EAP-FAST for Windows Vista Administrator Guide

June 2008

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-16949-01

CONTENTS

Preface

This preface provides an overview of the *EAP-FAST for Windows Vista Administrator Guide* and explains how to obtain other documentation and technical assistance.

The following topics are covered in this section:

Audience

This publication is for the administrator responsible for installing and configuring the EAP-FAST module for Windows Vista. The administrator should be familiar with computing devices and with network structures, terms, and concepts. The adminstrator should be familiar with the Windows Vista operating system. The administrator should be familiar with configuring and deploying Microsoft Group Policy Objects (GPOs) and using the Microsoft Group Policy Object Editor. The administrator should be familiar with working with XML schemas.

Purpose

This publication describes configuration settings for and administrative tasks related to the EAP-FAST module on computers running the Windows Vista operating system.

Note Windows Vista is the only supported operating system for the EAP-FAST module that is discussed in this publication.

Organization

This guide contains the following sections:

Chapter 1, "Overview of EAP-FAST," provides an overview of the EAP-FAST (Flexible Authentication via Secure Tunneling).

Chapter 2, "Installing the EAP-FAST Module," explains how to install the EAP-FAST module.

Chapter 3, "Configuring EAP-FAST," explains how configure EAP-FAST module settings in the user interface.

Chapter 4, "Creating and Modifying EAP-FAST Profiles for Distribution to Users," explains how to configure EAP-FAST module profiles both by using a Group Policy Object editor and by modifying XML schemas. It also discusses machine authentication single sign-on support for EAP-FAST.

Chapter 5, "Configuring Logging," describes how configure logging on the EAP-FAST module to assist with troubleshooting.

Chapter 6, "Troubleshooting," describes EAP-FAST error and prompt messages. It also provides guidelines for creating strong passwords.

Appendix A, "Abbreviations" includes expansions for all abbreviations that are used in this guide.

Conventions

This publication uses the following conventions to convey instructions and information:

- Commands are in **boldface** type.
- Variables are in *italic* type.
- Notes and cautions use the following conventions and symbols:

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

CHAPTER 1

Overview of EAP-FAST

This chapter provides an overview of EAP-FAST (Flexible Authentication via Secure Tunneling). This chapter includes the following sections:

Introduction to 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 1-2). 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.

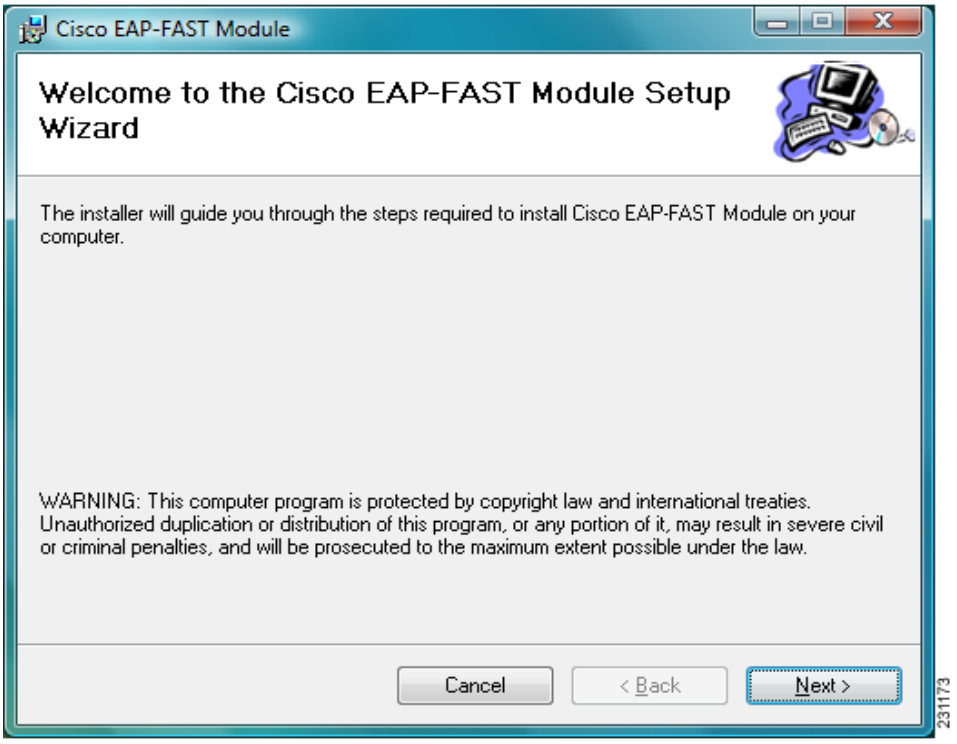
CHAPTER 2

Installing the EAP-FAST Module

To install the EAP-FAST module, perform the following steps:

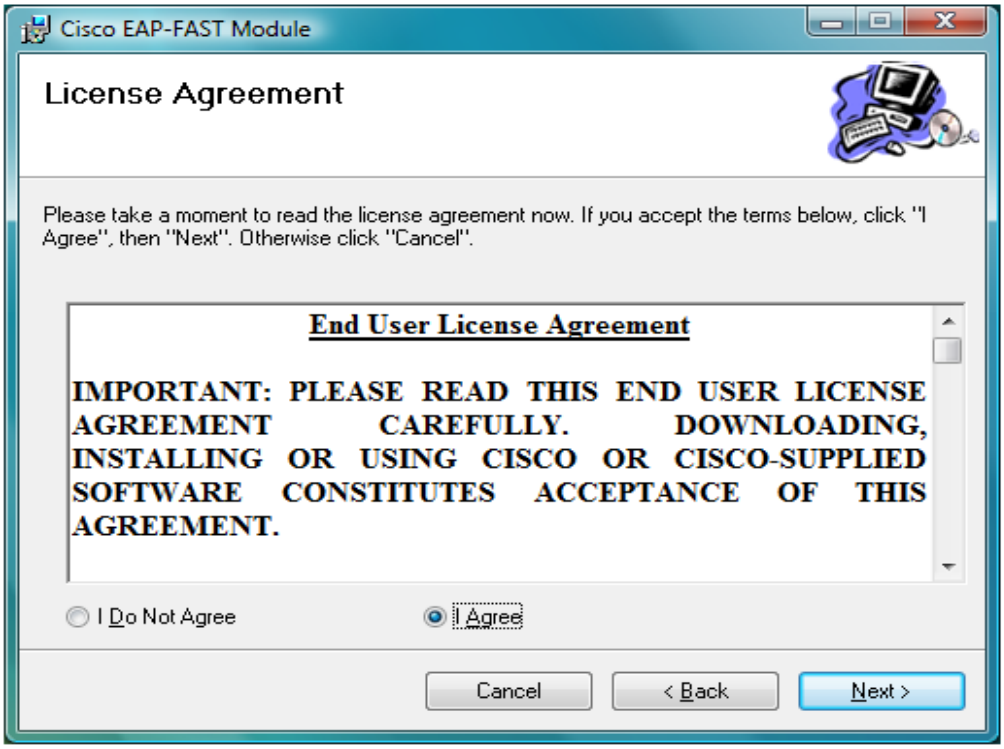
Step 1 Double-click the EAP-FAST Module Setup Wizard icon. The Welcome window appears (see Figure 2-1).

Figure 2-1 Welcome Window



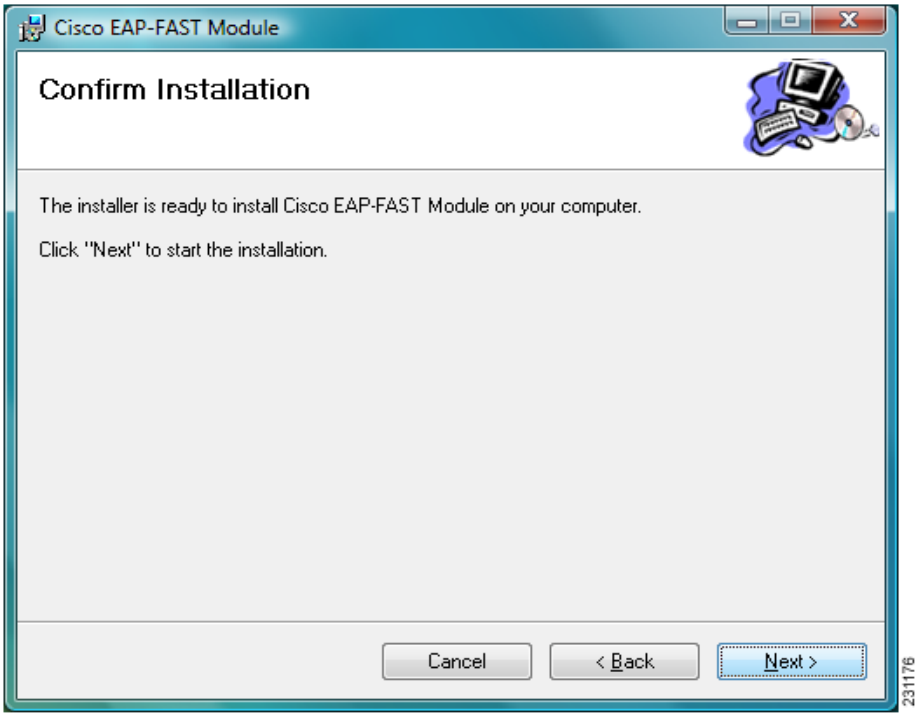
Step 2 In the Welcome window, click **Next**. The License Agreement window appears (see Figure 2-2).

