DigitalMedia NVX Series v5.2

Common Criteria Evaluated Configuration Guide (CCECG)

Version 1.0

February 15, 2022

Table of Contents

Referenced Documentation

[8391]	DM-NVX-350, DM-NVX-351, and DM-NVX-352 Quick Start (Doc.8391C)
[8392]	DM-NVX-350C, DM-NVX-351C, and DM-NVX-352C Quick Start (Doc. 8392B)
[8906]	DM-NVX-E30 and DM-NVX-D30 Quick Start (Doc.8906A)
[8346]	DM-NVX-E30C/DM-NVX-D30C Quick Start (Doc. 8346A)
[8526]	DM-NVX-D80-IOAV Quick Start (Doc. 8526A)
[8634]	DM-NVX-363 and DM-NVX-360 Quick Start (Doc. 8634)
[8636]	DM-NVX-363C and DM-NVX-360C Quick Start (Doc. 8636)
[8646]	DM-NVX-E760 Quick Start (Doc. 8646B)
[8638]	DM-NVX-E760C Quick Start (Doc. 8638B)
[CCECG]	Crestron DigitalMedia NVX Series v5.2 Common Criteria Evaluated Configuration Guide (CCECG) (This document)
[ST]	Crestron DigitalMedia NVX®AV-over-IP v5.2 Security Target
[PP]	collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020

Introduction

Crestron DigitalMedia NVX Series v5.2 comprises the following hardware appliances:

Appliance Model
DM-NVX-350
DM-NVX-350C
DM-NVX-351
DM-NVX-351C
DM-NVX-352
DM-NVX-352C
DM-NVX-E30
DM-NVX-E30C
DM-NVX-D30
DM-NVX-D30C
DM-NVX-D80-IOAV
DM-NVX-363
DM-NVX-363C
DM-NVX-E760
DM-NVX-E760C

The specific version in the evaluated configuration is v5.2.4651.00030. Each appliance contains an Intel Arria 10 SX SoC FPGA that includes an ARM Cortex-A9 MPCore processor implementing the ARMv7-A microarchitecture. "C" indicates that the model is a form factor with a chassis card.

Crestron Digital Media NVX Series is a series of audio & video (AV) over IP network devices that encrypt, decrypt and transmit HDMI video, USB and analog audio data over customer networks. The NVX TOE is deployed as a single physical appliance that serves as one endpoint for an audio/visual (AV) over IP (Transmission Control Protocol/Internet Protocol (TCP/IP)) connection.

About this Guide

This guide is intended for administrators responsible for installing, configuring, and/or operating the Crestron NVX appliances in accordance with the Common Criteria evaluation and the *collaborative Protection Profile for Network Devices, Version 2.2e*.

Guidance provided in this document allows an administrator to deploy the product in an environment that is consistent with the configuration that was evaluated as part of the product's Common Criteria testing process. It also provides the reader with instructions on how to exercise the security functions that were claimed as part of the Common Criteria evaluation.

Administrators are expected to be familiar with the security target for Crestron DigitalMedia NVX®AV-over-IP v5.2 and the general Common Criteria terminology that is referenced in it. This document references the Security Functional Requirements (SFRs) that are defined in the security target document and provides instructions for how to perform the security functions that are defined by these SFRs.

Supplemental Documentation

The following documentation is used or referenced to install and configure the Crestron DigitalMedia NVX Series v5.2 into the Common Criteria evaluated configuration.

- Crestron DigitalMedia NVX Series v5.2 Common Criteria Evaluated Configuration Guide (CCECG) Version 1.0, February 15, 2022 (This document) [CCECG]
- DM-NVX-350, DM-NVX-351, and DM-NVX-352 Quick Start (Doc.8391C)
- DM-NVX-350C, DM-NVX-351C, and DM-NVX-352C Quick Start (Doc. 8392B)
- DM-NVX-E30 and DM-NVX-D30 Quick Start (Doc.8906A)
- DM-NVX-E30C/DM-NVX-D30C Quick Start (Doc. 8346A)
- DM-NVX-D80-IOAV Quick Start (Doc. 8526A)
- DM-NVX-363 and DM-NVX-360 Quick Start (Doc. 8634)
- DM-NVX-363C and DM-NVX-360C Quick Start (Doc. 8636)
- DM-NVX-E760 Quick Start (Doc. 8646B)
- DM-NVX-E760C Quick Start (Doc. 8638B)

Configuration Prerequisites

Crestron Digital Media NVX Series v5.2 includes Crestron Crypto Kernel for Open SSL software module that includes third-party SafeLogic OpenSSL in support of higher level protocols (TLS, SSH). The module's FIPS-Approved cryptographic algorithms have obtained CAVP/ACVP certificates.

Crestron Digital Media NVX Series v5.2 uses its cryptographic libraries for all HTTPS, TLS, SSH and certificate functionality.

DISCLAIMER: Note that the use of other cryptographic engines was neither evaluated nor tested during the CC evaluation of Crestron Digital Media NVX Series v5.2.

Disable Auto Discovery

All devices support an auto discovery feature that allows them to be detected, report basic information, and do some basic configuration remotely. This feature is not protected by any type of authentication. Auto discovery must be disabled with the following command:

AUTODISCOVERY OFF

Disable Cloud Features

Cloud services are excluded from the evaluation and must be disabled by using the following commands:

ENABLEFEATURE CLOUDCLIENT OFF

HYDROGENENABLE OFF

Enable FIPSMODE

By default, NVX uses a set of ciphers for maximum compatibility with servers, when making TLS/SSH connections. This set of ciphers includes some that are not FIPS-compliant. The devices default to FIPS Mode ON. Should FIPS Mode be disabled, it should be re-enabled by using the FIPSMODE command: **FIPSMODE ON**. This command ensures that the NVX TOE runs in a FIPS-compliant mode only and using the approved ciphers identified in the [ST].

Scope of the Evaluation

The table below identifies features or protocols that are not evaluated or must be disabled and the rationale why.

Feature	Description
Net-SNMP, Telnet and HTTP Management Protocols	Net-SNMP, Telnet and HTTP are disabled by default and must not be enabled in the evaluated configuration. Only SSH and HTTPS are used for the remote management protocols to manage the TOE.
External LDAP/AD authentication	Users must be authenticated using the local authentication method. External LDAP/AD must not be used.
802.1X, SCIP traffic, AES-based HDCP	The TOE uses SCIP for device –to-device communication, 802.1X is used for network access, and AES based HDCP for Audio and video. The TOE is not distributed and therefore device-to-device communication and SCIP are not within scope of the evaluation. Additionally, the NDcPP does not define requirements for these types of traffic/protocols and therefore they have not been evaluated.
Crestron XiO Cloud® service	Allows supported Crestron devices across an enterprise to be managed and configured from one central and secure location in the cloud. It is disabled in the evaluated configuration.
Crestron Toolbox™ application	Crestron Toolbox™ application is excluded from the evaluated configuration. The evaluation only includes access to the GUI via browser.
Any features not associated with SFRs in claimed [NDcPP],	NDcPP forbids adding additional requirements to the Security Target (ST). If additional functionalities or products are mentioned, it is for completeness only.

Evaluation 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. The following assumptions were made in performing the Common Criteria evaluation.

Assumption	Guidance
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 ND cPP. 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.

Installation Guidance

Follow the steps within the following applicable guides to install the Crestron Digital Media NVX Series v5.2 Appliance as identified in the Crestron DigitalMedia NVX®AV-over-IP v5.2 Security Target.

Appliance Model	Quick Start Guide
DM-NVX-350	*DM-NVX-350, DM-NVX-351, and DM-NVX-352 Quick Start (Doc.8391C)*
DM-NVX-350C	*DM-NVX-350C, DM-NVX-351C, and DM-NVX-352C Quick Start (Doc. 8392B)*
DM-NVX-351	*DM-NVX-350, DM-NVX-351, and DM-NVX-352 Quick Start (Doc.8391C)*
DM-NVX-351C	*DM-NVX-350C, DM-NVX-351C, and DM-NVX-352C Quick Start (Doc. 8392B)*
DM-NVX-352	*DM-NVX-350, DM-NVX-351, and DM-NVX-352 Quick Start (Doc.8391C)*
DM-NVX-352C	*DM-NVX-350C, DM-NVX-351C, and DM-NVX-352C Quick Start (Doc. 8392B)*
DM-NVX-E30	*DM-NVX-E30 and DM-NVX-D30 Quick Start (Doc.8906A)*
DM-NVX-E30C	*DM-NVX-E30C/DM-NVX-D30C Quick Start (Doc. 8346A)*
DM-NVX-D30	*DM-NVX-E30 and DM-NVX-D30 Quick Start (Doc. 8906A)*
DM-NVX-D30C	*DM-NVX-E30C/DM-NVX-D30C Quick Start (Doc. 8346A)*
DM-NVX-D80-IOAV	*DM-NVX-D80-IOAV Quick Start (Doc. 8526A)*
DM-NVX-363	*DM-NVX-363 and DM-NVX-360 Quick Start (Doc. 8634)*
DM-NVX-363C	*DM-NVX-363C and DM-NVX-360C Quick Start (Doc. 8636)*
DM-NVX-E760	*DM-NVX-E760 Quick Start (Doc. 8646B)*
DM-NVX-E760C	*DM-NVX-E760C Quick Start (Doc. 8638B)*

Configuration Guidance

Follow the steps within the following sections to set up and configure the Crestron Digital Media NVX Series v5.2 Appliance as identified in the Crestron Digital Media NVX®AV-over-IP v5.2 Security Target.

