

Deploying Cisco IOx Applications on Cisco Catalyst IE9300 Rugged Series Switches

First Published: 2024-02-28

Last Modified: 2026-06-11

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2024–2026 Cisco Systems, Inc. All rights reserved.

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT 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 THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

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/c/en/us/about/legal/trademarks.html. 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. (1721R)

Communications, services, and additional information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.



CONTENTS

Full Cisco Trademarks with Software License iii

Communications, services, and additional information iv

Cisco Bug Search Tool iv

Documentation feedback iv

CHAPTER 1 **Cisco IOx Applications on Cisco Catalyst IE Switches** 1

Cisco IOx Application Framework 1

Capabilities of Cisco IOx Application 1

Manage Cisco IOx Application 1

CHAPTER 2 **Configure the Network for IOx Applications** 3

Connections from IE9300 Switch to IOx Applications 3

Workflow to Connect and Manage the VLAN 4

Configure a VLAN for the IOx Interface 4

Configure an SVI address for the VLAN 5

Enable IOx Application in the Switch 5

Verify the IOx Infrastructure 6

CHAPTER 3 **IOx Applications Deployment on the Switch** 7

Introduction to IOx Application Management on IE9300 Switch 7

Guidelines for IOx Applications Deployment 7

Limitations for IOx Application Deployment 8

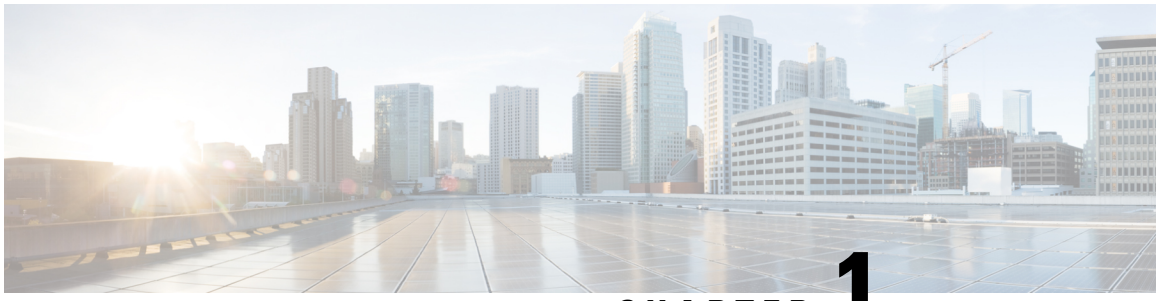
Methods of IOx Applications Deployment 8

Resource Profile Options in Cisco IOx Local Manager 8

Deployment of IOx Application Using the IOS-XE CLI 9

Configure IOx Application Using CLI 9
Configure Docker Runtime Options for IOx Applications 10
Configure Application Resource Profiles for Application Hosting 11
Install, Activate, and Start the IOx Application on the Switch 12
Cisco IOx Application Signature Verification and Automatic Activation 12
Signature Verification Management and Status Check 13
Display Maximum Resource Allocation for Application 14
Resources Available in the Switch After IOx Application Configuration 14
Display Application Information in the Switch 14
Stop, Deactivate, and Uninstall IOx Application on the Switch 15
Display App-Hosting Commands 16
Deploy an IOx Application using Cisco IOx Local Manager 16
IOx on IE9300 Stacked Environment 17

CHAPTER 4 **IOx Guest Shell** 19
Overview of Guest Shell 19
Prerequisites 19
Enable Guest Shell 20
Show commands 22



CHAPTER 1

Cisco IOx Applications on Cisco Catalyst IE Switches

- Cisco IOx Application Framework, on page 1
- Capabilities of Cisco IOx Application, on page 1
- Manage Cisco IOx Application, on page 1

Cisco IOx Application Framework

Cisco IOx is an end-to-end application framework that merges Cisco IOS-XE with Linux to offer secure hosting for applications on Cisco network platforms. This integrated framework allows the deployment of applications directly within the network infrastructure and provides secure management through Cisco application hosting tools.

From Cisco IOS XE Cupertino 17.8.1, Cisco Catalyst IE9300 Rugged Series Switches support IOx application hosting. This feature allows you to run your custom code, applications, and containers directly on the Cisco Catalyst IE9300 Rugged Series Switches.

See Cisco IOx page for more information.

