



Configuring Cisco vWAAS and Viewing vWAAS Components

This chapter describes how to configure vWAAS settings, such as Central Manager address and traffic interception settings, and how to identify a vWAAS on the Central Manager or through the WAAS CLI.

This chapter contains the following sections:

- [Configuring vWAAS](#)
- [Identifying a vWAAS Device](#)
- [vWAAS System Partitions](#)
- [Operating Considerations for vWAAS and WAAS](#)
- [vWAAS Upgrade and Downgrade Considerations](#)

Configuring vWAAS

This section contains the following topics:

- [Configuring vWAAS Settings](#)
- [Configuring vWAAS Traffic Interception](#)

Configuring vWAAS Settings

After the vWAAS VM has been installed, you must configure the following vWAAS settings:

- IP address and netmask
- Default gateway
- Central Manager address
- Settings for corresponding VLAN in VM for network reachability
- CMS (Centralized Management System)
- Traffic interception (described in [Configuring vWAAS Traffic Interception](#))

To configure vWAAS settings, follow these steps:

-
- Step 1** In the vSphere Client, choose the **Console** tab and log in to the vWAAS console.

The username is **admin**, and password is **default**.

- Step 2** Configure the IP address and netmask using the **interface virtual** command, as shown in the following example:

```
VWAAS(config)# interface virtual 1/0
VWAAS(config-if)# ip address 2.1.6.111 255.255.255.0
VWAAS(config-if)# exit
```



Note For vWAAS with WAAS Version 6.1.x and later, the vWAAS and vCM devices require both virtual (network) interfaces to be present. One or both virtual interfaces may be active for the vWAAS and vCM devices to be operational after power up.

- Step 3** Configure the default gateway using the **ip** command:

```
VWAAS(config)# ip default-gateway 2.1.6.1
```

Ping the IP addresses of the default gateway and Central Manager to verify they can be reached before continuing to the next step.

- Step 4** Add the Central Manager address using the **central-manager** command:

```
VWAAS(config)# central-manager address 2.75.16.100
```

- Step 5** Enable CMS to register with the Central Manager using the **cms** command:

```
VWAAS(config)# cms enable
```



Note vWAAS registration with the Central Manager is mandatory before traffic can be optimized.

- Step 6** Configure traffic interception: WCCP, AppNav, or L2 Inline. For more information on traffic interception methods for vWAAS, see [Configuring vWAAS Traffic Interception](#).
-

Configuring vWAAS Traffic Interception

You can configure the following traffic interception methods for vWAAS. [Table 2-1](#) provides descriptions of each traffic interception method.

- WCCP—Available for vWAAS with all WAAS versions.
- AppNav—Available for vWAAS with all WAAS versions
- L2 Inline—Available for WAAS Version 6.2.x and later, for vWAAS with RHEL KVM. [Table 2-2](#) shows the commands for configuring and displaying information on L2 Inline interception for vWAAS.

Table 2-1 Traffic Interception Methods for vWAAS



Traffic Interception Method	Description
WCCP	<p>Specifies interactions between one or more routers (or L3 switches) and one or more application appliances, web caches, and caches of other application protocols, to establish and maintain the transparent redirection of selected types of traffic. The selected traffic is redirected to a group of appliances. Any type of TCP traffic can be redirected.</p> <p>WCCP uses a WCCP-enabled router or L3 switch.</p> <p> Note You can configure WCCP-GRE or L2 Inline as the redirection method for vWAAS running on a UCS-E inside a Cisco ISR G2, where the UCS-E interface is configured as IP unnumbered in IOS.</p> <p>For more information on WCCP, see Chapter 5, “Configuring Traffic Interception” in the <i>Cisco Wide Area Application Services Configuration Guide</i>.</p>
AppNav	<p>A policy and class-based traffic interception method that reduces dependency on the intercepting switch or router by distributing traffic among WAAS devices for optimization.</p> <p>For more information on AppNav, see Chapter 4, “Configuring AppNav” and Chapter 5, “Configuring Traffic Interception” in the <i>Cisco Wide Area Application Services Configuration Guide</i>.</p>
L2 Inline	<p>Places the vWAAS in the data path between WAN and LAN, with an interface facing each segment to inspect and optimize the traffic as needed. For L2 Inline, traffic is forwarded directly without being sent back to the router.</p> <p>The vWAAS interfaces, with virtual NICs, appear as virtual interfaces in the WAAS CM for the running configuration. By default, the NICs supporting Inline mode do not appear in the running configuration when L2 Inline interception is not enabled.</p> <p> Note L2 Inline interception is available for vWAAS for RHEL KVM, for WAAS Version 6.2.1 and later. For vWAAS, L2 Inline interception does not include fail-to-wire capability.</p> <p>For more information on configuring L2 Inline interception on the WAAS CM, see Chapter 5, “Configuring Traffic Interception” in the <i>Cisco Wide Area Application Services Configuration Guide</i>.</p> <p>Table 2-2 shows the commands for configuring and displaying information on L2 Inline interception for vWAAS.</p>

