canarie

Get Serious about Wi-Fi Security:
Protect Users from Falling Victim to Credential Harvesting

Ed Kingscote | DevOps Specialist

March 10, 2022

BCNET Connect Summit

eduroam Characteristics

- Globally distributed
- Bring-Your-Own-Device
- Secure
- Large-scale
- Widening reach

Security is a practice, not a thing.

eduroam Security Features

- SSID
- Authentication
- Segregation
- Isolation
- Layers
- Guest Access
- Device Configuration
- PII Protection

It's EAPHammer Time!

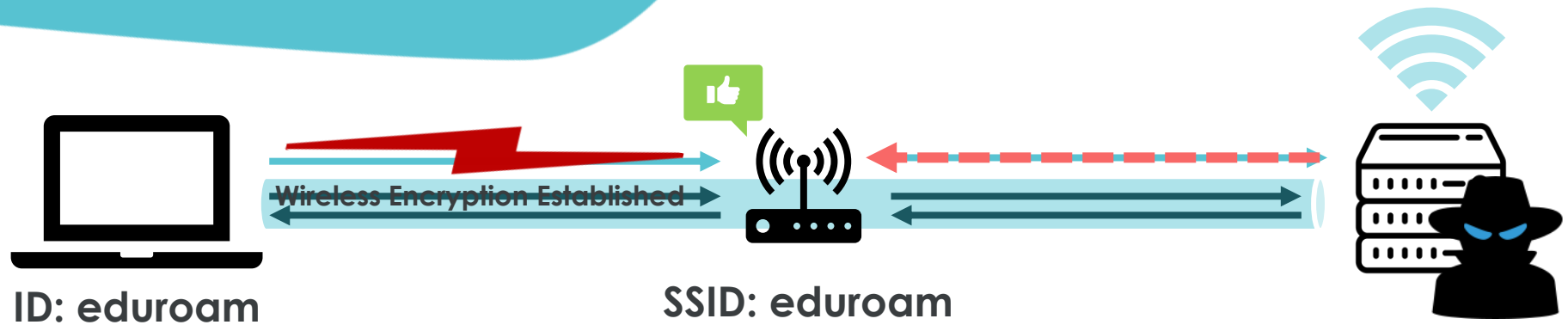
Demonstrating the Commoditized Harvesting of Wi-Fi Credentials

File Edit Tabs Help

pi@raspberr... × * pi@raspbe... ×

```
root@raspberrypi:/home/pi/eaphammer# ./eaphammer -i wlan0 --channel 4 --auth wpa-eap --essid eduroam --creds
```

What Happened?



