Configuration Guide
Windows PEAP-GTC Supplicant Plugin

This document describes the installation and configuration of a supplicant plug-in that supports Protected Extensible Authentication Protocol (PEAP) with EAP-Generic Token Card (GTC) authentication for Windows clients. This software can only be installed and used in conjunction with an Aruba Mobility Controller with the AAA FastConnect (EAP Termination) feature enabled.

This software supports 32-bit and 64-bit versions of Windows Vista, Windows 7, Windows 8.x, and Windows 10.

This document describes the following topics:

PEAP with EAP-GTC is only supported on Aruba Mobility Controllers running ArubaOS version 2.5.4 or later. The Mobility Controller administrator must enable the AAA FastConnect feature and configure EAP-GTC as the inner EAP type, as described in the ArubaOS User Guide.

Overview

The Extensible Authentication Protocol (EAP) type Protected EAP (PEAP) uses Transport Layer Security (TLS) to create an encrypted tunnel. Within the TLS tunnel, the client can be authenticated using one of the following “inner EAP” methods:

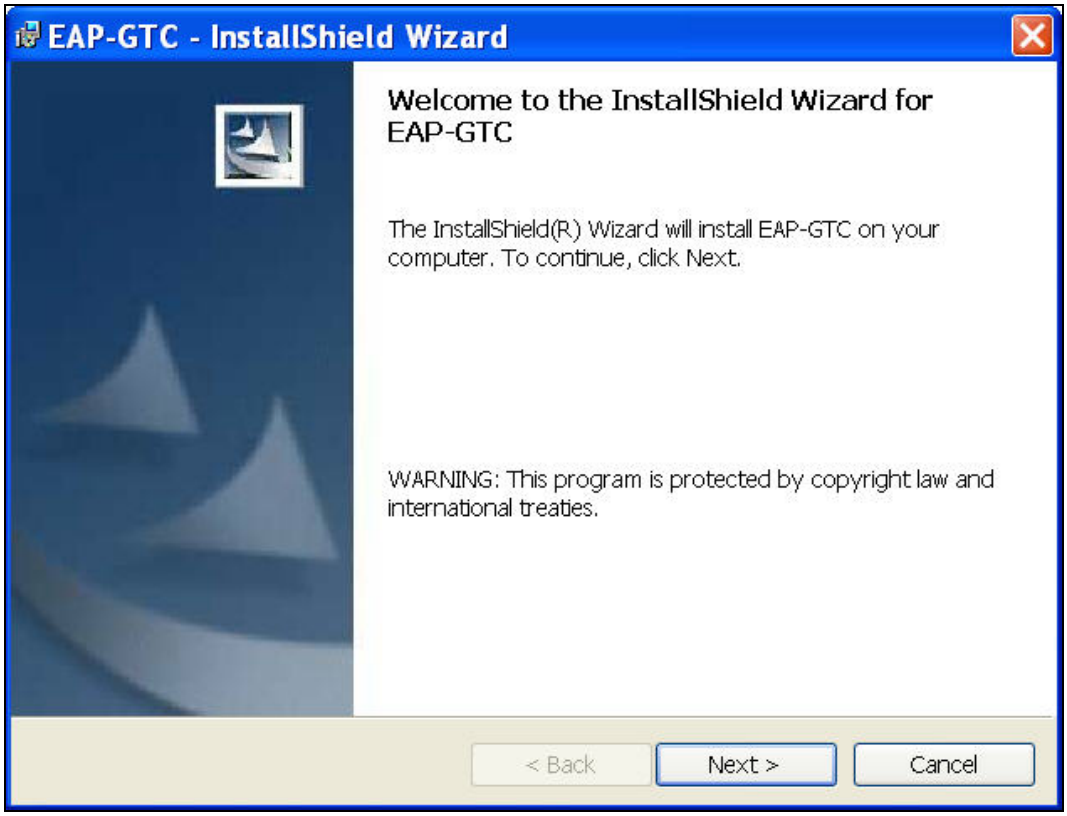
- EAP-Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2): Described in RFC 2759, this EAP method is widely supported by Microsoft clients. This is the default method and is supported by ArubaOS 2.5.1 and later.
- EAP-Generic Token Card (GTC): Described in RFC 2284, this EAP method permits the transfer of unencrypted usernames and passwords from client to server. The main uses for EAP-GTC are one-time token cards such as SecureID and the use of LDAP or RADIUS as the user authentication server. You can also enable caching of user credentials on the controller as a backup to an external authentication server. This method is supported by ArubaOS 2.5.4 and later.

