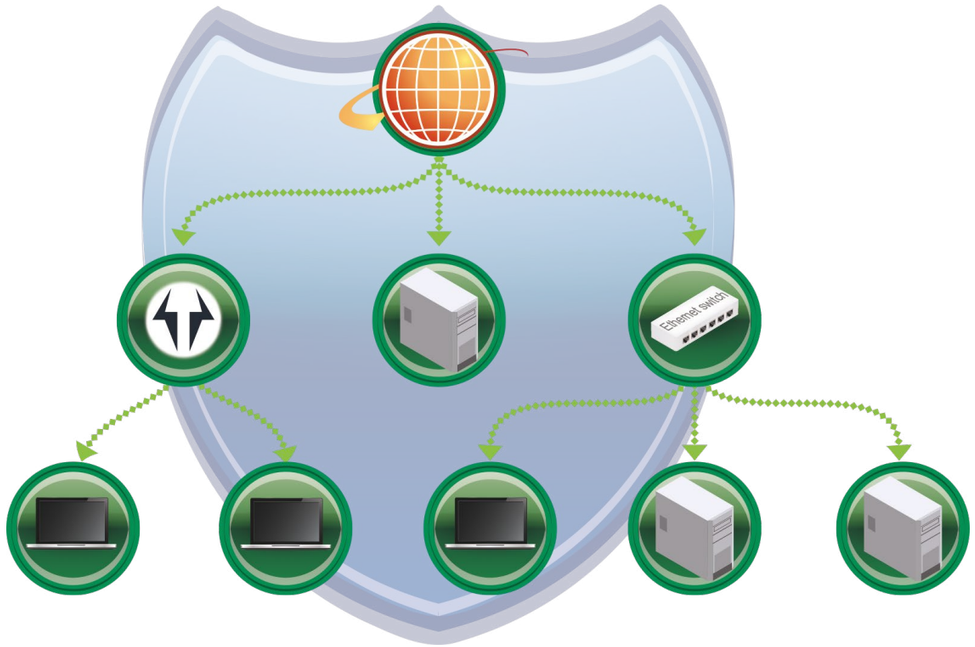
visual engineering
LIGHTWARE

Application Notes



Taurus UCX
Advanced Ethernet Security

v1.2 31-05-2023

Table of Contents

Document Information

Document revision: **v1.2**

Release date: **31-05-2023**

Editor: Nikolett Keindl

Contact Us

sales@lightware.com
+36 1 255 3800

support@lightware.com
+36 1 255 3810

Lightware Visual Engineering PLC.
Peterdy 15, Budapest H-1071, Hungary

www.lightware.com

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.

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)

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

Purpose/ function	Affected software	Protocol	Port number	Port disable option	Encryption	Authentication	Other features
HTTP port (LW3 over WS, REST API, LARA user panels)	LDC, LDU2	TCP	80	✔	✖	✔	FW update, Welcome Screen image upload, Log files, User Scripts Serial messaging
HTTPS port (LW3 over WSS, REST API, LARA management GUI)	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	✖	✖	✖	
Remote IP	LDC, LDU2	UDP	230.76.87.82: 37421	✖	✖	✖	

