Klas FastNet Series Switches KlasOS 5.3 Common Criteria Configuration Guide

Version: 1.0
Date: August 09, 2021

Prepared By:
Acumen Security
2400 Research Blvd Suite 395
Rockville, MD, 20850
www.acumensecurity.net

Table of Contents

Revision History

Version	Date	Changes
0.1	September 4th, 2020	Initial release
0.2	October 4th, 2020	Added log images
0.3	December 11th, 2020	Added visual examples and updated information
0.4	January 15th, 2021	Updated formatting
0.5	April 27th, 2021	Updated based on new ST
0.6	May 13th, 2021	Updated based on TR review
0.7	June 7th, 2021	Updated based on new ST
0.8	June 24th, 2021	Updated based on QA review
0.9	June 28th, 2021	Updated based on new ST
1.0	August 9th, 2021	Updated based on validator comments

1 Purpose of this Document

This document is a guide for the Klas FastNet Series Switches implementation of the Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e]. The information contained in this document is intended for Administrators who would be responsible for the configuration and management of the Klas FastNet Series Switches which runs on the KlasOS operating system.

This document will guide how to install, configure, and operate the device in a Common Criteria Compliant mode.

- Prerequisites for installing Klas FastNet Series Switches.
- How to Klas FastNet Series Switches.
- The secure communication mechanisms employed KlasOS.
- How to update the KlasOS Firmware.

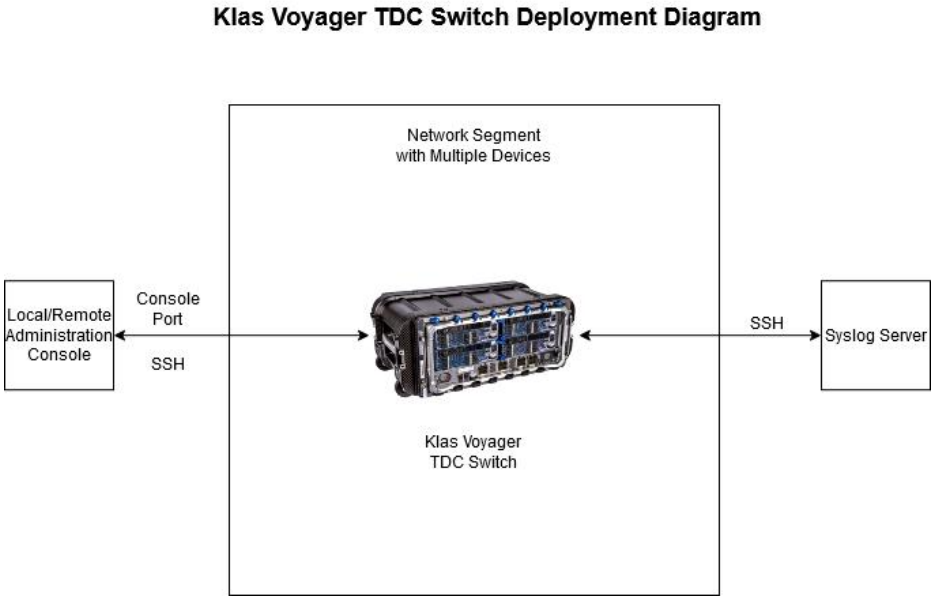


Figure 1: Klas Voyager TDC Deployment Diagram

1.1 TOE Overview

The TOE is the Klas Fastnet Series Switches Klas OS 5.3. (herein referred to as the “TOE”) It runs the KlasOS firmware, which provides connectivity to multiple devices contained within the same network segment. A real-time clock is present on all KlasOS devices. Authentication can be performed locally or over a trusted channel using SSH. All logs can be securely transferred to a syslog server. KlasOS provides a Command Line Interface (CLI) for device configuration. The Klas Fastnet switches range of products provide expandable, enterprise-grade, rugged mobility solutions.

2 TOE Description

2.1 Evaluated Configuration

The TOE also supports (sometimes optionally) secure connectivity with several other IT environment devices, including the following:

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation/SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channel. Any SSH client that supports SSHv2 may be used.
Syslog Server	Yes	The syslog audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE.

Table 1: IT Environment Components

2.2 Physical Boundaries

The TOE consists of the following devices:

- Klas Voyager TDC 10G Switch and Klas Voyager TDC 12GG Switch running KlasOS v 5.3.5 on Marvell Prestera 98DX8212 (ARM v7) processor.

2.3 Assumptions

This section describes the assumptions made in identification of the threats and security requirements for Network Devices. The Network Device is not expected to provide assurance in any of these areas, and as a result, requirements are not included to mitigate the threats associated with them. The table below describes conditions which are assumed to exist in the environment where the TOE is deployed. These assumptions are referenced from the PP and remain unchanged from their original source.

ID	Assumption
A.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).

