Author	Semtech		Date	June 10, 2025

Content Level	BASIC		INTERMEDIATE	Y	ADVANCED		Confidentiality	Public	Y	Private	

Hardware Compatibility	Product Line	IoT Modules	Series	EM: 74x1, 75xx, 7690, 86xx, 91xx, 92xx	HL: 78xx, 79xx
					MC: 74x1
				RC: 76xx	WP: 76xx, 77xx

Software Compatibility	Refer to module firmware Customer Release Notes for details	Document Type	App Note	Y	Tech Note	

1 Version

This document may be updated over its lifetime. To ensure you design with the correct version, please check The Source page at source.sierrawireless.com for the latest version.

2 Introduction

This document is provided to Semtech distributors and clients to aid more rapid development of embedded applications using the Semtech portfolio of cellular solutions. To request a new application/technical note, contact your regional Semtech Product Marketing Manager.

3 Description

This document describes Semtech's recommended cybersecurity design guidelines for OEMs integrating Semtech cellular modules into their end products (4 Semtech Modules Security Methods), and provides a checklist for performing a security assessment of an end product (5 OEM Platform Assessment).

These guidelines are recommended to help ensure end products with integrated Semtech cellular modules will meet security regulations and best practices.

Although Semtech cellular modules are provided with comprehensive security features, OEMs must ensure they properly configure these features. The OEM is ultimately responsible for the security posture of their end product integrating the Semtech cellular module. Semtech strongly recommends that OEMs implement the security methods and security assessment described in this document.

Important: *In the EU, OEM end products placed in the European market beginning August 01, 2025* ***must*** *comply with the cybersecurity requirements of the RED Delegated Act (2022/30). Products already placed on the market before this date can continue to be used without specific modifications.*

Proper implementation of these Semtech module recommendations is essential for regulatory compliance and protection against security threats. OEMs should work collaboratively with Semtech to ensure the complete security posture of their end products, including proper configuration and management of integrated modules. For any security concerns or questions, contact Semtech support (see 9 Support).

4 Semtech Modules Security Methods

Table 1 summarizes the security methods that Semtech recommends implementing on your Semtech cellular module prior to deployment.

Note: The topics/subtopics describing each recommended method indicate the modules that can use the method.

Table 1: Recommended Security Methods for Semtech Cellular Modules

Method	Affected Modules	Recommendation	Description	Type
Set a strong password for extended AT commands access	All module series	Strongly recommended	**Security Consideration** — The password to restrict access to extended AT commands is not set at the Semtech factory. **Risk** — Extended AT commands are intended for use by the OEM in development or factory settings. Unauthorized use of extended AT commands by end users could cause the Semtech module to become unstable or unusable. **Recommendation** — Assign strong, randomly-generated unique passwords to each Semtech module. **Effect** — Unauthorized users are prevented from using extended commands. For details, see 4.1 Set Extended AT Command Access Password.	Command level
Disable debug interfaces	EM7690 EM91xx EM92xx HL78xx HL79xx	Recommended	**Security Consideration** — Debug interfaces may be enabled by default. **Risk** — Unauthorized access to debug functionality could compromise the Semtech module's security. **Recommendation** — Disable the module's debug interface(s). **Effect** — Unauthorized users are prevented from accessing debug functionality. For details, see 4.2 Disable Debug/Diagnostic Interfaces.	Interface level
Disable unused physical interfaces	All module series	Recommended	**Security Consideration** — Semtech modules may expose physical interfaces that are not used in OEM end products. **Risk** — Unused physical interfaces increase the module's attack surface. **Recommendation** — Keep unused physical interfaces as NC (not connected) in the end product hardware design. **Effect** — Reduces the module's physical attack surface. For details, see 4.3 Disable Unused Physical Interfaces.	Hardware level
Secure the Linux open platform	WP76xx WP77xx	Strongly recommended	**Security Consideration** — Linux open platforms have additional interfaces enabled by default. **Risk** — Open platforms provide more attack vectors than closed platforms. **Recommendation** — Implement comprehensive security measures for Linux platforms. **Effect** — Reduces the attack surface on open platforms. For details, see 4.4 Secure Linux Open Platform.	Platform level

4.1 Set Extended AT Command Access Password

Recommendation: Strongly recommended

Applies to: All modules

Extended AT commands are typically used by OEMs, in development or factory settings, to exercise the module's RF functionality.

