



Lexmark<sup>TM</sup>

# Cloud Print Management ELATEC TCP3

---

## Configuration Guide

# Contents

**Overview..... 3**

    Overview..... 3

**Getting started..... 4**

    Deployment readiness checklist.....4

    Setting up a TCP3 device..... 5

**Configuring the TCP3 device..... 6**

    Accessing the TCP3 device Embedded Web Server (EWS).....6

    Configuring the TCP3 device using the EWS..... 10

    Configuring the TCP3 device using the TCP3 Config utility window..... 12

    Setting up authentication with Lexmark Cloud Services..... 14

    Obtaining the client ID and client secret.....14

    Configuring the TCP3 device OAuth settings.....16

    Managing certificates..... 19

    Saving a TCP3 device configuration..... 21

**Getting help.....23**

**Notices..... 24**

    Edition notice.....24

**Index.....25**

# Overview

## Overview

The ELATEC TCP3 device allows third-party printers and Lexmark printers that are not capable of Lexmark Embedded Solutions to use Lexmark Cloud Print Management services. The ELATEC TCP3 adapter is a network device, designed to be connected between the customer network and the printer. It also provides a USB connection for badge or card readers. The TCP3 device handles all user badge or card authentication and passes the user's print jobs from Lexmark Cloud Print Management service to the printer.



**Note:** For additional information, go to the latest *TCP3 Technical Manual* included in the TCP3 administrator pack at <https://www.elatec-rfid.com/en-us/tcp-adminpack-overview>.

# Getting started

## Deployment readiness checklist

Before you begin, make sure that you have the following:

- ☐ Cloud Print Management enabled in your organization.
- ☐ A Cloud Services user account with the Organization Administrator role.
- ☐ The printer to be used with the TCP3 device must be set for DHCP before connecting to the device.
- ☐ The client ID and client secret specific to your organization. For more information, see [“Obtaining the client ID and client secret” on page 14.](#)

- ☐ The following ELATEC components:
  - TCP3 adapter
  - Network cable supplied with the TCP3 adapter
  - Power adapter

**Note:** As power-adapter requirements vary in different countries, contact Professional Services to make sure that you have the required adapter.

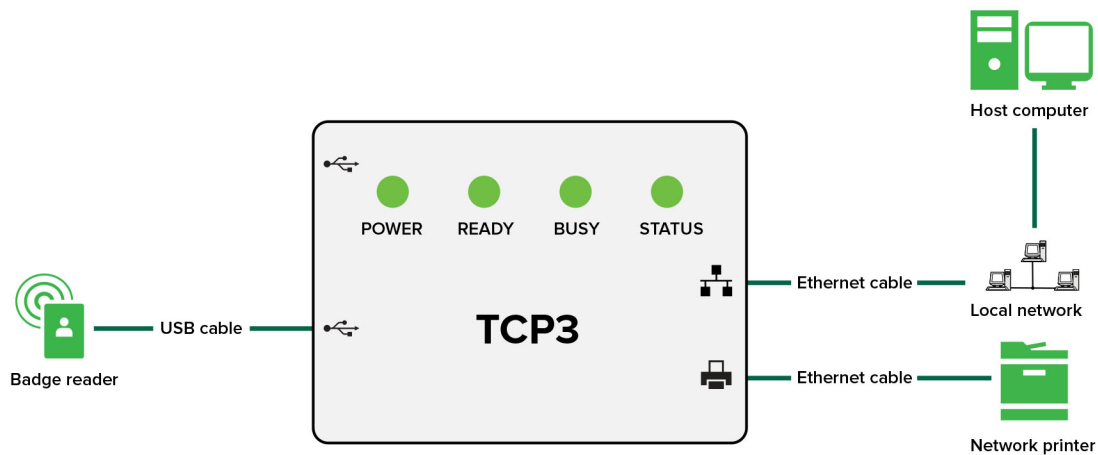
- Badge reader holder
- Supported badge reader

**Note:** The badge reader is available in a separate box as a part of the bundle.

- All ELATEC TWN4 readers are supported.
- For more information, see the latest *TCP3 Technical Manual* included in the TCP3 administrator pack at <https://www.elatec-rfid.com/en-us/tcp-adminpack-overview>.

