OmniVista 3600 Air Manager 8.2.13.1

Alcatel·Lucent Enterprise

Release Notes

Chapter 2
Revision History

The following table lists the revision numbers and the corresponding changes that were made in this release:

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

Chapter 1
Release Overview

OmniVista 3600 Air Manager 8.2.13.1 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 describes new features in this release.
- Resolved Issues describes the issues we've fixed.
- Known Issues describes known issues.
- Upgrade Instructions 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 introduces new features and fixes to issues detected in previous releases. There are no licensing changes in this release.

For a complete list of supported products and validated firmware versions, refer to the *OmniVista 3600 Air Manager 8.2.13.1 Supported Infrastructure Devices*.

New Features

Prefer AMON for New Rogue AP Detection

OV3600 8.2.13.1 now uses an AMON feed to detect a new rogue AP from a controller, but continues to poll SNMP for regular AP updates.

To use an AMON feed to detect a new rogue AP, set the **Prefer AMON for new rogue AP detection** option to **Yes** in the **OV3600 Setup > General > Additional AMP Services** page.

Download Crash File

OV3600 8.2.13.1 now allows users to download the crash file of the device crash trigger.

To download the crash dump, navigate to the **System >Alerts** page and click the **Download crash file** link.

Support for AP-635

OV3600 8.2.13.1 introduces support for a new device, AP-635.

In OV3600 8.2.13.1 release, VisualRF supports AP-635 in planning mode only. The complete AP support will be added in OV3600 8.2.14.0 release.

For more information, see ***OV3600 Supported Infrastructure Devices*** document.

AP1X Certificates

OV3600 8.2.13.1 introduces **AP1X CA Cert** and **AP1X Client Cert** options in the **Device Setup > Certificates** page that allows an IAP to authenticate against a switch in the uplink.

Support for HPE 5710 Switch Series

OV3600 8.2.13.1 introduces support for HPE 5710 Switch Series.

For more information, see ***OV3600 Supported Infrastructure Devices*** document.

IPsec Tunnel Monitoring

OV3600 8.2.13.1 now supports monitoring of an IPsec tunnel between a Mobility Conductor and a managed device.

To view the IPsec tunnel information, navigate to **Devices > List > Advanced Monitoring** page and select an IPsec tunnel from the **Tunnel Details** drop-down list.

Annotate Unauthenticated Clients

OV3600 8.2.13.1 now allows users to annotate unauthenticated wired clients within a group in bulk. The bulk annotation of unauthenticated clients can be done at the group level for switches within a group.

To annotate an unauthenticated wired client, navigate to **Groups > List > Basic** page and set the **Annotate Unauthenticated Clients** option to **Yes**.

Support for OAW-AP534

OV3600 8.2.13.1 introduces support for a new device, OAW-AP534.

For more information, see ***OV3600 Supported Infrastructure Devices*** document.

Default Wired Port Profile

OV3600 8.2.13.1 now allows users to edit the settings of a default wired port profile.

For more information, see ***OV3600 Deployment Guide*** document.

Support for ArubaOS-CX 4100 Switch Series

OV3600 8.2.13.1 introduces support for ArubaOS-CX 4100 Switch Series.

For more information, see ***OV3600 Supported Infrastructure Devices*** document.

Disabling Heap Dump

OV3600 8.2.13.1 introduces the `disable_heapdump` command that disables the Java memory dump (hprof) getting generated when VisualRF experiences performance issues. The same command is used to enable the Java memory dump.

Intelligent Power Monitoring

OV3600 8.2.13.1 now supports the Intelligent Power Monitoring (IPM) feature that actively measures the power utilization of an AP and dynamically adapts to the power resources. IPM allows you to define the features that must be disabled to save power, allowing the APs to operate at a lower power consumption without hampering the performance of the related features.

In the **Groups > List > Instant Config** page, navigate to **System > IPM** and select the **IPM Activation** check-box to enable IPM.

Chapter 3
Resolved Issues in OV3600 8.2.13.1

This section describes the issues resolved in this release.

