

Erstkonfiguration der Wireless Access Points WAP150, WAP351, WAP361 und WAP371 mithilfe des Installationsassistenten

Ziel

Der Installationsassistent ist eine integrierte Funktion, die bei der Erstkonfiguration der Wireless Access Points (WAPs) hilfreich ist. Dadurch wird die Konfiguration der Grundeinstellungen vereinfacht. Der schrittweise Prozess des Einrichtungsassistenten führt Sie durch die Ersteinrichtung des WAP-Geräts und bietet eine schnelle Möglichkeit, die grundlegenden Funktionen des WAP zu nutzen.

In diesem Dokument wird die Konfiguration der Wireless Access Points WAP150, WAP351, WAP361 und WAP371 mithilfe des Setup-Assistenten erläutert.

Anwendbare Geräte

- WAP150
- WAP351
- WAP361
- WAP371

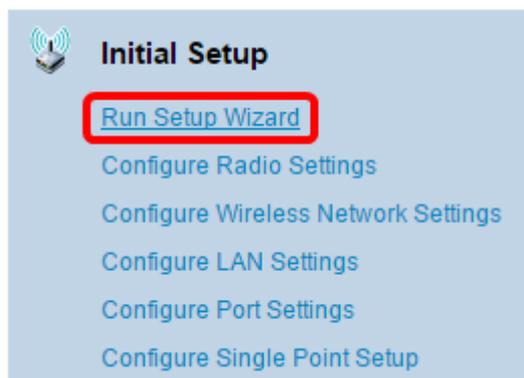
Softwareversion

- 1.0.1.7 - WAP150, WAP361
- 1.0.2.8 - WAP351
- 1.3.0.3 - WAP371

Konfiguration

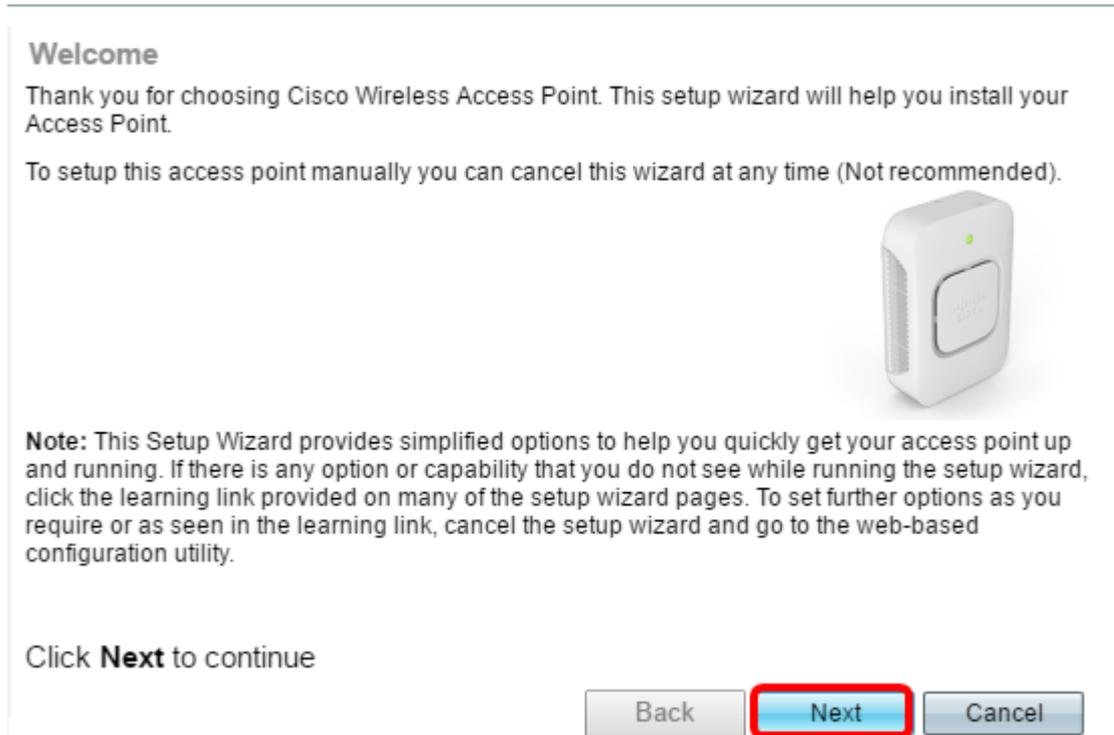
Hinweis: Die unten verwendeten Bilder stammen aus dem WAP361.

