

Connecting and Managing via Local Manager (LM)

This section contains the following topics:

- About Local Manager, on page 1
- Accessing the IC3000 via Local Manager, on page 1
- Setting the Date and Time, on page 3
- Setting NTP Manually, on page 5
- Setting DNS Manually, on page 7
- Software Reboot Button, on page 8
- Use Case Example: Installing a Prebuilt Application via Local Manager, on page 9
- Additional Examples, on page 12
- Remote Device Management, on page 12

About Local Manager

Cisco IOx Local Manager provides a web-based user interface that you can use to manage, administer, monitor, and troubleshoot applications on a device, and to perform a variety of related activities.

Accessing the IC3000 via Local Manager

Find the Management port address to access the IC3000 via a web browser. After connecting the IC3000 to a laptop, gather the svcbr_0 address whether you are in managed mode, or standalone mode. Use the **show interfaces** command to determine the IP address, or if you are managing the device via FND, get the device IP address. Use the ioxusername and ioxpassword to login via Local Manager, or you can create users on the IC3000 from the device configuration tab. Use the json commands to create users and passwords that Local Manger can use.

ic3k>show interfaces

```
svcbr_0 Link encap:Ethernet HWaddr f8:b7:e2:b5:26:80
inet addr:172.27.127.174
Bcast:172.27.127.255 Mask:255.255.255.0
inet6 addr: fe80::fab7:e2ff:feb5:2680/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
```

```
RX packets:396 errors:0 dropped:0 overruns:0 frame:0
TX packets:25 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:29614 (28.9 KiB) TX bytes:3373 (3.2 KiB)
```



Note If the IC3000 is in standalone mode, you will be using an IPv4 LLA address of 169.254.128.x. The rest of the following work flow is the same.

Procedure

Step 1 Open a web browser and enter https://169.254.128.2:8443 in the address bar.

Step 2 Login by using the default credentials admin/cisco123 for the first time if you are running release 1.2.1. For older devices running 1.1.1 or 1.0.1, use developer/<your-password>. This is the password that was created by the developer set-password or developer change-password command. You should have various tabs that Local Manager supports, since you are accessing the device via Local Manager. You should be familiar with the standalone mode options like Device Config tab.

If a security exception message appears in your browser, confirm the exception to continue to the Cisco IOx Local Manager Login screen.

If you see the message "For best results use a supported browser" near the top of this screen, your browser may have compatibility issues with this version of Cisco IOx Local Manager. In this case, we recommend that you load a compatible browser. Hover your mouse pointer over the down-arrow next to this message to see a list of compatible browsers as shown in Figure 1: Supported Browsers, on page 2.



Figure 1: Supported Browsers

Step 3 Click **Log In**. The **Local Manager Applications Tab** appears. See Figure 2: Local Manager Applications Tab, on page 3.

What to do next

Figure 2: Local Manager Applications Tab

cisco Sy cisco Cisco IO	ystems x Local Manager									Hello, admin	Log Out About
Applications	App Groups	Remote Docker Workflow	Docker Layers	System Info	System Setting	System Troub	leshoot I	Ox Tools	Device Config	User Cc »	
CyberVision3 CyberVision Sensa TYPE vm Columnation Columnation Start	Sensor Ir Image for IC3000 VERST 3.0.4 Ø Deactive	ACTIVATED ON PROFILE + CLippe 4.0% 5.8% ate � Manage		Add New	7 Ø Refresh						

Setting the Date and Time

The time feature in Local Manager provides the user with the ability to change the system time, date and time zone on an IC3000. Although this feature is available, it is still recommended to provide access to an NTP server to avoid any issues.

Release 1.3.1 provides enhanced capabilities. The user can now select the time source between manual date and time or NTP. When using NTP, the user can provide information about NTP servers manually, or get that information from a DHCP Server.

The following are options that the user can select from the Device Configuration page of the User Interface (UI):

- Manual Date and Time (User provides the information)
- Network Time Protocol (NTP)
 - Auto (DHCP Server provides the information)
 - Manual (User provides the information)



Note Either Manual or NTP date and time options can be selected.

Some of the feature caveats are:

- Time Zone can be individually selected by the customer regardless of the time source.
- Up to 5 NTP servers and 1 Preferred NTP server
- Polling interval includes max and min poll
- For NTP Authentication, the user provides the id, type, and value of the keys
- For NTP, either hostname or IP address can be used.

