



Set Up Your Cisco Router

Home > Work With My Routers > Cisco Routers > Set Up Your Cisco Router

Step 5: Configure Wireless Security on an Integrated Service Router

- Step 1: [SMB Support Assistant Site Survey](#)
- Step 2: [Set Up Your 800 or SB 100 Router Hardware](#)
[Set Up Your 1700 Series Router Hardware](#)
[Set Up Your 1800 Series Router Hardware](#)
[Set Up Your 2600 Series Router Hardware](#)
[Set Up Your 2800 Series Router Hardware](#)
[Set Up Your 3800 Series Router Hardware](#)
- Step 3: [Download and Install Security Device Manager](#)
- Step 4: [Configure Your Router with Security Device Manager](#)
- Step 5: Configure Wireless Security on an Integrated Services Router (ISR Only)**
[Introduction](#)
[Requirements](#)
[Overview](#)
[Configure Security Settings](#)
[Access the Router](#)
[Local RADIUS Server](#)
[Express Security](#)
[Encryption Manager](#)
[Next Step](#)
[Troubleshoot the Procedure](#)
[Related Information](#)
- Step 6: [Add or Remove a Wireless User on an Integrated Services Router \(ISR Only\)](#)
- Step 7: [Set Up an ADSL Internet Connection](#)
[Set Up an Ethernet Internet Connection](#)
[Set Up an ISDN Internet Connection](#)
[Set Up a T1, E1, or Serial Internet Connection](#)
- Step 8: [Set Up Internet Security on a Cisco Router](#)

Service Requests

- [Open a service request](#)
- [Update a service request](#)

Feedback

Please rate this document.

++ + +/- - --

This document solved my problem.

Yes No Just Browsing

Suggestions for improvement:

Download PDF

- [Step 5: Configure Wireless Security on an Integrated Service Router](#)
- [Set Up Your Cisco Router](#)

If Cisco may contact you for more details or for future feedback opportunities, please enter your contact information:

Full
Name:

Email:

Introduction

This document describes how to configure wireless security on a Cisco Integrated Services Router (ISR).

[Back to Top](#)

Requirements

- You must have completed the steps in [Configure Your Router with Security Device Manager](#)

To perform the steps described in this document, you need to have these items:

- Completed ISR Router Worksheet as instructed in the [Site Survey](#)
- An Wireless ISR that is powered on and connected to a PC with a [straight-through Ethernet cable](#)
- Cisco IOS® Software Release 12.2 installed on the ISR

[Back to Top](#)

Overview

Any wireless networking device within range of an AP can receive its radio transmissions. Therefore, you need to configure security settings to prevent unauthorized access to your network. This document explains how to configure security settings to ensure that unauthorized users cannot connect to your AP.

Cisco recommends LEAP for security, an implementation of the EAP/802.1x protocol.

[Back to Top](#)

Configure Security Settings

Follow these steps to configure security on the ISR:

Access the Router

Follow these steps to access the ISR:

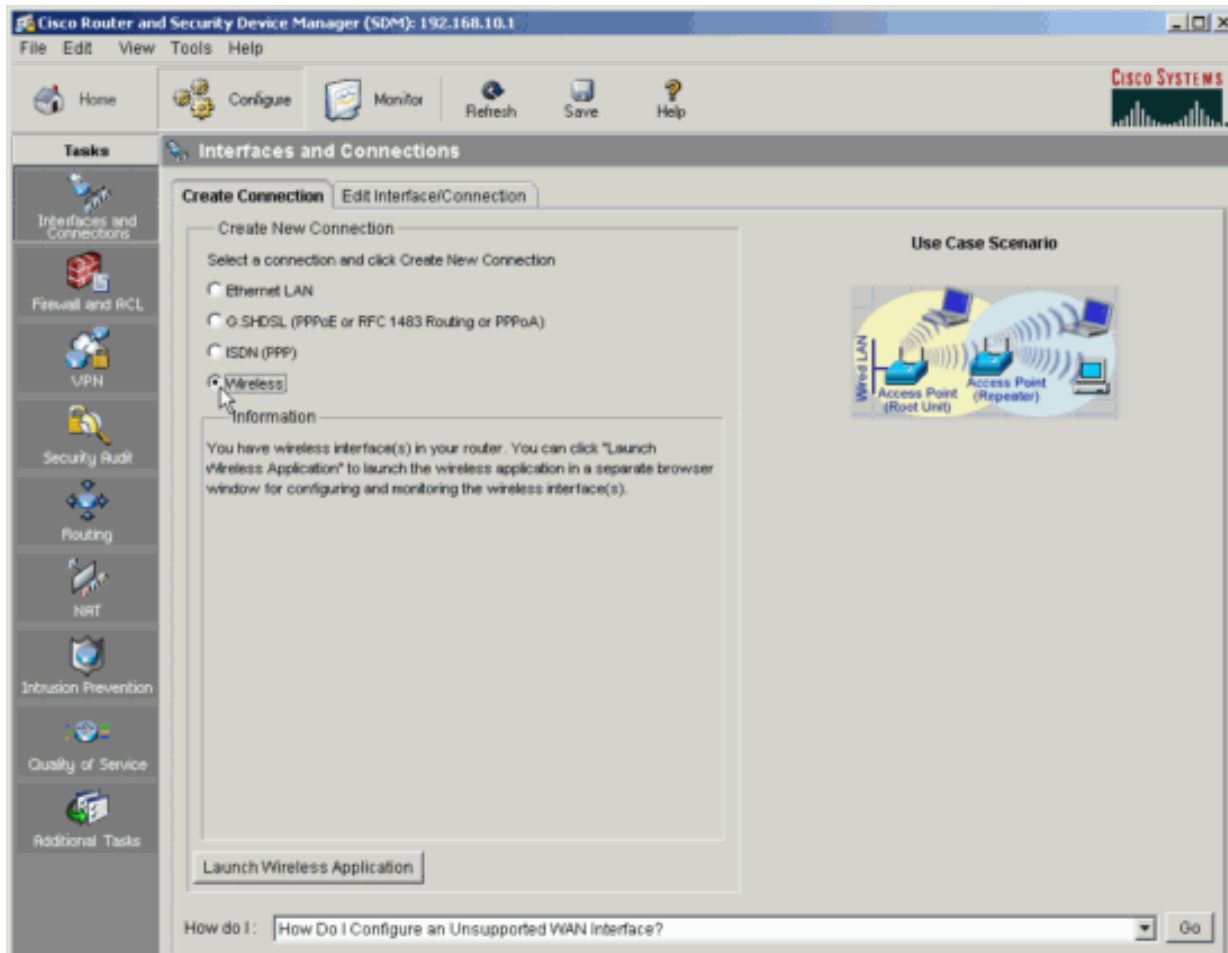
1. Open your browser and type **http://isr-ip-address** and press **Enter**. For isr-ip-address, use the IP address in field W10 of the ISR Router Worksheet.
2. Enter the ISR username and password that you entered in fields B10 and B11 of the Integrated Services Router worksheet and press **Enter**.

Note: If you cannot log into the router, see [Troubleshoot the Procedure](#).

