



Central Web Authentication

- [Central web authentication, on page 1](#)
- [How to configure ISE, on page 3](#)
- [How to configure central web authentication on the controller, on page 5](#)

Central web authentication

A central web authentication is a wireless security mechanism that

- delegates the user login webpage and credential processing to a centralized authentication server such as Cisco ISE
- initiates user redirection and authentication at Layer 2, often in combination with MAC filtering or 802.1X authentication, and
- uses RADIUS server attributes so that network controllers redirect web traffic to the authentication portal. This approach streamlines access and reduces delays.
- **ISE (Identity Services Engine)**: Cisco's centralized network access policy platform that delivers authentication, authorization, accounting, and guest access functionality.
- **ACL (Access control list)**: A set of rules used to control network traffic and enforce security policies, determining which clients can access which network resources.
- **Change of Authorization (CoA)**: A mechanism to reapply or update authorization parameters dynamically without requiring a new login.



Note Currently, Cisco Identity Services Engine (ISE) supports only one Attribute-Value Pair (AVP) for Access Control Lists (ACLs), either IPv4 or IPv6. This limitation prevents the simultaneous return of both ACLs within the same authentication profile. As a result, dual-stack clients (devices using both IPv4 and IPv6) can operate within a Central Web Authentication (CWA) flow, but only under specific configurations. To avoid issues, it is recommended to configure a default IPv6 ACL with a 'deny all' rule. This ensures that clients do not encounter connectivity problems while the limitation is addressed through a future feature enhancement

Prerequisite

Cisco ISE

Comparison with other authentication methods

Central web authentication (CWA) lets you manage web-based access for wireless clients through a dedicated authentication portal (typically Cisco ISE). Unlike traditional local web authentication, CWA performs core security and redirection at Layer 2, working with authentication mechanisms such as MAC filtering or 802.1X. The RADIUS server sends specific attributes to the controller, which then redirects web traffic for portal-based login. This approach helps streamline authentication, reduce delays, and improve policy enforcement.

There are multiple methods of web authentication used in wireless environments.

- **Local web authentication (LWA):** Local web authentication (LWA) is Layer 3 security configured on the controller. The authentication page and pre-authentication ACL are configured locally. The controller intercepts HTTP(S) traffic from the client and redirects the client to an internal authentication web page. The controller authenticates credentials locally or through RADIUS or LDAP.
- **External web authentication (EWA):** Also configured as Layer 3 security on the controller. The controller intercepts HTTP(S) traffic and redirects the client to a login page hosted on an external web server. Credentials are authenticated by the controller locally or through a RADIUS or LDAP server. The pre-authentication ACL is statically configured on the controller.
- **Central web authentication (CWA):** Typically configured as Layer 2 security, with the redirection URL and pre-authentication ACL residing on Cisco ISE. During Layer 2 authentication, Cisco ISE pushes the redirection attributes to the controller. The controller redirects all web traffic from the client to the Cisco ISE login page. Cisco ISE then validates the credentials entered by the client through HTTPS and authenticates the user.

This table compares different types of authentication methods used in wireless environments.

Table 1: Difference from other authentication types

Method	Layer	Portal	Credential processing	Key attributes
Local web authentication	Layer 3	Controller	Locally or through RADIUS or LDAP	Controller intercepts traffic
External web authentication	Layer 3	External server	Locally or through RADIUS or LDAP	Static ACLs and external portal
Central web authentication	Layer 2	Cisco ISE	Through Cisco ISE (HTTPS)	Cisco ISE

Analogy: concert tickets

Imagine a concert venue with several ways to check tickets and admit guests. You can have ticket booths at every entrance (local authentication), ticket checkers who send guests to a special desk outside (external authentication), or one main VIP booth at the heart of the venue that handles everyone's tickets and access (central authentication). Let's use this concert analogy to understand central web authentication and other methods.

At your concert venue, central web authentication (CWA) is what happens when, instead of letting every entrance or gate have their own ticket booth, you create one exclusive VIP booth—like Cisco ISE—that manages all ticketing for everyone. Instead of waiting until a guest actually tries to enter through a particular door (the way local booth might do), the venue’s security starts checking guests’ tickets as soon as they enter the red carpet. The VIP booth can give the gatekeepers special instructions: “If you don’t recognize someone’s ticket, redirect them straight to me!” This means the main ticketing process is handled efficiently and quickly by one central authority.

Let’s look at all the ticketing strategies you could use at your concert:

Local Ticket Booth (Local Web Authentication, LWA): Every entrance has its own mini ticket booth and rules. Guards at the door check tickets and can ask guests for their info. Ticket validation is handled locally at each gate, sometimes via a backstage manager or external system.

