Security Appliance User Guide

COPYRIGHT NOTICE

DISCLAIMER

The information in this document is subject to change without notice and does not represent a commitment on any part of IAR Systems. While the information contained herein is assumed to be accurate, IAR Systems assumes no responsibility for any errors or omissions.

In no event shall IAR Systems, its employees, its contractors, or the authors of this document be liable for special, direct, indirect, or consequential damage, losses, costs, charges, claims, demands, claim for lost profits, fees, or expenses of any nature or kind.

TRADEMARKS

IAR Systems, I-jet, IAR Embedded Secure IP, IAR Secure Deploy, Security Appliance, IAR Secure Deploy – Prototyping, IAR Secure Deploy – Manufacturing, and the logotypes of IAR Systems are trademarks or registered trademarks owned by IAR Systems AB.

All other product names are trademarks or registered trademarks of their respective owners.

EDITION NOTICE

Fifth edition: December 2023

Part number: UGSecApp-5

Internal reference: IJOA.

Safety note

Before starting the installation of the product, please read the safety information.

For your safety

To prevent damage to your product or an injury to the operator or others, please read and follow these safety precautions before starting the installation of the Security Appliance.

Please keep these safety instructions available to all users of the product.

	This icon identifies warnings. To prevent possible injury, read all warnings before using the Security Appliance product.

WARNINGS

	**DO NOT operate the equipment in overheat condition.** Keep the equipment away from the sun and do not operate if the operating temperature is seriously above or below the recommended range.
	**NEVER OPEN the casing.** Doing so voids your warranty.
	**The unit contains lithium-ion batteries, which are likely to cause a fire if misused, punctured, or damaged.**
	**DO NOT make any modifications to the product.**
	**Only use the approved power source (AC/DC adapter) which comes included with the kit.**
	**DO NOT use the equipment in the presence of flammable gas.** Do not use electronic equipment in the presence of flammable gas as this could result in high risk of explosion or fire.
	**DO NOT use the equipment in case of a power failure or general equipment failure.** Contact customer support for assistance.
	**ALWAYS USE the appropriate cables for the input/output ports, supplied with the product.**
	**NEVER REMOVE the batteries from the equipment.** If a replacement is needed, contact customer support for assistance.
	**DO NOT apply any mechanical stress/shock to the equipment while it is in operation.**
	**DO NOT use the equipment outdoors.** It is only intended for indoor usage. Do not route any cable outdoor due to the risk of lightning strikes.
	**Access to the power supply outlet must not be obstructed.**
	**The Security Appliance MUST be charged for three hours at least once every three months to ensure proper operation.**

Product information

Product name: Security Appliance

Model number: STZ-SECAPP-V1

Hardware version: Rev C2

PRODUCT DESCRIPTION

The Security Appliance is a Cryptographic Processing Unit that is used in both industrial manufacturing and low volume environment for programming security information into various secure Integrated Circuits. The Security Appliance is connected to various 3rd party programming systems and provides secure channel to protect end customer IP from potential counterfeit and theft.

ELECTRICAL SPECIFICATION

Power supply (AC/DC adapter)	100–240V AC, 50/60 Hz
Power supply (equipment)	5V DC, 3A (max)
Operating temperature	0–55° C
Operating relative humidity	30–50%
Dimensions	180x125x32mm

FCC COMPLIANCE STATEMENT

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

For more information on statutory regulatory compliance, please see our declaration of conformity at the back of this guide.

This guide describes

- Kit contents
- Security Appliance overview
- Setting up the IAR Secure Deploy – Prototyping low-volume production system
- Setting up a volume production system
- Configuring the network settings

For more information, see the *IAR Secure Deploy – Prototyping User Guide* or the *IAR Secure Deploy – Manufacturing User Guide*.

