

Configurar a integração da WLC 9800 com o Aruba ClearPass - Dot1x & FlexConnect para implantação em filiais

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Fluxo de tráfico](#)

[Diagrama de Rede](#)

[Configurar o Catalyst 9800 Wireless Controller](#)

[C9800 - Configurar parâmetros AAA para dot1x](#)

[C9800 - Configure o perfil de WLAN 'Corp'](#)

[C9800 - Configurar perfil de política](#)

[C9800 - Configurar marcação de política](#)

[C9800 - Perfil de junção de AP](#)

[C9800 - Perfil Flex](#)

[C9800 - Marca do local](#)

[C9800 - Tag de RF](#)

[C9800 - Atribuir tags ao AP](#)

[Configurar o Aruba CPPM](#)

[Configuração inicial do Aruba ClearPass Policy Manager Server](#)

[Aplicar licenças](#)

[Adicione o controlador sem fio C9800 como um dispositivo de rede](#)

[Configurar o CPPM para Usar o Windows AD como uma Origem de Autenticação](#)

[Configurar o Serviço de Autenticação CPPM Dot1X](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve a integração do Catalyst 9800 Wireless Controller com o Aruba ClearPass Policy Manager (CPPM) e o Microsoft Active Directory (AD) para fornecer autenticação dot1x a clientes sem fio em uma implantação Flexconnect.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento desses tópicos e que eles tenham sido configurados e verificados:

- Controlador sem fio Catalyst 9800
- Aruba ClearPass Server (requer licença de plataforma, licença de acesso, licença integrada)
- Windows AD operacional
- Autoridade de certificação (CA) opcional
- Servidor DHCP operacional
- Servidor DNS operacional (necessário para validação de CRL de certificado)
- ESXi
- Todos os componentes pertinentes são sincronizados com o NTP e verificados para ter a hora correta (necessária para validação do certificado)
- Conhecimento de tópicos: Implantação do C9800 e novo modelo de configuração Operação FlexConnect no C9800 Autenticação Dot1x

Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de hardware e software:

- C9800-L-C Cisco IOS-XE 17.3.3
- APs C9130AX, 4800
- Aruba ClearPass, patch 6-8-0-109592 e 6.8-3
- Servidor MS Windows Active Directory (GP configurado para emissão automatizada de certificados baseada em computador para endpoints gerenciados) Servidor DHCP com opção 43 e opção 60 Servidor DNS Servidor NTP para sincronizar com o tempo todos os componentes CA

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Fluxo de tráfego

Em uma implantação empresarial típica com várias filiais, cada filial é configurada para fornecer acesso dot1x aos funcionários corporativos. Neste exemplo de configuração, o PEAP é usado para fornecer acesso dot1x a usuários corporativos através de uma instância ClearPass implantada no data center central (DC). Os certificados de máquina são usados em conjunto com a verificação das credenciais do funcionário em um servidor Microsoft AD.