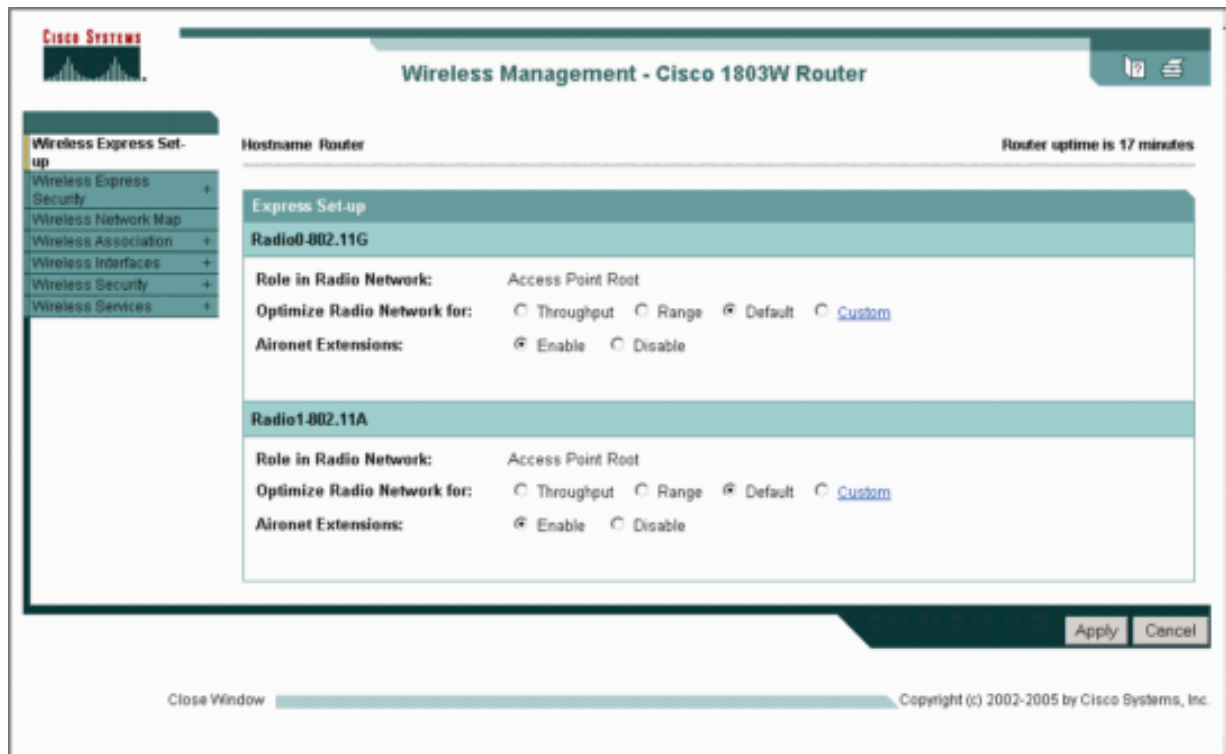
3. Click **Configure**.



4. In the **Create Connection** tab, select **Wireless** and click **Launch Wireless Application**.



5. The wireless application launches in a separate window.



Local RADIUS Server

Follow these steps to enable a local RADIUS server:

1. Click **Wireless Security > Local Radius Server**.



2. Click the **General Set-Up** tab.
3. Scroll to the **User Groups** area of the **Security: Local RADIUS Server** screen.

STATISTICS GENERAL SET-UP

Hostname Router

Security: Local RADIUS Server - General Set-up

Network Access Servers (AAA Clients)

Current Network Access Servers

< NEW >

Network Access Server: (IP Address)

Shared Secret:

Delete

Apply Cancel

Individual Users

Current Users

< NEW >

Username:

Password: Text NT Hash

Confirm Password:

Group Name:

MAC Authentication Only

Delete

Apply Cancel

User Groups

Current User Groups

< NEW >

Group Name:

Session Timeout (optional): (1-4294967295 sec)

Failed Authentications before Lockout (optional): (1-4294967295)

Lockout (optional): Infrite Interval (1-4294967295 sec)

VLAN ID (optional):

SSID (optional): Add

Delete

Apply Cancel

4. Enter these values under **User Groups**:

Field	Value
Group Name	Default

Session Timeout	(Leave this field blank)
Failed Authentication before Lockout	3
Lockout	Interval, 600
VLAN ID	20
SSID	(Enter the Wireless Network Name from field W14 of the ISR Router Worksheet)

Click **Add** to add the SSID number.

User Groups

Current User Groups

< NEW >

Delete

Group Name:

Session Timeout (optional): (1-4294967295 sec)

Failed Authentications before Lockout (optional): (1-4294967295)

Lockout (optional):

Infinite

Interval (1-4294967295 sec)

VLAN ID (optional):

SSID (optional): Add

Delete

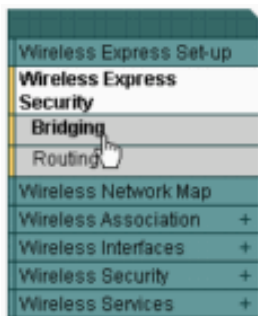
Apply Cancel

5. Click **Apply** to save the changes.

Express Security

Follow these steps to set up Express Security:

1. Click **Wireless Express Security > Bridging**.



2. Enter these values in the **Express Security Bridging** screen:

Field	Value
SSID	(Enter the Wireless Network Name from field W14 of the ISR Router Worksheet)
VLAN	Enable VLAN ID, 20 Check Native VLAN
Bridge	1
Security	EAP Authentication
RADIUS Server	Enter the router IP address from field W10 of the ISR Router Worksheet.
RADIUS Server Secret	Enter the RADIUS Password from field W15 of the ISR Router Worksheet.

