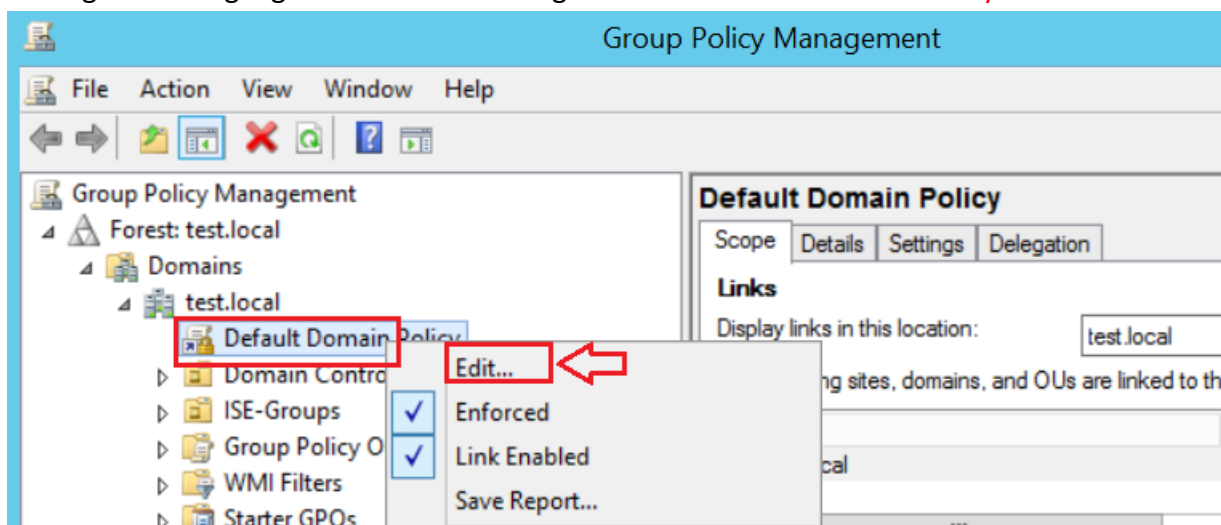
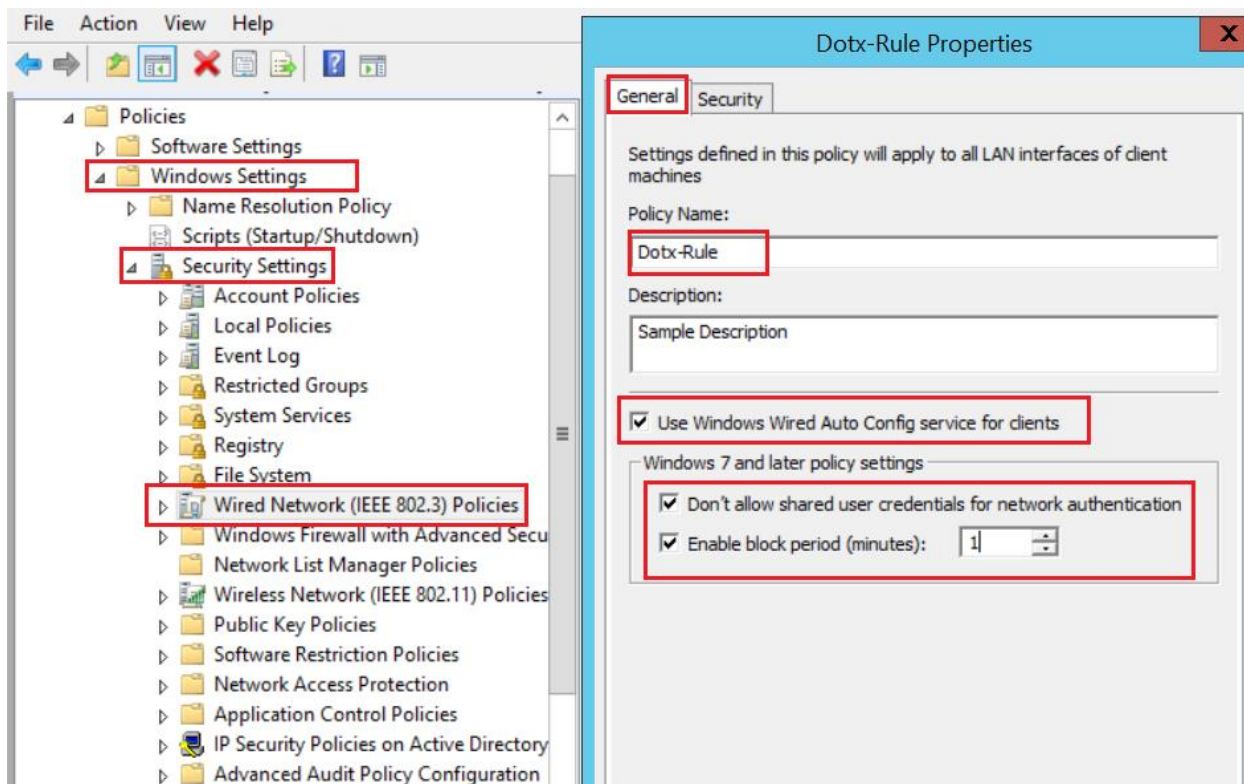


