

Konfiguration der Captive Portal Instance auf dem WAP321 Access Point

Ziel

Über das Captive Portal können Sie mit dem WAP-Netzwerk verbundene Clients blockieren. Clients sehen eine spezielle Webseite für Authentifizierungszwecke, bevor sie das Internet normal nutzen dürfen. Die Captive Portal-Verifizierung richtet sich sowohl an Gäste als auch an authentifizierte Benutzer und nutzt den Webbrowser, indem er ihn in ein Authentifizierungsgerät verwandelt. Captive Portal-Instanzen sind ein definierter Satz von Konfigurationen, die zur Authentifizierung von Clients im WAP-Netzwerk verwendet werden. Verschiedene Instanzen (maximal zwei) können so konfiguriert werden, dass sie auf andere Benutzer reagieren, wenn sie versuchen, auf den zugehörigen virtuellen Access Point zuzugreifen. Captive Portale werden an vielen Wi-Fi-Hotspots verwendet, um Benutzern den Zugang zum Internet in Rechnung zu stellen.

In diesem Dokument wird erläutert, wie die globale Konfiguration des Captive Portals auf dem WAP321 Access Point konfiguriert wird.

Anwendbare Geräte

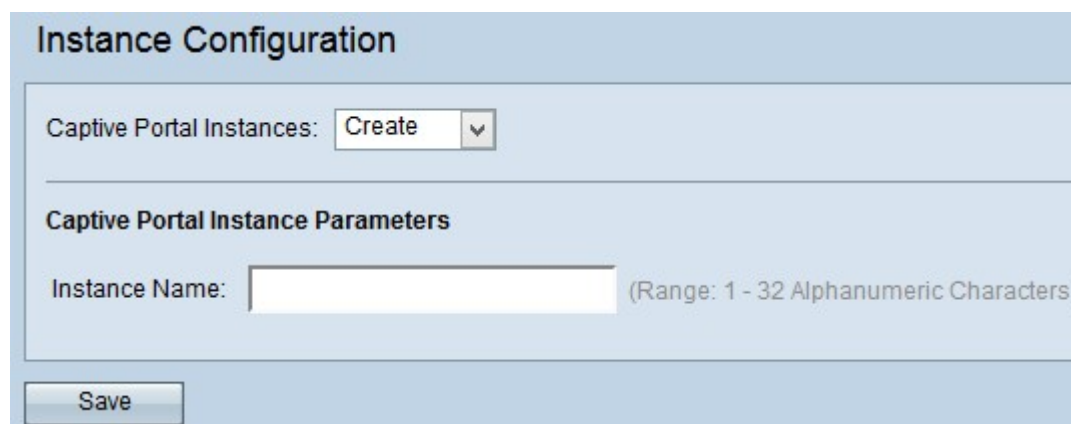
WAP321

Softwareversion

·1,0/3,4

Konfiguration der Captive Portal Instance

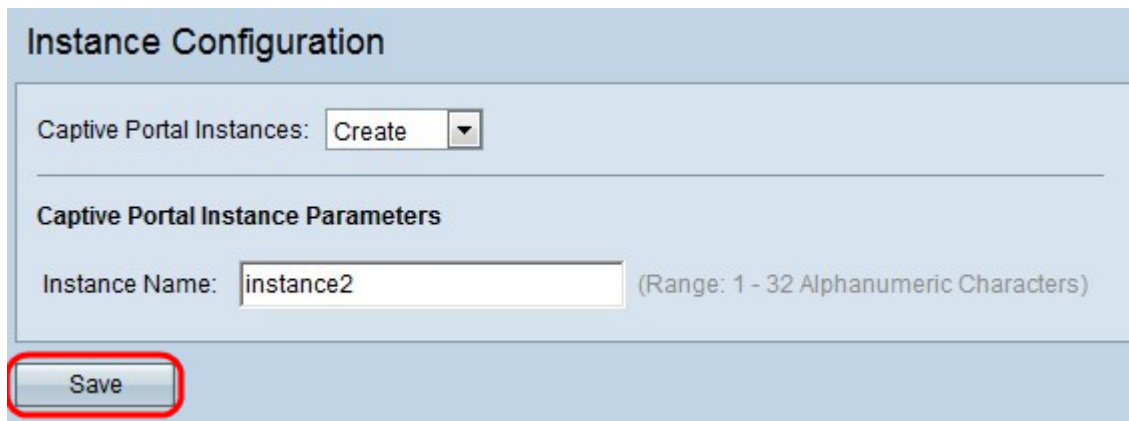
Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Captive Portal > Instance Configuration** aus. Die Seite *Instanzkonfiguration* wird geöffnet:



Schritt 2: Wählen Sie aus der Dropdown-Liste "Captive Portal Instances" (Instanzen des Captive Portals) die Option **Erstellen**, wenn Sie eine neue Konfiguration erstellen möchten. Um die aktuelle Konfiguration zu bearbeiten, wählen Sie die aktuelle Instanz aus der Dropdown-Liste aus, und fahren Sie mit Schritt 5 fort.

