UAM

Universidad Autónoma de Madrid

Carlos Maqueda Aroca
Nicolás Velázquez Campoy
Víctor Barahona Cabezón
Unidad Técnica de Comunicaciones Tecnologías de la Información

Grupos de Trabajo RedIRIS
Zaragoza junio 2023

IMPLEMENTACIÓN EDUROGUE EN LA RED INALÁMBRICA DE LA **UAM**

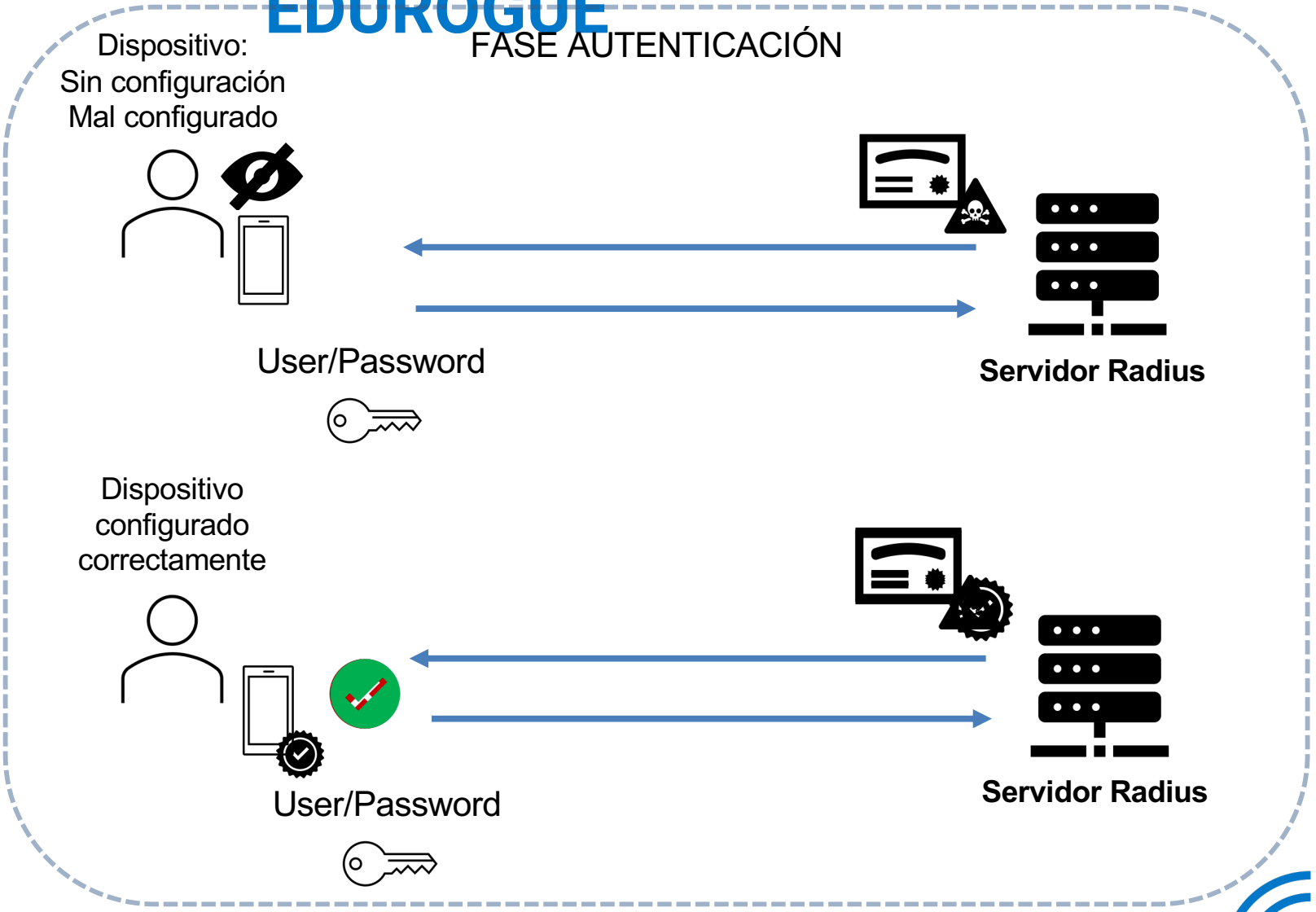
RECORDEMOS QUE ES EDUROGUE

Edurogue fue presentado en los Grupos de Trabajo de RedIRIS en 2017 por **Alberto Martínez** de la Universidad de Deusto.

Alberto realizó una demostración de una suplantación del servicio de autenticación en un freeRadius y se pudo comprobar como las credenciales eran expuestas, lo que supone un riesgo de seguridad.

Los dispositivos configurados incorrectamente son vulnerables al robo de credenciales ante un Man-in-the-Middle, como se ha comentado recientemente en la lista de TECNIRIS.