	In the case of vNDs, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device functionality.
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g.,firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

2.4 **Excluded Functionality**

The following TOE functionalities are not within the scope of the evaluation and have therefore been excluded from the evaluation:

- SNMP
- NTP

The TOE has all the above functionalities disabled by default and should not be enabled for the Common Criteria evaluated configuration.

The following TOE functionalities will not be evaluated to comply with the CC Compliant configuration of the TOE:

- Spanning Tree Protocol (STP)
- Port Security

3 Secure Installation and Configuration

3.1 Prerequisites

The device must be configured to operate in Common Criteria validated mode. Please refer to Section 3.3 'CC-Compliant-Configuration' for instructions on configuring the TOE in Common Criteria mode. Prior to configuration, the following steps must be followed to prepare the TOE for configuration:

- Ensure that the Klas Voyager TDC Switch is not connected to any external network prior to initial configuration. The proper firmware should be installed and verified prior to any network connectivity as well.

- Download the KlasOS Common Criteria validated firmware image from the source below:

    - https://helpdesk.klastelecomservices.com/customer/en/portal/topics/900574-voyager---software-downloads/articles

      NOTE: User registration is required to download the firmware images.

- Before powering on the TOE, connect a PC or laptop to the console port using an RJ-45 to RS-232 console cable and configure the terminal emulator with the following settings:

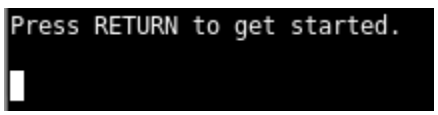
    - Baud: 9600
    - Data bits: 8
    - Parity: None
    - Stop bits: 1
    - Flow control: none

  Initial installation and configuration of the TOE must first be done through local console before remote administration through SSH can be enabled.

3.2 Installing and Updating the Software

Once all perquisites have been met, follow the steps below while still connected to the TOE via the console port:

1. Power on the TOE and wait until it boots completely. You will see the following once finished:



2. Pressing **<ENTER>** here will give a <**TDCswitch>** prompt.

3. Enable Privileged EXEC Mode:

```
TDCSwitch> enable
Dec 15 13:49:46 TDCSwitch CLI[23534]: (admin) (test) (ttyS0) startup : Success
TDCSwitch#
```

4. Configure interface Management0/0 with an IP address and subnet mask. An example can be seen below:

```
TDCSwitch# configure terminal
TDCSwitch(config)# interface Management0/0
TDCSwitch(config-if)# ip address 10.1.2.53 255.255.255.0
TDCSwitch(config-if)#
TDCSwitch(config-if)# end
TDCSwitch# _
```

Note: The IP address used above is for example purposes only. Please use an adequate IP address which complies with your appropriate network environment.

5. Configure the connected PC or laptop with an IP address on the same network as the IP address configured on the previous step.

6. Copy the downloaded software to the PC/laptop and move it to the SCP server or TFTP server directory.

    - If using SCP to copy the software do the following:

      copy scp: flash:

      You will be required to enter the IP address and username for the SCP server and the name of the firmware image to be copied.

    - If using TFTP to copy the software do the following:

      copy tftp: flash:

      You will be required to enter the IP address of the TFTP server and the name of the firmware image to be copied.

NOTE: The image that is loaded unto the TOE must be a different name than the currently active image. Sharing the same name would otherwise cause the active image to be overwritten and result in a digital signature verification failure, causing both images to be deleted.

    - An example of a full SCP file transfer can be seen below:

```
TDCSwitch# copy scp: flash: source 10.1.2.53
Address of remote host []? 10.1.2.121
Source username []? root
Source filename []? /KlasOS.fastnet.v5.3.5r20925.bin
Destination filename [KlasOS.fastnet.v5.3.5r20925.bin]?
Password:
KlasOS.fastnet.v5.3.5r20925.bin                                    100%   42MB  10.3MB/s   00:04
%INFO: 10.1.2.121:/KlasOS.fastnet.v5.3.5r20925.bin copied to flash:KlasOS.fastnet.v5.3.5r20925.bin
TDCSwitch#
```

- Check which images are present using the '**show flash**:' command:

```
TDCSwitch# show flash:
Directory of flash:/

    1  -rwx    43869476   Aug 24 2020 16:47:02   KlasOS.fastnet.v5.3.1rc3.bin
    2  -rw-    44019396   Nov 18 2020 06:26:31   KlasOS.fastnet.v5.3.1rc8.bin
    3  -rw-    44018799    Dec 8 2022 11:55:46   KlasOS.fastnet.v5.3.5r20908.bin
```

- Verify the signature on the firmware image:
    - The uploaded firmware image must be verified to check that the digital signature is correct before proceeding any further using

      verify /bootimgver flash: <name of image>

```
TDCSwitch# verify /bootimgver flash: KlasOS.fastnet.v5.3.5r20908.bin
%INFO: For large files this may take some time to complete.
Set exec-timeout accordingly.
\
Signature of flash:KlasOS.fastnet.v5.3.5r20908.bin = RSA VERIFY SUCCESS
```

- Specify that this newly copied image is the image to be booted:
    - **boot system flash <name of image>**

```
TDCSwitch(config)# boot system flash KlasOS.fastnet.v5.3.5r20908.bin
TDCSwitch(config)#
```

  Once this command is executed, the new image will now load when the system is rebooted.

