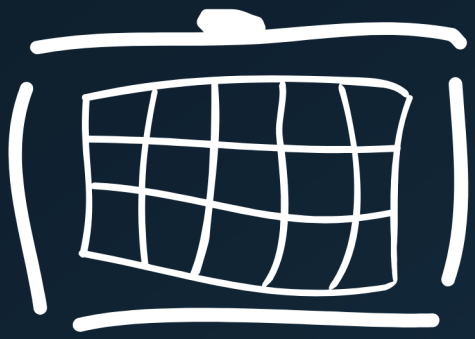


Radiator

CONFIGURATION GUIDE

EAP-TEAP Windows Configuration Guide

Date: 2026-11-16

This guide shows how to configure a Windows wireless profile for EAP-TEAP manually when Radiator Policy Server is set up to authenticate the machine first with a certificate and then authenticate the user with a username and password. If the Windows device is joined to a domain, these settings may already be applied automatically from a profile.

The following flow is used in this example:

- Outer method: EAP-TEAP
- Machine authentication inside TEAP: EAP-TLS
- User authentication inside TEAP: EAP-MSCHAPv2

The Radiator Policy Server configuration and the Windows configuration must match. For example, if user authentication uses EAP-TLS instead of EAP-MSCHAPv2, change the secondary EAP method in Windows to EAP-TLS as well. If the Radiator Policy Server configuration is changed to contain only user or machine authentication with EAP-MSCHAPv2, set the primary EAP method in Windows to EAP-MSCHAPv2 and set the secondary EAP method to `none`.

For the outer TLS tunnel, only TLS 1.2 is supported. For inner EAP-TLS, TLS v1.3 can also be used.

With this configuration, Windows can authenticate the device during computer authentication and then continue with user authentication after sign-in. This is commonly used in enterprise Wi-Fi deployments that need both machine trust and user credentials.

Before you begin

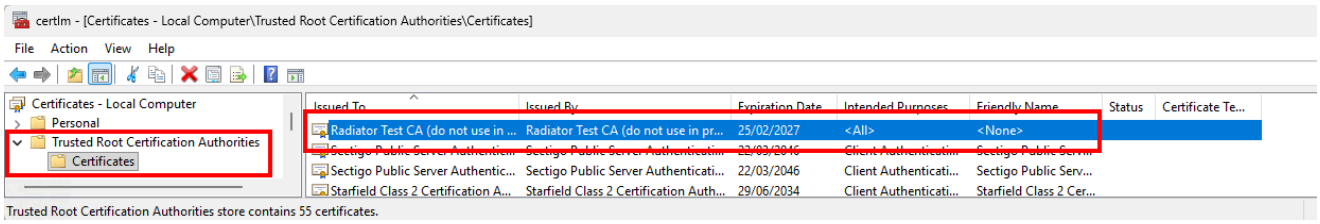
Make sure you have the following information and files available before starting:

- The root CA certificate that issued the server certificate
- When using EAP-TLS for machine authentication, a machine certificate and matching key for the Windows device, usually packaged as a `.p12` file
- If used in your environment, the server name from the Radiator server certificate
- When using EAP-TLS for user authentication, a user certificate for the signed-in user with a matching key, usually packaged as a `.p12` file
- When using EAP-MSCHAPv2 for authentication, valid credentials

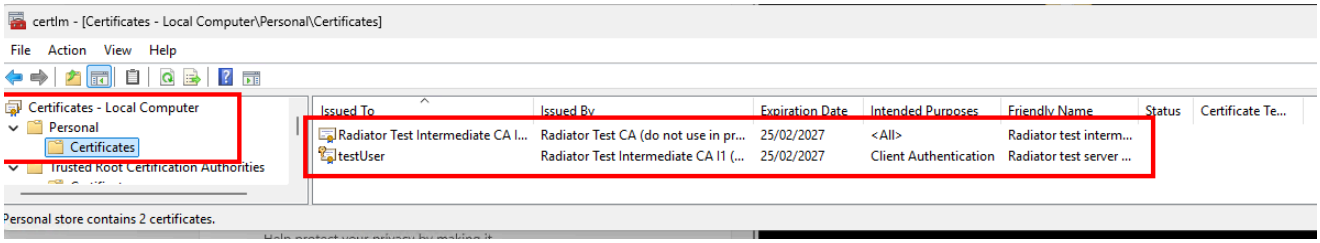
Certificates

Install the certificates before configuring the Wi-Fi profile. Windows must trust the server certificate chain, and the computer must have access to the certificate used for machine authentication.

