Cisco ISE/ACS Configuration for eduroam

?

Published: 12/09/2016

Updated: 21/12/2023 and 21/02/2025

Configuring Cisco ISE for eduroam

Contents

1. Published Documentation

We do not have any Jisc-produced documentation on configuring ISE for eduroam use, but Cisco's own general configuration doc **https://www.ise-support.com/2019/07/01/configuring-ise-for-eduroam-authentication/** [1] can be used as a starting point and contains eduroam-specific instructions however these contain errors! You **MUST** read these in conjuntion with our >> **Implementing eduroam roadmap** [2] <<. This contains relevant configuration guidance for Cisco ISE in each logical section.

ISE 3.1 - 3.2 - we've had reports of problems with the remote RADIUS configuration / RADIUS authenticators on various versions of ISE over time and issues have been reported with version 3.2 too. **A known good ISE version is ISE 3.1 patch 8** - as of 21/12/2023 this is the recommended version of ISE to be running. And version **ISE 3.2 patch 3** should also be good.

Hint: After applying any ISE update or patch or after editing remote RADIUS server in Network Resources > External RADIUS Servers or a RADIUS server sequence in Network Resources > RADIUS Server Sequences, you MUST check that ISE is still forwarding auth requests for your visitors to the NRPS. The Support Server Troubleshoot > Logs > Radius authog can be useful here - apply the filter Operator:<your realm> and the report will show only authentication requests that are being sent from your ORPS to the NRPS.

ISE 3.0 - 3.1 - version 3.0 was released c. Sept 2021. Nothing very much changed between 2.7 and 3.0 other than the addition of some new features. The GUI screens may have altered, but the above guide can still be used as a starting point.
https://community.cisco.com/t5/security-documents/configuring-eduroam-on-cisco-identity-services-engine-ise/ta-p/3655672 [3] Note the WARNINGs documented below.

2. Configuration Notes

WARNING(1)! The section in the Cisco guide beginning - "Create another condition 'Eduroam_User_Traveling' " which is intended to relate to your roaming users, i.e. authentication requests recieved from the NRPS, contains some conditions which have erroneously been included; these **MUST NOT** be applied, namely:

Radius:Service-Type = Framed
AND
Radius:NAS-Port-Type = Wireless 802.1X (type 19)
AND
Airespace:Airspace-WLAN-ID = 6 <This would be relevant to the Policy condition for auths from your visitors to campus>

Those attributes have no relevance to users roaming to other venues and have place in the Policy for Roaming Users. The condition you need to apply is that the RADIUS client belongs to your 'Eduroam network Device Group' (i.e. the NRPSs).

WARNING(2)! The section beginning "Create a new condition, 'Eduroam_User_External', this will be used to identify RADIUS requests that need to be handed off to the eduroam RADIUS Servers" contains errors. It is not clear why the conditions, Radius: Service-Type EQUALS Framed AND Radius: NAS-Port-Type EQUALS Wireless – IEEE 802.11 are included. Furthermore it is possible that these conditions will result in unwanted attributes being included in the RADIUS request sent to the NRPSs.

Our advice is - it is only necessary define a condition that identifies that the realm component of the username is NOT that of the local organisation and DOES include '@' (and ideally is NOT one of the 'bad usernames' that are detailed elsewhere in the eduroam(UK) documentation).

So, in your policy conditions for selecting authentication requests for visitors which will be forwarded to the eduroam(UK) NRPS, set the following conditions only:

Radius: User-Name NOT ENDS WITH @<your_domain>
AND
Radius: User-Name CONTAINS @ <This is the bare minimum as all it checks is that there is an @ in the username..>
You should also add a condition for matching the VLAN/WLAN-ID/network service from which the auth request has come. This will be highly dependent on your local Wi-Fi kit and network configuration. The Cisco guide - relating to Cisco WLAN kit provides (in the wrong section) the following:
AND
Airespace:Airspace-WLAN-ID = 6 <Alternatively you could match Radius:Called_Station-ID ENDS WITH eduroam>

See also: https://www.ise-support.com/2019/07/01/configuring-ise-for-eduroam-authentication/ [1]

