Extensible Authentication Protocol (EAP) Settings for Network Access

Updated: July 9, 2016

Applies To: Windows Server 2012, Windows 8

This topic presents information about the Extensible Authentication Protocol (EAP) default settings that you can use to configure computers running Windows® 8, Windows® 7, and Windows Vista®.

Authentication methods

This topic contains configuration information specific to the following authentication methods in EAP.

- **Protected EAP (PEAP)**

  Protected EAP Properties configuration items

  This section contains configuration information for the two default inner EAP methods that are provided with PEAP.

  - **EAP-Transport Layer Security (TLS)**

    Appears as **Smart Card or other Certificate Properties** in the operating system. EAP-TLS can be deployed as an inner method for PEAP or as a standalone EAP method. When it is configured as an inner authentication method, the configuration settings for EAP-TLS are identical to the settings that are used to deploy EAP-TLS as an outer method, except that it is configured to operate within PEAP. For configuration details, see Smart Card or other Certificate Properties configuration items.

  - **EAP-Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2)**

    Secure password (EAP-MSCHAP v2) Properties configuration items

    > **Note**
    >
    > EAP authentication methods that are used within tunneled EAP methods are commonly known as inner methods, and they are also referred to as **EAP types** in some documentation.

- **EAP-TLS**

  Smart Card or other Certificate Properties configuration items

  This section about Smart Card or other Certificate Properties includes information about the following configurations:

- Configure New Certificate Selection configuration items
- Select EKUs
- Add or Edit EKU

- **EAP-Tunneled Transport Layer Security (TTLS)**

  TTLS configuration items

- **EAP-Subscriber Identity Module (SIM), EAP-Authentication and Key Agreement (AKA), and EAP-AKA Prime (AKA')**

  EAP-SIM, EAP-AKA, and EAP-AKA'

  Enables authentication by using SIM cards, and is implemented when a customer purchases a wireless broadband service plan from a mobile network operator. As part of the plan, the customer commonly receives a wireless profile that is preconfigured for SIM authentication.

  This section provides information about the following configuration settings:

  - EAP-SIM
  - EAP-AKA
  - EAP-AKA'

EAP-TLS, PEAP, and EAP-TTLS

You can access the EAP properties for 802.1X authenticated wired and wireless access in the following ways:

- By configuring the Wired Network (IEEE 802.3) Policies and Wireless Network (IEEE 802.11) Policies extensions in Group Policy.
- By manually configuring wired or wireless connections on client computers.

You can access the EAP properties for virtual private network (VPN) connections in the following ways:

- By using Connection Manager Administration Kit (CMAK) to configure VPN connections.
- By manually configuring VPN connections on client computers.

By default, you can configure EAP settings for the following network authentication methods for 802.1X authenticated wired access, 802.1X authenticated wireless access, and VPN:

- **Microsoft: Smart Card or other Certificate** (EAP-TLS)

- **Microsoft: Protected EAP (PEAP)**
- **Microsoft: EAP-TTLS**

Additionally, the MS-CHAP-V2 network authentication method is available for VPN by default.

Protected EAP Properties configuration items

> **Important**
>
> Deploying the same type of authentication method for PEAP and EAP creates a security vulnerability. When you deploy both PEAP and EAP (which is not protected), do not use the same authentication type. For example, if you deploy PEAP-TLS, do not also deploy EAP-TLS.

Item	Details
Verify the Server's identity by validating the certificate	Specifies that the client verifies that server certificates presented to the client computer have the correct signatures, have not expired, and were issued by a trusted root certification authority (CA). **Important** If you disable this check box, client computers cannot verify the identity of your servers during the authentication process. If server authentication does not occur, users are exposed to severe security risks, including the possibility that users might unknowingly connect to a rogue network. Default = enabled
Connect to these servers	Allows you to specify the name for Remote Authentication Dial-In User Service (RADIUS) servers that provide network authentication and authorization. **Note** You must type the name exactly as it appears in the **Subject** field of each RADIUS server certificate, or use regular expressions to specify the server name. The complete syntax of the regular expression can be used to specify the server name, but to differentiate a regular expression with the literal string, you must use at least one "*" in the string specified. For example, you can specify *nps*.example.com* to specify the RADIUS server nps1.example.com or nps2.example.com.

