


Dot1xProfile 1.0



dot1x

@mitaCode

Table of Contents

Dot1xProfile User Manual	2
Using Dot1xProfile	3
802.1x Profiles	4
Configuring EAP-TLS	6
Configuring EAP-TTLS	8
Configuring PEAP	9
Configuring EAP-FAST	10
Configuring LEAP	12
Configuring EAP-AKA	13
Configuring EAP-SIM	14
Configuring Trusted Servers	15
Signing Profiles	19
Exporting Profiles	22
Installing Profiles	23



Dot1xProfile User manual

Dot1xProfile is a small utility to generate 802.1x network authentication profiles. Dot1xProfile can quickly create 802.1x profiles without using MDM (Mobile Device Management) tools such as Apple Configurator or OSX Server. Dot1xProfile does not replace these tools but can be helpful in test environments and when you need to quickly set up access to a network with 802.1x authentication.

Profiles can be exported in mobileconfig files and later installed on OSX or iOS devices or can be installed directly on the local computer.

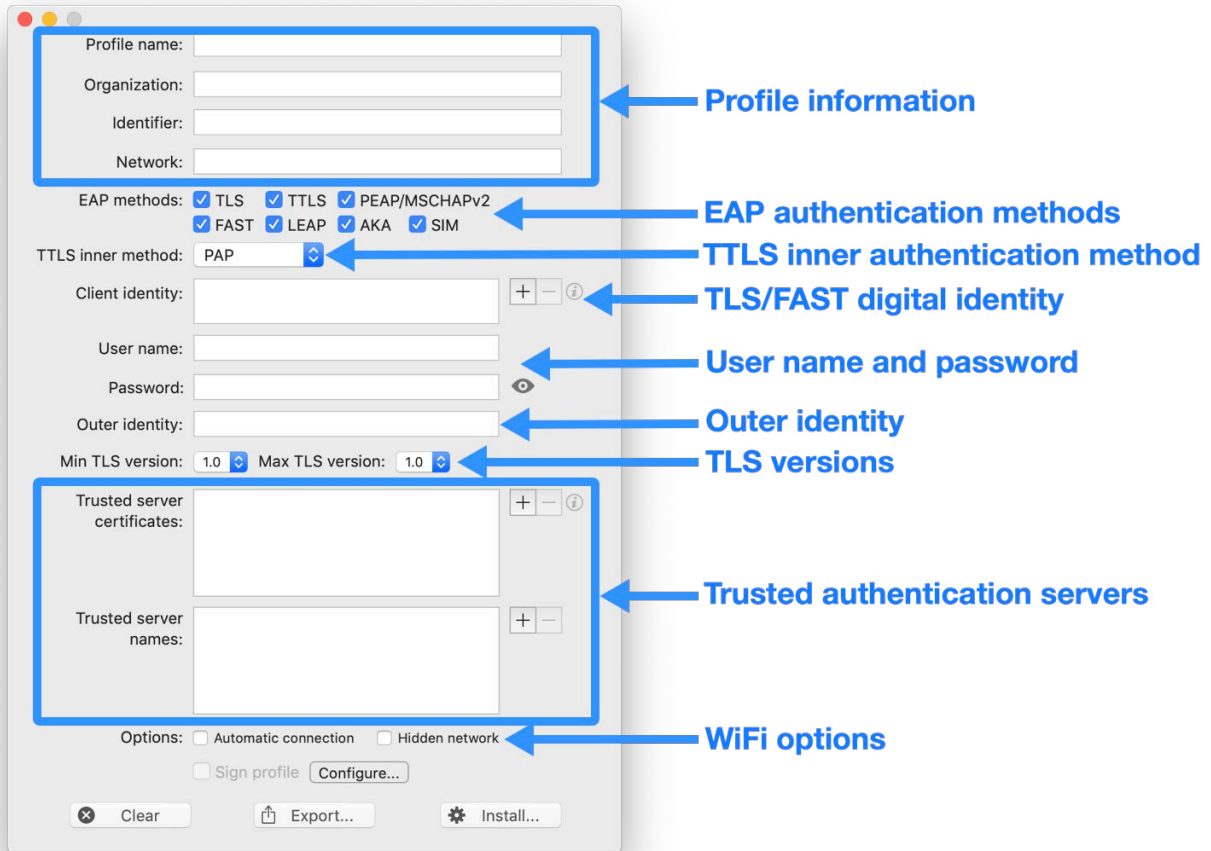
Dot1xProfile supports major authentication methods used in wired and wireless networks. The EAP (Extensible Authentication Protocol) methods implemented are TLS, TTLS and PEAP.

ermita@code

www.ermitacode.com

Using Dot1xProfile

The left part of the window contains the configurable parameters used to authenticate. The right part displays the RADIUS protocol messages interchanged with the authentication server.



The parameters are divided in several groups:

- **Profile data:** the **Profile name** and **Organization** fields are used to identify the profile in the System Preferences Profiles, the **Identifier** field is used to select the profile in the System Preferences Network connections and the **Network** defines the SSID to which the profile should be applied for WiFi network connections. Please see Installing 802.1x profiles.
- **EAP methods:** select the EAP (Extensible Authentication Protocol) methods to be enabled in the profile. If the TLS or FAST method is enabled a user identity should be specified in the **Client identity** field. If the TTLS method is enabled, an inner authentication method can be specified in the **TTLS inner method** field. If the PEAP method is enabled the MSCHAPv2 inner authentication method is used. At least 1 EAP method should be selected.
- **TTLS inner method:** method inside the secure tunnel used to authenticate with TTLS method.
- **Client identity:** digital identity used to authenticate with the TLS or FAST method.
- **User name:** user name used to authenticate with the TTLS, PEAP, FAST or LEAP methods.
- **Password:** user password used to authenticate with the TTLS, PEAP, FAST or LEAP methods.
- **Outer identity:** external user name sent in the RADIUS messages outside the secure TLS tunnel.
- **Min/Max TLS version:** minimum/maximum TLS version used for the TLS tunnel.
- **Trusted authentication servers:** trusted authentication servers certificates and names.
- **WiFi Options:** **Automatic connection** enables automatic connection to the specified SSID (Network field) for WiFi networks, **Hidden network** enables connecting to hidden SSID's.

You can use the **Clear** button to clear all the fields, the **Export...** button to export the profile to a file or the **Install...** button to install the profile in the local machine.

dot1x 802.1x Profiles

OSX configuration profiles (*.mobileconfig* files) are XML files that contain device security policies and restrictions, VPN configuration information, Wi-Fi settings, email and calendar accounts, and authentication credentials that permit OSX and iOS devices to work with enterprise systems. The *mobileconfig* files can also be encrypted.

You normally create *mobileconfig* files using the Apple Configurator utility, MDM (Mobile Device Management) tools and Device onboarding systems. *mobileconfig* files can be also created manually editing the XML file. The *mobileconfig* files can be sent to Macs, iPhone and iPad devices or iPod Touch to be installed.

Using Dot1xProfile you can also generate *mobileconfig* files containing 802.1x authentication configuration easily and can be specially helpful in test environments and when you need to quickly set up access to a 801.1x authenticated wired or wireless network.

