

Configurazione di Captive Portal sul punto di accesso wireless mediante l'Installazione guidata

Obiettivo

Captive Portal è una funzionalità del punto di accesso wireless che consente di configurare una rete guest in cui gli utenti wireless devono essere autenticati prima di poter accedere a Internet. Fornisce l'accesso wireless ai visitatori mantenendo la sicurezza della rete interna.

In questo articolo viene illustrato come configurare Captive Portal sul punto di accesso wireless utilizzando l'Installazione guidata.

Dispositivi interessati

- WAP131
- WAP150
- WAP321
- WAP361

Versione del software

- 1.0.2.8 — WAP131
- 1.0.1.7 — WAP150, WAP361
- 1.0.6.5 — WAP321

Configura Captive Portal

Configurazione di Captive Portal mediante l'Installazione guidata

Nota: Le immagini seguenti sono state acquisite da WAP150. Tali immagini possono variare a seconda del modello esatto del punto di accesso.

Passaggio 1. Accedere all'utility basata sul Web del punto di accesso e scegliere **Esegui Installazione guidata** dal riquadro di navigazione.



Passaggio 2. Continuare a fare clic su **Avanti** fino a visualizzare la schermata Abilita portale vincolato - Crea rete guest.

Enable Captive Portal - Create Your Guest Network

Use Captive Portal to set up a guest network, which means that wireless users need to be authenticated before they can access the Internet. For example, a hotel can create a guest network to redirect new wireless users to a page for authentication.

Do you want to create your guest network now?

Yes

No, thanks.

[? Learn more about captive portal guest networks](#)

Click **Next** to continue

Passaggio 3. Fare clic sul pulsante di opzione **Sì** per creare la rete guest, quindi fare clic su **Avanti**.

Enable Captive Portal - Create Your Guest Network

Use Captive Portal to set up a guest network, which means that wireless users need to be authenticated before they can access the Internet. For example, a hotel can create a guest network to redirect new wireless users to a page for authentication.

Do you want to create your guest network now?

Yes

No, thanks.

[? Learn more about captive portal guest networks](#)

Click **Next** to continue

Passaggio 4. Fare clic sul pulsante di opzione relativo alla banda Radio in cui si desidera creare la rete guest.

Enable Captive Portal - Name Your Guest Network

Your guest network needs a new name, known as an SSID. The name identifies your guest network so that wireless users can find it.

Enter a name for your guest network:

Radio: Radio 1 (2.4 GHz)

Radio 2 (5 GHz)

Guest Network name:

For example: MyGuestNetwork

Nota: Nell'esempio, viene scelto Radio 1 (2,4 GHz).

Passaggio 5. Creare un nome per la rete guest nel campo *Guest Network name* (Nome rete guest), quindi fare clic su **Avanti**.

Enable Captive Portal - Name Your Guest Network
Your guest network needs a new name, known as an SSID. The name identifies your guest network so that wireless users can find it.

Enter a name for your guest network:

Radio: Radio 1 (2.4 GHz)
 Radio 2 (5 GHz)

Guest Network name:
For example: MyGuestNetwork

[? Learn more about network names](#)

Click **Next** to continue

Back **Next** Cancel

Nota: In questo esempio, il nome della rete guest viene utilizzato per ForTheGuests.

Passaggio 6. Fare clic su un pulsante di opzione per scegliere un tipo di protezione da utilizzare nella rete guest. Le opzioni sono:

- Massima protezione (WPA2 Personal - AES): offre la massima protezione ed è consigliata se le periferiche wireless supportano questa opzione. WPA2 Personal utilizza AES (Advanced Encryption Standard) e PSK (Pre-Shared Key) tra i client e il punto di accesso. Utilizza una nuova chiave di crittografia per ogni sessione, il che rende difficile la compromissione.
- Migliore protezione (WPA/WPA2 Personal - TKIP/AES): fornisce protezione quando sono presenti dispositivi wireless meno recenti che non supportano WPA2. WPA Personal utilizza AES e TKIP (Temporal Key Integrity Protocol). Utilizza lo standard Wi-Fi IEEE 802.11i.
- Nessuna protezione (scelta non consigliata): la rete wireless non richiede una password e può essere utilizzata da chiunque. Se selezionato, viene visualizzata una finestra popup in cui viene chiesto se si desidera disattivare la protezione; fare clic su **Sì** per continuare. Se si sceglie questa opzione, andare al

Enable Captive Portal - Secure Your Guest Network
Select your network security strength.