Figure 2-2 License Agreement Window



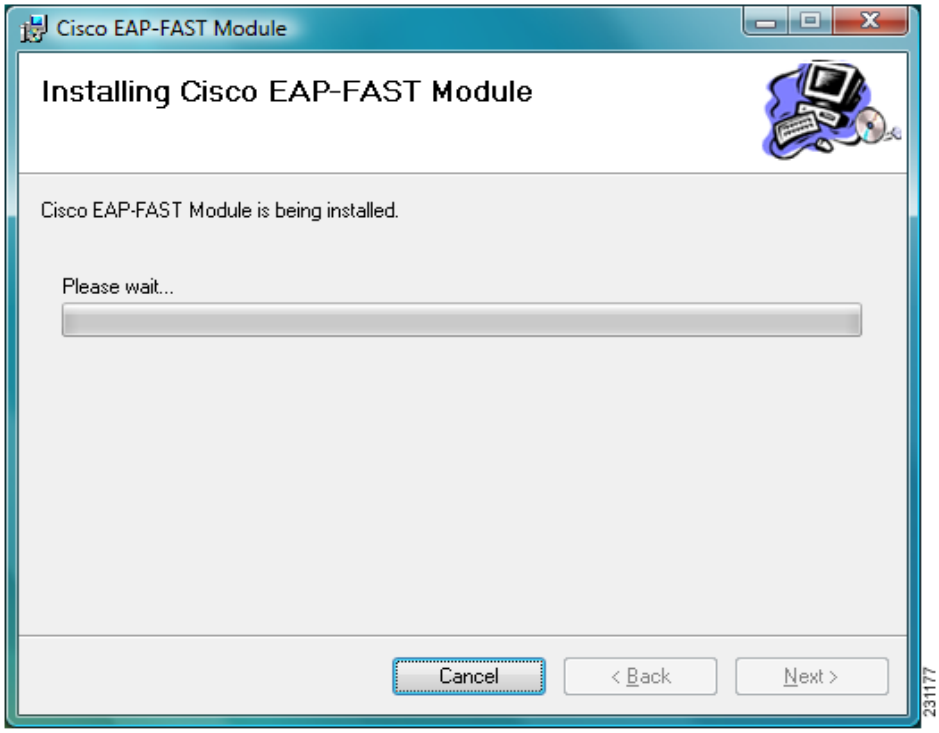
Step 3 In the License Agreement window, click the **I Agree** radio button to accept the license agreement. Then click **Next**. The Confirm Installation window appears (see Figure 2-3).

Figure 2-3 Confirm Installation Window



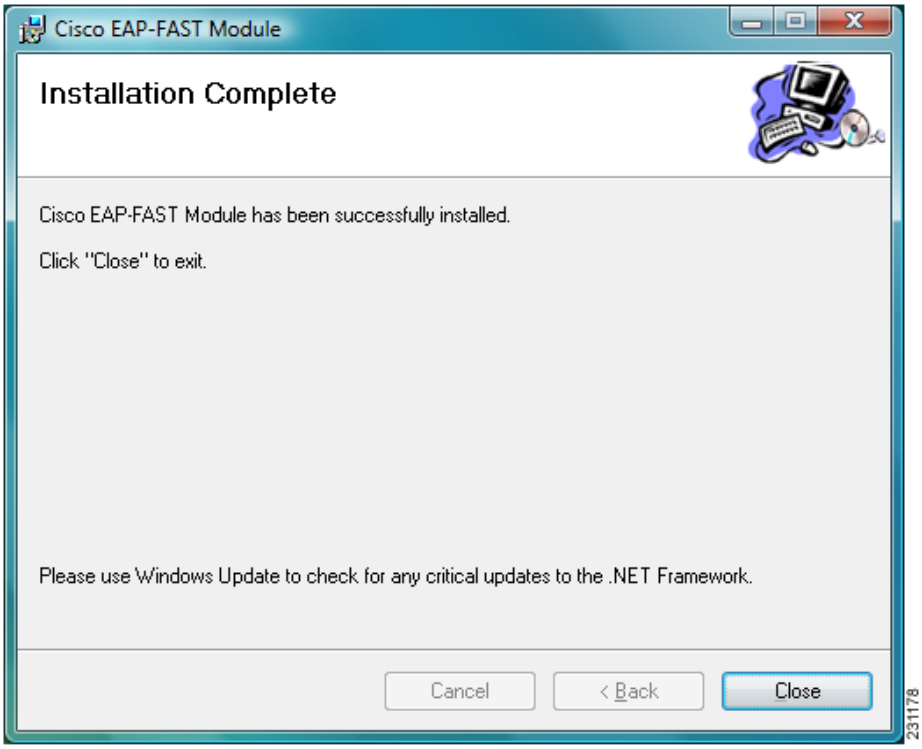
Step 4 In the Confirm Installation window, click **Next** to start the installation. The Installing Cisco EAP-FAST Module window appears and tracks the progress of the installation (see Figure 2-4).

Figure 2-4 Installing Cisco EAP-FAST Module Window



Step 5 After the EAP-FAST module has been installed successfully, the Installation Complete window appears (see Figure 2-5).

Figure 2-5 Installation Complete Window



Step 6 Click the **Close** button.

The EAP-FAST module is installed in the following directory destination:

%Program Files\Cisco\Cisco EAP-FAST Module.

CHAPTER 3

Configuring EAP-FAST

This chapter explains how to configure EAP-FAST module settings, such as connection settings, user credentials, and authentication methods.

The following topics are covered in this chapter:

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**.

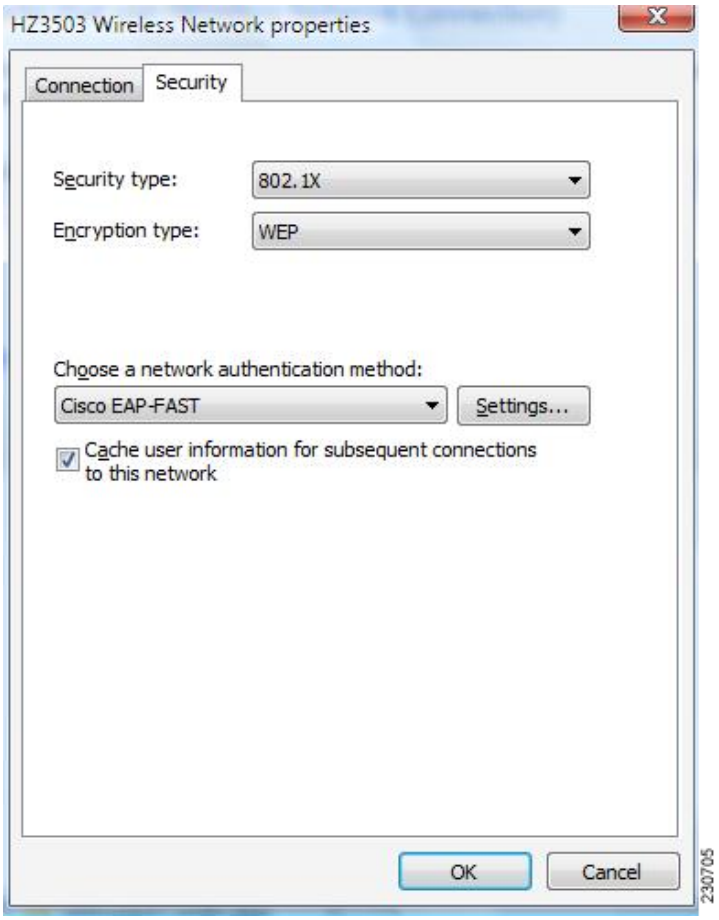
Step 3 Select **Properties**.

