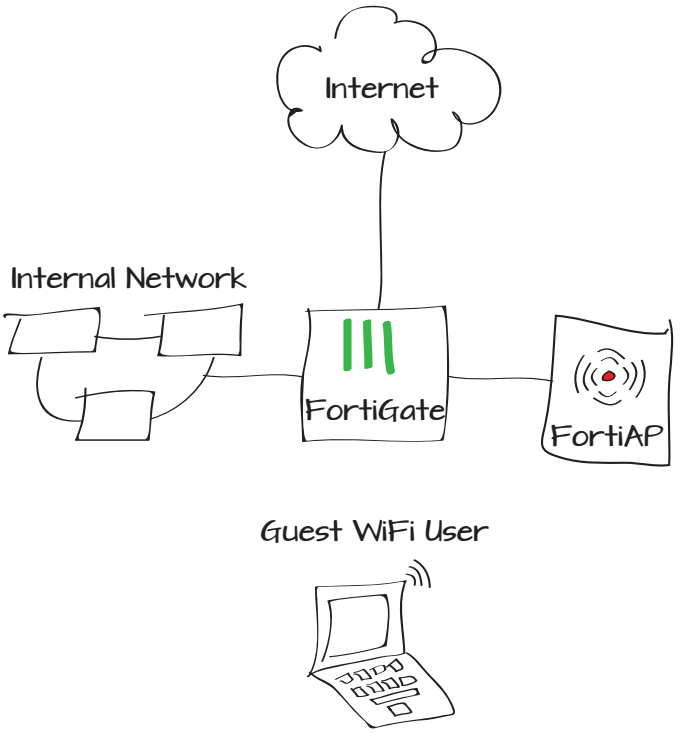
Setting up a temporary guest WiFi user

In this example, a temporary user account will be created and distributed to a guest user, allowing the guest to have wireless access to the Internet.

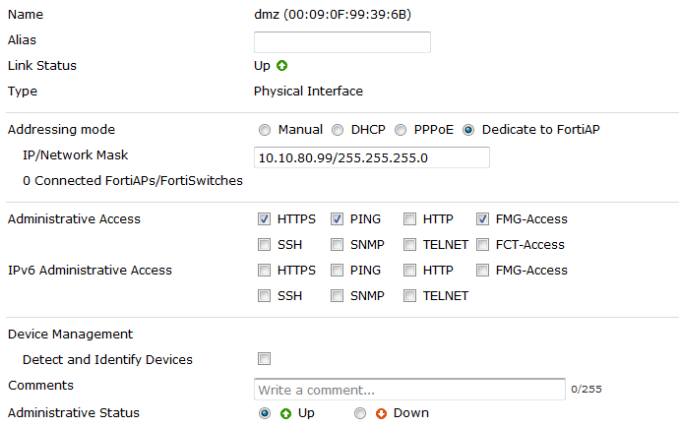
1. Connecting the FortiAP unit using the DMZ interface
2. Creating a WiFi guest user group
3. Creating an SSID using a captive portal
4. Creating a security policy to allow guest users Internet access
5. Creating a guest user management account
6. Results



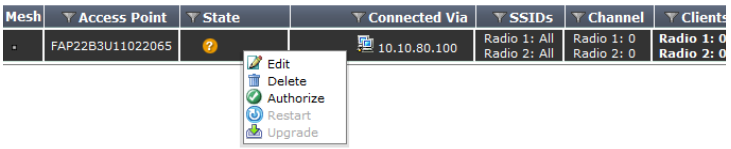
Connecting the FortiAP unit using the DMZ interface

Go to **System > Network > Interfaces**. Select the **dmz** interface.

Set the dmz interface to be **Dedicated to FortiAP**.



Connect the FortiAP to the DMZ interface. Go to **WiFi Controller > Managed Access Points > Managed FortiAPs** and right-click on the FortiAP unit. Select **Authorize**.