Dot1x Client Group Policy:

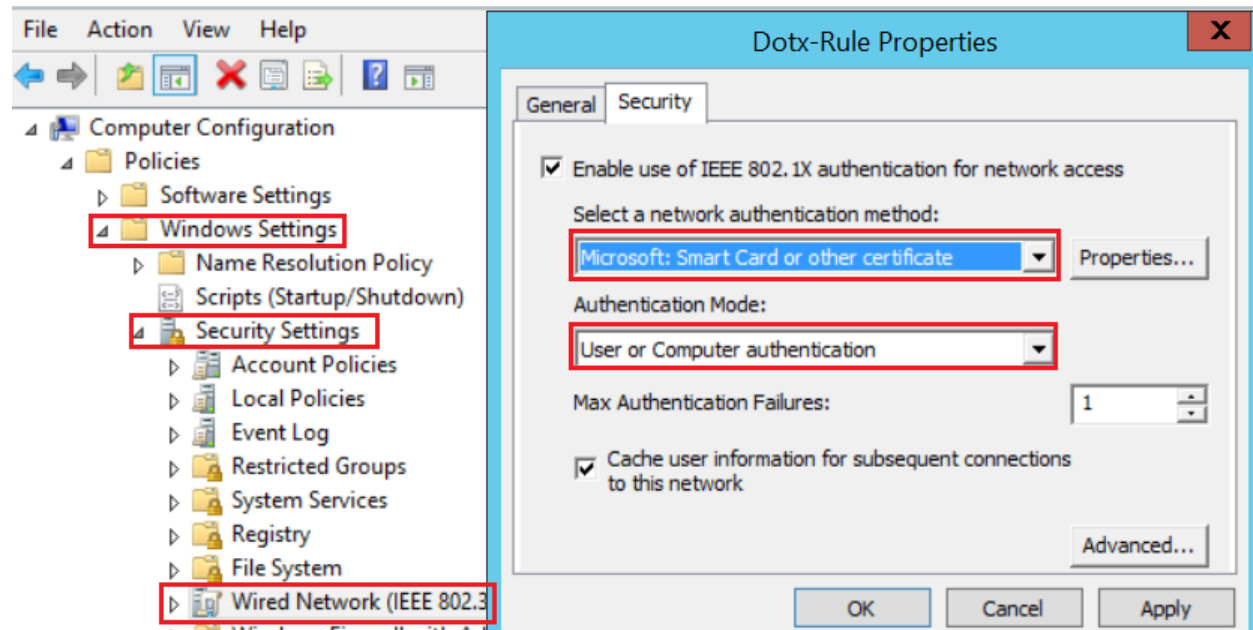
Let's create group policy to push down dot1x settings to clients. Open Group Policy Management. Highlight the domain and right-click on **Default Domain Policy** and click **Edit**.



