



# Cisco Configuration Professional Express 3.5.x User Guide

**First Published: June 26, 2018**  
**Last Updated: August 13, 2018**

## Overview

The Cisco Configuration Professional Express (Cisco CP Express) is an embedded, device-management tool that provides the ability to bootstrap and provision a Cisco Industrial Router (IR).

Cisco CP Express helps you to set up a network with complete WAN and LAN configurations, along with wireless access and security features. Security features are supported only if the IOS version is 15.5(1)T and later and the security license is enabled. For IR 800 Series routers, the recommended IOS version is 15.6(3)M2. CCP Express provides you two options to bring up a new router. You can use the Quick Setup Wizard to perform the basic configuration tasks and Advanced Setup option for detailed configuration options. For a new router, Quick Setup Wizard is the preferred option.

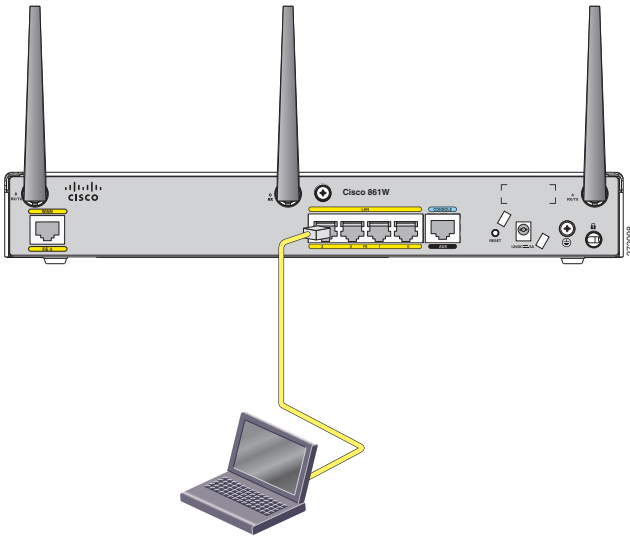
When you are running CCP Express for the first time, you can use the Quick Setup Wizard to perform the basic router configuration tasks including setting up WAN, configuring LAN, and basic security configuration.

All the configuration done through CCP Express is saved into startup configuration by default. When you use CCP Express for configuring a device, do not delete or modify the configuration directly by logging onto the device which will lead to misconfiguration. The Security tab is enabled only when the security license is enabled on the device and the IOS image is 15.5(1)T and later. For IR 800 Series routers, the recommended IOS version is 15.6(3)M2.

## Verifying CP Express Installation

1. Connect the PC to the router by using an Ethernet cable as shown in [Figure 1](#).

**Figure 1 Connecting PC to the Router**

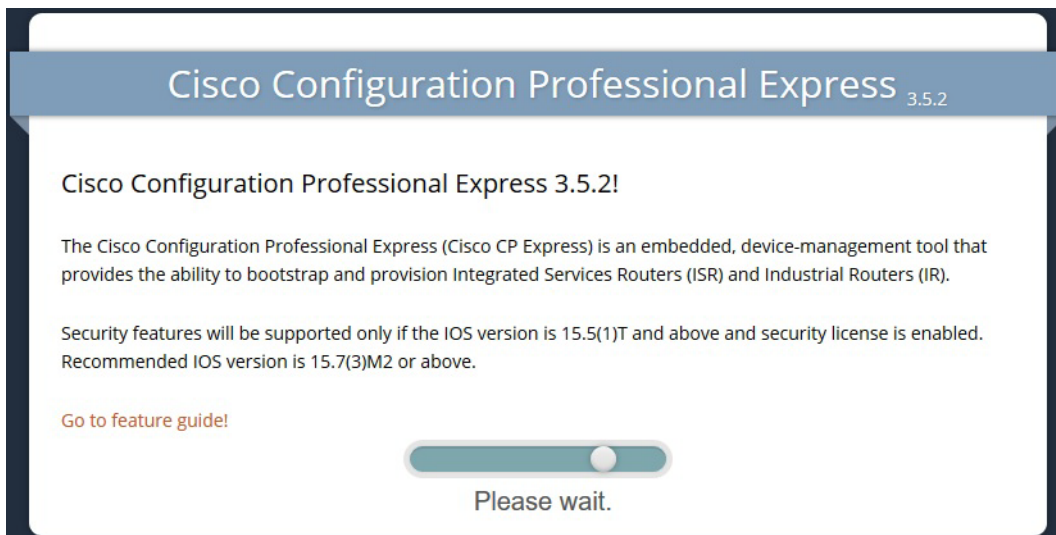


2. Verify the Cisco CP Express is installed correctly by performing the following steps:
  - a. Launch the browser.
  - b. In the address bar, type the IP address of the router where Cisco CP Express is installed.  
For example, type *http://10.10.10.1* or *https://10.10.10.1*
  - c. Provide the one-time user credentials when the router prompts for specifying new username and the password.
  - d. Click **Log In**.
  - e. Create a new user account and login with the new user credentials. Cisco CP Express Installation screen launches.

## Loading CCP Express

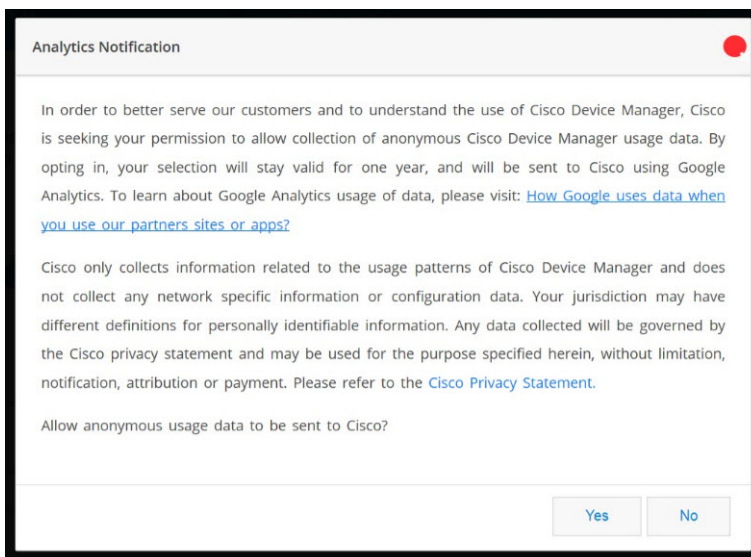
Splash Screen is displayed when CCP Express is loading. This screen gives information about the current release and a link to the feature guide.

**Figure 2** Splash Screen



The Analytics Notification window displays with information about usage data.

**Figure 3** Analytics Notification



1. Click **Yes** to continue.

If the device is new, the Quick Set Up Wizard displays along with Advanced Setup. If the device is already configured, the home page with the list of Advanced options is displayed.

**Figure 4 Quick Setup Wizard & Advanced Setup**

The device is detected as a brand new device based on the configuration. You can click on Quick Setup Wizard which guides you to quickly bring up the box. Advanced configuration lists all features using which user can complete all advanced configurations.

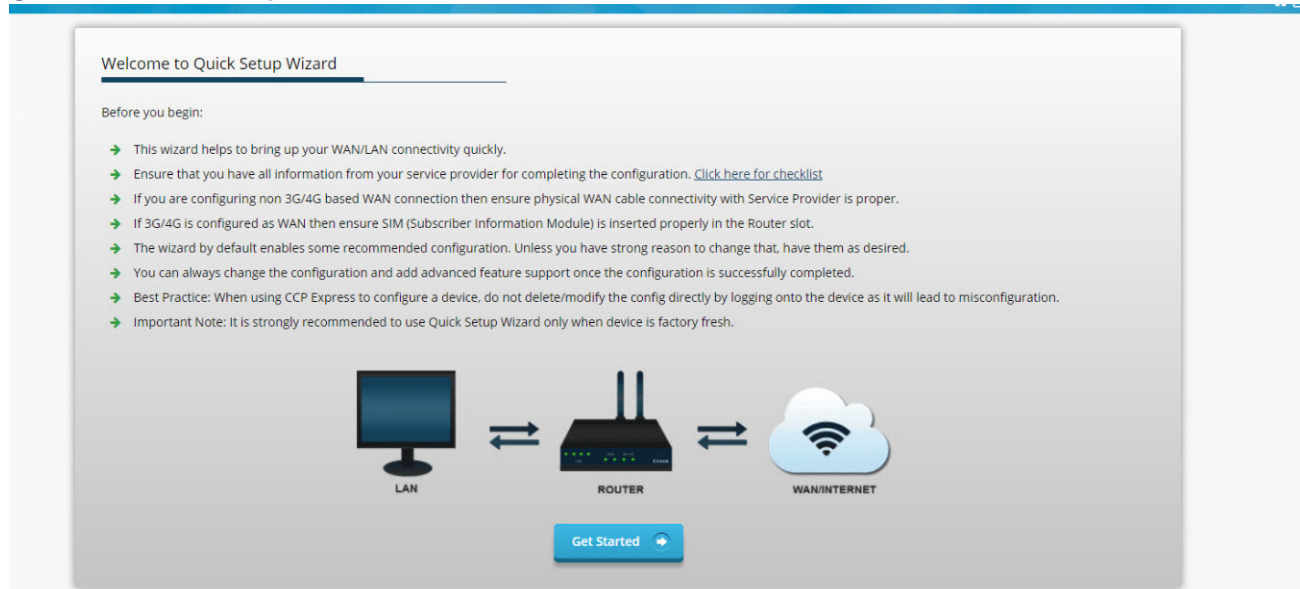


2. Click **Quick Setup Wizard** from the Quick Setup Wizard & Advanced Setup page to run the Quick Setup Wizard.

If you click on the Advanced Setup, you are taken to the CCP Express Landing page as shown in [Figure 26 on page 17](#).

## Using Quick Setup Wizard

Quick Setup Wizard helps you to perform the basic router configuration when you are running the Cisco CP Express for the first time.

**Figure 5 Cisco CP Express Installation**

Go through the configuration pre-requisites in the Quick Setup Wizard welcome screen, and then click **Get Started**.

**Note:** Since the IR 809 does not support Wi-Fi, this option is not available on the IR 809 Quick Setup Wizard.

## Basic Setup

1. Configure basic settings by entering Router Name, Domain Name, and selecting the appropriate Time Zone.

**Figure 6 Quick Setup Basic Setup Screen**

**Quick Setup Wizard**

Basic Settings

Router Name \* : IR829

Domain Name \* : cisco.com

TimeZone \* : (GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi

Synchronize with NTP Server

Make this router as NTP Master  
*All the Devices (DHCP Client) will have time synchronized with router*

Help and Tips ?

- The symbol "\*" indicates Mandatory field.

[Cancel](#) **Next**

2. Click **Next** to access the primary WAN Configuration window.

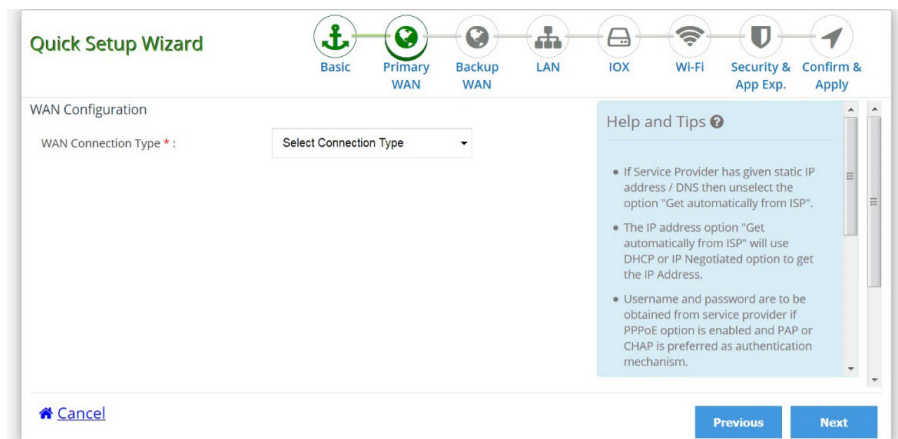
## WAN Configuration

See the following subtasks for each WAN option for configuring the required WAN:

- [Cellular WAN Configuration](#)
- [Ethernet WAN Configuration](#)

### Cellular WAN Configuration

1. Select the connected cellular WAN interface for configuring the primary WAN.
2. Select enable persistence if you want to establish a persistent connection to your service provider from the dialer interface.
3. Get DNS server information directly from ISP is selected by default. If this option is enabled you cannot assign IP addresses statically.
4. Select the SIM for activation. If you enable the auto firmware switch option to automatically switch over the firmware when you switch the SIM cards.

**Figure 7 Cellular Primary WAN Interface IR 829 Dual LTE**

5. Click **Next** to configure the Backup WAN.

6. Check the Enable Backup WAN box.

7. Select WAN Connection Type as 3G/4G. For dual LTE, the Interface is Cellular 1/0 (SIM 1). See [Figure 8](#).

For single LTE, the Interface is only Cellular. See [Figure 9](#).

## Using Quick Setup Wizard

**Figure 8 Cellular Backup WAN Configuration IR 829 Dual LTE**

**Quick Setup Wizard**

Basic Primary WAN Backup WAN LAN IOX Wi-Fi Security & App Exp. Confirm & Apply

Backup WAN

Enable Backup WAN

WAN Connection Type \*: 3G/4G

Interface \*: Cellular 1/0 (SIM 1)

Enable Persistence:

**NAT**

Enable NAT

**SLA Configuration**

IP Address: 8.8.8.8

**Modem Settings**

**SIM 1**

Attach Profile \*: 1 vzwims

Advance Profile Options:

[Cancel](#)

[Previous](#) [Next](#)

**Help and Tips**

- If Service Provider has given static IP address then unselect the option "Get automatically from ISP".
- The IP address option "Get automatically from ISP" will use DHCP or IP Negotiated option to get the IP Address.
- Username and password are to be obtained from service provider if PPPoE option is enabled and PAP or CHAP is preferred as authentication mechanism.
- APN is provided by Service Provider and has to be obtained from the Service Provider prior to using in WAN configuration. Attach profile is used by the modem to attach to the LTE network. Data profile is used to send and receive data over the cellular network.
- Important Note: Enabling DNS option adds DNS Proxy. Domain Filtering is not supported when DNS Proxy is enabled.
- IPv6 deployment configuration using PPPoE has support for IPv6o6 inclusive of the Bridge and DHCP options.

**Figure 9 Cellular Backup WAN Configuration IR 829 Single LTE**

**Quick Setup Wizard**

Basic Primary WAN Backup WAN LAN IOX Wi-Fi Security & App Exp. Confirm & Apply

Backup WAN

Enable Backup WAN

WAN Connection Type \*: 3G/4G

Interface \*: Cellular 1/0 (SIM 1)

Enable Persistence:

**NAT**

Enable NAT

**SLA Configuration**

IP Address: 8.8.8.8

**Modem Settings**

**SIM 1**

Attach Profile \*: 1 vzwims

Advance Profile Options:

[Cancel](#)

[Previous](#) [Next](#)

**Help and Tips**

- If Service Provider has given static IP address then unselect the option "Get automatically from ISP".
- The IP address option "Get automatically from ISP" will use DHCP or IP Negotiated option to get the IP Address.
- Username and password are to be obtained from service provider if PPPoE option is enabled and PAP or CHAP is preferred as authentication mechanism.
- APN is provided by Service Provider and has to be obtained from the Service Provider prior to using in WAN configuration. Attach profile is used by the modem to attach to the LTE network. Data profile is used to send and receive data over the cellular network.
- Important Note: Enabling DNS option adds DNS Proxy. Domain Filtering is not supported when DNS Proxy is enabled.
- IPv6 deployment configuration using PPPoE has support for IPv6o6 inclusive of the Bridge and DHCP options.

## Ethernet WAN Configuration

1. In Primary WAN, select the Ethernet (Direct/PPPoE) as the WAN Connection Type. The Interface defaults to Gigabitinterface0.  
Get DNS Server info directly from ISP is checked.
2. Select the appropriate IP address configuration information based on whether you are configuring an IPv4 or IPv6 address.

## Using Quick Setup Wizard

- a. Specify the details for the IP address depending on whether the IP address is dynamically or statically assigned. There is an option to enable NAT configuration, and it is recommended to enable NAT for WAN interfaces. The IPv6 address can be either AutoConfig, Use Prefix from Provider, or Static IP Address.
  - b. If you have selected AutoConfig, enable the **Act as an IPv6 DHCP client** option.
  - c. If you have selected Prefix from Provider or Static IP Address option, enter Prefix and Prefix Mask details.
3. If you have enabled PPPoE, select the required authentication mode. You have PAP and CHAP options.
  4. Enter the user name and password provided by the service provider.
  5. Click **Next**.

**Figure 10 Ethernet Primary WAN Configuration IR 829**

**Quick Setup Wizard**

Basic Primary WAN Backup WAN LAN IOX Wi-Fi Security & App Exp. Confirm & Apply

WAN Configuration

WAN Connection Type \*: Ethernet (Direct / PPPoE)

Interface \*: GigabitEthernet0

**DNS / IP Address**

**DNS:**

- Get DNS Server info directly from ISP

**IPv4:**

- Get automatically from ISP
- Enable NAT

**IPv6:**

- Enable IPv6

Enable PPPoE  Enable IPv6oE

[Cancel](#) Previous Next

**Help and Tips**

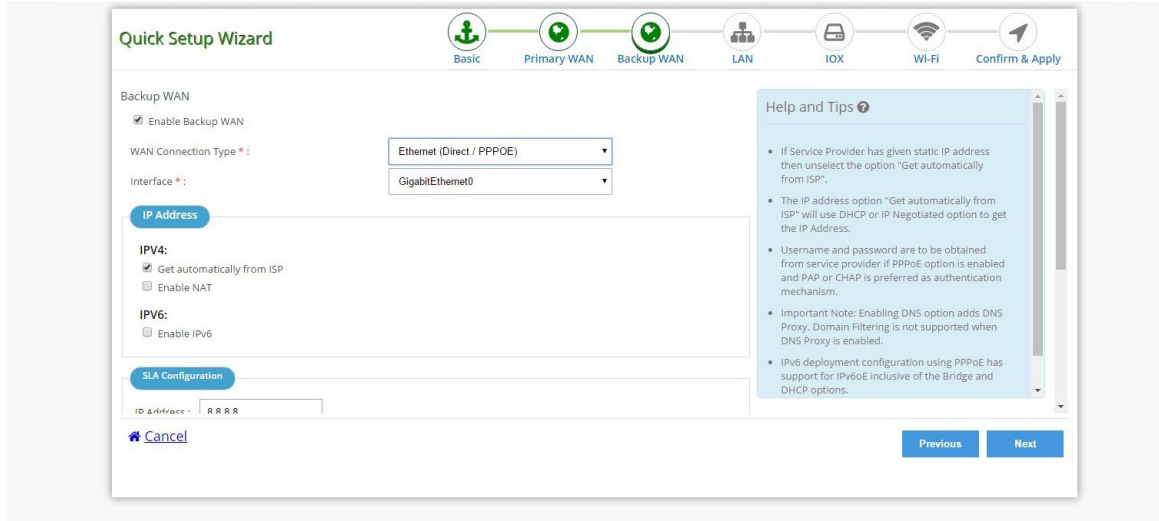
- If Service Provider has given static IP address / DNS then unselect the option "Get automatically from ISP".
- The IP address option "Get automatically from ISP" will use DHCP or IP Negotiated option to get the IP Address.
- Username and password are to be obtained from service provider: if PPPoE option is enabled and PAP or CHAP is preferred as authentication mechanism.
- APN is provided by Service Provider and has to be obtained from the Service Provider prior to using in WAN configuration.
- Important Note: Enabling DNS option adds DNS Proxy. Domain Filtering is not supported when DNS Proxy is enabled.

6. Select Enable Backup WAN option if you want to configure Back Up WAN. Follow the configuration steps 1 through 5, and then click **Next**.



Using Quick Setup Wizard

**Figure 11 Backup WAN Configuration IR 829**

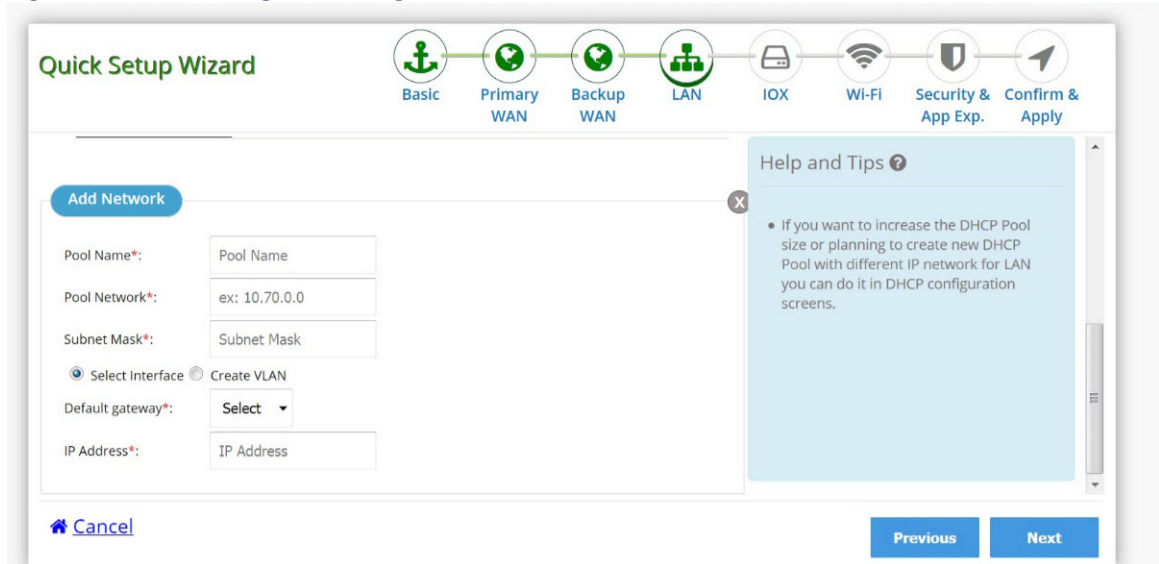


7. Click **Next** to complete the LAN configuration since the DHCP pool will be automatically configured. You can use the same DHCP pool for the LAN network.

## LAN Configuration

1. Select Change LAN network to edit the existing network.

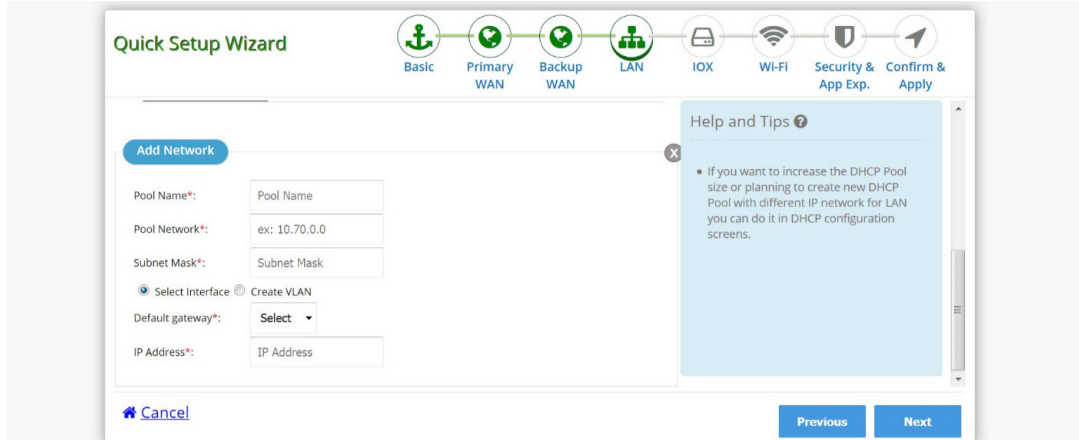
**Figure 12 LAN Configuration Page**



You will get a confirmation alert message before changing the existing network. Click OK to proceed.

2. If you want to add a new LAN network, select the add a new LAN network option.
3. Configure the new network with Pool Name, Pool Network, Subnet Mask, Default Gateway, and IP Address.

Figure 13 Configuration with LAN Network

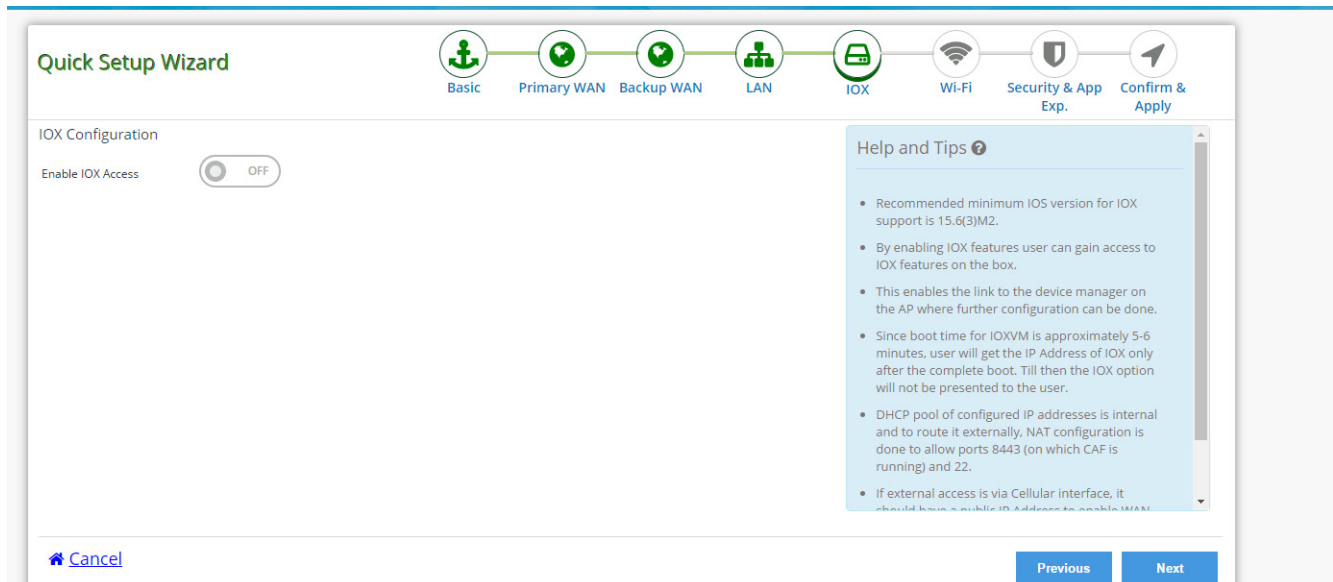


4. Click **Next** to configure IOX.

## IOX Configuration

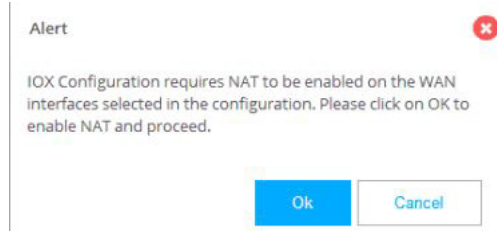
1. Click Enable IOX Access.

Figure 14 IOX



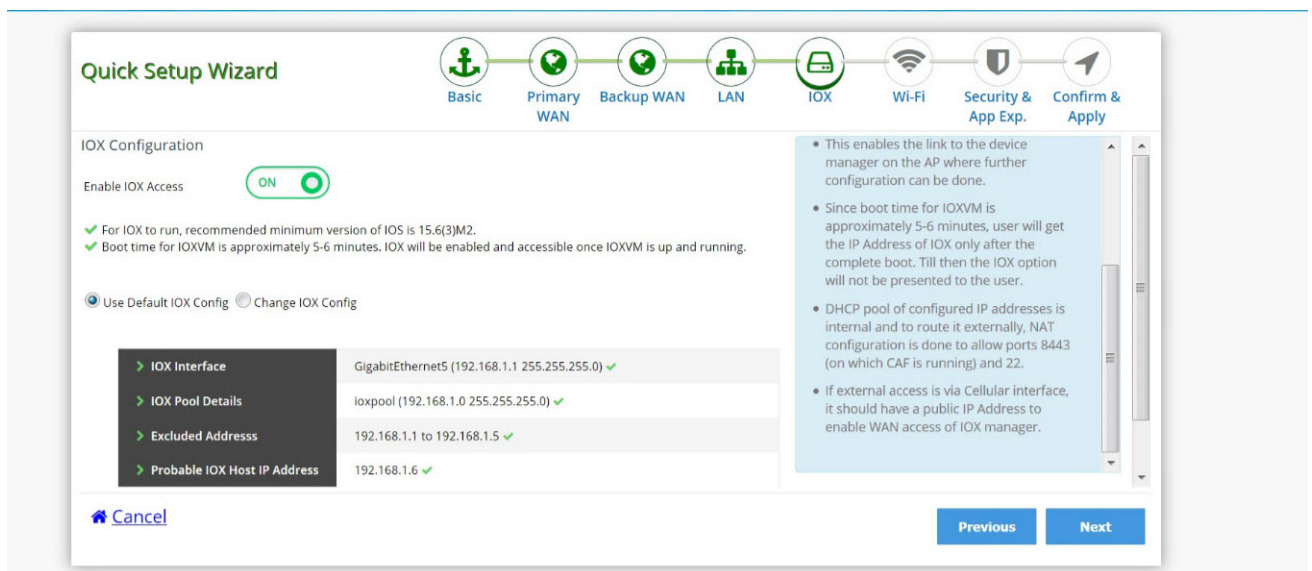
**Note:** If NAT is not enabled on the WAN, the following message appears:

Figure 15 NAT Alert Message



2. Click OK. Return back to the WAN page and enable NAT.
3. Click **Next** until you return to the IOX page.
4. Click Enable IOX Access. The button turns green for On.

