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

Home > **Network and technology service docs** > **eduroam** > **Technical Reference Docs** > RADIUS attribute filtering with Microsoft IAS and NPS

RADIUS attribute filtering with Microsoft IAS and NPS

Reviewed 12/06/2019

Why do we need to configure attribute filtering?

RADIUS packets contain various "attributes" which can be generated by the network access server (eg. AP or switch) and at RADIUS servers that handle the packets during authentication and accounting exchanges. Certain attributes play a key role in the process of correct assignment of the user to an appropriate VLAN. Depending on the manufacturer of the equipment, these can be RFC-defined attributes or vendor-specific ones.

Problems can arise when a roaming user attempts to authenticate at a visited site and the values of the attributes that have been set either cannot be correctly interpreted or result in unpredictable effects on either the Visited or Home networks. This will be a particular problem if the Visited and Home networks both utilise equipment from the same manufacturer and so use the same attributes.

To prevent the above situation, sites providing an eduroam(UK) service must employ attribute filtering at their ORPSs. In particular, sites offering a Visited service must filter attributes in incoming return access-accept packets. Visited sites should also filter out any troublesome attributes that are set by devices on their networks during the attempted visitor connection process. Good practice and good neighbourliness dictate that Home sites should also filter certain attributes in those access-accept replies outbound from their sites. This will avoid their own roaming users experiencing problems resulting from attributes that are applied during authentication by the Home site ORPS.

In some special circumstances, organisations may have agreed a common usage of attributes, for example where there is a pool of students shared between a number of institutions and similar VLAN assignment policies have been adopted at the sites involved. In these cases the institutions should implement realm-dependent attribute filtering rules.

Some organisations do not employ RADIUS VLAN assignment and have just the one network (eduroam) for both guests and own staff/students linked to the eduroam wireless service. Such organisations do not need to worry about incoming Access-Accept VLAN assignment attributes causing problems since their network access servers (APs and switches) will effectively be 'hard set' to a particular VLAN.

The role of attributes during authentication and VLAN assignment

A number attributes associated with VLAN assignment are set during authentication and are intended for use on the network local to the user. This applies both in the case of a user authenticating on their home network as well as the user authenticating when at a visited site

using the eduroam(UK) service. In both cases the same VLAN assignment attributes can be used by the networks the user is trying to connect to but they can have different effects – leading to failure to be connected to the guest network. This applies particularly to the attributes most commonly used during VLAN assignment as follows:

Tunnel-Medium-Type Tunnel-Type Tunnel-Private-Group-id	used with Cisco kit
Aruba-User-Vlan	used with Aruba kit
Trapeze-VLAN-Name	used with Trapeze kit
3Com-VLAN-Name	used with 3Com kit

When setting up a Visited eduroam(UK) service, the Visited site organisation must ensure that visitors are correctly assigned to the eduroam guest VLAN. This can effectively be accomplished by configuring the APs/switches to listen for and act on RADIUS attributes.

With Microsoft IAS/NPS, the relevant attribute values can be applied by the Visited site RADIUS server through both the RADIUS server network policy and connection request policy. The required result is that the relevant VLAN assignment attribute is set to the appropriate VLAN value depending on whether the user is a guest or a member of a particular user-group at the Visited institution. This attribute can then be used by the AP/switches to assign the user to the relevant eduroam or user-group VLAN.

The above works fine when only local realm users connect to the network. However when users from remote sites attempt to connect to the network, a problem can arise as the result of the user's Home RADIUS server applying various attribute values which are relevant only on the Home network. The returning Access-Accept packets if passed unmodified to the APs/switches on the Visited LAN contain VLAN-associated attributes which cannot be interpreted or acted upon by the Visited network APs/switches. The result is that the visitor will fail to be connected to the eduroam guest network.

It is therefore essential that Visited sites employ filtering of certain attributes to prevent the above from happening, although it must be noted that there is a set of key attributes (eg. Proxy-state, EAP and MPPE flags) that must not be filtered out, otherwise authentication will fail. See https://community.jisc.ac.uk/library/janet-services-documentation/faqs-eduroam-system-administrators-and-implementation-techs [1]and scroll down to '*I've set up Attribute filtering - what Attributes should I NOT filter out?*'

What's the issue with Microsoft IAS and NPS?

With most RADIUS server software, attribute filtering is straightforward, however with Microsoft IAS and NPS (in current implementation) there is unfortunately no method of removing specific attributes. Instead the only way to ensure that spurious attributes do not cause problems is to override the attributes that might be set by RADIUS servers at Home institutions and to replace them with ones that will not cause problems.