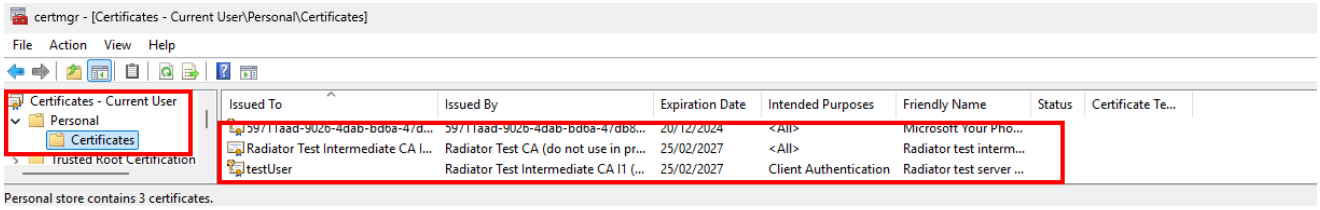
1. Import the issuing root CA certificate into `Local Computer -> Trusted Root Certification Authorities -> Certificates`.



2. Import the machine certificate used for EAP-TLS computer authentication into `Local Computer -> Personal -> Certificates`.



3. (Optional) Import the user certificate used for EAP-TLS user authentication into `Current User -> Personal -> Certificates`.

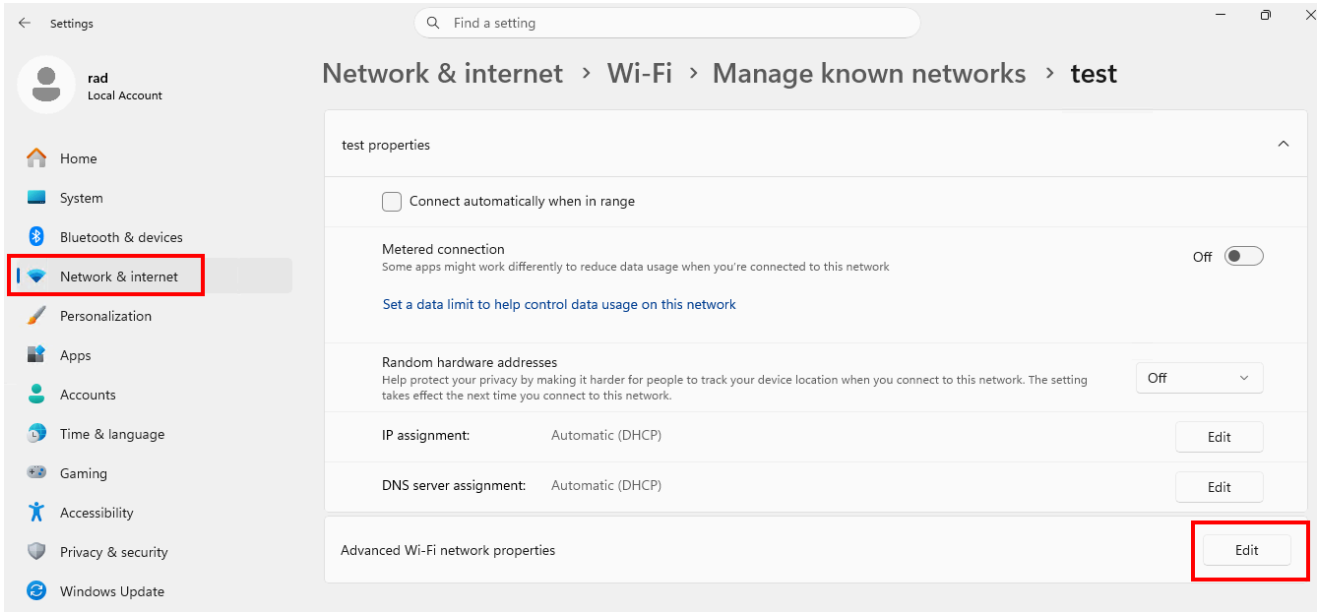


If the certificates are missing or installed in the wrong store, Windows may fail TEAP server validation or may not offer the expected client certificate during authentication.

