Central Web Authentication

Information About Central Web Authentication

Central web authentication offers the possibility to have a central device that acts as a web portal (in this example, the ISE). The major difference compared to the usual local web authentication is that it is shifted to Layer 2 along with MAC filtering or dot1x authentication. The concept also differs in that the radius server (ISE in this example) returns special attributes that indicate to the switch that a web redirection must occur. This solution eliminates any delay to start the web authentication.

The following are the different types of web authentication methods:

- Local Web Authentication (LWA): Configured as Layer 3 security on the controller, the web authentication page and the pre-authentication ACL are locally configured on the controller. The controller intercepts htttp(s) traffic and redirects the client to the internal web page for authentication. The credentials entered by the client on the login page is authenticated by the controller locally or through a RADIUS or LDAP server.
- External Web Authentication (EWA): Configured as Layer 3 security on the controller, the controller intercepts htttp(s) traffic and redirects the client to the login page hosted on the external web server. The credentials entered by the client on the login page is authenticated by the controller locally or through a RADIUS or LDAP server. The pre-authentication ACL is configured statically on the controller.
- Central Web Authentication (CWA): Configured mostly as Layer 2 security on the controller, the redirection URL and the pre-authentication ACL reside on ISE and are pushed during layer 2 authentication to the controller. The controller redirects all web traffic from the client to the ISE login page. ISE validates the credentials entered by the client through HTTPS and authenticates the user.

Globally, if the MAC address of the client station is not known by the radius server (but other criteria can also be used), the server returns the redirection attributes, and the controller authorizes the station (using the MAC filtering) but places an access list to redirect the web traffic to the portal.

Once the user logs into the guest portal, it is possible to re-authenticate the client so that a new Layer 2 MAC filtering occurs using the Change of Authorization (CoA). This way, the ISE remembers that it was a webauth user and pushes the necessary authorization attributes to the controller for accessing the network.

Note

- In Central Web Authentication (CWA) with dual VLAN posture scenario, Cisco AireOS and IOS-XE controller performs 2 and 3 EAPOL handshakes respectively. If a client is stuck in a quarantine VLAN because of any break in EAPOL handshake due to client or network issue, you need to analyze the client or network issue.
- However, you can manually disconnect or reconnect the client to come out of the quarantine loop (or) click the Scan Again on AnyConnect (Or) enable posture lease (Or) use the ISE posture sync feature.
- If the controller has no switch virtual interface (SVI) in the client subnet or VLAN, the controller has to use any of the other SVIs and send traffic as defined in the routing table. This means that the traffic is sent to another gateway in the core of the network; this traffic then reaches the client subnet. Firewalls typically block traffic from and to the same switch, as seen in this scenario, so redirection might not work properly. Workarounds are to allow this behavior on the firewall.

Prerequisites for Central Web Authentication

- Cisco Identity Services Engine (ISE)

How to Configure ISE

To configure ISE, proceed as follows:

1. Create an authorization profile.
2. Create an authentication rule.
3. Create an authorization rule.

Creating an Authorization Profile

Procedure

Step 1	Click **Policy**, and click **Policy Elements**.
Step 2	Click **Results**.
Step 3	Expand **Authorization**, and click **Authorization Profiles**.
Step 4	Click **Add** to create a new authorization profile for central webauth.
Step 5	In the **Name** field, enter a name for the profile. For example, CentralWebauth.
Step 6	Choose **ACCESS_ACCEPT** from the Access Type drop-down list.
Step 7	Check the **Web Redirection (CWA, MDM, NSP, CPP)** check box, and choose **Centralized Web Auth** from the drop-down list.
Step 8	In the **ACL** field, enter the name of the ACL that defines the traffic to be redirected. For example, redirect.
Step 9	In the **Value** field, choose the default or customized values.

The Value attribute defines whether the ISE sees the default or a custom web portal that the ISE admin created.

Step 10 Click **Save**.

Creating an Authentication Rule

Follow the procedure given below to use the authentication profile and create the authentication rule:

Procedure

Step 1 In the **Policy** > **Authentication** page, click **Authentication**.
Step 2 Enter a name for your authentication rule. For example, MAB.
Step 3 In the If condition field, select the plus (+) icon.
Step 4 Choose **Compound condition**, and choose **Wireless_MAB**.
Step 5 Click the arrow located next to **and ...** in order to expand the rule further.
Step 6 Click the + icon in the Identity Source field, and choose **Internal endpoints**.
Step 7 Choose **Continue** from the 'If user not found' drop-down list.

