Configure Guest Access Instance Table on the WAP125 Access Point

Objective

The Guest Access feature of the WAP125 access point provides wireless connectivity to temporary wireless clients within the range of the device. It works by having the access point broadcast two different Service Set Identifiers (SSIDs): one for the main network, and the other for the guest network. Guests are then redirected to a Captive Portal where they are required to enter their credentials. In effect, this would keep the main network secure while still giving guests access to the Internet.

The settings of the Captive Portal such as session timeout and redirect Uniform Resource Locator (URL) is configured at the Guest Access Instance Table of the web-based utility of the WAP125. The Guest Access feature has been particularly useful in hotel and office lobbies, restaurants, and malls.

This article aims to show you how to configure the Guest Access Instance Table of the WAP125 access point. It assumes that the settings for Web Portal Locale Table and the Guest Group Table are already configured. For instructions in configuring both of these settings, click here.

Applicable Devices

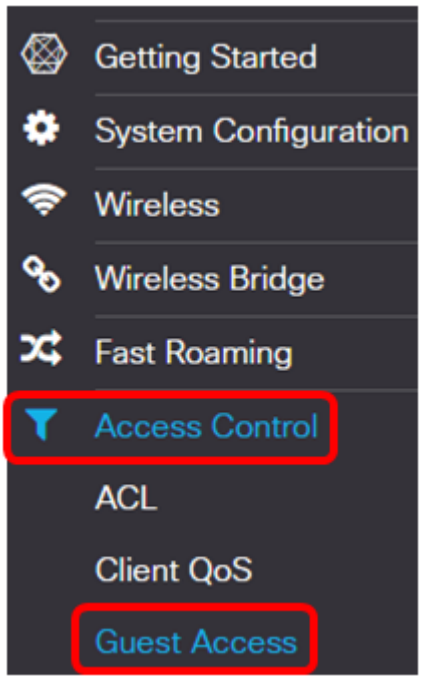
- WAP125

Software Version

- 1.0.0.4—WAP581
- 1.0.0.5— WAP125

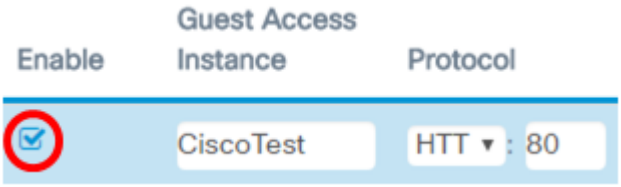
Configure Guest Access Instance Table

Step 1. Log in to the web-based utility of the WAP125 and choose **Access Control > Guest Access**.

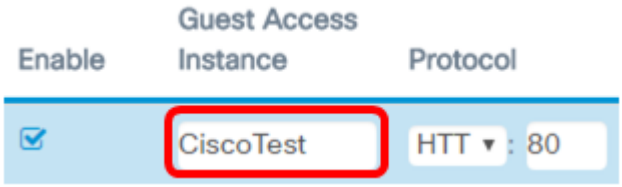


Note: The images on this article are taken from the WAP125. Menu options may vary depending on the model of your device.

Step 2. Verify that the Guest Access Instance **Enable** check box is checked to ensure that Guest Access is active.



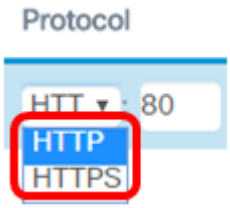
Step 3. Enter a name for the instance in the *Guest Access Instance* field. This can be up to 32 alphanumeric characters.



Note: In this example, CiscoTest is entered.

Step 4. Choose a protocol for the guest access instance. The options are:

- HTTP — This option is also known as HyperText Transfer Protocol (HTTP). It does not provide encryption during verification of the requested webpage.
- HTTPS — This option is also known as HyperText Transfer Protocol Secure (HTTPS). This means that all communications between the computer and the website it is contacting are encrypted.



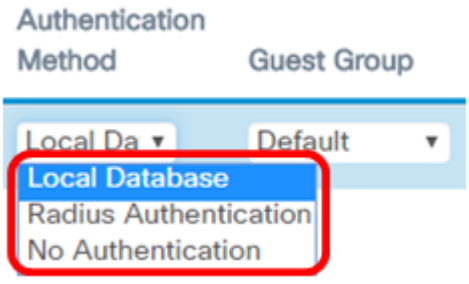
Note: In this example, HTTP is chosen.