FAU_GEN.1 Audit Generation

The Crestron Digital Media NVX Series v5.2 generates security relevant audit records, stores them locally, and can be configured to forward them to a syslog server over TLS. The locally stored audit records are protected from unauthorized access.

All devices have limited audit logging by default. Enable full audit logging with the following command: **AUDITLOGGING ON ALL.**

The audits shown below are from the TOE's internal storage. These audit records are displayed before the conversion to syslog format. Examples of each auditable event required by FAU_GEN.1 are provided from the actual audit records.

Requirement	Auditable Events	Example Audit Record

FAU_GEN.1	Start-up and shutdown of the audit functions	**Start Up of Audit Log**
		`Debug # 2021-10-26 15:32:09.693915-0400 # sys/systemd[1]: Started Crestron Audit Log service.`
		
		Shut Down Log Functions
		`[ 100.221657] systemd-shutdow: 71 output lines suppressed due to ratelimiting`
		`[ 100.235409] systemd-shutdown[1]: Sending SIGTERM to remaining processes...`
		`[ 100.265608] watchdog: watchdog0: watchdog did not stop!`
		`[ 100.266085] systemd-journald[2594]: Received SIGTERM from PID 1 (systemd-shutdow).`
		`[ 100.310721] systemd-shutdown[1]: Sending SIGKILL to remaining processes...`
		`[ 100.336720] systemd-shutdown[1]: Hardware watchdog 'Synopsys DesignWare Watchdog', version 0`
		`[ 100.346154] systemd-shutdown[1]: Unmounting file systems.`
		`[ 100.391369] EXT4-fs (dm-1): re-mounted. Opts: (null)`
		`[ 100.396366] EXT4-fs (dm-1): re-mounted. Opts: (null)`
		`[ 100.401408] systemd-shutdown[1]: All filesystems unmounted.`
		`[ 100.406978] systemd-shutdown[1]: Deactivating swaps.`
		`[ 100.412426] systemd-shutdown[1]: All swaps deactivated.`
		`[ 100.417652] systemd-shutdown[1]: Detaching loop devices.`
		`[ 100.424846] systemd-shutdown[1]: All loop devices detached.`
		`[ 100.430475] systemd-shutdown[1]: Detaching DM devices.`
		`[ 100.438316] socfpga system reboot ...`

		[100.453328] reboot: Restarting system
FAU_GEN.2	None.	
FAU_STG.1	None.	
FAU_STG_EXT.1	None.	
FCS_CKM.1	None.	
FCS_CKM.2	None.	
FCS_CKM.4	None.	
FCS_COP.1/DataEncryption	None.	
FCS_COP.1/SigGen	None.	
FCS_COP.1/Hash	None.	
FCS_COP.1/KeyedHash	None.	
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session Reason for failure	[2021-11-17T08:51:26-05:00]: EVENT: LOGON (ADServiceLocal) USER: admin3 # Failed with error: Username empty from 172.16.1.2 [2021-11-17T08:51:26-05:00]: EVENT: LOGON (WebServer) USER: admin3(172.16.1.2) (None) # invalid credentials
FCS_NTP_EXT.1	• Configuration of a new time server • Removal of configured time server Identity if new/removed time server	[2021-11-18T21:16:22-05:00]: EVENT: COMMAND (SHELL 172.16.1.50) USER: admin # SNTP SERVER:ntp1.leidos.ate [2021-11-18T22:37:59-05:00]: EVENT: COMMAND (SHELL 172.16.1.50) USER: admin # SNTP DELETE XXXX
FCS_RBG_EXT.1	None.	
FCS_SSHS_EXT.1	Failure to establish an SSH session	[2021-11-17T09:00:59-05:00]: EVENT: LOGON (SHELL 172.16.1.2) USER: admin2 # LOGON FAILED - INVALID USER/PASSWORD
FCS_TLSC_EXT.1	Failure to establish a TLS Session	[2021-11-17T08:30:33-05:00]: EVENT: SYSTEM # When connecting to 172.16.0.25:6518: TLS connection failed: Connection refused (33562735) [2021-10-25T10:46:07-04:00]: EVENT: SYSTEM # When

	Reason for failure	connecting to 172.16.0.25:8443: TLS connection failed: [2021-10-25T10:46:07-04:00]: EVENT: SYSTEM # Certificate error 62 (Hostname mismatch) at depth: 0 [2021-10-25T10:46:07-04:00]: EVENT: SYSTEM # Issuer = /CN=CA1.leidos.ate [2021-10-25T10:46:07-04:00]: EVENT: SYSTEM # Subject = /CN=BadCN [2021-10-25T10:46:07-04:00]: EVENT: SYSTEM # Cert expiration date: Oct 22 20:11:00 2022
FCS_TLSS_EXT.1	Failure to establish a TLS Session Reason for failure	[2021-11-16T07:41:52-05:00]: EVENT: LOGGING LEVEL (WebServer) USER: (172.16.0.25) # error:1408A0C1:SSL routines:ssl3_get_client_hello:no shared cipher
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded. Origin of the attempt (e.g., IP address).	[2021-11-17T08:55:06-05:00]: EVENT: LOGON (ADServiceLocal) USER: admin3 # Password mismatch for admin3 [2021-11-17T08:55:06-05:00]: EVENT: SYSTEM # IP Address Blocked (172.16.1.2)
FIA_PMG_EXT.1	None.	
FIA_UIA_EXT.1	All use of identification and authentication mechanism. Origin of the attempt (e.g., IP address).	**Successful Logon** [2021-11-17T08:49:22-05:00]: EVENT: LOGON (ADServiceLocal) USER: admin (Administrator) # Accepted password from 172.16.1.2 [2021-11-17T08:49:22-05:00]: EVENT: LOGON (WebServer) USER: admin(172.16.1.2) (None) # Login Successful **Failed Logon** [2021-11-17T08:51:26-05:00]: EVENT: LOGON (WebServer) USER: admin3(172.16.1.2) (None) # invalid credentials
FIA_UAU_EXT.2	All use of identification and authentication	**See above**

	mechanism. Origin of the attempt (e.g., IP address).	
FIA_UAU.7	None.	
FIA_X509_EXT.1 /Rev	Unsuccessful attempt to validate a certificate Reason for failure of certificate validation.	[2021-10-25T14:12:17-04:00]: EVENT: SYSTEM # When connecting to 172.16.0.25:8443: TLS connection failed: [2021-10-25T14:12:17-04:00]: EVENT: SYSTEM # OCSP error: unable to verify responder cert: signature failure
	Any addition, replacement or removal of trust anchors in the TOE's trust store Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store.	[2021-11-17T08:50:11-05:00]: EVENT: SYSTEM # ROOT certificate imported; subject = CA1.leidos.ate, serial = 6BA6C7E87F8CFC31
FIA_X509_EXT.2	None.	
FIA_X509_EXT.3	None.	
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	Ok: a_console # 2021-11-17 15:39:38 # populateFilePaths:flagFile:, updateFile:
FMT_MTD.1/CoreData	None.	
FMT_MTD.1/CryptoKeys	None.	
FMT_SMF.1	All	[2021-11-16T18:27:43-05:00]: EVENT: COMMAND (SHELL

	management activities of TSF data.	172.16.1.50) USER: admin # REMOTESYSLOG -S:ON -E:OK -I:tlss.leidos.ate -P:6518 -T:SSL -V:ON [2021-11-17T09:00:29-05:00]: EVENT: COMMAND (SHELL 172.16.1.50) USER: admin # REMBLOCKEDIP 172.16.1.2 [2021-11-17T09:00:29-05:00]: EVENT: ACCOUNT MANAGEMENT (SHELL 172.16.1.50) USER: admin # UNBLOCKED IP: 172.16.1.2 Also See Table below.
FMT_SMR.2	None.	
FPT_APW_EXT.1	None.	
FPT_SKP_EXT.1	None.	
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. 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).	Debug # 2021-10-26 15:32:09.535230-0400 # sys/systemd[1]: Starting Network Time Synchronization... Debug # 2021-10-26 15:32:09.535358-0400 # sys/systemd[1]: Started Update UTMP about System Boot/Shutdown. Debug # 2021-10-26 15:32:09.535466-0400 # sys/systemd-timesyncd[2824]: System clock time unset or jumped backwards, restoring from recorded timestamp: Wed 2021-01-27 10:35:14 EST Debug # 2021-10-26 15:32:09.535566-0400 # sys/systemd[1]: Time has been changed
FPT_TST_EXT.1	None.	
FPT_TUD_EXT.1	Initiation of update; result of the	**Successful Update** Ok: a_console # 2021-11-17 15:39:38 # populateFilePaths:flagFile:, updateFile:

	update attempt (success or failure)	**Failed Update**
		`Ok: a_console # 2021-11-17 15:39:38 # populateFilePaths:flagFile:, updateFile:`
		`Error: a_console # 2021-11-17 15:39:38 # Failed to populate file paths`
		`Error: a_console # 2021-11-17 15:39:38 # Upgrade image is not an official Crestron firmware.`
		`Error: CPHProcessor # 2021-11-17 15:39:38 # [/home/builduser/Linux_jstr1000/meta-crestron/recipes-platform/src/cph/.//libraries/systemclock/SystemClockImpl.cpp:521] runCommand execution failed`
		`Error: a_console # 2021-11-17 15:39:38 #`
		`ERROR: Invalid firmware image. Signature check failed`
		`Note that there is also a supplemental file called upgrade.log that is generated when a successful update takes place. Here is an example:`
		 
		upgrade.log

FTA_SSL_EXT.1 (If "terminate the session" is selected)	The termination of a local session by the session locking mechanism.	`[2021-11-17T08:41:46-05:00]: EVENT: LOGOFF (SHELL 127.0.0.1) USER: admin # Console Session Terminated`

FTA_SSL.3	The termination of a remote session by the session locking mechanism.	`[2021-11-17T09:22:09-05:00]: EVENT: LOGOFF (SHELL SHELL 172.16.1.50) USER: admin # Session Idle Timeout`
		
		`[2021-11-17T09:22:09-05:00]: EVENT: LOGOFF (SHELL 172.16.1.50) USER: admin # Console Session Terminated`

FTA_SSL.4	The termination of an interactive session.	`[2021-11-17T08:51:20-05:00]: EVENT: LOGOFF (SHELL WebServer) USER: admin(172.16.1.2) # LogOut`
		
		`[2021-11-17T11:58:32-05:00]: EVENT: LOGOFF (SHELL WebServer) USER: admin(172.16.1.50) # LogOut`

FTA_TAB.1	None.	

FTP_ITC.1	Initiation of the trusted channel.
	
	Termination of the trusted channel.
		Initiation of the Trusted Channel
		`2021-11-17T12:13:20.763893-05:00 DM-NVX-363-00107FEF8B88.leidos.ate crestErrorLogServer 2723 - - Notice : RSyslogger client connected.`
		
		Termination of the Trusted Channel
		`[2021-11-17T12:14:56-05:00]: EVENT: COMMAND (SHELL 172.16.1.50) USER: admin # REMOTESYSLOG -S:OFF`

	Failure of the trusted channel functions. Identification of the initiator and target of failed trusted channels establishment attempt.	**Failure of the Trusted Channel functions** `[2021-11-17T08:30:33-05:00]: EVENT: SYSTEM # When connecting to 172.16.0.25:6518: TLS connection failed: Connection refused (33562735)`

FTP_TRP.1/Admin	Initiation of the trusted path.
	
	Termination of the trusted path.
	
	Failure of the trusted path functions
		Initiation of the Trusted Path
		`[2021-11-17T08:40:13-05:00]: EVENT: LOGON (ADServiceLocal) USER: admin (Administrator) # Accepted password from 172.16.1.50`
		
		`[2021-11-17T08:40:13-05:00]: EVENT: LOGON (WebServer) USER: admin(172.16.1.50) (None) # Login Successful`
		Termination of the trusted path.
		`[2021-11-17T08:47:40-05:00]: EVENT: LOGOFF (SHELL WebServer) USER: admin(172.16.1.50) # LogOut`
		Failure of the trusted path functions
		`[2021-11-16T07:41:52-05:00]: EVENT: LOGGING LEVEL (WebServer) USER: (172.16.0.25) # error:1408A0C1:SSL routines:ssl3_get_client_hello:no shared cipher`

Administrative Action Audit Events

Admin Action	Actual Audit Record
Ability to administer the TOE locally and remotely	Collectively demonstrated in the other events.
Ability to reset passwords	`[2021-11-17T09:02:00-05:00]: EVENT: LOGGING LEVEL (WebServer) USER: admin(172.16.1.50) # {"Device":{"Authentication":{"ModifyUser":{"LocalUsers":{"Name":"admin3","LocalGroups":["Administrators","Connects","Operators","Programmers","Users"],"NewPassword":"XXXXXXXXXXX"}}}}}`
Generating/import of, changing, or deleting of cryptographic keys	`[2021-11-17T08:50:11-05:00]: EVENT: SYSTEM # ROOT certificate imported; subject = CA1.leidos.ate, serial = 6BA6C7E87F8CFC31`
Ability to configure the access banner	`[2021-11-18T22:42:55-05:00]: EVENT: SFTP (SFTP 172.16.1.50) USER: admin # uploading file "/SSHBanner/banner.txt"` `[2021-11-18T22:42:55-05:00]: EVENT: SFTP (SFTP 172.16.1.50) USER: admin # set "/SSHBanner/banner.txt" modtime 20211119-03:37:20`
Ability to configure the session inactivity time	`[2021-11-18T22:44:24-05:00]: EVENT: COMMAND (SHELL 172.16.1.50) USER: admin # SETLOGOFFIDLETIME 15` `[2021-11-18T22:44:24-05:00]: EVENT: ACCOUNT MANAGEMENT (source) USER: user # Logoff Idle Time CHANGED: 15 minutes`

before session termination or locking	
Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates;	Ok: a_console # 2021-11-17 15:39:38 # populateFilePaths:flagFile:, updateFile:
Ability to configure the authentication failure parameters for FIA_AFL.1	[2021-11-18T22:45:29-05:00]: EVENT: COMMAND (SHELL 172.16.1.50) USER: admin # SETUSERLOGINATTEMPTS 5 [2021-11-18T22:45:30-05:00]: EVENT: ACCOUNT MANAGEMENT (SHELL 172.16.1.50) USER: admin # Maximum user login attempts allowed: 5
Ability to manage the cryptographic keys;	[2021-11-17T08:50:11-05:00]: EVENT: SYSTEM # ROOT certificate imported; subject = CA1.leidos.ate, serial = 6BA6C7E87F8CFC31
Ability to re-enable an Administrator account	[2021-11-17T09:00:29-05:00]: EVENT: COMMAND (SHELL 172.16.1.50) USER: admin # REMBLOCKEDIP 172.16.1.2 [2021-11-17T09:00:29-05:00]: EVENT: ACCOUNT MANAGEMENT (SHELL 172.16.1.50) USER: admin # UNBLOCKED IP: 172.16.1.2
Ability to set the time which is used for time-stamps	[2021-11-18T22:47:22-05:00]: EVENT: COMMAND (SHELL 172.16.1.50) USER: admin # TIMEDATE 22:48:00 11-18-2021 [2021-11-18T22:48:00-05:00]: EVENT: SYSTEM # Time Change Event generated. (delta = 38 seconds)
Ability to configure NTP	**Configuring a new NTP server:** [2021-11-18T21:16:22-05:00]: EVENT: COMMAND (SHELL 172.16.1.50) USER: admin # SNTP SERVER:ntp1.leidos.ate **Removing an NTP server:** [2021-11-18T22:37:59-05:00]: EVENT: COMMAND (SHELL 172.16.1.50) USER: admin # SNTP DELETE XXXX
Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors	[2021-11-17T08:50:11-05:00]: EVENT: SYSTEM # ROOT certificate imported; subject = CA1.leidos.ate, serial = 6BA6C7E87F8CFC31
Ability to import X.509v3 certificates to the TOE's trust store	[2021-11-17T08:50:11-05:00]: EVENT: SYSTEM # ROOT certificate imported; subject = CA1.leidos.ate, serial = 6BA6C7E87F8CFC31

FAU_STG.1 Protected Audit Trail Storage

By default, the Crestron Digital Media NVX Series does not provide any interfaces to modify or manually delete the stored audit logs.

FAU_STG_EXT.1 Protected audit event storage

The TOE is a single instance of Crestron Digital Media NVX Series that stores audit data locally and can be configured to transmit the generated audit data to an external syslog server using TLS. Data is written to the external syslog in real time.

