

Walled garden for onboarding user devices to eduroam

This document is intended for the system administrators at member organisations and describes an implementation of a 'walled garden' network service that only gives access to setup tools to enable user devices to be correctly configured to run eduroam securely. The setup tools are the configuration installers produced using the eduroam CAT system, so administrators adopting this deployment will also need to learn how to use that. (See the associated document posted in this eduroam Group area - introduction to using the eduroam(UK) Support site together with an introduction to the eduroam Configuration Assistant Tool and a guide to getting started with the eduroam CAT site.)

<https://support.eduroam.uk/files/Walled%20garden%20for%20onboarding%20user%20devices%20to%20eduroam>
[1]

eduroam CAT is publicly accessible. To enable its use behind captive portals (e.g. on a 'setup' SSID which only allows access to CAT for device configuration), the following hostnames need to be allowed for port TCP/443 in the portal:

REQUIRED

- cat.eduroam.org (the service itself)
- list, of, CRL, pointers (the CRL Distribution Points for the site certificate), also TCP/80
- list, of, OCSP, pointers (the OCSP Responder for the site certificate), also TCP/80
- android.l.google.com (Google Play access for Android App)
- android.clients.google.com (Google Play access for Android App)
- play.google.com (Google Play access for Android App)
- ggphd.com (Google Play access for Android App)

RECOMMENDED for full Google Play functionality (otherwise, Play Store will look broken to users and/or some non-vital functionality will not be available)

- photos-ugc.l.google.com
- googleusercontent.com
- ajax.googleapis.com
- play.googleapis.com
- googleapis.l.google.com
- apis.google.com
- gstatic.com
- www.google-analytics.com [2]
- wallet.google.com
- plus.google.com
- checkout.google.com
- *.gvt1.com

AND particularly to support geteduroam:

- 19-courier.push.apple.com
- 21-courier.push.apple.com
- 44-courier.push.apple.com
- api.smoot.apple.com
- bag.itunes.apple.com
- buy.itunes.apple.com
- captive.apple.com
- cat.eduroam.org
- cf.iadsdk.apple.com
- cl2.apple.com
- cl3.apple.com
- cl4.apple.com
- cl5.apple.com
- configuration.apple.com
- configuration.ls.apple.com
- crt.sectigo.com
- crt.usertrust.com
- d5ymw72datw3x.cloudfront.net
- discovery.eduroam.app
- e10499.dsce9.akamaiedge.net
- e17437.dscb.akamaiedge.net
- e4478.a.akamaiedge.net
- e673.dsce9.akamaiedge.net
- e6858.dscx.akamaiedge.net
- gateway.fe.apple-dns.net
- gateway.icloud.com
- geant.ocsp.sectigo.com
- gs-loc.apple.com
- gsp10-ssl.apple.com
- gsp64-ssl.ls.apple.com
- gsp85-ssl.ls.apple.com
- gspe1-ssl.ls.apple.com
- gspe21-ssl.ls.apple.com
- gspe35-ssl.ls.apple.com
- gsp-ssl.ls.apple.com
- identity.ess.apple.com
- init.ess.apple.com
- init.itunes.apple.com
- init-p01md.apple.com
- init.push.apple.com
- iphone-ld.apple.com
- keyvalueservice.fe.apple-dns.net
- keyvalueservice.icloud.com
- lcdn-locator.apple.com
- mesu.apple.com
- ocsp.apple.com
- ocsp.digicert.com

- ocsf-lb.apple.com.akadns.net
- ocsf.pki.goog
- ocsf.sectigo.com
- ocsf.usertrust.com
- p29-fmip.icloud.com
- p29-keyvalueservice.icloud.com
- partiality.itunes.apple.com
- pd.itunes.apple.com
- play.itunes.apple.com
- safebrowsing.googleapis.com
- setup.icloud.com
- s.mzstatic.com
- static.ess.apple.com
- su.itunes.apple.com
- time-ios.apple.com
- updates.cdn-apple.com
- www.apple.com [3]
- www-cdn.icloud.com.akadns.net
- www.icloud.com [4]
- xp.apple.com
- xp.itunes-apple.com.akadns.net

Source URL: <https://community.jisc.ac.uk/library/network-and-technology-service-docs/walled-garden-onboarding-user-devices-eduroam>

Links

- [1] <https://support.eduroam.uk/files/Walled%20garden%20for%20onboarding%20user%20devices%20to%20eduroam.p>
- [2] <http://www.google-analytics.com>
- [3] <http://www.apple.com>
- [4] <http://www.icloud.com>