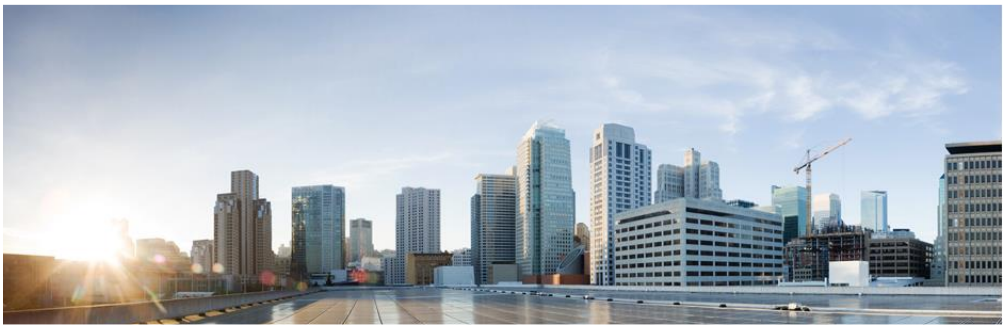

Cisco Catalyst 3650 and 3850 Series Switches running IOS-XE 16.12

Common Criteria Operational User Guidance

And Preparative Procedures

Version 2.0

4 December 2019

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Table of Contents

List of Tables

Acronyms

The following acronyms and abbreviations are common and may be used in this document:

Table 1 Acronyms

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control Lists
AES	Advanced Encryption Standard
BRI	Basic Rate Interface
CAK	Secure Connectivity Association Key
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CKN	Secure Connectivity Association Key Name
CM	Configuration Management
DHCP	Dynamic Host Configuration Protocol
EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
EAP-TLS	EAP Transport Layer Security
EAPOL	EAP over LANs
EHWIC	Ethernet High-Speed WIC
ESP	Encapsulating Security Payload
GCM	Galois Counter Mode
GE	Gigabit Ethernet port
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
ICMP	*Internet Control Message Protocol*
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IOS	The proprietary operating system developed by Cisco Systems.
IP	Internet Protocol
IPsec	IP Security
ISDN	*Integrated Services Digital Network*
IT	Information Technology
MAC	Media Access Control
MKA	MACsec Key Agreement protocol
MKPDU	MACsec Key Agreement Protocol Data Unit
MPDU	MAC Protocol Data Unit
MSAP	MAC Service Access Point
MSDU	MAC Service Data Unit
MSK	Master Session Key
NDcPP	collaborative Network Device Protection Profile
NVRAM	Non-volatile random access memory, specifically the memory in the switch where the configuration parameters are stored.
OS	Operating System
Packet	A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.
PBKDF2	Password-Based Key Derivation Function version 2

Acronyms / Abbreviations	Definition
PoE	Power over Ethernet
PP	Protection Profile
PRNG	Pseudo Random Number Generator
RADIUS	Remote Authentication Dial In User Service
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
SA	Security Association
SAK	Secure Association Key
SC	Secure Channel
SCI	Secure Channel Identifier
SecTAG	MAC Security TAG
SecY	MAC Security Entity
SCI	Secure Channel Identifier
SecTAG	MAC Security TAG
SecY	MAC Security Entity
SFP	Small–form-factor pluggable port
SHS	Secure Hash Standard
SM	Service Module
SNMP	Simple Network Management Protocol
SSHv2	Secure Shell (version 2)
ST	Security Target
TCP	Transport Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User datagram protocol
WAN	Wide Area Network
WIC	WAN Interface Card

Terminology

The following terms are common and may be used in this document:

Table 2 Terminology

Term	Definition
Authorized Administrator	Any user which has been assigned to a privilege level that is permitted to perform all TSF-related functions.
Peer	Another switch on the network that the TOE interfaces with.
MACsec Peer	This includes any MACsec peer with which the TOE participates in MACsec communications. MACsec Peer may be any device that supports MACsec communications.
Remote VPN Gateway/Peer	A remote VPN Gateway/Peer is another network device that the TOE sets up a VPN connection with. This could be a VPN client or another switch.

Term	Definition
Security Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
vty	vty is a term used by Cisco to describe a single terminal (whereas Terminal is more of a verb or general action term).
Firmware (per NIST for FIPS validated cryptographic modules)	The programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) within the cryptographic boundary and cannot be dynamically written or modified during execution.

DOCUMENT INTRODUCTION

Prepared By:
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Catalyst 3650 and 3850 Series Switches (Cat3K Series) running Cisco IOS-XE 16.12.1. This Operational User Guidance with Preparative Procedures addresses the administration of the TOE software and hardware and describes how to install, configure, and maintain the TOE in the Common Criteria evaluated configuration. Administrators of the TOE will be referred to as administrators, authorized administrators, TOE administrators, semi-privileged administrators, and privileged administrators in this document.

1. Introduction

This Operational User Guidance with Preparative Procedures documents the administration of the Cisco Catalyst 3650 and 3850 Series Switches (Cat3K Series) running Cisco IOS-XE 16.12.1 TOE certified under Common Criteria. The TOE may be referenced below as the Cat3K Series, TOE, or simply switch.

1.1 Audience

This document is written for administrators configuring the TOE, specifically the Cisco IOS-XE 16.12.1 software. This document assumes that you are familiar with the basic concepts and terminologies used in internetworking, understand your network topology and the protocols that the devices in your network can use, that you are a trusted individual, and that you are trained to use IOS software and the various operating systems on which you are running your network. For using the IOS command-line interface refer to **[3]** Using the Command-Line Interface and **[11]** Using the Cisco Command-Line Interface.

1.2 Purpose

This document is the Operational User Guidance with Preparative Procedures for the Common Criteria evaluation. It was written to highlight the specific TOE configuration and administrator functions and interfaces that are necessary to configure and maintain the TOE in the evaluated configuration. The evaluated configuration is the configuration of the TOE that satisfies the requirements as defined in the Security Target (ST). This document covers all of the security functional requirements specified in the ST and as summarized in Section 3 of this document. This document does not mandate configuration settings for the features of the TOE that are outside the evaluation scope, such as information flow polices and access control, which should be set according to your organizational security policies.

This document is not meant to detail specific actions performed by the administrator but rather is a road map for identifying the appropriate locations within Cisco documentation to get the specific details for configuring and maintaining Cat3K Series operations. It is recommended that you read all instructions in this document and any references before performing steps outlined and entering commands. Section 7 of this document provides information for obtaining assistance in using IOS/IOS XE.

1.3 Document References

This document makes reference to several Cisco Systems documents. The documents used are shown below in Table 3 Reference Documents. Throughout this document, the guides will be referred to by the "#", such as **[1]**.

Table 3 Reference Documents

Reference number	Document Name	Link
[1]	Release Notes for Cisco Catalyst 3650 and 3850 Series Switches running Cisco IOS-XE 16.12	3650 - https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3650/software/release/16-12/release_notes/ol-16-12-3650.html 3850 - https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/16-12/release_notes/ol-16-12-3850.html
[2]	Catalyst 3650 Switch Hardware Installation Guide Catalyst 3850 Switch Hardware Installation Guide	http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3650/hardware/installation/guide/Cat3650hig_book/HIGINSTL.html http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/hardware/installation/guide/b_c3850_hig.html
[3]	Software Configuration Guide, Cisco IOS XE 16.12.x (Catalyst 3650 Switches) Software Configuration Guide, Cisco IOS XE 16.12.x (Catalyst 3850 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3650/software/release/16-12/configuration_guide/b_1612_3650_cg.html https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/16-12/configuration_guide/b-1612-3850-cg.html
[4]	User Security Configuration Guide, Cisco IOS XE Fuji 16.12.x	(a) https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/xe-16-12/sec-usr-cfg-xe-16-12-book.pdf (b)

Reference number	Document Name	Link
		https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/xe-16-12/sec-usr-cfg-xe-16-12-book.html
[5]	Cisco IOS Network Management Configuration Guide, Release 15.0	http://www.cisco.com/c/en/us/td/docs/ios/netmgmt/configuration/guide/15_0s/nm_15_0s_book.html
[6]	Cisco IOS Security Command Reference A to Z	http://www.cisco.com/en/US/docs/ios-xml/ios/security/a1/sec-a1-cr-book.html (http://www.cisco.com/en/US/docs/ios-xml/ios/security/d1/sec-d1-cr-book.html http://www.cisco.com/en/US/docs/ios-xml/ios/security/m1/sec-m1-cr-book.html http://www.cisco.com/en/US/docs/ios-xml/ios/security/s1/sec-s1-cr-book.html (master list) http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html
[7]	FIPS Algorithm Certificate	https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program
[8]	Cisco IOS IP Routing Protocols Configuration Guides (multiple documents for supported routing protocols)	http://www.cisco.com/en/US/products/ps11845/products_installation_and_configuration_guides_list.html
[9]	Internet Key Exchange for IPsec VPNs Configuration Guide, Cisco IOS Release 16.5	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ikevpn/configuration/xe-16-5/sec-ike-for-ipsec-vpns-xe-16-5-book/sec-vrf-aware-ipsec.html
[10]	Cisco IOS Configuration Fundamentals Command Reference	http://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/cf_book.html
[11]	Configuration Fundamentals Configuration Guide	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/xe-16/fundamentals-xe-16-book.html

Reference number	Document Name	Link
[12]	Secure Shell v2 Configuration Guide, Cisco IOS XE 16.6	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_ssh/configuration/xe-16-12/sec-usr-ssh-xe-16-12-book.html
[13]	Errors and System Messages	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/16_xe/smg/ent-rout-smg.html
[14]	Configuring Certificate Enrollment for a PKI	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-16-12/sec-pki-xe-16-12-book/sec-cert-enroll-pki.html
[15]	Public Key Infrastructure Configuration Guide, Cisco IOS Release	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-16-12/sec-pki-xe-16-12-book.html
[16]	Loading and Managing System Images Configuration Guide	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sys-image-mgmt/configuration/xe-16-12/sysimgmgmt-xe-16-12-book.html

1.4 Supported Hardware and Software

Only the following hardware and software listed below is compliant with the Common Criteria Cisco Catalyst 3650 and 3850 Series Switches NDcPPv2.0e and MACsec EP v1.2 evaluation. Using hardware not specified invalidates the secure configuration. Likewise, using any software version other than the evaluated software listed below will invalidate the secure configuration.

1.4.1 Supported Configurations

The TOE is comprised of both software and hardware. The hardware is comprised of the following: Cisco Catalyst 3650 and 3850 Series Switches. The software is comprised of the Universal Cisco Internet Operating System (IOS) software image Release IOS XE 16.12.1.

The Cisco Catalyst 3650 and 3850 Series Switches (Cat3K Series) that comprises the TOE has common hardware characteristics. These characteristics affect only non-TSF relevant functions of the switches (such as throughput and amount of storage) and therefore support security equivalency of the switches in terms of hardware.

The Catalyst 3650 and 3850 Series Switches primary features include the following:

- Central processor that supports all system operations;
- Dynamic memory used by the central processor for all system operation.

- Flash memory (EEPROM), used to store the Cisco IOS image (binary program).
- USB port (v2.0) (note, none of the USB devices are included in the TOE).
    - Type A for Storage, all Cisco supported USB flash drives.
    - Type mini-B as console port in the front.
- Non-volatile read-only memory (ROM) is used to store the bootstrap program and power-on diagnostic programs.
- Non-volatile random-access memory (NVRAM) is used to store switch configuration parameters that are used to initialize the system at start-up.

Physical network interfaces (minimally two) (e.g. RJ45 serial and standard 10/100/1000 Ethernet ports). Some models have a fixed number and/or type of interfaces; some models have slots that accept additional network interfaces.

Cisco IOS is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching.

For detailed information about Software Activation, visit http://www.cisco.com/go/sa.

1.5 Operational Environment

The TOE supports the following hardware, software, and firmware components in its operational environment. Each component is identified as being required or not based on the claims made in this Security Target. All of the following environment components are supported by all TOE evaluated configurations.

Table 4 Required non-TOE Hardware/ Software/ Firmware

Component	Usage/Purpose Description for TOE performance
Management Workstation with SSH Client	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Local Console	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
RADIUS AAA Server	This includes any IT environment RADIUS AAA server that provides single-use authentication mechanisms. This can be any RADIUS AAA server that provides single-use authentication. The TOE correctly leverages the services provided by this RADIUS AAA server to provide single-use authentication to administrators.
Syslog Server	The syslog audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE. The syslog server will need to act as an IPsec peer or as an IPsec endpoint.
Certification Authority (CA)	This includes any IT Environment Certification Authority on the TOE network. This can be used to provide the TOE with a valid certificate during certificate enrollment.

1.6 Excluded Functionality

The exclusion of this functionality does not affect the compliance to the collaborative Protection Profile for Network Devices + Errata 20180314, Version 2.0e (NDcPPv2.0e)

and the Network Device Collaborative Protection Profile (NDcPP) Extended Package MACsec Ethernet Encryption (MACsec EP), version 1.2 (MACsec EP v1.2).

Table 5 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation on the switch.	This mode of operation includes non-FIPS allowed operations.

2. Secure Acceptance of the TOE

In order to ensure the correct TOE is received, the TOE should be examined to ensure that that is has not been tampered with during delivery.

Verify that the TOE software and hardware were not tampered with during delivery by performing the following actions:

Step 1 Before unpacking the TOE, inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the Cisco Systems logo and motifs. If it is not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 2 Verify that the packaging has not obviously been opened and resealed by examining the tape that seals the package. If the package appears to have been resealed, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 3 Verify that the box has a white tamper-resistant, tamper-evident Cisco Systems bar coded label applied to the external cardboard box. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This label will include the Cisco product number, serial number, and other information regarding the contents of the box.

Step 4 Note the serial number of the TOE on the shipping documentation. The serial number displayed on the white label affixed to the outer box will be that of the device. Verify the serial number on the shipping documentation matches the serial number on the separately mailed invoice for the equipment. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 5 Verify that the box was indeed shipped from the expected supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment note number for the shipment matches that used on the delivery. Also verify that the serial numbers of the items shipped match the serial numbers of the items delivered. This verification should be performed by some mechanism that was not involved in the actual equipment delivery, for example, phone/FAX or other online tracking service.

Step 6 Once the TOE is unpacked, inspect the unit. Verify that the serial number displayed on the unit itself matches the serial number on the shipping documentation and the invoice. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). Also verify that the unit has the following external identification:

Table 6: Evaluated Products and their External Identification

Product Name	External Identification
Cisco Catalyst 3650 Series Switches	Catalyst 3650
Cisco Catalyst 3850 Series Switches	Catalyst 3850

Step 7 Approved methods for obtaining a Common Criteria evaluated software images:

- Download the Common Criteria evaluated software image file from Cisco.com onto a trusted computer system. The reason to download to a trusted system within your organization, such as the management workstation, is to ensure the file has not been tampered with prior to securely copying to the TOE for installation.
- Software images are available from Cisco.com at the following: https://software.cisco.com/download/home.
- The TOE ships with the correct software images installed, however this may not be the evaluated version.

Step 8 Once the file is downloaded, copy (via tftp) the downloaded **[16]** and verified software image from the trusted system as described in Image Verification **[4(b)].**

Once the file has been copied, it is recommended that you read and familiarize yourself Overview Basic Configuration of a Cisco Networking Device and Using AutoInstall to Remotely Configure Cisco Networking Devices **[11]** before proceeding with the install. You may also want to familiarize yourself with **[6]** basic commands and **[11]** Using the Cisco IOS Command-Line Interface concepts before proceeding with the installation and configuration of the TOE.

To use the published hash verification prior to installation. The TOE will automatically display the hash verification on boot or by using the reload command. The successful hash verification message will display on the successful verification of the boot image. If the image was tampered with in any way, an error would display and the image will not boot. Confirm that the TOE loads the image correctly, completes internal self-checks and displays the cryptographic export warning on the console.

