OmniVista 3600
Air Manager
8.2.11.0

Alcatel·Lucent Enterprise

Release Notes

Copyright

Open Source Code

Chapter 1
Release Overview

OmniVista 3600 Air Manager 8.2.11.0 is a patch release that introduces new features and provides fixes to known issues. Refer to these release notes for the most up-to-date information.

These release notes contain the following chapters:

- "What's New in This Release" on page 4 describes new features in this release.
- "Resolved Issues" on page 14 describes the issues we've fixed.
- "Known Issues" on page 32 describes known issues.
- "Upgrade Instructions" on page 41 describes how to upgrade your software.

Contacting Support

Contact Center Online	
Main Site	https://www.al-enterprise.com/
Support Site	https://businessportal2.alcatel-lucent.com/
Email	ebg_global_supportcenter@al-enterprise.com
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

OV3600 8.2.11.0 introduces new features and fixes to issues detected in previous releases. There are no licensing changes in this release.

NOTE

For a complete list of supported products and validated firmware versions, refer to the *OmniVista 3600 Air Manager 8.2.11.0 Supported Infrastructure Devices*.

Important Changes

OV3600 8.2.11.0 updates the Java Platform Standard Edition 11 (JDK 11).

Support for New Devices

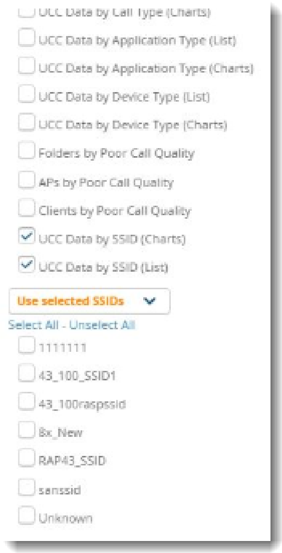
OV3600 8.2.11.0 introduces support for the following devices:

- ArubaOS-CX 6200F switch series with VSF monitoring
- ArubaOS-CX 6300 switch series with VSF monitoring
- Alcatel-Lucent 9012 Switch

New UCC Report Filters

You can now filter UCC reports by SSIDs as shown in Figure 1. To create a UCC report go to **Reports > Definitions**, then click **Add**.

Figure 1: *SSID Restrictions*



□ UCC Data by Call Type (Charts)
□ UCC Data by Application Type (List)
□ UCC Data by Application Type (Charts)
□ UCC Data by Device Type (List)
□ UCC Data by Device Type (Charts)
□ Folders by Poor Call Quality
□ APs by Poor Call Quality
□ Clients by Poor Call Quality
☑ UCC Data by SSID (Charts)
☑ UCC Data by SSID (List)

Use selected SSIDs

Select All - Unselect All

□ 1111111
□ 43_100_SSID1
□ 43_100raspssid
□ 8x_New
□ RAP43_SSID
□ sanssid
□ Unknown

AP Locations for Alcatel-Lucent AOS-W 8.x Switches

OV3600 now displays the AP location for Alcatel-Lucent AOS-W 8.x Switches. This location comes from the **System Location** setting for the Alcatel-Lucent AOS-W 8.x Switch.

Create Activate Credentials Using OV3600

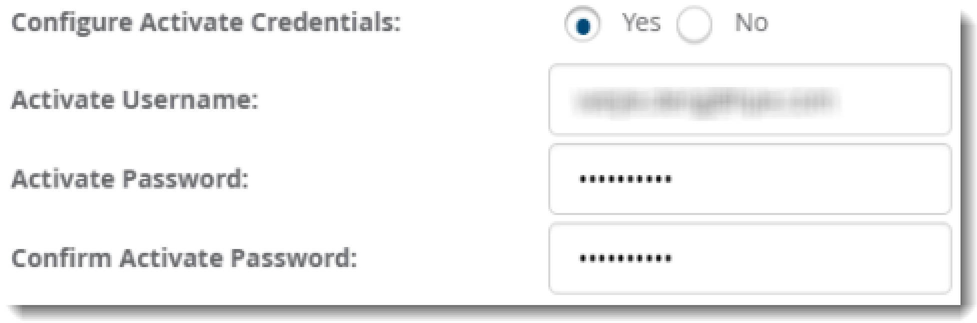
You can now create credentials to log in to the command-line interface or GUI for Activate. You must do this for each OV3600 server that will access Activate. After you save the credentials in OV3600, the Activate user can log in to Activate with these credentials. This feature allows OV3600 to sync the latest firmware from Activate.

NOTE

In order to use this feature, the Activate user must be configured in Activate.

To configure the Activate credentials, go to **OV3600 Setup > General**, then scroll down to **Additional OV3600 Services**.

Figure 2: *Configuring Activate Credentials*



Configure Activate Credentials: ● Yes ○ No

Activate Username: [redacted]

Activate Password: •••••••••••

Confirm Activate Password: •••••••••••

Integrating with an Aruba NetEdit Server

OV3600 supports Aruba NetEdit 2.0.3, the latest release of switching software for managing ArubaOS-CX switches. After you configure OV3600 to integrate with NetEdit, you can launch the NetEdit Network Advisor GUI from the device monitoring page.

To configure the OV3600 server to connect with a NetEdit server:

1. Go to **OV3600 Setup > External Server**, then scroll down the page to locate **Netedit Network Advisor**.
2. Enter the IP address or hostname for the NetEdit server.
3. Click **Save**.

Topology Enhancements

Finding tunneled controllers, switches and APs is easier in OV3600. In Topology, OV3600 displays only common spanning trees associated with a folder in the spanning tree overlay.

When working with Topology:

- Put tunneled controllers, switches and APs into a single folder to simplify how you map these components. If you put them in separate folders, select all folders or none; OV3600 displays the entire topology and all tunnels.
- For more than 2,500 devices, the Topology loading time takes approximately six minutes. Wait for two to three minutes for OV3600 to get the **getTopology** output and calculate the number of edges. When prompted, click **Proceed** so that the Topology page can continue to load which would take three more minutes to complete.

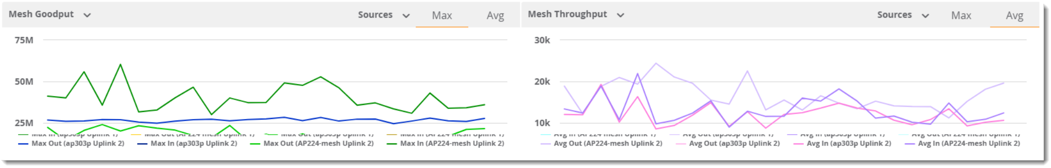
Monitoring Mesh Devices

OV3600 provides a dashboard view of your mesh topology on the **Home > Mesh** page. The **Cluster** dropdown menu allows you to select an available mesh cluster that has devices with mesh portal and mesh point topology.

OV3600 displays counters at the top of the page for **Mesh Portals**, **Mesh Points** and **Mesh Links** for a mesh cluster that you select from the **Cluster** drop-down menu at the top of the page.

The charts use color to display separate statistics for AP uplinks, as shown in Figure 3.

Figure 3: *Mesh Dashboard*

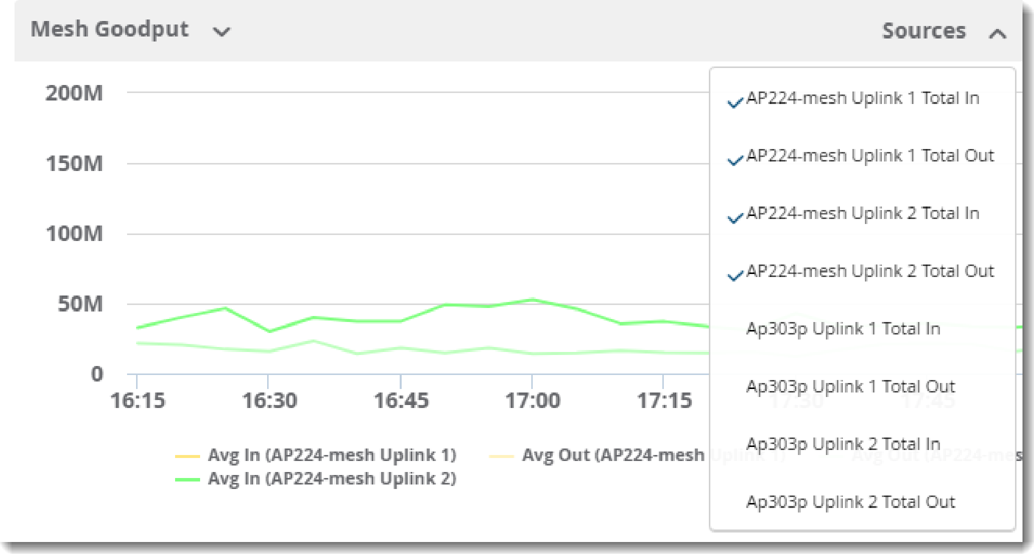


From the dashboard, you can view the following charts:

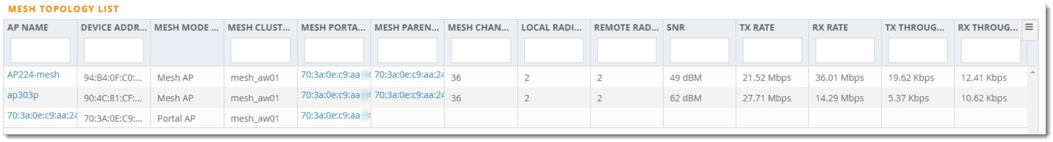
- Mesh Goodput. Shows the average load of traffic flow in and out to an uplink port by source, max, or average.
- Mesh Throughput. Shows the average rate at which traffic flows in and out to an uplink port by source, max, or average.
- Mesh SNR.

You can apply filters to your charts, as shown in Figure 4.

Figure 4: *Results Showing Filters*


Mesh Goodput
Sources
200M
150M
100M
50M
0
16:15
16:30
16:45
17:00
17:15
Avg In (AP224-mesh Uplink 1)
Avg Out (AP224-mesh
Avg In (AP224-mesh Uplink 2)
✓AP224-mesh Uplink 1 Total In
✓AP224-mesh Uplink 1 Total Out
✓AP224-mesh Uplink 2 Total In
✓AP224-mesh Uplink 2 Total Out
Ap303p Uplink 1 Total In
Ap303p Uplink 1 Total Out
Ap303p Uplink 2 Total In
Ap303p Uplink 2 Total Out

Mesh Topology List



MESH TOPOLOGY LIST

AP NAME	DEVICE ADDR...	MESH MODE ...	MESH CLUST...	MESH PORTA...	MESH PAREN...	MESH CHAN...	LOCAL RADI...	REMOTE RAD...	SNR	TX RATE	RX RATE	TX THROUG...	RX THROUG...
AP224-mesh	94:B4:0F:C0:...	Mesh AP	mesh_aw01	70:3a:0e:c9:aa	70:3a:0e:c9:aa:24	36	2	2	49 dBM	21.52 Mbps	36.01 Mbps	19.62 Kbps	12.41 Kbps
ap303p	90:4C:81:CF:...	Mesh AP	mesh_aw01	70:3a:0e:c9:aa	70:3a:0e:c9:aa:24	36	2	2	62 dBM	27.71 Mbps	14.29 Mbps	5.37 Kbps	10.62 Kbps
70:3a:0e:c9:aa:24	70:3A:0E:C9:...	Portal AP	mesh_aw01	70:3a:0e:c9:aa									

Figure 5 describes the Mesh Topology List fields. This table displays all columns by default. Click ☰ at the end of the table to select the fields you want.

Figure 5: *Mesh Topology List Fields and Descriptions*

Field	Description
AP Name	Displays the name of the mesh AP.
Device Address	Displays the MAC address of the mesh AP.
Mesh Mode	Displays whether the AP is configured as a mesh portal or mesh point.
Mesh Cluster	Name of the mesh cluster.
Mesh Portal	The gateway between the wireless mesh network and the enterprise wired LAN. You configure an Alcatel-Lucent AP to perform the mesh portal role, which uses its wired interface to establish a link to the wired LAN.
Mesh Parent	Displays the MAC address of the parent node for the mesh point.
Mesh Channel	Displays the channel used by the mesh cluster.
Local Radio	Radio used by local mesh points.
Remote Radio	Radio used by remote mesh portals.
SNR	Displays the mesh signal-to-noise ratio (SNR).
TX Rate	Displays the transmit data rate on the mesh network.
RX Rate	Displays the receive data rate on the mesh network.
TX Throughput	Displays the transmit throughput on the mesh network.
RX Throughput	Displays the receive throughput on the mesh network.

Traffic Analysis Improvements

OV3600 introduces the following new dashboard tools for:

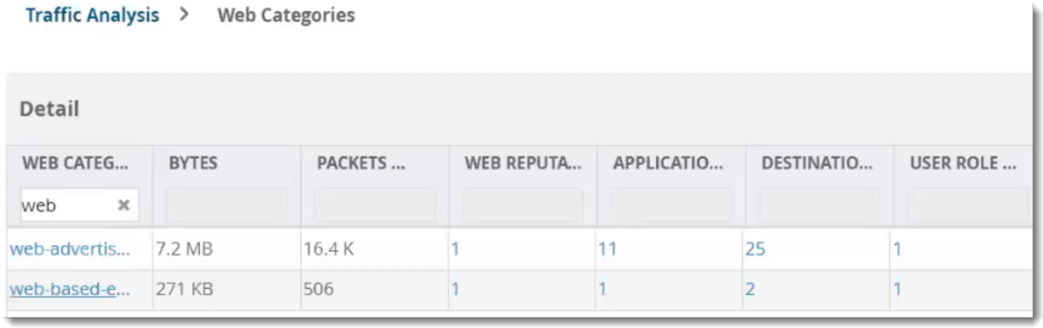
- Finding relevant data using the new search and filter capability
- Exporting traffic analysis data into CSV files
- Viewing dynamically segmented wired client data on the **Client Diagnostics** page

Search and Filter

You can apply filters to your views for all categories for all categories, except for **Web Reputations**.

1. Go to Home > Traffic Analysis, then click on the **Details** hyperlink of any category you want to view.
2. Enter text into the **Search** field.
3. Click 🔍 Filter to apply the filter. OV3600 displays matching results, as shown in Figure 4.

