Exemplo de configuração do portal cativo do DNA Spaces com controlador AireOS

Contents

Introduction

Este documento descreve como configurar portais cativos usando o Cisco DNA Spaces com um controlador AireOS.

Contribuição de Andres Silva, engenheiro do Cisco TAC.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso à interface de linha de comando (CLI) ou à interface gráfica de usuário (GUI) dos controladores sem fio
- Cisco DNA Spaces

Componentes Utilizados

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

- Controladora 5520 Wireless LAN versão 8.10.112.0

Configurar

Diagrama de Rede

Configurações

Conectar a WLC aos Cisco DNA Spaces

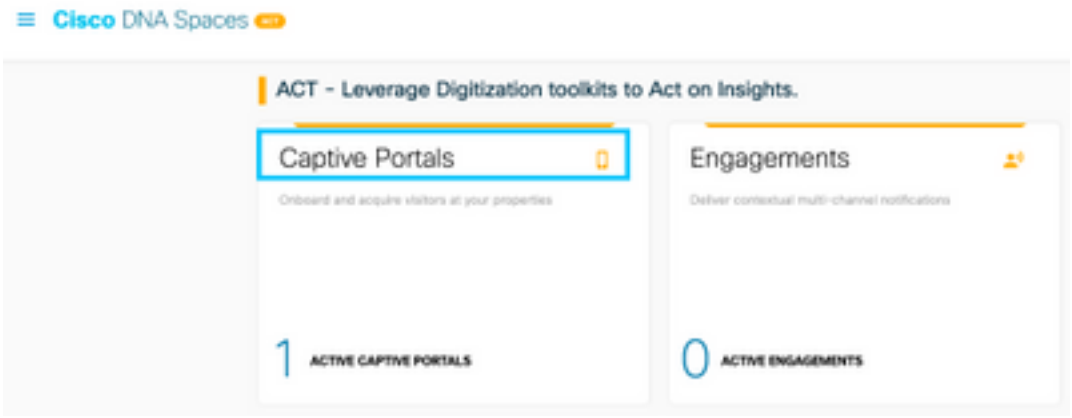
O controlador precisa ser conectado ao DNA Spaces usando qualquer uma das configurações disponíveis, Direct Connect, via DNA Spaces Connector ou usando Tethering CMX.

Neste exemplo, a opção Direct Connect está em uso, embora os portais cativos sejam configurados da mesma forma para todas as configurações.

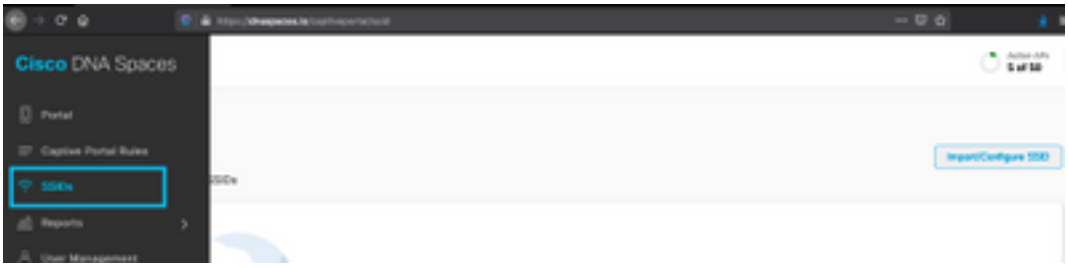
Para conectar o controlador ao Cisco DNA Spaces, ele deve conseguir acessar a nuvem do Cisco DNA Spaces por HTTPS. Para obter mais informações sobre como conectar o controlador ao DNA Spaces, consulte este link: Exemplo de configuração de conexão direta do DNA Spaces

Criar o SSID em espaços do DNA

Etapa 1. Clique em **Portais cativos** no painel do DNA Spaces:



Etapa 2. Abra o menu do portal cativo clicando no ícone de três linhas no canto superior esquerdo da página e clique em **SSIDs:**

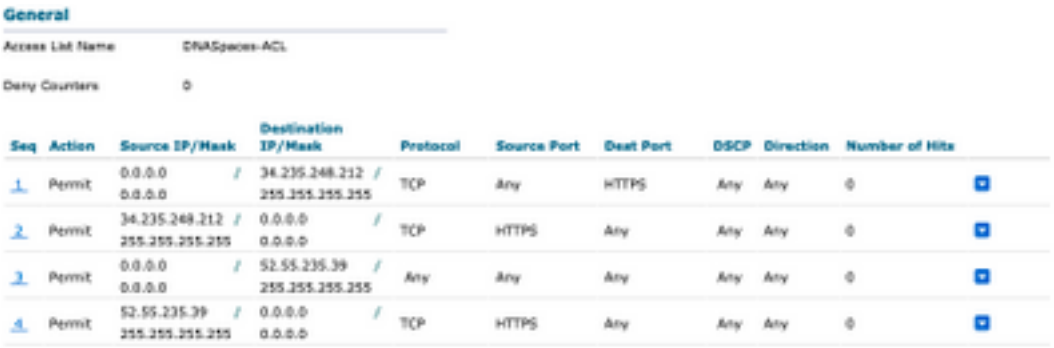


Etapa 3. Clique em **Import/Configure SSID**, selecione **CUWN (CMX/WLC)** como o tipo de "Wireless Network" e insira o nome do SSID:

Configuração da ACL no controlador

Uma ACL de pré-autenticação é necessária, pois é um SSID de autenticação da Web e assim que o dispositivo sem fio se conecta ao SSID e recebe um endereço IP, o estado do gerenciador de políticas do dispositivo passa para o estado **Webauth_Reqd** e a ACL é aplicada à sessão do cliente para restringir os recursos que o dispositivo pode acessar.

