

PacketFence for eduroam

Contents

Introduction.....	1
Configuration.....	2
Policies and Access Control	2
Roles	2
Domains.....	2
Authentication Sources	6
Network Devices.....	10
Connection Profiles.....	13
System Configuration	15
SSL Certificates > RADIUS tab	15
TLS profiles (Optional)	15
Status.....	16
Services.....	16
Testing	16

Introduction

PacketFence is a feature-rich open-source network access control system. It can also be used as a RADIUS server for eduroam. The following instructions are designed to complement the official PacketFence documentation https://www.packetfence.org/doc/PacketFence_Installation_Guide.html.

Community support is offered through [mailing lists](#) and high-quality [commercial support](#) is also available.

This guide assumes that you have already installed PacketFence and run through the initial configuration, which includes setting the PacketFence server IP address and admin password.

This document courtesy of Dale Lloyd, Oxford Centre of Islamic Studies


Configuration

Policies and Access Control

Roles

Click **New Role**

Name: eduroam



StatusReportsAuditingNodesUsers**Configuration**

admin ? 1

Filter

Policies and Access Control

Roles

Domains

Active Directory Domains

Realms

Authentication Sources

Network Devices

Switches

Switch Groups

Connection Profiles

Compliance

Integration

Advanced Access Configuration

Network Configuration

System Configuration

Role eduroam

Nameeduroam

Description

Parent roleSelect option

Max nodes per user0

The maximum number of nodes a user having this role can register. A number of 0 means unlimited number of devices.

Include Parent ACLsDisabled

Fingerbank Dynamic ACLsDisabled

Use the Fingerbank dynamic ACLS

ACLs

Access Control Lists

Inherit VLANDisabled

Inherit VLAN from parent if none is found

Inherit RoleDisabled

Inherit Role from parent if none is found

Inherit Web Auth URLDisabled

Inherit Web Auth URL from parent if none is found

SaveCloneResetCancelDelete

Click **Create**

Domains

Active Directory Domains

Click **New Domain**

Status Reports Auditing Nodes Users **Configuration**
admin

Policies and Access Control
Roles
Domains
Active Directory Domains
Realms
Authentication Sources
Network Devices
Switches
Switch Groups
Connection Profiles
Compliance
Integration
Advanced Access Configuration
Network Configuration
System Configuration

New Domain

Settings
NTLM cache

Identifier

camford

Workgroup

camford

DNS name of the domain

camford.ac.uk

The DNS name (FQDN) of the domain.

This server's name

%h

This server's name (account name) in your Active Directory. Use %h to automatically use this server hostname.

Sticky DC

*

This is used to specify a sticky domain controller to connect to. If not specified, default "" will be used to connect to any available domain controller.

Active Directory server

dc1.camford.ac.uk

The IP address or DNS name of your Active Directory server.

DNS server(s)

10.0.0.1,10.0.0.2

The IP address(es) of the DNS server(s) for this domain. Comma delimited if multiple.

OU

Computers

Use a specific OU for the PacketFence account. The OU string read from top to bottom without RDNs and delimited by a '.'. (ex: Computers/Servers/Unix).

NTLM v2 only

☐

If you enabled "Send NTLMv2 Response Only. Refuse LM & NTLM" (only allow ntlm v2) in Network Security: LAN Manager authentication level.

Allow on registration

☐

If this option is enabled, the device will be able to reach the Active Directory from the registration VLAN.

Note: "Allow on registration" option requires passthroughs to be enabled as well as configured to allow both the domain DNS name and each domain controllers DNS name (or *.dns name). Example: inverse.local, *.inverse.local

Create

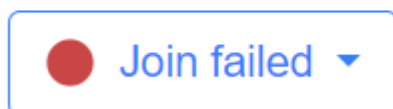
Reset

Cancel

Fill in the details then click **Create**

After clicking Create, near the top left of the webpage, you will see a join failed message. Click on it, click **Join** then provide the appropriate credentials to join the PacketFence server to the Active Directory domain.


Domain camford



Join camford domain



Please enter administrative credentials to connect to the domain.

Username 
Username required.

Password 
Password required.