Best Security (WPA2 Personal - AES)
Recommended for new wireless computers and devices that support this option.
Older wireless devices might not support this option.

Better Security (WPA/WPA2 Personal - TKIP/AES)
Recommended for older wireless computers and devices that might not support WPA2.

No Security (Not recommended)

Nota: Nell'esempio viene scelto Better Security (WPA/WPA2 Personal - TKIP/AES).

Passaggio 7. Creare una password per la rete guest nel campo fornito. La barra colorata a destra di questo campo indica la complessità della password immessa.



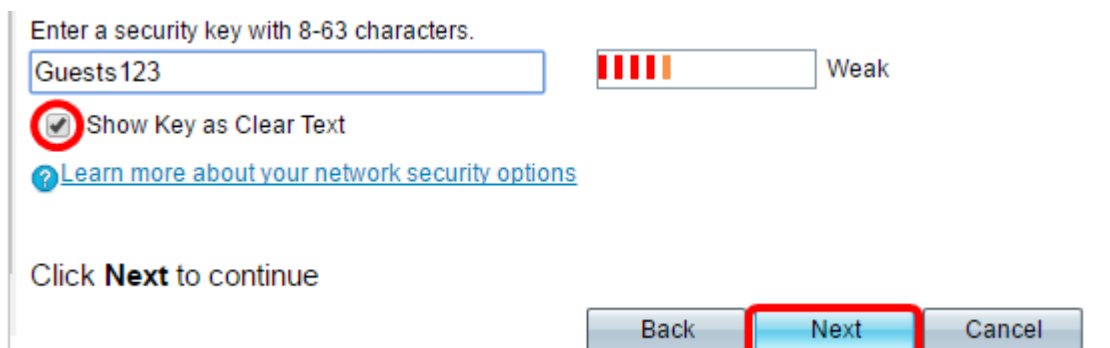
Enter a security key with 8-63 characters.

..... Session Key Refresh Rate

Show Key as Clear Text

[? Learn more about your network security options](#)

Passaggio 8. (Facoltativo) Per visualizzare la password durante la digitazione, selezionare la casella di controllo **Mostra chiave come testo non crittografato** e fare clic su **Avanti**.



Enter a security key with 8-63 characters.

Guests123 Weak

Show Key as Clear Text

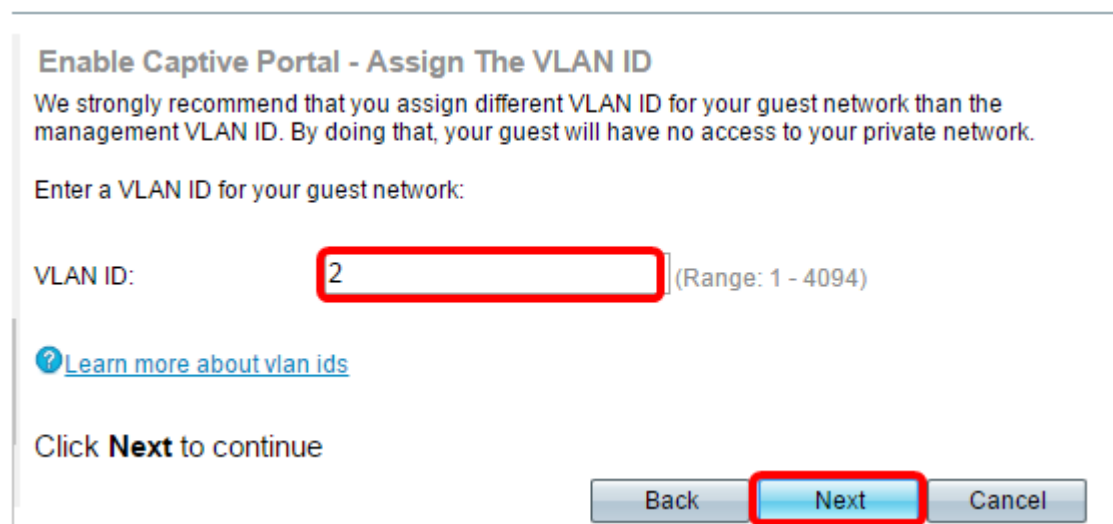
[? Learn more about your network security options](#)

Click **Next** to continue

Back **Next** Cancel

Passaggio 9. Nell'area Enable Captive Portal - Assegna l'ID VLAN, immettere l'ID VLAN per la rete guest e fare clic su **Next** (Avanti). L'intervallo di ID della VLAN è compreso tra 1 e 4094.