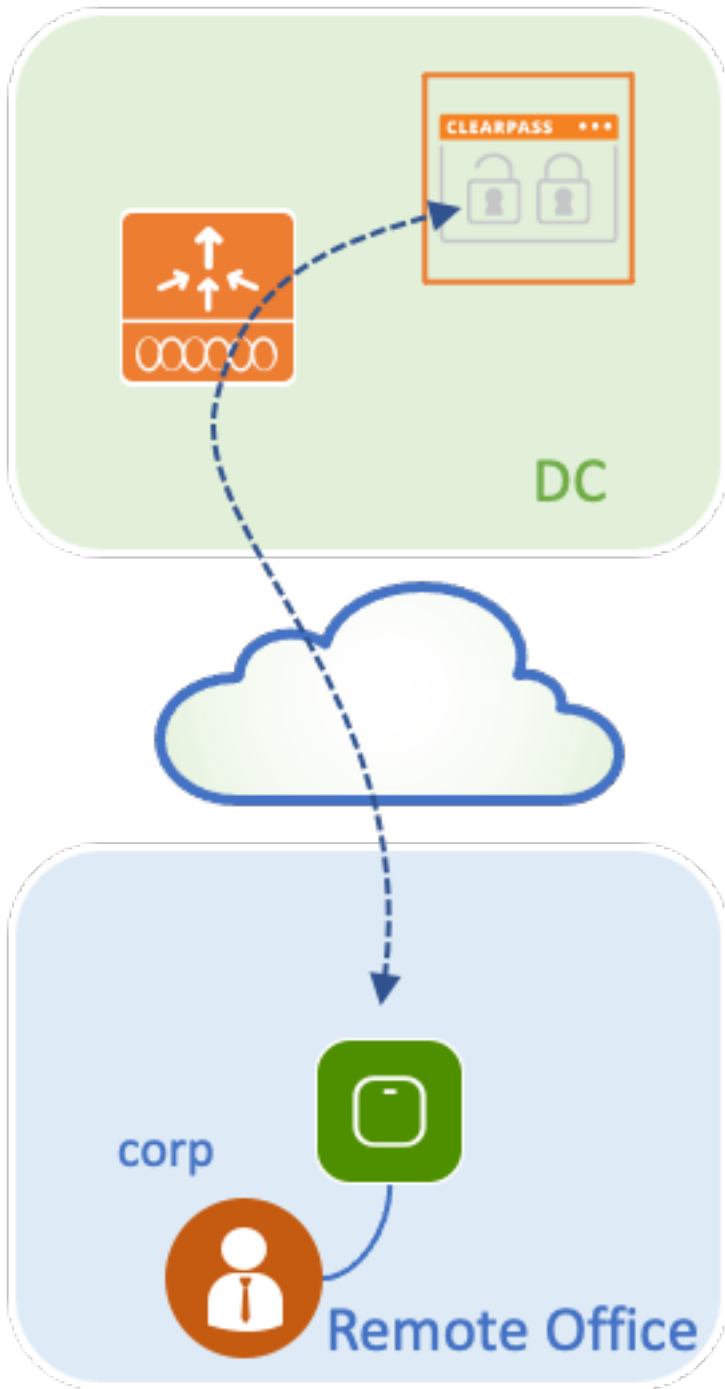
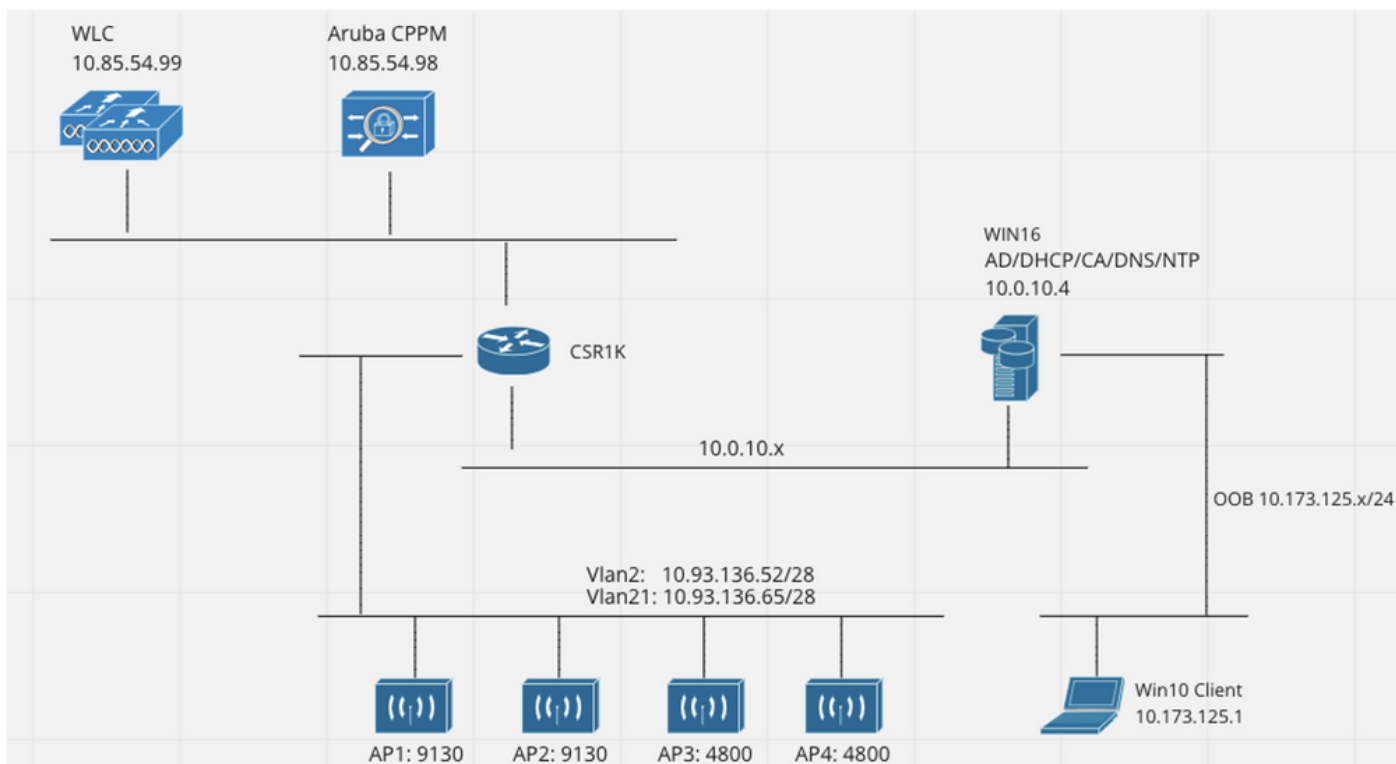


Diagrama de Rede



Configurar o Catalyst 9800 Wireless Controller

Neste exemplo de configuração, o novo modelo de configuração no C9800 é utilizado para criar os perfis e tags necessários para fornecer acesso corporativo dot1x às filiais da empresa. A configuração resultante é resumida no diagrama.



