eduroam CAT - admin improvements and testing RADIUS infrastructure

Tomasz Wolniewicz
Maja Górecka-Wolniewicz
Poznan supercomputing and networking center

Mobility Day – TNC24, Rennes, 10.06.2024

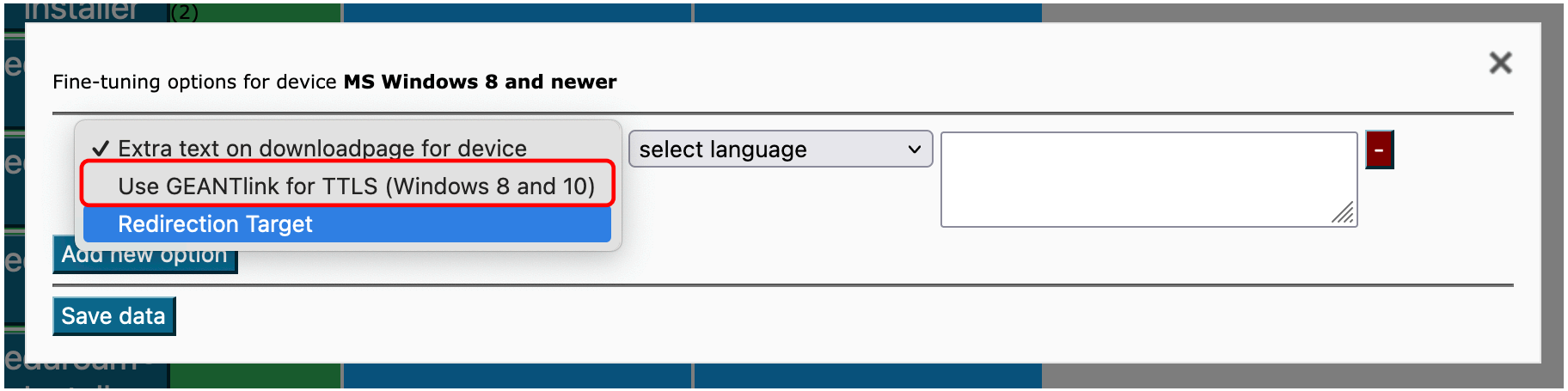
Public

www.geant.org

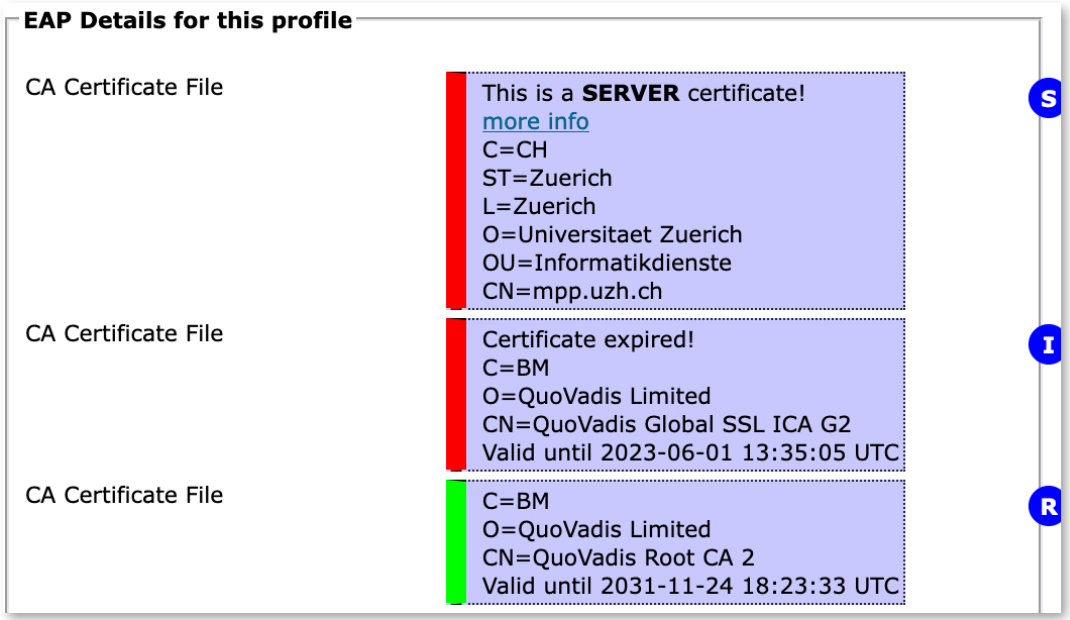
CAT release 2.1.2

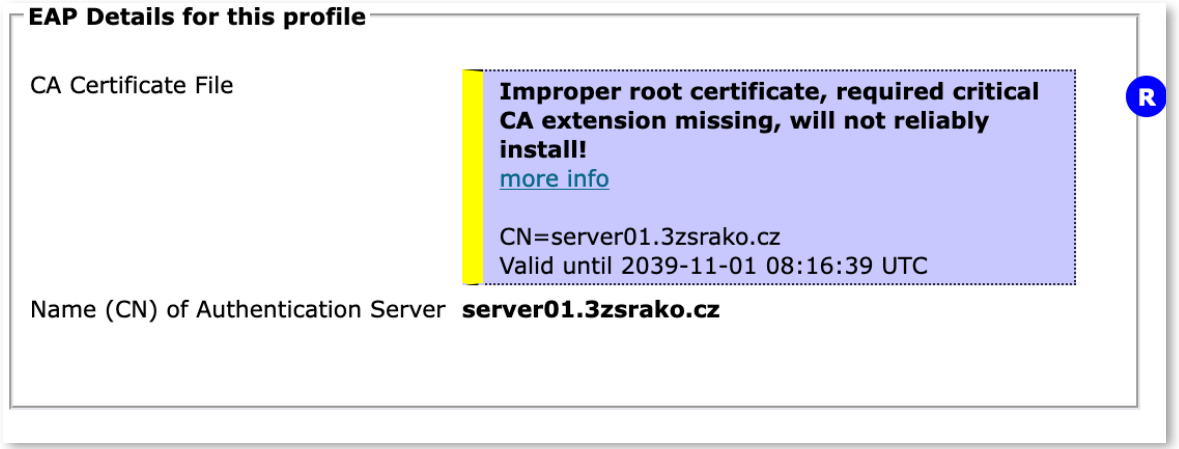
- support for device-specific options displayed only for devices they belong to
- warnings about certificate expiry and certificates without CA extensions to the profile management interface, block adding bad certificates to the system
- read-only mode for NRO admins and superadmins; enhancement of the NRO management page, in particular icons showing status, certificate validity problems and OpenRoaming readiness
- new script to be used to test the OpenRoaming readiness of IdPs
- per-idp statistics to the API calls STATISTICS-FED
- FLAG-NO-LOGO flag for DATADUMP-FED to eliminate logos from the dump
- replace Quetto icons with the Tabler ones
- new SUPPORT role with read-only access to IdP settings
- a rewrite of dynamic connectivity tests
- extensions to the eduPKI server certificates interface to display detailed information about certificates to be issued
- multiple improvements to the code, in particular eliminating the deprecated FILTER_SANITIZE_STRING usage
- optional local cache of the external (eduroam) database
- replaced slow SQL queries in Managed IdP area with much faster ones
- fixed blocking of Ajax requests caused by php sessions
- new language - Welsh