Table 2-2 CLI Commands for L2 Inline Traffic Interception

Mode	Command	Description
Global Configuration	(config) interception-method inline	Enables L2 inline traffic interception on vWAAS.
Interface Configuration	(config-if) cdp	Enables CDP (Cisco Discovery Protocol) on the interface on a WAAS device. (To globally enable the CDP interval and holdtime options, use the cdp global configuration command.)
	(config-if) description	Configures the description for a network interface.
	(config-if) encapsulation	Sets the encapsulation type for the interface.
	(config-if) exit	Terminates interface configuration mode and returns you to global configuration mode.
	(config-if) inline	Enables inline traffic interception for an inlineGroup interface. For more information on the inline interface configuration command, including specifying an inline group and inline interception for VLAN IDs, see the Cisco Wide Area Application Services Command Reference .
	(config-if) ip	Configures the IPv4 address or subnet mask on the interface of a WAAS device, or negotiates an IP address from DHCP on the interface of a WAAS device.
	(config-if) ipv6	Configures the IPv6 address on the interface of a WAAS device, or negotiates an IP address from DHCP on the interface of a WAAS device.
	(config-if) load-interval	Configures the interval at which to poll the network interface for statistics,
	(config-if) shutdown	Shuts down a specific hardware interface on a WAAS device.
EXEC	show interception-method	Displays the configured traffic interception method.
	show interface InlineGroup	Displays inline group information and the slot and inline group number for the selected interface.
	show interface inlineport	Displays the inline port information and the slot and inline group number for the selected interface.
	show running-config	Display the current running configuration.

For more information on these commands, see the [Cisco Wide Area Application Services Command Reference](#).

Identifying a vWAAS Device

This section has the following topics:

- [Identifying a vWAAS Model](#)

- [Identifying a vWAAS Device on the Central Manager](#)
- [Identifying a vWAAS Device with the WAAS CLI](#)

Identifying a vWAAS Model

As shown in [Table 2-3](#), a vWAAS model is determined by two features: the number of vCPUs and the maximum number of TCP connections.

Table 2-3 vWAAS Models with vCPUs and Maximum TCP Connections

vWAAS Model	Number of vCPUs	Maximum Number of TCP Connections
vWAAS-150	1	200
vWAAS-200	1	200
vWAAS-750	2	750
vWAAS-1300	2	1,300
vWAAS-2500	4	2,500
vWAAS-6000	4	6,000
vWAAS-6000-R (earliest WAAS Version 6.4.x)	4	6,000
vWAAS-12000	4	12,000
vWAAS-50000	8	50,000

Identifying a vWAAS Device on the Central Manager

There are two screens on the Central Manager that show identifying information for a vWAAS device. [Table 2-4](#) shows the displayed vWAAS device types.

- Navigate to **Devices** > *device-name*. On the dashboard for the device, in the **Device Info** > **Hardware Details** section, the Model shows the vWAAS device type.
- Navigate to the **Device** > **All Devices** screen, which shows a listing of all devices, with column headings for different information, including Device Type.

Table 2-4 vWAAS Device Types shown in Central Manager and CLI

vWAAS Device	vWAAS Device Type shown in Central Manager
vWAAS on VMware ESXi	OE-VWAAS-ESX
vWAAS on Microsoft Hyper-V	OE-VWAAS-HYPERV
vWAAS on RHEL KVM	OE-VWAAS-KVM
vWAAS on KVM on CentOS	OE-VWAAS-KVM
vWAAS in Microsoft Azure	OE-VWAAS-AZURE

Identifying a vWAAS Device with the WAAS CLI

Table 2-5 shows the commands used to display vWAAS device information: For more information on these commands, see the [Cisco Wide Area Application Services Command Reference](#).

