“Microsoft Direct Push” and the O2 Stellar and O2 Serra

IT Services recommend disabling “Microsoft Direct Push” on the O2 Stellar. “Microsoft Direct Push” is on by default but requires an active data connection. On campus this is fine as it will use the wireless connection where available but as soon as it is outside of the wireless range it will connect using GPRS.

Data downloaded using “Microsoft Direct Push” over the PGRS connection could easily take you over your data limit and you would then be charged by O2 for data transferred above your monthly limit. The charge for data downloads is higher when outside the UK and so, if you are planning to take your device outside of the UK, we would strongly advise that you contact Procurement and O2 about other available tariffs.

Disabling “Microsoft Direct Push”
1. Click on the Windows icon and select Settings
2. Click on the Connections tab
3. Select Comm Manager
4. If “Microsoft Direct Push” is enabled it will appear as a green button (indicated below) click on it to turn it off

Stellar

Serra
Using Eduroam on the O2 Stellar

Eduroam is a secure wireless network but does not work with Microsoft Windows Mobile 6.0 as supplied on the O2 Stellar. A free third party piece of software “SecureW2” can be downloaded and used to connect the Stellar to Eduroam. This is available at:

http://www.securew2.com/resources/SecureW2_EAP_Suite_106_CE.zip

Once downloaded you need to open the folder and install the application using the Windows PC that you connect your device to and follow the on screen instructions. This will install it and sync it will your O2 Stellar.

To configure the O2 Stellar for Eduroam:

1. Click on the Windows icon and select Settings
2. Click on the Connections tab
3. Select Comm Manager
4. Turn on the wireless if it is switched off

5. Close the window
6. Click on the Windows icon then Settings and select the Connections tab
7. Scroll down and click on Wi-Fi
8. Select Add New ...
9. In the Network name: box enter eduroam; now select Next
10. In the Authentication: box select WPA2 and in the Data Encryption: box select AES; now select Next
11. In the EAP type: box, select SecureW2 TTLS, then select Properties
12. Next select Configure
13. On the Connection tab set:

![Connection Tab](image1)

14. On the Certificates table select Add CA and then scroll through the list and select GTE CyberTrust Global Root then click on the [Add CA] button

![Certificates Tab](image2)

15. On the Authentication tab: in the Select Authentication Method: box, select PAP
16. On the User Account tab: in the Select Authentication Method: box, tick the box Prompt user for credentials
17. Select OK, then select OK again followed by Finish