

CISCO VALIDATED DESIGN

SD-WAN: Cloud onRamp for SaaS Deployment Guide

July 2018



Table of Contents

Introduction	1
Cloud onRamp for SaaS feature overview	2
Use cases	2
Application support	3
How it works.....	3
Cloud onRamp for SaaS prerequisites	7
Prerequisites	7
Cloud onRamp for SaaS Configuration.....	18
Cloud onRamp for SaaS Monitoring.....	28
Appendices	33
Appendix A: Product list.....	33
Appendix B: Cisco SD-WAN solution overview	34
Appendix C: Cloud onRamp example topology	37
Appendix D: Base vManage device template	38
Appendix E: Base CLI configuration	44
Appendix F: NAT, DNS, and VPN 0 default route configurations needed for DIA example.....	48
Appendix G: Cloud onRamp for SaaS CLI configurations.....	50
Appendix H: Cloud onRamp for SaaS CLI monitoring commands	51

Introduction

More and more enterprises have adopted business-critical software-as-a-service (SaaS) applications, including Salesforce, Box, and Office365. Many companies are still back-hauling this traffic from remote sites to a centralized location, such as a data center, for Internet access. This process can be inefficient because any data loss or latency affects application performance and, in turn, the end-user's experience. In addition, many network administrators have limited or no visibility into the performance of their SaaS applications, and when there is impairment to their applications, there may not be an easy way to move access to their applications to an alternate path.

With Cisco® Software-Defined WAN (SD-WAN), you can easily configure access to SaaS applications through a centralized GUI. Access can be either direct to the Internet from a remote site or through gateway locations, such as a regional data center or carrier-neutral facility (CNF). In addition, the Cisco SD-WAN solution continuously measures and monitors the performance of each application along with each path to that application, and it chooses the best-performing path for the most optimal user experience. If changes or impairment occur in the network, the solution can adjust dynamically and intelligently move SaaS traffic to the updated optimal path. This feature is called Cloud onRamp for SaaS, formerly called CloudExpress.

The benefits of Cloud onRamp for SaaS include:

- Improved branch-office user experience for SaaS applications by using the best-performing network path
- Increased SaaS application resiliency with multiple network path selections and active monitoring
- Visibility into SaaS application performance using probes that measure real-time data
- Modification of path selection depending on the application performance without any required administrator action
- Operational simplicity and consistency through centralized control and management of SaaS application policies

This guide presents an overview of the Cloud onRamp for SaaS feature, describes how it works, discusses its prerequisites, details its configuration, and finally shows how an administrator can monitor it. This document assumes that an SD-WAN deployment is already in place and the overlay is operational. It also assumes that you have a basic understanding of the Cisco SD-WAN solution and its concepts.

Please refer to Appendix A for the hardware models and software versions used in this deployment guide. Please refer to Appendix B for an SD-WAN solution overview and a brief description of its components that can aid in understanding the SaaS feature and its deployment if some of the concepts are unfamiliar. Appendix C describes the example topology used to demonstrate the Cloud onRamp SaaS configuration and monitoring.

Cloud onRamp for SaaS feature overview

Use cases

Two main use cases of interest for this feature are Direct Cloud Access (DCA) and cloud access through gateways.

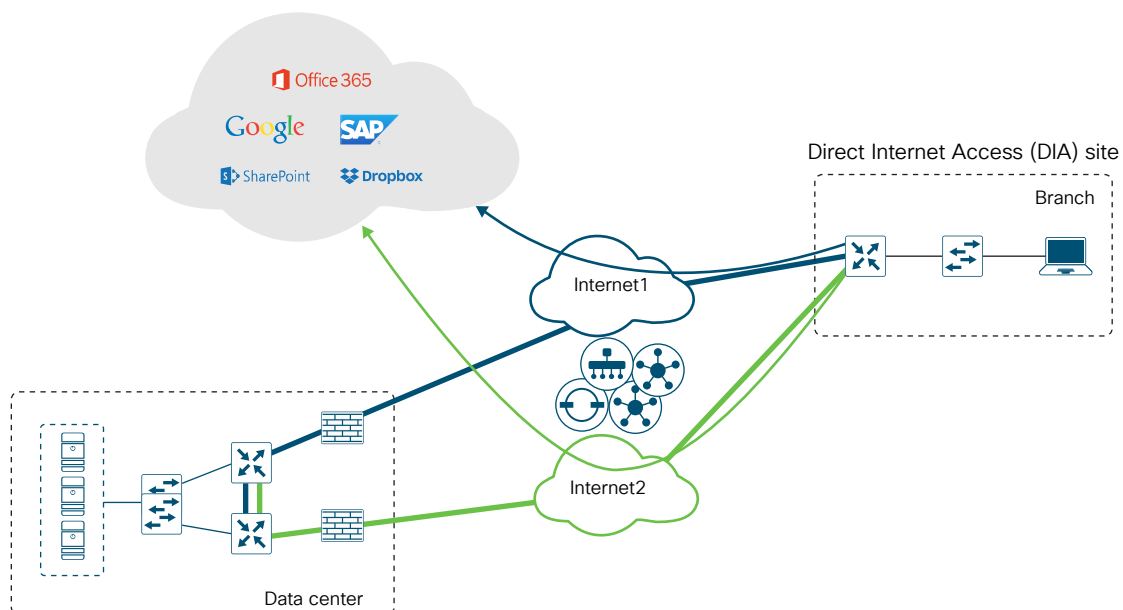
Direct Cloud Access

As shown in Figure 1, DCA allows a remote site to access SaaS applications directly from the Internet. Cloud onRamp for SaaS permits only the designated application traffic to use the directly connected Internet transport securely, while all other Internet-bound traffic takes the usual path, which could be through a regional hub, a data center, or a CNF. This feature allows the remote site to bypass the latency of tunneling Internet-bound traffic to a central site, subsequently improving the connectivity to the prioritized SaaS application; this feature is commonly referred to as Direct Internet Access (DIA). The Cisco vEdge router chooses the most optimal Internet path for access to these SaaS applications. Different applications could traverse different paths because the path selection is calculated on a per-application basis.

If any SaaS application path becomes unreachable or its performance score falls below an unacceptable level, the path is removed as a candidate path option. If all paths cannot be path candidates because of reachability or performance, then traffic to the SaaS application follows the normal, routed path.

Figure 1 illustrates a remote site using DIA to access SaaS applications.

Figure 1. DCA/DIA



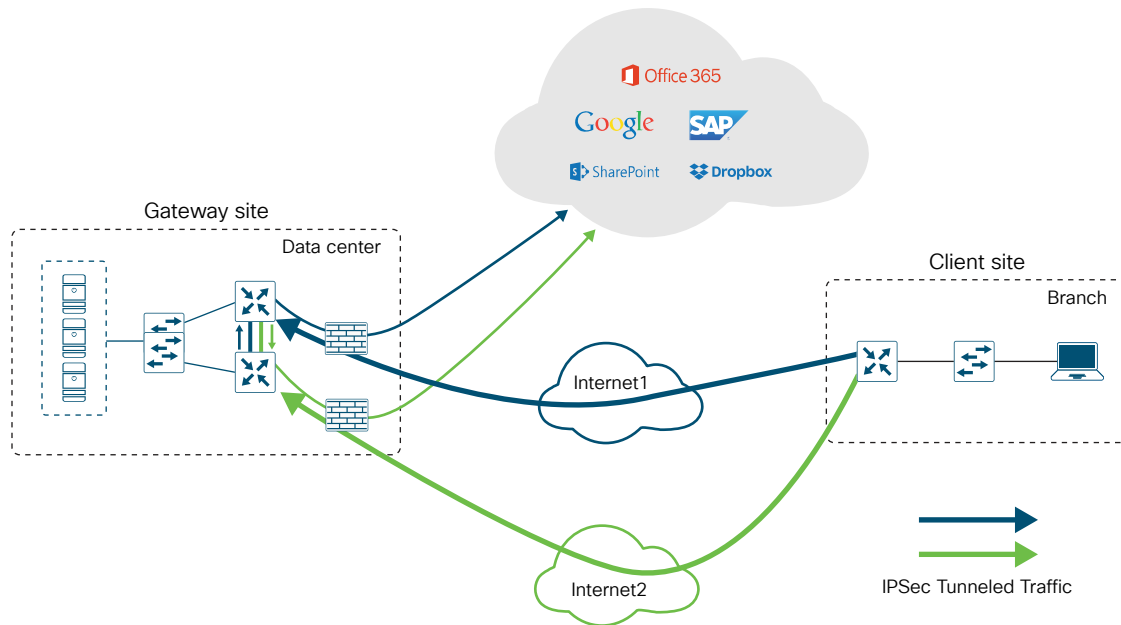
Cloud access through gateway

Many enterprises do not use DIA at the branch office, because either their sites are connected by only private providers (Multiprotocol Label Switching [MPLS], Virtual Private LAN Services [VPLS], etc.) or centralized policy or security requirements don't permit it. They may use data centers, regional hubs, or even CNFs to enable Internet connectivity. In this case, SaaS traffic is tunneled to the best-performing "gateway" site, where it is subsequently

routed to the Internet to reach the requested SaaS application service. Note that different remote sites and different applications may use different gateway sites and paths, depending on the application and measured application performance. Remote sites that use gateway sites for Internet access are referred to as “client sites”.

Figure 2 illustrates cloud access through a gateway. A branch office tunnels SaaS traffic to a gateway location, and then uses the Internet at the gateway location to access the SaaS applications.

Figure 2. Cloud access through a gateway



Hybrid approach

It is possible to have a combination of DIA sites and client/gateway sites. When you define both DIA sites and gateway sites, SaaS applications can use either the DIA exits of the remote site or the gateway sites for any given application, depending on which path provides the best performance. DIA sites are technically a special case of a client site, but the Internet exits are local instead of remote.

Application support

At the time of this writing, the following SaaS applications are supported: Intuit, Concur, Oracle, Amazon AWS, Salesforce, Zendesk, Dropbox, Sugar CRM, Office 365, Zoho CRM, Google Apps, Box, and Goto Meeting.

How it works

Performance statistics

The Cloud onRamp for SaaS feature actively monitors SaaS application performance from each site over multiple paths. The vEdge router views performance statistics differently, depending on whether it is part of a DIA, gateway, or client site. A DIA or gateway site calculates performance statistics of the SaaS application directly, but a client site does not. SaaS performance from a client site depends on the SaaS application performance from a gateway site, plus the performance of the path from the client site to that gateway site.

DIA or gateway site SaaS path performance statistics

In the case of a DIA or gateway site, the vEdge router issues numerous HTTP requests to each SaaS application over every available path to the application. Over a 2-minute sliding window, it calculates the average loss and latency for each application and path pair.

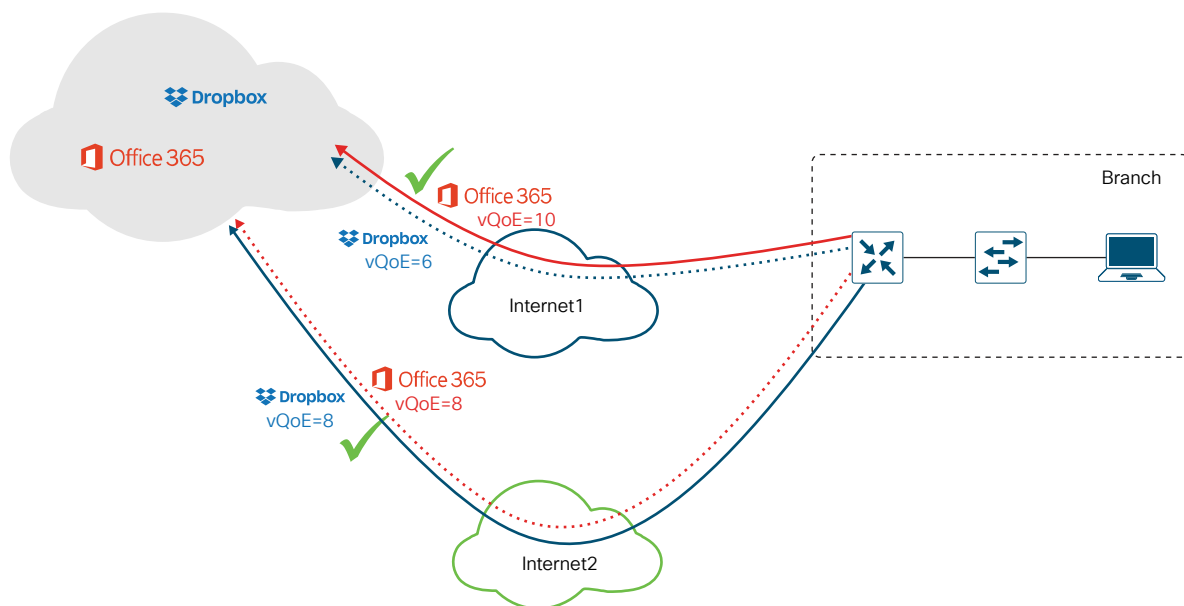
Using this data, the vEdge router calculates a Quality of Experience or vQoE score. To get this score, the vEdge router accounts for average loss and latency; vManage collects this data and keeps a record of expected average loss and latency values for all of the SaaS applications. If the actual measured loss and latency is less than the expected loss and latency, then a vQoE score of 10 is given. If actual loss or latency is more than the expected loss or latency, then a vQoE score that reflects a percentage of the baseline performance on a 10-point scale is assigned.

vManage assigns a color and vQoE status to each application and path. A vQoE score of 8 to 10 is green or good, a score of 5 to 8 is yellow or average, and a score of 0 to 5 is red or bad.

For any application, the vEdge router takes a moving average over several 2-minute time periods and then picks the path with the higher vQoE score.

Figure 3 shows vQoE scores for each application and path; Office 365 uses the Internet1 path, whereas Dropbox uses the Internet2 path.

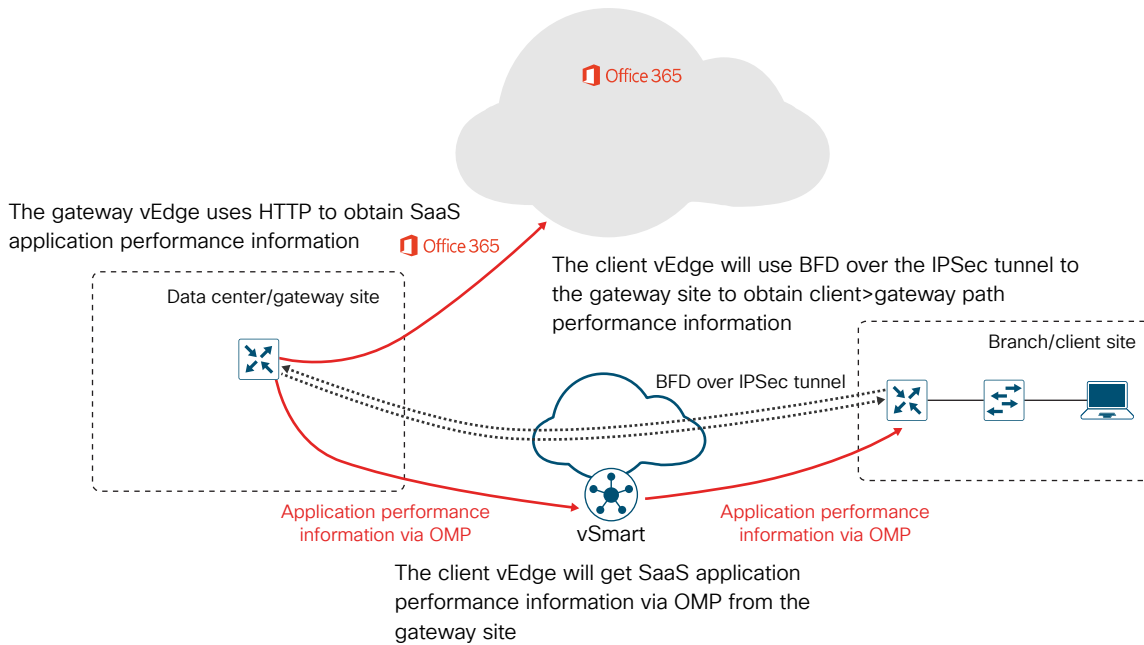
Figure 3. Example SaaS vQoE scoring and path selection for a DIA site



Client site SaaS path performance statistics

As covered in the previous section, the gateway site issues HTTP requests directly to the SaaS application and calculates loss and latency of the application along each of its Internet exit paths. It relays this information back to the client sites via the Overlay Management Protocol (OMP), which runs between the vEdge routers and establishes and maintains the control plane in the overlay network. The client site uses Bidirectional Forward Detection (BFD), which runs between vEdge routers over the IPSec tunnels to detect loss, latency, and jitter on the path to the gateway site. Figure 4 illustrates the process.

