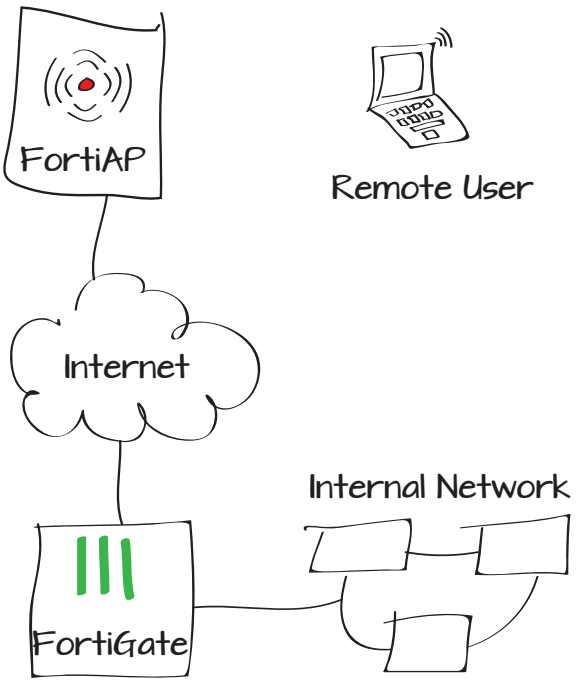
Providing remote users access to the corporate network and Internet

In this example, a user in a remote location, such as a hotel or their home, will use a FortiAP unit to securely connect to the corporate network and browse the Internet from behind the corporate firewall.

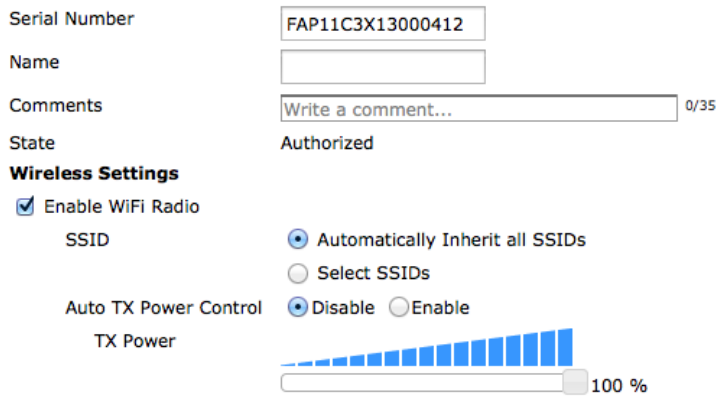
1. Preauthorizing the FortiAP unit on the FortiGate unit
2. Creating an SSID and firewall addresses
3. Creating security policies
4. Configuring the FortiAP unit to connect to the FortiGate unit
5. Connecting to the FortiGate unit remotely
6. Results



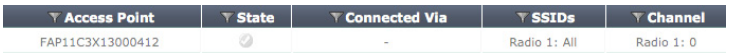
Pre-authorizing the FortiAP unit on the FortiGate unit

Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**.

Add a new FortiAP unit and enter the unit's **Serial Number** (in the example, *FAP11C3X13000412*).



The FortiAP unit will appear on the list of Managed FortiAPs as authorized and offline.'

