**Certificate requirements when you use EAP-TLS or PEAP with EAP-TLS**

* 09/08/2020
* 4 minutes to read
  + 

* + 

This article describes the requirements that your client certificates and your server certificates must meet when you use Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) or Protected Extensible Authentication Protocol (PEAP) with EAP-TLS.

*Original product version:*   Windows 10 - all editions  
*Original KB number:*   814394

**Summary**

When you use EAP with a strong EAP type, such as TLS with smart cards or TLS with certificates, both the client and the server use certificates to verify their identities to each other. Certificates must meet specific requirements both on the server and on the client for successful authentication.

One requirement is that the certificate must be configured with one or more purposes in Extended Key Usage (EKU) extensions that match the certificate use. For example, a certificate that is used for the authentication of a client to a server must be configured with the Client Authentication purpose. Or, a certificate that is used for the authentication of a server must be configured with the Server Authentication purpose. When certificates are used for authentication, the authenticator examines the client certificate and looks for the correct purpose object identifier in EKU extensions. For example, the object identifier for the Client Authentication purpose is 1.3.6.1.5.5.7.3.2.

**Minimum certificate requirements**

All certificates that are used for network access authentication must meet the requirements for X.509 certificates, and they must also meet the requirements for connections that use Secure Sockets Layer (SSL) encryption and Transport Level Security (TLS) encryption. After these minimum requirements are met, both the client certificates and the server certificates must meet the following additional requirements.

**Client certificate requirements**

With either EAP-TLS or PEAP with EAP-TLS, the server accepts the client's authentication when the certificate meets the following requirements:

* The client certificate is issued by an enterprise certification authority (CA), or it maps to a user account or to a computer account in the Active Directory directory service.
* The user or the computer certificate on the client chains to a trusted root CA.
* The user or the computer certificate on the client includes the Client Authentication purpose.
* The user or the computer certificate does not fail any one of the checks that are performed by the CryptoAPI certificate store, and the certificate passes requirements in the remote access policy.
* The user or the computer certificate does not fail any one of the certificate object identifier checks that are specified in the Internet Authentication Service (IAS) remote access policy.
* The 802.1 **x** client does not use registry-based certificates that are either smart-card certificates or certificates that are protected with a password.
* The Subject Alternative Name (SubjectAltName) extension in the certificate contains the user principal name (UPN) of the user.
* When clients use EAP-TLS or PEAP with EAP-TLS authentication, a list of all the installed certificates is displayed in the Certificates snap-in, with the following exceptions:
  + Wireless clients do not display registry-based certificates and smart card logon certificates.
  + Wireless clients and virtual private network (VPN) clients do not display certificates that are protected with a password.
  + Certificates that do not contain the Client Authentication purpose in EKU extensions are not displayed.

**Server certificate requirements**

You can configure clients to validate server certificates by using the **Validate server certificate** option on the **Authentication** tab in the Network Connection properties. When a client uses PEAP-EAP-MS-Challenge Handshake Authentication Protocol (CHAP) version 2 authentication, PEAP with EAP-TLS authentication, or EAP-TLS authentication, the client accepts the server's certificate when the certificate meets the following requirements:

* The computer certificate on the server chains to one of the following:
  + A trusted Microsoft root CA.
  + A Microsoft stand-alone root or third-party root CA in an Active Directory domain that has an NTAuthCertificates store that contains the published root certificate. For more information about how to import third-party CA certificates, see [How to import third-party certification authority (CA) certificates into the Enterprise NTAuth store](https://support.microsoft.com/help/295663).
* The IAS or the VPN server computer certificate is configured with the Server Authentication purpose. The object identifier for Server Authentication is 1.3.6.1.5.5.7.3.1.
* The computer certificate does not fail any one of the checks that are performed by the CryptoAPI certificate store, and it does not fail any one of the requirements in the remote access policy.
* The name in the Subject line of the server certificate matches the name that is configured on the client for the connection.
* For wireless clients, the Subject Alternative Name (SubjectAltName) extension contains the server's fully qualified domain name (FQDN).
* If the client is configured to trust a server certificate with a specific name, the user is prompted to make a decision about trusting a certificate with a different name. If the user rejects the certificate, authentication fails. If the user accepts the certificate, the certificate is added to the local computer trusted root certificate store.

**Note**

With PEAP or with EAP-TLS authentication, servers display a list of all the installed certificates in the Certificates snap-in. However, the certificates that contain the Server Authentication purpose in EKU extensions are not displayed.