- ☐ An Ethernet cable to connect the TCP3 device to a network (not included in the bundle).

## Setting up a TCP3 device



- 1 Unpack the device.
- 2 Connect the Ethernet cable from your local network to the TCP3 device.
- 3 Connect the Ethernet cable from the printer to the TCP3 device.

**Note:** The Ethernet port on the TCP3 device is marked with a printer icon.

- 4 Connect the ELATEC USB badge reader to the TCP3 device.

**Note:** The TCP3 device has two USB ports. You can connect the badge reader to either of them.

- 5 Connect the power cord to the TCP3 device, and then plug it into the electrical outlet.

**CAUTION—POTENTIAL INJURY:** To avoid the risk of fire or electrical shock, connect the power cord to an appropriately rated and properly grounded electrical outlet that is near the product and easily accessible.

### Notes:

- When the device is ready, the green indicator lights for POWER, READY, and STATUS come on. This process can take several minutes.
- The TCP3 device assigns an IP address to the printer. The IP address is used only by the TCP3 device. To access the Embedded Web Server (EWS) of the printer, type the IP address of the TCP3 device in a browser. For more information, see [“Obtaining the IP address of the TCP3 device” on page 6](#).

# Configuring the TCP3 device

## Accessing the TCP3 device Embedded Web Server (EWS)

You can access the Embedded Web Server of the TCP3 device using one of the following methods:

- Using a web browser and the TCP3 device IP address

**Note:** We recommend using the EWS method when setting up one device at a time.

- Using the TCP3 Config utility to open the TCP3 device EWS
- Using the TCP3 Config utility window

**Notes:**

- We recommend using the TCP3 Config utility window when setting up multiple devices with the same configuration. In this method, configuration files can be created and pushed to multiple TCP3 devices.
- This method is also used to discover TCP3 devices on a network when their IP addresses are unknown. For more information, see the *TCP3 Technical Manual* included in the TCP3 administrator pack at <https://www.elatec-rfid.com/en-us/tcp-adminpack-overview>.

### Obtaining the IP address of the TCP3 device

- 1 On the TCP3 device, press and hold the **Input** button near the USB ports until the BUSY light blinks three times, and then release it.
- 2 From the network settings page that is printed, locate the IP address of the TCP3 device. The IP address appears under the **HOST NETWORK** column in the **Address** row.

**Notes:**

- The TCP3 device uses DHCP to get an IP address from the local network. This IP address is used to access the EWS of both the printer and the TPC3 device.
- The TCP3 device EWS can be accessed using the IP address and port 81. Open a web browser, and then type **http://<TCP3\_device\_ip>:81** in the browser.
- The printer EWS can be accessed using just the IP address. Open a web browser, and then type **http://<TCP3\_device\_ip>** in the browser.

### Logging in to the TCP3 device EWS

- 1 Open a web browser, and then type **http://<TCP3\_device\_ip>:81** in the browser.

**Note:** <TCP3\_device\_ip> is the IP address of the TCP3 device.

- 2 Type the user name and password.

**Notes:**

- The default user name is admin, and the default password is the last eight characters in the host MAC address. The host MAC address is printed on the back of the TCP3 device. For example, if the host MAC address is **20:1D:03:01:7E:1C**, then the default password is **03017E1C**.
- The password is case-sensitive and must be typed in uppercase.

## Accessing the TCP3 device EWS using a web browser and IP address

To access the EWS of the TCP3 device using a web browser, you must get the IP address of the TCP3 device. For more information, see [“Obtaining the IP address of the TCP3 device” on page 6](#).

When you have the IP address of the TCP3 device, you can log in to the device EWS. For more information, see [“Logging in to the TCP3 device EWS” on page 6](#).

