Merlin – EN 303 645 v3.1.3

AN-006-WIE

Hardware Models	Merlin Series
Revision	1.00
Approval status	Approved
Date	6 November 2025
Brief description	Annex B response document for EN 303 645 v3.1.3
Author	Artur Wachowski

1 Overview

1.1 Firmware information

Firmware version: SXL-**25.05.15.000** or newer.

1.2 Assumptions

This EN 303645 Anex B.1 response document can be applied to all routers in the Merlin Series.

1.3 Corrections

Requests for new application notes or corrections or amendments to this application note are welcome and should be addressed to support.ie@westermo.com

1.4 Foreword

The **EN 303 645 V3.1.3** documentation, developed by **ETSI** experts, primarily addresses domestic, mass-produced consumer devices intended for personal use with limited industrial applicability. However, the inclusion of "IoT gateways, base stations and hubs to which multiple devices connect" to the scope alongside products such as baby toys, smart speakers, washing machines, smoke detectors, and window sensors has led to confusion among consumers of Westermo Ireland's Merlin Series.

Westermo Ireland devices are not designed to collect, process, track movement, behavioural monitoring or mainly storage/transmit personal data, adhering strictly to definitions pertaining to personal data and privacy protection.

Westermo Ireland devices provide advanced networking and routing solutions specifically engineered for radio communication technologies. It is assumed that administrative personnel deploying these devices have the necessary expertise to design, manage, secure, and troubleshoot OT/IT networks, including evaluating security features and performing basic threat modelling on Merlin Series routers prior to deployment in production environments. Installation should only occur after the successful completion of all provisioning procedures and acceptance testing, which must encompass the required on-site and production security assessments. In summary, Westermo Ireland devices should not be categorized as standard Internet of Things products intended for domestic use.

1.5 Executive summary

Westermo Ireland devices are compliant with **EN 303 645 V3.1.3** specifications.

2 Table B.1 Implementation of provisions for consumer IoT security

2.1 Implementation conformance statement pro forma

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document can freely reproduce the pro forma in the present annex so that it can be used for its intended purposes and can further publish the completed annex including table B.1.

Table B.1 can provide a mechanism for the user of the present document (who is expected to be an entity involved in the development or manufacturing of consumer IoT) to give information about the implementation of the provisions within the present document.

The reference column gives reference to the provisions in the present document.

The status column indicates the status of a provision. The following notations are used:

M The provision is a mandatory requirement

R The provision is a recommendation

C The provision is conditional. If the condition is not satisfied, the provision can be marked as N/A in an implementation conformance statement.

F This provision applies to a feature, capability or mechanism. The existence of the feature, capability or mechanism is not determined to be mandatory/recommended by the provision. If the feature, capability or mechanism does not exist, the provision can be marked as N/A in an implementation conformance statement.

NOTE 1: Where the Feature (F) notation is used, the provision applies to all instances of the feature. The feature, capability or mechanisms are identified by the lettered footnotes at the bottom of the table with references provided for the relevant provisions.

NOTE 2: Where the Conditional (C) notation is used, this is conditional on the text of the provision. The conditions are provided in the numbered footnotes at the bottom of the table with references provided for the relevant provisions to help with clarity.

The support column can be filled in by the user of the present document. The following notations are used:

Y The provision is supported by the implementation

N The provision is not supported by the implementation

N/A The provision is not applicable, either because a condition is not satisfied, or because a feature, capability or mechanism the provision applies to does not exist.

The detail column can be filled in by the user of the present document:

- If a provision is supported by the implementation, the entry in the detail column is to contain information on the measures that have been implemented to achieve support.

- If a provision is not supported by the implementation, the entry in the detail column is to contain information on the reasons why implementation is not possible or not appropriate.

- If a provision is not applicable, the entry in the detail column is to contain the rationale for this determination.

Table B.1: Implementation of provisions for consumer IoT security

Reference	Status	Sup.	Detail	EN 303 645 v3.1.3
Provision 5.0-1	M	Y	This document addresses the provision 5.0.1. Product's Thread Medeling is performed as a standard product security regression testing review.	Record justification for any recommendation not applicable or not fulfilled.
Provision 5.1-1	M F(a)	Y	The default configuration activates the "first logon" feature, which requires users to change their access password prior to initial use. Detailed options are provided in section 5.5 of the AN_005-WIE Security Hardening Guide, available on Merlin's product page.	All passwords unique per device or user-defined; no universal defaults beyond factory state.
Provision 5.1-2	M F(b)	Y	The default configuration enables the "first logon" feature, requiring users to update their access password prior to initial use. End-users are expected to adhere to recommended best practices, such as those outlined in NIST Special Publication 800-63B [i.3]. Detailed options for initial user-access are provided in section 5.5 of the AN_005-WIE Security Hardening Guide, available on Merlin's product page.	Pre-installed credentials (if any) are unique per device and sufficiently randomized.
Provision 5.1-2A	R	Y	Westermo Ireland devices are fully configurable; end-users are advised to follow recommended best practices to ensure device security. These devices support both password and certificate-based authentication, where applicable.	Passwords should not be used for machine-to-machine authentication.