	Defaults: • Wired and wireless = not enabled • VPN = enabled **Note** Even if no RADIUS servers are specified, the client will verify that the RADIUS server certificate was issued by a trusted root CA.
Trusted Root Certification Authorities	Lists the trusted root certification authorities. The list of trusted root certification authorities is built from the trusted root CAs that are installed in the computer and in the user certificate stores. You can specify which trusted root CA certificates supplicants use to determine whether they trust your servers, such as your server running Network Policy Server (NPS) or your provisioning server. If no trusted root CAs are selected, the 802.1X client verifies that the computer certificate of the RADIUS server was issued by an installed trusted root CA. If one or multiple trusted root CAs are selected, the 802.1X client verifies that the computer certificate of the RADIUS server was issued by a selected trusted root CA. If you have a public key infrastructure (PKI) on your network, and you use your CA to issue certificates to your RADIUS servers, your CA certificate is automatically added to the list of trusted root CAs. You can also purchase a CA certificate from a non-Microsoft vendor. Some non-Microsoft trusted root CAs provide software with your purchased certificate that automatically installs the purchased certificate into the **Trusted Root Certification Authorities** certificate store. In this case, the trusted root CA automatically appears in the list of trusted root CAs. **Note** Do not specify a trusted root CA certificate that is not already listed in client computers' **Trusted Root Certification Authorities** certificate stores for **Current User** and **Local Computer**. If you designate a certificate that is not installed on client computers, authentication will fail. Default = not enabled, no trusted root CAs selected. **Note** Even if no trusted root CAs are selected, the client will verify that the RADIUS server certificate was issued by a trusted root CA.

Notifications before connecting	Specifies whether the user is notified if the server name or root certificate is not specified, or whether the server's identity cannot be verified. By default, the following options are provided: • Case 1: **Do not ask user to authorize new servers or trusted CAs** specifies that if: 1. The server name is not in the **Connect to these servers** list 2. or the root certificate is found but is not selected in the list of **Trusted Root Certification Authorities** in **PEAP Properties** 3. or the root certificate is not found on the computer then the user is not notified, and the connection attempt fails. • Case 2: **Tell user if the server name or root certificate is not specified** specifies that if: 1. the server name is not in the **Connect to these servers** list 2. or the root certificate is found but is not selected in the list of **Trusted Root Certification Authorities** in **PEAP Properties** the user is prompted whether to accept the root certificate. If the user accepts the certificate, authentication proceeds. If the user rejects the certificate, the connection attempt fails. **Note** In this option, if the root certificate is not present on the computer, the user is not notified and the connection attempts fails. • Case 3: **Tell user if the server's identity cannot be verified** Specifies that if: 1. the server name is not in the **Connect to these servers** list 2. or the root certificate is found but is not selected in the list of **Trusted Root Certification Authorities** in **PEAP Properties** 3. or the root certificate is not found on the computer the user is prompted whether to accept the root certificate. If the user accepts the certificate, authentication proceeds. If the user rejects the certificate, the connection attempt fails.
Select Authentication Method	Allows you to select the EAP type to use with PEAP for network authentication. **Note** By default, two EAP types are available, **Secured password (EAP-MSCHAPv2)** and **Smart card or other certificate** (EAP-TLS). However, EAP is a flexible protocol that allows inclusion of additional EAP methods, and it is not restricted to these two types.

