

# Configurar SD-WAN Cloud OnRamp para SaaS

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Ativar o NAT na interface de transporte](#)

[Criar uma política de AAR centralizado](#)

[Habilitar acesso direto à Internet e a aplicativos no vManage](#)

[Verificação](#)

[Informações Relacionadas](#)

---

## Introdução

Este documento descreve a configuração para o Cloud OnRamp for Software as a Service (SaaS) usando a saída local da filial.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento da Rede de Longa Distância Definida por Software (SD-WAN).

### Componentes Utilizados

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

- Cisco vManage versão 20.9.4
- Roteador Cisco WAN Edge versão 17.9.3a

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

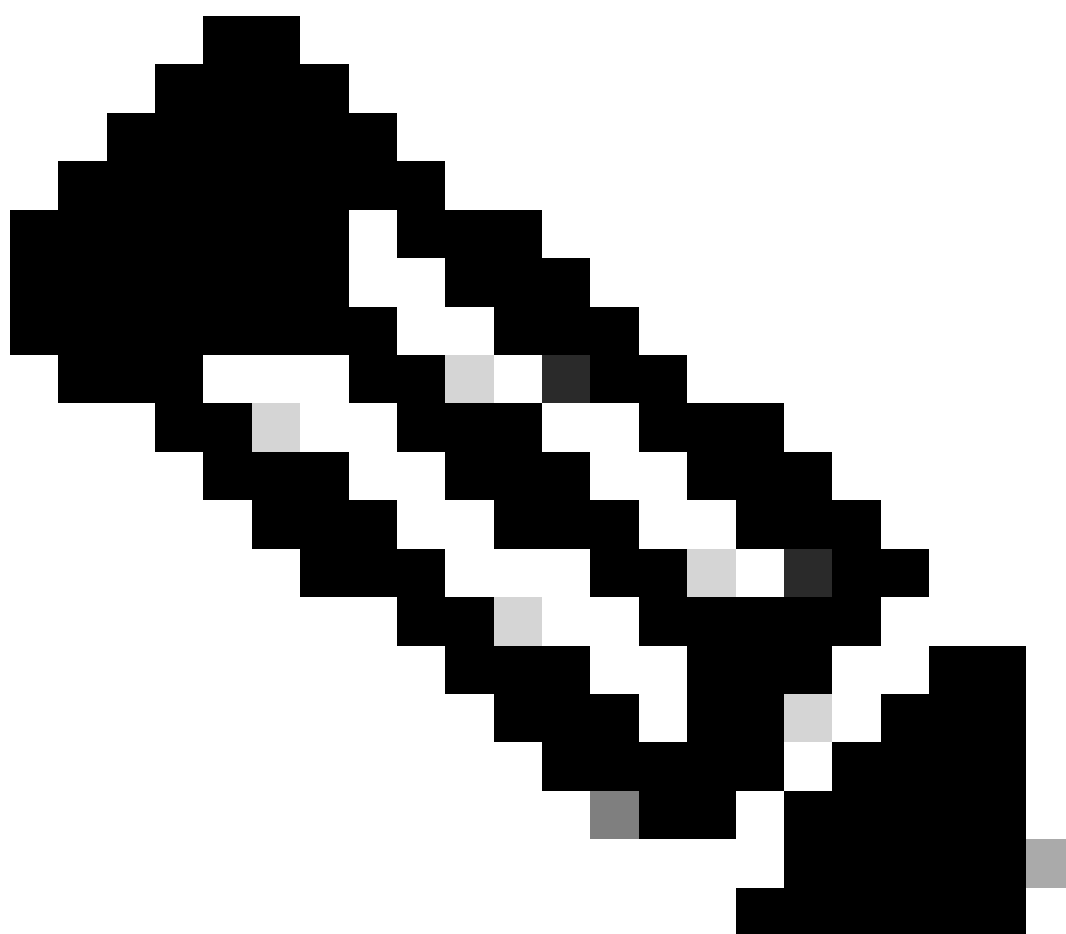
## Informações de Apoio

Para uma organização que usa SD-WAN, um local de filial normalmente roteia o tráfego de aplicativos SaaS por padrão por links de sobreposição de SD-WAN para um data center. A partir do data center, o tráfego de SaaS alcança o servidor de SaaS.

