文書番号： FY20-HPN-036

2020 年 2 月吉日

お客様各位

日本ヒューレット・パッカード株式会社
Aruba 事業統括本部

Aruba Instant Access Points シリーズの証明書失効に関する事象について（Rev-3）

拝啓、貴社益々ご清栄のこととお喜び申し上げます。平素は格別のご高配を賜り、厚く御礼申し上げます。
この度、Aruba Instant Access Points（以下：IAP）と Aruba Central、Activate、AirWave 間の通信に関する不具合が確認されました。この不具合は、Instant OS 内の Trust Anchor（以下：TA）ファイルの SSL 証明書に関するもので脆弱性に係る事象ではございませんが、IAP との管理通信に支障きたす恐れがあります。2020 年 2 月 7 日までに以下のアクションを実施頂く事で本不具合は解消されますので、対処方法について下記にご案内いたします。

敬具

記

1. 事象について

TA 証明書バンドルに含まれている証明書のうち、Verisign 社が発行した証明書の 1 つが 2020 年 2 月 7 日に失効予定です。Instant OS 内に失効した証明書が含まれている場合、他の有効な証明書を使用しない不具合が SSL ライブラリに確認されました。この不具合により IAP と Central、Activate、AirWave 間の SSL 通信ができなくなる事象が発生します。

Central、Activate、AirWave と SSL 通信を使用していない場合は、2020 年 2 月 7 日以降も問題なくご利用頂けます。また、2020 年 2 月 7 日より前に確立した通信は、切断されるまで継続して利用可能ですが、切断後は新規通信を確立することができず、IAP は local management モードに切り替わります。再接続するためには、手動で IAP をアップグレードする必要があります。以上より、2020 年 2 月 7 日までにアップグレードすることを強く推奨致します。

2. 影響を受ける製品

Aruba Central にて管理されている IAP

Affected Software Version (Currently Supported Only)	Affected IAP Platforms
All software versions prior to the following patches in each of the respective release streams: ・6.4.4.8-4.2.4.16 ・6.5.4.15 ・8.3.0.11 ・8.4.0.6	All IAP platforms (IAP-1XX, RAP-XXX, IAP-2XX, IAP-3XX and IAP-5XX series products)

・8.5.0.5	
Instant 8.6.0.0	RAP-155, IAP-214, IAP-215, IAP-224, IAP-225, IAP-228, IAP-274, IAP-275, and IAP-277

Airwave にて証明書認証を用いて管理されている IAP

Affected Software Version (Currently Supported Only)	Affected IAP Platforms
All software versions prior to the following patches in each of the respective release trains: ・6.4.4.8-4.2.4.16 ・6.5.4.15 ・8.3.0.11 ・8.4.0.6 ・8.5.0.5 ・8.6.0.1	All IAP platforms (IAP-1XX, RAP-XXX, IAP-2XX, IAP-3XX and IAP-5XX series products)
Instant 8.6.0.1	All AP-3XX, and AP-5XX, AP203H/203R/203RP, and IAP-207

3. 影響を受けない製品

Software Version	IAP Platforms
AP platforms running the following software versions: ・6.4.4.8-4.2.4.16 or later ・6.5.4.15 or later ・8.3.0.11 or later ・8.4.0.6 or later ・8.5.0.5 or later ・8.6.0.2 or later	All IAP platforms (IAP-1XX, RAP-XXX, IAP-2XX, IAP-3XX and IAP- 5XX series products)
AP platforms running Instant 8.6.0.1	RAP-155, IAP-214, IAP-215, IAP-224, IAP-225, IAP-228, IAP-274, IAP-275, and IAP-277
Controller-based access points (CAP) and Remote access points (RAP)	

4. 影響を受ける構成
影響を受ける製品およびソフトウェアバージョンをご利用で、下記のいずれかに IAP がアクセスする構成
・Central
・Activate

・AirWave にて証明書認証を利用している場合

5. 影響を受けない構成
・AirWave にて PSK 認証を利用している場合
・Central、Activate、AirWave のいずれも使用せず、ローカルで IAP を管理している場合
・修正済みバージョンで出荷された AP
・コントローラ管理の AP
・工場出荷状態でプロビジョニングされていない AP がインターネットに接続出来る環境で展開され Activate と通信が行える場合、修正済ソフトウェアバージョンに強制的にアップグレードされます。
【強制アップグレード動作条件】
・完全工場出荷状態であること
・推奨バージョンより古いファームウェアであること
・DHCP サーバから IP アドレス、DNS サーバ情報が自動的に付与され、インターネットアクセスができること

