



Lattice-Exor-TrustiPhi Reference Kit User Manual

Version 1.0

1	<i>About the Cyber Resilience Reference Kit</i>	<i>4</i>
1.1	What You Can Do with the Reference Kit	4
1.2	Terminology.....	5
2	<i>Quick Start</i>	<i>5</i>
2.1	Hardware Setup	5
2.1.1	Reference Kit Equipment List	5
2.1.2	uS10 Physical Setup	6
2.1.3	Verifying the Gateway Device is Running.....	7
2.1.4	Verifying Connections	8
2.2	Install Software on PC	10
2.2.1	Install ProtoPilot Server.....	10
2.2.2	Install JMobile Runtime	11
2.2.3	Install JMobile Runtime License	12
2.2.4	Install the Exor JMobile Runtime PC Reference Kit Application	14
3	<i>Cyber Resilience Reference Kit Demo Tutorial.....</i>	<i>15</i>
3.1	Initial State – Untrusted Connection	16
3.2	Establishing Hardware Trust	17
3.2.1	Access the ProtoPilot UI	17
3.2.2	Register the XO3D in ProtoPilot	18
3.3	Monitoring and Modifying Security State.....	26
3.4	Gateway Side Demo Page	28
3.4.1	Gateway Side Demo Page Status for Customer System (PC)	30
3.4.2	Gateway Side Demo Page Status for Connections Between Gateway and Customer System.....	31
3.4.3	Gateway Side Demo Page Status for Connections Between Gateway and SoftPLC (Raspberry Pi) ..	31
3.4.4	Gateway Side Demo Page Received PLC Data Counter	32
3.5	Gateway Side Connection Details.....	32
3.6	Customer System (PC) Demo Page	36
3.6.1	Example Customer System Demo Page Views	36
3.6.2	Customer System Side Demo Page Status for Connection to Gateway	40
3.6.3	Customer System Side Demo Page PLC Data Management	40
3.7	Customer System (PC) Connection Details.....	41
4	<i>Demo and Device Reset</i>	<i>42</i>
4.1	Factory Reset of XO3D.....	42
4.2	Factory Reset of ProtoPilot Database	44
5	<i>Programming the MachXO3D Bitstream</i>	<i>45</i>
6	<i>Connecting MachXO3D UART connection</i>	<i>47</i>
7	<i>Reference Documents</i>	<i>48</i>

Table 1 - Revision History

Version	Date	Description of Changes
1.0	2026-08-04	Initial release

1 About the Cyber Resilience Reference Kit

The Cyber Resilience Reference Kit, developed as a collaboration between Lattice Semiconductor, EXOR International, and TrustiPhi, is designed to help industrial and edge device manufacturers accelerate secure system design. Built with the Lattice MachXO3D secure control FPGA, EXOR International's uSOM10 industrial edge platform, and TrustiPhi's ProtoPilot security orchestration platform, the kit enables hardware rooted trust, secure lifecycle management, and industrial grade connectivity.

The Reference Kit delivers secure onboarding, authenticated communication, and continuous integrity validation without adding design complexity, offering:

- Hardware-rooted trust with the Lattice MachXO3D FPGA, including secure boot, protected device identity, and platform firmware resiliency.
- A production-grade IIoT environment via EXOR International's uSOM10 platform, enabling secure onboarding and authenticated industrial communication using JMobile.
- Centralized configuration of security features across device fleets with TrustiPhi ProtoPilot, providing cryptographic key and certificate management plus verified secure update workflows aligned with emerging cybersecurity standards.
- A unified, plug-and-play workflow that lets developers evaluate end-to-end cyber resilience without stitching together multiple vendor tools.
- A faster path to secure system design, helping teams explore practical threat mitigation, compliance readiness, and trusted device recovery.

The kit is intended to help manufacturers explore practical design patterns that support cyber resilience, compliance readiness, and secure lifecycle management expectations reflected in emerging regulations and guidance, including the EU Cyber Resilience Act (CRA) and NIST Special Publication 800-193.

1.1 What You Can Do with the Reference Kit

The Cyber Resilience Reference Kit can be used as an evaluation and reference design platform for hands-on experience with a cyber resilient industrial edge solution. You can first run the demo described in this guide on your own system to see secure onboarding, hardware-protected identity, authenticated communication, and integrity validation in action. You can then work with Lattice Semiconductor, EXOR International, and TrustiPhi to explore how cyber resilient technologies could be integrated into your own product.

With Lattice, you can explore use of the MachXO3D FPGA for flexible secure system control, hardware root-of-trust (HRoot), and platform firmware resiliency (PFR). With EXOR International, you can evaluate an integrated system-on-module built with MachXO3D technology and learn how

Corvina and the JMobile Suite support secure industrial connectivity and control. With TrustiPhi, you can use ProtoPilot to manage security lifecycles of your devices, generate hardware-protected keys and certificates, and support device identity, secure onboarding, and centralized fleet visibility.

1.2 Terminology

Depending on the context, different components of the Cyber Resilience Reference Kit may be referred to in different ways. The following table provides a quick reference for the names that may be used to refer to the different components.

Table 2 - Cyber Resilience Reference Kit Terminology

Name	Aliases
Exor uS10 Evaluation Board with Lattice XO3D FPGA	• Gateway Device • uS10 • uSOM10 • the board • Gateway Board • the device
Raspberry Pi 3	• Soft PLC • the PLC • PLC Device
Customer System	• your PC • the PC
Cyber Resilience Reference Kit	• the Reference Kit
TrustiPhi ProtoPilot Server	• ProtoPilot
Lattice MachXO3D FPGA	• XO3D • XO3D device • XO3D Root of Trust (RoT)

2 Quick Start

This section provides information about how to quickly get your Reference Kit up and running.

2.1 Hardware Setup

This section provides information about how to set up the Reference Kit hardware.

2.1.1 Reference Kit Equipment List

Inside the Reference Kit box, you should receive the following:

- Quick Start Guide
- Raspberry Pi 3 with power supply (“the PLC”)

- Exor uS10 Evaluation Board with Lattice XO3D FPGA with power supply (“the Gateway Device”)
- Two (2) Ethernet cables
- Lattice debugging hardware (UART-to-USB cable)

To fully utilize the Reference Kit, you should have the following equipment:

- Windows 10/11 PC (the “Customer System”) that meets the following requirements:
- Ability to be connected via Ethernet directly to the Gateway Device and obtain an IP address from the Gateway Device
- Allows installation of third-party applications on the system (e.g. ProtoPilot and JMobile runtime)
- Runs Windows Defender Firewall with rules that can be updated via installer or a firewall that can be manually updated
- USB-A mouse to plug into the Gateway Device
- (Recommended) Monitor with HDMI connector for use with the Gateway Device
- (If needed) One or more country-specific plug adapters that allows the included European Type C / Type F round-pin power plugs for the Gateway Device and Raspberry Pi to be used with your local wall outlet.

2.1.2 uS10 Physical Setup

To physically set up the board for use, plug in the board as shown in Figure 1:

- (Recommended) Plug in a monitor via HDMI cable (top left)
- Plug in a USB-A mouse into the USB port (bottom left)
- Connect board to PC via **Ethernet 2** (blue USB connection – third Ethernet connector from the right)
- Connect board to Raspberry Pi via **Ethernet 1** (yellow USB connection – second Ethernet connector from the right)
- When ready, plug in power connector (bottom right)
- (Optional) Plug in Lattice programming cable (upper left side) as described in Chapter 5.
- (Optional) Plug in serial cable (top right) as described in Chapter 6.

NOTE: The optional serial port connection (mini-USB serial connection for serial debug (top right)), Raspberry Pi connection (yellow USB connector in Ethernet 1 (Eth1)), PC connection (blue USB connector in Ethernet 2 (Eth2)), and Lattice Programmer (wires in blue connector box at top left) may be setup later.

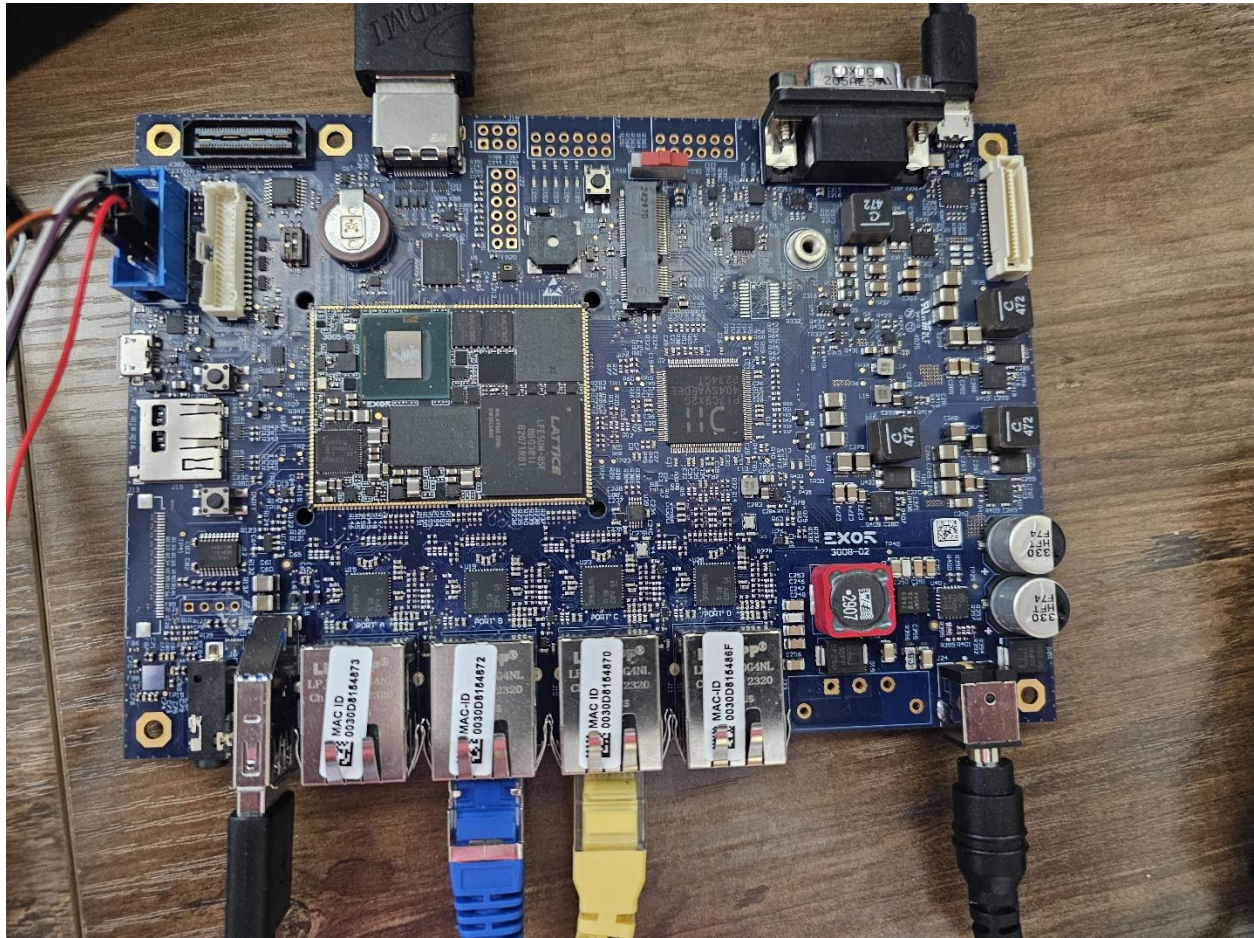


Figure 1 - Visual of Exor uS10 Board Setup

2.1.3 Verifying the Gateway Device is Running

When plugged in, the Gateway Device should automatically boot. Green, orange and light green LED lights should come on and the board should produce an audible beep. During the boot process, you may see Linux booting and a JMobile graphic. Upon boot, the attached monitor should show the demo Main Page as in Figure 2.

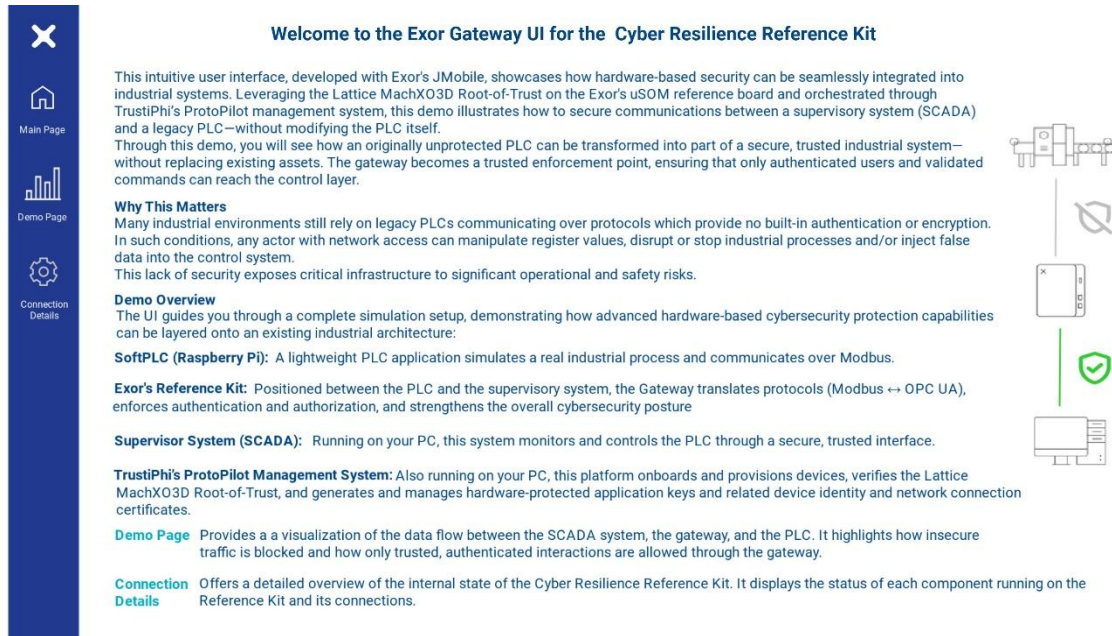


Figure 2 - Exor Gateway Main Page

2.1.4 Verifying Connections

After plugging in the board and attaching the monitor and mouse, you should be able to navigate the Exor UI on the board. If you click on the Demo Page, you will see a graphical view of the connections. If you have not yet powered on and connected the Raspberry Pi, the Demo Page may appear as in Figure 3.

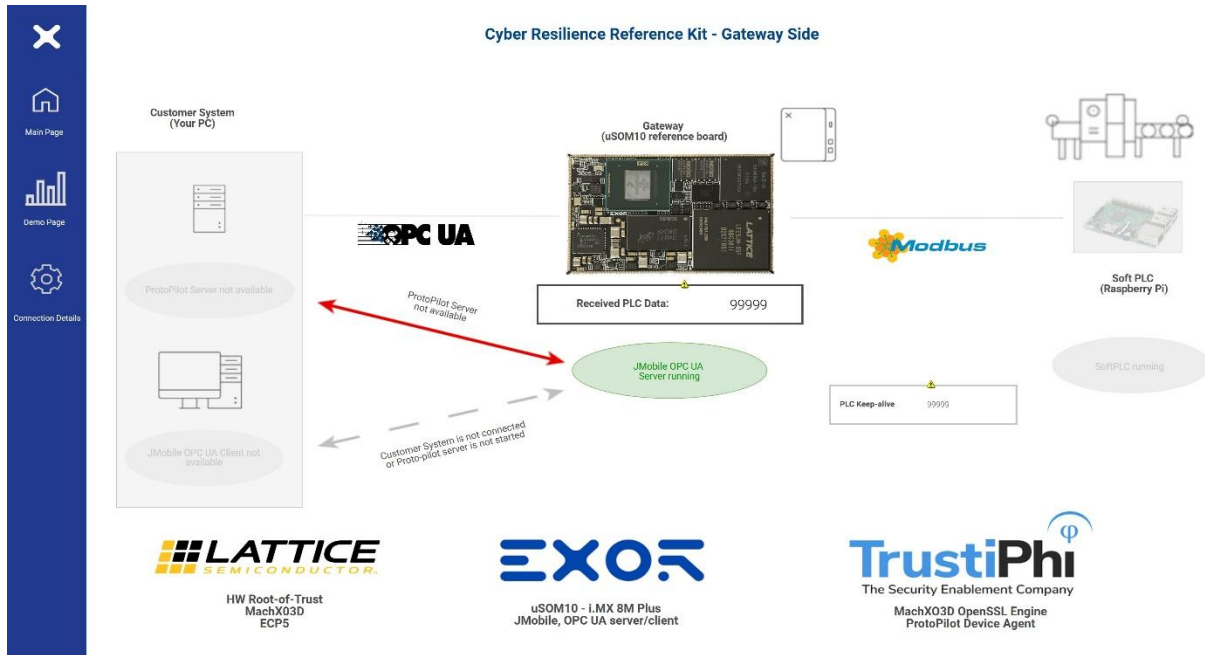


Figure 3 - Initial Gateway Demo Page without Connection to Raspberry Pi

Once the Raspberry Pi has been plugged in and the Ethernet on the Raspberry Pi has been connected to Eth1 on the board (yellow Ethernet connector in Figure 1), the UI should show the connection to the Soft PLC and the “PLC Keep-alive” counter should be running as shown in Figure 4.