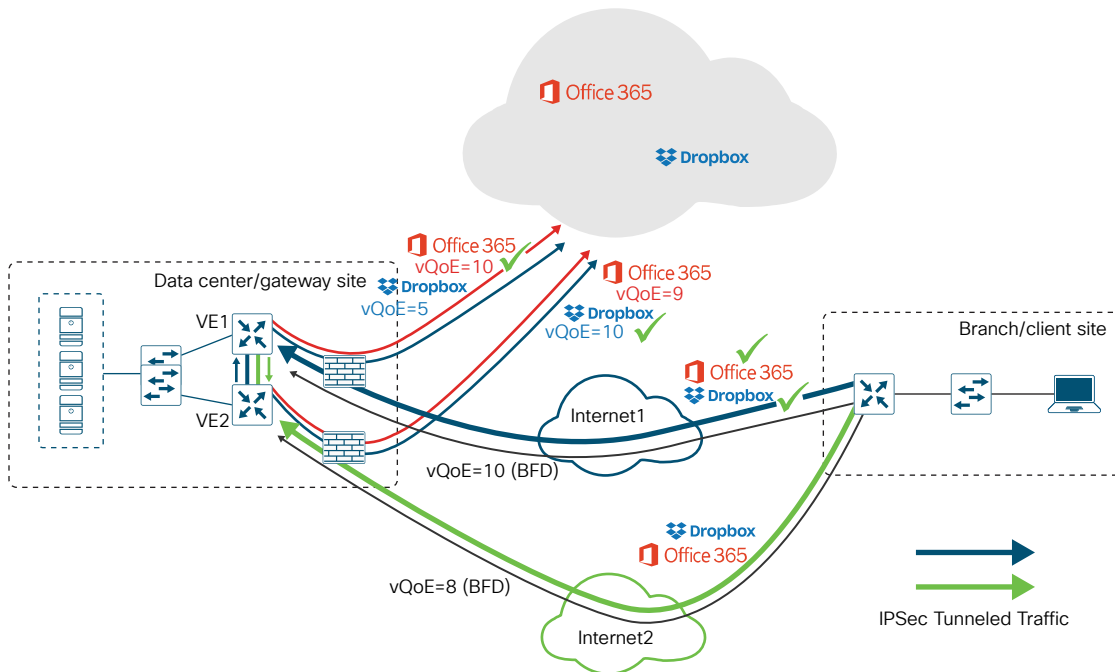
Figure 4. Obtaining performance metrics for client/gateway sites



The client vEdge router looks at the loss and latency on the paths to the gateway sites and the loss and latency to the SaaS applications from the exits on the gateway sites and calculates vQoE scores for each SaaS application and path based on that information. The vEdge router picks the optimal path based on this information.

Figure 5 shows vQoE scores calculated for each application and path; Office 365 uses the Client>Internet1>VE1>Internet1 path, whereas Dropbox uses the Client>Internet1>VE1>VE2>Internet2 path.

Figure 5. Example SaaS vQoE scoring and path selection for a client/gateway site



Traffic forwarding

Cisco SD-WAN Deep Packet Inspection (DPI) identifies SaaS applications. When a flow starts for the first time, the traffic takes the path indicated by the routing table. After a couple of packets, DPI identifies the application and stores its identity in a cache so that any subsequent flows going to that destination are sent out the optimal exit determined by the vQoE score instead of the normal routed path. DPI does not redirect the initial application flow because the redirection would cause Network Address Translation (NAT) changes that would break the TCP flow.

Tech Tip

Web proxies: DPI categorizes SaaS traffic by using destination IP/port number, so when you use a routed web proxy, all SaaS traffic looks identical because the URL from the client contains the same web-proxy IP and proxy port number. Thus the vEdge routers may pick the same forwarding path for the SaaS applications using the web proxy instead of being able to choose the paths for each independently. To work around this situation, either disable the web proxy for the SaaS domains or configure each SaaS domain for a different proxy port.

Tech Tip

Dual-vEdge sites: Because DPI is used to classify flows on a vEdge device, it is important for traffic to be symmetric; that is, DPI should be able to see both request and response traffic. If traffic from a branch office takes a routed path to the Internet out of one vEdge router but the return traffic comes back through a different vEdge router, DPI may not be able to classify the traffic correctly in order that a local exit or gateway can be chosen for it; it will continue to be routed normally. Care should be taken with routing metrics to ensure symmetry for normally routed traffic.

The role of DNS

In order to reach the SaaS applications to calculate performance statistics in the case of gateway and DIA sites, the vEdge router needs to first resolve the names of the Cloud onRamp SaaS applications into IP addresses. It performs this task by using the Domain Name System (DNS) server addresses defined in VPN 0, and it initiates a separate DNS query to the same application on each of its local Internet exits.

When a host at a site issues a DNS query, the DPI engine intercepts it. If the local DIA Internet exit is the best path and if the query is for a Cloud onRamp SaaS application, the vEdge router acts as a proxy and overrides the user DNS settings by forwarding the query to the DNS server defined under VPN 0 over the best-performing DIA Internet exit. If the best path is through a gateway vEdge router, then the DNS query is forwarded to the gateway, which intercepts it and forwards it to the DNS server under VPN 0 over its best-performing Internet exit. The DPI engine forwards any DNS queries for non-Cloud onRamp applications normally according to the routing table.

Cloud onRamp for SaaS prerequisites

Before you can configure Cloud onRamp for SaaS, prerequisites must first be in place.

Tech Tip

If you have existing data policies, be aware that centralized data policies that match the user traffic and change the next-hop Transport Location (TLOC) override Cloud onRamp forwarding decisions. In addition, if you use a **set local-tloc** action in a data policy, it will have no effect on the Cloud onRamp for SaaS feature.

Prerequisites

All site types (DIA, client, or gateway sites)

- vManage mode: Sites to be configured for Cloud onRamp for SaaS need to be in vManage mode as opposed to command-line interface (CLI) mode, meaning that the vManage GUI will control the configuration of the vEdge router as opposed to a user using the CLI to modify the configuration directly on a vEdge device. You need to apply a device template to the vEdge router from the vManage GUI in order to put it in vManage mode.
- Cisco vEdge software version: The minimum Cisco vEdge software version is 16.3.0 to configure DIA sites and 17.1.0 to configure gateway sites, but you should use the latest recommended maintenance release. Refer to Appendix A for the code version used in this guide.

Tech Tip

When configuring Cloud onRamp for SaaS, you will be able to select only sites in which all site vEdge routers are in vManage mode running Cisco vEdge software Version 16.3.0 or later. You will not be able to select sites that do not meet this criteria; the sites will be grayed out and cannot be selected.

- Default route for service VPN: A default route that directs traffic out to the Internet (perhaps through a data center, regional hub, CNF, or even locally) and can reach the SaaS applications must be present in the service VPNs before you configure the Cloud onRamp for SaaS feature. The first couple of packets of a flow need to take the traditional routing path before the Cisco SD-WAN DPI engine can identify the application and cache it so that subsequent flows can be directed to the Internet by a DIA path or a gateway site path, whichever is most optimal at that time. The initial flow continues to take the routed path until completion.

DIA or gateway sites only

- Network Address Translation (NAT) configuration: In order for SaaS traffic to be able to exit the site locally (for both DIA and gateway sites), NAT configuration is required under each VPN 0 physical interface attached to the Internet or Internet path. This requirement is necessary for the interface to be a candidate for local exit, regardless of any other NAT configured for the site. Enabling NAT, by default, causes translation of the source IP address of a site user to the outside IP address of the vEdge router when it uses the interface as a local exit to the SaaS applications.

Tech Tip

If you have no NAT-configured interfaces in VPN 0 and you are trying to configure a DIA or gateway site, SaaS traffic will not be able to use any local exits. If you try to explicitly specify exit interfaces in the configuration that are not in VPN 0, or interfaces that are in VPN 0 but do not have NAT configured on them, you will get a failure attempt when the vManage tries to push the Cloud onRamp SaaS configuration to the vEdge router.

- **DNS server configuration:** Configure DNS server addresses in VPN 0 so the vEdge router can resolve the SaaS application hostnames and initiate performance statistics to those SaaS servers, as well as intercept DNS queries to the configured SaaS applications and act as a DNS proxy for those users. The DNS server addresses that you specify need to be able to resolve the SaaS Fully Qualified Domain Names (FQDNs) and need to be reachable from VPN 0 or the local Internet exit.
- **Default route for local exit:** This guide assumes that the SD-WAN overlay is already operational. If so, you must have at least one default route defined under VPN 0 to allow the tunnel to connect to the remote sites and data centers through one or more of the physical interfaces. You can either statically define the configuration of this default route or obtain it via Dynamic Host Configuration Protocol (DHCP). For DIA and gateway sites, this default route gives the next-hop information for the direct Internet exits when the Cloud onRamp for SaaS feature is configured.

Tech Tip

For DIA/gateway sites: If you have not defined a default route in VPN 0 for the direct Internet exit, NAT on the interfaces, and/or DNS servers in the transport VPN, you may be able to configure Cloud onRamp for SaaS but the application won't be reachable through the VPN 0 interfaces. The SaaS application vQoE score will show up as 0 and status will show up as red/bad on the SaaS application monitoring page in the vManage GUI.

If you meet all of the prerequisite conditions, you can skip the next section and go to the Cloud onRamp SaaS configuration section. The next section assists with validating and configuring the prerequisite requirements for the Cloud onRamp for SaaS feature.

Refer to Appendix F to view the prerequisite configurations in the CLI.

Validate prerequisite configuration

For the following procedures, you need to access the vManage web instance by using a web browser; for example:

<https://vmanage1.cisco.com:8443/>

Procedure 1

Verify if a device is in vManage mode.

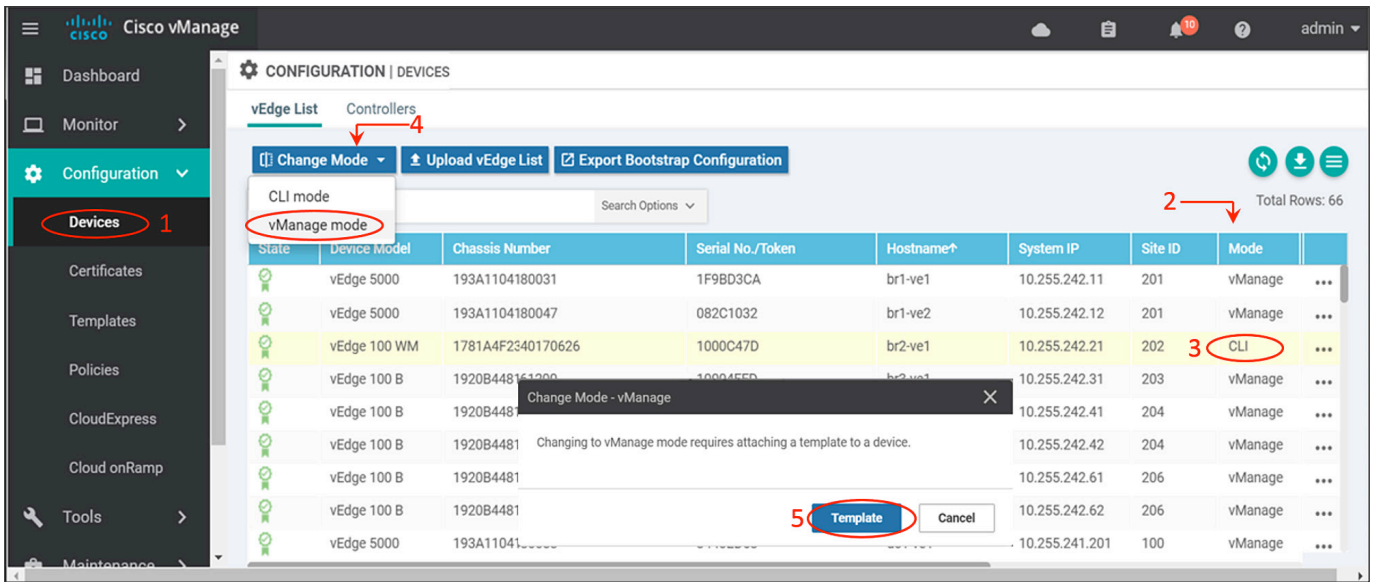
Step 1: Navigate to Configuration>Devices in the left column of the vManage GUI.

Step 2: Confirm that the targeted vEdge routers are set to vManage mode. If yes, then you have finished.

Step 3: If a device is set to CLI mode, select the row. The row should be highlighted.

Step 4: Select Change Mode>vManage mode. You will then be prompted to attach a template to the device.

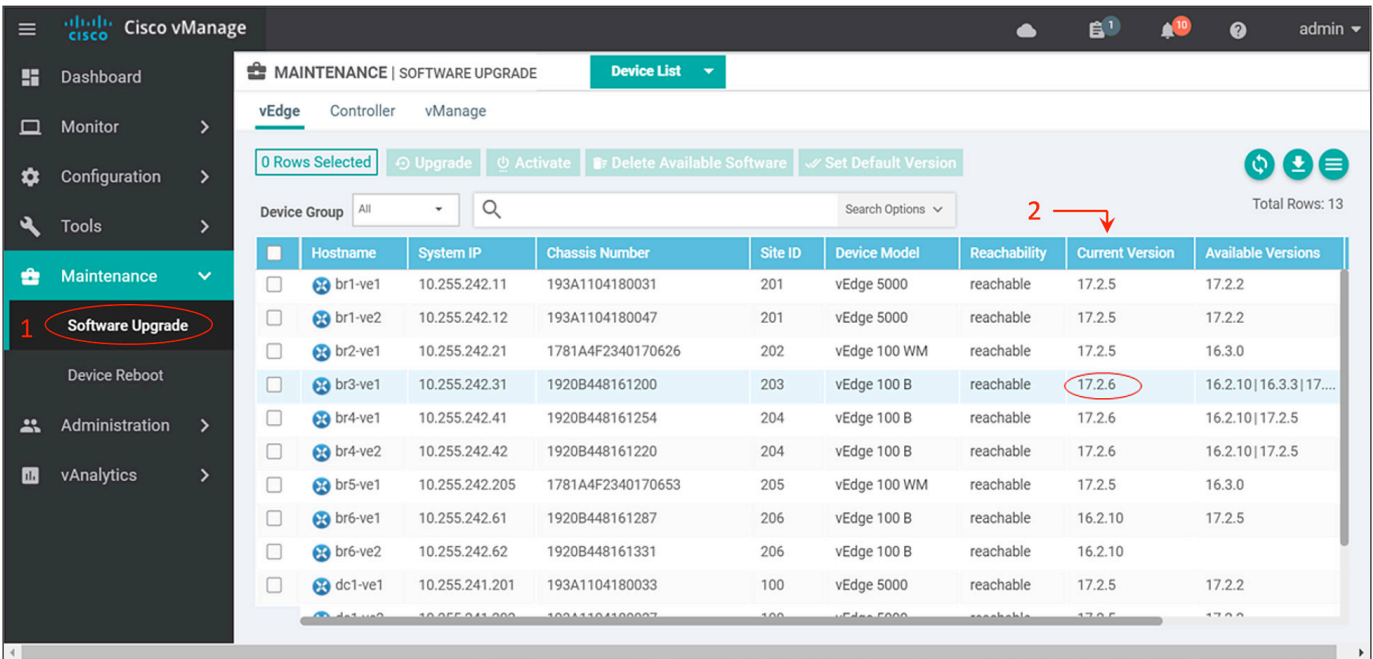
Step 5: Select the Template button, and you will be sent to the Configuration>Templates page, where you can attach a device to an existing template, or you can create new device/feature templates if desired.



Procedure 2 Verify the software version.

Step 1: Select Maintenance>Software Upgrade from the vManage GUI.

Step 2: Find the device and view the Current Version column. Upgrade if necessary.

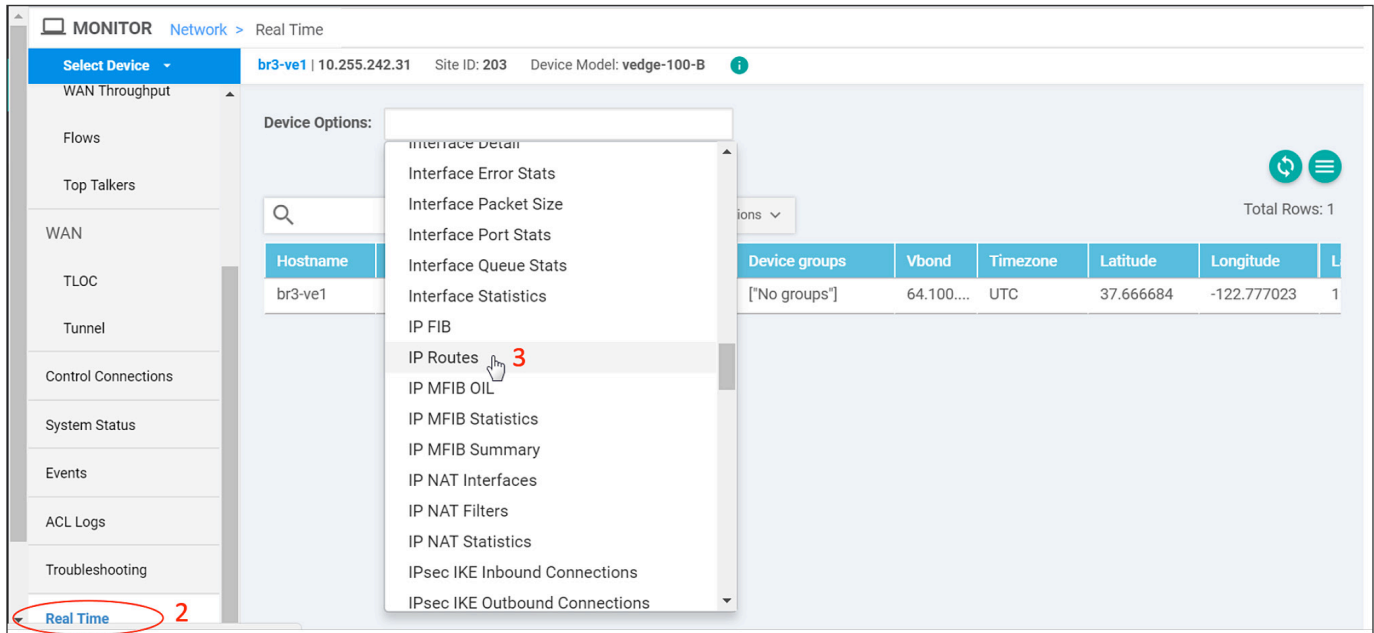


Procedure 3 Verify the default route to the Internet in the service VPN.