Kit contents

The Security Appliance kit contains the following components, when delivered with the IAR Secure Deploy – Prototyping software bundle:

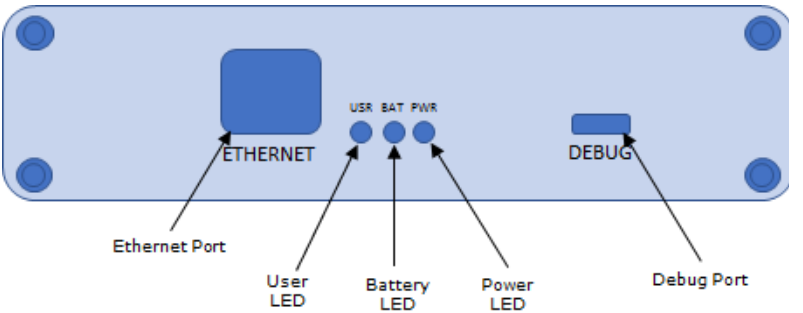
Quantity	Component
1	Security Appliance
1	I-jet In-Circuit debug probe
1	CAT-6,7 Ethernet cable (1 meter)
4	USB Micro cable
1	USB-C to USB-A cable
1	AC-DC Wall-mount power supply (5V, 3A), with plugs for EU, US, UK, Australia, for 90–260V AC input.
1	20-way ribbon cable

The kit contents when delivered with a volume production unit differ from this list.

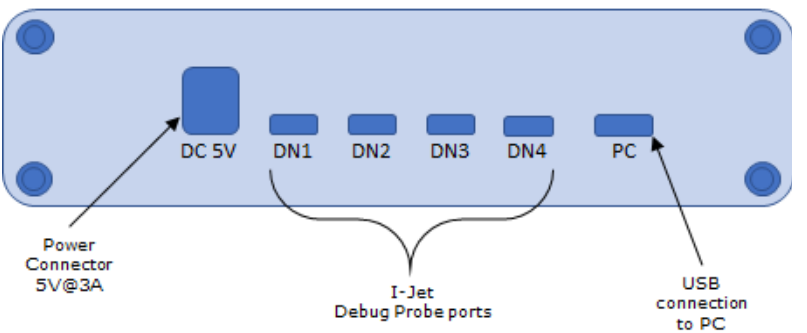
Security Appliance overview

These figures provide a schematic view of the front and rear panels of the Security Appliance.

Security Appliance front panel



Security Appliance rear panel



Installing the provisioning software

Before you can set up the system, you must install the provisioning software.

For instructions on installing the **IAR Secure Deploy – Prototyping** low-volume production system, see the *IAR Secure Deploy – Prototyping User Guide*.

For instructions on installing the **IAR Secure Deploy – Manufacturing** high-level management application for supervising volume production, see the *IAR Secure Deploy – Manufacturing User Guide*.

UPGRADING THE PROVISIONING SOFTWARE

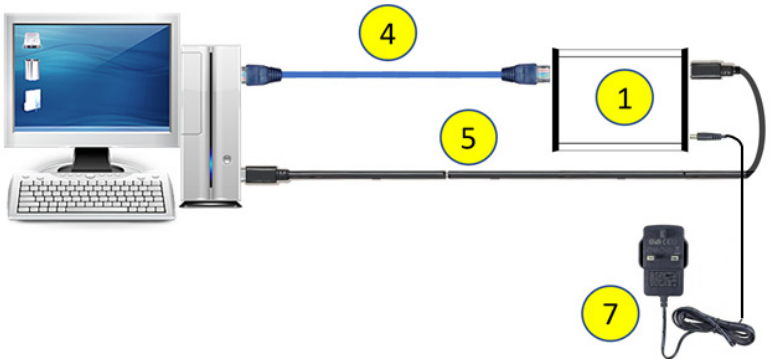
Important! If you upgrade the provisioning software, you must also upgrade the Security Appliance firmware to be able to communicate with the Security Appliance. The most recent firmware version is available on your My Pages at **iar.com**. For instructions on how to upgrade the Security Appliance firmware, see the *IAR Secure Deploy – Prototyping User Guide* or the *IAR Secure Deploy – Manufacturing User Guide.*

Setting up the IAR Secure Deploy – Prototyping low-volume production system

Note: Before you can set up the system, you must install the provisioning software. See the *IAR Secure Deploy – Prototyping User Guide* for instructions.

