

# AVALANCHE REPORT TEMPLATES

This paper provides descriptions of the reporting templates included in Avalanche 5.2. The reports are divided into logical groups depending on the type of information they provide. Reports are created, scheduled, and accessed from the Avalanche Web Console. Reports come in PDF, CSV, or XML formats. Reports that assist with PCI DSS compliance have the PCI DSS section listed after the description.

Avalanche has the following categories of report templates:

- Mobile Device Reports
- Profile Reports
- Infrastructure Security Reports
- Infrastructure Properties Reports
- Infrastructure Errors Reports
- Infrastructure Performance Reports
- Infrastructure Inventory Reports
- Infrastructure Performance Peak Reports

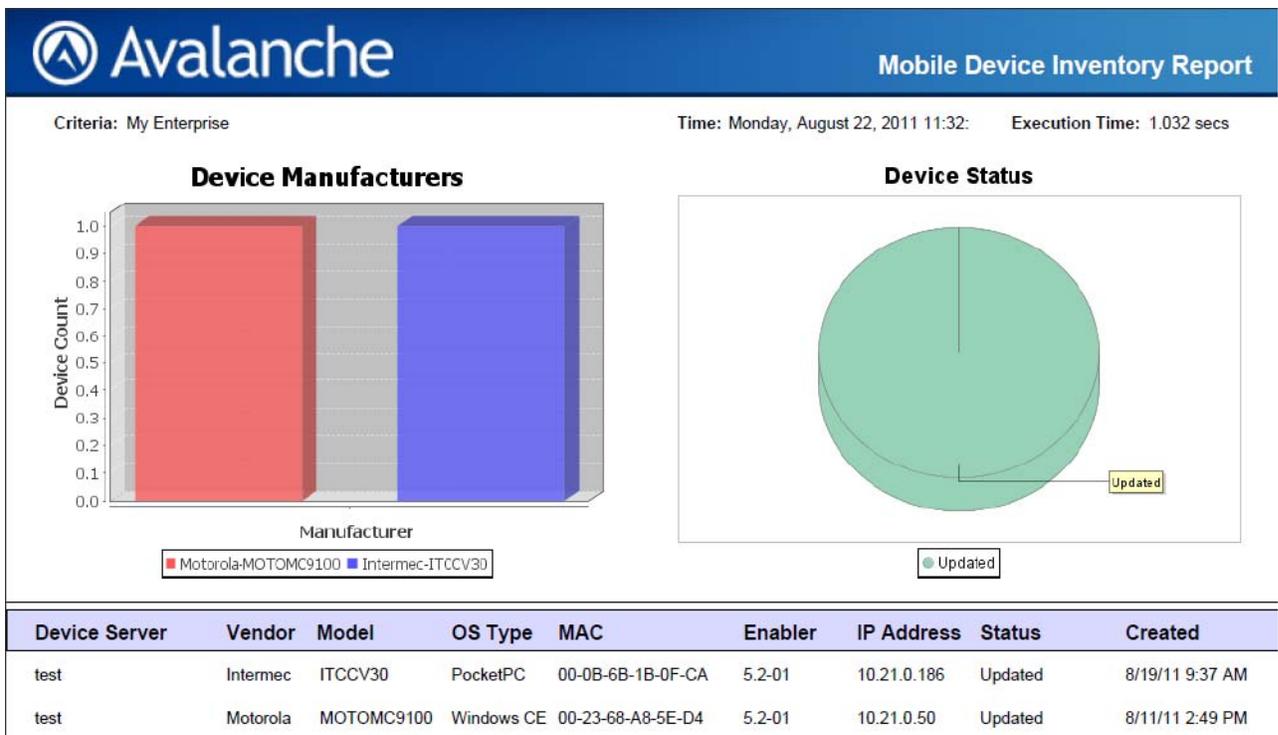
## MOBILE DEVICE REPORTS

Avalanche provides reports on the mobile devices being managed by Avalanche. This includes information such as location inventory, device properties and statistics, battery information, and profile and package information. You can limit each report by location, so that only the devices in the selected location are displayed. The report results are organized by the first field listed for each report.