Step 5. Enter a port number beside the Protocol field. The port number helps identify the protocol when it reaches a server.

Note: In this example, 80 is entered.

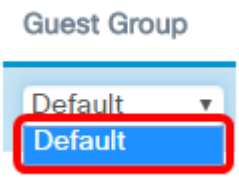
Step 6. Choose an authentication method from the Authentication Method drop-down list. This will be used by the access point when the clients authenticate through the Captive Portal. The options are:

- Local Database — This option lets the WAP device verify the credentials of the user from a file that is stored locally. If this option is chosen, finish to Step 7 to Step 10 and then proceed to configure the Guest Group Table.
- RADIUS Authentication — This option lets the access point verify the users through a Remote Authentication Dial-In User Service (RADIUS) server. If this option is chosen, finish to Step 7 to Step 10 and then proceed to configure RADIUS Authentication.
- No Authentication — This option disables authentication and allows wireless clients to connect to the guest network without entering their credentials. If this option is chosen, skip to Step 11.



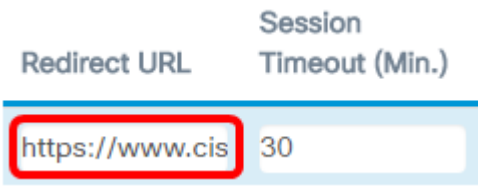
Note: In this example, Local Database is chosen.

Step 7. Choose a group from the Guest Group drop-down list.



Note: In this example, Default is automatically chosen.

Step 8. Enter the address to be redirected after entering the credentials in the *Redirect URL* field.

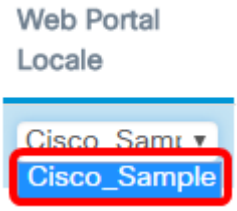


Note: The address should start with HTTP or HTTPS. In this example, https://www.cisco.com is entered.

Step 9. Enter the number of minutes before a session times out in the *Session Timeout (Min.)* field.

Note: In this example, 30 is entered.

Step 10. Choose a web portal profile from the Web Portal Locale drop-down list.



Note: In this example, Cisco_Sample is chosen automatically. For instructions on how to configure the Web Portal Locale, click here.

The Guest Access Instance Table should now be configured.

Configure Guest Group Table

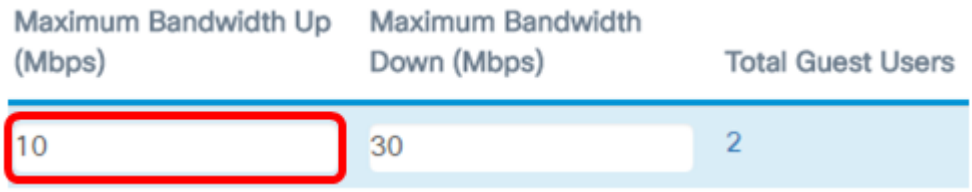
Step 7. Enter a name for the guest group in the *Guest Group Name* field. The Guest Group Name can be up to 32 characters long.

Note: In this example, CiscoGuests is entered.

Step 8. Enter the number of minutes before the prompt times out in the *Idle Timeout (Min.)* field.

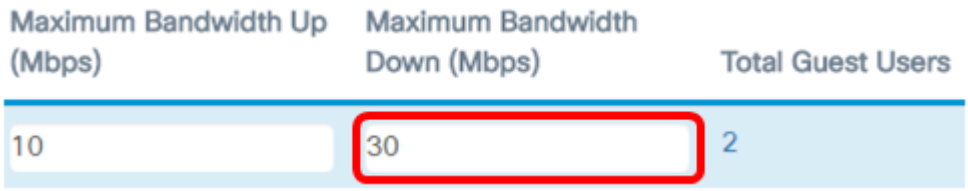
Note: In this example, 5 is entered.

Step 9. Enter the maximum upload speed in the *Maximum Bandwidth Up (Mbps)* field. This will be the maximum bandwidth, in Mbps, that a wireless client can send when using the Captive Portal. The Maximum Bandwidth can be from 0 to 300, where 0 is the default value.



