Guest and Public Network Access

Title: Guest and Public Network Access

Reference: GEN-DOC-002

Issue: 9

Document Owner: Iain Brown

Authorised by: Henry Hughes

Date: 5 September 2024

Last Reviewed Date: 1/09/2025

Document control

1. Superseded documents:

PB/INFO/073

2. Changes made:

1/9/2025 - Minor change - document owner and authoriser updated

Guest and Public Network Access

This factsheet suggests some ways for organisations that wish to provide guest and/or public network access for external visitors to do so. A Jisc Technical Guide [1] gives more details and case studies of implementations.

Janet is the UK's research and education network. An organisation connected to Janet will typically at its own discretion make access to Janet available to its own members but may also choose to offer it to other individuals visiting the organisation at its invitation and for purposes associated with the organisation's education, research and engagement missions. Examples of the latter case might include use of Janet by delegates at an academic conference or similar event (whether or not a fee is charged) held by the organisation under those missions, or use by individuals not formally associated with the organisation but to whom services are being provided under the organisation's missions, such as access to its library or similar resources. Such delegates or individuals are referred to in this factsheet as **'guests'** and may be visiting from another organisation with its own Janet connection, or from elsewhere (by convention, members of the education community from a different organisation such as visiting researchers who make use of roaming connectivity are referred to as **‘visitors’**).

Within the overall limits of this userbase, each connected organisation can decide as a matter of local policy what level(s) of access to Janet it provides and to whom. The Janet Security Policy requires organisations to have appropriate measures in place for giving, controlling and accounting for access to Janet. This normally involves each local or guest user having their own unique username and password (see the Jisc factsheet on User Authentication [2]).

Some Janet-connected organisations may in addition wish to provide Internet connections, either for a fee or free of charge, to members of the public who are not guests of the organisation (for example members of the public using accommodation or other facilities or simply walking across the campus). In order to protect the reputation and status of Janet as a private network, traffic from these users (referred to in this factsheet as **‘public users’**) must be kept separate from the organisation's normal research and education traffic. Janet must not be used to connect public users directly to the Internet. Subject to conditions set out in the Janet Network Connection Policy [3] and discussed below, an encrypted point-to-point tunnel across Janet may be used to backhaul public user traffic to a partner Internet Access Provider (e.g. a commercial ISP). Alternatively public users may be connected to the Internet by a separate dedicated network link. In both cases the organisation and its access provider are responsible for compliance with policies and legislation applying to public networks.

User designation:	**Description:**
Visitor	Member of the educational community or associated public sector body; typically using eduroam or govroam for access.
Guest	Not necessarily a member of an educational body but visiting the organisation for purposes aligned with its educational mission. Typically, the organisation will know something about guests in advance of their arrival on site, e.g. booked delegates to a conference.

Public user	A member of the general public requiring general purpose connectivity and not necessarily using it for education-related activities. Traffic originating from public users may not pass across Janet outside of an encrypted tunnel to a third party provider.

The network context to which these various classes of user connect will be referred to as a **‘guest network’**. For example, an organisation may determine that visitors and guests are trusted to a similar extent and have common requirements so both connect to the same locally-provided guest network that connects them to Janet; public users might in that case be connected to a different guest network with a less trusted level of access provided in partnership with a commercial ISP.

Providing Guest Access

The simplest and safest way to provide access for visitors from other Janet-connected organisations and equivalents abroad is to join Jisc's eduroam service [4] as a visited organisation or preferably a full participant (full participation provides both the capability to host visitors and for the organisation’s own staff and students to enjoy the same benefits when visiting other participating organisations). The international eduroam [5] federation provides a link between organisations so that a guest from another eduroam member can use their home organisation username and password to authenticate to a guest network provided by the visited organisation. Utilising the same technologies, eduroam’s sister service govroam [6] offers this facility to the wider public sector, allowing staff from local government, NHS and blue light services to connect. Education sector organisations are encouraged to offer govroam as a visited-only service alongside their eduroam coverage to facilitate collaboration.

The guest network in this case must provide access to Janet but need not give any access to local services[1] [7]. By providing an eduroam and/or govroam visitor facility, an organisation can trust that visitors who use it are current members, in good standing, of another peer organisation and, because that home organisation is bound by the relevant policy, that it will take responsibility for its user’s actions (including, if necessary, investigating and punishing any reported misuse of the visitor network facility or Janet).

Where a guest does not come from an eduroam or govroam member organisation, a facility for creating temporary local accounts may be required. A number of Janet-connected organisations allow authorised members of staff to assign short-lived accounts to visitors to their departments: these staff members are responsible for ensuring that the guest understands and complies with local and Janet policy requirements. This system relies heavily on the sponsor and their personal knowledge of the guest, since the guarantees provided by eduroam are not available. Many mechanisms can be used to assign such accounts, from an option in an identity management system to pre-prepared sealed envelopes or scratch cards that each contain one visitor username and password[2] [8]. Jisc’s eduroam Visitor Access (eVA) service [9] simplifies the creation of temporary local accounts able to authenticate through the existing eduroam network at the issuing organisation.