Capabilities of Cisco IOx Application

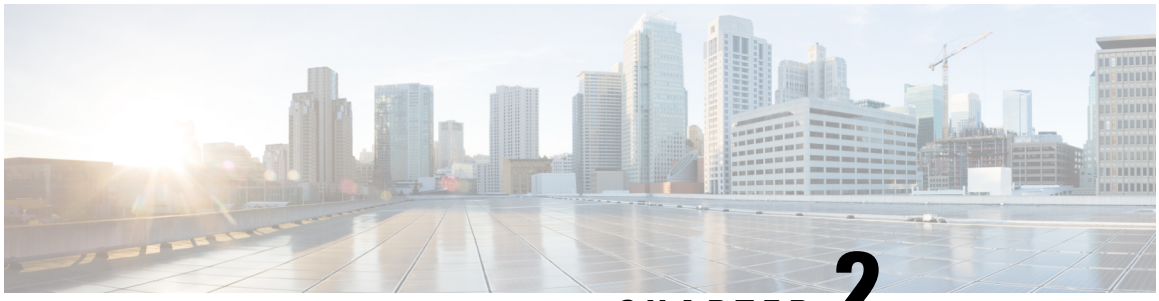
- **Application Deployment**: Provides consistent deployment capabilities, independent of network infrastructure variations.
- **Development Support**: Enhances development flow with Docker tooling support.
- **Data Management**: Offers options for backing up and restoring data using the Docker framework.
- **System Maintenance**: Facilitates system upgrades and allows access to logs for troubleshooting.

Manage Cisco IOx Application

Cisco IOx can be managed using:

- the graphical UI for comprehensive on-premises or cloud-based management.

- the on-device CLI for more direct, hands-on management.



CHAPTER 2

Configure the Network for IOx Applications

- Connections from IE9300 Switch to IOx Applications , on page 3
- Workflow to Connect and Manage the VLAN, on page 4

Connections from IE9300 Switch to IOx Applications

The IE9300 switch has an additional interface known as Ap1/0/1, which can be configured as a standard physical interface in trunk mode for connectivity with IOx applications.

Prerequisites for Establishing a Connection Between IE9300 Switch and Cisco IOx Applications

- Configure a VLAN ID for the Ap1/0/1 interface, regardless of trunk mode.

  Ensure that the configured VLAN is not the default VLAN. By default, VLAN 1 serves as the native VLAN and carries untagged packets.

- Assign an IP address to an IE9300 VLAN interface that is also a member of the Ap1/0/1 trunk interface.

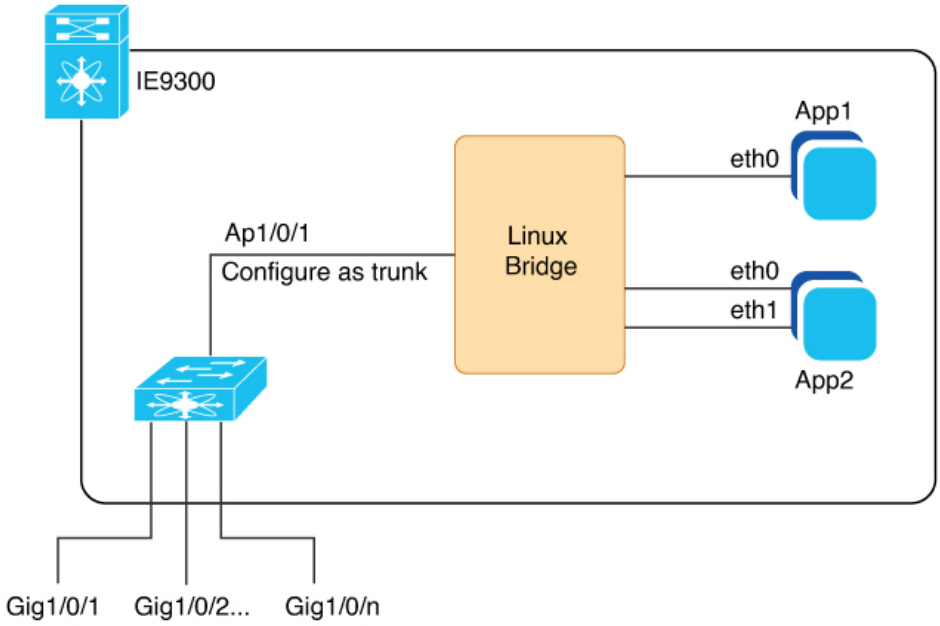


Note The VLANs on the Ap1/0/1 trunk interface should match VLANs (including management VLANs) that carry data traffic between applications on IOx. For example, if VLAN 10 carries traffic between application and network, including management IP traffic, use the same VLAN for managing applications.

If you intend to use vlan 1 to communicate with the network, then choose a different native VLAN on Ap1/0/1.

After configuring the network, enable IOx in the switch. For more information, see Enable IOx Application in the Switch section.

Figure 1: Connections with IE9300 IOx Network with Applications



This image depicts the Ethernet and Layer 2 connections within an IOx-enabled network on a Cisco Catalyst IE9300 Rugged Series Switch. The additional interface, Ap1/0/1, is internally connected to a Linux bridge and is configured as a trunk to support multiple IOx applications.

