GE VERNOVA

EDGE SOFTWARE & SERVICES

Secure Deployment Guide

GE VERNOVA

Proprietary Notice

Trademark Notices

We want to hear from you. If you have any comments, questions, or suggestions about our documentation, send them to the following email address:
doc@ge.com

Contents

Chapter 1. Secure Deployment Guide

Introduction

This section describes steps and considerations that end users of Predix Edge should be aware of to use the product in a safe and secure manner. As Predix Edge is an application platform and usage will vary situationally, this is not an exhaustive document, but provides guidance on some of the most important aspects of secure operation of the system.

Required Firewall Rules

A typical Predix Edge deployment involves connectivity to a variety of systems, including both assets at the customer location, and the Predix cloud environment where the corresponding Edge Manager instance is located. We recommend the application of a least-privilege based firewall policy within the installed environment to permit only required communications for typical operation. The Predix Edge virtual machine should be granted access to only those hosts required for their operation as a whitelist.

The table below lists the firewall rules required for Predix Edge. Note that only GE Digital-provided components and protocol adapters are listed, but firewall rules are required to be created only for the components used in the deployment. Additionally, either the customer or an approved third party may create custom adapters, which would likely require additional firewall rules. If this is the case, please consult with the application author to determine the requirements.

Table 1. Required Firewall Rules

Rule purpose	Direction	Protocol and Port
Edge device to Edge Manager	Outbound to External	HTTPS (TCP 443)
Cloud Gateway (to Predix Time-series)	Outbound to External	HTTPS/Web sockets (TCP 443)
Cloud Gateway (to Predix Event-Hub	Inbound from Management	HTTPS (TCP 443)
PETC	Inbound from Management	HTTPS (TCP 443)
Modbus	Outbound to Control	TCP 502
OPC-UA	Outbound to Control	TCP 4840
OSI Pi	Outbound to Control	HTTPS (TCP 443)

Table 1. Required Firewall Rules (continued)

Rule purpose	Direction	Protocol and Port
EGD	Inbound and Outbound from/to Control	UDP 18246
MQTT	Outbound to Control	TCP 1883
MQTT over WebSockets	Outbound to Control	HTTPS/WebSockets (TCP 9001)
SNMP monitoring of the Edge device	Inbound from Control or External	UDP 161
NTP (if using external)	Outbound to External	UDP 123

Note:

- The “control” network refers to the local assets the Predix Edge device connects to; “external” is the path to the open Internet.The “management” network is ideally a local management network used for site administration functions, if available. If unavailable, please default to whatever network is considered most secure/restricted.
- EGD typically makes heavy use of multicast and broadcast traffic.
- All of the above mentioned port numbers are considered standard IANA assigned port numbers, however deployments may often use different port numbers due to operational considerations. Consult with a network engineer familiar with the site network if you are unsure.

When possible, we also recommend further restricting firewall rules for specific ports to required hosts only. For example, the Modbus rule should be further refined to allow the Edge device to communicate on port 502 to only those devices with which it is intended to communicate. In addition there are several IPS/IDS options available to restrict control network traffic via segmentation and inspection, such as GE Digital's OpShield.

NTP Server Configuration

By default, the system is configured to use the following four servers for NTP:

- 0.pool.ntp.org
- 1.pool.ntp.org

- 2.pool.ntp.org
- 3.pool.ntp.org

Accurate time is required for the device to properly communicate with Edge Manager, for accurate logs, and for various other system behaviors to work as intended. If you are not able, or do not want, to use a public NTP server, please configure the device with time servers of your choosing. See Configuring the Network Time Service *(on page)*.

Managing Access to Predix Edge Technician Console

First logging into the Predix Edge Technician Console (PETC) is a requirement to perform device setup and enrolment. It also has an important security outcome, as until this point the device will have an insecure default username and password.

- user: admin
- password: admin

Upon first login, the user will be prompted to reset this to a new strong password. We recommend following general password hygiene practices when doing so. This includes using hard-to-guess passwords, and not reusing passwords from other accounts.

See the instructions for the first login to PETC *(on page)*.

We also recommend each person have their own account, rather than sharing credentials for a single account among multiple people. It is also good practice to promptly disable or remove users who have departed the organization. See the instructions for managing users within PETC *(on page)*.

Device Enrolment Best Practices

The following are considerations when adding enrolment information *(on page)* for a new Edge device.

- Be descriptive when selecting Device IDs and use optional fields such as Group or Description when possible. This information may assist you later in triaging issues (security or maintenance) as they arise.
- When defining a shared secret, avoid simple or reused secrets. Although this secret is used only at the time of enrolment, using unique and complex secrets will minimize the chance of an attacker

being able to impersonate a device after it is added to an Edge Manager instance, but before enrolment is completed. This is particularly important when performing bulk enrolment operations via the device list import *(on page)*.

Monitor Your System

Consult the PETC instructions for using journal-based logging *(on page)* or the equivalent page for collecting logs from Edge Manager *(on page)*.

It is recommended you set up your Edge appliance to publish system statistics via SNMP. See Configuring SNMP *(on page)*.

Predix Edge Virtual Machine Appliance

VMware ESXi and vSphere Hardening and Patch Management

The currently supported production platform for Predix Edge virtual machines is VMware vSphere/ESXi 6.5 and 6.7. As with any software platform, we recommend keeping your deployment up to date with the latest updates from VMware, in accordance with an overall vulnerability management process.

We recommend following the steps in the VMware hardening guides.

