Cisco App Center Development Principles and Guidelines

Introduction

Cisco App Center invites Cisco’s partners and developer community to build applications—or apps—that use Cisco® application-aware and programmable network infrastructure to help our customers attain their business goals. The infrastructure component includes industry-leading solutions such as Cisco Application Centric Infrastructure (Cisco ACI™), which delivers a transformational operating model for next-generation data center and cloud applications. You can find more details about Cisco ACI [here](http://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/aci-fabric-controller/at-a-glance-c45-729864.pdf).

Focus on Ecosystem Expansion

Our goal is to expand the Cisco ACI ecosystem by engaging with the software-defined networking (SDN) development community to create enhanced value for our customers. Cisco App Center is the realization of this vision. We want to help you understand App Center development guidelines so you can be assured that your app will proceed through our review process quickly. Additionally, to help create greater value for our customers, we are asking you to act in accordance with the principles and guidelines outlined in this document. Our guiding principle is simple: we want to provide a rewarding experience for our customers and offer you—our partners and developer community—opportunities to be successful.

Remember:

* Cisco cares deeply about its customers and partners. Therefore, through your apps we ask you to attempt to enhance the customer experience (and not diminish it).
* We will not accept apps that do not meet Cisco App Center development guidelines and violate the principles on which the Cisco ACI ecosystem is based.
* We will not accept any app that tries to cross the limits, cheat the network or system, or is built with secretive or malicious intent. [[I’M NOT SURE WHAT THESE ITEMS ALL MEAN. OK AS IS, OR DO YOU WANT TO ELABORATE?]]

Guidelines Overview

This document summarizes the guidelines and process for developing and submitting applications.

* App development guidelines
* Integrity
* Quality
* Safety and security
* Performance
* Hardware and software compatibility
* Monetization
* Authenticity
* Legal
* Content
* App review submission checklist
* App review procedure
* What to expect after you submit app for review

App Development Guidelines

**Integrity**

In this digital world, our customers and partners expect integrity from Cisco, and we expect the same from you. We understand that software applications might not be defect free. However, your goal must be to reduce the number of defects and transparently communicate any known limitations to our customers. Acting with honesty and integrity about the capabilities of your app and what it is intended to do is vital for long-term success for all the parties involved with your app. You should make clear to customers what they are downloading from the Cisco App Center. Therefore, make sure that the app logo, description, name, supporting screenshots, and notes in the App Center communicate what the customer can expect from your app.

**Quality**

We ask you to build a high-quality app that you can stand by. We recommend verifying it thoroughly in your physical deployment setting before submitting it to Cisco for formal review. Know that our customers might deploy your app in their production network settings, which might be running mission-critical services. Thereby, we ask you to do your part to make sure that the app is production quality in terms of performance, capability, conformance, serviceability, security, reliability, and scale. Verify that it does not crash and cause any catastrophic failures when in use. Use fault isolation and limitation techniques by following the best practices in software development and verification. Contain the core and peripheral effects of failure as much as possible. Do not try to exploit known defects or limitations of Cisco and other vendors’ products or inject faults or failures of any sort.

**Safety and Security**

Safety and security are paramount to Cisco and our customers and partners. When users download and install a Cisco App Center app in their network environments, we aim to provide the safe and secure experience. An app should offer a highly reliable business or technical solution for our customers. We ask you not to misuse, collect, transport, distribute, or upload any sort of data from a customer’s systems off a customer’s premises without explicit agreement from Cisco and the customer. Help ensure that your app does not compromise any security aspects of Cisco products and the customer’s other systems by making the products vulnerable to cyber attacks or similar security breaches.

**Performance**

You need to ensure that the application is 100 percent complete with respect to source code, verification, code comments, and mandatory notes when you submit it for review. It is your responsibility to ensure that the app is verified on a real device under test (DUT) and is not tested only in a virtual environment. For example, for a Cisco Application Policy Infrastructure Controller (APIC) app, you need to test the app for defects on real APIC hardware with the underlying physical network in place. We will disqualify any app that has obvious technical, performance, or usability problems. In addition, app installation should not require any reboot of existing ecosystem devices already running. Any upgrade or downgrade to a different version of your app must be transparent.

