

# Configurare e visualizzare i registri di sistema (syslog) su WAP125 e WAP581

## Obiettivo

Gli eventi di sistema sono attività che possono richiedere attenzione e che richiedono l'adozione delle azioni necessarie per eseguire il sistema senza problemi e prevenire errori. Questi eventi vengono registrati come registri. I registri di sistema (syslog) consentono all'amministratore di tenere traccia di eventi particolari che si verificano nel dispositivo.

Le impostazioni del registro definiscono le regole di registrazione e le destinazioni di output per i messaggi, le notifiche e altre informazioni man mano che sulla rete vengono registrati vari eventi. Questa funzionalità consente di notificare al personale responsabile che verranno intraprese le azioni necessarie quando si verifica un evento. I registri possono essere inviati a un server remoto dove vengono registrati tutti i registri dell'attività di rete. Per informazioni su come configurare le impostazioni del registro remoto, fare clic [qui](#). I log possono essere inviati anche agli amministratori di rete tramite e-mail di allarme. Per informazioni su come configurare le impostazioni di posta elettronica e personalizzare le notifiche di posta elettronica, fare clic [qui](#).

In questo articolo viene illustrato come gestire le impostazioni del registro di sistema ed esportare le impostazioni del registro su WAP125 e WAP581.

## Dispositivi interessati

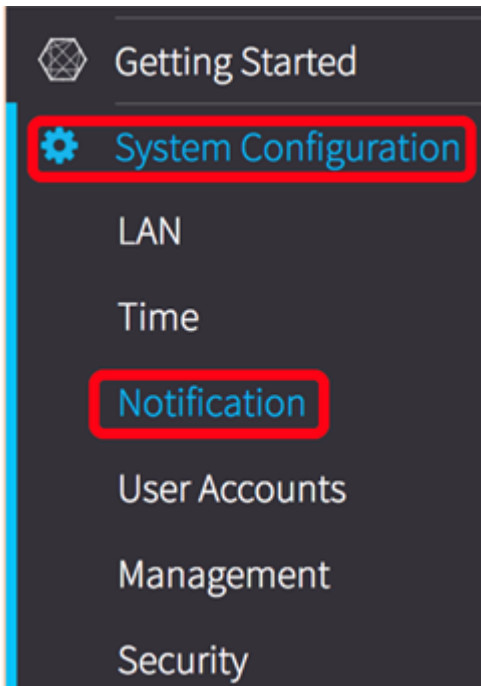
- WAP125
- WAP581

## Versione del software

- 1.0.0.4

## Configurazione delle impostazioni dei syslog

Passaggio 1. Accedere all'utility basata sul Web di WAP e scegliere **Configurazione di sistema > Notifica**.



Passaggio 2. Selezionare la casella di controllo **Abilita** persistenza per salvare i registri di sistema nella memoria non volatile. In questo modo, i log rimangono sul WAP dopo il riavvio. Un massimo di 1000 messaggi vengono salvati nella memoria non volatile e, quando viene raggiunto il limite, l'ultimo messaggio viene sovrascritto.

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...'.

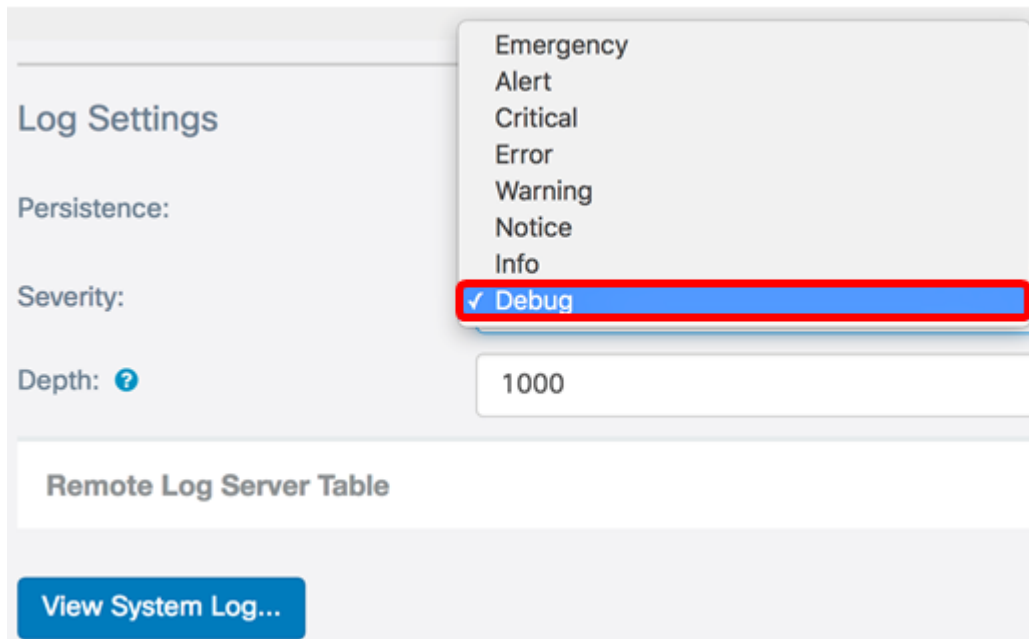
Remote Log Server Table	
-------------------------	--

Passaggio 3. Scegliere un'opzione dall'elenco a discesa Gravità. La severità scelta include tutti i livelli superiori, pertanto i log vengono conservati per tutti i livelli di severità dal livello superiore fino al livello scelto.