Provision 5.1-3	M F(c)	Y	Westermo Ireland devices offer comprehensive configuration capabilities, allowing users to specify or select cryptographic algorithms, ciphers, and key lengths as required. End-users are encouraged to adhere to established best practices for cryptography to ensure secure communications. It is also recommended that devices be integrated with Public Key Infrastructure (PKI) and that cryptographic feeds (e.g. certificates) are updated regularly. For further details regarding cryptographic access options, please refer to section 5.14 of the AN_005-WIE Security Hardening Guide, available on Merlin's product page.	Authentication mechanisms used to authenticate users against the consumer IoT device or used for machine-to-machine authentication shall use best practice cryptography, appropriate to the properties of the technology, operating environment, risk and usage.
Provision 5.1-4	M F(d)	Y	Westermo Ireland devices offer comprehensive configuration options, allowing end-users to access the device through either the CLI or WebUI to modify any configuration parameter only following successful authentication, including device access passwords. These devices feature advanced user management capabilities and support integration with third-party AAA services. For additional information on user management, please consult section 5.7 of the AN_005-WIE Security Hardening Guide, for additional information on password changing process consult Management Guide, both documents are available on Merlin's product page.	Where a user can authenticate against a consumer IoT device, the consumer IoT device shall provide to the user or an administrator a simple mechanism to change the authentication value used.

Provision 5.1-5	M C F(14,e)	Y	Westermo Ireland devices are equipped with advanced connection-oriented stateful firewall capabilities and integrated session control features, depending on the protocol. The firewall, along with its rate-limiting function, serves as the primary line of defence against attacks originating from public sources. A secondary layer of protection guards against internal threats, such as an attacker who has circumvented the firewall by exploiting an allowed addressing scheme; in these cases, application-level brute force protection mechanisms become active. Both layers provide monitoring logs that can be used to trigger alarms when an intrusion attempt is detected.	The consumer IoT device shall have a mechanism available which makes successful brute-force attacks on authentication mechanisms via network interfaces impracticable unless the device has a resource constraint determined by the use case that prevents the implementation.
Provision 5.2-1	M	Y	Details regarding vulnerability disclosure policy are available in Section 6 of the AN_005-WIE Security Hardening Guide.	The manufacturer shall make a vulnerability disclosure policy publicly available.
Provision 5.2-2	R	Y	Details regarding vulnerability remediation timelines are available in Section 6 of the AN_005-WIE Security Hardening Guide.	Disclosed vulnerabilities should be acted on in a timely manner.
Provision 5.2-3	R	Y	Details regarding continuous software composition monitoring are available in Section 6 of the AN_005-WIE Security Hardening Guide.	Monitor/rectify vulnerabilities across supported products/services during defined support period.
Provision 5.3-1	R F(f)	Y	The Merlin device supports only compacted image updates, with all images digitally signed to ensure the integrity of the software. Software image components are updatable and delivered securely. For reporting security issues or vulnerabilities related to Merlin devices, please contact: PSIRT.ie@westermo.com	All software components in consumer IoT devices that are not immutable due to security reasons should be securely updateable.
Provision 5.3-2	M C(15)	Y	The Merlin device utilises secure updates through authenticated channels only. Furthermore, software images are digitally signed to guarantee the integrity of the software.	The consumer IoT device shall have a secure update mechanism unless the device has a resource constraint determined by the use case that prevents the implementation.
Provision 5.3-3	M F(g)	Y	Software update feature is available via WebUI.	An update shall be simple for the user to apply.

