Configuring Token Authentication in Open Mobile

VERSION 2.0, APRIL 2012

Open Mobile 2.0 and later clients permit the use of authentication tokens for login credentials when connecting using the PEAP-GTC protocol. Enabling token authentication for an Open Mobile profile requires these steps:

- Creation of an account definition with hardware or software authentication token as a valid credential.
- Inclusion of the account definition in the profile.
- Enablement of the PEAP-GTC connection method in each user's Open Mobile client.

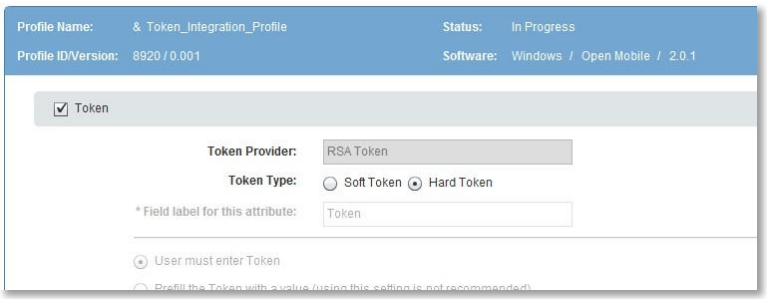
Hardware Token Authentication

Enabling Hardware Token Authentication in a Profile

To enable hardware token authentication for a profile, you must create (or select) an account type to accept the token credentials. You can enable hardware token authentication using these steps:

To enable hardware token authentication for a profile,

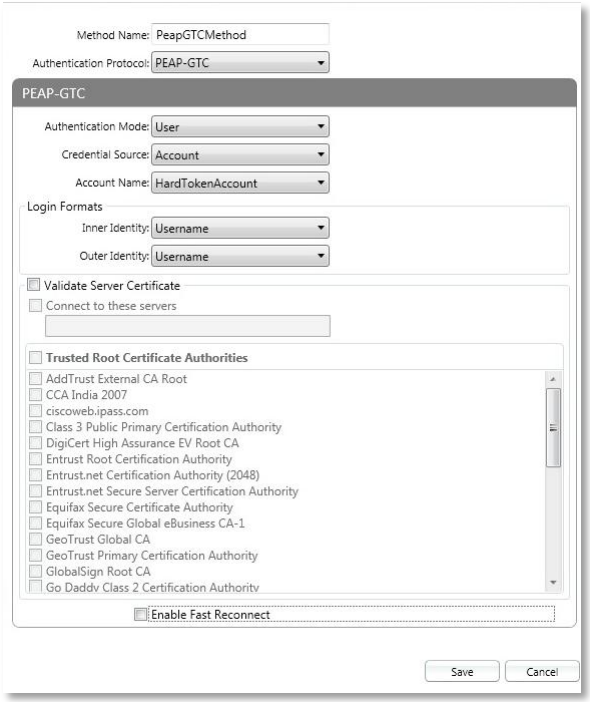
1. Log into the Open Mobile Portal.
2. Select (or create) a profile to include hardware token authentication.
3. Under **Accounts**, click **Configure**.
4. Click **Create New Account.**
5. In **Name** and **Display Name**, enter an account name and display name.
6. Under **Account Attributes**, select the attributes for the account type, including **Token**.
7. Under **Token Type**, select **Hard Token.**
8. Continue configuring the account type and profile as desired, and save.



Enabling Hardware Token Authentication in Open Mobile

Once they receive the profile you have modified or created, users can enable hardware token authentication in the Open Mobile client. You will need to supply users with the connection method details, including values for inner and outer identity.

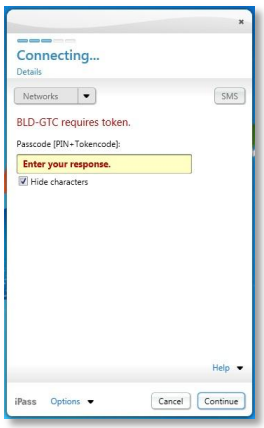
To enable token authentication in Open Mobile,



1. Launch Open Mobile.
2. Click **Options | Wi-Fi.**
3. Under **Campus Networks**, click **Add**.
4. In **Network Name**, enter the name of the network that requires token authentication.
5. In **Security**, select the security type used by the network.
6. In **Connection Method**, click **Add**.
7. In **Method Name**, assign a name to the connection method, such as *PEAPGTCMethod*.
8. In **Authentication Protocol**, select PEAP-GTC.
9. Under **PEAP-GTC**, select the following:
    - **Authentication Mode**: *User*
    - **Credential Source**: *Account*
    - **Account Name:** Select the name of the account used for hardware token authentication.
    - Under **Login Formats**, for both **Inner Identity** and **Outer Identity**, select the appropriate value from the drop-down list, as specified by your administrator .
10. Click **Save**.
11. Click **Close** to close the **Options** panel.

Note that once a single user (or administrator) has configured the PEAP-GTC connection method (that is, Steps 8-10), you can export that user's settings and then import them into Open Mobile profile for other users to make use of.

