Mitel Cloud VOIP

Integration Guide

Mitel VoIP, WatchGuard Wi-Fi Cloud, WatchGuard Firebox, and QoS

Deployment Overview

This document describes how to set up QoS from the communication path of the Mitel Mobile Client, WatchGuard AP420, WatchGuard FireboxV, to the Mitel Cloud VoIP service. The document does not include information on switch configuration for QoS or VLANs. If your deployment uses a switch, verify it can be configured for QoS and VLANs.

Integration Summary

To complete this integration, you must have these versions of hardware, software, and services:

- Mitel Connect – Mitel Cloud Portal
- WatchGuard:
  - AP420 Wi-Fi Cloud Account
  - FireboxV with Fireware v12.1

Test Topology

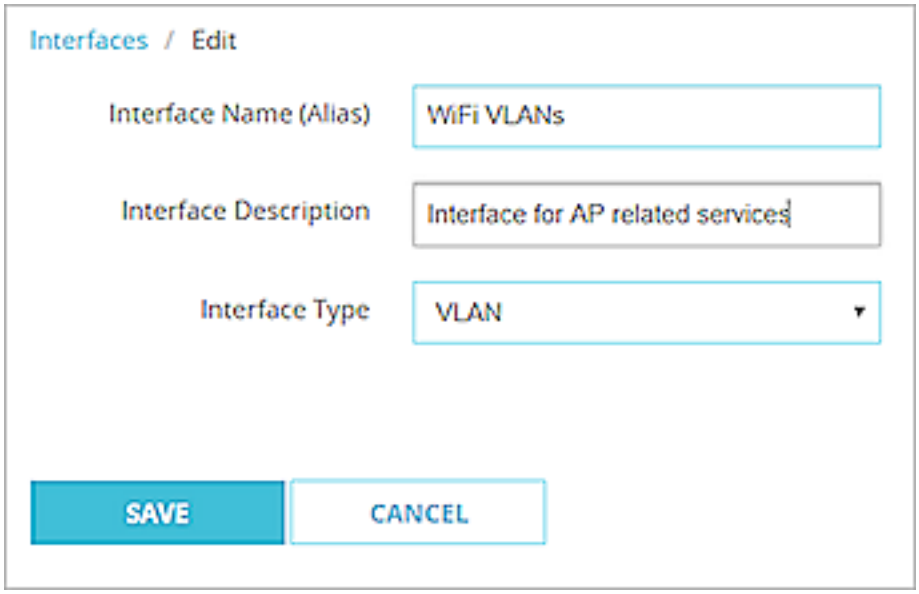
Configure Your Firebox with VLANs and Policies

In this example, we set up three VLANs – one for AP management, one for general use, and one for your mobile phone. The network traffic for the phone VLAN uses QoS markings for priority.

For more information on how to configure your Firebox for QoS, see About QoS Marking in *Fireware Help*.

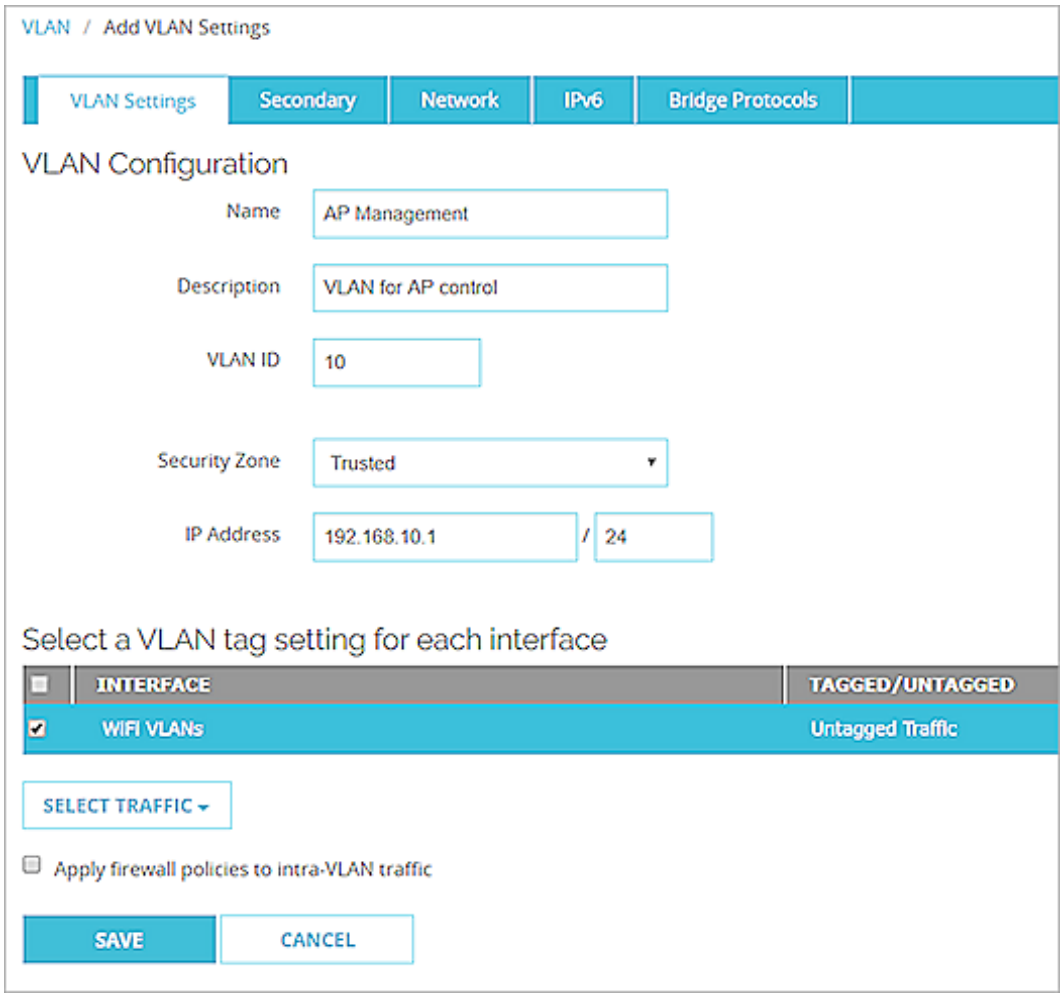
To configure an interface from, Fireware Web UI:

1. Select **Network > Interfaces**. Select an interface to configure and select **Edit**.
2. In the **Interface Name (Alias)** text box, type the name for the VLAN interface.
3. (Optional) In the **Interface Description** text box, type a description for the VLAN.
4. From the **Interface Type** drop-down list, select **VLAN**.
5. Click **Save**.