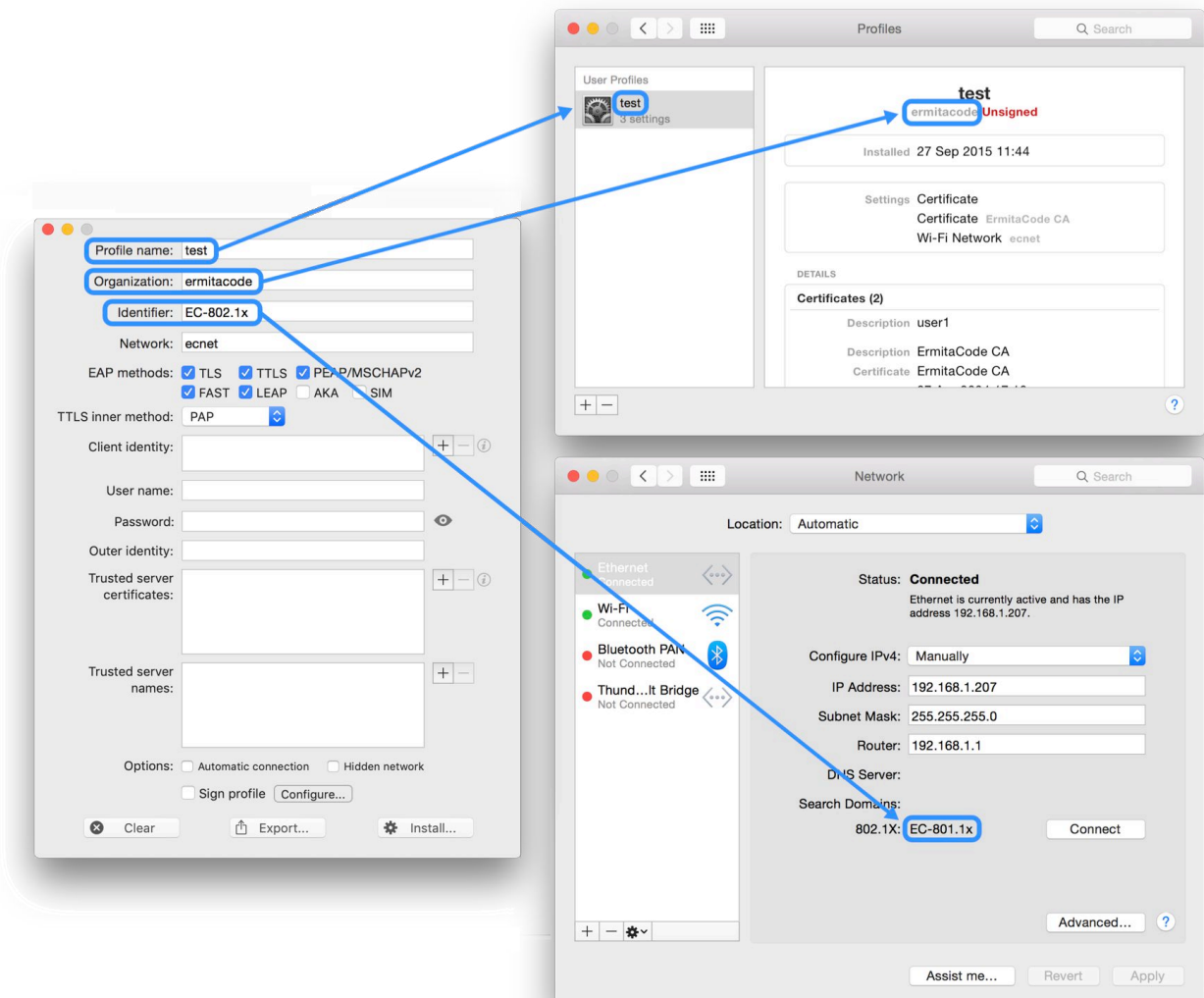
Dot1xProfile can generate signed profiles if a signing identity is configured in the Preferences Panel.

In Mac OSX you can install a *mobileconfig* profile simply double-clicking on its Finder icon. Finder will open System Preferences application and will try to install the profile. You can see the installed profiles clicking the **Profiles** icon in the System Preferences window:



Profiles

The following figure shows how the Dot1xProfile fields are used by the System Preferences when a profile is installed:

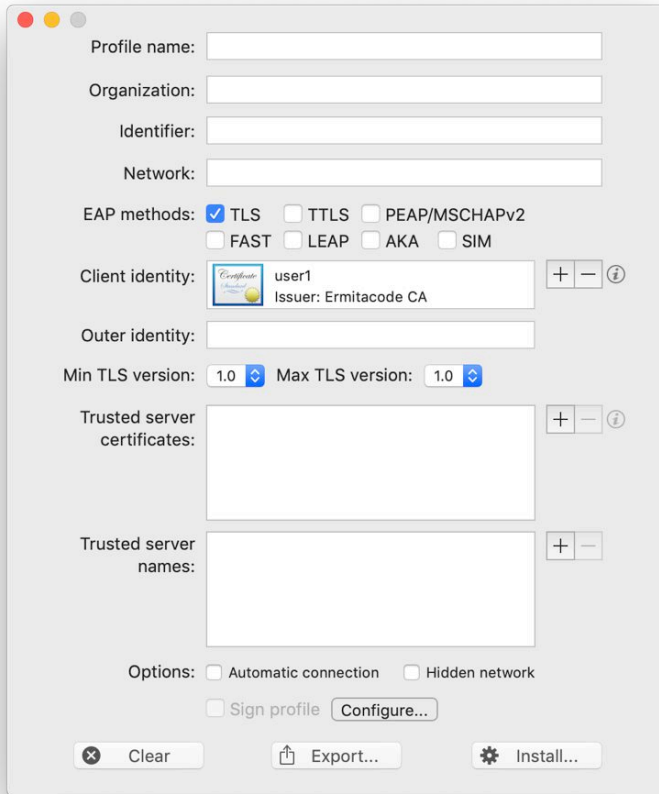



Profile name and **Organization** are user during the profile installation. The **Profile name** will also identify the profile in the System Preferences **Profile** section. The **Identifier** field will identify the profile in the System Preferences **Network** section when it is used

to perform 801.1x authentication in a network.

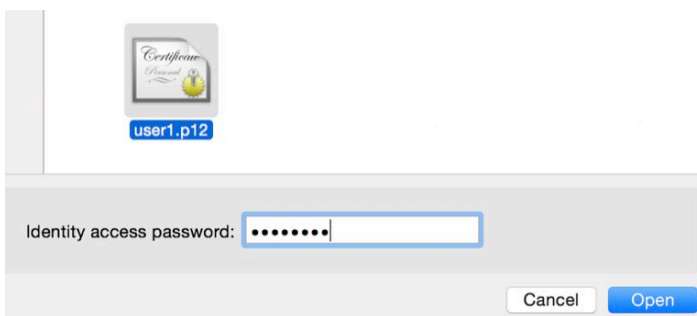
Configuring EAP-TLS

If the TLS authentication method is selected, a user digital identity must be provided. TLS authenticates using a user digital identity and sending its certificate to the RADIUS Server through a TLS session:



To select the digital identity to use in the authentication click the  button to the right of the TLS identity field and select a PKCS#12 Personal Information Interchange file. This file should have file PKCS12, P12 or PFX extension.

PKCS#12 files are protected by a password which optionally can be entered in the file selection panel:

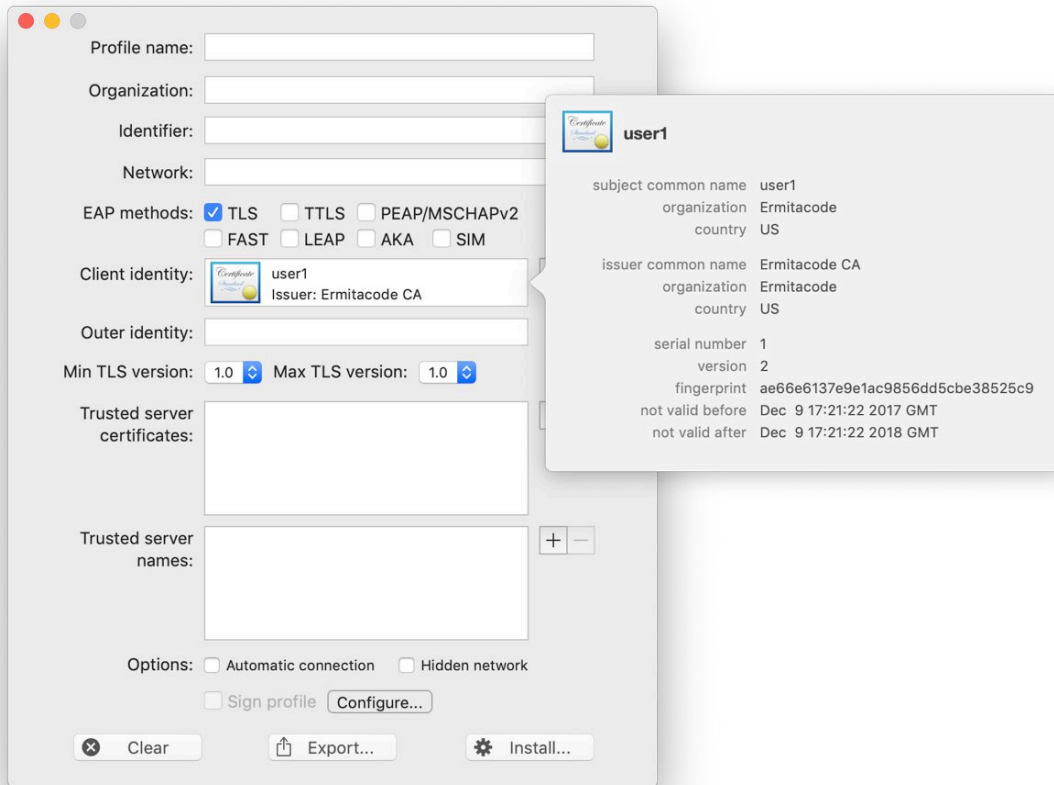


If the PKCS#12 password is correctly entered, the digital identity the CN (Common Name) of the subject and the certificate issuer will be shown in the **Client identity** field.

If the PKCS#12 password is not entered, only the PKCS#12 filename will be shown in the **Client identity** field.

To clear the **Client identity** field click the  button.

If the PKCS#12 password was supplied, you can click the  button to obtain the identity certificate information:



You can add **Trusted server certificates** and **Trusted server names** to define the authentication servers accepted for authentication.



You are not required to specify a **Client identity**. If the **Client identity** is not included in the profile, it will be requested to the user when using the profile.