MECÁNICA DE EDUROGUE

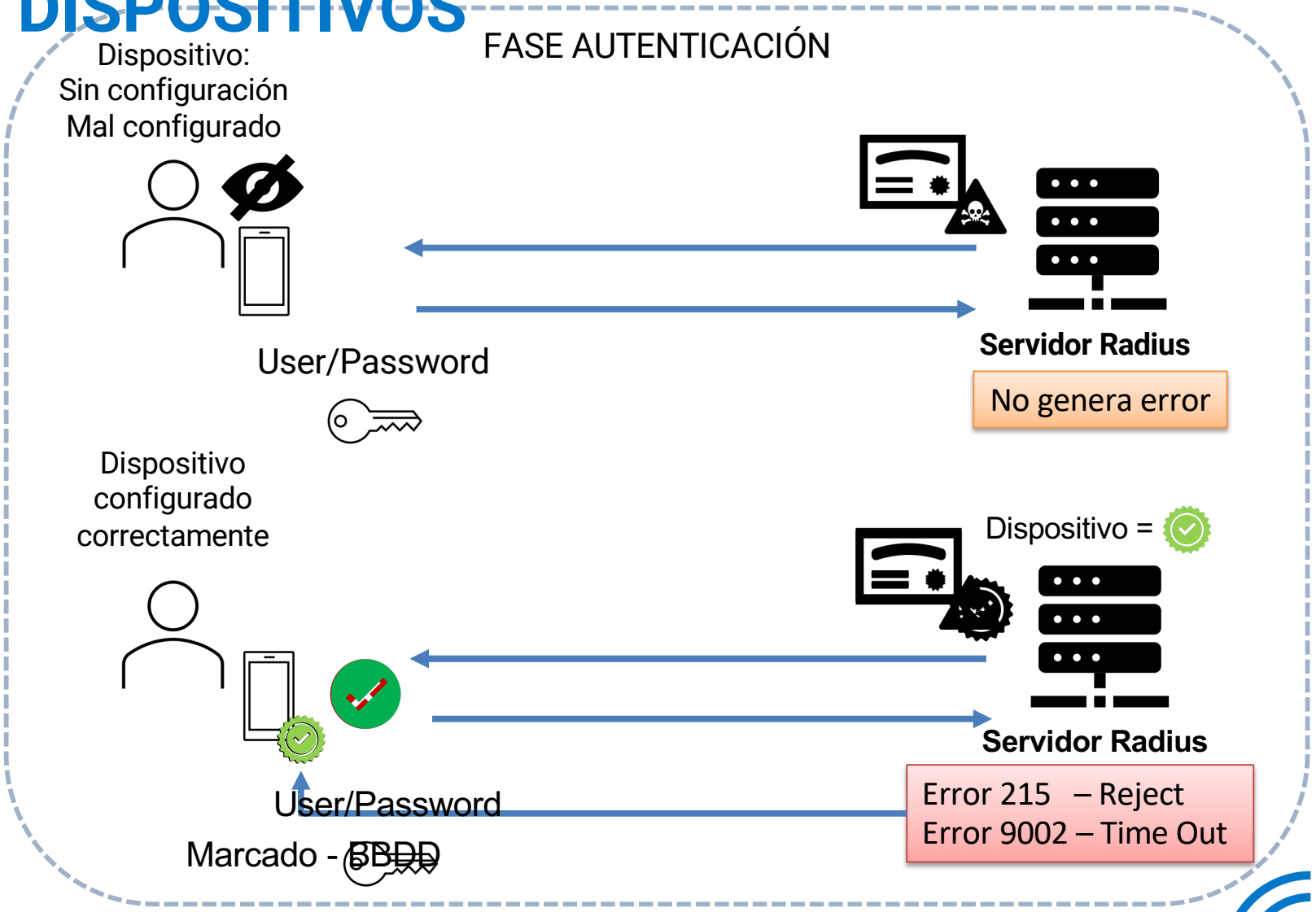


eduroam

CONSIDERACIONES PREVIAS

- El Radius de la UAM está gestionado por ClearPass.
- Se realiza un despliegue gradual y controlado por edificios.
- No es posible saber de forma remota o externa si un dispositivo está configurado correctamente.
- La solución diseñada simula un servidor no legítimo para comprobar el comportamiento o respuesta de los dispositivos en la fase de autenticación en el ClearPass.
- Utilizamos esta respuesta o comportamiento como condiciones para “suponer” que dispositivos no son vulnerables.
- Los dispositivos validados vuelven a ser evaluados pasado un mes.
- El objetivo es descubrir cuáles y cuántos dispositivos tiene una configuración incorrecta y poder tomar decisiones de actuación más adelante.
- En la configuración 802.1X de la UAM utilizamos una CA propia y la identidad anónima *anonymous042021@uam.es* para identificar la versión del perfil definido en eduroam CAT.

COMPORTAMIENTO DE LOS DISPOSITIVOS



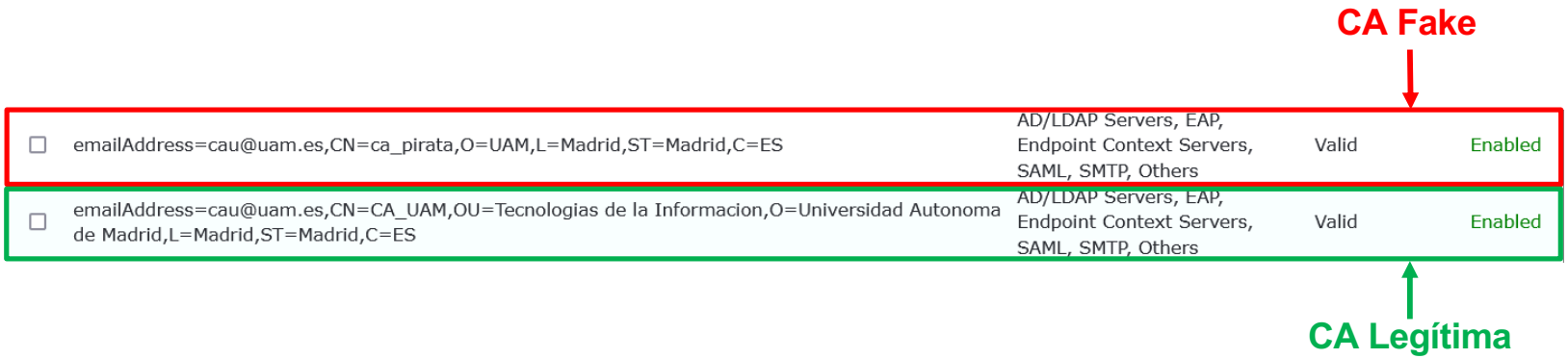
eduroam

CONFIGURACIÓN DE EDUROGUE EN EL RADIUS DE LA UAM

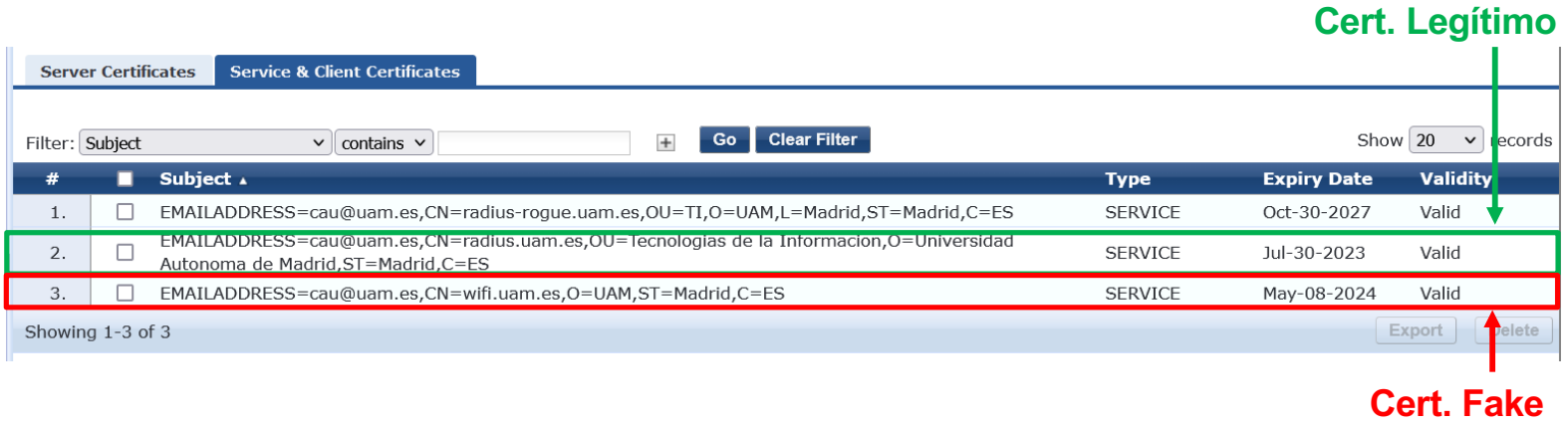
UAM Universidad Autónoma de Madrid

Certificado legítimo y Certificado fake

Importación de la Autoridad de Certificación: CA fake y CA legítima.



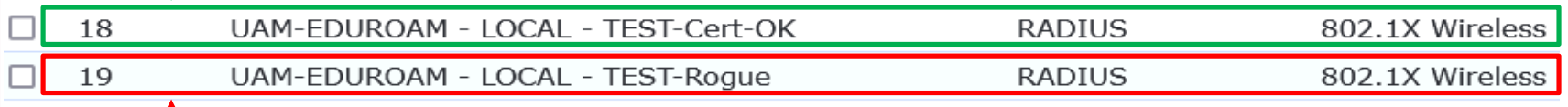
Creación de los Servicios de certificado



Servicios de autenticación

Disponemos de 2 servicios de autenticación.

Servicio legítimo de autenticación (más restrictivo)



Servicio Fake de autenticación (menos restrictivo)

- ClearPass procesa las peticiones de autenticación de forma secuencial, similar a las ACLs.
- El servicio fake es más genérico para así procesar todas las peticiones iniciales al ser menos restrictivo.
- El servicio legítimo sólo procesará las posteriores peticiones si el dispositivo está “marcado” como correcto.

