

# Aumente el descanso de la autenticación Web en el regulador del Wireless LAN

TAC

ID del Documento: 118963

Actualizado: Mayo 26, 2015

Contribuido por Dhiresh Yadav, ingeniero de Cisco TAC.



[Descarga PDF](#)



[Imprimir](#)

[Comentarios](#)

## Productos Relacionados

- [Wireless, LAN \(WLAN\)](#)
- [Cliente de Cisco VPN](#)
- [Software del controlador LAN de la tecnología inalámbrica de Cisco](#)

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Verificación](#)

[Troubleshooting](#)

[Discusiones relacionadas de la comunidad del soporte de Cisco](#)

## Introducción

Este documento proporciona los pasos requeridos para que el Service Set Identifier (SSID) del Red-auth permita un acceso de usuario de VPN sin la autenticación completa y sin una desconexión cada pocos minutos. Para alcanzar esto, un usuario debe aumentar el descanso de la autenticación Web (Red-auth) en el regulador del Wireless LAN (WLC).

## Prerrequisitos

## Requisitos

Cisco recomienda que usted sabe configurar el WLC para la operación básica y el Red-auth.

## Componentes Utilizados

La información en este documento se basa en un WLC de las Cisco 5500 Series que funciona con la versión de firmware 8.0.100.0.

**Observe** la configuración y la explicación del Red-auth en este documento es aplicable a todos los modelos y a cualquier versión de imagen 8.0.100.0 del WLC de la red del Cisco Unified Wireless y posterior.

## Antecedentes

En muchas configuraciones de la red del cliente, hay las configuraciones que permiten un grupo de acceso de los usuarios o de los invitados VPN de la compañía a ciertos IP Addresses sin el requisito de pasar la Seguridad del Red-auth. Estos usuarios reciben los address IP y conectan directamente con el VPN sin la necesidad de cualquier credencial para conseguir autenticados vía la Seguridad del Red-auth. Este SSID pudo ser funcionando por otro conjunto de los usuarios que también pasan con el Red-auth normal y lleno para tener el acceso a internet. Este escenario es posible vía una PRE-autenticación ACL configurada en el SSID que permite las conexiones del usuario a los IP Addresses VPN antes de que pasen la autenticación. El problema para estos usuarios de VPN es que escogen la dirección IP pero nunca acaba el Red-auth completo. Por lo tanto, se activa el temporizador del descanso del Red-auth y el cliente deauthenticated:

```
*apfReceiveTask: Sep 03 12:01:55.694: 00:24:d7:cd:ac:30 172.30.0.118 WEBAUTH_REQD (8)
Web-Auth Policy timeout
```

```
*apfReceiveTask: Sep 03 12:01:55.694: 00:24:d7:cd:ac:30 172.30.0.118 WEBAUTH_REQD (8)
Pem timed out, Try to delete client in 10 secs.
```

El valor de este descanso es 5 minutos y tiene un valor fijo en las versiones del WLC anterior de 7.6. Esta duración corta del descanso hace la red inalámbrica estar casi inutilizable para estas clases de usuarios. La capacidad para cambiar este valor se agrega en la versión 8.0 del WLC que permite que los usuarios accedan el VPN vía el PRE-auth ACL-permitido el tráfico.

## Configurar

Nota: Use la [Command Lookup Tool](#) ([clientes registrados solamente](#)) para obtener más información sobre los comandos usados en esta sección.

Complete estos pasos para aumentar el descanso del Red-auth en el WLC:

1. Cree un ACL que permita el tráfico a la dirección IP

Access Control Lists > Edit < Back

**General**

Access List Name: VPNUSER

Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1.	Permit	0.0.0.0 /	192.168.145.5 /	Any	Any	Any	Any	Any	0
		0.0.0.0 /	255.255.255.255 /	Any	Any	Any	Any	Any	0
2.	Permit	192.168.145.5 /	0.0.0.0 /	Any	Any	Any	Any	Any	0
		255.255.255.255 /	0.0.0.0 /	Any	Any	Any	Any	Any	0
3.	Deny	0.0.0.0 /	0.0.0.0 /	Any	Any	Any	Any	Any	0

VPN.

2. Aplique el ACL como **Preauthentication ACL** en la configuración del Wireless LAN (red inalámbrica (WLAN)) bajo Seguridad de la capa
- 3.



3. Inicie sesión vía el CLI y ingrese el **comando timeout del red-auth de la Seguridad de WLAN de los config** para aumentar el valor de agotamiento del tiempo del Red-auth. (WLC)>`config wlan security web-auth timeout ?`  
 <value> Configures Web authentication Timeout (300-14400 seconds).  
 (WLC)>`config wlan security web-auth timeout 3600 <Wlan_id>`

## Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

El valor de tiempo de espera de sesión del Red-auth para su red inalámbrica (WLAN) aparece como esta salida de ejemplo muestra:

```
(WLC)>show wlan 10
Web Based Authentication..... Enabled
Web Authentication Timeout..... 3600
```

## Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Ingrese el comando del **< MAC address > del cliente del debug** para ver el temporizador del Red-auth comenzar para el usuario que conecta con el VPN sin la autenticación.

¿Era este documento útil? [Sí ningún](#)

Gracias por su feedback.

[Abra un caso de soporte](#) (requiere un [contrato de servicios con Cisco](#).)

## Discusiones relacionadas de la comunidad del soporte de Cisco

[La comunidad del soporte de Cisco](#) es un foro para que usted haga y conteste a las preguntas, las sugerencias de la parte, y colabora con sus pares.

Refiera a los [convenios de los consejos técnicos de Cisco](#) para la información sobre los convenios usados en este documento.

Actualizado: Mayo 26, 2015

ID del Documento: 118963