Configuring the Cisco WAAS Container

The Cisco Wide Area Application Services (Cisco WAAS) container is a powerful WAN optimization acceleration solution.

Note In this chapter, ISR-WAAS device refers to the router and ISR-WAAS container refers to the container.

Prerequisites for Installing an ISR-WAAS Container

Before you install a Cisco WAAS container, you must configure the following in Prime Infrastructure:

Note Ensure that the name of the ISR-WAAS container does not exceed 22 characters.

Cisco WAAS Central Manager Integration

To manage thee ISR-WAAS with the Cisco WAAS Central Manager, you must register with the Cisco WAAS Central Manager. Registration of ISR-WAAS with Cisco WAAS Central Manager can be done either from the ISR-WAAS CLI, or from the Cisco WAAS Central Manager GUI, or while activating the ISR-WAAS through Prime Infrastructure. The WCM periodically polls the Cisco 4451-X Integrated Services Router (ISR) to retrieve the current status information and perform configuration synchronization.

Cisco WAAS Central Manager Integration

A typical Cisco WAAS deployment consists of both Prime Infrastructure and Cisco WAAS Central Manager applications. Cisco WAAS Central Manager IP is used during ISR-WAAS activation. After ISR-WAAS is activated, it registers with Cisco WAAS Central Manager. Prime Infrastructure needs the IP address of WCM for the following reasons:

- To inform Cisco WAAS Central Manager of the new Cisco ISR-WAAS

- For cross-launching Cisco WAAS Central Manager GUI for monitoring purposes

Note   Cisco WAAS Central Manager configuration is a one-time configuration. The Cisco WAAS Central Manager IP address is required for Prime Infrastructure to authenticate itself to Cisco WAAS Central Manager, and is configured in Prime Infrastructure using the Settings menu.

Note   If Cisco WAAS Central Manager IP is not configured in Prime Infrastructure, the newly activated ISR-WAAS will not be registered with Cisco WAAS Central Manager.

To configure the Cisco WAAS Central Manager IP address in Prime Infrastructure:

Step 1   Choose **Administration > System Settings**.

Step 2   Click **Service Container Management**.

Step 3   Enter the IP address in the **WCM IP Address** text box.

Step 4   Click **Save**.

WCM can be deployed under the following condition:

Prime Infrastructure works only with the active Cisco WAAS Central Manager that is configured in Prime Infrastructure.

After a Cisco WAAS Central Manager failover, one of the following must take place for Prime Infrastructure-Cisco WAAS Central Manager interworking to operate properly again:

- Prime Infrastructure is reconfigured with the IP address of the new Cisco WAAS Central Manager.

- The failed Cisco WAAS Central Manager must become active.

Configuring Single Sign-On

Configuring the Single Sign-On (SSO) feature provides a seamless method to launch Cisco WAAS Central Manager from Network Control System using the existing Prime Infrastructure 2.0 Single Sign-On functionality.

To configure SSO:

Step 1   Choose **Administration > User, Roles, AAA > SSO Servers**.

Step 2   Select **Add SSO Server** from the drop-down list on the right side of the pane.

Step 3   Enter the Prime Infrastructure IP address and click **GO**.

Step 4	Click **Save**.
Step 5	Select **AAA Mode Settings**.
Step 6	Select the **SSO** radio button.
Step 7	Select the **Enable fallback to local** check box.
Step 8	Click **Save**.
Step 9	Configure the WCM IP address. For information on how to configure the WCM IP address, see the Cisco WAAS Central Manager Integration, page 20-1.
Step 10	After you configure the IP address, log out of Prime Infrastructure and log in to WCM and create a username.

Creating a Username in Cisco WAAS Central Manager

Step 1	Log in to WCM.
Step 2	Choose **Home > Admin > AAA > Users**.
Step 3	Click **Create**.
Step 4	Enter a username that matches the Prime Infrastructure username.
Step 5	Choose **Role Management** and click **admin** to assign a RBAC role to create a user account.
Step 6	Choose **Domain Management** and assign a role and domain.
Step 7	Click **Submit**.
Step 8	Choose **Devices > Configure > AAA > NCS Single Sign-On**.
Step 9	Check the **Enable NCS Single Sign-On** check box and enter the CAS/SSO server URL.
Step 10	Click **Submit** to create the certificate.
Step 11	Click **Submit** after the certificate is created.