Cancel

Join Domain

You should then see Join success




Join success ▼

Realms

Click **New Realm**

On the General tab, type the realm

Status Reports Auditing Nodes Users **Configuration**admin ? 3

Filter

Policies and Access Control

Roles

Domains

Active Directory Domains

Realms

Authentication Sources

Network Devices

Switches

Switch Groups

Connection Profiles

Compliance

Integration

Advanced Access Configuration

Network Configuration

System Configuration

New Realm

General

NTLM Auth

EAP Configuration

Freeradius Proxy

Freeradius Eduroam Proxy

Stripping

Realm

camford.ac.uk

Regex Realm


PacketFence will use this Realm configuration if the regex match with the UserName (optional).

Create

Reset

Cancel

On the NTLM Auth tab, set the domain to the one created earlier



Status

Reports

Auditing

Nodes

Users

Configuration

admin

?

3

Filter

Policies and Access Control

Roles

Domains

Active Directory Domains

Realms

Authentication Sources

Network Devices

Switches

Switch Groups

Connection Profiles

Compliance

Integration

Advanced Access Configuration

Network Configuration

System Configuration

New Realm

X

General

NTLM Auth

EAP Configuration

Freeradius Proxy

Freeradius Eduroam Proxy

Stripping

Domain

camford

The domain to use for the authentication in that realm.

eDirectory

Select option


The eDirectory server to use for the authentication in that realm.

Create

Reset

Cancel

On the Stripping tab, turn off **Strip in RADIUS authorization**



StatusReportsAuditingNodesUsersConfiguration

admin

?

3

Filter

Policies and Access Control

Roles

Domains

Active Directory Domains

Realms

Authentication Sources

Network Devices

Switches

Switch Groups

Connection Profiles

Compliance

Integration

Advanced Access Configuration

Network Configuration

System Configuration

New Realm

GeneralNTLM AuthEAP ConfigurationFreeradius ProxyFreeradius Eduroam ProxyStripping

Strip on the portal

Enabled

Should the usernames matching this realm be stripped when used on the captive portal.

Strip on the admin

Enabled

Should the usernames matching this realm be stripped when used on the administration interface.

Strip in RADIUS authorization

Disabled

Should the usernames matching this realm be stripped when used in the authorization phase of 802.1x. Note that this doesn't control the stripping in FreeRADIUS, use the options above for that.

Custom attributes

Disabled

Allow to use custom attributes to authenticate 802.1x users (attributes are defined in the source).

LDAP source

Select option

The LDAP Server to query the custom attributes.

LDAP Source for TTLS PAP

Select option

The LDAP Server to use for EAP TTLS PAP authorization and authentication.

Azure AD Source for TTLS PAP

Select option

The Azure AD to use for EAP TTLS PAP authentication.

CreateResetCancel

Click **Create**

Authentication Sources

Internal Sources

Click **New internal source > RADIUS**

Status

Reports

Auditing

Nodes

Users

Configuration

admin

3

Filter

Policies and Access Control

Roles

Domains

Active Directory

Domains

Realms

Authentication Sources

Network Devices

Switches

Switch Groups

Connection Profiles

Compliance

Integration

Advanced Access Configuration

Network Configuration

System Configuration

Authentication Source roaming0_ja_net

RADIUS

Name

roaming0_ja_net

Description

roaming0.ja.net

Host

roaming0.ja.net

Port

1812

If you use this source in the realm configuration the accounting port will be this port + 1.

Secret

.....

Timeout

1

Monitor

☐

Do you want to monitor this source?

Use Connector

☒

Use the available PacketFence connectors to connect to this authentication source. By default, a local connector is hosted on this server. Using remote connectors is only supported on a standalone instance at the moment.

NAS IP Address

Which NAS IP Address to use when communicating with the RADIUS server. Leaving this empty will make the source use the management IP of the server (management VIP in a cluster).

Options

type = auth+acct

Define options for FreeRADIUS home_server definition (if you use the source in the realm configuration). Need a radiusd restart.

Associated Realms

Realms that will be associated with this source (for the portal/admin GUI/RADIUS post-auth, not for FreeRADIUS proxy).