The IOx applications can maintain several Ethernet connections and be assigned to any VLAN as required.

See Deployment of IOx Application Using the IOS-XE CLI for an illustration showing a sample network configuration in this guide.

Workflow to Connect and Manage the VLAN

To connect and manage the VLAN, complete all these procedures in given order:

Configure a VLAN for the IOx Interface

Note VLAN ID must be configured on the Ap1/0/1 interface, regardless of its trunk mode configuration. Also, verify that the VLAN is routable throughout the network.

Procedure

Step 1 Enter global configuration mode.

```
Device# configure terminal
```

Step 2 Enter interface configuration mode.

```
Device(config)# interface Ap1/0/1
```

Step 3 Configure allowed VLANs on the trunk.

```
Device(config-if)#switchport trunk allowed vlan 10
```

Step 4 Configure the interface to operate in trunk mode.

```
Device(config-if)#switchport mode trunk
```

Step 5 Exit interface configuration mode.

```
Device(config-if)#end
```

Configure an SVI address for the VLAN

Procedure

Step 1 Enter global configuration mode.

```
Device# configure terminal
```

Step 2 Enter VLAN interface configuration mode.

```
Device(config)# interface vlan 10
```

Step 3 Assign an IP Address to the VLAN Interface.

```
Device(config-if)#ip address 192.168.0.1 255.255.255.0
```

Step 4 Exit interface configuration mode.

```
Device(config-if)#end
```

Enable IOx Application in the Switch

Before you begin

- Verify that you have at least 1 GB on the SD card. If you have a 4 GB SD card partition for IOx, you can format up to 74 percent of the card.
- Verify that you have configured the VLAN for the IOx interface.

Procedure

Step 1 Format the SD card IOx partition with EXT4 filesystem.

```
Device# partition sdflash: iox
Partitioning IOS:IOX(34%:66%) Default
Partition command reloads the switch, Continue?[confirm]
Please make sure to back-up "sdflash:" contents
Partition operation will destroy all data in "sdflash:". Continue? [confirm]
```

Note
The partition command allocates 66 percent of space on the SD card to IOx and 34 percent to IOS as a backup.

After you enter the partition command, the switch reloads.

Step 2 Enter global configuration mode.

```
Device# configure terminal
```

Step 3 Enable IOx.

```
Device(config)#iox
Warning: Do not remove SD flash card when IOx is enabled or errors on SD device could occur.
*Feb 21 12:49:18.310: %UICFGEXP-6-SERVER_NOTIFIED_START: R0/0: psd: Server iox has been notified
to start
*Feb 21 12:49:48.165: %IM-6-IOX_ENABLEMENT: R0/0: ioxman: IOX is ready.
```

Step 4 Enable the web server.

```
Device(config)# ip http secure-server
```

Step 5 Create a user account for access.

```
Device(config)# username admin privilege 15 password 0 secret
```

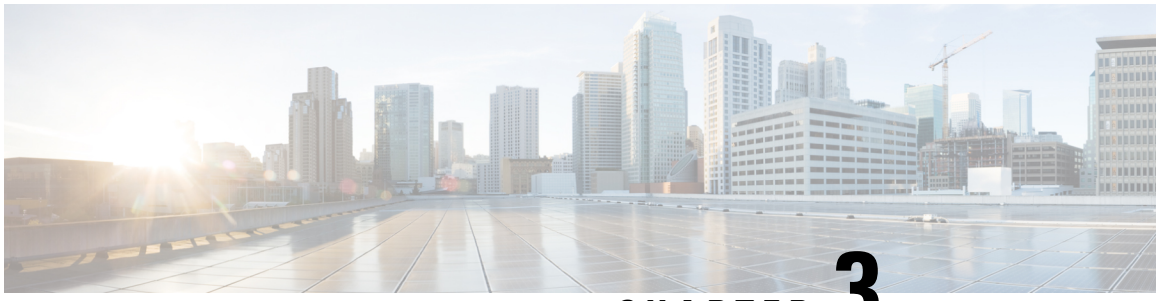
Step 6 Save the configuration and returns to privileged EXEC mode.

```
Device(config)# end
```

Verify the IOx Infrastructure

Verify that the IOx infrastructure is ready to use, as shown here.

```
Device#show iox-service
IOx Infrastructure Summary:
---------------------------
IOx service (CAF) : Running
IOx service (HA) : Running
IOx service (IOxman) : Running
IOx service (Sec storage) : Running
Libvirtd 5.5.0 : Running
Dockerd v19.03.13-ce : Running
```



