

# OmniVista 3600 Air Manager 8.2.0.3



## **Copyright**

© 2016 Alcatel-Lucent. All rights reserved.

Specifications in this manual are subject to change without notice.

Originated in the USA.

AOS-W, Alcatel 4302, Alcatel 4304, Alcatel 4306, Alcatel 4308, Alcatel 4324, Alcatel 4504, Alcatel 4604, Alcatel 4704, Alcatel 6000, OAW-AP41, OAW-AP68, OAW-AP60/61/65, OAW-AP70, OAW-AP80, OAW-AP92/93, OAW-AP105, OAW-AP120/121, OAW-AP124/125, OAW-AP175, OAW-IAP92/93/105, OAW-RAP2, OAW-RAP5, and Omnivista 3600 Air Manager are trademarks of Alcatel-Lucent in the United States and certain other countries.

Any other trademarks appearing in this manual are the property of their respective companies. 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.

OmniVista 3600 Air Manager 8.2.0.3 is a software release that introduces new features, enhancements, and fixes to issues detected in previous releases. For more information about the features described in the following sections, see the *OmniVista 3600 Air Manager 8.2 User Guide*, *OmniVista 3600 Air Manager 8.2 Supported Infrastructure Devices* document, and the *Alcatel-Lucent Instant in OV3600OV3600 8.2 Deployment Guide*.

## Chapter Overview

- "New Features in OmniVista 3600 Air Manager 8.2.0.3" on page 5 describes the new features and enhancements introduced this release.
- "Resolved Issues" on page 33 lists the issues resolved in OV3600 8.2.0.3 and previous releases.
- "Known Issues" on page 37 lists the known issues identified in OV3600 8.2.0.3 and previous releases.

## Contacting Support

Contact Center Online	
Main Site	<a href="http://www.alcatel-lucent.com/enterprise">http://www.alcatel-lucent.com/enterprise</a>
Support Site	<a href="https://service.esd.alcatel-lucent.com">https://service.esd.alcatel-lucent.com</a>
Email	<a href="mailto:esd.support@alcatel-lucent.com">esd.support@alcatel-lucent.com</a>
Service & Support Contact Center Telephone	
North America	1-800-995-2696
Latin America	1-877-919-9526
EMEA	+800 00200100 (Toll Free) or +1 (650) 385-2193
Asia Pacific	+65 6240 8484
Worldwide	1-818-878-4507



This latest release adds improvements to Alcatel-Lucent Instant, PAPI security, and client usage graphs in the WebUI. For more information about these features, refer to the *OmniVista 3600 Air Manager 8.2 User Guide*.

## New Features in OmniVista 3600 Air Manager 8.2.0.3

OmniVista 3600 Air Manager 8.2.0.3 introduces the following new features and enhancements.

### Enhanced Support for Alcatel-Lucent Instant

OmniVista 3600 Air Manager 8.2.0.3 introduces template and Instant GUI configuration (IGC) support for Instant 6.4.2.6-4.1.3.0 and 6.4.2.6-4.1.3.1. Although OV3600 supports template configuration for Instant 6.4.4.4-4.2.4.0, you must manually configure the wired port profile from the Instant command line interface using the **wired-port-profile <profile> [no] trusted** command.

### Security Improvements

Improvements have been made to the PAPI protocol, which is used by OmniVista 3600 Air Manager, Alcatel-Lucent Instant, and Alcatel-Lucent AOS-W for management and control functions.

### Resolution for OmniVista 3600 Air Manager Management Platform Multiple Vulnerabilities

In , the management interface of an underlying system component called RabbitMQ was inadvertently exposed to the network through removal of a firewall rule. Improvements to this management interface resolve the following security CVE-2016-2032.

### Resolution for PAPI Protocol Listener Exposed for Alcatel-Lucent Instant

OV3600 8.2.0.3 now supports Instant 4.1.3.x, which has been improved to not auto-populate firewall rules to permit PAPI when the OAW-IAP is in standalone mode. In non-standalone mode, a new Instant configuration setting has been added to disable auto-population of firewall rules to allow PAPI. When this setting is enabled, PAPI can be selectively permitted or blocked using firewall rules. This improvement resolves .

### Resolution for PAPI Authentication Bypass for Alcatel-Lucent Instant

PAPI messages contain a session ID to ensure that a valid administrative session is logged in to the WebUI. OV3600 8.2.0.3 supports Instant 4.1.3, which includes a security enhancement which prevents an unauthenticated user from using a PAPI vulnerability to execute commands on the IAP, including downloading the complete configuration file. This improvement resolves .

### Resolution for Alcatel-Lucent AOS-W PAPI Vulnerabilities

This release

- MD5 message validation with a key
- Improved PAPI encryption
- Message validation without a common static key for Alcatel-Lucent devices



---

If PAPI security is enabled in OmniVista 3600 Air Manager 8.2.0.3, OV3600 will only process PAPI messages from a controller running Alcatel-Lucent AOS-W 6.5 or later, where the controller PAPI security feature is also enabled.

---

## Resolution for OpenSSL Vulnerabilities

The following OpenSSL vulnerabilities have been resolved:

- Denial of service or other impact using a malformed DSA private key (CVE-2016-0705)
- Denial of service vulnerability against a server which processes public keys, certificate requests or certificates (CVE-2015-1788)

## Linux Security Updates

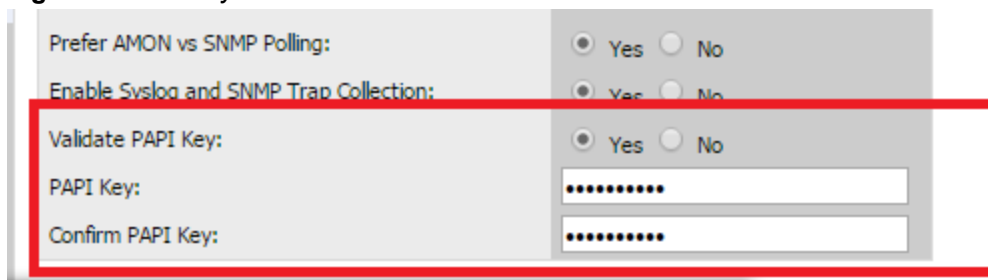
This release supports the following Linux updates:

- nss-util security update (RHSA-2016:0370-1)
- glibc security and bug fix update (RHSA-2016:0175-1)
- kernel security and bug fix update (RHSA-2015:2636-1)
- nss, nss-util, and NSPR security update (RHSA-2016:0591-1)

## Configurable PAPI Key

Previous versions of OV3600 supported only a single PAPI security key for all Alcatel-Lucent devices. Security improvements in this release allow you to specify a custom PAPI key and require PAPI key validation. You configure these settings on the **OV3600 Setup > General > Additional OV3600 Service** page.

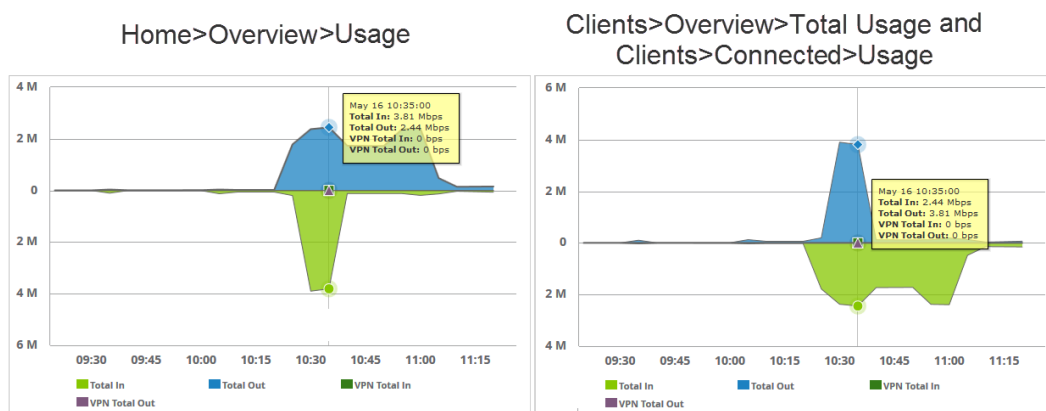
**Figure 1:** PAPI key validation



## Client Usage Graph Improvements

OV3600 8.2.0.3 improves client usage graphs on the **Clients > Connected** and **Clients > Overview** pages of the OV3600 WebUI. These improvements include using consistent labels for inbound and outbound traffic, called PAPI key and Total Out, and a similar axis for both graphs.

**Figure 2:** Client Usage graph improvements



In the graph on the left, Total In and Total Out represents data going to the AP and leaving the AP, respectively. In the graph on the right, Total In represents the traffic going in to the client; Total Out represents data going from the client to the AP.











## High Availability of APs

OV3600 8.2 introduces support for pairs of HP Unified Wired-WLAN (UWW) devices operating in HA mode. OV3600 will monitor the status of each controller. After OV3600 detects that a failover occurred and the APs failed over to the backup controller, OV3600 properly displays the status of the APs.

## Updated User Interface

OV3600 8.2 introduces an updated user interface. The statistics toolbar at the top of the OV3600 window uses new icons to display network health data. Click any of these icons to view detailed information for each user or device category.

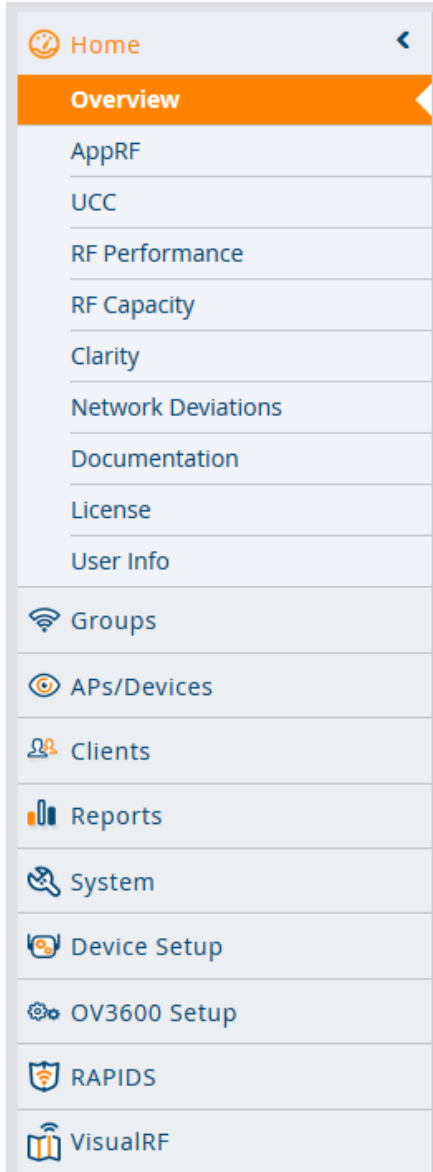
**Table 1:** Network Statistics Icons

Icon	Description
	Number of APs, controllers and switches that have not yet been authorized and added to OV3600
	Number of active APs, controllers and switches seen by OV3600. This icon can represent active wired and wireless <b>devices</b> , or just <b>active</b> wireless devices. To select which statistic (wired and wireless, or just wireless) is represented by this icon, modify the icon settings at the <b>OV3600 Setup &gt; General &gt; Top Header</b> .
	Number of inactive APs, controllers and switches seen by OV3600. This icon can represent inactive wired and wireless devices, or just active wireless devices. To select which statistic (wired and wireless, or just wireless) is represented by this icon, modify the icon settings at the <b>OV3600 Setup &gt; General &gt; Top Header</b> .
	Number of active wired devices that have not yet been authorized and added to OV3600.
	Number of inactive wired devices seen by OV3600.
	Number of mismatched devices. A device is considered to be mismatched if the settings on the device are different than the group configuration settings for the device stored in the OV3600 database.
	Number of rogue devices detected on the network.
	Number of WLAN clients seen by OV3600.
	Number of VPN clients or VPN sessions seen by OV3600. To select which statistic (clients or sessions) is represented by this icon, modify the displayed icon settings on the <b>OV3600 Setup &gt; General &gt; Top Header</b> fields.
	Number of OV3600 alerts.

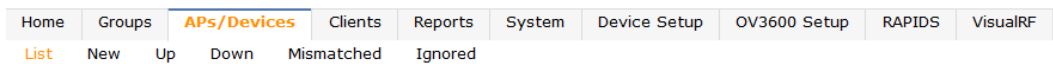
The navigation menu now appears on the left side of the browser window in a collapsible navigation bar that you can hide or display by clicking the arrow in the upper right corner of the toolbar. This navigation menu contains the same menu options in the same order as before.

