ExtremeCloud Appliance Smart RF Reference Guide

Table of Contents

Preface

This section describes the text conventions used in this document, where you can find additional information, and how you can provide feedback to us.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as ExtremeSwitching switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
💡	Tip	Helpful tips and notices for using the product.
📒	Note	Useful information or instructions.
➡	Important	Important features or instructions.

Table 1: Notes and warnings (continued)

Icon	Notice type	Alerts you to...
⚠️	Caution	Risk of personal injury, system damage, or loss of data.
⚠️	Warning	Risk of severe personal injury.

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it appears on the screen.
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, $member[member...]$.
\	In command examples, the backslash indicates a "soft" line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation

Release Notes

Hardware/software compatibility matrices for Campus and Edge products

Supported transceivers and cables for Data Center products

Other resources, like white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit www.extremenetworks.com/education/.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form (all fields are required).

3. Select the products for which you would like to receive notifications.

> **Note**
> You can modify your product selections or unsubscribe at any time.

4. Select **Submit**.

Providing Feedback

The Information Development team at Extreme Networks has made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information in the document.
- Broken links or usability issues.

If you would like to provide feedback, you can do so in three ways:

- In a web browser, select the feedback icon and complete the online feedback form.
- Access the feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

About Smart RF in ExtremeCloud Appliance

Self Monitoring At Run Time RF Management (Smart RF) is an ExtremeWireless WiNG™ innovation designed to simplify RF configurations for new deployments, while providing on-going optimization as the RF environment changes over time.

Smart RF can reduce deployment costs by scanning the RF environment to determine the best channel and transmit power for each Smart RF-managed radio. Smart RF policies are added to device groups to apply site-specific deployment configurations and self-healing values to groups of access points (APs). Smart RF distributes the decision process between RF Domain Managers (in a Distributed site) or within the ExtremeCloud Appliance (in a Centralized Site). Data is used from the RF environment to make intelligent RF configuration decisions.

Figure 1: Benefits of Smart RF

Smart RF helps reduce ongoing management and maintenance costs by constantly monitoring the RF environment for external wireless interference, neighbor wireless interference, non-wireless interference, and client connectivity. Smart RF then applies various algorithms to arrive at the optimal channel and power selection for all APs in the network, and constantly reacts to changes in the RF environment. Smart RF is supported on all 802.11n/ac/ax access points with ExtremeCloud Appliance v4.76.x.
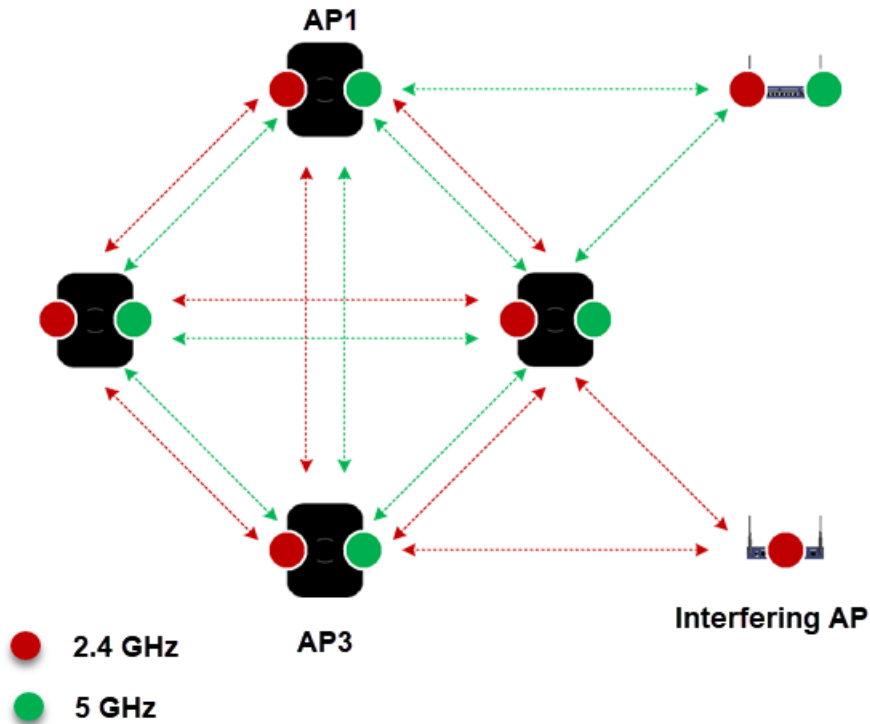
Off-Channel Scanning

Smart RF leverages the Off-Channel Scanning (OCS) capabilities built into each ExtremeWireless WiNG 802.11n/ac/ax AP to monitor the RF environment in real-time on both 2.4 GHz and 5 GHz bands. When Smart RF is enabled, by default, each Smart RF-managed radio will go off-channel for 50 milliseconds

every 6 seconds to monitor the RF environment for each channel. This is configurable. Over time, each radio is able to gain a full picture of the RF environment and learn:

- Neighboring APs
- Sources of Wi-Fi Interference
- Sources of Non-Wi-Fi Interference

Figure 2: Off-Channel Scanning

The RF environmental information is collected by each AP and forwarded to the elected RF Domain Manager or the ExtremeCloud Appliance who co-ordinates the channel and power decisions. Smart RF uses the RF environmental information to make intelligent power and channel changes as the RF environment evolves over time, and to initiate Neighbor Recovery, Interference Recovery, and Coverage Hole Recovery features.

