



Eduroam Istruzioni per l'uso Sistema Operativo Windows 7

Caratteristiche del servizio

Nome del SSID	eduroam
Autenticazione	WPA WPA2
Cifratura	WPA/TKIP/AES WPA2/AES/TKIP
Protocollo	802.1X
Credenziali	[nome_utente]@icar.cnr.it.it

Configurazione Client (1/8)

Cliccare in sequenza su:

- 1. «START»
- 2. «Selezionare Pannello di controllo»
- 3. «Centro di Connessione di Rete e Condivisione»



Configurazione Client (2/8)

Cliccare su

«Visualizza reti senza fili quindi aggiungi»

«creare manualmente profilo di rete»



Configurazione Client (3/8)

1.Inserire il nome della rete «eduroam»



Configurazione Client (4/8)

- Selezionare il tipo tipo di sicurezza (WPA/2 Enterprise)
- 2. Cliccare su «Tipo di crittografia AES»

eduroam - Proprietà ret	e wireless
Connessione Sicurezz	a
Tipo di sicurezza:	WPA2-Enterprise
Tipo di crittografia:	AES 🔹
Scegliere un metodo o Microsoft: PEAP (Pro Memorizza creden accesso	di autenticazione di rete: tected EAP) Impostazioni ziali per la connessione a ogni
Impostazioni avanza	ate

Configurazione Client (5/8)

- 1.Doppio click sulla rete «eduroam» selezionare la scheda sicurezza
- 2. Cliccare su PEAP «impostazioni»

duroam - Proprietà ret	e wireless
Connessione Sicurezza	a
Tipo di sicurezza:	WPA2-Enterprise
Tipo di crittografia:	AES 🔻
Scediere un metodo d	li autenticazione di reter
Microsoft: DEAD (Droi	tected EAD)
Impostazioni avanza	ate

Configurazione Client (6/8)

- 1. Deselezionare «Convalida certificato server»
- Selezionare «Password protetta (EAP-MSCHAPv2)» come metodo di autenticazione
- 3. Cliccare su «Configura…»

