Basic Configuration for PEAP Authentication

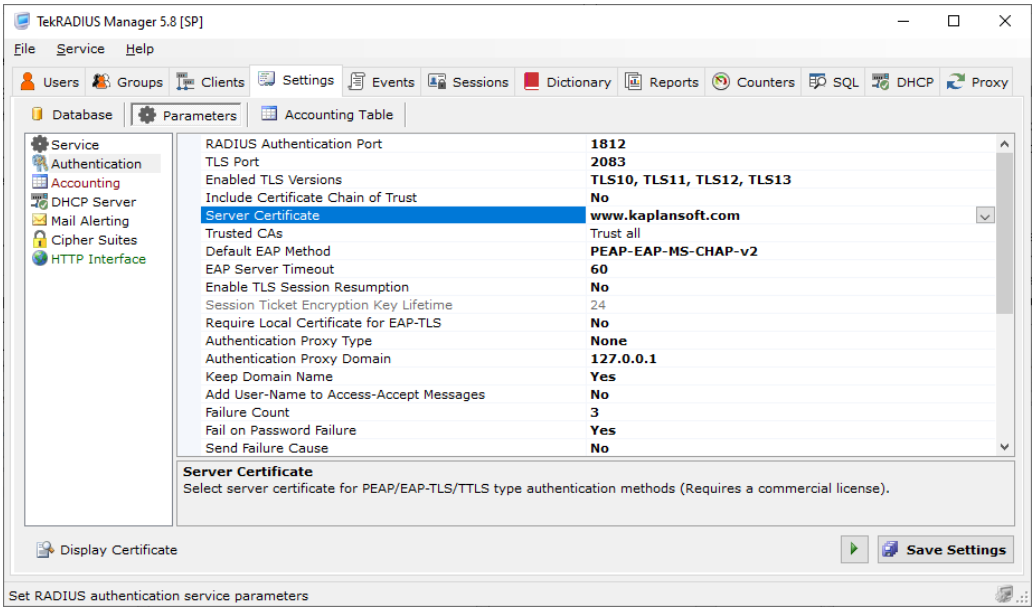
PEAP (Protected EAP) authentication in TekRADIUS is one of the most common methods used in 802.1X/WPA2-Enterprise environments. The basic setup involves the following steps.

Prerequisites

TekRADIUS SQL edition requires Microsoft SQL Server (the Express edition is sufficient) to store its configuration and user data. You can also install and use TekRADIUS LT which comes with its built-in SQLite database. After running Setup.exe and completing the installation wizard with default settings, launch TekRADIUS Manager. PEAP-EAP-MS-CHAP-v2 works in the free edition; methods like EAP-TLS and EAP-TTLS require a commercial license.

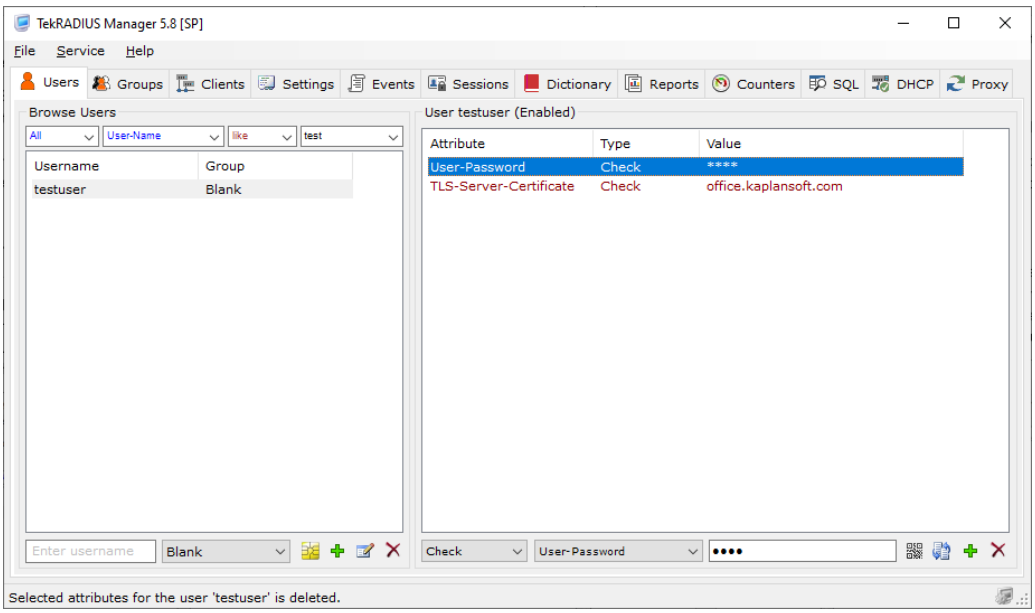
1. Prepare the server certificate

PEAP uses a TLS server certificate for its outer tunnel, so this step is mandatory. You can generate a self-signed certificate using the TekCERT[1]. The server certificate must be created for “Server Authentication” purpose. TekRADIUS also creates a self-signed certificate named TekRADIUS automatically when installed.



TekRADIUS lists valid certificates from the Windows Certificate Store / Local Machine, and it uses this certificate by default for PEAP sessions if you don't set a TLS-Server-Certificate in a user or group profile. Server Certificate selection at Settings / Parameters is not available in the freeware mode. Make sure the certificate you create is installed in the "Local Machine" store.

