

Configuración del registro de eventos en un punto de acceso inalámbrico

Objetivo

Los eventos del sistema son actividades que pueden requerir atención y la acción necesaria para ejecutar el sistema sin problemas y evitar fallos. Estos eventos se registran como registros. Los registros del sistema permiten al administrador realizar un seguimiento de los eventos concretos que se producen en el dispositivo.

Los registros de eventos son útiles para la resolución de problemas de red, la depuración del flujo de paquetes y el monitoreo de eventos. Estos registros se pueden guardar en la memoria de acceso aleatorio (RAM), la memoria de acceso aleatorio no volátil (NVRAM) y en los servidores de registro remotos. Estos eventos generalmente se borran del sistema cuando se reinician. Si el sistema se reinicia inesperadamente, los eventos del sistema no se pueden ver a menos que se guarden en la memoria no volátil. Si se habilita la función de registro de persistencia, los mensajes de eventos del sistema se escriben en la memoria no volátil.

La configuración del registro define las reglas de registro y los destinos de salida para los mensajes, las notificaciones y otra información, ya que varios eventos se registran en la red. Esta función notifica al personal responsable para que se tomen las medidas necesarias cuando se produzca un evento. Los registros también se pueden enviar por correo electrónico.

Este documento tiene como objetivo explicarle y guiarle a través de las diferentes configuraciones para recibir registros de eventos y del sistema.

Dispositivos aplicables

Serie WAP100

Serie WAP300

Serie WAP500

Versión del software

1.0.1.4 — WAP131, WAP351

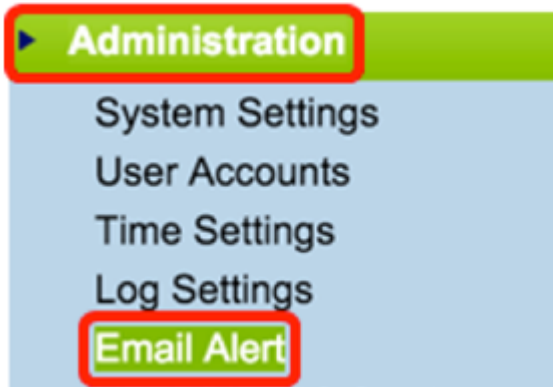
1.0.6.2 — WAP121, WAP321

1.2.1.3 — WAP371, WAP551, WAP561

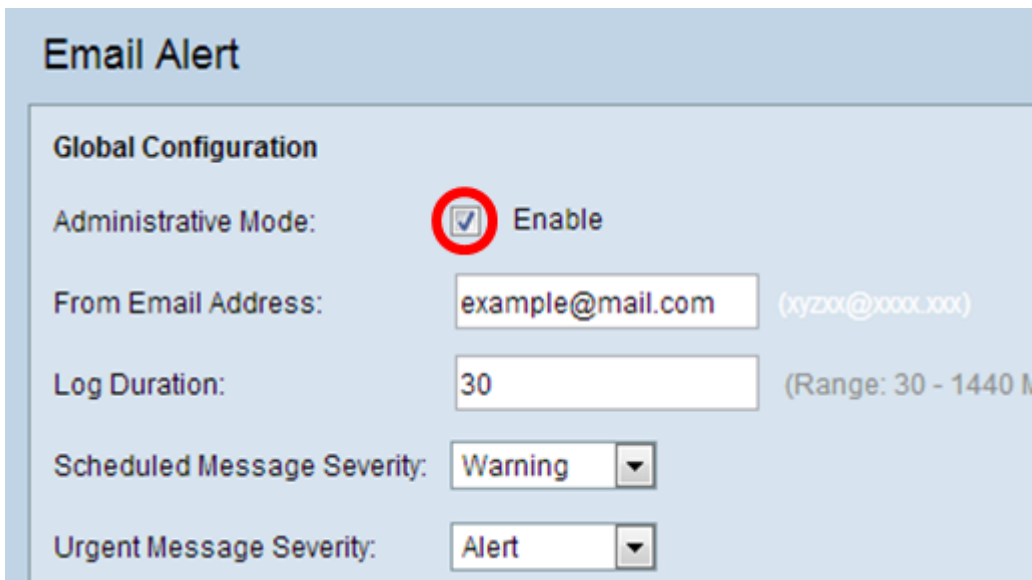
Configuración del registro de eventos

Configurar alerta de correo electrónico

Paso 1. Inicie sesión en la utilidad basada en Web y elija **Administration > Email Alert**.