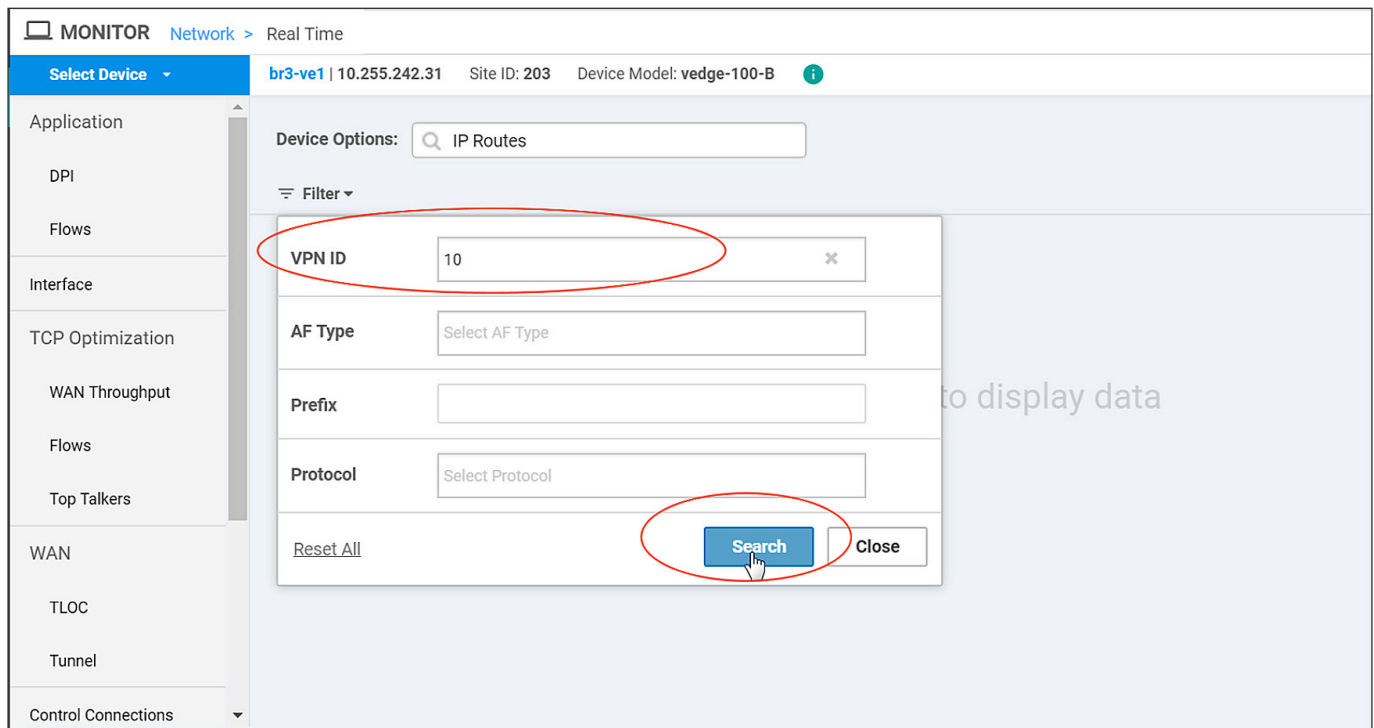
Step 1: Go to Monitor>Network from the vManage GUI and select the vEdge router of interest (br3-ve1).

Step 2: Select Real Time in the left column.

Step 3: In the Device Options textbox, select IP Routes from the drop-down menu.



Step 4: Select the Show Filters button from the popup window, and enter 10 in the box next to VPN ID, which is the service VPN in the example topology. Select the Search button.



Step 5: View the routing-table output.

Device Options:

Filter: VPN ID: 10

Search Options

VPN ID	AF Type	Prefix	Protocol	Next Hop If Name
10	ipv4	10.0.0.0/14	omp	--
10	ipv4	10.0.0.0/14	omp	--
10	ipv4	10.0.10.0/30	omp	--
10	ipv4	10.0.10.0/30	omp	--
10	ipv4	10.4.0.0/14	omp	--
10	ipv4	10.4.0.0/14	omp	--
10	ipv4	10.101.10.0/24	omp	--
10	ipv4	10.101.10.0/24	omp	--
10	ipv4	10.101.10.0/24	omp	--
10	ipv4	10.101.10.0/24	omp	--
10	ipv4	10.101.10.0/24	omp	--
10	ipv4	10.102.10.0/24	omp	--

The default route does not appear in the VPN10 routing table, so you need to perform additional troubleshooting to meet this prerequisite before configuring Cloud onRamp for SaaS.

Procedure 4

Verify NAT, DNS, and default route configuration for DIA and gateway sites.

To quickly verify the additional configurations required for Cloud onRamp for SaaS for DIA and gateway sites, you can review the running configuration of a vEdge router through vManage:

Step 1: Go to Configuration>Devices from the vManage GUI.

Step 2: Select the ... to the right of the desired vEdge device.

Step 3: Select Running Configuration, and a popup window will appear, displaying the running configuration.

Step 4: Check for the prerequisite configuration and move to the next procedures if additional configuration is necessary.

The screenshot displays two configuration windows from Cisco vManage. The left window shows the configuration for a VPN 0 interface (ge0/3), and the right window shows the configuration for another VPN 0 interface (ge0/4). Red annotations highlight specific configuration elements:

- Left Window (VPN 0 - ge0/3):**
 - DNS servers defined under VPN 0:** `dns 64.102.6.247 primary` and `dns 171.70.168.183 secondary`
 - NAT defined under interface under VPN 0:** `nat`
- Right Window (VPN 0 - ge0/4):**
 - NAT defined under interface under VPN 0:** `nat`
 - Default routes defined for local exit:** `ip route 0.0.0.0/0 64.100.103.17` and `ip route 0.0.0.0/0 144.254.103.17`

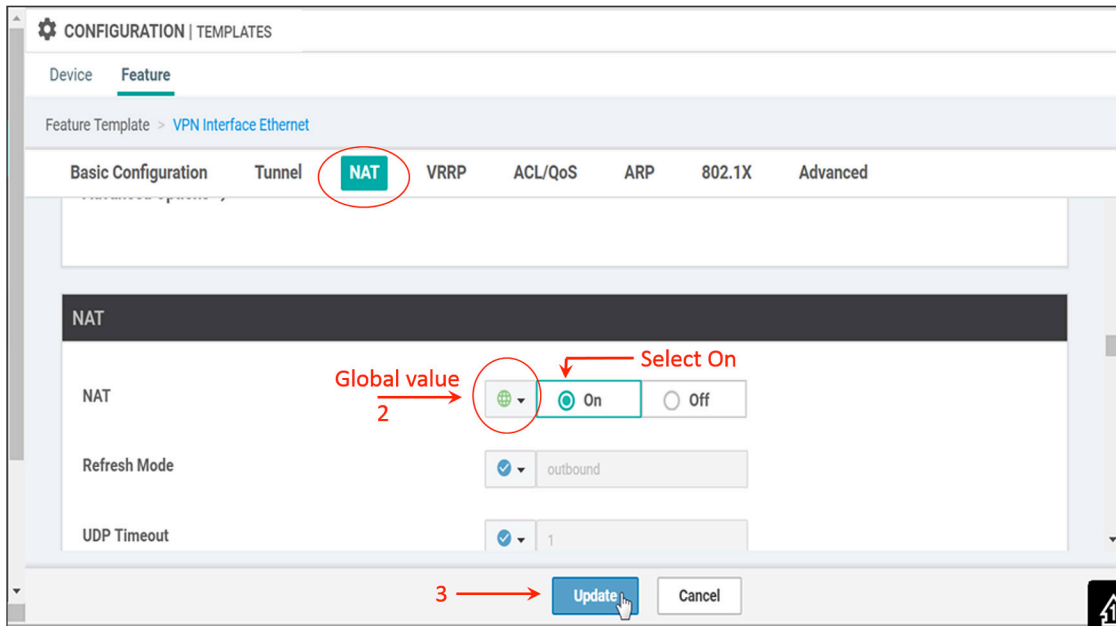
Procedure 5 Configure NAT on VPN 0 interfaces.

To configure NAT on the interfaces that will use SaaS applications directly from the Internet, you need to edit the configuration of each VPN interface feature template under VPN 0 from the applied device template. In the case of the Branch 3 vEdge router, you need to modify the **VPN0-Branch-Int1-SAAS** and **VPN0-Branch-Int2-SAAS** templates.

Step 1: Go to Configuration>Templates>Feature from the vManage GUI and highlight the desired template. Click the ... to the right of the template name and select Edit.

Step 2: Under the NAT section, select Global from the drop-down box and then select On. Because it is a Global value, this same value will be configured on all devices the template is applied to.

Step 3: Select Update to update the template.



Step 4: Next, push the updated configuration to the Branch 3 vEdge device. Select Next.

Step 5: Then select Configure Devices. If this feature template applies to more than one device, you will get a popup window alerting you that the changes will affect the configuration on multiple devices. Select the checkbox and click OK. The configuration push succeeds.

Step 6: Configure any additional interfaces that need NAT using the same procedures as outlined in steps 1 through 5.

Procedure 6 Configure the DNS server addresses.

To configure the DNS server addresses in the transport VPN, VPN 0, you need to modify the configuration of the VPN 0 feature template under the Transport and Management VPN section from the device template. In the case of the Branch 3 vEdge router, you need to modify the **VPN0-Branch-SAAS** template.

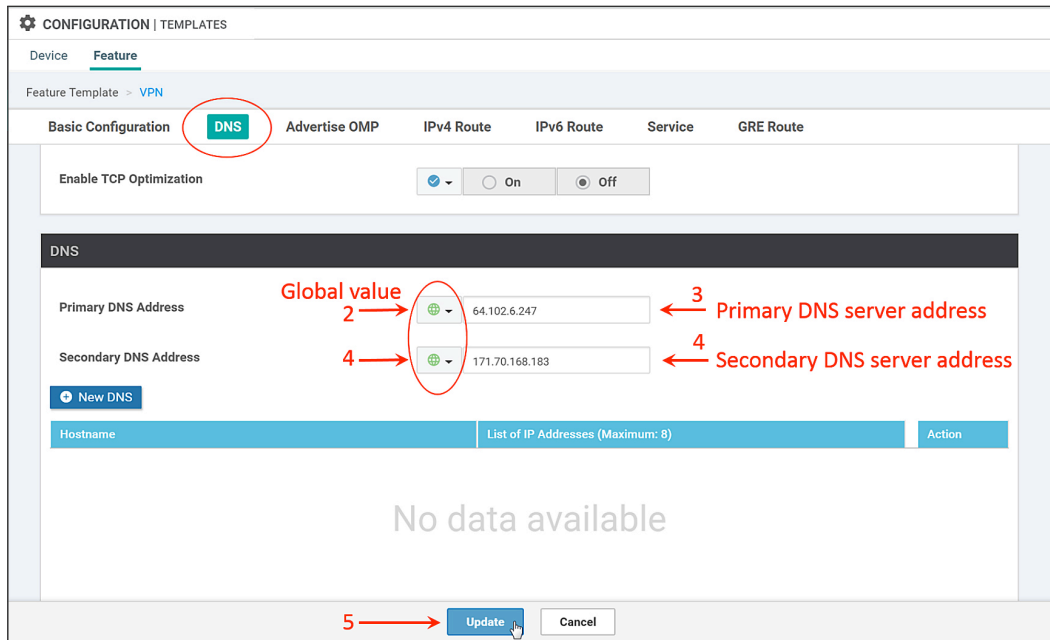
Step 1: Go to Configuration>Templates>Feature from the vManage GUI and highlight the desired template. Click the ... to the right of the template name and select Edit.

Step 2: Under the DNS section, choose the Global value from the drop-down box.

Step 3: Fill in the primary DNS server address in the Primary DNS Address textbox. A Secondary DNS Address textbox will appear.

Step 4: (Optional) If you need to configure a secondary DNS server, choose the Global value from the drop-down box and fill in the address in the Secondary DNS Address text box.

Step 5: Select Update to update the template. Because these values are marked as Global, they will be configured on all devices the template is applied to.



Step 6: Next, push the updated configuration to the Branch 3 vEdge device, and then select **Next**.

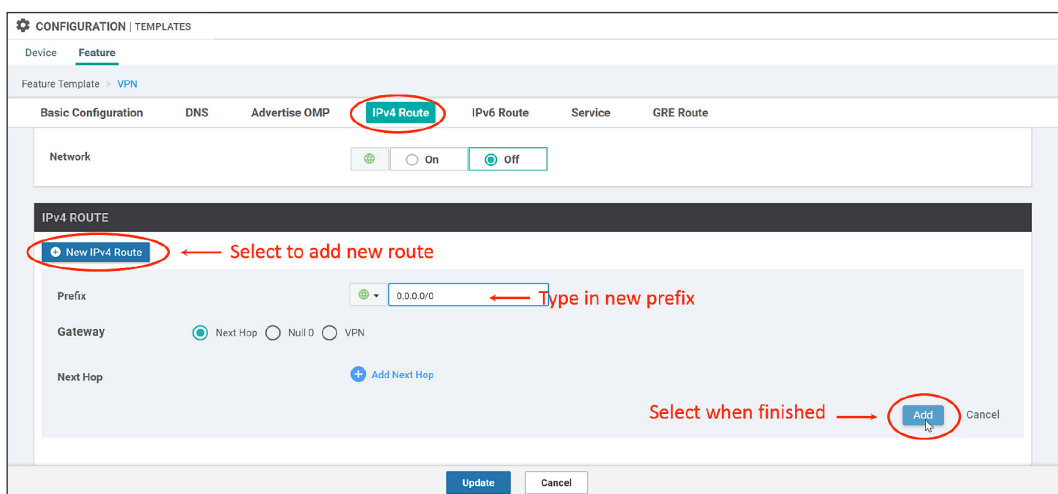
Step 7: Then select Configure Devices. If this feature template applies to more than one device, you will get a popup window alerting you that the changes will affect the configuration on multiple devices. Select the checkbox and click OK. The configuration push succeeds.

Procedure 7 Configure the default route for local exits.

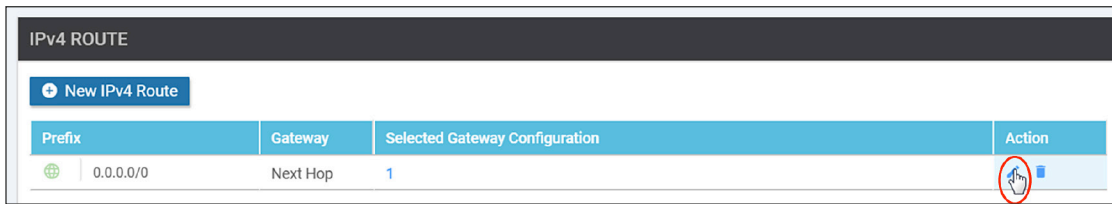
To define or modify a default route for the local exit, modify the feature template corresponding to the transport VPN, VPN 0. In the example given, the feature template is named **VPN0-Branch-SAAS**.

Step 1: Go to Configuration>Templates>Feature from the vManage GUI and highlight the desired template. Click the ... to the right of the template name and select Edit.

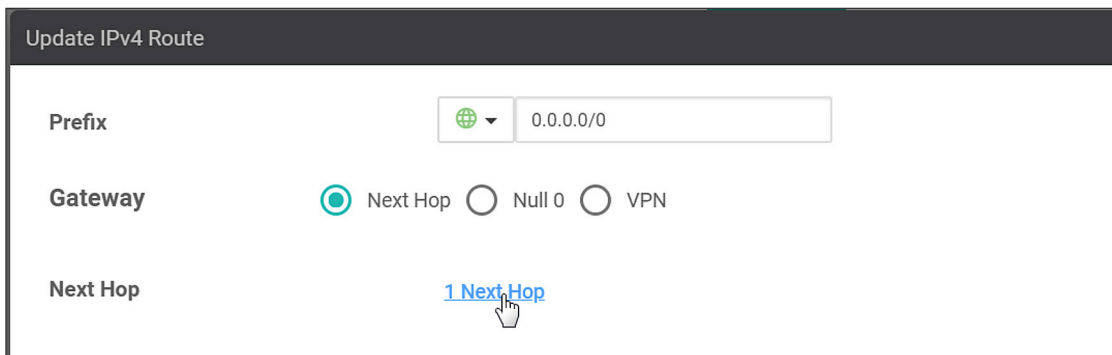
Step 2: If you are defining a new route, under IPv4 Route select the New IPv4 Route button, fill in the prefix **0.0.0.0/0** in the Prefix textbox, and then select Add. You still need to add next-hop information for this prefix (step 3).



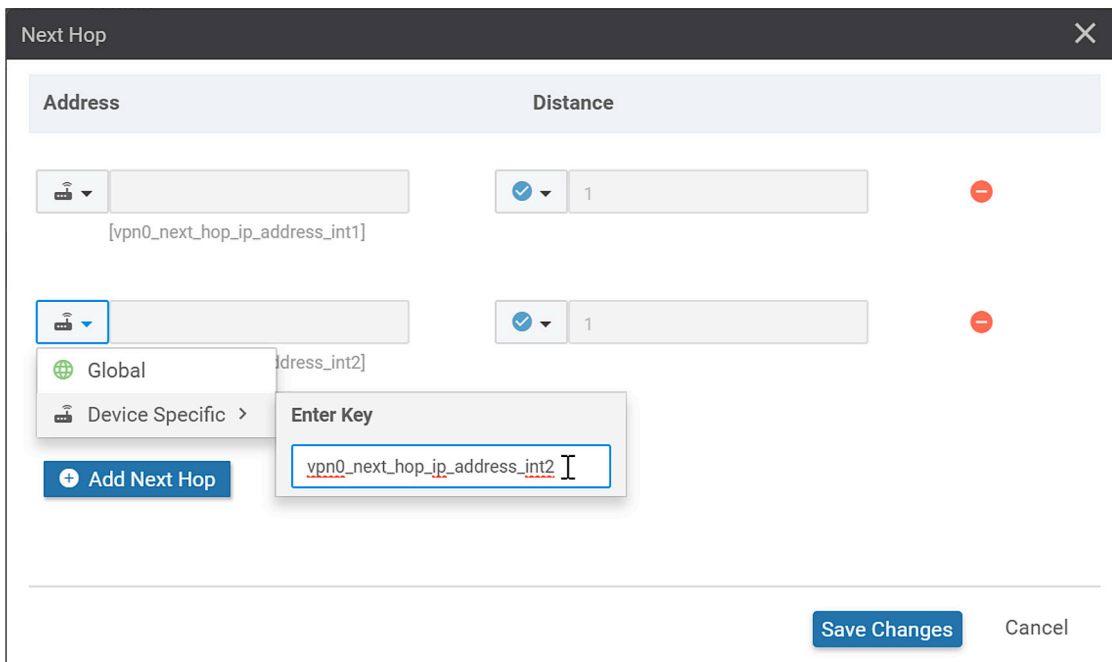
Step 3: To modify the default route next-hop information, select the edit symbol next to the existing prefix **0.0.0.0/0**.