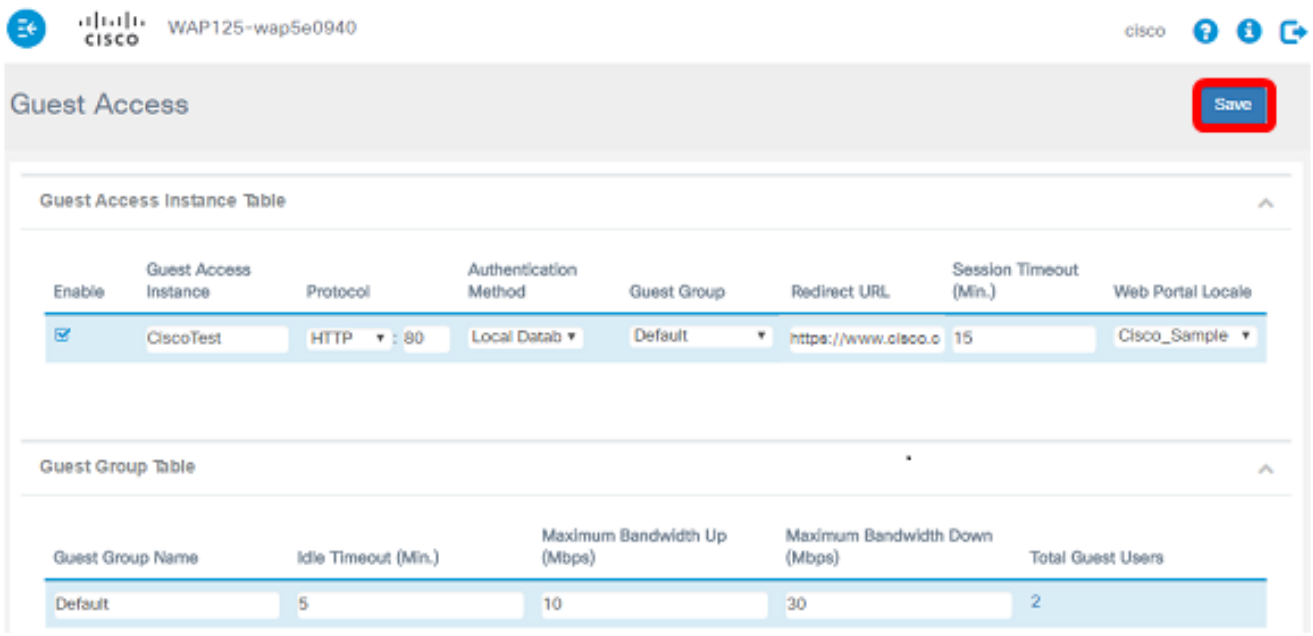
Note: In this example, 10 is entered.

Step 10. Enter the maximum download speed in the *Maximum Bandwidth Down (Mbps)* field. This will be the maximum bandwidth, in Mbps, that a wireless client can receive when using the Captive Portal. The Maximum Bandwidth can be from 0 to 300, where 0 is the default value.



Note: In this example, 30 is entered.

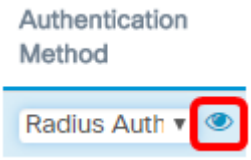
Step 11. Click **Save**.



The Guest Access Instance Table should now be configured with Local Database Authentication.

RADIUS Authentication

Step 1. Click the View button.

