

Application Notes

Taurus UCX Advanced Ethernet Security

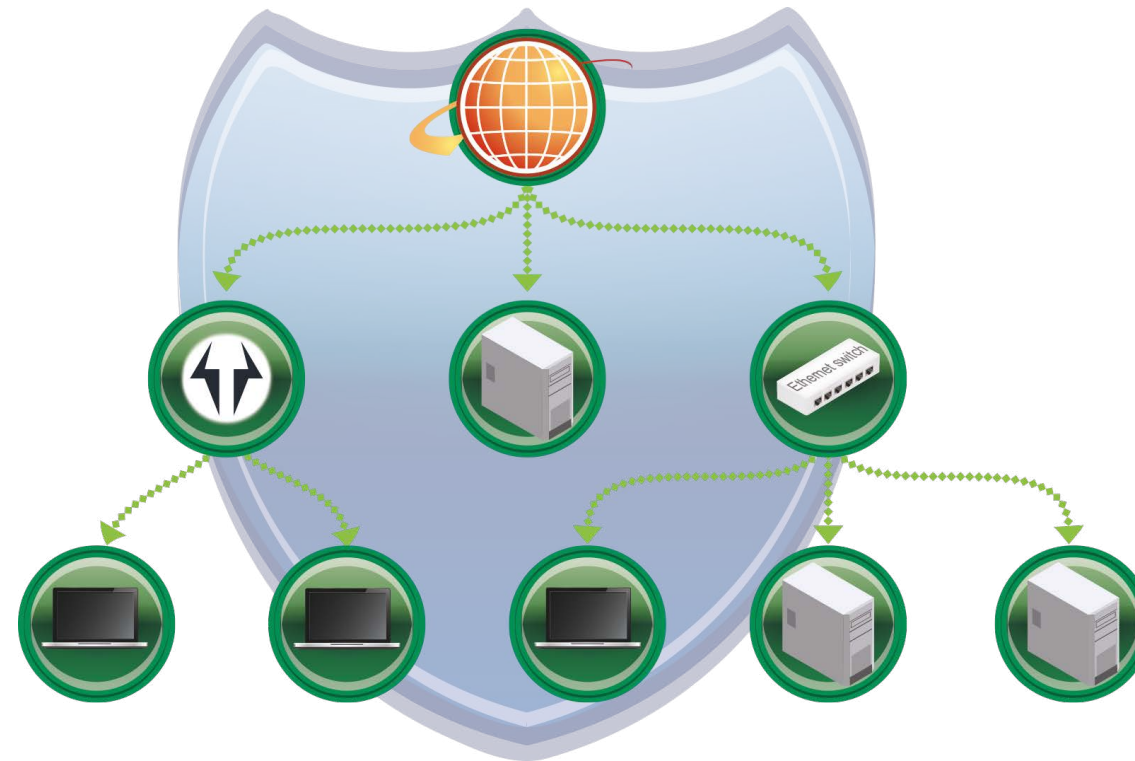


Table of Contents

1. BASIC NETWORK SECURITY IN UCX DEVICES.....3

1.1. INTRODUCTION..... 4

1.2. DISABLING ETHERNET PORTS..... 4

 1.2.1. Enabling/Disabling Ethernet Ports via LDC 4

 1.2.2. Enabling/Disabling Ethernet Ports via REST API..... 4

 1.2.3. Enabling/Disabling Ethernet Ports via LW3 5

1.3. ENABLING/DISABLING NETWORK SERVICES (HTTP/HTTPS)..... 5

 1.3.1. Enabling/Disabling Network services via LDC 5

 1.3.2. Enabling/Disabling the Network Service Port via REST API..... 6

 1.3.3. Enabling/Disabling the Service Port via LW3..... 6

1.4. BASIC AUTHENTICATION 6

 1.4.1. Setting the authentication via LDC..... 7

 1.4.2. Setting a Password for Authentication via REST API..... 7

 1.4.3. Setting a Password for Authentication via LW3 7

 1.4.4. Enabling the Authentication via REST API 8

 1.4.5. Enabling the Authentication via LW3..... 8

1.5. ENCRYPTION (HTTPS, WSS) 9

1.6. SESSION MANAGEMENT 11

1.7. LIGHTWARE CRYPTO CORE..... 11

2. ADVANCED NETWORK SECURITY IN UCX DEVICES 12

2.1. 802.1x AUTHENTICATION 13

 2.1.1. Authentication Process via LDC..... 13

2.2. 802.1X SECURITY FEATURE VIA REST API 14

 2.2.1. Querying the Security Status 15

 2.2.2. Example – Applying the TLS Method..... 15

2.3. VLAN MODE SETTING..... 15

 2.3.1. Application..... 15

 2.3.2. Custom..... 16

 2.3.3. Setting the Mode 17

 2.3.4. Setting the Mode Using the REST API Interface..... 18

 2.3.5. Setting the Mode Using LW3 19

 2.3.6. Network Separation..... 19

3. FEATURE AVAILABILITY TABLES 22

3.1. SETTING A PASSWORD 23

 3.1.1. 10-Character Minimum Limit..... 23

 3.1.2. Password History 23

3.2. VLAN MODE SETTING..... 23

 3.2.1. VLAN Presets 23

 3.2.2. Custom VLAN 23

 3.2.3. Network Separation..... 23

 3.2.4. Management VLAN..... 23

3.3. 802.1x AUTHENTICATION 23

3.4. CERTIFICATE MANAGEMENT 23

3.5. SESSION MANAGEMENT ON WEBLDC 23

Document Information

Document revision: **v1.5**

Release date: **30-07-2025**

Editor: Nikolett Keindl

Contact Us

sales@lightware.com
+36 1 255 3800

support@lightware.com
+36 1 255 3810

Lightware Visual Engineering PLC.
Gizella 51-57, Budapest H-1143, Hungary
www.lightware.com

©2025 Lightware Visual Engineering. All rights reserved. All trademarks mentioned are the property of their respective owners. Specifications subject to change without notice.

1

Basic Network Security in UCX Devices

This chapter gives a summary about the basic network security features the users can utilize when working with UCX devices.

- [INTRODUCTION](#)
- [DISABLING ETHERNET PORTS](#)
- [ENABLING/DISABLING NETWORK SERVICES \(HTTP/HTTPS\)](#)
- [BASIC AUTHENTICATION](#)
- [ENCRYPTION \(HTTPS, WSS\)](#)
- [SESSION MANAGEMENT](#)
- [LIGHTWARE CRYPTO CORE](#)

1.1. Introduction

These basic network security improvements help prevent unauthorized access to the UCX series switchers.

- Disabling Ethernet Ports
- Disabling Network Services
- Basic Authentication
- Encryption (HTTPS, WSS)
- Session Management (only in webLDC)
- Lightware Crypto Core

The following table summarizes the ports, protocols, features and the security options:

Port number	Protocol	Function	Affected software	Port disable option	Encryption	Authentication	Other features
80	TCP	HTTP port (LW3 over WS, REST API, LARA user panels)	LDC, LDU2	✓	✗	✓	FW update, Welcome Screen image upload, Log files, User Scripts Serial messaging
443	TCP	HTTPS port (LW3 over WSS, REST API, LARA management GUI)	LDC, LDU2	✓	✓	✓	
6107	TCP	LW3 protocol	LDC	✓	✗	✗	
8001, 8002	TCP	Serial over IP (RS-232)	-	✓	✗	✗	
224.0.0.251: 5353	UDP	mDNS / Bonjour (Device Discovery)	LDC, LDU2	✗	✗	✗	
230.76.87.82: 37421	UDP	Remote IP	LDC, LDU2	✗	✗	✗	
6970	TCP	TCI protocol between the UCX-TPX/TPN API server and the BlueRiver Control Server	BlueRiver Control Server	✗	✗	✗	
8080	TP			✗	✗	✗	

INFO: The ports are necessary to be passed via a network switch/firewall for proper operation between the device and the softwares.

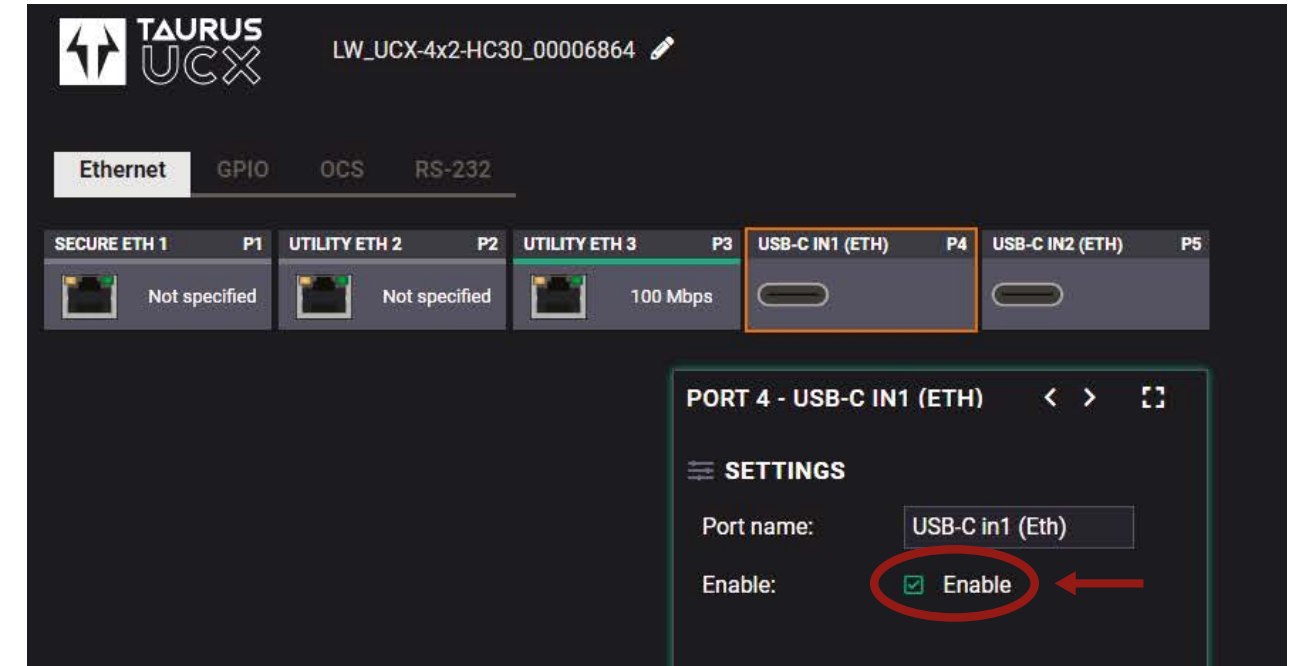
ATTENTION! Be careful when combining the security functions; improper settings may cause malfunction.

1.2. Disabling Ethernet Ports

Internal Ethernet connections can be limited by enabling/disabling the Ethernet ports depending on the actual system configuration (e.g. Ethernet layer of the USB Type-C port can be disabled if necessary).

1.2.1. Enabling/Disabling Ethernet Ports via LDC

Navigate to the Control menu, Ethernet tab of the Lightware Device Controller. After choosing the desired port, look to the side to see the port properties.



You can enable/disable the port by clicking in the green box.

Please note that the LDC operates over Ethernet, so disabling the used Ethernet port breaks the connection to the device. If all Ethernet ports are disabled, the device becomes unavailable. Factory default setting can be restored via the front panel buttons (this will enable the Ethernet ports again).

