9800 WLCとAruba ClearPassの設定: ゲストア クセスとFlexConnect

内容

概要 前提条件 要件 <u>使用するコンポーネント</u> 背景説明 <u>CWAゲストエンタープライズ導入のトラフィックフロー</u> ネットワーク図 設定 ゲストワイヤレスアクセスC9800パラメータの設定 C9800: ゲスト用AAA設定 C9800: リダイレクションACLの設定 C9800:ゲストWLANプロファイルの設定 C9800: ゲストポリシープロファイルの定義 C9800 – ポリシータグ C9800:AP加入プロファイル C9800:Flexプロファイル C9800 – サイトタグ C9800:RFプロファイル C9800:APへのタグの割り当て Aruba CPPMインスタンスの設定 Aruba ClearPassサーバの初期設定 ライセンスの申請 サーバホスト名 CPPM Webサーバ証明書(HTTPS)の生成 ネットワークデバイスとしてのC9800 WLCの定義 ゲストポータルページとCoAタイマー ClearPass: ゲストCWAの設定 ClearPassエンドポイントメタデータ属性: Allow-Guest-Internet ClearPass再認証適用ポリシー設定 ClearPassゲストポータルリダイレクト適用プロファイルの設定 ClearPassメタデータ強制プロファイルの設定 ClearPassゲストインターネットアクセス適用ポリシーの設定 ClearPassゲストのAUP後の適用ポリシーの設定 ClearPass MAB認証サ<u>ービスの設定</u> ClearPass Webauthサービスの設定 ClearPass:Webログイン 検証: ゲストCWA認証 付録

概要

このドキュメントでは、Catalyst 9800ワイヤレスLANコントローラ(WLC)をAruba ClearPassと統 合して、アクセスポイント(AP)のFlexconnectモードでのワイヤレスクライアントへのセントラル Web認証(CWA)を利用するゲストWireless Service Set Identifier(SSID)を提供する方法について説 明します。

ゲストワイヤレス認証は、Anonymous acceptable user policy(AUP)ページを使用してゲストポー タルでサポートされます。このページは、セキュアな非武装地帯(DMZ)セグメント内のAruba Clearpassでホストされます。

前提条件

このガイドでは、次のコンポーネントが設定および検証されていることを前提としています。

- •関連するすべてのコンポーネントがネットワークタイムプロトコル(NTP)に同期され、正しい 時刻であることが確認されます(証明書の検証に必要)
- ・動作可能なDNSサーバ(ゲストトラフィックフロー、証明書失効リスト(CRL)の検証に必要)
- DHCPサーバの動作
- オプションの認証局(CA)(CPPMホスト型ゲストポータルへの署名に必要)
- Catalyst 9800 WLC
- Aruba ClearPass Server (プラットフォームライセンス、アクセスライセンス、オンボード ライセンスが必要)
- VMware ESXi

要件

次の項目に関する知識があることが推奨されます。

- •C9800の導入と新しい設定モデル
- C9800でのFlexconnectスイッチング
- ・9800 CWA認証(<u>https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-</u> wireless-controllers/213920-central-web-authentication-cwa-on-cata.htmlを参照)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 17.3.4cが稼働するCisco Catalyst C9800-L-C
- Cisco Catalyst C9130AX
- Aruba ClearPass、6-8-0-109592および6.8-3パッチ
- MS Windowsサーバ Active Directory(管理対象エンドポイントへのマシンベースの証明書自 動発行用に設定されたGP)オプション43およびオプション60のDHCPサーバDNS サーバす べてのコンポーネントを時刻同期するNTPサーバCA

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

背景説明

次の図は、ゲストユーザがネットワークへの接続を許可される前に、ゲストWiFiアクセス交換の 詳細を示しています。

1.ゲストユーザは、リモートオフィスのゲストWiFiに関連付けられます。

2.最初のRADIUSアクセス要求は、C9800によってRADIUSサーバにプロキシされます。

3.サーバは、ローカルMACエンドポイントデータベースで指定されたゲストMACアドレスを検索 します。

MACアドレスが見つからない場合、サーバはMAC認証バイパス(MAB)プロファイルで応答します。このRADIUS応答には次が含まれます。

• URLリダイレクトアクセスコントロールリスト(ACL)

• URL リダイレクト

4.クライアントは、IPアドレスが割り当てられたIP Learnプロセスを実行します。

5. C9800は、ゲストクライアント(MACアドレスで識別される)を「Web Auth Pending」状態 に移行します。

6.ゲストWLANに関連する最新のデバイスOSのほとんどは、何らかのキャプティブポータル検出 を実行します。

正確な検出メカニズムは、特定のOSの実装によって異なります。クライアントOSは、RADIUS Access-Accept応答の一部として提供されるRADIUSサーバによってホストされるゲストポータル URLにC9800によってリダイレクトされたページを含むポップアップダイアログ(擬似ブラウザ)を開きます。

7.ゲストユーザが表示されたポップアップで利用規約に同意するClearPassは、クライアントが認証を完了し、ルーティングテーブルに基づいてインターフェイスを選択することによって (ClearPassに複数のインターフェイスがある場合)、RADIUS認可変更(CoA)を開始したことを示すために、エンドポイントデータベース(DB)にクライアントMACアドレスのフラグを設定します。

8. WLCはゲストクライアントを「Run」状態に移行し、ユーザにはインターネットへのアクセス 権が付与されますが、それ以上のリダイレクトは行われません。

注: Cisco 9800 Foreign、RADIUSを使用したアンカーワイヤレスコントローラの状態フロ ー図および外部でホストされるゲストポータルについては、この記事の「付録」セクション を参照してください。



ゲストセントラルWeb認証(CWA)の状態図

CWAゲストエンタープライズ導入のトラフィックフロー

複数のブランチオフィスを持つ一般的なエンタープライズ展開では、各ブランチオフィスは、ゲ ストがEULAを受け入れると、ゲストポータルを介してゲストに安全なセグメント化されたアク セスを提供するように設定されます。

この設定例では、9800 CWAは、ネットワークのセキュアDMZ内のゲストユーザ用に排他的に導入される個別のClearPassインスタンスへの統合を介したゲストアクセスに使用されます。

ゲストは、DMZ ClearPassサーバが提供するWeb同意ポップアップポータルに記載された利用規 約に同意する必要があります。この設定例では、匿名ゲストアクセス方式(つまり、ゲストポー タルへの認証にゲストのユーザ名とパスワードは不要)に焦点を当てています。

この導入に対応するトラフィックフローを図に示します。

1. RADIUS - MABフェーズ

2.ゲストポータルへのゲストクライアントURLリダイレクト

3.ゲストポータルでゲストがEULAを受け入れると、RADIUS CoA再認証がCPPMから9800 WLCに発行されます

4.ゲストはインターネットへのアクセスを許可される



ネットワーク図

注: ラボのデモ目的では、単一または組み合わされたAruba CPPMサーバインスタンスを使用して、ゲストと企業の両方のSSIDネットワークアクセスサーバ(NAS)機能を提供します。 ベストプラクティスの実装では、独立したNASインスタンスを推奨します。



設定

この設定例では、C9800の新しい設定モデルを利用して、必要なプロファイルとタグを作成し、 企業ブランチにdot1x企業アクセスとCWAゲストアクセスを提供します。結果の設定を次の図に 示します。

Policy Tag: PT_CAN01	WLAN Profile: WP_Guest SSID: Guest Layer 2: Security None Layer 2: MAC Filtering Enabled Authz List: AAA_Authz-CPPM	Policy Profile: PP_Guest Central Switching: Disabled Central Auth: Enabled Central DHCP: Disabled Vlan: guest (21) AAA Policy: Allow AAA Override Enabled AAA Policy: NAC State Enabled AAA Policy: NAC Type RADIUS AAA Policy Accounting List: Guest_Accounting
Site Tag: ST_CAN01 Enable Local Site: Off		AP Join Profile: MyApProfile NTP Server: 10.0.10.4 Flex Profile: FP_CAN01 Native Vlan 2 Policy ACL: CAPTIVE_PORTAL_REDIRECT, ACL CWA: Enabled VLAN: 21 (Guest)
		5GHz Band RF: Typical_Client_Density_rf_5gh
RF Tag: Branch_RF		2GHz Band RF: Typical_Client_Density_rf_2gh

ゲストワイヤレスアクセスC9800パラメータの設定

C9800: ゲスト用AAA設定

注:Cisco Bug ID <u>CSCvh03827</u>について、定義された認証、許可、アカウンティング (AAA)サーバがロードバランスされていないことを確認します。このメカニズムは、 ClearPass RADIUS交換に対してWLCのセッションIDの持続性に依存しているためです。

ステップ1:Aruba ClearPass DMZサーバを9800 WLC設定に追加し、認証方式リストを作成します 。[Configuration] > [Security] > [AAA] > [Servers/Groups] > [RADIUS] > [Servers] > [+Add] に移動 し、RADIUSサーバ情報を入力します。

Create AAA Radius Server		
Name*	СРРМ	
Server Address*	10.85.54.98	
PAC Key		
Кеу Туре	Clear Text	
Key* (i)		
Confirm Key*		
Auth Port	1812	
Acct Port	1813	
Server Timeout (seconds)	5	
Retry Count	3	
Support for CoA	ENABLED	
Cancel		Apply to De

ステップ2:ゲスト用のAAAサーバグループを定義し、ステップ1.で設定したサーバをこのサーバ グループに割り当てます。[Configuration] > [Security] > [AAA] > [Servers/Groups] > [RADIUS] > [Groups] > [+Add] に移動します。