[1] https://www.kaplansoft.com/tekcert/



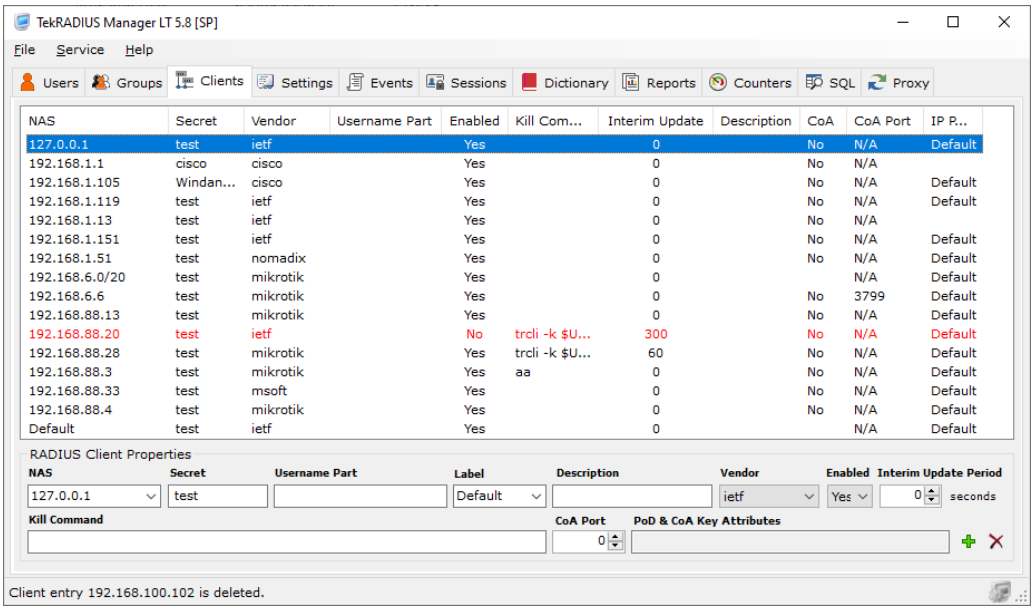
2. Service Parameters

In the Manager, go to Settings → Service Parameters and configure:

- **Authentication Port:** 1812 (default UDP port)
- **Default EAP Method:** PEAP-EAP-MS-CHAP-v2
- **Server Certificate:** select the certificate you created
- **Startup Logging: Debug** is recommended during initial setup and troubleshooting; once the deployment is verified, the logging level can be lowered to Automatic or None.

The supported inner authentication method for PEAP is EAP-MS-CHAP-v2. MS-CHAP-v2 is sufficient in most scenarios.

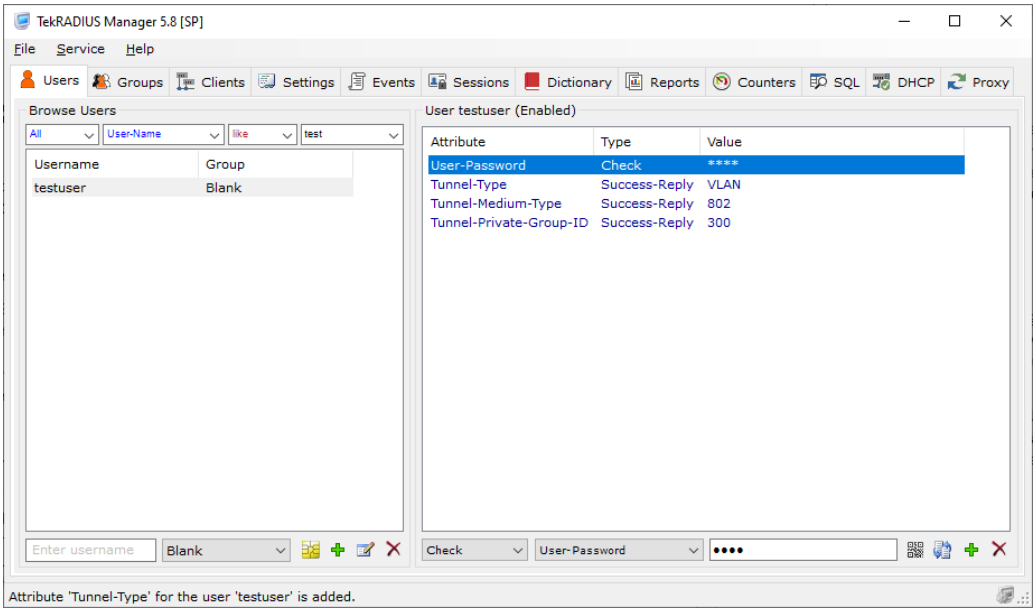
3. Define the RADIUS client (NAS)



Under the Clients tab, add your access point or switch: enter its IP address and set a **shared secret**. This secret must match exactly on both the TekRADIUS side and the RADIUS settings of the access device.

4. Create users

Under the Users tab, add a user and define the **User-Password** check attribute. Since MS-CHAP-v2 stores passwords in clear text, you need to enter the User-Password value as plain text. Optionally, you can add Success-Reply attributes (e.g., VLAN assignment) via the Default group or as user-specific reply attributes.



5. Start the service and test

After setting the startup mode and activating it with Save Settings, start the TekRADIUS Windows service. On the client side (e.g., Windows), configure the wireless connection to use "Protected EAP (PEAP)" as the EAP type with MS-CHAP-v2 as the inner method. You can follow the authentication flow by examining the Debug logs in the Logs folder under TekRADIUS application directory.

Certificate validation is usually the most common sticking point: if you're using a self-signed certificate, you'll need to install the root certificate into the clients' "Trusted Root Certification Authorities" store or disable server certificate validation in the client profile.