Figure 16 IOX Configuration Page



5. If you want to change the IOX configurations, click Change IOX Config.

## Using Quick Setup Wizard

Figure 17 Change IOX Configuration

Quick Setup Wizard

Basic Primary WAN Backup WAN LAN IOX Wi-Fi Security & App Exp. Confirm & Apply

✓ Boot time for IOXVM is approximately 5-6 minutes. IOX will be enabled and accessible once IOXVM is up and running.

Use Default IOX Config  Change IOX Config

**IOX Configuration**

Pool Name\*: ioxpool

Pool Network\*: 192.168.1.0

Subnet Mask\*: 255.255.255.0

Excluded Address Range (Start)\*: 192.168.1.1

Excluded Address Range (End): 192.168.1.5

Default Router\*: 192.168.1.1

IOX Host Address: 192.168.1.6 ⓘ

IOX Interface: GigabitEthernet5

IOX Interface IP Address / Mask: 192.168.1.1 255.255.255.0

External Access Interface\*: Cellular 0/0 ⓘ

[Cancel](#)

[Previous](#) [Next](#)

**Help and Tips**

- Recommended minimum IOS version for IOX support is 15.6(3)M2.
- By enabling IOX features user can gain access to IOX features on the box.
- This enables the link to the device manager on the AP where further configuration can be done.
- Since boot time for IOXVM is approximately 5-6 minutes, user will get the IP Address of IOX only after the complete boot. Till then the IOX option will not be presented to the user.
- DHCP pool of configured IP addresses is internal and to route it externally, NAT configuration is done to allow ports 8443 (on which CAF is running) and 22.
- If external access is via Cellular interface, it should have a public IP Address to enable WAN access of IOX manager.

6. Click **Next** to configure WiFi if you have an IR 829. Otherwise, click **Next** to configure Security.

## Wi-Fi Configuration (only on IR 829 Routers)

**Note:** If you have an IR 809, you do not see this option.

1. Click Turn on Wi-Fi.

Figure 18 Wi-Fi

Quick Setup Wizard

Basic Primary WAN Backup WAN LAN IOX Wi-Fi Security & App Exp. Confirm & Apply

Wi-Fi Configuration

Turn on Wifi:  OFF

[Cancel](#)

[Previous](#) [Next](#)

**Help and Tips**

- User is provided with the option to enable and configure Wifi.
- This enables the link to the device manager on the AP where further configuration can be done if required.

2. Provide the Network Name, Security type, and password (for WPA and WPA2) to be configured as SSID on the AP.

Figure 19 Wi-Fi Configuration

**Quick Setup Wizard**

Wi-Fi Configuration

Turn on Wifi  ON

**Wifi Configuration**

BVI Interface IP Address \*: 192.168.193.143

Network Name \*: SSID

Security \*: Open

**Help and Tips**

- User is provided with the option to enable and configure Wifi.
- This enables the link to the device manager on the AP where further configuration can be done if required.

[Cancel](#) Previous Next

3. Click **Next**.

## Security Configuration

By default, Enable firewall features and Enable Application Visibility & Control are not checked. If you require these security settings:

1. Select Enable firewall features and then select create policy which allows basic traffic option to configure the security features.
2. Select Enable Cisco recommended security settings and then click **Next**.

Figure 20 Security Configuration

**Quick Setup Wizard**

Security Configuration

Enable Firewall Features

Router is capable of having security features

✔ Create policy which allows basic traffic(Recommended)

Enable Cisco recommended security settings

✔ This will ensure all passwords are not shown in plain text. They will be encrypted

Application Experience

Enable Application Visibility and Control

**Help and Tips**

- Enabling security will move all the LAN and WAN interfaces to specific security zones which is mandatory for enabling many security features.
- If no policy is explicitly configured, all traffic moving between zones is blocked as Firewall's default policy between zones is deny all. So enable the option which allows basic traffic. This will create a rule which allows basic protocols like HTTP, HTTPS, etc. and you can later alter or create different rules in Policy page.
- Cisco Application Visibility and Control (AVC) isolation is a suite of services in Cisco network devices that provides application-level classification, monitoring, and traffic control.

[Cancel](#) Previous Next

3. Click **Submit** to confirm the configuration changes in the summary screen.

## Using Quick Setup Wizard

Figure 21 Confirmation Screen (IR 829)

**Quick Setup Wizard**

Basic Primary WAN Backup WAN LAN IOX Wi-Fi Security & App Exp. Confirm & Apply

Summary

Basic / IOX / Wifi	Primary WAN	Backup WAN	LAN	Security & App Exp.
<ul style="list-style-type: none"> <li>Router Name: IR829</li> <li>Domain Name: cisco.com</li> <li>TimeZone: (GMT-07:00) Arizona</li> <li>DNS Server: Automatic</li> <li>NTP Server: Disabled</li> <li>IoX: Enabled</li> <li>Wifi: Disabled</li> </ul>	<ul style="list-style-type: none"> <li>WAN Interface: Cellular 0/0</li> <li>Ipv4: Automatic</li> <li>Ipv6: Not configured</li> <li>NAT: Enabled</li> <li>Persistence: Disabled</li> </ul>	<ul style="list-style-type: none"> <li>WAN Interface: Cellular 1/0</li> <li>Ipv4: Automatic</li> <li>Ipv6: Not configured</li> <li>NAT: Enabled</li> <li>Persistence: Disabled</li> </ul>	<ul style="list-style-type: none"> <li>Pool Name: ccp-pool</li> <li>LAN Network: 10.10.10.0</li> <li>Subnet Mask: 255.255.255.128</li> <li>Default gateway: Vlan1 (10.10.10.1)</li> </ul>	<ul style="list-style-type: none"> <li>WAN Zone: Cellular 0/0 Cellular 1/0</li> <li>LAN Zone: Vlan 1 with switch ports GigabitEthernet</li> <li>Default policy creation: Allow</li> <li>Cisco recommended security settings: Enabled</li> <li>Application Visibility and Control(AVC): Enabled</li> </ul>

CLI Preview

[Cancel](#) Previous Submit

Figure 22 Confirmation Screen (IR 809)

**Quick Setup Wizard**

Basic Primary WAN Backup WAN LAN Security & App Exp. Confirm & Apply

Summary

Basic	Primary WAN	Backup WAN	LAN	Security & App Exp.
<ul style="list-style-type: none"> <li>Router Name: TestRouter</li> <li>Domain Name: MyDomain.com</li> <li>TimeZone: (GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi</li> <li>DNS Server: Automatic</li> <li>NTP Server: asia.pool.ntp.org</li> </ul>	<ul style="list-style-type: none"> <li>WAN Interface: GigabitEthernet0/0</li> <li>Ipv4: Automatic</li> <li>Ipv6: Not configured</li> <li>NAT: Enabled</li> <li>PPPoE: Enabled</li> </ul>	<ul style="list-style-type: none"> <li>WAN Interface: GigabitEthernet0/2</li> <li>Ipv4: Automatic</li> <li>Ipv6: Not configured</li> <li>NAT: Enabled</li> <li>PPPoE: Enabled</li> </ul>	<ul style="list-style-type: none"> <li>Pool Name: ccp-pool</li> <li>LAN Network: 10.10.10.0</li> <li>Subnet Mask: 255.255.255.128</li> <li>Default gateway: [10.10.10.1]</li> <li>New LAN Network</li> </ul>	<ul style="list-style-type: none"> <li>WAN Zone: GigabitEthernet0/0 GigabitEthernet0/2</li> <li>LAN Zone: Vlan 1 with switch ports GigabitEthernet</li> <li>Default policy creation: Allow</li> <li>Cisco recommended security settings: Enabled</li> <li>Application Visibility and</li> </ul>

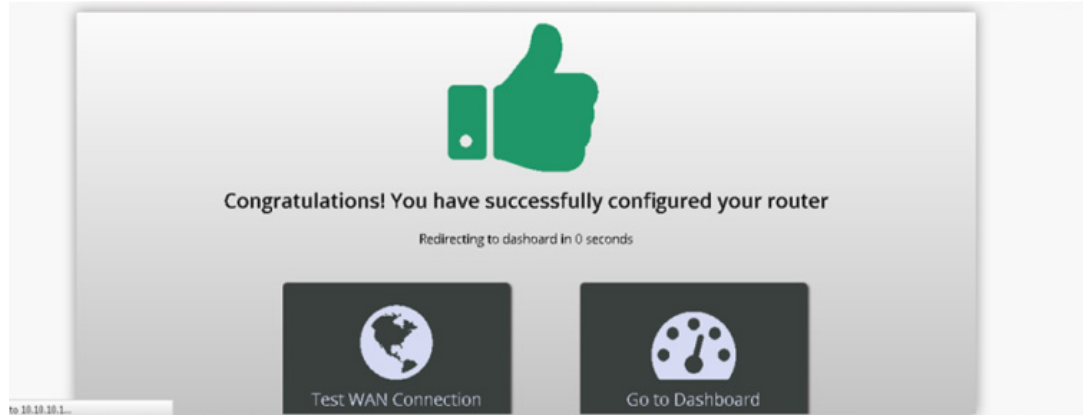
CLI Preview

[Cancel](#) Previous Submit

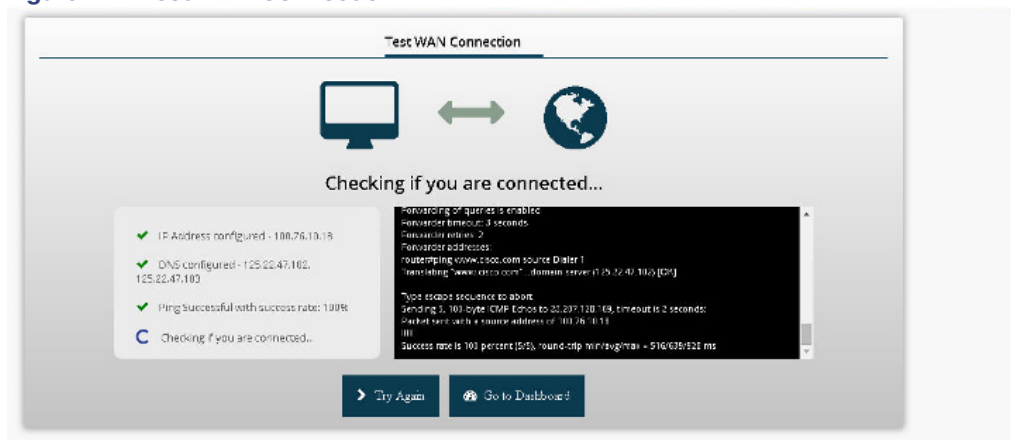
A message appears saying configuration may take some time to configure and whether you want to continue the configuration.

- Click **Yes** to continue the configuration changes.

Configuration using the Quick Setup Wizard is complete and a completion message appears.

**Figure 23 Configuration Completion using Quick Setup Wizard**

5. (Optional) If you want to check the status of your WAN connection, click **Test WAN Connection**.

**Figure 24 Test WAN Connection**

## Using CCP Express Advanced Mode

This section explains how to configure Cisco IR routers using CCP Express advanced mode. The screens and configuration steps may slightly vary depending on the WAN configuration options and the software features supported by the Cisco IR routers.

The Advanced Mode contains the following options:

- [CCP Express Home Page, page 16](#)
- [General Settings, page 17](#)
- [DHCP/DNS, page 21](#)
- [Interfaces, page 24](#)
- [Identity, page 30](#)

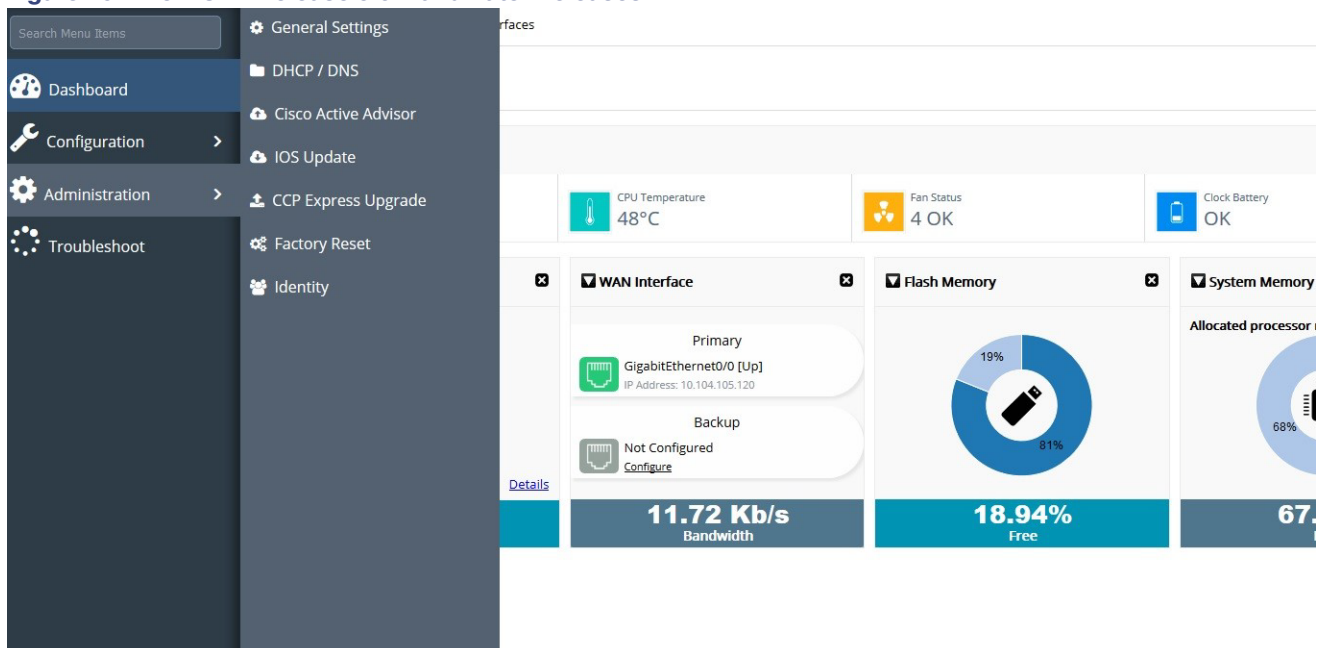
- [Static Routing, page 33](#)
- [Dashboard, page 35](#)
- [Troubleshooting, page 42](#)
- [Access Control Lists \(ACLs\), page 44](#)
- [IOx, page 48](#)
- [Wireless, page 52](#)
- [Security Features, page 54](#)

## CCP Express Home Page

Once the configuration is pushed, you will be automatically redirected to the Dashboard page in the Advanced Settings section.

CCP Express by default loads in the New UI from version 3.5.1 onwards. User can switch back to the old UI by using the Option in Preferences-> Classic View. All existing features are arranged under 4 groups on the left: Dashboard, Configuration, Administration and Troubleshoot. The quick access utility pages/options are on the top right.

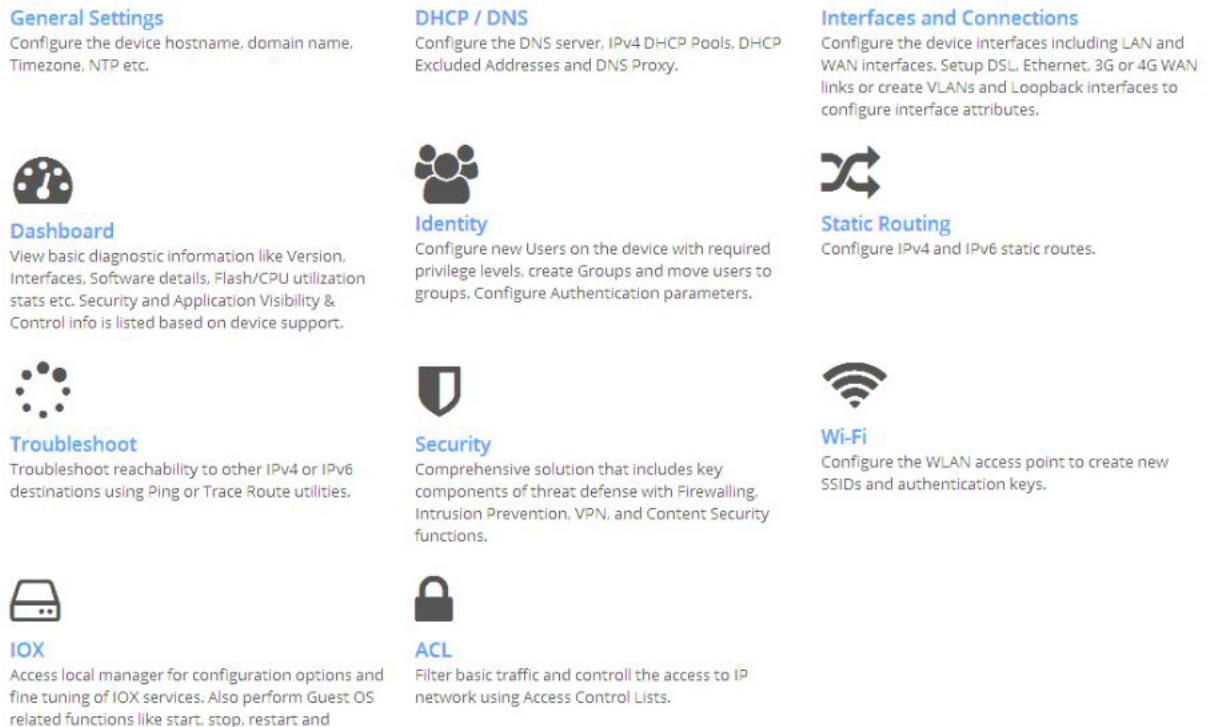
**Figure 25 New UI in Release 3.5.1 and Later Releases**



You can switch between the two UIs using the option in Preferences section.

Below are samples of the old UI.



**Figure 26 CCP Express Home Page (IR 829)**

You can get to the CCP Express Home page by clicking on Advance Mode after going through the Quick Setup Wizard or by clicking the home icon on the right side of the page:



Figure 26 shows CCP Express home page where you can navigate to all the features.

**Note:** Since the IR809 does not support Wi-Fi, the Wireless option is not available.

## General Settings

Click this option to configure Device and Time.

If you used the Quick Setup Wizard to configure your router, the device settings shown in Figure 27 are automatically listed here. If not, enter the Host name and Domain name.

**Figure 27 Device Settings**

The screenshot shows the 'Device' tab selected in the Cisco Configuration Professional Express interface. The 'Time' sub-tab is also visible. The main content area is titled 'Host name/Domain name'. It contains three input fields: 'Host name \*:' with the value 'yourname', 'Domain name:' with the value 'yourdomain.com', and a larger 'Banner' text area. An 'Apply' button is located at the bottom of the form.

Use the Time tab to change the timezone. You can also synchronize to the NTP server or make the router an NTP master.

**Figure 28 Time Settings**

The screenshot shows the 'Time' tab selected in the Cisco Configuration Professional Express interface. The main content area is titled 'Timezone/NTP'. It contains a 'TimeZone \*:' dropdown menu with the selected value '(GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi'. Below the dropdown are two checkboxes: 'Synchronize with NTP Server' and 'Make this router as NTP Master', both of which are currently unchecked. An 'Apply' button is located at the bottom of the form.

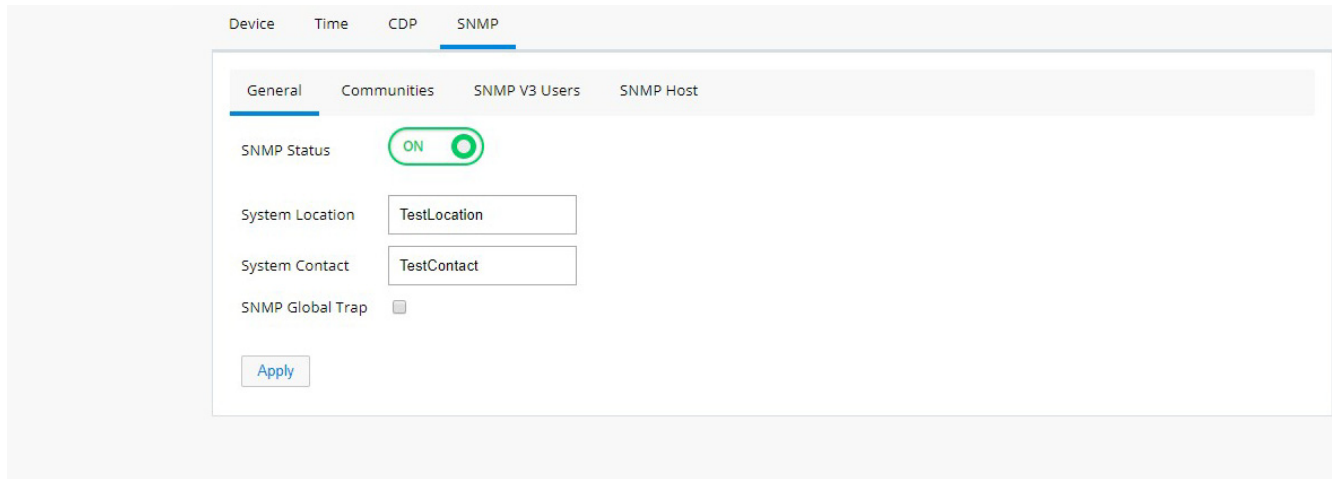
## SNMP Configuration

To enable SNMP configuration:

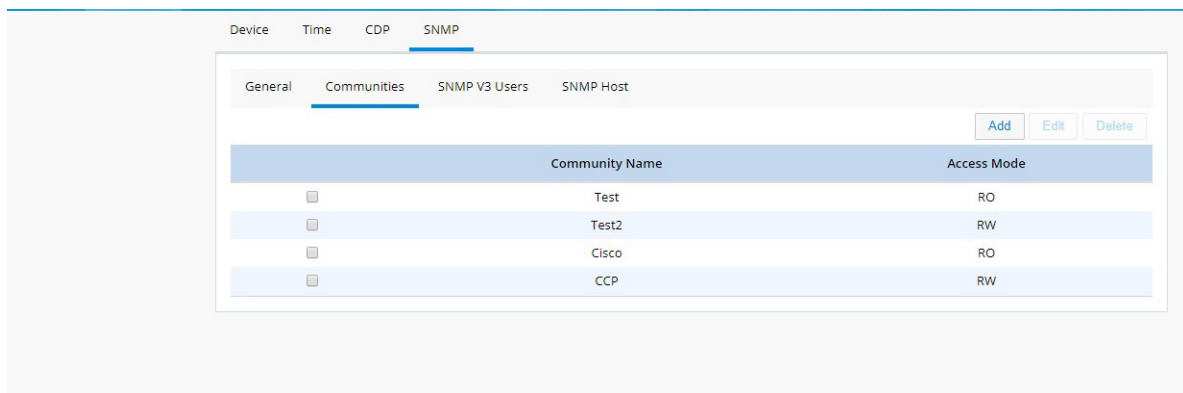
1. Go to General Settings
2. Click the SNMP Tab.

All options are available under different tabs once SNMP is enabled on the box.

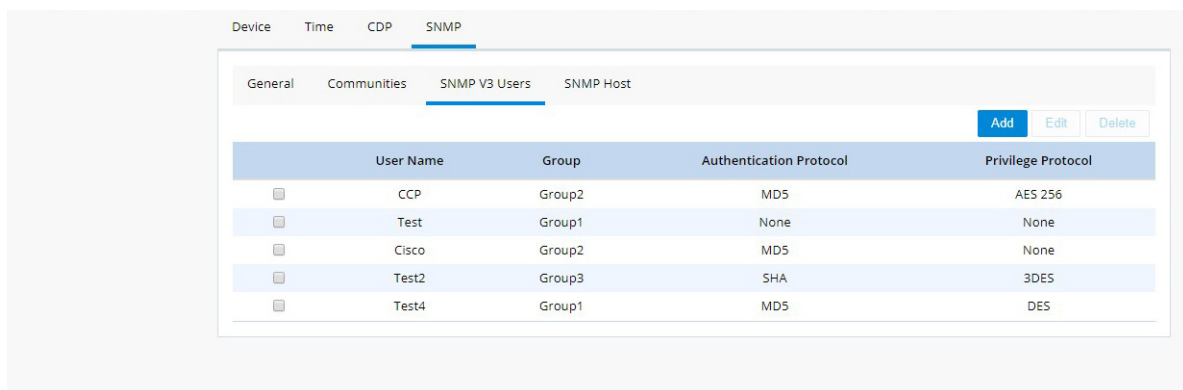
**Figure 29 General SNMP Settings**



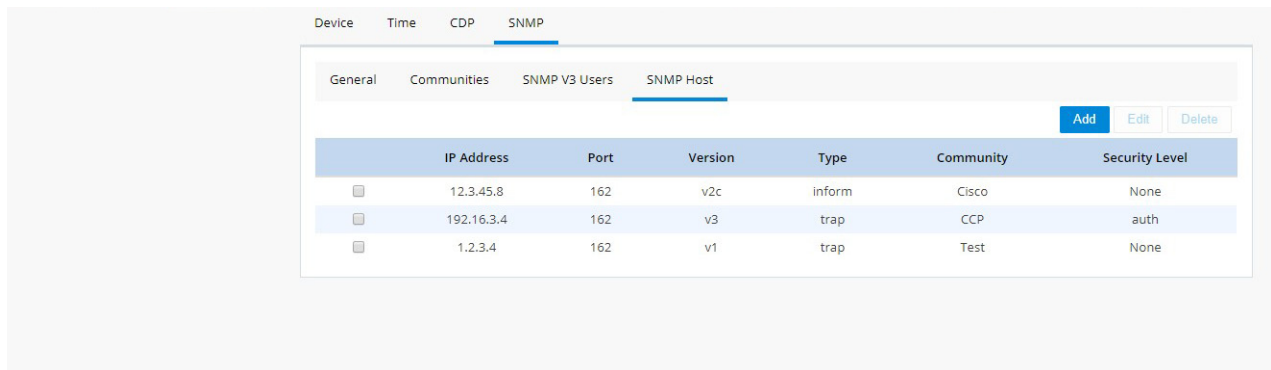
**Figure 30 SNMP Communities**



**Figure 31 SNMP V3 Users**



**Figure 32 SNMP Host**

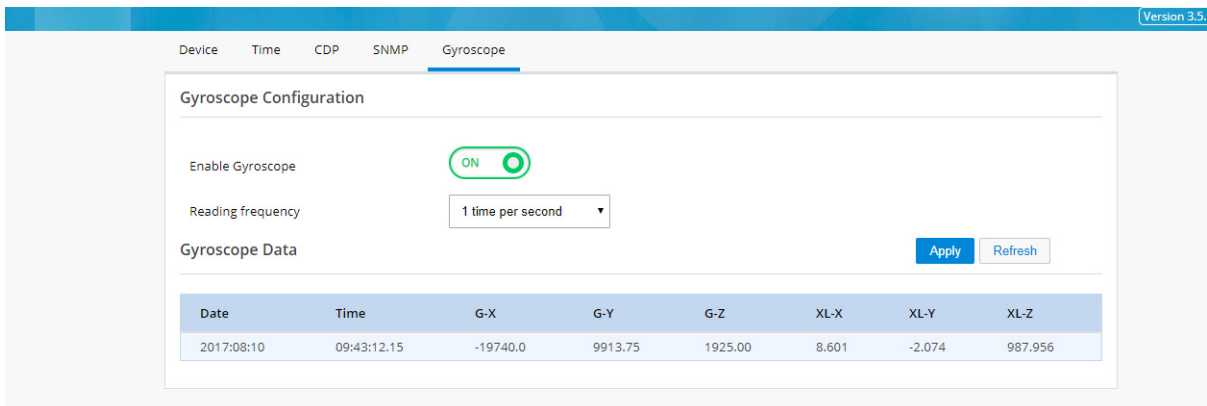


## Gyroscope

Gyroscope is used to determine the position of the device.

1. Go to General Settings
2. Click the Gyroscope Tab.

**Figure 33 Gyroscope**



3. Click the Enable Gyroscope.
4. Select the Reading frequency from the menu.
5. Click **Apply**.

## HTTP/HTTPS Configuration

Http/Https configuration is available under General Settings -> HTTP/HTTPS tab.

**Note:** This feature is available in Release 3.5.1 and later.

**Figure 34 HTTP/HTTPS Configuration**

**HTTP/HTTPS Access Configuration**

Enter the configuration for access via HTTP/HTTPS.