Authentication Rules

Add Rule

Administration Rules

Add Rule

Save

Clone

Reset

Cancel

Delete

Do the same for roaming1.ja.net and roaming2.ja.net

Click New internal source > Active Directory

Status

Reports

Auditing

Nodes

Users

Configuration

admin

1

Filter

Policies and Access Control

Roles

Domains

Active Directory Domains

Realms

Authentication Sources

Network Devices

Switches

Switch Groups

Connection Profiles

Compliance

Integration

Advanced Access Configuration

Network Configuration

System Configuration

Authentication Source Active_Directory_User_Auth_Eduroam

Active Directory

General

Certificates

Name

Active_Directory_User_Auth_Eduroam

Description

User authentication for eduroam SSID (internal members)

Host

camford.ac.uk

389

Start TLS

SSL Verify Mode

none

The SSL verify mode when connecting via LDAP. Only applies when using Start TLS or LDAPS.

Dead duration

60

How much time in seconds should a server be marked dead before it is retried. When specifying multiple LDAP servers or a DNS name pointing to multiple IPs, then this option can be used to offer more consistent failover. A value of 0 disables this feature.

Connection timeout

1

LDAP connection Timeout.

Request timeout

5

LDAP request timeout.

Response timeout

10

LDAP response timeout.

Base DN

DC=camford,DC=ac,DC=uk

Scope

Subtree

Username Attribute

UserPrincipalName

Main reference attribute that contain the username.

Search Attributes

Other attributes that can be used as the username (requires to restart the radiusd service to be effective).

Append search attributes LDAP filter

Append this ldap filter to the generated generated ldap filter generated for the search attributes.

Email Attribute

mail

LDAP attribute name that stores the email address against which the filter will match.

Bind DN

PacketFence@camford.ac.uk

Leave this field empty if you want to perform an anonymous bind.

Password

Test

Cache match

Will cache results of matching a rule.

Monitor

Do you want to monitor this source?

Shuffle

Randomly choose LDAP server to query.

Use Connector

Use the available PacketFence connectors to connect to this authentication source. By default, a local connector is hosted on this server. Using remote connectors is only supported on a standalone instance at the moment.

Associated Realms

camford.ac.uk

Realms that will be associated with this source.

Authentication Rules

assign_eduroam_role_for_internal_members

Status

Enabled

Name

assign_eduroam_role_for_internal_members

Description

Matches

All

Conditions

Add Condition

Actions

1

Role

eduroam

2

Access duration

12 hours

Administration Rules

Add Rule

Save

Clone

Reset





Cancel

Delete

You should now have the following listed under Internal Sources:

Internal Sources

New internal source ▾

⌵	<input type="checkbox"/>	Name	Type	Description	⌵
	<input type="checkbox"/>	roaming0_ja_net	RADIUS	roaming0.ja.net	<div>DeleteClone</div>
	<input type="checkbox"/>	roaming1_ja_net	RADIUS	roaming1.ja.net	<div>DeleteClone</div>
	<input type="checkbox"/>	roaming2_ja_net	RADIUS	roaming2.ja.net	<div>DeleteClone</div>
	<input type="checkbox"/>	Active_Directory_User_Auth_Eduroam	Active Directory	User authentication for eduroam SSID (internal members)	<div>DeleteClone</div>

Exclusive Sources

New exclusive source > Eduroam

Filter

Policies and Access Control

Roles

Domains

Active Directory Domains

Realms

Authentication Sources

Network Devices

Switches

Switch Groups

Connection Profiles

Compliance

Integration

Advanced Access Configuration

Network Configuration

System Configuration

Authentication Source Eduroam_Outbound

Name

Eduroam_Outbound

Description

Eduroam Source

Eduroam Realm Options

nostrip

Operator-Name

Eduroam RADIUS AUTH

roaming0_ja_net roaming1_ja_net roaming2_ja_net

Type

Keyed Balance

Authentication listening port

11812

Reject Realms

Local Realms

camford.ac.uk

Authentication Rules

catchall_for_eduroam_visitors_only

Status

Enabled

Name

catchall_for_eduroam_visitors_only

Description

Matches

All

Conditions

Add Condition

Actions

1

Role

eduroam

2

Access duration

12 hours

Save

Clone

Reset


Cancel

Delete

Network Devices

Switch Groups

Create a Switch Group for your access points



StatusReportsAuditingNodesUsersConfiguration

admin

Filter

Policies and Access Control

Roles

Domains

Active Directory Domains

Realms

Authentication Sources

Network Devices

Switches

Switch Groups

Connection Profiles

Compliance

Integration

Advanced Access Configuration

Network Configuration

System Configuration

Switch Group aruba_ap

DefinitionRolesInlineRADIUSSNMPCLISWeb ServicesMembers

Basic Mode

Identifieraruba_ap

Descriptionaruba_ap

TypeAruba Instant Access

ModeProduction

Deauthentication MethodRADIUS

Deauth on previous switchNo

External Portal EnforcementDefault (No)