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 Settings in the Connection Tab" section on page 3-4, the "Configuring User Credentials" section on page 3-8, and the "Configuring Authentication Methods" section on page 3-12. 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 3-13.

Overview of 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.

Configuring Settings in the Connection Tab

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

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

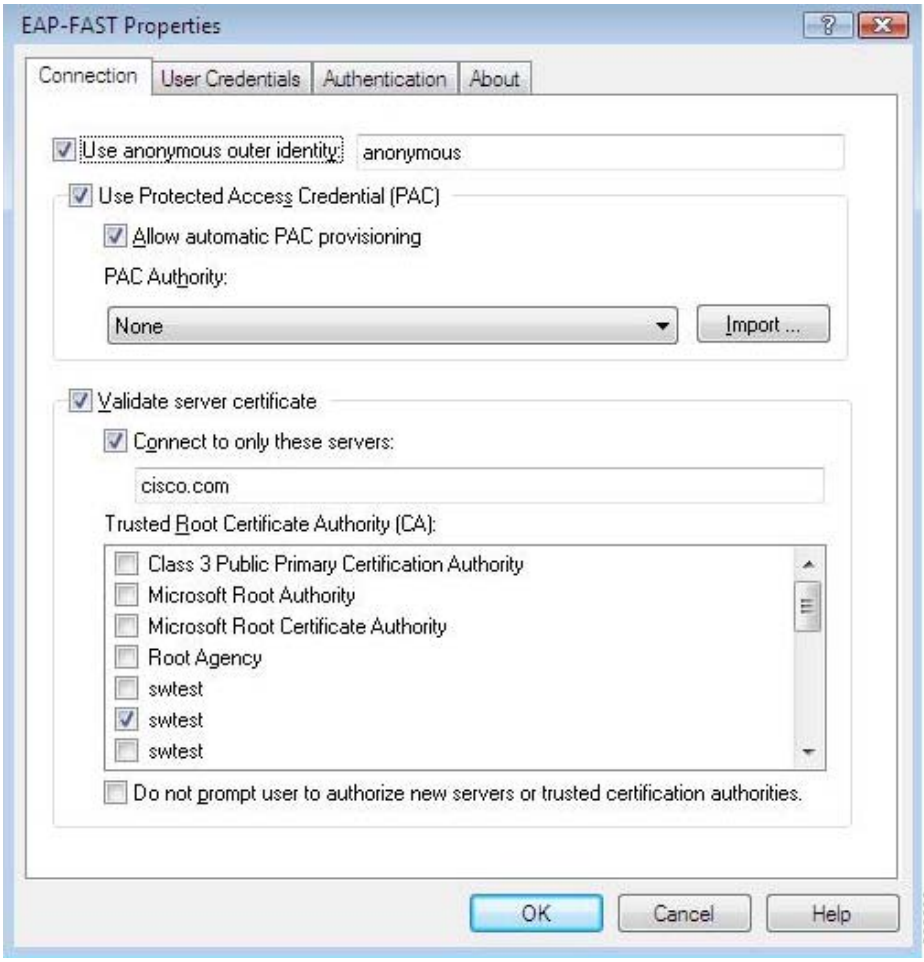


Table 3-2 lists and describes all connection settings.

Table 3-1 Connection Settings

Connection Settings	Description
Use anonymous outer identity	Check this box to enable identity privacy protection. **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. **Default:** anonymous **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. 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. 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. **Default:** On
Allow automatic PAC provisioning	Check this box to enable the automatic retrieval of a PAC during EAP-FAST authentication. 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. **Default:** On
PAC Authority	Select a PAC authority from the drop-down list. **Default:** None **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. After you have selected and imported a valid PAC file, the PAC authority is added to the PAC authority drop-down list. **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. 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. 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. **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. **Default:** Off **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. 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. **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. **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 User Credentials

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

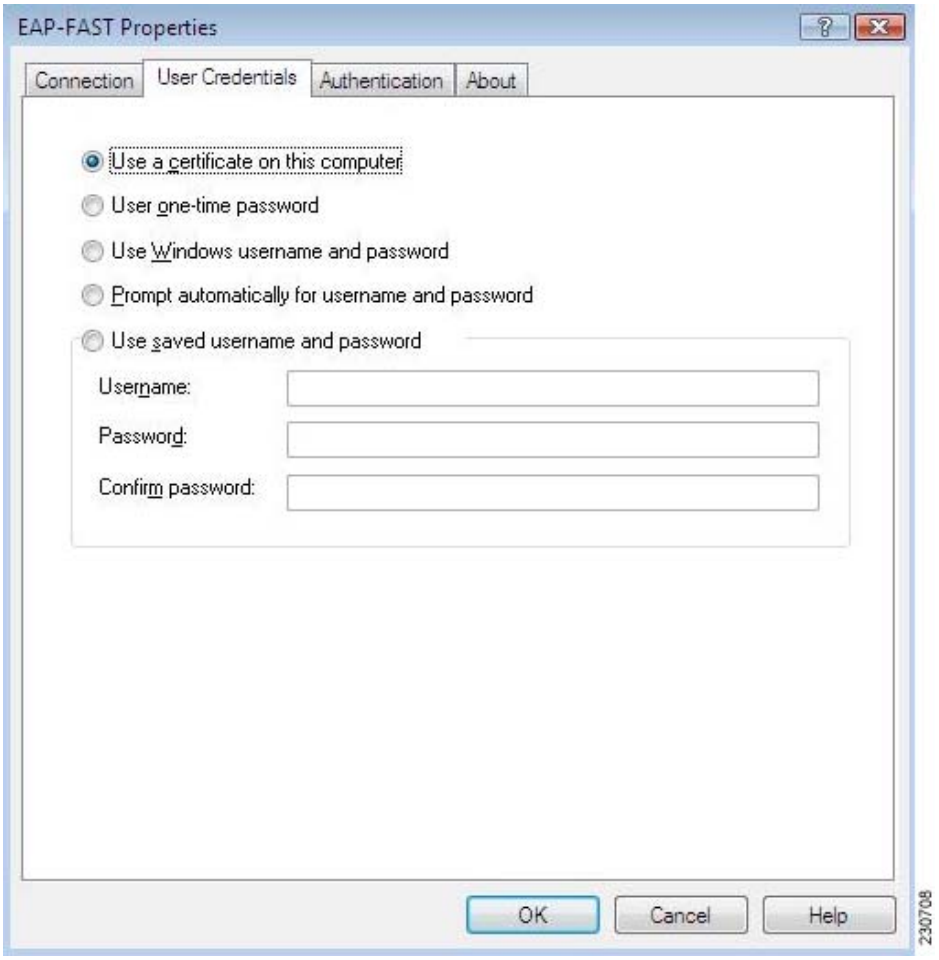


Table 3-2 lists and describes all options for user credentials.

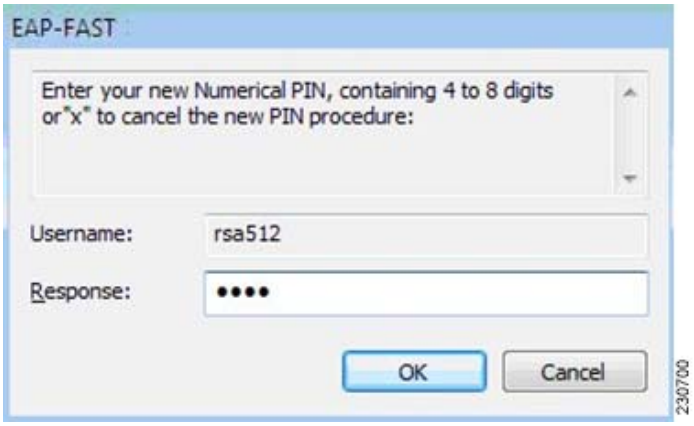
Table 3-2 User Credentials Options

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. **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 3-10. **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. **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. **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. **Default:** Off When selecting this option, the user must enter the following: • Username—Enter the username and the domain name in one of these two formats: – Domain-qualified user name—domain\user – User Principal Name (UPN)—user@domain.com • Password—Enter a password. This encrypted password is stored in the EAP-FAST configuration. • Confirm password—Enter the password again to verify that it was entered correctly. **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

Overview of 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.