Provision 5.3-4A	R F(g)	N	Not supported. The Merlin device does not support automatic software updates or a "call home" feature. Devices are designed to operate solely within the intended operational environment specified by end users. Users are advised to utilize the provided device management system, Activator, which facilitates software and configuration update tasks. Experienced users may develop specialized automation processes to manage software updates efficiently.	At least one secure update mechanism configurable to be automated.
Provision 5.3-4B	R F(h)	N	Not supported. The Merlin device does not support automatic software updates or a "call home" feature. Devices are designed to operate solely within the intended operational environment specified by end users. Users are advised to utilize the provided device management system, Activator, which facilitates software and configuration update tasks. Experienced users may develop specialized automation processes to manage software updates efficiently.	During initialization the consumer IoT device should activate an automatic secure update mechanism after user's consent.
Provision 5.3-5	R F(g)	N	Not supported. The Merlin device is designed to function exclusively within the operational environment designated by end users. It is recommended that users regularly monitor the system or coordinate with Westermo Ireland for security updates.	The consumer IoT device or an associated service should check after initialization whether security updates are available.
Provision 5.3-6A	R F(h)	N	Not supported. The Merlin device does not support automatic software updates nor a "call home" feature.	If the consumer IoT device supports automated updates, the user should be able to enable and disable the automatic update mechanism and postpone the installation of updates provided via an automatic update mechanism.
Provision 5.3-6B	R F(i)	N	Not supported. The Merlin device does not support automatic software updates nor a "call home" feature.	If the consumer IoT device supports update notifications, the user should be able to enable and disable the update notifications.

Provision 5.3-7	M F(g)	Y	Secure updates can be performed with authenticated channels only, CLI (SSH) or WebUI (HTTPs / TLS). Westermo Ireland devices offer comprehensive configuration capabilities, allowing users to specify or select cryptographic algorithms, ciphers, and key lengths as required. End-users are encouraged to adhere to established best practices for cryptography to ensure secure communications. It is also recommended that devices be integrated with Public Key Infrastructure (PKI) and that cryptographic feeds (e.g. certificates) are updated regularly. For further details regarding cryptographic access options, please refer to section 5.14 of the AN_005-WIE Security Hardening Guide, available on Merlin's product page.	The consumer IoT device shall use best practice cryptography to facilitate secure update mechanisms.
Provision 5.3-8	M C(12)	Y	Details regarding vulnerability remediation timelines are available in Section 6 of the AN_005-WIE Security Hardening Guide.	Security updates shall be timely (prioritize critical fixes).
Provision 5.3-9	R F(g)	Y	The Merlin device supports only compacted image updates, with all images digitally signed to ensure the integrity of the software. Device automatically Verify authenticity and integrity of updates before install and during every bootup.	Verify authenticity and integrity of updates before install.
Provision 5.3-10	M F(j)	Y	Secure updates can be performed with authenticated channels only, CLI (SSH) or WebUI (HTTPs / TLS). The Merlin device supports only compacted image updates, with all images digitally signed to ensure the integrity of the software. Device automatically Verify authenticity and integrity of updates before install and during every bootup.	Updates delivered over network must be verified via trust relationship (e.g., signatures, TLS).
Provision 5.3-11	R C(12)	Y	Details regarding Security Advisory statements are available in Section 6 of the AN_005-WIE Security Hardening Guide.	The user should be informed in a recognizable and apparent manner that a security update is required together with information on the risks mitigated by that update.

Provision 5.3-12	R C(12)	Y	Westermo Ireland's software release testing procedure ensures that basic functionality remains unaffected; new releases are subject to comprehensive regression testing. Detailed information about all software changes is available in the Release Notes documentation.	The user should be notified when the application of a software update will disrupt the basic functioning of the consumer IoT device.
Provision 5.3-13	M	Y	The warranty is specified in the product data sheet, which can be found on the product page and is typically five years. Special arrangements may be made to extend the support period upon request.	The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period.
Provision 5.3-14	R C(3)	Y	If the device is no longer under warranty and has been designated as end-of-life, it is advisable to decommission and replace the device. Otherwise, software updates will continue to be provided.	For consumer IoT devices that cannot have their software updated, the rationale for the absence of software updates, the period and method of hardware replacement support should be published by the manufacturer in an accessible way that is clear and transparent to the user.
Provision 5.3-15A	R C(3)	Y	If the device is no longer under warranty and has been designated as end-of-life, it is advisable to decommission and replace the device.	For devices that cannot have their software updated, the consumer IoT device should be isolable
Provision 5.3-15B	R C(3)	Y	If the device is no longer under warranty and has been designated as end-of-life, it is advisable to decommission and replace the device. Otherwise, software updates will continue to be provided.	For devices that cannot have their software updated, the consumer IoT device hardware should be replaceable.
Provision 5.3-16	M	Y	Westermo Ireland devices are clearly labelled and easily identifiable due to apparent interface differences across models. Additionally, device-specific information can be accessed directly from the device itself.	The model designation of the consumer IoT device shall be clearly recognizable, either by labelling on the consumer IoT device or via a user interface.
Provision 5.4-1	M F(k)	Y	Merlin Series routers are equipped with a Trusted Platform Module (TPM) for secure private key storage and support disk encryption tied to the hardware TPM. The storage encryption feature is designed to protect Data at Rest from external exfiltration attempts. The feature is optional and must be activated by the user. Further details about Data at Rest protection can be found in Section 15 of the AN_005-WIE Security Hardening Guide.	Sensitive security parameters in persistent storage shall be stored securely by the consumer IoT device.

