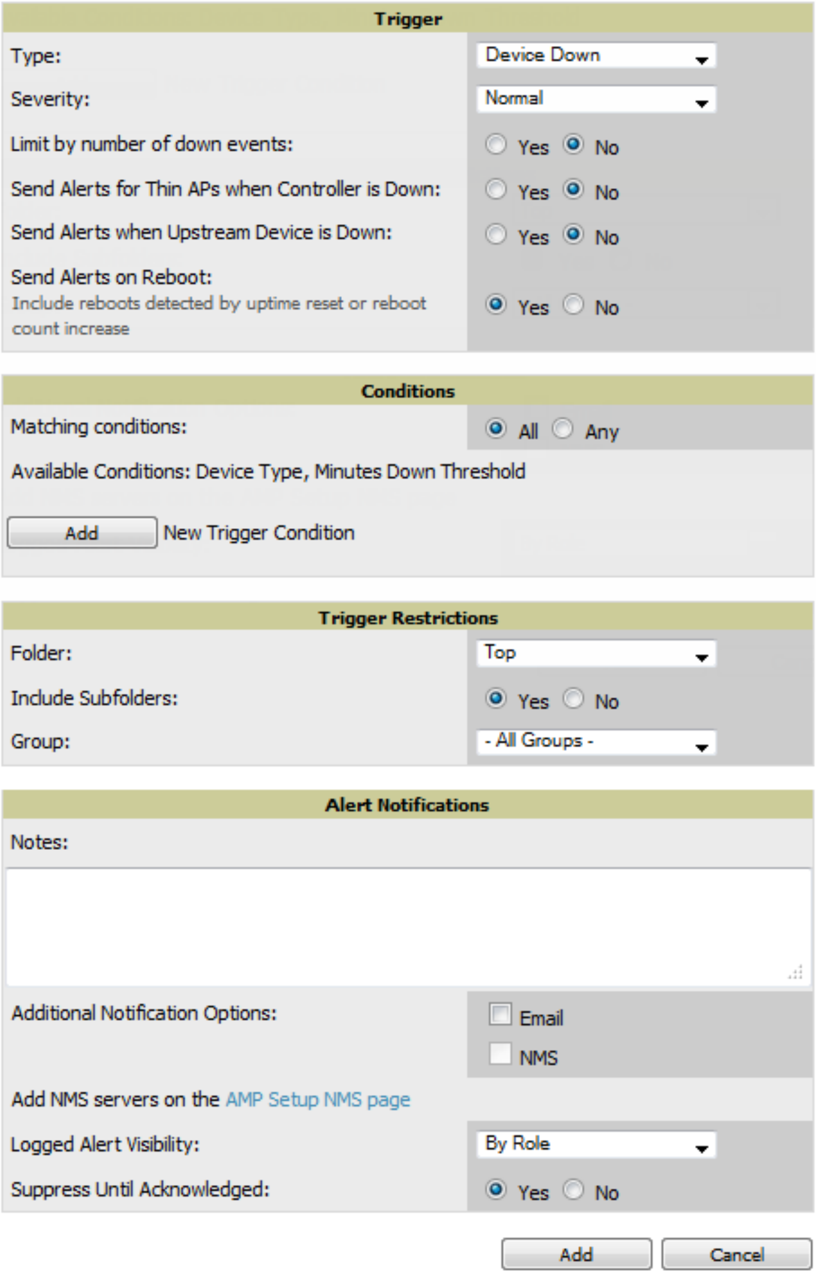
Creating New Triggers

Perform the following steps to create and configure one or more new triggers. These steps define settings that are required for any type of trigger.

1. To create a new trigger, select the **Add New Trigger** button from the **System > Triggers** page. The page that appears is illustrated in Figure 1.

Figure 1 ***Add New Trigger*** *Page Illustration*



Trigger

Type:	Device Down
Severity:	Normal
Limit by number of down events:	○ Yes ● No
Send Alerts for Thin APs when Controller is Down:	○ Yes ● No
Send Alerts when Upstream Device is Down:	○ Yes ● No
Send Alerts on Reboot: Include reboots detected by uptime reset or reboot count increase	● Yes ○ No

Conditions

Matching conditions:	● All ○ Any

Available Conditions: Device Type, Minutes Down Threshold

Add New Trigger Condition

Trigger Restrictions

Folder:	Top
Include Subfolders:	● Yes ○ No
Group:	- All Groups -

Alert Notifications

Notes:

Additional Notification Options:	□ Email □ NMS

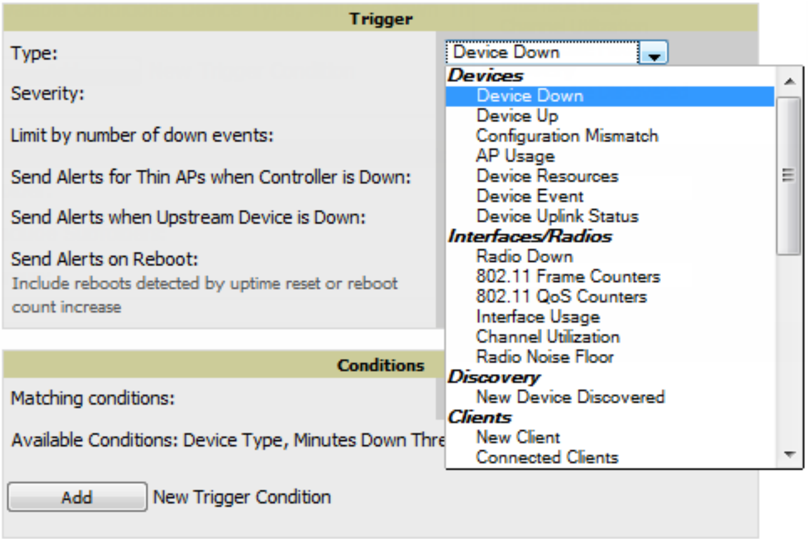
Add NMS servers on the AMP Setup NMS page

Logged Alert Visibility:	By Role
Suppress Until Acknowledged:	● Yes ○ No

2. In the **Trigger** section, choose the desired trigger **Type** and **Severity**. Figure 2 illustrates some of the supported trigger types.

> The alert summary information at the top of the AMP screen can be configured to separately display severe alerts. Refer to Configuring Your Own User Information with the Home > User Info Page for more details.

Figure 2 ***System > Triggers > Add Trigger Type*** *Drop Down Menu*



Trigger

Type: Device Down

Severity:

Limit by number of down events:

Send Alerts for Thin APs when Controller is Down:

Send Alerts when Upstream Device is Down:

Send Alerts on Reboot:
Include reboots detected by uptime reset or reboot count increase

Conditions

Matching conditions:

Available Conditions: Device Type, Minutes Down Thre

The **Add Trigger** page changes depending on the trigger type that you select. In many cases, you must configure at least one **Condition** setting. Conditions, settings and default values vary according to trigger type. Triggers with conditions can be configured to fire if any criteria match as well as if all criteria match.

- Some trigger types share common settings, such as **Duration** (which can be expressed in hours, minutes, seconds, or a combination of these) and **Severity** (from Normal to Critical).
- After you select **Save**, the trigger appears on your next viewing of the **System > Triggers** page with all other active triggers.
- You can edit or delete any trigger as desired from the **System > Triggers** page.
  - To edit an existing trigger, select the **pencil** icon next to the respective trigger and edit settings in the **Trigger Detail** page described in Table 2.
  - To delete a trigger, check the box next to the trigger to remove, and select **Delete**.

3. Configure the **Trigger Restrictions** and **Alert Notifications**. This configuration is consistent regardless of the trigger type to be defined.
   a. The **Trigger Restrictions** settings establishes how widely or how narrowly the trigger applies. Define the folder, subfolder, and Group covered by this trigger. Table 1 describes the options for trigger restrictions.

Table 1: ***System*** > ***Trigger Restrictions*** *Fields and Default Values*

Notification Option	Description
Folder	Sets the trigger to apply only to APs/Devices in the specified folder or subfolders depending on the **Include Subfolders** option. **NOTE:** If the trigger is restricted by folder and group, it only applies to the intersection of the two—it only applies to APs in the group and in the folder.
Include Subfolders	Sets the trigger to apply to all devices in the specified folder and all of the devices in folders under the specified folder.
Group	Sets the trigger to apply only to APs/Devices in the specified group. **NOTE:** If the trigger is restricted by folder and group, it only applies to the intersection of the two—it only applies to APs in the group and in the folder.

