eduroam-US Best Practices Guide

Repository ID:	TI.146.1
Authors:	Members of the eduroam Advisory Committee
Sponsor:	eduroam Advisory Committee (eAC)
Superseded documents:	n/a
Future review date:	November 2021
Subject tags:	eduroam, best practice, deployment, wireless

Overview

This Best Practices Guide provides [*direction / advice*] on deployment of eduroam wireless access within the research and education community, including higher education and community colleges, K-12, museums, and libraries. It examines tools and strategies for deploying and running eduroam, including a discussion identifying key decision points across the scope of deployment, and helpful information to consider when making those decisions. The goal is to encourage the eduroam community to build and operate the service in a way that is as interoperable, scalable, and sustainable as possible while still allowing for the differences in individual environments.

Target audience:

This Guide is intended for technical staff and network administrators within the eduroam-US community who are responsible for deployment and management of eduroam. Users will also find this Guide helpful for those state and regional providers who service contracts with K-12 entities, including charter and private schools.

The Guide includes a detailed discussion on information specific to U.S. federal guidelines for internet safety and security of children under the age of 18. Guidelines and laws on this topic vary across countries and are referenced as appropriate.

Additional technical detail on topics beyond the scope of this document is referenced and linked as needed.

eduroam is a global resource. Users are encouraged to review the global eduroam Compliance Statement for guidance on use when connecting to eduroam during international travel.

Topic Development:

1. Use eduroam as your organization's primary SSID.

The mobility of the eduroam federation depends on a common wireless network name ('eduroam') being offered at all participating service providing locations. It is the shared eduroam SSID that enables devices to be pre configured and seamlessly roam across all eduroam locations. While it may be advisable to test eduroam initially as a supplemental network, it is suggested to move to eduroam to your organization's primary day-to-day authenticated wireless SSID for the following reasons...

By encouraging your users to use eduroam on a daily basis at their home location, you immediately assure they are ready to travel. Because the distributed nature of eduroam adds a layer of complexity for support staff in troubleshooting connectivity problems while users are traveling, these issues are more easily dealt with if identified locally first. When using eduroam locally, users are continually testing their own connections and thus set up for the best possible success before traveling which reduces your organization's support burden.

Since eduroam is an authenticated service, it is capable of not only identifying visitors at your location but it is able to distinguish your own users from them. This means separate wireless networks aren't a requirement to deliver differing levels of network access locally. Based on who's authenticated, authorization policy in your wireless infrastructure can be used to deliver local access to users@yourschool.edu differently than visitor access to users@someschool.edu without the need for separate networks. The added benefit of this approach is a simplified front door for all users, where access becomes tailored based on who you are, not what you connect to.

Some schools have chosen to "brand" their existing wireless networks and are reluctant to adopt a more general brand such as eduroam. However, end users tend to care mostly about connectivity and very little about this branding especially in the context of device management where wireless profiles are configured automatically for them. Furthermore, the eduroam brand is globally recognizable and able to reach students, faculty, and staff all over the world. As next generation wireless technology becomes more ubiquitous, focus has shifted away from the SSID as a means of network identification which will lead to current emphasis on SSID branding ultimately fading.

While it is suggested that eduroam be used as your primary 802.1X SSID, we understand it won't always replace the need for all wireless networks in your organization. The following are typical exceptions encountered preventing eduroam from being the primary or only SSID:

- Pre-Shared Key (PSK) and open networks may remain relevant in supporting IoT/headless devices and general visitor access not addressed by eduroam.
- Situations where as an identity provider, your organization issues identities that are by design excluded for use on the eduroam federation.
- When devices authenticate using a machine identity (which may not be routable across the eduroam federation) instead of a user identity

2. What level of network access to give eduroam visitors?

Each institution participating in eduroam must choose the level(s) of security and access presented on their eduroam network. Policy can be set globally across the institution's eduroam network or based on the end-user's role. Role-based segmentation can be a way to use eduroam as the institution's primary SSID while still providing granular access control for various groups of users.

As an example, some institutions may configure roles as follows within their eduroam network:

a. **eduroam Visitor:** Granted access as if they were connecting into the institution's services from the Internet; no elevated access to institutional services.
b. **Faculty, Staff, and Student:** Granted access to institutional services as if they were connected to the traditional institutional SSID.
c. **Elevated Access Role(s):** Granted additional access to restricted networks based on the end-user's role.

As this is an institution by institution decision, the experience of the user will differ when roaming at other institutions. When roaming, the user may have access to fewer, or more, services than are available at their home institution and they will have no access to local-only services (i.e., printers) at their home institution.

Special consideration should be taken when your institution's eduroam network is broadcast in areas where other institutions are also broadcasting eduroam. In areas with overlap, your end-users may roam to the other institutions network and lose access to your non-Internet facing services. In these circumstances, coordinating with the other institutions in controlling coverage zones and power levels on wireless access points to minimize roaming is recommended.