HTTP Access	<input checked="" type="checkbox"/>	HTTP Port	<input type="text" value="80"/>
HTTPS Access	<input checked="" type="checkbox"/>	HTTPS Port	<input type="text" value="443"/>
Enable HTTP Upload	<input checked="" type="checkbox"/>		
Enable File Overwrite	<input checked="" type="checkbox"/>		
HTTP Upload Path	<input type="text" value="flash:"/>		

**Timeout Policy Configuration**

Session Idle Timeout (secs)	<input type="text" value="60"/>
Server Life Time (secs)	<input type="text" value="86400"/>
Max Number of Requests	<input type="text" value="10000"/>

## DHCP/DNS

In this area, you can configure the following options:

- [DNS](#)
- [DDNS](#)
- [DHCP](#)
- [DHCP Excluded Addresses](#)

## DNS

**Figure 35 Primary and Secondary DNS**

DNS DDNS DHCP DHCP Excluded Address

**DNS**

Enter the Primary and Secondary server IP addresses provided by your network administrator or ISP provider.

Primary DNS

Secondary DNS

## DDNS

If you have not completed setting up your WAN interface, you see the following message:

DNS DDNS DHCP DHCP Excluded Address

**DDNS**

WAN interface configuration not done yet, [click here](#) to Configure.

## DHCP

**Figure 36 DHCP**

DNS DDNS **DHCP** DHCP Excluded Address

**DHCP**

	Pool Name	Pool Network	Subnet Mask	Default Router	Action
<input type="checkbox"/>	ccp-pool	10.10.10.0	255.255.255.128	10.10.10.1	

### Configuring a LAN with DHCP

Perform the following steps to create a DHCP pool.

1. Click **DHCP/DNS** and DHCP to open the DHCP tab.
2. From the DHCP interface, click **Add** to create a new DHCP pool by specifying:

- **Pool Name:**—The name of the DHCP pool.
- **Pool Network:**—The IP address of the subnet that represents all IP addresses allocated to the wired or wireless clients.
- **Subnet Mask:**—The subnet mask.
- **Import all DHCP options in to the DHCP server database:** Check this check box to import all DHCP options into the DHCP server database. This ensures that the DNS is read from your service provider and is propagated to all DHCP clients.

**Figure 37 Add DHCP Pool**

The screenshot shows a dialog box titled "Add DHCP Pool" with a close button (red X) in the top right corner. The dialog contains the following fields and controls:

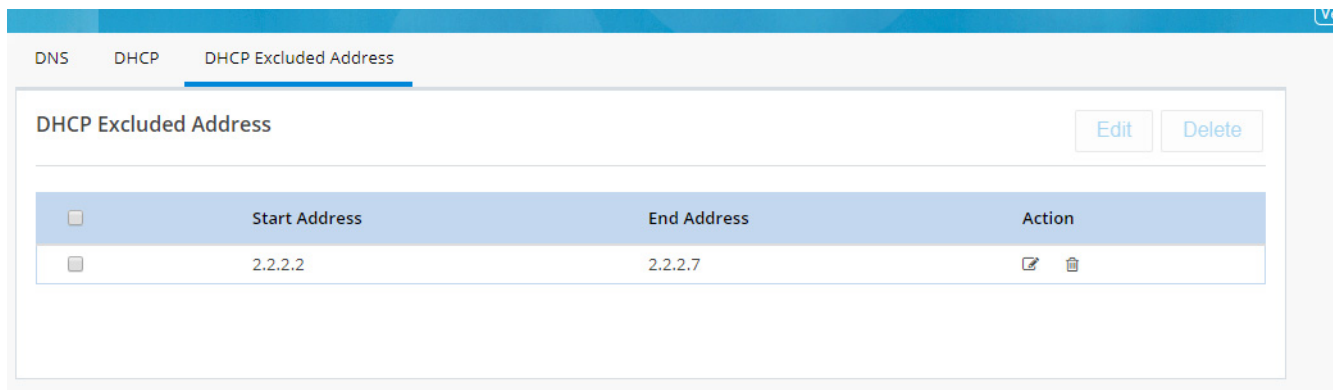
- Pool Name \*:** Text input field with placeholder "Pool Name".
- Pool Network \*:** Text input field with placeholder "ex: 10.70.0.0".
- Subnet Mask \*:** Text input field with placeholder "Subnet Mask".
- Default Gateway:** Text input field with placeholder "ex: 10.70.180.1".
- Enable DNS Proxy:** Unchecked checkbox.
- Include DNS values within this DHCP Pool:** Unchecked checkbox.
- DNS Primary Address:** Text input field with placeholder "ex: 10.70.172.10".
- DNS Secondary Address:** Text input field with placeholder "ex: 10.70.180.1".
- DHCP Exclude Start Address:** Text input field with placeholder "ex: 192.169.0.0".
- DHCP Exclude End Address:** Text input field with placeholder "ex: 192.169.0.0".
- Import all DHCP options in to the DHCP:** Checked checkbox.
- Buttons:** "Ok" and "Cancel" buttons at the bottom right.

3. Click **OK** to create the DHCP pool.

## DHCP Excluded Addresses

To configure DHCP Excluded Addresses:

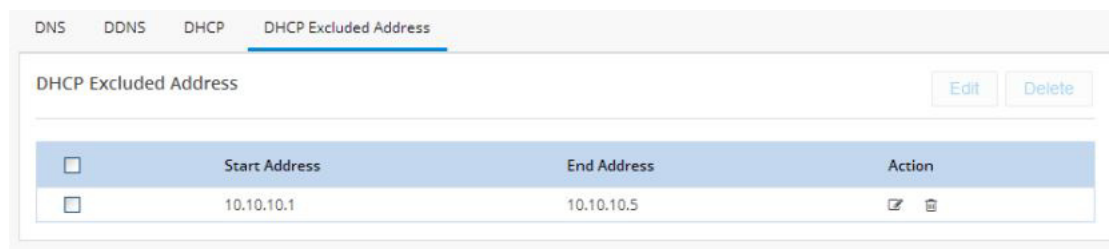
1. Click **DHCP/DNS** and **DHCP** to open the DHCP tab.
2. Click **Add** to create a new pool with the excluded addresses. Or, click **Edit** to add the excluded addresses to an existing pool.

**Figure 38 Configure DHCP Excluded Addresses**

3. Enter the Start and End DHCP excluded addresses. Ensure the start address value is smaller than the end address value.

To edit an existing DHCP Excluded Address:

1. Click **DHCP/DNS** and DHCP Excluded Addresses tab.
2. Select the address, and click **Edit**.

**Figure 39 Edit a DHCP Excluded Address**

3. Specify the IPv4 address which is the starting for the range to be excluded.
4. Specify the IPv4 address which is the end of range to be excluded.
5. Click OK.

To delete an existing DHCP Excluded Address:

1. Click **DHCP/DNS** and DHCP Excluded Addresses tab.
2. Select the address, and click **Delete**. See [Figure 39](#).

## Interfaces

Use this option to configure primary and/or backup for Ethernet and Cellular interfaces.



**Figure 40 Interfaces List**

Interface

ADD Loopback Create VLAN EDIT DELETE DETAILS

Primary WAN:Not Configured Backup WAN:Not Configured Zones

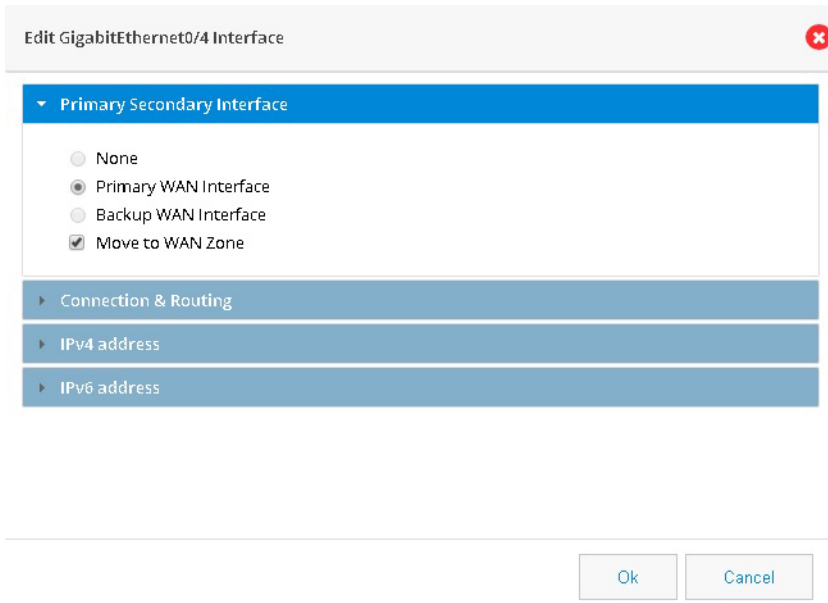
\*Note: Multiple selection is not allowed

Interface	IPv4 Address	IPv6 Address	Admin Status	Operational Status	Description	Action
Configurable Interfaces						
<input type="checkbox"/> GigabitEthernet0			⚠	down		✎ 🗑
<input type="checkbox"/> GigabitEthernet1			🟢	up		✎ 🗑
<input type="checkbox"/> GigabitEthernet2			🟢	up		✎ 🗑
<input type="checkbox"/> GigabitEthernet3			🟢	down		✎ 🗑
<input type="checkbox"/> GigabitEthernet4			🟢	down		✎ 🗑
<input checked="" type="checkbox"/> Cellular0/0		⋮ 🇺🇸	🟢	up		✎ 🗑
<input type="checkbox"/> Cellular1/0		⋮ 🇺🇸	🟢	up		✎ 🗑
<input type="checkbox"/> Vlan1	10.10.10.1		🟢	up	SETH_LANS	✎ 🗑
<input type="checkbox"/> Vlan100	192.168.193.118		🟢	up		✎ 🗑
Read-only interface						
Wlan-GigabitEthernet0			🟢	up		
Wpan2			🟢	down		
Async0			🟢	down		
Async1			🟢	down		
GigabitEthernet5			⚠	down		
Cellular0/1		⋮ 🇺🇸	🟢	down		
Cellular1/1		⋮ 🇺🇸	🟢	down		
wlan-ap0	10.10.10.1		🟢	up		

The Zones link takes you to the Zones page under the Security option. See [Figure 73 on page 54](#).

## Setting Up a Primary Ethernet WAN Interface

1. Click **Interfaces** to open the Interfaces page.
2. Select the GigabitEthernet Interface you want to configure and click **Edit**. The Edit GigabitEthernet Configuration page is displayed.

**Figure 41 GigabitEthernet Interface Configuration**

3. Select Primary WAN Interface from Primary Secondary Interface tab.
4. From the Connection & Routing tab, check Enable PPPoE check box, and enter the description in the description field. For IPv4 Routed Protocol, you may configure Ipv6oE with options of Bridge or DHCP configuration.
5. From the Connection tab, check Enable PPPoE check box, and enter the description in the Description field.
6. Based on whether you are configuring an IPv4 or IPv6 address, select the appropriate tab. Specify the details for the IP address depending on whether the IP address is dynamically or statically assigned.

For configuring an IPv4 address:

This can be either Easy IP (IP Negotiated), Static IP Address, or No IP Address. By default, the IPv4 address is IP negotiated. There is an option to enable NAT configuration and the recommendation is to enable NAT for WAN interfaces. This will create NAT overloading configuration hence all LAN IPs are translated to public IP before being sent to WAN uplink.

For configuring an IPv6 address:

Select the IPv6 address type. The IPv6 address can be either AutoConfig, Use Prefix from Provider, Static IP Address, or No IP Address.

7. From the Authentication tab, check CHAP or PAP check box and specify the username and password given by Service provider.
8. Click **OK** to confirm the configuration.

## Setting up a Primary Cellular Interface

1. Click on the cellular interface you want to create as a primary.

**Figure 42 Edit Cellular Interface**

Edit Cellular0/0 Interface

Primary Secondary Interface

Model Id:	MC7455MOBILE	Modem Firmware Version:	SW9X30C_02.20.03.00
IMEI:	352009080052058	IMSI:	001012345678901

None  
 Primary WAN Interface  
 Backup WAN Interface  
 Enable NAT

Do you want to make a Persistent connection?  Yes  No

Access Point Name

Ok Cancel

2. Select Primary WAN Interface.
3. (Optional) Enable NAT.
4. (Optional) Select Move to WAN Zone to add this interface to a zone. If you select this option, the following message appears:

Alert

This interface will be added to WAN zone. Please make sure to configure appropriate Firewall Policy. Also CWS and IPS will be applied to this interface, if they are already configured. Do you want to continue?

Yes No

5. Click Yes to continue.
6. If you want to establish a persistent connection to your service provider, select **Yes**. By default, this is set to **No** to disable persistent connection.
7. Click OK.

In the main Interfaces list, the Primary WAN Interface is green and lists the primary interface.

**Figure 43 Configured Cellular Primary Interface**

Interface ADD Loopback Create VLAN EDIT DELETE

Primary WAN: Cellular0/0 Backup WAN: Not Configured [Zones](#)

*\*Note: Multiple selection is not allowed*

Interface	IPv4 Address	IPv6 Address	Admin Status	Operational Status	Description	Action
Configurable Interfaces						
<input type="checkbox"/> GigabitEthernet0			⬇️	down		
<input type="checkbox"/> GigabitEthernet1			⬆️	up		
<input type="checkbox"/> GigabitEthernet2			⬆️	up		
<input type="checkbox"/> GigabitEthernet3			⬆️	down		
<input type="checkbox"/> GigabitEthernet4			⬆️	down		
<input type="checkbox"/> Cellular0/0			📶 🇺🇸	down		
<input type="checkbox"/> Cellular1/0			📶 🇺🇸	up		
<input type="checkbox"/> Vlan1	10.10.10.1		⬆️	up	SETH_LANS	
<input type="checkbox"/> Vlan100	192.168.193.118		⬆️	up		
Read-only interface						
Wlan-GigabitEthernet0			⬆️	up		
Wpan2			⬆️	down		
Async0			⬆️	down		
Async1			⬆️	down		
GigabitEthernet5			⬇️	down		
Cellular0/1			📶 🇺🇸	down		
Cellular1/1			📶 🇺🇸	down		
NVI0	127.1.3.2		⬆️	up		
wlan-ap0	10.10.10.1		⬆️	up		

## Setting up a Backup Cellular Interface

1. Click on the cellular interface you want to create as a primary.

**Figure 44 Edit Cellular Interface**

Edit Cellular0/0 Interface

Primary Secondary Interface

Model Id:	MC7455MOBILE	Modem Firmware Version:	SW19X30C_02.20.03.00
IMEI:	352009080052058	IMSI:	001012345678901

None  
 Primary WAN Interface  
 Backup WAN Interface  
 Enable NAT

Do you want to make a Persistent connection?  Yes  No

Access Point Name

Ok Cancel

**2. Select Backup WAN Interface.**

The SLA Configuration box displays.

**3. (Optional) Enter the IP address of a reliable website to check connectivity.**

**4. (Optional) Enable NAT.**

**5. (Optional) Select Move to WAN Zone to add this interface to a zone. If you select this option, the following message appears:**

Alert

This interface will be added to WAN zone. Please make sure to configure appropriate Firewall Policy. Also CWS and IPS will be applied to this interface, if they are already configured. Do you want to continue?

Yes No

In the main Interfaces list, the Backup WAN Interface is green and lists the backup interface.

**Figure 45 Configured Cellular Backup Interface**

Interface

ADD Loopback Create VLAN EDIT DELETE

Primary WAN: Cellular0/0 Backup WAN: Cellular1/0

[Zones](#)

\*Note: Multiple selection is not allowed

Interface	IPv4 Address	IPv6 Address	Admin Status	Operational Status	Description	Action
Configurable Interfaces						
<input type="checkbox"/>	GigabitEthernet0		⊖	down		✎ ⌵
<input type="checkbox"/>	GigabitEthernet1		⊕	up		✎ ⌵
<input type="checkbox"/>	GigabitEthernet2		⊕	up		✎ ⌵
<input type="checkbox"/>	GigabitEthernet3		⊕	down		✎ ⌵
<input type="checkbox"/>	GigabitEthernet4		⊕	down		✎ ⌵
<input type="checkbox"/>	Cellular0/0		⋮	down		✎ ⌵
<input type="checkbox"/>	Cellular1/0		📶	down		✎ ⌵
<input type="checkbox"/>	Vlan1	10.10.10.1	⊕	up	SETH_LANS	✎ ⌵
<input type="checkbox"/>	Vlan100	192.168.193.118	⊕	up		✎ ⌵
Read-only interface						
	Wlan-GigabitEthernet0		⊕	up		
	Wpan2		⊕	down		
	Async0		⊕	down		
	Async1		⊕	down		
	GigabitEthernet5		⊖	down		
	Cellular0/1		⋮	down		
	Cellular1/1		📶	down		
	NV10	127.1.3.2	⊕	up		
	wlan-ap0	10.10.10.1	⊕	up		

## Create VLANs (only for IR 829)

**Note:** VLANs are not supported on IR 809.

1. Click **Add VLAN** to open the Add VLAN dialog box and specify a unique ID for the VLAN being created.
2. From the IPv4 address tab, choose Select from DHCP, and then select the DHCP pool from the drop-down list. This enables you to assign the IP addresses from the DHCP pool that is created.

or

Select Static IP to assign a unique IP address to the VLAN.

3. Click **OK** to confirm the configuration.

## Identity

Identity awareness is a key requirement for any Security solution. It is defined as the ability of the device to be aware of end-user identities. Also this supports User and Group management that allows administration of user authentication and authorization profiles using either local or external service.

## Authentication

To configure authentication:

1. Click **Identity > Authentication**.
2. In Authentication Servers section, select the **local** or **remote** option.

- Enable local (on-box) server—Router acts as the local authentication server.
- Enable remote (external) server—Active Directory is supported.

If remote option is selected, the ADD new server option appears.

- a. Click ADD new server.
- b. Enter the LDAP details: IP address of the server and Base DN information. Click **OK**.

**Note:** You can choose to configure both the server options. If both are configured, first attempt with authentication is with the remote server. If the remote server is not reachable, authentication falls back to the local server.

3. In the Authentication Services section, you can select Web Auth or NTLM.

The authentication method can be chosen for different zones, but in the current release only LAN zone is supported. If LAN Zone is configured, all interfaces coming under LAN zone are configured accordingly. NTLM option is supported only for remote server option. If the you configure both on-box and remote server options, selecting NTLM option is not allowed.

**Figure 46 Authentication Page**

**Authentication Servers**

Enable local (on-box) server  
 Enable remote (external) server

Profile Name	Type	Server IP	Action
LDAP-SERVER	LDAP	1.1.1.1	

**Authentication Services**

Zone	Method
LAN	Web Auth

**Figure 47 Add/Edit LDAP Page**

Add/Edit LDAP

Type Of Server\*: LDAP

Server IP\*: 10.10.1.1

Base Dn\*: cn=users,dc=utm-ad,dc:

Ok Cancel

## Managing User Groups

To create or delete user groups or to see the list of created user groups:

1. Click **Identity > Groups**. The list of available groups is displayed.
2. Click **Add**. Enter the user name in the popup.
3. Enter the group name to be created.

**Figure 48 Group Management Page**

Authentication Groups Users Monitor View

Group Management Add Delete

<input type="checkbox"/>	Group Name	Action
<input type="checkbox"/>	test	

4. To delete any group, select the check box and click on **Delete** and confirm.

## Managing Users

Steps to create a new user and associate/dissociate a user with a group are listed below:

1. Click **Identity > Users**. All created user names are listed. (Figure 49)
2. Click Add. The add user popup is displayed.



3. Enter the user details and click **Ok**.

**Figure 49 User Management Page**

Authentication   Groups   **Users**   Monitor View

User Management

Search User(s)

	Username	Privilege Level	User Type	Parser View	Group	Action
<input type="checkbox"/>	jean	15	Admin User	NO	No Group	
<input type="checkbox"/>	ccp	15	Admin User	NO	No Group	
<input type="checkbox"/>	testuser	15	Admin User	NO	test	
<input type="checkbox"/>	priv7	7	No Access	NO	No Group	
<input type="checkbox"/>	priv14	14	Monitor User	NO	No Group	
<input type="checkbox"/>	test123	15	Admin User	NO	No Group	
<input type="checkbox"/>	p14user	14	Monitor User	NO	No Group	
<input type="checkbox"/>	monuser	14	Monitor User	NO	No Group	
<input type="checkbox"/>	ftp-user	1	No Access	NO	No Group	

**Figure 50 Add User Page**

**Add User**

Username \*:

Password \*:

Confirm Password \*:

Select Group:

User Type:  Admin User  Monitor User  No Access

Privilege Level:

Encrypt password using MD5 Hash Algorithm

## Static Routing

The Static Routing feature allows you to add, edit, and delete IP routes to a destination interface, or IP address from your IPv4 or IPv6 subnets.

This section contains:

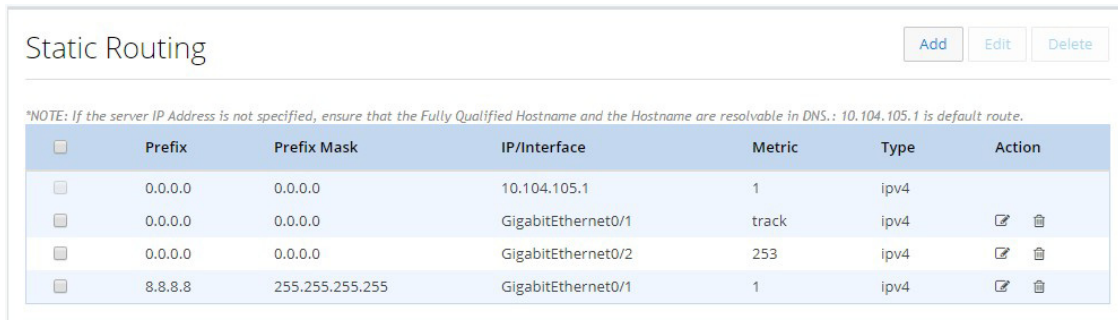
- [Creating a Static Route, page 34](#)
- [Editing a Static Route, page 35](#)
- [Deleting a Static Route, page 35](#)

## Creating a Static Route

To create a static route:

1. Click **Static Routing** to open the Static Routing page.

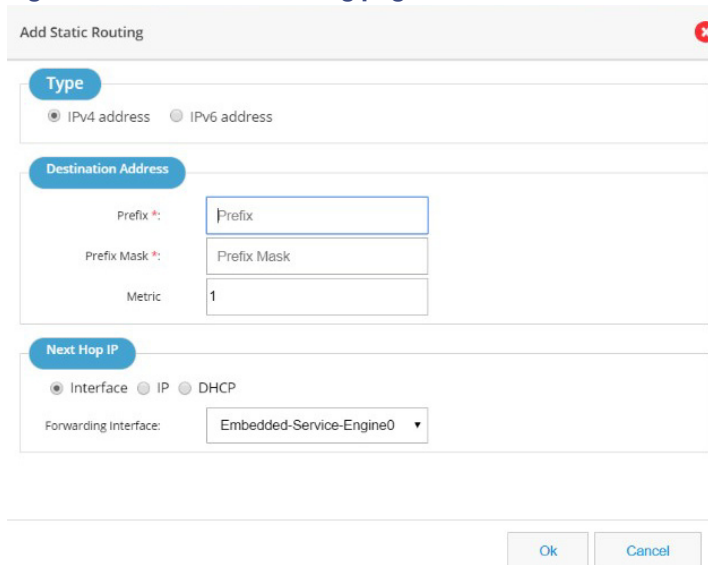
**Figure 51 Static Routing**



<input type="checkbox"/>	Prefix	Prefix Mask	IP/Interface	Metric	Type	Action
<input type="checkbox"/>	0.0.0.0	0.0.0.0	10.104.105.1	1	ipv4	
<input type="checkbox"/>	0.0.0.0	0.0.0.0	GigabitEthernet0/1	track	ipv4	
<input type="checkbox"/>	0.0.0.0	0.0.0.0	GigabitEthernet0/2	253	ipv4	
<input type="checkbox"/>	8.8.8.8	255.255.255.255	GigabitEthernet0/1	1	ipv4	

2. Click **Add** to open the Add Static Routing dialog box with options to specify an IPv4 or IPv6 static route.

**Figure 52 The Static Routing page**



Add Static Routing ✖

**Type**

IPv4 address  IPv6 address

**Destination Address**

Prefix \*:  
Prefix Mask \*:  
Metric: 1

**Next Hop IP**

Interface  IP  DHCP

Forwarding interface: Embedded-Service-Engine0 ▼

Ok Cancel

3. Based on whether the IP address is an IPv4 or IPv6 address, select the IPv4 or IPv6 tab, and specify the following:

- **Destination address:** Specify the prefix and prefix mask for your IPv4 or IPv6 address.

- **Next Hop IP:**  
If you select Interface as the next hop IP, select the forwarding interface from the drop-down list.  
If you select IP as the next hop IP, specify the Next Hop IP that must be used.  
You can also specify DHCP address.
- 4. Click **OK** to add the static route.

## Editing a Static Route

To edit an existing static route:

1. Click **Static Routing** to open the Static Routing page.
2. From the list of static routes, select the static route you want to edit, and click **Edit**.  
The Edit Static Routing page is displayed.
3. Specify these fields for your static route:
  - Destination address: specify the prefix and prefix mask for your IPv4 or IPv6 address
  - **Next Hop IP:**  
If you select Interface as the next hop IP, select the forwarding interface from the drop-down list.  
If you select IP as the next hop IP, specify the Next Hop IP that must be used.
4. Click **OK** to edit the static route.

## Deleting a Static Route

To delete a static route:

1. Click **Static Routing** to open the Static Routing page.
2. From the list of static routes, select the static route you want to delete, and click **Delete**.

## Dashboard

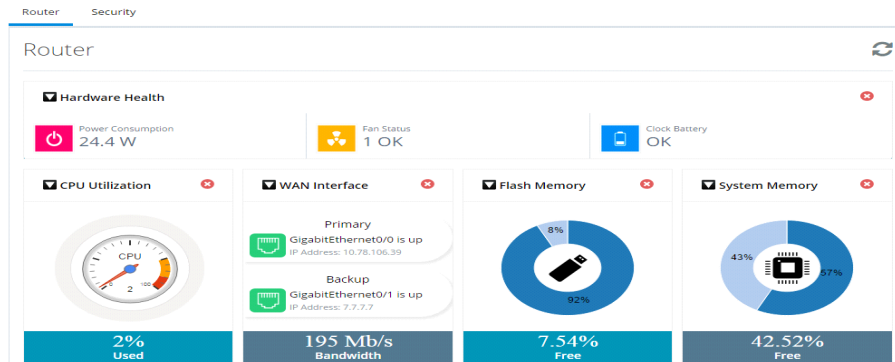
The Dashboard view shows the vital hardware health status of the router along with the flash and system memory, CPU utilization, and WAN Interface status and security aspects of network. The Dashboard has two sections Router and Security.

## Viewing Router Dashboard

To view the router diagnostics using the dashboard view, perform these steps:

1. Click on **Dashboard> Router** to open the Router Diagnostics dashboard view.

## The Dashboard page



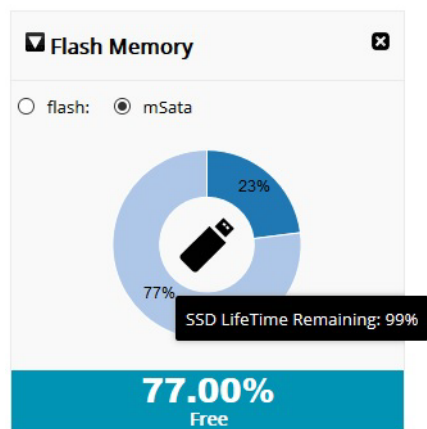
Hardware Health section shows the total Power Consumption of the router, Number of Fans on the system and their status, CPU Temperature and Battery health. If the router does not expose its hardware information, then this section will not be visible in the UI.

If Primary and Backup WAN Interfaces are configured, then the status of the same is displayed along with the interface Name. The status is shown in green only when both admin and operational status are up. This also shows the amount of traffic flowing through WAN Interfaces.

**Note:** The following sections have been moved to the System Information Popup: Hostname, Device Type, IOS Version, System Uptime from last reload, current System Time, and the Reason for Last Reload of the router. The Interfaces chart is moved under the Interfaces tab.

Beginning with CCP Express Release 3.5.2, for IR829M series devices, the Flash Memory dashlet will display two radio buttons: “flash” and “mSata.” The flash option retains the current dashlet data which is the pie chart that shows used and free space on the flash memory. If you select the mSata option, the used and free data of the SSD is displayed. You can hover on the flash icon and get the remaining lifetime for the SSD also.

**Figure 53 Flash Memory Dashlet**



- To update the charts, click on the refresh button given at the top of the charts section.

