

# Konfigurieren von SD-WAN Cloud OnRamp für SaaS

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[NAT auf der Transportschnittstelle aktivieren](#)

[Erstellen einer zentralisierten AAR-Richtlinie](#)

[Aktivieren von Anwendungs- und direktem Internetzugriff in vManage](#)

[Verifizierung](#)

[Zugehörige Informationen](#)

---

## Einleitung

In diesem Dokument wird die Konfiguration für Cloud OnRamp für Software as a Service (SaaS) mithilfe des lokalen Verlassens der Außenstelle beschrieben.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse des Cisco Software-Defined Wide Area Network (SD-WAN) verfügen.

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco vManage, Version 20.9.4
- Cisco WAN Edge-Router Version 17.9.3a

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

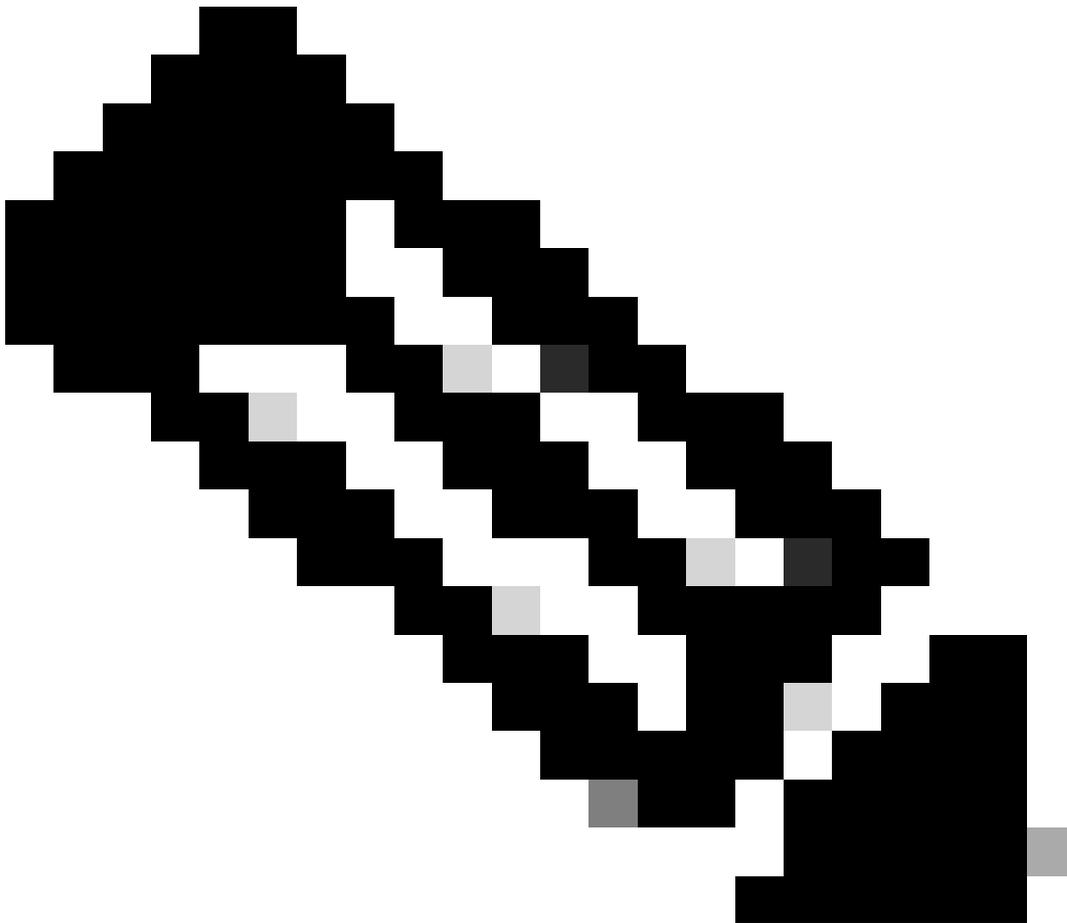
## Hintergrundinformationen

Bei Unternehmen, die SD-WAN verwenden, leitet eine Außenstelle den Datenverkehr von SaaS-Anwendungen standardmäßig über SD-WAN-Overlay-Links zu einem Rechenzentrum weiter. Vom Rechenzentrum aus gelangt der SaaS-Datenverkehr zum SaaS-Server.