※2020 年 2 月 3 日から 2020 年 2 月 7 日までは、AP で使用中の OS と同一リリースストリーム修正済みバージョンにアップグレードします。
※2020 年 2 月 7 日以降は、8.6.0.2 にアップグレードします。現時点でサポート対象の AP のうち 8.6.x をサポートしない AP については、下記の修正済みバージョンにアップグレードします。
・RAP-3, IAP-104, IAP-105, IAP-134, IAP135, and IAP-175 will be upgraded to Instant OS 6.4.4.8-4.2.4.16.
・IAP-204, IAP-205, IAP-205H, IAP-114, IAP-115, RAP-108, RAP-109, and IAP-103 will be upgraded to Instant OS 6.5.4.15.

※また、Instant OS 8.5.0.0 以降よりデフォルトの管理パスワードが、AP のシリアル番号に変更となっていますのでご注意下さい。
※修正済みバージョンイメージの URL については、原文をご確認下さい。
※工場出荷状態でプロビジョニングされていない AP がインターネットに接続出来ない環境で展開される場合、強制アップグレードは行われません。この場合、クラスター構成内のマスター AP のローカル管理オプションを使用して手動でアップグレードを行う必要があります。

6. 対処しない場合
影響を受ける製品および構成をご利用お客様で 2020 年 2 月 7 日までに IAP をアップグレードしない場合、IAP と Central、Activate、AirWave 間の新規 SSL 通信ができなくなり、IAP を管理することができません。なお、無線通信には影響はありません。

7. 対処方法
下記の修正済み OS バージョンにアップグレードしてください。

・6.4.4.8-4.2.4.16 and later
・6.5.4.15 and later
・8.3.0.11 and later
・8.4.0.6 and later
・8.5.0.5 and later
・8.6.0.2 and later

8. アップグレード方法
各種ガイドをご参照ください。なお、Central 管理の場合は、Central の管理画面もしくは

IAP の CLI よりアップグレードが可能です。IAP の GUI からアップグレードすることができませんが、IAP が Central と切断した場合は local management モードに切り替わり、IAP の GUI >> Maintenance >> Firmware からも、アップグレードすることが可能です。

※本アナウンスは 2020 年 1 月 31 日時点でのリリースをベースとしています。詳細および正確な記述は原文および最新のリリースを優先するものとします。

以上

Aruba Support Advisory ARUBA-SA-20191219-PLVL08

Aruba Instant Certificate Expiry Issue

Confidentiality Level: Aruba Customers & Partners only | Rev-3 (January 31, 2020)

OVERVIEW

There is a software defect that may impact Aruba Instant Access Points (IAP) and its accessibility through Aruba Central, Activate, and AirWave. This bug is tied to an SSL certificate in the Trust Anchor (TA) file of Instant OS, and may result in the loss of connectivity to management platforms unless the recommended action is taken prior to February 07, 2020. This is not a security vulnerability, but a software defect that may cause loss of connectivity to management plane.

DESCRIPTION OF THE ISSUE

One of the Verisign certificates within the TA certificate bundle will expire on February 07, 2020. Although an updated version of this certificate is included in Instant software, the defect in the SSL library will ignore all valid certificates if a single expired certificate is encountered. The existing IAP deployments will fail to set up an SSL connection to Central, Activate, and AirWave due to this defect.

Please Note: IAPs are designed to operate without these services, and they will remain functional and forward traffic after February 07, 2020. Also, existing Central and AirWave sessions will remain active after February 07, 2020. However, if there is loss of connectivity or a reset of any of the Central or AirWave service, the connectivity between IAP and the management platforms will not remain active and IAP deployments will revert to local management mode, built into the IAP. To re-connect to the management services, a manual upgrade of every IAP cluster and every IAP in standalone mode is required. The upgrade will load a patch that will re-establish connectivity to Central, Activate, or AirWave. Due to the above conditions, all customers with affected IAP deployments are strongly advised to upgrade to a software version with the fix prior to February 07, 2020.

