

Configure e exiba os registros do sistema (syslogs) no WAP125 e WAP581

Objetivo

Eventos do sistema são atividades que podem exigir atenção e ações necessárias para executar o sistema sem problemas e evitar falhas. Esses eventos são gravados como logs. Os registros de sistema (Syslogs) permitem que o administrador controle eventos específicos que ocorrem no dispositivo.

As configurações de log definem as regras de registro e os destinos de saída para mensagens, notificações e outras informações, à medida que vários eventos são gravados na rede. Este recurso notifica a equipe responsável para que as ações necessárias sejam tomadas quando um evento ocorrer. Os registros podem ser enviados a um servidor remoto onde os registros de todas as atividades da rede são registrados. Para saber como configurar as definições de registro remoto, clique [aqui](#). Os registros também podem ser enviados aos administradores de rede através de alertas por e-mail. Para saber como configurar definições de correio eletrônico e personalizar notificações por correio eletrônico, clique [aqui](#).

Este artigo tem como objetivo mostrar como gerenciar as configurações de log do sistema e exportar as configurações de log no WAP125 e no WAP581.

Dispositivos aplicáveis

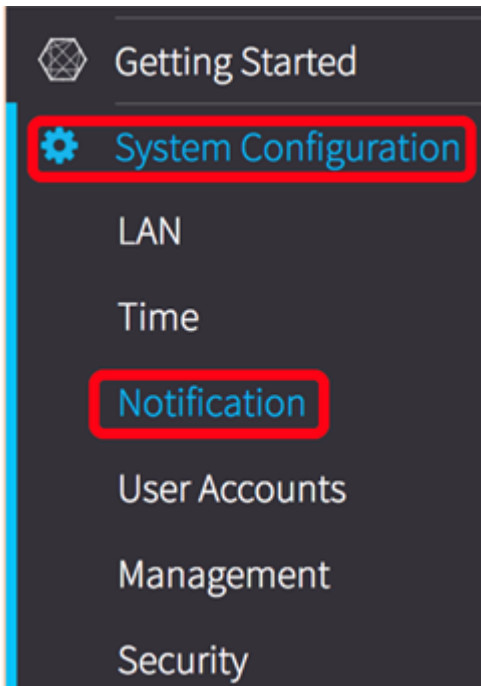
- WAP125
- WAP581

Versão de software

- 1.0.0.4

Configure as configurações de Syslogs

Etapa 1. Faça login no utilitário baseado na Web do WAP e escolha **Configuração do sistema > Notificação**.



Etapa 2. Marque a caixa de seleção **Habilitar** persistência para salvar os registros do sistema na memória não volátil. Isso permite que os registros permaneçam no WAP após serem reinicializados. Um máximo de 1000 mensagens são salvas na memória não volátil e quando o limite é atingido, a última mensagem é sobrescrita.

A screenshot of the 'Log Settings' configuration page. The page has a light gray background. At the top, the title 'Log Settings' is displayed. Below the title, there are three settings: 'Persistence:' with a checked checkbox and the text 'Enable'; 'Severity:' with a dropdown menu showing 'Debug'; and 'Depth:' with a text input field containing '1000'. Below these settings is a section titled 'Remote Log Server Table' which is currently empty. At the bottom of the page, there is a blue button labeled 'View System Log...'.

Persistence:	<input checked="" type="checkbox"/> Enable
Severity:	Debug
Depth: ?	1000

Remote Log Server Table

View System Log...

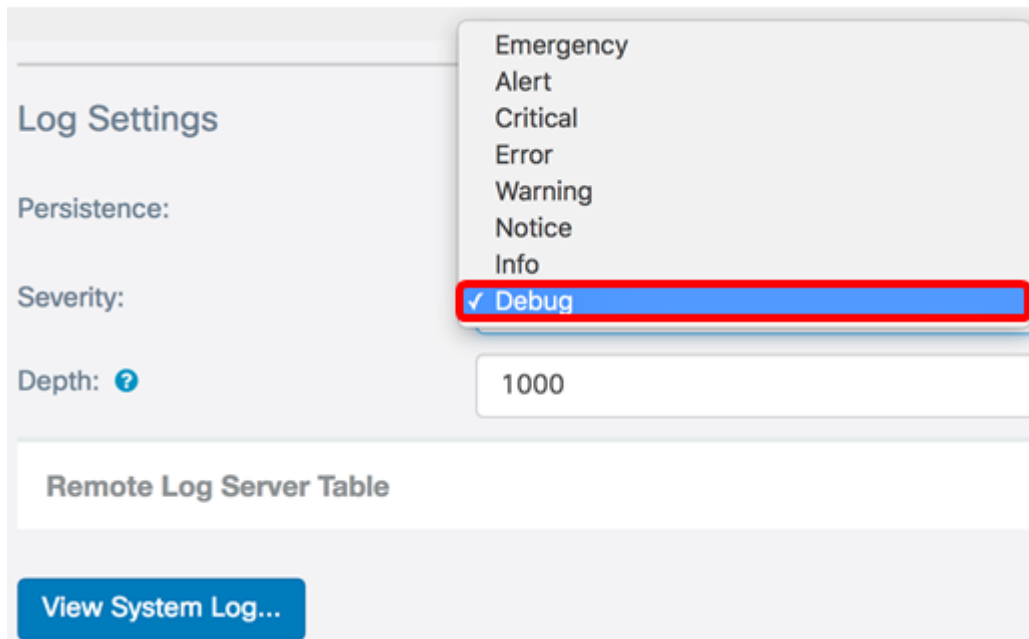
Etapa 3. Escolha uma opção na lista suspensa Gravidade. A gravidade escolhida inclui todos os níveis mais altos, portanto, os registros são mantidos para todos os níveis de gravidade do nível superior até o nível escolhido.

