Cisco AppHQ Validation Information
May 11, 2011
Rev. 0.3

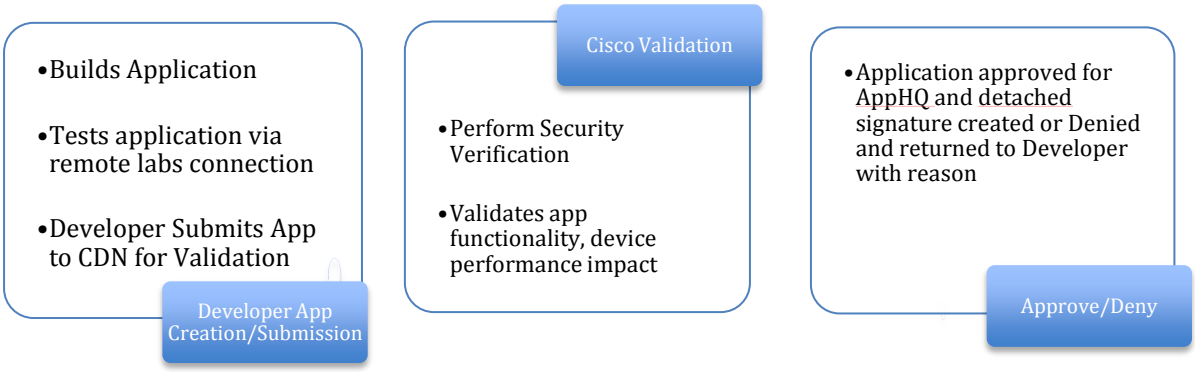
Cisco AppHQ is an enterprise focused application shop created for use with the new Cisco Cius android tablet.

The enterprise market is much more security and privacy conscious than the consumer market. Cisco has defined several validation and security checks that are critical to our customer needs and are included in this document.

Cisco believes these checks will help differentiate AppHQ as an enterprise focused trusted source of credible business applications.

All applications accepted into the shop must meet these criteria and pass all security tests.

Validation Process



Cisco Validation Focus

- Security (Enterprise level)
- Application impact on device health or operation
- Application quality

Rejection Reasons:

1) Not an Enterprise user application

Return Reasons (corrective action required):

1) Export Compliance information incorrect/not provided
2) Cisco Functional criteria not met.
3) Security issue or Cisco defined Critical Android Permission use in an APK
4) APK does not have a valid signature (ex: android debug)
5) APK signature does not match previous version
6) APK version number not sequentially incremented in a later submission.

Functional Validation Criteria:

- Install/Uninstall
- Application Run Time (Security agent)
- All buttons/links work
- App is what it says it is
- Display is correct (optimized for 7" display, orients)
- Resource Utilization: No excessive impact to device (cpu, memory, battery life)
- App releases device features when requested (camera, recorder etc) by Cisco priority app.

Security (sample list)

- Invalid Signature (Ex: Android Debug)
- Known threats and malware
- Known exploits or attempts to bypass the Android security framework
- Private API calls
- Executable binaries
- Root level privileges
- System level privilege
- Application contains profanity or pornography
- Application has malicious host or URLs (phishing or data mining)
- Permissions do not meet app type/category
- Critical Permission or unjustified High Permission in use

Critical Permissions List

Permission
android.permission.ACCESS_USB
android.permission.BACKUP
android.permission.ACCESS_CACHE_FILESYSTEM
android.permission.ACCESS_CHECKIN_PROPERTIES
android.permission.BIND_APPWIDGET
android.permission.MODIFY_PHONE_STATE
android.permission.PACKAGE_USAGE_STATS
android.permission.READ_CALENDAR
android.permission.READ_FRAME_BUFFER
android.permission.READ_LOGS
android.permission.DUMP
android.permission.WRITE_OWNER_DATA