Nota: Per i protocolli WAP131 e WAP361, è necessario scegliere l'ID VLAN dall'elenco a discesa.



Enable Captive Portal - Assign The VLAN ID

We strongly recommend that you assign different VLAN ID for your guest network than the management VLAN ID. By doing that, your guest will have no access to your private network.

Enter a VLAN ID for your guest network:

VLAN ID: (Range: 1 - 4094)

[? Learn more about vlan ids](#)

Click **Next** to continue

Back **Next** Cancel

Nota: nell'esempio viene usato l'ID VLAN 2.

Passaggio 10. (Facoltativo) Nella schermata Abilita URL di reindirizzamento del portale vincolato, selezionare la casella di controllo **Abilita URL di reindirizzamento** se si desidera visualizzare una pagina Web specifica dopo che gli utenti hanno accettato le condizioni per l'utilizzo del servizio nella pagina di benvenuto.

Enable Captive Portal - Enable Redirect URL

If you enable a redirect URL, when new wireless users have completed the authentication process, they can be redirected to an alternate startup page.

Enable Redirect URL

Redirect URL :

Passaggio 11. Immettere l'URL nel campo *Reindirizza URL*, quindi fare clic su **Avanti**.

Enable Captive Portal - Enable Redirect URL

If you enable a redirect URL, when new wireless users have completed the authentication process, they can be redirected to an alternate startup page.

Enable Redirect URL

Redirect URL :

[? Learn more about redirect urls](#)

Click **Next** to continue

Back

Next

Cancel

Passaggio 12. Controllare le impostazioni configurate nella schermata Riepilogo - Conferma impostazioni. Per modificare un'impostazione, fare clic sul pulsante **Indietro** fino a raggiungere la pagina desiderata. In caso contrario, fare clic su **Invia** per abilitare le impostazioni in WAP.

Summary - Confirm Your Settings

Security Key:

VLAN ID: 1

Radio 2 (5 GHz)

Network Name (SSID): ciscosb

Network Security Type: plain-text

Security Key:

VLAN ID: 1

Captive Portal (Guest Network) Summary

Guest Network Radio: Radio 1

Network Name (SSID): ForTheGuests

Network Security Type: WPA/WPA2 Personal - TKIP/AES

Security Key: Guests123

Verification: Guest

Redirect URL: http://MyWebsite.com

Click **Submit** to enable settings on your Cisco Wireless Access Point

Back

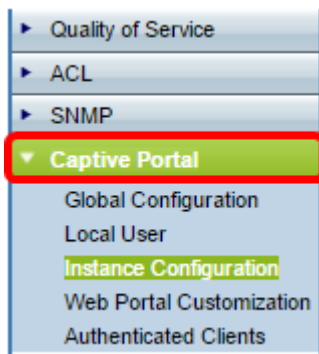
Submit

Cancel

Verifica impostazioni portale vincolato

Passaggio 13. Accedere all'utility basata sul Web e scegliere **Captive Portal > Instance**

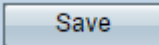
Configuration.



Passaggio 14. Nella pagina Configurazione istanza verificare le impostazioni configurate nell'Installazione guidata e assicurarsi che siano associate al punto di accesso virtuale (VAP) o alla rete corretti. Dovrebbe essere visualizzato anche il nome della rete guest.

A screenshot of the Captive Portal Instance Configuration page. The page contains the following fields and options:

- Administrative Mode: Enable
- Protocol: HTTP (dropdown)
- Verification: Guest (dropdown)
- Redirect: Enable
- Redirect URL: http://MyWebsite.com (Range: 0 - 256 Characters)
- Away Timeout: 60 (Range: 0 - 1440 Min, Default: 60)
- Session Timeout: 0 (Range: 0 - 1440 Min, Default: 0)
- Maximum Bandwidth Upstream: 0 (Range: 0 - 300 Mbps, Default: 0)
- Maximum Bandwidth Downstream: 0 (Range: 0 - 300 Mbps, Default: 0)
- Associate VAP (2.4 GHz): VAP 1 (ForTheGuests) (dropdown, highlighted with a red box)
- Associate VAP (5 GHz): (dropdown)

Passaggio 15. Fare clic su .

A questo punto, è necessario configurare Captive Portal sul punto di accesso wireless Cisco.

Qui è disponibile un video relativo a questo articolo...

[Fare clic qui per visualizzare altre Tech Talks di Cisco](#)