Figure 6: *Results Showing Filters*



Traffic Analysis > Web Categories

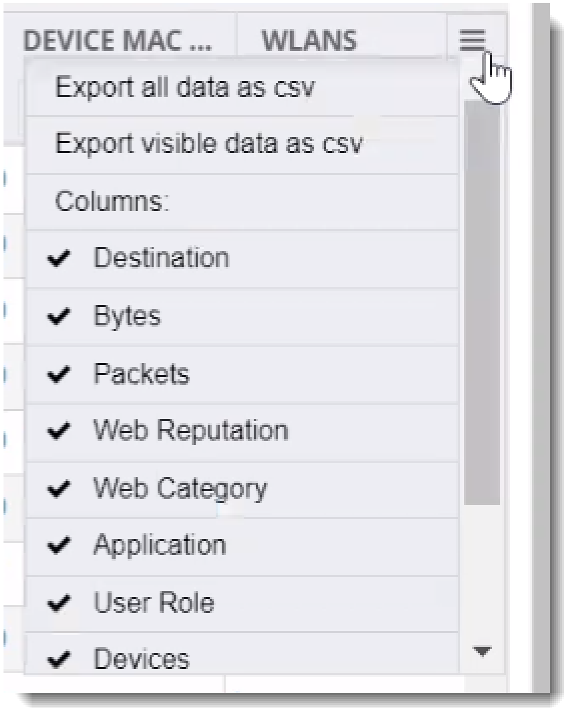
Detail

WEB CATEG...	BYTES	PACKETS ...	WEB REPUTA...	APPLICATIO...	DESTINATIO...	USER ROLE ...
web						
web-advertis...	7.2 MB	16.4 K	1	11	25	1
web-based-e...	271 KB	506	1	1	2	1

Export the Data

You can export all data or filtered data, as shown in Figure 7, Export Options .

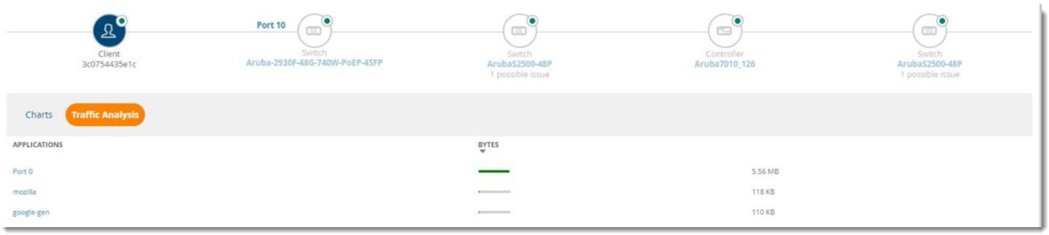
Figure 7: *Export Options*



View Traffic Analysis for Dynamically Segmented Wired Client Data

If you are monitoring a dynamically segmented wired tunnel client, OV3600 displays **Charts** and **Traffic Analysis** on the **Client Diagnostics** page, as shown in Figure 8.

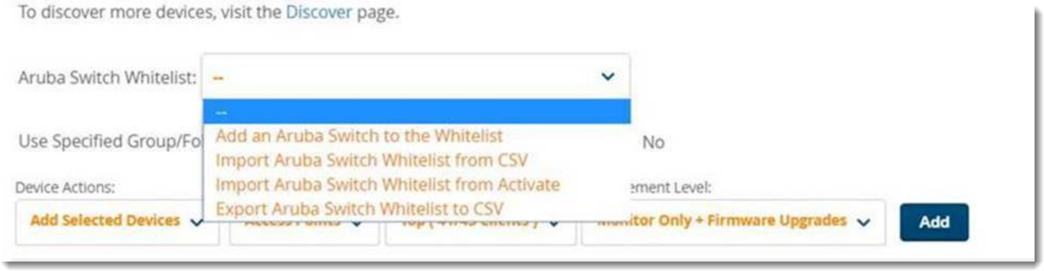
Figure 8: *Client Diagnostics Page*



APPLICATIONS	BYTES	
Port 0	🟩	5.56 MB
mozilla		118 KB
google-gen		110 KB

Configure Separate Whitelists for Instant APs and Aruba Switches

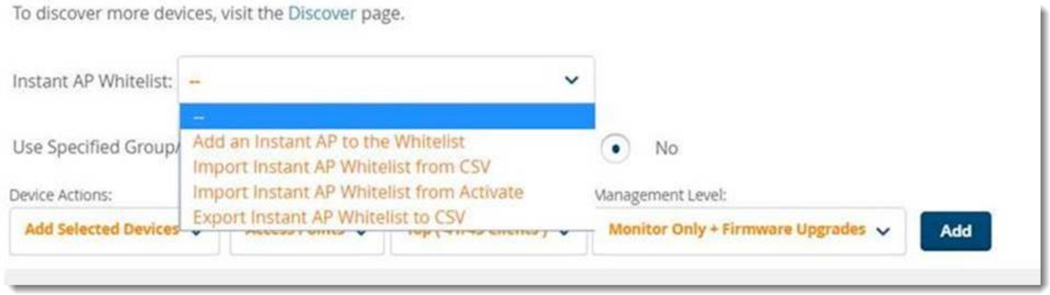
On the **AMP Setup > General** page, now you can configure two separate whitelists for IAPs and Aruba switches. Scroll down to the **Automatic Authorization** section, then select **Whitelist** option for the **Authorize Aruba Instant Aps** or **Authorize Aruba Switches to OV3600** settings. Previously, IAPs and Aruba switches were added to the same whitelist. For more information, see *"Automatic Authorization Settings,"* in the *OV3600 8.2.11.0 User Guide.*



To discover more devices, visit the Discover page.

Aruba Switch Whitelist: --

--
Add an Aruba Switch to the Whitelist
Import Aruba Switch Whitelist from CSV
Import Aruba Switch Whitelist from Activate
Export Aruba Switch Whitelist to CSV
Use Specified Group/Fo
No
Device Actions:
ement Level:
Add Selected Devices
onitor Only + Firmware Upgrades
Add



To discover more devices, visit the Discover page.

Instant AP Whitelist: --

--
Add an Instant AP to the Whitelist
Import Instant AP Whitelist from CSV
Import Instant AP Whitelist from Activate
Export Instant AP Whitelist to CSV
Use Specified Group/
● No
Device Actions:
Management Level:
Add Selected Devices
Monitor Only + Firmware Upgrades
Add

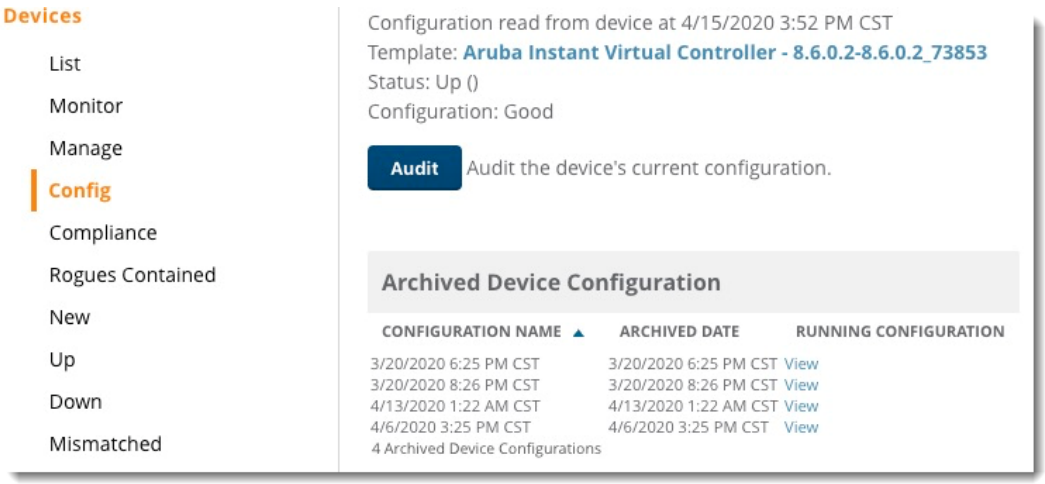
There are several restrictions that apply to this feature when adding and ignoring devices, or replacing device configurations because OV3600 can't distinguish between Instant APs and switches:

- When you add new devices, OV3600 displays a rejection message:
- When you import devices from a whitelist, OV3600 shows whitelisted devices in the Default View on pages that list devices.
- When you push a CLI command to a whitelisted device, OV3600 won't push the command to the device and displays an error message. Select **Ignore** to clear the message. This might occur even though you selected **All** for the **Authorize Aruba Instant Aps** or **Authorize Aruba Switches to OV3600** settings on the **AMP Setup > General** page.
- When you choose to export the whitelist for Instant APs, switches, or combined devices to a CSV, OV3600 exports all the whitelisted devices on the **New Device** page to a CSV regardless of your selection.

Configuration Backups for Instant APs

When a configuration change is made from the WebUI or CLI, OV3600 runs a backup and archives the device configuration on the **Devices > Config** page. You can use the device configuration for audits and data recovery.

Figure 9: *Archived Device Configuration for Instant APs*



Configuration read from device at 4/15/2020 3:52 PM CST
Template: **Aruba Instant Virtual Controller - 8.6.0.2-8.6.0.2_73853**
Status: Up ()
Configuration: Good

Audit the device's current configuration.

Archived Device Configuration

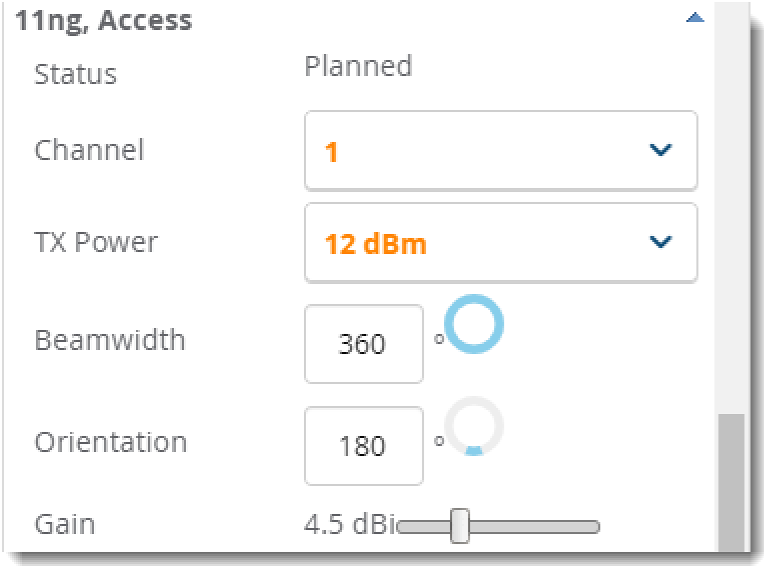
CONFIGURATION NAME ▲	ARCHIVED DATE	RUNNING CONFIGURATION
3/20/2020 6:25 PM CST	3/20/2020 6:25 PM CST	View
3/20/2020 8:26 PM CST	3/20/2020 8:26 PM CST	View
4/13/2020 1:22 AM CST	4/13/2020 1:22 AM CST	View
4/6/2020 3:25 PM CST	4/6/2020 3:25 PM CST	View

4 Archived Device Configurations

Configure the Orientation of APs in VisualRF

OV3600 8.2.11.0 includes the **Orientation** setting to help you with planning and provisioning APs that point downward. Go to the **VisualRF > Floor Plans** page, then click on each network, campus, or building successively to drill down to the floor plan and enter the degree of tilt, as shown in Figure 10.

Figure 10: *Configuring the Orientation*



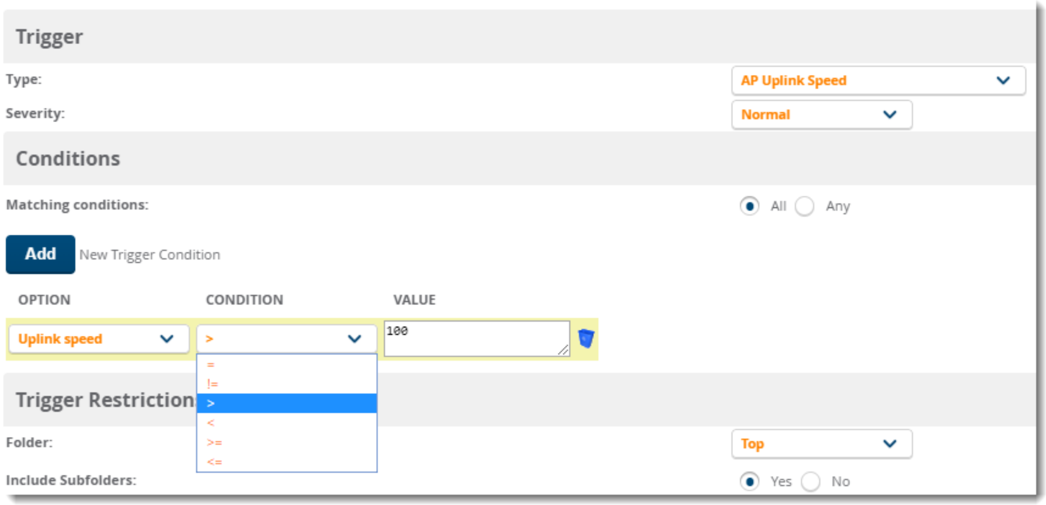
11ng, Access

Status	Planned
Channel	1
TX Power	12 dBm
Beamwidth	360 °
Orientation	180 °
Gain	4.5 dBi

New Device Triggers

You can set up triggers to alert you when there are uplink speed changes on the interface. Figure 11shows an example of a trigger set for an uplink speed greater than 100 Mbps.

Figure 11: *Example AP Uplink Speed Trigger*



Trigger

Type: AP Uplink Speed

Severity: Normal

Conditions

Matching conditions: ● All ○ Any

Add New Trigger Condition

OPTION	CONDITION	VALUE
Uplink speed	>	100

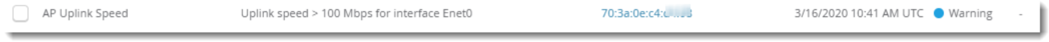
Trigger Restriction

Folder: Top

Include Subfolders: ● Yes ○ No

Figure 12 shows the triggered alert.

Figure 12: *AP Uplink Speed Alert*



□ AP Uplink Speed Uplink speed > 100 Mbps for interface Enet0 70:3a:0e:c4:[redacted] 3/16/2020 10:41 AM UTC ● Warning -

New Clarity Triggers

OV3600 8.2.11.0 includes the following new triggers:

- **Authentication Time**. Generates an alert if the authentication time matches the condition on the AP, client, or authentication server and authentication type (for example, dot1x, captive portal, and MAC address).
- **DHCP Response Time**. Generates an alert if the DHCP response time matches the condition on the client or DHCP server.