[CCECG] Section **FTP_ITC.1 Inter-TSF Trusted Channel** provides the guidance for the administrator to configure the syslog server, to configure TLS for the connection, and to add or remove trusted certificates to the Crestron NVX Appliance.

FCS_CKM.1 Cryptographic Key Generation

The Crestron DigitalMedia NVX Series v5.2 implements an SSH Server and TLS 1.2 (RFC 5246) Server and Client protocols and rejects all other TLS and SSL versions. There is no configuration required to restrict the Transport Layer Security (TLS) protocol to TLS v1.2 only.

The **FIPSMODE ON** command limits the generation of asymmetric cryptographic keys to the following cryptographic key generation algorithms:

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3;
- ECC schemes using “NIST curves” P-256, P-384, P-521 that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4;
- FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.1;
- FFC Schemes using ‘safe-prime’ groups that meet the following: “NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and RFC 3526.]

FCS_CKM.2 Cryptographic Key Establishment

The **FIPSMODE ON** command limits the generation of asymmetric cryptographic keys to the following cryptographic key establishment methods:

- Elliptic curve-based key establishment schemes that meets the following: NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”;
- Finite field-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”;
- FFC Schemes using “safe-prime” groups that meet the following: ‘NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and groups listed in RFC 3526.

FCS_CKM.4 Cryptographic Key Destruction

For plaintext keys in volatile storage, the destruction of keys is performed by OpenSSL cryptomodule APIs and executed by single overwrite consisting of zeroes. When ephemeral keys or secrets are no

longer needed (e.g. a network session has terminated), they are deleted. The TOE is not subject to situations that could prevent or delay key destruction.

For plaintext keys in non-volatile storage the destruction of keys is performed by file system APIs and executed by performing a single-pass overwrite consisting of a new value of the key at request of the administrator using the command: **`SSHSERVER GENHOSTKEY`**. The plaintext private keys and CSPs are managed by the cryptomodule and stored in RAM or Flash. Encrypted flash keys are copied unencrypted to a RAM drive at startup for runtime use. The cryptomodule does not store any other secret or private keys or CSPs persistently (beyond the lifetime of an API call).

FCS_COP.1/DataEncryption Cryptographic Operation (AES Data Encryption/Decryption)

For data encryption/decryption, the TOE supports AES CBC and GCM (128 and 256 bits) for TLS and AES CTR (both 128 and 256-bit) for SSH.

No additional configuration is required other than executing **FIPSMODE ON** to ensure the TOE uses only these algorithms for data encryption/decryption.

FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)

The TOE supports rDSA (modulus 2048/3072/4096) and ECDSA with elliptical curve key sizes 256, 384, or P-521 bits for signature generation and verification. RSA is used for X509 CSRs and signed updates. ECDSA is used for X509 CSRs.

No additional configuration is required other than executing **FIPSMODE ON** to ensure the TOE uses only these algorithms for signature generation and verification.

FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)

The TOE performs SHA-1, SHA-256, SHA-384, and SHA-512 cryptographic hashing services that meets ISO/IEC 10118-3:2004.

No additional configuration is required other than executing **FIPSMODE ON** to ensure the TOE uses only these hash algorithms.

FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)

The TOE performs keyed-hash message authentication that meets the following: ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2. The hash function used, key and block size, and output MAC lengths (message digest size) are identified in the table below.

Algorithm	Key Size	Block Size	Message Digest Size
SHA-1	256-2048 bits in 128 bit increments	512	160

SHA-256	256, 448, 512, 1536, 2048 bits	512	256
SHA-384	192, 320, 1024, 1920, 2048 bits	1024	384
SHA-512	256, 448, 1024, 1536, 2048 bits	1024	512

No additional configuration is required other than executing **FIPSMODE ON** to ensure the TOE uses only these keyed-hash algorithms.

FCS_HTTPS_EXT.1

The HTTPS protocol is used when Crestron NVX is acting as a web server. The X.509v3 certificate is used to secure all HTTPS traffic. The administrator can manage certificates, including installing certificates or creating CSRs to add a public certificate. See [CCECG] Section *FIA_X509_EXT.3 X.509 Certificate Requests* and Section *FTP_ITC.1 Inter-TSF Trusted Channel* for a description of the TLS certificate properties, creating a Certificate Signing Request, and Installing a certificate.

Executing the **FIPSMODE ON** command will limit the cryptographic key generation algorithms, cryptographic key establishment methods, data encryption/decryption algorithms, signature generation and verification services, cryptographic hashing services, and keyed-hash message authentication to those specified in [ST] for Crestron DigitalMedia NVX Series v5.2 acting as an HTTPS server. No further administrative actions are required to configure the TOE as an HTTPS server.

FCS_NTP_EXT.1 NTP Protocol

The TOE can be configured to use up to three NTP servers to synchronize its clock. The TOE supports NTP v4 only. No configuration is necessary, the TOE will use the supported version of the server it is using. If the server supports a version other than v4, the TOE will not establish a connection. After performing the configuration steps below, there is no additional configuration required to ensure that the device will not update NTP timestamp from broadcast and/or multicast addresses.

To enable NTP using the CLI, enter the following commands:

SNTP [START|STOP|SYNC|DELETE {SERVER|SERVER2|SERVER3}|SERVER {args}|SERVER2 {args}|SERVER3 {args}]

- START - start synchronization
- STOP - stop synchronization
- SYNC - force synchronization (one time)
    - DELETE {SERVER|SERVER2|SERVER3} - delete configuration for NTP server or server2 or server3

- SERVER:{address} [optional args] - address of primary NTP server with optional arguments
- SERVER2:{address} [optional args]- address of secondary NTP server to synchronize with optional arguments
- SERVER3:{address} [optional args]- address of secondary NTP server to synchronize with optional arguments

  optional args:

  PORT:{1-65535} - NTP Port (Default 123)

  AUTH:{MAC} - Secured NTP. MAC authentication.

  KEYTYPE:{MD5(less secured)|SHA1|SHA128|SHA256} - Key Type for MAC authentication only. (Default SHA1).

  NOTE: Use only SHA1 or SHA256 for the KEYTYPE authentication parameter.

  KEY:{shared key} - Pre-Shared key between NTP client and server. (MAC authentication only).

  KEYID:{1-65535} - Pre-Shared key index between NTP client and server. (MAC authentication only).

  Example:

  1. SNTP SERVER:ntps.example.com AUTH:nts
  2. SNTP SERVER:macntp.example.com AUTH:mac KEYID:1 KEY:e5fa44f2b31c1fb553b6021e7360d07d5d91ff5e
  3. SNTP SERVER:pool.example.com

  No parameter - displays current setting

To disable NTP synchronization and set the current date and time manually, use the following commands:

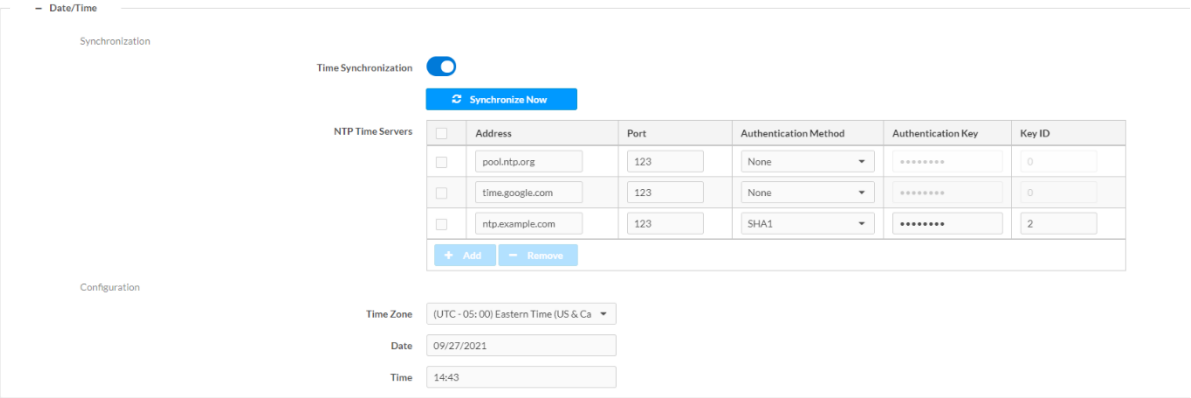
SNTP STOP

> **NOTE:** Enter the current time (24 hour clock format, including minutes and seconds) and date.

TIMEDATE hh:mm:ss mm-dd-yyyy

To enable NTP or set the date and time manually using the GUI:

1. navigate to the **Settings Page - Date/Time**



2. Move the Time Synchronization slider to the desired position to specify whether time synchronization using NTP servers will be enabled or disabled. By default, time synchronization is enabled.
3. In the NTP Time Server fields, enter the URL of the NTP server(s), and select either SHA1 or SHA256 as the authentication method for each NTP Server.
4. Click Synchronize Now to perform time synchronization between the device's internal clock and the time server.

