Cisco Catalyst 3850 Series Switches running IOS-XE 3.6.0E and Catalyst 6500 Series Switches running IOS 15.1(2)SY3

Common Criteria

Operational User Guidance

and

Preparative Procedures

Version 1.0

15 October 2014

EDCS 1427627

Table of Contents

DOCUMENT INTRODUCTION

This document provides supporting evidence for an evaluation of a specific Target of Evaluation (TOE), the Cisco Catalyst 3850 Series Switches running IOS-XE 3.6.0E and Catalyst 6500 Series Switches running IOS 15.1(2)SY3. 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.

1. Introduction

This Operational User Guidance with Preparative Procedures documents the administration of the Cisco Catalyst 3850 Series Switches running IOS-XE 3.6.0E and Catalyst 6500 Series Switches running IOS 15.1(2)SY3 TOE certified under Common Criteria. The Cisco Catalyst 3850 Series Switches running IOS-XE 3.6.0E and Catalyst 6500 Series Switches running IOS 15.1(2)SY3 TOE may be referenced below as the Cat3850, Cat6K, TOE, Catalyst Switches or simply switch.

1.1 Audience

This document is written for administrators configuring and maintaining the TOE, specifically the IOS and IOS-XE 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 and IOS-XE software and the various operating systems on which you are running your network.

For using the IOS command-line interfaces refer to **[4]a** Using the Cisco IOS Command-Line Interface.

For using the IOS XE command-line interfaces refer to **[4]b** Using the Command-Line Interface in Cisco IOS XE Software.

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 the TOE 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 and IOS-XE.

1.3 Document References

This document makes reference to several Cisco Systems documents. The documents used are shown below.

Reference number	Document Name	Link

Reference number	Document Name	Link
[1]	Cisco Catalyst 6500 Series Switches Release Notes for Cisco IOS Release 15.1SY	http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.1SY/release_notes.html
[2]	Installation guides (Hardware documents) (a)Catalyst 6500 Series Switches Installation Guide (b) Catalyst 3850 Switch Hardware Installation Guide	 http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Chassis_Installation/Cat6500/6500_ins.html http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/hardware/installation/guide/3850_hig.pdf
[3]	(a) Configuration Fundamentals Configuration Guide, Cisco IOS Release 15.1S (b)Cisco IOS XE Configuration Fundamentals Configuration Guide, Release 2	http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/configuration/15-1s/cf-15-1s-book.pdf http://www.cisco.com/c/en/us/td/docs/ios/ios_xe/fundamentals/configuration/guide/2_xe/cf_xe_book.pdf
[4]	(a) Security Configuration Guide: Securing User Services Cisco IOS Release 15.0S (b) Securing User Services Configuration Guide Library, Cisco IOS Release 15SY (c) User Security Configuration Guide, Cisco IOS XE Release 3S	http://www.cisco.com/c/en/us/td/docs/ios/sec_user_services/configuration/guide/15_0s/sec_securing_user_services_15_0S_book.pdf http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/config_library/15-sy/secuser-15-sy-library.html http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/xe-3s/sec-usr-cfg-xe-3s-book.pdf
[5]	Network Management Configuration Guide, Cisco IOS Release 15.1S	http://www.cisco.com/c/en/us/td/docs/ios/netmgmt/configuration/guide/15_1s/nm_15_1s_boo

Reference number	Document Name	Link
		k.pdf
[6]	Cisco IOS Software Configuration Guide Cisco IOS Release 15.0SY	http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.0SY/configuration/guide/15_0_sy_swcg.pdf
[7]	(a) Cisco IOS Security Command Reference A to Z (b) Cisco IOS Security Command Reference (c) Cisco IOS Master Command List, All Releases	(a) 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 (b) http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_cr_book.pdf (c) http://www.cisco.com/c/en/us/td/docs/ios/mcl/allreleasemcl/all_book.html
[8]	Cisco Catalyst 6500 Series Switch FIPS 140-2 Level 2 Non-Proprietary Security Policy Cisco Catalyst 3850 FIPS 140-2 Level 2 Non-Proprietary Security Policy	http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2013.htm#1940
[9]	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
[10]	(a)Basic System management Configuration Guide, Cisco IOS Release 15.0SY	http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/configuration/15-0sy/bsm-15-0sy-book.pdf

Reference number	Document Name	Link
	(b)Basic System Management Configuration Guide, Cisco IOS XE Release 3S	http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/configuration/xe-3s/bsm-xe-3s-book.html
[11]	(a)Cisco IOS Release 15.x SY System Message Guide	http://www.cisco.com/en/US/docs/ios/15_0sy/system/messages/15sysmg.html
	(b)Switch Cisco IOS XE System Message[1]	http://www.cisco.com/en/US/docs/ios/system/messages/guide/xemsg01.html
[12]	(a)LAN Switching Configuration Guide, Cisco IOS Release 15.0SY	http://www.cisco.com/en/US/docs/ios-xml/ios/lanswitch/configuration/15-0sy/lsw_15_0_book.html
	(b)Cisco IOS LAN Switching Command Reference	(http://www.cisco.com/en/US/docs/ios/lanswitch/command/reference/lsw_book.html)
[13]	Secure Shell Configuration Guide, Cisco IOS Release 15.0SY	http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_ssh/configuration/15-0sy/sec-usr-ssh-15-0sy-book.pdf
[14]	(a)Loading and Managing System Images Configuration Guide, Cisco IOS Release 15S	http://www.cisco.com/en/US/docs/ios-xml/ios/sys-image-mgmt/configuration/15-s/sysimgmgmt-15-s-book.pdf
	(b)Loading and Managing System Images Configuration Guide Cisco IOS XE Release 3S (FTP steps)	http://www.cisco.com/en/US/docs/ios-xml/ios/sys-image-mgmt/configuration/xe-3s/sysimgmgmt-xe-3s-book.pdf

1.4 Supported Hardware and Software

Only the following hardware and software listed below is compliant with the Common Criteria Cisco Catalyst 3850 Series with Network Modules running IOS-XE 3.6.0E and

[1] The system messages is a comprehensive list of auditable events that may be configured/captured depending on the level of auditing that is configured. .

Catalyst 6500 Series with Supervisor Engine 2T (Sup2T) Switches running IOS 15.1(2)SY1SY3 EAL3 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 Catalyst Switches that comprise the TOE (Cisco Catalyst 3850 Series with Network Modules and Catalyst 6500 Series with Supervisor Engine 2T (Sup2T) Switches have 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 TOE consists of any one of a number of hardware configurations for the 3850 and the 6500 Series switch, each running the same version of IOS-XE and IOS software respectively. The switch chassis provides power, cooling, and backplane for the Network Module, Supervisor Engine, line cards, and service modules. The evaluated configurations consist of the following:

- Cisco Catalyst 3850
  - One or more chassis: WS-C3850-24T, WS-C3850-48T, WS-C3850-24P, WS-C3850-48P, WS-C3850-48F, WS-C3850-24U, WS-C3850-48U, WS-C3850-12S, WS-C3850-24S
  - Dimensions: 1.75 x 17.5 x 17.7/ 1.75 x 17.5 x 19.2
  - Weight: 15.9 – 17.6
  - One or more network module: C3850-NM-4-1G, C3850-NM-2-10G, C3850-NM-4-10G
  - Running IOS-XE 3.6.0E
- Cisco Catalyst 6500 Series Switches
  - One or more chassis: WS-C6503-E, WS-C6504-E, WS-C6506-E, WS-C6509-E, WS-C6513-E
    - Dimensions: 7 x 17.37 x 21.75/ 8.75 x 17.5 x 21.75/ 19.2 x 17.5 x 18/ 24.5 x 17.5 x 18.2/32.7 x 17.3 x 18.1
    - Weight: 33/40/50/60/102
  - One or two Supervisor 2T (Sup 2T) Cards (VS-S2T-10G or VS-S2T-10G-XL) per chassis
  - One or more Line Cards (note, line cards are not TSF enforcing): 40G Ethernet Interfaces, including WS-X6904-40G-2T (with DFC4) and WS-X6904-40G-2TXL (with DFC4XL)/10G Ethernet Interfaces, including WS-X6908-10G-2T (with DFC4), WS-X6908-10G-2TXL (with DFC4XL), WS-X6816-10T-2T (with DFC4), WS-X6816-10T-2TXL (with DFC4XL), WS-X6816-10G-2T (with DFC4), WS-X6816-10G-2TXL (with DFC4XL), WS-X6716-10T-3C, WS-X6716-10T-3CXL, WS-X6704-10GE, WS-X6708-10G-3C, WS-X6708-10G-3CXL, WS-X6716-10GT-3C, WS-X6716-10GT-3CXL/Gigabit Ethernet Interfaces, including WS-X6824-SFP-2T (with DFC4), WS-X6824-SFP-2TXL (with DFC4XL), WS-X6848-SFP-2T (with DFC4), WS-X6848-SFP-2TXL (with DFC4XL), WS-X6848-TX-2T (with DFC4), WS-X6848-TX-2TXL (with DFC4XL), WS-X6748-SFP, WS-X6724-SFP, WS-X6516A-GBIC, WS-X6408A-GBIC