- Reboot the device:

- **reload**

```
TDCSwitch# reload
Proceed with reload? [confirm]y
//00
```

- You can verify the currently active version of the TOE with the following command:
  - **Show version**

3.3 CC Compliant Configuration

To ensure the TOE is operating in a CC-Compliant configuration the following actions must be performed on the TOE after the CC firmware image has been loaded and verified:

- Configure an administrator password.
- Configure username(s) and password(s).
- Configure an access banner.
- Configure the inactivity timer.
- Configure account locking.
- Configure the time.
- Generate a public/private key-pair.
- Configure SSH for remote administration.
- Configure SSH tunnel for trusted path.
- Ensure that the DNS is disabled.
- Configure a syslog server.

All these functions and their configuration are explained in detail below.

3.3.1 Configure an Administrator Password

The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper- and lower-case letters, numbers, and special characters that include these characters include the following:

“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, “~”, “<”, “>”, “,”, “.”, “/”, “:”, “;”, “_”, “+”, “-“, “=”, “{“, “}”, “[“, “]”, “|”

The minimum password length can be configured by the Administrator and can range from 15 to 128 characters.

The administrator password is configured on the TOE using the following command in Global Configuration mode:

```
TDCSwitch(config)# enable secret Qwerty123P@ssword!
```

The password must be at least 15 characters. The minimum password length of at least 15 characters can be set with the following command:

```
TDCSwitch(config)# security passwords min-length 15
```

NOTE: Only after the administrative user presents the correct authentication credentials will they be granted access to the TOE administrative functionality. No TOE administrative access is permitted until an administrator is successfully identified and authenticated. All administrative functions are available remotely and through local console as long as the user is properly authenticated.

3.3.2 Configure Username(s) and Password(s)

Non-administrative usernames and passwords are configured using one of the following commands in Global Configuration mode:

- For a password using a SHA512 hashing algorithm

```
TDCSwitch(config)# username Example2 algorithm-type sha512 secret Exampl3P@ssw0r
d123!
```

Passwords will appear in clear text during creation but will be obscured during login.

3.3.3 Configure an Access Banner

The TOE can use the login banner to display an advisory notice and consent warning message regarding use of the TOE. This message is displayed before the login prompt is shown. To set the login banner do the following from the Global Configuration mode:

- This command would set the login banner to “This is my login banner”:

```
TDCSwitch(config)# banner login "This is my login banner"
```

To add a banner with multiple lines, use “///” in the command above to add a carriage return/line feed (CR/LF).

- This command would set a multi-line login banner:

```
TDCSwitch(config)# banner login "This is my login banner///This is the second li
ne of my login banner"
```

3.3.4 Configure the Inactivity Timer

A session inactivity timer should be configured for both, local console, and remote SSH sessions. After this time-period expires, the session will close, and the user will be logged out. To configure the session inactivity timer for the local console, do the following from Global Configuration mode:

- **line console 0**
  - **exec-timeout <mins> <secs>**

```
TDCSwitch(config)# line console 0
TDCSwitch(config-line)#exec-timeout 1 30
```

3.3.5 Configure Account Locking

The TOE can be configured so that a remote user will be locked out after a number of unsuccessful login attempts. The remote user will be locked out until a local administrator manually unlocks the account from a local console.

NOTE: The TOE will always allow a user to authenticate using the local console port, even if the user account is locked. This behavior is not configurable.

The following command can be used to configure a maximum number of authentication attempts by a user from global configuration mode:

- **aaa authentication attempts max-fail <number of failures>**

```
TDCSwitch(config)# aaa authentication attempts max-fail 3
```

The administrator may re-establish a user's access with the following command:

- **clear aaa remote user username <name of user>**

```
TDCSwitch# clear aaa remote user username user1
```

3.3.6 Configure the Time

The TOE has a real-time clock that can be used as a reliable time source. The system clock can be set using the following command from Privileged EXEC mode:

- **clock set <HH:MM:SS> <MONTH> <DAY> <YEAR>**

```
TDCSwitch# clock set 09:25:00 December 11 2020
```

3.3.7 Generate a public/private key-pair

Instructions on performing this can be found in section 5.1 of this document.

3.3.8 Configure SSH for Remote Administration

NOTE: This is optional and only required if SSH is required for remote administration.

Instructions on performing this can be found in section 4.1 of this document.

3.3.9 Configure SSH Tunnel for Trusted Path

Instructions on performing this can be found in section 4.4 of this document.

