

# Application Visibility & Control How-To Guide



© 2015 ZIH Corp. All Rights Reserved.

Zebra and the Stylized Zebra Head are trademarks of ZIH Corp, registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners.

## Table of Contents

1. Introduction .....	4
1.1 Features and Benefits .....	5
1.2 Application Recognition .....	5
1.3 Viewing the applications .....	6
1.4 Application Control: .....	6
2. Deployment Scenarios .....	7
2.1 Traffic Flow .....	7
2.2 AVC Enforced at the controller .....	8
2.3 AVC enforced on the Access Points .....	8
3. Configuration .....	9
3.1 Enable Deep Packet Inspection (DPI) .....	9
3.2 Create an Application Policy .....	10
3.3 Assign the Application Policy .....	14
3.4 NSight Integration .....	15
3.5 User Defined Application .....	15
4. Validation .....	18
4.1 NSight GUI .....	18
4.2 Dashboard .....	19
4.3 WiNG UI Statistics .....	22
4.4 WiNG CLI Statistic .....	23
4.5 Log Messages .....	24
5. Appendix .....	25
5.1 Supported Platforms .....	25
5.2 Scaling .....	25
5.3 Performance impact .....	25
5.4 Licensing: .....	25

## 1. Introduction

With the advent of BYOD, you can see all kind of devices and applications being used on the enterprise wireless networks. Some of these applications can be bandwidth intensive like gaming applications or *youtube* videos. These applications compete with the enterprise applications for bandwidth. The organizations first want to have visibility on all the applications being used on their wireless networks - the usage patterns, the bandwidth consumption. Once they have this visibility the organizations want to control how the applications use the wireless network so that it is in line with their investment objectives. They may want to prioritize business critical applications while throttling other applications or altogether blocking some applications.

The WiNG devices already support some features to identify and allow or block applications with static signatures. With the WiNG 5.8 release, the Zebra WLAN devices support the **Application Visibility and Control** feature that can be used to identify thousands of applications based on their signatures and enforce fine grained control on how the applications access the wireless network.

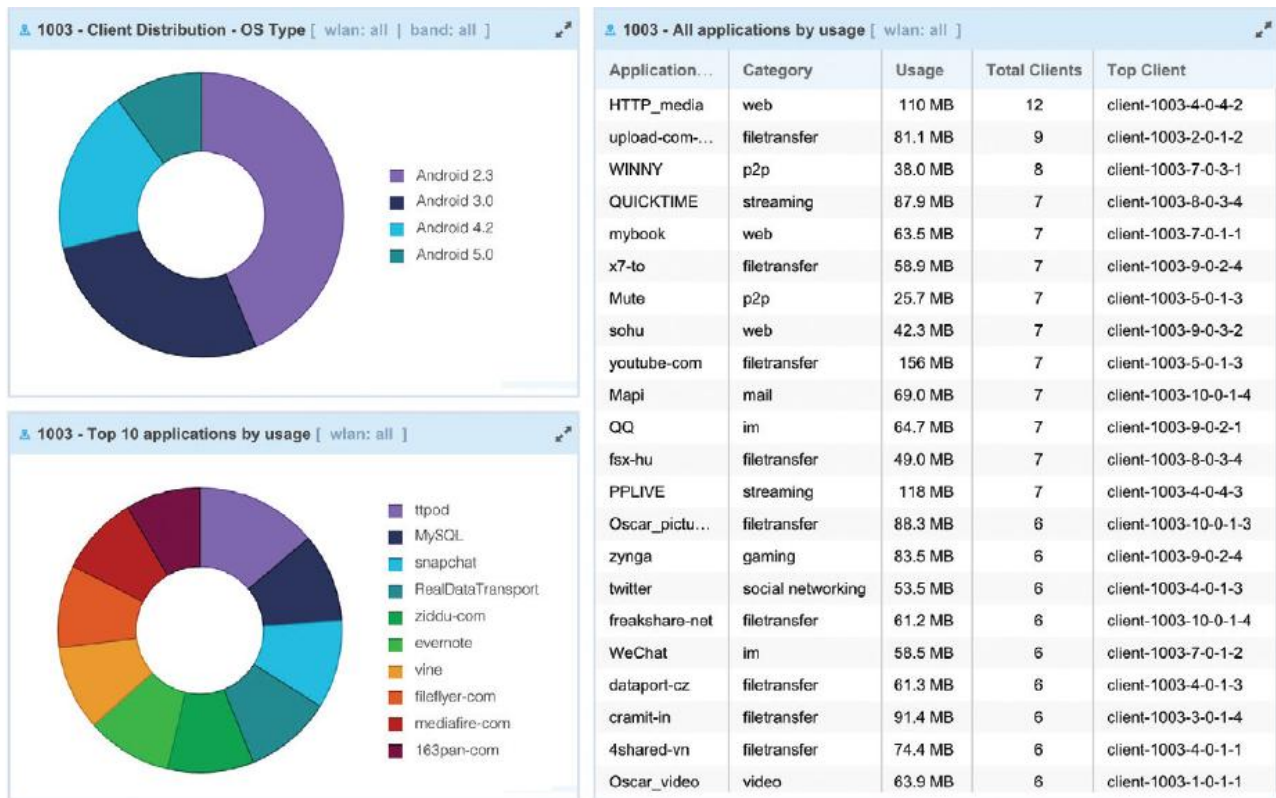


Figure 1-1: Application Visibility and Control Statistics

## 1.1 Features and Benefits

With a simple click, the administrators can view the top applications being used on the wireless network based on the client count or bandwidth usage. This can be viewed at each site level or the entire deployment. The same information can also be viewed for each AP or each client.

The feature provides tool to the **IT Administrators** that helps them get answers to the following questions:

- What are the Top 10 applications by bandwidth consumption and usage ?
- How can I prioritize critical enterprise applications like Salesforce.com, Lync over bandwidth intensive non-critical applications like Youtube or Netflix ?
- Can I block certain applications or put bandwidth limits on them ?

## 1.2 Application Recognition

The Zebra WiNG devices employ various mechanisms to identify applications and to enforce them to the corporate policies. Some applications may be easy to identify while some use dynamic signatures and difficult to identify with traditional methods of identifying the application based on the port and protocol combination.

1. **IP Access Control Lists (ACL):** The previous WiNG releases can make use of **IP ACLS** to identify applications or traffic flow. IP ACLS rules are based on the **source and destination IP address, Protocol and port number** in the **IP headers**. If a matching traffic is found, the traffic can be Allowed, Dropped, or prioritized or de-prioritized based on the configured rules. It's easy to identify applications like FTP, Ping which use the fixed port and protocol combination.

**Limitation:** The drawback with this mechanism is that it may be cumbersome for the network administrators to create the right rules, or the application may be using dynamic signatures with changing port numbers. Also, many applications use the well known ports like 80 and 443 in which case it is not possible to create rules to identify individual applications.

2. **Deep Packet Inspection (DPI):** The AVC feature introduced in WiNG 5.8 supports Deep Packet Inspection, whereby the AP or the controller not only inspects the IP headers, but also looks into the application payload to identify the application signatures. A wide range of applications in different categories like Gaming, Peer to Peer (P2P), Social media, etc can be identified.

The DPI engine can be run on controllers or the access points on any of the supported platforms (section 5.1).

3. **HTTP Properties:** When communicating over HTTP or HTTPS, an application can be identified based on a URL match or the HTTPS server name.

**URL List:** You can create a URL list and define a rule to take an action if any URL in the list or URLs is matched.

**HTTPS Server Name:** You can select an application based on attributes from the HTTP message exchanges. Currently, the match can be done based on the HTTPS server name.