Servicio Fake de autenticación

La **primera petición** de autenticación de un dispositivo será procesada por el servicio ***Rogue***

Reglas para entrar al servicio

Regla opcional para integración gradual por AP-Groups

Services - UAM-EDUROAM - LOCAL - TEST-Rogue

Summary | Service | Authentication | Authorization | Roles | Enforcement

	Type	Name	Operator	Value
1.	Radius:Aruba	Aruba-Essid-Name	EQUALS	eduroam
2.	Radius:Aruba	Aruba-AP-Group	MATCHES_REGEX	(Ciencias|EPS.+)
3.	Radius:IETF	User-Name	CONTAINS	uam.es

Authentication:

Authentication Methods:	1. [EAP TTLS] 2. [PAP]
Authentication Sources:	UAM LDAP [Generic LDAP]
Strip Username Rules:	-
Service Certificate:	EMAILADDRESS=cau@uam.es,CN=wifi.uam.es,O=UAM,ST=Madrid,C=ES

Cert. Fake

Authorization:

Authorization Details:	[Time Source] [Local SQL DB]

Roles:

Role Mapping Policy:	UAM - ROLES WIFI - CheckCertificado

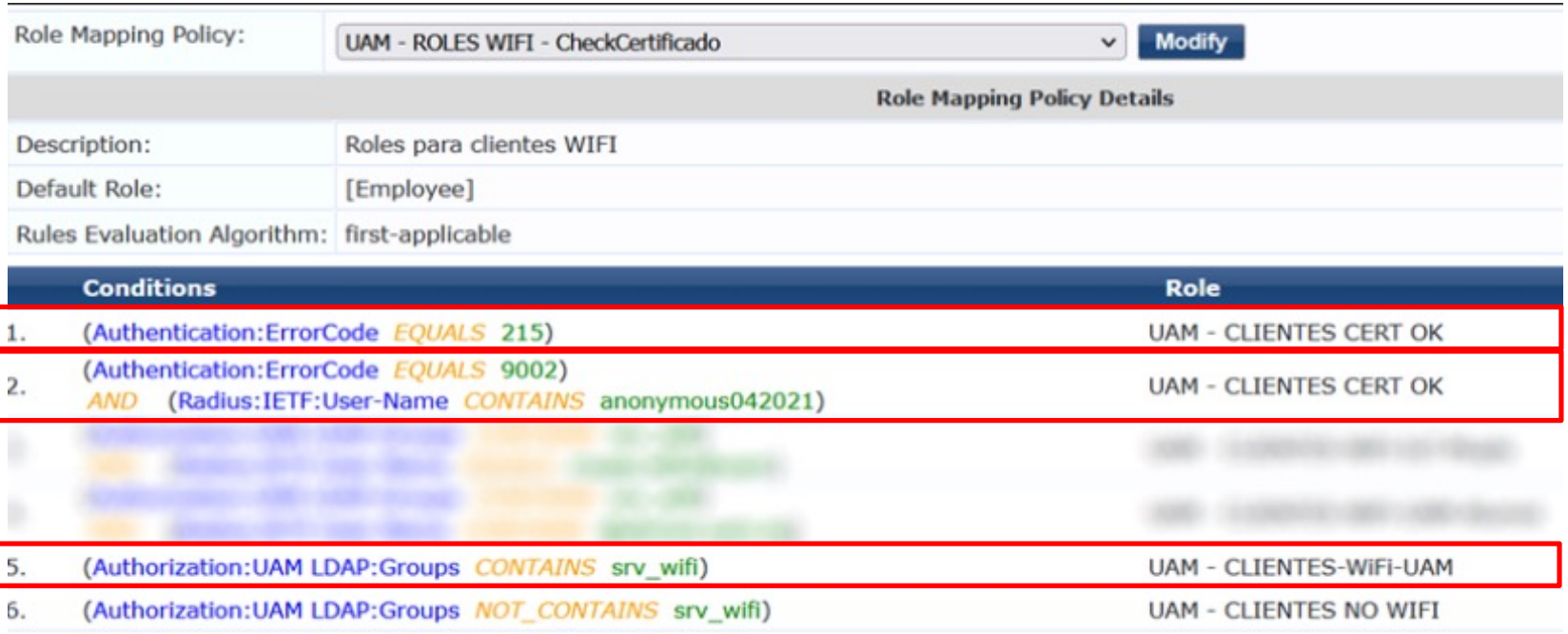
Enforcement:

Use Cached Results:	Disabled
Enforcement Policy:	UAM-ENFORCEMENT WiFi EDUROAM LOCAL - CheckCertificado

Servicio Fake de autenticación

Después de presentar el certificado fake al dispositivo, el proceso de autenticación deriva en 3 escenarios posibles:

- **Error 215**: el dispositivo **no entrega las credenciales** y en su lugar envía la outer-identity que provoca un REJECT. Se le asigna el role: **UAM – CLIENTES CERT OK**
- **Error 9002**: el dispositivo no continua el proceso y provoca un TIME-OUT y si la outer-identity es anonymous042021@uam.es se le asigna el role: **UAM – CLIENTES CERT OK**
- **Ningún error**: el dispositivo continua el proceso. Si las credenciales en LDAP tienen permisos de conexión WiFi, se le asigna el role: **UAM – CLIENTES-WiFi-UAM**



Servicio Fake de autenticación

Según el role asignado se ejecutan las siguientes acciones:

- **Role**: **UAM – CLIENTES-WiFi-UAM**: se envía un *ACCEPT*, el *ROLE* y el *USERNAME* a la controladora.

Enforcement Policy: UAM-ENFORCEMENT WiFi EDUROAM LOCAL - CheckCertificado [Modify] Add New Enfc

Enforcement Policy Details

Description:	Clientes WIFI Eduroam Local
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
2.	(Tips:Role EQUALS UAM - CLIENTES-WiFi-UAM)	UAM-Role-CLIENTES-WiFi-UAM
4.	(Tips:Role EQUALS UAM - CLIENTES NO WIFI)	UAM-USERNAME, [ArubaOS Wireless - Terminate Session]
5.	(Tips:Role EQUALS UAM - CLIENTES CERT OK)	UAM-Certificado-OK, [ArubaOS Wireless - Terminate Session]

Enforcement Profiles - UAM-Role-CLIENTES-WiFi-UAM

Summary | Profile | Attributes

Profile:

Name:	UAM-Role-CLIENTES-WiFi-UAM
Description:	Entregar Aruba Role Role-Clientes-WiFi-UAM
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	Clientes-WiFi-UAM
2.	Radius:IETF	User-Name	=	%{Authentication:Username}

Servicio Fake de autenticación

Según el role asignado se ejecutan las siguientes acciones:

- **Role**: **UAM – CLIENTES CERT OK**: se envía un *DISCONNECT* y añadimos 2 atributos a la BBDD de Endpoints: **Cert OK = *True*** y **Cert Date = *Fecha actual + 1 mes***

Enforcement Policy: UAM-ENFORCEMENT WiFi EDUROAM LOCAL - CheckCertificado [Modify] Add New Enfc

Enforcement Policy Details

Description:	Clientes WIFI Eduroam Local
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
2.	(Tips:Role EQUALS UAM - CLIENTES-WiFi-UAM)	UAM-Role-CLIENTES-WiFi-UAM
4.	(Tips:Role EQUALS UAM - CLIENTES NO WIFI)	UAM-USERNAME, [ArubaOS Wireless - Terminate Session]
5.	(Tips:Role EQUALS UAM - CLIENTES CERT OK)	UAM-Certificado-OK, [ArubaOS Wireless - Terminate Session]

Enforcement Profiles - UAM-Certificado-OK

Summary | Profile | Attributes

Profile:

Name:	UAM-Certificado-OK
Description:	Enforcement para marcar el endpoint como chequeado y fijar la fecha de reevaluación.
Type:	Post_Authentication
Action:	
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Endpoint	CertCheck	=	true
2.	Endpoint	CertDate	=	%{Authorization:[Time Source]:One Month DT}

