eduroam Guest Access requirements

Executive Summary

The Guest Access Working Group was chartered by the eduroam Advisory Committee to develop a set of requirements which Internet2 could use to evaluate solutions for enabling guest use of eduroam in a secure, scalable, and sustainable manner.

In addition to direct participants, guests play a role in eduroam's ubiquity, not only as an enhancement to the service but also as a driver of value. Having a solution to enable carefully scoped guest use benefits numerous segments of the eduroam community.

- Guest users: ease of use, security, consistent access for repeat visits or visits to multiple institutions
- Institutions: ease of management, no need to provision full accounts for non-student/staff, security, cost containment (no/few commercial solutions required)
- eduroam community at large: ease of use/seamless experience, provide consistent & positive experience for community, demonstrate value to current and prospective institutions, drive a consistent set of practices across community around guest access

The availability of a Guest Access service will also lower a major barrier for participating organizations to adopt eduroam as their primary or only SSID.

The working group strongly recommends Internet2 consider the risk of doing nothing - external, non-community solutions could take over and fill that need. Staying engaged in both near and long term will be important for continuing relevance of eduroam.

The eduroam Guest Access Working Group concludes that Internet2 consider a managed service with strong roots in the R&E community whose cost can be included in the existing fee structure for eduroam, with the benefit also being shared across the community.

Summary of Work

eduroam Guest Service Models

The working group identified five main approaches to guest access.

- A managed guest access service like eVA (eduroam Visitor Access), where the provider manages the infrastructure for provisioning and manages accounts, often with strong multi-tenancy functionality, and the home institution manages the identity store and issues, manages, and assumes responsibility for the guest accounts.
- An on-premises guest service which is fully owned and operated by the home institution.
- Fully hosted commercial solutions which are operated and managed by a 3rd party company, with the home institution issuing and assuming responsibility for the guest accounts.
- ANYROAM's guest service, which is based on Ruckus' Cloudpath and features little to no management of individual accounts beyond revocation of individual certificates.
- Open network with no authentication, or a simple anonymous click-through captive portal.

eduroam Guest Access Service Features

The working group has identified sets of Guest Access features, grouped into the following categories:

Required

- Flexibility of strict registration and open registration to serve a wide range of use cases, including long term (repeated visits for multiple days or weeks) and short term accounts (1-3 days)
- User accountability and accounting, including tightly binding guest accounts to traceable (both to the user and the issuing institution), verifiable identity elements such as phone numbers and email addresses
- Automated credential delivery via cell phone/SMS, self-service provisioning options
- Clientless operation
- Mobile device awareness – responsiveness
- Enterprise grade security
- Ability for institution staff to map guest accounts to verifiable information (e.g. phone number) via self service portal or other administrative interface (including bulk or individual provisioning)

Desired

- EAP-TLS enabled, includes method for certificate installation (possibly by leveraging geteduroam and CAT)
- Consumer federation (i.e. Google, Office 365, etc) proxy
- Embedded security - endpoint checking for up-to-date security patches and antimalware
- Customized role-based policies and workflows
- Custom, consistent branding for each institution
- Customized reporting and compliance
- Captive portal where client/supplicant can be obtained on-site
- Built-in feedback and review mechanisms
- API support to incorporate into in-house portals

- Provides consistent experience whether client is using wifi only or cellular data

Community Needs

Members of the eduroam community have expressed a need for a Guest Access Service which provides a consistent feature set and user experience. This working group believes a solution which avoids provisioning full accounts for one-time or limited purpose use and includes the means to manage those accounts ongoing would dramatically improve the value of eduroam for the community as a whole.

Currently, the availability of guest access services for eduroam enabled locations is limited to ANYROAM's guest service, 3rd party commercial offerings, or a locally managed guest network. This working group is of the opinion that while these options do work to some degree, they lack features and functionality which are needed by the community.

The institutions with the greatest need for this service are, by and large, the areas of the fastest growth in the eduroam community (e.g. K12, libraries, and smaller institutions of higher education). As such, this working group asserts that having a scaleable, sustainable means of managing guest access is critical to the success of eduroam.

Recommendations for Internet2

This working group recommends a service which:

- Allows for a variety of registration options, including, self registration of guests and delegated registration (e.g. organization staff can create accounts)
- Provides capability for participating organizations to directly manage guest accounts
- Accommodates the delivery of EAP-PEAP credentials via SMS at a minimum, with the option to integrate with services like CAT and geteduroam to accommodate EAP-TLS authentication, possibly at a later date.
- Bakes costs associated with the Guest Service into the standard eduroam fees as a companions service

The group has been very impressed with CANARIE's implementation of eVA and strongly recommends adoption of a solution with strong feature parity to that offering.

Technical Requirements for eduroam Guest Service

Technical Requirement	Relevant Standards/Guidelines
Meets GEANT requirements for participation in eduroam	https://www.eduroam.org/wp-content/uploads/2016/05/eduroam_Compliance_Statement_v1_0.pdf
Conforms to community best practices	https://spaces.at.internet2.edu/display/eduroam/Consultation+on+eduroam-US+Best+Practices+Guide?preview=%2F174066029%2F174066124%2Feduroam-US+Best+Practices+Guide.pdf
Operates in a manner consistent with US eduroam subscribers	https://incommon.org/wp-content/uploads/2019/05/eduroam-connector-agreement-201711-Rvw-Copy.pdf

References

Eduroam Advisory Committee Best Practices Guide

eVA user video

Appendix - User Stories

University of North Carolina at Greensboro offers eduroam as its primary wireless SSID to 20k+ faculty, staff and students along with two guest wifi solutions and an overall desire to consolidate/simplify guest services…

- Traditional guest wifi services from commercial provider Aruba leveraging a captive portal for in person self-registration using SMS or email verification and granting short lived (24hrs) access. Help desk retains the ability to generate blocks of codes in advance for planned on campus events/conferences.
- ANYROAM guest access for advance registration before arriving on campus, multi-day use for multi-day events, and multi-site compatibility (with NCA&T university, GTCC community college, and USCI training center all existing within a 5 mile radius of UNCG).

UNCG has selected to deliver a higher level of network access and performance to eduroam visiting students & educators than to self-asserted guests.

- University of Washington is transitioning from a branded SSID to making eduroam the predominant network across its 3 campuses, 3 hospitals and numerous remote sites and clinics. Guest access is currently through a captive portal with SSO authentication and we have Anyroam available as well. In our hospitals, we also have a simple click-through captive portal for patients and visitors. We are currently exploring providing a better guest experience and consolidating networks in use.Currently guests have to call our help desk to have temporary NetID assigned; these can be for individuals, or assigned to an event such as orientations, or be used for conferences on campus.
- ANYROAM is used for longer-term visitors. Could be visiting faculty, medical staff or even long-term patients

We don't currently differentiate between guest access and our students and staff; we are looking at this in the future.

We are also updating our "network portal" page for departmental IT administrators to manage their network related "things" from looking at MAC addresses, building network metrics, DNS and DHCP, and would like to include guest functionality into this framework as well.