Cisco vWAAS on Cisco ENCS 5400-W Series

This chapter describes Cisco vWAAS on the Cisco Enterprise Network Compute System, W Series appliance.

Cisco vWAAS on Cisco ENCS 5400-W Series

This section contains the following topics:

About the Cisco ENCS 5400-W and ENCS 5400 Series

The Cisco Enterprise Network Compute Series (ENCS) is used to host the Cisco Enterprise Network Functions Virtualization (NFV) solution. ENCS is also used to deploy the Cisco NFV Infrastructure Software (NFVIS), and Cisco and third party VNFs on Cisco Enterprise NFV.

For more information on Cisco NFVIS, see Chapter 9, "Cisco vWAAS with Cisco Enterprise NFVIS".

Table 7-1 describes how the ENCS 5400 Series and the ENCS 5400-W Series (used with vWAAS) are used with Enterprise NFV. For more information on the Cisco ENCS 5400-W series, see the *Cisco 5400 Enterprise Network Compute System Data Sheet*.

Table 7-1 Cisco ENCS 5400 Series and ENCS 5400-W Series

Cisco ENCS Series	Description
ENCS 5400 Series	The Cisco ENCS 5400 Series—ENCS 5406, 5408, and 5412—is a line of compute appliances designed for the Cisco SD-Branch and Enterprise NFV solution.
ENCS 5400-W Series	The ENCS 5400-W Series—ENCS 5406-W, 5408-W, and 5412-W—is an x86 hybrid platform is designed for the Cisco Enterprise NFV solution, for branch deployment and for hosting WAAS applications. These high-performance units achieves this goal by providing the infrastructure to deploy virtualized network functions while at the same time acting as a server that addresses processing, workload, and storage challenges. **Note** vWAAS is designed to run in appliance mode or as a Virtualized Network Function (VNF) in three Cisco ENCS 5400-W series models—ENCS 5406-W, ENCS 5408-W, ENCS 5412-W—and three Cisco PIDs—ENCS 5406-K9, ENCS 5408-K9, ENCS 5412-K9.

vWAAS as VM on Cisco ENCS 5400-W Series

For vWAAS with Cisco Enterprise NFVIS on ENCS, vWAAS operates as a VM to provide WAN and application optimization, and, optionally, application optimization with Akamai Connect.

vWAAS with Cisco Enterprise NFVIS runs on Cisco ENCS 5400-W series, the Cisco x86 hardware platform for branch deployment, for routing and hosted applications.

Table 7-2 shows supported vWAAS models for Cisco ENCS 5406-W, 5408-W, and 5412-W.

Table 7-2 Supported vWAAS Models for Cisco ENCS 5400-W Series

ENCS Model	Processor	CPUs	RAM	Supported vWAAS Model
ENCS 5406-W	Intel Xeon Processor D-1528 (1.9 GHz, 9 MB L2 cache)	6-core	16 GB	vWAAS-200 or vWAAS-750
ENCS 5408-W	Intel Xeon Processor D-1548 (2.0 GHz, and 12 MB L2 cache)	8-core	16 GB	vWAAS-1300
ENCS 5412-W	Intel Xeon Processor D-1557 (1.5 GHz, and 18 MB L2 cache)	12-core	32 GB	vWAAS-2500 or vWAAS 6000R

ENCS 5400-W Models that Replace EOL/EOS WAVE Devices

Cisco WAVE appliances have end-of-sale (EOS) and end-of-life (EOL) dates, highlighted in the *End-of-Sale and End-of-Life Announcement for the Cisco WAVE 294, 594, 694, 7541, 7571 and 8541*.

Table 7-3 shows the ENCS 5400-W Series models that replace the EOS/EOL WAVE models, and the supported vWAAS models for each ENCS 5400 model.

Table 7-3 ENCS 5400-W Series Replacment Models for WAVE Devices

EOS/EOL WAVE model	ENCS 5400 model to replace WAVE model	Supported vWAAS Models for ENCS 5400	Connection Size
WAVE-294	ENCS 5406-W	vWAAS 200	200 connections
WAVE-594-8G	ENCS 5406-W	vWAAS-750	750 connections
WAVE-594-12G	ENCS 5408-W	vWAAS-1300	1300 connections
WAVE-694-16G	ENCS 5412-W	vWAAS-2500	2500 connections
WAVE-694-24G	ENCS 5412-W	vWAAS-6000-R	6000 connections

ENCS 5400-W Hardware Features and Specifications

Table 7-4 shows features and specifications that apply to all three ENCS 5400-W series models. For views of the Cisco ENCS 5400-W Series and further information, see the *Cisco 5400 Enterprise Network Compute System Data Sheet*.