Figure 3 shows the location of the **APs/Devices > New** subheading in OV3600 8.2, and Figure 4 shows the **APs/Devices > New** subheading in an earlier version. Note that the top level headings and subheadings remain in the same relative locations in the new UI.

**Figure 3:** Left Navigation Menu in OV3600 8.2



**Figure 4:** Top Navigation prior to OmniVista 3600 Air Manager 8.2



## Clarity Monitoring

The Clarity Monitoring dashboard shows the progress of a client as it completes the following four steps to gain access to the WLAN:

- Associating to the network
- Completing authentication
- Obtaining an IP address via DHCP
- DNS resolution

OV3600 receives this data via AMON messages sent from the switches on the network.



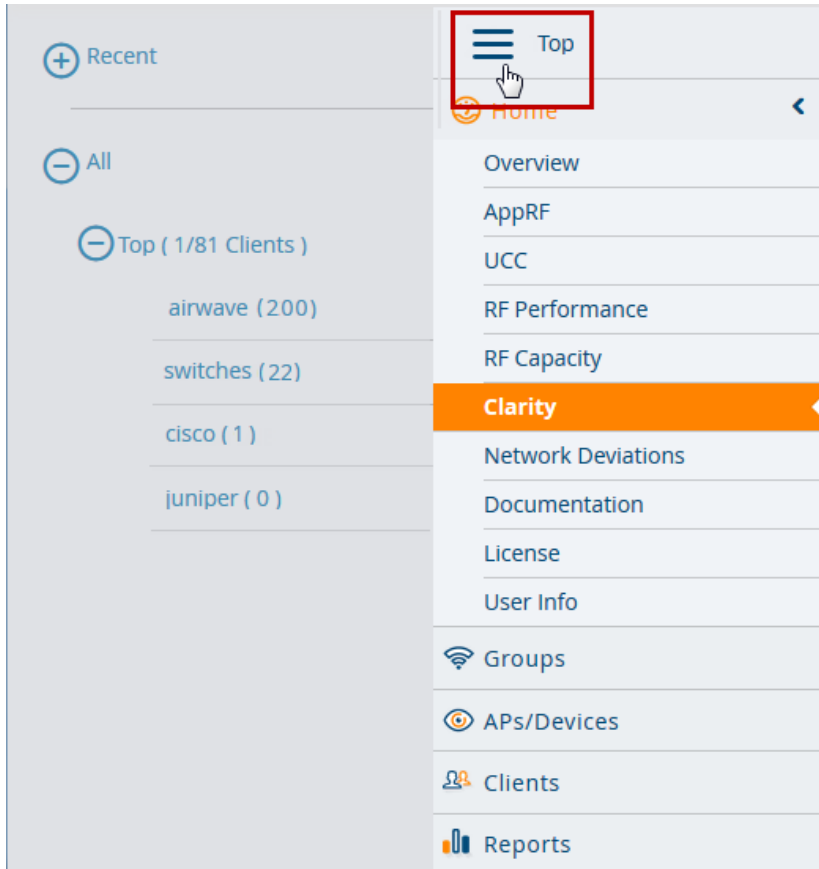


Clarity monitoring is a beta feature in OV3600 8.2, and is supported by switches running AOS-W 6.4.3 and later releases.

The Clarity dashboard contains graphs and tables to help you identify failures in each step of the process. The default view for the Clarity monitoring page displays data for all devices connecting to the WLAN during the previous two hours. You can drill down and view data for devices associating to APs in a specific subfolder, or view data for a different time interval.

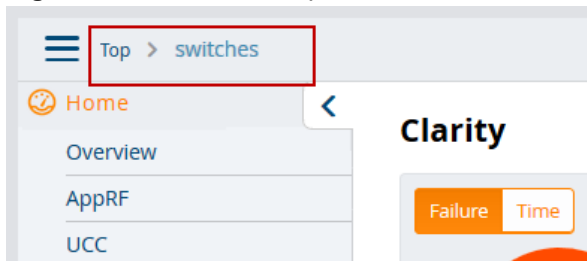
To display Clarity information for devices associated to a specific OV3600 folder, click the Menu icon (☰) in the upper right corner of the Clarity window. This opens a popup window that allows you to select a subfolder.

**Figure 5:** Select a Clarity Folder



The path for the new selected folder appears at the top of the page.

**Figure 6:** Selected Folder path



### Data Time Ranges

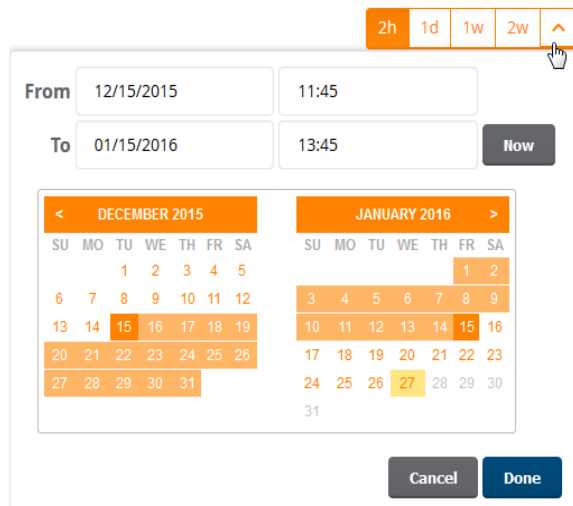
To display Clarity data for the previous day, week, or two weeks, select a time range option at the top of the Clarity monitoring page. The page will immediately refresh and display the updated information.

**Figure 7: Select a Clarity Time Range**



To select a custom time range, click the down arrow on the end of the time range toolbar. This option opens a popup window that allows you to define custom start and end times for your Clarity data tables.

**Figure 8: Select a Clarity Custom Time Range**



Clarity can be configured to retain server statistics for up to thirty days, and retain client statistics for up to seven days. To modify the default retention intervals (seven days of server statistics and two days of client statistics), navigate to **OV3600 Setup > General > Historical Data Retention**, and enter new values in the **Clarity Server Stats Retention Interval** and **Clarity Client Stats Retention Interval** fields.

## Clarity Graph and Table Data

The Clarity page includes the following graphs and tables.

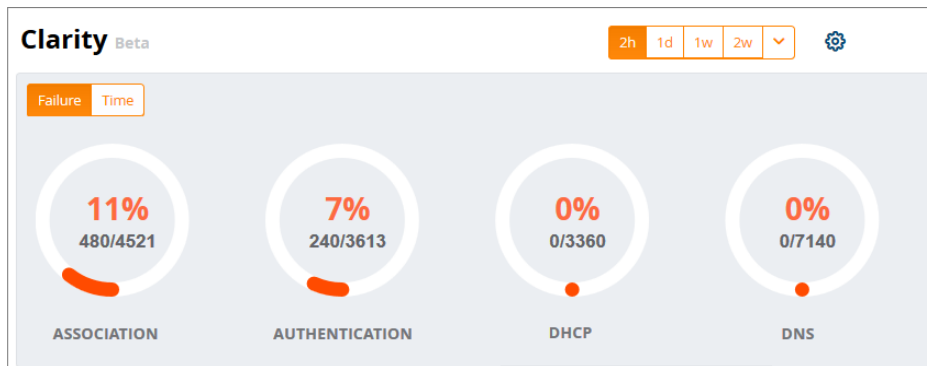
- "Live Statistics Dashboard" on page 10
- "Summary Table" on page 11
- "Authentication Failure Data" on page 12
- "DHCP Failure Data" on page 12
- "DNS Failure Data" on page 13
- "Association Data" on page 13

By default, each Clarity table displays entries for 25 devices or folders with the lowest performance levels. The clarity To display additional Clarity information for each table, or for information on modifying and sorting Clarity tables, see "[Modifying Clarity Thresholds](#)" on page 13

### Live Statistics Dashboard

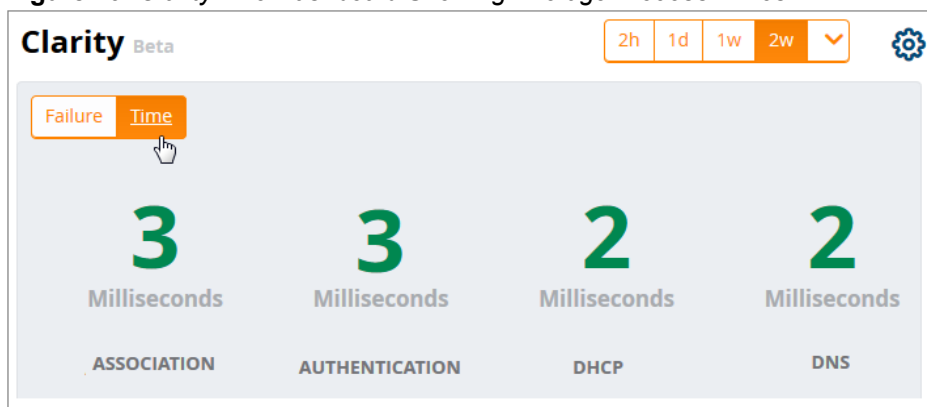
The **Live** statistics dashboard displays information for the failures in each process as a client associates and authenticates to the network, receives an IP address via DHCP, and resolves the IP address to a hostname via a DNS server. When you navigate to the **Home > Clarity** page, the **Live** dashboard displays the percentage of failures for each process, the number of failures, and the total number of attempts (both failed and successful) over the selected time period, as shown in [Figure 9](#).

**Figure 9: Clarity Live Dashboard Showing Failure Rates**



To display the average process times over the selected time interval, click the **Time** option in the upper left corner of the dashboard, as shown in Figure 10.

**Figure 10: Clarity Live Dashboard Showing Average Process Times**




### Summary Table

The **Summary** table on the **Home > Clarity** page is a color-coded dashboard that indicates the health and quality of the association, authentication and DHCP processes over the selected time period. Each icon in the table represents quality thresholds for the number failures *and* the average amount of time it takes the process to complete. The icon color represents aggregate data for failures and process times. For example, if a process has a high failure rate but a good process time, the icon will be red, indicating the most severe threshold crossed in either category. Hover your mouse over any icon to display the number of authentication process failures and successes for clients associating to individual APs or folders of APs, as well as the average time it took for each process to complete.



**Table 2: Default Summary Table Thresholds**

Icon Color	Description	Process Time Thresholds	Failure Rate Threshold
●	Good failure rate <i>and</i> process time	<ul style="list-style-type: none"> <li>Good Association time: &lt;10 ms</li> <li>Good Authentication time: &lt;500ms</li> <li>Good DHCP time: &lt;100 ms</li> <li>Good DNS time: &lt;100 ms</li> </ul>	< 10% failures
●	Fair failure rate <i>or</i> process time	<ul style="list-style-type: none"> <li>Fair Association time: 10 -20 ms</li> <li>Fair Authentication time: 500-1000ms</li> <li>Fair DHCP time: 100 - 200ms</li> <li>Fair DNS time: 100 -200ms</li> </ul>	>10% to 20% failures

**Table 2: Default Summary Table Thresholds (Continued)**

Icon Color	Description	Process Time Thresholds	Failure Rate Threshold
	Poor failure rate <i>or</i> process time.	<ul style="list-style-type: none"><li>Poor Association time: &gt;20 ms</li><li>Poor Authentication time: &gt;1000 ms</li><li>Poor DHCP time: &gt;200 ms</li><li>Poor DNS time: &gt;200ms</li></ul>	>20% failures

By default, the **Summary** table displays data for up to 25 subfolders or APs. If the selected Clarity folder contains more than 25 subfolders or APs, the **Summary** table displays only the 25 subfolders and APs with the lowest performance levels.



By default, the **Summary** table displays aggregate data for folders. Click the APs () icon to display information for individual APs. Click the folder icon () to return to the default folder view.

### Authentication Failure Data

The **Authentication** table on the **Home>Clarity** page displays the following information for the client authentication processes on the network.

**Table 3: Authentication Table fields**

Column	Description
Servers	IP address of an authentication server.
Type	Indicates the authentication server type: <ul style="list-style-type: none"><li>Dot1x: 802.1x</li><li>Captive Portal: Captive portal authentication</li><li>MAC Auth:MAC authentication</li><li>WPA-PSK: WPA encryption with pre-shared key (PSK) authentication</li></ul>
Failures (%)	This column shows the percentage of authentication failures for that server, followed by the total number of failures and the total number of authentication attempts over the selected time interval.
Avg. Time (ms)	The average time it took to successfully complete the authentication process over the selected time interval. Times for both failed and successful attempts are calculated in this average.