This option allows a device to be authenticated even if its MAC address is not known.

Step 8 Click **Save**.

Creating an Authorization Rule

You can configure many rules in the authorization policy. The *MAC not known* rule is configured in this section:

Procedure

Step 1 Click **Policy** > **Authorization**.
Step 2 In the Rule Name field, enter a name. For example: *Mac not known*.
Step 3 In the Conditions field, click the plus (+) icon.
Step 4 Choose **Compound Conditions**, and choose **Wireless_MAB**.
Step 5 From the settings icon, select **Add Attribute/Value** from the options.
Step 6 In the Description field, choose **Network Access** > **AuthenticationStatus** as the attribute from the drop-down list.
Step 7 Choose the **Equals** operator.
Step 8 From the right-hand field, choose **UnknownUser**.
Step 9 In the Permissions field, choose the authorization profile name that you had created earlier.

The ISE continues even though the user (or MAC) is not known.

Unknown users are now presented with the Login page. However, once they enter their credentials, they are presented again with an authentication request on the ISE; therefore, another rule must be configured with a condition that is met if the user is a guest user. For example, if UseridentityGroup Equals Guest is used then it is assumed that all guests belong to this group.

Step 10 In the Conditions field, click the plus (+) icon.

Step 11 Choose **Compound Conditions**, and choose to create a new condition.

The new rule must come before the *MAC not known* rule.

Step 12 From the settings icon, select **Add Attribute/Value** from the options.

Step 13 In the Description field, choose **Network Access** > **UseCase** as the attribute from the drop-down list.

Step 14 Choose the **Equals** operator.

Step 15 From the right-hand field, choose **GuestFlow**.

Step 16 In the Permissions field, click the plus (+) icon to select a result for your rule.

You can choose **Standard** > **PermitAccess** option or create a custom profile to return the attributes that you like.

When the user is authorized on the login page, the ISE triggers a COA that results in the restart of Layer 2 authentication. When the user is identified as a guest user, the user is authorized.

How to Configure Central Web Authentication on the Controller

To configure central web authentication on the controller, proceed as follows:

1. Configure WLAN.
2. Configure policy profile.
3. Configure redirect ACL.
4. Configure AAA for central web authentication.
5. Configure redirect ACL in Flex profile.

Configuring WLAN (GUI)

Before you begin

You need to enable MAC filtering for Layer 2 authentication to download the redirect URL and ACL.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 In the **WLANs** window, click the name of the **WLAN** or click **Add** to create a new one.

Step 3 In the **Add/Edit WLAN** window that is displayed, click the **General** tab to configure the following parameters.

- In the **Profile Name** field, enter or edit the name of the profile.
- In the **SSID** field, enter or edit the SSID name.

  The SSID name can be alphanumeric, and up to 32 characters in length.
- In the **WLAN ID** field, enter or edit the ID number. The valid range is between 1 and 512.
- From the **Radio Policy** drop-down list, choose the **802.11** radio band.
- Using the **Broadcast SSID** toggle button, change the status to either **Enabled** or **Disabled** .
- Using the **Status** toggle button, change the status to either **Enabled** or **Disabled** .

Step 4 Click the **Security** tab, and then **Layer 2** tab to configure the following parameters:

- From the **Layer 2 Security Mode** drop-down list, choose **None**. .This setting disables Layer 2 security.
- Enter the **Reassociation Timeout** value, in seconds. This is the time after which a fast transition reassociation times out.
- Check the **Over the DS** check box to enable Fast Transition over a distributed system.
- Choose OWE, Opportunistic Wireless Encryption (OWE) provides data confidentiality with encryption over the air between an AP radio and a wireless client. OWE Transition Mode is meant to provide a sort of backwards compatibility.
- Choose Fast Transition, 802.11r which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with a new AP is done even before the corresponding client roams to the target access point. This concept is called Fast Transition.
- Check the check box to enable MAC filtering in the WLAN.

Step 5 Click **Save & Apply to Device**.

Configuring WLAN (CLI)

Configure WLAN using commands.

Note You need to enable MAC filtering for Layer 2 authentication to download the redirect URL and ACL.