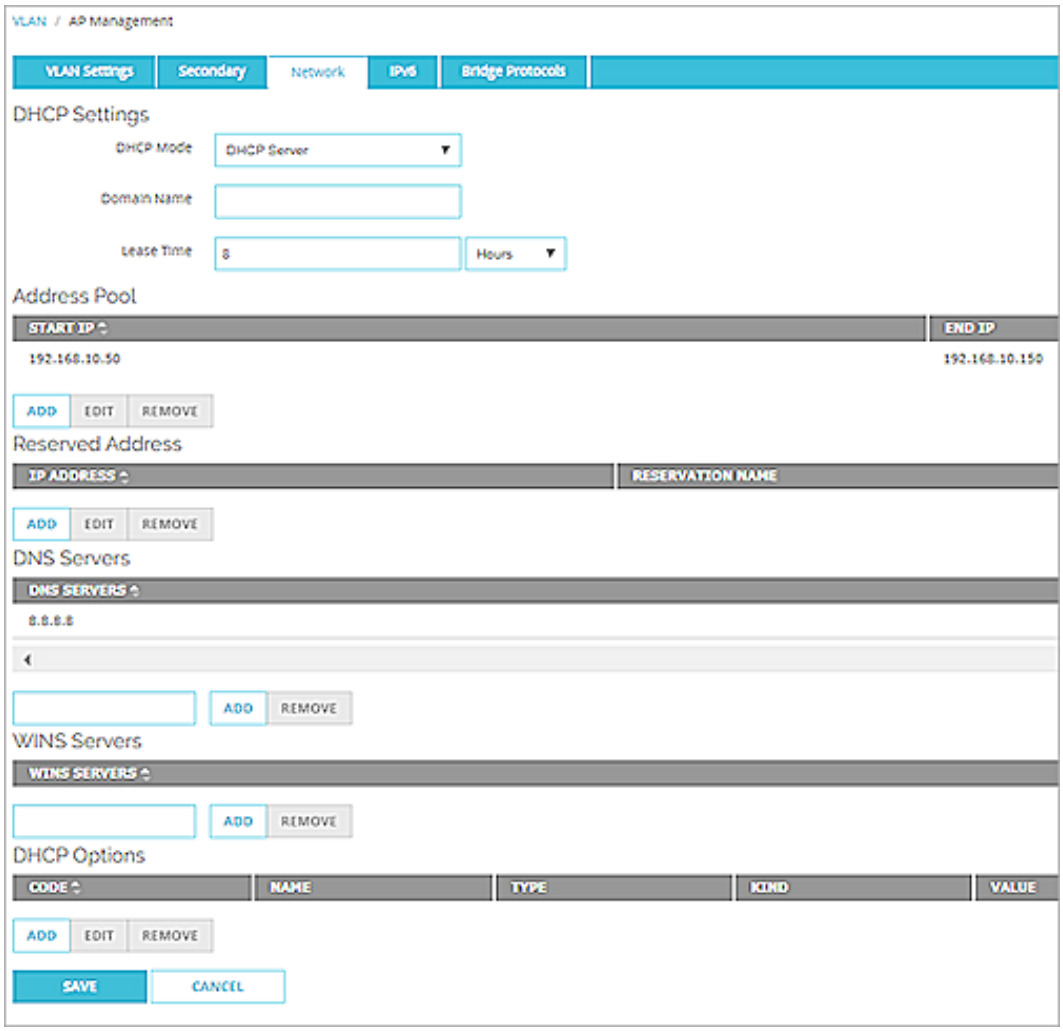
To create a VLAN and assign it an interface from Fireware Web UI:

1. Select **Network** > **VLAN**.
   The VLAN page appears, with a list of existing user-defined VLANs and their settings.
2. Click **Add**.
   The VLAN Settings page appears.
3. In the **Name** text box, type a name for the VLAN. The name cannot contain spaces.
4. (Optional) In the **Description** text box, type a description of the VLAN.
5. In the **VLAN ID** text box, or type or select a value for the VLAN.
6. From the **Security Zone** drop-down list, select the zone you want to assign.
7. In the **IP Address** text box, type the address of the VLAN gateway.
8. In the **Select a VLAN tag setting for each interface** section, select one or more interfaces.
9. From the **Select Traffic** drop-down list, select **Untagged Traffic**.



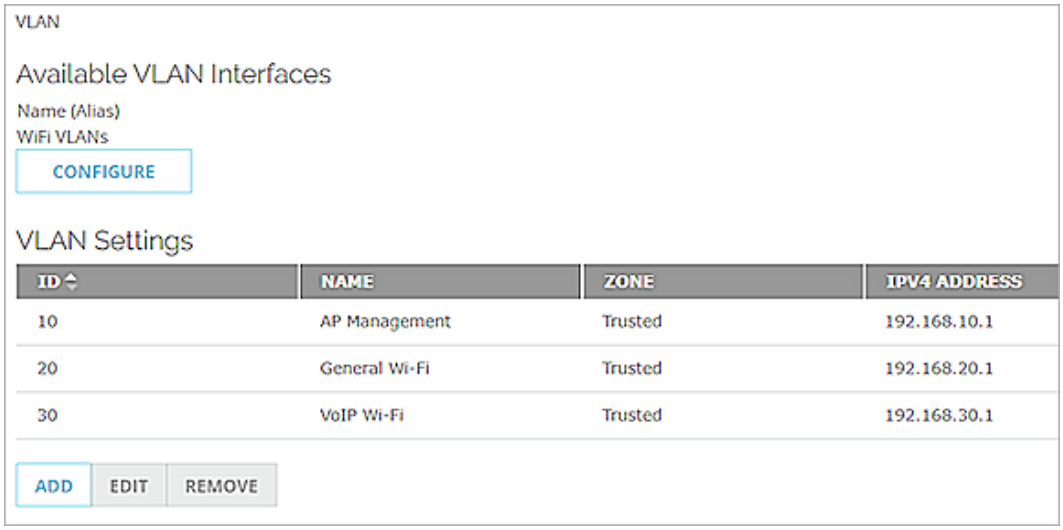
To configure DHCP for a VLAN from Fireware Web UI:

1. Select the **Network** tab.
2. In the DHCP Settings section, from the **DHCP Mode** drop-down list, select **DHCP Server**.
3. In the **Domain Name** text box, type an optional domain suffix to provide to clients.
4. To change the default lease time, from the drop-down list at the top of the page, select a different time interval.
5. Configure the **Address Pool**, **Reserved Address**, **DNS Servers**, **WINS Servers**, and **DHCP Options** sections. Click **Save**.



6. Add the other two VLANs for general Wi-Fi and VoIP Wi-Fi. From the **Select Traffic** drop-down list, select **Tagged Traffic**. This creates two tagged VLANs for Wi-Fi traffic.