## CPU Utilization Dashlet

To access the new CPU Utilization dashlet:

1. Go to the Router Dashboard.
2. Under the CPU dashlet, click Details.

A new dashlet is shown in a popup dialog. The details of CPU usage are in percents for different intervals available in the new dashlet.

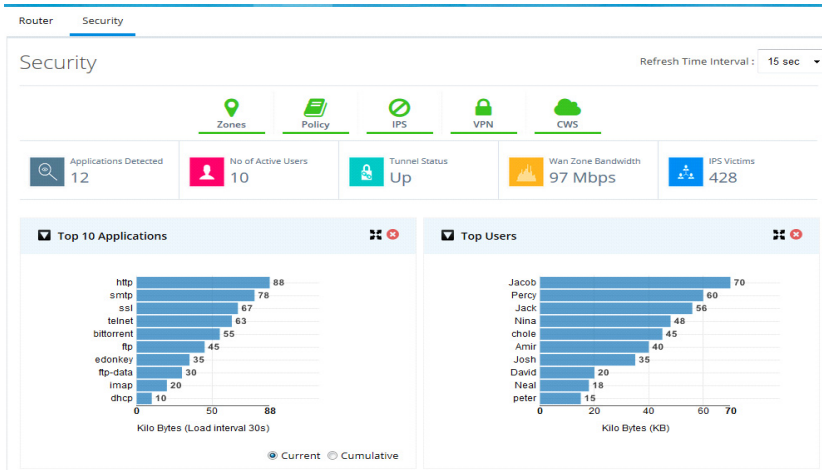


## Security Dashboard

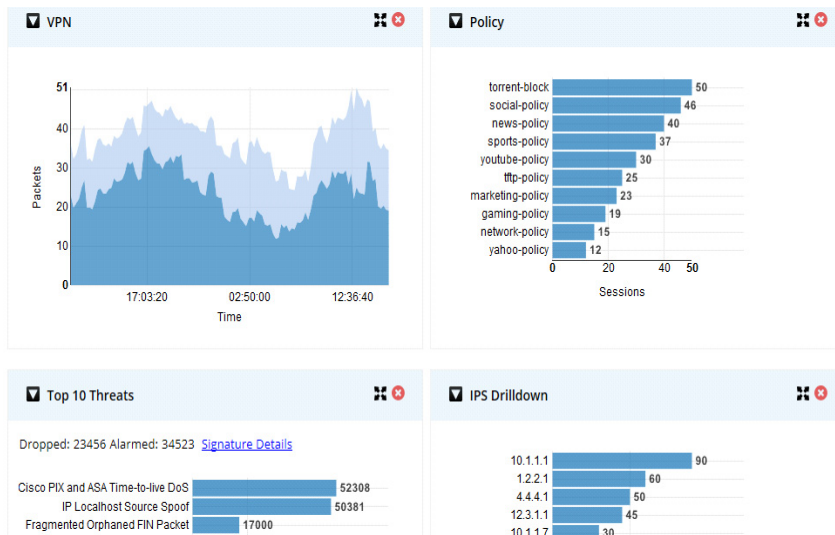
To view the security dashboard view, perform these steps:

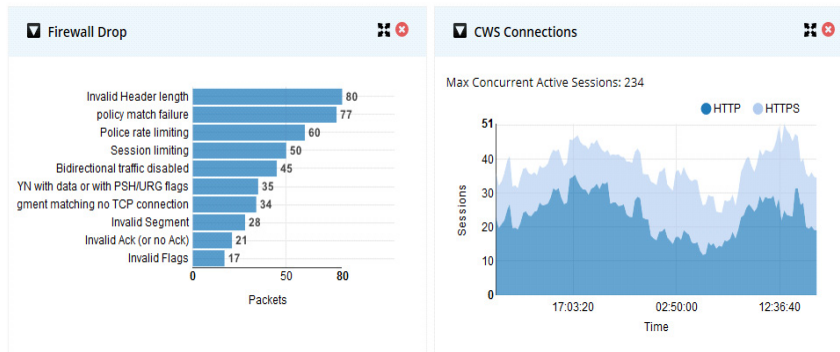
1. Click on **Dashboard** > **Security** to open the Security dashboard view.

**Figure 54 Security Dashboard (Dashlets displayed are Top 10 Applications and Top Users)**



**Figure 55 Security Dashboard (Dashlets displayed are VPN, Policy, Top 10 Threats and IPS Drilldown)**



**Figure 56 Security Dashboard (Dashlets displayed are Firewall Drop and CWS Connections)**

The top portion shows the security features enabled on the device. The green icon indicates they are enabled. User can click on a specific icon and navigate to that feature. If any security feature is not enabled, then the relevant charts are not visible. They will be minimized and shown in the tray above the pane which is showing the security features enablement status. To close any chart click on the close button of the chart and the chart will be minimized into the tray. The icons can be clicked to enable it again.

## Security Snapshot

- Applications Detected—Total number of Application protocols discovered by NBAR. While moving the mouse over, the list of applications will be displayed.
- Number of Active Users—Top users contributing to the traffic currently traversing the device.
- Tunnel Details—Hover over this option to list the VPN tunnels present along with the status (up or down).
- WAN Zone Bandwidth—Traffic going through the WAN Interfaces.
- IPS Victims—Total number of users impacted by some attack. The information is obtained by enabling the IPS feature.

## Security Charts

Following is the list of various charts supported to show the security information and bandwidth consumption statistics of the network. These charts will update periodically. The refresh interval can be modified.

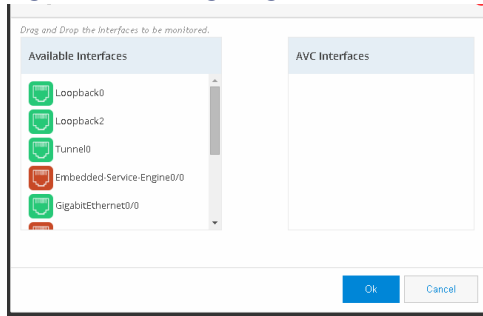
- Top Applications—This dashboard will list the top 10 application protocols contributing to the traffic through the router in terms of bandwidth consumption at any point of time. This chart will also provide the cumulative bandwidth consumption of the device from the time of router reload. CCP Express will get the update from device at configured regular intervals.
- Top Users—This dashboard will list the top users in the router in terms of bandwidth consumption at any point of time. It supports both current bandwidth consumption.
- VPN—VPN chart shows encrypted and decrypted traffic through the configured VPN tunnel.
- Policy—Policy chart shows the amount of data that matched a specific Firewall Policy configured on the device. This gives the snapshot view of which policy is hit the most in the network.
- Top Threats—This dashboard shows the Top 10 threats in the network in terms of malicious packets.
- IPS Drilldown—This dashboard shows the total attacks made by the attackers and attacks received by the victims.
- Firewall drop—This dashboard shows the Top 10 firewall drops and the cause of the drops.

## Application Visibility and Control (AVC) Dashboard

To view the AVC dashboard, perform these steps:

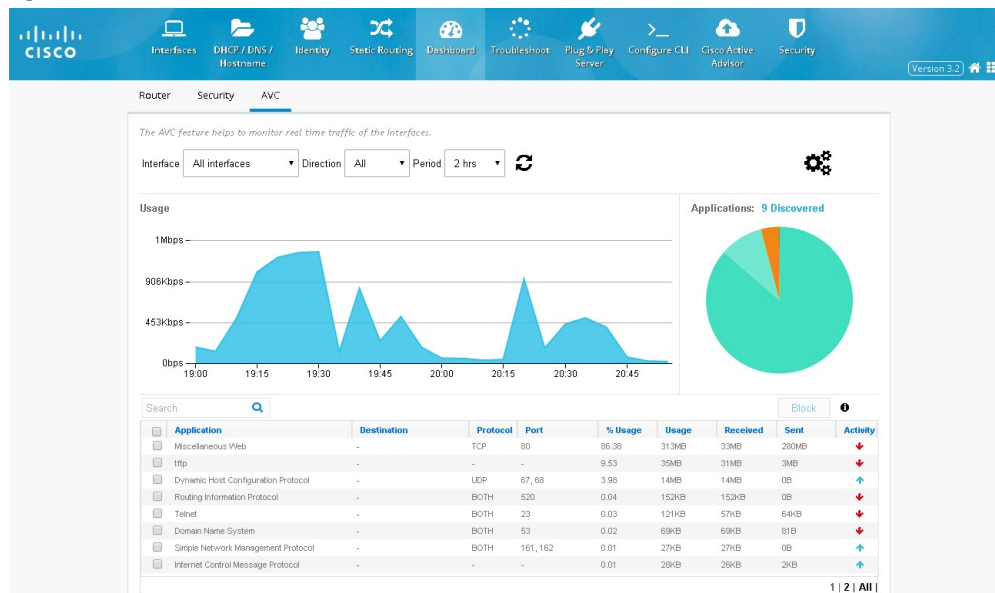
1. Click **Dashboard > AVC** to open the AVC dashboard view.
2. Enable AVC, a screen appears where you can drag and drop the interfaces to AVC interfaces.

**Figure 57 Configuring AVC**



3. Click OK. **Figure 58** displays. This page displays all the applications and the relevant data. At a time 8 applications are listed in the page. You can filter applications using the search option.

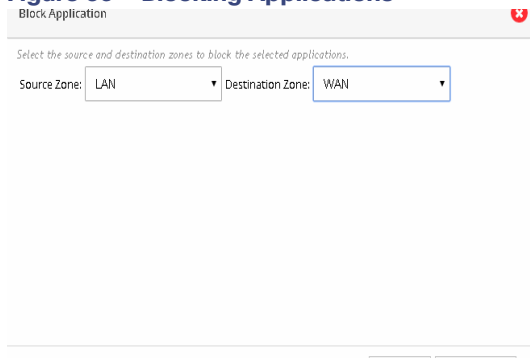
**Figure 58 AVC Dashboard**



4. You can also click Settings icon to add or remove interfaces for AVC.
5. If security is enabled, you can block the applications in AVC screen. Select the applications and click BLOCK. Select the Source and Destination Zone and click OK. (**Figure 59**). Selected application will be blocked. When an application is blocked, a policy is automatically created by the name `avc-app-block-1`. The subsequent blocking of applications will add policies with the same name format with only the numbering incremented.



**Figure 59 Blocking Applications**



## Interfaces Dashboard

To view the Interfaces dashboard, perform these steps:

1. Click **Dashboard > Interfaces** to open the Interfaces dashboard view.

Interfaces chart groups the Interfaces by type and shows the number of interfaces that are up and down. If the user moves the cursor over the chart, then the specific interfaces will be displayed as tool tip.

**Figure 60 Interfaces Dashboard**



## Troubleshooting

This section explains how to perform troubleshooting for your router.

This section discusses:

- “Ping and Traceroute” section on page 42
- “Test WAN Connection” section on page 42

## Ping and Traceroute

The Ping and Traceroute utility allows you to do a basic troubleshooting of the network and device connectivity.

To troubleshoot the device connectivity, perform these steps:

1. Click **Troubleshoot** to open the Ping and Traceroute tab.

**Figure 61 Ping and Traceroute**

Ping and Traceroute

\*Note: Destination will accept proper IPV4 address/IPV6 address/Hostname.

Source:

Destination:

|

2. (Optional) Specify the source IP address (IPv4 or IPv6 address) or interface.
3. Specify the destination IP address (IPv4 or IPv6 address) or hostname.
4. Click **Ping** to verify whether the destination IP address is reachable.
5. Click **Traceroute** to view the list of routes traversed between the source and destination IP addresses.
6. You can also copy-to-clipboard or download the retrieved data by clicking on COPY or DOWNLOAD icons to the right of the details box.

## Test WAN Connection

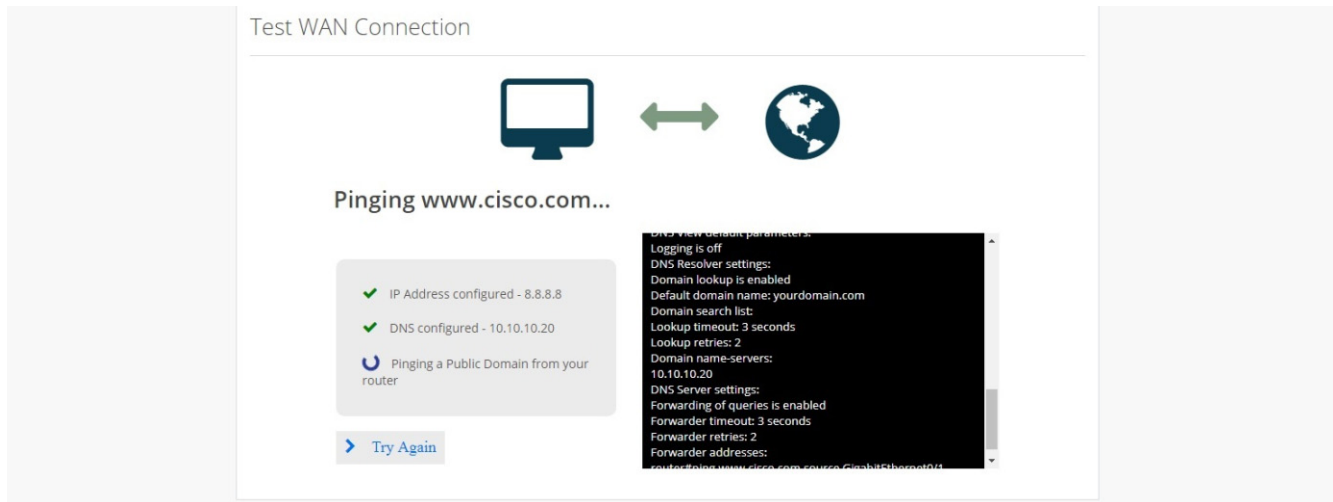
If you do not have a primary interface configured, the following message appears:



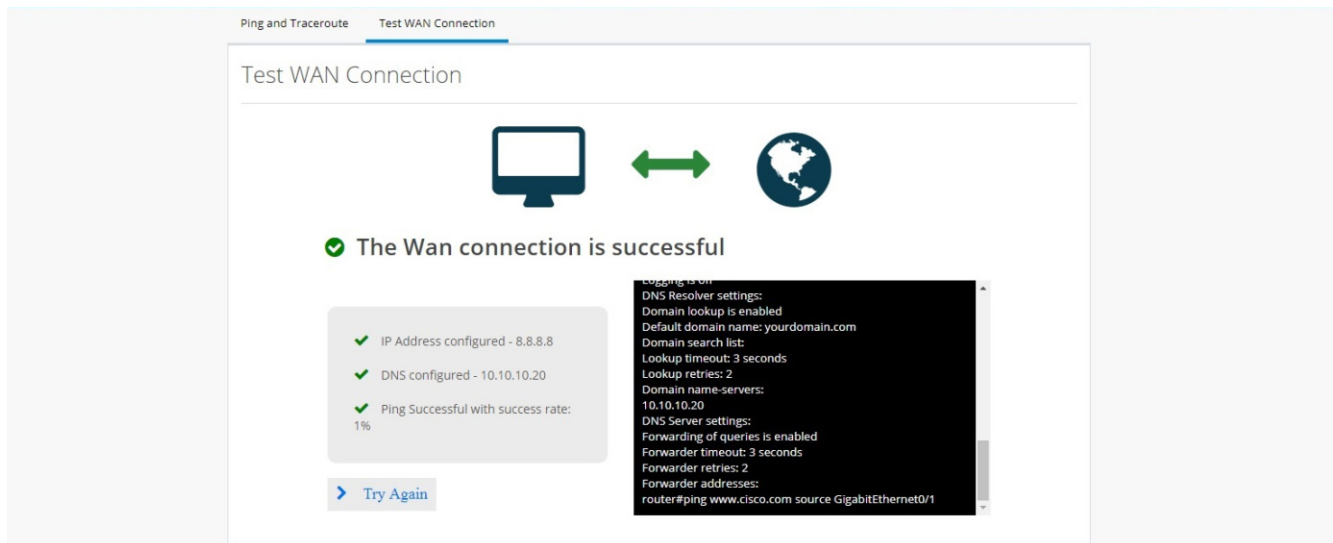
If a primary interface is configured without an IP address, the following information appears:



If a primary interface is configured with an IP Address and DNS details, the following information appears:



For a successful connection, the following information appears:



## Access Control Lists (ACLs)

Filter traffic and control access to the IP network using the ACL option from the main menu.

**Figure 62 ACL Summary**

ACL Add Delete

*ACL is the integrated feature that is used to filter the network traffic passing through the IOS devices.* [Expand All](#) [Collapse All](#)

Sequence	Access	Protocol	Source IP	Source Mask	Destination IP	Destination Mask	Source Port	Destination Port	Action
ACLName/Number : 23			Type : Standard		Mappings : 3		<a href="#">Map ACL</a>	<a href="#">Add ACE</a>	
10	permit	N/A	any	N/A	N/A	N/A	N/A	N/A	
ACLName/Number : 56			Type : Standard		Mappings : 1		<a href="#">Map ACL</a>	<a href="#">Add ACE</a>	
10	permit	N/A	any	N/A	N/A	N/A	N/A	N/A	
ACLName/Number : har123			Type : Standard		Mappings : 1		<a href="#">Map ACL</a>	<a href="#">Add ACE</a>	
10	permit	N/A	any	N/A	N/A	N/A	N/A	N/A	
20	deny	N/A	0.0.0.0	255.255.255.1	N/A	N/A	N/A	N/A	
ACLName/Number : ranjith			Type : Standard		Mappings : 3		<a href="#">Map ACL</a>	<a href="#">Add ACE</a>	
10	permit	N/A	any	N/A	N/A	N/A	N/A	N/A	
ACLName/Number : test123			Type : Standard		Mappings : 0		<a href="#">Map ACL</a>	<a href="#">Add ACE</a>	
10	permit	N/A	any	N/A	N/A	N/A	N/A	N/A	
ACLName/Number : test12345			Type : Standard		Mappings : 1		<a href="#">Map ACL</a>	<a href="#">Add ACE</a>	

This page includes the Map ACL and Add ACE buttons for each ACL. Hover over the icons on the right to remove an ACL, expand and collapse an ACL.

### Add an ACL

To add an ACL:

1. From the Summary screen, click **Add**.

**Figure 63 Add ACL**

The screenshot shows the 'Add ACL' configuration window. It is divided into several sections:

- ACL Identifier:** Includes radio buttons for IPv4 (selected) and IPv6, a 'Type' dropdown menu set to 'Extended', a 'Name/Number' field with a red asterisk, and a 'Remark' field with the text 'Maximum 100 characters allowed'.
- Configure ACE:** Contains dropdown menus for 'ACL Rule' (set to 'Permit'), 'Source IP' (set to 'Any'), 'Destination IP' (set to 'Any'), and 'Protocol' (set to 'IP').
- Enable Mapping:** A checkbox labeled 'Enable Mapping' is checked.
- HTTP Mapping:** A checkbox labeled 'HTTP Enable' is unchecked.
- Line VTU Mappings:** Includes a 'Route' dropdown menu, a 'Line VTU' field with a placeholder 'Single value or range(0-15)', and an 'Add' button.
- Interface Mappings:** Includes a 'Route' dropdown menu, an 'Interface Name' dropdown menu, and an 'Add' button.
- Buttons:** 'OK' and 'Cancel' buttons are located at the bottom right of the window.

2. Select the standard option from the Type menu and provide an ACL Name/Number (0-99 for standard).
3. Select the ACL Rule to permit or deny.
4. Select the IP address option with either 'any' or 'valid IP address and wildcard Mask'.

You can also add mappings while adding the ACL through this window.

## Add an Extended ACL

1. From the Summary screen, click **Add**.
2. Select the extended option from the Type menu and provide an ACL Name/Number (0-100 for extended).

**Figure 64 Add an Extended ACL**

**Add ACL**

**ACL Identifier**

IPv4  IPv6 Type **Extended** Name/Number \*  Remark

**Configure ACE**

ACL Rule **Permit**

Source IP **IP Address**

Destination IP **IP Address**

Protocol **TCP**

Source Port **Greater Than**

Destination Port **Less Than**

Enable Mapping

**HTTP Mapping**

3. Select a protocol. For TCP/UDP, select the source port and destination port from the lists.

## Map an ACL

To map an ACL:

1. Select the ACL, and click Map ACL. Existing mapping values are listed under one ACL.

**Figure 65 Map ACL**

Mapping for ACL: 23

**Line VTY Mappings**

Route: Select | Line VTY: Single value or range(0-15)

VTY Mapping		
0	in	✖
1-2	in	✖
3-4	in	✖

**Interface Mappings**

Route: Select | Interface Name: Select

Interface Mapping

**HTTP Mapping**

HTTP Enable:

Apply

2. Select Interface and add its route.

or

Select the VTY route, and add the VTY value.

**Note:** HTTP option will be enabled only for Standard numbered ACL.

## Add an Access Control Entry (ACE)

To add an ACE, click the ACE.

**Figure 66 ACE**

Add ACE

**Type**

IPv4 | IPv6 | Type: Extended | ACL Name/Number: INTRANET-WHITELIST

ACL Remark: No Remark

ACL Rule: Permit

Source IP: Any

Destination IP: Any

Protocol: IP

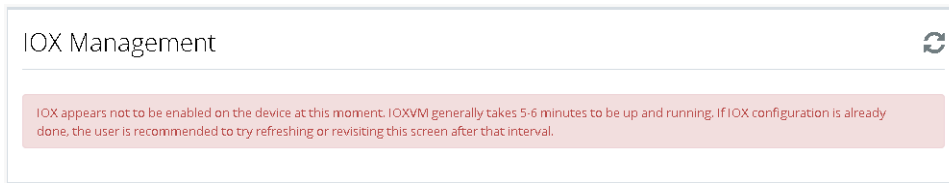
Ok | Cancel

## IOx

Use this option to access IOx services through the local management interface.

If IOx is not configured on the router, the following message displays:



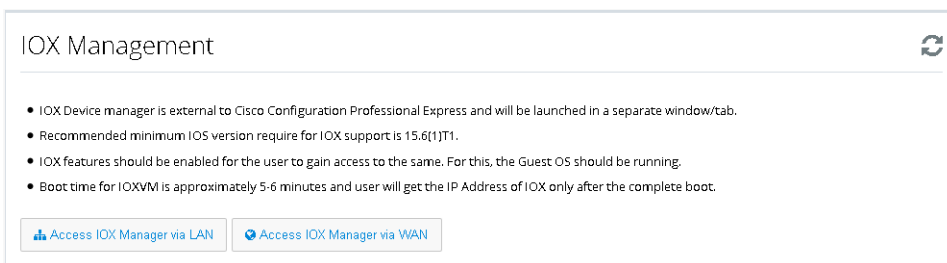


After you configure IOx on the router, select IOx from the Home menu.

Depending on your configuration, you can access IOx Manager through LAN or WAN.

Click either option to launch the Local Manager.

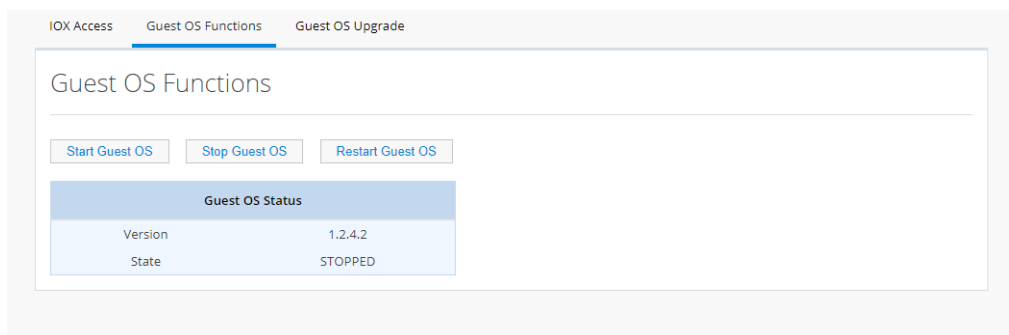
**Figure 67 IOx Management**

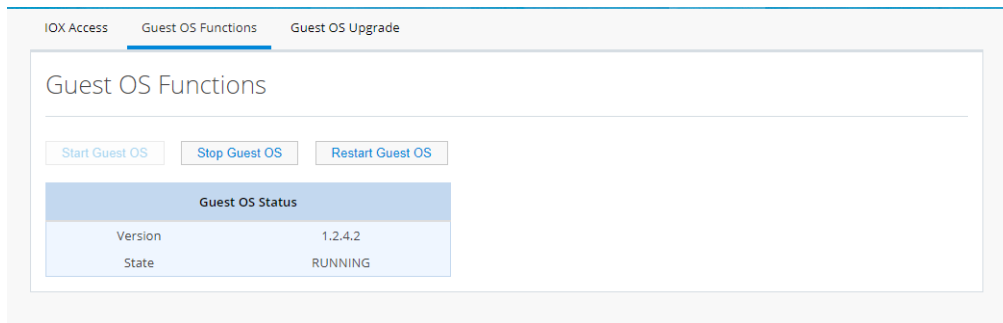


## Guest OS Functions

Use this window to start, stop, or restart Guest OS

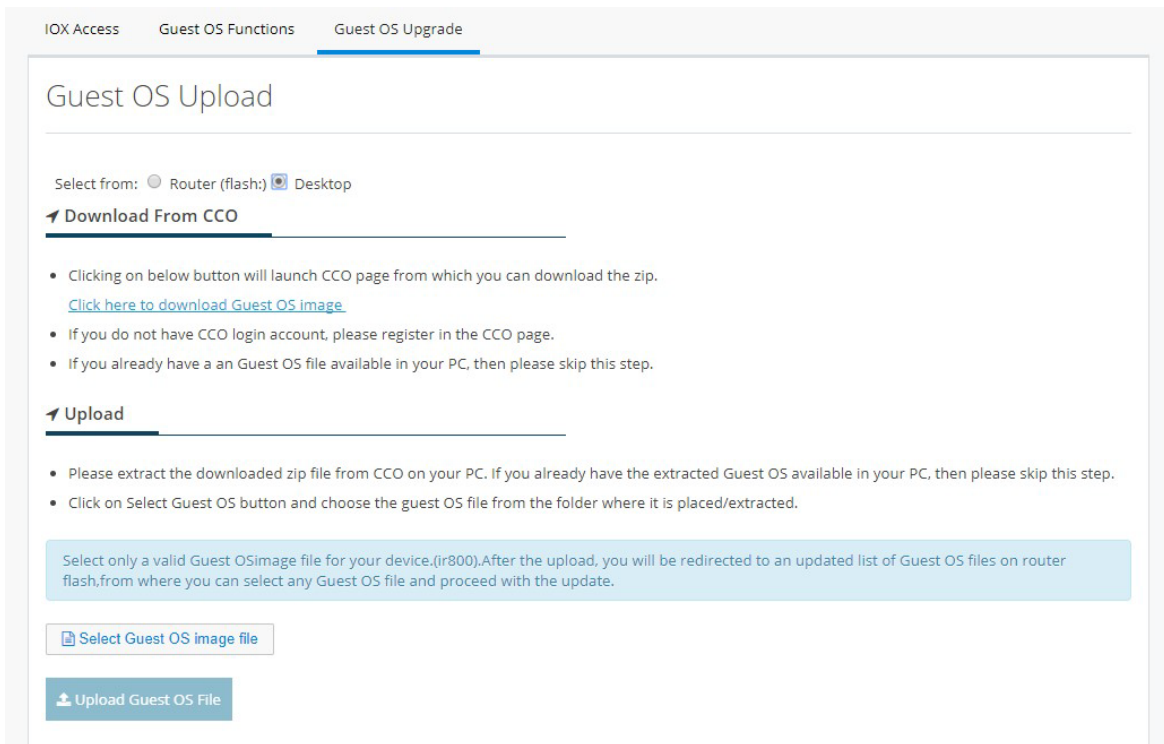
**Figure 68 Guest OS Stopped**



**Figure 69 Guest OS Start**

## Guest OS Upgrade

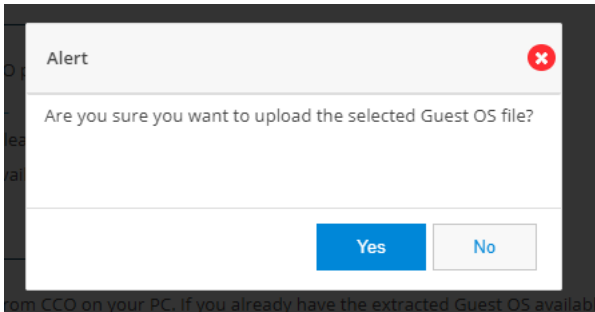
1. Click IOX from the main menu.
2. Select the Guest OS Upgrade tab to view the existing Guest OS images on the device.
3. To upload a Guest OS image, click the Desktop option.

**Figure 70 Guest OS Upgrade**

4. Click on the link to download the latest Guest OS version. You are taken to the Cisco.com download page.
5. Download the recommended latest version for the device.

If you do not have a Cisco.com login, ensure you register.

After you upload the file, the following message displays:



6. Click Select Guest OS image file, and choose the Guest OS file from the folder in which you downloaded it.
7. Click on Upload Guest OS File.

