

# Configurar o portal prisioneiro em seu ponto de acesso Wireless usando o assistente de configuração

## Objetivo

O portal prisioneiro é uma característica em seu ponto de acesso Wireless que permite que você estabeleça uma rede de convidado onde necessidade de usuários Wireless de ser autenticado primeiramente antes que possam ter o acesso ao Internet. Fornece o acesso Wireless a seus visitantes ao manter a Segurança de sua rede interna.

O objetivo deste artigo é mostrar-lhe como configurar o portal prisioneiro em seu ponto de acesso Wireless usando o assistente de configuração.

## Dispositivos aplicáveis

- WAP131
- WAP150
- WAP321
- WAP361

## Versão de software

- 1.0.2.8 — WAP131
- 1.0.1.7 — WAP150, WAP361
- 1.0.6.5 — WAP321

## Configuram o portal prisioneiro

### Configurar o portal prisioneiro usando o assistente de configuração

**Nota:** As imagens abaixo são tomadas de WAP150. Estas imagens podem variar segundo o modelo exato de seu Access point.

Etapa 1. Entre a sua utilidade com base na Web do Access point e escolha o **assistente de configuração da corrida** do painel de navegação.



Etapa 2. Keep que clica **em seguida** até que você obtenha ao portal prisioneiro da possibilidade – crie sua tela da rede de convidado.

**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

Etapa 3. Clique o **botão Yes Radio Button** para criar a rede de convidado 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 guest networks](#)

Click **Next** to continue

Etapa 4. Clique o botão de rádio para a faixa de rádio onde você quer criar a rede de convidado.

**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 (2.4 GHz)

Radio 2 (5 GHz)

Guest Network name:

For example: MyGuestNetwork

**Nota:** Neste exemplo, o rádio 1 (2.4 gigahertz) é escolhido.

Etapa 5. Crie um nome para a rede de convidado 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 (2.4 GHz)  
 Radio 2 (5 GHz)

Guest Network name:   
For example: MyGuestNetwork

[? Learn more about network names](#)

Click **Next** to continue

Back Next Cancel

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

Etapa 6. Clique um botão de rádio para escolher um tipo de Segurança que você quer se usar na rede de convidado. As opções são:

- 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

**Enable Captive Portal - Secure Your Guest 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 (WPA/WPA2 pessoal - TKIP/AES) é escolhida.

Etapa 7. Crie uma senha para a rede de convidado no campo fornecido. A barra colorida à direita deste campo mostra a complexidade da senha incorporada.

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 8. (opcional) para considerar a senha como você datilografa, verifica a **chave da mostra como a caixa de verificação do texto claro** a seguir clica-a **em seguida**.

Enter a security key with 8-63 characters.  
Guests123  Weak

Show Key as Clear Text

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

Click **Next** to continue

Etapa 9. No portal prisioneiro theEnable – Atribua a área do ID de VLAN, incorpore o ID de VLAN para a rede de convidado a seguir clique-o **em seguida**. A escala do ID de VLAN é de 1-4094.

**Nota:** Para WAP131 e WAP361, você precisa de escolher o ID de VLAN da lista de drop-down.

**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

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

Etapa 10. (opcional) no portal prisioneiro da possibilidade – permita reorientam a tela URL, verificam a **possibilidade reorientam a caixa de verificação URL** se você tem um página da web que específico você quer mostrar depois que os usuários aceitam os termos de serviço da página de boas-vindas.

**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 11. Incorpore a URL ao campo *URL da reorientação* a seguir clique-a **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

Etapa 12. Verifique seus ajustes configurados no sumário – confirme sua tela dos ajustes. 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**

Security Key:	
VLAN ID:	1

Radio 2 (5 GHz)

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

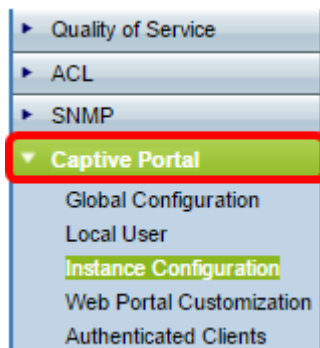
Captive Portal (Guest Network) Summary

Guest Network Radio:	Radio 1
Network Name (SSID):	ForTheGuests
Network Security Type:	WPA/WPA2 Personal - TKIP/AES
Security Key:	Guests123
Verification:	Guest
Redirect URL:	http://MyWebsite.com

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

## Verifique os ajustes portais prisioneiros

Etapa 13. Entre à utilidade com base na Web e escolha a **configuração prisioneira do portal > do exemplo**.



Etapa 14. Na página de configuração do exemplo, verifique os ajustes que você configurou no assistente de configuração e certifique-se que está associada ao ponto de acesso virtual correto (VAP) ou à rede. O nome de rede de convidado deve igualmente mostrar.

Administrative Mode:	<input checked="" type="checkbox"/> Enable
Protocol:	HTTP ▾
Verification:	Guest ▾
Redirect:	<input checked="" type="checkbox"/> Enable
Redirect URL:	<input type="text" value="http://MyWebsite.com"/> (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)
Associate VAP (2.4 GHz):	VAP 1 (ForTheGuests) ▾
Associate VAP (5 GHz):	▾

Etapa 15. Clique .

Você deve agora com sucesso ter configurado o portal prisioneiro em seu Access point do Cisco Wireless.