Device-specific options



Server certificates and missing CA extensions





Blocking bad certificates

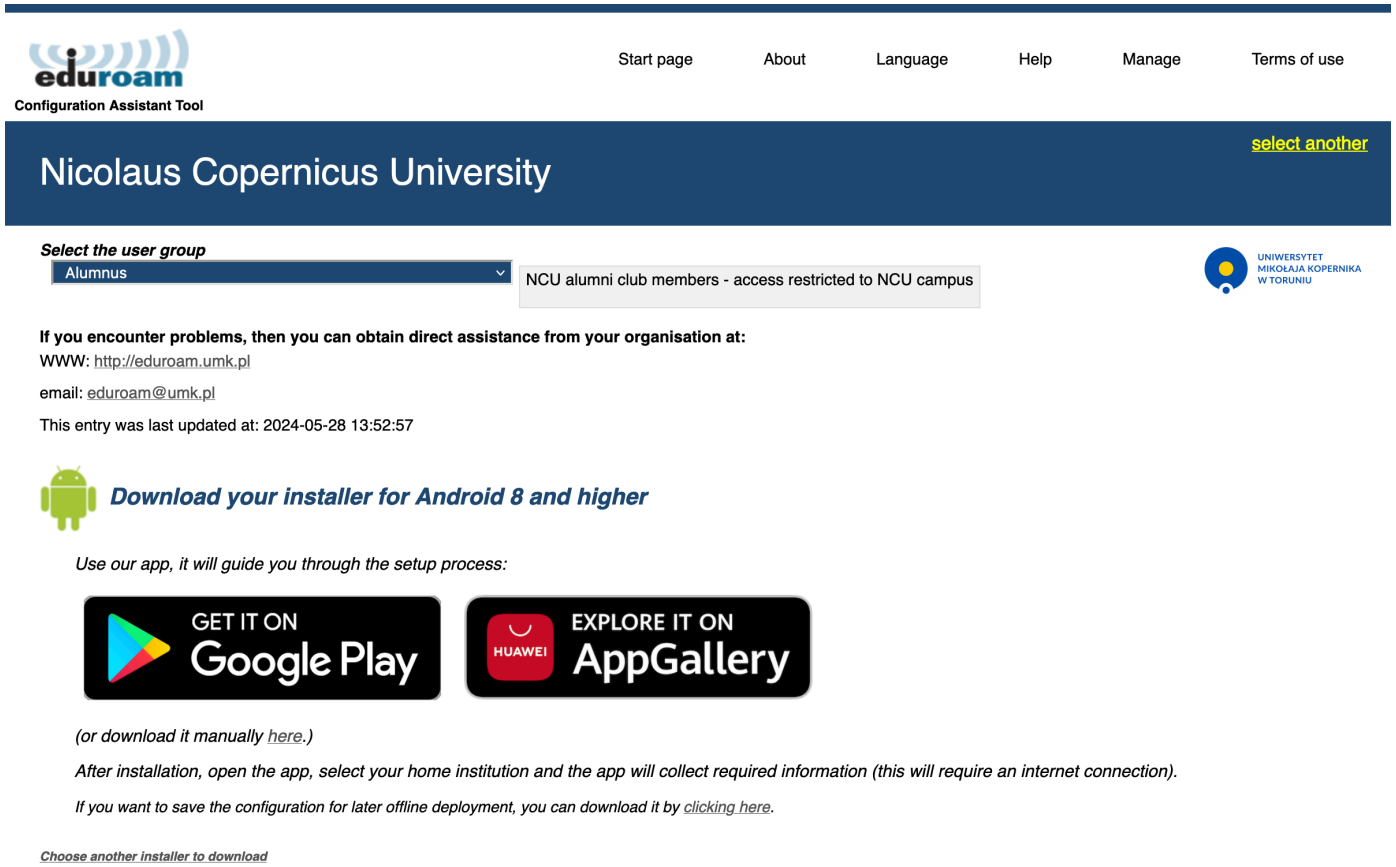
- ✓ 1x CA Certificate File
- ✓ 2x Name (CN) of Authentication Server
- ✗ CA Certificate File - eduroam.ucn.ca - missing required CA extensions (more info)
- ✓ Redirection is **OFF**
- ✓ Supported EAP Type: **PEAP-MSCHAPv2**
- ✓ Supported EAP Type: **TTLS-MSCHAPv2**
- ✓ Supported EAP Type: **TTLS-PAP**