In großen Unternehmen mit zentralem Rechenzentrum und Zweigstellen können Mitarbeiter beispielsweise Office 365 in Zweigstellen verwenden. Standardmäßig wird der Office 365-Datenverkehr in einer Zweigstelle über eine SD-WAN-Overlay-Verbindung zu einem zentralisierten Rechenzentrum und vom DIA-Ausgang zum Office 365-Cloud-Server geleitet.

In diesem Dokument wird folgendes Szenario behandelt: Wenn die Außenstelle über eine DIA-Verbindung (Direct Internet Access) verfügt, können Sie die Leistung verbessern, indem Sie den SaaS-Datenverkehr unter Umgehung des Rechenzentrums über die lokale DIA weiterleiten.

---

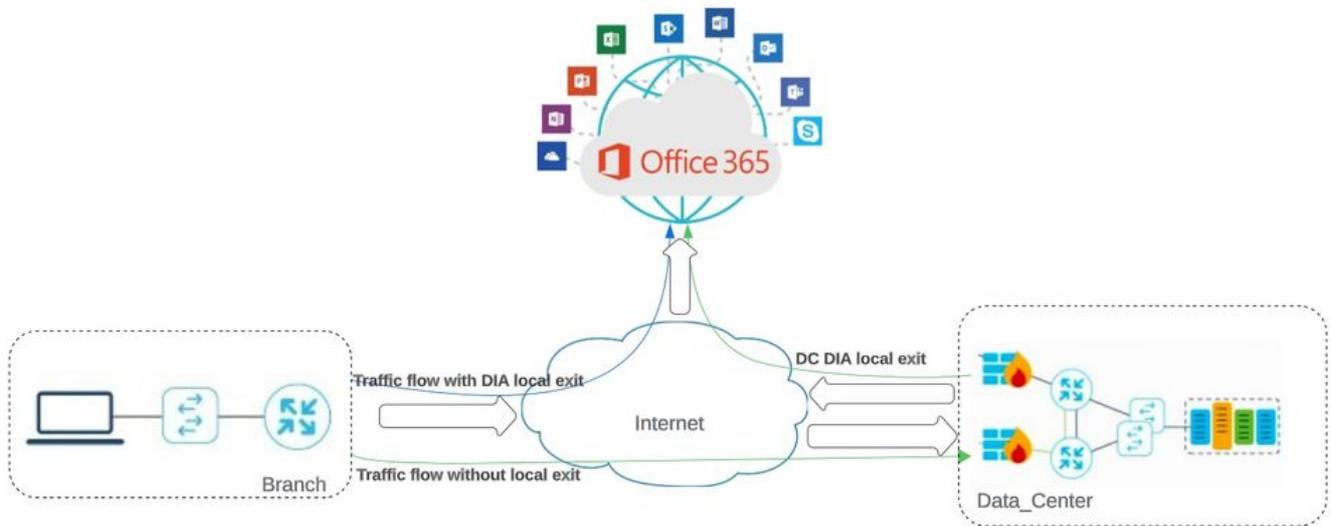


Hinweis: Die Konfiguration von Cloud OnRamp für SaaS, wenn ein Standort ein Loopback als TLOC-Schnittstelle (Transport Locator) verwendet, wird nicht unterstützt.

---

# Konfigurieren

## Netzwerkdiagramm



Netzwerktopologie

## Konfigurationen

### NAT auf der Transportschnittstelle aktivieren

Navigieren Sie zu Feature Template . Wählen Sie die **Transport VPN interface** Vorlage aus, und **aktivieren Sie 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

TCP Timeout

STATIC NAT PORT FORWARD

*NAT für Schnittstelle aktivieren*

CLI-äquivalente Konfiguration:

```
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
```

### Erstellen einer zentralisierten AAR-Richtlinie

Um eine zentrale Richtlinie einzurichten, müssen Sie dieses Verfahren befolgen:

#### Schritt 1: Erstellen einer Standortliste:

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...	

*NAT-Vorlage für VPN-Schnittstelle*

#### Schritt 2: VPN-Liste erstellen:

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...	