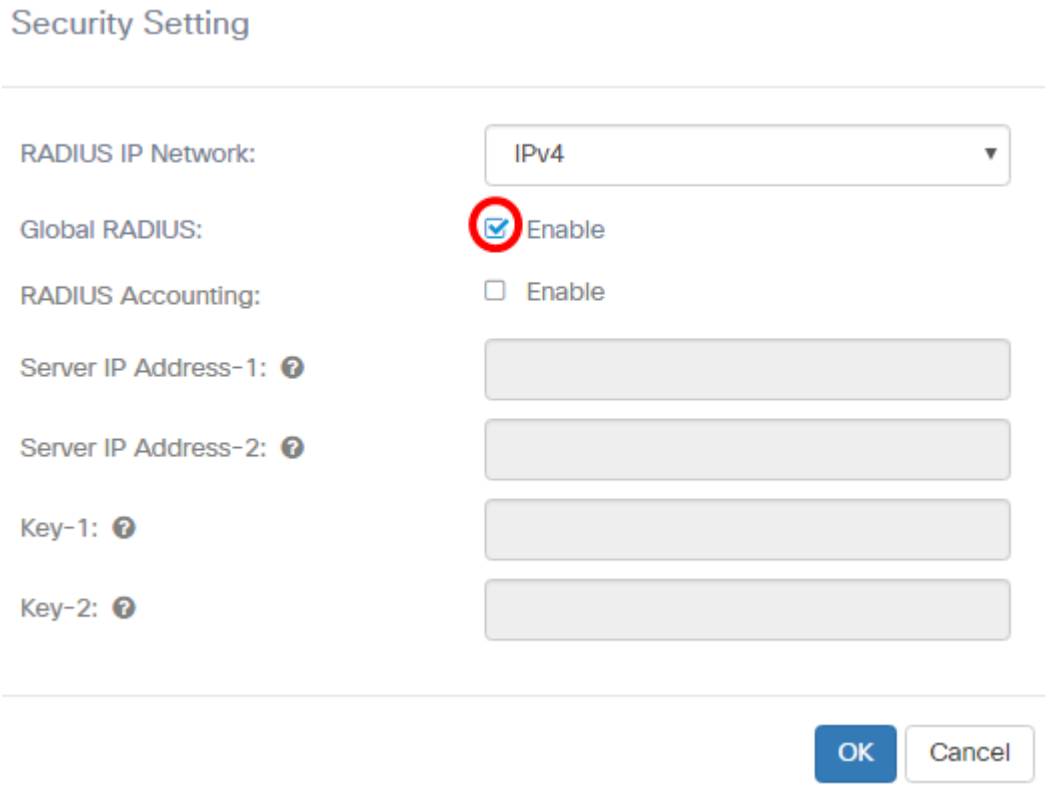


Step 2. In the Security Setting pop-up window, choose the radius IP network from the RADIUS IP Network drop-down list. The options are:

- IPv4 — This option is the most commonly used form of IP addressing on a network. It uses a 32-bit format to identify hosts on a network.
- IPv6 — This option is the next-generation IP address standard intended to replace the IPv4 format. IPv6 solves the address scarcity problem with the use of a 128-bit addressing system instead of the 32-bit used in IPv4.

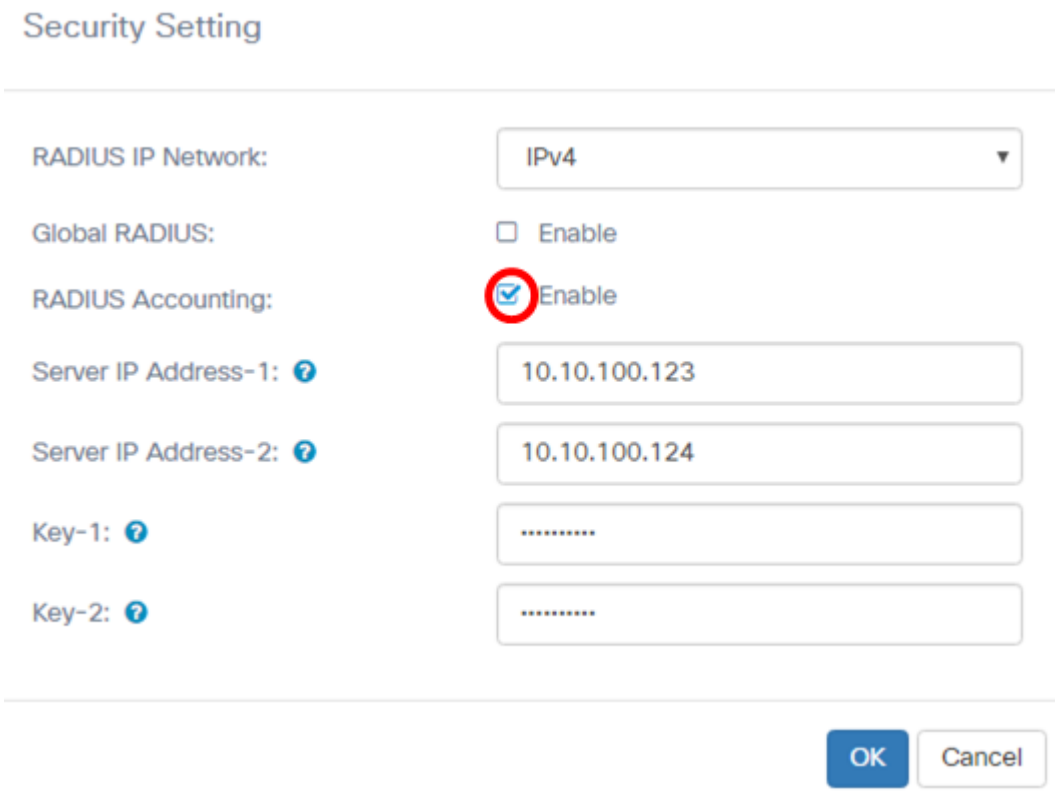
Note: In this example, IPv4 is chosen.

