Published on *Jisc community* (https://community-stg.jisc.ac.uk)

Home > Network and technology service docs > eduroam > Technical Reference Docs > Cisco ACS/ISE Configuration for eduroam

Cisco ACS/ISE Configuration for eduroam

Collection of How-to Guides for the Cisco ACS/ISE Family

Configuring Cisco ISE

We do not have any specific documentation on configuring ISE for eduroam use, but Cisco's own general configuration doc appears to be fairly comprehensive:

https://communities.cisco.com/docs/DOC-71299 [1] - eduroam-specific instructions

and

https://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user_guide/ise_user_guide/ise_man_id_stores.html [2]

https://community.cisco.com/t5/security-documents/configuring-eduroam-on-cisco-identity-services-engine-ise/ta-p/3655672 [3] - for 2.1

Sending operator name with ISE 2.0

Cisco ISE servers do not have the correct attribute set up for insertion of the Operator-Name attribute. However, the steps to achieve this are straight forward in the GUI. The following article describes how:

https://community.jisc.ac.uk/groups/eduroam/document/operator-name-cisco-ise-2 [4]

Configuring Cisco ACS 5.3 for a Visited (SP) eduroam Service

For details of how to configure Cisco ACS 5.3 for Visited site eduroam see:

https://community.jisc.ac.uk/blogs/scotts-eduroam-blog/article/eduroam-visited-configuration-cisco-acs-53 [5]

Sending Operator Name with ACS 5.4

Cisco ACS 5.4 provides the ability to inject and/or overwrite RADIUS attributes while proxying. This means that attribute 126 Operator Name can be injected for eduroam Visited sites (as per our recommendations).

Operator Name injection while proxying to NRPS

In the Visitor Access Policy (JRS in the example below) first remove any existing Operator Name attributes (which may have been added by the NAS) and add the Service Provide Operator Name.

1. Go to "Access Policies > Access Services" and click on the Visitor Access Policy (JRS)

2.Click on the "RADIUS Attibutes" drop down (Below "External Proxy Servers")

3. Select "RADIUS-IETF" as the "Dictionary Type:"

4.Click the 'Select' button for "RADIUS Attribute"

5.In the 'RADIUS Dictionary popup window select 'ID' in the "Filter:" field

6. In the 'RADIUS Dictionary popup window select 'Equals' in the "Match If:" field

7. In the 'RADIUS Dictionary popup window in the text box after the "Match If:" field enter 126 and click the 'Go' button

8. Then tick the radio button for 'Operator-Name' and click 'OK' at the bottom

9. In the "Operation:" field chose 'DELETE' and then click the 'Add ^' button

10. Repeat steps 3 to 8

11. In the "Operation:" field chose 'ADD'

12. In the "Attribute New Value:" text box enter the your sites realm prepended with 1 e.g. '1camford.ac.uk'

13. Click the 'Add ^' button

14. Click the 'Submit' button

Author: Scott Armitage

Configuring Cisco ACS 5.3 for a Home (IdP) eduroam Service

For details of how to configure Cisco ACS 5.3 for Home site eduroam see:

https://community.jisc.ac.uk/blogs/scotts-eduroam-blog/article/eduroam-h... [6]

Note to Cisco ACS 4.2 Users

In ACS 4.2 you can use a feature called "Domain Stripping" in the Home user authentication process. However it is strongly recommended that you upgrade to the latest version of ACS or employ Cisco ISE since 4.2 is no longer supported by Cisco and doesn't support newer versions of AD, injection of Operator-Name etc.

Links

[1] https://communities.cisco.com/docs/DOC-71299

[2] https://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user_guide/ise_user_guide/ise_man_id_stores.html

[3] https://community.cisco.com/t5/security-documents/configuring-eduroam-on-cisco-identity-services-engine-ise/ta-p/3655672

[4] https://community.jisc.ac.uk/groups/eduroam/document/operator-name-cisco-ise-2

[5] https://community.jisc.ac.uk/blogs/scotts-eduroam-blog/article/eduroam-visited-configuration-cisco-acs-53

[6] https://community.jisc.ac.uk/blogs/scotts-eduroam-blog/article/eduroam-home-configuration-cisco-acs-53