Table 7-4 ENCS 5400-W Series Features and Specifications

ENCS 5400 Feature/Specification	Description
vWAAS models supported	One of the following configurations: • ENCS 5406-W supports vWAAS 200, vWAAS-750 • ENCS 5408-W supports vWAAS-1300 • ENCS 5412-W supports vWAAS-2500, vWAAS-6000-R
CPU	One of the following specifications: • ENCS 5406-W: Intel Xeon Processor D-1528 (6-core, 1.9 GHz, and 9 MB cache) • ENCS-5408-W: Intel Xeon Processor D-1548 (8-core, 2.0 GHz, and 12 MB cache) • ENCS-5412-W: Intel Xeon Processor D-1557 (12-core, 1.5 GHz, and 18 MB cache)
BIOS	Version 2.4
Cisco NFVIS on KVM hypervisor	KVM hypervisor Version 3.10.0-327.el7.x86_64
CIMC	Version 3.2
Network Controller	Intel FTX710-AM2
WAN Ethernet port	Intel i350 dual port

ENCS 5400 Feature/Specification	Description
DIMM	Two DDR4 dual in-line memory module (DIMM) slots, for ENCS models with the following capacities: • ENCS 5406-W—16 GB • ENCS 5408-W—16 GB • ENCS 5412-W—32 GB The memory module in each of the slots can be upgraded to a maximum of 32 GB, so that you can have a maximum capacity of 64 GB DIMM.
Gigabit Ethernet ports	Two Gigabit Ethernet ports—For each RJ45 port, there is a corresponding fiber optic port. At a given time, you can use either the RJ45 connection or the corresponding fiber optic port.
NIM	One Network Interface Module (NIM) expansion slot—You can install a NIM in the NIM slot, or if the slot is not needed, you can remove the NIM from the NIM module. Each ENCS 5400 model supports one NIM slot, for a Cisco 4-port 1G fail-to-wire NIM card.
Management Controller	Ethernet management port for Cisco Integrated Management Controller (CIMC), which monitors the health of the entire system.
HDD Storage	Although there are two hot-swappable HDD slots, we do not recommend HDD storage for the ENCS 5400-W Series.
SSD Storage	• No RAID and 1 960 GB SSD • RAID-1 and 2 SSDs (960 GB SSD) **Note** If you need to add or remove RAID-1 for your system, see Adding or Removing RAID-1 for ENCS 5400-W Series. Note that the RAID-1 option is available for vWAAS for WAAS Version 6.4.1a and later.
Offload Capabilities	Optional crypto module to provide offload capabilities to optimize CPU resources like VM-toVM traffic and to maintain open software support.

vWAAS Bundled Image Install Procedure

Before You Begin

- Verify that the specified ENCS 5400-W Series chassis (ENCS 5406-W, 5408-W, or 5412-W) is already installed and powered up. For information on how to install the an ENCS 5400-W Series device, see the *Cisco 5400 Enterprise Network Compute System Hardware Installation Guide*.
- If you need to add or remove RAID-1 for your system, see Adding or Removing RAID-1 for ENCS 5400-W Series. Note that the RAID-1 option is available for vWAAS for WAAS Version 6.4.1a and later.

To install vWAAS with NFVIS an ENCS 5400-W Series device on your WAAS system, follow these steps:

Step 1 Copy the vWAAS bundled image file—an ISO file that contains the NFVIS 3.10.1 image (file format "Cisco_NFVIS...") and WAAS 6.4.3a image (file format "WAAS-APPLIANCE...")—on your laptop.

For how to upgrade to NFVIS 3.10.1, see the chapter "Cisco vWAAS with Cisco Enterprise NFVIS," section Upgrading to Cisco NFVIS 3.10.1.

Step 2 Connect your laptop's Ethernet port to the ENCS device's Cisco Integrated Management Controller (CIMC) port.

Step 3 Configure your laptop with a static IP address; for example, 192.168.1.3.

Note By default, the IP address on the ENCS device's CIMC port is configured as 192.168.1.2.

Step 4 Open your web browser and enter **https://192.168.1.2**.

The CIMC console login page appears.

Step 5 Log in with your user name and password.

Default user name is **admin**.

Default password is **password**.

Step 6 Click **Login**.

Note The Change Password dialog box appears the first time, only, that you log into the CIMC console. Change the password as needed and click **Save**.

Step 7 The CIMC Home page is displayed.