Configuring Authentication Methods

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

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

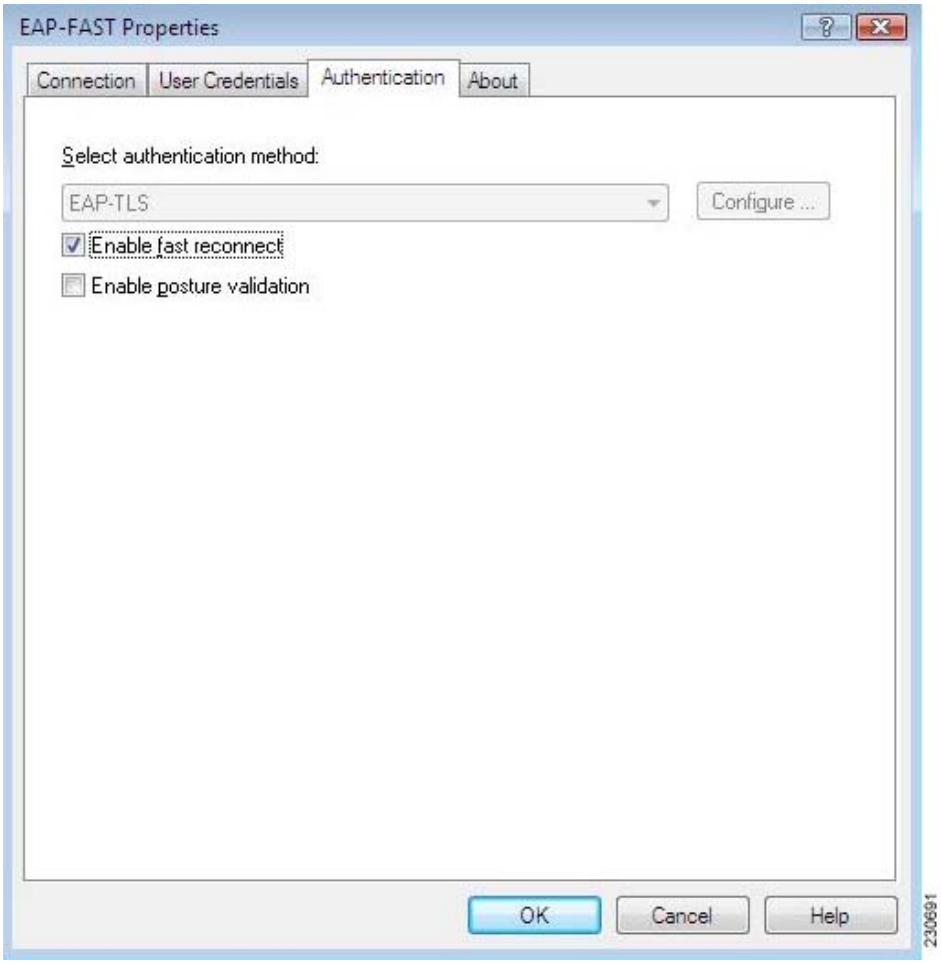


Table 3-3 lists and describes options for authentication.

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. 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. **Default:** Any Method **Note** EAP-GTC is the only option available if you selected the **Use one-time password** radio button in the User Credentials tab. **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. **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.
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. **Default:** Disabled
Enable fast reconnect	Check this box to allow session resumption. 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. **Default:** On **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.

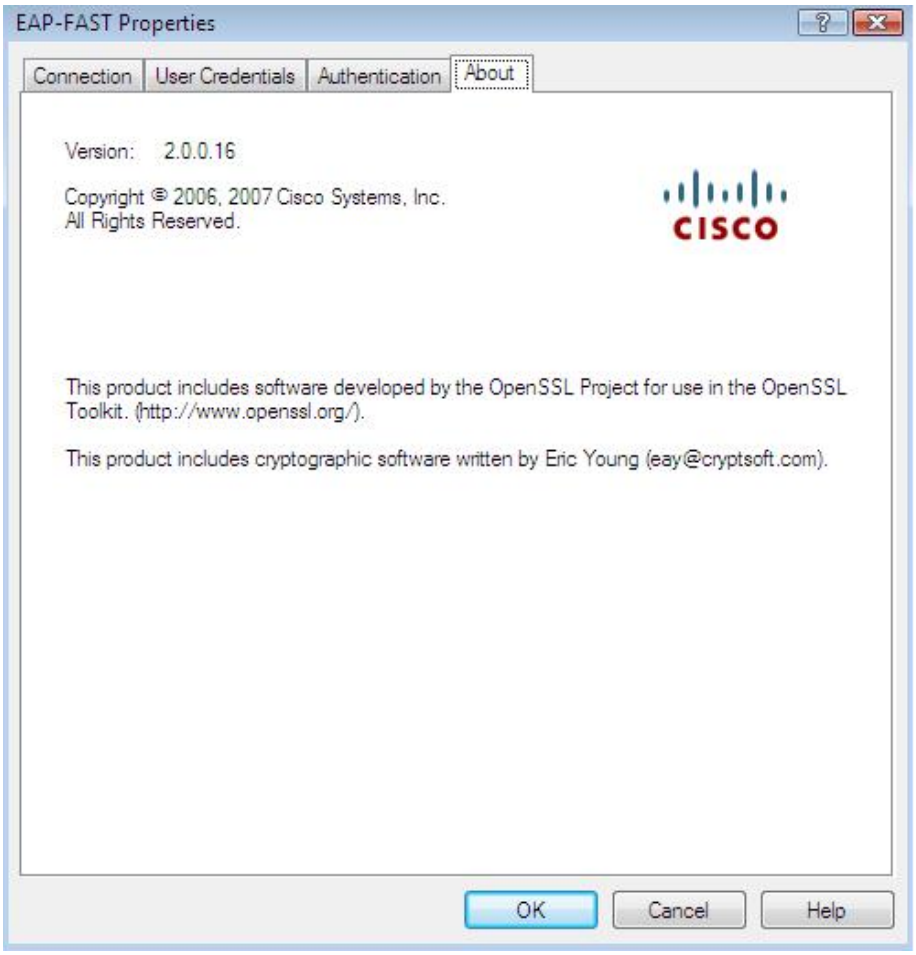
Finding the Version of the EAP-FAST Module

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 3-2.

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



CHAPTER 4

Creating and Modifying EAP-FAST Profiles for Distribution to Users

This chapter explains how configure EAP-FAST module profiles both by using a Group Policy Object editor and by modifying the EAP-FAST XML schema.

The following topics are covered in this chapter:

Overview of Group Policy Objects

Group Policy is an infrastructure that allows you to specify managed configurations for users and computers in an Active Directory directory service environment. Group Policy settings are contained in Group Policy objects (GPOs). GPOs exist in a domain and can be linked to the following Active Directory containers: sites, domains, or organizational units (OUs).

Microsoft provides a program snap-in that allows you to use the Group Policy Object editor in the Microsoft Management Console (MMC).

For more information about the MMC, refer to the Microsoft Management Console Help at this URL:

http://www.microsoft.com/technet/WindowsVista/library/ops/06e1cb7b-19c9-4c49-9db8-a941f6f593c3.mspx

Adding a Group Policy Object Editor

Before you configure a Group Policy Object, you must add a Group Policy Object Editor snap-in. To add the snap-in, perfom the following steps:

Step 1 Open the MMC:

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

b. Enter **mmc** in the **Search box** and press **Enter**.

Note To open an existing or saved MMC console, browse to the snap-in console or a shortcut to the snap-in console in Windows Explorer, and then double-click it.

You can also open an existing MMC console from another console in which you are working. To do this, click the **File** menu, and then click **Open**.

Step 2 Add the Group Policy Object Editor snap-in:

a. Go to **File > Add/Remove Snap-in...**

The **Add or Remove Snap-ins** dialog box is displayed.

b. From the **Add or Remove Snap-ins** dialog box, highlight **Group Policy Object Editor** in the **Available snap-ins** list, and click the **Add** button**.**

The **Select Group Policy Object** dialog box is displayed.

c. From the **Select Group Policy Object** dialog box, click **Browse**.

The **Browse for a Group Policy Object** dialog box is displayed.

d. From the **Browse for a Group Policy Object** dialog box, select the **Domains/O Us** tab.

e. Select your domain controller from the **Look in** drop down list.

f. Click **OK**.

g. From the **Select Group Policy Object** dialog box, click **Finish**.

h. From the **Add or Remove Snap-ins** dialog box, click **OK**.

Now the Group Policy Object Editor is ready for use.

Creating a Group Policy Object in Windows Vista

To create a new EAP group policy object, perform the following steps:

Step 1 In the **Default Domain Policy** pane, select **Windows Settings > Security Settings > Wireless Network Policies**.