1.2.2. Enabling/Disabling Ethernet Ports via REST API

→ request: POST <http://192.168.0.100/api/V1/MEDIA/ETHERNET/P1/Enabled>
 → body: false
 ← response: 200 OK
 ← body: false

1.2.3. Enabling/Disabling Ethernet Ports via LW3

Command and Response

- ▶ SET /V1/MEDIA/ETHERNET/<ethernet_port>.Enabled=<status>
- ◀ pw /V1/MEDIA/ETHERNET/<ethernet_port>.Enabled=<status>

Parameters

Parameter	Parameter description	Values	Value description
<ethernet_port>	Ethernet port number	P1-P5*	
<status>	Status of the port	true	The port is enabled.
		false	The port is disabled.

* The port numbering may differ depending on the model. Please refer to the User Manual for specifics.

Example

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

1.3. Enabling/Disabling Network Services (HTTP/HTTPS)

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

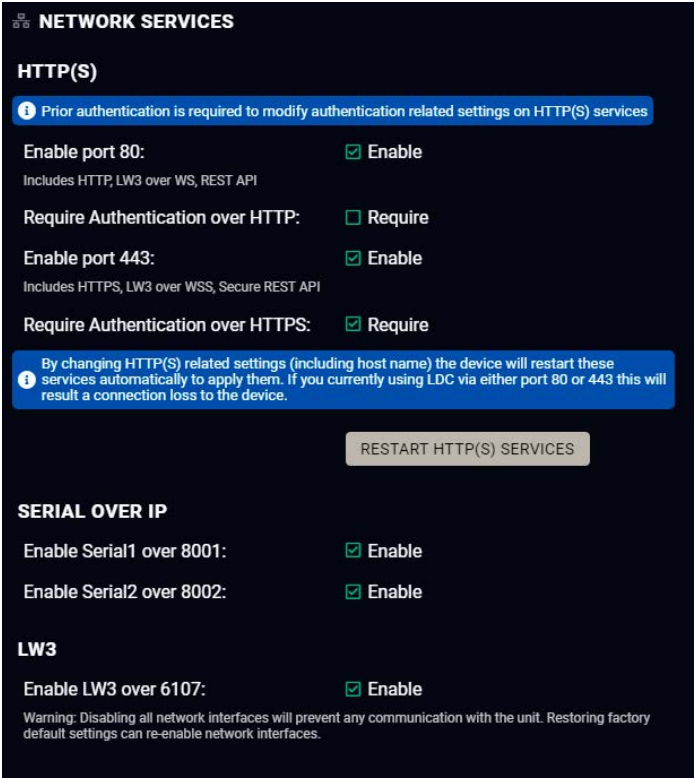
- LW3 over WebSocket (WS, WSS) for LW3 protocol or using LDC for device control
- REST API for device control
- Serial message sending with REST API
- Firmware update
- Uploading WelcomeScreen image
- Uploading UserScripts
- LARA interface
- Downloading logfiles from the device

DIFFERENCE: UserScripts are only available with up to FW version v1.4.4 (in UCX standalone models). From firmware version v1.5.0, LARA replaces functions previously managed by UserScripts.

ATTENTION! LARA management GUI is only available through HTTPS and it is password-protected.

1.3.1. Enabling/Disabling Network services via LDC

In the Settings menu, Services tab you can find the Network Services section. You can adjust the settings by clicking in the green boxes.



DIFFERENCE: The Services tab is available from LDC version v2.7.0. In the earlier versions the Network Services can be found under the Network tab.

1.3.2. Enabling/Disabling the Network Service Port via REST API

Request and Response

→ request-line: GET http://<ip>/api/V1/MANAGEMENT/NETWORK/SERVICES/<port>/Enabled
→ body: <status>
← status-line: 200 OK
← body: <status>

Parameters

Identifier	Parameter description	Parameter values
<port>	Port type	HTTP / HTTPS / LW3 / SERIAL1 / SERIAL2
<status>	The port is enabled.	true
	The port is disabled.	false

Example

→ request-line: POST http://192.168.0.100/api/V1/MANAGEMENT/NETWORK/SERVICES/HTTP/Enabled
→ body: false
← status-line: 200 OK
← body: false

1.3.3. Enabling/Disabling the Service Port via LW3

DIFFERENCE: This command is available from 1.2.0 firmware package in UCX standalone models.

Command and Response #http #https

► SET /V1/MANAGEMENT/NETWORK/SERVICES/<port>.Enabled=<status>
◄ pw /V1/MANAGEMENT/NETWORK/SERVICES/<port>.Enabled=<status>

Parameters

Parameter	Parameter description	Values	Value description
<port>	Port type	HTTP HTTPS LW3 SERIAL1 SERIAL2	
<status>		true	The port is enabled.
		false	The port is disabled.

Example

► SET /V1/MANAGEMENT/NETWORK/SERVICES/HTTP.Enabled=true
◄ pw /V1/MANAGEMENT/NETWORK/SERVICES/HTTP.Enabled=true

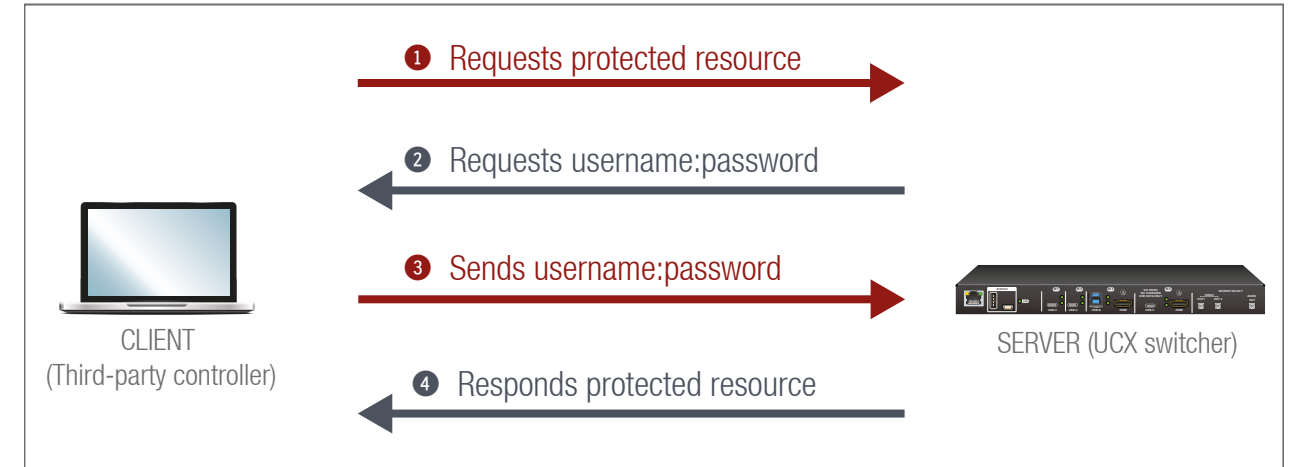
1.4. Basic Authentication

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

DIFFERENCE: Please see the feature availability in the [Setting a Password](#) tables.

ATTENTION! Authentication feature in UCX series is not equal to the Cleartext login feature in the Advanced Control Pack v3 of the TPS family extenders.

The picture below illustrates the successful authentication process:



User

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

Password

- No password is set by default, the authentication can be enabled after setting a password. The old password is not necessary for modifying prior to firmware version v2.0.0. From that version on, the old password is required when password is changed.
- From firmware version seen in the [10-Character Minimum Limit](#) table, the password must be at least 10 characters long, and any UTF-8 character is allowed.
- From firmware version seen in the [Password History](#) table and LDC version v2.8.0, password history is maintained in authentication, not allowing for the last 10 passwords to be set again.
- The device does not store the password string, so it can not be queried.
- The password can be reset by calling factory default settings

1.4.1. Setting the authentication via LDC

Follow the instructions to set the authentication:

- Step 1.** Set the password with Lightware Device Controller software or REST API protocol command.
- Step 2.** Enable the authentication on the chosen port (HTTP: 80 or HTTPS: 443) with the Lightware Device Controller software or LW3 protocol command.
- Step 3.** Restart network services.

ATTENTION! The password will not be encrypted by this authentication mode, it remains accessible when the communication happens on HTTP.

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

By changing HTTP(S) related settings (including host name) the device will restart these services automatically to apply them. If you currently using LDC via either port 80 or 443 this will result a connection loss to the device.

RESTART HTTP(S) SERVICES

SERIAL OVER IP

Enable Serial1 over 8001: ☒ Enable

Enable Serial2 over 8002: ☒ Enable

LW3

Enable LW3 over 6107: ☒ Enable

Warning: Disabling all network interfaces will prevent any communication with the unit. Restoring factory default settings can re-enable network interfaces.

LARA

Enable LARA : ☐ Enable

To access LARA, please enable HTTPS service (port 443) and set a valid password below, in advance.

CREDENTIALS

To change password, the current password is mandatory if exists, otherwise leave it blank.

Username: admin

Current password:

New password:

Confirm new password:

Show passwords

SAVE PASSWORD

1.4.2. Setting a Password for Authentication via REST API

- DIFFERENCE:** From firmware version seen in the [10-Character Minimum Limit](#) table, the minimum character requirement for the password is 10 characters, and it can contain any UTF-8 character.
- DIFFERENCE:** From firmware version seen in the [Password History](#) table and LDC version v2.8.0, password history is maintained in authentication, not allowing for the last 10 passwords to be set again.
- INFO:** Due to security reasons, the password is not stored in any property, so it can not be queried. No password is set by default, setting a password before authorizing the authentication is necessary.

Request and Response #password

- ➔ request-line: POST http://<ip>/api/V1/MANAGEMENT/NETWORK/AUTH/USER1/setPassword
- ➔ body: <password>
- ⬅ status-line: 200 OK
- ⬅ body: <password>

Parameters

Identifier	Parameter description	Value description
<password>	User defined password for authentication.	min. character length: 10 max. character length: 100 accepted characters: UTF-8 characters

Example

- ➔ request-line: POST http://192.168.0.100/api/V1/MANAGEMENT/NETWORK/AUTH/USER1/setPassword
- ➔ body: #password12
- ⬅ status-line: 200 OK
- ⬅ body: #password12

1.4.3. Setting a Password for Authentication via LW3

- DIFFERENCE:** From firmware version v2.2.0 in UCX standalone models, password setting via LW3 is unavailable due to character limitations. From this version on, password setting is only available via LDC or REST API. UCX-TPX and UCX-TPN models did not receive password setting via LW3 functionality in the first place.

1.4.4. Enabling the Authentication via REST API

INFO: Set the password before enabling the authentication, because no password is set by default. Restarting the HTTP(S) services is required to apply the authentication settings.

Request and Response

➔ request-line: POST http://<ip>/api/V1/MANAGEMENT/NETWORK/SERVICES/<port>/AuthenticationEnabled
➔ body: <status>
⬅ status-line: 200 OK
⬅ body: <status>

Parameters

Identifier	Parameter description	Parameter values
<port>	Port type	HTTP / HTTPS
<status>	Authentication enabled	true
	Authentication disabled	false

Example

➔ request-line: POST http://192.168.0.100/api/V1/MANAGEMENT/NETWORK/SERVICES/HTTP/AuthenticationEnabled
➔ body: false
⬅ status-line: 200 OK
⬅ body: false

1.4.5. Enabling the Authentication via LW3

DIFFERENCE: This command is available from 1.2.0 firmware package in UCX standalone models. UCX-TPX and UCX-TPN models contain this feature from FW v1.0.0.

INFO: Set the password before enabling the authentication, because no password is set by default.

