

# Configuração inicial dos pontos de acesso Wireless WAP150, WAP351, WAP361, e WAP371 usando o assistente de configuração

## Objetivo

O assistente de configuração é uma característica incorporado que seja usada para ajudar com a configuração inicial dos pontos de acesso Wireless (WAP). Faz a configuração das configurações básicas fácil. O processo passo a passo do assistente de configuração guia-o com a instalação inicial do dispositivo WAP, e fornece-o uma maneira rápida obter os recursos básicos do WAP funcionais.

O objetivo deste documento é mostrar-lhe como configurar os pontos de acesso Wireless WAP150, WAP351, WAP361, e WAP371 usando o assistente de configuração.

## Dispositivos aplicáveis

- WAP150
- WAP351
- WAP361
- WAP371

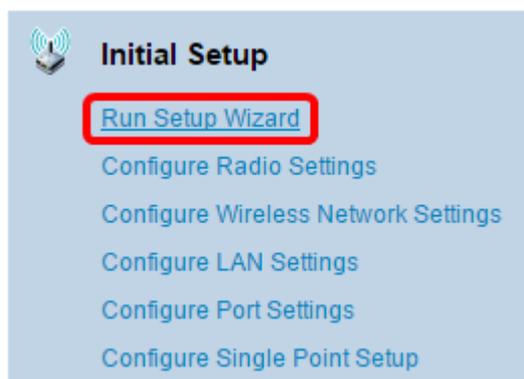
## Versão de software

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

## Configuração

**Nota:** As imagens usadas abaixo são tomadas de WAP361.

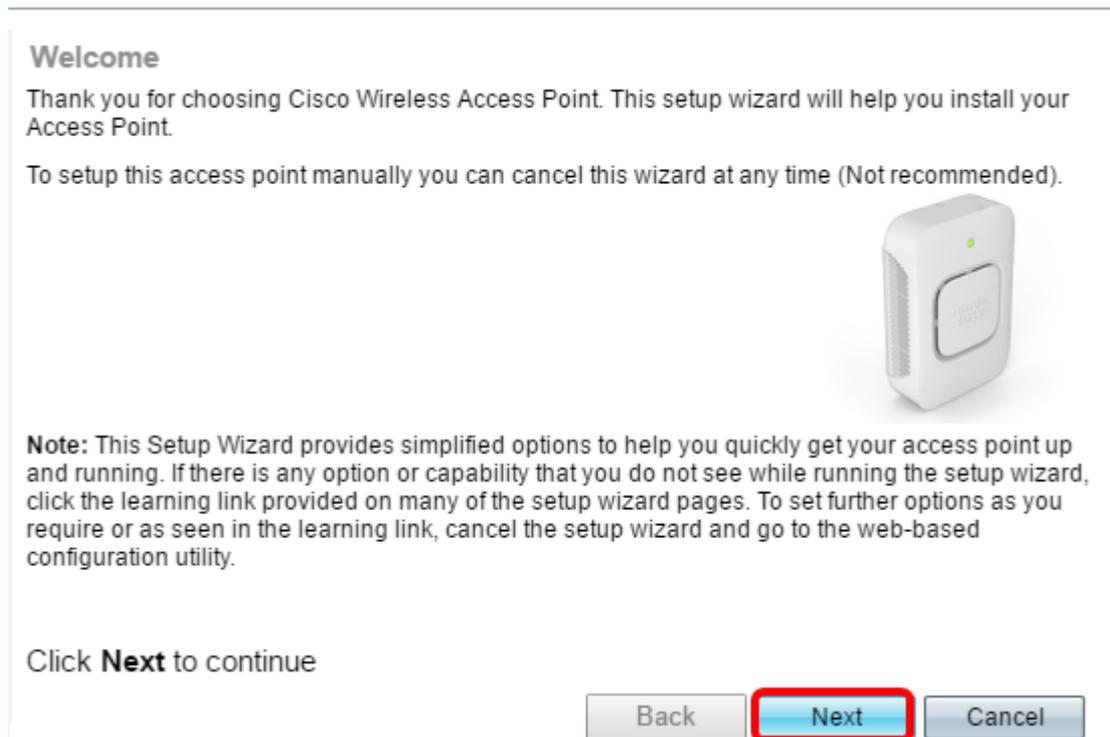
Etapa 1. Início de uma sessão à utilidade com base na Web do Access point. Sob a obtenção começou a página do menu, **assistente de configuração da corrida do clique.**



**Nota:** Se isto é a primeira vez você entrou ao WAP, o assistente de configuração abrirá automaticamente.

Etapa 2. Clique **em seguida** na página de boas-vindas do assistente de configuração do

Access point para continuar.