	For information about **Secured password (EAP-MSCHAPv2)** or **Smart card or other certificate** (EAP-TLS) configuration settings, see: • Secure password (EAP-MSCHAP v2) Properties configuration items • Smart Card or other Certificate Properties configuration items Default = **Secured password (EAP-MSCHAP v2)**
Configure	Provides access to property settings for the specified EAP type.
Enable Fast Reconnect	Enables the ability to create a new or refreshed security association more efficiently or in a smaller number of round- trips, in the case where a security association was previously established. For VPN connections, Fast Reconnect uses IKEv2 technology to provide seamless and consistent VPN connectivity, when users temporarily lose their Internet connections. Users who connect by using wireless mobile broadband will benefit most from this capability. An example of this benefit is a common scenario in which a user is traveling on a train, uses a wireless mobile broadband card to connect to the Internet, and then establishes a VPN connection to the corporate network. As the train passes through a tunnel, the Internet connection is lost. When the train is outside the tunnel, the wireless mobile broadband card automatically reconnects to the Internet. In client versions prior to Windows 7, VPN does not automatically reconnect. The user must repeat the multistep process to connect to the VPN each time Internet connectivity is interrupted. This can quickly become time consuming for mobile users with intermittent connectivity disruptions. In Windows 8, Fast Reconnect automatically re-establishes active VPN connections when Internet connectivity is re-established. Although the reconnection might take several seconds to occur, it is performed transparently to users. Default = enabled
Enforce Network Access Protection	Specifies that before connections to a network are permitted, system health checks are performed on EAP supplicants to determine if they meet system health requirements. Default = not enabled
Disconnect if server does not present cryptobinding TLV	Specifies that connecting clients must end the network authentication process if the RADIUS server does not present cryptobinding Type-Length-Value (TLV). **Note** Cryptobinding TLV increases the security of the TLS tunnel in PEAP by combining the inner method and the outer method authentications together so that attackers cannot perform man-in-the-middle attacks by redirecting an MS-CHAP v2 authentication by using the PEAP channel.

	Default = not enabled
Enable Identity Privacy	Specifies that clients are configured so that they cannot send their identity before the client has authenticated the RADIUS server, and optionally, provides a place to type an anonymous identity value. For example, if you select **Enable Identity Privacy**, and then type “guest” as the anonymous identity value, the identity response for a user with identity *alice@example* is *guest@example*. If you select **Enable Identity Privacy** but do not provide an anonymous identity value, the identity response for the user *alice@example* is *@example*. This setting applies only to computers running Windows 7 and Windows 8. Default = not enabled

Secure password (EAP-MSCHAP v2) Properties configuration items

Secure password EAP-MS-CHAP v2 is an EAP type that can be used with PEAP, for password-based network authentication. EAP-MsCHAPv2 can also be used as a standalone method for VPN, but only as a PEAP inner method for wireless.

Item	Details
Automatically use my Windows logon name and password (and domain if any)	Specifies that the current user-based Windows sign in name and password are used as network authentication credentials. Defaults: • Authenticated Wired and Wireless Access = enabled • VPN = not enabled

Smart Card or other Certificate Properties configuration items

Item	Details
Use my smart card	Specifies that clients making authentication requests must present a smart card certificate for network authentication. Defaults: • Wired and wireless = not enabled • VPN = enabled

Use a certificate on this computer	Specifies that authenticating clients must use a certificate located in the **Current User** or **Local Computer** certificate stores. Defaults: • Wired and wireless = enabled • VPN = not enabled
Use simple certificate selection (Recommended)	Specifies whether Windows filters out certificates that are unlikely to meet authentication requirements. This serves to limit the list of available certificates when prompting the user to select a certificate. Defaults: • Wired and wireless = enabled • VPN = not enabled
Advanced	Opens the **Configure Certificate Selection** dialog box. For more information about **Configure Certificate Selection**, see Configure New Certificate Selection configuration items.
Verify the server's identity by validating the certificate	Specifies that the client verifies that the server certificates presented to the client computer have the correct signatures, have not expired, and were issued by a trusted root certification authority (CA). **Important** Do not disable this check box or client computers cannot verify the identity of your servers during the authentication process. If server authentication does not occur, users are exposed to severe security risks, including the possibility that users might unknowingly connect to a rogue network. Default = enabled
Connect to these servers	Allows you to specify the name for RADIUS servers that provide network authentication and authorization. **Note** You must type the name exactly as it appears in the **Subject** field of each RADIUS server certificate, or use regular expressions to specify the server name. The complete syntax of the regular expression can be used to specify the server name, but to differentiate a regular expression with the literal string, you must use at least one "*" in the string that is specified. For example, you can specify *nps*.example.com* to

specify the RADIUS server nps1.example.com or nps2.example.com.

