connections only from computers running Remote Desktop with Network Level Authentication**. (For maximum compatibility ensure that Security Layer is set to **Negotiate**).

4. If the Allow connections only from computers running Remote Desktop with Network Level Authentication check box is selected and is not enabled, the **Require user authentication for remote connections by using Network Level Authentication Group Policy** setting has been enabled and has been applied to the RD Session Host server.
5. Click **OK**.

Windows 2008 and Windows 2008 R2 with RD Session Host Role

1. On the **RD Session Host** server, open **Remote Desktop Session Host Configuration**. To open Remote Desktop Session Host Configuration, click Start, point to Administrative Tools, point to Remote Desktop Services, and then click Remote Desktop Session Host Configuration.
2. Under **Connections**, right-click the name of the connection, and then click **Properties**.
3. In the **General** tab, un-tick the **Allow connections only from computers running Remote Desktop with Network Level Authentication** check box. (For maximum compatibility ensure that Security Layers are set to **Negotiate**).

4. If the **Allow connections only from computers running Remote Desktop with Network Level Authentication** check box is selected and is not enabled, the **Require user authentication for remote connections by using Network Level Authentication Group Policy** setting has been enabled and has been applied to the RD Session Host server.
5. Click **OK**.

Using Group Policies

Configure policies on Terminal Server:

- Open **gpedit.msc** applet.
    - Navigate to **Computer Configuration -> Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Session Host -> Security**.
    - Enable **Require use of specific security layer for remote (RDP) connections** and select **RDP** as **Security Layer**.
    - Disable **Require user authentication for remote connections by using Network Level Authentication** policy.
    - Reboot Terminal server.