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

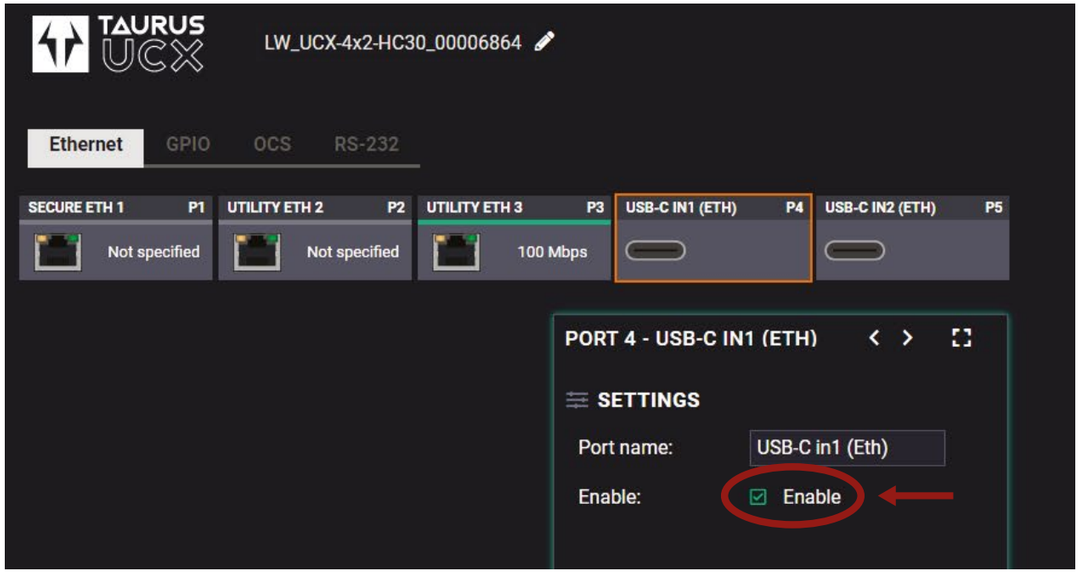
ATTENTION! Be careful when combining the security functions; improper settings may cause malfunction.

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://192.168.0.50/api/V1/MEDIA/ETHERNET/P1/Enabled HTTP/1.1
➔ 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.

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:

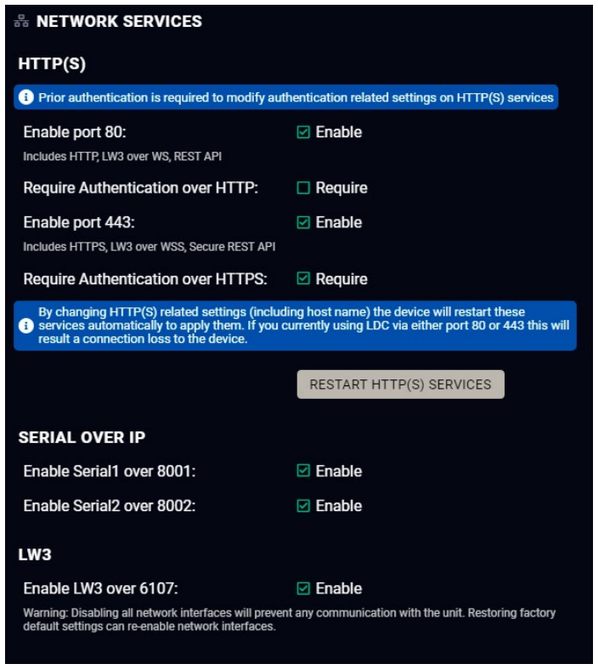
- LW3 over WebSocket (WS, WSS) for LW3 protocol or using LDC for device control
- REST API for device control
- Serial message sending with REST API
- Firmware update
- Uploading WelcomeScreen image
- Uploading UserScripts
- LARA interface
- Downloading logfiles from the device

DIFFERENCE: UserScripts are only available with up to firmware version v1.4.4. 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·HTTP/1.1
➜ body: <status>

➜ status-line: 200 OK
➜ body: <status>

Parameters

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

Example

➜ request-line: POST http://192.168.0.50/api/V1/MANAGEMENT/NETWORK/SERVICES/HTTP/Enabled HTTP/1.1
➜ 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.

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**	
<status>		**true**	The port is enabled.
		false	The port is disabled.