The current Wireless Zero Configuration (WZC) under Windows only supports PEAP with EAP-MS-CHAPv2. To use PEAP with EAP-GTC authentication in your wireless network, you need to install and configure the Aruba supplicant plug-in software on your Windows clients.

Installing the Supplicant Plugin Software

Download the software for the PEAP with EAP-GTC supplicant plug-in from the Aruba Networks support Web site. Versions are available for both 32-bit and 64-bit Windows. Install the software by opening the installer package on a Windows client and following the instructions in the InstallShield Wizard shown in Figure 1.

Figure 1 *The InstallShield Wizard*

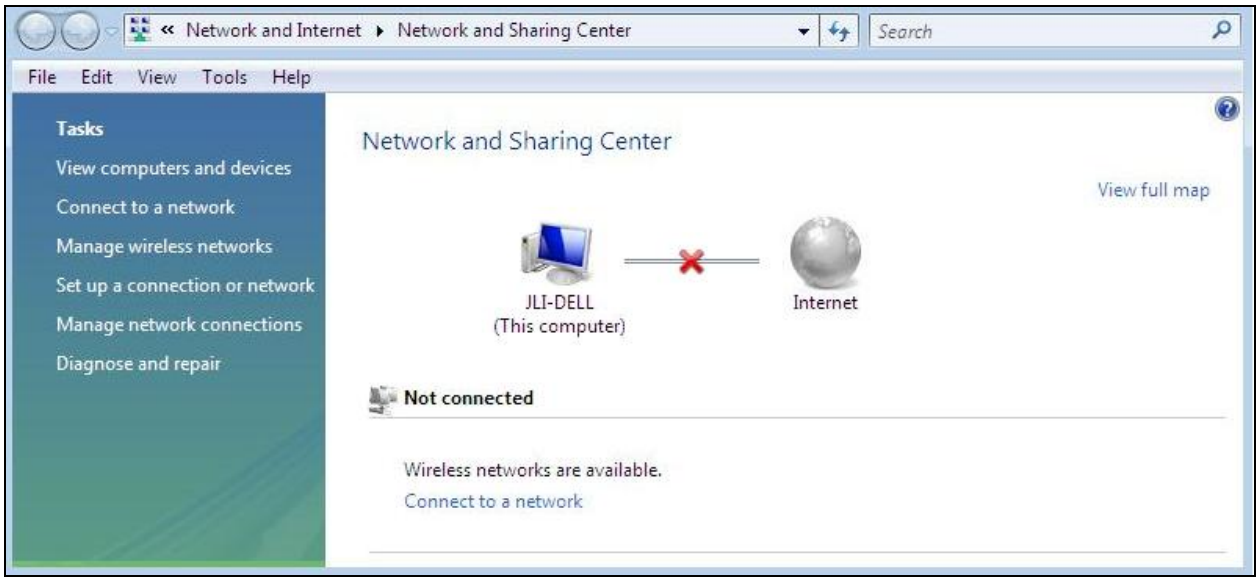


Configuring PEAP with EAP-GTC on the Windows Client

This section describes how to configure PEAP with EAP-GTC on a Windows client after you install the supplicant plug-in software .