#### Download From CCO

- Clicking on below button will launch CCO page from which you can download the zip.  
[Click here to download Guest OS image.](#)
- If you do not have CCO login account, please register in the CCO page.
- If you already have a an Guest OS file available in your PC, then please skip this step.

#### Upload

- Please extract the downloaded zip file from CCO on your PC. If you already have the extracted Guest OS available in your PC, then please skip this step.
- Click on Select Guest OS button and choose the guest OS file from the folder where it is placed/extracted.

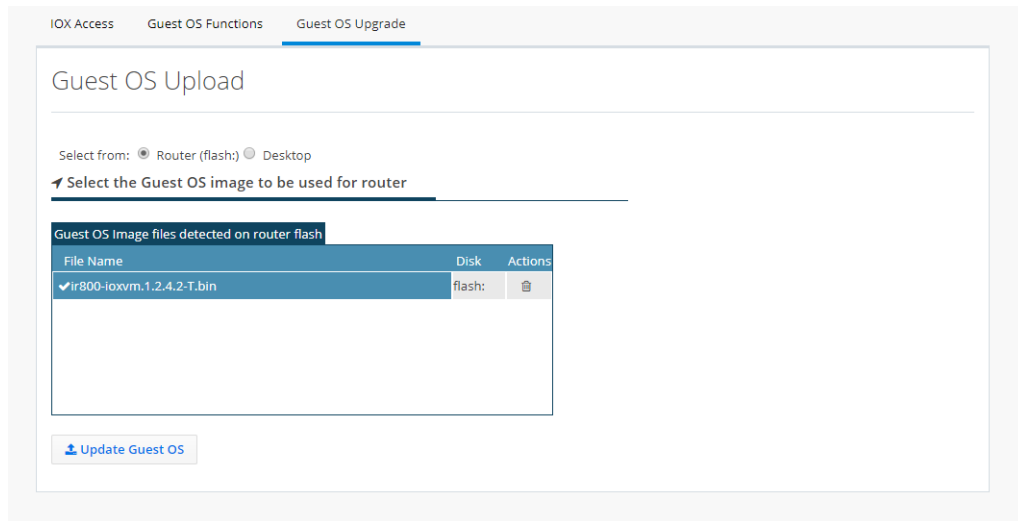
Select only a valid Guest OSimage file for your device.(ir800).After the upload, you will be redirected to an updated list of Guest OS files on router flash,from where you can select any Guest OS file and proceed with the update.

[Select Guest OS image file](#)

8. Proceed with the upload of the file to the box by clicking Yes. If the upload fails, click TRY AGAIN.

Once the upload is completed, the application automatically comes back to the Guest OS Update main page which lists all the available IOS images on the router.

9. Choose the Guest OS image you would like to add to the boot list.
10. Click Update Guest OS to install the new version

**Figure 71 Guest OS Upload Completed**

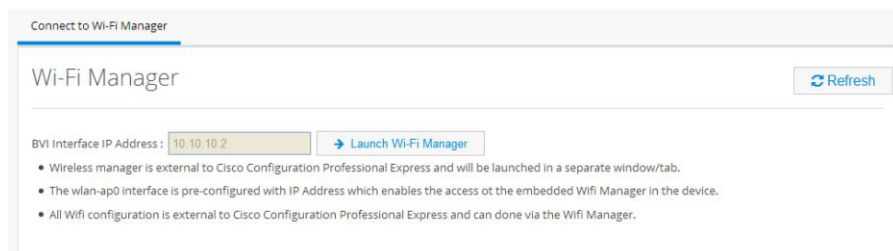
For more information about IOx, refer to the IOx documentation at the following URL:

<http://www.cisco.com/c/en/us/support/cloud-systems-management/iox/tsd-products-support-series-home.html>

## Wireless

Wireless configuration is done through the Wi-Fi Manager which is external to CCP Express.

When you click Wi-Fi, you receive the following message with a link to Wi-Fi Manager:



1. Click **Launch Wi-Fi Manager**.
2. Select Network Configuration under the Easy Setup menu.

**Figure 72 Wi-Fi Manager (External to CCP Express)**

The screenshot shows the Cisco Configuration Professional Express (CCP Express) interface for configuring a Wi-Fi access point. The interface is divided into two main sections: Network Configuration and Radio Configuration.

**Network Configuration:**

- Host Name:
- Server Protocol:  DHCP  Static IP
- IP Address:
- IP Subnet Mask:
- Default Gateway:
- IPv6 Protocol:  DHCP  Autoconfig  Static IP
- IPv6 Address:  (X:X:X:X::X/<0-128>)
- Create a user:**
  - Username:
  - Password:
- Change global authentication password:**
  - default enable secret:
  - confirm enable secret:
- SNMP Community:
- Read-Only  Read-Write

**Radio Configuration:**

The Radio Configuration section is split into two panels: Radio 2.4GHz and Radio 5GHz.

**Radio 2.4GHz:**

- SSID:
- Broadcast SSID in Beacon
- VLAN:  No VLAN  Enable VLAN ID:  (1-4094)  Native VLAN
- Universal Admin Mode:
- Security:
- Role in Radio Network:
- Optimize Radio Network:
- Aironet Extensions:
- Channel:
- Power:

**Radio 5GHz:**

- SSID:
- Broadcast SSID in Beacon
- VLAN:  No VLAN  Enable VLAN ID:  (1-4094)  Native VLAN
- Universal Admin Mode:
- Security:
- Role in Radio Network:
- Optimize Radio Network:
- Aironet Extensions:
- Channel:
- Power:

For more information about configuring access points, refer to the Cisco IOS Configuration Guide for Autonomous Aironet Access Points documentation at:

[http://www.cisco.com/c/en/us/td/docs/wireless/access\\_point/15\\_2\\_4\\_JB/configuration/guide/scg15-2-4-Book.html](http://www.cisco.com/c/en/us/td/docs/wireless/access_point/15_2_4_JB/configuration/guide/scg15-2-4-Book.html)

3. Specify an SSID that will be used to uniquely identify your wireless device. The SSID can contain up to 32 alphanumeric characters.
4. To broadcast the SSID in the access point beacon, check the **Broadcast SSID in Beacon** check box. When you broadcast the SSID, devices that do not specify an SSID can associate with the access point. This is a useful option for an SSID used by guests or by client devices in a public space. If you do not broadcast the SSID, client devices cannot associate to the access point unless their SSID matches this SSID. Only one SSID can be included in the access point beacon.
5. Select the **Enable VLAN ID** and specify the ID of the VLAN. This will enable the clients that connect to the SSID to use the IP addresses from the DHCP pool associated with this VLAN.
6. Select the security setting for the SSID.
  - **Static WEP Key:** choose the WEP key index and key size, and enter the static WEP encryption key. The key index can be between 1 and 4. The key size can be either 40 bits or 128 bits.
  - **WPA2:** specify the WPA2 encryption key and select the key type. The Key type can be either ASCII or Hexadecimal.
7. Click **Apply**. The SSID appears in the SSID table on the bottom of the page.

## Security Features

This section includes the following:

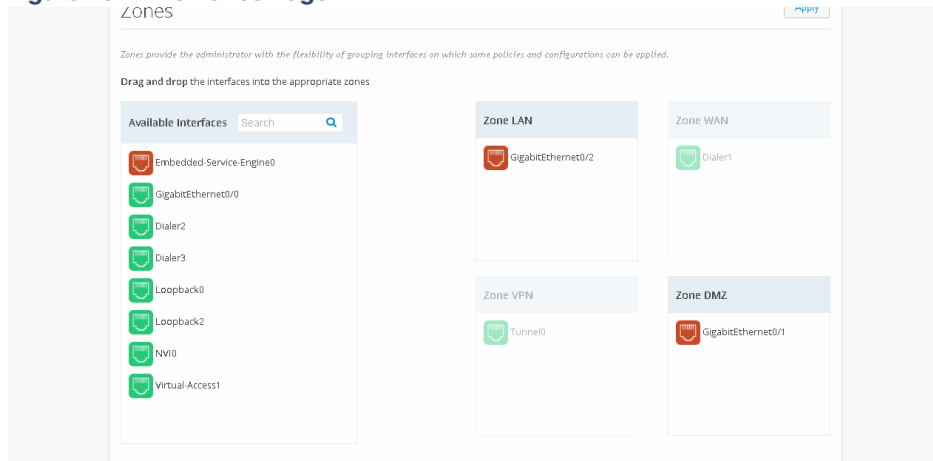
- [Zones, page 54](#)
- [Policy, page 54](#)
- [IPS, page 58](#)
- [VPN, page 63](#)
- [Content Security, page 82](#)
- [Static NAT, page 83](#)

## Zones

Zones establish the security borders of your network. A zone defines a boundary where traffic is subjected to policy restrictions as it crosses to another region of your network. ZFW's default policy between zones is deny all. If no policy is explicitly configured, all traffic moving between zones is blocked.

- Click **Security > Zones**. The left side list shows the list of available interfaces which can be moved to appropriate security zones. The supported zones are WAN, LAN, VPN, and DMZ.
- If any interface needs to be moved to any security zone, it can be just dragged and dropped into the zone. WAN and VPN zones are grayed out here and moving the WAN interface under WAN zone can be done in interface screen. Also when VPN is configured, the respective Tunnel interface will be moved to VPN zone internally.

**Figure 73 The Zones Page**



## Policy

With the Zones and Policy pages configured, users can enable Zone based Firewall on the device. Policy page applies user-defined rules or policy on the traffic that flows between source and destination zones. The source and destination zones are tied together to make a zone pair under which the policy is applied. Prior to creating and applying policy, user needs to configure and assign the interfaces under the right zones.

Policy feature provides more granularity in identifying and filtering the traffic. Within the traffic between source zone and destination zone, the user can filter the traffic further based on the source and destination network, application type, the source and destination ports, domains, and the user groups.

## Policy Summary

To view the policy summary, perform these steps:

1. Click **Security >Policy** to display the summary screen of Policy. The summary screen lists all existing policies and option to add, edit and delete an existing policy
  - The Policy display in the summary screen is based on the zone pairs. For e.g in the picture below there are two groups of policies and the groups based on zone pairs viz. LAN-WAN and LAN-VPN
  - The order of policies can be changed by just dragging and dropping the policies within the zone pair section table. The changes can be reverted by clicking the arrow icon placed on top of the zone pair section

**Figure 74 The Policy Page**

Policy Name	Description	Zone	Source Network	Destination Network	Source Ports	Destination Ports	Applications	Excludes	Policy Action	Action
LAN-WAN Policies										
ip_outside		Any	Any	Any	Any	Any	outside	Any	Block	CF
allow_facebook		Any	Any	Any	Any	Any	facebook	Any	Allow	CF
web		Any	Any	Any	Any	Any	http, https	Any	Allow	CF
LAN-VPN Policies										
ip_vpn		Any	Any	Any	Any	Any	ip, udp, ...	Any	Allow	CF

### Prerequisite for Creating Any Policy

- Prerequisite for creating a policy is assigning the specific interfaces to Zones.
- Provide Zone link here

Some sample use case scenarios are explained below

### Block a Specific Application

To block a specific application, perform these steps:

1. Click **Security > Policy**, and click **Add**. The Policy Dialog appears.
2. From the Policy Dialog, provide Policy Name, description, and the source and destination zones whose traffic needs to be processed. Also, the action needs to be taken on the selected traffic whether we need to block it or allow it.
3. Click **Network**. Add source and destination network if any specific network within the zone-pair is to be handled. Add the source network by specifying the network in the text field and add plus button. The same procedure needs to be followed for any destination network as well. By default, source and destination network would be 'any'.(Figure 75)

**Figure 75 The Security Policy Wizard (Landing screen with Network tab contents)**

The screenshot shows the Security Policy Wizard interface. At the top, there are fields for Policy Name, Policy Description, and Action (set to Allow). Below these are Source Zone (LAN) and Destination Zone (WAN) dropdown menus. The main area is divided into two panes: Source Networks and Destination Networks, both containing an 'Any' entry. At the bottom, there are input fields for Source Network Address and Destination Network Address, with a plus sign icon next to each. A small text at the bottom left provides an example: 'eg : 192.168.0.0, IP/Subnet : 192.168.0.0/8 or range : 192.168.0.0 - 192.200.0.0'.

4. Click **Application** to select the application to be inspected or blocked. The Available Applications shows the list of applications grouped as per the known category. The needed application or group can be dragged and dropped in the Selected Applications list.

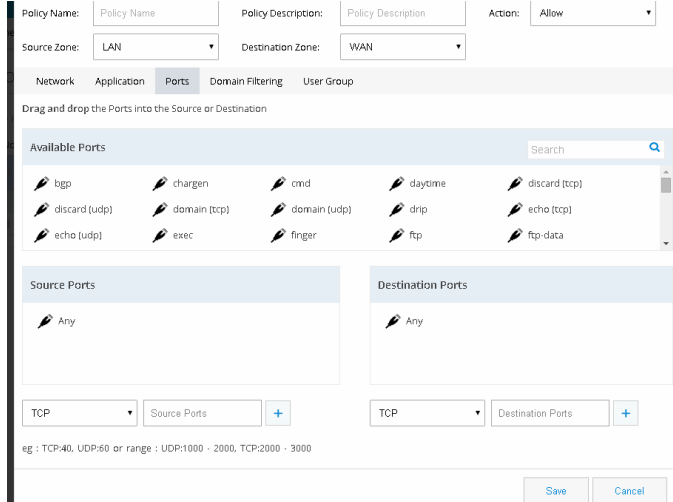
**Figure 76 The Security Policy Wizard (Application tab contents)**

The screenshot shows the Security Policy Wizard with the Application tab selected. The top section is identical to Figure 75. Below the tabs, there is a heading 'Drag and drop the Available Applications into the Selected Applications'. The interface is split into two panes: 'Available Applications' on the left and 'Selected Applications' on the right. The Available Applications pane contains a search bar and a list of application categories, each with a plus sign icon: other, net-admin, business-and-productivity-tools, email, file-sharing, browsing, voice-and-video, instant-messaging, newsgroup, internet-security, database, and inter-process-ipc. The Selected Applications pane is currently empty. At the bottom right, there are 'Save' and 'Cancel' buttons.

5. Click **Ports** if it is required to classify the application based on source and destination ports. By default, traffic originating from any ports of the selected networks will be processed. User can add a required source and destination ports. List of popular applications is given based on their Category and by dragging and dropping the needed one will handle the port specific to that.

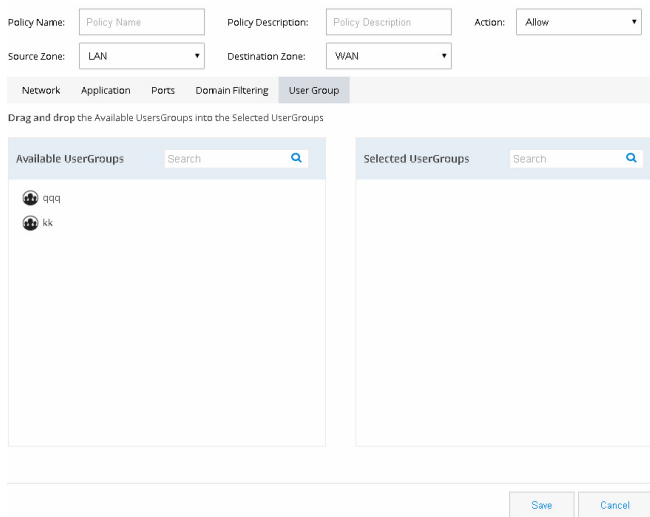


**Figure 77 The Security Policy Wizard (Ports tab contents)**



6. Click **User Groups** if the traffic filtering is to be handled based on the user or group originating the traffic.

**Figure 78 The Security Policy Wizard (User group tab contents)**



### Block a Specific Domain

To block a specific domain, perform these steps:

1. Click **Security > Policy**, and click **Add**.
2. Policy Dialog will appear. Provide Policy Name, description, and the source and destination zones whose traffic needs to be processed. Also the action needs to be taken on the selected traffic whether we need to block it or allow it.
3. Click **Network**. Add source and destination network if any specific network within the zone-pair is to be handled. Add the source network by specifying the network in the text field and add plus button. The same procedure needs to be followed for any destination network as well. By default all the networks in the Zone pair is processed.

**Figure 79 The Security Policy Wizard (Landing screen with Network tab contents)**

4. Click **Domain Filtering** and the screen shows list of popular sites. User can drag and drop if any of the popular websites need to be blocked. If any unlisted domain needs to be added that URL (wild card pattern accepted) can be given in the text box.

**Figure 80 The Security Policy Wizard (Domain Filtering tab contents)**

5. Click **User Groups** if the traffic filtering is to be handled based on the user or group originating the traffic.

**Note:** To select the specific User group it should have been already added through the Identity feature.

## IPS

Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet inspection feature that effectively mitigates a wide range of network attacks. A component of the Cisco IOS Integrated Threat Control framework and complemented by Cisco IOS Flexible Packet Matching feature, Cisco IOS IPS provides your network with the intelligence to accurately identify, classify, and stop or block malicious traffic in real time.

## Prerequisites for Using IPS

- Ensure the IPS Signature Packages are present on the router under flash:
- Enable Security License on the router.
- Complete WAN interface configuration.

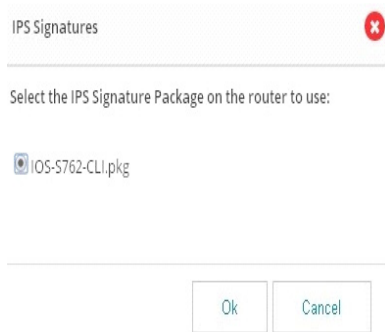
If these conditions are not met, respective error messages are displayed when the IPS feature is accessed.

## Enabling IPS

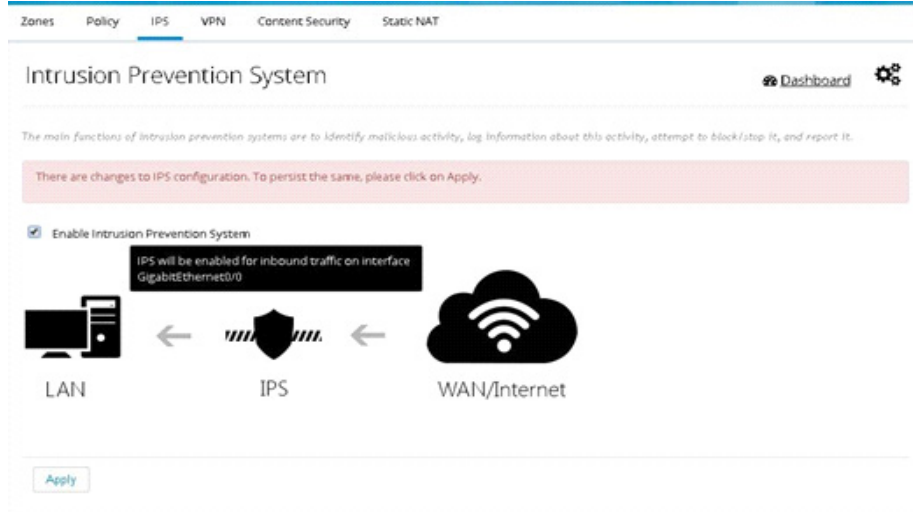
If all the prerequisites are met, you receive the option to enable IPS.

1. Click **Security > IPS**, and choose the **Enable IPS** check box.
2. When you enable IPS for the first time, a popup window lists all of the IPS Signature Packages available on the box. The first one is selected by default. Even if there is only a single package, you get this dialog box.

**Figure 81** IPS Signatures



3. Select appropriate one and click **OK**.
4. You get the message that there are changes to IPS configuration. Upon applying the changes, IPS is enabled on inbound traffic (depicted in the image below the check box). The selected signature package is compiled and applied too. To view the interface(s) on which this will be applied, hover on the image to view the tool tip containing that information.

**Figure 82** Intrusion Prevention System Page

5. Click on the **Apply** button to persist changes. You have to wait for a minute (depending on the signatures selected) as the signature compilation is occurring in the background.
6. After the settings are applied and the signature compilation is completed, the IPS screen with the information on the package version and count of failed signatures (if any) is displayed.

**Note:** For all further disable/enable cycles, you are not prompted to select the package. In those cycles, after enabling, you get a message that “Signature compilation is in progress”. You can choose to visit other pages and come back later or to hit “Refresh” after a while to see the IPS settings screen.

## Disabling IPS

To disable IPS at any point, uncheck the **Enable IPS** check box and click **Apply**.

## Uploading IPS Signature Packages

You have the option to upload signature packages onto the router at any point in time. To upload IPS signature packages, perform these steps:

1. Hover your cursor over the **Configure** icon that is available on the right pane. The settings menu appears.
2. Click on the **Upload IPS Signature Packages** option. A dialog box appears.
3. Click on the **Folder** button and select the file from the file selection dialog box and click **OK**.

CCP Express validates for the file name, duplication and free space on the router. If any of these validations fail, appropriate error message are displayed. If the file validations are completed, you receive the message that file is ready for upload and the “Upload” button is enabled.

4. Click on the **Upload** button to initiate the upload.

Upload takes a while as the file size is around 20MB. You are notified when the upload is completed. You can upload more files or quick the dialog.

## Changing IPS Signature Packages

When IPS is enabled, if the box has more than one Signature Package file, you are provided with an option to change the signature package. To change IPS signature packages:

1. Hover your cursor over the Configure icon that is available on the right pane. The settings menu appears.
2. Click on the Change IPS Signature Packages option.

A dialog box with the list of available packages on the box is displayed. The currently selected one is listed, but selection is disabled for this one. The packages are sorted in reverse alphabetical order to have the latest one at the top for easy selection.

3. Select the package of your choice and click **OK**. Signature compilation may take several seconds.
4. After the settings are applied and signature compilation is completed, the IPS screen with the information on the newly selected package version and count of failed signatures (if any) is displayed.

## Download Link for IPS Signature Packages

You can download the relevant signature package files from the link that is shared with you. This is a link that connects you to an internal CISCO page. To download IPS signature package:

1. Hover your cursor over the Configure icon that is available on the right pane. The settings menu appears.
2. Click on the Download IPS Signature Packages option. Upon clicking on the link, you are taken to the CISCO IPS Services page (external to CCP Express), from where the you can download signature packages that are needed.

## Enabling/Disabling Notifications/Log

You are provided with links to enable and disable SDEE and syslog notifications. The menu is smart to toggle between the enable and disable options for each based on the setting in the system.

### SDEE Notifications

To enable SDEE notifications:

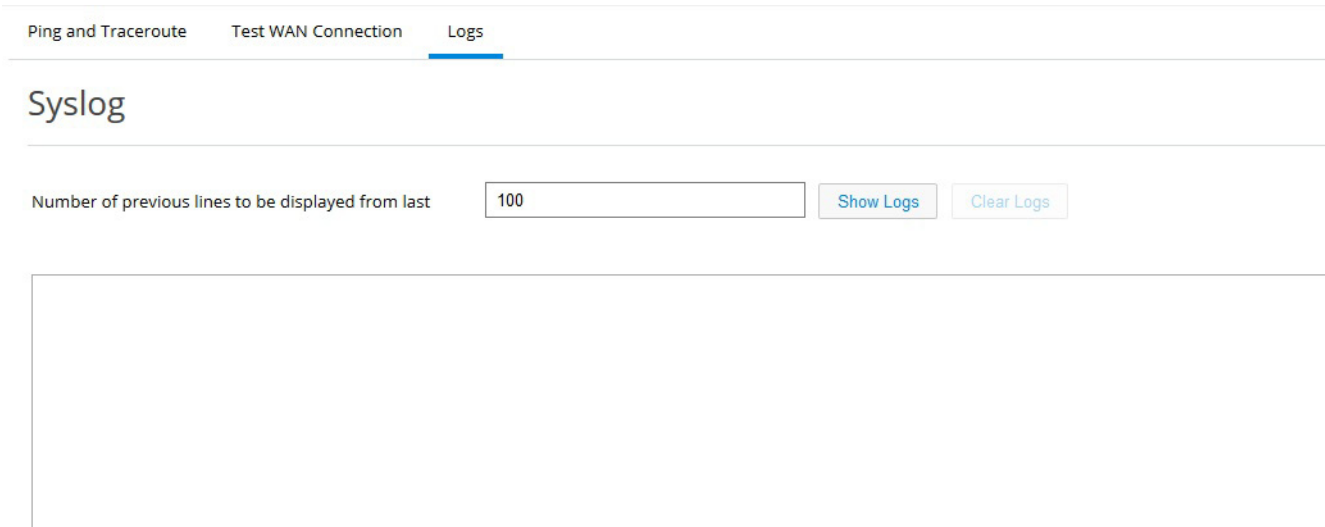
1. Hover mouse on the Configure icon that is available on the right pane. The settings menu appears.
2. Click on the Enable SDEE Notifications option.
3. After the setting is applied, the menu item changes to Disable SDEE Notifications. This is because in the device, it is enabled. If you click on this option again, it toggles the state on the device as well as on the menu.

### Syslog

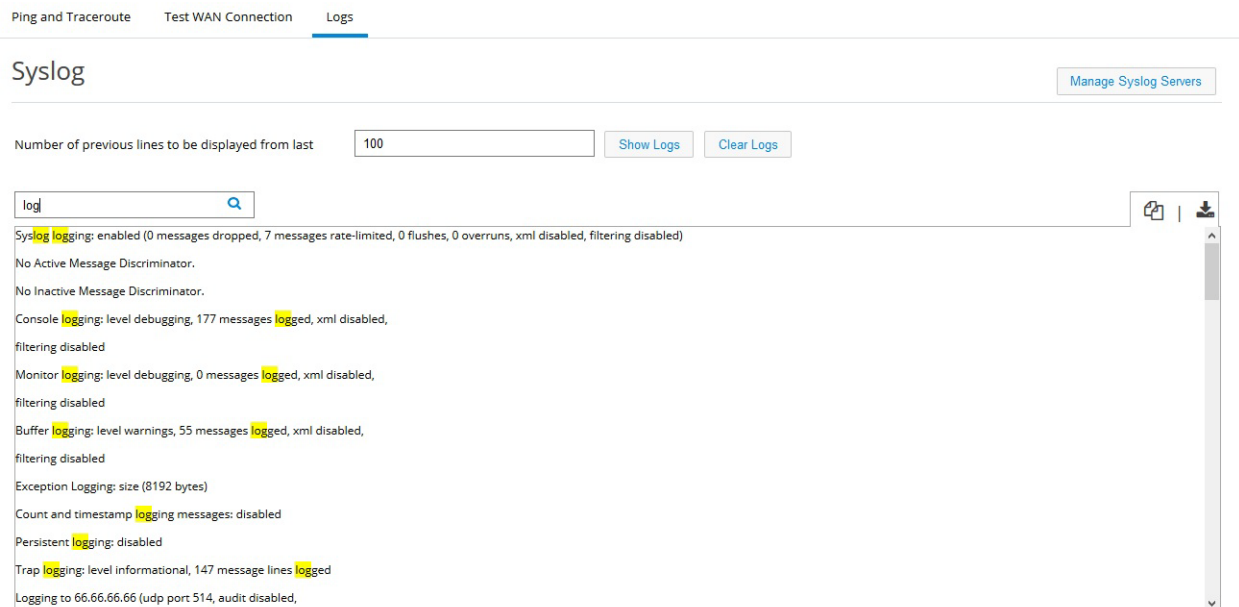
Use this section to check the Syslog on the device. This feature is available in CCP Express Release 3.5.2 and later releases.

To enable Syslog:

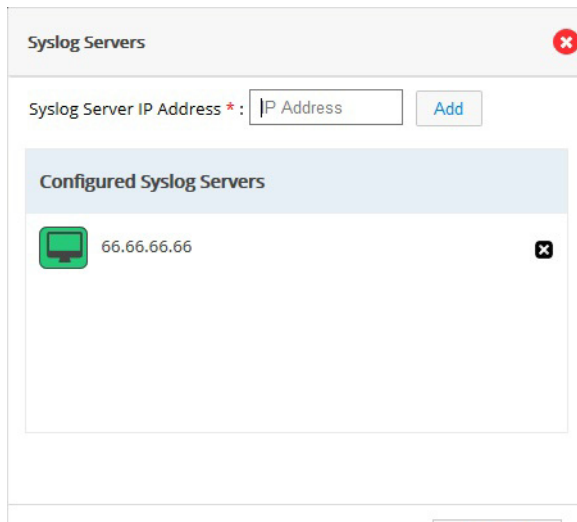
1. Click Troubleshoot and navigate to the Log option.

**Figure 83 Syslog View**

2. Enter the number of lines to be displayed and click on “Show Logs”. Once logs are listed user can search for a particular string and all the occurrences will be highlighted.

**Figure 84 Syslog - Show Logs**

3. You can also configure Syslog servers.

**Figure 85 Syslog Servers**

## VPN

CCP Express supports creation of IPsec multi-site VPN configuration, DMVPN spoke side configuration, DMVPN hub configuration, remote access configuration, a combination of IPsec multi-site with remote access configurations, and a combination of DMVPN hub with remote access VPN configurations.