Cross-Launching Cisco WAAS Central Manager

You can cross-launch Cisco WAAS Central Manager in the following ways:

- Cross-Launching Cisco WAAS Central Manager on a Single Device, page 20-3
- Cross-Launching Cisco WAAS Central Manager on Multiple Devices, page 20-4

Cross-Launching Cisco WAAS Central Manager on a Single Device

To cross-launch the Cisco WAAS Central Manager from the Device Work Center:

Step 1	Choose **Operate > Device Work Center**.
Step 2	Select the ISR-WAAS device.
	The device details are displayed in the pane below.

Step 3   Click the **Service Container** tab.

Step 4   Select the corresponding ISR-WAAS container and click **Launch WCM**.

Cross-Launching Cisco WAAS Central Manager on Multiple Devices

To cross-launch from the Deployed Services:

Step 1   Choose **Operate** > **Deployed Services**.

Step 2   Select the corresponding ISR-WAAS container and click **Launch WCM**.

Note   The Cisco ISR-WAAS Container Lifecycle enables a user to install, uninstall, activate, or deactivate the service container.

Defining Interface Roles

You can define interface roles in **Design** > **Shared Policy Objects** > **Interface Role**. For more information on creating interface roles, see the Creating Interface Roles, page 8-20. Policy objects enable users to define logical collections of elements. Policy Objects are reusable, named components that can be used by other objects and policies. The Shared Policy Objects also eliminate the need to define a component each time you define a policy. For more information on Shared Policy Objects, see the Creating Shared Policy Objects, page 8-20.

Importing an OVA image

To import an OVA image for an ISR-WAAS container:

Step 1   Choose **Operate** > **Service Catalogue**.

Step 2   Select an OVA image from one of the following locations:

- URL
- File

Step 3   Click **Submit** to import the image into Prime Infrastructure.

Step 4   Click **Refresh** to view the imported image in the **Service Catalogue** > **ISR-WAAS** folder.

Configuring Cisco AppNav Automatically During ISR-WAAS Container Activation

A Cisco WAAS container can be configured in two different ways depending on whether you want to configure it on a single router (Installing an ISR-WAAS Container on a Single Router, page 20-6) or multiple routers (Installing an ISR-WAAS Container on Multiple Routers, page 20-6).

Installation of the ISR-WAAS container can be done in two ways. You can either install the container and activate it later, or you can install and activate the container at the same instance.

> ✎
> **Note**   Ensure that the name of the ISR-WAAS container does not exceed 22 characters.

Installing an ISR-WAAS Container

To install an ISR-WAAS container:

Step 1   Choose **Operate** > **Service Catalogue** to import an OVA image. For information on how to import an OVA image, see the Defining Interface Roles, page 20-4.

Step 2   After importing, click **Refresh** to view the imported image.

Step 3   Click **Deploy**.

Step 4   In the Network Deploy Wizard page, select the ISR-WAAS device on which you want to configure the container.

Step 5   Choose the **Install** option and select a Resource Profile from the drop-down list.

Step 6   Click **OK** to install the ISR-WAAS container.

> ✎
> **Note**   To successfully install and activate an ISR-WAAS, you need to have enough memory for each resource profile. For ISR-WAAS-750, you need 4194304 KB memory and two CPUs, for ISR-WAAS-1300, you need 6291456 KB memory and four CPUs, and for ISR-WAAS-2500, you need 8388608 KB memory with six CPUs.

Installing and Activating an ISR-WAAS Container

To install and activate a ISR-WAAS container:

Step 1   Choose **Operate** > **Service Catalogue** to import an OVA image. For information on how to import an OVA image, see the Defining Interface Roles, page 20-4.