Once the image is loaded into bootflash, to display information related to software authenticity for a specific image file, use the verify command. For example:

<9300># verify <image name>

The image name and hash are listed below in Table 7: Evaluated Software Images

In the evaluated configuration the published hash is used to verify the software authenticity, however a digital signature is also available for verification. To verify the digital signature prior to installation, the show software authenticity file command allows you to display software authentication related information that includes image credential information, key type used for verification, signing information, and other attributes in the signature envelope, for a specific image file. The command handler will extract the signature envelope and its fields from the image file and dump the required information **[16]** Loading and Maintaining System Images -> Digitally Signed Cisco Software using the **show software authenticity file [6]**

Switch# **show software authenticity file** {bootflash0:filename | bootflash1:filename | bootflash:filename | nvram:filename | usbflash0:filename | usbflash1:filename}

To display the software public keys that are in the storage with the key types, use the **show software authenticity keys** command in privileged EXEC mode.

To display information related to software authentication for the current ROM monitor (ROMMON), monitor library (monlib), and Cisco IOS image used for booting, use the **show software authenticity running** command in privileged EXEC mode.

Step 9 To Install and configure your Cat3K Series switch follow the instructions as described in **[3]** Using the Command-Line Interface and then follow System Management and Security.

Start your Cat3K Series switch as described in **[11]**. Confirm that your Cat3K Series switch loads the image correctly, completes internal self-checks and displays the cryptographic export warning on the console.

Step 10 The end-user must confirm once the TOE has booted that they are indeed running the evaluated version. Use the "**show version**" command **[6]** show protocols through showmon to display the currently running system image filename and the system software release version. See below for the detailed hash value that must be checked to ensure the software has not been modified in anyway. It is also recommended the license level be verified and activated as described in **[1]**. It is assumed the end-user has acquired a *permanent license is valid for the lifetime of the system on which it is installed.*

Table 7: Evaluated Software Images

Software Version	Image Name / Description	Checksum Hash
IOS XE 16.12.1c	cat3k_caa-universalk9.16.12.01.SPA.bin / CAT3850/3650 UNIVERSAL	SHA512 Checksum: 5800720c79f217e150e50397006f199c…..…

When updates, including psirts (bug fixes) to the evaluated imagine are posted, customers are notified that updates are available (if they have purchased continuing support), information provided how to download updates and how to verify the updates is the same as described above.

3. Secure Installation and Configuration

To ensure the TOE is in its evaluated configuration, the configuration settings outlined in the following sections need to be followed and applied. The evaluated configuration includes the following security features that are relevant to the secure configuration and operation of the TOE.

- Security audit – ensures that audit records are generated for the relevant events and are securely transmitted to a remote syslog server
- Cryptographic support – ensures cryptography support for secure communications. The TOE also authenticates and encrypts packets between itself and a MACsec peer. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys to protect data exchanged by the peers.
- Identification and authentication – ensure a warning banner is displayed at login, that all users are successfully identified and authenticated prior to gaining access to the TOE, the users can only perform functions in which they have privileges, and terminates users after a configured period of inactivity
- Secure Management – provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 session or via a local console connection.
- Protection of the TSF - protects against interference and tampering by untrusted subjects by implementing identification, authentication, the access controls to limit configuration to Authorized Administrators and the TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software. TOE performs testing to verify correct operation of the switch itself and that of the cryptographic module The TOE is also able to detect replay of information received via secure channels (MACsec). Finally, the TOE maintains the date and time.
- TOE access - terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session. The TOE can also be configured to lock the Authorized Administrator account after a specified number of failed logon attempts until an authorized administrator can enable the user account. The TOE can also display an Authorized Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.
- Trusted Path/Channel - allows trusted channels to be established to itself from remote administrators over SSHv2 and initiates outbound IPsec tunnels to transmit audit messages to remote syslog servers. In addition, IPsec is used to secure the session between the TOE and the authentication servers

3.1 Physical Installation

Follow the Cisco Catalyst 3650 and 3850 Series Switches Hardware Installation Guide **[2]** for preparation of the physical site, and hardware installation.

3.2 Initial Setup via Direct Console Connection

The Cisco Catalyst 3650 and 3850 Series Switches must be given basic configuration via console connection prior to being connected to any network.

3.2.1 Options to be chosen during the initial setup of the Catalyst 3650 and 3850 Series Switches

The setup starts automatically when a device has no configuration file in NVRAM. When setup completes, it presents the System Configuration Dialog. This dialog guides the administrator through the initial configuration with prompts for basic information about the TOE and network and then creates an initial configuration file. After the file is created, an authorized administrator can use the CLI to perform additional configuration. *Performing Device Setup Configuration* in **[3]** describes how to use Setup to build a basic configuration and to make configuration changes. The following items must be noted during setup:

It should be noted that the account created during the initial installation of the TOE is considered the privileged administrator and has been granted access to all commands on the TOE (privilege level 15).

The privilege levels are not necessarily hierarchical in the sense they are configurable. The privilege level determines the functions the user can perform. Privilege levels 0 and 1 are defined by default, while levels 2-14 are undefined by default. Levels 0-14 are considered the semi-privileged administrator and can be set to include any of the commands available to the level 15 administrators.

The number of administrators created, and their various levels of access are based on organizational requirements and policies.

The term “authorized administrator” is used in this document to refer to any administrator that has successfully authenticated to the switch and has access to the appropriate privileges to perform the requested functions.

Refer to the IOS Command Reference Guide for available commands, associated roles and privilege levels **[3] [4(b)] [6] [10]**.

1 – Enable Secret – Must adhere to the password complexity requirements. Note that this setting can be confirmed after “setup” is complete by examining the configuration file for “enable secret 5 …” in Cisco IOS Security Command Reference: Commands D to L -> select E -> select enable secret -> **[6]**

2 – Enable Password - Must adhere to the password complexity requirements. Note that this must be set to something different than the enable secret during “setup”, however after setup this will not be used within the evaluated configuration. In Cisco IOS Security Command Reference: Commands D to L -> select E -> select enable password **[6]**

3 – Virtual Terminal Password - Must adhere to the password complexity requirements. Note that securing the virtual terminal (or vty) lines with a password in the evaluated configuration is suggested. This password allows access to the device through only the console port. Later in this guide steps will be given to allow ssh into the vty lines. Reference

password (line configuration) In Cisco IOS Security Command Reference: Commands M to R -> select pac key through port-misuse -> select password (line configuration) **[6]**

4 – Configure SNMP Network Management – NO (this is the default). Note that this setting can be confirmed after "setup" is complete by examining the configuration file to ensure that there is no "snmp-server" entry. To ensure there is no snmp server agent running, use the "**no snmp-server**' command as described in **[5]** select Configuring SNMP. Note, in the evaluated configuration, SNMP should remain disabled,

3.2.2 Saving Configuration

IOS uses both a running configuration and a starting configuration. Configuration changes affect the running configuration, in order to save that configuration, the running configuration (held in memory) must be copied to the startup configuration. Refer to Working with the Cisco IOS File System, Configuration Files, and Software Images **[3]**.

This may also be achieved by either using the **write memory** command **[6] [10]** test cable-diagnostics through xmodem or the **copy system:running-config nvram:startup-config** command in **[6]**. These commands should be used frequently when making changes to the configuration of the Switch. If the Switch reboots and resumes operation when uncommitted changes have been made, these changes will be lost, and the Switch will revert to the last configuration saved. To see the current configuration, use the **show running-config** command in **[6]** Cisco IOS Security Commands Reference: Commands S to Z -> show parameter-map type consent through show users -> show running-config.

3.2.3 Secure Remote Management

In the *Secure Acceptance of the TOE* section of this document, includes the instructions to verify the correct image of the evaluated TOE has been received.

Section 3 of this document describes the secure installation and configuration for the evaluated TOE. The configuration enables SSH-protected communications for secure remote management on the TOE with the **crypto key generate rsa** and **ip ssh version 2** and restricts remote access with the **line console** (or vty) **0 10** and **transport input ssh** commands as described in **[3] [6] [12]**.

For setting CLI sessions and passwords using the CLI, refer to Security with Passwords, Privileges, and Login Usernames for CLI Sessions on Networking Devices **[12]**

Note that these settings are not to be changed, although the **crypto key generate rsa** command can be used to generate new rsa keys of 2048 bits or larger **[3] [6]**.

See the following sub-sections, 3.2.4 – 3.2.9 and Section 4 within this document for complete commands and associated settings for secure management of the TOE.

3.2.4 FIPS Mode

The TOE must be run in the FIPS mode of operation.

The use of the cryptographic engine in any other mode was not evaluated nor tested during the CC evaluation of the TOE. This is done by setting the following in the configuration:

The value of the boot field must be 0x0102. This setting disables break from the console to the ROM monitor and automatically boots the IOS image. From the ROMMON command line enter the following under section C commands **[10]:**

confreg 0x0102

The Common Criteria certification evaluated the following cryptographic functionality, all of which must be configured as described in this guide:

- SSHv2 must be used instead of SSHv1 with minimum RSA modulus sizes as described in this document.
- IPsec must be used to secure connections to AAA servers and may be used to secure other traffic that originates from the TOE (Cat 3K Series), or terminates at the TOE (Cat 3K Series). The evaluated configuration does not require using IPsec to secure traffic flows through the TOE (Cat 3K Series).
    - IKEv1 and IKEv2 must be configured as described in this document.
    - ESP must be used as described in this document.

The Common Criteria certification did not evaluate any of the following cryptographic functionality:

- MD5 may be used, such as in authentication of routing protocols in features of the TOE that are outside the evaluation scope, such as in authentication of routing protocols.
- RADIUS may be used, but only when tunneled in IPsec.
- AH may be used in IPsec but use of ESP is mandatory.

3.2.5 Administration of Cryptographic Self-Tests

The TOE provides self-tests consistent with the FIPS 140-2 requirements. These self-test for the cryptographic functions in the TOE is run automatically during power-on as part of the POST. These self-tests include the following:

- Software Integrity Test -
  The firmware integrity test ensures the correct operation of the device and its components
- RNG/DRBG Known Answer Test:
  For this test, known seed values are provided to the DRBG implementation. The DRBG uses these values to generate random bits. These random bits are compared to known random bits to ensure that the DRBG is operating correctly.
- AES Known Answer Test
  For the encrypt test, a known key is used to encrypt a known plain text value resulting in an encrypted value. This encrypted value is compared to a known encrypted value to ensure that the encrypt operation is working correctly. The decrypt test is just the opposite. In this test a known key is used to decrypt a known encrypted value. The resulting plaintext value is compared to a known plaintext value to ensure that the decrypt operation is working correctly.

- RSA Signature Known Answer Test (both signature/verification) - This test takes a known plaintext value and Private/Public key pair and used the public key to encrypt the data. This value is compared to a known encrypted value to verify that encrypt operation is working properly. The encrypted data is then decrypted using the private key. This value is compared to the original plaintext value to ensure the decrypt operation is working properly.
- HMAC Known Answer Test - For each of the hash values listed, the HMAC implementation is fed known plaintext data and a known key. These values are used to generate a MAC. This MAC is compared to a known MAC to verify that the HMAC and hash operations are operating correctly

During the system bootup process (power on or reboot), all the Power on Startup Test (POST) components for all the cryptographic modules perform the POST for the corresponding component (hardware or software). Also, during the initialization and self-tests, the module inhibits all access to the cryptographic algorithms. Additionally, the power-on self-tests are performed after the cryptographic systems are initialized but prior to the underlying OS initialization of external interfaces; this prevents the security appliances from passing any data before completing self-tests and entering FIPS mode. In the event of a power-on self-test failure, the cryptographic module will force the IOS platform to reload and reinitialize the operating system and cryptographic module. This operation ensures no cryptographic algorithms can be accessed unless all power on self-tests are successful.

The Software Integrity Test is run automatically whenever the IOS-XE system images is loaded and confirms through use of digital signature verification that the image file that's about to be loaded was properly signed and has maintained its integrity since being signed. The system image is digitally signed by Cisco prior to being made available for download from CCO on Cisco.com website.

The TOE provides the ability to invoke Cryptographic Self-Tests on-demand.

- This functionality is available to the privileged administrator or a semi-privileged administrator with a specific privilege level.
- This functionality is facilitated using the test crypto self-test command

If any self-tests fail, the TOE transitions into an error state. In the error state, all secure data transmission is halted and the TOE outputs status information indicating the failure.

Note: If an error occurs during the self-test, a SELF_TEST_FAILURE system log is generated.

> Example Error Message _FIPS-2-SELF_TEST_IOS_FAILURE: "IOS crypto FIPS self test failed at %s."
>
> Explanation FIPS self test on IOS crypto routine failed.

Cisco provides an online error message decoder that can be used for looking up any error messages that may be received: https://www.cisco.com/pcgi-bin/Support/Errordecoder/index.cgi

Additional information regarding Administration of Cryptographic Self-Tests review and action to take can be found in Self-Test section of **[8]**.

3.2.6 Administration of Non-Cryptographic Self-Tests

The TOE provides self-tests to verify the correct image is running on the TOE. This functionality is available to all administrators and can be executed on demand by reloading the TOE via the **reload /verify** command and observing the following output:

Calculating SHA-1 hash...done

validate_package: SHA-1 hash:

calculated [hash value]

expected [same hash value as above]

Image validated

This functionality cannot be disabled by any administrator **[11]** Using the Command-Line Interface and **[6]**.

The privileged administrator can also run the **show diagnostic** command to display the online diagnostic test results and the supported test suites **[6]** Configuring Online Diagnostics. Using this command, you will also be able to set diagnostic for various levels, setting a schedule, set the diagnostic log size, etc. For troubleshooting any error messages received while running the tests, messages from running diagnostic and actions to take, refer to Troubleshooting, Logging, and Fault Management **[5]** and System Message Overview **[13].** Refer to **[7]** for supported power on self-tests related to supported cryptographic algorithms.

3.2.7 Access Control and Lockout

The Cat 3K Series must be configured to use a username and password for each administrator and one password for the enable command. Ensure all passwords are stored encrypted by using the following command **[6]:**

Commands S to Z -> sa ipsec through sessions maximum ->service password-encryption:

service password-encryption

When creating administrator accounts, all individual accounts are to be set to a privilege level of one. This is done by using the following commands:

Commands S to Z -> traffic-export through zone security -> username (with parameters listed below)

username <name> **password** <password>

to create a new username and password combination, and

username <name> **privilege 1**

to set the privilege level of <name> to 1. If combining to one command, the password must be the last parameter:

username <name> privilege 1 password <password>

Also note to prevent administrators from choosing insecure passwords, each password must be at least 15 characters long. You may use the following command to set the minimum length to 15 if available on the TOE model or set using the **aaa-common-criteria policy** command.

> **security passwords min-length** <*length*> **[6]** Cisco IOS Security Commands Reference: Commands S to Z -> sa ipsec through sessions maximum -> security passwords min-length

Refer to Section 4.2 in this document or **[6]** for configuring strong passwords and setting the minimum password length using the **aaa-common-criteria policy** command. Also refer to **[6]** for any of the following commands:

To ensure the plain text password is securely stored, use the **password encryption aes** command **[6]** Cisco IOS Security Commands Reference: Commands M to R -> password encryption aes

Identification and authentication on the console/auxiliary port is required for Users. In the configuration mode, enter the following command **[6]**:

> Switch(config)#**aaa authentication login via-console**
>
> Switch(config)#**line console 0**
>
> Switch(config-line)#**login authentication via-console**

Administrator account access is to be restricted to a specified number of authentication attempts before the administrator account in question is locked out. The account then requires unlocking by an authorized administrator before it can be used again. The evaluated configuration requires that the lockout occurs after a specified threshold for unsuccessful authentication attempts. Use the following command, with '<x>' being the required number of attempts before lockout, to set the authentication failure threshold (the authentication threshold must be non-zero):

Commands A to C -> aaa accounting -> aaa local authentication attempts max-fail (with parameters listed below)

> **aaa local authentication attempts max-fail <**x>

A locked user account may be unlocked by a privileged administrator by using the following command **[6]**:

Commands A to C -> ca trust-point -> clear aaa local user lockout (with parameters listed below)

> **clear aaa local user lockout** <username>

You can enter a single username, or you can enter 'all' to specify all locked users are to be unlocked.