Please see section 3.5 for more details on making a Application match based on HTTP properties.

## 1.3 Viewing the applications

The identified applications can be viewed on the WiNG Flex UI or NSight.

### Zebra NSight

Zebra NSight is the advanced management platform that is used to monitor and troubleshoot the entire wireless network centrally. The Access points send periodic statistics to the NSight server which are stored on the NSight database for real time and historical analysis.

The AVC feature is integrated with the *Zebra NSight* platform and the AVC applications and statistics can be viewed on the *Zebra NSight* server. As shown in **figure 1**, the NSight View shows the details on all applications and application categories being used on the wireless networks. You can visually identify the top 10 applications or you can see detailed statistics on the application. Like the number of users accessing the application, total bandwidth being consumed by that application, etc.

### Flexible Scope:

This information can be viewed for each client device or collated to get the usage for all client devices connected to an Access point. It can also be viewed for an entire site or the complete wireless network across multiple sites.

### WiNG Flex UI

The AVC statistics can also be viewed on the WiNG5 UI. But the statistics can only be seen for upto the last 24 hours. The AVC engine resets once every day and the statistics database is built afresh. For users that need to view the historical data can access it from the Zebra NSight Server.

## 1.4 Application Control:

Once the Application traffic is identified and the usage pattern is examined, the administrators may then decide on the kind of controls that must be subjected to the various applications. They may define the rules to enforce their security and IT access policies.

In order to get the best returns out of their investments on the wireless network, the organizations may want to:

- Give a higher priority to the business applications: They may assign a higher bandwidth quota for business applications. Or they may want to assign a higher priority for some applications so they get through first in case of contention.
- Restrict access to the network for other applications:
  - They may block certain applications or application categories. So, one can block all applications in the gaming categories. Or have granular rules to block *whatsapp*, but allow *facebook*.
  - They can put rate limits on how much bandwidth can be consumed by other applications. For an available WAN bandwidth of 10 Mbps, an organization may want to put a limit of 512 kbps for all social media applications. It will be an aggregate limit for any social media application being used by any user on any device connected to the wireless network.

**Time of Enforcement:** The Application Control can be enforced at scheduled times. For example, the application control can be enforced only during office times and only on weekdays. And all applications get unrestricted or a relaxed access at other times.

## 2. Deployment Scenarios

The AVC feature offers flexible deployment options to suit the needs of various customers. The Application controls can be enforced centrally on the controller or in a distributed fashion on the access points

### 2.1 Traffic Flow

The AVC feature can be enforced for both wired and wireless traffic. For wireless traffic, the feature can be enforced both for tunnel mode and the local bridging traffic forwarding mode.

**Tunnel mode:** In tunnel mode, all the traffic flows to the controllers in tunnel mode. The traffic is identified and the Application policies enforced on the controller. In tunnel mode, it does not matter which AP platform is used as the access points are just tunneling the traffic to the controllers.

**Local bridging mode:** In local bridging mode, all the traffic flows is locally bridged at the APs and the Access Points identify the application traffic and the Application policies are enforced on the access points.

**Wired Traffic:** The AVC feature can be enforced on any traffic that can be passed (routed or bridged) through the APs or controllers. It could be from a wired host or traffic from any wireless client that is routed to the controller via the wired network.

## 2.2 AVC Enforced at the controller

**Tunneled Traffic:** For deployments where user traffic is tunneled centrally to the controllers from the Access Points, the AVC feature is enforced on the centralized controller.

**Wired Traffic:** AVC is also enforced on the controllers for traffic that is bridged or routed to the centralized controllers. This traffic could be from wired devices or any traffic that is made to pass through the controllers.

In both these scenarios, the access points do not need to support the AVC feature. This option is especially useful when you have AP models that do not support Deep Packet Inspection (DPI), like the AP6532 or the AP6522.

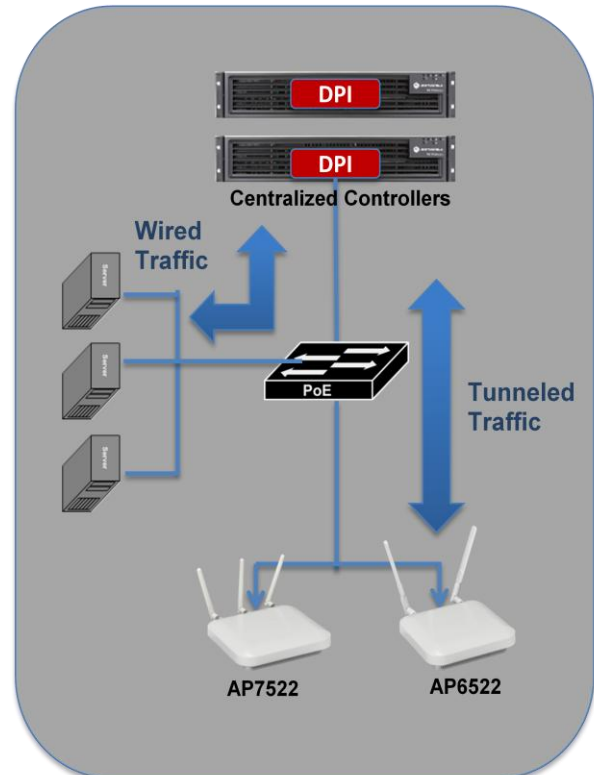


Figure 2-1: Centralized enforcement

## 2.3 AVC enforced on the Access Points

In distributed wireless deployments, the APs are deployed at remote sites often without a local controller. The user traffic is forwarded towards its destination by the access point in local bridging mode. In such cases, there is a requirement to enforce *Application Visibility and Control* right at the edge, on the access points, without the need to tunnel the traffic to the centralized controller for inspection.

WiNG 5.8 supports the DPI and AVC features on the access points. The user traffic is locally bridged at the access points and the Access points can perform DPI on the user traffic to identify the applications and enforce appropriate controls.

The Access points have no dependency on the controller to enforce this feature. Even if the controller is down or unreachable, the access points can identify the applications and enforce the configured policies without any loss of functionality.

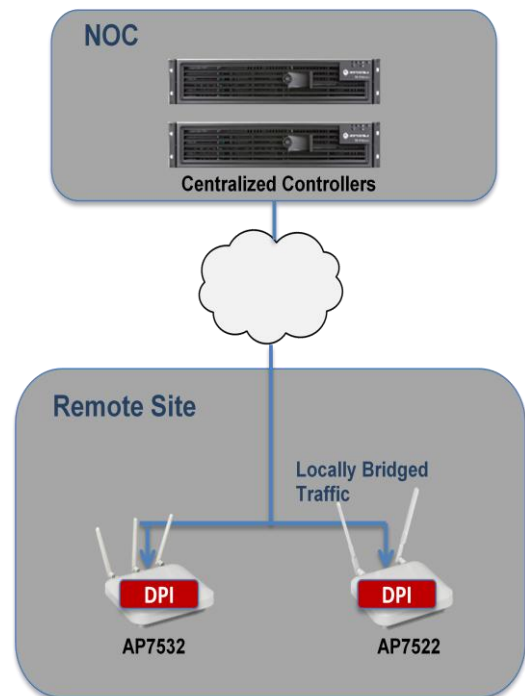


Figure 2-2: Distributed deployment



### 3. Configuration

There are 3 parts to the AVC configuration.