Paso 2. Marque **Enable** en la casilla de verificación Administrative Mode para habilitar globalmente la función de alerta de correo electrónico.

A screenshot of the "Email Alert" configuration page. The page has a light blue background. At the top, the title "Email Alert" is displayed. Below the title, there is a section titled "Global Configuration". Under this section, there are several configuration options: "Administrative Mode:" with a checked checkbox (circled in red) 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".

Paso 3. Introduzca una dirección de correo electrónico en el campo *From Email Address* (*Dirección de correo electrónico de origen*). La dirección se muestra como el remitente de la alerta de correo electrónico. El valor predeterminado es null.

Email Alert

Global Configuration

Administrative Mode: Enable

From Email Address:

Log Duration:

Scheduled Message Severity:

Urgent Message Severity:

Nota: Se recomienda encarecidamente utilizar una cuenta de correo electrónico independiente en lugar de utilizar su correo electrónico personal para mantener la privacidad.

Paso 4. En el campo *Duración del registro*, introduzca la hora (en minutos) a la que se deben enviar las alertas de correo electrónico a la dirección de correo electrónico configurada. El intervalo es de 30 a 1440 minutos y el valor predeterminado es 30.

Email Alert

Global Configuration

Administrative Mode: Enable

From Email Address:

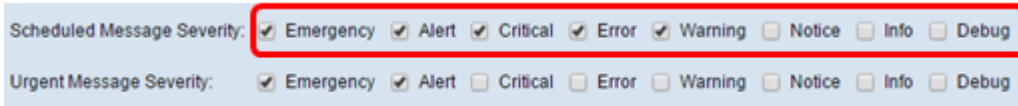
Log Duration:

Scheduled Message Severity:

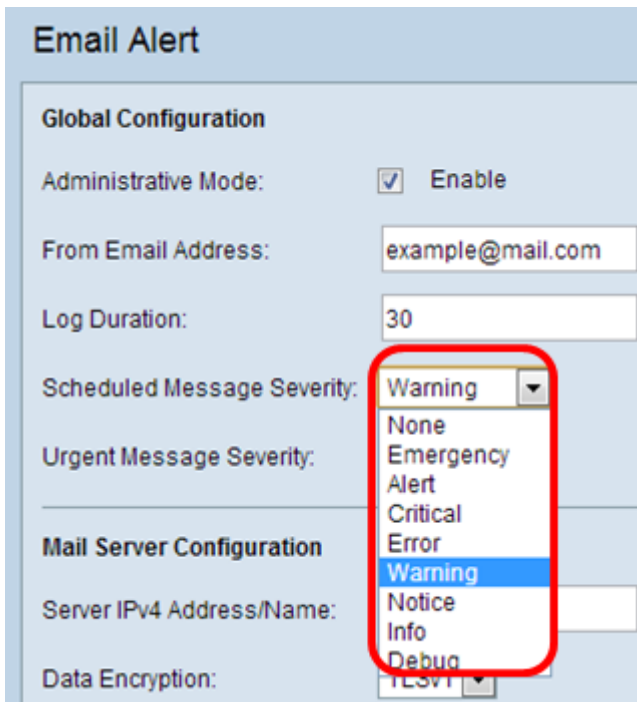
Urgent Message Severity:

Paso 5. Para establecer la gravedad del mensaje programado, elija el tipo de mensaje apropiado que se enviará, como Emergency, Alert, Critical, Error, Warning, Notice, Info o Debug. Estos mensajes se envían cada vez que caduca la Duración del registro. Estas opciones se muestran de forma diferente en la utilidad basada en Web, en función del modelo del dispositivo que esté utilizando.