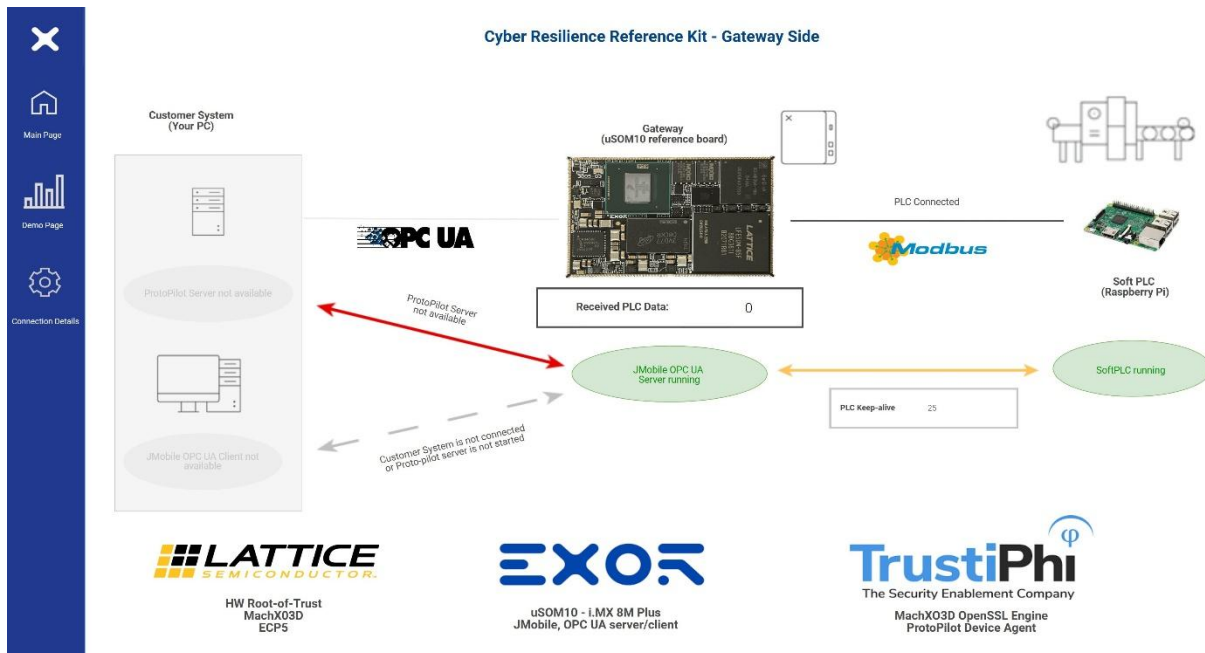


Figure 4 - Raspberry Pi connected to board

After connecting the Ethernet cord between your PC and the Eth2 port on the board (blue Ethernet connector in Figure 1), your PC should obtain an IP address (172.27.75.100) from the board and you should be able to view the demo using a browser such as Chrome or Edge by navigating to <http://172.27.75.99>. You may need to ignore browser warnings about an insecure connection when viewing the Exor UI through the browser. If successful, you will be able to navigate the Exor UI from your PC, confirming the connection between your PC and the board.

2.2 Install Software on PC

To run the demo and utilize the Reference Kit, you should install the following Reference Kit components on your PC:

- ProtoPilot Server
- JMobile Runtime (requires license)
- Exor JMobile Runtime Reference Kit Application

2.2.1 Install ProtoPilot Server

ProtoPilot should be installed by running the .msi installer found at Lattice XO3D Cyber Resilience Reference Kit webpage, accepting the license as shown in Figure 5 and following the prompts to install in the default location as shown in Figure 6.

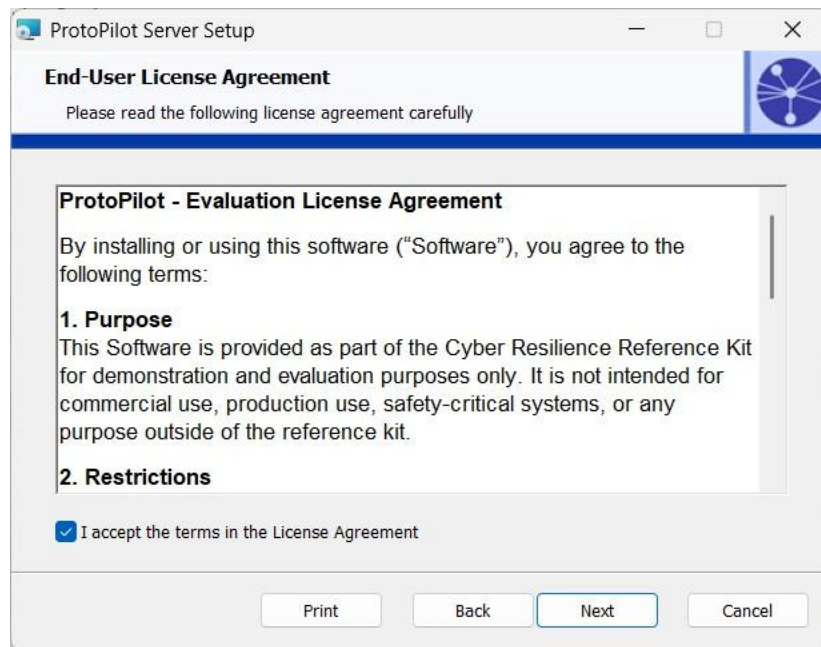


Figure 5 - Accepting the ProtoPilot Evaluation License Agreement

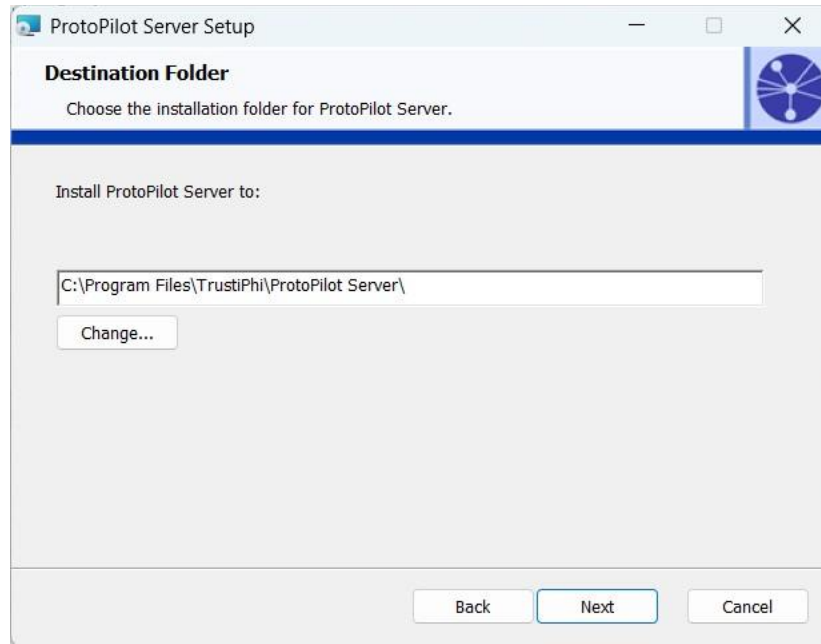


Figure 6 - Installing TrustiPhi ProtoPilot Server

To start ProtoPilot, open the Windows Start menu, type ProtoPilot, and select the ProtoPilot application. If needed, you can also launch it from the Windows Start Menu shortcut folder:

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\TrustiPhi ProtoPilot

Upon launch, the ProtoPilot Server will pop up a debug window that shows select information about the activities of the ProtoPilot Server. To close ProtoPilot, simply close the ProtoPilot Server window.

For additional details and advanced usage of the ProtoPilot Server (and ProtoPilot Agent), see [4].

2.2.2 Install JMobile Runtime

Install JMobile Runtime by running the .exe installer located at Lattice XO3D Cyber Resilience Reference Kit webpage and following the on-screen instructions.

For the purposes of this demo, only the Runtime component is required. When the Component Selection dialog is displayed, select the Runtime component only, as shown in Figure 7.

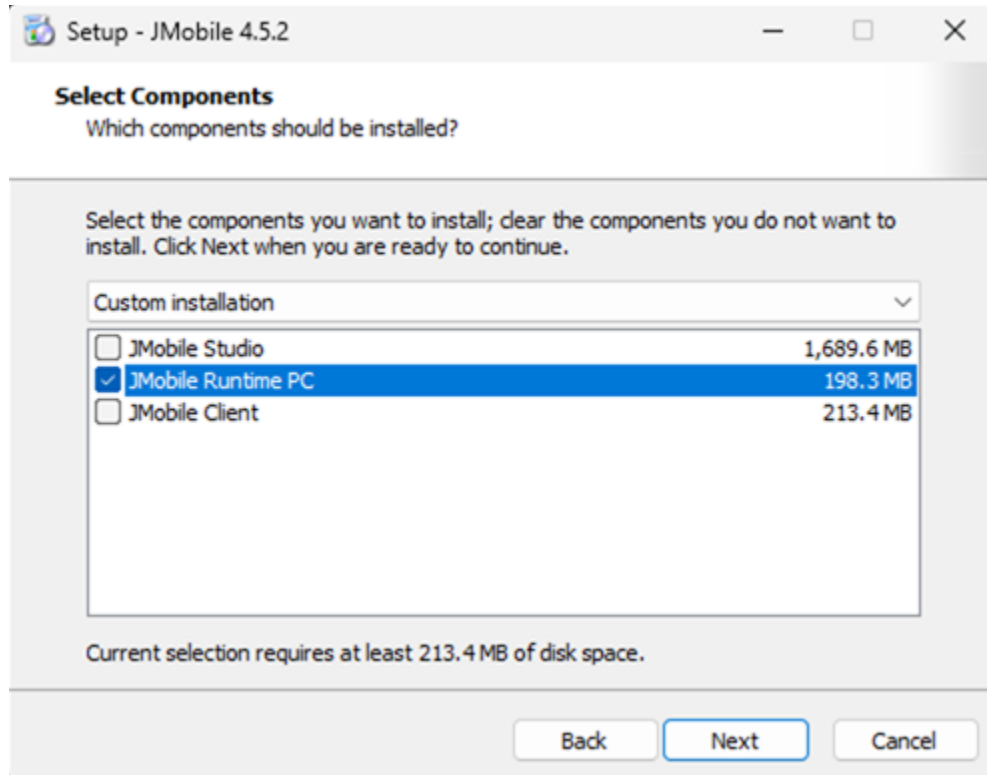


Figure 7 - Installing JMobile Runtime PC

2.2.3 Install JMobile Runtime License

Prerequisite: Ensure that the PC is connected to the Internet, as an active connection is required to verify and register the license.

1. Launch **JMobile Runtime** from the desktop icon or the Start menu
2. The application opens in **Full Screen** mode by default. Right-click anywhere in the application window and clear the **Full Screen** option, as shown in Figure 8. This enables the standard window resizing controls.

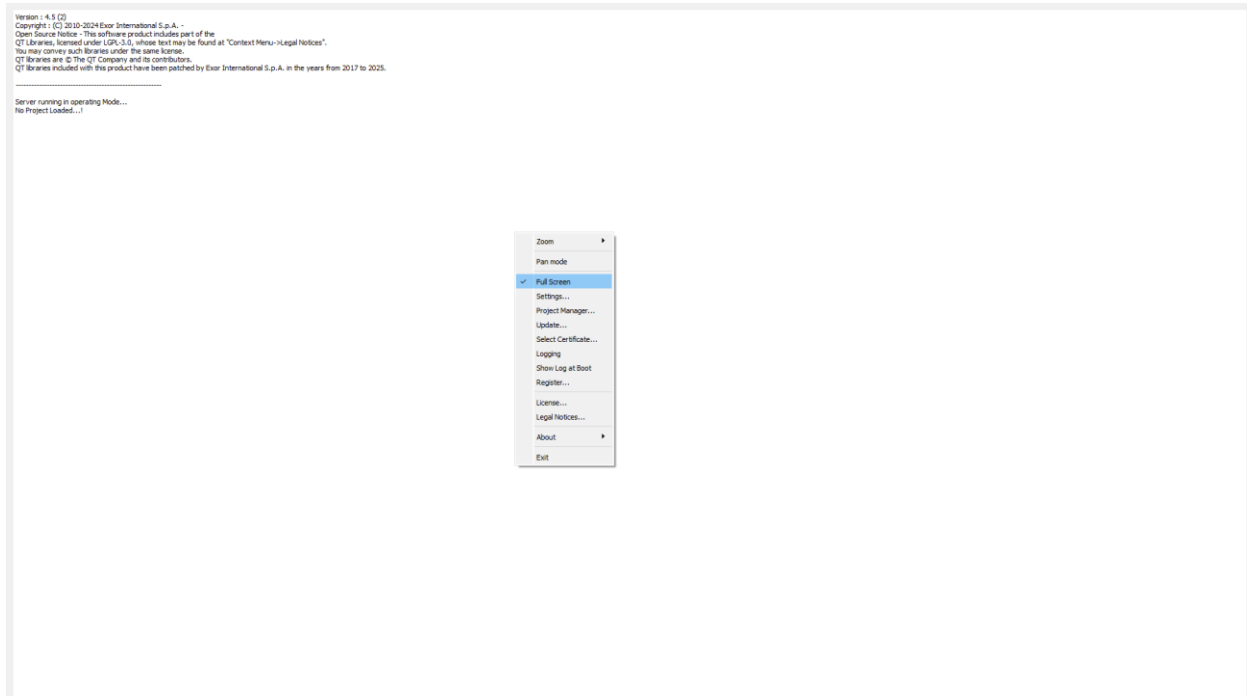


Figure 8 - Launching JMobile Runtime

3. Right click again and select **Register**

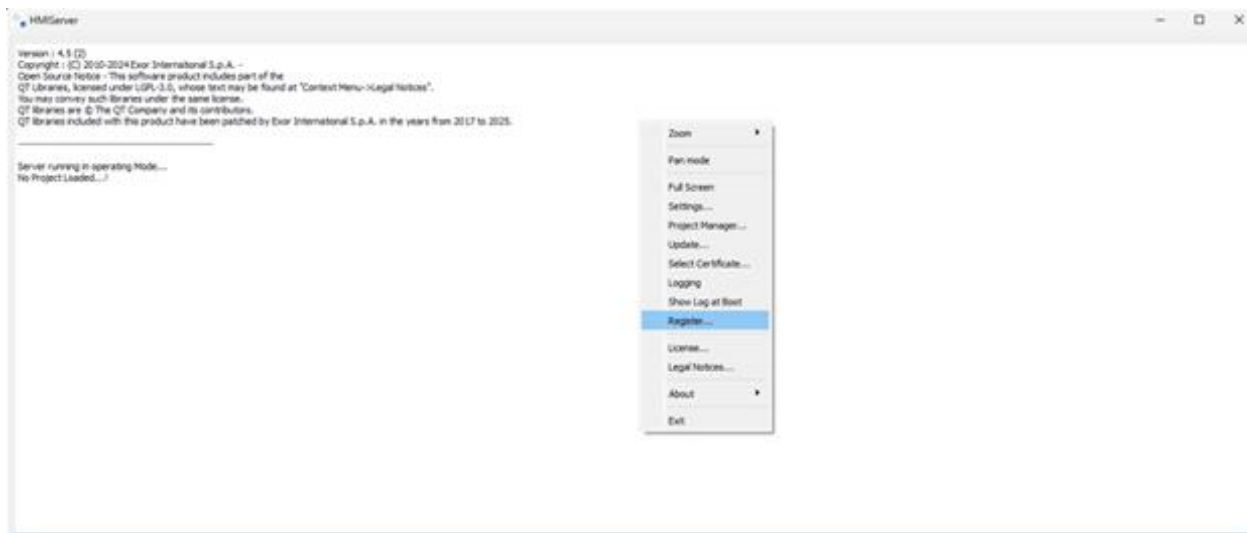


Figure 9 - Registering JMobile Runtime

4. Enter the license key provided to you and click **Register**.



Figure 10 - Entering the JMobile Runtime License Key

5. Once the registration process is complete, verify that the confirmation message shown in Figure 11 is displayed, indicating that the license has been successfully registered.

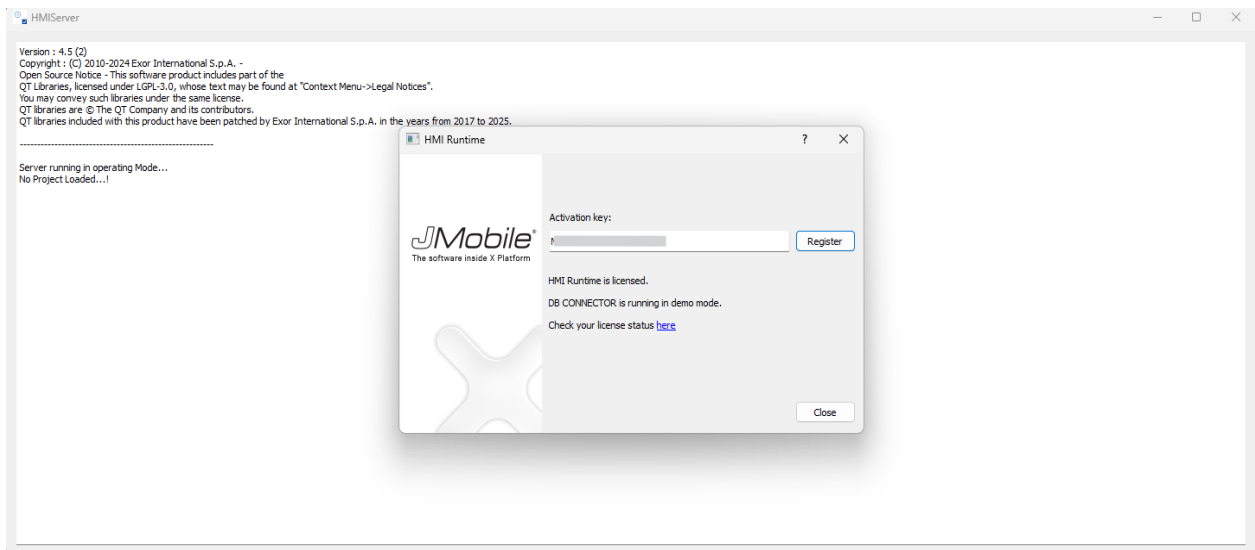


Figure 11 - JMobile Runtime License Confirmation

2.2.4 Install the Exor JMobile Runtime PC Reference Kit Application

Once the JMobile Runtime PC 4.5.2 has been installed and licensed, install the Exor JMobile Runtime PC Reference Kit Application. To do this, open the JMobile Runtime PC application and right-click anywhere in the window.