3. Considerations for eduroam in K12

Eduroam provides the opportunity for ubiquitous secure wireless access for K12 organizations. Participating K12 educational faculty, teachers, staff and students have ubiquitous wireless access in all educational sites in the state's/regional network and in all other eduroam participating sites throughout the world.

CIPA regulation and content filtering compliance approaches for K-12 member - eduroam access is generally not filtered, however, users do experience differing levels of network and content access when visiting host institutions based on how both eduroam is provisioned within the network and to the degree network security measures including firewalls. As it pertains to eduroam within K12, network and content access will be influenced by the Children's Internet Protection Act (CIPA). As part of a requirement for FCC Universal Service Administrative Company (USAC) E-rate funding for K12 broadband, CIPA requires content filtering.

https://www.fcc.gov/sites/default/files/childrens_internet_protection_act_cipa.pdf

Local Education Agencies (LEA) to include school districts, public charter schools and also private schools that receive E-rate funding are required to adhere to CIPA and provide content filtering for their students.

Content filtering will influence the level of access eduroam users experience within a K12 network. Content filtering may also extend beyond the LEA's network to district issued devices that are managed and filtered by the LEA. In this case, additional measures may be taken to ensure management and filtering of devices when used outside of the classroom, including at home or traveling for school events. In each case this is an LEA requirement separate from eduroam but will influence the eduroam experience for users including K12 students.

CIPA and content filtering considerations

- LEA content filtering is required
- LEA issued devices
    - Mobile Device Management (MDM) - content filtering is enforced through forced proxy, etc.
- Securing student eduroam certificates/credentials - not allowing students to use their credentials on their own non-managed devices
- Only provide student eduroam access on school owned and managed devices to help ensure filtering
- Unmanaged devices/BYOD - hard to support, no solution for K12 at this time

What does eduroam look like in the K12 education environment (use-case examples):

- Student teachers from Weber State University (WSU) are able to do their work and report on progress electronically without spending enormous amounts of their time, and that of WSU IT, to get them connected to the district. For this specific reason, Davis School District implemented eduroam district-wide.
- K12 teachers in Murray school district taking classes on Salt Lake Community College campus have eduroam access.
- Automatic connectivity for the educational technology professionals from the school districts attending statewide meetings/conferences such as SAINTCON, TCC, UETN Tech Summit, etc..
- Automatic connectivity for educational specialists from the state board of education traveling and working in schools across the state.
- Students traveling to other schools for academic and sport activities.

State network role/responsibility for K12:

- Foster collaboration across the districts in the state (example - implement and support a eduroam user group to develop expertise amongst its K12 members to continue to rollout eduroam statewide).
- Help K12 educational organizations understand the importance of eduroam in public education (initially there can be a general lack of what and why use eduroam).
- Help provide ongoing funding for the statewide implementation.
- Support district in finding and using filtering solutions for K-12 students.
- Sign the Internet Connector agreement for each of the LEAs in the state and provide a simpler participation agreement between the districts and the state network. (Example participation agreement from Utah Education and Telehealth Network)

4. Privacy and security suggestions for eduroam-US deployments.

eduroam derives security from the IEEE 802.1x standard for secure network access by authenticating using the encrypted Extensible Authentication Protocol (EAP). The eduroam federation acts as an “EAP router”, moving the client’s authentication request from service location to identity provider. eduroam nature can be privacy preserving if appropriately configured as it does not need to know who the user is to route, only the realm/domain the request belongs to. Because the transaction is specific between a user and his/her identity provider, the payload of the transaction remains private between the two parties and the particular EAP method an institution chooses is an institutional choice as users aren’t restricted to visiting locations using similar configurations.

With that in mind, not all possible configurations are equal in terms of security and privacy. To optimize this, it is recommended you consider the following:

- The method of EAP-TLS is highly recommended as this method provides mutual authentication via server and client certificates. When using EAP-TLS, care should be taken with X.509 certificates in order to avoid disclosing the user identity over transport.
- If a tunneling EAP method is used instead (TEAP, PEAP, EAP-TTLS), anonymous outer identities should be used to avoid disclosing a user identity during transport. Tunneled EAP methods should never be used without a supplicant configuration wizard (see eduroam CAT). Improperly configured supplicants result in high risk of credential exposure.
- It is important to note client MAC addresses may not persist across network sessions and should never be used as a user or device identifier. If tracking is important, RADIUS Chargeable User Identity (RFC 4372) can be used to provide a protected, pseudo-anonymous identifier for the user session.

As a member of the eduroam-US federation, it is important to remember your organization will maintain logging for visitors just as other organizations will maintain logging for your users. You should review logging and log retention schedules as required by your institution as well as the global eduroam Compliance Statement. Develop a formal policy for responding to requests for data from other eduroam members institutions.