Channel and Power Selection

The channels and power values assigned to the Smart RF-managed radios are dependent on the country code assigned to the site, the channel and power configuration defined in the Smart RF Policy, and whether the Smart RF Policy is enabled:

- If the Smart RF Policy assigned to the device group is enabled, the channel and power assigned to each Smart RF-managed radio is based on the channel and power values defined within the Smart RF Policy. The channel and power values are selected based on the neighbor AP placement and interfering devices.
- If the Smart RF Policy assigned to the device group is disabled, the assigned channels are randomly selected from the channel list defined within the Smart RF Policy. The assigned channels persist until the AP is rebooted or until the radios are disabled and re-enabled. The power of each radio is set to the highest permissible value.

Each channel and power parameter is fully configurable within the Smart RF Policy, enabling an administrator to tweak the system to suit their specific wireless deployment needs. For example, administrators can modify the Smart RF policy to exclude DFS channels or lower the minimum and maximum power values for high-density deployments. By default, Smart RF will assign radios a power value between 4 dBm and 17 dBm, a 20 MHz channel to each 2.4 GHz radio, and a 40 MHz channel to each 5 GHz radio.

Parameter	2.4GHz Radio Defaults	5GHz Radio Defaults
Min Power	4 dBm	4 dBm
Max Power	17 dBm	17 dBm
Channel Width	20 MHz	40 MHz
Channels	1,6,11	21,25,36,40,44,48,52,56,60,64,100,104,108, 112,116,120,124,128,132,136,140,149,153, 157,161,165,173

Figure 3: Channel and Power Defaults

Certain 5 GHz channels are subject to FCC / ETSI Dynamic Frequency Selection (DFS) regulations. If a Smart RF-enabled radio is on a channel subject to DFS, it will switch channels if radar is detected on the assigned 5 GHz channel.

Recovery Features

Smart RF supports self-healing features by monitoring the RF environment in real-time and provides automatic mitigation from potentially problematic events such as:

- neighbor interference
- non-Wi-Fi interference (noise)
- external Wi-Fi interference
- coverage holes
- radio failures

Smart RF employs self-healing to maintain wireless client performance and wireless coverage during dynamic RF environment changes that typically require manual intervention to resolve.

> **Note**
> The Smart RF recovery features are intended to provide a temporary measure until a permanent fix is applied.

For example, if a remote site is experiencing constant Coverage Hole Recovery events for wireless clients within a specific coverage area, the administrator will need to re-survey the area and determine if deploying an additional AP or different antennas can remediate the coverage problem. Likewise, if an AP in a coverage area fails or becomes faulty, the administrator will need to replace the failed AP to permanently remediate the problem.

With Interference Recovery, it is possible that the interfering APs are not owned or managed by the company or division. In this case, Smart RF will adjust the channels and power values on the Smart RF managed radios to provide the best possible RF environment around the interfering devices.

## Interference Recovery

Smart RF provides mitigation from wireless sources of interference by measuring noise and interference on the current channel of each Smart RF managed radio. When a noise threshold is exceeded, Smart RF can select an alternative channel for the Smart RF managed radio with less interference. To avoid channel flapping, a hold-timer is defined, which disables interference avoidance for a specific period of time upon detection. Interference Recovery is enabled by default.
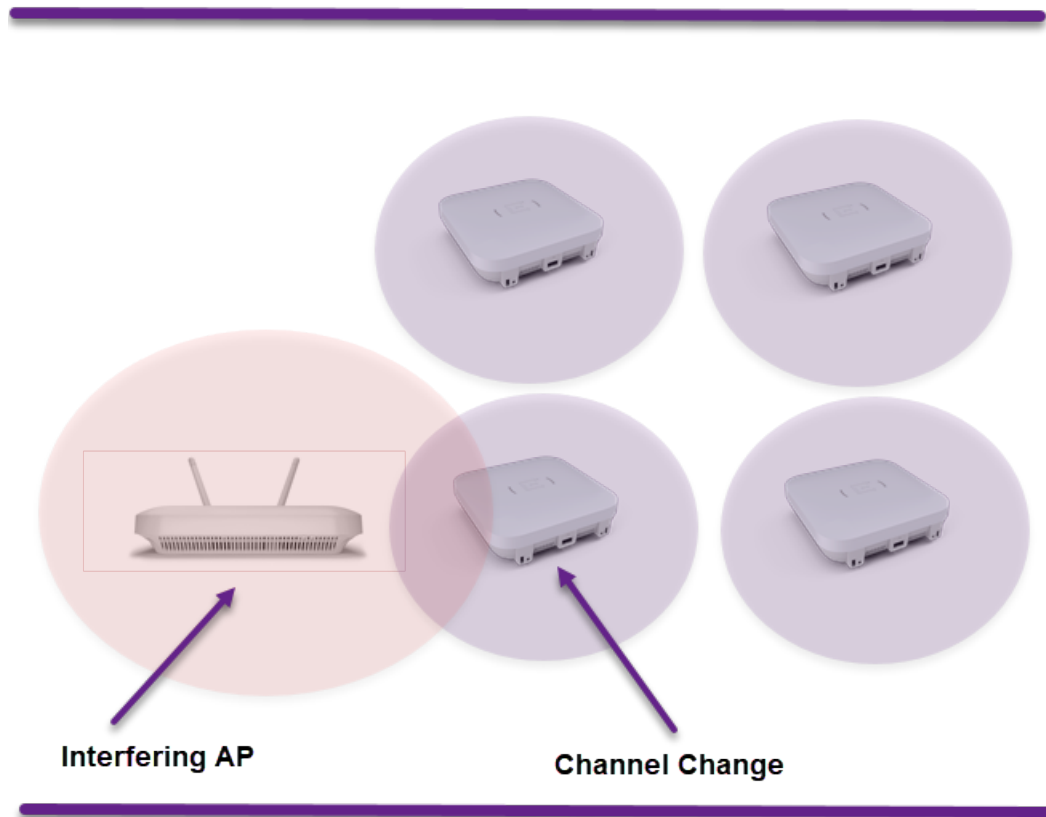
Figure 4: Interference Recovery