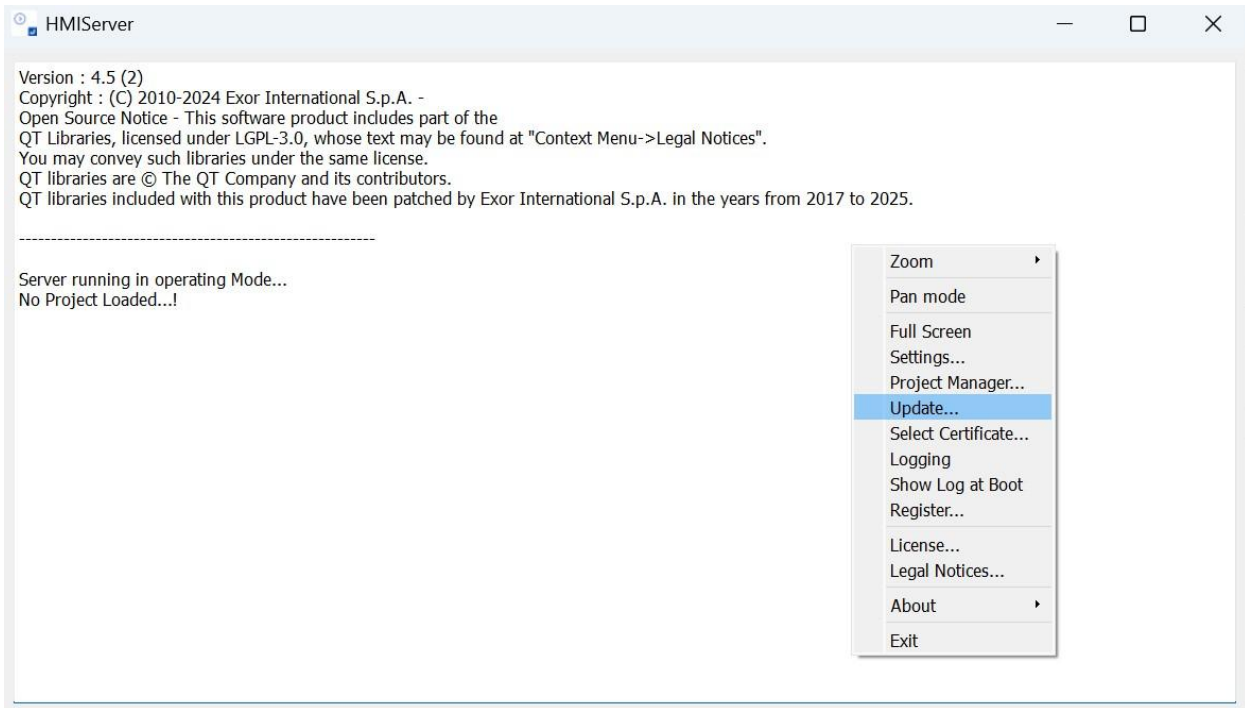


Figure 12 - Updating the JMobile Runtime PC Application

Browse to the update package you downloaded from Lattice XO3D Cyber Resilience Reference Kit webpage and click “Next”. The demo application will load and start. Each subsequent time JMobile Runtime PC is launched, this demo application will run.

For more information about the JMobile Suite and LogicLab, see [5] and [6] respectively.

3 Cyber Resilience Reference Kit Demo Tutorial

TrustiPhi, Exor and Lattice have developed a demonstration for the Cyber Resilience Reference Kit to enable users to explore its capabilities. Users can follow the instructions in this section to explore the demo and learn about cyber resilience. This section is intended to be used to supplement the instructions and explanations from the TrustiPhi ProtoPilot Server UI and the Exor Reference Kit UI.

The Reference Kit demonstration simulates securing an industrial system with the following components:

- A “legacy” programmable logic controller (**PLC**) (implemented using the Axel LogicLab SoftPLC on a Raspberry Pi) that does not implement sufficient communication security is placed in an industrial network
- The **Gateway Device** (implemented on the Exor uS10 Evaluation Board with Lattice XO3D FPGA) is added to the system to secure the connection to the PLC and to modernize the communication

- The **Supervisory System** (simulated using your PC running the Exor JMobile Runtime PC Demo Application) manages the PLC and participates in a mutually authenticated connection with the Gateway Device
- A **Trust Authority** (implemented by an instance of the TrustiPhi ProtoPilot Server running on your PC) is used to ensure that only authorized entities can participate in the secure communication

For the Reference Kit demonstration, we have pre-registered software “bootstrap” keys in the ProtoPilot Server that allow the Gateway Device and Supervisory System to establish a test connection. The Supervisory System is set up to require a verified hardware-protected key before allowing full access to the Gateway. As you explore the Cyber Resilience Reference Kit, you will go through the process of generating, verifying, and certifying keys protected by the Lattice XO3D FPGA’s Root-of-Trust (RoT) and using those keys to protect the connection between the Gateway and Supervisory System.

Since your PC may not have a hardware security module, the Gateway will always accept the (software) key in your PC’s bootstrap certificate. In a production system, the Supervisory System might also be required to implement hardware security to protect its key.

3.1 Initial State – Untrusted Connection

In order to get the Reference Kit into the intended initial state, follow all the instructions from Section 2 to set up the hardware and install the software on your PC.

Power up the Raspberry Pi, power up the Gateway Device, and start ProtoPilot Server and JMobile Runtime PC. When everything has been started, the Gateway demo application and PC demo application will attempt to establish a connection using the software bootstrap keys. The Gateway Device and your PC should be able to connect with the software keys, but the connection will not be trusted, so the OPC UA connection will be blocked and the PLC will not be manageable or allowed onto the industrial network. On the Exor UI on both the Board and on your PC (see Figure 13), you should see a connection with a gray shield with a question mark, indicating that the connection is established, but it is unknown if the Gateway can be trusted.

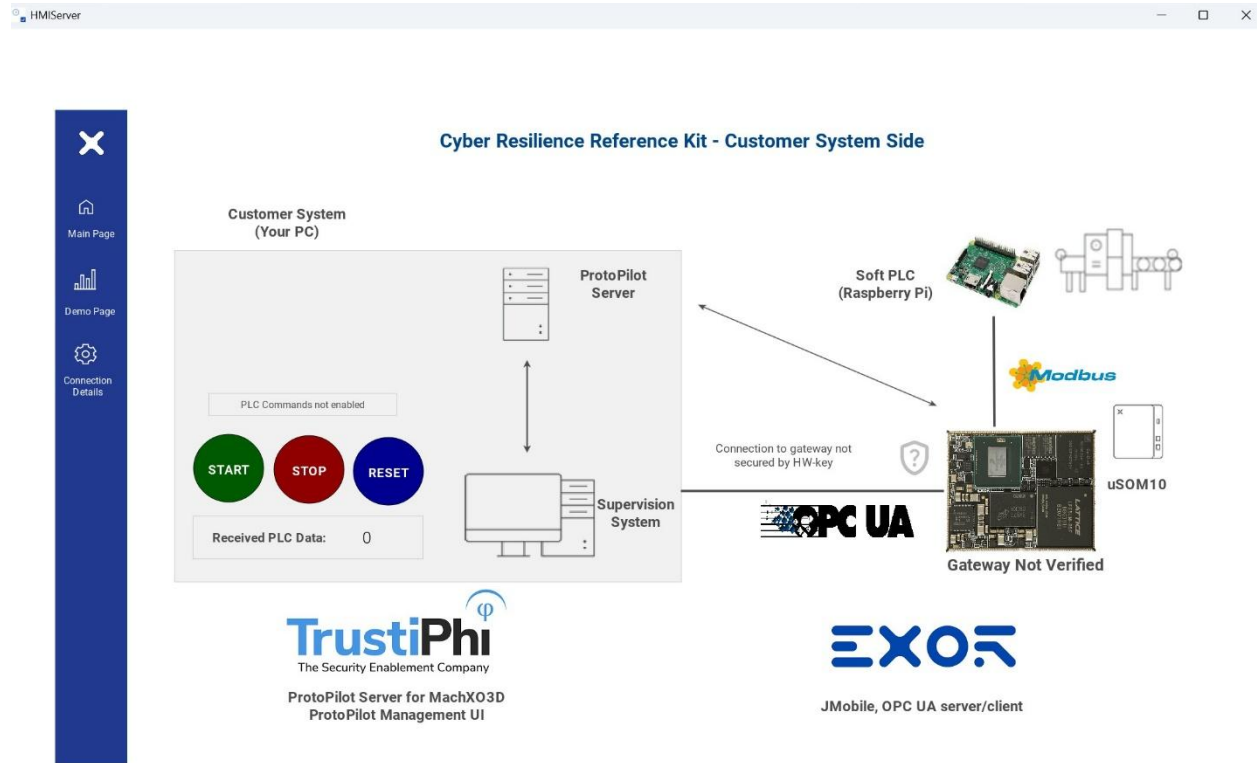


Figure 13 - Untrusted Connection - PC System View

3.2 Establishing Hardware Trust

In order to establish trust in the Gateway Device, the Gateway must prove that it has keys protected by secure hardware. To do this with the Reference Kit, you will use ProtoPilot to provision the RoT on the Lattice XO3D and generate both initial “manufacturing” certificates, called IDevID certificates, and then trusted application keys that will be used to authenticate to the Supervisory System. In order to do this, you will use the ProtoPilot UI.

3.2.1 Access the ProtoPilot UI

To access the ProtoPilot user interface (UI), make sure the ProtoPilot Server is started as described in Section 2.2.1. Then open the ProtoPilot Reference Kit administrative UI in a browser using Google Chrome or Microsoft Edge (or equivalent) at <http://localhost:5018>. You should see the landing page as shown in Figure 14. Note that in a production system, ProtoPilot will require user authentication and be protected via TLS.

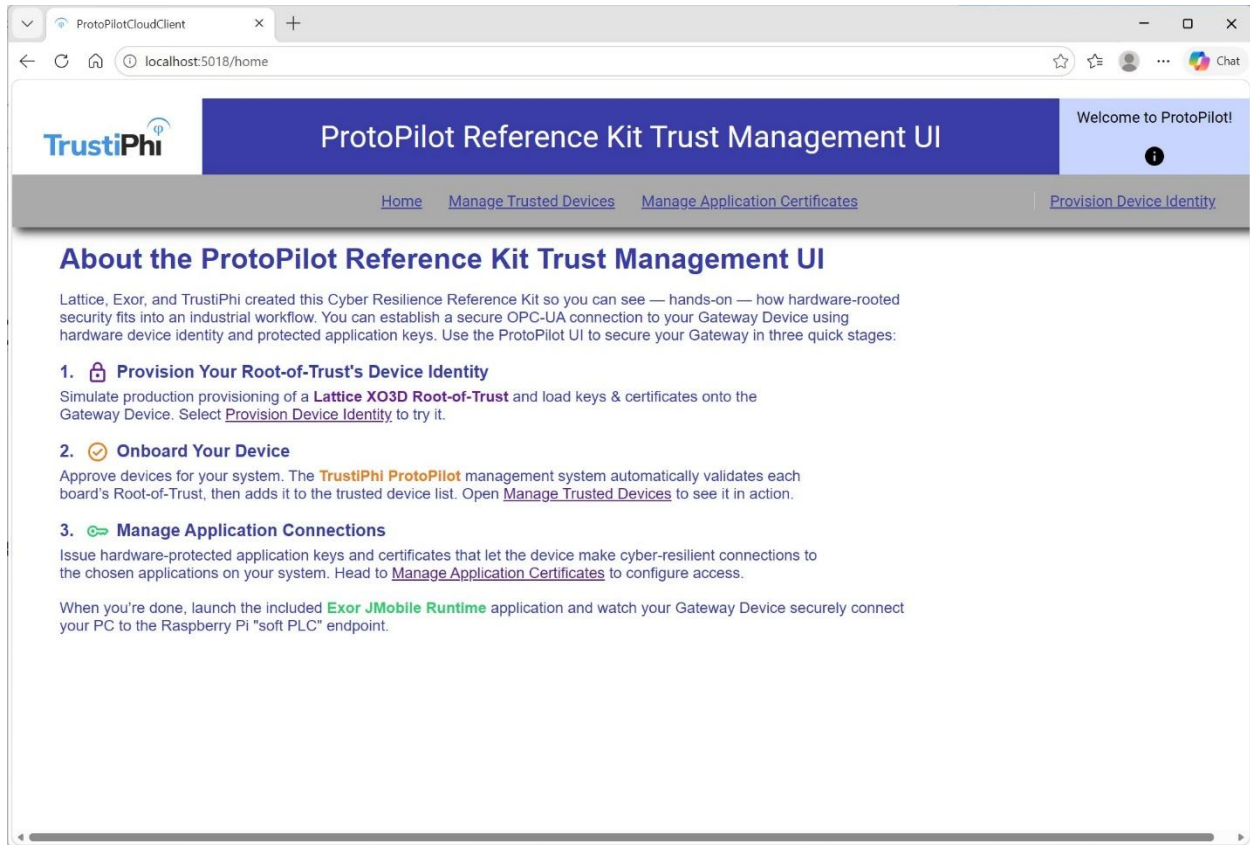


Figure 14 - TrustiPhi ProtoPilot Reference Kit UI Home Screen

3.2.2 Register the XO3D in ProtoPilot

Your Gateway Device is equipped with a Lattice XO3D FPGA with RoT. The XO3D is remotely managed by the ProtoPilot Server and is accessible via a ProtoPilot Agent running on the board. This agent is automatically started by the Exor JMobile Application on the board. The following subsections explain how to register your XO3D in ProtoPilot.

3.2.2.1 Generate IDevID Certificate

From the ProtoPilot UI, click on the “Provision Device Identity” link. The resulting page shown in Figure 15 contains an explanation of device identity provisioning, including the creation of an IDevID key and certificate on an XO3D hardware device.

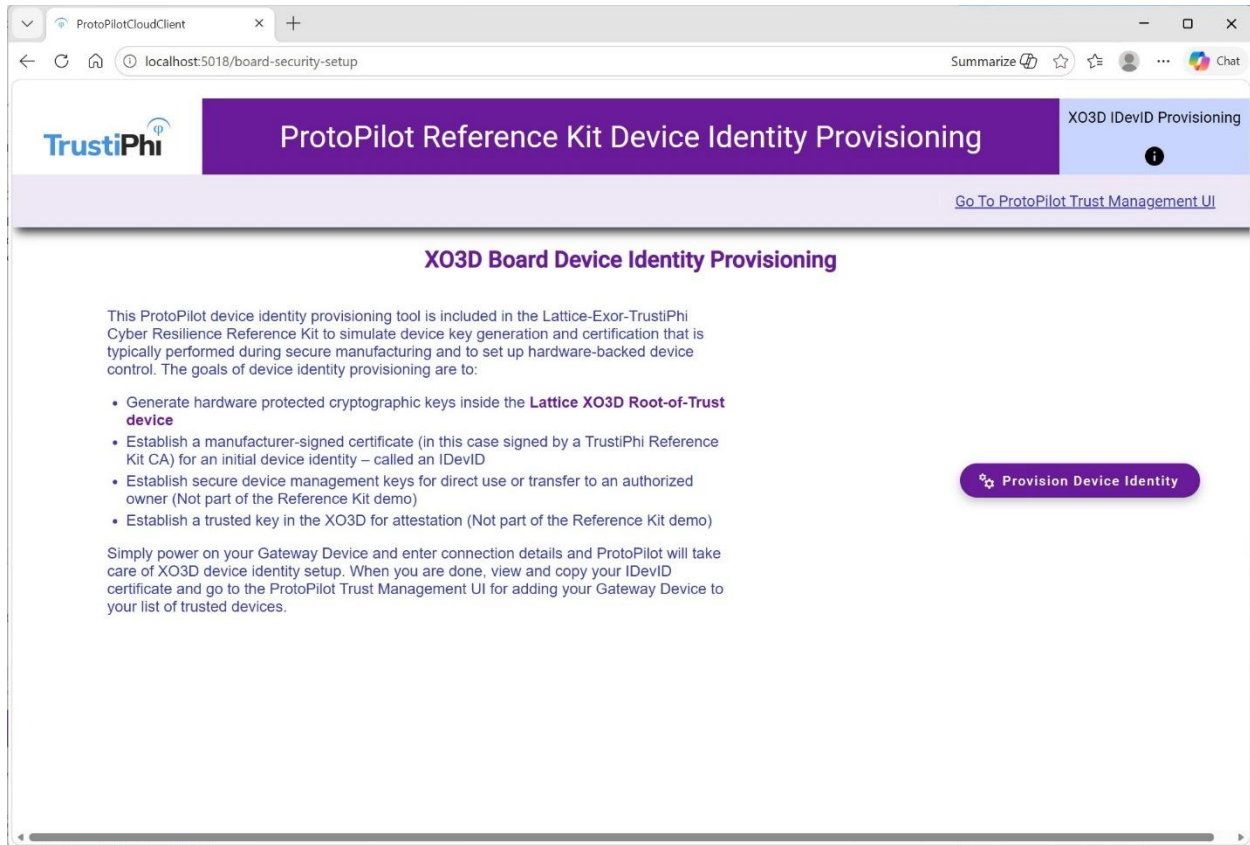


Figure 15 - TrustiPhi ProtoPilot Reference Kit Board Security Setup Screen

Click on the “Provision Device Identity” button on the ProtoPilot Reference Kit Board Security Setup page. A manufacture dialogue will pop up. Fill out the fields as follows:

- **IP Address and Port:** Use the default uS10 board IP address (172.27.75.99) and port (7255) that the XO3D device is listening on.
- **Certificate Template:** (Required) Enter any desired name in the Common Name field (e.g. uS10-Device). You may optionally set other certificate fields as desired. Since IDevIDs are typically generated once during manufacturing, the expiration time should be set beyond the expected lifetime of the device. The default expiration time for the reference kit is set for 10 years. NOTE: ProtoPilot provides a method to reset the device to factory defaults and to regenerate IDevID certificates at any time.
- **(Optional) Save IDevID Certificate:** This may be left blank. This allows you to save the IDevID Certificate on the Gateway Device.
- **(Optional) Save IDevID CA Certificate Chain:** This may be left blank. This allows you to save the IDevID Certificate Chain on the Gateway Device.