Create AAA Radius Serve	er Group	>
Name*	AAA_Radius_CPPM	
Group Type	RADIUS	
MAC-Delimiter	none 🔹	
MAC-Filtering	none 🔹	
Dead-Time (mins)	5	
Source Interface VLAN ID	1	
Available Servers	Assigned Servers	
	CPPM C N N N N N V	
Cancel	Apply to Device	

ステップ3 : ゲストアクセスの認可方式リストを定義し、ステップ2で作成したサーバグループを マッピングします。[Configuration] > [Security] > [AAA] > [AAA Method List] > [Authorization] > [+Add] に移動します。Type Networkを選択し、次にステップ2で設定したAAA Server Groupを選 択します。

Quick Setup: AAA Authoriza	ation	×
Method List Name*	AAA_Authz_CPPM	
Type*	network 🔹	
Group Type	group v (i)	
Fallback to local		
Authenticated		
Available Server Groups	Assigned Server Groups	
radius Idap tacacs+	AAA_Radius_CPPM <	<
Cancel		Apply to Device

ステップ4:ゲストアクセス用のアカウンティング方式リストを作成し、ステップ2で作成したサ ーバグループをマッピングします。[Configuration] > [Security] > [AAA] > [AAA Method List] > [Accounting] > [+Add] に移動します。ドロップダウンメニューから[Type Identity] を選択し、次に ステップ2で設定した[AAA Server Group] を選択します。

Quick Setup: AAA Accountin	ng		×
Method List Name* Type*	AAA_Accounting_CPPM	i	
Available Server Groups	Assigned Ser	ver Groups	
radius Idap tacacs+	> AAA_ <	_Radius_CPPM	
Cancel			Apply to Device

リダイレクトACLは、どのトラフィックをゲストポータルにリダイレクトする必要があるかを定 義し、リダイレクトなしで通過できるようにします。この場合、ACL denyはリダイレクトまたは パススルーのバイパスを意味し、permitはポータルへのリダイレクトを意味します。トラフィッ ククラスごとに、アクセスコントロールエントリ(ACE)を作成し、入力トラフィックと出力トラ フィックの両方に一致するACEを作成する際に、トラフィックの方向を考慮する必要があります 。

[Configuration] > [Security] > [ACL] に移動し、**CAPTIVE_PORTAL_REDIRECT**という名前の新し いACLを定義します。次のACEでACLを設定します。

- ACE1:双方向のInternet Control Message Protocol(ICMP)トラフィックがリダイレクトをバイ パスできるようにします。主に到達可能性を確認するために使用されます。
- ACE10、ACE30:DNSサーバ10.0.10.4への双方向DNSトラフィックフローを許可し、ポータ ルにリダイレクトされないようにします。ゲストフローをトリガーするには、応答のための DNSルックアップと代行受信が必要です。
- ACE70、ACE80、ACE110、ACE120:ユーザにポータルを提示するために、ゲストキャプティブポータルへのHTTPおよびHTTPSアクセスを許可します。
- ACE150:すべてのHTTPトラフィック(UDPポート80)がリダイレクトされます。

Sequence 🗸	Action 🗸	Source vi IP	Source v Wildcard	Destination < IP	Destination V Wildcard	Protocol 🖂	Source v Port	Destination v Port
1	deny	any		ajęy		icmp		
10	deny	any		10.0.10.4		udp		eq domain
30	deny	10.0.10.4		any		udp	eq domain	
70	deny	any		10.85.54.98		tcp		eq 443
80	deny	10.85.54.98		any		tcp	eq 443	
110	deny	any		10.85.54.98		tcp		eq www
120	deny	10.85.54.98		any		tcp	eq www	
150	permit	any		any		tcp		eq www

C9800: ゲストWLANプロファイルの設定

ステップ1:[Configuration] > [Tags & Profiles] > [Wireless] > [+Add] に移動します。ゲストクライ アントが関連付けるSSID「Guest」のブロードキャストを使用して、新しいSSIDプロファイル WP_Guestを作成します。

Ad	d WLAN						×
G	General	Security	Advanced				
	Profile N	lame*	WP_Guest	Radio Policy	All	•	
	SSID*		Guest	Broadcast SSID	ENABLED		
	WLAN II	D*	3				
	Status		ENABLED				



同じ[Add WLAN] ダイアログで、[Security] > [Layer 2] タブに移動します。

- レイヤ2セキュリティモード:なし

-MAC フィルタリング:有効

- 許可リスト:ドロップダウンメニューからAAA_Authz_CPPM(AAA設定の一部としてステップ 3で設定)

А	dd WLAN					×
	General	Security	Advanced			
	Layer2	Layer3	ААА			
	Layer 2 Sec	urity Mode		None	Lobby Admin Access	
	MAC Filterin	g			Fast Transition	Adaptive Enab 🔻
	OWE Transit	tion Mode			Over the DS	20
	Transition M	lode WLAN I	D*	1-4096	Reassociation filleout	20
	Authorizatio	n List*		AAA_Authz_C 🗸		
	Cancel]				Apply to Device

C9800:ゲストポリシープロファイルの定義

C9800 WLC GUIで、[Configuration] > [Tags & Profiles] > [Policy] > [+Add] に移動します。

[Name] : PP_Guest

ステータス:有効

中央スイッチング:Disabled

中央認証:有効

中央DHCP:Disabled

中央関連付け:Disabled

Add Pol	licy Profile						×
General	Access Policies	QOS and AVC	Mobility	Advanced			
	A Configuri	ng in enabled state will r	esult in loss of	connectivity fo	or clients associated wit	th this profile.	
Nam	ie*	PP_Guest		WLAN	Switching Policy		
Des	cription	Policy Profile for 0	àuest	Centra	I Switching	DISABLED	
Stat	us	ENABLED		Central	I Authentication		
Pass	sive Client	DISABLED		Central	I DHCP	DISABLED	
Encr	ypted Traffic Analytics	DISABLED		Central	I Association	DISABLED	
CTS	S Policy			Flex NA	AT/PAT	DISABLED	
Inline	e Tagging						
SGA	CL Enforcement						
Defa	ault SGT	2-65519					
Can	cel						wico

Add Po	olicy Profile	e						×
		A Configurin	ng in enabled state wil	I result in loss of	fconr	nectivity for clients associated with th	nis profile.	
Genera	al Acces	ss Policies	QOS and AVC	Mobility	Ad	vanced		
Nar	me*		PP_Guest			WLAN Switching Policy		
Des	scription		Profile for Branch	Guest		Central Switching	DISABLED	
Sta	atus		DISABLED			Central Authentication		
Pas	ssive Client		DISABLED			Central DHCP	DISABLED	
Enc	crypted Traffic	c Analytics	DISABLED			Central Association	DISABLED	
СТ	TS Policy					Flex NAT/PAT	DISABLED	
Inlir	ne Tagging							
SG	ACL Enforcer	ment						
Def	fault SGT		2-65519					
່ວ Ca	incel						Apply to Devi	ice

同じ[Add Policy Profile] ダイアログの[Access Policies] タブに移動します。

- RADIUSプロファイリング:有効

- VLAN/VLANグループ:210(つまり、VLAN 210は各ブランチロケーションのゲストローカル VLANです)

注:Flex用のゲストVLANは、VLANの下の9800 WLCでVLAN/VLANグループタイプVLAN番号で定義する必要はありません。

既知の不具合:Cisco Bug ID <u>CSCvn48234</u>では、同じFlexゲストVLANがWLCの下およびFlexプロ ファイルで定義されている場合、SSIDがブロードキャストされません。

Add Policy	Profile						2
	A Configuri	ng in enabled state will r	esult in loss of	f connectivity for	r clients associated	d with this profile.	
General	Access Policies	QOS and AVC	Mobility	Advanced			
RADIUS Pr	ofiling				WLAN ACL		
HTTP TLV	Caching				IPv4 ACL	Search or Select	•
DHCP TLV	Caching				IPv6 ACL	Search or Select	•
WLAN Lo	cal Profiling				URL Filters		
Global Stat Classification	e of Device on	(i)			Pre Auth	Search or Select	•
Local Subs	criber Policy Name	Search or S	Select 🔻]	Post Auth	Search or Select	•
VLAN							
VLAN/VLA	N Group	210	v	J			
Multicast V	'LAN	Enter Mul	ticast VLAN]			

Cancel

同じ[Add Policy Profile] ダイアログで、[Advanced] タブに移動します。

-Allow AAA Override:有効

-NAC State:有効

- アカウンティング一覧: AAA_Accounting_CPPM(AAA設定の一部としてステップ4で定義)

⁻ NACタイプ: RADIUS

Add Policy Profile

	uring in enabled state will	result in loss	of connectivity for clients associated with this profile.
General Access Policies	QOS and AVC	Mobility	Advanced
WLAN Timeout			Fabric Profile Search or Select
Session Timeout (sec)	1800		mDNS Service Search or Select
Idle Timeout (sec)	300		Hotspot Server Search or Select 🔹
Idle Threshold (bytes)	0		User Defined (Private) Network
Client Exclusion Timeout (sec)	60		Status
DHCP			Drop Unicast
Brior			Umbrella
IPv4 DHCP Required DHCP Server IP Address			Umbrella Parameter Map
Show more >>>			Flex DHCP Option ENABLED
AAA Policy			DNS Traffic Redirect IGNORE
Allow AAA Override	 Image: A start of the start of		WLAN Flex Policy
NAC State	 Image: A set of the set of the		VLAN Central Switching
NAC Type	RADIUS	•	Split MAC ACL Search or Select 🔻
Policy Name	default-aaa-policy	× Ŧ	Air Time Fairness Policies
Accounting List	AAA_Accounting_(• • ×	2.4 GHz Policy Search or Select