External Ticket Desk (External Web Authentication, EWA): Instead of ticket checks at the gate, guests are sent to a desk outside the stadium. The desk is run by another company. The security at the entrance gates redirects guests and the validation can still interact with the backstage manager if needed. Rules for who gets through are set upfront.

VIP Central Ticket Booth (Central Web Authentication, CWA): The gates just check basic details (like guest’s wristband color), and anyone who isn’t recognized is sent straight to the main VIP booth (Cisco ISE) to have their ticket or credentials checked and get access granted for the whole event.

How to configure ISE

To configure ISE, follow these tasks:

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

Create an authorization profile

Define an authorization profile for central web authentication with required redirect attributes.

Before you begin

Ensure you have the required access and know the ACL name for redirection.

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 web authentication. |
| 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.
This field defines whether the Cisco ISE displays the default or a custom web portal that the Cisco ISE admin created.
- Step 10** Click **Save**.

The authorization profile is created and is available for use in your central web authentication policies.

Create an authentication rule

Define an authentication rule to control network access based on specified conditions.

Use authentication rules to specify how users or devices are authenticated in your policy system. This rule determines which authentication methods and identity sources are applied when network access is requested.

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 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.
A device can be authenticated even if its MAC address is not known when you select this option.
- Step 8** Click **Save**.

Your new authentication rule is added to the authentication policy.

Create an authorization rule

Define and enforce policies to control access to network resources for users and devices.

Use authorization rules to allow or deny access based on user, device, or authentication attributes in Cisco ISE.

You can configure many rules in the authorization policy, such as the *MAC not known*.

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 name of the authorization profile you had created earlier.
- The Cisco ISE continues even though the user (or MAC) is not known.
- Unknown users now see the login page. When they enter their credentials, the Cisco ISE sends another authentication request. To support guest users, configure a rule to check if the user is in the guest group. For instance, if `UseridentityGroup Equals Guest` is used, all guests are included in this group.
- Step 10** In the **Conditions** field, click the plus (+) icon.
- Step 11** Choose **Compound Conditions**, and choose to create a new condition.
- Place the new rule so it is evaluated prior to 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 Cisco ISE triggers a Change of Authorization (COA). This process restarts Layer 2 authentication. If the user is identified as a guest, the user is authorized.

Cisco ISE evaluates user or device access requests against these rules and enforces the appropriate policy. Unknown users see the login page and, if identified as guests, receive guest access upon authentication.

How to configure central web authentication on the controller

To configure central web authentication on the controller, proceed with these tasks.

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.

Configure WLAN (GUI)

Set up a new WLAN on your wireless controller using the GUI.

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. The **Add/Edit WLAN** window is displayed.
- Step 3** In the **Add/Edit WLAN** window, click the **General** tab to configure these 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 is alphanumeric and can be up to 32 characters in length.
 - In the **WLAN ID** field, enter or edit the ID number. The valid range is between one and 512.
 - Select the **802.11** radio band from the **Radio Policy** drop-down list.
 - 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 select the **Layer 2** tab to configure these parameters:
- Select **None** from the **Layer 2 Security Mode** drop-down list. This setting disables Layer 2 security.
 - Enter the **Reassociation Timeout** value, in seconds. This value specifies the duration before 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 ensures backwards compatibility.
 - Choose Fast Transition (802.11r), the IEEE standard for fast roaming. This standard allows the initial handshake with a new AP to occur before the client roams to the target AP. This method is known as Fast Transition.
 - Check the check box to enable MAC filtering in the WLAN.
- Step 5** Click **Save & Apply to Device**.
-

Configure WLAN (CLI)

Set up a new WLAN on your wireless controller using the CLI.

Before you begin

Enable MAC filtering for Layer 2 authentication to download the redirect URL and ACL.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the WLAN.

Example:

```
Device(config)# wlan wlan-name wlan-id SSID-name
```

- **wlan-name** is the name of the configured WLAN.
- **wlan-id** is the WLAN identifier. The range is one to 512.
- **SSID-name** is the SSID name which can have up to 32 alphanumeric characters.

If you have already created and configured the WLAN, use the **wlan wlan-name** command.

Step 3 Enable MAC filtering on a WLAN.

Example:

```
Device(config-wlan)# mac-filtering name
```

If the authentication list is not already configured, the default authentication list is used when configuring MAC filtering.

Step 4 Disable WPA security.

Example:

```
Device(config-wlan)# no security wpa
```

Step 5 Enable the WLAN.