CHAPTER 3

IOx Applications Deployment on the Switch

- Introduction to IOx Application Management on IE9300 Switch, on page 7
- Guidelines for IOx Applications Deployment, on page 7
- Limitations for IOx Application Deployment, on page 8
- Methods of IOx Applications Deployment, on page 8
- Resource Profile Options in Cisco IOx Local Manager, on page 8
- Deployment of IOx Application Using the IOS-XE CLI, on page 9
- Deploy an IOx Application using Cisco IOx Local Manager, on page 16
- IOx on IE9300 Stacked Environment, on page 17

Introduction to IOx Application Management on IE9300 Switch

The most commonly used IOx applications are Cisco Cyber Vision and iPerf. Cisco Catalyst IE9300 Rugged Series Switches support both LXC and Docker-based applications that utilize ARM64 architecture, offering a range of deployment options. The IE9300 switches are designed to accommodate IPv4 and IPv6 configurations, allowing for flexible network integration.

The IOx application framework provides configuration options for Docker runtime settings and supports configuring multiple guest or Layer 2 interfaces (ranging from 0 to 63) for each application. Each Layer 2 interface can be assigned to a distinct VLAN, enhancing network organization and segmentation.

Guidelines for IOx Applications Deployment

- Place the application package or tar file in the flash or SD card storage within the IOS partition.
- Use interface Ap1/0/1 on the IE9300 switch to forward Layer 2 application traffic. Verify that the interface is active and configured as a trunk port.
- Use interface Ap1/0/1 on the IE9300 switch to configure Layer 2 interfaces and assign a VLAN with an IP address within the same VLAN network. Next, configure gateway interfaces with an SVI or an IP address in the same network.

Limitations for IOx Application Deployment

- Only up to three gateway interfaces are permitted per-application configuration.
- Only one default gateway can be configured to support all interfaces.

Methods of IOx Applications Deployment

The Cisco Catalyst IE9300 Rugged Series Switch supports these two methods for deploying IOx applications.

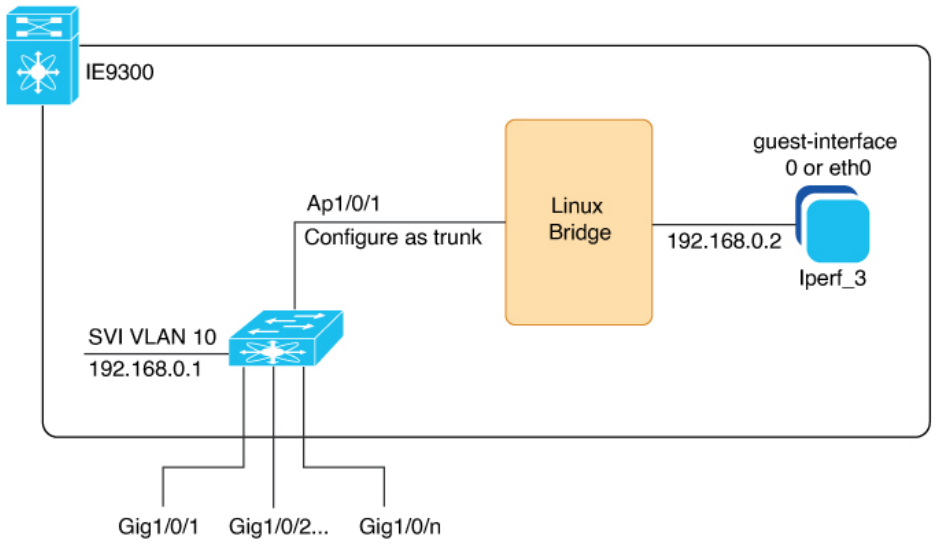
- Deploy IOx application using IOS-XE Command-Line Interface (CLI).
- Deploy IOx application using Cisco IOx Local Manager (GUI).

Resource Profile Options in Cisco IOx Local Manager

- The Cisco IOx Local Manager provides several resource profiles, such as:
  - tiny
  - exclusive
  - default, and
  - custom.
- The custom profile allows you to adjust CPU, memory, and disk allocations according to the specific requirements of your IOx application.

Deployment of IOx Application Using the IOS-XE CLI

Figure 2: Example of IOx Deployment with Application



The configuration example here depicts a typical IOx application deployment on a Cisco Catalyst IE9300 Rugged Series Switch. The interface Ap1/0/1 is internally linked to a Linux bridge and set up as a trunk to facilitate multiple IOx applications. The application "Iperf_3" is assigned the IP address 192.168.0.2 on its guest interface. And the default gateway for the network is configured on the Switch Virtual Interface (SVI) VLAN 10, using the IP address 192.168.0.1.

See Connections from IE9300 Switch to IOx Applications , on page 3 for an illustration without interface examples in this guide.