注:C9800 WLCがRADIUS CoAメッセージを受け入れることができるようにするには、 [Network Admission Control (NAC) State - Enable]が必要です。

C9800 – ポリシータグ

C9800 GUIで、[Configuration] > [Tags & Profiles] > [Tags] > [Policy] > [+Add] に移動します。

-Name : PT_CAN01

-説明:CAN01ブランチサイトのポリシータグ

同じダイアログボックスの[Add Policy Tag] で、[WLAN-POLICY MAPS] の下の[Add] をクリック し、以前に作成したWLANプロファイルをポリシープロファイルにマッピングします。

×

- WLANプロファイル:WP_Guest

- ポリシープロファイル : PP_Guest

Add Policy Tag			×
Name*	PT_CAN01		
Description	Policy Tag for CAN01		
V WLAN-POLICY	Y Maps: 0		
+ Add × Dele	ete		
WLAN Profile		 Policy Profile 	×.
	10 🔻 items per page		No items to display
Map WLAN and Pol	icy		
WLAN Profile*	WP_Guest	Policy Profile*	PP_Guest
	×	~	
RLAN-POLICY	Maps: 0		
Cancel			Apply to Device

C9800:AP加入プロファイル

C9800 WLC GUIで、[Configuration] > [Tags & Profiles] > [AP Join] > [+Add] に移動します。

-Name : Branch_AP_Profile

-NTP サーバ:10.0.10.4(ラボトポロジ図を参照)。 これは、ブランチのAPが同期に使用する NTPサーバです。

Add AP J	oin Profile									×
General	Client	CAPWAP	AP	Management	Sec	urity	ICap	QoS		
Name*		Branch	_AP_Pro	ofile		Office	Extend A	P Configuration	on	
Descri	otion	Branch	n AP Join	Profile		Local	Access	~		
LED St	ate	\checkmark				Link E	ncryption	 		
LAG M	ode					Rogue	Detection			
NTP Se	erver	10.0.1	0.4							
GAS A	P Rate Limit									
Appho	st									
Cance	I								Apply to Devi	ice

C9800:Flexプロファイル

プロファイルとタグはモジュール化されており、複数のサイトで再利用できます。

FlexConnect導入の場合、すべてのブランチサイトで同じVLAN IDを使用すると、同じFlexプロファイルを再利用できます。

ステップ1:C9800 WLCのGUIで、[Configuration] > [Tags & Profiles] > [Flex] > [+Add] に移動します。

-Name : FP_Branch

- ネイティブVLAN ID:10(デフォルト以外のネイティブVLANがあり、AP管理インターフェイス が必要な場合のみ必要)

Add Flex Profile				×
General Local Authentic	cation Policy ACL VLA	N Umbrella		
Name*	FP_Branch	Fallback Radio Shut		
Description	Branch Flex Profile	Flex Resilient		
Native VLAN ID	10	ARP Caching		
HTTP Proxy Port	0	Efficient Image Upgrade		
HTTP-Proxy IP Address	0.0.0.0	OfficeExtend AP		
CTS Policy		Join Minimum Latency		
Inline Tagging		IP Overlap		
SGACL Enforcement		mDNS Flex Profile	Search or Select 🚽	
CTS Profile Name	default-sxp-profile x			
Cancel				Apply to Device

同じ[Add Flex Profile] ダイアログで、[Policy ACL] タブに移動し、[Add] をクリックします。

-ACL 名:CAPTIVE_PORTAL_REDIRECT

- 中央Web認証:有効

Flexconnect導入では、C9800ではなくAPでリダイレクションが発生するため、管理対象の各 APはローカルにリダイレクトACLをダウンロードすることが想定されます。

Add Flex Profile		×
General Local Authentica	ation Policy ACL VLAN Umbrella	
+ Add × Delete		
ACL Name	✓ Central Web Auth ✓ Pre Auth URL Filter	ACL Name* CAPTIVE_PORTAL_F
	0 v items per page No items to display	Central Web Auth
		Pre Auth URL Filter Search or Select
		Save
່ ວ Cancel		Apply to Device

同じ[Add Flex Profile] ダイアログで、[VLAN] タブに移動し、[Add] をクリックします(ラボトポ ロジ図を参照)。

- VLAN名:ゲスト

-VLAN ID:210

Add Flex Profile	×
General Local Authentication Policy ACL VLAN Umbrella	
+ Add × Delete	
VLAN Name v ID v ACL Name v	
data 2 VLAN Name* guest	
Image: Market and Ma	
1 - 1 of 1 items ACL Name Select ACL	
✓ Save つ Cancel	
	_
Cancel	vice

C9800 – サイトタグ

9800 WLC GUIで、[Configuration] > [Tags & Profiles] > [Tags] > [Site] > [Add] に移動します。

注:説明に従って、2つのワイヤレスSSIDをサポートする必要がある各リモートサイトに一意のサイトタグを作成します。

地理的な場所、サイトタグ、およびFlex Profile設定の間には1~1のマッピングがあります。

Flex Connectサイトには、Flex Connectプロファイルが関連付けられている必要があります。 Flex Connectサイトごとに最大100のアクセスポイントを設定できます。

-Name : ST_CAN01

- AP加入プロファイル:Branch_AP_Profile

- フレックスプロファイル:FP_Branch

- ローカルサイトの有効化: Disabled

Add Site Tag		
Name*	ST_CAN01	
Description	Site Tag for Branch	CA
AP Join Profile	Branch_AP_Profile	•
Flex Profile	FP_Branch	•
Fabric Control Plane Name		•
Enable Local Site		
Cancel		

C9800:RFプロファイル

```
9800 WLC GUIで、[Configuration] > [Tags & Profiles] > [Tags] > [RF] > [Add] に移動します。
```

-Name : Branch_RF

- 5 GHz帯域無線周波数(RF)プロファイル:Typical_Client_Density_5gh(システム定義オプション)

- 2.4 GHz帯域RFプロファイル: Typical_Client_Density_2gh(システム定義オプション)

Add RF Tag		×
Name*	Branch_RF	
Description	Typical Branch RF	
5 GHz Band RF Profile	Client_Density_rf_5gh	
2.4 GHz Band RF Profile	Typical_Client_Densi	
Cancel		Apply to Device

C9800:APへのタグの割り当て

展開内の個々のAPに定義済みタグを割り当てるには、次の2つのオプションがあります。

- AP名ベースの割り当て。これは、[AP Name]フィールド([Configure] > [Tags & Profiles] > [Tags] >[AP] > [Filter])のパターンに一致する正規表現ルールを利用します。

- APイーサネットMACアドレスベースの割り当て([Configure] > [Tags & Profiles] > [Tags] > [AP] > [Static])

DNA Centerを使用した実稼働環境への導入では、手動によるAP単位の割り当てを避けるために、DNACとAPのPNPワークフローを使用するか、9800で使用可能な静的な一括のカンマ区切り値 (CSV)アップロード方式を使用することを強く推奨します。[Configure] > [Tags & Profiles] > [Tags] > [AP] > [Static] > [Add] に移動します([Upload File] オプションに注意してください)。

-AP MACアドレス:<AP_ETHERNET_MAC>

- ポリシータグ名:PT_CAN01

- サイトタグ名:ST_CAN01

- RFタグ名:Branch_RF

注: Cisco IOS®-XE 17.3.4cの時点では、コントローラの制限ごとに最大1,000個の正規表現 規則があります。導入環境のサイト数がこの数を超える場合は、MAC単位の静的な割り当 てを利用する必要があります。

Associate Tags to	AP	
AP MAC Address*	aaaa.bbbb.cccc	
Policy Tag Name	PT_CAN01	•
Site Tag Name	ST_CAN01	•
RF Tag Name	Branch_RF	•
Cancel		

注:または、AP名の正規表現ベースのタグ割り当て方法を利用するには、[Configure] > [Tags & Profiles] > [Tags] > [AP] > [Filter] > [Add] に移動します。

-Name : BR_CAN01

- AP名regex:BR-CAN01-.(7)(このルールは、組織内で採用されているAP名の表記法に一致します 。この例では、タグは、「BR_CAN01 – 」の後に7文字が続くAP名フィールドを持つAPに割り当 てられます)。

-Priority:1

- ポリシータグ名: PT_CAN01 (定義どおり)

- サイトタグ名:ST_CAN01

- RFタグ名:Branch_RF

Associate Tags to AP

A Rule "BR-CAN01" has this priority. Assigning it to the current rule will swap the priorites.

