

Configurar o registro de eventos em um ponto de acesso sem fio

Objetivo

Eventos do sistema são atividades que podem exigir atenção e a ação necessária para executar o sistema sem problemas e evitar falhas. Esses eventos são gravados como logs. Os registros do sistema permitem que o administrador controle eventos específicos que ocorrem no dispositivo.

Os registros de eventos são úteis para a solução de problemas de rede, debugging packet flow e para monitorar eventos. Esses registros podem ser salvos na memória de acesso aleatório (RAM), na memória de acesso aleatório não volátil (NVRAM) e em servidores de registro remotos. Esses eventos geralmente são apagados do sistema quando reinicializados. Se o sistema for reinicializado inesperadamente, os eventos do sistema não poderão ser exibidos a menos que sejam salvos na memória não volátil. Se o recurso de registro de persistência estiver ativado, as mensagens de evento do sistema serão gravadas na memória não volátil.

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 também podem ser enviados a eles por meio de alertas por e-mail.

Este documento tem como objetivo explicar e guiá-lo pelas diferentes configurações para receber registros de sistema e eventos.

Dispositivos aplicáveis

WAP100 Series

WAP300 Series

WAP500 Series

Versão de software

1.0.1.4 — WAP131, WAP351

1.0.6.2 — WAP121, WAP321

1.2.1.3 — WAP371, WAP551, WAP561

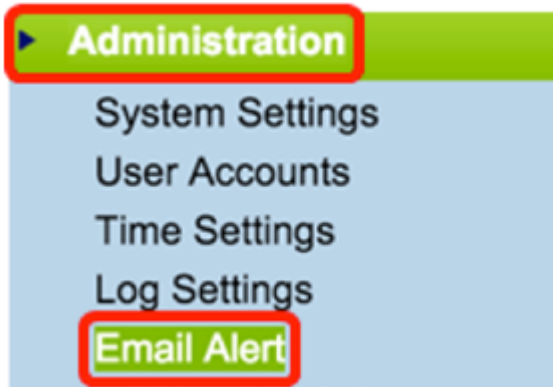
1.0.1.2 — WAP150, WAP361

1.0.0.17 — WAP571, WAP571E

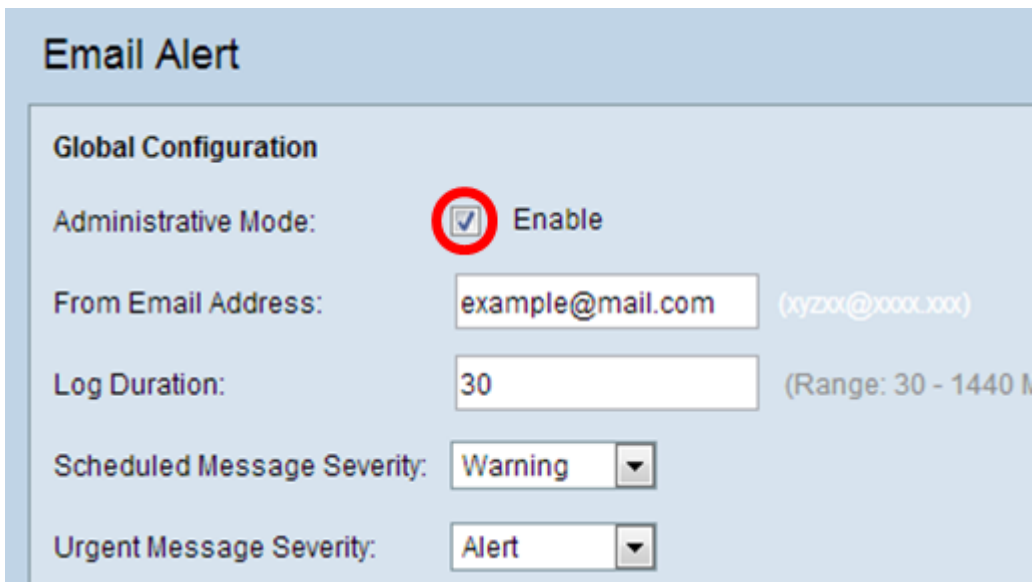
Configurar registro de eventos

Configurar alerta por e-mail

Etapa 1. Faça login no utilitário baseado na Web e escolha **Administração > Alerta por e-mail**.