From the Local Manager GUI, click on the **Device Config** Tab. The following shows the Time Source section highlighted.

			♥ Refresh
 Data Inter 	face Config		▼ Standalone Mode
Interface	IP Address	Action	Standalone Mode: On Remote Device Management: Enabled
svcbr_0	172.27.168.53	edit view	🖒 Standalone Mode Off Disable Remote Management
int1		disable edit view	
int2		disable edit view	Default Route Gateway IP: 170 D7 160 1 Interface: such: 0
int3		disable edit view	Sectory 1. 1/2.2/.106.1
int4	100	disable edit view	意 Delete Default Route
Software U Select Image: Upload 8	Jpgrade Choose File No file cho	osen	Im Delete Delatit Kodde
Software t Select Image: Upload 8 FND Certif Select Certification	Jpgrade Choose File No file ch k Install icate a: Choose File No fi	osen file chosen	Time Source Manual @ MTP
Software U Select Image: Upload 8 FND Certif Select Certificate Upload	Jpgrade Choose File No file cho Install icate a: Choose File No file No file cho Choose File No file Choose File No file No file cho Choose File No file cho Choose File Cho Choose File Cho Cho Choose File Choose File Cho Cho Cho Cho Cho Cho Cho Cho	osen file chosen	Time Source Manual NrP
Software I Select Image: Upload 8 FND Certif Select Certificate Upload	Ipgrade Choose File No file cho Install icate : Choose File No file No file cho icate	osen file chosen	W Delete Delatit Koute ✓ DNS Domain: Name Servers: Search Domain : Configure DNS ✓ Time Source Manual ③ NTP ✓ NTP ✓ NTP
 Software I Select Image: Upload 8 FND Certif Select Certificate Upload Upload 	Install Choose File No file choose File Choose File No file choose	osen flie chosen	W Delete Delatit Kodde ✓ DNS Domain: Name Servers: Search Domain : Configure DNS ✓ Time Source Manual ③ NTP ✓ NTP Mode: Auto ✓
 Software to Select Image: Upload 8 FND Certification Upload Upload Certification Upload 	Ipgrade Choose File No file cho Install icate B: Choose File No file No file Choose File No file Choose Fi	osen file chosen	DINS Domain: Name Servers: Search Domain : Configure DNS Time Source Manual NTP w NTP Mode: Auto Configure NTP
Software to Select Image: Upload 8 FND Certificat Upload Upload C Reload	Ipgrade Choose File No file cho Install icate B: Choose File No file No file Choose File No file Choose Fi	osen file chosen	Direct Derivativ Kodde Domain: Name Servers: Search Domain : Configure DNS Time Source Manual ③ NTP V NTP Mode: Auto Configure NTP V Time Source Configure NTP Time Source Time Source
Software I Select Image: Upload 8 FND Certif Select Certificat Upload Ö Reload	Ipgrade Choose File No file choose File Choose File No file choose File No file choose File Choose File Choose File Choose Fi	osen file chosen	W Delete Delatin Kodde ✓ DNS Domain: Name Servers: Search Domain : Configure DNS ✓ Time Source ✓ Manual ⓒ NTP ✓ NTP Mode: Auto ✓ Configure NTP ✓ Timezone Timezone Timezone: (UTC-08:00) Pacfic Time (US & Canada) ✓)

Figure 3: Local Manager Time Source

From this section, you can click on Manuel or NTP as your time source. Choosing NTP defaults to Auto. Click Configure NTP and the settings are updated.

To configure your Date and Time manually, select the Manual button. The Time Source window appears as the following:

Figure 4: Manual Date and Time

 Time Source 	
💽 Manual 🔘 I	ITP
▼ Date and	īme
Date:	The second secon
Time:	HH:MM:SS
Configure 1	ïme
▼ Timezone	
Timezone:	(UTC-08:00) Pacific Time (US & Canada)
Configure 1	ïmezone

Fill in the date and time you wish and then click Configure Time.

To configure NTP manually, move on to the next section.

Setting NTP Manually

The NTP feature in Local Manager provides the user with the ability to set Network Time Protocol (NTP) manually on an IC3000.