Defaults:

- Wired and wireless = not enabled
- VPN = enabled

Note

Even if no RADIUS servers are specified, the client will verify that the RADIUS server certificate was issued by a trusted root CA.

Trusted Root Certification Authorities

The list in **Trusted Root Certification Authorities** is built from the trusted root CAs that are installed in the computer and user certificate stores. You can specify which trusted root CA certificates that supplicants use to determine whether they trust your servers, such as your server running NPS or your provisioning server. If no trusted root CAs are selected, the 802.1X client verifies that the computer certificate of the RADIUS server was issued by an installed trusted root CA. If one or multiple trusted root CAs are selected, the 802.1X client verifies that the computer certificate of the RADIUS server was issued by a selected trusted root CA.

If you have a public key infrastructure (PKI) on your network, and you use your CA to issue certificates to your RADIUS servers, your CA certificate is automatically added to the list of trusted root CAs.

You can also purchase a CA certificate from a non-Microsoft vendor. Some non-Microsoft trusted root CAs provide software with your purchased certificate that automatically installs the purchased certificate into the **Trusted Root Certification Authorities** certificate store. In this case, the trusted root CA automatically appears in the list of trusted root CAs.

Do not specify a trusted root CA certificate that is not already listed in client computers' **Trusted Root Certification Authorities** certificate stores for **Current User** and **Local Computer**.

Note

If you designate a certificate that is not installed on client computers, authentication will fail.

Default = not enabled, no trusted root CAs selected.

Note

	Even if no trusted root CAs are selected, the client will verify that the RADIUS server certificate was issued by a trusted root CA.
View Certificate	Enables you to view the properties of the selected certificate.
Do not prompt user to authorize new servers or trusted certification authorities	Prevents the user from being prompted to trust a server certificate if that certificate is incorrectly configured, is not already trusted, or both (if enabled). It is recommended that you select this check box to simplify the user experience and to prevent users from inadvertently choosing to trust a server that is deployed by an attacker. Default = not enabled
Use a different user name for the connection	Specifies whether to use a user name for authentication that is different from the user name in the certificate. Default = not enabled

Configure New Certificate Selection configuration items

Use **New Certificate Selection** to configure the criteria that client computers use to automatically select the right certificate on the client computer for the purpose of authentication. When the configuration is provided to network client computers through the Wired Network (IEEE 802.3) Policies, the Wireless Network (IEEE 802.11) Policies, or through Connection Manager Administration Kit (CMAK) for VPN, clients are automatically provisioned with the specified authentication criteria.

Item	Details
Certificate Issuer	Specifies whether Certificate Issuer filtering is enabled. Default = not selected

Certificate Issuer list	Used to specify one or multiple certificate issuers for the certificates.
	
	Lists the names of all of the issuers for which corresponding certification authority (CA) certificates are present in the **Trusted Root Certification Authorities** or **Intermediate Certification Authorities** certificate store of local computer account.
	
	•
	  ○ Includes all the root certification authorities and intermediate certification authorities.
	  ○ Contains only those issuers for which there are corresponding valid certificates that are present on the computer (for example, certificates that are not expired or not revoked).
	
