# IQ Engine 10.0r9a Release Notes

**Release date**: August 14, 2020

**Hardware platforms supported**: Atom AP30, AP122, AP122X, AP130, AP150W, AP230, AP245X, AP250, AP510C, AP510CX, AP550, AP630, AP650, AP650X, and AP1130

**Management platforms supported**: ExtremeCloud IQ 20.8.1.1 and later

## New Features and Enhancements

This release introduces the following new features and enhancements:

**SD-WAN Tunnel Enhancements**: Routers and VGVA devices running IQ Engine 10.0r9a can now use one of three tunnel addressing settings:

- **Management Subnet (new default)**: The device uses and address from the management subnet, which ensures that each device receives a unique WAN address.
- **WAN Address (former default)**: The devices uses the WAN address supplied by the WAN device, such as a cable or DSL modem.
- **Custom Address**: The administrator can define a pool of IP address for devices to use for the WAN address.

**VPN Gateway Enhancements**: Routers and VGVA devices running IQ Engine 10.0r9a and acting as a VPN gateway can now use ports other that the well known ports 500 and 4500 to terminate tunnels, allowing multiple VPN gateways to function behind a firewall.

## Known and Addressed Issues

The following tables list known and addressed issues in IQ Engine 10.0.

### Known Issues in IQ Engine 10.0r9a

There are no known issues in this release.

### Addressed Issues in IQ Engine 10.0r9a

| | |
|---|---|
| CFD-4802 | Administrators could not retrieve tech data for AP1130 access points running HOS 10.0r8. |
| CFD-4710 | Client devices sometimes disconnected because the VLAN changed during user profile reassignment. |
| CFD-4671 | Remote sites lost VPN connection to VGVA, requiring administrators to restart the IPsec session. |
| CFD-4641 | AP650 access points sometimes initiated a system core dump, and then rebooted or became unresponsive. |
| CFD-4005 | When the XR600 router was used as a Layer 2 VPN server, TCP sessions within the tunnel sometimes closed unexpectedly. |

## Addressed Issues in IQ Engine 10.0r9

| | |
|---|---|
| CVE-2019-15126<br>HOS-15944 | Broadcom access points and wireless clients were vulnerable to traffic decryption during a very short time window during the dissociation process. |

## Addressed Issues in IQ Engine 10.0r8

| | |
|---|---|
| CFD-4471 | When an admin configured an SSID to drop all non-management traffic destined for the ap, users were unable to authenticate to the network using PPSK self-registration. |
| CFD-4470 | Wildcard characters did not function properly in walled garden captive web portals when NAT was enable on a user profile. |
| CFD-4453 | Disconnecting a client from a WPA3 SSID caused all other clients to disconnect. |
| CFD-4422 | In the output of different commands, IQ Engine reported different values for the same transmit power parameter. |
| CFD-4398 | BLE iBeacons were inconsistently reported in the AP650 iBeacon monitor list output. |
| CFD-4309 | AP650 access points rebooted soon after Cisco phones connected. |
| CFD-4300 | When some APs were configured for scheduled reboot, Wi-Fi interfaces were shut down, preventing clients from reconnecting after the reboot. |
| CFD-4245 | AP630 and AP650 access points were dropping a high number of packets. |
| CFD-4242 | Some internal running processes of AP630 access points became unresponsive. |
| CFD-4190 | AP1130 access point were rebooting spontaneously. |
| CFD-4126 | When NTLMv1 was disabled in Active Directory, some access points were unable to act as RADIUS servers using PEAP with MS-CHAP-v2 authentication. |
| CFD-4086 | Network users were sometime assigned to incorrect VLANs and RADIUS attributes were used for classification. |
| CFD-4085 | IQ Engine was reporting high interference to ExtremeCloud IQ. |