AP Device Certificate Refresh
FAQ

Beginning in November 2016, the existing default SSL device certificates on Ruckus APs will expire. Ruckus has been rolling out replacement certificates on APs since January 2016.

APs manufactured since January 2016 are assured to have the new certificate. However, APs shipped with factory images prior to release 104 (even though they may include the new certificate) may still require customer action because pre-104 AP firmware does not point to the new certificate. Refer to the following table for a breakdown of which APs are affected.

Table 1. Affected APs

AP Mfg. Date	AP Firmware	Required Customer Action
Before 2016	Any	Perform certificate refresh procedure.
Jan. 2016 onward	< 104.x	Temporarily disable cert check after Nov. 27, 2016, to allow AP's to join the controller. Re-enable cert check after the AP's have joined. No further action required.
	104.x and later	No action required.

A certificate refresh feature is included in the latest ZoneDirector and SmartZone controller firmware releases (9.13 and 3.0.5 and above, respectively).

What is the reason for this refresh?

Device certificates installed on Ruckus APs at the time of manufacture allow secure communication between APs and a controller.

Without a valid certificate, this communication cannot occur causing significant impact to service, up to and including clients being unable to connect and use the Wi-Fi network.

What is the Impact?

Table 2. Impact Analysis

Controller	Impact
Standalone (unmanaged) APs	On most browsers there will be a warning stating that the site is not secure. Users can ignore the warning and will be able to access the AP. Some browsers, based on local policy and configuration, may enforce this and not allow the connection to go through. To avoid this issue, enable HTTP (via CLI) and use HTTP rather than HTTPS to access the AP web UI.
ZoneDirector	No impact, unless you plan to migrate APs from ZD to SZ or Ruckus Cloud management.
FlexMaster	None
Unleashed	None
SmartZone (incl. SZ, vSZ, SCG)	Device certificate authorization fails on joining SmartZone. AP remains offline unless certificate check is explicitly disabled on controller through CLI configuration. Note that this results in controller not verifying the AP and allowing it to join on a trusted basis. APs not already configured on the controller will be limited to the staging zone.

Is this specific to SmartZone managed APs?

Although all Ruckus APs are impacted by this, SmartZone (SCG) managed APs will face issues (if certificates are not updated) since SmartZone-managed APs use HTTPS for secure connectivity between the AP and controller, and SmartZone enforces device certificate validation before allowing APs to join the controller.

ZoneDirector-controlled APs are unaffected because ZoneDirector does not enforce the certificate verification. (Note however, that Ruckus still recommends upgrading the certificates on ZoneDirector-controlled APs as well.)

What is the solution for SmartZone managed APs?

A detailed and easy to follow procedure is being provided to all customers through the AP certificate refresh feature included in all SZ software versions 3.1.2 and above.

The AP certificate refresh feature helps identify and group affected APs and produces the required 'request file'. This request file is then uploaded to the Ruckus Support site which in return provides a 'response file' for the customer to then apply to the controller. The controller then pushes the new certificates to all affected APs, affected APs reboot and service is reestablished with the new certificates.

If any affected APs are detected at a later date the yellow warning message on the Controller dashboard will be displayed once again and then disappears when all APs have had their certificates successfully refreshed.

What is the Certificate Refresh Process?

Follow these steps to refresh AP certificates:

1. The AP certificate refresh feature is provided as a part of SmartZone releases 3.0.5, 3.1.2, 3.2.1, 3.4 and later, and as part of ZoneDirector release 9.13 and later.
2. After upgrading to the new release, the updated controller UI displays a warning message about any required certificate refresh on the controller's Dashboard. All controllers running the updated software will perform an auto check on all APs' certificates, and generate an alarm for any AP whose certificate still needs to be replaced.
3. Access the AP Certificate Replacement feature in the controller's web UI.
   - **SmartZone**: Go to *Administration* > *AP Certificate Replacement*.
   - **ZoneDirector**: Go to *Configure* > *Certificate* > *Advanced Options* > *Import Ruckus PKI Certificate Package*.

Published October 2016, Part Number 800-71343-001 Rev C

4 Follow the instructions on the controller UI to generate a certificate request file, which you can then upload to the Ruckus Support website to request a package of new certificates.

5 Go to https://support.ruckuswireless.com/ and select **AP Certificate Replacement** in the **Tools** section. When prompted, select and upload the cert request file, provide an email address, and click **Upload**. You will then receive an automated email notification that the request has been received and is being processed.

6 The Ruckus IT system receives the request file, validates it, and sends an email containing the response file.

7 Download the response file, and then import it into the controller using the controller's AP Certificate Replacement feature, which triggers the certificate update process. All APs that have the new certificate refreshed WILL RESTART AT THIS TIME.

8 Using the AP Certificate Replacement feature, you can monitor the progress of the affected APs as they are refreshed, rebooted and come back online. Any AP that fails the process will revert to the existing certificate and come back online to allow troubleshooting. A troubleshooting guide will be made available by engineering for this purpose.

9 You can repeat the process for any remaining APs requiring certificate refresh, or for any APs added to the controller at a later date.

What if my customer chooses not to upgrade to 3.0.5, 3.1.2, 3.2.1 or later release?

If a customer chooses NOT to upgrade to SmartZone release 3.0.5, 3.1.2, 3.2.1, 3.4 or later, AP certificate checks will fail in November 2016 and the APs will NOT be able to connect to the controller. Therefore, all Ruckus APs running SmartZone software should be updated to release 3.1.2 or later and then follow the **Certificate Refresh Process** in a planned and systematic manner before the November 2016 deadline. Please ensure that this process is followed by your customers without fail.

NOTE: Customers also have the additional option of temporarily disabling the certificate check on the controller through the SZ CLI. If you do this, please be sure to re-enable the certificate check after AP certificates have been updated.

What is the procedure for standalone APs?

For standalone APs, you can check whether the AP has an updated certificate and update it if needed using the *Administration > Management > Certificate Verification* section.

If needed, click the "*Request to reissue a new certificate*" link, save the file to your local computer, and email the file as an attachment to certs@ruckuswireless.com in an empty email.

Ruckus will generate an encrypted package containing the replacement certificate/key and return it by email. Import the replacement certificate package using the *Maintenance > Upgrade* page. Select **Local** in *Upgrade Method*, and in *Target Selection*, select **Device Certificate**. Click **Upload Certificate** to upload the certificate package to the AP, and reboot.

For More Information

For more information about AP Device Certificate Refresh, refer to the *SmartZone™ 100/Virtual SmartZone™ Essentials Administrator Guide* and *SmartCell Gateway™200/Virtual SmartZone™ High-Scale Administrator Guide* for Release 3.1.2 and 3.2.1, or visit http://support.ruckuswireless.com.

Published October 2016, Part Number 800-71343-001 Rev C