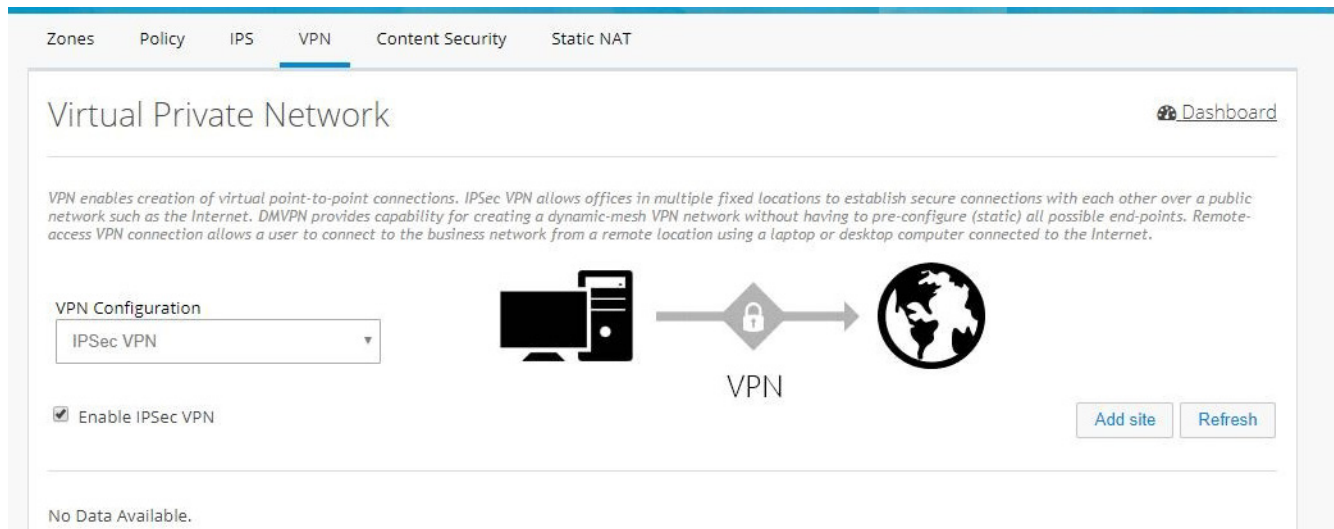
### Prerequisite for VPN

Primary WAN interface must be configured and should be part of WAN Zone. Also, LAN interfaces should be part of LAN Zone before configuring any VPN.

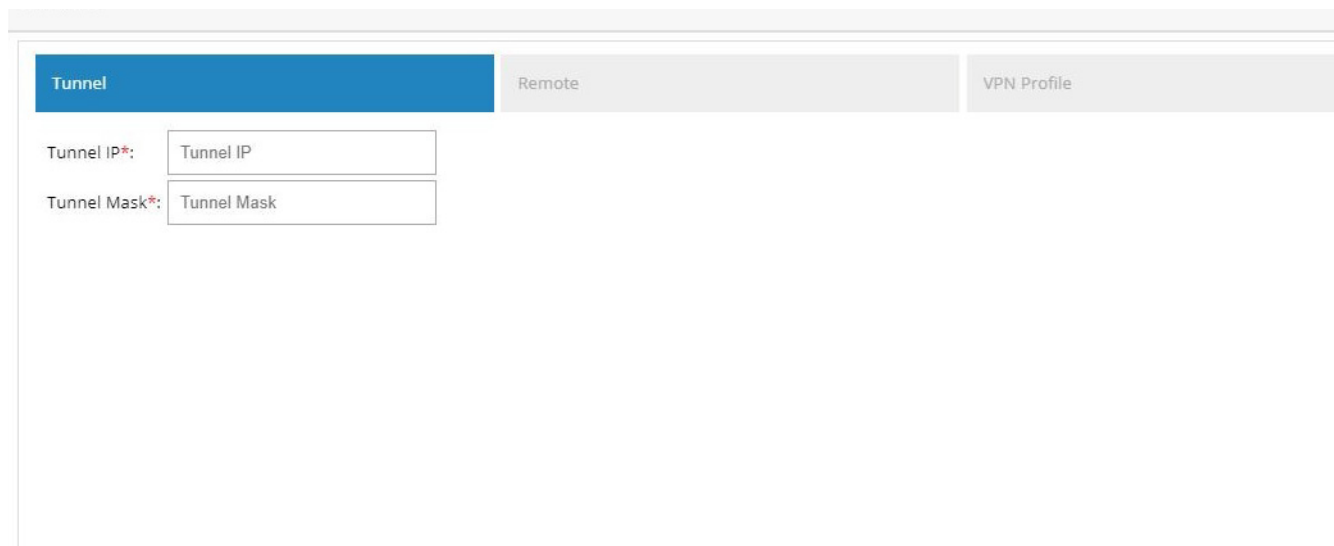
### IPsec Multi-Site Configuration

To configure multi-site VPN:

1. Click **Security** > **VPN** and select **IPsec** option from the VPN Configuration drop-down list.
2. Click the Enable VPN check box and click **Add Site**. The VPN wizard is displayed as a popup dialog.

**Figure 86 IPsec Multi-Site VPN**

3. Provide Tunnel IP and Mask for the site being configured.

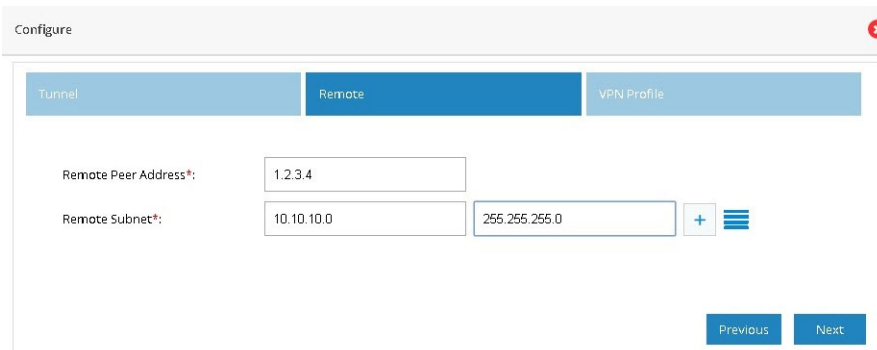
**Figure 87 IPsec Multi-Site VPN (Tunnel Configuration)**

**Note:** By default, from configuring site end, all the LAN side networks are allowed to access the other end through VPN tunnel.

4. Provide the remote peer address (WAN IP address of the other end).



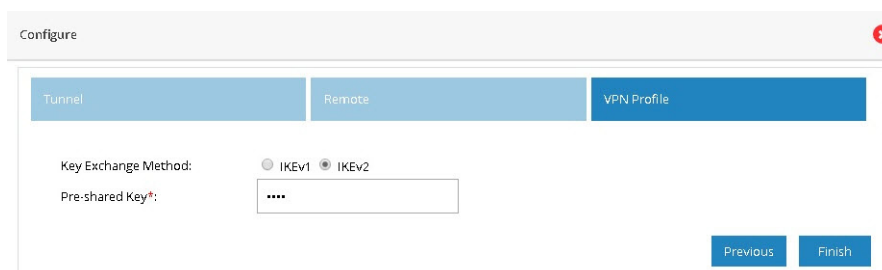
**Figure 88 IPsec Multi-Site VPN (Remote Configuration)**



5. Select an appropriate Key Exchange model (either IKEv1 or IKEv2). By default, IKEv2 is selected and that is recommended.

6. Provide Pre shared Key.

**Figure 89 IPsec Multi-Site VPN (Profile)**



7. (Optional) Select Advance to manually configure IKE and IPsec parameters.

**Figure 90** IPsec Multi-Site VPN (Advanced Options)

Configure

Tunnel Remote VPN Profile

Key Exchange Method:  IKEv1  IKEv2

Pre-shared Key\*:

Configuration Level:  Basic  Advanced

Group:

Transform Set:

Integrity:

Encryption:

8. Click Finish.

After the configuration is complete, the list of sites is displayed. You can choose to add more or delete sites from the available list.

**Figure 91** IPsec Multi-Site VPN (Completed)

Zones Policy IPS VPN Content Security Static NAT

Virtual Private Network [Dashboard](#)

VPN enables creation of virtual point-to-point connections. IPsec VPN allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the Internet. DMVPN provides capability for creating a dynamic-mesh VPN network without having to pre-configure (static) all possible end-points. Remote-access VPN connection allows a user to connect to the business network from a remote location using a laptop or desktop computer connected to the Internet.

VPN Configuration:

Enable IPsec VPN

Destination Site	Tunnel	Site Status	Action
<input type="checkbox"/> 112.11.11.1	Tunnel0	Down	

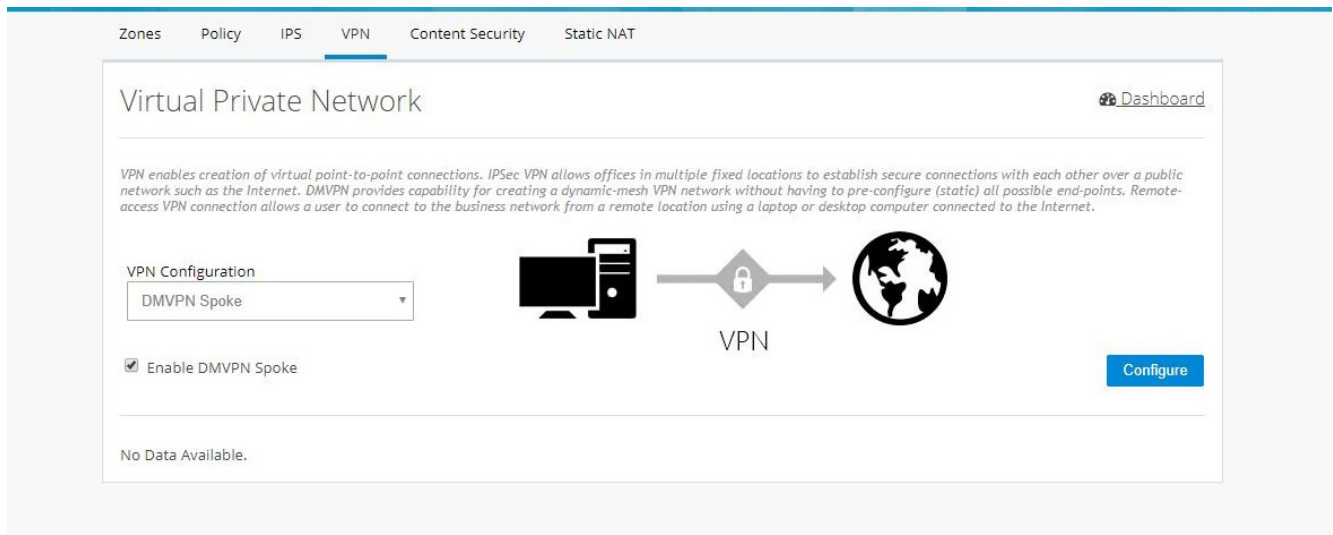
**Note:** If CCP Express is used to configure the Multi-Site VPN, ensure that both the ends are configured with CCP Express only. CCP Express internally uses the transform set as esp-aes, esp-sha-hmac and IKEv2 Proposal with encryption as 3des, integrity as md5 and Diffie Helman group as 2.

## DMVPN Spoke Configuration

To enable DMVPN Spoke configuration:

1. Click **Security** > **VPN** and select **DMVPN Spoke** option from the VPN Configuration drop-down list.
2. Click Enable DMVPN Spoke check box, and click **Configure**.

**Figure 92 DMVPN Spoke Configuration**



3. Provide Tunnel IP, Backup Tunnel IP, and Tunnel Mask for site being configured.
4. Provide the Remote Tunnel Address (WAN IP address of the other end). You can also provide the FQDN of the Hub device. Click **Next**.

**Figure 93 DMVPN Spoke Configuration (VPN Peers)**

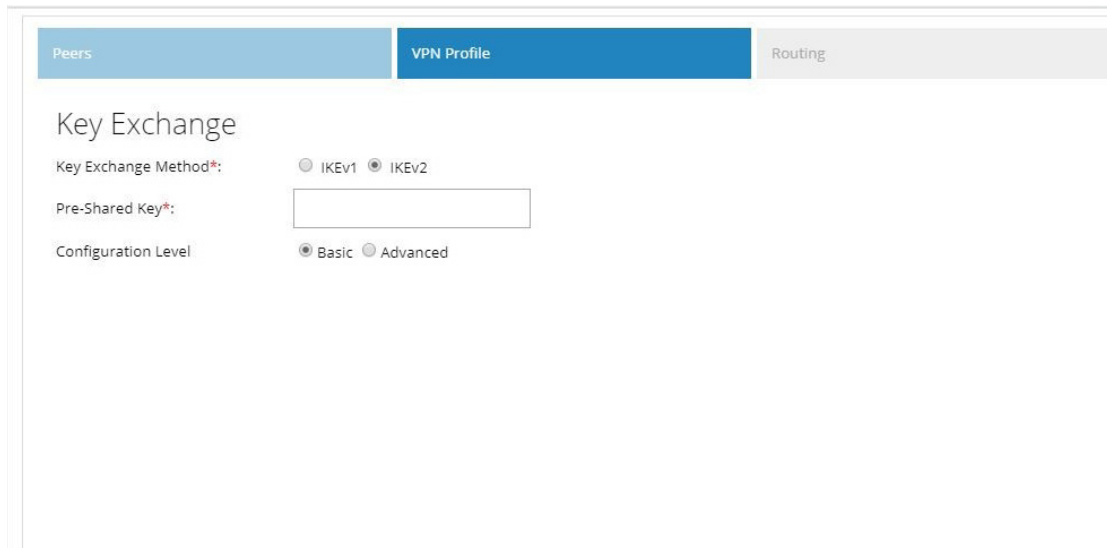
The screenshot shows the 'Configure' window for DMVPN Spoke Configuration (VPN Peers). The 'Peers' tab is active. The configuration is divided into 'Spoke' and 'Hub' sections. The 'Spoke' section has three required fields: Tunnel IP, Backup Tunnel IP, and Tunnel Mask. The 'Hub' section has two radio buttons for 'Transport Address' (selected) and 'FQDN', and two input fields: Transport Address and Remote Tunnel Address. Navigation buttons 'Previous' and 'Next' are at the bottom right.

By default from configuring site end all the LAN side networks are allowed to access the other end through VPN Tunnel.

When DMVPN Spoke configuration is successfully completed, and the Hub is configured and active, the tunnel will come up between Hub and Spoke.

5. Select an appropriate Key Exchange model (either IKEv1 or IKEv2). By default, IKEv2 is selected and is recommended.
6. Provide the Pre-Shared Key.

**Figure 94 DMVPN Spoke Configuration (VPN Profile)**



**Figure 95 DMVPN Spoke Configuration (VPN Profile Advanced Options)**



7. Provide an EIGRP Autonomous number in the range of 1-65535.

**Figure 96 DMVPN Spoke Configuration (Routing)**

8. Click **Finish**.

**Figure 97 DMVPN Spoke Configuration (Completed)**

Virtual Private Network [Dashboard](#)

VPN enables creation of virtual point-to-point connections. IPsec VPN allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the Internet. DMVPN provides capability for creating a dynamic-mesh VPN network without having to pre-configure (static) all possible end-points. Remote-access VPN connection allows a user to connect to the business network from a remote location using a laptop or desktop computer connected to the Internet.

VPN Configuration  
DMVPN Spoke

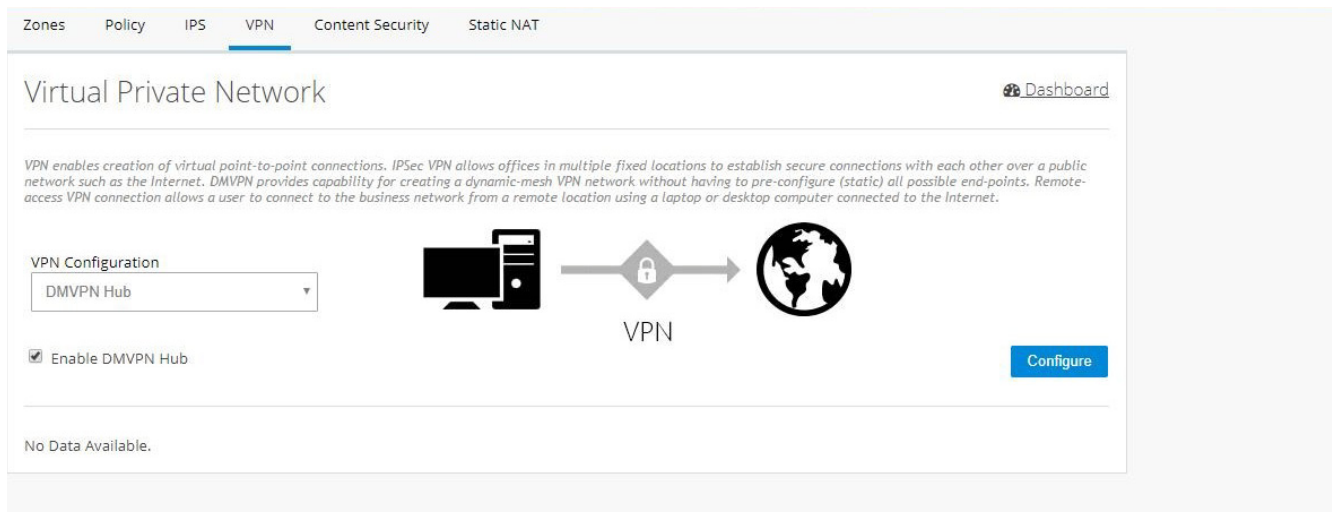
Enable DMVPN Spoke

Destination Site	Tunnel	Site Status	Action
123.22.22.2	Tunnel0	DOWN-NEGOTIATING	

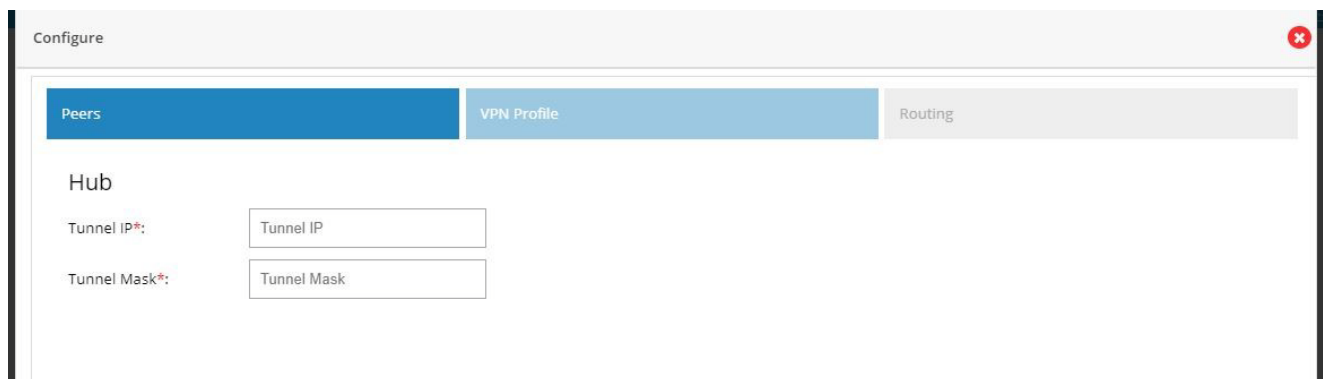
## DMVPN Hub Configuration

To configure DMVPN Hub:

1. Click **Security** > **VPN** and select **DMVPN Hub** option from the VPN Configuration drop-down list.
2. Click Enable DMVPN Hub check box, and click **Configure**.

**Figure 98 DMVPN Hub Configuration**

3. Provide Tunnel IP and Mask for the hub being configured.

**Figure 99 DMVPN Hub Configuration (VPN Peers)**

4. Select an appropriate Key Exchange model (either IKEv1 or IKEv2). By default, IKEv2 is selected and is recommended.
5. Provide the Pre-Shared Key.

**Figure 100 DMVPN Hub Configuration (VPN Profile)**

The screenshot shows the 'VPN Profile' configuration page in the Cisco Configuration Professional Express interface. The 'Key Exchange' section is active, showing the following settings:

- Key Exchange Method\*:** IKEv1 (unselected), IKEv2 (selected)
- Pre-Shared Key\*:** An empty text input field.
- Configuration Level:** Basic (selected), Advanced (unselected)

**Figure 101 DMVPN Hub Configuration (VPN Profile Advanced Options)**

The screenshot shows the 'VPN Profile' configuration page in the Cisco Configuration Professional Express interface, displaying advanced options. The 'Key Exchange' section is active, showing the following settings:

- Key Exchange Method\*:** IKEv1 (unselected), IKEv2 (selected)
- Pre-Shared Key\*:** An empty text input field.
- Configuration Level:** Basic (unselected), Advanced (selected)

Below the 'Key Exchange' section, the following options are available:

- Group:** 1, 2, 5, 14, 15, 16, 19, 20, 21, 24
- Transform Set:** ah-md5-hmac, ah-sha-hmac, ah-sha256-hmac, ah-sha384-hmac, ah-sha512-hmac, comp-lzs, esp-3des, esp-aes, esp-des, esp-gcm, esp-gmac, esp-md5-hmac, esp-null, esp-seal, esp-sha-hmac, esp-sha256-hmac, esp-sha384-hmac, esp-sha512-hmac
- Integrity:** md5, sha1, sha256, sha384, sha512
- Encryption:** 3des, aes-cbc-128, aes-cbc-192, aes-cbc-256, aes-gcm-128, aes-gcm-256, des

Navigation buttons 'Previous' and 'Next' are visible at the bottom right of the configuration area.

6. Provide the routing configuration.

7. Provide an EIGRP Autonomous number in the range 1–65535.



**Figure 102 DMVPN Hub Configuration (Routing)**

Peers	VPN Profile	Routing
Eigrp Autonomous No.*:	<input type="text"/>	
Local LAN Subnet:	<input type="text" value="Local LAN Subnet"/>	
Wildcard Mask:	<input type="text" value="Wildcard Mask"/> <input type="button" value="+"/>	
		<input type="button" value="Previous"/> <input type="button" value="Finish"/>

8. Click **Finish**.

**Figure 103 DMVPN Hub Configuration (Completed)**

Virtual Private Network Dashboard

VPN enables creation of virtual point-to-point connections. IPsec VPN allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the Internet. DMVPN provides capability for creating a dynamic-mesh VPN network without having to pre-configure (static) all possible end-points. Remote-access VPN connection allows a user to connect to the business network from a remote location using a laptop or desktop computer connected to the Internet.

VPN Configuration

Enable DMVPN HUB + Remote Access VPN

Pool Name	Address(From)	Address(To)
demopool	10.10.10.2	10.10.10.8

Destination Site	Tunnel	Action
11.11.11.5	Tunnel0	<input type="button" value="edit"/> <input type="button" value="delete"/>

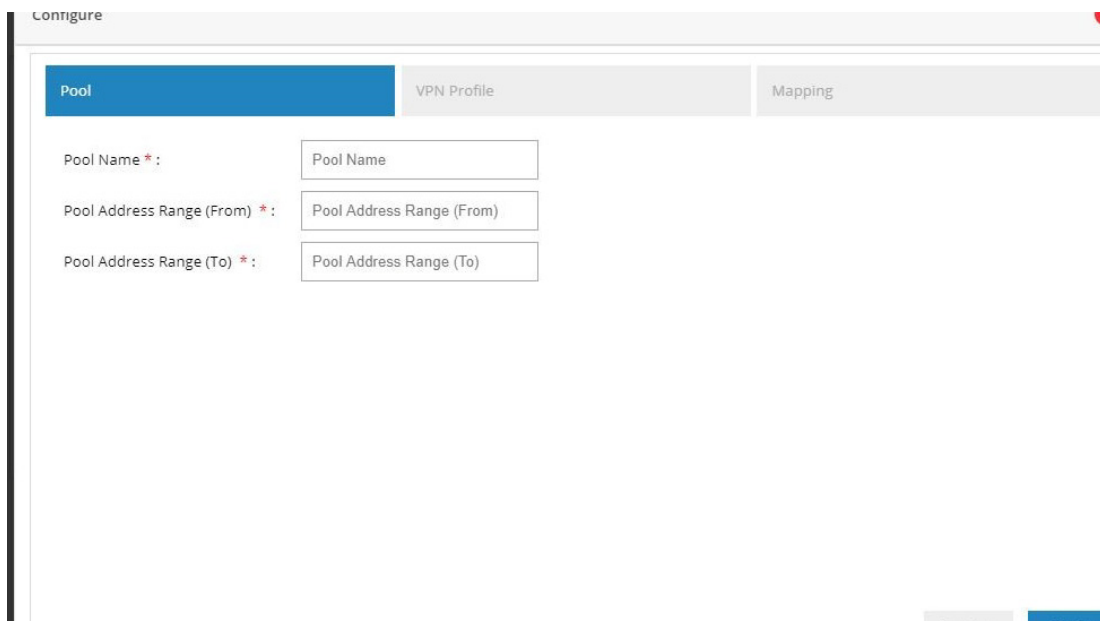
## Remote Access VPN Configuration

To configure Remote Access VPN, perform these steps:

1. Click **Security** > **VPN** and select **Remote Access VPN** option.
2. Click the Enable Remote Access VPN check box, and click **Configure**.

**Figure 104 Remote Access Configuration**

3. Provide Pool Name and the range of IP Addresses for the pool.

**Figure 105 Remote Access Configuration (Pool)**

4. Provide the Pre shared Key.

**Note:** By default, Remote Access VPN configuration supports only IKEv1 Key Exchange model and IP Sec enabled L2TP protocol.

**Figure 106 Remote Access Configuration (VPN Profile)**

The screenshot shows a configuration wizard with three tabs: 'Pool', 'VPN Profile', and 'Mapping'. The 'VPN Profile' tab is selected. Below the tabs, there is a label 'Pre-shared Key \*' followed by a text input field containing the text 'Pre-shared Key'. At the bottom right of the wizard, there are two buttons: 'Previous' and 'Next'.

5. Select the Crypto Map interface.

**Figure 107 Remote Access Configuration (Mapping)**

The screenshot shows the same configuration wizard with the 'Mapping' tab selected. Below the tabs, there is a label 'Crypto Map Interface \*' followed by a dropdown menu showing 'GigabitEthernet0/1'. At the bottom right of the wizard, there are two buttons: 'Previous' and 'Finish'.

6. Click **Finish**.

**Figure 108 Remote Access Configuration (Completed)**

The screenshot shows the 'Virtual Private Network' configuration page in the Cisco Configuration Professional Express. The 'VPN Configuration' dropdown is set to 'Remote Access VPN'. The 'Enable Remote Access VPN' checkbox is checked. Below this, a table lists the VPN configuration details:

Pool Name	Address(From)	Address(To)	Actions
demo	10.10.10.3	10.10.10.6	

### IPSec Multi-Site and Remote Access VPN Configuration Combination

To configure the combination of IPSec Multi-Site and Remote Access VPN configurations:

1. Click **Security > VPN** and select **IPSec VPN + Remote Access** option from **VPN Configuration** option.
2. Click the **Enable IPSEC + Remote Access VPN** check box, and click **Configure**.

**Figure 109 IPSec Multi-Site and Remote Access Configuration Combination**

The screenshot shows the 'Virtual Private Network' configuration page in the Cisco Configuration Professional Express. The 'VPN Configuration' dropdown is set to 'IPSec VPN + Remote Access VPN'. The 'Enable IPSEC + Remote Access VPN' checkbox is checked. A 'Configure' button is visible on the right side of the page. Below the configuration options, the text 'No Data Available.' is displayed.

3. Provide Tunnel IP and Mask for the site being configured.

**Figure 110 IPsec Multi-Site and Remote Access Configuration Combination (Tunnel)**

The screenshot shows the 'Configure' page with three tabs: 'Tunnel', 'Remote', and 'VPN Profile'. The 'Tunnel' tab is active. Below the tabs, there are two input fields: 'Tunnel IP\*' with the value 'Tunnel IP' and 'Tunnel Mask\*' with the value 'Tunnel Mask'.

**Note:** By default, from configuring site end, all the LAN side networks are allowed to access the other end through VPN tunnel.

4. Provide the Remote Peer Address (WAN IP address of the other end) information.

Enter the pool information, Preshared Key, and Crypto Map Interface.