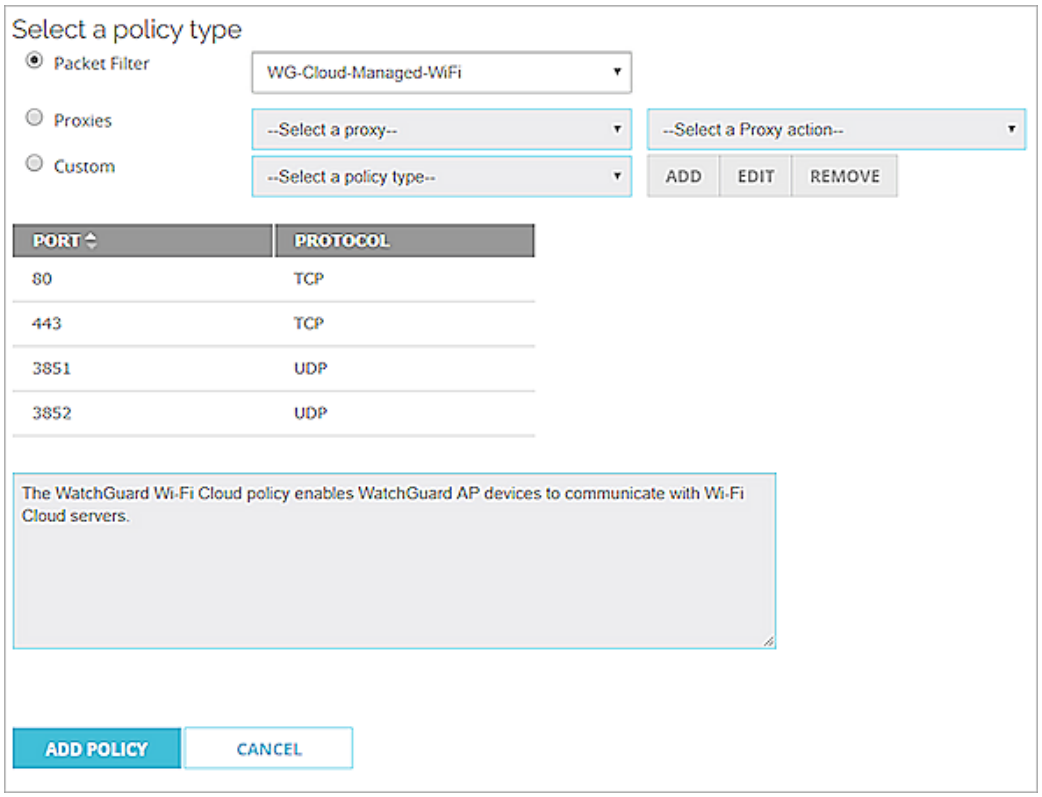
This is the example configuration for all available VLAN interfaces.



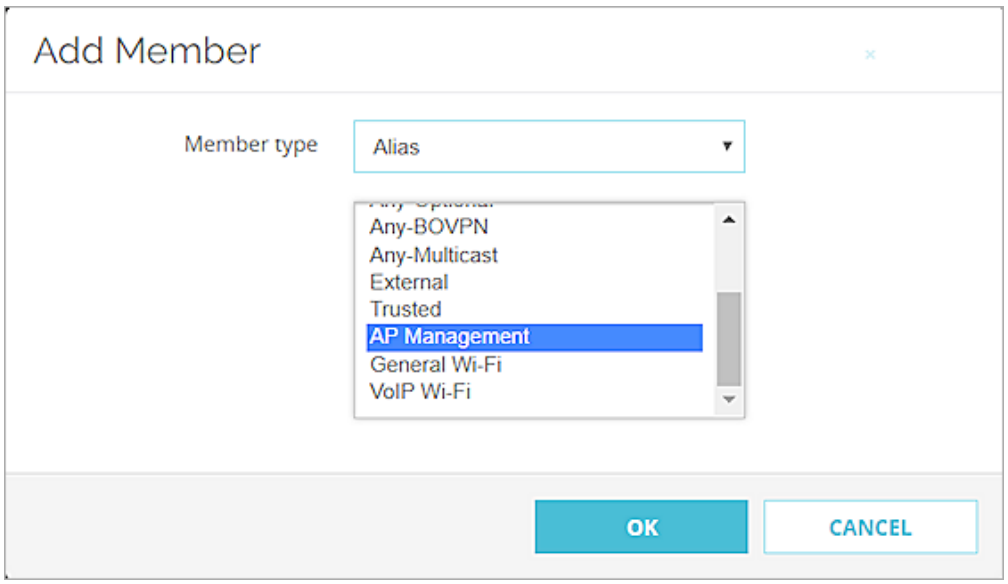
Add two policies to use for General Wi-Fi and AP Cloud Management. The WatchGuard Wi-Fi Cloud requires HTTP TCP ports 80 and 443, and UDP port 3851 and 3852 to be open in an outbound policy. This example uses the WG-Cloud-Managed-Wi-Fi packet filter policy. For more information about WatchGuard Wi-Fi Cloud, see About WatchGuard Wi-Fi Cloud.

The first policy handles traffic for AP management. To add a firewall policy from Fireware Web UI:

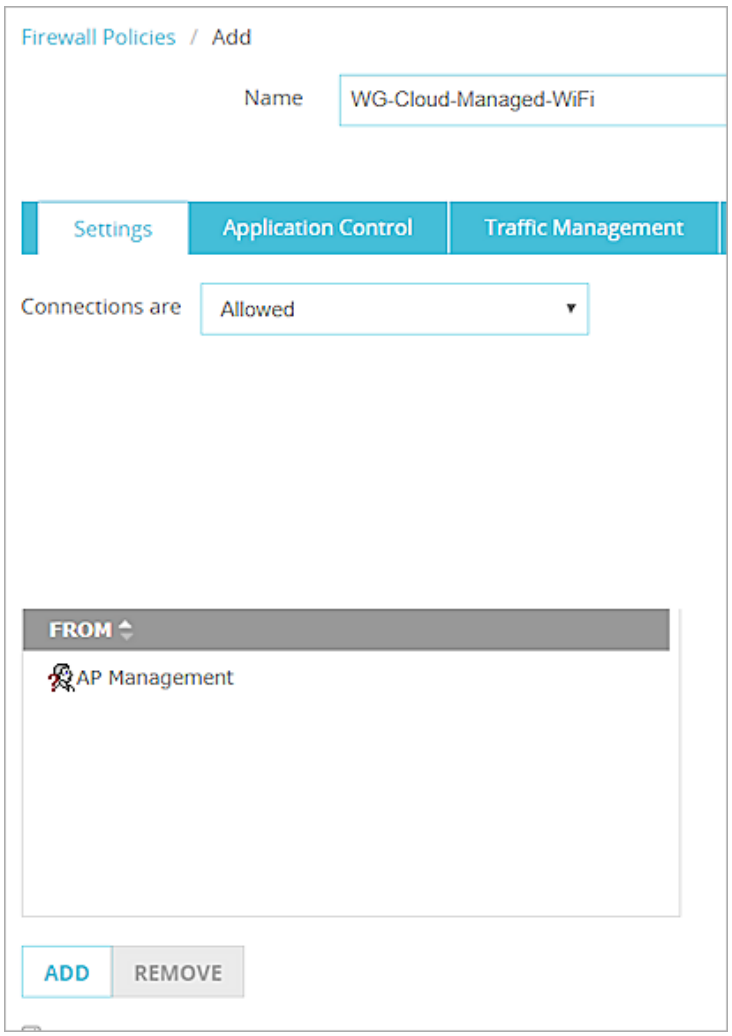
1. Select **Firewall > Firewall Policies**.
2. Click **Add Policy**.
3. Select **Packet Filter**. From the drop-down list, select **WG-Cloud-managed-WiFi** .
4. Click **Add Policy**.
   The full settings of the created policy appear.