   If not using synchronization with an NTP server, you can manually configure the time as follows:

1. Click on the Time Zone drop-down to select the applicable time zone.
2. In the Time (24hr Format) field, enter current time in 24-hour format.
3. In the Date field, enter the current date.

FCS_RBG_EXT.1 Random Bit Generation

No administrator configuration is required for the RNG Functionality.

FCS_SSHS_EXT.1 SSH Server Protocol

The following commands must be executed to disable insecure diffie hellman group key exchange algorithms:

- SSHSERVER KEYEXCHANGE -A: DHGEX256 off
- sshserver hmac -a:HMACSHA2256ETM off
- sshserver hmac -a:HMACSHA2512ETM off

No other configuration is required to ensure that only the allowed algorithms are used in SSH Server connections with the TOE.

The SSH Host Private Key is generated using the **SSHSERVER GENHOSTKEY** command. This key is used for client authentication of the TOE's SSH server.

Within SSH connections the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, the TOE performs a rekey. No configuration is necessary or permitted to enforce this behavior.

An administrator can be configured to authenticate using an SSH key instead of a password. To set up SSH to use a public/private key pair for a user, perform the following steps:

- Use SFTP to copy a file with the user key to the /user folder. The key file must be in OpenSSH public key format.
- Use the ADDUSERKEY command in the console to install the key. For example ADDUSERKEY –N:username –K:filename

FCS_TLSC_EXT.1 TLS Client Protocol without Mutual Authentication

The TLS 1.2 client protocol is used with the audit server (syslog).

The **FIPSMODE ON** command limits the TOE to the following ciphersuites:

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

The TOE's TLS client implementation establishes its reference identifiers from the administrator-configured reference identifiers per Section 6 of RFC 6125, using the hostname as a reference identifier and checking that the syslog server's certificate includes the specified identifier.

For remote Syslog, the identity is configured using the REMOTESYSLOG command as shown in the FTP_ITC.1 Inter-TSF Trusted Channel section below. The –I option specifies the DNS name which is used as the identifier.

The TOE supports the Subject Alternate Name (SAN) extension however, the use of IP Addresses in the SAN is not supported.

The TLS client supports the Elliptic Curves Extension (specifying only P-256, P-384, and P-521) in its Client Hello, and the TOE does not require (nor allow) administrative configuration of this extension.

Executing the **FIPSMODE ON** command will limit the cryptographic key generation algorithms, cryptographic key establishment methods, data encryption/decryption algorithms, signature generation and verification services, cryptographic hashing services, and keyed-hash message authentication to those specified in [ST] for Crestron DigitalMedia NVX Series v5.2 acting as a TLS Client.

FCS_TLSS_EXT.1 TLS Server Protocol without Mutual Authentication

The TLS 1.2 server protocol without mutual authentication is used for the web server.

The **FIPSMODE ON** command limits the TOE to the same TLS ciphersuites as identified above for the TOE's TLS Client.

The **FIPSMODE ON** command limits the key establishment for TLS using 2048/3072-bit RSA, 2048-bit DHE, and secp256r1, secp384r1, secp521r1 ECDHE curves and or session tickets. Session resumption is not supported.

Executing the **FIPSMODE ON** command will limit the cryptographic key generation algorithms, cryptographic key establishment methods, data encryption/decryption algorithms, signature generation and verification services, cryptographic hashing services, and keyed-hash message authentication to those specified in [ST] for Crestron DigitalMedia NVX Series v5.2 acting as a TLS server.

No further administrative actions are required to configure the appliance to operate as a TLS server without mutual authentication.

FIA_AFL.1 Authentication failure management

It is the responsibility of the administrator to initially set up user login controls such as the number of failed login attempts before locking out an account.

The **SETUSERLOGINATTEMPTS** command configures the number of consecutive failed login attempts that will result in the user account being locked. The range is 1 to 65534 failed sign-in attempts. A value of 0 (zero) disables user account locking and the user's account will never be locked due to failed log in attempts. However, the value of 0 must never be selected in the Common Criteria configuration. By default SETUSERLOGINATTEMPTS is disabled and must be enabled in Common Criteria configuration.

The number set using the **SETUSERLOCKOUTTIME** command is the number of hours an account will be locked for. The number can range from 0 to 255, where a value of 0 indicates that the account will remain locked indefinitely or until unlocked by an administrator using the **REMLOCKEDUSER** command.

Authentication failure handling is only enforced on password credentials. User authentication based on SSH private key is not subject to the lockout mechanism. To ensure there is never a case where all administrators are locked out due to the session locking mechanism, at least one admin account must be set up to use SSH public key authentication.

FIA_PMG_EXT.1 Password Management

Password rules define the complexity requirements for user authentication to Crestron DigitalMedia NVX. Crestron NVX devices accept passwords that consist of any combination of uppercase letters,

lowercase letters, numbers, and special characters. The TOE supports characters defined by the following regular expression: ^[\p{L}\p{N}\p{Zs}\p{S}\p{P}]*$. This includes all letters, numbers, symbols, punctuation, and space separators. The **SETPASSWORDRULE** command is used by administrators to change the minimum password length to values between 6 and 128 characters (default is 8 characters). To ensure strong passwords, the password must be a mix of upper- and lower-case characters, numbers and special characters.

To change the default minimum password length, enter the following command:

SETPASSWORDRULE -LENGTH:[XX]

Where [xx] is the desired minimum password length.

FIA_UIA_EXT.1 User Identification and Authentication

The administrative functions are accessed remotely via an HTTPS/TLS Web-based GUI and both locally /remotely via SSH to CLI. The administrator uses an SSH client to connect to the device. This provides access to the console commands used to configure the device. A subset of management functions are also available from the GUI.

The only security-relevant action prior to the identification and authentication process is the display of the warning banner. For the GUI the user must acknowledge the banner by clicking on an 'ok' button.

Before allowing any other TSF-mediated actions on behalf of that administrative user, the TOE requires each administrative user to be successfully identified and authenticated using either the TOE's local password-based authentication mechanism (or public key for SSH).

When the device is powered up for the first time, it requires that an admin account be created. The admin can choose this account name and password.

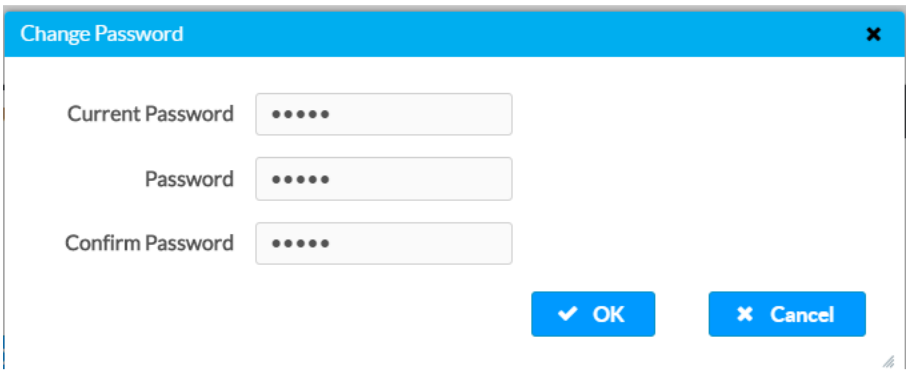
NOTE: Do not lose this information. The system cannot be accessed without it.

An administrator can also change passwords (for other users or their own) from the Security tab in the navigation bar of the web user interface.

To change the current user password: **Security Page - Current User - Change Current User Password**

In the Change Password dialog, enter the current password in the Current Password field, the new password in the Password field, then reenter the same new password in the Confirm Password field.

Change Password Dialog Box



Click OK to save or click Cancel to cancel the changes.

To change another user's password from the web Security Page - Click the information button in the Actions column to update information for the selected user. Enter a password in the Password field; reenter the same password in the Confirm Password field. Click OK to save or click Cancel to cancel the changes.

Local access to the CLI is achieved by connecting directly to a network port and using SSH. When prompted, enter username and password or use an SSH key.

To access the console remotely, the administrator must use an SSH client. The administrator establishes a remote administrative session over SSH by starting up an SSH client on the administrator's workstation or laptop and connecting to the TOE using a configured administrative account and the TOE's hostname or IP address Passwords or keys can be used for the SSH connection. See [CCECG] Section FCS_SSHS_EXT.1 SSH Server Protocol for additional information on configuring an administrative key.

The web-based interface is accessed remotely using a browser from a client workstation by entering the IP address of the TOE and user credentials (username and password). Supported browsers include:

- Firefox® web browser, version 31 and later
- Internet Explorer web browser, version 11 and later
    - Microsoft Edge web browser
    - Safari® web browser, version 6 and later
    - Chrome™ web browser, version 31 and later

To login to the web-based interface:

1. Enter the IP address of the Crestron NVX into the browser.
2. If a login notification displays, click **OK** to accept the notifications stated.
3. Enter your credentials in the Device Administration dialog (note that the user name and password are case sensitive) and click **Sign In**.