Etapa 3. Clique o botão de rádio que corresponde ao método que você quer se usar para determinar o endereço IP de Um ou Mais Servidores Cisco ICM NT do WAP.

As opções são definidas como segue:

- O endereço IP dinâmico (DHCP) (recomendado) — permite que o servidor DHCP atribua um endereço IP dinâmico para o WAP. Se você escolhe este, clique **em seguida** então a faixa clara [para pisar 9](#).
- Endereço IP estático — Permite que você crie um endereço IP de Um ou Mais Servidores Cisco ICM NT (estático) fixo para o WAP. Um endereço IP estático não muda.

**Nota:** Neste exemplo, o endereço IP dinâmico (DHCP) é escolhido.

### 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

Etapa 4. Se o endereço IP estático foi escolhido na etapa precedente, incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do WAP ao campo de *endereço IP estático*. Este endereço IP de Um ou Mais Servidores Cisco ICM NT é original ao WAP e não deve ser usado por um outro dispositivo na rede.

Dynamic IP Address (DHCP) (Recommended)

Static IP Address

Static IP Address:  .  .  .

Subnet Mask:  .  .  .

Default Gateway:  .  .  .

DNS:  .  .  .

Secondary DNS (optional):  .  .  .

**Nota:** Neste exemplo, 192.168.1.121 é usado como o endereço IP estático.

Etapa 5. Incorpore a máscara de sub-rede ao campo da *máscara de sub-rede*.

Dynamic IP Address (DHCP) (Recommended)

Static IP Address

Static IP Address:  .  .  .

Subnet Mask:  .  .  .

Default Gateway:  .  .  .

DNS:  .  .  .

Secondary DNS (optional):  .  .  .

**Nota:** Neste exemplo, 255.255.255.0 é usado como a máscara de sub-rede.

Etapa 6. Inscreva o gateway padrão para o WAP no campo do *gateway padrão*. Este é o endereço IP privado de seu roteador.

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

Static IP Address: 192 . 168 . 1 . 121  
Subnet Mask: 255 . 255 . 255 . 0  
Default Gateway: 192 . 168 . 1 . 1  
DNS: . . . .  
Secondary DNS (optional): . . . .

**Nota:** Neste exemplo, 192.168.1.1 é usado como o gateway padrão.

Etapa 7. (opcional) se você quer alcançar a parte externa de serviço público com base na Web de sua rede, incorpora o endereço preliminar do Domain Name System (DNS) ao campo *DNS*. Seu provedor de serviço do Internet (ISP) deve fornecer o endereço de servidor de DNS a você.

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

Static IP Address: 192 . 168 . 1 . 121  
Subnet Mask: 255 . 255 . 255 . 0  
Default Gateway: 192 . 168 . 1 . 1  
DNS: 192 . 168 . 1 . 2  
Secondary DNS (optional): . . . .

**Nota:** Neste exemplo, 192.168.1.2 é usado como o endereço DNS.

Etapa 8. (opcional) incorpora um endereço dos DN secundários aos campos dos *DN secundários* a seguir clica-o **em seguida**.

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

Static IP Address: 192 . 168 . 1 . 121  
Subnet Mask: 255 . 255 . 255 . 0  
Default Gateway: 192 . 168 . 1 . 1  
DNS: 192 . 168 . 1 . 2  
Secondary DNS (optional): 192 . 168 . 1 . 3

**Nota:** Neste exemplo, 192.168.1.3 é usado como o endereço dos DN secundários.

## Única instalação do ponto

**Etapa 9.** No único ponto Setup – Ajuste uma tela do conjunto, selecione um botão de rádio que corresponda a como você quer configurar os ajustes do conjunto do WAP. Aglomerar-se permite que você controle pontos de acesso múltiplo de um único ponto, em vez de ir a cada dispositivo e de mudar os ajustes individualmente.

As opções são definidas como segue:

- Nome de grânulos novo — Selecione esta opção se você quer criar um conjunto novo.

