



**SUMMARY OF
LIGHTWARE'S
BASIC NETWORK
SECURITY FEATURES
in TAURUS UCX**

Introduction

This document gives a summary about the security features of Taurus UCX switchers. Security settings are available from firmware package 1.2.0.

Security Tools



Disable Ethernet Layer and Network Services

Ethernet connections and network services can be limited by enabling/disabling the Ethernet ports depending on the actual system configuration.



Encryption (HTTPS, WSS)

Requests and responses can be transferred via HTTPS (port no. 443). HTTPS protocol encrypts clear text, so it becomes incomprehensible for a third-party. Secure websocket (WSS) service on 443 port can be used for control the UCX switcher with LW3 protocol commands.



Basic Network Authentication

To limit the user access for the HTTP/HTTPS server services, username and password requirement can be enabled for these sessions.

All security settings can be configured:

- via Lightware Device Controller Software (LDC)
- via Lightware REST API
- via LW3 protocol commands

Summary of Ports, Protocols, Features and the Security Options

Purpose/function	Affected software	Protocol	Port nr.	Port disable option	Encryption	Authentication option	Other features
HTTP port (LW3 over WS, REST API)	LDC, LDU2	TCP	80	✓	✗	✓	FW update, Welcome Screen image upload, Log files, User Scripts, Serial messaging
HTTPS port (LW3 over WSS, REST API)	LDC, LDU2	TCP	443	✓	✓	✓	
LW3 protocol	LDC	TCP	6107	✓	✗	✗	
Serial over IP (RS-232)	-	TCP	8001, 8002	✓	✗	✗	
mDNS/Bonjour (Device Discovery)	LDC, LDU2	UDP	224.0.0.251: 5353	✗	✗	✗	
LMDMP (Remote IP)	LDC, LDU2	UDP	230.76.87.82: 37421	✗	✗	✗	

The ports must not be filtered by a network switch/firewall in order to maintain operation between the device and control software.

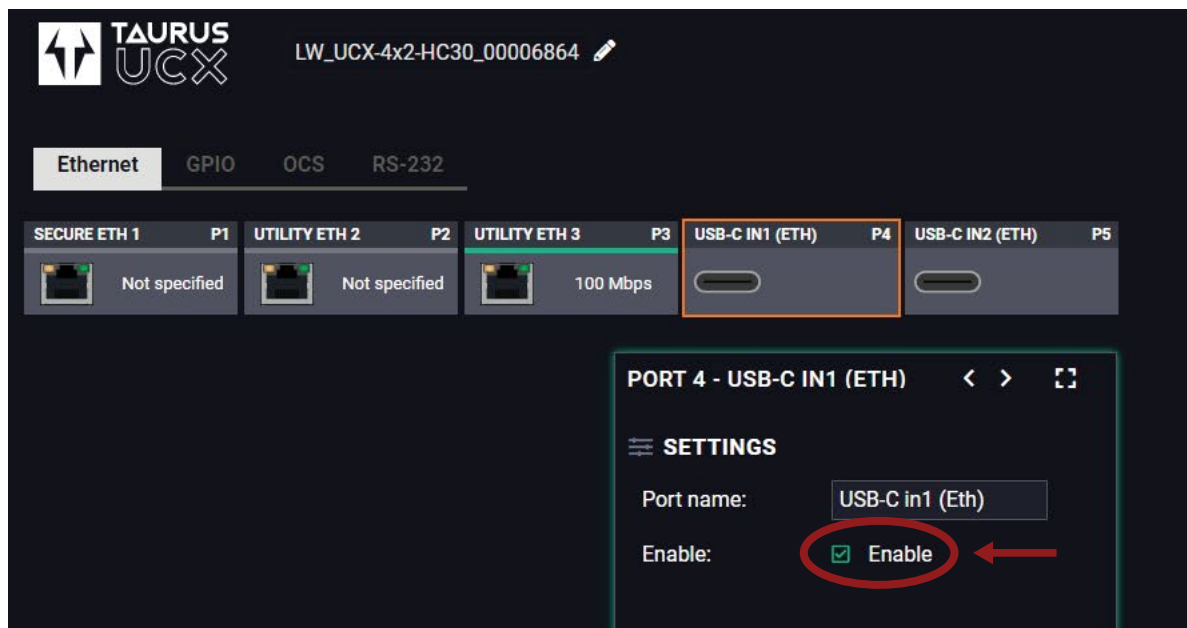
Be careful when combining the security functions; improper settings may cause malfunction. Factory default settings can be restored by a button press on the front panel.