Wi-Fi Profile

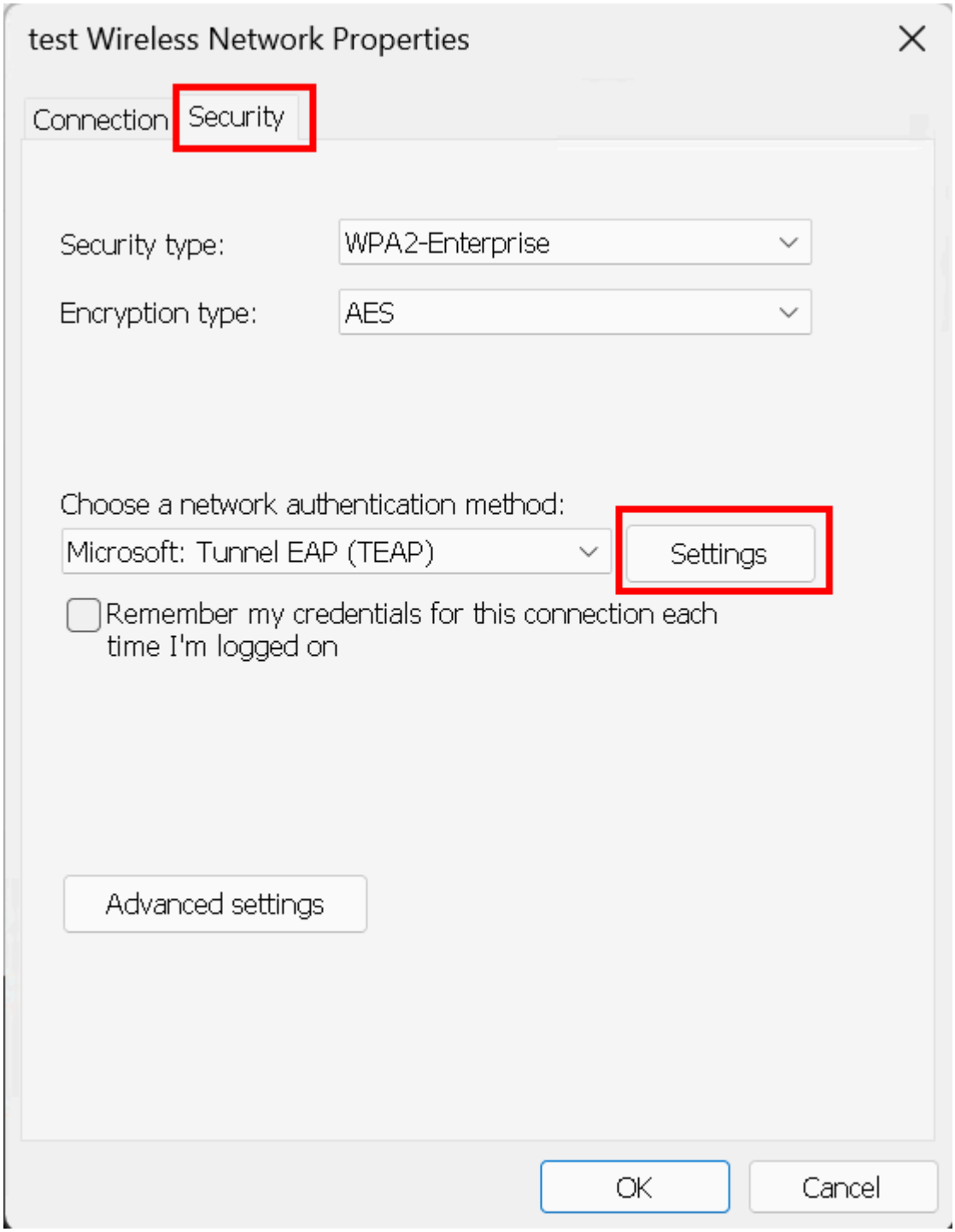
Configure the wireless profile after the certificates are in place. The TEAP settings below match the Radiator Policy Server configuration exactly: EAP-TEAP as the outer method, EAP-TLS for the machine phase, and EAP-MSCHAPv2 for the user phase.