	The final list of certificates that are allowed for authentication contains only those certificates

	that were issued by any of the issuers selected in this list. Default = none selected
Extended Key Usage (EKU)	You can select **All Purpose**, **Client Authentication**, **Any purpose**, or any combination of these. Specifies that when a combination is selected, all the certificates satisfying at least one of the three conditions are considered valid certificates for the purpose of authenticating the client to the server. If EKU filtering is enabled, one of the choices must be selected; otherwise, the **OK** command control is disabled. Default = not enabled
All Purpose	Specifies that (when selected) certificates having the **All Purpose** EKU are considered valid certificates for the purpose of authenticating the client to the server. Default = selected when **Extended Key Usage (EKU)** is selected.
Client Authentication	Specifies that (when selected) certificates having the **Client Authentication** EKU, and the specified list of EKUs are considered valid certificates for the purpose of authenticating the client to the server. Default = selected when **Extended Key Usage (EKU)** is selected.
Add	Opens the Select EKUs dialog box, which enables you to add standard, custom, or vendor-specific EKUs to the **Client Authentication** list. Default = no EKUs listed
Remove	Removes the selected EKU item from the **Client Authentication** list. Default = N/A
Any Purpose	Specifies that (when selected) all certificates having **Any Purpose** EKU and the specified list of EKUs are considered valid certificates for the purpose of authenticating the client to the server. Default = selected when **Extended Key Usage (EKU)** is selected.
Add	Opens the Select EKUs dialog box, which enables you to add standard, custom, or vendor-specific EKUs into the **Any Purpose** list. Default = no EKUs listed
Remove	Removes the selected EKU item from the **Any Purpose** list. Default = N/A

Note

When both **Certificate Issuer** and **Extended Key Usage (EKU)** are enabled, only those certificates that satisfy

both conditions are considered valid for the purpose of authenticating the client to the server.

Select EKUs

You can select an EKU from the list provided, or add a new EKU.

Item	Details
Add	Opens the Add or Edit EKU dialog box, which enables you to define and add custom EKUs. In **Select the EKUs from the list below**, select an EKU in the list, and then click **OK** to add that EKU to the **Client Authentication** or the **Any Purpose** list.
Edit	Opens the Add or Edit EKU dialog box, and enables you to edit custom EKUs that you have added. You cannot edit the default, predefined EKUs.
Remove	Removes the selected custom EKU from the list of EKUs in the Select EKUs dialog box. You cannot remove the default, predefined EKUs.

Add or Edit EKU

Item	Details
Enter the name of the EKU	Provides a place to type the name of the custom EKU.
Enter the EKU OID:	Provides a place to type the OID for the EKU. Only numeric digits, separators, and "." are allowed. Wild cards are permitted, in which case all of the child OIDs in the hierarchy are allowed. For example, entering **1.3.6.1.4.1.311.*** allows 1.3.6.1.4.1.311.42 and 1.3.6.1.4.1.311.42.2.1

TTLS configuration items

EAP-TTLS is a standards-based EAP tunneling method that supports mutual authentication and provides a secure tunnel for client inclusion authentication by using EAP methods and other legacy protocols. The addition of EAP-TTLS in Windows Server 2012 provides only client-side support, for the purpose of supporting interoperation with the most commonly-deployed RADIUS servers that support EAP-TTLS.