Step 3. (Optional) Check the Global RADIUS **Enable** check box to let the Captive Portal use a different set of RADIUS servers.

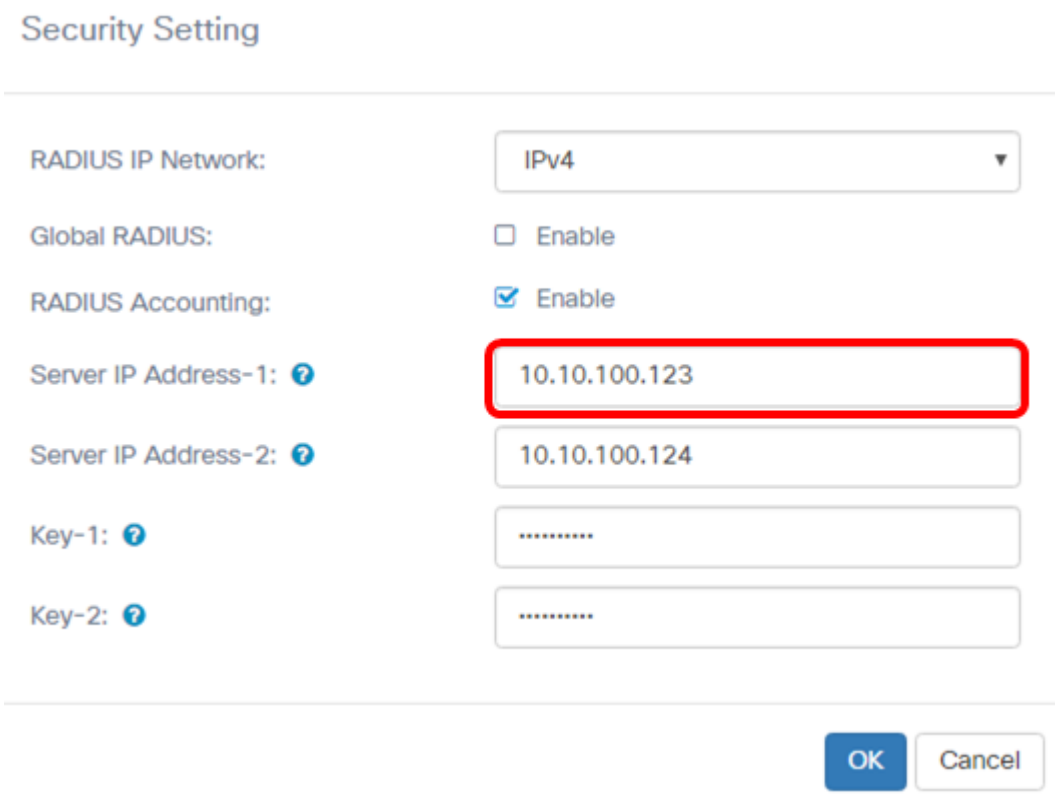


Note: When enabled, no other configuration for the Security Setting area needs to be configured. Proceed to Step 9. In this example, Global RADIUS is enabled.

Step 4. (Optional) Check the RADIUS Accounting **Enable** check box to let the access point track and measure the resources that a particular user has consumed, such as system time and the amount of data transmitted and received.

