Cyber Security Guideline

LOYTEC electronics GmbH

Contact

LOYTEC electronics GmbH
Blumengasse 35
1170 Vienna
AUSTRIA/EUROPE
support@loytec.com
http://www.loytec.com

Version 1.1

Document № 88092302

Contents

1 Disclaimer Cyber Security

LOYTEC offers a portfolio of products, solutions and systems with cyber security functions that enable the secure operation of devices, systems and networks in the field of building automation and control technology. To ensure that devices, systems, and networks are always protected against online threats, a holistic security concept is required that is implemented using the latest technology and is being kept up-to-date. The LOYTEC portfolio is only one component of such an overall concept.

The customer is responsible for preventing unauthorized access to the devices, systems and networks. These should only be connected to a network or the Internet if adequate security measures are in place (e.g. firewalls, separate networks) and a connection is required for operation. In addition, LOYTEC's recommendations for securing devices in the Security Hardening Guide (Chapter 2) must be followed. For additional information, please contact your support person at LOYTEC or visit our website.

LOYTEC is constantly working on improving the existing products in order to follow the latest cyber security standards. Therefore, LOYTEC strongly recommends installing updates as soon as they become available and always using the latest software versions. LOYTEC explicitly points out that using older versions or refraining from updates increases the risk of online security threats.

2 Security Hardening Guide

This guide contains security-relevant information for operating the product on IT networks. The information refers to the firmware version 7.6.

2.1 Installation Instructions

Install the device over the Web interface:

- Set up the basic device functions and protocol settings. When connecting over the Web UI use https:// in the URL.
- Set a secure password for the admin and operator accounts.
- Disable the HTTP, FTP, and Telnet servers in the IP port configuration as described in the LOYTEC Device User Manual [1]. Note, that FTP and Telnet are disabled in factory defaults as of firmware 7.0.0.
- Create a new HTTPS server certificate as described in the LOYTEC Device User Manual [1].
- Set a password for the “guest” user to protect information of the device info page from unwanted disclosure.

2.2 Firmware

The device is equipped with one piece of software. This is the firmware image and its related firmware version. The firmware is distributed as a downloadable file. The device can be upgraded by placing the firmware image onto the device. The device firmware is signed by LOYTEC and its signature integrity is verified before the upgrade is allowed.

2.3 Ports

This Section lists all ports, which may be used by the device. The ports are default settings for their respective services. If not stated otherwise, the ports can be changed.

Required Ports:

- 80 tcp: This port is opened by the Web server and the OPC XML-DA server. It can be disabled if OPC XML-DA is not required. The port can be changed.
- 1628 udp/tcp: This is the data exchange port for CEA-852 (LON over IP). It is required for the primary function of the device to exchange control network data between routers over the IP network. Each device needs this port open. The port can be changed.
- 1629 udp/tcp: This is the configuration server port of CEA-852. Exactly one device in the system needs this port open. Other devices register with the configuration server to form the IP-852 channel list. The port can be changed.
- 47808 udp: This is the data exchange port for BACnet/IP. It is required for the primary function of the device to exchange control network data between routers over the IP network. Each device needs this port open. The port can be changed.

Optional ports not necessary for the primary product function. They can be disabled.

- 21 tcp: This port is opened by the FTP server. The port can be changed and disabled.

- 22 tcp: This port is opened by the SSH server. The port can be changed and disabled.
- 23 tcp: This port is opened by the Telnet server. The port can be changed and disabled.
- 161 tcp: This port is opened by the SNMP server. This port is disabled by default. The port can be changed.
- 443 tcp: This port is opened by the secure Web server for HTTPS. It can be disabled.
- 5900 tcp: This port is opened by the VNC server, if it is enabled. This port is disabled by default. The port can be changed.
- 502 tcp: This port is opened, if Modbus TCP is configured in slave mode. This port is disabled by default. The port can be changed.
- 3671 udp: This port is opened by KNXnet/IP, if KNX is enabled on the Ethernet interface. This port is disabled by default. The port can be changed.
- 1630 udp/tcp: This port is used by the CEA-709 RNI and for the remote LPA. The port can be changed and disabled.
- 2048 tcp: This port is opened by the logiCAD online test. It cannot be changed. The service can be disabled but the port will remain open.
- 16028/16029 udp: These ports are opened for LIOB-IP on the device. These ports cannot be changed. They can be disabled.
- 2002 tcp: This port is opened by the Wireshark protocol analyzer front-end. This port is disabled by default. The port can be changed.
- 4840 tcp: This port is opened by the OPC UA server. This port is disabled by default. The port can be changed.