**Nota:** Para WAP351 e WAP371, a opção é cria um conjunto novo.

- Junte-se a um conjunto existente — Selecione esta opção se você quer o WAP se juntar a um conjunto existente. Se você escolhe esta opção, salte a [etapa 11](#).
- Não permita o único ponto de setup — Escolha esta opção se você não quer o WAP ser parte de um conjunto. Se você escolhe esta opção, clique **em seguida** então a faixa clara a [etapa 13](#).

**Nota:** Neste exemplo, não permita o único ponto de setup é escolhido.

**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

Etapa 10. Se você escolheu o nome de grânulos novo na etapa precedente, dê entrada com o nome do conjunto novo e seu lugar nos campos *novos do nome de grânulos* e *do lugar AP*, respectivamente clica então **em seguida**. O lugar AP é o local físico do Access point definido pelo usuário (por exemplo escritório). Vá a [Step13](#).

**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

**Etapa 11.** Se você escolheu **junte-se a um conjunto existente** na etapa 9, dão entrada com o nome do conjunto e seu lugar nos campos do *nome do conjunto existente* e do *lugar AP*, respectivamente clica então **em seguida**.

**Nota:** Esta opção é ideal se há já uma rede Wireless existente e todos os ajustes têm sido configurados já.

**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

**Etapa 12.** Reveja seus ajustes para certificar-se que os dados estão corretos clicam então **se submetem**.

**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

## Configurações de tempo

[Etapa 13](#). Escolha sua zona de hora (fuso horário) da lista de drop-down da zona de hora (fuso horário).

**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)**

NTP Server 1:      Uzbekistan  
NTP Server 2:      Vanuatu  
NTP Server 3:      Vatican City  
NTP Server 4:      Venezuela  
Vietnam  
Wake Islands  
Wallis & Futana Islands  
Western Samoa  
Windward Islands  
Yemen  
Zaire (Kasai)  
Zaire (Kinshasa)  
Zambia  
Zimbabwe

[? Learn more about t](#)

Click **Next** to continue

Back    **Next**    Cancel

**Nota:** Neste exemplo, o USA (pacífico) é escolhido.

Etapa 14. Clique o botão de rádio que corresponde ao método que você deseja se usar para ajustar a época do WAP.

As opções são como segue:

- Network Time Protocol (NTP) — O WAP obtém o tempo de um servidor de NTP.
- Manualmente — O tempo é incorporado manualmente no WAP. Se esta opção é escolhida, salte a [etapa 16](#).

**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

**Nota:** Neste exemplo, o Network Time Protocol (NTP) é usado.

Etapa 15. Incorpore o Domain Name do servidor de NTP que fornece a data e hora no campo do *servidor de NTP 1*. Você pode adicionar acima a quatro servidores de NTP diferentes inscrevendo os em seus campos respectivos e então clicar **em seguida**. Então, faça clara a [etapa 17](#).

**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

**Nota:** Neste exemplo, há quatro servidores de NTP entrados.

[Etapa 16](#). (Opcional) se você escolheu manualmente em etapa 14, selecione a data nas listas de drop-down da data do sistema para escolher o mês, o dia, e o ano respectivamente. Selecione a hora e os minutos das listas de drop-down do tempo de sistema a seguir clicam **em seguida**.

**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

## Senha do dispositivo

**Etapa 17.** In o dispositivo configurar - Ajuste a tela da senha, incorpore uma senha nova para o WAP ao campo de *senha novo* e confirme-a. Esta senha é usada para ganhar o acesso administrativo à utilidade com base na Web do WAP próprio e não para conectar à rede Wireless.

New Password:

Confirm Password:

Password Strength Meter:  Below Minimum

**Nota:** O campo do *medidor da força da senha* indica as varras vertical que mudam enquanto você incorpora a senha.

As cores do medidor da força da senha são definidas como segue:

- Vermelho — O requisito de complexidade mínimo da senha não é cumprido.
- Alaranjado — O requisito de complexidade mínimo da senha é cumprido, mas a força da senha é fraca.
- Verde — O requisito de complexidade mínimo da senha é cumprido, e a força da senha é forte.

**Etapa 18.** (Opcional) permita a complexidade da senha verificando a caixa de verificação da complexidade da senha da **possibilidade**. Isto exige que a senha é pelo menos 8 caracteres por muito tempo e composto letras de umas mais baixas e de caixa e de uns números ou de uns símbolos. A complexidade da senha é permitida à revelia.