- Running IOS 15.1(2)SY3

Cisco IOS and IOS-XE are a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. IOS XE represents the continuing evolution of Cisco's pre-eminent IOS operating system. IOS XE leverages the functionality that is provided by IOS, while adding new functionality and benefits, such as a set of infrastructure modules which define how software is installed, how processes are started and sequenced, how high-availability and software upgrades are performed and, lastly, how the applications are managed from an operational perspective. IOS XE looks and feels the same as the IOS. There is almost no change in the different feature configurations. The only minor difference in the CLI, and some outputs, is due to the customization that reflects the process-oriented approach of IOS XE, and the ability to use a multi-core CPU. For example, the "show version" command is changed to reflect the IOS XE naming convention, and licensing information.

Although IOS and IOS-XE performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself as described in the this document and the Cisco Catalyst 3850 Series Switches running IOS-XE 3.6.0E and Catalyst 6500 Series Switches running IOS 15.1(2)SY3. For example,

- Security audit – ensures that audit records are generated for the relevant events and can optionally be transmitted to a syslog
- Cryptographic support – ensures cryptography support for secure communications
- User Data Protection – ensures traffic is mediated by VLAN polices, access controls restrict administration access and packets transmitted from the TOE do not contain residual information from previous packets
- Identification and authentication – ensures 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 – ensures secure administrative services for management of general TOE configuration and the security functionality provided by the TOE
- Protection of the TSF - provides secure transmission when TSF data is transmitted between the TOE and other IT entities, is also able to detect replay of information received via secure channels (e.g. SSH), ensures updates have not been modified and are from a trusted source and maintains the date and time. that is used as the timestamp applied to audit records
- TOE access - ensures inactive sessions are terminated after an authorized administrator configurable time-period
- Trusted Path/Channel - a trusted path between the TOE and the CLI using SSHv2

1.5 Operational Environment

1.5.1 Required software for the operational environment

Component	Usage/Purpose Description for TOE performance
Management Workstation	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support

Component	Usage/Purpose Description for TOE performance
	TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.

1.5.2 Optional software for the operational environment:

Component	Usage/Purpose Description for TOE performance
NTP Server	The TOE supports communications with an NTP server to receive clock updates.
Syslog server	The syslog audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE.
Authentication Server	The authentication server (RADIUS and TACACS+) is used to provide centralized authentication and related auditing for one or more distributed instances of the TOE.

1.6 Excluded Functionality

Excluded Functionality and Rationale
SNMP does not enforce the required privilege levels. This feature is disabled by default and cannot be configured for use in the evaluated configuration. Including this feature would not meet the security policies as defined in the Security Target.
HTTP Server for web user interface management sends authentication data in the clear and does not enforce the required privilege levels. This feature is enabled by default. The HTTP Server needs to be disabled and should not be configured for use. Not including this feature does not interfere with the management of TOE as defined in the Security Target.
IEEE 802.11 Wireless Standards: The evaluated configuration of Catalyst Switches as described is this Security Target does not support implementing wireless local area network, as it requires additional hardware beyond what is included in the evaluated configuration.
VPN enabling and configuring VPN requires additional licenses beyond what is included in the evaluated configuration.
MAC address filtering restricts a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port. This feature is disabled by default and should not be configured for use, as it may interfere with the enforcement of the security policies as defined in the Security Target.
Flexible NetFlow is used for a traffic analysis and optimization, and SFRs do not include performance/optimization features. Not including this feature does not interfere with the enforcement of the security policies as defined in the Security Target.
Security Group Tags (SGT) are a 16-bit single label indicating the security classification of a source in the TrustSec domain and it is appended to an Ethernet frame or an IP packet. Not including this feature does not interfere with the enforcement of the security policies as defined in the Security Target.
TrustSec is classification and policy enforcement that is based on contextual identity of the endpoint versus its IP address. A Cisco TrustSec policy group called a Security Group Tag (SGT) is assigned to an endpoint, typically based on that endpoint's user, device, and location attributes. The SGT denotes the endpoint's

Excluded Functionality and Rationale
access entitlements, and all traffic from the endpoint will carry the SGT information. The SGT is used to make forwarding decisions. As such, this feature may interfere with the enforcement of the security policies as defined in the Security Target. Not including this feature does not interfere with the enforcement of the security policies as defined in the Security Target.
VLAN Trunking, 802.1Q tunneling, VLAN mapping, dynamic VLAN membership and the supporting protocols Dynamic Trunking Protocol (DTP) and VLAN Trunk Protocol (VTP). These features may be available by default, although not configured and should not be configured for use in the evaluated configuration. DTP is a point-to-point protocol that manages trunk auto-negotiations, as such configuring and enabling DPT would automatically configure trunks that could affect the security policies as defined in the Security Target. To ensure DTP is not configured to run, enter the following command in interface configuration mode, **no switchport mode**. VTP allows the configuration of one VLAN to be distributed through all switches in the domain that could affect the security policies. To ensure global VLAN Trunking Protocol (VTP) protocol is not configured to run; enter the following command in global configuration mode **no vtp**. Not including these features, do not interfere with the enforcement of the security policies as defined in the Security Target.
Cisco Discovery Protocol (CDP) allows network management applications to discover Cisco devices that are neighbors of already known devices, in particular, neighbors running lower-layer, transparent protocols such as SNMP. As a result, this protocol allows applications to send SNMP queries to neighboring devices. This feature may be available by default, though not configured and should not be configured for use in the evaluated configuration. To ensure CDP is not running, enter the following command in global configuration mode **no cdp enable**. Including this feature would not meet the security policies as defined in the Security Target. However, this protocol may be useful in troubleshooting and may be used when the TOE is no longer considered in the evaluated configuration.
Smart Install is a feature to configure IOS/IOS-XE Software and switch configuration without user intervention. The Smart Install uses dynamic IP address allocation to facilitate installation providing transparent network plug and play. This feature is not to be used as it could result in settings/configurations that would interfere with the enforcement of the security policies as defined in the Security Target.
Term Shell (Cisco IOS.sh) allows the use of shell scripting from the CLI. This feature may be available by default, although not configured and must not be configured for use in the evaluated configuration. Enabling and configuring this shell scripting may provide users access to privileges, commands and sensitive information, such as passwords and configuration settings that by default would not be available. Including this feature would not meet the security policies as defined

Excluded Functionality and Rationale
in the Security Target. For information on using Cisco IOS.sh and controlling access see Network Management Guide, Cisco IOS Release 15.1S at http://www.cisco.com/c/en/us/td/docs/ios/netmgmt/configuration/guide/15_1s/nm_15_1s_book.pdf

2. Secure Acceptance of the TOE

In order to ensure the correct TOE is received, the TOE should be examined to ensure that it 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 1: Evaluated Products and their External Identification

Product Name	External Identification
Cisco Catalyst 3850	Cisco Catalyst 3850
Cisco Catalyst 6503-E	Catalyst 6503-E

Product Name	External Identification
Cisco Catalyst 6504-E	Catalyst 6504-E
Cisco Catalyst 6506-E	Catalyst 6506-E
Cisco Catalyst 6509-E	Catalyst 6509-E
Cisco Catalyst 6513-E	Catalyst 6513-E

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. Software images are available from Cisco.com at the following: http://www.cisco.com/cisco/software/navigator.html [Login to CCO is required to download, but not to search.]
- The TOE ships with the correct software images installed.