Neighbor Recovery

Smart RF provides automatic recovery for failed or faulty access points or faulty antennas by instructing neighboring APs to increase their transmit power to compensate for the coverage loss. Using Smart RF probes, each Smart RF-managed radio maintains an active list of neighboring Smart RF-managed radios. The list includes each neighbors' channel, power, and attenuation. If a neighboring Smart RF radio drops below a defined power threshold, one or more Smart RF-managed radios can increase their power to compensate for the coverage loss. Neighbor recovery is enabled by default and requires a minimum of four APs to function.
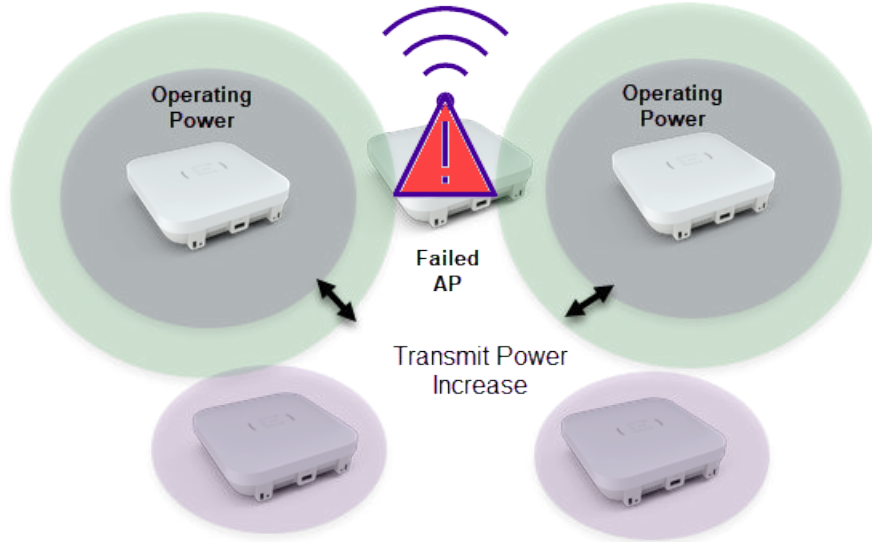
Figure 5: Neighbor Recovery

> **Note**
> A Smart RF managed radio will only change power if a power difference of +/-3 is necessary. The power adjustment can also be >3. For example, if a radio is operating at 10 and the Smart RF algorithm determines that the power needs to be 17, the Smart RF radio will increase power to 17 immediately. However, if the power must decrease, it will always decrease in increments of 3.

Coverage Hole Recovery

Smart RF provides mitigation for coverage issues for wireless clients located at the fringes of the network or in poor coverage areas. When a coverage hole is detected, Smart RF first determines the power compensation needed based on the signal to noise ratio (SNR) for a client as seen by the Smart RF-managed radio. If a client's signal to noise value is above the threshold, the transmit power is increased until the SNR falls below the threshold. Coverage Hole Recovery is enabled by default.
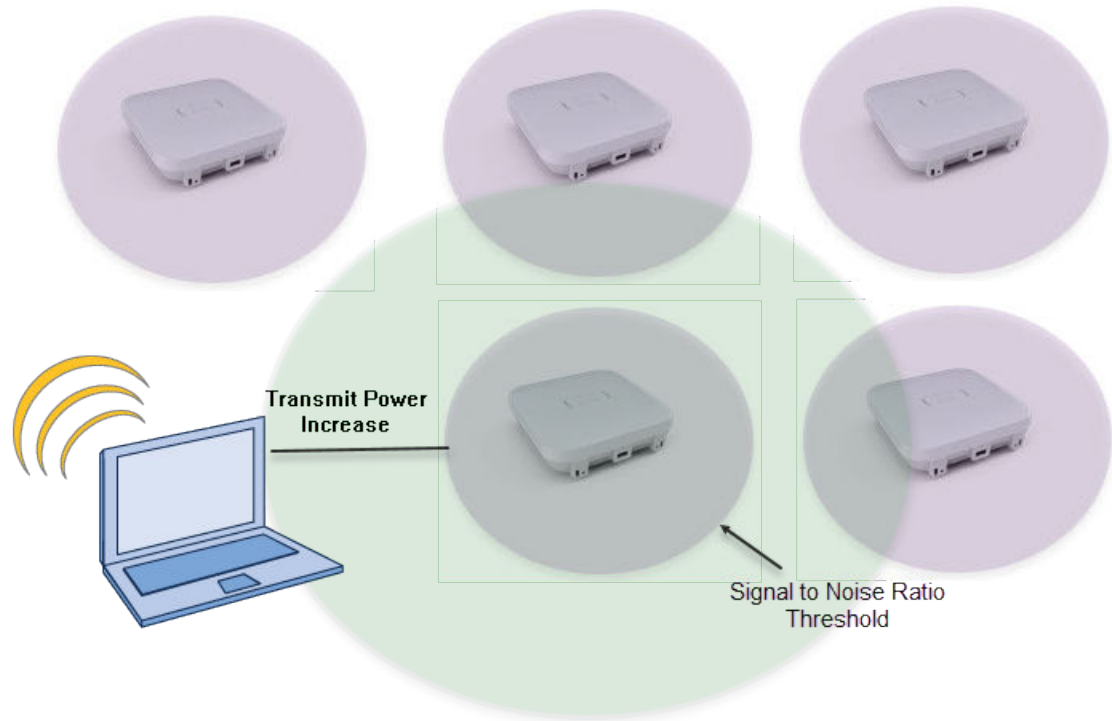
Figure 6: Coverage Hole Recovery

Smart RF Policy

Enabling Smart RF requires that you define a Smart RF Policy that is assigned to one or more device groups. By default, at the device group level, you configure each radio to use Smart RF for both channel and transmit power assignments.

