

# SaaS向けSD-WANクラウドオンランプの設定

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[転送インターフェイスでのNATの有効化](#)

[中央集中型AARポリシーの作成](#)

[vManageでアプリケーションと直接インターネットアクセスを有効にする](#)

[検証](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、ブランチローカルEXITを使用したSoftware as a Service(SaaS)向けクラウドオンランプの設定について説明します。

## 前提条件

### 要件

Cisco Software-Defined Wide Area Network(SD-WAN)に関する知識があることが推奨されます。

### 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。

- Cisco vManageバージョン20.9.4
- Cisco WANエッジルーターバージョン17.9.3a

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、クリアな(デフォルト)設定で作業を開始しています。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。

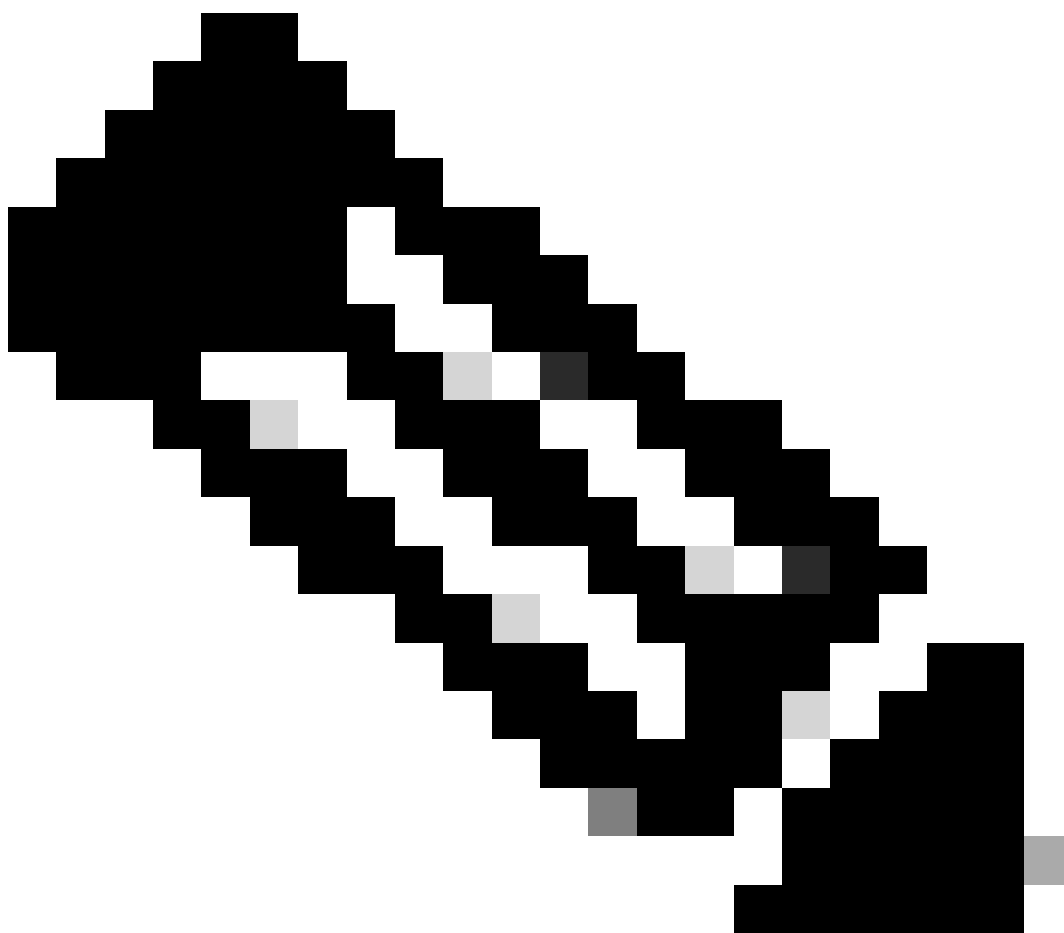
## 背景説明

SD-WANを使用している組織では、通常、ブランチサイトがデフォルトでSaaSアプリケーション

トラフィックをSD-WANオーバーレイリンク経由でデータセンターにルーティングします。データセンターから、SaaSトラフィックはSaaSサーバに到達します。

たとえば、中央のデータセンターとブランチサイトを持つ大規模な組織では、従業員はブランチサイトでOffice 365を使用できます。デフォルトでは、ブランチサイトのOffice 365トラフィックはSD-WANオーバーレイリンクを介して中央のデータセンターにルーティングされ、DIA出口からOffice 365クラウドサーバにルーティングされます。