1. **Enable Deep Packet Inspection (DPI).**
2. **Create an Application Policy.**
3. **Assign the Application Policy.**

Optionally, configure the time period for the policy enforcement

In this example configuration, we will enable DPI on the access point and create an application policy to deny all social media traffic and rate limit the youtube traffic. As the traffic passes through the AP, the application traffic will be identified and appropriate rules enforced. The application categorization is viewed on *Zebra NSight*.

#### 3.1 Enable Deep Packet Inspection (DPI)

Enable DPI on the devices to enable the Application Recognition. This can be done in the device or profile context.

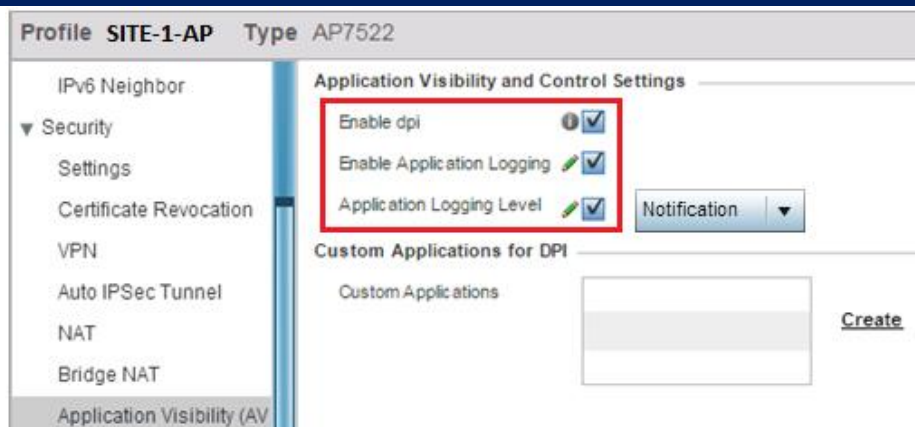
**Local bridging:** For local bridging mode, the DPI should be enabled on the Access Points.

**Tunnel Mode:** For tunnel mode, the DPI should be enabled on the Controller. As the traffic is tunneled to the controllers, the DPI will be enforced.

**Logging:** You can optionally enable DPI logging and specify the log level. When logging is enabled in the device or profile context, the logging is applicable for the AVC feature globally. Alternately, it can be enabled for specific application policy as shown in the next section.

#### GUI Configuration:

- 1 **Select the Site-1 AP profile *Configuration* → *Profiles* → *SITE-1-AP*. Navigate to the *Security* → *Application Visibility* and enable *DPI*.  
Optionally enable *DPI logging* and specify the *log level*.**



## CLI Configuration:

```
profile ap7522 SITE-1-AP
  dpi
  dpi logging on
  dpi logging level notifications
```

### 3.2 Create an Application Policy.

An **Application Policy** contains rules that should be enforced on the applications accessing the wireless network.

#### 3.2.1. Select the Applications:

Select the *application* or the *application category* of interest.

#### 3.2.2. Select the Action:

The applications or application categories can be subjected to the following rules/actions:

- **Allow:** Allow traffic from an application or application category
- **Deny:** Deny traffic from an application or application category
- **Mark:** Mark the application traffic with a specific DSCP or 802.1p priority value
- **Rate Limit:** Rate limit traffic from specific application or application category.

#### 3.2.3. Select the Logging Level:

You can optionally enable DPI logging and specify the log level. When logging is enabled in the application policy, the logs are generated only when rules for this specific application policy are hit.

#### 3.2.4. Select the Enforcement period:

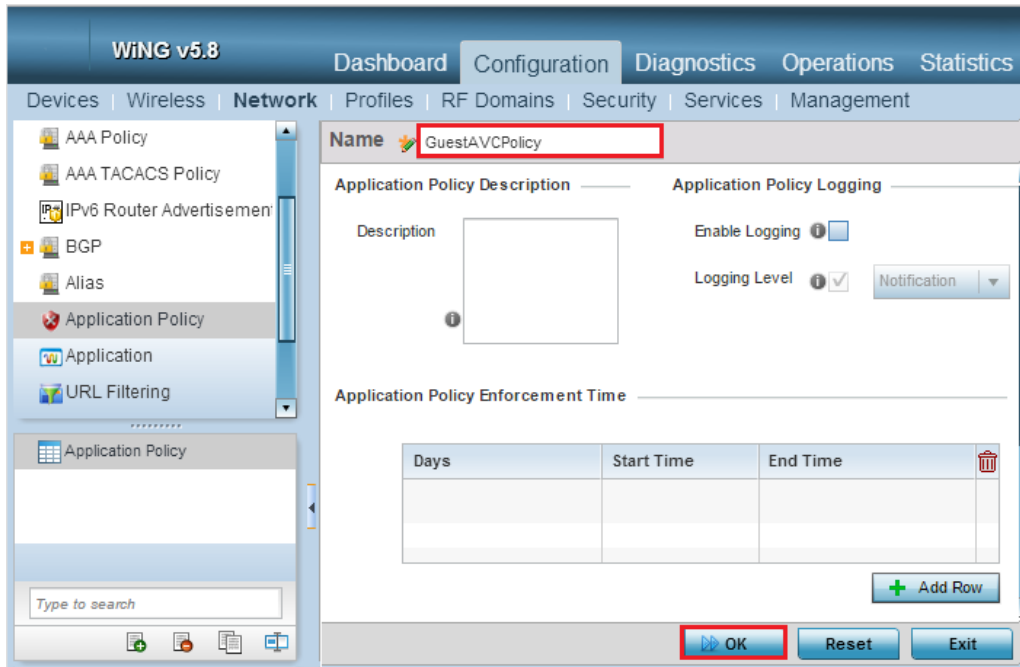
You can also specify the **time period** when this application policy should be enforced.

### GUI configuration Steps:

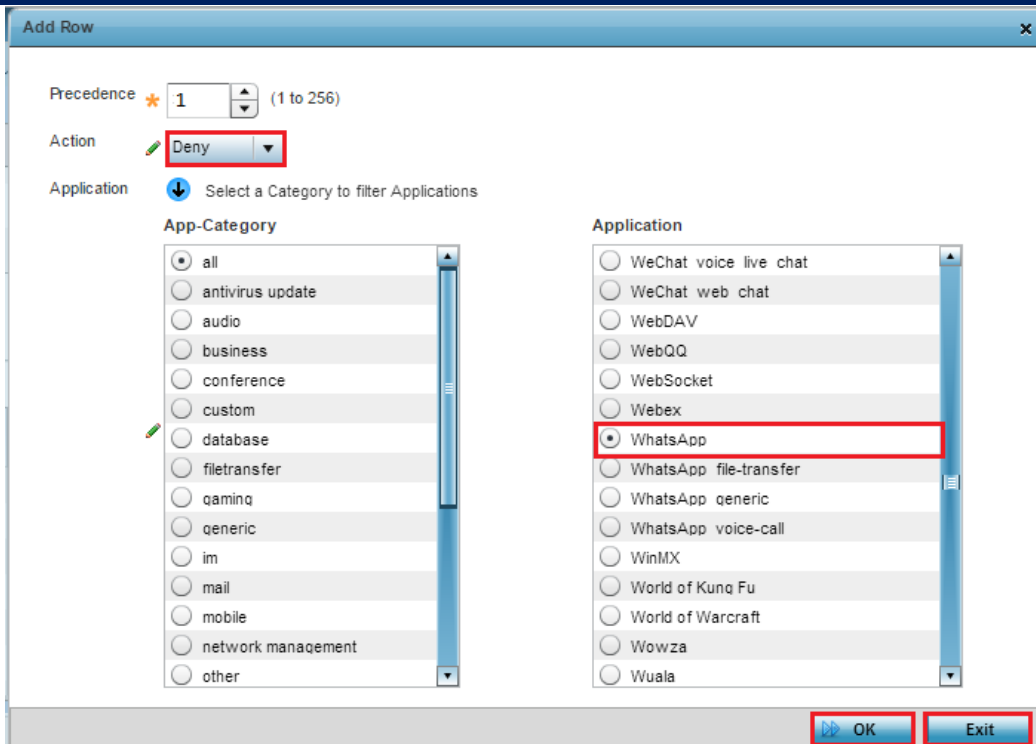
In this sample configuration, we will create an Application Policy with the following rules:

1. Block all **Whatsapp** application traffic
2. Rate-limit **youtube traffic** to 128 Kbps both upstream and downstream

1 Navigate to *Configuration* → *Network* → *Application Policy*. Click *Add* to create a new Application Policy. Give it a name *GuestAVCPolicy*. Click *OK*.



