How to support to end users

Introduction

This information is meant for eduroam Identity Providers (IdPs) and assumes familiarity with eduroam in general and a working IdP RADIUS server. For general information about both topics, please visit the eduroam in a nutshell and eduroam on-site page; in particular the chapter "eduroam IdP".

Helpdesk Principles

As an eduroam Identity Provider, you are the first point of contact for your end users, regardless whether they are using eduroam at your own campus or whether they are roaming nationally or internationally with an account issued by you.

It is your duty to inform your users about the applicable Terms of Use / Acceptable Use Policy (AUP) when connecting to an eduroam network (both your own AUP and that of the visited hotspot apply).

You are also responsible for providing enough technical information so that users can set up their device securely.

Parameters for Secure Device Configuration

The security of your end-users' credentials (which often means: their institutional username and password) depends on the question whether they verify that they are revealing their password only to their own IdP's RADIUS server or whether they tell it to any random other server. Failure to verify the identity of the RADIUS server means that anyone can set up a fake RADIUS server, wait until your users connect to it, and log the passwords they used for this login.

eduroam Operations sometimes observes practices of eduroam IdPs who actively instruct their users to turn off server identity validation for "ease of use" sake. Such practices include "Uncheck the 'Verify Server Certificate' checkbox" or "when you are shown a certificate warning, just click Accept". We would like to note that such behaviour of IdPs is a breach of the eduroam policy; the instructions MUST include the proper verification of the server identity. In practice, this means:

The security-related public details of your RADIUS infrastructure must be readily available to to end users, including at least:

- the Certification Authority (CA) that issued the EAP Server Certificate of your RADIUS Installation
- the Common Name (CN) of the server certificate of the EAP Server Certificate of your RADIUS Installation (this detail is mandatory in most cases; it is optional *ONLY* if the Certification Authority *exclusively* issues server certificates to your own eduroam EAP servers)
- the EAP type(s) you support
- information regarding which credential users need to use when logging in

Using eduroam CAT for popular operating system support

For many common operating systems, the above information can be configured automatically on your end user devices; either by pushing a configuration file to the device, or by executing a configuration program which installs certificates and makes all required settings on the device.

eduroam Operations has created a tool which allows you to upload the information above, and in return generates custom installers for your IdP, for immediate consumption by your end users. The tool is called the "eduroam Configuration Assistant Tool" (eduroam CAT website; IdP Administrator manual). For the operating systems supported by CAT, helpdesk instructions can be limited to "go to this website, use the installer". Please see the section on compatible devices further down on this page.

Manual configuration instructions for other operating systems

For other operating systems, you need to create installation instructions (screenshots, click-through videos, ...) yourself. Be aware though that the security model of eduroam depends heavily on the validation of the EAP server certificate; due to that, your end-user instructions for all devices MUST include

- the installation of the CA certificate of your EAP server certificate
- the configuration of the name (CN) of the EAP server certificate (verification of this detail can be omitted *ONLY* if the Certification Authority *exclusively* issues server certificates to your own eduroam EAP servers)
- the EAP type to use

⚠️ We understand that there is a temptation to use some devices with half-baked support for IEEE 802.1X and EAP, where half-baked means they either don't support server certificate validation at all or only in a suboptimal way (e.g. only CA check, no server name validation; or only validation of a certificate fingerprint without certificate chain check). Due to its popularity, we explicitly name Android at this point - it does not allow to configure the expected server name. You may want to support such devices as best as you can, but be aware that you may be putting your own users and their credentials at risk when doing so. In Android's case, a secure configuration is only possible if you deploy a private CA which issues server certificates exclusively to your own eduroam EAP servers.

In the compatibility matrix, devices with known deficiencies are marked as such.

You can also comment on this page if you have found a nifty way to ease eduroam configuration on devices not currently supported by CAT.

