Configuring IPv6 Web Authentication

Prerequisites for IPv6 Web Authentication

The following configurations must be in place before you start with IPv6 Web Authentication:

- IPv6 Device Tracking.
- IPv6 DHCP Snooping.
- Disable security of type 802.1x on the wlan.
- Each WLAN must have a vlan associated to it.
- Change the default wlan setting from **shutdown** to **no shutdown**.

Related Topics

Enabling Security on the WLAN, on page 4

Restrictions for IPv6 Web Authentication

The following restrictions are implied when using IPv6 web authentication:

Related Topics

Enabling Security on the WLAN, on page 4

Information About IPv6 Web Authentication

Web authentication is a Layer 3 security feature and the switch disallows IP traffic (except DHCP and DNS -related packets) from a particular client until it supplies a valid username and password. It is a simple authentication method without the need for a supplicant or client utility. Web authentication is typically used by customers who deploy a guest-access network. Traffic from both, HTTP and HTTPS, page is allowed to display the login page.

Note Web authentication does not provide data encryption and is typically used as simple guest access for either a hot spot or campus atmosphere, where connectivity is always a factor.

A WLAN is configured as **security webauth** for web based authentication. The switch supports the following types of web based authentication:

- Web Authentication – The client enters the credentials in a web page which is then validated by the Wlan controller.
- Web Consent – The Wlan controller presents a policy page with Accept/Deny buttons. Click Accept button to access the network.

A Wlan is typically configured for open authentication, that is without Layer 2 authentication, when web-based authentication mechanism is used.

Web Authentication Process

The following events occur when a WLAN is configured for web authentication:

- The user opens a web browser and enters a URL address, for example, *http://www.example.com*. The client sends out a DNS request for this URL to get the IP address for the destination. The switch bypasses the DNS request to the DNS server, which in turn responds with a DNS reply that contains the IP address of the destination *www.example.com*. This, in turn, is forwarded to the wireless clients.
- The client then tries to open a TCP connection with the destination IP address. It sends out a TCP SYN packet destined to the IP address of *www.example.com*.
- The switch has rules configured for the client and cannot act as a proxy for *www.example.com*. It sends back a TCP SYN-ACK packet to the client with source as the IP address of *www.example.com*. The client sends back a TCP ACK packet in order to complete the three-way TCP handshake and the TCP connection is fully established.
- The client sends an HTTP GET packet destined to *www.example.com*. The switch intercepts this packet and sends it for redirection handling. The HTTP application gateway prepares an HTML body and sends it back as the reply to the HTTP GET requested by the client. This HTML makes the client go to the default web-page of the switch, for example, *http://<Virtual-Server-IP>/login.html*.
- The client closes the TCP connection with the IP address, for example, *www.example.com*.
- If the client wants to go to virtual IP, the client tries to open a TCP connection with the virtual IP address of the switch. It sends a TCP SYN packet for virtual IP to the switch.

- The switch responds back with a TCP SYN-ACK and the client sends back a TCP ACK to the switch in order to complete the handshake.
- The client sends an HTTP GET for */login.html* destined to virtual IP in order to request for the login page.
- This request is allowed to the web server of the switch, and the server responds with the default login page. The client receives the login page in the browser window where the user can log in.

Related Topics

Disabling WPA, on page 3
Enabling Security on the WLAN, on page 4
Enabling a Parameter Map on the WLAN, on page 4
Enabling Authentication List on WLAN, on page 5
Configuring a Global WebAuth WLAN Parameter Map, on page 5
Configuring the WLAN, on page 6
Enabling IPv6 in Global Configuration Mode, on page 7
Verifying the Parameter Map, on page 8
Verifying Authentication List, on page 8

How to Configure IPv6 Web Authentication

Disabling WPA

Before you begin

Disable 802.1x. A typical web authentication does not use Layer 2 security. Use this configuration to remove Layer 2 security.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**wlan test1 2 test1** **Example:** `Device(config)# wlan test1 2 test1`	Creates a WLAN and assign an SSID to it.
Step 3	**no security** wpa **Example:** `Device(config-wlan)# no security wpa`	Disables the WPA support for Wlan.

What to do next

Enable the following:

- Security Web Authentication.
- Parameter Local.
- Authentication List.

Related Topics

Web Authentication Process, on page 2

Enabling Security on the WLAN

Procedure

	Command or Action	Purpose
Step 1	**parameter-map type web-auth global** **Example:** `Device(config)# parameter-map type web-auth global`	Applies the parameter map to all the web-auth wlans.
Step 2	**virtual-ip ipv4 `192.0.2.1`** **Example:** `Device(config-params-parameter-map)# virtual-ip ipv4 192.0.2.1`	Defines the virtual gateway IPv4 address.
Step 3	**virtual-ip ipv6 `2001:db8::24:2`** **Example:** `Device(config-params-parameter-map)# virtual-ip ipv6 2001:db8::24:2`	Defines the virtual gateway IPv6 address.

Related Topics

Prerequisites for IPv6 Web Authentication, on page 1
Restrictions for IPv6 Web Authentication, on page 1
Web Authentication Process, on page 2

Enabling a Parameter Map on the WLAN

Procedure

	Command or Action	Purpose
Step 1	**security web-auth parameter-map `<mapname>`** **Example:**	Enables web authentication for the wlan and creates a parameter map.

