CHAPTER 3

# Configuring EAP Types

This chapter explains the EAP types that are used for authenication to wireless networks.

The following topics are covered:



## Overview of EAP-FAST

**Note** For additional information about EAP-FAST, see RFC4851.

EAP-FAST is an EAP method that enables secure communication between a client and an authentication server by using Transport Layer Security (TLS) to establish a mutually authenticated tunnel. Within the tunnel, data in the form of type, length, and value (TLV) objects are used to send further authentication-related data between the client and the authentication server.

EAP-FAST supports the TLS extension as defined in RFC 4507 to support the fast re-establishment of the secure tunnel without having to maintain per-session state on the server. EAP-FAST-based mechanisms are defined to provision the credentials for the TLS extension. These credentials are called Protected Access Credentials (PACs).

EAP-FAST provides the following:

- Mutual authentication

  An EAP server must be able to verify the identity and authenticity of the client, and the client must be able to verify the authenticity of the EAP server.

- Immunity to passive dictionary attacks

Many authentication protocols require a password to be explicitly provided (either as cleartext or hashed) by the client to the EAP server. The communication of the weak credential (such as a password) must be immune from eavesdropping.

- Immunity to man-in-the-middle (MitM) attacks

  In establishing a mutually authenticated protected tunnel, the protocol must prevent adversaries from successfully interjecting information into the communication between the client and the EAP server.

- Flexibility to enable support for most password authentication interfaces

  Many different password interfaces exist to authenticate a client—for example, Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), Lightweight Directory Access Protocol (LDAP), and One-Time Password (OTP). EAP-FAST provides support for these different password types.

- Efficiency in computational and power resources

  Especially when using wireless media, clients have limited computational and power resources. EAP-FAST enables network access communication to occur in a more efficient manner.

- Flexibility to extend the communications inside the tunnel

  Because network infrastructures are becoming increasingly complex, authentication, authorization, and accounting is also becoming more complex. For example, there are instances in which multiple existing authentication protocols are required to achieve mutual authentication. Also, different protected conversations might be required to achieve the proper authorization when a client has successfully authenticated.

- Minimize authentication server requirements for per-user authentication

  With large deployments, it is typical to have several servers that act as authentication servers for several clients. A client uses the same shared secret to secure a tunnel in much the same way that is uses a username and password to gain access to the network. EAP-FAST facilitates the use of a single strong shared secret by the client, while enabling the authentication servers to minimize the per-user and device state that they must cache and manage.

# How EAP-FAST Works

The following sections describe how EAP-FAST works:



## Two-Phase Tunneled Authentication

EAP-FAST uses a two-phase tunneled authentication process.

In the first phase of authentication, EAP-FAST employs the TLS handshake to provide an authenticated key exchange and to establish a protected tunnel between the client and the authentication server. The tunnel protects client identity information from disclosure outside the tunnel. During this phase, the client and the server engage in EAP-FAST version negotiation to ensure that they are using a compatible version of the protocol.

After the tunnel is established, the second phase of authentication begins. The client and server communicate further to establish the required authentication and authorization policies. This phase consists of a series of requests and responses that are encapsulated in TLV objects. The TLV exchange includes the EAP method to be used within the protected tunnel. For more information about TLV objects and format, see section 4.2 of RFC 4851.

The EAP-FAST module offers a variety of EAP-FAST configuration options, including whether automatic or manual PAC provisioning is used to establish a tunnel, whether or not server certificate is used to establish a tunnel, what type of user credentials to use for authentication and provisioning, and what type of authentication method to use to in the established tunnel.

# Protected Access Credentials

Protected Access Credentials (PACs) are credentials that are distributed to clients for optimized network authentication. PACs can be used to establish an authentication tunnel between the client and the authentication server (the first phase of authentication as described in the "Two-Phase Tunneled Authentication" section on page 3-2). A PAC consists of, at most, three components: a shared secret, an opaque element, and other information.

The shared secret component contains the pre-shared key between the client and authentication server. Called the PAC-Key, this pre-shared key establishes the tunnel in the first phase of authentication.

The opaque component is provided to the client and is presented to the authentication server when the client wants to obtain access to network resources. Called the PAC-Opaque, this component is a variable length field that is sent to the authentication server during tunnel establishment. The EAP server interprets the PAC-Opaque to obtain the required information to validate the client's identity and authentication. The PAC-Opaque includes the PAC-Key and may contain the PAC's client identity.

The PAC might contain other information. Called PAC-Info, this component is a variable length field that is used to provide, at a minimum, the authority identity of the PAC issuer (the server that created the PAC). Other useful but not mandatory information, such as the PAC-Key lifetime, can also be conveyed by the PAC-issuing server to the client during PAC provisioning or refreshment.

PACs are created and issued by a PAC authority, such as Cisco Secure ACS, and are identified by an ID. A user obtains his or her own copy of a PAC from a server, and the ID links the PAC to a profile.

Persistent PACs, such as machine PACs, are stored in the EAP-FAST registry and encrypted. These PACs are also protected with access control lists (ACLs) so only designated users (the owners of the PACs) and members of privileged user groups (for example, administrators) can access them. Machine PACs are stored globally so that all users of a machine can use the PACs.

All PACs are encrypted and tied to the host machine with Microsoft Crypto API (CryptoProtectData). PACs cannot be copied and used on other machines.

All non-persistent PACs, such as User Authorization PACs, are stored in volatile memory and do not persist after reboot or after a user has logged off.

# Server Certificate Validation

As a part of TLS negotiation in the first phase of EAP-FAST authentication, the authentication server presents the client with a certificate. The client must verify the validity of the EAP server certificate and also examines the EAP server name that is presented in order to determine if the server can be trusted.

# Configuring EAP-FAST

This section explains how to configure EAP-FAST module settings, such as connection settings, user credentials, and authentication methods. The following topics are covered:



## Accessing EAP-FAST Properties for Configuration

To access the EAP-FAST Properties window, perform the following steps:

**Step 1** Click the **Start** button on the lower-left corner of the desktop.

**Step 2** From the right pane, right-click **Network**.

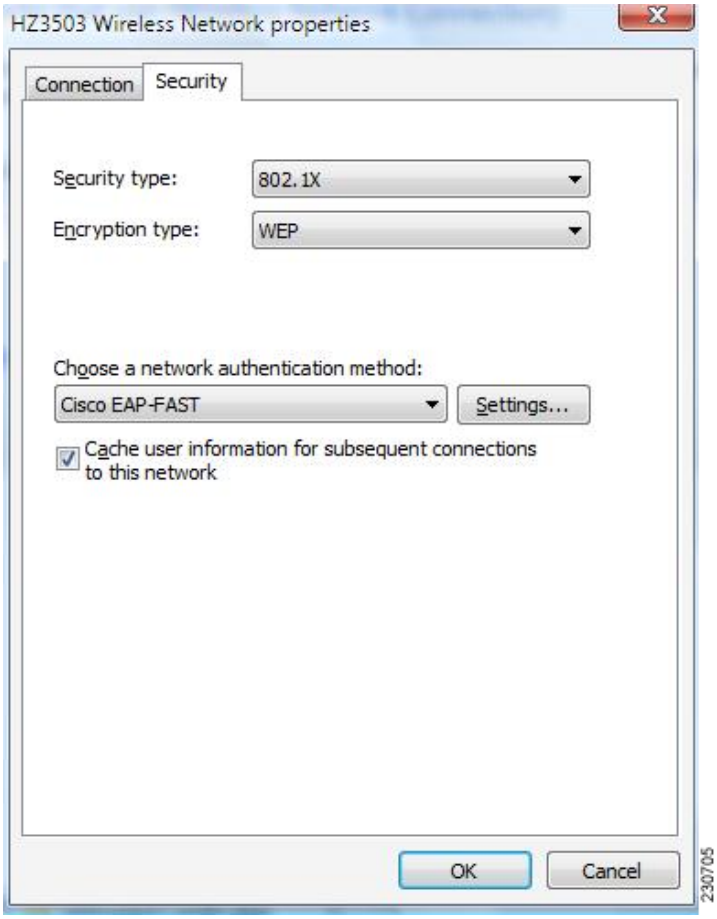
**Step 3** Select **Properties**.