Configuring EAP-TTLS

If the TTLS authentication method is selected, the inner (tunneled) authentication method to be used can be specified in the **TTLS inner method** popup button. Optionally, the user credential (**User name** and **Password**) can be specified:

Profile name:

Organization:

Identifier:

Network:

EAP methods: TLS TTLS PEAP/MSCHAPv2
 FAST LEAP AKA SIM

TTLS inner method: PAP

User name:

Password:

Outer identity:

Min TLS version: 1.0 Max TLS version: 1.0

Trusted server certificates:

Trusted server names:

Options: Automatic connection Hidden network
 Sign profile

Clear

The **TTLS inner method** values are PAP (default method), CHAP, MSCHAP and MSCHAPv2.

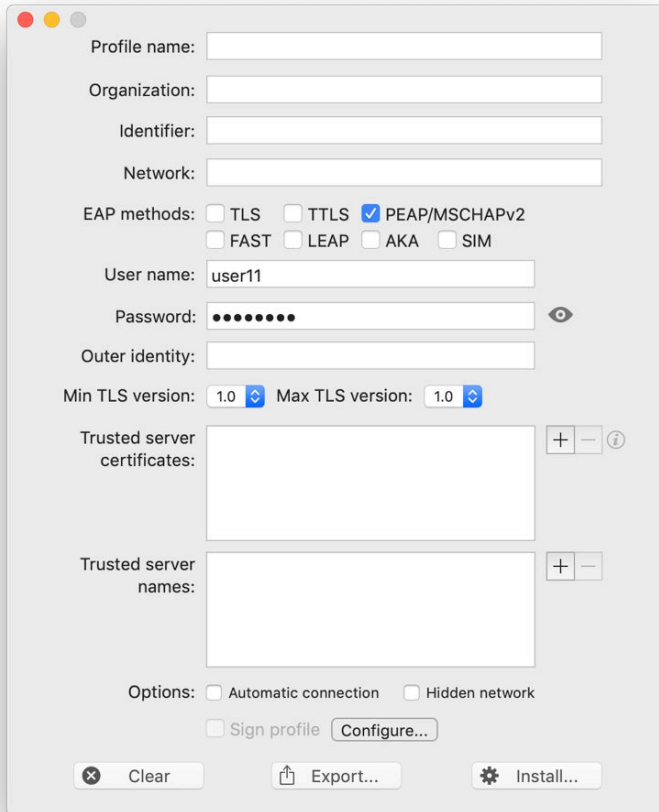
You can add **Trusted server certificates** and **Trusted server names** to define the authentication servers accepted for authentication.



You are not required to specify a **User name** and **Password**. If the TTLS credential is not included in the profile, it will be requested to the user when using the profile.

Configuring PEAP

The PEAP authentication method uses the MSCHAPv2 inner (tunneled) authentication method. Optionally, the user credential (**User name** and **Password**) can be specified:



Profile name:


Organization:

Identifier:

Network:


EAP methods: TLS TTLS PEAP/MSCHAPv2
 FAST LEAP AKA SIM

User name:

Password: 

Outer identity:

Min TLS version: Max TLS version:

Trusted server certificates: 

Trusted server names:

Options: Automatic connection Hidden network
 Sign profile

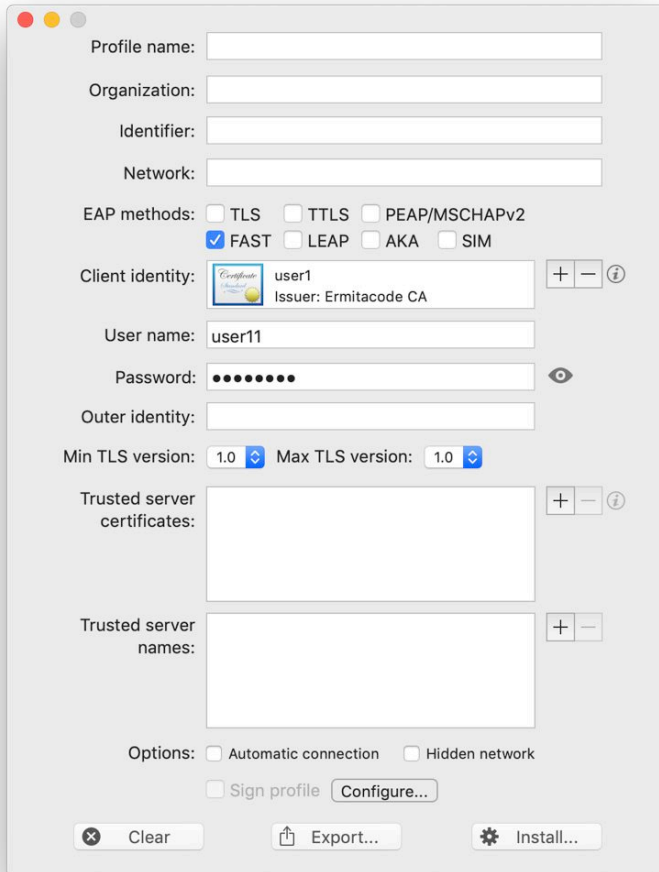
You can add **Trusted server certificates** and **Trusted server names** to define the authentication servers accepted for authentication.



You are not required to specify a **User name** and **Password**. If the PEAP credential is not included in the profile, it will be requested to the user when using the profile.

Configuring EAP-FAST

If the EAP-FAST authentication method is selected, a user digital identity and a user credential (**User name** and **Password**) can be optionally specified:




Profile name:

Organization:

Identifier:

Network:

EAP methods: TLS TTLS PEAP/MSCHAPv2
 FAST LEAP AKA SIM

Client identity:  user1
Issuer: Ermitacode CA

User name:

Password:

Outer identity:

Min TLS version: Max TLS version:

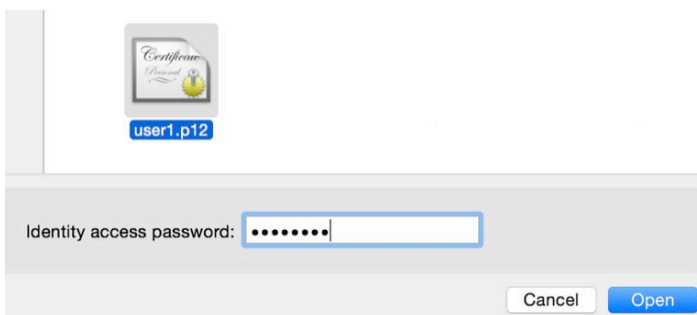
Trusted server certificates:


Trusted server names:

Options: Automatic connection Hidden network
 Sign profile

To select the digital identity to use in the authentication click the button to the right of the TLS identity field and select a PKCS#12 Personal Information Interchange file. This file should have file PKCS12, P12 or PFX extension.

PKCS#12 files are protected by a password which optionally can be entered in the file selection panel:



 user1.p12

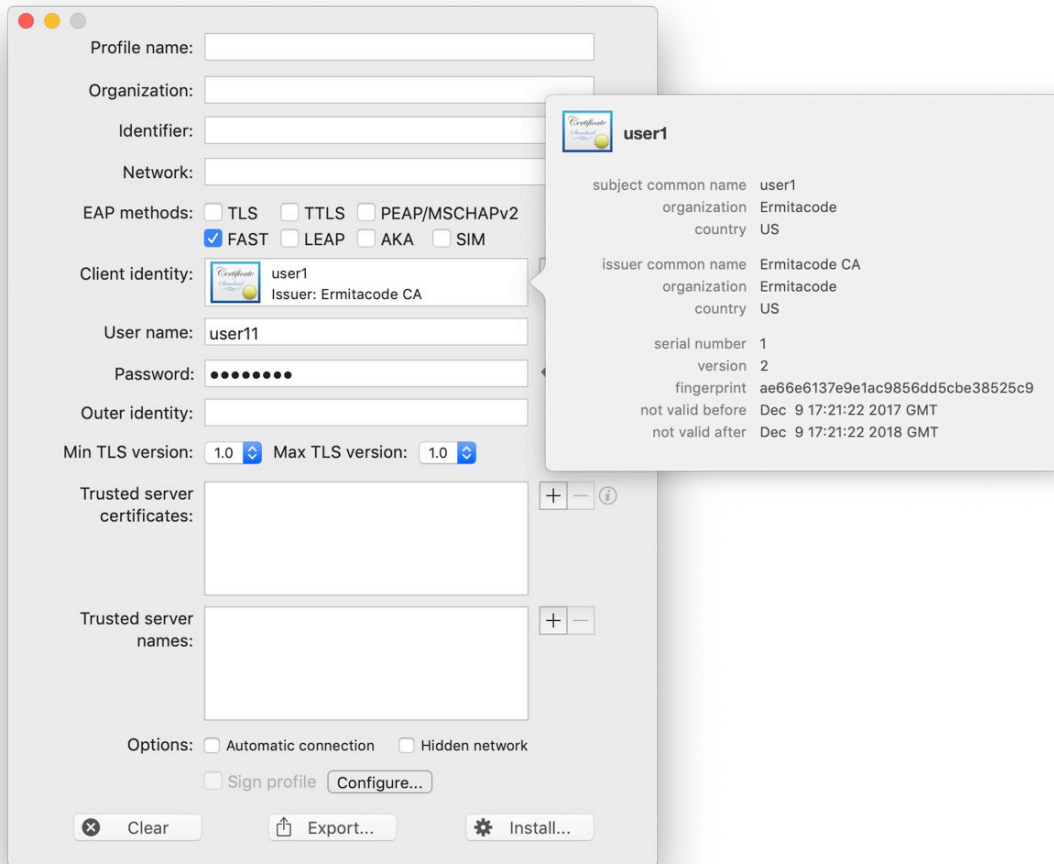
Identity access password:

If the PKCS#12 password is correctly entered, the digital identity the CN (Common Name) of the subject and the certificate issuer will be shown in the **Client identity** field.