Command and Response

▶ SET /V1/MANAGEMENT/NETWORK/SERVICES/<port>.AuthenticationEnabled=<status>
⬅ pw /V1/MANAGEMENT/NETWORK/SERVICES/<port>.AuthenticationEnabled=<status>
▶ CALL /V1/MANAGEMENT/NETWORK/SERVICES/HTTP:restart()
⬅ m0 /V1/MANAGEMENT/NETWORK/SERVICES/HTTP:restart=

Parameters

Parameter	Parameter description	Values	Value description
<port>	Port type	HTTP HTTPS	
<status>		true	The authentication is enabled.
		false	The authentication is disabled.

Example

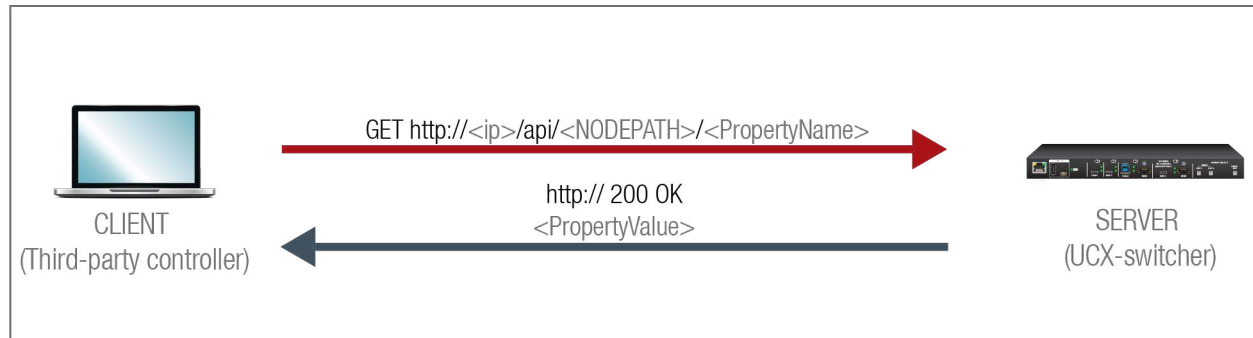
▶ SET /V1/MANAGEMENT/NETWORK/SERVICES/HTTP.AuthenticationEnabled=true
⬅ pw /V1/MANAGEMENT/NETWORK/SERVICES/HTTP.AuthenticationEnabled=true
▶ CALL /V1/MANAGEMENT/NETWORK/SERVICES/HTTP:restart()
⬅ m0 /V1/MANAGEMENT/NETWORK/SERVICES/HTTP:restart=

INFO: Restart HTTP(S) Services is required after the authentication settings changed.

1.5. Encryption (HTTPS, WSS)

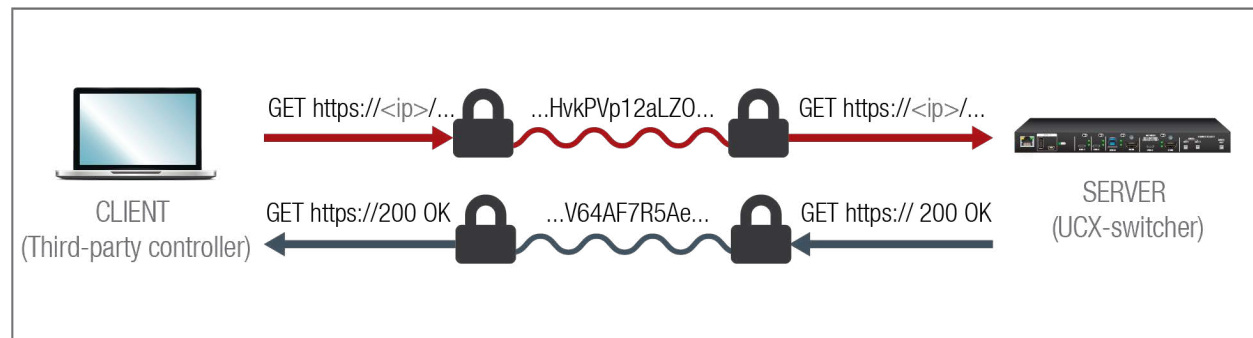
HTTP protocol uses clear text format for data transport. This method allows a third-party to listen in and eavesdrop on the transferred information.

HTTP request-response



To ensure the secure data transmission, the HTTP port (80) can be disabled, and the all the information can be transferred via HTTPS (443 port). HTTPS protocol encrypts the clear text, so it becomes incomprehensible for a third-party and keeps the data secure.

HTTPS request-response



The same services are available on HTTPS as HTTP.

- The UCX series switcher generates a self-signed certificate, so the user does not have to deal with the configuration.
- From firmware version v2.2.0, SSL certificates can also be uploaded into the device.
- A new certificate is generated after hostname changing or restoring the factory default settings.
- Please ensure proper UCX time and date setting in UCX, because it affects the self-signed certificate (SSL) generation when using WSS or HTTPS. Improper time and date setting may lead to certificate rejection.

ATTENTION! HTTPS does not guarantee that the communication is secure. Make sure that the client communicates with the server directly, without any third-party element in the communication route (Man-in-the-middle attack).

Certificate Management

DIFFERENCE: Please see the feature availability in the [Certificate Management](#) table.

You can upload certificates signed by the Certificate Authority (CA) to provide secure connection to the devices with the webLDC.

To download a Certificate Signing Request (CSR), follow these steps:

Step 1. Navigate to the Settings menu, Services tab and click on the **Certificate Signing Request** button.

Step 2. Enter the data required for the authentication process. It is important to provide all information related to your organization, because it will be used to verify your identity.

Step 3. Once all the necessary data has been entered, the file can be downloaded via the button in the bottom, and sent for signing.

Step 4. When the CA signs the certificate, it will create a .pem file, which then can be uploaded onto the device.

Step 5. After uploading, press the **Refresh** button in the Certificate Management section and the signed certificate shall be active.

Please be aware that the certificate will use the device's own private key and will not work for any other device. Each device must have its own certification file.

DOWNLOAD CERTIFICATE SIGNING REQUEST

Updating CSR parameters based on the installed certificate is automatic when the page loads, in any other case please use the 'Load CSR info/Refresh' button to update it.

Get CSR field informations from current certificate: **REFRESH**

Common Name: (Not present)

Organization Name: (Not present)

Organizational Unit: (Not present)

Locality: (Not present)

State: (Not present)

Country: Select a country

Email Address: (Not present)

Subject Alt Name(s): #1
DNS (Not present)

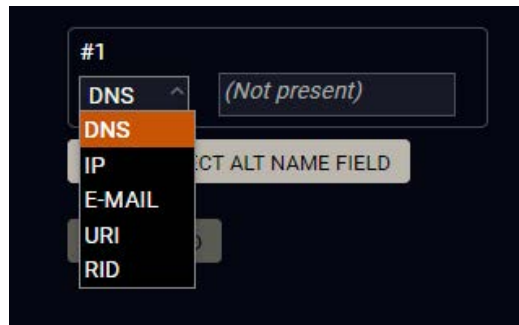
ADD SUBJECT ALT NAME FIELD

DOWNLOAD

The certificate signing request form

Information	Description	Example
Common Name	The domain name you wish to secure.	www.example.com
Organization Name	The legal name of the company or organization, any suffix included.	Lightware Visual Engineering PLC
Organizational Unit	The name of the internal organizational department/division.	IT
Locality	The name of the city, town, village etc. of the organization.	Budapest
State	Province, region, county or state, not abbreviated.	Pest county
Country	The country of the organization can be chose from the drop-down menu.	Hungary
Email Address	The contact address of the certificate administrator or the IT department of the company.	example@lightware.com

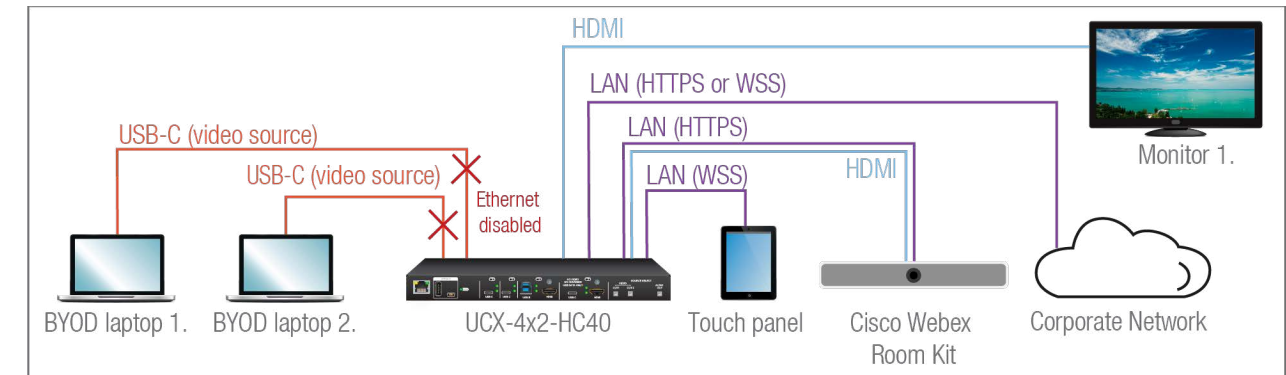
In the Subject Alt Name(s) field you can enter additional information for more hosts to be certified with one SSL file. The information type can be chosen from the drop down menu. You can have several Subject Alt Name fields.



You can enter the following information in the Subject Alt Name field:

- DNS
- IP address
- E-mail address
- URI
- RID

Basic Security System Example



To keep the system protected, the unsecured ports should be disabled and data traffic should be managed by secured channels.

Step 1. Disable the Ethernet layer of the USB-C ports towards the laptops. The video and USB data transmission still work.

The setting is available in the following ways:

- Lightware Device Controller software
- Lightware REST API HTTP posts
- LW3 protocol commands

Step 2. Disable the HTTP port (80) and use HTTPS (443) instead.

The setting is available in the following ways:

- Lightware REST API HTTP posts
- LW3 protocol commands

Step 3. Set the password and enable the authentication.

The username is always fix (admin) and the password has to be set before authentication is enabled.

The setting is available in the following ways:

- Lightware Device Controller software
- Lightware REST API HTTP posts

Step 4. Disable 6107 port, use Lightware REST API HTTPS (443 port) or WSS for LW3 protocol to control the device.

The setting is available in the following ways:

- Lightware REST API HTTP posts
- LW3 protocol commands

Step 5. Disable the remaining unsecured Serial over IP ports (8001 and 8002).

The setting is available in the following ways:

- Lightware REST API HTTP posts
- LW3 protocol commands

1.6. Session Management

The layout of the built-in web is generally the same as the LDC, with a few differences:

- There is no **Device Discovery** button.
- From a given FW version there is a **Logout** button.

INFO: The **Logout** button will only appear if the device has a password and the user is logged in.

DIFFERENCE: Please see the feature availability in the [Session Management on WebLDC](#) table.

DIFFERENCE: From a given FW version, the maximum length of a single session is **120 minutes**. If this time is up, you will be logged out, and the device will only be available upon logging in again.

DIFFERENCE: From a given FW version, in case of **30 minutes** of inactivity the session will expire. The system will remind you in a pop-up window if the current session is about to expire five minutes before the time limit. If the reminder receives no answer, the session will restart and you will be forced to log out.

