## eduroam設定方式說明

Android平台設定方式如下:

⊕ <b>€</b>		Ĺ	?≑∎	下午 <b>4:48</b>
Ξ \	eduroam			
開啟	訊號強度 優			
iNSRF 已連線	安全性 <b>802.1x EAP</b> EAP 方法			(((.
NSRR	PEAP		•	(((-
巳1話仔	階段2驗證			
eduro	MSCHAPV2		•	(ie
NSRR	CA 憑證			(((•
NSRR	不進行驗證		•	(((-
NODE	您未指定任何您證,因此無为 身分	<b>公</b> 為您設定私人建線。		
NSKR	xxx@nsrrc.org.tw			•
NSRR	匿名身分			(((-
TANe				(((•
DIREC	密碼			(70
NSRR	顯示密碼			(•
ARPE	進階選項		~	
	取消	連線		
+ ,,,	こっ日 ミットロ			
	<b>5</b> 1			

「EAP方法」選用「PEAP」。

「 階段2驗證 」選用「 MSCHAPV2 」。

「CA憑證」選用「不進行驗證」。

「身份」輸入中心AD帳號,格式為xxx@nsrrc.org.tw。

「匿名身份」無需輸入。

「密碼」輸入中心AD帳號之密碼。

## Windows 平台設定方式如下,以 Win 10 為例:

設定			- 🗆 X
	Windo	ows 設定	
	尋找設定	٩	
▲ 糸統 顯示器、音效、通知、電源		<b>電話</b> 連結您的 Android ∖ iPhone	網路和網際網路 Wi-Fi、飛航模式、VPN
個人化	<b>應用程式</b> 解除安裝、預設值、腦用功能	幌戶 您的嗎戶、電子鄧件、同步設定、工作、家庭	<b>好了 時間與語言</b> 語言、地區、日期
び載 遊戯列、DVR、直播、遊戯模式	軽鬆存取     朗康程式、放大鏡、高對比	☐ 隱私權 位置、相機	更新與安全性 Windows Update、復原、備份
✓ 搜尋 語言、權限、應程記錄			

Step1. 開啟「Windows 設定」視窗,點選「網路和網際網路」。

Step 2. 點選「網路和共用中心」。

←設定		_	×
命 首頁	狀態		
尋找設定 。	網路狀態		
網路和網際網路	Π		
₿ 狀態			
<i>ſſ</i> ≈ Wi-Fi	未連線		
<b>聖</b> 乙太網路	您未連線到任何網路。		
☞ 撥號			
% VPN	觀不可用的網路		
♪ 飛航模式	變更您的網路設定		
(小) 行動熱點	變更介面卡選項 檢視網路介面卡及變更連線設定。		
└ 數據使用量	共用選項 對於您連線的網路,決定您要共用的項目。		
Proxy	檢視您的網路內容		
	Windows 防火牆		
	網路和共用中心		

Step 3. 點選「設定新的連線或網路」。

🕎 網路和共用中心		-	$\times$
← → 丶 个 🚆 > 控制台 >	網路和網際網路 > 網路和共用中心 v O 授尋控制台		P
控制台首頁	檢視您基本的網路資訊並設定連線		
變更介面卡設定	檢視作用中的網路		
變更進階共用設定	變更網路設定		
	設定新的連線或網路 設定寬頻、撥號或 VPN 連線,或設定路由器或存取點。		
	疑難排解問題 診斷與依須須致問題,計助溫諾戰排解容却,		
	Keizegendige , www.krithfen.		
請參閱			
Windows Defender 防火牆			
紅外線			
網際網路選項			

Step 4. 在「設定連線或網路」視窗裡,點選「手動連線到無線網路」,接著點選「下一步」。

			-		×
🔶 🚽 設定連線或網路					
選擇連線選項					
· 連線到網際網路 設定寬頻或撥號	連線以連線到網際網路。				
<b>建</b> 設定新網路 設定新的路由器	或存取點。				
<b>手動連線到無線</b> 請連線到隔藏的	網路 網路或建立新的無線設定檔。				
■ 連線到工作地點 設定撥號或 VPN	↓連線以連線到您的工作地點	0			
			下一步(N)	取	淌

Step 5. 在「手動連線到無線網路」視窗中,輸入您要新增之無線網路的資訊,「網路名稱」 輸入「eduroam」、「安全性類型」選擇「WPA2-Enterprise」,再點選「下一步」。