Table 2: *Resolved Issues in OV3600 8.2.13.1*

Bug ID	Description	Reported Version
DE34786	The **Traffic Analysis** data was unavailable even though the data was available in the **Traffic Analysis Data Retention Interval**.	OV3600 8.2.11.0
DE34891	In the **Devices > Device Configuration** page, the **Config Backups** data was unavailable for the HPE 5710 switch.	OV3600 8.2.11.2
DE34926	OV3600 was unable to push the AP1X TLS certificates to the uplink ports of all the Instant APs within the group.	OV3600 8.2.8.1
DE34975	The user was unable to perform an online upgrade of OV3600 server from the AMP CLI even after downloading the upgrade package from Aruba Support Portal (asp.arubanetworks.com).	OV3600 8.2.11.1
DE35006	The **Client Diagnostics** page displayed stale wired clients for the uplink ports of a switch.	OV3600 8.2.11.2
DE35112	After an upgrade to OV3600 8.2.12.1, the **Traffic Analysis Client Sessions Processor** restarted repeatedly.	OV3600 8.2.12.1
DE35114	The Aruba branded Alcatel Lucent AP-534 device model was not recognized on Alcatel OV3600.	OV3600 8.2.11.1
DE35131	The topology map in the **Home > Topology** page did not display all the switches managed by OV3600. Also, the topology of the devices changed frequently.	OV3600 8.2.13.0
DE35178	The user was unable to edit the default wired port profile in the **Groups > Instant Config** page.	OV3600 8.2.11.0
DE35197	During an upgrade, the **Sequential Reboot** feature in the **Groups > Firmware** page did not work properly for the Instant AP clusters managed by OV3600.	OV3600 8.2.12.1
DE35202	The user was unable to transfer the automatic backup file to the jump servers.	OV3600 8.2.12.1
DE35212	The RADIUS authentication failed after the OV3600 server was upgraded from 8.2.11.1 to 8.2.12.1.	OV3600 8.2.12.1
DE35222	The topology map in the **Home > Topology** page did not display all the switches managed by OV3600. Also, the topology of the devices changed frequently.	OV3600 8.2.12.1
DE35223	Some APs were shown as down in OV3600 because of process restarts caused by the high memory utilization of Redis process.	OV3600 8.2.12.1

Bug ID	Description	Reported Version
DE35253	The user was unable to create a SSID when the **High throughput** option was unchecked in the **Groups > Instant Config** page and an error message was displayed. This issue was observed in Instant AP clusters running firmware version 6.5.4.19 and managed by OV3600 Instant GUI Config (IGC).	OV3600 8.2.12.1
DE35272	An OV3600 user with a read-only user role was unable to view all the alerts in the **Alerts & Events** page.	OV3600 8.2.12.1
DE35275	OV3600 generated incorrect information when the **Export CSV** option was clicked in the **Devices > Monitor > Alerts & Events** page.	OV3600 8.2.12.1
DE35277	OV3600 displayed incorrect memory utilization for the Clear Pass Policy Manager (CPPM) servers in the **Devices > Monitor** page.	OV3600 8.2.12.1
DE35298	Security vulnerabilities were discovered in OV3600 8.2.13.0.	OV3600 8.2.13.0
DE35314	By default, OV3600 has a limit of 1000 lines for exporting the report through pdf in email and anything beyond will return "**Detail sections have been omitted from this email because they are too large**".	OV3600 8.2.13.0

Chapter 4
Known Issues in OV3600 8.2.13.1

Following are the known issues observed in this release.

Table 3: *Known Issues in OV3600 8.2.13.1*

Bug ID	Description	Reported Version
DE34756	The user is able to monitor or view the Cisco 9800 WLC device in the **Devices > List > Devices List** table. However, the **Location** column in the **Device List** table does not display any data corresponding to the device. Also, the event logs for the controller displays the **Not applying configuration because thin APs have not read configuration** error message.	OV3600 8.2.9.1
DE34849	SSH or Telnet command timed out message appears in the AMP **Events Log** and the controller configuration backup fails, although SSH or Telnet credentials are correct in the OV3600 UI.	OV3600 8.2.11.1
DE35291	The Instant APs within a group are shown in a **Mismatched** state after **Server Cert** is pushed from the OV3600 server.	OV3600 8.2.13.1
DE35312	If the AMON data processing is disabled in OV3600, the **Client Connection Mode** displays incorrect mode when a client connects to the 6 GHz radio.	OV3600 8.2.13.1
DE35320	In the **Instant Config > Networks** page, the **default_wired_port_profile** does not display the override settings icon even though an override was available. **Workaround:** Navigate to the **default_wired_port_profile** page, delete the overrides present in the **VC List** page, and then **Apply** the settings.	OV3600 8.2.13.1
DE35361	In the **Instant Config > System > Uplink** page, the **6GHz** option is unavailable in the **Bands** drop-down list for Instant AP groups containing AP-635 running on firmware version 8.9.0.0.	OV3600 8.2.13.1
DE35362	In the **Instant Config > Networks > General** page, the **6 GHz** parameters are unavailable in the **Transmit Rates** option for Instant AP groups containing AP-635 running on firmware version 8.9.0.0.	OV3600 8.2.13.1
DE35363	In the **Instant Config > System > Uplink** page, the **WPA-3 Personal** option is unavailable in the **Key management** drop-down list for Instant AP groups containing AP-635 running on firmware version 8.9.0.0.	OV3600 8.2.13.1
DE35369	The 6GHz Phytype9 elements are missing from the **monStaInfoPhy** and **monAPInfoPhyType** SNMP Objects.	OV3600 8.2.13.1
DE35371	Support for 160 MHz channel width in AP-635 is unavailable for 5GHz radio in the **Groups > Instant Config** page.	OV3600 8.2.13.1
DE35372	Instant APs running firmware version 8.9.0.0 did not validate incorrect DHCP server IP address as OV3600 server configures only a valid DHCP IP address successfully.	OV3600 8.2.13.1