2.4 Services

Required services:

- CEA-852 (LON over IP): Primary function of the device. This service is in accordance with the standard ANSI/CEA-852-B.
- BACnet/IP: Primary function of the device. This service is in accordance with the standard ANSI/ASHRAE 135-2010.
- OPC XML-DA: This Web service provides access to data points over the OPC XML-DA standard.

Optional services not necessary for the primary product function. They can be disabled as described in the installation instructions in Section 2.1:

- HTTP: Web server. It provides a Web-based configuration UI. The Web UI can be disabled after setting up the device. The Web service is also used for the Configurator connection for configuration, firmware upgrade, and access to the log file.
- HTTPS: Secure Web server. It provides a Web-based configuration UI using HTTPS. It is also used for a secure Configurator connection.
- SSH: SSH server. It provides secure access to the device console menu over the network.
- FTP and Telnet: The FTP and Telnet server is used for connection to the device by the Configurator for configuration, firmware upgrade, and access to the log file. On devices without SSH these services must be enabled during device configuration.
- VNC: The VNC server can be used for remote access to the LCD display on devices that have it. The service is disabled by default.
- Modbus TCP: A Modbus TCP server is running when Modbus TCP is operated in slave mode. In all other cases this service is not needed.
- KNXnet/IP: A KNXnet/IP server is running if KNX is enabled on the Ethernet port. In all other cases this service is not needed.

- RNI: This service provides the remote network interface (RNI) function. It is also used by the remote LPA feature. If these features are not needed the service can be disabled.
- logiCAD online test: This service is used by the L-logiCAD programming tool for online debugging of IEC61131 programs. It is enabled by default on L-INX devices that have the IEC61131 logic kernel. The service can be disabled.
- LIOB-IP: This service is used by the L-IOB host function to operate LIOB-IP I/O modules. This service is enabled by default on all L-INX devices. The service can be disabled.
- OPC UA: This secure service provides access to data points over the OPC UA standard. The service is disabled by default.
- SNMP: SNMP server. It provides network management information on the device used by standard IT tools. The service is disabled by default.
- Wireshark front-end: The Wireshark protocol analyzer may connect to this service and retrieve online protocol analyzer logs. The service is disabled by default.

2.5 Upgrade Key Strength

The secure services (HTTPS, SSH) rely on certificates to authenticate the device against the connecting client. This is key to prevent man-in-the-middle attacks. The device comes with pre-installed server certificates. It is recommended to upgrade the pre-installed certificate to an individual server-certificate and use stronger key length.

- Server certificate (for HTTPS, OPC UA): Follow the instructions in the LOYTEC Device User Manual [1] Section 3.2.29 Certificate Management on how to upgrade the pre-installed X.509 server certificate to a custom, self-signed or CA-signed certificate with stronger key length.
- SSH key upgrade: If SSH is enabled it is recommended to upgrade the SSH key length. Refer to the LOYTEC Device User Manual [1] Section 3.2.28 SSH Server Config on how to upgrade your RSA key to 2048 bits.

2.6 Logging and Auditing

The device contains a log file, which can be read out over FTP or the Web server. This log contains information when the device started and when crucial communication errors occur. Other information such user log-on are not logged as they are not part of the primary services of this device.

Logged events:

- Time of the last power-on reset of the L-INX/L-GATE device.
- Time and version of the last firmware upgrade.
- Time when the device configuration has been cleared or the device was reset to factory defaults.
- Commission of the CEA-709 node/router.
- Static errors in the device and data point configuration.
- System overload situations as one-time log messages since last power-on.
- Crucial communication errors as they occur.
- Logins and login failures.

2.7 Network Access

Network access can be protected by using 802.1X port authentication (as of firmware 7.4.0) using EAP-TLS, PEAP, or TTLS. Unused Ethernet ports can be disabled.

2.8 Password Protection

Devices provide separate administrative (admin) and operative (operator) user accounts. Passwords are stored using a strong cryptographic hash (salted SHA256). Device login is protected by a login trap, that blocks logins after five consecutive failed login attempts to protect against brute-force password attacks. Initial password setting is enforced.