- Emergenza: livello 0. Il sistema non è utilizzabile. Questo viene in genere trasmesso a tutti i processi.
- Alert: livello 1. È necessario intervenire immediatamente.
- Critico: livello 2. Condizioni critiche, ad esempio un errore della periferica hardware.
- Errore: livello 3. Condizioni di errore.
- Avvertenza: livello 4. Condizioni di avvertenza.
- Avviso: livello 5. Condizione normale ma significativa.
- Info - Livello 6. Solo messaggi informativi. Condizione che non rappresenta una condizione di errore, ma che può richiedere una gestione speciale.

- Debug — livello 7. I messaggi di debug contengono informazioni normalmente utili solo per il debug di un programma.

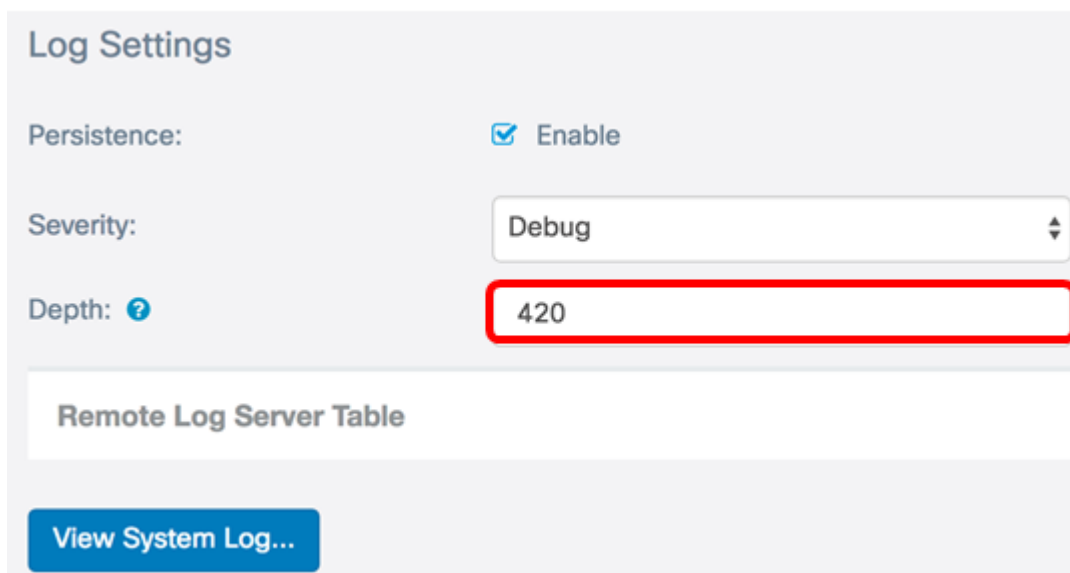
**Nota:** Nell'esempio riportato di seguito, viene scelto Debug.



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.

Passaggio 4. Nel campo *Depth*, immettere un valore compreso tra 1 e 1000 per impostare il numero di messaggi syslog che possono essere memorizzati nella memoria volatile. Tutti i registri nella memoria volatile vengono eliminati al riavvio del sistema.

**Nota:** nell'esempio viene utilizzato 420.



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

Passaggio 5. Fare clic su [Save](#).

Passaggio 6. Fare clic sul pulsante **View System Log...** per visualizzare i log.

## Log Settings

Persistence:  Enable

Severity:

Depth:

Remote Log Server Table

[View System Log...](#)

Nella tabella vengono visualizzati l'indicatore orario, la gravità, il servizio e la descrizione. Le definizioni sono le seguenti:

Timestamp: l'ora in cui è stato creato il messaggio syslog. La data viene visualizzata nel formato MM-GG-AAAA e l'ora nel formato militare.

- Gravità — Gravità del messaggio syslog.
- Servizio - Il servizio associato all'evento.
- Descrizione — il messaggio principale del 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

Passaggio 7. (Facoltativo) Nell'area Intestazione della tabella Log di sistema, fare clic sulle frecce per filtrare i dati in ordine cronologico o alfabetico.

**Nota:** In questo esempio, viene fatto clic su Timestamp (Data e ora) per disporre le voci del

syslog dalla più recente alla prima.



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

Passaggio 8. (Facoltativo) Per visualizzare altri log, fare clic sui **numeri di pagina** per scorrere le pagine di log.



Passaggio 9. (Facoltativo) Fare clic sul pulsante **Aggiorna** per aggiornare la pagina e visualizzare i log più recenti.



Passaggio 10. (Facoltativo) Per cancellare o cancellare i registri dalla tabella, fare clic su **Cancella tutto**.



Passaggio 11. (Facoltativo) Per esportare e scaricare i registri in un computer, fare clic su **Download**. Verrà avviato un download nel browser.



**Nota:** Il file viene salvato in 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
```

Passaggio 12. Fare clic su **Indietro** per tornare alla pagina Configurazione notifica.

Refresh

Clear All

Download

Back

A questo punto i log sono stati esportati su WAP125 e WAP581.