## Accessing the TCP3 device using the TCP3 Config utility

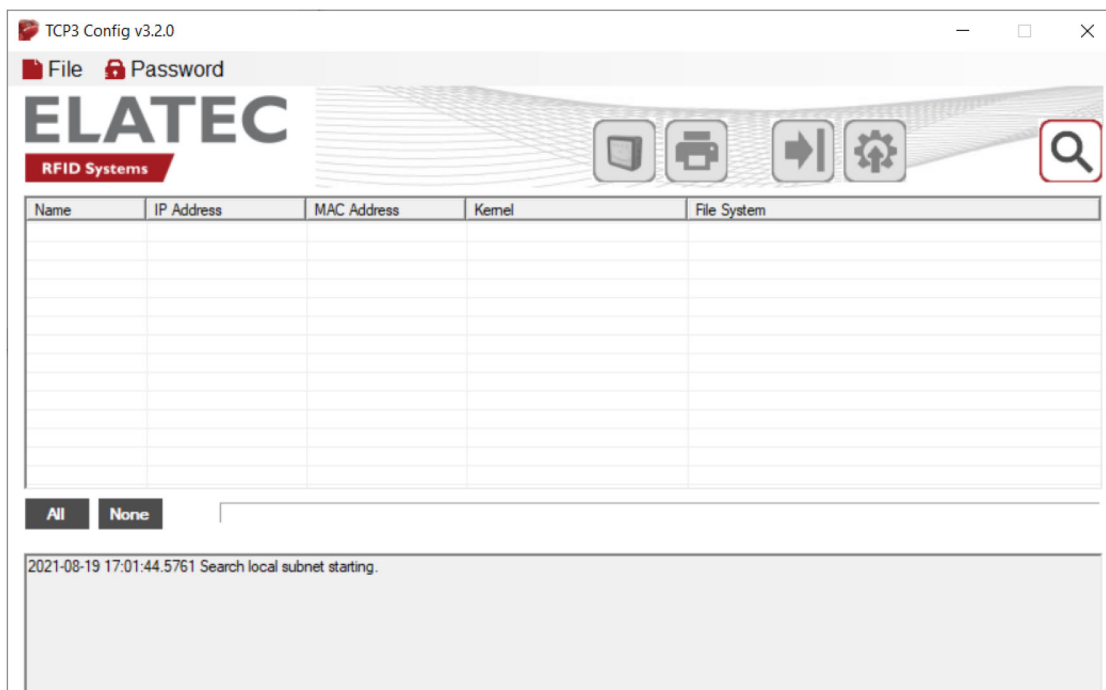
The TCP3 Config utility (TCP3Config.exe) is used to discover, configure, save, and push configurations to TCP3 devices.

### Discovering TCP3 adapters on the network

- When started, the TCP3 Config utility automatically performs a local subnet search for TCP3 devices.
- You can search for other subnets using cross-subnet discovery.

#### TCP CLIENT CONFIGURATION

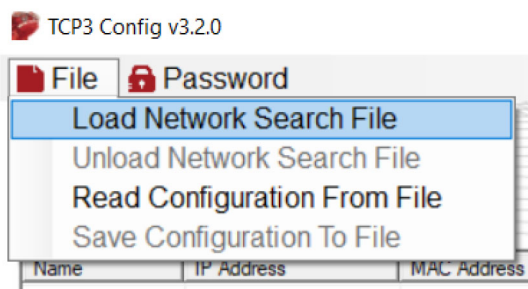
☐ Connect to a Remote Host



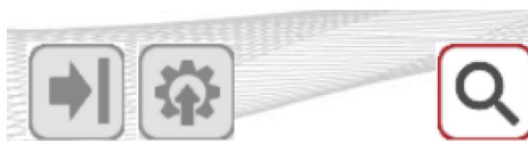
## Discovering across subnets

You can search other network subnets by creating a search file. The search file is a TXT file containing one or more IP addresses or search criteria. Each line of text in the file must have only one IP address or one search criteria.

- 1 On the TCP3 Config utility, click **File > Load Network Search File**.



- 2 Click **Start Discovery**.