If the PKCS#12 password is not entered, only the PKCS#12 filename will be shown in the **Client identity** field.

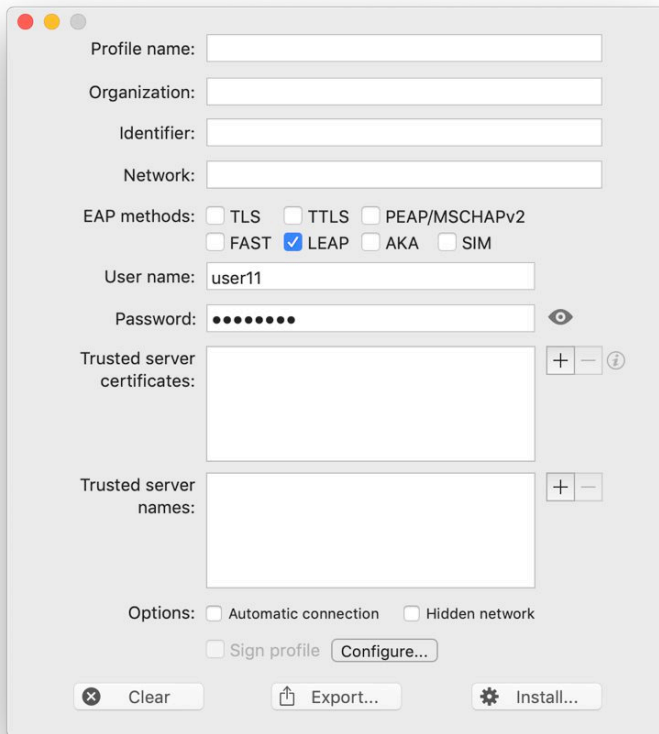
To clear the **Client identity** field click the button.

If the PKCS#12 password was supplied, you can click the ⓘ button to obtain the identity certificate information:





Configuring LEAP

For the LEAP authentication, an user credential (**User name** and **Password**) can be specified:



The screenshot shows a configuration window with the following fields and options:

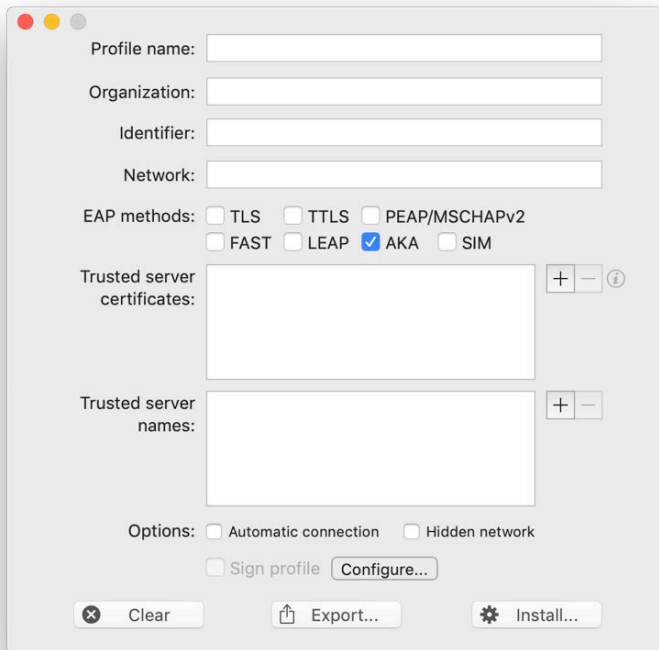
- Profile name:
- Organization:
- Identifier:
- Network:
- EAP methods: TLS TTLS PEAP/MSCHAPv2 FAST LEAP AKA SIM
- User name:
- Password: 
- Trusted server certificates: 
- Trusted server names:
- Options: Automatic connection Hidden network Sign profile
- Buttons:



You are not required to specify a **User name** and **Password**. If the LEAP credential is not included in the profile, it will be requested to the user when using the profile.

Configuring EAP-AKA

The EAP-AKA authentication method does not require additional parameters to be specified:



The image shows a configuration dialog box for EAP-AKA. It features several input fields and checkboxes. The 'EAP methods' section has 'AKA' selected. There are also sections for 'Trusted server certificates' and 'Trusted server names', each with a list box and '+' '-' buttons. At the bottom, there are 'Clear', 'Export...', and 'Install...' buttons, along with a 'Sign profile' checkbox and a 'Configure...' button.

Profile name:

Organization:

Identifier:

Network:

EAP methods: TLS TTLS PEAP/MSCHAPv2
 FAST LEAP AKA SIM

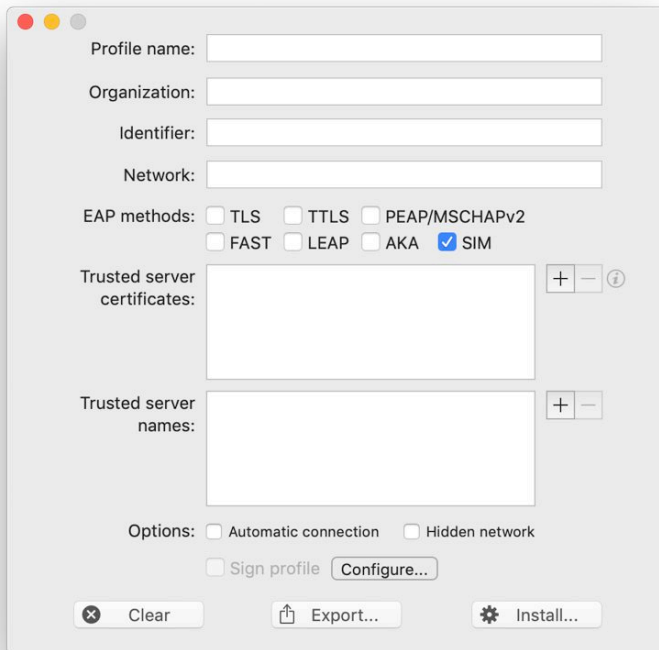
Trusted server certificates: + - ⓘ

Trusted server names: + -

Options: Automatic connection Hidden network
 Sign profile

Configuring EAP-SIM

The EAP-SIM authentication method does not require additional parameters to be specified:



The screenshot shows a configuration window for EAP-SIM. It features several input fields and checkboxes. The 'EAP methods' section has 'SIM' selected. There are also sections for 'Trusted server certificates' and 'Trusted server names', each with a list box and '+' '-' buttons. At the bottom, there are 'Options' for 'Automatic connection', 'Hidden network', and 'Sign profile', along with 'Clear', 'Export...', and 'Install...' buttons.

Profile name:

Organization:

Identifier:

Network:


EAP methods: TLS TTLS PEAP/MSCHAPv2
 FAST LEAP AKA SIM

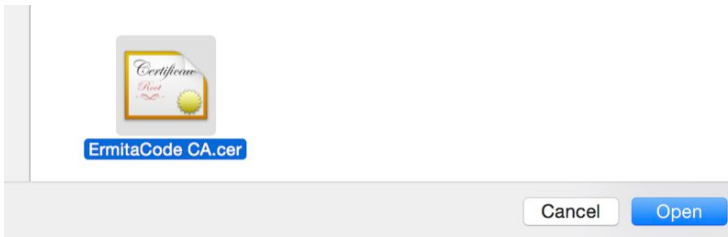
Trusted server certificates: + - ⓘ

Trusted server names: + -

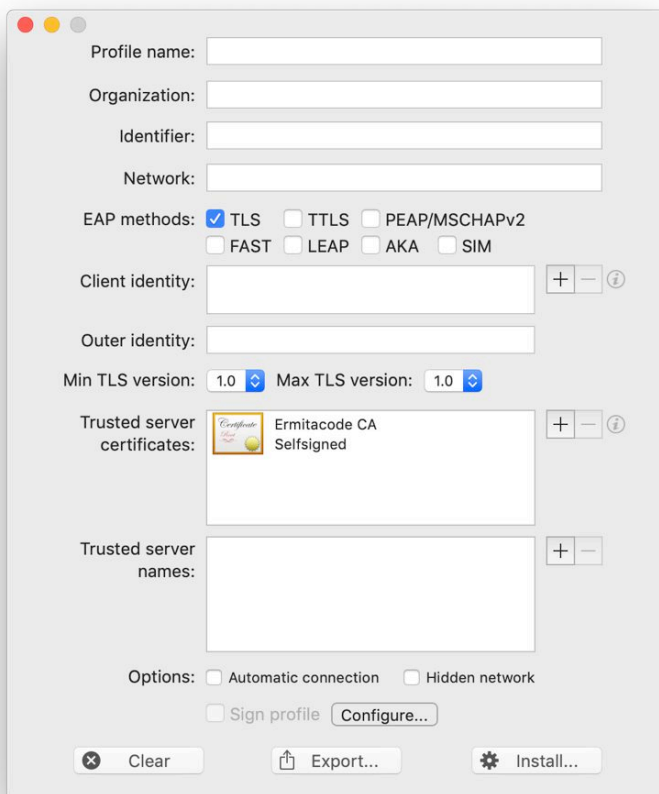
Options: Automatic connection Hidden network
 Sign profile

