

EAPTest 3.0



Table of Contents

EAPTest User Manual	2
Using EAPTest	3
Verifying Connectivity	5
Adding RADIUS Attributes	6
Removing RADIUS Attributes	7
Modifying RADIUS Attributes	8
Test modes	9
Authentication Tests	10
Authentication Methods	11
Using PAP Method	12
Using TTLS Method	13
Using PEAP Method	14
Using TLS Method	15
Using MSCHAPv2 Method	16
Using MD5 Method	17
Using GTC Method	18
Protocol Tests	19
Performance Tests	22
Performance Reports	24
Accounting Tests	26
Session Tests	28
Using Profiles	31
Saving Profiles	32
Loading Profiles	33
Deleting Profiles	34
Exporting Profiles	35
Importing Profiles	36
Saving to an Image File	37
Printing	38
Managing Dictionaries	39
Importing Dictionaries	40
Removing Dictionaries	41
Resetting the Database	42



EAPTest User manual

EAPTest performs testing of RADIUS servers using common Extended Authentication Protocol (EAP) methods.

The tool implements 3 test modes: Authentication, Accounting and Session tests. For Authentication mode, 3 tests are available: Protocol Test, Performance Test and Performance Report. Using the first 3 tests you can see the messages interchanged with the authentication server, the Performance tests allow testing server performance under different traffic loads.

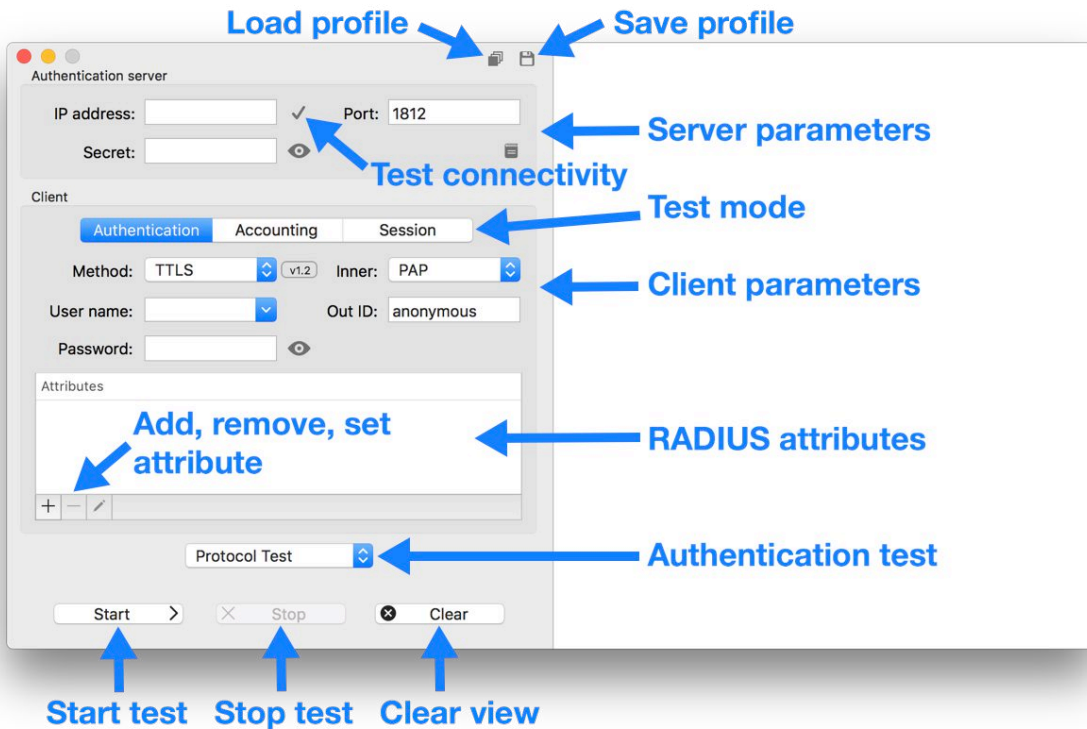
EAP methods supported are TTLS, PEAP, MSCHAPv2, MD5 and GTC. For TTLS is possible to use PAP, CHAP, MSCHAP, MSCHAPv2, MD5 and GTC as inner methods. For PEAP, the inner methods supported are MSCHAPv2, MD5 and GTC. In addition to EAP methods, the PAP protocol is also implemented.

@ermita@code


www.ermitacode.com

Using EAPTest

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



The parameters are divided in 2 areas:

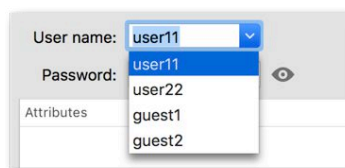
- **Authentication Server:** enter the **IP address** (or DNS name) of the server perform authentication, the **Port** number used by the RADIUS service and the RADIUS **Secret** configured in the server for this client. The **Test connectivity** button allows you to verify the network connectivity to the server. You can click the  button to manage the RADIUS attributes database dictionaries.
- **Client:** the contents depends on the **Test mode** selected. For **Authentication** test mode: the **Auth method** (PAP and the EAP methods TTLS, PEAP, MSCHAPv2, MD5 or GTC) and the **Inner authentication** method for TTLS or PEAP. Possible Inner methods for EAP TTLS are PAP, CHAP, MSCHAP, MSCHAPv2, MD5 and GTC. Available Inner methods for EAP PEAP are MSCHAPv2, MD5 and GTC. Enter the credentials (**User name** and **Password**) to be authenticated and optionally the **Out ID** (outer identity) sent in tunneled EAP methods (TTLS and PEAP).

For methods using TLS (TTLS, PEAP and TLS) it is possible to select the TLS version:



You can select a specific version (v1, v1.1 or v1.2) or select **Max** to use the maximum version supported by the authentication server.

The different user names used in tests are available for later use in the **User name** dropdown list:



The user list can be cleared using the **Edit>Clear Users** main menu option.

Additionally to PAP, the following EAP methods are supported:

TTLS. Inner methods: PAP, CHAP, MSCHAP, MSCHAPv2, MD5, GTC

PEAP. Inner methods: MSCHAPv2, MD5, GTC

TLS

MSCHAPv2

MD5

GTC



Accounting protocol tests and full session tests can be performed using the **Accounting** and **Session** test modes.

Using the buttons below the RADIUS attributes you can add an attribute to the list of attributes to be sent in the RADIUS messages, remove an attribute or modify an attribute value.

For Authentication mode, below the client parameters area is located the **Authentication test** selection popup menu allowing to choose the test mode:

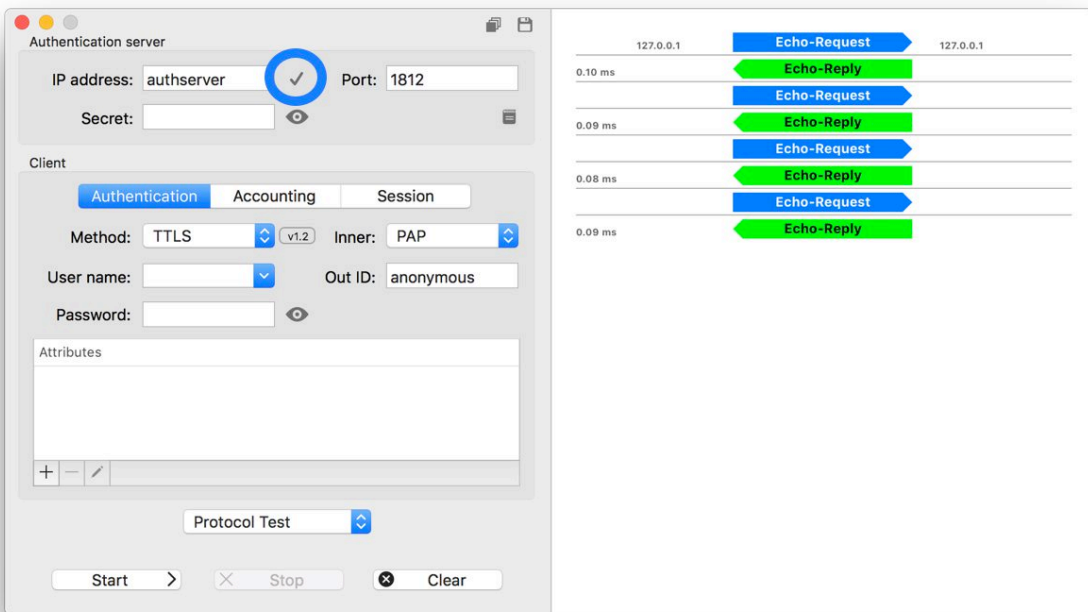
- **Protocol Test:** observe RADIUS messages interchanged with the authentication server.
- **Performance Test:** test server performance under different traffic loads.
- **Performance Report:** compare server performance under different traffic loads.

After defining the authentication parameters and selecting the test mode you can perform the test using the **Start Test** button. You can abort a running test using the **Stop Test** button. The **Clear View** button clears the information displayed in the protocol view.

Test parameters including can be saved to a profile for later retrieval. Profiles allow you to have different configurations of test parameters and load a specific profile when needed. You can access this functions through the buttons  and  located at the top of the window.

Verifying Connectivity

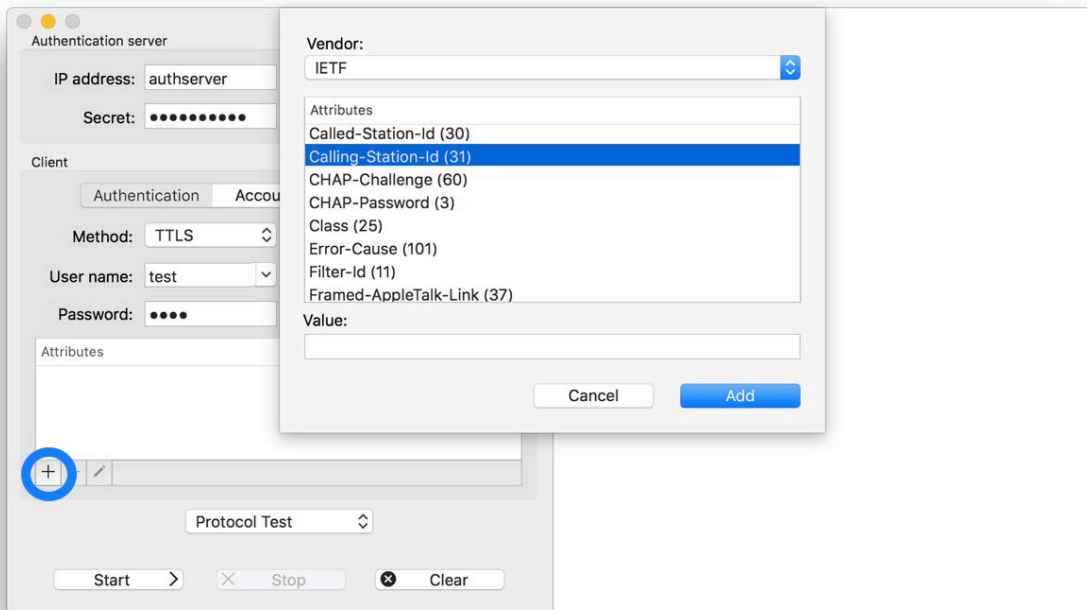
To check the network connectivity to the Authentication Server using an ICMP echo request click the ✓ button located to the right of the **Authentication server IP address**.