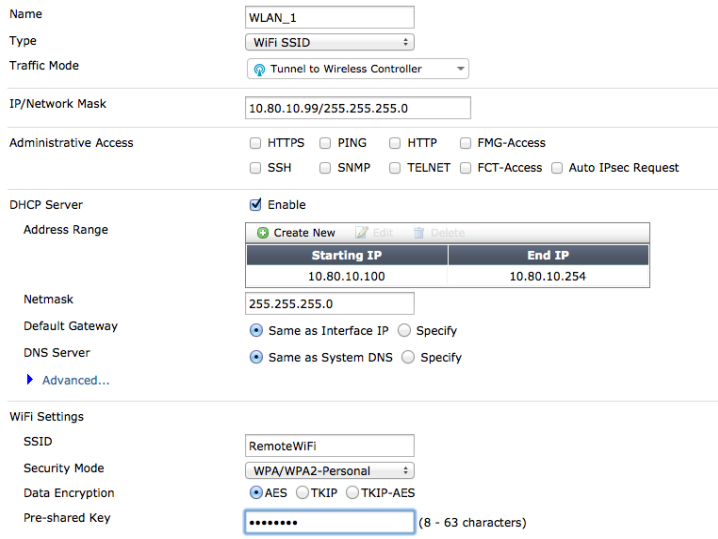


Creating an SSID and a firewall addresses

Go to **WiFi Controller > WiFi Network > SSID.** Select **Create New**.

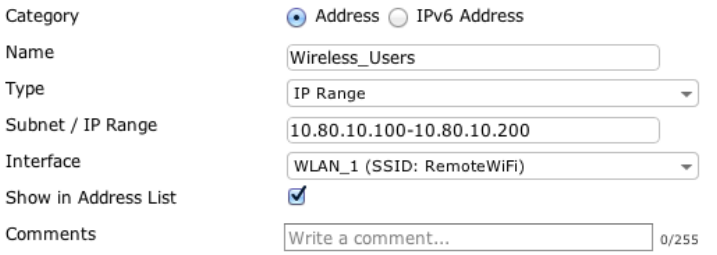
Enable the **DHCP Server** and make note of the IP range.

Configure the **WiFi Settings** with a unique **SSID** name and **Pre-shared Key**.

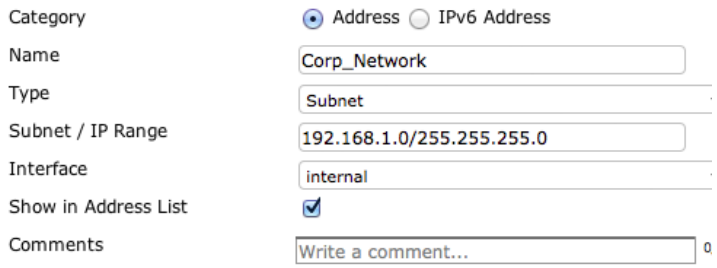


Go to **Firewall Objects > Address > Addresses.** Create addresses for both the remote users and the corporate network.

For the remote users, set **Type** to **IP Range**. The range for the remote users should be within the range used for the DHCP server. Set **Interface** to the new SSID.



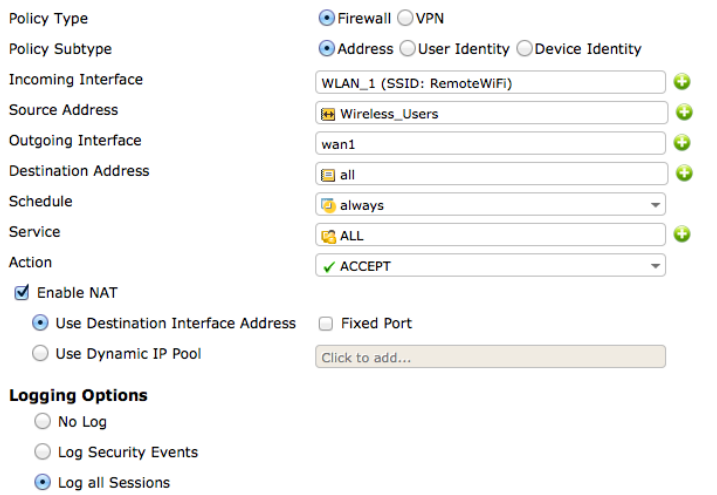
For the corporate network, set **Type** to **Subnet** and use the corporate network's IP address. Set **Interface** to an internal interface.



