Oracle Utilities Live Energy Connect

Security Guide

Release 25.12.0.0.0
G49425-03
January 2025

ORACLE

Oracle Utilities Live Energy Connect Security Guide, Release 25.12.0.0.0

G49425-03

Contents

1

Getting Started

Introduction to the Oracle Utilities Live Energy Connect V25.12.0.0.0 Security Guide.

Welcome to the Oracle Utilities Live Energy Connect V25.12.0.0.0 Security Guide. This security guide provides an overview of the Oracle Utilities Live Energy Connect (LEC) V25.12.0.0.0 security process and covers the following:

- Establishing machine-level roles and security policies limiting access to the system on which LEC is deployed.
- Setting appropriate firewall rules to limit security vulnerabilities.
- Specific protocol security measures.

Audience

This guide is intended for system, network, and security administrators tasked with installing, configuring, and maintaining Oracle Utilities Live Energy Connect.

It covers the following topics:

- Installing system prerequisites and the Oracle Utilities Live Energy Connect software.
- Setting appropriate firewall rules to limit security vulnerabilities.
- Specific protocol security measures.

Prerequisites

Oracle Linux 9 (OL9) must be installed on the target host prior to installing Oracle Utilities Live Energy Connect. An additional dependency, the Oracle Cloud Native Environment (OCNE) framework, must be downloaded and installed separately to the host system.

It is strongly recommended that the OL9 operating system be installed with a security profile such as NIST 800-171 and that OpenSCAP be used periodically to confirm security compliance for the host system.

Oracle Utilities Live Energy Connect will typically be deployed to on-premises systems that are air-gapped, with no direct public network access. Procedures should be in place to push critical updates and patches of OL9 and OCNE to production systems in a timely fashion.

> **Note**
>
> See the Oracle Linux documentation on Oracle Help Center for details.

2

Protocol-Specific Considerations

The following sections describe the protocol-specific considerations for Oracle Utilities Live Energy Connect (LEC) V25.12.0.0.0.

ICCP

The ICCP protocol (IEC 60870-6/TASE.2) is based on MMS (ISO 9506) and allows for client and server roles. ICCP and MMS allow for TCP/IP connections to be inbound, outbound, or both, irrespective of the client/server role. The default MMS IP port is 102.

When LEC is configured for an ICCP VCC accepting an inbound association (connection), the LEC cluster node is automatically configured to allow inbound connections from the cluster node host machine's LAN interface to the internal Kubernetes ICCP/VCC pod, on the configured port.

MMS TCP/IP port 102 connections and traffic must be allowed between the LEC system and any configured ICCP peers, based on the connection inbound/outbound configurations.

DNP3

DNP3 (IEEE 1815) is a protocol that uses TCP/IP as a transport layer. Running as a DNP3 "Master" (or client), LEC will make outbound TCP/IP connections to configured "Outstation", RTU, IED, or other DNP3-enabled devices..

DNP3 is an unsecured protocol that offers no encryption nor authentication, and therefore must only be enabled for use on a secure operating network. DNP3 also uses configurable IP ports. TCP/IP connections and traffic must be allowed between the Server machine and any configured DNP3 master/outstation (client/server) peers based on connection inbound/ outbound configurations.

2030.5/CSIP

2030.5/CSIP is a REST-based networking protocol for transmitting control messages to and status messages from aggregators and other systems important to renewable power generation. The Oracle Utilities Live Energy Connect cluster supports a containerized implementation of a 2030.5 server. For secure operation, a NGINX web server is installed on the Oracle Utilities Live Energy Connect V25.12.0.0.0 host machine and configured as a HTTPS reverse proxy to the 2030.5 server running inside the Oracle Utilities Live Energy Connect cluster. Current standards for HTTPS security, certificate key length, and other relevant standards should be followed.

3
General Operational Considerations

The following sections describe the operational considerations when deploying Oracle Utilities Live Energy Connect V25.12.0.0.0.

Oracle Utilities Live Energy Connect V25.12.0.0.0 is a microservices-based server application that is deployed in a Kubernetes cluster to host systems running Oracle Linux 9 (OL9) and Oracle Cloud Native Environment (OCNE). Upon initial installation, the Oracle Utilities Live Energy Connect cluster runs in a default mode, with a single configuration pod and no networking pods installed. As pods supporting network protocol interfaces are installed in the cluster, various protocol-specific IP ports will need to be opened to support interfaces to remote devices and systems.

Customer network and security policies vary, but in general it is recommended that inbound and outbound network access to and from the Oracle Utilities Live Energy Connect cluster be limited to the specific ports required for enabled protocol functionality and be limited to specific peer IP addresses. Enforcement at the network level and the local machine firewall level is recommended.

4

Installing Oracle Utilities Live Energy Connect V25.12.0.0.0

This section describes Oracle Utilities Live Energy Connect V25.12.0.0.0 distribution and how it is installed.

Oracle Utilities Live Energy Connect V25.12.0.0.0 is distributed as a self-extracting `.run` file. The Oracle Utilities Live Energy Connect distribution includes bash scripting that manages the installation and configuration of the software on the host system. The bash installation scripts must be run as the root user. The script will apply appropriate access controls to installed and configured components using the least privilege principle. See the *Oracle Utilities Live Energy Connect V25.12.0.0.0 Installation Guide* for more information.