Procedure

Step 1 From the Local Manager GUI, click on the **Device Config** Tab.

Step 2 Under the Time Source section, click on **NTP**. Refer to the following:

er Workflow	Docker Layers	System Info	System Setting	System Troubleshoot	IOx Tools	Device Config	User Config	>>
								C Refresh
▼ Data Interf	ace Config			▼ Stan	dalone Mode			
Interface	IP Address		Action	Standalo	ne Mode: On	Remote Device	Management: Enabled	
svcbr_0	172.27.168.53		edit view	🖱 Sta	andalone Mode Of	f Disable Re	mote Management	6
int1	111		disable edit view	- 0-6				
int2			disable edit view	Gateway	IP: 172 27 168 1	Interface: svc	br 0 👻	
int3	111		disable edit view		1/2.2/100.1			
int4			disable edit view	De De	lete Default Route	2		
Select Certificate:	Choose Choose	e File No file choser		▼ Time ○ Manu ▼ NT	source Jal NTP P			
O Reload				Mode: Cor • Tin Timeza	Auto	C-08:00) Pacific Time (US & Canada) 🛛 🗸	

Step 3 Beside the Mode, select the pulldown and click **Manual**. Refer to the following graphic.

Figure 5: NTP Manual Configuration

Time Source) Manual NTF 	,				
▼ NTP					
Mode:	Manual	T			
MinPoll	6				
MaxPoll	10				
NTP Key					
key ID	SHA1	password	3	• +	
KeyID			Action		
NTP Server					
Server:IPv4/IPV6	/Hosname	- no ntp key -	• ▼ False		+ +
NTP Server(Hostname/	IPv4/IPv6)	Auth ID	Preferred-Server	Action	
Configure NTP)				
▼ Timezone					
Timezone:	(UTC-08	:00) Pacific Tim	e (US & Canada)	~	
Configure Tim	ezone				

Step 4 Fill out the NTP entries, then click the plus sign (+)

- **Note Optional**: Add an **NTP Key** entry if the NTP server has been configured with authentication. Add the **Key ID** and corresponding **SHA1 key** as the password.
- Note Note: Authentication is only offered for NTP servers that support SHA1.

Step 5 Click Configure NTP.

What to do next

Note

To check if the device has synchronized to the NTP server, run the command **show ntp status** on the IC3000. If the NTP server is reachable, it will show a message stating the clock is synchronized:

```
IC3000> show ntp status
Clock is synchronized, stratum 3, reference is <your ip address>
```

Setting DNS Manually

The DNS feature in Local Manager provides the user with the ability to push a DNS configuration on an IC3000 device that's in standalone mode.

To push DNS configuration via LM perform the following:

Procedure

- **Step 1** From the Local Manager GUI, click on the **Device Config**Tab.
- Step 2 Under the DNS section, click on Configure DNS. Refer to Figure 6: Configure DNS, on page 7.

Figure 6: Configure DNS

Address 2.27.168.53	Action edit] view disable [edit] view disable [edit] view disable [edit] view disable [edit] view	Standalone Mode Standalone Mode On Standalone Mode Off Disable Remote Management: Enabled Default Route Default Route Delete Default Route Delete Default Route Sarch
Address 2.27.168.53 Choose File No file chosen	Action editį view disable į editį view disable į editį view disable į editį view disable į editį view	Standalone Mode: On Remote Device Management: Enabled Standalone Mode: Of Disable Remote Management Default Route Gateway IP: 172.27.168.1 Interface: wvbr_0 Delete Default Route VDS Search
Address 2.27.168.53 Choose File No file chosen	Action edit view disable edit view disable edit view disable edit view disable edit view	Standalone Mode: On Remote Device Management: Enabled
2.27.168.53	edit] view disable edit view disable edit view disable edit view disable edit view	[©] Standalone Mode Off Disable Remote Management • Default Route [®] Standalone Mode Off [©] Default Route [®] Standalone Mode Off [©] Default Route [®] Standalone Mode Off [©] Delete Default Route [®] Standalone Mode Off [•] DNS Search
Choose File) No file chosen	disable edit view disable edit view disable edit view disable edit view	▼ Default Route Gateway IP: 172.27.168.1 Interface: svcbr_0
Choose File) No file chosen	disable edit view disable edit view disable edit view	Default Route Gateway IP: 172.27.186.1 Interface: svcbr_0 The lete Default Route DNS Search
Choose File No file chosen	disable edit) view disable edit view	Delete Default Route DNS Search
Choose File No file chosen	disable edit view	■ Delete Default Route
Choose File No file chosen		▼ DNS Search
Choose File No file choose	sen	Time Source Manual NTP The Source
		Mode: Auto - Configure NTP
		▼ Timezone
		Timezone: (UTC-08:00) Pacific Time (US & Canada) V