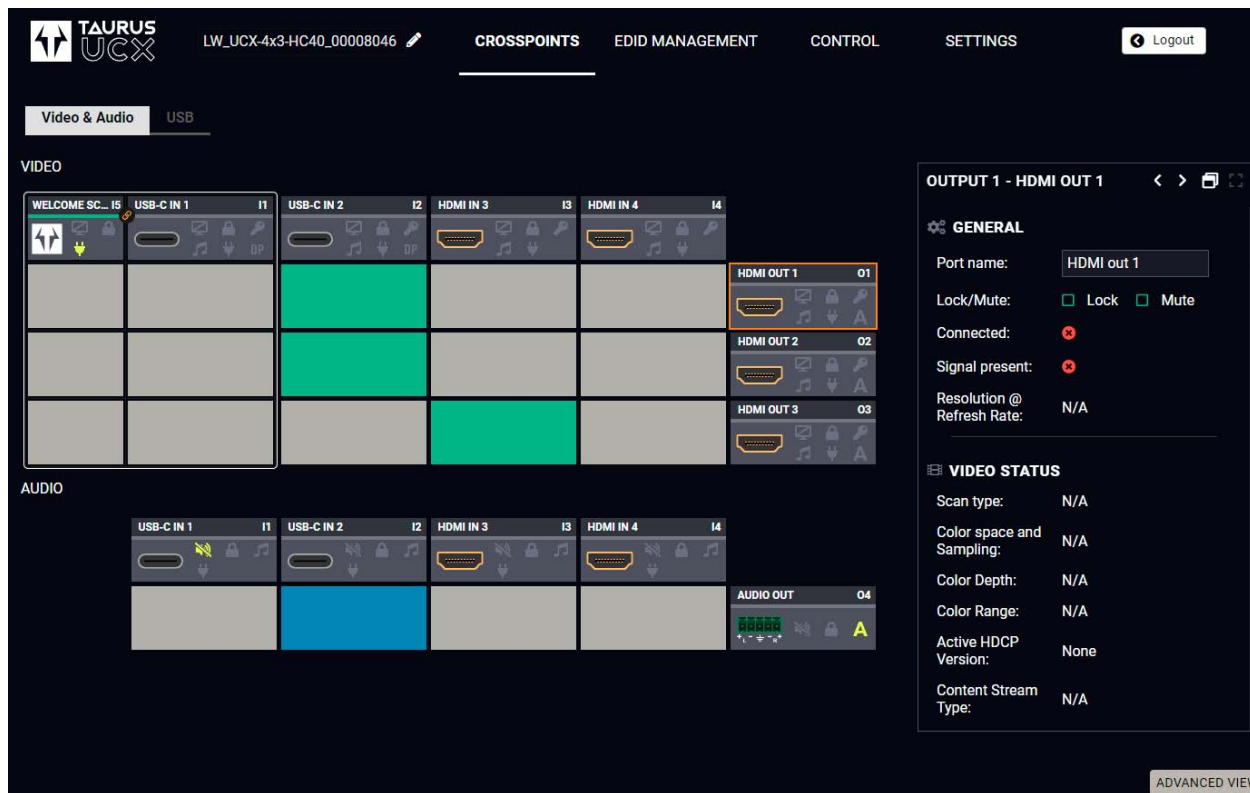
1.7. Lightware Crypto Core

DIFFERENCE: This feature is only available for the -LCC models of the UCX, UCX-TPX and UCX-TPN family.

Lightware Crypto Core is a standards-based cryptographic engine for embedded Linux systems. The module delivers core cryptographic functions to the embedded systems of Taurus product family's hardware devices and features robust algorithm support.

It also offloads functions for secure key management, data integrity, data at rest encryption, and secure communications to a trusted implementation.

Lightware Crypto Core is Lightware's own FIPS 140-2-validated, Level 1-certified, cryptographic software module that is integrated into UCX-TPX products.



The Logout button appears in the upper right corner upon login

2

Advanced Network Security in UCX Devices

This chapter describes further security measures that can be taken while using UCX devices.

- [802.1X AUTHENTICATION](#)
- [802.1X SECURITY FEATURE VIA REST API](#)
- [VLAN MODE SETTING](#)

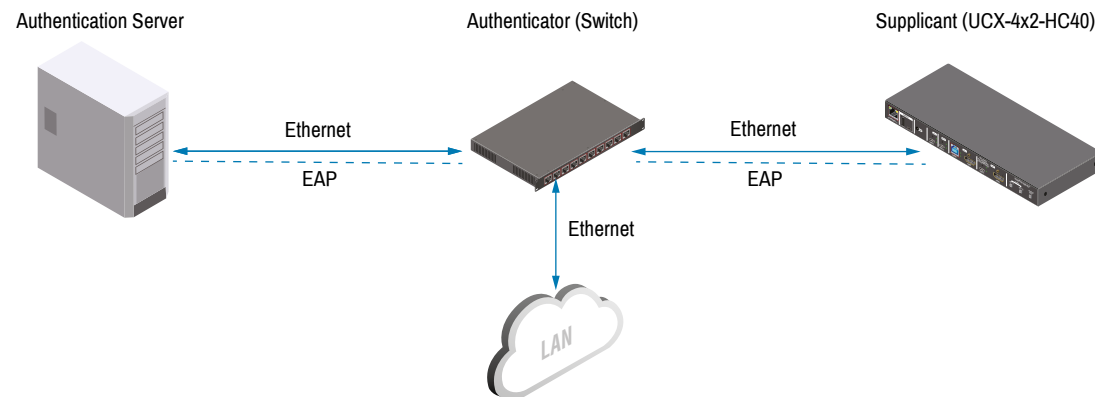
2.1. 802.1x Authentication

DIFFERENCE: Please see feature availability in the [802.1x Authentication](#) table.

DIFFERENCE: From FW version v1.16.0 in UCX-TPX-TX and UCX-TPN-TX models, 802.1x authentication over the Management network provides authentication for both the UCX-TPX/TPN and the BYOD device, but only when there is exactly one port in the Management VLAN.

ATTENTION! In case of UCX-TPX-TX and UCX-TPN-TX models, the 802.1x authentication must only be turned on after the Management network has been set up, otherwise the certificate must be uploaded again.

802.1x is a server-based port authentication protocol that restricts unauthorized clients from accessing a LAN through a public port. Three parties make up the most basic setup of 802.1x: a supplicant (client device), an authenticator (Ethernet switch) and an authentication server. Before the device is permitted access to the network, port communication is restricted to Extensible Authentication Protocol over LAN (EAPOL) traffic.



After the device passes the authentication process, the authentication server notifies the switch, allowing the client to access the LAN.

There are two available methods for 802.1x authentication in the UCX devices:

- **EAP-MD5:** This commonly used method authenticates by verifying MD5 (Message Digest 5) hash of a user password.
- **EAP-TLS:** This method utilizes Public Key Infrastructure to authenticate with an authentication server. To communicate with the server, a certification authority (CA) certificate and a client-side certificate that is signed by a known certification authority are needed.

DIFFERENCE: From firmware version v2.12.0 in UCX standalone models and v1.9.0 in UCX-TPX-TX and UCX-TPN-TX models, EAP-MD5 authentication is unavailable.

The UCX itself can act as a supplicant, but also as a route through which a BYOD device can reach the authenticator as a supplicant.

ATTENTION! If the Management network is not used, this method authenticates the UCX device, not the BYOD connected to the UCX! If you only want to authenticate the connected BYOD device and not the UCX, you do not need to activate 802.1x authentication in the UCX device. After FW update to v1.16.0 in UCX-TPX-TX and UCX-TPN-TX models, both the UCX and the BYOD device can be authenticated over the Management network.

ATTENTION! If your device is using the **Dedicated** VLAN preset and the BYOD device is disconnected from the UCX, please be aware that the Ethernet port connected to the affected USB-C port will be blocked. You will be asked to authenticate again upon reconnecting a BYOD device. In **Transparent** mode the port blocking function is inactive.

INFO: When updating the firmware of the UCX device, sensitive information (passwords, keys etc.) on the authentication will not be downloaded into the backup file, but it will be retained in the device during the update.

2.1.1. Authentication Process via LDC

The 802.1x authentication section can be found on the right side of the Settings menu, Network tab.

You can enable authentication by ticking in the Enable box. Once 802.1x authentication is enabled, you can choose the authentication method from the drop-down menu: **EAP-MD5** or **EAP-TLS**.

DIFFERENCE: From firmware version v2.12.0 in case of standalone UCX models and v1.9.0 in case of UCX-TPX-TX and UCX-TPN-TX models, EAP-MD5 is unavailable.

With EAP-TLS, you will also need CA and Client certificates, a Client Private Key, and a password for the Key.

802.1X CONFIGURATION

Enable 802.1X: ☒ Enable

Authentication method: **EAP-TLS**

Identity*:

CA Certificate*: **BROWSE**

Client Certificate*: **BROWSE**

Client Private Key*: **BROWSE**

Client Private Key Password:

Show password

*Required fields

APPLY NEW CONFIGURATION **CANCEL**

When using 802.1X, make sure to only connect a single port to the protected network. Either disable all other Ethernet ports or put them in a different VLAN.

802.1X STATUS

After entering every necessary information, click on the **Apply new configuration** button, and the authentication process starts.

If every component is correct, the device will gain access to the secure LAN.

DIFFERENCE: From FW version v1.16.0 in case of UCX-TPX-TX and UCX-TPN-TX models, 802.1x will only work properly, if there is **exactly one** port in the Management VLAN. The authentication can still be turned on when several or none of the ports are in the Management VLAN, however, it will not operate properly.

2.2. 802.1X Security Feature via REST API

This feature can be set via REST API by the following methods. All the parameters can be set and stored at the following URL:

`http://<ip_or_host>/api/V1/MANAGEMENT/SECURITY/IEEE8021X/Configuration`

Parameters

The following keys are in the Configuration structure:

Parameter	Parameter description	Values
<ip_or_host>	The IP address or the host name of the device.	e.g.: 192.168.0.110, myDevice
<enabled>	(de)activating the security feature	true false
<eap>	EAP method	MD5 TLS
<identity>	User name (identity string for EAP)	
<password>	If the EAP method is MD5, this parameter must be set. PROTECTED INFO.	
<caCert>	Plain/text in PEM format containing one or more trusted CA certificates. If the EAP method is TLS, this parameter must be set.	
<clientCert>	Plain/text in PEM format containing the certificate of the client. If the EAP method is TLS, this parameter must be set.	
<privateKey>	Plain/text in PEM format containing the private key of the client. If the EAP method is TLS, this parameter must be set. PROTECTED INFO.	
<privateKeyPasswd>	The password for the private key. Optional, it can be used if the EAP method is TLS. PROTECTED INFO.	

PROTECTED INFO: the information is protected: it can be set (POST) as a JSON object but cannot be queried (GET).

Way of Working

The Successful Request

If the POSTed JSON structure is valid and consistent, the setting is applied immediately and stored in case of a reboot as well. HTTP status response is **'200 OK'**. The response is in plain/text format containing **'OK'**.

The Unsuccessful Request

If the structure fails (e.g. EAP method is **TLS** and the **clientCert** parameter is missing or in unaccepted format), the response is **'406 Not Acceptable'**. The response format is text/plain in this case, with a reference to the nature of the failure (e.g. Client certificate required in TLS mode.).

2.2.1. Querying the Security Status

Request and Response

→ request: GET-http://<ip_or_host>/api/V1/MANAGEMENT/SECURITY/IEEE8021X/Configuration/
← response: <standard_response>
← body: <enabled>

Parameters

Parameter	Parameter description	Values	Value description
<enabled>	The current status of the security feature as a JSON object.	true false	
<standard_response>	Standard HTTP response	200 OK	<message>: <Product_name> The request has succeeded; the product name of the device is sent as text/plain content.

