Overview

This document describes AirWave's alert/trap workflow when integrating with a centralized NMS Event Correlation System, using the following topics:

- "Adding NMS Event Correlation Servers to AirWave" on page 1
- "Configuring Alerts/Traps in AirWave" on page 2
- "Viewing Alerts in Various Destinations" on page 2
- "Acknowledging Alerts" on page 3
- "Compiling the AirWave MIB on NMS" on page 3
- "Matching Severity in the NMS Event Correlation Servers" on page 4
- "Enhanced Integration" on page 4
- "Actual MIB" on page 4

Adding NMS Event Correlation Servers to AirWave

To add a event correlation server to the AirWave Management Platform (AMP):

- 1. Navigate to AMP Setup > NMS and click Add.
- 2. Configure server settings.

Figure 1 AMP Setup > NMS Page Illustration

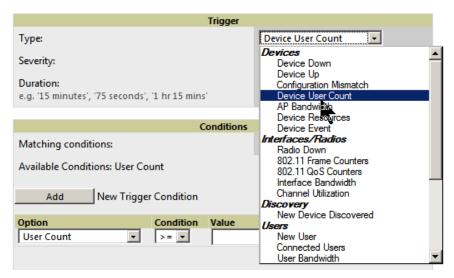
NMS Integration	
AMP can send SNMP traps to NMS servers. First, add one or more NMS servers below, then select <i>NMS</i> as a notification option for triggers. The <i>Sync</i> action will send one trap for each device managed by AMP to inform an NMS of each one's up/down and configuration status.	
Download the AMP MIB files.	
NMS Server	
Hostname:	
Port (1-65535):	162
Community String:	
Confirm Community String:	
SNMP Version:	2c 💌
Enabled:	⊙ Yes ○ No
Send Configuration Traps:	⊙ γ _{es} ⊙ No
	Add Cancel

0511042-02 | Aug 2012

Configuring Alerts/Traps in AirWave

- 1. Navigate to Systems > Triggers, as shown in Figure 2.
- 2. Select one of the built-in Alerts/Traps.
- 3. Click Add.

Figure 2 Configuring a Device Count Trigger



Configure properties for the Alert/Trap

- Thresholds for the alert (quantity and time)
- Severity of alert
- Distribution options
- Notification Method
 - Sender
 - Recipient
 - NMS sends SNMP traps
- Alert Suppression

Viewing Alerts in Various Destinations

As seen on the System > Alerts page of the AirWave console:

Figure 3 System > Alerts Page Illustration



As seen in email from the recipient's perspective:

Figure 4 Email recipient of an alert

Cc:
Subject: AMP Alert: AP User Count

AP User Count >= 2 users for 60 seconds
Severity: Critical
Time: Thu Dec 21 09:01:51 2006

Device: HQ-BoardRoom - https://demo.airwave.com/ap_monitoring?id=11276
Group: Acme Corp - IT
Folder: Top
Location: Board Room Wall

As seen by the NMS server via a topdump of the actual alert:

Device User Count

10:32:52.964243 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto 17, length: 284) demo.airwave.com.38979 > airwave-openvie.snmptrap: [bad udp cksum ebf4!] { SNMPv2c C=foo { V2Trap(242) R=47680 system.sysUpTime.0=10 S:1.1.4.1.0=E:12028.4.15.0.3 E:12028.4.15.1.101=2 E:12028.4.15.1.102=4 E:12028.4.15.1.103="Device: HQ-Engineering - https://demo.airwave.com/ap_monitoringid=11277: AP User Count >= 2 users for 60 seconds" E:12028.4.104=10.2.26.164 }}

Device Down

10:32:23.055999 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto 17, length: 261) demo.airwave.com.38934 > airwave-openvie.snmptrap: [bad udp cksum e740!] { SNMPv2c C=foo { V2Trap(219) R=47676 system.sysUpTime.0=10 S:1.1.4.1.0=E:12028.4.15.0.13 E:12028.4.15.1.101=2 E:12028.4.15.1.102=4 E:12028.4.15.1.103="Device: Aruba-AP65-ap.2.2.3 - https://demo.airwave.com/ap_monitoringid=11797: Device Down " E:12028.4.104=10.51.3.46 }}