Table 2-5 CLI Commands for vWAAS Device Information

CLI EXEC Command	Description
show version	<p>Displays version information about the WAAS software currently running on the vWAAS device, including date and time system last started, and the length of time the system has been running since the last reboot.</p> <ul style="list-style-type: none"> • (Optional) Use show version last to display version information for the last saved image. • (Optional) Use show version pending to display version information for the pending upgraded image.
show hardware	<p>Displays system hardware status for the vWAAS device, including:</p> <ul style="list-style-type: none"> • startup date and time, the run time since startup, microprocessor type and speed, and a list of disk drives.
show tfo detail	<p>Displays TCP Fast Open (TFO) information, including:</p> <ul style="list-style-type: none"> • State—Registered or Not Registered • Default Action—Drop or Use • Connection Limit—The maximum TFO connections handled before new connection requests are rejected. • Effective Limit—The dynamic limit relating to how many connections are handled before new connection requests are rejected. • Keepalive Timeout—The connection keepalive timeout, in seconds.

vWAAS System Partitions

For all vWAAS models the system partition size for /sw and /swstore is increased from 1 GB to 2GB. Note the following considerations for the new system partition size:

- The **disk delete-preserve-software** command deletes all disk partitions and preserves the current software version.
- The partition size of 2GB each for /sw and /swstore is effective only after a new OVA/ISO installation.
- During an upgrade, the newly defined partition size becomes effective *only after* you run the **disk delete-partitions *diskname*** command.



Caution During a downgrade, the partition size of /sw and /swstore each remains at 2GB, which would lead to a file system size mismatch.

For detailed information on Object Cache data partitions and Akamai Cache data partitions, see Chapter 15, “Maintaining Your WAAS System” in the [Cisco Wide Area Application Services Configuration Guide](#).

Operating Considerations for vWAAS and WAAS

Consider the following guidelines when using Cisco vWAAS with WAAS:

- For vWAAS with WAAS Version 6.1.x and later, the vWAAS and vCM devices require both virtual (network) interfaces to be present, but both need not be active. If only one virtual interface is active, the vWAAS and vCM devices will not be operational after power up. For more information, see [Configuring vWAAS](#).
- If the virtual host was created using an OVA file of vWAAS for WAAS Version 5.0 or earlier, and you have upgraded vWAAS within WAAS, you must verify that the SCSI Controller Type is set to VMware Paravirtual. Otherwise, vWAAS will boot with no disk available and will fail to load the specified configuration.

If needed, change the SCSI controller type to VMware Paravirtual by following these steps:

- a. Power down the vWAAS.
- b. From the VMware vCenter, navigate to vSphere Client > Edit Settings > Hardware.
- c. Choose SCSI controller 0.
- d. From the Change Type drop-down list, verify that the SCSI Controller Type is set to VMware Paravirtual. If this is not the case, choose VMware Paravirtual.
- e. Click OK.
- f. Power up the vWAAS, with WAAS Version 6.1.x or later.

vWAAS Upgrade and Downgrade Considerations

This section has the following upgrade and downgrade topics for vWAAS and vCM models.

For full information on the upgrade or downgrade process for WAAS and vWAAS devices, see the [Release Note for Cisco Wide Area Application Services](#).

- [vWAAS Upgrade and vWAAS Nodes](#)
- [vWAAS Upgrade and SCSI Controller Type](#)
- [vWAAS Upgrade and vCM-100 with RHEL KVM or KVM on CentOS](#)
- [Migrating a Physical Appliance Being Used as a WAAS CM a vCM](#)
- [vWAAS Downgrade Considerations](#)

vWAAS Upgrade and vWAAS Nodes

- When upgrading vWAAS, do not upgrade more than five vWAAS nodes at the same time on a single UCS box. Upgrading more than five vWAAS nodes at the same time may cause the vWAAS devices to go offline and to diskless mode.
- vWAAS for WAAS 6.4.1 requires additional resources before upgrading from WAAS 6.2.3d to WAAS 6.4.1.