C9800 - Configurar parâmetros AAA para dot1x

Etapa 1. Adicione o servidor 'Corp' do Aruba ClearPass Policy Manager à configuração da WLC 9800. Navegue até **Configuration > Security > AAA > Servers/Groups > RADIUS > Servers**. Clique em **+Add** e insira as informações do servidor RADIUS. Clique no botão **Apply to Device** como mostrado nesta imagem.

Name*	<input type="text" value="CPPM_Corp"/>
Server Address*	<input type="text" value="10.85.54.97"/>
PAC Key	<input type="checkbox"/>
Key Type	<input type="text" value="Clear Text"/>
Key* ⓘ	<input type="text" value="....."/>
Confirm Key*	<input type="text" value="....."/>
Auth Port	<input type="text" value="1812"/>
Acct Port	<input type="text" value="1813"/>
Server Timeout (seconds)	<input type="text" value="5"/>
Retry Count	<input type="text" value="3"/>
Support for CoA	<input checked="" type="checkbox"/> ENABLED

Etapa 2. Defina o grupo de servidores AAA para usuários corporativos. Navegue para **Configuration > Security > AAA > Servers/Groups > RADIUS > Groups** e clique em **+Add**, insira o nome do grupo de servidores RADIUS e atribua as informações do servidor RADIUS. Clique no botão **Apply to Device** como mostrado nesta imagem.

Create AAA Radius Server Group ✕

Name*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Source Interface VLAN ID

Available Servers Assigned Servers

CPPM_Guest	>	CPPM_Corp	^
	<		^
	»		v
	«		v

Etapa 3. Definir a lista de métodos de autenticação dot1x para usuários corporativos. Navegue para **Configuration > Security > AAA > AAA Method List > Authentication** e clique em **+Add**. Selecione **Type dot1x** no menu suspenso. Clique no botão **Apply to Device** como mostrado nesta imagem.

Quick Setup: AAA Authentication



Method List Name*

Dot1X_Authentication

Type*

dot1x



Group Type

group



Fallback to local

Available Server Groups

radius
ldap
tacacs+
WLC_Tacacs_Servers
AAA_Group_Guest



Assigned Server Groups

AAA_Group_Corp



Cancel

Apply to Device

C9800 - Configure o perfil de WLAN 'Corp'

Etapa 1. Navegue até **Configuration > Tags & Profiles > Wireless** e clique em **+Add**. Insira um nome de perfil, o SSID 'Corp' e uma ID de WLAN que ainda não esteja em uso.

Add WLAN



General

Security

Advanced

Profile Name*

WP_Corp

Radio Policy

All

SSID*

Corp

Broadcast SSID

ENABLED



WLAN ID*

3

Status

ENABLED



Cancel

Apply to Device

Etapa 2. Navegue até a guia **Security** e a subguia **Layer2**. Não é necessário alterar nenhum dos parâmetros padrão para este exemplo de configuração.

Add WLAN

General **Security** Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode

MAC Filtering

Protected Management Frame

PMF

WPA Parameters

WPA Policy

WPA2 Policy

GTK Randomize

OSEN Policy

WPA2 Encryption AES(CCMP128)
 CCMP256
 GCMP128
 GCMP256

Auth Key Mgmt 802.1x
 PSK
 CCKM
 FT + 802.1x
 FT + PSK
 802.1x-SHA256
 PSK-SHA256

Lobby Admin Access

Fast Transition

Over the DS

Reassociation Timeout

MPSK Configuration

MPSK

Etapa 3. Navegue até a subguia **AAA** e selecione a Authentication Method List configurada anteriormente. Clique no botão **Apply to Device** como mostrado nesta imagem.

Add WLAN ✕

General **Security** Advanced

Layer2 Layer3 **AAA**

Authentication List Dot1X_Authenticatio ▼ i

Local EAP Authentication

↶ Cancel Apply to Device

C9800 - Configurar perfil de política

Etapa 1. Navegue até **Configuration > Tags & Profiles > Policy** e clique em **+Add** e insira um nome e uma descrição do perfil da política. Habilite a política e desabilite a comutação central, o DHCP e a associação, já que o tráfego de usuário corporativo é comutado localmente no AP como mostrado na imagem.