このドキュメントでは、次のシナリオについて説明します。ブランチサイトに直接インターネットアクセス(DIA)接続がある場合、データセンターをバイパスしてローカルDIAを介してSaaSトラフィックをルーティングすることで、パフォーマンスを向上できます。

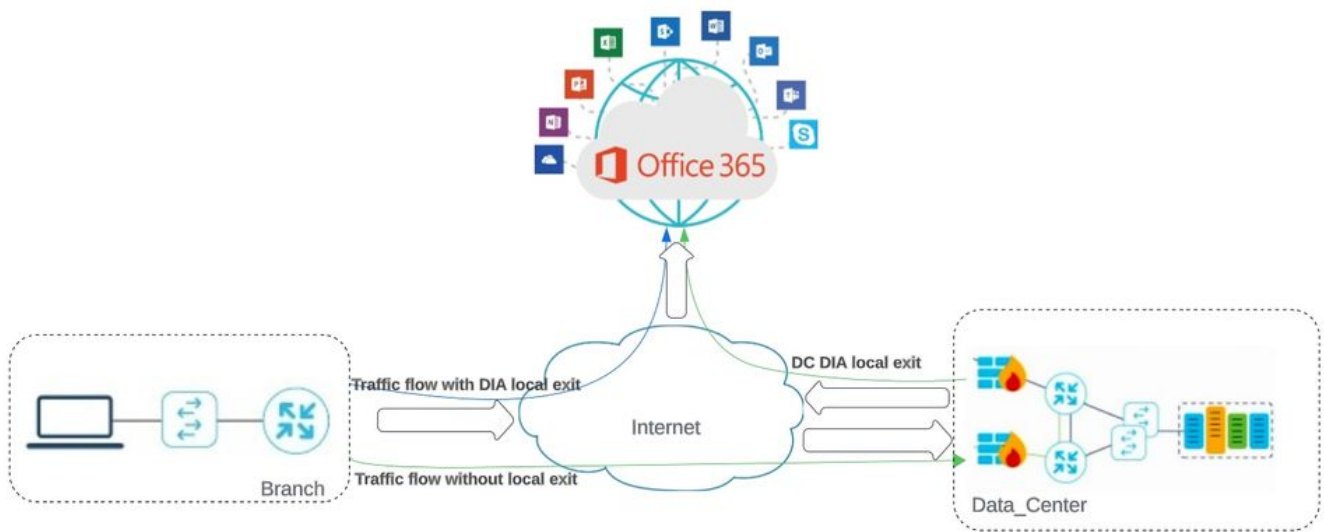


注：サイトがTransport Locator(TLOC)インターフェイスとしてループバックを使用する場合、SaaS用のクラウドオンランプの設定はサポートされません。

---

## 設定

## ネットワーク図



Network Topology

## コンフィギュレーション

### 転送インターフェイスでのNATの有効化

Feature Template に移動します。テンTransport VPN interface プレートを選択し、NATをイネーブルにします。

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

インターフェイスNATの有効化

CLIに相当する設定：

```
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
```

## 中央集中型AARポリシーの作成

中央集中型ポリシーを確立するには、次の手順に従う必要があります。

ステップ 1 : サイトリストを作成します。

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...	

VPNインターフェイスNATテンプレート

ステップ 2 : VPNリストを作成します。

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...	

一元化されたポリシーのカスタムサイトリスト

ステップ 3 : を設定Traffic Rules し、Application Aware Routing Policyを作成します。

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

アプリケーション認識型ルートポリシー

ステップ 4 : ポリシーをに追加しSites、VPNします。

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

サイトとVPNへのポリシーの追加

CLIに相当するポリシー :