5. Service Support Considerations

As a distributed system separating authentication from authorization across a distance, eduroam can present unfamiliar challenges to organizations less accustomed with concepts of identity federation and single sign on. However, rest assured, supporting eduroam doesn't have to be more difficult or limiting than traditional services you're used to on premise provided your understanding of roles and cooperation within the federation. Recognizing that supporting eduroam doesn't come from one organization, but from cooperation as a whole, is the first step in creating a successful support strategy. Not all problems may be directly solvable in isolation, but answers are derivable from identity providers working with service providers under the framework established by the roaming operator.

These topics can be difficult for end users where eduroam is seen as "one big network" instead of a "shared means to access multiple networks" leading to confusion of why the service can vary depending on location. Leveraging the following "Golden Rules" combined with a steady communication campaign is the best strategy for combating such stigma.

Golden Rules:

- Always set up (and test) each device BEFORE traveling.
  How each organization configures their devices for eduroam authentication is an

individual decision may be different from the site being visited making it difficult to perform initial setup remotely. Making sure devices are configured before traveling is best reinforced by using eduroam as your primary SSID at your home location (link to #1 best practice).

- Users should always call their home institution for support first.
  The majority of connection problems are credential related (eg. expired password), which only your home institution can assist with. Users should never contact an eduroam service provider until first speaking with their identity provider.

For more difficult troubleshooting topics that require escalation, it's recommended that identity providers and service providers communicate directly opposed to referring the end user. The roaming operator can assist in setting up this backchannel when necessary. Through such cooperation, it's possible to bring puzzle pieces together necessary to arrive at a conclusion. We suggest service providers report any issues (including evidence) of users misbehaving at their site to the identity provider for follow-up (including punitive action). Acting locally may be necessary, but won't stop the user from continuing within the eduroam federation.

6. Infrastructure Tuning

This section is for technical IT staff (system administrators, network engineers, etc.) who will be responsible for configuring eduroam at their site and includes helpful guidance, that while might not be required, should ease and optimize the experience of deploying eduroam.

Networking

Firewall

- As a federated service, eduroam depends on continuous communication between your internal RADIUS environment and the eduroam-US top level over the Internet. RADIUS protocol (port udp/1812, udp/1813) is required to traverse your perimeter firewall to allow communication to/from the federation.

Load Balancers

- Check with your Load Balancer vendor regarding load balancing of RADIUS/EAP. Generally speaking, UDP protocols present challenges for load balancers and for this reason load balancers are generally discouraged from being part of a first time eduroam setups.

Wireless Controllers

- EAP-Termination should never be enabled on local controllers, this option will break eduroam since EAP tunnels need to be proxied back to home institutions. EAP termination should always occur on a RADIUS server.

RADIUS and EAP

- RADIUS Shared Secret - this unique secret generated by each site that plays a vital role in securing the communication between you and the eduroam-US top level RADIUS servers. It is recommended to choose a minimum of 50 characters with complexity. The value should be safely retained (but never shared) as it is pivotal to your sites peering with the federation and if lost/forgotten, could result in disruption to your site.
- RADIUS Status-Server - if your RADIUS implementation supports this option, it's recommended you enable it and the corresponding option in the eduroam-US Admin Tool to provide enhanced diagnostic information to the eduroam-US top level.
- Realm Filtering - be mindful eduroam routing occurs based upon top level domain (yourschool.edu) only and any subdomain will be routed as a wildcard. If you use a subdomain to authenticate with, make sure to account for these in your local RADIUS policy. Default routing your own subdomain back onto the eduroam federation will create a routing loop which will result in dropped connections.
- EAP Server Certificates - As a best practice, EAP server certificates should be signed by a PKI in your organization’s control and should never be self-signed. If a public CA-signed certificate is used, you may run into issues with certificate chain changes when you renew your certificate every year.
- EAP Methods - EAP-TLS is strongly recommended as it uses a strong credential (certificate) and is mutually authenticated. If certificate-based authentication is not possible and passwords must be used, devices should be configured using a management platform (if the device is under management) or a supplicant provisioning wizard (for unmanaged devices) to ensure the supplicant is properly configured. A user-configured supplicant will likely result in credential compromise. When a password-based tunneled EAP method is used, an anonymous outer identity (@mydomain.edu, no user portion) should always be used to protect user privacy as they roam.

Identity

- If you choose an EAP method that relies on usernames and password for eduroam, users need to be trained using username@realm. This is often most easily described as logging in with their email address (provided it is the same format). Utilize profile management tools (i.e. eduroam CAT) to ensure profiles

are set up correctly. You may choose to disallow “empty realm” authentication locally to reinforce this habit.

Useful Tools

- Testing is often one of the first acts we want to perform and while testing as a local user at your site is straightforward, testing as an eduroam visitor at your site brings some new challenges. For this reason, the eduroam-US Admin Tool offers the ability to generate a set of remote credentials for self-testing as a visitor. These credentials are for testing only and will only be permitted to work originating from your site.
- Sometimes problems exist or can only be witnessed from beyond your site. For this reason, eduroam-US admin tool offers a Log Viewer tool that allows for reviewing routing events to and from your site as witnessed by the eduroam-US top level RADIUS servers. These events can often very quickly identify routing problems stemming from misconfiguration.