Prepared by:
John Walker
Compliance Engineer
Pyronix Ltd

Date:
17.07.2025

Published version:
01

ENFORCER V11

EN18031-1 DECISION TREE REFERENCE GUIDE

All Questions and Answers from the EN 18031-1 Decision Trees

Pyronix

Product
Enforcer V11

Security Assets
- User access codes
- Wi-Fi credentials

Network Assets
- Wi-Fi connection to router
- 4G connection to cell service

Requirement	Decision Tree Question	Yes/No	Outcome	Reason
[ACM] Access control mechanism				
[ACM-1] Applicability of access control mechanisms	**DT.ACM-1-DN-1**			
	Is the public accessibility of the asset the Equipments intended equipment function?	No	Proceed to DT.ACM-1.DN-2	"Users need to remotely access panel via app, to control the panel. Public Access – Definition of public access (within EN 18031-1:2024 context) Public access means any access to a product, system, or location that is not restricted by physical or logical access controls — in other words, access is open to any member of the public without prior authentication, authorisation, or validation."
	DT.ACM-1.DN-2			
	Do physical or logical measures in the targeted operational environment limit the accessibility to authorized entities?	Yes	ACM-1 Not applicable	Yes? Physical barriers block unauthorised physical access to the device. Logical barriers such as user codes and passwords exist to limit remote (and physical) access to the panel. Different codes can provide different levels of access, also.
	DT.ACM-1.DT-3			
	Do legal implications not allow access control mechanisms?	N/A	N/A	N/A
	DT.ACM-1.DN-4			
	Are there access control mechanisms that manage entities' access to the security assets?	N/A	N/A	N/A
[ACM-2] Appropriate access control mechanisms	**DT.ACM-2.DN-1**			
	Do the access control mechanisms ensure that only authorized entities have access to the protected security asset or network asset?	Yes	Pass ACM.2	HSL-001 All operations that can manage and control the system and access to sensitive resources must undergo security authentication HSL-002 All security authentication processes must be completed on the server side HSL-003 Functions that bypass system security mechanisms and directly access the system or data are prohibited HSL-004 User access authorization and permission control are required
[AUM] Authentication mechanism				
[AUM-1-1]	**DT.AUM-1-1.DN-1**			
	Is the managed access for network functions or network functions configuration and is the absence of authentication required for the equipment's intended functionality?	No	Proceed to DT.AUM-1-1.DN-2	HSL-001 All operations that can manage and control the system and access to sensitive resources must undergo security authentication HSL-002 All security authentication processes must be completed on the server side HSL-003 Functions that bypass system security mechanisms and directly access the system or data are prohibited

Requirement	Decision Tree Question	Yes/No	Outcome	Reason
	DT.AUM-1-1.DN-2			
	Is the managed access performed over networks where access is limited to authorized entities?	Yes	Proceed to DT.AUM-1-1.DN-3	HSL-001 All operations that can manage and control the system and access to sensitive resources must undergo security authentication HSL-002 All security authentication processes must be completed on the server side HSL-003 Functions that bypass system security mechanisms and directly access the system or data are prohibited
	DT.AUM-1-1.DN-3			
	Does the managed access use authentication mechanisms?	Yes	Pass AUM-1-1	Authentication methods used app for cloud and app functionality
[AUM-1-2] Requirement user interface	**DT.AUM-1-2.DN-1**			
	Is the managed access performed over a user interface where physical or logical measures in the targeted environment provide confidence in the correctness of an entity's claim?	No	Proceed to DT.AUM-1-2.DN-2	Authentication methods used
	DT.AUM-1-2.DN-2			
	Is the managed access only for reading of network functions or network functions configuration where access without authentication is needed to enable the intended equipment functionality?	No	Proceed to DT.AUM-1-2.DN-3	Authentication is required for access
	DT.AUM-1-2.DN-3			
	Is the managed access only for reading of network functions or network functions configuration where access without authentication is needed because legal implications do not allow for authentication mechanisms?	No	Proceed to DT.AUM-1-2.DN-4	Authentication method are employed
	DT.AUM-1-2.DN-4			
	Does the managed access use authentication mechanisms?	Yes	Pass AUM-1-2	For entities to access manages security and network assets needs valid authentication credentials
[AUM-2] Appropriate authentication mechanisms for external interfaces	**DT.AUM-2.DN-1**			
	Does the authentication mechanism examine evidence from at least one element of the categories knowledge, possession and inherence (one factor authentication)?	Yes	PASS AUM-2	Entities need to pass at least 1 area of authentication (password or biometric can be employed)