The screenshot displays a network configuration interface with two main panels. The left panel, titled "Authentication server", contains fields for "IP address" (set to "authserver") and "Port" (set to "1812"). A blue circle highlights a checkmark button next to the IP address field. Below these are fields for "Secret" and "Client" settings, including "Method" (TTLS), "Inner" (PAP), "User name", and "Password". The right panel shows a network diagram with two nodes labeled "127.0.0.1". It displays a sequence of "Echo-Request" (blue arrows) and "Echo-Reply" (green arrows) packets between the nodes, with response times of 0.10 ms, 0.09 ms, 0.08 ms, and 0.09 ms.

Adding RADIUS Attributes

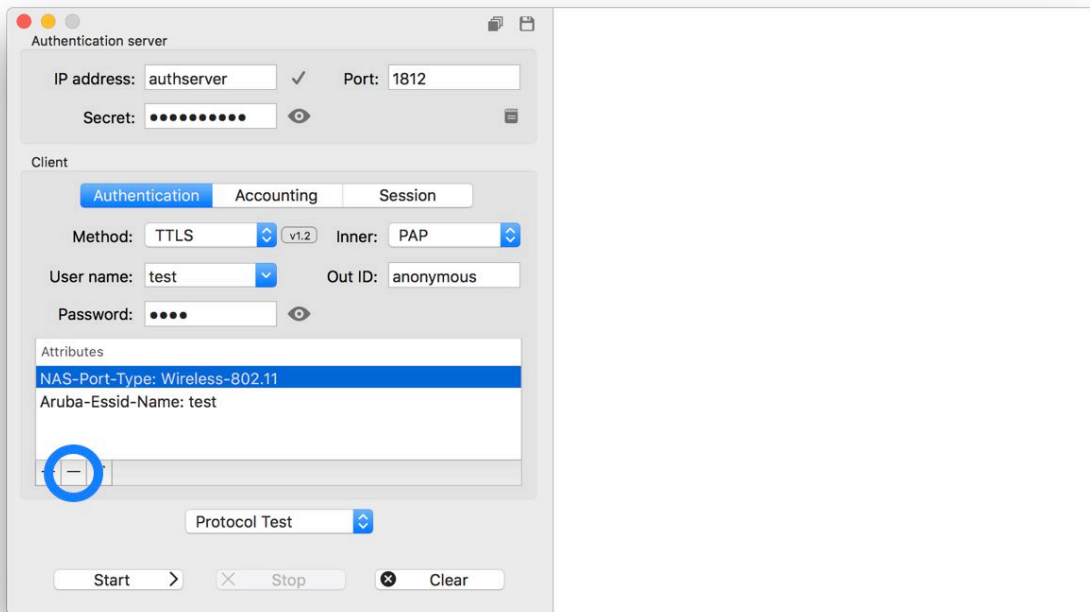
To add a new RADIUS attribute to be sent to the authentication server click the  button below the **Attributes** list.



Select the **Vendor**, select the attribute name in the **Attributes** list, enter a **Value** for the attribute and press the **Add** button. The new added attribute name and value will be shown in the **Attributes** list.

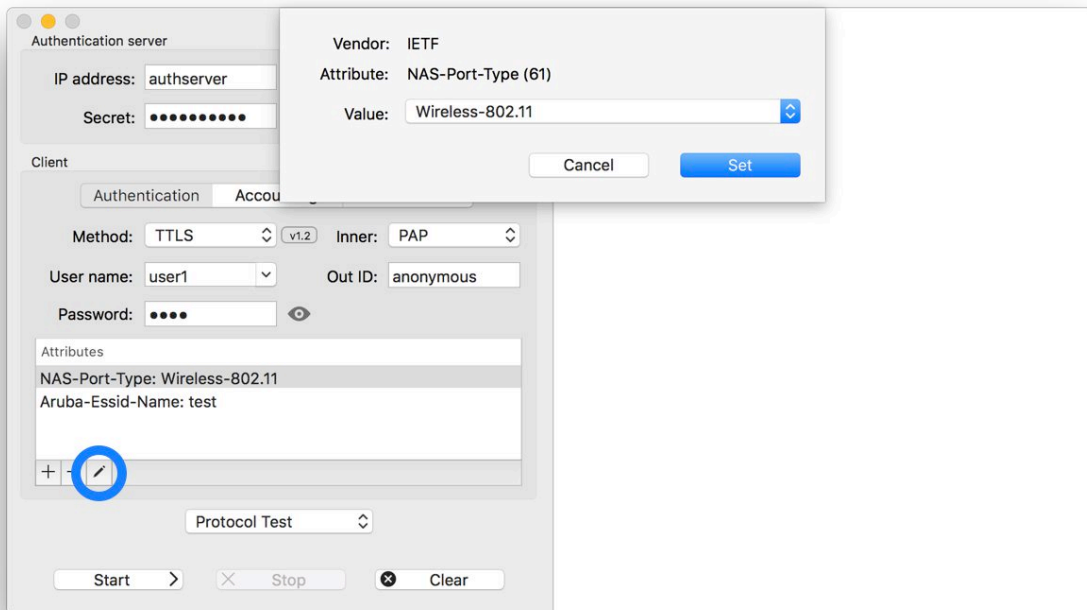
Removing RADIUS Attributes

To remove an attribute from the **Attributes** list select it and click the  button.



Modifying RADIUS Attributes

To modify the value assigned to a previously added attribute select it in the **Attributes** list and click the  button.



Enter a new **Value** for the attribute and press the **Set** button.



Test modes

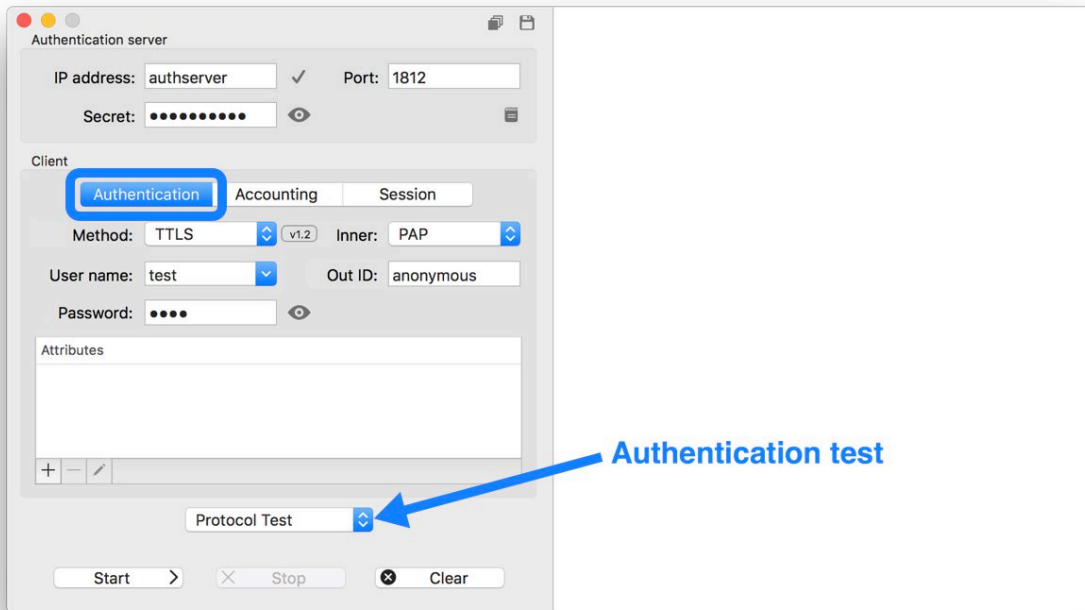
3 test modes are available:

- Authentication. This mode permits displaying the RADIUS authentication messages interchanged with the authentication server or test server performance under different traffic loads.
- Accounting. This mode permits allows to you send RADIUS accounting to the authentication server.
- Session. This mode simulates a complete RADIUS client session by performing authentication, accounting (Start, Updates and Stop) and receiving dynamic RADIUS messages (Disconnect and Change of Authorization)-

Mode selection is down using the **Test mode** selector (see Using EAPTest).

Authentication Tests

To perform Authentication Tests select **Authentication** in the test mode selector or select the **File>Test>Authentication** main menu option:



3 Authentication test modes are available using the **Authentication test** selector:

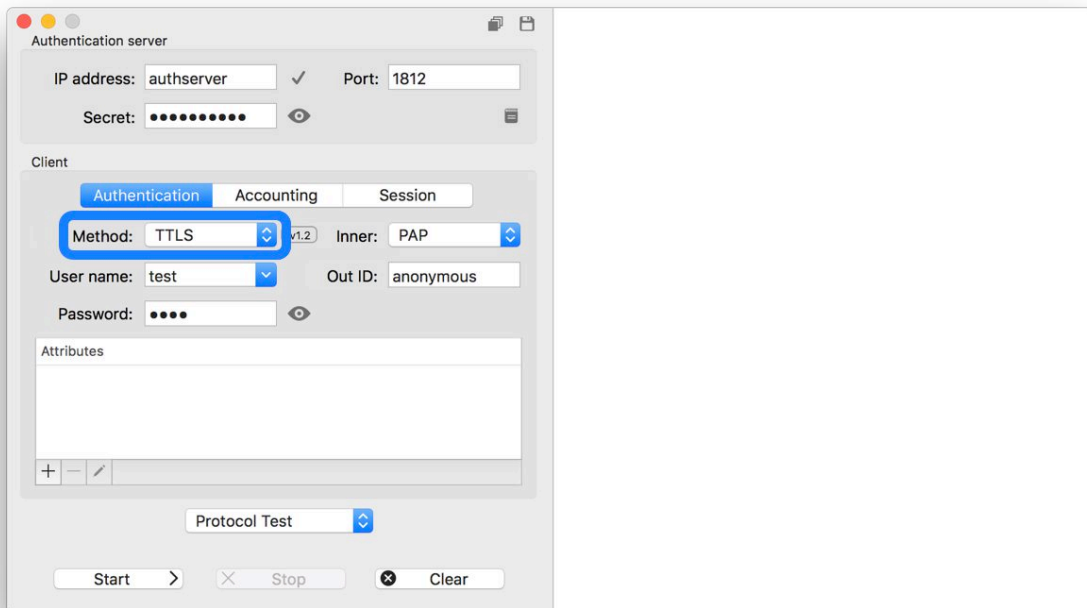
- Protocol Test.
- Performance Test.
- Performance Report.