**Figure 111 IPsec Multi-Site and Remote Access Configuration Combination (Remote)**

The screenshot shows the 'Configure' page with three tabs: 'Tunnel', 'Remote', and 'VPN Profile'. The 'Remote' tab is active. Below the tabs, there are several input fields and a dropdown menu:

- 'Remote Peer Address\*' with the value 'Remote Peer Address'
- 'Remote Subnet\*' with two fields: 'IP Address' and 'Subnet Mask', and a '+' button.
- 'Remote Access VPN' section:
  - 'Pool Name \*' with the value 'Pool Name'
  - 'Pool Address Range (From) \*' with the value 'Pool Address Range (From)'
  - 'Pool Address Range (To) \*' with the value 'Pool Address Range (To)'
  - 'Pre-shared Key \*' with the value 'Pre-shared Key'
  - 'Crypto Map Interface \*' with a dropdown menu showing 'GigabitEthernet0/1'

At the bottom right, there are two buttons: 'Previous' and 'Next'.

5. Ensure that the IKEv2 is selected.

**Note:** IKEv2 is the only key exchange method available.

**Figure 112 IPsec Multi-Site and Remote Access Configuration Combination (VPN Profile)**

Configure

Tunnel Remote VPN Profile

Key Exchange Method:  IKEv2

Pre-shared Key\*:

Configuration Level:  Basic  Advanced

Previous Finish

**Figure 113 IPsec Multi-Site and Remote Access Configuration Combination (Advanced Options)**

Configure

Tunnel Remote VPN Profile

Key Exchange Method:  IKEv2

Pre-shared Key\*:

Configuration Level:  Basic  Advanced

Group:

Transform Set:

ah-md5-hmac	ah-sha-hmac	ah-sha256-hmac	ah-sha384-hmac	ah-sha512-hmac	comp-lzs
esp-3des	esp-aes	esp-des	esp-gcm	esp-gmac	esp-md5-hmac
esp-null	esp-seal	esp-sha-hmac	esp-sha256-hmac	esp-sha384-hmac	esp-sha512-hmac

Integrity:

md5	sha1	sha256	sha384	sha512
-----	------	--------	--------	--------

Encryption:

3des	aes-cbc-128	aes-cbc-192	aes-cbc-256	aes-gcm-128	aes-gcm-256
des					

Previous Finish

**Note:** If CCP Express is used to configure the Multi-Site VPN, ensure that both the ends are configured with CCP Express only. CCP Express internally uses the transform set as esp-aes, esp-sha-hmac and IKEv2 Proposal with encryption as 3des, integrity as md5 and Diffie Helman group as 2.

6. Click **Finish**.

**Figure 114 IPsec Multi-Site and Remote Access Configuration Combination (Completed)**

Virtual Private Network [Dashboard](#)

VPN enables creation of virtual point-to-point connections. IPsec VPN allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the Internet. DMVPN provides capability for creating a dynamic-mesh VPN network without having to pre-configure (static) all possible end-points. Remote-access VPN connection allows a user to connect to the business network from a remote location using a laptop or desktop computer connected to the Internet.

VPN Configuration  
IPsec VPN + Remote Access VPN

Enable IPSEC + Remote Access VPN Configure

Pool Name	Address(From)	Address(To)
demopool	10.10.10.8	10.10.10.10

Destination Site	Tunnel	Site Status	Action
112.11.11.1	Tunnel0	Down	

### DMVPN Hub and Remote Access Configuration Combination

To configure the combination of DMVPN Hub and Remote Access VPN configurations:

1. Click **Security** > **VPN** and select the **DMVPN Hub + Remote Access VPN** option from the VPN Configuration drop-down list.
2. Click Enable DMVPN Hub + Remote Access VPN check box, and click **Configure**.

**Figure 115 DMVPN Hub and Remote Access Configuration Combination**

Zones Policy IPS **VPN** Content Security Static NAT

Virtual Private Network [Dashboard](#)

VPN enables creation of virtual point-to-point connections. IPsec VPN allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the Internet. DMVPN provides capability for creating a dynamic-mesh VPN network without having to pre-configure (static) all possible end-points. Remote-access VPN connection allows a user to connect to the business network from a remote location using a laptop or desktop computer connected to the Internet.

VPN Configuration  
DMVPN Hub + Remote Access VPN

Enable DMVPN HUB + Remote Access VPN Configure

No Data Available.

3. Provide Tunnel IP and Mask for the hub being configured.

Enter the pool information, Preshared Key, and Crypto Map Interface.

**Figure 116 DMVPN Hub and Remote Access Configuration Combination (VPN Peers)**

Configure

Peers VPN Profile Routing

Hub

Tunnel IP\*: Tunnel IP

Tunnel Mask\*: Tunnel Mask

Remote Access VPN

Pool Name \* : Pool Name

Pool Address Range (From) \* : Pool Address Range (From)

Pool Address Range (To) \* : Pool Address Range (To)

Pre-shared Key \* : Pre-shared Key

Crypto Map Interface \* : GigabitEthernet0/1

Previous Next

**4. Ensure that the IKEv2 is selected.**

**Note:** IKEv2 is the only key exchange method available.

**5. Provide the Pre-Shared Key.****Figure 117 DMVPN Hub and Remote Access Configuration Combination (VPN Profile)**

Peers VPN Profile Routing

Key Exchange

Key Exchange Method\*:  IKEv2

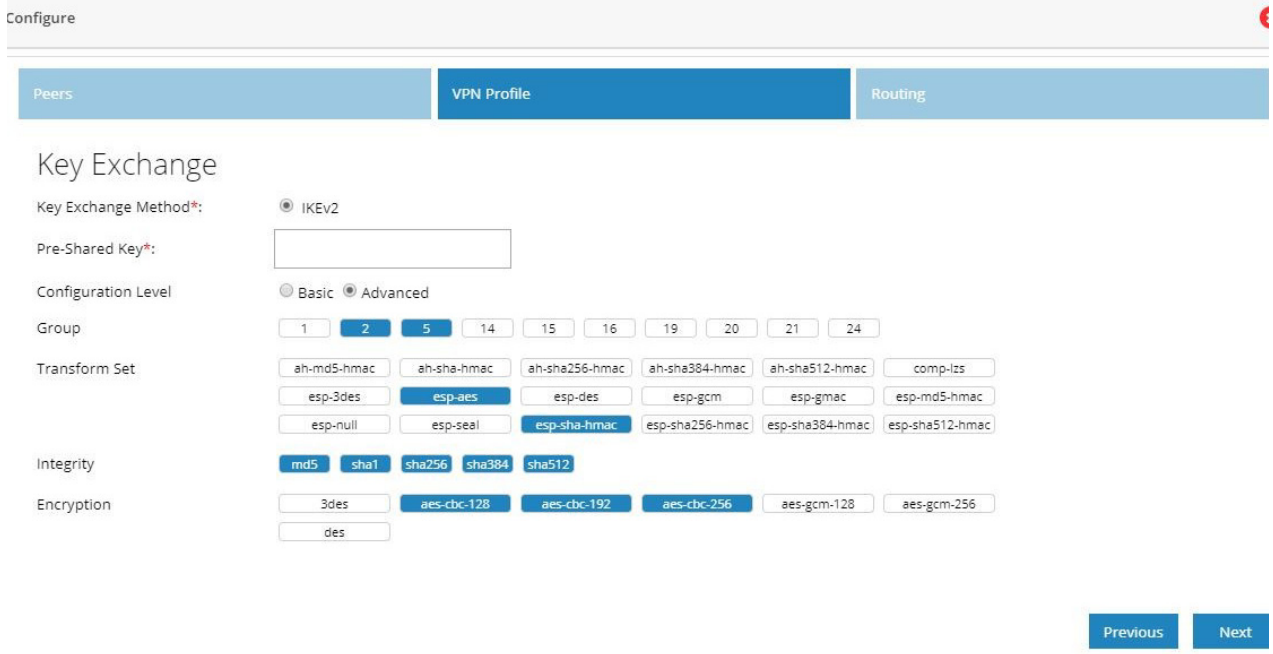
Pre-Shared Key\*:

Configuration Level  Basic  Advanced

Previous

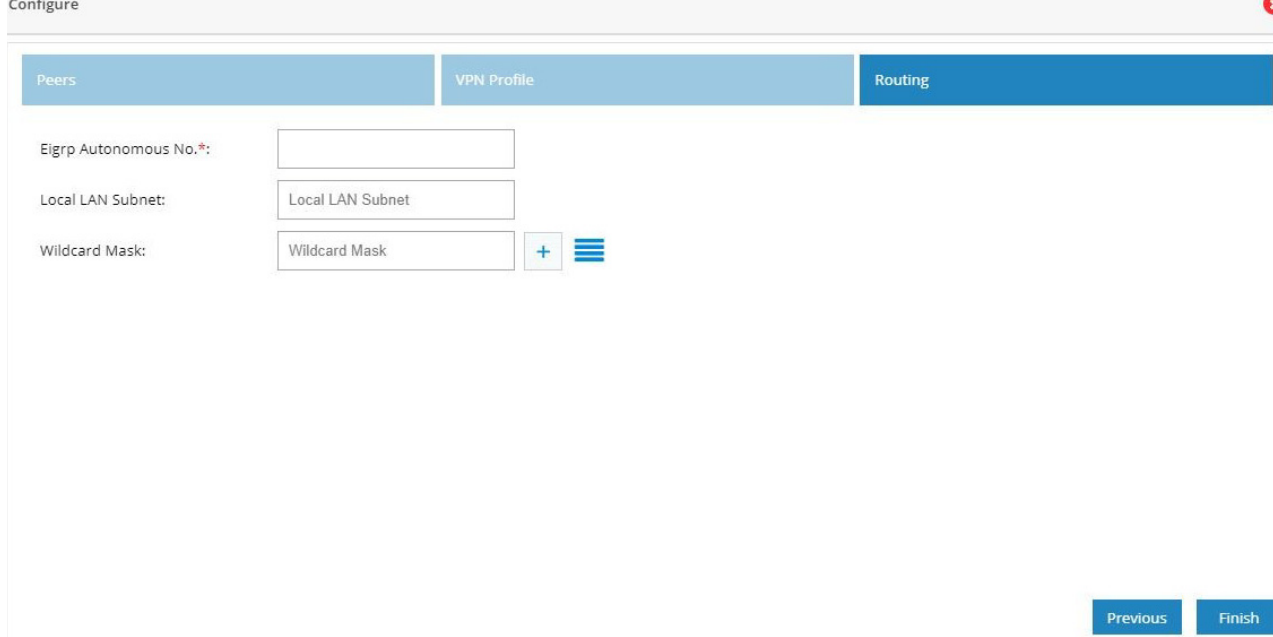


**Figure 118 DMVPN Hub and Remote Access Configuration Combination (VPN Profile Advanced Options)**



6. Provide the routing configuration.
7. Provide an EIGRP Autonomous number in the range 1–65535.

**Figure 119 DMVPN Hub and Remote Access Configuration Combination (Routing)**



8. Click **Finish**.

**Figure 120 DMVPN Hub and Remote Access Configuration Combination (Completed)**

Virtual Private Network [Dashboard](#)

VPN enables creation of virtual point-to-point connections. IPsec VPN allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the Internet. DMVPN provides capability for creating a dynamic-mesh VPN network without having to pre-configure (static) all possible end-points. Remote-access VPN connection allows a user to connect to the business network from a remote location using a laptop or desktop computer connected to the Internet.

VPN Configuration  
DMVPN Hub + Remote Access VPN

Enable DMVPN HUB + Remote Access VPN

Pool Name	Address(From)	Address(To)
demopool	10.10.10.2	10.10.10.8

Destination Site	Tunnel	Action
11.11.11.5	Tunnel0	<a href="#">✎</a> <a href="#">🗑️</a>

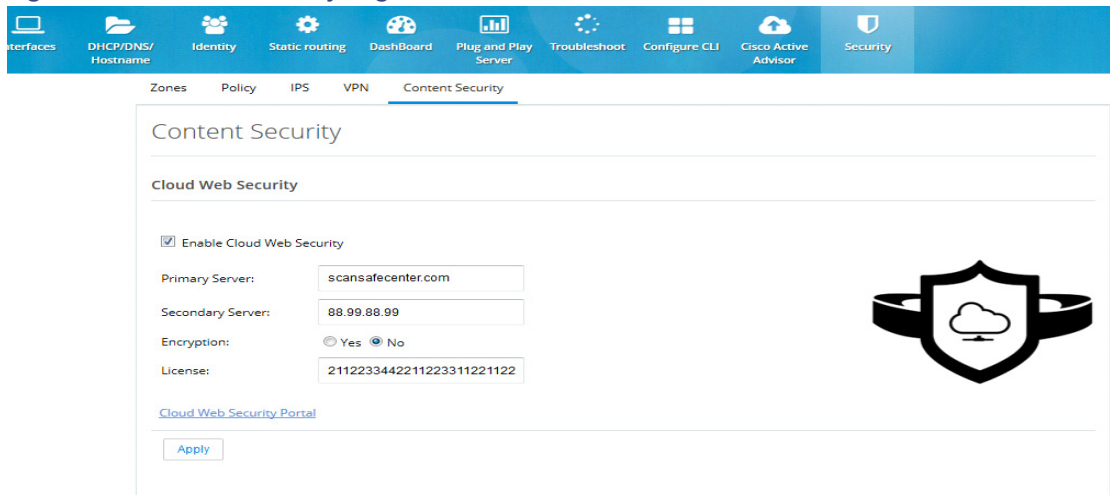
## Content Security

Cloud based 'Security as a Service' (SecaaS) such as Cloud Web Security (CWS) is a scalable means to provide market-leading web security to quickly and easily protect the network from web-based threats, such as Malware, while saving bandwidth, money, and resources. CWS provides Anti-X functionality (anti-malware, anti-bot, anti-virus, and anti-phishing) on ISR-G2 itself without the need for expensive Security Appliances in branch, small offices.

To configure content security, perform these steps:

1. Click **Security > Content Security**.
2. Provide Primary CWS Server IP address or DNS resolvable hostname and Secondary server information.
3. Provide the license key received from CWS service provider and specify if it is an encrypted or unencrypted key.

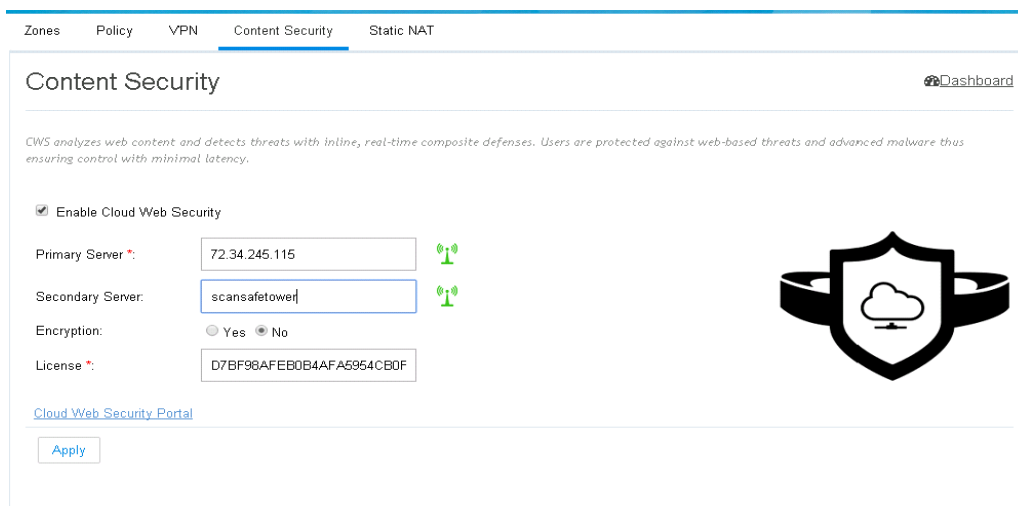
**Figure 121 Content Security Page**



### Edit Content Security

After CWS is fully configured and the tower is reachable, a green tower icon displays as shown in the screen below. Otherwise, the tower is displayed in red.

**Figure 122 Content Security Page**



### Static NAT

Static NAT creates a fixed translation of unregistered real address to mapped registered address. Also with port forwarding option, it is possible to open ports in response to inbound traffic for a specified service.

## More Options - Top Menu Small Icons

To create a static NAT:

1. Click **Security > Static NAT**. To add a Static NAT, click **Add**. A dialog box opens.

**Figure 123 Static NAT Page**

	Internal IP	External IP/Interface	Port Forwarding	Action
<input type="checkbox"/>	10.30.10.10	GigabitEthernet0/1	false	
<input type="checkbox"/>	10.10.20.30	77.77.88.88	false	
<input type="checkbox"/>	10.20.20.20	88.88.99.99	true (TCP)	

2. Provide the Internal IP address which needs to be translated and the external IP address or Interface.
3. If you need to send the traffic to specific port, click **Enable Port Forwarding** check box, and select the type of port, for example TCP or UDP. If the port type is not known, select Any option which supports both the type of ports.
4. After selecting the ports, specify the internal and external ports.

**Figure 124 Edit Static NAT Page**

IP Type

Internal IP\*: 10.34.170.1

External IP/Interface\*: 34.45.1.7

Enable Port Forwarding

Port Forwarding

TCP  UDP  Any

Internal Port\*: 45

External Port\*: 67

Ok Cancel

## More Options - Top Menu Small Icons

You can perform the following tasks by hovering over the icons on the right side of the page:

## More Options - Top Menu Small Icons

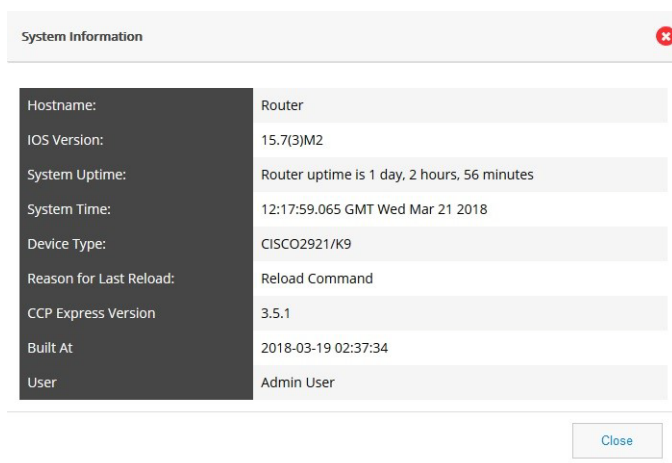


- [System Information, page 85](#)
- [Configure CLI, page 85](#)
- [Save Configuration, page 86](#)
- [Running Configuration Download, page 87](#)
- [Options Menu, page 87](#)
- [Upgrade CCP Express, page 90](#)
- [Upgrade IOS, page 94](#)

## System Information

To access the basic system information window, click the “info” icon (i) on top right.


**Figure 125 System Information**



## Configure CLI

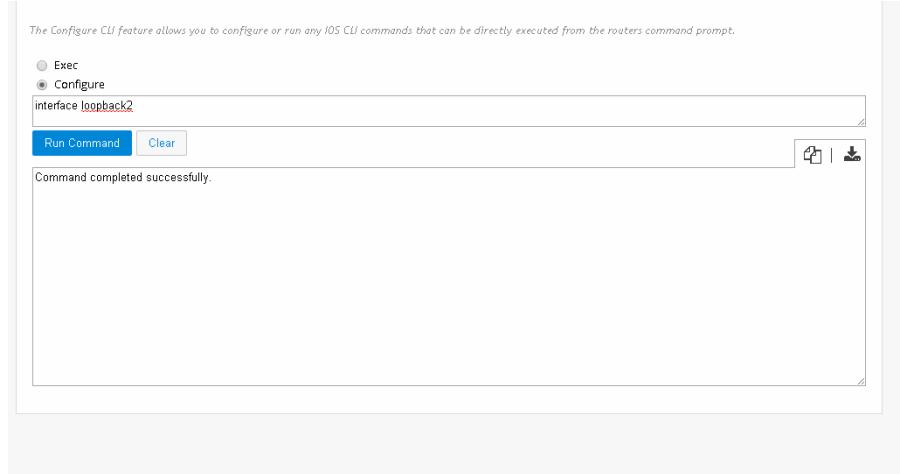
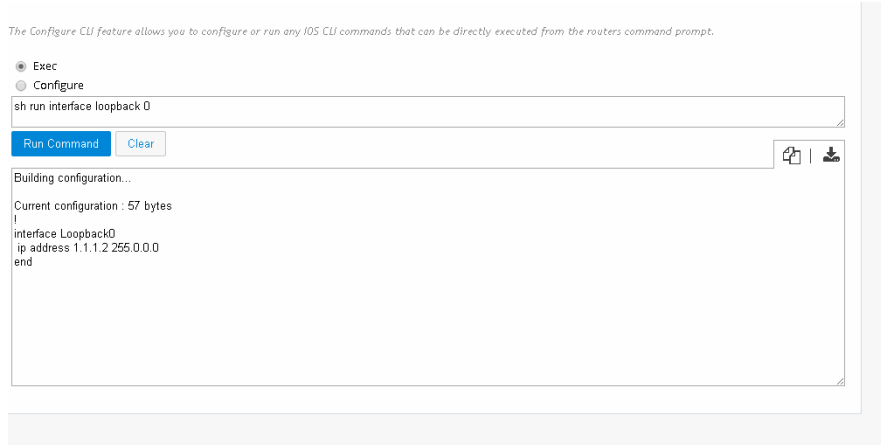
The Configure CLI feature allows you to configure or run any IOS CLI commands that can be directly executed from the router’s command prompt.

To configure a CLI, perform these steps:

1. Click the **Configure CLI** icon  to open the CLI configuration page.
2. From the Configure CLI tab, select the mode in which you want to execute the CLI. You can select either the **Exec** or **Configure** mode.

**Note:** If you issue multiple commands, the output is listed for each command as shown in a terminal window with the command followed by the output.

## More Options - Top Menu Small Icons

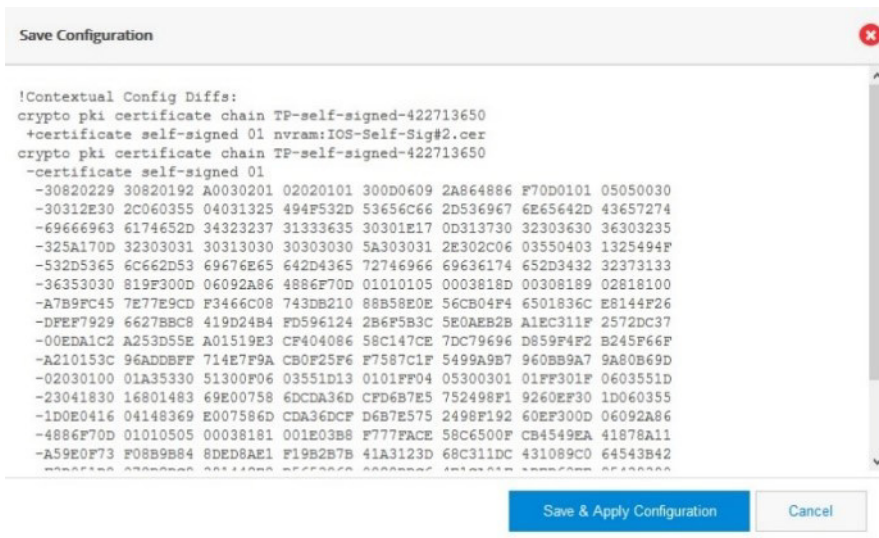
**Figure 126** An example of a command executed in Config mode**Figure 127** An example of a command executed in Exec mode

3. In the text box, type the CLI you want to execute.
4. Click **Run Command** to execute the CLI. The CLI's output is displayed.
5. You can also copy-to-clipboard or download the retrieved data by clicking on COPY or DOWNLOAD icons to the right of the details box.

**Note** Using the Configure CLI feature, you cannot configure interactive commands and service module related commands.

## Save Configuration

Save Configuration helps you check and sync the difference between the running and startup configs. To access the Save Configuration window, click the save button on the top right.

**Figure 128 Save Configuration**

This window lists the Startup Configuration. Click Save and Apply Configuration to apply the Startup Configuration.

## Running Configuration Download

Click on Running Config icon allows you to save the running configuration to memory.

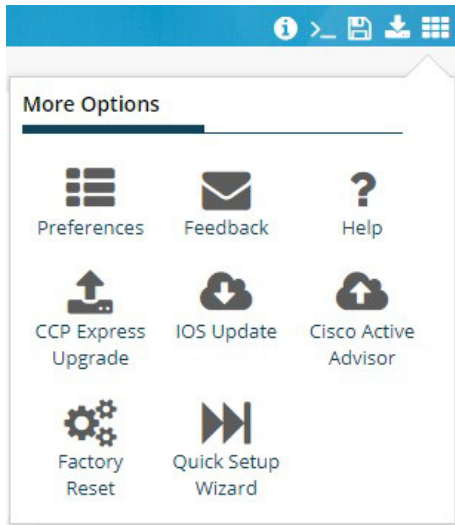
## Options Menu

**Note:** This Options menu is only available in the old UI. The new UI has these features on top right side and also in main menu options.

In the upper right side, click the  icon to display the More Options window.

## More Options - Top Menu Small Icons

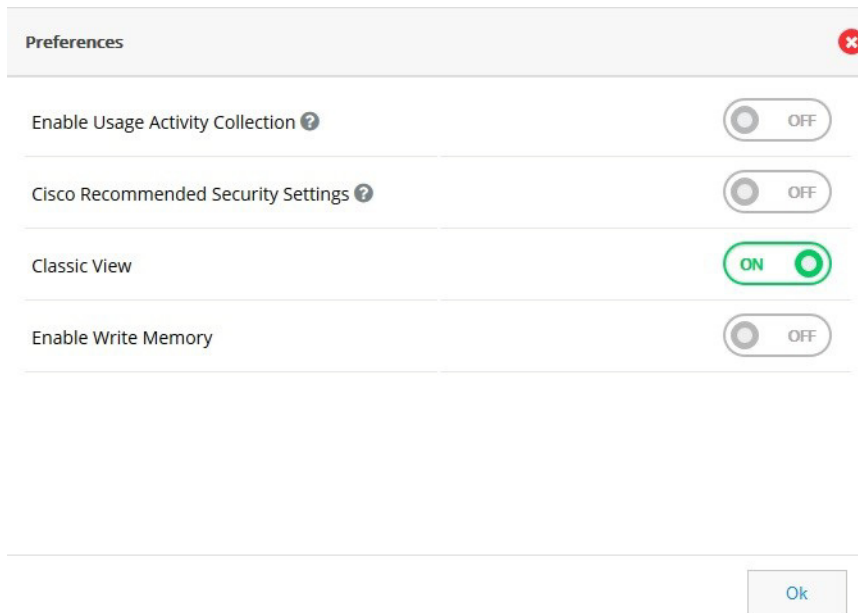
Figure 129 More Options



**Note:** The Quick Setup Wizard icon appears only if the device is factory fresh.

## Preferences

Figure 130 Preferences



## Enable Usage Activity Collection

Turning this option On allows Cisco to collect data on the usage patterns of the Device Manager. Cisco only collects data on the usage patterns and does not collect network or configuration data.



## More Options - Top Menu Small Icons

### Cisco Recommended Security Settings

Turning this option On ensures all passwords are encrypted and are not shown in plain text.

### Feedback

Use this option to provide your user experience to Cisco. Let us know how we can improve the product.

### Help

Help takes you to this feature guide on Cisco.com.

## Cisco Active Advisor

The Cisco Active Advisor feature provides the essential life cycle information about your network inventory. Cisco Active Advisor also helps to reduce network's overall risks by updating the status of the products in the network periodically. Cisco Active Advisor shows the following information:

- Warranty and service contract status
- Product advisories, including Product Security Incident Response Teams (PSIRTs) and field notices
- End-of-Life notifications for hardware and software

The CAA feature is available in More Options.

