思科業務控制面板中的外部強制門戶

目標

本文的目標是介紹在Cisco Business Dashboard(CBD)版本2.5.1及更高版本中配置外部 強制網路門戶功能的步驟。

適用裝置 |軟體版本

思科業務控制面板 | 2.5.1(下載**最新版本**) CBW140系列 | 10.8.1.0(下載**最新版**) CBW150系列 | 10.3.2.0(下載**最新版**)

簡介

CBD 2.5.1版為CBW140和CBW150系列網路實施了外部強制網路門戶頁面。這可以用 作訪客網路身份驗證頁面,並且與本地強制網路門戶頁面相比具有多項優勢。

它使用CBD的FQDN和SSL證書重定向到CBD,而不是將客戶端重定向到192.0.2.1處的本 地強制網路門戶頁面。這可避免觸發現代瀏覽器實*施的*增強型HTTP嚴格傳輸安全 (HSTS)。

外部Captive Portal頁面具有簡化的部署,便於使用訪客網路管理多個站點。

頁面和身份驗證策略的所有設定均在CBD中配置。

當您設定訪客網路時,它支援網路同意、電子郵件地址和登入CBD帳戶或訪問其他 RADIUS伺服器。

目錄

- 訪客網路要求
- 配置訪客身份驗證
- <u>配置無線LAN</u>
- CBW訪客網路設定
- •<u>強制網路門戶頁面</u>

訪客網路要求

要使用新的訪客網路身份驗證頁面,您必須擁有

CBD 2.5.1版 CBW140系列韌體10.8.1.0(或更高版本) CBW150系列韌體10.3.2.0(或更高版本)



配置強制網路門戶網頁:

步驟1

登入到您的CBD,然後導航到Network Configuration > Guest Portals。



*Guest Portals*頁面顯示每個CBD組織的網頁。要編輯頁面,請選擇配置檔案並按「編輯」按鈕。

Guest Portals				
2				
2				
1	Profile Name	Organization		
0>	Default guest portal	Default		

如果您有兩個或多個網路需要唯一的強制網路門戶頁面,則需要設定單獨的CBD組織,並讓 每個網路加入單獨的組織。

步驟3

配置選項包括

- 簡檔名稱 它是CBD中的唯一識別符號,因此您可以輕鬆跟蹤每個組織的頁面。
- 組織 顯示強制網路門戶所連線的組織。
- 標題文本 顯示Web瀏覽器顯示的標題。
- 背景圖像和徽標圖像顯示您可在其中拖放圖形以在強制網路門戶頁面上顯示。

- 前景、背景、分隔符、內容前景、內容背景和帳戶提示背景顏色欄位都允許您更改顯示器 各個方面的顏色。
- Fonts選單允許您選擇強制網路門戶頁面上使用的字型。
- 其他欄位允許您編輯頁面上顯示的文本。

		Separator Color		Acceptance Prompt	Check here to indicate that you have read and accepted the Acceptance Lise Policy
Device Group Selection					Acceptance ose roney
Profile Name	Default guest portal	Content Foreground Color			11
Organization	Default 👻	Content Background Color		No Acceptance Warning	Error: You must acknowledge the
Web Portal Customization		Account Tips Background Color			Acceptance Use Policy before connecting!
Header Text	Web Portal Guest Access				
Background Image		Fonts	Arial -		11.
		Button Label	Connect	Work In Progress Message	Connecting, please be patient
	Drag and drop file here, or click to select from the filesystem	Browser Header Text	Captive Portal		
					11.
	background.png	Ê	11.	Invalid Credentials Message	Error: Invalid Credentials, please
Logo Image		Portal Title	Welcome to the Wireless Network		try again!
	Drag and drop file here, or click to select from the filesystem				li.
			11.	Connection Succeeded Message	Congratulations!
	loginlogo.png	Acceptable Use Policy	Acceptance Use Policy		
Foreground Color					1
Background Color					<i>III.</i>
				Welcome Message	You are now authorized and

///.

步驟4

按一下以下頁籤之一配置用於身份驗證的文本選項。

- 使用者名稱/密碼
- Web同意
- 電子郵件地址

按一下Preview按鈕檢視每個選單選項的顯示方式。

Username

Password

 $\mathbf{\mathbf{S}}$

Enter your Username/Password



Username Input Label

Password Input Label

Input Prompt

Enable Acceptable Use Policy



步驟1

導覽至Network Configuration > Wireless LANs。

Cisco Business Dashboard				
			ξŝζ	Network Configuration
11.	Dashboard		Wiza	rd
<u></u> ж	Network		Time	Management
000	Inventory		DNS	Resolvers
	Port Management		Auth	entication
<u> </u>	Network Configuration	、	Virtu	allans
~//	inothonk conliguration	-	Wire	less LANs
Ŷ	Network Plug and Play	>	Wire	less Radios
步驟	2			

您可以新增或編輯現有無*線LAN配置*檔案。在此範例中,選擇「add」。

Wireless LANs

Wireless LANs

+ 🗹 🖻 😂

步驟3

指定將應用於的組織內的配置檔名稱、組織和裝置組。

Wireless LANs->Add WLAN			
Device Group Selection			
Profile Name	Training Test	~	
Organization	Default	 ✓ 	2
Device Groups 3	Available Groups Default	> < >> <<	Selected Groups