1. Open the Wi-Fi network properties for the target SSID.



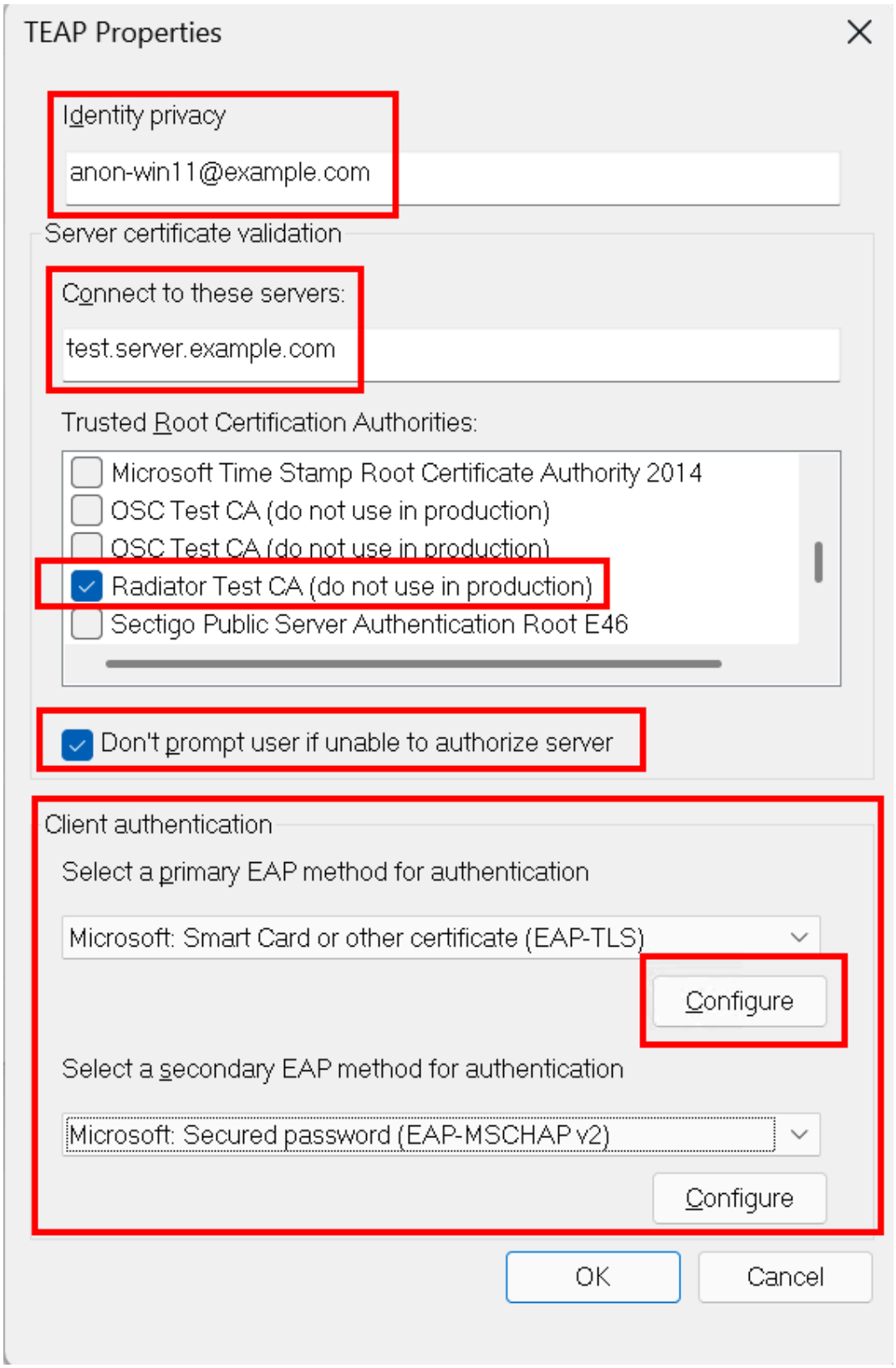
2. Open the `Security` tab.
3. Set `Choose a network authentication method` to `Microsoft: Tunnel EAP (TEAP)`.