**Note:** The search returns a list of all the discovered TCP3 devices.

The screenshot shows the ELATEC RFID Systems application interface. The 'File' menu is open, and 'Password' is highlighted. The application title 'ELATEC' and 'RFID Systems' are visible. A toolbar contains icons for a monitor, printer, left arrow, gear, and magnifying glass. Below the toolbar is a table with the following data:

| Name           | IP Address    | MAC Address       | Kernel           | File System                      |
|----------------|---------------|-------------------|------------------|----------------------------------|
| TCP3CS410      | 10.199.98.184 | 20:1D:03:01:7D:C8 | 4.14.16+gdfc1b13 | STD3.0.3.0.BETA-16-23-08-07-2021 |
| TCP3CanonMF... | 10.199.98.194 | 20:1D:03:01:7D:94 | 4.14.16+gdfc1b13 | STD3.0.3.0.BETA-16-23-08-07-2021 |

Below the table are buttons for 'All' and 'None'. At the bottom, a log window displays the following messages:

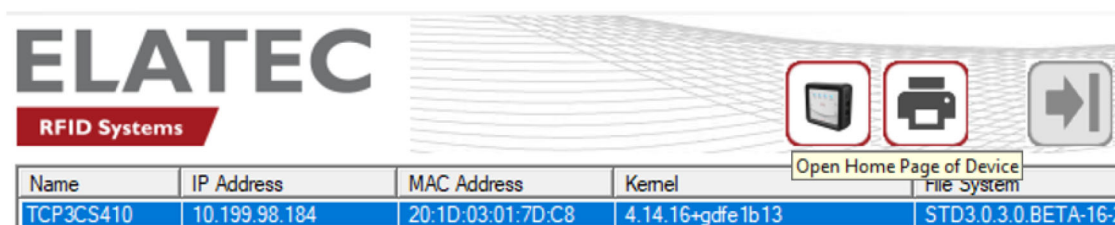
```

2021-08-10 13:20:06.8447 Search local subnet starting.
2021-08-10 13:20:59.8939 Search complete.
2021-08-10 13:21:53.6267 Loading network search file C:\Documents\Elatec\IP_Address_Search.txt
2021-08-10 13:21:58.6034 Search with network file starting.
2021-08-10 13:22:32.9367 Found device 10.199.98.184
2021-08-10 13:22:33.8921 Found device 10.199.98.194
2021-08-10 13:22:50.6912 Search complete.
  
```

At the bottom of the application, there is a copyright notice '© 2019 Elatec GmbH All Rights Reserved', the website 'www.elatec.com', and a 'Clear Log' button.



- 3** Select a TCP3 device, and then click **Open Home Page of Device**.



**Note:** The TCP3 home page opens in a web browser. Type the user name and password to access the page. For more information, see [“Logging in to the TCP3 device EWS” on page 6](#).

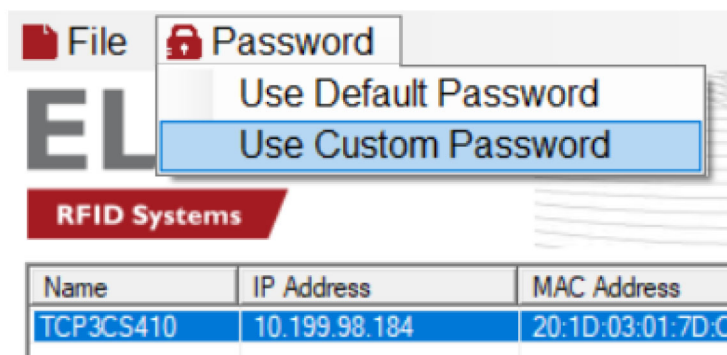
## Accessing the TCP3 Config utility configuration window

TCP3 devices can be configured using the configuration window on the TCP3 Config utility. The configuration window is similar to the TCP3 device EWS. Use this window of the utility to configure TCP3 devices and save the configurations for future deployment.