Example

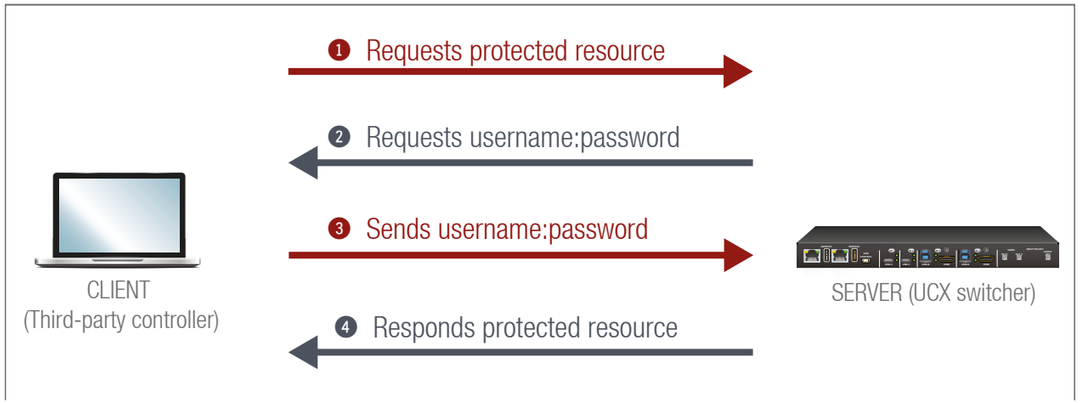
▸ SET /V1/MANAGEMENT/NETWORK/SERVICES/HTTP.Enabled=true
◂ pw /V1/MANAGEMENT/NETWORK/SERVICES/HTTP.Enabled=true

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.

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 v2.2.0, the password must be at least 10 characters long, and any UTF-8 character is allowed.
- 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

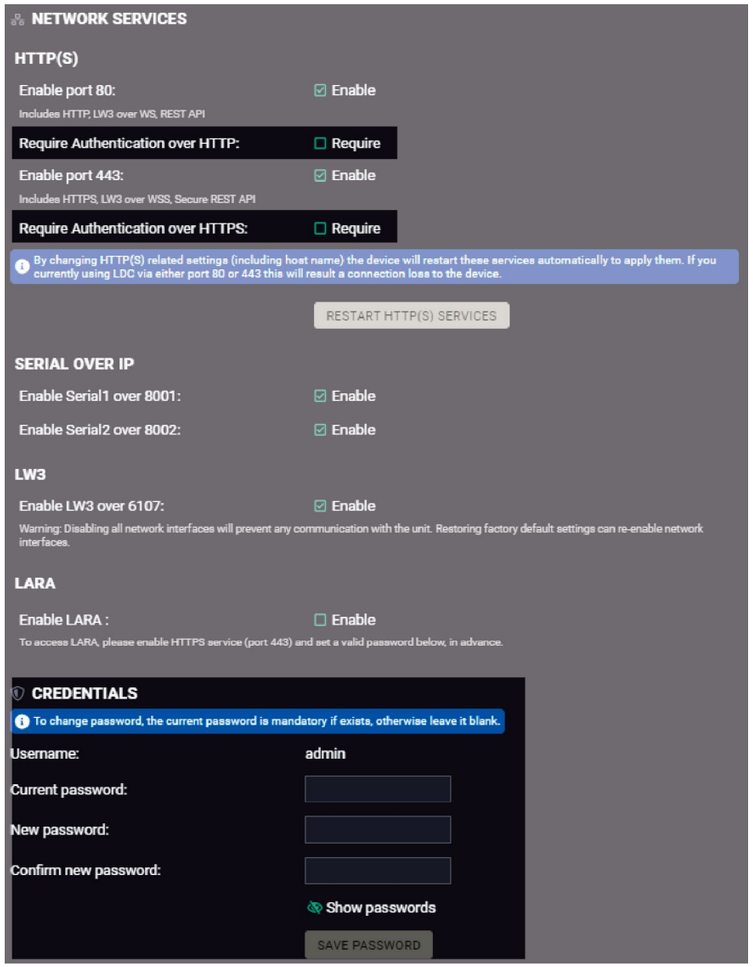
Follow the instructions to set the authentication:

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.



1.4.2. Setting a Password for Authentication via REST API

DIFFERENCE: From firmware version v 2.2.0, The minimum character requirement for the password is 10 characters, and it can contain any UTF-8 character.

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·HTTP/1.1
➜ 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://192.168.0.50/api/V1/MANAGEMENT/NETWORK/AUTH/USER1/setPassword HTTP/1.1
➜ 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, password setting via LW3 is unavailable due to character limitations. From this version on, password setting is only available via LDC or REST API.