Example

→ request: http://192.168.0.100/api/V1/MANAGEMENT/SECURITY/IEEE8021X/Configuration/
← response: 200 OK
← body: {
← "enabled": false
← }

2.2.2. Example – Applying the TLS Method

→ request: POST http://192.168.0.100/api/V1/MANAGEMENT/SECURITY/IEEE8021X/Configuration/
→ body: {
 "enabled": true,
 "eap": "TLS",
 "identity": "John",
 "caCert": "-----BEGIN CERTIFICATE-----\n<CA certificate in PEM format>\n-----END CERTIFICATE-----\n",
 "clientCert": <client certificate in PEM format>,
 "privateKey": <encrypted private key of the client in PEM format>,
 "privateKeyPasswd": "myPassword"
}
← response: 200 OK
← body: OK

2.3. VLAN Mode Setting

This section offers a brief explanation about the different options available through the Advanced Ethernet Security feature.

DIFFERENCE: Please see the feature availability in the [VLAN Presets](#) table.

ATTENTION! Please note that availability of some VLAN presets described here depends on the UCX model. See the User Manual of the device for specific details.

This feature is a port-based VLAN setting, which allows the user to decide which network(s) the USB-C ports are connected to, and thus which network(s) the connected devices can use. This way the connected devices can be separated from the corporate network, increasing network security.

There are three options available, which are the following:

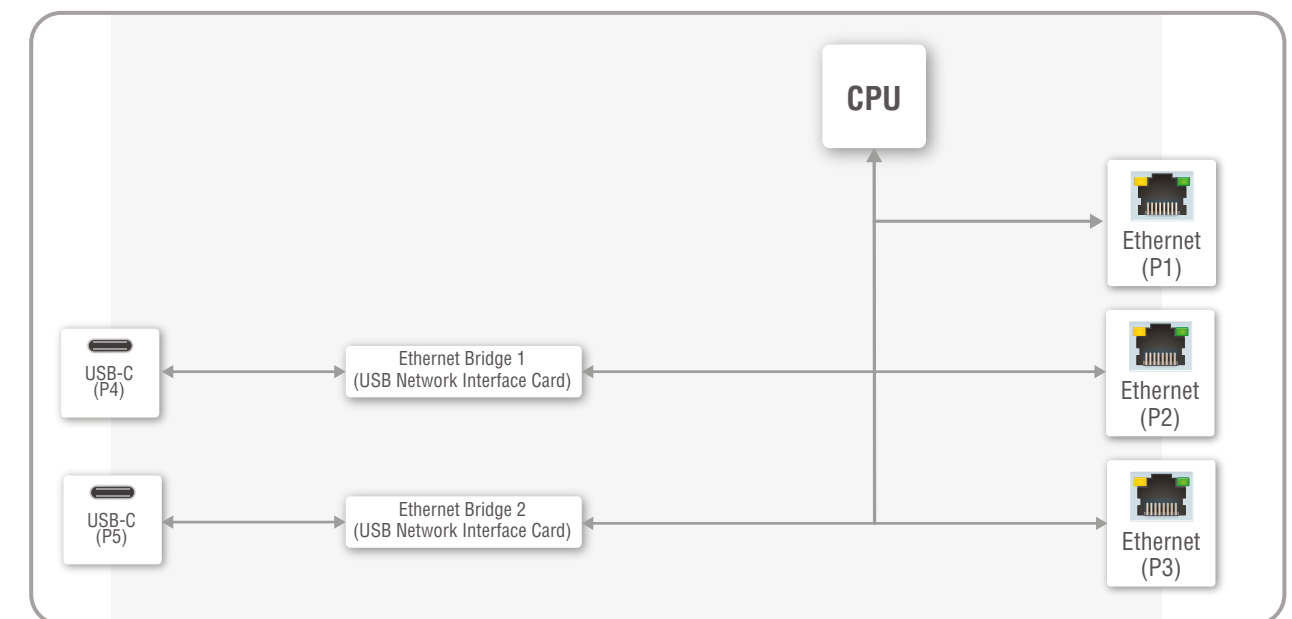
- **Transparent:** this is the default mode, with the network openly used by Taurus and the BYOD devices. If you want to authenticate the connected BYOD through 802.1x, this option is not recommended.
- **Separated BYOD:** the network provided for the BYOD devices is separated from the control network. If you want to authenticate the connected BYOD through 802.1x, then the 802.1x authenticator port must support multi-authentication.
- **Dedicated:** each connected BYOD device receives an independent network. If you want to authenticate the connected BYOD device(s) through 802.1x, the 802.1x authenticator port can be single-host, however make sure every BYOD is connected to the UCX via a CATx cable.
- **Custom:** the user can sort the Ethernet ports into separate groups.

2.3.1. Application

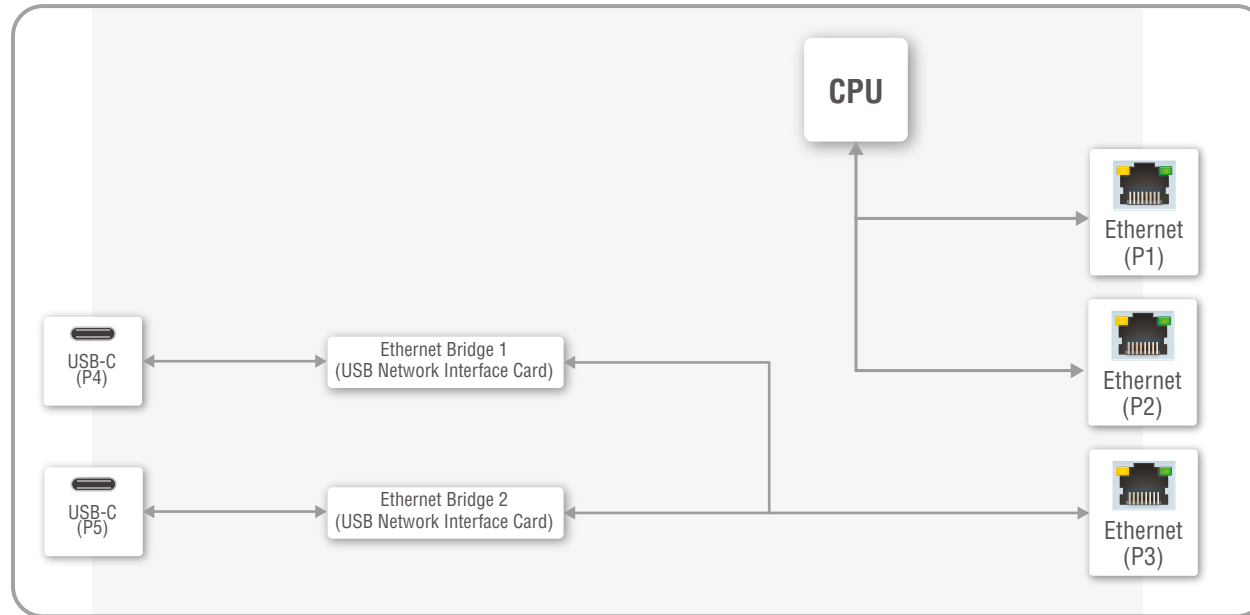
These port diagrams offer a simple breakdown of the different modes of the feature.

INFO: Only one mode can be active at the same time.

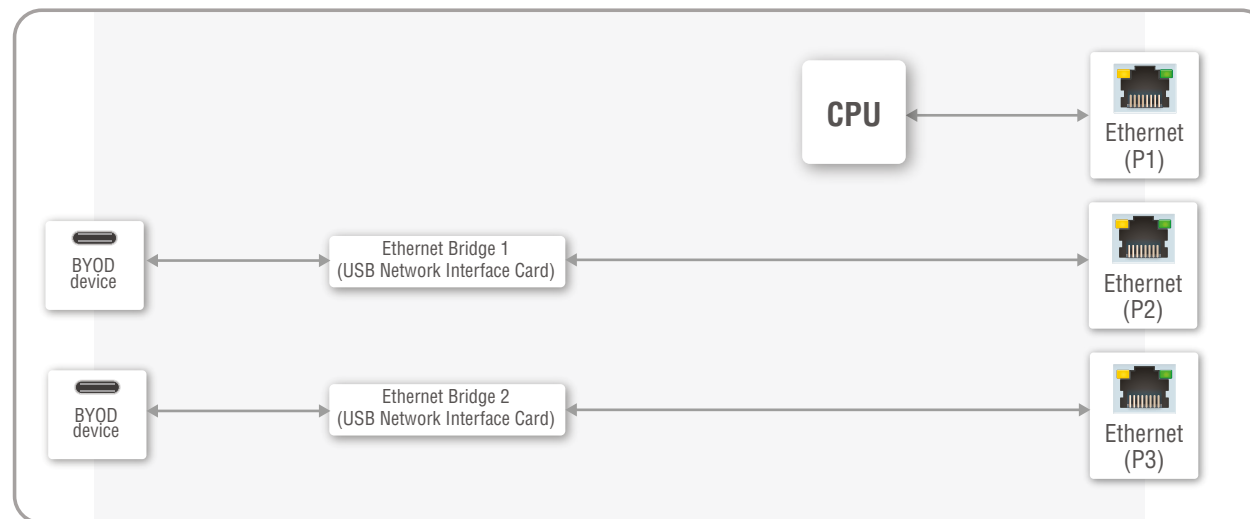
Transparent



Separated BYOD



Dedicated

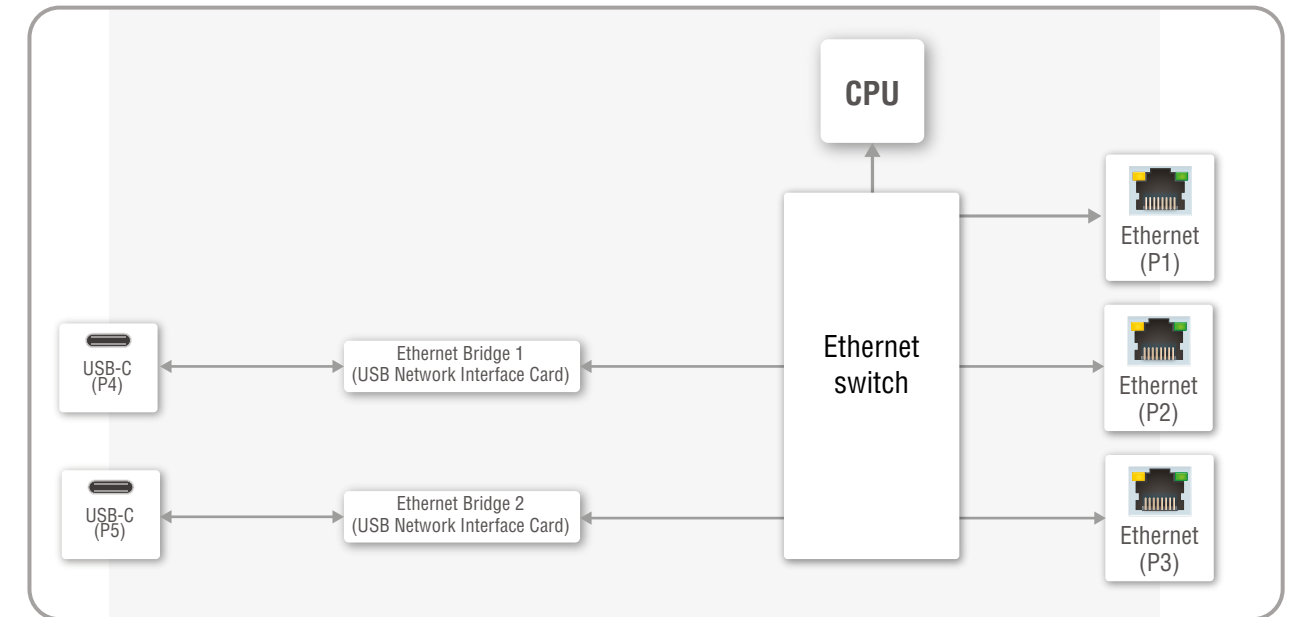


2.3.2. Custom

DIFFERENCE: Please see the feature availability in the [Custom VLAN](#) table.