Etapa 2. Marque a caixa de seleção **Habilitar** no Modo Administrativo para habilitar o recurso de alerta de email globalmente.

A screenshot of the 'Email Alert' configuration page. The page has a light blue header with the title 'Email Alert'. Below the header is a section titled 'Global Configuration'. It contains several fields: 'Administrative Mode:' with a checked checkbox and the text 'Enable'; 'From Email Address:' with a text input field containing 'example@mail.com' and a placeholder '(xyz0x@xxxx.xxx)'; 'Log Duration:' with a text input field containing '30' and a range '(Range: 30 - 1440 M)'; 'Scheduled Message Severity:' with a dropdown menu showing 'Warning'; and 'Urgent Message Severity:' with a dropdown menu showing 'Alert'.

Etapa 3. Insira um endereço de e-mail no campo *Do endereço de e-mail*. O endereço é exibido como remetente do alerta por e-mail. O valor padrão é nulo.

Email Alert

Global Configuration

Administrative Mode: Enable

From Email Address:

Log Duration:

Scheduled Message Severity:

Urgent Message Severity:

Note: É altamente recomendável usar uma conta de e-mail separada em vez de usar seu e-mail pessoal para manter a privacidade.

Etapa 4. No campo *Duração do log*, insira o tempo (em minutos) de envio dos alertas por e-mail para o endereço de e-mail configurado. O intervalo é de 30 a 1440 minutos e o valor padrão é 30.

Email Alert

Global Configuration

Administrative Mode: Enable

From Email Address:

Log Duration:

Scheduled Message Severity:

Urgent Message Severity:

Etapa 5. Para definir a Gravidade da mensagem agendada, escolha o tipo apropriado de mensagem a ser enviada, como Emergência, Alerta, Crítico, Erro, Aviso, Aviso, Informações ou Depuração. Essas mensagens são enviadas toda vez que a Duração do log expira. Essas opções são exibidas de forma diferente no utilitário baseado na Web, dependendo do modelo do dispositivo que você está usando.

Para WAP131, WAP150, WAP351 e WAP361, marque o tipo de mensagem apropriado nas caixas de seleção Agendado Message Severity.

Scheduled Message Severity: Emergency Alert Critical Error Warning Notice Info Debug

Urgent Message Severity: Emergency Alert Critical Error Warning Notice Info Debug

Para WAP121, WAP321, WAP371, WAP551, WAP561, WAP571 e WAP571E, clique no tipo de mensagem apropriado na lista suspensa Gravidade da mensagem programada.

Email Alert

Global Configuration

Administrative Mode: Enable

From Email Address:

Log Duration:

Scheduled Message Severity: ▼

- None
- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Info
- Debug

Urgent Message Severity:

Mail Server Configuration

Server IPv4 Address/Name:

Data Encryption:

Nenhum — Nenhuma mensagem é enviada.

Emergência — Esse tipo de mensagem é enviada ao usuário quando o dispositivo está em uma situação crítica e é necessária atenção imediata.

Alerta — Esse tipo de mensagem é enviada ao usuário quando ocorre qualquer ação diferente da configuração normal.

Crítico — Esse tipo de mensagem é enviada ao usuário quando há uma situação em que uma porta está inativa ou o usuário não pode acessar a rede. É necessária uma ação imediata.

Erro — Este tipo de mensagem é enviada ao usuário quando há um erro de configuração.

Aviso — esse tipo de mensagem é enviada ao usuário quando outro usuário tenta acessar as áreas restritas.