- ✓ 1x CA Certificate File
- ✓ 2x Name (CN) of Authentication Server
- ✗ CA Certificate File - radius.ijp.pan.pl - server certificate (more info)
- ✓ Redirection is **OFF**
- ✓ Supported EAP Type: **PEAP-MSCHAPv2**
- ✓ Supported EAP Type: **TTLS-MSCHAPv2**
- ✓ Supported EAP Type: **TTLS-PAP**

Admin API extensions

- Introduced flags as possible names for PARAMETERS with admissible values of TRUE or FALSE (currently just one flag exists)
- Action DATADUMP-FED
  - New flag FLAG-NO-LOGO
    - Removes logos from the federation dump to make it smaller and easier to handle
- Action STATISTICS-FED (request by Stefan Paetow)
  - New attribute ATTRIB-DETAIL
    - Possible values: FEDERATION, ORGANISATIONS, PROFILES
    - Adds download statistics of appropriate detail

The geteduroam download page

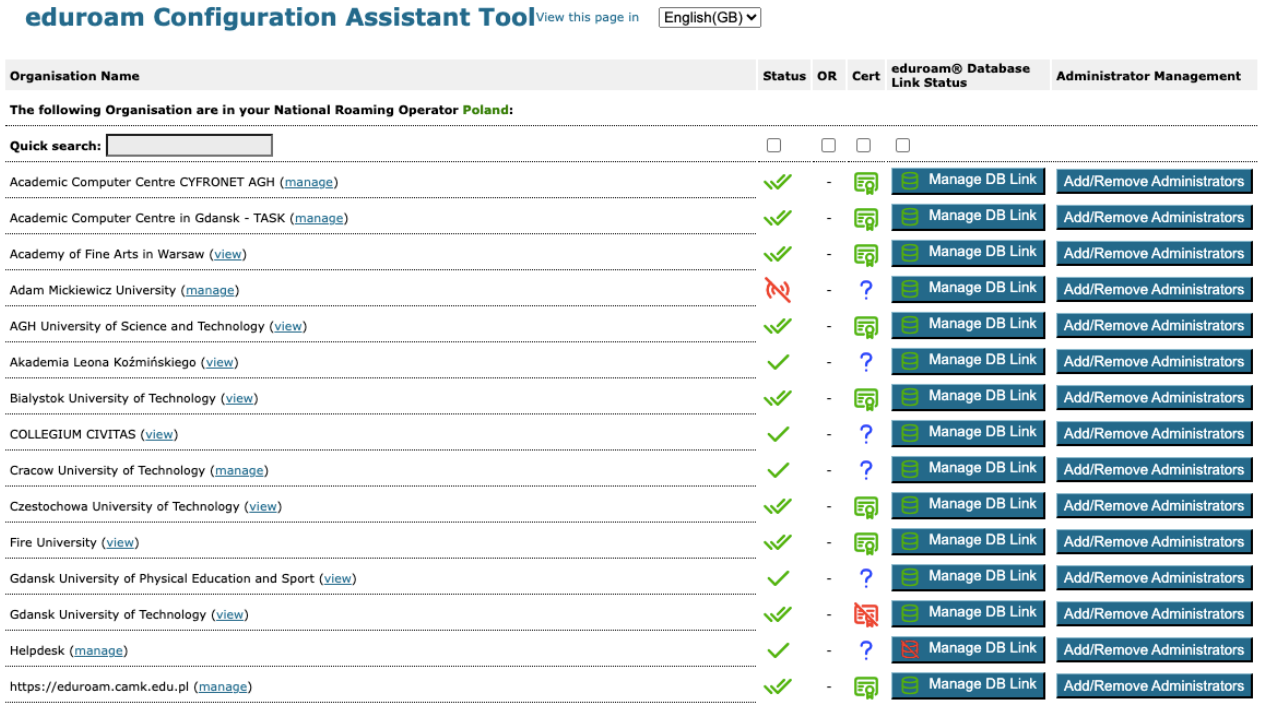


New geteduroam download pages in CAT

- Only 24 profiles (23 institutions) are production-ready with geteduroam option set correctly and no redirection