Step 8 Navigate to **Home** > **Compute** > **BIOS** > **Configure Boot Order**.

The Configure Boot Order dialog box appears.

Step 9 At the Device Types listing, select **CD/DVD Linux Virtual CD/DVD**.

Click **Add**.

Step 10 At the Device Type listing, select **HDD**.

Click **Add**.

Step 11 Using the **Up** and **Down** options, set the boot order sequence.

Step 12 **CD/DVD Linux Virtual CD/DVD** must be the first listing in the boot order.

Step 13 To complete the boot order setup, click **Apply**.

Step 14 Launch the KVM console. You can launch the KVM console from CIMC Home page or the Remote Management area.

Step 15 *At the KVM console:*

After the KVM console is initialized, map the vWAAS bundled image through the **Server** > **Remote Presence** > **Virtual Media** tab on the KVM console.

Step 16 To load the mapped image, at the KVM Console Power tab, use the **Power Cycle System [cold boot]** option to power off and then power on the device.

Note When the server reboots, the KVM Console will automatically install the Cisco Enterpirse NFVIS from the virtual CD/DVD drive. The entire installation may take 30 minutes to one hour to complete.

Step 17 With the installation running in the background, use your laptop to connect via SSH to the CIMC default IP (192.168.1.2).

Step 18 After the installation is successful, the ENCS device reboots.

```
[  OK  ] Unmounted /mnt/sysimage/dev.
[  OK  ] Unmounted /mnt/sysimage/sys.
Unmounting /mnt/sysimage...
[  OK  ] Unmounted /mnt/sysimage.
[  OK  ] Reached target Unmount All Filesystems.
[  OK  ] Stopped target Local File Systems (Pre).
[  OK  ] Stopped Create Static Device Nodes in /dev.
Stopping Create Static Device Nodes in /dev...
[  OK  ] Stopped Remount Root and Kernel File Systems.
Stopping Remount Root and Kernel File Systems...
[  OK  ] Stopped Collect Read-Ahead Data.
Stopping Collect Read-Ahead Data...
Stopping Monitoring of LVM2 mirrors...
dmeventd or progress polling...
[  OK  ] Stopped Monitoring of LVM2 mirrors,...
ng dmeventd or progress polling.
Stopping LVM2 metadata daemon...
[  OK  ] Stopped LVM2 metadata daemon.
[  OK  ] Started Restore /rdracut Warning: Killing all remaining processes
Rebooting.

[ deviceID] Restarting system.
```

Step 19 The ENCS device boots up and displays options to install vWAAS. Depending on your ENCS model, one of the following choices is displayed:

- For ENCS 5406-W—vWAAS 200 and vWAAS-750 are displayed.
  Select one vWAAS model for ENCS 5406-W.
- For ENCS 5408-W—vWAAS-1300 is the only choice displayed.
  vWAAS-1300 is automatically selected for ENCS 5408-W.
- For ENCS 5412-W—vWAAS-2500 and vWAAS-6000-R are displayed.
  Select one model for ENCS 5412-W.

  Example:

  In the following example, a vWAAS-6000-R is selected for an ENCS 5412-W:

  ```
  vWAAS Model
  1) vWAAS-2500
  2) vWAAS-6000-R
  3) Quit
  Please enter your choice: 2
  ```

Table 7-5 shows installation times by vWAAS model/number of connections:

Table 7-5 Installation Time by vWAAS Model/Number of Connections

vWAAS Model	Number of connections	Minimum NFVIS Installation Time	Minimum WAAS Installation Time	Minimum Total Installation Time
vWAAS-200	200 connections	60 minutes	15 minutes	75 minutes
vWAAS-750	750 connections	60 minutes	24 minutes	84 minutes
vWAAS-1300	1300 connections	55 minutes	28 minutes	83 minutes
vWAAS-2500	2500 connections	67 minutes	34 minutes	101 minutes
vWAAS-6000-R	6000 connections	66 minutes	38 minutes	104 minutes

Step 20 After installation is complete, the Cisco WAAS login prompt appears.

Step 21 The new OE-ENCS device will be displayed in the WAAS Central Manager **Devices** > **All Devices** listing table.

Step 22 You can view detailed information on the new OE-ENCS device by navigating to **Devices** > *DeviceName* > **Dashboard**.

CLI Commands Used with vWAAS on ENCS 5400-W

Table 7-6 shows the CLI commands used to display information about vWAAS on ENCS.