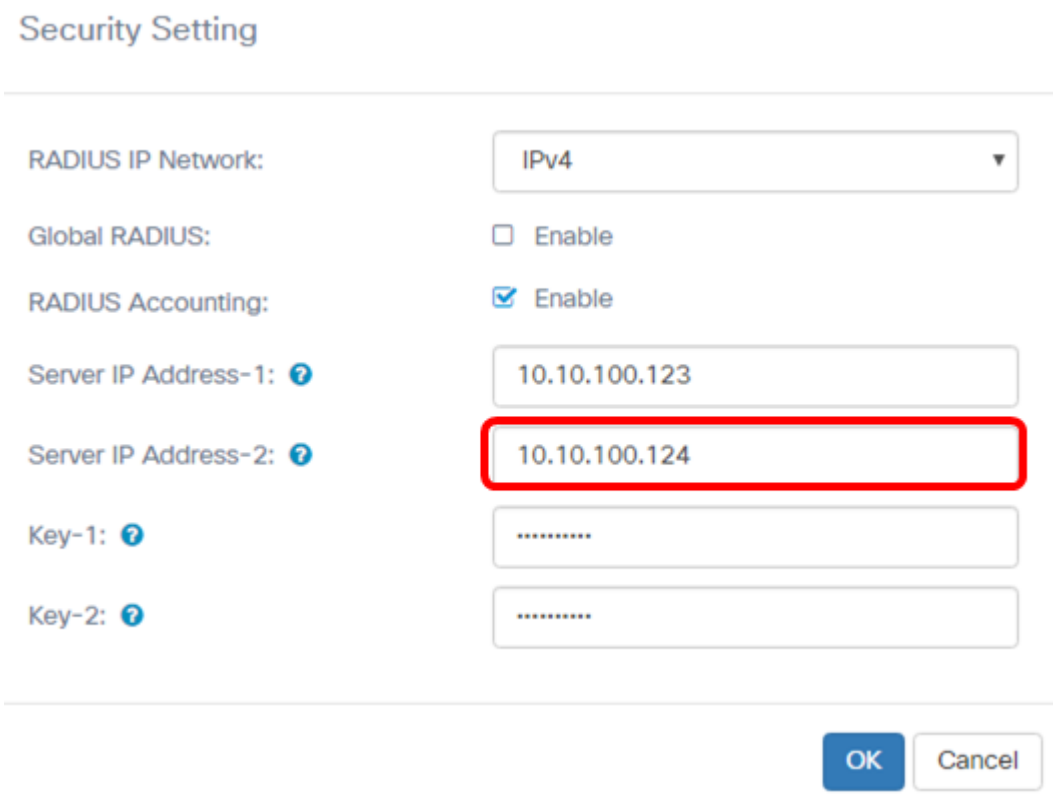


Step 5. (Optional) Enter the IPv4 or IPv6 address of the primary RADIUS server in the *Server IP Address-1* field.



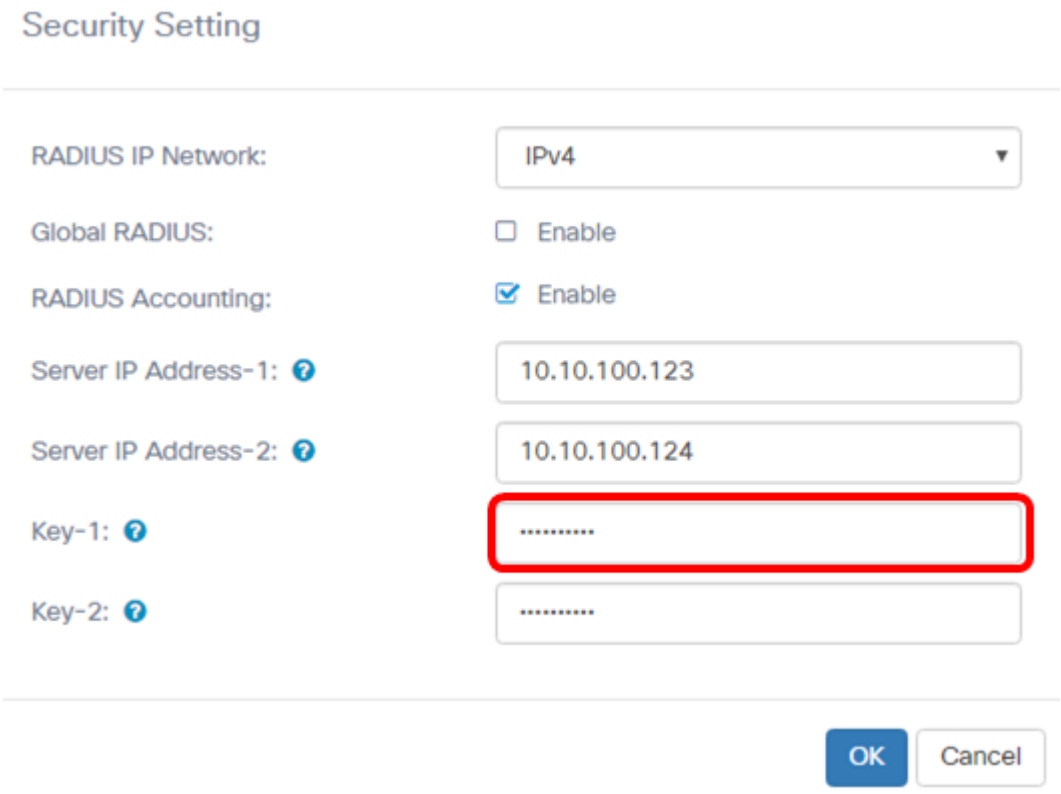
Note: In this example, 10.10.100.123 is entered.

