

Konfiguration des Einrichtungsassistenten auf dem WAP551

Ziel

Der Installationsassistent besteht aus interaktiven Anweisungen, die Sie durch die Erstkonfiguration des WAP551 führen. Diese Anleitungen beziehen sich auf die grundlegenden Konfigurationen, die für den Betrieb des WAP551 erforderlich sind. Das Fenster *Access Point Setup Wizard (Access Point-Einrichtungsassistent)* wird bei der ersten Anmeldung am WAP automatisch angezeigt. Es kann jedoch jederzeit verwendet werden.

In diesem Artikel wird erläutert, wie der WAP551 mithilfe des Setup-Assistenten konfiguriert wird.

Anwendbare Geräte

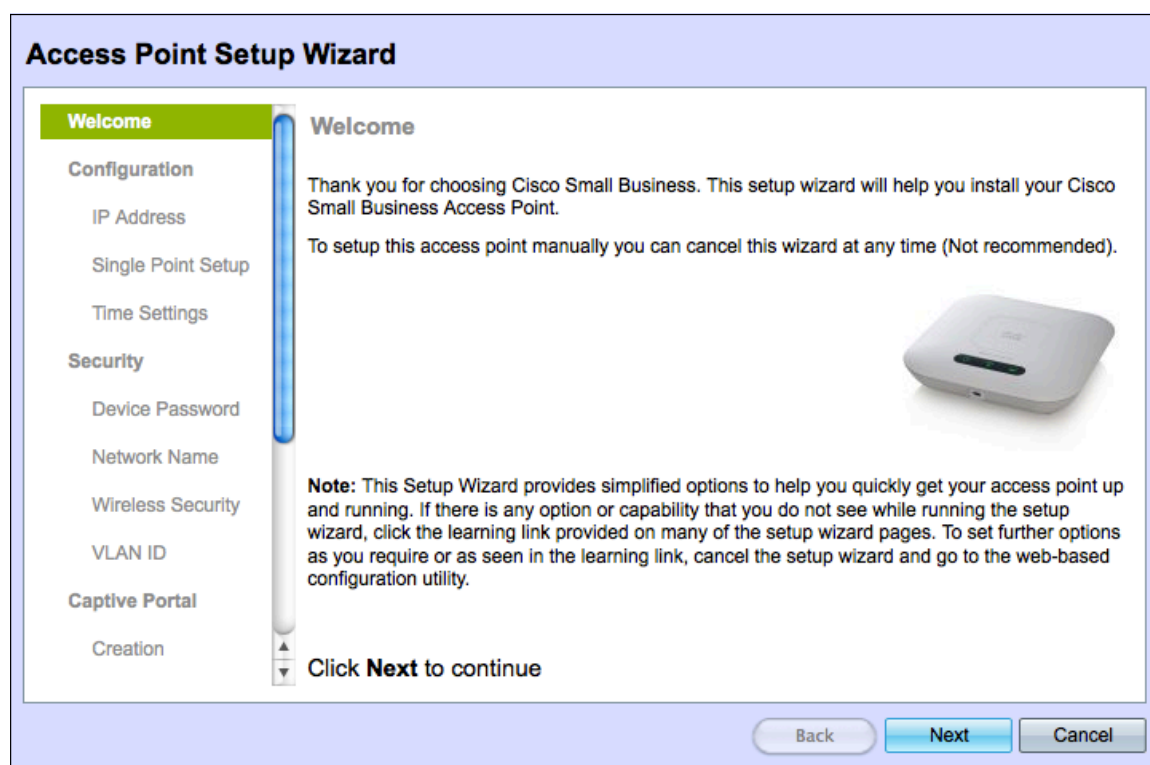
WAP551

Softwareversion

·v1.0.4.2

Einrichtungsassistent konfigurieren

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Setup Wizard (Installationsassistent ausführen)** aus. Das Fenster *Access Point Setup Wizard (Assistent für Access Point-Einrichtung)* wird angezeigt.