- *Upgrading from the WAAS Central Manager:* If you initiate and complete the upgrade from the WAAS Central Manager without increasing resources for vWAAS, alarms (CPU & RAM) to indicate insufficient resource allocation will be displayed on the WAAS Central Manager *after* the upgrade process is completed. No alarms are displayed at the beginning of the upgrade process.
- *Upgrading from the WAAS CLI:* If you initiate an upgrade to WAAS 6.4.1 with the CLI, a warning on insufficient resources is displayed at the *start* of the upgrade process.

vWAAS Upgrade and SCSI Controller Type

If the virtual host was created using an OVA file of vWAAS for WAAS Version 5.0 or earlier, and you have upgraded vWAAS within WAAS, you must verify that the SCSI Controller Type is set to **VMware Paravirtual**. Otherwise, vWAAS will boot with no disk available and will fail to load the specified configuration.

If needed, change the SCSI controller type to **VMware Paravirtual** by following these steps:

-
- Step 1 Power down the vWAAS.
 - Step 2 From the VMware vCenter, navigate to **vSphere Client > Edit Settings > Hardware**.
 - Step 3 Choose **SCSI controller 0**.
 - Step 4 From the Change Type drop-down list, verify that the SCSI Controller Type is set to **VMware Paravirtual**. If this is not the case, choose **VMware Paravirtual**.
 - Step 5 Click **OK**.
 - Step 6 Power up the vWAAS, with WAAS Version 6.2.3, or WAAS 6.1.x or later. WAAS Version 6.1.x is the minimum version used.
-

vWAAS Upgrade and vCM-100 with RHEL KVM or KVM on CentOS

If you upgrade to WAAS Version 6.2.3, or downgrade from WAAS Version 6.2.3 to an earlier version, and use a vCM-100 model with the following parameters, the vCM-100 may not come up due to GUID Partition Table (GPT) boot order errors.

- vCM-100 has default memory size of 2 GB
- vCM-100 uses the RHEL KVM or KVM on CentOS hypervisor
- You use the **restore factory-default** command or the **restore factory-default preserve basic-config** command



Caution

If you are upgrading a vCM-100 model from an earlier WAAS version to WAAS Version 6.2.3, the upgrade process on this type of configuration will automatically clear system and data partition.

If you upgrade the vCM device to WAAS Version 6.2.3 via the console, a warning message similar to the following will be displayed:

```
WARNING: Upgrade of vcm device to 6.2.0 (or) higher version with '/sw' and '/swstore'
```


size less than 2GB will clear system and data partition.

If you upgrade the vCM device to WAAS Version 6.2.3 via the GUI, a warning message is not displayed.



Caution

The **restore factory-default** command erases user-specified information stored in the flash image, including the starting configuration of the device, and also removes data from the disk, user-defined partitions, and the entire Central Manager database.

To resolve this situation, follow these steps:

- Step 1 Power down the vWAAS using the **virsh destroy** *vmname* command or the virt manager.
- Step 2 Power up the vWAAS using the **virsh start** *vmname* command or the virt manager.



Note

This upgrade/downgrade scenario does not occur for vCM-100 models whose memory size is upgraded to 4 GB.

Migrating a Physical Appliance Being Used as a WAAS CM a vCM

To migrate a physical appliance being used as a primary WAAS Central Manager to a vCM, follow these steps:

- Step 1 Introduce vCM as the Standby Central Manager by registering it to the Primary Central Manager.
- Step 2 Configure both device and device-group settings through Primary CM and ensure that devices are getting updates. Wait for two to three data feed poll rate so that the Standby CM gets configuration sync from the Primary CM.
- Step 3 Ensure that the Primary CM and Standby CM updates are working.
- Step 4 Switch over CM roles so that vCM works as Primary CM. For additional details please refer to [“Converting a Standby Central Manager to a Primary Central Manager”](#) section of the WAAS Configuration Guide.

vWAAS Downgrade Considerations

Consider the following when you downgrade vWAAS to an earlier WAAS version:

- vWAAS models vCM-500N and vCM-1000N, introduced in WAAS v5.5.1, cannot be downgraded to a version less than v5.5.1.
- On the UCS E-Series Server Module running vWAAS, downgrading to a version earlier than 5.1.1 is not supported. On other vWAAS devices you cannot downgrade to a version earlier than 4.3.1.

**Note**

If the vWAAS device is downgraded in the following scenarios:

- from vWAAS for WAAS Version 6.4.1a to WAAS Version 6.2.3x, or
- from vWAAS for WAAS Version 6.x to 5.x

the WAAS alarm `filesystem_size_mismatch` is displayed; it indicates that the partition was not created as expected. To clear the alarm, use the `disk delete-data-partitions` command to re-create the DRE partitions.