Step 8 Once the file is downloaded, verify that it was not tampered with by using a MD5 utility to compute a MD5 hash for the downloaded file and comparing this with the MD5 hash for the image listed in Table 2: Evaluated Software Images below. Refer to Part 8 Loading and Maintaining System Images → MD5 File Validation **[14]**.

If the MD5 hashes do not match, contact Cisco Technical Assistance Center (TAC) http://tools.cisco.com/ServiceRequestTool/create/launch.do. [Login to CCO is required.]

As noted in **[4]** you may choose to not use MD5 digest verification because it is 256-bits long and the verification itself is manual; such as running a MD5 utility of your choice to compute the MD5 hash for the downloaded image file and then comparing the results against the image MD5 hash listed below. Therefore you can follow the steps to verify the image for

- IOS following Image Verification → Information About Image Verification → How To Use Image Verification **[4]a**

  Step 9 Copy (via ftp) the downloaded and verified software image from the trusted system as described in **[14]a**

  Once the file has been copied, it is recommended that you read and familiarize yourself with the Part 2: Configuration Using Setup and Autoinstall → Overview – Basic Configuration of a Cisco Networking Device before proceeding with the install **[14]a**. You may also want to familiarize yourself with **[7](a)** basic commands and **[3]a** fundamental Catalyst Switches and IOS concepts before proceeding with the installation and configuration of the TOE.

  To install and configure the TOE follow the instructions as described in **[3](a)** Loading and Maintaining System Images → Loading and Managing System Images → How to Work with and Manage System Images

  Start the TOE as described in **[3](a)**. Confirm the TOE loads the image correctly, completes internal self-checks and displays the cryptographic export warning on the console.

- IOS-XE you can follow the steps to verify the image following Image Verification → Information About Image Verification → How To Use Image Verification **[14]b**

  Step 9 Copy (via ftp) the downloaded and verified software image from the trusted system as described in **[4](c)**.

  Once the file has been copied, it is recommended that you read and familiarize yourself with the Part 2: Configuration Using Setup and Autoinstall → Overview – Basic Configuration of a Cisco Networking Device before proceeding with the install **[14](b)**. You may also want to familiarize yourself with **[7](a)** basic commands and **[3](b)** fundamental Catalyst Switches and IOS-XE concepts before proceeding with the installation and configuration of the TOE.

  To install and configure your Cat4K switch follow the instructions as described in **[3](b)** Configuration Using Setup and Autoinstall → Overview – Basic Configuration of a Cisco Networking Device → Cisco IOS EX Setup Mode. Depending on your organization and current network environment, at, Where to Go Next section, select either 'Using AutoInstall to Remotely Configure Cisco Networking Device' or Using Setup Mode to Configure a Cisco Networking Device'.

  Follow up with Managing Configuration Files **[3](b)** to save the configuration file.

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 **[7](a)** 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 **[14]**. 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 2: Evaluated Software Images

Software Version	Image Name	Image hash values
IOS-XE 3.6.0E	**cat3k_caa-universalk9.SPA.03.06.00.E.152-2.E.bin**	**308bdf0ac1b98032412a3b560b7a7302**
IOS 15.1(2)SY3	**s2t54-adventerprisek9-mz.SPA.151-2.SY3.bin**	**82ee2206e4b6d2108cf53e03bd416e01**

3. Secure Installation and Configuration

3.1 Physical Installation

Follow the TOE Hardware Installation Guide **[2](a)** or **[2](b)** for preparation of the physical site and hardware installation.

3.2 Initial Setup via Direct Console Connection

The TOE 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 Switch

After initially configuring and turning on the switch you are free to choose answers that fit your policies with the exception of the following values as noted in 1-4 below**.** It should be noted that the person that initial installs 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. 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.

The privilege level determines the functions the user can perform; hence the authorized administrator with the appropriate privileges. Furthermore, all users of the TOE are considered administrators and that the number of administrators created and their various levels of access are based on organizational requirements and policies. Following are a few examples how privileges can be configured for the various administrators in an organization. Furthermore, not all administrators require access to all commands and privileges. For example, not all administrators require access to commands associated with privilege levels above level 1, therefore passwords can be set to enable higher privilege levels and the enable passwords would not be provided to all administrators. Therefore careful consideration regarding assignment of administrative privileges should be based on organizational needs, policies and requirements.

For levels, level 0 is the most restrictive and 15 is the least restrictive.

For level 0, there are five commands associated with privilege level 0: disable, enable, exit, help, and logout. However, the level could be configured to allow a user to have access to the ‘show’ command.

Level 1 is normal EXEC-mode user privileges

Following is ***an example*** of how privileges are set, rules in setting privilege levels and assigning users to those privilege levels. **Note, that the administrator needs to have the appropriate privilege level and if required, applicable password to execute the commands**:

When setting the privilege level for a command with multiple words (commands), the commands starting with the first word will also have the specified access level. For example, if the **show ip route** command is set to level 15, the **show** commands and **show**

ip commands are automatically set to privilege level 15—unless they are individually set to different levels. This is necessary because a user cannot execute, for example, the **show ip** command unless the user also has access to **show** commands.

To change the privilege level of a group of commands, the **all** keyword is used. When a group of commands is set to a privilege level using the **all** keyword, all commands which match the beginning string are enabled for that level, and all commands which are available in submodes of that command are enabled for that level. For example, if the **show ip** keywords is set to level 5, **show** and **ip** will be changed to level 5 and all the options that follow the **show ip** string (such as **show ip accounting**, **show ip aliases**, **show ip bgp**, and so on) will be available at privilege level 5.

The **privilege** command is used to move commands from one privilege level to another in order to create the additional levels of administration. The default configuration permits two types of users to access the CLI. The first type of user is a person who is only allowed to access user EXEC mode. The second type of user is a person who is allowed access to privileged EXEC mode. A user who is only allowed to access user EXEC mode is not allowed to view or change the configuration of the networking device, or to make any changes to the operational status of the networking device. On the other hand, a user who is allowed access to privileged EXEC mode can make any change to a networking device that is allowed by the CLI.

Following is an ***example*** for setting the privilege levels for staff that are usually not allowed to run all of the commands available in privileged EXEC mode (privilege level 15) on a networking device. ***They are prevented from running commands that they are not authorized for by not being granted access to the password assigned to privileged EXEC mode*** or to other levels that have been configured on the networking device.

The steps and commands show setting privilege level 7 with access to two commands, clear counters and reload.

Step 1 **enable** password

Enters privileged EXEC mode. Enter the password when prompted.

Router> **enable**

Step 2 **configure terminal**

Enters global configuration mode.

Router# **configure terminal**

Step 3 **enable secret level** *level password*

Configures a new enable secret password for privilege level 7.

Router(config)# **enable secret level** *7 Zy72sKj*

Step 4 **privilege exec level** *level command-string*

Changes the privilege level of the clear counters command from privilege level 15 to privilege level 7.

Router(config)# **privilege exec level** *7 clear counters*

Step 5 **privilege exec all level** *level command-string*

Changes the privilege level of the reload command from privilege level 15 to privilege level 7.

Router(config)# **privilege exec all level** *7 reload*

Step 6 **end**

Exits global configuration mode.

Router(config)# **end**

The following example shows the enforcement of the settings above and privilege levels.

Step 1 **enable** *level password*

Logs the user into the networking device at the privilege level specified for the level argument.