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des Access Points an. Klicken Sie auf der Seite "Getting Started" auf **Setup Wizard (Installationsassistent ausführen)**.



Hinweis: Wenn Sie sich zum ersten Mal beim WAP angemeldet haben, wird der Installationsassistent automatisch geöffnet.

Schritt 2: Klicken Sie im Access Point-Einrichtungsassistenten auf **Weiter** auf der Willkommenseite, um fortzufahren.



Schritt 3: Klicken Sie auf das Optionsfeld für die Methode, mit der Sie die IP-Adresse des WAP bestimmen möchten.

Die Optionen sind wie folgt definiert:

- Dynamische IP-Adresse (DHCP) (empfohlen) - Ermöglicht dem DHCP-Server, eine dynamische IP-Adresse für den WAP zuzuweisen. Wenn Sie diese Option auswählen, klicken Sie auf **Weiter** und fahren Sie dann mit [Schritt 9 fort](#).
- Statische IP-Adresse - Ermöglicht das Erstellen einer statischen (statischen) IP-Adresse für den WAP. Eine statische IP-Adresse ändert sich nicht.

Hinweis: In diesem Beispiel wird Dynamic IP Address (DHCP) ausgewählt.

Configure Device - IP Address

Select either Dynamic or Static IP address for your device.

Dynamic IP Address (DHCP) (Recommended)

Static IP Address

Static IP Address: . . .

Subnet Mask: . . .

Default Gateway: . . .

DNS: . . .

Secondary DNS (optional): . . .

[? Learn more about the different connection types](#)

Click **Next** to continue

Schritt 4: Wenn im vorherigen Schritt die statische IP-Adresse ausgewählt wurde, geben Sie die IP-Adresse des WAP im Feld *Statische IP-Adresse* ein. Diese IP-Adresse ist nur für den WAP bestimmt und sollte nicht von einem anderen Gerät im Netzwerk verwendet werden.

Dynamic IP Address (DHCP) (Recommended)

Static IP Address

Static IP Address: . . .

Subnet Mask: . . .

Default Gateway: . . .

DNS: . . .

Secondary DNS (optional): . . .

Hinweis: In diesem Beispiel wird 192.168.1.121 als statische IP-Adresse verwendet.

Schritt 5: Geben Sie die Subnetzmaske im Feld *Subnetzmaske* ein.

Dynamic IP Address (DHCP) (Recommended)

Static IP Address

Static IP Address: . . .

Subnet Mask: . . .

Default Gateway: . . .

DNS: . . .

Secondary DNS (optional): . . .

Hinweis: In diesem Beispiel wird 255.255.255.0 als Subnetzmaske verwendet.

Schritt 6: Geben Sie das Standard-Gateway für den WAP im Feld *Standard-Gateway* ein. Dies ist die private IP-Adresse Ihres Routers.

Dynamic IP Address (DHCP) (Recommended)
 Static IP Address

Static IP Address: . . .
 Subnet Mask: . . .
 Default Gateway: . . .
 DNS: . . .
 Secondary DNS (optional): . . .

Hinweis: In diesem Beispiel wird 192.168.1.1 als Standard-Gateway verwendet.

Schritt 7: (Optional) Wenn Sie außerhalb Ihres Netzwerks auf das webbasierte Dienstprogramm zugreifen möchten, geben Sie die primäre DNS-Adresse (Domain Name System) in das *DNS*-Feld ein. Ihr Internetdienstanbieter (ISP) sollte Ihnen die DNS-Serveradresse angeben.

Dynamic IP Address (DHCP) (Recommended)
 Static IP Address

Static IP Address: . . .
 Subnet Mask: . . .
 Default Gateway: . . .
 DNS: . . .
 Secondary DNS (optional): . . .

Hinweis: In diesem Beispiel wird 192.168.1.2 als DNS-Adresse verwendet.

Schritt 8: (Optional) Geben Sie eine sekundäre DNS-Adresse in die Felder *Sekundäres DNS ein* und klicken Sie dann auf **Weiter**.