**Hardware and Software Compatibility**

If your app is verified, supported, or qualified for a specific software version and hardware product combination, you should provide a clear hardware and software compatibility matrix along with your app in the Cisco App Center notes. Not disclosing this information is considered misguiding customers and is against our principles.

**Monetization**

We are working with our partners and the developer community to help monetize apps. At present, the Cisco App Center accepts only apps that are offered for use for free. You may expect us to provide more details about monetization of apps when we start accepting paid apps through the App Center. When this opportunity is available, you will be required to abide by payment and other guidelines that relate to monetization of your apps.

**Authenticity**

We need you to be authentic and to come up with innovative ideas of your own and not simply develop apps that copy other offerings. You should be transparent in communicating the app features you provide. Make sure that your app includes the minimum valuable capabilities that any user would expect in your app. Moreover, an app should stand alone and not require the installation of any other app or connection to an external service or other external resource.

**Legal**

Every Cisco App Center app must comply with all requirements listed in the App Center development guide. Your license terms must comply with the requirements of the developer agreement. In addition, you must meet the following requirements:

* **Privacy**: Our customers expect that the privacy of their data, intellectual property, and information related to their infrastructure deployments will be maintained. Your apps must comply with the following requirements in connection with the handling of customer data:

* Personally identifiable information: Apps submitted to the App Center may not collect and share personally identifiable information derived from a customer beyond the customer’s domain. In other words, in no event can your app collect personally identifiable information and transmit that information to you or to anyone outside the customer’s control.

* Consent for other information shared: If your apps use or transmit a customer’s business and infrastructure information (other than personally identifiable information), you must ensure that the app does so only after the customer has expressly agreed to both the scope of information collected and the use to be made of such information. You must protect the confidentiality of customer information and ensure that it is used only in the manner consented to. You must agree to take reasonable precautions (for example, through confidentiality or other agreements) to ensure that those within your control (for example, employees, contractors, and third-parties) who may gain access to any such customer information also maintain its confidentiality and limit its use in such manner.
* **Export compliance, with limited encryption permitted:** Initially Cisco will reject for the App Center any app that contains or calls on encryption capabilities in a manner that would require export review. Developers will be required to respond to and certify the questions that follow as part of the app submission. If any of the answers are affirmative, Cisco may not accept your app.

***Export Questions***

1. Does your app contain encryption of any type, such as SSL, SSH, HTTPS, VPN, IPsec, AES, or 3DES?

1. Does your app contain, use, or make calls to encryption for any purpose other than authentication or antivirus protection (such as encryption used for secure network management, HTTPS, VPN, or wireless security)?

1. Does your app contain, use, or make calls to encryption for any purpose other than piracy- and theft-prevention for software?

1. Does your app contain, use, or make calls toencryption greater than 64-bit symmetric or greater than 1024-bit asymmetric algorithms?

1. Does your app contain, use, or access encryption for protection of data or information security purposes?

If yes, you will need to describe the encryption used in your app and the type of information it secures: for example, network management data, user data, or \_\_Blob Field when you submit export compliance questionnaire. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Do any of the following describe your app or a feature or function of your app? Check all that apply.

 ☐ A. App that provides or performs [nonstandard cryptography](#_Text_for_Export) such as WAPI or other proprietary encryption means

☐ B. An application-specific software development kit using cryptography

☐ C. A cryptographic library, development kit, or toolkit

☐ D. App that provides or performs vulnerability analysis, network forensics, or computer forensics

☐ E. App that provides or performs investigation of data leakage, network breaches, and other malicious intrusion activities through triage of captured digital forensic data: for example, a Communications Assistance for Law Enforcement Act (CALEA) app

☐ F. App that provides secure WAN, metropolitan area network (MAN), VPN, satellite, or digital packet telephony or media (voice, video, or data)

☐ G. App designed, modified, adapted, or customized for government end users, or with cryptographic functions that have been modified or customized to customer specifications

☐ H. App with cryptographic functions or encryption components (except encryption software that is publicly available) that is user accessible and can be easily changed by the user

☐ I. App with an [open cryptographic interface](#_Text_for_Export) or a means for a user to insert cryptographic functions without assistance

☐ J. App that provides cryptanalysis or [cryptanalytic](#_Text_for_Export) functions

☐ K. None of the preceding criteria apply.

