

# Stysteem berichtenlogboek instellen (Syslogs) op een CBW-netwerk

## Doel

Het doel van dit artikel is om houtkap op een Cisco Business Wireless (CBW) traditioneel of mesh-netwerk in te stellen en te bekijken.

## Toepasselijke apparaten | Software versie

- 140 AC ([gegevensblad](#)) | 10.4.1.0 ([laatste download](#))
- 145 AC ([informatieblad](#)) | 10.4.1.0 ([laatste download](#))
- 240 AC ([gegevensblad](#)) | 10.4.1.0 ([laatste download](#))

## Inleiding

Cisco Business draadloze access points zijn op 802.11a/b/g/n/ac (Wave 2) gebaseerd, met interne antennes. Ze kunnen worden gebruikt als traditionele standalone apparaten of als onderdeel van een netwerk met mazen.

Zodra uw netwerk is opgezet, gebeuren er dingen die aandacht nodig kunnen hebben. Om van deze gebeurtenissen op de hoogte te blijven, kunt u de Vastlegging van de systeem berichten controleren, die vaak Syslogs worden genoemd.

Wanneer u op de hoogte bent van gebeurtenissen, kan dit ertoe bijdragen dat het netwerk vlot functioneert en fouten voorkomen. Syslogs zijn handig voor het oplossen van netwerkproblemen, het zuiveren van pakketstroom en het bewaken van gebeurtenissen.

Deze logbestanden kunnen worden bekeken op de Web User Interface (UI) van de primaire AP en, indien geconfigureerd, op de externe logservers. Voorvallen worden gewoonlijk uit het systeem gewist als ze worden herstart als ze niet op een externe server worden opgeslagen.


## Vastlegging systeem berichten instellen

In dit ingesloten gedeelte worden tips voor beginners gemarkeerd.

## Inloggen

Log in op de webgebruikersinterface (UI) van de primaire AP. Om dit te doen, open een web browser en voer `https://ciscobusiness.cisco` in. U kunt een waarschuwing ontvangen voordat u doorgaat. Voer uw aanmeldingsgegevens in. U kunt ook toegang krijgen tot de primaire AP door `https://[ipaddress]` (van de primaire AP) in een webbrowsers in te voeren.

## Tips voor gereedschap

Als u vragen hebt over een veld in de gebruikersinterface, controleert u op een snijpunt dat er als volgt uitziet: 

## Problemen met de locatie van het pictogram Hoofdmenu uitvouwen?

Navigeer naar het menu aan de linkerkant van het scherm, als u de menuknop niet ziet, klik dan



op dit pictogram om het zijbalkmenu te openen.

### Cisco Business-app

Deze apparaten hebben metgezelapps die bepaalde beheerfuncties delen met de web gebruikersinterface. Niet alle functies in de gebruikersinterface van het web zijn in de app beschikbaar.

[iOS-app downloaden](#) [Android-app downloaden](#)

### Veelgestelde vragen

Als u nog steeds onbeantwoorde vragen hebt, kunt u ons vaak gestelde vragen document controleren. [FAQ](#)