Router> **enable** *7 Zy72sKj*

Step 2 **show privilege**

Displays the privilege level of the current CLI session

Router# **show privilege**

Current privilege level is 7

Step 3 **clear counters**

The clear counters command clears the interface counters. This command has been changed from privilege level 15 to privilege level 7.

Router# **clear counters**

Clear "show interface" counters on all interfaces [confirm]

Router#

02:41:37: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console

Step 4 **clear ip route** *

The *ip route* argument string for the **clear** command should not be allowed because it was not changed from privilege level 15 to privilege level 7. Note, the * parameter essentially removes all ip routes configured

Router# **clear ip route ***

^

% Invalid input detected at '^' marker.

Router#

Step 5 **reload in time**

The reload command causes the networking device to reboot.

Router# **reload in** *10*

Reload scheduled in 10 minutes by console

Proceed with reload? [confirm]

Router#

***

*** --- SHUTDOWN in 0:10:00 ---

***

02:59:50: %SYS-5-SCHEDULED_RELOAD: Reload requested for 23:08:30 PST Sun Mar 20

Step 6 **reload cancel**

The reload cancel terminates a reload that was previously setup with the reload in time command.

Router# **reload cancel**

***

*** --- SHUTDOWN ABORTED ---

***

04:34:08: %SYS-5-SCHEDULED_RELOAD_CANCELLED: Scheduled reload cancelled at 15:38:46 PST

Sun Mar 27 2005

Step 7 **disable**

Exits the current privilege level and returns to privilege level 1.

Router# **disable**

Step 8 **show privilege**

Displays the privilege level of the current CLI session

Router> **show privilege**

Current privilege level is 1

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. 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, associated roles and privilege levels as used in the example above **[3](a)(b) [4](a)(b)(c) [7](a)**.

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 …" **[7](a)**

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. **[7](a)**

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 (in section 3.3.1), steps will be given to allow ssh into the vty lines. For additional information refer to "password (line configuration)" in **[7](a).**

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 **[7](a)**.

3.2.2 Saving Configuration

IOS/IOS-XE 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. For further detail refer to Managing Configuration Files in **[3](a)(b)**.

Saving configuration files may be achieved by either using the **write memory** command or the **copy system:running-config nvram:startup-config** command. 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 **[7](a)**.

3.2.3 Secure Remote Management

The TOE provides SSH-protected communications for remote management sessions.

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. This configuration enables SSH management on the TOE, with the **hostname**, **crypto key generate rsa**, and **ip ssh version 2** commands, and restricts remote access with the **line console** (or vty) **0 15** and **transport input ssh** commands in **[3] [4]** and **[7]**. 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 **[7]**.

Note, automated processes using TCL scripting or other scripting services should not be used in the evaluated configuration. Configuring automated scripts to run only audits the execution of the TCL script and not the changes that were processed by the sTCL script.

3.2.4 Administration of Cryptographic Self-Tests

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

Power-on Self-Tests:

- IOS Known Answer Tests:
  - AES KAT
  - Triple-DES KAT
  - SHA-1 KAT
  - HMAC KAT
- Power up bypass test
- Firmware Integrity Test
- Diffie-Hellman test

Conditional Self-Tests:

- Conditional Bypass Test
- Continuous Random Number Generator test on all RNGs

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

The command is **test crypto self-test** as described in **[7](a)**. Additional information regarding Administration of Cryptographic Self-Tests review can be found in Self-Test section of **[8]**.

3.2.5 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: example

```
Router# reload /verify
Verifying file integrity of bootflash:c7200-kboot-mz.121-8a.E
%ERROR:Signature not found in file bootflash:c7200-kboot-mz.121-8a.E.
Signature not present. Proceed with verify? [confirm]
Verifying file disk0:c7200-js-mz
.....................................................................
.....................................Done!
Embedded Hash MD5 :CFA258948C4ECE52085DCF428A426DCD
Computed Hash MD5 :CFA258948C4ECE52085DCF428A426DCD
CCO Hash MD5 :44A7B9BDDD9638128C35528466318183
```

Signature Verified
Proceed with reload? [confirm]

This functionality cannot be disabled by any administrator **[4]**.

The privileged administrator can also run the **show diagnostic** command to display the online diagnostic test results and the supported test suites **[7](a) [8]**.

3.2.6 Access Control and Lockout

The TOE must be configured to use a username and password for each administrator and one password for the enable command. To have passwords stored as a SHA-256 hash, use the "service password-encryption" command in config mode **[7](a)**:

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

service password-encryption

Once that service has been enabled, passwords can be entered in plaintext, or as SHA-256 hash values, and will be stored as SHA-256 hash values in the configuration file when using the "username" command. 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 by using the following command:

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

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> | **password** <encryption-type encrypted-password>}

or if the password encryption service has not been enabled use

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

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>

Note to prevent administrators from choosing insecure passwords, each password must be at least 15 characters long. Use the following command to set the minimum length to 15 or greater. Refer to Section 4.2 in this document or **[7](a)** for configuring strong

passwords using the **aaa-common-criteria policy** command. Also refer to **[7](a)** for any of the following commands.

Usernames should also be limited to 15 alphanumeric characters, excluding all special characters. This will limit the possibility of usernames being truncated in audit and associated syslog records.

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

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

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

Switch(config)#**line console**

Switch(config-line)#**login authentication local**

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:

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.

The number of attempts is based on the organizations policy, though best practices recommend three (3) attempts before locking the user account.

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 and TACACS+), 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), while TACACS+ encrypts the entire packet body except the header). This AAA server must only be accessible via the protected internal network that is meant to be separated effectively from unauthorized individuals and user traffic (preferably through a secured tunnel); one that is in a controlled environment where there is physical protection and implementation of security policies can be enforced..

The switch provides the capability to support the following routing protocols BGPv4, EIGRP, EIGRPv6 for IPv6 and OSPFv2. EIGRP and EIGRPv6 supports routing updates with IPv6 or IPv4, as does BGPv4, while and OSPFv2 routing protocol support routing updates for IPv4 only. Each of these protocols supports authentication by transmission of MD5-hashed password strings, which each neighbor router uses to authenticate others. For additional security, it is recommended router protocol traffic also be isolated to separate VLANs.

3.3.1 Remote Administration Protocols

To only allow SSHv2 for remote administrator sessions, use the **transport input ssh** command. This command disables telnet by only allowing ssh connections for remote administrator access. Note, in the evaluated configuration, the TOE does not act as an SSH client and should not be configured to act as an SSH client. The SSH client is provided by the IT operational environment to be used for remote administration.

- Telnet is enabled by default and 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 **[7](a) and [13]**.

  line vty 0 15

  transport input ssh

- SSHv2 must be used. To enable sshv2, use the "**ip ssh version 2**" command **[7](a)**. Note before SSH is configured, the rsa keys need to be generated for the SSH server using the following command, with an RSA key size of 2048 bits **[7](a) and [13]**.

  crypto key generate rsa [7](a) Commands A to C -> crypto isakmp aggressive-mode disable -> crypto key generate

- To ensure the TOE is configured not to support diffie-hellman-group1-sha1 key exchange using the following command: :

  ip ssh dh min size 2048 [13] or **[7](a)** Commands D to L -> ip source-track through ivrf

  In addition, configure your environment ssh client to not offer diffie-hellman-group1-sha1 key exchange; to offer for dh-group-14 as the first choice. To configure the SSH client to support only diffie-hellman-group14-sha1 key exchange, using Putty as the environment SSH Client, 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 configured to use SSHv2, the following four encryption options are available for use in IOS, aes128-cbc, aes192-cbc, aes256-cbc, and 3des-cbc and all are permitted in the evaluated configuration except for aes192-cbc and 3des-cbc. IOS does not provide an option to restricting which algorithm is negotiated for inbound SSHv2 connections. Those restrictions must be configured on the SSH Client side. Since security-relevant use of the SSH connection only occurs after the session parameters are negotiated (when authentication parameters are being exchanged during login, and after successful authentication), the TOE administrators should configure their SSH clients to either:

- not establish connections using AES192-CBC and/or 3DES-CBC; or
- warn about potential use of AES192-CBC and/or 3DES-CBC, at which point the administrator must reject the session and reconfigure the client, or use a different client.

