Table of Contents

Introduction 3  
   About eduroam visitor access 3  
   Who can use eduroam visitor access? 3  
   What will you find in this manual? 3  
   Questions 3  
Three key principles 4  
Create user profiles 5  
   Profile types 5  
   Rights within a profile 6  
   Create profile 7  
   Edit or delete profile 9  
1-day SMS 10  
Overview of all visitors 11  
Functions for CERT members to deal with incidents 12
Introduction

About eduroam visitor access
As a host, you can use eduroam visitor access to create temporary eduroam accounts for visitors to your educational or research institution. These accounts will give visitors temporary access to the organisation’s eduroam Wi-Fi network.

You can create accounts using the visitor access eduroam online portal. All you need is an Internet browser; there is nothing to be installed.

eduroam visitor access is provided for you by Jisc.

Who can use eduroam visitor access?
Your educational or research institution determines who may act as hosts for the purpose of using eduroam visitor access and what conditions hosts need to meet when creating temporary eduroam accounts on the Wi-Fi network. eduroam visitor access can only be used by host users if you as the organisation’s eduroam visitor access administrator have enabled the users.

The Jisc authorisation role of AAI Coordinator needs to be applied to your eVA account to enable you as the eduroam visitor access administrator to carry out the host user assignment and management tasks described in this manual.

CERT employees can also be given access to eduroam visitor access. They require the authorisation role of Security Coordinator. CERT members can view, edit and terminate all temporary eduroam accounts for their own organisation.

What will you find in this manual?
This manual describes the functions of eduroam visitor access for administrators:

• Create and manage user profiles (see page 5). You use a profile to define which rights users have under which conditions

• 1-day SMS (see page 9). SURFnet can create 365 SMS keywords that are valid for 1 day, so that your visitors can use this SMS self service every day

• Functions for CERT members (see page 11). In case of incidents, CERT members can view and manage all user accounts

The other functions are described in the basic manual “Creating temporary eduroam accounts in 5 steps” and “Creating groups and SMS events”.

Questions
If you have any further questions about using eduroam visitor access after reading the manual, please contact Jisc on eva@jisc.ac.uk.
Three key principles

The eduroam network is used by students and staff in your organisation. Their organisational accounts give them access to this secure, reliable network. To keep the network secure and reliable, it is important that access is refused to unauthorised outsiders.

As an eduroam visitor access administrator, you play an important role in this since you are enabling staff or employees of your organisation who are acting as hosts to give visitors temporary access to eduroam. During the configuration and administration of eduroam visitor access, always apply the following principles when creating user accounts. This will ensure we keep eduroam secure and reliable together.

1. The purpose of the individual's visit must be associated with the organisation's education, research and engagement missions.

2. An eduroam visitor access account must only be valid for the duration of the visit.

3. eduroam visitor access enables you to provide guests with eduroam access and your organisation is responsible for the hosting, support and guidance of visitors and the proper operation of the network.
Create user profiles

Before a member of staff or employee acting as a host can create temporary visitor accounts using eduroam visitor access, a profile which defines the user’s rights needs to be created in eVA. As an eduroam visitor access administrator (AAI Coordinator), you create staff host profiles.

Without profiles, users can log on to eduroam visitor access, but they cannot actively use it.

Important
Profiles are quick and easy for you to create, but it is important to think carefully about their design and the rights to give to a user. This will prevent unintentional or deliberate unauthorised use of eduroam visitor access.

Profile types
eduroam visitor access has three profile types:

- **Role-based profiles**: are valid for groups of users with the same role. This type of role is based on the *eduPersonScopedAffiliation* UAM attribute. This can be employee or staff. The organisation’s federated access management system provides this attribute when the user logs on to eduroam visitor access. The value of this attribute is determined by the organisation’s identity management system (such as LDAP or Active Directory).

- **Personal profiles**: are valid for one person only. This type of profile is based on the user’s email address.

- **Group profiles**: are valid for several persons. This type of profile is based on the email addresses of users that have been placed in a group. Every group has its own configuration. If several users have the same configuration, you are recommended to give them a group profile rather than create several individual personal profiles.

Important
Only the values *employee* and *staff* are supported in eduroam visitor access for the *eduPersonScopedAffiliation* attribute. Click here for more information about the *eduPersonScopedAffiliation* attribute.

- **Personal profiles**: are valid for one person only. This type of profile is based on the user’s email address.

