# Oracle Utilities Live Energy Connect Security Guide

F48850-04

Last Updated October 23, 2023

ORACLE

Oracle Utilities Live Energy Connect Security Guide

F49120-04

# Contents


Getting Started ..... 4
- Audience ..... 4
- Prerequisite Knowledge ..... 4
- Related Documents ..... 4
- Definitions ..... 4
- Conventions ..... 6

Machine-Level Access Control ..... 6
- Configuration Files ..... 7
- Script Files ..... 7
- Log Files ..... 7
- Certificates ..... 7
- General Firewall and Network Considerations ..... 8

Protocol-Specific Considerations ..... 8
- ICCP ..... 8
- Secure ICCP ..... 8
- OPC UA ..... 9
- DNP3 ..... 9
- REST ..... 10
- RTP/NMS ..... 10

# Getting Started

This security guide provides an overview of the Oracle Utilities Live Energy Connect (LEC) 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

The audience for this guide includes system, network, and security administrators who install and maintain Oracle Utilities Live Energy Connect (LEC).

## Prerequisite Knowledge

You must have administrative privileges on the host machine where you're installing or upgrading the software.

## Related Documents

For more information about Oracle Utilities LEC, refer to the following Oracle resources:

- Oracle Utilities Live Energy Connect Release Notes
- Oracle Utilities Live Energy Connect Installation Guide
- Oracle Utilities Live Energy Connect Licensing Information User Manual
- Oracle Utilities Live Energy Connect Asset ID Manager User Guide
- Oracle Utilities Live Energy Connect Configuration Manager User Guide
- Oracle Utilities Live Energy Connect Certificate Deployment Procedure for Using Secure ICCP

## Definitions

The following are terms used throughout this security guide.

| Term | Definition |
|---|---|
| LEC | Oracle Utilities Live Energy Connect |
| LEC Server | Oracle Utilities Live Energy Connect Server |
| LCM | An acronym for LEC Configuration Manager, which is a GUI application used to configure and monitor the LEC Server |
| Data Directory | LEC runtime directory where configuration files, Python script files, and log files are located; the default location is **C:\Program-Data\LiveEnergyConnect**, which can be modified during installing LEC installation. |
| Install Directory | Primary software installation directory; the default location is **C:\Program Files\LiveEnergyConnect**, which can be modified during LEC installation. |
| Log Directory | A subdirectory of Data Directory named Logs |
| Config Directory | A subdirectory of Data Directory named Config |
| Scripts Directory | A subdirectory of Data Directory named Scripts |
| Stunnel Directory | Directory containing Stunnel program and configuration files located at **C:\Program Files (x86)\Stunnel** |

| Term | Definition |
| --- | --- |
| Service Account | Any account used to run LEC as a Windows services; the default service account is the Windows LocalSystem account |

## Conventions

The following are text conventions used throughout this security guide.

| Convention | Meaning |
| --- | --- |
| **Boldface** | **Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.** |
| *Italic* | *Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.* |
| `Monospace` | `Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.` |

# Machine-Level Access Control

The Oracle Utilities Live Energy Connect (LEC) Server runs in production as a Windows service. During installation, a single Windows service, Live Energy Connect LEC Server, is created and configured to run the Server with the default configuration. Additional Windows services may be created to run multiple LEC instances as Windows services on the same machine.

By default, Administrator access is required to alter, start, or stop Windows services should not be overridden. Any additional restrictions that allow the service to run automatically at system startup are allowed. It is recommended that all Oracle Utilities Live Energy Connect services run as the standard Windows LocalSystem account user unless another account is required for a specific purpose. For example, Native Windows Auth to an external system. It is the local system administrator's

responsibility to ensure that any other account used to run Oracle Utilities Live Energy Connect services has limited permissions.

## Configuration Files

The Oracle Utilities Live Energy Connect Server configurations are stored in SQLite (.db) files in the Data Directory. In addition, configuration batch files are stored in the Config Directory as JSON or CSV files (.csv or .json). By default, access to these files at the directory level is read-only for all non-Administrator users. To allow the configuration of the Server, read/write access to these files should be retained for Administrator users and not extended to other users.

Service Account users only require read access to configuration files and should not be allowed write access.

## Script Files

Python script (.py) files are located in the Scripts Directory. Access to these files is read-only at the directory level for all non-Administrator users. Read/write access should be maintained for Administrator uses to allow addition of user or site-specific scripts, and not extended to other users.

## Log Files

Log files are located in the Log Directory. By default, access to log files is read-only at the directory level to all non-Administrator users. Service Account users must also have read/write access to this directory, and the default Local System Account is granted this permission at install time.