Step 4: Select the Next Hop text to modify the next hops for this prefix (it will list the number of next hops configured}. If none are configured yet, the text will state Add Next Hop instead).



Step 5: In this example, one next hop is correctly configured, but a second one needs to be added. Select Add Next Hop, and then choose Device Specific in the drop-down menu in the new textbox and assign a variable to it, **vpn0_next_hop_ip_address_int2**, to allow the template to apply to multiple devices; you will be required to give a value to this variable before applying the configuration to a vEdge device. Click Save Changes.



Step 6: A popup window will appear for the prefix 0.0.0.0/0, indicating there are now two next hops configured. Select Save Changes.

Update IPv4 Route
✕

Prefix 🌐 0.0.0.0/0

Gateway Next Hop Null 0 VPN

Next Hop 2 Next Hop

Save Changes
Cancel

Step 7: Select Update to save the feature template.

Step 8: You then need to push out the added configuration to the vEdge router, but you first need to supply a value for the new variable that was created. Select ... to the far right and select Edit Device Template from the drop-down menu.

⚙️
CONFIGURATION | TEMPLATES

Device **Feature**

Device Template | [vEdge-Branch3-Template](#)

↑ ↓

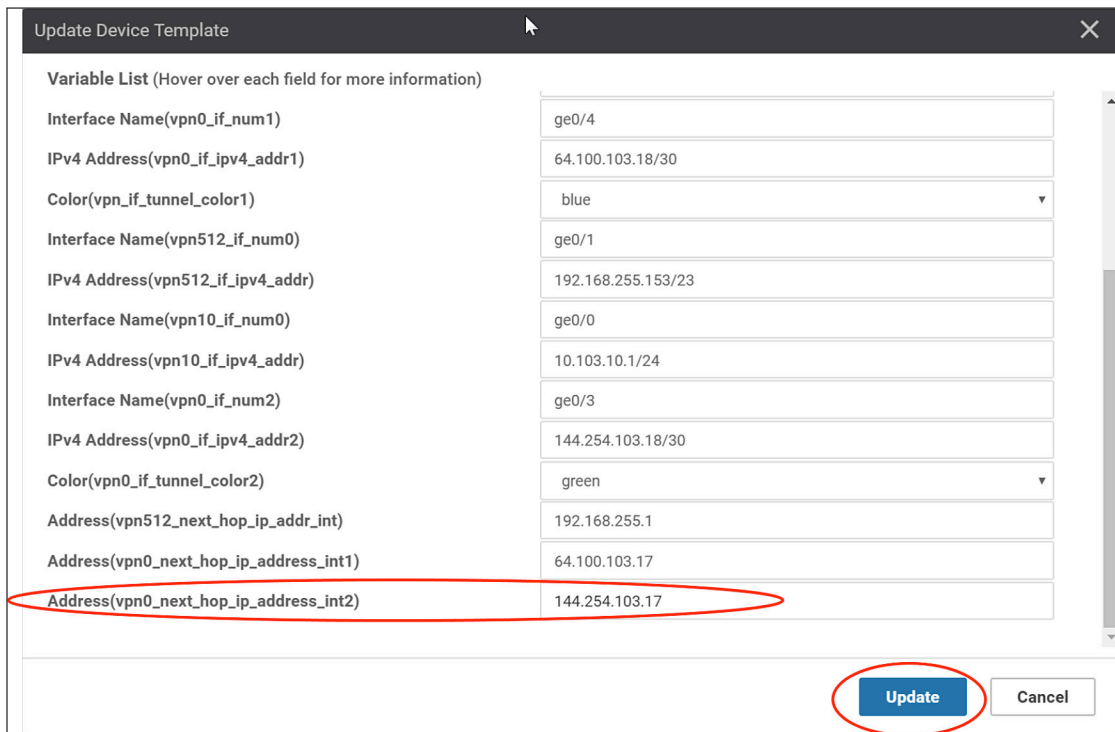
Search Options ▾

Total Rows: 1

S...	Chassis Number	System IP	Hostname	Hostname	System IP	Site ID	Address(v
✕	1920B448161200	10.255.242.31	br3-ve1	br3-ve1	10.255.242.31	203	10.103.0.1 ...

Edit Device Template

Step 9: Add the new next-hop information to the empty textbox and click Update.



Update Device Template

Variable List (Hover over each field for more information)

Interface Name(vpn0_if_num1)	ge0/4
IPv4 Address(vpn0_if_ipv4_addr1)	64.100.103.18/30
Color(vpn_if_tunnel_color1)	blue
Interface Name(vpn512_if_num0)	ge0/1
IPv4 Address(vpn512_if_ipv4_addr)	192.168.255.153/23
Interface Name(vpn10_if_num0)	ge0/0
IPv4 Address(vpn10_if_ipv4_addr)	10.103.10.1/24
Interface Name(vpn0_if_num2)	ge0/3
IPv4 Address(vpn0_if_ipv4_addr2)	144.254.103.18/30
Color(vpn0_if_tunnel_color2)	green
Address(vpn512_next_hop_ip_addr_int)	192.168.255.1
Address(vpn0_next_hop_ip_address_int1)	64.100.103.17
Address(vpn0_next_hop_ip_address_int2)	144.254.103.17

Update Cancel

Step 10: Repeat steps 8 and 9 for any other devices this template will apply to.

Step 11: Then select Next, and then Configure Devices. If this feature template applies to more than one device, you will get a popup window alerting you that the changes will affect the configuration on multiple devices. Select the checkbox and click OK to push the modified configuration out to any vEdge the template is attached to.

Refer to Appendix F for the CLI view of the configuration.

Cloud onRamp for SaaS Configuration

Enable cloud onRamp for SaaS

To enable the Cloud onRamp for SaaS feature, you must first enable it globally. Then the SaaS applications that will be used and monitored will be defined. After that, the various sites will be enabled (DIA, gateway, and client sites). You must complete the first two procedures before you can enable the sites; you can enable them in any order and in any combination.

If you define only DIA sites, then site users will use their local exits until the SaaS applications become unreachable or performance becomes unacceptable; at that point, the SaaS traffic will fall back to normal routing and follow the default route for Internet access.

If you define client sites, you must also define gateway sites so that the client-site traffic will have performance-monitored sites to use for Internet exits; otherwise this traffic will follow the normal default routed path.

If you define both gateway and DIA sites, the site users at a DIA site could use either the local exit or the gateway site for Internet access, depending on the performance of the application and path.

Procedure 1

Enable Cloud onRamp for SaaS globally (required)

The first task is to ensure that the feature is enabled globally. Note that this feature is still referenced by its former name, CloudExpress, in several places in the GUI.

Step 1: Using a web browser, navigate to the vManage web instance; for example:

<https://vmanage1.cisco.com:8443/>

Step 2: Select Administration>Settings. In the CloudExpress row, select Edit.

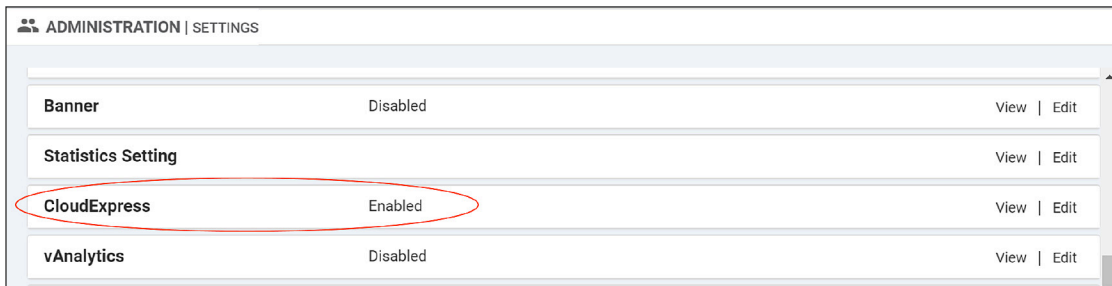
The screenshot shows the Cisco vManage Administration Settings page. The left sidebar is expanded to 'Administration' > 'Settings'. The main content area displays a table of settings. The 'CloudExpress' row is highlighted with a red oval, and the 'Edit' link in the 'View | Edit' column is also circled in red.

Setting Name	Value	Actions
Organization Name	ENB-Solutions - 21615	View
vBond	64.100.100.50 : 12346	View Edit
Certificate Authorization	Manual	View Edit
vEdge Cloud Certificate Authorization	Automated	View Edit
Web Server Certificate	04 Nov 2019 12:07:40 PM	CSR Certificate
Enforce Software Version (ZTP)	Disabled	View Edit
Banner	Disabled	View Edit
Statistics Setting		View Edit
CloudExpress	Disabled	View Edit
vAnalytics	Disabled	View Edit

Step 3: Click Enabled and press Save.



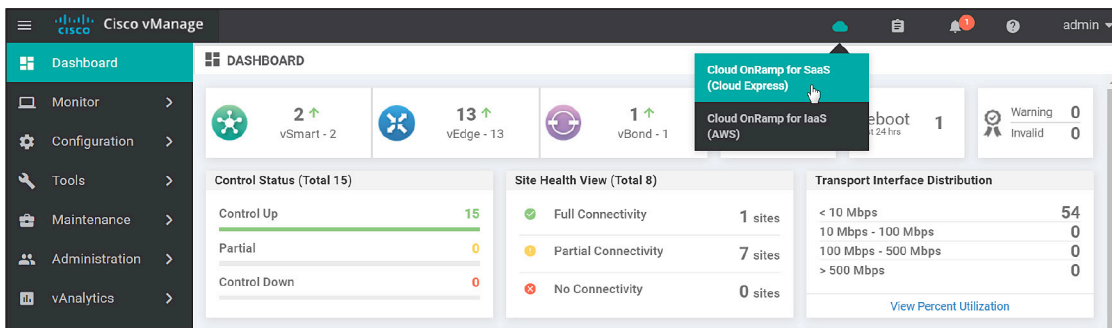
Step 4: Validate that CloudExpress is now enabled.



Procedure 2 Define the SaaS applications (required).

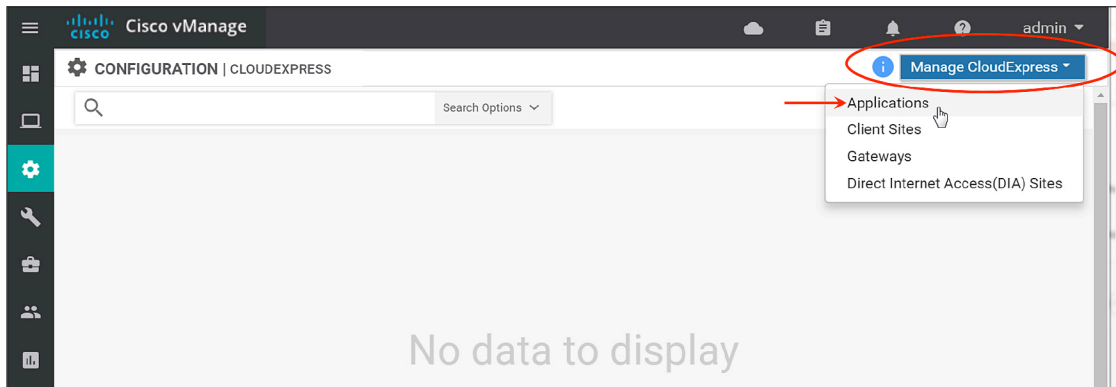
Step 1: To define the SaaS applications, first select the cloud icon at the top of the vManage GUI window, and select Cloud onRamp for SaaS (Cloud Express).

Alternatively, you can go to Configuration>CloudExpress from the menu on the left side of the GUI.



Step 2: A screen pops up that welcomes you to CloudExpress, states that CloudExpress has been enabled, and instructs you to add applications and VPNs, client sites, gateways, and DIA sites; it invites you to start using CloudExpress through the Dashboard. Click Dismiss.

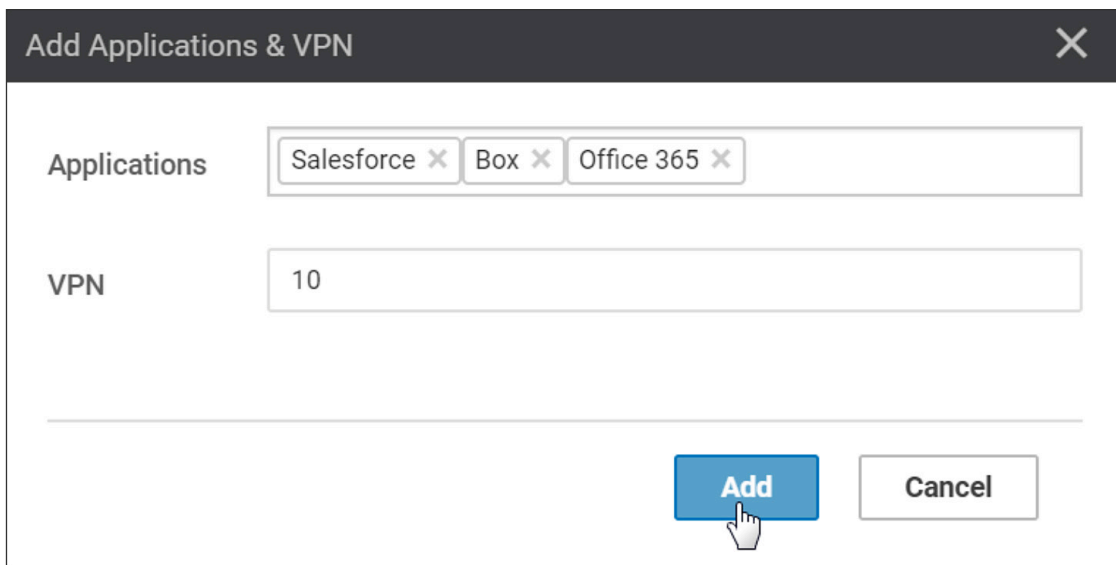
Step 3: Click the Manage CloudExpress drop-down menu and select Applications to enable the desired SaaS applications.



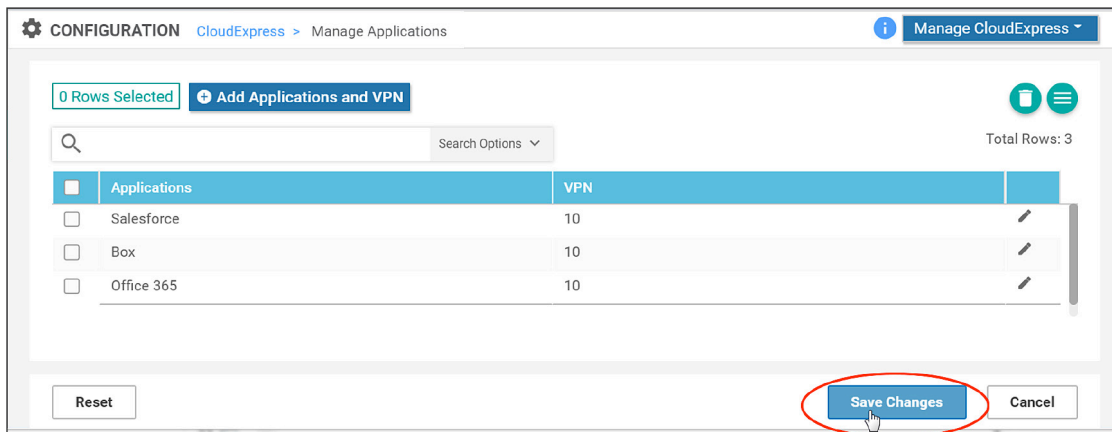
Because no applications have been previously configured, an Add Applications and VPN window pops up automatically. Click the Applications box and select an application (**Salesforce**) from the drop-down menu.

Step 4: Click the Applications box again and add any additional applications (**Box, Office 365**) from the drop-down menu.

Step 5: When you have finished, specify the service VPNs where users who will access the SaaS applications will reside. You can enter a VPN number, a list, a range, or a combination (example: **10,20,30-35**). If you use the example topology, type **10** in the VPN field and click Add.



Step 6: Select Save Changes.



Tech Tip

If you add any additional applications or VPNs, be sure to select the Save Changes button before moving to a different screen or you will lose your edits.