5. In the **From** section, remove the **Any-Trusted** alias. Select **Add**.
   The Add Member page appears.
6. From the**Member type** drop-down list, select **Alias**. Select **AP Management**.


Add Member
Member type
Alias
Any-BOVPN
Any-Multicast
External
Trusted
AP Management
General Wi-Fi
VoIP Wi-Fi
OK
CANCEL

7. Click **OK**.



8. C;ocl **Save** to add the policy.

Add another policy for general Wi-Fi traffic to match your company's corporate policy on filtering traffic.

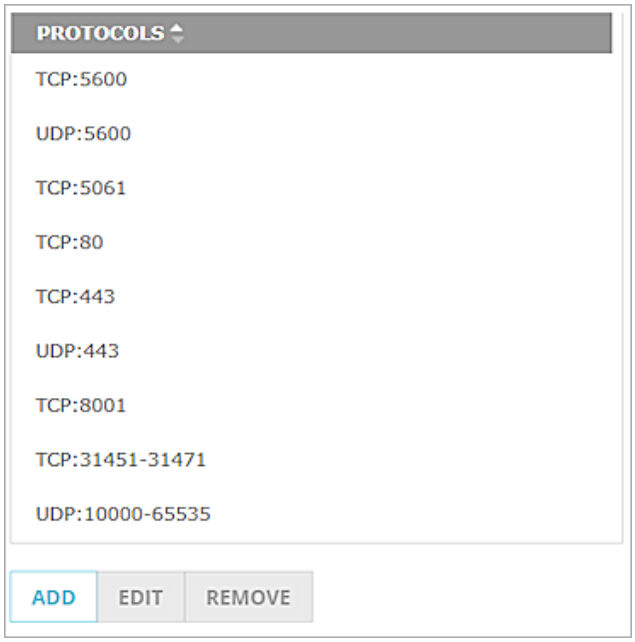
The last policy is specific to traffic that passes through the Mitel mobile phone communication. Mitel documentation includes the Mitel Connect Cloud Ports necessary for communication to be successful. These ports include:

- TCP/UDP 5600 SIP
- TCP 5061 SIPS
- TCP 80 HTTP
- TCP/UDP 443
- TCP 8001 Admin
- TCP 31451 - 31471 ECC Supervisor
- UDP 10000 - 65535

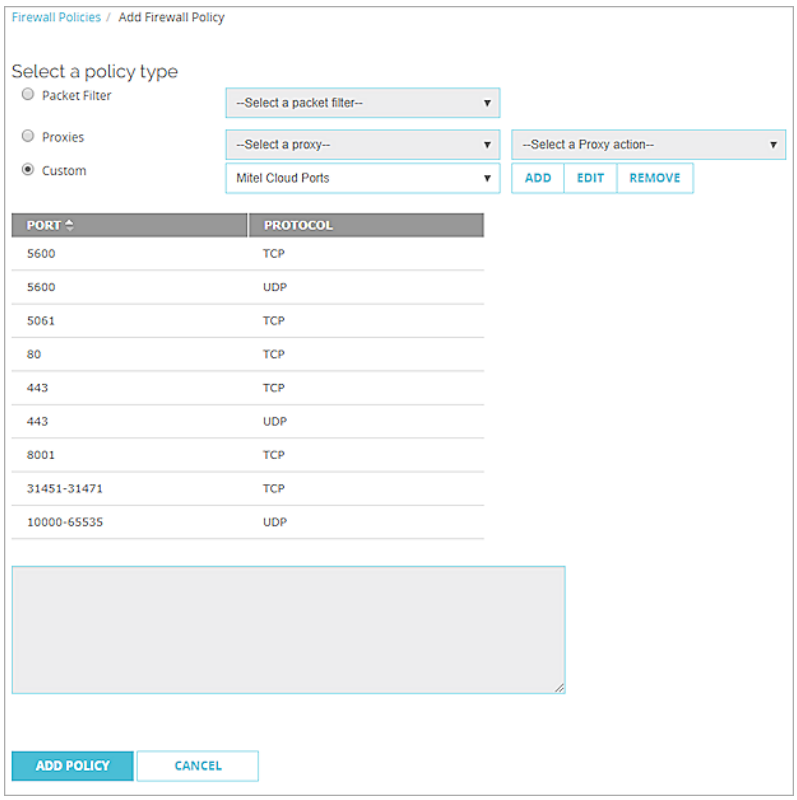
To pass Mitel mobile phone communication traffic, add a policy from Fireware Web UI:

1. Select **Firewall > Firewall Policies > Add Policy**.
2. Select **Custom** policy type. Click **Add**.
   A new custom policy type is created.