Step 3 After clicking on Configure DNS, the DNS Config window opens. Refer to Figure 7: DNS Config Window, on page 8.

Step 4 Step 5

DNS Config	-			
Туре:	🔾 Auto 💿 Manual			
Domain Name:				
Name Server:	Server:IPv4/IPV6	+ Search Doma	iin:	+
	171.70.168.183		example.com	
		-		-
				ОКСа

Software Reboot Button

When managing the IC3000 in standalone mode, and the device is not functioning as expected, a software reboot button is provided under the Device Config tab. Refer to Figure 8: GUI Reload Button, on page 8.

Figure 8: GUI Reload Button

			↓ nortan
 Data Interfa 	ace Config		Standalone Mode Standalone Mode Device Macagements Enabled
Interface	IP Address	Action	Ch Standalone Mode Off Disable Device Management. Enabled
svcbr_0	172.27.168.53	edit view	Disable Remote Management
int1		disable edit view	▼ Default Route
int2		disable edit view	Gateway IP: 172.27.168.1 Interface: svcbr_0 +
int3		disable edit view	
int4	1	disable edit view	Delete Default Route
FND Certific elect Certificate:	Choose File No f	ile chosen	Configure DNS ▼ Time Source ○ Manual ④ NTP
O Upload	T Delete		▼ NTP
🖱 Reload			Mode: Auto v Configure NTP
			▼ Timezone
			Timezone: (UTC-08:00) Pacific Time (US & Canada)

Note After pressing the **Reload** button, you will temporarily lose access to the LM GUI for approximately 2 to 3 minutes until the device comes back up.

Your IC3000 is now ready for Cisco IOx application development.

Use Case Example: Installing a Prebuilt Application via Local Manager

This section shows you how to use Cisco IOx Local Manager to load a sample EFM application and how to run the application

Procedure

- Step 1Download the Docker application on to your desktop. Go to the following link:
https://software.cisco.com/download/home/286316104/type/286312892/release/1.5.0
- **Step 2** In the Cisco IOx Local Manager Applications Tab, click **Add New**. The **Deploy application** dialog box appears.

Figure 9: Deploy application

cisco Cisco Systems Cisco Cisco IOx Local Manager			Helo, test Log Out Abo
Applications Cartridges/Layers	System Info System Setting	System Troubleshoot Device Config	
O Add New C Refresh			
		Deploy application x Asplication Id: <u>test app</u> Select Application Archive Choose File No file chosen CK Cancel	

Step 3

- In the Deploy Application dialog box, take these actions:
 - a) In the **Application ID** field, enter a name. The App ID requires more than one character and follows this regex syntax: [a-zA-Z0-9][a-zA-Z0-9_.-]
 - b) In the **Select Application Archive** field, click **Choose File** and navigate to, then select the sample application file that you downloaded in Step 1.
 - c) Click **OK**
- **Step 4** The application file uploads to Cisco IOx.



Note Do **NOT** refresh the browser during the upload.

When you see the pop-up message "Successfully Deployed", click **OK**.

Figure 10: Application Successfully Deployed

ications	Cartridges/Layers	System Info	System Setting	System Troubleshoot	Device Config
st1		DEP	LOYED		
mple LXC Style	app that creates creates tty VERSION	processes	PROFILE		
c Memory *	2.0		c1.small	• Add New	C Refresh
CPU *			1.9%		
✓ Activate	e 🔷 Upgrade	Delete			
					No file chosen

Note The Cisco IOx Local Manager Applications tab updates to show the EFM application area.

Step 6 In the test1/APP area, click the Activate button. The Applications > Resources tab displays, see #unique_ 38 unique_38_Connect_42_fig_1060957.