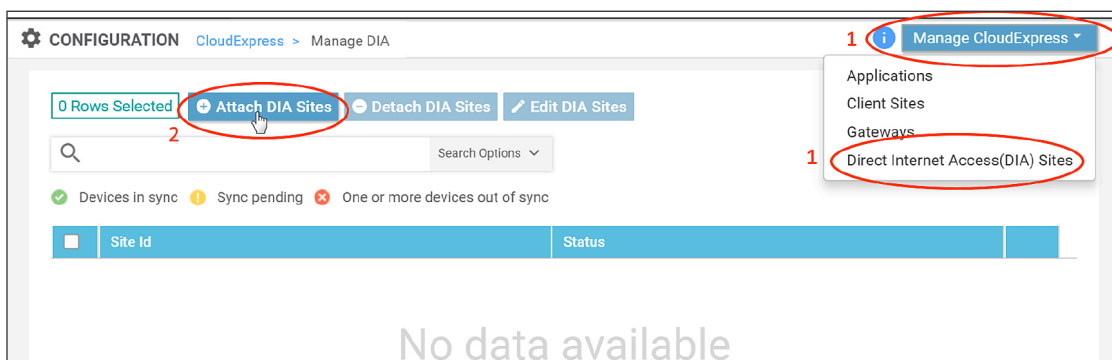
Procedure 3

Configure the DIA sites (optional)

Use the following steps to configure any DIA sites present in the network:

Step 1: To configure DIA sites, select Manage CloudExpress>Direct Internet Access (DIA) Sites in the drop-down menu.

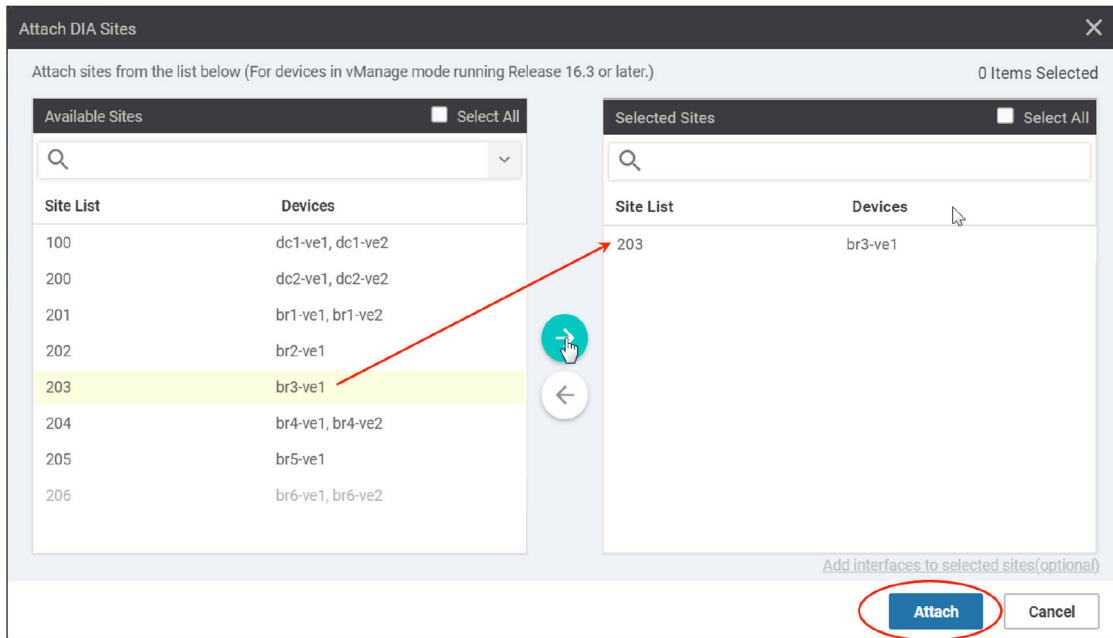
Step 2: Select Attach DIA Sites.



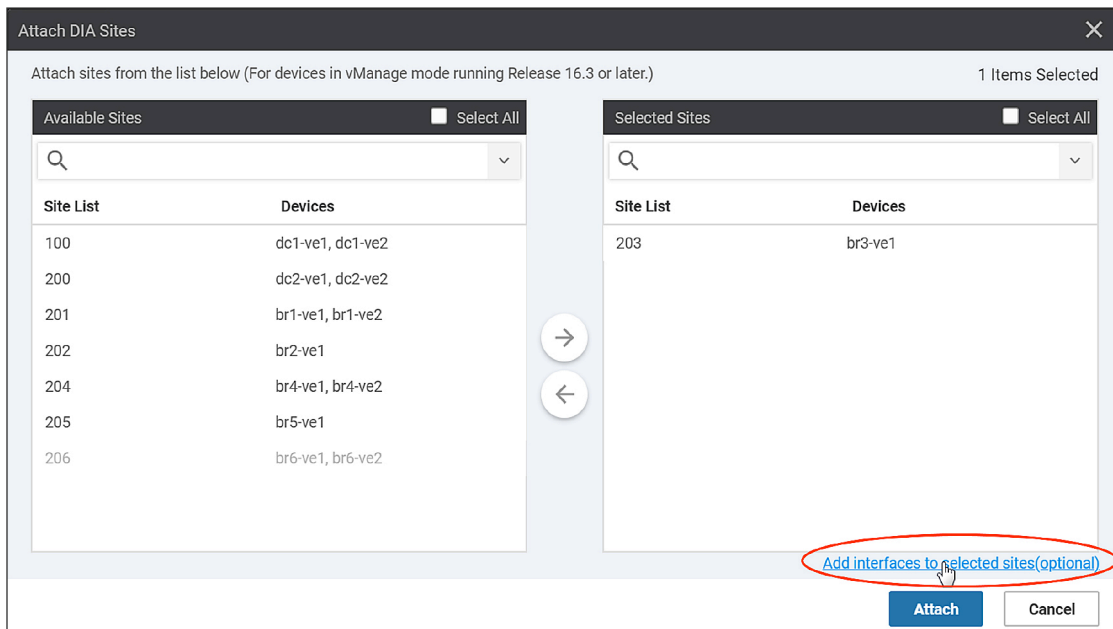
Step 3: A popup window will appear. Choose the direct-access sites by selecting the site and clicking the arrow to bring the selected site to the Selected Sites box.

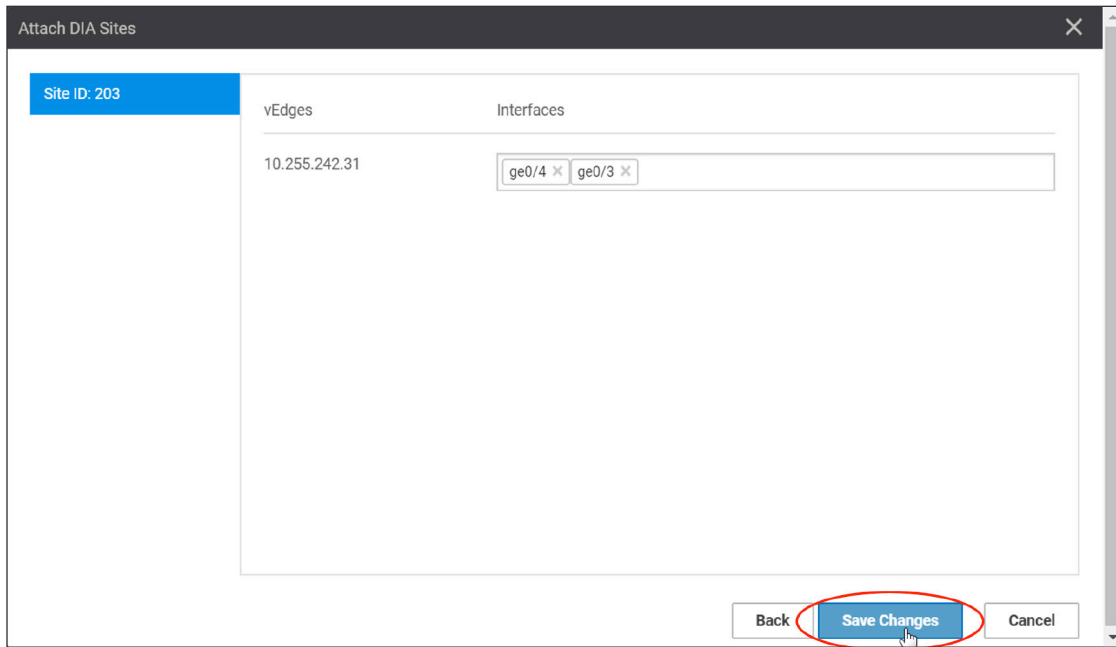
Step 4: By default, any interface in VPN 0 that has a NAT configuration is a candidate for local Internet exit. If you want to explicitly specify the interfaces to use for the local Internet exit, please skip to step 5. This configuration is useful when you want to exclude a candidate interface for SaaS access, such as in the case of an LTE interface, for instance.

Select Attach to complete the DIA site configuration. Then vManage inserts the Cloud onRamp for SaaS configuration into the full configuration vManage has stored and it then pushes the entire configuration to the vEdge router.



Step 5: (Optional) Select interfaces to use for local Internet exit. To configure, select Add Interfaces to selected sites (optional) at the bottom of the popup screen, and then select the vEdge interfaces in the textbox drop-down menu that you will use as direct exits for the SaaS applications. Select Save Changes.





After you save the changes, vManage inserts the Cloud onRamp for SaaS configuration into the full configuration vManage has stored and it then pushes the entire configuration to the selected vEdge routers.

Step 6: Verify that all configurations have been pushed out successfully. This process could take 30 seconds or longer.

vManage automatically switches to a screen that indicates the configurations are being built and then pushed out to the vEdge devices. It finishes by indicating success or failure.

TASK VIEW

Push Feature Template Configuration | ✔ Validation Success | Initiated By: admin | From: 192.168.255.200

Total Task: 1 | Success: 1

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
✔ Success	Done - Push Fe...	1920B448161200	vedge-100-B	br3-ve1	10.255.242.31	203	10.255.100.150

Refer to Appendix G to see the CLI-equivalent configuration that has been inserted and pushed.

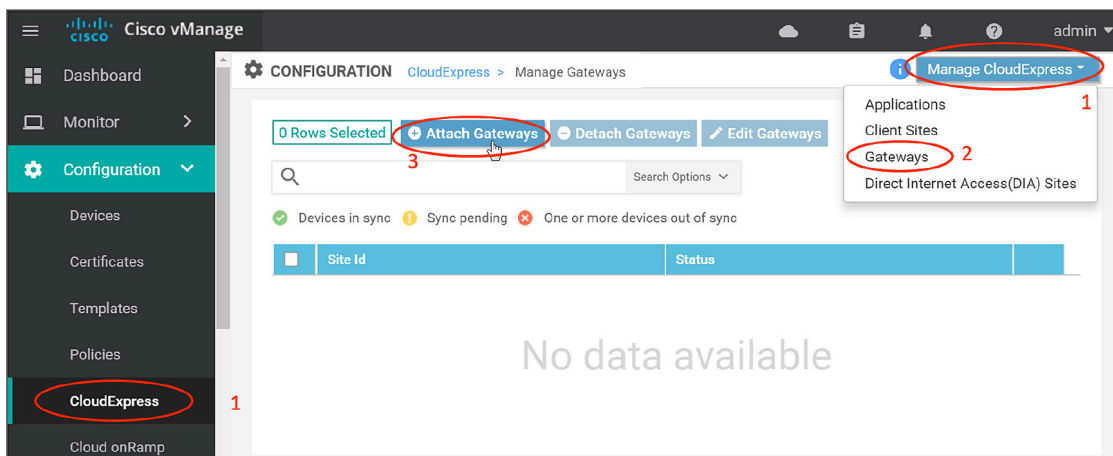
Procedure 4 Configure the gateway sites (optional)

Gateway sites are configured in a similar manner as DIA sites.

Step 1: To configure gateway sites, select Configuration>CloudExpress and select Manage CloudExpress.

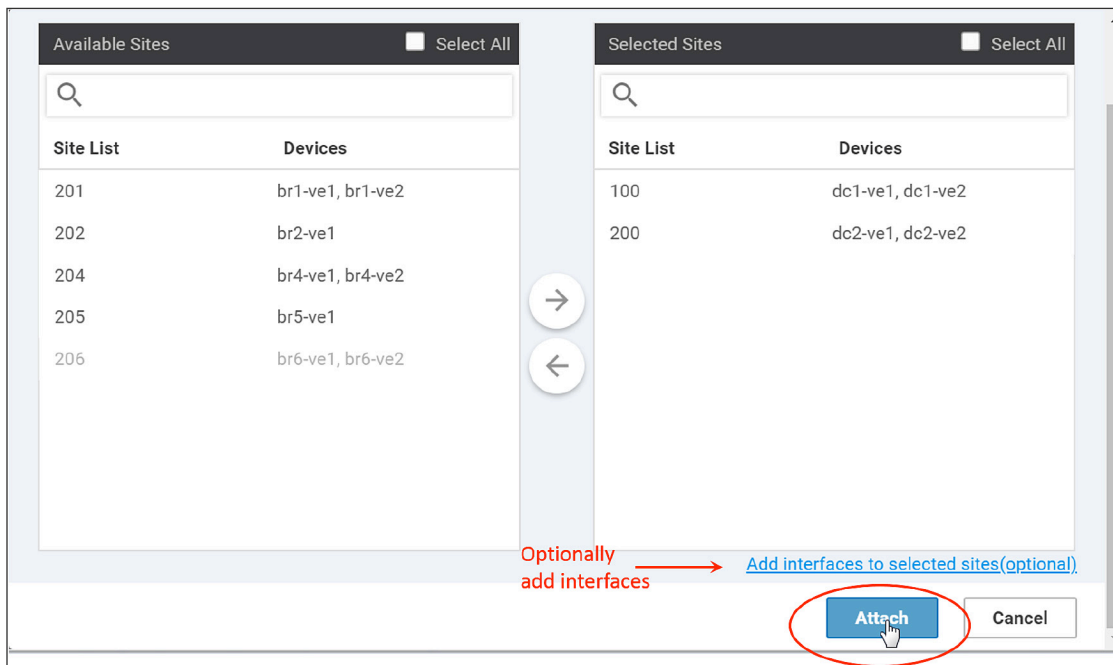
Step 2: Select **Gateways** from the drop-down menu.

Step 3: Select Attach Gateways.



Step 4: A popup window will appear. Choose the gateway sites by selecting the site and clicking the arrow to bring the selected sites to the Selected Sites box.

Step 5: If you want to specify explicitly the local exit interfaces used to access the SaaS applications, select Add Interfaces to selected sites (optional); otherwise, just select Attach.



vManage inserts the Cloud onRamp for SaaS configuration into the full configuration vManage has stored and it then pushes the entire configuration to the selected vEdge routers.

Step 6: Verify that all configurations have been pushed out successfully. This process could take 30 seconds or longer.

vManage automatically switches to a screen that indicates the configurations are being built and then pushed out to the vEdge devices. It finishes by indicating success or failure.

TASK VIEW

Push Feature Template Configuration | ✔ Validation Success - Initiated By: admin From: 192.168.255.200

Total Task: 4 | Success : 4

Search Options ▾ Total Rows: 4

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
✔ Success	Done - Push Fe...	193A1104180033	vedge-5000	dc1-ve1	10.255.241.201	100	10.255.100.150
✔ Success	Done - Push Fe...	193A1104180027	vedge-5000	dc1-ve2	10.255.241.202	100	10.255.100.150
✔ Success	Done - Push Fe...	110G403180418	vedge-1000	dc2-ve1	10.255.242.241	200	10.255.100.150
✔ Success	Done - Push Fe...	110G403180460	vedge-1000	dc2-ve2	10.255.242.242	200	10.255.100.150

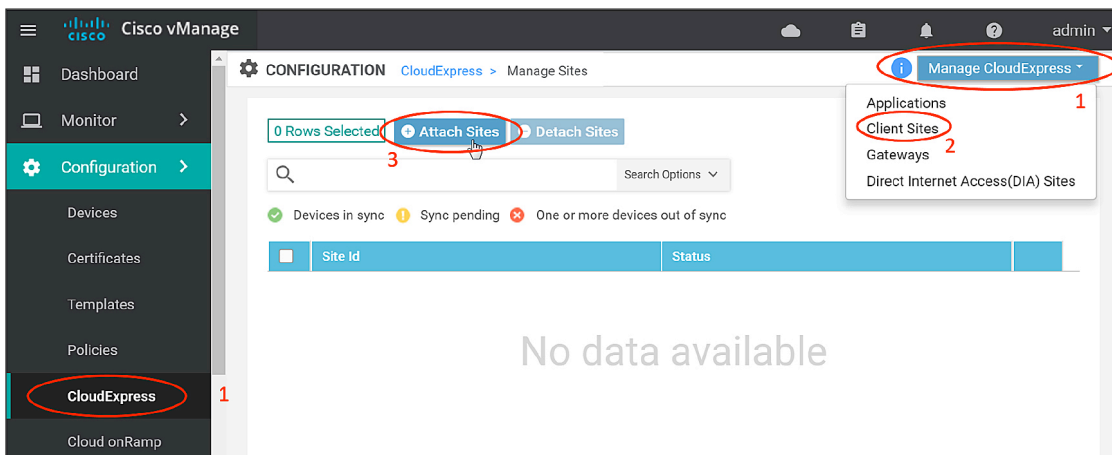
Procedure 5 Configure the client sites (optional)

Client sites are configured in a similar manner as DIA and gateway sites, except that you do not optionally select interfaces for local Internet exits because clients use gateways for their Internet access.

Step 1: To configure client sites, select Configuration>CloudExpress, and then select Manage CloudExpress.

