Best Practices for Automatic Password Management for Loosely Connected Devices (Laptops, Tablets, etc)

All below settings are configured via Platform Management:

1. Set the delay between retries to something much higher than the default, retrying every 14 hours, with 15-20 retries, which will allow the process to factor in if someone is on vacation for a week and their laptop isn’t turned on. The number of retries should be kept to a minimum and interval times extended to reduce the strain on the CPM and the total number of cycles.
2. A guideline for the password rotation time period is something greater than 90 days. This allows for the length of time that a laptop may be offline before CyberArk can make a connection and attempt a password change. In larger environments a longer time period may be desirable.
3. You may also consider creating different policies for different time zone locations of target workstations. Setting the “from hour” and “to hour” to be something that would pertain to a typical workday schedule (when we most likely expect that the user will be working and have their workstation turned on).
4. You can also set up the times of the week to avoid weekends (since the end users may not work on weekends). Keep in mind that multiple policies may be beneficial to accommodate work schedules or geographic locations.