Most ExtremeWireless WiNG deployments consist of a common Smart RF Policy that is assigned to each device group in the system. However, customers often define separate Smart RF Policies for stores, offices, and warehouses because APs are deployed differently in each environment, and the wireless clients will have different coverage and density requirements.

Create a Smart RF Policy using the ExtremeCloud Appliance user interface. Go to **Configure** > **Sites** > **Device Groups** > **RF Management** and add or edit the RF Management policy assigned to the device group.

> **Note**
> By default, the Smart RF Policy is assigned a **Medium** sensitivity value.

Basic Configuration

The **Basic Configuration** screen displays basic settings that determine the sensitivity, policy state, and Smart RF recovery features.

Figure 7: Basic tab

The Basic Settings parameters are used to determine the Off-Channel Scanning (OCS) aggressiveness used by Smart RF for monitoring and configuration. Changing the Smart RF Sensitivity modifies values in the **Scanning Configuration**, **Neighbor Recovery**, **Interference Recovery**, and **Coverage Hole Recovery** screens. A best practice is to use the default **Medium** Sensitivity. It has been proven to work well in retail, office, and warehouse environments. If customization is required, base your customizations on the **Medium** Sensitivity values.

The additional Basic Settings parameters determine if the Smart RF Policy is enabled and which Recovery features are enabled. Deciding which Recovery features to enable is determined by the AP placement and overlapping coverage provided at each site.

> **Note**
> Recovery features can operate correctly only if adequate coverage and overlap has been designed into the system. A site survey and proper deployment for Smart RF is required for Recovery to work correctly.

> **Note**
> If the Smart RF Policy is disabled but assigned to an RF Domain, the access point radio channels are assigned randomly from the defined channel settings in the **Channel and Power Configuration** screen. The transmit power for each radio is set to the maximum permitted value.

Channel and Power

The **Channel and Power** screen in the Smart RF Policy includes the following configuration sections:

- **Power Settings** – Determine the minimum and maximum transmit power values assigned to Smart RF managed radios.
- **Channel Settings** – Determine the pool of channels and channel widths assigned to the Smart RF managed radios.

Figure 8: Channel and Power tab

The Power Settings parameters determines the minimum and maximum power values (in dBm) that can be assigned to 2.4 GHz and 5 GHz Smart RF managed radios. By default, each 2.4 GHz and 5 GHz radio is assigned a transmit power value between 4 – 17 dBm, which can be configured by modifying the Minimum Power and Maximum Power parameters for each radio type.

> **Note**
> The power specified here is per chain.

As a general best practice, do not increase the Maximum Power values for the 2.4 GHz or 5 GHz radios beyond the default 17 dBm value. The default value has been defined to provide a 3 dBm margin for the Neighbor Recovery and Coverage Hole Recovery features. If each radio in the system is operating at a maximum of 20 dBm, the Smart RF managed radios will be unable to increase the transmit power if a neighboring AP fails or a coverage hole is detected.

> **Note**
> Only increase the Maximum Power values if the Neighbor Recovery and Coverage Hole Recovery features are disabled.

The Channel Settings parameters define the pool of channels that can be assigned to the 2.4 GHz and 5 GHz Smart RF-managed radios in addition to the channel width (20 MHz, 40 MHz, 80 MHz, or Auto). By default, the 2.4 GHz radios are assigned a 20 MHz wide channel, and the 5 GHz radios are assigned a 40 MHz wide channel.

> **Note**
> The 80 MHz wide channel is supported by the 802.11ac/ax radios only.

- **2.4 GHz Radios** – Smart RF will assign a 20 MHz wide channel (1, 6, or 11) to each Smart RF managed radio.
- **5 GHz Radios** – Smart RF will assign a permitted 40 MHz channel (21, 25, 36, 40, 44, 48, 52, 56, 60,64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, 165, or 173) to each Smart RF-managed radio.

A best practice is to use automatic Channel Width on the 5GHz band in low density deployments and 20MHz channel width in high density environments where channel reuse must be achieved.
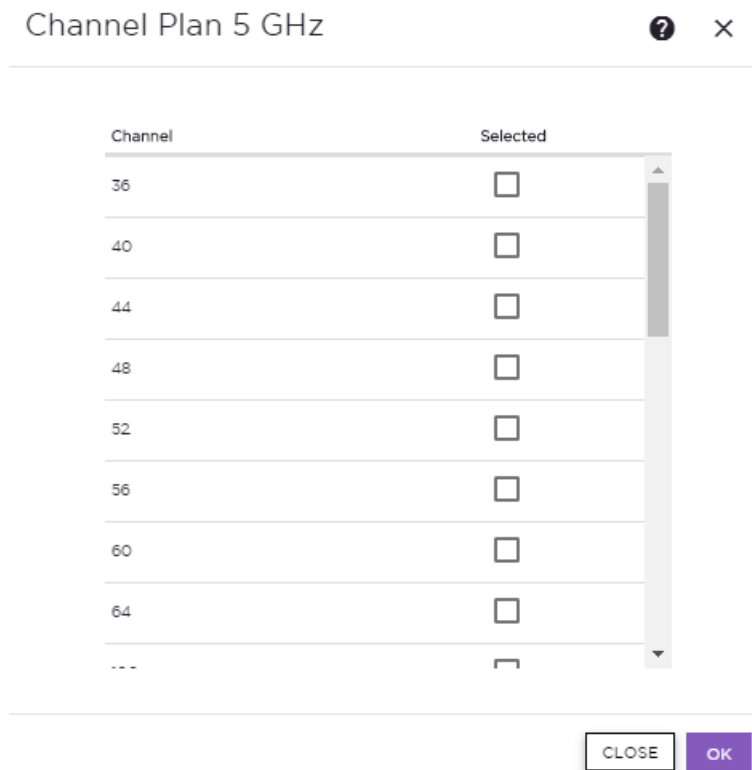
Figure 9: Channel Plan dialog
For 5 GHz Smart RF managed radios, consider removing channels from the available channel list. For example, consider removing channels subject to Dynamic Frequency Selection (DFS) to minimize the impact to wireless clients if a radar is detected. It may also be desirable to remove certain channels for voice handsets to optimize roaming or legacy 802.11a devices, which do not support the UNII2/2e high band.