A. Connecting the Security Appliance

These components are needed to connect the PC to the Security Appliance:



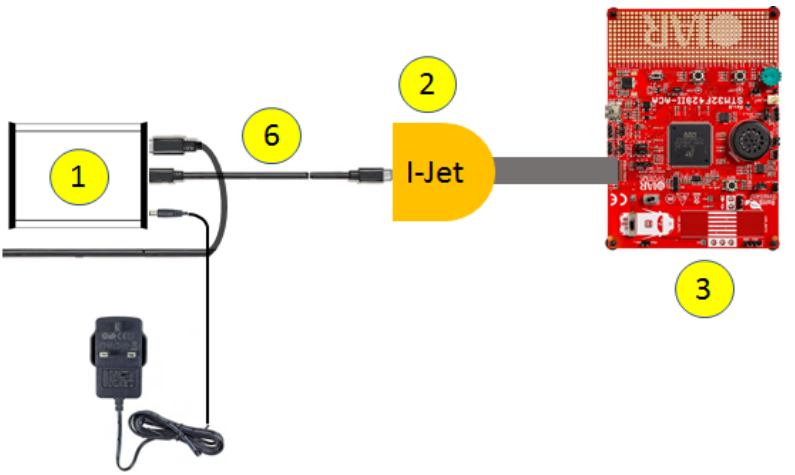
Item	Component
1	Security Appliance
4	Ethernet cable (1 meter)
5	USB-C to USB-A cable
7	Power supply

1. Connect the PC and the Security Appliance using the Ethernet cable. (If your PC does not have a free Ethernet port, you can use a USB–Ethernet adapter.)
2. Attach the power supply to the Security Appliance, and then plug it in to a power socket. Switch the Security Appliance on. The rear panel LEDs will begin flashing.
3. Wait for one minute to allow the Security Appliance to complete its power-up process.

4 Connect the PC and the PC port on the Security Appliance using the USB-C to USB-A cable.

B. Connecting the hardware provisioning equipment

When the Security Appliance has been connected to the PC, you can connect the hardware provisioning equipment to the Security Appliance. These components are needed:

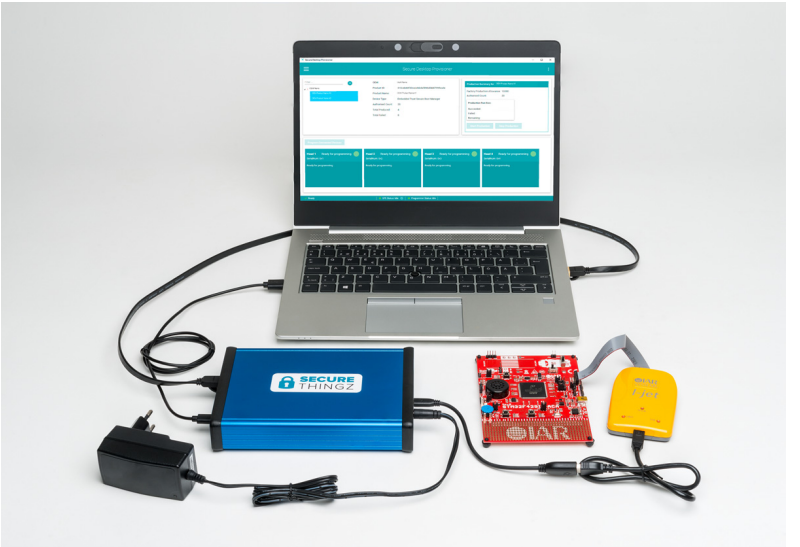


Item	Component
1	Security Appliance
2	I-jet Debug probe
3	Prototyping board—not included in the kit
6	USB Micro cable

1 Attach a USB Micro cable to the DN1 port on the front panel of the Security Appliance and attach the other end of the cable to the I-jet debug probe.