Step 6. (Optional) Enter the IPv4 or IPv6 address of the backup RADIUS server in the *Server IP Address-2* field.



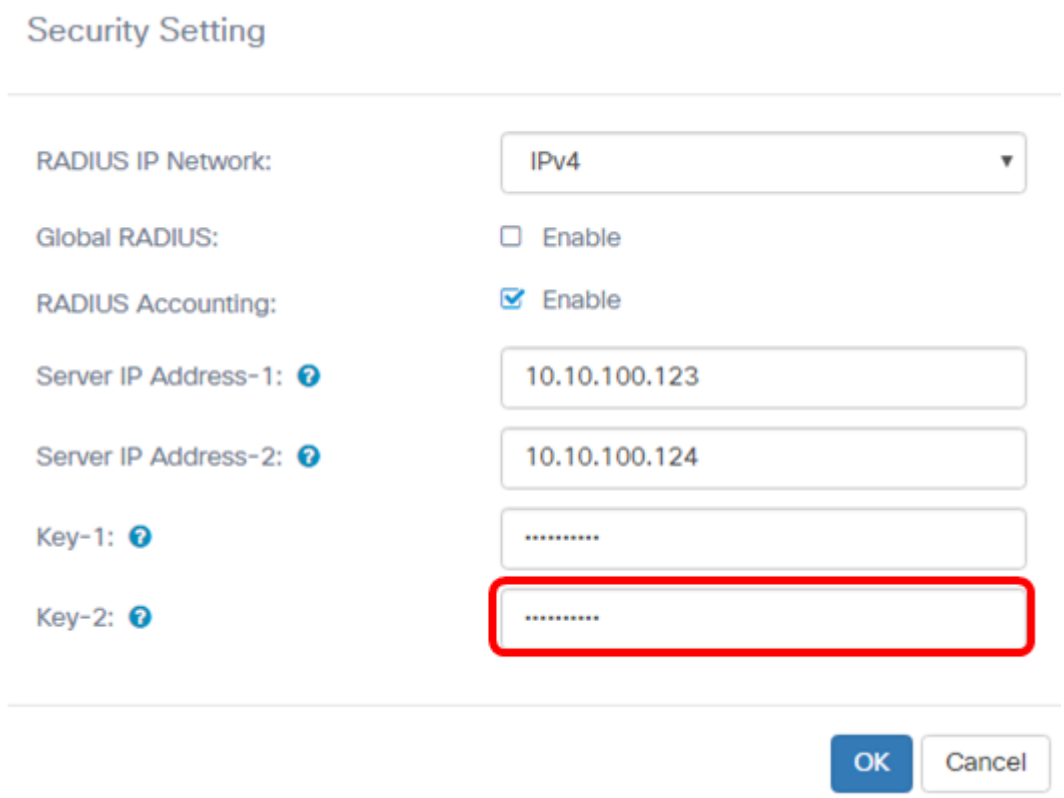
Note: In this example, 10.10.100.124 is entered.

Step 7. (Optional) Enter the password that the access point uses to authenticate the primary RADIUS server in the *Key-1* field. The entry in this field is case-sensitive and must match the entry configured on the primary RADIUS server. The key can be up to 63 alphanumeric characters.