Configure IOx Application Using CLI

Before you begin

Verify that you have configured the network for IOx, as described in the Connections from IE9300 Switch to IOx Applications , on page 3 section.

Procedure

Step 1 Enter global configuration mode.

```
Device# configure terminal
```

Step 2 Configure an application name and enter application-hosting configuration mode.

```
Device(config)# app-hosting appid iperf_3
```

Step 3 Configure AppGigabitEthernet trunk.

```
Device(config-app-hosting)#app-vnic AppGigabitEthernet trunk
```

Step 4 Configure a VLAN guest interface. This configuration places Eth0 into VLAN 10.

```
Device(config-config-app-hosting-trunk)#vlan 10 guest-interface 0
```

Step 5 Configure a static IP address.

- IPv4

  ```
  Device(config-config-app-hosting-vlan-access-ip)#guest-ipaddress 192.168.0.2 netmask 255.255.255.0
  ```

- IPv6

  ```
  Device(config-config-app-hosting-vlan-access-ip)#guest-ipv6address 2001::1 prefix 64
  ```

Step 6 Exit sub-interface mode.

```
Device(config-config-app-hosting-vlan-access-ip)#exit
```

Step 7 Exit app hosting trunk sub-interface mode.

```
Device(config-config-app-hosting-trunk)#exit
```

Step 8 Configure the default gateway for the application. Use the VLAN ID interface of the switch as the gateway.

```
Device(config-app-hosting)#app-default-gateway 192.168.0.1 guest-interface 0
```

Note
Supports up to three gateways.

Step 9 Save the configuration and return to privileged EXEC mode

```
Device(config-if)#end
```

Configure Docker Runtime Options for IOx Applications

Before you begin

- **Set Up Runtime Options:** You can configure up to 30 separate lines of Docker runtime options for IOx applications. The system compiles these options into a single string, proceeding from line 1 through line 30. Each string may contain multiple Docker runtime options.
- **Apply Changes to Runtime Options:** To apply changes to the runtime options, first stop the application, then deactivate it, reactivate it, and finally restart it. This process guarantees the correct implementation of the new runtime options.

Procedure

Step 1 Enter global configuration mode.

```
Device# configure terminal
```

Step 2 Configure an application name and enter application-hosting configuration mode.

```
Device(config)# app-hosting appid iperf_3
```

Step 3 Enter application-hosting Docker-configuration mode.

```
Device(config-app-hosting)#app-resource docker
```

Step 4 Specify the Docker run time options.

```
Device(config-app-hosting-docker)#run-opts 1 "--entrypoint '/bin/sleep 10000'"
```

Step 5 Exit application-hosting Docker-configuration mode.

```
Device(config-app-hosting-docker)#exit
```

Step 6 Save the configuration and return to privileged EXEC mode

```
Device(config-if)#end
```

Configure Application Resource Profiles for Application Hosting

Before you begin

- Activate the application hosting, before making resource changes.
- Check the memory and storage using **show app-hosting resource** command.

Procedure

Step 1 Enter global configuration mode.

```
Device# configure terminal
```

Step 2 Configure an application name to enter application-hosting configuration mode.

```
Device(config)# app-hosting appid iperf_3
```

Step 3 Configure the custom application resource profile.

```
Device(config-app-hosting)#app-resource profile custom
```

Note
The system supports only custom profile name.

Step 4 Configure the CPU resources.

```
Device(config-app-resource-profile-custom)#cpu 500
```

Step 5 Allocate memory for the application in megabytes.

```
Device(config-app-resource-profile-custom)#memory 256
```

Step 6 Assign persistent disk space for the application, in megabytes.

```
Device(config-app-resource-profile-custom)#persist-disk 256
```

Step 7 Save the configuration and return to privileged EXEC mode

```
Device(config-if)#end
```

Install, Activate, and Start the IOx Application on the Switch

Before you begin

Verify that you have configured the network and the IOx application, as described in the Configure the Network for IOx Applications section.

Procedure

Step 1 Install the application and move it into the deployed state.

```
Device#app-hosting install appid iperf_3 package flash:iperf_3_eft_dockerimage_aarch.tar
Installing package 'flash:iperf_3_eft_dockerimage_aarch.tar' for 'iperf_3'. Use 'show app-hosting
list' for progress
```

Note
During installation, the application's signature is verified if signature verification is enabled, as described in the Cisco IOx Application Signature Verification and Automatic Activation section.

Step 2 (Optional) Enter this show command to check the state of the IOx application.

```
switch #show app-hosting list
App id                                   State
---------------------------------------------------------
iperf_3                                  DEPLOYED
```

Step 3 Allocate resources and activate the application.

```
Device# app-hosting activate appid iperf_3
Current state is: ACTIVATED
```

Step 4 Start the IOx application.

```
Device# app-hosting start appid iperf_3
iperf_3 started successfully
Current state is: RUNNING
```

Cisco IOx Application Signature Verification and Automatic Activation

IOx infrastructure checks the signature verification of a Cisco IOx application during its installation. The application package signature ensures the validity of the package and confirms that the installed application on the device comes from a trusted source.