Etapa 1. Navegue até **Segurança > Listas de controle de acesso > Listas de controle de acesso,** clique em **Novo** e configure as regras para permitir a comunicação entre os clientes sem fio para o DNA Spaces da seguinte maneira. Substitua os endereços IP pelos fornecidos pelos espaços do DNA para a conta em uso:



> **Observação**: para obter os endereços IP dos espaços do DNA a serem permitidos na ACL, clique na opção **Configurar manualmente** do SSID criado na etapa 3 da seção **Criar o SSID nos espaços do DNA** na seção de configuração da ACL.

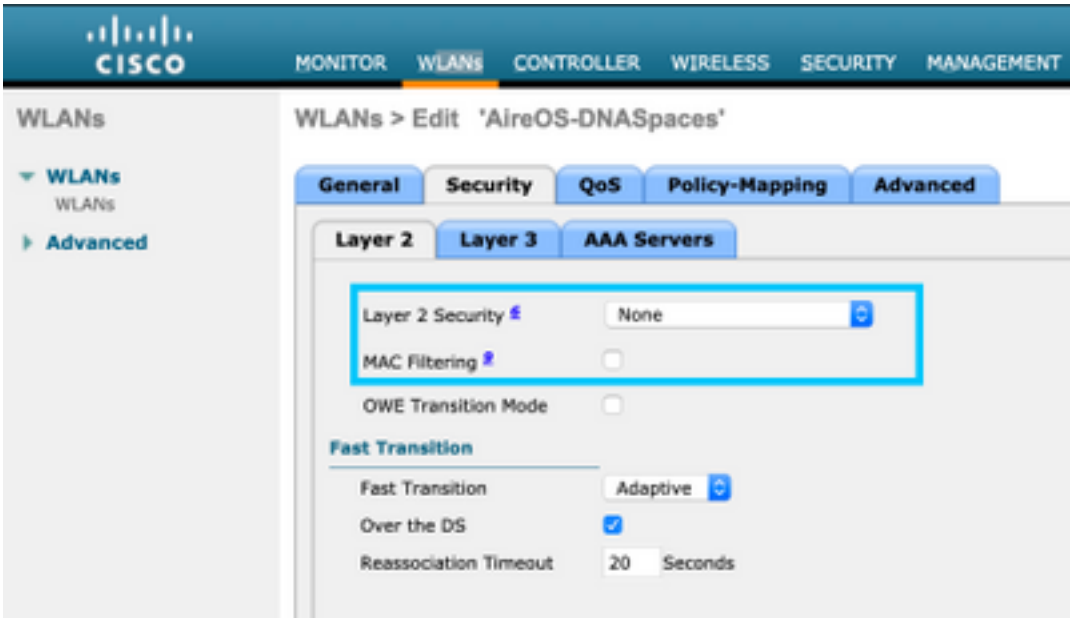
O SSID pode ser configurado para usar um servidor RADIUS ou sem ele. Se a Duração da sessão, o Limite de largura de banda ou o Provisionamento contínuo da Internet estiverem configurados na seção **Ações** da configuração Regra de portal cativo, o SSID precisará ser configurado com um Servidor RADIUS; caso contrário, não haverá necessidade de usar o Servidor RADIUS. Há suporte para todos os tipos de portais nos espaços do DNA em ambas as configurações.

Portal cativo sem servidor RADIUS em espaços do DNA

Configuração de SSID no controlador

Etapa 1. Navegue até **WLAN > WLANs.** Crie uma nova WLAN. Configure o Nome do perfil e o SSID. Certifique-se de que o nome do SSID seja o mesmo que o configurado na etapa 3 da seção **Criar o SSID em espaços do DNA.**

Etapa 2. Configure a segurança da camada 2. Navegue até a guia **Security > Layer 2** na guia Configuration da WLAN e selecione as **None** no menu suspenso Layer 2 Security. Certifique-se de que a filtragem MAC esteja desativada.



Etapa 3. Configure a segurança da camada 3. Navegue até a guia Security > Layer 3 na guia de configuração da WLAN, configure Web **Policy como o método de segurança da Camada 3, Enable Passthrough, configure a ACL de pré-autenticação, enable** Override Global Config como o Web Auth Type como External, **configure a URL de redirecionamento.**

Observação: para obter o URL de redirecionamento, clique na opção **Configurar manualmente**, no SSID criado na etapa 3 da seção **Criar o SSID em espaços do DNA,** na seção de configuração do SSID.

Portal cativo com servidor RADIUS em espaços do DNA

Observação: o servidor RADIUS do DNA Spaces oferece suporte apenas à autenticação PAP proveniente do controlador.

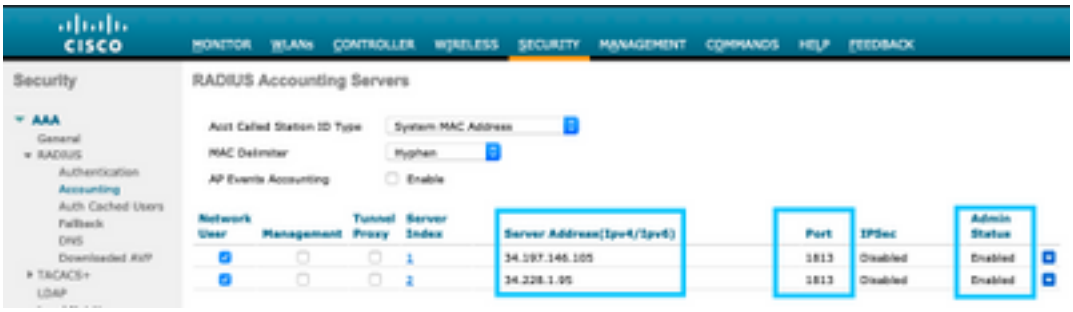
Configuração de servidores RADIUS no controlador

Etapa 1. Navegue para **Security > AAA > RADIUS > Authentication,** clique em **New** e insira as informações do servidor RADIUS. O Cisco DNA Spaces atua como um servidor RADIUS para

autenticação de usuário e pode responder em dois endereços IP. Configure os dois servidores RADIUS:

> **Observação**: para obter o endereço IP RADIUS e a chave secreta para servidores primários e secundários, clique na opção **Configurar manualmente** do SSID criado na etapa 3 da seção **Criar o SSID nos espaços do DNA** e navegue até a seção **Configuração do servidor RADIUS**.