Scanning Configuration

The **Scanning Configuration** screen in the Smart RF Policy includes the following configuration sections:

- **Monitoring Configuration** – Enables / disables Off-Channel Scanning (OCS) for Neighbor Recovery and Interference Recovery features.
- **Scanning Configuration** – Determines the frequency of Off-Channel Scanning (OCS), deciding which channels are scanned, and how Smart RF uses OCS when Voice or Power Save Poling wireless clients are detected.

The **Smart Monitoring Enable** parameter determines if Off-Channel Scanning (OCS) is enabled or disabled on the Smart RF managed radios. Enabled by default, this parameter allows Smart RF managed radios to monitor their coverage areas for the Neighbor Recovery and Interference Recovery features.

OCS Monitoring Awareness

Smart RF relies on Off-Channel Scanning (OCS) to monitor the RF environment in real-time, enabling the Smart RF-managed radios to adapt to changes in the RF environment in real-time. Smart RF-managed radios that go off-channel can impact certain devices; therefore, Smart RF is

adaptive. By default it prevents OCS on a Smart RF-managed radio if it detects an active voice call or if packets are queued for clients in Power Save (PS) dozing state.

Voice and PS awareness is set to dynamic mode by default. When in dynamic mode, a Smart RF-managed radio can avoid going off-channel when a voice call is in progress, or packets are queued for PS clients. You can also set Voice or PS awareness to strict mode. Strict mode prevents OCS when a Voice or PS wireless client is associated to a Smart RF-managed radio. Additionally, to prevent OCS, you can define a Client Aware Scanning threshold for 2.4 GHz and 5 GHz radios to determine the number of associated wireless clients on a given Smart RF-managed radio.

If the deployment includes wireless devices that support PS or Voice, some Smart RF-managed radios may not be able to go off-channel for an extended period of time, which means those radios may not have the current interference or neighbor data.

Scanning Configuration (2.4GHz and 5GHz)

The Scanning Configuration determines the Off-Channel Scanning (OCS) configuration parameters assigned to the 2.4 GHz and 5 GHz Smart RF managed radios. The values for the Frequency, Extended Scan, and Sample Count are assigned automatically to the most optimum values based on the Sensitivity value selected in the **Basic Configuration** screen. These values can also be modified when setting the Sensitivity value to **Custom**.

The Client Aware Scanning parameter can also be optionally enabled to determine a threshold for the number of associated wireless clients on a Smart RF managed radio before it avoids going off-channel.

The Duration, Frequency, Extended Scan Frequency, and Sample count values determine how often and for how long Smart RF managed radios go off-channel, and how much data is recorded. The following figure provides a detailed overview of each OCS parameter:

Parameter	Description
Duration	The amount of time in milliseconds Smart RF managed radios remain off-channel when they perform a scan. The default setting is 50 milliseconds for both the 2.4 GHz and 5 GHz radios.
Frequency	The frequency in which Smart RF managed radios change channels for an off-channel scan. The default setting is 6 seconds when a Medium Sensitivity is selected.
Extended Scan Frequency	Smart RF will perform an off-channel scan of a single channel every 6 seconds with a total of 10 off-channel scans in a one-minute period. Every nth time (extended-scan-frequency value) the Smart RF managed radio will perform an extended scan of the environment as a whole, including outside noise factors. The default is 5 when a Medium Sensitivity is selected.
Sample Count	The number of samples each Smart RF managed radio takes before reporting XCA. The default is 5 samples for the 5 GHz radios and 10 samples for the 2.4 GHz radios when a Medium Sensitivity is selected.

Figure 10: Off-Channel Scanning (OCS) parameters

> **Note**
> Calculate how long it takes each Smart RF managed radio to report to the elected RF Domain Manager by using the following formula:
>
> FREQUENCY x SAMPLE-COUNT x NUM-CHANNELS
>
> For example, a 2.4 GHz radio will take 180 seconds (6 x 10 x 3 = 180).

Power Save Aware Scanning

The Power Save Aware Scanning parameter allows Smart RF managed radios to detect wireless clients in power-save mode and take them into consideration when performing off-channel scans. By default, each Smart RF managed radio is set to **Dynamic**, and each radio will consider wireless clients in a Power Save (PS) state and may postpone the off-channel scan until the wireless client awakens at the DTIM interval. If set to **Strict**, the Smart RF-managed radios do not perform an off-channel scan when a wireless client in Power Save state is detected.

This parameter may be set to **Strict** in an environment where off-channel scanning may interfere with the DTIM and clients waking to receive data. For example, warehouse environments related to logistics and shipping where there may be hundreds of hand-held devices scanning thousands of packages in a given shift. These clients alternate between power-save mode and awake mode constantly; therefore, it would be beneficial to set the Power Save Aware Scanning mode to **Strict**.

Voice Aware Scanning

As with Power Save Aware Scanning, Voice Aware Scanning allows Smart RF managed radios to delay off-channel scanning when Voice clients are present on the network. In a mixed client environment, the default setting of **Dynamic** is sufficient. However, if a Wireless LAN is dedicated to Voice, set Voice Aware Scanning to **Strict**.