2 Navigate to *Application Policy Rules*. Click *Add Row* to create an Application Policy Rule. Create a rule to deny all *Whatsapp* Application Traffic. Click *OK*.



**3** Click *Add Row* and create a rule to rate-limit *youtube* traffic to *128 Kbps* both upstream and downstream. Click *OK*.

**Add Row**

Precedence: \* 2 (1 to 256)

Action: rate-limit

Application: Select a Category to filter Applications

**App-Category**

- all
- antivirus update
- audio
- business
- conference
- custom
- database

**Application**

- yikyak
- youku
- youporn
- yourfilehost-com
- yourfiles-biz
- youtube
- youtube-com
- yuilop

Enable Outbound Rating:

Outbound Max Burst Size: 2 (2 to 1,024)

Outbound Traffic Rate: 128 (50 to 1,000,000)

Enable Inbound Rating:

Inbound Max Burst Size: 2 (2 to 1,024)

Inbound Traffic Rate: 128 (50 to 1,000,000)

OK Exit

**4** Verify the newly created rules.

Name: GuestAVCPolicy

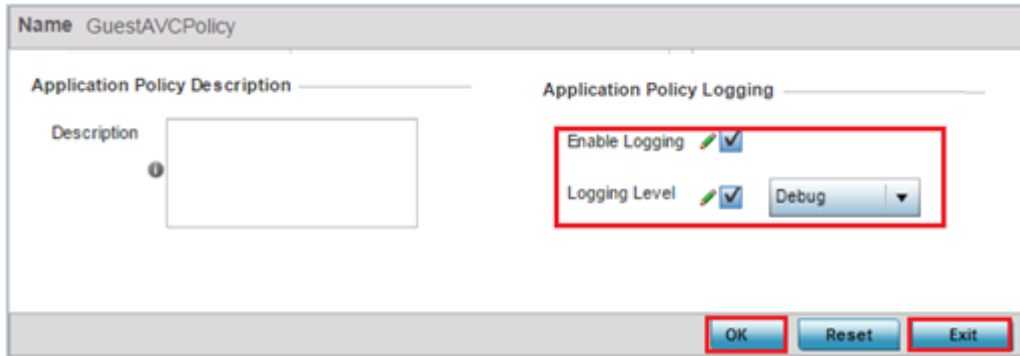
Application Policy Rules

Precedence	Action	Application Category	Default Application	Custom Application	Mark Type	Mark Value	Outbound Traffic Rate	Inbound Traffic Rate	
1	deny	-	WhatsApp	-	-	Not Set	Not Set	Not Set	
2	rate-limit	-	facebook	-	-	Not Set	128	128	

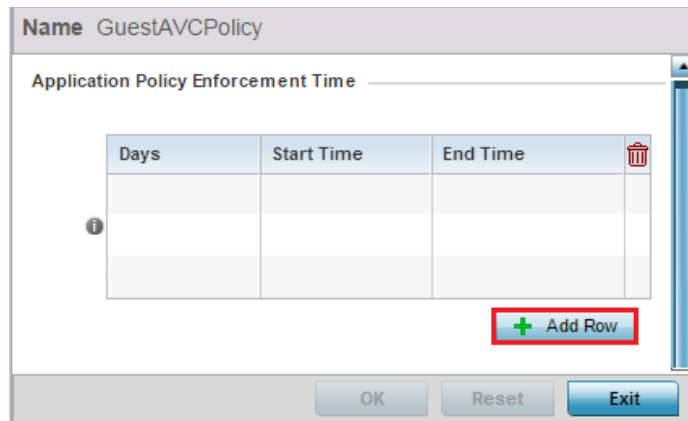
+ Add Row

OK Reset Exit

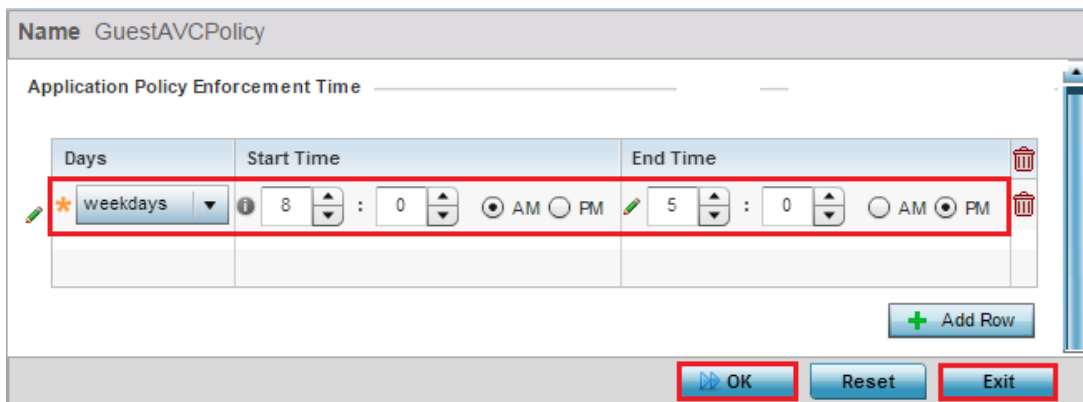
5 Optionally enable *DPI logging* and specify the *log level*. Click *Ok* and *Exit*.



6 Optional step:  
 Navigate to *Configuration* → *Network* → *Application Policy*. Select the Application Policy *GuestAVCPolicy*. Click *Edit*. Go to the table *Application Policy Enforcement Time* and click *Add Row*.



7 Select the time period over which the application policy should be enforced. Click *Ok*.



8 Click *Commit and Save* to save changes.



## CLI Configuration

```

application-policy GuestAVCPolicy
 enforcement-time days weekdays start-time 08:00 end-time 17:00
 deny application WhatsApp precedence 1
 rate-limit application youtube ingress rate 128 max-burst-size 2 egress rate 128 max-burst-size 2
 precedence 2
 logging on
 logging level debugging
  
```

### 3.3 Assign the Application Policy

The application policy can be assigned to one of the following interfaces. The Application policy Rules will be enforced on all the traffic passing through these interfaces.

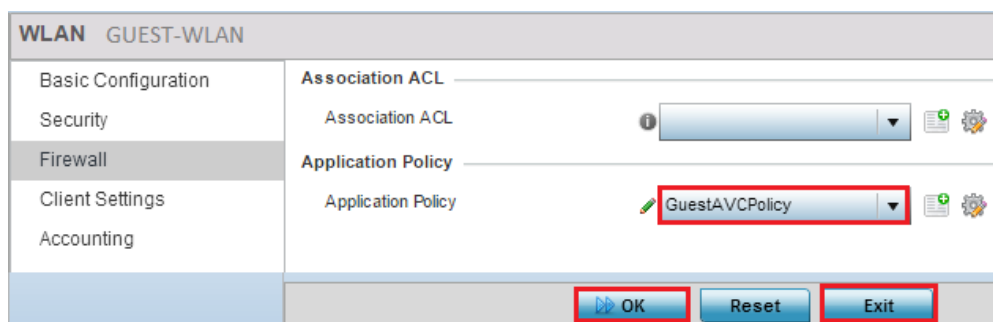
- **Wireless LAN:**
- **Bridge VLAN:**
- **User Role:**

Apply the application policy to the appropriate interface. Application control will be enforced on Any traffic that passes through that interface.