Click the graph icon () in the table heading to display of graph of average authentication times for each server during the selected time interval. Hover your mouse over any section of the graph to view details about the authentication times during that portion of the time interval, or click the table icon () to return to the table view.

### DHCP Failure Data

The **DHCP** table on the **Home > Clarity** page displays the following information for authentication on the network.

**Table 4: DHCP Table fields**

Column	Description
Servers	IP address of a DHCP server.
Avg. Time (ms)	The average time it took to successfully complete the DHCP provisioning process over the selected time interval. Times for both failed and successful attempts are calculated in this average.



Click the graph icon () in the table heading to display of graph of DHCP times for each server during the selected time interval. Hover your mouse over any section of the graph to view details about the DHCP provisioning times during that portion of the time interval, or click the table icon () to return to the table view.

### DNS Failure Data

The **DNS** table on the **Home > Clarity** page displays the following information for DNS resolution attempts.

**Table 5:** *DNS Table fields*

Column	Description
Servers	IP address of a DNS server.
Failures (%)	This column shows the percentage of DNS resolution failures for that server, followed by the total number of failures and the total number of DNS resolution attempts over the selected time interval.
Avg. Time (ms)	The average time it took to successfully complete the DNS resolution process over the selected time interval. Times for both failed and successful attempts are calculated in this average.



Click the graph icon () in the table heading to display of graph of DNS resolution times for each server during the selected time interval. Hover your mouse over any section of the graph to view details about the resolution times during that portion of the time interval, or click the table icon () to return to the table view.

### Association Data

The **Association** table on the **Home > Clarity** page displays the following information for association times and failures on the network.

**Table 6:** *Association Table fields*

Column	Description
APs	Name of an AP.
Failures (%)	This column shows the percentage of failed association attempts failures for that AP, followed by the total number of failures and the total number of association attempts over the selected time interval.
Avg. Time (ms)	The average time it took to for a client to associated to the AP over the selected time interval. Times for both failed and successful attempts are calculated in this average.

Click the graph icon () in the table heading to display of graph of association times for each AP during the selected time interval. Hover your mouse over any section of the graph to view details about the association times during that portion of the time interval, or click the table icon () to return to the table view.

### Modifying Clarity Thresholds


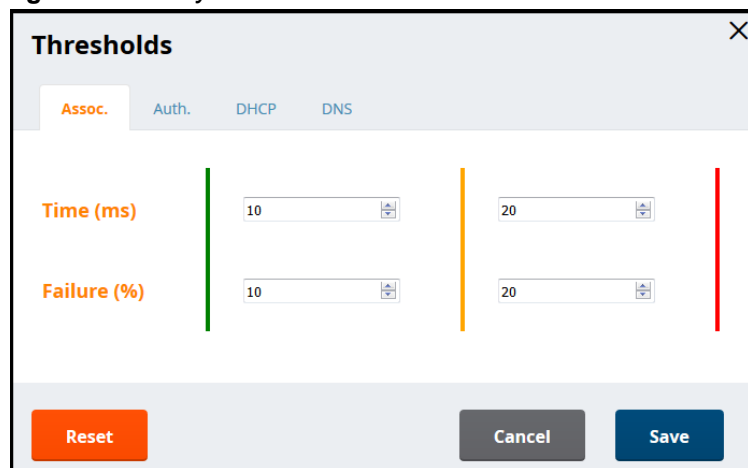
To modify any of the default thresholds for good, fair or poor performance, select the options () icon at the top of the page and specify a new process time or failure count for any threshold. [Figure 11](#) shows the default thresholds for client association times. Modify the numbers in the first column to raise or lower the threshold for a *good* association time or failure rate. Modify the numbers in the second column to raise or lower the threshold for a *poor* association time or failure rate. The values between the two numbers represent the *fair* range of association and failure rate values.

Figure 11: Clarity Association Thresholds



## Sorting and Filtering Clarity Data

Select any column heading in a Clarity table to sort the table by that value.

By default, each Clarity table displays entries for 25 devices with the lowest performance levels. To display additional Clarity data, including entries that do not appear on the main Clarity page:

1. Click the **Details** link at the bottom of a Clarity table. A **Details** popup window appears.
2. Click the **per page** dropdown list in the lower left corner of the window and select the number of entries to be displayed on the page.

You can also select one or more column headings in the **Details** page to sort or filter the table by the selected values.

## Exporting Clarity Data

Click the Menu icon (☰) by a Clarity table titlebar to display the following list of data export options and table display settings.

- **Export all data as csv:** Export the entries currently displayed in the table to a .csv formatted file.
- **Export visible data as csv:** Export all entries recorded for the selected time frame to a .csv formatted file.
- **Export all data as pdf:** Export the entries currently displayed in the table to a PDF.
- **Export visible data as pdf:** Export all entries recorded for the selected time frame to a PDF
- **Details:** Display the details window for the table.
- **Columns:** Click a column heading to hide or display a column in the table.

## Enhanced AppRF Analysis

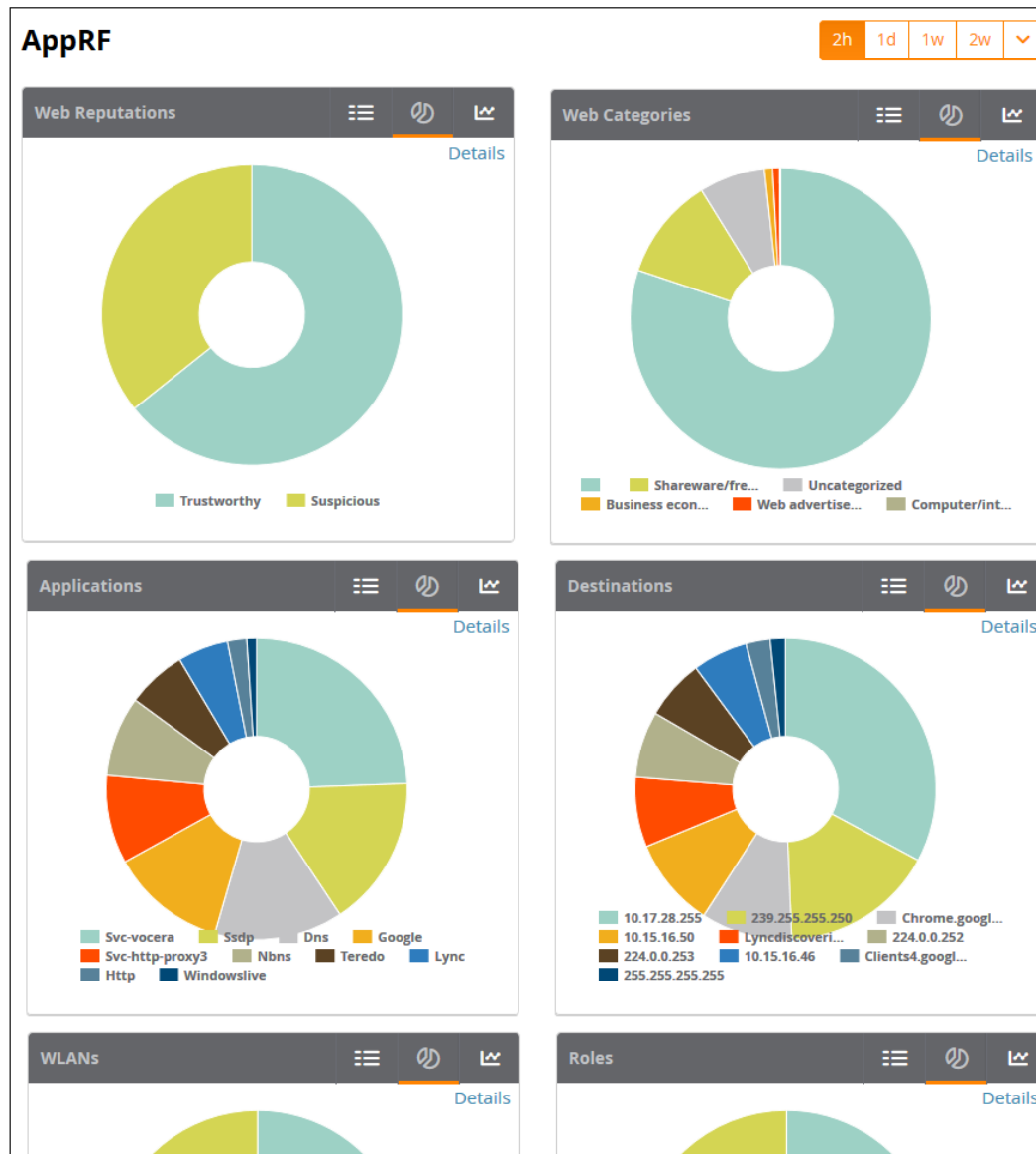
The following enhancements have been made to the **Home > AppRF** page:

- AppRF dashboard
- Widget directives

## AppRF Dashboard

The AppRF dashboard provides a comprehensive overview on the different widgets available for AppRF. Each widget is presented as a directive, with various functions to view in-depth details on the users and applications within a widget.

Figure 12: AppRF Dashboard (Partial)



Each widget contains toggle buttons to switch between the following views:

- - List showing all the categories within the widget
- - Donut chart representing the proportional usage of categories
- - Usage graph displaying usage (in MB) over time

### Widget Directives

The AppRF dashboard displays each widget as a directive containing the following functions:

- **List:** List of categories available for each specific widget (for example, Application Categories: Social Media, Torrent, Chat Protocols, Games, Web Development Tools, Ad Blocker).
- **Details Link:** Link to the **Details** page, where you can view the following information for each category:
  - **Category:** Name of the user
  - **Bytes:** Total usage in bytes (MB)

- **Packets:** Total number of packets transmitted/received
- **Web Reputation:** Web reputation, indicating the safety of the site.
- **Web Category:** Website type
- **Destination:** Number of destinations reached through the given category
- **User Role:** Number of roles assigned to the user
- **Devices:** Number of devices connected to the given category
- **User Name:** Name of the user
- **Device MAC:** MAC address of the user
- **WLANS:** Number of WLANS to which the user is connected



NOTE

Before you can view **Web Reputation** and **Web Category** information on the **Details** page, you must enable the web content classification feature on the switch, and define a server for name and IP address resolution. To enable these features, access the switch command line interface and issue the commands **firewall web-cc** and **ip name-server**. For more information, refer to the *Alcatel-Lucent AOS-W User Guide*.

- **Category Details:** Under the **Details** page of each widget, you can select a category to view details for the individual category.
- **Donut Chart:** Chart representing the proportional usage of categories within a widget. Hover your mouse above each section of the chart to view the category name and usage, in KB and percentage (%).
- **Usage Graph:** Graph displaying usage over time.

## UCC Enhancements

OV3600 8.2 introduces a number of enhancements to the call details provided on the Unified Communication and Collaboration (UCC) Dashboard.

### UCC Settings in OV3600 Setup

Three new UCC settings have been added to the OV3600 Setup page in the OV3600 WebUI.

- **UCC Call History:** Located in **OV3600 Setup > General > Historical Data Retention**, this setting lets you configure the number of days that calls remain in OV3600's call history. This is set to two days by default.
- **UCC Call Details:** Located in **OV3600 Setup > General > Historical Data Retention**, this setting lets you configure the number of days that the OV3600 retains details for individual calls. This is set to 30 days by default.
- **Enable UCC Calls Stitching (Heuristics):** Located in **OV3600 Setup > General > Additional OV3600 Services**, this setting enables or disables caller-to-callee call stitching for non-SDN deployments. This feature is enabled by default. This should be disabled for NAT and BOC deployments.

### UCC Dashboard Tabs

Two new tabs have been added to the graphs and tables on the UCC dashboard.

- **Call Quality > Folders:** This table lists all folders that carried calls and, for each folder, lists the percentage of calls that were rated as poor by UCC.
- **Quality Correlation > Connectivity:** This table lists the number of calls of each quality level (Good, Fair, Poor, and Unknown) by connectivity type (Wi-Fi Conference, Wi-Fi to External, and Wi-Fi to Wi-Fi).

### UCC Dashboard Filtering

Two drop-down menus have been added to the top-right of the UCC dashboard to provide a way to filter the UCC information presented by the graphs and tables.



- **WLAN or End-to-End:** This drop-down menu includes two options, WLAN and End-to-End. End-to-End is the default setting. When End-to-End is selected, quality information displayed on the dashboard is based on the end-to-end quality of the calls. If WLAN is selected, information displayed is based on the UCC score of the calls. Note that if end-to-end quality information is not available and heuristics is enabled, then WLAN is selected by default.
- **Voice or Other:** This drop-down allows you to filter the information displayed on the dashboard by voice calls or other types of calls. Voice is any voice-only calls, including voice conference calls. Other is any other type of call, such as video, desktop sharing, etc. This options is available to help reduce the amount calls that appear as unknown on the UCC dashboard.