New Password:

Confirm Password:

Password Strength Meter:  Below Minimum

Password Complexity:  Enable

[? Learn more about passwords](#)

Click **Next** to continue

Etapa 19. Clique em Avançar para continuar.

## Configurar transmite por rádio 1 e 2 (2.4 e os gigahertz 5)

Os ajustes da rede Wireless devem ser configurados individualmente para cada canal de rádio. O processo para estabelecer a rede Wireless é o mesmo para cada canal.

**Nota:** Para o WAP371, o rádio 1 é para a faixa gigahertz 5 e o rádio 2 é para a faixa 2.4 gigahertz.

Etapa 20. No rádio 1 configurar - Nomeie sua área da rede Wireless, dê entrada com um nome para a rede Wireless no campo do *nome de rede (SSID)* a seguir clique-o **em seguida**

**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

**Nota:** Neste exemplo, WAP361\_L2 é usado como o nome de rede.

Etapa 21. No rádio 1 configurar - Fixe sua área da rede Wireless, clique o botão de rádio que corresponde com a segurança de rede que você gostaria de se aplicar a sua rede Wireless.

As opções são definidas como segue:

- A melhor Segurança (WPA2 pessoal - AES) — fornece a melhor Segurança e é recomendado se seus dispositivos Wireless apoiam esta opção. Advanced Encryption Standard (AES) pessoal dos usos WPA2 e uma chave pré-compartilhada (PSK) entre os clientes e o Access point. Usa uma chave de criptografia nova para cada sessão, que faz difícil comprometer.
- Melhor Segurança (WPA/WPA2 pessoais - TKIP/AES) — fornece a Segurança quando há uns dispositivos Wireless mais velhos que não apoiem o WPA2. Usos pessoais AES WPA e Temporal Key Integrity Protocol (TKIP). Usa o padrão do Wi-fi da IEEE 802.11i.
- Nenhuma Segurança (não recomendada) — A rede Wireless não exige uma senha e pode ser alcançada por qualquer um. Se escolhida, uma janela pop-up aparecerá perguntando se você quer desabilitar a Segurança; clique **sim** para continuar. Se esta opção é escolhida, salte a [etapa 24](#).

### 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)

**Nota:** Neste exemplo, a melhor Segurança (WPA2 pessoal - AES) é escolhida.

Etapa 22. Incorpore a senha para sua rede ao campo de *chave de segurança*. A barra colorida à direita deste campo mostra a complexidade da senha incorporada.

### 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](#)

Etapa 23. (Opcional) para ver a senha como você datilografa, verifique a **chave da mostra como a caixa de verificação do texto claro** a seguir clique-a **em seguida**.

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

Etapa 24. No rádio 1 configurar - Atribua O ID de VLAN para sua área da rede Wireless, escolha um ID para a rede da lista de drop-down do ID de VLAN. Se o VLAN de gerenciamento é o mesmo que o VLAN atribuído à rede Wireless, os clientes Wireless na rede podem administrar o dispositivo. Você pode igualmente usar as listas de controle de acesso (ACL) para desabilitar a administração dos clientes Wireless.

**Nota:** Para WAP371 e WAP150, você precisa de datilografar dentro o ID no campo do *ID de VLAN* fornecido. A escala do ID de VLAN é de 1-4094.

### 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

**Nota:** Neste exemplo, o ID de VLAN 1 é usado.

Etapa 25. O clique **ao lado** do continua com o assistente de configuração configurar o rádio 2.

Nota: O processo para configurar ajustes da rede Wireless para o rádio 2 é o mesmo que aquele do rádio 1.

## Portal prisioneiro

O portal prisioneiro permite que você estabeleça uma rede de convidado onde necessidade de usuários Wireless de ser autenticado primeiramente antes que puderem ter o acesso ao Internet. Siga as etapas abaixo para configurar o portal prisioneiro.

Etapa 26. No portal prisioneiro da possibilidade - Crie sua área da rede de convidado, escolha o **botão Yes Radio Button** a seguir clique-o **em seguida**.

**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

**Nota:** Se você prefere não permitir o portal prisioneiro, clique o **nenhum** e o assistente de configuração tomá-lo-á à página de sumário. Então, faça uma referência a [etapa 35](#).