Step 2 Right-click **Wireless Network Policies** and select **Create a New Policy**.

Step 3 Set your wireless network properties, such as SSID, encryption, and authentication method.

Step 4 Select the EAP method.

Step 5 Open the EAP-FAST properties and configure the EAP-FAST settings.

Note In the **Advanced Security** screen, you can configure supplicant settings such as machine authentication and SSO. For more information about machine authentication, see the "Configuring Machine Authentication" section on page 4-15. For more information about SSO see the "Configuring Single Sign-On" section on page 4-15.

Note You can configure settings for a wired network by selecting the **Wired Network Policy** object.

Step 6 After you are done, save the GPO. You can refresh the Vista client by running "gpupdate /force" to force update of the GPO. You should see the new profile being added to Vista machine.

After you create a GPO network profile, it cannot be changed by the user on the Vista machine.

On the General tab of a wireless network policy, you can configure a name and description for the policy, specify whether the WLAN AutoConfig service is enabled, and configure a list of wireless network policies and their settings in a preferred order. You can also export profiles as XML files and import XML files as wireless profiles.

For detailed information about configuring policies, exporting profiles, and importing profiles, see the following documentation:

- *Windows Vista Wireless Networking Evaluation Guide*

http://technet2.microsoft.com/WindowsVista/en/library/f0b0d1fd-6dff-46a2-8e6a-bdd152d2337f1033.mspx?mfr=true

