

Configurazione dell'istanza del portale vincolata sul punto di accesso WAP321

Obiettivo

Il portale captive consente di bloccare i client connessi alla rete WAP. I client visualizzano una pagina Web speciale a scopo di autenticazione prima di poter utilizzare Internet normalmente. La verifica Captive Portal è destinata sia ai guest che agli utenti autenticati e utilizza il browser Web trasformandolo in un dispositivo di autenticazione. Le istanze Captive Portal sono un set definito di configurazioni utilizzate per autenticare i client sulla rete WAP. È possibile configurare istanze diverse (massimo due) in modo che rispondano in modo diverso agli utenti che tentano di accedere al punto di accesso virtuale associato. I portali vincolati sono utilizzati in molti hotspot Wi-Fi per far pagare agli utenti l'accesso a Internet.

In questo documento viene spiegato come configurare la configurazione globale di Captive Portal sul punto di accesso WAP321.

Dispositivi interessati

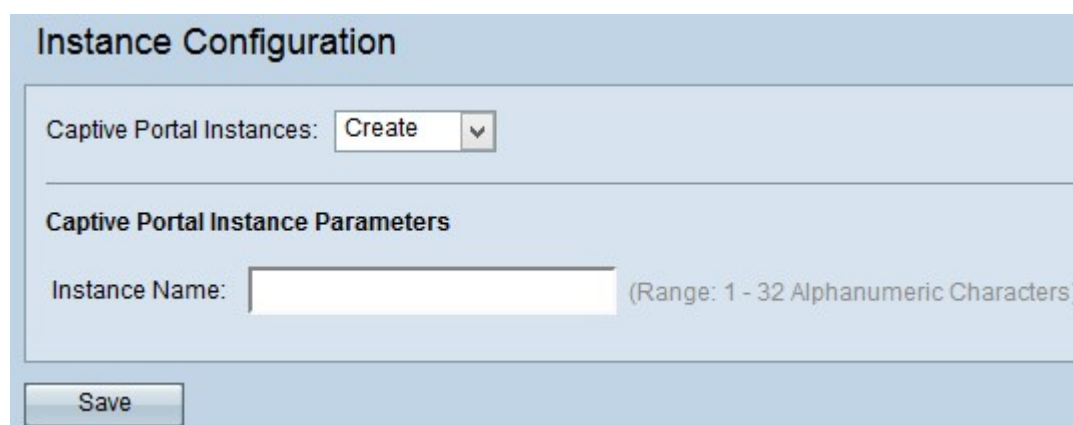
·WAP321

Versione del software

•1.0.3.4

Configurazione istanza portale vincolata

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Captive Portal > Instance Configuration**. Viene visualizzata la pagina *Configurazione istanza*:



The screenshot shows a web utility interface titled "Instance Configuration". At the top, there is a section labeled "Captive Portal Instances:" with a dropdown menu currently set to "Create". Below this is a section titled "Captive Portal Instance Parameters". It contains a text input field for "Instance Name:" with a placeholder "(Range: 1 - 32 Alphanumeric Characters)". At the bottom left of the form is a "Save" button.

Passaggio 2. Per creare una nuova configurazione, scegliere **Crea** dall'elenco a discesa Istanze portale captive. Per modificare la configurazione corrente, scegliere l'istanza corrente dall'elenco a discesa e andare al passo 5.

Nota: È possibile creare un massimo di due configurazioni.

Passaggio 3. Inserire un nome per la configurazione nel campo Nome istanza. L'intervallo è compreso tra 1 e 32 caratteri alfanumerici.

Instance Configuration

Captive Portal Instances: ▼

Captive Portal Instance Parameters

Instance Name: (Range: 1 - 32 Alphanumeric Characters)

Passaggio 4. Fare clic su **Salva** per salvare le modifiche apportate. La pagina viene nuovamente visualizzata con campi aggiuntivi per la configurazione dell'istanza.

Instance Configuration

Captive Portal Instances: instance2 ▼

Captive Portal Instance Parameters

Instance ID:	2
Administrative Mode:	<input checked="" type="checkbox"/> Enable
Protocol:	HTTP ▼
Verification:	Guest ▼
Redirect:	<input type="checkbox"/> Enable
Redirect URL:	<input type="text"/> (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)
User Group Name:	Default ▼
RADIUS IP Network:	IPv4 ▼
Global RADIUS:	<input checked="" type="checkbox"/> Enable
RADIUS Accounting:	<input type="checkbox"/> Enable
Server IP Address-1:	<input type="text"/> (xxx.xxx.xxx.xxx)
Server IP Address-2:	<input type="text"/> (xxx.xxx.xxx.xxx)
Server IP Address-3:	<input type="text"/> (xxx.xxx.xxx.xxx)
Server IP Address-4:	<input type="text"/> (xxx.xxx.xxx.xxx)
Key-1:	<input type="text"/> (Range: 1 - 63 Characters)
Key-2:	<input type="text"/> (Range: 1 - 63 Characters)
Key-3:	<input type="text"/> (Range: 1 - 63 Characters)
Key-4:	<input type="text"/> (Range: 1 - 63 Characters)
Locale Count:	0
Delete Instance:	<input type="checkbox"/>