Provision 5.4-2	M F(l)	Y	All devices connecting to cellular networks (LTE/5G) require a UICC, which may be either a physical SIM card or an embedded eSIM. The UICC securely stores authentication keys and subscriber identity in encrypted format for network access. For "user space" secure communication configurations, the Westermo Ireland device utilises serial numbers as unique, hard-coded identifiers that are specifically designed to be tamper-resistant and immutable. It is recommended to integrate these identifiers with public key infrastructure (PKI) and utilize certificates over passwords for all secure communications.	Hard-coded unique per-device identity (if used) must resist tampering.
Provision 5.4-3	M	Y	Westermo Ireland devices are subject to regular product security testing procedures, including binary analysis - credential scans, to ensure that no hardcoded credentials are present in standard device operations.	Hard-coded critical security parameters in consumer IoT device software source code shall not be used
Provision 5.4-4	M F(m)	Y	Westermo Ireland devices do not contain hardcoded security parameters for verifying integrity and authenticity; these responsibilities rest solely with users. Proper administration of passwords and certificates—collectively known as "secrets"—is critical to maintaining device security. Westermo Ireland highly recommends integrating devices into a public key infrastructure (PKI) and enabling certificate auto-enrolment using the SCEP protocol. Software integrity and authenticity verification, commonly referred to as Hardware Secure Boot, is performed with the support of Public Key securely stored in hardware, in One Time Memory (OTM) fuse.	Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated services in consumer IoT device software shall be unique per device and shall be produced with a mechanism that reduces the risk of automated attacks against classes of consumer IoT devices.

Provision 5.5-1	M	Y	Westermo Ireland devices offer comprehensive configuration capabilities, allowing users to specify or select cryptographic algorithms, ciphers, and key lengths as required. End-users are encouraged to adhere to established best practices for cryptography to ensure secure communications. It is also recommended that devices be integrated with Public Key Infrastructure (PKI) and that cryptographic feeds (e.g. certificates) are updated regularly. For further details regarding cryptographic access options, please refer to section 5.14 of the AN_005-WIE Security Hardening Guide, available on Merlin's product page.	The consumer IoT device shall use best practice cryptography to communicate securely.
Provision 5.5-2	R	Y	Westermo Ireland devices offer comprehensive configuration capabilities, allowing users to specify or select cryptographic algorithms, ciphers, and key lengths as required. End-users are encouraged to adhere to established best practices for cryptography to ensure secure communications. It is also recommended that devices be integrated with Public Key Infrastructure (PKI) and that cryptographic feeds (e.g. certificates) are updated regularly. For further details regarding cryptographic access options, please refer to section 5.14 of the AN_005-WIE Security Hardening Guide, available on Merlin's product page.	The consumer IoT device should use reviewed or evaluated implementations to deliver network and security functionalities, particularly in the field of cryptography.

Provision 5.5-3	R	Y	Westermo Ireland devices offer comprehensive configuration capabilities, allowing users to specify or select cryptographic algorithms, ciphers, and key lengths as required. End-users are encouraged to adhere to established best practices for cryptography to ensure secure communications. It is also recommended that devices be integrated with Public Key Infrastructure (PKI) and that cryptographic feeds (e.g. certificates) are updated regularly. For further details regarding cryptographic access options, please refer to section 5.14 of the AN_005-WIE Security Hardening Guide, available on Merlin's product page.	Cryptographic algorithms and primitives should be replaceable (cryptoagility).
Provision 5.5-4	R	Y	Access to Westermo Ireland devices by humans, whether via the CLI or WebUI, is permitted only following successful authentication. Machine-to-machine access and service communications, such as networked server interfaces (for example, on-device SNMP servers), should be configured according to industry standards, always utilizing the latest version with robust security parameters. Westermo Ireland strongly recommends configuring client services on end devices and securing all service communications through VPN technology.	Access to consumer IoT device functionality via a network interface in the initialized state should only be possible after authentication on that interface.
Provision 5.5-5	M F(n)	Y	Westermo Ireland devices provide extensive configuration capabilities, enabling only authenticated users to access the device via either the CLI or WebUI to modify any configuration parameter, including device access passwords. The listed EN303645 exceptions such as ARP, DHCP, DNS, ICMP, and NTP may be managed and monitored through firewall settings.	Consumer IoT device functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication.
Provision 5.5-6	R F(o)	Y	Configuration management, including the handling of critical security parameters, should be conducted through CLI (SSH) or WebUI (HTTPS). These access protocols ensure confidentiality and integrity for data in transit.	Critical security parameters should be encrypted in transit, with such encryption appropriate to the properties of the technology, risk and usage.