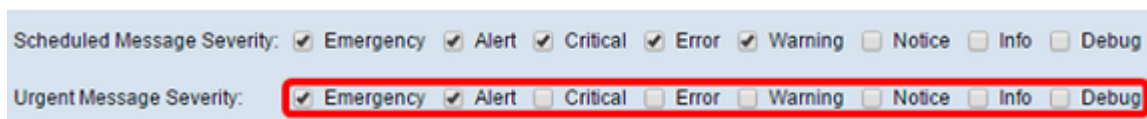
Aviso — Esse tipo de mensagem é enviada ao usuário quando há alterações de baixa prioridade na rede.

Info — Este tipo de mensagem é enviada ao usuário para descrever como a rede se comporta.

Depuração — Esse tipo de mensagem é enviada ao usuário com os logs do tráfego de rede.

Etapa 6. Para definir a Gravidade Urgente da Mensagem, escolha o tipo apropriado de mensagem urgente a ser enviada, como Emergência, Alerta, Crítico, Erro, Aviso, Aviso, Informações ou Depuração. Essas mensagens são enviadas imediatamente. Essas opções são exibidas de forma diferente no utilitário baseado na Web, dependendo do modelo do dispositivo que você está usando.

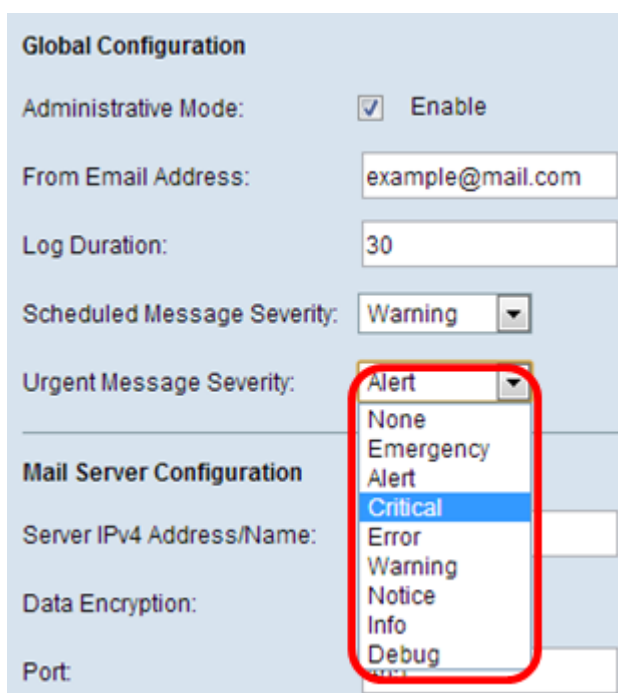
Para WAP131, WAP150, WAP351 e WAP361, marque o tipo de mensagem urgente apropriado nas caixas de seleção Gravidade da mensagem urgente.



Scheduled Message Severity: Emergency Alert Critical Error Warning Notice Info Debug

Urgent Message Severity: Emergency Alert Critical Error Warning Notice Info Debug

Para WAP121, WAP321, WAP371, WAP551, WAP561, WAP571 e WAP571E, clique no tipo de mensagem urgente apropriado na lista suspensa Gravidade da mensagem urgente.



Global Configuration

Administrative Mode: Enable

From Email Address:

Log Duration:

Scheduled Message Severity:

Urgent Message Severity:

Mail Server Configuration

Server IPv4 Address/Name:

Data Encryption:

Port:

Urgent Message Severity dropdown menu options: Alert, None, Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug

Nota: se a opção estiver definida como Nenhum, nenhuma mensagem será enviada.

Passo 7. Insira o nome de host válido do servidor de e-mail ou endereço IP no campo *Server IPv4 Address/Name* (*Endereço/Nome do IPv4 do servidor*).

Nota: No exemplo abaixo, 200.168.20.10 é usado.

Mail Server Configuration

Server IPv4 Address/Name: 200.168.20.10

Data Encryption: TLSv1

Port: 465

Username: Cisco_1

Password:

Etapa 8. Escolha o modo de segurança na lista suspensa Criptografia de dados. As opções disponíveis são:

- TLSv1 — O Transport Layer Security versão 1 é um protocolo criptográfico que fornece segurança e integridade de dados para comunicação pela Internet.
- Aberto — É o protocolo de criptografia padrão, mas não tem medidas de segurança para criptografia de dados.