VoIPDefault (No)

VoIP DHCP DetectDefault (Yes)

Dynamic UplinksDefault (Dynamic)

Note: Some RADIUS related settings have been moved to the RADIUS tab

Save

Clone

Reset

Cancel

Delete

StatusReportsAuditingNodesUsersConfiguration

admin

Filter

Policies and Access Control

Roles

Domains

Active Directory Domains

Realms

Authentication Sources

Network Devices

Switches

Switch Groups

Connection Profiles

Compliance

Integration

Advanced Access Configuration

Network Configuration

System Configuration

Switch Group aruba_ap

DefinitionRolesInlineRADIUSSNMPCLISWeb ServicesMembers

Basic Mode

Role mapping by VLAN ID

Role by VLAN IDNo

Role mapping by Switch Role

Role by Switch RoleYes

registration

isolation

macDetection

inline

Machine

REJECT

User

default

eduroam0

gaming

guest

voice

Role mapping by Web Auth URL

Role by Web Auth URLDefault (No)

SaveCloneResetCancelDelete

StatusReportsAuditingNodesUsersConfiguration

admin

Filter

Policies and Access Control

Roles

Domains

Active Directory Domains

Realms

Authentication Sources

Network Devices

Switches

Switch Groups

Connection Profiles

Compliance

Integration

Advanced Access Configuration

Network Configuration

System Configuration

Switch Group aruba_ap

DefinitionRolesInlineRADIUSSNMPCLISWeb ServicesMembers

Basic Mode

Secret Passphrase

Use CoADefault (Yes)

Use CoA when available to deauthenticate the user. When disabled, RADIUS Disconnect will be used instead if it is available.

Use Connector For DeauthDefault (Yes)

Use the available PacketFence connectors to perform RADIUS deauth (access reevaluation). By default, a local connector is hosted on this server.

Controller IP Address

Use instead this IP address for de-authentication requests. Normally used for Wi-Fi only.

Disconnect Port

For Disconnect request, if we have to send to another port.

CoA Port

For CoA request, if we have to send to another port.

Post MFA ValidationDefault (No)

Add an extra validation in the RADIUS flow to detect if the user successfully validate the MFA.

CLI/VPN Access EnabledDefault (No)

Allow this network equipment to use PacketFence as a RADIUS server for CLI or VPN access.

SaveCloneResetCancelDelete

Switches

Create a switch using an IP address or range, linked to the switch group that you just created.

The screenshot shows the configuration page for a switch with IP address 10.10.200.0/24. The page is titled "Switch 10.10.200.0/24" and has a tab labeled "aruba_ap". The left sidebar contains a navigation menu with the following items: Policies and Access Control, Roles, Domains, Active Directory Domains, Realms, Authentication Sources, Network Devices, Switches, Switch Groups, Connection Profiles, Compliance, Integration, Advanced Access Configuration, Network Configuration, and System Configuration. The main content area has tabs for Definition, Roles, Inline, RADIUS, SNMP, CLI, and Web Services. The "Definition" tab is active, showing the following configuration fields: IP Address/MAC Address/Range (CIDR) set to 10.10.0/24, Description set to aruba_ap, Type set to Aruba Instant Access, Mode set to Production, Switch Group set to aruba_ap - (aruba_ap), Deauthentication Method set to RADIUS, Deauth on previous switch set to No, External Portal Enforcement set to Default (No), VoIP set to Default (No), VoIP DHCP Detect set to Default (Yes), and Dynamic Uplinks set to Default (Dynamic). A note at the bottom states: "Note: Some RADIUS related settings have been moved to the RADIUS tab". At the bottom of the page are buttons for Save, Clone, Reset, Cancel, and Delete.

Switch 10.10.200.0/24 **aruba_ap**

Definition Roles Inline RADIUS SNMP CLI Web Services Basic Mode ☐

IP Address/MAC Address/Range (CIDR) 10.10.0/24

Description

Type

Mode

Switch Group

Deauthentication Method

Deauth on previous switch ☐ No
This option parameter will allow you to do the deauthentication/CoA on the previous switch where the device was connected.

External Portal Enforcement ☐ Default (No)
Enable external portal enforcement when supported by network equipment.

