802.1X/EAP AUTHENTICATION GUIDE
RADIUSNT/X V5.1

IEA Software, Inc.

Administrative and Support Office
PO BOX 1170
Veradale, Washington 99037
Phone: (509) 444-BILL

Sales@iea-software.com
Support@iea-software.com

Software License Agreement

By purchasing or installing RadiusNT or RadiusX, you indicate your acceptance of the following License Agreement.

Ownership of Software You acknowledge and agree that the computer program(s) and associated documentation contained with RadiusNT or RadiusX (collectively, the Software) are owned exclusively by IEA Software, Inc. and/or its licensors. The Software contained in the package is protected under copyright laws and all copyright and other intellectual property rights relating to the Software are and remain the exclusive property of IEA Software, Inc. and/or its licensors. You may not rent or lease the Software, but you may transfer the Software and accompanying materials on a permanent basis provided you retain no copies and the recipient agrees to the terms of this Agreement.

License IEA Software, Inc. grants to you, and you accept, a limited, non-exclusive and revocable license to use the Software. You agree to use the Software in machine-readable object code form only as authorized in this License Agreement. This License Agreement does not convey any title or interest in the Software to you.

Scope of License You may not make any changes or modifications to the Software, and you may not de-compile, disassemble, or otherwise reverse engineer the Software. You may not lend, rent, lease or sublicense the Software or any copy to others for any purpose. RadiusNT or RadiusX may only be installed on a single WindowsNT, Solaris, Linux or Cobalt Networks workstation or server. Additional servers may be purchased separately. You agree to use reasonable efforts to protect the Software from unauthorized use, modifications, reproduction, distribution and publication. You are not permitted to make any uses or copies of the Software that are not specifically authorized by the terms of this License Agreement. Your adherence to this License Agreement will allow IEA Software, Inc. to continue developing innovative and useful products and providing a high level of customer service and support. If you do not comply with the terms of this License Agreement, your license will be revoked.

Updates and Support All software updates and fixes are available via the IEA Software, Inc. Web site. Major version upgrades are not included or covered as part of the basic purchase agreement. Technical support is currently available via methods listed on our Web site Support section at http://www.iea-software.com/support.

Restricted Rights The Software is provided with U.S. Governmental Restricted Rights. Use, duplication, or disclosure by the Government is subject to restrictions set forth in subparagraph ©(1)(ii) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs ©(1) and (2) of the Commercial Computer Software - Restricted Rights at 48 CFR 52.227-19 as applicable. The Software is also protected by International Treaty Provisions. Manufacturer is IEA Software, Inc. PO BOX 1170 Veradale WA, 99037.

Miscellaneous This License Agreement shall be construed, interpreted and governed by the laws of the State of Washington. Should any term of this License Agreement be declared void or unenforceable by any court of competent jurisdiction, enforcement of the remaining terms shall not be affected. Failure of either party to enforce any rights or to take action against the other party in the event of any breach of this Licensing Agreement shall not be deemed a waiver of any subsequent enforcement of rights.

Limitations of Liability and Remedies In no event shall IEA Software, Inc. or its licensors be liable for any loss of profit or any other commercial damage, including but not limited to special, incidental, consequential or other damage, even if IEA Software, Inc. or its licensors are advised, in advance, of the possibility of such damages. IEA Software, Inc. and its licensor's entire liability and your exclusive remedy shall be, at IEA Software's option, either (a) return of the price paid, or (b) repair or replacement of the Software. To the maximum extent permitted by applicable law, IEA Software, Inc. and its licensors disclaim all other warranties, either express or implied, including but not limited to, implied warranties with regard to the Software and the accompanying material. This Limited Warranty is void if failure of the Software has resulted from accident, abuse or misapplication. You may have other specific legal rights, which vary from state/jurisdiction to state/jurisdiction.

