Initial configuration

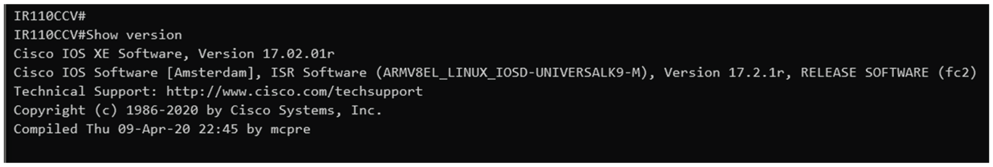
To install Cisco Cyber Vision on the Cisco IR1101, you must perform the Initial configuration which steps are described in this section.

Check the software version

- Check the software version using the following command in the router's CLI:

  ```
  Show version
  ```

  The displayed version must be 17.2.1 or higher to be compatible with the Cisco Cyber Vision Sensor Application.

  ```
  IR110CCV#
  IR110CCV#Show version
  Cisco IOS XE Software, Version 17.02.01r
  Cisco IOS Software [Amsterdam], ISR Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version 17.2.1r, RELEASE SOFTWARE (fc2)
  Technical Support: http://www.cisco.com/techsupport
  Copyright (c) 1986-2020 by Cisco Systems, Inc.
  Compiled Thu 09-Apr-20 22:45 by mcpre
  ```

  If the version is lower, you must update the router firmware. To do so, go to cisco.com and refer to the Cisco IR1101's documentation.

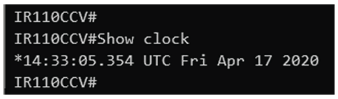
Check date and time

The internal clock of the router must be synchronized and configured properly.

Note The Cisco Cyber Vision IOx sensor application gets the time from the host. Therefore, it is critical that the host synchronizes its time with the Center or a valid NTP server. If the time difference is large (hours or more), the user should adjust the Cisco IR1101 time using the CLI or the WebUI so it is close to the reference time. If not, the synchronization may take many update cycles.

1. Check the date and time using the following command:

   ```
   Show clock
   ```

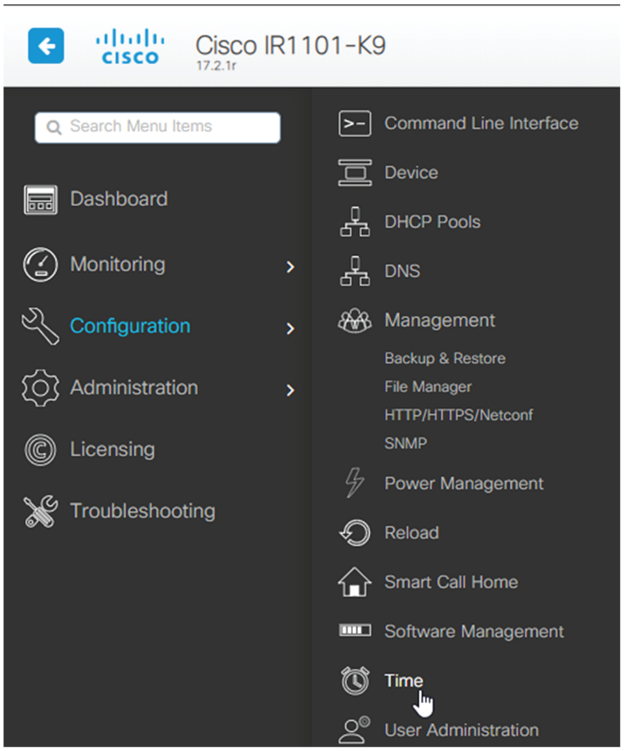
   

   ```
   IR110CCV#
   IR110CCV#Show clock
   *14:33:05.354 UTC Fri Apr 17 2020
   IR110CCV#
   ```

2. If needed, adjust to the UTC time using the following command:

   ```
   clock set [hh:mm:ss] [month] [day] [year]
   ```

Or in the WebUI, navigate to Configuration > Time.



Enable IOx

Before installing the Cisco Cyber Vision sensor on the Cisco IR1101, you must enable IOx.