- **Group profiles**: are valid for several persons. This type of profile is based on the email addresses of users that have been placed in a group. Every group has its own configuration. If several users have the same configuration, you are recommended to give them a group profile rather than create several individual personal profiles.

Important
If it is unclear which user email address is used in eduroam visitor access, the email address is provided in the My details section the host user sees on the eduroam visitor access homepage.

If a user matches a role-based profile, but also has a personal profile, the rights of the personal profile will apply. You can create a role-based profile with a global configuration for a large group of users and then also create a personal profile with a different configuration (with more rights, for example).
Rights within a profile

When you create a profile, you can give the user(s) of that profile one or more rights. You can choose from the following rights:

- Users can create separate, temporary eduroam accounts
- Users can create a number of temporary eduroam accounts simultaneously by uploading a CSV file
- Users can create a group of temporary eduroam accounts that are not yet linked to any visitors, for example, for an upcoming event for which the visitors’ names are not known yet. However, it is important that the user fills in the visitor details as completely as possible afterwards
- Users can create SMS events. This allows visitors to create a temporary eduroam account using a keyword for themselves without any user intervention

Important

- Assign the **create group** and **create SMS** event rights to a very limited group of users. These functions allow the user to create temporary eduroam accounts without knowing who will be using them. Improper use of these functions can have a major negative impact on the (Wi-Fi) networks of your organisation and other eduroam providers.
- We also recommend making it compulsory to provide visitors’ mobile phone numbers. This allows visitors to receive their account details by text message. This is useful when visitors are unable to see the account details by email.
Create a profile

1. Log on to eduroam visitor access at https://eva.eduroam.uk
2. From the main menu, click on Admin > Profiles.
3. Now select Add a profile (fig1)
4. The screen fig3 appears
5. Enter the information (fig4)
Profile

A,B,C

Choose one of the following options:

A. Email profile: personal profile based on the user’s email address
B. Group profile: group profile based on email addresses of users in the group (several persons)
C. Role profile: role-based profile based on the user’s

1. Profile name
   For example: “employees of the organisation”

2. SAML role / SAML email address
   For a personal profile (A): enter the user’s email address.
   For a group profile (B): enter several user email addresses here.
   For a role-based profile (C): choose Employee or Staff.

3. Maximum number of visitors
   The maximum number of visitors is the maximum number of active accounts a user can create.

4. Maximum period
   The maximum period (number of days) the user can assign to a temporary account.

5. Rights
   Tick 1 or several options.
Edit or delete profile

From the main menu, click on Admin > Profiles. The following screen appears:

- Click on to edit the profile details.
- Click on to delete the profile.
- Click on to edit or delete the email addresses. This icon is only visible for group profiles.

If you delete a profile, the rights of the host users in this profile expire. However, any temporary eduroam visitor accounts that the users had previously created will continue to exist.
1-day SMS

The primary eduroam visitor access administrator for your organisation can request Jisc to create 365 SMS keywords that are valid for one day. Send the request to eva@jisc.ac.uk.

Jisc will then create SMS keywords for an entire year. Each SMS keyword is valid for one day. This allows your organisation to provide SMS event functionality and give users a temporary self-service eduroam account on a daily basis.

You can view the 1-day SMS keywords that were created via the menu option Admin > 1-day SMS.

You have the following options here:

- Click on [ ] to see which temporary accounts are included in the group.
- Click on [ ] to edit the group details.
- Click on [ ] to delete the group.

You can change the details of a 1-day SMS keyword. You can only change the maximum number of visitors that can access eduroam simultaneously using this keyword. The keyword itself cannot be changed.

Click on [ ] to delete a 1-day SMS keyword.
Overview of all visitors

Admins (with the authorisation role of AAI Coordinator) can view all visitor accounts for their own institution. Editing and deleting visitor accounts is not possible; this can only be done by the users themselves or by CERT members).

In the main menu, click on Admin > All visitors.
Functions for CERT members to deal with incidents

CERT members (with the authorisation role of Security Coordinator) can view, edit and terminate all the visitor accounts for their own institution. In the main menu, click on CERT > Visitor accounts.

CERT users can also edit user profiles and in the event of incidents or other disasters, they can adjust the profile parameters to prevent unauthorised abuse. In the main menu, click on CERT > Profiles.

The SMS event has been created.
Share our vision to make the UK the most digitally advanced education and research nation in the world

jisc.ac.uk