Schritt 2: Klicken Sie auf **Weiter**, um fortzufahren. Die Seite *Gerät konfigurieren - IP-Adresse* wird geöffnet:

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

·Dynamische IP-Adresse (DHCP) (empfohlen) - Die IP-Adresse des WAP wird von einem DHCP-Server zugewiesen. Wenn Sie Dynamic IP Address (Dynamische IP-Adresse) auswählen, fahren Sie 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.

Schritt 4: Geben Sie im Feld Static IP Address (Statische IP-Adresse) die IP-Adresse des WAP ein. Diese IP-Adresse wird von Ihnen erstellt und sollte nicht von einem anderen Gerät im Netzwerk verwendet werden.

Schritt 5: Geben Sie im Feld Subnetzmaske die Subnetzmaske der IP-Adresse ein.

Schritt 6: Geben Sie im Feld Default Gateway (Standard-Gateway) die IP-Adresse des Standard-Gateways für den WAP ein. Das Standard-Gateway ist in der Regel die private IP-Adresse, die dem Router zugewiesen ist.

Schritt 7: Geben Sie in das DNS-Feld die IP-Adresse des DNS-Servers (Primary Domain Name System) ein. Wenn Sie auf Webseiten außerhalb Ihres Netzwerks zugreifen möchten, sollte die IP-Adresse des DNS-Servers von Ihrem Internetdienstanbieter (Internet Service Provider, ISP) angegeben werden.

Schritt 8: (Optional) Geben Sie im Feld *Sekundärer DNS* die IP-Adresse des sekundären DNS ein.

Schritt 9: Klicken Sie auf **Weiter**, um fortzufahren. Die Seite *"Single Point Setup - Set a Cluster"* (*Single-Point-Einrichtung - Cluster einrichten*) wird geöffnet:

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.

Create a New Cluster

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.

Click **Next** to continue

Schritt 10: Klicken Sie auf das Optionsfeld für die Cluster-Einstellungen, die Sie verwenden möchten. Mit einem Cluster können Sie mehrere Access Points (APs) als ein Gerät konfigurieren. Wenn Sie sich dafür entscheiden, keinen Cluster zu verwenden, müssen Sie diese einzeln konfigurieren.

·Neuen Cluster erstellen - Erstellen Sie einen neuen Cluster für APs.

·Einem vorhandenen Cluster beitreten - Verbindet sich mit einem vorhandenen AP-Cluster in Ihrem Netzwerk.

·Single-Point-Einrichtung nicht aktivieren - Single-Point-Einrichtung (Cluster) ist nicht zulässig. Fahren Sie mit Schritt 13 fort, wenn Sie diese Option auswählen.

Schritt 11: Geben Sie im Feld *Cluster-Name* entweder einen vorhandenen Cluster-Namen ein, oder erstellen Sie einen neuen Cluster-Namen, der auf Ihrer Entscheidung in Schritt 10 basiert.

Schritt 12: Geben Sie im Feld "AP Location" (AP-Standort) den physischen Standort des WAP ein.

Timesaver: Wenn Sie auf das Optionsfeld An bestehendem Cluster hinzufügen geklickt haben, konfiguriert der WAP die übrigen Einstellungen basierend auf dem Cluster. Klicken Sie auf **Weiter**, um eine Bestätigungsseite anzuzeigen und zu fragen, ob Sie dem Cluster sicher beitreten möchten. Klicken Sie auf **Senden**, um dem Cluster beizutreten. Wenn die Konfiguration abgeschlossen ist, klicken Sie auf **Fertig stellen**, um den Installationsassistenten zu beenden.

Schritt 13: Klicken Sie auf **Weiter**, um fortzufahren. Die Seite *Gerät konfigurieren - Systemdatum und -zeit festlegen* wird geöffnet:

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:

[? Learn more about time settings](#)

Click **Next** to continue

Schritt 14: Wählen Sie aus der Dropdown-Liste *Time Zone* eine Zeitzone aus.