To configure an environment Linux-based SSH client to support only the following specific encryption algorithms AES-CBC-128 and AES-CBC-256 the following commands can be used. Configure a SSH client to support only the following specific encryption algorithms:

- AES-CBC-128
- AES-CBC-256

TOEEnvironmentSSHClient#ssh -l cisco -c aes128-cbc 1.1.1.1

TOEEnvironmentSSHClient #ssh -l cisco -c aes256-cbc 1.1.1.1

To configure an environment Linux-based SSH client to support message authentication. Only the following MACs are allowed and "None" for MAC is not allowed:

- hmac-sha1
- hmac-sha1-96

TOEEnvironmentSSHClient #ssh -l cisco -m hmac-sha1-160 1.1.1.1

TOEEnvironmentSSHClient #ssh -l cisco -m hmac-sha1-96 1.1.1.1

TOEEnvironmentSSHClient #ssh -l cisco -m hmac-sha2-256 1.1.1.1

TOEEnvironmentSSHClient #ssh -l cisco -m hmac-sha2-512 1.1.1.1

To verify the proper encryption algorithms are used for established connections, use the **show ssh sessions** command **[7](a)**:

TOE-common-criteria# **show ssh sessions**

Note: To disconnect SSH sessions, use the **ssh disconnect** command:

TOE-common-criteria# **ssh disconnect**

- 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) **[7](a) and [13]**.

  ip ssh authentication-retries <integer> (note in the evaluated configuration is limited to 3. The default is 3, with a maximum of 5) **[7](a) and [13]**.

- HTTP server was not evaluated and must be disabled **[7](a)**:

  no ip http <host name or IP address>

- HTTPS server was not evaluated and must be disabled **[7](a)**:

  no ip http <host name or IP address>

- SNMP server was not evaluated and must be disabled **[7](a)**:

  no snmp-server

- Smart Install was not evaluated and must be disabled **[7](a)**:

  hostname(config)# no vstack.

3.3.2 Authentication Server Protocols

RADIUS **or** TACACS+ (outbound) for authentication of TOE administrators to remote authentication servers are disabled by default but can be enabled by administrators in the evaluated configuration.

To configure RADIUS **or** TACACS+ refer to **[3] [6] [7](a)** for configuring remote (AAA) authentication using RADIUS or TACACS+. 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. It is recommended to read this section to become familiar with remote authentication concepts prior to configuration.

3.3.3 Routing Protocols

As noted above, the switch provides support for the following routing protocols BGPv4, EIGRP, EIGRPv6 for IPv6 and OSPFv2. The hash mechanism is implemented as specified in the relevant RFCs:

- BGPv4 uses MD5 for authentication of routing updates as defined in RFC 2385 (Protection of BGP Sessions via TCP MD5 Signature Option).
- EIGRP and EIGRPv6 (Cisco proprietary) uses MD5 for authentication of routing updates.
- OSPFv2 uses MD5 for authentication of routing updates as defined in Appendix D of RFC 2328 (OSPF version 2).

Routing tables for IPv4 and IPv6 can be created and maintained manually using static routes configured by the administrator. Use of routing protocols in IPv4 or IPv6 is not required to support or enforce any TOE security functionality including filtering of IPv4

or IPv6 traffic. BGPv4 and EIGRP and EIGRPv6 supports MD5-authenticated routing updates with IPv6 or IPv4 while OSPFv2 routing protocol support MD5-authenticated routing updates for IPv4 only.

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 **[9]** for configuration of the routing protocol.

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 can be found in **[11]**.

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. Refer to the "logging enabled" command in **[7](a)**, or "Configure Logging System Messages" in **[10]**:

  Switch(config)#**archive**

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

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

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

  * Optional - 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)#**hidekeys** (this ensures the password and keys are not displayed in the audit records)

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**

- Set the size and severity of the local logging buffer. The local logging buffer size can be configured from a range of 4096 (default) to 2147483647 bytes. It is noted to not make the buffer size too large because the TOE could run out of memory for other tasks.

  Switch(config)#**logging buffer 150000000**

  Switch(config)#**logging buffer debug**

- To specify the severity level for logging to the syslog host, use the **logging trap** command. Level 7 will send all logs required in the evaluation up to the debug level logs (as enabled in step 3 above) to the syslog server:

  Switch(config)#**logging trap 7**

  WARNING: this setting has the ability to generate a large number of events that could affect the performance of your device, network, and syslog host.

- 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 **or** tacacs debugging in privileged EXEC mode enter the following:

  Switch#debug radius authentication or debug tacacs authentication

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

  Switch#debug ip ssh detail

  Note, after a reboot the debugging command above will need to be re-entered to ensure logging of the ssh sessions.

- Enable Network Time Protocol (NTP) debugging in privileged EXEC mode enter the following:

  Switch#debug ntp all

- 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

  Switch(config)#**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 view the audit records after they have been saved, use the privileged EXEC command to display its contents

  more flash: ***filename***

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

  Switch#logging trap debugging

  Note, if it discovered the required events are not audited after the reboot, all of the debugging commands above will need to be re-entered.

- Syslog (outbound) for transmission of syslog events to a remote syslog server is disabled by default. To configure syslog, refer to the instructions below in 'Remote Logging".

Note: 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 **[7](a)**. Verify that you have ample CPU available before you begin the debugs and use the debug commands with caution.

Note, automated processes using TCL scripting or other scripting services should not be used in the evaluated configuration. Configuring automated scripts to run only audits the execution of the TCL script itself and not any changes to the system that may have been processed by the TCL script.

In order to ensure that all commands executed by administrators are captured in a syslog record, the following Cisco Embedded Event Manager script can be used. In the config mode (config terminal), enter configuration commands, one per line, ending with CNTL/Z at the CLI as follows:

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

Switch(config-applet)#**event cli pattern ".*" sync yes**

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

Switch(config-applet)#**action 2.0 if $_cli_privilege gt "0"**

Switch(config-applet)#**action 3.0 syslog msg "host[$_info_routername] user[$_cli_username] port[$_cli_tty] exec_lvl[$_cli_privilege] command[$_cli_msg] Executed"**

Switch(config-applet)#**action 4.0 end**

Switch(config-applet)#**action 5.0 set _exit_status "1"**

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

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

3.4.1 Remote Logging

To protect against audit data loss the TOE should be configured to send the audit records to an external TCP syslog server. If syslog servers are used, they must only be accessible via the protected internal network that is meant to be separated effectively from unauthorized individuals and user traffic (preferably through a secured tunnel); one that is in a controlled environment where there is physical protection and implementation of security policies can be enforced

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 the following commands must be entered at the CLI to configure this option. Refer to "Logging System Messages" in **[3] [6]** for available settings and options; perform this task in privileged mode. It is recommended to read the entire section to become familiar with the concept and configuration before configuring local and remote logging.

Switch# **configure terminal**
Switch(config)#**set logging server *ip_addr*** (the IP address of the syslog server)
Switch(config)#**set logging server severity *server_severity level*** (you can limit the messages logged to the syslog server. By default syslog servers receive informational messages and lower)
Switch(config)#**logging facility *facility type*** (the UNIX system facilities supported; the default is local7)
Switch(config)#**set logging server enable** (enables the system message logging to the configured syslog server (a maximum of three syslog servers can be configured)
Switch(config)#**end**

To configure the logs to be sent to a syslog server:

Switch(config)#**logging host <ip address of syslog server>**

3.4.2 Reviewing Audited Events

The TOE 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 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] [7]**. 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.