After completing the WLAN configuration, if the changes are not pushed to all the APs, the following syslog message appears:

2021/01/06 16:20:00.597927186 {wncd_x_R0-4}{1}: [wlanmgr-db] [20583]: UUID: 0, ra: 0, TID: 0 (note): Unable to push WLAN config changes to all APs, cleanup required for WlanId: 2, profile: wlan1 state: Delete pending

If the above mentioned syslog message appears for more than six minutes, reload the controller.

If the controller does not reload and still the syslog message appears, then collect the archive logs, wncd core file, and raise a case by clicking the following link: Support Case Manager.

Procedure

	Command or Action	Purpose
Step 1	**wlan `wlan-name wlan-id SSID-name`** **Example:** `Device(config)# wlan wlanProfileName 1 ngwcSSID`	Enters the WLAN configuration sub-mode. **wlan-name** is the name of the configured WLAN. **wlan-id** is the wireless LAN identifier. The range is 1 to 512. **SSID-name** is the SSID name which can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter **`wlan wlan-name`** command.
Step 2	**mac-filtering** [*name*] **Example:** `Device(config-wlan)# mac-filtering name`	Enables MAC filtering on a WLAN. **Note** While configuring mac-filtering the default authentication list is considered, if the authentication list is not configured earlier.
Step 3	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disable WPA security.
Step 4	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 5	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode.

Example

```
Device# config terminal
Device(config)# wlan wlanProfileName 1 ngwcSSID
Device(config-wlan)# mac-filtering default
Device(config-wlan)# no security wpa
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

Configuring Policy Profile (CLI)

Configure Policy Profile using commands.

Note You need a AAA override to apply policies coming from the AAA or ISE servers. When a redirect URL and redirect ACL is received from the ISE server, NAC is used to trigger the Central Web Authentication (CWA).

Both NAC and AAA override must be available in the policy profile to which the client is being associated.

The default policy profile is associated to an AP, if the AP is not associated to any other policy profiles.

Procedure

	Command or Action	Purpose
Step 1	**wireless profile policy default-policy-profile** **Example:** `Device(config)# wireless profile policy default-policy-profile`	Sets the policy profile.
Step 2	**vlan `vlan-id`** **Example:** `Device(config-wireless-policy)# vlan 41`	Maps the VLAN to a policy profile. If vlan-id is not specified, the default native vlan 1 is applied. The valid range for vlan-id is 1 to 4096. Management VLAN is applied if no VLAN is configured on the policy profile.
Step 3	**aaa-override** **Example:** `Device(config-wireless-policy)# aaa-override`	Configures AAA override to apply policies coming from the AAA or ISE servers.
Step 4	**nac** **Example:** `Device(config-wireless-policy)# nac`	Configures Network Access Control in the policy profile. NAC is used to trigger the Central Web Authentication (CWA).
Step 5	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the WLAN.
Step 6	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode.

Example

```
Device# configure terminal
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# vlan 41
Device(config-wireless-policy)# aaa-override
Device(config-wireless-policy)# nac
```