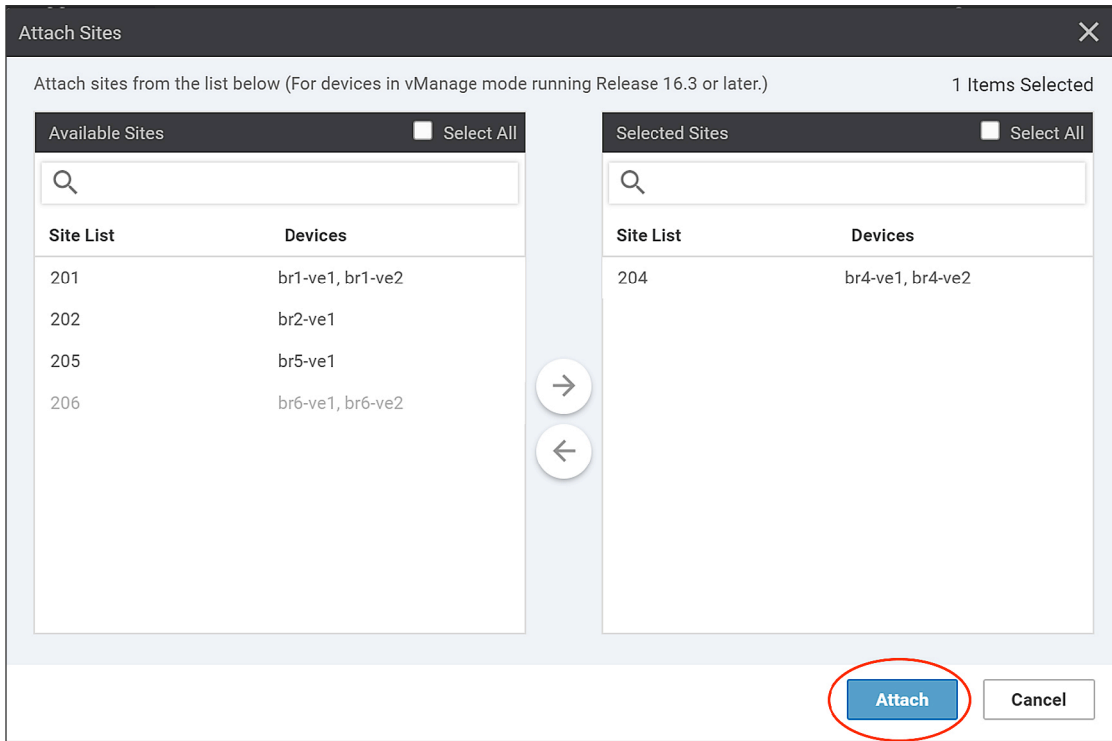
Step 2: Select Client Sites from the drop-down menu.

Step 3: Select Attach Sites.



Step 4: A popup window will appear. Choose the client sites by selecting the site and clicking the arrow to bring the selected site to the Selected Sites box.

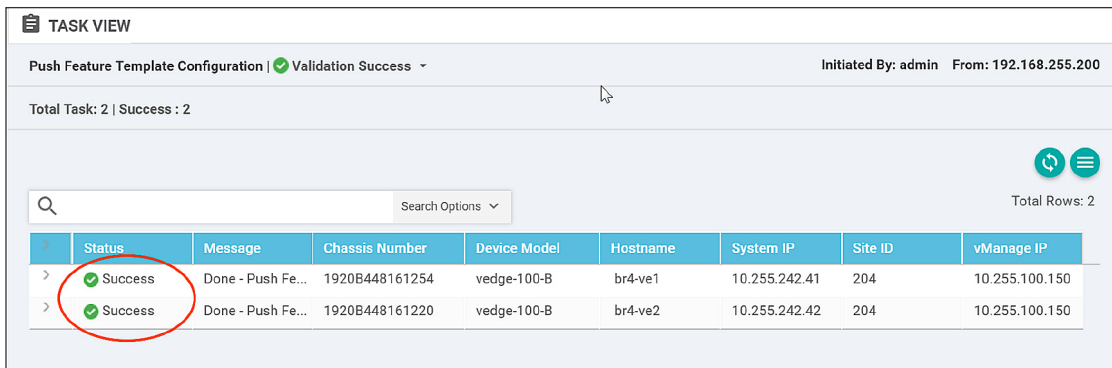
Step 5: Select Attach.



vManage inserts the Cloud onRamp for SaaS configuration into the full configuration vManage has stored and it then pushes the entire configuration to the selected vEdge routers.

Step 6: Verify that all configurations have been pushed out successfully. This process could take 30 seconds or longer.

vManage automatically switches to a screen that indicates the configurations are being built and then pushed out to the vEdge devices. It finishes by indicating success or failure.



Refer to Appendix G to see the CLI-equivalent configuration that has been inserted and pushed.

Tech Tip

After you define the applications and then enable DIA, gateway, or client sites, it could take up to 2 minutes to see the vQoE score move to a nonzero value.

Tech Tip

If you need to modify any site from one type to another, you first need to de-configure the site by selecting the site and selecting the Detach Sites button. The only exception is moving a vEdge router from a client site to a DIA site; you can move it directly without needing to first remove the configuration with the Detach Sites button.

Cloud onRamp for SaaS Monitoring

Monitor Cloud onRamp for SaaS

When you monitor Cloud onRamp for SaaS, you can view vQoE performance scores, view the network path selected for each application and site, and view the detailed loss and latency data for each application and path as well.

Procedure 1

View SaaS application vQoE scores and path selection

Step 1: Select the cloud icon at the top of the vManage GUI, and then select Cloud OnRamp for SaaS (CloudExpress). Alternatively, to get to this page, you can select Configuration>CloudExpress in the left column of vManage.

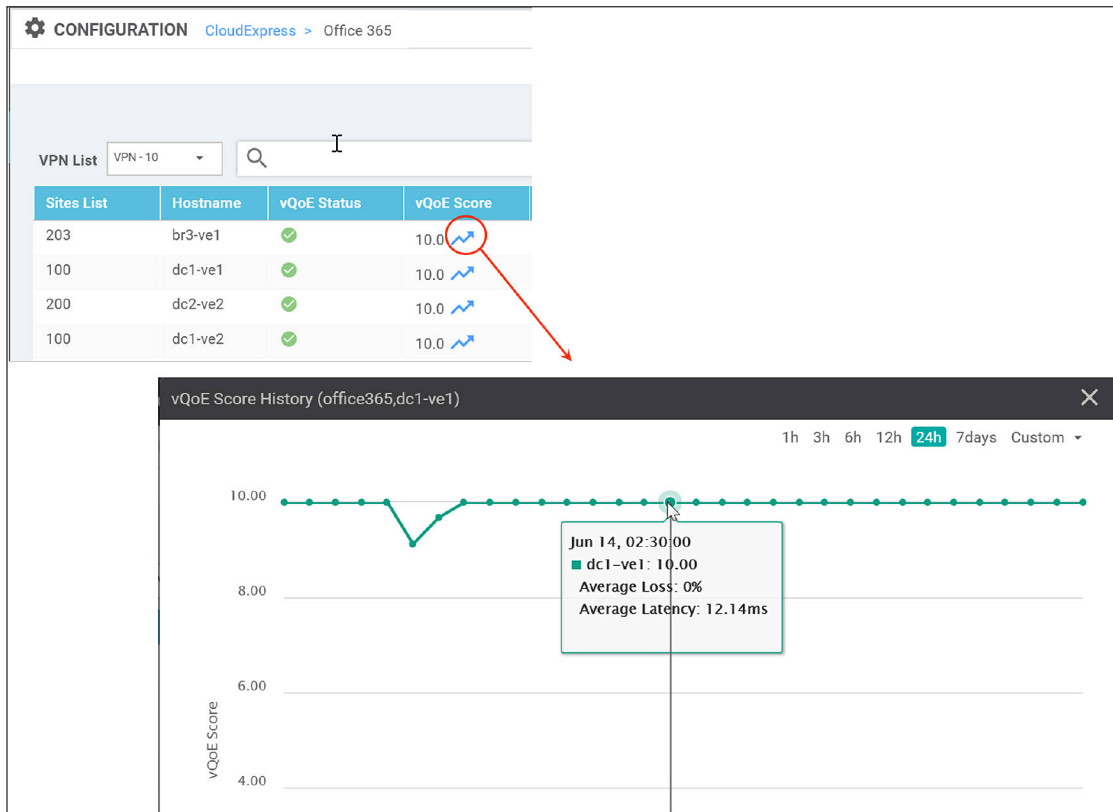
You will come to a page displaying each configured SaaS application as a widget. Each widget lists the number of active sites and vEdge devices that use that application, and the number of vEdge devices that show vQoE scores in the good, average, and bad range. Note that these vQoE scores are shown only for the best-performing path according to each vEdge device.

Step 2: From this page, select an application widget to get additional details about the vQoE scores and optimal paths selected. The resulting page will show the list of sites, the vEdge name, the vQoE status (a symbol indicating good, average, or bad), the vQoE number score, and the optimal path in use (local exit or gateway, selected local interface or system IP of the gateway, and an indication of the IPsec tunnel transports used to reach the remote gateway).

The screenshot shows the vManage GUI for CloudExpress configuration. The top section displays three widgets for Salesforce, Office 365, and Box. The Office 365 widget is circled in red, and a red arrow points to a detailed view of the Office 365 configuration. This detailed view shows a table of sites with columns for Sites List, Hostname, vQoE Status, vQoE Score, DIA Status, Selected Interface, Activated Gateway, Local Color, and Remote Color.

Sites List	Hostname	vQoE Status	vQoE Score	DIA Status	Selected Interface	Activated Gateway	Local Color	Remote Color
203	br3-ve1	Good	10.0	local	ge0/3	N/A	N/A	N/A
100	dc1-ve1	Good	10.0	local	ge0/3	N/A	N/A	N/A
200	dc2-ve2	Good	10.0	local	ge0/3	N/A	N/A	N/A
100	dc1-ve2	Good	10.0	local	ge0/4	N/A	N/A	N/A
200	dc2-ve1	Good	10.0	local	ge0/3	N/A	N/A	N/A
204	br4-ve2	Good	10.0	gateway	N/A	10.255.241.201	green	green
204	br4-ve1	Good	10.0	gateway	N/A	10.255.241.201	green	green

Step 3: If you select an arrow under the vQoE score column, a window will pop up to show the vQoE score history on a graph. You can see a 1-, 3-, 6-, 12-, or 24-hour; 7-day; or custom view of this data.



Procedure 2

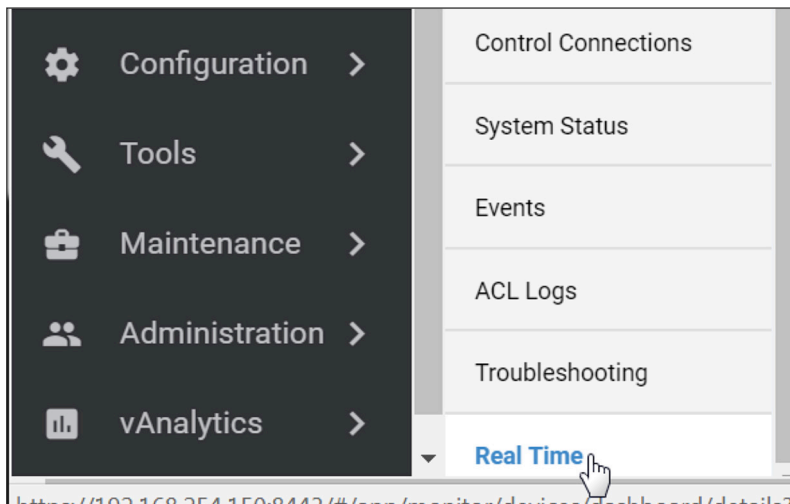
View detailed loss and latency data

Step 1: If you want to see detailed loss and latency data and additional detailed output from a particular vEdge device, navigate to Monitor>Network and then choose the device (br3-ve1).

The screenshot shows the Cisco vManage interface. The left sidebar has 'Monitor' selected. The main panel is titled 'MONITOR | NETWORK' and shows a table of network devices. A hand cursor is pointing to the 'br3-ve1' device in the table.

Hostname	State	System IP	Reachability
br1-ve1	✓	10.255.242.11	reachable
br1-ve2	✓	10.255.242.12	reachable
br2-ve1	✓	10.255.242.21	reachable
br3-ve1	✓	10.255.242.31	reachable
br4-ve1	✓	10.255.242.41	reachable

Step 2: On the left side of the main screen, scroll down to the bottom and then select Real Time.



Step 3: In the Device Options box, select any one of the following device options from the drop-down menu (CloudExpress Applications, CloudExpress Gateway Exits, CloudExpress Local Exits, and OMP CloudExpress Routes). When the Select Filter box pops up, select Do Not Filter.

Option 1. CloudExpress Applications

The CloudExpress option shows each application, the optimal path that has been chosen, and the mean latency and loss associated with the application for each optimal path.

br3-ve1 | 10.255.242.31 Site ID: 203 Device Model: vedge-100-B

Device Options:

Filter ↕ ↻ ☰

Search Options ▾ Total Rows: 3

VPN ID	Application	Exit Type	Gateway System IP	Interface	Mean Latency	Mean Loss
10	salesforce	gateway	10.255.241.201	N/A	45	22
10	office365	local	N/A	ge0/3	13	0
10	box_net	local	N/A	ge0/3	8	0

Option 2. CloudExpress Gateway Exits

This output shows each application, what the gateway exits are, and the mean latency and loss associated with the application for each gateway path available. It also indicates the tunnel transport that is taken to reach the gateway site (local color/remote color columns).

br3-ve1 | 10.255.242.31 Site ID: 203 Device Model: vedge-100-B

Device Options:

Filter ↕ ↻ ☰

Search Options ▾ Total Rows: 12

VPN ID	Application	Gateway IP	Mean Latency	Mean Loss	Local Color	Remote Color
10	salesforce	10.255.241.201	40	44	green	green
10	salesforce	10.255.241.202	40	50	green	green
10	salesforce	10.255.242.241	45	38	green	green
10	salesforce	10.255.242.242	41	23	green	green
10	office365	10.255.241.201	12	0	green	green
10	office365	10.255.241.202	12	0	green	green

Option 3. CloudExpress Local Exits

This output shows each application and the mean latency and loss associated with each of its local Internet exits.

br3-ve1 | 10.255.242.31 Site ID: 203 Device Model: vedge-100-B

Device Options:

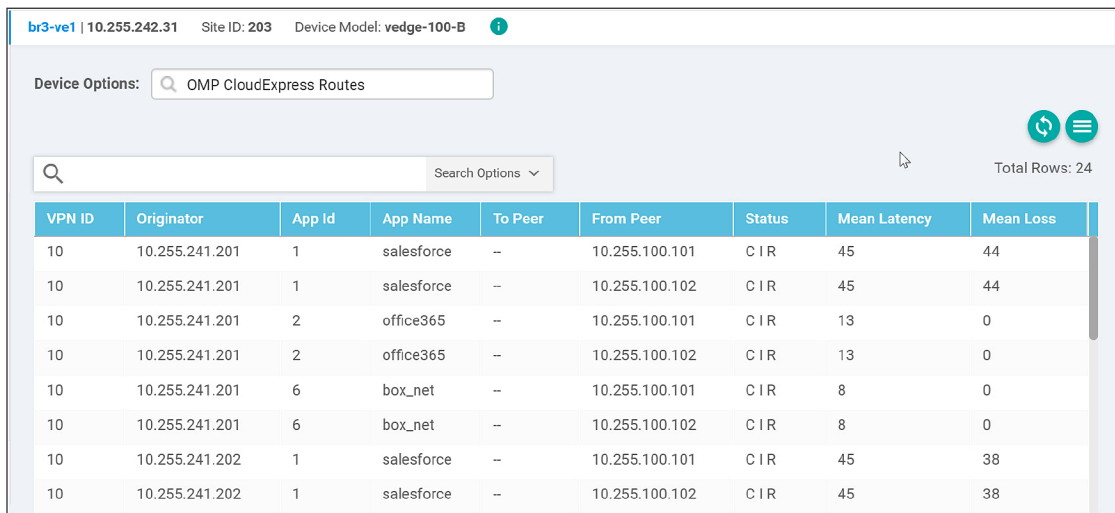
Filter ↕ ↻ ☰

Search Options ▾ Total Rows: 6

VPN ID	Application	Interface	Mean Latency	Mean Loss	Last Updated
10	salesforce	ge0/3	45	56	14 Jun 2018 1:30:48 P
10	salesforce	ge0/4	45	44	14 Jun 2018 1:30:48 P
10	office365	ge0/3	13	0	14 Jun 2018 1:30:48 P
10	office365	ge0/4	13	0	14 Jun 2018 1:30:48 P
10	box_net	ge0/3	10	0	14 Jun 2018 1:30:48 P
10	box_net	ge0/4	8	0	14 Jun 2018 1:30:48 P

Option 4. OMP CloudExpress Routes

This output shows the OMP routes received from the various gateways and the mean latency and loss associated with the applications and paths originating from them.



Device Options:

Search Options Total Rows: 24

VPN ID	Originator	App id	App Name	To Peer	From Peer	Status	Mean Latency	Mean Loss
10	10.255.241.201	1	salesforce	--	10.255.100.101	C I R	45	44
10	10.255.241.201	1	salesforce	--	10.255.100.102	C I R	45	44
10	10.255.241.201	2	office365	--	10.255.100.101	C I R	13	0
10	10.255.241.201	2	office365	--	10.255.100.102	C I R	13	0
10	10.255.241.201	6	box_net	--	10.255.100.101	C I R	8	0
10	10.255.241.201	6	box_net	--	10.255.100.102	C I R	8	0
10	10.255.241.202	1	salesforce	--	10.255.100.101	C I R	45	38
10	10.255.241.202	1	salesforce	--	10.255.100.102	C I R	45	38

Refer to Appendix H for equivalent CLI show commands for monitoring.

Appendices

Appendix A: Product list

Table A1 lists the products and versions that were included as part of the validation in this deployment guide.

Table A1. Products and versions used in validation

Location	Product	Cisco IOS Software version
Cloud	vManage	17.2.6
Cloud	Cisco vSmart Controller	17.2.6
Cloud	Cisco vBond Orchestrator	17.2.6
Data center	Cisco vEdge 5000 Series Routers	17.2.6
Data center	Cisco vEdge 1000 Series Routers	17.2.6
Branch office	Cisco vEdge 100 Series Routers	17.2.6

Appendix B: Cisco SD-WAN solution overview

The Cloud OnRamp for SaaS feature is enabled on top of a functional SD-WAN network. Understanding how this SD-WAN solution works at a high level will provide context in order to further understand the feature and configuration.