The Janet Security Policy [10] requirement to control access to Janet means that it is not appropriate simply to provide guests with access to an unauthenticated network port or open

wireless network. It is also inadvisable to allow a local user to log the guest on using their own credentials since this is likely to give the guest far more access to local systems and to Janet than was intended. Similarly, if the organisation does not provide a separate segment or VLAN for guests then care will be needed to ensure that guests do not gain unintended access to internal or licensed resources which may trust IP addresses for authorisation.

Providing Public User Access

If an organisation wishes to provide Internet access to members of the public who are on its premises other than as guests then this must be done in partnership with an Internet Access Provider such as a commercial ISP. The Janet Network Connection Policy [3] permits the network to be used to backhaul traffic to a partner access provider, but only if users are authenticated - either by the access provider or the organisation - the traffic is carried across Janet in an encrypted tunnel and the traffic is identified as originating from the access provider - not Janet or the organisation - when it reaches the public Internet. Alternatively the connection between the organisation and the access provider may use a dedicated network link. Janet must not be used to connect public users directly to the Internet.

Public users generally require a wireless network connection. This may be achieved by allowing a commercial ISP to install their own separate equipment on the organisation's premises; or, more usually, the existing wireless LAN infrastructure will be shared with the partner access provider and the network configured to route public traffic to them, either over a dedicated link or an encrypted point-to-point tunnel over Janet.

In a typical shared installation, wireless access points are configured to broadcast at least two different SSIDs (Service Set Identifiers). Visitors (and in the case of eVA, guests) connect to the 'eduroam' or ‘govroam’ SSIDs automatically, since they typically have created a connection profile on their device(s) when the credentials are issued to them, and authenticate with their local or eduroam credentials. Their traffic is then routed to Janet. Public users connect to the ‘commercial’ SSID (which may either have local naming reflecting the visited organisation, or that of a recognised commercial national wireless service), and are connected to the Internet via the commercial ISP’s authentication system and network. Each SSID is associated with a VLAN that logically segregates the traffic and routes it to the appropriate upstream connectivity: Janet or commercial ISP.

Organisations considering such partnerships should note that any network that offers Internet access to the public is likely to be classified in law as a public electronic communications service, whereas Janet and the networks of its customers are generally classified as private. Operating a public service is likely to involve more onerous duties, for example:

- protection of the privacy of users (*Investigatory Powers Act 2016* and *Privacy and Electronic Communications (EC Directive) Regulations 2003*)
- notification of privacy breaches to the Information Commissioner and users (*Privacy and Electronic Communications (EC Directive)(Amendment) Regulations 2011*)
- blocking sites on the BBFC list of adult content providers that do not implement age verification (*Digital Economy Act 2017*)
- retention of data about usage for criminal and terrorist investigations (*Investigatory Powers Act 2016*)
- further obligations on copyright enforcement and hate speech are being discussed.

It seems likely that these obligations would only apply to those parts of the network that

actually carry public traffic, so segregating this traffic either logically or physically should allow the rest of the organisation's LAN to continue to operate on a private network basis. Organisations should seek individual legal advice on the implications for their own networks.

The privacy-related duties of a public communications service provider are likely to apply to both the organisation and their partner Internet Access Provider and should be explicitly addressed in the agreement between the parties. Responsibility for compliance with other laws and policies should also be assigned by contract between the organisation and the access provider.

[1] [11] If you do choose to offer one or more local services (e.g. printing), they must be documented and supported locally. The minimum expected provision for roaming services such as eduroam is access to email, web and vpn.

[2] [12] Care should be taken that such temporary accounts expire promptly when the guest has finished with them; leaving unattended accounts 'live' unnecessarily increases the attack surface of your network.

Links
[1] https://community.ja.net/library/janet-policies/network-access-guests-technical-guide
[2] https://community.ja.net/library/janet-policies/user-authentication
[3] https://community.jisc.ac.uk/library/network-and-technology-policies/janet-network-connection-policy
[4] https://www.jisc.ac.uk/eduroam
[5] http://www.eduroam.org/
[6] http://www.jisc.ac.uk/govroam
[7] https://jisc365.sharepoint.com/sites/QIS/Published/Cross%20Area%20Processes/Other%20Quality%20Documents/C DOC-002.docx#_ftn1
[8] https://jisc365.sharepoint.com/sites/QIS/Published/Cross%20Area%20Processes/Other%20Quality%20Documents/C DOC-002.docx#_ftn2
[9] https://www.jisc.ac.uk/eduroam-visitor-access
[10] https://community.ja.net/library/janet-policies/security-policy
[11] https://jisc365.sharepoint.com/sites/QIS/Published/Cross%20Area%20Processes/Other%20Quality%20Documents/C DOC-002.docx#_ftnref1
[12] https://jisc365.sharepoint.com/sites/QIS/Published/Cross%20Area%20Processes/Other%20Quality%20Documents/C DOC-002.docx#_ftnref2