Configuring Trusted Servers

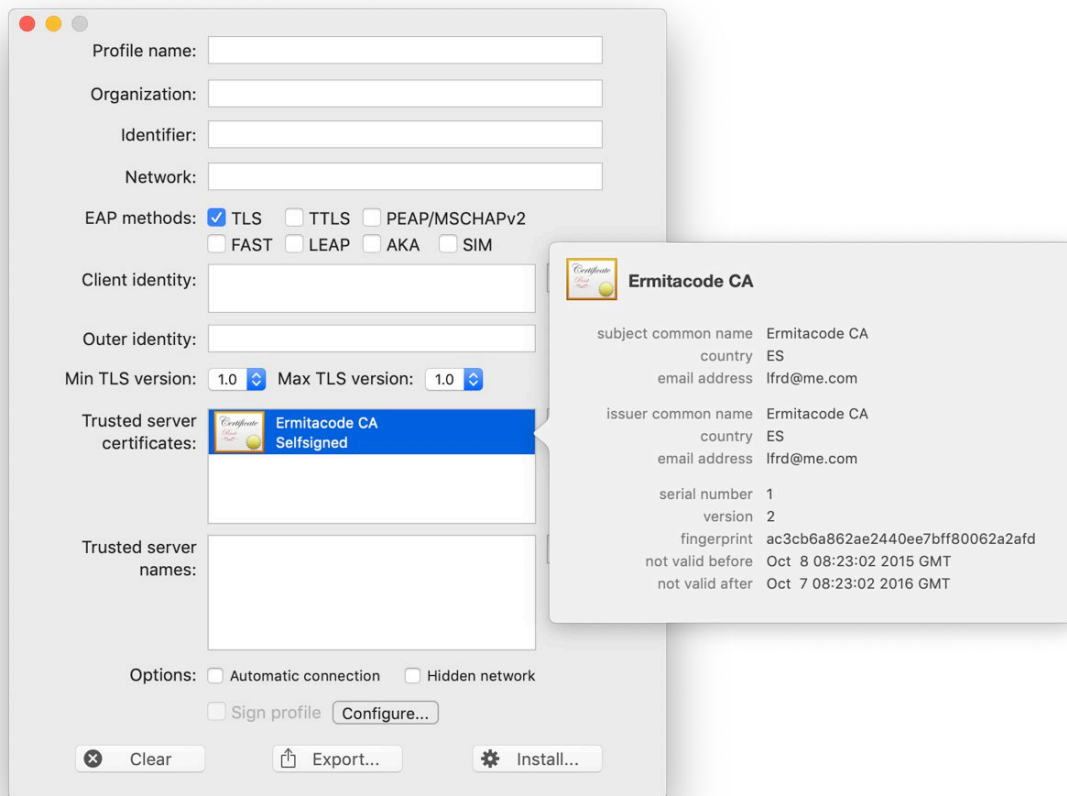
To configure the certificates accepted from authentication servers or the CA certificates signing the accepted server certificates click the  button to the right of the **Trusted server certificates** list and select a certificate file:



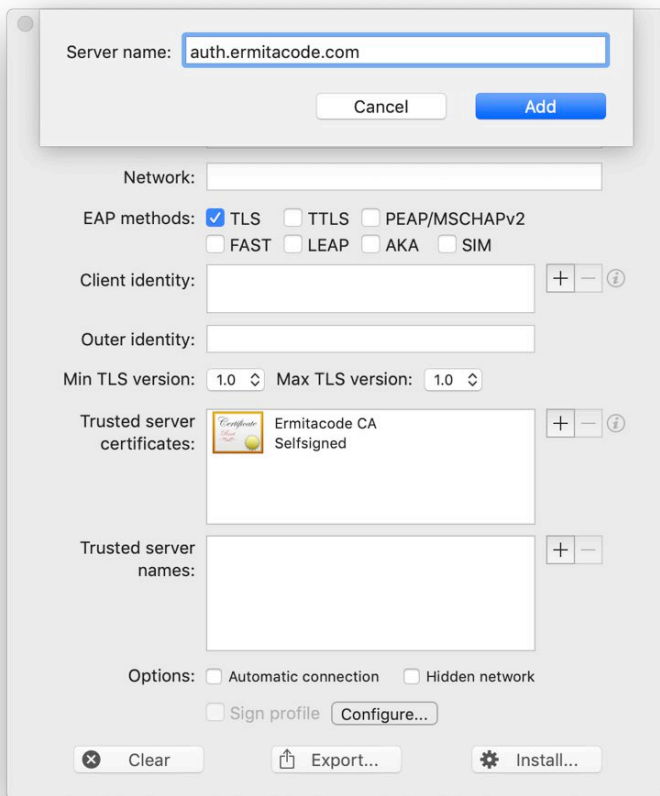
The certificate will be added to the list:



To get information of a certificate in the list select it and click the  button:



To configure the names of the certificates received from authentication servers click the **+** button to the right of the **Trusted server names** list and enter the name:



The name will be added to the list:

Profile name:

Organization:

Identifier:


Network:

EAP methods: TLS TTLS PEAP/MSCHAPv2
 FAST LEAP AKA SIM

Client identity: + - ⓘ

Outer identity:

Min TLS version: 1.0 ⓘ Max TLS version: 1.0 ⓘ

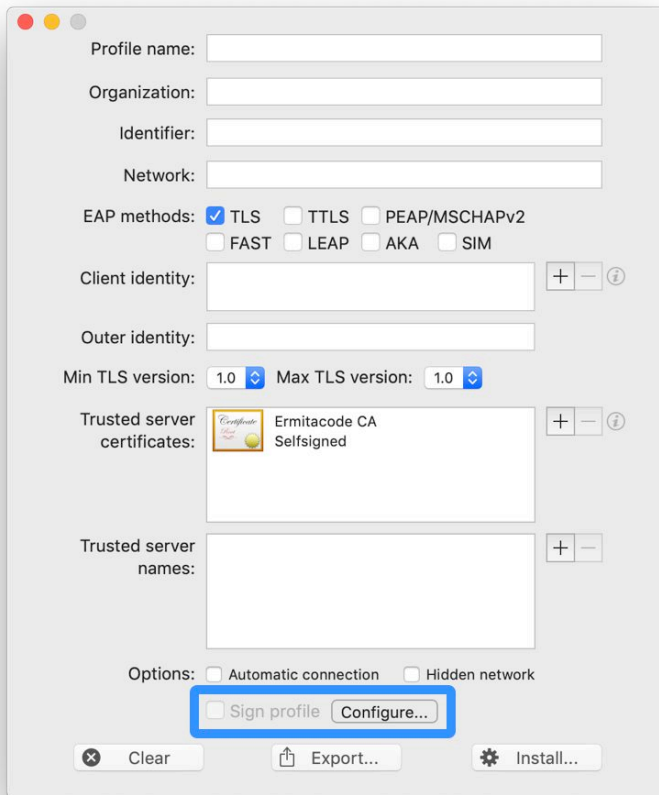
Trusted server certificates:  Ermitacode CA
Selfsigned + - ⓘ