***If any of questions 6 A to J applies to your app:***

The use of encryption in your app requires an encryption registration number (ERN) from the U.S. Department of Commerce as well as a formal review and Commodity Classification Automated Tracking System (CCATS) classification by the U.S. Department of Commerce. At this point, Cisco’s current policy denies acceptance of such apps. We encourage you to not submit the app for further review. You will have the opportunity to resubmit your app when we change our policy. At that point, you will be required to resubmit your app and upload a copy of your ERN and CCATS. To obtain an ERN, please see <http://www.bis.doc.gov/encryption/question3_sub.htm> or consult the U.S. Bureau of Industry and Security at 1-202-482-0707 or your trusted legal advisor. To receive a CCATS classification, you must submit a commodity classification request to the U.S. Department of Commerce. More information can be found at http://www.bis.doc.gov/encryption/question5sub\_2.htm, or in sections 740.17b.3, 740.17b.2, and 742.15 (b)(3) of the U.S. Export Administration Regulations.

**Note:** Apps implementing strong encryption functions classified under U.S. Encryption Commodities, Software, and Technology (ENC) section 742.15, 740.17b.3, or 740.17b.1 may be posted to Cisco App Center. Apps classified under ENC section 740.17b.2 are more tightly controlled and cannot be posted to Cisco App Center.

***If question 6 K applies to your app:***

Your app requires an ERN from the U.S. Department of Commerce. To obtain an ERN, please see <http://www.bis.doc.gov/encryption/question3_sub.htm> or consult the U.S. Bureau of Industry and Security at 1-202-482-0707 or your trusted legal advisor. Please upload your ERN on your company’s letterhead and list the export control classification number (ECCN) for your item.

Developers posting to Cisco App Center are responsible for obtaining required government approvals. Export laws require that apps containing encryption be properly authorized for export. Failure to comply could result in severe penalties. For further information, click [here](http://www.bis.doc.gov/encryption/default.htm). Along with your app submission package, you are required to submit the responses to the preceding export compliance questions on your company letterhead with an authorized signature and date.

**Content**

It is your responsibility to ensure that your app includes or uses content that is created by you or that you possess the license to use. We reserve the right to remove your app should we discover that your app violates this condition, using unauthorized content.

We are not, by any means, endorsing your app regarding its proper functioning or quality. Hence, you are not allowed to publicize that the app is endorsed or verified or supplied by Cisco.

Exercise caution when using third-party data. Do not use third-party source code or any form of patented material or copyrighted data (including but not limited to logos, trademarks, and patented ideas).

For Cisco’s app review committee, any subsequent update in your app is a new review process, and your app will go through the same review cycle. Hence, as a best practice, you should limit the number of updates.

App Review Submission Checklist

Use the following checklist to help ensure that your submission is complete.

☐ I have tested my app for defects and high-severity and critical bugs including but not limited to crashes.

☐ My app follows the Cisco App Center development guidelines presented in this document.

☐ I have provided my contact information.

☐ I have provided the details of my verification environment.

☐ I have followed industry-standard coding and verification guidelines, including the use of comments where necessary.

☐ I have attached the responses to the export compliance questions on my company letterhead with an authorized signature and date.

App Review Procedure

After submission, your app will go through technical and export compliance reviews. The following list shows some of the checks we have in place. Note that this is not a complete list of all checks.

1.     Does the app’s function adhere to the use case and specifications and description provided by the app developer?

2.     Does the app use updated and secure software components as part of its package, and is it free from vulnerable software components?

3.     Does the app have a Readme file, appropriate icons, snapshots, and other help material that allows app users to be able to use the app?

4.     Does the app package adhere to the developer’s guidelines outlined in this document?

5.     Does the app belong to one of the categories listed in App Center?

6.     Is the app built using Cisco provided packager utility? (Use of this utility helps ensure that the app’s package has valid metadata and a valid structure. The app must have valid metadata and a valid package structure for acceptance.)

What to Expect After You Submit App for Review

The Cisco App Center review committee will review your app for quality and compliance. Our review will be holistic. We will apply both qualitative and quantitative criteria to our evaluation. We will use both automated and manual verification methodologies.

If we have any questions or concerns regarding your app, we will reach out to you. If you have any questions or a need to expedite the review, please use the App Center portal to contact us.

We look forward to your partnership in helping our customers attain their business goals.