Profile	Organisation	Fed
QMUL eduroam	Queen Mary University of London	UK
eduroam@wcg	Warwickshire College Group	UK
eduroam TEST profile	HEAnet CLG	IE
Eduroam	University of Franche-Comte	FR
University of Warwick	University of Warwick	UK
No Intermediate	CAT Training Organization	CA
personnels ou prestataires	GIP RENATER	FR
Eduroam-AD(staff)	University of Foggia	IT
Older username/password method - Staff and Students	Birmingham Newman University	UK
MPIPKS eduroam + pks-members	Max Planck Institute for the Physics of Complex Systems MPIPKS	DE
Bilborough College	BFmat	UK
Gateway College	BFmat	UK
SMUCB Eduroam	St Mary's University College, Belfast	UK
eduroam	Karadeniz Technical University	TR
USask - eduroam	University of Saskatchewan	CA
Pravni fakultet u Kragujevcu	Faculty of Law, University of Kragujevac	RS
	CISIA - Consorzio Interuniversitario Sistemi Integrati per l'Accesso	IT
All Groups	Queen's University at Kingston	CA
Met Office (2024)	Met Office	UK
Havforskningsinstituttet	Havforskningsinstituttet	NO
eduroam	Deutsches Zentrum fuer Luft- und Raumfahrt e. V.	DE
	TUBITAK ULAKBIM	TR
eVA.eduroam.ca	eduroam Visitor Access Canada	CA
	Gaziantep University	TR

The NRO page functionality



- Quick name/realm filter
- Checkbox filters
  - bad/incomplete configuration
  - OpenRoaming settings
  - Expiring/expired certificates
- If multiple federations are managed, filters act separately on each
- Ability to view all federations for superadmin and support
- Quick demo

eduroam Configuration Assistant Tool

View this page in English(GB)

National Roaming Operator Overview

Your Personal Information

E-Mail Address	**twoln@umk.pl**
Real Name	**Tomasz Wolniewicz**
National Roaming Operator Administrator	**PL**
Unique Identifier	click to display

Select a different federation

United Kingdom

National Roaming Operator Properties: United Kingdom

Country		**United Kingdom**
OpenRoaming: Allow Organisation Opt-In		**on**
National Roaming Operator Name	default/other languages	**Jisc**
National Roaming Operator Homepage	default/other languages	**https://www.jisc.ac.uk/eduroam**

View ...

National Roaming Operator Statistics: United Kingdom

IdPs Total	Public Download
374	332

Show downloads

Diagnose reachability and connection parameters of any eduroam® Identity Provider Go!

Organisation Name	Status	OR	Cert	eduroam® Database Link Status	Administrator Management
The following Organisation are in your National Roaming Operator United Kingdom:					
Quick search:					
Aberystwyth University (view)		-		Manage DB Link	Add/Remove Administrators
Activate Learning (view)		-		Manage DB Link	Add/Remove Administrators
Advance HE (view)		-		Manage DB Link	Add/Remove Administrators
AECC University College (view)		-		Manage DB Link	Add/Remove Administrators
Al-Maktoum College of Higher Education (view)		-		Manage DB Link	Add/Remove Administrators

National Roaming Operator Overview

Your Personal Information

E-Mail Address	**twoln@umk.pl**
Real Name	**Tomasz Wolniewicz**
National Roaming Operator Administrator	**PL**
Unique Identifier	click to display

Select a different federation

United Kingdom

National Roaming Operator Properties: United Kingdom

Country		**United Kingdom**
OpenRoaming: Allow Organisation Opt-In		**on**
National Roaming Operator Name	default/other languages	**Jisc**
National Roaming Operator Homepage	default/other languages	**https://www.jisc.ac.uk/eduroam**

View ...