Per la connessione: Convalida certificato server Connetti ai server seguenti: Autorità di certificazione radice attendibili: AAA Certificate Services AC Raíz Certicámara S.A. ACEDICOM Root AddTrust Class 1 CA Root AddTrust External CA Root AddTrust Public CA Root AddTrust Public CA Root AddTrust Qualified CA Root Mod Arust Qualified CA Root Non chiedere all'utente di autorizzare nuovi server o autorità di certificazione attendibili. Celezionare il metodo di autenticazione: Password protetta (EAP-MSCHAP v2) Configura	roprietà PEAP		X
Convalida certificato server Connetti ai server seguenti: Autorità di certificazione radice attendibili: Autorità di certificazione radice attendibili: Autorità di certificate Services AC Raíz Certicámara S.A. ACEDICOM Root AddTrust Class 1 CA Root AddTrust Class 1 CA Root AddTrust Public CA Root AddTrust Qualified CA Root AddTrust Qualified CA Root Non chiedere all'utente di autorizzare nuovi server o autorità di certificazione attendibili. Selezionare il metodo di autenticazione: Password protetta (EAP-MSCHAP v2) Configura	Per la connessio	ne:	
Connetti ai server seguenti: Autorità di certificazione radice attendibili: AAA Certificate Services AC Raíz Certicámara S.A. ACEDICOM Root AddTrust Class 1 CA Root AddTrust External CA Root AddTrust Public CA Root AddTrust Qualified CA Root AddTrust Qualified CA Root Mon chiedere all'utente di autorizzare nuovi server o autorità di certificazione attendibili. Selezionare il metodo di autenticazione: Password protetta (EAP-MSCHAP v2) Configura	Convalida	certificato server	
Autorità di certificazione radice attendibili: AAA Certificate Services AC Raíz Certicámara S.A. ACEDICOM Root AddTrust Class 1 CA Root AddTrust External CA Root AddTrust Public CA Root AddTrust Qualified CA Root AddTrust Qualified CA Root Mon chiedere all'utente di autorizzare nuovi server o autorità di certificazione attendibili. Selezionare il metodo di autenticazione: Password protetta (EAP-MSCHAP v2) Configura	Connetti	ai server seguenti:	
AAA Certificate Services AC Raíz Certicámara S.A. ACEDICOM Root AddTrust Class 1 CA Root AddTrust Class 1 CA Root AddTrust External CA Root AddTrust Public CA Root AddTrust Qualified CA Root AddTrust Qualified CA Root INOn chiedere all'utente di autorizzare nuovi server o autorità di certificazione attendibili. Selezionare il metodo di autenticazione: Password protetta (EAP-MSCHAP v2) Configura Abilita riconnessione rapida Imponi Protezione accesso alla rete	Autorità di ce	rtificazione radice attendibili;	
 AC Raíz Certicámara S.A. ACEDICOM Root AddTrust Class 1 CA Root AddTrust External CA Root AddTrust Public CA Root AddTrust Qualified CA Root AddTrust Qualified CA Root Mon chiedere all'utente di autorizzare nuovi server o autorità di certificazione attendibili. Selezionare il metodo di autenticazione: Password protetta (EAP-MSCHAP v2) Configura Abilita riconnessione rapida Imponi Protezione accesso alla rete 	AAA Cer	ificate Services	^
ACEDICOM Root AddTrust Class 1 CA Root AddTrust External CA Root AddTrust Public CA Root AddTrust Qualified CA Root AddTrust Qualified CA Root III Non chiedere all'utente di autorizzare nuovi server o autorità di certificazione attendibili. Selezionare il metodo di autenticazione: Password protetta (EAP-MSCHAP v2) Configura Abilita riconnessione rapida Timponi Protezione accesso alla rete	AC Raíz	Certicámara S.A.	
AddTrust Class 1 CA Root AddTrust External CA Root AddTrust Public CA Root AddTrust Public CA Root AddTrust Qualified CA Root III Non chiedere all'utente di autorizzare nuovi server o autorità di certificazione attendibili. Selezionare il metodo di autenticazione: Password protetta (EAP-MSCHAP v2) Configura Abilita riconnessione rapida Timponi Protezione accesso alla rete	ACEDICO	MRoot	
Add Irust External CA Root AddTrust Public CA Root AddTrust Qualified CA Root AddTrust Qualified CA Root Non chiedere all'utente di autorizzare nuovi server o autorità ci certificazione attendibili. Selezionare il metodo di autenticazione: Password protetta (EAP-MSCHAP v2) Configura Abilita riconnessione rapida Imponi Protezione accesso alla rete	AddTrus	Class 1 CA Root	
Add Trust Public CA Root Add Trust Qualified CA Root Add Trust Qualified CA Root Add Trust Qualified	AddIrus	External CA Root	
Addrivst Qualified CA Root A	AddIrus	Public CA Root	100
Non chiedere all'utente di autorizzare nuovi server o autorità di certificazione attendibili. Selezionare il metodo di autenticazione: Password protetta (EAP-MSCHAP v2) Configura Abilita riconnessione rapida Imponi Protezione accesso alla rete	Adurrus		
Password protetta (EAP-MSCHAP v2) ▼ Configura ✓ Abilita riconnessione rapida Imponi Protezione accesso alla rete	Non chied di certifica Selezionare il m	ere all'utente di autorizzare nuovi se zione attendibili. etodo di autenticazione:	erver o autorità
Abilita riconnessione rapida Imponi Protezione accesso alla rete	Password prot	etta (EAP-MSCHAP v2)	▼ Configura
Imponi Protezione accesso alla rete	Abilita ricon	nessione ranida	
	Imponi Prote	zione accesso alla rete	

Configurazione Client (7/8)

- Deselezionare «Utilizza automaticamente il nome di accesso...»
- 2. Cliccare su «OK»
- 3. Impostazioni avanzate selezionare scheda 802.1X

Proprietà PEAP	23
Proprietà EAP MSCHAPv2	
Per la connessione: Utilizza automaticamente il nome utente, la password e, se disponibile, il dominio di accesso a Windows. OK Annulla	
AddTrust Class 1 CA Root	
AddTrust Public CA Root	
Add Irust Qualified CA Root	T

Configurazione Client (8/8)

 Cliccare su «specifica la modalità di autenticazione» quindi «autenticazione utente»
 Inserire le credenziali ICAR in vostro possesso
 Salvare le impostazioni.

nnessio	one Impostaz	ioni 802.1X	Impostazi	oni 802.11			
ipq .			modalita di	autenticazi	one:		
ipt _	curezza di Wind	lows	-		1.000		
	Salva crede	enziali					
	Il salvataggio d	delle creder	nziali cons	ente la cor	nessione del	computer alla	
	aggiornament	i.	e conness	o, ad esen	ipio per il do	whicad di	
ice							
Mid		[il tuo u	(ername@	icar oprit			
v		In tuo us	semannew	icanchini	=		
		•••••					
					OK	Annulla	
Impos	stat						
Impor							

Buona navigazione con...