Bug ID	Description	Reported Version
DE35385	Some AP-635 access points within a group are shown in a **Mismatched** state when you configure the Wi-Fi2 access mode for the 6 GHz radio in the **Groups > Instant Config > Access Points** page.	OV3600 8.2.13.1
DE35399	OV3600 8.2.13.1 web application uses a JavaScript library that contains at least one vulnerability. A vulnerability is found in Angular up to 11.0.4/11.1.0-next.2 on npm (JavaScript library) that is classified as problematic. An unknown function of Application Handler is affected which manipulates with an unknown input that leads to a cross-site scripting vulnerability.	OV3600 8.2.13.1

Chapter 5
Upgrade Instructions

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

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 latest *OmniVista 3600 Air Manager 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
- To uprade from OV3600 8.2.4.3, OV3600 8.2.10.x, or OV3600 8.2.11.x with CentOS 7, follow the steps in Upgrade from OV3600 8.2.4.3, 8.2.10.x or 8.2.11.0 with CentOS 7.

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 8.2.13.1 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 8.2.13.1.

After you perform this upgrade, follow the steps in Upgrade from OV3600 8.2.4.3, 8.2.10.x or 8.2.11.0 with CentOS 7 to upgrade to 8.2.13.1.

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 OV36008.2.13.1.

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 OV36008.2.13.1, refer to the OV3600 Installation Guide.

Upgrades from 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 ManagementSoftware**.

b. Select the option for **8.2.10.1**.

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 on page 13 to download the software. At the next prompt:

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

   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

Perform a fresh installation of OV3600 8.2.10.1 to automatically upgrade CentOS 6.x to CentOS 7.

For more information on installing a new instance of OV3600 8.2.10.1 on your server, refer to the OV3600 8.2.10.1 Installation Guide*Pre-Installation Checklist.*

Step 5: Upload the Backup

Follow one of these steps to upload the backup on the OV3600 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 8.2.12.0

Proceed to Upgrade from OV3600 8.2.4.3, 8.2.10.x or 8.2.11.0 with CentOS 7.

Upgrade from OV3600 8.2.4.3, 8.2.10.x or 8.2.11.0 with CentOS 7

An upgrade from OV3600 versions 8.2.4.3, 8.2.10.x or 8.2.11.0 using CentOS 7 is straightforward and does not require a CentOS migration. If you are upgrading from OV3600 versions 8.2.4.3 or 8.2.10.x upgrade to OV3600 8.2.11.x before upgrading to OV3600 8.2.12.0.Use the AMP CLI to install the OmniVista 3600 Air Manager 8.2.13.1 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.

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)* in the *OV36008.2.13.1 Installation Guide*.

Follow these steps to upgrade to OV3600 8.2.13.1:

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 **8.2.13.1**.

If the 8.2.13.1 software doesn't appear in the list of local upgrade versions, select option **2 None of the Above**, then manually enter **8.2.13.1**.

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 on page 13 to download the software. At the next prompt:

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

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.

Upgrade to OV3600 8.2.12.0 in Aruba Central (on-premises) Server

If you are performing a fresh installation of OV3600 8.2.12.0 on Aruba Central (on-premises) servers, interfaces on the Aruba Central (on-premises) server will always be in the following order:

- eth0- eth3 – 1G interfaces
- eth4 and eth5 - 10G interfaces

If you are upgrading from a prior OV3600 version to OV3600 8.2.12.0 on Aruba Central (on-premises) servers, the following message is displayed.

```
Running Upgrade

Local upgrade versions:

1. 8.2.12.0.20201112.0001
2. None of the above.

Which version? 1
Upgrading to 8.2.12.0.20201112.0001.  The system will be rebooted when the upgrade completes.
Proceed? (y/N) y
Upgrade script AMP-8.2.12.0.20201112.0001-amp_upgrade was not found in local cache.
Upgrade package found in local cache.
Validating the upgrade package...
Using upgrade script extracted from local package.
Upgrade package found in local cache.

 Vendor = HPE , Product = ProLiant DL360 Gen10

 Old Version --> 8.2.11.0 ; New Version --> 8.2.12.0.20201112.0001
Do not proceed if you are not using console. You may lose connectivity and must
reconfigure network from "Configuration->Configure Network Settings" menu using
the console after upgrade. Would you like to continue with the upgrade? (y/N):
```

Perform the following steps on Aruba Central (on-premises) server Gen10 server with both 1G and 10G interfaces only.