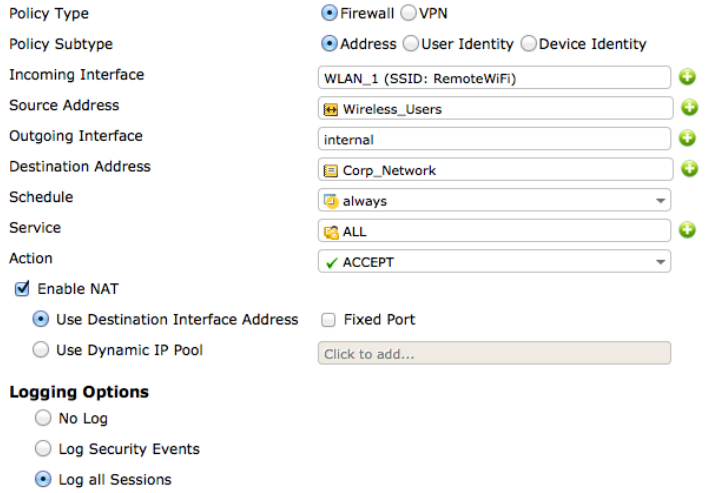
Creating security policies

Go to **Policy > Policy > Policy**.

Create a policy that allows remote wireless users to access the Internet. Set the **Incoming Interface** to the SSID and the **Outgoing Interface** as your Internet-facing interface.



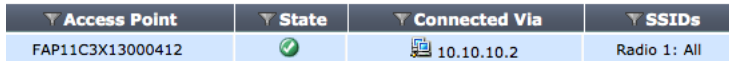
Create a second policy for remote wireless users to access the corporate network. Again, set the **Incoming Interface** to the SSID but now the **Outgoing Interface** is an internal interface.



Configuring the FortiAP unit to connect to the corporate FortiGate unit

Go to **WiFi Controller > Managed Access Points > Managed FortiAPs** and note the IP Address assigned to your FortiAP.

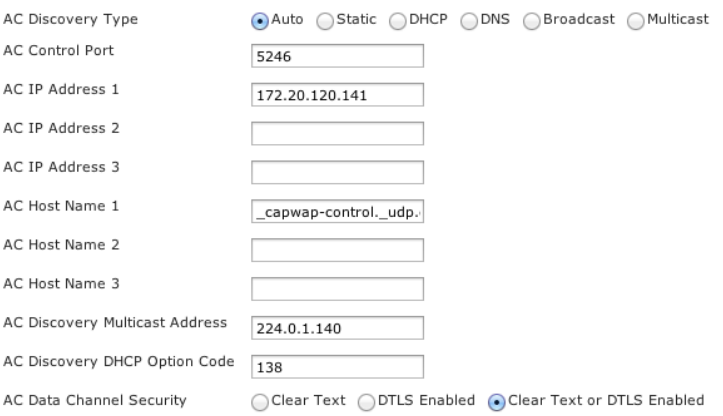
Enter the address into your browser's address bar to access your FortiAP web manager.



In the **System Information** tab, enter the **AC IP Address** of the public facing interface of the corporate FortiGate unit. The Internet-facing interface is also the public facing interface. To locate this IP address, go to **System > Network > Interfaces**.

The FortiAP will search for this FortiGate interface when it tries to connect.

The remote user may now take this device to the desired remote location to connect securely to the corporate FortiGate unit.



Connecting to the corporate FortiGate remotely

At the remote location, connect the FortiAP to the Internet using an Ethernet cable. Next, connect the FortiAP to power.

Once connected, the FortiAP requests an IP address and locates the FortiGate wireless controller.

The remote user can now access the corporate network and browse the Internet securely from behind the corporate firewall.

Results

Go to **WiFi Controller > Monitor > Client Monitor** to see remote wireless users connected to the FortiAP unit.

Go to **Log & Report > Traffic Log > Forward Traffic** to see remote wireless users appear in the logs.

Select an entry to view more information about remote traffic to the corporate network and to the Internet.