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FCS_SSH_EXT.1	Failure to establish an SSH session Establishment/ Termination of an SSH session	Reason for failure Non-TOE endpoint of connection (IP address) for both successes and failures.	• Failure to establish a SSH Session. o IP address of remote host o 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 a SSH session o 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 • Termination of a SSH session. Output on ssh device [root@swr-ucs200-3 ~]# ssh -c aes256-cbc -l testuser 20.20.20.1 Password: >exit Connection to 20.20.20.1 closed by remote host. Connection to 20.20.20.1 closed.
FDP_ACF.1	All decisions on request for access control (execute a command)	None	*May 4 08:36:16.214 MST: %SEC_LOGIN-SW1-5-LOGIN_SUCCESS: Login Success [user: testadmin] [Sour ce: 0.0.0.0] [localport: 0] at 08:36:16 MST Fri May 4 2012 *May 4 08:36:25.778 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:!exec: enable *May 4 08:36:37.782 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:interface GigabitEthernet0 *May 4 08:36:47.446 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:mac access-group macfilter in *May 4 08:36:57.382 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:no mac access-group macfilter in *May 4 08:36:58.590 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:exit *May 4 08:38:45.910 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:username admin5 privilege 5 password admin

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			*May 4 08:39:01.350 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:privilege exec level 5 conf t *May 4 08:39:01.398 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:privilege configure all level 5 mac access-group *May 4 08:39:01.442 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:privilege exec level 5 show mac access-group *May 4 08:39:01.486 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:privilege configure level 5 no mac access-group *May 4 08:39:01.534 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:privilege exec level 5 show show run | include *May 4 08:39:01.570 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:privilege configure level 5 exit *May 4 08:59:29.562 MST: %SEC_LOGIN-SW1-5-LOGIN_SUCCESS: Login Success [user: admin5] [Source: 0.0.0.0] [localport: 0] at 08:59:29 MST Fri May 4 2012 *May 4 08:59:31.422 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:admin5 logged command:!exec: enable failed *May 4 08:59:40.558 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:admin5 logged command:interface GigabitEthernet1/6/3 *May 4 09:04:31.598 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:admin5 logged command:mac access-group macfilter in *May 4 09:04:46.186 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:admin5 logged command:no mac access-group macfilter in
FDP_IFF.1(2)	All decisions on requests for information flow.	None.	Logs for the permitted and denied tcp packets step 11: Apr 19 2012 19:57:11 UTC: %SEC-6-IPACCESSLOGP: list 110 permitted tcp

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			10.1.1.10(1877) -> 172.18.51.202(21), 1 packet Apr 19 2012 19:57:12 UTC: %SEC-6-IPACCESSLOGP: list 110 permitted tcp 10.1.1.10(1878) -> 172.18.51.202(21), 1 packet Apr 19 2012 19:57:14 UTC: %SEC-6-IPACCESSLOGP: list 110 permitted tcp 10.1.1.10(1880) -> 172.18.51.202(21), 1 packet Apr 19 2012 20:05:15 UTC: %SEC-6-IPACCESSLOGP: list 110 denied tcp 10.1.1.10(2476) -> 172.18.51.202(21), 1 packet Apr 19 2012 20:05:17 UTC: %SEC-6-IPACCESSLOGP: list 110 denied tcp 10.1.1.10(2478) -> 172.18.51.202(21), 1 packet Apr 19 2012 20:05:18 UTC: %SEC-6-IPACCESSLOGP: list 110 denied tcp 10.1.1.10(2479) -> 172.18.51.202(21), 1 packet
FDP_IFF.1(3)	IP packet flows denied by VACL	None	Apr 27 10:41:56.847 MST: %SEC-SW1-6-IPACCESSLOGP: list 101 denied tcp 100.0.1.50(54922) -> 100.0.2.50(21), 1 packet
FIA_UAU.2	All use of the authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).	Audit events in FIA_UAU_EXT.5
FIA_UAU_EXT.5	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: ASR-SL-491>? 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-

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			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.
FIA_UID.2	All use of the identification mechanism.	Provided user identity, origin of the attempt (e.g., IP address).	Audit events in FIA_UAU_EXT.5
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	None.	*May 4 10:03:30.431 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:hostname TOE -security *May 4 10:04:14.975 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:interface Gi gabitEthernet1/6/3 *May 4 10:04:20.855 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:switchport a ccess vlan 891 *May 4 10:04:25.591 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:switchport m ode access *May 4 10:04:28.099 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:shutdown *May 4 10:04:28.119 MST: %LINK-SW1-5-CHANGED: Interface GigabitEthernet1/6/3, changed state to administratively down *May 4 10:04:28.123 MST: %LINEPROTO-SW1-5-UPDOWN: Line protocol on Interface GigabitEthernet1/6/3, changed state to down *May 4 10:04:30.131 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:no shutdown *May 4 10:04:30.171 MST: %LINK-SW1-3-UPDOWN: Interface GigabitEthernet1/6/3, changed state to down *May 4 10:37:27.087 MST: %SEC_LOGIN-SW1-5-LOGIN_SUCCESS: Login Success [user: testuser] [Source: 0.0.0.0] [localport: 0] at

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			10:37:27 MST Fri May 4 2012 *May 4 10:37:35.263 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testuser logged command:!exec: enable failed *May 4 10:40:50.000 MST: %SYS-SW1-6-CLOCKUPDATE: System clock has been updated from 10:40:30 MST Fri May 4 2012 to 10:40:50 MST Fri May 4 2012, configured from console by testadmin on console. .May 4 10:41:34.471 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:username admin5 password admin .May 4 10:41:34.471 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:!config: USER TABLE MODIFIED .May 4 10:41:53.531 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:username admin5 privilege 5 password admin .May 4 10:41:53.531 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:!config: USER TABLE MODIFIED .May 4 10:41:58.323 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:no username admin5 .May 4 10:41:59.927 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:username admin5 privilege 5 password admin .May 4 10:41:59.927 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:!config: USER TABLE MODIFIED .May 4 10:42:09.291 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:privilege exec level 5 conf t .May 4 10:42:09.331 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:privilege configure level 5 clock set .May 4 10:42:09.367 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			logged command:privilege configure level 5 exit .May 4 10:43:00.799 MST: %SYS-SW1-5-CONFIG_I: Configured from console by testadmin on console .May 4 10:43:10.431 MST: %SEC_LOGIN-SW1-5-LOGIN_SUCCESS: Login Success [user: admin5] [Source: 0.0.0.0] [localport: 0] at 10:43:10 MST Fri May 4 2012 .May 4 11:05:21.587 MST: %SYS-SW1-5-CONFIG_I: Configured from console by admin5 on console .May 4 11:05:27.075 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:admin5 logged command:!exec: enable .May 4 11:05:47.995 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:admin5 logged command:no ntp max-associations .May 4 11:06:01.443 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:admin5 logged command:ntp authentication-key 100 md5 attack .May 4 11:06:06.987 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:admin5 logged command:ntp trusted-key 100 .May 4 11:06:14.703 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:admin5 logged command:ntp authenticate .May 4 11:06:24.295 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:admin5 logged command:ntp server 10.1.1.10 version 3 key 100 prefer .May 4 11:06:26.739 MST: %SYS-SW1-5-CONFIG_I: Configured from console by admin5 on console
FMT_MSA.3(1)(2)	Modifications of the default setting of permissive or restrictive rules and all modifications of the initial values of security	None.	May 4 08:36:16.214 MST: %SEC_LOGIN-SW1-5-LOGIN_SUCCESS: Login Success [user: testadmin] [Sour ce: 0.0.0.0] [localport: 0] at 08:36:16 MST Fri May 4 2012 *May 4 08:36:25.778 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:!exec: enable *May 4 08:36:37.782 MST: %PARSER-SW1-

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
	attributes.		5-CFGLOG_LOGGEDCMD: User:testadmin logged command:interface GigabitEthernet0 *May 4 08:36:47.446 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:mac access-group macfilter in *May 4 08:36:57.382 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:no mac access-group macfilter in *May 4 08:36:58.590 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:exit *May 4 08:38:45.910 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:username admin5 privilege 5 password admin *May 4 08:39:01.350 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:privilege exec level 5 conf t *May 4 08:39:01.398 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:privilege configure all level 5 mac access-group *May 4 08:39:01.442 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:privilege exec level 5 show mac access-group *May 4 08:39:01.486 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:privilege configure level 5 no mac access-group *May 4 08:39:01.534 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:privilege exec level 5 show show run | include *May 4 08:39:01.570 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:testadmin logged command:privilege configure level 5 exit *May 4 08:59:29.562 MST: %SEC_LOGIN-SW1-5-LOGIN_SUCCESS: Login Success [user: admin5] [Source: 0.0.0.0] [localport: 0] at 08:59:29 MST Fri May 4 2012 *May 4 08:59:31.422 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:admin5