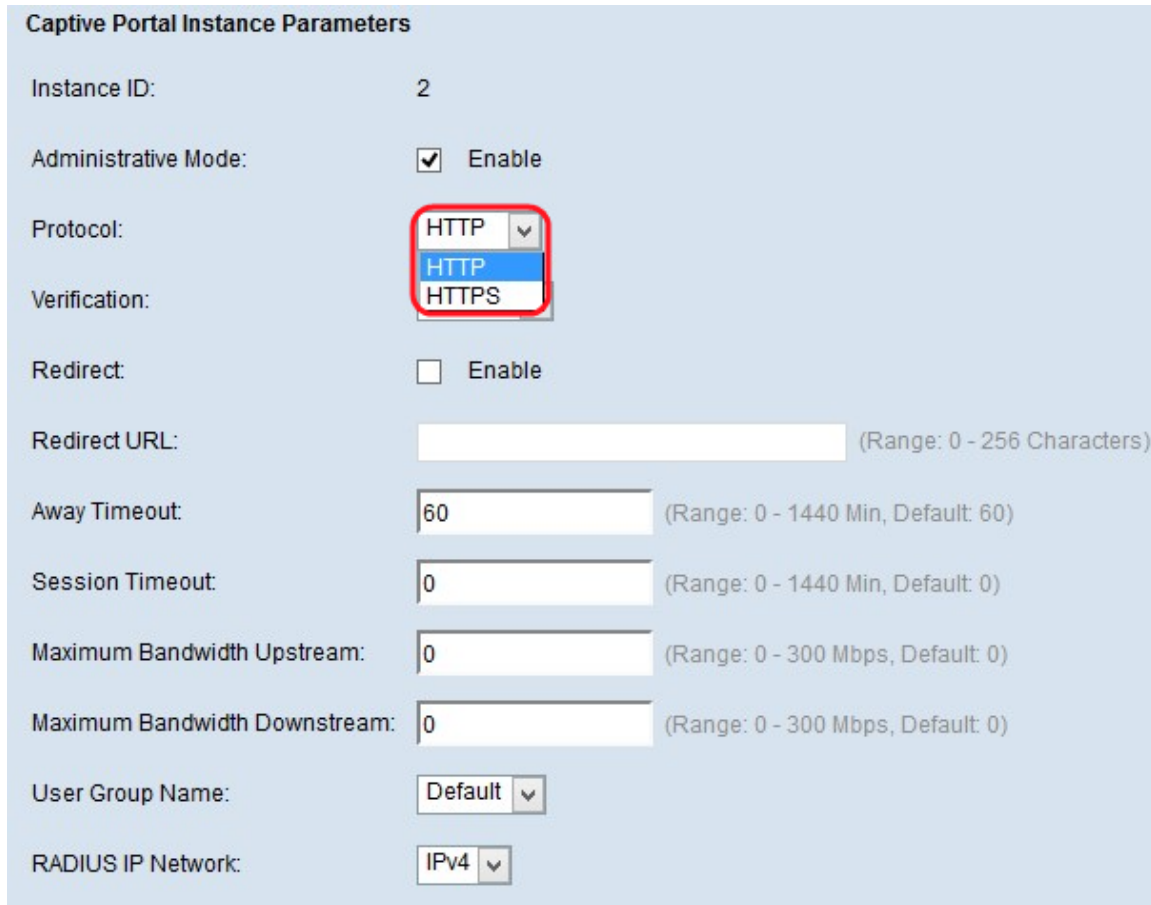
Save

La pagina *Configurazione istanza* contiene alcuni campi non configurabili che visualizzano le informazioni riportate di seguito.

- ID istanza - Specifica il numero di rango dell'istanza CP attualmente configurata sul dispositivo WAP.
- Conteggio impostazioni internazionali — specifica il numero di impostazioni internazionali

(set di parametri specifici della lingua e del paese delle preferenze utente) associate all'istanza.

Passaggio 5. Selezionare la casella di controllo **Abilita** per abilitare l'istanza CP nel campo Modalità amministrativa.