Return Policy It is our goal to provide customers with the highest level of satisfaction possible. In order to ensure that our products work well in your environment, IEA Software offers a 30-day FULL functioning software trial that includes documentation and support. If you require more than 30 days to evaluate the software, we are happy to work with you to extend the trial to a length that fits your timetable. This gives you, the user, an opportunity to ensure that the product fully meets your needs. (Please test the software in a non-production environment.) In light of the trial period and opportunity to fully test our software, IEA Software maintains the policy that no refunds will be offered. We will, however, address any problems with the software.

Should a software anomaly occur, our Development and Support Teams will work to correct the problem. Please note that you must be using the application normally, as defined, and you must ensure that the bug is not due to anomalies in other programs, the operating system, your hardware, or data.

In order to address any problems, please note that the bug must be able to be reproduced. Our Development and Support Teams will require full documentation of the steps taken by the user that caused the error in the software as well as necessary data and scenario files to reproduce the error.

Contact Should you have any questions concerning this license agreement, please contact IEA Software, Inc. PO BOX 1170 Veradale, WA 99037 U.S.A. (509) 444-BILL (2455).

Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, without the express written consent of IEA Software, Inc.

Trademarks

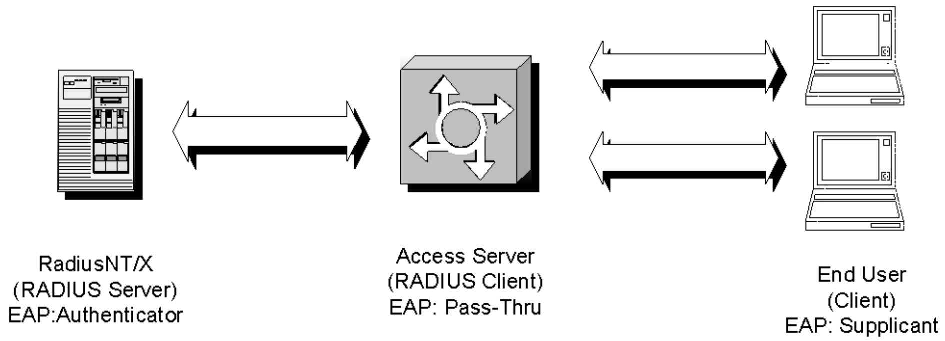
Emerald Management Suite, RadiusNT and *RadiusX* are trademarks of IEA Software, Inc. All images, photographs, animations, audio, video and text incorporated into the Software are owned by IEA Software, Inc., unless otherwise noted by Trademark. *Intel* is a registered trademark of Intel Corporation. *Transact-SQL* is a registered trademark and *DB-Library* is a trademark of Sybase, Inc. *Cobalt*, *RAQ*, and *Solaris* are trademarks of Sun Microsystems. *Cisco* is a trademark of Cisco Systems. All other trademarks are the property of their respective owners.

Table Of Contents

EAP Authentication, what is it and how does it work?

In the RADIUS world several standard authentication protocols exist such as PAP, CHAP and MSCHAPv1/2. Normally to authenticate -- The Access server and end user client first negotiate the authentication protocol to be used. After choosing one (PAP, CHAP, MSCHAPv1/2, EAP,…) the appropriate data for the choosen authentication protocol is sent to the RADIUS server for authentication.

In this standard scenario all three systems (RADIUS, Access Server, End User client) must agree with and have specific knowledge of the authentication protocol being used.



As the complexity of relationships between systems and increasing need for more elaborate and secure authentication methods grows the problems associated with this solution become difficult to manage. The Extensible Authentication Protocol (EAP) protocol attempts to solve the following problems with minimal change to existing network infrastructure.