Hinweis: Sie können maximal zwei Konfigurationen erstellen.

Schritt 3: Geben Sie im Feld Instanzname einen Namen für die Konfiguration ein. Der Bereich umfasst 1 bis 32 alphanumerische Zeichen.



Instance Configuration

Captive Portal Instances: ▼

Captive Portal Instance Parameters

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

Schritt 4: Klicken Sie auf **Speichern**, um die vorgenommenen Änderungen zu speichern. Die Seite wird erneut mit zusätzlichen Feldern angezeigt, z. B. für die Konfiguration.

Instance Configuration

Captive Portal Instances:

Captive Portal Instance Parameters

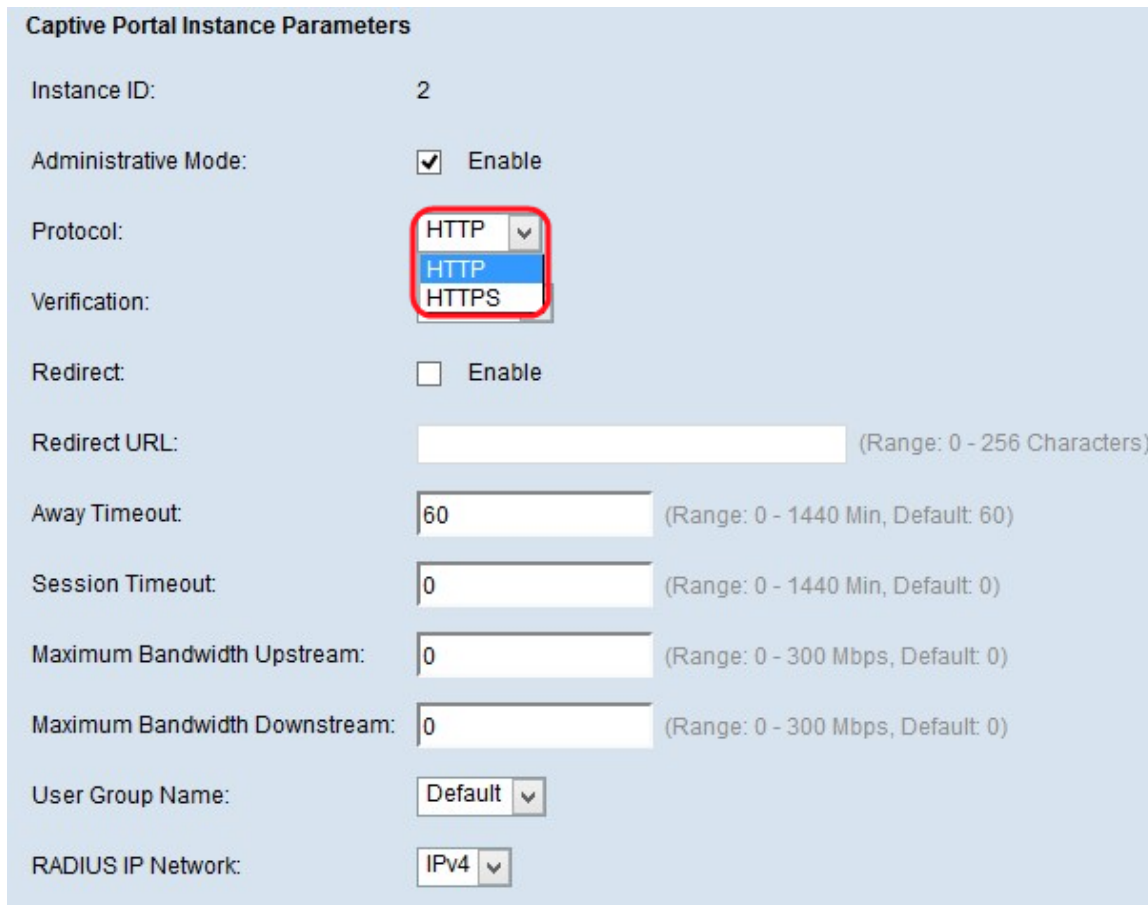
Instance ID:	2
Administrative Mode:	<input checked="" type="checkbox"/> Enable
Protocol:	<input type="text" value="HTTP"/>
Verification:	<input type="text" value="Guest"/>
Redirect:	<input type="checkbox"/> Enable
Redirect URL:	<input type="text"/> (Range: 0 - 256 Characters)
Away Timeout:	<input type="text" value="60"/> (Range: 0 - 1440 Min, Default: 60)
Session Timeout:	<input type="text" value="0"/> (Range: 0 - 1440 Min, Default: 0)
Maximum Bandwidth Upstream:	<input type="text" value="0"/> (Range: 0 - 300 Mbps, Default: 0)
Maximum Bandwidth Downstream:	<input type="text" value="0"/> (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
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"/>