4. Click `Settings`.



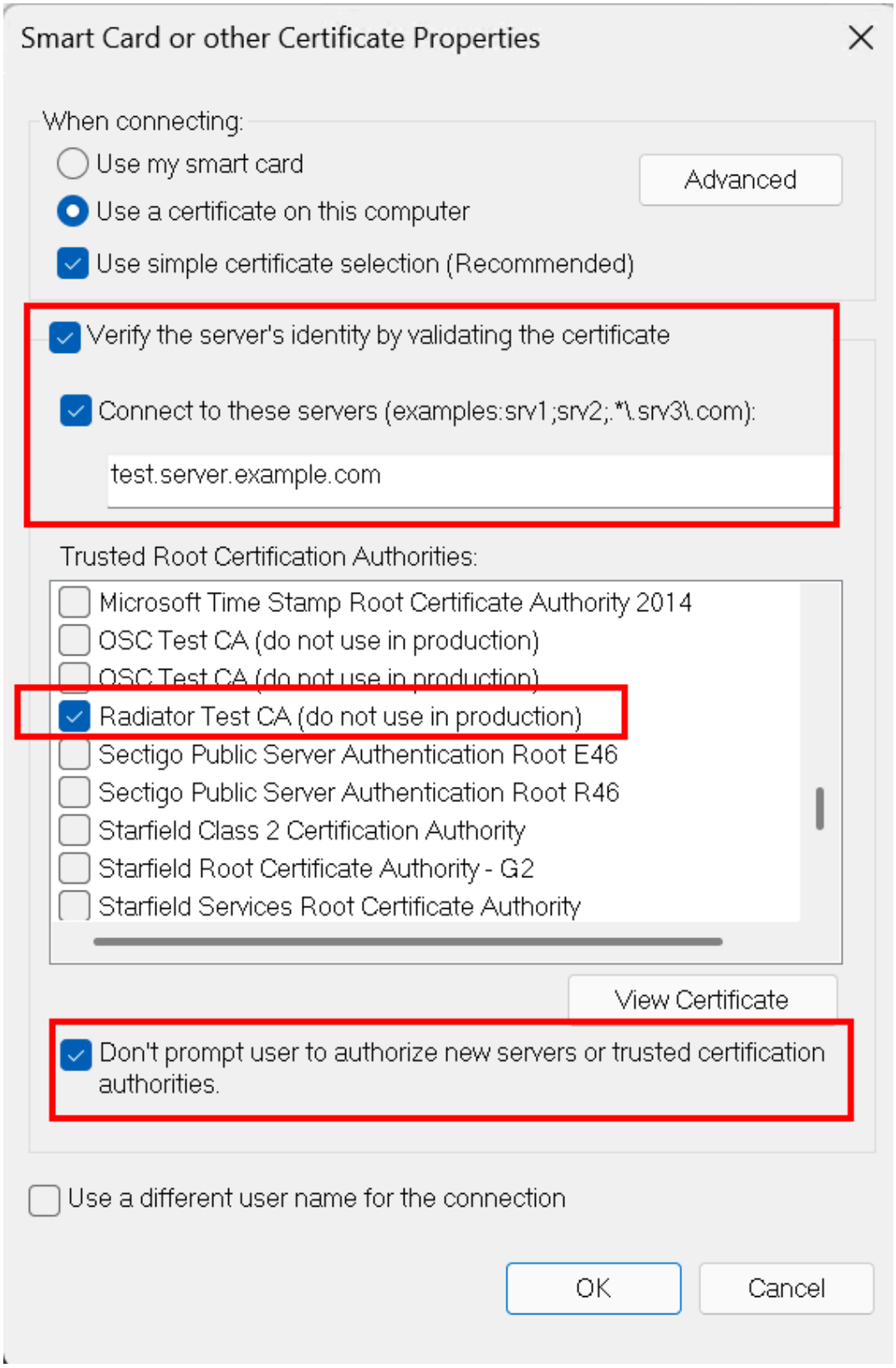
5. In `TEAP Properties`, set `Identity privacy` to the anonymous identity used by your deployment.
6. (Optional) In `Connect to these servers`, enter the server name from the Radiator server certificate.
7. In `Trusted Root Certification Authorities`, select the CA that issued the server certificate.
8. (Optional) Enable `Don't prompt user to authorize new servers or trusted certification authorities`.

9. In `Select a primary EAP method for authentication`, select the same EAP method that is used first on the Radiator Policy Server configuration. In the example configuration this is `Microsoft: Smart Card or other certificate (EAP-TLS)`.