3.2.8 Session Termination

Inactivity settings must trigger termination of the administrator session. These settings are configurable using the following listed commands. See **[6]** *Cisco IOS Security Command References: Commands A to Z for the following commands.*

line vty <first> <last>

exec-timeout <time>

where first and last are the range of vty lines on the box (i.e. “0 4”), and time is the period of inactivity after which the session should be terminated for remote administration access via SSH.

See **[6]** D through E to set the local line console and time out

line console

exec-timeout <time>

The line console setting is not immediately activated for the current session. The current console session must be exited. When the user logs back in, the inactivity timer will be activated for the new session.

A user can also terminate the session by entering the exit command. The exit command is used to log off and exit the active session. See [6] *Cisco IOS Security Command References: Commands A to Z.*

To close an active terminal session by logging off the router, use the exit command in EXEC mode.

exit

3.2.9 User Lockout

User accounts must be configured to lockout after a specified number of authentication failures. See **[6]** *Cisco IOS Security Command References: Commands A to Z for the following commands.*

aaa local authentication attempts max-fail [*number of failures*]

where number of failures is the number of consecutive failures that will trigger locking of the account. Configuration of these settings is limited to the privileged administrator (see 4.1 User Roles).

Related commands:

Table 8 AAA Commands

AAA Command	AAA Command Result
clear aaa local user fail-attempts	Clears the unsuccessful login attempts of the user.
clear aaa local user lockout	Unlocks the locked-out user.
show aaa local user lockout	Displays a list of all locked-out users.

This applies to consecutive failures on the TOE during a given session and is not affected by the SSH session disconnections after their default number of failures.

3.3 Network Protocols and Cryptographic Settings

The switch provides secure transmission when TSF data is transmitted between separate parts of the TOE (encrypted sessions for remote administration (via SSHv2)).

The switch also supports the use of a remote AAA server (RADIUS), provided by the environment that is used as the enforcement point for identifying and authenticating users, including login and password dialog, challenge and response, and messaging support. Encryption of the packet body is provided through the use of RADIUS (note RADIUS only encrypts the password within the packet body). This AAA server should be on an internal protected network, such as a network isolated behind a VPN gateway, through which the Cat 3K Series can reach the AAA server using an IPsec tunnel.

The switch provides the capability to support the following routing protocols EIGRP, EIGRPv6 for IPv6, PIMv2, PIM-SMv2, PIM-SSMv2, OSPFv2, OSPFv3 for IPv6, RIP for IPv6, and RIPv2.

3.3.1 Remote Administration Protocols

Telnet should not be used for management purposes as there is no protection for the data that is transmitted. To ensure the administrator does not use Telnet for management purposes, the following commands sets the vty port to only accept ssh connections **[6] [12]**.

line vty 0 10

transport input ssh

SSHv2 must be used to secure the trusted path for remote administration for all SSHv2 sessions. To enable sshv2, use the "**ip ssh version 2**" command **[6]** Commands D to L -> ip source-track through ivrf -> ip ssh version.

Note before SSH is configured, the rsa keys need to be generated for the SSH server using the following command:

crypto key generate rsa with an RSA key size of **2048 bits [6]** Commands A to C -> crypto isakmp aggressive-mode disable -> crypto key generate.

RSA keys are generated in pairs—one public RSA key and one private RSA key. This command is not saved in the router configuration; however, the RSA keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device) the next time the configuration is written to NVRAM.

Only one set of keys can be configured using the **crypto key generate** command at a time. Repeating the command overwrites the old keys.

If the configuration is not saved to NVRAM with a "**copy run start**", the generated keys are lost on the next reload of the router.

If the error "% Please define a domain-name first" is received, enter the command '**ip domain-name [domain name]**'.

SSH must be configured to require use of as a minimum, Diffie-Hellmann group 14. IOS allows the required DH groups to be specified by their modulus size. The default is modulus 1024 (DH Group 1). To require use of DH Group 14, specify a minimum modulus size of 2048 using the following command **[12]** or **[6]** Commands D to L -> ip source-track through ivrf:

ip ssh dh min size 2048

In addition, configure your ssh client for dh-group-14, in Putty, configure the SSH client to support only diffie-hellman-group14-sha1 key exchange. To configure Putty, do the following:

- Go into Putty Configuration Select > Connection > SSH > Kex;
- Under Algorithm selection policy: move Diffie-Hellman group 14 to the top of the list;
- Move the "warn below here" option to right below DH group14

When SSHv2 is enabled the TOE can be configured to limit the algorithms and ciphers that can be used for the secure SSH connection.

To secure and control SSH sessions, the evaluated configuration requires SSHv2 session to only use AES-CBC-128 and AES-CBC-256 encryption key algorithms. To set, use the following command **[12]** How to Configure SSH Algorithms for Common Criteria Certification -> Configuring an Encryption Key Algorithm for a Cisco IOS SSH Server and Client:

ip ssh server algorithm encryption aes128-cbc aes256-cbc

The TOE also needs to be configured to only support hmac-sha1 and hmac-sha1-96 MAC algorithms using the following command **[12]** How to Configure SSH Algorithms for Common Criteria Certification -> Configuring a MAC Algorithm for a Cisco IOS SSH Server and Client:

ip ssh server algorithm mac hmac-sha1 hmac-sha1-96

To secure and control SSH sessions, the evaluated configuration requires that the SSHv2 session timeout period and maximum number of failed login attempts to be set. This is done by using the following command:

ip ssh timeout <seconds> (note in the evaluated configuration this is set to 120 seconds. The default and maximum is 120 seconds) **[6]**. Commands D to L -> ip source-track through ivrf (with the parameters listed above) and **[12]**

ip ssh authentication-retries <integer> (note in the evaluated configuration is limited to 3. The default is 3, with a maximum of 5) **[6]**. Commands D to L -> ip source-track through ivrf (with the parameters listed above) and **[12]**

The evaluated configuration also requires the TOE to re-key of no longer than one hour and no more than one gigabyte of transmitted data. This can be initiated by the client of by issuing the following command **[6]** and **[12]**

ip ssh rekey { **time** *time* | **volume** *volume* }

To verify the proper encryption algorithms are used for established SSHv2 connections; use the "**show ssh sessions**" command **[6]**. To disconnect SSH sessions, use the **ssh disconnect** command **[6]**.

The TOE acting as the SSH server supports three types of user authentication methods and sends these authentication methods to the SSH client in the following predefined order:

- Public-key authentication method
- Keyboard-interactive authentication method (note this method is not included nor allowed in the evaluated configuration and must be disabled using the following command **no ip ssh server authenticate user keyboard**
- Password authentication method

By default, all the user authentication methods are enabled. Use the **no ip ssh server authenticate user {publickey | keyboard | pasword }** command to disable any specific user authentication method so that the disabled method is not negotiated in the SSH user authentication protocol. This feature helps the SSH server offer any preferred user authentication method in an order different from the predefined order. The disabled user authentication method can be enabled using **the ip ssh server authenticate user {publickey | keyboard | pasword }** command. Refer to Secure Shell -> Configuring User Authentication Methods **[12]**.

In addition, the following configurations also need to be set for the excluded functionality.

HTTP server was not evaluated and must be disabled **[6]**

no ip http server [6]

HTTPS server was not evaluated and must be disabled **[6]**

no ip http secure-server

SNMP server was not evaluated and must be disabled **[6]** and **[5]** select Configuring SNMP

no snmp-server

Smart Install was not evaluated and must be disabled by issuing the following command **[6]**

hostname(config)# no vstack

3.3.2 Authentication Server Protocols

RADIUS (outbound) for authentication of TOE administrators to remote authentication servers is disabled by default but can be enabled by administrators in the evaluated configuration. Use best practice for selection and protection of a key to ensure that the key is not easily guessable and is not shared with unauthorized users.

For further information about configuring RADIUS, refer to Securing User Services Overview -> Security Server Protocols -> RADUIS / Securing User Services Overview -> Securing User Services Overview -> RADIUS Attributes **[4(a)],** Cisco IOS Security Command Reference: Commands M to R -> radius attributes nas-port-type through rd -> radius server **[6]** or Configuring Switch-Based Authentication -> Controlling Switch Access with (selecting RADIUS) **[5]**.

It is recommended to read the referenced sections to become familiar with remote authentication concepts prior to configuration.

If using RADIUS for remote authentication, the connection must be secured using IPsec. See IPsec Overview, Configuration of IPsec and Session Protection in this document.

3.3.3 Routing Protocols

As noted above, The TOE provides MD5 hashing for authentication of neighbor switches via EIGRP, EIGRPv6 for IPv6, PIMv2, PIM-SMv2, PIM-SSMv2, OSPFv2, OSPFv3 for IPv6, RIP for IPv6, and RIPv2 with shared passwords. The hash mechanism is implemented as specified in MD5 RFC 1321 and applied as specified in the related routing protocol RFCs and EIGRP (Cisco proprietary).

Routing tables can be created and maintained manually using static routes configured by the administrator. Use of routing protocols is not required to support or enforce any TOE security functionality including filtering of IPv6 traffic.

The routing protocols are used to maintain routing tables, though with any of the IP routing protocols, you must create the routing process, associate networks with the routing process, and customize the routing protocol for your particular network. You will need to perform some combination of the tasks before routing activities can begin, such as specifying interior (routing networks that are under a common network administration) and exterior (used to exchange routing information between networks that do not share a common administration) gateway protocols. There are other routing configurations such as multiple routing protocols in a single router to connect networks that use different routing protocols, however by default the internal and external (if applicable) need to be configured. Refer to the applicable sections in **[8]** for configuration of the routing protocol.

Note: When operating the TOE in accordance with the FIPS Security Policy, use of MD5 is not permitted, so neighbor router authentication would not be permitted unless the routing protocols are being transmitted through one or more IPsec tunnels.

3.3.4 MACSEC and MKA Configuration

The TOE authenticates and encrypts packets between itself and a MACsec peer. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys to protect data exchanged by the peers

By default, MACsec is disabled and there are no MKA policies are configured on the Cat 3K Series TOE. Following is an example of an MKA policy:

Switch(config)# **mka policy mka_policy**

Switch(config-mka-policy)# **key-server priority 200**

Switch(config-mka-policy)# **macsec-cipher-suite gcm-aes-128**

Switch(config-mka-policy)# **confidentiality-offset 30**

Switch(config-mka-policy)# **end**

The detailed steps to configure MACsec and MKA policy on interfaces are listed in **[3]**.

3.3.5 X.509 Certificates

The TOE may be configured by the privileged administrators to use X.509v3 certificates to authenticate IPsec peers. RSA certificates are supported.

Creation of these certificates and loading them on the TOE is covered in **[14]**, and a portion of the TOE configuration for use of these certificates follows below.

3.3.5.1 Creation of the Certificate Signing Request

The certificate signing request for the TOE will be created using the RSA key pair and the domain name configured in Section 3.3.1 above.

In order for a certificate signing request to be generated, the TOE must be configured with a hostname, trustpoint, enrollment method and revocation checking. This is done by using the following commands **[6]**:

- To specify the hostname for the peer in the IKE keyring exchange, use the **hostname** *name* in configuration mode

  Hostname <**name**>

  Where the <**name**> is the name of the peer (**hostname catTOE**)

- To declare the trustpoint that the TOE should use, use the **crypto pki trustpoint** *name* command in configuration mode

  crypto pki trustpoint <**name**>

  Where the <**name**> creates the name of the trustpoint (**crypto pki trustpoint ciscotest**)

- To specify the enrollment parameters of a certification authority (CA), use the enrollment [terminal or url] command in ca-trustpoint configuration mode

  enrollment url <**url**>

  Where the <**url**> specifies the URL of the file system where the TOE should send certificate requests (**enrollment url http://192.168.2.137:80**)

- To specify the subject name settings in the certificate request, use the subject-name command in ca-trustpoint configuration mode.

  subject-name <**x.500-name**>

  Where the <**x.500-name**> specifies the subject name used in the certificate request. If the <**x.500-name**> argument is not specified, the fully qualified domain name (FQDN), which is the default subject name, will be used (**subject-name CN=catTOE.cisco.com,OU=TAC**)

- All of the certificates include at least the following information:

  public key and (Common Name, Organization, Organizational Unit, Country) <**subject-name**> **CN=catTOE.cisco.com,O=cisco,OU=TAC,C=U**

- To specify the revocation check method, use the revocation-check command in ca-trustpool configuration mode.

  revocation-check <method1> [*method2 method3*]

  Where the **<method1>** specifies the method used by the TOE to check the revocation status of the certificate. Available methods are identified by the following keywords:

  - crl--Certificate checking is performed by a certificate revocation list (CRL). This is the default behavior.
  - ocsp--Certificate checking is performed by an online certificate status protocol (OCSP) server.

  If a second and third method is specified, each method is used only if the previous method returns an error, such as a server being down.

- To create the certificate signing request, use the crypto pki enroll command in global configuration mode.

  crypto pki enroll <name>

  Where **<name>** is the CA that was set above using the **crypto pki trustpoint** command (**crypto pki enroll ciscotest**)

3.3.5.2 Securely Connecting to a Certificate Authority for Certificate Signing

The TOE must communicate with the CA for Certificate Signing over IPSEC. This authentication will use pre-shared keys.

Following are sample instructions to configure the TOE to support an IPSec tunnel with aes encryption, with 10.10.10.102 as the IPSec peer IP on the CA, 10.10.10.110 as the local TOE IP.

TOE-common-criteria#**configure terminal**

TOE-common-criteria(config)#**crypto isakmp policy 1**

TOE-common-criteria(config-isakmp)#**encryption aes**

TOE-common-criteria(config-isakmp)#**authentication pre-share**

TOE-common-criteria(config-isakmp)#**group 14**

TOE-common-criteria(config-isakmp)#**lifetime 86400**

TOE-common-criteria(config)#**crypto isakmp key** [*insert 22 character preshared key*] **address 10.10.10.101**

TOE-common-criteria(config)#**crypto ipsec transform-set sampleset esp-aes esp-sha-hmac**

TOE-common-criteria(cfg-crypto-trans)#**mode tunnel**

TOE-common-criteria(config)#**crypto map sample 19 ipsec-isakmp**

TOE-common-criteria(config-crypto-map)#**set peer 10.10.10.102**

TOE-common-criteria(config-crypto-map)#**set transform-set sampleset**

TOE-common-criteria(config-crypto-map)#**set pfs group14**

TOE-common-criteria(config-crypto-map)#**match address 170**

TOE-common-criteria(config-crypto-map)#**exi**t

TOE-common-criteria(config)#**interface g0/0**

TOE-common-criteria(config-if)#**ip address 10.10.10.110 255.255.255.0**

TOE-common-criteria(config-if)#**crypto map sample**

TOE-common-criteria(config-if)#**exit**

TOE-common-criteria(config)#**access-list 170 permit ip 10.10.10.0 0.255.255.255 10.10.10.0 0.255.255.255**

3.3.5.3 Authenticating the Certificate Authority

The TOE must authenticate the CA by acknowledging its attributes match the publicly posted fingerprint.

- To authenticate the certification authority (by getting the certificate of the CA), use the crypto ca authenticate command in global configuration mode.

  crypto ca authenticate <**trustpoint-name**>

  Where <**trustpoint-name**> specifies the name of the CA that was set above using the **crypto pki trustpoint** command (**crypto ca authenticate ciscotest**)

The TOE administrator must verify that the output of the command below matches the fingerprint of the CA on its public site.

Device (config)#**crypto ca authenticate ciscotest**

Certificate has the following attributes:

Fingerprint MD5: 8DE88FE5 78FF27DF 97BA7CCA 57DC1217

Fingerprint SHA1: 271E80EC 30304CC1 624EEE32 99F43AF8 DB9D0280

% Do you accept this certificate? [yes/no]: **yes**

Trustpoint CA certificate accepted.