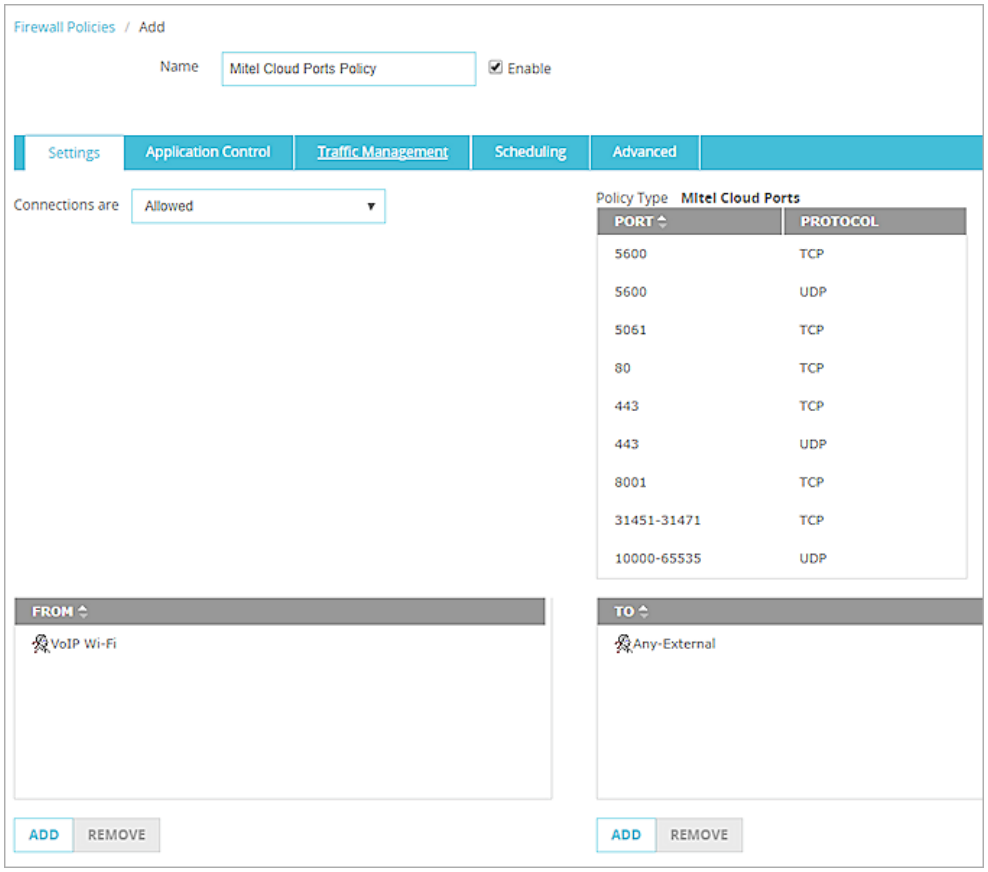
3. In the **Protocol** section, add each TCP or UDP port until the list is complete.
   The Select a policy type page appears.



4. Click **Save**.
   The Add Firewall Policy page appears with your custom selections.
5. Click **Add Policy**.



6. Select the **Settings** tab.
7. In the **From** section, replace the Any-Trusted alias with the alias you created for the VoIP VLAN. Click **Save**.



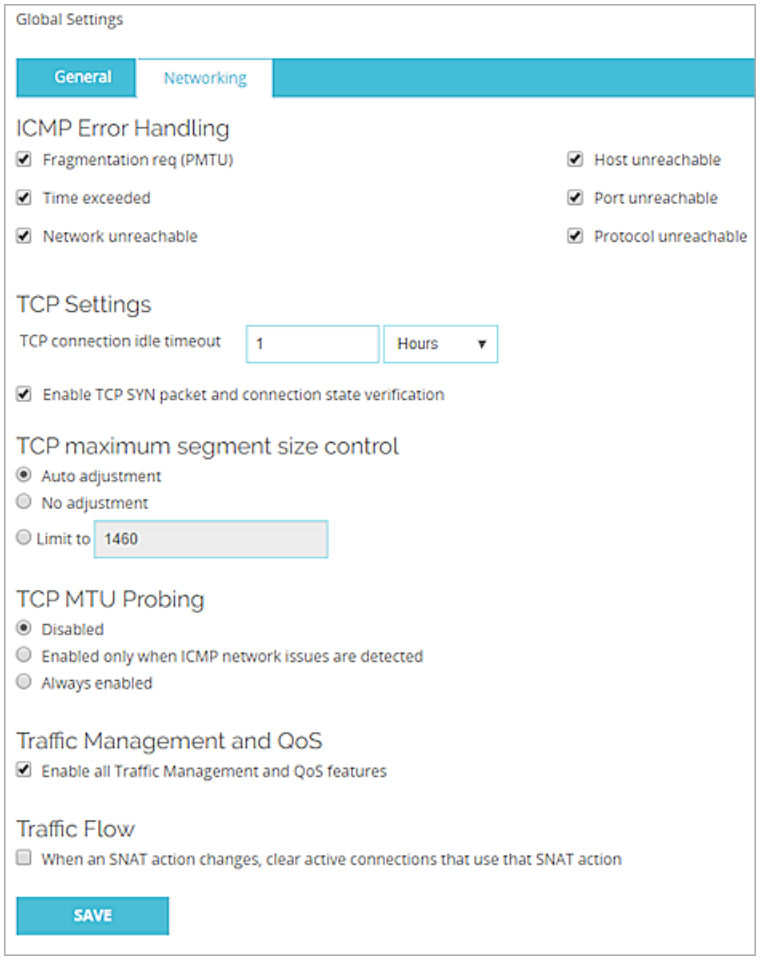
ⓘ You must have an active DNS policy for Mitel MiCloud communication. You can modify the policy you created or add this subnet to your current DNS policy.

Apply QoS to Firewall Policies

Firewall policies can apply QoS markings for each policy and take precedence over the QoS settings for an interface. Globally, QoS, must be enabled before you configure the policy.

To preserve QoS marking from Fireware Web UI:

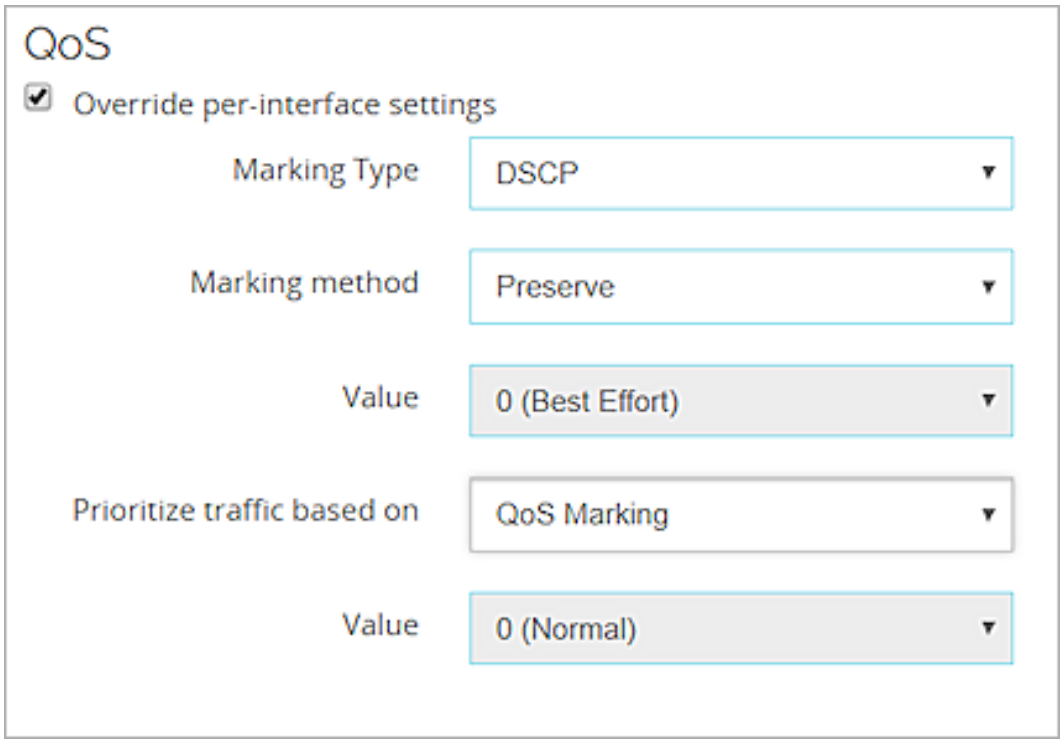
1. Select **System > Global Settings**.
2. On the **Networking** tab, below Traffic Management and QoS, select the **Enable all Traffic Management and QoS features** check box.