1. Run upgrade to OV3600 8.2.12.0.
2. Post upgrade, run **intfinorder**, reboot, and configure network setup by entering the following options in AMP CLI:

a. Enter option **8 - Advanced**.

b. Enter option **1 - Custom Commands**.

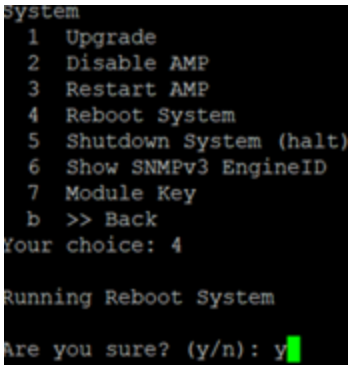
c. Enter option **2 - Enter Commands**.

d. This will run the enter commands, execute **$ intfinorder**

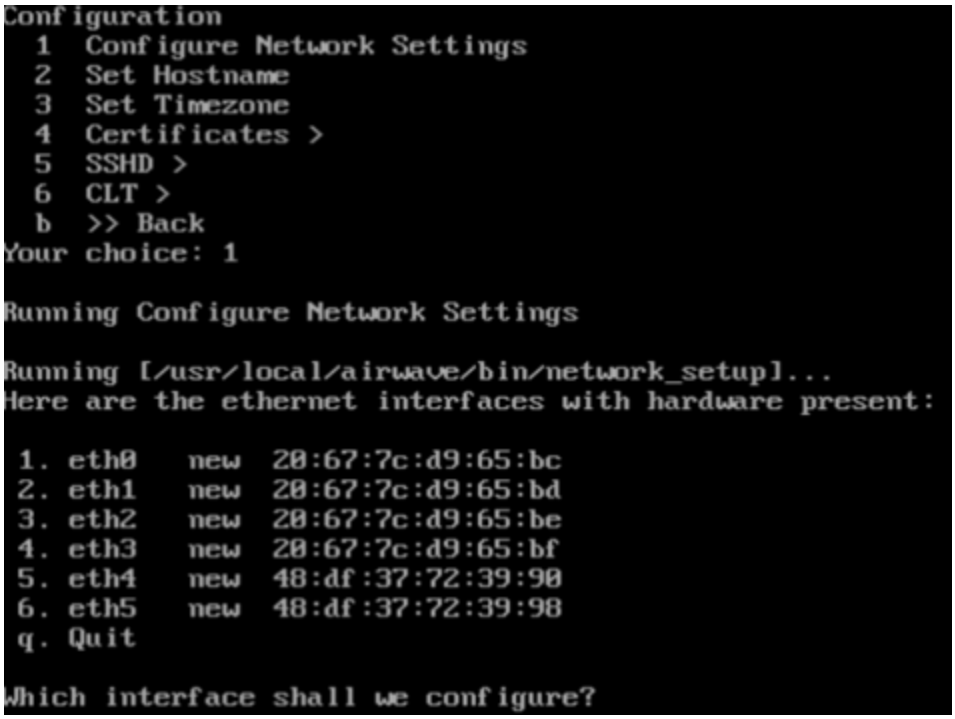
```
Advanced
  1  Custom Commands >
  2  Enter Commands
  b  >> Back
Your choice: 2

Running Enter Commands

Type 'help' for the list of commands.
$ intfinorder
Use this script on HPE physical appliance especially if you intend to use 10G ports.
Running this script will ensure interfaces are detected / named in the same order
everytime the system is rebooted. Not required to be run for systems using fresh installed 8.2.12
and beyond releases.


 Please make sure you have console access. You need to reboot and do a network setup (AMPCLI->Configura
tion (3) -> Configure Network Settings(1)) post reboot after the execution of this command.

 Do you want to continue (y/N)? :
```

e. Click **y** when prompted with **Do you want to continue (y/N)? :** message.

3. Type **exit** and navigate to the CLI prompt and select option **4 – System** and then, select option **4 - Reboot System** to reboot the system.



4. If you lose connection to Aruba Central (on-premises) server post step 3, login to the ILO/console of the server and navigate to the CLI prompt, and select option **3 – configuration** and **option 1- Configure Network Settings**.



5. Select the proper network interface and configure the IP address for your AMP and commit the changes. The AMP should be reachable with the IP address configured.

   This will enable reliable ordering of interfaces in upgrade scenario that is, eth0 - eth3 mapped to1G interfaces and eth4 -eth5 mapped to 10G interfaces at the end. Once interfaces are set in proper order, future AMP upgrades will be smooth. The intfinorder script should be run mandatorily from the AMPCLI menu as described above for users using Aruba Central (on-premises) server after upgrading to 8.2.12 build.

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:

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, 8.2.11.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 8.2.13.1 upgrade file from the remote server into the OV3600 **/user** directory.