Conditions for Signature Verification

IOx infrastructure checks for a signature under these circumstances:

- when signature verification is enabled.
- when IOx infra uses bootflash as storage, then it checks for a signature regardless of signature verification status.
- the application utilizes a restricted resource, such as secure storage.

If signature verification is enabled, and the application lacks a signature, the system prevents the application from running.

Conditions to Run Unsigned Non-Cisco Applications

The system does not permit non-Cisco applications to operate without enabling signature verification. However, the system permits unsigned non-Cisco applications to run if:

- signature verification is disabled.
- the application uses an SD card for storage, or.
- the application is not using a restricted resource.

Automated Activation and Startup of Applications with the Start Keyword

The system provides a start keyword option under the application-hosting configuration. When this start keyword is used, the IOx infrastructure automatically activates and starts the application after installation. If the start keyword is not used, manual activation and startup are required using the activate and start commands.

Signature Verification Management and Status Check

Procedure

Step 1 To enable signature verification, use this command.

```
Device#app-hosting verification enable
```

Step 2 (Optional)To disable signature verification, use this command.

```
Device#app-hosting verification disable
```

Step 3 (Optional)To check whether signature verification is enabled or disabled, use this command.

```
Device# show app-hosting infra
IOX version: 2.7.0.0
App signature verification: disabled
Internal working directory: /mnt/usb0/iox
Application Interface Mapping
AppGigabitEthernet Port # Interface Name Port Type Bandwidth
1 AppGigabitEthernet1/0/1 KR Port - Internal 1G
CPU:
Quota: 33(Percentage)
Available: 26(Percentage)
```

```
Quota: 1000(Units)
Available: 800(Units)
```

Note
You can enable or disable sign verification at any time regardless of any installed application states.

Display Maximum Resource Allocation for Application

To display the maximum resources allocated to an application in the switch, use this command:

```
Device# show app-hosting resource
CPU:
  Quota: 33(Percentage)
  Available: 0(Percentage)
VCPU:
  Count: 2
Memory:
  Quota: 862(MB)
  Available: 0(MB)
Storage space:
  Total: 3668(MB)
  Available: 2849(MB)
```

Resources Available in the Switch After IOx Application Configuration

To view the resources remaining in the switch after IOx application configuration, use this command:

```
Device# show app-hosting infra
IOX version: 2.7.0.0
App signature verification: disabled
Internal working directory: /mnt/usb0/iox
Application Interface Mapping
AppGigabitEthernet Port #  Interface Name    Port Type                   Bandwidth
                           1                 AppGigabitEthernet1/0/1     KR Port - Internal
   1G
CPU:
  Quota: 33(Percentage)
  Available: 0(Percentage)
  Quota: 1000(Units)
  Available: 0(Units)
```

Display Application Information in the Switch

To display detailed application-related information in the switch, use this command:

```
Device# show app-hosting detail appid iperf_3
App id                 : iperf_3
Owner                  : iox
State                  : RUNNING
Application
  Type                 : docker
  Name                 : networkstatic/iperf_3
  Version              : latest
  Description          :
  Author               : Brent Salisbury <brent.salisbury@gmail.com>
  Path                 : bootflash:iperf_3x86.tar
  URL Path             :
```

```
Activated profile name : custom
Resource reservation
  Memory               : 500 MB
  Disk                 : 500 MB
  CPU                  : 173 units
  CPU-percent          : 5 %
  VCPU                 : 1
Platform resource profiles
  Profile Name                  CPU(unit)  Memory(MB)  Disk(MB)
  ----------------------------------------------------------------
Attached devices
  Type              Name               Alias
  ---------------------------------------------
  serial/shell     iox_console_shell   serial0
  serial/aux       iox_console_aux     serial1
  serial/syslog    iox_syslog          serial2
  serial/trace     iox_trace           serial3
Network interfaces
   ---------------------------------------
eth0:
   MAC address         : 52:54:dd:67:81:6f
   IPv6 address        : ::
   Network name        : mgmt-bridge300
eth3:
   MAC address         : 52:54:dd:b2:4d:86
   IPv4 address        : 20.1.2.2
   IPv6 address        : ::
   Network name        : VPG0
eth1:
   MAC address         : 52:54:dd:f2:29:67
   IPv4 address        : 10.1.1.2
   IPv6 address        : 2001:1::5054:ddff:fef2:2967
   Network name        : mgmt-bridge-v2340
Docker
------
Run-time information
  Command              :
  Entry-point          : /bin/sleep 10000
  Run options in use   : --entrypoint '/bin/sleep 10000'
  Package run options  :
Application health information
  Status               : 0
  Last probe error     :
  Last probe output    :
```