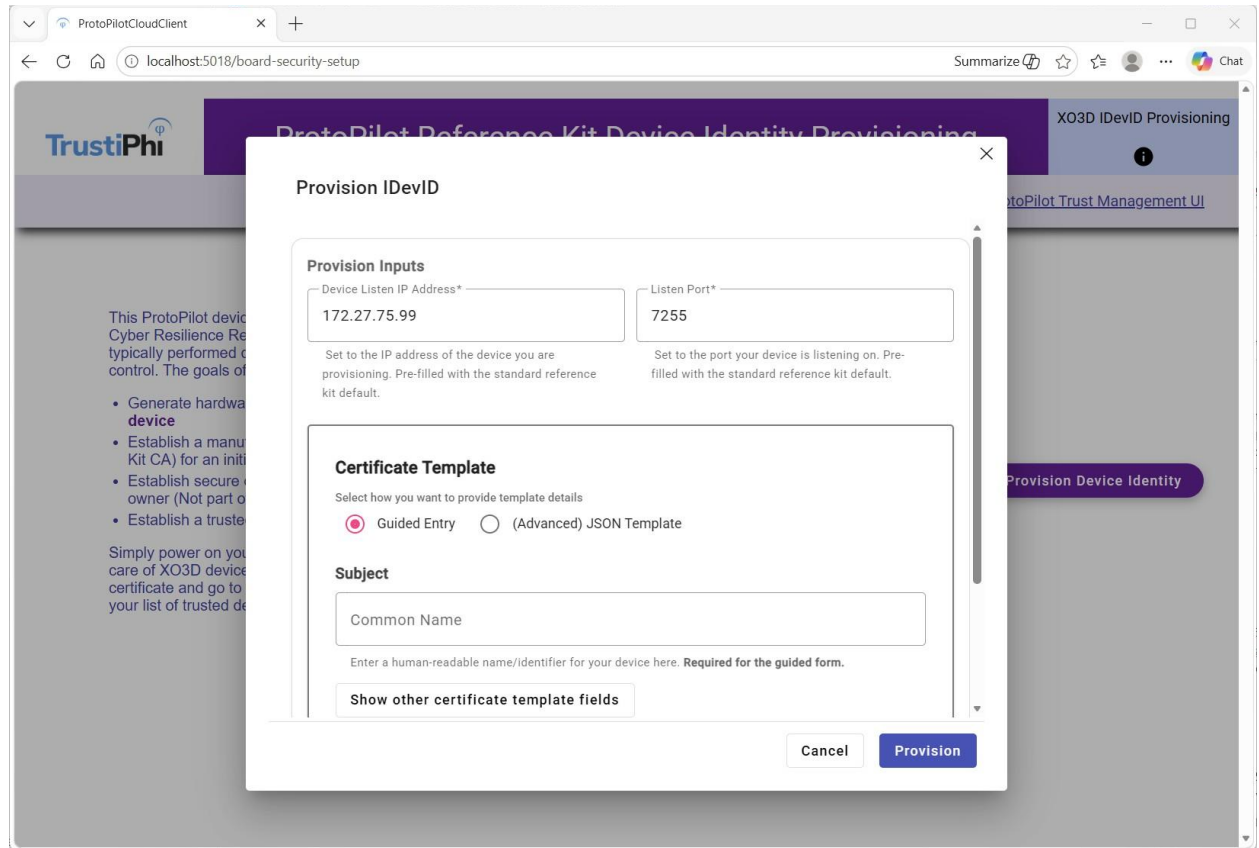


Figure 16 - Provisioning an XO3D device

Click the “Provision” button. This should result in the creation of an IDevID certificate. If successful, scroll down in the window and copy the IDevID certificate. NOTE: If you accidentally close the window without copying the certificate, simply follow the process again and create another certificate. ProtoPilot will reuse the IDevID key generated in the Lattice XO3D the first time the IDevID certificate is created.

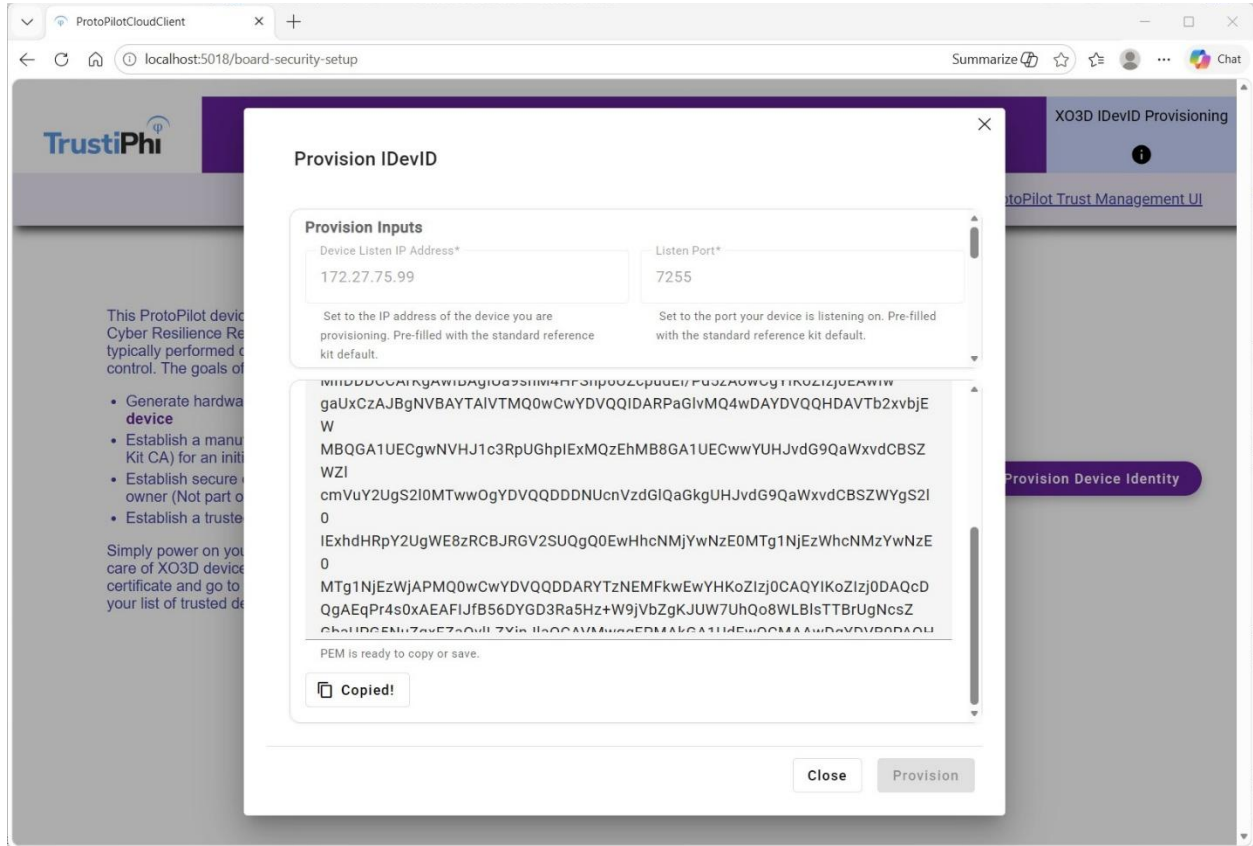


Figure 17 - Copied XO3D IDevID Certificate

3.2.2.2 Add the XO3D Trusted Device to ProtoPilot

Close the popup window from the provisioning process and click on the “Go To ProtoPilot Trust Management UI” link in the top right. Then Click on the “Manage Trusted Devices” link in the middle. On this page, you will see the two pre-registered “bootstrap” software devices – one for software-based access on the Gateway and one for the default software “device” used on your PC by the Exor JMobile Runtime PC application as shown in Figure 18.

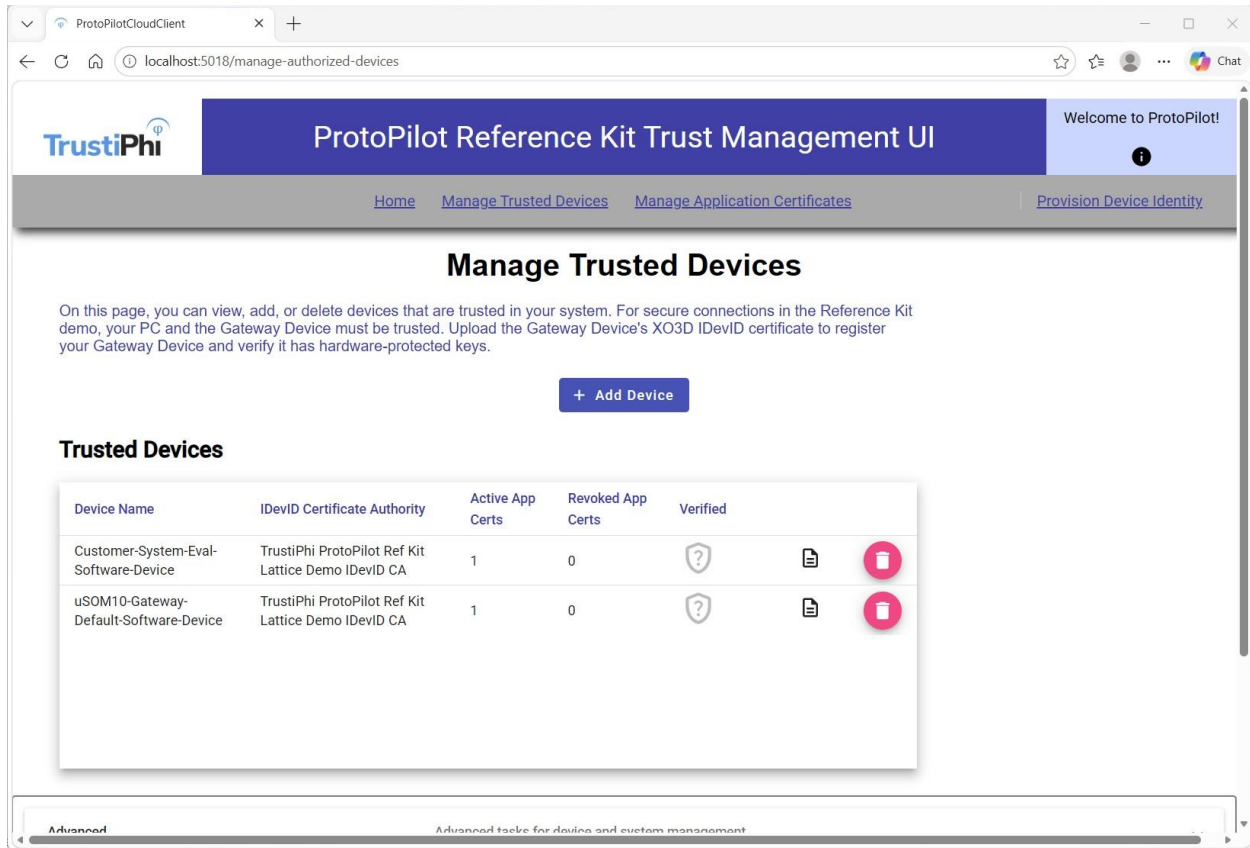


Figure 18 - ProtoPilot Manage Trusted Devices Page with Default Trusted Devices

Click on the “+ Add Device” button to add your XO3D to your list of trusted devices.

A window will pop up to add a new device. In the pop-up window, enter the following values:

- **Displayable Text Name:** Any desired name such as “uS10-with-XO3D”
- **IDevID Certificate:** Paste the certificate that was copied in the previous step. (NOTE: If you accidentally lost the certificate from the previous step, simply go back and create another IDevID certificate). This certificate and the corresponding key will be used by ProtoPilot as the basis for verifying that the device has a valid Lattice XO3D RoT
- **Device Listen IP Address** and **Listen Port:** Use the prefilled uS10 board IP address (172.25.75.99) and port (7255) that the XO3D device is listening on.

Then click “Add Device”.

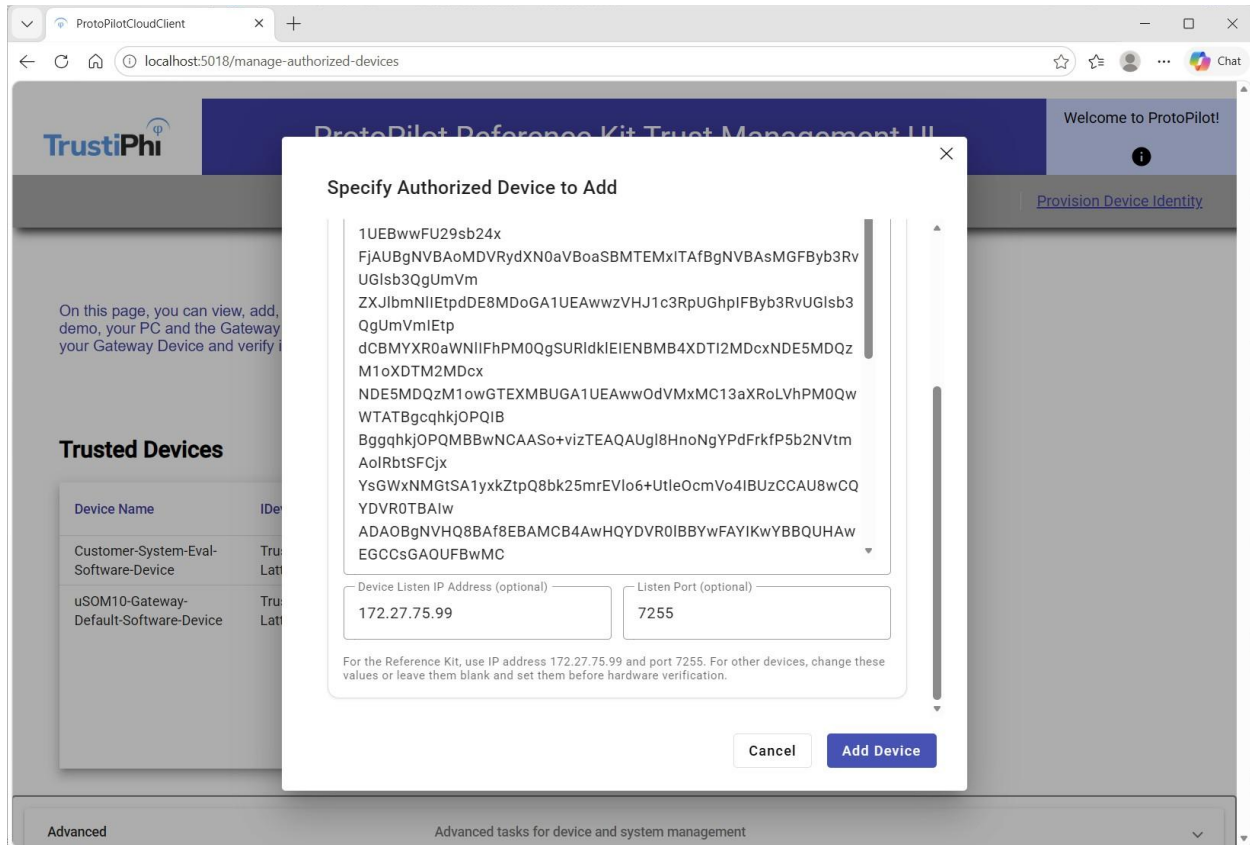


Figure 19 - Adding Your Gateway Device to the List of Trusted Devices in ProtoPilot

If successful, upon closing the popup window, a new Device entry should be visible with a button to verify your device. Click the “Verify” button. If successful, a popup should indicate success and a green shield should appear for the uS10 XO3D device.