Rule Name*	BR_CAN01	Policy Tag Name	PT_CAN01	××
AP name regex*	BR-CAN01{7}	Site Tag Name	ST_CAN01	×
Active	YES	RF Tag Name	Branch_RF	× v
Priority*	1			
Cancel				Apply to Device

Aruba CPPMインスタンスの設定

Aruba CPPM構成に基づく実稼働/ベストプラクティスについては、最寄りのHPE Aruba SEリソ

ースにお問い合わせください。

Aruba ClearPassサーバの初期設定

Aruba ClearPassは、次のリソースを割り当てるESXi <>サーバ上でOpen Virtualization Format(OVF)テンプレートを使用して導入されます。

・2つの予約済み仮想CPU

- メモリ 6 GB
- •80 GBディスク(マシンの電源を入れる前に、最初のVM導入後に手動で追加する必要がある)

ライセンスの申請

プラットフォームライセンスを適用するには、[Administration] > [Server Manager] > [Licensing] を選択します。**Platform、Access**、および**Onboard**ライセンスを追加します。

サーバホスト名

[Administration] > [Server Manager] > [Server Configuration] に移動し、新しくプロビジョニング されたCPPMサーバを選択します。

-Hostname : cppm

- FQDN:cppm.example.com

- 管理ポートのIPアドレスとDNSの確認

Administration » Server Manager » Server Configuration - cppm Server Configuration - cppm (10.85.54.98)

System	Services Control	Service Parameters	System Monitoring	Network	FIPS		
Hostname:		cppm					
FQDN:		cppm.example	e.com				
Policy Man	ager Zone:	default	~				Manage F
Enable Per	formance Monitoring [Display: 🗹 Enable this	server for performant	e monitoring	display		
Insight Set	ting:	🗹 Enable Insi	ight 🔽 En	able as Insigh	t Master	Current Master:cppm(10.85.54.98)	
Enable Ing	ress Events Processing	g: 🗌 Enable Ing	ress Events processing	on this serve	er		
Master Ser	ver in Zone:	Primary mast	er v				
Span Port:		None	~				
			IPv	4		IPv6	Action
		IP Address	10.0	35.54.98			
Managem	ent Port	Subnet Mask	255	.255.255.224			Configure
		Default Gateway	10.8	35.54.97			
		IP Address			_		
Data/Exte	ernal Port	Subnet Mask					Configure
	Default Gateway						
		Primary	10.8	35.54.122			
DNS Settings		Secondary					Configure
2.10 000		Tertiary					comgaro

CPPM Webサーバ証明書(HTTPS)の生成

この証明書は、ClearPassゲストポータルページがHTTPS経由でブランチのゲストWiFiに接続す るゲストクライアントに提示されるときに使用されます。

ステップ1:CAパブリッシャチェーン証明書をアップロードします。

[Administration] > [Certificates] > [Trust List] > [Add] に移動します。

-使用方法:他を有効にする

View Certificate Details		8
Subject DN:		
Issuer DN:		
Issue Date/Time:	Dec 23, 2020 16:55:10 EST	
Expiry Date/Time:	Dec 24, 2025 17:05:10 EST	
Validity Status:	Valid	
Signature Algorithm:	SHA256WithRSAEncryption	
Public Key Format:	X.509	
Serial Number:	86452691282006080280068723651711271611	
Enabled:	true	
Usage:	🗹 EAP 🗹 RadSec 🗹 Database 🔽 Others	
	Update Disable Export Close	

ステップ2:証明書署名要求を作成します。

[Administration] > [Certificates] > [Certificate Store] > [Server Certificates] > [Usage:HTTPSサーバ 証明書。

- [Create] [Certificate Signing Request]をクリックします

– 共通名:CPPM

-組織:cppm.example.com

SANフィールドに入力してください(必要に応じて、IPおよびその他のFQDNと同様に、SANに

も共通名が存在する必要があります)。形式はDNSです。<fqdn1>,DNS:<fqdn2>,IP<ip1>。

Create Certificate Signing Request					
Common Name (CN):	Create Certificate Signing Request				
Organization (O):	Cisco				
Organizational Unit (OU):	Engineering				
Location (L):	Toronto				
State (ST):	ON				
Country (C):	CA				
Subject Alternate Name (SAN):	DNS:cppm.example.com				
Private Key Password:	•••••				
Verify Private Key Password:	•••••				
Private Key Type:	2048-bit RSA ~				
Digest Algorithm:	SHA-512 ~				
	Submit Cancel				

ステップ3:選択したCAで、新しく生成されたCPPM HTTPSサービスCSRに署名します。

ステップ4:[Certificate Template] > [Web Server] > [Import Certificate] に移動します。

- 証明書タイプ:サーバ証明書

-使用方法:HTTPサーバ証明書

- 証明書ファイル: CA署名付きCPPM HTTPSサービス証明書を参照して選択します

Import Certificate			8
Certificate Type:	Server Certificate		
Server:	cppm v		
Usage:	HTTPS Server Certificate		
Upload Method:	Upload Certificate and Use Saved Private Key	~	
Certificate File:	Browse No file selected.		
		Import	Cancel

ネットワークデバイスとしてのC9800 WLCの定義

[Configuration] > [Network] > [Devices] > [Add] に移動します。

-Name : WLC_9800_Branch

- IPアドレスまたはサブネットアドレス:10.85.54.99(ラボトポロジ図を参照)
- RADIUS Shared Cisco:<WLC RADIUSパスワード>

- ベンダー名: 『シスコ

- [Enable RADIUS Dynamic Authorization]:1700

Add Device					
Device SNMP Read Settings St	MP Write Settings	LI Settings	OnConnect Enfor	cement Attributes	
Name:	WLC_9800_Branch				
IP or Subnet Address:	10.85.54.99	(e.g	., 192.168.1.10 or	192.168.1.1/24 or 19	2.168.1.1-20)
Description:	Cisco 9800 WLC for	Branch Gues	t <u>Wifi</u>		
RADIUS Shared Secret:			Verify:	•••••	
TACACS+ Shared Secret:			Verify:		
Vendor Name:	Cisco	*			
Enable RADIUS Dynamic Authorization	: 🔽 Port: 1700				
Enable RadSec:					

Add Cancel

ゲストポータルページとCoAタイマー

設定全体を通して正しいタイマー値を設定することが非常に重要です。タイマーが調整されてい ない場合は、クライアントが「実行状態」でない状態で、循環するWebポータルリダイレクトが 発生する可能性があります。 注意すべきタイマー:

 ポータルWebログインタイマー:このタイマーは、リダイレクトページがゲストポータルペ ージへのアクセスを許可する前にリダイレクトページを遅延させ、CPPMサービスに状態遷 移を通知し、エンドポイントカスタム属性の「Allow-Guest-Internet」値を登録し、CPPMか らWLCへのCoAプロセスをトリガーします。[Guest] > [Configuration] > [Pages] > [Web Logins] に移動します。

– ゲストポータル名を選択します。ラボ匿名ゲスト登録(このゲストポータルページの設定 は次のように詳細に説明されています)

- [Edit] をクリックします。

- ログイン遅延:6 seconds

* Login Delay: 6 C

• ClearPass CoA遅延タイマー:これにより、ClearPassからWLCへのCoAメッセージの発信が 遅延します。これは、CoA確認応答(ACK)がWLCから戻る前に、CPPMがクライアントエン ドポイントの状態を内部で正常に移行するために必要です。ラボテストでは、WLCからの 1ミリ秒未満の応答時間が示されます。また、CPPMがエンドポイント属性の更新を完了して いない場合、WLCからの新しいRADIUSセッションは非認証MABサービス適用ポリシーに一 致し、クライアントには再びリダイレクトページが与えられます。[CPPM] > [Administration] > [Server Manager] > [Server Configuration] に移動し、[CPPM Server] > [Service Parameters] を選択します。

- RADIUS Dynamic Authorization(DM/CoA)Delay:6秒に設定

aruda	LiearPass Policy Ma	nager
Dashboard O	Administration » Server Manager » Server Configuration - cppm	
Monitoring O	Server Configuration - cppm (10.85.54.98)	
🖧 Configuration 🔹 💿		
🔐 Administration 📀		
- A ClearPass Portal		
Users and Privileges	System Services Control Service Parameters System Monitoring Network FIPS	
🖃 🕍 Server Manager		
- 🧀 Server Configuration	Select Service: Async network services	
- 🥜 Log Configuration	Parameter Name	Parameter Value
- June 2018 - June	Ingress Event	
- Jucensing	Batch Dessering Interval	20 enconde
- Jevice Insight	Batch Processing Interval	seconds
External Servers	Command Control	
- Je External Accounts	RADIUS Dynamic Authorization (DM/CoA) Delay	6 seconds
🖃 🚔 Certificates	Enable SNMP Bounce Action	FALSE v
Certificate Store	Post Auth	
- January Contract List	Number of request processing threads	20 threads
Revocation Lists Dictionaries	Lazy handler polling frequency	5 minutes
Agents and Software Updates	Eager handler polling frequency	30 seconds
a Support	Connection Timeout	10 seconds
	Palo Alto User Identification Timeout	45 minutes

ClearPass: ゲストCWAの設定

ClearPass側のCWA設定は、(3)サービスポイント/ステージで構成されます。

ClearPassコンポーネント	サービスタイプ	目的
1.ポリシーマネージャ	Service(サービス):MAC 認証	カスタム属性Allow-Guest-Inte TRUEの場合は、ネットワーク 接続を許可します。それ以外の は、Redirectをトリガーし、C 認証。
2.ゲスト	Webログイン	匿名ログインAUPページを表示 す。 Post-auth set custom attribute Allow-Guest-Internet = TRUE。
3.ポリシーマネージャ	Service(サービス):Web ベース の認証	エンドポイントを既知に 更新 カスタム属性 Allow-Guest-Inte TRUEに設定します。 COA:再認証

ClearPassエンドポイントメタデータ属性: Allow-Guest-Internet

タイプがブールのメタデータ属性を作成して、クライアントが「Webauth Pending」と「Run」 状態の間を遷移するときにゲストエンドポイントの状態を追跡します。