Etapa 27. Selecione a frequência de rádio desejada para a rede de convidado. O apoio de 2.4 ofertas da faixa gigahertz para dispositivos legado e pode propagar um sinal wireless mais longo através das paredes múltiplas. A faixa gigahertz 5, por outro lado, menos é aglomerada e pode fornecer mais taxa de transferência tomando acima de umas 40 frequências MHZ da faixa em vez do padrão 20 megahertz na faixa 2.4 gigahertz. Além do que o intervalo mais curto, há igualmente menos dispositivos que apoiam a faixa gigahertz 5 comparada a 2.4 gigahertz.

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

Guest Network name:   
For example: MyGuestNetwork

**Nota:** Neste exemplo, o rádio 1 (gigahertz 5) é escolhido.

Etapa 28. Dê entrada com o nome do convidado SSID no *campo de nome da rede de convidado* a seguir clique-o **em seguida**.

**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

**Nota:** Neste exemplo, BeMyGuest! é usado como o nome de rede de convidado.

Etapa 29. Clique o botão de rádio que corresponde à segurança de rede que você gostaria de se aplicar a sua rede Wireless do convidado.

As opções são definidas como segue:

- A melhor Segurança (WPA2 pessoal - AES) — fornece a melhor Segurança e é recomendado se seus dispositivos Wireless apoiam esta opção. WPA2 usos pessoais AES e uma chave pré-compartilhada (PSK) entre os clientes e o Access point. Usa uma chave de criptografia nova para cada sessão que faz difícil comprometer.
- Melhor Segurança (WPA pessoal - TKIP/AES) — fornece a Segurança quando há uns dispositivos Wireless mais velhos que não apoiem o WPA2. Usos pessoais AES e TKIP WPA. Usa o padrão do Wi-fi da IEEE 802.11i.
- Nenhuma Segurança (não recomendada) — A rede Wireless não exige uma senha e pode ser alcançada por qualquer um. Se escolhida, uma janela pop-up aparecerá perguntando se você quer desabilitar a Segurança; clique **sim** para continuar. Se esta opção é escolhida, clique **em seguida** então a faixa clara a [etapa 35](#).

**Nota:** Neste exemplo, a melhor Segurança (WPA pessoal - TKIP/AES) é escolhida.

**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)

Etapa 30. Incorpore a senha para sua rede ao campo de *chave de segurança*. A barra colorida à direita deste campo mostra a complexidade da senha incorporada.

Enter a security key with 8-63 characters.

.....

Show Key as Clear Text

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

Click **Next** to continue

Back Next Cancel

Etapa 31. (Opcional) para ver a senha como você datilografa, verifique a **chave da mostra como a** caixa de verificação do **texto claro** a seguir clique-a **em seguida**.

Enter a security key with 8-63 characters.

GuestPassw0rd

Show Key as Clear Text

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

Click **Next** to continue

Back Next Cancel

Etapa 32. No portal prisioneiro theEnable – Atribua a área do ID de VLAN, escolha um ID para a rede de convidado da lista de drop-down do ID de VLAN a seguir clique-o **em seguida**.

**Nota:** Para WAP371 e WAP150, você precisa de datilografar dentro o ID no campo do *ID de VLAN* fornecido. A escala do ID de VLAN é de 1-4094.

**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

**Nota:** Neste exemplo, o ID de VLAN 2 é escolhido.

Etapa 33. (Opcional) se você quer novos usuários ser reorientado a uma página startup alternativa, verifique a **possibilidade reorientam a** caixa de verificação **URL no portal**

prisioneiro da possibilidade – permita reorientam a tela URL.

### 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 :

Etapa 34. (Opcional) incorpore a URL para o seu reorientam a URL no campo *URL da reorientação* a seguir clicam-na **em seguida**.

### 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

Nota: Neste exemplo, <http://newuser.com> é usado como a reorientação URL.

## Resumo

[Etapa 35](#). Reveja os ajustes mostrados e assegure-se de que a informação esteja correta. Se você gostaria de mudar um ajuste, clique o **botão Back Button** até que a página desejada esteja alcançada. Se não, o clique **submete-se** para permitir seus ajustes no WAP.

### 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

Etapa 36. A tela completa da instalação de dispositivo parecerá então confirmar que seu dispositivo se estabeleceu com sucesso. Clique em Finish.

### 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.

Você deve agora com sucesso ter configurado seu ponto de acesso Wireless usando o

assistente de configuração.