To set a trigger for Clarity issues, click the **Type** drop-down list on the **System > Triggers > Add** page, and select one of these health triggers. For more information on creating a new trigger, see the *OV3600 8.2.11.0 User Guide*.

Instant GUI Config Enhancements

OV3600 introduces the following new features:

- Configuring a centralized DHCP scope for L2 and L3 clients
- Configuring MPSK and WPNA3-CNSA

Configuring a Centralized DHCP Scope

To configure a centralized DHCP scope for L2 and L3 clients, go to **Groups > Instant Config**, then click **DHCP** or ⊕ to open the **DHCP Servers** page.

Centralized, L2 Clients

In this mode, the VC bridges the DHCP traffic to the Switch over the VPN or GRE tunnel. The IP address is obtained from the DHCP server behind the controller serving the VLAN or GRE of the client.

1. Enter a name for the DHCP profile.
2. Select **Centralized, L2** for the type of scope.
3. Enter the VLAN ID. Or, disable the **Split tunnel** option to enter a comma-separated VLAN range.

4. If the **DHCP relay** option is enabled, enter the IP addresses of the DHCP server.
5. Optionally, add a **DHCP Option 82** to the DHCP traffic forwarded to the Switch.

Centralized, L3 Clients

In this mode, the VC acts as a DHCP relay agent that forwards the DHCP traffic to the DHCP server located either in the corporate or local network. The centralized, L3 VLAN IP is used as the source IP. The IP address is obtained from the DHCP server.

1. Enter a name for the DHCP profile.
2. Select **Centralized, L3** for the type of scope.
3. Enter the VLAN ID.
4. Optionally, enter the IP addresses of the DHCP server.
5. Enter the centralized, L3 DHCP subnet gateway IP address.
6. Enter the subnet mask of the centralized, L3 DHCP subnet gateway IP address.
7. Select **Alcatel** to enable the **DHCP Option 82**. The format for the Option 82 string, specific to Alcatel, consists of the following:
   - Remote Circuit ID; X AP-MAC; SSID; SSID-Type
   - Remote Agent; X IDUE-MAC

Configuring MPSK and WPNA3-CNSA

To configure these security settings, go to the **Networks** page.

1. Click **+** to add a network.
2. Enter the network name, or SSID, then click **Next**.
3. In the Security tab, select one of the following **Key management** options:
   - **MPSK-AES**. Personal security settings for employee and voice users.
   - **WPA3 Enterprise (CNSA)**. Enterprise security settings for the employee and voice network SSID profiles
4. Select the authentication server.
5. Enter the RADIUS re-authentication interval in minutes.
6. Click **Apply**. OV3600 updates the **Network** page with the network profile.

Security Enhancements

OV3600 8.2.11.0 introduces the following security enhancements:

- You can configure secure logging for syslog servers with TLS encryption.

  Before configuring secure syslogging, make sure that your certificates meet the following requirements:
  - The signed certificate file is generated by a trusted CA, in PEM format, and is present in both the syslog server and syslog client.
  - You upload the generated client certificate, or CA certificate, to OV3600 before you configure the syslog server. This certificate must be named *client-certificate.pem*.

  To configure the syslog server, go to the **AMP Setup > General** page, scroll down to **External Logging** and choose to enable secure logging for the syslog servers.
- OV3600 provides the following new configuration options:
  - Set Lockout Threshold
  - Set Lockout Timer
  - Set Password Length

  - Set Inactivity Threshold for CLI Users
  - Unlock Web Users

  To access these options from the CLI, select **5-5** to open the **Users > Advanced** menu.

- OV3600 logs the certificate signing request (CSR) hash when creating the certificate. Now you can track multiple CSRs for each key pair generated.
- OV3600 supports password and key-based client authentication for SSH clients and provides a way to erase SSH keys.
- OV3600 supports re-keying based on time (one-hour) or data throughput (one GB).
- OV3600 provides a new configuration option to enable a firmware code check.

  From the CLI, select **7-4** to open the **Security** menu and turn on the **Enable Firmware Integrity Check** option.

- OV3600 sets the password for the default Web and CLI administrator user to expire after you complete the installation, forcing a password reset.

Resolved Issues

Issues that have been fixed in OV3600 8.2.11.0, 8.2.10.1, 8.2.10, 8.2.9.1, and 8.2.9.0 are described in the tables that follow.

Table 1: *Issues Resolved in OV3600 8.2.11.0*

Bug ID	Description	Reported Version
DE34121	OV3600 8.2.11.0 fixes an online upgrade running CentOS 7 from OV3600 8.2.11.0 to future versions. To upgrade from OV3600 8.2.10.x, you must contact Technical Support to apply a patch.	OV3600 8.2.10.0
DE34066	Improvements to how OV3600 exports floor plans in .svg format resolves an issue where the background image in these files could appear to be blank when the backup file was restored.	OV3600 8.2.10.1
DE34033	Security improvements in OV3600 8.2.11.0 prevent an issue where a root user could log in with a default password even though that root user was correctly prevented from accessing the shell.	OV3600 8.2.10.1
DE34016	Improvements to VisualRF resolves an issue that prevented the **VisualRF >Floorplan** page from displaying data correctly, and allowed the **Home > Overview** page to incorrectly display a message saying that the nightly VisualRF backup failed.	OV3600 8.2.10.1
DE33996	An issue is resolved where nightly backups triggered a **Nightly Maintenance Failed** error in the WebUI every other day.	OV3600 8.2.10.0
DE33975	Improvements to the method OV3600 uses to obtain the serial number of Alcatel-Lucent Mobility Master resolves an issue that allowed OV3600 to incorrectly display only nine digits of Mobility Master's ten-digit serial number.	OV3600 8.2.10.1
DE33962	Improvements to the **System > Triggers** pages in the OV3600 WebUI prevent users from entering invalid entries in the **Response Time** field for an **Authentication Time** trigger.	OV3600 8.2.11.0
DE33961	OV3600 8.2.11.0 resolved an issue where the OV3600 server would periodically stop processing RAPIDS rogue detection data, preventing rogue device entries from correctly appearing in the **RAPIDS > Overview** page of the OV3600 WebUI.	OV3600 8.2.10.1
DE33951 DE34056 DE34067	Improvements to VisualRF resolved an issue that allowed a client to incorrectly appear on a floor with an AP to which that client was previously associated, even after that client associated to a different AP on a different floor.	OV3600 8.2.10.1
DE33937 DE33729	OV3600 8.2.11.0 includes the open source package FreeRADIUS v3, which resolves an issue that prevented users from logging into OV3600 8.2.10.1 running on CentOS 7 with RADIUS credentials and PEAP MSCHAP v2 authentication.	OV3600 8.2.10.1
DE33932	An issue is resolved where nightly backup transfers could fail in OV3600 8.2.10.1 because the Solarwinds SCP/SFTP server used for the backup transfer didn't support RSYNC and therefore couldn't allow the backup transfers to continue if they were temporarily interrupted. OV3600 8.2.11.0 can use SFTP in place of RSYNC (when used from an OpenSSH perl package) while performing nightly backup transfer.	OV3600 8.2.10.1

Table 1: *Issues Resolved in OV3600 8.2.11.0 (Continued)*

Bug ID	Description	Reported Version
DE33929	An upgrade from OV3600 8.2.8.2 to OV3600 8.2.10.1 caused an error that triggered a high load on the OV3600 server, preventing Instant APs from correctly reporting to OV3600, and causing issues that prevented OV3600 from correctly managing and upgrading Instant APs.	OV3600 8.2.10.1
DE33923	An issue is resolved where the floorplan image on the **Devices > Monitor** page for an AP would incorrectly show the thumbnail image of a Lancom AP, regardless of the model of AP being viewed.	
DE33921	An upgrade from OV3600 8.2.10.0 to OV3600 8.2.10.1 could create duplicate devices.	OV3600 8.2.10.0
DE33908	VisualRF improvements in OV3600 8.2.11.0 resolve an issue where importing a .zip file into VisualRF could cause the WebUI to stop responding, or to respond very slowly.	OV3600 8.2.9.1
DE33903	OV3600 8.2.11.0 resolves an issue where APs monitored by OV3600 would continually change the information for their upstream devices, toggling between two different switches.	OV3600 8.2.10.1
DE33891	Errors in the process to upgrade the OV3600 database caused generating reports to get stuck in an I**n Progress** or **Pending** state, which in turn completely utilized all available database connections.	OV3600 8.2.10.1
DE33845	Improvements in VisualRF resolve an issue where VisualRF could display incorrect client counts, and client data could load very slowly on VisualRF floorplans.	OV3600 8.2.9.1
DE33822	OV3600 failed to push an AP name configuration change to a managed AP, causing the AP Name setting in the AP configuration to become mismatched in OV3600 , and the AP name to display incorrectly the **Devices > Manage** page for that AP.	OV3600 8.2.9.1
DE33806	The patch RPM for CentOS 7 was not included in the upgrade to OV3600 8.2.10.1, so the patch had to be manually installed. This patch is now automatically available when the OV3600 server upgrades to OV3600 8.2.11.0.	OV3600 8.2.10.1
DE33805	The **System > Status** page incorrectly showed the **Glass Feeder** service was down.	OV3600 8.2.10.1
DE33804	After an upgrade to OV3600 8.2.10.0, CPU utilization on the OV3600 sever unexpectedly increased when password encryption in the database was enabled. This issue is resolved in OV3600 8.2.11.0 by internal changes that avoid password decryption when querying the AP table when passwords are not used.	OV3600 8.2.10.0
DE33803	After migrating to Centos 7, an OV3600 deployment was impacted by an unusually high server load. Internal changes to the OV3600 papi handler have resolved this issue in OV3600 8.2.11.0.	OV3600 8.2.10.1
DE33801	OV3600 8.2.11.0 supports Alcatel-Lucent AP model AP-318 in OV3600 topologies, resolving an issue where APs and switches in a selected folder did not display correctly in the OV3600 WebUI.	OV3600 8.2.7

Table 1: *Issues Resolved in OV3600 8.2.11.0 (Continued)*

Bug ID	Description	Reported Version
DE33794	An issue is resolved where the internal httpd process stopped, preventing the failover OV3600 server from taking over for the primary OV3600 server.	OV3600 8.2.10.1
DE33793	When a 3810 Switch in monitor-only mode in OV3600 8.2.10.1 was upgraded to AOS-Switch version16.10.002 directly from the switch (and not through OV3600) OV3600 could no longer reach the switch and could report the device as down, even if it was up and active. The OV3600 WebUI also did not correctly display the switch IP address and gateway and community string information.	OV3600 8.2.10.1
DE33790	Security improvements in OV3600 now verify that all menu modules added through the **Advanced > Custom Commands** section of the OV3600 command-line interface are encrypted to the specific key of the OV3600 appliance, or are officially signed by Alcatel-Lucent. These improvements resolve a vulnerability that could allow remote code execution through a malicious menu module.	OV3600 8.2.10.1
DE33789	Security improvements in OV3600 prevent a vulnerability that could allow remote code execution via a command injection in the **Primary Server Hostname/IP Address** setting in the **RADIUS authentication** option.	OV3600 8.2.10.1
DE33788	Improvements to the memory limit of the internal OV3600 PAPI handler resolved an issue that prevented OV3600 from correctly displaying data for several hours.	OV3600 8.2.10.1
DE33785	OV3600 now correctly displays UTF-8 characters in the OV3600 WebUI.	OV3600 8.2.10.0

Table 1: *Issues Resolved in OV3600 8.2.11.0 (Continued)*

Bug ID	Description	Reported Version

DE33783	OV3600 8.2.11.0 addresses the following security vulnerabilities:
	● **Disable ICMP redirect support for CentOS Linux 7.7.1908**
	The following settings have been added to /etc/sysctl.conf:
	`sysctl -w net.ipv4.conf.all.accept_redirects=0`
	`sysctl -w net.ipv4.conf.default.accept_redirects=0`
	`sysctl -w net.ipv4.conf.all.secure_redirects=0`
	`sysctl -w net.ipv4.conf.default.secure_redirects=0`
	● **Disable TLS/SSL support for static key cipher suites for NGINX**
	OV3600 8.2.11.0 has been set up to disable TLS/SSL support for static key cipher suites.
	Only the following TLS/SSL ciphers are supported now:
	● ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCMSHA256:
	● ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSAAES256-GCM-SHA384:
	● DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCMSHA256:
	● kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:
	● ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:
	● ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:
	● DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:
	● DHE-RSAAES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSAAES256-SHA:
	● !aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK
	● **Delete files or directories with no real owner or group**
	All orphan files created by temporary SCP users are deleted now upon user deletion.
		OV3600 8.2.10.0

DE33770	When you export a bill of materials for a campus from the **VisualRF > Floor Plans > Edit** menu, images in the exported file can appear to be distorted, even if they appear correctly in the floor plan.	OV3600 8.2.10.0
DE33768	If an AP provisioned in a group where the Instant GUI Config (IGC) feature enabled was later moved to a group where IGC is disabled, the attributes for the AP on the **Devices > Manage** page were not updated, and the default uplink-vlan parameter of 1 was pushed to the device.	OV3600 8.2.9.1
DE33767	Improvements to the VisualRF floorplan import process resolves an issue where floorplans imported in .dwg format were resized with an incorrect height.	OV3600 8.2.10.1
DE33760	VisualRF displayed incorrect transmit power for a planned 530 Series access point, and incorrectly displayed configuration fields for orientation, beamwidth, and gain that were not applicable to that device. Updates to the internal VisualRF catalog repository has resolved this issue in OV3600 8.2.11.0.	OV3600 8.2.10.1

