Xirrus WebTitan Content Filtering Configuration Guide

Xirrus and TitanHQ have partnered to deliver a powerful yet very simple to implement cloud based content filter for your Wi-Fi network. The content filtering can be turned on in a few minutes delivering robust protection to your network when you need it. Even if a client device is misconfigured or maliciously configured to bypass content filtering, the Xirrus AP will intercept such DNS requests and route them to the WebTitan DNS servers to enforce policies.

NOTE: This feature requires the "Technology" firmware version running on the Xirrus APs. You can select this option under *Settings / Firmware Upgrades.*

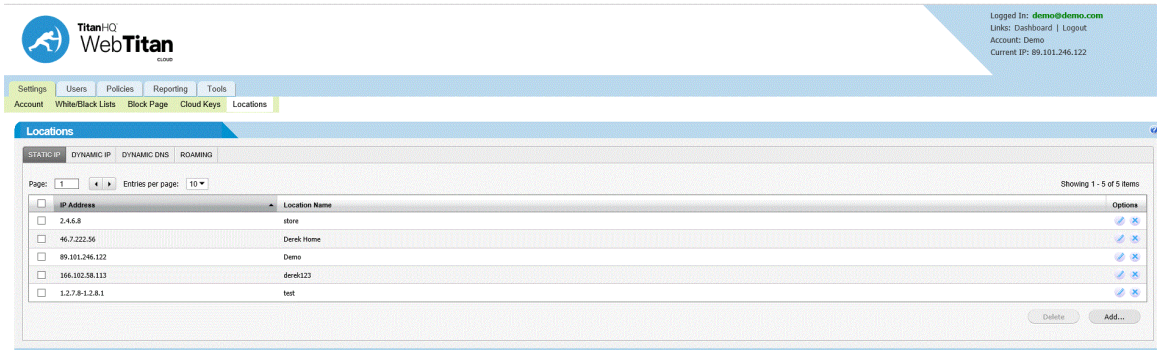
Before you start you need:

- Xirrus Wi-Fi network with "Technology" firmware on the APs
- Administrative access to XMS-Cloud (https://login.xirrus.com)
- WebTitan for Wi-Fi cloud account (Contact Derek Higgins at dhiggins@titanhq.com)

Simple Three-Step Process:

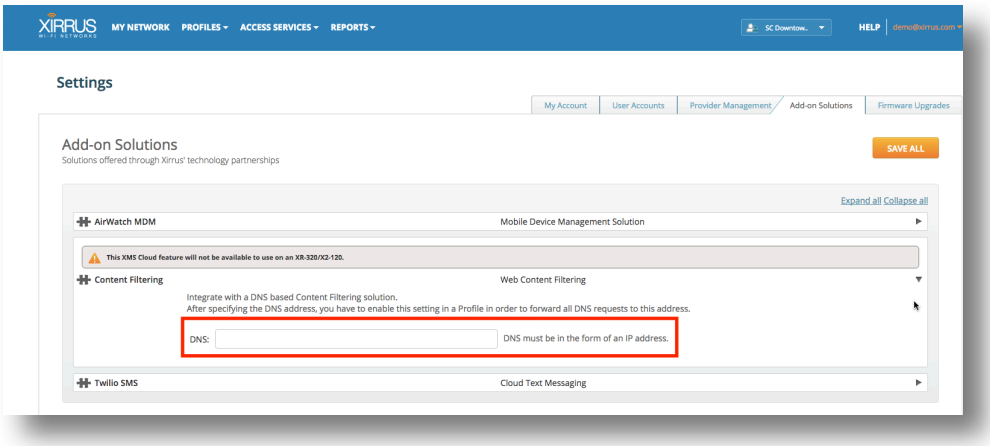
STEP 1: Configure WebTitan DNS servers

- Log into WebTitan Cloud
- Go to "*Settings*" > *"Locations"* & add external IP of customer site to be filtered
- Go to *"Policies"* tab, click *"edit"*, then configure policy



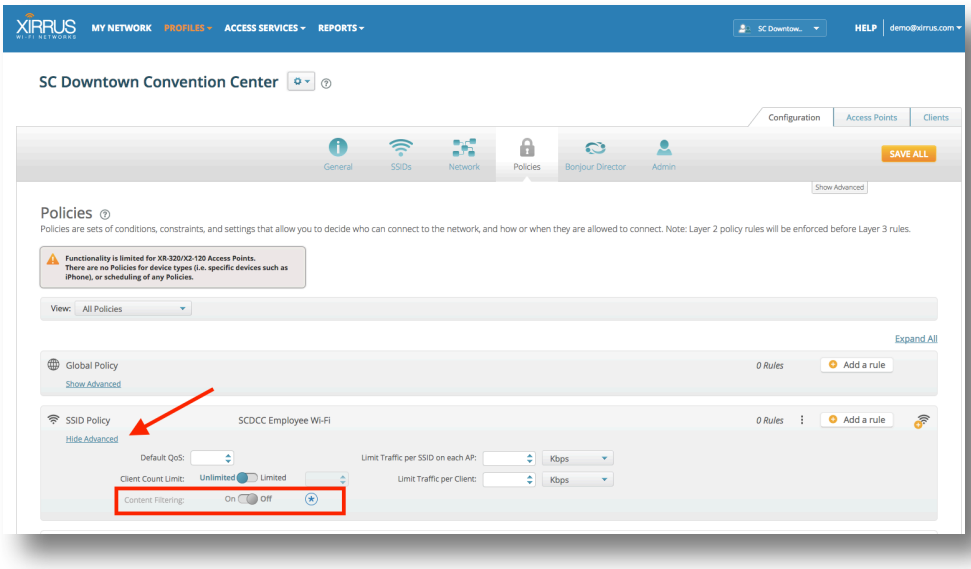
STEP 2: Configure XMS-Cloud

- Log into XMS-Cloud
- From the user name drop down menu at the top right corner of the dashboard, select "*Settings*". Configure the IP address of the WebTitan DNS server in the "*Add-on Solutions*" tab.



STEP 3: Enable Content Filtering on the Wi-Fi Network (SSID)

- Select the "*Profile*" hosting the SSID from the top-level menu. Choose the "*Policies*" tab and add a new SSID policy for the specific network. From the "*Show Advanced*" option under *SSID Policy*, turn on "*Content Filtering*".



- Save the configuration
- Congratulations your Wi-Fi content filtering is now live.

If you need assistance, contact Xirrus Support (support@xirrus.com), TitanHQ Support (webtitancloud@titanhq.com) or your channel partner.