Mobile device reports include the following templates:

- **Mobile Device Inventory** Provides the server location, make (vendor), model, OS, Enabler version, MAC address, update status, and IP address of each mobile device. Graphs associated with this report show device count by manufacturer and device status. The report uses one line for each device.
- **Mobile Device Summary** Provides the vendor, model, and OS version for devices. The pie chart associated with this report displays the percentage of devices of each type. The report uses one line for each set of devices with identical vendor, model, and OS version.
- **Mobile Device Property** Provides the IP address, model, server location, region, and each property (with its value) for each device. This report uses one line for each property of each device and has the potential to generate very large results.
- **Mobile Device Roaming** Provides the IP address, model, Enabler version, current and last server location, the number of times the device has roamed (switched APs), and the last time the device roamed. The chart associated with this report shows the percentage of devices that have not roamed, roamed once, twice, or three or more times. The report uses one line for each device.
- **Mobile Device Statistics** Provides statistics about radio performance. This includes the BSSID, total and average bytes, total and average packets, and total and average errors for each device. This information is useful in evaluating network traffic for a location.

- **Battery Summary** Provides the IP address, vendor, model, Enabler version, server location, battery status (e.g., charging) and percentage of battery power for each mobile device. The pie chart associated with this report displays the number of devices for each battery level reported as well as the number of devices that did not report a battery level. The report uses one line for each device.
- **Mobile Device History** Provides the MAC address, IP address, vendor, model, server location, and details about the events associated with each device. The event information includes the date, time, event name and status, and a description of the event. Events may include installing packages or applying profiles. The report uses multiple lines for each device.
- **Mobile Device Realtime Data** Provides a list of the mobile devices in the location, with the realtime statistics for each device and the date the properties were most recently added, changed, or deleted. The report uses a table for each device.
- **Mobile Device Property Data** Provides a list of the mobile devices in the location, with the properties for each device and the date the properties were most recently added, changed, or deleted. The report uses a table for each device.
- **Mobile Enabler Profiles** Provides a list of the mobile devices in the location, with the profiles that are applied on each device. This includes the profile name and type, the parent location and the last time the profile was modified.
- **Mobile Last Contact** Provides the timestamp for the last time each mobile device contacted the device server. This includes the MAC, IP address, manufacturer, model, and the device server address for each device. The graph for this report shows is a pie chart showing percentages of devices that have contacted the server within specified time ranges.
- **Mobile Package Status** Provides a list of the mobile devices in the location that have a selected package installed. This report includes the MAC address, terminal ID, manufacturer, model, device server, version of the package installed, sync state, and the timestamp for the device's last contact.



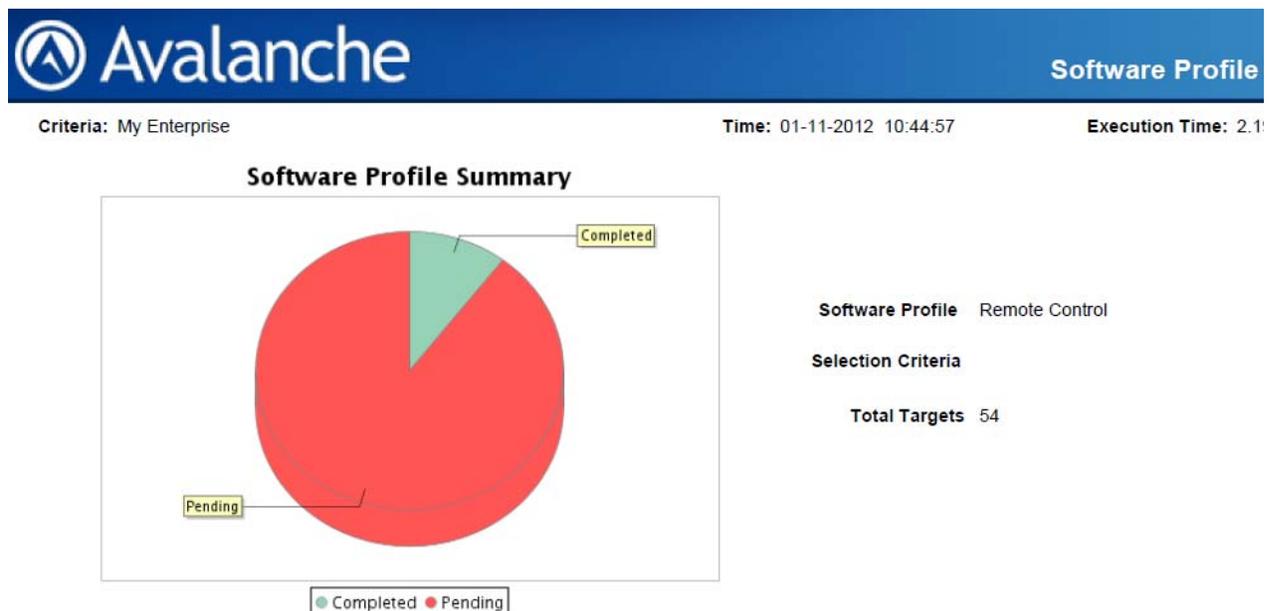
Mobile Device Inventory (PDF)