- Emergência — Este é o nível 0. O sistema não pode ser usado. Isso é normalmente transmitido para todos os processos.
- Alerta — Este é o nível 1. Ação imediata necessária.
- Crítico — Este é o nível 2. Condições críticas, como um erro de dispositivo de hardware.
- Erro — Este é o nível 3. Condições de erro.
- Aviso — Este é o nível 4. Condições de aviso.
- Aviso — Este é o nível 5. Condição normal, mas significativa.
- Informações — Este é o nível 6. Somente mensagens informativas. Uma condição que

não é uma condição de erro, mas que pode exigir tratamento especial.

- Depuração — Este é o nível 7. A depuração de mensagens contém informações normalmente de uso somente durante a depuração de um programa.

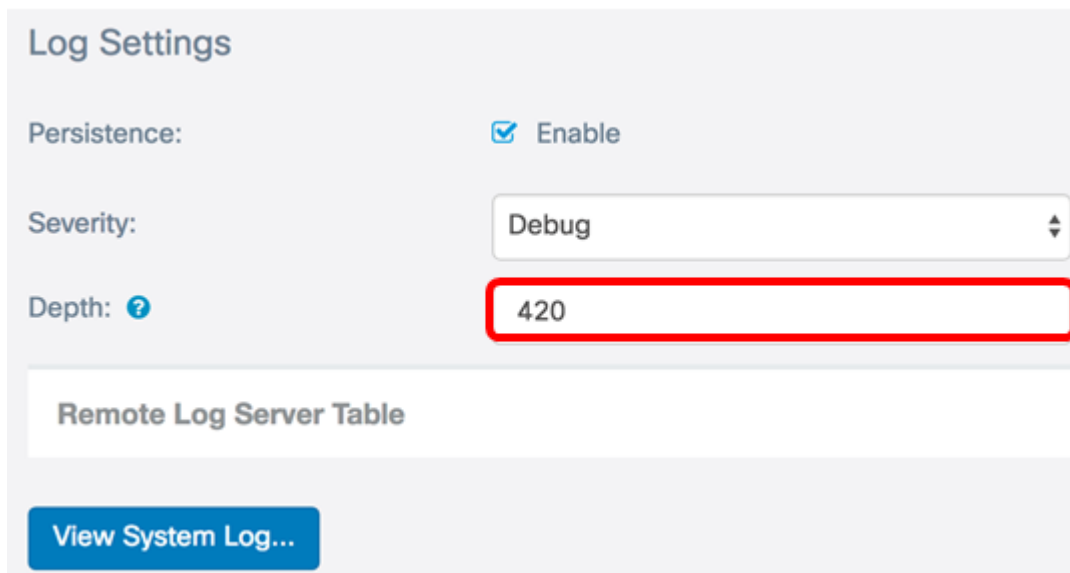
Note: Neste exemplo, Depurar é escolhido.



The screenshot shows the 'Log Settings' configuration page. The 'Severity' dropdown menu is open, displaying a list of severity levels: Emergency, Alert, Critical, Error, Warning, Notice, Info, and Debug. The 'Debug' option is highlighted with a blue background and a red border. The 'Depth' field is set to 1000. Below the settings is a 'Remote Log Server Table' section and a 'View System Log...' button.

Etapa 4. No campo *Profundidade*, insira um valor entre 1 e 1000 para definir o número de mensagens de syslog que podem ser armazenadas na memória volátil. Todos os registros na memória volátil são excluídos quando o sistema é reinicializado.