**Step 4** From the left pane, select **Manage wireless networks**.

**Step 5** Double-click the wireless network.

**Step 6** From the **Wireless Network properties** window, select the **Security** tab (see Figure 3-1).

*Figure 3-1 Wireless Network Properties Window*




**Step 7** Select **Cisco EAP-FAST** from the "Choose a network authentication method" drop down list.

**Step 8** Click the **Settings** button.

**Step 9** Click the **Connection** tab, the **User Credentials** tab, the **Authentication** tab, or the **About** tab. For more information about configuring settings in those tabs, see the "Configuring EAP-FAST Settings in the Connection Tab" section on page 3-6, the "Configuring EAP-FAST Settings in the User Credentials Tab" section on page 3-10, and the "Configuring EAP-FAST Settings in the Authentication Tab" section on page 3-13. For information about finding the version of the module on the device, see the "Finding the Version of the EAP-FAST Module" section on page 3-16.

**Note** For single sign-on to work when an EAP-FAST profile is used and the selected authentication method is EAP-GTC, you must check the **Cache user information for subsequent connections to this network** check box. The credentials pop-up dialog box appears with the first authentication.

# Configuring EAP-FAST Settings in the Connection Tab

The EAP-FAST Connection tab includes settings for the establishment of an outer Transport Layer Security (TLS) tunnel. Settings include identity protection, the use of a Protected Access Credential (PAC), PAC provisioning, the use of authenticated server certificates to establish the tunnel, and the use of a Trusted Root Certificate Authority (CA) from a list of Trusted Root CA certificates.

You can configure connection settings from the Connection tab (see Figure 3-2).

***Figure 3-2 Connection Tab in EAP-FAST Properties Window***

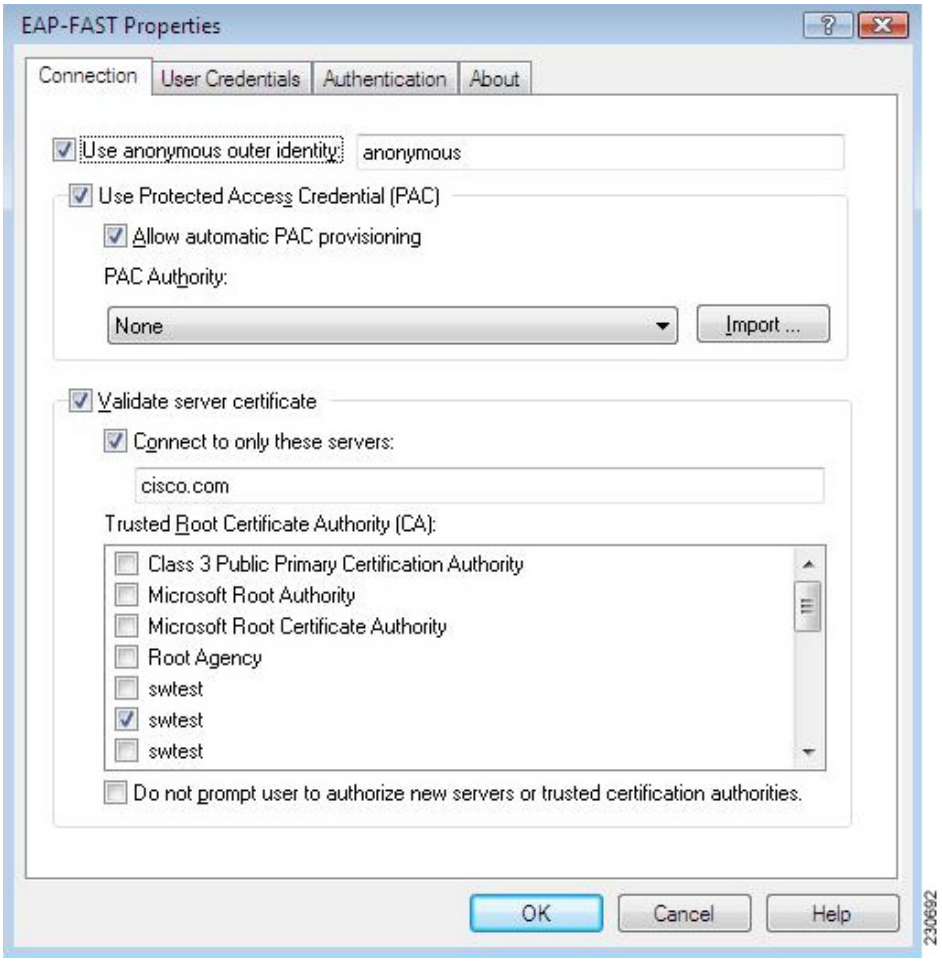


Table 3-2 lists and describes all connection settings.

***Table 3-1 Connection Settings***

| Connection Settings | Description |
|---|---|
| Use anonymous outer identity | Check this box to enable identity privacy protection.<br>**Default:** On |
| Outer identity field | Enter an outer identity if the Use anonymous outer identity check box is checked. Follow an administrator's instructions, or follow RFC 4282 for guidelines about what to enter in the outer identity field.<br>**Default:** anonymous<br>**Note** The maximum number of characters allowed in this field is 256. |
| Use Protected Access Credential (PAC) | Check this box to enable the use of a PAC to establish a tunnel. When this box is checked, PAC provisioning is requested. If this box is not checked, EAP-FAST acts as PEAP and uses only the authenticated server certificate to establish the tunnel every time.<br>The PAC is a unique shared credential used to mutually authenticate a client and a server. The PAC is associated with a specific client username and a server authority ID. A PAC removes the need for PKI and digital certificates. The PAC is distributed or imported to the client automatically or manually.<br>Manual PAC provisioning generates the PAC file locally on the AAA or EAP-FAST server. With manual provisioning, the user credentials are supplied to the server to generate the PAC file for that user. This PAC must then be manually installed on the client device.<br>**Default:** On |
| Allow automatic PAC provisioning | Check this box to enable the automatic retrieval of a PAC during EAP-FAST authentication.<br>Automatic PAC provisioning enables the automatic retrieval of a PAC during EAP-FAST authentication. Automatic PAC provisioning uses TLS with a Diffie-Hellman Key Agreement protocol to establish a secure tunnel. In addition, MSCHAPv2 is used to authenticate the client and for early man-in-the-middle (MITM) attack detection.<br>**Default:** On |
| PAC Authority | Select a PAC authority from the drop-down list.<br>**Default:** None<br>**Note** The drop-down list contains the names of all of the PAC authorities from which you have previously provisioned a tunnel PAC. If you have not provisioned a PAC, then "none" is the only option. You can also select "none" to force the host to request provisioning a PAC. |

*Table 3-1 Connection Settings (continued)*

| Connection Settings | Description |
|---|---|
| Import | Click the **Import** button to manually import a PAC file. When you click on this button, the Import Protected Access Credentials (PAC) File window appears. If you need to enter a password for the PAC file that you have selected, a password window will appear.<br><br>After you have selected and imported a valid PAC file, the PAC authority is added to the PAC authority drop-down list.<br><br>**Default:** Enabled |
| Validate server certificate | Check this box to use an authenticated server certificate to establish a tunnel. You can check both the **Use Protected Access Credentials (PAC)** box and the **Validate Server Certificate** box at the same time. If both are checked, you can select one or more Trusted Root CA certificates from the list of trusted Certificate Authority certificates that are installed on the host system.<br><br>The EAP-FAST module always tries to use the PAC first if both check boxes are checked. The module uses the server certifcate if the PAC is missing or rejected by the server.<br><br>If both check boxes are unchecked, EAP-FAST functions as PEAP does without validating server certificate. We do not recommend leaving both boxes unchecked because the module bypasses fundamental trust validation.<br><br>**Default:** Off |
| Connect to only these servers | Check this box to enter an optional server name that must match the server certificate that is presented by the server. You can enter multiple server names; separate multiple server names with semicolons. The EAP-FAST module only allows connections to continue without prompting if the subject field (CN) in the server certificate matches the server names that you enter in this field.<br><br>**Default:** Off<br><br>**Note** You can use an asterisk (*) as a wildcard character in server names only if the asterisk appears before the first period (.) in the name.domain.com format. For example, "*.cisco.com" matches any server name that ends with ".cisco.com." If you put an asterisk anywhere else in the server name, it is not treated as a wildcard character. |

*Table 3-1 Connection Settings (continued)*

| Connection Settings | Description |
|---|---|
| Trusted Root CA | Select one of more Trusted Root CA certificates from the list of certificates that are installed on the system. Only trusted CA certificates that are installed on the host system are displayed in the drop-down list.<br>To view details about the selected Trusted Root CA certificate, double-click the certificate name. Double-clicking the certificate name opens the Windows certificate property screen, where certificate details are available.<br>**Default:** None |
| Do not prompt user to authorize new servers or trusted certificate authorities. | Check this box if you do not want the user to be prompted to authorize a connection when the server name does not match or the server certificate is not signed by one of the Trusted Root CA certiticates that was selected. If this box is checked, the authentication fails.<br>**Default:** Off |

# Overview of the User Credentials Tab

The EAP-FAST module supports the use of both a client certificate and a username and password as user credentials for authentication and provisioning.