Etapa 2. Configure o servidor RADIUS de contabilização. Navegue para **Security > AAA > RADIUS > Accounting** e clique em **New**. Configure os mesmos dois servidores RADIUS:

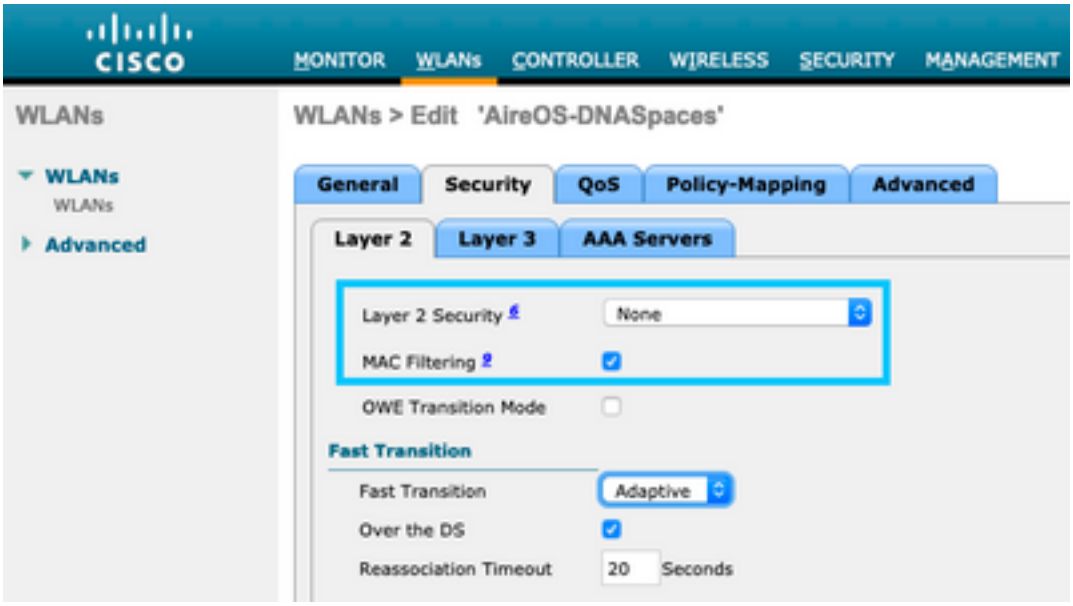


Configuração de SSID no controlador

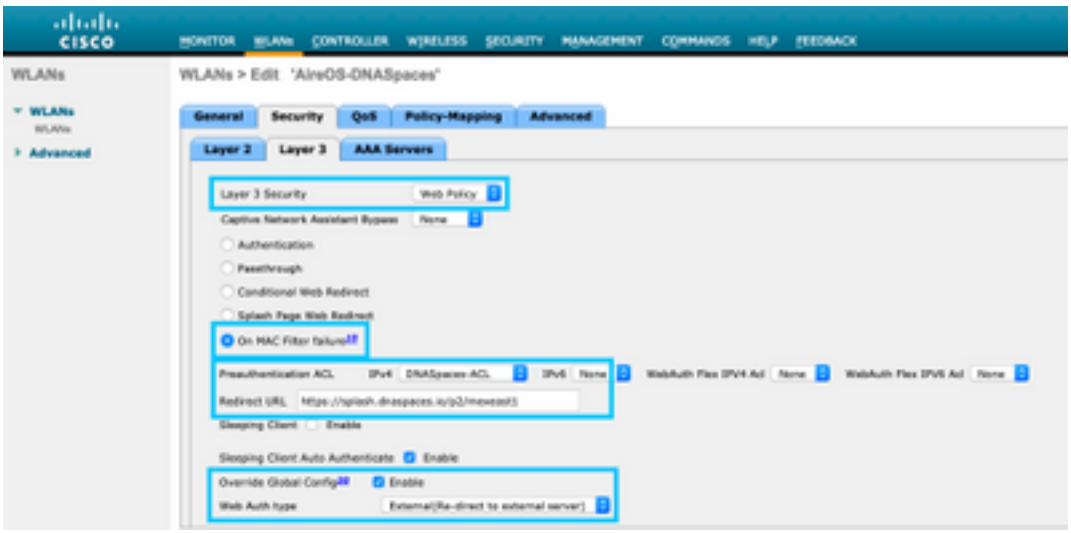
> **Importante**: antes de iniciar com a configuração SSID, certifique-se de que a **Web Radius Authentication** esteja definida como "PAP" em Controller > General.