- wifiに接続する新しいゲストには、デフォルトのメタデータ属性がAllow-Guest-Internet=falseに 設定されています。この属性に基づいて、クライアント認証はMABサービスを通過します - [AUP Accept]ボタンをクリックすると、ゲストクライアントのメタデータ属性がAllow-Guest-Internet=trueに更新されます。この属性をTrueに設定した後続のMABは、インターネットへのリ ダイレクトされないアクセスを許可します

[ClearPass] > [Configuration] > [Endpoints]に移動し、リストから任意のエンドポイントを選択し て、[Attributes] タブをクリックし、値をfalseにしてAllow-Guest-Internetを追加し、さらに値を Saveにします。

注:同じエンドポイントを編集し、この属性を後で削除することもできます。この手順では、ポリシーで使用できるエンドポイントメタデータDBにフィールドを作成するだけです。

Edi	t Endpoint				8
_	Endpoint Attributes				
	Attribute		Value		
1.	Allow-Guest-Internet	=	false 💌	Ð	Ť
2.	Click to add				

ClearPass再認証適用ポリシー設定

ゲストポータルページでクライアントがAUPを受け入れた直後にゲストクライアントに割り当て られる強制プロファイルを作成します。

[ClearPass] > [Configuration] > [Profiles] > [Add] に移動します。

- テンプレート:RADIUS動的認可

-Name : Cisco_WLC_Guest_COA

Enforcement Profiles

Profile Attribute	es Summary	
Template:	RADIUS Dynamic Authorization	~
Name:	Cisco_WLC_Guest_COA	
Description:		
Туре:	RADIUS_CoA	
Action:	Accept O Reject O Drop	
Device Group List:		Remove View Details Modify
	Select	~
半径:IETF	Calling-Station-Id	%{Radius:IETF:Calling-Station
半径:Cisco	Cisco-AVPair	subscriber:command=reauther
半径:Cisco	Cisco-AVPair	%{Radius:Cisco:Cisco- AVPair:subscriber:audit-sessio
半径:Cisco	Cisco-AVPair	subscriber:reauthenticate-type

ClearPassゲストポータルリダイレクト適用プロファイルの設定

「Allow-Guest-Internet」が「**true**」に設定されたCPPMエンドポイントデータベースでMACアド レスが見つからない場合、初期MABフェーズでゲストに適用される強制プロファイルを作成しま す。

type=last

これにより、9800 WLCは外部認証のためにゲストクライアントをCPPMゲストポータルにリダ イレクトします。

[ClearPass] > [Enforcement] > [Profiles] > [Add] に移動します。

-Name : Cisco_Portal_Redirect

-タイプ:RADIUS

-Action:Accept

Enforcement Profiles

Profile	Attributes	Summary	
Template:		Aruba RADIUS Enforcement	~
Name:		Cisco_Portal_Redirect	
Description	:		11.
Гуре:		RADIUS	
Action:		💿 Accept 🔘 Reject 🔘 Drop	
Device Gro	up List:		Remove
			View Details
			Modify
		Select v	

ClearPassリダイレクト強制プロファイル

同じダイアログの[Attributes] タブで、次のイメージに従って2つの属性を設定します。

Enforcement Profiles - Cisco_Portal_Redirect

_	Summary Profile Attributes				
	Туре	Name		Value	
1	. Radius:Cisco	Cisco-AVPair	-	url-redirect-acl=CAPTIVE_PORTAL_REDIRECT	60
2	. Radius:Cisco	Cisco-AVPair	=	url-redirect=https://cppm.example.com/guest/laccept.php?cmd- login&mac=%{Connection:Client-Mac-Address-Hyphen}&switchip=% {Radius:IETF:NAS-IP-Address}	6
_					

ClearPassリダイレクトプロファイル属性

url-redirect-acl属性は、C9800で作成されたACLの名前である**CAPTIVE-PORTAL-REDIRECT**に設 定されます。

注:RADIUSメッセージでは、ACLへの参照だけが渡され、ACLの内容は渡されません。 9800 WLC上で作成されたACLの名前が、次に示すように、このRADIUS属性の値と正確に 一致することが重要です。

url-redirect属性は、複数のパラメータで構成されます。

- ゲストポータルがホストされているターゲット URL(<u>https://cppm.example.com/guest/iaccept.php</u>)
- ゲストクライアントMAC、マクロ%{Connection:Client-Mac-Address-Hyphen}
- 認証者IP(9800 WLCがリダイレクトをトリガー)、マクロ%{Radius:IETF:NAS-IP-Address}
- cmd-login action

ClearPass Guest Web LoginページのURLは、[CPPM] > [Guest] > [Configuration] > [Pages] > [Web Logins] > [Edit] に移動すると表示されます。

この例では、CPPMのゲストポータルページ名はiacceptとして定義されています。

注:ゲストポータルページの設定手順は次のとおりです。

aruba		(
Guest O	Home » Configuration	n » Pages » Web Logins b Anonynous Guest Regist
Configuration	Use this form to make	e changes to the Web Login Lab Anon
 Authentication Content Manager Guest Manager Hotspot Manager Pages 	* Name: Page Name:	Lab Anonynous Guest Registration Enter a name for this web login page. iaccept Enter a page name for this web login. The web login will be accessible from "/guest/
 Image Fields Image Forms Image List Views Self-Registrations 	Description:	Comments or descriptive text about the web I
- 🥵 Web Logins - 🔍 Web Pages	* Vendor Settings:	Aruba Networks Select a predefined group of settings suitable

注:シスコデバイスの場合、通常はaudit_session_idが使用されますが、他のベンダーでは サポートされていません。

ClearPassメタデータ強制プロファイルの設定

CPPMによる状態遷移の追跡に使用されるEndpointメタデータ属性を更新するように、強制プロファイルを構成します。

このプロファイルは、エンドポイントデータベースのゲストクライアントMACアドレスエントリ に適用され、「Allow-Guest-Internet」引数を「true」に設定します。

[ClearPass] > [Enforcement] > [Profiles] > [Add] に移動します。

- テンプレート: ClearPassエンティティ更新の強制

-タイプ:Post_Authentication

Enforcement Profiles

Profile	Attributes	Summary
Template:		ClearPass Entity Update Enforcement
Name:		Make-Cisco-Guest-Valid
Descriptior	י:	
Туре:		Post_Authentication
Action:		Accept O Reject O Drop

同じダイアログで、[Attributes] タブを選択します。

-タイプ:エンドポイント

-Name : Allow-Guest-Internet

注:この名前をドロップダウンメニューに表示するには、手順で説明されているように、少なくとも1つのエンドポイントに対してこのフィールドを手動で定義する必要があります。

-値:true

Co	Configuration » Enforcement » Profiles » Add Enforcement Profile						
E	Enforcement Profiles						
F	Profile Attributes Summary						
_	Type Name Value						
	Туре			Name		Value	
1.	Type Endpo	oint	•	Name Allow-Guest-Internet	=	Value true	•

ClearPassゲストインターネットアクセス適用ポリシーの設定

[ClearPass] > [Enforcement] > [Policies] > [Add] に移動します。

-Name:WLCのCiscoゲスト許可

- 適用タイプ:RADIUS

- デフォルトプロファイル:Cisco_Portal_Redirect

Configuration » Enforcement » Policies » Add

Enforcemer	Enforcement Policies						
Enforcement	Rules	Jummary					
Name:		WLC Cisco Guest Allow					
Description:							
Enforcement Typ	e:	● RADIUS ● TACACS+ ○ WEBAUTH (SNMP/Agent/CLI/CoA) ○ Application ○ Event					
Default Profile:		Cisco_Portal_Redirect View Details Modify					

同じダイアログで、[Rules] タブに移動し、[Add Rule] をクリックします。

-タイプ:エンドポイント

-Name : Allow-Guest-Internet

-Operator : [Equals]

- 値True

– プロファイル名/追加する選択:[RADIUS] [Allow Access Profile]

Rules Editor					•
	c c	Conditions			
Match ALL of the follow	ving conditions:				
Туре	Name	Operator	Value		
1. Endpoint	 Allow-Guest-Internet 	EQUALS	▼ true	•	D +
2. Click to add					
	Enforc	cement Profiles			
Profile Names:	[RADIUS] [Allow Access Profile] Move Up ↑				
	Move Down ↓				
	Remove	l l			
	Select to Add	~			
				Save	Cancel

ClearPassゲストのAUP後の適用ポリシーの設定

[ClearPass] > [Enforcement] > [Policies] > [Add] に移動します。

-Name:Cisco WLC Webauth適用ポリシー

- 適用タイプ:WEBAUTH (SNMP/エージェント/CLI/CoA)

- デフォルトプロファイル:[RADIUS_CoA] Cisco_Reauthenticate_Session

Configuration » Enforcement » Policies » Add

Enforcement Policies

Enforcement	Rules	Summary
Name:		Cisco WLC Webauth Enforcement Policy
Description:		
Enforcement Typ	e:	○ RADIUS ○ TACACS+
Default Profile:		[RADIUS_CoA] Cisco_Reauti ~ View Details Modify

同じダイアログで、[Rules] > [Add] に移動します。

-条件:[Authentication]

-Name:ステータス

-Operator : [Equals]

-値:User

- プロファイル名: <それぞれに追加>:
- [Post Authentication] [Update Endpoint Known]
- [認証後] [Make-Cisco-Guest-Valid]
- [RADIUS_CoA] [Cisco_WLC_Guest_COA]