3.3.10 Ensure that the DNS Server is Disabled

The DNS server is disabled by default. However, the administrator can verify this by running the following command:

```
TDCSwitch# show running-config | grep "ip dns server"
TDCSwitch#
```

The command should yield no output, such as in the example above. A blank output means that the DNS Server is not configured. This is the desired CC-Compliant output.

If the DNS Server were to be enabled, inputting the above command would yield the following result:

```
TDCSwitch# show running-config | grep "ip dns server"
ip dns server
TDCSwitch#
```

In the case that the DNS Server is enabled, it must be disabled with the following command:

```
TDCSwitch# configure terminal
TDCSwitch(config)# no ip dns server
```

3.3.11 Configure a Syslog Server

Instructions on performing this can be found in section 4.3 of this document.

NOTE: The Random Number Generator does not need to be configured and is automatically functional when the TOE has completed boot up.

Official documentation on the Klas Voyager TDC Switch with additional information may be found in the link below:

- https://helpdesk.klastelecomservices.com/customer/en/portal/topics/1070295-voyager---tactical-data-center/articles

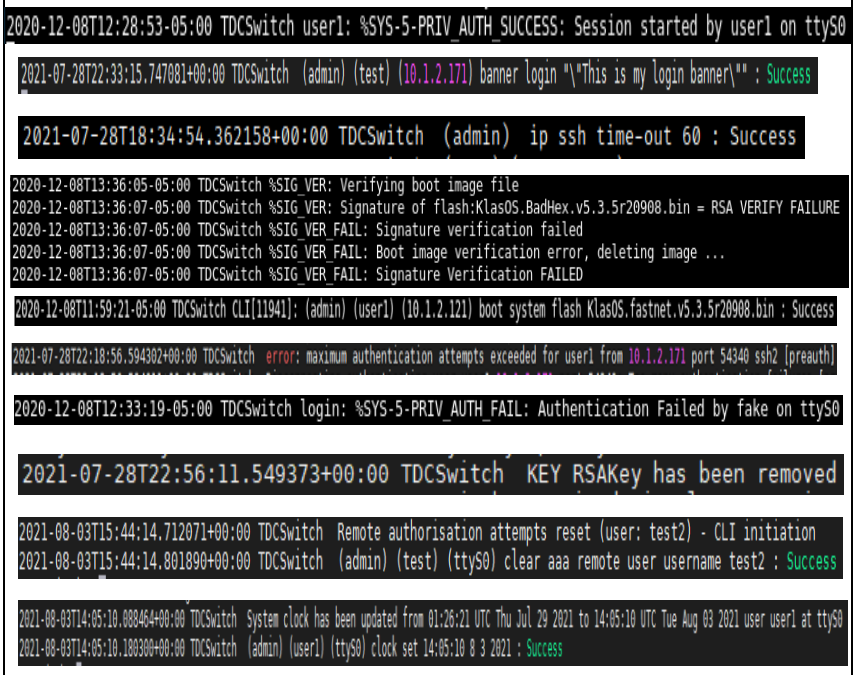
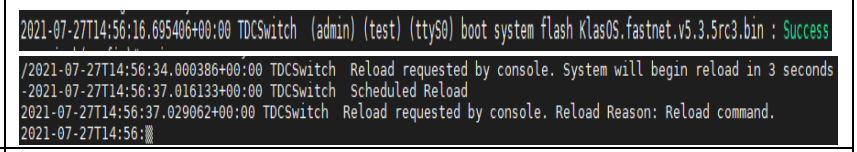
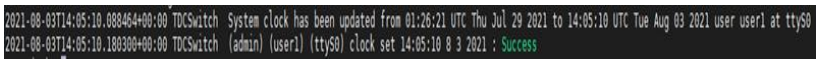
4 Audit Logs

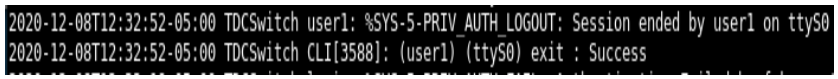
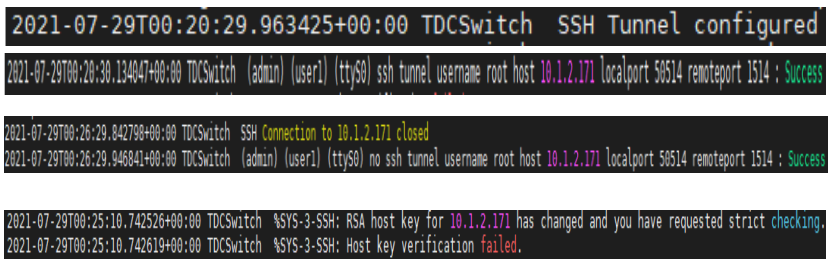
The TOE is a standalone device that can be configured to export audit events securely to an external syslog server using SSHv2. The audit logs are transmitted to the external syslog server in real time. The TOE also stores audit records locally in a local audit log file store in volatile memory. The TOE stores log files locally as Audit log and System log. The Audit log file stores the CLI commands entered by the user while the System log stores the general system log messages.