National Roaming Operator Statistics: United Kingdom

IdPs Total	**Public Download**
374	332

Downloads	**Admin**	**Managed IdP**	**User**
MS Windows 8 and newer	658	0	1012679
Linux	208	0	87949
MS Windows 7	374	0	150889
MS Windows 8	43	0	38332
Android 8.0 Oreo	25	0	134275
Apple OS X El Capitan	48	0	18563
Apple OS X Yosemite	35	0	12938
Apple OS X Mavericks	74	0	12557
Chrome OS	98	0	110790
Android 8 and higher	104	0	278622
Apple device	94	0	1383261
EAP config	7	0	2478
Android 6.0 Marshmallow	37	0	140608
Android 4.4 KitKat	54	0	533543
Android 7.0 Nougat	42	0	78536
Apple macOS Sierra	28	0	26363
Apple OS X Lion	105	0	6052
Test	34	0	349
(discontinued) xp	3	0	1368
(discontinued) welcomeletter	0	0	0

eduroam Configuration Assistant Tool

View this page in English(GB)

Diagnose reachability and connection parameters of any eduroam® Identity Provider Go!

Organisation Name	Status	OR	Cert	eduroam® Database Link Status	Administrator Management
The following Organisation are in your National Roaming Operator United Kingdom:					
Quick search:	☐	☐	☐	☐	
Aberystwyth University (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Activate Learning (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Advance HE (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
AECC University College (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Al-Maktoum College of Higher Education (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Anglia Ruskin University (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Angus Council (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Armagh Observatory & Planetarium (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Arts University Bournemouth (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Arts University Plymouth (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Aston University (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Ayrshire College (view)	✗	-	?	Manage DB Link	Add/Remove Administrators
Babraham Institute (view)	✓✓	-		Manage DB Link	Add/Remove Administrators

The following Organisation are in your National Roaming Operator United Kingdom:

Quick search: camb					
Cambridge Assessment (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Cambridge Education Group (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Cambridge Regional College (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Coleg Cambria (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
University of Cambridge (view)	✓✓	-		Manage DB Link	Add/Remove Administrators

The following Organisation are in your National Roaming Operator United Kingdom:

Quick search:	☑	☐	☐	☐		
Ayrshire College (view)	✗	-	?	Manage DB Link	Add/Remove Administrators
Belfast Health and Social Care Trust (view)	✓	-	?	Manage DB Link	Add/Remove Administrators
BioSS (view)	✓	!	?	Manage DB Link	Add/Remove Administrators
Birkenhead Sixth Form College (view)	✗	-	?	Manage DB Link	Add/Remove Administrators
Birmingham Metropolitan College (view)	✓	-	?	Manage DB Link	Add/Remove Administrators
Bolton College (view)	✓	-	?	Manage DB Link	Add/Remove Administrators
Bridgwater and Taunton College (view)	✗	-	?	Manage DB Link	Add/Remove Administrators
Brunel University (view)	✗	-	?	Manage DB Link	Add/Remove Administrators
City of Wolverhampton College (view)	✓	-	?	Manage DB Link	Add/Remove Administrators
Graduate Prospects (view)	✓	-	?	Manage DB Link	Add/Remove Administrators
Hull York Medical School (view)	✓	-	?	Manage DB Link	Add/Remove Administrators
IAAPS Limited (view)	✗	-	?	Manage DB Link	Add/Remove Administrators
Itchen College (view)	✗	-	?	Manage DB Link	Add/Remove Administrators
Jisc Regional Support Centre Wales (view)	✓	-	?	Manage DB Link	Add/Remove Administrators
Kingston University (view)	✗	-	?	Manage DB Link	Add/Remove Administrators
Leeds Beckett University (view)	✗	-	?	Manage DB Link	Add/Remove Administrators