## UCC Call Details

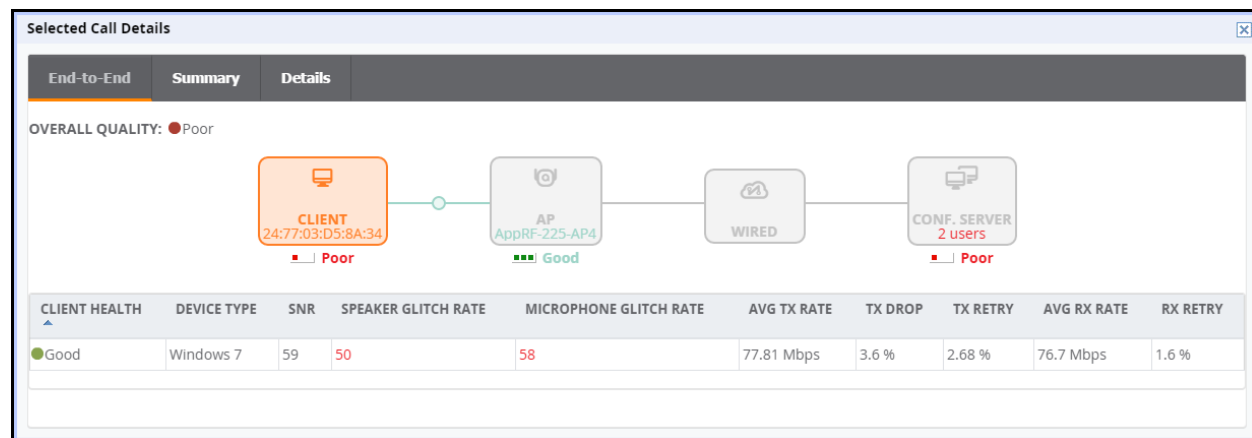
The following new columns have been added to the **Call Details** table found under **Home > UCC > Call Quality > Call Details**:

- **Peer Client:** This field lists client receiving the call if that information is available. If the call type is a conference call, this field is left blank.
- **Device Type:** This field displays the operating system of the client device as a description of the device.
- **Protocol:** The protocol used to complete the call, such as Skype for Business.
- **Connectivity Type:** The method used to facilitate the call, such as Wi-Fi.
- **End-to-End Quality:** This metric is determined by the mean opinion score (MOS) and any device issues that are detected during the call.

## Lync End-to-End Visibility

The Lync End-to-End Visibility features gives the network administrator overall view of a specific call. To view a specific call, navigate to **Home > UCC > Call Quality > Call Details** and click the magnifying glass icon in the **Details** column. This opens up the window shown in [Figure 13](#).

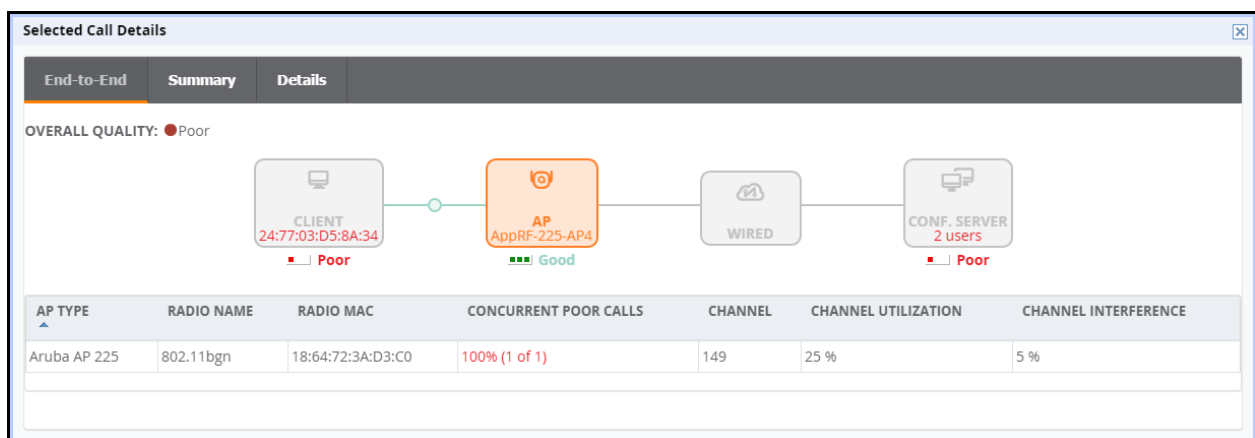
**Figure 13:** Client Detail (End-to-End View)



**Table 7: Client Details**

Metric	Description
Overall Quality	<p>Overall quality is displayed as Good, Fair, or Poor. The quality is determined using the calls UCC Score, a proprietary Alcatel-Lucent metric.</p> <ul style="list-style-type: none"> <li>• Good: score of 71 or greater</li> <li>• Fair: score of 31 to 70</li> <li>• Poor: score of 0 to 30</li> </ul> <p>For more information on the UCC Score, see the <i>OV3600 User Guide</i>.</p>
Client Health	<p>The client health metric compares the actual airtime the AP spends transmitting data is equal to the ideal amount of time required to send data to the client. A client health metric of 50% means the AP is taking twice as long as is ideal, or is sending one extra transmission to that client for every packet. A metric of 25% means the AP is taking four times longer than the ideal transmission time, or sending 3 extra transmissions to that client for every packet.</p>
Device Type	<p>A description of the client device. In the example above, the device is identified by it's operating system; in this case, Windows 7.</p>
SNR	<p>The signal-to-noise ration for the call on the client's connection.</p>
Speaker Glitch Rate	<p>The average number of speaker glitches per five minutes.</p>
Microphone Glitch Rate	<p>Average number of microphone glitches per five minutes.</p>
Avg TX Rate	<p>Displays the average transmission rate of the call in Mbps</p>
Tx Drop	<p>Displays the transmission packet drop in percentage.</p>
Tx Retry	<p>Displays the transmission retry in percentage.</p>
Avg Rx Rate	<p>Displays the average receive rate of the call in Mbps</p>
Rx Retry	<p>Displays the receive retry in percentage.</p>

**Figure 14: AP Details (End-to-End View)**



**Table 8: AP Details**

Column Name	Description
AP Type	The type of AP to which the client is connected.

**Table 8: AP Details (Continued)**

Column Name	Description
Radio Name	The AP's radio being used for the call (802.11bgn or 802.11ac)
Radio MAC	The AP radio's MAC address.
Concurrent Poor Calls	The number of poor calls occurring simultaneously with the call being viewed.
Channel	The channel used for the call.
Channel Utilization	The used channel's utilization as a percentage.
Channel Interference	The interference impacting the used channel as a percentage.

The **Summary** tab provides a more detailed view of the call than the **End-to-End** tab. Much of the information from the **End-to-End** tab is repeated but on this tab it is supplemented with a graph displaying the quality of the call as it progressed. Mousing over the graph displays a pop-up that provides a snap-shot of the call at two-minute intervals, which can help identify when changes occurred during the call.

**Figure 15: Call Summary Information**



At the bottom of the Summary tab, there is a link titled **More**. Clicking this link reveals additional tables that capture more details that can help provide an overall view of many details of the call.

- **Microphone Details** provides information about the client's microphone, such as manufacturer and model, the capture device driver, glitch rate, and audio microphone error.
- **WLAN** repeats some of the information provided on the End-to-End tab but also includes details about WLAN delay, jitter, and packet loss.
- **End To End** provides details about connection between the caller and receiver as it relates the call. This includes information such as MOS, delay, jitter, packet loss, and burst gap details.
- **End Point Details** provides information about the device used by the caller, such as IP address, Wi-Fi device driver, CPU details, and OS.
- **Speaker Details** describes the speaker used by the caller.

The Details Tab provides much of the same information as the graph and tables on the Summary tab but on single table and broken up into two-minute intervals. This provides another more granular look at the call in question.

## Using the UCC Report

The UCC report provides an overall look at UCC activity on your network in the specified time period. This information is displayed in a series of tables representing the top connectivity types, call types, application types, device types, folders, APs, and clients with the highest percentage of poor quality calls.

**Table 9: UCC Report Fields**

Field	Description
Quality Metric	The metric used to determine the quality of calls.
Connectivity Type	The type of connection (such as Wi-Fi to Wi-Fi or Wi-Fi to external) used to complete calls.
Call Type	The type of call, such as voice or video.
Application Type	The software application used to complete a call.
Device Type	The client device used to complete a call. The device type is displayed as the device's operating system.
% of Poor Calls	The percentage of poor calls completed on the specified metric such as device type, application type, etc.
Poor Calls	The number of poor calls completed on the specified metric such as device type, application type, etc.
Total Calls	The total number of calls completed on the specified metric such as device type, application type, etc.
Folders	The device folder from which calls were completed.
APs	The APs that carried calls.
Clients	The clients who completed calls. This is displayed by MAC address and username.
% of Poor Calls by MOS Score	The percentage of poor calls completed by a folder, AP, or client based on the MOS Score.
% of Poor Calls by UCC Score	The percentage of poor calls completed by a folder, AP, or client based on the UCC Score.
Average Client Health (Poor Calls)	The average client health when completing a call.
Total Calls	Total number of calls from a folder, AP, or client.
Total Call Time	Total call time of all calls from a folder, AP, or client.

## Aruba Switch Configuration Through OV3600

OV3600 8.2 introduces smart template configuration support for multiple models of Aruba switches when these devices are running ArubaOS-Switch Version 16.01. [Table 10](#) lists supported switches that include support for template configuration via OV3600.

**Table 10: Aruba Switches (Validated to ArubaOS-Switch Version 16.01)**

Device	Monitoring Support	Firmware Changes	Show Commands On Monitor page	Template Configuration	Stacking Monitoring and Configuration
Aruba 2530YA	Yes	Yes	Yes	Yes	No
Aruba 2530YB			Yes	Yes	No
Aruba 2620			Yes	Yes	No
Aruba 2920			Yes	Yes	Yes
Aruba 3800			Yes	Yes	Yes
Aruba 3810			Yes	Yes	Yes
Aruba 5400R			Yes	Yes	Yes

### Delta Configuration Push

You can use OV3600 template configuration to set or modify individual settings in the configuration profiles listed in Table 11. When you modify any of these profiles on an Aruba switch that supports template configuration, OV3600 does not push a complete configuration file. Instead, OmniVista 3600 Air Manager pushes a set of configuration changes, called a delta configuration, to the switch without requiring a reboot.



Template configuration for Aruba switches is a beta feature in OV3600 8.2, and may be modified in future versions of OV3600.

To set or modify other configuration settings that are not associated with these profiles, you must define a complete switch configuration within the template, then push that entire configuration to the switch. In this instance, all configuration settings are overwritten, and *the switch must reboot to apply those settings*.

**Table 11: Profiles Individually Supported by Template Config**

Profiles	Configuration Examples
Telnet, SSH access	Switch(config)# telnet-server Switch(config)# ip ssh Switch(config)# no ip ssh Switch(config)# no telnet-server
ACLs for Telnet/SSH access	Switch(config)# console inactivity-timer 5 Switch(config)# ip authorized-managers 10.28.227.101 255.255.255.0 access manager
Banner	Switch(config)# banner motd % <b>NOTE:</b> % is the delimiter
Port/Trunk Configuration	Switch(config)# trunk 1/23-1/24 trk1
VLAN Configuration	Switch#config Switch(config)# vlan 200 Switch(vlan-200)# name Datapath Switch(vlan-200)# untagged 1/22

**Table 11: Profiles Individually Supported by Template Config (Continued)**

Profiles	Configuration Examples
SNMP	<pre>Switch(config)# snmp-server community &lt;community_name&gt; restricted Switch(config)# snmp-server contact &lt; contact-info&gt; Switch(config)# snmp-server location &lt;location-info&gt; Switch(config)# snmp-server community "hp-read" operator Switch(config)# snmp-server community "hp-write" unrestricted Switch(config)# snmp-server host x.x.x.x community "lab" trap-level all</pre>
Syslog	<pre>Switch(config)# logging &lt;syslog IP server address&gt;</pre>
Layer-3 VLAN Interface Configuration	<pre>Switch(config)# vlan 200 Switch(vlan-200)# ip address 10.200.200.10 255.255.255.0</pre>
MSTP and RPVST Configuration	<pre>Switch(config)#spanning-tree 1-44 admin-edge-port Switch(config)#spanning-tree bpdu-protection-timeout 3600</pre>
DLDP and UDLD Configuration	<pre>Switch(config)# dldp enable Switch(config)#interface al link-keepalive</pre>
LLDP Configuration	<pre>Switch(config)# lldp refresh-interval &lt;5-32768&gt;</pre>
POE Configuration	<pre>Switch(config)# lldp refresh-interval &lt;5-32768&gt;</pre>
Port Mirroring Configuration	<pre>Switch(config)# mirror-port 2</pre>
QOS Configuration	<pre>Switch(config)# show qos queue-config</pre>
802.1X authentication settings (including MAC, web, RADIUS, and Local MAC, and Captive Portal)	<pre>Switch(config)# radius-server host 10.200.0.32 key HPE-Aruba Switch(config)# aaa authentication captive-portal</pre>

## Viewing and Adding Templates

The following set of tasks describes the procedure to view and add variables to a template. For more information about template configuration, see the *OV3600 User Guide*.