Example:

```
Device(config-wlan)# no shutdown
```

Step 6 Return to privileged EXEC mode.

Example:

```
Device(config-wlan)# end
```

The new WLAN is available and active on the controller.

After completing the WLAN configuration, if the changes are not pushed to all the APs, a 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 this syslog message appears for more than six minutes, reload the controller

If the controller does not reload and the syslog message continues to appear, collect the archive logs and wncd core file. Then, raise a case by clicking the link: [Support Case Manager](#).

```
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
```

Configure policy profile (CLI)

Define and activate a policy profile to control WLAN behavior using the CLI.

Use the CLI to set up policy profiles that govern AAA, NAC, and VLAN assignment for wireless clients on Cisco devices. Apply this procedure when building new WLAN policies or adjusting network admission controls.

Before you begin

- Both NAC and AAA override must be configured in the policy profile for proper CWA operation.
- 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).
- The default policy profile is used for APs not associated with a specific policy.
- Clients may experience VLAN assignment during the final RADIUS access-accept following successful authentication.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the WLAN.

Example:

```
Device(config)# wlan wlan-name wlan-id SSID-name
```

- **wlan-name** is the name of the configured WLAN.
- **wlan-id** is the WLAN identifier. The range is one to 512.
- **SSID-name** is the SSID name which can have up to 32 alphanumeric characters.

If you have already created and configured the WLAN, use the **wlan** *wlan-name* command.

Step 3 Set the policy profile.

Example:

```
Device(config)# wireless profile policy default-policy-profile
```

Step 4 Map the VLAN to a policy profile.

Example:

```
Device(config-wireless-policy)# vlan wlan-id
```

If *wlan-id* is not specified, the default native vlan one is applied. The valid range for *wlan-id* is one to 4096. Management VLAN is applied if no VLAN is configured on the policy profile.

Step 5 Configure AAA override to apply policies coming from the AAA or ISE servers.

Example:

```
Device(config-wireless-policy)# aaa-override
```

Step 6 Configure Network Access Control in the policy profile. NAC is used to trigger the Central Web Authentication (CWA).

Example:

```
Device(config-wireless-policy)# nac
```

Step 7 Enable the WLAN.

Example:

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

Step 8 Return to privileged EXEC mode.

Example:

```
Device(config-wlan)# end
```

The policy profile is configured and active, applying the desired AAA, NAC, and VLAN parameters to WLAN clients.

```
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
```

Configure a policy profile (GUI)

Create and apply a new policy profile using the GUI.

Use this task to define access and traffic management settings by configuring a policy profile in the system's 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 an embedded wireless controller, controller, or AP understands the source SGT.
 - SGACL Enforcement
- Step 7** Specify a default **SGT**. The valid range is from two to 65519.
- Step 8** In the **WLAN Switching Policy** section, choose as required:
- Central Switching
 - Central Authentication
 - Central DHCP
 - Central Association Enable
 - Flex NAT/PAT
- Step 9** Click **Save & Apply to Device**.
-

The new policy profile is created and applied to the device using your configured settings.

Create redirect ACL

Create a redirect access control list (ACL). Direct unauthenticated HTTP and HTTPS traffic to the Cisco Identity Service Engine login page. Allow traffic to Cisco ISE and block other traffic

The redirect ACL is a punt ACL that must be predefined on the controller. For FlexConnect local switching, the ACL must be predefined on the AP. The Authentication, authorization, and accounting (AAA) server returns only the name of the ACL, not its definition.

The redirect ACL defines traffic matching "deny" statements, allowing this traffic to pass through the data plane. Traffic matching "permit" statements is sent to the control plane for further processing, which includes web interception and redirection.

The redirect ACL includes implicit statements that allow DHCP and DNS traffic to all IP addresses, similar to LWA.

It also ends with an implicit deny statement in the security ACL.

Before you begin

Ensure you have the IP address of your Cisco ISE deployment.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create an extended access list.

Example:

```
Device(config)# ip access-list extended redirect
```

If users are not authenticated, HTTP and HTTPS browsing fails because Cisco ISE uses a redirect ACL (named **redirect**).

Step 3 Permit traffic to Cisco ISE and block all other traffic.

Example:

```
Device(config)# deny ip any host ISE-IP-address
```

Step 4 Permit traffic to Cisco ISE and all other traffic is blocked.

Example:

```
Device(config)# deny ip host ISE-IP-add any
```

Note

This ACL is applicable for both local and flex mode.

Step 5 Redirect 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, configured with the **permit TCP any any eq web address/port-number** command.