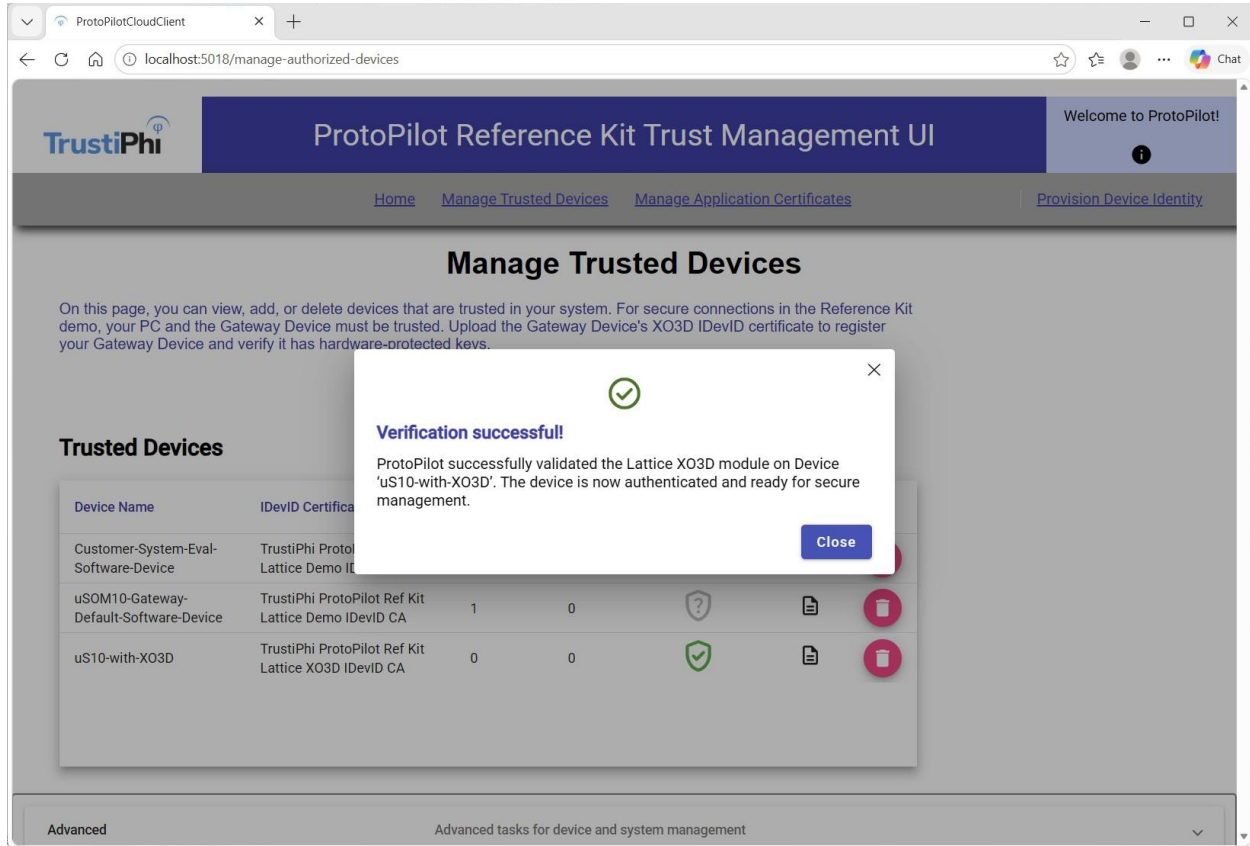


Figure 20 - Verified Lattice MachXO3D Hardware Device in ProtoPilot

3.2.2.3 Add Application Certificate

Once the Gateway Device with Lattice XO3D RoT has been added as a trusted device, a new application certificate can be created. Application certificates are the keys that are used by the Exor JMobile applications for secure communications.

Click on the “Manage Application Certificates” link at the top. Click the “Add Application Certificate” button to create and register a new application certificate associated with an XO3D device.

In the popup, fill out the fields as follows:

- **Trusted Device:** Select the XO3D device name that was added in section 3.2.2.2 from the dropdown menu.
- **Device IP Address** and **Device Port:** These fields should populate with the IP address and port for that device. These values should be left as-is.
- **Replace existing key if present:** This field may be checked or left unchecked. If checked, the application key will be replaced inside the XO3D RoT and any previously generated application certificates will no longer be usable. If unchecked, a new application key will be

generated if none existed and a new application certificate will be created with the new or existing key, depending on the selection.

- **Certificate Template:** (Required) Provide any name for the application certificate such as uS10-XO3D-App-Key-1. You may optionally set other certificate fields as desired. **IMPORTANT:** For the application certificate to work with the Exor software, ensure that the “serverAuth” check box in Extended Key Usage remains checked. This field is checked by the secure connection software to ensure that the application key may be used in the server role.
- **Save App Certificate:** Select the “Save App Certificate” checkbox and use the default app cert name and file location. **IMPORTANT:** The Exor software will look for its certificate in the default location. This is required to establish a secure connection.
- **Save App CA Certificate Chain:** Select the “Save App CA Certificate Chain” checkbox and use the default app CA certificate chain name and default location. **IMPORTANT:** The Exor software will look for its certificate chain in the default location. This is required to establish a secure connection.

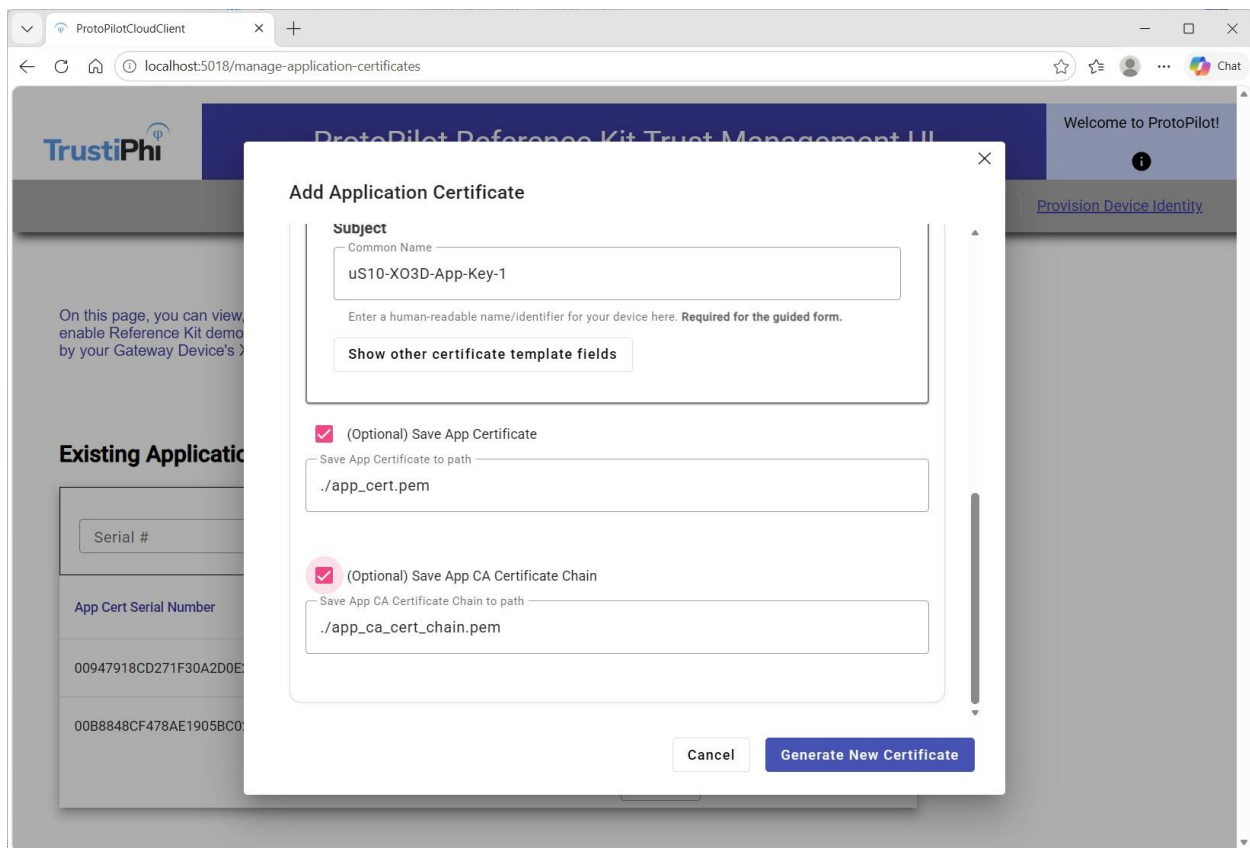


Figure 21 – Generating an XO3D-protected Application Key and Certificate

Click “Generate New Certificate”. Make sure that the application certificate was successfully created. If so, when the popup window is closed, the new application certificate should show up in the application certificate list.

3.3 Monitoring and Modifying Security State

Once the process in Section 3.2 has been completed, the Gateway Device and the Supervisory System running on your PC in the Exor JMobile Runtime PC should automatically connect using the new XO3D-protected application certificate. On the Gateway Device, the Exor JMobile application is using the **TrustiPhi XO3D OpenSSL ENGINE** to access the hardware-protected application key in the XO3D RoT. Since the application certificates for the Gateway Device and your PC are valid and trusted, each side allows the connection. Figure 22 shows a screen shot of a PC with the Exor JMobile Runtime PC, Exor JMobile Runtime on the Gateway (remote view via browser), and the table of application certificates in TrustiPhi ProtoPilot showing a fully secured connection.

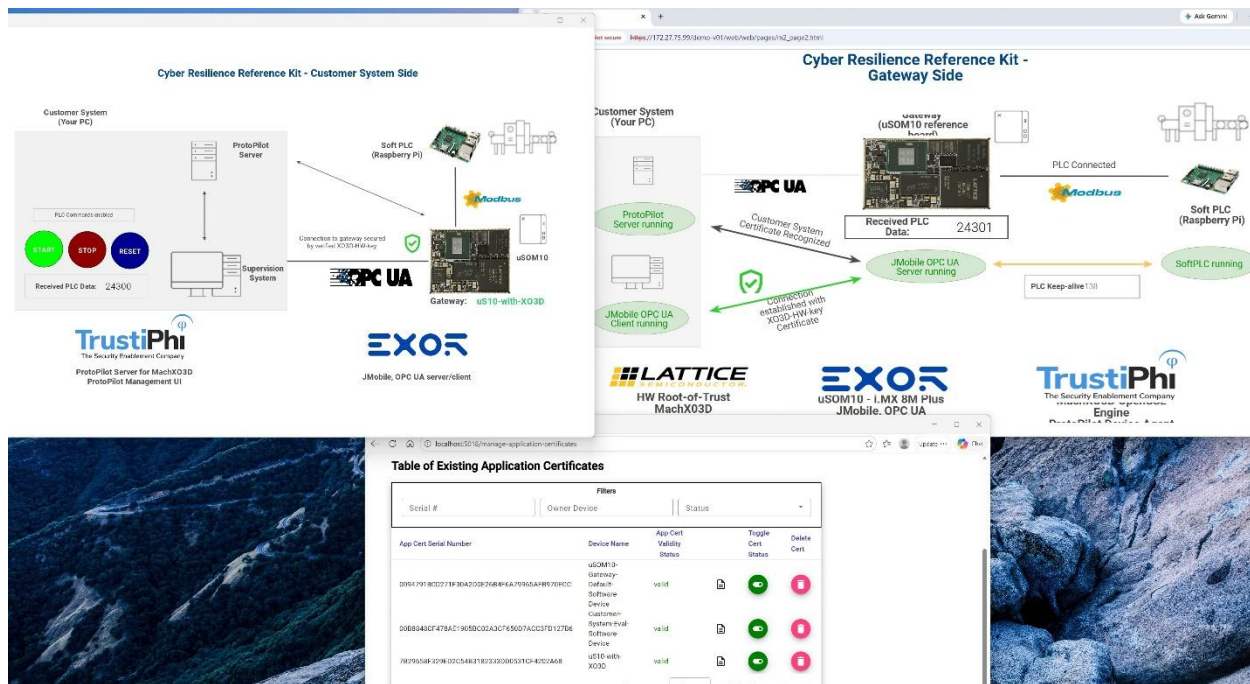


Figure 22 - PC View of Secure Connection with JMobile, ProtoPilot, and XO3D-protected Connection

CONGRATULATIONS! If you see secure connections with a verified XO3D hardware key, you have successfully modernized your industrial connection to your legacy PLC, using the latest OPC UA protocols and ensuring only hardware-protected, pre-registered devices are allowed on your network.

Now that you have set up a trusted connection, you can experiment with different security states to see how the system maintains its protections. On the ProtoPilot UI for the Reference Kit, buttons for easy toggling of certificate revocation status and deletion of devices and certificates are provided.

Feel free to try out setting the system in different states to see how the connection state changes. NOTE: If you delete any of the software certificates or software devices, they can only be recovered by performing a factory reset in ProtoPilot to return the database to the default state. In this scenario, you will need to reregister the Gateway Device with XO3D and generate a new hardware-protected application key.

For demonstration purposes, the Exor JMobile applications on the PC and Gateway are designed to poll the ProtoPilot Server to detect state changes with the application certificates. When you change the list of application certificates by revoking, unrevoking, deleting certificates, or adding certificates, the Exor JMobile applications will detect the changes and adjust their state accordingly.

NOTE1: It may take several seconds for the applications to detect the changes and they may not report the status change at the same time.

NOTE2: The Exor JMobile Runtime PC demo application will assume the FIRST hardware-protected certificate listed in the ProtoPilot database is the certificate that will be used by the Gateway when it connects. If the certificate saved on the Gateway does not match the first hardware-protected certificate in ProtoPilot, the PC will not recognize the certificate.

The following lists the expected behavior based on the state of the three application certificates in ProtoPilot:

Table 3 - Expected Exor JMobile Application States Based on Certificate Status

uSOM10 Gateway Software Cert	Customer System Eval Software Cert	(First) XO3D-protected Device Cert	Expected System State
Valid	Valid	Valid	Secure Connection
Revoked/Absent	Valid	Valid	Secure Connection (XO3D Cert Used)
Valid	Valid	Revoked/Absent	Bootstrap Connection
Revoked/Absent	Valid	Revoked/Absent	Gateway Untrusted
Valid	Revoked/Absent	Valid	Customer System Untrusted
Valid	Revoked/Absent	Revoked/Absent	Customer System Untrusted
Revoked/Absent	Revoked/Absent	Valid	Customer System Untrusted
Revoked/Absent	Revoked/Absent	Revoked/Absent	Neither Side Trusted

3.4 Gateway Side Demo Page

The Gateway Side view of the JMobile Runtime shows the Gateway’s perspective of the connection with the Customer System. The view changes depending on the status of a variety of variables.

For example, Figure 23 shows the Reference Kit fully trusted ProtoPilot configuration with all three certificates valid and all demo applications started as described in the first row of Table 3.

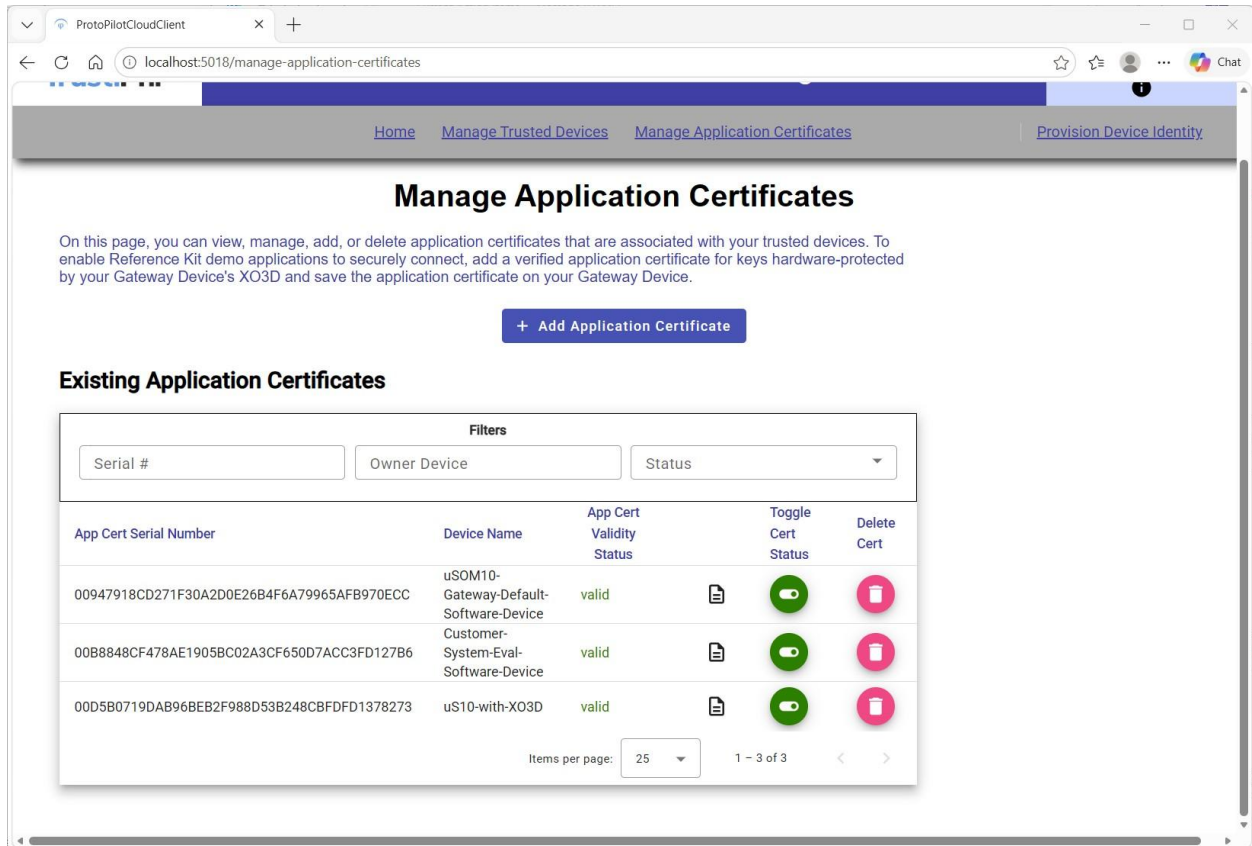


Figure 23 – Application Certificates List with XO3D Hardware Certificate

In this scenario, when you click on the “Demo Page” graphic with the bar graph icon on the left hand side of the Gateway JMobile Runtime application, you should see a graphical view of the connections to the Gateway as in Figure 24:

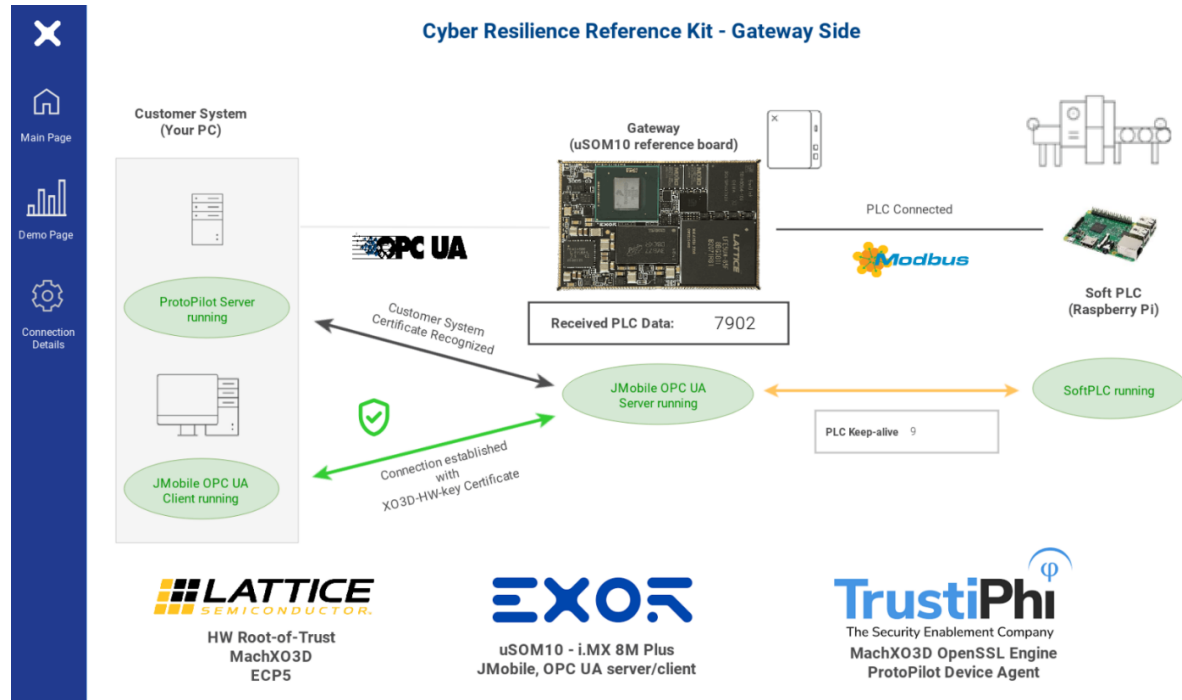


Figure 24 – Example of Demo Page on Gateway with Hardware-Protected Connection

You can interpret the graphical view on the Demo Page as consisting of three main parts and their interconnections as shown in Figure 25.

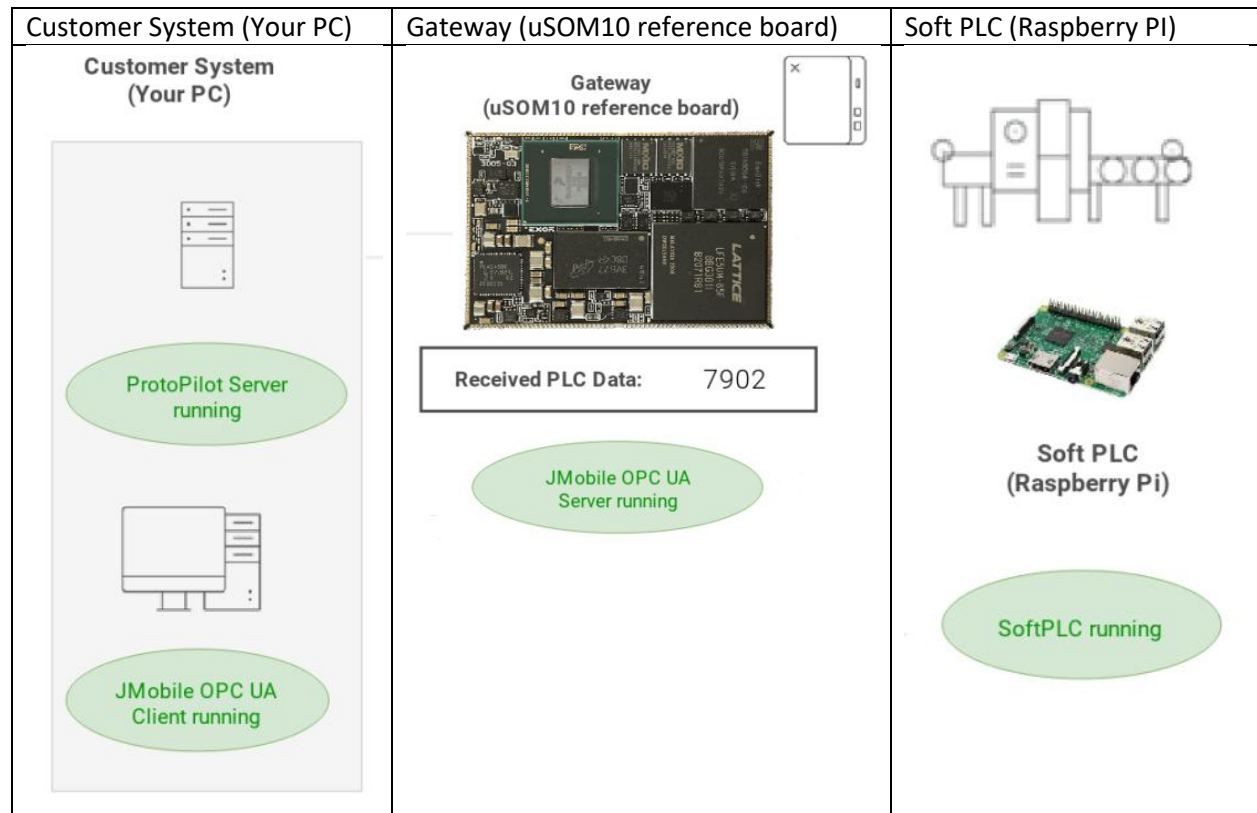


Figure 25 - Overview of Graphical Elements on the Gateway Side Demo Page

3.4.1 Gateway Side Demo Page Status for Customer System (PC)

The Customer System runs two applications: **ProtoPilot Server** and **JMobile OPC UA Client**.

The Demo Page bubble view of **ProtoPilot Server** will show the Customer System operational states of the ProtoPilot Server:

Operation State	Description
ProtoPilot Server running	Correct operation state.
ProtoPilot Server not available	ProtoPilot Server is not running or that Customer System is not physically connected to Gateway.

The Demo Page view of **JMobile OPC UA Client** will show the operational states of the JMobile Runtime application on the Customer System:

Operation State	Description
JMobile OPC UA Client running	Correct operation state.

JMobile OPC UA Client not available	JMobile Runtime PC with updated JMobile OPC UA Client is not running or that Customer System is not physically connected to Gateway.
-------------------------------------	--

3.4.2 Gateway Side Demo Page Status for Connections Between Gateway and Customer System

The connection shown by arrow between the **ProtoPilot Server** and the **JMobile OPC UA Server** shows a description of the certificate trust status read from the ProtoPilot Server:

Operation State	Description
Customer System Certificate Recognized	Correct operation state.
ProtoPilot Server not available	ProtoPilot Server is not running or Customer System is not physically connected to Gateway.
Customer System Certificate Revoked	Some needed Certificate is revoked by Reference Kit UI
Checking Customer System Trust Status	Checking customer system trust status is in progress.

The connection shown by arrow between the **JMobile OPC UA Client** and the **JMobile OPC UA Server** shows a description of the OPC-UA connection status:

Operation State	Description
Connection established with XO3D-HW-key Certificate	Correct operation state if XO3D-HW-key Certificate exists and is not revoked.
Connection established with Software-key Certificate	Correct operation state if XO3D-HW-key Certificate doesn't exist or is revoked.
Customer System is not connected or ProtoPilot Server is not started	ProtoPilot server is not running or Customer System is not physically connected to Gateway.
Connection cannot be established	Some needed Certificate is revoked by Reference Kit UI
No valid Customer System or Software-key/XO3D-HW-key certificate exists	Neither Customer System or Software-key/XO3D-HW-key certificate exists.

3.4.3 Gateway Side Demo Page Status for Connections Between Gateway and SoftPLC (Raspberry Pi)

Above the Modbus logo on the Gateway Side Demo Page, a graphical connection line indicator, together with a status message, shows whether the Gateway is successfully connected to the Soft PLC. This enables you to verify the communication status between the Gateway and the Soft PLC at a glance.

Operation State	Description
PLC Connected	Correct operation state with the SoftPLC plugged into the Gateway

(Gray line with no words) + SoftPLC image is grayed out	SoftPLC is not physically plugged in and/or detected by the Gateway
---	---

The connection shown by arrow between the **JMobile OPC UA Server running** bubble and the **SoftPLC running** bubble indicates the logical connection status between the Gateway and SoftPLC “PLC Keep Alive” counter.

Operation State	Description
Soft PLC running shown in green bubble + yellow arrow between bubbles	Correct operation state with the SoftPLC plugged into the Gateway and SoftPLC Keep-alive counter running
SoftPLC running shown in grayed out bubble + no arrow between bubbles	SoftPLC is not physically plugged in and/or SoftPLC Keep-alive counter is not reachable by the Gateway

3.4.4 Gateway Side Demo Page Received PLC Data Counter

The “Received PLC Data:” box under the Gateway image shows the current value of the PLC Customer System-Managed data. This counter will start running on initial boot and can be managed (started, stopped, reset) from the JMobile Runtime application on the PC when a fully trusted (hardware-protected) connection has been established between the Customer System and Gateway. See section 3.6.3 for details of the management of the PLC Data Counter on the Customer System.

3.5 Gateway Side Connection Details

At any time while running the Exor JMobile Runtime applications on the Gateway, you can check the current status of the demo and trusted connection from the Gateway JMobile Runtime Application UI.

On the Gateway side, click on the “Connection Details” gear icon on the left side to view the following information as shown in the example screen shot in Figure 26.

- Gateway IP Addresses
- Eth0
- Eth1 (should show 172.27.74.99 for the PLC network)
- Eth2 (should show 172.27.75.99 for the PC network)
- Eth3
- PLC IP Address (fixed at 172.27.74.100)
- Communication Diagram – This diagram shows the conceptual operations and connection between the Gateway and Customer System (PC).

- **“Gateway:”** XO3D-protected identity name – This will show the name of the XO3D device that you registered in ProtoPilot if a valid hardware-protected application certificate is detected in the ProtoPilot Server trusted devices list.
- Demo operation state details
- Connection to Raspberry Pi
- State of PLC on Raspberry Pi
- State of Exor Gateway Agent
- State of Connection with PC
- State of Gateway OPC UA Server
- State of ProtoPilot Agent on Gateway
- Connection status with ProtoPilot Server on PC
- State of Gateway XO3D Hardware certificate
- State of Gateway software bootstrap certificate



Figure 26 - Example Connection Details Page on Gateway with XO3D Hardware Certificate Revoked

RaspberryPi connection operation states:

Indicator State Example	Operation State	Description
 RaspberryPi is connected	RaspberryPi is connected	Correct operation state.
	RaspberryPi is not connected. Connect RaspberryPi eth port	RaspberryPi is not connected. The solution should be to connect RaspberryPi ethernet port to Gateway eth1 port (yellow cable on the Figure 1).

PLC operation states:

Indicator State Example	Operation State	Description
 PLC is running.	PLC is running.	Correct operation state.
	PLC is not running. Check connection cable.	PLC is not running. The solution could be to connect RaspberryPi ethernet port to Gateway eth1 port (yellow cable on the Figure 1).

Gateway operation states:

Indicator State Example	Operation State	Description
 gateway_agent is running	Gateway agent is running.	Correct operation state.
	Gateway_agent is not running. Try restarting the Gateway.	Gateway_agent is not running. Try restarting the Gateway.

Connection operation states:

Indicator State Example	Operation State	Description
 Connection established with XO3D-HW-key Certificate	Connection established with XO3D-HW-key Certificate.	Correct operation state.
	Connection established with Software-key Certificate	“Bootstrap” connected state when the Gateway software certificate is usable, but the Gateway hardware certificate is not available.
	Encrypted Tunnel is not active. Ensure the ProtoPilot Server and OPC UA client are running and certificates are not revoked	Encrypted Tunnel is not active. Ensure the ProtoPilot Server and OPC UA client are running and certificates are not revoked
	Customer System is not connected or Proto-pilot server is not started	Customer System is not connected or Proto-pilot server is not started. Ensure the ProtoPilot Server and OPC UA client are running and certificates are not revoked
	Connection cannot be established	Customer System is not connected or Proto-pilot server is not started.

		Ensure the ProtoPilot Server and OPC UA client are running and certificates are not revoked
	No valid Customer System or Software-key/ XO3D-HW-key certificate exists	No valid Customer System or Software-key/ XO3D-HW-key certificate exists. Ensure that certificates are not revoked or deleted.

Mobile OPC UA Server operation state:

Indicator State Example	Operation State	Description
 JMobile OPC UA Server is running	JMobile OPC UA Server is running	Correct operation state.

ProtoPilot_agent operation states:

Indicator State Example	Operation State	Description
 ProtoPilot_agent is running	ProtoPilot_agent is running	Correct operation state.
	ProtoPilot_agent is not running. Try to restart the Gateway.	ProtoPilot_agent is not running. Try to restart the Gateway.

ProtoPilot Server operation states:

Indicator State Example	Operation State	Description
 ProtoPilot Server is running	ProtoPilot Server is running	Correct operation state.
	ProtoPilot Server not running. Start ProtoPilot Server on Customer System.	ProtoPilot Server not running or reachable. Start ProtoPilot Server on Customer System.

XO3D-HW-key Certificate states:

Indicator State Example	Operation State	Description
 XO3D-HW-key certificate is valid	XO3D-HW-key Certificate is valid	Correct operation state.
	XO3D-HW-key Certificate is revoked	XO3D-HW-key Certificate is revoked

	XO3D-HW-key Certificate is invalid or unknown	XO3D-HW-key Certificate is invalid or unknown
--	---	---

Software-key Certificate states:

Indicator State Example	Operation State	Description
 Software-key certificate is valid	Software-key Certificate is valid	Correct operation state.
	Software-key Certificate is revoked	Software-key Certificate is revoked
	Software-key Certificate is invalid or unknown	Software-key Certificate is invalid or unknown

3.6 Customer System (PC) Demo Page

On the Customer System Side JMobile Runtime application, you can see the status of the demo from the Customer System perspective on the Demo Page. Click on the “Demo Page” icon with the bar graph to go to the Demo Page. The view changes depending on the status of a variety of variables.

3.6.1 Example Customer System Demo Page Views

The following sections show two common statuses that you may see while using the Cyber Resilience Reference Kit Demo.

3.6.1.1 Hardware-protected Secure Connection

Figure 27 shows the Reference Kit fully trusted ProtoPilot configuration with all three certificates valid and all demo applications started as described in the first row of Table 3.

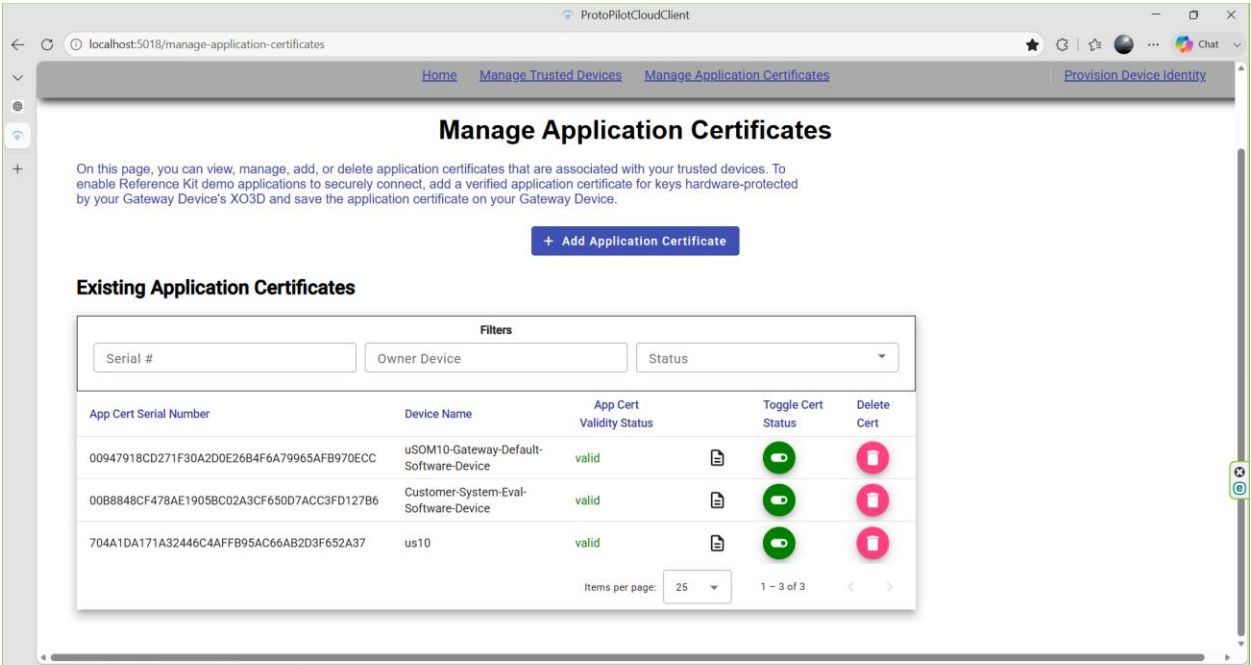


Figure 27 – Application Certificates Configuration

In this scenario, when you click on the “Demo Page” graphic with the bar graph icon on the left hand side of the PC JMobile Runtime application, you should see a graphical view of the connections to the Gateway as in Figure 28:

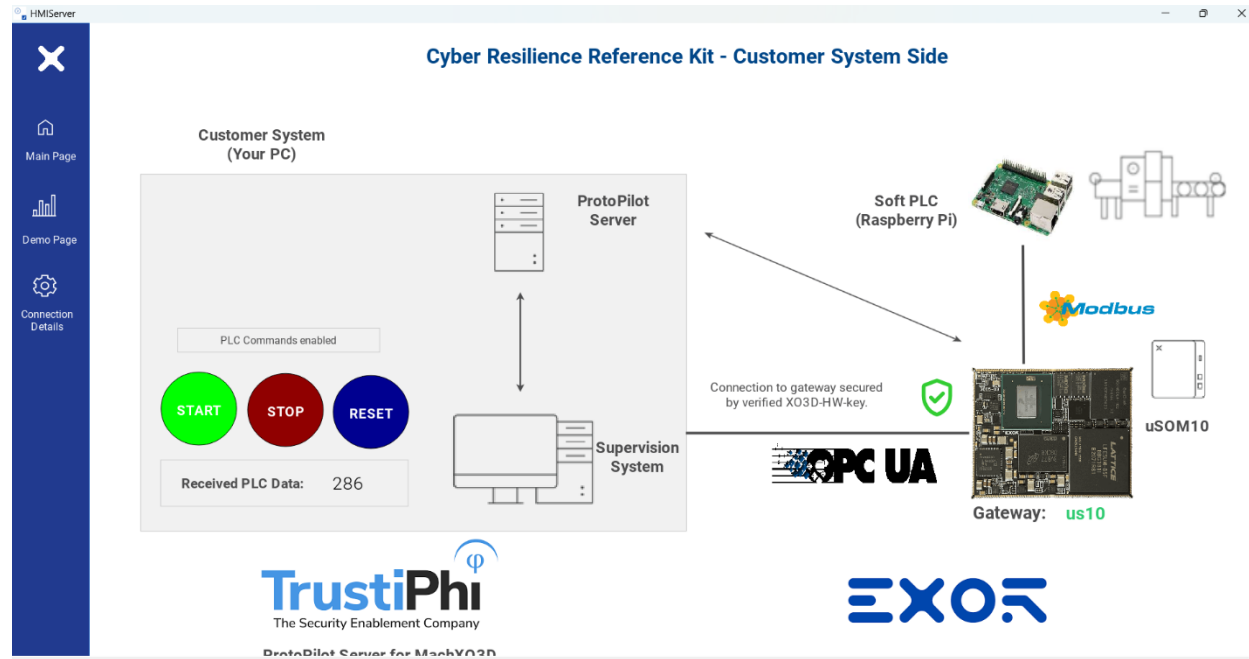


Figure 28 – Example of Demo Page on Customer System

3.6.1.2 Software-Protected Bootstrap Connection

You can use the ProtoPilot UI to quickly modify the validity status of the application certificates. If you revoke the hardware-protected application key by clicking on the toggle button in the correct row, you should see a status as in Figure 29.

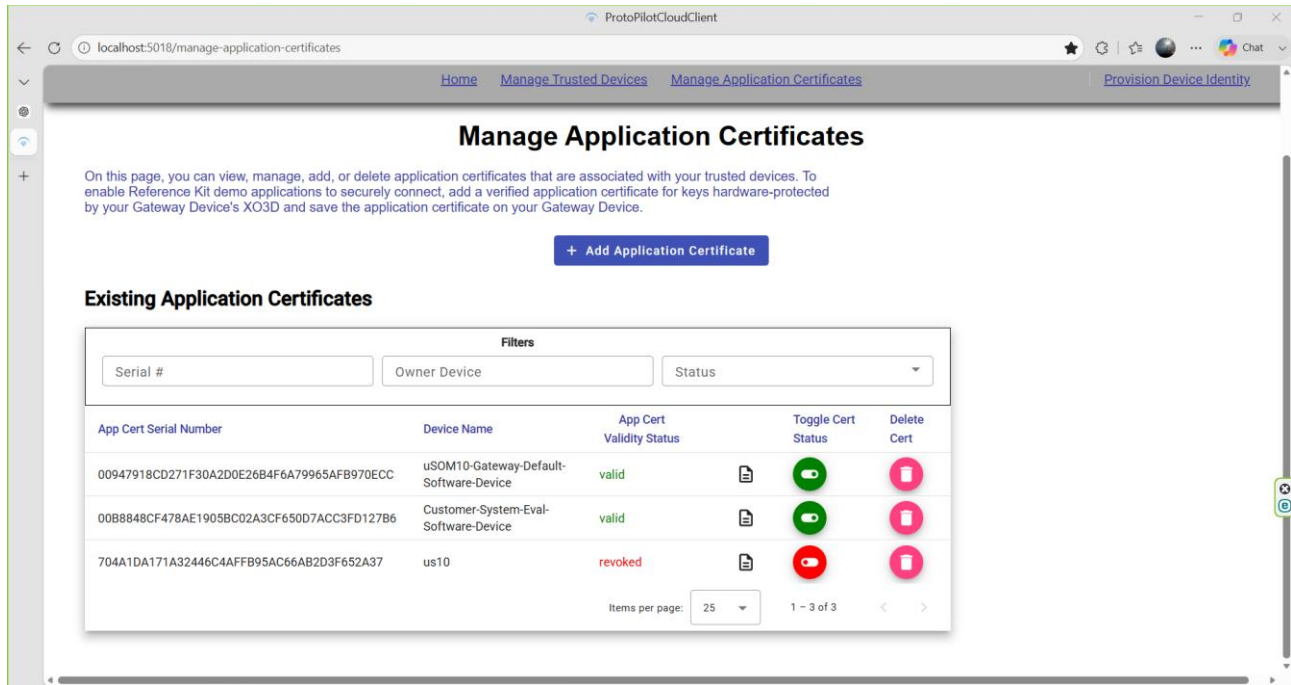


Figure 29 – Revoked Application Certificate example

In this scenario, when you click on the “Demo Page” graphic with the bar graph icon on the left hand side of the Customer System Side JMobile Runtime application, you should see a graphical view of a bootstrap connection using the software certificate as in Figure 30.

When the XO3D-HW-key certificate is revoked, the system automatically falls back to the Software-key certificate. In this case, the Customer System can still establish a secure connection and read the initial value of the PLC counter at the moment the connection is established. However, real-time updates are no longer available, and the Customer System is not authorized to send PLC control commands. As a result, the Start, Stop, and Reset functions are disabled, and the displayed counter value remains unchanged after the connection is established. This demonstrates that full monitoring and machine control are available only to systems authenticated with a valid XO3D-HW-key certificate.

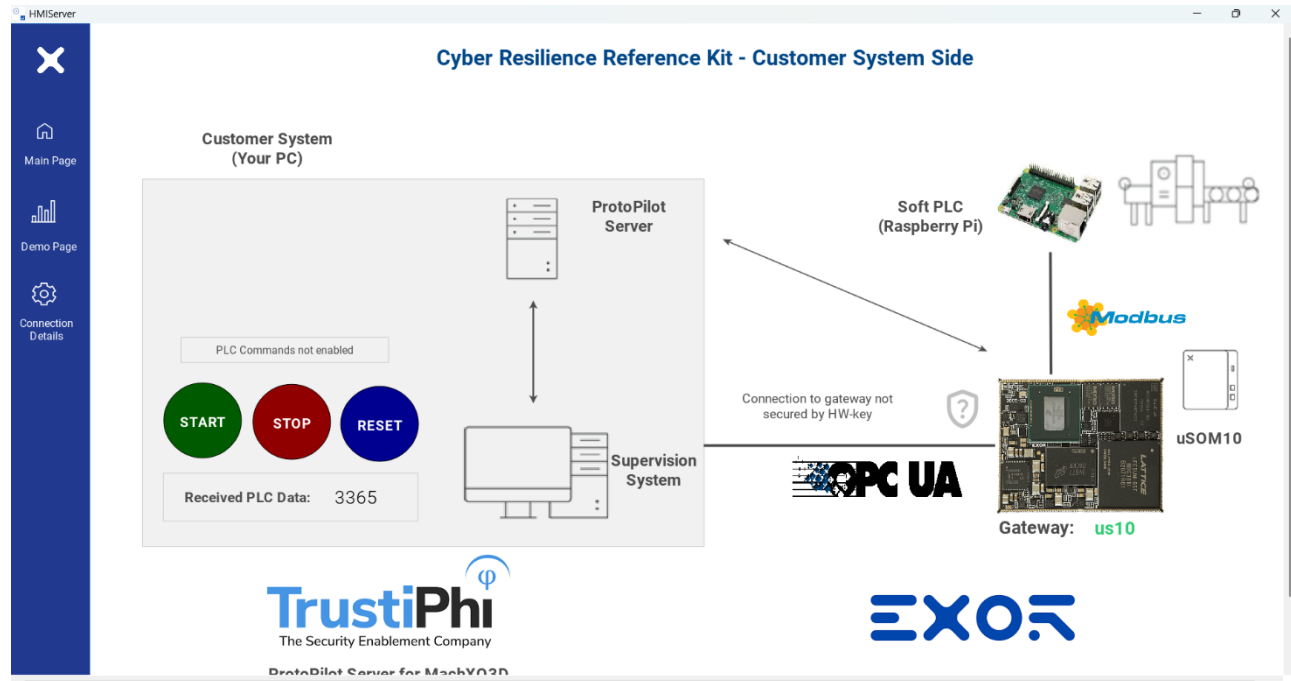


Figure 30 – Demo Page with revoked Application Certificate

3.6.2 Customer System Side Demo Page Status for Connection to Gateway

The connection text shown on the line between **Customer System (Your PC)** and the **Gateway** indicates the status of the connection:

Operation State	Description
Connection to gateway secured by verified XO3D-HW-key Certificate.	Correct operation state if XO3D-HW-key Certificate exists and is not revoked.
Connection to gateway secured by Software-key Certificate.	“Bootstrap” connection state if XO3D-HW-key Certificate doesn’t exist or is revoked.
No connection to gateway.	ProtoPilot server is not running or Customer System is not physically connected to Gateway.
Connection cannot be established. One or more certificates may be revoked.	Some needed Certificate is revoked by Reference Kit UI
No valid certificate exists.	Neither Customer System or Software-key/ XO3D-HW-key certificate exists.

3.6.3 Customer System Side Demo Page PLC Data Management

After hardware trust has been successfully established, the Received PLC Data counter displayed on the JMobile OPC UA Client (running on the Customer System) begins updating with live values from the XPLC

using Modbus industrial communication protocol. The counter represents an internal machine control logic variable within the PLC. The Gateway reads this variable from the PLC and makes it available to the Customer System through an encrypted communication channel. This communication is enabled only after mutual authentication using a valid XO3D-HW-key certificate, ensuring that PLC data is accessible exclusively by authenticated and trusted hardware.

This Demo Page in Figure 28 also demonstrates secure machine control through the PLC Start, Stop, and Reset commands. Once the authenticated and encrypted communication channel has been established using a valid XO3D-HW-key certificate, the Customer System can securely send control commands to the PLC. Pressing Start begins the counter, Stop pauses it, and Reset clears the counter to zero, demonstrating bidirectional, trusted communication between the Customer System and the XPLC.

Note that when managing the PLC counter on the Customer System, you can also view the counter modifications on the Gateway Side Demo Page (see section 3.4.4). On the JMobile OPC UA Server running on the Gateway, you can observe that after a Stop or Reset command is issued, the displayed PLC counter reflects the resulting state of the counter in the PLC. To demonstrate that the PLC and its control logic remain operational after these commands, a separate PLC Keep-alive counter from the XPLC is also displayed. Unlike the main PLC counter, the PLC Keep-alive counter continues running continuously and is not affected by the Start, Stop, or Reset commands. This confirms that the PLC and Gateway remain connected and that the machine control logic is still active even when the main counter has been stopped or reset.

3.7 Customer System (PC) Connection Details

On the PC side, the Connection Details provides the following information as shown in the example screen shot in Figure 31.

- Gateway IP Address (fixed at 172.27.75.99)
- My IP Addresses – This displays all of the network adapters and associated IP addresses on your PC. The contents are unique to your system. You should verify that there is an adapter with the IP address 172.27.75.100. This corresponds to the network on which the Gateway and your PC are connected. If this address is not present, verify that the board is powered on and connected to your PC via Ethernet.

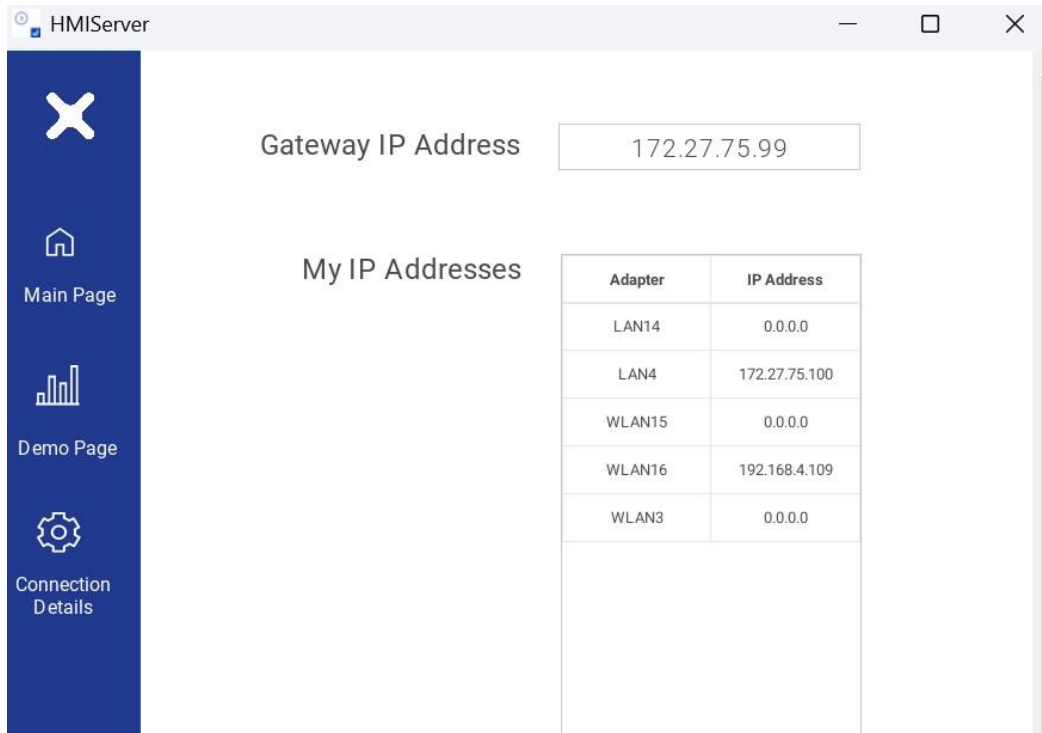


Figure 31 - Example PC Connection Details with Ethernet Connection to Gateway

4 Demo and Device Reset

If you would like to start the demonstration over from the beginning, there are two independent demo components that may be managed. The components that retain state are:

- The XO3D Root of Trust on the Gateway Device
- The ProtoPilot Server

You can use the ProtoPilot UI to manage/reset these components in a single flow.

4.1 Factory Reset of XO3D

The XO3D may be reset using either of two mechanisms.

You can reflash the XO3D following the process described in Section 5. This will remove and reset all data of the XO3D firmware.

Alternatively, you can reset the XO3D Root of Trust using TrustiPhi ProtoPilot by doing the following:

- On the “Manage Authorized Devices” page, expand the Advanced menu at the bottom and select the “**Factory Reset Options**”

- Select **“Yes, continue”**
- Make sure that your device is listed with the correct IP address (the device will be present if registered with ProtoPilot) and the checkbox for your device is selected
- If your device is not listed, click **+ reset an unregistered device** and enter the IP address (172.27.75.99) and port (7255) of your Gateway Device.
- Make sure the Gateway Device is powered on and connected to your PC and click **“Reset selected devices”**
- Click **“Yes, perform reset”**

ProtoPilot will report the results of the reset process at the bottom of the window (see Figure 32). On success, all keys will be deleted from the XO3D RoT and the Gateway Device and any certificates that were created for the Gateway Device will be removed from the ProtoPilot database.

If desired, you can continue with a reset of the ProtoPilot server or close the window.

NOTE: In order to ensure the state of Exor JMobile Runtime PC is properly updated after XO3D deletion, you may need to restart the application on the PC.