## PROFILE REPORTS

Avalanche provides reports on the profiles being managed by Avalanche. This includes information such as package status and targeted devices. You can limit each report by location, so that only the devices in the selected location are displayed. The report results are organized by the first field listed for each report.

There are two templates for profile reports:

- **Software Profile** Provides the status of software packages: installed, failed, or pending. The details for each package include the selection criteria, number of targeted devices, number of devices where the package is installed, number of devices where the installation is pending and the number of devices where the installation failed. The chart associated with this report displays the installed, pending, and failed numbers.
- **Software Profile Summary** Provides a chart and list for each software profile, displaying the name, criteria, number of targeted devices, pending/completed status, and information about targeted devices. Each device is listed with its IP address, manufacturer, Enabler version, server location, and package status, as well as the time the package was created.



*Software Profile Summary (PDF)*

## INFRASTRUCTURE SECURITY REPORTS

Avalanche provides reports on security issues reported by infrastructure devices. This includes information such as rogue infrastructure devices, insecure protocols, default passwords, and unmanaged or rogue mobile devices.

A rogue device is a device on your wired network that is transmitting wirelessly but isn't being managed by Avalanche. A foreign device is a device that is detected on the wireless network but is not on the wired network. For reporting purposes, foreign devices are included in the rogue device reports. The properties reported vary between device manufacturers and models.

Infrastructure security reports include the following templates:

- **WLAN Security** Provides a list of the infrastructure devices in the location with specifics about the security of the WLANs. This includes the name and IP address of the device, the location the device is associated with, and the device's radio type, WLANs, encryption, SSID, broadcasting status, and the last time the device was contacted by Avalanche. (PCI DSS section 4.1.c)
- **Devices with Default Passwords** Provides a list of devices that have a default password for at least one protocol. This includes the name and IP address of the device, the location the device is associated with, the password status (default, secured, or N/A) for CLI, SNMP RO and RW, SNMP v3, and the last time the device was contacted by Avalanche. (PCI DSS sections 2.1.1.b and 2.1.1.c)
- **Insecure Protocols in Use** Provides a list of protocols used by the server to contact the infrastructure device, identifies devices which are using insecure protocols, and highlights the specific insecure protocol being used. This includes a line for each device with its name, MAC and IP address, the location the device is associated with, the protocols in use, and the last time the device was contacted by Avalanche. (PCI DSS sections 2.2.2.b and 4.1.c)
- **Rogue Device by Threat Level** Provides a list of rogue devices detected. The list is organized by perceived threat level and may include information about the rogue such as signal strength, SSID, the device that detected the rogue, or the channel used. (PCI DSS section 11.1.c)
- **Rogue Device by Finder** Provides a list of rogue devices detected. The list is organized by device and lists all managed devices that detect the rogue and the RSSI (received signal strength) and channel for each device, as well as timestamps for when the rogue was detected.
- **Rogue Device Properties (AP View)** Provides a graph of device properties for each rogue, organized by rogue property and finding AP. Each graph provides a timeline view of a given property for a given rogue. This report can only be run for a group location or a single device.
- **Rogue Device Properties (Rogue View)** Provides a graph of device properties for each rogue, organized by rogue property and rogue device. Each graph provides a timeline view of a given property for a given rogue. This report can only be run for a group location or a single device.
- **Rogue Device Count** Provides a graph of the type of rogues detected on your wireless network and the number of rogues detected that are also seen over Ethernet.
- **Trap Data** Provides trap information received by the server. Traps may be converted into readable strings if MIBs are added to the infrastructure server's `mibs` folder. Traps will only be stored if they are type V2c. This report uses one line for each type of trap per device, and displays the value, count, and time.
- **Unmanaged Mobiles** Provides a list of mobile devices that are not managed by Avalanche that are seen by your infrastructure devices. If a mobile device has associated with more than one AP, it will only show the most recent contact. The information includes the mobile device's MAC and manufacturer, and the details of the infrastructure device.
- **Rogue Mobiles** Provides a list of mobile devices that are not managed by Avalanche that are communicating on the wired network. If a mobile device has associated with more than one AP, it will only show the most recent contact. The information includes the mobile device's MAC and manufacturer, and the details of the infrastructure device.