The custom VLAN setting enables the user to set up their own Ethernet networks by putting the ports in separate groups. An Ethernet switch inside the device acts like a crosspoint for the Ethernet ports. Any VLAN setting that does not fall into the premade categories (Transparent, Separated BYOD or Dedicated) will be classified as **Custom**.

INFO: This mode cannot be directly chosen - it automatically switches to this mode when the settings are changed accordingly.



Custom VLAN preset in UCX-4x2-HC30(D)

2.3.3. Setting the Mode

This can either be set through the Lightware Device Controller (LDC), LW3 or the REST API interface.

Setting the Mode Using LDC

ATTENTION! Make sure that you are connected to the device via the P1 Ethernet port (Secure Control LAN), otherwise you could lose connection to the device.

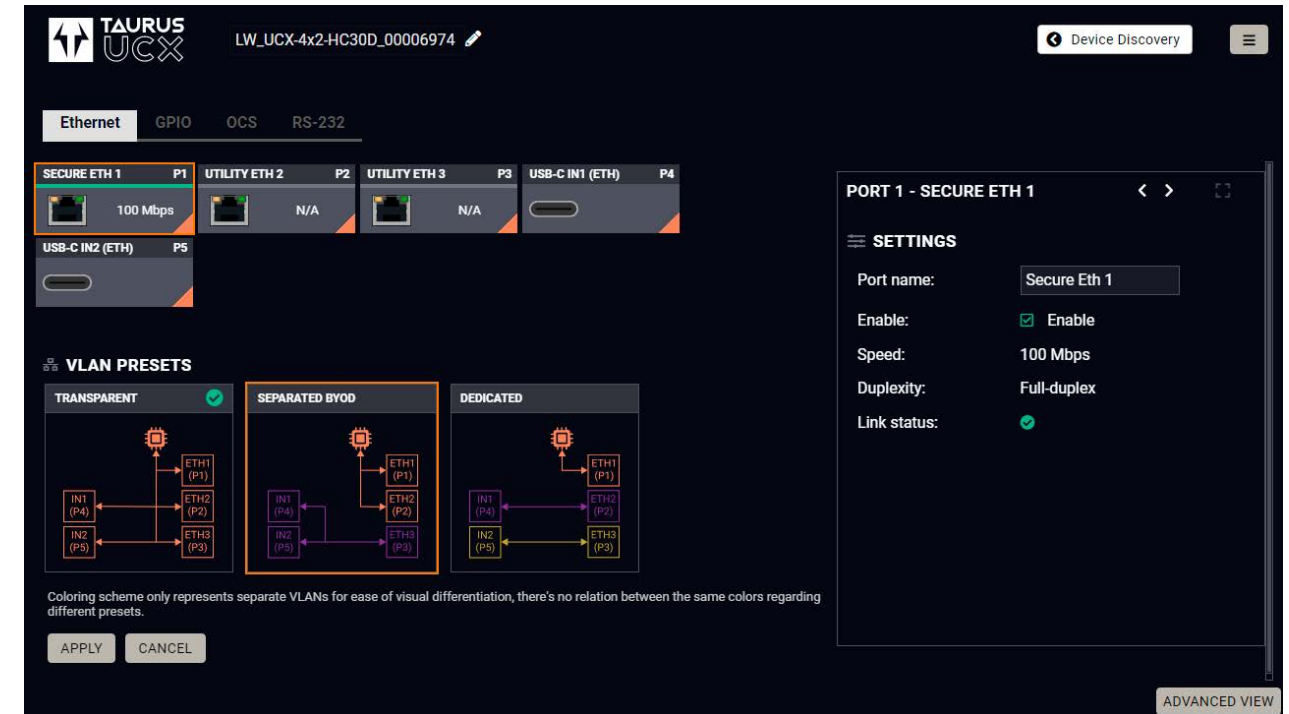
Step 1. Open the LDC, or download it from our website (www.lightware.com) if you haven't done so yet.

Step 2. Click on the Control menu. By default, the Ethernet tab will appear. You will see a VLAN Presets section under the ports.

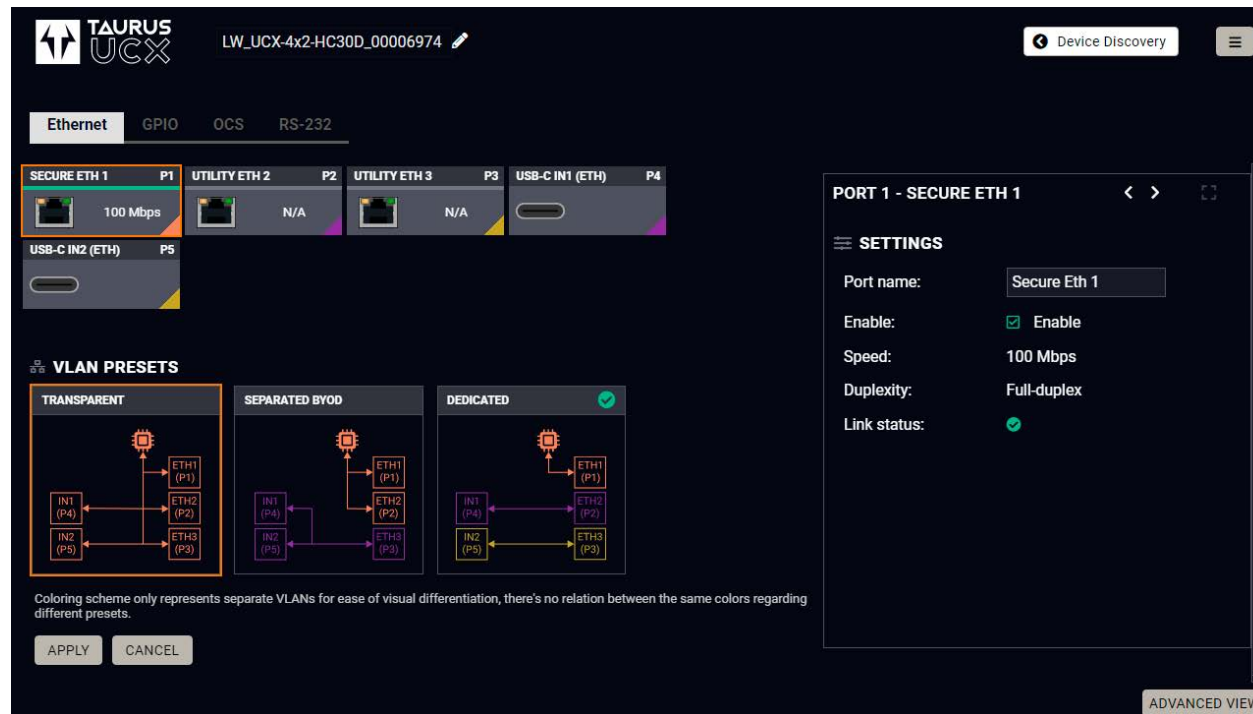
Step 3. Here you can choose the desired mode via the diagrams. Default is the **Transparent** mode, you can choose a different mode by clicking on it, and the click on the **Apply** button. The change is immediate, there is no need for reboot.

INFO: You can see which network the USB-C ports are connected to by checking the colored triangles in the lower right corner of the port tiles.

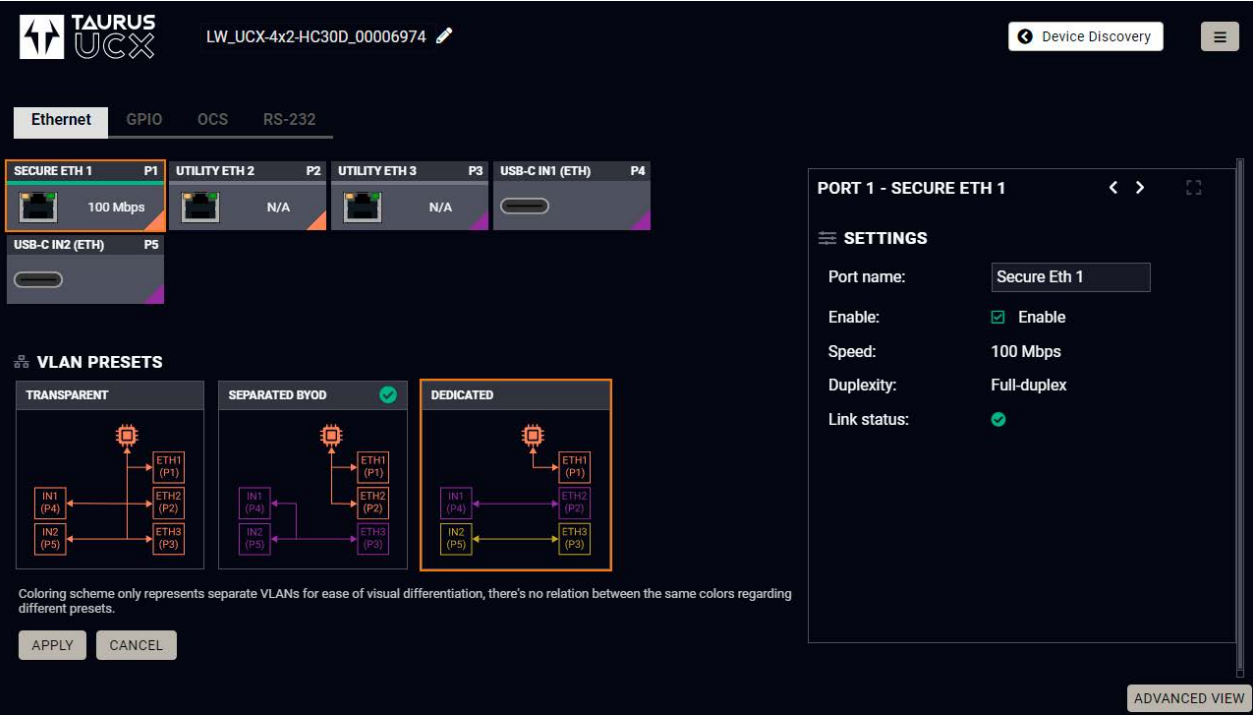
INFO: The active VLAN preset will have a green tick in the upper right corner.



Active VLAN preset is Separated BYOD



Transparent is the default VLAN preset



Active VLAN preset is Dedicated

Setting the mode in advanced view for standalone UCX switchers

- Step 1. Navigate to the /V1/MEDIA/ETHERNET node.
- Step 2. Here you can find the **VLAN preset** property, where you can set the ethernet security mode.
The default is **Transparent** mode.
To separate the BYOD network from the main line, type **SeparatedByod**.
To provide a separate network for each BYOD device, type **Dedicated** into the text field.