Dynamic IP Address (DHCP) (Recommended)
 Static IP Address

Static IP Address: . . .
 Subnet Mask: . . .
 Default Gateway: . . .
 DNS: . . .
 Secondary DNS (optional): . . .

Hinweis: In diesem Beispiel wird 192.168.1.3 als sekundäre DNS-Adresse verwendet.

Single-Point-Einrichtung

Schritt 9: Wählen Sie im Bildschirm Single Point Setup - Set A Cluster (Single-Point-Einrichtung - Cluster einrichten) ein Optionsfeld aus, das der Konfiguration der Cluster-Einstellungen des WAP entspricht. Durch Clustering können Sie mehrere Access Points von einem einzigen Punkt aus verwalten, anstatt jedes Gerät einzeln zu verwalten.

Die Optionen sind wie folgt definiert:

- Neuer Cluster-Name - Wählen Sie diese Option aus, wenn Sie einen neuen Cluster erstellen möchten.

Hinweis: Für WAP351 und WAP371 besteht die Option Neuen Cluster erstellen.

- Einem vorhandenen Cluster beitreten: Wählen Sie diese Option aus, wenn der WAP einem vorhandenen Cluster beitreten soll. Wenn Sie diese Option auswählen, fahren Sie mit [Schritt 11 fort](#).
- Single Point Setup (Single-Point-Einrichtung nicht aktivieren): Wählen Sie diese Option aus, wenn der WAP nicht Teil eines Clusters sein soll. Wenn Sie diese Option auswählen, klicken Sie auf **Weiter** und fahren Sie dann mit [Schritt 13 fort](#).

Hinweis: In diesem Beispiel wird die Option Single-Point-Einrichtung nicht aktivieren ausgewählt.

Single Point Setup -- Set A Cluster

A cluster provides a single point of administration and lets you view, deploy, configure, and secure the wireless network as a single entity, rather than as a series of separate wireless devices.

New Cluster Name
Recommended for a new deployment environment.
New Cluster Name:
AP Location:

Join an Existing Cluster
Recommended for adding new wireless access points to the existing deployment environment.
Existing Cluster Name:
AP Location:

Do not Enable Single Point Setup
Recommended for single device deployments or if you prefer to configure each device individually.

[? Learn more about single point setup](#)

Click **Next** to continue

Back Next Cancel

Schritt 10: Wenn Sie im vorherigen Schritt New Cluster Name (Neuer Cluster-Name) ausgewählt haben, geben Sie den Namen des neuen Clusters und dessen Speicherort in die Felder *Neuer Cluster-Name* und *AP-Speicherort* ein, und klicken Sie dann auf **Weiter**. Der AP-Standort ist der physische Standort des vom Benutzer definierten Access Points (z. B. Office). Fahren Sie mit [Schritt 13 fort](#).

Single Point Setup -- Set A Cluster

A cluster provides a single point of administration and lets you view, deploy, configure, and secure the wireless network as a single entity, rather than as a series of separate wireless devices.

New Cluster Name
Recommended for a new deployment environment
New Cluster Name:
AP Location:

Join an Existing Cluster
Recommended for adding new wireless access points to the existing deployment environment.
Existing Cluster Name:
AP Location:

Do not Enable Single Point Setup
Recommended for single device deployments or if you prefer to configure each device individually.

[? Learn more about single point setup](#)

Click **Next** to continue

Back **Next** Cancel

Schritt 11: Wenn Sie in Schritt 9 **Join an Existing Cluster (An bestehendem Cluster beitreten)** ausgewählt haben, geben Sie den Namen des Clusters und dessen Speicherort in die Felder *Vorhandener Cluster Name* und *AP Location (AP-Speicherort)* ein, und klicken Sie dann auf **Weiter**.

Hinweis: Diese Option ist ideal, wenn bereits ein Wireless-Netzwerk vorhanden ist und alle Einstellungen bereits konfiguriert wurden.

Single Point Setup -- Set A Cluster

A cluster provides a single point of administration and lets you view, deploy, configure, and secure the wireless network as a single entity, rather than as a series of separate wireless devices.

New Cluster Name
Recommended for a new deployment environment.
New Cluster Name:
AP Location:

Join an Existing Cluster
Recommended for adding new wireless access points to the existing deployment environment.
Existing Cluster Name:
AP Location:

Do not Enable Single Point Setup
Recommended for single device deployments or if you prefer to configure each device individually.