Item	Description
Enable Identity Privacy	Specifies that clients are configured so that they cannot send their identity before the client has authenticated the RADIUS server, and optionally, provides a place to type an anonymous identity value. For example, if you select **Enable Identity Privacy**, and then type "guest" as the anonymous identity value, the identity response for a user with identity *alice@example* is *guest@example*. If you select **Enable Identity Privacy** but do not provide an anonymous identity value, the identity response for the user *alice@example* is *@example*. This setting applies only to computers running Windows 8. Default = not enabled
Connect to these servers	Enables you to specify the name for RADIUS servers that provide network authentication and authorization. **Note** You must type the name exactly as it appears in the **Subject** field of each RADIUS server certificate, or use regular expressions to specify the server name. The complete syntax of the regular expression can be used to specify the server name. But to differentiate a regular expression with the literal string, you must use at least one '*' in the string specified. For example, you can specify *nps*.example.com* to specify the RADIUS server nps1.example.com or nps2.example.com. Defaults: = none **Note** Even if no RADIUS servers are specified, the client will verify that the RADIUS server certificate was issued by a trusted root CA.
Trusted Root Certification Authorities	The list in **Trusted Root Certification Authorities** is built from the trusted root CAs that are installed in the computer and user certificate stores. You can specify which trusted root CA certificates that supplicants use to determine whether they trust your servers, such as your server running NPS or your provisioning server. If no trusted root CAs are selected, the 802.1X client verifies that the computer certificate of the RADIUS server was issued by an installed trusted root CA. If one or multiple trusted root CAs are selected, the 802.1X client verifies that the computer certificate of the RADIUS server was issued by a selected trusted root CA. If you have a public key infrastructure (PKI) on your network, and you use your CA to issue certificates to your RADIUS servers, your CA certificate is automatically added to the list of trusted root CAs. If selected, your root CA certificate is installed on a client computer when the computers are joined to the domain.

	You can also purchase a CA certificate from a non-Microsoft vendor. Some non-Microsoft trusted root CAs provide software with your purchased certificate that automatically installs the purchased certificate into the **Trusted Root Certification Authorities** certificate store. In this case, the trusted root CA automatically appears in the list of trusted root CAs. Do not specify a trusted root CA certificate that is not already listed in client computers' **Trusted Root Certification Authorities** certificate stores for **Current User** and **Local Computer**. **Note** If you designate a certificate that is not installed on client computers, authentication will fail. Default = not enabled, no trusted root CAs selected. **Note** Even if no trusted root CAs are selected, the client will verify that the RADIUS server certificate was issued by a trusted root CA.
Do not prompt user if unable to authorize server	Specifies (when not selected) that if server certificate validation fails due to any of the following reasons, the user is prompted to accept or reject the server: • A root certificate for the server certificate is not found or not selected in the **Trusted Root Certification Authorities** list. • One or more of the intermediate root certificates in the certificate chain is not found. • The subject name in the server certificate does not match any of the servers that are specified in the **Connect to these servers** list. Default = not selected
Select a non-EAP method for authentication	Specifies whether a non-EAP or an EAP type is used for authentication. If **Select a non-EAP method for authentication** is selected, **Select an EAP method for authentication** is disabled. If **Select a non-EAP method for authentication** is selected, the following non-EAP authentication types are provided in the drop-down list: • PAP • CHAP • MS-CHAP • MS-CHAP v2 Defaults: • **Select a non-EAP method for authentication** = enabled

	• Non-EAP type = PAP
Automatically use my Windows logon name and password	Uses Windows sign in credentials when enabled. This check-box is enabled only if **MS-CHAP v2** is selected in the **Select a non-EAP method for authentication** drop-down list. **Automatically use my Windows logon name and password** is disabled for PAP, CHAP and MS-CHAP authentication types.
Select an EAP method for authentication	Specifies whether an EAP type or a non-EAP type is used for authentication. If **Select an EAP method for authentication** is selected, **Select a non-EAP method for authentication** is disabled. If **Select a non-EAP method for authentication** is selected, by default, the following non-EAP authentication types are provided in the drop-down list: • Microsoft: Smart Card or other Certificate • Microsoft: MS-CHAP v2 • MS-CHAP • MS-CHAP v2 **Note** The **Select an EAP method for authentication** drop-down list will enumerate all the EAP methods that are installed on the server, except for PEAP and FAST tunnel methods. The EAP types are listed in the order that they are discovered by the computer.
Configure	Opens the properties dialog box of the specified EAP type. For details about the default EAP-types, see Smart Card or other Certificate Properties configuration items or Secure password (EAP-MSCHAP v2) Properties configuration items.