Critical Security

Permission
android.permission.ACCESS_USB
android.permission.BACKUP
android.intent.category.MASTER_CLEAR.permission.C2D_MESSAGE
android.permission.ACCESS_SURFACE_FLINGER
android.permission.ACCOUNT_MANAGER
android.permission.ASEC_ACCESS
android.permission.ASEC_CREATE
android.permission.ASEC_DESTROY
android.permission.ASEC_MOUNT_UNMOUNT
android.permission.ASEC_RENAME
android.permission.BIND_WALLPAPER
android.permission.BRICK
android.permission.BROADCAST_PACKAGE_REMOVED
android.permission.BROADCAST_SMS
android.permission.BROADCAST_WAP_PUSH
android.permission.CALL_PRIVILEGED
android.permission.CHANGE_BACKGROUND_DATA_SETTING
android.permission.CHANGE_COMPONENT_ENABLED_STATE
android.permission.CLEAR_APP_USER_DATA
android.permission.CONTROL_LOCATION_UPDATES
android.permission.COPY_PROTECTED_DATA
android.permission.DELETE_CACHE_FILES
android.permission.DELETE_PACKAGES
android.permission.DEVICE_POWER
android.permission.DIAGNOSTIC
android.permission.FACTORY_TEST
android.permission.FORCE_BACK

android.permission.FORCE_STOP_PACKAGES
android.permission.GLOBAL_SEARCH
android.permission.GLOBAL_SEARCH_CONTROL
android.permission.HARDWARE_TEST
android.permission.INJECT_EVENTS
android.permission.INSTALL_LOCATION_PROVIDER
android.permission.INSTALL_PACKAGES
android.permission.INTERNAL_SYSTEM_WINDOW
android.permission.KILL_BACKGROUND_PROCESSES
android.permission.MANAGE_APP_TOKENS
android.permission.MASTER_CLEAR
android.permission.MOUNT_FORMAT_FILESYSTEMS
android.permission.MOUNT_UNMOUNT_FILESYSTEMS
android.permission.MOVE_PACKAGE
android.permission.PERFORM_CDMA_PROVISIONING
android.permission.READ_INPUT_STATE
android.permission.REBOOT
android.permission.RESTART_PACKAGES
android.permission.SET_ACTIVITY_WATCHER
android.permission.SET_ORIENTATION
android.permission.SET_PREFERRED_APPLICATIONS
android.permission.SET_TIME
android.permission.SET_WALLPAPER_COMPONENT
android.permission.SHUTDOWN
android.permission.STATUS_BAR
android.permission.STATUS_BAR_SERVICE

android.permission.STOP_APP_SWITCHES
android.permission.SYSTEM_ALERT_WINDOW
android.permission.UPDATE_DEVICE_STATS
android.permission.WRITE_APN_SETTINGS
android.permission.WRITE_GSERVICES
android.permission.WRITE_SECURE_SETTINGS
android.permission.WRITE_SMS

High Security Permissions

The following permission are considered High risk for the enterprise. Developers can inform Cisco of use of these permissions and provide the reason it is needed if Cisco requests more information. Only applications with a reasonable justification for use of permissions on this list will be accepted.

Example of a reasonable justification:
Note Taking App using: RECORD_AUDIO
Justification: Audio notes functionality

Example of an unreasonable justification:
Calculator using: RECORD_AUDIO
Justification: Debugging purposes or null.

The justification will be reviewed by Cisco to determine if the use supports the product type and functionality provided.

High Permissions

Permission
android.permission.NFC
android.permission.RECEIVE_MMS
android.permission.RECEIVE_SMS
com.google.android.c2dm.permission.RECEIVE
android.permission.ACCESS_FINE_LOCATION
android.permission.MANAGE_ACCOUNTS
android.permission.READ_CONTACTS
android.permission.READ_SMS
android.permission.RECORD_AUDIO
com.android.browser.permission.READ_HISTORY_BOOKMARKS

High Privacy:

Permission
android.permission.NFC
android.permission.SEND_SMS
android.permission.AUTHENTICATE_ACCOUNTS
android.permission.BIND_DEVICE_ADMIN
android.permission.BIND_INPUT_METHOD
android.permission.BIND_REMOTEVIEWS
android.permission.BLUETOOTH_ADMIN
android.permission.CALL_PHONE
android.permission.CHANGE_NETWORK_STATE
android.permission.CHANGE_WIFI_MULTICAST_STATE
android.permission.CHANGE_WIFI_STATE
android.permission.PROCESS_OUTGOING_CALLS
android.permission.SET_ALWAYS_FINISH
android.permission.SET_PROCESS_LIMIT
android.permission.SIGNAL_PERSISTENT_PROCESSES
android.permission.USE_CREDENTIALS
android.permission.WRITE_CALENDAR
android.permission.WRITE_CONTACTS
android.permission.WRITE_SETTINGS