The log files can be read only by an authorized Security Administrator but cannot be modified. Each log file is deleted when it reaches a size of 10MB and a new log file is created.

Below is an example of audit logs generated by the TOE which fulfill the requirements for auditable events:

Requirement	Auditable Events	Additional Audit Record Contents	Sample Audit Records
FAU_GEN.1			
FAU_GEN.2			
FAU_STG_EXT.1			
FCS_CKM.1			
FCS_CKM.2			
FCS_CKM.4			
FCS_COP.1 /DataEncryption			
FCS_COP.1 /SigGen			
FCS_COP.1 /Hash			
FCS_COP.1 /KeyedHash			
FCS_RBG_EXT.1			
FCS_SSHC_EXT.1	Failure to establish an SSH Session	Reason for failure	2021-07-28T20:59:50.985377+00:00 TDCSwitch %SYS-3-SSH: RSA host key for 10.1.2.171 has changed and you have requested strict checking. 2021-07-28T20:59:50.985490+00:00 TDCSwitch %SYS-3-SSH: Host key verification failed. %%ERROR SSH failed to start. See logging for more details!
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure	2021-07-29T00:51:36.877942+00:00 TDCSwitch Failed password for test from 10.1.2.171 port 55358 ssh2
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).	2021-07-28T22:18:52.429914+00:00 TDCSwitch Failed password for user1 from 10.1.2.171 port 54340 ssh2 2021-07-28T22:18:56.593472+00:00 TDCSwitch Failed password for user1 from 10.1.2.171 port 54340 ssh2 2021-07-28T22:18:56.594302+00:00 TDCSwitch error: maximum authentication attempts exceeded for user1 from 10.1.2.171 port 54340 ssh2 [preauth] 2021-07-28T22:18:56.594611+00:00 TDCSwitch Disconnecting authenticating user user1 10.1.2.171 port 54340: Too many authentication failures [preauth]
FIA_PMG_EXT.1	None.	None.	
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	2020-12-08T12:28:53-05:00 TDCSwitch user1: %SYS-5-PRIV_AUTH_SUCCESS: Session started by user1 on ttyS0 2020-12-08T12:33:19-05:00 TDCSwitch login: %SYS-5-PRIV_AUTH_FAIL: Authentication Failed by fake on ttyS0
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	2021-07-28T22:30:37.741912+00:00 TDCSwitch Failed password for test from 10.1.2.171 port 54344 ssh2 2021-07-28T22:30:42.621474+00:00 TDCSwitch Accepted password for test from 10.1.2.171 port 54344 ssh2 2021-07-28T22:30:42.656285+00:00 TDCSwitch %SYS-5-PRIV_AUTH_SUCCESS: Session started by test on ttyS0 2021-07-28T22:30:42.846574+00:00 TDCSwitch (test) (10.1.2.171) startup : Success
FIA_UAU.7			

FMT_MOF.1 /ManualUpdate	Any attempt to initiate a manual update		The TOE does not recognize any commands to initiate updates prior to proper authentication. Since an update cannot even be attempted, no log can be generated for said attempt.
FMT_MOF.1 /Functions			
FMT_MTD.1 /CoreData			
FMT_MTD.1 /CryptoKeys			
FMT_MTD.1 /Services			
FMT_SMF.1	All management activities of TSF data		
FMT_SMR.2			
FPT SKP EXT.1			
FPT APW EXT.1			
FPT TST EXT.1			
FPT TUD EXT.1	Initiation of update; result of the update attempt (success or failure)		
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).	

FTA_SSL_EXT.1 (if "terminate the session" is selected)	The termination of a local session by the session locking mechanism.		
FTA_SSL.3	The termination of a remote session by the session locking mechanism.		
FTA_SSL.4	The termination of an interactive session.		
FTA_TAB.1			
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.	
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions		

5 Configuring Secure Communications

5.1 Using SSH for Remote Administration

The TOE is capable of being remotely administrated through the use of SSH. Remote authentication is achieved either through the use of a public key or password. The TOE will default in authenticating with a public key first. If no public key is found, then it will resort to password authentication.

SSH server on the TOE is restricted to the following algorithms:

- Encryption using AES-CBC-256 or AES-CBC-128
- Public key authentication using SSH-RSA, ECDSA-SHA2-NISTP256 or ECDSA-SHA2-NISTP384
- Integrity using HMAC-SHA1, HMAC-SHA2-256, or HMAC-SHA2-512
- Key exchange using DIFFIE-HELLMAN-GROUP14-SHA1, ECDH over NIST P256 with SHA2 or ECDH over NIST P384 with SHA2.

These algorithms are not configurable by the TOE. Attempting to authenticate with an unsupported algorithm will result in a failure to establish a connection.