1. Navigate the **Groups > List**, and select a group to which you will add or edit templates. Create a new group by clicking the **Add** button, or edit an existing group by selecting the corresponding pencil icon. The **Groups > Basic** page for that group appears.
2. From the OV3600 navigation pane, select **Templates**. The **Templates** page appears.
3. To create a new template and add it to the OV3600 template inventory, navigate to **Groups > List**, and select the group name. The **Details** page appears.
4. Select **Templates**, and then **Add**.
5. Add template details and variables to complete the configurations, as illustrated in [Figure 16](#)
6. (Optional) Click the **Push complete configuration file** drop-down list and define the configuration push settings for the device by selecting one of three options:

- **Yes:** Select this option to push complete configuration to devices using that template. The device will reboot after the push.
- **No:** Push only a partial configuration to the devices. A reboot is not required for this option.
- **Factory Default Devices only:** Use a complete configuration push only for factory default devices added via the Zero-Touch Provisioning (ZTP) process. A factory default device will reboot after the push. All other devices will use partial configuration push, which doesn't require a reboot. This is the default option.

**Figure 16:** *Groups > Templates*

**Group: HPE Switches**

Name:

Device Type:

Restrict to this version:  Yes  No

Template firmware version:

Push complete configuration file: Device is rebooted after config push

**Template Select**

Fetch template from device:

**Template**

```

; hpStack Configuration Editor; Created on release #KA.
; Ver #0a:59.34.6b.fb.ff.fd.ff.ff.3f.ef:25

%stack_command%
hostname "%hostname%"
no rest-interface
include-credentials
snmp-server community "public" unrestricted
snmpv3 engineid "00:00:00:0b:00:00:3c:a8:2a:47:50:e5"
%oobm_command%
vlan 1
  name "DEFAULT_VLAN"
  untagged %vlan_1_untag_command%
%if use_dhcp=1%
  ip address dhcp-bootp
%endif%
%if use_dhcp=0%
  ip address %ip_address% %netmask%
%endif%
exit
          
```

The following variables may be used in the template. The value of each variable is configured on the APs/Devices Manage page for each device in the group. Each variable must be surrounded by percent signs: %hostname%. The %if...% statements must be terminated by %endif% and cannot be nested. Available Variables:

ap_include_1	is_poe
ap_include_10	location
ap_include_2	manager_ip_address
ap_include_3	netmask
ap_include_4	num_of_a_port
ap_include_5	num_of_b_port
ap_include_6	num_of_normal_port
ap_include_7	oobm_command
ap_include_8	stack_command
ap_include_9	use_dhcp
contact	vlan_1_tag_command
gateway	vlan_1_untag_command
hostname	vlan_1_untag_command
interface_command	vlan_command
ip address	vlan_command

Change credentials the AMP uses to contact devices after successful config push:  Yes  No

## Device Monitoring

OV3600 allows you to execute show commands on some models of Aruba switches by clicking the **Run Command** drop-down list on the **APs/Devices > Monitor** page of the OV3600 WebUI, and selecting a supported show command. (See [Figure 17](#).)

For a list of devices that support show commands via the OV3600 **APs/Devices > Monitor** page, refer to the *OV3600 Supported Infrastructure Devices* document. For complete information about the output of each command, refer to the documentation for that switch.

**Figure 17: Show Commands on an Aruba Switch**

## Zero Touch Provisioning

Zero Touch Provisioning (ZTP) for Aruba switches is delivered through OV3600 via a DHCP server. The following sections describe the procedure to provision an Aruba switch using ZTP.



Some Aruba switches support commands that allow you to view current OV3600 settings or manually configure that switch to associate to an OV3600 server via the switch command line interface. For details on these switch commands (including **amp-server** and **show amp**), refer to the documentation for that switch.

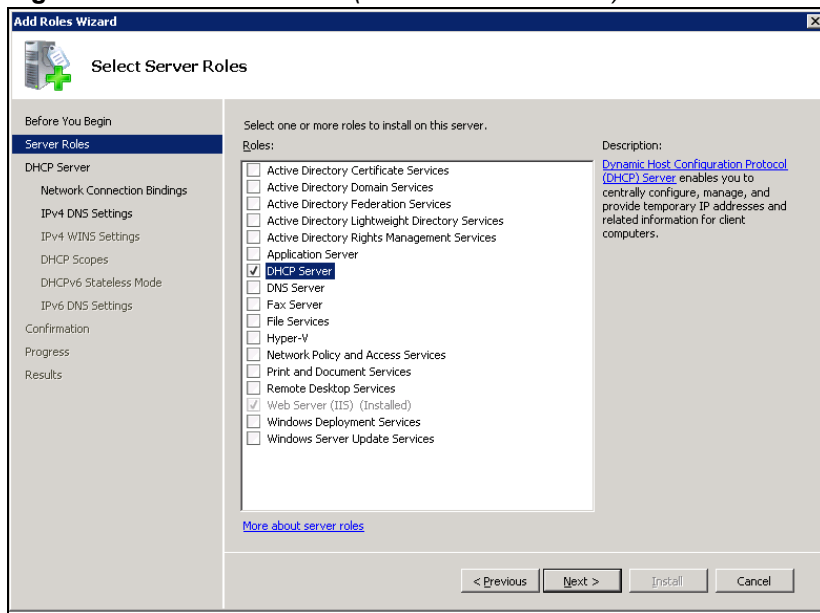
### Configuring the DHCP Server

The DHCP discovery must include a DHCP option 60 (Vendor class identifier) to identify the product brand and model, as well as DHCP option 43 (Vendor specific information).

Use the **Add Roles** wizard on your Windows Server 2008 server to complete the following procedure:

1. Add a DHCP server role.
2. From the Add Roles Wizard window, select **Server Roles > DHCP Server**.

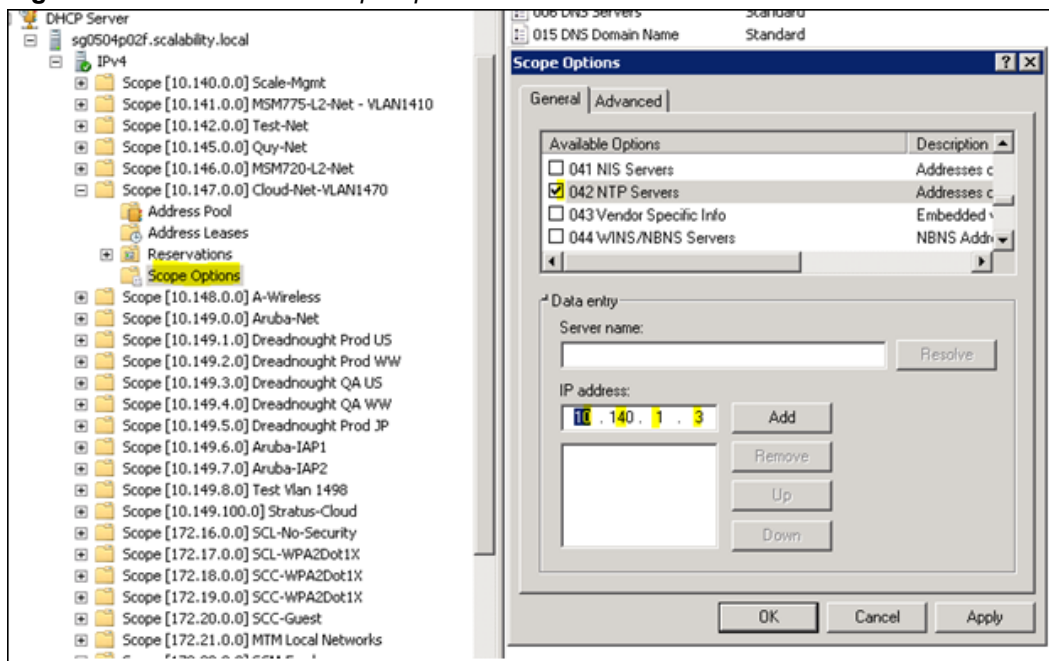
**Figure 18: Add Roles Wizard (Windows Server 2008)**



3. Click **Next**.
4. From the Server Manager window, select **Roles > DHCP Server > the desired domain DHCP Server > IPv4**.
5. Right click **Scope Options** and select **Configure Options**.



Figure 19: Windows 2008 Scope Options

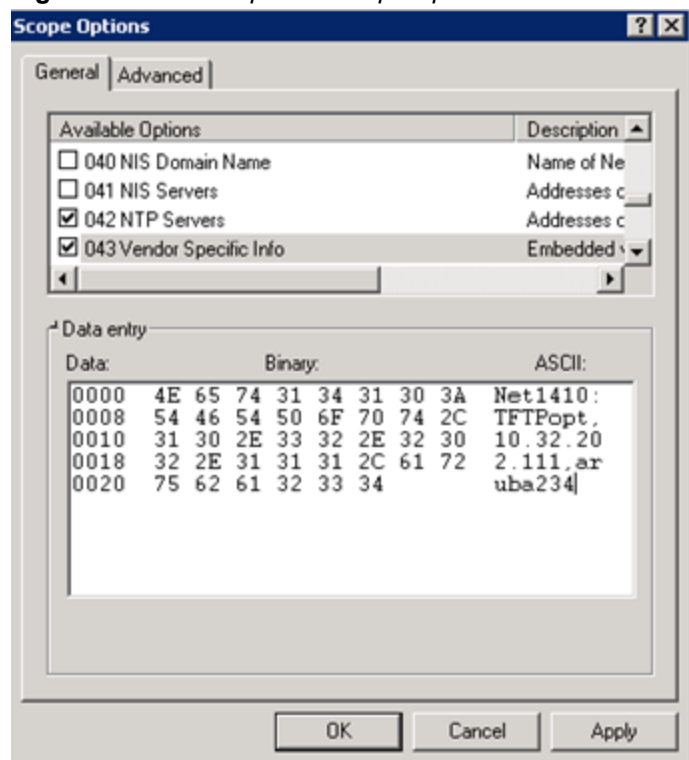


6. Select option **042 NTP Servers** and specify the IP address of the NTP Servers.
7. Click Add.
8. Right click **Scope Options** again and select **Configure Options**.
9. Select option **043 Vendor Specific Info** and specify the following AirWave configuration parameters in the **ASCII** field.

<Group>:<Topfolder>:<folder1>,<AMP IP>,<shared secret>

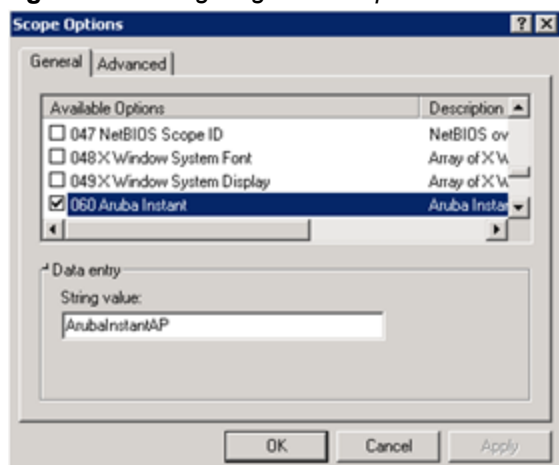
For example, **Net1410;FTTPopt:10.32.202.111,aruba234**

Figure 20: Vendor-Specific Scope Options



10. Click **OK**.
11. Right click **Scope Options** again and select **Configure Options**.
12. Select option **060** and enter the value **ArubaInstantAP** in the **String Value** field.