Stop, Deactivate, and Uninstall IOx Application on the Switch

Procedure

Step 1 To stop the IOx application, use this command.

```
Device# app-hosting stop appid iperf_3
iperf_3 stopped successfully
Current state is: STOPPED
```

Step 2 To deactivate the IOx application, use this command.

```
Device# app-hosting deactivate appid iperf_3
iperf_3 deactivated successfully
Current state is: DEPLOYED
```

Step 3 To uninstall the IOx application, use this command.

```
Device# app-hosting uninstall appid iperf_3
Uninstalling 'iperf_3'. Use 'show app-hosting list' for progress.
```

Display App-Hosting Commands

To display the list of subcommands for the **app-hosting** command, use the command as given here:

```
Device# app-hosting ?
  activate      Application activate  <== to activate app
  clear         Clear console/aux connection     <== to clear console or aux session if
connected
  connect       Application connect              <== to connect the app console or aux or
session once in run state
  data          Application data            <== to upload files to the apps
  deactivate    Application deactivate      <== to deactivate an app
  debug         debug            <== for caf related debug commands
  install       Application install         <== to install app
  move          Move File             <== to move trace or core file
  settings      Application settings        <== to configure app specific setting using
file
  start         Application start           <== to start an app
  stop          Application stop            <== to stop an app
  uninstall     Application uninstall       <== to uninstall an app`
  upgrade       Application upgrade         <== to upgrade app to new version
  verification Application signature verification setting (global)  <== to enable/disable
the sign verification
```

Deploy an IOx Application using Cisco IOx Local Manager

Cisco IOx Local Manager offers a web-based interface for managing, administering, monitoring, and troubleshooting applications on a host system and to perform various related activities.

You can access Cisco IOx Local Manager from the Cisco Catalyst IE9300 Rugged Series Switch web-based UI and use Cisco IOx Local Manager to deploy applications.

Access the Cisco IOx Local Manager Application

- Log in to the Cisco Catalyst IE9300 Rugged Series Switch web-based UI.
- Navigate to **Configuration > IOx**. The IOx option is located under the **Services** section.
- In the Cisco IOx Local Manager, enter your Cisco IOS username and password.
- Click Log In to proceed.

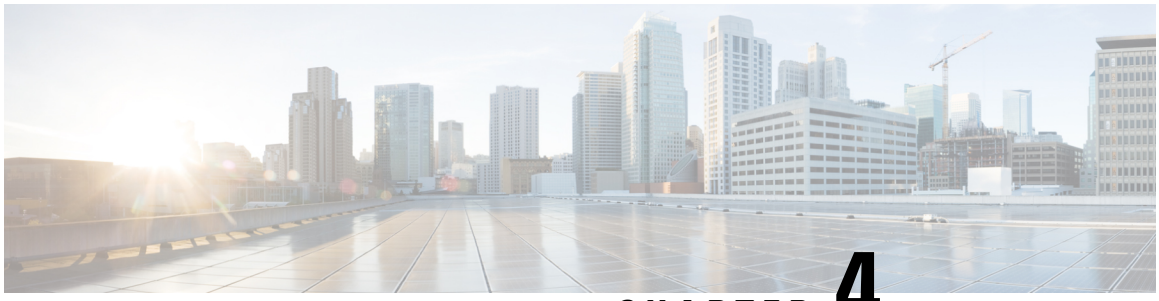
See Cisco IOx Local Manager Reference Guide. page for more information

Note You can access WebUI when the management interface is in a VRF.

IOx on IE9300 Stacked Environment

These are the guidelines for IE9300 stacked environment.

- IOx HA is not supported.
- To enable the iox-service, the SD card is needed on active and member devices.
- When IOx is enabled, the service executes on the Active switch of the stack.
- The IOx service and metadata do not sync with the standby.
- Only the active switch uses sdflash for IOx storage.
- The system syncs app-related configuration with the standby, and after switchover, the apps require a fresh installation.
- On the new active device, if sdflash is not partitioned, disable IOx and partition sdflash as described in Formatting an SD Card and Enabling IOx.



CHAPTER 4

IOx Guest Shell

- Overview of Guest Shell, on page 19
- Prerequisites, on page 19
- Enable Guest Shell, on page 20
- Show commands, on page 22

Overview of Guest Shell

Guest Shell is a built-in, Linux-based container environment on Cisco IOS XE, managed by IOx on the Cisco Catalyst IE9300 Rugged Series Switch. It is designed for operational automation and manageability, such as running Python scripts that interact with Cisco IOS XE. Guest-Shell cannot be used for Data-plane forwarding. The key characteristics include

- Guest Shell is bundled with the Cisco IOS XE system image on supported releases.
- Guest Shell runs as an IOx-hosted Linux container (LXC), sharing the kernel with IOS XE.
- You can install scripts and software packages inside the container.
- Guest Shell does not modify the host IOS XE file system or processes.