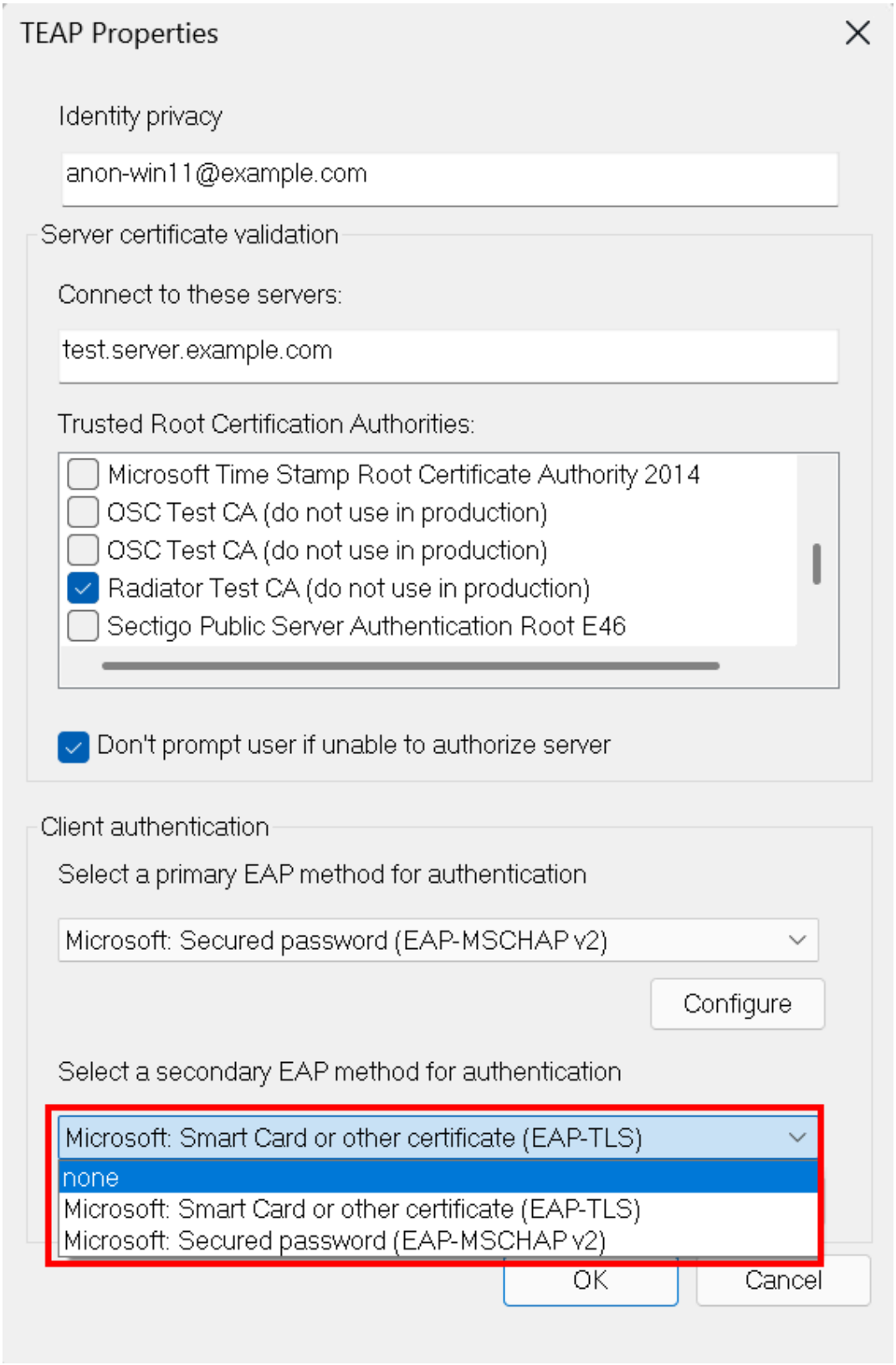
10. Open the primary EAP method settings for `Microsoft: Smart Card or other certificate (EAP-TLS)`.
11. In `Smart Card or other Certificate Properties`, select `Use a certificate on this computer`.
12. Keep `Use simple certificate selection (Recommended)` enabled.
13. Enable `Verify the server's identity by validating the certificate`.
14. Enable `Connect to these servers` and enter the server name from the Radiator server certificate.
15. In `Trusted Root Certification Authorities`, select the CA that issued the server certificate.

16. Enable `Don't prompt user to authorize new servers or trusted certification authorities`.



17. Click `OK`.
18. In `Select a secondary EAP method for authentication`, select the same EAP method that is used for the second authentication in the Radiator Policy Server configuration. In the example configuration this is `Microsoft: Secured password (EAP-MSCHAP v2)`.
19. Click `OK`.