Figure 21: Configuring DHCP Option 60



13. Click **OK**.

### Configuring OV3600 for ZTP

To configure OV3600 to support ZTP for Aruba switches, complete the following procedure:

1. Add the first device to create the initial configuration (golden configuration). You can do this via DHCP or add the device manually by issuing the command **amp-server ip <ip\_addr> group <group\_name> folder <folder\_name> secret <shared\_secret>** on the switch.
2. Once the device state is UP on OV3600, navigate to **APs/Device > Manage > Device Communication**, enter the Telnet/SSH username and password, then confirm the password.



Before proceeding, verify that your configuration is in a good state.

3. Select the first device in the **APs/Devices > List** page.
4. Navigate to the **APs/Devices > Audit** page for that device.
5. Click the link to the device template on that page to open the **Groups > Templates** page.

**Figure 22: Selecting the Device Template**

DEVICE SETTINGS	
Actual hostname	"HP-2920-Switch"
Actual include-credentials	
Desired hostname	"PoC Switch"
ip default-gateway	10.70.24.11
ip route	0.0.0.0 0.0.0.0 10.70.16.190
module 1 type	39727a

6. In the **Groups > Templates** page, scroll down to the **Credentials** table.
7. In the **Change credentials OV3600 uses to contact devices after successful config push** field, select **Yes**.
8. (Optional) Enter a new Telnet/SSH username and password to change the credentials OV3600 uses to contact the devices.
9. Navigate to **OV3600 Setup> General > Automatic Authorization**.
10. In the **Automatically Authorized Switch Mode** field, select the **Manage Read/Write** option.
11. When you power on additional factory-default devices that match the same group and shared secret as the "golden config" device, those devices are automatically authorized, and receive their configuration information. The devices then reboot and up comes back up with a good configuration state.

## Improved CAD Import

OV3600 8.2 introduces an enhancement to the importation of CAD (.dwg) files. When importing a CAD file to VisualRF, you are now given the option to define CAD layers as walls on your floor plan.

Beginning in 8.2, after uploading a CAD file, there is a new step on the Define New Floor page called CAD Layer. VisualRF generates a list of the layers in the uploaded CAD file. Any of the layer can then be defined as walls on the floorplan.

To define a layer as walls, complete the following steps:

1. Check the checkbox to the left of the layer name to define it as walls.
2. Select the type of wall using the options in the drop-down list to the right of the layer name.
3. Click Next to continue defining the floor plan



Each floor plan is limited to 200 walls.

Figure 23: CAD Layer - VisualRF



## Alcatel-Lucent switch Configuration Enhancements

The following additions have been made to OV3600's switch configuration options to support AOS-W6.4.3.1. See the latest AOS-W User Guide and CLI Guide for more information about each of these new fields.

- **ARM Profile: Client Match 11v BSS Transition Management** enables client match using 802.11v BSS Transition Management; this value is enabled by default. **Client Match IOS Steer Backoff Interval** sets the backoff interval (in seconds) between IOS steering attempts.
- **IKE Profile** and **Site to Site IKE Profile**: Support added for **Configure Hex Key** and **Disable IP COMP**(Site to Site IKE only) under **Advanced Services > VPN Services > Site to Site IKE** for switches running AOS-W 6.4.3.0 and later.
- **Virtual AP Profile**: Supported added for **WAN Operation** under the **Virtual AP Profile**. This specifies the wan-operation to enable Virtual AP depending on the state of the WAN link. The default value is always but can be changed to backup or primary.
- **AAA Profile**: Support added for **Open SSID Radius Accounting** and **Max IPv4 for Wireless User**. **Open SSID Radius Accounting** initiates RADIUS accounting as soon as the user associates to an Open SSID without any authentication; disabled by default. **Max IPv4 for Wireless User** specifies the number of IPv4 addresses that can be associated to single wireless user; the default value is two (2).
- **Web SSH Management Profile**: The following fields have been added to the Web SSH Management profile page.
  - **Bypass Captive Portal Landing Page**: if disabled, the controller uses the new redirection scheme also known as the landing page by default including the meta tag. This can reduce the CPU load on the controller. The controller falls back to the old redirection scheme if this parameter is enabled. Disabled by default.
  - **Configure Lync Listen Port Access**: Configures the port number on which the Skype4B plug-in sends HTTP/HTTPS messages to the Alcatel-Lucent switch.
  - **TLS Protocol, TLS Protocol 1.1, TLS Protocol 1.2**: Enables the TLS protocol version.
  - **IDP Certificate**: Specifies the IDP certificate name configured in the controller.
- **Session Access List**: web-cc-category and web-cc-reputaion are now supported services types.

- **IPSEC Transform Set Profile:** GCM encryption does not support hash algorithms from AOS-W 6.4.3.1 or later.
- **AP System Profile:** The **GRE Striping IP** field has been removed from the **AP System Profile**.
- **Netservice Profile:** Fields for **http-proxy** and **https-proxy** have been added to the **Netservice Profile** to configure the application access level.
- **Management Config:** New options have been added to the **Management Config** profile to **Disable Inline DHCP Stats**, **Disable Inline AP Stats**, **Disable Inline Auth Stats**, and **Disable Inline DNS Stats**. These options are set to **No** by default.

## VisualRF UI Changes

The OV3600 8.2 VisualRF feature only supports the HTML5-based UI. OV3600 8.2 has deprecated the **Enable HTML5-based UI** setting added to the the **VisualRF > Setup > Server Settings** page in OV3600 8.0, removing the option to toggle between the legacy flash-based UI and the newer HTML5 UI.

The legacy flash-based VisualRF UI allowed users to add a wiring closet to a floor plan or create a client survey. If you created a wiring closet or client survey in a previous release, this information is still be displayed in OV3600 8.2, but cannot be modified.



OmniVista 3600 Air Manager provides a range of features to manage network infrastructure devices from Alcatel-Lucent and other vendors. OV3600 introduces support for the following Aruba and Hewlett Packard Enterprise products.

For a complete list of supported products from other vendors, see the *OmniVista 3600 Air Manager 8.2 Supported Infrastructure Devices* document. You can find this document at <https://service.esd.alcatel-lucent.com>.

### New Supported Devices

OV3600 introduces support for the following wireless access points, switches and access point module:

- OAW-AP324 and OAW-AP325 Alcatel-Lucent access points
- OAW-AP324 and OAW-AP325; Alcatel-Lucent Instant access points 4.2.4 (template configuration only)

### Instant Support

OV3600 8.2.0.3 supports Alcatel-Lucent OAW-IAPs running Instant 6.4.4.4-4.2.4.0 and prior versions, including the management of configuration settings and software upgrades. The following table shows when each new version of Instant was initially supported in OV3600.

**Table 12:** *OmniVista 3600 Air Manager Support for Instant*

Instant Version	Support for Template Configuration	Support for IGC configuration
Instant 4.2.4	OmniVista 3600 Air Manager 8.2.0.3*	N/A
Instant 4.2.3	OmniVista 3600 Air Manager 8.2	OmniVista 3600 Air Manager 8.2, with the Instant 4.2.1 UI
Instant 4.2.2	OmniVista 3600 Air Manager 8.2	OmniVista 3600 Air Manager 8.2, with the Instant 4.2.1 UI
Instant 4.2.1	OmniVista 3600 Air Manager 8.0.10.0	OmniVista 3600 Air Manager 8.0.10.0
Instant 4.2	OmniVista 3600 Air Manager 8.0.9	OmniVista 3600 Air Manager 8.0.9
Instant 4.1.3.1	OmniVista 3600 Air Manager 8.2.0.3 and 8.0.11.2	OmniVista 3600 Air Manager 8.2.0.3 and 8.0.11.2
Instant 4.1.3	OmniVista 3600 Air Manager 8.2.0.3 and 8.0.11.2	OmniVista 3600 Air Manager 8.2.0.3 and 8.0.11.2
Instant 4.1.2	OmniVista 3600 Air Manager 8.0.9	OmniVista 3600 Air Manager 8.0.9
Instant 4.1.1	OmniVista 3600 Air Manager 8.0.4	OmniVista 3600 Air Manager 8.0.4
Instant 4.1	OmniVista 3600 Air Manager 8.0	OmniVista 3600 Air Manager 8.0.4
Instant 4.0	OmniVista 3600 Air Manager 8.0 and OmniVista 3600 Air Manager 7.7.10	OmniVista 3600 Air Manager 7.7.8

**Table 12:** *OmniVista 3600 Air Manager Support for Instant (Continued)*

Instant Version	Support for Template Configuration	Support for IGC configuration
Instant 3.4	OmniVista 3600 Air Manager 7.7.3	OmniVista 3600 Air Manager 7.7.8
Instant 3.3	OmniVista 3600 Air Manager 7.6.4	OmniVista 3600 Air Manager 7.7.8
Instant 3.2	OmniVista 3600 Air Manager 7.6.1	OmniVista 3600 Air Manager 7.7.5
Instant 3.1	OmniVista 3600 Air Manager 7.5.6	N/A
Instant 3.0	OmniVista 3600 Air Manager 7.5	N/A

\*OmniVista 3600 Air Manager 8.2.0.3 supports template configuration for Instant 6.4.4.4-4.2.4.0, with the exception of the **wired-port-profile <profile> [no] trusted** command, which must be manually configured using the OAW-IAP command-line interface.



The following tables list issues resolved in OV3600 8.2.0.3 and prior releases.

**Table 13:** *Issues Resolved in OV3600 8.2.0.3*

ID	Description
DE25624	<p><b>Symptom:</b> OmniVista 3600 Air Manager did not generate matching event reports for an AP on the <b>Reports &gt; Detail</b> page although it had connected clients.</p> <p><b>Scenario:</b> This issue occurred when OmniVista 3600 Air Manager skipped AMON messages that didn't contain AP identification information. The method in which OmniVista 3600 Air Manager obtains the identification information for an AP has been changed to resolve this issue.</p>
DE25570	<p><b>Symptom:</b> When VisualRF ran calculations to build the campus grid, it generated large amounts of data which resulted in extremely large backups.</p> <p><b>Scenario:</b> As a result of this issue, VisualRF ran out of memory and crashed. Visual RF now runs calculations in smaller intervals.</p>
DE25448	<p><b>Symptom:</b> Sometimes the Domain Name System (DNS) Resolution graph in the Clarity dashboard wouldn't display.</p> <p><b>Scenario:</b> This graph wouldn't load because of an underlying AOS-W issue, where the DNS samples field populated when it shouldn't. The mechanism for querying the DNS samples measured has been corrected.</p>
DE25419	<p><b>Symptom:</b> Old JRE files remained after an upgrade.</p> <p><b>Scenario:</b> When upgrading from an earlier version of OmniVista 3600 Air Manager, a new JRE installs over itself, leaving JREs from previous installations. You can run a script and select which JRE files to delete. The script is in the <code>/src/x86_64/rpms/Makefile</code> directory.</p>
DE25416	<p><b>Symptom:</b> After upgrading from OmniVista 3600 Air Manager 8.0.11.1 to 8.2.x, the Network view in VisualRF displayed incorrect results on the campus map.</p> <p><b>Scenario:</b> OmniVista 3600 Air Manager 8.2.0.3 fixes an issue where the data migration of pixel width and height didn't work during an upgrade from 8.0.11.x. Campuses no longer overlay each other on the map, and you can drag and drop, or auto arrange items again.</p>
DE25408	<p><b>Symptom:</b> You could not modify the primary, secondary, or tertiary switches from the <b>Cisco Thin AP Settings</b> or the <b>Manage Configuration</b> page.</p> <p><b>Scenario:</b> After upgrading from an earlier version of OmniVista 3600 Air Manager to 8.2.0.1, you couldn't make a selection from the drop down menu, or access the drop down menu. These issues are resolved for all web browsers.</p>
DE25352	<p><b>Symptom:</b> In the Usage graph for connected clients, accessed from the <b>Client &gt; Connection</b> page, the labels and color codings were incorrect.</p> <p><b>Scenario:</b> The information in these graphs, such as color coding, axis direction, and client traffic direction, were changed to match other Usage graphs in the WebUI.</p>