Prerequisites

Note Day-0 ZTP-based device provisioning uses Guest Shell and does not require an SD card.

Before you enable Guest Shell on IE9300, verify these prerequisites.

- Cisco IOS XE release on your IE9300 SKU supports Guest Shell and IOx.
- You have privileged EXEC (enable) access to the switch.
- Enable IOx (**iox** in global configuration mode) and verify that IOx services are healthy.
- IOx uses SD card storage when you configure it.You must have at least 4GB of available storage on the SD card.

- Format the SD card with the EXT4 file system.
- Network connectivity for Guest Shell is configured if external access is required (for example, management interface using the **app-vnic management** command).



Note The initial enablement of Guest Shell may take several minutes as the container needs to be provisioned.

Enable Guest Shell

Enable Guest Shell on IOS XE devices so you can run Linux tools and scripts in a secure container environment.

Guest Shell is a built-in, containerized Linux environment on Cisco IOS XE platforms. When enabled, network administrators can use Guest Shell to run custom scripts, conduct local analytics, and improve operational workflows directly on the device.

Before you begin

Ensure you have administrative access to the device.

Verify your device supports IOx and Guest Shell.

Procedure

Step 1 Use the **enable** command to enter privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 Use the **configure terminal** command to enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 3 Use the **iox** command to enable IOx services.

Example:

```
Device(config)# iox
Device(config)# end
Device# write memory
Device# show iox-service
```

Verify that IOx infrastructure services show as running.

Example:

```
Device# show iox

IOx Infrastructure Summary:
---------------------------
IOx service (CAF)              : Running
IOx service (HA)               : Running
IOx service (IOxman)           : Running
IOx service (Sec storage)      : Running
```

```
Libvirtd 5.5.0                 : Running
Dockerd v19.03.13-ce           : Running
Redundancy Status              : Non-Redundant
```

Step 4 Use the **app-hosting appid guestshell** command to configure application hosting for Guest Shell.

Example:

```
Device# configure terminal
Device(config)# app-hosting appid guestshell
Device(config-app-hosting)# app-vnic management guest-interface 0
Device(config-app-hosting)# end
Device# write memory
```

Step 5 Use the **guest shell enable** command to enter the Guest Shell.

Example:

```
Device# guestshell enable
Interface will be selected if configured in app-hosting
Please wait for completion
guestshell installed successfully
Current state is: DEPLOYED
guestshell activated successfully
Current state is: ACTIVATED
guestshell started successfully
Current state is: RUNNING
Guestshell enabled successfully
```

Use the **guestshell disable** command to disable the Guest Shell.

Example:

```
Device# guestshell disable
Guestshell disabled successfully
```

Step 6 Use the **show app-hosting list** command for viewing the list of IOx applications and their states.

Example:

```
Device# show app-hosting list
App id                                   State
---------------------------------------------------------
guestshell                               RUNNING
```

Additionally, you can use the **show app-hosting detail appid guestshell** command to get more information about the guestshell application.

Note
To run commands from IOS XE without entering the shell, use the **guestshell run** command.

Example:

```
Device# guestshell run python3 --version
Python 3.6.8

Device# guestshell run bash -c "uname -a"
Linux guestshell 5.15.178 #1 SMP Mon May 12 10:05:06 UTC 2025 aarch64 aarch64 aarch64 GNU/Linux
```

Note
Use the same method to run any automation scripts you have by executing: **guestshell run bash <myscript.py>**

Step 7 Use the **guestshell run bash** command to enter the bash environment and run commands from within the shell.

Example:

```
Device# guestshell run bash
[guestshell@guestshell ~]$ cat /etc/os-release
```

Step 8 Use the **exit** command to exit out of the shell and return to the IOS-XE.

Example:

```
[guestshell@guestshell ~]$ exit
```

Show commands

Use these show commands to verify IOx and Guest Shell (GS) status on IE9300.

Table 1: Guest Shell status on IE9300

Command	Description
show iox-service	Displays the status of the IOx infrastructure service.
show app-hosting list	Lists the IOx applications and their states.
show app-hosting detail appid guestshell	Displays detailed information about the Guest Shell application.
show guestshell detail	Displays the status and configuration specific to the Guest Shell.
show app-hosting resource	Displays the available CPU, memory, and storage for IOx applications.
show app-hosting infra	Displays IOx infrastructure settings (for example, signature verification).