#### GUI Configuration Steps:

In this configuration example, we assign the application policy *GuestAVCPolicy*, created in the earlier step to the Guest Wireless LAN.

1 Navigate to *Configuration* → *Wireless LANs* → *GUEST-WLAN* → *Firewall*. Select the Application Policy *GuestAVCPolicy*. Click *Ok* and *Exit*.



- 2 Click *Commit* and *Save* to save the changes.



### CLI Configuration:

```
wlan GUEST-WLAN
use application-policy GuestAVCPolicy
```

### 3.4 NSight Integration

If **Zebra NSight** is deployed, you can view the AVC statistics on the NSight GUI. Please see the NSight Deployment Guide for details on using and deploying *Zebra NSight*. There is no additional configuration related to AVC required for NSight.

### 3.5 User Defined Application

Users can categorize applications by defining custom filters based on various parameters and use application controls that are available as part of the AVC feature.

- 1 Navigate to *Configuration* → *Network* → *Applications*. Click on *Add*.  
Enter the application name, select the category for the custom application. Add + to define a new *Network Service*.

 A screenshot of the 'Add Application' dialog box in the WING interface. The dialog has a title bar with 'Name' and a question mark icon. The 'Name' field contains 'CustomApp'. Below this, there are two sections: 'Basic Configuration' and 'Application Definition'. In the 'Basic Configuration' section, the 'Category' dropdown is set to 'custom'. In the 'Application Definition' section, the 'Network Service' button is highlighted with a red box. Other buttons in this section include 'URL List' and 'HTTPS'. To the right of the 'Network Service' button, there is a 'Network Service' dropdown menu, a red '+' icon, a gear icon, and a green arrow icon. At the bottom of the dialog, there are three buttons: 'OK', 'Reset', and 'Exit'.

- 2 Give a name to the Network Service and click *Add Row*. Select the port and protocol combination for your network service.

Protocol	Source Port(Low and High)	Destination Port(Low and High)
TCP	6	2026

- 3 Assign the network service to the custom application. Click on Arrow to assign it. Click on *OK* and *Exit*.



- 4 Use the custom application into the Application Policy *GuestAVCPolicy*.  
Go to *Application Policy Rules* and click on *Add Row*. Select action *Mark*. Select the *custom* category and select the custom application created in the last step. Assign a 8021p priority of 4 to this custom application traffic.

The screenshot shows the 'Add Row' dialog box with the following configuration:

- Precedence: 3 (1 to 256)
- Action: Mark
- Application: Select a Category to filter Applications
- App-Category: custom
- Application: CustomApp
- Mark Type: 8021p
- Mark Value: 4 (0 to 7)

Buttons: OK, Exit

- 5 Click Ok. Then Click *Commit* and *Save* to save the changes.



### CLI Configuration:

```
alias network-service $CustomApp1 proto tcp 2026 sourceport 2025
```

```
application CustomApp
use network-service $CustomApp1
```

```
application-policy GuestAVCPolicy
```