				_		×
←	🔮 手動連線到無線網路					
	輸入您要新增之無線維	图路的資訊				
	網路名稱(E):	eduroam				
	安全性類型( <u>S</u> ):	WPA2-Enterprise ~				
	加密類型( <u>R</u> ):	AES $\lor$				
	安全性金銷(C):		□ 隱藏字元( <u>H</u> )			
	☑ 自動啟動這個連線① □ 即使網路未廣播,還易 警告:若選取此選項,	!進行連線(Q) 您電腦的隱私權可能會有風險。				
			- 不	步( <u>N</u> )	取	消

Step 6. 在「手動連線到無線網路」視窗出現「已成功新增 eduroam」後,點選「變更連線設定」。

			_		$\times$
$\leftarrow$	<u>.</u>	手動連線到無線網路			
	E)	成功新增 eduroam			
		→ 變更連線設定( <u>H</u> ) 開啟[連線] 內容讓我可以變更設定。			
				關問	眀

Step 7. 在「eduroam 無線網路內容」視窗的「安全性」頁籤中,確認相關設定資訊如圖所示,並點選「設定」。

eduroam 無線網路內容			×
連線 安全性			
安全性類型(E):	WPA2-Enterpris	e	$\sim$
加密類型( <u>N</u> ):	AES		$\sim$
選擇網路驗證方法( <u>O</u> ):			
Microsoft: Protected	EAP (PEAP)	~ 設定	<u>(2)</u>
☑ 每次登入時都記住我	在此連線的認證(E	Ø	
進階設定( <u>D</u> )			
		確定	取消

Step8. 在「受保護的 EAP 內容」視窗中,請「不要」勾選「確認伺服器憑證」,確定選擇驗證方法為「Secured password (EAP-MSCHAP v2)」,並點選「設定」。