2 Attach one end of the 20-way ribbon cable to the I-Jet debug probe, and the other end to the development board. Note the keying (pin 4 is missing).

When you have finished setting up, it will look something like this:

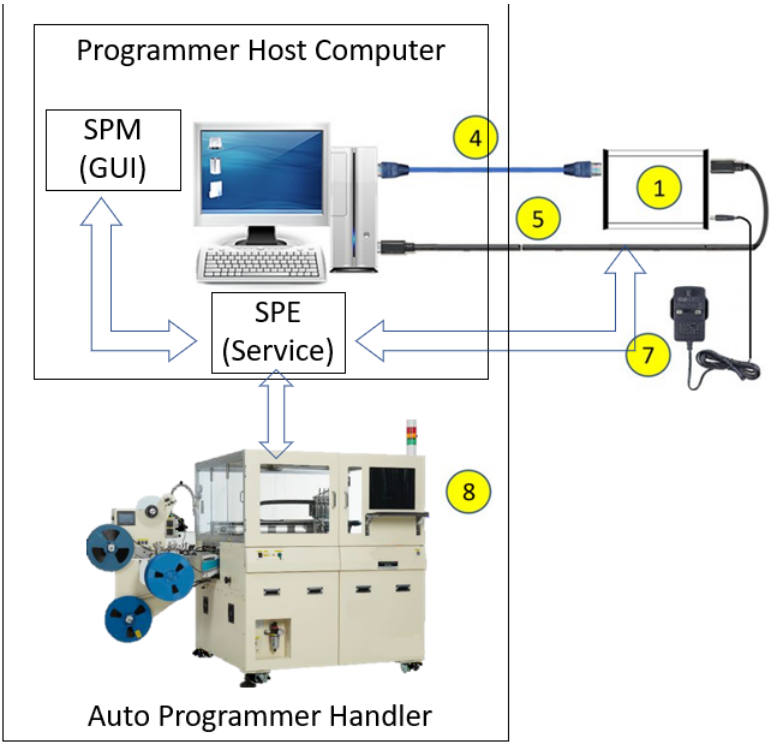


Setting up a volume production system

Note: Before you can set up the system, you must install the provisioning software. See the *IAR Secure Deploy – Manufacturing User Guide* for instructions.

A. System without an intermediary security PC

These components are needed to connect the programmer host PC to the Security Appliance:



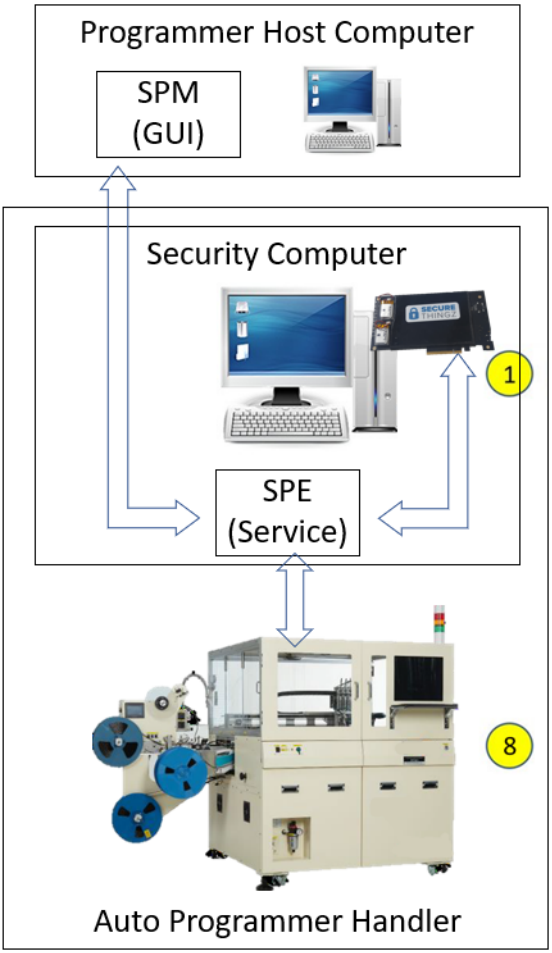
Item	Component
1	Security Appliance
4	Ethernet cable (1 meter)