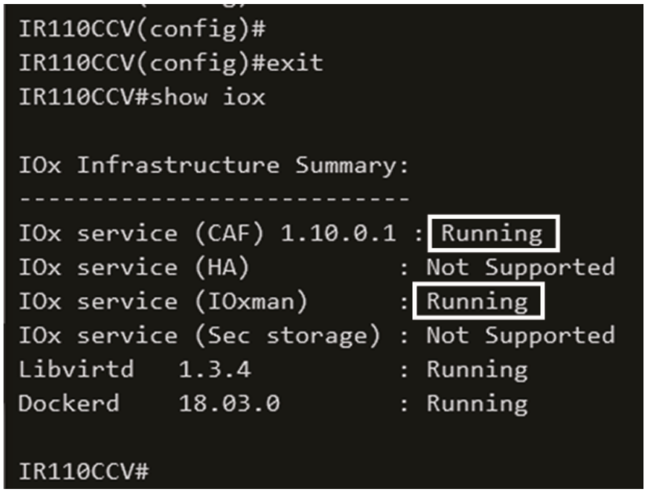
Procedure

Step 1 Enable IOx using the following command.

```
configure terminal
iox
```

Step 2 Check that the CAF and IOxman services are running using the following command.

```
exit
show iox
```



```
IR110CCV(config)#
IR110CCV(config)#exit
IR110CCV#show iox

IOx Infrastructure Summary:
---------------------------
IOx service (CAF) 1.10.0.1 : Running
IOx service (HA)           : Not Supported
IOx service (IOxman)       : Running
IOx service (Sec storage)  : Not Supported
Libvirtd   1.3.4           : Running
Dockerd    18.03.0         : Running

IR110CCV#
```

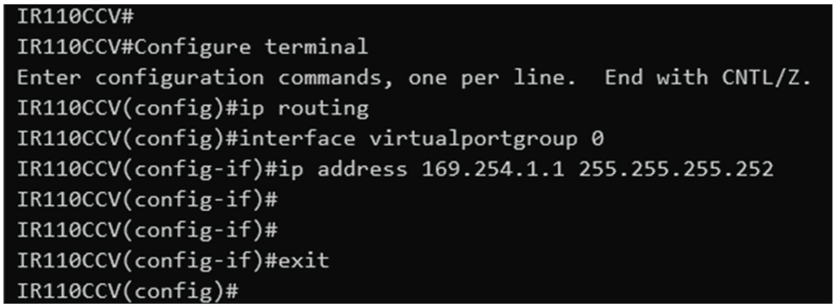
Setup ERSPAN

In order to receive traffic in the Cisco Cyber Vision IOx application, the application:

- must be connected to a VirtualPortGroup,
- must have the correct IP address assigned,
- must have a monitor session created.

1. Connect the application to a VirtualPortGroup and set an IP address using the following commands:

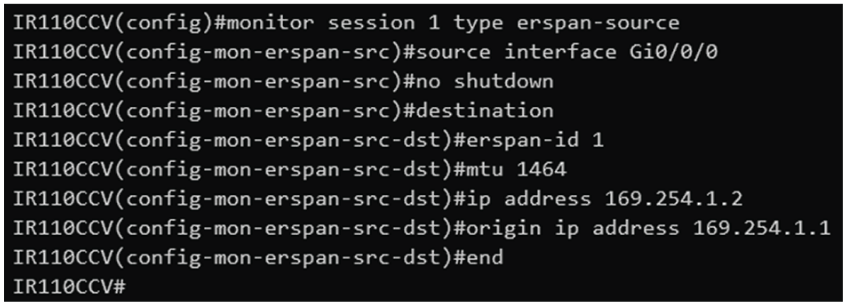
```
Configure terminal
ip routing
interface virtualportgroup 0
ip address 169.254.1.1 255.255.255.252
exit
```



```
IR110CCV#
IR110CCV#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
IR110CCV(config)#ip routing
IR110CCV(config)#interface virtualportgroup 0
IR110CCV(config-if)#ip address 169.254.1.1 255.255.255.252
IR110CCV(config-if)#
IR110CCV(config-if)#
IR110CCV(config-if)#exit
IR110CCV(config)#
```