EAP-SIM, EAP-AKA, and EAP-AKA'

The following tables list the configuration settings for:

- EAP-SIM
- EAP-AKA
- EAP-AKA'

EAP-SIM

EAP Subscriber Identity Module (SIM) is used for authentication and session key distribution for the Global System for Mobile Communications (GSM). EAP-SIM is defined in RFC 4186.

EAP-SIM Properties

Item	Description
Use strong Cipher keys	Specifies that if selected, the profile uses strong encryption.
Do not reveal real identity to server when pseudonym identity is available	When enabled, forces the client to fail the authentication if server requests for permanent identity though the client have a pseudonym identity with it. Pseudonym identities are used for identity privacy so that the actual or permanent identity of a user is not revealed during authentication.
Enable usage of realms	Provides a place to type the realm name. If this field is left blank with **Enabled usage of realms** selected, the realm is derived from the International Mobile Subscriber Identity (IMSI) using the realm 3gpp.org, as described in the 3rd Generation Partnership Project (3GPP) standard 23.003 V6.8.0.
Specify a realm:	Provides a place to type the realm name.

EAP-AKA

EAP Authentication and Key Agreement (AKA) for Universal Mobile Telecommunications System (UMTS) is used for authentication and session key distribution by using the UMTS Universal Subscriber Identity Module (USIM). EAP AKA is defined in RFC 4187.

EAP-AKA Properties

Item	Description
Do not reveal real identity to server when pseudonym identity is available	When enabled, forces the client to fail the authentication if server requests for permanent identity though the client have a pseudonym identity with it. Pseudonym identities are used for identity privacy so that the actual or permanent identity of a user is not revealed during authentication.
Enable usage of realms	Provides a place to type the realm name. If this field is left blank with **Enabled usage of realms** selected, the realm is derived from the International Mobile Subscriber Identity (IMSI) using the realm 3gpp.org, as described in the 3rd Generation Partnership Project (3GPP) standard 23.003 V6.8.0.
Specify a realm	Provides a place to type the realm name.

EAP-AKA'

EAP- AKA Prime (AKA') is a modified version of EAP-AKA that is used to enable access to the 3rd-Generation Partnership Project (3GPP)-based networks by using non-3GPP standards, such as:

- WiFi - sometimes referred to as wireless fidelity
- Evolution-Data Optimized (EVDO)
- Worldwide Interoperability for Microwave Access (WiMax)

EAP-AKA' is defined in RFC 5448.

EAP-AKA' Properties

Item	Description
Do not reveal real identity to server when pseudonym identity is available	When enabled, forces the client to fail the authentication if server requests for permanent identity though the client have a pseudonym identity with it. Pseudonym identities are used for identity privacy so that the actual or permanent identity of a user is not revealed during authentication.
Enable usage of realms	Provides a place to type the realm name. If this field is left blank with **Enabled usage of realms** selected, the realm is derived from the International Mobile Subscriber Identity (IMSI) using the realm 3gpp.org, as described in the 3rd Generation Partnership Project (3GPP) standard 23.003 V6.8.0.
Specify a realm	Provides a place to type the realm name.
Ignore network name mismatch	The client compares the name of network known to it, with the name sent by the RADIUS server during authentication. If there is mismatch: • If selected, the mismatch is ignored. • If not selected, authentication fails.
Enable Fast Reauthentication	Specifies that fast reauthentication is enabled. Fast Reauthentication is useful when SIM authentication happens frequently. The encryption keys that are derived from full authentication are reused. As a result, the SIM algorithm is not required to run for every authentication attempt, and the number of network operations that result from frequent authentication attempts is reduced.

Additional resources

For additional information about authenticated wireless settings in Group Policy, see Managing the New Wireless Network

(IEEE 802.11) Policies Settings

For additional information about authenticated wired settings in Group Policy, see Managing the New Wired Network (IEEE 802.3) Policies Settings

For information about advanced settings for authenticated wired access and authenticated wireless access, see Advanced Security Settings for Wired and Wireless Network Policies.

Extensible Authentication Protocol (EAP)