您只需選擇Default組織和Default Device Group。

步驟4

按一下plus圖示新增無線LAN。

Wireless LANs				
+				
SSID Name	VLAN ID	Enable	Security	Action

步驟5

指定SSID名稱和VLAN ID。從Security下拉選單中選擇Guest。

Add Wireless LANs		×
Enable	Enable	
SSID Name	Guest Test	 ✓
VLAN ID	1	 ✓
Security	Guest	- 3

第6步

選擇Guest authentication方法。選項包括:

- 使用者名稱/密碼
- Web同意
- 電子郵件地址

Guest authentication	Username/Password 🔹
 Advanced Settings 	Username/Password
Auvanced Settings	Web Consent
Broadcast	Email Address

第7步

在Advanced Settings下,您還可以指定是否希望SSID為Broadcast、Application Visibility、Local Profiling和Radio設定。

 Advanced Settings 	
Broadcast	Enable
Application Visibility	Enable
Local Profiling	Enable
Radio	вотн 👻

在大多數情況下,這些選項將保留預設設定。

第8步

按一下「Save」。

Add Wireless LANs

\sim	

Enable	Enable
SSID Name	Guest Test 🗸
VLAN ID	1 🖌
Security	Guest
Guest authentication	Username/Password
 Advanced Settings 	
Broadcast	Enable
Application Visibility	Enable
Local Profiling	Enable
Radio	BOTH
	Save Cancel

第9步

再次按一下**Save**。

Wireless LANs->Add WLAN

Device Group Selection				
Profile Name	Training Test	~		
Organization	Default	~		
Device Groups	Available Group: Default	s >	Selected Groups	
\searrow		< >> <<		
Wireless LANs				
SSID Name	VLAN ID	Enable	Security	Action

CBW訪客網路設定

步驟1

登入您的Cisco Business Wireless(CBW)存取點。

diale Cisco Business



Welcome! Please click the login button to enter your user name and password



步驟2

導覽至Wireless Settings > WLANs。

步驟3

您可以編輯WLAN並轉至**WLAN Security**頁籤。*Captive Portal*將設定為**External Splash** 頁面,其中包含CBD伺服器的**Captive Portal URL**。將自動配置*ACL名稱*。

General	WLAN Security	VLAN & Firewall	Traffic Sha	ping Scheduling
	Guest Network			
Captiv	ve Network Assistant			
	MAC Filtering	3		
	Captive Portal	External Splash p	age 🔻	
'	Captive Portal URL	https://cbd2.	iet/contro	0
	Access Type	RADIUS	•	_
	ACL Name(IPv4)	CBD_cbd2.	n 🔻	03
	ACL Name(IPv6)	None	•	0

步驟4

RADIUS伺服器會自動配置。要檢視該文檔,請按一下頁面頂部的雙向箭頭,切換到 Expert View。

? Q 🗛 🕑 🖺 💳 🌣

步驟5

導航到管理>管理員帳戶。



第6步

按一下RADIUS頁籤。

Managem	Management User Priority Order		Local Admin Accounts TA		TACAG	CS+ R/	ADIUS	
Auth Cach	ied Users							
Authenticat	ion Call Stat	ion ID Type	AP MAC	Address:SSIE	•			
Authe	ntication MA	C Delimiter	Hyphen		•			
Account	ing Call Stat	ion ID Type	IP Addre	ss	•			
Ac	counting MA	C Delimiter	Hyphen		•			
	Fal	lback Mode	Passive		•			
		Username	cisco-pro	be				
Interval			300		٢	Seconds		
	AP Events Accounting							
	Apply							
Add RADIU	Add RADIUS Authentication Server							
Action	Server Index	Network User	Management	State 5	Server IP A	Shared Ke	y Port	
⊘ x	1						1812	

第7步

它還將在Advanced > Security Settings下為CBD動態新增安全ACL。

Monitoring	ان 😑	ı.ı ı. Isco	Cisco Busin	uess Wireless 14	0AC Access Point	Q	▲	٩		₽	Х
 Wireless Settings Management 	Security	Security Settings									
✓ Services	🐮 Sec	Security Settings									
Advanced											
🗟 Logging	Add new ACL										
I RF Optimization	Action	ACL Ty	be	ACL Name				Policy AC	iL.		
I RF Profiles	♂ ×	IPv4		CBD_	r.net_0			Not mapp	ed		
& Primary AR Tools	⊠ ×	IPv4		Enable_Face	book_Login			Not mapp	ed		
Primary AP Tools	⊠ ×	IPv4		Enable_Goog	le_Login			Not mapp	ed		
Security Settings	⊠ ×	IPv4		Enable_Socia	al_Login			Not mapp	ed		

強制網路門戶頁面

根據您配置設定的方式, 強制網路門戶頁面將如下所示:

使用者名稱/密碼身份驗證

cisco	Web Portal Guest Access	
		Welcome to the Wireless Network
		To start using this service, enter your credentials and click the connect button
		Username
		Enter your Username/Password
		Password
		·····
		Acceptable Use Policy
		 Check here to indicate that you have read and accepted the Acceptable Use Policy
		Connect

Web同意

alialia cisco	Web Portal Guest Access	
		Welcome to the Wireless Network
		Please accept the Acceptable Use Policy
		Acceptable Use Policy
		 Check here to indicate that you have read and accepted the Acceptable Use Policy
		Connect

電子郵件驗證

cisco	Web Portal Guest Access	
		Welcome to the Wireless Network
		Please enter your email address to login
		Email Address
		Enter your Email Address
		Acceptable Use Policy
		Check here to indicate that you have read and accepted the Acceptable Use Policy Connect



你成功了!您已使用CBD成功設定外部強制網路門戶頁面。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。