Components

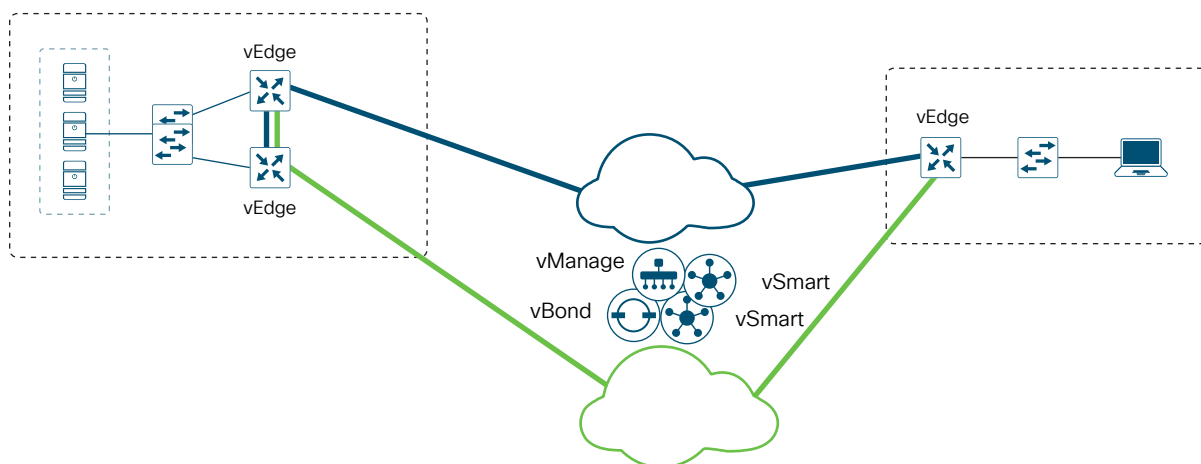
The primary components for the Cisco SD-WAN solution consist of the following:

- Cisco vManage: This centralized network management system provides a GUI interface to easily monitor, configure, and maintain all Cisco SD-WAN devices and links in the underlay and overlay network.
- Cisco vEdge router: This hardware appliance or software-based router sits at a physical site or in the cloud and provides connectivity among the sites over one or more WAN transports. It is responsible for traffic forwarding, security, encryption, quality of service (QoS), routing protocols (Border Gateway Protocol [BGP] and Open Shortest Path First [OSPF]), and more.
- Cisco vSmart Controller: This software-based component is responsible for the centralized control plane of the SD-WAN network. It establishes a secure connection to each vEdge router and distributes routes and policy information via the Overlay Management Protocol (OMP). The policies it provides can manipulate routes, access control, segmentation, and service chaining.
- Cisco vBond Orchestrator: This software-based component performs the initial authentication of vEdge devices and orchestrates vSmart and vEdge connectivity.

Topology

Figure B1 demonstrates several aspects of the Cisco SD-WAN solution.

Figure B1. Cisco SD-WAN topology



This topology depicts two sites and two public Internet transports. The SD-WAN controllers, vSmart controllers, and vBond orchestrator, along with the vManage management GUI that resides on the Internet are reachable through either transport.

At each site, vEdge routers are used to directly connect to the available transports. At the site that depicts two vEdge routers are cross-links between the vEdge routers so that each vEdge router can connect directly to

one transport, and also has access to the opposite transport. The ability for a vEdge router to use an indirectly connected transport is called Transport Location-extension (TLOC-extension). A TLOC is the physical point where a vEdge router connects into a transport network. It is identified uniquely by IP address, link color, and encapsulation (generic routing encapsulation [GRE] or IP Security [IPSec]). Color identifies an individual WAN transport; different WAN transports are assigned different colors (options include 3g, biz-internet, blue, bronze, custom1, custom2, gold, green, lte, mpls, etc.).

The vEdge routers form a Datagram Transport Layer Security (DTLS) control connection to the vSmart controllers and, by default, connect to two vSmart controllers over each transport. The vEdge routers securely connect to vEdge routers with IPsec tunnels at other sites over each transport. The Bidirectional Forwarding Detection (BFD) protocol is enabled by default; it runs over each of these tunnels, detecting loss, latency, jitter, and path failures.

In addition, the OMP routing protocol runs between the vSmart controllers and vEdge routers where control-plane information, such as routes and policies, is exchanged. The routes are advertised, using next hops that are reachable over the IPsec tunnels. No policies are configured in this base network, so the default behavior is a full-mesh topology, where each vEdge router can connect directly to a vEdge router at another site and receive full routing information from each site.

VPNs

In the SD-WAN overlay, VPNs provide segmentation, much like Virtual Route Forwarding instances (VRFs) that many are already familiar with. By default, two VPNs are present by default in the vEdge devices and controllers, VPN 0 and VPN 512.

- VPN 0 is the transport VPN. It contains the interfaces that connect to the WAN transports. Secure DTLS/TLS connections to the vSmart controllers or between vSmart controllers and vBond orchestrators are initiated from this VPN. You need to configure static or default routes or a dynamic routing protocol inside this VPN to get appropriate next-hop information so the control plane can be established and IPsec tunnels can connect to remote sites.
- VPN 512 is the management VPN. It carries the out-of-band management traffic to/from the Cisco SD-WAN devices.

In addition to the default VPNs that are already defined, you need to create one or more service-side VPNs that contain interfaces that will connect to the local-site network and carry user data traffic. You can enable these VPNs for features such as OSPF, BGP, Virtual Router Redundancy Protocol (VRRP), QoS, and traffic shaping or policing. You can direct user traffic over the IPsec tunnels to other sites by redistributing OMP routes received from the vSmart controllers at the site into the service-side VPN routing protocol. In turn, you can advertise routes from the local site to other sites by advertising the service VPN routes into the OMP routing protocol that is sent to the vSmart controllers and redistributed to the other vEdge routers in the network.

Device templates

Configurations and policies apply to vEdge routers and vSmart devices that enable traffic to flow between the data center and the branch office or between branch offices. An administrator can enable configurations and policies through the command-line interface (CLI) using console or Secure Shell (SSH) Protocol on the vEdge device or remotely through the vManage GUI.

To configure a vEdge device on the network using the vManage GUI, an administrator applies a device template to a vEdge or multiple vEdge devices. These templates can be CLI-based or feature-based. Although you can create CLI-based templates, we recommend feature-based templates because they are modular, more scalable, and less error-prone. Each device template is made up of several feature templates, such as authentication,

authorization, and accounting (AAA), security, and Network Time Protocol (NTP); and templates that describe the interface configurations, tunnel configurations, and local routing behavior.

The administrator uses vManage to configure device and feature templates, specifying variables where needed because templates can apply to multiple vEdge devices that have unique settings. The administrator fills in the values for the variables for each vEdge router the template will apply to, either through the vManage GUI directly or through a .csv file that can be uploaded. vManage then modifies the configuration of the targeted vEdge device in the database and pushes out the entire configuration to the intended vEdge device sitting on the network.

Policies

Policies are an important part of the Cisco SD-WAN solution; they are used to influence the flow of data traffic among the vEdge routers in the overlay network. Policies apply either to control- or data-plane traffic and are configured either centrally on vSmart controllers or locally on vEdge routers.

Control policies operate on the routing information and allow for customizing routing decisions and determining routing paths through the overlay network. You can use control policies when configuring traffic engineering, path affinity, and different types of VPN topologies (full-mesh, hub-and-spoke, etc.).

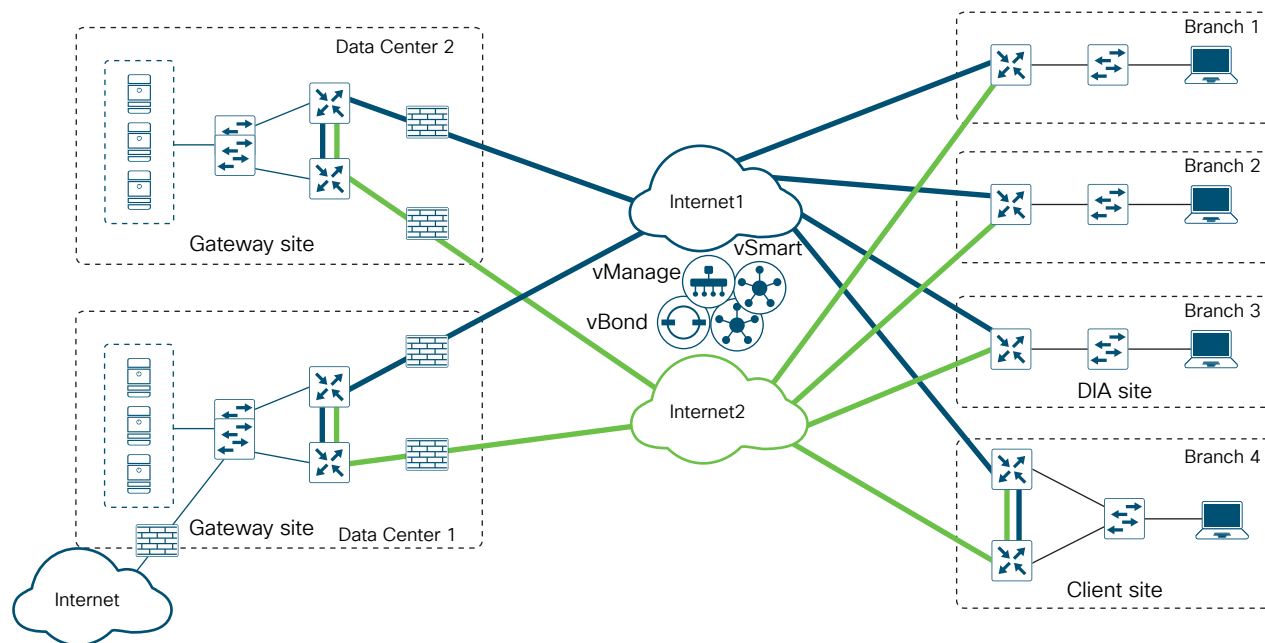
Data policies influence the flow of data traffic through the network based on fields in the IP packet headers and VPN membership. You can use data policies when configuring service chaining and traffic policing.

There are also policies for application-aware routing, which selects the optimal path based on real-time path performance characteristics for different traffic types, and for cflowd, which is used for monitoring traffic flows.

Appendix C: Cloud onRamp example topology

Figure C1 shows an example topology used to demonstrate the Cloud onRamp SaaS configuration and monitoring.

Figure C1. Example topology for Cloud onRamp for SaaS configuration



In this topology, there are two data centers and four remote sites. The transports shown are two public Internet providers, labeled Internet1 and Internet2. The SD-WAN controllers, the vSmart controllers, and the vBond orchestrator, along with the vManage management GUI that reside in the cloud are reachable through either public transport.

In Branches 1–3, one vEdge router is depicted at each site with direct connections to both transports. In each of the data centers and in Branch 4, two vEdge routers are depicted, each with one direct connection to one of the transport providers. These sites have TLOC-extension links between the vEdge routers to give each vEdge router access to both transports. In Data center 1, Internet access is through a separate connection off a network distribution block that already exists before Cloud onRamp is enabled.

The Data centers and Branches 3 and 4 are each configured with a basic device template. The template defines the interfaces in the transport and service VPN. It also defines the properties of the Open Shortest Path First (OSPF) routing protocol in the service transport, which is VPN 10 at each site. The basic configuration allows for traffic to flow from site to site. No policies are defined for the network.

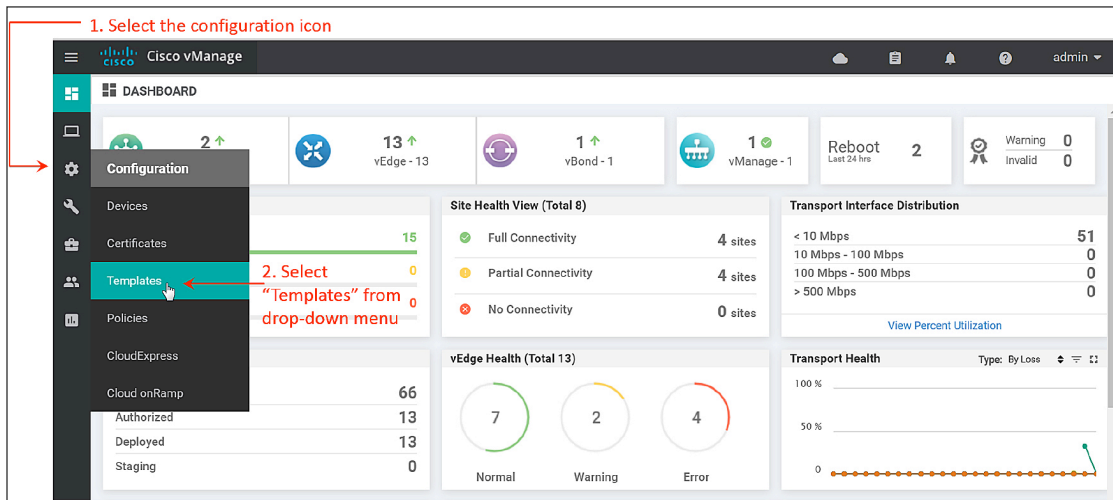
For the Cloud onRamp for SaaS configurations, Data Centers 1 and 2 are configured as gateway sites, Branch 3 as a Direct Internet Access (DIA) site, and Branch 4 as a client site. Branches 1 and 2 are not configured.

Refer to Appendix D for a basic vManage device template configuration example for Branch 3, which shows a base configuration before Cloud onRamp for SaaS is enabled.

Appendix D: Base vManage device template

You can review the template configuration for the Branch 3 vEdge device by first going to Configuration>Templates from the left menu in the vManage GUI (Figure D1).

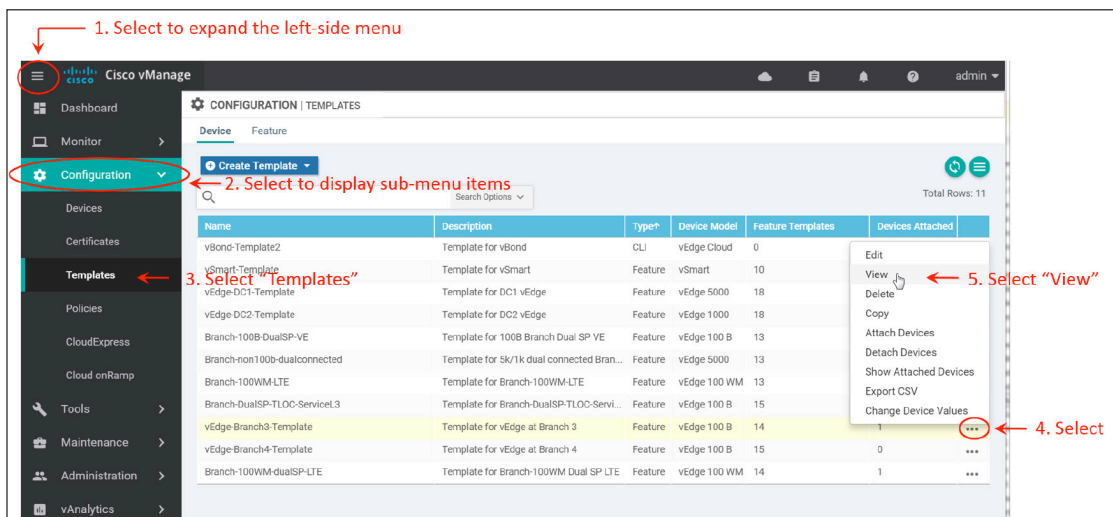
Figure D1. Configuration>Templates menu



Alternatively, you can expand the left menu by clicking the 3 horizontal bars in the top-left corner of the GUI before going to Configuration>Templates.

You will then see a list of device templates. You can view an individual one by selecting ... to the right of the desired device template (**vEdge-Branch3-Template**), and then selecting View (Figure D2).

Figure D2. Expanded Configuration>Templates menu and device template list



The resulting page shows the device template and all of the feature template components that make up the device template (Figure D3).

Figure D3. Device template for Branch 3 vEdge router

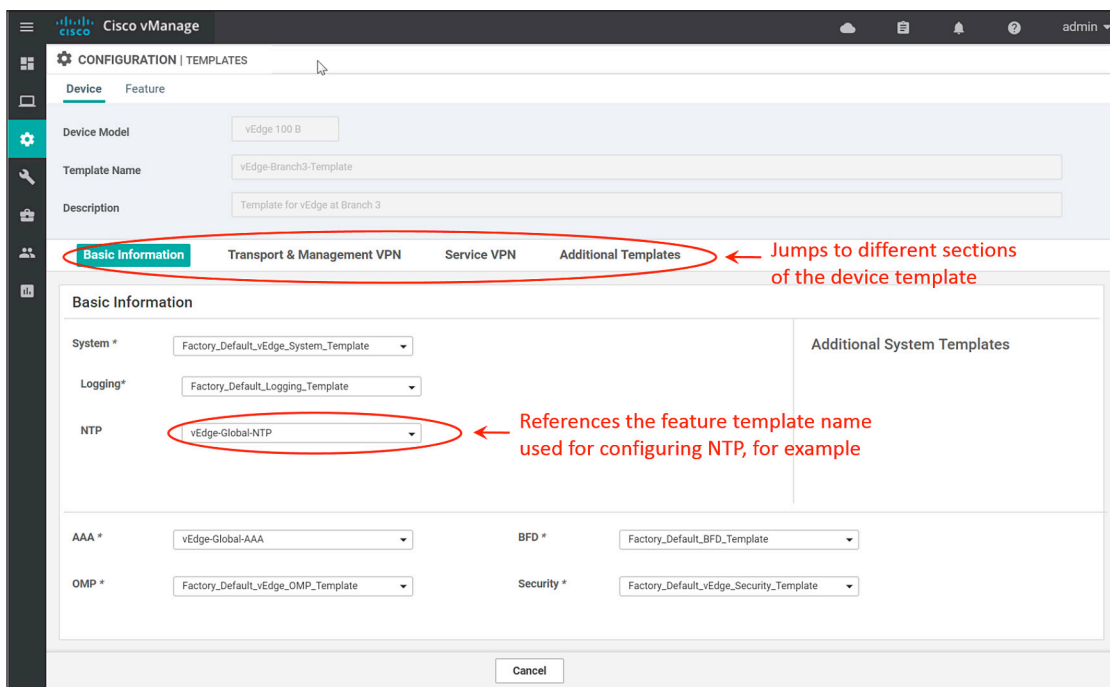


Table D1 lists all of the nondefault feature templates that are referenced in the Branch 3 vEdge router device template.