Disable Ethernet Layer

Internal Ethernet connections can be limited by enabling/disabling the Ethernet ports depending on the actual system configuration. Ethernet layer of the USB Type-C port can be disabled if necessary, in this case, video and USB 3.1 transmission remain available.

Enable/Disable Ethernet Port with LDC

The Ethernet tab in the Control menu contains the below indicated section:



Choose the desired port and put a tick to enable or disable the Ethernet layer.

Please note that the Lightware Device Controller operates over Ethernet, so disabling the used Ethernet port brakes the connection. When all Ethernet ports are disabled, the device becomes unavailable. Factory default settings can be restored by a button press on the front panel (this will enable the Ethernet ports again).

Enable/Disable Ethernet Port with REST API

- ➔ header: POST http://192.168.0.50/api/V1/MEDIA/ETHERNET/P1/Enabled HTTP/1.1
- ➔ body: false
- ⬅ header: 200 OK
- ⬅ body: false

Enable/Disable Ethernet Port with LW3

- ▶ SET /V1/MEDIA/ETHERNET/P1.Enabled=true
- ⬅ pw /V1/MEDIA/ETHERNET/P1.Enabled=true

Parameters: P1 is the Ethernet port number; when the value is true, the port is enabled, false means that the port is blocked.

Disable Network Services

UCX series switcher provides HTTP/HTTPS server services on its 80 (for HTTP) and 443 (for HTTPS) ports. It makes possible to use the following services via HTTP/HTTPS:

- **80: HTTP**

LW3 over WebSocket: WS for LW3 protocol or using LDC for device control; REST API for device control; Serial message sending with REST API; Firmware update; WelcomeScreen image upload; UserScripts upload; Logfiles download from the device.

- **443: HTTPS**

LW3 over WebSocket: WSS for LW3 protocol or using LDC for device control; REST API for device control; Serial message sending with REST API; Firmware update; WelcomeScreen image upload; UserScripts upload; Logfiles download from the device.

⚠ 80 or 443 port is necessary to upload/download WelcomeScreen image a UserScripts, log and clone files so one of them should be opened to reach these functions.

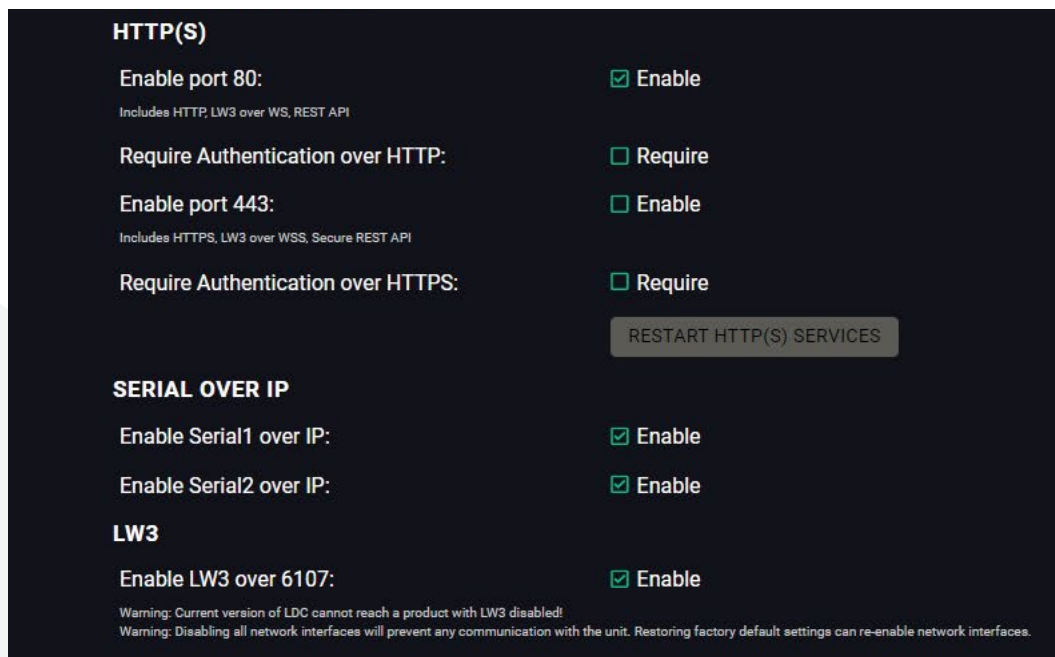
Serial data transmission and LW3 port can be also blocked:

- **8001:** Serial over IP
- **8002:** Serial over IP
- **6107:** LW3 protocol commands, Lightware Device Controller software

⚠ Lightware Device Controller software operates on 6107 port, when it is disabled, the UCX series switcher can be controlled only with protocol commands via http(s).

