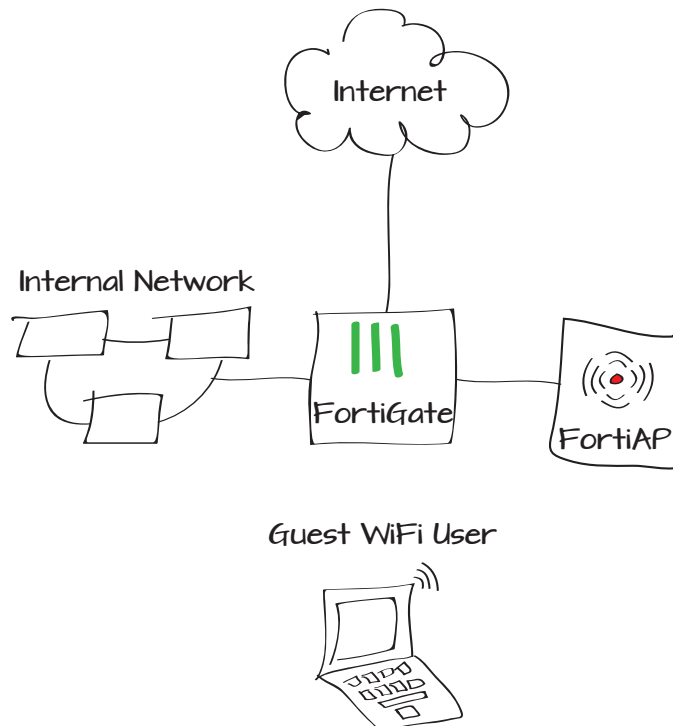


Setting up a temporary guest WiFi user

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.

Name	dmz (00:09:0F:99:39:6B)
Alias	<input type="text"/>
Link Status	Up
Type	Physical Interface
Addressing mode	<input type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input checked="" type="radio"/> Dedicate to FortiAP
IP/Network Mask	<input type="text" value="10.10.80.99/255.255.255.0"/>
0 Connected FortiAPs/FortiSwitches	
Administrative Access	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input type="checkbox"/> HTTP <input checked="" type="checkbox"/> FMG-Access <input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET <input type="checkbox"/> FCT-Access
IPv6 Administrative Access	<input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET
Device Management	
Detect and Identify Devices	<input type="checkbox"/>
Comments	<input type="text" value="Write a comment..."/> 0/255
Administrative Status	<input checked="" type="radio"/> Up <input type="radio"/> Down

Mesh	Access Point	State	Connected Via	SSIDs	Channel	Clients
-	FAP2283U11022065		10.10.80.100	Radio 1: All Radio 2: All	Radio 1: 0 Radio 2: 0	Radio 1: 0 Radio 2: 0

- Edit
- Delete
- Authorize
- Restart
- Upgrade

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.

The image shows two screenshots from the FortiGate web interface. The top screenshot is the 'User Group' configuration page for 'Guest_WiFi_Users'. The 'Type' is set to 'Guest', 'User ID' is 'Email', and 'Password' is 'Auto-Generate'. 'Enable Sponsor', 'Enable Company', and 'Enable Email' are checked. 'Expire Type' is 'After first login' and 'Default Expire Time' is '4 Hours'. The bottom screenshot is the 'WiFi SSID' configuration page for 'WLAN'. 'Traffic Mode' is 'Tunnel to Wireless Controller'. 'IP/Network Mask' is '10.10.10.1/255.255.255.0'. Under 'Administrative Access', 'HTTPS', 'PING', and 'SSH' are checked. Under 'DHCP Server', 'Enable' is checked. The 'Address Range' table shows 'Starting IP' as '10.10.10.2' and 'End IP' as '10.10.10.254'. Under 'WiFi Settings', 'SSID' is 'Guest WiFi Access', 'Security Mode' is 'Captive Portal', and 'User Groups' is 'Guest_WiFi_Users'.