3. Click **Save**.

To configure QoS marking, from Fireware Web UI:

1. Select **Firewall > Firewall Policies**. Select the check box for the Mitel Cloud Portal policy. Use the **Action** drop-down list to edit the policy.
2. Click the **Advanced** tab.
3. Select **Override per-interface settings**.
   The QoS page appears.
4. From the **Marking Type** drop-down list, select an option. For this example we chose **DSCP**.
5. From the **Marking Method** drop-down list select an option. For this example we chose **Preserve**.
6. If you selected **Assign**, from the **Value** drop-down list, select a marking value.
   If you selected the **IP Precedence** marking type, select a value from 0 (normal priority) through 7 (highest priority).
   If you selected the **DSCP** marking type, the values are 0-56.
7. From the **Prioritize Traffic Based On** drop-down list, select **QoS Marking**.



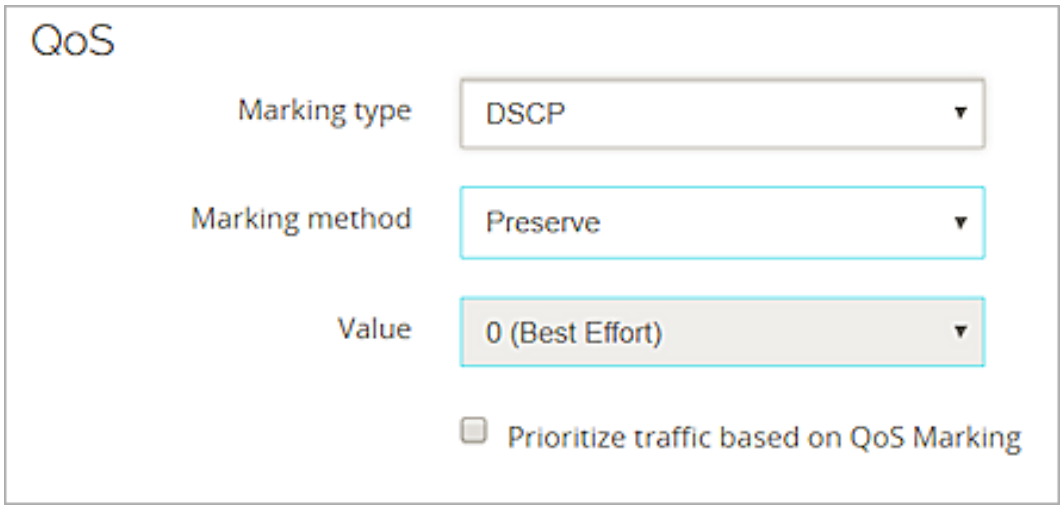
8. Click **Save**.

WatchGuard External Interface Configuration for QoS

Many Internet Service Providers drop the marking on the QoS packet when it is received. Make sure you understand how QoS is handled by your ISP before you configure the external interface of your Firebox to pass QoS marking.

From Fireware Web UI:

1. Select **Network > Interfaces**.
2. Highlight the external interface. Select **Edit**.
3. Select the **Advanced** tab.
4. From the **Marking type** drop-down list, select **DSCP**.
5. From the **Marking method**drop-down list, select **Preserve**.
6. Click **Save**.



WatchGuard Wi-Fi Cloud Basic Configuration

This integration guide covers only part of the configuration of APs in WatchGuard Wi-Fi Cloud. To complete the configuration of your APs, you must:

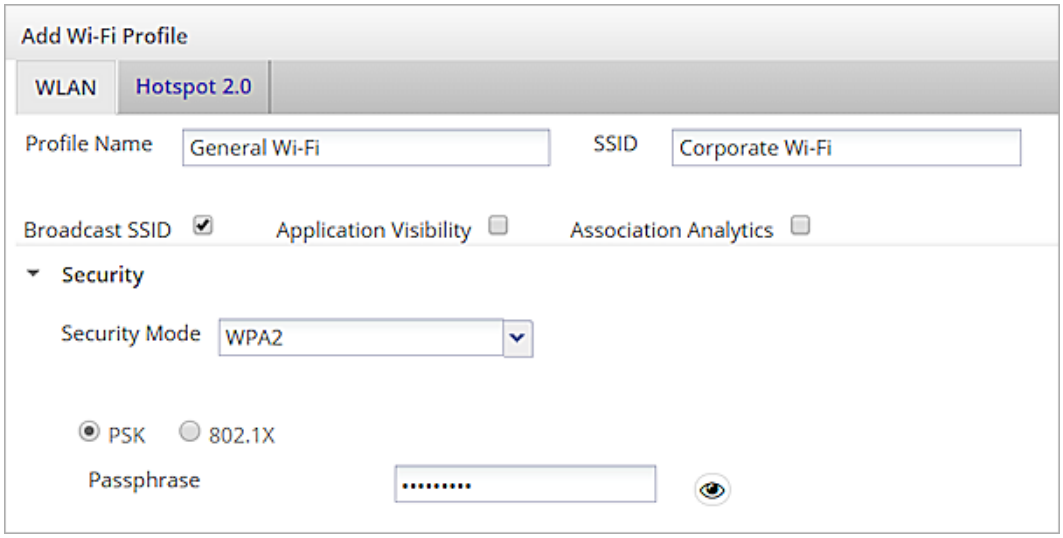
- Upgrade your AP software
- Add the AP to a location in your organization tree
- Create SSID profiles for your AP
- Create a device template to apply common device, radio, and SSID settings to your AP
- Create and apply an authorized WLAN security policy for your SSID

For more information on how to prioritize traffic with Wi-Fi Cloud, see Quality of Service (QoS).