Table 7-6 CLI Commands Used with vWAAS on ENCS

Mode	Command	Description
EXEC	**copy sysreport disk**	The ENCS logs are part of the sysreport generation for debugging.
	reload	Halts the operation and performs a cold restart of the VM.
	show hardware	Displays the following information for the specified device: • Hardware Information—Manufacturer, PID, serial number, hardware version, CPU information, Memory information, and disk size. • System Information—UUID, NFVIS version, compile time, kernel version, Qemu version, LibVirt version, and OVS version.
	show inventory	Displays system inventory information, including a description of the device, and the device's PID, chassis or slot number, version number, and serial number.
	show nfvis version	Displays NFVIS and BIOS version.
	show version	Displays the version of the OE-ENCS device, as well as device ID, system restart time, system restart reason, and amount of time system has been up.
	shutdown	Powers down the ENCS host/server.
global config	**interface virtual**	The internal interface is used for communication between the NFVIS host and the WAAS guest. The IP address associated with this interface (virtual 1/0) is assigned automatically by NFVIS while booting up, and cannot be modified. **Note** The interface virtual slot/port command cannot be used to configure ENCS internal interface.

System Requirements for vWAAS on ENCS-W with Akamai Connect

Table 7-7 shows memory and disk requirements for vWAAS on ENCS-W with Akamai Connect, by vWAAS model.

Table 7-7 Memory and Disk Requirements for vWAAS on ENCS with Akamai Connect

vWAAS model, Number of ENCS Connections	Memory	Data Disk	Akamai Cache
vWAAS-200, 200 ENCS connections	3 GB	160 GB	100 GB
vWAAS-750, 750 ENCS connections	4 GB	250 GB	250 GB
vWAAS-1300, 1300 ENCS connections	6 GB	300 GB	300 GB
vWAAS-2500, 2500 ENCS connections	8 GB	400 GB	350 GB
vWAAS-6000 6000 ENCS connections	11 GB	500 GB	350 GB

Registering and Deploying vWAAS ENCS 5400-W Series

This section contains the following procedures:

- Registering vWAAS on ENCS 5400-W
- Deploying vWAAS on ENCS 5400-W
- Registering vWAAS on ENCS 5400-W with the Central Manager

Registering vWAAS on ENCS 5400-W

Before you begin, verify the following:

- The disk is already mounted.
- Gigabit Ethernet port 0/0 can be used for vWAAS management or data.
- Gigabit Ethernet port 0/1 can be used for vWAAS management or data.
- The existing LAN-net and SR-IOV will be used.

To register vWAAS on ENCS, follow these steps:

Step 1 Power on the ENCS device.

The vWAAS automatically starts up when the ENCS device is powered on.

Step 2 Using an Ethernet cable, connect your laptop to the MGMT port of the ENCS device.

Step 3 Verify that the WiFi is disabled on your laptop.

Step 4 Perform the following steps on a MAC system:

- Navigate to **Preferences > Network > Thunderbolt**.
- From the Configure IPv4 drop-down list, choose **Manually**.
- In the IP Address field, enter an IP address, for example, 192.168.1.5.
- In the Subnet Mask field, enter 255.255.255.0.
- Open the terminal and use SSH to connect to the device (192.168.1.1).

  Use **admin** for login and password credentials.

Step 5 Run the shell script (mfg.sh), which registers, installs, and checks the status of the vWAAS instance.

Step 6 Exit.

Deploying vWAAS on ENCS 5400-W

To deploy vWAAS on NFVIS on ENCS, follow these steps:

Step 1 Perform the steps shown in Registering vWAAS on ENCS 5400-W.

Step 2 Copy the vWAAS KVM tar.gz file to a directory on your laptop, for example, "/downloads."

Step 3 Navigate to the directory that you have created.

Step 4 Start an HTTP server on your laptop to upload and register the image.

Step 5 Connect the Ethernet port of your laptop to the Management port of the Cisco ENCS device.

Step 6 Configure the laptop with static IP, for example, 192.168.1.2.

By default, the Management port on the Cisco ENCS is 192.168.1.1.

Step 7 On your laptop, start the manufacturing script from the directory you have created.

The manufacturing script performs the following actions:

a. Connect to the Cisco ENCS device.

b. The following status messages will be displayed:

```
Trying to connect to ENCS Device
NFVIS server up and running
Reconfiguring the LAN bridge.......
Reconfiguring the WAN bridge.......
Cleaning existing vWAAS instance.......
Checking disk health.......
Following vWAAS images are available:
list of images
```

c. At the **Enter the image number:** prompt, enter your image number.

d. The following status messages will be displayed:

```
Preparing for WAAS installation
Progress: ############ 100%
Installation is in progress.......
Progress: ############ 100%
Installation is completed!!!
```

Step 8 Registration and installation are complete.