Table 1: *Issues Resolved in OV3600 8.2.11.0 (Continued)*

Bug ID	Description	Reported Version
DE33759	An issue is resolved that prevented OV3600 8.2.10.0 from correctly saving the whitelist of IPs/subnets allowed the access the OV3600 WebUI.	OV3600 8.2.10.0
DE33756 DE33758	An issue is resolved that prevented the failover OV3600 server from taking over for the primary OV3600 server due to ltree objects included in the backup. This issue was previously reported as DE32013 and DE32919, and is fixed in OV3600 8.2.8.2, OV3600 8.2.9.0, and OV3600 8.2.10.1.	OV3600 8.2.8.1
DE33737	Changes introduced in OV3600 8.2.8.1 prevented OV3600 users from setting empty values in a subscriber group template, which triggered the message "Please provide variable value" when a user tried to save templates with empty values. Changes in OV3600 8.2.11.0 allow subscriber template variables to support null values once again.	OV3600 8.2.8.1
DE33734	Reports run from a master OV3600 console did not generate correctly, even though the reports did generate as expected when run from the primary OV3600 server. The **Reports > Generated** page of the OV3600 master console WebUI showed that these reports were stuck in the **Pending** or **In Progress** states.	OV3600 8.2.10.0
DE33732	Events information on the **Devices > Monitor > Device Events** page could fail to load correctly due to corrupted events data.	OV3600 8.2.10.0
DE33731	The **tcpdump** command did not work correctly when issued from the **8 Advanced > 2 Enter Commands** menu in the OV3600 command-line interface, and displayed the error message **sh: /usr/sbin/tcpdump: No such file or directory**.	OV3600 8.2.10.0
DE33729	An issue is resolved that prevented the OV3600 server from sending traffic to a RADIUS authentication server, causing RADIUS authentication to fail.	OV3600 8.2.10.0
DE33725	Improvements to the process that manages expired user sessions has resolved an issue that prevented users from logging in to the OV3600 WebUI after upgrading to OV3600 8.2.10.0 and CentOS 7.	OV3600 8.2.10.0
DE33704	When users changed the name of an access point through the Switch, VisualRF did not update with the new name immediately, and changes appeared in VisualRF only after a noticeable delay.	OV3600 8.2.10.1
DE33703	When an OV3600 user logs in with a non-admin user role and creates a new config or audit job for a group of switches, the **Snippet Type** field in the **Add Snippet** window and the **Job Type** field in the **Add Job** window now display correct names, resolving an issue where these fields could display incorrect information.	OV3600 8.2.10.1
DE33682	An Edge-Core AS4610-54P switch running Pico8 software is added to OV3600 server as Universal Network Device. The connected device or neighbor information could not be seen though thus limiting OV3600 from identifying wired rogues.	OV3600 8.2.10.0
DE33657	An issue is resolved where creating a new custom view that included radio information on the **Devices > List** page allowed the radio filter dropdown menu to incorrectly display keyword variables.	OV3600 8.2.10.1

Table 1: *Issues Resolved in OV3600 8.2.11.0 (Continued)*

Bug ID	Description	Reported Version
DE33605	The Instant GUI Config feature took two hours to start after an upgrade to OV3600 8.2.9.1, and log files for the event displayed the message "Container waiting for the DatabaseService to bootstrap."	OV3600 8.2.9.1
DE33563	When you selected a link in the **Auth Failures** column of the **Authentication** table on the **Home** > **Clarity** page, the **Clarity** > **User Details** page could fail to load if the default time for the page was set to **2H** (two hours).	OV3600 8.2.9.1
DE33556	An issue is resolved that allowed OV3600 to generate a large number of unnecessary messages in the **System** > **Event** Log after registering a custom device.	OV3600 8.2.9.1
DE33537	An issue is resolved that removed special characters from the username of an OV3600 administrator if that user failed a login attempt.	OV3600 8.2.9.1
DE33500	An issue is resolved that allowed OV3600 to perform an excessive amount of logins to the WebUI of connected controllers. Improvements in OV3600 8.2.11.0 reduce the number of logins to once every fifteen minutes.	OV3600 8.2.9.1
DE33437	High CPU utilization by the internal PAPIHandler process caused the OV3600 server to stop responding and become inaccessible via HTTPS or SSH.	OV3600 8.2.9.1
DE33378	An issue is resolved that prevented the **Groups** > **Instant Config** page from correctly displaying all APs if there were more than 80 APs in the group.	OV3600 8.2.9.1
DE33331	In VisualRF, a floor plan in .SVG format appeared to be blurred after being uploaded, and could not be fixed unless the floor plan was deleted and added back.	OV3600 8.2.7.0
DE33328	An OV3600 upgrade failed because an SCP user was mapped to a group ID that was already in use by the deprecated ElasticSearch group.	OV3600 8.2.7.1
DE33326	An issue is resolved that allowed the Devices List to incorrectly display device type data for Aruba 2930M-24G-PoE+ and Aruba 2930M-24SR-PoE+ switches when the **Type** filter on the Devices List was modified to display data for either one of these two device types.	OV3600 8.2.9.1
DE33323	The **Devices** > **Monitoring** page for an AP incorrectly reported zero bandwidth usage during a period of continuous traffic on that device.	OV3600 8.2.5.1
DE33291	When an OV3600 user generated a network-wide client inventory report filtered limit to the output to active devices for report duration, the report displayed correctly the first time it was generated , but could incorrectly display the warning "no data to report" when the report was run a second time.	OV3600 8.2.9.0
DE33266	An issue is resolved that prevented OV3600 users from moving VisualRF floorplans imported from Ekahau Site Survey (*.esx) project files from one VisualRF building to another.	OV3600 8.2.9.0
DE33224	OV3600 displayed incorrect role information in the **Role** column of the **Radios** table on the **Devices** > **Monitoring** page for an AP with only a mesh link SSID.	OV3600 8.2.6.0

Table 1: *Issues Resolved in OV3600 8.2.11.0 (Continued)*

Bug ID	Description	Reported Version
DE33223	An issue is resolved that prevented the **Devices > Monitor** page from correctly displaying location information for an AP connected to a Switch configured with syslocation data, and connected to a Switch running Alcatel-Lucent AOS-W 8.x.	OV3600 8.2.9.0
DE33202	OV3600 did not update a link status in the **Home > Topology** page when a new link was added between managed devices, and the device was polled manually.	OV3600 8.2.7.0
DE33194	An issue is resolved that prevented OV3600 from correctly generating traffic analysis reports filtered to display information for selected clients.	OV3600 8.2.8.1
DE33174	Configuration audit, template and warning messages were difficult to read due to a lack of line breaks. The formatting of these messages have been improved with added line breaks for enhanced readability in OV3600 8.2.11.0.	OV3600 8.2.8.2
DE33167	The **VisualRF > Floor Plans** page did not correctly display a 5 GHz radio band heatmap on the building floor where the AP was located when the AP was a mesh portal or mesh point.	OV3600 8.2.6.0
DE33163	The topology on the **Home > Topology** page took longer than expected to load when websocket updates were enabled on managed devices.	OV3600 8.2.8.2
DE33162	OV3600 periodically displayed lower than expected client counts on **Devices > Monitor** pages. Improvements to how AP names are parsed resolves this issue in OV3600 8.2.11.0.	OV3600 8.2.9.0
DE33160	When an AP was changed from standard AP access mode to Air Monitor mode, there was no corresponding update in the **TX power** column of the **Radios** graph on the **Devices > Monitor** page for that AP.	OV3600 8.2.9.0
DE33076	The **HeatMap History** playback option on the **VisualRF > Floor Plans** page failed to correctly play back the desired heatmap history recording.	OV3600 8.2.8.2
DE33025	Improvements to how OV3600 HTML documentation is generated resolved a jQuery vulnerability.	OV3600 8.2.7.1
DE33019	In previous releases, after upgrading the firmware on an Aruba 8320 Switch from 10.02 to 10.03, OV3600 didn't update the **CPU Utilization** or **Usage** graphs on the **Devices > Monitor** page for the switch until the AMP process was manually restarted.	OV3600 8.2.8.2
DE33005	The **Usage** graph on the OV3600 **Home > Overview** page displayed higher than expected usage rates.	OV3600 8.2.8.2
DE32967 DE33388	Ekahau floor plans could display incorrectly when imported into OV3600. For example, concrete walls could be incorrectly imported as cubicle walls, and drywall walls could be imported as glass walls with attenuation levels that very greatly from the original materials. Improvements to the floor plan import process resolves this issue in OV3600 8.2.11.0.	OV3600 8.2.8.2
DE32945	The **Usage** graph on the **Devices > Monitor** page for an AP could show gaps in the data when an interface on the AP is configured to allow a VLAN range, such as **2-4096**.	OV3600 8.2.8.2

Table 1: *Issues Resolved in OV3600 8.2.11.0 (Continued)*

Bug ID	Description	Reported Version
DE32943	When you selected an 303H access point from the **Devices > Monitor** page, the **Usage** graph did not display information for the **Enet3: Usage to Clients** or **Enet 3: Usage from Clients** options, even if both of these options are initially selected from the **WLANs** drop-down menu for this graph.	OV3600 8.2.8.2
DE32860	Differences in how radio information was rounded caused the **Devices > Monitor** page to display inconsistent frame retry rate information in the **802.11 Radio Counters Summary** table and the maximum and average **802.11 counters** graphs.	OV3600 8.2.8.2
DE32846	OV3600 was sending a large number of false positive alerts for rogue APs based upon information sent to OV3600 from Instant APs. Improvements to the alerts sent from Instant APs to OV3600 resolved this issue.	
DE32587	Uploading a floor plan larger than maximum supported size (2400 X 2400 feet) incorrectly displayed the watermark text "Empty View" on the **VisualRF > Floor Plans** page.	OV3600 8.2.7.0
DE32542	An issue is resolved where the **Devices > Monitor** page failed to correctly show IP address of connected clients in deployments with Mobility Master and Managed Devices (local Switches), where the **Prefer AMON vs SNMP polling** setting is enabled on the **OV3600 Setup > General** page.	OV3600 8.2.7.1
DE32353	An issue is resolved where the **Firmware > Update** page of the OV3600 WebUI didn't show the latest firmware versions for Instant APs recently added to a group.	OV3600 8.2.9.0
DE32239	OV3600 did not display data for PUTN (Per-User Tunneled Node) clients and tunnels for controllers and switches configured with IPv6 tunnels, if OV3600 managed these devices using IPv4. This issue is resolved in OV3600 8.2.11.0 for deployments running Alcatel-Lucent AOS-W 8.6.0.0 and later releases.	OV3600 8.2.8.2
DE30661	An OV3600 license report incorrectly showed that there was zero license usage for Mobility Master and Managed Devices (local Switches). This error was triggered by a communication issue between OV3600 and the Switches that prevented OV3600 from correctly decoding controller license data.	OV3600 8.2.9.0
DE30461	FIPS mode could not be enabled on the OV3600 server if OV3600 was actively monitoring devices configured using SNMPv2, and the SNMPv3 credentials were undefined. This issue occurred because the SNMPv3 columns for MD5 and DES were default values. Starting with OV3600 8.2.11.0, OV3600 disregards SNMPv3 credentials if the credential fields are not defined, allowing you to enable FIPS mode.	OV3600 8.2.4.2
DE30018	The **Home > Topology** page did not show interface information for HP OfficeConnect Switches. Starting with OV3600 8.2.11.0, OV3600 collects information for these switches, and interface information for these devices now appear in the **Home > Topology** page.	OV3600 8.2.5.0
DE 34038	Improvements to the process OV3600 uses to clean the device event table prevents an issue where the cleanup process could time out before completing.	OV3600 8.2.9.1

Table 2: *Issues Resolved in OV3600 8.2.10.1*

Bug ID	Description	Reported Version
DE29816	An issue is resolved that prevented OV3600 from showing the correct wired client count when wired clients were located downstream from an Alcatel-Lucent Switch sending information to OV3600 via AMON messages.	OV3600 8.2.4.1
DE31783	OV3600 8.2.10.1 offers improved support for AutoCAD 2019 map files in VisualRF, resolving an issue where VisualRF could blur an imported CAD map file, and could stop responding when DWG files were imported into VisualRF.	OV3600 8.2.7.0
DE33384	After an OV3600 server upgraded from OV3600 8.2.4.3 to 8.2.10.0, an auto-polling error prevented the **Home>Topology** page from loading. Log files in the /var/log/topology folder displayed an internal server error message for the event. This issue is resolved in OV3600 8.2.10.1.	OV3600 8.2.10.0
DE33403	In a previous release, when exporting port information for a switch in a stack, the CSV output displayed data in the **Interface Name** and **Name** columns as dates when the CSV file was opened in Microsoft Excel. This issue is resolved in OV3600 8.2.10.1.	OV3600 8.2.10.0
DE33456 DE33178	When users assigned to a custom or read-only user role accessed the VisualRF feature, OV3600 displayed the logon page instead of VisualRF data, and error messages were recorded to VisualRF log files. This issue is resolved in OV3600 8.2.10.1.	OV3600 8.2.8.2
DE33538	An issue is resolved that prevented OV3600 from correctly populating the LAN MAC data field for some Cisco Switches, such as the Cisco Catalyst 2921/K9 and ISR4331/K9.	OV3600 8.2.9.1
DE33622	After an upgrade to OV3600 8.2.10 and CentOS 7, OV3600 failed to complete an IAP firmware upgrade after sending firmware upgrade files to the IAPs. This issue is resolved in OV3600 8.2.10.1.	OV3600 8.2.10.0
DE33646	OV3600 8.2.10.1 resolves an issue that allowed the **Client** and **Usage** graphs on the **Home > Overview** page to display significantly fewer clients and usage levels than expected for brief intervals.	OV3600 8.2.10.0

Table 3: *Issues Resolved in OV3600 8.2.10*

Bug ID	Description	Reported Version
DE25667	Security improvements ensure that user access to API and CSV download data are restricted to only those users whose roles explicitly allow them to view that information.	OV3600 8.2.9.0
DE28187	Client session reports could include information for external unsupported MDM servers in the **Asset Category** and **Asset Group** lists and charts. To resolve this issue, the **Session Data by Asset Group** and **Session Data by Asset** options are removed from the list of available **Client Session** report widgets on the **Reports > Definitions** page, and from the output of **Client Sessions** reports.	OV3600 8.2.9
DE28614	The **Simulate Failure** option that appears when you select an AP on the **VisualRF > Floor Plans** page is improved in this release, resolving an issue that required a user to click on the **Simulate Failure** option twice to enable that feature, or that could incorrectly unsimulate multiple devices if the **Unsimulate Failure** option was selected.	OV3600 8.2.3.1