Setting the mode in advanced view for UCX-TPX and UCX-TPN switcher extenders

- Step 1. Navigate to the /V1/MEDIA/ETHERNET node.
- Step 2. Choose the port number you wish to change the settings of.
- Step 3. Here you can find the **VLAN Membership** property, where you can set the ethernet security mode.
The default is **1**. Values can range from 1 to 4094. The number **1000** is reserved for Management network.

INFO: Management network is currently only available in UCX-TPX and UCX-TPN devices.

For more information about the LDC, please see the User's Manual of the device.

2.3.4. Setting the Mode Using the REST API Interface

REST API interface can be easily accessed via a web browser's plugin, or the REST API requests can be applied to the switcher using a terminal application. You need to install one of them on your control device, for example, Putty, CLI or Curl.

Curl

Curl is a command line tool that can also connect to the Taurus REST SERVER and display communication in a terminal window. It supports data transferring with HTTP and HTTPS standards and handles the basic authentication (username and password) in Windows® and Linux operating systems. Multi-line commands are also accepted, so a script can be stored in a .txt file for future reference.

Check if the Curl package is installed on your system. Type into your console: curl. When the answer is 'curl: try 'curl --help' for more information', curl is installed.

Some web browser plugins (e.g. REST Client) display the curl version of the sent request. Once the terminal window is opened, you can enter the commands.

Setting the Transparent Mode

➔ header: POST http://192.168.0.100/api/V1/MEDIA/ETHERNET.VlanPreset

➔ body: transparent

⬅ header: 200 OK

⬅ body: transparent

Separating the BYOD Network from the Main Line

➔ header: POST http://192.168.0.100/api/V1/MEDIA/ETHERNET.VlanPreset

➔ body: separate byod

⬅ header: 200 OK

⬅ body: separate byod

Creating a Separate Network for Each BYOD Device

➔ header: POST http://192.168.0.100/api/V1/MEDIA/ETHERNET.VlanPreset

➔ body: dedicated

⬅ header: 200 OK

⬅ body: dedicated

For more information about the REST API interface, please see the User's Manual of the device.

2.3.5. Setting the Mode Using LW3

The mode can be set by using the Lightware 3 (LW3) protocol.

Terminal Application

The LW3 protocol commands can be applied to the switcher using a terminal application. You need to install one of them on your control device, for example **Putty** or **CLI**. *#terminal*

Establishing Connection

Follow the steps to establish connection to the switcher:

Step 1. Connect the device to a LAN over Ethernet.

Step 2. Open the terminal application (e.g. Putty).

Step 3. Add the **IP address** of the device (default: DHCP) and the **port number (6107)**.

Step 4. Select the **Raw** connection type, and open the connection.

Once the terminal window is opened, you can enter the LW3 protocol commands.

Setting the transparent mode

◀ **SET /V1/MEDIA/ETHERNET.VlanPreset=Transparent**

▶ **pw /V1/MEDIA/ETHERNET.VlanPreset=Transparent**

Separating the BYOD network from the main line

◀ **SET /V1/MEDIA/ETHERNET.VlanPreset=SeparateByod**

▶ **pw /V1/MEDIA/ETHERNET.VlanPreset=SeparateByod**

Creating a separate network for each BYOD device

◀ **SET /V1/MEDIA/ETHERNET.VlanPreset=Dedicated**

▶ **pw /V1/MEDIA/ETHERNET.VlanPreset=Dedicated**

For more information about the LW3 interface, please see the User's Manual of the device.

2.3.6. Network Separation

DIFFERENCE: Please see the feature availability in the [Network Separation](#) table.

The TPX matrix switch supports two VLANs: the Default/AV network and the Management network. However, due to a topology limitation, both VLANs may currently operate under the same MAC address. This setup can lead to connectivity issues such as:

- Packet Misrouting: Network traffic may be sent to the incorrect VLAN.
- Loop and Congestion: Duplicate MAC addresses can cause loops or broadcast storms.
- Device Inaccessibility: Difficulty in managing devices or maintaining network reliability.

To ensure stable operation and avoid connectivity conflicts, follow this practice:

On the switch, disable any ports or VLANs that are not actively in use. This reduces the chance of unintended traffic crossing between VLANs.

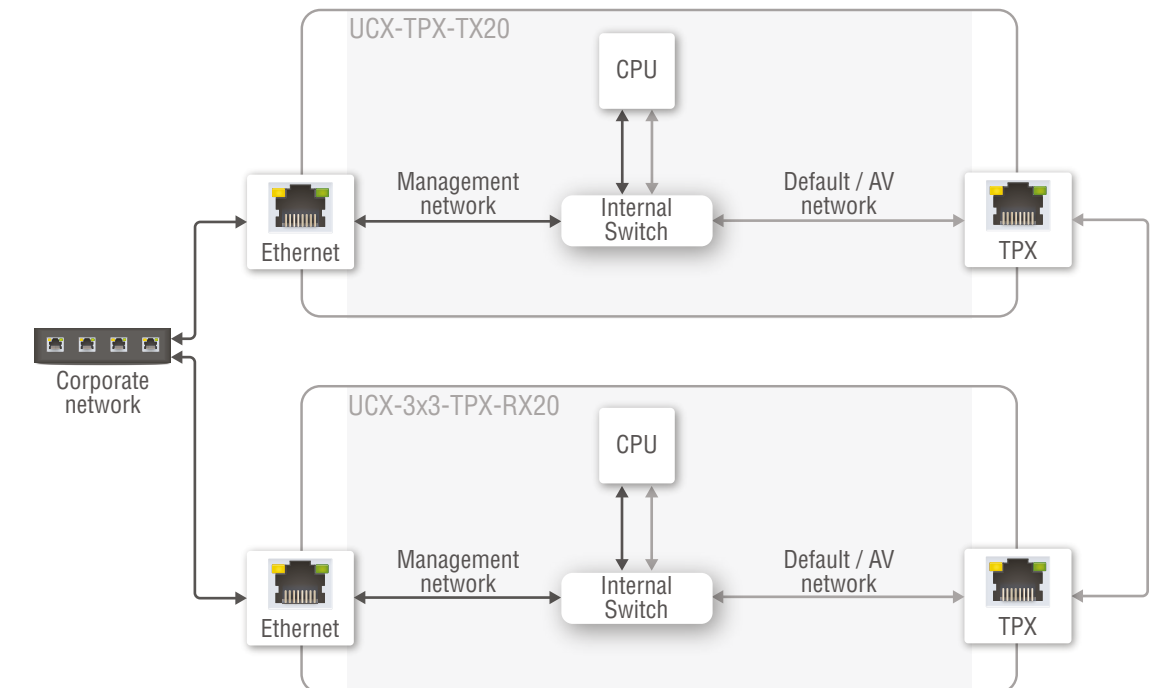
DEFINITION: Management network is a VLAN Membership setting that creates an Ethernet port that can be used to only connect to the CPU for controlling and updating purposes. Its VLAN Membership number is set to 1000.

INFO: The illustrations have been simplified for easier understanding. Please see the full port layouts in the User Manual of the device.

Example Scenario

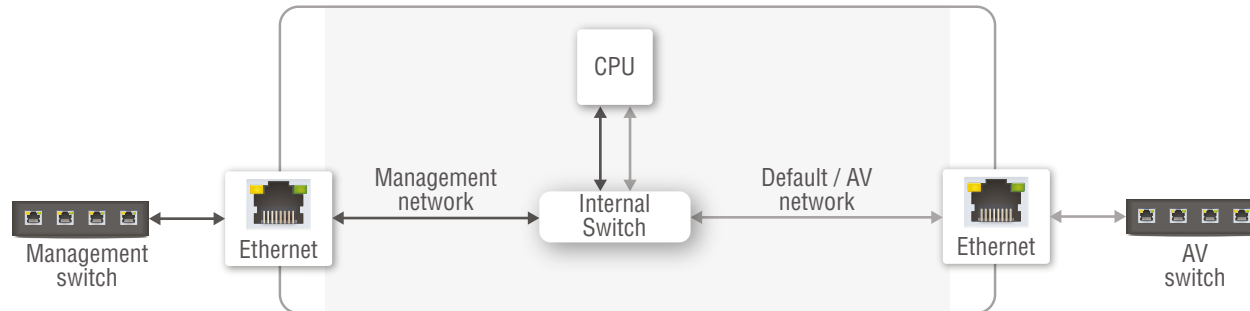
Both the TX and the RX are connected to the Corporate network through the Management network, and to each other through the Default/AV network via the TPX ports. In this case the switches will see the same MAC addresses on both networks, and would be unable to tell which network to route to a MAC address.

One of the endpoints must be disconnected from the Management network in order for the system to work.



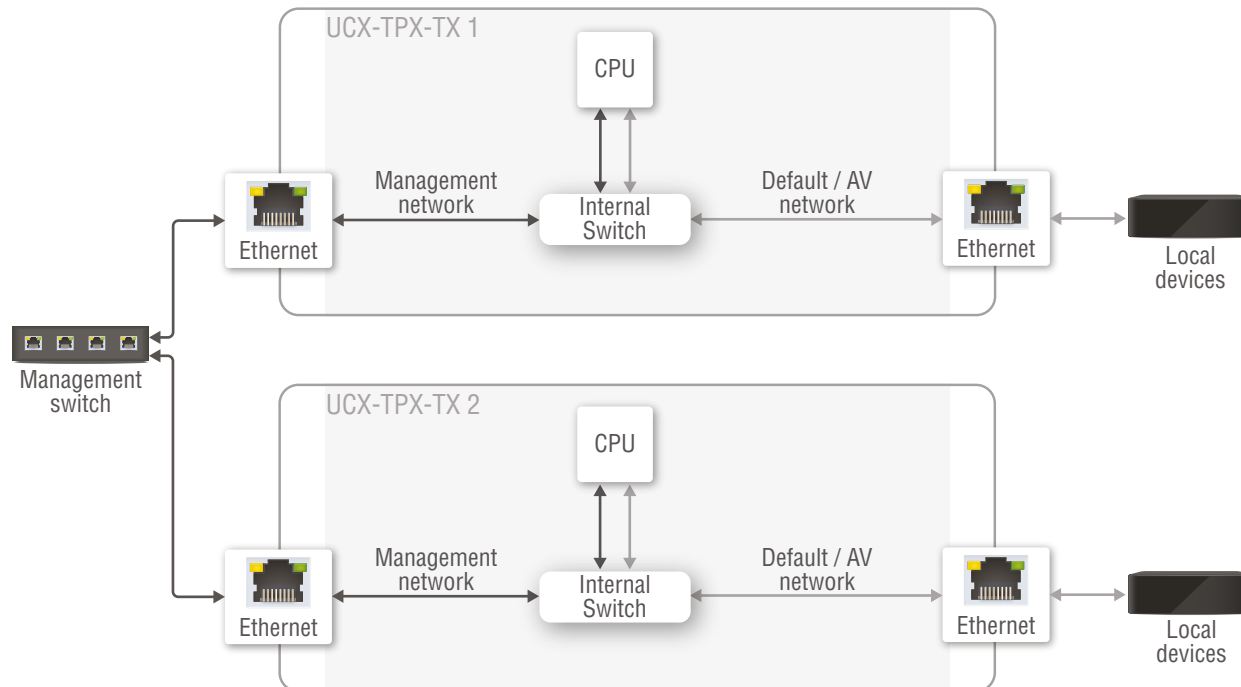
Switch Restrictions - One UCX-TPX-TX device

If the networks are only separated via VLANs, but not outer switches, the switch inside the transmitter will be unable to tell which VLAN to route packets to. To solve this, make sure to connect the ports of the separate networks to physically separate switches.