OID Breakdown

12028.4.15.1.102 contains Severity Code

- 2 = Normal
- 3 = Warning
- 4 = Minor
- 5 = Major
- 6 = Critical

12028.4.15.1.103 contains several fields separated by colons

- Object Type {Client, AirWave, Device/AP, Group)
- Object Name and URL (the URL is optional, if it exist then it will be separated by a dash "-"}
- Trap Description and Evaluation Elements

12028.4.15.1.104 contains device IP Address

Group Traps will contain AirWave's IP address.

Acknowledging Alerts

AirWave alerts must be manually acknowledge from the **System > Alert** page. AirWave does not currently provide an external interface to acknowledge alerts from an NMS server.

Compiling the AirWave MIB on NMS

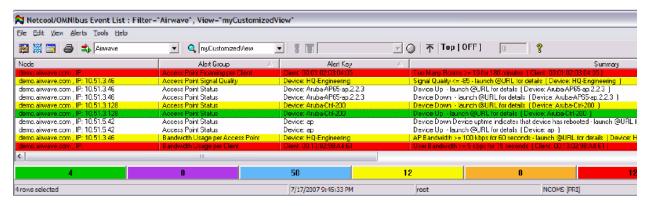
- 1. Navigate to AMP Setup > NMS.
- 2. Click on the **Download** link.
- 3. Transfer to NMS server.

4. Compile on NMS server.

Matching Severity in the NMS Event Correlation Servers

Most NMS Event Correlation systems have the ability to color code and esclate based on information received in the trap, as shown in Figure 5. The OID 12028.4.15.1.102 contians the AirWave severity code.

Figure 5 Color Codes



Enhanced Integration

AirWave has enhanced integration modules with several NMS Event Correlation Systems. These integrations provide enhanced functionality like quicklink porblem diagnostics, configuration, and WLAN topology views.

- IBM Netcool navigate to https://www-304.ibm.com/software/brandcatalog/ismlibrary/ details?catalog.label=1TW10NC16 to download the certified NetCool NIM
- ProCurve Manager Navigate to AMP Setup > NMS and click on the HP ProCurve Manager section to obtain additional information.
- HP OpenView NNM Contact Dell Support at support.dell.com for additional information.