Step 9 Exit.

Registering vWAAS on ENCS 5400-W with the Central Manager

You must register the vWAAS instance and/or the WAAS appliance running in accelerator mode with the WAAS Central Manager.

To register vWAAS on NFVIS on ENCS with the Central Manager, these steps:

Step 1 The Central Manager IP address is 10.78.99.142.

At the vWAAS instance or WAAS appliance that you want to register, enter the following Central Manager IP address information:

```
DC2-WAE-1(config)#central-manager address 10.78.99.142
DC2-WAE-1(config)#
DC2-WAE-1(config)#end
DC2-WAE-1#show running-config | i central
central-manager address 10.78.99.142
```

Step 2 At the vWAAS instance or WAAS appliance that you want to register, enable the Centralized Management System (CMS) service:

```
DC2-WAE-1(config)#cms enable
Registering WAAS Application Engine...
Sending  device registration request to Central Manager with address 10.78.99.142
Please wait, initializing CMS tables
Successfully initialized CMS tables
Registration complete.
Please preserve running configuration using 'copy running-config startup-config'.
Otherwise management service will not be started on reload and node will be shown
'offline' in WAAS Central Manager UI.
management services enabled
```

Step 3 In the Central Manager, navigate to **Devices > All Devices**.

- The WAAS appliance will be displayed in the Device Type column as **OE-ENCS**.

Step 4 Exit.

Adding or Removing RAID-1 for ENCS 5400-W Series

Note The RAID-1 option is available for vWAAS for WAAS Version 6.4.1a and later.

This section contains the following topics:

Note For further information on RAID and the ENCS 5400-W Series, see the *Cisco 5400 Enterprise Network Compute System Hardware Installation Guide*.

Migrating Equipment from No RAID and 1 SSD to RAID-1 and 2 SSDs

Note The RAID-1 option is available for vWAAS for WAAS Version 6.4.1a and later.

Before You Begin

- To enable RAID-1 virtual disk on ENCS, refer to Mixing Drives Types in RAID Groups for hard drive compatibility and best practice for performance. Before creating virtual disk, both drives must be in **Unconfigured Good** state. If drive is in other status, use the CIMC Web GUI or CLI and do the following:

  If disk is in JBOD state:

  a. Navigate to **Storage** tab > **Physical Drive Info** tab.
  b. In the Actions area, choose **Set State as Unconfigured Good**.
  c. Confirm that disk is in Unconfigured Good state.

  *If disk is in **Foreign Config** state:*

  a. Navigate to **Storage** tab > **Controller Info** tab.
  b. In the Actions area, choose **Clear Foreign Config**.
  c. In the Actions area, choose **Unconfigured Good**.
  d. Confirm that disk is in Unconfigured Good state.

To create the virtual disk, follow these steps:

Step 1 Log in to the CIMC console.

Step 2 In the CIMC console left pane, click the **Storage** tab.

Step 3 In the CIMC console middle pane, click the **Controller Info** tab.

Step 4 In the Action area, click **Create Virtual Drive from Unused Physical Drives**.\

The Create Virtual Drive from Unused Physical Drives Wait dialog box is displayed.

Step 5 In the Create Virtual Drive from Unused Physical Drives dialog box, choose the following:

a. At the RAID Level drop-down box, choose **1**.
b. In the Create Drive Groups area:

   Select physical drives for your system from the Physical Drives pane and click >> to add these to the Drive Groups pane.
c. In the Virtual Drive Properties area:
   - The Virtual Drive Name field displays the automatically assigned name.
   - At the Strip Size drop-down list, select the strip size (default is 64k).
   - At the Write Policy drop-down list, select the Write policy (default is Write Through)
   - At the Access Policy drop-down list, select the Access policy (default is Read Write).

- At the Read Policy drop-down list, select the Read policy (default is No Read Ahead).
- At the Cache Policy drop-down list, select the Cache policy (default is Direct IO)
- At the Disk Cache Policy drop-down list, select the Disk Cache policy (default is Unchanged).
- The value for the Size drop-down list automatically filled.

Step 6 Click **Create Virtual Drive**.

Migrating Equipment from RAID-1 and 2 SSDs to No RAID and 1 SSD

Note The RAID-1 option is available for vWAAS for WAAS Version 6.4.1a and later.

Before You Begin

- You must wait for the disk to be completely shut down before you physically remove the disk from the WAE. When the RAID removal process is complete, WAAS generates a disk failure alarm and trap. In addition, a syslog error message is logged.
- If the removal event occurs while the RAID array is in the rebuild process, the RAID removal process may take up to 1 minute to complete. The duration of this process depends on the size of the disk.