To perform Authentication tests you should configure the Authentication method to be used. The following methods are supported:

- PAP
- TTLS
- PEAP
- TLS
- MSCHAPv2
- MD5
- GTC

Authentication Methods

Authentication tests require an Authentication method to be selected:



The following methods are available:

- PAP
- TTLS
- PEAP
- TLS
- MSCHAPv2
- MD5
- GTC

Using PAP Method

Select **PAP** in the in the **Auth method** popup button. The PAP fields will be shown:



The screenshot shows a configuration form for the PAP method. It contains three fields: 'Method' set to 'PAP', 'User name' set to 'test', and 'Password' masked with four dots. Each field has a dropdown arrow on its right side, and there is an eye icon to the right of the password field to toggle visibility.

This method will use the specified **User name** and **Password** credentials to authenticate.

Yo can clear the las used credentials stored in the **User name** field using the **Edit>Clear Users** main menu option.

Using TTLS Method

Select **TTLS** in the in the **Auth method** popup button. The TTLS fields will be shown:



The screenshot shows a configuration window for the TTLS method. It contains the following fields:

- Method:** A dropdown menu set to "TTLS" with a "v1.2" version indicator.
- Inner:** A dropdown menu set to "PAP".
- User name:** A text input field containing "test".
- Out ID:** A text input field containing "anonymous".
- Password:** A text input field with four dots, and an eye icon to toggle visibility.

TTLS creates a secure SSL Tunnel to send the user credentials. Inside the Tunnel, the credentials are sent using an Inner (tunneled) Authentication Method. This method is selected using the **Inner auth** popup menu. Supported Inner Methods are: PAP, CHAP, MSCHAP, EAP-MSCHAPv2, EAP-MD5 and EAP-GTC.

These Inner methods will use the **User name** and **Password** credentials to authenticate.

An **Out ID** user name can be specified to avoid sending the real User Name in the non secured RADIUS attribute outside the SSL Tunnel. The Outer ID field can also be used to specify domain information (for example: anonymous@somedomain.com) to enable RADIUS proxying to the remote servers managing external domains.

You can clear the last used credentials stored in the **User name** field using the **Edit>Clear Users** main menu option.

Using PEAP Method

Select **PEAP** in the in the **Auth method** popup button. The PEAP fields will be shown:



Method:	PEAP	v1.2	Inner:	MSCHAPv2
User name:	test		Out ID:	anonymous
Password:			

PEAP creates a secure SSL Tunnel to send the user credentials. Inside the Tunnel, the credentials are sent using an Inner (tunneled) EAP Method. This method is selected using the **Inner auth** popup menu. Supported Inner EAP Methods are: EAP-MSCHAPv2, EAP-MD5 and EAP-GTC.

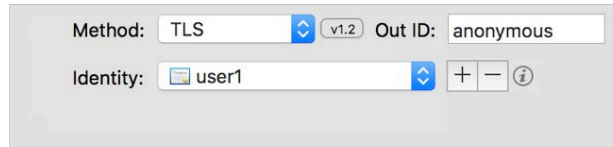
These Inner methods will use the **User name** and **Password** credentials to authenticate.

An **Out ID** user name can be specified to avoid sending the real User Name in the non secured RADIUS attribute outside the SSL Tunnel. The Outer ID field can also be used to specify domain information (for example: anonymous@somedomain.com) to enable RADIUS proxying to the remote servers managing external domains.

Yo can clear the las used credentials stored in the **User name** field using the **Edit>Clear Users** main menu option.

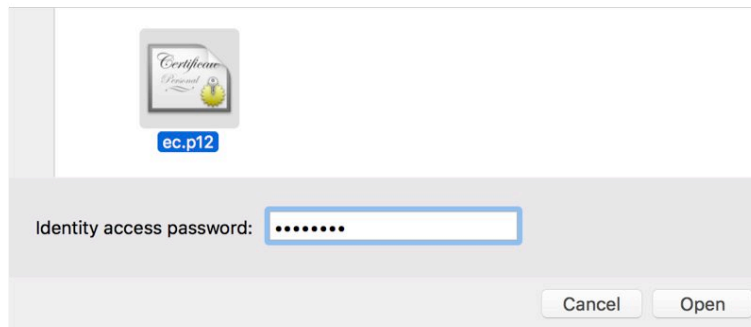
Using TLS Method

Select **TLS** in the in the **Auth method** popup button. The TLS fields will be shown:



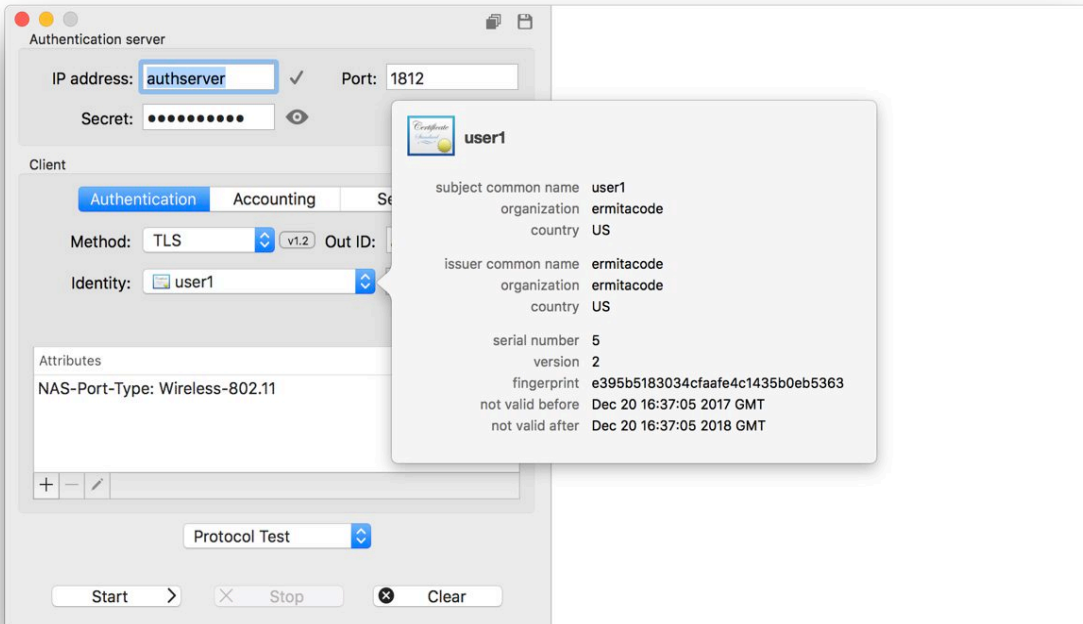
TLS authenticates using a User Digital Identity and sending its Digital Certificate to the RADIUS Server through a TLS session.

To add a Digital Identity to use in the authentication click in 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:



An **Out ID** user name needs to be specified to send the real User Name in the non secured RADIUS attribute outside the TLS session. The Outer ID field can also be used to specify domain information (for example: anonymous@somedomain.com) to enable RADIUS proxying to the remote servers managing external domains. To remove the actually used Identity click the **-** button.

The **Identity** field shows the Common Name (CN) of the actually used identity and the issuer. Click the **i** button to open a popover showing more information about the digital Identity:



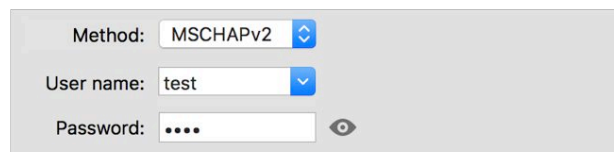
The screenshot shows the 'Authentication server' configuration window. The 'Client' tab is active, showing 'Method: TLS' and 'Identity: user1'. A popover window is open over the 'Identity' field, displaying the following certificate details:

subject common name	user1
organization	ermitacode
country	US
issuer common name	ermitacode
organization	ermitacode
country	US
serial number	5
version	2
fingerprint	e395b5183034cfaafe4c1435b0eb5363
not valid before	Dec 20 16:37:05 2017 GMT
not valid after	Dec 20 16:37:05 2018 GMT

You can clear the last used identities stored in the **Identity** field using the **Edit > Clear Identities** main menu option.

Using MSCHAPv2 Method

Select **MSCHAPv2** in the in the **Auth method** popup button. The MSCHAPv2 fields will be shown:



The screenshot shows a configuration window for MSCHAPv2 authentication. It contains three fields: 'Method' set to 'MSCHAPv2', 'User name' set to 'test', and 'Password' masked with four dots. Each field has a small blue dropdown arrow on its right side. To the right of the password field is an eye icon for toggling visibility.

This method will use the specified **User name** and **Password** credentials to authenticate.

Yo can clear the las used credentials stored in the **User name** field using the **Edit>Clear Users** main menu option.



Using MD5 Method

Select **MD5** in the in the **Auth method** popup button. The MD5 fields will be shown:

A screenshot of a configuration window for the MD5 authentication method. It contains three fields: 'Method' with a dropdown menu set to 'MD5', 'User name' with a dropdown menu set to 'test', and 'Password' with a text input field containing four dots and a toggle eye icon to the right.

This method will use the specified **User name** and **Password** credentials to authenticate.

You can clear the last used credentials stored in the **User name** field using the **Edit>Clear Users** main menu option.

Using GTC Method

Select **GTC** in the in the **Auth method** popup button. The GTC fields will be shown:



The screenshot shows a configuration dialog box with three fields:

- Method:** A dropdown menu with "GTC" selected.
- User name:** A text input field containing "test".
- Password:** A text input field with four dots, and an eye icon to its right for toggling visibility.

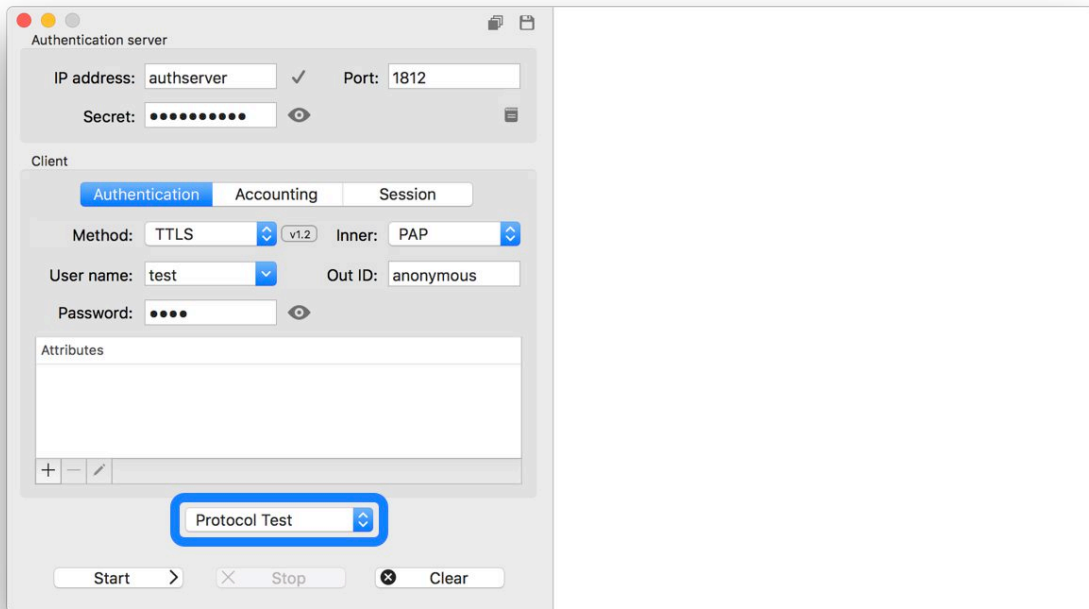
This method will use the specified **User name** and **Password** credentials to authenticate.