1. On the Windows client, open the **Network and Sharing Center** window shown Figure 2.

Figure 2 *Network and Sharing Center*



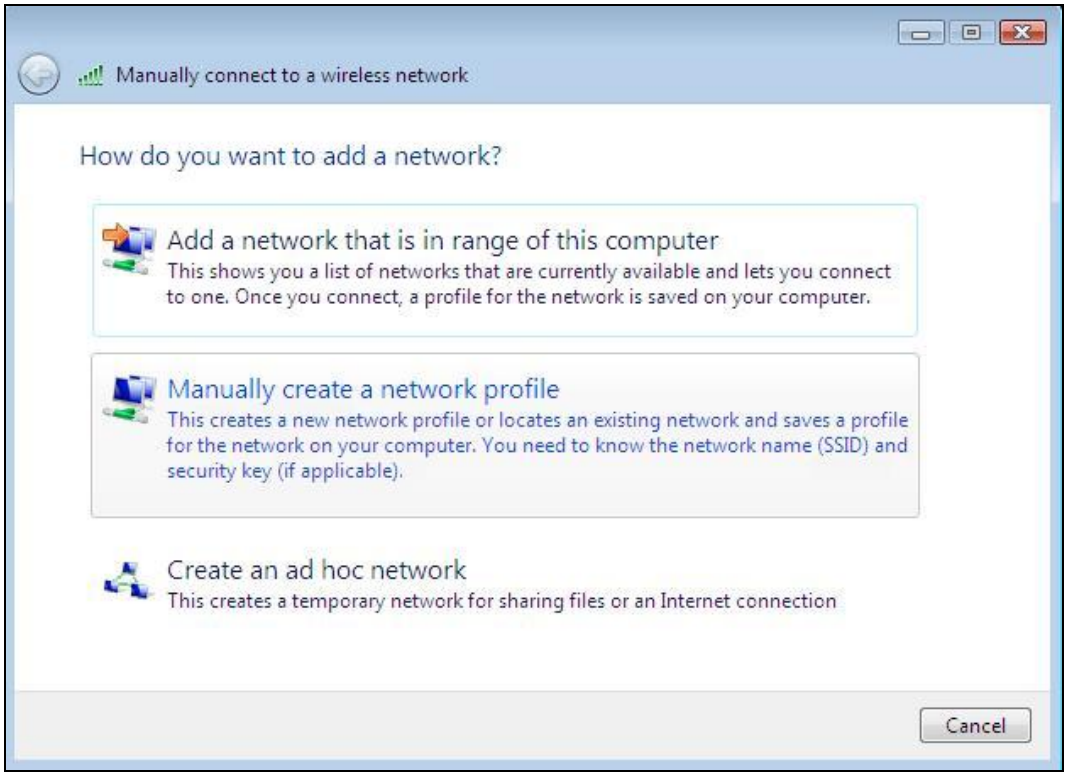
2. Click **Manage Wireless Networks**.

3. In the **Manage Wireless Networks** window shown in Figure 3, click **Add**.

Figure 3 *The Manage Wireless Networks Window*

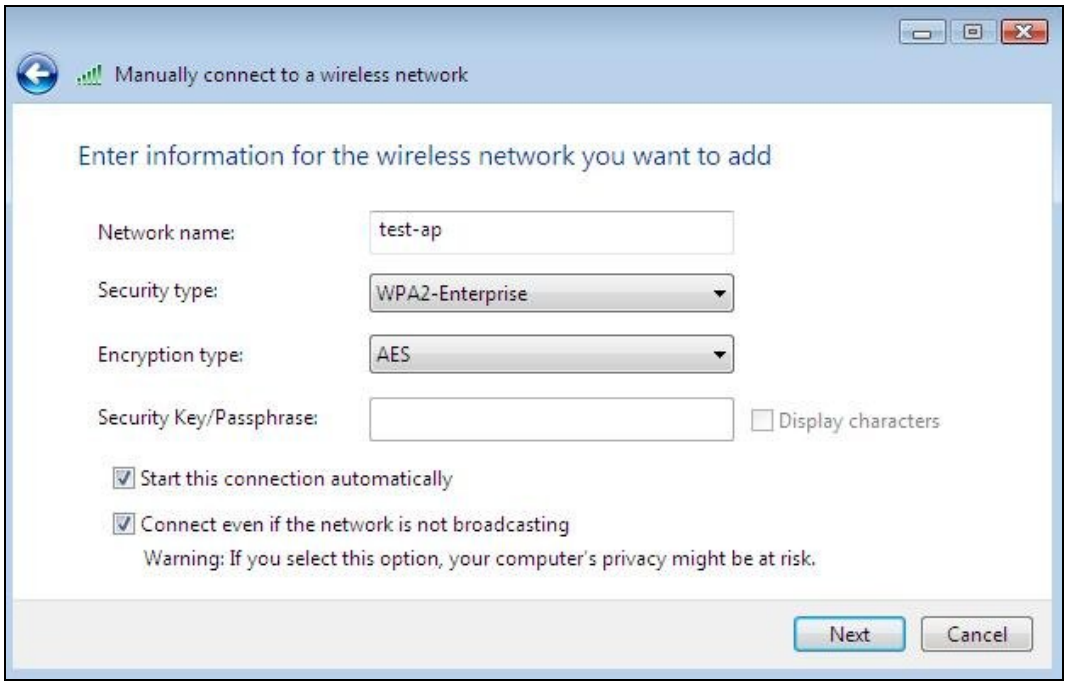
4. Click the **Manually create a network profile** option shown in Figure 4.