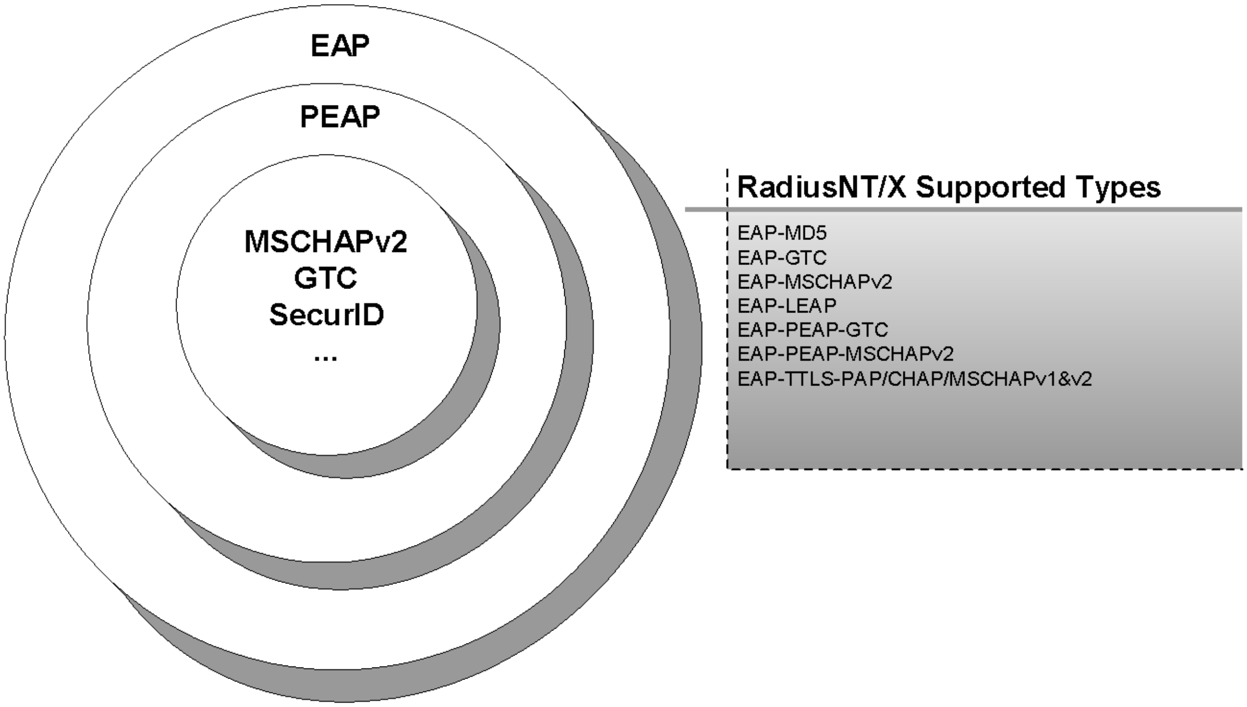
1. Authentication protocol negotiation between access server and end user does not consult the RADIUS authentication in the initial authentication step. The RADIUS server may not allow or agree with the authentication protocol negotiated between access server and end user. If this happens the authentication fails. A classic example of this problem can be found with RADIUS servers configured to authenticate against a one-way encrypted backend database. This was common with many UNIX and Windows user databases. Since the RADIUS CHAP protocol requires access to plain text unencrypted passwords, a client and server that unknowingly agree on CHAP are in for quite a surprise when the RADIUS server finds its impossible to authenticate their request.

2. Today the variety of RADIUS capable access servers number in the hundreds, many have very limited processing and memory capacity available for client authentication. Allowing authentication details to pass through the access server allows newer authentication protocols to be deployed with fewer changes and with less interoperability problems.

3. Trust is the foundation of every network security system. Historically RADIUS in the dialup environment trusted the public telephone network enough to enable most applications to be considered secure. Given today’s wireless networks, global roaming environments and large areas on shared cable networks there is no clear single entity providing services over the avaliable medium. Therefore in many cases the End User cannot trust the Access Server or intermediate proxies with the task of handling passwords or authentication protocol negotiation.

In order to solve these and other problems with minimal change to existing systems the EAP and later Protected-EAP protocols were designed. EAP simply provides a conduit between the Authenticator and Supplicant (RADIUS and End-User client) where they discuss the best way to authenticate and then actually go about the task of authenticating. This removes the Access Server from taking part in the authentication process. Since EAP itself is merely a conduit, it can be thought of as a computers operating system. An operating system in itself is useless without applications to run. EAP types provide these ‘applications’ by providing the authentication protocol used to perform the actual authentication step. In this way future authentication protocols can be easily added by adding new EAP types to the Authenticator and Supplicant.