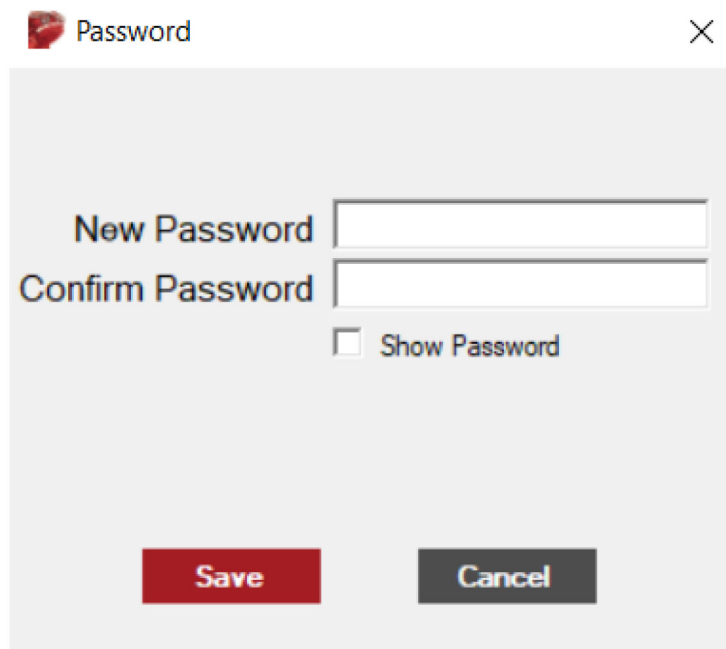
Use the default password to access the TCP3 Config utility window. If the default password has been changed, then set the new password of the TCP3 device within the TCP3 Config utility.

**Note:** The Use Custom Password is used only when the default password is not being used.

- 1** From the Password menu, select **Use Custom Password**.



- 2 Type the new password and then confirm it.

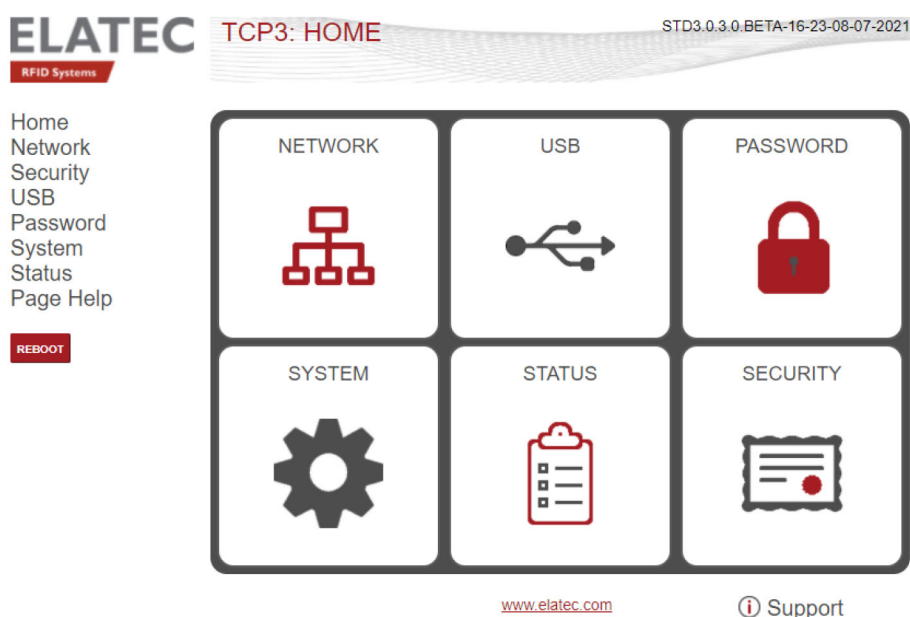


A dialog box titled "Password" with a close button (X) in the top right corner. It contains two input fields: "New Password" and "Confirm Password". Below the "Confirm Password" field is a checkbox labeled "Show Password". At the bottom, there are two buttons: "Save" (red) and "Cancel" (dark gray).

- 3 Double-click the entry of the TCP3 device to open the configuration window.

## Configuring the TCP3 device using the EWS

You can configure the TCP3 device using the EWS. For more information on accessing the TCP3 EWS, see [“Accessing the TCP3 device Embedded Web Server \(EWS\)” on page 6](#).



## Setting SYSTEM TIME using the EWS

- 1 From the System menu, in the SYSTEM TIME section, set the **Time Zone**.

SYSTEM TIME

System Time Aug,03,2021 09:16:46 AM

Time Zone

Please reboot the converter once all of the configuration items have been addressed.

LOAD DEFAULTS APPLY

- 2 Click **APPLY**.