Provision 5.5-7	M F(o)	Y	Westermo Ireland devices facilitate configuration management through either a Command Line Interface (CLI) accessed via SSH, or a Web User Interface (WebUI) accessed via HTTPS. Provision is rather not applicable. Rationale: Typical devices do not employ the concept of "critical security parameters used by the device can be communicated outside of the device." For any devices configured with multi-factor authentication, the generation and delivery of authentication factors to users shall be handled by third-party services, such as authenticator applications, rather than by the devices themselves for security reasons.	The consumer IoT device shall protect the confidentiality of critical security parameters that are communicated via remotely accessible network interfaces.
Provision 5.5-8	M C(16)	Y	Westermo Ireland's SDLC process is certified with IEC62443-4-1. Current certificate is available at https://www.exida.com	The manufacturer shall follow secure management processes for critical security parameters that relate to the consumer IoT device and for the entire lifecycle of the critical security parameters.
Provision 5.6-1	M F(p)	Y	Westermo Ireland devices offer comprehensive configuration options, allowing users to tailor device parameters and behaviour as needed, including the ability to deactivate unused network interfaces. It is the sole responsibility of end users to ensure their production configurations adhere to industry security standards. To support this effort, Westermo Ireland offers a comprehensive Security Hardening Guide (AN_005-WIE), which is available online on the product pages, its intention is to assist users with their configuration decisions.	All unused network interfaces and all unused logical interfaces that are accessible through a network interface shall be disabled.

Provision 5.6-2	M	Y	Westermo Ireland devices provide extensive configuration capabilities, enabling users to customise device parameters and behaviour to their specific requirements. By default, these devices are not preconfigured for public network access and are initially accessible only through local connections. While directly connected security scanners may detect the devices' MAC addresses—revealing only the manufacturer and not the specific model—it is recommended to implement restrictive firewall settings before enabling remote access to enhance security against potential threats.	In the initialized state, the network interfaces of the consumer IoT device shall minimize the unauthenticated disclosure of security-relevant information.
Provision 5.6-3	R	Y	Westermo Ireland devices offer comprehensive configuration options, allowing users to tailor device parameters and behaviour as needed, including the ability to deactivate all physical interfaces. It is the sole responsibility of end users to ensure their production configurations adhere to industry security standards. To support this effort, Westermo Ireland offers a comprehensive Security Hardening Guide (AN_005-WIE), which is available online on the product pages, its intention is to assist users with their configuration decisions.	Consumer IoT device hardware should not unnecessarily expose physical interfaces to attack.
Provision 5.6-4A	M F(q)	Y	Westermo Ireland devices offer comprehensive configuration options, allowing users to tailor device parameters and behaviour as needed, including the ability to deactivate all physical interfaces, which could be considered as debug interfaces. It is the sole responsibility of end users to ensure their production configurations adhere to industry security standards. To support this effort, Westermo Ireland offers a comprehensive Security Hardening Guide (AN_005-WIE), which is available online on the product pages, its intention is to assist users with their configuration decisions.	Debug interfaces shall be disabled or protected via a best practice authentication or access control mechanism.

Provision 5.6-4B	R F(r)	Y	Westermo Ireland devices are commonly deployed in applications involving critical infrastructure. These devices are generally expected to be protected within secure enclosures and subject to physical monitoring measures. The recommended operational environment is outlined in the Security Hardening Guide (AN_005-WIE). Certain Merlin Series routers feature an exposed physical console port (USB-C), classified as a UART port; this port can be deactivated through configuration settings. The device does not incorporate physical self-defence mechanisms.	Debug interfaces that are physical ports should be physically protected by the device. NOTE 1: If a debug interface has been disabled, it is not necessary to physically protect it.
Provision 5.6-5	R	Y	Westermo Ireland devices offer comprehensive configuration options, allowing users to tailor device parameters and behaviour as needed for the intended use. End users are solely responsible for verifying that their production configurations meet industry security standards and have undergone appropriate security testing before deployment.	The manufacturer should only enable software services that are used or required for the intended use or operation of the consumer IoT device.
Provision 5.6-6	R	Y	The code is controlled via comprehensive configuration options, allowing users to tailor device parameters and behaviour as needed for the intended use. End users are solely responsible for verifying that their production configurations meet industry security standards and have undergone appropriate security testing before deployment.	Code should be minimized to the functionality necessary for the consumer IoT device to operate.
Provision 5.6-7	R	Y	Westermo Ireland devices implement the principle of least privilege by assigning critical services to dedicated system users with restricted system control capabilities. Furthermore, these devices incorporate a range of binary and kernel-level protections—including ASLR, NX, PIE, RELRO, and stripping—depending on the specific user space application.	Software should run with least necessary privileges, taking account of both security and functionality