Enable/Disable Network Services with LDC

The Network tab in the Settings menu contains the below indicated section:



HTTP(S)

Enable port 80: ☒ Enable
Includes HTTP, LW3 over WS, REST API

Require Authentication over HTTP: ☐ Require

Enable port 443: ☒ Enable
Includes HTTPS, LW3 over WSS, Secure REST API

Require Authentication over HTTPS: ☐ Require

RESTART HTTP(S) SERVICES

SERIAL OVER IP

Enable Serial1 over IP: ☒ Enable

Enable Serial2 over IP: ☒ Enable

LW3

Enable LW3 over 6107: ☒ Enable

Warning: Current version of LDC cannot reach a product with LW3 disabled!
Warning: Disabling all network interfaces will prevent any communication with the unit. Restoring factory default settings can re-enable network interfaces.

Enable/Disable Network Service Port with REST API

- ➔ header: POST http://192.168.0.50/api/V1/MANAGEMENT/NETWORK/SERVICES/HTTP/Enabled HTTP/1.1
- ➔ body: false
- ⬅ header: 200 OK
- ⬅ body: false



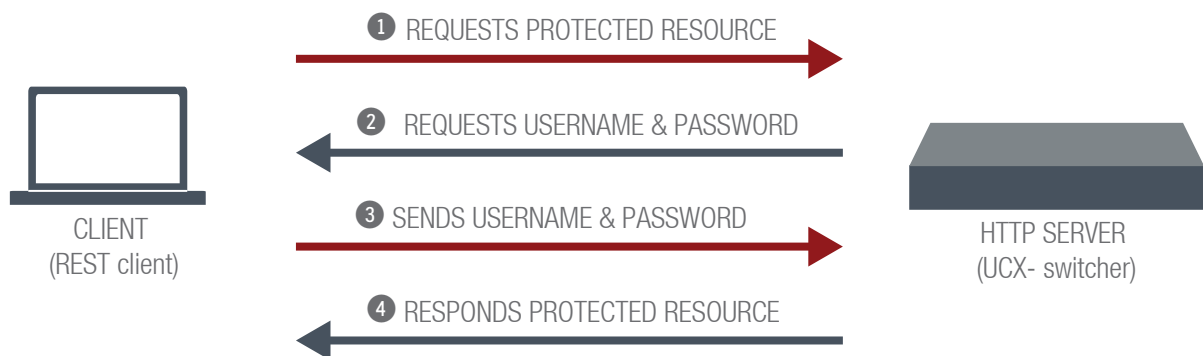
Enable/Disable Service Port with LW3

- ▶ `SET /V1/MANAGEMENT/NETWORK/SERVICES/HTTP.Enabled=true`
- ◀ `pw /V1/MANAGEMENT/NETWORK/SERVICES/HTTP.Enabled=true`

Parameters: HTTPS/LW3/ UART1/UART2 ports can be disabled, too.

Basic Authentication

To limit the user access for the HTTP/HTTPS server services, basic authentication can be turned on ports 80 and 443 separately. The picture below illustrates the successful authentication process.



i Authentication feature in UCX series is not the same as the Cleartext login feature in the Advanced Control Pack in the TPS family extenders.

User

- The current implementation can manage one user (with fixed username: admin) with full access.

Password

- No password is set for default, authentication can be enabled after setting a password.
- Due to security reasons, the password is not stored, so it can not be queried.
- The following characters are allowed: Letters (A-Z) and (a-z) and numbers (0-9). Max length: 100 characters.
- The password can be reset by calling factory defaults by a button press on the front panel.
- The password will not be encrypted by this standard HTTP authentication mode, it remains accessible when the communication happens on HTTP. Use HTTPS for encrypted communication.

Follow the instructions to set the authentication:

1. Set the password.
2. Enable the basic authentication on the chosen port (HTTP: 80 or HTTPS: 443).
3. Restart network services.

Authentication setting with LDC

The Network tab in the Settings menu contains the below indicated section:

NETWORK SERVICES

HTTP(S)

Enable port 80: ☒ Enable
Includes HTTP, LW3 over WS, REST API

Require Authentication over HTTP: ☐ Require ←

Enable port 443: ☒ Enable
Includes HTTPS, LW3 over WSS, Secure REST API

Require Authentication over HTTPS: ☒ Require ←

HTTP(S) settings have changed. Restart services to apply the settings, or restart the device.

RESTART HTTP(S) SERVICES ←

SERIAL OVER IP

Enable Serial1 over IP: ☒ Enable

Enable Serial2 over IP: ☒ Enable

LW3

Enable LW3 over 6107: ☒ Enable
Warning: Current version of LDC cannot reach a product with LW3 disabled!
Warning: Disabling all network interfaces will prevent any communication with the unit. Restoring factory default settings can re-enable network interfaces.

