Configure Wireless Clients running Windows 7 and Windows Vista for EAP-TLS Authentication

Use this procedure to configure an Extensible Authentication Protocol–Transport Layer Security (EAP-TLS) profile for authentication using smart cards or other certificates.

Note:

Membership in Domain Admins, or equivalent, is the minimum required to complete this procedure.

Applies To: Windows Server 2008 R2 and up

To configure an EAP-TLS wireless profile for computers running Windows Vista

1. Open the New Wireless Network (IEEE 802.11) Policies Properties dialog box.
2. On the **General** tab, in **Policy Name**, type a new name for your policy, or leave the default.
3. In **Description**, type a description of your policy.
4. Select **Use Windows to configure wireless network settings for clients** to specify that WLAN AutoConfig is used to configure wireless network adapter settings.
5. On the **General** tab, do one of the following:
    - To add and configure a new profile, click **Add**, and then select **Infrastructure**.
    - To edit an existing profile, select the profile you want to modify, and then click **Edit**.
6. On the **Connection** tab, in **Profile Name**, if you are adding a new profile, type a name for the profile. If you are editing a profile that is already added, use the existing profile name, or modify the name as needed.
7. In **Network Name(s) (SSID)**, type the service set identifier (SSID) for your wireless APs, and then click **Add**.

If your deployment uses multiple SSIDs and each wireless AP uses the same wireless security settings, repeat this step to add the SSID for each wireless AP to which you want this profile to apply.

If your deployment uses multiple SSIDs and the security settings for each SSID do not match, configure a separate profile for each group of SSIDs that use the same security settings. For example, if you have one group of wireless APs configured to use WPA2-Enterprise and AES, and another group of wireless APs to use WPA-Enterprise and TKIP, configure a profile for each group of wireless APs.

8. To specify that wireless clients automatically connect to wireless APs for which the SSID is specified in **Network Name(s) (SSID)**, select **Connect automatically when this network is in range**.
9. To specify that wireless clients connect to networks in order of preference, select **Connect to a more preferred network if available**.
10. If you deployed wireless access points that are configured to suppress the broadcast beacon, select **Connect even if the network is not broadcasting**.

Security Note

Enabling this option can create a security risk because wireless clients will probe for and attempt connections to any wireless network. By default, this setting is not enabled.

11. Click the **Security** tab. In **Select the security methods for this network**, in **Authentication**, select **WPA2-Enterprise** if it is supported by your wireless AP and wireless client network adapters. Otherwise, select **WPA-Enterprise**.

Note

Selecting WPA2 exposes settings for Fast Roaming that are not displayed if WPA is selected. The default settings for Fast Roaming are sufficient for most wireless deployments.

12. In **Encryption**, select **AES**, if it is supported by your wireless AP and wireless client network adapters. Otherwise, select **TKIP**.

Note

The settings for both **Authentication** and **Encryption** must match the settings configured on your wireless AP.

13. In **Select a network authentication method**, select **Microsoft: Smart card or other certificate**.
14. In **Authentication mode**, select from the following, depending on your needs: **User or Computer authentication**, **Computer authentication**, **User authentication**, **Guest authentication**. By default, **User or Computer authentication** is selected.
15. In **Max Authentication Failures**, specify the maximum number of failed attempts allowed before the user is notified that authentication has failed. By default, the value is set to “1.”
16. To specify that user credentials are held in cache, select **Cache user information for subsequent connections to this network**.
17. Click **Advanced**, and then configure the following:

    a. To configure advanced 802.1X settings, in **IEEE 802.1X**, select **Enforce advanced 802.1X settings**, and then configure the following settings, depending on your needs: **Max Eapol-Start Msgs**, **Held Period**, **Start Period**, and **Auth Period**.

When the advanced 802.1X settings are enforced, the default values are sufficient for most wireless deployments.

    b. To enable Single Sign On, select **Enable Single Sign On for this network**.

    c. To specify when Single Sign On occurs, select either **Perform immediately before User Logon** or **Perform immediately after User Logon**, depending on your needs.

The remaining default values in **Single Sign On** are sufficient for typical wireless deployments.

    d. To specify the maximum amount of time, in seconds, in which 802.1X authentication must complete and authorize network access, in **Max delay for connectivity (seconds)**, enter a value, depending on your needs.

e. To allow dialogs during Single Sing On, select **Allow additional dialogs to be displayed during Single Sign On**.

f. To specify that wireless computers are placed on one virtual local area network (VLAN) at startup, and then transitioned to a different network after the user logs on to the computer, select **This network uses different VLAN for authentication with machine and user credentials**.

g. To enable Fast Roaming, in **Fast Roaming**, select **Enable Pairwise Master Key (PMK) Caching**. The default values for **PMK Time to Live (minutes)** and **Number of entries in PMK Cache** are typically sufficient for Fast Roaming.

h. Select **This network uses pre-authentication**, if your wireless AP is configured for pre-authentication. The default value of 3 is typically sufficient for **Maximum Pre-authentication attempts**.

i. To specify that cryptography adheres to the FIPS 140-2 certified mode, select **Perform cryptography in FIPS 140-2 certified mode**.

18. Click **Properties**. In the **Smart Card or other Certificate Properties** dialog box, in **When connecting**, select either **Use my smart card** or select both **Use a certificate on this computer** and **Use simple certificate selection (Recommended)**.
19. To require that access clients validate the Network Policy Server (NPS) server certificate, select **Validate server certificate**.
20. To specify which Remote Authentication Dial-In User Service (RADIUS) servers your wired access clients must use for authentication and authorization, in **Connect to these servers**, type then name of each RADIUS server, exactly as it appears in the subject field of the server certificate. Use semicolons to specify multiple RADIUS server names.
21. In **Trusted Root Certification Authorities**, select the CA that issued certificates to your servers running NPS.
22. To specify that clients use an alternate name for the access attempt, select **Use a different user name for the connection**.
23. For improved security and a better user experience, select **Do not prompt user to authorize new servers or trusted certification authorities**.
24. Click **OK** to close the **Smart card or other Certificate Properties** dialog box, and return to the **New Wireless Network Policy Properties** dialog box.