

Configuring the Infranet Controller as a RADIUS Server (NSM Procedure)

The Infranet Controller contains an internal RADIUS server that can be configured to perform Extensible Authentication Protocol (EAP) inner and outer authentication, non-tunneled Web authentication without EAP, and MAC address authentication.

To configure the Infranet Controller as a RADIUS server, the following configurations must be performed:

1. Configuring Authentication Protocol Sets on page 1
2. Using RADIUS Proxy on page 2

Configuring Authentication Protocol Sets

To configure an authentication protocol set:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to configure authentication protocol sets.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Signing In > Authentication Protocols**.



NOTE: The default 802.1X protocol set is configured to work with either EAP-TTLS or EAP-PEAP as the primary outer authentication protocol, and EAP-JUAC or EAP-MSCHAP- V2 for inner authentication (if EAP-PEAP is used) and EAP-JUAC, PAP, MSCHAP- V2, EAP-MS-CHAP-V2, or EAP-GenericTokenCard (if EAP-TTLS is used).

4. Add or modify settings on the authentication protocol sets as specified in Table 1 on page 1.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 1: Authentication Protocol Sets Configuration Details

Option	Function	Your Action
Authentication Protocol		
Name	Specifies a unique name for the authentication protocol.	Enter a name for the authentication protocol.
Description	Describes the authentication protocol.	Enter a brief description for the authentication protocol.
Authentication Protocol > Authentication Protocol		

Table 1: Authentication Protocol Sets Configuration Details (continued)

Option	Function	Your Action
New Authentication Protocol	Specifies the main authentication protocol.	Select the authentication protocol from the list. NOTE: If you are using inner RADIUS proxy, do not select an inner protocol with EAP-PEAP or EAP-TTLS. See “Using RADIUS Proxy.”
Authentication Protocol > PEAP		
New PEAP	Specifies the inner authentication protocol.	If you select EAP-PEAP as the main authentication protocol, under PEAP click Add and select an inner authentication protocol from the New PEAP list. NOTE: If you are configuring a protocol set to work with the Windows client and a Host Checker Statement of Health policy, you must choose the EAP-SOH protocol as the inner authentication method within a PEAP tunnel.
Authentication Protocol > TTLS		
New TTLS	Specifies the inner authentication protocol.	If you select EAP-TTLS as the main authentication protocol, under TTLS click Add and select an inner authentication protocol from the New TTLS list.

Using RADIUS Proxy

You can configure the Infranet Controller to proxy RADIUS inner or outer authentication to an external RADIUS server.

With RADIUS proxy, the Infranet Controller RADIUS server can forward authentication requests from a network access device to an external RADIUS server. The proxy target receives the request, performs the authentication, and returns the results. The Infranet Controller RADIUS server then passes the results to the network access device.



NOTE: When RADIUS proxy is used, realm or role restrictions cannot be enforced. Host Checker policies, source IP restrictions, and any other limits that have been assigned are bypassed. RADIUS proxy should be used only if no restrictions have been applied. The exception is that session limitations can be enforced for inner proxy. With outer proxy, no session is established.

You configure RADIUS proxy at the realm level. If the authentication server for the realm is a RADIUS server, option buttons on the page allow you to select inner proxy, outer proxy, or do not proxy. Do not proxy is selected by default. If the authentication server is not a RADIUS server, the proxy option buttons are hidden.

If the authentication server selected for a realm is a RADIUS server, the Proxy Outer Authentication option button controls whether outer authentication is proxied, and

the Proxy Inner Authentication option button controls whether inner authentication is proxied.

You can also choose the Do not proxy option button if you do not want inner or outer authentication to be proxied. In this case, the Infranet Controller handles both inner and outer authentication. You must enable the JUAC protocol for this option.

- Related Topics**
- [Configuring Role Mapping Rules \(NSM Procedure\)](#)
 - [Configuring RADIUS Clients \(NSM Procedure\)](#)
 - [Using the Infranet Controller for 802.1X Network Access \(NSM Procedure\)](#)

