



Mist Integration with ISE for EAP



Table of Contents

MIST AP CONFIGURATION	3
ISE CONFIGURATRION	6
DYNAMIC VLAN CONFIGURATION/SGT INTEGRATION	7



Mist AP Configuration

- 1) WLAN Configuration
 - a. Network -> WLAN -> Add WLANs

The screenshot shows the Mist AP configuration interface. On the left is a navigation sidebar with icons for MONITOR, CLIENTS, ACCESS POINTS, LOCATION, ANALYTICS, NETWORK, and ORGANIZATION. The main content area is divided into several sections:

- SSID:** A text input field containing "Test-Dot1x".
- Labels:** A text input field with a "+" icon.
- Security:** Radio button options for:
 - WPA-2/PSK with passphrase (disabled)
 - WPA-2/EAP (802.1X) (selected)
 - Open AccessA "Reveal" button is next to the WPA-2/PSK option. A "More Options" link is below.
- Fast Roaming:** Radio button options for:
 - Default (selected)
 - Opportunistic Key Caching (OKC)
- WLAN Status:** A section partially obscured by a menu.
- Drop inactive clients after:** A field with "1800" and "seconds".
- Geofence:** A section partially obscured by a menu.
- Packet Captures:** A section partially obscured by a menu.
- Radio Management:** A section partially obscured by a menu.
- Pre-shared Keys:** A section partially obscured by a menu.
- 54.175.176.99 : 1812:** A section partially obscured by a menu.
- Add a Server:** A button with the text "Add a Server".

A dark blue menu is overlaid on the screen, listing the following options:

- WLANs: Setup wireless networks and guest portal pages
- Labels: Define labels for users, APs, WLANs, etc
- Policy: Control access to network resources
- Security: View threats on your wireless network
- Tunnels: Configure tunnels for WLAN data
- Packet Captures: Create and download packet captures
- Radio Management: Setup and configure settings for RRM
- Pre-shared Keys: Create keys for users and groups



b. Create an WLAN with Security 802.1x

<p>SSID</p> <input type="text" value="Test-Dot1x"/>	<p>Security</p> <p><input type="radio"/> WPA-2/PSK with passphrase <input type="text" value=""/>Reveal</p> <p><input checked="" type="radio"/> WPA-2/EAP (802.1X)</p> <p><input type="radio"/> Open Access</p> <p>More Options</p> <p>Fast Roaming</p> <p><input checked="" type="radio"/> Default</p> <p><input type="radio"/> Opportunistic Key Caching (OKC)</p> <p><input type="radio"/> .11r</p>				
<p>Labels</p> <input type="text" value="+"/>					
<p>WLAN Status</p> <p><input checked="" type="radio"/> Enabled <input type="radio"/> Disabled</p> <p><input type="checkbox"/> Hide SSID</p> <p><input type="checkbox"/> No Static IP Devices</p> <p>Radio Band</p> <p><input type="radio"/> 2.4G and 5G <input type="radio"/> 2.4G <input checked="" type="radio"/> 5G</p> <p>Client Inactivity</p> <p>Drop inactive clients after <input type="text" value="1800"/> seconds</p>	<p>RadSec</p> <p><input type="radio"/> Enabled <input checked="" type="radio"/> Disabled</p> <p>RADIUS Authentication Servers</p> <table border="1"><tr><td>10.2.2.30 : 1812</td><td>primary</td></tr><tr><td>54.175.176.99 : 1812</td><td></td></tr></table> <p>Add a Server</p>	10.2.2.30 : 1812	primary	54.175.176.99 : 1812	
10.2.2.30 : 1812	primary				
54.175.176.99 : 1812					



- c. Add the Radius Server of Choice (RadSec is disabled when not used)
 - i. Click on the Radius server and it will provide an option to input the Radius Server details (IP, Port, Shared Secret) which would be the ISE server IP and port details
 - ii. You would also have the option of adding a secondary-server/tertiary servers
 - iii. You will also be edit the order of the preference for servers using the arrow keys place beside them.

A screenshot of a web-based configuration interface. A modal dialog box titled "RADIUS Authentication Server" is open, featuring a close button (X) in the top right corner. The dialog contains three input fields: "Hostname" with the value "10.2.2.30", "Port" with the value "1812", and "Shared Secret" with the value "xxxxxxxx". At the bottom of the dialog are three buttons: "Remove Server" (red), "OK" (blue), and "Cancel" (grey). The background shows a blurred interface with various settings and a list of items, including "Opportunistic Key Caching (OKC)".



ISE CONFIGURATION

- 1) Get the Radius Client IP, in our case the Mist Access Point IP
 - a. From the Access Point tab, select the access point of interest and get the IP of the AP under the Status tab

You could also use a subnet of AP IP addresses – if you would choose to do so in ISE

- 2) Under ISE -> Administration -> Network Devices -> Add Network Device

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is Administration > Network Resources > Network Devices > Add Network Device. The form is titled "New Network Device".

Key configuration fields and callouts:

- Name:** WLC-backbone (Callout: Mist AP Name)
- Description:** (Empty)
- IP Address:** 10.201.228.93 / 32 (Callout: AP IP address with /32 OR Subnet of AP IP with right Mask)
- Device Profile:** Cisco
- Model Name:** (Empty)
- Software Version:** (Empty)
- Network Device Group:** Device Type: All Device Types, Location: All Locations
- RADIUS Authentication Settings:** (Expanded)
 - Enable Authentication Settings:
 - Protocol: RADIUS
 - Shared Secret: [Redacted] (Callout: Under Radius Auth Settings – Input Radius Shared secret)
 - Enable KeyWrap:
 - Key Encryption Key: [Redacted]
 - Message Authenticator Code Key: [Redacted]
 - Key Input Format: ASCII (selected), HEXADECIMAL
 - CoA Port: 1700



Dynamic VLAN Configuration

VLAN

Untagged Tagged Pool Dynamic

Static VLAN ID

(1 - 4094)

VLAN Type

Dynamic VLAN ID	Interface Name(s)	
<input type="text" value="101"/>	<input type="text" value="Employee"/>	
<input type="text" value="102"/>	<input type="text" value="Contractor"/>	
<input type="text" value="103"/>	<input type="text" value="Guest"/>	
<input type="text"/>	<input type="text"/>	
<input type="text"/>	<input type="text"/>	

- Use DNAC/ISE to provision IP-SGT/VLAN-SGT bindings and push it down to the edge node/switches.
- ISE would push down dynamic VLANs based on the role of the client associating and Mist AP would place the clients on the respective VLANs
- Once the client traffic reaches the Edge node/Switch, the enforcement of the policy occurs here. The source IP/VLAN of the client corresponds to respective SGTs. Based on this the policy enforcement or SGACLs rule apply to this particular traffic – still leaving policy definition at a single point: ISE.