

# Configuration de SD-WAN Cloud OnRamp pour SaaS

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Activer NAT sur l'interface de transport](#)

[Créer une politique AAR centralisée](#)

[Activer l'application et l'accès Internet direct dans vManage](#)

[Vérification](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit la configuration de Cloud OnRamp pour le logiciel en tant que service (SaaS) à l'aide de la sortie locale de la filiale.

## Conditions préalables

### Exigences

Cisco recommande que vous ayez connaissance du réseau étendu défini par logiciel (SD-WAN) de Cisco.

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco vManage version 20.9.4
- Routeur de périphérie WAN Cisco version 17.9.3a

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

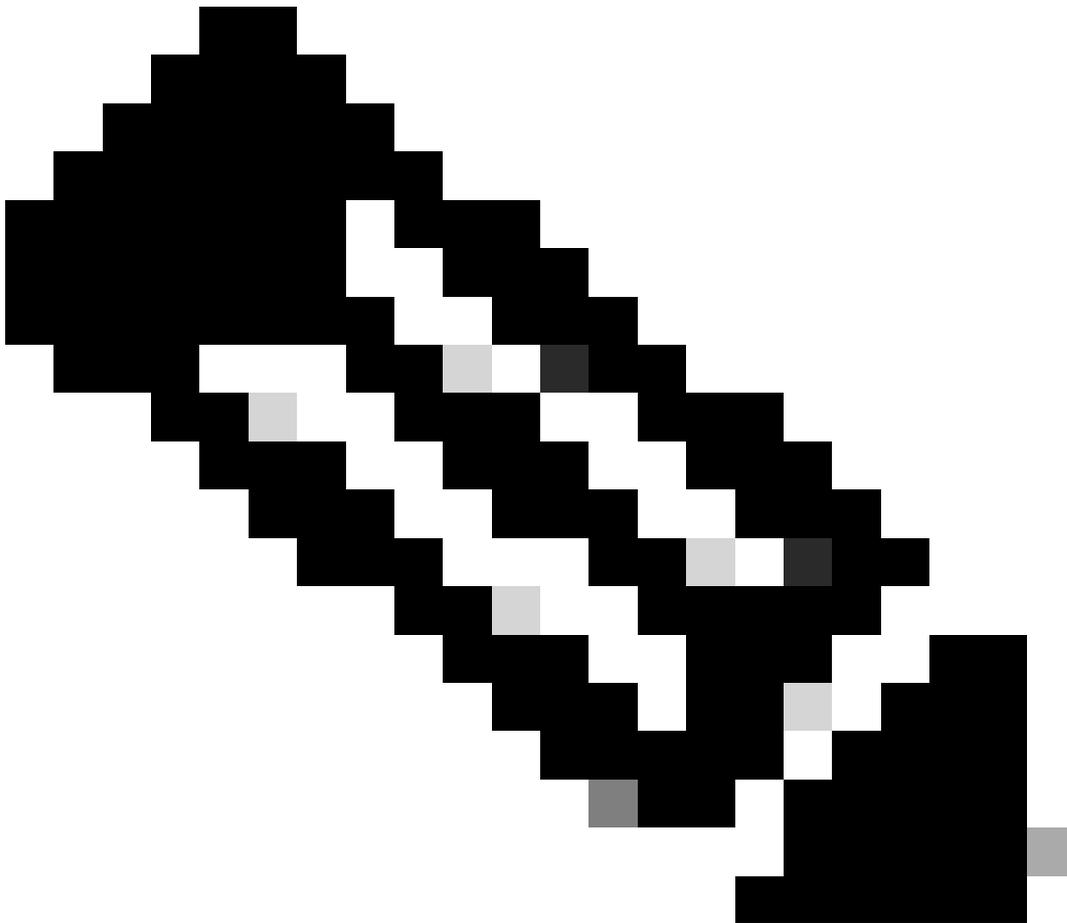
## Informations générales

Pour une entreprise utilisant le SD-WAN, un site de filiale achemine généralement le trafic des applications SaaS par défaut sur des liaisons de superposition SD-WAN vers un data center. À partir du data center, le trafic SaaS atteint le serveur SaaS.