   b. The **Alert Notifications** settings section allows you to enter a note that will be included with the alert. This note will appear with the alert on the **System > Alerts** page. The **Alert Notification** section also allows you to specify whether the alert will be distributed via email, to a network management system (NMS), or to both.
      - If you select **Email**, you are prompted to set the sender and recipient email addresses.
      - If you select **NMS**, you are prompted to choose one or more of the pre-defined trap destinations, which are configured on the **AMP Setup >NMS** page. Note that this option is only available if an NMS server has been added to AMP.
      - Define the **Logged Alert Visibility**, in which you can choose how this trigger is distributed. The trigger can distribute according to how is it generated (triggering agent), or by the role with which it is associated.
      - The **Suppress Until Acknowledged** setting defines whether the trigger requires manual and administrative acknowledgement to gain visibility. If **No**, a new alert will be created every time the trigger criteria are met. If **Yes**, an alert will only be received the first time the criteria is met. A new alert for the device is not created until the initial one is acknowledged.

Repeat this procedure for as many triggers and conditions as desired.

Complete the creation of your trigger type using one of the following procedures for each trigger:

- Setting Triggers for Devices
- Setting Triggers for Interfaces and Radios
- Setting Triggers for Discovery
- Setting Triggers for Clients
- Setting Triggers for RADIUS Authentication Issues
- Setting Triggers for IDS Events
- Setting Triggers for AMP Health

Setting Triggers for Devices

Perform the following steps to configure device-related triggers.

a. Choose a device type from the **Devices** listed in the **Type** drop-down menu. See Figure 2. Table 2 itemizes and describes device trigger options and condition settings.

Table 2: ***Device*** *Trigger Types*

Device Down	This is the default type whenever configuring a new trigger. This type of trigger activates when an authorized, monitored AP has failed to respond to SNMP queries from AMP. To set the conditions for this trigger type, select **Add** in the **Conditions** section. Complete the conditions with the **Option**, **Condition**, and **Value** drop-down menus. The conditions establish the device type. Multiple conditions can apply to this type of trigger. The Device Down trigger can be configured to send alerts for thin APs when the controller is down; this behavior is turned off by default. Triggers with the **Minutes Down** condition enabled will compare the amount of time an AP has been down to the value (in minutes) set for the condition. When the **Limit by number of down events** is enabled, you can set the number of down events that activate the trigger, as well as the duration of the time window to be measured. AMP will then count the number of times that the device has gone from Up to Down in the specified span of time and display this in the Device Down alert.
Device Up	This trigger type activates when an authorized, previously down AP is now responding to SNMP queries. To set the conditions for this trigger type, select **Add** in the **Conditions** section.
Configuration Mismatch	This trigger type activates when the actual configuration on the AP does not match the defined **Group** configuration policy. To set the conditions for this trigger type, select **Add** in the **Conditions** section.
AP Usage	Activates when the total bandwidth through the device has exceeded a predefined threshold for more than a specified period (such as more than 1500 Kbps for more than 120 seconds). You can also select bandwidth direction and page/radio. Selecting this type displays the following new fields in the **Type** section. Define these settings. ● **Alert if AP Usage >= (Kbps)**—This threshold establishes a device-specific bandwidth policy, not a bandwidth policy on the network as a whole. ● **Usage Direction**—Choose In, Out, or Combined. This bandwidth is monitored on the device itself, not on the network as a whole. ● **Severity** - Specify the severity type for the trigger. ● **Duration** - Specify the time frame for the trigger.
Device Resources	This type of trigger indicates that the CPU or memory utilization for a device (including router or switch) has exceeded a defined percentage for a specified period of time.
Device Event	This trigger is used for alerting based on SNMP traps and syslog messages, which are displayed in **System > Syslogs & Traps**, **APs/Devices > Monitor** for affected devices, and in **Clients > Client Detail.** The conditions supported are: ● **Event Contents** (case insensitive substring matches on message content) ● **Event Type** (syslog or trap) ● **Syslog Severity**: Emergency, Alert, Critical, Bug, Error, Warning, Notice, or Info ● Syslog Category ● **SNMP Trap Category**: Hardware, IDS, Client Security, AP Security, AP Status, Software, or Rogue Detection ● **Syslog Category** **NOTE:** During the process of upgrading or installation for non-Master Console/Failover AMPs, AMP creates two default trigger definitions for Device Events: ● SNMP Trap Category of **Hardware** or **Software**

	● Event Type is **Syslog** and **Syslog Severity** >= **Critical**
Device Uplink Status	This trigger deploys whenever a RAP's active uplink changes from Ethernet to USB or vice versa. The corresponding events are captured in a RAP's **APs/Devices > Monitor** page.

b. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of Creating New Triggers to create a new trigger.