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
```

To allow traffic to Cisco ISE, configure Cisco ISE before the HTTP or HTTPS ACE entry.

Step 6 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

HTTP

```
Device# configure terminal
Device(config)# ip access-list extended redirect
Device(config)# deny ip any host 123.123.134.112
Device(config)# deny ip host 123.123.134.112 any
Device(config)# permit TCP any any eq www
Device(config)# permit TCP any any eq 80
Device(config)# end
```

HTTPS

```
Device# configure terminal
Device(config)# ip access-list extended redirect
Device(config)# deny ip any host 123.123.134.112
Device(config)# deny ip host 123.123.134.112 any
Device(config)# permit TCP any any eq 443
```

```
Device(config)# end
```

Configure AAA for CWA

Set up AAA to support Central Web Authentication using CLI.

Central Web Authentication requires proper AAA configuration to enable Change of Authorization (CoA) functions using a RADIUS (Remote Authentication Dial-In User Service) server.

Before you begin

Ensure AAA authentication is configured on your device. For more details, see the *Configuring AAA Authentication* documentation.

Procedure

Step 1 Configure the Change of Authorization (CoA) on the controller.

Example:

```
Device(config)# aaa server radius dynamic-author
```

Step 2 Specify a RADIUS client and configure the RADIUS key that is shared between the device and the RADIUS client.

Example:

```
Device(config-locsvr-da-radius)# client ISE-IP-add server-key
radius-shared-secret
```

ISE-IP-add is the IP address of the RADIUS client.

server-key is the radius client server-key.

radius-shared-secret can have these values:

- **0**—Specifies unencrypted key.
- **6**—Specifies encrypted key.
- **7**—Specifies HIDDEN key.
- **Word**—Unencrypted (cleartext) server key.

When configuring WSMA data in GUI, ensure that the RADIUS shared secret does not exceed 240 characters.

AAA is configured to support Central Web Authentication with dynamic CoA, enabling secure device communication with the RADIUS server.

```
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
```

Configure redirect ACL in flex profile (GUI)

Set up a redirect ACL within a flex profile so that APs enforce specified access control and web authentication policies.

The redirect ACL definition must be sent to the AP in the FlexConnect profile. The redirect ACL associated with an AP must be configured in the FlexConnect profile that hosts the client. If an AP is not configured with a FlexConnect profile, it is associated with the default FlexConnect profile.

Before you begin

- Identify the FlexConnect profile to be updated or verify if a new Flex profile needs to be created.
- Prepare the ACL details, central web authentication requirements, and any preauthentication URL filters.

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**.

The AP applies the configured redirect ACL parameters for client traffic as specified in the flex profile.

Configure redirect ACL in flex profile (CLI)

Set up a redirect ACL within a flex profile so that APs enforce specified access control and web authentication policies.

The redirect ACL definition must be sent to the AP in the FlexConnect profile. The redirect ACL associated with an AP must be configured in the FlexConnect profile that hosts the client. If an AP is not configured with a FlexConnect profile, it is associated with the default FlexConnect profile.



Note When the ACL is pushed down to the APs, the permission must change from **deny** to **permit** or the other way around. This change does not occur if the ACL contains an object group, causing the ACL not to be fully translated, which may cause the redirection to fail.

Before you begin

- Ensure you have the required ACL policy created on the controller.
- Confirm that AP is operating in FlexConnect mode.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create a new flex policy.

Example:

```
Device(config)# wireless profile flex default-flex-profile
```

The default flex profile name is **default-flex-profile**.

Step 3 Configure an ACL policy.

Example:

```
Device(config-wireless-flex-profile)# acl-policy
acl-policyname
```

Step 4 Configure central web authentication.

Example:

```
Device(config-wireless-flex-profile-acl)# central-webauth
```

Step 5 Return to privileged EXEC mode.

Example:

```
Device(config-wireless-flex-profile-acl)# end
```

The AP in flex profile has the redirect ACL configured. The ACL is now applied and used for client redirection during centralized web authentication.

Troubleshoot CWA

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 expected behavior. For central web authentication, the init-state timeout does not apply directly. The reap timer—three times the init-state timeout plus five seconds ($3 \times \text{init-state timeout} + 5$)—determines when your device deauthenticates in seconds.

Problem For example, if you have configured the init-state timeout as 10 seconds, then the client devices are deauthenticated if users fail to enter their credentials after 35 seconds; that is $(3 \times 10 + 5) = 35$ seconds.

Problem For example, if you set the init-state timeout to 10 seconds, your device deauthenticates after 35 seconds if you do not enter your credentials. (This calculation is: $3 \times 10 + 5 = 35$ seconds.)