Table 3: *Issues Resolved in OV3600 8.2.10 (Continued)*

Bug ID	Description	Reported Version
DE29306	Improvements in OV3600 8.2.10 allow Instant APs send AppRF data to OV3600 more frequently than in previous releases. In previous releases, Instant APs reported AppRF data every fifteen minutes, which could prevent OV3600 from displaying information for users that stay on an AP for a shorter amount of time.	OV3600 8.2.3.1
DE31038	Improvements to how OV3600 manages devices with an LMS IP address of 0.0.0.0 resolves an issue that prevented OV3600 from correctly determining the client count in deployments that included a device with that LMS IP.	OV3600 8.2.0.0
DE31368	The **Folder Overview** section of the **Home > Overview** page now correctly displays information for the **Top** folder by default, resolving an issue where another folder would display in the default view.	OV3600 8.2.5.1
DE31906	When you export a bill of materials that includes the **Show Heatmap** option on the **VisualRF > Floor Plans** page, the heatmaps on the **Bill of Materials** report now accurately reflects the configured **Signal Cutoff** value for that floor plan.	OV3600 8.2.7
DE31997	OV3600 now displays the IPv4 and IPv6 addresses for clients with both IP address types, resolving an issue where the **Clients > Client Detail** page displayed only an IPv4 *or* an IPv6 address for these devices.	OV3600 8.2.7
DE32367	The Refresh icon (↻) on the **VisualRF > Floor Plans** page now correctly refreshes the page for users logging in with a read-only role for that OV3600 server.	OV3600 8.2.7.1
DE32373	Planned APs no longer incorrectly broadcast heat maps on the **VisualRF > Floor Plans** page if the **TX power** setting for these devices is set to 0dBm.	OV3600 8.2.7.1
DE32375	An issue is resolved that allowed the **Devices > Monitor** page to display incorrect information for an IPv6-managed device in the **Master IP** and **Cluster** fields.	Alcatel-Lucent AOS-W 8.4
DE32551	In deployments with Cisco switches deployed via OV3600, valid devices could be incorrectly classified as rogue devices by the **Detected on Wireless and LAN** classification rule. If the rogue device was deleted from OV3600, its discovery event history was not deleted. If the rogue was subsequently rediscovered, OV3600 retained the history of discovery events for that device.	OV3600 8.2.8.0
DE32597	OV3600 executed the **show user mac <client mac>** command on the incorrect Managed Device in a Mobility Master/Managed Device deployment, causing the **Clients > Client Detail** page for the client and the **Devices > Monitor** page for the AP to which the client was associated to display inconsistent controller information.	OV3600 8.2.7.1
DE32601	OV3600 executed the **show ap virtual-beacon-report client-mac <client mac address>** command on a Managed Device instead of Mobility Master in a Mobility Master/Managed Device deployment, causing the **Clients > Client Detail** page for the client to display inconsistent Switch information.	OV3600 8.2.7.1

Table 3: *Issues Resolved in OV3600 8.2.10 (Continued)*

Bug ID	Description	Reported Version
DE32619	Improvements to the OV3600 backup processes allow OV3600 to correctly create backups in a deployment where the OV3600 server has separate partitions for */var/airwave-backup* and */var/ampcli/users*. In the event that a partition does not allow OV3600 to use a hard link to create a backup, the backup file is manually copied across partitions.	OV3600 8.2.7.1
DE32627	An issue is resolved where the **Topology** page didn't display aggregated links between switches properly. When this issue occured, all links between core and end switches wereaggregated links and only two links in the topology map had a circle in the middle, which denoted an aggregated link.	OV3600 8.2.7.0
DE32629	Alcatel-Lucent switches monitored as a group now display correct aggregate usage data on the **Groups > Monitor** page.	OV3600 8.2.8
DE32637	OV3600 can use AMON to monitor wired clients in deployments running Alcatel-Lucent AOS-W 8.4 or later releases. Deployments running previous versions of Alcatel-Lucent AOS-W can monitor wired clients using SNMP only, which can cause a client count mismatch when switching between AMON and SNMP monitoring protocols.	Alcatel-Lucent AOS-W 8.3.x
DE32658	OV3600 no longer considers subscription licenses to be a type of evaluation license, so the **Home > License** page no longer displays warning messages about evaluation license for any subscription licenses on the system.	OV3600 8.2.7.1
DE32677	Clients that complete MAC authentication and are hard-wired to an Aruba switch now correctly increment the number of connected devices in the **Clients** field of the **Devices > Monitor > Summary** page, and in the **Clients** counter in the top header of the OV3600 WebUI.	OV3600 8.2.7.1
DE32684	An issue is resolved where the **Usage** graph on the **Home > Overview** page did not correctly display information for a DataZone SSID because the **Sources** drop-down menu on this graph did not display the DataZone SSID as an option in the list of available SSIDs.	OV3600 8.2.8.1
DE32699	OV3600 displays consistent information about the number of clients on a selected SSID when this information is viewed on the **Clients** graph on the **Home > Overview** page and the **Clients** section of a network usage report for that SSID.	OV3600 8.2.7.0
DE32714	The Instant GUI Config (IGC) feature failed to correctly push policy text for a captive portal splash page when the text contained special characters in Portuguese.	OV3600 8.2.8.1
DE32747	The **Authentication** table on the **Home > Clarity** page incorrectly displayed information about active APs in the list of authentication servers. When one of these APs was selected from the **Authentication** table, the **Clarity > User Details** table also incorrectly indicated that the AP was an authentication server.	OV3600 8.2.6.1
DE32754	An issue is resolved where OV3600 failed to push a template to Alcatel-Lucent 2930F switches when enhanced security was enabled on the switch template using the **Do you want to show sensitive information (y/n)?** option.	OV3600 8.2.4.3

Table 3: *Issues Resolved in OV3600 8.2.10 (Continued)*

Bug ID	Description	Reported Version
DE32762	OV3600 includes two 1024-bit Digital Signature Algorithm (DSA) keys in the /etc/ssh folder, even though the OV3600 sever uses a more secure RSA key when connecting to the server. These two DSA keys could be manually removed but would be recreated when the SSHd service was restarted, and could cause a Qualys vulnerability scan to trigger an alert for vulnerability **QID 38738: SSH Server Public Key Too Small**.	OV3600 8.2.7.1
DE32783	OV3600 displays the channel width used by an Instant APs radio on the **Devices > Monitor > Radio Statistics** page.	OV3600 8.2.7.1
DE32818	An issue is resolved where the restart of an internal *rrdcached* service allowed the **Clients** and **Usage** graphs on the **Home > Overview** page to incorrectly show zero clients and usage levels for a few moments before again displaying correct data.	OV3600 8.2.8.1
DE32819	**Bill of Materials** reports generated from the **VisualRF > Floor Plans** page correctly display AP names, resolving an issue that allowed the names of some APs at the bottom of the floor plan to get cut off on the report.	OV3600 8.2.8.1
DE32828	The **VisualRF > Floor Plans** page correctly displays floor plans imported from Ekahau backups, resolving an issue where backup campuses were created without floor plans.	OV3600 8.2.8.1
DE32839	OV3600 now validates the required a eight-character password for SNMPv3 users when configuring SNMP on the **Device Setup > Add** page and the **Devices > Manage** page, resolving an issue where the eight-digit minimum character requirement was validated on the **Device Setup** pages only.	OV3600 8.2.8.2
DE32845	OV3600 was sending a large number of false positive alerts for rogue APs based upon information sent to OV3600 from Instant APs. Improvements to the alerts sent from Instant APs to OV3600 resolved this issue. The current behavior is that OV3600 will not report a recorded client as rogue, no matter how long ago it connected to OV3600.	OV3600 8.2.8.1
DE32880 DE33006	Insufficient SNMP packet sizes on HPE Comware switches prevented OV3600 from correctly displaying the switch on the **Home > Topology** page and triggered SNMP polling error messages in the system event logs. To resolve this issue, increase the SNMP packet size on the switch from 1500 to 3500 using the command **snmp-agent packet max-size 3500**	OV3600 8.2.8.2
DE32895	The **Send Test Email** feature available when configuring a mail relay server on the **OV3600 Setup > General > Additional OV3600 Services** page has been improved to prevent a potential Cross-site Scripting (XSS) command injection vulnerability.	OV3600 8.2.9.0
DE32896	The VisualRF feature that allows users to import Floor Plans from various sources has been improved to prevent a potential XML External Entity (XXE) vulnerability that could allow the execution of unauthorized commands on the OV3600 server.	OV3600 8.2.9.0
DE32897	The certificate import feature available on the **Device Setup > Certificates** page has been improved to prevent a potential XML External Entity (XXE) vulnerability that could allow users to execute unauthorized commands on the OV3600 server as an apache user.	OV3600 8.2.9.0

Table 3: *Issues Resolved in OV3600 8.2.10 (Continued)*

Bug ID	Description	Reported Version
DE32899	OV3600 8.2.10 is improved to prevent a potential preauthorization SQL injection vulnerability in the OV3600 authentication cookie.	OV3600 8.2.9.0
DE32910	VisualRF backups can now be restored from both the OV3600 command-line interface and the WebUI.	OV3600 8.2.8.2
DE32945	OV3600 was unable to recognize a VLAN range configured on a Switch as a valid uplink for WAN monitoring, causing gaps in the data on **Usage** table in the **Home > Overview** page.	OV3600 8.2.8.2
DE32978	Improvements to **Network Usage** reports allow these reports to correctly display **Usage** and **Clients** graphs for all subfolders when the SSIDs field for the report definition on the **Reports > Definition** page is set to **Use Selected SSIDs**, and all available SSIDs are selected.	OV3600 8.2.5.0
DE32986	In a deployment with Instant APs connected in a daisy-chain mode (where an OAW-IAP's downlink port is used to connect to the other OAW-IAPs), the **Devices > Monitor > Neighbors** page failed to correctly display all LLDP neighbors for the device, even though all neighbors are showing correctly on the **Home > Topology** page.	OV3600 8.2.9.0
DE32998	In a deployment where the *nightly_data*.tar.gz* and *weekly_data*.tar.gz* files were customized by adding additional characters to the beginning of the file names, a local backup file taken before a failover incorrectly included files with these customized names, making the local backup extremely large and delaying the failover process. This issue is resolved in OV3600 8.2.10, as OV3600 now excludes all files of the pattern ***nightly_data*.tar.gz* and ***weekly_data*.tar.gz*. **NOTE:** Best practices is to either remove old backups after restoring them on recovered/reinstalled systems, or maintain nightly/weekly naming conventions for backup files.	OV3600 8.2.8.2
DE33024	Improved API security in OV3600 8.2.10 prevents authorized users from changing label inputs on OV3600 charts and graphs.	OV3600 8.2.7.1
DE33038	The **Home > Topology** page now allows you to select multiple folders and view the contents of just those selected folders in an expanded view. Previous releases only displayed an expanded view of all folders or a single selected folder.	OV3600 8.2.7.0
DE33047	An issue is resolved that prevented users from changing the time zone setting of the OV3600 server using the **Configuration > Set Timezone > [continent or ocean] > [country]** settings in the OV3600 command-line interface.	OV3600 8.2.4.3
DE33056	OV3600 failed to back up a Switch after the OV3600 server upgraded from OV3600 8.2.7.1 to OV3600 8.2.8.2, because some ciphers supported by the Switch were missing in OV3600 8.2.8.2. Starting with OV3600 10, a new **3 Configuration > 5 SSHD > 2 User Compatible Ciphers** setting in the command-line interface enables weak ciphers **aes128-cbc**, **aes192-cbc**, and **aes256-cbc** if the config file has ciphers set and these algorithms are not part of the existing OV3600 ciphers.	OV3600 8.2.8.2

Table 3: *Issues Resolved in OV3600 8.2.10 (Continued)*

Bug ID	Description	Reported Version
DE33063	By default, OV3600 supports the following strong ciphers. - DHE-RSA-AES128-SHA - DHE-RSA-AES256-SHA - DHE-RSA-AES128-SHA256 - DHE-RSA-AES256-SHA256 - ECDHE-ECDSA-AES128-SHA256 - ECDHE-ECDSA-AES256-SHA384 - ECDHE-ECDSA-AES128-GCM-SHA256 - ECDHE-ECDSA-AES256-GCM-SHA384 The **OV3600 Setup > Authentication > LDAP Authentication** fields in the OV3600 WebUI now include a new **Support Deprecated Ciphers** option to allow OV3600 to also use following legacy ciphers: - AES128-SHA - AES256-SHA - DES-CBC3-SHA - DHE-DSS-AES128-SHA - DHE-DSS-AES256-SHA - EDH-DSS-DES-CBC3-SHA - EDH-RSA-DES-CBC3-SHA - KRB5-DES-CBC3-MD5 - KRB5-DES-CBC3-SHA **NOTE:** Note: OV3600 does not recommend using legacy ciphers for an extended period of time.	OV3600 8.2.7
DE33083	An issue is resolved that caused the **Home > Topology** page to display incorrect edge count, edge icon and edge details information for an aggregated link after a topology restart.	OV3600 8.2.8.2
DE33100	After upgrading to OV3600 8.2.8.2, Aruba 2930 switches were incorrectly showing a DOWN status with the error message **ICMP ping failed after SNMP get failed**. This issue is resolved in OV3600 8.2.10.	OV3600 8.2.8.2
DE33171	Users were unable to use the Instant GUI Config feature to add multiple gateway VPN routes to a group of Instant APs using the **Groups > Instant Config > VPN > Routing** options.	OV3600 8.2.9.0
DE33175	A VisualRF **Bill of Materials** report generated for floor plans with a large number of APs displayed errors and could not be opened using Microsoft Word.	OV3600 8.2.9.0
DE33177	When AP device groups and AP folder names contained non-ASCII (UTF-8) characters such as Japanese characters, the **Systems > Triggers** page could display the error message "The server has encountered an error while performing your request" and failed to display correct trigger data. This issue is resolved for OV3600 8.2.10 deployments in a CentOS7-based environment only. The fix for this issue is not supported by deployments based on CentOS6.	OV3600 8.2.8.1
DE33182	Users were unable to use the Instant GUI Config feature to create two profiles with the same ESSID, even though these profiles could be defined on a standalone virtual Switch.	OV3600 8.2.9.0