Setting Triggers for Interfaces and Radios

To configure radio- and interface-related triggers, choose a trigger type from the **Interfaces/ Radios** category, listed in the **Type** drop-down menu. Table 3 itemizes and describes the radio trigger types and condition settings.

Table 3: *Interfaces/Radio-Related Trigger Types*

Radio Trigger Options	**Description**
Radio Down	Indicates that a device's radio is down on the network. Once you choose this trigger type, select **Add New Trigger Condition** to create at least one condition. **This type** requires that a radio capability be set as a condition. The **Value** drop-down menu supports several condition options.
802.11 Frame Counters	Enables monitoring of traffic levels. There are multiple rate-related parameters for which you define conditions including ACK Failures, Retry Rate, and Rx Fragment Rate. See the **Option** drop-down menu in the **Conditions** section of the trigger page for a complete list of parameters. Select **Add New Trigger Condition** to access these settings. Define at least one condition for this trigger type.
802.11 QoS Counters	Enables monitoring of Quality of Service (QoS) parameters on the network, according to traffic type. The rate of different parameters includes ACK Failures, Duplicated Frames and Transmitted Fragments. See the drop-down field menu in the conditions section of the trigger page for a complete list of parameters. Select **Add New Trigger Condition** to access these settings. Define at least one condition for this trigger type.
Interface Usage	Interface labels defined on the trigger page will be used to set up triggers on one or more interfaces and/or radios. Available conditions are **Device Type**, **Interface Description**, **Interface Label**, **Interface Mode**, **Interface Speed In (Mbps)**, **Interface Speed Out (Mbps)**, **Interface Type**, and **Radio Type**.
Channel Utilization	Indicates that channel utilization has crossed particular thresholds. Available conditions are **Interference (%)**, **Radio Type**, **Time Busy (%)**, **Time Receiving (%)**, and **Time Transmitting (%)**.
Radio Noise Floor	Indicates that the Noise Floor dBM has exceeded a certain value for aspecified period of time.

Setting Triggers for Discovery

Perform the following steps to configure triggers related to device discovery.

a. Choose a trigger type from the **Discovery** category, listed in the **Type** drop-down menu. See Figure 2.

Table 4: *Discovery Trigger Types and Condition Settings*

Discovery Trigger Options	**Description**
New Device Discovered	This trigger type flags the discovery of a new AP, router, or switch connected to the network (an device that AMP can monitor and configure). Once you choose this trigger type, select **Add New Trigger Condition** to specify a **Device Type** (Access Point, Controller, Remote AP, or Router/Switch)

b. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of Creating New Triggers to create a new trigger.

Setting Triggers for Clients

Perform the following steps to configure user-related triggers.

a. Choose a trigger type from the **Clients** category, listed in the **Type** drop-down menu. See Figure 2. Table 5 itemizes and describes the Client-related trigger types, and condition settings for each discovery trigger type.

Table 5: *Client Trigger Types and Condition Settings*

Client Trigger Option	Description
New Client	This trigger type indicates a new user has associated to a device within a defined set of groups or folders. A Filter on connection mode field appears to allow you to filter by **Wired** or **Wireless** clients. Note that the **New Client** trigger type does not require the configuration of any condition settings, so the **Condition** section disappears.
Connected Clients	This trigger type indicates a device (based on an input list of MAC addresses) has associated to the wireless network. It is required to define one or more MAC addresses with the field that appears.
Client Count	Activates when a device, Radio/Interface, or BSSID reaches a user-count threshold for more than a specified period (such as more than 10 users associated for more than 60 seconds).
Client Usage	This trigger type indicates that the sustained rate of bandwidth used by an individual user has exceeded a predefined threshold for more than a specified period, in seconds (such as more than 1500 Kbps for more than 120 seconds). Once you choose this trigger type, select **Add New Trigger Condition** to specify the bandwidth characteristics that triggers an alert. You can apply multiple conditions to this type of trigger. The **Value** field requires that you input a numerical figure for kilobits per second (Kbps).
New VPN User	This trigger type indicates a new VPN user has associated to a device within a defined set of groups or folders. Note that the **New VPN User** trigger type does not require the configuration of any condition settings, so the **Condition** section disappears.
Connected VPN Users	This trigger type indicates a VPN device (based on an input list of MAC addresses) has associated to the VPN network. It is required to define one or more VPN usernames with the field that appears.
VPN Session Usage	This trigger type indicates that the sustained rate of bandwidth used in an individual VPN session has exceeded a predefined threshold for more than a specified period, in seconds (such as more than 1500 Kbps for more than 120 seconds). Once you choose this trigger type, select **Add New Trigger Condition** to specify the bandwidth characteristics that triggers an alert. You can apply multiple conditions to this type of trigger. The **Value** field requires that you input a numerical figure for kilobits per second (Kbps).
Inactive Tag	This trigger type flags events in which an RFID tag has not been reported back to AMP by a controller for more than a certain number of hours. This trigger can be used to help identify inventory that might be lost or stolen. Set the time duration for this trigger type if not already completed.
IPv4 Link-Local Addresses	When enabled, this trigger checks whether the total count of self-assigned IP addresses has crossed a set threshold for clients within a selected folder or group. The alert deployed by this trigger includes a link to search for IP addresses containing 169.254.x.x.
Client Goodput	This trigger type indicates that the goodput for an individual client has exceeded a predefined threshold. Available conditions are Usage Kbps (combined), Usage Kbps (in), and Usage Kbps (out).
Client Speed	This trigger type indicates that the speed for an individual client has exceeded a predefined threshold. The available condition for this trigger is Speed Mbps.

b. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of Creating New Triggers to create a new trigger.

Setting Triggers for RADIUS Authentication Issues

Perform the following steps to configure RADIUS-related triggers.

a. Choose a trigger type from the **RADIUS Authentication Issues** list in the drop-down **Type** menu. Table 6 itemizes and describes the condition settings for each **RADIUS Authentication** trigger type.

Table 6: *RADIUS Authentication Trigger Types and Condition Settings*

	Description
Client RADIUS Authentication Issues	This trigger type sets the threshold for the maximum number of failures before an alert is issued for a user. Select **Add New Trigger Condition** to specify the count characteristics that trigger an alert. The **Option**, **Condition**, and **Value** fields allow you to define the numeric value of user issues.
Device RADIUS Authentication Issues	This trigger type sets the threshold for the maximum number of failures before an alert is issued for a device. The **Option**, **Condition**, and **Value** fields allow you to define the numeric value of user issues.
Total RADIUS Authentication Issues	This trigger sets the threshold for the maximum number of failures before an alert is issued for both users and devices.

b. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of Creating New Triggers to create a new trigger.

Setting Triggers for IDS Events

Perform the following steps to configure Intrusion Detection System (IDS)-related triggers.

a. Choose the **Device IDS Events** trigger type from the drop-down **Type** menu. See Figure 2. Table 7 describes condition settings for this trigger type.

Table 7: ***Device IDS Events Authentication*** *Trigger Types and Condition Settings*

IDS Trigger Options	**Description**
Device IDS Events	This trigger type is based on the number of IDS events has exceeded the threshold specified as Count in the Condition within the period of time specified in seconds in Duration. Alerts can also be generated for traps based on name, category or severity. Select **Add New Trigger Condition**to specify the count characteristics that trigger an IDS alert.
Rogue Device Classified	This trigger type indicates that a device has been discovered with the specified Rogue Score. Ad-hoc devices can be excluded automatically from this trigger by selecting **Yes**. See Using RAPIDS and Rogue Classification for more information on score definitions and discovery methods. Once you choose this trigger type, select **Add New Trigger Condition** to create one or more conditions. A condition for this trigger enables you to specify the nature of the rogue device in multiple ways.
Client on Rogue AP	This trigger type indicates that a client has associated to a rogue AP. Available conditions include rogue classification, and whether the client is valid.

b. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of Creating New Triggers to create a new trigger.

Setting Triggers for AMP Health

After completing steps 1-3 in Creating New Triggers, perform the following steps to configure IDS-related triggers.

a. Choose the **Disk Usage** trigger type from the drop-down **Type** menu. See Figure 2 for trigger types. Table 8 describes the condition settings for this trigger type.

Table 8: *Disk Usage Trigger and Condition Settings*

AMP Health Trigger	**Description**
Disk Usage	This trigger type is based on the disk usage of AMP. This type of trigger indicates that disk usage for the AMP server has met or surpassed a defined threshold. Select **Add New Trigger Condition** to specify the disk usage characteristics that trigger an alert.

AMP Health Trigger	Description
	Set one of these triggers at **90%** so you receive a warning before AMP suffers performance degradation due to lack of disk space.

b. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of Creating New Triggers to create a new trigger.