Should a connection to the session be broken at any time, it will become inactive and terminate. The user is then required to establish a new session.

To enable SSH server on the TOE, do the following:

- Generate a host key. Section 4.3 describes how to do this.
  NOTE: The key-pair stored in flash is the one that will be used as the SSH host key**.**

The following commands can be used to configure SSH authentication-retries (default is 3) and SSH time-out (default is 60 seconds) if required:

- **Line authentication-retries <number of retries>**

```
TDCSwitch(config)# ip ssh authentication-retries 3
```

- **ip ssh time-out <number of seconds>**

```
TDCSwitch(config)# ip ssh time-out 120
```

The administrator may re-establish a user's access with the following command:

- **clear aaa remote user username <name of user>**

```
TDCSwitch# clear aaa remote user username user1
```

NOTE: The TOE will always allow a user to authenticate using the local console port, even if the user account is locked. This behavior is not configurable.

The user may terminate the active session using the **exit** command.

5.2 Adding a Public Key to an SSH or Syslog Server

In order to configure an SSH tunnel on the TOE, the generated public key must be copied to the syslog or SSH server authorized key file. This is the same keypair used by the TOE SSH Server for the Host Key. To view the public key from the TOE, run the following command in privileged EXEC mode:

```
TDCSwitch# show ip ssh
SSH Enabled - version 2
Keys in OpenSSH format:
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDLlaiG6ce2F/gIicodr0MpUQj2cyKLLg4xX9exOUBMtUqaDy15deOMV2yEHNVVU5y/Xt4yL5+pwKFiCwI0xqw3rmiAP+8O6VQ
c/UVA/JyGs63qJLyI515Rv+Uu7HWqPqYaw3Nin+kfSZeekV73k/Yty9RlG2HcP2YraSJgcH+ReYfI9qf6byLoVymkbGbnpmjs+L4v/m+63si3AanWqCwTmNZ47aCM5eyo//48Sl
IaGeZQ0w4HOtPCsxN98/axGBTQu9tS/shqUcyrslrOIjEA5L6UoWMJnQf/kHfMRIgMpj2vui0rc9kdMMYPLV42NGFG6/jiLB6yY1gKjOrRcwyN klasrsakey
```

The TOE will initiate a rekey after 1 gigabyte of data has been transferred or 1 hour of time has elapsed; whichever comes first. The rekey parameters are not configurable.

5.3 Adding an SSH Server Host Key to the TOE known_hosts

Ensure that strict host key checking is enabled. Run the following command in global configuration mode:

```
TDCSwitch(config)# ip ssh strict hostkey checking
```

Add the SSH server's hostkey to the known_hosts file on the TOE. Run the following commands in global configuration mode to add the hostkey on the TOE:

- **ip ssh known-hosts**
- **key-string <server ip address> <public key algorithm> <key data>**

  Replace <server ip address> with IP address of syslog server
  Replace <public key algorithm> with the server's public key algorithm
  Replace <key data> with the public key string.

Below is an example of the above two commands being executed:

```
TDCSwitch(config)# ip ssh known-hosts
TDCSwitch(conf-ssh-known-hosts)# key-string 10.1.2.121 ssh-rsa AAAAB3NzaC1yc2EAA
AADAQABAAABAQC4kudK2Zw86bItaIEAUD2LHIHwn4aqVzwrDbrG0a9OhymY5vzbIZ2bgJncN+IXT13/I
RJcaZOpe2ajavr/mAdOWMsLYe9+BsBLz9Zio6cuX9K2ePrcVs4lkTIJ+wzd0mNcGlCr0/VvlqMN2PNSB
A4bxFXVsOBtFuT3NznBkMDhxbuLXOxYauqpyh1+JOCB8WrzoWdFXu5k11en0UXHDnAUBy3Sh1qV+CSxH
BH9uqgzqERC7Txo7ufGhSIIPC1L91PVsNaEeSfW9yTie4lKnCyGpooArSNgxZoDTuJPxpQs178ZY0s5N
bK7sUFGQfpol8FiYmYQj2VgLCGE6BQcxEzf
```

To view the entries in the known_hosts file on the TOE, run the following command in privileged EXEC mode:

```
TDCSwitch# show ip ssh known-hosts
10.1.2.121 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC4kudK2Zw86bItaIEAUD2LHIHwn4aqVzwrDbrG0a9OhymY5vzbIZ2bgJncN+IXT13/IRJcaZOpe2ajavr/mAdO
WMsLYe9+BsBLz9Zio6cuX9K2ePrcVs4lkTIJ+wzd0mNcGlCr0/VvlqMN2PNSBA4bxFXVsOBtFuT3NznBkMDhxbuLXOxYauqpyh1+JOCB8WrzoWdFXu5k11en0UXHDnAUBy3Sh1q
V+CSxHBH9uqgzqERC7Txo7ufGhSIIPC1L91PVsNaEeSfW9yTie4lKnCyGpooArSNgxZoDTuJPxpQs178ZY0s5NbK7sUFGQfpol8FiYmYQj2VgLCGE6BQcxEzf
```