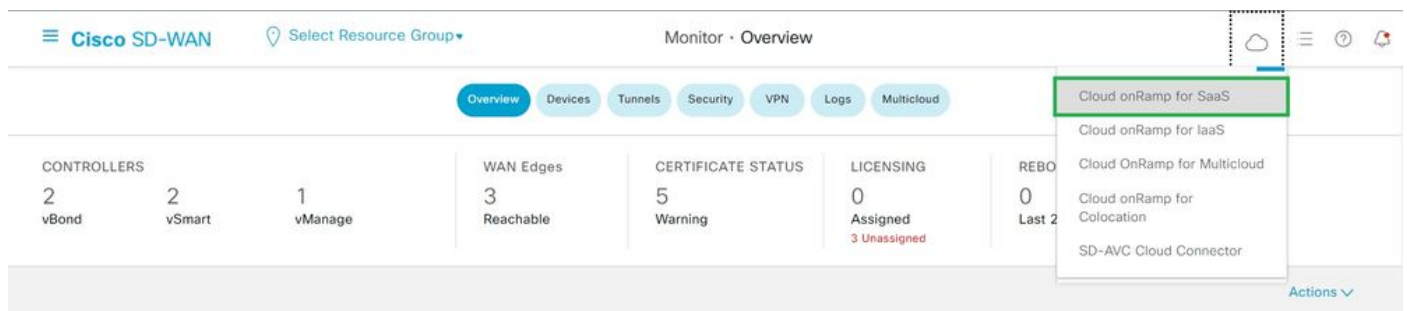
viptela-policy:policy  
app-route-policy\_VPN1\_Cloud\_OnRamp\_SAAS  
vpn-list VPN1

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  
!  
!

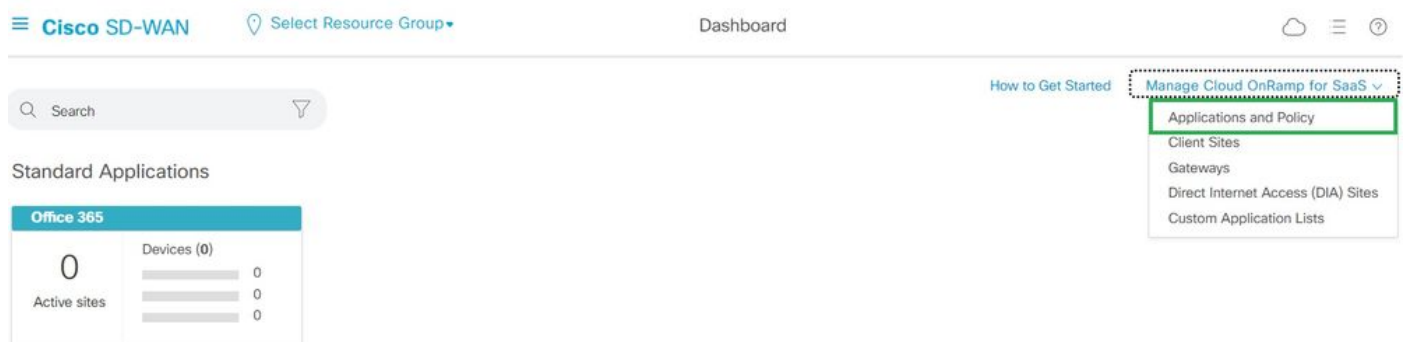
vManageでアプリケーションと直接インターネットアクセスを有効にする

ステップ 1 : Cloud OnRamp for SaaSに移動します。



SaaS向けクラウド・オン・ランプの選択

ステップ 2 : Applications and Policyに移動します。



アプリケーションとポリシーの選択

ステップ 3 : Application > Enableおよび Saveに移動します。次にNextをクリックします。

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

アプリケーションの選択とモニタリングの有効化

ステップ 4 : Direct Internet Access (DIA) Sitesに移動します。

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

ダイレクトインターネットアクセスサイトの選択

ステップ 5 : サイトに移動Attach DIA Sites し、サイトを選択します。



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'. The main area displays a table with one row: Site Id 100001, with a green status indicator. The status bar at the bottom indicates 'Devices in sync'.

DIAサイトの接続

## 検証

このセクションでは、SaaS向けクラウドオンランプを検証するための結果について説明します。

- 次の出力は、Cloudexpressのlocal-exitを示しています。

```
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
```

- 次の出力は、Cloudexpressアプリケーションを示しています。

```
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
```

- 次の出力は、対象トラフィックのカウンタの増加を示しています。

<#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	

- 次の出力は、vQoEのステータスとスコアを示しています。

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

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>

vQoEのステータスとスコア

- 次の出力は、vManage GUIからのservice-pathを示しています。

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 - 10.2.2.1 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

The diagram illustrates a service path starting from a source IP of 1.1.1.101. An arrow points to a box labeled 'Remote' which contains the Remote IP 10.2.30.129 and the Interface GigabitEthernet2.

## サービスパス

- 次の出力は、デバイスCLIからのservice-pathを示しています。

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

## 関連情報

- [Cisco Catalyst SD-WANクラウドオンランブコンフィギュレーションガイド](#)
- [シスコのテクニカルサポートとダウンロード](#)

## 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。