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

General	Access Policies	QOS and AVC	Mobility	Advanced
Name*	<input type="text" value="PP_Corp"/>			WLAN Switching Policy
Description	<input type="text" value="Policy Profile for Corp"/>			Central Switching <input type="checkbox"/> DISABLED
Status	<input checked="" type="checkbox"/> ENABLED			Central Authentication <input checked="" type="checkbox"/> ENABLED
Passive Client	<input type="checkbox"/> DISABLED			Central DHCP <input type="checkbox"/> DISABLED
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED			Central Association <input type="checkbox"/> DISABLED
CTS Policy				Flex NAT/PAT <input type="checkbox"/> DISABLED
Inline Tagging	<input type="checkbox"/>			
SGACL Enforcement	<input type="checkbox"/>			
Default SGT	<input type="text" value="2-65519"/>			

Etapa 2. Navegue até a guia **Access Policies** e insira manualmente o ID da VLAN a ser usada na filial para o tráfego de usuário corporativo. Essa VLAN não precisa ser configurada no próprio C9800. Ele deve ser configurado no perfil Flex, conforme detalhado adiante. Não selecione um nome de VLAN na lista suspensa (consulte o bug da Cisco ID [CSCvn48234](#) para obter mais informações). Clique no botão **Apply to Device** como mostrado nesta imagem.

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

General	Access Policies	QOS and AVC	Mobility	Advanced
RADIUS Profiling	<input type="checkbox"/>			
HTTP TLV Caching	<input type="checkbox"/>			
DHCP TLV Caching	<input type="checkbox"/>			
WLAN Local Profiling				
Global State of Device Classification	<input type="checkbox"/>			
Local Subscriber Policy Name	<input type="text" value="Search or Select"/>			
VLAN				
VLAN/VLAN Group	<input type="text" value="2"/>			
Multicast VLAN	<input type="text" value="Enter Multicast VLAN"/>			
				WLAN ACL
				IPv4 ACL <input type="text" value="Search or Select"/>
				IPv6 ACL <input type="text" value="Search or Select"/>
URL Filters				
				Pre Auth <input type="text" value="Search or Select"/>
				Post Auth <input type="text" value="Search or Select"/>
<input type="button" value="Cancel"/>				<input type="button" value="Apply to Device"/>

C9800 - Configurar marcação de política

Depois que o Perfil de WLAN (WP_Corp) e o Perfil de política (PP_Corp) forem criados, uma Marca de política deverá ser criada para vincular esses Perfis de WLAN e de política. Esta marca de política é aplicada aos pontos de acesso. Atribua esta marca de política aos pontos de acesso para disparar a configuração deles para habilitar os SSIDs selecionados neles.

Etapa 1. Navegue até **Configuration > Tags & Profiles > Tags**, selecione a guia **Policy** e clique em **+Add**. Insira o nome e a descrição da tag de política. Clique em **+Add** em **WLAN-POLICY Maps**. Selecione o perfil de WLAN e o perfil de política criados anteriormente e clique no botão de marca de seleção como mostrado nesta imagem.

Add Policy Tag ✕

Name*

Description

▼ **WLAN-POLICY Maps: 0**

WLAN Profile	Policy Profile
◀ 0 ▶ 10 items per page No items to display	

Map WLAN and Policy

WLAN Profile* Policy Profile*

➤ **RLAN-POLICY Maps: 0**

Etapa 2. Verifique e clique no botão **Apply to Device** como mostrado nesta imagem.

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 1

WLAN Profile	Policy Profile
<input checked="" type="checkbox"/> WP_Corp	PP_Corp

◀ 1 ▶ 10 items per page 1 - 1 of 1 items

➤ RLAN-POLICY Maps: 0

C9800 - Perfil de junção de AP

Os perfis de ingresso AP e os perfis Flex precisam ser configurados e atribuídos aos pontos de acesso com marcas de site. Uma Tag de Site diferente deve ser usada para cada ramificação para oferecer suporte à Transição Rápida (FT) 802.11r dentro de uma ramificação, ainda que limite a distribuição do PMK cliente apenas entre os APs dessa ramificação. É importante não reutilizar a mesma tag de site em várias ramificações. Configure um perfil de ingresso AP. Você pode usar um único perfil de junção AP se todas as ramificações forem semelhantes, ou criar vários perfis se alguns dos parâmetros configurados precisarem ser diferentes.

Etapa 1. Navegue até **Configuration > Tags & Profiles > AP Join** e clique em **+Add**. Insira o nome e a descrição do AP Join Profile. Clique no botão **Apply to Device** como mostrado nesta imagem.