# Client Certificates

If a client certificate is used, the EAP-FAST module automatically obtains the client certificate from the Windows certificate store of the current user. The EAP-FAST module finds the user certificate that matches the username of the user who is logged on. The certificate cannot be expired.

If multiple user certificates are available, the EAP-FAST module prompts the user to select one, and that selection is saved to the profile. By default, the user certificate is sent securely through TLS renegotiation or through the EAP-TLS inner method in the protected TLS tunnel. If the EAP-FAST server does not start TLS renegotiation to request the client certificate after the tunnel is established, then the EAP-FAST module sends the certificate through the EAP-TLS inner method.

The EAP-FAST module administrator can configure the EAP-FAST module XML schema to send the user certificate without using these security measures.

# Usernames and Passwords

If a username and password are used, the user provide one of the following types of username and password:

- Windows username and password—The Windows username and password are used as network access credentials. The user is not prompted to enter the username and password unless the password is invalid or must be changed.
- Prompted user credentials—The user is prompted during authentication for credentials. These credentials are credentials that are separate from the Windows username and password, such as Lightweight Directory Access Protocol (LDAP) credentials.

- Saved user credentials—These are user credentials that are entered as part of the EAP-FAST configuration. The user is not prompted for credentials during authentication unless the saved credentials fail or have expired. New credentials that the user enters after successful authentication are saved automatically in the configuration. The user does not have to return to the configuration screen to change the old saved credentials.
- One-time password (OTP)—The user must manually enter a OTP. New PIN mode and next token mode for OTP are supported.

# Configuring EAP-FAST Settings in the User Credentials Tab

The user can configure user credentials from the User Credentials tab (see Figure 3-3).

***Figure 3-3 User Credentials Tab in EAP-FAST Properties Window***

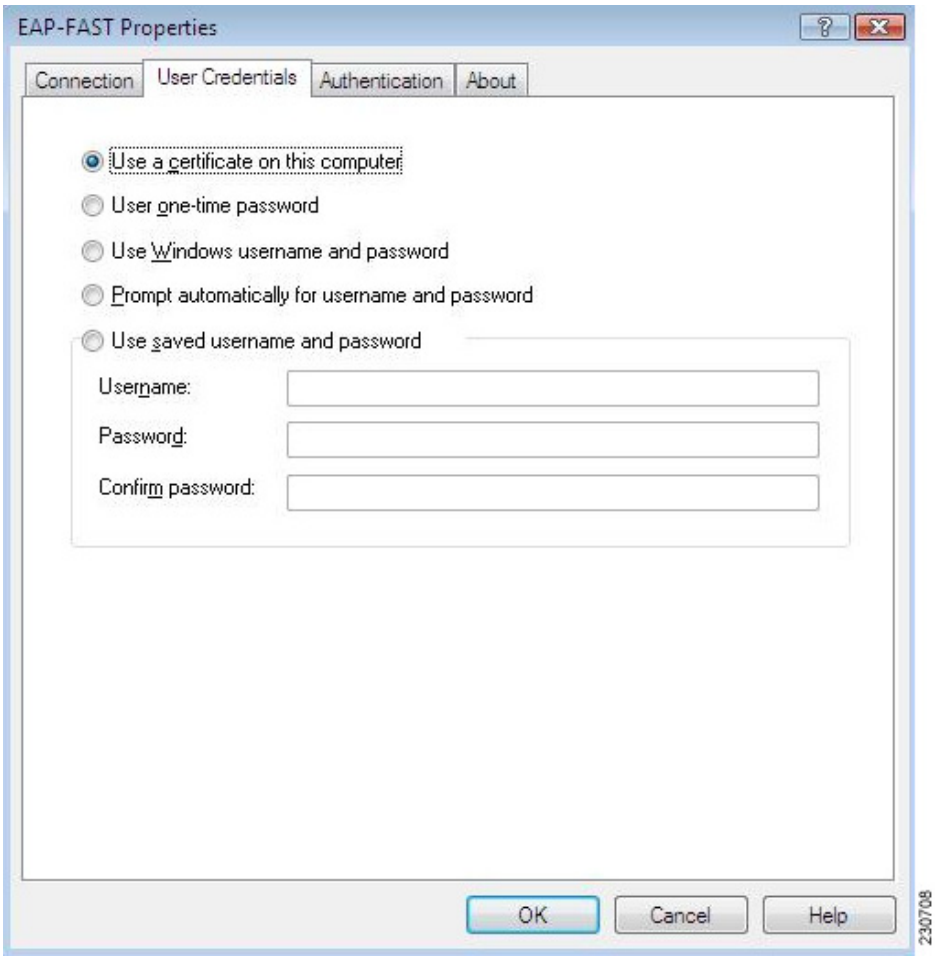



Table 3-2 lists and describes all options for user credentials.

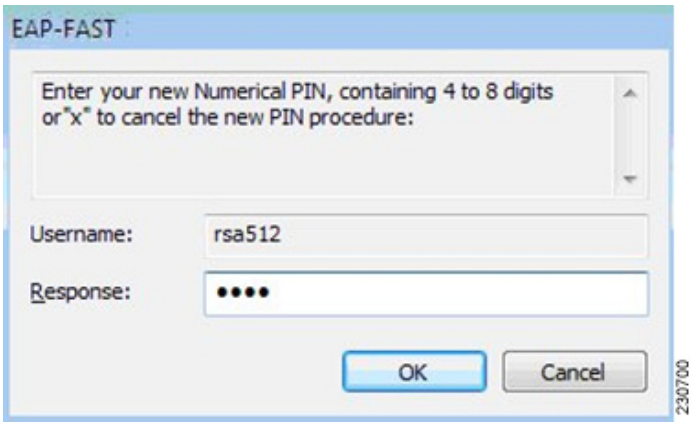
*Table 3-2 User Credentials Options*

| User Credentials | Description |
|---|---|
| Use a certificate on this computer | Click this radio button to automatically obtain the client certificate from the Windows certificate store of the current user.<br>**Default:** Off |
| Use one-time password | Click this radio button to use a one-time password (OTP). For more information about OTP, see the "Understanding PIN Mode and Token Mode with OTP" section on page 3-12.<br>**Default:** Off |
| Use Windows username and password | Click this radio button to use the Windows username and password as the EAP-FAST username and password for network authentication.<br>**Default:** On |
| Prompt automatically for username and password | Click this radio button to require the user to enter a separate EAP-FAST username and password in addition to a Windows username and password with every authentication attempt. This options supports non-Windows passwords, such as LDAP.<br>**Default:** Off |
| Use saved username and password | Click this radio button so that the user is not required to enter an EAP-FAST username and password each time. Authentication occurs automatically as needed using a saved user name and password, which are registered with the backend server.<br>**Default:** Off<br>When selecting this option, the user must enter the following:<br>• Username—Enter the username and the domain name in one of these two formats:<br>– Domain-qualified user name—domain\user<br>– User Principal Name (UPN)—user@domain.com<br>• Password—Enter a password. This encrypted password is stored in the EAP-FAST configuration.<br>• Confirm password—Enter the password again to verify that it was entered correctly.<br>**Note** The maximum number of characters allowed for the username and password is 256. |

# Understanding PIN Mode and Token Mode with OTP

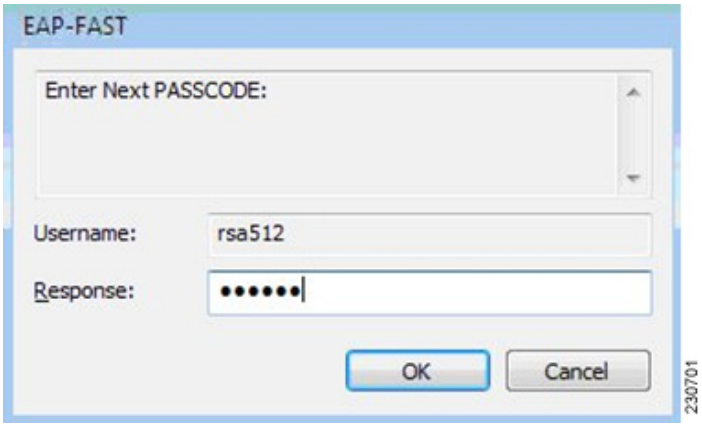
New PIN mode for OTP is supported. If a new PIN is needed, the backend server sends a text message (for example, “Enter New PIN”) to indicate that a new PIN is neeeded. The EAP-FAST module displays a prompt window that includes the text message from the server (see Figure 3-4). The backend server might prompt the user twice to confirm the new PIN that the user entered.