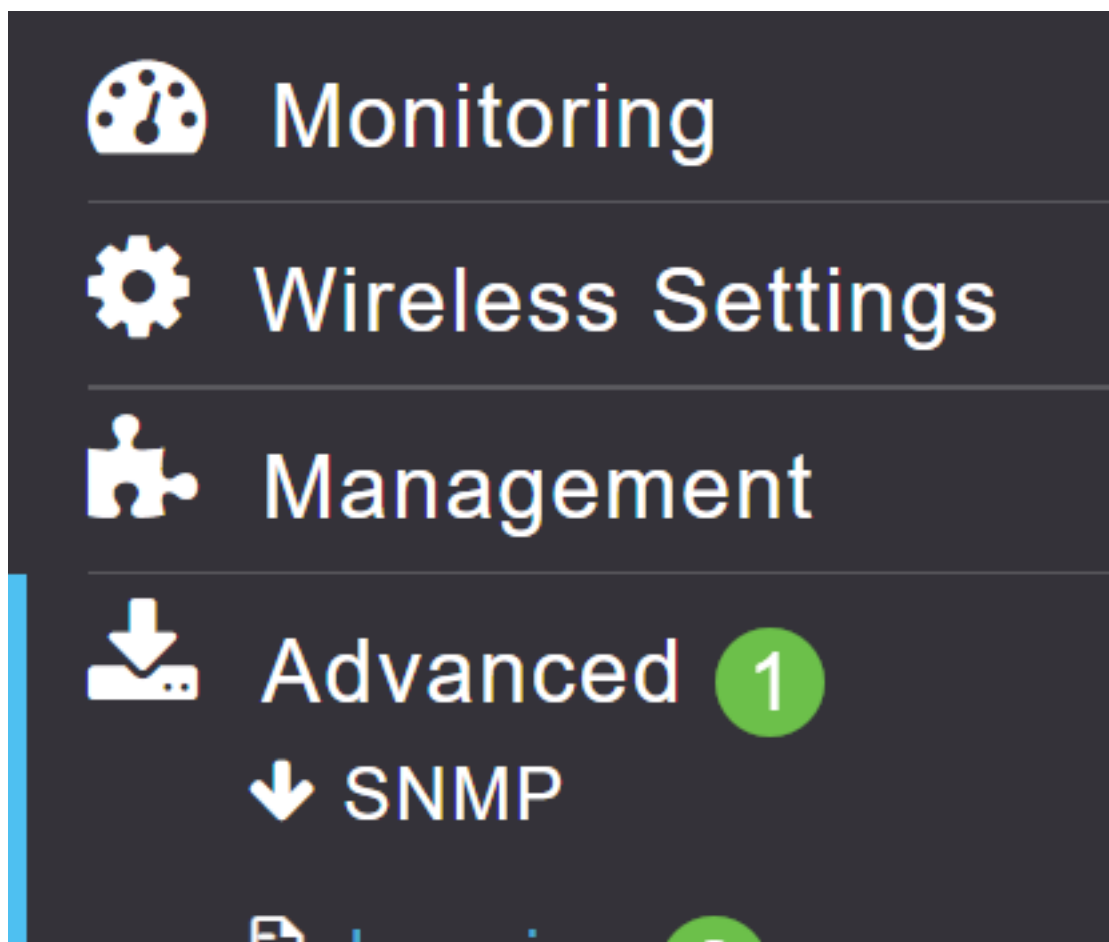
### Stap 1

Log in op de web UI van de primaire AP. Om dit te doen, open een web browser en voer <https://ciscobusiness.cisco> in. U kunt een waarschuwing ontvangen voordat u doorgaat. Voer je geloofsbrieven in.

U kunt ook toegang krijgen tot de primaire AP door `https://<ipaddress>` (of de Primaire AP) in een webbrowser in te voeren. Voor sommige acties kunt u de Cisco Business Mobile app gebruiken.

### Stap 2

Selecteer **Geavanceerd > Vastleggen**.

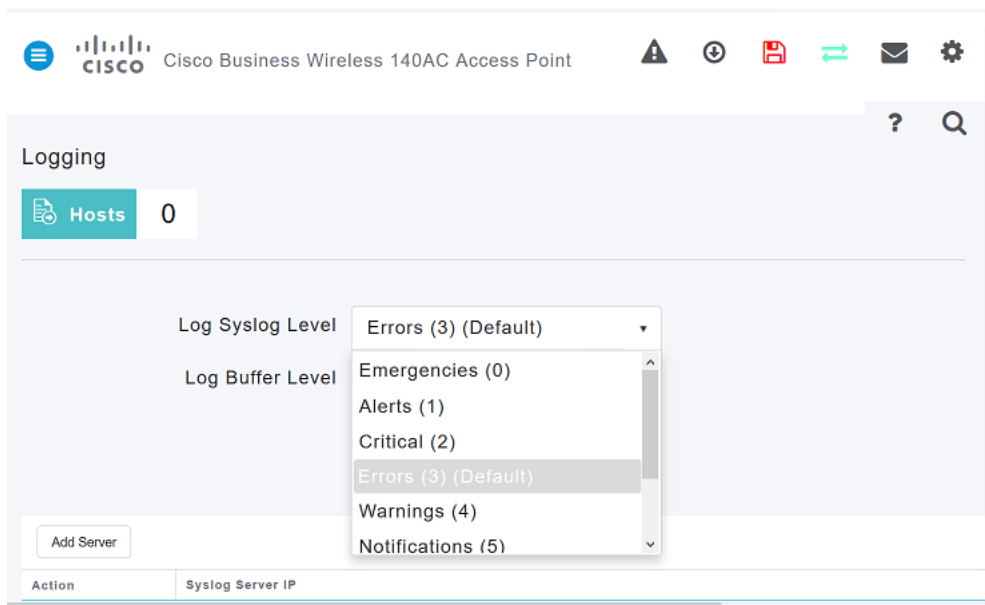


## Stap 3

Klik op het inlogniveau. Selecteer vanuit het vervolgkeuzemenu voor het niveau van de meldingen. Fout (3) is de default. Dit betekent dat een niveau 3 of meer ernstig is gelogd.

In de volgorde van ernst:

- *Noodgevallen* (hoogste ernst) — Dit type bericht wordt gelogd wanneer het apparaat in een kritieke situatie verkeert en er onmiddellijke aandacht nodig is. Het systeem is onbruikbaar.
- *Waarschuwingen* — Dit type bericht is vastgelegd wanneer er een voorwaarde is die onmiddellijke aandacht nodig heeft.
- *kritiek*
- *fouten* (standaardinstelling)
- *Waarschuwingen*
- *Meldingen*
- *informatief*
- *Debugging* (lage ernst) — Dit wordt normaal gesproken alleen gebruikt wanneer u actief problemen oplossen, aangezien u vrij snel overstroomd raakt met logs.



## Stap 4

Klik op **Apply** (Toepassen).