Protected-EAP (PEAP) is an EAP type providing the EAP protocol over an encrypted, certificate-authenticated conduit. In addition to the encryption it also offers keying material that can be used by the RADIUS server and End-User client to establish a secure link for all future network traffic (WEP, WPA/AES, etc). Since PEAP itself implements the EAP protocol, just over a more secure, encrypted channel, it too requires an EAP type of its own to execute. The diagram below illustrates this relationship.



PEAP uses the same technology used today to protect secure web sites on the Internet. The PEAP protocol uses TLS v1 (essentially SSL) and utilizes the same trusted third party public key infrastructure (PKI) as secure web sites.

EAP-TTLS is identical to PEAP using PKI infustructure to protect PAP, CHAP and MSCHAPv2 authentication protocols.

Which EAP Type (authentication protocol) is right for me?

Typically for 802.1x/EAP you choose EAP types supported by client software your end users already have or can reasonably be made available to them. EAP-PEAPv0-MSCHAPv2 is a popular choice as it is included with all currently available versions of Microsoft windows and supported by major competing platforms such as Linux and MAC.

When using a backend authentication database containing UNIX or LDAP passwords choices for authentication may be limited to PAP, EAP-TTLS-PAP or EAP-PEAP-GTC. This is because CHAP requires access to password plaintext and MSCHAP requires access to plaintext or NT Hash.

The following table provides a simple listing of all supported authentication protocols and their realitive strengths and weaknesses. Detailed evaluations of each protocol can be found on the Internet.

Protocol	Offline attack	Severe flaws known	UNIX/NT/LDAP compatibility	Mutual auth	Encryption keys
PAP	See #1	See #1	Yes	No	No
CHAP	Yes	No	See #4	No	No
MSCHAPV1	Yes	Yes	See #3	No	Yes
MSCHAPV2	Yes	No	See #3	Yes	Yes
HTTP Digest	Yes	No	See #4	Yes	No
EAP-MD5	Yes	No	See #4	No	No
EAP-GTC	See #2	See #2	Yes	No	No
EAP-LEAP	Yes	Yes	See #3	Yes	Yes
EAP-PEAP-MSCHAPv2	No	No	See #3	Yes	Yes
EAP-PEAP-GTC	No	No	Yes	No	Yes
EAP-PEAP-MD5	No	No	See #4	No	Yes
EAP-TTLS-MSCHAPv2	No	No	See #3	Yes	Yes
EAP-TTLS-PAP	No	No	See #3	No	Yes
EAP-TTLS-CHAP	No	No	See #4	No	Yes
EAP-TTLS-MSCHAPv1	No	No	See #3	No	Yes

#1. PAP passwords are encrypted between RADIUS server and access server. Password security is dependant upon link between access server and client over which the password travels. RADIUS encryption can be improved by choosing RADIUS shared secrets with 16 or more characters. It can be further improved by using additional layer2/3 security such as a physically secure switched network and IPSec.

#2. GTC information is not encrypted between RADIUS server and access server providing less security than standard RADIUS PAP. Security can be improved by using additional layer2/3 security such as a physically secure switched network and IPSec.

#3. While possible RadiusNT/X v4 and v5 does not currently support authentication against Active directory or NT SAM using this protocol. UNIX password authentication is not possible using this protocol. LDAP authentication is possible provided clear text passwords are made available to RadiusNT/X by the directory server.

#4. Of the three only LDAP authentication is possible provided clear text passwords are made available to RadiusNT/X by the directory server.

Versions and editions of RadiusNT/X supporting EAP Authentication

We recommend at least RadiusNT/X 5.1.36 to authenticate and proxy EAP authentication requests. While previous versions of RadiusNT 5 work successfully in most environments, additional EAP types, EAP proxy and compatibility improvements have since been made to better support EAP in a variety of environments. If you are using a prior version of RadiusNT/X v5 contact our support department (support@iea-software.com) to obtain an update or visit the IEA Software download center.