3.3.5.4 Storing Certificates to a Local Storage Location

Certificates are stored to NVRAM by default; however, some switches do not have the required amount of NVRAM to successfully store certificates. All Cisco platforms support NVRAM and flash local storage. Depending on the platform, an authorized administrator may have other supported local storage options including bootflash, slot, disk, USB flash, or USB token. During run time, an authorized administrator can specify what active local storage device will be used to store certificates. For more detailed information see the *Public Key Infrastructure Configuration Guide* Guidance document **[15]** section "How to Configure PKI Storage."

3.3.5.5 How to Specify a Local Storage Location for Certificates

The summary steps for storing certificates locally to the TOE are as follows:

1. Enter configure terminal mode:

   TOE-common-criteria# **configure terminal**

2. Specify the local storage location for certificates: **crypto pki certificate storage *location-name***

   Device(config)# **crypto pki certificate storage flash:/certs**

3. Exit:

   Device(config)# **exit**

4. Save the changes made:

   Device# **copy system:running-config nvram:startup-config**

5. Display the current setting for the PKI certificate storage location:

   Device# **show crypto pki certificates storage**

The following is sample output from the show crypto pki certificates storage command, which shows that the certificates are stored in the certs subdirectory of disk0:

```
Device# show crypto pki certificates storage
Certificates will be stored in disk0:/certs/
```

The authorized administrator can also configure one or more certificate fields together with their matching criteria to match. Such as:

- alt-subject-name
- expires-on
- issuer-name
- name
- serial-number
- subject-name
- unstructured-subject-name
- valid-start

This allows for installing more than one certificate from one or more CAs on the TOE. For example, one certificate from one CA could be used for SSH connections, while another certificate from another CA could be used for IPsec connections. However the default configuration is a single certificate from one CA that is used for all authenticated connections.

3.3.5.6 Configuring a Revocation Mechanism for PKI Certificate Status Checking

Perform this task to set up the certificate revocation mechanism CRLs or OCSP--that is used to check the status of certificates in a PKI.

Use the **revocation-check** command to specify at least one method (OCSP, CRL) that is to be used to ensure that the certificate of a peer has not been revoked. For multiple methods, the order in which the methods are applied is determined by the order specified via this command.

If the TOE does not have the applicable CRL and is unable to obtain one, or if the OCSP server returns an error, the TOE will reject the peer's certificate, however the response will allow the Authorized Administrator to continue with the connection if they deem, they can trust the certificate or to not continue with the connection.

When using OCSP, nonces, unique identifiers for OCSP requests, are sent by default during peer communications with an OCSP server. The use of nonces offers a more secure and reliable communication channel between the peer and OCSP server. If the OCSP server does not support nonces, an authorized administrator may disable the sending of nonces.

3.3.5.7 Manually Overriding the OCSP Server Setting in a Certificate

Administrators can override the OCSP server setting specified in the Authority Information Access (AIA) field of the client certificate or set by the issuing the **ocsp url** command. One or more OCSP servers may be manually specified, either per client certificate or per group of client certificates by the match certificate override ocsp command. The match certificate override ocsp command overrides the client certificate AIA field or the ocsp url command setting if a client certificate is successfully matched to a certificate map during the revocation check

3.3.5.8 Configuring Certificate Chain Validation

Perform this task to configure the processing level for the certificate chain path of peer certificates.

Prerequisites:

- The device must be enrolled in your PKI hierarchy.
- The appropriate key pair must be associated with the certificate.

1. Enter configure terminal mode:

   TOE-common-criteria# **configure terminal**

2. Set the crypto pki trustpoint name:

TOE-common-criteria(config)# **crypto pki trustpoint ca-sub1**

3. Configure the level to which a certificate chain is processed on all certificates including subordinate CA certificates using **the chain-validation [{stop | continue} [parent-trustpoint]] command**:

   TOE-common-criteria(ca-trustpoint)# **chain-validation continue ca-sub1**

   - Use the **stop** keyword to specify that the certificate is already trusted. This is the default setting.
   - Use the **continue** keyword to specify that the subordinate CA certificate associated with the trustpoint must be validated.
   - The **parent-trustpoint** argument specifies the name of the parent trustpoint the certificate must be validated against.

   A trustpoint associated with the root CA cannot be configured to be validated to the next level. The **chain-validation** command is configured with the continue keyword for the trust point associated with the root CA, an error message will be displayed and the chain validation will revert to the default **chain-validation** command setting.

4. Exit:

   TOE-common-criteria(ca-trustpoint)# **exit**

3.3.5.9 Setting X.509 for use with IKE

Once X.509v3 keys are installed on the TOE, they can be set for use with IKEv1 with the commands:

TOE-common-criteria (config)# **crypto isakmp policy 1**

TOE-common-criteria (config-isakmp)# **authentication rsa-sig**

If an invalid certificate is loaded, authentication will not succeed.

3.3.6 IPsec Overview

The TOE allows all privileged administrators to configure Internet Key Exchange (IKE) and IPsec policies. IPsec provides the following network security services:

- Data confidentiality--The IPsec sender can encrypt packets before transmitting them across a network.
- Data integrity--The IPsec receiver can authenticate packets sent by the IPsec sender to ensure that the data has not been altered during transmission.
- Data origin authentication--The IPsec receiver can authenticate the source of the sent IPsec packets. This service is dependent upon the data integrity service.
- Anti-replay--The IPsec receiver can detect and reject replayed packets.

IPsec provides secure tunnels between two peers, such as two switches. The privileged administrator defines which packets are considered sensitive and should be sent through these secure tunnels and specifies the parameters that should be used to protect these sensitive packets by specifying the characteristics of these tunnels. When the IPsec peer

recognizes a sensitive packet, the peer sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer.

More accurately, these tunnels are sets of security associations (SAs) that are established between two IPsec peers. The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used by the two peers. SAs are unidirectional and are established per security protocol (AH or ESP).

With IPsec, privileged administrators can define the traffic that needs to be protected between two IPsec peers by configuring access lists and applying these access lists to interfaces using crypto map sets. Therefore, traffic may be selected on the basis of the source and destination address, and optionally the Layer 4 protocol and port. (The access lists used for IPsec are only used to determine the traffic that needs to be protected by IPsec, not the traffic that should be blocked or permitted through the interface. Separate access lists define blocking and permitting at the interface.)

A crypto map set can contain multiple entries, each with a different access list. The crypto map entries are searched in a sequence--the router attempts to match the packet to the access list specified in that entry, for example:

- The ‘discard’ option is accomplished using access lists with deny entries, which are applied to interfaces within access-groups.
- The ‘bypassing’ option is accomplished using access lists with deny entries, which are applied to interfaces within crypto maps for IPSec.
- The ‘protecting’ option is accomplished using access lists with permit entries, which are applied to interfaces within crypto maps for IPsec.

When a packet matches a permit entry in a particular access list, and the corresponding crypto map entry is tagged as cisco, connections are established, if necessary. If the crypto map entry is tagged as ipsec-isakmp, IPsec is triggered. If there is no SA that the IPsec can use to protect this traffic to the peer, IPsec uses IKE to negotiate with the remote peer to set up the necessary IPsec SAs on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry.

Once established, the set of SAs (outbound to the peer) is then applied to the triggering packet and to subsequent applicable packets as those packets exit the router. "Applicable" packets are packets that match the same access list criteria that the original packet matched. For example, all applicable packets could be encrypted before being forwarded to the remote peer. The corresponding inbound SAs are used when processing the incoming traffic from that peer.

Access lists associated with IPsec crypto map entries also represent the traffic that the router needs protected by IPsec. Inbound traffic is processed against crypto map entries--if an unprotected packet matches a permit entry in a particular access list associated with an IPsec crypto map entry, that packet is dropped because it was not sent as an IPsec-protected packet.

Crypto map entries also include transform sets. A transform set is an acceptable combination of security protocols, algorithms, and other settings that can be applied to

IPsec-protected traffic. During the IPsec SA negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

3.3.7 Configuration of IPsec

IPsec tunnels must be used for remote administration, transmission of audit records, and whenever connecting to AAA servers (RADIUS). If an IPsec tunnel terminates in a router (rather than a syslog or RADIUS attached to that router) then the connection from the server to the router has to be physically secure. Refer to **[9]** for detailed guidance to configure IPsec tunnels. To ensure the IPsec tunnels will be consistent with the evaluated configuration, use parameters as described in this section. Configuring IPsec tunnels requires configuration of the following elements:

- **Layer-3 Interfaces:** IP-enabled interfaces that can be local tunnel endpoints.
- **Crypto Access Lists:** Any access lists that will be applied to Crypto Maps.
- **Crypto Maps:** An association of a crypto access list (a "match address"), one or more IPsec peers (accessible from a valid local layer-3 interface), and with one or more transforms or transform sets.
- **IKEv1 Transforms:** Administratively-specified parameters to be permitted during IKE SA negotiation (see tables below for permitted parameters).
- **IKEv1 Transform Sets:** Administratively named sets of IKEv1 Transforms that can be applied within crypto maps instead of assigning parameters individually.
- **IPsec Transforms:** Administratively-specified parameters to be permitted during IPsec SA negotiation (see tables below for permitted parameters).

3.3.7.1 Configuration Reference Identifier

Certificate maps provide the ability for a certificate to be matched with a given set of criteria. You can specify which fields within a certificate should be checked and which values those fields may or may not have. There are six logical tests for comparing the field with the value: equal, not equal, contains, does not contain, less than, and greater than or equal. ISAKMP and ikev2 profiles can bind themselves to certificate maps, and the TOE will determine if they are valid during IKE authentication.

Table 9 Reference Identifier Configuration

Step	Command	Results
Step1	(config)# **crypto pki certificate map** *label sequence-number*	Starts certificate-map mode
Step2	*(ca-certificate-map)# field-name match-criteria match-value*	In ca-certificate-map mode, you specify one or more certificate fields together with their matching criteria and the value to match. • *field-name*—Specifies one of the following case-insensitive name strings or a date: –subject-name –issuer-name

Step	Command	Results
		–unstructured-subject-name –alt-subject-name –name –valid-start –expires-on Note Date field format is dd mm yyyy hh:mm:ss or mm dd yyyy hh:mm:ss. • *match-criteria*—Specifies one of the following logical operators: –eq—Equal (valid for name and date fields) –ne—Not equal (valid for name and date fields) –co—Contains (valid only for name fields) –nc—Does not contain (valid only for name fields) –lt —Less than (valid only for date fields) –ge —Greater than or equal (valid only for date fields) • *match-value*—Specifies the name or date to test with the logical operator assigned by match-criteria.
Step3	(ca-certificate-map)# **exit**	Exits ca-certificate-map mode.
Step4	For IKEv1: crypto isakmp profile ikev1-profile1 match certificate *label* For IKEv2: crypto ikev2 profile ikev2-profile1 match certificate *label*	Associates the certificate-based ACL defined with the crypto pki certificate map command to the profile.

For example: To create a certificate map for IKEv1 to match four subject-name values of the peer enter:

```
# conf t
(config)# crypto pki certificate map cert-map-match-all 99
(ca-certificate-map)# subject-name co cn=CC_PEER
(ca-certificate-map)# subject-name co o=ACME
(ca-certificate-map)# subject-name co ou=North America
(ca-certificate-map)# subject-name co c=US
(ca-certificate-map)#exit
(config)# crypto isakmp profile ike1-profile-match-cert
```

(conf-isa-prof)# match certificate cert-map-match-all

3.3.7.2 IKEv1 Transform Sets

An Internet Key Exchange version 1 (IKEv1) transform set represents a certain combination of security protocols and algorithms. During the IPsec SA negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

Privileged administrators can specify multiple transform sets and then specify one or more of these transform sets in a crypto map entry. The transform set defined in the crypto map entry is used in the IPsec SA negotiation to protect the data flows specified by that crypto map entry's access list.

During IPsec security association negotiations with IKE, peers search for a transform set that is the same at both peers. When such a transform set is found, it is selected and applied to the protected traffic as part of both peers' IPsec SAs. (With manually established SAs, there is no negotiation with the peer, so both sides must specify the same transform set.)

Note: If a transform set definition is changed during operation that the change is not applied to existing security associations but is used in subsequent negotiations to establish new SAs. If you want the new settings to take effect sooner, you can clear all or part of the SA database by using the **clear crypto sa command [6] [9]**.

The following settings must be set in configuring the IPSec with IKEv1 functionality for the TOE **[6] [9]**:

Switch# **conf t**

Switch(config)#**crypto isakmp policy 1**

Switch(config-isakmp)#**hash sha**

Switch(config-isakmp)#**encryption aes**

This configures IPSec IKEv1 to use AES-CBC-128 for payload encryption. AES-CBC-256 can be selected with '**encryption aes 256**'.

The authorized administrator must ensure that the keysize for this setting is greater than or equal to the keysize selected for ESP in Section 4.6.2 below. If AES 128 is selected here, then the highest keysize that can be selected on the TOE for ESP is AES 128 (CBC).

Both confidentiality and integrity are configured with the hash sha and encryption aes commands respectively. As a result, confidentiality-only mode is disabled.

Switch(config-isakmp)#**authentication pre-share**

This configures IPSec to use pre-shared keys.

Switch(config-isakmp)#**exit**

Switch(config)#**crypto isakmp key cisco123!cisco123!CISC address 11.1.1.4**

Pre-shared keys on the TOE must be at least 22 characters in length and can be composed of any combination of upper and lower case letters, numbers,

and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")").

The TOE supports pre-shared keys up to 128 bytes in length. While longer keys increase the difficulty of brute-force attacks, longer keys increase processing time.

Switch(config-isakmp)#**group 14**

This selects DH Group 14 (2048-bit MODP) for IKE

Switch(config-isakmp)#**lifetime 86400**

The default time value for Phase 1 SAs is 24 hours (86400 seconds), but this setting can be changed using the command above with different values.

Switch(config-isakmp)#**crypto isakmp aggressive-mode disable**

Main mode is the default mode and the **crypto isakmp aggressive-mode disable** ensures all IKEv1 Phase 1 exchanges will be handled in the default main mode.

TOE-common-criteria(config-isakmp)#**exit**

3.3.7.3 IKEv2 Transform Sets

An Internet Key Exchange version 2 (IKEv2) proposal is a set of transforms used in the negotiation of IKEv2 SA as part of the IKE_SA_INIT exchange. An IKEv2 proposal is regarded as complete only when it has at least an encryption algorithm, an integrity algorithm, and a Diffie-Hellman (DH) group configured. If no proposal is configured and attached to an IKEv2 policy, then the default proposal is used in the negotiation, and it contains selections that are not valid for the TOE. Thus, the following settings must be set in configuring the IPSec with IKEv2 functionality for the TOE:

Switch#**conf t**

Switch(config)#**crypto ikev2 proposal sample**

Switch(config-ikev2-proposal)#**integrity sha1**

Switch(config-ikev2-proposal)#**encryption aes-cbc-128**

This configures IPSec IKEv2 to use AES-CBC-128 for payload encryption. AES-CBC-256 can be selected with '**encryption aes-cbc-256**'.

The authorized administrator must ensure that the keysize for this setting is greater than or equal to the keysize selected for ESP in Section 4.6.2 below. If AES 128 is selected here, then the highest keysize that can be selected on the TOE for ESP is AES 128 (either CBC).

Both confidentiality and integrity are configured with the hash sha and encryption aes commands respectively. As a result, confidentiality-only mode is disabled.

Switch(config-ikev2-proposal)#**group 14**

This selects DH Group 14 (2048-bit MODP) for IKE

Switch(config-ikev2-proposal)#**lifetime 86400**

The default time value for Phase 1 SAs is 24 hours (86400 seconds), but this setting can be changed using the command above with different values.