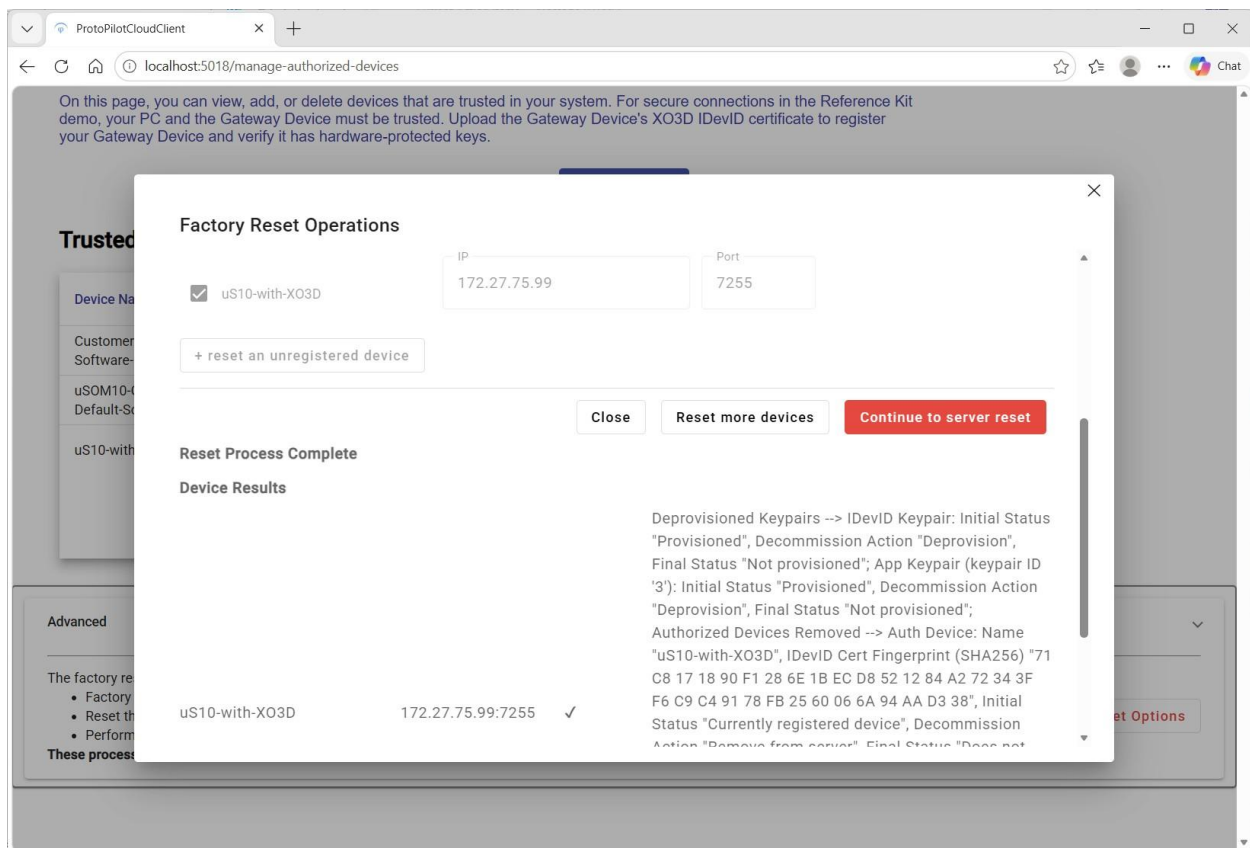


Figure 32 - Factory Reset of XO3D Root of Trust Using TrustiPhi ProtoPilot

4.2 Factory Reset of ProtoPilot Database

To reset the ProtoPilot database to remove all added devices and certificates and to restore the default demo software devices and certificates, perform the following steps:

- On the “Manage Authorized Devices” page, expand the Advanced menu at the bottom and select the “**Factory Reset Options**”
- Select “**Yes, continue**”
- If desired, factory reset the XO3D RoT as described in Section 4.1 and then click “**Continue to server reset**” or simply click “**Skip device reset**”
- Select “**Reset Trusted Device database only**”
- Click “**Reset Server**”
- Click “**Yes, perform reset**”

Upon successful completion of the above process, you should see the results in the window as in Figure 33.

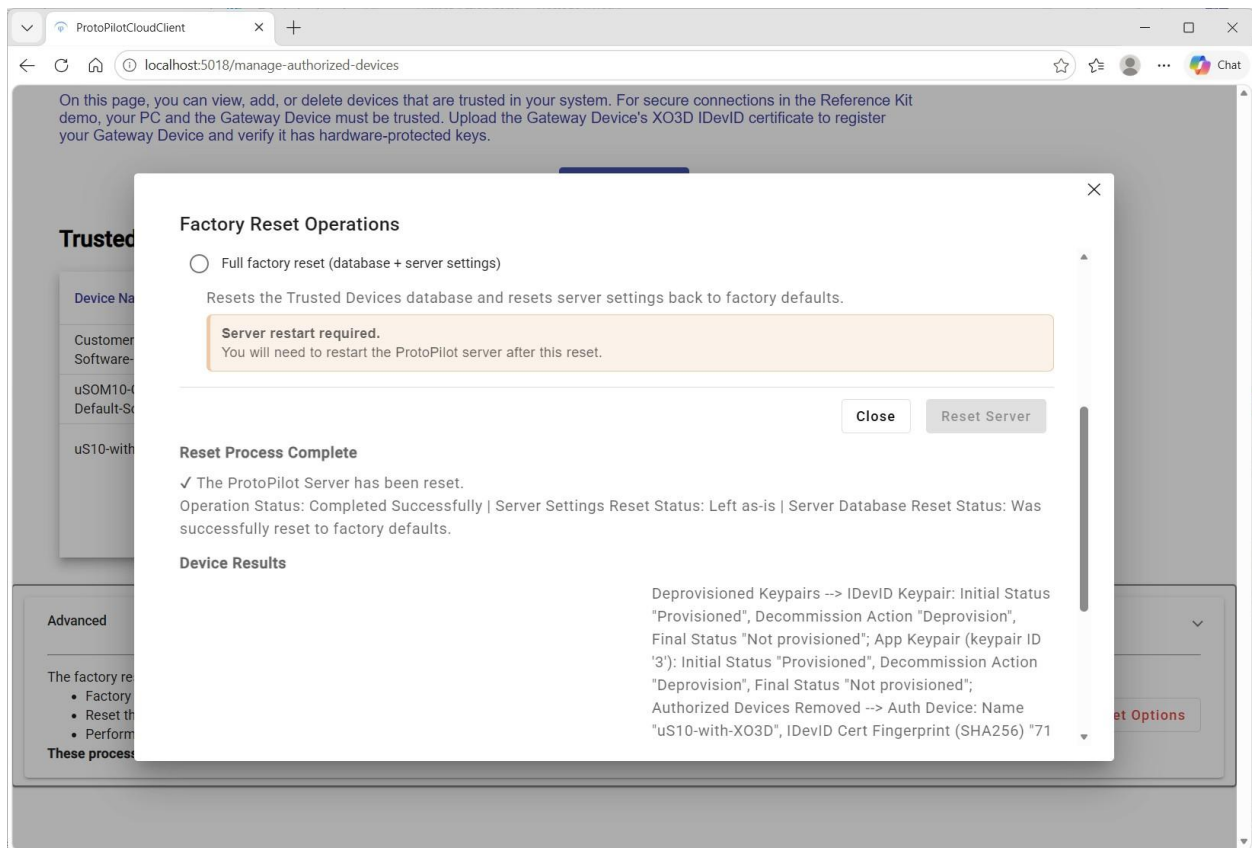


Figure 33 - Successful ProtoPilot Server Factory Reset After XO3D Reset

5 Programming the MachXO3D Bitstream

The MachXO3D bitstream is programmed using Lattice Diamond Programmer v3.13.0.56.2 via the JTAG interface (J21) on the EXOR uS10 board. The J21 header is arranged in two columns of five pins — when oriented from the corner of the board, the column closest to the board edge contains pins 1, 3, 5, 7, and 9, while the column further from the edge contains pins 2, 4, 6, 8, and 10.

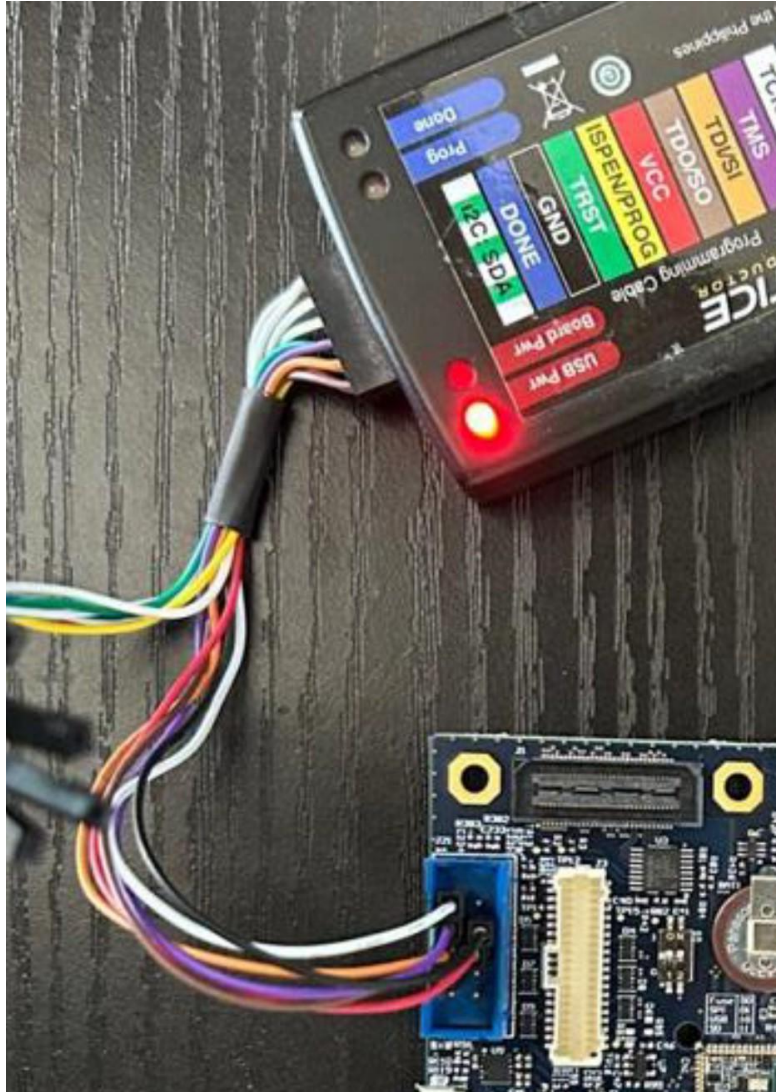


Figure 34 - Wiring for Programming the MachXO3D FPGA

To begin programming, connect the Lattice 2B programming cable to the J21 JTAG interface and wire the cable according to the pin assignment table below.

Table 4 - MachXO3D FPGA Programming Pin Configuration

uS10 J21 Header Pins	JTAG Signal Name
1	TCK
3	TMS
4	GND
5	TDI
6	VCC
7	TDO

To program the MachXO3D firmware, follow these steps:

1. Launch Diamond Programmer.
2. Detect the device.
3. Untick the ECP5 device from the device list.
4. Right click on the MachXO3D device and select “Device Properties”
5. In the Device Properties window, set Operation to "FLASH CFG Erase, Program, Verify".
6. Ensure the "CFG0 Programming Options" is checked.
7. Select the bitstream with the .jed extension.

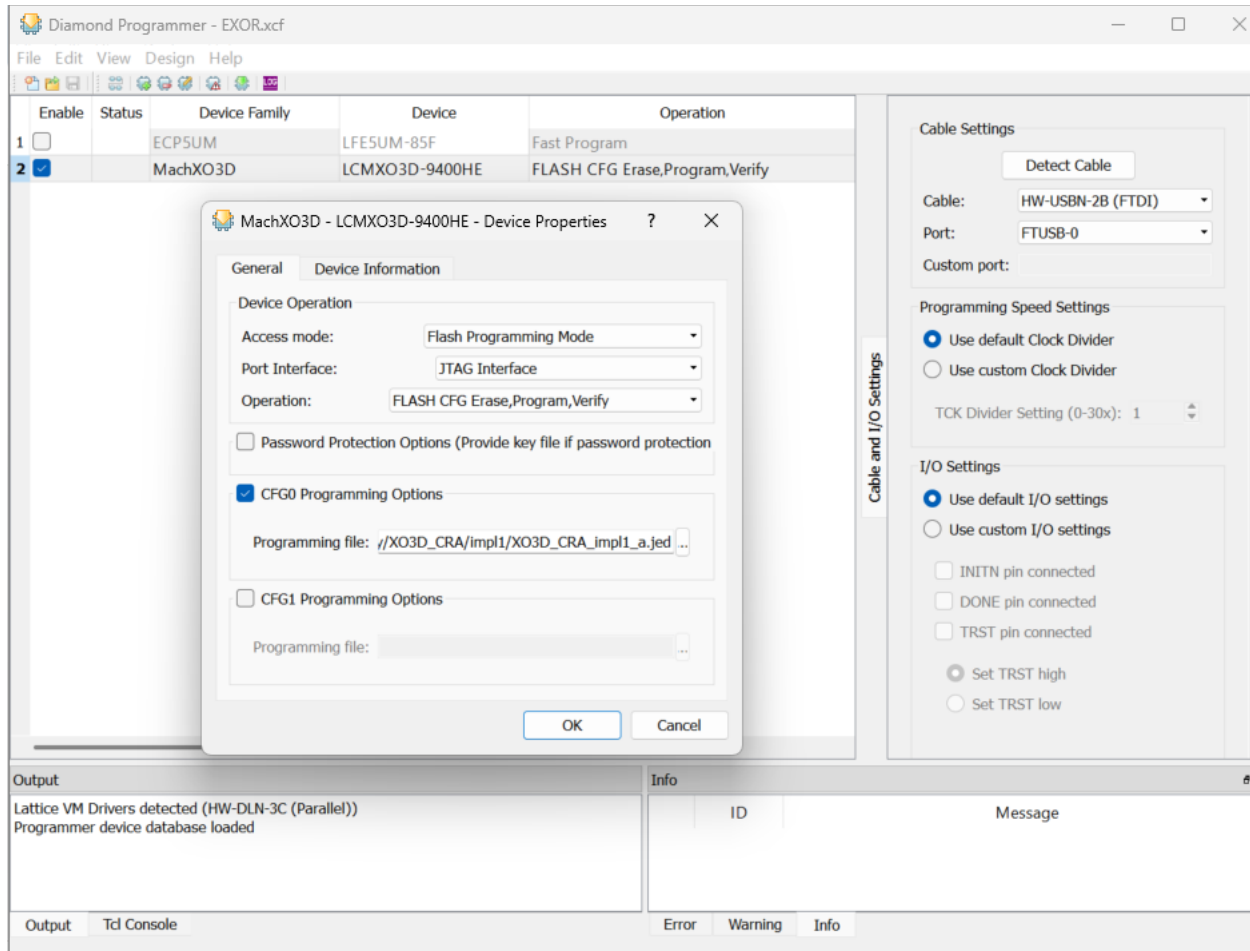


Figure 35 - Programming MachXO3D bitstream

8. Click the Program button – identified by a downward-pointing green arrow – located in the top menu bar.

6 Connecting MachXO3D UART connection

The MachXO3D UART interface can be connected to a host PC via the J19 header on the uS10 board and an external USB-to-UART module. This connection is particularly useful when debugging applications running on the MachXO3D design.

Wire the connections according to the pin assignment table below.

Table 5 - MachXO3D UART Connection PIN Configuration

uS10 J19 Header Pins	Signal Name	USB-to-UART module
2	GND	GND
3	UART TX	RXD
5	UART RX	TXD

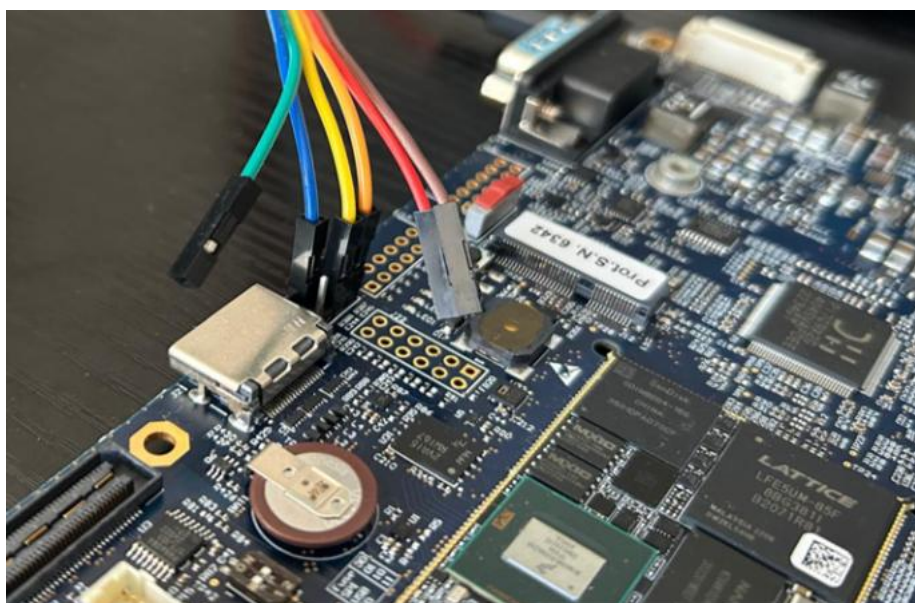


Figure 36 - MachXO3D UART Connection on EXOR uS10 board

7 Reference Documents

- [1] Lattice Press Release Announcing the Cyber Resilience Reference Kit - <https://www.latticesemi.com/en/About/Newsroom/PressReleases/2026/Lattice-Launches-Joint-Cyber-Resilience-Reference-Kit-with-EXOR-International-and-TrustiPhi>
- [2] EXOR International Blog on the Cyber Resilience Reference Kit - <https://www.exorint.com/exor-innovation-blog/designing-cyber-resilience-at-the-hardware-edge>
- [3] Cyber Resilience Reference Kit Demo Video - <https://www.latticesemi.com/en/Solutions/Lattice-FPGA-Security-Solutions#5350D17DDC4D4F108478D5BC47027F47::~:~:text=Lattice%20Cyber%20Resilience%3A%20Reference%20Kit%20Automate%20Protection%20and%20Recovery>
- [4] TrustiPhi ProtoPilot - <https://trustiphi.com/platform/protopilot/>

- [5] JMobile Suite: <https://doc.exorint.net/jmobile/v4.05.02/en/index.html>
- [6] LogicLab: <https://www.axelsoftware.it/en/logiclab/>