eVA Guidance for UK federation IdP operators

Contents

Introduction

Logging in to the eVA portal (which enables the admins/events organisers/hosts at the organisation to use the service) is only supported through federated SSO via eduGAIN. Federated access facilitates access and will lead to enhances management of portal access accounts. Therefore membership of the UKAMF/eduGAIN is a mandatory pre-requisite.

Prospective participants should check that their UK federation registered SSO IdP production system can resolve and release the attributes detailed below to the eduroamvisitoraccess SP which has an entityID:
https://eduroamvisitoraccess.org/simplesaml/module.php/saml/sp/metadata.php/edugain-sp

In addition, the SSO IdP must not be 'hidden' in the UKAMF metadata and must also be published through eduGAIN. (The eVA SP uses the eduTEAMS discovery service, which references eduGAIN).

SAML Attributes to be released

urn:oid:2.16.840.1.113730.3.1.241 (**displayName**)
urn:oid:1.3.6.1.4.1.5923.1.1.1.9 (**eduPersonScopedAffiliation**)
urn:oid:0.9.2342.19200300.100.1.3 (**mail**)
urn:oid:1.3.6.1.4.1.5923.1.1.1.6 (**eduPersonPrincipalName**)

A SAML2 Persistent NameID (named identifier) may be required which may require reconfiguration on some IdP software, and for all IdPs and on-going management of that identifier.

Example for Shibboleth IdP 3.3.0 (onwards)

Here is an example Attribute Filter Policy that can be added to the attribute filter (assuming existing filter releases **eduPersonScopedAffiliation**);

```
    <AttributeFilterPolicy id="eduroamvisitoraccess-org">
        <PolicyRequirementRule xsi:type="Requester"
value="https://eduroamvisitoraccess.org/simplesaml/module.php/saml/sp/metadata.php/edugain-sp" />
         <AttributeRule attributeID="displayName">
            <PermitValueRule xsi:type="ANY" />
         </AttributeRule>
         <AttributeRule attributeID="mail">
            <PermitValueRule xsi:type="ANY" />
        </AttributeRule>
         <AttributeRule attributeID="eduPersonPrincipalName">
            <PermitValueRule xsi:type="ANY" />
        </AttributeRule>     </AttributeFilterPolicy>
```

You may also need to configure displayName, mail, and eduPersonPrincipalName against your attribute resolver, we would advise to refer to the example attribute resolver files provided in your Shibboleth IdP installation e.g. attribute-resolver-ldap.xml

Testing

To test, go to **https://eva.eduroam.uk/login**
Attempt to log in using the eduTEAMS discovery service (your organisation should be selectable from the list)
As part of the login process the SP will have requested SAML attributes
You will be denied access as you are not registered, but the above demonstrates proper attribute release.

You can check what attributes are being released by your IdP to the eVA SP by visiting:

https://eduroamvisitoraccess.org/simplesaml/module.php/core/authenticate.php?as=edugain-sp
or
https://eva.eduroam.uk/simplesaml/module.php/core/authenticate.php?as=eva-sp

Scroll down to **AuthData** and click on:

> Click to view AuthData