Par exemple, dans une grande entreprise disposant d'un data center central et de sites de filiale, les employés peuvent utiliser Office 365 sur un site de filiale. Par défaut, le trafic Office 365 d'une filiale est acheminé via une liaison de superposition SD-WAN vers un data center centralisé et, à partir de la sortie DIA, vers le serveur cloud Office 365.

Ce document couvre ce scénario : Si le site de la filiale dispose d'une connexion d'accès direct à Internet (DIA), vous pouvez améliorer les performances en acheminant le trafic SaaS via le DIA local, en contournant le centre de données.

---

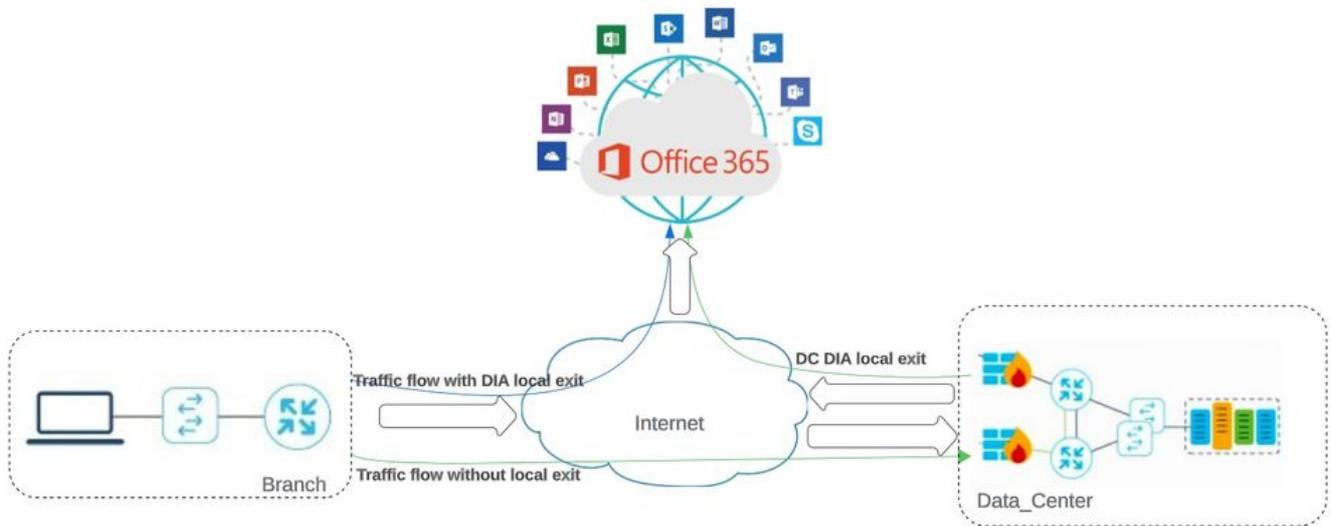


Remarque : la configuration de Cloud OnRamp pour SaaS lorsqu'un site utilise un bouclage comme interface de localisation de transport (TLOC) n'est pas prise en charge.

---

# Configurer

## Diagramme du réseau



Topologie du réseau

## Configurations

### Activer NAT sur l'interface de transport

Accédez à Feature Template . Sélectionnez le **Transport VPN interface** modèle et **Activer NAT**.

Cisco SD-WAN Select Resource Group Configuration · Templates

Configuration Groups Feature Profiles Device Templates Feature Templates

Feature Template > Cisco VPN Interface Ethernet > cEdge\_Basic\_Transport1\_NAT

▼ NAT

IPv4 IPv6

NAT  On  Off

NAT Type  Interface  Pool  Loopback

UDP Timeout 1

TCP Timeout 60

STATIC NAT PORT FORWARD

Activer l'interface NAT

Configuration CLI équivalente :

```
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
```

### Créer une politique AAR centralisée

Pour établir une stratégie centralisée, vous devez suivre la procédure suivante :

#### Étape 1. Créer une liste 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...	

*Modèle NAT d'interface VPN*

#### Étape 2. Créer une liste 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...	

*Liste des sites personnalisés de stratégie centralisée*

#### Étape 3. Configurez le Traffic Rules et créez le 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

Stratégie de routage sensible aux applications

Étape 4. Ajoutez la stratégie à la stratégie souhaitée Sites et 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

Ajouter des stratégies aux sites et aux VPN

Politique d'équivalence 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  
!  
!