CREDENTIALS

New password:

Confirm new password: ←

☒ Show passwords

SAVE PASSWORD

Authentication setting with REST API

Password setting

→ header: POST http://192.168.0.50/api/V1/MANAGEMENT/NETWORK/AUTH/USER1/setPassword HTTP/1.1
→ body: password
← header: 200 OK
← body: password

Enable the authentication

→ header: POST http://192.168.0.50/api/V1/MANAGEMENT/NETWORK/SERVICES/HTTP/
AuthenticationEnabled HTTP/1.1
→ body: true
← header: 200 OK
← body: true

Restart HTTP(S) services

→ header: POST http://192.168.0.55/Apl/V1/MANAGEMENT/NETWORK/SERVICES/HTTP/restart

Authentication setting with LW3

Password setting

▶ CALL /V1/MANAGEMENT/NETWORK/AUTH/USER1:setPassword(password)
◀ m0 /V1/MANAGEMENT/NETWORK/AUTH/USER1:setPassword=

Enable the authentication

▶ SET /V1/MANAGEMENT/NETWORK/SERVICES/HTTP.AuthenticationEnabled=false
◀ pw /V1/MANAGEMENT/NETWORK/SERVICES/HTTP.AuthenticationEnabled=false

Restart HTTP(S) services

▶ CALL /V1/MANAGEMENT/NETWORK/SERVICES/HTTPS:restart()
◀ m0 /V1/MANAGEMENT/NETWORK/SERVICES/HTTPS:restart=

Encryption (HTTPS, WSS)

HTTP protocol uses clear text format for data transfer. This method allows a third-party to listen in and eavesdrop on the transferred information. To ensure secure data transmission, the HTTP port (80) can be disabled, and all the information can be transferred via HTTPS (443 port). HTTPS protocol encrypts clear text, so it becomes incomprehensible for a third-party and keeps the data secure.

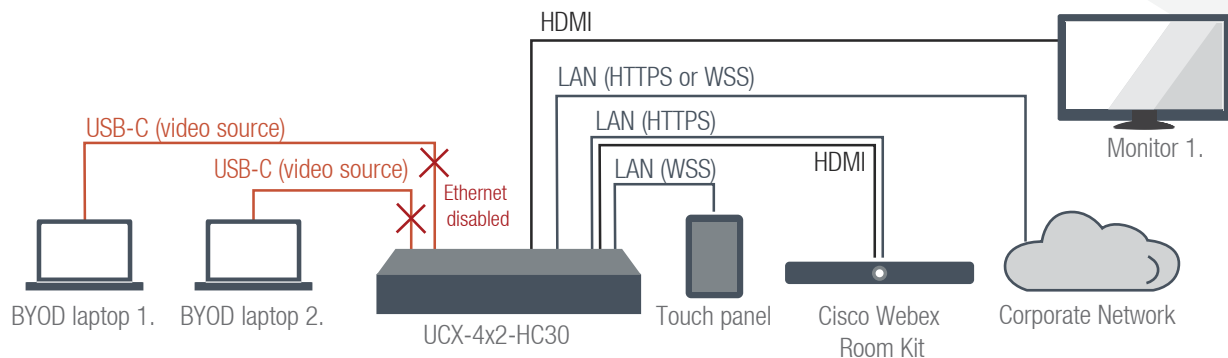
SSL

- The UCX series switcher generates a self-signed certificate (SSL), which is used to authenticate to identify itself. Self signed certificate shall be accepted and added as exception to the trusted certificates by the client for a successful communication setup.
- The user does not have to deal with its configuration.
- A new certificate is generated when the hostname changes or the factory default settings are restored.

⚠ Improper time/date setting in UCX may lead to certificate rejection by the client. Please ensure proper UCX time/date setting.



Basic Security System Example



To keep the system protected, the security features can be combined the following way:

- Step 1.** Disable the Ethernet layer of the USB-C ports towards the laptops. The video and USB 3.1 data transmission still work. This step is necessary when the BYOD laptops are not trusted for security reasons.
- Step 2.** Disable the HTTP port (80) and use HTTPS (443) instead.
- Step 3.** Disable 6107 port, use Lightware REST API HTTPS (443 port) or WSS for LW3 protocol for control the device.
 - ⚠ Lightware Device Controller software operates on 6107 port, in this case the UCX series switcher can be controlled with protocol commands via http(s).
- Step 4.** Disable the remaining unsecured Serial over IP ports (8001 and 8002).