1. Negotiate authentication model
EAP-PEAPv0-GTC, EAP-PEAPv0-MSCHAPv2

2. Certification validation (TLS Setup)

3. Establish secure tunnel (TLS)
Prevents eavesdropping

4. Perform authentication through tunnel

5. Authentication successful!
Establish encryption, connect to internet

6. Client acquires IP address (DHCP)

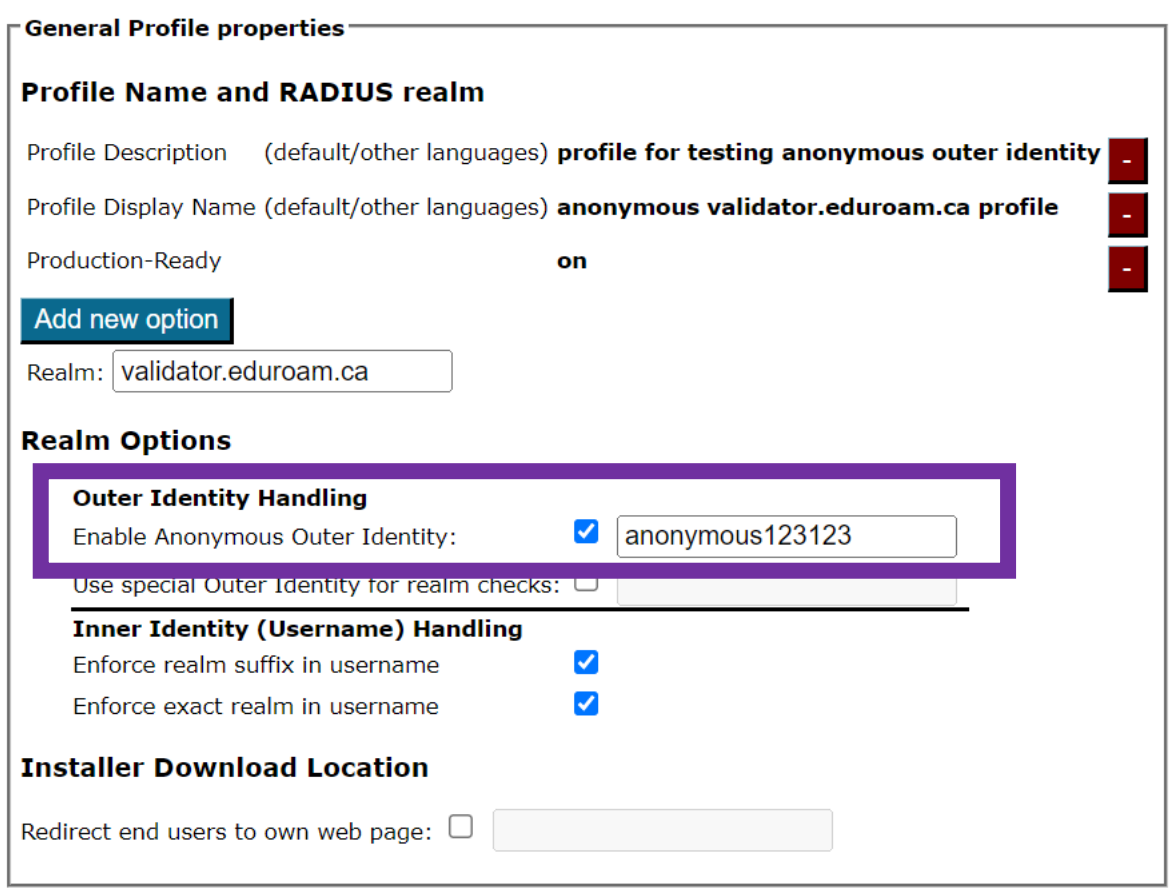
It is the client's responsibility to ensure that they are communicating with a trusted server.