***Figure 3-4 New PIN Prompt Window***




Next Token mode for OTP is also supported. If the next token is needed, the backend server sends a text message (for example, “Enter Next PASSCODE:”) to indicate that the next token is needed. The EAP-FAST module displays a prompt window that includes the text message sent from the server (see Figure 3-5). The user must get the next token from the OTP device or from the software and enter it in the prompt field.

***Figure 3-5 Next Token Prompt Window***



# Configuring EAP-FAST Settings in the Authentication Tab

The EAP-FAST module supports three authentication methods: EAP-GTC, EAP-MSCHAPv2, and EAP-TLS.

These three authentication methods use the following types of credentials:

- EAP-GTC—Active Directory password, OTP, Token, LDAP
- EAP-MSCHAPv2—Active Directory password
- EAP-TLS—certificate

The EAP-GTC module is bundled with the EAP-FAST module. The EAP-GTC module is not registered with the EAPHost framework; it is not available to other applications.

A modified version of the EAP-MSCHAPv2 module is also bundled with the EAP-FAST module. This modified version is used in anonymous TLS provisioning mode to support the modification of EAP-MSCHAPv2 challenges. This same module also supports user authentication in authentication mode without modification.

The EAP-FAST module uses the standard EAP-TLS module that is shipped with Windows Vista.

The user can select only one of these three inner authentication methods through the user interface. Although other third-party EAP methods are registered with the EAPHost framework and can be selected in the administrator interface, these methods have not been officially tested.

You can choose settings for authentication in the Authentication tab (see Figure 3-6).

***Figure 3-6 Authentication Tab in EAP-FAST Properties Window***

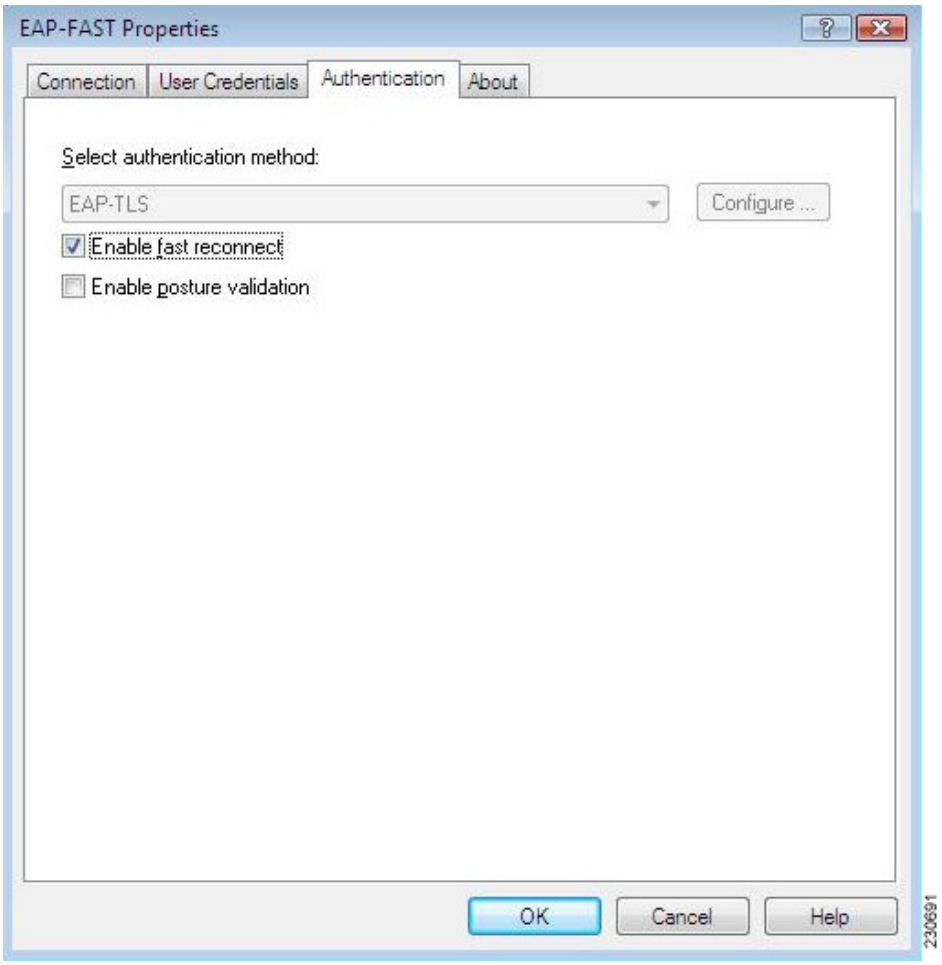



Table 3-3 lists and describes options for authentication.

*Table 3-3 Authentication Settings*

| Authentication Settings | Description |
|---|---|
| Select an authentication method | Select the inner tunnel EAP method from the drop-down list. Available methods are EAP-GTC, EAP-MSCHAPv2, EAP-TLS, and Any Method.<br><br>The Any Method option allows the EAP-FAST module to choose any of the supported methods that the EAP server requests. The method must also be appropriate to the user credentials that are used.<br><br>**Default:** Any Method<br><br>**Note** EAP-GTC is the only option available if you selected the **Use one-time password** radio button in the User Credentials tab.<br><br>**Note** EAP-TLS is the only option available if you selected the **Use a certificate on this computer** radio button in the User Credentials tab.<br><br>**Note** The use of the Any Method value to allow all methods is unsupported by Cisco or Microsoft and is not recommended. This configuration is used "as-is"; Cisco makes no guarantee that there will not be adverse performance to the system if unsupported methods are used. Unsupported methods should never be used in a production environment.<br><br>**Note** For single sign-on to work when an EAP-FAST profile is used and the selected authentication method is EAP-GTC, you must check the **Cache user information for subsequent connections to this network** check box in the Security tab (for instruction on getting to the Security tab, see the "Accessing EAP-FAST Properties for Configuration" section on page 3-4). The credentials pop-up dialog box appears with the first authentication. |
| Configure | Click the **Configure** button to configure EAP-TLS options. This option is available only if EAP-TLS is the selected authentication method. When you click this button, the standard Windows Vista EAP-TLS Properties Screen appears.<br><br>**Default:** Disabled |

*Table 3-3 Authentication Settings (continued)*

| Authentication Settings | Description |
|---|---|
| Enable fast reconnect | Check this box to allow session resumption.<br><br>The EAP-FAST module supports fast reconnect (also called session resumption) by using the User Authorization PAC. When you enable fast reconnect, you can roam or return from suspend mode without re-entering your credentials. Fast reconnect can be used across different network access servers.<br><br>**Default:** On<br><br>**Note** If you switch profiles, logs off, or reboot, fast reconnect is not attempted. You must be reauthenticated. |
| Enable posture validation | Check this box to allow the health information of the host machine to be queried. |