2.9 Secure Building Automation Protocols using VPN

A VPN feature allows configuring IP-based control protocols to be running directly on the VPN client. This effectively secures otherwise unsecured automation protocols such as BACnet/IP, Modbus TCP, KNXnet/IP or CEA-852. When running on the VPN interface, the protocols are assigned the VPN's IP address and as a protocol node, the LOYTEC device is also reachable over multi-NAT access networks, such as LTE.

LOYTEC devices support joining a virtual private network (VPN). This feature is based on the widely-used and open-protocol OpenVPN technology. An OpenVPN configuration file (.ovpn) can be installed on the Web interface and makes the LOYTEC device a VPN client and dial into the OpenVPN server defined by that file. Any standard OpenVPN configuration file can be used, which is auto-login, i.e. does not require entering a password when connecting. After having registered, the LOYTEC device can be reached via its VPN address.

Setting up a VPN client on the LOYTEC device may solve NAT router issues, because no port forwarding rules need to be configured. The device dials out to the OpenVPN server running on a public IP and establishes the VPN channel. This VPN channel provides a secure connection for building automation protocols, such as BACnet/IP, Modbus TCP or CEA-852. Being part of a VPN the LOYTEC device is also reachable over multi-NAT access networks, such as LTE.

An alternative method is to enable simple server mode on the LOYTEC device. In this mode, the device provides an OpenVPN server and allows downloading a client configuration file from the Web interface. This file can be installed on any OpenVPN client and allows that client connect to the LOYTEC device over the secure VPN channel. Only one client may connect at a time.

3 LWEB-900 Security

LWEB-900 is an innovative and comprehensive solution for building management. The software covers the whole sequence of activities, from installation of the building management system through configuring the devices, all the way to daily operation of the facilities.

The central component is the LWEB-900 Server, which stores all configuration data in a database and communicates with the devices of the building management system in real time. The LWEB-900 Client is the user interface of the building management system. When a user starts the client, he has to log on to the server before receiving access. Client and server exchange data using web services only.

Due to this system architecture, remote access is easily possible through firewalls and NAT routers.

3.1 Password Protection

Per default the LWEB-900 Server user interface is not protected by a password. The password protection can be activated in the **Login** Tab of the menu **File → Preferences.**

Note *Do not confuse the server login with the client login. The LWEB-900 Server user interface can be started on the server PC only and is used to manage multiple projects. The LWEB-900 Client can be started on a remote PC and connects to a specific project. The user name and password specified in the client login is part of the project.*

3.2 Certificate Management

Certificates are part of Secure Socket Layer (SSL) encryption. The server certificate enables the user to confirm the identity of the LWEB 900 Server. The **Certificate management** tab allows you to create a self-signed certificate, import a certificate, or create a certification request which can be sent to a certification authority.

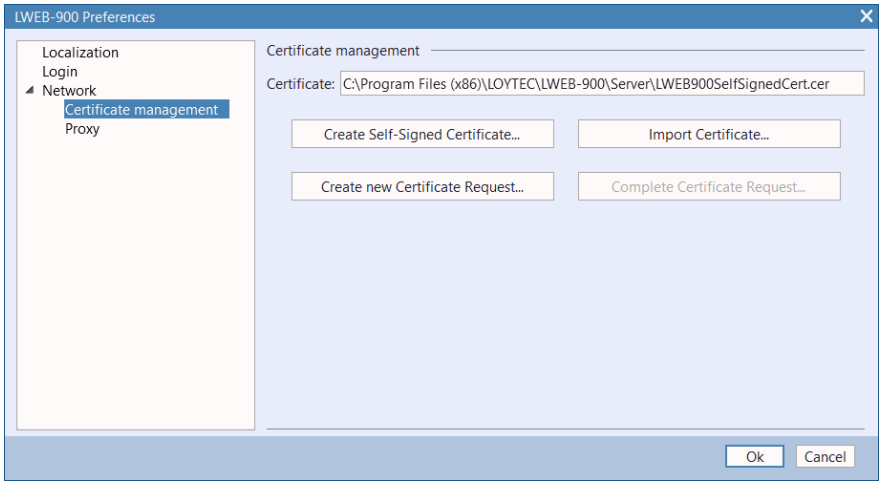

Figure 1: LWEB-900 Server Certificate Management

Enable secure connection using a self-signed certificate

1. Start the LWEB-900 Server UI and select the **Network** tab of the **File → Preferences** menu.
2. Activate the **Enable HTTPS** checkbox.
3. Select the **Certificate management** tab and click on the button **Create Self-Signed Certificate**.
4. Switch to the **Network** tab and activate the **Enable HTTPS** checkbox.