- *Wireless Group Policy Settings for Windows Vista*

http://www.microsoft.com/technet/technetmag/issues/2007/04/CableGuy/default.aspx

The EAP-FAST XML Schema

The EAP-FAST module stores all settings in the Native EAP method section of the network profile as XML by using the following schema:

```
<?xml version="1.0"?>

<!--
********************************************************************************
                    Cisco EAP-FAST Schema          (1.0.40)
Copyright 2006-2007, Cisco Systems, Inc.          All rights reserved.
********************************************************************************
-->

<xs:schema
 xmlns:xs="http://www.w3.org/2001/XMLSchema"
 xmlns="http://www.cisco.com/CCX"
 targetNamespace="http://www.cisco.com/CCX"
 elementFormDefault="qualified"
 attributeFormDefault="unqualified">

 <xs:element name="eapFast" type="EapFast"/>

 <xs:complexType name="EapFast">
  <xs:complexContent>
   <xs:extension base="TunnelMethods">
    <xs:sequence>
     <xs:choice>
      <xs:element name="usePac">
       <xs:complexType>
        <xs:sequence>
         <xs:element name="allowUnauthPacProvisioning" type="xs:boolean" default="true">
          <xs:annotation>
         <xs:documentation>Will accept a PAC from an unauthenticated server.</xs:documentation>
          </xs:annotation>
         </xs:element>
         <xs:element name="autoGrouping" type="xs:boolean" default="true">
          <xs:annotation>
```

```
            <xs:documentation>
An aid-group is a set of A-IDs that are all trusted equally.  Any A-ID in the group can be utilized.
Auto-grouping means that when  an untrusted A-ID is accepted by the end-user then that A-ID is grouped
with the A-ID(s) that were already trusted for that profile, hence automatically creating and growing an
A-ID group based on user actions.  The advantage of an A-ID group is that if a profile initially starts
with the same trusted A-ID(1) and then  at some point the end-user authorizes the use of a new A-ID(2)
when using this profile it will  accept A-ID(2) without bothering the end-user a second
time.</xs:documentation>
            </xs:annotation>
          </xs:element>
          <xs:element name="userValidatesServerIdFromUnauthProv" type="xs:boolean"
default="true">
            <xs:annotation>
              <xs:documentation>
If true,  then when the client is about to do unauthenticated provisioning, the user will be prompted to
allow or disallow the unauthenticated provisioning.</xs:documentation>
            </xs:annotation>
          </xs:element>
        <xs:element name="unauthProvAllowedTilPacReceived" type="xs:boolean" default="false">
            <xs:annotation>
              <xs:documentation>if true, then unauthenticated provisioning is allowed to occur until it
succeeds and a PAC is received, then only authenticated provisioning will be
allowed.</xs:documentation>
            </xs:annotation>
          </xs:element>
          <xs:choice>
            <xs:element name="validateWithSpecificPacs" type="ValidateWithSpecificPacs">
              <xs:annotation>
                <xs:documentation>This indicates that only those PACs referenced in this element (as
well as PACs that are auto-provisioned to this profile when this profile is in use) shall be used for
validation.  </xs:documentation>
              </xs:annotation>
            </xs:element>
          </xs:choice>
        </xs:sequence>
      </xs:complexType>
    </xs:element>
    <xs:element name="doNotUsePac" type="Empty">
      <xs:annotation>
        <xs:documentation>Will not utilize PAC for authentication.</xs:documentation>
      </xs:annotation>
```

```
  </xs:element>
 </xs:choice>
 <xs:element name="enablePosture" type="xs:boolean" default="false">
  <xs:annotation>
   <xs:documentation>Allow posture information to be processed.</xs:documentation>
  </xs:annotation>
 </xs:element>
 <xs:element name="authMethods">
  <xs:complexType>
   <xs:choice>
    <xs:element name="builtinMethods">
     <xs:complexType>
      <xs:choice>
       <xs:element name="authenticateWithPassword">
        <xs:complexType>
         <xs:sequence>
         <xs:element name="protectedIdentityPattern" type="IdentityPattern" minOccurs="0">
           <xs:annotation>
             <xs:documentation>Format rules same as for unprotectedIdentityPattern.  Typical
pattern: [username]@[domain] or if password source is this profile then the pattern would be the actual
string to send as the username. </xs:documentation>
           </xs:annotation>
          </xs:element>
          <xs:element name="passwordSource" type="PasswordSource"/>
          <xs:element name="methods">
           <xs:annotation>
            <xs:documentation>At least 1 child element is required.</xs:documentation>
           </xs:annotation>
           <xs:complexType>
            <xs:all>
             <xs:element name="eapMschapv2" type="Empty" minOccurs="0"/>
             <xs:element name="eapGtc" type="Empty" minOccurs="0"/>
            </xs:all>
           </xs:complexType>
          </xs:element>
         </xs:sequence>
        </xs:complexType>
       </xs:element>
```

```
                    <xs:element name="authenticateWithToken">
                     <xs:complexType>
                      <xs:sequence>
                      <xs:element name="protectedIdentityPattern" type="IdentityPattern" minOccurs="0">
                        <xs:annotation>
                          <xs:documentation>Format rules same as for unprotectedIdentityPattern.  Typical
pattern: [username]@[domain] </xs:documentation>
                        </xs:annotation>
                       </xs:element>
                       <xs:element name="tokenSource" type="TokenSource"/>
                       <xs:element name="methods">
                        <xs:complexType>
                         <xs:all>
                          <xs:element name="eapGtc" type="Empty"/>
                         </xs:all>
                        </xs:complexType>
                       </xs:element>
                      </xs:sequence>
                     </xs:complexType>
                    </xs:element>
                    <xs:element name="authenticateWithCertificate">
                     <xs:complexType>
                      <xs:sequence>
                      <xs:element name="protectedIdentityPattern" type="IdentityPattern" minOccurs="0">
                        <xs:annotation>
                          <xs:documentation>Format rules same as for unprotectedIdentityPattern. Typical
pattern: [username]@[domain] </xs:documentation>
                        </xs:annotation>
                       </xs:element>
                       <xs:element name="certificateSource" type="CertificateSource"/>
                       <xs:choice>
                        <xs:element name="doNotUseInnerMethod">
                         <xs:complexType>
                          <xs:choice>
                           <xs:element name="sendWheneverRequested" type="Empty"/>
                           <xs:element name="sendSecurelyOnly" type="Empty"/>
                          </xs:choice>
                         </xs:complexType>
```

```
                    </xs:element>
                    <xs:element name="sendViaInnerMethod">
                     <xs:complexType>
                      <xs:all>
                       <xs:element name="eapTls" type="Empty"/>
                      </xs:all>
                     </xs:complexType>
                    </xs:element>
                   </xs:choice>
                  </xs:sequence>
                 </xs:complexType>
                </xs:element>
               </xs:choice>
              </xs:complexType>
             </xs:element>
             <xs:element name="extendedInnerMethods" type="ExtendedInnerEapMethod"
maxOccurs="unbounded"/>
            </xs:choice>
           </xs:complexType>
          </xs:element>
         </xs:sequence>
        </xs:extension>
       </xs:complexContent>
      </xs:complexType>

      <xs:complexType name="IdentityPattern">
       <xs:simpleContent>
        <xs:extension base="NonEmptyString">
         <xs:attribute name="encryptContent" type="xs:boolean" use="optional" default="true">
          <xs:annotation>
           <xs:documentation>this is defaulted to 'true' as an indication to  the post-process tool that it
should encrypt this element.</xs:documentation>
          </xs:annotation>
         </xs:attribute>
        </xs:extension>
       </xs:simpleContent>
      </xs:complexType>
```

```
<xs:complexType name="PasswordFromProfile">
 <xs:simpleContent>
  <xs:extension base="xs:string">
   <xs:attribute name="encryptContent" type="xs:boolean" use="optional" default="true">
    <xs:annotation>
     <xs:documentation>this is defaulted to 'true' as an indication to  the post-process tool that it should encrypt this element.</xs:documentation>
    </xs:annotation>
   </xs:attribute>
  </xs:extension>
 </xs:simpleContent>
</xs:complexType>

<xs:complexType name="PasswordSource">
 <xs:choice>
  <xs:element name="passwordFromLogon" type="Empty"/>
  <xs:element name="passwordFromUser" type="Empty"/>
  <xs:element name="passwordFromProfile" type="PasswordFromProfile"/>
 </xs:choice>
</xs:complexType>

<xs:complexType name="TokenSource">
 <xs:choice>
  <xs:element name="passwordFromOtherToken" type="Empty">
   <xs:annotation>
    <xs:documentation>this will result in a prompt to user to obtain identity and otp from token</xs:documentation>
   </xs:annotation>
  </xs:element>
 </xs:choice>
</xs:complexType>

<xs:complexType name="CertificateSource">
 <xs:choice>
  <xs:element name="certificateFromUser" type="Empty">
   <xs:annotation>
    <xs:documentation>
```

```
The client certificate to use during authentication is the one that the end-user selects from a list presented to them.</xs:documentation>
      </xs:annotation>
    </xs:element>
    <xs:element name="certificateFromLogon" type="Empty">
      <xs:annotation>
       <xs:documentation>The client certificate to use during authentication is the one the end-user used in order to logon to windows.</xs:documentation>
      </xs:annotation>
    </xs:element>
    <xs:element name="certificateFromProfile" type="ClientCertificate">
      <xs:annotation>
        <xs:documentation>The client user certificate to use during authentication is indicated here.</xs:documentation>
      </xs:annotation>
    </xs:element>
  </xs:choice>
 </xs:complexType>

 <xs:complexType name="ExtendedInnerEapMethod">
  <xs:sequence>
   <xs:element name="methodName" type="xs:string"/>
   <xs:element name="methodEapId" type="xs:unsignedInt"/>
   <xs:element name="vendorId" type="xs:integer" default="0"/>
   <xs:element name="AuthorName" type="xs:string"/>
   <xs:element name="AuthorId" type="xs:unsignedInt"/>
   <xs:any namespace="##any" processContents="lax" minOccurs="0"/>
  </xs:sequence>
 </xs:complexType>

 <xs:complexType name="TunnelMethods">
  <xs:sequence>
   <xs:choice>
    <xs:element name="validateServerCertificate" type="serverCertificateValidationParameters"/>
    <xs:element name="doNotValidateServerCertificate" type="Empty"/>
   </xs:choice>
   <xs:element name="unprotectedIdentityPattern" type="IdentityPattern" minOccurs="0">
    <xs:annotation>
```

```
      <xs:documentation>If the [username] and/or  [domain] placeholders are used in the pattern then: if a client certificate is used for authentication then placeholder's values shall be obtained from the CN field of the client certificate.  if the credentials are obtained from the end-user then these shall be obtained from the information the user enters.  if the credentials are obtained from the operating system then these shall be obtained from the information the logon provides.  Typical pattern: anonymous@[domain] for tunneled methods or  [username]@[domain] for non-tunneled methods.  If the credential source is this profile then the pattern would be the actual string to send as the username (no placeholders).</xs:documentation>
     </xs:annotation>
    </xs:element>
    <xs:choice>
     <xs:element name="enableFastReconnect">
      <xs:complexType>
       <xs:complexContent>
        <xs:extension base="Empty">
         <xs:choice>
          <xs:element name="alwaysAttempt" type="Empty"/>
         </xs:choice>
        </xs:extension>
       </xs:complexContent>
      </xs:complexType>
     </xs:element>
     <xs:element name="disableFastReconnect" type="Empty"/>
    </xs:choice>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="ClientCertificate">
  <xs:choice>
   <xs:element name="certificateId" type="CertificateIdentifier">
    <xs:annotation>
     <xs:documentation>This is a reference to an OS pre-stored certificate.</xs:documentation>
    </xs:annotation>
   </xs:element>
  </xs:choice>
</xs:complexType>

<xs:complexType name="CertificateContainer">
  <xs:choice minOccurs="0" maxOccurs="unbounded">
   <xs:element name="certificateId" type="CertificateIdentifier">
```

```
      <xs:annotation>
        <xs:documentation>This is a reference to an OS pre-stored certificate.</xs:documentation>
      </xs:annotation>
    </xs:element>
  </xs:choice>
 </xs:complexType>

 <xs:complexType name="CertificateIdentifier">
  <xs:simpleContent>
   <xs:annotation>
    <xs:documentation>SHA 1 hash over the whole binary certificate in X509 format that uniquely
identifies a certificate in the global list of trusted CAs for the machine (OS managed store in
windows).</xs:documentation>
   </xs:annotation>
   <xs:extension base="NonEmptyString">
    <xs:attribute name="reference" type="xs:boolean">
     <xs:annotation>
      <xs:documentation>true means the element value is a file reference to a certificate in PEM format,
the post-process tool will retrieve the certificate file, convert to a hash, populate the certificateId
element, and set the reference to false to indicate this is the SHA1 hash over that
certificate.</xs:documentation>
     </xs:annotation>
    </xs:attribute>
   </xs:extension>
  </xs:simpleContent>
 </xs:complexType>

 <xs:complexType name="Empty"/>

 <xs:simpleType name="NonEmptyString">
  <xs:restriction base="xs:string">
   <xs:minLength value="1"/>
  </xs:restriction>
 </xs:simpleType>

 <xs:complexType name="ServerRuleFormat">
  <xs:simpleContent>
   <xs:extension base="NonEmptyString">
    <xs:attribute name="match" use="required">
```

```
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:enumeration value="exactly"/>
            <xs:enumeration value="endsWith"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:extension>
  </xs:simpleContent>
 </xs:complexType>

 <xs:complexType name="ServerValidationRules">
  <xs:choice minOccurs="0" maxOccurs="unbounded">
   <xs:annotation>
    <xs:documentation>
Optional only when product allows user to trust server. In which case it allows a profile that has no server validations rules to start with and when a user validates an untrusted server the validation process still validates the server name.</xs:documentation>
   </xs:annotation>
   <xs:element name="matchSubjectAlternativeName" type="ServerRuleFormat">
    <xs:annotation>
     <xs:documentation>DNSName: typically takes the form of a Fully Qualified Domain Name (FQDN)</xs:documentation>
    </xs:annotation>
   </xs:element>
   <xs:element name="matchSubject" type="ServerRuleFormat">
    <xs:annotation>
     <xs:documentation>Either Subject: CN (Common Name) - typically a simple ASCII string.Or Subject: DN (Domain Name) - a composite of a set of DC (Domain Component) attributes</xs:documentation>
    </xs:annotation>
   </xs:element>
  </xs:choice>
 </xs:complexType>

 <xs:complexType name="serverCertificateValidationParameters">
  <xs:sequence>
   <xs:choice>
    <xs:element name="serverNameValidationRules" type="ServerValidationRules"/>
```

```
      <xs:element name="anyServerName" type="Empty">
       <xs:annotation>
       <xs:documentation>the server name within the certificate will not be tested.</xs:documentation>
       </xs:annotation>
      </xs:element>
     </xs:choice>
     <xs:choice>
      <xs:element name="validateChainWithSpecificCa">
       <xs:complexType>
        <xs:complexContent>
         <xs:extension base="CertificateContainer"/>
        </xs:complexContent>
       </xs:complexType>
      </xs:element>
      <xs:element name="validateChainWithAnyCaFromOs" type="Empty">
       <xs:annotation>
        <xs:documentation>the certificate chain will be trusted if it ends in a CA cert from the global
CA cert store.</xs:documentation>
       </xs:annotation>
      </xs:element>
     </xs:choice>
     <xs:element name="userValidatesUntrustedServerCertificate" type="xs:boolean">
      <xs:annotation>
       <xs:documentation>if the server certificate fails to validate then if this is true the end-user will be
asked to validate the server.  If they do so then appropriate trustedCaCerts will be remembered as well
as the server name fields so it will be automatically trusted in the future.</xs:documentation>
      </xs:annotation>
     </xs:element>
    </xs:sequence>
   </xs:complexType>

   <xs:complexType name="ValidateWithSpecificPacs">
    <xs:choice minOccurs="0" maxOccurs="unbounded">
     <xs:annotation>
      <xs:documentation>This is optional because it allows the profile to indicate that we want the engine
to validate the server PACs but that the PACs will be dynamically added by the end-user actions or via
unauthenticated provisioning rather than being statically defined here in the
profile.</xs:documentation>
     </xs:annotation>
```

```
    <xs:element name="trustPacFromGlobalPacStoreWithThisId" type="xs:string">
     <xs:annotation>
      <xs:documentation>
Utilized when there is a global store used for PACs (rather than just per-profile).</xs:documentation>
     </xs:annotation>
    </xs:element>
   </xs:choice>
  </xs:complexType>

</xs:schema>
```