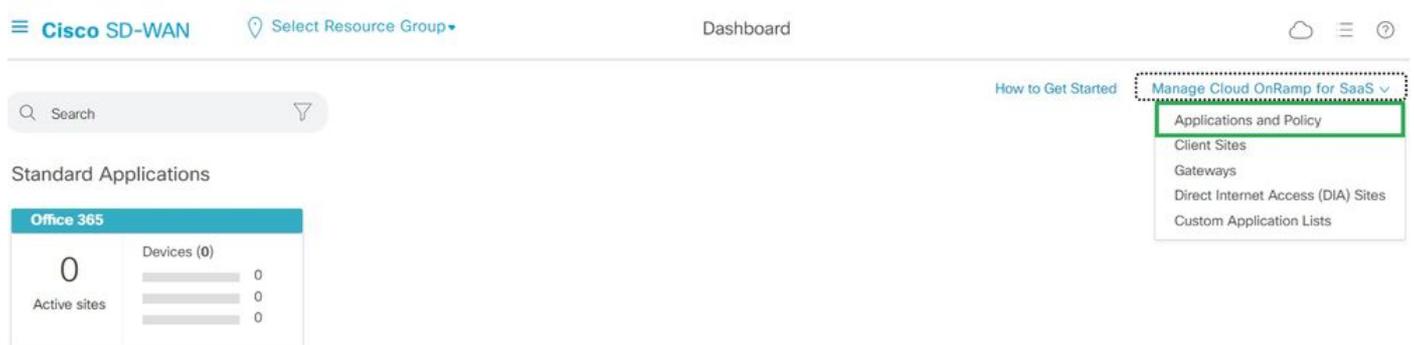
Activer l'application et l'accès Internet direct dans vManage

Étape 1. Accédez à Cloud OnRamp for SaaS.



Sélectionner Cloud onRamp pour SaaS

Étape 2. Accédez à Applications and Policy.



Sélectionner les applications et la stratégie

Étape 3. Accédez à Application > Enable et Save. Cliquez ensuite sur 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

Sélectionner des applications et activer la surveillance

Étape 4. Accédez à Direct Internet Access (DIA) Sites.

Cisco SD-WAN Select Resource Group Dashboard

Search

Standard Applications

Office 365

0 Active sites

Devices (0)

0

0

0

How to Get Started

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

Sélectionner des sites d'accès Internet direct

Étape 5. Naviguez jusqu'Attach DIA Sites aux sites et sélectionnez-les.

The screenshot shows the Cisco SD-WAN CloudExpress interface for managing Cloud OnRamp for SaaS. At the top, there is a navigation bar with 'Cisco SD-WAN', 'Select Resource Group', and 'Dashboard'. 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	✓

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'.

*Joindre des sites DIA*

## Vérification

Cette section décrit les résultats afin de vérifier le Cloud OnRamp pour SaaS.

- Ce résultat montre Cloudexpress local-exits :

```
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
```

- Ce résultat montre les applications 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
```

- Ce résultat montre les compteurs incrémentés pour le trafic intéressé :

<#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
```

- Ce résultat montre l'état et le score de la vQoE :

The screenshot shows the Cisco SD-WAN Dashboard for 'Office 365'. A table titled 'VPN List' displays the following data for site 100001:

Sites List	Hostname	vQoE Status	vQoE Score	DIA Status	Selected Interface	Activated Gateway	Local Color	Remote Color	Application Usage
100001	cEdge_West-01	Good (8-10)	10.0	local	GigabitEthernet2	N/A	N/A	N/A	<a href="#">View Usage</a>

État et score vQoE

- Ce résultat montre le chemin de service de l'interface graphique utilisateur vManage :

Cisco SD-WAN 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

Custom Application (created in CLI):

Advanced Options >

Simulate

Output: Total next hops: 1 | Remote : 1

```

graph LR
    A((1.1.1.101)) --> B(( ))
    B --> C[Remote]
    subgraph C [Remote]
        D[Remote IP: 10.2.30.129]
        E[Interface: GigabitEthernet2]
    end
  
```

*Chemin de service*

- Ce résultat montre le chemin de service de l'interface de ligne de commande du périphérique :

```

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
  
```

## Informations connexes

- [Guide de configuration de Cisco Catalyst SD-WAN Cloud OnRamp](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.