This section contains:

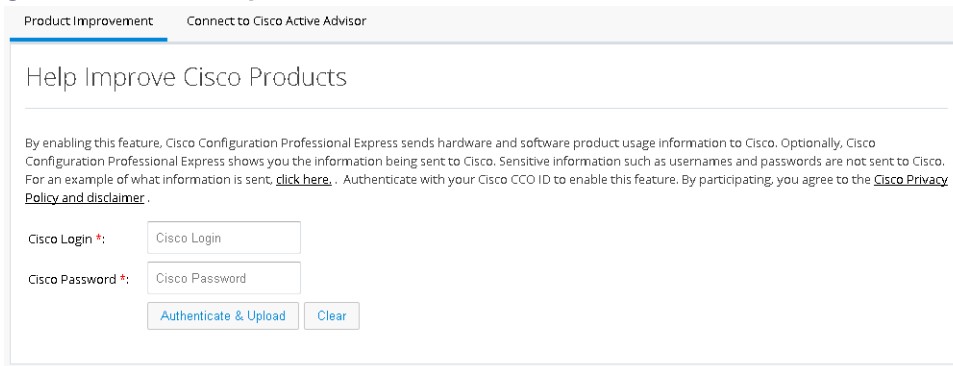
- [Uploading the Configuration, page 89](#)
- [Viewing the Device Details, page 90](#)

## Uploading the Configuration

To upload the router configuration, perform these steps:

1. Click **Cisco Active Advisor** to open Cisco Active Advisor page.
2. Enter your CEC username and password in the Product Improvement tab

**Figure 131 Product Improvement tab**



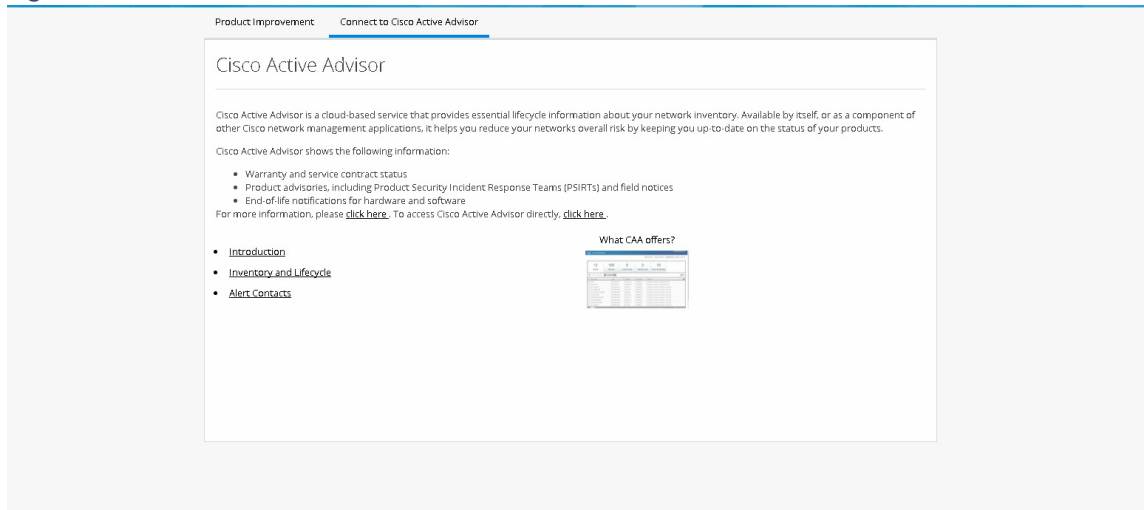
The screenshot shows a web interface for the 'Product Improvement' tab. At the top, there are two tabs: 'Product Improvement' (selected) and 'Connect to Cisco Active Advisor'. Below the tabs is a header 'Help Improve Cisco Products'. A paragraph of text explains that enabling this feature sends hardware and software product usage information to Cisco, and that sensitive information like usernames and passwords is not sent. It includes a link to 'click here' for an example and another link to 'Cisco Privacy Policy and disclaimer'. Below the text are two input fields: 'Cisco Login \*:' and 'Cisco Password \*:'. The 'Cisco Login' field contains the text 'Cisco Login' and the 'Cisco Password' field contains 'Cisco Password'. At the bottom of the form are two buttons: 'Authenticate & Upload' and 'Clear'.

3. Click **Authenticate & Upload**.

## Viewing the Device Details

1. Click **Connect to Cisco Active Advisor** tab,
2. Click **Inventory and Lifecycle** to view the device details.

**Figure 132 Connect to Cisco Active Advisor tab**



## Upgrade CCP Express

To upgrade the CCP Express, follow these steps:

1. Click on **Options** menu on the page header.
2. Select Upgrade option. The Upgrade CCP Express page is displayed. (Figure 133)

**Figure 133 Upgrade CCP Express**

## Upgrade CCP Express

### Download From CCO

- Clicking on below button will launch CCO page from which you can download the zip.  
[Click here to download latest CCP Express Version](#)
- If you do not have CCO login account, please register in the CCO page.
- If you already have a zip/Admin-tar available in your PC, then please skip this step.

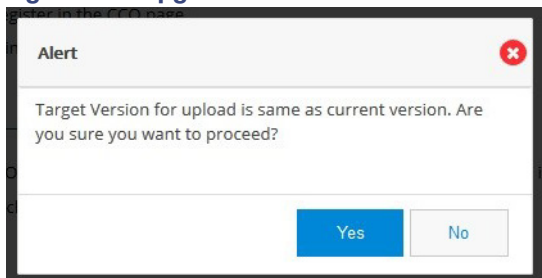
### Upload and Install

- Please extract the downloaded zip file from CCO on your PC. If you already have the extracted Admin-tar available in your PC, then
- Click on Select CCP Express Tar file button and choose the tar file from the folder where it is placed/extracted.

ccpexpressAdmin\_3\_5\_1\_en.tar is selected.

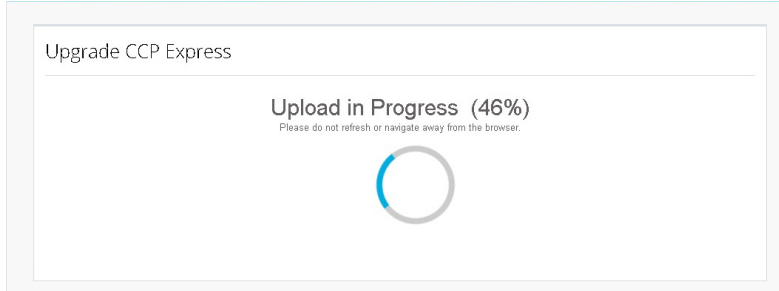
Delete tar from router after installation

3. Click on the link to download the latest CCP express version. It navigates to CCO page. If you do not have a CCO login, register it.
4. If you already have a zip/Admin tar in your PC, skip the above step.
5. Click on CCP Express Tar File and choose the tar file from the folder where it is extracted.
6. After selecting the tar, click on **Upgrade CCP Express** and it asks for confirmation as shown. (Figure 134)

**Figure 134 Upgrade Confirmation**

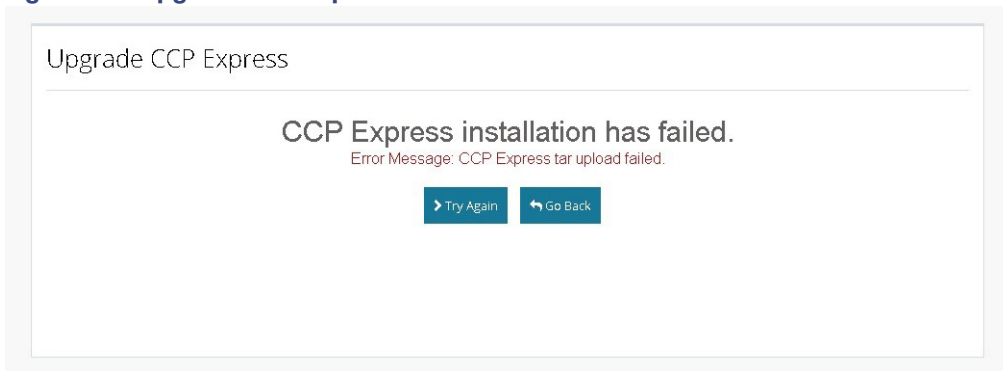
7. Click **YES** to confirm Upgrade CCP express. It takes time to upgrade and below page will be displayed. (Figure 135)

**Figure 135 Upgrade CCP Express**



8. If upgrade fails, click **TRY AGAIN**. (Figure 136)

**Figure 136 Upgrade CCP Express**



9. After upgrading the CCP Express, it automatically takes you to the Landing Page with updated version. If you are using the UI prior to Release 3.5, you see the Landing Page in [Figure 137](#).

More Options - Top Menu Small Icons

Figure 137 Upgrade CCP Express

The figure displays a grid of 12 icons, each with a title and a brief description of its function:

- Basic Settings**: Configure the device hostname, domain name, Timezone, NTP, DNS server, IPv4 DHCP Pools and DNS Proxy.
- Interface and Connections**: Configure all device interfaces including LAN and WAN interfaces. Setup DSL, Ethernet, 3G or 4G WAN links or create VLANs and Loopback interfaces to configure interface attributes.
- Quick Setup Wizard**: The wizard helps to bring up your WAN/LAN connectivity quickly. It is strongly recommended to use Quick Setup Wizard only when the device is factory fresh.
- Dashboard**: View basic diagnostic information like Version, Interfaces, Software details, Flash/CPU utilization stats etc. Security and Application Visibility & Control info is listed based on device support.
- Identity**: Configure new Users on the device with required privilege levels, create Groups and move users to groups. Configure Authentication parameters.
- Static Routing**: Configure IPv4 and IPv6 static routes.
- Any CLI to the box**: Configure IOS CLI commands. Execute Show commands and copy/download the output.
- Troubleshoot**: Troubleshoot reachability to other IPv4 or IPv6 destinations using Ping or Trace Route utilities.
- Security**: Comprehensive solution that includes key components of threat defense with Firewalling, Intrusion Prevention, VPN, and Content Security functions.
- Wi-Fi**: Configure the WLAN access point to create new SSIDs and authentication keys.
- IOX**: IOX configuration via external Device Manager.
- ACL**: Basic traffic filtering and controlling the access to IP network is possible using Access Control Lists.

If you are using the UI in Release 3.5 or greater, you see the Landing Page in Figure 138.

Figure 138 New UI in Release 3.5

The screenshot shows the Router landing page with a sidebar menu and several monitoring widgets:

- Sidebar Menu**: Dashboard, Configuration, Administration, Troubleshoot.
- CPU Utilization**: Gauge showing 10% Used.
- WAN Interface**: Shows Primary (GigabitEthernet0 is up, IP Address: 10.104.105.166) and Backup (Cellular0/0 is down, IP Address: network).
- Flash Memory**: Donut chart showing 50% Free.
- System Memory**: Donut chart showing 24.90% Free.
- Device Details**: Hostname: mylr800, System Time: 16 : 38 : 26 GMT, IOS Version: 15.7(3)M, System Uptime: 1 week, 1 hour, 34 minutes.
- Interfaces**: Horizontal bar chart showing status for GigabitEthernet (2 Up, 4 Down), Cellular (1 Up, 3 Down), and Loopback (0 Up, 0 Down).

## Upgrade IOS

Upgrade IOS when you are notified of a new IOS release.

1. Click on Options icon on the page header.
2. Select IOS Update option. The IOS Update page is displayed as shown in [Figure 139](#).

**Figure 139 IOS Update**

IOS Update

Select from:  Router (flash:)  Desktop

↗ Select the IOS image to be used for router

File Name	Disk	Actions
<input checked="" type="radio"/> c800m-universalk9-mz.SPA.155-3.M.bin	sdflash:	
<input checked="" type="radio"/> c800m-universalk9-mz.SPA.156-3.M0a.bin	sdflash:	

Boot List ⓘ

Move to top  Clear list

[Update IOS](#)

3. Upload the image to the device by selecting Desktop.

**Figure 140 IOS Update Page**

IOS Update

---

Select from:  Router (flash:)  Desktop

**Download From CCO**

- Clicking on below button will launch CCO page from which you can download the zip.  
[Click here to download IOS image](#)
- If you do not have CCO login account, please register in the CCO page.
- If you already have an IOS file available in your PC, then please skip this step.

**Upload**

- Please extract the downloaded zip file from CCO on your PC. If you already have the extracted IOS available in your PC, then please skip this step.
- Click on Select IOS button and choose the ios file from the folder where it is placed/extracted.

Select only a valid IOS image file for your device.(ir800).After the upload, you will be redirected to an updated list of IOS files on router flash,from where you can select any IOS file and proceed with the update.

- If you do not have the latest IOS image, click the link in IOS Update window. You are taken to the IOS Download page with the latest images.
- Go back to the IOS Update window, and follow the instructions in the Upload section.
- From the Router (Flash) window, select the IOS image and click Update IOS. The following message appears:

Alert ✖

Are you sure you want to update your device IOS?

- Click **Yes**.

## Using CCP Express in Restricted Access Mode (Monitor User)

The Monitor User feature addition allows a user of privilege 14 to login to CCP Express with restricted access. The only features available to this user would be Dashboard (Router & Interfaces), any CLI, and Troubleshoot.

**Note:** This feature is available in Cisco CCP Express Release 3.5.1 and greater releases.

### Prerequisites

- IOS version 15.7(3)M2 or greater

## Using CCP Express in Restricted Access Mode (Monitor User)

- Privilege 14 (already installed)

To access CCP Express as a monitor user:

1. Clear cache from the browser and then relaunch it.
2. Access CCP Express by using the IP address or the friendly URL.
3. Enter your login credentials, and enter the Privilege 14 level user's credentials. This is the Monitor User.

The splash screen displays after you enter the credentials.

**Figure 141 Monitor User Splash Screen**



Based on the Admin User's preference for the UI, the Monitor User is be presented with Old UI (Figure 142) or New UI (Figure 143).

**Figure 142 Old UI Landing Page for Monitor User**

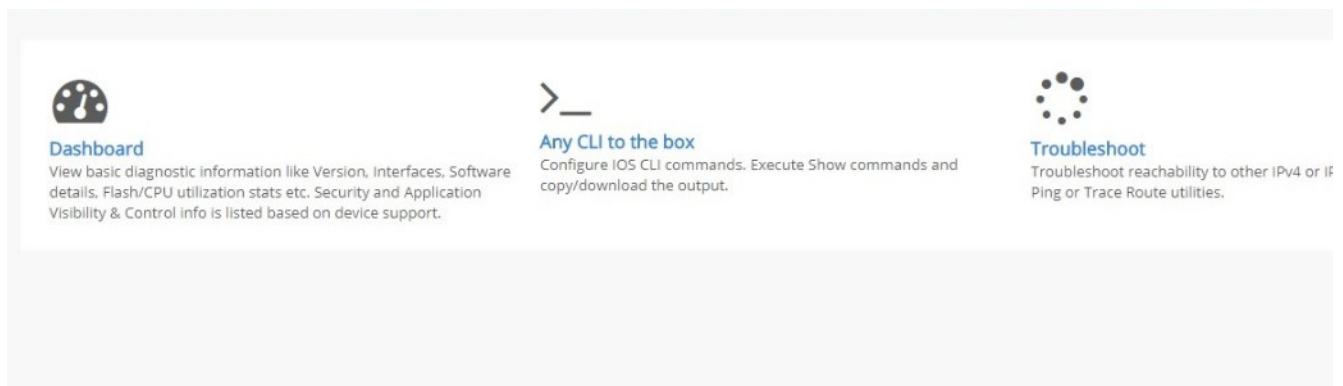
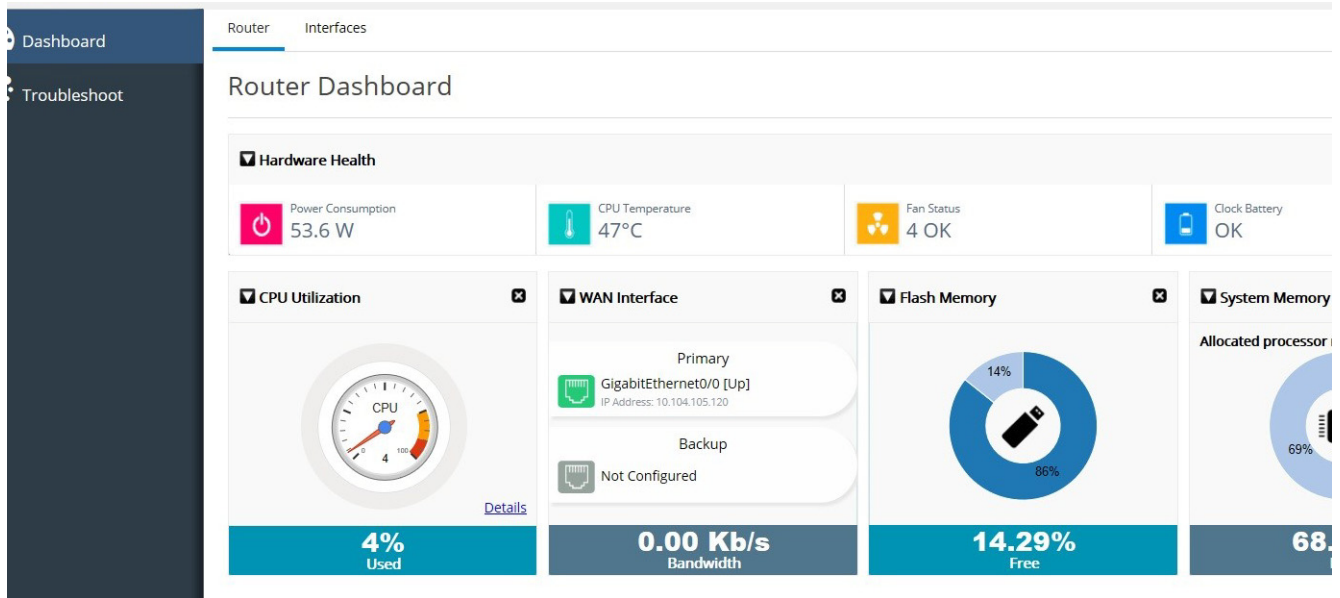


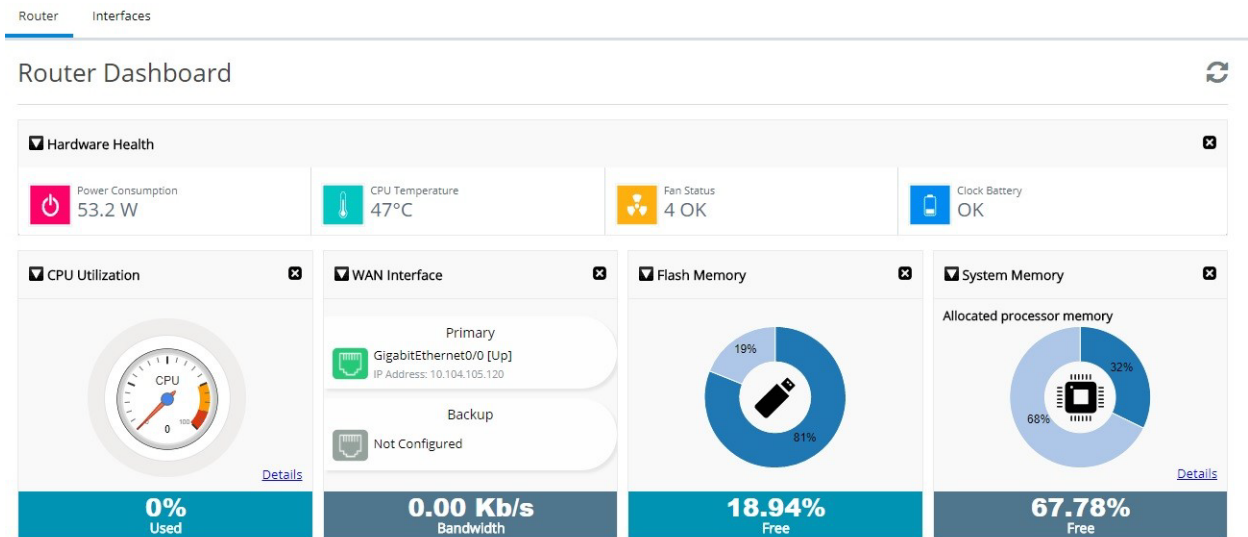


Figure 143 New UI Landing Page for Monitor User



Under Dashboard, Monitor User can access the Router Dashboard (Figure 144) and Interfaces Dashboard (Figure 145).

Figure 144 Router Dashboard for Monitor User



**Figure 145 Interfaces Dashboard for Monitor User**

Under the Troubleshoot Dashboard, the Monitor User can access the Ping and Traceroute (Figure 146) and Test WAN Connection (Figure 147).

**Note:** Specifying the source is not available for the Monitor User.

**Figure 146 Ping and Traceroute for Monitor User**

Ping and Traceroute

*\*Note: Destination will accept proper IPv4 address/IPv6 address/Hostname.*

Destination:



Figure 147 Test WAN Connection for Monitor User

Ping and Traceroute    Test WAN Connection

---

Test WAN Connection

---

 ↔ 

Pinging www.cisco.com...

- ✓ IP Address configured - 10.104.105.120
- ✓ DNS configured - 8.8.8.8
- 🔄 Pinging a Public Domain from your router

[Try Again](#)

```
DNS view default parameters:  
Logging is off  
DNS Resolver settings:  
Domain lookup is enabled  
Default domain name: te  
Domain search list:  
Lookup timeout: 3 seconds  
Lookup retries: 2  
Domain name-servers:  
8.8.8.8  
DNS Server settings:  
Forwarding of queries is enabled  
Forwarder timeout: 3 seconds  
Forwarder retries: 2  
Forwarder addresses:  
router#ping www.cisco.com
```

Monitor User can also access the Syslog Views.

Figure 148 Syslog View

Ping and Traceroute    Test WAN Connection    Logs

---

Syslog

---

Number of previous lines to be displayed from last  [Show Logs](#) [Clear Logs](#)

---

**Figure 149 Syslog - Show Logs**

Ping and Traceroute   Test WAN Connection   **Logs**

## Syslog

Number of previous lines to be displayed from last:

log

Syslog logging: enabled (0 messages dropped, 7 messages rate-limited, 0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: level debugging, 177 messages logged, xml disabled, filtering disabled

Monitor logging: level debugging, 0 messages logged, xml disabled, filtering disabled

Buffer logging: level warnings, 55 messages logged, xml disabled, filtering disabled

Exception Logging: size (8192 bytes)

Count and timestamp logging messages: disabled

Persistent logging: disabled

Trap logging: level informational, 147 message lines logged

Logging to 66.66.66.66 (udp port 514, audit disabled)

Monitor User can issue commands using the Any CLI feature. Monitor User has privilege 14 which is allowed only to execute a subset of the show commands available for privilege 15 users. Monitor User has only the Execute option and not the Config option as compared to the Admin User.

Monitor User can view the system information (Figure 150) by clicking on the info button on top right side.

**Figure 150 System Information for Monitor User**

Parameter	Value
Hostname:	Router
IOS Version:	15.7(3)M2
System Uptime:	Router uptime is 1 day, 2 hours, 54 minutes
System Time:	12:15:57.073 GMT Wed Mar 21 2018
Device Type:	CISCO2921/K9
Reason for Last Reload:	Reload Command
CCP Express Version	3.5.1
Built At	2018-03-19 02:13:01
User	Monitor User

## Monitor User Management (for Admin User)

A user logged into CCP Express with privilege 15 level access is an Admin User who is authorized to use all features and operations within CCP Express. Since Monitor User has lesser privilege and read-only access, Admin User is given the provision to manage the Monitor User from the Monitor View tab under Identity.

To manage Monitor Users:

1. Login as an Admin user, and navigate to Identity -> User.
2. If the IOS version is 15.7(3)M2 and greater and Monitor User is not enabled, you will see the Enable Monitor User button available (Figure 151).

**Figure 151 Enable Monitor Users**

The screenshot shows the 'Users' management interface. At the top, there are tabs for 'Authentication', 'Groups', and 'Users'. Below the tabs is the title 'User Management' and a search bar labeled 'Search User(s)'. On the right side, there are buttons for 'Enable Monitor User', 'Add', and 'Delete'. The main part of the page is a table with the following data:

	Username	Privilege Level	User Type	Parser View	Group	
<input type="checkbox"/>	jean	15	Admin User	NO	No Group	
<input type="checkbox"/>	ccp	15	Admin User	NO	No Group	
<input type="checkbox"/>	testuser	15	Admin User	NO	test	
<input type="checkbox"/>	priv7	7	No Access	NO	No Group	
<input type="checkbox"/>	priv14	14	No Access	NO	No Group	
<input type="checkbox"/>	test123	15	Admin User	NO	No Group	
<input type="checkbox"/>	p14user	14	No Access	NO	No Group	
<input type="checkbox"/>	monuser	14	No Access	NO	No Group	
<input type="checkbox"/>	ftp-user	1	No Access	NO	No Group	

A tooltip message is displayed over the 'test' user row, stating: 'Monitor User is not enabled. Click here to enable Monitor User feature on this device.'

3. Click the Enable Monitor User button, and the config required to support Monitor User gets pushed.

Whether Monitor User support was enabled manually by the Admin User or was configured on the device already, the data listed in User tab will list the type of user.

## Monitor User Management (for Admin User)

Figure 152 Users Tab

	Username	Privilege Level	User Type	Parser View	Group
<input type="checkbox"/>	jean	15	Admin User	NO	No Group
<input type="checkbox"/>	ccp	15	Admin User	NO	No Group
<input type="checkbox"/>	testuser	15	Admin User	NO	test
<input type="checkbox"/>	priv7	7	No Access	NO	No Group
<input type="checkbox"/>	priv14	14	Monitor User	NO	No Group
<input type="checkbox"/>	test123	15	Admin User	NO	No Group
<input type="checkbox"/>	p14user	14	Monitor User	NO	No Group
<input type="checkbox"/>	monuser	14	Monitor User	NO	No Group
<input type="checkbox"/>	ftp-user	1	No Access	NO	No Group

The Monitor View tab shows a list of Monitor Users as well as the commands pertaining to CCP Express which are available to the Monitor User.

Figure 153 Monitor View Tab

Authentication Groups Users **Monitor View**

### Monitor User Management

**Monitor Users** Search

monitoruser1 No Group

**Commands Enabled by Admin** Add Commands

**Commands Available by Default**

- show version
- show processes cpu
- show process memory
- show zone security
- show license feature
- show environment all

**System/Application defined Commands**

- dir
- show license udi
- show file systems
- show ip dns view
- show platform
- show logging

Admin User can enable new commands for the Monitor User using the Add Commands button. The commands are validated before those are enabled for monitor user.

## Friendly URL

Figure 154 Enable New Commands for Monitor User

Enable New Commands for Monitor User
✖

Command to be enabled for Monitor User \* :

Add
Cancel

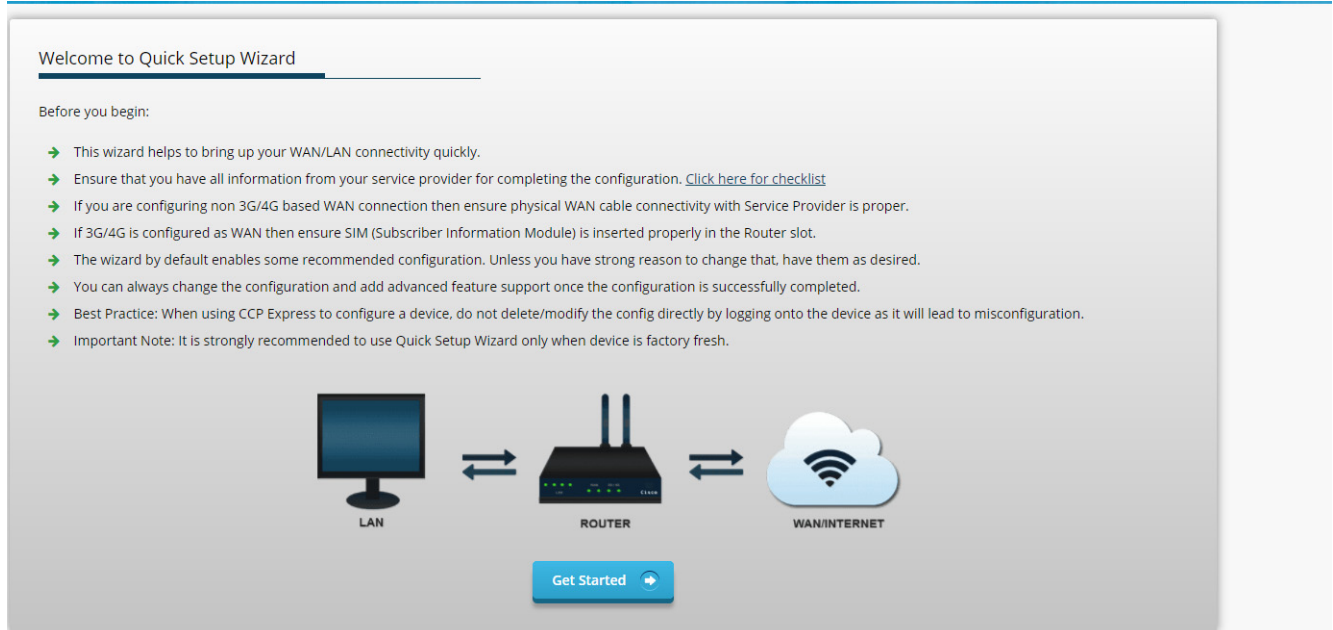
## Friendly URL

To Access CCP Express using a friendly URL:

1. Connect the device directly to the laptop or desktop.
2. Open a browser, and enter “myir800.com”.

You are directed to the CCP Express application.

Figure 155 CCP Express UI



## Related Documentation

IR 800 Series documentation:

<http://www.cisco.com/c/en/us/support/routers/800-series-industrial-routers/tsd-products-support-series-home.html>

Release Notes for Cisco Configuration Professional Express 3.5.x:

<https://www.cisco.com/c/en/us/support/routers/800-series-industrial-routers/products-release-notes-list.html>

Cisco Configuration Professional Express Quick Start Guide:

<https://www.cisco.com/c/en/us/support/routers/800-series-industrial-routers/products-installation-guides-list.html>

Cisco Configuration Professional Express 3.5 Administration Guide:

<https://www.cisco.com/c/en/us/support/routers/800-series-industrial-routers/products-installation-and-configuration-guides-list.html>

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: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). 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. (1110R)

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.

© 2018 Cisco Systems, Inc. All rights reserved.