2. Create the monitor session using the following commands:

```
monitor session 1 type erspan-source
source interface Gi0/0/0
no shutdown
destination
erspan-id 1
mtu 1464
ip address 169.254.1.2
origin ip address 169.254.1.1
end
```



```
IR110CCV(config)#monitor session 1 type erspan-source
IR110CCV(config-mon-erspan-src)#source interface Gi0/0/0
IR110CCV(config-mon-erspan-src)#no shutdown
IR110CCV(config-mon-erspan-src)#destination
IR110CCV(config-mon-erspan-src-dst)#erspan-id 1
IR110CCV(config-mon-erspan-src-dst)#mtu 1464
IR110CCV(config-mon-erspan-src-dst)#ip address 169.254.1.2
IR110CCV(config-mon-erspan-src-dst)#origin ip address 169.254.1.1
IR110CCV(config-mon-erspan-src-dst)#end
IR110CCV#
```

Setup NAT

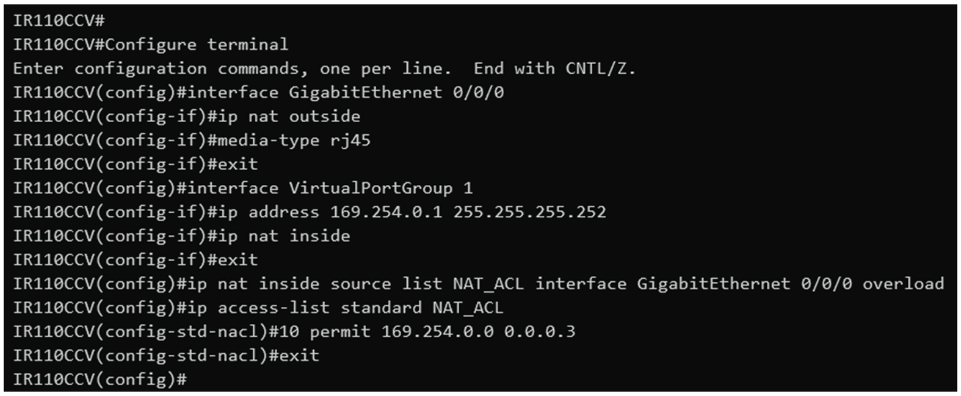
You must add NAT rules so that the container can reach the outside. This will be on a different virtual port group from the ERSPAN to separate the traffic.

Procedure

Step 1 Type the following commands to achieve this configuration.

```
Configure terminal
interface GigabitEthernet 0/0/0
ip nat outside
media-type rj45
exit
interface VirtualPortGroup 1
ip address 169.254.0.1 255.255.255.252
ip nat inside
```

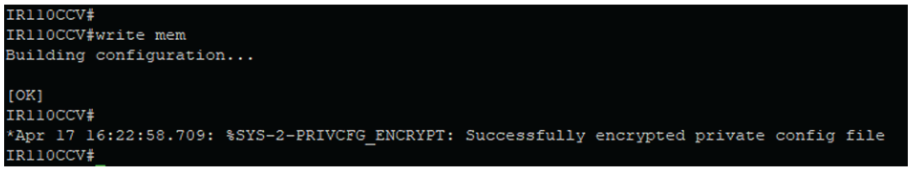
```
exit
ip nat inside source list NAT_ACL interface GigabitEthernet 0/0/0 overload
ip access-list standard NAT_ACL
10 permit 169.254.0.0 0.0.0.3
exit
```



```
IR110CCV#
IR110CCV#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
IR110CCV(config)#interface GigabitEthernet 0/0/0
IR110CCV(config-if)#ip nat outside
IR110CCV(config-if)#media-type rj45
IR110CCV(config-if)#exit
IR110CCV(config)#interface VirtualPortGroup 1
IR110CCV(config-if)#ip address 169.254.0.1 255.255.255.252
IR110CCV(config-if)#ip nat inside
IR110CCV(config-if)#exit
IR110CCV(config)#ip nat inside source list NAT_ACL interface GigabitEthernet 0/0/0 overload
IR110CCV(config)#ip access-list standard NAT_ACL
IR110CCV(config-std-nacl)#10 permit 169.254.0.0 0.0.0.3
IR110CCV(config-std-nacl)#exit
IR110CCV(config)#
```

Step 2 Save the configuration.

```
exit
write mem
```



```
IR110CCV#
IR110CCV#write mem
Building configuration...

[OK]
IR110CCV#
*Apr 17 16:22:58.709: %SYS-2-PRIVCFG_ENCRYPT: Successfully encrypted private config file
IR110CCV#
```

What to do next

Proceed with one of the following procedures:

- Procedure with the Cisco Cyber Vision sensor management extension
- Procedure with the Local Manager
- Procedure with the CLI