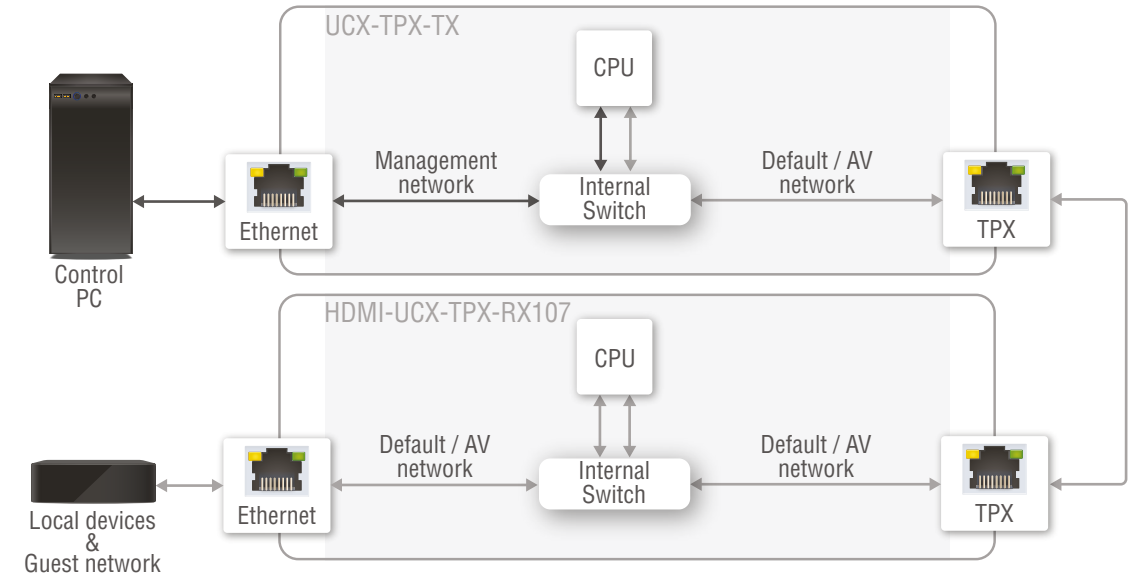
Switch Restrictions - Several UCX-TPX-TX devices

The system can only work properly if the transmitters are only connected to each other through a switch on the management network. If they are also connected to each other through a switch on the Default/AV network at the same time, the switches will be unable to tell which network to route to a MAC address.



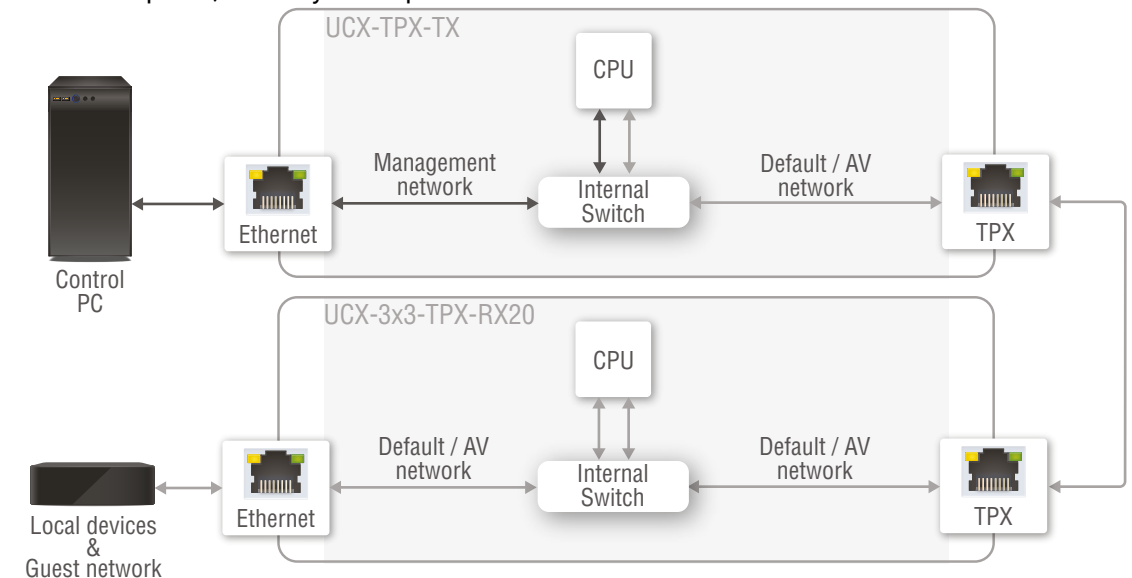
Update Restrictions - UCX-TPX-TX with HDMI-UCX-TPX-RX107

The transmitter is connected to the Management network, and the receiver is connected to the transmitter through the Default/AV network. In this case, updating the receiver remotely is not possible. Either disabling the network separation or a physical connection to the RX is required for the update.



Update Restrictions - UCX-TPX-TX with UCX-3x3-TPX-RX20

The endpoints are connected to each other through the Default/AV network, and either of them can be connected to the Management network, **but only one at a time**. In this case, remotely updating the endpoint **not** connected to the Management network is not possible - a physical connection to the remote endpoint is required for the update, similarly to the previous case.



Management Network

DIFFERENCE: Management network is introduced in UCX-TPX-TX devices from FW version v1.13.0 and in UCX-3x3-TPX-RX20 from FW version v1.6.0.

DEFINITION: Management network is a VLAN Membership setting that creates an Ethernet port that can be used to only connect to the CPU for controlling and updating purposes.

Management network is a special VLAN setting for secure connection to the CPU and for supporting 802.1x authentication. This VLAN separates corporate network from all AV networks, creating a secure environment.

VLAN ID 1000 is reserved for Management, which can be set via LDC ([VLAN Membership](#)), REST API ([Enabling the Management Network on an Ethernet Port](#)) and LW3 ([Enabling the Management Network on an Ethernet Port](#)) as seen below.

INFO: The CPU will appear with the **Main_2** MAC address within the Management network.

WARNING! Please be aware that Management network is only available for UCX-TPX transmitter (TX), UCX-TPN transmitter (TX) models and UCX-3x3-TPX-RX20. It cannot be utilized in a network topology that contains devices different from these, as other extenders do not support Management network.

Setting Up the Management Network

In order to be able to reach the device after setting up the Management network, you need to make sure it will have an IP address. By default, it is set to DHCP, so it will be able to get an IP address if you have a DHCP server. However, without a DHCP server, you need to enable and set a static IP address before you enable the Management network.

These settings currently can only be done via REST API or LW3 commands.

Step 1. To enable Static IP, do the following:

REST API	LW3
➔ request-line: POST http://<ip_address>/api/EXPERIMENTAL/MANAGEMENT/NETWORKINTERFACES/IPV4/STATIC/Enabled ➔ body: true	▶ SET /EXPERIMENTAL/MANAGEMENT/NETWORKINTERFACES/IPV4/STATIC.Enabled=true

Step 2. To set the static IP address and gateway, do the following:

REST API	LW3
➔ request-line: POST http://<ip_address>/api/EXPERIMENTAL/MANAGEMENT/NETWORKINTERFACES/MANAGEMENT/IPV4/STATIC/ConfiguredIpAddress ➔ body: <configured_ip_address>	▶ SET /EXPERIMENTAL/MANAGEMENT/NETWORKINTERFACES/MANAGEMENT/IPV4/STATIC.ConfiguredIpAddress=<configured_ip_address>
➔ request-line: POST http://<ip_address>/api/EXPERIMENTAL/MANAGEMENT/NETWORKINTERFACES/MANAGEMENT/IPV4/STATIC/ConfiguredGatewayAddress ➔ body: <configured_gateway>	▶ SET /EXPERIMENTAL/MANAGEMENT/NETWORKINTERFACES/MANAGEMENT/IPV4/STATIC.ConfiguredGatewayAddress=<configured_gateway>

Step 3. Finally, enable Management network/set Management ID on the desired port:

REST API	LW3
➔ request-line: POST http://<ip_address>/api/V1/MEDIA/ETHERNET/<port>/VlanMembership ➔ body: 1000	▶ SET /V1/MEDIA/ETHERNET/<ethernet_port>.VlanMembership=1000

ATTENTION! Please make sure there is only one port in the Management network.

3

Feature Availability Tables

These tables summarize the availability of a feature based on firmware in the different model groups.

- ▣ [SETTING A PASSWORD](#)
- ▣ [VLAN MODE SETTING](#)
- ▣ [802.1X AUTHENTICATION](#)
- ▣ [CERTIFICATE MANAGEMENT](#)
- ▣ [SESSION MANAGEMENT ON WEBLDC](#)

3.1. Setting a Password

3.1.1. 10-Character Minimum Limit

Device Family	Feature availability from FW	Release date
UCX standalone models	v2.2.0b4	2023-03-30
UCX-TPX/TPN TX models	v1.0.0b5	2023-07-27
UCX-3x3-TPX-RX20 model	v1.0.0b2	2024-06-28

3.1.2. Password History

Device Family	Feature availability from FW	Release date
UCX standalone models	v2.12.0b3	2024-06-03
UCX-TPX/TPN TX models	v1.9.0b9	2024-06-14
UCX-3x3-TPX-RX20 model	v1.0.0b2	2024-06-28

3.2. VLAN Mode Setting

3.2.1. VLAN Presets

Device Family	Feature availability from FW	Release date
UCX standalone models	v1.6.0b3	2022-10-27
UCX-TPX/TPN TX models	v1.0.0b5	2023-07-27
UCX-3x3-TPX-RX20 model	v1.0.0b2	2024-06-28

3.2.2. Custom VLAN

Device Family	Feature availability from FW	Release date
UCX standalone models	v2.9.0b6	2024-01-17
UCX-TPX/TPN TX models	v1.7.0b6	2024-01-16
UCX-3x3-TPX-RX20 model	v1.0.0b2	2024-06-28

3.2.3. Network Separation

Device Family	Feature availability from FW	Release date
UCX standalone models	-	-
UCX-TPX-TX models	v1.7.0b6	2024-01-16
UCX-TPN-TX models	-	-
UCX-3x3-TPX-RX20 model	-	-

3.2.4. Management VLAN

Device Family	Feature availability from FW	Release date
UCX standalone models	-	-
UCX-TPX-TX models	v1.13.0b2	2024-11-19
UCX-TPN-TX models	v1.16.0b6	2025-06-05
UCX-3x3-TPX-RX20 model	v1.6.0b1	2025-07-01

3.3. 802.1x Authentication

Device Family	Feature availability from FW	Release date
UCX standalone models	v2.0.0b5	2023-02-06
UCX-TPX/TPN TX models	v1.0.0b5	2023-07-27
UCX-3x3-TPX-RX20 model	v1.0.0b2	2024-06-28

3.4. Certificate Management

Device Family	Feature availability from FW	Release date
UCX standalone models	v2.2.0b4	2023-03-30
UCX-TPX/TPN TX models	v1.0.0b5	2023-07-27
UCX-3x3-TPX-RX20 model	v1.0.0b2	2024-06-28

3.5. Session Management on WebLDC

Device Family	Feature availability from FW	Release date
UCX standalone models	v2.9.0b6	2024-01-17
UCX-TPX/TPN TX models	v1.7.0b6	2024-01-16
UCX-3x3-TPX-RX20 model	v1.0.0b2	2024-06-28