Captive Portal Instance Parameters

Instance ID: 2

Administrative Mode: Enable

Protocol: HTTP ▼
HTTP
HTTPS

Verification:

Redirect: Enable

Redirect URL: (Range: 0 - 256 Characters)

Away Timeout: (Range: 0 - 1440 Min, Default: 60)

Session Timeout: (Range: 0 - 1440 Min, Default: 0)

Maximum Bandwidth Upstream: (Range: 0 - 300 Mbps, Default: 0)

Maximum Bandwidth Downstream: (Range: 0 - 300 Mbps, Default: 0)

User Group Name: ▼

RADIUS IP Network: ▼

Passaggio 6. Scegliere il protocollo che l'istanza CP deve utilizzare per la verifica nel campo Protocollo. I valori possibili sono:

- HTTP: non esegue la crittografia delle informazioni per il processo di verifica.
- HTTPS: utilizza SSL (Secure Sockets Layer), che richiede un certificato per fornire la crittografia utilizzata nel processo di autenticazione.

Captive Portal Instance Parameters

Instance ID: 2

Administrative Mode: Enable

Protocol: HTTP

Verification: **Guest** (dropdown menu showing Guest, Local, RADIUS)

Redirect:

Redirect URL: (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)

User Group Name: Default

RADIUS IP Network: IPv4

Global RADIUS: Enable

Passaggio 7. Scegliere il metodo di autenticazione per CP da utilizzare per la verifica dall'elenco a discesa Verifica. I metodi di autenticazione vengono utilizzati per negare l'accesso al dispositivo a utenti malintenzionati. Il metodo di autenticazione scelto viene utilizzato per verificare i client. I valori possibili sono:

- Guest: non utilizza alcuna autenticazione.
- Locale: utilizza un database locale per l'autenticazione.
- RADIUS: utilizza un database server RADIUS remoto per l'autenticazione.

Verification:	<input type="text" value="Guest"/>	
Redirect:	<input checked="" type="checkbox"/> Enable	
Redirect URL:	<input type="text" value="http://www.example.com"/>	(Range: 0 - 256 Characters)
Away Timeout:	<input type="text" value="75"/>	(Range: 0 - 1440 Min, Default: 60)
Session Timeout:	<input type="text" value="1200"/>	(Range: 0 - 1440 Min, Default: 0)
Maximum Bandwidth Upstream:	<input type="text" value="10"/>	(Range: 0 - 300 Mbps, Default: 0)
Maximum Bandwidth Downstream:	<input type="text" value="300"/>	(Range: 0 - 300 Mbps, Default: 0)
User Group Name:	<input type="text" value="Default"/>	
RADIUS IP Network:	<input type="text" value="IPv4"/>	
Global RADIUS:	<input checked="" type="checkbox"/> Enable	
RADIUS Accounting:	<input type="checkbox"/> Enable	

Passaggio 8. Selezionare la casella di controllo **Abilita** nel campo Reindirizzamento per reindirizzare il client appena autenticato a un URL configurato.

Passaggio 9. Nel campo Reindirizza URL, immettere l'URL con il prefisso "http://" al quale verrà reindirizzato il client appena autenticato. L'intervallo ammesso è compreso da 0 a 256 caratteri.

Passaggio 10. Immettere il periodo di tempo durante il quale un utente può rimanere inattivo prima di essere disconnesso automaticamente nel campo Timeout Utente assente. Se il valore è impostato su 0, il timeout non viene applicato. L'intervallo è compreso tra 0 e 1440 minuti. Il valore predefinito è 60 minuti.

Passaggio 11. Inserire nel campo Timeout sessione la quantità di tempo di attesa prima della fine della sessione. L'intervallo è compreso tra 0 e 1440 minuti. Il valore predefinito è 0, che significa che il timeout non viene applicato.

Passaggio 12. Immettere la velocità di caricamento massima con cui un client può inviare i dati tramite il portale vincolato nel campo Upstream larghezza di banda massima. L'intervallo è compreso tra 0 e 300 Mbps. Il valore predefinito è 0.

Passaggio 13. Immettere la velocità massima di download con cui un client può ricevere dati tramite il portale vincolato nel campo Downstream larghezza di banda massima. L'intervallo è compreso tra 0 e 300 Mbps. Il valore predefinito è 0.

Verification:	<input type="text" value="Guest"/>	
Redirect:	<input checked="" type="checkbox"/> Enable	
Redirect URL:	<input type="text" value="http://www.example.com"/>	(Range: 0 - 256 Characters)
Away Timeout:	<input type="text" value="75"/>	(Range: 0 - 1440 Min, Default: 60)
Session Timeout:	<input type="text" value="1200"/>	(Range: 0 - 1440 Min, Default: 0)
Maximum Bandwidth Upstream:	<input type="text" value="10"/>	(Range: 0 - 300 Mbps, Default: 0)
Maximum Bandwidth Downstream:	<input type="text" value="300"/>	(Range: 0 - 300 Mbps, Default: 0)
User Group Name:	<input type="text" value="Default"/>	
RADIUS IP Network:	<input type="text" value="Default"/>	
Global RADIUS:	<input checked="" type="checkbox"/> Enable	
RADIUS Accounting:	<input type="checkbox"/> Enable	

Passaggio 14. Scegliere il gruppo desiderato nel campo Nome gruppo utenti che si desidera assegnare all'istanza CP dall'elenco a discesa dei gruppi preconfigurati.