	Command or Action	Purpose
	`Device(config-wlan)# security web-auth parameter-map webparalocal`	

Related Topics

Web Authentication Process, on page 2

Enabling Authentication List on WLAN

Procedure

	Command or Action	Purpose
Step 1	**security web-auth authentication-list `webauthlistlocal`** **Example:** `Device(config-wlan)# security web-auth`	Enables web authentication for the wlan and creates a local web authentication list.

Related Topics

Web Authentication Process, on page 2

Configuring a Global WebAuth WLAN Parameter Map

Use this example to configure a global web auth WLAN and add a parameter map to it.

Procedure

	Command or Action	Purpose
Step 1	**parameter-map type webauth global** **Example:** `Device (config)# parameter-map type webauth global`	Configures a global webauth and adds a parameter map to it.
Step 2	**virtual-ip ipv6 `2001:db8:4::1`** **Example:** `Device (config-params-parameter-map)# virtual-ip ipv6 2001:db8:4::1`	Defines a virtual gateway IP address that appears to the wireless clients for authentication.
Step 3	**ratelimit init-state-sessions `120`** **Example:** `Device (config-params-parameter-map)# ratelimit init-state-sessions 120`	Sets the global ratelimit to limit the bandwidth that the web clients can use on the switch to avoid over-flooding attacks.

	Command or Action	Purpose
Step 4	**max-https-conns 70** **Example:** `Device (config-params-parameter-map)# max-http-conns 70`	Sets the maximum number of attempted http connections on the switch to avoid over-flooding atatcks.

Related Topics

Web Authentication Process, on page 2
Configuring the WLAN, on page 6

Configuring the WLAN

Before you begin

- The WLAN must have a Vlan associated with it. By default, a new Wlan is always associated with Vlan 1, which can be changed as per the configuration requirements.
- Configure and enable the WLAN to *no shutdown*. By default, the Wlan is configured with the *shutdown* parameter and is disabled.

Procedure

	Command or Action	Purpose
Step 1	**wlan** *1* **Example:** `Device(config-wlan)# wlan 1 name vicweb ssid vicweb`	Creates a wlan and assign an SSID to it.
Step 2	**client vlan** *interface ID* **Example:** `Device(config-wlan)# client vlan VLAN0136`	Assigns the client to vlan interface.
Step 3	**security web-auth authentication list webauthlistlocal** **Example:** `Device(config-wlan)# security web-auth authentication-list webauthlistlocal`	Configures web authentication for the wlan.
Step 4	**security web-auth parameter-map global** **Example:** `Device(config-wlan)# security web-auth parameter-map global`	Configures the parameter map on the wlan.
Step 5	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Configures the security policy for a wlan. This enables the wlan.

	Command or Action	Purpose
Step 6	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Configures and enables the Wlan.
Step 7	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Configuring a Global WebAuth WLAN Parameter Map, on page 5
Web Authentication Process, on page 2
Enabling IPv6 in Global Configuration Mode, on page 7

Enabling IPv6 in Global Configuration Mode

Enable IPv6 in global configuration for web authentication.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**web-auth global** **Example:** `Device(config)# parameter-map type webauth global`	Globally configures the parameter map type as web authentication.
Step 3	**virtual IPv6** **Example:** `Device(config-params-parameter-map)# virtual-ip ipv6`	Selects IPv6 as the virtaul IP for web authentication. **Note** You can also select IPv4 as the preferred IP for web authentication.

Related Topics

Configuring the WLAN, on page 6
Web Authentication Process, on page 2
Verifying the Parameter Map, on page 8

Verifying IPv6 Web Authentication

Verifying the Parameter Map

Use the **show running configuration** command to verify the parameter map configured for Wlan.

Procedure

	Command or Action	Purpose
Step 1	**show running config** **Example:** `Deviceshow running config`	Displays the entire running configuration for the switch. Grep for parameter map to view the result.

```
wlan alpha 2 alpha
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth
 security web-auth authentication-list webauthlistlocal
 security web-auth parameter-map webparalocal
```

Related Topics

Enabling IPv6 in Global Configuration Mode, on page 7
Web Authentication Process, on page 2
Verifying Authentication List, on page 8

Verifying Authentication List

Use the **show running configuration** command to verify the authentication list configured for the Wlan.

Procedure

	Command or Action	Purpose
Step 1	**show running configuration** **Example:** `Device#show running-config`	Displays the Wlan configuration. `Device# show running-config`
Step 2	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

```
Device#show running-config
 ..................................
 ..................................
 ..................................
 wlan alpha 2 alpha
```

```
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list webauthlistlocal
security web-auth parameter-map webparalocal
.................................
.................................
.................................
```

Related Topics

Verifying the Parameter Map, on page 8
Web Authentication Process, on page 2

Additional References

Related Documents

Related Topic	Document Title
IPv6 command reference	*IPv6 Command Reference (Catalyst 3850 Switches)*
Web Authentication configuration	*Security Configuration Guide (Catalyst 3850 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for IPv6 Web Authentication

This table lists the features in this module and provides links to specific configuration information:

Feature	Release	Modification
IPv6 Web Authentication Functionality	Cisco IOS XE 3.2SE	This feature was introduced.