UÁM	TITULO	Código KDBC 07_05_02	Versión 1.1
Universidad Autónoma	Configuración red cableada autenticada para Linux	Fecha: 07/07/2023	
de Madrid	(Ubuntu)	Página 1 de 6	

Instrucciones de configuración acceso autenticado a la red cableada para Linux (Ubuntu).

Autor:	Revisión y publicación:	Aprobado por:
Carlos Maqueda Aroca	Nicolás Velázquez Campoy	Jefe de Unidad Técnica de
Fecha: 07/07/2023		Comunicaciones
		Miguel Ángel García Martínez



ÍNDICE

1.	Objeto	3
2.	Configuración	3
3.	Solución problema de autenticación en Ubuntu 22.04	6
4.	Registro de cambios	6

Autor:	Revisión y publicación:	Aprobado por:
Carlos Maqueda Aroca	Nicolás Velázquez Campoy	Jefe de Unidad Técnica de
Fecha: 07/07/2023		Comunicaciones
		Miguel Ángel García Martínez



1. Objeto.

El objeto de esta documentación es dar las instrucciones básicas para la configuración en equipos con sistema operativo Linux (Ubuntu) para acceso autenticado a la red cableada mediante el protocolo 802.1X.

Este protocolo tiene como objetivo permitir el acceso a una roseta de red sólo a aquellos usuarios que dispongan de credenciales corporativas <u>ID-UAM</u> válidas, permitiendo un control del acceso a la red en determinadas ubicaciones. La Universidad Autónoma irá extendiendo progresivamente este tipo de acceso a todas las rosetas.

2. Configuración.

• Dirigirse a la siguiente dirección para descargar el certificado:

https://www.uam.es/wifi

• Al final de la sección *Documentación* está disponible para descargar el certificado:

Certificado CA (formato PEM)	业 DESCARGAR [1.83 KB]
Certificado CA (formato DER)	↓ DESCARGAR

• Hacer click con el botón derecho sobre *DESCARGAR* y después en "Guardar como" para guardar el certificado en un directorio de forma permanente y no en un directorio temporal.



• En la barra superior, pulsar sobre el icono de triángulo y después en *Configuración*:

	🔹 🤹 👬 🌒 🖗	98 % -
(1)		_
Ŷ		
÷.		_
<u>^</u>	PCI Ethernet conectada	•
$\mathbf{\nabla}$	eduroam	•
UPD	VPN apagada	•
*	Encendido	•
+1	0:08 para la carga completa (98 %)	•
	Configuración	
	Bloquear	
Ċ	Apagar / cerrar sesión	•

• En la siguiente pantalla, acceder al apartado *Red* y en la sección *802.1x* pulsar sobre la rueda dentada.

Q Configuración ≡	Red	- 0 😣
🗟 Inalámbrica	PCI Ethoroot	4
💿 Red	PCIEthernet	T
Bluetooth	802.1x	
Fondo de escritorio	sin 802.1x 🗸	0
Apariencia	Dirección IPv4 150.244.2.25 Dirección IPv6 fe80::d7a5:a5ce:e890:268	a
Q Notificaciones	Dirección física 48:BA:4E:46:6D:51	
Q Buscar	DNS 150.244.214.200 150.244.2	214.100
III Aplicaciones	USB Ethernet	+
Privacidad	Cable desconectado	
 Cuentas en línea 		
∝° Compartir	VPN	+
♫ Sonido	VPN «VPN-Empresa»	
④ Energía	VPN «VPN-TI»	
Monitores	VPN «VPN-uam»	
🖱 Ratón y panel táctil		
Combinaciones de teclas	Proxy de la red	Apagado 🔘
Impresoras		



• En la siguiente ventana de configuración, se debe seleccionar y completar las opciones indicadas en la siguiente captura de pantalla:

Cancelar			802	.1x	Aplicar
Detalles	Identida	ad IPv4	IPv6	Seguridad	
		Segurida	d 802.1x		
		Auten	ticación	TLS a través de túnel	•
		Identidad a	anónima	anonymous042021@uam.es	
		1	Dominio		
	Γ	Certifi	cado CA	🖻 ca-uam.pem	ē
				🗌 No se necesita la CA del certi	ficado
		Autenticaciór	n interna	PAP	•
		Nombre de	usuario	nombre.apellidos@uam.es	
	_	Cor	ntraseña		?
				Mostrar la contraseña	

- En el campo *Certificado CA* se debe indicar el certificado descargado en el paso 1 de este manual.
- Introducir sus credenciales corporativas <u>ID-UAM</u> (<u>nombre.apellido@uam.es</u> o equivalente).

NOTA: Se recomienda no completar el campo de contraseña en esta ventana de configuración para que así no quede almacenada y sea solicitada cada vez que el equipo se conecte a una red 802.1X.



3. Solución problema de autenticación en Ubuntu 22.04

En la última versión de Ubuntu 22.04 se ha detectado una incompatibilidad en el módulo OpenSSL que impide el correcto funcionamiento en redes 802.1x.

Mientras los fabricantes implementan una solución, se puede llevar a cabo una solución temporal siguiendo los siguientes pasos:

- Editar el fichero: /usr/lib/ssl/openssl.cnf
- Añadir al fichero lo siguiente:

openssl_conf = openssl_init

[openssl_init] ssl_conf = ssl_sect

[ssl_sect] system_default = system_default_sect

[system_default_sect] Options = UnsafeLegacyRenegotiation

- Guardar el documento y ejecutar el siguiente comando:

systemctl restart wpa_supplicant

4. Registro de cambios.

Fecha	Versión	Motivo de cambio	Autor cambio
07/07/2023	1.0	Elaboración del documento	Carlos Maqueda