**Table 13: Issues Resolved in OV3600 8.2.0.3 (Continued)**

ID	Description
DE25346	<p><b>Symptom:</b> During an upgrade to OmniVista 3600 Air Manager 8.2.x, the system attempted to upgrade the firmware after exceeding the maximum retries limit.</p> <p><b>Scenario:</b> The system now stops the upgrade when it reaches the maximum retries limit.</p>
DE25320	<p><b>Symptom:</b> The row of statistics hyperlinks, called Top Header Stats, displayed incorrectly.</p> <p><b>Scenario:</b>OmniVista 3600 Air Manager 8.2.0.3 corrects this screen output issue.</p>
DE25312	<p><b>Symptom:</b> Security flaws in the OmniVista 3600 Air Manager 8.0.x release could have caused an application that is compiled against the NSS library to crash, or execute arbitrary code, using the permissions of the user running the application (CVE-2016-1978 and CVE-2016-1979).</p> <p><b>Scenario:</b> OmniVista 3600 Air Manager 8.2.0.3 contains the following Linux security updates, which correct these issues:</p> <ul style="list-style-type: none"> <li>• nss-util security update RHSA-2016:0370-1</li> <li>• glibc security and bug fix update RHSA-2016:0175-1</li> <li>• kernel security and bug fix update RHSA-2015:2636-1</li> <li>• nss, nss-util, and NSPR security update RHSA-2016:0591-1</li> </ul>
DE25310	<p><b>Symptom:</b> AMON messages sent from Alcatel-Lucent AOS-W switches contain timestamps in various formats.</p> <p><b>Scenario:</b> OmniVista 3600 Air Manager 8.2.0.3 resolves this issue by reporting all messages in the <b>Clarity</b> dashboard in milliseconds. In order to view complete Clarity data, upgrade AirWave to 8.2.0.3 and ensure that the controller is running AOS-W 6.4.3.9, 6.4.4.8, or later.</p>
DE25067	<p><b>Symptom:</b> When you deploy an AP in a floor plan, VisualRF doesn't display a heatmap for the AP unless you restart VisualRF.</p> <p><b>Scenario:</b> VisualRF automatically refreshes and displays a heatmap for APs added to a floor plan.</p>
DE24962	<p><b>Symptom:</b> The <b>telnet_cmds</b> log file tracks commands sent between OmniVista 3600 Air Manager and a device using Telnet or SSH and might include passwords and secret data.</p> <p><b>Scenario:</b> Security enhancements in OmniVista 3600 Air Manager 8.2.0.3 prevent these files from being viewed using the WebUI and prevent them from being included in an OmniVista 3600 Air Manager backup file.</p>

**Table 14: Issues Resolved in OV3600 8.2.0.2**

ID	Description
DE25409 DE25378	<p><b>Symptom:</b> Clients associated to an Instant AP correctly appear in VisualRF.</p> <p><b>Scenario:</b> In previous releases of OV3600 8.2.x, IAP clients did not appear correctly in VisualRF floor plans.</p>

**Table 14: Issues Resolved in OV3600 8.2.0.2 (Continued)**

ID	Description
DE25333	<p><b>Symptom:</b> OV3600 processed incoming rogue data and didn't update the AP database correctly.</p> <p><b>Scenario:</b> OV3600 stores this rogue AP data and shows rogue devices accurately in the RAPIDs overview pages.</p>
DE25314	<p><b>Symptom:</b> In the <b>Home &gt; Clarity</b> Monitoring pages of the WebUI, the <b>AP Name</b> column in the <b>AP Summary table</b> and APs column of the <b>AP Association</b> table display the AP name defined by the switch to which that AP is associated.</p> <p><b>Scenario:</b> OmniVista 3600 Air Manager displays the correct AP name sent by the switch in the Clarity monitoring tables and graphs.</p>
DE25260	<p><b>Symptom</b> An issue prevented OmniVista 3600 Air Manager 7.7.14 from upgrading to earlier releases of OmniVista 3600 Air Manager 8.2.x.</p> <p><b>Scenario:</b> This issue is resolved by changes to the internal installation process that modified the order in which some modules were installed.</p>
DE25429	<p><b>Symptom:</b> The DNS failure graph on the <b>Home &gt; Clarity</b> pages of the WebUI displayed inaccurate DNS data.</p> <p><b>Scenario:</b> Alcatel-Lucent switches running Alcatel-Lucent AOS-W 6.4.4.6 sent continuous server timeout errors. As a result, the DNS failure graphs displayed inaccurate data. This issue has been resolved.</p>
US14749	<p><b>Symptom:</b> The accuracy of Clarity data is improved with a change that allows OV3600 to use VLAN IP addresses to validate the source of the AMON messages sent to the OV3600 server.</p> <p><b>Scenario:</b> This change resolves an issue that allowed the <b>Home &gt; Clarity</b> Monitoring pages to display inaccurate information for the following deployments:</p> <ul style="list-style-type: none"> <li>• In a Master+Master-Standby switch deployment with VRRP and LMS IP set on the switch, AMON AP messages were being sent with the LMS IP, preventing OV3600 from processing them.</li> <li>• If messages were sent from the AP use a different VLAN IP than the switch, OV3600 would not process them correctly.</li> <li>• If the IP address used by a single switch VLAN is defined as the IP address by which OV3600 communicates with the switch, AP station AMON messages sent from any other VLAN IP defined on the switch would not be processed correctly by OV3600.</li> </ul>

**Table 15: Issues Resolved in OV3600 8.2.0.1**

ID	Description
DE25275 DE25251	<p><b>Symptom:</b> An issue is resolved where an OV3600 server upgrading to OV3600 8.2.0 might have insufficient disk space issue to allow the upgrade to completing successfully.</p> <p><b>Scenario:</b> This issue is resolved by changes to the internal upgrade procedures in OV3600 8.2.0.1 that reduced the required disk space for the upgrade.</p>
DE23592	<p><b>Symptom:</b> VisualRF correctly saves grid size modifications to floor plans.</p> <p><b>Scenario:</b> OV3600 8.2.0.1 resolves an issue that prevented VisualRF section of the OV3600 UI from saving modifications to the floor plan grid size property.</p>

**Table 16:** *Issues Resolved in OV3600 8.2*


ID	Description
DE23305	<p><b>Symptom:</b> VisualRF floor plans could display floor plan dimensions in feet, even if VisualRF was configured to display metric units. OV3600 8.2 resolves this issue, and floor plan dimensions are correctly converted from imperial to metric measurements.</p> <p><b>Scenario:</b> This issue was observed when VisualRF settings were changed to display dimensions in metric units.</p>

The tables below lists known issues identified in OV3600 8.2, 8.2.0.2, and 8.2.0.3 releases. There are no known issues in OmniVista 3600 Air Manager 8.2.0.1.

**Table 17:** *Known Issue in OmniVista 3600 Air Manager 8.2.0.3*

ID	Description
DE25598 DE25522 DE25500	<p><b>Symptom:</b> After updating the IP address of the switch, you see syslog error messages listed under device events in the <b>Clients &gt; Detail</b> page and not in the <b>Clarity</b> dashboard.</p> <p><b>Scenario:</b> Underlying issues with Alcatel-Lucent AOS-W caused OV3600 to report only DNS information in the <b>Clarity</b> dashboard.</p> <p><b>Workaround:</b> In order to view complete Clarity data, upgrade OV3600 to 8.2.0.3 and ensure that the switch is running Alcatel-Lucent AOS-W 6.4.3.9, 6.4.4.8, or later.</p>
DE25434	<p><b>Symptom:</b> OV3600 sends hundreds of alerts for high CPU or memory usage.</p> <p><b>Scenario:</b> You might encounter this issue if you configured OV3600 to send alert notification until it is acknowledged.</p> <p><b>Workaround:</b> When adding a trigger on the <b>System &gt; Triggers</b> page, set the Suppress until acknowledge option to Yes.</p>
DE25324	<p><b>Symptom:</b> Upgrading from OV3600 8.0.x caused VisualRF beamwidth, orientation and gain values to reset to their default values.</p> <p><b>Scenario:</b> The beamwidth, orientation and gain values are not retained after flushing the bootstrap file or upgrading the OmniVista 3600 Air Manager server.</p> <p><b>Workaround:</b> None.</p>
DE25226	<p><b>Symptom:</b> OmniVista 3600 Air Manager takes longer to process station statistics AMON messages than it did in OmniVista 3600 Air Manager 8.0.x.</p> <p><b>Scenario:</b> This issue has been associated with the Internet Explorer web browser.</p> <p><b>Workaround:</b> None.</p>

**Table 18:** *Known Issue in OV3600 8.2.0.2*

ID	Description
DE25398	<p><b>Symptom:</b> When you hover your mouse over the configuration () icon on the <b>Groups &gt; List</b> page, the popup window of available actions might not appear in the correct spot, be hidden out of view, or display at the very bottom of the page.</p> <p><b>Scenario:</b> This issue has been associated with the Internet Explorer web browser.</p> <p><b>Workaround:</b> Use another web browser to access the WebUI, or select a group from the <b>Groups &gt; List</b> page and use the navigation bar.</p>

**Table 18:** *Known Issue in OV3600 8.2.0.2 (Continued)*

ID	Description
DE25282	<p><b>Symptom:</b> An OV3600 server running OV3600 8.2.0.x might send random authentication requests to the RADIUS server.</p> <p><b>Scenario:</b> This issue occurs only with RADIUS authentication, where unexpected RADIUS requests are repeatedly sent to the RADIUS server, and continually fail.</p> <p><b>Workaround:</b> None.</p>

**Table 19:** *Known Issues in OV3600 8.2*

ID	Description
DE25324	<p><b>Symptom:</b> VisualRF Beamwidth, Orientation and Gain values on deployed APs automatically reset when you upgrade AirWave to any version, or when you remove the bootstrap file.</p> <p><b>Scenario:</b> The beamwidth, orientation and gain values are not retained after flushing the bootstrap file or upgrading the OV3600 server.</p>
DE25220	<p><b>Symptom:</b> VisualRF indicated an incorrect number of APs associated with the OV3600 server.</p> <p><b>Scenario:</b> In a deployment where over 4,000 APs were associated to an OV3600 server, and the active APs status icon at the top of the WebUI page showed the correct number of APs, VisualRF incorrectly indicated that OV3600 had over 10,000 associated APs.</p>
DE25154	<p><b>Symptom:</b> If an AP upgrades to Instant 4.2.3 and uses Lync applications in its access control rules, Instant GUI Config (IGC) may show a configuration mismatch for that device.</p> <p><b>Scenario:</b> This issue occurs because the list of Lync applications that can be included in an access control rule in the OV3600 8.2 IGC feature differs from the list of available rules in Instant 4.2.3. The following applications are unsupported by IGC in OV3600 8.2.</p> <ul style="list-style-type: none"> <li>• SOS ALG SVP</li> <li>• SOS ALG Vocera</li> <li>• SOS ALG FTP</li> <li>• SOS ALG RTSP</li> <li>• SOS ALG SIP</li> <li>• SOS ALG NOE</li> <li>• SOS ALG SIPS</li> <li>• SOS ALG H323</li> <li>• SOS ALG Facetime</li> <li>• SOS ALG Skype4B Voice</li> <li>• SOS ALG Skype4B Video</li> <li>• SOS ALG Skype4B File-Transfer</li> <li>• SOS ALG Skype4B</li> <li>• SOS ALG SIP-Audio</li> <li>• SOS ALG SIP-Video</li> <li>• SOS ALG Skype4B Desktop-Sharing</li> <li>• SOS ALG Jabber</li> <li>• SOS ALG Jabber-MC</li> <li>• square application</li> <li>• pearsonvue web</li> <li>• squirrelysystems web</li> <li>• learninganalytics web</li> <li>• youtubeeducation web</li> </ul>
DE25110	<p><b>Symptom:</b> If a switch IP address is changed from a static IP address to an IP address dynamically assigned via DHCP, the device may appear as down in OV3600.</p> <p><b>Scenario:</b> This issue is triggered because OV3600 has no way to determine the IP address that will be assigned to the switch after the change to a DHCP-assigned IP address.</p> <p><b>Workaround:</b> Manually change the IP address when the IP provisioning option is changed from static to DHCP.</p>