[? Learn more about single point setup](#)

Click **Next** to continue

Back **Next** Cancel

Schritt 12: Überprüfen Sie Ihre Einstellungen, um sicherzustellen, dass die Daten korrekt sind, und klicken Sie dann auf **Senden**.

Summary - Confirm Your Settings
 Please review the following settings and ensure the data is correct.

You are about to join this cluster: Main Point

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

Back **Submit** Cancel

Zeiteinstellungen

[Schritt 13](#): Wählen Sie Ihre Zeitzone aus der Dropdown-Liste "Time Zone" (Zeitzone) aus.

Configure Device - Set System Date And Time
 Enter the time zone, date and time.

Time Zone: USA (Pacific) ▼

Set System Time: USA (Aleutian Islands) ▲
 USA (Arizona)
 USA (Central)
 USA (Eastern)
 USA (Mountain)
 USA (Pacific)
 Uzbekistan
 Vanuatu
 Vatican City
 Venezuela
 Vietnam
 Wake Islands
 Wallis & Futana Islands
 Western Samoa
 Windward Islands
 Yemen
 Zaire (Kasai)
 Zaire (Kinshasa)
 Zambia
 Zimbabwe ▼

NTP Server 1:
 NTP Server 2:
 NTP Server 3:
 NTP Server 4:

[? Learn more about t](#)

Click **Next** to continue

Back **Next** Cancel

Hinweis: In diesem Beispiel wird USA (Pazifik) ausgewählt.

Schritt 14: Klicken Sie auf das Optionsfeld, das der Methode entspricht, mit der Sie die Uhrzeit des WAP festlegen möchten.

Folgende Optionen sind verfügbar:

- Network Time Protocol (NTP) - Der WAP erhält die Zeit von einem NTP-Server.
- Manuell — Die Uhrzeit wird manuell in den WAP eingegeben. Wenn diese Option ausgewählt ist, fahren Sie mit [Schritt 16 fort](#).

Configure Device - Set System Date And Time
Enter the time zone, date and time.

Time Zone:

Set System Time: Network Time Protocol (NTP)
 Manually

NTP Server 1:

NTP Server 2:

NTP Server 3:

NTP Server 4:

[? Learn more about time settings](#)

Click **Next** to continue

Hinweis: In diesem Beispiel wird das Network Time Protocol (NTP) verwendet.

Schritt 15: Geben Sie den Domännennamen des NTP-Servers ein, der das Datum und die Uhrzeit in das Feld *NTP-Server 1* angibt. Sie können bis zu vier verschiedene NTP-Server hinzufügen, indem Sie diese in die entsprechenden Felder eingeben und dann auf **Weiter** klicken. Fahren Sie anschließend mit [Schritt 17 fort](#).

Configure Device - Set System Date And Time
Enter the time zone, date and time.

Time Zone:

Set System Time: Network Time Protocol (NTP)
 Manually

NTP Server 1:

NTP Server 2:

NTP Server 3:

NTP Server 4:

[? Learn more about time settings](#)

Click **Next** to continue

Hinweis: In diesem Beispiel werden vier NTP-Server eingegeben.

[Schritt 16:](#) (Optional) Wenn Sie in Schritt 14 die Option Manuell ausgewählt haben, wählen Sie das Datum in den Dropdown-Listen Systemdatum aus, um den Monat, den Tag bzw. das Jahr auszuwählen. Wählen Sie die Stunde und die Minuten aus den Dropdown-Listen Systemzeit aus, und klicken Sie dann auf **Weiter**.

Configure Device - Set System Date And Time
 Enter the time zone, date and time.

Time Zone:

Set System Time: Network Time Protocol (NTP)
 Manually

System Date:

System Time: :

[Learn more about time settings](#)

Click **Next** to continue

Gerätekenwort

Schritt 17. Geben Sie im Bildschirm Gerät konfigurieren - Kennwort festlegen im Feld *Neues Kennwort* ein neues Kennwort für den WAP ein, und bestätigen Sie es. Dieses Kennwort wird verwendet, um Administratorzugriff auf das webbasierte Dienstprogramm des WAP selbst zu erhalten, nicht um eine Verbindung zum Wireless-Netzwerk herzustellen.