```
Device(config-wireless-policy)# no shutdown
Device(config-wireless-policy)# end
```

Configuring a Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy Profile** page, click **Add**.

Step 3 In the **Add Policy Profile** window, in General Tab, enter a name and description for the policy profile.

Step 4 To enable the policy profile, set **Status** as Enabled.

Step 5 Use the slider to enable or disable **Passive Client** and **Encrypted Traffic Analytics**.

Step 6 (Optional) In the **CTS Policy** section, choose the appropriate status for the following:

- Inline Tagging—a transport mechanism using which a controller embedded wireless controller or access point understands the source SGT.
- SGACL Enforcement

Step 7 Specify a default **SGT**. The valid range is from 2 to 65519.

Step 8 In the WLAN Switching Policy section, choose the following, as required:

- Central Switching
- Central Authentication
- Central DHCP
- Central Association Enable
- Flex NAT/PAT

Step 9 Click **Save & Apply to Device**.

Creating Redirect ACL

The redirect ACL is a punt ACL that needs to be predefined on the controller (or the AP in case of FlexConnect local switching): the AAA server returns the name of the ACL and not its definition. The redirect ACL defines traffic (matching “deny”statements, as it denies redirection for it) that will be allowed through on the data plane and traffic (matching “permit” statements) that will be sent to the control plane towards the CPU for further processing (that is, the web interception and redirection in this case). The ACL has implicit (that is, the invisible) statements allowing DHCP and DNS traffic towards all IPs, just like it is the case with LWA. It also ends with a statement that a security ACL implicit deny.

Procedure

	Command or Action	Purpose
Step 1	**ip access-list extended redirect** **Example:** `Device(config)# ip access-list extended redirect`	The HTTP and HTTPS browsing does not work without authentication (per the other ACL) as ISE is configured to use a redirect ACL (named **redirect**).
Step 2	**deny ip any host ISE-IP-add** **Example:** `Device(config)# deny ip any host 123.123.134.112`	Allows traffic to ISE and all other traffic is blocked.
Step 3	**deny ip host ISE-IP-add any** **Example:** `Device(config)# deny ip host 123.123.134.112 any`	Allows traffic to ISE and all other traffic is blocked. **Note** This ACL is applicable for both local and flex mode.

Step 4	**permit TCP any any eq web address/port-number**
	Example:
	In case of HTTP:
	`Device(config)# permit TCP any any eq www`
	`Device(config)# permit TCP any any eq 80`
	Example:
	In case of HTTPS:
	`Device(config)# permit TCP any any eq 443`
		Redirects all HTTP or HTTPS access to the ISE login page. port-number 80 is used for HTTP and port-number 443 is used for HTTPS.
		For the ACE to allow traffic to ISE, ISE should be configured above the HTTP/HTTPS ACE.

Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring AAA for Central Web Authentication

Procedure

	Command or Action	Purpose
Step 1	**aaa server radius dynamic-author** **Example:** `Device(config)# aaa server radius dynamic-author`	Configures the Change of Authorization (CoA) on the controller.

	Command or Action	Purpose
Step 2	**client ISE-IP-add server-key radius-shared-secret** **Example:** `Device(config-locsvr-da-radius)# client 123.123.134.112 server-key 0 SECRET`	Specifies a RADIUS client and the RADIUS key to be shared between a device and a RADIUS client. **ISE-IP-add** is the IP address of the RADIUS client. **server-key** is the radius client server-key. **radius-shared-secret** covers the following: • **0**—Specifies unencrypted key. • **6**—Specifies encrypted key. • **7**—Specifies HIDDEN key. • **Word**—Unencrypted (cleartext) server key. The RADIUS shared secret should not exceed 240 characters while configuring WSMA data in GUI. **Note** All these steps work only if the AAA configuration is in place. See the *Configuring AAA Authentication* for details.

Example