Step 5

Figure 11: Applications > Resources Tab

Applications	x Local Manager Cartridges/Layers	System Info	System Setting	System Troubleshoot	Device Config	test1	
Resources	App-info App-Confi	ig App-Dat	aDir Logs				
Resouces							
▼ Resource P	Profile				· Network 0	Configuration	
Profile:	c1.small \$				eth0	v iox-nat0 - nat	Port Mapping
CPU	200	cpu-units				int1 Data interface via int1 int2 Data interface via int2	
Mamon		MD				int3 Data interface via int3	
memory	64	MD				int4 Data interface via int4	
Disk	10	MB					
Avail. CPU (cp	u-units) 10260 Avail. Mem	ory (Mb) 6400					
Astimto							

Step 7 In the **Network Configuration** area of the **Applications** > **Resources** tab, perform the following:

- a) Choose int1 Default Network from the eth0 drop-down list.
- b) Choose **int2** from the eth1 drop down list.

Note Always use eth1 to connect your device to your local network.

Step 8 While still in the **Applications** > **Resources** tab, click the **Activate** button to activate the application.

- Step 9 Click the Applications tab.
- **Step 10** In the EFM area, click the **Start** button.

Note Make sure that activated the application before clicking **Start**.

Figure 12: Applications > Start

test1 ACTIVATED Simple LXC Style app that creates creates thy processes TYPE VERSION PROFILE xc 2.0 CLSmall Memory ^s 1.0% EPU ^s 1.9%	ACTIVATED Simple LXC Style app that creates try processes TYPE VERSION 2.0 PROFILE cLsmall Memory * 1.0% PPU = 1.9% Start Ø Deactivate Manage	Applications	Cartridges/Layers	System Info	System Setting	System Troubleshoot	Device Config	test1
Imple LXC Style app that creates try processes YPE VERSION 2.0 Cl.small Memory * 1.0% CPU * 1.9%	imple LXC Style app that creates creates try processes YPE VERSION 2.0 CLsmall Memory * 1.0% CPU * 1.9% > Start Ø Deactivate	est1		ACTI	VATED			
VPF VERSION PROFILE xc 2.0 cl.small Memory * 1.0% CPU * 1.9%	YPE VERSION PROFILE Lamal Lamal Memory * 1.0% CPU * 1.9% ▶ Start Ø Deactivate	Simple LXC Style ap	p that creates creates tty p	rocesses				
Hemory * 1.0% CPU * 1.9% ► Start Ø Deactivate ✿ Manage	Memory * 1.0% CPU * 1.9% ► Start ⊘ Deactivate ♥ Manage	TYPE	VERSION 2.0		PROFILE			
PPU	CPU = 1.9% ► Start Ø Deactivate ✿ Manage	Memory *	LIV		1.0%	O Add New	${\cal C}$ Refresh	
PPU ■ 1.9%	▶ Start Ø Deactivate							
► Start Ø Deactivate ✿ Manage	► Start Ø Deactivate ✿ Manage	CPU *			1.9%			
		► Start	Ø Deactivate	🌣 Manage				
		,						

Step 11 Click the **App-info** tab and make sure that data ports int1 and int2 are up. Then, once the application is started check the dhcp obtained address in the **App-info** tab.

Figure 13: App-info Tab

		Network	Network information	
lications Cartridges/Laye	rs System Info System Setting	interface-name:	interface-name: eth0	
		TCP:	Info	
sources App-info	App-Config App-DataDir Logs	UDP:	Info	
		mac_address:	06:f8:b7:e2:b5:f2	
	Application information	network_name:	int1	
	tort1			
Etato:	ACTIVATED		C	
kate.	200MR ADD	Profiles		
Castidae Desuised:	ZUUHD_AFF	Piele		
carooge Requireu:	• None	DISK:		
/ersion:	2.0			
Author:	Cisco Systems		Netw	
uthor link:	http://www.cisco.com	interface-name:		
pplication type:	lxc			
escription:	Simple LXC Style app that creates creates tty			
	processes	App Health		
solkit service:	None	Reconcile Attempte	d	
Debug mode:	false	Reconcile Failure		
		race/rene renere		
			Re	
C Refresh		Disk:		
		Disk Remaining:		

Additional Examples

There are a number of applications that can be loaded onto the IC3000. Developers can package any application as long as it is in a container or VM. Additional information and examples are located on DevNet documentation on IOx. Provides an overview as well as details by scrolling down the left hand side:

https://developer.cisco.com/site/devnet/support/

Remote Device Management

The remote device management feature provides the user with the ability to enable or disable the remote access to the device configuration page from Cisco IOx Local Manager over a non-link local address. This is turned ON or enabled by default thus allowing for local and remote access of the local manager GUI. The below steps are valid for older release, for example 1.1.1, where the user needs remote management.

