BYOD System Release Notes

Revised: August 7, 2013

This appendix contains information regarding known caveats within Cisco product software revisions which could impact the Cisco BYOD solution documented in this design guide. The caveats are organized around product and software releases within this appendix for ease of reference.

IOS XE 3.2.2 SE Software Release—Catalyst 3850 Series Switches and Cisco 5760 Wireless Controllers

- Wireless clients associated with Access Points connected to Catalyst 3850 Series switches may unexpectedly go into an IDLE state. This rare occurrence can happen after a client has been on-boarded and is connected to the employee SSID with full, partial, or Internet only access, during on-boarding (using a single or dual-SSID design), while a client is blacklisted, or during MDM or ISE remediation.

  The network administrator can view a wireless client in this state via the **show wireless client summary** CLI command. An example is shown below in which the two highlighted wireless clients are in an IDLE state.

```
uasl-3850-2# show wireless client summary
Number of Local Clients : 5

MAC Address    AP Name                          WLAN State              Protocol
-------------------------------------------------------------------------------
38aa.3c44.a224 test_ap                          1    UP                 11n(2.4)
789e.d0cd.f8ac test_ap                          1    Idle               11n(2.4)
8832.9b0d.e554 test_ap                          1    WEBAUTH_PEND       11n(2.4)
c860.001a.a77e test_ap                          3    WEBAUTH_PEND       11n(2.4)
f0b4.7953.26b8 test_ap                          1    Idle               11n(2.4)
```

  Once in this state, the wireless client cannot disconnect and re-connect to the wireless network without assistance from a network administrator. The network administrator can clear an IDLE client by issuing the **wireless client mac-address** <*mac-address of the wireless client*> **deauthenticate forced** CLI command. Note that this command does not appear within the existing Cisco IOS 3.2.xSE command reference. For example, in order to clear the wireless client with mac address f0b4.7953.26b8 shown in the example above, the network administrator would issue the following command:

```
uasl-3850-2# wireless client mac-address f0b4.7953.26b8 deauthenticate forced
```

- Blacklisted wireless clients associated with Access Points connected to Catalyst 3850 Series switches may occasionally require manual intervention in order to regain access to network resources when attempting to reinstate the client. This rare occurrence happens when the Catalyst 3850 Series switch is unable to process the CoA request to remove the ACL_BLACKHOLE and ACL_BLACKHOLE_Redirect ACLs applied to a Blacklisted device as part of the Cisco BYOD solution. The end user can toggle WiFi access on the mobile device in order to regain network access. Alternatively, the network administrator can de-authenticate the wireless client via the **wireless client mac-address** <*mac-address of the wireless client*> **deauthenticate** CLI command and then allow the device to normally reconnect to the network. For example, in order to clear a wireless client with mac address b4f0.abce.fa66, the network administrator would issue the following command:

  ```
  uasl-3850-2# wireless client mac-address f0b4.7953.26b8 deauthenticate
  ```

  This caveat is documented as bug ID CSCuh66924 within the Cisco Bug Toolkit.

Additional Observations

The Release Notes for the Catalyst 3850 Series Switch, Cisco IOS XE Release 3.2.xSE contains additional caveats specific to the Catalyst 3850 Series Switch and can be found at: http://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/release_notes/OL28114.html#wp224029