Table 3: *Issues Resolved in OV3600 8.2.10 (Continued)*

Bug ID	Description	Reported Version
DE33215 DE33188	After upgrading from OV3600 8.2.8.2, Aruba switches displayed an error status in the **Devices List** table on the **Devices > List** page. Improvements to how **Message of the Day** (MOTD) banner messages are displayed have resolved this issue.	OV3600 8.2.8.2
DE33241	OV3600 introduces updated CentOS6 and CentOS 7 security RPMs. OV3600 security has also been improved to support the following CentOS security vulnerability updates: ● RHSA-2018:1879--glibc security and bug fix update ● RHSA-2018:2180--gnupg2 security update ● RHSA-2018:2284--yum-utils security update ● RHSA-2018:2892--glusterfs security, bug fix, and enhancement update ● RHSA-2018:3854--ntp security update ● RHSA-2019:1467-- python security update ● RHSA-2019:1652--libssh2 security update ● RHSA-2019:1492--bind security update ● cve-2019-13139--command injection flaw	OV3600 8.2.9.1
DE33263	Enhanced support for Alcatel-Lucent APs that support 802.11ax resolves an issue that allowed the system event logs to display the error message *Internal Error: Couldn't determine class for type 'ax'* in deployments that included 802.1ax APs such as the OAW-AP-515.	OV3600 8.2.9.1

Table 4: *Issues Resolved in OV3600 8.2.9.1*

Bug ID	Description	Reported Version
DE33131	OV3600 8.2.9.1 contains the kernel security update for Red Hat Enterprise Linux 6. Refer to RHSA-2019:1488 for information about the security advisory.	OV3600 8.2.9.0
DE33116	After upgrading the software version to OV3600 8.2.9.0, OV3600 reported all Instant APs as being down. This issue was due to message formatting change for the Alcatel-Lucent AOS-W 8.5.0.0 Instant AP firmware.	OV3600 8.2.9.0
DE33093 DE33092	From the **Clients** menu, when filtering the client connection mode in the default view by 802.11ax, OV3600 displayed the value **"RADIO_MODE-ENUM-VALUE-X/Y"** Now, OV3600 displays **"11ax"**.	OV3600 8.2.9.0
DE33440	The **Audit Configuration on Devices** feature stopped working after the OV3600 server was upgraded to a newer version of OV3600, and the **Configuration** field on the **Devices > Config** page for impacted devices displayed the message **Telnet/SSH Error: (pattern match timed-out) in password failure**. This issue is resolved by upgrading to OV3600 8.2.10.	OV3600 9.2.9.1

Table 5: *Issues Resolved in OV3600 8.2.9.0*

Bug ID	Description	Reported Version
DE32997	In the *OV3600 8.2.9 User Guide*, the description for the **Help improve OV3600 by sending anonymous usage data** has been updated.	OV3600 8.2.x.x
DE32971	OV3600 8.2.9 contains the kernel security and bug fix update for Red Hat Enterprise Linux 6. Refer to RHSA-2019:1169 for information about the security advisory.	OV3600 8.2.9.0
DE32919	The failover OV3600 didn't take over for the primary OV3600 due to ltree objects included in the backup. This issue was previously reported as DE32013 and fixed in OV3600 8.2.8.2.	OV3600 8.2.9.0
DE32859	You couldn't resize an Ekahau backup floor plan in VisualRF.	OV3600 8.2.8.2
DE32851	The *OV3600 8.2.9 User Guide* now includes Appendix C, "VisualRF and Performance".	OV3600 8.2.8.2
DE32838	Upgrading from OAW-IAP 6.5.1.5 to OAW-IAP 6.5.4.12 broke OV3600 communication.	OV3600 8.2.7.1
DE32759	OV3600 became unresponsive and had to be rebooted.	OV3600 8.2.7.0
DE32723	AP names weren't updated in VisualRF after being renamed in OV3600.	OV3600 8.2.7.1
DE32709	Master Console search queries weren't optimized and slowed down communication with OV3600.	OV3600 8.2.7.0
DE32668	OV3600 becomes unresponsive and has to be rebooted in order to get SSH access.	OV3600 8.2.7.0
DE32667	The *OV3600 8.2.9 Switch Configuration Guide* has been updated with examples of configuring ZTP with templates and variables for Alcatel-Lucent AOS-W switches.	OV3600 8.2.8.1
DE32636	OV3600 displayed the wrong radio channels in the RF neighbor list.	OV3600 8.2.7.1
DE32632	OV3600 8.2.9 addresses an XSS vulnerability found in the index.html file.	OV3600 8.2.8.1
DE32624 DE32258 DE32257	OV3600 8.2.9 addresses an XML External Entity (XXE) vulnerability found in the XML parser.	OV3600 8.2.6.1 OV3600 8.2.7.1
DE32596	Additional changes to the Ethernet bonding workflow was required. OV3600 8.2.9 introduces an Enter Command to remove Ethernet bonding, called **remove_ethernet_bonding**. **NOTE:** This new command will not remove bonding if the bonding was created using shell access, as it relies on the ethernet_bonding path to save the pre-bonded state.	OV3600 8.2.5.0

Table 5: *Issues Resolved in OV3600 8.2.9.0 (Continued)*

Bug ID	Description	Reported Version
DE32585	You couldn't manually override a rogue classification when the rogues cache file was greater than 6.6 GB.	OV3600 8.2.7.1
DE32562	OV3600 displayed flat lines in graphs after the internal Rabbitmq process crashed.	OV3600 8.2.7.0
DE32541	OV3600 8.2.9 addresses an XSS vulnerability found when calling the RRD export tool using a URL.	OV3600 8.2.8.0
DE32540	OV3600 8.2.9 addresses an XSS vulnerability found in RAPIDS URL variables.	OV3600 8.2.8.0
DE32455	The underlying Alcatel-Lucent AOS-W defect which caused channel utilization and config page issues for APs monitored with IPv6 has been fixed.	OV3600 8.2.7.1
DE32423	Previously, when the database was down, the OV3600 CLI menu was be unreachable. The fix removes the dependency on database, no longer requiring data from the database in order to load OV3600 CLI menu.	OV3600 8.2.7.1
DE32414	The interference calculation which caused the channel utilization graph errors has been fixed.	OV3600 8.2.7.1
DE32382	In OV3600 8.2.7.1, you couldn't transfer or upload a file on the OV3600 from the OV3600 CLI using the Advanced menu option 8-7. Permissions on files that the file transfer user can see have been adjusted.	OV3600 8.2.7.1
DE32291	After upgrading from OV3600 8.2.6.1 to OV3600 8.2.7.1, the previously installed custom certificate trust chain wasn't copied from the OV3600 8.2.6 Java certificate store to the upgraded Java certificate store. This issue has been fixed using the OV3600 CLI and selecting **9-3** for the **Add SSL Certificate** option.	OV3600 8.2.7.1
DE32267	Clients graph for tunneled client fluctuated every 7 minutes if **Prefer AMON vs SNMP Polling** was enabled. This issue occurred in an Alcatel-Lucent AOS-W 8 setup. OV3600 shows the client count and then disconnects, dropping to zero, every 7 minutes.	OV3600 8.2.7.1
DE32256	OV3600 8.2.9 addresses an XSS vulnerability found when running the RF health report for a folder.	OV3600 8.2.7.1
DE32255	OV3600 8.2.9 addresses an XSS vulnerability found in VisualRF XML files.	OV3600 8.2.7.1
DE32211	OV3600 8.2.9 addresses an XSS vulnerability exercised by nested calls to Alcatel-Lucent AP groups.	OV3600 8.2.7.1
DE32202	OV3600 8.2.9 addresses an XSS vulnerability found in nested template names.	OV3600 8.2.7.1
DE32201	OV3600 8.2.9 addresses an XSS vulnerability found in discovery scan credentials.	OV3600 8.2.7.1

Table 5: *Issues Resolved in OV3600 8.2.9.0 (Continued)*

Bug ID	Description	Reported Version
DE32019	Cisco 2600 and 2700 APs showed the wrong radio interface information, and the transmit power couldn't be determined for some of the interfaces.	OV3600 8.2.7.0
DE31978	PDF floor plans weren't clear after you uploaded them into VisualRF.	OV3600 8.2.7.0
DE31793	When you configured **AP Fully Qualified Domain Name Options** under Display in AMP settings to **Use AP Name and FQDN** and if the AP name began with a lower case letter, OV3600 didn't prepend the AP name to the FQDN.	OV3600 8.2.7.0
DE31782	Network scan discovery failed for Cisco 3650 and 3850 switches if the native VLAN (VLAN1) wasn't configured in Interfaces 1 to 8.	OV3600 8.2.7.1
DE31779	OV3600 failed to sync to the Net Cool NMS server using SNMPv3.	OV3600 8.2.6.0
DE31719	There was no option to regenerate the self-signed certificate on OV3600 using the CLI. Now, you can select **9-13** from the Security menu to regenerate the self-signed certificate.	OV3600 8.2.7.0
DE31690	FTP export feature in reports didn't work.	OV3600 8.2.6.1
DE31577	When performing a manual failover for testing, you couldn't disable OV3600 using the CLI . Now, there is an Advanced menu option that lets you enable or disable the OV3600. At the CLI prompt, select **8** to open the Advanced menu, then select **2**.	OV3600 8.2.6.1
DE31572	VisualRF some times created duplicate walls if you deselected the option to draw a wall and then selected a previously drawn wall. This issue affected heatmaps for planning and deploying APs because the walls contributed to attenuation.	OV3600 8.2.7.1
DE31265	OV3600 didn't display the CPU utilization graph.	OV3600 8.2.3.1
DE31030	When creating a new floorplan and adding campuses, the new campus wasn't available in the drop-down menu. This issue occurred even though you provided an address when creating a new building in the campus.	OV3600 8.2.6.0
DE30742	Open Virtual Machine Tools (open-vm-tools), which is installed during an OV3600 installation or upgrade, runs automatically when the system starts. Now, you can permanently disable this set of services and modules from the CLI using the Enter Commands menu.	OV3600 8.2.6.0
DE30738	System check for serial port was flooding syslog. The fix requires a reboot after the upgrade to OV3600 8.2.9 to force the re-run of hardware detection to adjust configuration as needed.	Not available

Known Issues

Known issues and workarounds in OV3600 8.2.11.0, 8.2.10.1, 8.2.10, 8.2.9.1, and 8.2.9.0 are described in the tables that follow.

Table 6: *Known issues in OV3600 8.2.11.0*

Bug ID	Description	Reported Version
DE34119	The **Devices > Monitor** page failed to correctly display accurate uptime information for Aruba AOS-CX 6300 switches running firmware version FL.10.04.0030. **Workaround**: Upgrade the switch to the last software version FL.10.04.2000AP.	OV3600 8.2.11
DE34117	OV3600 is unable to create a VLAN configuration for an AOS-CX switch running firmware version 10.04, because the switch does not allow write memory operations when in config mode. **Workaround**: This issue is not seen in AOS-CX software versions prior to TL.10.04.0030.	OV3600 8.2.11
DE34102	If OV3600 8.2.11 is installed on a Central On-Premise server, or the server is rebooted after enabling FIPS mode, the server may not reachable because it is mapped to an an incorrect interface. On a Gen-10 Central On-Premise server where there is an external 10G NIC via PCIe and a 1G interface NIC, even though the physical connectivity is provided on the 1G interface, during kernel bootup, the order of NIC discovery becomes unpredictable. In this scenario, it is possible that the eth0 interface is assigned to the 10G MAC address, making the network become unreachable. **Workaround**: Contact support for a procedure to block the detection of the 10G NIC during the kernel bootup.	OV3600 8.2.11
DE34101	After upgrading to OV3600 8.2.10.1, the Async Logger Client reaches the memory limit and restarts approximately every six minutes. **NOTE:** Issue has been seen in a specific customer environment. A patch has been installed in the customer's setup with a modified ALC restart algorithm.	OV3600 8.2.10.1
DE34098	Reports generated on the master console could get stuck in a pending or in-progress state. **Workaround**: Delete the reports in the in-progress state to allow OV3600 to proceed with the next pending report.	OV3600 8.2.11
DE34092	The **Devices > List** page displays incorrect information for devices not actually present on the network after the switchover of an Aruba CX 6300 Virtual Switching Framework (VRF) stack. **Workaround**: Change the **Up/Down Status Polling Period** to five minutes to allow the switches to come up properly.	OV3600 8.2.11
DE34086	AOS-CX switches are not coming up in OV3600 after the switchover of an Aruba CX 6300 Virtual Switching Framework (VRF) stack. **Workaround**: Change the **Up/Down Status Polling Period** to five minutes to allow the switches to come up properly.	OV3600 8.2.11

Table 6: *Known issues in OV3600 8.2.11.0 (Continued)*

Bug ID	Description	Reported Version
DE34072	OV3600 reports the status for APs as being down and times out when polling the SNMPv2 Fetcher. This issue occurs when the SNMPv2 Fetcher daemon receives SNMP packets greater than 1472 octets and then crashes. **NOTE:** Newly built net-snmp RPM with fix has been applied in the customer's setup.	OV3600 8.2.10.1
DE34015	OV3600 fails to correctly generate a custom report if the **RF Health: Radio Statistics by Folder** option is the only option selected. **Workaround**: None.	OV3600 8.2.10.1
DE33938	OV3600 failed to correctly display CPU and memory utilization information for member switches of an Aruba AOS-CX 6300 Virtual Switching Framework (VSF) stack. **Workaround**: None.	OV3600 8.2.11
DE33890	A rogue SSID displayed in the **VisualRF > Floorplan > Rogue Properties** tab could be different than the SSID displayed on the **RAPIDS > Detail** page. **Workaround**: Delete the AP in which Rogue is detected from the VisualRF Floorplan, then add it back.	OV3600 8.2.11
DE33848	The **VisualRF** section of the OV3600 WebUI can fail to display correctly because VisualRF processes time out before the pages load. VisualRF floorplans with a large number of APs may take a long time to load, and the procedure to deploy new devices in Visual RF takes a log time to list newly added APs. **Workaround**: None.	OV3600 8.2.9
DE33689	The **Devices > Monitor** page for an access point took an unusually long time to load, even though information about connected and rogue clients displayed as expected on the **Clients** pages. **Workaround**: None	OV3600 8.2.10
DE33683	The internal docker service continuously restarted and log files for the docker service displayed the error "Shutting down due to ServeAPI error: is a directory" **Workaround**: None	OV3600 8.2.10
DE33636	When a Switch on a managed network was replaced or APs were moved from one Switch to another, the AP moved to a different Switch appeared to be in a DOWN state in OV3600 until the OV3600 services were restarted.	OV3600 8.2.8.2
DE33595	The **Devices > Monitoring** page displayed incorrect transmit power levels for 5GHz radios using channels 36 or 52E in the Spain regulatory domain. **Workaround**: None	OV3600 8.2.9.1
DE33526	The **Clients > Client** details page showed the incorrect VLAN for wired clients connected behind an IP phone on a switch, even thought the **Clients > Diagnostics** page displayed the correct information. **Workaround**: None	OV3600 8.2.9