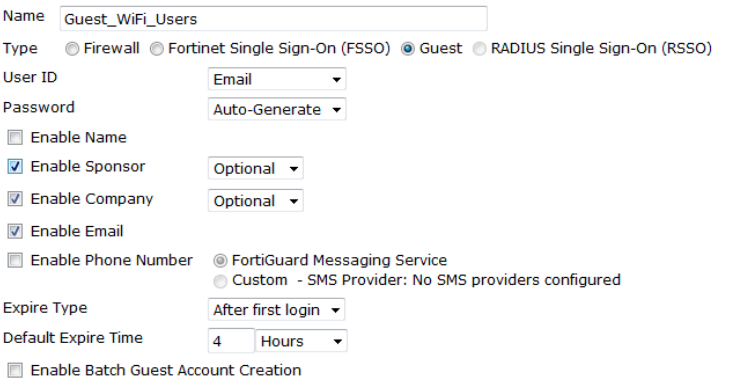
Using the DMZ interface creates a secure network that will only grant access if it is explicitly allowed. This allows guest access to be carefully controlled.

Creating a WiFi guest user group

Go to **User & Device > User > User Groups**.

Create a new group, setting **Type** to **Guest**, **User ID** to **Email**, and **Password** to **Auto-Generate**.

These guest user accounts are temporary and will expire four hours after the first login.



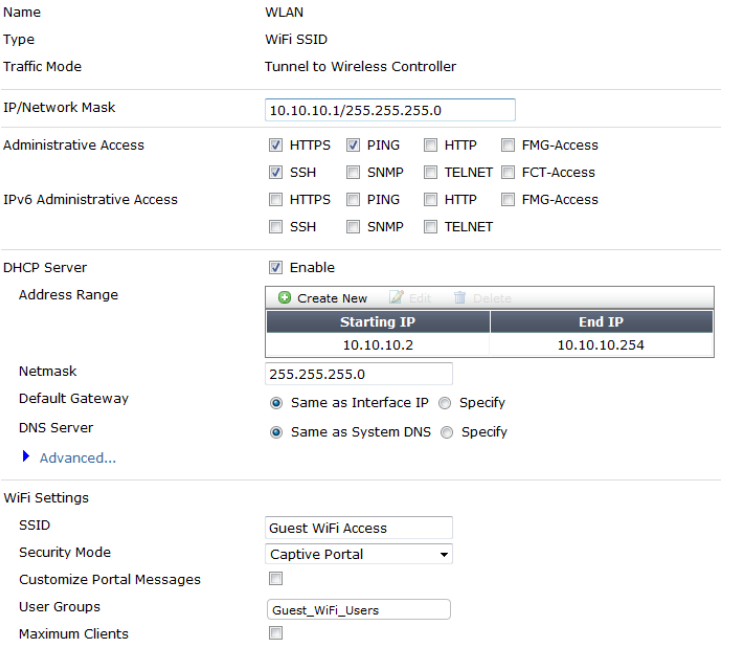
Creating an SSID using a captive portal

Go to **WiFi Controller > WiFi Network > SSID**.

Create a new SSID. Set **Traffic Mode** to **Tunnel to Wireless Controller** and enable **DHCP Server**, taking note of the IP range assigned.

Under **WiFi Settings**, set **Security Mode** to **Captive Portal** and **User Groups** to the new guest user group.

A Captive Portal will intercept connections to the wireless network and display a login screen on the guest user's device. The guest must then authenticate with the portal to gain access to the wireless network.



Creating a security policy to allow guest users Internet access

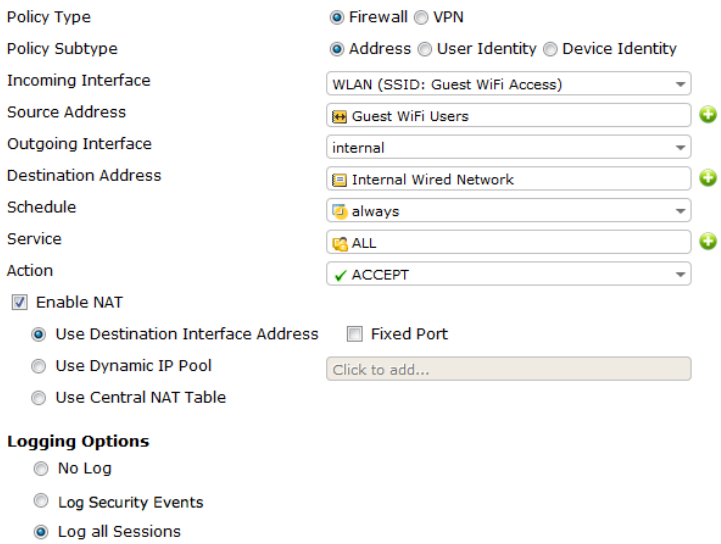
Go to **Firewall Objects > Address > Addresses.**

Create a firewall address for the guest WiFi users. Use the DHCP IP range for **Subnet/IP Range** and set the **Interface** to the wireless interface.

