

# O domínio Wireless presta serviços de manutenção ao AP como um exemplo da configuração do servidor AAA

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Informações de Apoio](#)

[Configurar](#)

[Configurar o WDS AP](#)

[Configurar a infraestrutura AP](#)

[Configurar o método de autenticação do cliente](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

## Introdução

Este documento oferece uma configuração de exemplo para configurar um ponto de acesso (AP) para:

- Forneça o Wireless Domain Services (WDS).
- Execute o papel de um server do Authentication, Authorization, and Accounting (AAA).

Você pode usar este tipo da instalação quando você não têm um servidor de raio externo para autenticar a infraestrutura AP e os dispositivos do cliente que participam no WDS.

## Pré-requisitos

### Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento básico do WDS
- Métodos de segurança do Extensible Authentication Protocol (EAP) do conhecimento dos atuais

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Aironet série 1200 AP que executa o Software Release 12.3(7)JA1 de Cisco IOS®

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

## Informações de Apoio

O WDS é parte da Rede Cisco Structured Wireless Aware (CISNE). O WDS é uma coleção das Funcionalidades do software Cisco IOS que aumentam a mobilidade de cliente do Wireless LAN (WLAN) e simplificam a distribuição de WLAN e o Gerenciamento.

O WDS é a base para muitas características tais como rápido fixa vaguear, mergulha a mobilidade 3, e o Gerenciamento do rádio.

Refira [configurar o WDS, rápido fixam vaguear, Gerenciamento de rádio, e serviços wireless da intrusion detection](#) para obter mais informações sobre destas características.

Um dos propósitos principais do WDS é pôr em esconderijo as credenciais do usuário na primeira autenticação do cliente pelo Authentication Server. Em tentativas subsequentes, o WDS autentica o cliente com base na informação posta em esconderijo. A fim realizar isto:

- Um dos AP deve ser configurado como um WDS AP.
- Outros AP devem ser configurados como a infraestrutura AP que se comunicam ao WDS AP.
- O WDS AP deve estabelecer um relacionamento com o Authentication Server autenticando a ele com um nome de usuário e senha WDS.

Este Authentication Server validam as credenciais da infraestrutura AP e os clientes quando estes dispositivos autenticam pela primeira vez. O Authentication Server pode ser um servidor de raio externo ou o servidor Radius local no WDS AP.

O WDS e a infraestrutura AP comunicam-se sobre um protocolo de transmissão múltipla chamado o protocolo de controle do contexto do Wireless LAN (WLCCP). Estes mensagens de transmissão múltipla não podem ser distribuídos. Conseqüentemente, um WDS e uma infraestrutura associada AP devem estar na mesma sub-rede IP e no mesmo segmento LAN.

Este documento explica como usar a característica local do servidor Radius no WDS AP para executar a validação de credenciais.

## Configurar

## Configurar o WDS AP

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

A fim configurar o AP para servir como um WDS AP com funcionalidade do servidor AAA, você deve primeiramente permitir a característica local do servidor Radius no AP.

Conclua estes passos:

1. Entre ao AP com o GUI.A página do status sumário publica-se.
2. Selecione a **Segurança > o gerenciador do servidor do** menu do lado esquerdo no AP.
3. Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT e o segredo compartilhado do AP que atua como o servidor Radius sob servidores corporativos.Incorpore neste caso o endereço IP de Um ou Mais Servidores Cisco ICM NT do WDS AP desde que o WDS AP está indo atuar como o servidor Radius. O exemplo usa o endereço IP 10.0.0.1. Desde que este é um servidor Radius local você deve usar 1812 e 1813 enquanto a autenticação e as portas de relatório como este exemplo mostram.
4. Clique em Apply.
5. Selecione o endereço IP de Um ou Mais Servidores Cisco ICM NT WDS AP como a **prioridade 1** sob prioridades do server do padrão para a autenticação de EAP.Clique em Apply.Isto permite que o servidor Radius local seja a primeira escolha para a infraestrutura de autenticação AP e os clientes.
6. Selecione a **Segurança > servidor Radius local do menu do lado esquerdo**.Clique a **instalação geral** a fim configurar parâmetros locais do servidor Radius.Selecione o **PULO** sob ajustes locais da autenticação de servidor Radius e o clique **aplica-se**.Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do WDS AP e uma senha secundária compartilhada sob servidores do acesso de rede. Este exemplo usa a senha secundária compartilhada como **test123**.Clique em Apply.
7. Incorpore o nome de usuário e senha de toda a infraestrutura AP e de clientes que se comunicam com o WDS AP sob usuários individuais.Clique em Apply.Este exemplo inclui o nome de usuário e senha da infraestrutura AP que você configura para registrar com o WDS AP. Este exemplo usa o username como **infrastructureAP1** e a senha como **Cisco**. O mesmo nome de usuário e a senha precisam de ser configurados no Access point da infraestrutura.

Depois que você configura a característica local do servidor Radius no AP, você precisa de permitir a funcionalidade WDS no AP.

Conclua estes passos:

1. Selecione **Serviços sem fio > WDS do** menu do lado esquerdo no AP.
2. Clique a **instalação geral**.
3. Verifique o **uso este AP como serviços do domínio Wireless** na página de instalação geral.Incorpore **254** ao campo de prioridade dos serviços do domínio Wireless. Clique em Apply.
4. Permita a autenticação de infraestrutura.Clique **grupos de servidor na** página WDS.Dê entrada com um nome no campo de nome do grupo de servidor para autenticar a infraestrutura AP. Este exemplo usa o nome de grupo de servidor como a **infraestrutura**.Selecione o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius local da lista de drop-down das prioridades do server do grupo.O WDS AP usa este

server para autenticar a infraestrutura AP. Selecione a **autenticação de infraestrutura** sob o grupo do uso para. Clique em Apply.