## INFRASTRUCTURE PROPERTIES REPORTS

Avalanche provides reports on the properties of your infrastructure devices. This includes information such as when devices were ready, queried, updated with new firmware, and last contact. They also can provide information about the mobile devices associated with the selected infrastructure. The properties reported vary between device manufacturers and models.

Infrastructure properties reports include the following templates:

- **Infrastructure Device Properties** Provides a timetable of events for the infrastructure devices as seen by the infrastructure server. Events include when the device is ready, query failed, mobile query, firmware updates, action requested, and the latest timestamp.
- **Associated Mobile Properties** Provides a chart and table for each property of the mobile devices associating with the selected infrastructure. Each table lists the MAC addresses of the mobile device and access point, the IP address and name of the AP, and the latest value and timestamp for the property.

## INFRASTRUCTURE ERRORS REPORTS

Avalanche provides reports on the errors reported by infrastructure devices. This includes information about the device reporting the error, the error, and the current status of the device. The properties reported vary between device manufacturers and models.

Infrastructure errors reports include the following templates:

- **In Error State** Provides a list of all the infrastructure devices reporting an error state (e.g., query failed). The devices are organized according to type of device, location, and the time the error was reported. The report uses one line for each error, and includes the device's name, IP and MAC address, the error reported, and the time of the error.
- **Unreachable Infrastructure Devices** Provides a list of all the infrastructure devices that the infrastructure server has not been able to contact (because of crash, internal error, or network problem). The devices are organized according to type of device, location, and the time the error was reported. The report uses one line for each device, and includes the device's name, IP and MAC address, and the time of the failed contact.

### Wavelink Avalanche - Unreachable Infrastructure Devices

**Report Name:** unreachable infra

**Report Type:** Unreachable Infrastructure Devices

**Report Creation Date:** Friday, January 6, 2012 4:23:57 PM MST

**Report Range:** Wednesday, January 4, 2012 9:55:38 PM MST to Thursday, January 5, 2012 5:58:01 PM MST

**Region:** My Enterprise

**Devices in error (last 24hr):** 2

**Devices in error (prior to 24hr ago):** 3

View device details on the following page(s).

Table of Contents of groups:

Subgroup	Location	Last 24 Hours?	Count
<a href="#">Not in Group (null)</a>	SouthJordan	Yes	2
<a href="#">Not in Group (null)</a>	SouthJordan	No	3

*Unreachable Infrastructure Devices report (PDF)*

# INFRASTRUCTURE PERFORMANCE REPORTS

Avalanche provides reports on the performance of infrastructure devices. This includes information such as the bandwidth being used, the reported device capacity, errors in transmission, and associated mobile devices.

These reports are good for monitoring general infrastructure traffic behavior. They can be used to indicate problem areas. Use the Infrastructure Peak Performance reports to identify peak resource consumers within any given time in the chart, then use the normal Performance report to gather information for a specific device.