To delete a specific entry in the known_hosts file, run the following commands in global configuration mode:

- **ip ssh known-hosts**
- **no key-string <server ip address> <public key algorithm>**

  Replace <server ip address> with IP address of syslog server
  Replace <public key algorithm> with the server's public key algorithm

Below is an example of the above two commands being executed:

```
TDCSwitch(config)# ip ssh known-hosts
TDCSwitch(conf-ssh-known-hosts)# no key-string 10.1.2.121 ssh-rsa
```

To clear all entries in the known_hosts file, run the following command in privileged EXEC mode:

```
TDCSwitch# clear ip ssh known-hosts
```

5.4 Configuring an SSH Tunnel

The Security Administrator can start the SSH tunnel and stop the SSH tunnel. To configure the SSH tunnel on the TOE, run the following command in global configuration mode:

- **ssh tunnel username <username> host <syslog server IP> localport <port> remoteport <port>**

```
TDCSwitch(config)# ssh tunnel username root host 10.1.2.121 localport 50515 remo
teport 1514
```

  - Replace <username> with the correct username on the syslog server we will be building the SSH tunnel to.
  - The <syslog server IP> is the IP address of the syslog server.
  - Localport can be any unused port on the TOE.
  - Remote port is the port the syslog server will be listening to for incoming syslog messages.

To terminate the SSH tunnel on the TOE, run the following command in global configuration mode:

- **no ssh tunnel username <username> host <syslog server IP> localport <port> remoteport <port>**

```
TDCSwitch(config)# no ssh tunnel username root host 10.1.2.121 localport 50515 r
emoteport 1514
```

The SSH tunnel will attempt to reconnect automatically when it detects the connection to the remote SSH server is broken. An administrator can also manually restart the tunnel by performing the following commands in global configuration mode:

- **no ssh tunnel username <username> host <syslog server IP> localport <port> remoteport <port>**
- **ssh tunnel username <username> host <syslog server IP> localport <port> remoteport <port>**

```
TDCSwitch(config)# no ssh tunnel username root host 10.1.2.121 localport 50515 r
emoteport 1514
TDCSwitch(config)# ssh tunnel username root host 10.1.2.121 localport 50515 remo
teport 1514
```

6 Cryptographic Support

6.1 Cryptographic Key Generation

The TOE can support the generation of one (1) EC/RSA cryptographic keypair as follows in Common Criteria evaluated mode. This keypair is used by both the SSH Server on the TOE for the SSH Host Key, and the SSH client on the TOE for establishing an SSH tunnel to a remote server:

- EC keys of size 256 or 384
- RSA keys of size 2048 or 3072

Before keys can be generated, a domain name must be configured on the TOE with the following command entered in global configuration mode:

```
TDCSwitch(config)# ip domain-name klas.cc.test
```

Each private key generated is stored on the system flash and each key can be zeroized securely as per Common Criteria requirements.

6.1.1 SSH Host Key

The SSH host key is obtained from the generated keypair and is used for SSH remote administration of the TOE. To see details of existing keys generated, enter the '**show crypto key mypubkey all'** from privileged EXEC mode. The output will show the key names. To generate a new SSH host key, you need to firstly zeroize any existing keypairs. Instructions on zeroizing cryptographic keys can be found on section 5.3 'Cryptographic Key Zeroization' of this document.

6.1.2 Generating Key Pairs

1. ECDSA Keypair

   To generate an ECDSA keypair do the following in global configuration mode:

   crypto key generate ec keysize <256|384> label <label name>

   ```
   TDCSwitch(config)# crypto key generate ec keysize 256 label ECKeyExample
   ```

   The <label name> is a unique identifier for the key.

2. RSA Keypair

   To generate an RSA keypair do the following in global configuration mode:

   crypto key generate rsa general-keys modulus <2048|3072> label <label name>

```
TDCSwitch(config)# crypto key generate rsa general-keys modulus 2048 label RSAKe
yExample
```

The <label name> is a unique identifier for the key.

Running the same command again with the same label name will overwrite the existing key with that label name.

6.2 Information on Crypto Key Generation

Crypto keys are generated in pairs: one private and one public key. If the user repeats the command using the same label name then the old keypair will be zeroized and a new keypair created.