Step 2   After importing, click **Refresh** to view the imported image

Step 3   Click **Deploy**.

Step 4   In the Network Deploy wizard screen, select the device on which you want to configure the container

Step 5   Choose the **Install and Activate** option.

Step 6   Choose a Resource Profile from the drop-down list.

Step 7   Select the **Redirect Traffic to WAAS-XE with AppNav-XE** check box.

Step 8   Click **OK** to install and activate the ISR-WAAS container.

Note   Once the ISR-WAAS is installed and activated, the Cisco AppNav configuration is automatically configured.

Note   To successfully install and activate a ISR-WAAS, you should at least have 8 GB RAM in the router for the 750 resource profile.

Installing an ISR-WAAS Container on a Single Router

To install an ISR-WAAS container on a single router:

Step 1   Choose **Operate > Device Work Center**.

Step 2   From the list that is displayed, choose the router on which you want to install the ISR-WAAS container.

Step 3   Click the **Service Container** tab.

Step 4   Click **Add** and enter the configuration details in each field. For information about the field descriptions, see the *Cisco Prime Infrastructure 2.0 Reference Guide*.

Step 5   Click **OK**.

Installing an ISR-WAAS Container on Multiple Routers

To install an ISR-WAAS container on multiple routers:

Step 1   Choose **Operate > Service Catalogue**.

Step 2   Select the ISR-WAAS folder that contains the imported OVA image.

Step 3   Click **Deploy**.

From the list that is displayed, select the routers on which you want to install the ISR-WAAS container.

After you deploy, you can either click **Install** (Installing an ISR-WAAS Container, page 20-5) or **Install and Activate** (Installing and Activating an ISR-WAAS Container, page 20-5)

Step 4   If you choose **Install and Activate**, enter the following details in the Value Assignment area:

  – Enter the ISR-WAAS IP Address/Mask

  – Enter the Router IP/ Mask

  – Enter the Storage Location.

  – Enter a Service Container name

  – Select a Resource Profile

Step 5 Click **OK**.

Uninstalling and Deactivating a Cisco WAAS Container

You can deactivate a Cisco WAAS Container either from the Device Work Center or from the Deployed Services. From the Device Work Center, you can deactivate a single ISR-WAAS container, but from the Deployed Services, you can deactivate multiple ISR-WAAS containers.

Uninstalling a Single Cisco ISR-WAAS Container

To uninstall a single ISR-WAAS container from the Device Work Center:

Step 1 Choose **Operate > Device Work Center**.

Step 2 From the list that is displayed, select the router from which you want to uninstall the Cisco WAAS container by clicking it.

Step 3 Click the **Service Container** tab in the bottom pane.

Step 4 Click **Uninstall**.

Step 5 Click **OK**.

Uninstalling a Multiple Cisco ISR-WAAS Container

To uninstall multiple a Cisco ISR-WAAS containers from the Deployed Services:

Step 1 Choose **Operate > Deployed Services**.

Step 2 From the list that is displayed, select the routers from which you want to uninstall the Cisco WAAS containers by clicking them.

Step 3 Click **Uninstall**.

Step 4 Click **OK**.

Note When a Cisco WAAS virtual appliance is uninstalled through Prime Infrastructure, the corresponding Cisco AppNav configuration is removed.

Deactivating a Cisco ISR-WAAS Container

You can deactivate a Cisco ISR-WAAS container in the following two ways:

Deactivating a Single Cisco ISR-WAAS Container

To deactivate a single Cisco ISR-WAAS container from the Device Work Center:

Step 1   Choose **Operate > Device Work Center**.

Step 2   Select a Cisco ISR-WAAS device name from the device group list.

Step 3   Click the **Service Container** tab.

Step 4   Click **Deactivate**.

Deactivating Multiple Cisco ISR-WAAS Containers

To deactivate multiple Cisco WAAS containers from the Deployed Services:

Step 1   Choose **Operate > Deployed Services**.

Step 2   Select multiple ISR-WAAS device names from the list.

Step 3   Click **Deactivate**.