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·HTTP/1.1
➜ 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://192.168.0.50/api/V1/MANAGEMENT/NETWORK/SERVICES/HTTP/AuthenticationEnabled HTTP/1.1
➜ 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.

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()
◂ mO /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

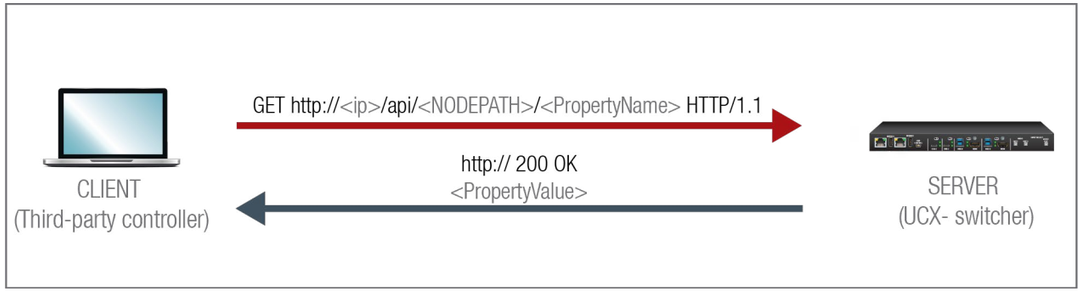
▸ CALL /V1/MANAGEMENT/NETWORK/SERVICES/HTTP:restart()
◂ mO /V1/MANAGEMENT/NETWORK/SERVICES/HTTP:restart=

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

1.5. Encryption (HTTPS, WSS)

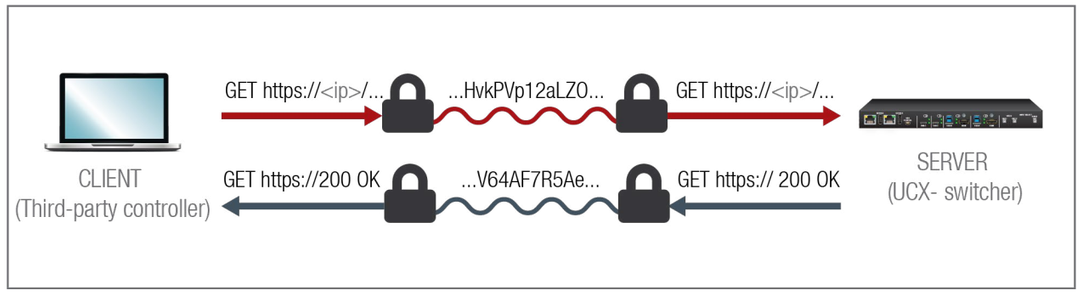
HTTP protocol uses clear text format for data transport. This method allows a third-party to listen in and eavesdrop on the transferred information.

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: This feature is available from firmware version v2.2.0.

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.

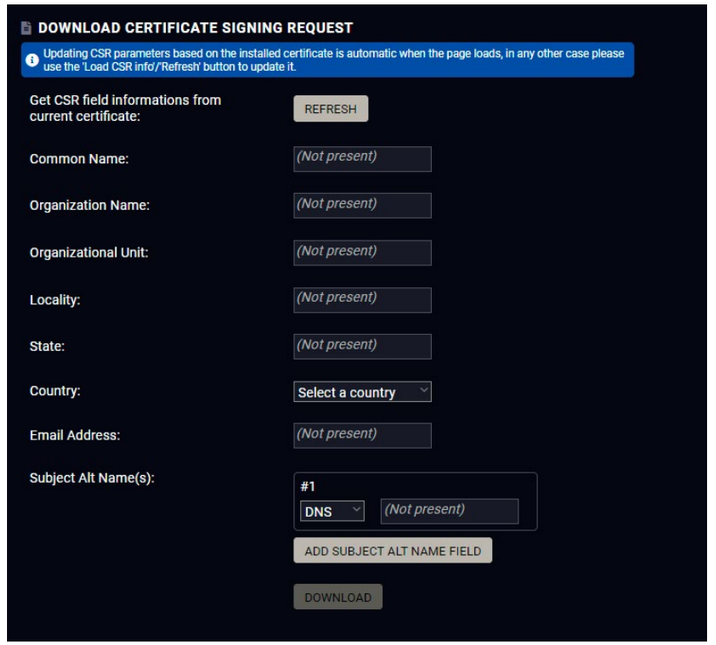
Step 2. Enter the data required for the authentication process. It is important to provide all information related to your organization, because it will be used to verify your identity.