To prevent unauthorized access to extended AT commands and to help ensure proper device operation is maintained, Semtech strongly recommends setting a strong, unique password on each module. (By default, passwords are not set at the Semtech factory.)

Note: To identify extended commands that will be password-restricted when a password has been set, refer to the module's AT command reference document on the device page at source.sierrawireless.com.

To set the extended AT command access password on a Semtech module:

1. Connect to the module's AT COM port.
2. Set a strong, unique password for the module. Passwords should be unique for each module, and randomly generated for optimal security.

```
at!setcnd=<"strong_unique_password">   ← Note: The password must be quoted. e.g., at!setcnd="Lx49*&Q."
OK
```

   (Minimum password length: 8 characters. For full command and password format details, refer to the module's AT command reference document.)
3. Verify that the password was set correctly:

```
at!setcnd?
!SETCND: <state>
OK
```

   where <state> will be "Password Present" if the password has been set, or "No Password" if it has not been set.

To access extended AT commands after setting a password:

1. Enable extended AT command access:

```
at!entercnd=<"your_password">   ← Note: The password must be quoted. e.g., at!setcnd="Lx49*&Q."
OK
```

   Note: Access remains enabled only until the module is reset (i.e., it is not persistent).

4.2 Disable Debug / Diagnostic Interfaces

Recommendation: Recommended

Applies to: EM7690, EM91xx, EM92xx, HL78xx, HL79xx

If enabled, the Semtech module's debug interface(s) can provide unauthorized access to diagnostic functionality and be a vector for attack. Semtech recommends that OEMs disable debug interfaces in production builds.

The methods for disabling debug interfaces vary by module series, as described below in sections 4.2.1–4.2.3.

4.2.1 Disable Diagnostic Functions via !CUSTOM

Applies to: EM7690, EM91xx, EM92xx

To disable the diagnostic functionality via the "DIAGENABLE" customization on the Semtech 5G module series (EM91xx (including EM7690) and EM92xx):

1. Connect to the module's AT COM port.
2. Enable extended AT command access:

```
at!entercnd=<"your_password">   ← Note: The password must be quoted. e.g., at!setcnd="Lx49*&Q."
OK
```

3. Set the DIAGENABLE customization to 0 (Disable):

```
at!custom="DIAGENABLE",0
OK
```

Note that, if necessary (e.g., when investigating field issues with Semtech), diagnostic functions may need to be temporarily re-enabled.

To re-enable diagnostic functions:

1. Connect to the module's AT COM port.
2. Enable extended AT command access:

```
at!entercnd=<your_password>
OK
```

   Note: Access remains enabled only until the module is reset (i.e., it is not persistent).

3. Set the DIAGENABLE customization to 1 (Enable):

```
at!custom="DIAGENABLE",1
OK
```

4. When finished with the task (e.g., field investigation, etc.), disable the diagnostic functionality again.

4.2.2 Disable Debug Functionality via +SWITRACEMODE

Applies to: HL78xx

To disable debug functionality on Semtech HL78xx modules:

1. Connect to the module's AT COM port.
2. Disable debug functionality:

```
at+switracemode=CUSTOMER
OK
```

4.2.3 Disable Debug Functionality via %SETSRMCFG

Applies to: HL79xx

To disable debug functionality on Semtech HL79xx modules:

1. Connect to the module's AT COM port.
2. Disable debug functionality:

```
at%setsrmcfg="EMUXMCUCLI",2
OK

at%setsrmcfg="EMUXAPPCLI",2
OK

at%setsrmcfg="DBGUARTMODE",2
OK
```

4.3 Disable Unused Physical Interfaces

Recommendation: Recommended

Applies to: All modules

Semtech modules (especially CF3 form factor modules) may expose physical interfaces that are not used in an OEM's end products.