Por exemplo, em uma grande organização com um data center central e filiais, os funcionários podem usar o Office 365 em uma filial. Por padrão, o tráfego do Office 365 em uma filial é roteado por um link de sobreposição SD-WAN para um data center centralizado e, da saída DIA, para o servidor de nuvem do Office 365.

Este documento aborda este cenário: se o local da filial tiver uma conexão de acesso direto à Internet (DIA), você poderá melhorar o desempenho roteando o tráfego de SaaS através do DIA local, ignorando o data center.

---

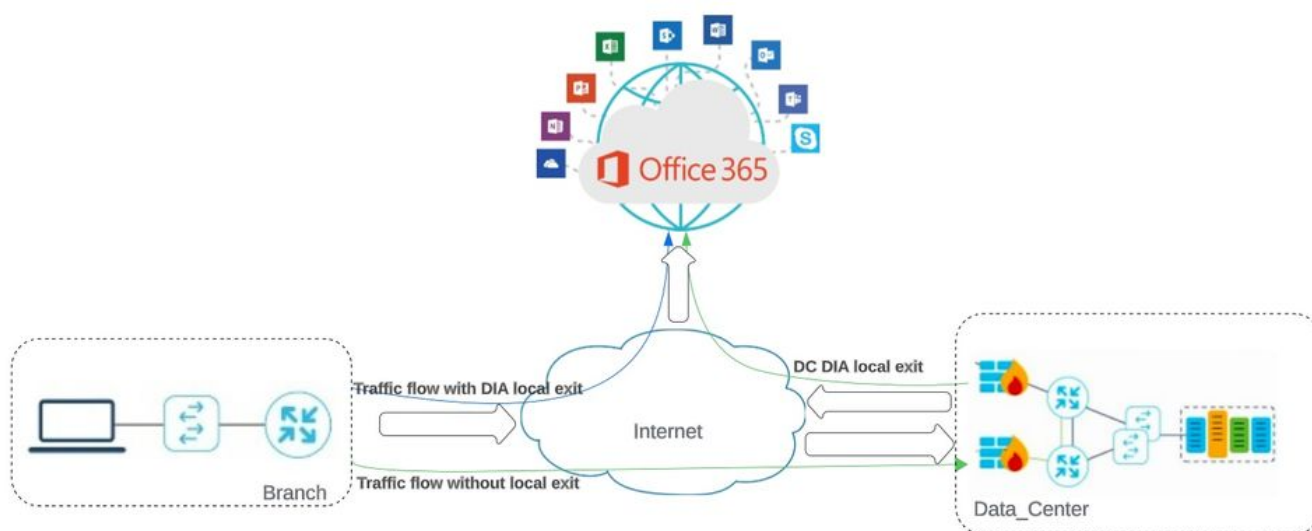


Observação: não há suporte para a configuração do Cloud OnRamp para SaaS quando um site usa um loopback como uma interface de localizador de transporte (TLOC).

---

Configurar

# Diagrama de Rede



Topologia de rede

## Configurações

Ativar o NAT na interface de transporte

Navegue até Feature Template . Escolha o **Transport VPN interface** modelo e Habilitar NAT.

The screenshot shows the Cisco SD-WAN configuration interface. The breadcrumb path is: Feature Template > Cisco VPN Interface Ethernet > cEdge\_Basic\_Transport1\_NAT. The 'NAT' section is expanded, showing the following configuration:

- NAT:  On  Off
- NAT Type:  Interface  Pool  Loopback
- UDP Timeout: 1
- TCP Timeout: 60

At the bottom, there are tabs for 'STATIC NAT' and 'PORT FORWARD', with 'STATIC NAT' being the active tab.

Ativar NAT de interface

Configuração equivalente de CLI:

```
interface GigabitEthernet2
ip nat outside
```

```
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet2 overload
ip nat translation tcp-timeout 3600
ip nat translation udp-timeout 60
```

Criar uma política de AAR centralizado

Para estabelecer uma política centralizada, você deve seguir este procedimento:

Etapa 1. Crie uma lista de sites:

Centralized Policy > Define Lists

Select a list type on the left and start creating your groups of interest

Application  
Color  
Community  
Data Prefix  
Policer  
Prefix  
**Site**

+ New Site List

Name	Entries	Reference Count	Updated By	Last Updated	Action
DCsite_100001	100001	3	admin	11 Sep 2023 12:46:54 PM P...	