  If you administratively shut down the disk during the RAID rebuild process, a RAID rebuild abort alarm is generated instead.

To remove a RAID-1 disk, follow these steps:

Step 1 To manually shut down the disk, enter global configuration mode and then enter the **disk disk-name** *diskxx* **shutdown** command:

```
WAE# configure
WAE(config)# disk disk-name diskxx shutdown
```

Step 2 Wait for the disk to be completely shut down before you physically remove the disk from the WAE.

Step 3 When the RAID removal process is complete, WAAS generates a disk failure alarm and trap. In addition, a syslog error message is logged.

Note We recommend that you disable the **disk error-handling reload** option if it is enabled because it is not necessary to power down the system to remove a disk.

Fail-to-Wire on vWAAS on ENCS 5400-W

This section contains the following topics:

About FTW on vWAAS on ENCS

Fail-to-Wire (FTW) is a physical layer (Layer 1) bypass that allows interface port pairs to go into bypass mode—so that the hardware forwards packets between these port pairs without software intervention. FTW provides network connectivity when there are software or hardware failures.

Operating Guidelines for FTW on vWAAS on ENCS:

- FTW is available for vWAAS for WAAS Version 6.4.3 and later.
- Hardware bypass is supported for a fixed set of ports. For example, you can pair Port 1 with Port 2, or Port 3 with Port 4, but you cannot pair Port 1 with Port 4.
- Configuring standby and port channel in on-board interface is supported; configuring standby over portchannel in the on-board interface is not supported.
- Configuring standby, port channel, and standby over port channel in FTW interface is supported.

FTW Traffic Interception Modes

FTW uses two traffic interception modes: inline interception and WCCP.

- Inline interception uses the following operating modes:
  - Interception Mode—The NIM ports are in interception mode. Two inline groups are created for the four-port NIM card in vWAAS. The NIM card ports will fail-to-wire after a failover timeout.
  - Bypass Mode—You can shut down the inline group, putting the corresponding pair of ports in bypass mode. In Bypass mode, traffic coming into Port 0 is redirected to Port 1, and traffic coming into Port 1 is redirected to Port 0.
  - Bypass All Mode—If the system reloads or if the software experiences an unexpected event, all the inline groups can be put in bypass mode; no Ethernet connection can be established between the devices.
- WCCP traffic interception mode:
  - Standalone Mode—Each port in the NIM can be used separately. WAAS can use this mode to enable WCCP interception. The ports of the NIM card do not fail-to-wire in this mode, and the watchdog timer remains disabled.

FTW Failure Handling

Here is how FTW handles the following system failure scenarios:

- Disk issue—NFVIS detects the disk issue and puts the NIM into bypass mode.
- NFVIS unexpected event—FTW detects that vWAAS keep-alive messages have stopped, and FTW puts the NIM to pass-through FTW.
- WAAS reload—The vWAAS puts the FTW card to FTW mode immediately.

- WAASnet restarts or experiences an unexpected event—The vWAAS puts the FTW NIM card into FTW mode immediately. When the WAASnet datapath is restored, the vWAAS returns the FTW ports to inline mode.

CLI Commands for Port Channel and Standby Interfaces

This section contains the following topics:

Show Commands Used with Port Channel and Standby Interfaces

Table 7-8 Show Commands Used with Port Channel and Standby Interfaces

Show Command	Description
show statistics f2w	Displays InlineGroup status, including the amount of time, in seconds, since the last keepalive was received, and how many bypass alarms have been received or cleared.
show interface InlineGroup	Displays InlineGroup connection statistics and InlineGroup status, as well as the failover timeout frequency.
show interface InlinePort LAN	Displays InlinePort LAN connection statistics and specific port status of the InlineGroup.
show interface InlinePort WAN	Displays InlinePort WAN connection statistics and specific port status of the InlineGroup.

Creating, Removing, Showing Port Channel Interfaces

The following example shows how to create a port channel with the **interface portchannel** global configuration command:

```
vWAAS#configure
vWAAS(config)#interface portchannel 1
vWAAS(config-if)#ip address 10.10.10.10 255.0.0.0
vWAAS(config-if)#exit
```

The following example shows how to remove a port channel with the **no interface portchannel** global configuration command:

```
vWAAS#configure
vWAAS(config)#interface portchannel 1
vWAAS(config-if)#ip address 10.10.10.10 255.0.0.0
vWAAS(config-if)#exit
vWAAS(config-if)#no interface portchannel 1
```

Note The global configuration commands **interface port channel** and **no interface port channel** will be saved across reloads if you run the **copy running-config startup-config** command or the **write-mem** command.