When you connect with the LWEB-900 Client to the LWEB-900 Server for the first time, a warning will be displayed because the certificate was not issued by a trusted certification authority (see Figure 2). If you set the checkbox **Do not show this warning again**, the certificate will be accepted without warning in the future.

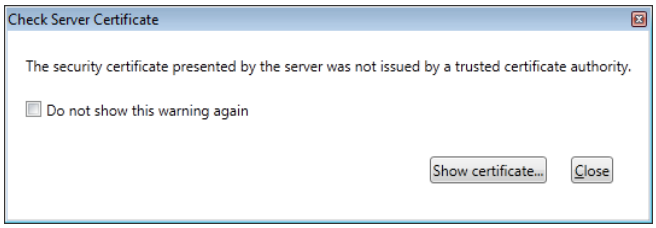

Figure 2: Server Certificate Warning

Enable secure connection using a certificate issued by a public certification authority

1. Start the LWEB-900 Server UI and select the **Network** tab of the **File → Preferences** menu.
2. Activate the **Enable HTTPS** checkbox.
3. Select the **Certificate management** tab and click on the button **Create new Certificate Request**.
4. In the certificate request dialog fill out the following data:
   - **Common Name**: The name through which LWEB-900 Server will be accessed (usually the fully-qualified domain name).
   - **Organization**: The legally registered name of your organization/company.
   - **Organizational unit**: The name of your department within the organization.
   - **City/Locality**: The city in which your organization is located.
   - **State/Province**: The state in which your organization is located.
   - **Country/Region**: Enter your two-digit country code (e.g. AT: Austria, DE Germany, US United States).
   - **Bit Length**: In the drop-down box, select a bit length for the RSA encryption algorithm.
5. Specify the path where the certification request should be set or use the browser button (…) and press **OK**.
6. Send the request to a public certification authority (CA).

After you received a response from the public certification authority, perform the following actions to install the certificate:

1. Start the LWEB-900 Server UI and select the **Certificate management** tab of the **File → Preferences** menu.
2. Click on the **Complete Certificate Request** button.
3. Select the certificate signed by your certification authority and click on **Install Certificate**.

3.3 User Management

When the LWEB-900 client is started, a login is required. There is a default admin user (user name: “admin”, password: “loytec4u”) who has full access rights. New users can be created in the user management dialog. Users can be assigned to user groups. User groups are the basis to define detailed access rights on objects.

Figure 3: User Management Toolbar

LWEB-900 supports two types of user authentication:

- LWEB-900 Authentication: The user name and password are stored in the LWEB-900 data base. The LWEB-900 Server performs the authentication.
- Windows Authentication: The LWEB-900 Server is connected to an Active Directory server which performs the authentication.

3.4 Access Rights

The global access level specified for each user defines the default access rights. These default access rights can be further refined by defining access rights to the individual objects in the navigation tree. The effective access rights can never exceed the user access level.

LWEB-900 uses access control lists (ACL) to define which operations a user can perform on a certain object (e.g. folders, data points, visualization view, parameter view, trend charts), with following Access Levels:

1.

Access Level	Description
Allow Read	The user is allowed to see the value of the object (e.g. data point value, parameter value).
Allow Write	In addition to the permissions granted by **Allow Read**, the user is allowed to change the value of the object (e.g. data point value, parameter value).
Allow Configure	In addition to the permissions granted by **Allow Read**, the user is allowed to change the configuration of the object (e.g. change graphical view, add object in folder).
Allow Full Control	In addition to the permissions granted by **Allow Configure**, the user is allowed to edit the access rights of the object.
Deny Full Control	The user is denied to change the access rights of the object.
Deny Configure	In addition to the permissions denied by **Deny Full Control**, the user is denied to change the configuration of the object (e.g. change graphical view, add object in folder).
Deny Write	In addition to the permissions denied by **Deny Configure**, the user is denied to change the value of the object (e.g. data point value, parameter value).
Deny Read	In addition to the permissions denied by **Deny Write**, the user is denied to see the value of the object (e.g. data point value, parameter value).

Table 1: Access Levels

4 References

[1] LINX/LGATE User Manual 7.6, LOYTEC electronics GmbH, Document № 88073029, January 2022.

5 Revision History

Date	Version	Author	Description
2021-04-20	1.0	STS	Initial revision V1.0
2022-07-08	1.1	STS	Added requirement to set password for guest user.