Yo can clear the las used credentials stored in the **User name** field using the **Edit>Clear Users** main menu option.

Protocol Tests

Authentication Protocol tests generate individual authentication to the authentication server. Protocol messages interchanged with the authentication server are shown in the right view of the EAPTest window.

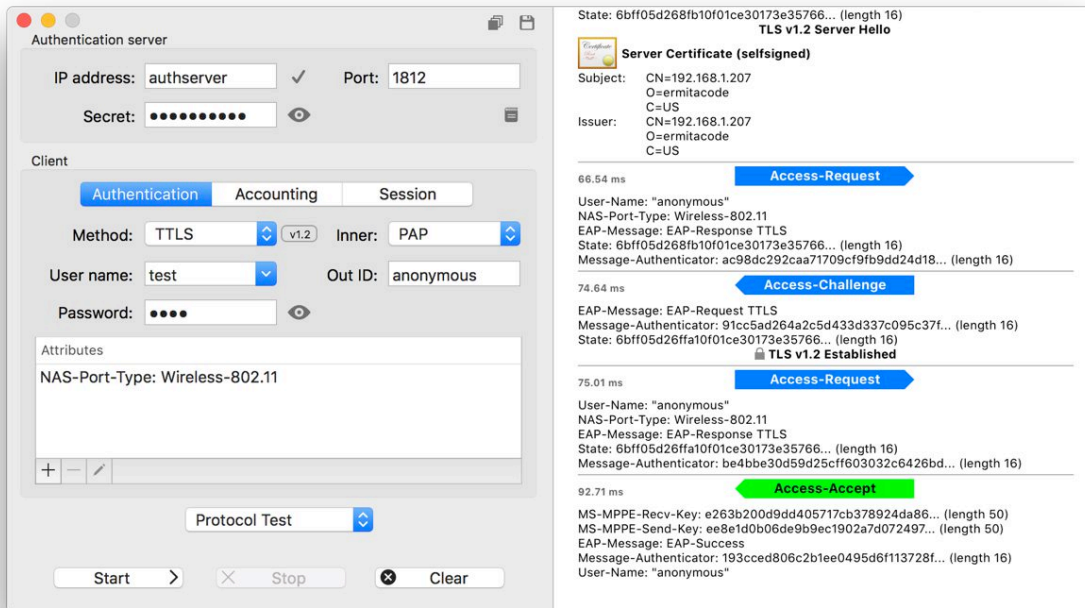
To perform protocol tests select **Protocol Test** in the Authentication test mode selection popup menu or select **File>Authentication Test>Protocol Test** main menu option:



To start the test click the **Start** button or select the **File>Start Test** menu option (keyboard shortcut: ⌘R).

To stop an authentication before it has been completed click the **Stop** button or select the **File>Stop Test** menu option (keyboard shortcut: ⌘T).

During the authentication the right area of the window displays the RADIUS messages being interchanged and the RADIUS attributes included in the messages. In the following figure a TTLS/PAP authentication is shown:



The following messages are shown:

- **Access-Request** message sent to the server:

32.03 ms **Access-Request**

User-Name: "anonymous"
 NAS-Port-Type: Wireless-802.11
 EAP-Message: EAP-Response TTLS
 EAP-Message: 1a0016000e000d000b000c0009000a... (length 60)
 State: 97d3a20096d1b7938bcc52777db1af... (length 16)
 Message-Authenticator: 514711ef48f47f88ba966b2ae7479e... (length 16)
TLS v1.2 Client Hello

- **Access-Challenge** message received from the server:

74.64 ms **Access-Challenge**

EAP-Message: EAP-Request TTLS
 Message-Authenticator: 91cc5ad264a2c5d433d337c095c37f... (length 16)
 State: 6bff05d26ffa10f01ce30173e35766... (length 16)
TLS v1.2 Established

- **Access-Accept** message received from the server:

92.71 ms **Access-Accept**

MS-MPPE-Recv-Key: e263b200d9dd405717cb378924da86... (length 50)
 MS-MPPE-Send-Key: ee8e1d0b06de9b9ec1902a7d072497... (length 50)
 EAP-Message: EAP-Success
 Message-Authenticator: 193cced806c2b1ee0495d6f113728f... (length 16)
 User-Name: "anonymous"

- **Access-Reject** message received from the server:

84.50 ms **Access-Reject**

EAP-Message: EAP-Failure
 Message-Authenticator: 0cee804ef878ba6a5729cd398daaea... (length 16)

- When the expected message is not received from the authentication server in response to an **Access-Request** message sent, the message is resent several times:

3.01 sec

Access-Request

User-Name: "anonymous"
NAS-Port-Type: Wireless-802.11
EAP-Message: EAP-Response Identity
Message-Authenticator: 43e3e13b0789af2d58499ef1f3beec... (length 16)

- If the response timer expires without server response the following indication is shown:

Timeout

You can stop the authentication using the **Stop** button or selecting the **File>Stop Test** menu option.

For SSL based methods (TTLS, PEAP and TLS) a server certificate is sent from the authentication server. This certificate or certificate chain is displayed below the RADIUS attributes of the message:

63.53 ms

Access-Challenge

EAP-Message: EAP-Request TTLS
Message-Authenticator: 8c3e544b25b93b9db5407a45e2df10... (length 16)
State: 97d3a20094d7b7938bcc52777db1af... (length 16)
TLS v1.2 Server Hello



Server Certificate (selfsigned)

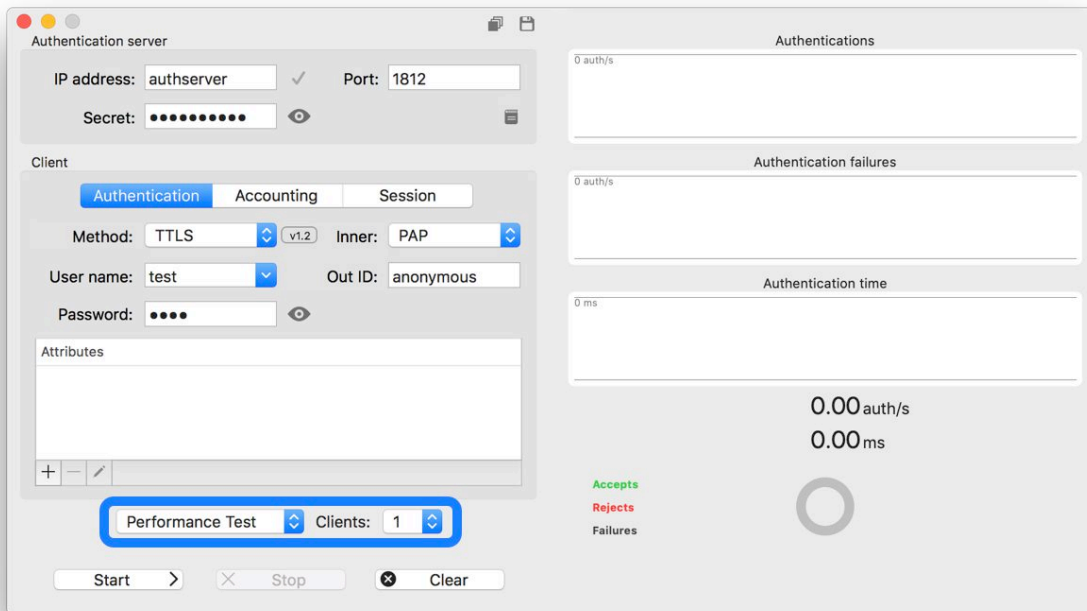
Subject: CN=192.168.1.207
O=ermitacode
C=US
Issuer: CN=192.168.1.207
O=ermitacode
C=US

To clear the content of the view click the **Clear** button or select the **File>Clear View** menu option.

Performance Tests

Performance Tests performs automatically repeated Performance Tests with different number of concurrent clients to test server performance under different traffic loads.

To start an authentication test select **Performance Test** in the test mode selection popup menu or select the **File>Authentication Test>Performance Test** main menu option:



To start the test click the **Start** button or select the **File>Start Test** menu option (keyboard shortcut: ⌘R).

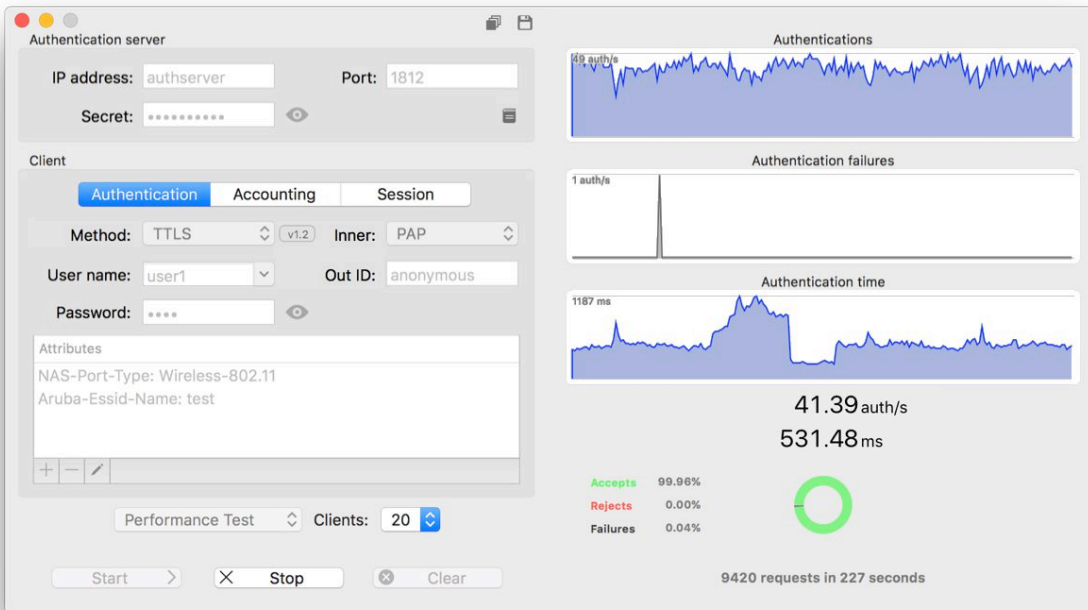
When you select the Performance Test mode the **Clients** popup menu is displayed. This menu allows you to select the number of concurrent requests sent to the authentication server simulating a number of clients performing authentications simultaneously. This parameter sets the workload requested to the server and can be modified on the fly during the test.

To stop the test click the **Stop** button or select the **File>Stop Test** menu option (keyboard shortcut: ⌘T).