VoIP ☐ Default (No)

VoIP DHCP Detect ☒ Default (Yes)
Detect VoIP with the DHCP Fingerprint.

Dynamic Uplinks ☒ Default (Dynamic)
Dynamically lookup uplinks.

Note: Some RADIUS related settings have been moved to the RADIUS tab

Connection Profiles

Eduroam for internal members

Eduroam for visitors

Status

Reports

Auditing

Nodes

Users

Configuration

admin

Filter

Policies and Access Control

Roles

Domains

Active Directory Domains

Realms

Authentication Sources

Network Devices

Switches

Switch Groups

Connection Profiles

Compliance

Integration

Advanced Access Configuration

Network Configuration

System Configuration

Standard Connection Profile Catch_Eduroam_Outbound_eduroam_visitors

Preview

Settings

Captive Portal

Files

Profile Name

Catch_Eduroam_Outbound_eduroam_visitors

A profile id can only contain alphanumeric characters, dashes, period and/or underscores.

Profile Description

Outbound requests to Eduroam servers for visitors coming from other universities

Enable profile

Enabled

Root Portal Module

Default portal policy

The Root Portal Module to use.

Activate preregistration

Disabled

This activates preregistration on the connection profile. Meaning, instead of applying the access to the currently connected device, it displays a local account that is created while registering. Note that activating this disables the on-site registration on this connection profile. Also, make sure the sources on the connection profile have "Create local account" enabled.

Automatically register devices

Enabled

This activates automatic registration of devices for the profile. Devices will not be shown a captive portal and RADIUS authentication credentials will be used to register the device. This option only makes sense in the context of an 802.1x authentication.

Reuse dot1x credentials

Disabled

This option emulates SSO when someone needs to face the captive portal after a successful 802.1x connection. 802.1x credentials are reused on the portal to match an authentication and get the appropriate actions. As a security precaution, this option will only reuse 802.1x credentials if there is an authentication source matching the provided realm. This means, if users use 802.1x credentials with a domain part (username@domain, domain\username), the domain part needs to be configured as a realm under the RADIUS section and an authentication source needs to be configured for that realm. If users do not use 802.1x credentials with a domain part, only the NULL realm will be match if an authentication source is configured for it.

Dot1x recompute role from portal

Enabled

When enabled, PacketFence will not use the role initially computed on the portal but will use the dot1x username to recompute the role.

MAC Auth recompute role from portal

Disabled

When enabled, PacketFence will not use the role initially computed on the portal but will use an authorized source if defined to recompute the role.

Dot1x unset on unmatched

Enabled

When enabled, PacketFence will unset the role of the device if no authentication sources returned one.

Enable DPSK

Disabled

This enables the Dynamic PSK feature on this connection profile. It means that the RADIUS server will answer requests with specific attributes like the PSK key to use to connect on the SSID.

Default PSK key

This is the default PSK key when you enable DPSK on this connection profile. The minimum length is eight characters.

Enable Unbound DPSK

Disabled

This enables Dynamic Unbound PSK. If the network equipment supports sending attributes that allow to identify the PSK using the Access-Request attributes, then the user attached to the PSK can be found and used in the same manner as in 802.1x.

Automatically deregister devices on accounting stop

Disabled

This activates automatic deregistration of devices for the profile if PacketFence receives a RADIUS accounting stop. This option only makes sense in the context of an 802.1x authentication.

VLAN pool technique

username_hash

The algorithm used to calculate the VLAN in a VLAN pool.

Filters

any

Filter

Realm

eduroam

With no filter specified, an advanced filter must be specified.

Advanced filter

Basic Mode

ALL (AND)

The advanced filter acts as an additional filter that is combined with the basic filters and respects all any.

Sources

Add Source

With no source specified, all internal and external sources will be used.

Billing Tiers

Add Billing Tier

With no billing tiers specified, all billing tiers will be used.

Provisioners

Add Provisioner

With no provisioners specified, the provisioners of the default profile will be used.

Scanners

Add Scanner

With no scan specified, the scan engine will not be triggered.

Self service policy

Select option

Save

Clone

Reset

Cancel

Delete

System Configuration

SSL Certificates > RADIUS tab

Create the appropriate RADIUS certificates and place them here.

TLS profiles (Optional)

If you wish to accept connections from outdated operating systems, lower the TLS minimum version