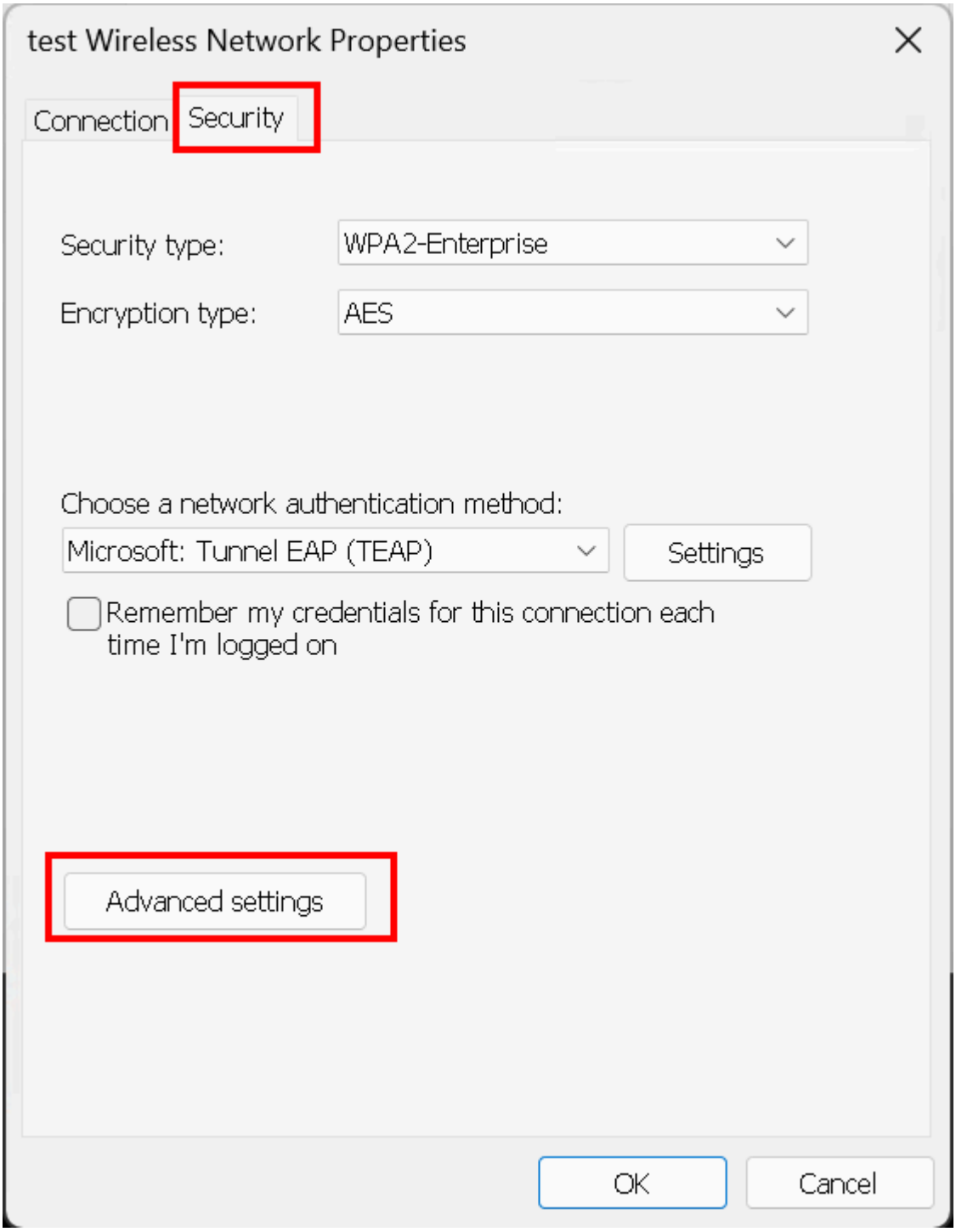
The method order matters. In this example, Windows uses the TEAP configuration to support certificate-based computer authentication and then continues with user authentication inside the same TEAP tunnel. If the configuration is changed to do only computer or user authentication, set the secondary EAP method to `none`.