WatchGuard Wi-Fi Cloud VLAN and QoS Assignment

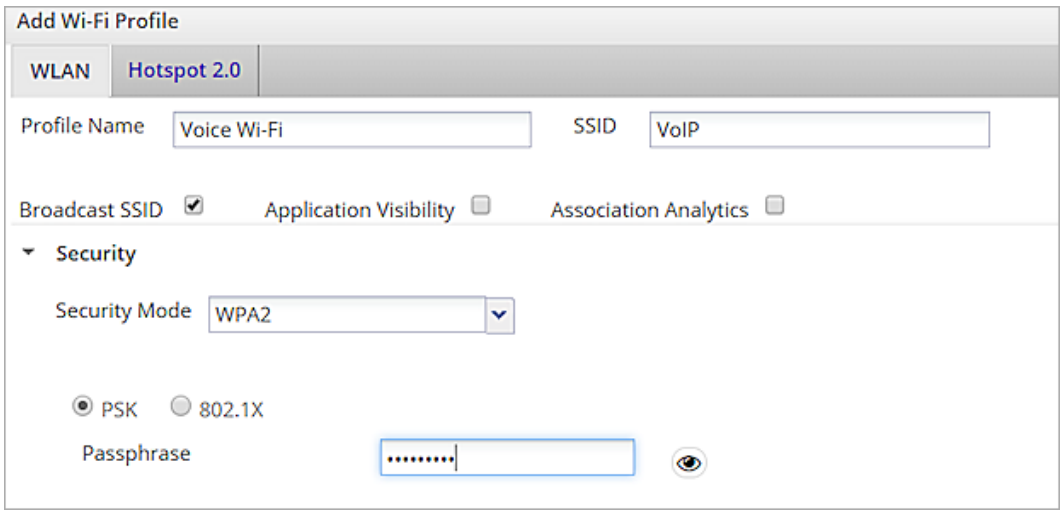
To create the SSID profile for general Wi-Fi use:

1. Log in to your WatchGuard Cloud Wi-Fi account.
2. Select **My WatchGuard > Manage Wi-Fi Cloud**. Select **Manage**.
3. Select **Configuration > Device Configuration > SSID Profiles**.
4. Click **Add New Wi-Fi Profile**.
   The Add Wi-Fi Profile dialog box appears.
5. Type a **Profile Name** and **SSID** name. Add the appropriate security settings for your general traffic.

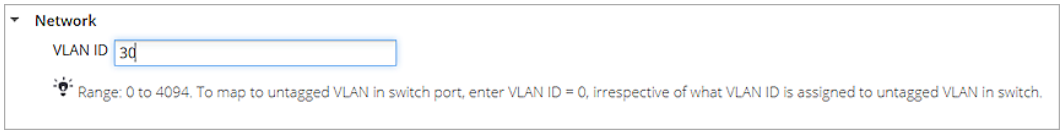


6. Expand the **Network** section. Add the VLAN ID for general traffic.

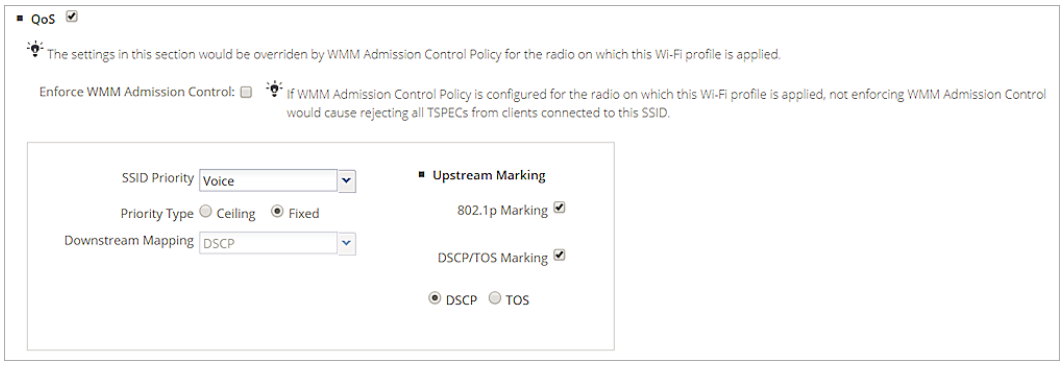
7. Click **Save**.
8. Select **Add New Wi-Fi Profile** to add the SSID profile for Mitel VoIP VLAN.
9. Type a **Profile Name** and **SSID** name. Add the appropriate security settings for VoIP traffic.



10. Expand the **Network** section. Add the VLAN ID for the VoIP subnet.



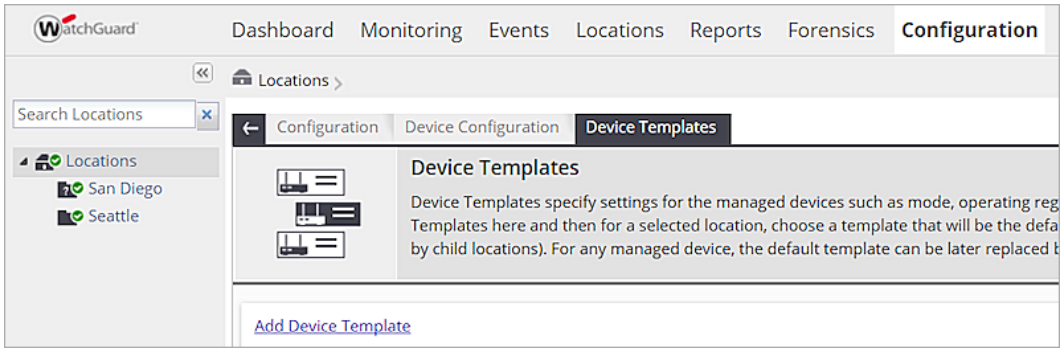
11. Expand the **Traffic Shaping & QoS** section. Select the **Enable QoS** check box.
12. Set the **SSID Priority** to **Voice**.
13. Select the **802.1p Marking** check box. This enables the **Upstream Marking** to map to a priority subject to a maximum of the selected SSID priority and set in the 802.1p header and the IP header.
14. Select **DSCP** to enable the **DCSP/TOS Marking**.
15. Set the **Priority Type** to **Fixed**. All traffic for this SSID must be transmitted at the selected priority regardless of the priority indicated in the 802.1p or IP header.
16. Select **Save**.