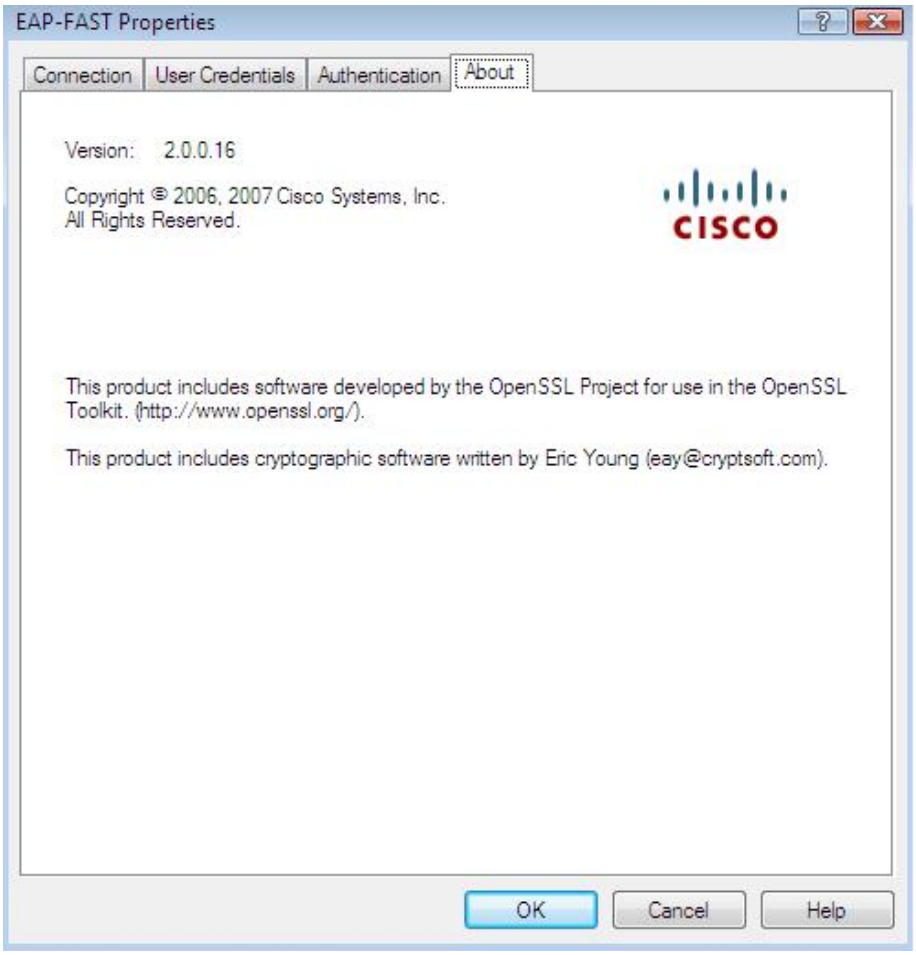
# Finding the Version of the EAP-FAST Module

Follow these steps to learn the current version of the EAP-FAST module on the device:

**Step 1** Access the EAP-FAST Properties window. The procedure for accessing this window is detailed in the "Accessing EAP-FAST Properties for Configuration" section on page 3-4.

**Step 2** Click the **About** tab (see Figure 3-7). The version number, copyright information, and open-source software information are in this tab.

*Figure 3-7 About Tab in EAP-FAST Properties Window*




# Overview of LEAP

Cisco LEAP is an authentication protocol that is designed for use in IEEE 802.11 wireless local are networks (WLANs). Important features of LEAP include the following:

- Mutual authentication between the network infrastructure and the user.
- Secure derivation of random, user-specific cryptographic session keys.
- Compatibility with existing and widespread network authentication mechanisms (for example, RADIUS).
- Computational speed.

Although Cisco LEAP is a Cisco proprietary protocol, it is based on existing IETF and IEEE standards. Cisco LEAP relies on the following:

- Extensible Authentication Protocol (EAP)

EAP was originally designed to provide an framework so that new authentication methods could be introduced into Point-to-Point Protocol (PPP). Before EAP existed, entirely new PPP authentication protocols had to be defined to create new authentication methods. However, with EAP, new authentication types simply require the definition of a new EAP type. A new EAP type comprises a set of set of EAP request and response messages and their associated semantics.

- Extensible Authentication Protocol over LAN (EAPOL)

  Although originally designed to operate as part of PPP, EAP is flexible enough to be mapped to most types of framed link layer. With a wireless access point, this link layer is a wireless LAN, not PPP. The IEEE 802.1X EAP over LAN (EAPOL) specifies a method for encapsulating EAP packets in Ethernet packets so that they can be transmitted over a LAN.

- Encryption and Key Exchange

  The 802.11 specification allows for data traffic between the client and access point to be encrypted using an encryption key. As a result of key exchange through WPA, WPA2, CCKM, or WEP, the client and the network access device derive the same pair of keys—one key for broadcast and multicast traffic from the network access device and another key for all other packets.

- Remote Authentication Dial-In User Service (RADIUS) Servers

  Network access servers (such as WLAN access points) often rely on a centralized AAA server to authenticate clients on their behalf. One of the more popular types of AAA servers is a RADIUS server. Extensions to the RADIUS protocol have been defined to allow the transfer of the EAP packets between the authentication server and the network access server. In this case, the network access server is a relay agent; the authentication conversation takes place between the client and the RADIUS server. The RADIUS server informs the access point of the result of the authentication and whether to allow the client to access the network. Other parameters might be returned as well, including session keys for use between the client and the access point.

# How LEAP Works

Because most RADIUS servers support the MS Challenge Handshake Authentication Protocol (MS-CHAP), MS-CHAP is the basis for LEAP. The protocol consists of the authenticator sending a random challenge to client. The client's data encryption standard (DES) encrypts the challenge by using an MD4 hash of the password. The authenticator then verifies the response by using its knowledge of the client username and password.

During authentication, the access point acts as a transparent relay for the conversation between the client and the RADIUS server. The EAPOL header is removed from EAPOL packets that come from the client. The contents of the EAPOL packet are added as an EAP attribute to a RADIUS request packet and sent to the RADIUS server. RADIUS packets from the server have the EAP attribute contents added to an EAPOL packet and sent to the client. The access point never examines the contents of the EAP data.

When the client associates to an access point, the access point sends an EAP identity request to the client. The client responds with a username. The RADIUS server then formats a LEAP challenge EAP attribute. The client sends a LEAP challenge response back to the RADIUS server.

If the user is invalid, the RADIUS server sends a RADIUS access-deny message that contains an EAP failure attribute. If the user is valid, the server sends a RADIUS access-challenge packet with an EAP success attribute. The client responds with a LEAP challenge. The server responds with a RADIUS access-accept packet that contains an EAP attribute with the LEAP challenge response. This packet also contains a Cisco vendor-specific attribute that informs the access point of the value of the encryption key. The client verifies the challenge response. If the response is invalid, client disassociates and attempts to find another access point.

802.11 supports the use of up to four encryption keys for the traffic between a client and its access point. The access point uses one of the key indices for the session key. This key has a different value for each connection between the client and the access point.

The session key is derived from the user password and the contents of the LEAP challenges and responses that go to and from the client. 802.11 encryption might be based on a 40-bit key or a 128-bit key. The key derivation routines provide a key that is longer than needed.

# Configuring LEAP

This section explains how to configure LEAP module settings. The following topics are covered in this section:



## Accessing LEAP Properties for Configuration

To access the LEAP Properties window, perform the following steps:

**Step 1** Click the **Start** button on the lower-left corner of the desktop.

**Step 2** From the right pane, right-click **Network**.

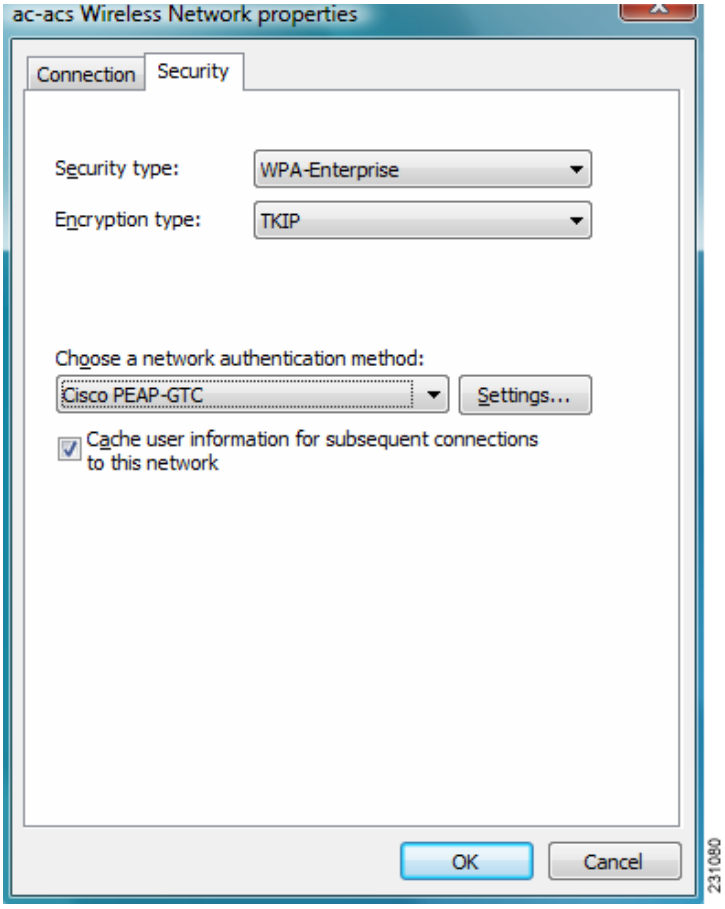
**Step 3** Select **Properties**.

