IAR Embedded Trust

Enabling product security adoption as well as secure, encrypted software to inhibit IP theft, malware injection, and unauthorized over-production.

The End-to-End Embedded Security Solution

Embedded security is critical due to evolving threats and compliance requirements like the European EN 303 645. IAR Embedded Trust offers an end-to-end solution to secure both new and existing applications. It allows you to create custom Security Contexts, ensuring secure production, lifecycle management, updates, and feature releases.

With integrated encryption and code signing, it prevents malware injection and protects intellectual property across the supply chain, safeguarding hardware, software, and data.

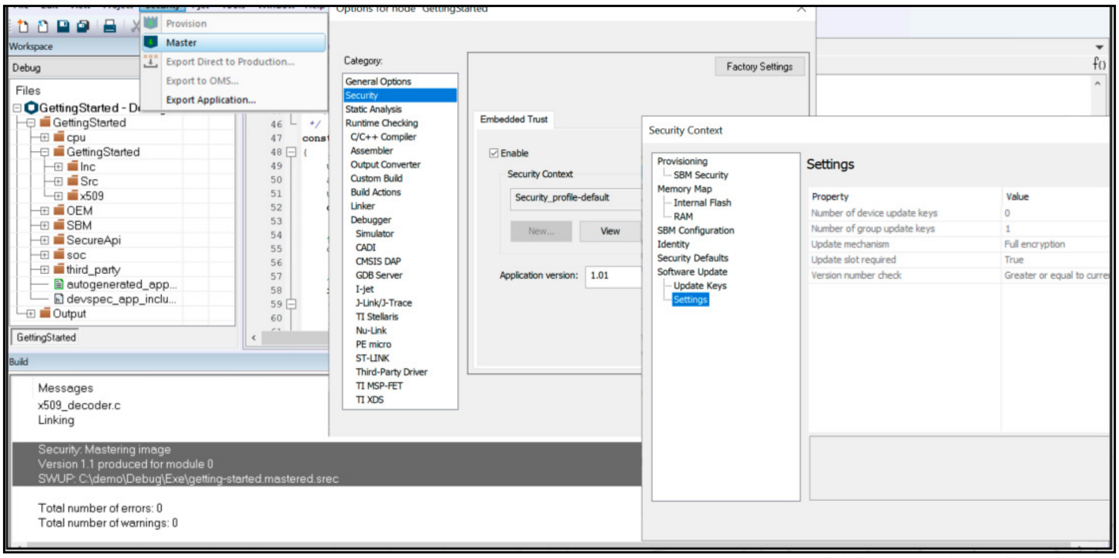
Key Highlight Features

- Easily port the current framework to a new microcontroller with a device-agnostic security solution
- Reuse code without starting from scratch while adding decisive security features to the entire firmware or application
- Use the Root of Trust (RoT) as a secure immutable boot path with anchors in hardware and device specific features
- Defends against malware injection with robust code defenses
- Supports developers to align with security standards, such as EN 303645 and NISTIR 8259
- Custom Security Contexts examples help with unique security needs and accelerates development

Working with IAR Embedded Workbench and IAR Embedded Trust

IAR Embedded Trust seamlessly integrates with IAR Embedded Workbench, adding customizable Security Contexts for baseline protection against malware, counterfeiting, and cloning. It also enables auto-generation of a Secure Boot Manager (SBM) and example applications.

If you're already using IAR Embedded Workbench, adding IAR Embedded Trust to your existing license makes implementing security straightforward without disrupting your development process.



```
Messages
x509_decoder.c
Linking
Security: Mastering image
Version 1.1 produced for module 0
SWUP: C:\demo\Debug\Exe\getting-started.mastered.srec

Total number of errors: 0
Total number of warnings: 0
```

☑ Enable

Security Context: Security_profile-default

Application version: 1.01

Settings

Property	Value
Number of device update keys	0
Number of group update keys	1
Update mechanism	Full encryption
Update slot required	True
Version number check	Greater or equal to curre

Configuring IAR Embedded Trust in IAR Embedded Workbench

Security Context

Security Contexts allow developers to quickly protect critical IP by encrypting software images and ensuring only authorized, authenticated IP is installed on devices. With IAR Embedded Trust, companies can create custom Security Contexts tailored to their needs. The standalone Security Context Manager offers flexibility and versatility.

Key Features and Benefits are

Secure application and credential provisioning
Ensuring devices are born securely with correct software and credential provisioning

Integrated Secure Boot Manager (SBM)
Providing the most powerful device services to manage device access and updates

Device-specific Security Management
Servicing the device specific Root of Trust (RoT), secure enclaves, and system configuration

Authenticated and authorized data protection
Cryptographic enforcement of sensitive data at-rest ensures integrity and authenticity

Automatic encryption and signature of code
Ensuring only correctly managed and digitally signed code can be installed

Update policing in Secure Boot Manager
Integrated device level configuration for seamless updates and patches

Integration into secure provisioning flow
Compatible with Secure Deploy - Prototyping

Integrated application versioning management
Providing structured versioning in the development flow

OEM-Developer defined software key infrastructure
Enabling developers to define the critical key management of their application

Anti-rollback protection for application updates
Providing protection against rollback attacks and versioning threats and protecting brand reputation

Bootloader device level trace and debug management
Configuration of the device to ensure integrity of the boot process thanks to the RoT.

Secure Application Maker Tool Update
With the Secure Application Maker (SAM) Tool and standalone Security Context Manager, IAR Embedded Trust's security features can be added to the Secure Boot Manager and applications built outside IAR Embedded Workbench, such as with GCC in STM32CubeIDE or NXP MCUXpresso.

Standalone Security Context Manager
An application for creating, editing, or cloning Security Contexts. Using it, a security engineer can manage the Security Context for a project without installing the application development tools.

Supported Devices

IAR Embedded Trust supports a wide range of validated and verified devices, including Arm-based MCUs from STMicroelectronics, Microchip, Renesas, Infineon, Silicon Labs, NXP, and the Renesas RX MCU family. This allows you to select the best MCU for your application's security and functional needs. For a full list of supported devices, visit: iar.com/embeddedtrust

Does your application require embedded security?

From project inception to the end of your product's life cycle, we're here to support you every step of the way.

Explore real-world use cases and see how industry leaders are leveraging IAR's solutions to succeed. Visit

www.iar.com/security-resources for insights and success stories. Ready to get started? Contact your local IAR

team at iar.com/contact.