safe connect
network access control

Safe•Connect Integration Script

For Juniper-Mist Controller Wireless Layer 2 Integration

This document provides a configuration example depicting the integration of the Safe•Connect RADIUS Server with a Juniper-Mist Wireless Layer 2 Controller

OPSWAT

OPSWAT
5650 Breckenridge Park Dr.
Suite 201
Tampa, FL 33610
863-802-3738
www.opswat.com

February 2020

COPYRIGHT © 2020 OPSWAT ALL RIGHTS RESERVED

Table of Contents

Summary 3
Safe•Connect Guest SSID Configuration 3
Safe•Connect Secure SSID Configuration 6
This concludes the integration of the Mist Controller with SafeConnect 10

COPYRIGHT © 2020 OPSWAT ALL RIGHTS RESERVED

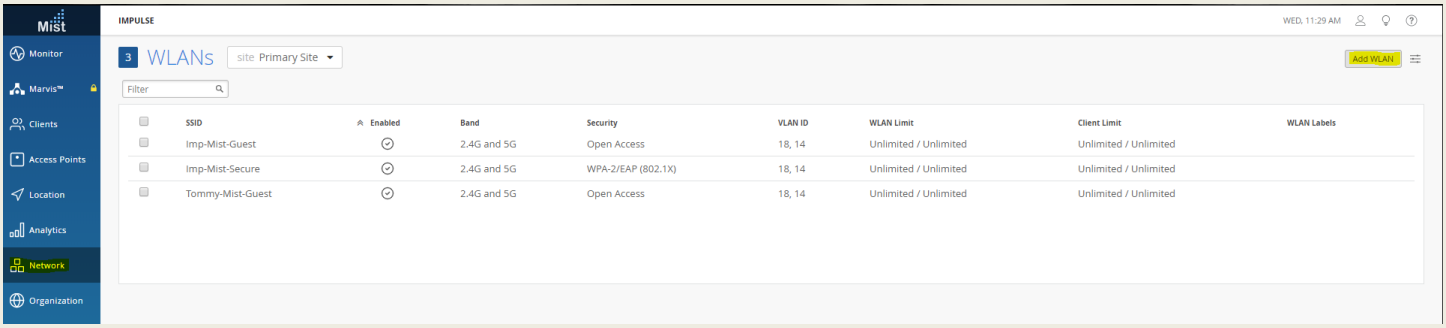
Summary

This document provides scripts complete the installation of Safe•Connect Radius Based Enforcement.