Revision-3 of this advisory as of Jan 31, 2020 includes an Appendix with Aruba Instant software image URLs for use when manually upgrading a multi-class IAP cluster. It also includes details on forced upgrade of APs in factory default state from Activate.

Revision-2 as of Jan 06, 2020, included an update and remediation for - a different defect that affects Instant 8.6.0.0 and 8.6.0.1 deployments managed by AirWave with certificate-based authentication.

Please read the entire advisory for relevant details.

AFFECTED PRODUCTS

IAPs that require connectivity to Central, Activate, and/or AirWave may be affected.

- For IAPs managed by Central with connectivity to Activate, following software versions and IAP platforms are affected.

Affected Software Version (Currently Supported Only)	Affected IAP Platforms
All software versions prior to the following patches in each of the respective release streams: ▪ 6.4.4.8-4.2.4.16 ▪ 6.5.4.15 ▪ 8.3.0.11 ▪ 8.4.0.6 ▪ 8.5.0.5	All IAP platforms (IAP-1XX, RAP-XXX, IAP-2XX, IAP-3XX and IAP-5XX series products)
Instant 8.6.0.0	RAP-155, IAP-214, IAP-215, IAP-224, IAP-225, IAP-228, IAP-274, IAP-275, and IAP-277

- For IAPs managed by AirWave with certificate-only authentication, following software versions and IAP platforms are affected. It is estimated that less than 10% of IAPs deployed use this option.

Affected Software Version (Currently Supported Only)	Affected IAP Platforms
All software versions prior to the following patches in each of the respective release trains: ▪ 6.4.4.8-4.2.4.16 ▪ 6.5.4.15 ▪ 8.3.0.11 ▪ 8.4.0.6 ▪ 8.5.0.5 ▪ 8.6.0.1	All IAP platforms (IAP-1XX, RAP-XXX, IAP-2XX, IAP-3XX and IAP-5XX series products)
Instant 8.6.0.1	All AP-3XX, and AP-5XX, AP203H/203R/203RP, and IAP-207

For details on the impact to customer deployments using different management options, refer to the section titled **DETAILED CUSTOMER IMPACT DUE TO DEFECT** below.

Note: An Instant deployment running a C-build that meets any one of the above listed conditions is also impacted.

PRODUCTS NOT AFFECTED

Software Version	IAP Platforms
AP platforms running the following software versions: ▪ 6.4.4.8-4.2.4.16 or later ▪ 6.5.4.15 or later ▪ 8.3.0.11 or later ▪ 8.4.0.6 or later ▪ 8.5.0.5 or later ▪ 8.6.0.2 or later	All IAP platforms (IAP-1XX, RAP-XXX, IAP-2XX, IAP-3XX and IAP-5XX series products)
AP platforms running Instant 8.6.0.1	RAP-155, IAP-214, IAP-215, IAP-224, IAP-225, IAP-228, IAP-274, IAP-275, and IAP-277
Controller-based access points (CAP) and Remote access points (RAP)	

CUSTOMER DEPLOYMENTS NOT AFFECTED

This issue does NOT affect the following Instant deployment scenarios with any IAP platforms.

- AirWave managed deployments using PSK-based device authentication
- Instant customers not using Central, AirWave, or Activate, but locally managing Instant clusters
- Customers with deployment of FIPS certified version of IAP
- Deployment of un-provisioned APs in factory-default state
    - If un-provisioned APs in factory-default state (including new APs and provisioned APs that are reset to factory default state) are deployed in an environment that offers connection to the internet for the APs to reach Activate, then Activate will force an upgrade to a software version with a fix for the issue. The upgraded APs will then come back online, set up a secure connection with Activate, and proceed to the next step that includes redirection to Aruba Central or AirWave successfully. Please ensure that standard ports (e.g. NTP, HTTP, HTTPS, ICMP) are allowed through the firewall for Zero Touch Provisioning to work.
    - Between February 3, 2020 and February 7, 2020
        - Factory default APs will still be able to set up a secure connection to Activate prior to February 7, 2020. In this case, Activate will force an upgrade of the APs to a patch (with fix) belonging to the same release stream as the existing software on the AP.
    - After February 7, 2020
        - In this case, an AP in factory default state will only be able to set up an unsecure connection with Activate if it is running an impacted software version. Activate will force upgrade the AP in factory default state to Instant

8.6.0.2 if the AP platform is supported in 8.6.x software stream. For AP platforms that are not supported in 8.6.x software stream but supported in a prior software stream, Activate will force upgrade that AP to the highest software version supported by the AP and has the fix.