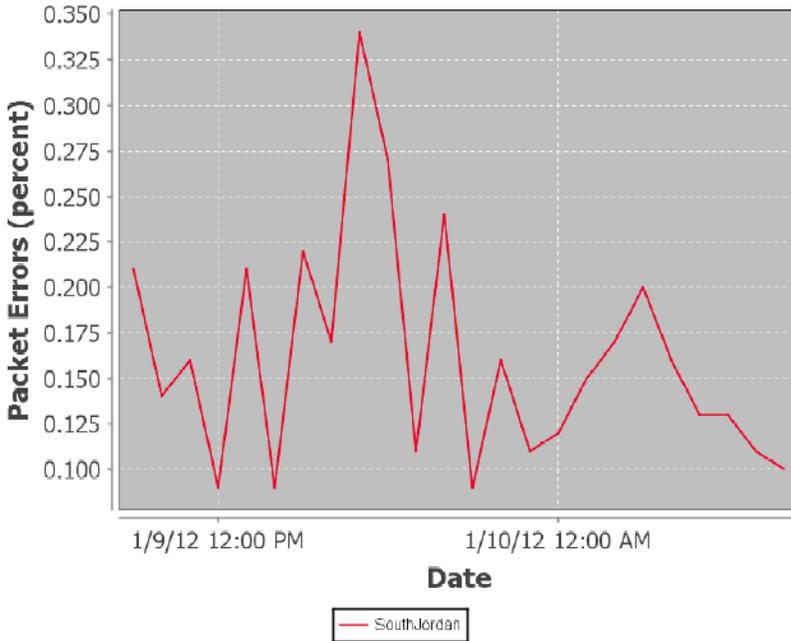
The properties reported may vary between device manufacturers and models.

Infrastructure performance reports include the following templates:

- **Utilization** Provides a timeline of the percentage of available bandwidth being used by infrastructure devices. If the report is run for more than one device, the results will show the average of all devices at the location for each time period. Utilization is the ratio of the bits per second being transmitted to the maximum theoretical bits per second. The theoretical maximum bits per second is proportional to the medium's capacity multiplied by the protocol's maximum data rate (for example, 54 Mbps for a G radio). Capacity decreases when there are more devices or a greater proportion of small packets. Utilization is affected by the device capacity, the total bytes received/transmitted, and the bit rate. Only successful transmissions affect the reported utilization.
- **Capacity** Provides a timeline of the highest reported wireless capacity by an infrastructure device in the selected location. This shows how much data can be sent and received by the access point within a given period of time, based on the amount of wireless activity. Available capacity is calculated using packet size and the number of associated mobile devices. For example, typically an 802.11b access point (11Mbps) with no mobile devices associated would have maximum capacity of about 72% of the theoretical throughput (~7.92Mbps). The reason the capacity can never reach the theoretical maximum is due to miscellaneous radio overhead. Capacity decreases with increasing number of associated mobile devices and smaller packet sizes.
- **WEP Errors** Provides a timeline of the highest number of WEP errors reported by an infrastructure device in the selected location. The chart displays the percentage of packets exchanged that contained a WEP-related error. A WEP error on a packet cannot be detected unless the packet is transmitted successfully.
- **Packet Errors** Provides a timeline of the highest percentage of packet errors reported by an infrastructure device in the selected location. Often, these errors are the result of packet collisions, indicating an overburdened section of the network; however, other causes exist, such as WEP errors or foreign device interference. Criteria affecting the Packet Errors report include: inbound and outbound errors, packets received, packets sent, CRC errors (typically, an error in the packet header), and retry count.
- **Inbound Errors** Provides a timeline of the highest percentage of inbound errors reported by an infrastructure device in the selected location. These errors occur when an access point has difficulty receiving a packet. A high number of inbound packet errors might indicate an interference issue or a malfunction within the access point itself.
- **Outbound Errors** Provides a timeline of the highest percentage of outbound traffic errors reported by an infrastructure device in the selected location. These errors occur when the receiving device has informed the access point that the transmission was not received successfully.
- **CRC Errors** Provides a timeline of the highest percentage of cyclic redundancy check (CRC) errors reported by an infrastructure device in the selected location. Infrastructure devices and the reported CRC (data integrity) errors for each device. A CRC is a process through which a device ensures that a transmission has been received successfully. If the check fails, it is likely that the transmission was not received successfully, and often the source of the transmission is requested to re-send the data. CRC errors are typically caused by interference or problems with the access point itself.