*Modelo NAT da interface VPN*

Etapa 2. Crie uma lista VPN:

Centralized Policy > Define Lists

Select a list type on the left and start creating your groups of interest

Application  
Color  
Community  
Data Prefix  
Policer  
Prefix  
**Site**

+ New Site List

Name	Entries	Reference Count	Updated By	Last Updated	Action
DCsite_100001	100001	3	admin	11 Sep 2023 12:46:54 PM P...	

*Lista de sites personalizados de política centralizada*

Etapa 3. Configure o Traffic Rules e crie o Application Aware Routing Policy.

Cisco SD-WAN Monitor · VPN

Centralized Policy > Application Aware Routing Policy > Edit Application Aware Route Policy

Name\* Cloud\_OnRamp\_SAAS  
Description\* Cloud\_OnRamp\_SAAS

**App Route** Application Router

Sequence Type  
Drag & drop to reorder

Sequence Rule ACI Sequence Rules Drag and drop to re-arrange rules

Match Actions  
Backup SLA Preferred Color Counter Log SLA Class List Cloud SLA

Protocol IPv4

Match Conditions  
Cloud Saas Application/Application Family List  
office365\_apps

Actions  
Counter Name  
Cloud\_OnRamp  
Cloud SLA Enabled

Cancel Save Match And Actions

Preview Save Application Aware Routing Policy Cancel

Política de Rota com Reconhecimento de Aplicativo

Etapa 4. Adicione a política ao e pretendido Sites VPN:

Cisco SD-WAN Configuration · Policies

Centralized Policy > Add Policy

Create Groups of Interest Configure Topology and VPN Membership Configure Traffic Rules Apply Policies to Sites and VPNs

Add policies to sites and VPNs

Policy Name\* Cloud\_OnRamp\_SAAS  
Policy Description\* Cloud\_OnRamp\_SAAS

Topology Application-Aware Routing Traffic Data Cflowd Role Mapping for Regions

Cloud\_OnRamp\_SAAS

New Site/Region List and VPN List

Site List Region

Select Site List  
DCsite\_100001

Select VPN List  
VPN1

Add Cancel

Site/Region List	Region ID	VPN List	Action
Back			Preview Save Policy Cancel

Adicionar políticas a Sites e VPNs

Política equivalente de CLI:

```

viptela-policy:policy
app-route-policy _VPN1_Cloud_OnRamp_SAAS
vpn-list VPN1
sequence 1

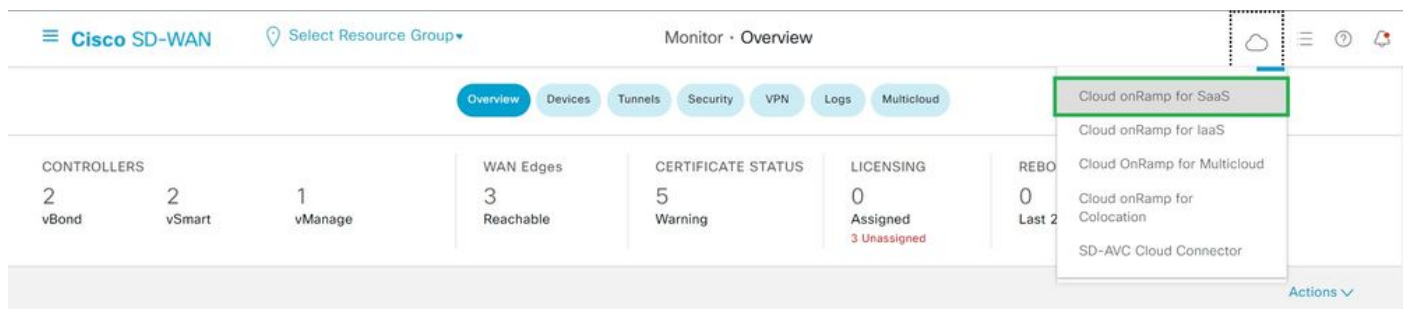
```