- RAP-3, IAP-104, IAP-105, IAP-134, IAP135, and IAP-175 will be upgraded to Instant OS 6.4.4.8-4.2.4.16.
- IAP-204, IAP-205, IAP-205H, IAP-114, IAP-115, RAP-108, RAP-109, and IAP-103 will be upgraded to Instant OS 6.5.4.15.
- All other supported AP platforms will be upgraded to Instant 8.6.0.2.

– Please note that the default management password for an AP in factory default state has been changed to the serial number of the AP starting with Instant 8.5.0.0 software.

– It is important that Firmware Compliance setting on Central or Airwave is updated to a software version with the fix. This will enable Central or Airwave to upgrade or downgrade the AP to the appropriate software version for the deployment.

- If un-provisioned APs in factory-default state are deployed in an environment that offers no connection to Internet for the APs to reach Activate, then Activate will not be able to perform an upgrade of the APs automatically. In such cases, the customer must manually upgrade the APs to a software version with the fix, by either using Airwave with PSK based authentication or using local management option within the master AP of the Instant cluster.

- New controller-based AP deployments (including Remote APs)
  - If Internet connection is available to the APs in a new controller-based deployment, the APs will still reach out to Activate and Activate will force an upgrade of the APs to a software version with the fix. After the upgrade, the APs will connect to the controller.
  - If Internet connection is not available, the APs will still be able to connect to the controller.

WHAT HAPPENS IF …

If the affected customer deployments are NOT upgraded by Feb 07, 2020, then,

- IAPs will continue to provide client connectivity and forward traffic as designed. There is no impact to WLAN operation of the Instant cluster.
- Existing connection of IAPs with Central and AirWave will continue to remain as is after February 07, 2020. However, if that connection were to reset due to either a loss of Internet connectivity, a reboot of AirWave, or a reset of Central, the impacted versions of IAP will not be able to reestablish a new SSL connection back to the management platform. This issue only affects connectivity between IAP and management platforms.

RESOLUTION

The certificate expiry error bug is fixed in following software patches of all the supported release streams.

- 6.4.4.8-4.2.4.16 and later
- 6.5.4.15 and later
- 8.3.0.11 and later
- 8.4.0.6 and later
- 8.5.0.5 and later
- 8.6.0.2 and later

Please note the following:

- Instant OS 6.5.x.x-4.3.x.x and 6.5.3.x release versions are at end-of-support. Customers running either of these two software versions are advised to upgrade to Instant OS 6.5.4.15.
- Instant OS 6.4.4.8-4.2.x.x is the last supported release version for RAP-3, RAP-108, RAP-109, IAP-103, IAP-104, IAP-105, IAP-134, IAP135, and IAP-175. Customer deployments with these AP platforms are advised to upgrade to Instant OS 6.4.4.8-4.2.4.16.
- Instant OS 6.5.4.x is the last supported version for IAP-204, IAP-205, IAP-205H, IAP-114, and IAP-115. Customer deployments with these AP platforms are advised to upgrade to Instant OS 6.5.4.15.
- Instant 8.6.x.x is the last supported version for RAP-155, IAP-214, IAP-215, IAP-224, IAP-225, IAP-228, IAP-274, IAP-275, IAP-277. Customer deployments with these AP platforms are advised to upgrade to Instant 8.5.0.6 or Instant 8.6.0.2.
- Customer deployments running c-builds need to upgrade to one of the software patches with the bug fix, as applicable. You may reach out to your Aruba Account team or Aruba Global Support, to review your upgrade options or if you have any questions.
- Please ensure that Firmware Compliance on Central or Airwave is set to a software version with the fix.

Software upgrade test of an Aruba Central-managed IAP Cluster

- In Aruba's testing, Instant OS upgrade of a (mixed / two-class) 128 IAP cluster, managed through Aruba Central over a 1Mbps (worst-case) internet link, took less than 15 minutes to upgrade all the IAPs.
- With 15 minutes for pre-upgrade inspections and post-upgrade validation, a 128 Instant AP cluster upgrade should be completed in under 30 minutes, on an average.