If you are evaluating Emerald v5 standard or RadiusNT/X standard EAP feature licensing is available which allows you to take advantage of EAP features without having to move to the professional or hotspot editions of the software. Please contact your sales representative or sales@iea-software.com to discuss EAP feature licensing.

Customers using the previous versions of Emerald 4.5 /w RadiusNT/X version 4 must purchase a RadiusNT/X version 5 upgrade licenses. If you have purchased Emerald 4.5 in December of 2003 or later and are currently using RadiusNT/X v4, contact our sales group to receive a complimentary RadiusNT/X version 5 upgrade license.

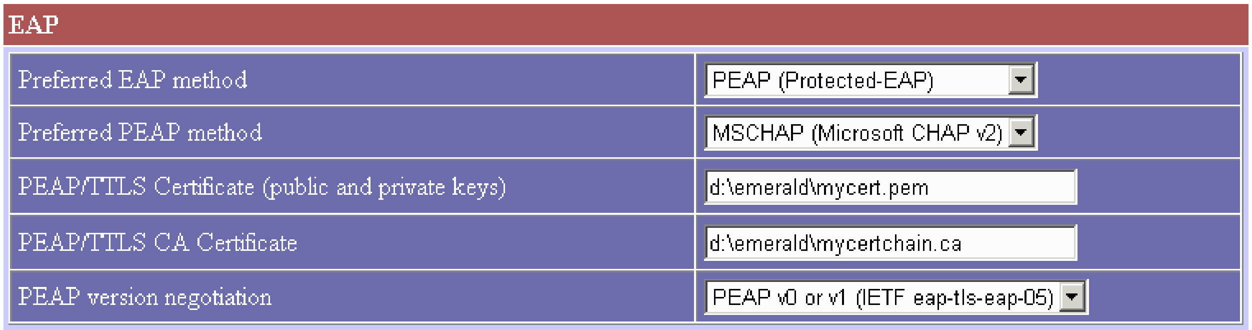
If you have a RadiusNT/X v5 license, it must be a RadiusNT/X v5 professional or enterprise license. RadiusNT/X v5 standard does **NOT** support EAP without the EAP feature enabled.

In summary EAP requires at least RadiusNT/X 5.0.42 Professional, Enterprise or the standard edition with the EAP license feature enabled.

If you have RadiusNT 2.5, 3.0, or 4.0 and would like to take advantage of EAP features please contact our sales group about purchasing an upgrade license (sales@iea-software.com)

Configuring RadiusNT/X for EAP Authentication

Generally very little if any configuration is necessary to support most end user clients. EAP support is automatically enabled as long as you're licensed for EAP features. To configure EAP Authentication, open the RadiusNT/X admin and select the EAP menu option.



EAP

Preferred EAP method	PEAP (Protected-EAP)
Preferred PEAP method	MSCHAP (Microsoft CHAP v2)
PEAP/TTLS Certificate (public and private keys)	d:\emerald\mycert.pem
PEAP/TTLS CA Certificate	d:\emerald\mycertchain.ca
PEAP version negotiation	PEAP v0 or v1 (IETF eap-tls-eap-05)

Option	Description
Preferred EAP method	This should reflect the EAP method most of your clients will be using. This improves latency of requests slightly by making protocol negotiation easier for the client and server.
Preferred PEAP method	This should reflect the PEAP method most of your clients will be using. This improves latency of requests slightly by making protocol negotiation easier for the client and server.
PEAP/TTLS Certificate	SSL certificate file containing a public and private key in PEM (Base64) format concatenated together in a single file. Please see the section on PEAP certificates below for more information.
PEAP/TTLS CA Certificate	Your CA's certificate chain file in PEM (Base64) format.
PEAP version negotiation	PEAP protocol version negotiation, the default setting is 'PEAP v0 or v1' to allow either version client to authenticate. Typically limiting negotiation to version 0 provides the best compatibility between clients.

Note: We have tested RadiusNT/X with some older supplicants that do not support EAP Type negotiation. If newer versions cannot be obtained you should set the Preferred EAP and Preferred PEAP methods to match these clients EAP or PEAP Types to prevent authentication failure. If all clients are capable of negotiating EAP and PEAP types you should set the preferred methods to the one that most of your clients will be using to speed the authentication process.

