Configuring RADIUS NAC Support

- Information About RADIUS NAC Support, page 1
- Guidelines and Restrictions on RADIUS NAC Support, page 2
- Configuring RADIUS NAC Support (GUI), page 3
- Configuring RADIUS NAC Support (CLI), page 4

Information About RADIUS NAC Support

The Cisco Identity Services Engine (ISE) is a next-generation, context-based access control solution that provides the functions of Cisco Secure Access Control System (ACS) and Cisco Network Admission Control (NAC) in one integrated platform.

Cisco ISE was introduced in Cisco Wireless Release 7.0.116.0. Cisco ISE can be used to provide advanced security for your deployed network. It is an authentication server that you can configure on your controller. When a client associates with a Cisco WLC on a RADIUS NAC–enabled WLAN, the controller forwards the request to the Cisco ISE server.

The Cisco ISE server validates a user in the database, and on successful authentication, the URL and the pre-AUTH ACL are sent to the client. The client then moves to the Posture Required state and is redirected to the URL returned by the ISE server.

Note

The client moves to the Central Web Authentication state, if the URL returned by the Cisco ISE server has the keyword cwa.

The NAC agent in the client triggers the posture validation process. On successful posture validation by the Cisco ISE server, the client is moved to the Run state.

Note

FlexConnect local switching with RADIUS NAC support is added in Release 7.2.110.0. It is not supported in the 7.0 releases and Release 7.2.103.0. Downgrading from Release 7.2.110.0 or a later release to either Release 7.2.103.0 or a 7.0 release will require you to reconfigure the WLAN for the RADIUS NAC feature to work.
Device Registration

Device registration enables you to authenticate and provision new devices on the WLAN with RADIUS NAC enabled. When a device is registered on the WLAN, it can use the network based on the configured ACL.

Central Web Authentication

In the case of Central Web Authentication (CWA), web authentication occurs on the Cisco ISE server. The web portal in the Cisco ISE server provides a login page to a client. After the credentials are verified on the Cisco ISE server, the client is provisioned. The client remains in the POSTURE_REQD state until a change of authorization (CoA) is reached. The credentials and ACLs are received from the Cisco ISE server.

Local Web Authentication

Local web authentication is not supported for RADIUS NAC.

This table describes the possible combinations in a typical ISE deployment with Device Registration, CWA and LWA enabled:

<table>
<thead>
<tr>
<th>WLAN Configuration</th>
<th>CWA</th>
<th>LWA</th>
<th>Device Registration</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS NAC Enabled</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>L2 None</td>
<td>No</td>
<td>PSK, Static WEP, CKIP</td>
<td>No</td>
</tr>
<tr>
<td>L3 None</td>
<td>N/A</td>
<td>Internal/External</td>
<td>N/A</td>
</tr>
<tr>
<td>MAC Filtering Enabled</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Guidelines and Restrictions on RADIUS NAC Support

Guidelines

- When a client moves from one WLAN to another, the Cisco WLC retains the client’s audit session ID if it returns to the WLAN before the idle timeout occurs. As a result, when the client associates with the Cisco WLC before the idle timeout session expires, it is immediately moved to Run state. The client is validated if it reassociates with the Cisco WLC after the session timeout.
- If you have two WLANs, and WLAN 1 is configured on a Cisco WLC (WLC1) and WLAN2 is configured on another Cisco WLC (WLC2) and both are RADIUS NAC enabled, the client first connects to WLC1 and moves to the RUN state after posture validation. Assume that the client now moves to WLC2. If the client connects back to WLC1 before the PMK expires for this client in WLC1, the posture validation is skipped for the client. The client directly moves to Run state by passing posture validation because the Cisco WLC retains the old audit session ID for the client that is already known to Cisco ISE.
When deploying RADIUS NAC in your wireless network, do not configure a primary and secondary Cisco ISE server. Instead, we recommend that you configure High Availability (HA) between the two Cisco ISE servers. Having a primary and secondary ISE setup will require posture validation to occur before the clients move to the Run state. If HA is configured, the client is automatically moved to the Run state in the fallback Cisco ISE server.

Do not swap AAA server indexes in a live network because clients might get disconnected and have to reconnect to the RADIUS server, which might result in log messages to be appended to the ISE server logs.

Enable AAA override on the WLAN to use RADIUS NAC.

WPA and WPA2 or dot1X must be enabled on the WLAN. This is also required in case of PSK in Layer 2 security.

During slow roaming, clients go through posture validation.

If the AAA url-redirect-acl and url-redirect attributes are expected from the AAA server, the AAA override feature must be enabled on the controller.

Restrictions

- A RADIUS NAC-enabled WLAN supports only Open Authentication and MAC filtering.
- The RADIUS NAC functionality does not work if the configured accounting server is different from the authentication (Cisco ISE) server. You should configure the same server as the authentication and accounting server if Cisco ISE functionalities are used. If Cisco ISE is used only for Cisco ACS functionality, the accounting server can be flexible.
- The controller software configured with RADIUS NAC does not support a CoA on the service port.
- Guest tunneling mobility is supported only for ISE NAC–enabled WLANs.
- VLAN select is not supported.
- Workgroup bridges are not supported.
- The AP Group over NAC is not supported in RADIUS NAC.
- When RADIUS NAC is enabled, the RADIUS server overwrite interface is not supported.

Configuring RADIUS NAC Support (GUI)

**Step 1** Choose WLANs.

**Step 2** Click the WLAN ID.
The WLANs > Edit page appears.

**Step 3** Click the Advanced tab.

**Step 4** From the NAC State drop-down list, choose from the following options:

- None
- SNMP NAC—Uses SNMP NAC for the WLAN.
• **RADIUS NAC**—Uses RADIUS NAC for the WLAN.

**Note**  
AAA override is automatically enabled when you use RADIUS NAC on a WLAN.

---

**Step 5**  
Save the configuration.

---

**Configuring RADIUS NAC Support (CLI)**

Enter the following command:

```
config wlan nac radius {enable | disable} wlan_id
```