- 3 Click **REBOOT**.

**Note:** After rebooting, wait for the TCP3 device to get ready. When the device is ready, the green indicator lights for POWER, READY, and STATUS come on.

## Updating the TCP3 firmware using the EWS

The firmware of the TCP3 device must be version 3.0.3.0 or later. To get the latest firmware, download the TCP3 administrator pack at <https://www.elatec-rfid.com/en-us/tcp-adminpack-overview>.

- 1 From the System menu, in the FIRMWARE section, update the firmware, if necessary.

FIRMWARE

TCP CONVERTER

Current Version STD3.0.3.0.BETA-16-23-08-07-2021

Select TCP Firmware (.zip)

Drag-n-drop file here  
or click to browse.

- 2 Click **APPLY**.

**Note:** The firmware must be submitted as a compressed ZIP file. The file name has the format of STD<version\_number>.zip.

## Configuring the TCP3 device using the TCP3 Config utility window

You can configure the TCP3 device using the TCP3 Config utility window. For more information on accessing the EWS, see [“Accessing the TCP3 device Embedded Web Server \(EWS\)”](#) on page 6.

The screenshot shows the 'Configuration' window with tabs for Network, USB, System, and Password. The 'Network' tab is active, displaying settings for Name Resolution, Printer IP, Host IP, and Watchdog.

**Configuration**

Network | USB | System | Password

**Name Resolution**

Name: TCP3CS410

Workgroup: WORKGROUP

**Printer: IP Settings**

Address: 192.168.50.100

**Host: IP Settings**

☒ DHCP ☐ Static IP

Address: 10.199.98.184

Netmask: 255.255.252.0

Gateway: 10.199.96.1

☐ Configure DNS Manually

DNS0: 157.184.56.1

DNS1: 10.199.21.38

☐ Configure WINS Manually

WINS0: 4.4.4.4

WINS1: 8.8.8.8

☐ Configure NTP Manually

Main NTP Server:

Backup NTP Server:

**Watchdog**

|                               | Host                                | Printer                             |
|-------------------------------|-------------------------------------|-------------------------------------|
| Ping Interval                 | 1 - 30 Minutes<br>5                 | 1 - 30 Minutes<br>1                 |
| Number of Tries Before Reboot | 0 - 30 Tries<br>3                   | 0 - 30 Tries<br>-1                  |
| Enable Watchdog               | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Watchdog IP Address           |                                     |                                     |

Apply Save Cancel

# Setting the system time using the TCP3 Config utility window

1 From the System menu, set the **Time Zone**.

Configuration

Network | USB | **System** | Password

Setup

☐ Record event on Syslog Server

IP/Hostname

Port

Send Events

☒ Power is applied

☒ Send DHCP Event

☒ Card reader is connected/disconnected

☒ Configuration is changed

System Time

Time Zone

Apply Save Cancel

2 Click **Apply**.

**Note:** The device reboots. The Log window on the TCP3 Config home screen shows the status of the reboot.

# Updating the TCP3 device firmware using the TCP3 Config utility window

The TCP3 device firmware must be version 3.0.3.0 or later. To get the latest firmware, download the TCP3 administrator pack at <https://www.elatec-rfid.com/en-us/tcp-adminpack-overview>.

The TCP3 device firmware must be submitted as a compressed ZIP file. The file name has the format of STD.zip.

1 Select one or more TCP3 devices, and then click **Upload Firmware to Selected Devices**.

2 Select the firmware to install.

| Name      | IP Address    | MAC Address       | Kemel            | File System                      | Upload Firmware to Selected Devices |
|-----------|---------------|-------------------|------------------|----------------------------------|-------------------------------------|
| TCP3CS410 | 10.199.98.184 | 20:1D:03:01:7D:C8 | 4.14.16+gdfc1b13 | STD3.0.3.0.BETA-16-23-08-07-2021 |                                     |