A PEAP certificate file is required before the EAP-PEAP type is available to clients for authentication. See the next section on PEAP certificates for information on PEAP and how to create the required certificates. If you've installed Emerald with RadiusNT you can use Emeralds default sample certificate file 'ieas.pem' located in your Emerald folder as a PEAP certificate. Doing this will provide data encryption but will not provide certificate validation. You must disable certificate validation on the end users supplicant (client) when using the sample certificate. We recommend the included sample certificate be used for testing purposes only.

PEAP/TTLS certificates, signing requirements and examples

There are only minor differences between standard SSL certificates used by secure web sites and those used with PEAP on 802.1x wireless networks.

With PEAP the common name (cn) of the certificate is used to identify the certificate. It does not necessarily represent a hostname. Additionally an EKU (Enhanced Key Usage) for Server Authentication (OID 1.3.6.1.5.5.7.3.1) must be specified when creating your public certificate or signing request.

In these examples we will use the OpenSSL utility to create a Certificate Signing Request (CSR) used with a third party certificate authority such as Verisign or Thawte. We will also generate a 'self-signed' certificate that does not require a certificate authority but does require users to first accept your certificate as valid on a one time basis depending on the supplicant and its configuration.

The openssl utility used to create the certificates in this example is included with windows versions of Emerald and RadiusNT.

Example creating a certificate signing request for a certificate authority

```
openssl req -new -nodes -keyout private.pem -out public.csr -extensions PEAP -config openssl.cnf
```

```
Using configuration from openssl.cnf
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.....++++++
.............++++++
writing new private key to 'private.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Washington
Locality Name (eg, city) []:Spokane
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IEA Software, Inc.
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:ieas
Email Address []:support@iea-software.com
```

The output file public.csr is processed by your certificate authority (CA), which will return a signed certificate file to you. Combine private.pem with the certificate returned from the CA into a single file. This file becomes the 'PEAP Certificate' file. The resulting file should appear to have the following components representing public and private key pairs.

```
-----BEGIN RSA PRIVATE KEY-----
...
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
```

You will likely also need the CA's certificate chain file if one is required. This file becomes the 'PEAP CA Certificate'. The full pathnames for both files must be configured in the EAP section of the RadiusNT/X administrator.

Example creating a 'self-signed' certificate

```
openssl genrsa -out private.pem 2048
```

```
Loading 'screen' into random state - done
warning, not much extra random data, consider using the -rand option
Generating RSA private key, 2048 bit long modulus
.........................++++++++++++
..++++++++++++
e is 65537 (0x10001)
```

```
openssl req -new -x509 -key private.pem -out public.pem -extensions PEAP -config openssl.cnf -days 5000
```

```
Using configuration from openssl.cnf
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Washington
Locality Name (eg, city) []:Spokane
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IEA Software, Inc.
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:ieas
Email Address []:support@iea-software.com
```

Combine the two files private.pem and public.pem into one. The resulting file should appear to have the following components representing public and private key pairs.

```
-----BEGIN RSA PRIVATE KEY-----
...
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
```

The full pathname of this file becomes the 'PEAP/TTLS Certificate' file configured in the EAP section of the RadiusNT/X administrator. 'PEAP/TTLS CA Certificate' is not used and should be left blank.