Name: Guest_WiFi_Users
Type: Firewall Fortinet Single Sign-On (FSSO) Guest RADIUS Single Sign-On (RSSO)
User ID: Email
Password: Auto-Generate
 Enable Name
 Enable Sponsor: Optional
 Enable Company: Optional
 Enable Email
 Enable Phone Number
 FortiGuard Messaging Service
 Custom - SMS Provider: No SMS providers configured
Expire Type: After first login
Default Expire Time: 4 Hours
 Enable Batch Guest Account Creation

Name: WLAN
Type: WiFi SSID
Traffic Mode: Tunnel to Wireless Controller
IP/Network Mask: 10.10.10.1/255.255.255.0
Administrative Access: HTTPS PING HTTP FMG-Access
 SSH SNMP TELNET FCT-Access
IPv6 Administrative Access: HTTPS PING HTTP FMG-Access
 SSH SNMP TELNET
DHCP Server: Enable
Address Range:

Starting IP	End IP
10.10.10.2	10.10.10.254

Netmask: 255.255.255.0
Default Gateway: Same as Interface IP Specify
DNS Server: Same as System DNS Specify
Advanced...
WiFi Settings:
SSID: Guest WiFi Access
Security Mode: Captive Portal
Customize Portal Messages:
User Groups: Guest_WiFi_Users
Maximum Clients:

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.

Policy Type Firewall VPN

Policy Subtype Address User Identity Device Identity

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

Enable NAT

Use Destination Interface Address Fixed Port

Use Dynamic IP Pool

Use Central NAT Table

Logging Options

No Log

Log Security Events


Log all Sessions

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 simplify 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.

Administrator	<input type="text" value="Receptionist"/>
Type	<input checked="" type="radio"/> Regular <input type="radio"/> Remote <input type="radio"/> PKI
Password	<input type="password" value="*****"/>
Confirm Password	<input type="password" value="*****"/>
Comments	<input type="text" value="For providing wifi access to guests"/> 35/255
Contact Info	
<input type="checkbox"/> Email Address	<input type="text"/>
<input type="checkbox"/> SMS	<input checked="" type="radio"/> FortiGuard Messaging Service <input type="radio"/> Custom
	Phone Number <input type="text"/>
<input type="checkbox"/> Enable Two-factor Authentication	
<input type="checkbox"/> Restrict this Admin Login from Trusted Hosts Only	
<input checked="" type="checkbox"/> Restrict to Provision Guest Accounts	
Guest Groups	<input type="text" value="Guest_WiFi_Users"/> 

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.

User ID	Use Email Address
Password	Auto Generated
Sponsor	<input type="text" value="Terry White"/> Optional
Company	<input type="text" value="BigCo"/> Optional
Email	<input type="text" value="pbrown@bigco.com"/>
Expiration	<input type="text" value="2013-04-16 12:51"/>

User Successfully Created

User ID	pbrown@bigco.com
Password	X876Yq
Company	BigCo
Sponsor	Terry White
Email	pbrown@bigco.com
Expiration	2013-04-16 12:51:00
Send	 



Terms and Disclaimer Agreement

You are about to access Internet content that is not under the control of the network access provider. The network access provider is therefore not responsible for any of these sites, their content or their privacy policies. The network access provider and its staff do not endorse nor make any representations about these sites, or any information, software or other products or materials found there, or any results that may be obtained from using them. If you decide to access any Internet content, you do this entirely at your own risk and you are responsible for ensuring that any accessed material does not infringe the laws governing, but not exhaustively covering,

I accept the terms and disclaimer agreement

Authentication for SSID: Guest WiFi Access

Please enter your username and password to continue

Username:

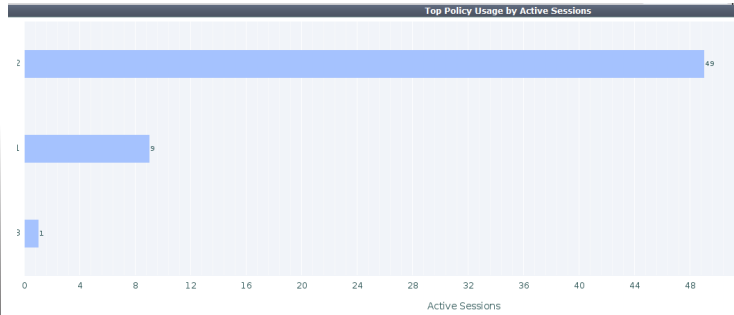
Password:

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

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

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

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



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