Apply

## Stap 5

Logs worden weergegeven wanneer u op de logpagina scant. Klik op **Wissen** als u de logbestanden wilt wissen. Als u geen externe SLB-server wilt instellen, gaat u naar [Stap 8](#).

### LOGS

1

```
*spamReceiveTask: Mar 11 12:25:30.558: %APF-3-MESH_EXTENDER_AUTHORIZED:
spam_radius.c:288 Wireless Mesh Extender - 68:ca:e4:6e:15:58 authorized by Master AP
*spamApTask0: Mar 11 12:25:30.557: %APF-3-MESH_EXTENDER_ASSOC_REQ:
spam_meshsec.c:1678 Wireless Mesh Extender - 68:ca:e4:6e:15:58 is sending Association
Request to join the network
*spamApTask0: Mar 11 12:24:54.556: %LWAPP-3-AP_DEL: spam_lrad.c:6079
68:ca:e4:6e:ba:60: Entry deleted for AP: 192.168.1.110 (5264) reason : Echo Timer Expiry.
*spamApTask0: Mar 11 12:24:54.551: %WLAN-3-AP_DISCONNECTED: capwap_ac_sm.c:8410
AP68CA.E46E.1558 is disconnected.
*spamApTask0: Mar 11 12:24:54.550: %CAPWAP-3-ECHO_ERR: capwap_ac_sm.c:8373 Did not
receive heartbeat reply; AP: 68:ca:e4:6e:ba:60
*spamReceiveTask: Mar 11 12:23:09.460: %APF-3-MESH_EXTENDER_AUTHORIZED:
spam_radius.c:288 Wireless Mesh Extender - 68:ca:e4:6e:15:58 authorized by Master AP
```

## Stap 6 (optioneel)

Als u wilt dat de logbestanden naar een externe server worden verzonden, klikt u op **Server toevoegen**.

The screenshot shows the 'Logging' configuration page. At the top, there is a 'Hosts' section with a document icon and the number '0'. Below this, there are two dropdown menus: 'Log Syslog Level' and 'Log Buffer Level', both set to 'Errors (3) (Default)'. A green 'Apply' button is centered below these dropdowns. At the bottom left, there is a green 'Add Server' button. Below the 'Add Server' button is a table with two columns: 'Action' and 'Syslog Server IP'.

## Stap 7 (optioneel)

Voer in het veld *IP-server Syslog Server* het IPv4-adres in van de server waarop de slogberichten moeten worden verzonden. Klik op **Apply** (Toepassen).

This screenshot shows the same 'Logging' configuration page as in Step 6, but with a blue dialog box overlaid. The dialog box has the title 'Add Syslog Server IP' and a text input field. A green circle with the number '1' is next to the input field. Below the dialog box, the 'Apply' button from the main page is visible, and a green circle with the number '2' is next to it. At the bottom of the dialog box, there are 'Apply' and 'Cancel' buttons.

## Stap 8

U moet een TFTP-server hebben geopend en de Syslog-functie moet worden ingeschakeld, zodat de logbestanden naar een bestand op de server kunnen worden verzonden.

The screenshot shows the 'TFTP Server' configuration window. The window title is 'Tftp64 by Ph. Jonin'. It has a 'Current Directory' field set to 'C:\Users\aren\Desktop' and a 'Server interfaces' dropdown set to '10.13.53.0/24 ThinkPad T81 3 Dock Ethernet'. Below these fields are tabs for 'Tftp Server', 'Tftp Client', 'Syslog server', and 'Log viewer'. The 'Syslog server' tab is selected, showing a table with columns 'test', 'from', and 'date'. At the bottom of the window, there are 'Clear' and 'Copy' buttons, and 'About', 'Settings', and 'Help' buttons.

## Stap 9

Vergeet niet uw configuraties op te slaan door op het pictogram Opslaan in het rechter bovenpaneel van het Web UI-scherm te klikken.



## Voorbeeld van systeemberichten

In dit voorbeeld, toont het bericht hoog verkeersgebruik. Als dit in de syslogs zou verschijnen, zou je het radiofrequentiekanaal waarschijnlijk willen veranderen in een kanaal dat minder gericht is op een stabielere bedrijfsomgeving.

```
*RRM-DCLNT-5_0: Dec 25 16:51:34:543: %RRM-3-HIGHCHANNEL_UTN: mmLrad.c:7678 Interference is high on AP: APA453.0E1F.E480 [Level: 85] on Radio: 5Ghz(Radio2)
```

## Conclusie

U hebt nu toegang tot de systeemregisters. U kunt teruggaan en het ernst-niveau wijzigen of een externe server op elk moment toevoegen. Dit zou u op de hoogte moeten houden van mogelijke kwesties in het netwerk.

[Veelgestelde vragen](#) [Straal upgrade van firmware](#) [RLAN's](#) [Toepassingsprofielen](#) [Clientprofielen](#) [Primaire AP-tools](#) [Umbrella](#) [WLAN-gebruikers](#) [Vastlegging traffic shaping](#) [Rogues](#) [Interferiers](#) [Configuratie-beheer](#) [mesh-modus voor poortconfiguratie](#)