Item	Component
5	USB-C to USB-A cable
7	Power supply
8	Automated programmer

1. Connect the PC and the Security Appliance using the Ethernet cable. (If the PC does not have a free Ethernet port, you can use a USB–Ethernet adapter.)
2. Attach the power supply to the Security Appliance, and then plug it in to a power socket. Switch the Security Appliance on. The rear panel LEDs will begin flashing.
3. Wait for one minute to allow the Security Appliance to complete its power-up process.
4. Connect the PC and the PC port on the Security Appliance using the USB-C to USB-A cable.

B. System with an intermediary security PC

When the Security Appliance has been connected to the PC, you can connect the hardware provisioning equipment to the Security Appliance. These components are needed:



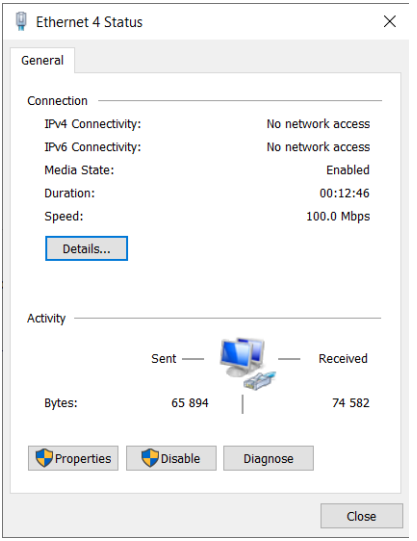
Item	Component
1	Security Appliance (PCI mounted)
8	Automated programmer

To prepare the system for production, switch off the Security PC and attach the Security Appliance to the PCI slot. Then start the Security PC again.

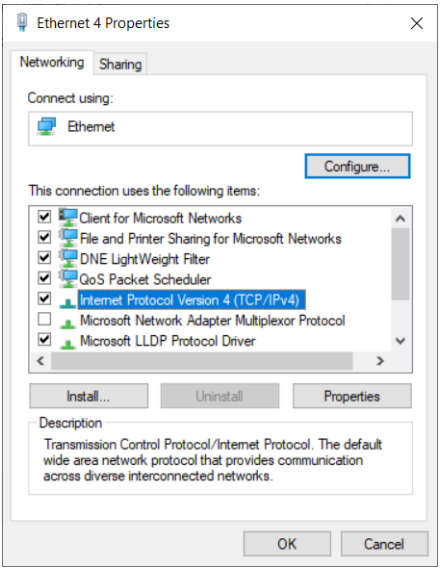
Configuring the network settings

Follow these steps to ensure that the connection is operating correctly:

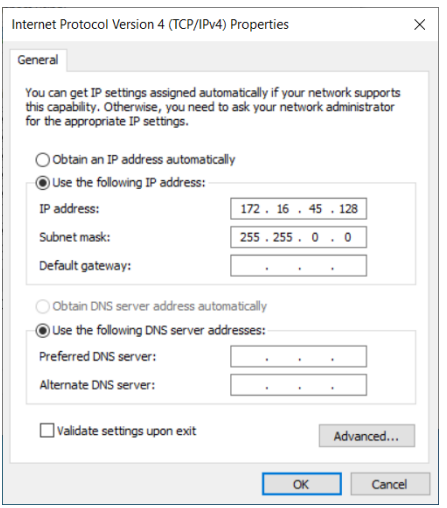
1. Open the Windows Device Manager and check under **Network adapters** that the Ethernet connection with the Security Appliance is recognized.
2. Open **Control Panel>Network and Internet>Network and Sharing Center>View network status and tasks** and click the Ethernet link after **Connections** to open the status dialog box. Click on **Properties**.