What filtering / replacement is needed?

The attributes used for VLAN assignment by the network access servers on the Visited site network need to be identified. Filtering / attribute replacement can then be configured to protect these. Some of these attributes will be vendor specific and if there is more than one vendor of APs/switches on the network, the full list of attributes will be greater than those in the example below.

Be aware that problems can manifest themselves some time after an initial deployment and configuration of your eduroam guest network. For example you may suddenly receive visitors from an organisation site that has recently deployed new equipment from the same vendor as the equipment on your network (or part of it) or you deploy equipment from a new vendor and your filtering / attribute replacement rules which were fine before but now will have left your network vulnerable to problems caused by the new attributes.

Essentially there are three main attributes that must be overridden on Access-Accept packets returning from the Home institution RADIUS servers as follows (for Cisco-based networks):

Attribute Name	Value
Tunnel-Medium-Type	"802" (the transport medium)
Tunnel-Pvt-Group-ID* **this is vendor-specific**	[VLAN name or number] (the id of the VLAN you want your guests to be placed on)
Tunnel-Type	"VLAN"

* Vendor-specific VLAN assignment attributes:

Cisco	Tunnel-Private-Group-ID
Trapeze	Trapeze-VLAN-Name
Aruba	Aruba-User-Vlan
3Com	3Com-VLAN-Name

How to set up the necessary attribute override with Microsoft IAS / NPS

1. Under Microsoft IAS, open the 'Policies' list and expand the 'Connection Request Policies' folder to reveal the various connection policies (which will comprise at least your roaming own users policy, local network connection own users policy and visiting users policy). Here we are interested in the two policies that were created for Home user connection and Visitor auth requests forwarding).
2. Open the Connection Request Forwarding Policy for visiting users (the policy for visitors which forwards requests from non-local realms to the NRPS).
3. Select "Edit Profile", then select the "Advanced" tab.

4. ... t return attributes can be modified – note **)
5. ... -Medium-Type", then select "Add".
6. ... he value for the attribute (see screenshot)

Multivalued Attribute Information

Attribute name:
Tunnel-Medium-Type

Attribute number:
65

Attribute format:
Enumerator

Attribute values:

Vendor	Value
RADIUS Standard	802 (includes all 802 media plus E

[Move Up] [Move Down] [Add] [Remove] [Edit]

[OK] [Cancel]

[2]

7. OK all the open windows.
8. Repeat the above process from step 3. This time choosing "Tunnel-Type" in step 5 as the attribute and the eduroam VLAN name or number id you want your guests to be placed on.
9. Repeat the above process for relevant VLAN assignment attribute (on Cisco networks this will be "Tunnel-Pvt-Group-ID" – see list in previous section for the attribute name used with other vendors). The value of this attribute is usually the name of the VLAN as set on the AP/switch or in some cases it is the VLAN number. This must be established either through testing or checking the documentation. Enter the name or number id you want your eduroam guests to be placed on.

Even if your visitor's Home organisation has not implemented an outbound attribute filtering system on their ORPS the above process will replace any attributes that may have been set at the Home organisation with values that are relevant to your Visited guest network service

NB. **Although it appears that the above settings substitute your preferred attributes into the Access-Request message to be forwarded to the NRPS and thence the Home organisation ORPS, in fact these attributes are only stored in the proxy session table. The attributes are not actually added to the Access-Request message but are saved for the response to the Access-Request message. The effect is to substitute your preferred attributes into the Access-Accept message and so to correctly set your visitor onto the eduroam guest network. See:
http://technet.microsoft.com/en-us/library/cc773343(WS.10).aspx#w2k3tr_ias_how_zyra [3]

This document was produced at the result of problems encountered during deployment of Microsoft IAS to support 802.1X and eduroam as a new installation at Royal Holloway University of London. Thanks to James Borne (Royal Holloway University of London), the originator of this document and to Alexander Clouter of SOAS for his extensive help with troubleshooting this issue.

Source URL: https://community.jisc.ac.uk/library/janet-services-documentation/radius-attribute-filtering-microsoft-ias-and-nps

Links
[1] https://community.jisc.ac.uk/library/janet-services-documentation/faqs-eduroam-system-administrators-and-implementation-techs
[2] http://community.ja.net/sites/default/files/JRS-filtering-RADIUS-attributes-with-MS-IAS-and-NPS.jpg
[3] http://technet.microsoft.com/en-us/library/cc773343(WS.10).aspx#w2k3tr_ias_how_zyra