Add AP Join Profile

General Client CAPWAP AP Management Security ICap QoS

Name* APJP_Branch

Description Profiles for branches

LED State

LAG Mode

NTP Server 0.0.0.0

GAS AP Rate Limit

Apphost

OfficeExtend AP Configuration

Local Access

Link Encryption

Rogue Detection

Cancel Apply to Device

C9800 - Perfil Flex

Agora configure um perfil Flex. Novamente, você pode usar um único perfil para todas as ramificações, se forem semelhantes, e ter o mesmo mapeamento VLAN/SSID. Ou você pode criar vários perfis se alguns dos parâmetros configurados, como as atribuições de VLAN, forem diferentes.

Etapa 1. Navegue até **Configuration > Tags & Profiles > Flex** e clique em **+Add**. Insira o nome e a descrição do perfil Flex.

Add Flex Profile

General Local Authentication Policy ACL VLAN Umbrella

Name* FP_Branch

Description Flex Profile for branches

Native VLAN ID 1

HTTP Proxy Port 0

HTTP-Proxy IP Address 0.0.0.0

CTS Policy

Inline Tagging

SGACL Enforcement

CTS Profile Name default-sxp-profile x

Fallback Radio Shut

Flex Resilient

ARP Caching

Efficient Image Upgrade

OfficeExtend AP

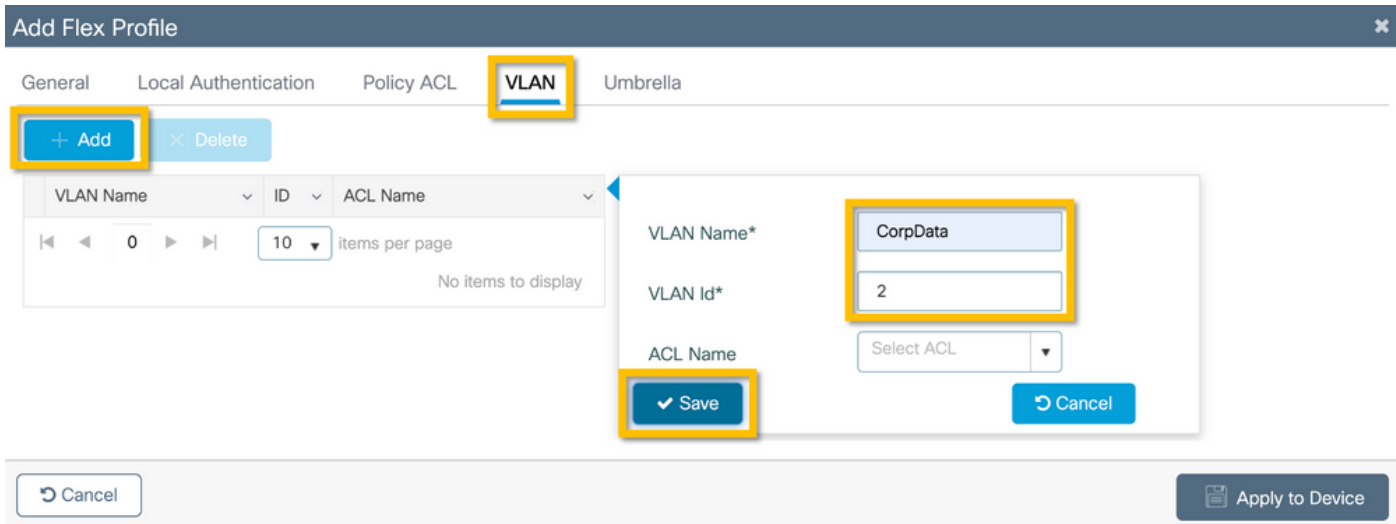
Join Minimum Latency

IP Overlap

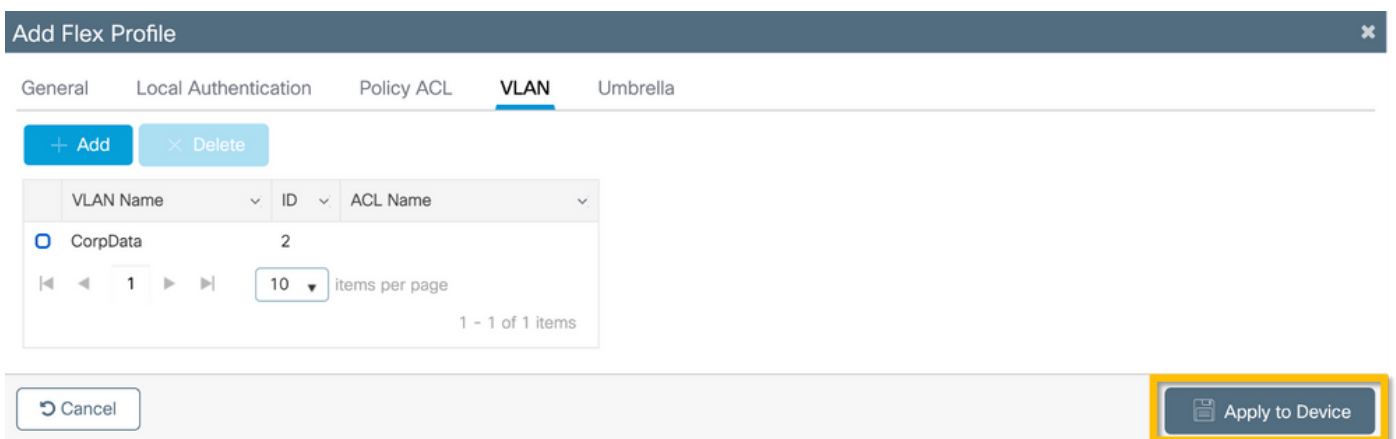
mDNS Flex Profile Search or Select

Cancel Apply to Device

Etapa 2. Navegue até a guia **VLAN** e clique em **+Add**. Insira o nome e a ID da VLAN local na filial que o AP deve usar para alternar localmente o tráfego de usuário corporativo. Clique no botão **Save**, conforme mostrado nesta imagem.



Etapa 3. Verifique e clique no botão **Apply to Device** como mostrado nesta imagem.



C9800 - Marca do local

As Marcas de Site são usadas para atribuir Perfis de Junção e Perfis Flex a pontos de acesso. Como mencionado anteriormente, uma Marca de Site diferente deve ser usada para cada filial para oferecer suporte à Transição Rápida (FT) 802.11r em uma filial, ainda que limite a distribuição da PMK do cliente apenas entre os APs dessa filial. É importante não reutilizar a mesma marca de site em várias filiais.

Etapa 1. Navegue até **Configuration > Tags & Profiles > Tags**, selecione a guia **Site** e clique em **+Add**. Insira um nome e uma descrição de marca de site, selecione o Perfil de associação AP criado, desmarque a caixa **Habilitar site local** e, finalmente, selecione o Perfil Flex criado anteriormente. Desmarque a caixa **Enable Local Site** para alterar o ponto de acesso de **Local Mode** para **FlexConnect**. Finalmente, clique no botão **Apply to Device**, como mostrado nesta imagem.