The following example shows output from the **show running config** command for port channel interfaces:

```
interface PortChannel 1
ip address 10.10.10.10 255.0.0.0
exit
!
interface Virtual 1/0
channel-group 1
exit
interface Virtual 2/0
channel-group 1
exit
```

Creating, Removing, Showing Standby Interfaces

The following example shows how to create a standby interface with the **interface standby** global configuration command:

```
ENCS-APPLIANCE#configure
ENCS-APPLIANCE(config)#interface standby 1
ENCS-APPLIANCE(config-if)#ip address 10.10.10.10 255.0.0.0
ENCS-APPLIANCE(config-if)#exit
```

The following example shows how to remove a standby interface with the **no interface portchannel** global configuration command:

```
ENCS-APPLIANCE#configure
ENCS-APPLIANCE(config)#interface standby 1
ENCS-APPLIANCE(config-if)#ip address 10.10.10.10 255.0.0.0
ENCS-APPLIANCE(config-if)#exit
ENCS-APPLIANCE(config-if)#no interface standby 1
```

Note The global configuration commands **interface standby** and **no interface standby** will be saved across reloads if you run the **copy running-config startup-config** command or the **write-mem** command.

The following example shows output from the **show running config** command for standby interfaces:

```
interface Standby 1
 ip address <addr>  <netmask>
 exit
!
interface Virtual 1/0
 standby 1 primary
 exit
interface Virtual 2/0
 standby 1
 exit
```

Configuring Inline Interception for FTW on ENCS

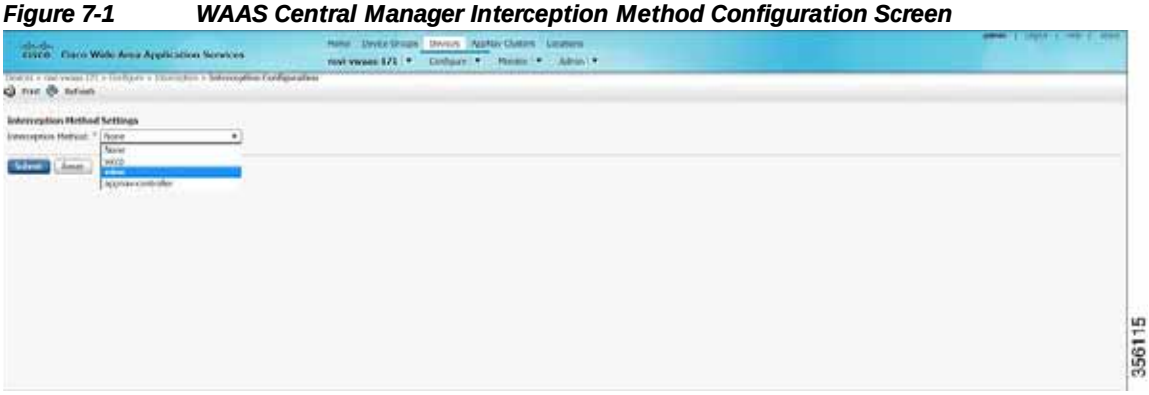
This section contains the following topics:

Configuring Inline Interception with the WAAS Central Manager

To configure inline interception for FTW on ENCS, follow these steps:

Step 1 Navigate to **Devices** > *DeviceName* > **Configure > Interception > Interception Configuration** (Figure 7-1).