Mail Server Configuration

Server IPv4 Address/Name: 200.168.20.10

Data Encryption: Open
✓ TLSv1

Port: 465

Username: Cisco_1

Password:

Note: Neste exemplo, TLSv1 é escolhido. Se você escolheu Abrir, vá para a [Etapa 12](#).

Etapa 9. Digite o número da porta do servidor de e-mail no campo *Porta*. É um número de porta de saída usado para enviar emails. O intervalo de números de porta válido é de 0 a 65535 e o padrão é 465 para SMTP (Simple Mail Transfer Protocol).

Mail Server Configuration

Server IPv4 Address/Name: 200.168.20.10

Data Encryption: TLSv1

Port: 465

Username: Cisco_1

Password:

Etapa 10. Digite o nome de usuário para autenticação no campo *Nome de usuário*.

Mail Server Configuration

Server IPv4 Address/Name: 200.168.20.10

Data Encryption: TLSv1

Port: 465

Username: Cisco_1

Password:

Observação: Cisco_1 é usado como exemplo.

Etapa 11. Digite a senha para autenticação no campo *Senha*.

Mail Server Configuration

Server IPv4 Address/Name: 200.168.20.10

Data Encryption: TLSv1

Port: 465

Username: Cisco_1

Password:

[Etapa 12.](#) Em Configuração da mensagem, insira o endereço de e-mail necessário nos campos *Para endereço de e-mail 1, 2 e 3*.

Note: Com base no requisito, você pode inserir valores em todos os campos *Para endereço de e-mail* ou inserir apenas um endereço de e-mail e deixar o restante em branco.

Message Configuration

To Email Address 1: Test_1@mail.com (xyz@xxx.xxx)

To Email Address 2: Test_2@mail.com (xyz@xxx.xxx)

To Email Address 3: Test_3@mail.com (xyz@xxx.xxx)

Email Subject: Log message from AP

Save Test Mail

Etapa 13. Digite o assunto do email no campo *Assunto do email*. O assunto pode ter até 255 caracteres alfanuméricos.

Message Configuration

To Email Address 1: (xyz@xxx.xxx)

To Email Address 2: (xyz@xxx.xxx)

To Email Address 3: (xyz@xxx.xxx)

Email Subject:

Nota: Neste exemplo, a mensagem Log do AP é usada.

Etapa 14. Clique em **Testar email** para validar as credenciais do servidor de email configurado. Isso envia um e-mail para os endereços de e-mail configurados para verificar se a configuração funciona.

Message Configuration

To Email Address 1: (xyz@xxx.xxx)

To Email Address 2: (xyz@xxx.xxx)

To Email Address 3: (xyz@xxx.xxx)

Email Subject:

Etapa 15. Clique em **Save**.

Message Configuration

To Email Address 1:

To Email Address 2:

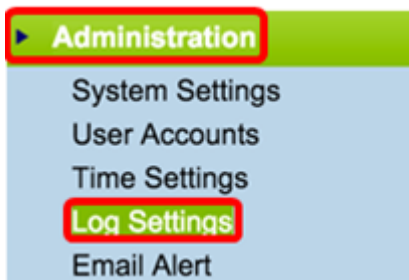
To Email Address 3:

Email Subject:

Definir configurações de log

Essa área configura localmente o sistema e os registros de eventos no volátil e na NVRAM.

Etapa 1. Efetue login no utilitário baseado na Web do ponto de acesso para escolher **Administration > Log Settings**.