DETAILED CUSTOMER IMPACT DUE TO DEFECT

Listed below are the management service options that will be impacted by this issue, if the software is not upgraded to the recommended version, before February 07, 2020.

Activate connection

- All IAPs with an Internet connection connect to Activate to get zero-touch provisioning (ZTP) rules. Also, IAPs periodically connect with Activate to synchronize on provisioning rules and software versions available. Without running one of the recommended fixed software versions, IAP will lose connectivity to Activate. Clients continue to be served and traffic within clusters is maintained. Periodic synchronization to Activate will not be available until the cluster is upgraded to a software version with the fix.

Central-managed IAPs

- For Central-managed IAPs, connectivity to Central is lost on connection reset. Clients continue to be served and traffic within clusters is maintained. However, the IAPs become unreachable from Central and they fall back to local management built into the IAPs. Restoring connectivity to Central requires a manual upgrade of the cluster to a software version with the fix.
- An existing connection between IAP and Central may be reset due to several reasons including WAN or Internet connection issues, reboot of the IAP, and Central upgrades that include Context Engine changes.
- If Central connection is reset due to any reason, then Central will lose access to the IAPs. This will impact all Central customers who do not upgrade their affected IAPs to a software version with the fix before February 07, 2020.
- In an IAP-VPN deployment managed by Aruba Central
    - If the VPN headend controller is running an ArubaOS version prior to 8.4.0.0,
        - An Access Point upon factory reset that is upgraded to Instant 8.6.0.2 by Activate, may not be able to setup user data tunnels over the VPN tunnel established with the VPN headend controller (running ArubaOS version prior to 8.4.0.0). This is due to a security enhancement in Instant 8.4.0.0 and later versions which requires the VPN headend controller to be running ArubaOS 8.4.0.0 or higher version if the AP is running an Instant version higher than 8.4.0.0.
    - Customers are advised to set up Firmware Compliance rule in Central so that the AP is downgraded to the appropriate pre-8.4 Instant software version (with the fix), enabling the AP to set up VPN tunnel with the VPN headend controller.

AirWave-managed IAPs

- The impact on AirWave managed IAP deployments upon reset of existing connection depends on the selected authentication method (certificate-only or PSK-based).
    - For customers using certificate-only authentication option between AirWave and IAP, there will be a loss of connection to Airwave when the existing connection is reset.
    - For customers using PSK or PSK + certificate based authentication option between AirWave and IAP, there is no impact.

- An existing connection between IAP and AirWave may reset due to several reasons including LAN or WAN connection issues between IAP and Airwave, reboot of the IAP, reboot of AirWave, and upgrade of AirWave software
- There is a different defect present in Instant 8.6.0.0 and 8.6.0.1 software versions that impacts connectivity of the following AP platforms with AirWave when using certificate-based authentication: all AP-3XX, and AP-5XX, AP203H/203R/203RP, and IAP-207. This issue is fixed in Instant 8.6.0.2.
- In an IAP-VPN deployment managed by AirWave
    - If the VPN head-end controller is running an ArubaOS version prior to 8.4.0.0,
        - An Access Point upon factory reset that is upgraded to Instant 8.6.0.2 by Activate, may not be able to setup user data tunnels over the VPN established with the VPN head-end controller (running ArubaOS version prior to 8.4.0.0). This is due to a security enhancement in Instant 8.4.0.0 and later versions which requires the VPN head-end controller to be running ArubaOS 8.4.0.0 or higher version if the AP is running an Instant version higher than 8.4.0.0.
    - Customers are advised to enable “Enforce Group Firmware Version” and “Allow Downgrade of Devices” under the Firmware upgrade options along with selecting the appropriate pre-8.4 Instant version (with the fix) under “Desired Version” in AirWave. This should allow the AP to be downgraded to the selected pre-8.4 Instant version (with the fix), enabling the AP to set up VPN tunnel with the VPN head-end controller.

      Note: Even if the AirWave is only accessible through the VPN tunnel, the AP running Instant 8.6.0.2 would still be able to set up control traffic over the VPN tunnel with the controller running pre-8.4 software to access AirWave for downgrading itself.