Servicio Legítimo de autenticación

Después de evaluarse el dispositivo y ser *marcado* como dispositivo correctamente configurado, las posteriores peticiones de autenticación serán procesadas por el servicio ***CERT-OK***

Reglas para entrar al servicio

Regla opcional para integración gradual por AP-Groups

Services - UAM-EDUROAM - LOCAL - TEST-Cert-OK

Summary | Service | Authentication | Authorization | Roles | Enforcement

	Type	Name	Operator	Value
1.	Radius:Aruba	Aruba-Essid-Name	EQUALS	eduroam
2.	Endpoint (BBDD)	CertCheck (Atributo)	EQUALS	true (Valor)
3.	Radius:Aruba	Aruba-AP-Group	MATCHES_REGEX	(Ciencias|Economicas|EPS.+)
4.	Radius:IETF	User-Name	CONTAINS	uam.es

Authentication:

Authentication Methods:	1. [EAP TTLS] 2. [PAP]
Authentication Sources:	UAM LDAP [Generic LDAP]
Strip Username Rules:	-
Service Certificate:	EMAILADDRESS=cau@uam.es,CN=radius.uam.es,OU=Tecnologias de la Informacion,O=Universidad Autonoma de Madrid,ST=Madrid,C=ES

Authorization:

Authorization Details:	[Time Source] [Local SQL DB]

Roles:

Role Mapping Policy:	UAM - ROLES WIFI - Cert OK

Enforcement:

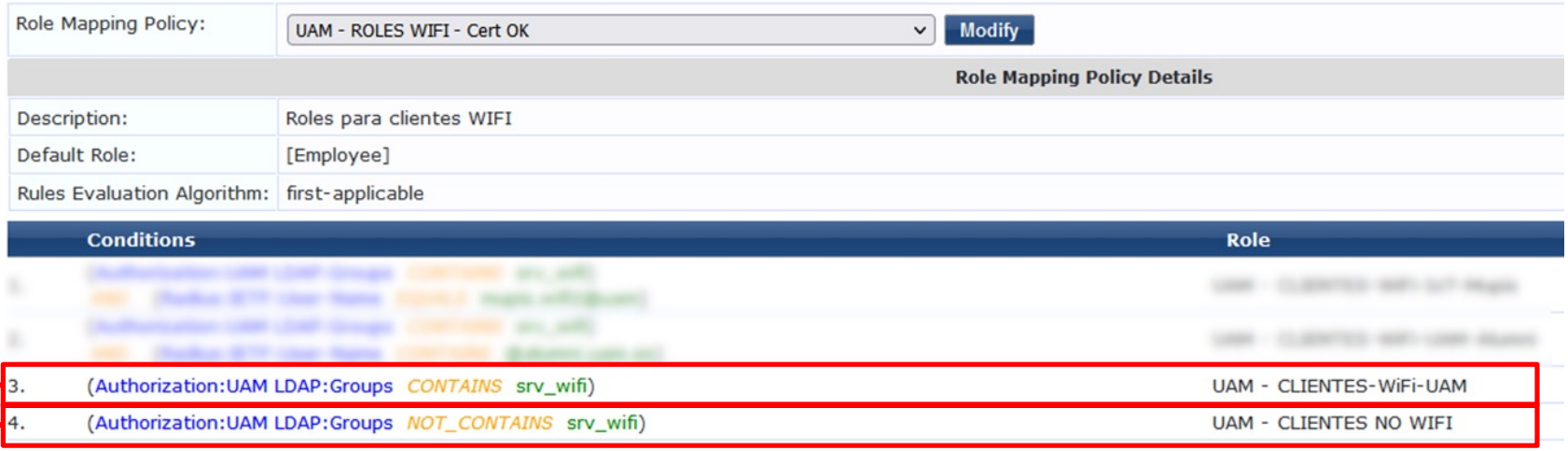
Use Cached Results:	Disabled

Cert. Legítimo

Servicio Legítimo de autenticación

El proceso para la autorización y asignación de roles:

- Si las credenciales en LDAP tienen permisos de conexión WiFi se asigna el role: **UAM – CLIENTES-WiFi-UAM**
- Si las credenciales en LDAP no tienen permisos de conexión WiFi se le asigna el role: **UAM – CLIENTES NO WIFI**



Role Mapping Policy:	UAM - ROLES WIFI - Cert OK	Modify

Role Mapping Policy Details

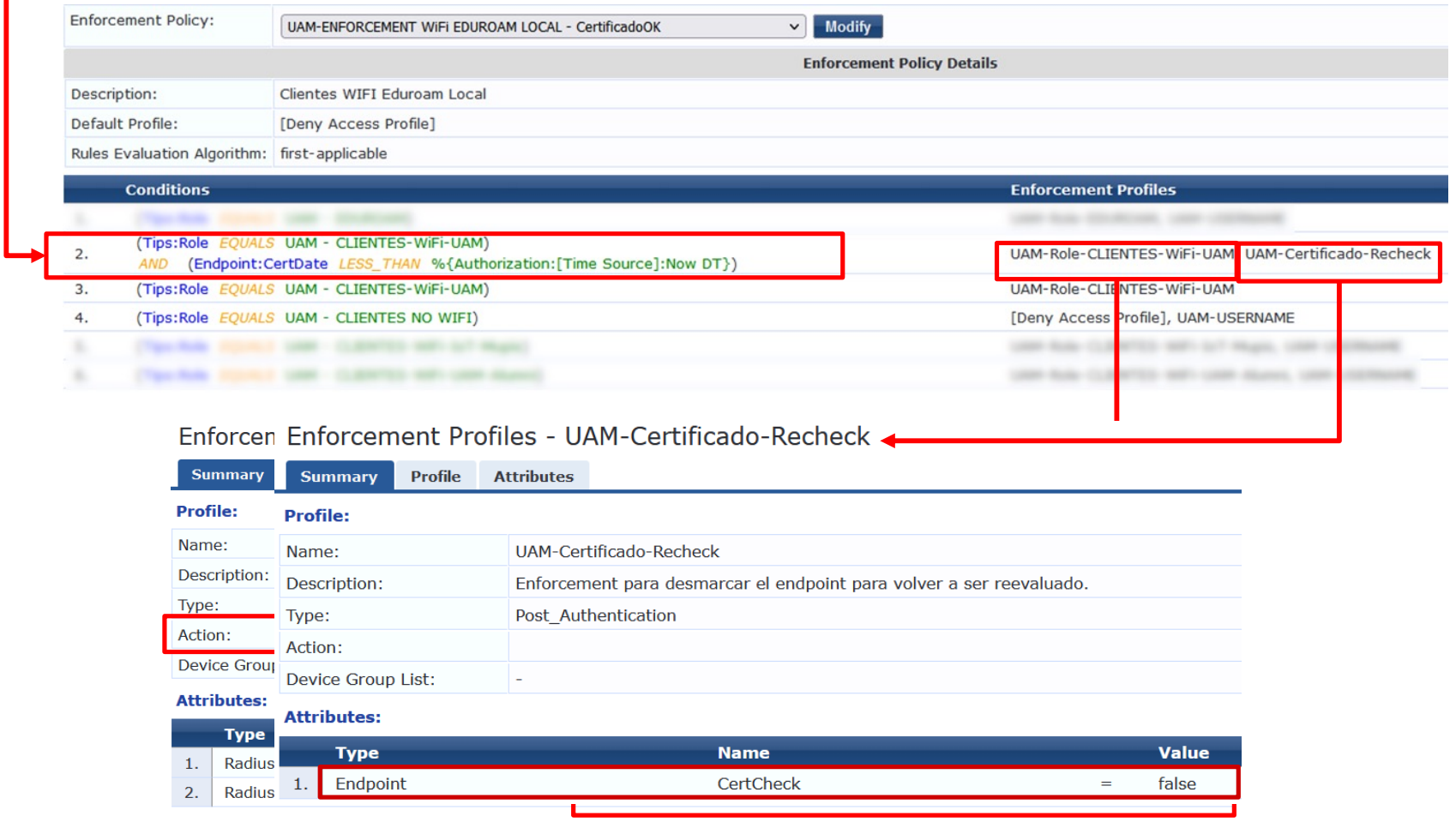
Description:	Roles para clientes WIFI
Default Role:	[Employee]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Role
3.	(Authorization:UAM LDAP:Groups *CONTAINS* srv_wifi)	UAM - CLIENTES-WiFi-UAM
4.	(Authorization:UAM LDAP:Groups *NOT_CONTAINS* srv_wifi)	UAM - CLIENTES NO WIFI