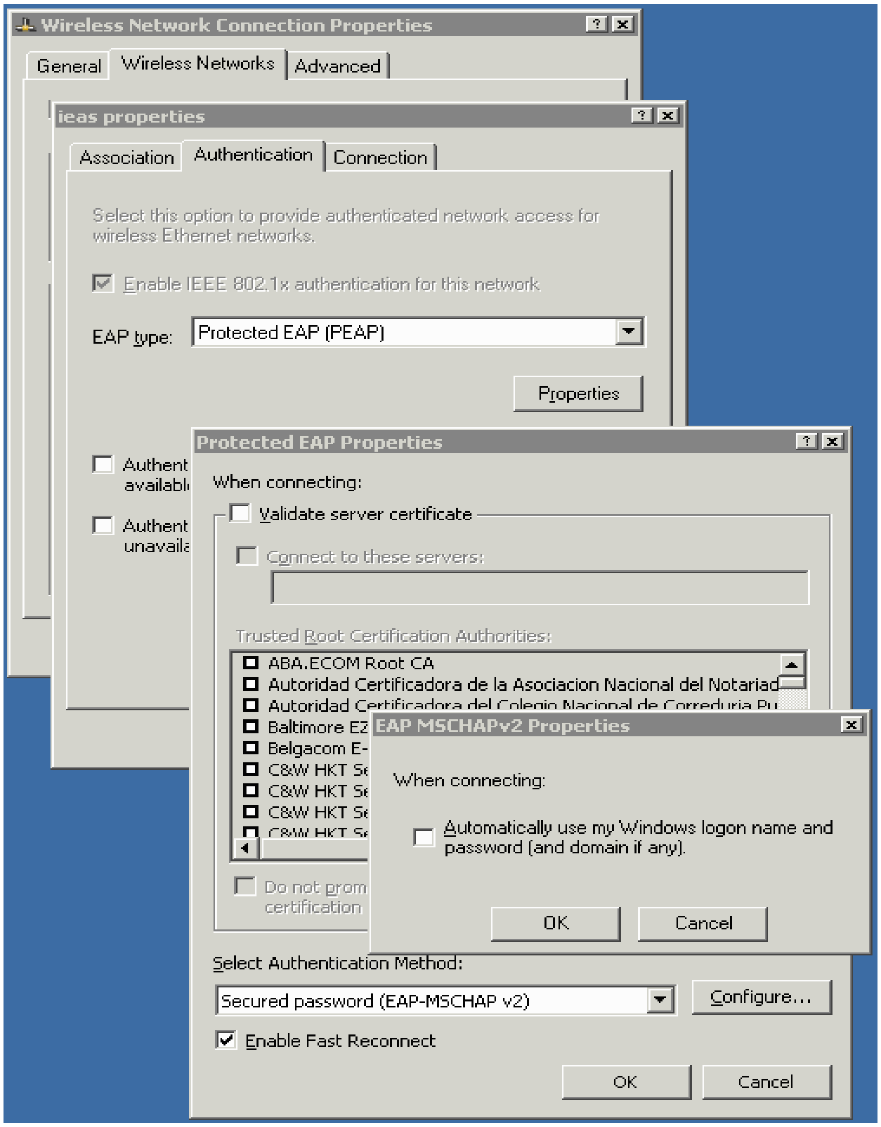
After configuring the PEAP certificate file locations, save your changes. Stop RadiusNT if running as a windows service and start RadiusNT/X in debug 'radius –x15 –X4'. At startup you should see all supported EAP types being registered.

```
Registered: EAP-Identity
Registered: EAP-GTC
Registered: EAP-MD5
Registered: EAP-LEAP
```

Registered: EAP-MSCHAPV2
Registered: EAP-PEAP
Registered: EAP-TTLS
Registered: EAP-PEAP-Identity
Registered: EAP-PEAP-GTC
Registered: EAP-PEAP-MSCHAPV2

If EAP-PEAP fails to register with a reason of N/A or missing file, check the file locations of the certificate files you created with the full pathname+filename entered for PEAP/TTLS Certificate and PEAP/TTLS CA Certificate in the RadiusNT/X admin.

Windows supplicant configuration example



Wireless Network Connection Properties

General | Wireless Networks | Advanced

ieas properties

Association | Authentication | Connection

Select this option to provide authenticated network access for wireless Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: Protected EAP (PEAP)

□ Authent availabl

□ Authent unavaila

Protected EAP Properties

When connecting:

□ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ ABA.ECOM Root CA
□ Autoridad Certificadora de la Asociacion Nacional del Notariad
□ Autoridad Certificadora del Colegio Nacional de Correduria Pu
□ Baltimore EZ
□ Belgacom E-
□ C&W HKT Se
□ C&W HKT Se
□ C&W HKT Se
□ C&W HKT Se

□ Do not prom certification

EAP MSCHAPv2 Properties

When connecting:

□ Automatically use my Windows logon name and password (and domain if any).