New Password:

Confirm Password:

Password Strength Meter: Below Minimum

Hinweis: Das Feld *Kennwortstärkeregelung* zeigt vertikale Balken an, die sich bei Eingabe des Kennworts ändern.

Die Farben des Kennwortstärkemessgeräts sind wie folgt definiert:

- Rot: Die Mindestanforderung an die Kennwortkomplexität wird nicht erfüllt.
- Orange - Die Mindestanforderung an die Passwortkomplexität ist erfüllt, aber die Kennwortstärke ist schwach.
- Grün - Die Mindestanforderung an die Kennwortkomplexität ist erfüllt, und die Kennwortstärke ist hoch.

Schritt 18: (Optional) Aktivieren Sie das Kontrollkästchen **Enable Password Complexity** (Kennwortkomplexität **aktivieren**), um die Kennwortkomplexität zu aktivieren. Das Kennwort muss mindestens 8 Zeichen lang sein und aus Groß- und Kleinbuchstaben sowie Ziffern oder Symbolen bestehen. Die Kennwortkomplexität ist standardmäßig aktiviert.

New Password:

Confirm Password:

Password Strength Meter: Below Minimum

Password Complexity: Enable

[? Learn more about passwords](#)

Click **Next** to continue

Schritt 19: Klicken Sie auf **Weiter**, um fortzufahren.

Konfigurieren der Funkmodule 1 und 2 (2,4 und 5 GHz)

Die Wireless-Netzwerkeinstellungen müssen für jeden Funkkanal einzeln konfiguriert werden. Das Verfahren zum Einrichten des Wireless-Netzwerks ist für jeden Kanal identisch.

Hinweis: Für den WAP371 gilt Radio 1 für das 5-GHz-Band und Radio 2 für das 2,4-GHz-Band.

Schritt 20: Geben Sie im Feld Configure Radio 1 - Name Your Wireless Network (Funkmodul 1 konfigurieren - Wireless-Netzwerk benennen) im Feld *Network Name (SSID)* einen Namen für das Wireless-Netzwerk ein, und klicken Sie dann auf **Next (Weiter)**.

Configure Radio 1 - Name Your Wireless Network

The name of your wireless network, known as an SSID, identifies your network so that wireless devices can find it.

Enter a name for your wireless network:

Network Name (SSID):

For example: MyNetwork

[? Learn more about network names](#)

Click **Next** to continue

Hinweis: In diesem Beispiel wird WAP361_L2 als Netzwerkname verwendet.

Schritt 21: Klicken Sie im Bereich Configure Radio 1 - Secure Your Wireless Network (Funkmodul 1 konfigurieren - Ihr Wireless-Netzwerk sichern) auf das Optionsfeld, das der Netzwerksicherheit entspricht, die Sie auf Ihr Wireless-Netzwerk anwenden möchten.

Die Optionen sind wie folgt definiert:

- Best Security (WPA2 Personal - AES): Bietet die beste Sicherheit und wird empfohlen, wenn Ihre Wireless-Geräte diese Option unterstützen. WPA2 Personal verwendet Advanced Encryption Standard (AES) und einen Pre-Shared Key (PSK) zwischen den Clients und dem Access Point. Für jede Sitzung wird ein neuer Verschlüsselungsschlüssel verwendet, was die Kompromittierung erschwert.
- Starke Sicherheit (WPA/WPA2 Personal - TKIP/AES) - Bietet Sicherheit, wenn es ältere Wireless-Geräte gibt, die WPA2 nicht unterstützen. WPA Personal verwendet AES und Temporal Key Integrity Protocol (TKIP). Er verwendet den IEEE 802.11i Wi-Fi-Standard.
- Keine Sicherheit (Nicht empfohlen) - Das Wireless-Netzwerk benötigt kein Kennwort und kann von jedem Benutzer aufgerufen werden. Bei Auswahl dieser Option wird ein Popup-Fenster mit der Frage angezeigt, ob Sie die Sicherheit deaktivieren möchten. Klicken Sie auf **Ja**, um fortzufahren. Wenn diese Option ausgewählt ist, fahren Sie mit [Schritt 24 fort](#).

Configure Radio 1 - Secure Your Wireless 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)

Hinweis: In diesem Beispiel wird Best Security (WPA2 Personal - AES) ausgewählt.