To reduce the chance of unauthorized access, Semtech recommends that unused physical interfaces be not connected (NC) in the OEM end product hardware to reduce the module's attack surface.

4.4 Secure Linux Open Platform

Recommendation: Strongly recommended

Applies to: WP76xx, WP77xx

Semtech's Linux open platform modules (WP76xx and WP77xx) require extra security methods, in addition to the other methods described above. For details, refer to *[1] Securing WP Series Devices (Doc# 2174116-1).*

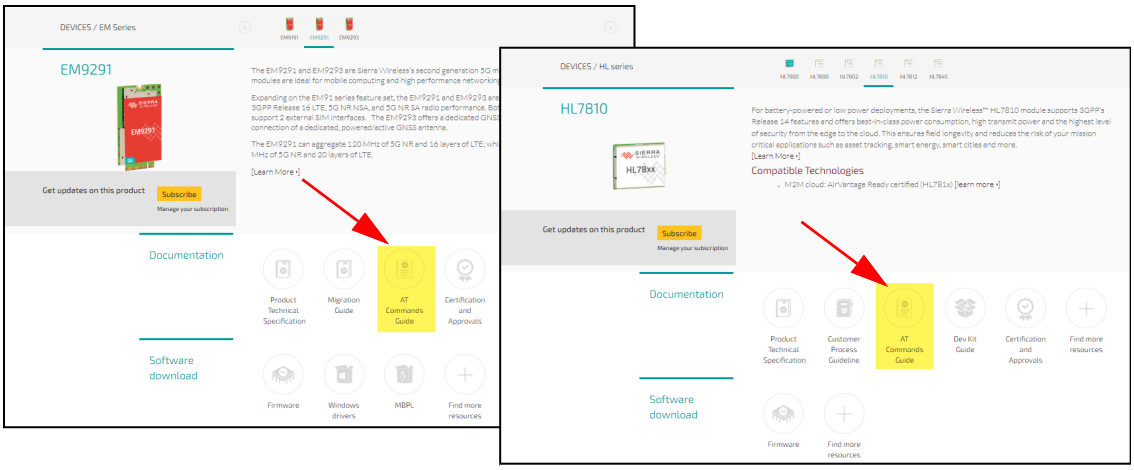
5 OEM Platform Assessment

OEMs should conduct a comprehensive security assessment of their complete end product with an integrated Semtech cellular module, which includes:

- Threat Modeling:
  - Identify potential attack vectors introduced by the Semtech module, specifically around the wireless connectivity it provides.
  - Assess the impact of security breaches if the Semtech module is compromised.
  - Document security assumptions with respect to the Semtech module and its interfaces. If required details are not included in available documentation (e.g., Firmware Customer Release Note, module Product Technical Specifications, etc.), contact Semtech support (see 9 Support).
- Compliance Verification:
  - Verify adherence to applicable regulations with the Semtech module integrated in the end product.
  - Document security controls on Semtech module interfaces.
  - Maintain security compliance records, including Semtech-provided compliance records.

6 AT Commands

Note that the command formats and parameter details of the AT command examples shown in this document are for the specific requirements of this application note — parameters and supported values that are not applicable to the use cases in this application note are not displayed. For full command details, refer to the module's AT command reference document on the device page at source.sierrawireless.com. For example:



7 References

Sierra Wireless

[1] Securing WP Series Devices (Doc# 2174116-1)

8 Glossary

Term	Definition
attack surface	All potential entry points that could be used for unauthorized access
extended AT commands	AT commands that can only be accessed when the module's unique password is entered

9 Support

For direct clients: contact your Semtech FAE.

For distributor clients: contact your distributor FAE.

For distributors: contact your Semtech FAE.

10 Document History

Rev #	Release date	Description
1	June 2025	Document created
2	June 2025	Updated Disable Debug/Diagnostic Interfaces on page 3 (methods, module applicability)

11 Legal Notice