match  
cloud-saas-app-list office365\_apps  
source-ip 0.0.0.0/0  
!  
action  
count Cloud\_OnRamp\_-92622761  
!  
!  
!  
lists  
app-list office365\_apps  
app skype  
app ms\_communicator  
app windows\_marketplace  
app livemail\_mobile  
app word\_online  
app excel\_online  
app onedrive  
app yammer  
app sharepoint  
app ms-office-365  
app hockeyapp  
app live\_hotmail  
app live\_storage  
app outlook-web-service  
app skydrive  
app ms\_teams  
app skydrive\_login  
app sharepoint\_admin  
app ms-office-web-apps  
app ms-teams-audio  
app share-point  
app powerpoint\_online  
app ms-lync-video  
app live\_mesh  
app ms-lync-control  
app groove  
app ms-live-accounts  
app office\_docs  
app owa  
app ms\_sway  
app ms-lync-audio  
app live\_groups  
app office365  
app windowslive  
app ms-lync  
app ms-services  
app ms\_translator  
app microsoft  
app sharepoint\_blog  
app ms\_onenote  
app ms-teams-video  
app ms-update  
app ms-teams-media  
app ms\_planner  
app lync  
app outlook  
app sharepoint\_online  
app lync\_online

app sharepoint\_calendar  
app ms-teams  
app sharepoint\_document  
!  
site-list DCsite\_100001  
site-id 100001  
!  
vpn-list VPN1  
vpn 1  
!  
!  
!  
apply-policy  
site-list DCsite\_100001  
app-route-policy \_VPN1\_Cloud\_OnRamp\_SAAS  
!  
!

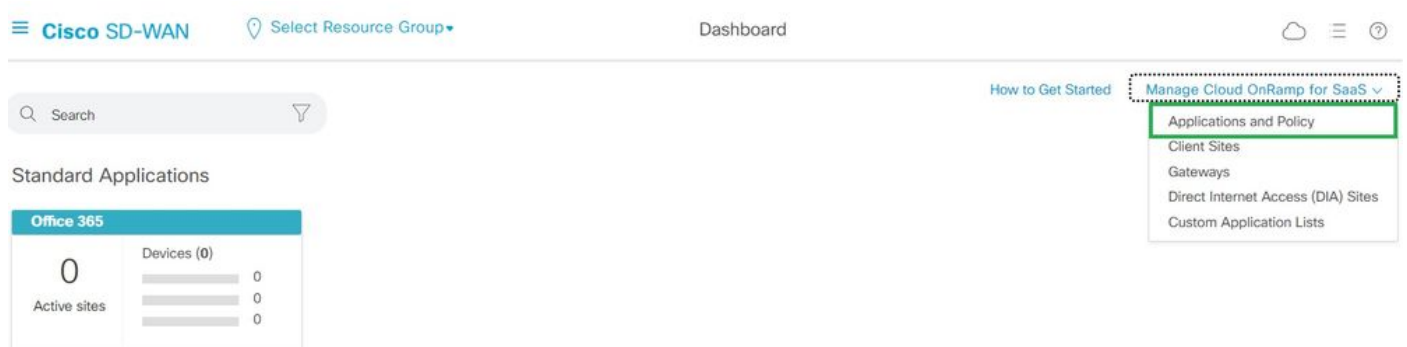
Habilitar acesso direto à Internet e a aplicativos no vManage

Etapa 1. Navegue até Cloud OnRamp for SaaS.



Selecione Cloud onRamp para SaaS

Etapa 2. Navegue até Applications and Policy.



Selecionar aplicativos e política

Etapa 3. Navegue até Application > Enablee Save. Em seguida, clique em Next.

Cisco SD-WAN Select Resource Group Dashboard

Cloud onRamp for SaaS > Applications and Policy

App Type: All Standard Custom

Search

Please click on the table cells Monitoring and Policy/Cloud SLA to enable/disable them for the Cloud Applications.

Total Rows: 14

Applications	Monitoring	VPN (for Viptela OS Device Models)	Policy/Cloud SLA (for Cisco OS Device Models)
Office 365 (Opted Out) Enable Application Feedback for Path ...	Enabled	-	Disabled
Oracle	Enabled	-	Disabled
Salesforce	Disabled	-	Disabled
Sugar CRM	Disabled	-	Disabled

*Selecionar Aplicativos e Habilitar Monitoramento*

Etapa 4. Navegue até Direct Internet Access (DIA) Sites.