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect

Select PEAP as the eap type and EAP-MSCHAPv2 as the PEAP authentication method. If you created a PEAP certificate for use with your wireless network make sure the 'validate server certificate' checkbox is checked. If you are using the default ieas.pem certificate 'validate server certificate' must not be checked.

Wireless LAN supplicant interoperability

While our aim is maximum compatibility with all 802.1x supplicants unfortunately inconsistencies between clients sometimes require manual and confusing configuration of technical items to account for differences between implementations.

If you are experiencing compatibility problems with supplicants that have negotiated PEAP v1 our recommendation is to configure RadiusNT/X so that it is only able to negotiate PEAPv0 (Microsoft). Version 0 may tend to be more consistant between implementations due to Microsofts support of PEAPv0. Most supplicants capable of negotiating version 1 are also capable of negotiating version 0. Both versions offer the same features and security.

If you are experiencing a problem with a particular supplicant we recommend trying a different EAP protocol supported by RadiusNT/X such as EAP-TTLS. If there are still problems please follow the troubleshooting steps in the next section to help resolve or isolate and report the problem.

Questions & Answers

Q. Does RadiusNT/X support certificate only authentication such as EAP-TLS or EAP-PEAP phase 1 only?
A. No, while RadiusNT/X supports validating server and client certificates it also requires password authentication be performed before a client will successfully authenticate.

Q. I'm getting an error NO PASSWORD when authenticating using EAP, what could be wrong?
A. The most likely cause is that you are using a version of RadiusNT/X that does not support EAP or are not licensed for the feature. See the Versions and editions of RadiusNT/X supporting EAP Authentication section above.

Q. I'm getting an error SSL routines:SSL3_GET_CLIENT_HELLO when authenticating using PEAP. How can I fix this problem?
A. The most common cause of this error is not having a PEAP certificate installed. PEAP certificates are required to use EAP-PEAP. See the section above on PEAP certificates, signing requirements and examples for more information on creating a PEAP certificate.

Q. While authenticating clients RadiusNT/X reports the error 'PEAP err - SSL_write wants read, however the protocol has no provision for it'. What can I do to fix this problem?
A. The most likely cause is the client's failure to successfully validate the server's certificate. If your clients have certificate validation enabled and you have chosen a 'self-signed' server certificate make sure clients have the RadiusNT/X servers public key installed as a trusted certificate. On the windows platform this can be done by distributing the server's public key in a file with an extension of .cer. The user simply needs to right-click over the file and select 'Install certificate'. Disabling the clients certificate validation will also prevent the error however it bypasses the benefits associated with certificates. If you're using a third party Certificate Authority (CA) such as Verisign or Thawte make sure your CA's certificate chain file if required has also been installed in the RadiusNT/X administrator.

Q. I can't seem to authenticate using EAP, where should I look to find and solve this problem?
A. There are several possible sources of clues about EAP authentication failures. First and foremost run RadiusNT/X in debug mode using the following command-line parameters 'radius –x15 –X4'. Save a copy of all data shown during the authentication attempt. Another good source of information is debug or trace data from the supplicant (client). If not obvious from this data our support staff (support@iea-software.com) can assist you to further trouble shooting the problem. Possible authentication problems may be related to one of the following:

- Wrong default EAP type selected and supplicant (client) does not support EAP type negotiation.
- RadiusNT/X has multiple IP addresses on the same subnet and is not configured to bind to one of the two addresses.
- RadiusNT/X shared secret does not match access server shared secret
- Using PEAP without having first defined a PEAP certificate file in RadiusNT/X admin
- Client configured to validate server certificate when the server certificate is the default cert included with Emerald (ieas.pem) or another SSL certificate which does not have a Client Authentication EKU.
- RadiusNT is running as a service as well as debug mode.
- EAP type being used is not compatible with the backend authentication database.