Locally managed IAPs

- For IAPs managed using management options that are built into the AP, the impact is limited. The IAPs will continue to serve clients, pass traffic, and be managed locally. However, connectivity to Activate will be lost. This will imply that IAPs will not be able to synchronize on any new provisioning rules in Activate and will not be able to get new image information automatically from Activate for upgrade, using local WebUI.
- Upgrade of a locally managed Instant cluster with multiple classes of AP platforms usually depends on Activate to serve image files for AP classes other than the master AP’s class. As APs will no longer be able to connect with Activate, upgrade of clusters with multiple classes of AP platforms will be impacted after February 07, 2020. You may use the following steps to upgrade an impacted Instant cluster with multiple classes of APs.
    1. Log into the local management user interface (UI) built in to the master AP of the cluster.
    2. Navigate to “Firmware” section under “Maintenance” in the left navigation panel.
    3. Under “Manual” firmware upgrade, choose “Image URL” radio button.
    4. Enter the URL for the deployed AP classes and desired software version from the list of image URLs in the Appendix-A.

5. Upgrade the cluster.
   Refer to the Release Notes for detailed upgrade instructions.

- If an AP belonging to a new image class needs to be added to an existing Instant cluster, then the cluster must first be upgraded to a software version with the fix following the steps above prior to adding the AP.

Additional Use Cases

- There is no impact of this issue in controller-based AP (CAP) deployments. APs terminating on Aruba controllers are defined as CAPs and run ArubaOS software. This defect applies only to Instant software (Instant OS) and does not impact ArubaOS.
- The current (Instant OS 8.5.0.3) and previous (Instant OS 6.5.4.3) manufacturing images used by the factory to build new APs have this bug. New deployment of APs in factory default state would potentially exhibit this issue. However, check the fourth bullet in Customer Deployments Not Affected section (above) to understand how Activate will be able to force an upgrade of APs in factory default state to a software image with the fix, so the deployment can proceed without any problem.
- The factory is in the process of updating the AP manufacturing image to Instant OS 8.6.0.2
- Customers with Instant deployments (without an official software image) running an existing c-build will be impacted.
- If IAPs managed by Central or Airwave with certificate-only based authentication are not upgraded to a software version with the fix prior to February 07, 2020, the IAPs will fall back to local management when connectivity to management platform is lost. Refer to Locally managed IAPs section for steps on how to upgrade the Instant cluster to recover the connection to the management platform.

ARUBA TECHNICAL ASSISTANCE CENTER

Should you require any assistance or clarification regarding this advisory, you can open a support case through the Aruba Support Portal at https://asp.arubanetworks.com. To call, please use the numbers found @ https://www.arubanetworks.com/support-services/contact-support/

This Support Advisory will be posted on the Aruba Support Site under the Announcements section and may be revised as applicable. Ensure that you check again for further updates.

Aruba is committed to communicating code revision, feature, and function recommendations to ensure optimal network operation and high customer satisfaction. The Aruba Global Support team can facilitate further product related discussions with the Product Management team for customers who desire to do so.

Thank you,
Aruba Global Support Services

APPENDIX–A

Aruba Instant software image URLs for use when manually upgrading a multi-class IAP cluster.

Instant 6.4.4.8-4.2.4.16 Build 73658

Access Point Models	Image URL
IAP-103, IAP-114/115, RAP-108/109	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Pegasus_6.4.4.8-4.2.4.16_73658
IAP-104, IAP-105, IAP-175AC, IAP-175P, IAP-92/93, RAP-3WN/3WNP	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Orion_6.4.4.8-4.2.4.16_73658
IAP-134/135	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Cassiopeia_6.4.4.8-4.2.4.16_73658
IAP-204/205, IAP-205H	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Taurus_6.4.4.8-4.2.4.16_73658
IAP-214/215, IAP-224/225, IAP-228, IAP-274/275, IAP-277	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Centaurus_6.4.4.8-4.2.4.16_73658
IAP-324/325	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Hercules_6.4.4.8-4.2.4.16_73658
RAP-155/155P	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Aries_6.4.4.8-4.2.4.16_73658