Requirement	Decision Tree Question	Yes/No	Outcome	Reason
[AUM-3] Authenticator validation	**DT.AUM-3.DN-1**			
	Does the authentication mechanism validate all relevant properties considering the available information about the authenticator in the operational environments of use?	Yes	PASS AUM-3	for entities to access manages security and network assets needs valid authentication credentials, this covers all the relevant information for authentication
[AUM-4] Changing authenticators	**DT.AUM-4.DN-1**			
	Does the change of the authenticator conflict security goals?	No	Proceed to DT.AUM-4.DN-2	Multiple entities can be added all with different authentication credentials
	DT.AUM-4.DN-2			
	Does the authentication mechanism allow the change of the authenticator?	Yes	PASS AUM-4	Multiple entities can be added all with different authentication credentials
[AUM-5] Password strength				
[AUM-5 -1] Requirement for factory default passwords Factory default password strength	**DT.AUM-5-1.DN-1**			
	Is the password enforced to be changed by the user before or on first use?	Yes	PASS AUM-5-1	On first using engineer default changing the engineer code is enforced and adding level 2 manager code is added
	DT.AUM-5-1.DN-2			
	Is the password unique per equipment?	N/A	N/A	N/A
	DT.AUM-5-1.DN-3			
	Does the password follow best practice concerning strength?	N/A	N/A	N/A
[AUM- 5-2] Requirement for non-factory default passwords	**DT.AUM-5-2.DN-1**			
	Is the password enforced to be set by the user before or on first use and before the equipment is logically connected to a network?	Yes	Pass AUM-5	User is instructed to change password when first entering configuration menus, which are required for network functionality.
	DT.AUM-5-2.DN-2			
	Is the password defined by an authorized entity within a network where access is limited to authorised entities?	N/A	N/A	N/A

Requirement	Decision Tree Question	Yes/No	Outcome	Reason
	DT.AUM-5-2.DN-3			
	Is the password generated by the equipment using best practice concerning strength and only communicated to an authorized entity within a network where access is limited to authorised entities?	N/A	N/A	N/A
[AUM-6] Brute force protection	**DT.AUM-6.DN-1**			
	Has the authentication mechanism the capability to be resilient against brute force attacks?	Yes	Pass AUM-6	Code guessing system protects panel from direct brute force attacks
[SUM] Secure update mechanism				
[SUM-1] Applicability of update mechanisms	**DT.SUM-1.DN-1**			
	Does the part of the software affect security assets and/or network assets?	Yes	Proceed to DT.SUM-1.DN-2	
	DT.SUM-1.DN-2			
	Do functional safety implications prohibit updatability?	No	Proceed to DT.SUM-1.DN-3	
	DT.SUM-1.DN-3			
	Is the software or firmware immutable?	No	Proceed to DT.SUM-1.DN-4	
	DT.SUM-1.DN-4			
	Do alternative measures exist that protect security assets and/or network assets during the entire lifecycle?	Yes	SUM-1 Not applicable	Software updates need to be done locally so are protected by system security features.
	DT.SUM-1.DN-5			
	Does the equipment provide at least one update mechanism for updating the part of the software?	Yes	Pass SUM-1	Update mechanism requires physical access to the equipment and proprietary equipment to affect the update
[SUM-2] Secure updates	**DT.SUM-2.DN-1**			
	Does the update mechanism ensure to only install software whose integrity and authenticity are valid at the time of installation?	Yes	Pass SUM-2	"Updates can only be completed by engineer with level 3 access with correctly configured software on proprietary update dongle. If we are allowing physical OTA methods, I disagree that this complies. The uploaded software is not authenticated to be genuine."
[SUM-3] Automated updates	**DT.SUM-3.DN-1**			
	Is the update mechanism capable of updating the software without human intervention at the equipment?	No	Proceed to DT.SUM-3.DN-2	N/A

Requirement	Decision Tree Question	Yes/No	Outcome	Reason
	DT.SUM-3.DN-2			
	Is the update mechanism capable of updating the software via scheduling the installation of an update under human approval?	No	Proceed to DT.SUM-3.DN-3	
	DT.SUM-3.DN-2			
	Is the update mechanism capable of updating the software via triggering theinstallation of an update under human approval?	Yes	pass SUM-3	Updates are performed by authorised personnel with engineer level access at the equipment
[SSM] Secure storage Mechanism				
[SSM-1] Applicability of secure storage mechanisms	**DT.SSM-1.DN-1**			
	Is the storage of the network asset or security asset protected by physical or logical measures in the equipment's target operational environment?	Yes	SSM-1 not applicable	Physical measures protect the storage of security and network assets. No direct access or ability to manipulate stored information with out triggering alarms
	DT.SSM-1.DN-2			
	Is the storage of the network asset or security asset implemented by a secure storage mechanism?	N/A	N/A	N/A
[SSM-2] Appropriate integrity protection for secure storage mechanisms	**DT.SSM-2.DN-1**			
	Is the integrity of the asset protected to ensure that attacks on secure storage do not lead to its manipulation?	N/A	N/A	N/A
[SSM-3] Appropriate confidentiality protection for secure storage mechanisms	DN.SSM-3.DN-1			
	Is the secrecy of the confidential security parameter and confidential network function protected to ensure that attacks on secure storage do not lead to its disclosure?	N/A	N/A	N/A
[SCM] Secure communication mechanism				
[SCM-1] Applicability of secure communication mechanisms	**DT.SCM-1.DN-1**			
	Is the secure communication of network assets or security assets ensured by a secure communication mechanism?	Yes	Pass SCM-1	Sensitive data is encrypted, over a conventionally insecure link, using standard symmetric key encryption mechanism(s).