Switch(config)#**crypto ikev2 keyring keyring-1**

Switch(config-ikev2-keyring)#**peer peer1**

Switch(config-ikev2-keyring-peer)#**address 0.0.0.0 0.0.0.0**

Switch(config-ikev2-keyring-peer)#**pre-shared-key cisco123!cisco123!CISC**

This section creates a keyring to hold the pre-shared keys referenced in the steps above. In IKEv2 these pre-shared keys are specific to the peer.

Pre-shared keys on the TOE must be at least 22 characters in length and can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")").

The TOE supports pre-shared keys up to 128 bytes in length. While longer keys increase the difficulty of brute-force attacks, longer keys increase processing time.

HEX keys generated off system can also be input for IKEv2 using the following instead of the pre-shared-key command above: '**pre-shared-key hex [hex key]**'. For example: **pre-shared-key hex 0x6A6B6C**, refer to **[9]** for more information on this command.

This configures IPSec to use pre-shared keys. X.509 v3 certificates are also supported for authentication of IPSec peers. See Section 4.6.3 below for additional information.

Switch(config)#**crypto logging ikev2**

This setting enables IKEv2 syslog messages.

The configuration above is not a complete IKE v2 configuration, and that additional settings will be needed. See [18] Configuring Internet Key Exchange Version 2 (IKEv2) for additional information on IKE v2 configuration.

3.3.7.4 IPsec Transform and Lifetimes

Regardless of the IKE version selected, the TOE must be configured with the proper transform for IPsec ESP encryption and integrity as well as IPsec lifetimes.

To configure IPsec ESP to use HMAC-SHA-1 and AES-CBC-128 use the following command:

crypto ipsec transform-set example esp-aes 128 esp-sha-hmac

To configure IPsec ESP to the other allowed algorithms the following command:

crypto ipsec transform-set example esp-aes 256 esp-sha-hmac-256

or

crypto ipsec transform-set example esp-aes 512 esp-sha-hmac-512

The default time value for Phase 2 SAs is 1 hour. There is no configuration required for this setting since the default is acceptable, however to change the setting to 8 hours as claimed in the Security Target the "**crypto ipsec security-association lifetime"** command can be used as specified below:

crypto ipsec security-association lifetime seconds 28800

The following command configures a lifetime of 100 MB of traffic for Phase 2 SAs. The default amount for this setting is 2560KB, which is the minimum configurable value for this command. The maximum configurable value for this command is 4GB. Therefore the security association lifetime range is 2560KB - 4GB (100,000 to 4,000,000 Kilobytes)

crypto ipsec security-association lifetime kilobytes 100000

Additional information regarding configuration of IPsec can be found in the **[8]**. The IPSEC commands are also dispersed within the Security Command References **[5] [6]**.

This functionality is available to the Privileged Administrator. Configuration of VPN settings is restricted to the privileged administrator.

3.3.7.5 Main Mode vs. Aggressive Mode for IKEv1

By default the IOS action will initiate IKE authentication (rsasig, rsa-encr, or preshared) negotiations in main mode. Do not configure IKE to initiate using aggressive mode. If the device has been configured with the crypto isakmp peer address and the "set aggressive-mode password" or "set aggressive-mode client-endpoint" commands the device will initiate aggressive mode. Do not use those commands or the "initiate mode aggressive" command.

To block all Internet Security Association and Key Management Protocol (ISAKMP) aggressive mode requests to and from a device, use the command "**crypto isakmp aggressive-mode disable**" **[6]** Cisco IOS Security Command Reference: Commands A to C, command in global configuration mode. If this command is not configured, Cisco IOS software will attempt to process all incoming ISAKMP aggressive mode security association (SA) connections.

3.3.7.6 Using Pre-Shared Keys for Authentication

When using pre-shared keys to secure IPsec tunnels, the keys must be entered by an administrator via the CLI. If the remote VPN peer is not administered by the same people, the preshared keys must be exchanged securely, ensuring the keys are never stored or transmitted in unencrypted form. Pre-shared keys can be composed of any combination of upper and lower case letters, numbers, and special characters (including: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")"). Pre-shared keys can be up to 128 characters, with a recommended minimum length of 22 characters from all character sets. The password complexity is not automatically enforced by the TOE and must be mandated in a policy.

Crypto isakmp key {enc-type-digit | keystring} address {peer-address} [6]

To ensure the preshared key is stored in encrypted form (AES encrypted) in the configuration file, enable the storing of encrypted keys:

key config-key password-encryption [text] [6] Cisco IOS Security Command Reference: Commands D to L -> K through L -> key config-key password-encryption

password encryption aes [6] Cisco IOS Security Command Reference: Commands M to R -> pac key through port-misue -> password encryption aes

- If an encryption key is not present, you will be prompted for the following: New key and Confirm key.
- If an encrypted key already exists, you will be prompted for the following: Old key, New key, and Confirm key.
- If you want to remove the password that is already encrypted, you will see the following prompt: "WARNING: All type 6 encrypted keys will become unusable. Continue with master key deletion? [yes/no]:".

To set the key for a tunnel, use the following command after configuring that tunnel to authenticate using a pre-shared key instead of RSA:

crypto isakmp key <*enc-type-digit*> <*keystring*>

To enter the keystring in encrypted form (AES encrypted), specify 6 as the enc-type-digit. **[6]** Cisco IOS Security Command Reference: Commands A to C -> crypto isakmp aggressive-mode disable -> crypto isakmp key (with parameters as noted above).

3.3.7.7 Tunnel Mode vs. Transport Mode

Tunnel mode is the default mode for all IKE connections. The mode setting is applicable only to traffic whose source and destination addresses are the IPsec peer addresses; the mode setting is ignored for all other traffic. This mode ensures secure connectivity between the TOE and the authorized remote entity (i.e. syslog server).

Tunnel mode can be specified with the following command in crypto ipsec transform set mode:

mode tunnel

However in the evaluated configuration transport mode is required. Transport mode provides end-to-end communications between a client and server.

Transport mode can be specified with the following command in crypto ipsec transform set mode:

mode transport

3.3.7.8 IKEv1 and IKEv2 Parameters Permitted in the Evaluated Configuration

Following are the allowed parameters for IKEv1 and IKEv2.

Table 10 IKEv1 and IKEv2 Parameters in the Evaluated Configuration

IKEv1 and IKEv2 Transform Types	IKEv1 and IKEv2 Transform Options	Permitted in the Evaluated Configuration	Required in the Evaluated Configuration
Authentication	rsa-sig (default) (RSA signature) rsa-encr (RSA encrypted nonces) pre-share	rsa-sig (default) (RSA signature) pre-share	Yes.
Encryption	des (default) 3des aes 128 aes 256	 aes 128 aes 256	Yes.
Group	1, 2, 5, 14, 15, 16, 19, 20, 24	14	Yes.
Hash	sha (default sha 1) sha256 sha512	sha (default sha 1) sha256 sha512	Yes.
Lifetime	number of seconds	Yes.	Any time limit is acceptable. The recommended limit for IKEv1 and IKEv2 SA (IKE Phase 1 SA) lifetimes is 24 hours (86,400 seconds).

Following are the allowable IPsec parameters.

Table 11 IPsec Parameters Permitted in the Evaluated Configuration

IPsec Transform Types	IPsec Transform Options	Permitted in the Evaluated Configuration	Required in the Evaluated Configuration
AH Transform	ah-md5-hmac ah-sha-hmac	No	No. Use of AH is irrelevant to evaluated security functionality.

IPsec Transform Types	IPsec Transform Options	Permitted in the Evaluated Configuration	Required in the Evaluated Configuration
ESP Encryption Transform	esp-3des esp-aes esp-des esp-null esp-seal	esp-aes	Yes. AES must be used in the evaluated configuration.
ESP Authentication Transform	esp-md5-hmac esp-sha-hmac	esp-sha-hmac	Yes. Not specifying an ESP Authentication Transform would equate to using ESP in "confidentiality only" mode, which is not permitted in the evaluated configuration.
IP Compression Transform	comp-lzs	Yes.	No.
Mode	tunnel (default) transport	Yes.	Tunnel mode is always preferred.
Lifetime	Seconds and/or kilobytes	Yes.	IPsec SAs (IKEv1 and IKEv2 Phase 2 SAs) can be restricted within the range of 2560KB - 4GB (100,000 to 4,000,000 Kilobytes). The recommended time limit for IKEv1 and IKEv2 Phase 2 SAs is no more than 8 hours (28,800 seconds).

3.3.8 Session Protection

TOE communications with the AAA server (RADIUS) and the syslog server must be secured using IPsec. If an authorized administrator wants to authenticate using a RADIUS server, then the session between the TOE and AAA server must be protected to ensure the authentication data is not passed in the clear. If an authorized administrator wants to back-up the audit logs to a syslog server, then protection must be provided for the syslog server communications so that audit data is protected.

This session protection can be provided in one of two ways:

1. With a syslog/AAA server acting as an IPsec peer of the TOE and the records tunneled over that connection, or

2. With a syslog/AAA server that is not an IPsec peer of the TOE, but is physically co-located with an IPsec peer of the TOE within a trusted facility, and the records are tunneled over the connection to that IPsec peer.

The syslog/AAA servers will need to act as an IPsec peer or as an IPsec endpoint where there would be a direct connection from the TOE to the syslog/AAA servers.

If the syslog/AAA server is not capable of acting as an IPsec peer or as an IPsec endpoint, then the syslog/AAA server must be located in a physically protected facility and connected to a router capable of establishing an IPsec tunnel with the TOE.

3.3.8.1 Syslog Server Running on an IPsec Endpoint

For deployments where the syslog/AAA server is able to operate as an IPsec peer of the TOE, the IPsec tunnel will protect events as they are sent to the server. Examples of free VPN endpoint products that can be installed on a syslog server to allow it to be an IPsec peer include the Racoon tool that is part of the IPsec Tools on many Linux systems, strongSwan, Openswan, FreeS/WAN, Social VPN, tcpcrypt, tinc and Cloudvpn.

Following are sample instructions to configure the TOE to support an IPsec tunnel with aes encryption, with 10.10.10.101 as the IPsec peer IP on the syslog server, 10.10.10.110 and 30.0.0.1 as the local TOE IPs, and the syslog server running on 40.0.0.1 (a separate interface on the syslog server). For the following commands see the **[6]**.

Changes to the IP addressing scheme and routing policies may need to be changed to support the organization network.

Switch#**configure terminal**
Switch(config)#**crypto isakmp policy 1**
Switch(config)#**encryption aes**
Switch(config)#**authentication pre-share**
Switch(config)#**group 14**
Switch(config)#**lifetime 86400**
Switch(config)#**crypto isakmp key {*keystring*} address 10.10.10.101**
Switch(config)#**crypto isakmp key {*keystring*} address 40.0.0.1**
Switch(config)#**crypto ipsec transform-set sampleset esp-aes esp-sha-hmac**
Switch(config)#**mode tunnel**
Switch(config)#**crypto map sample 19 ipsec-isakmp**
Switch(config-crypto-map)#**set peer 10.10.10.101**
Switch (config-crypto-map)#**set transform-set sampleset**
Switch (config-crypto-map)#**set pfs group14**
Switch (config-crypto-map)#**match address 170**
Switch (config-crypto-map)#**exit**
Switch (config)#**interface g0/0**
Switch (config-if)#**ip address 10.10.10.110 255.255.255.0**
Switch (config-if)#**crypto map sample**
Switch(config-if)#**interface Loopback1**
Switch(config-if)#**ip address 30.0.0.1 255.0.0.0**
Switch(config-if)#**exit**
Switch(config)#**ip route 40.0.0.0 255.0.0.0 10.10.10.101**

Switch(config)#**access-list 170 permit ip 30.0.0.0 0.255.255.255 40.0.0.0 0.255.255.255**
Switch(config)#**logging source-interface Loopback1**
Switch(config)#**logging host 40.0.0.1**

3.3.8.2 Syslog Server Adjacent to an IPsec Peer

If the syslog server is not directly co-located with the TOE, then the syslog server must be located in a physically protected facility and connected to a router capable of establishing an IPsec tunnel with the TOE. This will protect the syslog records as they traverse the public network.

Following are sample instructions to configure the TOE to support an IPsec tunnel with aes encryption, with 11.1.1.4 as the IPsec peer, 10.1.1.7 and 11.1.1.6 as the local IPs, and the syslog server on the 12.1.1.0 /28 subnet. For the following commands see the **[6]**.

Changes to the IP addressing scheme and routing policies may need to be changed to support the organization network.

Switch#**configure terminal**
Switch#**crypto isakmp policy 1**
Switch(config-isakmp)#**encryption aes**
Switch(config-isakmp)#**authentication pre-share**
Switch(config-isakmp)#**group 14**
Switch(config-isakmp)#**lifetime 28800**
Switch(config)#**crypto isakmp key {*keystring*} address 10.10.10.101**
Switch(config)#**crypto ipsec transform-set sampleset esp-aes esp-sha-hmac**
Switch(cfg-crypto-trans)#**mode tunnel**
Switch(config)#**crypto map sample 1 ipsec-isakmp**
Switch(config-crypto-map)#**set peer 11.1.1.4**
Switch(config-crypto-map)#**set transform-set sampleset**
Switch(config-crypto-map)#**match address 115**
Switch(config-crypto-map)#**exit**
Switch(config)#**interface g0/1**
Switch(config-if)#**ip address 10.1.1.7 255.255.255.0**
Switch(config-if)#**no ip route-cache**
Switch(config-if)#**crypto map sample**
Switch(config-if)#**interface g0/0**
Switch(config-if)#**ip address 11.1.1.6 255.255.255.0**
Switch(config-if)#**crypto map sample**
Switch(config-if)#**exit**
Switch(config)#**ip route 12.1.1.0 255.255.255.0 11.1.1.4**
Switch(config)#**access-list 115 permit ip 10.1.1.0 0.0.0.255 12.1.1.0 0.0.0.255 log**
Switch(config)#**logging host 12.1.1.1**

3.4 Logging Configuration

The switch can be configured to generate an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include events related to the

enforcement of information flow policies, identification and authentication related events, and administrative events. Additionally, the startup and shutdown of the TOE generates an audit record to indicate the TOE is up and operational or is shutting down and all processes are stopping. A complete list of available audit messages for the Cat 3K Series product, beyond what is required for the evaluated configuration can be found in **[10]**.

To ensure audit records are generated for the required auditable events, the TOE must be configured in its evaluated configuration as specified in this document. This is to ensure that auditing is enabled so that the audit records are being generated for the required auditable events. If the command 'no logging on' is entered the TOE is deemed no longer in the evaluated configuration.

- Logging of command execution must be enabled **[5] [6] [10]**:

  Switch(config)#**archive**

  Switch(config-archive)#**log config**

  Switch(config-archive-log-cfg)#**logging enable**

  Switch(config-archive-log-cfg)**#hidekeys** (this ensures that keys and passwprds are not displayed in the clear)

  Switch(config-archive-log-cfg)#**logging size *entires*** (number of entries to be retained in the configuration log. The range is from 1 to 1000; the default is 100)

  Switch(config-archive-log-cfg)#**notify syslog** (this enables the sending of notifications of configuration changes to a remote syslog server if configured. See Remote Logging below for configuring the syslog server)

  Switch(config-archive-log-cfg)#**end**

  Switch(config-archive)#**exit**

- Timestamps, including the year must be enabled for the audit records:

  Switch(config)#**service timestamps log datetime year**

  Switch(config)#**service timestamps debug datetime year**

- To protect against audit data loss if the switch fails, the audit records can be saved to flash memory by using the global configuration command

  logging file flash: ***filename***.