Para WAP131, WAP150, WAP351 y WAP361, active el tipo de mensaje apropiado en las casillas de verificación de Gravedad del mensaje programado.



Para WAP121, WAP321, WAP371, WAP551, WAP561, WAP571 y WAP571E, haga clic en el tipo de mensaje apropiado en la lista desplegable de gravedad del mensaje programado.



Ninguno: no se envía ningún mensaje.

Emergencia: este tipo de mensaje se envía al usuario cuando el dispositivo se encuentra en una situación crítica y se requiere atención inmediata.

Alerta: este tipo de mensaje se envía al usuario cuando se produce una acción diferente a la configuración normal.

Crítico: este tipo de mensaje se envía al usuario cuando hay una situación en la que un puerto está caído o el usuario no puede acceder a la red. Se requiere una acción inmediata.

Error: este tipo de mensaje se envía al usuario cuando hay un error de configuración.

Advertencia: este tipo de mensaje se envía al usuario cuando otro usuario intenta acceder a las áreas restringidas.

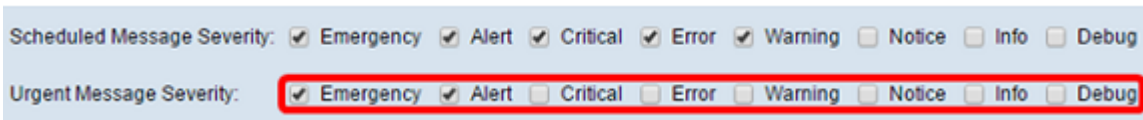
Aviso: este tipo de mensaje se envía al usuario cuando hay cambios de baja prioridad en la red.

Información: este tipo de mensaje se envía al usuario para describir cómo se comporta la red.

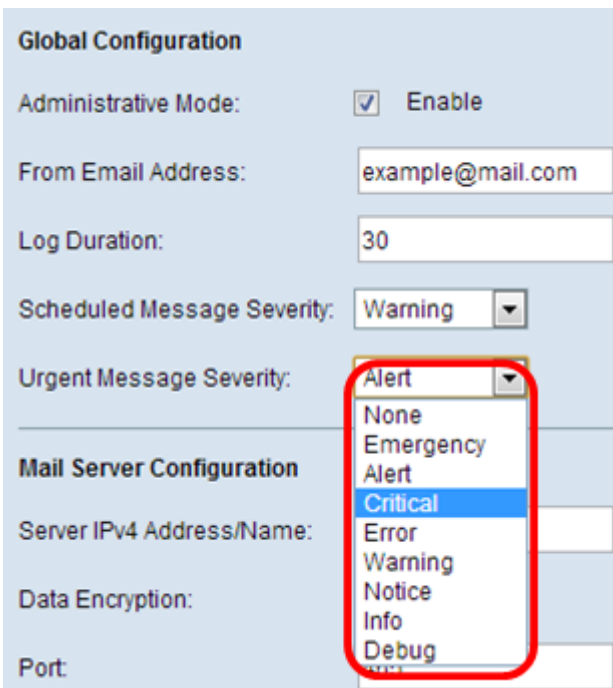
Depuración: este tipo de mensaje se envía al usuario con los registros del tráfico de red.

Paso 6. Para establecer la gravedad del mensaje urgente, elija el tipo apropiado de mensaje urgente que se enviará como Emergencia, Alerta, Crítico, Error, Advertencia, Aviso, Información o Depuración. Estos mensajes se envían inmediatamente. Estas opciones se muestran de forma diferente en la utilidad basada en Web, en función del modelo del dispositivo que esté utilizando.

Para WAP131, WAP150, WAP351 y WAP361, active el tipo de mensaje urgente apropiado en las casillas de verificación Urgente Message Severity.



Para WAP121, WAP321, WAP371, WAP551, WAP561, WAP571 y WAP571E, haga clic en el tipo de mensaje urgente apropiado en la lista desplegable Urgente Gravedad del mensaje.



