

# Configuração e status das configurações de log nos pontos de acesso WAP121 e WAP321

## Objetivo

Os registros do sistema são conjuntos de mensagens que registram eventos do sistema. Os registros ajudam a administrar o status do dispositivo. Eles também são usados para depurar o fluxo do pacote e para monitorar eventos. Os registros são geralmente armazenados na memória volátil, o que significa que os registros serão excluídos quando o WAP for redefinido ou desligado; entretanto, você pode armazenar logs em memória não volátil (permanente) se precisar manter os registros. Isso pode ser útil se você tiver que depurar um problema. Este documento o orienta na configuração das configurações de log e explica o status do log no WAP121 e no WAP321.

## Dispositivos aplicáveis

WAP121  
WAP321

## Versão de software

•1.0.3.4

## Configuração das configurações de log

**Caution:** O registro persistente pode diminuir o desempenho da memória flash (não volátil) e também do desempenho da rede. O registro persistente só deve ser usado quando você quiser depurar um problema. Certifique-se de desabilitar o registro persistente após concluir.

Etapa 1. Faça login no utilitário de configuração da Web e escolha **Administration > Log Settings**. A página *Configurações de log* é aberta:

The screenshot shows the 'Log Settings' configuration window. Under the 'Options' section, the 'Persistence' checkbox is checked and labeled 'Enable', and this entire section is circled in red. The 'Severity' dropdown is set to '7 - Debug' and the 'Depth' text box contains '512'. The 'Remote Log Server' section has 'Remote Log' unchecked. A 'Save' button is at the bottom left.

Etapa 2. Marque a caixa de seleção **Habilitar** no campo Persistência para habilitar o recurso de persistência que salva os registros do sistema na RAM não volátil (NVRAM) quando o dispositivo é reinicializado. Isso faz com que os logs não sejam apagados quando o dispositivo é reinicializado. Até 128 mensagens de log podem ser salvas na NVRAM. Se os logs excederem mais de 128 mensagens, os novos substituirão os logs antigos.

This screenshot shows the 'Log Settings' window with the 'Severity' dropdown menu open. The menu lists severity levels from 0 to 7, with '7 - Debug' highlighted in blue. A red box highlights the entire dropdown menu. Other settings like 'Persistence' (checked) and 'Depth' (512) are visible in the background. A 'Save' button is at the bottom left.

Etapa 3. Escolha o nível de gravidade na lista suspensa Gravidade. Todos os registros no nível de gravidade escolhido e superiores serão registrados. Os níveis de gravidade disponíveis são:

**Emergência** — Uma situação de pânico que afeta várias aplicações e locais.

**Alerta** — Quando uma mensagem de alerta é registrada, o dispositivo precisa de uma ação imediata para ser executado.

**Crítico** — O sistema está em um estado crítico. Há que tomar algumas medidas para ultrapassar a situação quando se vê esta mensagem.

**Erro** — Ocorreu um erro de sistema, como falhas não urgentes. Elas devem ser resolvidas em um determinado tempo.

**Aviso** — Não é um erro, mas uma indicação de que um erro ocorrerá se não for tomada uma ação.

- Aviso - O sistema funciona corretamente, mas ocorreu um aviso do sistema. Esses são eventos incomuns, mas não condições de erro.

**Informativo** — Fornece informações sobre o dispositivo.

**Debug** — Fornece informações detalhadas sobre o tipo de depuração e o tempo da depuração.

**Log Settings**

**Options**

Persistence:  Enable

Severity: 7 - Debug

Depth: 500

**Remote Log Server**

Remote Log:  Enable

Server IPv4/IPv6 Address/Name: 192.168.0.1

UDP Port: 520

Save

Etapa 4. Insira a quantidade máxima de mensagens que podem ser armazenadas na memória volátil no campo Profundidade. Por padrão, um ponto de acesso enfileira até 512 mensagens.

Etapa 5. (Opcional) Se desejar enviar as mensagens de log para um servidor syslog remoto, marque a caixa de seleção **Enable (Habilitar)** no campo Remote Log (Registro remoto).

**Proteção de tempo:** Se você não marcar a caixa de seleção Enable (Habilitar), vá para a etapa 8.

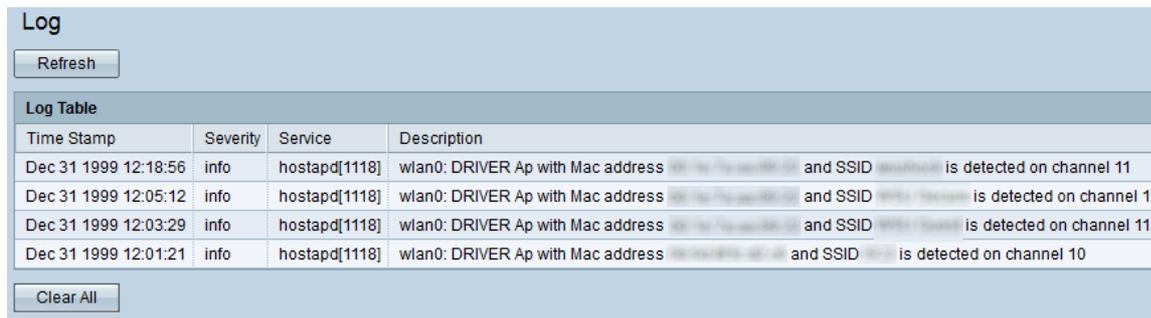
Etapa 6. Insira o nome de domínio ou o endereço IP do Servidor syslog no campo Server IPv4/IPv6 Address/Name.

Passo 7. Digite o número da porta UDP do Servidor syslog onde os logs são enviados no campo Porta UDP. A porta padrão é 514.

Etapa 8. Clique em **Salvar** para salvar as alterações feitas.

# Status e estatísticas do log

Etapa 1. Faça login no utilitário de configuração da Web e escolha **Status e Statistics > Log**. A página *Log* é aberta:



| Time Stamp           | Severity | Service       | Description  |
|----------------------|----------|---------------|--|
| Dec 31 1999 12:18:56 | info     | hostapd[1118] | wlan0: DRIVER Ap with Mac address [redacted] and SSID [redacted] is detected on channel 11 |
| Dec 31 1999 12:05:12 | info     | hostapd[1118] | wlan0: DRIVER Ap with Mac address [redacted] and SSID [redacted] is detected on channel 11 |
| Dec 31 1999 12:03:29 | info     | hostapd[1118] | wlan0: DRIVER Ap with Mac address [redacted] and SSID [redacted] is detected on channel 11 |
| Dec 31 1999 12:01:21 | info     | hostapd[1118] | wlan0: DRIVER Ap with Mac address [redacted] and SSID [redacted] is detected on channel 10 |

A tabela de log tem os seguintes campos:

Carimbo de data/hora — Exibe o mês, dia, ano e a hora em que o log foi criado.

Severidade — Exibe a gravidade do evento.

Service — O componente de software relacionado ao evento.

Descrição — Exibe uma mensagem informativa que descreve o evento registrado.

Etapa 2. (Opcional) Para limpar os registros, clique em **Limpar tudo**.

Etapa 3. (Opcional) Se quiser atualizar a tabela de log, clique em **Atualizar**.