Table 6: *Known issues in OV3600 8.2.11.0 (Continued)*

Bug ID	Description	Reported Version
DE33339	The **RAPIDS > List** page failed to correctly display information for some wired devices impacted by a RAPIDS classification rule. **Workaround**: None	OV3600 8.2.9.1
DE33312	OV3600 did not correctly display channel change information on the **Channel Change Reasons** graph and **Channel Change** table on the **Home > AirMatch** page. **Workaround**: None	OV3600 8.2.9.0
DE33257	An AP initially classified as a rogue device and then manually reclassified as valid was not correctly reclassified as valid if that device aged out of the Wireless Management System (WMS) database, then reconnected again. **Workaround**: None	OV3600 8.2.9.0
DE33032	LDAP authentication failed when the **Verify Server Certificate** field in the**OV3600 Setup > Authentication > LDAP Configuration** section of the WebUI was set to **require** or **optional**. **Workaround**: None	OV3600 8.2.8.2

Table 7: *Known issues in OV3600 8.2.10.1*

Bug ID	Description	Reported Version
DE33731	OV3600 deployments using CentOS 7 can display the error message **/usr/sbin/tcpdump: No such file or directory** when you issue the command **tcpdump** from the **8** (**Advanced**) > **1** (**Custom Commands**) menu in the OV3600 command-line interface. **Workaround**: Contact support for assistance installing the tcpdump RPM.	OV3600 8.2.10.0
DE33707	Upgrades from OV3600 8.2.8.x, 8.2.9.x, or 8.2.10.0 on CentOS 6 and OV3600 8.2.10.0 on CentOS 7 to OV3600 8.2.10.1 might fail with the following PuTTY fatal error message: **Server unexpectedly closed network connection** when your SSH session becomes unresponsive. To avoid this issue, change the keep-alive interval to a low setting as follows: 1. Using a terminal console, such as PuTTY, open an SSH connection with the OV3600. 2. Enter 30 to 60 seconds for sending null packets between keep-alive messages.	OV3600 8.2.10.1
DE33704	When you use a Switch to change the name of an access point, VisualRF does not update with the new name immediately, and changes appear in VisualRF only after a noticeable delay. **Workaround**: To immediately update the VisualRF floorplan with the new AP name, restart VisualRF by toggling the **Enable VisualRF Engine** setting in the **VisualRF > Setup** page to **No** and then back to **Yes**.	OV3600 8.2.10.1

Table 7: *Known issues in OV3600 8.2.10.1 (Continued)*

Bug ID	Description	Reported Version
DE33686	The **Devices > Monitor** page can incorrectly classify an Aruba 6405 or 6410 switch as an Aruba 6400 switch. **Workaround**: None.	OV3600 8.2.10.1
DE33669	The topology on the **Home > Topology** page failed to load. Log files in the **/var/log/topology** folder listed the cause of the issue as a bind failure for port 8085. **Workaround**: Navigate to **System > Status**, then click **Restart OV3600** to restart the OV3600 services.	OV3600 8.2.10.1
DE33666	After upgrading to OV3600 8.2.10.0, users were unable log into the OV3600 server using certificate authentication. **Workaround**: OV3600 8.2.10.0 introduced Certificate Revocation List (CRL) certificate validation, which is required by default. To make this feature optional, access the OV3600 command-line interface and select options **3 (Configuration** > **4 (Certificates)** > **7 (CRL)** > **1 (Make CRL optional/required**).	OV3600 8.2.10.0
DE33434	If you migrate your OV3600 deployment from CentOS 6 to CentOS 7, you will be unable to restore a backup file taken from an OV3600 server running CentOS 6 on an OV3600 server running CentOS 7 if the **/var/log** directory is larger than 20GB. **Workaround**: Contact support for assistance in reducing the size of the **/var/log** directory.	OV3600 8.2.10.0
DE33240	OV3600 deployments using CentOS 6 are impacted by CVE-2013-4885 (Nmap http-domino-enum-passwords NSE Script Arbitrary File Upload Vulnerability). **Workaround**: This issue is resolved by an upgrade to an OV3600 8.2.10.x or 8.2.4.3 deployment using CentOS 7, as CentOS 7 is not impacted by this vulnerability.	OV3600 8.2.10.1

Table 8: *Known issues in OV3600 8.2.10.0*

Bug ID	Description	Reported Version
DE33384	After an OV3600 server upgraded from OV3600 8.2.4.3 to 8.2.10.0, an auto-polling error prevented the **Home >Topology** page from loading. Log files in the /var/log/topology folder displayed an internal server error message for the event. **NOTE:** This issue is resolved in OV3600 8.2.10.1 **Workaround**: Select a monitored device to display the device in the **Devices> Monitor** page, then click **Poll Now**.	OV3600 8.2.10
DE33347	The **Devices > Monitor** page for an Aruba switch incorrectly indicates that a switch using a group template configuration has a configuration mismatch, when there is no mismatch except for the SNMPv3 auth and priv hash value.	OV3600 8.2.8.1
DE33323	The **Devices > Monitor** page for an AP incorrectly reported zero bandwidth usage during a period of continuous traffic on that device. **Workaround**: None	OV3600 8.2.5.1

Table 8: *Known issues in OV3600 8.2.10.0 (Continued)*

Bug ID	Description	Reported Version
DE33256	OV3600 reports incorrect role information for clients. When OV3600 updates incorrect role information for a user role is not entered into the ignore list of a PCI Compliance report, the report fails. **Workaround**: none:	OV3600 8.2.8.2
DE33232	Timeout issues can cause devices to disappear from the **Home > Topology** page. **Workaround**: 1. Check for the following upstream failure error in /var/log/topology, topology.1, topology.2 or topology.3. `2019-09-18 11:19:56.897 Aborting tcp connection to /127.0.0.1:60724 because of upstream failure akka.http.impl.engine.HttpIdleTimeoutException: HTTP idle-timeout encountered, no bytes passed in the last 5 minutes. This is configurable by akka.http.[server|client].idle-timeout.` 2. If you see an upstream failure as above, restart the topology using the psk topology command in the command-line interface. 3. If still some devices are still missing in the topology view, wait for automatic polling to complete, or poll those devices manually to allow them to appear in the topology.	
DE33229	OV3600 failed to perform VisualRF backups during nightly maintenance because the backup process timed out. **Workaround**: None.	OV3600 8.2.9.0
DE33178	When users assigned to a custom user role access the VisualRF feature, OV3600 displays the logon page instead of VisualRF data, and error messages are recorded to VisualRF log files. **NOTE:** This issue is resolved in OV3600 8.2.10.1. **Workaround:** Restart VisualRF by disabling and then reenabling the VisualRF engine on the **VisualRF > Setup** page.	OV3600 8.2.8.2
DE33177	When AP device groups and AP folder names contained non-ASCII (UTF-8) characters such as Japanese characters, the **Systems > Triggers** page could display the error message "The server has encountered an error while performing your request" and failed to display correct trigger data. **Workaround:** use only ASCII characters in AP folder and group names.	OV3600 8.2.8.1
DE33176	The Async Logger Service that tracks many device monitoring processes (including user-AP association) frequently stops responding. **Workaround**: None.	OV3600 8.2.6.0
DE33138	When a Cisco switch is added to OV3600 using SNMPv3 credentials, the **Connected Devices** table on the **Devices > Monitor > Neighbors** tab does not correctly display information for devices connected to the switch. **Workaround**: None.	OV3600 8.2.8.1

Table 8: *Known issues in OV3600 8.2.10.0 (Continued)*

Bug ID	Description	Reported Version
DE32795	A backup of a VisualRF Floor plan background image had a reduced image quality when the VisualRF backup was restored on another server. **Workaround**: None.	OV3600 8.2.6.0
DE32349	VisualRF incorrectly displays heatmap data for an AP on a floor above the selected floor, even if both the 5 GHz and 2.4 GHz frequencies are disabled on the heatmap view. **Workaround**: None.	OV3600 8.2.7.1
DE30939	OV3600 does not correctly display local port information for an AP associated to an Alcatel-Lucent Switch in the **Devices > Monitor > Neighbors** table for the Switch, and the AP does not appear on the **Home > Topology** page. **Workaround**: None.	OV3600 8.2.7.0
DE30461	When an user adds devices to OV3600 but does not define SNMPv3 credentials, that user cannot enable FIPS mode on the OV3600 server. **Workaround**: Delete impacted devices, enable FIPs, then add the devices again. If several devices are impacted by this issue, contact Alcatel-Lucent support for help.	OV3600 8.2.4.2
DE29085	OV3600 uses DTLS, a standard security protocol, to encrypt AMON traffic between mobility controllers and OV3600. OV3600 users must configure only one DTLS management server in a Switch running Alcatel-Lucent AOS-W 8.1or later. This issue is cause by a limitation when OV3600 interacts with a controller running ArubaOS 8.1 or later **Workaround**: Configure one DTLS management server on your Alcatel-Lucent AOS-W Switch or managed device using the command: **mgmt-server primary-server <dlst amp IP> profile default amp transport udp secure**.	OV3600 8.2.4.0
DE26895	When a user changes the default **Gain** setting for an AP on the **VisualRF > Floor Plan**s page, those changes are not saved when VisualRF is restarted. **Workaround**: None	OV3600 8.2.10.1
DE30661	An OV3600 license report incorrectly shows that there is zero license usage for a Mobility Master and Managed Devices (local Switches). This error is triggered by a communication issue between OV3600 and the Switches that prevents OV3600 from correctly decoding Switch license data. **Workaround:** None.	OV3600 8.2.5.1

Table 9: *Known issues in OV3600 8.2.9.1*

Bug ID	Description	Reported Version
DE33190	Logs files located in */var/lib/docker* are incorrectly inflating in size. This issue can impact OV3600s monitored by Aruba Glass, causing the log files to occupy all available disk space. **Workaround:** None.	OV3600 8.2.9.0

Table 10: *Known Issues in OV3600 8.2.9.0*

Bug ID	Description	Reported Version
DE33050	No appropriate status exists to indicate when an SFTP failure (between the device and OV3600) caused the switch deployment to fail. This issue occurs because OV3600 pushes the config template to the device and doesn't expect feedback until the device comes back up.	OV3600 8.2.9.0
DE33046 DE32625	Unable to view HPE (Comware) switches in Topology or interface data on switch monitoring pages when SNMP Get requests return errors. **Workaround:** Increase the SNMP agent packet size using the **snmp-agent packet max-size 3500** command on the switch.	OV3600 8.2.x.x
DE33019	After upgrading the Aruba 8320 Switch firmware from 10.02 to 10.03, or after rebooting the switch, OV3600 doesn't update the CPU Utilization, Memory, Usage graphs and other information on the switch monitoring page. This happens when OV3600 is using SNMPv3 to monitor switch **Workaround:** Restart the AMP processes, by going to **System > Status** and clicking **Restart AMP**. Or, contact Technical Support to help restart the SNMP fetcher.	OV3600 8.2.8.2
DE33008	When removing an Ethernet bond interface using the CLI, "Error adding default gateway <ip address> on eth0" is returned. This error is expected and can be ignored as the default gateway is established later in the process. **Workaround:** Not applicable.	OV3600 8.2.9.0
DE32935	In Topology, spanning tree details don't display properly for Siemens switches. **Workaround:** None.	OV3600 8.2.9.0
DE32931	OV3600 reports the incorrect interface name on the monitoring page for Siemens switches. **Workaround:** None.	OV3600 8.2.9.0
DE32929	When you import settings from the device manage page, OV3600 removes the IP address on the switch. This issue occurs if VLAN1 doesn't have any IP addresses in the running config because the **use_dhcp,ip_address,netmask** variable gets updated with null values. If you use those variables in the template to configure IP addresses for other VLANs, null values will be passed and cause template push failures and IP address removals from switch. **Workaround:** Use **use_dhcp,ip_address,netmask** variables only in VLAN1 and create and use new dynamic variables in the template for assigning IP addresses to other VLANs.	OV3600 8.2.8.2
DE32926	OV3600 doesn't display CPU and memory graphs for Siemens switches on the monitoring page. **Workaround:** None.	OV3600 8.2.9.0

Table 10: *Known Issues in OV3600 8.2.9.0 (Continued)*

Bug ID	Description	Reported Version
DE32922	Connected devices aren't showing in OV3600 for Siemens switch. **Workaround:** To see the connected devices for Siemens switches, modify the group settings: 1. Go to **Groups > Basic**; then scroll down to the **Routers and Switches** section. 2. Set the **Use Q-Bridge Forwarding Table For Generic Switches** option to **Yes**. 3. Click **Save**.	OV3600 8.2.9.0
DE32914	On the monitoring page for Siemens switches, OV3600 displays blank usage graphs. **Workaround:** None.	OV3600 8.2.9.0
DE32901	The local port information for neighbor details on the monitoring page of a Siemens switch shows the interface name instead of the interface ID. **Workaround:** None.	OV3600 8.2.9.0
DE32854	A switch provisioned using ZTP doesn't join the same group or folder. On the OV3600-side, the member 1 MAC address is added to the whitelist, but, on the switch-side, member 2 is the commander. During ZTP, OV3600 expects the commander's MAC address to be in whitelist, and, since the member 2 MAC address isn't in the whitelist, OV3600 doesn't move the device to the respective folder and group. **Workaround:** Enter the **redundancy switch over** command to force the commander status to member 1. This triggers ZTP, OV3600 and moves the device to the respective folder and group.	OV3600 8.2.8.1
DE32848	The usage graph in controller monitoring page for the mobility device reports the data for client usage twice although only one client is connected. **Workaround:** None.	OV3600 8.2.9.0
DE32840	OV3600 doesn't back up the Alcatel-Lucent 9004 controller after you click **Create Backup** on the Config page. **Workaround:** None.	OV3600 8.2.9.0
DE32797	Advanced search won't work if RAPIDS is hidden from the navigation menu. **Workaround:** Go to **AMP Setup > General > AMP features** and change the **Display RAPIDS** option to **Yes**.	OV3600 8.2.8.1
DE32655 DE32654	The usage graph was blank in an Alcatel-Lucent AOS-W 8.x.x.x cluster setup due to invalid data in the **AMON_BSSID_TUNNEL_STATS_MESSAGE** on the controller. **Workaround:** Upgrade the Switch to Alcatel-Lucent AOS-W 8.4.0.3.	OV3600 8.2.8.2

