SmartSuite

Framework / Cybersecurity / Other

ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements

ETSI EN 303 645 sets baseline security and data protection provisions for consumer IoT devices and their associated services, from banning default passwords to keeping software updated.



What it is

ETSI EN 303 645 is a European Standard that specifies high-level, outcome-focused security and data protection provisions for consumer Internet of Things (IoT) devices connected to the internet or a home network, together with the services they interact with. It brings widely accepted good practice for connected products into 13 groups of provisions plus data protection provisions, so manufacturers can build security in from design rather than patch it afterward.

The standard is produced by ETSI Technical Committee Cyber Security (CYBER). The current version is V3.1.3 (2024-09), adopted on 11 September 2024, which succeeded the first edition V2.1.1 (2020-06). It is voluntary as a standard, but it is referenced by national consumer IoT security regimes and labeling schemes and is the baseline against which ETSI TS 103 701 conformance assessments are run, so manufacturers, importers, test laboratories, and certification bodies treat it as a de facto requirement.

At a glance

PUBLISHER European Telecommunications Standards Institute (ETSI)	TYPE Standard	VERSION V3.1.3 (2024-09)
EFFECTIVE September 11, 2024 (V3.1.3 adopted)	DOMAIN Cybersecurity	FAMILY Other
REGION ETSI (Europe), adopted internationally	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY Medium

Source: etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

Why it matters

- **Reduce the most common consumer IoT attacks** The provisions target the weaknesses that drive real incidents: universal default passwords, unpatched software, insecure interfaces, and exposed sensitive parameters.
- **Meet regulator and labeling expectations** National consumer device security laws and labeling schemes reference EN 303 645, so conformance shortens the route to market.
- **Demonstrate security by design** The implementation conformance statement and ETSI TS 103 701 assessment give customers and assessors verifiable evidence rather than marketing claims.
- **Protect personal data on devices** Data protection provisions require transparency, consent for telemetry, and easy deletion of user data, supporting privacy law compliance.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports ETSI EN 303 645

EN 303 645 Provision Library

Load the clause 5 and clause 6 provisions with their shall/should status and link each to product designs and policies.

Ownership and Release Cadence

Assign provision owners per product line and schedule reviews for each firmware release and support-period milestone.

Conformance Statement and Evidence

Record the Annex B implementation conformance statement with design documents, test reports, and reviewer sign-off.

Assessment and Remediation Tracking

Capture ETSI TS 103 701 test results and labeling scheme findings and drive remediation to closure.

Vulnerability Disclosure and Update Management

Track vulnerability reports, response times, and security update releases against the published support period.

Product Security Reporting

Report conformance status, open findings, and support-period commitments to leadership, customers, and certification bodies.

Common framework mappings

EU CRA | Australia IoT Code | CSA IoT SCF v2 | IEC 62443-4-2 | UL 2900-1 | NCA CGIoT-1:2024 | ISO 27001:2022 | NIST CSF 2.0 | GDPR

Official resources

ETSI EN 303 645 V3.1.3 (2024-09)

The full text of the consumer IoT baseline security standard, free to download from ETSI.

etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

ETSI TS 103 701 Conformance Assessment

Specifies the test cases and assessment method used to verify a device against EN 303 645.

etsi.org/deliver/etsi_ts/103700_103799/103701/02.01.01_60/ts_103701v020101p.pdf

ETSI TR 103 621 Implementation Guide

Gives implementation examples and notes for each EN 303 645 provision.

etsi.org/deliver/etsi_tr/103600_103699/103621/02.01.01_60/tr_103621v020101p.pdf

ETSI Press Release on EN 303 645 V3.1.3

Announces the 2024 revision of the consumer IoT security standard and its aims.

etsi.org/newsroom/press-releases/2457-etsi-releases-new-guidelines-to-enhance-cyber-security-for-consumer-iot-devices

Frequently asked questions

What is ETSI EN 303 645?

ETSI EN 303 645 is a European Standard, produced by ETSI Technical Committee Cyber Security (CYBER), that specifies baseline security and data protection provisions for consumer IoT devices and their associated services. The current version is V3.1.3 (2024-09). ETSI publishes it free of charge as a PDF, along with the TS 103 701 assessment specification and the TR 103 621 guide, and the text remains ETSI copyright.

Is ETSI EN 303 645 mandatory?

As a standard it is voluntary. However, national consumer IoT security laws and labeling schemes reference its provisions, and customers and certification bodies often require conformance, so most consumer device manufacturers treat it as a baseline requirement.

Which devices does ETSI EN 303 645 cover?

It covers consumer IoT devices that connect to the internet or a home network, such as connected toys and baby monitors, smart locks and smoke detectors, cameras, speakers and televisions, wearable health trackers, home automation hubs, connected appliances, and smart home assistants. Industrial, medical, and enterprise devices are addressed by other standards.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What are the 13 provisions of ETSI EN 303 645?

Clause 5 has 13 provision groups: 5.1 no universal default passwords; 5.2 implement a means to manage reports of vulnerabilities; 5.3 keep software updated; 5.4 securely store sensitive security parameters; 5.5 communicate securely; 5.6 minimize exposed attack surfaces; 5.7 ensure software integrity; 5.8 ensure that personal data is secure; 5.9 make systems resilient to outages; 5.10 examine system telemetry data; 5.11 make it easy for users to delete user data; 5.12 make installation and maintenance of devices easy; and 5.13 validate input data. Clause 6 adds data protection provisions, and clause 5.0 covers reporting the implementation.

How is conformance with ETSI EN 303 645 assessed?

Manufacturers complete the implementation conformance statement in Annex B of the standard, and independent assessment follows ETSI TS 103 701, which defines test cases for each provision. ETSI TR 103 621 provides implementation guidance with examples for each provision.

License included / downloadable: Yes ETSI publishes EN 303 645 free of charge as a PDF on its deliver site; the text remains ETSI copyright and is not reproduced within the platform.

Full framework page and mappings: smartsuite.com/frameworks/etsi-en-303-645-cyber-security-for-consumer-internet-of-things