The right area of the window shows 6 elements of performance measurement:

- **Authentications** strip chart. Shows the number of authentications per second successfully completed (terminated with a received Accept or Reject RADIUS message).
- **Authentication Failures** strip chart. Shows the number of authentication per second failed (some response message from the server timed out).
- **Authentication Time** strip chart. Shows the average of the time spent in successfully completed authentications.
- Average Authentications/second. Shows the current average of all authentications in the test.
- Average Authentication Time in milliseconds. Shows the current average authentication time in the test.
- Authentications request results distribution chart. Shows the current fraction of authentications completed with an **Accept** message, with a **Reject** message and unsuccessfully terminated (**Failures**).

In the following figure a TTLS/PAP performance test is shown:

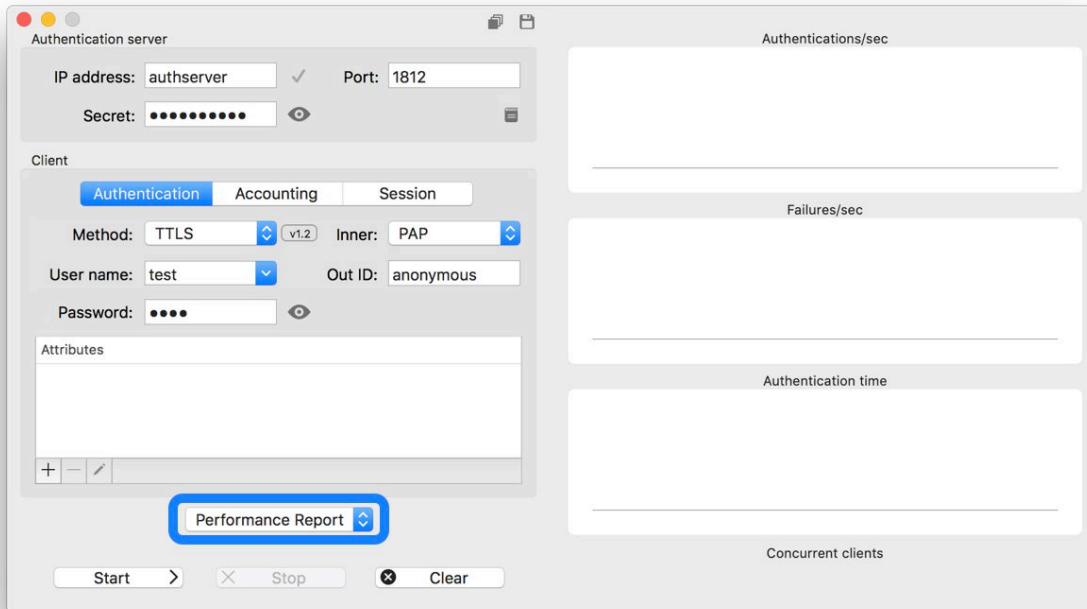


To clear the content of the view click the **Clear** button or select the **File>Clear View** menu option. You can examine the values of the charts right clicking and dragging on them.

Performance Reports

Performance Reports performs automatically several Performance Tests with different number of clients to test server performance under different traffic loads.

To generate an performance report select **Performance Report** in the test mode selection popup menu or select the **File>Authentication Test>Performance Report** main menu option:



To start the test click the **Start** button or select the **File>Start Test** menu option (keyboard shortcut: ⌘R).

To stop the test click the **Stop** button or select the **File>Stop Test** menu option (keyboard shortcut: ⌘T).

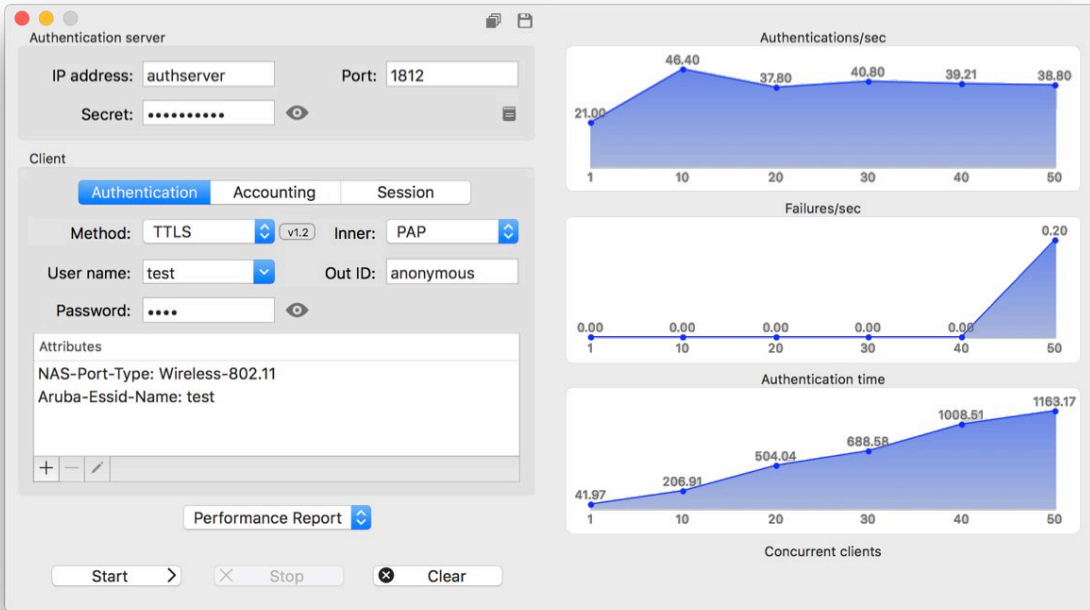
The report automatically test server performance in several workload conditions defined by the number of concurrent requests sent to the server. The charts show the server behavior when the number of customers (simultaneous requests) increases. The server is tested with 1, 10, 20, 30, 40 and 50 simultaneous clients during 5 seconds (total time is 30 seconds).

The right area of the window shows 3 elements of performance measurement:

- **Authentications/sec** chart. Shows the average number of authentications per second successfully completed (terminated with a received Accept or Reject RADIUS message).
- **Failures/sec** chart. Shows the average number of authentications per second failed (some response message from the server timed out).
- **Authentication Time** chart. Shows the average of the time spent in successfully completed authentications.

The X axis of all charts is the number of Concurrent Clients.

In the following figure a TTLS/PAP performance report is shown:

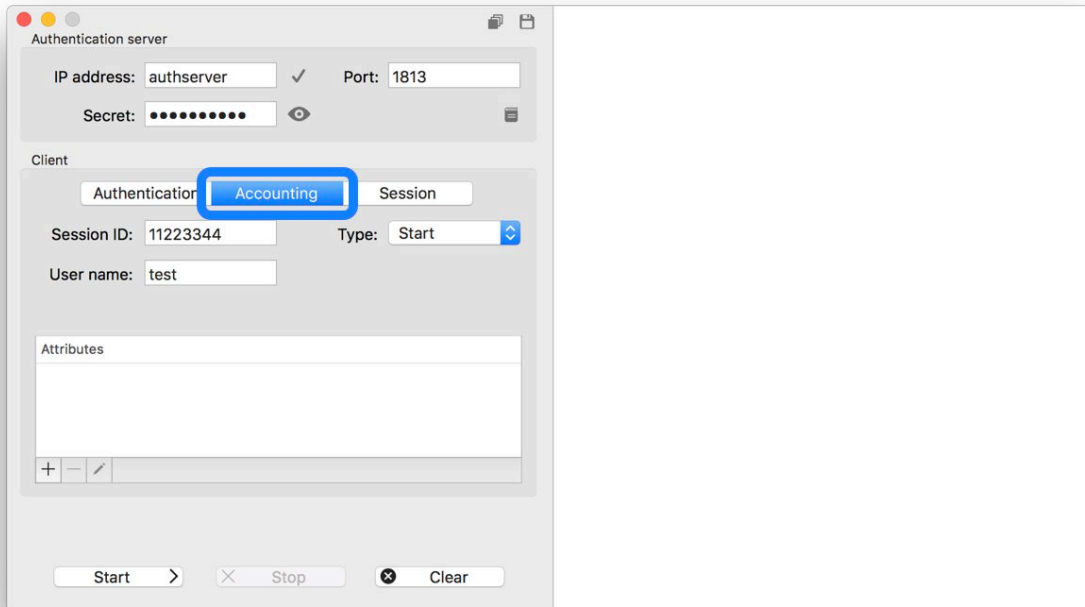


To clear the content of the view click the **Clear** button or select the **File>Clear View** menu option.

Accounting Tests

Accounting tests generate individual accounting requests to the authentication server. Protocol messages interchanged with the authentication server are shown in the right view of the EAPTest window.

To perform Accounting Tests select **Accounting** in the test mode selector or select the **File>Test>Accounting** main menu option:



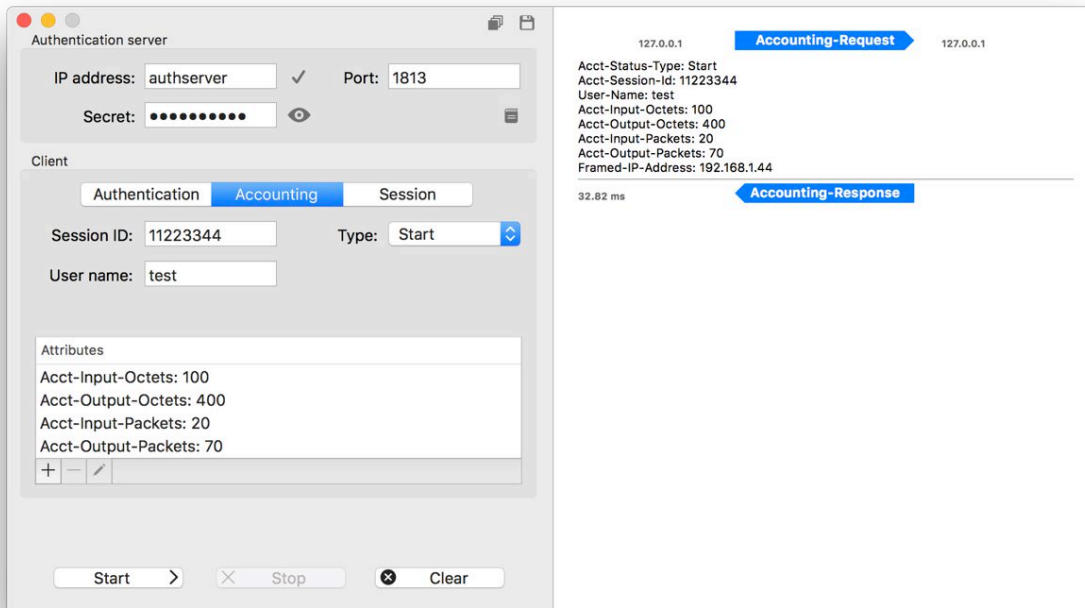
To start the test click the **Start** button or select the **File>Start Test** menu option (keyboard shortcut: ⌘R).

To perform an Accounting Test you should specify a **Session ID** string and an **User name** and select the **Type** of the Accounting request message:

- **Start**
- **Stop**
- **Update (Interim)**

To stop the accounting process before it has been completed click the **Stop** button or select the **File>Stop Test** menu option (keyboard shortcut: ⌘T).

