



Verifyfaces
PERCEPT Gateway Solution

Integration Guide

Document Date: February 5, 2026

1 Introduction

This technical note describes the high-level steps required to activate the Verifyfaces integration on an IONODES PERCEPT Gateway.

The intent of this document is to outline the integration workflow without duplicating configuration procedures that are already covered in existing product documentation. Verifyfaces maintains its own installation and onboarding documentation, and IONODES provides detailed manuals for the PERCEPT Gateway Solution. Those references should be consulted as needed, as they may evolve independently over time.

This document focuses specifically on enabling the Verifyfaces integration once all prerequisite components are already in place.

2 Assumptions and Prerequisites

This technical note assumes the following conditions are already met:

- A PERCEPT Gateway is physically installed, powered on, and operational
- The PERCEPT Gateway is fully configured and accessible via its web interface
- Administrative access to the PERCEPT Gateway is available
- The PERCEPT Gateway has a stable internet connection (non-LTE connection recommended for initial setup)
- All required Verifyfaces accounts, licenses, and registrations have been completed and are accessible
- The customer is familiar with both the PERCEPT Gateway interface and the Verifyfaces platform

No steps in this document replace or override official documentation provided by IONODES or Verifyfaces.

3 Overview of the Integration

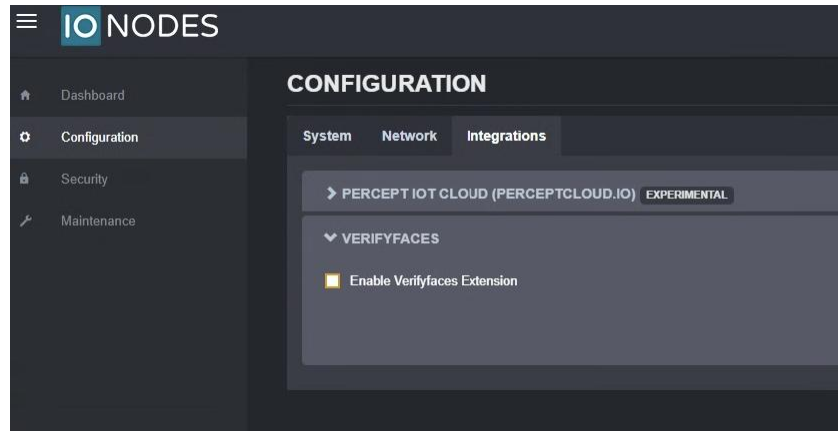
The Verifyfaces integration on the PERCEPT Gateway runs as an embedded virtualized service. Once enabled, the PERCEPT Gateway automatically initializes the Verifyfaces environment, and retrieves required components.

During this process, the PERCEPT Gateway will:

- Launch the Verifyfaces virtual machine (VM)
- Download and apply Verifyfaces updates
- Generate a unique Verifyfaces Device ID (also referred to as the FMU ID)

4 Enabling the Verifyfaces Integration

1. Log in to the PERCEPT Gateway web interface using an administrator account.
2. Navigate to Configuration → Integrations → Verifyfaces.



3. Enable the option labeled “Enable Verifyfaces Extension”.
4. Save or apply the configuration change.

Once enabled, the PERCEPT Gateway will automatically begin initializing the Verifyfaces environment.

5 System Behavior During Initialization

After activation, the following behavior is expected:

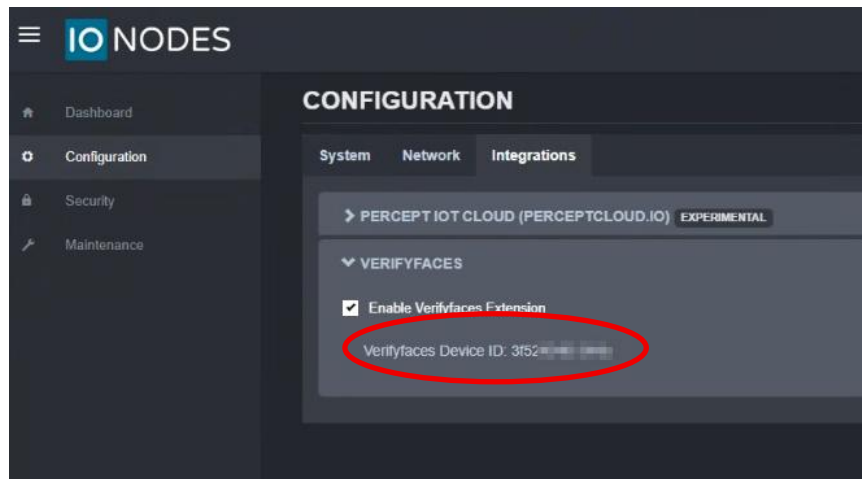
- The Verifyfaces VM will start automatically
- The PERCEPT Gateway will begin downloading Verifyfaces components and updates
- Network usage may be significant during this phase (downloads can be multiple gigabytes) and a noticeable increase in memory usage will occur while the VM is running

This process may take some time depending on network conditions and system resources.

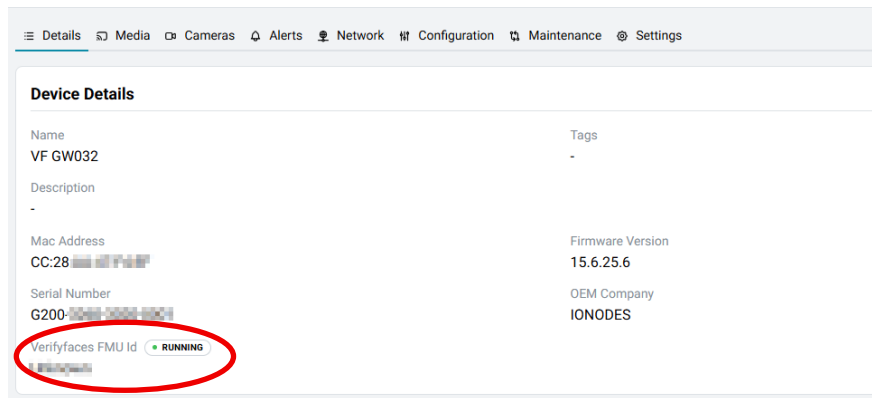
6 Verifyfaces Device ID (FMU ID)

Once initialization and updates are complete, the Verifyfaces Device ID will appear:

- On the Verifyfaces integration page within the PERCEPT Gateway web interface



- In PERCEPT Cloud device details, if the gateway is cloud-connected



7 Validation and Next Steps

After the Device ID (FMU) is visible:

- Confirm the ID matches between the gateway and PERCEPT Cloud (if applicable)
- Complete any remaining steps within the Verifyfaces platform to Register your FMU ID
- Refer to Verifyfaces documentation for analytics and usage

At this point, the Verifyfaces integration is enabled and ready for use.

8 Support

For PERCEPT Gateway assistance, contact IONODES Support by emailing support@ionodes.com.

For Verifyfaces platform questions, consult Verifyfaces documentation or support channels.