Safe•Connect Guest SSID Configuration

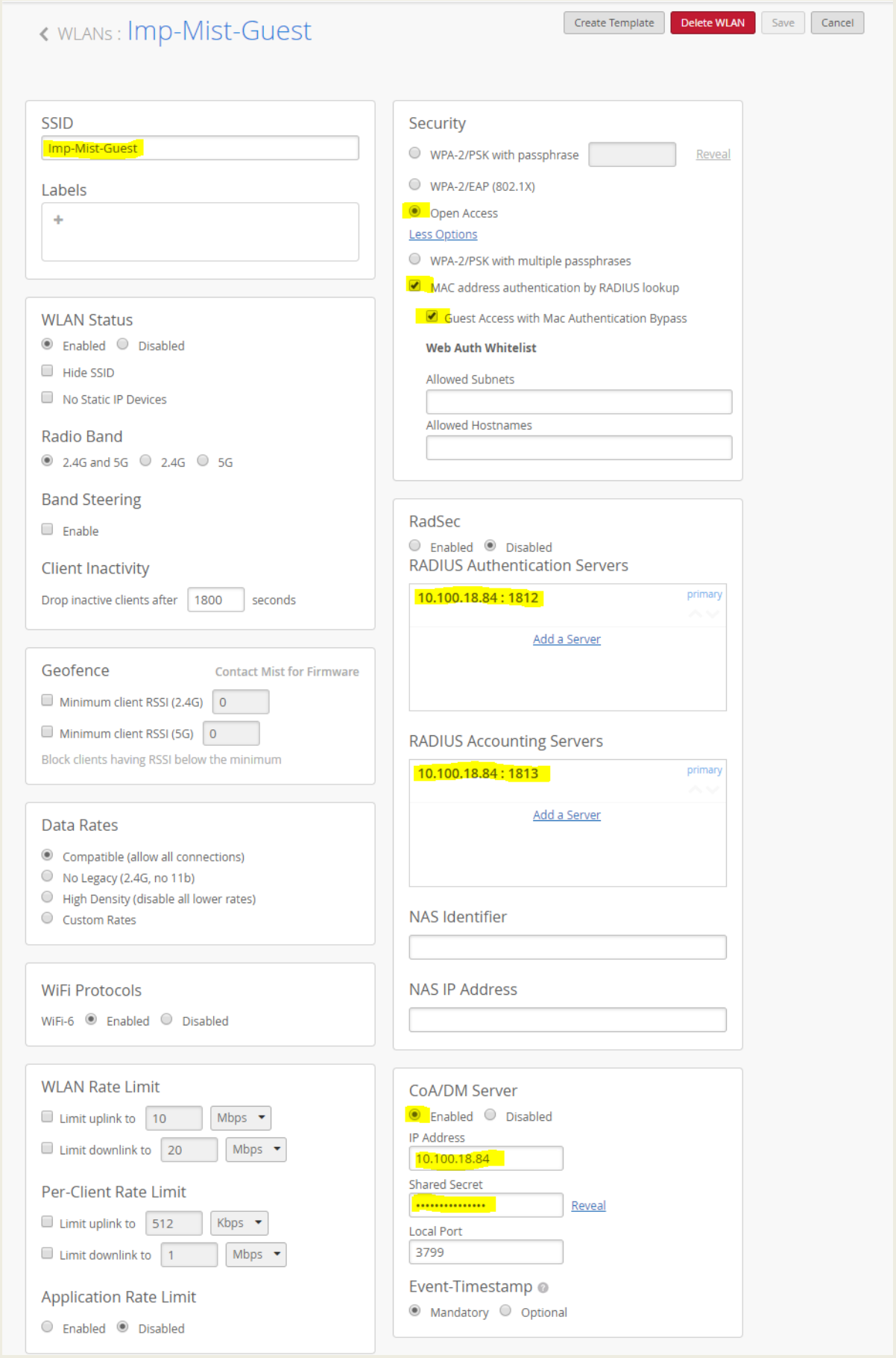
NOTE – SafeConnect can be configured to return a VLAN if desired or devices can use the default VLAN

Navigate to Network > WLANs and click Add WLAN



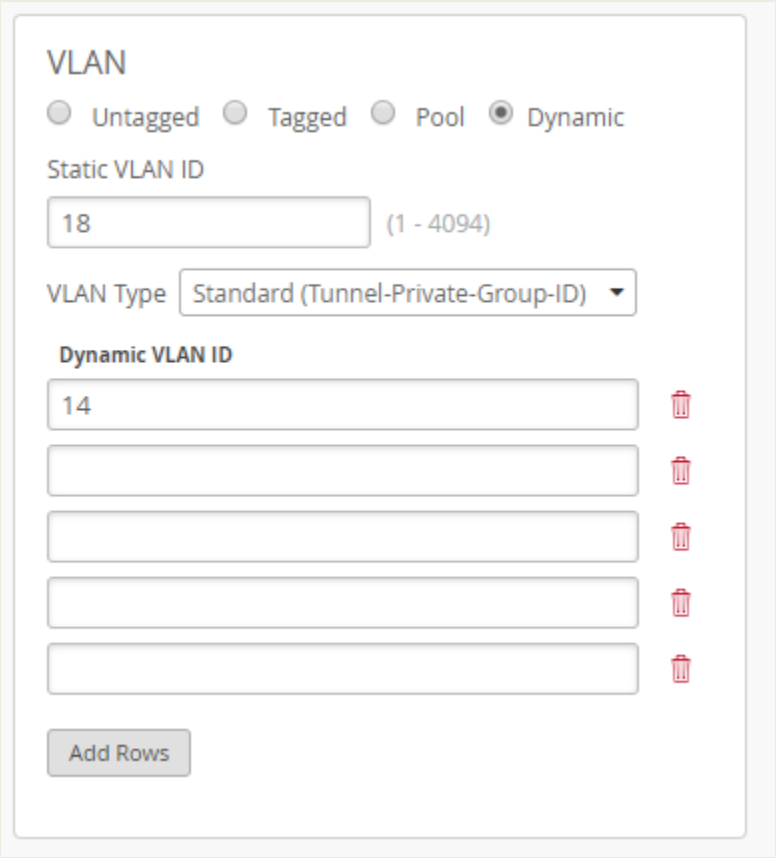
As shown in the picture below give the SSID a name (for example, Imp-Mist-Guest), set Security to Open Access and check the MAC address authentication by RADIUS lookup and Guest Access with MAC Authentication Bypass boxes. Add the SafeConnect appliance IP address as a RADIUS Authentication and RADIUS Accounting Server. Set COA/DM Server to enabled and add the IP address of the SafeConnect appliance and a shared secret (you will need this when adding the controller as a NAS on the SafeConnect appliance as well).

