Enterprise wireless security with User Manager v5

User Manager version 5 (available for RouterOS v7) supports user authentication via the Extensible Authentication Protocol (EAP).

This guide will explain the steps needed to configure User Manager v5 as the authentication server for MikroTik wireless access points with users being offered PEAP and EAP-TLS authentication methods.

The guide assumes a standalone device running User Manager at the network address 10.0.0.10 and 2 Access Points - one at 10.0.0.11 and the other at 10.0.0.12

Installing User Manager

User Manager v5 can be found in the 'Extra packages' archive for the latest release of RouterOS v7.

Download the archive for the appropriate CPU architecture, extract it, upload the User Manager package to the router and reboot it.

Generating TLS certificates

When using secure EAP methods, the client device (supplicant) verifies the identity of the authenication server before sending its own credentials to it. For this to happen, the authentication server needs a TLS certificate.

This certificate should:

1. Be valid and signed by a certificate authority which is trusted by the client device
2. Have a fully qualified domain name in the Common Name (CN) and Subject Alt Name fields
3. Have the Extended Key Usage attribute indicating that it is authorized for authentcating a TLS server
4. Have Validity period of no more than 825 days

The EAP-TLS method requires the client device to have a TLS certificate (instead of a password).

To be considered valid by User Manager, a client certificate must:

1. Be valid and signed by an authority, which is trusted by the device running User Manager
2. Have the user name in the Subject Alt Name (SAN) field. For backward compatibility, you can also add it in the CN field. For more information please see: https://datatracker.ietf.org/doc/html/rfc5216#section-5.2

Finally, the WPA3 enterprise specification includes an extra secure mode, which provides 192-bit cryptographic security.

This mode requires using EAP-TLS with certificates that:

1. Use either P-384 elliptic curve keys or RSA keys which are at least 3072 bits in length
2. Use SHA384 as the digest (hashing) algorithm

For the sake of brevity (and to showcase more of RouterOS' capabilities), this guide will show how to generate all the certificates on the device running User Manager, but in a large scale enterprise environment, the authentication server and client devices would each generate private keys and certificate signing requests locally, then upload CSRs to a certificate authority for signing.

Commands executed on device running User Manager

```
# Generating a Certificate Authority
/certificate
add name=radius-ca common-name="RADIUS CA" key-size=secp384r1 digest-algorithm=sha384 days-valid=1825 key-
usage=key-cert-sign,crl-sign
sign radius-ca ca-crl-host=radius.mikrotik.test
# Generating a server certificate for User Manager
add name=userman-cert common-name=radius.mikrotik.test subject-alt-name=DNS:radius.mikrotik.test key-
size=secp384r1 digest-algorithm=sha384 days-valid=800 key-usage=tls-server
sign userman-cert ca=radius-ca
# Generating a client certificate
add name=maija-client-cert common-name=maija@mikrotik.test key-usage=tls-client days-valid=800 key-
size=secp384r1 digest-algorithm=sha384
sign maija-client-cert ca=radius-ca
# Exporting the public key of the CA as well as the generated client private key and certificate for
distribution to client devices
export-certificate radius-ca file-name=radius-ca
# A passphrase is needed for the export to include the private key
export-certificate maija-client-cert type=pkcs12 export-passphrase="true zebra capacitor ziptie"
```

Configuring User Manager

Commands executed on device running User Manager

```
# Enabling User Manager and specifying, which certificate to use
/user-manager
set enabled=yes certificate=userman-cert
# Enabling CRL checking to avoid accepting revoked user certificates
/certificate settings
set crl-download=yes crl-use=yes
# Adding access points
/user-manager router
add name=ap1 address=10.0.0.11 shared-secret="Use a secure password generator for this"
add name=ap2 address=10.0.0.12 shared-secret="Use a secure password generator for this too"
# Limiting allowed authentication methods
/user-manager user group
set [find where name=default] outer-auths=eap-tls,eap-peap
add name=certificate-authenticated outer-auths=eap-tls
# Adding users
/user-manager user
add name=maija@mikrotik.test group=certificate-authenticated
add name=paija@mikrotik.test group=default password="right mule accumulator nail"
```

Configuring access points

AP running regular wireless package

Commands executed on ap1

```
# Configuring radius client
/radius
add address=10.0.0.10 secret="Use a secure password generator for this" service=wireless timeout=1s
/radius incoming
set accept=yes
# Adding a security profile and applying it to wireless interfaces
/interface/wireless/security-profile
add name=radius mode=dynamic-keys authentication-types=wpa2-eap
/interface/wireless
set [find] security-profile=radius
```

AP running wifiwave2 package

Commands executed on ap2

```
# Configuring radius client
/radius
add address=10.0.0.10 secret="Use a secure password generator for this too" service=wireless timeout=1s
/radius incoming
set accept=yes
# Configuring enabled authentication types. Can also be done via a security profile, but note that interface
properties, if specified, override profile properties
/interface/wifiwave2 set [find] security.authentication-types=wpa2-eap,wpa3-eap
```

A wifiwave2 AP can also be configured to use the extra secure wpa3-eap-192 mode, but note that it requires that all client devices support the GCMP-256 cipher and use EAP-TLS authentication.

Notes on client device configuration

Windows

When manually installing a CA in Windows, make sure to explicitly place it in the 'Trusted Root Certification Authorities' certificate store. It will not be placed there automatically.

Android

When connecting to a network with EAP authentication, Android devices ask the user to specify a 'domain'. This refers to the expected domain of the host name included in the RADIUS server's TLS certificate ('mikrotik.test' in our example).

By default, Android devices use the device's built-in root CA list for validating the RADIUS server's certificate. When using your own CA, it needs to be selected in the appropriate dropdown menu.

iOS

Apple iOS does not appear to actually trust a manually imported CA to authenticate RADIUS servers. The server certificate is marked as 'Not Trusted' unless the CA was imported using Apple's proprietary 'Configurator' utility or an approved third party MDM tool.