**Step 4** From the left pane, select **Manage Wireless Networks**.

**Step 5** Double-click the wireless network.

**Step 6** From the **Wireless Network properties** window, select the **Security** tab (see Figure 3-1).

*Figure 3-8 Wireless Network Properties Window*




**Step 7** Select **LEAP** from the "Choose a network authentication method" drop down list.

**Step 8** Click the **Settings** button. You are now ready to configure settings for LEAP.

# Configuring LEAP Settings in the Network Credentials Tab

The user provides one of the following types of network credentials:

- Windows username and password—The Windows username and password are used as network access credentials. The user is not prompted to enter a username and password if this option is selected.
- Prompted user credentials—The user is prompted during authentication for credentials. These credentials are credentials that are separate from the Windows username and password, such as Lightweight Directory Access Protocol (LDAP) credentials.

- Saved user credentials—These are user credentials that are entered as part of the LEAP configuration. The user is not prompted for credentials during authentication unless the saved credentials fail or have expired. New credentials that the user enters after successful authentication are saved automatically in the configuration. The user does not have to return to the configuration screen to change the old saved credentials.

You can configure LEAP network credentials settings from the Network Credentials tab (see Figure 3-9).

*Figure 3-9 Network Credentials Tab in LEAP Properties Window*

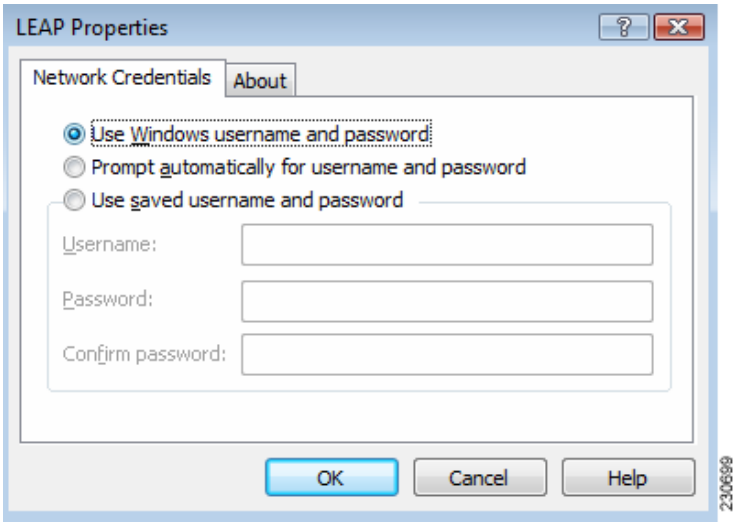



Table 3-4 lists and describes LEAP network credentials settings.

*Table 3-4 LEAP Network Credentials Settings*

| LEAP Network Credentials Settings | Description |
|---|---|
| Use Windows username and password | Click this radio button to use the Windows username and password as the LEAP username and password for network authentication.<br>**Default:** On |

*Table 3-4 LEAP Network Credentials Settings (continued)*

| LEAP Network Credentials Settings | Description |
|---|---|
| Prompt automatically for username and password | Click this radio button to require the user to enter a separate LEAP username and password, which are registered with the backend server, in addition to a Windows username and password with every authentication attempt.<br>**Default:** Off |
| Use saved username and password | Click this radio button so that the user is not required to enter a LEAP username and password with each Windows login. Authentication occurs automatically as needed using a saved username and password, which are registered with the backend server.<br>**Default:** Off<br>When selecting this option, the user must do the following:<br>• Enter a username in the **Username** field.<br>• Enter a password in the **Password** field.<br>• Confirm password—Enter the password again to verify that it was entered correctly.<br>**Note** The maximum number of characters allowed for the username and password is 256. |

The following three scenarios for credentials entry are supported by the LEAP module:

- Boot time—During this state, no users are logged on. The LEAP module uses machine credentials for network authentication. The LEAP module does not prompt the user for information but instead obtains the machine credentials by using Microsoft's Local Security Authority (LSA) API.
- Pre-Logon—During this state, Microsoft's Layer 2 credential provider (L2NA) queries the LEAP module through Microsoft's EAPHost APIs for types of credentials that are needed. The LEAP module indicates the appropriate type: Windows, network, or none. The user enters the appropriate credentials in a Microsoft L2NA prompt.
- Post-Logon—Although the user has already logged on, the LEAP module might need to prompt the user for network credentials because a card was inserted or because network authentication failed. The LEAP module invokes the EapInvokeInteractiveUI API, which is a Microsoft EAPHost API. A LEAP credentials prompt appears, and the user must enter a username and password.

## Finding the Version of the LEAP Module

The LEAP module version number, copyright information, and open-source software information are in About tab (see Figure 3-9).

# Overview of PEAP-GTC

Extensible Authentication Protocol (EAP) provides support for multiple authentication methods. While EAP was originally created for use with PPP, it has since been adopted for use with IEEE 802.1X, which is Network Port Authentication. Since its deployment, a number of weaknesses in EAP have become

apparent. These weaknesses include a lack of protection of user identity, notification messages, or the EAP negotiation; no standardized mechanism for key exchange; no built-in support for fragmentation and reassembly; no support for acknowledged success or failure indicators; and a lack of support for fast reconnect.

Protected Extensible Authentication Protocol (PEAP) addresses these weaknesses by wrapping the EAP protocol within a Transport Layer Security (TLS) channel. Any EAP method running within PEAP is provided with the following:

- Identity protection—The identity exchange is encrypted, and client certificates are provided after negotiation of the TLS channel.
- Header protection—Because the EAP method conversation is conducted within a TLS channel, the EAP header is protected against modification.
- Protected negotiation—Within PEAP, the EAP conversation is authenticated; integrity and replay are protected on a per-packet basis; and the EAP method negotiation that occurs within PEAP is protected, as are error messages sent within the TLS channel.
- Support for key exchange—To provide keying material for a wide range of link-layer ciphersuites, EAP methods should provide a key hierarchy that generates authentication and encryption keys, as well as initialization vectors. By relying on the TLS key derivation method, PEAP provides the required keying material for any EAP method running within it.
- Packet fragmentation and reassembly—Because EAP does not include support for fragmentation and reassembly, individual EAP methods need to include this capability. By including support for fragmentation and reassembly within PEAP, methods leveraging PEAP do not need to support fragmentation and reassembly on their own.
- Acknowledged success or failure indications—By sending success or failure indications within the TLS channel, PEAP provides support for protected termination of the EAP conversation. Acknowledged indications prevent an attacker from carrying out denial-of-service (DOS) attacks by spoofing EAP failure messages or by tricking the EAP peer into accepting a rogue NAS by spoofing an EAP success message.
- Fast reconnect—Where EAP is used for authentication in wireless networks, the EAP method should be able to quickly reauthenticate when the client is roaming between access points. PEAP supports fast reconnect by leveraging the TLS session resumption facility. Any EAP method running within PEAP can use fast reconnect.
- Dictionary attack resistance—By conducting the EAP conversation within a TLS channel, PEAP protects an EAP method that might be subject to offline dictionary attacks if the EAP conversation had been conducted in the clear.

# How PEAP-GTC Works

PEAP-GTC works in two phases.

In phase 1, an authentication server performs TLS authentication to create an encrypted tunnel and to achieve server-side authentication in a manner that is similar to Web server authentication that uses Secure Sockets Layer (SSL). When phase 1 of PEAP is successfully completed, all data is encrypted, including all sensitive user information.

Phase 2 is extensible. The client can authenticate by using the GTC method within the TLS tunnel.