Schritt 22: Geben Sie das Kennwort für Ihr Netzwerk in das Feld *Sicherheitsschlüssel ein*. Die farbige Leiste rechts neben diesem Feld zeigt die Komplexität des eingegebenen Kennworts.

Configure Radio 1 - Secure Your Wireless 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)

Enter a security key with 8-63 characters.

Session Key Refresh Rate

Show Key as Clear Text

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

Schritt 23: (Optional) Um das Kennwort während der Eingabe anzuzeigen, aktivieren Sie das Kontrollkästchen **Schlüssel als Klartext anzeigen**, und klicken Sie dann auf **Weiter**.

Enter a security key with 8-63 characters.

SecretKey1

Weak

Show Key as Clear Text

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

Click **Next** to continue

Back Next Cancel

Schritt 24: Wählen Sie im Bereich Configure Radio 1 - Assign the VLAN ID For Your Wireless Network (Funkmodul 1 konfigurieren - die VLAN-ID für Ihr Wireless-Netzwerk zuweisen) aus der Dropdown-Liste eine ID für das Netzwerk aus. Wenn das Management-VLAN mit dem dem Wireless-Netzwerk zugewiesenen VLAN identisch ist, können Wireless-Clients im Netzwerk das Gerät verwalten. Sie können auch Zugriffskontrolllisten (ACLs) verwenden, um die Administration von Wireless-Clients zu deaktivieren.

Hinweis: Für WAP371 und WAP150 müssen Sie die ID in das angegebene *VLAN-ID*-Feld eingeben. Der Bereich der VLAN-ID liegt zwischen 1 und 4094.

Configure Radio 1 - Assign The VLAN ID For Your Wireless Network

By default, the VLAN ID assigned to the management interface for your access point is 1, which is also the default untagged VLAN ID. If the management VLAN ID is the same as the VLAN ID assigned to your wireless network, then the wireless clients associated with this specific wireless network can administer this device. If needed, an access control list (ACL) can be created to disable administration from wireless clients.

Enter a VLAN ID for your wireless network:

VLAN ID: 1 ▼

[? Learn more about vlan ids](#)

Click **Next** to continue

Back Next Cancel

Hinweis: In diesem Beispiel wird die VLAN-ID 2 verwendet.

Schritt 25: Klicken Sie auf **Weiter**, um mit dem Installationsassistenten zur Konfiguration von Radio 2 fortzufahren.

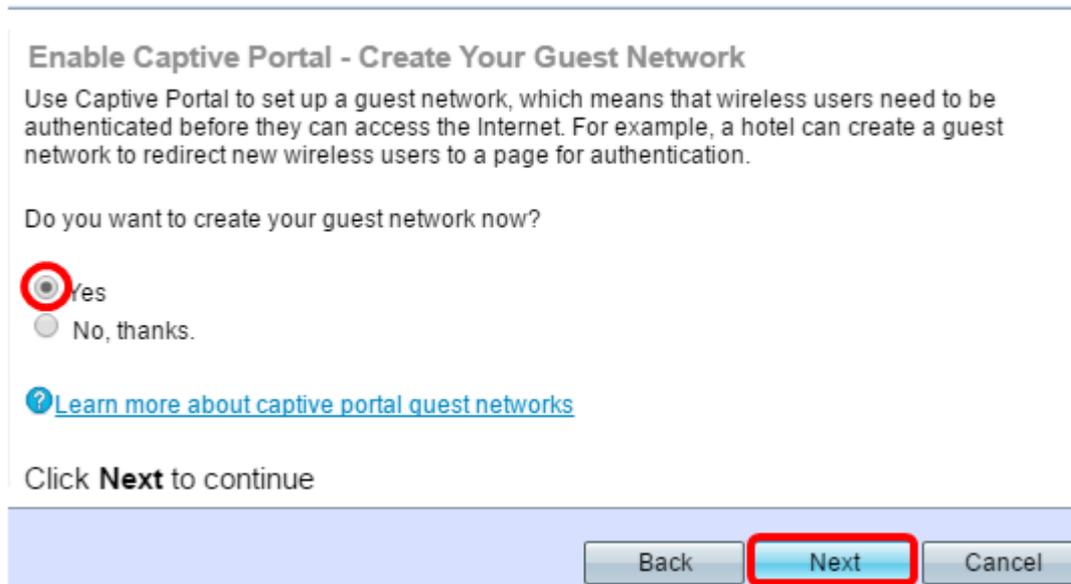
Hinweis: Das Verfahren zum Konfigurieren der Wireless-Netzwerkeinstellungen für Radio 2 ist identisch mit dem Verfahren für Radio 1.