Trusted server names: **auth.ermitacode.com** + - ⓘ

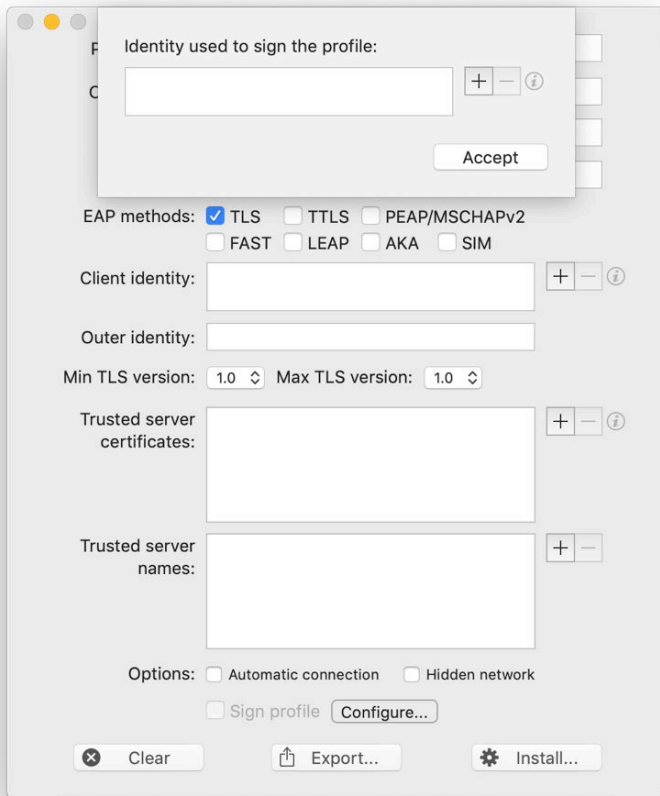
Options: Automatic connection Hidden network
 Sign profile

Signing Profiles

Dot1xProfile can optionally sign the generated profiles. The **Sign profile** check box enables or disables profile signing:

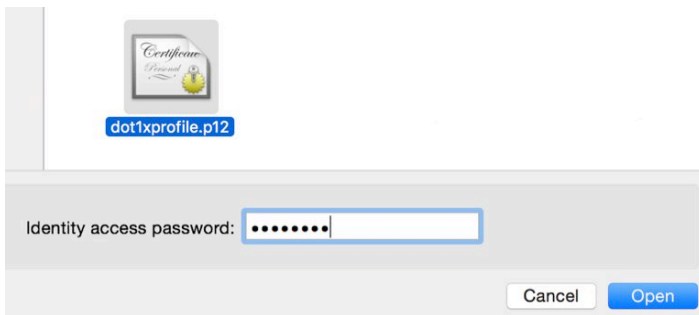


To configure the digital identity used to sign the profiles click the **Configure...** button:



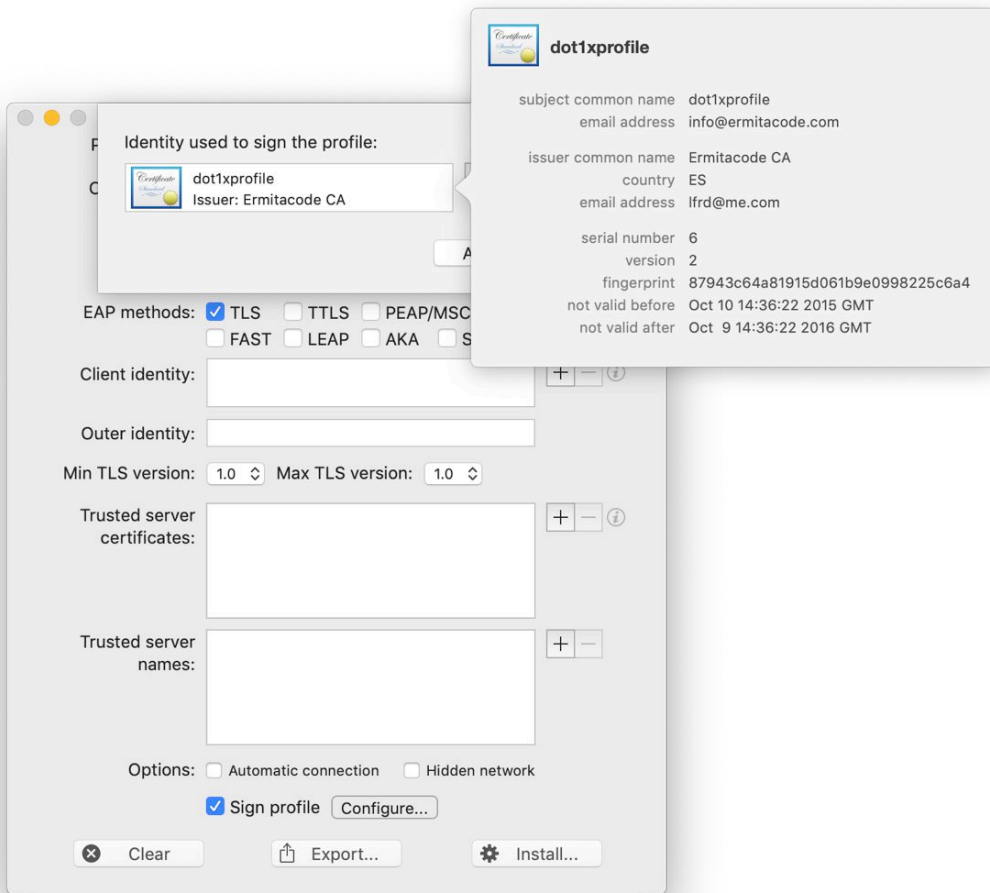
Click the **+** button and select a PKCS#12 (Personal Information Interchange) file. This file should have file PKCS12, P12 or PFX extension.

PKCS#12 files are protected by a password which should be entered in the file selection panel:



To clear the signing identity click **-** the button.

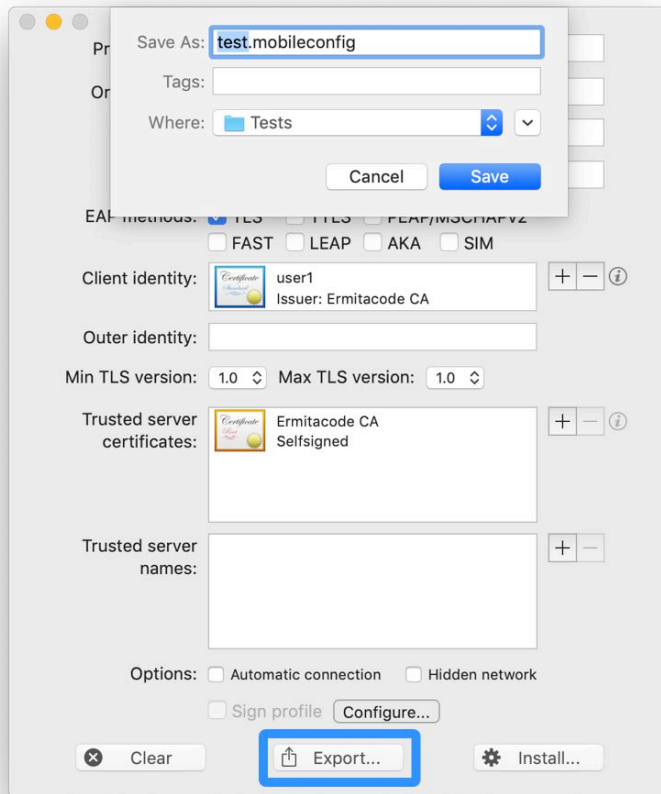
You can click the **i** button to obtain the identity certificate information:



Exporting Profiles

You can export the 802.1x profile to a mobileconfig file for later installation or for distribution to other machines.

To export the profile click the **Export...** button or select the **File>Export Profile...** menu option:



The generated profile will optionally be signed if a signing identity is configured in the Preferences Panel.

You also can directly install the profile in the local Mac without generating a *mobileconfig* file.