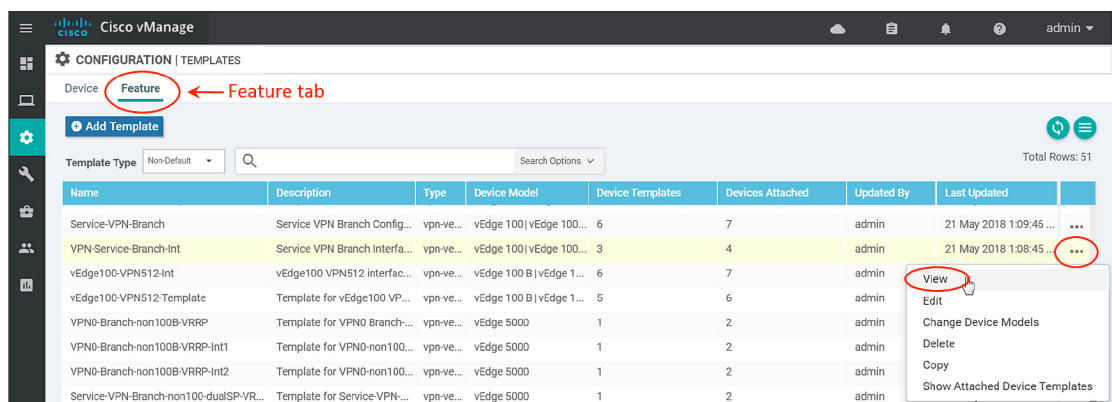
Table D1. Nondefault feature templates used in Branch 3 vEdge device template

Device template section	Template type	Template name	Description
Basic Information	NTP	vEdge-Global-NTP	NTP Configuration for all vEdges
	AAA	vEdge-Global-AAA	AAA Configuration for all vEdges
Transport and Management VPN	VPN 0	VPN0-Branch-SAAS	Branch VPN0 SAAS Configuration
	VPN 0 VPN Interface Ethernet	VPN0-Branch-Int1-SAAS	Branch VPN0 SAAS Interface1 Configuration
	VPN 0 VPN Interface Ethernet	VPN0-Branch-Int2-SAAS	Branch VPN0 SAAS Interface2 Configuration
	VPN 512	vEdge100-VPN512	vEdge100 VPN512 Configuration
	VPN 512 VPN Interface Ethernet	vEdge100-VPN512-Int	vEdge100 VPN512 interface Configuration

Device template section	Template type	Template name	Description
Service VPN	VPN	Service-VPN-Branch	Service VPN Branch Configuration
	VPN VPN Interface Ethernet	Service-VPN-Branch-Int	Service VPN Branch Interface Configuration

To view the components of an individual feature template, select the Feature tab. Then select the ... to the right of the desired feature template (**Service-VPN-Branch-Int**), and then select View (Figure D4).

Figure D4. Feature template list



You will see the output of the feature template. You can scroll through the various sections, or select the different topics near the top under the template description to jump to various sections of the template.

Each configuration parameter has different types of settings: global, default, and device-specific settings. Global settings apply the same value that you specify to all devices that the template applies to, and default settings apply the default value (no input required). With device-specific settings, a variable is defined, so when the device template is applied, the administrator needs to input values for those variables for each device the template will apply to. This process can be done through the GUI itself, or the administrator can upload a .csv file with the variable values listed (Figure D5).

Figure D5. Feature template example

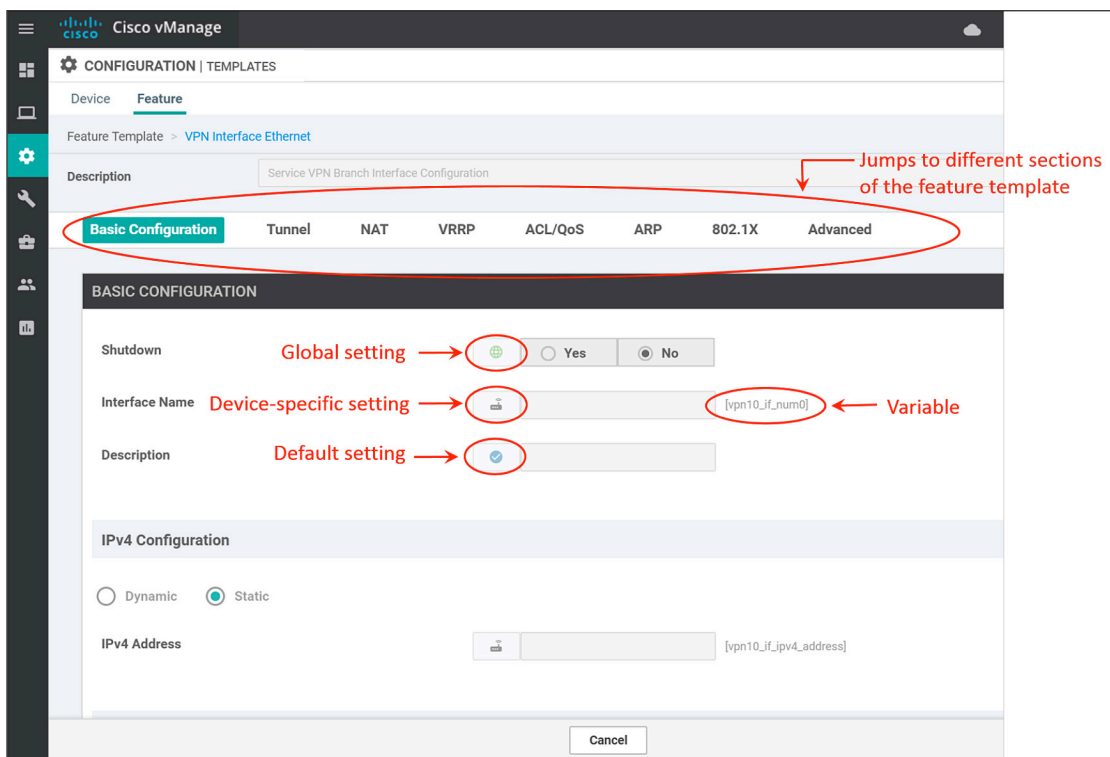


Table D2 outlines the configuration parameters that are contained within each nondefault feature template referenced by the Branch 3 device template. The default system template is also included.

Table D2. Parameters and values for feature templates for Branch 3 vEdge router

Feature template	Parameter	Type (global or device-specific)	Variable or value
Factory_Default_vEdge_System_Template	Basic Configuration>Site ID	Device-specific	system_site_id 203
	Basic Configuration>System IP	Device-specific	system_system_ip 10.255.242.31
	Basic Configuration>Hostname	Device-specific	system_host_name br3-ve1
vEdge-Global-NTP	NTP>New Server>Hostname/ IP address	Global	10.4.47.17
	NTP>New Server>VPN ID	Global	10
vEdge-Global-AAA	AAA> Local>Username/ Password	Global	admin/*****
VPN0-Branch-SAAS	Basic Configuration>VPN	Global	0

Feature template	Parameter	Type (global or device-specific)	Variable or value
	IPv4 Route>Prefix	Global	0.0.0.0
	IPv4 Route>Gateway	Global	“Next Hop”
	IPv4 Route>Next Hop	Device-specific	vpn0_next_hop_ip_addr_int1 64.100.103.17
	IPv4 Route>Next Hop	Device-specific	vpn0_next_hop_ip_addr_int2 144.254.103.17
VPN0-Branch-Int1-SAAS	Basic Configuration>Shutdown	Global	No
	Basic Configuration>Interface Name	Device-specific	vpn0_if_num1 ge0/4
	IPv4 Configuration>IPv4 Address	Device-specific	vpn0_if_ipv4_addr1 64.100.103.18/30
	Tunnel>Tunnel Interface	Global	On
	Tunnel>Color	Device-specific	vpn0_if_tunnel_color1 blue
VPN0-Branch-Int2-SAAS	Basic Configuration>Shutdown	Global	No
	Basic Configuration>Interface Name	Device-specific	vpn0_if_num2 ge0/3
	IPv4 Configuration>IPv4 Address	Device-specific	vpn0_if_ipv4_addr2 144.254.103.18/30
	Tunnel>Tunnel Interface	Global	On
	Tunnel>Color	Device-specific	vpn0_if_tunnel_color2 green
vEdge100-VPN512	Basic Configuration>VPN	Global	512
	IPv4 Route>Prefix	Global	0.0.0.0
	IPv4 Route>Gateway	Global	“Next Hop”
	IPv4 Route>Next Hop	Device-specific	vpn512_next_hop_ip_addr_int 192.168.255.1

Feature template	Parameter	Type (global or device-specific)	Variable or value
vEdge100-VPN512-Int	Basic Configuration>Shutdown	Global	No
	Basic Configuration>Interface Name	Device-specific	vpn512_if_num0 ge0/1
	IPv4 Configuration>IPv4 Address	Device-specific	vpn512_if_ipv4_addr 192.168.255.154/23
Service-VPN-Branch	Basic Configuration>VPN	Global	10
	Advertise OMP>Connected	Global	On
Service-VPN-Branch-Int	Basic Configuration>Shutdown	Global	No
	Basic Configuration>Interface Name	Device-specific	vpn10_if_num0 ge0/0
	IPv4 Configuration>IPv4 Address	Device-specific	vpn10_if_ipv4_addr 10.103.10.1/24

Please refer to Appendix E to view the equivalent base CLI configuration for this vEdge router.

Appendix E: Base CLI configuration

The following is the base deployment example for the Branch 3 vEdge router before enabling Cloud onRamp for SaaS.

Tech Tip

The configurations shown are for informational purposes only. You must go through the vManage GUI and deploy a device template to the vEdge device in order to use the Cloud onRamp for SaaS feature. This process puts the vEdge into vManage mode. You can still run show commands on the vEdge through the CLI, but you cannot update the configuration through the CLI while the device is in vManage mode.

```
system
host-name          br3-ve1
system-ip          10.255.242.31
site-id            203
admin-tech-on-failure
no route-consistency-check
sp-organization-name  "ENB-Solutions - 21615"
organization-name    "ENB-Solutions - 21615"
vbond 64.100.100.50
aaa
  auth-order local radius tacacs
  usergroup basic
    task system read write
    task interface read write
  !
  usergroup netadmin
  !
  usergroup operator
    task system read
    task interface read
    task policy read
    task routing read
    task security read
  !
  user admin
```

```
password $6$NRTGow==$S4496aABngLBCX1o5sDdVd/TgcE.d3zWSDzdKe167Z385T.
Dk5TbikpMne21SUEsCBMT9fMq2WyNqZTN7kQeM1
!
!
logging
  disk
    enable
!
!
ntp
  server 10.4.47.17
  vpn    10
  version 4
  exit
!
!
omp
  no shutdown
  graceful-restart
  advertise connected
  advertise static
!
security
  ipsec
    authentication-type sha1-hmac ah-sha1-hmac
!
!
vpn 0
  interface ge0/3
    ip address 144.254.103.18/30
  !
  tunnel-interface
    encapsulation ipsec
    color green
```

```
no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
!
no shutdown
!
interface ge0/4
ip address 64.100.103.18/30
!
tunnel-interface
encapsulation ipsec
color blue
no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
!
no shutdown
!
ip route 0.0.0.0/0 64.100.103.17
ip route 0.0.0.0/0 144.254.103.17
!
vpn 10
```

```
interface ge0/0
  ip address 10.103.10.1/24
  no shutdown
!
omp
  advertise connected
!
!
vpn 512
interface ge0/1
  ip address 192.168.255.153/23
  no shutdown
!
ip route 0.0.0.0/0 192.168.255.1
!
```

Appendix F: NAT, DNS, and VPN 0 default route configurations needed for DIA example

The following configuration shows the Network Address Translation (NAT), Domain Name System (DNS) server address configuration, and VPN 0 default route configuration necessary for the Direct Internet Access (DIA) site example in bold text.

```
vpn 0
  dns 64.102.6.247 primary
  dns 171.70.168.183 secondary
interface ge0/3
  ip address 10.103.0.6/30
  nat
  !
  tunnel-interface
    encapsulation ipsec
    color green
    no allow-service bgp
    allow-service dhcp
    allow-service dns
    allow-service icmp
    no allow-service sshd
    no allow-service netconf
    no allow-service ntp
    no allow-service ospf
    no allow-service stun
  !
  no shutdown
  !
interface ge0/4
  ip address 10.103.0.2/30
  nat
  !
  tunnel-interface
    encapsulation ipsec
    color blue
    no allow-service bgp
```

```
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
!
no shutdown
!
ip route 0.0.0.0/0 10.103.0.1
ip route 0.0.0.0/0 10.103.0.5
```

Appendix G: Cloud onRamp for SaaS CLI configurations

Following are the Cloud onRamp for SaaS configurations that are pushed to the vEdge devices when Cloud onRamp for SaaS is configured:

Direct Internet Access (DIA):

```
!  
vpn 10  
  cloudexpress  
    node-type      client  
    allow-local-exit  
    applications    salesforce office365 box_net  
!
```

Client:

```
vpn 10  
!  
  cloudexpress  
    node-type client  
!
```

Gateway:

```
vpn 10  
!  
  cloudexpress  
    node-type gateway  
    applications salesforce office365 box_net  
!
```


Appendix H: Cloud onRamp for SaaS CLI monitoring commands

The following shows the output of several CLI monitoring commands on a vEdge router:

```
br3-ve1# show cloudexpress applications
cloudexpress applications vpn 10 salesforce
  exit-type local
  interface ge0/3
  latency    33
  loss       5
cloudexpress applications vpn 10 office365
  exit-type local
  interface ge0/3
  latency    17
  loss       0
cloudexpress applications vpn 10 box_net
  exit-type local
  interface ge0/4
  latency    7
  loss       0
```

```
br3-ve1# show cloudexpress gateway-exits
```

VPN	APPLICATION	GATEWAY IP	LATENCY	LOSS	COLOR	COLOR
10	salesforce	10.255.241.201	33	27	green	green
10	salesforce	10.255.241.202	32	38	green	green
10	salesforce	10.255.242.241	32	33	green	green
10	salesforce	10.255.242.242	26	33	green	green
10	office365	10.255.241.201	17	0	green	green
10	office365	10.255.241.202	17	0	green	green
10	office365	10.255.242.241	17	0	green	green
10	office365	10.255.242.242	17	0	green	green
10	box_net	10.255.241.201	8	0	green	green
10	box_net	10.255.241.202	8	0	green	green
10	box_net	10.255.242.241	8	0	green	green
10	box_net	10.255.242.242	7	0	green	green

```
br3-ve1# show cloudexpress local-exits
```

VPN	APPLICATION	INTERFACE	LATENCY	LOSS
10	salesforce	ge0/3	34	22
10	salesforce	ge0/4	37	27
10	office365	ge0/3	17	0
10	office365	ge0/4	17	0
10	box_net	ge0/3	8	0
10	box_net	ge0/4	8	0

```
br3-ve1# show omp cloudexpress
```

```
Code:
```

```
C -> chosen
```

```
I -> installed
```

```
Red -> redistributed
```

```
Rej -> rejected
```

```
L -> looped
```

```
R -> resolved
```

```
S -> stale
```

```
Ext -> extranet
```

```
Stg -> staged
```

```
Inv -> invalid
```

VPN	ORIGINATOR	APP		FROM PEER	STATUS
		ID	APP NAME		
10	10.255.241.201	1	salesforce	10.255.100.101	C,I,R
				10.255.100.102	C,I,R
10	10.255.241.201	2	office365	10.255.100.101	C,I,R
				10.255.100.102	C,I,R
10	10.255.241.201	6	box_net	10.255.100.101	C,I,R
				10.255.100.102	C,I,R
10	10.255.241.202	1	salesforce	10.255.100.101	C,I,R

				10.255.100.102	C,I,R
10	10.255.241.202	2	office365	10.255.100.101	C,I,R
				10.255.100.102	C,I,R
10	10.255.241.202	6	box_net	10.255.100.101	C,I,R
				10.255.100.102	C,I,R
10	10.255.242.241	1	salesforce	10.255.100.101	C,I,R
				10.255.100.102	C,I,R
10	10.255.242.241	2	office365	10.255.100.101	C,I,R
				10.255.100.102	C,I,R
10	10.255.242.241	6	box_net	10.255.100.101	C,I,R
				10.255.100.102	C,I,R
10	10.255.242.242	1	salesforce	10.255.100.101	C,I,R
				10.255.100.102	C,I,R
10	10.255.242.242	2	office365	10.255.100.101	C,I,R
				10.255.100.102	C,I,R
10	10.255.242.242	6	box_net	10.255.100.101	C,I,R
				10.255.100.102	C,I,R



Please use the [feedback form](#) to send comments and suggestions about this guide.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2018 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)