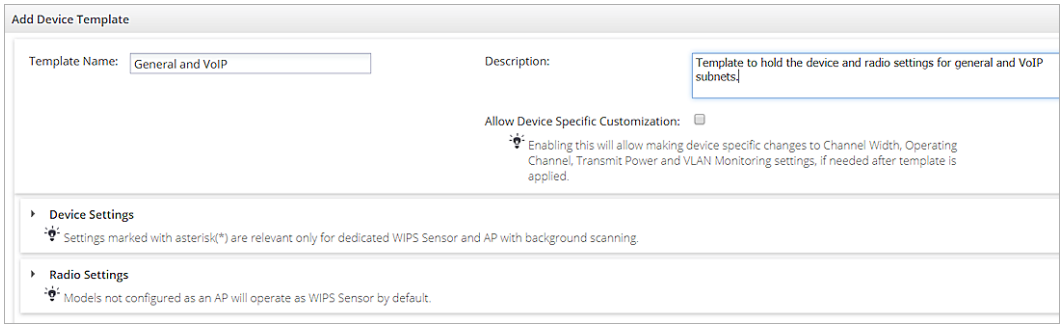
WatchGuard Wi-Fi Cloud Template Assignment

To transfer the created settings to a template to apply to a device, from WatchGuard Wi-Fi Cloud:

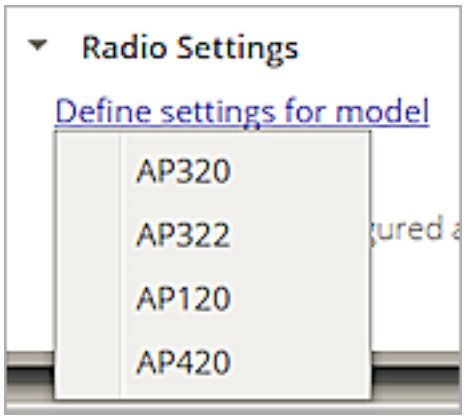
1. Select **Manage > Configuration > Device Configuration > Device Templates**.



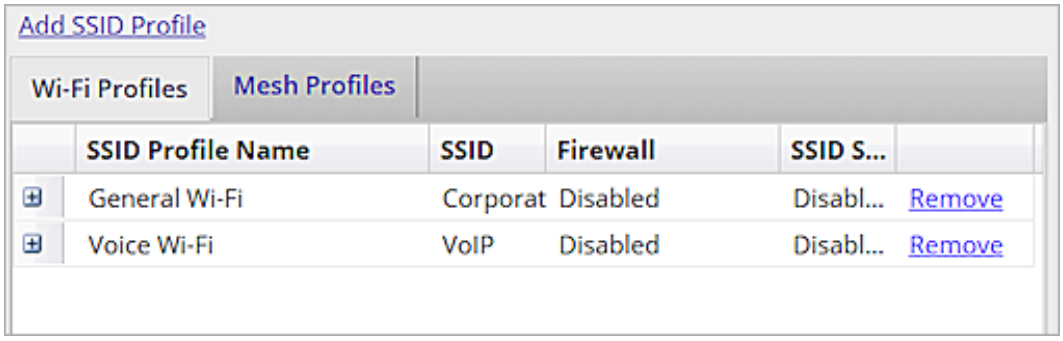
2. Click **Add Device Template**.
   The Add Device Template dialog box appears.
3. In the **Template Name** text box, type a descriptive name for this template.



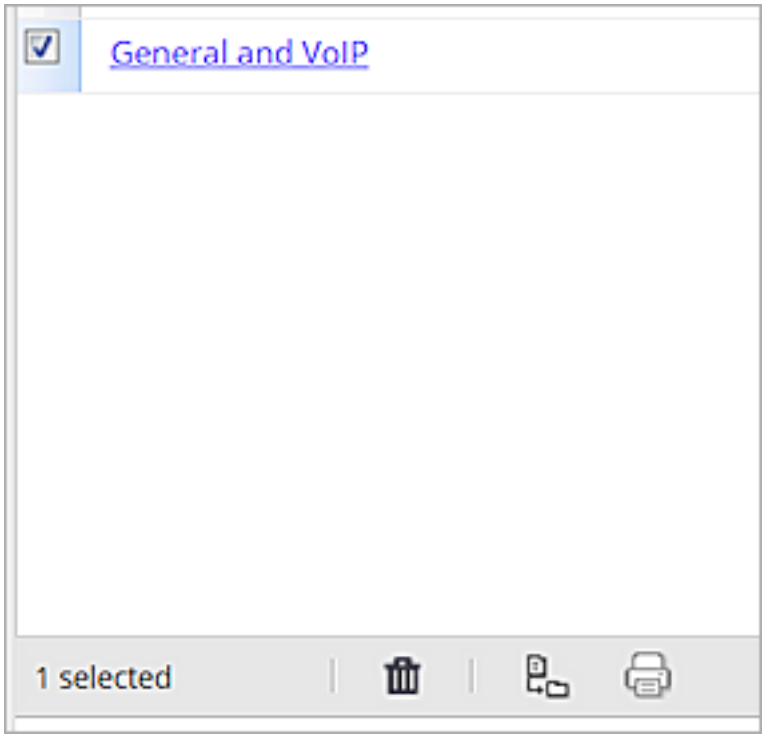
4. Expand the **Device Settings** section.
5. Expand the **Device Password** section and specify a user name and password.
   The New password is applied on all the devices associated with the device template.
6. Expand the **Radio Settings** section.
7. Click **Define settings for model** and select your AP model.



8. For each radio, click **Add SSID Profile** and select the created SSID profiles for each radio.



9. Specify the other radio settings as required for your network. Click **Save**. If this template is needed for a different location, select the Copy-to icon to copy the template.



Apply the Device Template to an AP

The configuration is complete after you mark the template as default for the selected location. Apply it to the APs in the selected location. APs deployed in the future are configured with the settings in the default template.

1. Open **Manage** and select the desired location.
2. Select **Configuration > Device Configuration > Device Templates**.
3. Click **Make Default**.
4. To apply the template to the APs in this location, click **Yes**.

Test the Integration with the Mitel Phone Application

1. Get a Mitel MiCloud user account with user names, passwords, and assigned phone numbers.
2. Download and install the Mitel Connect App for iOS or Andriod.
3. Connect to the configured VoIP SSID.
4. Open the Mitel application and type the user name, password, and assigned phone number.

About This Guide

Guide Type

Documented Integration – WatchGuard or a Technology Partner has provided documentation demonstrating integration.

Guide Details

WatchGuard provides integration instructions to help our customers configure WatchGuard products to work with products created by other organizations. If you need more information or technical support about how to configure a third-party product, see the documentation and support resources for that product.

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Guide revised: 2/20/2018

Copyright, Trademark, and Patent Information

Complete copyright, trademark, patent, and licensing information can be found in the Copyright and Licensing Guide, available online at http://www.watchguard.com/wgrd-help/documentation/overview.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, providing best-in-class Unified Threat Management, Next Generation Firewall, secure Wi-Fi, and network intelligence products and services to more than 75,000 customers worldwide. The company's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for Distributed Enterprises and SMBs. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

For additional information, promotions and updates, follow WatchGuard on Twitter, @WatchGuard on Facebook, or on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at www.secplicity.org.

Address

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

Support

www.watchguard.com/support
U.S. and Canada +877.232.3531
All Other Countries +1.206.521.3575

Sales

U.S. and Canada +1.800.734.9905
All Other Countries +1.206.613.0895