Organisation Name	Status	OR	Cert	eduroam® Database Link Status	Administrator Management
The following Organisation are in your National Roaming Operator United Kingdom:					
Quick search:	☐	☑	☐	☐	
BioSS (view)	✓	!	?	Manage DB Link	Add/Remove Administrators
Camford University (eduroam UK) (view)	✓✓	i		Manage DB Link	Add/Remove Administrators
Loughborough College (view)	✓✓	!		Manage DB Link	Add/Remove Administrators
Oxford Centre for Islamic Studies (view)	✓✓	i		Manage DB Link	Add/Remove Administrators
Royal College of Music (view)		!	?	Manage DB Link	Add/Remove Administrators
Training 2000 (view)	✓✓	!		Manage DB Link	Add/Remove Administrators

Organisation Name	Status	OR	Cert	eduroam® Database Link Status	Administrator Management
The following Organisation are in your National Roaming Operator United Kingdom:					
Quick search:	☐	☐	☑	☐	
Arts University Bournemouth (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Barnfield College (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Bath College (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Cardiff & Vale College (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Cardiff Metropolitan University (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Carshalton College (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Coventry University (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Dudley College of Technology (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
EIS - Kent Learning Zone (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Epping Forest College (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Forth Valley College of Further and Higher Education (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Goldsmiths, University of London (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Harper Adams University (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Henley College Coventry (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
Janet (view)	✓✓	-		Manage DB Link	Add/Remove Administrators
London Research Institute (view)	✓✓	-		Manage DB Link	Add/Remove Administrators

Some OpenRoaming statistics from CAT

- 11 federations allowing OpenRoaming for their IdPs

How many institutions are using this?

Some OpenRoaming statistics from CAT

- Only 8 profiles are production-ready with OpenRomaing set and no redirection and they come from 5 institutions

Profile	Institution	Fed
OpenRoaming TEST Profile	HEAnet CLG	IE
Eduroam para Colaboradores FCCN	FCCN - Unidade da FCT I.P.	PT
student	Perdana University	MY
visitor	Perdana University	MY
staff	Perdana University	MY
eduroam plus edu RCOI	Camford University (eduroam UK)	UK
Personnel ESIEA	ESIEA - École supérieure d'informatique électronique automatique	FR
Etudiants ESIEA	ESIEA - École supérieure d'informatique électronique automatique	FR

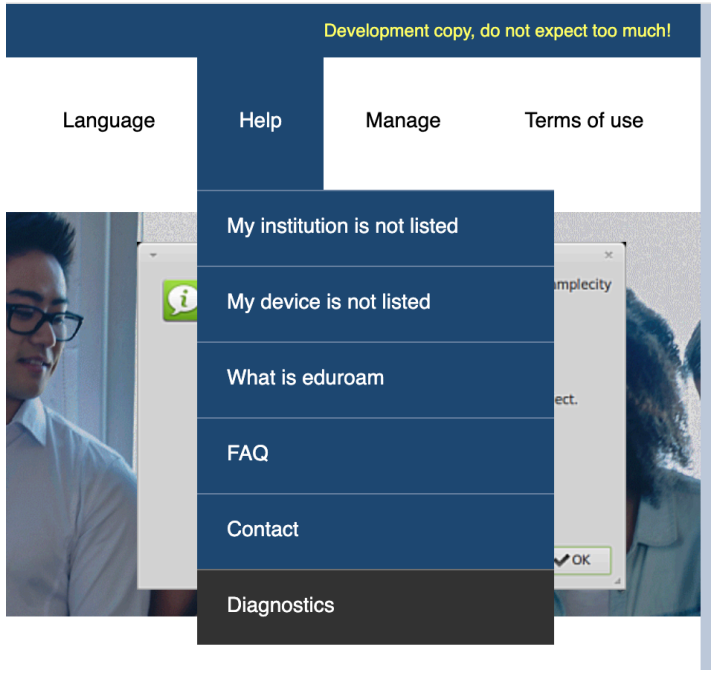
Reachability / Diagnostics tests

- **Organisation Overview** page for each defined profile when a profile realm is set

  button 

  to conduct a test for a given realm

- Diagnostic tests are also available from Help menu
  - tests for end-user
  - tests for eduroam administrator
- Realm check tests in both places are executed almost in the same way
  - tests are done in parallel
  - UDP reachability – via eapol_test
  - additional tests when realm is declared as dynamic, i.e. having NAPTR, SRV records or openroaming – via openssl
  - “check realm reachability” test of profile prepared for an institution includes such settings as outer identity and verifies server certificate using CA certificate indicated in this profile