Captive Portal

Captive Portal ermöglicht Ihnen, ein Gastnetzwerk einzurichten, in dem Wireless-Benutzer zuerst authentifiziert werden müssen, bevor sie auf das Internet zugreifen können. Führen Sie die unten stehenden Schritte aus, um Captive Portal zu konfigurieren.

Schritt 26: Wählen Sie im Bereich Enable Captive Portal - Create Your Guest Network (Captive Portal aktivieren - Gastnetzwerk erstellen) das Optionsfeld **Yes (Ja)** aus, und

klicken Sie dann auf **Next (Weiter)**.



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 quest networks](#)

Click **Next** to continue

Back Next Cancel

Hinweis: Wenn Sie Captive Portal nicht aktivieren möchten, klicken Sie auf **Nein**, und der Installationsassistent führt Sie zur Seite Übersicht. Fahren Sie anschließend mit [Schritt 35 fort](#).

Schritt 27: Wählen Sie die gewünschte Funkfrequenz für das Gastnetzwerk aus. Das 2,4-GHz-Band unterstützt ältere Geräte und kann ein breiteres drahtloses Signal über mehrere Wände übertragen. Das 5-GHz-Band hingegen ist weniger ausgelastet und kann einen höheren Durchsatz erzielen, indem es eine 40-MHz-Frequenz des Bands anstatt der 20-MHz-Standardfrequenz im 2,4-GHz-Band aufnimmt. Neben dem kürzeren Bereich sind im Vergleich zu 2,4 GHz auch weniger Geräte für das 5-GHz-Band verfügbar.



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

Guest Network name:
For example: MyGuestNetwork

Hinweis: In diesem Beispiel wird Radio 1 (5 GHz) ausgewählt.

Schritt 28: Geben Sie den Namen der Gast-SSID in das Feld *Gastnetzwerk-Name ein*, und klicken Sie dann auf **Weiter**.

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 (5 GHz)
 Radio 2 (2.4 GHz)

Guest Network name:
 For example: MyGuestNetwork

[? Learn more about network names](#)

Click **Next** to continue

Back Next Cancel

Hinweis: In diesem Beispiel BeMyGuest. wird als Gastnetzwerkname verwendet.

Schritt 29: Klicken Sie auf das Optionsfeld, das der Netzwerksicherheit entspricht, die Sie auf Ihr Wireless-Gastnetzwerk anwenden möchten.

Die Optionen sind wie folgt definiert:

- **Best Security (WPA2 Personal - AES):** Bietet die beste Sicherheit und wird empfohlen, wenn Ihre Wireless-Geräte diese Option unterstützen. WPA2 Personal verwendet AES und einen Pre-Shared Key (PSK) zwischen den Clients und dem Access Point. Für jede Sitzung wird ein neuer Verschlüsselungsschlüssel verwendet, der die Kompromittierung erschwert.
- **Better Security (WPA Personal - TKIP/AES) -** Bietet Sicherheit, wenn es ältere Wireless-Geräte gibt, die WPA2 nicht unterstützen. WPA Personal verwendet AES und TKIP. Er verwendet den IEEE 802.11i Wi-Fi-Standard.
- **Keine Sicherheit (Nicht empfohlen) -** Das Wireless-Netzwerk benötigt kein Kennwort und kann von jedem Benutzer aufgerufen werden. Bei Auswahl dieser Option wird ein Popup-Fenster mit der Frage angezeigt, ob Sie die Sicherheit deaktivieren möchten. klicken Sie auf **Ja**, um fortzufahren. Wenn diese Option ausgewählt ist, klicken Sie auf **Weiter** und fahren Sie dann mit [Schritt 35 fort](#).

Hinweis: In diesem Beispiel wird Better Security (WPA Personal - TKIP/AES) ausgewählt.

Enable Captive Portal - Secure Your Guest Network

Select your guest 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)

Schritt 30: Geben Sie das Kennwort für Ihr Netzwerk in das Feld *Sicherheitsschlüssel ein*. Die farbige Leiste rechts neben diesem Feld zeigt die Komplexität des eingegebenen

Kennworts.