Add Site Tag ✕

Name*	ST_Branch_01
Description	Site Tag for Branch 01
AP Join Profile	APJP_Branch ▼
Flex Profile	FP_Branch ▼
Fabric Control Plane Name	▼
Enable Local Site	<input checked="" type="checkbox"/>

↶ Cancel 📄 Apply to Device

C9800 - Tag de RF

Etapa 1. Navegue até **Configuration > Tags & Profiles > Tags**, selecione a guia **RF** e clique em **+Add**. Insira um nome e uma descrição para a marca RF. Selecione os perfis de RF definidos pelo sistema no menu suspenso. Clique no botão **Apply to Device** como mostrado nesta imagem.

Add RF Tag ✕

Name*	RFT_Branch
Description	RF in Typical Branch
5 GHz Band RF Profile	Typical_Client_Densi ▼
2.4 GHz Band RF Profile	Typical_Client_Densi ▼

↶ Cancel 📄 Apply to Device

C9800 - Atribuir tags ao AP

Agora que as tags são criadas e incluem as várias políticas e perfis necessários para configurar os access points, devemos atribuí-los aos access points. Esta seção mostra como executar uma tag estática atribuída manualmente a um ponto de acesso, com base no seu endereço MAC Ethernet. Para ambientes de produção de produtos, é recomendável usar o Cisco DNA Center AP PNP Workflow ou usar um método de carregamento CSV em massa estático disponível no 9800.

Etapa 1. Navegue até **Configure > Tags & Profiles > Tags**, selecione a guia **AP** e depois a guia **Static**. Clique em **+Add**, insira o endereço MAC do AP e selecione a tag Policy, a tag Site e a tag RF definidas anteriormente. Clique no botão **Apply to Device**, conforme mostrado nesta imagem.

Associate Tags to AP ✕

AP MAC Address*	<input type="text" value="380e.4dbf.589a"/>
Policy Tag Name	<input type="text" value="PT_Branch"/> ▼
Site Tag Name	<input type="text" value="ST_Branch_01"/> ▼
RF Tag Name	<input type="text" value="RFT_Branch"/> ▼

Configurar o Aruba CPPM

Configuração inicial do Aruba ClearPass Policy Manager Server

O Aruba clearpass é implantado por meio do modelo OVF no servidor ESXi com estes recursos:

- 2 CPUs virtuais reservadas
- 6 GB de RAM
- Disco de 80 GB (deve ser adicionado manualmente após a implantação inicial da VM antes que a máquina seja ligada)

Aplicar licenças

Aplice a licença da plataforma via: **Administração > Gerenciador de servidores > Licenciamento**. Adicionar **acesso e integrado**

Adicione o controlador sem fio C9800 como um dispositivo de rede

Navegue até **Configuration > Network > Devices > Add** conforme mostrado nesta imagem.