Schritt 15: Klicken Sie auf das Optionsfeld, das der Methode entspricht, mit der Sie die Uhrzeit des WAP festlegen möchten.

- Network Time Protocol (NTP) - Der WAP erhält die Zeit von einem NTP-Server.
- Manuell — Die Uhrzeit wird manuell in den WAP eingegeben. Wenn Sie die Option manuell auswählen, fahren Sie mit Schritt 17 fort.

Schritt 16: Geben Sie im Feld *NTP-Server* die URL des NTP-Servers ein, der das Datum und die Uhrzeit angibt. Fahren Sie mit Schritt 19 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:

[? Learn more about time settings](#)

Click **Next** to continue

Schritt 17: Wählen Sie aus den Dropdown-Listen *Systemdatum* den Monat, den Tag bzw. das Jahr aus.

Schritt 18: Wählen Sie aus den Dropdown-Listen *Systemzeit* die Stunde bzw. Minuten aus.

Schritt 19: Klicken Sie auf **Weiter**, um fortzufahren. Die Seite *Sicherheit aktivieren - Kennwort festlegen* wird geöffnet:

Enable Security - Set Password


The administrative password protects your access point from unauthorized access. For security reasons, you should change the access point password from its default settings. Please write this password down for future reference.

Enter a new device password:

New password needs at least 8 characters composed of lower and upper case letters as well as numbers/symbols by default.

New Password:

Confirm Password:

Password Strength Meter:  Strong

Password Complexity: Enable

[? Learn more about passwords](#)

Click **Next** to continue

Schritt 20: Geben Sie im Feld *Neues Kennwort* ein neues Kennwort ein. Dies ist das Kennwort, mit dem Sie administrativen Zugriff auf den WAP erhalten.

Schritt 21: Geben Sie im Feld *Kennwort bestätigen* dasselbe Kennwort erneut ein.

Hinweis: Wenn Sie ein Kennwort eingeben, ändert sich die Anzahl und Farbe der vertikalen Balken, um die Kennwortstärke anzugeben:

- Rot: Das Kennwort erfüllt nicht die Mindestanforderungen an die Komplexität.
- Orange - Das Kennwort erfüllt die minimalen Komplexitätsanforderungen, aber die Kennwortstärke ist schwach.
- Grün - Das Kennwort ist stark.

Schritt 22: (Optional) Um die Komplexität von Kennwörtern zu aktivieren, aktivieren Sie das Kontrollkästchen **Aktivieren**. Das Kennwort muss mindestens 8 Zeichen lang sein und aus Groß- und Kleinbuchstaben sowie Zahlen und Symbolen bestehen.

Schritt 23: Klicken Sie auf **Weiter**, um fortzufahren. Die Seite *Sicherheit aktivieren - Wireless-Netzwerk benennen* wird geöffnet:

Enable Security - 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

Schritt 24: Geben Sie im Feld Network Name (SSID) (Netzwerkname (SSID)) die Service Set Identification (SSID) des Wireless-Netzwerks ein. Der SSID ist der Name des Wireless Local Area Network.

Schritt 25: Klicken Sie auf **Weiter**, um fortzufahren. Die Seite *Sicherheit aktivieren - Wireless-Netzwerk sichern* wird geöffnet.

Enable Security - 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 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.

 Strong

Show Key as Clear Text

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

Click **Next** to continue

Schritt 26: Klicken Sie auf das Optionsfeld für die Netzwerksicherheit, die Sie auf Ihr Wireless-Netzwerk anwenden möchten.