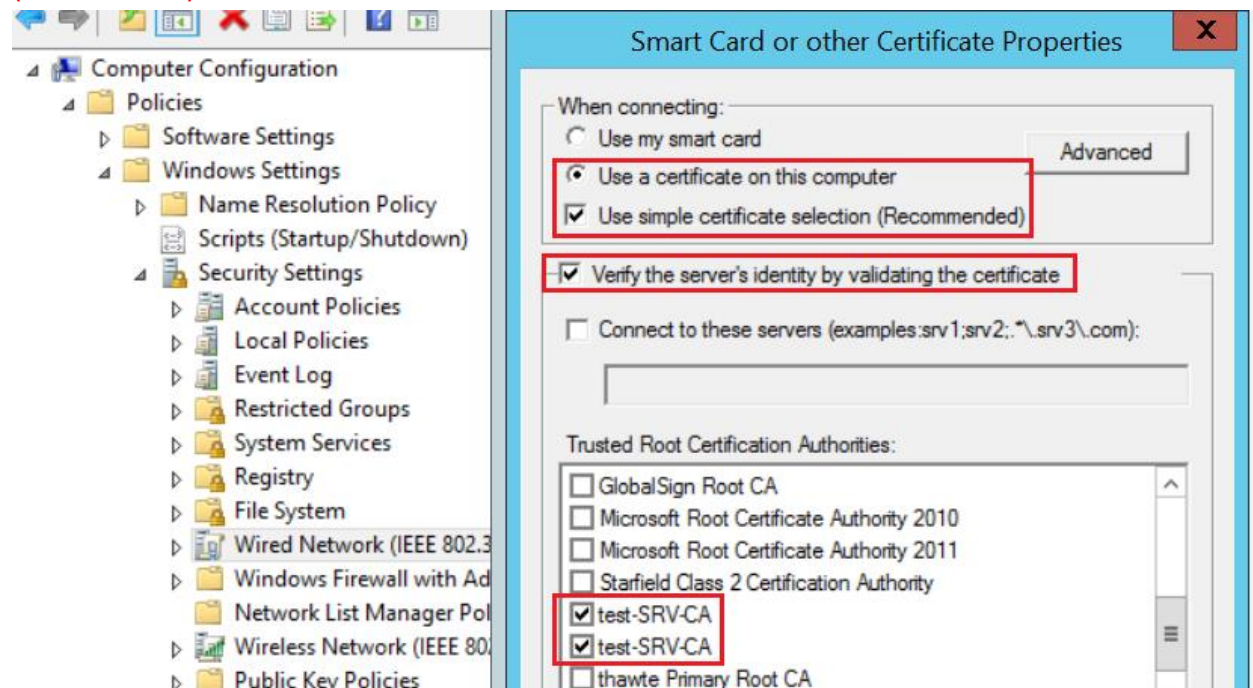
Navigate to **Computer Configuration > Windows Settings > Security Settings > Wired Network** and right-click on it. Choose **Create a New Wired Network Policy**. This will open the New Wired Network Policy Properties box. Name your policy whatever. Select **Use Windows Wired Auto Config service for clients**. Check **Don't allow shared user credentials ...**. Select **Enable block period** and set to one minute.



On the **Security** tab, ensure that **Enable use of IEEE 802.1X authentication for network access** box is checked and from the Select a network authentication method drop-down, choose **Microsoft: Smart Card or other certificate** and **Authentication Mode: User or Computer** **Authentication** Click on the **Properties** button next to Select a network authentication method.



In **Properties** box that pops up, verify check boxes next to **Verify the server's identity by validating the certificate**, **Use a certificate on this computer** and **Use simple certificate selection (Recommend)** **Trusted Root Certificate Authorities**: Check the box of the Root CA.



Wired Autoconfig Service:

Wired Autoconfig service is not enabled by default on Windows machines. In order to get the dot1x wired settings to work, this should be enabled so let's create a group policy. Navigate to **Computer Configuration>Policies>Windows Settings>Security Settings>System Settings>Wired Autoconfig**. Check box for Define this policy setting and choose the radio button for **Automatic**.