O WDS AP atua agora como um servidor AAA. Configure uma da infraestrutura AP para registrar-se com o WDS AP.

**Note:** Use a ferramenta [Command Lookup Tool](#) ([apenas para clientes registrados](#)) para obter mais informações sobre os comandos usados neste documento.

## [Configurar a infraestrutura AP](#)

Esta seção explica a configuração exigida na infraestrutura AP para registrar-se com o WDS AP. Os clientes associam à infraestrutura AP. A infraestrutura AP pede o WDS AP para executar a autenticação para eles.

Termine estas etapas para adicionar uma infraestrutura AP que use os serviços do WDS:

1. Selecione **Serviços sem fio > AP** do menu do lado esquerdo.
2. Seletor **permita** participam abaixo na infraestrutura de swan.
3. Selecione a **descoberta automática** sob a descoberta de WDS.
4. Incorpore o nome de usuário e senha WDS aos campos apropriados. Clique em Apply. O nome de usuário e senha deve existir no servidor Radius local. Você deve definir um nome de usuário e senha WDS no Authentication Server para todos os dispositivos que são ser membros do WDS.

A infraestrutura AP aparece na área de informação AP com estado como REGISTRADA uma vez que você configura o WDS AP e a infraestrutura AP no WDS AP, aba do Status WDS. Isto está sob os Serviços sem fio > o item de menu WDS.

Os ajustes incorretos da autenticação no WDS AP ou a infraestrutura AP podem fazer com que o AP não apareça como o ACTIVE e/ou REGISTRARAM-SE. Verifique as estatísticas do Authentication Server para ver se há todos os erros ou tentativas de autenticação falha. Selecione a **Segurança > servidor Radius local > estatísticas** para estatísticas do Authentication Server.

Você pode igualmente usar o comando show wlccp wds ap do CLI no WDS AP verificar a configuração. No registro bem-sucedido com o WDS AP, a saída após um registro bem-sucedido com o WDS AP olha como este exemplo:

```
WDS#show wlccp wds ap
MAC-ADDR      IP-ADDR      STATE      LIFETIME      CDP-NEIGHBOR
000e.d7e4.a629 10.0.0.2     REGISTERED 97             10.77.241.161
```

## [Configurar o método de autenticação do cliente](#)

Adicionar um método de autenticação do cliente ao WDS.

Conclua estes passos:

1. Selecione **Serviços sem fio > WDS > grupos de servidor** no WDS AP. Defina um grupo de servidor que autentique clientes (um grupo de cliente). Isto deve ser diferente previamente do grupo de servidor configurado para a autenticação de infraestrutura. Este exemplo usa o nome de grupo de servidor como **clientes**. Ajuste a prioridade 1 ao servidor Radius

local. Selecione o tipo de autenticação (PULO, EAP, MAC, e assim por diante) para usar-se para a autenticação do cliente. Este exemplo usa a autenticação de leap. Aplique os ajustes aos SSID relevantes.

2. Termine estas etapas na infraestrutura AP: Selecione a **Segurança > o gerenciador de criptografia** e clique a **criptografia de WEP** e escolha **imperativo** do menu suspenso. Sob chaves de criptografia, incorpore a chave de criptografia de WEP do 128-bit. Este exemplo usa a chave de criptografia como **1234567890abcdef1234567890**. Selecione a **Segurança > o gerenciador de SSID** e crie um SSID novo. Este exemplo usa o SSID como o **cisco123**. Em seguida, escolha o método de autenticação. Selecione a **rede EAP** na infraestrutura AP.

Teste que os clientes autenticam com sucesso e associe com a infraestrutura AP. O cliente passa sobre suas credenciais à infraestrutura AP quando vem acima pela primeira vez. A infraestrutura AP então para a frente o mesmo ao WDS AP, que valida as credenciais.

**Note:** Este documento não explica como configurar o adaptador cliente. Refira o [Adaptadores de clientes LAN sem fio Cisco Aironet](#) para obter informações sobre de como configurar o adaptador cliente.

## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

- **show WLCCP WDS mn** - Use este comando do CLI no WDS AP verificar a autenticação do cliente e a associação bem sucedidas com o WDS AP.

```
WDS#show wlccp wds mn
  MAC-ADDR      IP-ADDR      Curr-AP      STATE
0040.96a5.b5d4  10.0.0.15    000e.d7e4.a629 REGISTERED
```

Os seguintes comandos debug são igualmente úteis.

- **debugar o wlccp ap {manganês | wds-descoberta | estado}** - use este comando girar sobre o indicador de debugam as mensagens relativas aos dispositivos do cliente (**manganês**), ao **processo de descoberta de WDS**, e à autenticação do Access point ao Access point WDS (**estado**).
- **debugar o pacote do wlccp** - Use este comando girar sobre o indicador dos pacotes a e do Access point WDS.
- **debugar o Servidor local do raio** - Ativa o indicador dos Mensagens de Erro relativos às autenticações do cliente falhadas ao autenticador local

## Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

## Informações Relacionadas

- [Configuração dos serviços do domínio sem fio](#)
- [Adaptadores cliente do Cisco Aironet](#)

- [O domínio Wireless presta serviços de manutenção ao FAQ](#)
- [Exemplos de configuração e TechNotes WLAN](#)
- [Exemplos de configuração e TechNotes do Cisco Aironet série 1200](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)