Configuring Machine Authentication

You can enable machine authentication from the Advanced Security screen when you create a Group Policy Object.

The EAPHost notifies the EAP-FAST module that the current authentication is a machine authentication.

Machine authentication is achieved by using one of the following:

- a machine PAC
- a machine certificate
- a machine password

The EAP-FAST module attempts to fetch the machine PAC first. If a machine PAC is unavailable, the EAP-FAST module attempts to fetch a machine certificate. If a machine certificate is unavailable, the EAP-FAST module attempts to fetch the machine password for the machine account in the Active Directory.

When the machine is authenticated with either a machine certificate or a machine password, the EAP-FAST module then requests the provisioning of a machine PAC for subsequent use. If neither a machine certificate nor a machine password is available, the EAP-FAST module requests a machine PAC during the next successful user authentication after a user has logged on. If an existing machine PAC is invalid or expired, the EAP-FAST module relies on this process to request a new machine PAC.

Because machine authentication is integrated with and supported by the Windows 802.1X supplicant, the EAP-FAST module is only responsible for authentication to gain network access. Additional network operations to support machine authentication, such as DHCP, machine-level GPO, and other related network services, are the responsibility of the operating system and the 802.1X supplicant.

Configuring Single Sign-On

SSO is supported by Microsoft Windows Vista in the following ways:

- Windows user credentials are passed to the EAP-FAST module through the EAPHost interface. The system does not prompt the user to provide additional credentials if the EAP-FAST module is configured to use Windows user credentials for network authentication and if the network profile is configured for single sign-on.

- Non-Windows network credentials are collected during the Microsoft Windows Vista logon process. The EAP-FAST module requests the logon module to prompt the user for these network credentials.
- If necessary, the EAP-FAST module is able to prompt the user for additional network credentials before the user logs in to Microsoft Windows Vista.
- If network credentials are stored in the configuration, the EAP-FAST module has access to these credentials before the user logs in to Microsoft Windows Vista.

CHAPTER 5

Configuring Logging

This chapter describes how configure logging on the EAP-FAST module to assist with troubleshooting.

The following topics are covered in this chapter:

Overview of Logging

To generate logs to assist with troubleshooting, the EAP-FAST module utilizes Windows Event Log Service. The logs include information such as the type of event, the event location, the function that was affected by the event, and the date and time of the event.

Configuring and Starting Logging

To access the administrator command prompt and to configure and start logging, perform the following steps:

Step 1 Choose **Start > All Programs > Accessories**.

Step 2 Right-click **Command Prompt** and select **Run as administrator**.

Step 3 At the prompt, enter the following command to configure and start logging:

wevtutil sl Cisco-EAP-FAST/Debug /e:true /k:*category_mask* **/l:***log_level*

Syntax Description

category_mask	Bitmask of categories of logging to be turned on. Valid values are as follows: • **0**—logs all categories. • **1**—logs all messages not falling into the next two categories. • **2**—logs the flow of function entry and exit points with return code only on Verbose log level. • **4**—logs packet dumps only on Verbose log level. The default value is 0.
log_level	Level of logging to be turned on. Valid values are as follows: • **0**—all log levels. • **1**—critical. • **2**—error. • **3**—warning. • **4**—informational. • **5**—verbose. The default value is 0.

Note If you must shut down the device on which logging was running before logging finishes, logging resumes after reboot. When logging is started either automatically or manually, however, the logs are cleared.

Disabling Logging and Flushing Internal Buffers

After you have collected the information that you need, the following command stops logging and flushes all internal buffers:

wevtutil sl Cisco-EAP-FAST/Debug /e:false

Note You must enter this command before you can analyze the .etl file.

Locating Log Files

By default, an .etl file that you can use for analysis and debugging are created at this location:

C:\Windows\System32\Winevt\Logs\Cisco-EAP-FAST%4Debug.etl

If you would like to change this location, enter this command at the administator prompt:

wevtutil sl Cisco-EAP-FAST/Debug /lfn:"*path_to_etl_log_file***"**

Note Logging must not be running when you enter the command to change the path to the log file.

You can also change the path to the .etl file when you start logging. To start logging and specify the location of the .etl file, enter this command at the administrator prompt:

wevtutil sl Cisco-EAP-FAST/Debug /e:true /lfn:"*path_to_etl_log_file***"**

CHAPTER 6

Troubleshooting

This chapter describes EAP-FAST error messages. This chapter also provides guidelines for creating strong passwords.

The following topics are covered in this chapter:

EAP-FAST Error Messages

Error Message `Automatic PAC provisioning is enabled for this profile. However, a valid PAC that matches the server to which the client adapter is connecting could not be found. Do you wish to obtain a new security credential (PAC)?`

Recommended Action Click **Yes** to provision a new PAC for this server using your existing credentials or click **No** to cancel the operation. If you click **No**, the client adapter will fail the authentication.

Caution To prevent possible attacks from rogue access points, do not reprovision a PAC unless it is necessary.

Error Message `While attempting to provision your PAC during auto-provisioning, the network access device failed to authenticate itself. This condition might indicate an attack on your password by a rogue access device. Try again with your current password?`

Recommended Action Click **Yes** to attempt to reauthenticate with your current password. Click **No** to cancel the operation.

Note If the authentication attempt fails again, contact your system administrator to report a rogue access device. Use strong passwords in the future to reduce the chance of your password being compromised; see the "Creating Strong Passwords" section on page 6-6 for tips on creating strong passwords.

Error Message `While attempting to provision your PAC, the network access device timed out. A timeout might indicate an attack on your password by a rogue access device. However, a timeout could be caused by a server outage or a faulty connection. Try again with your current password?`

Recommended Action Click **Yes** to attempt to reauthenticate with your current password. Click **No** to cancel the operation.

Note If a timeout occurs again, contact your system administrator to report a potential rogue access device. Use strong passwords in the future to reduce the chance of your password being compromised; see the "Creating Strong Passwords" section on page 6-6 for tips on creating strong passwords.

Error Message `A valid PAC was not found for your username <username>. Click OK. Re-enter your username in the credential prompt or the User Credentials tab of the EAP-FAST Properties screen. If you entered your username correctly, go to the Connection tab of the EAP-FAST Properties screen either to enable automatic PAC provisioning or Validate server certificate or import a PAC file.`

Recommended Action Click **OK**. Then perform one of the following:

- Re-enter your username.
- If you entered your username correctly, go to the Connection tab of the EAP-FAST Properties screen either to enable automatic PAC provisioning or to import a PAC file.

Error Message `The EAP-FAST authentication attempt failed because you entered the wrong username and password. Please re-enter your username and password.`

Recommended Action Click **OK**. Then re-enter your EAP-FAST credentials when the Enter Wireless Network Password screen appears.

Error Message `The EAP-FAST authentication attempt failed because you might have entered the wrong username and password. Please re-enter your username and password.`

`Warning: If you are sure that you have typed in the right username and password, you may have connected to a rogue device. This can indicate an attack on your password. Using a strong password will reduce the chance of your password being compromised. If this failure happens again, contact your system administrator to report a potential rogue access device.`

Recommended Action Click **OK**. Then perform one of the following:

- If you entered your EAP-FAST credentials correctly, contact your system administrator to report a potential rogue access point. Use strong passwords in the future to reduce the chance of your password being compromised. See the "Creating Strong Passwords" section on page 6-6 for tips on creating strong passwords.
- If you entered your EAP-FAST credentials incorrectly, re-enter your credentials at the Enter Wireless Network Password screen.