Servicio Legítimo de autenticación

Según el role asignado se ejecutan las siguientes acciones:

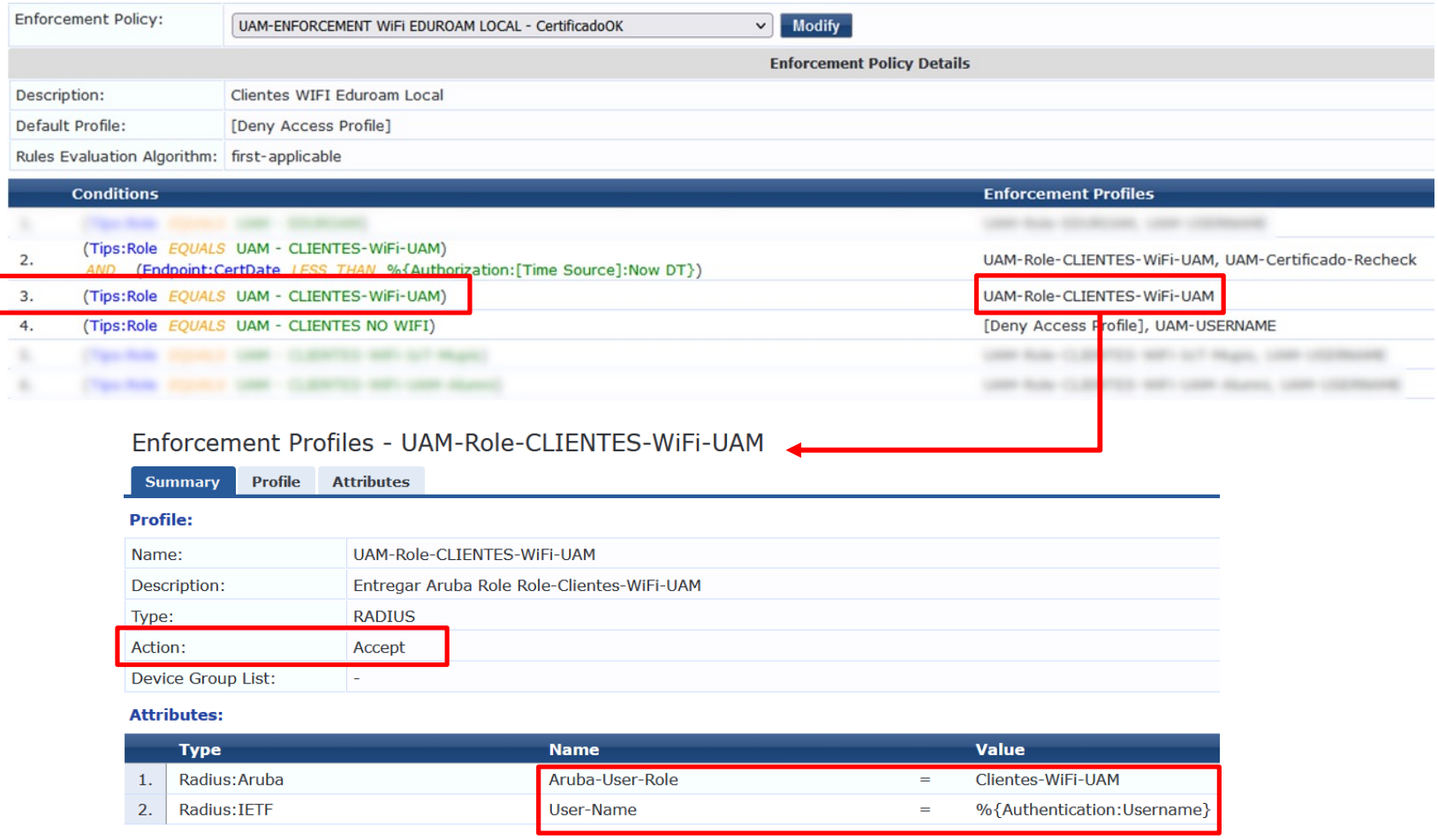
- Si el role es **UAM – CLIENTES-WiFi-UAM** y la fecha del atributo **CertDate** es anterior a la fecha actual: se envía un *ACCEPT,* el *ROLE* y el *USERNAME* a la controladora, y se cambia el atributo **CertCheck** al valor ***False*** para volver a evaluar al dispositivo en la siguiente conexión.



Servicio Legítimo de autenticación

Según el role asignado se ejecutan las siguientes acciones:

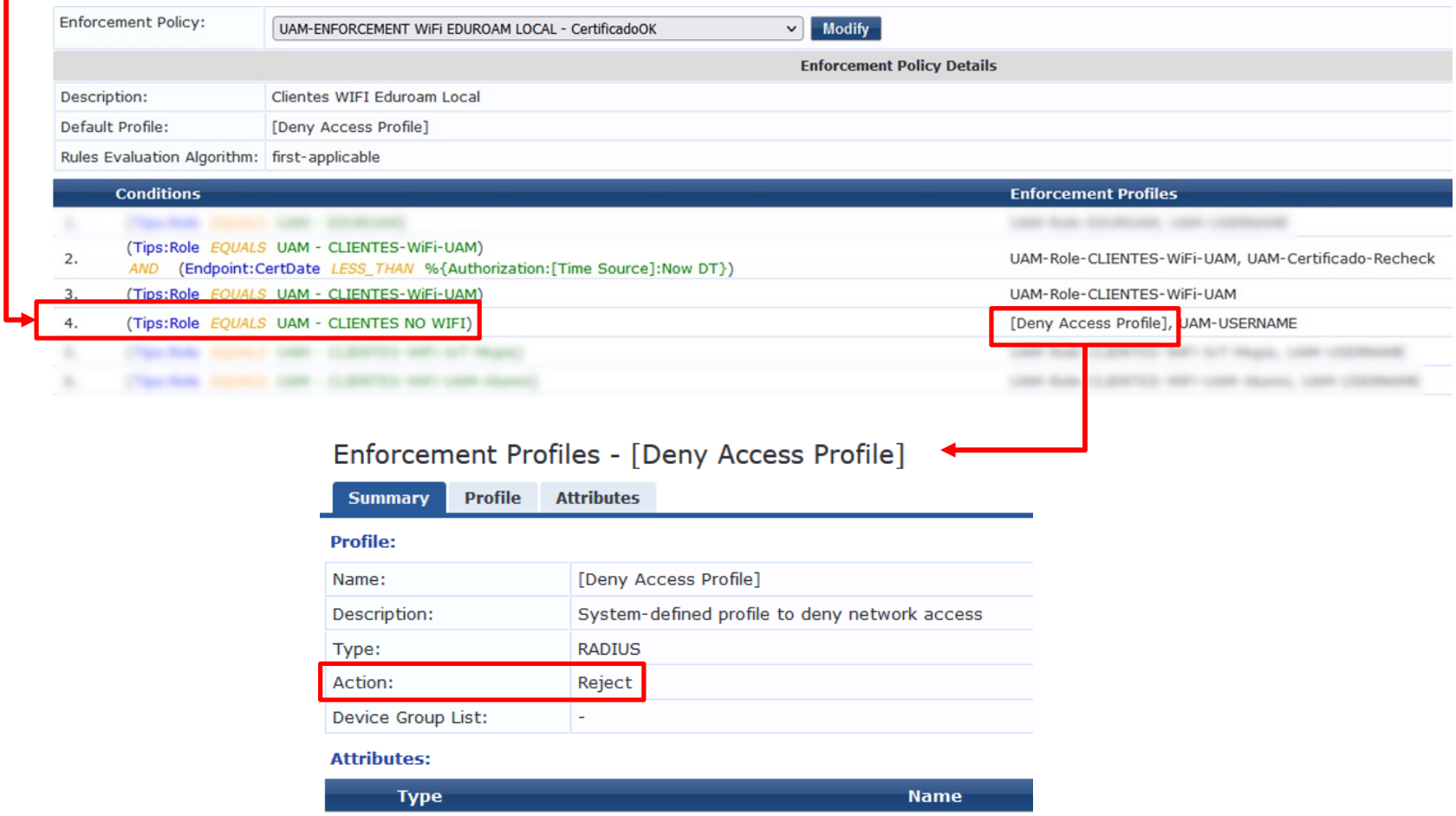
- Si el role es **UAM – CLIENTES-WiFi-UAM** y la fecha del atributo **CertDate** es posterior a la fecha actual: se envía un *ACCEPT*, el *ROLE* y el *USERNAME* a la controladora.