Figure 11: RF Management Scanning tab

Related Topics

> Basic Configuration on page 14

Recovery

The **Recovery** screen in the Smart RF Policy includes the following configuration sections:

- **Neighbor Recovery** – Determines the hold-time, thresholds, and sampling values for the Neighbor Recovery feature.

- **Interference Recovery** – Determines the noise factor, thresholds, hold-times, and deltas for the Interference Recovery feature.

- **Coverage Hole Recovery** – Determines the thresholds and intervals for the Coverage Hole Recovery feature.

Edit RF Management Policy

Name   Default Smart RF

BASIC   CHANNEL AND POWER   SCANNING   RECOVERY   SELECT SHUTDOWN

NEIGHBOR RECOVERY   INTERFERENCE RECOVERY

Hold Time

Power Hold Time   0   Seconds

Neighbor Recovery

2.4 GHz Neighbor Power Threshold   -70   dBm

5 GHz Neighbor Power Threshold   -70   dBm

Dynamic Sample Recovery

Dynamic Sample Enabled   ☐

Figure 12: Neighbor Recovery settings

Hold Time

> The **Power Hold Time** parameter determines the time in seconds that a Smart RF- managed radio waits between two power changes. By default, the Power Hold Time parameter value is set to **0** (disabled) when the Sensitivity is set to **Medium** on the **Basic Configuration** screen. The value can be modified when the Sensitivity is set to **Custom** on the **Basic Configuration** screen.

Neighbor Recovery

> The **Neighbor Power Threshold** parameters determine the maximum power increase threshold used by each Smart RF managed radio if the radio is required to increase its power to compensate for a failed neighbor. By default, the Neighbor Thresholds for both 2.4 GHz and 5 GHz radios is set to -70 dBm when the Sensitivity is set to **Medium** in the **Basic Configuration** screen. These values can be modified when the Sensitivity is set to **Custom**.

> Optimal radio power settings are derived by determining the attenuation of all Smart RF neighbors for a given radio. A Smart RF probe is transmitted by each Smart RF-managed radio, and then the RSSI (Received Signal Strength Indicator) of each neighbor response is sent to ExtremeCloud Appliance. Based on Off-Channel Scanning (OCS) Sample Count in the **Scanning and Configuration** screen, an average RSSI for each neighbor is determined from the overall attenuation of the neighbors. The attenuation plus power threshold is the power setting. If a neighbor attenuation is calculated at 80, and the threshold is set to -70, the radio power will be set to `10 (80 +(-70) = 10)`.

In environments that have excessive obstructions where neighboring radios may not be heard as well, the Power Threshold may be lowered (example -65) in order to arrive at a better overall power setting.

Dynamic Sample Recovery

The **Dynamic Sampling Recovery** parameter enables an administrator to define how Smart RF adjustments are triggered by locking retry and threshold values. This parameter is disabled by default. Select **Dynamic Sample Enabled** to enable this setting.

When Dynamic Sampling is enabled, the Smart RF managed radios perform extra sampling to avoid excessive power changes. The Smart RF-managed radios keep track of the number of samples that were processed without a power change. If a power change has not occurred in a while and the Dynamic Sample Threshold has been exceeded, the Smart RF Managed radio can perform a power change immediately. If a power change has occurred recently and another power changed is required (within the Dynamic Sample Threshold), the Smart RF-managed radio sends additional samples to see if the power change is still required. The power is changed only after confirming that it is required. Configure the number of retries in the **Dynamic Sample Retries** field.

Interference Recovery

The Interference Recovery feature performs channel changes when noise from neighboring wireless devices or outside interference is detected and the delta between the current channel energy and the perceived energy from other signals falls below a threshold. The **Channel Hold Time**, **Client Threshold**, and **Channel Switch Delta** parameters are automatically assigned the optimum values based on the Sensitivity value selected in the **Basic Configuration** screen. These values can also be modified when setting the Sensitivity value to **Custom**.

Figure 14 provides a detailed overview of each Interference Recovery parameter, which can be defined for both 2.4 GHz and 5 GHz Smart RF managed radios.

Figure 13: Interference Recovery tab

Parameter	Description
Channel Hold Time	The minimum amount between two channel changes due to interference on a Smart RF managed radio. The default is 30 minutes when a Medium Sensitivity is selected.
Client Threshold	The number of wireless clients for which a Smart RF managed radio will not perform a channel change due to interference. The default is 50 clients when a Medium Sensitivity is selected.
2.4 GHz Channel Switch Delta	The minimum expected between the perceived energy on the 2.4 GHz radios current channel compared to that of the best possible alternate channel. The default is 20 dBm when a Medium Sensitivity is selected.
5 GHz Channel Switch Delta	The minimum expected between the perceived energy on the 5 GHz radios current channel compared to that of the best possible alternate channel. The default is 20 dBm when a Medium Sensitivity is selected.

Figure 14: Interference Recovery parameters

Coverage Hole Recovery

The Coverage Hole feature performs power changes when wireless device connectivity falls below a defined SNR threshold. The **Client Threshold**, **SNR Threshold**, **Coverage Interval**, and **Interval** parameters are automatically assigned the optimum values based on the Sensitivity value selected

in the **Basic Configuration** screen. These values can also be modified when setting the Sensitivity value to **Custom**.