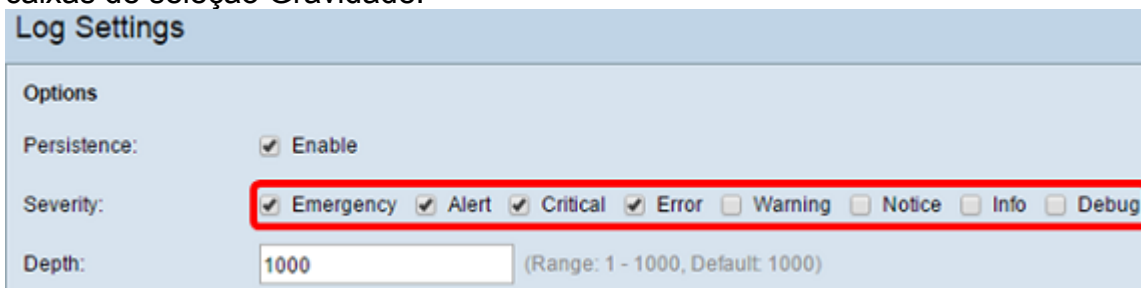
Etapa 2. (Opcional) Se desejar que os registros sejam salvos permanentemente para que as configurações permaneçam enquanto o WAP é reinicializado, ative a Persistência marcando a caixa de seleção **Habilitar**. Isso é especialmente útil no caso de reinicializações inesperadas do sistema quando ocorre um evento indesejável ou uma falha. Até 128 mensagens de log podem ser salvas na NVRAM, após as quais os logs são sobrescritos.



Note: Se a opção Ativar estiver desmarcada, os registros serão salvos na memória volátil.

Etapa 3. Para definir a Gravidade, escolha o tipo apropriado de mensagem a ser enviada, como Emergência, Alerta, Crítico, Erro, Aviso, Aviso, Informações ou Depuração. Essas mensagens são enviadas toda vez que a Duração do log expira. Essas opções são exibidas de forma diferente no utilitário baseado na Web, dependendo do modelo do dispositivo que você está usando.

Para WAP131, WAP150, WAP351 e WAP361, marque o tipo de mensagem apropriado nas caixas de seleção Gravidade.



Para WAP121, WAP321, WAP371, WAP551, WAP561, WAP571 e WAP571E, clique no tipo de mensagem apropriado na lista suspensa Severidade.

The screenshot shows the 'Log Settings' configuration page. Under the 'Options' section, 'Persistence' is checked and set to 'Enable'. The 'Severity' dropdown menu is open, showing a list of severity levels: 7 - Debug (highlighted in blue), 0 - Emergency, 1 - Alert, 2 - Critical, 3 - Error, 4 - Warning, 5 - Notice, and 6 - Info. The 'Depth' field is currently empty. Below this, the 'Remote Log Server' section is partially visible, showing 'Remote Log:' and 'Server IPv4/IPv6 Address/Name:'.

Etapa 4. À medida que as mensagens de log são geradas, elas são colocadas em uma fila para transmissão. Especifique o número de mensagens que podem ser enfileiradas ao mesmo tempo na memória volátil no campo *Profundidade*. Até 512 mensagens podem ser enfileiradas ao mesmo tempo.

Para WAP131, WAP150, WAP351 e WAP361, insira o intervalo de profundidade no campo Profundidade. O intervalo é 1-1000. O valor padrão é 1000.

The screenshot shows the 'Log Settings' configuration page. Under the 'Options' section, 'Persistence' is checked and set to 'Enable'. The 'Severity' section has three checkboxes checked: 'Emergency', 'Alert', and 'Info'. The 'Depth' field is set to '1000' and is highlighted with a red box.

Para WAP121, WAP321, WAP371, WAP551, WAP561, WAP571 e WAP571E, insira o intervalo de profundidade no campo Profundidade. O intervalo é 1-512 e 512 é o padrão. Para este exemplo, 67 é usado.

The screenshot shows the 'Log Settings' configuration page. Under the 'Options' section, 'Persistence' is checked and set to 'Enable'. The 'Severity' dropdown menu is set to '7 - Debug'. The 'Depth' field is set to '67' and is highlighted with a red box.

Etapa 5. Click **Save**.

Note: O ponto de acesso adquire informações de data e hora usando um servidor Network Time Protocol. Esses dados estão no formato UTC (Hora de Greenwich).

Essas configurações devem propagar o registro de eventos no dispositivo local e receber alertas por e-mail.