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.



The certificate signing request form

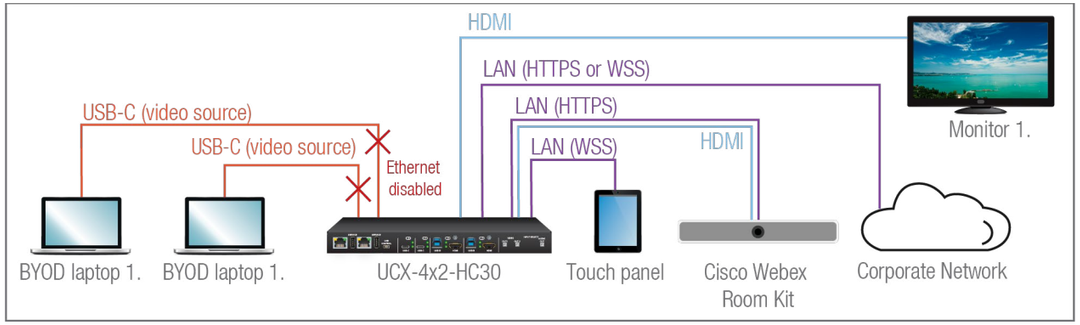
Information	Description	Example
Common Name	The domain name you wish to secure.	www.example.com
Organization Name	The legal name of the company or organization, any suffix included.	Lightware Visual Engineering PLC
Organizational Unit	The name of the internal organizational department/ division.	IT
Locality	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 certfied 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

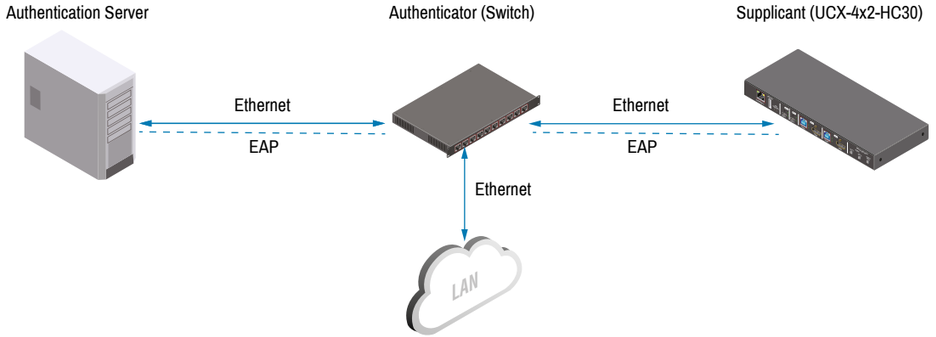
2

Advanced Network Security in UCX Devices

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

2.1. 802.1x Authentication

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.

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 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.

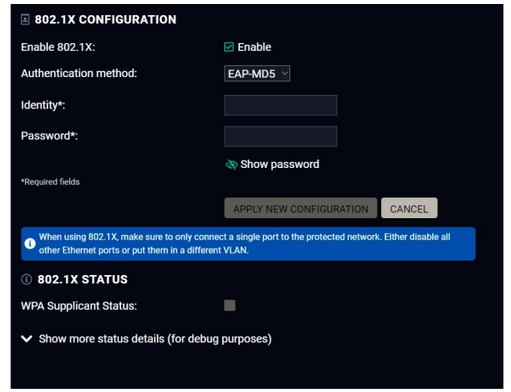
INFO: When updating the firmware of the UCX device, sensitive information (passwords, keys etc.) on the authentication will not be downloaded into the backup file, but it will be retained in the device during the update.