```
Device# config terminal
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 123.123.134.112 server-key 0 SECRET
Device(config-locsvr-da-radius)# end
```

Configuring Redirect ACL in Flex Profile (GUI)

The redirect ACL definition must be sent to the access point in the FlexConnect profile. For this, the redirect ACL associated with an AP must be configured in the FlexConnect profile where the client is hosted. If an access point is not configured with any of the FlexConnect profiles, the default FlexConnect profile is associated with it.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex**.

Step 2 On the **Flex Profile** page, click the name of the FlexConnect profile or click **Add** to create a new FlexConnect profile.

Step 3 In the **Add/Edit Flex Profile** window that is displayed, click the **Policy ACL** tab.

Step 4 Click **Add** to map an ACL to the FlexConnect profile.

Step 5 Choose the ACL name, enable central web authentication, and specify the preauthentication URL filter.

Step 6 Click **Save**.

Step 7 Click **Update & Apply to Device**.

Configuring Redirect ACL in Flex Profile (CLI)

The redirect ACL definition must be sent to the access point in the Flex profile. For this, the redirect ACL associated to an AP must be configured in the Flex profile where the client is being hosted. If an access point is not configured with any of the Flex profiles, the default Flex profile is associated with it.

Procedure

	Command or Action	Purpose
Step 1	**wireless profile flex default-flex-profile** **Example:** `Device(config)# wireless profile flex default-flex-profile`	Creates a new flex policy. The default flex profile name is **`default-flex-profile`**.
Step 2	**acl-policy** *acl policy name* **Example:** `Device(config-wireless-flex-profile)# acl-policy acl1`	Configures ACL policy.
Step 3	**central-webauth** **Example:** `Device(config-wireless-flex-profile-acl)# central-webauth`	Configures central web authentication.
Step 4	**end** **Example:** `Device(config-wireless-flex-profile-acl)# end`	Returns to privileged EXEC mode.

Troubleshooting Central Web Authentication

Init-State timer running out

Problem Issue: The client devices are deauthenticated by the controller if users fail to enter their credentials in a limited time interval. The clients are deauthenticated after three times the time configured for the init-state timeout in the controller.

Problem Explanation: This is the expected functionality as the init-state timeout is not directly applicable for central web authentication; instead, it is the reap timer's value which is three times the init-state time plus five seconds (3*init-state timeout + 5) that determines the time interval in seconds for client deauthentication. For example, if you have configured the init-state timeout as 10 seconds, then the client devices are deuathenticated if users fail to enter their credentials after 35 seconds; that is (3*10 + 5) = 35 seconds.

Authentication for Sleeping Clients

Information About Authenticating Sleeping Clients

Clients with guest access that have had successful web authentication are allowed to sleep and wake up without having to go through another authentication process through the login page. You can configure the duration for which sleeping clients should be remembered for before reauthentication becomes necessary. The valid range is 10 minutes to 43200 minutes, with the default being 720 minutes. You can also configure this duration on WebAuth parameter map that is mapped to a WLAN. Note that the sleeping client timer comes into effect due to instances such as idle timeout, session timeout, disabling of the WLAN, and the AP being nonoperational.

This feature is supported in the following FlexConnect scenario: local switching and central authentication.

Caution If the MAC address of a client that goes to sleep mode is spoofed, the fake device such as a laptop can be authenticated.

Mobility Scenarios

Following are some guidelines in a mobility scenario:

- L2 roaming in the same subnet is supported.
- Anchor sleeping timer is applicable.
- The sleeping client information is shared between multiple autoanchors when a sleeping client moves from one anchor to another.

A sleeping client does not require reauthentication in the following scenarios:

- Suppose there are two controller s in a mobility group. A client that is associated with one controller goes to sleep and then wakes up and gets associated with the other controller .
- Suppose there are three controller s in a mobility group. A client that is associated with the second controller that is anchored to the first controller goes to sleep, wakes up, and gets associated with the third controller .
- A client sleeps, wakes up and gets associated with the same or different export foreign controller that is anchored to the export anchor.

Restrictions on Authenticating Sleeping Clients

- The sleep client feature works only for WLAN configured with WebAuth security.
- You can configure the sleeping clients only on a per WebAuth parameter-map basis.
- The authentication of sleeping clients feature is supported only on WLANs that have Layer 3 security enabled.
- With Layer 3 security, the Authentication, Passthrough, and On MAC Filter failure web policies are supported. The Conditional Web Redirect and Splash Page Web Redirect web policies are not supported.

- The central web authentication of sleeping clients is not supported.
- The authentication of sleeping clients feature is not supported on guest LANs and remote LANs.
- A guest access sleeping client that has a local user policy is not supported. In this case, the WLAN-specific timer is applied.

Configuring Authentication for Sleeping Clients (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Web Auth**.

Step 2 In the **Webauth Parameter Map** tab, click the parameter map name. The **Edit WebAuth Parameter** window is displayed.

Step 3 Select **Sleeping Client Status** check box.

Step 4 Click **Update & Apply to Device**.

Configuring Authentication for Sleeping Clients (CLI)

Procedure

	Command or Action	Purpose
Step 1	**[no] parameter-map type webauth** {*parameter-map-name* | **global**} **Example:** `Device(config)# parameter-map type webauth global`	Creates a parameter map and enters parameter-map webauth configuration mode.
Step 2	**sleeping-client** [**timeout** *time*] **Example:** `Device(config-params-parameter-map)# sleeping-client timeout 100`	Configures the sleeping client timeout to 100 minutes. Valid range is between 10 minutes and 43200 minutes. **Note** If you do not use the timeout keyword, the sleeping client is configured with the default timeout value of 720 minutes.
Step 3	**end**	Exits parameter-map webauth configuration mode and returns to privileged EXEC mode.
Step 4	(Optional) **show wireless client sleeping-client** **Example:** `Device# show wireless client sleeping-client`	Shows the MAC address of the clients and the time remaining in their respective sessions.

	Command or Action	Purpose
Step 5	(Optional) **clear wireless client sleeping-client** [**mac-address** *mac-addr*] **Example:** `Device# clear wireless client sleeping-client mac-address 00e1.e1e1.0001`	• **clear wireless client sleeping-client**—Deletes all sleeping client entries from the sleeping client cache. • **clear wireless client sleeping-client mac-address** *mac-addr*—Deletes the specific MAC entry from the sleeping client cache.