COPYRIGHT © 2020 OPSWAT ALL RIGHTS RESERVED

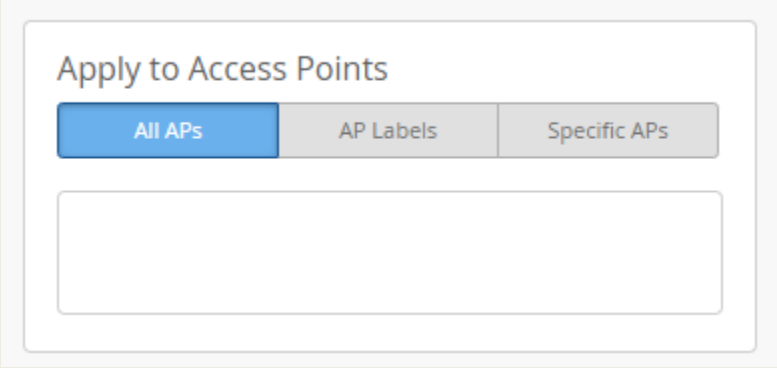


COPYRIGHT © 2020 OPSWAT ALL RIGHTS RESERVED

At this point you will need to configure the VLANs per your network. SafeConnect can be configured to use only the static VLAN as tagged/untagged or dynamic VLANs can be returned if that is preferred. For static VLAN select Untagged or Tagged and enter the Static VLAN ID. For RADIUS assigned VLANs select Dynamic, enter the Static VLAN ID (used if no VLAN is returned via RADIUS), set the VLAN type to Standard and enter the Dynamic VLAN IDs to be used as pictured below.

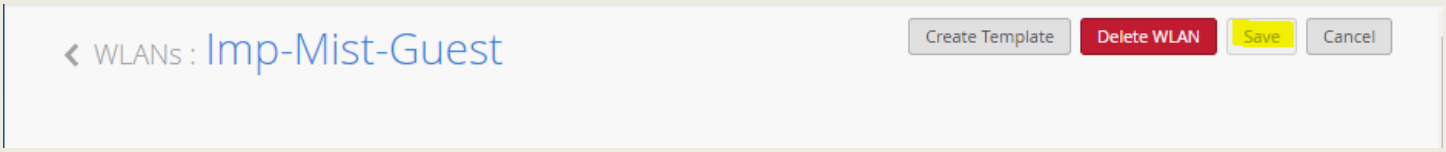


This WLAN can be added to all APs or Specific Aps as shown below:



Click Save in order to push the changes to the AP(s).