Edit Device Details

Device | SNMP Read Settings | SNMP Write Settings | CLI Settings | OnConnect Enforcement | Attributes

Name: >WLC-10.85.54.99

IP or Subnet Address: 10.85.54.99 (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20)

Description: LAB WLC 9800

RADIUS Shared Secret: Verify:

TACACS+ Shared Secret: Verify:

Vendor Name: Cisco

Enable RADIUS Dynamic Authorization: Port: 1700

Enable RadSec:

Copy Save Cancel

Configurar o CPPM para Usar o Windows AD como uma Origem de Autenticação

Navegue até Configuration > Authentication > Sources > Add. Selecionar tipo: Ative Directory no menu suspenso como mostrado nesta imagem.

aruba ClearPass Policy Manager

Configuration » Authentication » Sources » Add

Authentication Sources

General | Primary | Attributes | Summary

Name: LAB_AD

Description:

Type: Active Directory

Use for Authorization: Enable to use this Authentication Source to also fetch role mapping attributes

Authorization Sources: -- Select --

Server Timeout: 10 seconds

Cache Timeout: 36000 seconds

Backup Servers Priority: Move Up ↑ Move Down ↓ Add Backup Remove

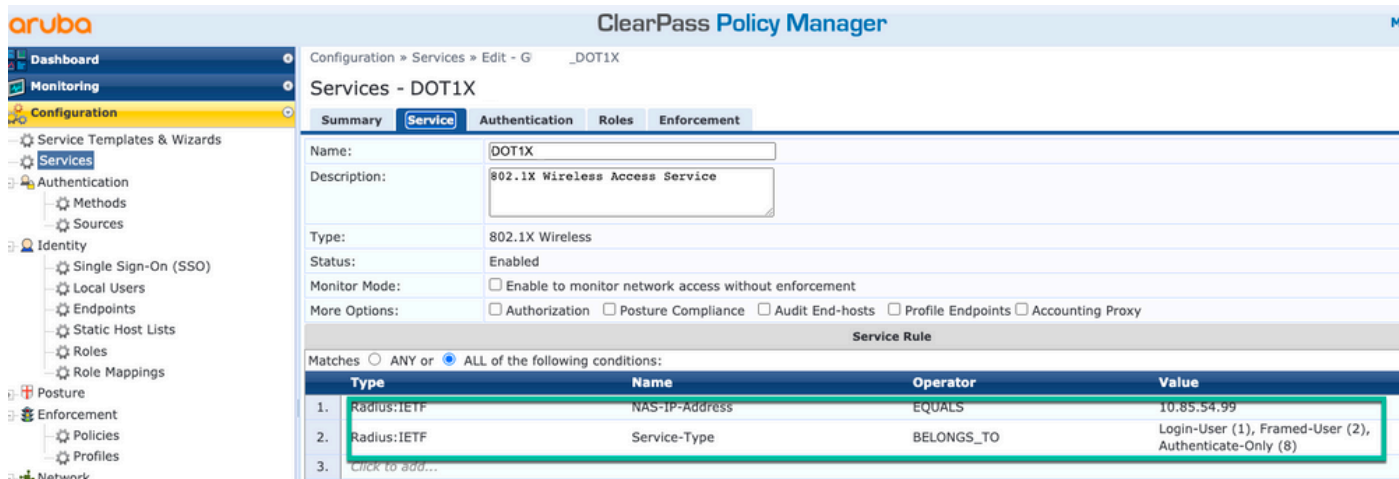
Configurar CPPM Serviço de Autenticação Dot1X

Etapa 1. Crie um 'serviço' que corresponda a vários Atributos RADIUS:

- Radius:IETF | Nome: NAS-IP-Address | IGUAL A | <END. IP>
- Radius:IETF | Nome: Tipo de serviço | IGUAL A | 1,2,8

Etapa 2. Para a produção, é recomendável combinar o nome SSID em vez do 'NAS-IP-Address'

para que uma condição seja suficiente em uma implantação de várias WLCs. Radius: Cisco: Cisco-AVPair | cisco-wlan-ssid | Ponto1XSSID