During the accounting process the right area of the window displays the RADIUS messages being interchanged and the RADIUS attributes included in the messages:



The following messages are shown:

- **Accounting-Request** message sent to the server:

Accounting-Request

Acct-Status-Type: Start
 Acct-Session-Id: 11223344
 User-Name: test
 Acct-Input-Octets: 2000
 Acct-Input-Packets: 400
 Acct-Output-Octets: 4000
 Acct-Output-Packets: 100

- When the accounting response message is not received from the authentication server in response to the **Accounting-Request** message sent, the message is resent several times:

Accounting-Request

Acct-Status-Type: Start
 Acct-Session-Id: 11223344
 User-Name: test
 Acct-Input-Octets: 2000
 Acct-Input-Packets: 400
 Acct-Output-Octets: 4000
 Acct-Output-Packets: 100

- **Accounting-Response** message received from the server:

Accounting-Response

- If the response timer expires without server response the following indication is shown:

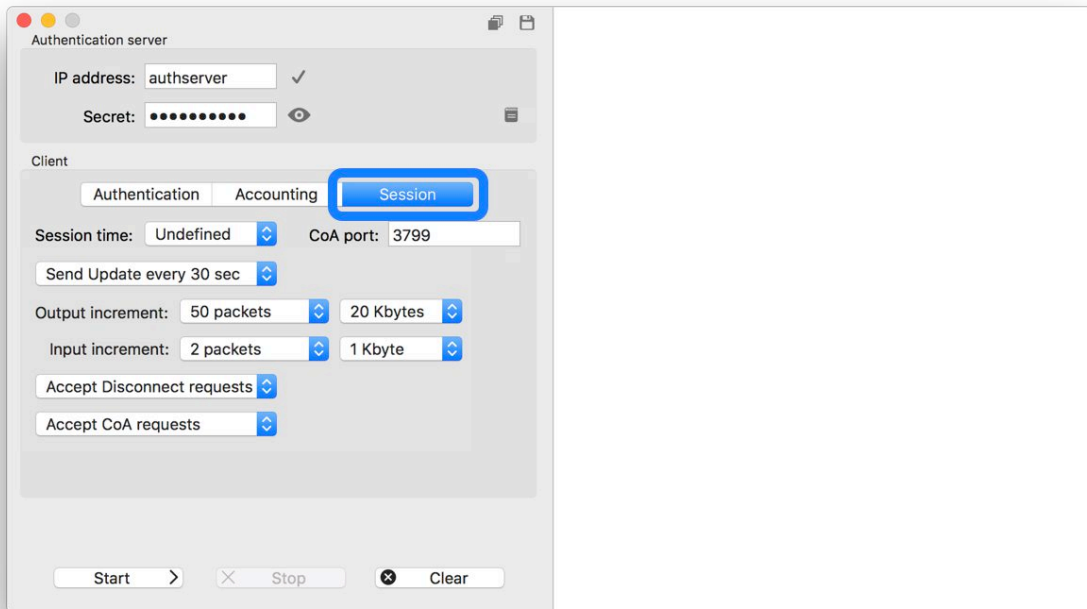
Timeout

To clear the content of the view click the **Clear** button or select the **File>Clear View** menu option.

EAP Session Tests

Accounting tests simulate a complete client session by performing authentication, accounting and listening for dynamic RADIUS messages sent by the authentication server. Protocol messages interchanged with the authentication server are shown in the right view of the EAP Test window.

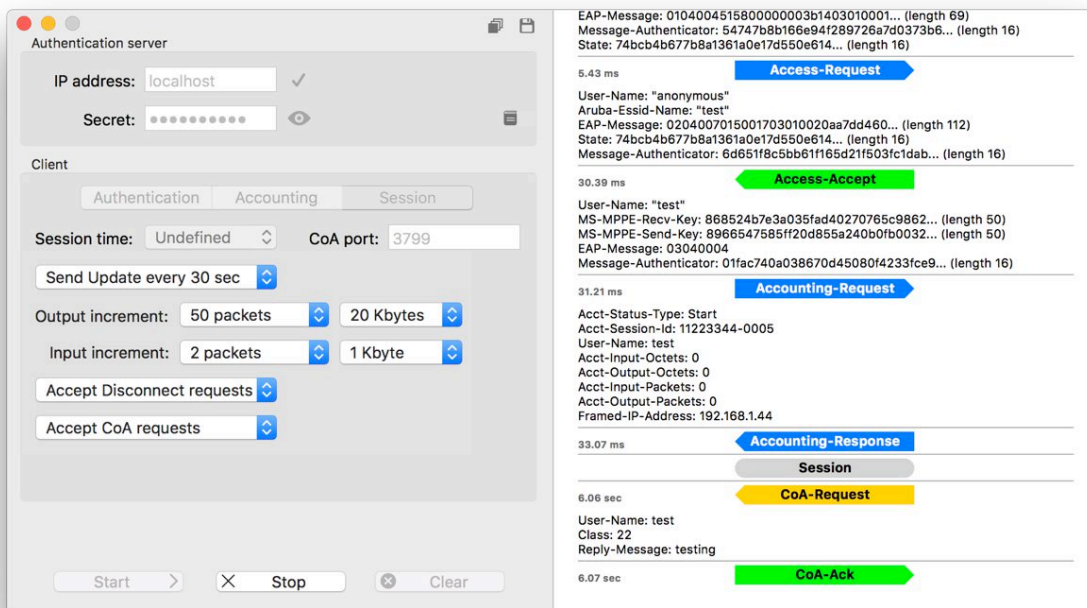
To perform Session Tests select **Session** in the test mode selector or select the **File>Test>Session** main menu option:



To start the test click the **Start** button or select the **File>Start Test** menu option (keyboard shortcut: ⌘R).

To terminate the session simulated click the **Stop** button or select the **File>Stop Test** menu option (keyboard shortcut: ⌘T).

During the session simulation the right area of the window displays the RADIUS messages being interchanged and the RADIUS attributes included in the messages:



A session test is composed of the following phases:

- **Authentication.** The client authentication parameters (method, credential and attributes) are defined in the Authentication test mode fields. Interchanged messages are displayed as shown in the Authentication Protocol Test section.
- **Accounting.** If the Authentication phase is terminated with an **Accept** message from the authentication server, an **Accounting Start** message is sent to the server. The client accounting parameters (session ID and attributes) are defined in the Accounting test mode fields. Interchanged messages are displayed as shown in the Accounting Test section.
- **Session.** The duration of the Session phase is specified using the **Session time** popup menu. The following values are available:
 - Undefined.** The session is maintained until the test is terminated clicking the **Stop** button or selecting the **File>Start Test** menu option (keyboard shortcut: ⌘R).
 - 1 second.** The session is held for 1 second.
 - 5 seconds.** The session is held for 5 seconds.
 - 10 seconds.** The session is held for 10 seconds.
 - 30 seconds.** The session is held for 30 seconds.

During the session, **Accounting Update** messages can be periodically sent to the authentication server in function to the value selected in the **Updates** popup menu:

- No updates.** This value disables sending Accounting Update messages.
- Send Update every 5 sec.**
- Send Update every 10 sec.**
- Send Update every 20 sec.**
- Send Update every 30 sec.**
- Send Update every 60 sec.**

The **Output increment** and **Input increment** packets and bytes popups define the increment in the values of the traffic counters (**Acct-Output-Packets**, **Acct-Output-Octets**, **Acct-Input-Packets** and **Acct-Input-Octets** attributes) sent in each **Accounting Update**.

During the session, dynamic RADIUS Disconnect and Change of Authorization (CoA) messages can be received from the authentication server. The client port to listen for dynamic RADIUS messages can be configured in the **CoA port** field.

The behavior for received **Disconnect-Request** messages is defined by the Disconnect Action popup menu:

- Accept Disconnect requests.** The received message is acknowledged (a **Disconnect-Ack** message is sent to the server) and the session is ended (the **Session end** phase is entered).
- Reject Disconnect requests.** The received message is rejected (a **Disconnect-Nak** message is sent to the server).
- Ignore Disconnect requests.** The received message is ignored.

The behavior for received **CoA-Request** messages is defined by the CoA Action popup menu:

- Accept CoA requests.** The received message is acknowledged (a **CoA-Ack** message is sent to the server).
- Reject CoA requests.** The received message is rejected (a **CoA-Nak** message is sent to the server).
- Ignore CoA requests.** The received message is ignored.

The Accounting **Updates** period, the **Output/Input increments** and the **Disconnect** and **CoA** actions can be modified during the session.

- **Session end.** Session ending is performed sending an **Accounting Stop** to the authentication server. Interchanged messages are displayed as shown in the Accounting Test section.

In the Session phase the following messages are shown:

- Session phase indicator:

Session

- **Disconnect-Request** received from the server:

Disconnect-Request

User-Name: test
Reply-Message: disconnected

- **Disconnect-Ack** message sent to the server:

Disconnect-Ack

- **Disconnect-Nak** message sent to the server:

Disconnect-Nak

- **CoA-Request** received from the server:

CoA-Request

User-Name: test
Class: 22
Reply-Message: testing

- **CoA-Ack** message sent to the server:

CoA-Ack


- **CoA-Nak** message sent to the server:


CoA-Nak

To clear the content of the view click the **Clear** button or select the **File>Clear View** menu option.

Using Profiles

Profiles allow you to save different configurations of test parameters for later retrieval. Test parameters including the attributes and the digital Identity used in TLS authentication can be saved to a profile for later retrieval. You can load a specific profile when needed.


To save current test configuration to a profile click the  button located at the top of the window or select the **File>Save Profile...** menu option (keyboard shortcut: ⌘S).

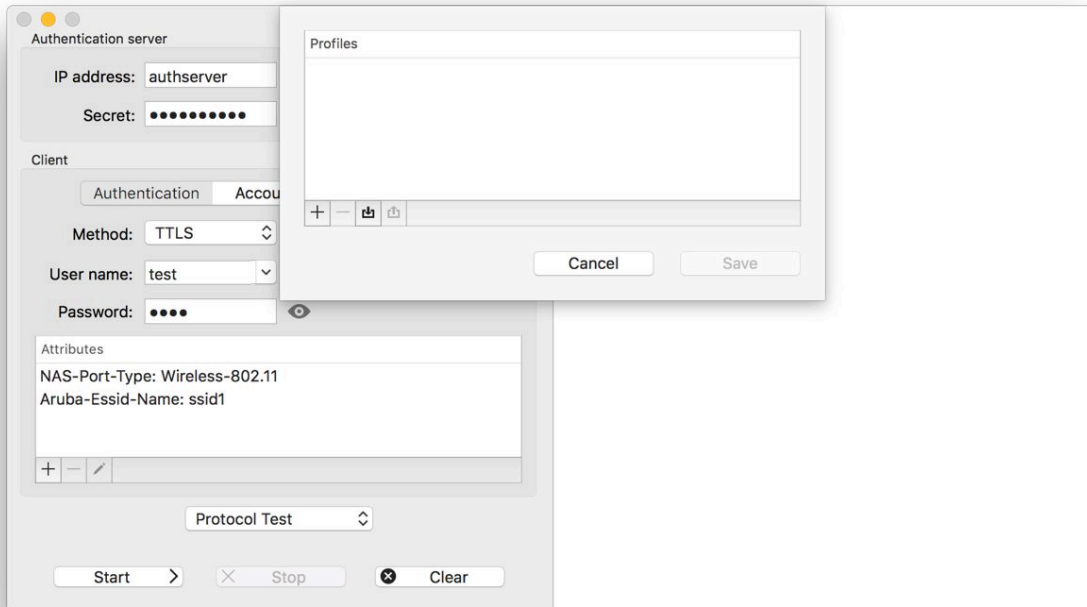
To load a profile click the  button located at the top of the window or select the **File>Load Profile...** menu option (keyboard shortcut: ⌘L).