Note: Neste exemplo, 420 é usado.



The screenshot shows the 'Log Settings' configuration page. The 'Persistence' checkbox is checked and labeled 'Enable'. The 'Severity' dropdown menu is set to 'Debug'. The 'Depth' field is set to 420 and is highlighted with a red border. Below the settings is a 'Remote Log Server Table' section and a 'View System Log...' button.

Etapa 5. Clique em [Save](#).

Etapa 6. Clique no botão **Exibir log do sistema...** para exibir os logs.

Log Settings

Persistence: Enable

Severity:

Depth:

Remote Log Server Table

[View System Log...](#)

A tabela exibe o Carimbo de data/hora, Gravidade, Serviço e Descrição. As definições são as seguintes:

Carimbo de data/hora — A hora em que a mensagem syslog foi feita. Exibe a data no formato MM-DD-AAAA e a hora no formato militar.

- Severidade — Gravidade da mensagem de syslog.
- Serviço — O serviço associado ao evento.
- Descrição — A mensagem principal do syslog.

Time Stamp	Severity	Service	Description
May 12,2017 09:47:20	err	syslog	User logon failed for incorrect username and password
May 12,2017 09:12:25	debug	hostapd[14990]	station: b4:4b:d2:0c:70:89 deauthenticated
May 12,2017 09:12:25	info	hostapd[14990]	STA b4:4b:d2:0c:70:89 deauthed from BSSID 00:eb:d5:5e:02:58 reason 4: Disassociated due to inactivity
May 12,2017 09:06:47	debug	hostapd[14990]	station: b4:4b:d2:0c:70:89 deauthenticated
May 12,2017 09:06:47	info	hostapd[14990]	STA b4:4b:d2:0c:70:89 associated with BSSID 00:eb:d5:5e:02:58
May 12,2017 09:06:47	info	hostapd[14990]	STA b4:4b:d2:0c:70:89 deauthed from BSSID 00:eb:d5:5e:02:58 reason 3: STA is leaving IBSS or ESS
May 12,2017 09:06:47	info	hostapd[14990]	Assoc request from b4:4b:d2:0c:70:89 BSSID 00:eb:d5:5e:02:58 SSID ciscosb
May 12,2017 09:06:47	debug	hostapd[14990]	station: b4:4b:d2:0c:70:89 deauthenticated
May 12,2017 09:06:47	info	hostapd[14990]	STA b4:4b:d2:0c:70:89 disassociated from BSSID 00:eb:d5:5e:02:58 reason 8: Sending STA is leaving BSS
May 12,2017 08:48:02	info	hostapd[14990]	STA b4:4b:d2:0c:70:89 associated with BSSID 00:eb:d5:5e:02:58

Passo 7. (Opcional) Na área Cabeçalho da Tabela de log do sistema, clique nas setas para filtrar dados em ordem cronológica ou alfabética.

Note: Neste exemplo, o carimbo de data e hora é clicado para organizar as entradas de

syslog da mais recente para a mais recente.



Time Stamp	Severity	Service	Description
May 12,2017 02:14:00	info	hostapd[1510]	STA 4c:34:88:42:22:0a deauthed from BSSID 00:eb:d5:5e:02:5c reason 1: Unspecified Reason
May 12,2017 02:14:00	debug	hostapd[1510]	station: 4c:34:88:42:22:0a deauthenticated

Etapa 8. (Opcional) Para ver mais registros, clique nos **números** da **página** para navegar pelas páginas de registro.



Etapa 9. (Opcional) Clique no botão **Atualizar** para atualizar a página para permitir que você exiba registros mais recentes e mais recentes.



Etapa 10. (Opcional) Para limpar ou apagar os registros da tabela, clique em **Limpar tudo**.



Etapa 11. (Opcional) Para exportar e baixar os registros em um computador, clique em **Download**. Um download será iniciado no seu navegador.



Note: O arquivo é salvo em formato .txt.

```
-----  
number      1  
time        May 15 2017 08:23:27  
priority    err  
daemon      syslog  
message     User logon failed for incorrect username and password  
-----  
number      2  
time        May 12 2017 08:42:28  
priority    warn  
daemon      dman[1236]  
message     DHCP-client: Interface brtrunk obtained lease on new address  
192.168.100.109.  
-----  
number      3  
time        May 12 2017 08:41:56  
priority    info  
daemon      dman[1236]  
message     SSL certificate generated for Clusterd
```

Etapa 12. Clique em **Voltar** para retornar à página de configuração Notificação.

Refresh

Clear All

Download

Back

Agora você exportou logs com êxito no WAP125 e no WAP581.