建總部證憑證來確認伺服器身分識別()         建總到這些伺服器(例如:srv1;srv2;:*\.srv3\.com)(Q):         ////////////////////////////////////	受保護的 EAP 內容	Х
● 透過驗證憑證來確認伺服器身分識別(少)         ● 達線到這些伺服器(例如:srv1;srv2;:*\.srv3\.com)(②):         ● 应信任的根憑證按權單位(B):         ● OddTrust External CA Root         ● Baltimore CyberTrust Root         ● Certum CA         ● Certum Trusted Network CA         ● Class 3 Public Primary Certification Authority         ● DigiCert Assured ID Root CA         ● DigiCert Assured ID Root CA </td <td>連線時:</td> <td></td>	連線時:	
● 建線到這些伺服器(例如:srv1;srv2;:*\.srv3\.com)(Q):   Centen 和憑證授權 單位(R):   ● Centen 和憑證授權 單位(R):   ● Centen 和憑證授權 單位(R):   ● Centum CA   ● Centum Trusted Network CA   ● DigiCent Assured ID Root	透過驗證憑證來確認伺服器身分識別♥️	
受信任的根憑證授權單位(?)     ● AdTrust External CA Root   ● Baltimore CyberTrust Root   ● Certum Trusted Network CA   ● Certum Trusted Network CA   ● Cass 3 Public Primary Certification Authority   ● DigiCert Assured ID Root CA   ● DigiCert Assured ID Root CA   ● DigiCert Assured ID Root CA   ● DigiCert Assured JD Root CA   ● DigiCert Assured ID Root CA		
受信任的根憑證授權單位(E):         AddTust External CA Root         Baltimore CyberTrust Root         Certum CA         Certum Trusted Network CA         Class 3 Public Primary Certification Authority         DigiCert Assured ID Root CA         DigiCert Assured ID Root CA      <		1
AddTrust External CA Root         Baltimore CyberTrust Root         Certum CA         Certum Trusted Network CA         Class 3 Public Primary Certification Authority         DigiCert Assured ID Root CA         Control         Ciertum External CA Root         Lass 3 Public Primary Certification Authority         DigiCert Assured ID Root CA         Cierced Clear Clear Detector         Cierced password (EAP-MSCHAP v2)         Ware External	受信任的根源證授權 單位(R):	1
□ Baltimore CyberTrust Root         □ Certum CA         □ Certum Trusted Network CA         □ Class 3 Public Primary Certification Authority         □ DigiCert Assured ID Root CA         ○ Secured password (EAP-MSCHAP v2)	AddTrust External CA Root	1
□ Certum CA         □ Certum Trusted Network CA         □ Class 3 Public Primary Certification Authority         □ DigiCert Assured ID Root CA         ② 如果無法驗證伺服器的身分識別則告知使用者         ② & Brite         □ 如果伺服器未顧示加密繫結的 TLV 就中斷連線(D)         □ 如果伺服器未顧示加密繫結的 TLV 就中斷連線(D)         □ 如果伺服器未顧示加密繫結的 TLV 就中斷連線(D)	Baltimore CyberTrust Root	
□ Certum Trusted Network CA         □ Class 3 Public Primary Certification Authority         □ DigiCert Assured ID Root CA         □ 如果無法驗證伺服器的身分識別則告知使用者         ☑ 放用快速重新連線(E)         □ 如果伺服器未顯示加密繫結的 TLV 就中斷連線(D)         □ 飲用識別陽私權(D)	Certum CA	
□ Class 3 Public Primary Certification Authority         □ DigiCert Assured ID Root CA         □ DigiCert Assured ID Root CA         □ DigiCert Class 1 Part CA         く         連線前的通知(1):         如果無法驗證伺服器的身分識別則告知使用者         選擇驗證方法(S):         Secured password (EAP-MSCHAP v2)         ○ 啟用快速重新連線(P)         □ 如果伺服器未顯示加密繫結的 TLV 就中斷連線(D)         □ 啟用識別陽私權(1)	Certum Trusted Network CA	
□ COMODO RSA Certification Authority         □ DigiCert Assured ID Root CA         □ 如果無法驗證伺服器的身分識別則告知使用者         ○ Apple DigiCert Assured (EAP-MSCHAP v2)         ○ Apple Digitation (EA	Class 3 Public Primary Certification Authority	
□ DigiCert Assured ID Root CA         □ DigiCert Assured ID Root CA         □ DigiCert Assured ID Root CA         ■ DigiCert Assured ID Root CA	COMODO RSA Certification Authority	
□ D:=:C-4 Cl-L-1 D ==+ CA         連線前的通知(D:         如果無法驗證伺服器的身分識別則告知使用者         選擇驗證方法(S):         Secured password (EAP-MSCHAP v2)       ②         ② 啟用快速重新連線(D)         □ 如果伺服器未顯示加密繫結的 TLV 就中斷連線(D)         □ 啟用識別陽私權()	DigiCert Assured ID Root CA	
連線前的通知(D):         如果無法驗證伺服器的身分識別則告知使用者         選擇驗證方法(S):         Secured password (EAP-MSCHAP v2)          設定(C)             ② 愈用快速重新連線(P)         ③ 如果伺服器未顯示加密繫結的 TLV 就中斷連線(D)         ⑤         ③ 愈用識別陽私權(I)		
如果無法驗證伺服器的身分識別則告知使用者          選擇驗證方法(S):          Secured password (EAP-MSCHAP v2)          ② 啟用快速重新連線(P)          □ 如果伺服器未顧示加密繫結的 TLV 就中斷連線(D)         □ 啟用識別隱私權(I)		_
選擇驗證方法(S):          Secured password (EAP-MSCHAP v2)       ✓       設定(C)         ✓       愈用快速重新連線(P)         □       如果伺服器未顯示加密繫結的 TLV 就中斷連線(D)         □       愈用識別陽私權(I)	如果無法驗證伺服器的身分識別則告知使用者	
選擇驗證方法(S):          Secured password (EAP-MSCHAP v2)       設定(C)		
Secured password (EAP-MSCHAP v2)        設定(C)	選擇驗證方法( <u>S</u> ):	
<ul> <li>☑ 啟用快速重新連線(E)</li> <li>□ 如果伺服器未顯示加密繫結的 TLV 就中斷連線(D)</li> <li>□ 啟用識別隱私權(I)</li> <li>□ 融用識別隱私權(I)</li> </ul>	Secured password (EAP-MSCHAP v2) V 設定(C)	
<ul> <li>▲ 用 (D)</li> <li>● 如果伺服器未顯示加密繫結的 TLV 就中斷連線(D)</li> <li>● 愈用識別陽私權(I)</li> <li>● 融合</li> </ul>		0000000
	□加里伺服器主頭示加容離結約ⅠⅣ群由影通線(□)	
建宁 取当		
建宁 取当		
建宁 即当		
	確定取消	