ClearPass Policy Manager

Configuration » Services » Edit - G _DOT1X

Services - DOT1X

Summary Service Authentication Roles Enforcement

Name: DOT1X

Description: 802.1X Wireless Access Service

Type: 802.1X Wireless

Status: Enabled

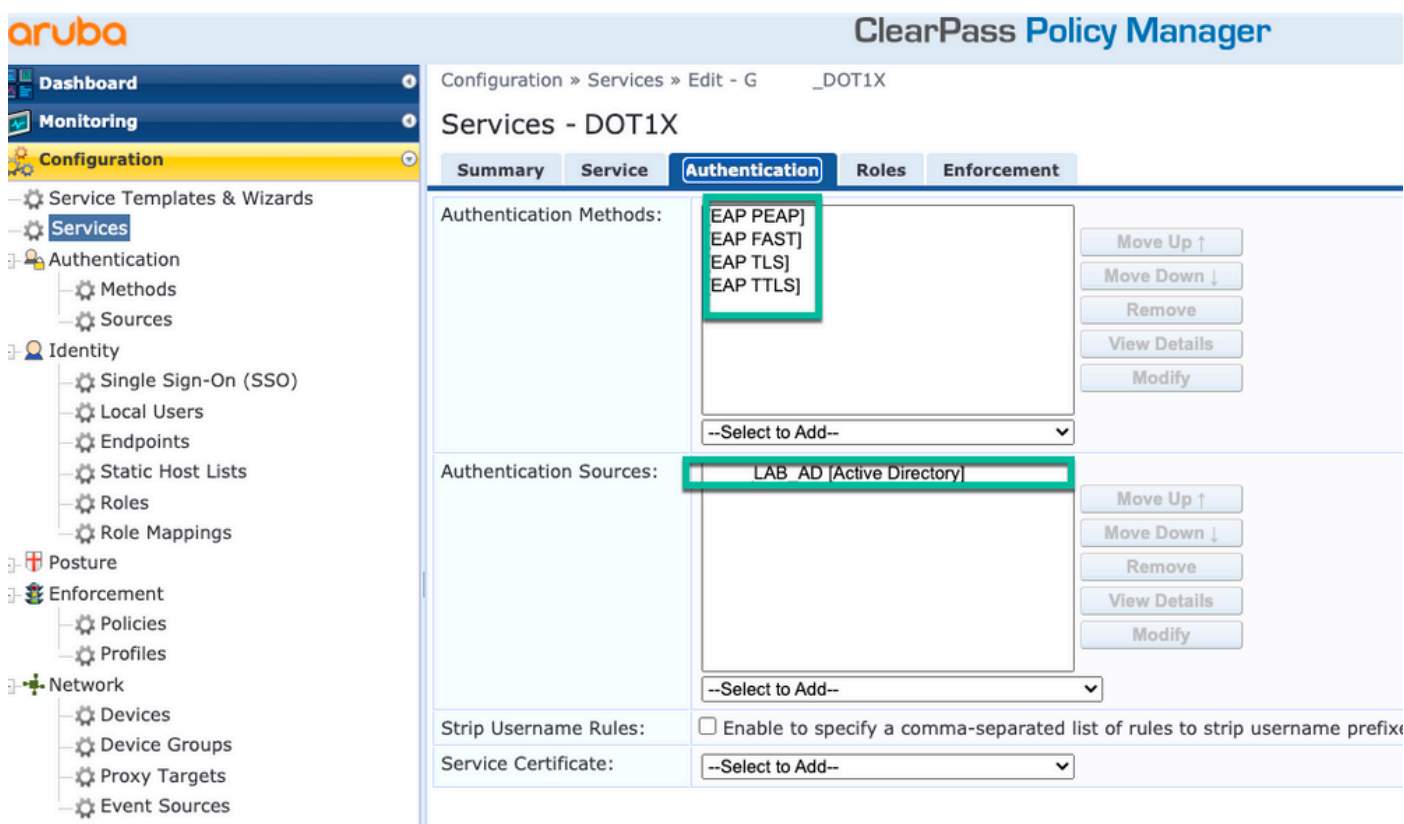
Monitor Mode: Enable to monitor network access without enforcement

More Options: Authorization Posture Compliance Audit End-hosts Profile Endpoints Accounting Proxy

Service Rule

Matches: ANY or ALL of the following conditions:

Type	Name	Operator	Value
1.	Radius:IETF NAS-IP-Address	EQUALS	10.85.54.99
2.	Radius:IETF Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)



ClearPass Policy Manager

Configuration » Services » Edit - G _DOT1X

Services - DOT1X

Summary Service Authentication Roles Enforcement

Authentication Methods:

- EAP PEAP]
- EAP FAST]
- EAP TLS]
- EAP TTLS]

--Select to Add--

Authentication Sources:

- LAB_AD [Active Directory]

--Select to Add--

Strip Username Rules: Enable to specify a comma-separated list of rules to strip username prefix

Service Certificate: --Select to Add--

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- [Guia de práticas recomendadas de implantação do Cisco 9800](#)

- [Compreender o Modelo de Configuração dos Catalyst 9800 Wireless Controllers](#)
- [Entender o FlexConnect no Catalyst 9800 Wireless Controller](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.