Key-pairs are not stored in the configuration and private keys are not visible by a user or administrator. The administrator can see what keys have been generated by executing the command from privileged EXEC mode:

- **show crypto key mypubkey <all | rsa | ec>**
    - This will output details of the generated keys and the public component. The private key will not be displayed.
    - The Key name field corresponds to the label name. The Key type field displays if the key is RSA or ECDSA. The Key storage field displays the secure partition the key is stored in.
    - Use **'all'** to display all keypairs. Use **'ec'** to display EC keypairs. Use **'rsa'** to display RSA keys

```
TDCSwitch# show crypto key mypubkey all
% Key pair was generated on: Thu Dec 15 14:46:29 2022
Key name: klasrsakey
Key type: RSA KEYS
Key is not exportable.
Public-Key: (2048 bit)
Modulus:
    00:cb:95:a8:86:e9:c7:b6:17:f8:08:89:ca:1d:af:
    43:29:51:08:f6:73:22:8b:2e:0e:31:5f:d7:b1:39:
    40:4c:b5:4a:9a:0f:2d:79:75:e3:8c:57:6c:84:1c:
    d5:55:53:9c:bf:5e:de:32:2f:9f:a9:c0:a1:62:0b:
    02:34:c6:ac:37:ae:68:80:3f:ef:0e:e9:54:1c:fd:
    45:40:fc:9c:86:b3:ad:ea:24:bc:88:e7:5e:51:bf:
    e5:2e:ec:75:aa:3e:a6:1a:c3:73:62:9f:e9:1f:49:
    97:9e:91:5e:f7:93:f6:2d:cb:d4:65:1b:61:dc:3f:
    66:2b:69:22:60:70:7f:91:79:87:c8:f6:a7:fa:6f:
    22:e8:57:29:a4:6c:66:e7:a6:68:ec:f8:be:2f:fe:
    6f:ba:de:c8:b7:01:a9:d6:a8:2c:13:98:d6:78:ed:
    a0:8c:e5:ec:a8:ff:fe:3c:4a:52:1a:19:e6:50:d3:
    0e:07:3a:d3:c2:b3:13:7d:f3:f6:b1:18:14:d0:bb:
    db:52:fe:c8:6a:51:cc:ab:b2:5a:ce:22:31:00:e4:
    be:94:a1:63:09:9d:07:ff:90:77:cc:44:88:0c:a6:
    3d:af:ba:2d:2b:73:d9:1d:30:c6:0f:2d:5e:36:34:
    61:46:eb:f8:e2:2c:1e:b2:63:58:0a:8c:ea:d1:73:
    0c:8d
Exponent: 65537 (0x10001)
```

Keypairs are persistent across reboots as they are stored in secure flash partitions. If the error **"% Please define a domain-name first.**" is displayed after trying to run the crypto key generate command then the

administrator is required to configure a domain-name using the **'ip domain-name <domain-name>'** command from global configuration mode.

6.3 Cryptographic Key Zeroization

Cryptographic keys can be zeroized using the following methods:

- Zeroize the individual key stored in flash:
    - **crypto key zeroize <ec|rsa> <label name>**
        - where the <label name> matches the Key name in flash.

```
TDCSwitch(config)# crypto key zeroize rsa RSAKeyExample
```

```
TDCSwitch(config)# crypto key zeroize ec ECKeyExample
```

- Zeroize all existing keys:
    - **crypto key zeroize**

```
TDCSwitch(config)# crypto key zeroize
```

- Generating a new key will immediately overwrite and erase any existing keys and replacing the old keys with a new key value.

6.4 Self Tests

The TOE performs the following self-tests:

- Integrity check of the firmware image (during bootup):

  During system boot the TOE performs an integrity check of the installed firmware by comparing the RSA 4096 using SHA-256 digital signature of the firmware image. This happens before any configuration has been loaded or any interfaces are enabled. If signature verification fails, all SSH functionality is disabled.

- Cryptographic algorithm known-answer tests (during bootup):

  All approved cryptographic algorithms are tested at boot using known-answer tests. If any cryptographic algorithm or entropy tests fail, the TOE will immediately reboot. An error message will be displayed on the console.

- Entropy self-tests (continuous, bootup and on-demand):

  The entropy noise source health tests are performed during bootup as part of the self-tests. They also are run continuously during system runtime. If any of the entropy health tests fail, the system will reboot immediately and an error message will be displayed to the console.

If any cryptographic algorithm known-answer tests or entropy self-tests failures are observed, the user should no longer use the device for cryptographic operations with the current firmware image. The user should try to load a new firmware image and check if the issue still occurs. If the problem continues to exist please discontinue usage of the device and contact Klas Telecom for assistance.

7 Operational Modes

When a Klas FastNet Series Switch is initially installed, it is under normal operational mode. After initial installation, the device must still be placed into its evaluated common criteria mode configuration by performing the steps described in Section 3.3 of this guidance. Once configured in its evaluated configuration, the switch is considered to be running in Common Criteria mode and will perform the functions as described.

8 References

The following documents were created and evaluated as part of the Klas FastNet Series Switches CC evaluation:

- Klas FastNet Series Switches KlasOS 5.3 Common Criteria Configuration Guide [AGD} version 1.0
- Klas Fastnet Series Switches KlasOS 5.3 Security Target [ST] version 1.7

End of Document