- If the username does not match the provisioned PAC, and automatic provisioning is enabled for this profile, click **Yes** at the following message: "You do not appear to be registered with the authentication server. Registration requires that this device be initialized with a security credential. Do you wish to obtain a security credential?"
- If the username does not match the provisioned PAC, and manual provisioning is enabled for this profile, go to the Connection tab of the EAP-FAST properties dialog box and either enable automatic PAC provisioning or import a PAC file.

Error Message `PAC provisioning has failed. This failure is not related to an issue with the username and password. This failure is commonly caused by a server configuration issue. Contact your administrator for assistance.`

Recommended Action Contact your system administrator for assistance.

Error Message `The PAC that you selected for this profile does not match the server to which the client is connecting. However, a matching PAC has been found in your PAC database. Would you like to use this matching credential authority and save it to the profile?`

Recommended Action Click **Yes** to use the matching PAC and to update the profile with this new PAC, or click **No** to cancel the operation and to leave the profile as it is. If you click **No**, the client adapter will be unable to authenticate using the existing profile.

Error Message `You entered different values in the New Password field and the Confirm New Password field. The passwords must be identical. Please try again.`

Recommended Action Re-enter your new password in both fields.

Error Message `The password that you entered in the Old Password field does not match the password that you previously used. Please try again.`

Recommended Action Re-enter your old password in the Old Password field.

Error Message `An error occurred when you attempted to change your EAP-FAST password. The new password might not conform to the server's password policy. Please try again.`

Recommended Action Re-enter your password in the Change Password screen.

Error Message `The EAP-FAST authentication process failed during initialization. Make sure that EAP-FAST and the Trusted Root Certificate Authority certificate are installed correctly.`

Recommended Action Ensure that EAP-FAST and the Trusted Root Certificate Authority certificate are installed correctly.

Error Message `You have connected to a server with the following server name`

`<server_name>`

`The server certificate is signed by the following Root Certification Authority (CA):`

`<root_ca>`

`This Root CA does not match the specified trusted Root CA(s).`

`Do you want to accept this connection?`

`Warning: Connecting to a server signed with untrusted CA might compromise your security.`

Recommended Action If you want the client adapter to connect to this server even though doing so might present a security risk, click **Yes**. Otherwise, click **No**.

Error Message `You have connected to a server with the following server name:`

`<server_name>`

`This server name does not match the specified server name(s).`

`Do you want to accept this connection?`

`Warning: Connecting to an unsecured server might compromise your security.`

Recommended Action If you want the client adapter to connect to this server even though doing so might present a security risk, click **Yes**. Otherwise, click **No**.

Error Message `Your password has expired. Please enter a new password.`

Recommended Action Enter a new password to change the expired password.

Error Message `You entered an empty username, which is not allowed.`

Recommended Action Enter a username.

Error Message `You must select a PAC when using manual PAC provisioning.`

Recommended Action You clicked **OK** on the EAP-FAST Properties screen when automatic provisioning was disabled and no PAC authority was selected. Either enable automatic provisioning or choose a PAC authority from the drop-down list. If the list is empty, import a PAC file.

Error Message `Error opening or reading file: <filename>.`

Recommended Action Try to import the PAC file again. If the same message appears, obtain a new PAC file from your system administrator and import it again.

Error Message `The file is not a valid PAC file: <filename>.`

Recommended Action Try to import the PAC file again. If the same message appears, obtain a new PAC file from your system administrator and import it again.

Error Message `The file does not contain a valid PAC: <filename>.`

Recommended Action Try to import the PAC file again. If the same message appears, obtain a new PAC file from your system administrator and import it using the EAP-FAST Settings screen.

Error Message `The file contains a PAC that will replace an existing PAC already provisioned on your system. Would you like to replace the existing PAC?`

Recommended Action Click **Yes** to replace the existing PAC with the new one from the imported file, or click **No** to cancel the operation.

Error Message `The password you entered to import the PAC file is incorrect. Please try again.`

Recommended Action Try entering your password again.

Error Message `The PAC file import operation has been aborted because of three or more attempts of incorrect passwords.`

Recommended Action Press **OK** to continue.

Error Message `An internal error occurred.`

Recommended Action An internal error occurred when the PAC was being imported. Try importing the PAC again.

Error Message `Insufficient memory or other system error.`

Recommended Action Close other programs and free up some more memory.

Error Message `You must select "Validate server certificate" or a PAC to use user's certificate or one-time password for authentication.`

Recommended Action One-time password or user certificate is selected as the user credential, but there is no PAC selected or Validate Server Certificate option is not checked. Change the settings.

Error Message `You tried to import a PAC file with the same PAC ID as a previously imported or provisioned PAC. Would you like to replace the existing PAC?`

Recommended Action Click **Yes** to replace the existing PAC with the new one from the imported file, or click **No** to cancel the operation.

Creating Strong Passwords

Never write passwords down, on paper or online. Instead, create passwords that you can remember easily but no one can guess easily. One way to do this is create a password that is based on a song title, affirmation, or other phrase. For example, the phrase could be "This May Be One Way To Remember" and the password could be "TmB1w2R!" or "Tmb1W>r~" or some other variation.

Note Do not use either of those examples as passwords.

Characteristics of Strong Passwords

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z).
- Contain numerals and punctuation as well as letters (e.g., 0-9, !@#$%^&*()_+|~ =\`{}[]:";'<>?,./)
- Are at least five alphanumeric characters long.
- Are not a word in any language.
- Are not slang, dialect, or jargon.
- Are not based on personal information, such as the names of family members.

Characteristics of Weak Passwords

A weak password has the following characteristics:

- Contains fewer than eight characters.
- Is a word found in a dictionary (English or foreign)
- Is any other term that is easily guessed or found in common usage. The following are examples of terms that are easily guessed:
  - The name of family, pet, friend, coworker, or fantasy character.
  - A computing term or name, such as a command, site, company, model, or application.
  - A birthday or another kind of personal information, such as an address or telephone number.
  - A predictable letter pattern or number pattern, such as aaabbb, qwerty, zyxwvuts, or 123321.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit.

Password Security Basics

Follow these basic guidelines when dealing with passwords:

- Never reveal a password, even to family members.
- Never talk about a password in front of others.
- Never hint at the format of a password (such as "my family name").

- Never use characters from outside the standard ASCII character set. Some symbols, such the pound sterling symbol (£), are known to cause login problems on some systems.

APPENDIX A

Abbreviations

Table A-1 defines the acronyms used in this publication.

Table A-1 List of Acronyms

Acronym	Expansion
AAA	authentication, authorization, and accounting
API	application program interface
ASCII	American Standard Code for Information Interchange
CA	Certificate Authority
CCX	Cisco Compatible eXtensions
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
EAP-FAST	Extensible Authentication Protocol—Flexible Authentication via Secure Tunneling
EAP-GTC	Extensible Authentication Protocol—Generic Token Card
EAP-MSCHAPv2	Extensible Authentication Protocol—Microsoft Challenge Handshake Authentication Protocol Version 2
EAP-TLS	Extensible Authentication Protocol—Transport Layer Security
ETW	Vista's Event Tracing for Windows
GPO	Group Policy Object
LDAP	Lightweight Directory Access Protocol
MITM	man-in-the-middle
MMC	Microsoft Management Console
MSCHAPv2	Microsoft Challenge Handshake Authentication Protocol Version 2
OTP	one-time password
OU	organizational unit
PAC	Protected Access Credential
PEAP	Protected Extensible Authentication Protocol
PIN	personal identification number
PKI	public-key infrastructure

Table A-1 List of Acronyms (continued)

Acronym	Expansion
RADIUS	Remote Authentication Dial-In User Service
RFC	Request for Comments
SDK	Software Development Kit
SSID	Service Set Identifier
SSO	single sign-on
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
UPN	User Principal Name
XML	eXtensible Markup Language

APPENDIX B

Acknowledgments and Licensing

This product includes software developed by the OpenSSL Project for use in the OpenSSL toolkit (http://www.openssl.org/).

This product inlcudes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptosoft.com).

```
OpenSSL License
---------------

/* ====================================================================
 * Copyright (c) 1998-2007 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
```

```
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */

 Original SSLeay License
 -----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
 *    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
```

```
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed.  i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/
```