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			logged command:!exec: enable failed *May 4 08:59:40.558 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:admin5 logged command:interface GigabitEthernet1/6/3 *May 4 09:04:31.598 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:admin5 logged command:mac access-group macfilter in *May 4 09:04:46.186 MST: %PARSER-SW1-5-CFGLOG_LOGGEDCMD: User:admin5 logged command:no mac access-group macfilter in
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt (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. • One audit record for NTP changing the time: Jun 20 09:52:39.622: NTP Core(NOTICE): Clock is synchronized.
FPT_TST_EXT.1	Indication that TSF self-test was completed.	Any additional information generated by the tests beyond "success" or "failure".	Jan 23 2013 06:53:24.570: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Self test activated by user: admin) Jan 23 2013 06:53:24.670: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Software checksum ... passed)

3.4.3 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 **[6] [7](a)**.

3.5 Information Flow Policies - ACL

The evaluated configuration of the TOE is initially configured with a permissive default setting that allows all traffic to pass through the TOE.

Access lists must be configured on the TOE to prevent spoofing of external or internal addresses through the opposite interface and also to block broadcast source address and loopback source address traffic. In addition, traffic to the management interface from untrusted sources should also be blocked.

Note, *these access lists must be integrated with the defined security policy for your TOE switch. Enabling just these access lists with no permits will result in traffic being dropped.*

A privileged authorized administrator may manipulate the ACLs using the commands "ip inspect", "access-list" and "access-group" as described in **[7]**.

In this example, we are assuming that interface GigabitEthernet0/0 is the external interface, and is assigned an IP address of 10.200.1.1. Interface GigabitEthernet0/1 is the internal interface and is assigned an IP address of 10.100.1.1.

To prevent the passing of traffic with an internal source address on the external Interface, apply the following access control list to the external interface:

Switch# **configure terminal**

Switch(config)# **access-list 199 deny ip 10.100.0.0 0.0.255.255 any log-input**

To prevent the passing of traffic with an external source address on the internal Interface, apply the following access control list to the internal interface:

Switch# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)# **access-list 100 deny ip 10.200.0.0 0.0.255.255 any log-input**

To prevent the passing of traffic with a broadcast or loopback address on either interface, apply the following access control list to both interfaces:

Switch# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)# **access-list 100 deny ip 224.0.0.0 15.255.255.255 any log-input**

Switch(config)# **access-list 100 deny ip 255.255.255.255 0.0.0.0 any log-input**

Switch(config)# **access-list 100 deny ip 127.0.0.0 0.255.255.255 any log-input**

Switch(config)# **access-list 199 deny ip 224.0.0.0 15.255.255.255 any log-input**

Switch(config)# **access-list 199 deny ip 255.255.255.255 0.0.0.0 any log-input**

Switch(config)# **access-list 199 deny ip 127.0.0.0 0.255.255.255 any log-input**

If remote administration is required, ssh has to be explicitly allowed through either the internal or external interfaces.

Switch# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)# **access-list 199 permit tcp host 10.200.0.1 host 10.200.1.1 eq 22 log-input**

To close ports that don't need to be open and may introduce additional vulnerabilities, implement the following acl:.

Switch(config)# **access-list 100 deny 132 any any log-input**

Switch(config)# **access-list 199 deny 132 any any log-input**

To apply the acls to the interfaces:

Switch(config)# **interface GigabitEthernet0/0**

Switch(config-if)# **ip access-group 199 in**

Switch(config)# **interface GigabitEthernet0/1**

Switch(config-if)# **ip access-group 100 in**

3.6 Information Flow Policies - VLAN

Following are some VLAN configuration guidelines.

- Switches running the IP Base or IP Services feature set support 1005 VLANs. Switches running the LAN base feature set support 255 VLANs.
- Normal-range VLANs are identified with a number between 1 and 1001. VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs. ***Note***, *the switch does not support Token Ring or FDDI media*
- VLAN configurations for VLANs 1 to 1005 are always saved in the VLAN database.

A privileged authorized administrator may define the VLANs as described in "Virtual Local Area Networks (VLANs)" and "Private VLANs" in **[6]**.

3.7 Information Flow Policies - VACL

The evaluated configuration supports VACLs (VLAN ACLs), which can filter traffic traversing VLANs on the TOE based on IP addressing and MAC addressing. This determines whether to forward or drop it, on the basis of criteria specified within the VLANs and access lists applied to the interfaces through which the traffic would enter and leave the switch.

Unlike regular Cisco IOS ACLs that are assigned to Layer 3 interfaces only and have effect on routed packets only, a VACL is assigned to a VLAN and its rules affect all traffic traversing ports in that VLAN. As with ACLs for Layer 3 interfaces, IOS controls the flow of IP traffic by matching information contained in the headers of connection-oriented or connection-less IP packets against a set of rules specified by the authorized administrator in the IP flow control policies.

VACLs provide traffic control for frames/packets that traverse ports with VLANs to which VACLs are applied, whether bridged within a VLAN or routed into or out of a VLAN.

- When a VACL is applied to a VLAN, all packets traversing a port in that VLAN are checked against this VACL.
- When a VACL is applied to a VLAN, and an ACL is applied a routed interface in that VLAN, a packet entering the TOE through a port in the VLAN is first checked against the VACL, and, if permitted, is then checked against the inbound/ingress ACL applied to the Layer 3 interface.
- When the packet is routed within IOS to another VLAN, it is first checked against the outbound/egress ACL applied to the layer 3 interface, and, if

permitted, is then checked against the VACL configured for the destination VLAN.

The following example shows how to define and apply a VLAN access map labeled "*vmap4"* to VLANs 5 and 6 that causes the VLAN to forward an IP packet if the packet matches the conditions defined in access list labled "*al2"*:

```
Switch(config)# vlan access-map vmap4
Switch(config-access-map)# match ip address al2
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan filter vmap4 vlan-list 5-6
```

For more detail on configuration of VACLs, refer to "VLAN ACLs (VACLs)" in **[6]**.

In addition to the policies described above, you may want to consider setting Quality of Service (QoS) rate limits and/or a Control Plane Policy (CoPP). Both of these options protect the TOE from unnecessary or DoS traffic while providing priority to important control plane and management traffic. For more information refer to the Security Chapter in the Release 15.1SY Supervisor Engine 2T Software Configuration Guide available at http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T/ios_acl_support.html and the QoS Chapter in the Consolidated Platform Configuration Guide, Cisco IOS XE 3E (Catalyst 3850 Switches) available at http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3e/consolidated_guide/configuration_guide/b_consolidated_3850_3e_cg/b_consolidated_3850_3e_cg_chapter_01001011.html.

4. Secure Management

4.1 User Roles

The TOE maintains administrative privilege level and non-administrative access. Non-administrative access is granted to authenticated neighbor routers for the ability to receive updated routing tables per the information flow rules. There is no other access or functions associated with non-administrative access. The administrative privilege levels include:

- Administrators are assigned to privilege levels 0 and 1. Privilege levels 0 and 1 are defined by default and are customizable. These levels have a very limited scope and access to CLI commands that include basic functions such as login, show running system information, turn on/off privileged commands, logout.
- Semi-privileged administrators equate to any privilege level that has a subset of the privileges assigned to level 15; levels 2-14. These levels are undefined by default and are customizable.
- Privileged administrators are equivalent to full administrative access to the CLI, which is the default access for IOS privilege level 15.

Refer to Section 3.2.1 in this document.