- To view the audit records after they have been saved, use the privileged EXEC command to display its contents

  more flash: ***filename***

- Set the size logging file size. The range is 4096 to 2147483647:

  logging file *filesystem:filename* (alias for a flash file system. Contains the path and name of the file that contains the log messages) ***max-file-size*** (Specify the maximum logging file size)

- To generate logging messages for failed and successful login attempts in the evaluated configuration, issue the login on-failure and login on-success commands. Note these requirements are syslog level 6 (informational) so if debugging level (**logging buffer debug**) of audit is not set as a default, then at least informational (**logging buffer informational**) level will need to be set:

  Switch(config)**#login on-failure log**

  Switch(config)**#login on-success log**

- Enable radius and ssh debugging:

  Switch(config)**#debug radius authentication**

  Switch(config)**#debug ip ssh authentication**

- Enable IPsec related debugging

  Switch(config)**#debug crypto isakmp**

  Switch(config)**#debug crypto ipsec**

  Switch(config)**#debug crypto ikev1** or **ikev2**

- Enable logging of ssh session establishment, authentication request, terminations and timeouts in privileged EXEC mode enter the following:

  Switch#debug ip ssh detail

- To enable remote logging of debugging information after a reboot, use the following command in privileged EXEC mode.

  Switch#logging trap debugging

Debug level auditing is required for specific protocols and events to ensure the audit records with the level of information are generated to meet the requirements in the Security Target. When that level of auditing is required, it is annotated as such throughout this AGD document.

Before you start a debug command, always consider the output that this command will generate and the amount of time this can take. Before debugging, look at your CPU load with the "**show processes cpu"** command **[6]**. Verify that you have ample CPU available before you begin the debugs and use the debug commands with caution.

3.4.1 Usage of Embedded Event Manager

It may be necessary to use the following Cisco Embedded Event Manager (EEM) script in order to ensure that all commands executed by a level 15 user are captured in a syslog record, the following EEM script can be used. Enter it at the CLI as follows:

Switch(config)#**event manager applet cli_log**

Switch(config-applet)#**event cli pattern "." *mode exec enter**

Switch(config-applet)#**action 1.0 info type routername**

Switch(config-applet)#**action 2.0 syslog msg "User:$_cli_username via Port:$_cli_tty Executed[$_cli_msg]"**

Switch(config-applet)#**action 3.0 set _exit_status "1"**

Switch(config-applet)#**end**

See https://supportforums.cisco.com/community/netpro/network-infrastructure/eem for more information on EEM scripting.

3.4.2 Remote Logging

To protect against audit data loss the TOE must be configured to send the audit records securely (through an IPsec tunnel) to an external TCP syslog server. For instance all emergency, alerts, critical, errors, and warning message can be sent to the console alerting the administrator that some action needs to be taken as these types of messages mean that the functionality of the switch is affected. All notifications and information type message can be sent to the syslog server, whereas message is only for information and the switch functionality is not affected.

Since this functionality is not enabled by default refer to "Configuring System Messages Logging" in **[5]** to configure this option. You will also need to configure local logging. Refer to **[5]** Configuring System Message Logging to configure local logging. It is recommended to read the entire section to become familiar with the concept and configuration before configuring local and remote logging.

Configure IPsec tunnel(s) to transport the syslog messages to syslog server(s). Without using IPsec, the syslog connection would not have confidentiality and integrity of the audit data secured in transit. For guidance on configuration of IPsec tunnels, refer to Session Protection in this document. The set of logging messages sent to the remote syslog server with the **logging host <ip address of syslog server>** command **[6]**, can be the same or different from the set written to the local logging buffer. To specify the severity level for logging to the syslog host, use the **logging trap** command **[6]**. Level 7 will send all logs required in the evaluation up to the debug level logs, as configured above to the syslog server.

When connection to the remote audit server is down (either because the IPsec tunnel is down, or the syslog server is unavailable), Cat 3K Series will continue to logging messages to the logging buffer. Messages in the logging buffer can be viewed with the "**show logging buffer**" command **[10]** show gsr through show monitor event trace -> **show logging**. When the buffer is full, the oldest messages will be overwritten with new messages. The buffer size can be increased from the default using the command, "**logging buffered [buffer size in bytes]**". You will also need to set the command, **logging buffer debug** to ensure an audit record is generated if there is an issue with the logging buffer.

3.4.3 Logging Protection

If an authorized administrator wants to back-up the logs to a syslog server, then protection must be provided for the syslog server communications. This can be provided in one of two ways:

1. With a syslog server operating as an IPsec peer of the TOE and the records tunneled over that connection, or
2. With a syslog server is not directly co-located with the TOE, but is adjacent to an IPsec peer within a trusted facility, and the records are tunneled over the public network.

Note in either configuration the IPsec peer must, at a minimum support peer authentication using RSA and pre-shared keys and the following algorithms AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-CBC-256 (as specified by RFC 3602) and DH Groups 14 (2048-bit MODP).

Refer to 3.3.8 Session Protection for deployment configuration examples where the syslog server is able to operate as an IPsec peer of the TOE or if the syslog server is not directly co-located with the TOE, then the syslog server must be located in a physically protected facility and connected to a router capable of establishing an IPsec tunnel with the TOE. This will protect the syslog records as they traverse the public network.

4. Secure Management

4.1 User Roles

The Cat 3K Series has both privileged and semi-privileged administrator roles as well as non-administrative access. Non-administrative access is granted to authenticated neighbor switches for the ability to receive updated routing tables. There is no other access or functions associated with non-administrative access. These privileged and semi-privileged roles are configured in the Access Control and Session Termination section above. The TOE also allows for customization of other levels. Privileged access is defined by any privilege level entering an 'enable secret 5' after their individual login. Note: The command 'enable secret' is a replacement for the 'enable password' command since the 'enable secret' creates the password and stores it in encrypted. Privilege levels are number 0-15 that specifies the various levels for the user. The privilege levels are not necessarily hierarchical. Privilege level 15 has access to all commands on the TOE. Privilege levels 0 and 1 are defined by default, while levels 2-14 are undefined by default. Levels 0-14 can be set to include any of the commands available to the level 15 administrators, and are considered the semi-privileged administrator for purposes of this evaluation. The privilege level determines the functions the user can perform; hence the authorized administrator with the appropriate privileges.

Refer to the IOS Command Reference Guide for available commands and associated roles and privilege levels. **[3] [4(b)] [6] [10]**.

4.2 Passwords

The password complexity is not enforced by the router by default, and must be administratively set in the configuration. To prevent administrators from choosing insecure passwords, each password must be at least 15 characters.

Use the following command (if supported) **[6]** to set the minimum length to 15.

security passwords min-length <length>

You can also set the password minimum length in the **aaa common-criteria policy** using the **min-length** <length> option **[6]** Cisco IOS Security Command Reference: Commands A to C -> aaa accounting through aaa local authentication attempts max-fail -> aaa common-criteria policy. See below for syntax.

The password can be composed of any combination of characters that includes characters for at least 3 of these four character sets: upper case letters, lower case letters, numerals, and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")".

Configure the TOE to enforce that complexity requirement by enabling **aaa password restriction** command that will also enforce the following restrictions:

1. The new password cannot have any character repeated more than three times consecutively.
2. The new password cannot be the same as the associated username.
3. The password obtained by capitalization of the username or username reversed is not accepted.

4. The new password cannot be “cisco”, “ocsic”, or any variant obtained by changing the capitalization of letters therein, or by substituting “1”, “|”, or “!” for i, or by substituting “0” for “o”, or substituting “$” for “s”.

The **aaa password restriction** command **[6]** can only be used after the **aaa new-model** command is configured (described below).

To prevent users from choosing insecure passwords, password should meet the following requirements:

- Does not contain more than three consecutive characters, such as abcd
- Does not contain more than two repeating characters, such as aaabbb
- Does not contain dictionary words
- Does not contain common proper names

The above items are recommended but are not enforced by the TOE:

The Cat 3K Series can enforce the use of strong passwords by using options listed below with the “**aaa common-criteria policy**” command **[6]** Cisco IOS Security Command Reference: Commands A to C -> aaa accounting through aaa local authentication attempts max-fail -> aaa common-criteria policy. To view the current policy use, “**show aaa common-criteria policy”** command **[6]** Cisco IOS Security Command Reference: Commands S to Z-> set aggressive-mode client-endpoint through show content-scan -> show aaa common-criteria policy.

The following are common criteria policy guidelines and password options that are available:

- First enable the authentication, authorization, and accounting (AAA) access control model with the “**aaa new-model”** command **[6]** Cisco IOS Security Command Reference: Commands A toC -> Cisco IOS Security Command Reference: Commands A to C aaa max-sessions through algorithm -> aaa new-model.

  aaa new-model

- Configure authentication, authorization, and accounting (AAA) common criteria security policies with the “**aaa common-criteria policy**” command **[6]** Cisco IOS Security Command Reference: Commands A toC -> aaa accounting through aaa local authentication attempts max-fail -> aaa common-criteria policy

  aaa common-criteria policy <policy>

  - Passwords must be set to a minimum length of 15 characters. To set the password minimum length use the min-length option use the aaa common-criteria policy command to enter the common criteria configuration policy mode..

    Switch(config)#**aaa common-criteria** <policy>

Switch(config-cc-policy)#**min-length** 15

- The aaa common criteria policy cannot be assigned to a user account without also setting a password within the same "**username**" command **[6]** Cisco IOS Security Command Reference: Commands S to Z -> traffic-export through zone security -> username. Following is an example command to set username, password and policy

  username <username> **common-criteria-policy** <policy> **password** <password>

To store passwords in encrypted form in the configuration file, use the "**service password-encryption**" command **[6]** Cisco IOS Security Command Reference: Cisco IOS Security Command Reference: Commands S to Z -> sa ipsec through sessions maximum -> service password-encryption.

service password-encryption

Whether or not "service password-encryption" has been enabled, a password for an individual username can be entered in either plaintext or as a SHA-256 hash value, and be stored as a SHA-256 hash value in the configuration file when using the "**username**" command. **[6]** Cisco IOS Security Command Reference: Commands S to Z -> traffic-export through zone security -> username. Following is an example command to set username, password and password encryption service

username *name* **secret** {**0** *password* | **4** *secret-string* | **5** *SHA256 secret-string*}

password is the password that a user enters.

0 - Specifies an unencrypted clear-text password. The password is converted to a SHA256 secret and gets stored in the router.

4 - Specifies an SHA256 encrypted secret string. The SHA256 secret string is copied from the router configuration.

5 - Specifies a message digest alogrithm5 (MD5) encrypted secret

To store the enable password in non-plaintext form, use the '**enable secret'** command when setting the enable password. The enable password can be entered as plaintext, or as an MD5 hash value. Example:

enable secret [**level** *level*] {*password* | **0** | **4** | **5** [*encryption-type*] *encrypted-password* }

level - (Optional) Specifies the level for which the password applies. You can specify up to sixteen privilege levels, using the numerals 0 through 15.

password – password that will be entered

0 - Specifies an unencrypted clear-text password. The password is converted to a SHA256 secret and gets stored in the router.

4 - Specifies an SHA256 encrypted secret string. The SHA256 secret string is copied from the router configuration.

5 - Specifies a message digest alogrithm5 (MD5) encrypted secret.

encryption-type - (Optional) Cisco-proprietary algorithm used to encrypt the password. The encryption types available for this command are 4 and 5. If you specify a value for *encryption-type* argument, the next argument you supply must be an encrypted password (a password encrypted by a Cisco router).

encrypted-password - Encrypted password that is copied from another router configuration.

Use of enable passwords are not necessary, so all administrative passwords can be stored as SHA-256 if enable passwords are not used.

Note: Cisco no longer recommends that the 'enable password' command be used to configure a password for privileged EXEC mode. The password that is entered with the 'enable password' command is stored as plain text in the configuration file of the networking device. If passwords were created with the 'enable password' command, it can be hashed by using the 'service password-encryption' command. Instead of using the 'enable password' command, Cisco recommends using the 'enable secret' command because it stores a SHA-256 hash value of the password.

To have IKE preshared keys stored in encrypted form, use the **password encryption aes** command **[6]** to enable the functionality and the **key config-key password-encrypt** {*text*} command **[6]** to set the master password to be used to encrypt the preshared keys. The preshared keys will be stored encrypted with symmetric cipher Advanced Encryption Standard [AES].

4.3 Clock Management

Some platforms have a hardware clock (calendar) in addition to a software clock. The hardware clock is battery operated, and runs continuously, even if the router is powered off or rebooted. If the software clock and hardware clock are not synchronized, and the software clock is more accurate, use the "calendar set" command **[5]** Basic System Management -> Setting Time and Calendar Services -> Setting the Hardware Clock to update the hardware clock to the correct date and time after setup and configuration is complete. Clock management is restricted to the privileged administrator.

For further details refer to Basic System Management -> Setting Time and Calendar Services in **[5]** and Using the Cisco IOS Command-Line Interface (CLI) in **[11]**.

4.4 Identification and Authentication

Configuration of Identification and Authentication settings is restricted to the privileged administrator.

The Cat 3K Series can be configured to use local authentication and authorization secured using SSHv2 or RADIUS secured using IPsec. Refer to Securing User Services Overview -> RADIUS and TACACS+ Attributes **[4(a)]**. It is recommended to read this section to

become familiar with remote authentication concepts prior to configuration. You can also refer to the specific commands in **[6]** regarding configuring RADIUS commands.

4.5 Administrative Banner Configuration

The TOE provides the authorized administrator the ability to configure a banner that displays on the CLI management interface prior to allowing any administrative access to the TOE.

- This functionality is available to the privileged administrator.
- This functionality is facilitated using the "**banner login**" command **[10]**

For example, to create a banner of text "This is a banner" use the command

banner login d This is a banner d

Information regarding banner configuration can be found in Managing Connection, Menus, and System Banners ->Managing Connections, Menus and System Banners Task List in **[11]**.

4.6 Use of Administrative Session Lockout and Termination

The TOE allows the privileged administrator to configure the length of time that an inactive administrative session remains open. After the configured period of time, the administrative session is locked and the screen is flushed. No further activity is allowed to until the administrator has successfully re-authenticated to the Switch. The administrator is required to re-authenticate after the session becomes locked and the screen is cleared.

The **exec-timeout** command is used to configure this locking of the session after the administrator is inactive for the specified number of minutes and seconds on the console (or vty) lines:

Switch(config)**# line console**

Switch(config-line)**# exec-timeout 0 10**

The example above sets the console time interval of 10 seconds. Use the **no** form of this command (**no exec-timeout**) to remove the timeout definition **[10]** D through E.

4.7 Product Updates

Verification of authenticity of updated software is done in the same manner as ensuring that the TOE is running a valid image. See 2 Secure Acceptance of the TOE above in this document; specially steps 7 and 9 for the method to download and verify an image prior to running it on the TOE.

5. Security Relevant Events

The TOE is able to generate audit records that are stored internally within the TOE whenever an audited event occurs, as well as simultaneously offloaded to an external syslog server. The details for protection of that communication are covered in section Logging Protection above.

The administrator can set the level of the audit records to be stored in a local buffer, displayed on the console, sent to the syslog server, or all of the above. The details for configuration of these settings are covered in the relevant section above in this document.

The local log buffer is circular. Newer messages overwrite older messages after the buffer is full. Administrators are instructed to monitor the log buffer using the show logging privileged EXEC command to view the audit records. The first message displayed is the oldest message in the buffer.

When configured for a syslog backup the TOE will simultaneously offload events from a separate buffer to the external syslog server. This buffer is used to queue events to be sent to the syslog server if the connection to the server is lost. It is a circular buffer, so when the events overrun the storage space overwrites older events.

Refer to the relevant section below in this document that include the security relevant events that are applicable to the TOE.

5.1 Deleting Audit Records

The TOE provides the privileged administrator the ability to delete audit records stored within the TOE. This is done with the "**clear logging"** command **[10]** C commands -> clear logging.

5.2 Reviewing Audited Events

Cat 3K Series maintains logs in multiple locations: local storage of the generated audit records, and simultaneous offload of those events to the external syslog server. For the most complete view of audited events, across all devices, and to view the auditable events defined in the Security Target administrators should review the Audit Log on a regular basis.