Servicio Legítimo de autenticación

Según el role asignado se ejecutan las siguientes acciones:

- Si el role es **UAM – CLIENTES- NO WIFI**: se envía un *REJECT* a la controladora.



Enforcement Policy: UAM-ENFORCEMENT WiFi EDUROAM LOCAL - CertificadoOK [Modify]

Enforcement Policy Details

Description:	Clientes WIFI Eduroam Local
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
2.	(Tips:Role EQUALS UAM - CLIENTES-WiFi-UAM) AND (Endpoint:CertDate LESS_THAN %{Authorization:[Time Source]:Now DT})	UAM-Role-CLIENTES-WiFi-UAM, UAM-Certificado-Recheck
3.	(Tips:Role EQUALS UAM - CLIENTES-WiFi-UAM)	UAM-Role-CLIENTES-WiFi-UAM
4.	(Tips:Role EQUALS UAM - CLIENTES NO WIFI)	[Deny Access Profile], UAM-USERNAME

Enforcement Profiles - [Deny Access Profile]

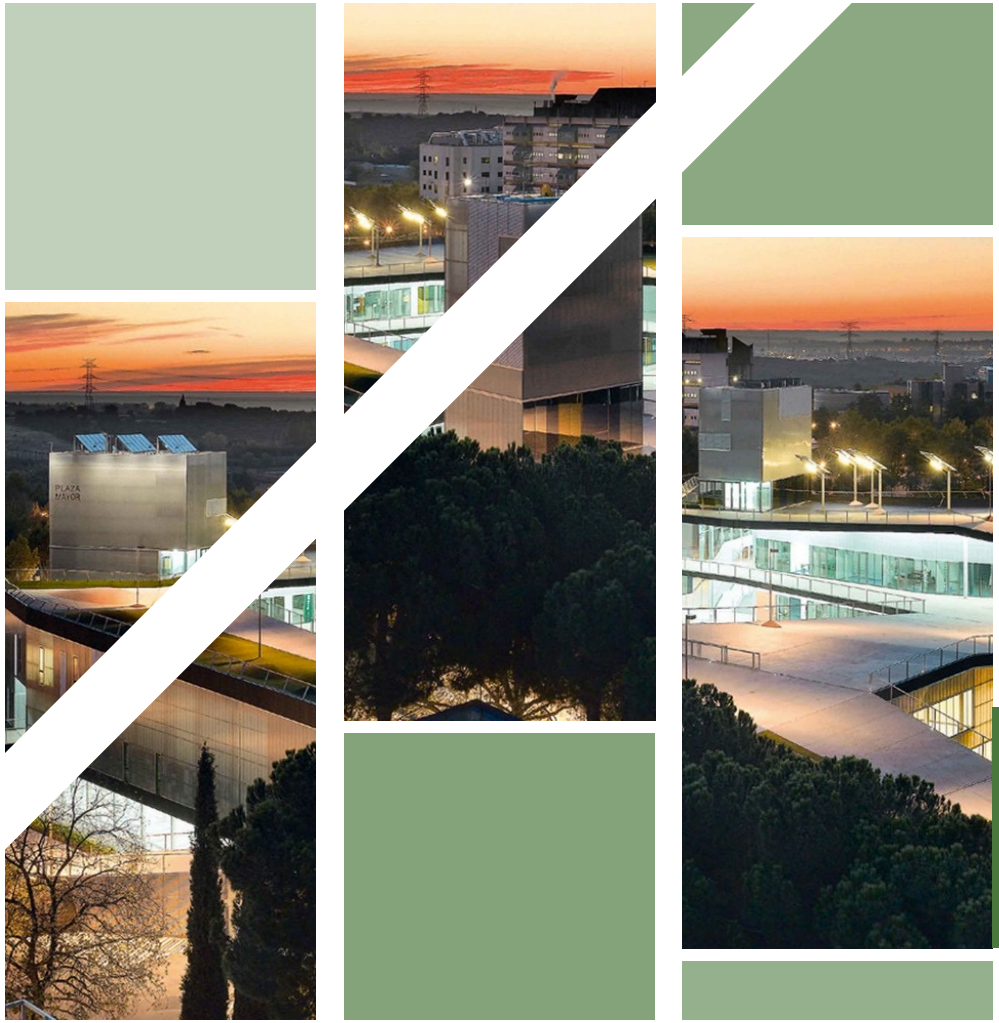
Summary | Profile | Attributes

Profile:

Name:	[Deny Access Profile]
Description:	System-defined profile to deny network access
Type:	RADIUS
Action:	Reject
Device Group List:	-

Attributes:

Type	Name



LOGS DE CONEXIONES

Ejemplo para dispositivo sin configuración

Log de sesión para dispositivo sin configuración:

RADIUS	carlos.maqueda@externo.uam.es	UAM-EDUROAM - LOCAL - TEST-Rogue	ACCEPT	2023/05/16 11:10:40

Summary | Input | Output | Accounting

Login Status:	ACCEPT	
Session Identifier:	R0026f669-13-6463488e	
Date and Time:	May 16, 2023 11:10:40 CEST	
End-Host Identifier:	3C-9C-0F-51-85-60 (Computer / Windows / Windows)	Open in AirWave
Username:	carlos.maqueda@externo.uam.es	
Access Device IP (Port):	172.16.0.152	
Access Device Name:	172.16.0.252 (JANE - IP Priv / Aruba)	
System Posture Status:	UNKNOWN (100)	
Policies Used -		
Service:	UAM-EDUROAM - LOCAL - TEST-Rogue	
Authentication Method:	EAP-TTLS,PAP	
Authentication Source:	Ldap:ldap.uam.es	
Authorization Source:	[Time Source], UAM LDAP	
Roles:	UAM - CLIENTES-WiFi-UAM, [User Authenticated]	
Enforcement Profiles:	UAM-Role-CLIENTES-WiFi-UAM	

Ejemplo para dispositivo configurado: Reject

Logs de sesiones para un dispositivo correctamente configurado:

RADIUS	[redacted]@uam.es	UAM-EDUROAM - LOCAL - TEST-Cert-OK	ACCEPT	2023/05/16 12:37:37
RADIUS	anonymous042021@uam.es	UAM-EDUROAM - LOCAL - TEST-Rogue	REJECT	2023/05/16 12:37:31

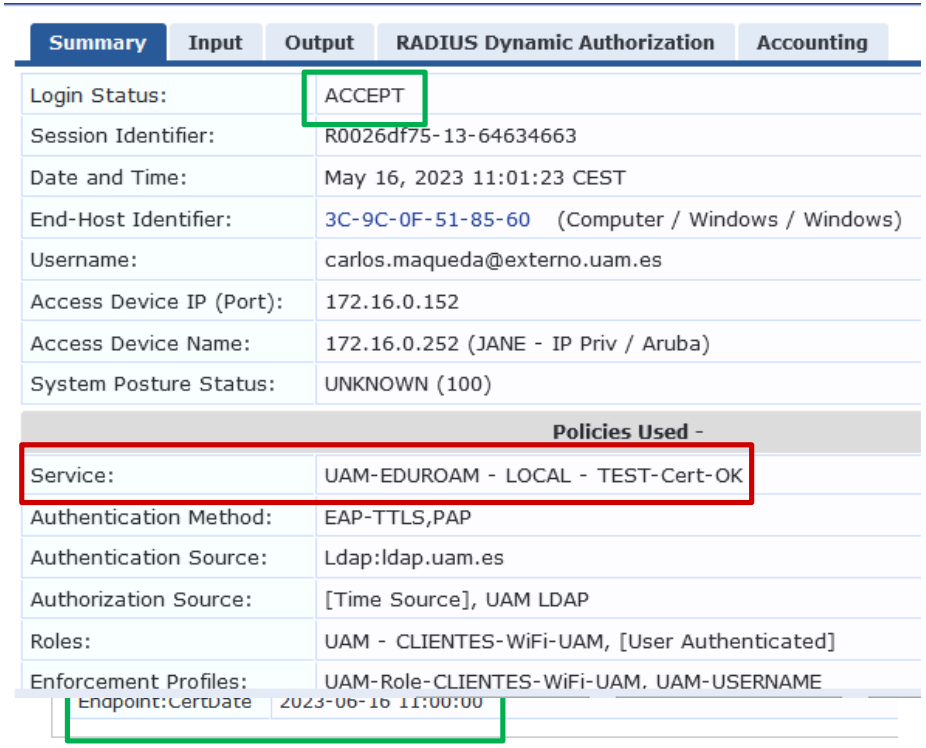
Summary | Input | Output | Accounting

Login Status:	ACCEPT
Session Identifier:	R00279e37-13-64635cf1
Date and Time:	May 16, 2023 12:37:37 CEST
End-Host Identifier:	CE-4A-0E-B6-0A-58 (Generic / Generic / Unclassified Device) Open in AirWave
Username:	[redacted]@uam.es
Access Device IP (Port):	172.16.0.150
Access Device Name:	172.16.0.250
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	UAM-EDUROAM - LOCAL - TEST-Cert-OK
Authentication Method:	EAP-TTLS,PAP
Authentication Source:	Ldap:ldap.uam.es
Authorization Source:	[Time Source], UAM LDAP
Roles:	UAM - CLIENTES-WiFi-UAM, [User Authenticated]

Ejemplo para dispositivo configurado: Time Out

Logs de sesiones para un dispositivo correctamente configurado:

RADIUS	carlos.maqueda@externo.uam.es	UAM-EDUROAM - LOCAL - TEST-Cert-OK	ACCEPT	2023/05/16 11:01:23
RADIUS	anonymous042021@uam.es	UAM-EDUROAM - LOCAL - TEST-Rogue	TIMEOUT	2023/05/16 11:01:16

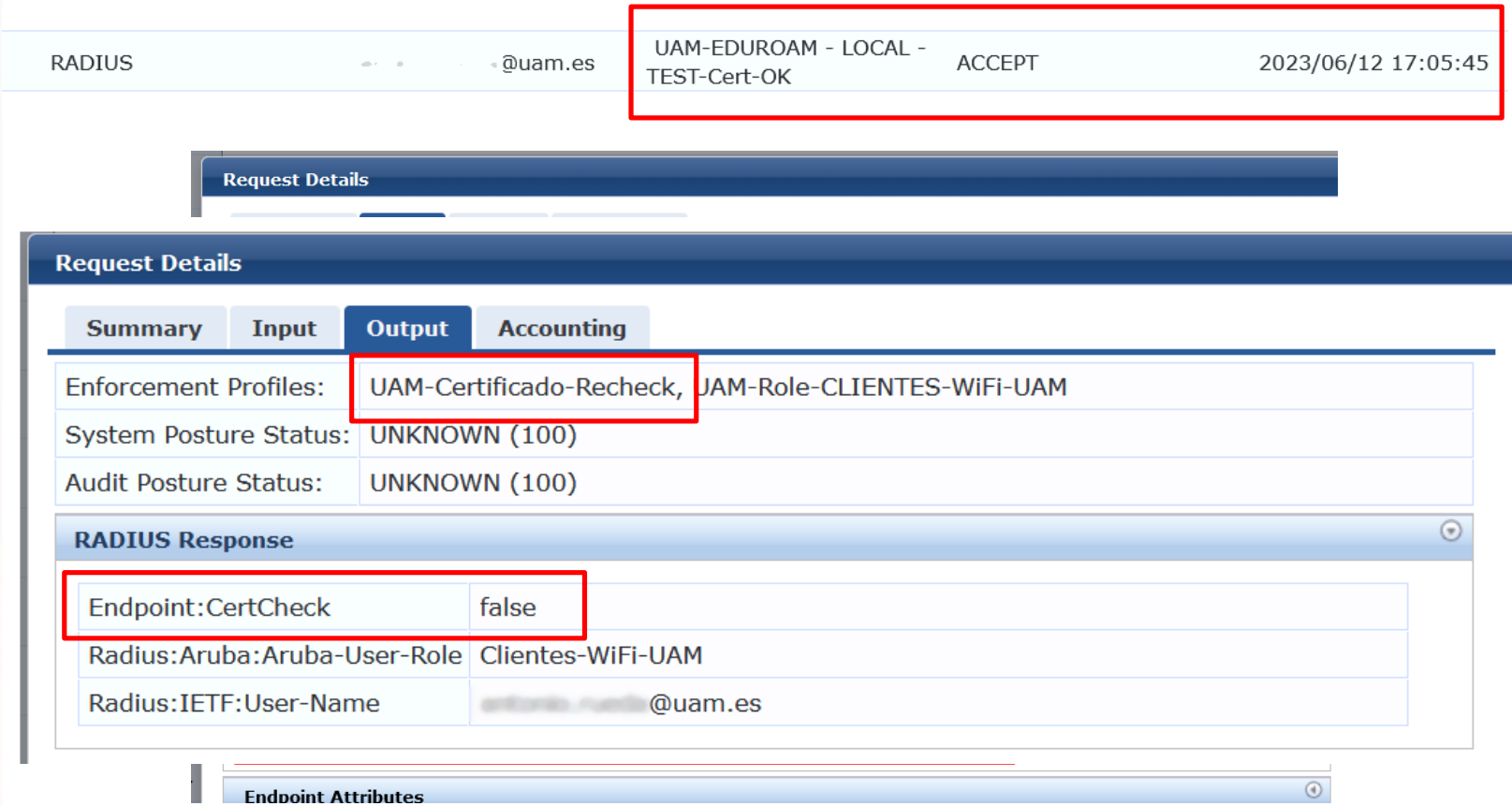


Summary | Input | Output | RADIUS Dynamic Authorization | Accounting

Login Status:	ACCEPT
Session Identifier:	R0026df75-13-64634663
Date and Time:	May 16, 2023 11:01:23 CEST
End-Host Identifier:	3C-9C-0F-51-85-60 (Computer / Windows / Windows)
Username:	carlos.maqueda@externo.uam.es
Access Device IP (Port):	172.16.0.152
Access Device Name:	172.16.0.252 (JANE - IP Priv / Aruba)
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	UAM-EDUROAM - LOCAL - TEST-Cert-OK
Authentication Method:	EAP-TTLS,PAP
Authentication Source:	Ldap:ldap.uam.es
Authorization Source:	[Time Source], UAM LDAP
Roles:	UAM - CLIENTES-WiFi-UAM, [User Authenticated]
Enforcement Profiles:	UAM-Role-CLIENTES-WiFi-UAM, UAM-USERNAME
Endpoint:CertDate	2023-06-16 11:00:00