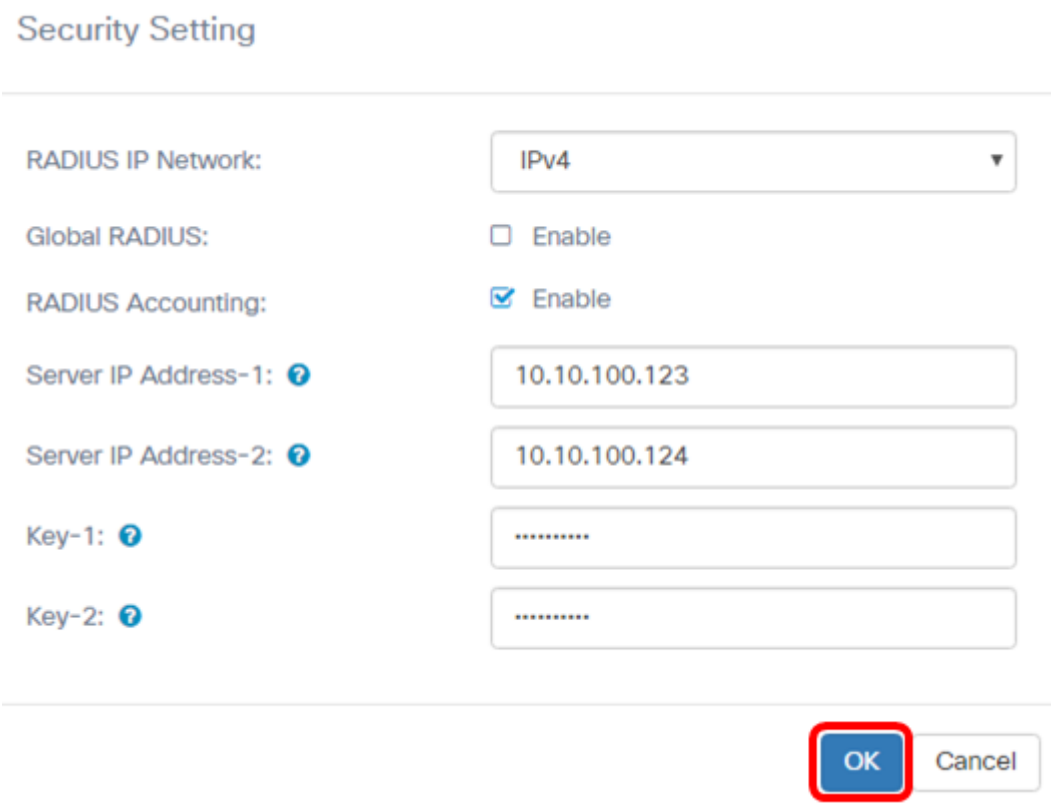


Step 8. (Optional) Enter the password that the access point uses to authenticate the secondary RADIUS server in the *Key-2* field. The entry in this field is case-sensitive and must match the entry configured on the primary RADIUS server. The key can be up to 63

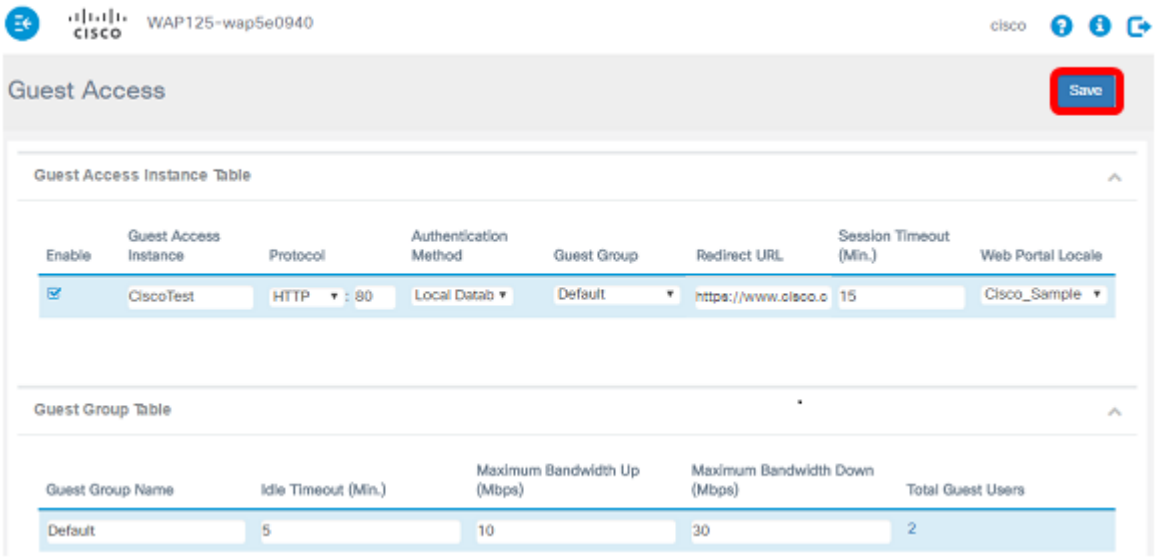
alphanumeric characters.



Step 9. Click **OK**.



Step 10. Click **Save**.



The Guest Access Instance table should now be configured with RADIUS authentication method.