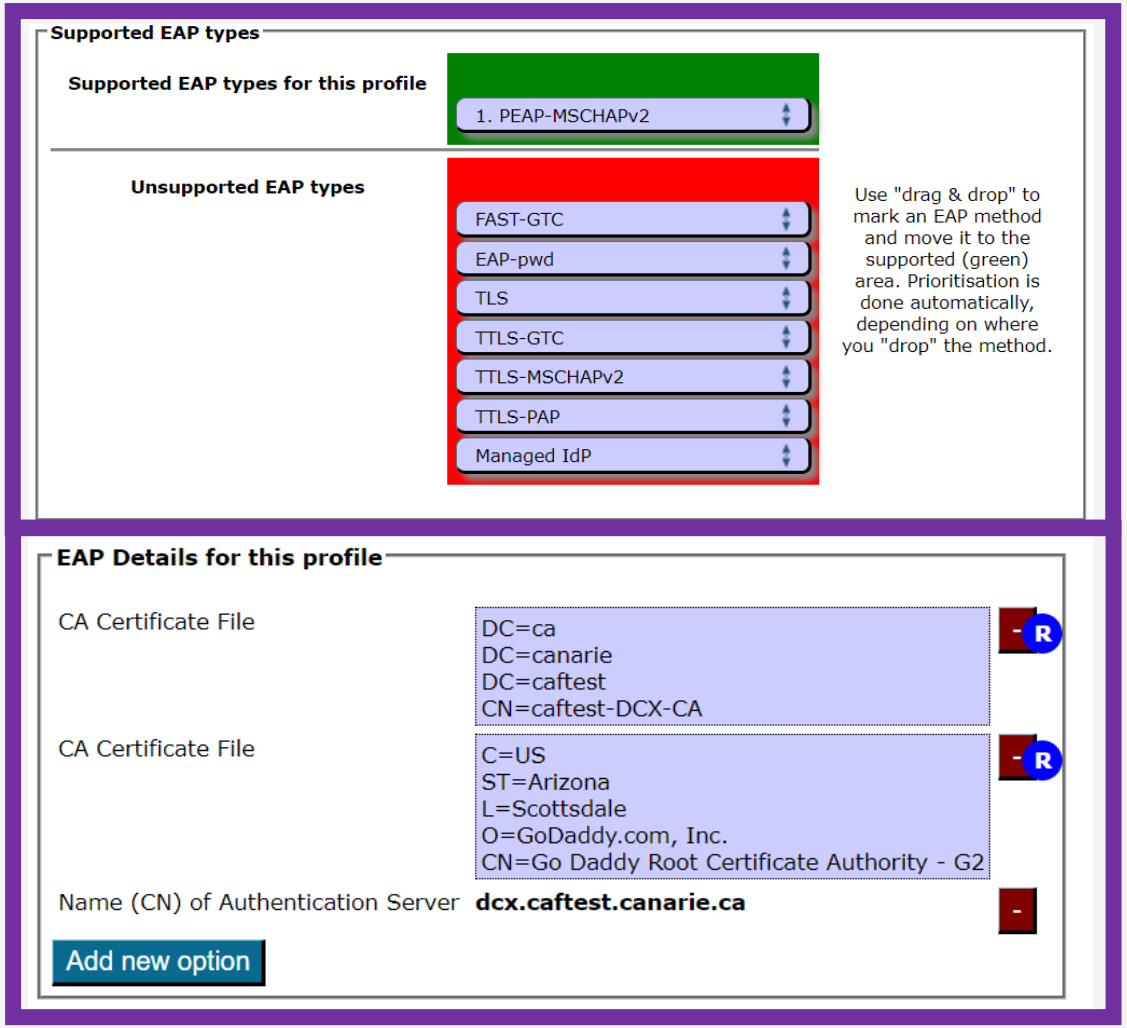
Mitigation – Next Steps

- Device Configuration
  - Setup eduroam CAT Profile
  - User device enrolment

- Enforcement
  - For an institution
  - For roaming

Mitigation: Device Configuration
Set Up eduroam CAT Profile





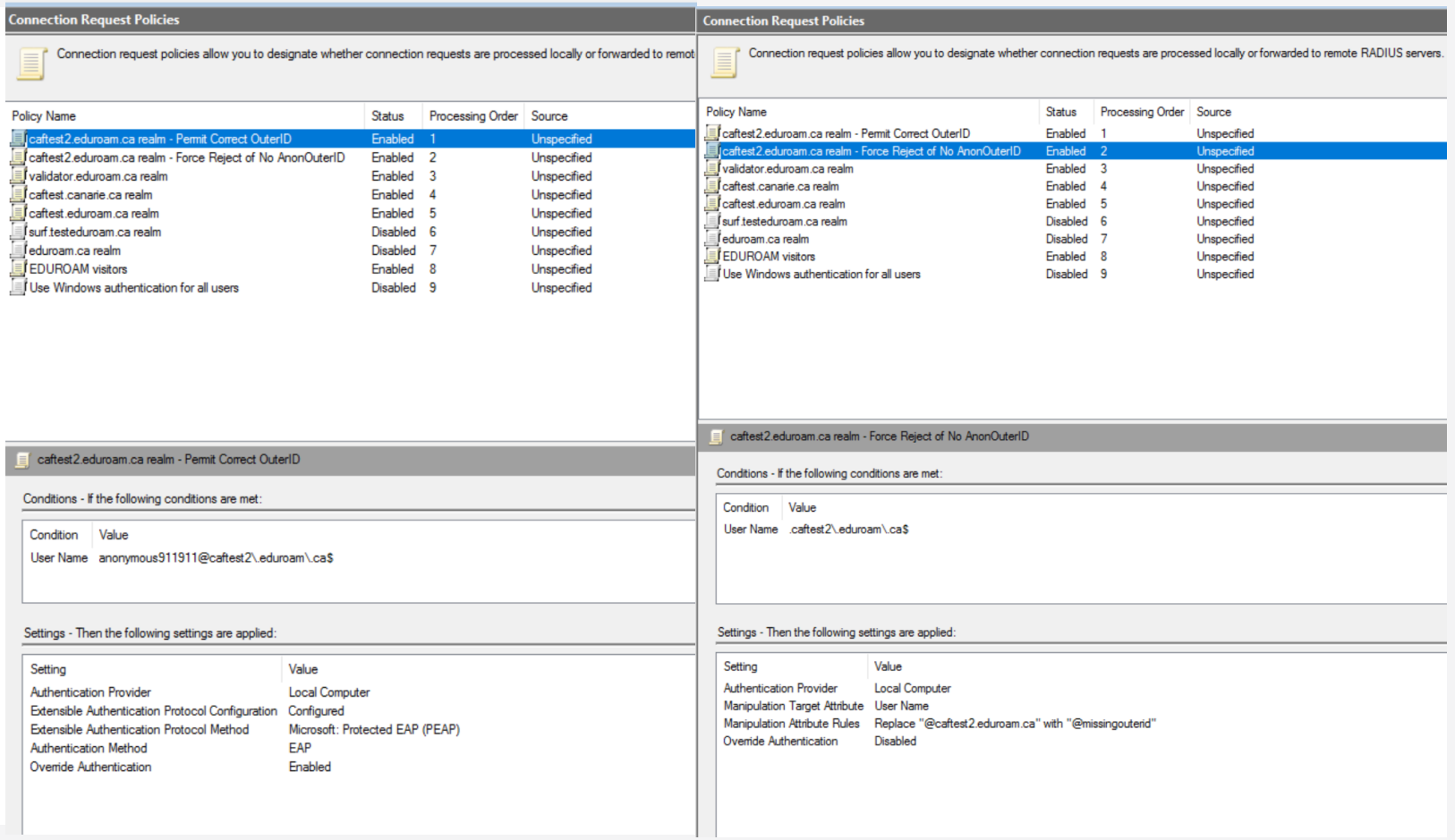
https://cat.eduroam.org/

Mitigation: Device Configuration
User Device Enrolment

- Android 11+/Apple/Microsoft
  - geteduroam.app / App Stores