# Configuring PEAP-GTC

This section explains how to configure PEAP-GTC module settings. The following topics are covered:



## Accessing PEAP-GTC Properties for Configuration

To access the PEAP-GTC Properties window, perform the following steps:

**Step 1** Click the **Start** button on the lower-left corner of the desktop.

**Step 2** From the right pane, right-click **Network**.

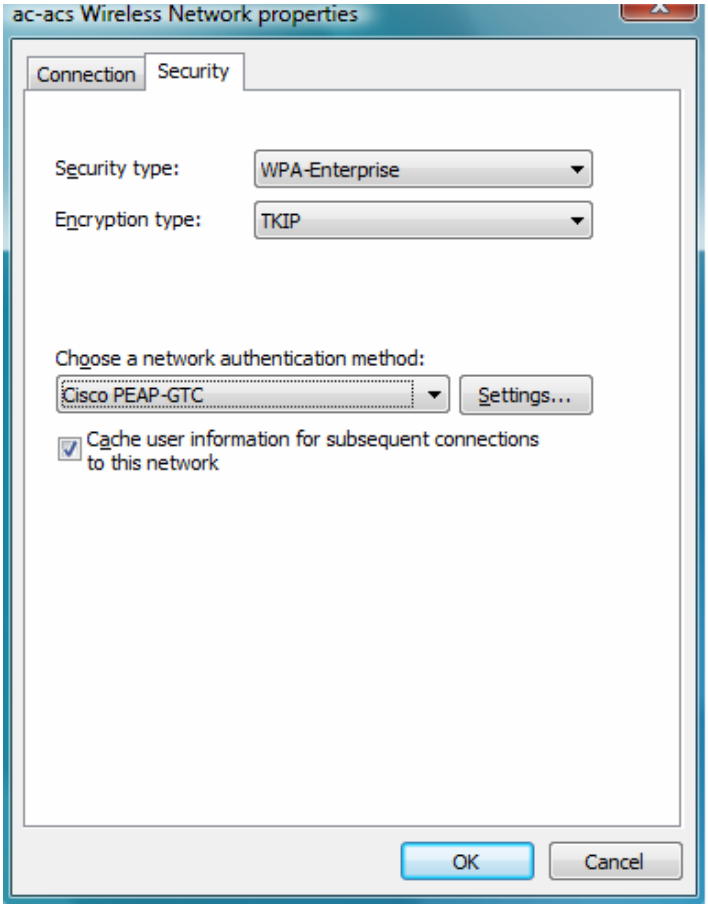
**Step 3** Select **Properties**.

**Step 4** From the left pane, select **Manage Wireless Networks**.

**Step 5** Double-click the wireless network.

**Step 6** From the **Wireless Network properties** window, select the **Security** tab (see Figure 3-10).

*Figure 3-10 Wireless Network Properties Window*




**Step 7** Select **PEAP-GTC or LEAP** from the "Choose a network authentication method" drop down list.

**Step 8** Click the **Settings** button. You are now ready to configure settings for PEAP-GTC.

# Configuring PEAP-GTC Settings in the Connection Tab

You can configure connection settings from the PEAP-GTC Connection tab (see Figure 3-11).

***Figure 3-11 Connection Tab in PEAP-GTC Properties Window***

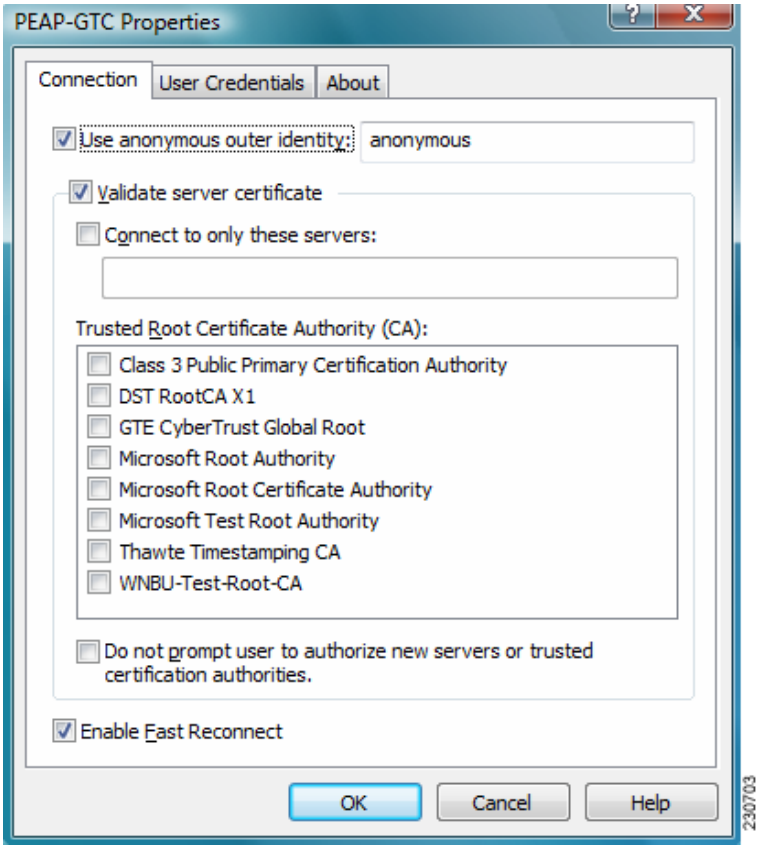


Table 3-5 lists and describes PEAP-GTC connection settings.

*Table 3-5 PEAP-GTC Connection Settings*

| PEAP-GTC Connection Settings | Description |
|---|---|
| Use anonymous outer identity | Check this box to enable identity privacy protection. If this box is checked, the Outer identity field is enabled, and the outer identity in this field is used in response to an EAP identity request, which is sent in the clear.<br><br>**Default:** On |
| Outer identity field | Enter an outer identity if the Use anonymous outer identity check box is checked. Follow an administrator's instructions, or follow RFC 4282 for guidelines about what to enter in the outer identity field.<br><br>**Default:** anonymous<br><br>**Note** The maximum numberl of characters allowed in this field is 256. |
| Validate server certificate | Check this box to validate the server certificate that is used to establish a tunnel.<br><br>If the **Validate server certificate** box is checked and the **Do not prompt user to authorize new servers or trusted certificate authorities** box is checked, you must select one or more Trusted Root CA certificates from the list of trusted Certificate Authority certificates that are installed on the host system.<br><br>If the **Validate server certificate** box is checked but the **Do not prompt user to authorize new servers or trusted certificate authorities** box is not checked, the list can be empty, and the user is prompted to validate the certificate. If authentication succeeds, then the Root CA that signed the server certificate is marked as trusted in the profile. The name of the server is then added to the **Connect to only these servers** field.<br><br>**Default:** On |
| Connect to only these servers | Check this box to enter an optional server name that must match the server certificate that is presented by the server. You can enter multiple server names; separate multiple server names with semicolons. The PEAP-GTC module only allows connections to continue without prompting if the subject field (CN) or the subject alternative name in the server certificate matches the server names that you enter in this field.<br><br>**Default:** Off<br><br>**Note** You can use an asterisk (*) as a wildcard character in server names only if the asterisk appears before the first period (.) in the name.domain.com format. For example, "*.cisco.com" matches any server name that ends with ".cisco.com." If you put an asterisk anywhere else in the server name, it is not treated as a wildcard character. |

*Table 3-5 PEAP-GTC Connection Settings (continued)*

| PEAP-GTC Connection Settings | Description |
|---|---|
| Trusted Root Certificate Authority (CA) | Select one of more Trusted Root CA certificates from the list of certificates that are installed on the system. Only trusted CA certificates that are installed on the host system are displayed in the drop-down list, so you must make sure that the desired trusted root CA certificate is installed.<br>To view details about the selected Trusted Root CA certificate, double-click the certificate name. Double-clicking the certificate name opens the Windows certificate property screen, where certificate details are available.<br>**Default:** None |
| Do not prompt user to authorize new servers or trusted certificate authorities. | Check this box if you do not want the user to be prompted to authorize a connection when the server name does not match or the server certificate is not signed by one of the Trusted Root CA certiticates that was selected. If this box is checked and the server certificate is not trusted, the authentication fails.<br>**Default:** Off |
| Enable fast reconnect | Check this box to allow session resumption.<br>The PEAP-GTC module supports fast reconnect (also called session resumption). When you enable fast reconnect, you can roam without re-entering your credentials. Fast reconnect can be used across different network access servers.<br>**Default:** On<br>**Note** If you switch profiles, log off, or reboot, fast reconnect is not attempted. You must be reauthenticated. |

# Configuring PEAP-GTC Settings in the User Credentials Tab

The PEAP-GTC module supports OTP and a username and password as user credentials for authentication.