Note that the Crestron Toolbox is not included in the TOE and should not be used.

FIA_UAU_EXT.2 Password-Based Authentication Mechanism

See [CCECG] Section ***FIA_UIA_EXT.1 User Identification and Authentication*** above.

FIA_UAU.7 Protected Authentication Feedback

Password data is obfuscated while it is being entered and only generic success/failure messages are provided. There are no preparatory steps required to ensure authentication data is not revealed while entering for the login information.

FIA_X509_EXT.1/Rev X.509 Certificate Validation

Certificate revocation checking using OCSP is performed for communications with the syslog server.

To configure the OCSP checking and certificate validation for the TOEs web server and for syslog servers, use the SSLVERIFY and OCSP commands as defined below.

SSLVERIFY [[OFF|CA] | [-T:ON|OFF]] [-X:ON|OFF] [-C:ON|OFF] [-S:ON|OFF] [-H:ON|OFF] 'OFF' disables server certificate trust check (allow both SELF and CA certificates), 'CA' ensures that a server certificate is issued by a trusted CA,
-T:ON|OFF enable/disable verification that a server certificate is issued by a trusted CA,
-X:ON|OFF enable/disable required presence of extendedKeyUsage in server certs,
-C:ON|OFF enable/disable required presence of CA in basicConstraints of server cert trust chains,
-S:ON|OFF enable/disable required trusted signer on installed server certs,
-H:ON|OFF enable/disable server certificate hostname checking,
The OFF and CA parameters are deprecated; use the -T switch instead.
The X and C options apply to outgoing TLS connections and to
installed server certificates.
No parameter - displays current setting

In the evaluated configuration all parameters should be enabled. For example: SSLVERIFY -T:ON -X:ON -C:ON -S:ON -H:ON (Enables all certificate related checks)

To validate certificate revocation status when establishing TLS connections and when installing CA-signed certificates, configure for OCSP validation using following command:

OCSP -L:OFF|STAPLEONLY|ONLINE {-N:NumOfNonces} {-T:TimeoutInSeconds}
where 'OFF' is no OCSP verification,
where 'STAPLEONLY' check certificate staple (no staple is a failure),
where 'ONLINE' checks staple, if no staple then check validity with responder,
where '-N:#' sets the number of nonces (currently 0 is none, any non-zero means use a nonce.)
where '-T:#' sets the timeout in seconds to connect to responder (for ONLINE only)
No parameter - displays current settings

The ONLINE parameter must be set. In the evaluated configuration, certificate stapling cannot be used.

The TOE validates the extendedKeyUsage field according to the following rules:

- Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
- Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
- OCSP certificates presented for OCSP responses which have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

The TOE does not support the use of certificates for trusted updates or for executable code integrity verification. Therefore the following extendedKeyUsage field is not validated by the appliance:

- Certificates used for trusted updates and executable code integrity verification which have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.

FIA_X509_EXT.2 X.509 Certificate Authentication

The TOE uses X.509 certificates for authentication of TLS and HTTPS trusted channels. The administrator is entrusted to add or remove CA certificates (root CA and any needed intermediate certificates) to the Crestron NVX Appliance as needed for the TLS/HTTPS channels.

The root CA certificates and intermediate CA certificates used for validating a certificate can be added to or removed from the TOE's trust store using the certificate console command: **CERTIFicate Cmd Certificate_Store** as described in [CCECG] Section *FTP_ITC.1 Inter-TSF Trusted Channel.* This section also describes how to configure the syslog server.

There is no administrative option for when a connection cannot be established during the certificate validity check. The TOE will not accept the certificate and the connection will not be established.

FIA_X509_EXT.3 X.509 Certificate Requests

The TOE supports a createcsr command that allows it to generate an internal RSA 2048 bit server key and Certificate signing request file as follows:

CREATECSR C:ST:L:O:OU:CN:E [-I:option]

where C = 2 letter country code
where ST = Full state or province name
where L = Locality or city name
where O = Organization or company name
where OU= Organizational Unit name or division
where CN = site name or domain name
where E = Email address
where -I: Ignore blank parameters. Options are True or False.

Example Command: **CREATECSR US:NJ:DA:CRESTRON:QE:nvx-test:email@test.com.** This will create a request.csr file in the "/SYS" folder of the NVX device. You can get this file using SFTP and administrator credentials.

The device can use RSA 2048, 3072 and 4096 bit key pairs, but when creating CSRs is only capable of generating 2048 bit key pairs. Therefore specifying a key size is not necessary. A SHA1 hash is used to sign the CSR.

Setup a CA signed server certificate using a CSR file generated from NVX.

Step1: Ensure that SSLverify is set in such a way that trusted CA and chain verification has been setup See the SSLVERIFY command in [CCECG] Section *FIA_X509_EXT.1/Rev X.509 Certificate Validation*.

Step 2: Now initiate the certificate signing request process from the device. Refer to the Create a certificate signing request command: **CREATECSR** above.

Step3: Use an SFTP client to download the CSR from the device. The CSR is in a file named "request.csr", located in the /SYS folder.

Step 4: Obtain the signed certificate and the trust list for that certificate. The trust list must contain the root certificate and may optionally contain one or more intermediate certificates. Each certificate must be in a separate file, in PEM format.

Step 5: Upload the root certificate to the device, followed by any intermediate certificates. Refer to Certificate Console Commands section in [CCECG] Section *FTP_ITC.1 Inter-TSF Trusted Channel* below.

Step6: Use and SFTP client to upload the signed certificate to the device. The certificate must be in a file names “”srv_cert.cer” and be put in the “/SYS” directory.

Step6: Now on the Console issue the command “SSL CA”

Step7: You should see a success message asking to reboot the device. Reboot it. This completes loading the certificate and it will be used following the reboot.

FMT_MOF.1/ManualUpdate Management of Security Functions Behavior

See Section ***FPT_TUD_EXT.1 Trusted Update*** below for the details of this function.

FMT_MTD.1/CoreData Management of TSF Data

[CCECG] Section *FMT_SMF.1: Specification of Management Functions* describes the administrator permissions and roles provided by the Crestron NVX.

[CCECG] Section *FMT_SMF.1: Specification of Management Functions* identifies the TSF-data-manipulating functions implemented in response to the requirements of the Protection Profile.

[CCECG] Section *FTP_ITC.1 Inter-TSF Trusted Channel* provides the guidance for the administrator to add or remove certificates and root CAs to the Certificates Store in Crestron NVX.

FMT_MTD.1/CryptoKeys Management of TSF Data

The TOE restricts the ability to manage the cryptographic keys to Security Administrators using role-based access control methods. Specifically, the Security Administrator may use the TOE to generate CSRs (which contain key pair)s and load certificates (whether it is certificate for the TOE generated by an external CA or a certificate used to validate a presented TLS client or server certificate) into the TOE’s Trust Store. Certificate management commands available to authorized administrators from the console are:

Command	Description	
CREATECSR	Generates a Certificate Signing Request that can be downloaded from the device.	See section *FIA_X509_EXT.3 X.509 Certificate Requests*
CERTIFICATE	Manage device certificate stores.	See *FTP_ITC.1 Inter-TSF Trusted Channel*
SSLVERIFY	Enable/disable certificate validation options.	i.e. SSLVERIFY -C:ON See section *FIA_X509_EXT.3 X.509 Certificate Requests*

FMT_SMF.1: Specification of Management Functions

The Crestron DigitalMedia NVX Series v5.2 provides a number of roles for local and remote management of the TOE, of which only the ‘Administrators’ role corresponds to the Security Administrator as defined in the PP. The TOE provides the Security Administrator administrative access through its HTTPS server and via a CLI. The CLI can be accessed remotely over SSH or locally by directing connecting a user laptop to a network port and using an SSH client. The web-based interface is accessed remotely from a web browser.

Crestron DigitalMedia NVX Series v5.2 provides the following default roles:

- Administrators – Allows the user full access to the appliance settings and interfaces including but not limited to configure and update the appliance, syslog, and unlock users. This user corresponds with the System administrator as defined in the NDcPP.
- Programmer– unprivileged.
- Operator– unprivileged. Allows the user to reboot and monitor the appliance
- User– unprivileged.
- Connect– unprivileged.

Only the 'Administrators' role corresponds to the Security Administrator as defined by [PP]. The other roles are unprivileged users without any management capabilities. A user can only be assigned to one role.

A factory default pre-defined Administrator account is used for initial configuration. The password must be changed and must conform to the configured password rules. To update the default password rules, enter the following command:

SETPASSWORDRULE -LENGTH:[XX]SETPASSWORDRULE –ALL

Where [XX] is an integer between 6 and 128 characters (default is 8 characters).