Express Security Bridging

SSID Configuration

1. **SSID** [Broadcast SSID in Beacon](#)

2. **VLAN** No VLAN Enable VLAN ID: (1-4094) Native VLAN

3. **Bridge** Bridge Group Number: (1-255)

4. **Security** [No Security](#)

[Static WEP Key](#)

[EAP Authentication](#)

RADIUS Server: (Hostname or IP Address)

RADIUS Server Secret:

[WPA](#)

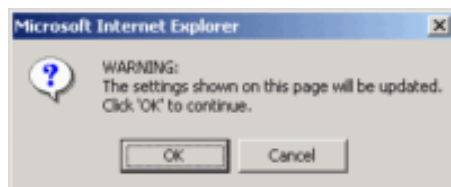
RADIUS Server: (Hostname or IP Address)

RADIUS Server Secret:

SSID Table

SSID	VLAN	Bridge Grp. Number	Encryption	Authentication	Key Management	Native VLAN	Broadcast SSID

3. Click **Apply** to save the changes. If a warning message appears to indicate that you are about to update your settings, click **OK** to continue.



Encryption Manager

Follow these steps to complete the Encryption Manager:

1. Click **Wireless Security > Encryption Manager**.



2. In the **Encryption Modes** area, choose **WEP Encryption** and **Mandatory**.

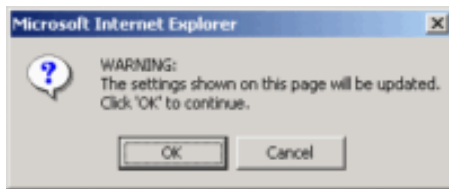
 A screenshot of the configuration page for RADIO0-802.11G. The page shows the following settings:

- Hostname: Router
- Security: Encryption Manager Radio0-802.11G
- Set Encryption Mode and Keys for VLAN: 20 (with a "Define VLANs" link)
- Encryption Modes:
 - None
 - WEP Encryption (with a dropdown menu set to "Mandatory")
 - Cipher (with a dropdown menu set to "WEP 128 bit")
- Global Properties:
 - Broadcast Key Rotation Interval:
 - Disable Rotation
 - Enable Rotation with Interval: DISABLED (10-10000000 sec)
 - WPA Group Key Update:
 - Enable Group Key Update On Membership Termination
 - Enable Group Key Update On Member's Capability Change

 At the bottom right, there are "Apply" and "Cancel" buttons.

3. Click **Apply** to save the changes. When a warning message appears to indicate that you are about to

update your settings, click **OK** to continue.



[Back to Top](#)

Next Step

You have completed basic configuration of the wireless module of your router.

To add additional users to your wireless network, refer to [Add or Remove a Wireless User](#).

If you want to configure an Internet connection, refer to the appropriate document for your connection. If you are not sure what connection type you have, refer to your Internet Worksheet.

- [Set Up an Ethernet Connection](#)
- [Set Up an ADSL Connection](#)
- [Set up a T1/E1/Serial Connection](#)
- [Set up an ISDN Connection](#)

Note: If your router is already connected to the Internet, refer to [Set Up Internet Security on a Cisco Router](#).

[Back to Top](#)

Troubleshoot the Procedure

This section provides information about common problems that you may encounter. If this information does not solve your problem, contact the [SMB Technical Assistance Center \(SMB TAC\)](#) for assistance.

Problem	Cause(s) and Suggested Solution(s)

I cannot access the router.

Refer to [Configure Your Router with Security Device Manager](#).

[Back to Top](#)

Related Information

- [Configure Your Router with Security Device Manager](#)
- [Add or Remove a Wireless User](#)
- [Password Security](#)
- [Configure an IP Address on Your PC](#)