Requirement	Decision Tree Question	Yes/No	Outcome	Reason
	DT.SCM-1.DN-2			
	Is the temporary exposure of network assets or security assets required as part ofestablishing or managing a connection?	N/A	N/A	N/A
	DT.SCM-1.DN-3			
	Does the targeted environment ensure that network assets or security assets are not exposed to unauthorised entities?	N/A	N/A	N/A
[SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms	**DT.SCM-2.DN-1**			
	Are best practices applied to protect theintegrity and authenticity of the communicated asset?	Yes	Pass SCM-2	Encrypted data communicated with a signature for example, to provide both authenticity and integrity.
	DT.SCM-2.DN-2			
	Is a deviation from best practice for integrity or authenticity protection inevitable for interoperability reasons?	N/A	N/A	N/A
[SCM-3] Appropriate confidentiality protection for secure communication mechanisms	**DT.SCM-3.DN-1**			Perhaps should be N/A?
	Is best practices applied to protect the confidentiality of the communicated asset?	Yes	Pass SCM-3	No data that is personally confidential or identifying (except to identify the specific device) is passed in the communicated assets by default. An exception occurs here where a user has provided specific input that may contain sensitive information, but this is encrypted and access restricted. But the key here is that no information is provided that may allow a malicious actor to impersonate the device's owner / user.
	DT.SCM-3.DN-2			
	Is a deviation from best practice inevitable for interoperability reasons?	N/A	N/A	N/A
[SCM-4] Appropriate replay protection for secure communication mechanisms	**DT.SCM-4.DN-1**			
	Are best practices applied to protect the communicated asset against replay attacks?	Yes	Pass SCM-4	"What is best practice and who defines it. The encryption is strong, also uses an internal counter to stops replay attacks, which is within the encrypted message."
	DT.SCM-4.DN-2			
	Does a duplicate transfer not impose a threat of a replay attack?	N/A	N/A	N/A

Requirement	Decision Tree Question	Yes/No	Outcome	Reason
	DT.SCM-4.DN-3			
	Is a deviation from best practice inevitable for interoperability reasons?	N/A	N/A	N/A
[RLM] Resilience mechanism				
[RLM-1] Applicability of resilience mechanisms	**DT.RLM-1.DN-1**			
	Does the equipment use resilience mechanisms to mitigate the effects of DoS attacks on the network interfaces and return to a defined state after the attack?	Yes	Pass RLM-1	Panel creates a fault for loss of normal communication (timed) panel comms will recover after the DoS attack conditions are removed.
	DT.RLM-1.DN-2			
	Is the network interface intended to be used to communicate with other equipment in a local network only?	N/A	N/A	N/A
	DT.RLM-1.DN-3			
	Do other devices in the network provide sufficient protection against DoS attacks and loss of function of the equipment?	N/A	N/A	N/A
[NMM] Network monitoring mechanism				
[NMM-1] Applicability of and appropriate network monitoring mechanisms	**DT.NMM-1.DN-1**			
	Is the equipment a Network Equipment?	Yes	Proceed to DT.NMM-1.DN-2	
	DT.NMM-1.DN-2			
	Does the Network Equipment provide a network monitoring mechanism to detect indicators of DoS attacks?	Yes	pass NMM-1	Panel has comms fault timer as a mechanism that can detect if internet connection is lost
[TCM] Traffic control mechanism				
[TCM-1] Applicability of and appropriate traffic control mechanisms	**DT.TCM-1.DN-1**			
	Is the equipment a Network Equipment?	Yes	Proceed to DT.TCM-1.DN-2	
	DT.TCM-1.DN-2			
	Does the Network Equipment provide a traffic control mechanism?	Yes	Pass TCM-1	"Panel only uses outbound, whilst incoming traffic is silently dropped. Panel uses TCP which includes traffic control measures."