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

Create a security policy allowing guest users to have wireless access to the Internet.

Set **Incoming Interface** to the wireless interface, **Outgoing Interface** to your Internet-facing interface, and **Source Address** to the guest WiFi users group.

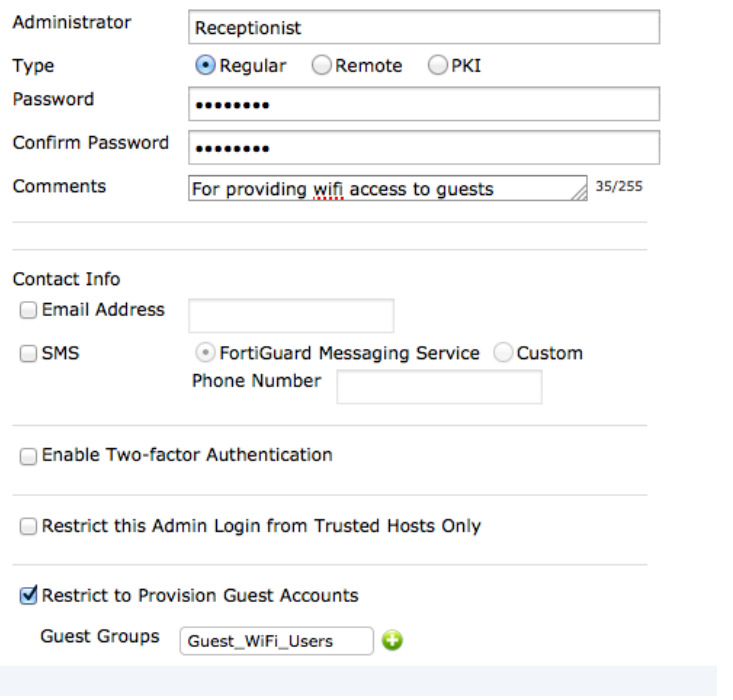


Creating a guest user management account

Optionally, you can create an administrator that is used only to create guest accounts. Access to this account can be given to a receptionist, to simply the process of making new accounts.

Go to **System > Admin > Administrators**.

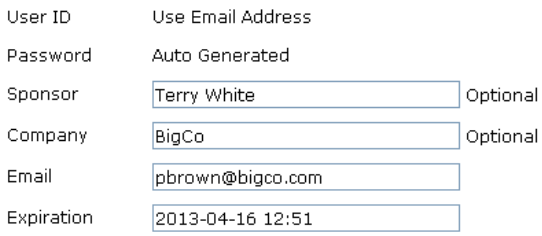
Create a new account. Set the **Type** to **Regular** and set a **Password**. Enable **Restrict to Provision Guest Accounts** and set **Guest Groups** to the WiFi guest user group.



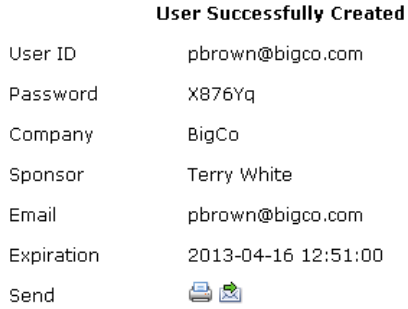
Results

Log in to the FortiGate unit using the guest user management account. Go to **User & Device > User > Guest Management** and select **Create New**.

Use a guest's email account to create a new user ID.



The FortiGate unit generates a user account and password. This account is only valid for four hours (the default time limit for the guest user group).



The guest can now log in using the FortiGate Captive Portal. Once authenticated, the guest is able to connect wirelessly to the Internet.

To verify that the guest user logged in successfully, go to **WiFi Controller > Monitor > Client Monitor**.

SSID	FortiAP	User	IP	
Guest WiFi Access	FAP22B3U11022065 (2)	pbrown@bigco.com	10.10.10.7	70:f1

Go to **Policy > Monitor > Policy Monitor** and verify the active sessions.

Policy ID	Source Interface/Zone	Destination Interface/Zone	Action	Active Sessions	Bytes	Packets
2	WLAN	wan1	✓	49	31.88 MB	50,434
1	internal	wan1	✓	9	2.97 MB	13,133
3	WLAN	internal	✓	1	219.71 KB	358

Select one of the bars to view more information about a session.