Rules Editor				0
		Conditions		
Match ALL of the follow	ing conditions:			
Туре	Name	Operator	Value	
1. Authentication	Status	EQUALS	User	Ba 11
2. Click to add				
		Enforcement Profiles		
Profile Names:	[Post Authentication] [Update Endpoint Known]			
	[Post Authentication] Make-Cisco-Guest-Valid	Move Up ↑		
	[RADIUS_CoA] Cisco_WLC_Guest_COA	Move Down ↓		
		Remove		
	Select to Add	~		
				Save Cancel

注:継続的なゲストポータルリダイレクト疑似ブラウザのポップアップが表示されるシナリ オが発生した場合は、CPPMタイマーの調整が必要か、CPPMと9800 WLCの間でRADIUS CoAメッセージが正しく交換されていないことを示しています。これらのサイトを確認しま す。

- [CPPM] > [Monitoring] > [Live Monitoring] > [Access Tracker] に移動し、RADIUSログエントリに RADIUS CoAの詳細が含まれていることを確認します。

- **9800 WLC**で、[Troubleshooting] > [Packet Capture] に移動し、RADIUS CoAパケットの到着が 予想されるインターフェイスでpcapを有効にし、RADIUS CoAメッセージがCPPMから受信され

ることを確認します。

ClearPass MAB認証サービスの設定

サービスは、属性値(AV)ペアのRADIUSで照合されます。『シスコ | CiscoAVPair | cisco-wlanssid

[ClearPass] > [Configuration] > [Services] > [Add] に移動します。

[Service]タブ:

-Name:ゲストポータル – Mac認証

-タイプ:MAC 認証

- その他のオプション: [Authorization]、[Profile Endpoints]の選択

一致ルールの追加:

-タイプ:Radius:『シスコ

-Name : Cisco-AVPair

-Operator : [Equals]

-値:cisco-wlan-ssid=Guest(設定したゲストSSID名と一致)

注:「Guest」は、9800 WLCによってブロードキャストされるゲストSSIDの名前です。

Confi	onfiguration » Services » Add										
Ser	rvices										
Ser	vice Authentication	Authorization	Roles	Enforcement	Profiler	Summary					
Туре	ype: MAC Authentication										
Nam	e:	GuestPortal - Mac A	uth								
Desc	Description: MAC-based Authentication Service										
Moni	tor Mode:	Enable to monite	or networ	k access without	enforcemer	nt					
More	Options:	Authorization	Audit E	nd-hosts 🗹 Pro	ile Endpoin	ts [] Account	ing Proxy				
						Serv	ice Rule				
Matcl	nes 🔘 ANY or 🧿 ALI	L of the following co	nditions:								
	Туре		Na	ame			Operator	Value			
1.	Radius:IETF		NA	S-Port-Type			BELONGS_TO	Ethernet (15), Wire	eless-802.11 (19)	6 <u>6</u>	÷
2.	Radius:IETF		Se	rvice-Type			BELONGS_TO	Login-User (1), Ca	ll-Check (10)	66	Ť
3.	Connection		Cli	ent-Mac-Address			EQUALS	%{Radius:IETF:Us	er-Name}	6	Ť
4.	Radius:Cisco		Ci	sco-AVPair			EQUALS	cisco-wlan-ssid=G	Jest	66	Ť

同じダイアログで、[Authentication] タブを選択します。

-認証方式:[MAC AUTH]を削除し、[Allow All MAC AUTH]を追加します。

– 認証元 : [エンドポイントリポジトリ][ローカルSQL DB]、[ゲストユーザリポジトリ][ローカル SQL DB]

aruba	ClearPass Policy Manager						
Dashboard 0	Configuration	» Services	» Edit - GuestPort	al - Mac Auth			
Monitoring O	Services	- Guest	Portal - Mac	Auth			
🔏 Configuration 📀	Summary	Service	Authentication	Authorization	Roles	Enforcement	Profiler
—	Authentication	n Methods:	[Allow All MAC A	.0тнј		Marca Unit]
- Authentication					-	Move Up 1	
- 🗘 Methods					-	Remove	
- 🗘 Sources						Kemove	
- <u>Q</u> Identity						view Details	J
- 🛱 Single Sign-On (SSO)						Modify	J
- 🛱 Local Users							
- 🛱 Endpoints			Select to Add	•	~		
- 🛱 Static Host Lists	Authentication	n Sources:	[Endpoints Repo	sitory] [Local SQL D	B]		
- 🛱 Roles			[Guest User Rep	ository] [Local SQL	DB]	Move Up ↑]
🛱 Role Mappings						Move Down ↓	
+- 🖶 Posture						Remove	í
Enforcement						View Details	
- 🛱 Policies						Ne dife]
right Profiles					L	Modity	J
Network			Select to Add			~	
- 🗘 Devices	Chris Hears	Dulas.			nambed 1		
- 🖧 Device Groups	Strip Usernan	ne Kulës:	Enable to sp	eciry a comma-se	parated lis	st of rules to strip	username prefixes or suffixes
H D To to							

同じダイアログで、[Enforcement] タブを選択します。

- 適用ポリシー:WLCのCiscoゲスト許可

Configuration » Services » Add

Services

Service	Authentication	Roles	Enforcement	Summary					
Use Cached Results:		🗌 Use cach	ed Roles and Pos	sture attribute	s from prev	vious ses	sions		
Enforcemer	nt Policy:	WLC Cisco	Guest Allow	~)	Modify				
						Enfo	orcement F	olicy Deta	ails
Description	:	MAB Enfor	cement Redirect						
Default Pro	file:	Cisco_Port	al_Redirect						
Rules Evalu	ation Algorithm:	first-applic	able						
Cond	ditions								Enforcement Profi
1. (Endpoint:Allow-Guest-Internet EQUALS true)								[Allow Access Profile	

同じダイアログで、[Enforcement] タブを選択します。

Configuration » Services » Add

Services

Service	Authentication	Authorization	Roles	Enforcement	Profiler	Summary	
Endpoint Cl	assification:	Select the classifica	ation(s) af	ter which an a	ction must be Remove	triggered -	
RADIUS Co	A Action:	Cisco_Reauthentica	te_Sessio	1	View Det	ails Modify	

ClearPass Webauthサービスの設定

[ClearPass] > [Enforcement] > [Policies] > [Add] に移動します。

-Name : Guest_Portal_Webauth

-タイプ:Web ベースの認証

Configuration » Services » Add

Services

Ser	vice	Authentication	Roles	Enforcement	Summary	
Туре	:		Web-based	d Authentication		~
Name	e:		Guest			
Desc	ription	:				11.
Moni	tor Mo	de:	🗌 Enable t	o monitor networ	k access with	out enforcement
More	Option	ns:	🗌 Authoriz	ation 🗌 Posture	Compliance	
						S
Match	nes ()	ANY or 🧿 ALL	of the follo	wing conditions:		
	Туре	•		Na	ame	
1.	Host			Cł	neckType	
2.	Click	to add				

同じダイアログの[Enforcement] タブで、[Enforcement Policy:Cisco WLC Webauth Enforcement Policy_o

Configuratio	on » Services » A	bb			
Services	5				
Service	Authentication	Roles	Enforcement	Summary	
Use Cached	Results:	Use cach	ied Roles and Po	sture attribute	es from previous sessions
Enforcemen	t Policy:	Cisco WLC	Webauth Enforce	ment Policy	Modify Add New Enforcement Pol
					Enforcement Policy Details
Description	:				
Default Prof	file:	Cisco_Rea	uthenticate_Ses	sion	
Rules Evalu	ation Algorithm:	first-applic	able		
Cond	litions				Enforcement Profiles
1 (Au	theoptication (Ctate		Licer)		[Undate Endapint Known] Make Class Quart Valid, Class Deputhentiente Session

thentication:Status EQUALS User)

ClearPass:Webログイン

Anonymous AUP Guest Portalページでは、パスワードフィールドのない単一のユーザ名を使用し ます。

使用するユーザ名には、次のフィールドが定義または設定されている必要があります。

username_auth |ユーザー名認証:|1

[[]Update Endpoint Known], Make-Cisco-Guest-Valid, Cisco_Reauthenticate

ユーザの「username_auth」フィールドを設定するには、そのフィールドを最初に「edit user」 フォームで公開する必要があります。[ClearPass] > [Guest] > [Configuration] > [Pages] > [Forms] に移動し、[create_user] フォームを選択します。

aruba	Cle	arPass Guest			
🖳 Guest 🛛 🛛 0	Home » Configuration » Pages » Forms				
👔 Devices 🔹 📀	Customize Forms				
Configuration	Use this list view to customize the forms within the application.				
- 🍣 Authentication	△ Name	Title			
Content Manager Original Private Files	change_expiration Change the expiration time of a single guest account.	Change Expiration			
Public Files	create_multi Create multiple guest accounts.	Create Multiple Guest Accounts			
🛃 Guest Manager 🖅 🌯 Hotspot Manager	create_multi_result Create multiple accounts results page.	Create Multiple Accounts Results			
Pages	Create a single guest account.	Create New Guest Account			
	Edit Edit Fields Constants Edit Fields Constants Edit Fields Edit Fields	🍕 Show Usage 🧕 Translations			
Self-Registrations	Create single guest account receipt.	Create New Guest Account Receipt			
- 🔐 Web Logins	🖂 quest edit				

visitor_name(行20)を選択し、[Insert After] をクリックします。

Home » Configuration » Pages » Forms

Customize Form Fields (create_user)

Use this list view to modify the fields of the form create_user.