Requirement	Decision Tree Question	Yes/No	Outcome	Reason
[CCK] Confidential cryptographic keys				
[CCK-1] Appropriate Confidential cryptographic keys (CCKs)	**DT.CCK-1.DN-1**			
	Is the CCK solely used by a specific security mechanism,where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM?	Yes	DT.CCK-1 not applicable	The CCK is solely used by a specific security mechanism e.g. encrypted cloud communication.
	DT.CCK-1.DN-2			
	Does the CCK support a minimum security strength of 112-bits?	N/A	N/A	N/A
[CCK-2] Confidential cryptographic key generation mechanisms	**DT.CCK-2.DN-1**			
	Is the CCK solely used for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM, AUM, SCM, SUM or SSM?	No	Proceed to DT.CCK-2.DN-2	
	DT.CCK-2.DN-2			
	Does the generation mechanism for the CCK adhere to best practice cryptography?	Yes	pass CCK-2	Keys used as 1/2 of symmetric key pair to generate a shared secret (ECDH) which is a standard mechanism.
[CCK-3] Preventing static default values for confidential cryptographic keys	**DT.CCK-3.DN-1**			
	Is this CCK practically unique per equipment?	Yes	Pass CCK-3	CCK generated by the device, using device characteristics and chaotic quantities e.g. a time stamp [don't know if it actually uses a time stamp but example of chaotic quantity]
	DT.CCK-3.DN-2			
	Is the CCK only used for establishing initial trust relationships under conditions controlled by an authorized entity?	N/A	N/A	N/A
	DT.CCK-3.DN-3			
	Is the CCK a shared parameter required for the equipment's intended functionality?	N/A	N/A	N/A

Requirement	Decision Tree Question	Yes/No	Outcome	Reason
[GEC] General equipment capabilities				
[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities	**DT.GEC-1.DN-1**			
	Does the software and/or the hardware contain publicly known exploitable vulnerabilities?	No	Pass GEC-1	No known reported vulnerabilities
	DT.GEC-1.DN-2			
	Does the vulnerability affect security assetsor network assets?	N/A	N/A	N/A
	DT.GEC-1.DN-3			
	Is the vulnerability exploitable in the specific conditions of the equipment?	N/A	N/A	N/A
	DT.GEC-1.DN-4			
	Has the vulnerability been mitigated to an acceptable residual risk?	N/A	N/A	N/A
	DT.GEC-1.DN-5			
	Has the vulnerability been accepted on a risk basis?	N/A	N/A	N/A
[GEC-2] Limit exposure of services via related network interfaces	**DT.GEC-2.DN-1**			
	Is the network interface or service available in the factory default state?	No	DT.GEC-2 not applicable	Wi-Fi credentials need to be added before internet connection can be established. Cellular connection is by additional hardware that is added during product configuration after initial power up.
	DT.GEC-2.DN-2			
	Does the network interface or service affect security assets or network assets?	N/A	N/A	N/A
	DT.GEC-2.DN-3			
	Is the network interface or service necessary for equipment setup or for the basic operation?	N/A	N/A	N/A
[GEC-3] Configuration of optional services and the related exposed network interfaces	**DT.GEC-3.DN-1**			
	Are security assets or network assets affected by the network interface or service?	Yes	Proceed to DT.GEC-3.DN-2	

Requirement	Decision Tree Question	Yes/No	Outcome	Reason
	DT.GEC-3.DN-2			
	Is an option provided for an authorized user to enable and disable the network interface or service?	Yes	Pass GEC-3	Engineer can disable Wi-Fi and GPRS connections - remote connections entirely.
[GEC-4] Documentation of exposed services via network interfaces	**DT.GEC-4.DN-1**			
	Is the network interface or service delivered as part of the factory default state?	No	DT.GEC-4 not applicable	
	DT.GEC-4.DN-2			
	Is the exposed network interface or exposed described in the user documentation?	N/A	N/A	N/A
[GEC-5] No unnecessary external interfaces	**DT.GEC-5.DN-1**			
	Is the physical external interface necessary for the intended functionality?	Yes	Pass GEC-5	Panel needs user input for normal operation via control and indicating equipment
[GEC-6] Input validation	**DT.GEC-6.DN-1**			
	Is the interface capable of receiving input?	Yes	Proceed to DT.GEC-6.DN-2	For all considered interfaced external input can be received
	For every means of receiving input			
	DT.GEC-6.DN-2			
	Is input validation functionality used for input that has potential impact on security assets and/or network assets?	Yes	Pass GEC-6	"Wireless Hub replay attacks, Cannot be used to attack the wireless interface. Wireless communication protocol uses a sequential numbering system for message validation purposes SMS Also only allow incoming messages from numbers registered in the panel as a means of validating SMS input. Any SMS messages from numbers not registered gets dropped. set to IP by default (internet)."
[CRY] Cryptography				
[CRY-1] Best practice Cryptography	**DT.CRY-1.DN-1**			
	Is the cryptography used for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM, AUM, SCM, SUM or SSM?	No		Cannot have deviation.
	DT.CRY-1.DN-2			
	Is the cryptography best practice concerning the protection of the security assets or network assets?	Yes	Pass CRY-1	Encryption method uses best practice.