Provision 5.6-8	R	Y	Westermo Ireland devices incorporate a range of binary and kernel-level protections—including ASLR, NX, PIE, RELRO, and stripping—depending on the specific application.	The consumer IoT device should include a hardware-level access control mechanism for memory
Provision 5.6-9	R	Y	Westermo Ireland's SDLC process is certified with IEC62443-4-1. Current certificate is available at https://www.exida.com	The manufacturer should follow secure development processes for software deployed on the consumer IoT device.
Provision 5.7-1	R	Y	Merlin Series devices support Hardware Secure Boot, using an on-board processor with One-Time Programmable (OTP) fuses to provide a hardware-anchored software validation chain. Each software component in the boot process is digitally signed with RSASSA_PKCS1_V1_5_SHA_256. If unauthorized software is detected, the boot process is halted, and the last known-good image is loaded.	The consumer IoT device should verify its software using secure boot mechanisms.
Provision 5.7-2	R F(s)	Y	Westermo Ireland devices are equipped with a built-in feature that enables them to automatically restore their software and file system from a ROM source upon the next reboot. These devices also offer comprehensive monitoring capabilities; administrators can configure them to track and record any configuration changes using tools such as the Audit Log. To implement any modifications or attempt to upload corrupted software, an adversary would first need to bypass the primary line of defence - authentication. Any such attempts will generate sufficient alerts to notify the administrative staff.	If an unauthorized change is detected to the software, the consumer IoT device should alert the user and/or administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function.
Provision 5.8-1	R F(t)	Y	Westermo Ireland highly recommends that all service communications, also known as data-in-transit, be secured using VPN technology. For further information, please refer to section 5.4 of the AN_005-WIE Security Hardening Guide, which can be found on Merlin's product page.	The confidentiality of personal data transiting between the consumer IoT device and associated services should be protected with best practice cryptography, appropriate to the properties of the technology, operating environment, risk and usage.

Provision 5.8-2	M F(u)	Y	Westermo Ireland highly recommends that all service communications, also known as data-in-transit, be secured using VPN technology. For further information, please refer to section 5.4 of the AN_005-WIE Security Hardening Guide, which can be found on Merlin's product page.	The confidentiality of sensitive personal data communicated between the consumer IoT device and associated services shall be protected with best practice cryptography, appropriate to the properties of the technology, operating environment, risk and usage.
Provision 5.8-3	M F(v)	Y	Certain Westermo Ireland devices are equipped with an integrated GPIO unit that serves as an external sensing capability. Comprehensive information can be found in the Management Guide, which is available on the Merlin product page.	All external sensing capabilities of the consumer IoT device shall be documented in an accessible way that is clear and transparent for the user.
Provision 5.9-1	R	Y	Westermo Ireland devices are advanced networking equipment focused on radio communication technologies like 4G and 5G. They feature automated failover, connectivity restoration and monitoring, power outage detection, and automatic boot. For more details, refer to the Management Guide on the Merlin product page.	Resilience should be built into consumer IoT products, taking into account the possibility of outages of data networks and power.
Provision 5.9-2	R	Y	Westermo Ireland devices are advanced networking equipment focused on radio communication technologies such as 4G and 5G. They feature automated failover, connectivity restoration and monitoring, power outage detection, and automatic boot. The devices are fully configurable and always recover cleanly according to user configurations. For more details, refer to the Management Guide on the Merlin product page.	Consumer IoT devices should remain operating and locally functional in the case of a loss of network access and should recover cleanly in the case of restoration of a loss of power.

Provision 5.9-3	R	Y	Westermo Ireland devices are advanced networking solutions designed to support radio communication technologies such as 4G and 5G. Key features include automated failover, connectivity restoration and monitoring, power outage detection, and automatic boot functionality. Given their operational context, these devices prioritize prompt connectivity restoration. The management of randomized delays is handled at the hub level and falls outside the responsibilities of Merlin's operations. Additionally, software update capabilities are comprehensively addressed in Provision 5.3.	The consumer IoT device should connect to networks in an expected, operational and stable state and in an orderly fashion, taking the capability of the infrastructure into consideration.
Provision 5.10-1	R F(w)	Y	Westermo Ireland devices provide extensive monitoring functionalities, enabling administrators to configure tracking of operations, communication changes such as connection attempts—including abnormal surges in failed login attempts—as well as traffic characteristics such as TX/RX rates and signal strengths. Additionally, advanced Deep Packet Inspection (DPI) allows for the monitoring of certain IP-based telemetry protocols, including Modbus, DNP3, and IEC104. Comprehensive software update procedures are detailed in Provision 5.3.	If telemetry data is collected from consumer IoT products, such as usage and measurement data, it should be examined for security anomalies.
Provision 5.11-1	M	Y	Westermo Ireland devices offer three options for Factory Reset and Decommissioning: • **Factory Reset:** Restores the current configuration (Config 1) to factory default settings and initiates a reboot using Config 1. • **Factory Reset and Certificate Deletion:** Returns Config 1 to its factory defaults, removes all security certificates, and reboots with Config 1. • **Reset for Decommissioning:** Resets both Config 1 and Config 2 to recovery settings, deletes all data including security certificates, and reboots the device using Config 1.	Users shall be provided with functionality such that all their user data can be erased from the consumer IoT device in a simple manner.