Die Seite *Instanzkonfiguration* enthält einige nicht konfigurierbare Felder, die folgende Informationen anzeigen:

- Instanz-ID: Gibt die Rang-Anzahl der derzeit auf dem WAP-Gerät konfigurierten CP-Instanzen an.
- Locale Count (Gebietsschemaanzahl): Gibt die Anzahl der Gebietsschemas (Satz von

sprachlichen und länderspezifischen Parametern für Benutzereinstellungen) an, die der Instanz zugeordnet sind.

Schritt 5: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um die CP-Instanz im Feld Verwaltungsmodus zu aktivieren.



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: ▼

Schritt 6: Wählen Sie das Protokoll aus, das die CP-Instanz im Feld Protokoll zur Überprüfung verwenden soll. Mögliche Werte sind:

- HTTP - Keine Verschlüsselung von Informationen für den Verifizierungsprozess.
- HTTPS - Verwendet SSL (Secure Sockets Layer), das ein Zertifikat für die Verschlüsselung erfordert, die im Authentifizierungsprozess verwendet wird.

Captive Portal Instance Parameters

Instance ID: 2

Administrative Mode: Enable

Protocol: HTTP

Verification: **Guest** (dropdown menu open 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

Schritt 7: Wählen Sie aus der Dropdown-Liste Überprüfung die Authentifizierungsmethode für den CP aus, der zur Überprüfung verwendet werden soll. Authentifizierungsmethoden werden verwendet, um böswilligen Benutzern den Zugriff auf das Gerät zu verweigern. Die gewählte Authentifizierungsmethode wird zur Überprüfung der Clients verwendet. Mögliche Werte sind:

- Guest (Gast): Keine Authentifizierung.
- Local (Lokal): Verwendet eine lokale Datenbank für die Authentifizierung.
- RADIUS - Verwendet eine Remote-RADIUS-Serverdatenbank für die Authentifizierung.

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

Schritt 8: Aktivieren Sie das **Kontrollkästchen Aktivieren** im Feld Umleiten, wenn Sie den neu authentifizierten Client an eine konfigurierte URL umleiten möchten.

Schritt 9: Geben Sie die URL mit dem Präfix "http://" ein, zu der der neu authentifizierte Client im Feld "Umleiten-URL" umgeleitet wird. Der Bereich liegt zwischen 0 und 256 Zeichen.

Schritt 10: Geben Sie die Zeitdauer ein, die ein Benutzer vor dem automatischen Abmelden im Feld "Away Timeout" (Abwesenheitszeit) inaktiv bleiben kann. Wenn der Wert auf 0 gesetzt ist, wird das Timeout nicht erzwungen. Der Bereich liegt zwischen 0 und 1440 Minuten. Der Standardwert ist 60 Minuten.

Schritt 11: Geben Sie im Feld Session Timeout (Sitzungszeitüberschreitung) die Wartezeit ein, bis die Sitzung beendet wird. Der Bereich liegt zwischen 0 und 1440 Minuten. Der Standardwert ist 0, d. h. die Zeitüberschreitung wird nicht erzwungen.

Schritt 12: Geben Sie die maximale Upload-Geschwindigkeit ein, die ein Client über das Captive Portal im Feld Maximum Bandwidth Upstream (Maximale Upstream-Bandbreite) senden kann. Der Bereich liegt zwischen 0 und 300 Mbit/s. Der Standardwert ist 0.