- **Retries** Provides a timeline of the highest percentage of retries reported by an infrastructure device in the selected location. An excessive number of retries might indicate a high number of device associations, excessive frequency overlap between access points (they are communicating on or near the same channel), utilization/capacity issues, or problems with the access point itself.
- **Mobile Count** Provides a timeline of the highest number of associated mobile devices reported by an infrastructure device in the selected location. A table also shows the highest count per hour.

### Packet Errors (percent)



Location Name: SouthJordan

Date/Time	Percent
Jan 9, 2012 9:00:00 AM	0.21
Jan 9, 2012 10:00:00 AM	0.14
Jan 9, 2012 11:00:00 AM	0.16
Jan 9, 2012 12:00:00 PM	0.09
Jan 9, 2012 1:00:00 PM	0.21
Jan 9, 2012 2:00:00 PM	0.09
Jan 9, 2012 3:00:00 PM	0.22

[Packet Errors Report \(PDF\)](#)

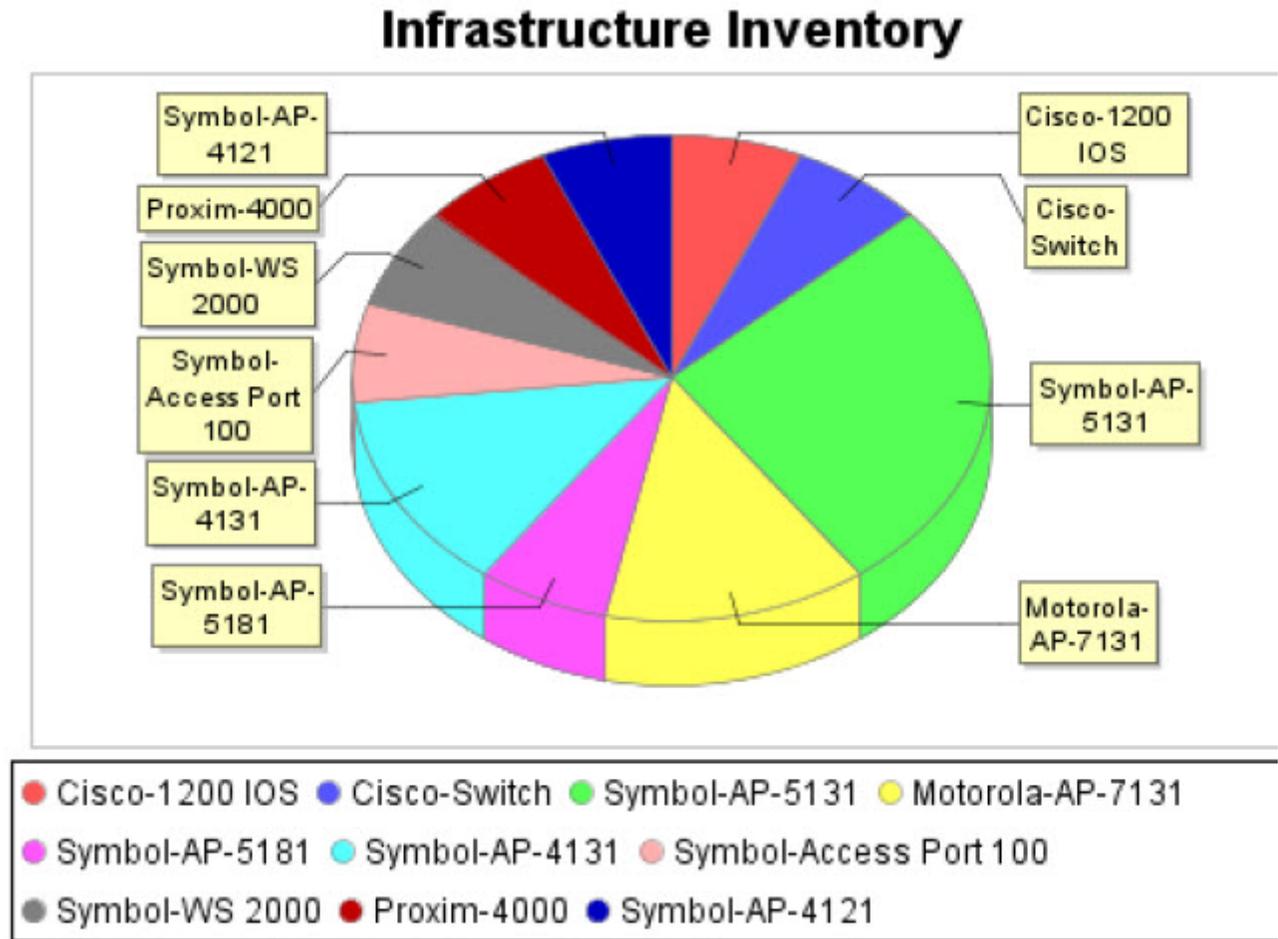
## INFRASTRUCTURE INVENTORY REPORTS

Avalanche provides reports on your infrastructure device inventory. This includes information such as details of each device and the number of mobile devices associated with your infrastructure devices. The properties reported vary between device manufacturers and models.

Infrastructure inventory reports include the following templates:

- **Infrastructure Device Inventory** Provides the server location, manufacturer, model, firmware version, IP address, MAC address, and status for each infrastructure device (including foreign and rogue devices). This report also has charts displaying the percentage of devices for each device type and for each reported status. (PCI DSS section 11.1.a)

- **Access Point Associations** Provides a list of infrastructure devices with IP and MAC address, manufacturer, server location, and the number of mobile devices associated with each infrastructure device. This report includes a chart displaying the percentage of infrastructure devices that have 0, 1-2, 2-5, or more than 5 associated mobile devices.



Infrastructure Inventory pie chart

## INFRASTRUCTURE PERFORMANCE PEAK REPORTS

Avalanche provides reports on your infrastructure device inventory. This includes information such as the bandwidth being used, the reported device capacity, errors in transmission, and associated mobile devices.

These reports are useful for identifying excessive or insufficient network and wireless performance at a given location for a specific time period (one hour resolution). The results represent the maximum across all devices at a given location. Use the Infrastructure Peak Performance reports to identify peak resource consumers within any given time in the chart, then use the normal Performance report to gather information for a specific device.

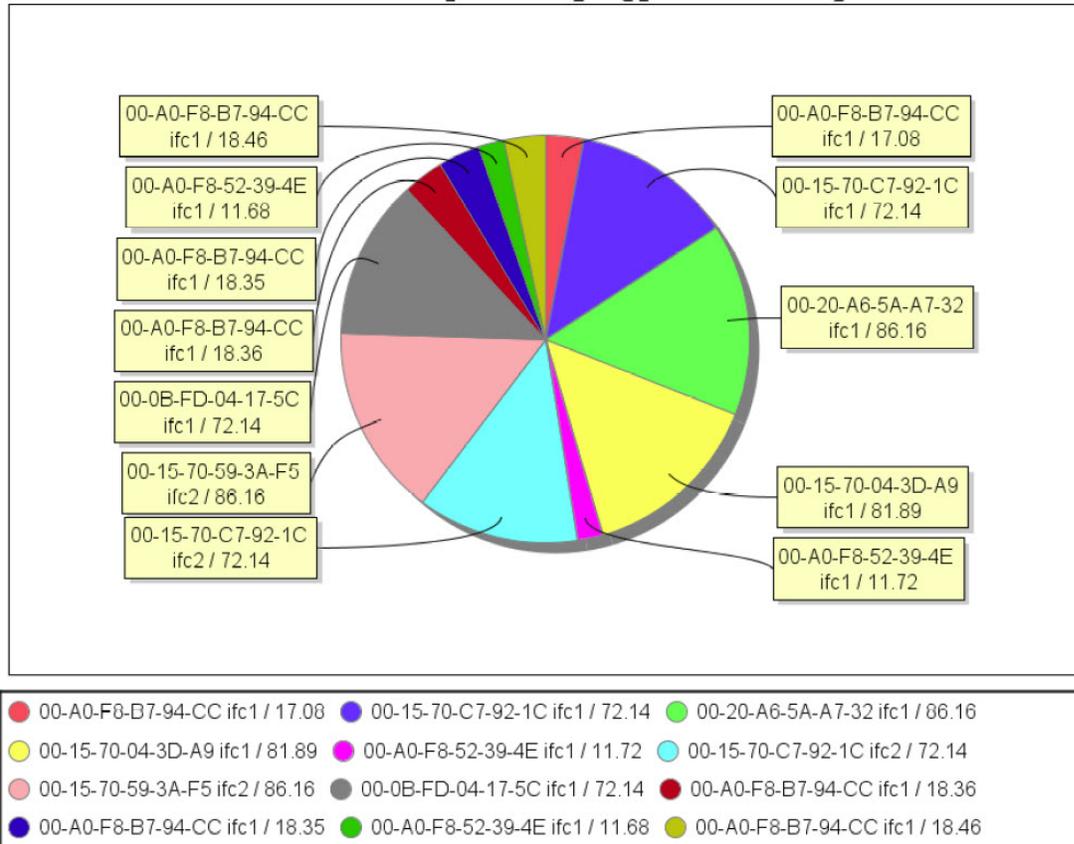
Infrastructure performance peak reports include the following templates:

- **Peak Utilization** Provides a pie chart showing percentages of the maximum utilization for each device at the location. A table also shows the peak utilization for each device each hour for the reported time.

Utilization is affected by the total bytes received/transmitted and bit rate. Only successful transmissions affect the reported utilization.

- Min Capacity** Provides a pie chart showing percentages of the available wireless capacity for each device at the location, based on the amount of wireless activity. A table also shows the capacity for each device each hour for the reported time. Available capacity is calculated using packet size and the number of associated mobile devices. Capacity decreases with more associated mobile devices and smaller packet sizes. For example, typically an 802.11b access point (11Mbps) with no mobile devices associated would have maximum capacity of about 72% of the theoretical throughput (~7.92Mbps). The reason the capacity can never reach the theoretical maximum is due to miscellaneous radio overhead.

## Peak Capacity (percent)



Min Capacity pie chart (PDF)

- Peak WEP Errors** Provides a pie chart showing percentages of the WEP errors reported by each infrastructure device in the selected location. A table also shows the percentages of WEP errors for each device each hour for the reported time. A WEP error on a packet cannot be detected unless the packet is transmitted successfully.
- Peak Packet Errors** Provides a pie chart showing percentages of packet errors reported by each infrastructure device in the selected location. A table also shows the percentages of packet errors for each device each hour for the reported time. Often, these errors are the result of packet collisions, indicating an over-burdened section of the network; however, other causes exist, such as WEP errors or foreign device interference. Criteria affecting the Packet Errors report include: inbound and outbound errors, packets received, packets sent, CRC errors (typically, an error in the packet header), and retry count.

- **Peak Inbound Errors** Provides a pie chart showing percentages of inbound traffic errors reported by each infrastructure device in the selected location. A table also shows the percentages of inbound errors for each device each hour for the reported time. These errors occur when an access point has difficulty receiving a packet.
- **Peak Outbound Errors** Provides a pie chart showing percentages of outbound traffic errors reported by each infrastructure device in the selected location. A table also shows the percentages of inbound errors for each device each hour for the reported time. These errors occur when the receiving device has informed the access point that the transmission was not received successfully.
- **Peak CRC Errors** Provides a pie chart of the percentages of CRC (data integrity) errors reported by each infrastructure device in the selected location. A table also shows the percentages of CRC errors for each device each hour for the reported time. CRC errors are typically caused by interference or problems with the access point itself.
- **Peak Retries** Provides a pie chart of the percentages of retries reported by each infrastructure device in the selected location. A table also shows the percentages of retries for each device each hour for the reported time. An excessive number of retries might indicate a high number of device associations, excessive frequency overlap between access points (they are communicating on or near the same channel), utilization/capacity issues, or problems with the access point itself.
- **Peak Mobile Count** Provides a pie chart of the number of associated mobile devices reported by each infrastructure device in the selected location. A table also shows the count for each infrastructure device each hour for the reported time.



Wavelink Corporation  
USA and Canada: 1.888.697.WAVE (9283)  
Outside the USA and Canada: + 800 WAVELINK (9283 5465)  
CustomerService@wavelink.com