Cisco SD-WAN Select Resource Group Dashboard

Search

Standard Applications

Office 365

0 Active sites

Devices (0)

How to Get Started

- Manage Cloud OnRamp for SaaS
  - Applications and Policy
  - Client Sites
  - Gateways
  - Direct Internet Access (DIA) Sites
  - Custom Application Lists

*Selecionar Sites de Acesso Direto à Internet*

Etapa 5. Navegue até Attach DIA Sites e escolha os Sites.



The screenshot shows the Cisco SD-WAN CloudExpress Manage DIA interface. At the top, there is a navigation bar with the Cisco SD-WAN logo, a 'Select Resource Group' dropdown, and a 'Dashboard' link. Below this, there are links for 'How to Get Started' and 'Manage Cloud OnRamp for SaaS'. A search bar is present, and below it, there are buttons for 'Attach DIA Sites', 'Detach DIA Sites', and 'Edit DIA Sites'. A table displays the following data:

Site Id	Status
100001	in sync

Additional information includes '0 Rows Selected', 'Total Rows: 1', and status indicators for 'Devices in sync', 'Sync pending', and 'One or more devices out of sync'.

Anexar sites DIA

## Verificação

Esta seção descreve os resultados para verificar o Cloud OnRamp para SaaS.

- Esta saída mostra as saídas locais do Cloudexpress:

```
cEdge_West-01#sh sdwan cloudexpress local-exits
cloudexpress local-exits vpn 1 app 2 type app-group subapp 0 GigabitEthernet2
application office365
latency 6
loss 0
```

- Esta saída mostra os aplicativos do Cloudexpress:

```
cEdge_West-01#sh sdwan cloudexpress applications
cloudexpress applications vpn 1 app 2 type app-group subapp 0
application office365
exit-type local
interface GigabitEthernet2
latency 6
loss 0
```

- Esta saída mostra contadores de incremento para tráfego interessado:

<#root>

```
cEdge_West-01#sh sdwan policy app-route-policy-filter
```

NAME	NAME	COUNTER NAME	PACKETS	BYTES
_VPN1_Cloud_OnRamp_SAAS	VPN1	default_action_count	640	66303
Cloud_OnRamp_-403085179		600	432292	

- Esta saída mostra o status e a pontuação do vQoE:

The screenshot shows the Cisco SD-WAN dashboard for 'Office 365'. A table displays the vQoE status and score for the site 'cEdge\_West-01'. The vQoE Status is 'Good' (indicated by a green circle) and the vQoE Score is '10.0' (indicated by a green circle and a signal icon).

Sites List	Hostname	vQoE Status	vQoE Score	DIA Status	Selected Interface	Activated Gateway	Local Color	Remote Color	Application Usage
100001	cEdge_West-01	Good	10.0	local	GigabitEthernet2	N/A	N/A	N/A	<a href="#">View Usage</a>

Status e pontuação do vQoE

- Esta saída mostra o caminho de serviço da GUI do vManage:

Cisco SD-WAN | Select Resource Group | Monitor · Devices · Device 360

Devices > Troubleshooting > Simulate Flows

Select Device: cEdge\_West-01 | 1.1.1.101 | Site ID: 100001 | Device Model: C8000v

VPN: VPN - 1 | Source/Interface for VPN - 1: GigabitEthernet4 - ipv4 - 10.2.20.70 | Source IP: 10.2.20.88 | Destination IP: ms-office-server-ip | Application: ms-office-365

Advanced Options >

Simulate



*Caminho do serviço*

- Esta saída mostra o caminho de serviço da CLI do dispositivo:

```
cEdge_West-01#sh sdwan policy service-path vpn 1 interface GigabitEthernet4 source-ip 10.2.20.70 dest-ip 10.2.30.129
Next Hop: Remote
Remote IP: 10.2.30.129, Interface GigabitEthernet2 Index: 8
```

## Informações Relacionadas

- [Guia de configuração do Cisco Catalyst SD-WAN Cloud OnRamp](#)
- [Suporte técnico e downloads da Cisco](#)

## 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.