Nota: Si la opción está establecida en Ninguno, no se envía ningún mensaje.

Paso 7. Ingrese el nombre de host válido del servidor de correo o la dirección IP en el campo *Server IPv4 Address/Name*.

Nota: En el ejemplo siguiente, se utiliza 200.168.20.10.

Mail Server Configuration

Server IPv4 Address/Name: 200.168.20.10

Data Encryption: TLSv1

Port: 465

Username: Cisco_1

Password:

Paso 8. Elija el modo de seguridad en la lista desplegable Cifrado de datos. Las opciones disponibles son:

- TLSv1: Transport Layer Security versión 1 es un protocolo criptográfico que proporciona seguridad e integridad de datos para la comunicación a través de Internet.
- Open: es el protocolo de cifrado predeterminado pero no tiene medidas de seguridad para el cifrado de datos.

Mail Server Configuration

Server IPv4 Address/Name: 200.168.20.10

Data Encryption: Open
✓ TLSv1

Port: 465

Username: Cisco_1

Password:

Nota: En este ejemplo, se elige TLSv1. Si selecciona Abrir, vaya directamente al [Paso 12](#).

Paso 9. Introduzca el número de puerto del servidor de correo en el campo *Port*. Se trata de un número de puerto saliente que se utiliza para enviar correos electrónicos. El intervalo de números de puerto válido es de 0 a 65535 y el valor predeterminado es 465 para el protocolo simple de transferencia de correo (SMTP).

Mail Server Configuration

Server IPv4 Address/Name: 200.168.20.10

Data Encryption: TLSv1

Port: 465

Username: Cisco_1

Password:

Paso 10. Ingrese el nombre de usuario para la autenticación en el campo *Nombre de usuario*.

Mail Server Configuration

Server IPv4 Address/Name: 200.168.20.10

Data Encryption: TLSv1

Port: 465

Username: Cisco_1

Password:

Nota: Cisco_1 se utiliza como ejemplo.

Paso 11. Introduzca la contraseña para la autenticación en el campo *Password*.

Mail Server Configuration

Server IPv4 Address/Name: 200.168.20.10

Data Encryption: TLSv1

Port: 465

Username: Cisco_1

Password:

[Paso 12.](#) En Message Configuration (Configuración de mensajes), introduzca la dirección de correo electrónico necesaria en los campos *To Email Address 1, 2 y 3*.

Nota: Según el requisito, puede introducir valores en todos los campos *To Email Address* (*Dirección de correo electrónico de destino*) o introducir sólo una dirección de correo electrónico y dejar el resto en blanco.

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

Paso 13. Introduzca el asunto del correo electrónico en el campo *Asunto del correo electrónico*. El asunto puede tener hasta 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: En este ejemplo, se utiliza el mensaje de registro del AP.

Paso 14. Haga clic en **Probar correo** para validar las credenciales configuradas del servidor de correo. Esto envía un correo electrónico a las direcciones de correo electrónico configuradas para comprobar que la configuración 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:

Paso 15. Click **Save**.

Message Configuration

To Email Address 1:

To Email Address 2:

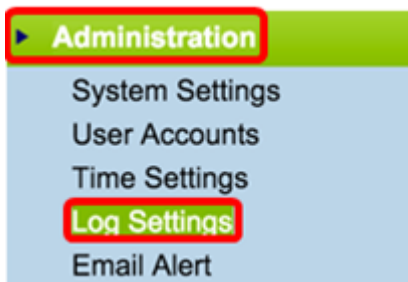
To Email Address 3:

Email Subject:

Configuración de los parámetros de registro

Esta área configura localmente los registros del sistema y de eventos en la volátil y la NVRAM.

Paso 1. Inicie sesión en la utilidad basada en Web del punto de acceso para elegir **Administration > Log Settings**.