Instant 6.5.4.15 Build 73677

Access Point Models	Image URL
AP-203H, AP-203R, AP-203RP, IAP-207	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Vela_6.5.4.15_73677
AP-303H, AP-365/367, IAP-304/305	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Ursa_6.5.4.15_73677
IAP-103, IAP-114/115, RAP-108/109	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Pegasus_6.5.4.15_73677
IAP-204/205, IAP-205H	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Taurus_6.5.4.15_73677
IAP-214/215, IAP-224/225, IAP-228, IAP-274/275, IAP-277	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Centaurus_6.5.4.15_73677
IAP-314/315, IAP-324/325	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Hercules_6.5.4.15_73677
IAP-334/335	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Lupus_6.5.4.15_73677
RAP-155/155P	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Aries_6.5.4.15_73677

Instant 8.3.0.11 Build 73691

Access Point Models	Image URL
AP-203H, AP-203R, AP-203RP, IAP-207	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Vela_8.3.0.11_73691
AP-303, AP-303H, AP-365/367, IAP-304/305	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Ursa_8.3.0.11_73691
AP-318, AP-374/375/377, IAP-314/315, IAP-324/325	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Hercules_8.3.0.11_73691
AP-344/345	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Draco_8.3.0.11_73691
IAP-214/215, IAP-224/225, IAP-228, IAP-274/275, IAP-277	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Centaurus_8.3.0.11_73691
IAP-334/335	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Lupus_8.3.0.11_73691
RAP-155/155P	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Aries_8.3.0.11_73691

Instant 8.4.0.6 Build 73542

Access Point Models	Image URL
AP-203H, AP-203R, AP-203RP, IAP-207	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Vela_8.4.0.6_73542
AP-303, AP-303H, AP-303P, AP-365/367, IAP-304/305	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Ursa_8.4.0.6_73542
AP-318, AP-374/375/377, AP-387, IAP-314/315, IAP-324/325	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Hercules_8.4.0.6_73542
AP-344/345, AP-514/515	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Draco_8.4.0.6_73542
IAP-214/215, IAP-224/225, IAP-228, IAP-274/275, IAP-277	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Centaurus_8.4.0.6_73542
IAP-334/335	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Lupus_8.4.0.6_73542
RAP-155/155P	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Aries_8.4.0.6_73542

Instant 8.5.0.5 Build 73491

Access Point Models	Image URL
AP-203H, AP-203R, AP-203RP, IAP-207	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Vela_8.5.0.5_73491
AP-303, AP-303H, AP-303P, AP-365/367, IAP-304/305	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Ursa_8.5.0.5_73491
AP-318, AP-374/375/377, AP-387, IAP-314/315, IAP-324/325	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Hercules_8.5.0.5_73491
AP-344/345, AP-514/515	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Draco_8.5.0.5_73491
AP-534/535, AP-555	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Scorpio_8.5.0.5_73491
IAP-214/215, IAP-224/225, IAP-228, IAP-274/275, IAP-277	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Centaurus_8.5.0.5_73491
IAP-334/335	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Lupus_8.5.0.5_73491
RAP-155/155P	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Aries_8.5.0.5_73491

Instant 8.6.0.2 Build 73853

Access Point Models	Image URL
AP-203H, AP-203R, AP-203RP, IAP-207	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Vela_8.6.0.2_73853
AP-303, AP-303H, AP-303P, AP-365/367, IAP-304/305	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Ursa_8.6.0.2_73853
AP-318, AP-374/375/377, AP-387, IAP-314/315, IAP-324/325	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Hercules_8.6.0.2_73853
AP-344/345, AP-514/515	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Draco_8.6.0.2_73853
AP-504/505	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Gemini_8.6.0.2_73853
AP-534/535, AP-555	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Scorpio_8.6.0.2_73853
IAP-214/215, IAP-224/225, IAP-228, IAP-274/275, IAP-277	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Centaurus_8.6.0.2_73853
IAP-334/335	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Lupus_8.6.0.2_73853
RAP-155/155P	http://d2vxf1j0rhr3p0.cloudfront.net/fwfiles/ArubaInstant_Aries_8.6.0.2_73853

Appendix – End.

This is the last page and intentionally left blank.

aruba
a Hewlett Packard Enterprise company
www.arubanetworks.com

3333 SCOTT BLVD | SANTA CLARA, CA 95054
T: 1.408.227.4500 | FAX: 1.408.752.0626