The user provides one of the following types of username and password:

- One-time password (OTP)—The user must manually enter a OTP. New PIN mode and next token mode for OTP are supported.
- Windows username and password—The Windows username and password are used as network access credentials. The user is always prompted to enter a password unless PEAP-GTC is configured to use single sign-on (SSO) or the password is cached.
- Prompted user credentials—The user is prompted during authentication for credentials. These credentials are credentials that are separate from the Windows username and password, such as Lightweight Directory Access Protocol (LDAP) credentials.
- Saved user credentials—These are user credentials that are entered as part of the PEAP-GTC configuration. The user is not prompted for credentials during authentication unless the saved credentials fail or have expired. New credentials that the user enters after successful authentication are saved automatically in the configuration. The user does not have to return to the configuration screen to change the old saved credentials.

The user can configure PEAP-GTC user credentials from the User Credentials tab (see Figure 3-12).

*Figure 3-12 User Credentials Tab in PEAP-GTC Properties Window*

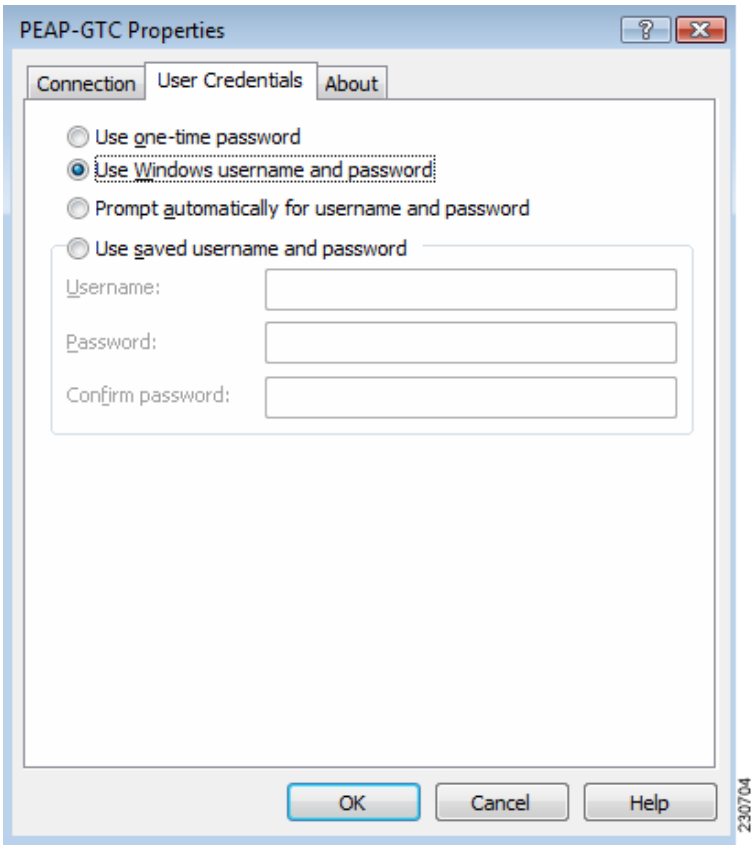



Table 3-2 lists and describes options for PEAP-GTC user credentials.

*Table 3-6 PEAP-GTC User Credentials Options*

| User Credentials | Description |
|---|---|
| Use one-time password | Click this radio button to use a one-time password (OTP). In this mode, credentials are never cached. Each time the server asks for credentials, the user is prompted to supply credentials.<br><br>For more information about OTP, see the "Understanding PIN Mode and Token Mode with OTP" section on page 3-12.<br><br>**Default:** Off |
| Use Windows username and password | Click this radio button to use the Windows username and password as the PEAP-GTC username and password for network authentication. This mode only affects single sign-on authentication when the login screen has one set of credentials instead of two sets of credentials, which is the case for the **Prompt automatically for username and password** option.<br><br>**Default:** On |

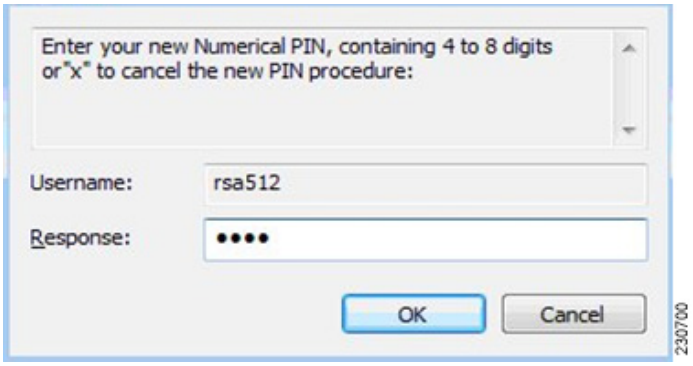
*Table 3-6 PEAP-GTC User Credentials Options (continued)*

| User Credentials | Description |
|---|---|
| Prompt automatically for username and password | Click this radio button to require the user to enter a separate PEAP-GTC username and password, which are registered with a RADIUS server, in addition to a Windows username and password with every authentication attempt. This option supports non-Windows passwords, such as LDAP.<br>**Default:** Off |
| Use saved username and password | Click this radio button so that the user is not required to enter a PEAP-GTC username and password with each Windows login. Authentication occurs automatically as needed using a saved username and password, which are registered with the backend server.<br>**Default:** Off<br>When selecting this option, the user must enter the following:<br>• Username—Enter the username and the domain name in one of these two formats:<br>– Domain-qualified username—domain\user<br>– UPN—user@domain.com<br>• Password—Enter a password. This encrypted password is stored in the PEAP-GTC configuration.<br>• Confirm password—Enter the password again to verify that it was entered correctly.<br>**Note** The maximum number of characters allowed for the username and password is 256. |

# Understanding PIN Mode and Token Mode with OTP

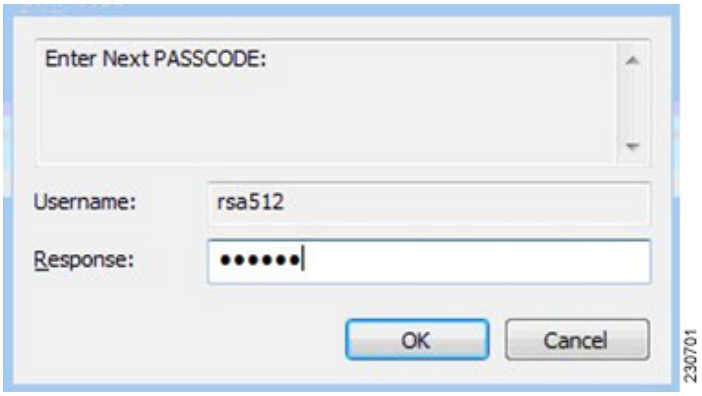
New PIN mode for OTP is supported. If a new PIN is needed, the backend server sends a text message (for example, “Enter New PIN”) to indicate that a new PIN is neeeded. The PEAP-GTC module displays a prompt window that includes the text message from the server (see Figure 3-13). The backend server might prompt the user twice to confirm the new PIN that the user entered.

*Figure 3-13 New PIN Prompt Window*



Next Token mode for OTP is also supported. If the next token is needed, the backend server sends a text message (for example, “Enter Next PASSCODE:”) to indicate that the next token is needed. The PEAP-GTC module displays a prompt window that includes the text message sent from the server (see Figure 3-14). The user must get the next token from the OTP device or from the software and enter it in the prompt field.

***Figure 3-14 Next Token Prompt Window***




# Understanding PEAP-GTC Authentication

The PEAP-GTC module prompts the user for a username and password (or PIN for OTP) if the supplicant is configured to prompt for credentials during Windows logon or after the user is notified of an authentication error or failure.

If the user password expires, the PEAP-GTC modules prompts the user to enter a new password and to confirm the new password.

# Finding the Version of the PEAP-GTC Module

The PEAP-GTC module version number, copyright information, and open-source software information are in About tab (see Figure 3-12).