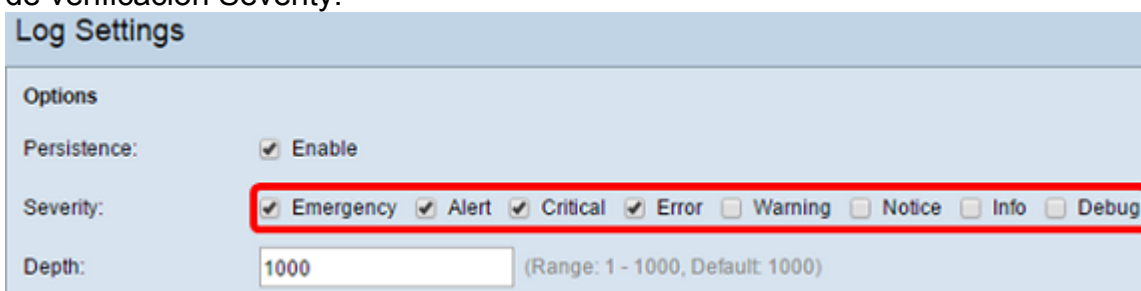
Paso 2. (Opcional) Si desea que los registros se guarden permanentemente para que la configuración permanezca mientras se reinicia WAP, active Persistencia activando la casilla de verificación **Enable**. Esto es especialmente útil en caso de que se reinicie el sistema cuando se produzca un evento o fallo no deseado. Se pueden guardar hasta 128 mensajes de registro en la NVRAM, después de lo cual se sobrescriben los registros.



Nota: Si la opción Activar está desactivada, los registros se guardan en la memoria volátil.

Paso 3. Para establecer la gravedad, elija el tipo de mensaje adecuado que se enviará, como Emergencia, Alerta, Crítica, Error, Advertencia, Aviso, Información o Depuración. Estos mensajes se envían cada vez que caduca la Duración del registro. Estas opciones se muestran de forma diferente en la utilidad basada en Web, en función del modelo del dispositivo que esté utilizando.

Para WAP131, WAP150, WAP351 y WAP361, active el tipo de mensaje apropiado en las casillas de verificación Severity.



Para WAP121, WAP321, WAP371, WAP551, WAP561, WAP571 y WAP571E, haga clic en el tipo de mensaje adecuado de la lista desplegable Gravedad.

The screenshot shows the 'Log Settings' window. Under the 'Options' section, 'Persistence' is checked and set to 'Enable'. The 'Severity' dropdown menu is open, showing a list of 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 visible with a 'Remote Log' checkbox and a 'Server IPv4/IPv6 Address/Name' field.

Paso 4. A medida que se generan los mensajes de registro, se colocan en una cola de transmisión. Especifique el número de mensajes que se pueden poner en cola a la vez en la memoria volátil en el campo *Profundidad*. Se pueden poner en cola hasta 512 mensajes al mismo tiempo.

Para WAP131, WAP150, WAP351 y WAP361, introduzca el intervalo de profundidad en el campo Profundidad. El intervalo es de 1 a 1000. El valor predeterminado es 1000.

This screenshot shows the 'Log Settings' window with 'Persistence' checked and 'Enable'. Under 'Severity', 'Emergency', 'Alert', and 'Info' are all checked. The 'Depth' field is a text input containing the number '1000', which is highlighted with a red box.

Para WAP121, WAP321, WAP371, WAP551, WAP561, WAP571 y WAP571E, introduzca el intervalo de profundidad en el campo Profundidad. El rango es 1-512 y 512 es el valor predeterminado. Para este ejemplo, se utiliza 67.

This screenshot shows the 'Log Settings' window with 'Persistence' checked and 'Enable'. The 'Severity' dropdown is set to '7 - Debug'. The 'Depth' field is a text input containing the number '67', which is highlighted with a red box.

Paso 5. Click **Save**.

Nota: El punto de acceso adquiere información de fecha y hora mediante el uso de un servidor Network Time Protocol . Estos datos están en formato UTC (Hora del meridiano de Greenwich).

Estas configuraciones deben propagar el registro de eventos en su dispositivo local y recibir alertas por correo electrónico.