Etapa 1. Navegue até **WLAN > WLANs.** Crie uma nova WLAN. Configure o Nome do perfil e o SSID. Certifique-se de que o nome do SSID seja o mesmo que o configurado na etapa 3 da seção **Criar o SSID em espaços do DNA.**

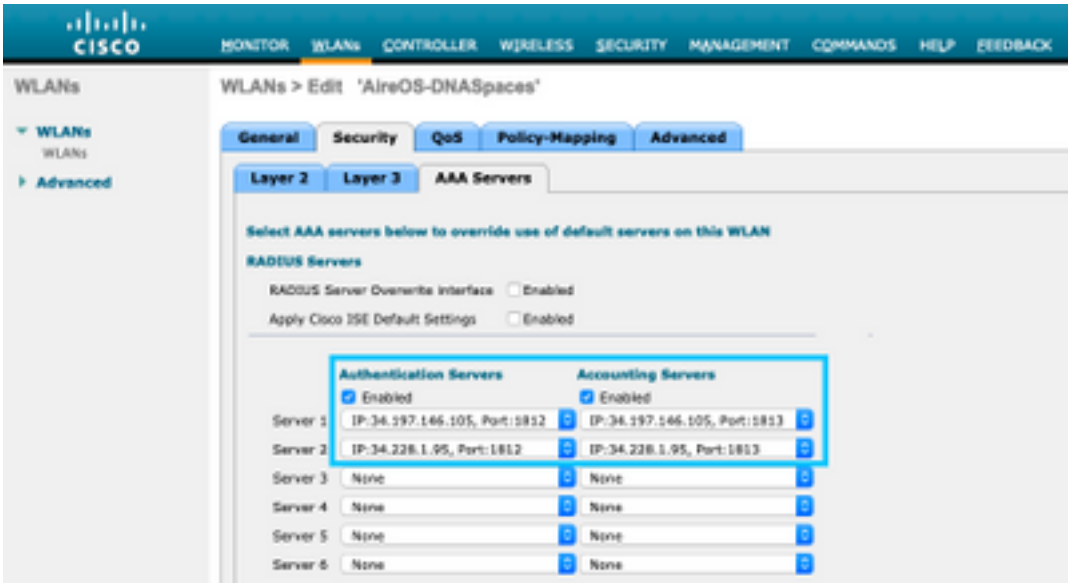
Etapa 2. Configure a segurança da camada 2. Navegue até a guia **Security > Layer 2** na guia de configuração da WLAN. Configure a segurança de camada 2 como **None**. Ative A Filtragem Mac.



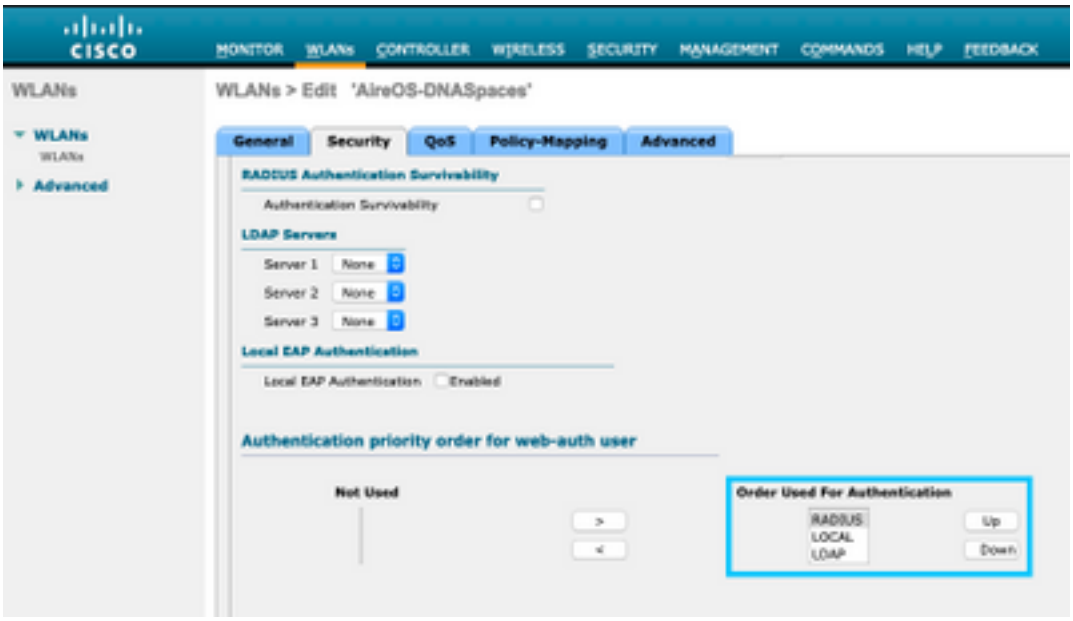
Etapa 3. Configure a segurança da camada 3. Navegue para a guia Security > Layer 3 na guia de configuração da WLAN, configure Web **Policy como o método de segurança da Camada 3, Enable On Mac Filter failure, configure a ACL de pré-autenticação, enable Override Global Config** como definido o Web Auth Type como External, **configure o Redirect URL.**