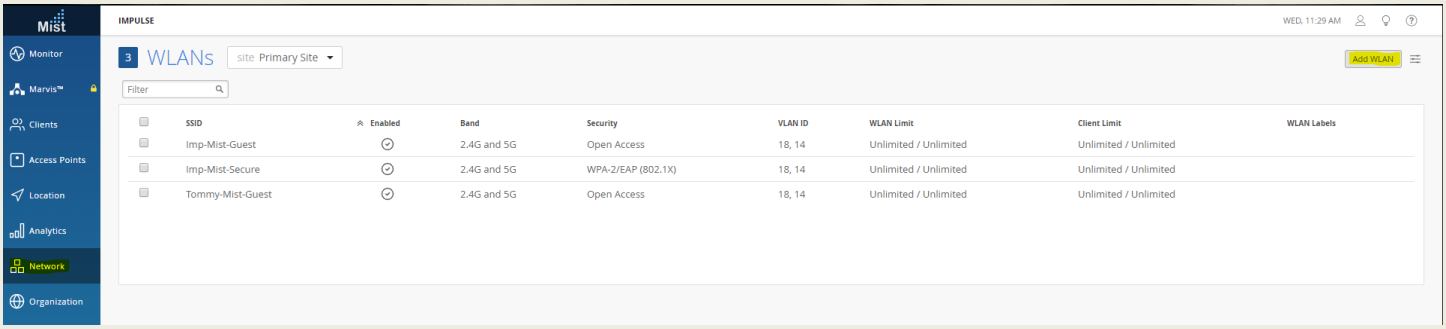
COPYRIGHT © 2020 OPSWAT ALL RIGHTS RESERVED



Safe•Connect Secure SSID Configuration

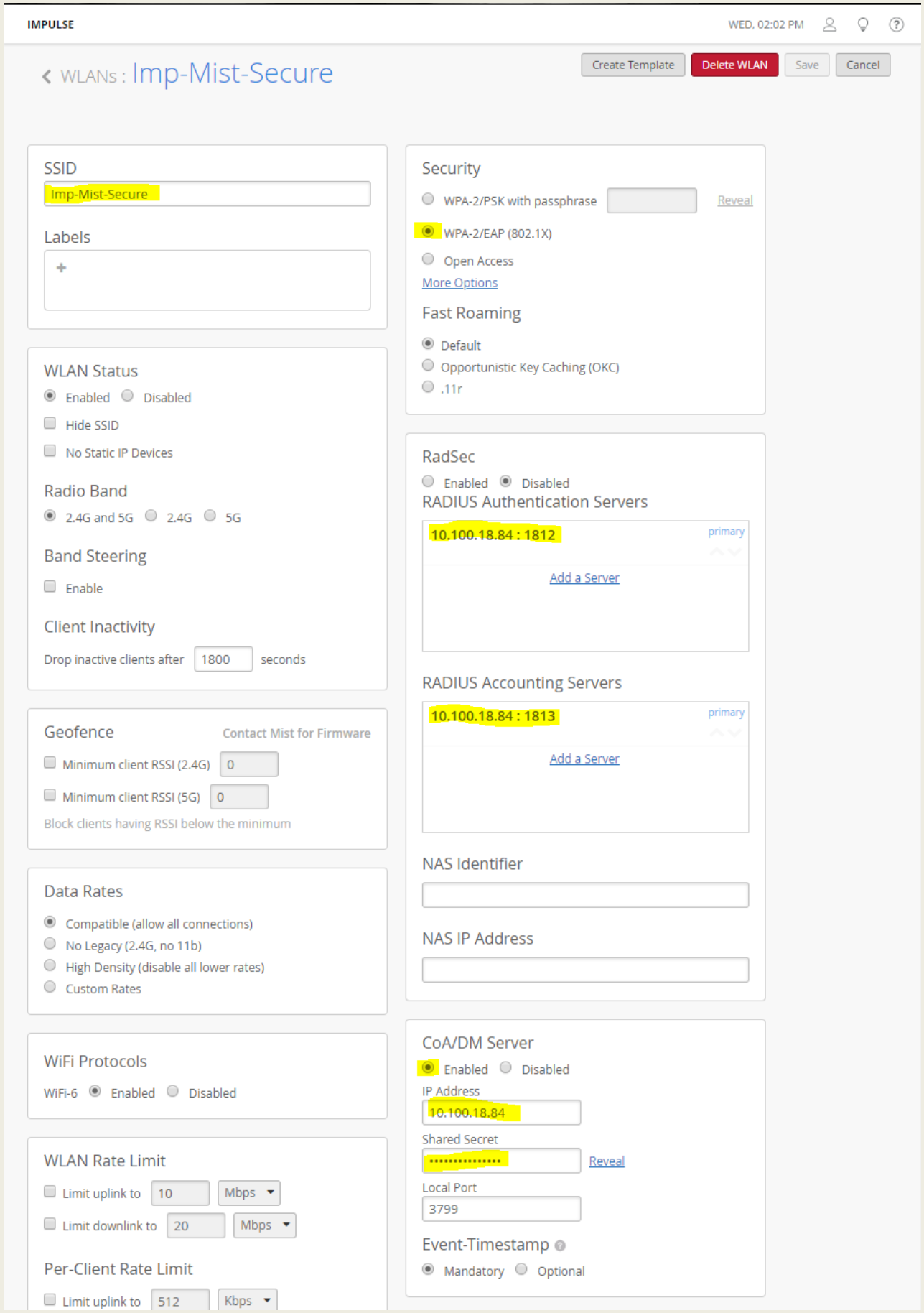
NOTE – SafeConnect can be configured to return a VLAN if desired or devices can use the default VLAN. COA redirect is not currently supported on Mist for Secure SSIDs, so either initial VLAN assignment via RADIUS can be configured or policy-based routing on the upstream device would need to be leveraged for redirection.