*Benutzerdefinierte Siteliste für zentrale Richtlinie*

#### Schritt 3: Konfigurieren Sie die Traffic Rules und erstellen Sie die 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

### Anwendungssensitive Routing-Richtlinie

Schritt 4: Fügen Sie die Richtlinie dem vorgesehenen Sites hinzu, und 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

### Hinzufügen von Richtlinien zu Standorten und VPNs

CLI-äquivalente Richtlinie:

```

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  
!  
!

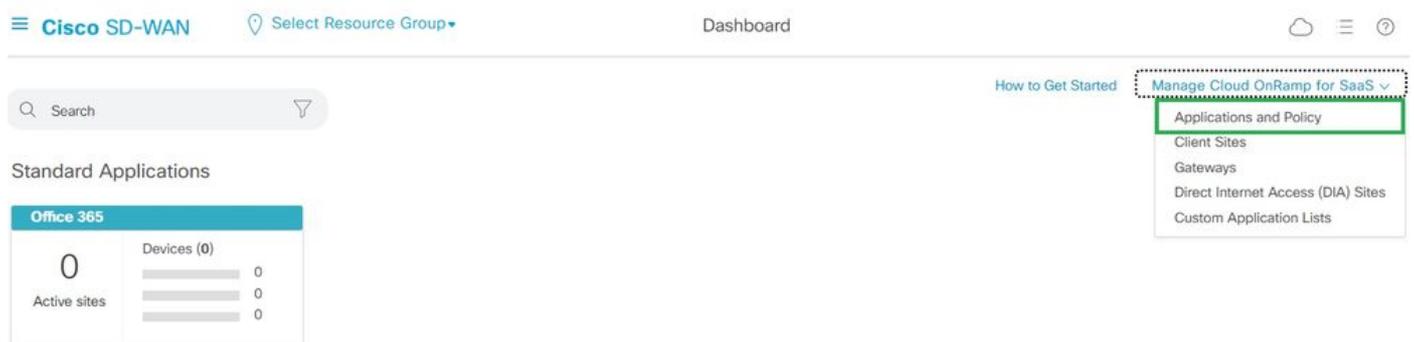
Aktivieren von Anwendungs- und direktem Internetzugriff in vManage

Schritt 1: Navigieren Sie zu Cloud OnRamp for SaaS.



Wählen Sie Cloud onRamp für SaaS

Schritt 2: Navigieren Sie zu Applications and Policy.



Auswählen von Anwendungen und Richtlinien

Schritt 3: Navigieren Sie zu Application > Enable und Save. Klicken Sie dann auf 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

Anwendungen auswählen und Überwachung aktivieren

Schritt 4: Navigieren Sie zu 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

Direkten Internetzugriff auswählen

Schritt 5: Navigieren Sie zu, Attach DIA Sites und wählen Sie Sites aus.

The screenshot shows the Cisco SD-WAN CloudExpress Manage DIA interface. At the top, there is a navigation bar with 'Cisco SD-WAN', 'Select Resource Group', and 'Dashboard'. Below this, there is a search bar and a table with one row. The table has columns for 'Site Id' and 'Status'. The 'Site Id' column contains '100001' and the 'Status' column contains a green checkmark. Above the table, there are buttons for 'Attach DIA Sites', 'Detach DIA Sites', and 'Edit DIA Sites'. The 'Attach DIA Sites' button is highlighted with a green box. Below the table, there is a status bar with icons for 'Devices in sync', 'Sync pending', and 'One or more devices out of sync'. The 'Devices in sync' icon is green and active.

*DIA-Standorte anhängen*

Verifizierung

In diesem Abschnitt werden die Ergebnisse zur Verifizierung der Cloud-OnRamp für SaaS beschrieben.

- Diese Ausgabe zeigt 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
```

- Diese Ausgabe zeigt CloudExpress-Anwendungen:

```
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
```

- Diese Ausgabe zeigt Zähler für interessierten Datenverkehr inkrementiert an:

<#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
```

- Diese Ausgabe zeigt den vQoE-Status und die Bewertung an:

The screenshot shows the Cisco SD-WAN dashboard with a table of VPNs. The 'vQoE Status' and 'vQoE Score' columns for the first VPN are highlighted with green boxes. The vQoE Status is 'Good' (green circle) and the vQoE Score is '10.0' (blue circle with a checkmark).

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>

vQoE-Status und -Bewertung

- Diese Ausgabe zeigt den Dienstpfad der vManage-GUI:

### Servicepfad

- Diese Ausgabe zeigt den Dienstpfad von der Geräte-CLI an:

```
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
```

## Zugehörige Informationen

- [Cisco Catalyst SD-WAN Cloud OnRamp - Konfigurationsleitfaden](#)
- [Technischer Support und Downloads von Cisco](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.