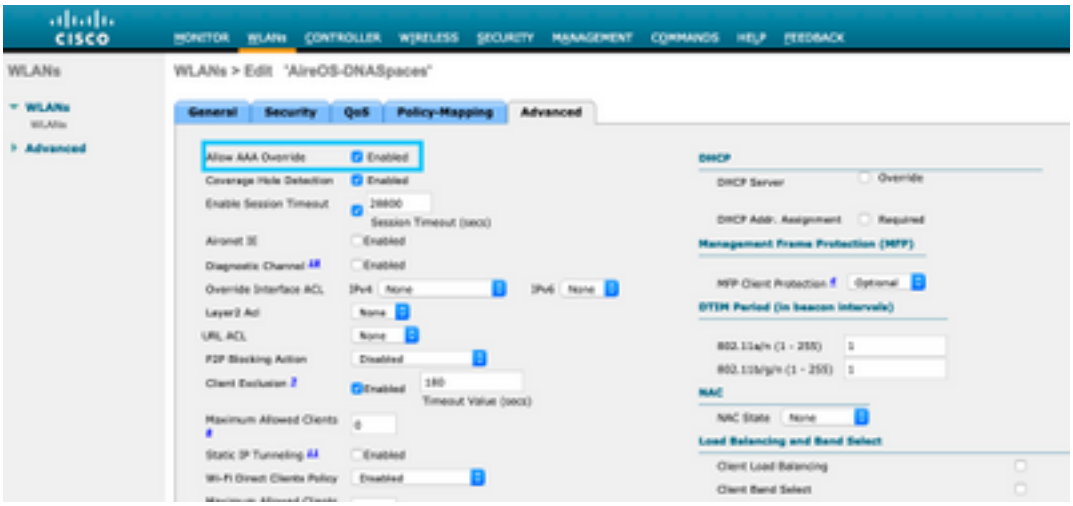
Etapa 4. Configure os servidores AAA. Navegue até a guia **Security > AAA Servers** na guia de configuração da WLAN, habilite **Authentication Servers** e **Accounting Servers** e, no menu suspenso, escolha os dois servidores RADIUS:



Etapa 6. Configure a **ordem de prioridade de autenticação para usuários de autenticação da Web**. Navegue até a guia **Security > AAA Servers** na guia de configuração da WLAN e defina RADIUS como o primeiro na ordem.

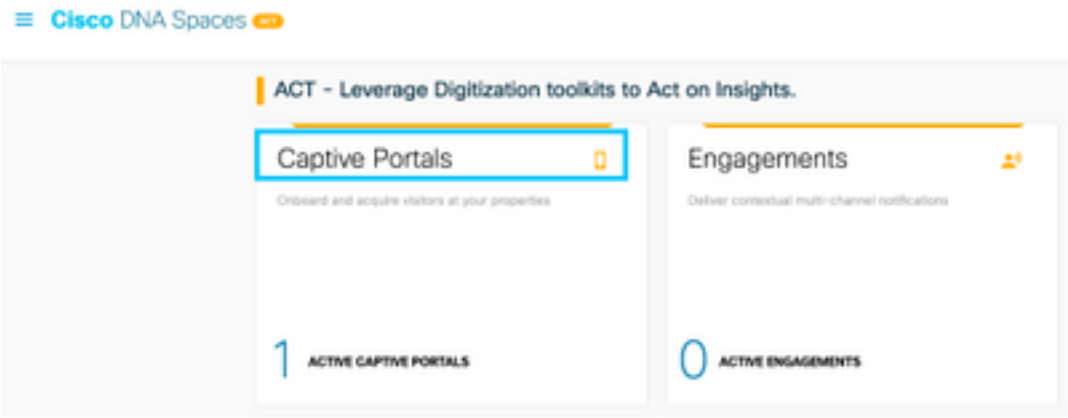


Passo 7. Navegue até a guia **Advanced** na guia de configuração da WLAN e habilite **Allow AAA Override.**