Note Remote Device Management is new with Local Manager version 1.8. If your device is still running version 1.7, you will need to upload the new image. See Step 1 below.

The procedure to bring the IC3000 up into Standalone Mode remains exactly same as previously described in Phase 3: Standalone Mode: Testing IOx Applications via Local Manager, page 1. Use the pre-defined link-local address169.254.128.2 to get the device up in standalone mode.

Next, follow these additional steps to enable remote device management:

Procedure

- **Step 1** If required, upload the new Image from the Device Config tab and it will reload the device with the latest image.
- **Step 2** Open a **NEW** browser and login again with the 169.254.128.2 address to the Local Manager using default credentials. (admin/cisco123) or the new password if the credentials are changed.

Note The old browser is now non-functional.

Step 3 In the Device Config tab there is a new section on the right side called "Remote Device Management". See the highlighted area in the following graphic.

Figure 14: Remote Device Management

cisco Cisco IO:	ystems x Local Manager		
Applications	Cartridges/Layers System Info	System Setting System Troubleshoot	Device Config
Data Interface svcbr_0 int1 int2 int3	P Address 156.254.128.2 22.22.22.22	Action edit view disable edit view disable edit view enable edit view	User Config Name tot2 Change Reserved Developer Mode Developer Mode Developer Mode D Developer Mode Off D Developer Mode Off Enable Remote Management District
Software Upg Select Image: Upload & Ir C Refresh	stall	energi (och) voor	v Default Route Getewy IP: v factoria Scherificae: v

Step 4 Click **Enable Remote Management**, and then respond with **Yes/Okay** for any pop-ups.

After enabling remote device management, the user can access the device configuration page from any IP address other than the link local address.

- **Note** Since the HTTP server is not only binding with the link local IP address, the user can access the device config page from the data port as long as it has routable IP address configured with an up state.
- **Step 5** Use the https://<*new address*> :8443 in a new browser window to login to Local Manager using developer credentials. See Figure 15: Remote Device Management (Enabled), on page 14 for guidance for these steps.
- **Step 6** Make sure you are aware of your network topology (static ip address or DHCP) for the management interface svcbr_0.

If the address is non link local address other than 169.x.x.x

- a) Edit the svcbr_0 address to <*your ip address*> and make sure to add a network on the laptop to connect to the Local Manager.
- b) Use the new address from the browser to login to the Local Manager with developer credentials.

If the address is a static routable address:

- a) Obtain the default-route details and add the Gateway IP route details to the svcbr_0 interface below" Default Route" section below.
- b) On the left side of the Device Config screen, edit the svcbr_0 interface, static option, with chosen IP address and set mask. Click **Ok**.
- c) Attach the MGMT port to the network where the address is reachable. **NOTE**: The Local Manager is not reachable anymore once the configuration is pushed, you have to connect the MGMT port of the IC3000 to a network where the address is reachable.

d) Use the new chosen address from a new browser window to login into Local Manager with the developer credentials.

If the MGMT/svcbr_0 is connected to a DHCP network, after enabling remote management edit the svcbr_0 interface to select the DHCP option.

- a) Disconnect IC3000 management port from laptop and connect to the network for active DHCP learning on svcbr_0.
- b) Check the ip address learned via DHCP on the platform console using the CLI show interfaces.
- c) Use the https://<new address> :8443 in a new browser window to login to LM using developer credentials.
- Step 7 Obtain the default-route details and add the Gateway IP route details to the svcbr_0 interface below Default Route.
- **Step 8** On the left side of the Device Config screen, edit the svcbr_0 interface with chosen IP address and mask. Click **Ok**
- **Step 9** See Figure 15: Remote Device Management (Enabled), on page 14 for guidance for these steps.