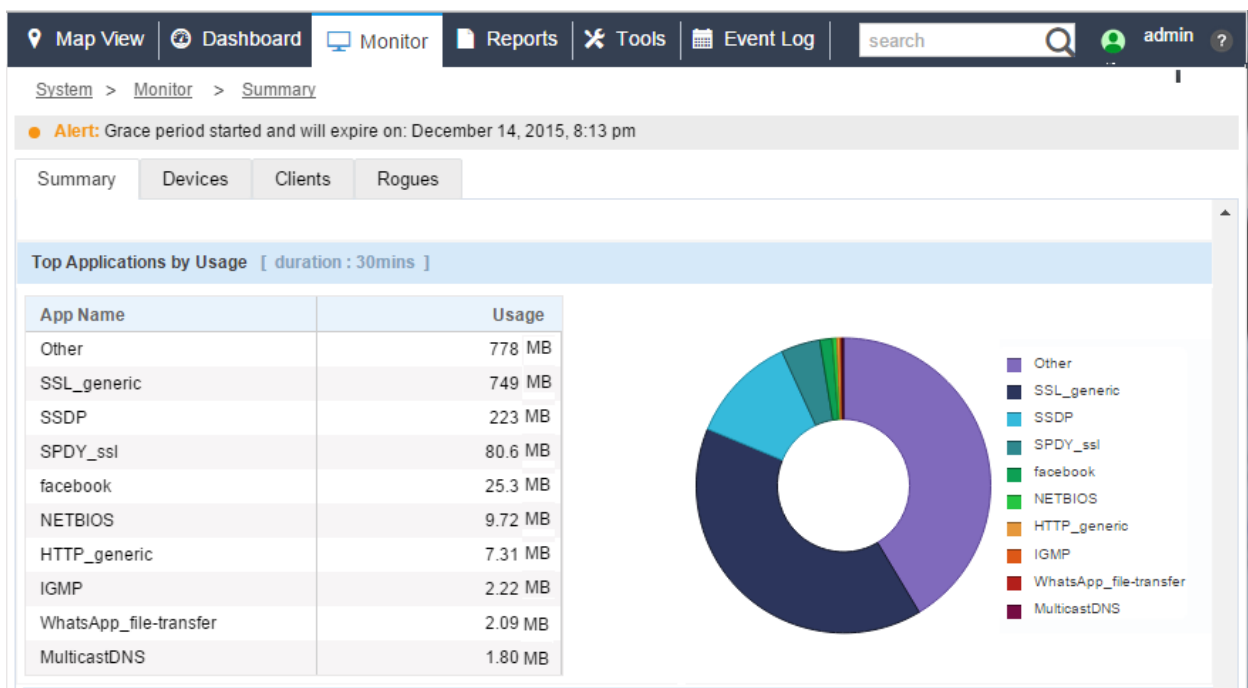
## 4. Validation

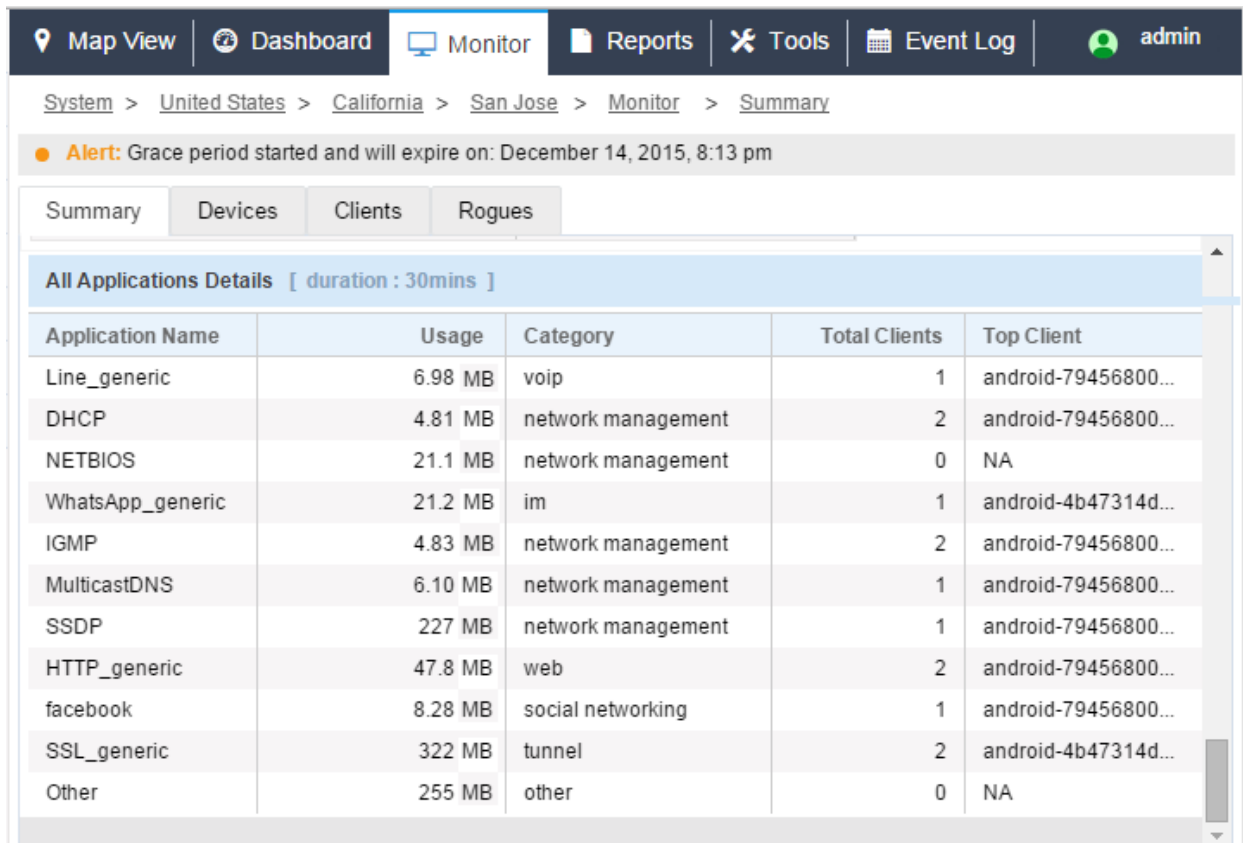
### 4.1 NSight GUI

Login to the *Zebra NSight* GUI. Select the **Monitor View** and navigate to the **Application Statistics**.

The NSight View shows the details on all applications and application categories being used on the wireless networks. You can visually identify the **Top 10 applications by usage** or you can see detailed statistics on each application, including the number of users accessing the application, total bandwidth being consumed by that application, etc.

The statistics can be seen at the site level, or at the client or AP level.





System > United States > California > San Jose > Monitor > Summary

Alert: Grace period started and will expire on: December 14, 2015, 8:13 pm

Summary | Devices | Clients | Rogues

All Applications Details [ duration : 30mins ]

Application Name	Usage	Category	Total Clients	Top Client
Line_generic	6.98 MB	voip	1	android-79456800...
DHCP	4.81 MB	network management	2	android-79456800...
NETBIOS	21.1 MB	network management	0	NA
WhatsApp_generic	21.2 MB	im	1	android-4b47314d...
IGMP	4.83 MB	network management	2	android-79456800...
MulticastDNS	6.10 MB	network management	1	android-79456800...
SSDP	227 MB	network management	1	android-79456800...
HTTP_generic	47.8 MB	web	2	android-79456800...
facebook	8.28 MB	social networking	1	android-79456800...
SSL_generic	322 MB	tunnel	2	android-4b47314d...
Other	255 MB	other	0	NA

## 4.2 Dashboard

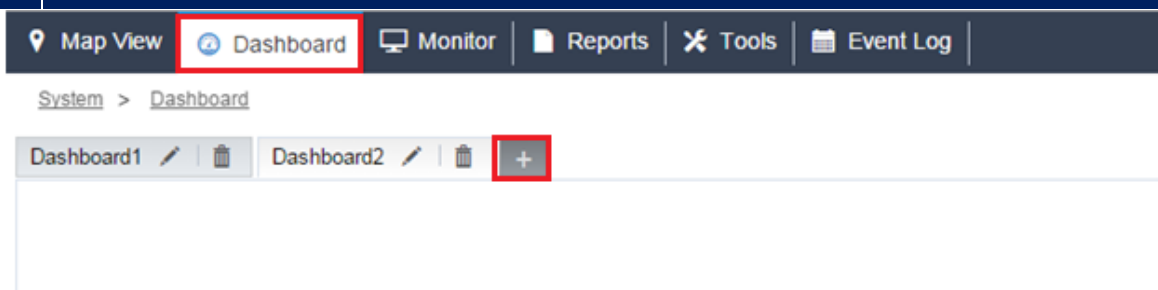
There are 2 widgets specific to the AVC feature that can be used on the *Zebra NSight* dashboards:

1. **Top 10 applications by usage:** Shows the top applications by usage on a pie chart.
2. **All Applications by Usage:** Lists all applications along with their usage details, like the bandwidth being used by the app, the number of clients using the application, etc.

The data can be seen at a System or Site Level.

In the example below, we will create a **dashboard** on *Zebra NSight* to show AVC related statistics.

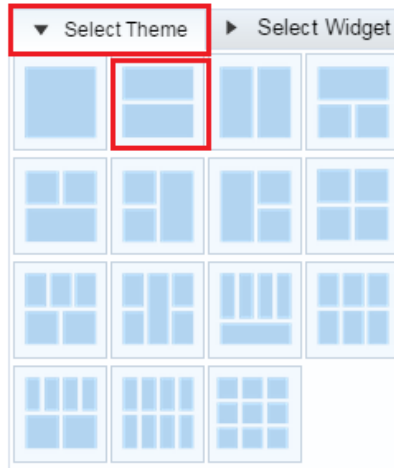
1 Login to *Zebra NSight*. Navigate to *Dashboard* Tab.. Click on the '+' sign to create a new Dashboard.