RADIUS IP Network:	<input type="text" value="IPv4"/>	
Global RADIUS:	<input checked="" type="checkbox"/> Enable	
RADIUS Accounting:	<input type="checkbox"/> Enable	
Server IP Address-1:	<input type="text"/>	(xxx.xxx.xxx.xxx)
Server IP Address-2:	<input type="text"/>	(xxx.xxx.xxx.xxx)
Server IP Address-3:	<input type="text"/>	(xxx.xxx.xxx.xxx)
Server IP Address-4:	<input type="text"/>	(xxx.xxx.xxx.xxx)
Key-1:	<input type="text"/>	(Range: 1 - 63 Characters)
Key-2:	<input type="text"/>	(Range: 1 - 63 Characters)
Key-3:	<input type="text"/>	(Range: 1 - 63 Characters)
Key-4:	<input type="text"/>	(Range: 1 - 63 Characters)
Locale Count:	<input type="text" value="0"/>	
Delete Instance:	<input type="checkbox"/>	

Passaggio 15. Selezionare il tipo di protocollo Internet nel campo Rete IP RADIUS, che verrà utilizzato dall'istanza TCP dall'elenco a discesa Rete IP RADIUS. I valori possibili sono:

- IPv4: l'indirizzo del client RADIUS è nella quarta versione di IP con il formato

xxx.xxx.xxx.xxx (192.0.2.10).

·IPv6: l'indirizzo del client RADIUS sarà nella sesta versione dell'IP con il formato di indirizzo xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91).

RADIUS IP Network: IPv4

Global RADIUS: Enable

RADIUS Accounting: Enable

Server IP Address-1: 192.168.1.250 (xxx.xxx.xxx.xxx)

Server IP Address-2: 192.0.2.10 (xxx.xxx.xxx.xxx)

Server IP Address-3: 192.0.2.11 (xxx.xxx.xxx.xxx)

Server IP Address-4: 192.0.2.12 (xxx.xxx.xxx.xxx)

Key-1: (Range: 1 - 63 Characters)

Key-2: (Range: 1 - 63 Characters)

Key-3: (Range: 1 - 63 Characters)

Key-4: (Range: 1 - 63 Characters)

Locale Count: 0

Delete Instance:

Save

Passaggio 16. Selezionare la casella di controllo **Abilita** nel campo RADIUS globale se si desidera utilizzare l'elenco dei server RADIUS globali per l'autenticazione.

Timesaver: Se scegliete RAGGIO globale, passate al passo 22. Se è stata abilitata l'opzione Global RADIUS, non è necessario immettere l'indirizzo IP del server RADIUS, in quanto la funzionalità CP utilizzerà i server RADIUS globali preconfigurati.

Passaggio 17. Selezionare la casella di controllo **Abilita** nel campo Accounting RADIUS se si desidera registrare e misurare il tempo e l'utilizzo dei dati dei client sulla rete WAP.

Passaggio 18. Immettere l'indirizzo IP del server RADIUS che si desidera utilizzare come server primario nel campo Indirizzo IP server-1. L'indirizzo IP deve essere nel formato IPv4 o IPv6 a seconda dell'opzione scelta in Rete IP RADIUS al passaggio 15.

Passaggio 19. (Facoltativo) Immettere gli indirizzi IP dei server RADIUS di backup nei campi Indirizzo IP server-2 - Indirizzo IP server-4. Questi server vengono utilizzati se l'autenticazione non riesce con il server primario. È possibile configurare fino a tre server IP di backup che verranno autenticati in sequenza in caso di errore del predecessore.

Passaggio 20. Immettere la chiave privata condivisa nel campo Key-1 utilizzato dal dispositivo WAP per l'autenticazione al server RADIUS primario. È possibile utilizzare fino a 63 caratteri alfanumerici e speciali standard. La chiave fa distinzione tra maiuscole e minuscole.

Passaggio 21. (Facoltativo) Immettere la chiave segreta condivisa nei campi da Chiave 2 a 4

utilizzati dal dispositivo WAP per l'autenticazione nei rispettivi server RADIUS di backup.

Nel campo Conteggio impostazioni internazionali viene visualizzato il numero di impostazioni internazionali associate all'istanza corrente. Dalla pagina di personalizzazione Web è possibile creare e assegnare a ciascuna istanza tre impostazioni internazionali diverse.

Passaggio 22. (Facoltativo) Se si desidera eliminare l'istanza attualmente configurata, selezionare la casella di controllo **Elimina istanza** per eliminare l'istanza attualmente configurata.

Passaggio 23. Fare clic su **Salva** per salvare tutte le modifiche apportate.