After updating the password rules, change the password by entering the following command:

UPDATEPASSWORD

You will be prompted for a new password that requires a minimum number of characters as configured in the "XX" parameter. For local password-based credentials, the TOE accepts passwords that consist of any combination of uppercase letters, lowercase letters, numbers, and special characters. The TOE supports characters defined by the following regular expression: ^[\p{L}\p{N}\p{Zs}\p{S}\p{P}]*$. This includes all letters, numbers, symbols, punctuation, and space separators. To ensure that passwords are secure, the use of a mix of the available characters are encouraged, as well as a minimum password length that is at least as large as defined by local site policies. The TOE provides an eight character minimum by default, however the user can modify this value using the SETPASSWORDRULE commands described above.

NOTE: Do not lose this login information—the system cannot be accessed without it.

The Crestron DigitalMedia NVX Series v5.2 is capable of performing the following management functions:

- **Ability to administer the TOE locally and remotely**

  Refer to [CCECG] Section *FIA_UIA_EXT.1 User Identification and Authentication*.

- **Ability to configure the access banner (Console only)**

  Refer to [CCECG] Section *FTA_TAB.1 Default TOE Access Banners.*

- **Ability to configure the session inactivity time before session termination (Console only)**

  Refer to [CCECG] Section *FTA_SSL.3 TSF-Initiated Termination and* Section *FTA_SSL_EXT.1 TSF-Initiated Session Locking*.

- **Ability to update the TOE, and to verify the updates using a digital signature capability prior to installing those updates** (Console, Web UI)

  Refer to [CCECG] Section *FPT_TUD_EXT.1 Trusted Update*

- **Ability to configure the authentication failure parameters for FIA_AFL.1 (Console only)**

  Refer to [CCECG] Section *FIA_AFL.1 Authentication failure management.*

- **Ability to manage the cryptographic keys: CSRs and TLS private key for web server (Console only)**

  Refer to [CCECG] Section *FIA_X509_EXT.3 X.509 Certificate Requests.*

  See [CCECG] Section FCS_SSHS_EXT.1 *SSH Server Protocol*

  Refer to [CCECG] Section *Configuration Prerequisites,* **Enable FIPSMODE**. The **FIPSMODE ON** command will limit the cryptographic key generation algorithms, cryptographic key establishment methods, data encryption/decryption algorithms, signature generation and verification services, cryptographic hashing services, and keyed-hash message authentication to those specified in [ST].

- **Ability to re-enable an Administrator account (Console only)**

  See [CCECG] Section *FIA_AFL.1 Authentication failure management*.

- **Ability to set the time which is used for time-stamps (Console, Web UI)**

  Refer to [CCECG] Section *FCS_NTP_EXT.1 NTP Protocol.*

- **Configure NTP (Console, Web UI)**

  Refer to [CCECG] Section *FCS_NTP_EXT.1 NTP Protocol.*

- **Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors; and Ability to import X.509v3 certificates to the TOE's trust store (Console only)**

  Refer to [CCECG] Section *FIA_X509_EXT.3 X.509 Certificate Requests and* Section *FTP_ITC.1 Inter-TSF Trusted Channel.*

FMT_SMR.2 Restrictions on Security Roles

Refer to [CCECG] Section *FMT_SMF.1: Specification of Management Functions*

FPT_APW_EXT.1 Protection of Administrator Passwords

No Guidance required.

FPT_SKP_EXT.1 Protection of TSF Data (for reading of all symmetric and private keys)

No Guidance required.

FPT_STM_EXT.1 Reliable Time Stamps

The Crestron DigitalMedia NVX Series are hardware appliances that includes a hardware-based real-time clock. The TOE's embedded OS manages the clock and exposes administrator clock-related functions such as set time.

Refer to [CCECG] Section ***FCS_NTP_EXT.1 NTP Protocol*** for guidance on setting the time.

FPT_TST_EXT.1 TSF Testing

During initial start-up (on power on), the TOE performs a series of power-up Known Answer Tests (a KAT for each library cryptographic algorithm that the TOE utilizes) as well as an integrity test during power-up. In particular, the TOE executes the following KAT tests: AES, RSA, ECDSA, DH, ECDH, DRBG, HMAC, and SHA. The self-test for verification of the integrity of the TOE firmware and software using RSA 2048-bit signature and SHA-256 hash algorithm. For each self-test, the TOE uses known inputs to calculate an expected cryptographic result, and compares that result to the known result. If the calculated result matches the expected result, the test passes; if it does not match, the test fails. A failure of a power-up self-test causes the TOE to halt its boot and reboot. This will happen automatically and there is no action required by the administrator. Should the TOE continually reboot, the administrator can reset the device to factory default or can contact Crestron Support: https://www.crestron.com/Support. A factory reset can be performed as follows.

1. Press the RESET button 11 times, allowing 7-10 seconds between presses.

2. Wait until the green PWR LED illuminates, and then press and hold the SETUP button for 5 seconds.

3. The power button will display Amber while the device is booting and then will display Green indicating the device is operational.

FPT_TUD_EXT.1 Trusted Update

Administrators can query the currently executing TOE version from the **STATUS** tab in the navigation bar of the web-based user interface or from the CLI using: **`version'`**. This tab shows the model name, serial number, and firmware version.

The administrator can manually initiate updates to the TOE firmware through the GUI **Upload Firmware File** radio button. To initiate the firmware upgrade, the administrator must first obtain the firmware file by loading it onto the device and clicking OK. Specifically, the firmware file is available by entering: https://www.crestron.com/Support/Resource-Library into a web browser and entering "NVX" into the search box and then finding the TOE firmware version in the list. The administrator must enter their customer information and credentials to download the file. Download the file to the **/firmware** location on the device. Crestron digitally signs its firmware files using RSA 2048 bit and SHA-256; automatically verifies the digital signature during the download process; and only installs the updates if the signatures verify. From the web interface, it is not possible to download an update and then install it at a later date.

Updates can also be manually initiated from the console's CLI. The update files must first be obtained by the administrator from Crestron's website over SFTP. It is possible to upload a file and then install it at a later time. The file is not active until it is installed by the administrator. There are no specific commands for viewing the version of downloaded but uninstalled firmware, however the version of the firmware is

identified in the filename and can be queried by navigating to the firmware directory and examining the filename. Once installed, it is immediately activated. When the firmware update files are uploaded over SFTP, the files are verified at installation, not when the file is uploaded. If the digital signatures cannot be verified then the TOE will not perform the update and the failure will be audited.

Perform a firmware update from the CLI as follows:

1. Download the firmware update file from Crestron.com for the specific device model, such as Dm-nvx-35x-enc_6.0.4835.00015_r412939.zip
2. Use SFTP to transfer the firmware file to the "firmware" directory (must use administrator credentials) on the device.
3. On the console, enter the command **`Imgupd`**

Note that all functions of the device will temporarily cease to operate, either shortly before the reboot or because of the reboot. The TOE will automatically become fully operational once the install is completed. In the evaluated configuration, the TOE does not provide an automated update mechanism.

When an upgrade fails the device remains in the current version and this can be verified by running the '`ver -v`' command. All failures are recorded in the audit log.

FTA_SSL_EXT.1 TSF-Initiated Session Locking

The TOE terminates local interactive sessions when the administrative configurable inactive timeout value is reached. This is configured with **SETLOGOFFIDLETIME** on the console. The default is 20 minutes and can be configured to values between 1 and 60 minutes. '0' disables the inactive timeout feature. This function applies to the CLI console.

Examples of command usage include:

SETLOGOFFIDLETIME 10

FTA_SSL.3 TSF-Initiated Termination

The TOE terminates remote interactive sessions when the administrative configurable inactive timeout value is reached. This is configured with **SETLOGOFFIDLETIME** on the console. The default is 20 minutes and can be configured to values between 1 and 60 minutes. '0' disables the inactive timeout feature. For the web server, the inactive time is configured with the **WEBSERVER** command and can be configured for between 600 and 3600 seconds (1200 seconds is the default). The configuration will take effect during the next administrative session. This function applies to the CLI accessed via SSH and the GUI web server.

Examples of command usage include:

SETLOGOFFIDLETIME 10

Webserver timeout 1200

FTA_SSL.4 User-Initiated Termination

The TOE allows administrator-initiated termination of the administrator's own interactive session from the console using the '**BYE**' command that will logout the user. From the web GUI, the administrator can click on the profile icon/image in the upper right and select **logout**.

FTA_TAB.1 Default TOE Access Banners

It is the responsibility of the administrator to configure the login notification displayed when a user logs into Crestron NVX. This feature is typically used for describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

Devices initially do not display a banner to a user before they log in. Activate the banner by using an SFTP client to copy a file containing the text the administrator wishes to display onto the device at the following location:

/SSHBanner/banner.txt

The configured banner is displayed at all interfaces.