Advanced Settings

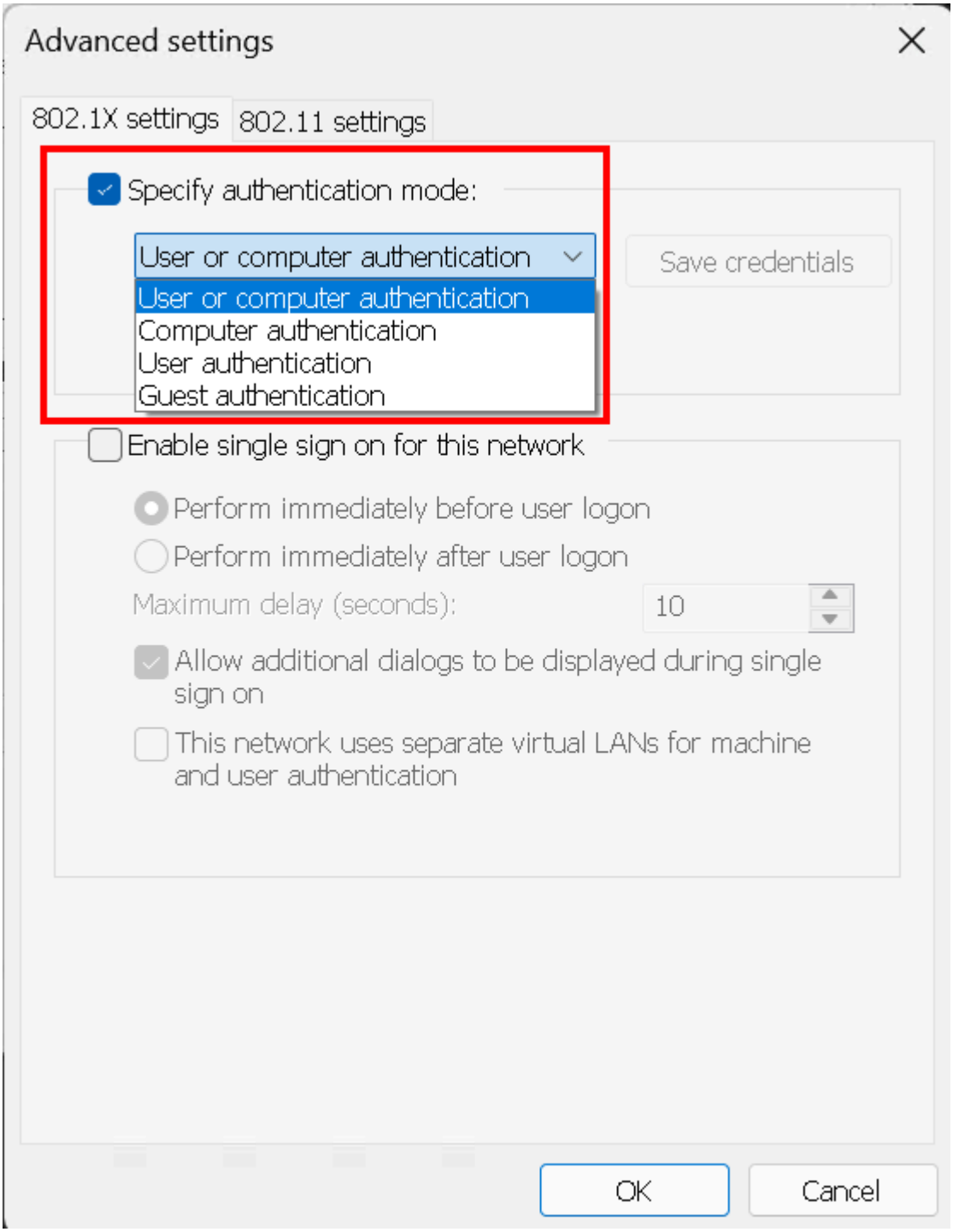
Set the authentication mode so Windows can perform both computer and user authentication on the same network profile.

1. From the Wi-Fi profile, open `Advanced settings`.



2. Enable `Specify authentication mode`.

3. Set the mode to `User or computer authentication`.



4. Click `OK`.

This setting allows flexibility in the Radiator Policy Server configuration, because the server can be configured for computer authentication, user authentication, or both.

After you save the profile, test the connection with the device joined to the network and the required certificates installed. Computer authentication should complete without prompts, but Windows should show a credential prompt for user authentication. The example Radiator Policy Server configuration uses a 60-second timeout for this phase to give the user enough time to enter their username and password.