2.1.1. Authentication Process via LDC

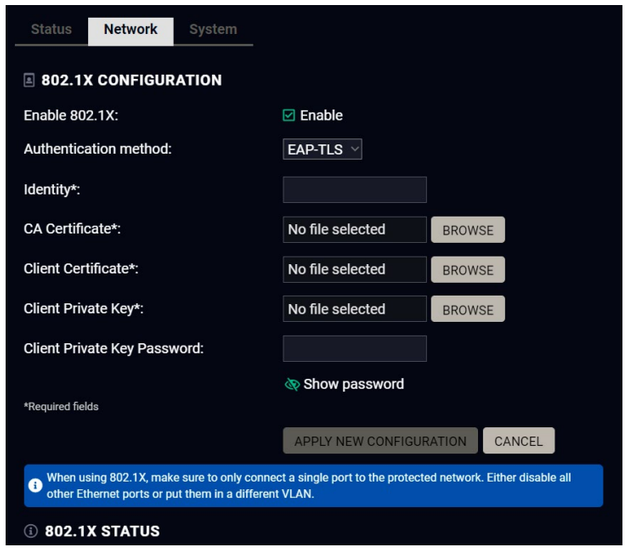
The 802.1x authentication section can be found on the right side of the Settings menu, Network tab.

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**.

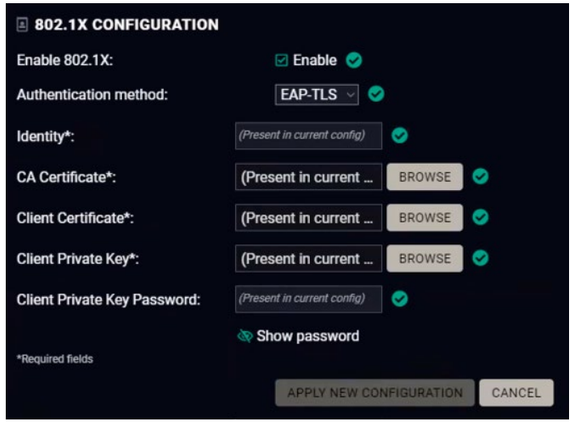
When using EAP-MD5, authentication will require an Identity and a Password to gain access to the secure network.



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



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.

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://192.168.0.110/api/V1/MANAGEMENT/SECURITY/IEEE8021X/Configuration/

➜ response: 200 OK
➜ body: {
➜ "enabled": false
➜ }

2.2.2. Example 1 – Applying the MD5 Method

So:

➜ request: POST http://192.168.0.110/api/V1/MANAGEMENT/SECURITY/IEEE8021X/Configuration/
➜ body:
```
{
    "enabled": true,
    "eap": "MD5",
    "identity": "John",
    "password": "myPassword"
}
```
➜ response: 200 OK
➜ body: OK