Navigate to Network > WLANs and click Add WLAN



As shown in the picture below give the SSID a name (for example, Imp-Mist-Secure), set Security to WPA/EAP (802.1X). Add the SafeConnect appliance IP address as a RADIUS Authentication and RADIUS Accounting Server. Set COA/DM Server to enabled and add the IP address of the SafeConnect appliance and a shared secret (you will need this when adding the controller as a NAS on the SafeConnect appliance as well).

COPYRIGHT © 2020 OPSWAT ALL RIGHTS RESERVED

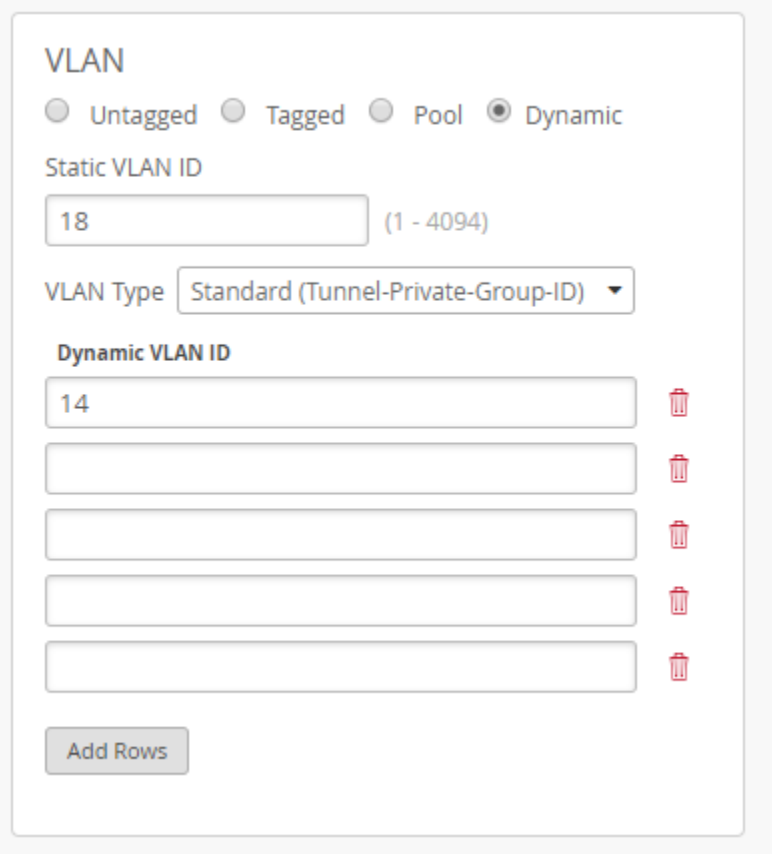


COPYRIGHT © 2020 OPSWAT ALL RIGHTS RESERVED

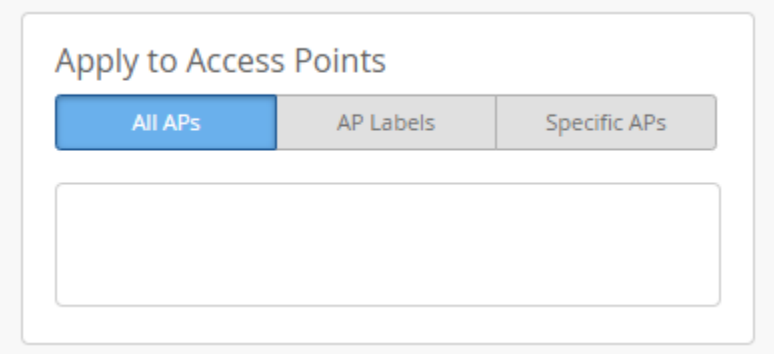
At this point you will need to configure the VLANs per your network. SafeConnect can be configured to use only the static VLAN as tagged/untagged or dynamic VLANs can be returned if that is preferred.

NOTE – If initial VLAN assignment only via RADIUS is desired, a single VLAN can be used, if redirection to SafeConnect is desired Dynamic would need to be selected and a quarantine VLAN will need to be added as well as the user VLANs.

For static VLAN select Untagged or Tagged and enter the Static VLAN ID. For RADIUS assigned VLANs select Dynamic, enter the Static VLAN ID (used if no VLAN is returned via RADIUS), set the VLAN type to Standard and enter the Dynamic VLAN IDs to be used as pictured below.

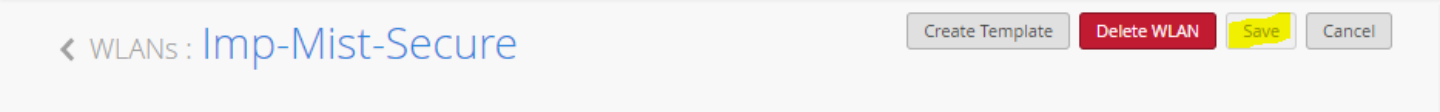


This WLAN can be added to all APs or Specific Aps as shown below:



COPYRIGHT © 2020 OPSWAT ALL RIGHTS RESERVED

Click Save in order to push the changes to the AP(s).



NOTE – If you are only configuring initial VLAN assignment via RADIUS, click Save as shown below. If you are configuring redirection to SafeConnect the upstream device will need to be configured with policy-based routing for the quarantine VLAN as shown in the example below.

Policy-based routing example for a Juniper EX4200 running version 9.6R1.13.

```
10.100.18.84 = SafeConnect appliance
10.100.14.0 = quarantine VLAN

routing-instances {
    to-safeconnect {
        instance-type forwarding;
        routing-options {
            static {
                route 0.0.0.0/0 next-hop 10.100.18.84;
            }
        }
    }
}
firewall {
    family inet {
        filter fil {
            term impulse_block {
                from {
                    source-address {
                      10.100.14.0/24;
                    }
                }
                then {
                    routing-instance to-safeconnect;
                }
        }
    }
}
```


COPYRIGHT © 2020 OPSWAT ALL RIGHTS RESERVED

This concludes the integration of the Mist Controller with SafeConnect

COPYRIGHT © 2020 OPSWAT ALL RIGHTS RESERVED