Table 10: *Known Issues in OV3600 8.2.9.0 (Continued)*

Bug ID	Description	Reported Version
DE32560	VisualRF page does not load. **Workaround:** Follow these steps to clear the caches and restart VisualRF: 1. Contact Technical Support to help clear the Redis cache. 2. From the CLI, select **11** to open the Enter Commands menu. 3. At the prompt, enter **remove_visualrf_cache**. 4. From the WebUI, go to **VisualRF > Setup**, and, under the Server Settings, click **No** for the "Enable VisualRF Engine" option and click **Save** to stop VisualRF. 5. Change the setting back to **Yes** and click **Save** to restart VisualRF.	OV3600 8.2.7.1
DE32353	When you add Instant APs to a group and then go to **Firmware > Update**, OV3600 doesn't show the latest firmware codes for the Instant APs. **Workaround:** None.	OV3600 8.2.7.1
DE32084	Database cleaning fails with the error message: **ERROR: cannot freeze committed xmax**. This issue is related to a database issue in PGSQL 9.4.17, which OV3600 uses. **Workaround:** Contact Technical Support to help manually fix the failed table.	OV3600 8.2.7.0
DE31913	Any hotspot device which is broadcasting SSID other then the SSID we have entered in valid rule should be contained. **Workaround:** None.	OV3600 8.2.7.0
DE31875	OV3600 8.2.4.1 to OV3600 8.2.6.1 upgrade failed. This issue occurs when installing or upgrading OV3600 8.2.6.x on RHEL. **Workaround:** None.	OV3600 8.2.6.1

This chapter provides the following information to help you with the upgrade process:

- "Minimum Requirements" on page 41
- "Verify Current CentOS Version" on page 41
- "Upgrade Paths" on page 41
- "Upgrade from OV3600 8.2.9.x or 8.2.10.x with CentOS 6 Migration" on page 41
- "Upgrade from OV3600 8.2.4.3 or 8.2.10.x with CentOS 7" on page 44

Minimum Requirements

Ensure that you have sufficient disk storage, memory, and hardware or software versions. As additional features are added to OV3600, increased hardware resources become necessary and hardware requirements vary by version. For the most recent hardware requirements, refer to the *OmniVista 3600 Air Manager 8.2.10.0 Server Sizing Guide*.

Verify Current CentOS Version

Before you upgrade, verify the version of CentOS currently running on your OV3600 server.

1. From the OV3600 command-line interface, enter **8** to select **Advanced**, then enter **2** to select **Enter Commands**.
2. Enter the command **$osrel**.

The output of this command indicates the version of CentOS currently in use. Use this information to determine your upgrade path.

Upgrade Paths

Your upgrade workflow depends on your current version of OV3600 and CentOS:

- To upgrade from OV3600 8.2.9.x, or OV3600 8.2.10.x with CentOS 6, follow the steps in "Upgrade from OV3600 8.2.9.x or 8.2.10.x with CentOS 6 Migration" on page 41
- To uprade from OV3600 8.2.4.3 or OV3600 8.2.10.x with CentOS 7, follow the steps in "Upgrade from OV3600 8.2.4.3 or 8.2.10.x with CentOS 7" on page 44.

NOTE

If you are upgrading from OV3600 8.2.8.x or earlier, contact Technical Support for help with a multiple-step upgrade path.

Upgrade from OV3600 8.2.9.x or 8.2.10.x with CentOS 6 Migration

OV3600 8.2.11.0 requires an upgrade to CentOS 7. The migration process involves upgrading to OV3600 8.2.10.1, backing up your data, exporting the backup file, performing a fresh install of OV3600 8.2.10.1 and CentOS 7 on your server, then restoring the backup data onto that server and then upgrading to OV3600 8.2.11.0.

After you perform this upgrade, follow the steps in "Upgrade from OV3600 8.2.4.3 or 8.2.10.x with CentOS 7" on page 44 to upgrade to 8.2.11.0.

NOTE

Upgrade to OV3600 8.2.10.1 before backing up your data. You cannot restore an OV3600 8.2.8.x, 8.2.9.x, or 8.2.10.0 (on CentOS 6) backup on an OV3600 server running OV3600 8.2.10.1.

NOTE

For more information on creating backups of your data, refer to the **System Pages** section of the OV3600 User Guide. For information on performing a fresh installation of OV3600 8.2.11.0, refer to the OV3600 Installation Guide.

NOTE

Upgrades from OV3600 8.2.8.x, 8.2.9.x, or 8.2.10.0 on CentOS 6 might fail with the following PuTTY fatal error message: **Server unexpectedly closed network connection** when your SSH session becomes unresponsive.
To avoid this issue, change the keep-alive interval to a low setting as follows:
1. Using a terminal console, such as PuTTY, open an SSH connection with the OV3600.
2. Enter 30 to 60 seconds for sending null packets between keep-alive messages.

Before You Begin

Prior to migration, navigate to **Home > License** and save a copy of the license key. OV3600 licenses are associated with the server IP address. All new installations of OV3600 have a 90-day grace period for licenses.

Keep these considerations in mind when working with OV3600 licenses:

- If you plan to reuse the same IP address, then apply the license key after you restore the OV3600 8.2.9.x backup.
- If you are planning to migrate data to a new server, work with Aruba support or use the license portal, to generate the new license in advance, then follow the migration path and apply the new license key. Keep in mind that you may have to adjust some devices (such as Instant APs and devices that send AMON or syslog messages to OV3600) in order for those devices to send updates to the new IP address.

Step 1: Upgrade to OV3600 8.2.10.1

1. Log in to the OV3600 server with the "ampadmin" user name and password. If you previously changed the ampadmin user name and password, enter the current admin name and password.
2. Enter **4** to select **System**.
   a. At the next prompt, enter **1** to select **Upgrade,** then enter 1 to select **Upgrade OV3600 Management Software.**
   b. Select the option for **8.2.10.1**.

NOTE

If the **8.2.10.1** software doesn't appear in the list of local upgrade versions, select option **2 None of the Above**, then manually enter **8.2.10.1**.

   c. Enter **y** to enable OV3600 to connect to a proxy server. Or, you can enter **N** to bypass this step and go to step d on page 42 to download the software. At the next prompt:
      (1) Enter the server address and port number (for example, *test.proxy.com* and port *22*).
      (2) Enter **y** to enter the proxy user name and password (for example, *testuser* and *password*).
   d. Enter **1** or **2** to log in to your customer portal with your support user name and password.
   e. Follow the onscreen instructions to download the software.

Step 2: Back up your OV3600 8.2.10.x Data

1. Log in to the OV3600 server with the "ampadmin" user name and password. If you previously changed the "ampadmin" user name and password, enter the current credentials.
2. Enter **2** to select **Backup**
3. Enter 1 to open the **Backup** menu.

4. Enter 1 to select the **Backup Now** option.

Step 3: Export the Backup

1. After creating your backup, enter **b** to return to the previous **Backup** menu
2. Enter **5** to open the **Users** menu options, then enter **3** to add a file transfer user.
3. Enter a user name for the file transfer user, then click **Enter**. The user name for an OV3600 image file transfer user must be five characters or longer, and contain only lowercase letters and numbers. To use the default file transfer user name **awscp**, click **Enter** without entering a user name.
4. Enter a password for the file transfer user, then click **Enter**.The password must be eight characters or longer, and can contain uppercase and lowercase letters, numbers, and non-alphanumeric characters. Spaces are not allowed.
5. Enter **b** to go back to the main CLI menu.
6. Use SCP to connect to your remote repository and move the OV3600 8.2.10.1 backup file from the OV3600 **/user** directory to a remove server.

Step 4: Migrate to CentOS 7.7

Perform a fresh installation of OV3600 8.2.10.1 to automatically upgrade CentOS 6.x to CentOS 7.7.

NOTE

For more information on installing a new instance of OV3600 8.2.10.1 on your server, refer to the OmniVista 3600 Air Manager 8.2.11.0 Installation Guide.

Step 5: Upload the Backup

Follow one of these steps to upload the backup on the OV3600 8.2.10.1 server:

- If using SCP, enter **1-1** to open the **File** and **Upload File** menus. Provide the user name, host, and path for an SCP server using FIPS-approved encryption.
- If using SFTP, enter **5-3** to open the **User** and **Add File Transfer User** menus. Log in from another system using those credentials, and upload the backup.

Step 6: Restore the Data

Follow these steps to restore the backup on OV3600 8.2.10.1:

1. From the OV3600 CLI, enter **2-2** to open the **Backups** and **Restore** menus.
2. Enter **1** to restore the server from the uploaded backup.

Step 7: Install Certificates

In this step, you will add an SSL certificate, or generate a certificate signing request and install a signed certificate.

To add the SSL certificate:

1. From the command-line interface, enter **3-4** to open the **Configuration** and **Certificates** menus.
2. Enter **1** to open the **Add SSL Certificate** menu.
3. Follow the prompt to install the SSL certificate on your AMP server. The signed certificate should be in PKCS12 format with a *.pfx or *.p12 file extension.

To generate a CSR and install the certificate:

1. From the command-line interface, enter **3-4** to open the **Configuration** and **Certificates** menus.
2. Enter **2** to open the **Generate Certificate Signing Request** menu.
3. Follow the prompt to creates a CSR that identifies which server will use the certificate.

4. Next, enter **b** to return to the previous menu,
5. Enter **1**-**2** to open the **Files** and **Download File** menu to download the resulting CSR.
6. Send the CSR to your certificate signer.
7. Once the certificate is signed, upload the certificate to the OV3600 8.2.10.1 server.
   - If using SCP, enter **1-1** to open the **File** and **Upload File** menus. Provide the user name, host, and path for an SCP server using FIPS-approved encryption.
   - If using SFTP, enter **5-3** to open the **User** and **Add File Transfer User** menus. Log in from another system using those credentials, and upload the backup.
8. From the WebUI, go to **Device Setup** > **Certificates**, then click **Add** to add a trusted root CA certificate. Provide the following information:
   - Certificate name.
   - Certificate file. Click **Upload File** to find the certificate file on your local system, then click **Open**.
   - Password.
   - Certificate format.
   - Certificate type.
9. From the **3-4 Configuration** and **Certificates** menu, enter **3** to open the **Install Signed Certificate** menu.

10.Follow the prompts to install the certificate.

Step 8: Upgrade to OV3600 8.2.11.0

Proceed to "Upgrade from OV3600 8.2.4.3 or 8.2.10.x with CentOS 7" on page 44.

Upgrade from OV3600 8.2.4.3 or 8.2.10.x with CentOS 7

An upgrade from OV3600 versions 8.2.4.3 or 8.2.10.x using CentOS 7 is straightforward and does not require a CentOS migration. Use the AMP CLI to install the OmniVista 3600 Air Manager 8.2.11.0 upgrade package on your system. If your network doesn't allow OV3600 to connect to the Internet, you must manually download the software and upload the software before performing this upgrade.

NOTE

OV3600 8.2.11.0 fixes an online upgrade running CentOS 7 from OV3600 8.2.11.0 to future versions. To upgrade from OV3600 8.2.10.x, you must contact Technical Support to apply a patch.

NOTE

You can change the existing amprecovery user name by backing up the server, reinstalling the software, and restoring from the backup. For information about setting up the amprecovery account, refer to "Installing the Software (Phase 2) " on page 1 in the *OV3600 8.2.11.0 Installation Guide*.

NOTE

Upgrades from OV3600 8.2.10.0 to 8.2.10.1 on CentOS 7 might fail with the following PuTTY fatal error message: **Server unexpectedly closed network connection** when your SSH session becomes unresponsive.
To avoid this issue, change the keep-alive interval to a low setting as follows:
1. Using a terminal console, such as PuTTY, open an SSH connection with the OV3600.
2. Enter 30 to 60 seconds for sending null packets between keep-alive messages.

Follow these steps to upgrade to OV36008.2.11.0:

1. Log in to the OV3600 server with the "ampadmin" user name and password. If you subsequently changed the "ampadmin" user name and password, enter the current admin name and password.
2. Enter **4** to select **System**.
   a. At the next prompt, enter **1** to select **Upgrade**.
   b. Select the option for **8.2.11.0**.

NOTE

If the 8.2.11.0 software doesn't appear in the list of local upgrade versions, select option **2 None of the Above**, then manually enter **8.2.11.0**.

c. Enter **y** to enable OV3600 to connect to a proxy server. Or, you can enter **N** to bypass this step and go to step d on page 42 to download the software. At the next prompt:

   (1) Enter the server address and port number (for example, *test.proxy.com* and port *22*).

   (2) Enter **y** to enter the proxy user name and password (for example, *testuser* and *password*).

d. Enter **1** or **2** to log in to your customer portal with your support user name and password.

e. Follow the onscreen instructions to download the software.

Manually Download the Software

You can manually download the software if your OV3600 server can't access the Internet.

1. Enter your Alcatel-Lucent support user name and password to get the software from the Alcatel-Lucent Support Center.
2. Click the upgrade package, then click **Save** and install the file later.
3. Define a user that can transfer OV3600 images, and then upload the software:

NOTE

For security purposes, image file transfer users are automatically removed every night during nightly maintenance operations.

4. From the OV3600 command-line interface, with the "ampadmin" user name and password. If you subsequently changed the ampadmin user name and password, enter the current admin name and password.
5. Add a file transfer user. This process varies, depending upon the version of OV3600 currently running on your system.
   a. *If you are upgrading from OV3600 versions 8.2.10.x or 8.2.4.3*, enter **5** to open the **Users** menu options, then enter **3** to add a file transfer user.
   b. *If you are upgrading from OV3600 8.2.9.x*, enter **8** to open the **Advanced** menu options, then enter **7** to add a file transfer user.
6. Enter a user name for the file transfer user, then click **Enter**. The user name for an OV3600 image file transfer user must be five characters or longer, and contain only lowercase letters and numbers. To use the default file transfer user name **awsftp**, click **Enter** without entering a user name.
7. Enter a password for the file transfer user, then click **Enter**.The password must be eight characters or longer, and can contain uppercase and lowercase letters, numbers, and non-alphanumeric characters. Spaces are not allowed.
8. Enter **b** to go back to the main CLI menu.
9. Use SFTP to connect to your remote repository and upload the OV3600 8.2.11.0 upgrade file from the remote server into the OV3600 **/user** directory.