2.2.3. Example 2 – Applying the TLS Method

➜ request: POST http://192.168.0.110/api/V1/MANAGEMENT/SECURITY/IEEE8021X/Configuration/
➜ body:
```
{
    "enabled": true,
    "eap": "TLS",
    "identity": "John",
    "caCert": "-----BEGIN CERTIFICATE-----\n
        <CA certificate in PEM format>
        -----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 explanantion about the different options available through the Advanced Ethernet Security feature.

DIFFERENCE: The advanced ethernet security feature is available only from FW package v1.6.0.

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:

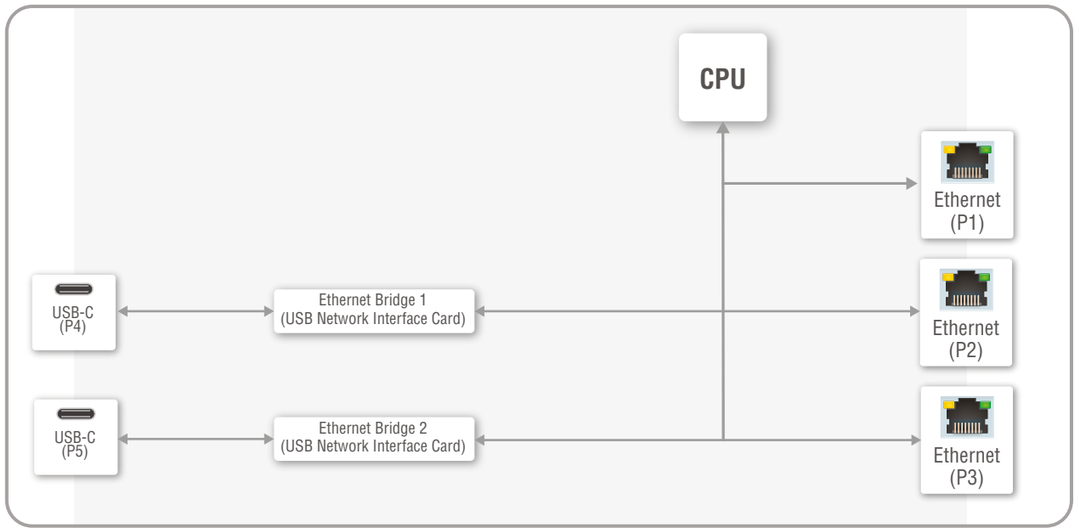
- **Transparent**: this is the default mode, with a network openly used by Taurus and the BYOD devices,
- **Separated BYOD**: the network provided for the BYOD devices is separated from the control network
- **Dedicated**: each connected BYOD device receives an indepentent network.

2.3.1. Application

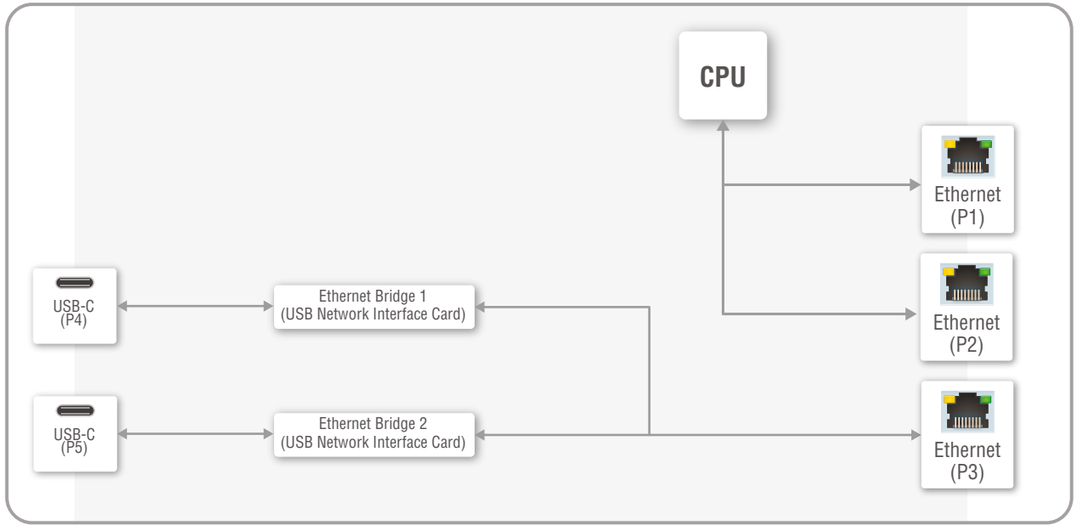
These port diagrams offer a simple breakdown of the different modes of the feature.

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

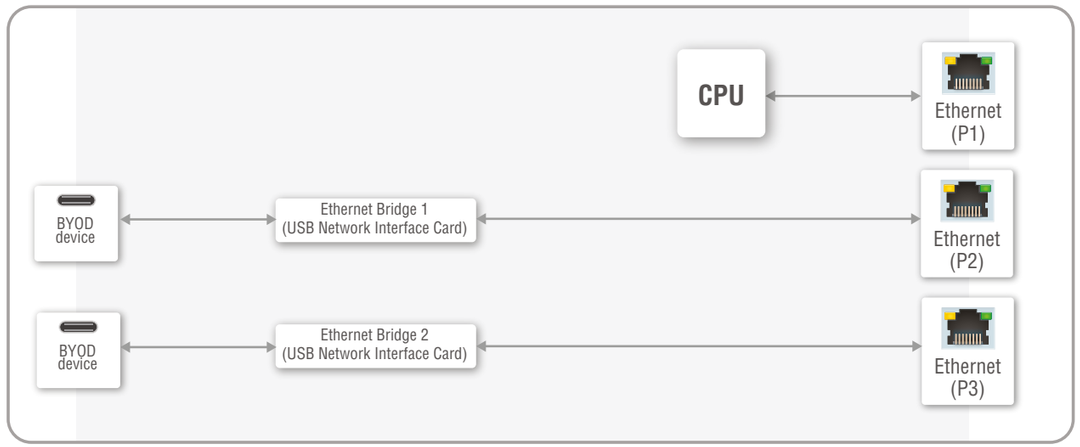
Transparent



Separated BYOD



Dedicated



2.3.2. 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.