Production and Development VM Images

Two variants of the virtual machine image are available: production and development. Only the production image should ever be used in production/deployment scenarios.

There are several features that differ between the two images that are optimized for security (for production) or ease of use (for development).

Though not an exhaustive list, some important differences include:

- Production images require all Predix Edge applications to contain a valid signature, whereas development images do not enforce application signatures, allowing potentially malicious applications to be run.
- Production images have SSH disabled, whereas development images allow logging into the system with the insecure account (user: root/password: root) in addition to the developer RSA key pair.

Predix Edge Gateway 3002

Default Network Settings

As described in the product overview *(on page)*, this device is equipped with two ethernet ports. Please note the default settings for each port, LAN1 is PoE and defaults to a static IP of 192.168.100.2, and LAN2 is DHCP by default. The Predix Edge Technician Console (PETC) is available only via LAN1.

The intended use of each port can be described in terms of LAN and WAN, Purdue Levels, etc., but the idea is that LAN1 is placed on the more restrictive network to segregate access to PETC as much as is possible.

Outbound traffic will be routed to the appropriate outbound physical port, but should also be taken into consideration when creating firewall/IDS/ACL rules.

Physical Security

Note that physical access to a Predix Edge Gateway may allow an attacker to bypass some or all security controls. Please ensure that the environment the device operates in is sufficiently secured from intruders, as is appropriate to the situation.

Unsupported IO Devices

Note: The following hardware IO are not supported:

- Bluetooth
- ZigBee
- WiFi
- CANBus
- MicroSD storage
- USB peripherals, including mass storage devices

Edge Agent for Ubuntu

Edge Agent for Ubuntu has considerable flexibility as compared to the Predix Edge Gateway 3002 and the VM Appliance. With this flexibility are additional responsibilities for maintaining a secure system. A comprehensive guide to these are beyond the scope that can be covered here, however, the following are some key points to consider.

Note:

To install Edge Agent for Ubuntu, see Installation *(on page)*.

Differences From Other Edge Devices

- The Predix Edge Technician Console (PETC) is not supported on Ubuntu, and as such, advice related to PETC is not applicable to this system. This also means the internal API that drives PETC is not present.
- SNMP is not installed as a dependency of Edge Agent for Ubuntu. It is recommended that another performance monitoring solution be added.
- Edge Agent for Ubuntu does not benefit from any of the log management improvements added to Edge OS through journald and syslog. It is recommended to add a log streaming/management capability to the system, either through Edge Manager Custom Commands (with System Builder Commands), or some other third-party tool.
- There is no hard distinction between Production and Development images as there is for the VM. Code signing is enabled by default, but can be disabled for development purposes by editing `/etc/edge-agent/agent-data.json` and changing `"enforce_signing":true` to `false`. It is highly recommended that code signing be left on in any production setting. Refer to the Application Signing *(on page)* instructions for more information on getting an Edge Application signed by GE Digital.

Restricting Access to Docker the Edge Agent User

Access to `eauser`, the user that the Edge Agent runs as, should be highly restricted. This is because `eauser` is highly privileged (effectively root). Similarly any user with access to running docker should be understood to be highly privileged as this will allow the user to not just impact the availability/integrity of Edge applications, but of the system as a whole.

It is recommend as much of your device administration as possible be performed through Edge Manager, and only using CLI level access to Edge Agent as a last resort to minimize this risk. This goes hand in hand with having good user management practices in general, to avoid unintended access to support/admin accounts.

Building a Minimal System

Edge Agent for Ubuntu will install a minimal set of dependencies, and is able to remotely deploy additional software via `apt`. However it is good practice to reduce the amount of software installed to the system in general. Each additional software package brings not just its own set of risks to the system, but also those inherited from its full dependency tree. In particular, caution should be exercised when adding new network listening code, or anything that elevates privileges.

There is often a wide variety of tools on Linux for any given job. Selecting the right one can be hard, but when in doubt, favor software that is well vetted, minimal to the required task, and still actively supported by the vendor.

It is also worth recommending that any software that does not need access to the root system could instead be turned into an Edge Application. This allows the application to benefit from all of the security boundaries built into the Edge Application framework, such as chroot, apparmor, seccomp, and code signing.

Monitoring for Updates

Unlike other Edge platforms, the onus is on the user to maintaining an up-to-date system. It is important to stay informed of not just security updates from GE Digital, but also Ubuntu, and any other third-party software you add to the system.

It is recommended to subscribe to receive the latest security updates directly from Ubuntu.

Additional Resources For Ubuntu Security

- Ubuntu provides a cross version matrix of security features. Each feature comes with an explanation and information for digging deeper into that topic, which is useful for designing an approach to various aspects of the system, such as filesystem encryption or configuring a firewall.
- The United Kingdom's National Cyber Security Centre (NCSC) has released a hardening guide for Ubuntu that covers topics in greater depth.

Other Platforms

Predix Embedded System Developers or Custom Devices

The Predix Edge stack is available to be licensed, integrated, and modified to fit the use case of other businesses. If you are using such a device, please consult with the producer of that custom device, as this information may be incorrect or incomplete.

VMware Fusion and Workstation

VMware Fusion and Workstation are excellent choices for a convenient, laptop friendly development solution for developing Predix Edge applications. However, they are not suitable for real-world production use, and as such, are not in scope of this document.

Raspberry Pi

The Raspberry Pi image provided by GE Digital is infrequently updated and not suitable for use as a production system. The image is intended to be used only for prototyping, learning, and demonstration purposes.