Figure 15 provides a detailed overview of each important Coverage Hole Recovery parameter, which can be defined for both 2.4 GHz and 5 GHz Smart RF managed radios:

Parameter	Description
Client Threshold	Defines the number of wireless clients detected that fall below the SNR threshold before recovery takes place. The default is 1 client when a Medium Sensitivity is selected. This setting can be modified as it may not be desirable to adjust power every time a single wireless client falls before the defined SNR threshold.
SNR Threshold	Defines the minimum signal-to-noise ratio heard from the wireless client before recovery takes place. The default is 20 dB when a Medium Sensitivity is selected. As a best practice is it never recommended to set the SNR below 20 dB. When wireless clients are detected below the defined SNR, recovery will take place.
Coverage Interval	Defines the interval coverage hole recovery should be initiated by a Smart RF managed radio when a coverage hole is detected. The default is 10 seconds when a Medium Sensitivity is selected. When a coverage hole has been detected and recovery is taking place, the detection becomes more aggressive in determining if the coverage hole still exists.
Interval	Defines the interval in which coverage hole detection takes place by a Smart RF managed radio. The default is 30 seconds when a Medium Sensitivity is selected. Note that this interval may need to be lowered in environments such as warehouses where coverage is critical (i.e. low cell count, large cell size).

Figure 15: Coverage Hole Recovery parameters

Related Topics

Basic Configuration on page 14

Select Shutdown

The **Select Shutdown** feature is used to reduce the Co-Channel Interference (CCI) on 2.4 GHz radios in deployments that were designed for 5 GHz. Such deployments are too dense for the number of 2.4 GHz radios. Therefore, radios can be safely shut down to reduce the CCI. The CCI High/Low thresholds, Frequency, and Frequency Limiter are set to optimum values based on the Sensitivity value selected in the **Basic Configuration** screen. This feature is disabled by default.

Edit RF Management Policy

Default Smart RF

BASIC   CHANNEL AND POWER   SCANNING   RECOVERY   SELECT SHUTDOWN

Enable	☐	
CCI High Threshold	-80	dBm
CCI Low Threshold	-100	dBm
Frequency	60	minutes
Frequency Limiter	10	multiples

Figure 16: Select Shutdown settings

Parameter	Description
Enable	Enables/Disables the Select Shutdown algorithm
CCI High Threshold	Threshold that determines when the Select Shutdown algorithm will start to hide 2.4 GHz radios
CCI Low Threshold	Threshold that determines when the Select Shutdown algorithm will start to unhide 2.4 GHz radios
Frequency	How often the Select Shutdown algorithm runs
Frequency Limiter	Limits the Frequency value, preventing the Frequency value from becoming too fast compared to the OCS Frequency.

Figure 17: Select Shutdown parameters

Related Topics
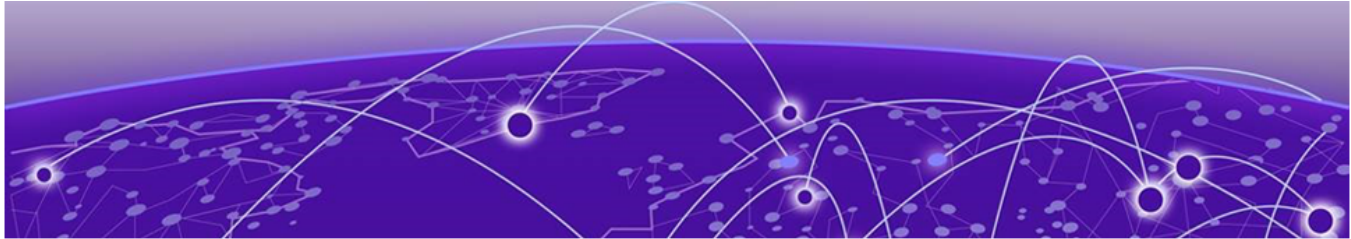
RF Domain

Smart RF Policies are assigned to radios at the device group level. Each device group is configured with one Smart RF Policy. Use the ExtremeCloud Appliance user interface to assign a Smart RF Policy to a device group:

1. Go to **Configure** > **Sites** > **Device Groups**.
2. Select a device group or select **Add**.
3. Select **RF Management**.

Figure 18: RF Management on Device Group tab

Verification and Troubleshooting

Smart RF charts are available in ExtremeCloud Appliance to help verify successful Smart RF functionality and to assist in troubleshooting.

1. Go to **Monitor** > **Devices** > **Access Points**.
2. Select an AP, and then select the **Smart RF** tab.

Related Topics

Channel and Power Assignments

You can view Channel and power values for Smart RF managed radios per site in real-time from the ExtremeCloud Appliance user interface.

1. Go to **Monitor** > **Devices** > **Access Points**.
2. Select an AP, and then select the **Smart RF** tab.

By default, each radio is configured to be Smart RF managed and counts toward the Smart RF totals. All radios that are not managed by Smart RF are either ACS (for legacy ExtremeWireless APs) or STATIC RF for statically configured channel and power.
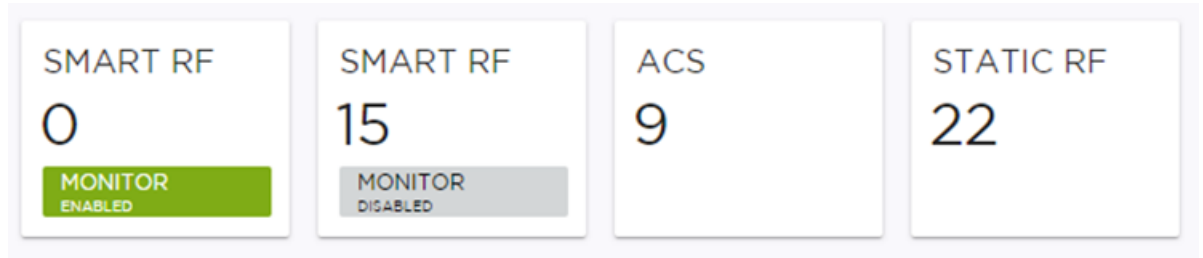
Figure 19: Channel and Power statistics in ExtremeCloud Appliance

Channel and Power Distribution

2.4 GHz and 5 GHz channel distribution for Smart RF-managed radios can be viewed in real-time per site using the ExtremeCloud Appliance user interface. The channel distribution statistics are useful for ensuring that the 2.4 GHz and 5 GHz channels are evenly distributed throughout the site. However, depending on the number of APs and the RF environment (interference or noise), equal distribution is not always possible.