Schritt 13: Geben Sie die maximale Download-Geschwindigkeit ein, die ein Client über das Captive Portal im Feld Maximum Bandwidth Downstream (Maximale Bandbreite für Downstream) empfangen kann. Der Bereich liegt zwischen 0 und 300 Mbit/s. Der Standardwert ist 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	

Schritt 14: Wählen Sie im Feld User Group Name (Benutzergruppenname) die gewünschte Gruppe aus, die Sie der CP-Instanz aus der Dropdown-Liste der vorkonfigurierten Gruppen zuweisen möchten.

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"/>	

Schritt 15: Wählen Sie im Feld RADIUS IP Network (RADIUS-IP-Netzwerk) den Typ des Internetprotokolls aus, der von der CP-Instanz verwendet wird. Wählen Sie diesen Typ aus der Dropdown-Liste RADIUS IP network (RADIUS-IP-Netzwerk) aus. Mögliche Werte sind:

·IPv4 - Die Adresse des RADIUS-Clients befindet sich in der vierten Version von IP mit dem Adressformat xxx.xxx.xxx.xxx (192.0.2.10).

·IPv6 - Die Adresse des RADIUS-Clients befindet sich in der sechsten Version der IP-Adresse mit dem Adressformat xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91).

RADIUS IP Network:	IPv4	
Global RADIUS:	<input type="checkbox"/>	Enable
RADIUS Accounting:	<input checked="" type="checkbox"/>	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:	<input type="checkbox"/>	

Save

Schritt 16: Aktivieren Sie das **Kontrollkästchen Aktivieren** im Feld Global RADIUS, wenn Sie die globale RADIUS-Serverliste für die Authentifizierung verwenden möchten.

Zeitgeber: Fahren Sie mit Schritt 22 fort, wenn Sie Global RADIUS auswählen. Wenn Sie die globale RADIUS-Option aktiviert haben, müssen Sie die RADIUS-Server-IP nicht eingeben, da die CP-Funktion die vorkonfigurierten globalen RADIUS-Server verwendet.

Schritt 17: Aktivieren Sie das Kontrollkästchen **Aktivieren** im Feld RADIUS Accounting (RADIUS Accounting), wenn Sie die Zeit- und Datenauslastung der Clients im WAP-Netzwerk nachverfolgen und messen möchten.

Schritt 18: Geben Sie im Feld Server IP Address-1 (Server-IP-Adresse-1) die IP-Adresse des RADIUS-Servers ein, den Sie als Primärserver verwenden möchten. Die IP-Adresse sollte das Format IPv4 oder IPv6 haben, je nachdem, was Sie in Schritt 15 im RADIUS IP Network ausgewählt haben.

Schritt 19: (Optional) Geben Sie die IP-Adressen des Backup-RADIUS-Servers in die Felder Server IP Address-2 to Server IP Address-4 (Server-IP-Adresse 2 bis Server-IP-Adresse-4) ein. Diese Server werden verwendet, wenn die Authentifizierung mit dem primären Server fehlschlägt. Sie können bis zu drei Backup-IP-Server konfigurieren, die nacheinander authentifiziert werden, wenn der Vorgänger ausfällt.

Schritt 20: Geben Sie den gemeinsamen geheimen Schlüssel in das Feld Key-1 ein, das das

WAP-Gerät für die Authentifizierung beim primären RADIUS-Server verwendet. Sie können bis zu 63 alphanumerische Standardzeichen und Sonderzeichen verwenden. Beim Schlüssel wird Groß- und Kleinschreibung unterschieden.

Schritt 21: (Optional) Geben Sie den gemeinsamen geheimen Schlüssel in die Felder Schlüssel 2 bis 4 ein, die das WAP-Gerät zur Authentifizierung der entsprechenden Backup-RADIUS-Server verwendet.

Das Feld Locale Count (Gebietsschemazahl) zeigt die Anzahl der Gebietsschemas an, die der aktuellen Instanz zugeordnet sind. Auf der Webseite zur Anpassung können drei verschiedene Gebietsschemas erstellt und jeder Instanz zugewiesen werden.

Schritt 22: (Optional) Wenn Sie die aktuell konfigurierte Instanz löschen möchten, aktivieren Sie das Kontrollkästchen **Instanz löschen**, um die aktuell konfigurierte Instanz zu löschen.

Schritt 23: Klicken Sie auf **Speichern**, um alle vorgenommenen Änderungen zu speichern.