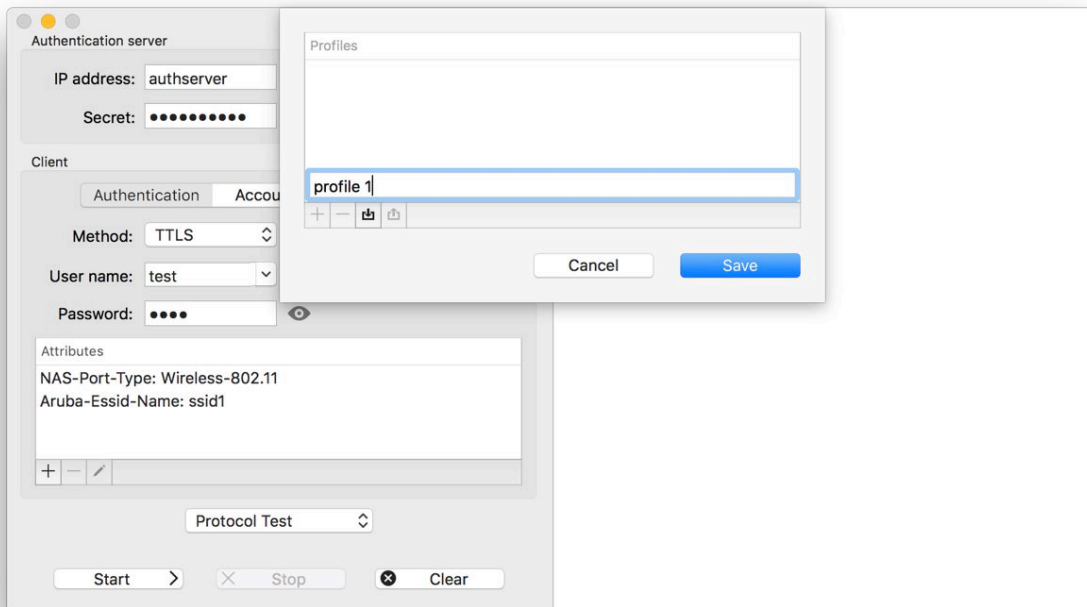
Profiles can be exported and imported.

Saving Profiles

To save the current test parameters to a profile click the  button or select the **File>Save Profile...** menu option (keyboard shortcut: ⌘S).



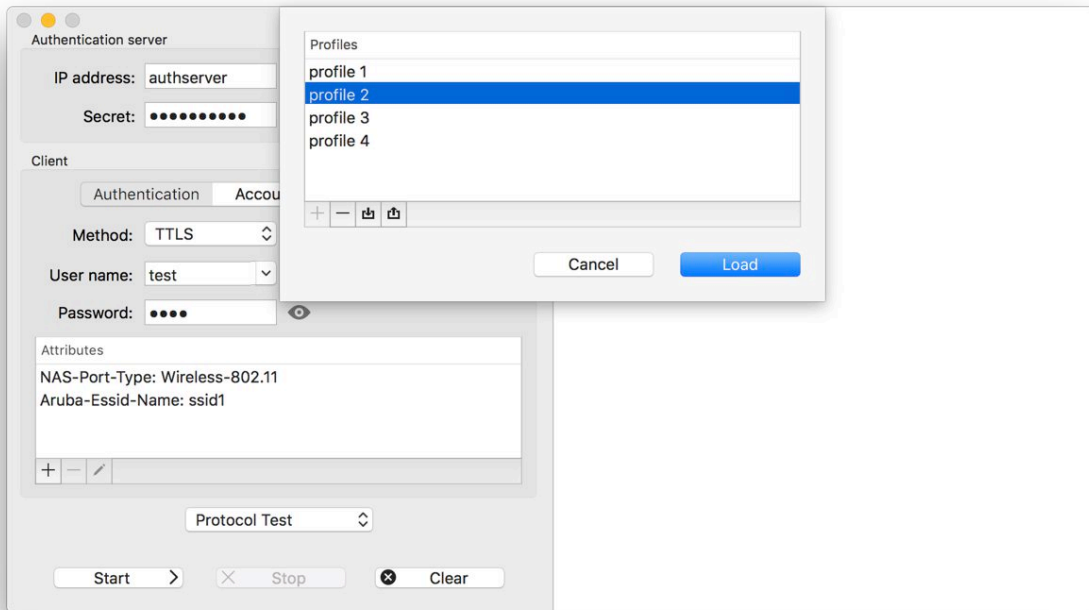
In the displayed dialog click the  button to create a new profile:



Enter the profile name and click **Save**.


Loading Profiles

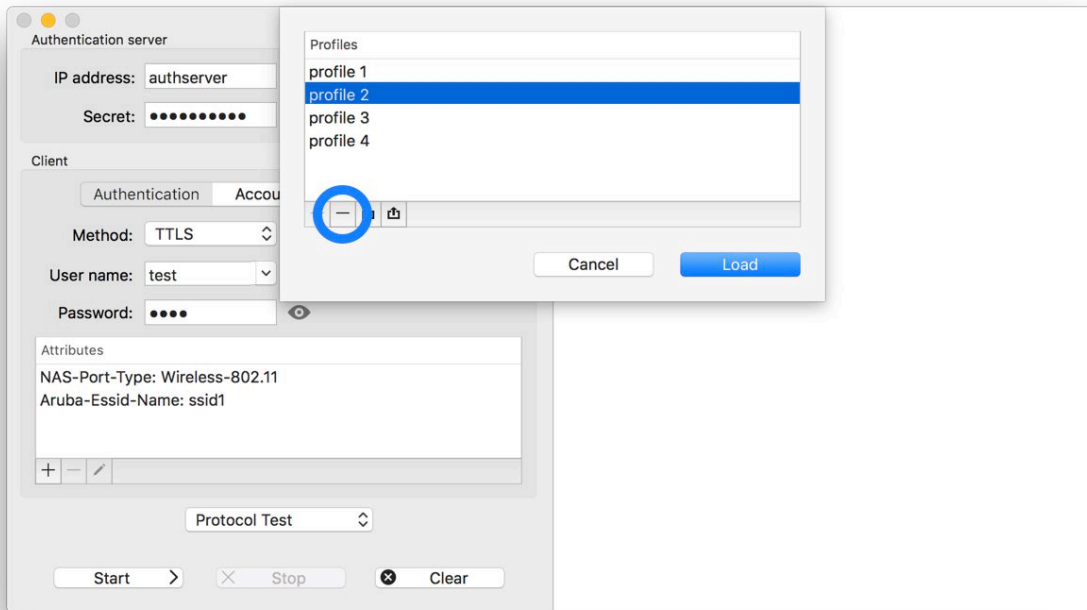
To load a profile click the  button or select the **File>Load Profile...** menu option (keyboard shortcut: ⌘L).



Select a profile and click **Load**.


Deleting Profiles

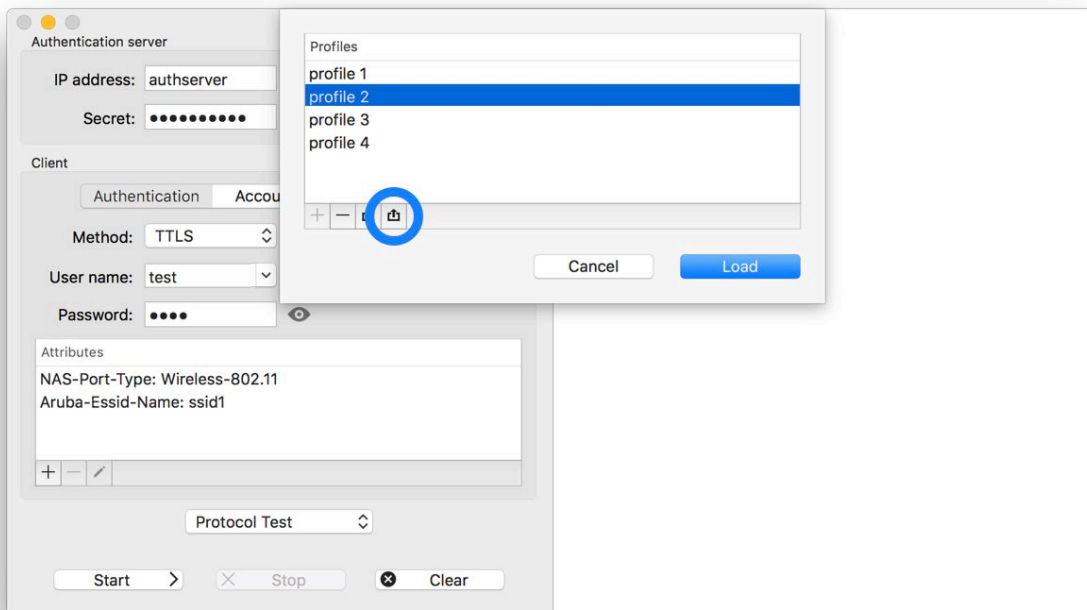
You can delete previously saved clicking the  button or selecting the **File>Load Profile...** menu option (keyboard shortcut: ⌘L).



Select the profile name to delete and click the  button.