- Linux, Android 4.3-10, ChromeOS
  - https://cat.eduroam.org

Mitigation: Enforcement Institution

- Audit
- Communicate
- Enroll
- Enforce

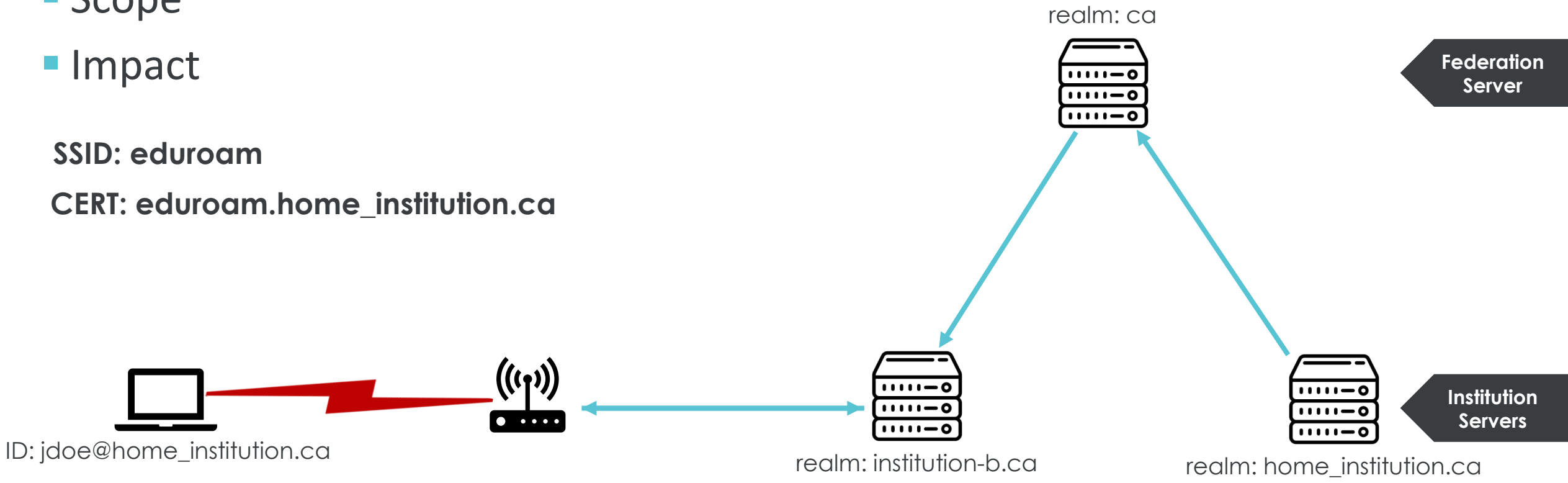


Mitigation: Enforcement
Roaming via the Canadian Access Federation (CAF)

- Enforce Anonymous Outer ID
- Scope
- Impact

SSID: eduroam

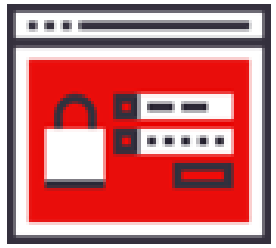
CERT: eduroam.home_institution.ca



Phishing is not tolerated.