Provision 5.11-2	R F(x)	Y	Westermo Ireland devices provide three methods for factory reset and decommissioning, accessible via the WebUI interface.	The consumer should be provided with functionality on the consumer IoT device such that personal data can be deleted from associated services in a simple manner.
Provision 5.11-3	R	Y	Westermo Ireland devices provide three distinct methods for factory reset and decommissioning, each accompanied by clear descriptions.	Users should be given clear instructions on how to delete and where possible to erase their personal data from the device and associated services.
Provision 5.11-4	R	Y	Westermo Ireland devices provide three distinct options for Factory Reset and Decommissioning, each accompanied by comprehensive descriptions accessible through the WebUI. These options are thoroughly documented. For further information, please consult the Management Guide available on the Merlin product page.	Users should be provided with clear confirmation that personal data has been deleted and where possible erased from devices and associated services.
Provision 5.12-1	R	Y	Westermo Ireland devices offer advanced networking capabilities tailored for radio communication technologies. It is expected that administrative personnel possess the necessary qualifications to design, manage, secure, and troubleshoot OT/IT networks, including assessing security features and conducting fundamental threat modelling on Merlin Series routers prior to deployment in the production environment. Devices should only be installed following the successful completion of all provisioning procedures and acceptance testing. Installation and maintenance processes are structured to require minimal user intervention.	Installation and maintenance of consumer IoT should involve minimal decisions by the user and should follow security best practice on usability.
Provision 5.12-2	R	Y	The Management and Security hardening guides are publicly available on the Merlin product page. Westermo Ireland devices are provided with a minimal configuration, designed solely for local connectivity and initial setup procedures. Access to these devices is restricted to users who have successfully authenticated. Unconfigured units pose only a minimal security risk to both themselves and their surrounding environment.	The manufacturer should provide users with guidance on how to securely set up their consumer IoT device.

Provision 5.12-3	R	Y	Self-verification feature is not supported. Westermo Ireland devices offer advanced networking capabilities tailored for radio communication technologies. It is expected that administrative personnel possess the necessary qualifications to design, manage, secure, and troubleshoot OT/IT networks, including assessing security features and conducting fundamental threat modelling on Merlin Series routers prior to deployment in the production environment. Devices should only be installed following the successful completion of all provisioning procedures and acceptance testing that include necessary on-site/production security testing.	The manufacturer should provide users with guidance on how to check whether their consumer IoT device is securely set up and maintained in a secure state.
Provision 5.13-1A	M	Y	Westermo Ireland devices are network devices designed solely for data transit, not for storing or processing data content. They support various data transmission protocols, each with dedicated integrity and authenticity checks to prevent manipulation and system failures by discarding invalid inputs.	Data input at application layer to the device via user interfaces shall be validated by the device regarding unexpected data input to prevent system manipulations and failures.
Provision 5.13-1B	M	Y	Westermo Ireland devices are network devices designed solely for data transit, not for storing or processing data content. They support various data transmission protocols, each with dedicated integrity and authenticity checks to prevent manipulation and system failures by discarding invalid inputs.	Data input at application layer to the device via network interfaces shall be validated by the device regarding unexpected data input to prevent system manipulations and failures