Figure 4 *Manually Create a Profile*



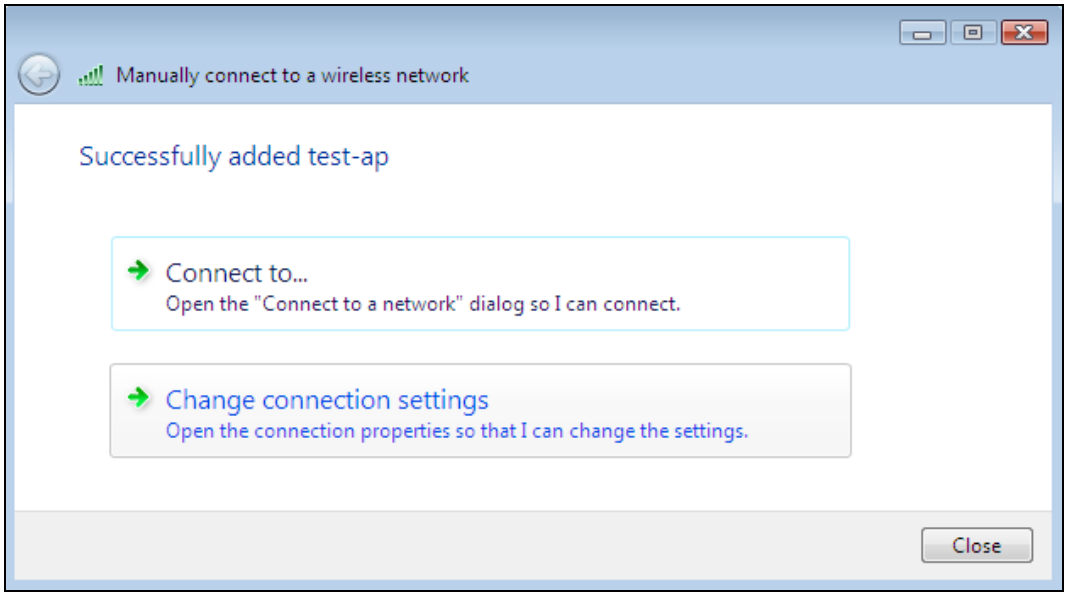
5. Enter the following information in the **Wireless Network Information** window shown in Figure 5:
   - Network name: Enter the network SSID
   - Security type: Select **WPA2-Enterprise**, **WPA-Enterprise**, or **802.1x** from the drop-down list.
   - Encryption type: Select **AES**, **TKIP**, or **WEP** from the drop-down list.

Figure 5 *Configure Wireless Network Information*



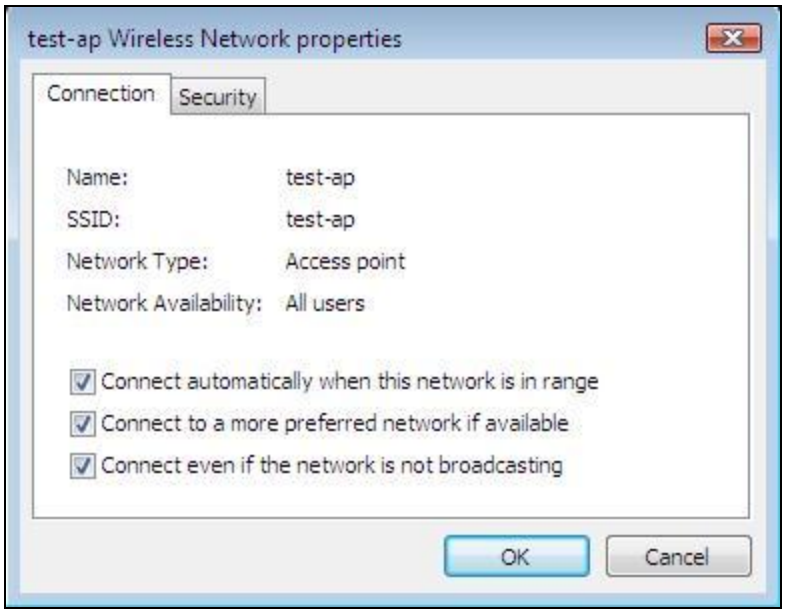
6. Click **Next**.
7. Select the **Change connection settings** option shown in Figure 6.

Figure 6 *Change Connection Settings*



8. The **Wireless Network properties** dialog box appears with the **Connection** tab selected, as shown in Figure 7. Click the **Security** tab.