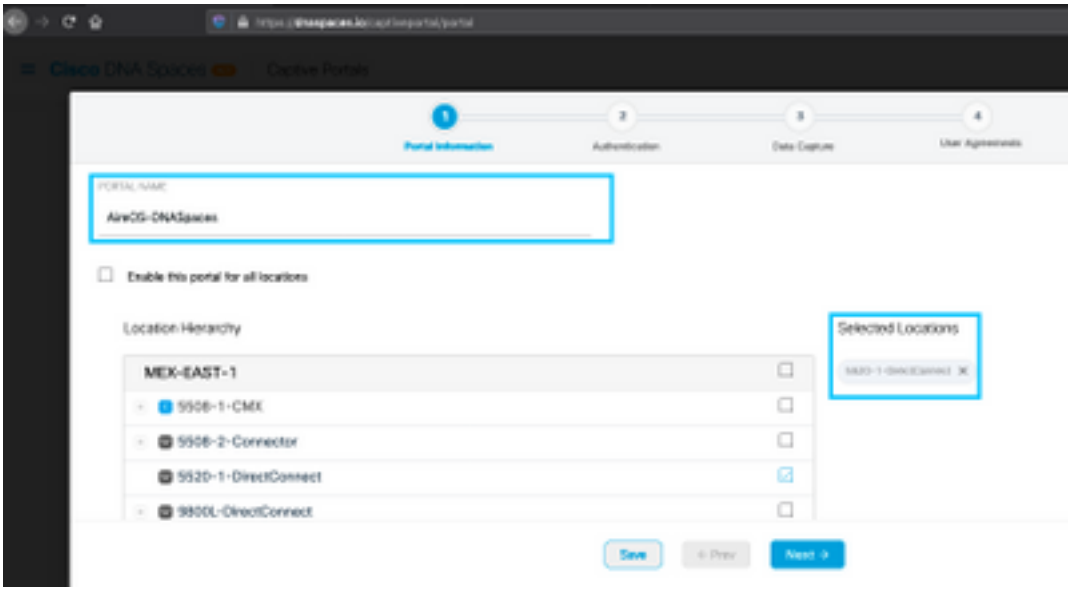


Criar o portal no DNA Spaces

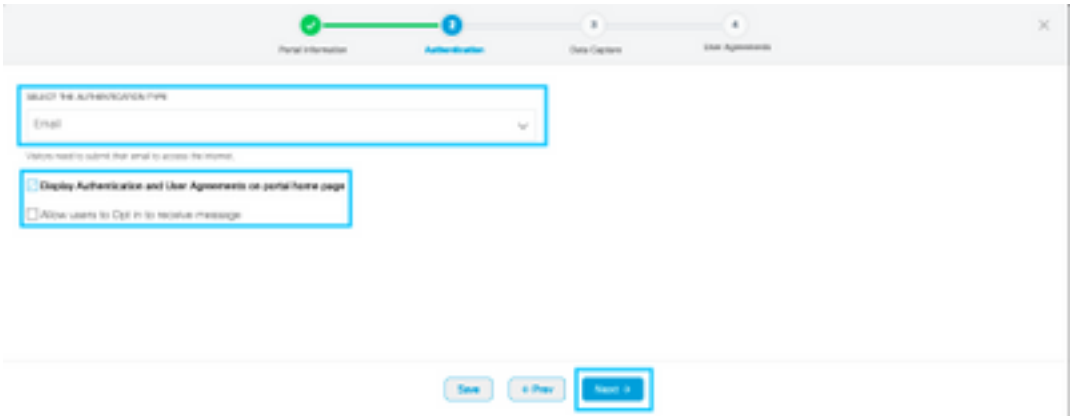
Etapa 1. Clique em **Portais cativos** no painel do DNA Spaces:



Etapa 2. Clique em **Criar novo,** insira o nome do portal e selecione os locais que podem usar o portal:

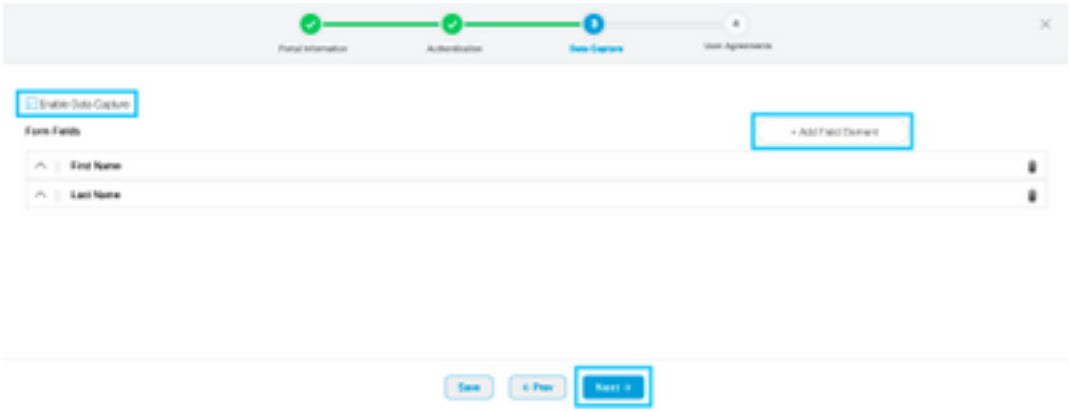


Etapa 3. Selecione o tipo de autenticação, escolha se deseja exibir a captura de dados e os contratos de usuário na home page do portal e se os usuários têm permissão para optar por receber uma mensagem. Clique em Next:



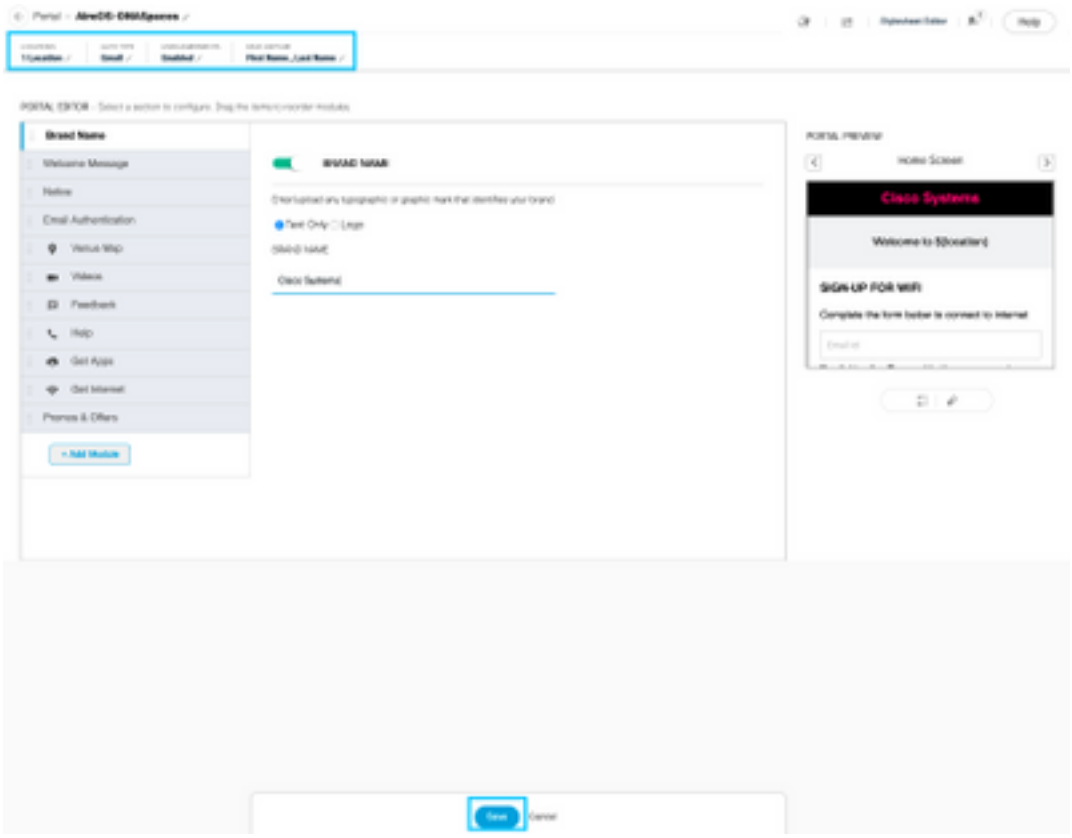
Etapa 4. Configurar elementos de captura de dados. Se você quiser capturar dados dos usuários, marque a caixa **Enable Data Capture** e clique em **+Add Field Element** para adicionar os campos

desejados. Clique em Next:



Etapa 5. Marque **Ativar termos e condições** e clique em **Salvar e configurar o portal**:

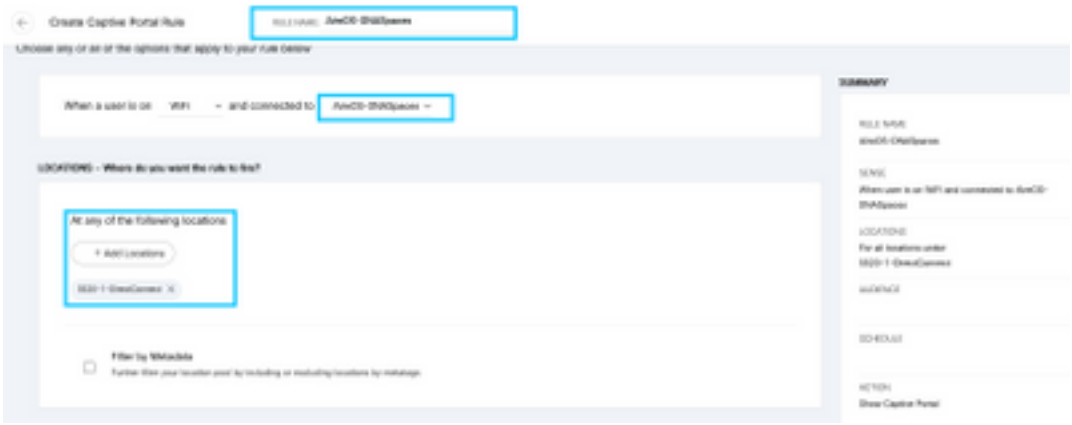
Etapa 6. Edite o portal conforme necessário. Clique em **Salvar:**



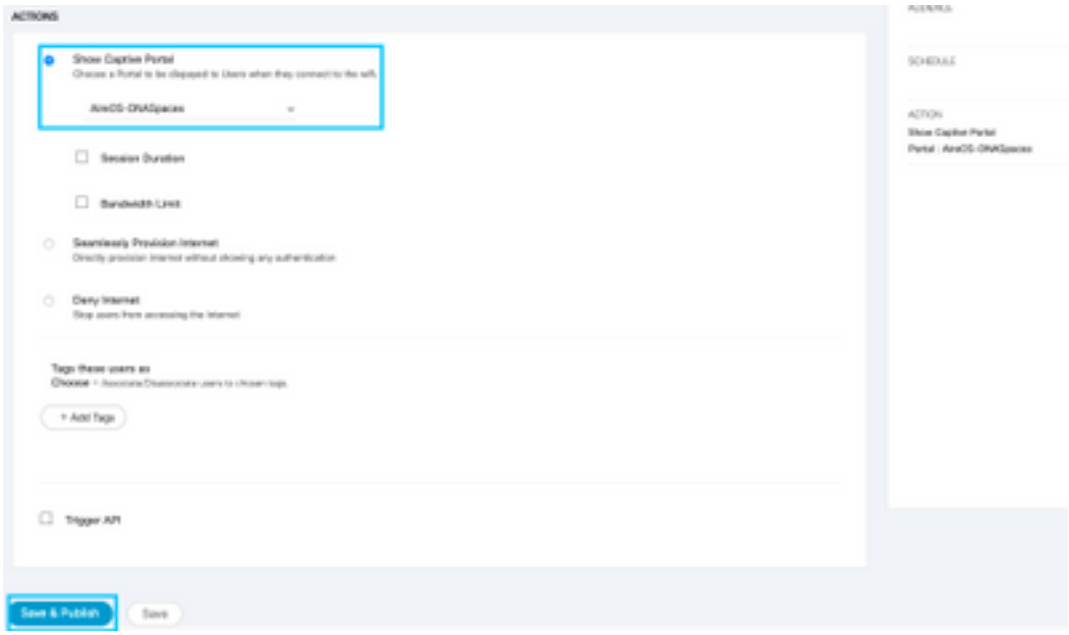
Configurar as regras do portal cativo em espaços do DNA

Etapa 1. Abra o menu do portal cativo e clique em **Captive Portal Rules:**

Etapa 2. Clique em **+** Criar nova regra. Insira o nome da regra, escolha o SSID configurado anteriormente e selecione os locais para os quais esta regra de portal está disponível:

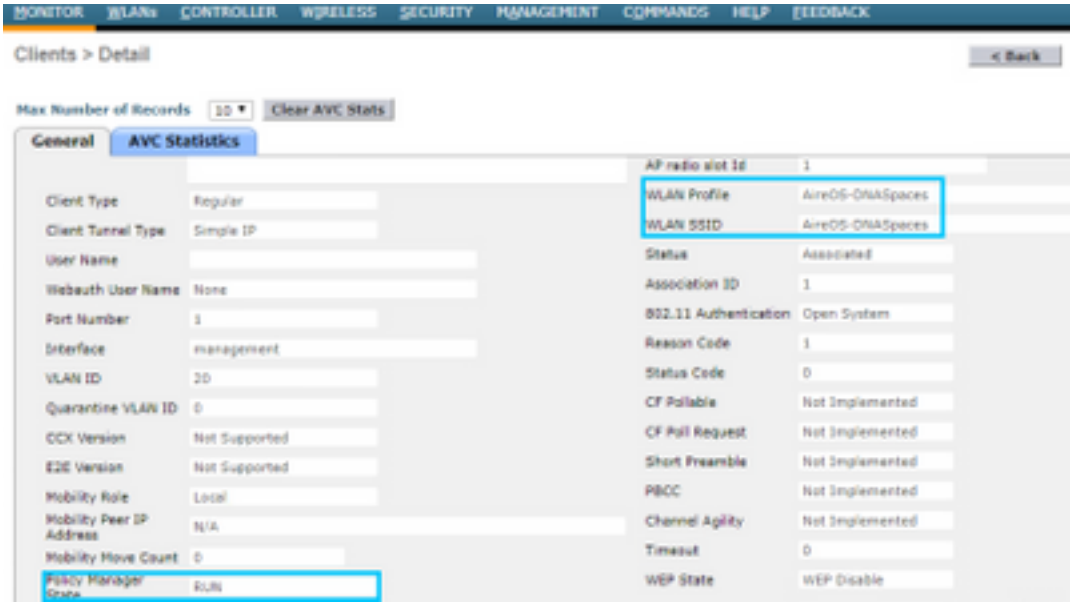


Etapa 3. Escolha a ação do portal cativo. Nesse caso, quando a regra é atingida, o portal é mostrado. Clique em **Salvar e publicar.**



Verificar

Para confirmar o status de um cliente conectado ao SSID, navegue para **Monitor > Clients**, clique no endereço MAC e procure Policy Manager State:



Troubleshoot

O comando a seguir pode ser ativado no controlador antes do teste para confirmar o processo de associação e autenticação do cliente.

```
(5520-Andressi) >debug client
```

```
(5520-Andressi) >debug web-auth redirect enable mac
```

Este é o resultado de uma tentativa bem-sucedida de identificar cada uma das fases durante o processo de associação/autenticação durante a conexão a um SSID sem servidor RADIUS:

Associação/autenticação 802.11:

```
*apfOpenDtlSocket: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Received management frame ASSOCIATION
REQUEST on BSSID 70:d3:79:dd:d2:0f destination addr 70:d3:79:dd:d2:0f slotid 1
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Updating the client capabiility as 4
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Processing assoc-req
station:34:e1:2d:23:a6:68 AP:70:d3:79:dd:d2:00-01 ssid : AireOS-DNASpaces thread:bd271d6280
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 CL_EVENT_ASSOC_START (1), reasonCode
(1), Result (0), Ssid (AireOS-DNASpaces), ApMac (70:d3:79:dd:d2:00), RSSI (-72), SNR (22)
*apfMsConnTask_5: Apr 09 21:49:06.228: 34:e1:2d:23:a6:68 Sending assoc-resp with status 0
station:34:e1:2d:23:a6:68 AP:70:d3:79:dd:d2:00-01 on apVapId 1
```

Autenticação de DHCP e Camada 3:

```
*apfMsConnTask_5: Apr 09 21:49:06.228: 34:e1:2d:23:a6:68 Mobility query, PEM State: DHCP_REQD
*webauthRedirect: Apr 09 21:49:51.949: captive-bypass detection enabled, checking for wispr in
HTTP GET, client mac=34:e1:2d:23:a6:68
*webauthRedirect: Apr 09 21:49:51.949: captiveNetworkMode enabled, mac=34:e1:2d:23:a6:68
```

```
user_agent = AnyConnect Agent 4.7.04056
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Preparing redirect URL according to
configured Web-Auth type
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- unable to get the hostName for virtual
IP, using virtual IP =192.0.2.1
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Checking custom-web config for WLAN
ID:1
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Global status is 0 on WLAN
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- checking on WLAN web-auth type
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Web-auth type External, using
URL:https://splash.dnaspaces.io/p2/mexeast1
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added switch_url, redirect URL is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added ap_mac (Radio ), redirect URL is
now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added client_mac , redirect URL is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23:a6
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- Added wlan, redirect URL is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23:a6:68&wla
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- http_response_msg_body1 is
<HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv="Cache-control"
content="no-cache"><META http-equiv="Pragma" content="
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- added redirect=, URL is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23:a6:68&wlan=Ai
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- str1 is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23:a6:68&wlan=AireOS-DNASpaces&r

*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- Message to be sent is
HTTP/1.1 200 OK
Location:
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- 200 send_data =HTTP/1.1 200 OK
Location:
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- send data length=688
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68-
Url:https://splash.dnaspaces.io/p2/mexeast1
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- cleaning up after send
```

Autenticação da camada 3 bem-sucedida, mova o cliente para o estado RUN:

```
*emWeb: Apr 09 21:49:57.633: Connection created for MAC:34:e1:2d:23:a6:68
*emWeb: Apr 09 21:49:57.634:
ewaURLHook: Entering:url=/login.html, virtIp = 192.0.2.1, ssl_connection=0, secureweb=1

*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 10.10.30.42 WEBAUTH_NOL3SEC (14) Change
state to RUN (20) last state WEBAUTH_NOL3SEC (14)
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL_EVENT_WEB_AUTH_DONE (8), reasonCode
(0), Result (0), ServerIp (), UserName ()
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL_EVENT_RUN (9), reasonCode (0), Result
(0), Role (1), VLAN/VNID (20), Ipv4Addr (10.10.30.42), Ipv6Present (No)
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 10.10.30.42 RUN (20) Successfully
plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255,URL ACL ID 255,URL ACL
Action 0)
```

```
*emWeb: Apr 09 21:49:57.634: User login successful, presenting login success page to user
```

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.