·Best Security (WPA2 Personal - AES) - WPA2 ist die zweite Version der WPA-Sicherheits- und Zugriffskontrolltechnologie für Wi-Fi-Wireless-Netzwerke, die AES-CCMP-

Verschlüsselung enthält. Diese Protokollversion bietet die beste Sicherheit gemäß IEEE 802.11i-Standard. Alle Client-Stationen im Netzwerk müssen WPA2 unterstützen können. WPA2 erlaubt keine Verwendung des Protokolls TKIP (Temporal Key Integrity Protocol), das bekannte Einschränkungen aufweist.

·Better Security (WPA Personal - TKIP/AES) - WPA Personal ist ein IEEE 802.11i-Standard der Wi-Fi Alliance, der AES-CCMP- und TKIP-Verschlüsselung umfasst. Sie bietet Sicherheit, wenn ältere Wireless-Geräte das ursprüngliche WPA unterstützen, die neuere WPA2 jedoch nicht unterstützen.

·Keine Sicherheit - Das Wireless-Netzwerk benötigt kein Kennwort und kann von jedem verwendet werden. Wenn Sie No Security (Keine Sicherheit) auswählen, fahren Sie mit Schritt 29 fort.

Schritt 27: Geben Sie im Feld Sicherheitsschlüssel das Kennwort für Ihr Netzwerk ein.

Schritt 28: (Optional) Um das Kennwort während der Eingabe anzuzeigen, aktivieren Sie das Kontrollkästchen **Schlüssel als Text löschen**.

Schritt 29: Klicken Sie auf **Weiter**, um fortzufahren. Die Seite *Sicherheit aktivieren - Zuweisen der VLAN-ID für Ihr Wireless-Netzwerk* wird geöffnet.

Enable Security - 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: (Range: 1 - 4094)

[? Learn more about vlan ids](#)

Click **Next** to continue

Schritt 30: Geben Sie im Feld VLAN ID (VLAN-ID) die ID-Nummer des VLAN ein, zu dem der WAP gehören soll.

Hinweis: Die VLAN-ID muss mit einer der VLAN-IDs übereinstimmen, die auf dem Port des Remote-Geräts unterstützt wird, das mit dem WAP verbunden ist.

Schritt 31: Klicken Sie auf **Weiter**, um fortzufahren. Die Seite *Enable Captive Portal - Create Your Guest Network* (Captive Portal aktivieren - Gastnetzwerk erstellen) wird geöffnet:

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

Schritt 32: Klicken Sie auf das Optionsfeld **Ja**, wenn Sie ein Gastnetzwerk erstellen möchten. Bei einem Gastnetzwerk müssen Benutzer authentifiziert werden, bevor sie das Internet nutzen können. Ein Gastnetzwerk ist nicht erforderlich. Klicken Sie auf das Optionsfeld **Nein**, wenn Sie kein Gastnetzwerk erstellen möchten, und fahren Sie mit Schritt 45 fort.

Schritt 33: Klicken Sie auf **Weiter**, um fortzufahren. Die Seite *Enable Captive Portal - Name Your Guest Network (Captive Portal aktivieren - Gastnetzwerk benennen)* wird geöffnet:

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:

Guest Network name:

For example: MyGuestNetwork

[? Learn more about network names](#)

Click **Next** to continue

Schritt 34: Geben Sie im Feld Guest Network name (Gastnetzwerk) die SSID des Gastnetzwerks ein.

Schritt 35: Klicken Sie auf **Weiter**, um fortzufahren. Die Seite *Enable Captive Portal - Secure Your Guest Network* wird geöffnet:

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 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.



Show Key as Clear Text

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

Click **Next** to continue

Schritt 36: Klicken Sie auf das Optionsfeld für die Netzwerksicherheit, die Sie auf Ihr Gastnetzwerk anwenden möchten.

·Optimale Sicherheit (WPA2 Personal - AES) - Bietet die beste Sicherheit und wird empfohlen, wenn Ihre Wireless-Geräte diese Option unterstützen.

·Bessere Sicherheit - Bietet Sicherheit, wenn ältere Wireless-Geräte WPA2 nicht unterstützen.