Interfering Access Points

A list of Neighbor and Interfering access points can be view per AP in real-time using the ExtremeCloud Appliance user interface:

1. Go to **Monitor** > **Devices** > **Access Points**.
2. Select an AP, and then select the **Smart RF** tab.

Each Smart RF managed radio captures the MAC address, Channel, and RSSI of each neighbor or interfering wireless AP that the selected AP sees. The Neighbor List can be useful when trying to resolve RF issues. The following information is available:

- Name
- BSSID (MAC)
- SSID
- Type
- Radio Index
- Last Seen
- Power (dBm)
- Attenuation (dB)
- Channel
- Channel Width (MHz)

Neighbor List

Name	BSSID(MAC)	SSID	Type	Radio Index	Last Seen
	00:D7:8F:B4:7C:91		External	0	1586462494
	D8:84:66:84:FD:D0		External	1	1586462494
	48:9B:D5:EE:0C:72		External	1	1586462132
	48:9B:D5:ED:F2:D1		External	1	1586461650
	20:6C:8A:06:0E:E0		External	1	1586458760
	20:9E:F7:4C:FA:B3		External	1	1586462494
	00:42:68:13:AC:CE		External	1	1586461650
	5C:0E:8C:FF:10:D0		External	1	1586459723
	00:6B:F1:68:12:40		External	0	1586462494

Figure 20: Neighbor List

Energy Graphs

Each Smart RF managed radio maintains an energy graph, which is used for channel and power assignments as well as for Interference Recovery. The energy graph can be displayed per Smart RF managed radio using the ExtremeCloud Appliance user interface.

1. Go to **Monitor** > **Devices** > **Access Points**.
2. Select an AP, and then select the **Smart RF** tab.

Each radio energy graph displays the External Noise, Neighbor Noise, and Total energy for each channel.
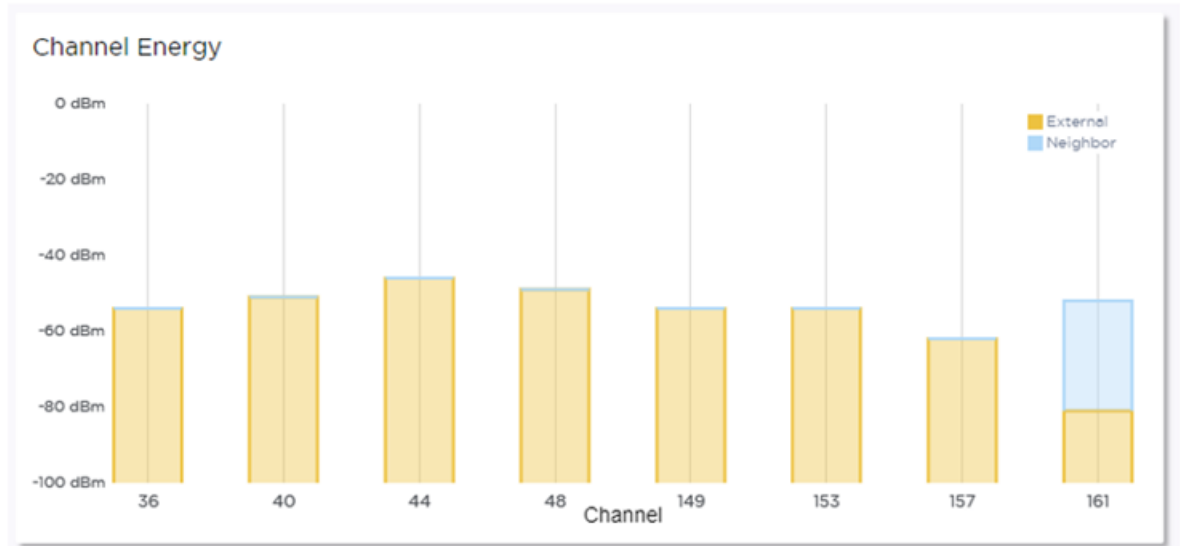
Figure 21: Channel Energy Graph per AP

Smart RF History

ExtremeCloud Appliance maintains a history of all Smart RF events that can be displayed in real-time using the ExtremeCloud Appliance user interface. Go to **Tools** > **Logs** > **AP Logs**.

The Smart RF History includes all Smart RF related events including:

- radios being added
- channel and power changes
- Neighbor Recovery, Interference Recovery, and Coverage Hole Recovery events.

View these events from the **AP Logs** tab.

Figure 22: Smart RF History from AP Logs

Index

B

Basic settings 14

C

Channel and Power assignments 27
Channel and Power Distribution 28
channel and power selection 9
Channel and Power settings 15
conventions
    notice icons 4
    text 4
Coverage Hole Recovery 12

D

documentation
    feedback 7
    location 6

E

Energy Graphs 29

F

feedback 7

I

Interference Recovery 11
Interfering Access Points 28

N

Neighbor Recovery 11
notices 4

O

OCS Off-Channel Scanning 8
Off-Channel Scanning 8

R

recovery features 10
Recovery settings 20
RF Domain 26

S

Scanning Configuration 17
Select Shutdown settings 24
self-healing RF environment 10
Smart RF 8
Smart RF History 30
Smart RF Policy
    Basic settings 14
    Channel and Power settings 15
    Recovery settings 20
    Scanning Configuration 17
    Select Shutdown settings 24
support, *see* technical support

T

technical support
    contacting 6

V

verification and troubleshooting Smart RF 27

W

warnings 4