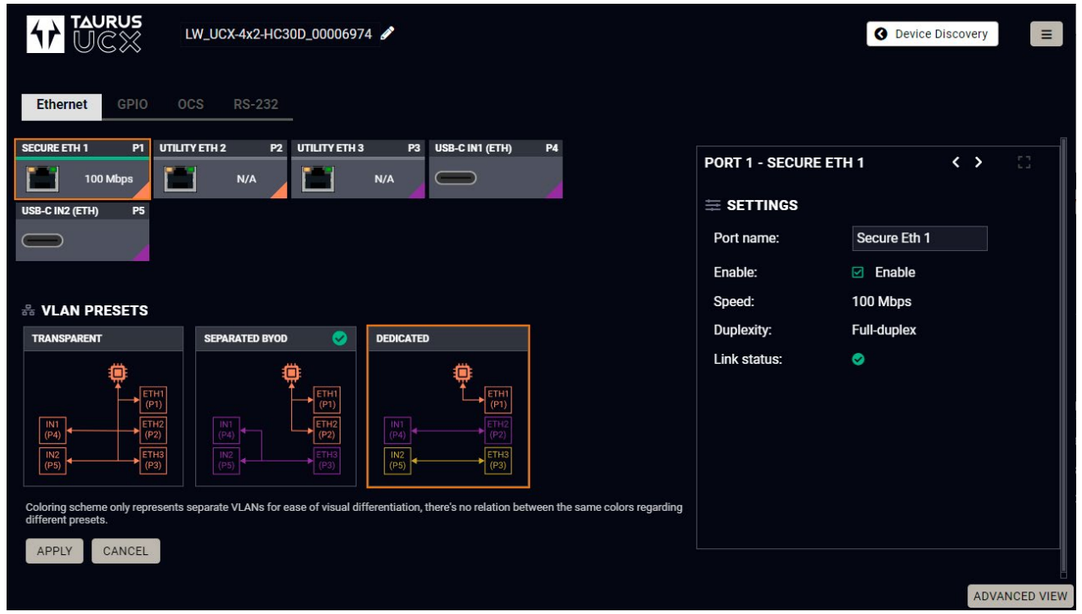
Step 3. Here you can choose the desired mode via the diagrams. Default is the **Transparent** mode, you can choose a different mode by clicking on it, and the click on the **Apply** button. The change is immediate, there is no need for reboot.

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.

Transparent is the default VLAN preset

Active VLAN preset is Separated BYOD



Active VLAN preset is Dedicated

Setting the mode in advanced view

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.

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

2.3.3. 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://192.168.0.125/api/V1/MEDIA/ETHERNET.VlanPreset HTTP/1.1
➜ body: transparent

➜ header: 200 OK
➜ body: transparent

Separating the BYOD Network from the Main Line

➜ header: POST http://192.168.0.125/api/V1/MEDIA/ETHERNET.VlanPreset HTTP/1.1
➜ body: separate byod

➜ header: 200 OK
➜ body: separate byod

Creating a Separate Network for Each BYOD Device

➜ header: POST http://192.168.0.125/api/V1/MEDIA/ETHERNET.VlanPreset HTTP/1.1
➜ body: dedicated

➜ header: 200 OK
➜ body: dedicated

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

2.3.4. 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.