·Keine Sicherheit - Das Wireless-Netzwerk benötigt kein Kennwort und kann von jedem verwendet werden. Wenn Sie No Security (Keine Sicherheit) auswählen, fahren Sie mit Schritt 39 fort.

Schritt 37: Geben Sie im Feld Sicherheitsschlüssel das Kennwort für das Gastnetzwerk ein.

Schritt 38: (Optional) Um das Kennwort während der Eingabe anzuzeigen, aktivieren Sie das Kontrollkästchen **Schlüssel als Klartext anzeigen**.

Schritt 39: Klicken Sie auf **Weiter**, um fortzufahren. Die Seite *Enable Captive Portal - Assign The VLAN ID* (Captive Portal aktivieren - VLAN-ID zuweisen) wird geöffnet:

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

Schritt 40: Geben Sie im Feld VLAN ID (VLAN-ID) die ID-Nummer des VLAN ein, zu dem das Gastnetzwerk gehören soll.

Hinweis: Die VLAN-ID muss mit einer der VLAN-IDs übereinstimmen, die auf dem Port des Remote-Geräts unterstützt wird, das mit dem WAP verbunden ist.

Schritt 41: Klicken Sie auf **Weiter**, um fortzufahren. Die Seite *Enable Captive Portal - Enable Redirect URL* wird geöffnet:

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

Schritt 42: (Optional) Um Wireless-Benutzer nach der Anmeldung beim Gastnetzwerk auf eine Webseite umzuleiten, aktivieren Sie das Kontrollkästchen **Enable Redirect URL** (Umleiten-URL aktivieren).

Zeitgeber: Wenn Sie das Kontrollkästchen **Aktivieren** nicht aktivieren, fahren Sie mit Schritt 44 fort.

Schritt 43: Geben Sie im Feld "Redirect URL" (URL umleiten) die Webseite ein, auf die Benutzer umgeleitet werden sollen, nachdem sie sich beim Gastnetzwerk angemeldet haben.

Schritt 44: Klicken Sie auf **Weiter**, um fortzufahren. Die Seite *Zusammenfassung - Einstellungen bestätigen* wird geöffnet:

Summary - Confirm Your Settings

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

Network Name (SSID):	ciscosb
Network Security Type:	plain-text
Security Key:	
VLAN ID:	1

Captive Portal (Guest Network) Summary

Network Name (SSID):	Guest
Network Security Type:	WPA2 Personal - AES
Security Key:	*****
Verification:	Guest
Redirect URL:	http://www.example.com
VLAN ID:	5

Note: The AP Radio will be enabled after clicking Submit.

Click **Submit** to enable settings on your Cisco Small Business Access Point


Schritt 45: (Optional) Um eine von Ihnen gewählte Einstellung zu bearbeiten, klicken Sie auf **Zurück**.

Schritt 46: (Optional) Wenn Sie den Installationsassistenten beenden und alle vorgenommenen Änderungen rückgängig machen möchten, klicken Sie auf **Abbrechen**.

Schritt 47: Überprüfen Sie die Netzwerk- und Gastnetzwerkeinstellungen. Klicken Sie auf **Senden**, um die Einstellungen auf dem WAP zu aktivieren. Eine Ladeleiste wird angezeigt, wenn der WAP Ihre Einstellungen aktiviert. Wenn der WAP abgeschlossen ist, wird die Seite *Beenden* geöffnet:

Hinweis: Schritt 48 ist nur anwendbar, wenn Sie auf der Seite *Einstellungen bestätigen* auf **Senden** klicken.

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
Network Name (SSID):	ciscosb
Network Security Type:	plain-text
Security Key:	



Note: To configure WPS, Click "Run WPS" on the Getting Started page, under Initial Setup.

Click **Finish** to close this wizard.

Back

Finish

Cancel

Schritt 48: Klicken Sie auf **Fertig stellen**, um den Installationsassistenten zu beenden.