Figure 15: Remote Device Management (Enabled)

← → ℃ (▲	Not Secure https://33.33.33.33.8443/a	dmin		x • Y 📕 🕸 Q 😝 E
cisco Cisco IOx	stems Local Manager			Helfe, tead2 + Log Out + About
Applications	Cartridges/Layers System Info	System Setting System Troubleshoot	Device Config	
▼ Data Interface	a Config			▼ User Config
Interface svcbr_0	1P Address 33.33.33.33	Action edit view		Change Password
int1 int2	22.22.22.22	disable edit view disable edit view		▼ Developer Mode
int3		enable edit view		Developer Mode Off Disable Remote Management
				▼ Default Route
Software Upge Select Image: Upload & Ins	Choose File No file chosen			calativity or prostruct: v
C Refresh				

To disable remote device management

From the same Device Config tab window, you can see the Remote Device Management section status has toggled to "Enabled". To disable the feature, click **Disable Remote Management.**

Disabling the remote device management feature will bind the server back to the 169.254.128.2 address of the link local manager. The user will not be allowed to disable the remote device management unless they change the IP address for "svcbr_0" back to 169.254.128.2.

Figure 16: Disable Remote Device Management Warning

• Data Interface Config • User Config Interface IP Address Accor seb: 0 33.33.33.3 exit (view intit 22.22.22.22 dasha (exit (view intit 22.22.22.23 dasha (exit (view intit dasha (exit (view intit dasha (exit (view intit enable (exit (view intit enable (intit (view intit enable (intit (view intit enable (intit (view intit enable (intit (view O Developer Mode Off Initial Rester Disable Rendee Maragement: Evabled Initial Rester	Log Out Abou	Helo, test2 y	agement. Please configure the IP address for svctr_0	Setting Unable to disable remo	sger s/Layers System Info System Setting	Applications Cartridges/Layer
Joneface IP Address Actor webs_0 32.33.33.33 exth / wer Change Passance with 22.22.22 daabal (ext) / wer Change Passance with 22.22.22 daabal (ext) / wer Change Passance with 22.22.22 daabal (ext) / wer Change Passance with			▼ User Config			Data Interface Config
sectr.0 33.33.33 est iver Dange Password intt 22.22.22 dable (est iver * Developer Mode int2 dable (est iver * Developer Mode int3 endte (est iver Disdele Rente Nangement: Endted int4 endte (est iver Disdele Rente Nangement: Endted int5 endte (est iver Disdele Rente Nangement int5 endte (est iver * Devloper Mode Off Disdele Rente Nangement			Name: test2	Action	IP Address	Interface IP
int1 22.22.22 dtable (edf. (ver • Developer Mode int2 dtable (edf. (ver • Developer Mode int3 dtable (edf. (ver • Developer Mode int3 enable (edf. (ver • Developer Mode int3 enable (ver • Developer Mode int3 enable (ver • Developer Mode int3 enable (ver • Developer Mode int4 enable (ver • Developer Mode • Developer Mode • Developer Mode • Developer Mode • O Developer Mode • Developer Mode • Developer Mode • O Developer Mode • Developer Mode • Developer Mode • O Developer Mode • Developer Mode • Developer Mode • O Developer Mode • Developer • Developer			Change Password	edit view	33.33.33.33	svcbr_0 33.
Int2 diable (eff) (view Perceptor Mode Int2 enable (eff) (view O Developer Mode Off Diable Remote Management: Enabled Int3 enable (eff) (view O Developer Mode Off Diable Remote Management: Int3 enable (eff) (view O Developer Mode Off Diable Remote Management: Int3 enable (eff) (view O Developer Mode Off Diable Remote Management: * Default Route * Default Route *				disable edit view	22.22.22.22	int1 22.
ind			Developer Mode	disable edit view		int2
lot			Considered Marte Off Displace Marte Off Displace Marte Off Displace Marte Off Displace Marte	enable edit view		int3
			O beveruper mode on Disable Remote Management	enable edit view		int4
* Software Upgrade Gateway IP; Interface:			▼ Default Route			
Seite Image Choose File No file Cholen © Uplood & Install			Gateway Pr Interface: *		ose File . No file chosen	Software Upgrade Select Image: Choose File Upload & Install