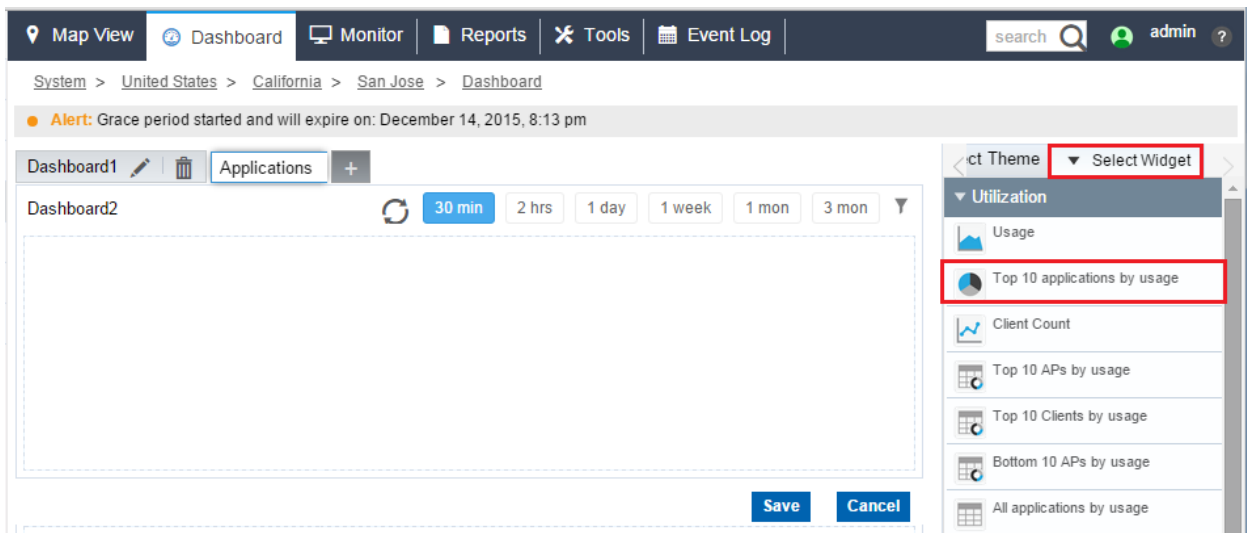
System > Dashboard

Dashboard1 | Dashboard2 | +

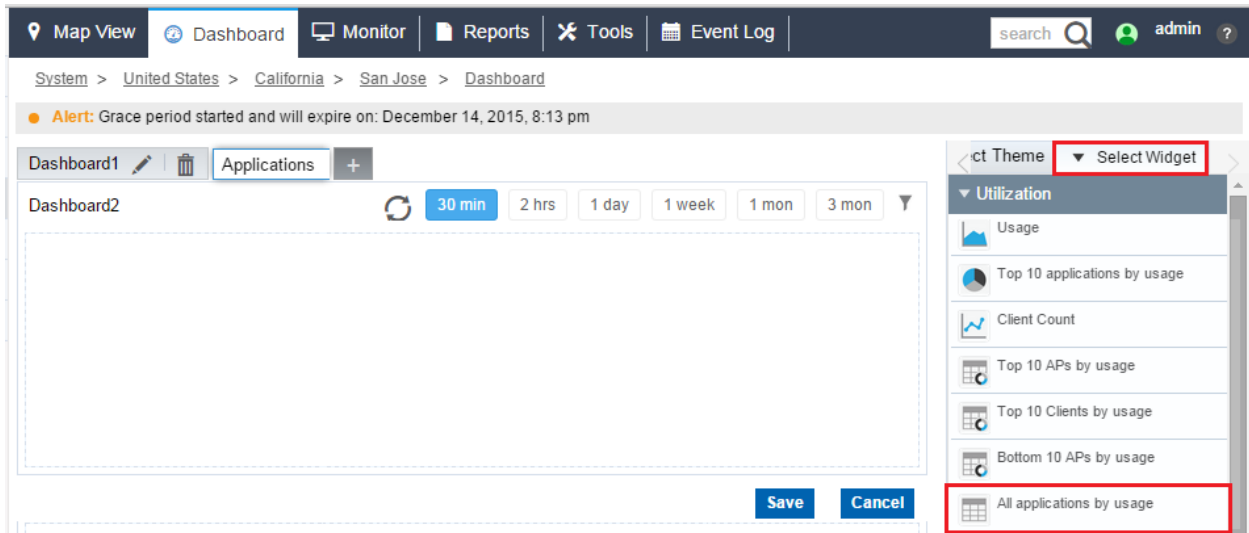
- 2 Select the layout for your new dashboard in the right side of the screen.  
On the 'Select Theme' tab, select a theme for the dashboard layout and drag & drop it on the main dashboard screen.



- 3 To select the Widgets, on the *Select Widgets Tab*, click on the *Utilization* section and *Top 10 Applications by Usage* and drag and drop them into the layout.

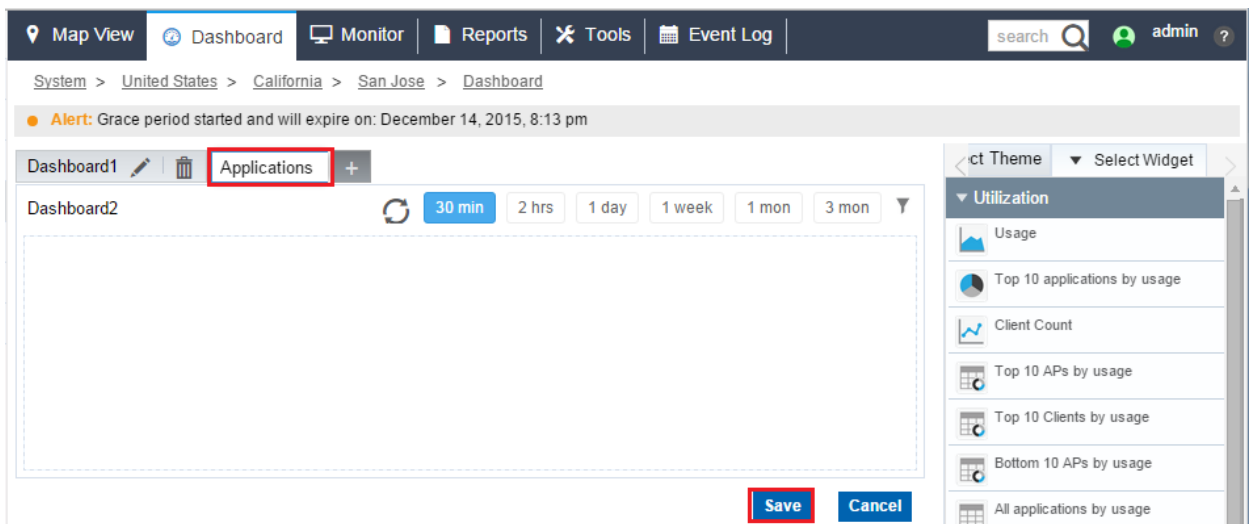


4 Then select the *All Applications by Usage* and drag & drop it into the Dashboard layout:



5 Give a name to the Dashboard and click on *Save*.

Note: The Dashboard changes will be lost if you navigate to another screen without saving the changes.



### 4.3 WiNG UI Statistics

The AVC statistics can also be viewed on the WiNG Flex UI. But the statistics will be limited for a duration up to 24 hours. You can view the AVC statistics per RF-Domain and per device. You can see the statistics for each application or each application category. You cannot view the per-client statistics on the WiNG UI. It is available on the CLI for the last 24 hours.