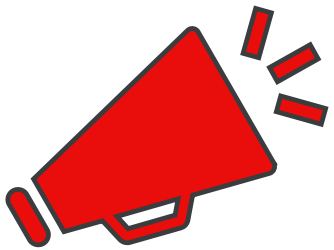
eduroam Wi-Fi credential harvesting shouldn't be either.

Conclusion



Configure

CAT Profile



Communicate

Educate users on geteduroam app (Apple, Android, Microsoft)

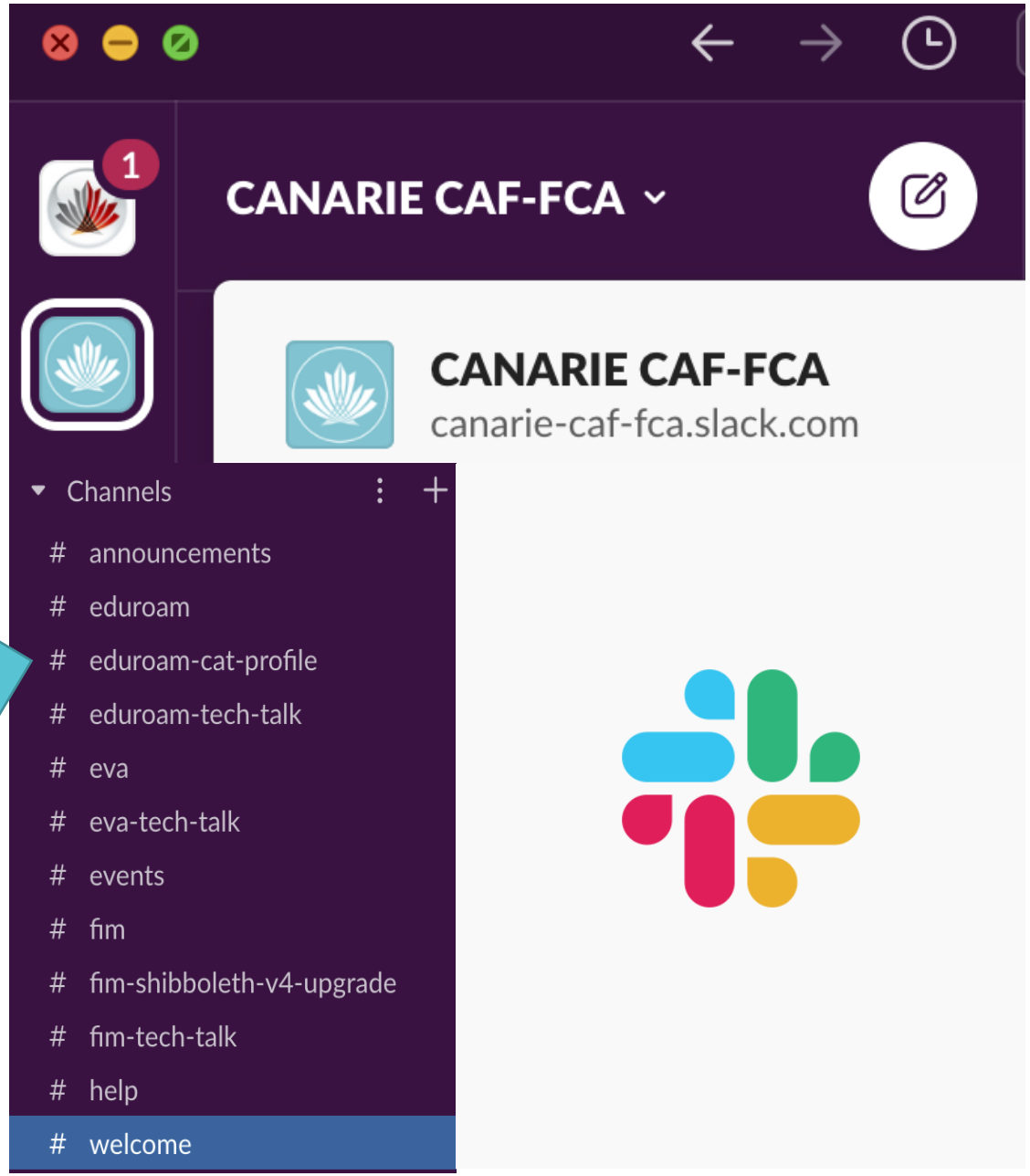
or

cat.eduroam.org (Linux etc.)

Start Enforcement

Deny access

Let's continue the conversation!




A
Q

canarie

canarie.ca | @canarie_inc

CAF Support: tickets@canarie.ca

ed.kingscote@canarie.ca