Provision 6.1	M	N/A	Not Applicable. Westermo Ireland devices operate solely as network devices, facilitating data transit without storing or processing personal data or the content of transmitted data, in line with definitions related to personal data and privacy protection. It is highly recommended that administrators employ generic identifiers (e.g., "operator1") rather than personal information identifiers (PII) such as "John.Doe." Additional configuration elements are comprised of standard network and security parameters, which do not constitute personal data.	The manufacturer shall provide consumers with clear and transparent information about what personal data is processed and for what purposes, by whom, and for how long, for each consumer IoT device and associated service. This also applies to third parties that can be involved, including advertisers.
Provision 6.2	M F(y)	N/A	Not Applicable. Westermo Ireland devices operate solely as network devices, facilitating data transit without storing or processing personal data or the content of transmitted data, in line with definitions related to personal data and privacy protection. It is highly recommended that administrators employ generic identifiers (e.g., "operator1") rather than personal information identifiers (PII) such as "John.Doe." Additional configuration elements are comprised of standard network and security parameters, which do not constitute personal data.	Where personal data will be processed on the basis of consumers' consent, the consumer IoT device shall provide a means to acquire this consent in a valid way.
Provision 6.3A	M F(y)	N/A	Not Applicable. Westermo Ireland devices operate solely as network devices, facilitating data transit without storing or processing personal data or the content of transmitted data, in line with definitions related to personal data and privacy protection. It is highly recommended that administrators employ generic identifiers (e.g., "operator1") rather than personal information identifiers (PII) such as "John.Doe." Additional configuration elements are comprised of standard network and security parameters, which do not constitute personal data.	Where personal data will be processed on the basis of consumers' consent, the consumer IoT device shall provide a means to withdraw this consent at any time.

Provision 6.3B	M F(y)	N/A	Not Applicable. Westermo Ireland devices operate solely as network devices, facilitating data transit without storing or processing personal data or the content of transmitted data, in line with definitions related to personal data and privacy protection. It is highly recommended that administrators employ generic identifiers (e.g., "operator1") rather than personal information identifiers (PII) such as "John.Doe." Additional configuration elements are comprised of standard network and security parameters, which do not constitute personal data.	Where personal data will be processed on the basis of consumers' consent, the consumer IoT device shall provide a means of storing information about this consent.
Provision 6.4	R F(w)	N/A	Not Applicable. Westermo Ireland devices operate solely as network devices, facilitating data transit without storing or processing personal data or the content of transmitted data, in line with definitions related to personal data and privacy protection. It is highly recommended that administrators employ generic identifiers (e.g., "operator1") rather than personal information identifiers (PII) such as "John.Doe." Additional configuration elements are comprised of standard network and security parameters, which do not constitute personal data.	If telemetry data is collected from consumer IoT products, the processing of personal data should be limited to that which is necessary for the intended functionality identified in provision 6-5.
Provision 6.5	M F(w)	N/A	Not Applicable. Westermo Ireland devices operate solely as network devices, facilitating data transit without storing or processing personal data or the content of transmitted data, in line with definitions related to personal data and privacy protection. It is highly recommended that administrators employ generic identifiers (e.g., "operator1") rather than personal information identifiers (PII) such as "John.Doe." Additional configuration elements are comprised of standard network and security parameters, which do not constitute personal data.	If telemetry data is collected from consumer IoT products, consumers shall be provided with information on what telemetry data is collected, how it is being used, by whom, and for what purposes.

Provision 6.6	M F(z)	N/A	Not Applicable. Westermo Ireland devices operate solely as network devices, facilitating data transit without storing or processing personal data or the content of transmitted data, in line with definitions related to personal data and privacy protection. It is highly recommended that administrators employ generic identifiers (e.g., "operator1") rather than personal information identifiers (PII) such as "John.Doe." Additional configuration elements are comprised of standard network and security parameters, which do not constitute personal data.	Data stored and processed on a consumer IoT device, or made available to an associated service by the consumer IoT device, for purposes identified in provision 6-1 shall be limited to that which is necessary for the purpose for which it is being collected or processed and deleted once no longer necessary for any of the purposes identified.
Provision 6.7	R F(aa)	N/A	Not Applicable. Westermo Ireland devices operate solely as network devices, facilitating data transit without storing or processing personal data or the content of transmitted data, in line with definitions related to personal data and privacy protection. It is highly recommended that administrators employ generic identifiers (e.g., "operator1") rather than personal information identifiers (PII) such as "John.Doe." Additional configuration elements are comprised of standard network and security parameters, which do not constitute personal data.	When the purpose of data collection from consumer IoT devices, or processing on the consumer IoT device, is solely to compute an aggregate result, the data collected should be the minimum required to compute the aggregate, the aggregation should happen as early as possible, and the retention of both collected data and the resulting aggregate should be minimized.
Provision 6.8	R F(z)	N/A	Not Applicable. Westermo Ireland devices operate solely as network devices, facilitating data transit without storing or processing personal data or the content of transmitted data, in line with definitions related to personal data and privacy protection. It is highly recommended that administrators employ generic identifiers (e.g., "operator1") rather than personal information identifiers (PII) such as "John.Doe." Additional configuration elements are comprised of standard network and security parameters, which do not constitute personal data.	Data anonymization technologies should be used to protect privacy during data collection, processing and storage.