Figure 7 *Wireless Network Properties*



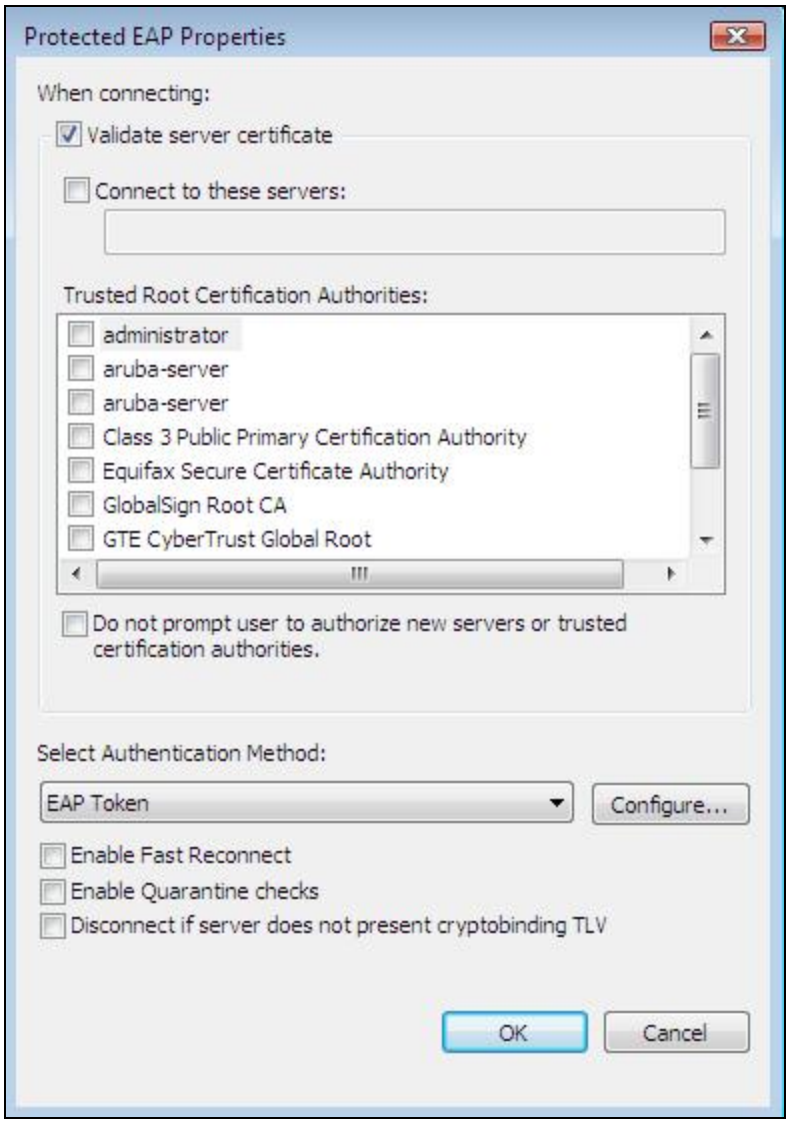
9. Select **Protected EAP** from the **Choose a network authentication method** drop-down menu shown in Figure 8.

Figure 8 *Select Protected EAP*

While EAP-GTC (EAP token) appears in both the inner and outer authentication method lists, it should only appear in the inner method list. This is a bug in Windows Vista. If you see this issue, check with Microsoft for a possible fix.

10. Click on **Settings** to display the **Protected EAP Properties** dialog box shown in Figure 9.

Figure 9 *Protected EAP Properties*



11. Select **EAP Token** from the **Select Authentication Method** drop-down list.

NOTE

When you select **EAP Token** as the authentication method, no dialog box is displayed if you click **Configure**.

12. Click **OK**.

Log Files

The supplicant plug-in software logs authentication events to the Windows tracing directory located at \Windows\Tracing\eap-gtc.log. Inspecting the log file is normally not necessary; however, if there is a problem with client authentication, you can view the log file with a text editor.

To enable logging, access the Windows command-line interface (command.exe) and issue the following command:

```
Netsh ras set tracing eap-gtc enable
```

To disable logging, access the Windows command-line interface and issue the command:

```
Netsh ras set tracing eap-gtc disable
```

The following messages in the log file indicate a successful client authentication (messages are preceded by the date and time of the event):

```
RasEapMakeMessage :: Got EAPCODE_success
```

```
RasEapMakeMessage :: Authentication succeeded
```

The following messages in the log file indicate a client authentication failure because the wrong password was entered for the authentication:

```
RasEapMakeMessage :: Got EAPCODE_failure
```

```
RasEapMakeMessage :: Authentication failed. Wrong password.
```

The following messages in the log file indicate that the AAA FastConnect feature is not enabled on the Mobility Controller:

```
RasEapMakeMessage :: Got EAPCODE_Request
```

```
RasEapMakeMessage :: AAA FastConnect (dot1x termination) is not enabled on the
Aruba switch
```