## Certificates

File-based certificates, including private key certificates for some protocols like Secure ICCP and REST, are stored in the following locations. Access to these directories should be read/write for Administrator users and read-only for Service Account users. All other users should be restricted from both read and write access.

- <Install Directory>\Server\certificates
- <Data Directory>\Certificates
- <Stunnel Directory>\Config

## General Firewall and Network Considerations

As installed, the server listens to no network ports. Its private SOAP server, used for communication with the Oracle Utilities Live Energy Connect Configuration Manager and its MMS service, listens on localhost only. As network protocol interfaces are configured for use, various protocol-specific IP ports may be opened for inbound connections on external network interfaces.

Customer network and security policies vary. In general, it is recommended that both inbound and outbound network access to or from the server is limited to the specific ports required for enabled protocol functionality, and is limited to specific peer IP addresses (white listing). Enforcement at both the network level and at the local machine firewall level are recommended.

# Protocol-Specific Considerations

This section lists the protocol specific considerations for Oracle Utilities Live Energy Connect (LEC).

## ICCP

The ICCP protocol (IEC 60870-6/TASE.2) is based on MMS (ISO 9506) and allows for both 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.

By default, the LEC Server listens on localhost:102. To override this when required to allow an inbound connection, the following command line modification must be added (via the Extra params field in the LCM Server tab): /listen=<interface> (example: /listen=192.168.1.1). You can specify 0.0.0.0 to listen on all local interfaces. For more information refer to the LEC Configuration Manager User Guide.

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

## Secure ICCP

Secure ICCP is simply ICCP tunneled via TLS, with some additional protocol message signing. Default settings for ICCP as described above are sufficient and no

override is required. When the LEC Server is configured to accept inbound Secure ICCP connections, it always listens on localhost for TCP/IP connections on the standard Secure ICCP port 3782.

Secure ICCP TCP/IP port 3782 connections and traffic must be allowed between the LEC Server machine and any configured Secure ICCP peers, based on the connection inbound/outbound configurations.

## OPC UA

OPC UA is a TCP/IP protocol that allows both client and server roles. OPC UA servers listen for TCP/IP connections, and clients make outbound TCP/IP connections, on configurable ports.

OPC UA allows for both unencrypted/unauthenticated and encrypted/authenticated connections with varying levels of security:

- Basic256/Sha256 (most secure)
- Basic256
- Basic256/Sha15

By default, when the LEC Server is configured as an OPC UA server or client, Basic256/Sha256 is used. This can be overridden to use lesser security when required (example: when connecting with a legacy system). For more information refer to the Configure LEC as an OPC UA/ICCP Front End to an OEM Application.

Unencrypted/unauthenticated connections should only be used when absolutely necessary and such usage requires that the operating network be secured.

OPC UA uses configurable IP ports. TCP/IP connections and traffic must be allowed between the Server machine and any configured OPC UA client/server peers based on the connection inbound/outbound configurations.

## DNP3

DNP3 (IEEE 1815) is a protocol that uses TCP/IP or UDP/IP as a transport layer. LEC Server can be configured to accept inbound connections, make outbound connections, listen for inbound UDP messages, and send outbound UDP messages.

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 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 and listen inbound/outbound configurations.

## REST

LEC Server REST interface implements an HTTPS REST client and server. The REST server handles inbound HTTPS REST requests (example: GET, POST, PUT, …) to read and write data. The REST client pushes data to a configurable external REST server. Both the client and server use standard HTTPS (TLS 1.x) security for encryption and can use client certificate or Windows Native authentication. Microsoft IIS on the local machine is used as a reverse HTTPS proxy for inbound HTTPS connections.

IIS must be installed and configured as a HTTPS reverse proxy to use the Server REST in production. For more information refer to the LEC RESTful API Specification and Configuration Guide. IIS listens for inbound HTTPS connections on either the standard or an alternatively configured TCP/IP port.

When configured as a REST client, the remote REST server must be configured to use secure HTTPS URLs and client/server authentication. For more details refer to the LEC RESTful API Specification and Configuration Guide.

Current standards for HTTPS security, certificate key length, etc., should be followed.

## RTP/NMS

When LEC Server is configured as and ICCP or DNP3 front end for Oracle Utilities Network Management System, the Server's RTP binary protocol is used. RTP is a simple TCP/IP protocol that operates on a configurable port. Connections originate from Oracle Utilities Network Management System to the Server.

RTP is an unsecured protocol that offers no encryption nor authentication and therefore must only be enabled for use on a secure operating network.

TCP/IP connections and traffic must be allowed from the Oracle Utilities Network Management System machine to the Server machine on the configured port.