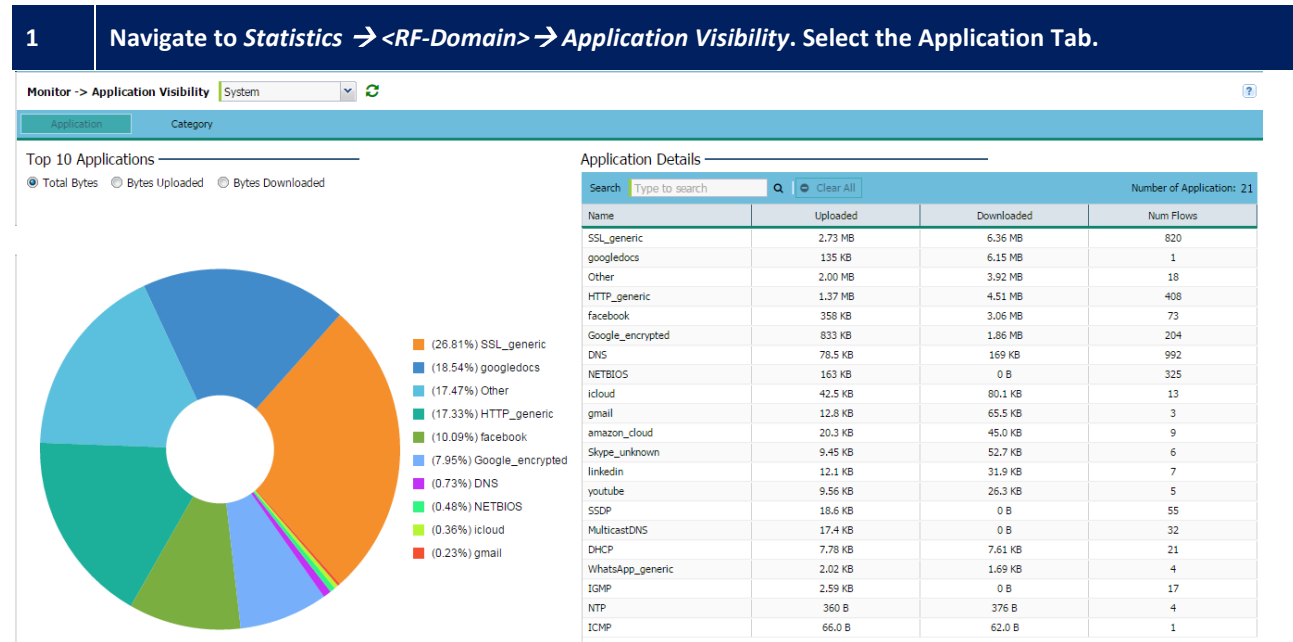


Figure 4-1: AVC statistics listed by Application

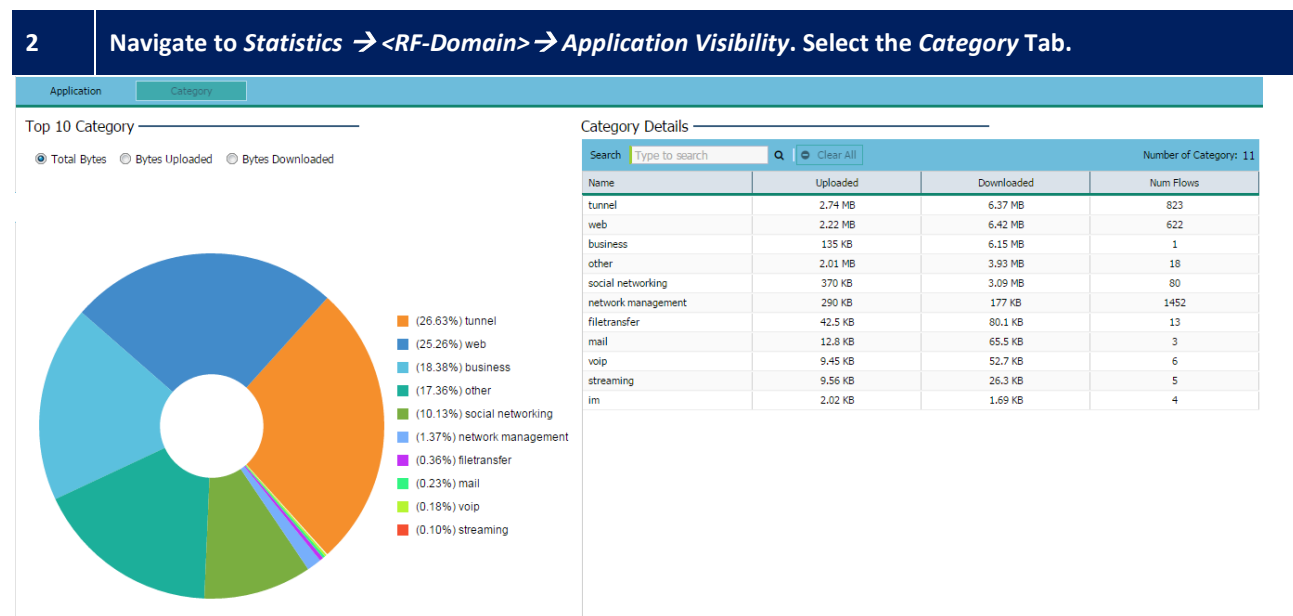


Figure 4-2: AVC statistics listed by Application Category

## 4.4 WiNG CLI Statistic

The application statistics for up to the last 24 hours can also be viewed on the WiNG platform using CLIC commands. The statistics are available for each wireless client or per application or application category.

### ➤ Wireless Client statistics:

The statistics are available for each wireless client or for all clients.

**\$> show dpi app wireless-client stats <client MAC> on <Device / RF Domain>**

```
VX9000 # show dpi app wireless-client stats CC-FA-00-B3-F5-AC on SITE-1
===== Wireless Client CC-FA-00-B3-F5-AC Application Statistics =====
-----
APPLICATION      BYTES_UPLOADED  BYTES_DOWNLOADED  --- NUM_FLOWS
-----
facebook          6276            6866              2
gmail             7838            48173             1
amazon_cloud     30136           43294             7
youtube          2224            5061              1
Other            16784           26806             1
DNS               5399            9644              73
DHCP              357             342               2
IGMP              0               184               2
NTP               450             450               5
SSDP              171             0                 1
Skype_unknown    1463            9197              1
HTTP_generic     10262           70754             11
SSL_generic      96163           202896            44
WhatsApp_generic  945             881               1
Google_encrypted 259306          353250            18
-----
```

### ➤ Application statistics:

**\$> show dpi app stats <application>**

```
VX9000 # show dpi app stats facebook
-----
APPLICATION      BYTES_UPLOADED  BYTES_DOWNLOADED  NUM_FLOWS
-----
facebook          118.484 KB      2.695 MB          31
-----
```

➤ **Application Category statistics:**

**\$> show dpi app-category stats <application-category>**

```
VX9000 # show dpi app-category stats social\ networking
```

APPLICATION	BYTES_UPLOADED	BYTES_DOWNLOADED	NUM_FLOWS
social networking	139.960 KB	2.836 MB	60

## 4.5 Log Messages

When logging is enabled, the messages are sent to the *Syslog* server in case an action is triggered. The Syslog messages have the following format

```
DATAPLANE: Matched application 2:whatsapp category social networking policy 0:AVC
Actions: D. Src MAC:<CC-FA-00-B3-F5-AC> Dst MAC:<B4-C7-99-5A-3E-A1>
EtherType:0x0800 Src IP:172.31.0.146 Dst IP:31.13.73.1 Proto:6 Src Port:55408 Dst
Port:443
```

**Action Codes:**

- M – Mark
- D – Drop
- R – Rate-Limit
- S – Traffic Shape
- C – Monitor (=Allow)



## 5. Appendix

### 5.1 Supported Platforms

The AVC feature is supported on the following platforms:

Controller Platform	Access Points
NX 9610	AP 7532
NX 9510	AP 7522
NX 7510	AP 7562
NX 5510	
RFS 6000	
RFS 4000	

On supported AP platforms, the AVC feature can be used in local bridging mode.

If the AVC functionality is needed on other AP platforms, the traffic can be tunneled to the controller and AVC is enforced on the controller.

### 5.2 Scaling

Multiple Application policies can be created and the limit is based on the supported platform. Please check the **WING Feature Matrix** to see the scaling information for the AVC feature on each platform.

### 5.3 Performance impact

The AVC feature performs Deep Packet Inspection (DPI) to inspect the application payload to identify the applications. When a new application session is initiated, the DPI engine inspects the first few packets exchanged to identify the application flow. For subsequent packets for that application, the packets are identified with the flow by just observing the packet headers. DPI is not needed on subsequent packet exchange on a continuous basis. Due to this, the performance impact is very limited when the AVC feature is enabled, whether on the APs or the controller platforms.

### 5.4 Licensing:

The AVC feature does not require a license, either to view the applications or to enforce the Application Rules.

But to see the historical data, one may need to procure Zebra NSight. Please see the deployment guide on Zebra NSight for more details on NSight Licensing.