Nb. Upgrade matix - https://community.cisco.com/t5/security-knowledge-base/ise-version-upgrade-matrix/ta-p/3653501 [4]

ISE 2.3 - 2.7 - a new Policy Engine was introduced in version 2.3 and with that came changes to how RADIUS Proxy Sequences are used for authentication. Because of this change in behavior https://community.cisco.com/t5/security-documents/configuring-eduroam-on-cisco-identity-services-engine-ise/ta-p/3655672 [3] (note this guide can be used for versions 2.2 and lower since it breaks the Policy Sets section into sections detailing the configurations necessary for both strands).

(*) 2.7 has entered end-of-life and the last date of software maintenance releases will be 22 Sept 2023 https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/bulletin-c25-2943876.html [5]

ISE 2.0 - 2.2 - https://community.cisco.com/t5/security-knowledge-base/configuring-eduroam-on-cisco-identity-services-engine-ise-2-1/ta-p/3655770 [6] (was https://communities.cisco.com/docs/DOC-71299 [7])

ISE 1.2 - 1.4 - has been retired; you should upgrade to ISE 2.7 (stable) or 3.0

3. ISE Distributed Deployments

Understanding the roles of different nodes—specifically the Admin Node and the Policy Node—is crucial for both setting up networks and maintaining security protocols efficiently.

ISE has 3 components/personas:

- Administration (PAN) – Administration Node is a single point of ISE deployment configuration. This persona provides full access to administration GUI
- Policy Service (PSN) – Policy Service Node is a node that handles traffic between network devices and ISE (its IP is used as Radius for devices). To achieve radius traffic sharing you can scale the PSNs up.
- Monitoring (MnT) – monitoring node is responsible for logs aggregation across deployment.

Which nodes are the ones you peer with the eduroam(UK) NRPS? The Policy Service Nodes

are the ones that handle authentication traffic and these need to be peered with the eduroam NRPS and your WLCs.

4. 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://jisc365.sharepoint.com/:w:/s/PublicDocumentLinks/EV0MDZgs1ypHjNClhcrRaoQBTUJKZvUkT7
Psg?e=jTcikD [8]

Configuring Cisco ISE 1.2 - archive material

Cisco Identity Services Engine 1.2 has been retired and is no longer supported
https://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user_guide/ise_user_guide/ise_man_id_stores.html [9]

Configuring Cisco ACS - archive material

The Cisco ACS services of products has now been retired. The last version 5.8 will become unsupported after August 2022.

https://www.cisco.com/c/en/us/obsolete/security/cisco-secure-access-cont... [10]

The information below should be considered as archive material.

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 [11]

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... [12]

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://www.ise-support.com/2019/07/01/configuring-ise-for-eduroam-authentication/
[2] https://community.jisc.ac.uk/library/janet-services-documentation/implementing-eduroam-roadmap-part-2
[3] https://community.cisco.com/t5/security-documents/configuring-eduroam-on-cisco-identity-services-engine-ise/ta-p/3655672
[4] https://community.cisco.com/t5/security-knowledge-base/ise-version-upgrade-matrix/ta-p/3653501
[5] https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/bulletin-c25-2943876.html

[6] https://community.cisco.com/t5/security-knowledge-base/configuring-eduroam-on-cisco-identity-services-engine-ise-2-1/ta-p/3655770
[7] https://communities.cisco.com/docs/DOC-71299
[8] https://jisc365.sharepoint.com/:w:/s/PublicDocumentLinks/EV0MDZgs1ypHjNClhcrRaoQBTUJKZvUkT7vXHPUOkl-Psg?e=jTcikD
[9] https://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user_guide/ise_user_guide/ise_man_id_stores.html
[10] https://www.cisco.com/c/en/us/obsolete/security/cisco-secure-access-control-system-5-4.html
[11] https://community.jisc.ac.uk/blogs/scotts-eduroam-blog/article/eduroam-visited-configuration-cisco-acs-53
[12] https://community.jisc.ac.uk/blogs/scotts-eduroam-blog/article/eduroam-home-configuration-cisco-acs-53