Dynamic connectivity tests

- Include
  - getting information on all dynamic hosts
  - verifying CA certificate (as an eduPKI certificate with correctly set policies)
  - checking communication with each host using different client certificates: correct, expired, revoked, with wrong policies setting, issued by not accredited CA
- Openssl command
  - used from the very beginning for tests
  - after switching to Ubuntu 22 and openssl 3 some issues appeared
  - openssl does not give a precise return code and never done that before – the command output has to be analysed
  - messages on stdout / stderr mixed and some buffering problems to catch full output when stderr outputs last line (problem seen when openssl is executed in batch and PHP code)
  - running openssl with sites having TLSv1.3 enabled is very problematic – it happens that information on errors disappears
  - we decided to avoid using TLSv1.3 for running tests
    - for now all servers with enabled TLSv1.3 have TLSv1.2 enabled as well

Connectivity tests

- Sslscan command as an alternative
  - reports the protocol versions, cipher suites, key exchanges etc.
  - has a possibility to connect with a client certificate but it does not work as expected in my tests
  - can output a result in XML format

  but
  - when called without any limitations the command output is very extensive
  - it can take a long while…
  - v. 2.0.7 coming with Ubuntu 22 package is really poor – no connect timeout and sometimes freezes for very long

  fortunately
  - git version 2.1.3 is much better
  - we plan to add sslscan test to diagnostics/reachability test and improve diagnostics messages to show enabled protocols etc.
- UDP connectivity test – few problems spotted and fixed
  - openssl used to verify a server certificate – again mixed stdout / stderr in openssl 3
  - a site with given CRL Distribution Points but getting it “last forever” – a timeout added to get *not available* quicker

Some stats

- over 5000 unique realms in CAT profiles
- only 490 have dynamic connectivity settings (less than 10%)
- leaders:

country	dyn. realms	all realms	%
UK	193	418	46,2
DE	145	407	35,6
FR	24	300	8,0
ES	22	145	15,2
CH	17	65	25,2
PT	14	68	20,5
PL	13	102	12,7
NL	11	95	11,5
CZ	9	333	2,7
ZA	8	32	25,0

Some stats

- 76 dynamic servers:

country	servers
AM	1
AT	2
BE	2
BR	2
CH	2
CZ	2
DE	5
ES	2
FI	2
FR	2
HU	3

country	servers
IE	3
IT	2
LU	2
MY	2
NL	7
NO	3
PL	10
PT	16
UA	1
UK	3
ZA	2

Some stats

- TLS protocol support:
  - some servers are not available ~10 (e.g. BR, UA, AM, two servers for DE– handling hs-fulda.de)
  - 11 servers have TLSv1.0 and 1.1 enabled (PT – 4, NO – 2, NL – 2, PL – 2, CZ – 1)
  - all available servers have TLSv1.2 enabled
  - 34 servers support TLSv1.3
- Sslscan results
  - time-consuming, relatively fast responses 1-3 secs for UK, IE, CH, AT and NL, for other servers the average time was 3-8 secs, for MY > 40 secs and for ZA ~30 secs
- Openssl results for different client certificates
  - revoked client certificate – only 20 servers respond properly on revoked client certificate: DE, LU, MY, ZA, PT (4) and PL (7)
  - expired and wrong-policy client certificate is treated correctly by all available servers but received openssl error is not always “expired” or “certificate unknown”, some servers respond with “unexpected eof while reading”

GÉANT
Networks • Services • People

Thank you

Any questions?

www.geant.org

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

The scientific work is published for the realization of the international project co-financed by Polish Ministry of Science and Higher Education from financial resources of the programme entitled "PMW"