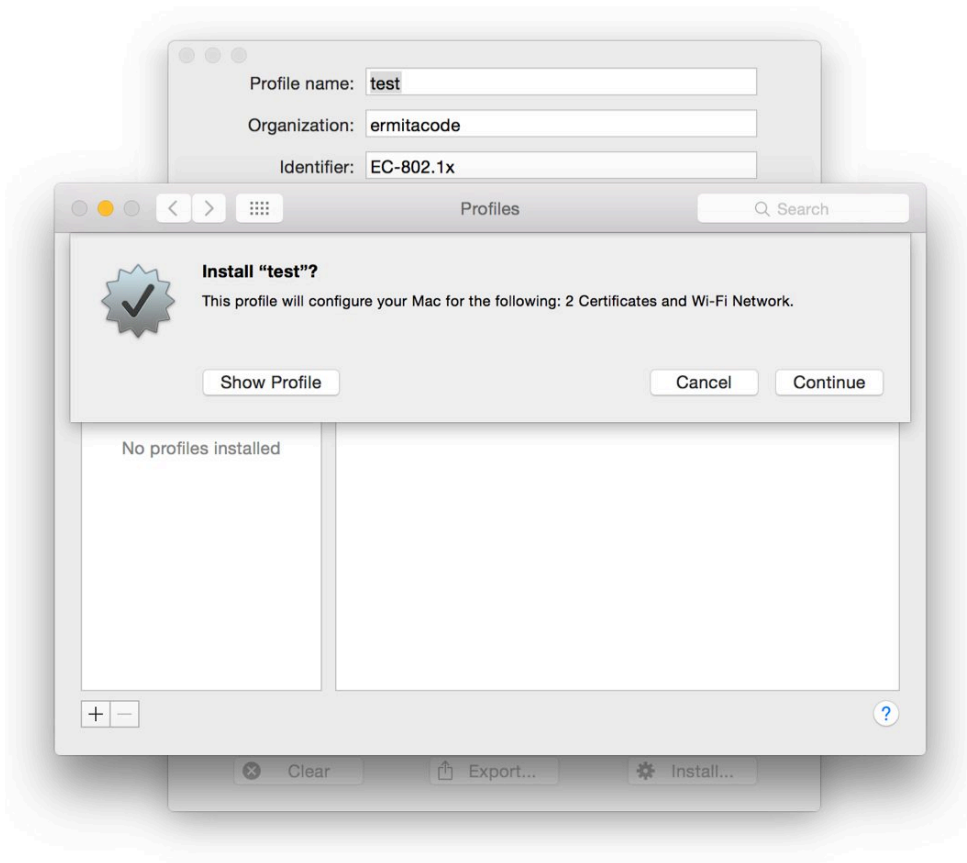


Installing Profiles

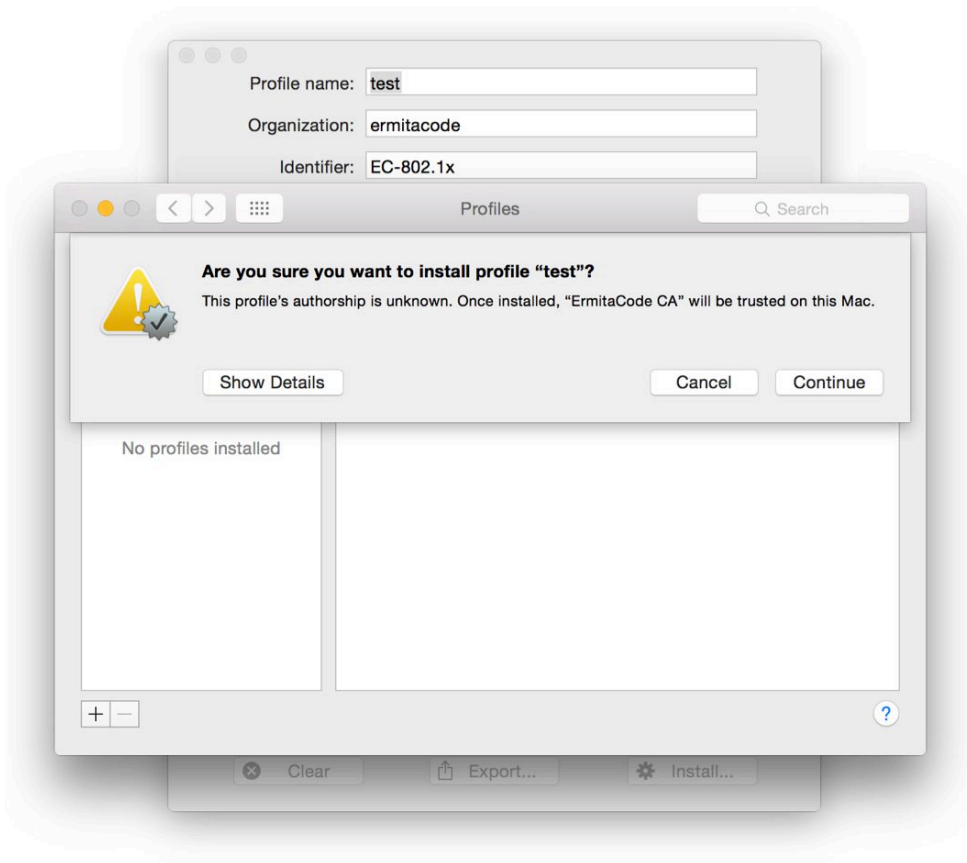
To install the 802.1x profile in the local Mac click the **Install...** button or select the **File>Install Profile...** menu option:

The generated profile will optionally signed if a signing identity is configured in the Preferences Panel.

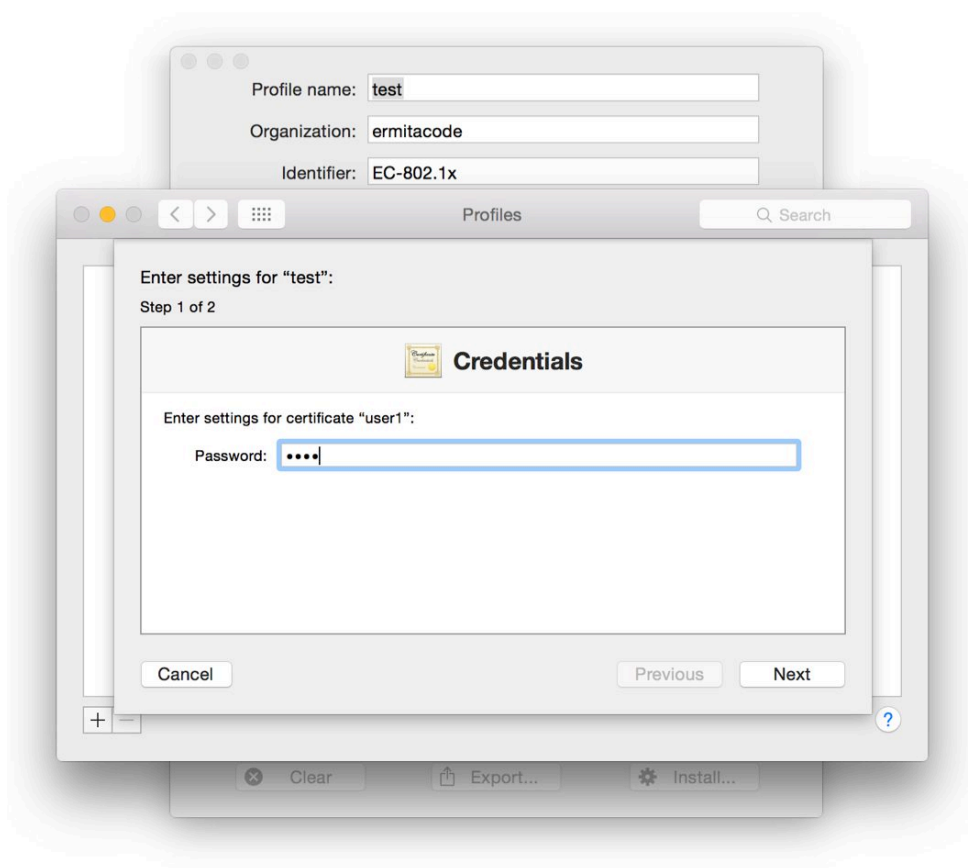
Dot1xProfile starts the OSX System Preferences to install the profile:



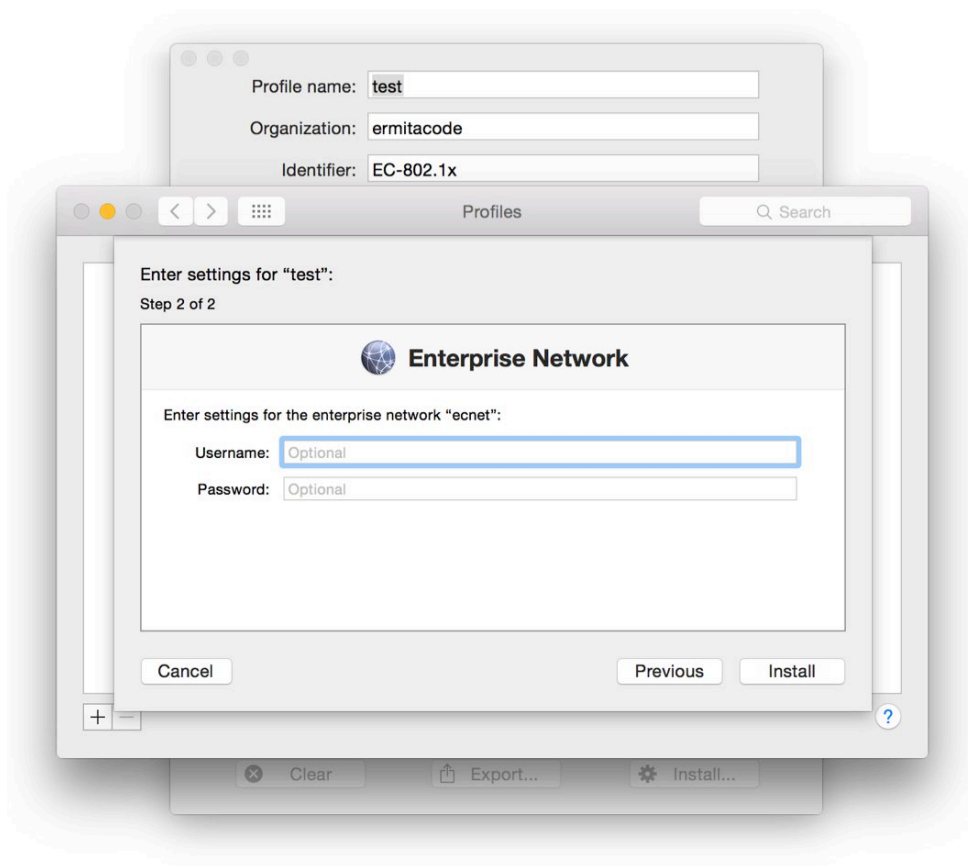
Click **Continue**:



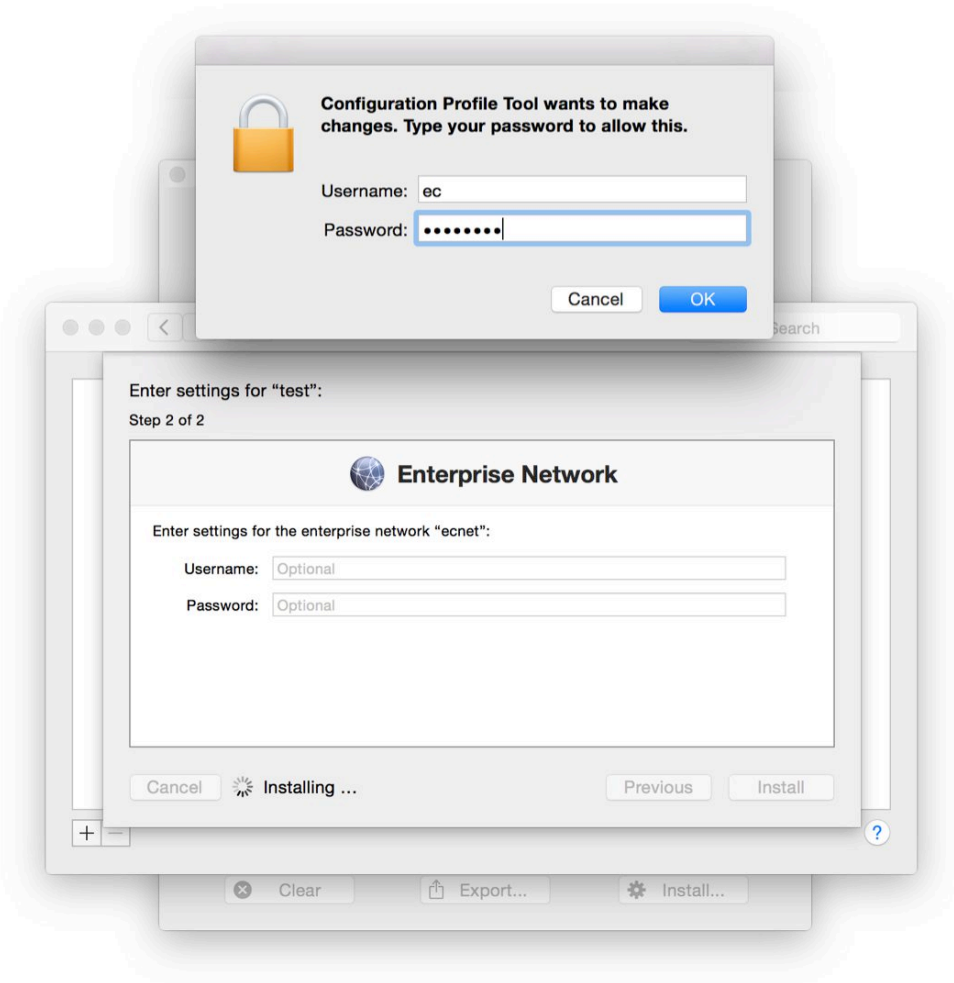
Click **Continue**. If TLS method is selected in the profile, the password to access the PKCS#12 digital identify is requested:



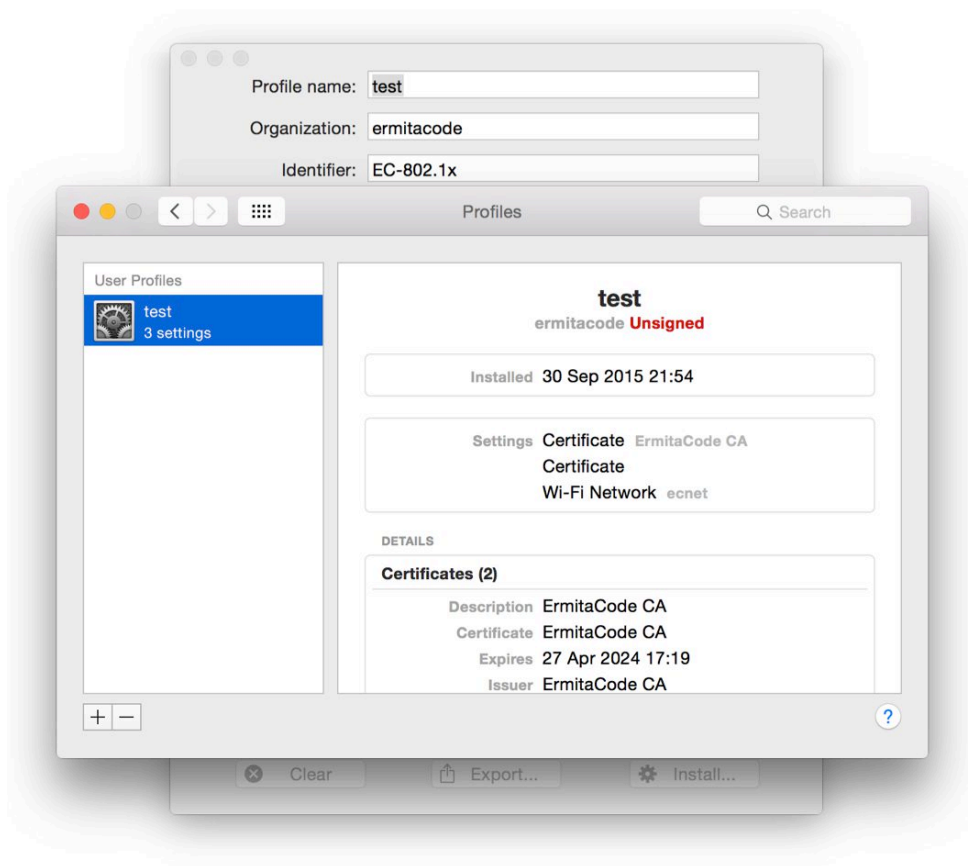
If TTLS or PEAP method is selected in the profile, the username and password to be used to authenticate to the network using this profile are requested. You can skip entering this information. In this case, username and password will be requested at the time of authenticating in the network with this profile:



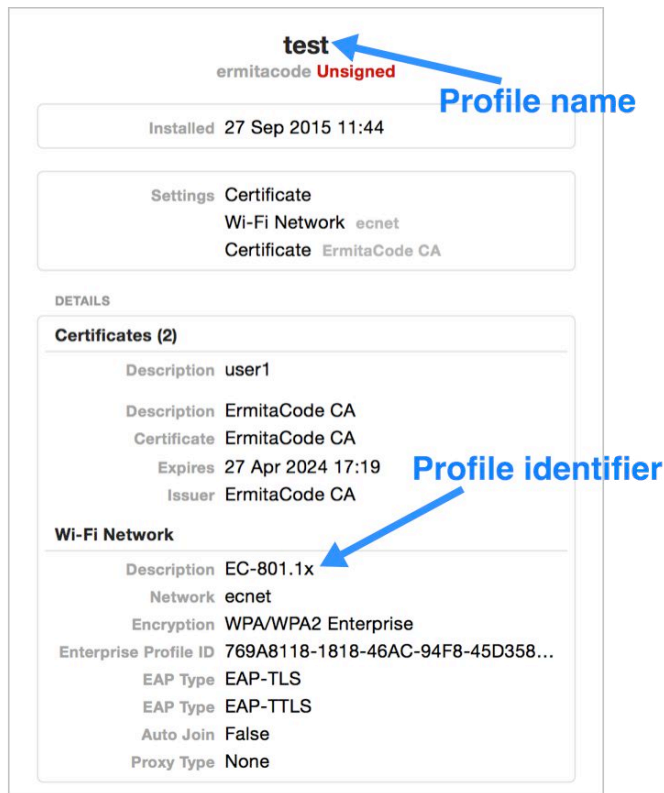
Finally, your system password is requested to complete profile installation:



If the profile is correctly installed, it will be added to the list of profiles:



The OSX System Preferences will show the information of the installed profile:



The **Profile identifier** entered into the Dot1xProfile window is shown as *Description* and will identify the 802.1x profile in the System Preferences **Network** section when it is used to perform authentication in a network.

If a signing identity has been configured in the Preferences panel, the installed certificate will be signed and the indication to the

right of the organization name will be **Verified** instead of **Unsigned**:

