



Installation Guide

**Odyssey Access Client FE 4.5
Windows Mobile 5.0
on the Intermecc CK61-G with the Apriva CSP**



Juniper Networks, Inc.
2251 Corporate Park Drive
Herndon, VA 20170

October 2008

Installing Juniper Networks OAC FE 4.5 for Windows Mobile 5.0 on the Intermec CK61-G with the Apriva CSP


Apriva Software considerations

Before installing OAC, ensure that the Apriva CSP and Smartcard reader are installed and functioning correctly. Install OAC prior to Apriva SensaGuard.

Intermec Settings considerations

If the Intermec device is clean booted or the Assured Radio Deactivation state is changed, the setup program asks a few questions. The answers to these questions should be as follows:

1. DHCP – answer Yes.
2. 802.11 – answer No, as this enables a different supplicant which will not let OAC run correctly.

The Intermec Assured Radio Deactivation should be 'Disabled'. The box should be **Red** in the bottom right hand corner. If the Assured Radio Deactivation is 'Enabled', then the box is Green; therefore the Wi-Fi radio can not be turned on. If you click on the iConnect  icon on the bottom right, the configuration should look like the right picture. Wireless may or may not be checked; either case is ok.



OAC Installation Pre-requisites

Items needed for the OAC installation and configuration

1. The OAC 4.5 install cab - 'OdCeClientPPCSigned.ARMV4.CAB'
2. The OAC configuration cab - 'Intermec Funk_Config3.cab'
3. Safeboot executable (installed in Apriva Software folder)
4. OAC FE 4.5 License Key. OAC on WM 5.0 requires a key to finish install.
5. Valid CAC Card
6. Name of the Network - SSID. SSID is case sensitive.
7. Confirm Network is using Aruba xSec as the association mode.
8. Intermediate and Root certificate for the Client Authentication certificate on the CAC Card.
9. RADIUS server Root CA certificate.

Installing OAC

Using ActiveSync to copy the following files to My Documents on the Intermec device:

- OdCeClientPPCSigned.ARMV4.CAB
- Intermec Funk_ConfigX.cab
- Safeboot executable file if not in the Apriva directory
- Intermediate and Root CA certificates of CAC Card
- RADIUS server Root CA certificate

Once these files are on the target device, use File Explore on Windows Mobile locate these files.

Install the Root and Intermediate certificates by tapping on each file. You can verify these certificates are installed by going to Certificate Settings.

Start
Settings
System tab
Certificates
Root tab



Install OAC by tapping the file `OdCeClientPPCSigned.ARMV4.CAB` . The installation program will ask where to install OAC.

Select the radio button – Device
Tap on Install



OAC will install. When the installation is successful the following dialog box will be displayed.

Tap on ok



Install the Intermec Funk_Config3.cab. Again, select the radio button - Device and Install.

Close File Explore

Launch OAC

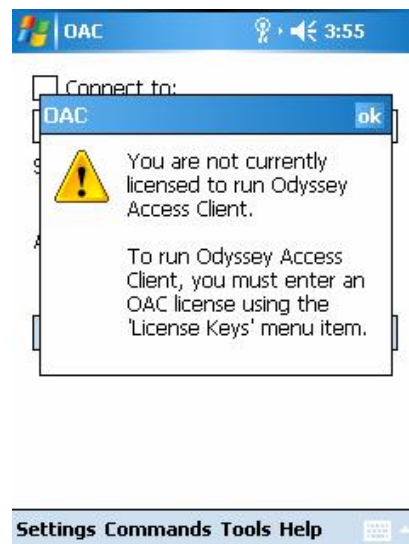
Start

Program Files

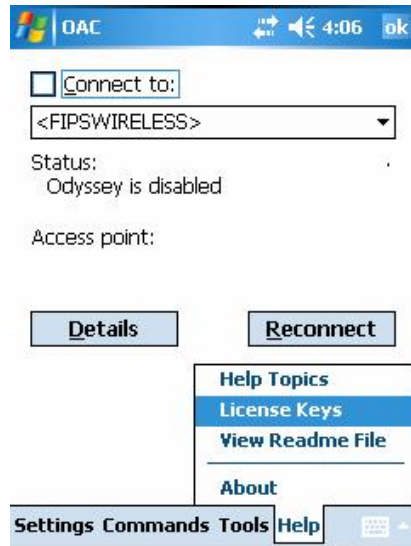
Tap on OAC (the Odyssey ship icon)



OAC will display a dialog box requesting a license key. Tap on ok.



Input the OAC license key. At the bottom of the OAC UI, select
Help
License Keys



Type in license key string
Tap on Add



This example shows an evaluation key message. A production key will just state license is valid.

Tap on ok



At this point make sure OAC is not checked to connect
Exit OAC (Settings -> Exit)
Reboot the terminal using, for instance, the **SafeBoot** executable.



Install Apriva SensaGuard (see Apriva installation instructions).

After Apriva SensaGuard is installed and tested with your reader and CAC Card, continue the OAC installation.

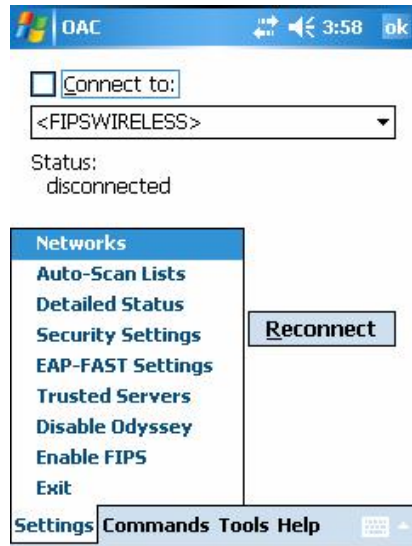
The Apriva SensaGuard will automatically launch OAC in about 15-25 seconds after the PIN has been validated by Apriva SensaGuard.

When OAC launches, the status message will change from null, to 'locating adapter' and settle on 'disconnected'.

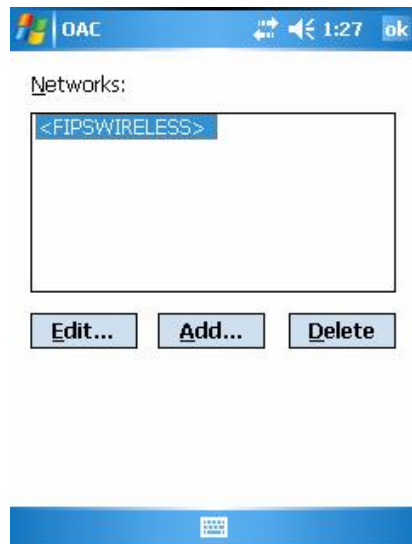
If however OAC does try to connect just uncheck the 'Connect to:' check box.



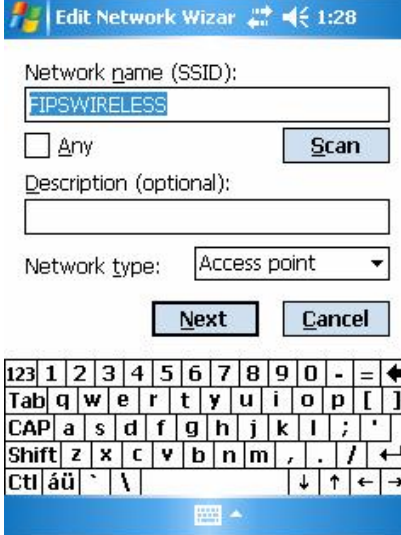
Once OAC Manager UI is launched - tap on
Settings
Networks



Highlight on the network <FIPSWIRELESS>
Edit



Change the SSID name from FIPSWIRELESS to your SSID (case sensitive)



Edit Network Wizard 1:28

Network name (SSID):
FIPSWIRELESS

Any Scan

Description (optional):
[Empty field]

Network type: Access point

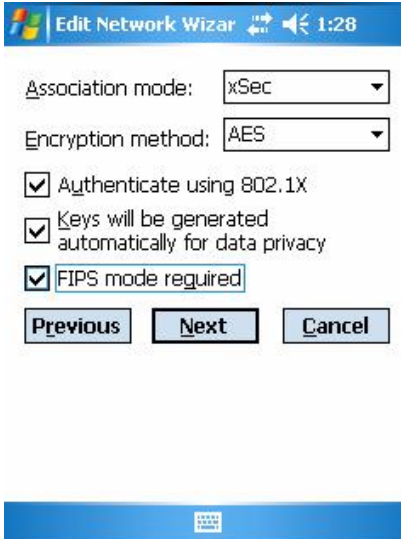
Next Cancel

123 1 2 3 4 5 6 7 8 9 0 - = < >
Tab q w e r t y u i o p []
CAP a s d f g h j k l ; ' < >
Shift z x c v b n m , . / < >
Ctl áú ` \ [] < >

Next

Ensure Association mode is xSec and all three check boxes are checked.

- Authenticate using 802.1X
- Key s will be generated automatically for data privacy
- FIPS mode is required



Edit Network Wizard 1:28

Association mode: xSec

Encryption method: AES

Authenticate using 802.1X

Keys will be generated automatically for data privacy

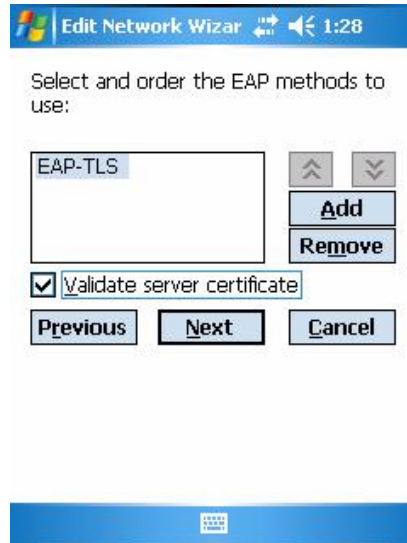
FIPS mode required

Previous Next Cancel

[Keyboard icon]

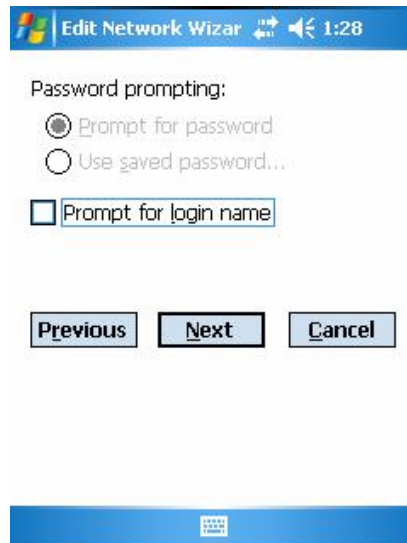
Next

If the RADIUS Root CA is not yet loaded on the terminal, uncheck 'Validate server certificate'. Later when the correct CA certificate for the RADIUS server is added to the terminal, remember to return to this panel and check 'Validate server certificate'.



Next

'Prompt for login name' should be unchecked

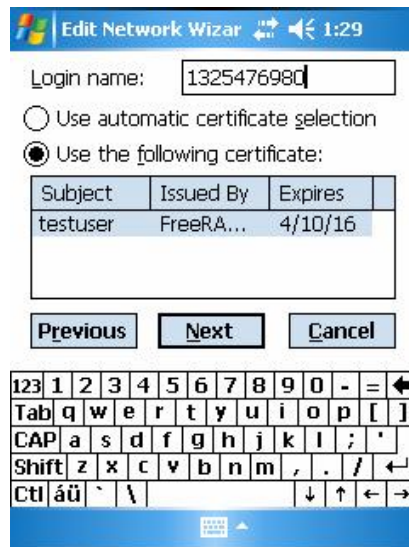


Next

Your EDIPI should be in the Login Name: and your authentication certificate highlighted. The email signing certificate is the authentication certificate for 802.1X not the ID certificate. The login name and certificate choice are automatically configured by Apriva SensaGuard when the terminal is unlocked.

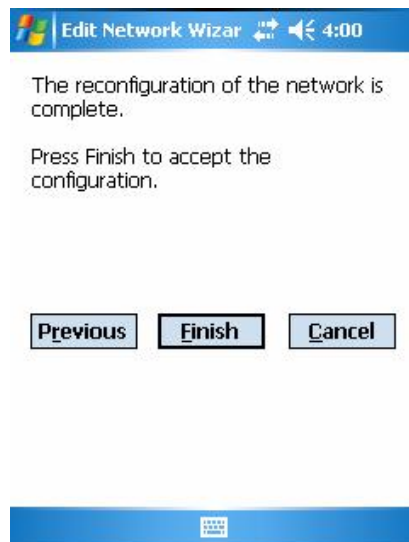
'Use the following certificate:' should be selected.

Do not select 'Use automatic certificate selection.'



Next

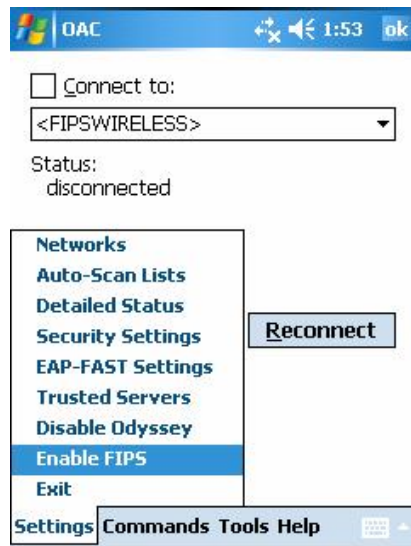
Finish



ok



Enable FIPS Mode by tapping
Settings
Enable FIPS



OAC will unbind from the Wi-Fi radio and rebind to it to clear possible cached settings.

Use the drop down menu to select your SSID
Check 'Connect to'



OAC status will change during the authentication process and a successful authentication will have a Status: 'open and authenticated'.



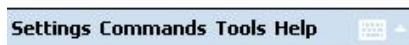
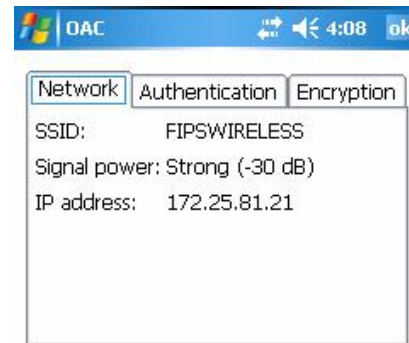
OAC status messages will typically proceed in this order:

- 'disconnected'
- 'searching for access point'
- 'authenticating'
- 'waiting on keys' (usually not seen)
- 'open and authenticated'

If you see the following messages and these messages never change, then go to the trouble shooting section.

- 'locating adapter'
- 'waiting on authentication'
- 'requesting authentication'

Once OAC is 'open and authenticated', you might want to see if the terminal received an IP Address. Tap on 'Details'. The Network tab will display the IP Address. If an IP Address is not displayed or if a Microsoft 169 IP address is displayed, contact your network administrator to ensure the DHCP server is receiving DHCP requests from the Intermec terminal.



Troubleshooting Section

When OAC is showing the following status messages continually, try the suggested trouble shooting steps.

'locating adapter'

If the OAC status continues to state 'locating adapter' after OAC launches and never changes to 'disconnected' or 'searching for access point', OAC is complaining that it can not bind to the Wi-Fi adapter.

1. If the terminal is in the cradle and the USB is connected to a PC for ActiveSync, detach the USB cable. The Intermec terminal turns off the Wi-Fi radio when ActiveSync is active.
2. Ensure that the Intermec 'Assured Radio Deactivation' is disabled as described above.

'waiting on authentication'

1. Ensure the RADIUS Server Root CA is installed on the terminal.
2. Ensure that both Intermediate and Root CA certificates for the user authentication certificate are installed on the terminal or installed on the RADIUS Server.
3. If you changed FIPS Mode between enabled - disabled, you might try exiting OAC and re-launching OAC.
4. EAP type mismatch between OAC and RADIUS. Make sure both OAC and RADIUS are using EAP-TLS.

'requesting authentication'

Requesting Authentication is an indicator that the RADIUS Client is not communicating properly with the RADIUS Server. The RADIUS Client is the Aruba Controller. Here are some likely causes:

1. RADIUS Server is not online.
2. The Aruba Controller does not have the correct IP Address of the RADIUS Server.
3. The RADIUS Server is not configured with the correct IP Address of the Aruba Controller.
4. The Aruba Controller does not have the correct shared secret.