2.7.1 Provisioning Profile

1. Provisioning profile

Provisioning profile is a PrivateWave configuration template, that can be re-used across different VoIP accounts. It is possible to create different provisioning profile, depending on organization and groups of users.

Provisioning profile can be assigned to a group, as a default profile for all VoIP account in that group. It is possible to assign a provisioning profile to a specific VoIP account, overriding the group configuration.

CSR can select and assign a specific provisioning profile.

Show ProvisioningProfile						
General Options Name: pTime: Customer Service Email: SIP Proxy Port: Logging: Dialing timeout: Binging timeout: Connecting timeout: Connecting timeout: Disconnecting timeout: Disconnecting timeout: Disconnecting timeout: Bead only settings: Multilevel Security: Enable messaging: User can edit history log size: History log size: PIN: cache timeout: DIN max refries: PIN hock time: Enable read notification: User can enable-disable read notification	OPTIONAL	Mutual Authentication Opti Mutual Authentication: Server Cert. Name: Client Cert. Extension: Client Cert. Extension: Genver Cordownload URL: Client Cert. Download URL: User for Client Cert. Download Pav for Client Cert. Download S/MIME: CSR: Country Name: Organization Name: Organization Name: Organization Name: Organization Name: Organization Name: Street Address: Postal Code: Title: Email Address: Postal Code: Title: Email for gend CSR:	True *.privatewave.eu.cer .pem pw_client(dev).p12 pw_client https://download.privatewa https://download.privatewa developer		Certificate Pinning Options SSL Pinning: Server Cert. Name: Jserver Cert. Download URL: User for Server Cert. Download Paw for Server Cert. Download	
Message expiration timeout:	2	CSR Email Subject: CSR Email Body:	CSR- Certificate Signing Request in Attachment CSR- Certificate Signing Request in Attachment	6		

figure 1. default provisioning profile

By default the appliance comes with a default provisioning profile (shown in figure 1. default provisioning profile).

2. Create a new provisioning profile

Create ProvisioningProfile

In order to create a new provisioning profile you have to press the "New ProvisioningProfile" button and get a new profile form as below:

General Options		Mutual Authentication	Certificate Pinning Options	
Name: \star		Mutual Authentication:	SSL Pinning:	
pTime:	100	Server Cert, Name:	 Server Cert. Name:	
	100	Server Cert, Name:	Server Cert, Download URL:	
Customer Service Email: 🔹 😽		Client Cert. Extension:		
SIP Proxy Port:		Client Generic Cert, Name:	User for Server Cert. Download:	
Logging:			Psw for Server Cert. Download:	
	✓	Cert. Password:		
Logging Level:	INFO V	Server Cert. Download URL:		
Dialing timeout:	120	Client Cert, Download URL:		
Ringing timeout:		Client Cert, Download URL:		
	120	User for Client Cert. Download:		
Connecting timeout:	30	Psw for Client Cert, Download:		
Dialing timeout:	90			
Disconnecting timeout:		S/MIME:		
-	10	CSR:		
Read only settings:	v	CSR Extension:		
Multilevel Security:		Country Name:		
Enable messaging:	 Image: A set of the set of the			
User can edit history log size:	•	Organization Name:		
History log size:	50 🔻	Organizational Unit Name:		
PIN:	MANDATORY V	Common Name:		
PIN cache timeout:	600	Locality Name:		
PIN max retries:	5	State or Province Name:		
PIN lock time:	900	Email Address:		
Enable read notification:	×	Street Address:		
User can enable-disable read notification:	×	Postal Code:		
Message expiration:	OPTIONAL V	Title:		
Message expiration timeout:	15			
		Email for send CSR:		
		CSR Email Subject:		
		CSR Email Body:		
		Cox cinali body:		



- Customer Service Phone: number to be called to reach the customer service
- Customer Service Email: email that will receive the logs and the complaints about the issues
- Logging: it's not mandatory but still very suggested to enable the logging in the clients for possible troubleshooting analysis
- Read only settings: very handy to keep the application control. This wouldn't let the user to change the settings by his/hers own.

2.2. Secure Messaging options

By default this option is set to enabled.

• Enable Messaging: enables Secure Messaging feature on PrivateWave .

If you want your customers to use this feature then you are obliged to check the above option and then you have to provision the new configuration to all the interested clients.

2.3. Privacy options

9

- User can edit history log size: if checked, then customers can change theirs History log size. History is a new way of grouping events occurred on the client, both Secure Calls and Secure Messages. Thus it's an important privacy subject how many events can stay in the History list.
- History log size: In case users were not able to set their history size it could be convenient to decide a maximum amount of events to be shown client side. This option is where you can take this decision. Please consider that default value is 50 events per user.

As History groups events by the contact's numbers they occurred to, then History size number is to be meant as per contact's number. Eg: if there's a 50 events value set in History log size, each contact listed in History can show up to 50 events. 10 contacts who had events with a customer then create 500 (50 max events list * 10 contacts) history log lines, all grouped by contact's number.

Once you completed to fill the form you can proceed with the profile creation just pressing the "Create" button at the bottom.

Show ProvisioningProfile



2.4. PIN options

- PIN: configure if PIN is OPTIONAL or MANDATORY on clients
- PIN cache timeout: configure how many seconds PIN is cached, before asking again the PrivateWave 's user to input his own PIN
- PIN max retries: how many times user can insert the wrong PIN number, before PrivateWave is locked
- PIN lock time: how many seconds PrivateWave remains locked, before user is able again to input the right PIN, after he inserted the wrong one "PIN max retries" times.

2.5. Read Notification

- Enable read notification: this option is to configure if client have to send read notification when a secure message is read.
- User can enable-disable read notification: this option is to let user to enable or disable read notification feature from client setting screen.

2.6. Message expiration

- Message expiration: this options make sense when PIN is enabled. If set to OPTIONAL messages will not expire automatically otherwise if set to MANDATORY messages will expire automatically after "Message expiration timeout"
- Message expiration timeout: how many minutes messages remains readable after beeing read the first time when PIN is enabled and "Message expiration" is MANDATORY.

When PIN is not enabled messages automatically expires after 15 minutes

2.7. Mutual authentication

Mutual authentication requires a client authentication through X.509 certificate. This are some options required for client enrollment. In order to make mutual authentication work the following steps are needed

1. server certificate has to be copied in /data/shared/client_cert in DER format:

```
openssl x509 -in server_certificate.pem -inform pem -outform der -out server_certificate.der
```

- 2. certificate of the issuer (CA) of the client certificate has to be inserted in Certification Authority List as described in 2.3 Certificates management
- 3. TCP port 9443, used by client to download certificate during the provisioning, has to opened in firewall rules:

```
iptables -I INPUT 10 -i <nic> -p tcp -m tcp --dport 9443 -j ACCEPT service iptables save
```

 If "CSR encrypted" is enabled than CSR generated by client has to be decrypted through the web page Open configuration -> Client Provisioning -> CSR Decryption

🛉 Home					
CSR Decryption					
Browse No file selected.					
Decrypt & Download					

- 5. Once the certificates has been signed has to be copied in /data/shared/client_cert and the file name must <username>.pem
- 6. In order to use a generic certificate (the same for each client) it has to be copied in /data/shared/client_cert

2.8. SSL certificate pinning

SSL certificate pinning is a stronger way for server authentication by the client. Clients are strictly

2.9. Edit a provisioning profile

From the Provisioning Profile list, choose the profile you need to edit and click on it with your mouse. the "Show Provisioning Profile" page will appear (see f igure 3. new provisioning profile created).

Press the "Edit" button.

Show ProvisioningProfile



Change the fields you need to and when you're done press the "Update" button at the bottom of the form to save the changes.

3. Delete a Provisioning Profile

By the very same form shown above in figure 3. new provisioning profile created you can also delete your Provisioning Profile.

You have to click on the "Delete" button and Confirm the operation by clicking "Ok" in the warning pop-up window. The Profile should be gone.

2.7.2 SMS Gateway