**Table 19: Known Issues in OV3600 8.2 (Continued)**

ID	Description
<p>DE24785 DE24834 DE24836 DE24872</p>	<p><b>Symptom:</b> When the <b>Groups &gt; Instant Config</b> pages of the OV3600 WebUI are accessed using the Internet Explorer web browser, these pages may not properly display Instant Config (IGC) configuration settings or browser elements, and may not correctly save or update configuration changes.</p> <p><b>Scenario:</b> This issue occurs when you attempt to use Internet Explorer to create or modify a configuration for Instant devices via <b>Groups &gt; Instant Config</b>. This issue does not occur with other supported web browsers.</p> <p>Possible IGC behaviors in Internet Explorer include the following:</p> <ul style="list-style-type: none"> <li>● Drop-down lists may not display properly</li> <li>● Configured settings may not save or update properly</li> <li>● Scrolling down a page in the IGC WebUI may cause the browser to unexpectedly return to the top of the page.</li> <li>● Clicking the <b>Save</b> or <b>Apply</b> button may not save any configuration changes, may cause the browser to unexpectedly return to the top of the page.</li> </ul> <p><b>Workaround:</b> Use an alternate web browser, such as Mozilla, to configure Instant devices.</p>
<p>DE24424</p>	<p><b>Symptom:</b> A non-default <b>Failure Timeout</b> value configured via <b>OV3600 Setup &gt; General &gt; Firmware upgrade/Reboot Options</b> is not correctly applied.</p> <p><b>Scenario:</b> By default, if a firmware upgrade on a switch fails, that switch state is locked, and the switch cannot attempt another upgrade until the default failure timeout period of 60 minutes has elapsed. In OV3600 8.2, if you configure a non-default value for this failure timeout, the switch state may be locked for a time period equal to the default value of 60 minutes <i>plus</i> the new failure timeout period. For example, if you configure a custom failure timeout period of 15 minutes, that setting may keep a switch locked in a pending state for 75 minutes, instead of the expected 15.</p>
<p>DE24417</p>	<p><b>Symptom:</b> Firmware updates on HPE switches may fail when firmware changes are simultaneously sent to switches in a multi-level switch topology, where an upstream switch is located between a downstream switch and the OV3600 server.</p> <p><b>Scenario:</b> This issue occurs when an upstream switch downloads the firmware image and reboots, temporarily disrupting the firmware download on the second, downstream switch. This disruption may cause the firmware upgrade on the second switch to fail.</p> <p><b>Workaround:</b> Perform separate firmware upgrades on switches at different levels. (For example, upgrade the first-level (upstream) switches before you upgrade any second level (downstream) switches.</p>
<p>DE24406</p>	<p><b>Symptom:</b> Backup configurations downloaded from the OV3600 WebUI are not compressed properly, cannot be restored.</p> <p><b>Scenario:</b> This issue occurs when a nightly backup file is downloaded using the Chrome web browser.</p> <p><b>Workaround:</b> Use an alternate web browser, such as Mozilla, to download the backup file.</p>
<p>DE24163</p>	<p><b>Symptom:</b> The <b>Current Secondary Version</b> column in the <b>System &gt; Firmware Upgrade Job Detail &gt; Devices Being Upgraded</b> table displays incorrect image information for an HPE switch.</p> <p><b>Scenario:</b> The <b>Devices Being Upgraded</b> table should display the version number for the software stored in the secondary flash in the <b>Current Secondary Version</b> column. This column may instead display the boot ROM software version.</p> <p><b>Workaround:</b> Access the switch command-line interface and issue the command <b>show flash</b> to view the primary and secondary image versions.</p>

**Table 19: Known Issues in OV3600 8.2 (Continued)**

ID	Description
DE24019	<p><b>Symptom:</b> The <b>Member Switches</b> table on the <b>APs/Devices &gt; Monitor</b> page for an HPE switch may display incorrect stack member information.</p> <p><b>Scenario:</b> If a HPE 3810 stack is discovered via SNMP discovery on the network, and the stack member with commander status is moved to another stack, an invalid stack record may appear in the <b>Member Switch</b> table for members of the original stack.</p> <p><b>Workaround:</b> Adding another stack to the OV3600 server may clear these invalid entries.</p>
DE23592	<p><b>Symptom:</b> VisualRF does not correctly save modifications to floor plans.</p> <p><b>Scenario:</b> When modifying floor plans using the <b>VisualRF</b> section of the OV3600 WebUI, changes to the floor plans settings (like the floor name or number) are not correctly saved.</p> <p><b>Workaround:</b> Re-measure the floor plan to save modifications to the floor plan settings.</p>
DE23289	<p><b>Symptom:</b> VisualRF floor plans do not open correctly for clients accessing the OmniVista 3600 Air Manager WebUI via the Microsoft Edge browser.</p> <p><b>Scenario:</b> When viewing the <b>VisualRF</b> section of the OV3600 WebUI using the Microsoft Edge browser on a Windows 10 client, double clicking on a building or floor does not open the page for that building or floor.</p>
DE23281	<p><b>Symptom:</b> If the <b>APs/Devices &gt; Monitor</b> page for a device displays a VPN IP address, hovering your mouse over that VPN IP address displays a HTTPS and SSH tooltip that contains invalid links.</p> <p><b>Scenario:</b> This issue occurs because the VPN IP address displayed on that page is an internal IP address. Clicking the HTTP link in the tooltip displays a blank page, and on the SSH link does not log a user into any device.</p>
DE19402	<p><b>Symptom:</b> Reports exported via FTP are not sent if the report is modified, as the modified report fails to authenticate to the FTP server.</p> <p><b>Scenario:</b> This issue occurs when you modify an existing FTP report and do not re-enter the FTP server passwords in the <b>Export Options</b> section of the <b>Reports &gt; Definition &gt; Export Options</b> page.</p> <p><b>Workaround:</b> Redefine the FTP server password when you modify a report to be exported via FTP.</p>
US14365	<p><b>Symptom:</b> PVOS commands values are unnecessarily grouped in the device running-config</p> <p><b>Scenario:</b> Some ProVision Operation System (PVOS) commands which are executed individually on the switch appear in a group in the device running-config. OV3600 supports a 1:1 comparison of commands from the template and the device running-config, so this grouping may incorrectly cause the device to show a mismatch.</p> <p>For example, the template may show two separate commands:</p> <pre>loop-protect transmit-interval 10 loop-protect disable-timer 3000</pre> <p>While the running-config groups these into a single line:</p> <pre>loop-protect transmit-interval 10 disable-timer 3000</pre> <p><b>Workaround:</b> Use the grouped command directly in the template to avoid a mismatch.</p>



**Table 19: Known Issues in OV3600 8.2 (Continued)**

ID	Description
US14468	<p><b>Symptom:</b> PVOS commands values may vary between the template and device running-config</p> <p><b>Scenario:</b> When using template configuration to configure Power over Ethernet settings, the template command <b>power-over-ethernet pre-std-detect</b> is modified in the running configuration to add port values. OV3600 supports a 1:1 comparison of commands from the template and the device running-config, so this modification of the value may incorrectly cause the device to show a mismatch.</p> <p>For example, the template may show the command:  <pre>power-over-ethernet pre-std-detect</pre> While the running-config adds port number values  <pre>power-over-ethernet pre-std-detect ports 1-48</pre></p>
US14468	<p><b>Symptom:</b> PVOS commands values may vary between the template and device running-config</p> <p><b>Scenario:</b> When using template configuration for 5400R, 3810, and 3800 ProVision switches, if the template command <b>ip aspath list</b> does not include a sequence number, the running configuration applies a sequence value of <b>5</b>. OV3600 supports a 1:1 comparison of commands from the template and the device running-config, so this modification of the value may incorrectly cause the device to show a mismatch.</p> <p>For example, the template may show the commands:  <pre>ip aspath-list listname deny abcd</pre> While the running-config adds a sequence number to the running configuration:  <pre>ip aspath-list "listname" seq 5 deny "abcd"</pre></p>
US14471	<p><b>Symptom:</b> PVOS commands values may vary between the template and device running-config</p> <p><b>Scenario:</b> On 2530 and 2620 ProVision switches, some ProVision Operation System (PVOS) commands which are executed individually on the switch appear in a modified format in the device running-config, where leading zeros in a configuration value are added or deleted, and hexadecimal values in a template configuration may appear in a decimal value in the running configuration. OV3600 supports a 1:1 comparison of commands from the template and the device running-config, so this modification of the value format may incorrectly cause the device to show a mismatch.</p> <p>For example, the template may show the command:  <pre>qos rate-limit dscp 0 1 kbps 0</pre> While the running-config adds one or more leading zeros to the value:  <pre>qos rate-limit dscp 000000 1 kbps 0</pre></p> <p><b>Workaround:</b> Use the expanded command set in the template to avoid a mismatch.</p>

**Table 19: Known Issues in OV3600 8.2 (Continued)**

ID	Description
US14471	<p><b>Symptom:</b> PVOS commands values may vary between the template and device running-config</p> <p><b>Scenario:</b> On 2530 and 2620 ProVision switches, some ProVision Operation System (PVOS) commands which are executed individually on the switch appear in a modified format in the device running-config, where leading zeros in a configuration value are added or deleted, and hexadecimal values in a template configuration may appear in a decimal value in the running configuration. OV3600 supports a 1:1 comparison of commands from the template and the device running-config, so this modification of the value format may incorrectly cause the device to show a mismatch.</p> <p>For example, the template may show the command:  <pre>qos rate-limit dscp 0 1 kbps 0</pre></p> <p>While the running-config adds one or more leading zeros to the value:  <pre>qos rate-limit dscp 000000 1 kbps 0</pre></p> <p><b>Workaround:</b> Use the expanded command set in the template to avoid a mismatch.</p>
US14471	<p><b>Symptom:</b> Individual PVOS commands values are unnecessarily divided in the device running-config</p> <p><b>Scenario:</b> Some ProVision Operation System (PVOS) commands which are executed individually on the switch appear in multiple lines in the device running-config. OV3600 supports a 1:1 comparison of commands from the template and the device running-config, so this grouping may incorrectly cause the device to show a configuration mismatch.</p> <p>For example, the template may show one individual command:  <pre>ip source-interface all vlan 1</pre></p> <p>While the running-config divides the values from this command into multiple lines:  <pre>ip source-interface tacacs vlan 1 ip source-interface radius vlan 1 ip source-interface syslog vlan 1 ip source-interface telnet vlan 1 ip source-interface tftp vlan 1 ip source-interface snmp vlan 1 ip source-interface sflow vlan 1</pre></p> <p><b>Workaround:</b> Use the expanded command set in the template to avoid a mismatch.</p>
N/A	<p><b>Symptom:</b> Due to a known issue on an HPE switch (CR191863), the switch state does not change from <b>Factory</b> to <b>Non-Factory</b> unless the switch reboots. If OV3600 pushes a partial configuration that does not require a reboot, OV3600 continues to see the switch in the <b>Factory</b> state.</p> <p><b>Scenario:</b> The switch UI page that allows you to fetch a template includes a <b>Push complete configuration file: Device is rebooted after config push</b> option. If a user selects <b>No</b> for this option on a factory-default switch provisioned via a DHCP server, OV3600 only pushes a delta configuration, which does not result in a switch reboot. If a user adds settings via OV3600 that are not supported by OV3600 8.2, the full configuration is not pushed and hence the unsupported commands are not applied on the switch.</p>
N/A	<p><b>Symptom:</b> If a user decides to reset the switch to a factory default state from the switch command-line interface, all stored passwords, security credentials and system settings will reboot in a factory default state.</p> <p><b>Scenario:</b> This issue occurs because OV3600 always executes the <b>include-credentials</b> command when pushing a configuration to a switch.</p>

**Table 19: Known Issues in OV3600 8.2 (Continued)**

ID	Description
N/A	<p><b>Symptom:</b> Unrecognized PVOS command syntax.</p> <p><b>Scenario:</b> OV3600 may not recognize some syntax for some ProVision Operating System (PVOS) commands, and therefore will not allow to users to configure these commands via OV3600.</p>
N/A	<p><b>Symptom:</b> Unrecognized PVOS defaults and values.</p> <p><b>Scenario:</b> OV3600 may not recognize some default values or the "no" syntax for some ProVision Operating System (PVOS) commands, and therefore will not recognize these values when these commands are configured via OV3600.</p> <p>For example, if a template has the command <b>ipv6 hop-limit 100</b>, OV3600 would be expected to push the default value for this command ( 64 hops) if that line is removed from the template. If the default value is missing from the command and not recognized by OV3600, the device could not return to its default value, and a configuration mismatch could occur.</p> <p><b>Workaround:</b> Issue the default value for the command within <b>&lt;push_to_exclude&gt;</b> tags in the template, as shown below.</p> <pre data-bbox="344 783 625 867">&lt;push_to_exclude&gt;     ipv6 hop-limit 64 &lt;/push_to_exclude&gt;</pre>
N/A	<p><b>Symptom:</b> Commands are hidden in the running-config.</p> <p><b>Scenario:</b> Some commands may be hidden by the switch in the running-config and CLI help. Additional steps may be required to add these command settings via template configuration.</p> <p><b>Workaround:</b> Add a hidden command to a device running config by including within <b>&lt;push_to_exclude&gt;</b> tags. For example, to ad the commands <b>crypto key zeroize autorun rsa</b> and <b>crypto key zeroize ssh-client-key</b>, to the template, use the following format:</p> <pre data-bbox="344 1136 808 1247">&lt;push_to_exclude&gt; crypto key zeroize autorun rsa crypto key zeroize ssh-client-key &lt;/push_to_exclude&gt;</pre>

