|  |  |
| --- | --- |
| **Document Number:** | EDCS-1274160 |
| **Last Revision Date:** | 07/10/14 |
| **Policy Owner:** | J.P. HamiltonC. Candelaria |
| **Policy Owners’ Organizations:** | Threat Response, Intelligence and Development (TRIAD) Engineering  |
| **Next Review Date:** | 07/28/16 |

****

**Cisco Image Signing Policy**

**– Table of Contents –**

[Purpose/Executive Summary 3](#_Toc391356228)

[Overview 3](#_Toc391356229)

[Scope 3](#_Toc391356230)

[Compliance Effective Date 3](#_Toc391356231)

[Policy Statement 4](#_Toc391356232)

[1.1 Image Signing Policy 4](#_Toc391356233)

[Policy Compliance 4](#_Toc391356234)

[1.2 Roles and Responsibilities 4](#_Toc391356235)

[1.3 Compliance Measurement 5](#_Toc391356236)

[1.4 Exceptions 5](#_Toc391356237)

[1.5 Non-Compliance 5](#_Toc391356238)

[Supporting Documents 5](#_Toc391356239)

[Related Information 6](#_Toc391356240)

[Definitions 6](#_Toc391356241)

[Approvals 7](#_Toc391356242)

[Revision History 7](#_Toc391356243)

[Appendix 8](#_Toc391356244)

# Purpose/Executive Summary

Image Signing is essential to Cisco’s trusted software foundation. Most additional layers of trust and security build on Image Signing. This document outlines the Cisco Image Signing policy and refers to requirements and standards along with supporting documents that further govern Image Signing.

# Overview

Cisco Image Signing is a security technology method which allows the user to certify that a software image was created and/or provided by Cisco. Once an image is signed any change to the image, whether the change is introduced accidentally or intentionally, can be detected automatically. This document outlines the master policy requirements for implementing Image Signing correctly within the Cisco development environment. Implementation specifics are contained in an approved standard and may vary. However, compliance to this policy is mandatory.

Image signing is considered the initial foundation on which the entire chain of trust is built for Cisco products. Most additional product security features are built on top of Image Signing.

A wide variety of code can be signed including tools, applications, scripts, libraries, plug-ins, and other “code-like” data.

From the customer’s perspective, image signing achieves the following goals:

1. Asserts that the code came from Cisco Systems, Inc.
2. Provides cryptographically strong proof that the code has not been modified since signing
3. Asserts that Cisco accepts responsibility for the functionality of all portions of the code

From Cisco’s perspective, image signing provides the following:

1. Extends anti-counterfeit protections
2. Provides revenue loss protection by protecting Cisco’s brand against license check modifications or other tampering attempt mechanisms
3. Can be used as a forensic tool should the need arise

# Scope

This policy applies to all released Cisco code or software images worldwide, including, but not limited to the following types of deployments:

* Software or firmware loaded on a hardware product
* Standalone software and applications software releases for upgrades, installation images or replacement images

# Compliance Effective Date

This policy is effective 07/28/2014.

# Policy Statement

### Image Signing Policy

This section outlines the Cisco image signing policy and refers to multiple standards and supporting documents that are considered part of the policy. Any of these standards may change over time to include current best practices.

Cisco’s image signing policy consists of the following requirements:

#### All customer-facing (or “released”) software images must be signed and follow Cisco’s image signing process outlined in the appropriate Cisco Image Signing standard listed below. This includes software produced by or on behalf of Cisco.

* [Cisco Software on Cisco Hardware Image Signing Standard, EDCS-1337783](http://wwwin-eng.cisco.com/Eng/GSU/Image_Signing_Prog/EDCS_1337783.docx)
* [Cisco Software on Third Party Hardware Image Signing Standard, EDCS-1337784](http://wwwin-eng.cisco.com/Eng/GSU/Image_Signing_Prog/Standards/EDCS-1337784.docx)
* [Cisco Service and Feature Software Image Signing Standard, EDCS-1337785](http://wwwin-eng.cisco.com/Eng/GSU/Image_Signing_Prog/Standards/EDCS-1337785.docx)
* [Third Party Software on Cisco Hardware Image Signing Standard, EDCS-1337786](http://wwwin-eng.cisco.com/Eng/GSU/Image_Signing_Prog/Standards/EDCS-1337786.docx)

#### The customer must be able to cryptographically verify all Cisco-developed software. The cryptographic verification mechanisms are found in the standards. Any verification mechanisms on a Cisco product operating in a customer environment must only accept Cisco software signed by a Release Key.

#### Only fulltime Cisco employees (blue badge) who are approved by TRIAD and meet the requirements listed in the[Cisco Authorization Criteria List for Image Signing, EDCS-1337777](http://wwwin-eng.cisco.com/Eng/GSU/Image_Signing_Prog/EDCS_1337777.docx), may sign release images.