Actual MIB



NOTE: Traps in grey text are unused.

```
*************************
awampEventID OBJECT-TYPE
      SYNTAX INTEGER
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
          "Random number AMP assigns to the event."
   ::= { awampEventObject 101 ]
awampEventSeverityCode OBJECT-TYPE
SYNTAX INTEGER
      MAX-ACCESS read-only
       STATUS current
      DESCRIPTION
          "Level 1-6'
   ::= { awampEventObject 102 }
awampEventDescription OBJECT-TYPE
      SYNTAX DisplayString
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
          "Concatenated String produced from AMP."
   ::= { awampEventObject 103 }
```

```
awampEventAPIPOId OBJECT-TYPE
              SYNTAX IpAddress
MAX-ACCESS read-only
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Old IP of the AP when AMP changes and sends trap to HPOV."
::= { awampEventObject 104 }
awampEventAPMngURL OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
              STATUS current
DESCRIPTION
                      "URL to manage AP on AMP from HPOV."
"URL to manage AP on AMP from HPUV."

::= { awampEventObject 105 }

awampEventAPMonURL OBJECT-TYPE

SYNTAX DisplayString

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"URL to monitor AP on AMP from HPOV."

::= { awampEventObject 106 }

awampEventGroupModURL OR JECT-TYPE
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"URL to monitor Group on AMP from HPOV."
::= { awampEventObject 108 }
awampEventAPICON OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
               STATUS current
              DESCRIPTION
    "Name of ICON to display on HPOV screen"
::= { awampEventObject 109 }
-- * Fault Traps generated by the AMP
-- * (1.3.6.1.4.12028.4.15.0.)
 tooManyDevAssocAMP NOTIFICATION-TYPE
  OBJECTS { awampEventID,
awampEventSeverityCode,
              awampEventDescription }
    STATUS current
DESCRIPTION
 "This trap is sent when too many devices are simultaneously associated with AMP for a period of time."
::= { awampEventPrefix 1 }
tooManyDevAssocGroup NOTIFICATION-TYPE
  OBJECTS { awampEventID,
              awampEventSeverityCode,
              awampEventDescription }
    STATUS current
DESCRIPTION
 "This trap is sent when too many devices are simultaneously associated with AMP for a period of time." := { awampEventPrefix 2 }
 tooManyDevAssocAp NOTIFICATION-TYPE
  OBJECTS { awampEventID,
              awampEventSeverityCode,
    awampEventDescription,
awampAPIP}
STATUS current
DESCRIPTION
  "This trap is sent when too many devices are associated
  simultaneously associated with AP for a period of time.
    ::= { awampEventPrefix 3 }
 toomuchBWAMP NOTIFICATION-TYPE OBJECTS { awampEventID,
              awampEventSeverityCode,
              awampEventDescription }
    STATUS current
    DESCRIPTION
  "This trap is sent when there is too much BW being
```

```
used on the WLAN for a period of time."
  ::= { awampEventPrefix 4 }
toomuchBWGroup NOTIFICATION-TYPE
 OBJECTS { awampEventID,
         awampEventSeverityCode,
          awampEventDescription }
  STATUS current
  DESCRIPTION
 "This trap is sent when there is too much BW being
used by a Group for a period of time.'
   ::= { awampEventPrefix 5 }
toomuchBWAP NOTIFICATION-TYPE
 OBJECTS { awampEventID,
          awampEventSeverityCode,
          awampEventDescription,
  awampAPIP }
STATUS current
DESCRIPTION
"This trap is sent when there is too much BW being used on an AP for a period of time."
  ::= { awampEventPrefix 6 }
toomuchBWClient NOTIFICATION-TYPE
OBJECTS { awampEventID,
          awampEventSeverityCode,
  awampEventDescription }
STATUS current
DESCRIPTION
 "This trap is sent when there is too much BW being
used by a Client for a period of time.'
  ::= { awampEventPrefix 7 }
toomanyRoamsClient NOTIFICATION-TYPE OBJECTS { awampEventID,
         awampEventSeverityCode, awampEventDescription }
  STATUS current
DESCRIPTION
 "This trap is sent when Client roams too often from
 AP to AP for a period of time.
  ::= { awampEventPrefix 8 }
poorSignalAP NOTIFICATION-TYPE OBJECTS { awampEventID,
         awampEventSeverityCode,
awampEventDescription,
          awampAPIP }
  STATUS current
  DESCRIPTION
 "This trap is sent when an AP has poor Signal
quality for a period of time.
   ::= { awampEventPrefix 9 }
nonAMPAPChange NOTIFICATION-TYPE
OBJECTS { awampEventID,
          awampEventSeverityCode,
   awampEventDescription, awampAPIP }
  STATUS current
DESCRIPTION
"This trap is sent when an AP Changes configuration without the AMP knowledge"
  ::= { awampEventPrefix 10 }
unauthenticatedClient NOTIFICATION-TYPE OBJECTS { awampEventID,
          awampEventSeverityCode,
          awampEventDescription }
  STATUS current
  DESCRIPTION
 "This trap is sent when Client is associated with
WLAN for a period of time without authenticating."
:= { awampEventPrefix 11 }
rogueAPDetected NOTIFICATION-TYPE
 OBJECTS { awampEventID,
          awampEventSeverityCode,
          awampEventDescription }
   STATUS current
  DESCRIPTION
 "This trap is sent when the AMP discovers a Rogue
AP."
  ::= { awampEventPrefix 12 }
downAP NOTIFICATION-TYPE
OBJECTS { awampEventID,
```

Copyright

All rights reserved. Specifications in this manual are subject to change without notice.

Originated in the USA. All other trademarks are the property of their respective owners.

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg, et al. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.