Devices that are compatible with eduroam

The following list is sorted alphabetically by vendors. The table notes which EAP methods are supported. Legend:

CAT - this device/EAP type combination is supported by eduroam CAT; can probably also be configured securely manually

Yes - the device can be configured securely manually for this EAP type

Deficient - the device lacks important security features, but workarounds exist which can make its use safe

Insecure - the device can be configured manually for this EAP type, but not all security parameters can be set up

No - device is known not to support IEEE 802.1X/EAP

? - Unknown

TPS - supported with Third-Party Software (possibly commercial)

Compatibility Matrix

Device/OS Vendor	Device/OS	Version	TTLS-PAP	PEAP	TTLS-MSCHAPv2	TLS	PWD	TTLS-GTC	FAST
Android	tested on: Samsung Galaxy S2 Huawei Sonic u8650	2.3	Deficient[1]	Deficient[1]	Deficient[1]	Deficient[1]	?	Deficient[1]	?
Android	tested on: Motorola Xoom2	4.0+	Deficient[1]	Deficient[1]	Deficient[1]	Deficient[1]	?	Deficient[1]	?
Apple	iPhone	iOS 4.0+	CAT	CAT	CAT	Yes	No	Yes	Yes
Apple	iPad	iOS 4.0+	CAT	CAT	CAT	Yes	No	Yes	Yes
Apple	iPod touch	iOS 4.0+	CAT	CAT	CAT	Yes	No	Yes	Yes
Apple	Mac OS X	10.7+	CAT	CAT	CAT	Yes	No	?	Yes
Apple	Mac OS X	10.4-10.6	Yes[4]	Yes[4]	Yes[4]	Yes[4]	No	?	Yes[4]
Blackberry	Playbook OS	2	Yes	?	?	?	?	?	?
Linux	NetworkManager		CAT	CAT	CAT	CAT	No	?	?
Linux	wpa_supplicant		CAT	CAT	CAT	CAT	Yes[2]	Yes	Yes
Microsoft	Windows	XP SP3	TPS	Yes	TPS	Yes	No	TPS	TPS
Microsoft	Windows	Vista	TPS	CAT	TPS	CAT	CAT	TPS	TPS
Microsoft	Windows	7	TPS	CAT	TPS	CAT	CAT	TPS	TPS
Microsoft	Windows	8 / 8.1	CAT	CAT	CAT	CAT	CAT	?	?
Microsoft	Windows	10	CAT	CAT	CAT	CAT	CAT	?	?
Microsoft	Windows Phone	7.x	No	Insecure[3]	?	No	?	?	?
Microsoft	Windows Phone	8.x	No	Deficient[1]	?	?	?	?	?
Microsoft	Xbox	all	No	No	No	No	No	No	No
Microsoft	XBoxONE	all	No	No	No	No	No	No	No
Nokia	Symbian OS	Series 6	No	Yes	?	Yes	?	Yes	No
Nokia	Symbian OS	9.x	Yes	Yes	?	Yes	?	Yes	No
Sony	Playstation3 (PS3)	all	No	No	No	No	No	No	No
Sony	Playstation4 (PS4)	all	No	No	No	No	No	No	No
Jolla	Sailfish OS	2	Yes	Yes	Yes	Yes	?	?	?

[1] Installation and pinpointing of CA possible; verification of expected server name (CN) not possible. A secure configuration is only possible if the Identity Provider deploys a private CA which issues exclusively server certificates for his own eduroam EAP servers. All other Identity Provider deployments are INSECURE.

[2] Version 1.0 or higher required

[3] Verifying that the server is signed by the proper CA is not possible; this means users will not be able to detect fake hotspots and might send their username/password to an unauthorised third party.

[4] Only with 10.6.x (Snow Leopard) and later does OSX allow the configuration of of CA/server trust settings (Pinning 802.1X to specific CA and RADIUS server CommonName)

Reporting a new device

Please let us know in the "Comments" field what device you have, and what EAP method(s) you have found working. We will update the list periodically.