Exporting Profiles

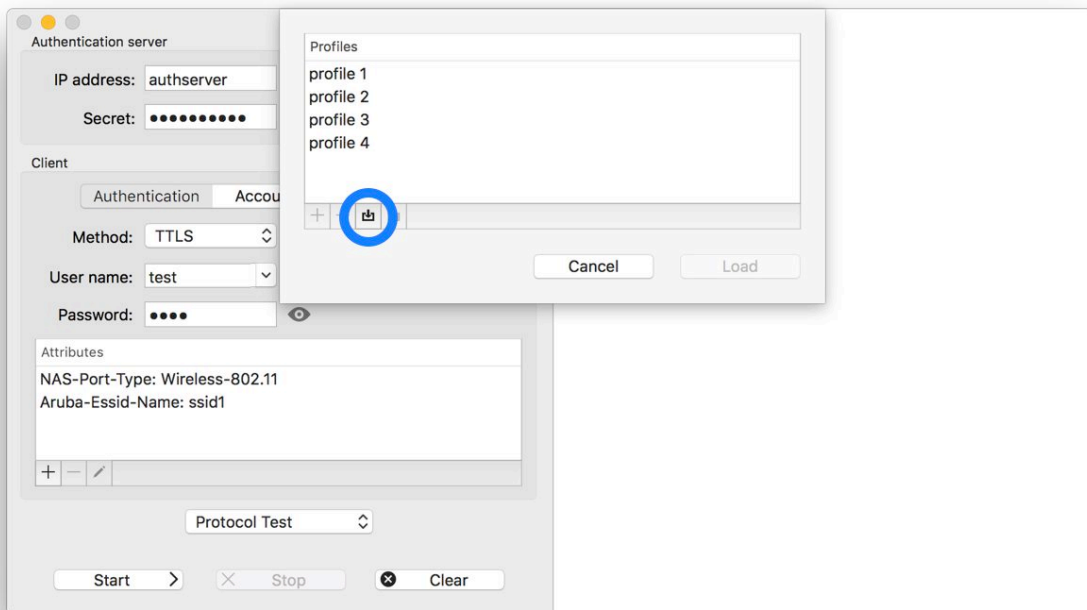
You can export a previously saved profile clicking the  button or selecting the **File>Load Profile...** menu option (keyboard shortcut: ⌘L).




Select the profile name to export and click the  button to select the file name to export the profile.

Importing Profiles

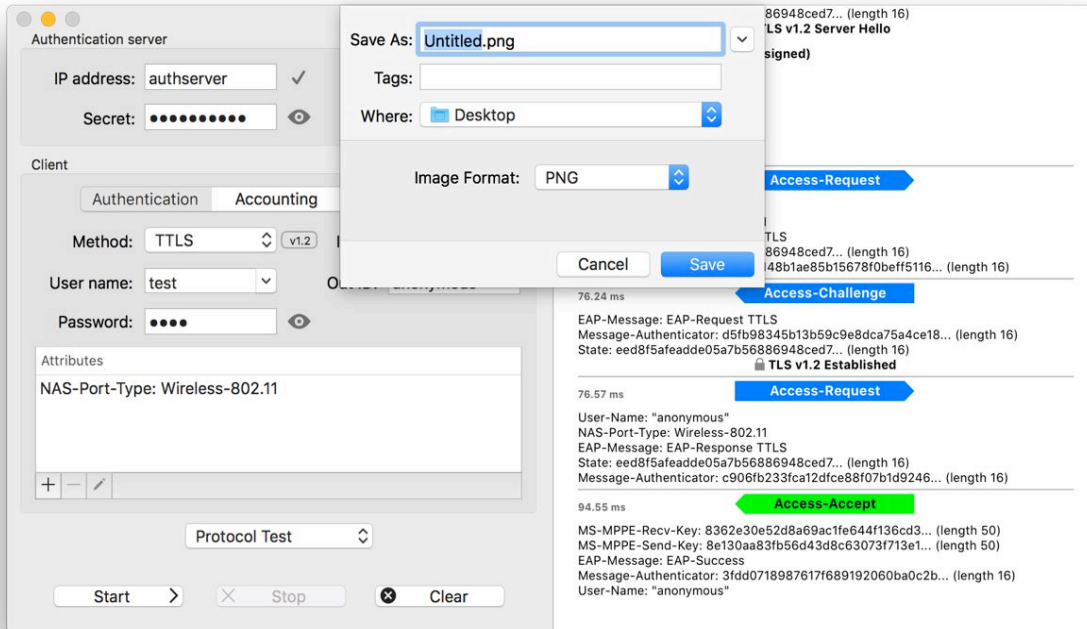
You can export a previously saved profile clicking the  button or selecting the **File>Load Profile...** menu option (keyboard shortcut: ⌘L).



Click the  button to select the file containing the profile to import.

Saving to an Image File

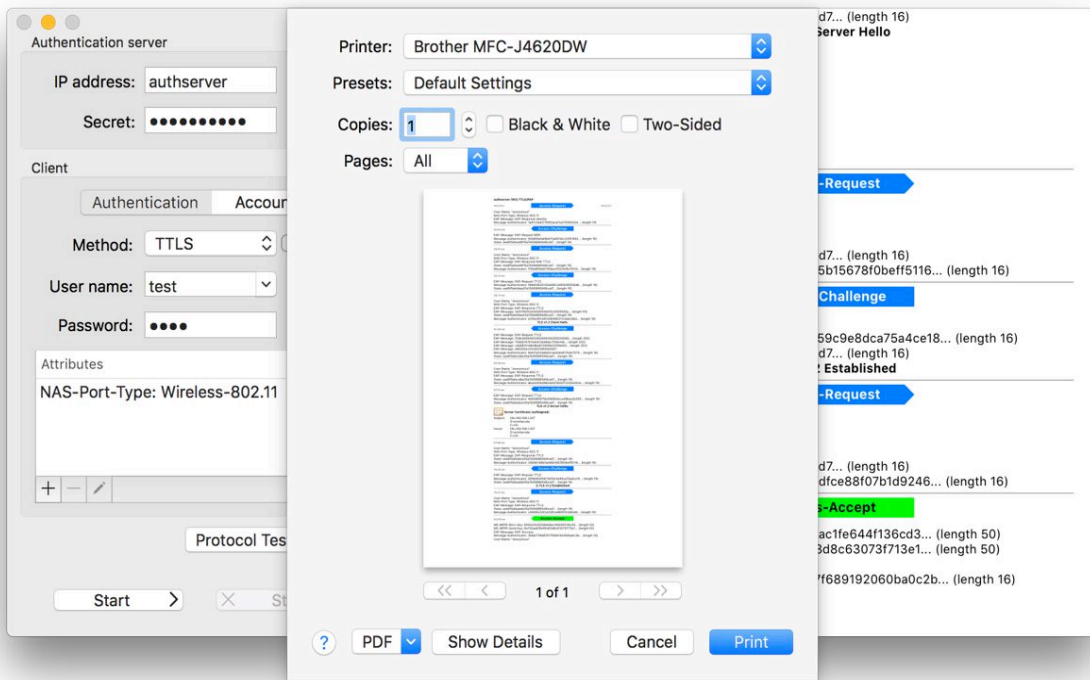
If you need to include a test result in a document, you can save the results view (the RADIUS messages interchanged during an authentication in **Authentication Test** mode, or the performance information in **Performance Test** and **Report** modes) to an Image File and then import it into your document. To save the view to an Image File click the **File>Save Image...** menu option.



Available Image Formats are JPEG, JPEG-2000, PNG, GIF and TIFF.

EAP Printing

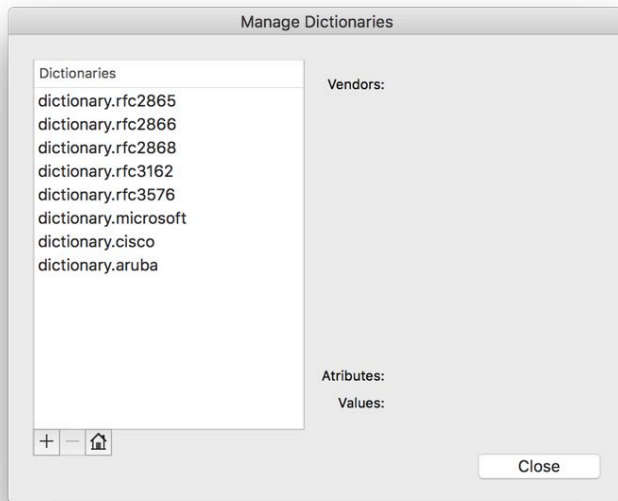
To print the results view (the RADIUS messages interchanged during an authentication in **Authentication Test** mode, or the performance information in **Performance Test** and **Report** modes) click the **File>Print...** menu option.



Select the printer and press the **Print** button or use the **PDF** menu to save a PDF copy to the disk.




Managing Dictionaries

To manage the RADIUS attributes database use the **File>Manage Dictionaries...** menu option or click the  button in the **Server parameters** area:



The window shows the the left list all the dictionaries actually contained in the database. When a dictionary item is selected in the list, information about the dictionary is shown in the right part of the window: the **Vendors** for which some attributes or values are defined in the dictionary and the number of **Attributes** and **Values** defined in the dictionary.

Using the buttons below the **Dictionaries** list you can:

-  Import Dictionary Files
-  Remove Dictionaries
-  Reset the Dictionary Database


Importing Dictionaries

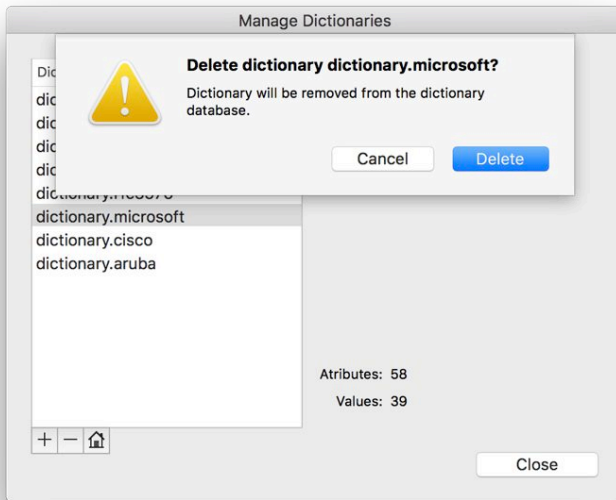
To import a dictionary file to the RADIUS attributes database click the  button in the Manage Dictionaries window.

Select the dictionary file in the displayed file dialog and press the **Open** button.

The new imported dictionary will be shown in the **Dictionaries** list in the Manage Dictionaries windows.


Removing Dictionaries

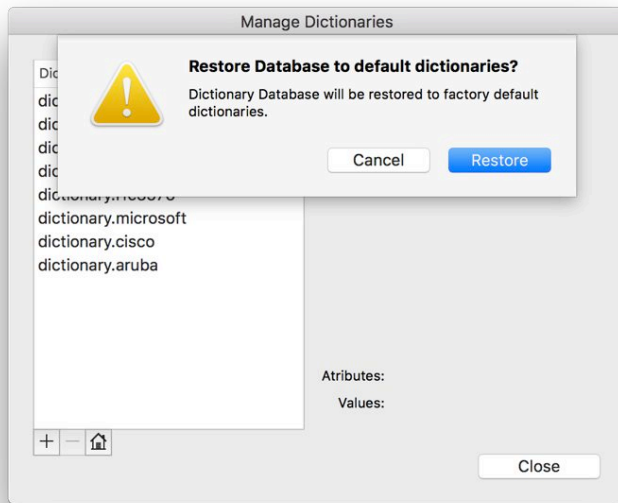
To remove a dictionary from the RADIUS attributes database select it in the Dictionaries list and click the  button in the Manage Dictionaries window.



Press the **Delete** button in the displayed alert.

Resetting the Database

To reset the RADIUS attributes database to the default dictionaries click the  button in the Manage Dictionaries window.



Press the **Restore** button in the displayed alert dialog.

The established default dictionaries are:

- RFC2865
- RFC2866
- RFC2868
- RFC3162
- RFC3576
- Microsoft
- Cisco
- Aruba