Using the Cat 3K Series Command Line Interface (CLI) administrators can review audited events. The information provided in the audit records include the date and time of the event, the type of event, subject identity (if applicable), the outcome of the event, and additional information related to the event. To review locally stored audit records, enter the command "**show logging**" **[6] ->** configuring System Message Logging and Smart Logging or **[10]** -> show gsr through show monitor event trace -> show logging (*). Also, to display logging information see **[5]** Troubleshooting and Fault Management -> Logging System Messages -> Displaying Logging Information,

System log messages can contain up to 80 characters and a percent sign (%), which follows the optional sequence number or time-stamp information The part of the message preceding the percent sign depends on the setting of the service sequence-numbers, service timestamps log datetime, service timestamps log datetime [localtime] [msec] [show-timezone], or service timestamps log uptime global configuration command. The following information is basic information that is included in an audit/log record.

- Element - Description
- seq no: - Stamps log messages with a sequence number only if the service sequence-numbers global configuration command is configured. For more information, see the "Enabling and Disabling Sequence Numbers in Log Messages" section.

- timestamp formats:
    - mm/dd hh:mm:ss or hh:mm:ss (short uptime) or d h (long uptime)
- Date and time of the message or event. This information appears only if the service timestamps log [datetime | log] global configuration command is configured. For more information, see the "Enabling and Disabling Time Stamps on Log Messages" section.
- Facility - The facility to which the message refers (for example, SNMP, SYS, and so forth). For a list of supported facilities, see Table 34-4.
- severity - Single-digit code from 0 to 7 that is the severity of the message. For a description of the severity levels, see Table 34-3.
- MNEMONIC - Text string that uniquely describes the message.
- description - Text string containing detailed information about the event being reported.
- hostname-n - Hostname of a stack member and its switch number in the stack. Though the stack master is a stack member, it does not append its hostname to system messages.

Below is a sample of audit records for the various required auditable events; note these records are a sample and not meant as an exact record for the particular event. In addition, for some cryptographic failures producing an audit record would require extensive manipulation and therefore snippets of source code is provided to illustrate what would be displayed in an audit record. The indication that the TSF self-test was completed successful is indicated by reaching a log-in prompt. If TSF self-test did not complete successfully, a system failure error message would be displayed.

Table 12 Audit Records (sample)

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FCS_MACSEC_EXT.1	Session establishment	Secure Channel Identifier (SCI)	• **Session Establishment** Mar 15 2016 12:49:11.891 IST: %MKA-5-SESSION_START: (Te1/2 : 22) MKA Session started for RxSCI 188b.9d3c.c83f/0000, AuditSessionID 092B033C0000000E000C08B8, AuthMgr-Handle 45000002 Mar 15 2016 12:49:11.891 IST: MKA-EVENT: Started a new MKA Session on interface TenGigabitEthernet1/2 for Peer MAC 188b.9d3c.c83f with SCI80E0.1DC6.3E7F/0016 successfully
FCS_MACSEC_EXT.1.7	Creation of Connectivity Association	Connectivity Association Key Names	• **Creation of Connectivity Association** Mar 15 2016 <Gi1/0/2 : 9> 14:38:53.326 IST: %MKA-5-SESSION_SECURED:

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			(Gi1/0/2 : 9) MKA Session was secured for RxSCI 90e2.ba12.a00d/0000, AuditSessionID 000000000000000D001C2D92, CKN 24AA15376050334AE1EA9BE8A1D0894B 00000000000000000000000000000000
FCS_MACSEC_EXT.3.1	Creation and update of Secure Association Key	Creation and update times	• **For SAK (Security Association Key) creation-** Mar 15 2016 12:54:49.937 IST: MKA-EVENT 80e0.1dc6.3e7f/0016 C7000003: Generation of new Latest SAK succeeded (Latest AN=0, KN=1)... • **For SAK (Security Association Key) update –** Mar 15 2016 <tel:2016> 14:38:53.326 IST: %MKA-6-SAK_REKEY: (Gi0/1/0 : 10) MKA Session is beginning a SAK Rekey (current Latest AN/KN 0/1, Old AN/KN 0/1) for RxSCI f4cf.e298.ccb8/000a, AuditSessionID CKN 10000000000000000000000000000000000000000000000000000000000000000000
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA. Session establishment with peer	Reason for failure. Entire packet contents of packets transmitted/received during session establishment	**Initiation of IPSEC session (outbound):** Jun 20 07:42:26.823: ISAKMP (0): received packet from 100.1.1.5 dport 500 sport 500 Global (N) NEW SA Jun 20 07:42:26.823: ISAKMP: Created a peer struct for 100.1.1.5, peer port 500 Jun 20 07:42:26.823: ISAKMP: New peer created peer = 0x89C3879C peer_handle = 0x8000000C Jun 20 07:42:26.823: ISAKMP: Locking peer struct 0x89C3879C, refcount 1 for crypto_isakmp_process_block Jun 20 07:42:26.823: ISAKMP: local port 500, remote port 500 Jun 20 07:42:26.823: ISAKMP:(0):insert sa successfully sa = 8C1C1FD4 Jun 20 07:42:26.823: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH Jun 20 07:42:26.823: ISAKMP:(0):Old State = IKE_READY New State = IKE_R_MM1 …

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			Jun 20 07:42:26.823: ISAKMP:(0):found peer pre-shared key matching 100.1.1.5 Jun 20 07:42:26.823: ISAKMP:(0): local preshared key found Jun 20 07:42:26.823: ISAKMP : Scanning profiles for xauth ... Jun 20 07:42:26.823: ISAKMP:(0):Checking ISAKMP transform 1 against priority 1 policy Jun 20 07:42:26.827: ISAKMP: encryption AES-CBC Jun 20 07:42:26.827: ISAKMP: keylength of 128 Jun 20 07:42:26.827: ISAKMP: hash SHA Jun 20 07:42:26.827: ISAKMP: default group 14 Jun 20 07:42:26.827: ISAKMP: auth pre-share… Jun 20 07:42:26.843: ISAKMP (0): received packet from 100.1.1.5 dport 500 sport 500 Global (R) MM_SA_SETUP Jun 20 07:42:26.843: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH Jun 20 07:42:26.843: ISAKMP:(0):Old State = IKE_R_MM2 New State = IKE_R_MM3 Jun 20 07:42:26.843: ISAKMP:(0): processing KE payload. message ID = 0 Jun 20 07:42:27.055: ISAKMP:(0): processing NONCE payload. message ID = 0 Jun 20 07:42:27.059: ISAKMP:(0):found peer pre-shared key matching 100.1.1.5 **Termination of IPSEC session (outbound-initiated):** .Jun 19 21:09:49.619: IPSEC(delete_sa): deleting SA, (sa) sa_dest= 100.1.1.5, sa_proto= 50, sa_spi= 0x3C81B171(1015132529), sa_trans= esp-aes esp-sha-hmac , sa_conn_id= 62 sa_lifetime(k/sec)= (4608000/28800), (identity) local= 100.1.1.1:0, remote= 100.1.1.5:0, local_proxy= 10.1.1.0/255.255.255.0/256/0,

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			remote_proxy= 12.1.1.0/255.255.255.0/256/0 Jun 19 21:10:37.575: ISAKMP:(2034):purging node -506111676 .Jun 19 21:10:39.615: ISAKMP:(2034):purging node -22679511 .Jun 20 04:46:14.789: IPSEC(lifetime_expiry): SA lifetime threshold reached, expiring in 1412 seconds **Failure to establish an IPSEC session (outbound-initiated):** Jun 19 11:12:33.905: %CRYPTO-5-IKMP_AG_MODE_DISABLED: Unable to initiate or respond to Aggressive Mode while disabled
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure	**Failure to establish an SSH Session.** **IP address of remote host** **Reason for failure.** GENERIC EXAMPLE: Jun 18 2012 11:19:06 UTC: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: anonymous] [Source: 100.1.1.5] [localport: 22] [Reason: Login Authentication Failed] at 11:19:06 UTC Mon Jun 18 2012 **Establishment of an SSH session** **IP address of remote host** Jun 18 2012 11:31:35 UTC: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: ranger] [Source: 100.1.1.5] [localport: 22] at 11:31:35 UTC Mon Jun 18 2012 Feb 8 06:47:17.041: %SSH-5-SSH2_CLOSE: SSH2 Session from 1.1.1.1 (tty = 0) for user 'cisco' using crypto cipher 'aes256-cbc', hmac 'hmac-sha1-96' closed

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded. Administrator lockout due to excessive authentication failures	Origin of the attempt (e.g., IP address).	**Unsuccessful login attempts limit is met or exceeded:** Nov 25 2017 10:52:47.652: \%SEC_LOGIN-4-LOGIN_FAILED: Login failed [user:] [Source: 10.21.0.101] [localport: 22] [Reason: Login Authentication Failed] at 10:52:47 EST Sat Nov 25 2017 Nov 25 2017 10:52:49.655: \%SEC_LOGIN-4-LOGIN_FAILED: Login failed [user:] [Source: 10.21.0.101] [localport: 22] [Reason: Login Authentication Failed] at 10:52:49 EST Sat Nov 25 2017 Nov 25 2017 10:53:05.678: \%SEC_LOGIN-4-LOGIN_FAILED: Login failed [user:] [Source: 10.21.0.101] [localport: 22] [Reason: Login Authentication Failed] at 10:53:05 EST Sat Nov 25 2017 Nov 25 2017 10:53:26.693: \%AAA-5-USER_LOCKED: User testuser locked out on authentication failure
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).	All use of the identification and authentication mechanism.

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).	**Login as an administrative user at the console:** Username: auditperson Password: 000278: *Apr 23 07:11:56: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: auditperson] [Source: 0.0.0.0] [localport: 0] at 07:11:56 UTC Thu Apr 23 2009? Failed login via the console does not allow any actions Username: auditperson Password: % Authentication failed Username: 000254: *Apr 26 00:45:43.340: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: auditperson] [Source: 0.0.0.0] [localport: 0] [Reason: Login Authentication Failed] at 23:45:43 a Sat Apr 25 2009 See FCS_SSH_EXT.1 for remote login audit events.

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FIA_X509_EXT.1	Unsuccessful attempt to validate a certificate Session establishment with CA	Reason for failure Entire packet contents of packets transmitted/received during session establishment.	**Session establishment with CA:** 42479: Initiator SPI : 6038B31E75BFF128 - Responder SPI : ECB6C134F5652076 Message id: 1 42478: *Feb 5 11:10:18.749: IKEv2:(SA ID = 1):Sending Packet [To 210.1.1.1:500/From 110.1.1.1:500/VRF i0:f0]42442: *Feb 5 11:10:18.747: IKEv2:(SA ID = 1):[PKI -> IKEv2] Getting of cert chain for the trustpoint PASSED 42441: *Feb 5 11:10:18.747: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Getting cert chain for the trustpoint rahul 42440: *Feb 5 11:10:18.747: IKEv2:(SA ID = 1):[PKI -> IKEv2] Retrieved trustpoint(s): 'rahul' 42439: *Feb 5 11:10:18.747: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Retrieving trustpoint(s) from received certificate hash(es) 42438: *Feb 5 11:10:18.747: IKEv2:(SA ID = 1):Processing IKE_SA_INIT message 42437: *Feb 5 11:10:18.747: IKEv2:(SA ID = 1):Verify SA init message 42436: *Feb 5 11:10:18.747: IKEv2:(SA ID = 1):Processing IKE_SA_INIT message 42435: SA KE N VID VID NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP) CERTREQ NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED) **Unsuccessful attempt to validate a certificate:** Aug 3 19:10:18.621: %PKI-3-CERTIFICATE_REVOKED: Certificate chain validation has failed. The certificate (SN: 04) is revoked

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FMT_MOF.1/Services	Starting and stopping of services	None	Jul 19 12:10:00 toe-loopback 289: *Jul 19 2018 12:10:00.678: \%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.24.0.1 port 514 started - CLI initiated Jul 19 12:09:51 toe-loopback 282: *Jul 19 2018 12:09:51.963: \%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.24.0.1 port 514 stopped - CLI initiated
FMT_MOF.1/ Manual Update	Any attempt to initiate a manual update	None	Jul 10 11:04:09.179: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command:upgrade
FMT_MTD.1/CryptoKeys	Management of Cryptographic keys	None	**Resetting of passwords:** Nov 21 2017 15:06:53.679: \%PARSER-5CFGLOG_LOGGEDCMD: User:admin logged command:no enable password Nov 21 2017 15:06:53.724: \%PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:no username script privilege 15 password 0 password Nov 21 2017 15:08:54.042: \%PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:username script privilege 15 password 0 secret Nov 21 2017 15:08:54.070: \%PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:enable password secret See all other records in Table 8 “Auditable Administrative Events”.

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FMT_MTD.1/CoreData	All management activities of TSF data	None	**Resetting of passwords:** Nov 21 2017 15:06:53.679: \%PARSER-5CFGLOG_LOGGEDCMD: User:admin logged command:no enable password Nov 21 2017 15:06:53.724: \%PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:no username script privilege 15 password 0 password Nov 21 2017 15:08:54.042: \%PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:username script privilege 15 password 0 secret Nov 21 2017 15:08:54.070: \%PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:enable password secret See all other records in Table 8 “Auditable Administrative Events”.
FPT_RPL.1	Detected replay attempt	None	*Jul 7 18:43:14.595: %MKA-3-MKPDU_VALIDATE_FAILURE: (Gi0/0/1 : 11) Validation of a MKPDU failed for RxSCI 6412.25a1.a409/0009, AuditSessionID , CKN 12340000000000000000000000000000000000000000000000000000000000000000
FPT_STM_EXT.1	Discontinuous changes to time – either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).	**Local Clock Update:** CLOCKUPDATE: System clock has been updated from 06:11:37 EDT Mon Dec 20 2010 to 06:10:00 EDT Tue Dec 20 2011, configured from console by user on console.