Step 9. 在「EAP MSCHAPv2 內容」視窗中,請「不要」勾選「自動使用我的 Windows 登入 名稱及密碼」,點選「確定」,接著在「受保護的 EAP 內容」點選「確定」。

EAP MSCHAPv2 內容	$\times$
連線時:	
□ 自動使用我的 Windows 登入名稱及密	碼 (及網域,
確定 取消	

受保護的 EAP 內容	$\times$
連線時:	
□透過驗證憑證來確認伺服器身分識別──	
受信任的根憑證授權單位( <u>R</u> ):	
AddTrust External CA Root       ▲         Baltimore CyberTrust Root       ▲         Certum CA       ■         Certum Trusted Network CA       ■         Class 3 Public Primary Certification Authority       ■         COMODO RSA Certification Authority       ■         DigiCert Assured ID Root CA       ✓         基線前的通知①:       >	
如果無法驗證伺服器的身分識別則告知使用者	
選擇驗證方法(S): Secured password (EAP-MSCHAP v2) ✓ 設定(C) ✓ 愈用快速重新連線(F) □ 如果伺服器未顯示加密繫結的 TLV 就中斷連線(D) □ 愈用識別隱私權(I)	
確定取消	

eduroam 無線網路內容			×
連線 安全性			
安全性類型(E):	WPA2-Enterprise		~
加密類型( <u>N</u> ):	AES		~
選擇網路驗證方法(O):			
Microsoft: Protected 8	EAP (PEAP) 🛛 🗸	設定( <u>S</u> )	
☑每次登入時都記住我	在此連線的認證( <u>R</u> )		
進階設定( <u>D</u> )			
		確定	取消

Step 10. 在「eduroam 無線網路內容」視窗的「安全性」頁籤中,點選「進階設定」。

Step 11. 在「進階設定」視窗的「802.1X 設定」頁籤中,勾選「指定驗證模式」,並選擇「使用者驗證」,接著點選「儲存認證」。

進階設定	×
802.1X 設定 802.11 設定	
✓ 指定驗證模式(P):	
使用者驗證 > 儲存認證(C)	
──刪除所有使用者的認證(D)	
□ 對此網路啟用單一登入( <u>S</u> )	
◎ 在使用者登入前立即執行(E)	
○ 在使用者登入後立即執行(E)	
最大延遲(秒)(M): 10 €	
☑ 單一登入期間允許顯示其他對話方塊(L)	
☐ 此網路使用不同的虛擬 LAN 來驗證電腦和使用者(⊻)	
<b>雇定</b> 取消	

Step 12. 在「Windows 安全性」視窗中,「儲存認證」請輸入使用者認證資訊, 同仁請輸入 中心 AD 帳號及密碼,使用者名稱格式為 xxx@nsrrc.org.tw,並按「確定」,接著在「進階設 定」視窗中,點選「確定」。

Windows 安全性 儲存認證	×
儲存您的認證,可讓您的電腦在 就連線到網路。	E您未登入 (例如下載更新) 時
使用者名稱	
密碼	
確定	取消

進階設定	$\times$
802.1X 設定 802.11 設定	
✓ 指定驗證模式(P):	
使用者驗證 ~ 儲存認證( <u>C</u> )	
□刪除所有使用者的認證(D)	
□ 對此網路啟用單一登入( <u>S</u> )	
● 在使用者登入前立即執行(E)	
○ 在使用者登入後立即執行(E)	
最大延遲(秒)(M): 10	
✓ 單一登入期間允許顯示其他對話方塊(L)	
□此網路使用不同的虛擬 LAN 來驗證電腦和使用者(V)	
確定取消	

eduroam 無線網路內容			×
連線 安全性			
安全性類型(E):	WPA2-Enterprise		$\sim$
加密類型( <u>N</u> ):	AES		~
			_
選擇網路驗證方法(Q):			
Microsoft: Protected	EAP (PEAP)	~ 設定( <u>S</u> )	
🗹 每次登入時都記住我	在此連線的認證( <u>R</u> )		
10 00 00 0	_		
進階設定( <u>D</u> )			
		確定	取消

Step 13. 在「eduroam無線網路內容」視窗的「安全性」頁籤中,點選「確定」。

Step 14. 完成上述步驟後,確認「eduroam」出現「已連線,安全」的訊息,表示認證完成, 即可開始使用無線網路。