FTP_ITC.1 Inter-TSF Trusted Channel

The TOE supports the use of trusted communication channels between itself and authorized IT entities for assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

The TOE can be configured to send audit records to external syslog server(s) using TLS in real-time and allows the TSF to initiate communication for sending remote audit:

- **Syslog server using TLS**

  The TOE supports TLS communication without mutual authentication using X.509v3 certificates for communications with the audit server and does not implement any administrator override mechanism for invalid certificates. The TOE requires the external audit server to support TLS v1.2 in order to be able to establish the trusted channel between the TOE and the audit server. Devices initially do not send audit logs to a remote Syslog server. To enable sending to a remote Syslog server, use the following command:

  REMOTESYSLOG [-S:] {-E:} {-A} [-I:address] [-P:port] {-T:protocol} {- V:ON|OFF}

  - -S:ON|OFF enables or disables remote system error logging //This must be set to ON
  - -E:OK|INFO|NOTICE|WARNING|ERROR|FATAL decides which types of errors are logged. Selecting a tier results in logging errors of that level of importance and above in a hierarchy from OK to FATAL. In order to obtain the required audit logs for Common Criteria, this must be set to “OK”.
    - OK- log all "OK" errors and above to Syslog
    - INFO- log all "info" errors and above to Syslog
    - NOTICE- log all "notice" errors and above to Syslog (default)
    - WARNING- log all "warning" errors and above to Syslog
    - ERROR- log all "error" errors and above to Syslog
    - FATAL- log all "fatal" errors and above to Syslog
  - -A Log
    - Accesses Syslog contents of the audit log if remote system error logging is enabled
  - -I:address

- Replace with an ASCII string containing the server host name (max 255 characters)

- P:port
  - Replace port with the remote Syslog server port number in decimal notation
- -T:TCP|UDP|SSL
  - SSL must be selected to secure the channel
- -V:ON|OFF
  - ON must be selected to authenticate the server.
    Not entering a parameter displays the current setting.

To test the command, run the following script:
rsyslog -S:ON -A -I:172.30.144.58 -P:23456 -T:SSL -V:OFF

The TOE automatically attempts to re-connect to the external syslog server should the TLSv1.2 channel be broken. If the connection remains broken, the administrator should perform the following steps to diagnose and fix the problem:

- Check the error logs on the TOE to see if there is a reason for re-connect failures.
- If a certificate issue is indicated in the error logs, check that the syslog server's certificate is valid and trusted by the TOE.
- If OCSP is enabled on the TOE and the syslog server provides either a stapled OCSP response or an OCSP responder URI, check the error logs to see if OCSP validation failed.
- Use the 'ping' command on the TOE to see if the syslog server is reachable.
- Check the physical network cables.
- Check that the syslog server is still running.
- Reconfigure the Log Settings.
- If these steps do not resolve the problem, reboot the TOE and/or syslog server.

The administrator must add the syslog server trusted certificate to the Crestron NVX Appliance. In order to verify the server certificate, you need a certificate from the server certificates chain of trust in Certificate Store.

For an X.509v3 certificate, when Crestron NVX connects to a syslog server, Crestron NVX compares the signing authority of the certificate presented by the syslog server to the certificates in the Certificate Store. Trust must be established for the connection to be established. For Crestron NVX to verify a certificate, you must add the syslog server signing authority certificate to the Certificate Store.

The syslog server trusted certificate, root CA certificate, and intermediate CA certificates used for validating a presented certificate can be added or removed to the TOE's trust store from the console using the **CERTIFicate Cmd Certificate Store** command as follows.

CERTIFICATE CONSOLE COMMANDS – used to load certificates

CERTIFicate Cmd Certificate_Store <Certificate_Name> <Certificate_UID> <Password>
Where Cmd = [ADD|REM|LIST|LISTN|VIEW]
Where Certificate_Store = [ROOT|MACHINE|INTERMEDIATE|WEBSERVER]
ADD Certificate_Store - Add Certificate(from known location) To Specified Certificate Store
(MACHINE, WEBSERVER stores requires password)
ADDF filename Certificate_Store - Add Certificate To Specified Certificate Store

REM Certificate_Store [#|Certificate_Name Certificate_UID] - Remove Specified Certificate From Specified Certificate Store

LIST Certificate_Store - List All Certificates In Specified Certificate Store

LISTN Certificate_Store - List and number all Certificates In Specified Certificate Store

VIEW Certificate_Store [#|Certificate_Name Certificate_UID] - View Details Of Specified Certificate In Specified Certificate Store

No parameter - Lists Usage

By default, NVX uses a common list of public signing authorities for verifying X.509 certificates. It may be necessary for the administrator to load their own public or site-wide root and intermediate certificate to the trusted list. To add any additional trusted authorities, do the following:

- INTERMEDIATE CERTIFICATE
  - To add an intermediate certificate, use SCP to copy the certificate into the file User\Cert\intermediate_cert.cer on the NVX. Then add it with the following command:

    CERTIFICATE ADD INTERMEDIATE
- ROOT CERTIFICATE
  - Similarly, to add a root certificate, use SCP to copy the certificate into the file User\Cert\root_cert.cer on the NVX. Then add it with the following command:

    CERTIFICATE ADD ROOT
- WEBSERVER CERTIFICATE
  - To add a webserver certificate, use SCP to copy the certificate into the file User\Cert\webserver_cert.pfx on the control system. Then add it with the following command:

    CERTIFICATE ADD WEBSERVER <password>

    Note:- Webserver certificate supports only PFX format, i.e p12 certificates

REMOVING CERTIFICATES

CERTIFICATE REM <certificate_store> <certificate_number|certificate_name> <UUID>

For removing certificates from a store you will need either the certificate number (as obtained from LISTN command) or certificate name and the UUID of the certificate.

CONFIGURE EXTERNAL SYSLOG

To configure a syslog-ng server follow the instructions in: https://www.syslog-ng.com/technical-documents/doc/syslog-ng-open-source-edition/3.26/administration-guide/61#TOPIC-1431138.

In particular, after installing the syslog-ng on a server host ensure that log messages can be received by using syslog over TLS as described in the above link. This includes the following elements: The certificate

of the Certificate Authority that issued the certificate of the syslog-ng server must be available on the syslog-ng client. This can be added using the instructions in Section *FTP_ITC.1 Inter-TSF Trusted Channel.* A certificate on the syslog-ng server that identifies the syslog-ng server.:

1. Create an X.509 certificate for the syslog server:

   The Common Name parameter of the server's certificate must contain the hostname of the server (for example syslog-ng.example.com).
   The certificate must be signed by a third-party trusted certificate authority (CA) such as Commodo, Symantec, GoDaddy and Digicert.

2. Copy the certificate (for example syslog-ng.cert) of the syslog-ng server to the syslog-ng server host, for example into the /opt/syslog-ng/etc/syslog-ng/cert.d directory. The certificate must be a valid X.509 certificate in PEM format.

3. Copy the private key (for example syslog-ng.key) matching the certificate of the syslog-ng server to the syslog-ng server host, for example into the /opt/syslog-ng/etc/syslog-ng/key.d directory. The key must be in PEM format, and must not be password-protected.

4. Add a source statement to the syslog-ng configuration file that uses the tls(key-file(key_file_fullpathname) cert-file(cert_file_fullpathname)) option and specify the key and certificate files. The source must use the source driver (network() or syslog()) matching the destination driver used by the syslog-ng client. See the provided example at the above link.

5. Disable mutual authentication for the source by setting the following TLS option in the source statement: tls(peer-verify(optional-untrusted).

Use of a “syslog-ng” syslog server is not required. Any syslog server could similarly be configured with the previous settings specific to the syslog server being used.

FTP_TRP.1/Admin Trusted Path

The TOE provides HTTPS (TLSv1.2) and SSH to support secure remote administration when administrators access the web server GUI or CLI remotely.

Executing the **FIPSMODE ON** command will limit the cryptographic key generation algorithms, cryptographic key establishment methods, data encryption/decryption algorithms, signature generation and verification services, cryptographic hashing services, and keyed-hash message authentication to those specified in [ST] for Crestron DigitalMedia NVX Series v5.2 acting as an HTTPS/TLS server.

See [CCECG] Section FCS_SSHS_EXT.1 *SSH Server Protocol* for configuration required for the TOEs SSH Server.

The administrator establishes a remote administrative session over HTTPS by opening a browser on the administrator’s workstation or laptop, and navigating to the applicable URL to access the TOE’s web server GUI. The administrator establishes a remote administrative session over SSH by starting up an SSH client on the administrator’s workstation or laptop and connecting to the TOE using a configured administrative account and the TOE’s hostname or IP address.