3 Select **Internet Protocol Version 4 (TCP/IPv4)** and click on **Properties**.



4 Set the IP address to `172.16.45.128` and click **OK**.



Now you can start the provisioning application. See the *IAR Secure Deploy – Prototyping User Guide* or the *IAR Secure Deploy – Manufacturing User Guide*.

Declaration of Conformity

This declaration of conformity is issued under the sole responsibility of IAR Systems AB.

Product name: **Security Appliance (Hardware Security Module)**

Model number: **STZ-SECAPP-V1**

The product listed above, manufactured by Secure Thingz Ltd. UK, an I.A.R. Systems Group AB company, is in compliance with the following directives or standards:

- CE/UKCA: EMC Directive 2014/30/EU on the following test standards for IT products:
  - EN 61000-6-1:2007, Class B / BS EN 61000-6-1:2007, Class B
  - EN 61000-6-3:2007 + A1:2011 / BS EN 61000-6-3:2007 + A1:2011
- IEC 62368-1:2014 on safety requirements for audio/video, information and communication technology equipment
- CE: RoHS 3 Directive (EU) 2011/65/EU and amending Annex II (EU) 2015/863
- UKCA: RoHS: SI 2012 No.3032 (Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012)
- China RoHS SJ/T 11364-2014 for Controlling Pollution by Electronic Information Products
- VCCI-CISPR 32:2016 VCCI Technical Requirement VCCI-CISPR 32:2016 covering RF Emissions
- FCC: The requirements of 47 CFR Part 15.107 & 15.109 regulations, ICES-003 Issue 6 & ANSI C63.4 Class B for the evaluation of electromagnetic compatibility
- EU Regulation (EC) No 1907/2006 concerning the Registration, Evaluation, Authorization and Restriction of Chemicals (REACH)
- Regulation (EC) No 850/2004, (EU) No 519/2012 on Persistent Organic Pollutants (POPs)
- US provision to the Wall Street Reform and Consumer Protection Act (Dodd-Frank Act 1502 on conflict minerals)
- California proposition 65—California Safe Drinking Water and Toxic Enforcement Act of 1986
- US Final rules under Toxic Substances Control Act (TSCA) Section 6(h) to restrict the importation and use of five persistent, bio-accumulative, and toxic (PBT) chemicals
- Directive 2012/19/EU on Waste from Electrical and Electronic Equipment (WEEE)
- EU Directive 94/62/EC on Packaging and Packaging Waste (P&PW), Article 11, as amended by Directive 2018/852/EU
- EU Directive 2006/66/EC on batteries and accumulators and waste batteries and accumulators, on the following test standards:
  - IEC 62133-2: 2013
  - UN 38.3 (ST/SG/AC.10/11/Rev.7/Section 38.3)
  - Maximum limits of Hg<0.0005%, Cd<0.002%, Pb<0.004% by weight

We keep working together with our partners and suppliers to fulfill our responsibility to ensure our products are compliant with the above directives, regulations, and requirements.

Haiying Yuan

ESG & Compliance Manager

IAR Systems AB

Uppsala, May 25, 2023

Place and date of issue

Locating the part and serial numbers

In some cases, you must provide the serial number of the Security Appliance you are using. You might also need to know the part number when you contact support.

Both the part number and the serial number can be found on the smaller of the two labels underneath the Security Appliance.

Troubleshooting

If you have problems concerning the installation or use of the product:

- Read the user documentation that came with the provisioning software.
- See the technical notes on the Technical Support pages on the IAR website: `www.iar.com/support`
- Contact IAR Technical Support. Information about how to access our Technical Support can be found at `www.iar.com/support`.