Ejemplo de revaluación dispositivo configurado

Logs de sesión la revaluación de un dispositivo correctamente configurado:

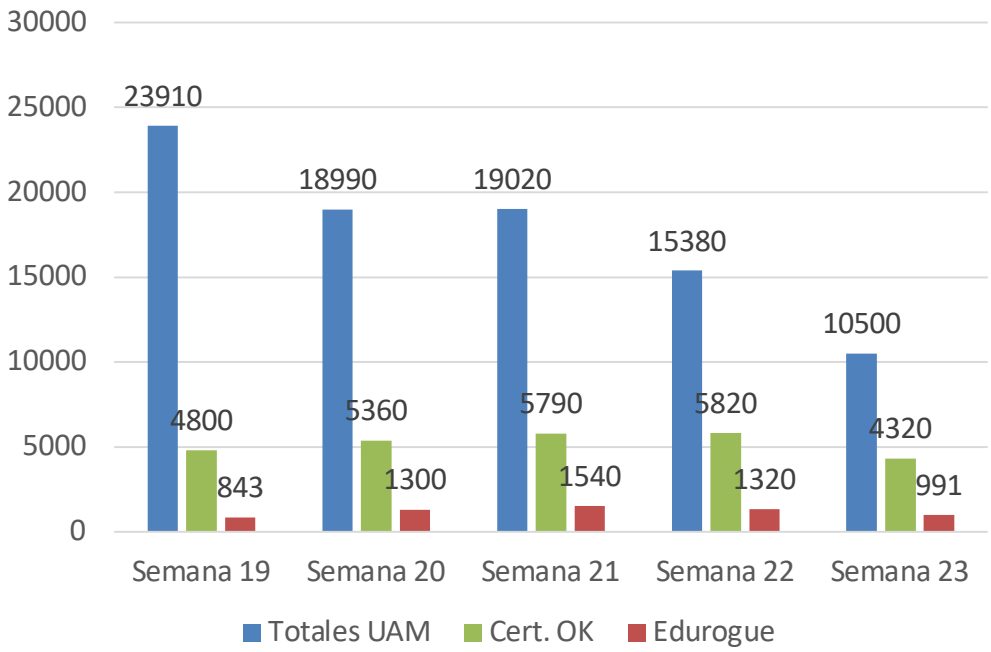


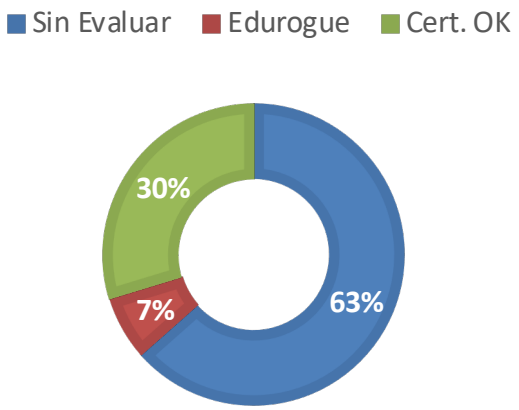
CONCLUSIONES FINALES

UAM Universidad Autónoma de Madrid

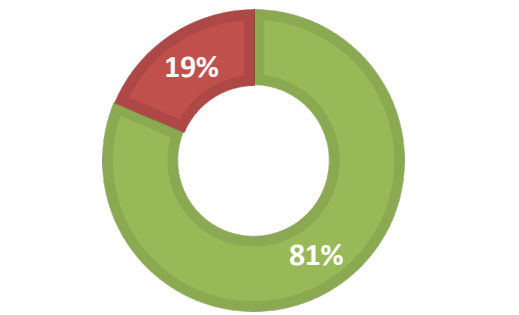
Evolución del despliegue en la UAM

Número de dispositivos desglosado y evolución





Cert OK vs Edurogue



Semana 19: Facultad de Ciencias y EPS
Semana 20: Facultad de Ciencias, EPS y Económicas
Semana 21: Facultad de Ciencias, EPS y Económicas
Semana 22: Facultad de Ciencias, EPS, Económicas, Filosofía y Profesorado
Semana 23: Facultad de Ciencias, EPS, Económicas, Filosofía y Profesorado

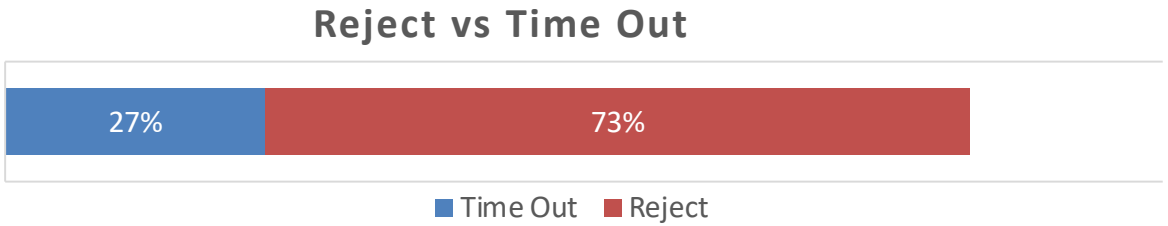
Problemas detectados

- Tiempo de espera elevado establecido por ClearPass para los dispositivos que producen *Time out*. (Pte. Resolver)
- Problemas con certificado fake de máquina autofirmado. Algunos dispositivos sin configuración requerían del certificado validado por una entidad certificadora. (Resuelto)
- Expansión progresiva por facultades. (Resuelto)
- Problemas con el tiempo de validez de dispositivos “marcados”. Establecido inicialmente en 3 meses.
- Penalización a los dispositivos correctamente configurados ya que deben de ser reevaluados cada mes.
- Los dispositivos con Android OS de versiones actuales ya obligan a utilizar certificado en el perfil para redes Enterprise.
- Los dispositivos con sistema operativo Microsoft Windows pasan a ser los dispositivos más vulnerables.

Tareas pendientes

- Finalizar el despliegue a todos los edificios de la UAM.
- Resolver los problemas técnicos:

  - Reducir el tiempo de Time Out que alcanza en algunos casos 1 minuto en producirse.



  - Aumentar el tiempo de validez para la reevaluación.

- Decidir qué hacer con los dispositivos mal configurados (actualmente no estamos actuando, sólo observando):

  - VLAN de cuarentena o un portal cautivo.

  - Email informativo a los usuarios con dispositivos vulnerables.

  - Denegar la conexión a los dispositivos vulnerables.

PREGUNTAS Y DUDAS

Carlos Maqueda Aroca
carlos.maqueda@externo.uam.es

Nicolás Velázquez Campoy
nicolas.velazquez@uam.es

Víctor Barahona Cabezón
victor.barahona@uam.es

UAM

Universidad Autónoma
de Madrid