() Q	uick Help			Preview Form
 Rank	Field	Туре	Label	Description
1	enabled	dropdown	Account Status:	Select an option for changing the status of this account.
10	sponsor_name	text	Sponsor's Name:	Name of the person sponsoring this account.
13	sponsor_profile_name	text	Sponsor's Profile:	Profile of the person sponsoring this account.
15	sponsor_email	text	Sponsor's Email:	Email of the person sponsoring this account.
20	visitor_name	text	Guest's Name:	Name of the guest.
📑 E	dit 🛛 🚡 Edit Base Field	😣 Remove	峇 Insert Before 🕞	Insert After Disable Field

Customize Form Field (new)

Use this form to add a new field to the form create_user.

	Form Field Editor
* Field Name:	username_auth
Form Display Prope These properties control the	user interface displayed for this field.
Field:	Enable this field When checked, the field will be included as part of the form.
* Rank:	22 Number indicating the relative ordering of user interface fields, which are displayed in order of increasing rank.
* User Interface:	No user interface Revert Re
Form Validation Pro	the value of this field is checked.
Field Required:	Field value must be supplied Select this option if the field cannot be omitted or left blank.
Initial Value:	Revert to initialize this field with when the form is first displayed.
* Validator:	IsValidBool The function used to validate the contents of a field.
Validator Param:	(None) V Optional name of field whose value will be supplied as the argument to a validator.
Validator Argument:	Optional value to supply as the argument to a validator.
Validation Error:	The error message to display if the field's value fails validation and the validator does not return an error message directly.

ここで、AUPゲストポータルページの背後で使用するユーザ名を作成します。

[CPPM] > [Guest] > [Guest] > [Manage Accounts] > [Create] に移動します。

- ゲスト名:GuestWiFi

-会社名:『シスコ

- 電子メールアドレス: guest@example.com

- ユーザ名認証: ユーザ名のみを使用してゲストアクセスを許可する: 有効

- アカウントの有効化:現在

- アカウントの有効期限:アカウントは期限切れになりません

- 使用条件:私がスポンサーです。有効

Create Guest Account

New guest account being created by admin.

Create New Guest Account					
* Guest's Name:	GuestWiFi Name of the guest.				
* Company Name:	Cisco Company name of the guest.				
* Email Address:	guest@example.com The guest's email address. This will become their username to log into the network.				
Username Authentication:	✓ Allow guest access using their username only Guests will require the login screen setup for username-based authentication as well.				
Account Activation:	Now Select an option for changing the activation time of this account.				
Account Expiration:	Account will not expire Select an option for changing the expiration time of this account.				
* Account Role:	[Guest] v Role to assign to this account.				
Password:	281355				
Notes:					
* Terms of Use:	I am the sponsor of this account and accept the terms of use				
	Create				

Webログインフォームを作成します。[CPPM] > [Guest] > [Configuration] > [Web Logins] に移動 します。

事後認証セクションのエンドポイント属性:

username |ユーザー名 visitor_name |訪問者名 cn |訪問者名 visitor_phone |ビジターの電話番号 電子メール |電子メール メール |電子メール sponsor_name |スポンサー名 sponsor_email |スポンサー電子メール **Allow-Guest-Internet | true**

aruba		ClearPass Guest
Guest 0 Deckes 0		Web Login Editor
Onlocand 0	* Name:	Tortar a name for this web legin page.
Configuration 0	Page Name:	The end logs value for the web logic. The end logic will be assessable from "(parti)page, narrowale".
K Authentication		
Private Files	Description:	
Guest Manager	* Vendor Settinger	Andra Mathania VI
Hotapet Henager	- and a secondar	Solar a personal proc of extrap advance for standard review tamperation. Solar a contract — Change of automatics (PCCISTR) solar to sandader Y
- Telds	Lagin Method:	server how the user instance upon will be handled. Bener-instance legene require the user's MMC address to be avoidable, usually from the captive portal redirection process.
- Torms Ust Views	Page Redirect Dataset for spectrum page	eterotype parced in the initial reduvet.
Self-Repotrations	becarity made	Co rat sheek - login will always be permitted w
Web Logins	Louis from	Dar Bis splan is detert of an UEL parameters have been multiplied by the aver, for manyle their NEC address.
Receipts	Options for specifying the	a laboving and context of the logic form.
Translations		Anarymaus - De tet negute a saamene er password V Seconda samene seconda programme.
	Autor destant	Accuracy allows a blank from requiring just the terms or a Log in factors. A pre-existing account is required, Acts is similar to anonymus but the page is externational submitted.
		Access Calo and Ananymeus requires the access to have the Usemanie Authentication Field ed. Oreate a new anonymeus access to
	Aata-Generate:	The accurate will be created without a sectory test or expenditors from, and with the fluent rate (10-2), testar a value for "econymous been" to use a specific username, or leave totals to randomly generate a username.
		Ours/WP1
	* Ananymeus Geert	The parameter will be which within the HTML. It is reconversated in increase the account Density Divit in the monitor of guards you with its support.
	Descent Chile:	Enable bypassing the Apple Capitive Matwork Assistant
Administration 0	r sundrik Carlie	Note that this option interview into work with all vandors, depending on how the captive pertail is implemented.
	Quatom Form:	(c) Preside a cadare legit form E schedel, yns med sopply ywr ann KTM, legit fam is the Header in Faster KTM, anna.
	Curtore Labels:	Override the default labels and error messages Facebook, you will be able to able labels and error messages for the summit legit form.
	* Pro-Auth Check:	Lacal — match a local account v
	in the second	and a second second and particular and an experimental and a second processing of the MC antibacturation.
	Pre-Auth Error:	The best to display if the coentains and password lookup fails. Laure blant to use the default (bruthd coentains or password).
	Terms:	Bequire a Terms and Conditions confirmation If should, the user will be forced to accept a Terms and Conditions shouldes.
	Terms Label-	The form label for the tarme cherolice.
	Carlos Cardos	Lauve Mark to use the default (Yerma).
	Terms Text)	
		#THL code cartaining your Terms and Conditions.
		Laws Mark to use the default () accept the name+" (was, global name-guest, account, terms, of, use, ant/" target=", block">terms of use n/m>). (Namber balance terms of acception of a
	Terma Layout:	Rebuilt the layout for the large and conditions load.
	Terms Error:	The text to display if the terms are not accepted.
	CAPTOR-	Name
		arrespi and common
	Leg to Label	The form table for the lag in tubles. Sense blank to use the default (sig in).
	Translations	Skip submitte translation handling New Skits and pages have translation analistic under Configuration + Translations + Page Customizations, Salect this option to keep all text as default.
	Default Destination	
	Options for contraining t	Periodia and the second se
	* Default URL	Initar the default URL to redrect clients. Heade ensure you prepend "Http://" for any external demans.
	Override Destination:	Porce default deplination for all clients Proce default destination will be oversible regardless of its value.
	Login Page Options for controlling	Her lands and Heel of Her lagin page.
	* Skin:	Gen Fass Gues Skin v
		Anonymous Guest WHITI Die Hist ogen page is onsoletet.
	Tick:	The title to deplay on the web login page, cases black to any the default (Login).
		(www_enablierhech)
		Chendby Chend sular = "savy"> Chend sular = "savy">
		Carbo
	Header HTML	Garb (Fank malay = "black">
		surgement and Conditions:(70) Sphile more you review the forms and Conditions in the link being because by deciding the tick has and
		selecting "Register", you are confirming that you've
		WTHL inequisite code singleyed before the logic form.
		(nwa_text_id=78/3) sp= Contact_s staff member if you are experiencing
		Mifficulty legalsg in. */p=(/me_text)
	Trace Pairs	
	Advertising Service	- The test of Second shall be deploying the legis message.
	Evaluate advertising control	en an the lagin page.
	Cleve Libert Ry	L. Initial Admitting Service context
	Optionally present quest	to with various dout identity / social legit options.
	Hulti-Paster Authen	un er einen vegnet eine sande annen promationen einen bereiten. Abzeiten
	Require a recordary fac	tor when suffering the second se
	Network Login Acce	100 CONTRACTOR (CONTRACTOR)
	Cartirols assess to the Is	lip tele-
	Allowed Access	
		Enter the IP addresses and retworks from which logits are permitted.
	Denied Access:	
		tinder the 3P addresses and redworks that are denied topic access.
	* Deny Behaviari	Earled HTTP 434 Mel Found status v Earled the requests of the system to a request that is not preveiling.
	Post-Authentication Astern to perform play	a waaraalal yee achtesiaalaa.
	Health Check	Require a successful OnGuard health check
	Balance and	In process, the sust will be received to case a health check prior to accessive the retwork. Mark the user's Mic address as a known wrigher?
	upeate chopoate	If delotad, the endpoint's attributes will also be updated with other details from the user account.
	Atvanced	United to the second se
	Endpoint data in Ann	visitor_meme Visitor Name cm Nisitor Name
	Longoon, new public	Visitor shore Visitor Phene /

検証:ゲストCWA認証

CPPMで、[Live Monitoring] > [Access Tracker] に移動します。

MABサービスに接続してトリガーする新しいゲストユーザ。

[Summary]タブ:

Request Details							
Summary	Input	Output	RADIUS CoA				
Login Status:		ACCE	т				
Session Identi	ifier:	R0000)471a-01-6282a	110			
Date and Time	e:	May 1	6, 2022 15:08:	00 EDT			
End-Host Ider	ntifier:	d4-3b	-04-7a-64-7b	(Computer / Windows / Wind	ows)		
Username:		d43b0	47a647b				
Access Device	e IP/Port:	10.85	.54.99:73120	(WLC_9800_Branch / Cisco)			
Access Device	e Name:	wlc01					
System Postu	re Status:	UNKN	OWN (100)				
Policies Used -							
Service:		Guest	SSID - GuestPo	ortal - Mac Auth			
Authentication	n Method:	MAC-A	AUTH				
Authentication	n Source:	None					
Authorization	Source:	[Gues	t User Repositor	ry], [Endpoints Repository]			
Roles:		[Empl	oyee], [User Au	thenticated]			
Enforcement F	Profiles:	Cisco	Portal_Redirect				
I ≤ Showing 8 of 1-8 records ► ► Change Status Show Configuration Export Show Logs Close							

同じダイアログで、[Input] タブに移動します。

Request Details			
Summary Input	Output	RADIUS CoA	
Username:	d43b047a64	17b	
End-Host Identifier:	d4-3b-04-7a	a-64-7b (Computer / Windows / Windows)	
Access Device IP/Port:	10.85.54.99	9:73120 (WLC_9800_Branch / Cisco)	
RADIUS Request			•
Radius:Airespace:Air	respace-Wlan-	Id 4	
Radius:Cisco:Cisco-A	AVPair	audit-session-id=6336550A00006227CE452457	
Radius:Cisco:Cisco-A	AVPair	cisco-wian-ssid=Guest	
Radius:Cisco:Cisco-A	VPair	client-iif-id=1728058392	
Radius:Cisco:Cisco-A	VPair	method=mab	
Radius:Cisco:Cisco-A	VPair	service-type=Call Check	
Radius:Cisco:Cisco-A	VPair	vlan-id=21	
Radius:Cisco:Cisco-A	VPair	wlan-profile-name=WP_Guest	
Radius:IETF:Called-S	Station-Id	14-16-9d-df-16-20:Guest	
Radius:IETF:Calling-	Station-Id	d4-3b-04-7a-64-7b	
I ◄ Showing 8 of 1-8	records 🕨 🕨	Change Status Show Configuration Export Show Logs	Close

同じダイアログで、[Output] タブに移動します。

Request Details						
Output RADIUS CoA						
Cisco_Portal_Redirect						
UNKNOWN (100)						
UNKNOWN (100)						
RADIUS Response						
	1					
'Pair url-redirect-acl=CAPTIVE_PORTAL_REDIRECT						
'Pair url-redirect=https://cppm.example.com/guest/iaccept.php?cmd-login&mac=d4-3b- 04-7a-64-7b&switchip=10.85.54.99						
	Output RADIUS CoA Cisco_Portal_Redirect UNKNOWN (100) UNKNOWN (100) UNKNOWN (100) Pair url-redirect-acl=CAPTIVE_PORTAL_REDIRECT Pair url-redirect=https://cppm.example.com/guest/iaccept.php?cmd-login&mac=d4-3b- 04-7a-64-7b&switchip=10.85.54.99					

8

I < Showing 8 of 1-8 records ► ► Change Status Show Configuration Export Show Logs Close</p>

参考として、Cisco 9800外部、アンカーコントローラとRADIUSサーバおよび外部ホスト型ゲス

トポータルとのインタラクションの状態フロー図を示します。

				9800 Foreign-WLC Guest Portal CWA flow					
Clie	AP	WLC-F	WLC-J	Inchor	рнср р	NS	adius	Guest	Portal(CPPM)
p.	[Client Assocication]						—	1	
1	[1] Assoc Regu	est 🔸							
	Guest Client joli								
			[MAB procedure]						
				ACCESS-Request Clessionic+1E1E1E1E02000000.0F3F8768899	-	[3] #REDIRECT URL>##REDIRECT URL>##Thessionid			
			[4] Access-Accept [] <redirect url="">, <redirect acl="">] <redirec< td=""><td>T_URL>: https://<copm.fpdn.com>/guest/<page.name>.php?session</page.name></copm.fpdn.com></td><td>Id+1E1E1E02</td><td>0000003F3F8768696portal=194a5780)</td><td>-</td><td></td><td></td></redirec<></redirect></redirect>	T_URL>: https:// <copm.fpdn.com>/guest/<page.name>.php?session</page.name></copm.fpdn.com>	Id+1E1E1E02	0000003F3F8768696portal=194a5780)	-		
	10 Acres Barrie	L							
		*196	[6] Export Anchor Request [<redirect url="">, <redirect acl="">, <vlan>]</vlan></redirect></redirect>						
			[7] Export Anchor Response						
			Foreign: Client goes to run state. Traffic is forwarded on Mobility Tunnel (CAPWAP)						
	(External WebAuth)				-			1	
	(contrast of contrast,		(8) Redirect ACL enforcement for Client <mac_addr></mac_addr>						
	[Client IP DHCP Process]			•	÷				
				Client goes to DHCP-Required stats	1				
			AND AND A LOT MANY AND						
	IN PARTS Have been		The provide statement allows price, they include the						
	[9] DHCP Handsh	hake +	[10] CHCP Handshake [12] MSG: scient iso	[11] DHCP Handshake	•				
				Cleant open to webauth peopling state	1				
L					-				
	[Client OS Guest Portal Detection]					1			
	[13] DNS Query www.msttconnect	om is at IP HIX X X X ICAPWAP	[14] DNS Query (CAPRAP)	1151 DNS Query					
	(19) TCP SYN IP <xxxx>30</xxxx>	(msftconnecttest)	[20] TCP SYN (CAPWAP)						
				Anchor: «REDIRECT_ACL>: redirect enforced					
	[22] TCP SYN-ACK	UACK	[21] TCP SYN ACK/ACK spoofing <x.x.x.x> (WebAuth <global> VP)</global></x.x.x.x>						
	[23] HTTP GET http://www.msftconnec	cttest.com/connecttest.txt	[24] HTTP GET (CAPWAP)						
	[26] HTTP-302 Redirect Location-Guest Po	VINICPPM) «REDIRECT URL»	[25] HTTP-302 (CAPWAP)						
	Display Pseudo Browse								
	[27] DNS Query <redi< td=""><td>NECT URL></td><td>[28] DNS Query (CAPWAP)</td><td>[29] DNS Query</td><td></td><td>F</td><td></td><td></td><td></td></redi<>	NECT URL>	[28] DNS Query (CAPWAP)	[29] DNS Query		F			
	(32) DNS Response <redirect td="" u<=""><td>RL> IS M. P. <y, td="" y,="" y<=""><td>[31] DNS Response (CAPWAP)</td><td>[30] DNS Response</td><td></td><td>]</td><td></td><td></td><td></td></y,></td></redirect>	RL> IS M. P. <y, td="" y,="" y<=""><td>[31] DNS Response (CAPWAP)</td><td>[30] DNS Response</td><td></td><td>]</td><td></td><td></td><td></td></y,>	[31] DNS Response (CAPWAP)	[30] DNS Response]			
	Client must trust Guest Portal certificate								
				Anchor: <redirect_acl>: redirect bypass <vvv.v.> (Guest Porta</vvv.v.></redirect_acl>	h				
	1331 Guest Portall CRIME TCP. SYN/SYN ACK	ACK on a second 3 (CARWAR)	That TOP, SYNCHIA A KIACK (CARWAR)			DATE TO A STREET ACKNOW			
	(36) HTTP GET «REDIRECT	URL/sessionid>	[37] HTTP GET (CAPWAP)			[38] HTTP GET			1
	(41) HTTP/1.1.20	0.0K	[40] HTTP/L.1.200.0K (CAPWAP)	4		[39] HTTP:1.1 200 OK			-
	Client clicks 'Accept' AUP button								
	(42) HTTP POST/HTTP1	1.1 200 OK	[43] HTTP POST/HTTP1.1 200 OK	4		[44] HTTP POST/HTTP1.1 200 OK			•
							[45] Update En	<pre>idpoint D8: <client_mac>:AllowInternetAccess=T</client_mac></pre>	
								[46] Captive Portal page refresh de	elay
		alt	(CoA Reauth)						
						[47] CoA delay tim			
			•	481 CoA Request (Type= <reauthenticate>, <sessionid>)</sessionid></reauthenticate>	-		-		
			[MAB]	[49] CoA Ack (<sessionid>)</sessionid>	-		×.		
				[50] Access Request (<sessionid>)</sessionid>					
			•	[51] Access Accept (No redirect URL, «sessionid»)	_				
			(52) Export Anchor Reguest				T		
			[53] Export Anchor Response. No [<redirect_url>, <redirect_acl>]</redirect_acl></redirect_url>						
				Anchor: Client goes to run state					
				1541 HTTP GETAITTP 2000K Landing Page	1				
				Client goes to RUN state					
_									
Clie	AP AP	WLC-F	oreign WLC-4	Inchor	рнср р	NSR	adius	Guest	Portal(CPPM)

アンカーWLCを使用したゲストセントラルWeb認証の状態図

関連情報

- <u>Cisco 9800 Deployment Best Practices Guide</u>
- <u>Catalyst 9800ワイヤレスコントローラの設定モデルについて</u>
- Catalyst 9800ワイヤレスコントローラでのFlexConnectについて
- <u>テクニカル サポートとドキュメント Cisco Systems</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。