Figure 7-1 WAAS Central Manager Interception Method Configuration Screen

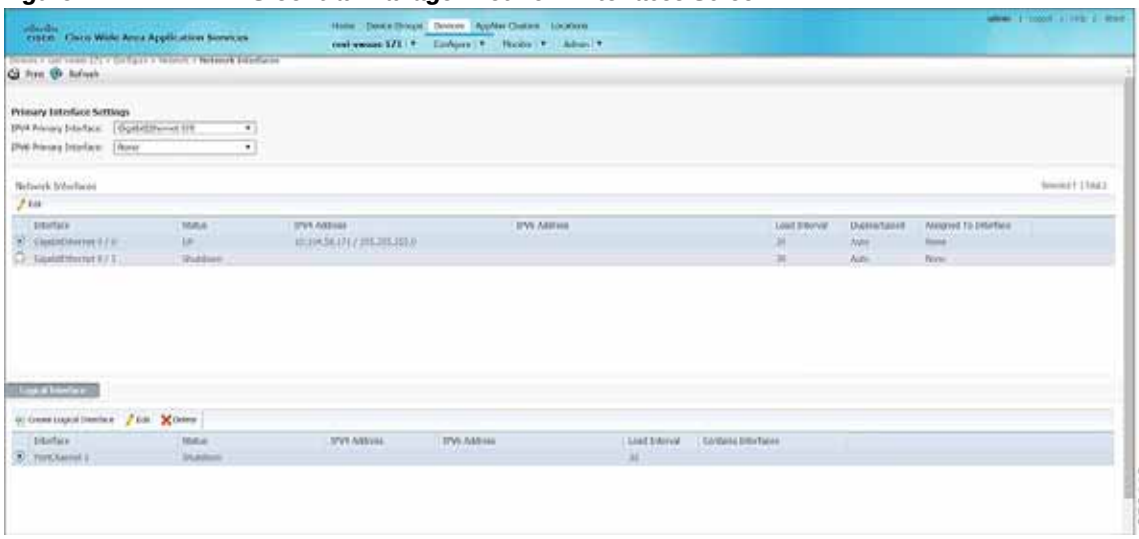


Step 2 At the **Interception Method** drop-down list, choose **Inline**.

Step 3 Click **Submit**.

Step 4 Navigate to **Devices** > *DeviceName* > **Configure > Network > Network Interfaces** (Figure 7-2).

Figure 7-2 WAAS Central Manager Network Interfaces Screen



Step 5 At the **Primary Interface Settings** area, at the **IPv4 Primary Interface** drop-down list, select the interface to be the primary interface.

Step 6 At the **IPv6 Primary Interface** drop-down list, select **None**.

Step 7 For information on the **Network Interface** table listing, see the "Configuring Network Settings" chapter, section "Configuring Network Interfaces," of the *Cisco Wide Area Application Services Configuration Guide*.

Step 8 For information on the **Logical Interface** table listing, see the "Configuring Network Settings" chapter, section "Configuring Network Interfaces," of the *Cisco Wide Area Application Services Configuration Guide*.

Configuring Inline Interception with the WAAS CLI

Table 7-9 shows the CLI commands used to configure inline interception for FTW on ENCS:

Table 7-9 CLI Commands for Inline Interception

Mode	Command	Description
Global Configuration	**(config) inline failover timeout {1 | 3 | 5 | 25}**	Configures the failover timeout for the inline interfaces. Valid values are 1, 3, 5, or 25 seconds. The default value is 3.
	(config) interception-method inline	Enables inline traffic interception.
	(config) interface InlineGroup *slot/groupnumber*	Configures an inline group interface.
EXEC	**show interface inlinegroup *slot/groupnumber***	Displays the inline group information and the slot and inline group number for the selected interface.

FTW Upgrade/Downgrade Guidelines

Consider the following for upgrading or downgrading a WAAS device with FTW:

- FTW is not supported for vWAAS for WAAS versions earlier than WAAS 6.4.3.
- In a mixed version Cisco WAAS network with FTW, the Central Manager must be running WAAS 6.4.3.

Upgrade/Downgrade Guidelines for vWAAS on ENCS-W

Consider the following for upgrading or downgrading a WAAS device on ENCS:

- You can use the WAAS Central Manager or the CLI to upgrade a vWAAS on ENCS-W device to the following WAAS and NFVIS versions:
  - WAAS Version 6.4.3a and NFVIS 3.10.1
  - WAAS Version 6.4.3 and NFVIS 3.9.1
  - WAAS Version 6.4.1x and NFVIS 3.71

Note If you are running nfvis-371-waas-641a or 641b on an ENCS 5400-W device—Before upgrading NFVIS, upgrade to WAAS Version 6.4.3.

- You can use the Central Manager to upgrade from the device level and the device group level. To use the Central Manager to upgrade a vWAAS on ENCS-W device:
  1. Telnet to the vWAAS device.
  2. Update the Central Manager IP address.
  3. Login to the Central Manager.
- The Central Manager supports downgrade of all *applicable* device types in a device group.

  For example, if you are downgrading a device group that has a physical WAE, a virtual WAE, and an ENCS platform to a version earlier than WAAS Version 6.4.1, the Central Manager will initiate the downgrade process only for the physical and virtual WAEs, but not for the ENCS platform.
- For upgrade/downgrade guidelines for vWAAS on NFVIS, see the chapter “Cisco vWAAS with Cisco Enterprise NFVIS,” section Upgrade Guidelines for vWAAS with NFVIS.