#### No image shall be released to anyone or any organization outside of Cisco Systems, Inc. that has not been through the proper release and image signing processes.

#### Development staff must comply with all standard documents referenced in this document.

#### Only InfoSec-approved tools or systems may be used to sign an image.

# Policy Compliance

### Roles and Responsibilities

A designated engineer is the only authorized individual who can sign Cisco images for release.

To determine the designated engineer in your organization to sign images or to request authorization status to sign images, refer to your Security Officer (SO) or Release Management organization.

To provide the necessary checks and balances to successfully and correctly implement and enforce the Cisco Image Signing Policy requires various roles with associated responsibilities. See the appendix for a list of these roles and responsibilities.

### Compliance Measurement

Compliance to this policy is required. Threat Response, Intelligence and Development (TRIAD) Engineering is responsible to verify that Cisco groups and released images comply with this policy and its related standards. TRIAD confirms compliance through various methods including, but not limited to tool reports, random internal and external audits, and feedback to the Image Signing program team.

### Exceptions

Any exceptions to this policy must be approved **before** the image is released to an external customer, partner or vendor by TRIAD and your Sr. VP. Exceptions, either temporary or permanent, require documentation. For temporary exceptions the documentation must outline the process for eventual compliance.

A product or software image released before the Cisco Image Signing Policy took effect (07/28/2014) is not required to be re-released to comply with this policy. All subsequent releases shall, however, be required to comply with this policy unless an exception is requested and granted.

To request an exception refer to <http://iwe.cisco.com/web/cspo-pki/image-signing>.

Records of exceptions are to be archived according to the Cisco Records Management Process, <http://wwwin.cisco.com/process/bes/iso/record_mgmt.shtml>.

### Non-Compliance

Compliance with Cisco policies is required. Deviations or non-compliance with this policy, including attempts to circumvent the stated policy or process by bypassing or knowingly manipulating the process, system or data may result in disciplinary actions, up to and including termination, as allowed by local laws.

A violation of this policy by a temporary worker, contractor, consultant or vendor may result in the termination of the vendor’s contract or an individual’s assignment at Cisco Systems, Inc.

# Supporting Documents

This Cisco Image Signing Policy refers to the following standards and are considered part of the Cisco Image Signing Policy:

* [Cisco Software on Cisco Hardware Image Signing Standard, EDCS-1337783](http://wwwin-eng.cisco.com/Eng/GSU/Image_Signing_Prog/EDCS_1337783.docx)
* [Cisco Software on Third Party Hardware Image Signing Standard, EDCS-1337784](http://wwwin-eng.cisco.com/Eng/GSU/Image_Signing_Prog/Standards/EDCS-1337784.docx)
* [Cisco Service and Feature Software Image Signing Standard, EDCS-1337785](http://wwwin-eng.cisco.com/Eng/GSU/Image_Signing_Prog/Standards/EDCS-1337785.docx)
* [Third Party Software on Cisco Hardware Image Signing Standard, EDCS-1337786](http://wwwin-eng.cisco.com/Eng/GSU/Image_Signing_Prog/Standards/EDCS-1337786.docx)
* InfoSec PKI Identity Assurance Services: Image Signing:
<http://iwe.cisco.com/web/cspo-pki/image-signing>

The following documents also support the Cisco Image Signing Policy:

* [Cisco Authorization Criteria List for Image Signing, EDCS-1337777](http://wwwin-eng.cisco.com/Eng/GSU/Image_Signing_Prog/EDCS_1337777.docx)
* [Image Signing Playbook, EDCS-1347136](http://wwwin-eng.cisco.com/Eng/GSU/Image_Signing_Prog/Program_Plans/Image_Signing_Playbook.ppt)
* [Image Signing Enrollment Request Form, EDCS-1337779](http://wwwin-eng.cisco.com/Eng/GSU/Image_Signing_Prog/EDCS-1337779.docx)
* [Roles and Responsibilities for Image Signing, EDCS-1337778](http://wwwin-eng.cisco.com/Eng/GSU/Image_Signing_Prog/EDCS_1337778.docx)
* [Product Key Naming Guidelines, EDCS-1337780](http://wwwin-eng.cisco.com/Eng/GSU/Image_Signing_Prog/EDCS-1337780.docx)
* [Test Requirements and Test Plan Examples for Image Signing, EDCS-1337781](http://wwwin-eng.cisco.com/Eng/GSU/Image_Signing_Prog/EDCS-1337781.docx)
* [Cryptographic Key Management Standard, EDCS-806750](http://wwwin-eng.cisco.com/IT/Infrastructure/Arch/SEC/Standards/CSPO_Cryptographic_Key_Management_Standard.doc)

# Related Information

The following documents provide additional information on Image Signing and related topics:

* [Information Security: Data Classification Policy](http://wwwin.cisco.com/infosec/policies/classification.shtml)
* [Information Security: Security Support](http://wwwin.cisco.com/infosec/support/)
* [Information Security: Network Access Policy](http://wwwin.cisco.com/infosec/policies/networkaccess/)
* [SSL/TLS Certificate Standard](http://wwwin-eng.cisco.com/IT/Infrastructure/Arch/SEC/Standards/CSPO_SSL_TLS_Certificate_Standard.doc)
* [Cisco Policies: Information Security Policies](http://wwwin.cisco.com/cisco/policy/InformationSecurity.shtml#infosecDocsTab=0)
* [Information Security: Policies & Standards](http://wwwin.cisco.com/infosec/policies/)
* For InfoSec-approved tools or systems that may be used to sign an image refer to the following URL:<http://iwe.cisco.com/web/cspo-pki/image-signing>

# Definitions

The following terms and definitions are used in this document:

|  |  |
| --- | --- |
| Code | Includes software tools, applications, scripts, libraries and plug-ins |
| DE | Development Engineer |
| Development Image  | Images created during the development stage of a product, normally used for functional or feature testing. These images are not customer facing. |
| DT | Development Tester |
| EDCS | Electronic Document Control System |
| IAS | Identity Assurance Services |
| Image Signing | Security technology which can automatically detect that a software image has changed |
| InfoSec | Information Security |
| RE  | Release Engineer |
| Release Key | Highly secured cryptographic credentials used to assert the authenticity of Cisco software |
| Release Image  | Customer facing image created and fitted for customer use. Release Images meet release image requirements. |
| SO | Security Officer |
| SSL | Secure Sockets Layer |
| TLS | Transport Layer Security |
| TRIAD | Threat Response, Intelligence and Development |

# Approvals

|  |  |
| --- | --- |
| **Organization** |  **Name** |
| SVP TRIAD | John Stewart |
| VP TRIAD Engineering | Edward Paradise |
| SVP Advanced Security Initiatives Group | Gregory Neal Akers |
| VP Information Technology | Steve Martino |

# Revision History

|  |  |  |
| --- | --- | --- |
|  **Date** |  **Name or Userid** |  **Modifications Made** |
| 06/06/13 | carcande | Created original document |
| 07/12/13 | mcwillis | Prepared first full draft |
| 02/17/14 | mcwillis | Approved version 1 |
| 06/24/14 | carcande, lholmqui | Edited content, modified format to standard template, linked documents, changed policy effective date to 07/28/2014. |
| 07/10/14 | lholmqui | Changed the date before which a product or software image is not required to be re-released to comply with the Image Signing policy to 07/28/2014. Improved formatting. |

# Appendix

The following individuals provide the necessary checks and balances to successfully and correctly implement and enforce the Cisco Image Signing Policy:

* Administrator—Fulltime Cisco employee and member of the InfoSec IAS team who has full privileges in the InfoSec tool system. Administrators can perform the following tasks:
* Create and remove users
* Assign user accounts to roles within the system
* Create new keys in the system
* Map new keys to user accounts
* Assist with policy enforcement
* Security Officer (SO)—Fulltime Cisco employee who is granted access to a particular InfoSec system key. The SO is responsible for the following tasks:
* Add and remove users to the access lists for the key or keys for which the SO is responsible.
* Generate new keys and map users to them
* Actively manage keys and users related to the respective product keys
* Create or designate alternate SO users for their own keys
* Ensure policy adherence
* Release Engineer (RE)—Must be a fulltime Cisco employee, in an authorized business entity, and satisfy the requirements listed in the *Cisco Authorization List Criteria Standards* document. The RE uses the InfoSec product key to build and sign release images that are deployed to Cisco customers.
* Build Engineer–Responsible for building images and documenting the aspects of images, scripts, and the tools used to build images.
* Development Engineer (DE)—Implements image signing into code and is granted access to specific product keys for signing activities, and is authorized to sign development images. Some development keys in the system automatically grant access to all users.
* Development Tester (DT)—Develops and executes tests plans that include testing the strength of the image signing implementation by using at least a minimum predetermined set of test requirements. For more information on the minimum predetermined set of test requirements refer to [Test Requirements and Test Plan Examples for Image Signing, EDCS-1337781](http://wwwin-eng.cisco.com/Eng/GSU/Image_Signing_Prog/EDCS-1337781.docx)
* Web Management User—Has access to reporting functions in the InfoSec key system, and may examine the settings within the system, but may not change them.

For additional information on roles and responsibilities refer to[Roles and Responsibilities for Image Signing, EDCS-1337778](http://wwwin-eng.cisco.com/Eng/GSU/Image_Signing_Prog/EDCS_1337778.docx).