4.2 Passwords

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

- At least eight characters long
- 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

This requirement applies to the local password database and on the password selection functions provided by the TOE, but remote authentication servers may have pre-configured passwords which do not meet the quality metrics. The above quality metrics are guidelines to follow, not necessarily enforceable.

The TOE can enforce the use of strong passwords by using options listed below with the "**aaa common-criteria policy**" command. To view the current policy use, "**show aaa common-criteria policy**" command **[7]a** Cisco IOS Security Command Reference: Commands A toC -> 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 **[7]a** 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 options are available:

- char-change--Number of changed characters between old and new passwords. The range is from 1 to 64.
- lifetime--Configure the maximum lifetime of a password by providing the configurable value in years, months, days, hours, minutes, and seconds. If the lifetime parameter is not configured, the password will never expire. Note: to ensure the lifetime settings are accurately enforced, time (clock) must be set to UTC (without day-light/summer settings). The following commands will set the TOE timezone to UTC:
  - Switch(config)#clock timezone UTC +0
  - Switch(config)#no clock summer-time UTC
  - Switch(config)#end
- lower-case--Number of lowercase characters. The range is from 0 to 64.
- upper-case--Number of uppercase characters. The range is from 0 to 64.
- min-length--Minimum length of the password. The range is from 1 to 64.
- max-length--Maximum length of the password. The range is from 1 to 64.
- numeric-count--Number of numeric characters. The range is from 0 to 64.
- special-case--Number of special characters. The range is from 0 to 64.

To store passwords in encrypted form in the configuration file, use the "**service password-encryption**" command **[7]**.

Administrative passwords, including any "enable" password that may be set for any privilege level, must be stored in non-plaintext form. To have passwords stored as a SHA-256 hash, use the "**service password-encryption**" command **[7]** in config mode.

Switch(config)#**service password-encryption**

Once that service has been enabled, passwords can be entered in plaintext, or has SHA-256 hash values, and will be stored as SHA-256 hash values in the configuration file when using the "username" command.

Switch(config)#**username** *name* {**password** *password* | **password** *encryption-type encrypted-password*}

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:

TOE-common-criteria(config)#**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.*

4.3 Clock Management

Clock management is restricted to the privileged administrator.

The NTP server, if configured, is provided by the IT environment. It is recommended that the NTP server be on a protected internal network. that is meant to be separated effectively from unauthorized individuals and user traffic (preferably through a secured tunnel); one that is in a controlled environment where there is physical protection and implementation of security policies can be enforced. Without authentication or access control, Network Time Protocol (NTP) is insecure and can be used by an attacker to send NTP packets to attempt to crash or overload the switch. If NTP is to be used, configure NTP authentication using Message Digest 5 (MD5) and the "**ntp access-group**" command. If NTP is enabled globally, disable it on all interfaces on which it is not needed.

For further details on Cat6K, refer to "Setting Time and Calendar Services" in **[10]** and for Cat3K, refer to Administrating the Switch -> Configuring NTP in **[3](b)**.

4.4 Identification and Authentication

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

The Cat6K can be configured to use local authentication and authorization (the local user database of IOS), or defer authentication (for console and/or SSH access) to a

TACACS+, or RADIUS server. For details, refer to "Securing User Services Overview" in **[4](a)(b)**.

The Cat3K can be configured to use local authentication and authorization (SSH), TACACS+, or RADIUS. Refer to Configuring RADIUS **[3](b)** (book index -> R) for configuring remote (AAA) authentication using RADIUS or refer to Configuring TACACS+ **[3](b)** (book index -> T) for configuring remote (AAA) authentication using TACACS+. It is recommended to read this section to become familiar with remote authentication concepts prior to configuration.

The sections contain information to set the following identification and authentication controls on the Switch. You can also refer to the specific commands in **[7](a)** regarding configuring RADIUS and or TACACS+ 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

For Cat6K, information regarding banner configuration can be found in the "Part 4: Managing Connections, Menus, and System Banners" → "Enabling Terminal Banners" → "Configuring a Login Banner" in section of **[3](a)**.

For Cat3K, information regarding banner configuration can be found in the "Administrating the Switch" → "Creating a Banner" → "Configuring a Login Banner" in section of **[3](b)**

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 terminated 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 is terminated 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 **[7](a)**.

In addition, the TOE allows each administrative user of the TOE to locally lock their administrative sessions. After the session is locked, the screen is flushed. No further activity is allowed to until the administrator has successfully re-authenticated to the TOE.

The **exit** command is used for this on-demand locking of administrator sessions **[7](a)**.

5. 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. 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 an operational system error (including power loss) the switch will reboot (assuming the 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.

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.

5.1 Network Processes Available During Normal Operation

The following network-based processes are running, or can be run in the evaluated configurations of the TOE, except where restricted by ACLs, or VLAN ACLs.:

- ICMP is supported inbound and outbound for detection and troubleshooting of network connectivity. To ensure there is no data leakage, use default size packets and refrain from using small and varying size packets.

- 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 and OSPFv2. EIGRP supports routing updates with IPv6 or IPv4, as does BGPv4, while OSPFv2 routing protocol support routing updates for IPv4 only. All these routing protocols support authentication of neighbor routers using MD5.
- SSHv2 is supported inbound for remote administrative access to the Catalyst Switches or to initiate administrative access to an external network device or other device/server running SSH.
- Syslog is supported outbound for transmission of audit records to a remote syslog server (syslog connections are recommended to be through a secure connection).
- TACACS+ is supported for authentication of administrative connections to the console and/or via SSH.
- NTP is supported for time synchronization (NTP connections are recommended to be through a secure connection).
- 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 and IOS-XE 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.
- 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).

Processes that should not be used in the evaluated configuration are SSH as a client (outbound connections) and SCP client as neither process provide man-in-the-middle protection.

6. 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.

Security Objective for the Operational Environment (from the Security Target)	**Definition of the Security Objective** (from the Security Target)	**Responsibility of the Administrators**
OE.AUDIT_REVIEW	Administrators will be trained to periodically review the audit logs to identify sources of concern, and will make a syslog server available for use by the TOE and TOE administrators.	Administrators must read, understand, and follow the guidance in this document to securely operate the Catalyst Switches
OE.CONFIDENTIALITY	The hard copy documents and soft-copy representations that describe the configuration of the TOE, I&A information and Audit storage will be kept confidential and access will be limited to authorized administrators. Audit data transmitted by the TOE and routing table updates exchanged with neighbor routers, and associated neighbor router authentication data will be protected from unauthorized disclosure through isolation of associated network traffic.	Administrators must read, understand, and follow the guidance in this document to securely operate the Catalyst Switches
OE.INTEROPERABILITY	The TOE will be able to function with the software and hardware of other vendors on the network when the TOE administrators follow software and hardware interoperability guidance provided by the manufacturer.	Administrators must read, understand, and follow the guidance in this document to securely install and operate the Catalyst Switches and maintain secure communications with components of the operational environment.
OE.LOCATE	The processing resources of the TOE and those services provided by the operational environment will be located within controlled access facilities, which will prevent unauthorized physical access.	The Catalyst Switches must be installed to a physically secured location that only allows physical access to authorized personnel.
OE.LOWEXP	The threat of malicious attacks aimed at exploiting the TOE is considered low.	The Catalyst Switches must be installed to a physically secured location that only allows physical access to

Security Objective for the Operational Environment (from the Security Target)	**Definition of the Security Objective** (from the Security Target)	**Responsibility of the Administrators**
		authorized personnel. In addition, the TOE does not allow installation of additional software. Furthermore, administrators are trained to securely install and operate the Catalyst Switches.
OE.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance; however, they are capable of error.	Administrators must read, understand, and follow the guidance in this document to securely install and operate the Catalyst Switches.
OE.TRAIN_GUIDAN	Personnel will be trained in the appropriate use of the TOE to ensure security and will refer to all administrative guidance to ensure the correct operation of the TOE.	Administrators must be trained and must read, understand, and follow the guidance in this document to securely install and operate the Catalyst Switches.

7. 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

7.1 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.

7.2 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 anytime, 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