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FPT_TUD_EXT.1	Initiation of update. result of the update attempt (success or failure)	None.	**Use of the "upgrade" command:** *Jul 10 11:04:09.179: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command:upgrade *Jul 10 11:04:09.179: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command:copy tftp …. *Jul 10 11:04:09.179: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command:reload **Update Failure:** autoboot: boot failed, restarting...
FTA_SSL_EXT.1	Any attempts at unlocking of an [local] interactive session.	None.	**In the TOE this is represented by login attempts that occur after the timeout of a local administrative user.** 001383: May 10 18:06:34.091: %SYS-6-EXEC_EXPIRE_TIMER: (tty 0 (0.0.0.0)) exec-timeout timer expired for user securityperson 001384: May 10 18:06:34.091: %SYS-6-EXIT_CONFIG: User securityperson has exited tty session 0(0.0.0.0)
FTA_SSL.3	The termination of a *remote* session by the session locking mechanism.	None.	**Audit record generated when SSH session is terminated because of idle timeout:** May 29 2012 15:18:00 UTC: %SYS-6-TTY_EXPIRE_TIMER: (exec timer expired, tty 0 (0.0.0.0)), user admin

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FTA_SSL.4	The termination of an interactive session.	None.	**Audit record generate when admin logs out of CONSOLE.** May 17 2011 16:29:09: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command:exit **Audit record generated when the admin logs out of SSH:** Jun 18 11:17:36.653: SSH0: Session terminated normally
FTA_TAB.1	Administrative Action: Configuring the banner displayed prior to authentication.	None	Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco **logged command: banner login d This is a banner d**
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.	AUDIT: See logs provided by FCS_IPSEC_EXT.1.
FTP_TRP.1	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.	AUDIT: See logs provided by FCS_SSH_EXT.1

Table 13 Auditable Administrative Events

Requirement	Management Action to Log	Sample Log
FAU_GEN.1: Audit data generation	Changing logging settings. Clearing logs.	**Changing logging settings:** Feb 17 2013 16:29:07: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command:logging enable Feb 17 2013 16:34:02: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command:logging informational **Clearing logs:** Feb 17 2013 17:05:16: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command:clear logging
FAU_GEN.2: User identity association	None	N/A
FAU_STG_EXT.1: External audit trail storage	Configuration of syslog export settings	Feb 17 2013 17:05:16: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command:logging host
FCS_CKM.1: Cryptographic key generation (for asymmetric keys)	Manual key generation	Feb 17 2013 16:14:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command:crypto key ***** Jan 24 2013 03:10:08.878: %GDOI-5-KS_REKEY_TRANS_2_UNI: Group getvpn transitioned to Unicast Rekey.ip
FCS_CKM_EXT.4: Cryptographic key zeroization	Manual key zeroization	Feb 17 2013 16:37:27: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command:crypto key zeroize
FCS_COP.1/DataEncryption: Cryptographic operation (for data encryption/decryption)	None	N/A
FCS_COP.1/SigGen: Cryptographic operation (for cryptographic signature)	None	N/A
FCS_COP.1/Hash: Cryptographic operation (for cryptographic hashing)	None	N/A
FCS_COP.1/KeyedHash: Cryptographic operation (for keyed-hash message authentication)	None	N/A

Requirement	Management Action to Log	Sample Log
FCS_RBG_EXT.1: Cryptographic operation (random bit generation)	None	N/A
FCS_IPSEC_EXT.1	Configuration of IPsec settings: including mode, security policy, IKE version, algorithms, lifetimes, DH group, and certificates.	Feb 17 2013 16:14:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command: crypto isakmp policy 1
FCS_SSH_EXT.1	Configuration of SSH settings: including certificates or passwords, algorithms, host names, users.	Feb 17 2013 16:14:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command: ip ssh version 2
FIA_AFL.1	Configuring number of failures. Unlocking the user.	**Configuring number of failures:** Feb 17 2013 16:14:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command: aaa local authentication attempts max-fail [number of failures] **Unlocking the user:** Feb 7 2013 02:05:41.953: %AAA-5-USER_UNLOCKED: User user unlocked by admin on vty0 (21.0.0.1)
FIA_PMG_EXT.1: Password management	Setting length requirement for passwords.	Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: security passwords min-length 15
FIA_PSK_EXT.1: Pre-Shared Key Composition	Creation of a pre-shared key.	Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: crypto isakmp key *****
FIA_UIA_EXT.1: User identification and authentication	Logging into TOE.	Jan 17 2013 05:05:49.460: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: ranger] [Source: 21.0.0.3] [localport: 22] at 00:05:49 EST Thu Jan 17 2013
FIA_UAU_EXT.2: Password-based authentication mechanism	None	N/A
FIA_UAU.7: Protected authentication feedback	None	N/A
FIA_X509_EXT.1/Rev: X.509 Certificates	Generating a certificate.	Feb 17 2013 16:14:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command: crypto key generate

Requirement	Management Action to Log	Sample Log
FMT_MOF.1/ManualUpdate: Management of Security Functions Behavior	See all other rows in table.	N/A
FMT_MTD.1/CoreData: Management of TSF data (for general TSF data)	See all other rows in table.	N/A
FMT_SMF.1: Specification of management functions	See all other rows in table.	N/A
FMT_SMR.2: Restrictions on Security roles	Configuring administrative users with specified roles.	Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: username admin 15
FPT_RUL_EXT.1: Packet Filtering	Configuring packet filtering rules.	Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: access-list 199 deny ip 10.100.0.0 0.0.255.255 any log-input
FPT_SKP_EXT.1: Protection of TSF Data (for reading of all symmetric keys)	None	N/A
FPT_APW_EXT.1: Protection of Administrator Passwords	None	N/A
FPT_STM_EXT.1: Reliable time stamps	Manual changes to the system time.	Feb 5 2013 06:28:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 11:27:52 UTC Tue Feb 5 2013 to 06:28:00 UTC Tue Feb 5 2013, configured from console by admin on console.
FPT_TUD_EXT.1: Trusted update	Software updates	Jul 10 2013 11:04:09.179: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command:upgrade
FPT_TST_EXT.1: TSF testing	None	N/A
FTA_SSL_EXT.1: TSF-initiated session locking	Specifying the inactivity time period.	Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: exec-timeout 60
FTA_SSL.3: TSF-initiated termination	Specifying the inactivity time period.	Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: exec-timeout 60
FTA_SSL.4: User-initiated termination	Logging out of TOE.	Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: exit
FTA_TAB.1: Default TOE access banners	Configuring the banner displayed prior to authentication.	Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: banner login d This is a banner d
FTP_ITC.1: Inter-TSF trusted channel	None	N/A

Requirement	Management Action to Log	Sample Log
FTP_TRP.1: Trusted path	Connecting to the TOE with SSH.	Jan 17 05:05:49.460: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: ranger] [Source: 21.0.0.3] [localport: 22] at 00:05:49 EST Thu Jan 17 2013

6. Network Services and Protocols

The table below lists the network services/protocols available on the TOE as a client (initiated outbound) and/or server (listening for inbound connections), all of which run as system-level processes. The table indicates whether each service or protocol is allowed to be used in the certified configuration.

For more detail about each service, including whether the service is limited by firewall mode (routed or transparent), or by context (single, multiple, system), refer to the ***Command Reference*** guides listed above in this document

Table 14 Protocols and Services

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the certified configuration
AH	Authentication Header (part of IPsec)	Yes	No	Yes	No	No, ESP must be used in all IPsec connections.
DHCP	Dynamic Host Configuration Protocol	Yes	Yes	Yes	Yes	No restrictions.
DNS	Domain Name Service	Yes	Yes	No	n/a	No restrictions.
ESP	Encapsulating Security Payload (part of IPsec)	Yes	Yes	Yes	Yes	Configure ESP as described in relevant section of this document.
FTP	File Transfer Protocol	Yes	No	No	n/a	Use tunneling through IPsec
HTTP	Hypertext Transfer Protocol	Yes	No	Yes	No	Use tunneling through IPsec
HTTPS	Hypertext Transfer Protocol Secure	Yes	No	Yes	No	Use tunneling through IPsec
ICMP	Internet Control Message Protocol	Yes	Yes	Yes	Yes	No restrictions.
IKE	Internet Key Exchange	Yes	Yes	Yes	Yes	As described in the relevant sections of this document.

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the certified configuration
IMAP4S	Internet Message Access Protocol Secure version 4	Yes	Over IPsec	No	n/a	No restrictions.
IPsec	Internet Protocol Security (suite of protocols including IKE, ESP and AH)	Yes	Yes	Yes	Yes	Only to be used for securing traffic that originates from or terminates at the TOE, not for "VPN Gateway" functionality to secure traffic through the TOE. See IKE and ESP for other usage restrictions.
Kerberos	A ticket-based authentication protocol	Yes	Over IPsec	No	n/a	If used for authentication of TOE administrators, tunnel this authentication protocol secure with IPsec.
LDAP	Lightweight Directory Access Protocol	Yes	No, use RADIUS	No	n/a	Use RADIUS instead
LDAP-over-SSL	LDAP over Secure Sockets Layer	Yes	No, use RADIUS	No	n/a	Use RADIUS instead
RADIUS	Remote Authentication Dial In User Service	Yes	Yes	No	n/a	If used for authentication of TOE administrators, secure through IPsec.
SNMP	Simple Network Management Protocol	Yes (snmp-trap)	Yes	Yes	No	Outbound (traps) only. Recommended to tunnel through IPsec.

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the certified configuration
SSH	Secure Shell	Yes	Over IPsec secured connection	Yes	Yes	As described in the relevant section of this document.
SSL (not TLS)	Secure Sockets Layer	Yes	No	Yes	No	Use IPsec instead.
TACACS+	Terminal Access Controller Access-Control System Plus	Yes	No, use RADIUS	No	n/a	Use RADIUS instead
Telnet	A protocol used for terminal emulation	Yes	No	Yes	No	Use SSH instead.
TLS	Transport Layer Security	Yes	No	Yes	No	Not claimed; use IPsec instead
TFTP	Trivial File Transfer Protocol	Yes	Yes	No	n/a	Recommend using SCP or HTTPS instead, or tunneling through IPsec.

The table above does not include the types of protocols and services listed here:

- OSI Layer 2 protocols such as CDP, VLAN protocols like 802.11q, Ethernet encapsulation protocols like PPPoE, etc. The certified configuration places no restrictions on the use of these protocols; however evaluation of these protocols was beyond the scope of the Common Criteria product evaluation. Follow best practices for the secure usage of these services.
- Routing protocols such as EIGRP, OSPF, and RIP. The certified configuration places no restrictions on the use of these protocols, however evaluation of these protocols was beyond the scope of the Common Criteria product evaluation, so follow best practices for the secure usage of these protocols.
- Protocol inspection engines that can be enabled with "inspect" commands because inspection engines are used for filtering traffic, not for initiating or terminating sessions, so they're not considered network 'services' or 'processes' in the context of this table. The certified configuration places no restrictions on the use protocol inspection functionality; however evaluation of this functionality was beyond the scope of the Common Criteria product evaluation. Follow best practices for the secure usage of these services.
- Network protocols that can be proxied through/by the TOE. Proxying of services by the TOE does not result in running said service on the TOE in any way that would allow the TOE itself to be remotely accessible via that service, nor does it allow the TOE to initiate a connection to a remote server independent of the remote client that has initiated the connection. The certified configuration places no restrictions on enabling of proxy functionality; however, the evaluation of this functionality was beyond the scope of the Common Criteria product evaluation. Follow best practices for the secure usage of these services.

7. Modes of Operation

An IOS switch has several modes of operation, these modes are as follows:

Booting – while booting, the switches drop all network traffic until the switch image and configuration has loaded. This mode of operation automatically progresses to the Normal mode of operation. During booting, a user may press the break key on a console connection within the first 60 seconds of startup to enter the ROM Monitor mode of operation. This Booting mode is referred to in the IOS guidance documentation as "ROM Monitor Initialization". Additionally, if the Switch does not find a valid operating system image it will enter ROM Monitor mode and not normal mode therefore protecting the switch from booting into an insecure state.

Normal - The IOS switch image and configuration is loaded and the switch is operating as configured. It should be noted that all levels of administrative access occur in this mode and that all switch based security functions are operating. Once in the normal operating mode and fully configured, there is little interaction between the switch and the administrator. However, the configuration of the switch can have a detrimental effect on security; therefore, adherence to the guidelines in this document should be followed. Misconfiguration of the switch could result in the unprotected network having access to the internal/protected network

ROM Monitor – This mode of operation is a maintenance, debugging and disaster recovery mode. While the switch is in this mode, no network traffic is routed between the network interfaces. In this state the switch may be configured to upload a new boot image from a specified TFTP server, perform configuration tasks and run various debugging commands.

Note: If nvram is empty and a reload is done, IOS will try to boot automatically from an image top down that is in the flash directory. Make sure the valid IOS image is listed above any other images in flash.

To ensure the correct image is booted on startup use the boot system command **[6] [10]**:

#**boot system flash**:<image filename>

To return to EXEC mode from ROM monitor mode, use the "continue" command in ROM monitor mode.

rommon 1> **continue**

It should be noted that while no administrator password is required to enter ROM monitor mode, physical access to the switch is required, therefore the switch should be stored in a physically secure location to avoid unauthorized access which may lead to the switch being placed in an insecure state.

Following operational error the switch reboots (once power supply is available) and enters booting mode. The only exception to this is if there is an error during the Power on Startup

Test (POST) during bootup, then the TOE will shutdown or reboot to try to correct the issues. If any component reports failure for the POST, the system crashes and appropriate information is displayed on the screen and saved in the crashinfo file. Within the POST, self-tests for the cryptographic operations are performed. The same cryptographic POSTs can also be run on-demand as described above in this document and when the tests are run on-demand after system startup has completed (and the syslog daemon has started), error messages will be written to the log.

All ports are blocked from moving to forwarding state during the POST. Only when all components of all modules pass the POST is the system placed in FIPS PASS state and ports are allowed to forward data traffic.

If any of the POST fail, the following actions should be taken:

- If possible, review the crashinfo file. This will provide additional information on the cause of the crash
- Restart the TOE to perform POST and determine if normal operation can be resumed
- If the problem persists, contact Cisco Technical Assistance via http://www.cisco.com/techsupport or 1 800 553-2447
- If necessary, return the TOE to Cisco under guidance of Cisco Technical Assistance.

If a software upgrade fails, the Cat3K series will display an error when an authorized administrator tries to boot the system. The Cat3K series then boot into the rommon prompt.

```
Directory an_image.bin not  found
Unable to locate an_image.bin  directory
Unable to load an_image.bin
boot: error executing "boot  harddisk:an_image.bin"
autoboot: boot failed,  restarting
```

7.1 Network Processes Available During Normal Operation

The following network-based processes may be running, or can be run in the evaluated configurations of the Cat 3K Series, except where explicitly stated:

- ICMP is supported inbound and outbound for detection and troubleshooting of network connectivity.
- IPsec including ESP and IKE is supported for encryption of syslog traffic to an external audit server, and potentially to secure other traffic to/from external entities.
- RADIUS is supported for authentication of administrative connections to the console and/or via SSH.
- Routing protocols: The evaluated configuration supports use of BGPv4, EIGRP, EIGRPv6 for IPv6, PIM-SMv2, and OSPFv2, OSPFv3 for IPv6 and RIPv2. The routing protocols, BGPv4, EIGRP, EIGRPv6 for IPv6, PIM-SMv2, and OSPFv2, OSPFv3 for IPv6 supports routing updates with IPv4 or IPv6, while RIPv2 routing protocol support routing updates for IPv4 only. All these routing protocols support authentication of neighbor switches using MD5. Neither the authentication functions of those protocols, nor the use of MD5 were evaluated under Common Criteria.

- SSHv2 sessions secured connection is supported inbound and outbound for remote administrative access to the Cat3K series, or to initiate administrative access to an external network device or other device/server running SSHv2.
- Syslog is supported outbound for transmission of audit records to a remote syslog server (syslog connections must be tunneled through IPsec).
- SSL (not TLS) may be running, however there are no claims being made, was not evaluated and should not be used in the evaluated configuration.
- TLS to secure communications may be running, however there are no claims being made, was not evaluated and should not be used in the evaluated configuration.

Infrastructure services

- Cisco IOS software; to be configured for use as described in this document.
- Redundant components, such as power supplies and fans.
- Automation through Embedded Event Manager (EEM); no claims are made in the evaluated configuration. Note, this may not be supported on all TOE models due to limited space.
- AutoQoS (quality of services responding to traffic flows); no claims are made in the evaluated configuration.

Borderless services

- Rich layer 2/3/4 information (MAC, VLAN, TCP flags); no claims are made in the evaluated configuration.

8. Security Measures for the Operational Environment

Proper operation of the TOE requires functionality from the environment. It is the responsibility of the authorized users of the TOE to ensure that the TOE environment provides the necessary functions. The following identifies the requirements and the associated security measures of the authorized users.

Table 15 Security Objective for the Operational Environment

Security Objective for the Operational Environment	Definition of the Security Objective	Responsibility of the Administrators
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	The Cat 3K Series must be installed to a physically secured location that only allows physical access to authorized personnel.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.	None. IOS is a purpose-built operating system that does not allow installation of additional software.
~~OE.NO_THRU_TRAFFIC_PROTECTION~~	~~The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.~~	~~Administrators will ensure protection of any critical network traffic (administration traffic, authentication traffic, audit traffic, etc.) and ensure appropriate operational environment measures and policies are in place for all other types of traffic.~~
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.	Administrators must read, understand, and follow the guidance in this document to securely install and operate the TOE and maintain secure communications with components of the operational environment.
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	Administrators must download updates, including psirts (bug fixes) to the evaluated image to ensure that the security functionality of the TOE is maintained
OE.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the TOE must be protected on any other	Administrators must securely store and appropriately restrict access to credentials that are

Security Objective for the Operational Environment	Definition of the Security Objective	Responsibility of the Administrators
	platform on which they reside.	used to access the TOE (i.e. private keys and passwords)

9. Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation at:

With CCO login:
http://www.cisco.com/en/US/partner/docs/general/whatsnew/whatsnew.html

Without CCO login:
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

9.1 Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click Feedback in the toolbar and select Documentation. After you complete the form, click Submit to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc., Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

9.2 Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at any time, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com