Enter a security key with 8-63 characters.

..... Strong

Show Key as Clear Text

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

Click **Next** to continue

Back Next Cancel

Schritt 31: (Optional) Um das Kennwort während der Eingabe anzuzeigen, aktivieren Sie das Kontrollkästchen **Schlüssel als Klartext anzeigen**, und klicken Sie dann auf **Weiter**.

Enter a security key with 8-63 characters.

GuestPassw0rd Strong

Show Key as Clear Text

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

Click **Next** to continue

Back Next Cancel

Schritt 32: Wählen Sie in der Dropdown-Liste Enable Captive Portal - Assign the VLAN ID area (Captive Portal aktivieren - VLAN-ID-Bereich zuweisen) eine ID für das Gastnetzwerk aus, und klicken Sie dann auf **Next (Weiter)**.

Hinweis: Für WAP371 und WAP150 müssen Sie die ID in das angegebene *VLAN-ID*-Feld eingeben. Der Bereich der VLAN-ID liegt zwischen 1 und 4094.

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: 2 ▼

[? Learn more about vlan ids](#)

Click **Next** to continue

Back Next Cancel

Hinweis: In diesem Beispiel wird die VLAN-ID 2 ausgewählt.

Schritt 33: (Optional) Wenn neue Benutzer zu einer alternativen Startseite umgeleitet werden sollen, aktivieren Sie das Kontrollkästchen **Umleitung aktivieren** im Bildschirm Enable Captive Portal - Enable Redirect URL (Umleiten-URL aktivieren).

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 :

Schritt 34: (Optional) Geben Sie die URL für Ihre Umleitungs-URL in das Feld *Umleiten-URL* ein, und klicken Sie dann auf **Weiter**.

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

Hinweis: In diesem Beispiel wird <http://newuser.com> als Redirect URL verwendet.

Zusammenfassung

Schritt 35: Überprüfen Sie die angezeigten Einstellungen, und stellen Sie sicher, dass die Informationen korrekt sind. Wenn Sie eine Einstellung ändern möchten, klicken Sie auf die **Zurück**-Schaltfläche, bis die gewünschte Seite angezeigt wird. Andernfalls klicken Sie auf **Senden**, um die Einstellungen auf dem WAP zu aktivieren.

Summary - Confirm Your Settings

Please review the following settings and ensure the data is correct.

Radio 1 (2.4 GHz)

| | |
|------------------------|---------------------|
| Network Name (SSID): | WAP361_L2 |
| Network Security Type: | WPA2 Personal - AES |
| Security Key: | SecretKey1 |
| VLAN ID: | 1 |

Radio 2 (5 GHz)

| | |
|------------------------|---------------------|
| Network Name (SSID): | WAP361_L 2 _5ghz |
| Network Security Type: | WPA2 Personal - AES |
| Security Key: | SecretKey2 |
| VLAN ID: | 1 |

Captive Portal (Guest Network) Summary

| | |
|----------------------|---------------------|
| Guest Network Radio: | Radio 1 |
| Network Name (SSID): | BeMyGuest! |
| Network Security | WPA2 Personal - AES |

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

Schritt 36: Der Bildschirm Device Setup Complete (Geräte-Setup abgeschlossen) wird angezeigt, um zu bestätigen, dass das Gerät erfolgreich eingerichtet wurde. Klicken Sie auf **Fertig stellen**.

Device Setup Complete

Congratulations, your access point has been set up successfully. We strongly recommend that you save these settings by writing them down or by copying and pasting them into a text document. You will need these settings later when you add other wireless computers or devices to your network.

Cluster Name: ciscosb-cluster

Radio 1 (2.4 GHz)

| | |
|------------------------|---------------------|
| Network Name (SSID): | WAP361_L2 |
| Network Security Type: | WPA2 Personal - AES |
| Security Key: | SecretKey1 |

Radio 2 (5 GHz)

| | |
|------------------------|---------------------|
| Network Name (SSID): | WAP361_L 2 _5ghz |
| Network Security Type: | WPA2 Personal - AES |
| Security Key: | SecretKey2 |



Click **Finish** to close this wizard.

Sie sollten jetzt den Wireless Access Point mithilfe des Installationsassistenten erfolgreich konfiguriert haben.