When included in a profile, user with the profile s will no longer need to configure the method individually, but will be able to select the method from the list of available connection methods to assign to the campus network. See the iPass Online Reference article #2987, *Configuring OCR in Open Mobile*, for more information.



Connecting to a Network using Hardware Token Authentication

Having configured a campus connection for token authentication, users can now connect to the network.

To connect using hardware token authentication:

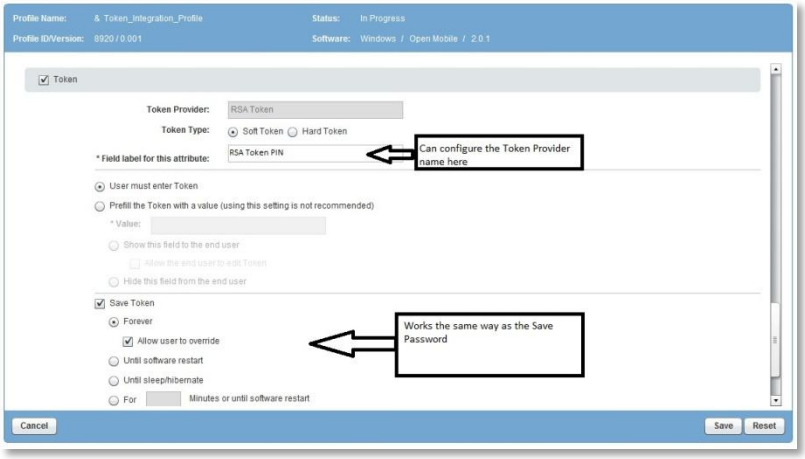
1. Launch Open Mobile.
2. In the list of Available Networks, select the network that supports token authentication.
3. Under the name of the account, enter the prompted credentials for Hard Token (Username and Domain). Click **Continue**.
4. In **Passcode**, enter your PIN plus the token code.
    - To mask the entered characters for additional security, select **Hide characters.**
    - If the entered passcode has expired, you will be prompted to generate a new one.
5. Click **Continue**. You will be connected to the network.

Software Token Authentication

Enabling Software Token Authentication in a Profile

To enable software token authentication for a profile, you must create (or select) an account type to accept token credentials. You can customize the behavior of Open Mobile regarding software token authentication.

- **Rename Text Label:** The text label used for the token entry box in Open Mobile can be renamed.
- **Token Entry:** You can choose to require token entry by the user, or pre-fill the token value with a value contained in the profile. For optimal security, pre-filling the value is not recommended.
- **Save Token:** You can choose to have Open Mobile save the value of the token entered by the user. If saved, you can choose how long Open Mobile will save the value: forever (users can override the saved value), until software restart, until sleep or hibernation, or for a defined interval.



To enable software token authentication for a profile,

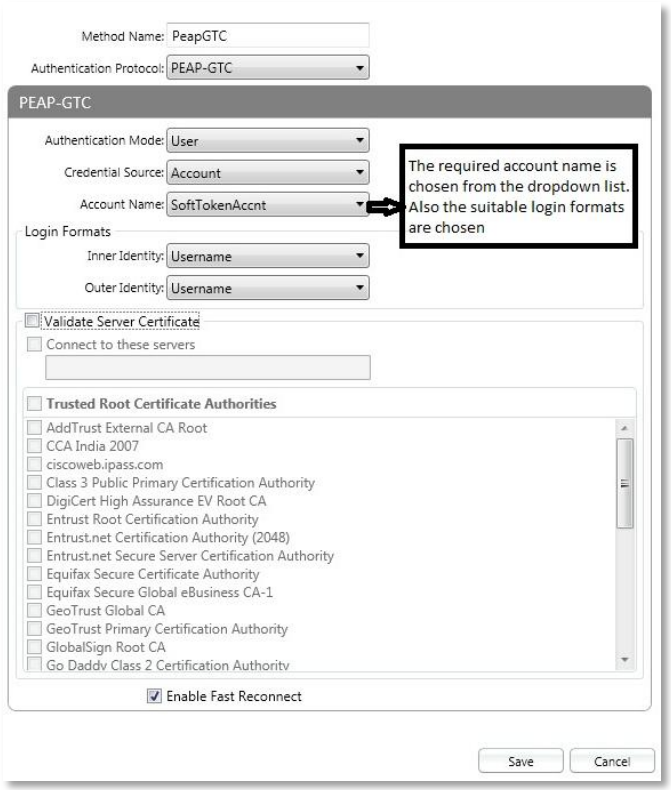
1. Log into the Open Mobile Portal.
2. Select (or create) a profile to include Software token authentication.
3. Under **Accounts**, click **Configure**.
4. Click **Create New Account.**
5. In **Name** and **Display Name**, enter an account name and display name.

6. Under **Account Attributes**, select the attributes for the account type, including Token.
7. Under **Token Type**, select *Soft Token*.
8. In **Field Label for this attribute**, if you wish to customize the label shown to users, enter a custom value.
9. Select values for token entry and for token saving.
10. Continue configuring the account type and profile as desired, and save.

Enabling Software Token Authentication in Open Mobile

Once they receive the profile you have modified or created, users can enable software token authentication in the Open Mobile client. You will need to supply users with the connection method details, including values for inner and outer identity.

To enable token authentication in Open Mobile,



1. Launch Open Mobile.
2. Click **Options | Wi-Fi.**
3. Under **Campus Networks**, click **Add**.
4. In **Network Name**, enter the name of the network that requires token authentication.
5. In **Security**, select the security type used by the network.
6. In **Connection Method**, click **Add**.
7. In **Method Name**, assign a name to the connection method, such as *PEAPGTCMethod*.
8. In **Authentication Protocol**, select PEAP-GTC.
9. Under **PEAP-GTC**, select the following:
   - **Authentication Mode**: *User*
   - **Credential Source**: *Account*
   - **Account Name:** Select the name of the account used for hardware token authentication.
   - Under **Login Formats**, for both **Inner Identity** and **Outer Identity**, select the appropriate value from the drop-down list, as specified by your administrator .
10. Click **Save**.
11. Click **Close** to close the **Options** panel.

Note that once a single user (or administrator) has configured the PEAP-GTC connection method (Steps 8-10), you can export that user's settings and then import them into an Open Mobile profile for other users to make use of. When included in a profile, users with the profile will no longer need to configure the method individually, but will be able to

select the method from the list of available connection methods to assign to the campus network. See the iPass Online Reference article #2987, *Configuring OCR in Open Mobile*,for more information.

Selecting a Token Provider

Several software token providers may be available, and each can provide multiple tokens (distinguished by serial number). If so, the user will need to select the correct provider and token serial number before connecting.

To select a token provider,

1. Click **Options | Preferences.**
2. Click **Token**.
3. Under **Preferred Token Type**, select the token provider and serial number of the token to be used for authentication.
4. Click **Close**.

Connecting to a Network using Software Token Authentication

Having configured a campus connection method for token authentication, and selected a token provider, users can now connect to the network.

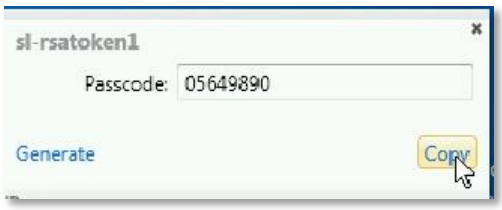
To connect using software token authentication,

1. Launch Open Mobile.
2. In the list of Available Networks, select the network which supports token authentication
3. Under the name of the account, enter the prompted credentials, including the token PIN.
4. Click **Continue**. You will be connected to the network.

Generating a Passcode

If a passcode is required as a one-time password (OTP), you can use Open Mobile to generate one. Open Mobile will generate the passcode using the configured software token settings.

> *Note: Passcode generation will be available only if an account with Software Token authentication is configured in the user's profile.*



To generate a new passcode,

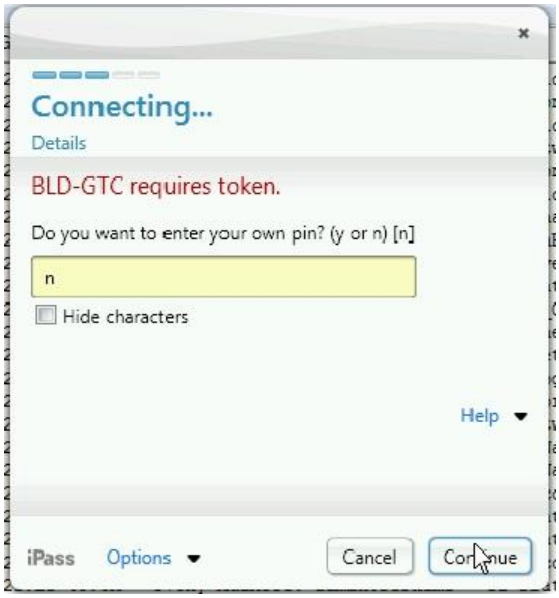
1. Right-click the Open Mobile system tray icon and pick Generate Passcode.
2. If the token PIN is not available, in Enter PIN, type the token PIN, and then click OK.
3. A new passcode is generated. Click **Copy** to copy the generated passcode to the clipboard, where it can be used for other applications or connections.

Generating a New PIN

If the hardware or software PIN has expired, the user will be prompted to generate a new PIN or allow the server to generate one using Open Mobile. New PIN generation is performed during the connection process.

To generate a new PIN if prompted,

1. After receiving the expired PIN message, in **Do you want to enter your own PIN?,** do one of the following:
   - Enter **Y** to enter your new PIN. Click **Continue**, and skip to Step 2.
   - Enter **N** to have Open Mobile generate a PIN. Click **Continue**, and skip to Step 5.
2. Click **Continue**.
3. Enter your new PIN. The new PIN must be a numerical string 4 to 8 digits in length. To mask the entered characters for additional security, select **Hide characters**.
4. Click **Continue**. Re-enter your new PIN to confirm it. Skip to Step 6.
5. Under **Are you prepared to accept a system generated PIN?** Enter **Y**. Click **Continue**.



6. A new PIN is generated, and you will be connected to the network with your new PIN.