## Setting up authentication with Lexmark Cloud Services

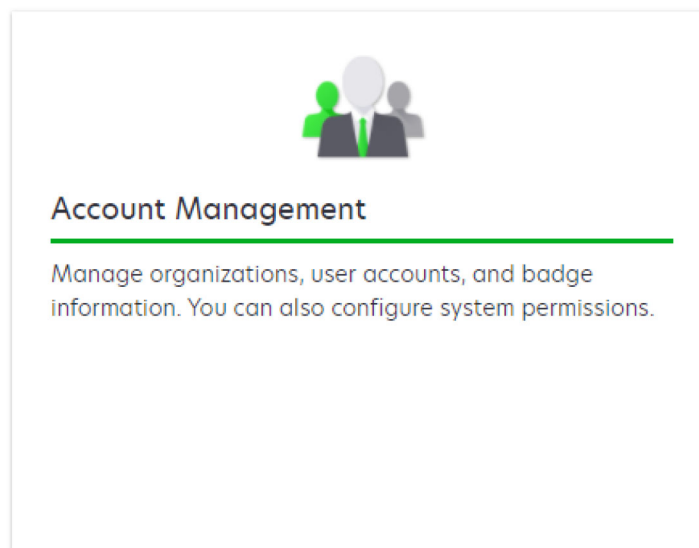
Lexmark Cloud Services uses an industry-standard OAuth credentials flow. The TCP3 device is provided with the URLs for the authentication interface, and a client ID and a client secret, specific to the organization. The client ID and client secret are obtained from a Device Authentication application in the Account Management portal. The default device authentication application for your organization can be used for this purpose. For more information, see [“Obtaining the client ID and client secret” on page 14](#).


An authentication application can be created for all TCP3 devices, or a separate device authentication application can be created for each TCP3 device.

## Obtaining the client ID and client secret

The client ID and client secret must be obtained from the Account Management service in the Cloud Services portal. A user account with Organization Administrator role is required.

- 1 Open a web browser, and then access the Lexmark Cloud Services dashboard.
- 2 Click the **Account Management** card.



**Note:** If the card is not available in the dashboard, then click  on the upper-right corner of the page, and then click **Account Management**.

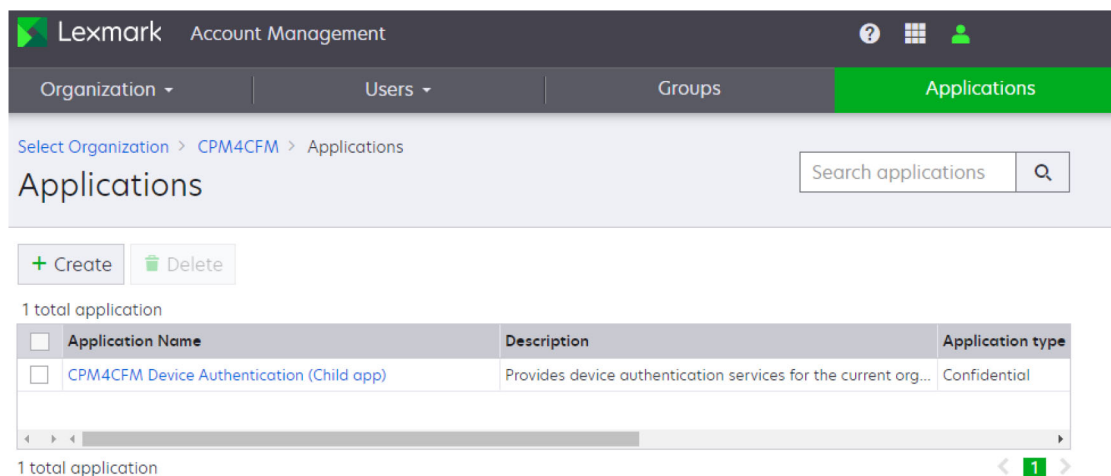
- 3 Select the organization, and then click **Next**.

Select Organization

Phoenix MPS (My Organization)

Next

#### 4 Click the **Applications** tab.



#### 5 In the Search applications field, type **Device Authentication (Child app)**, and press **Enter**.

#### 6 In the Application Name list, click the **<organization\_name>Device Authentication (Child app)** link.

#### 7 From the Device Authentication page, in the Permission section, make sure that badges-auth is listed under Scopes.

### Permissions

1 total permission

| Application Name                                     | Client ID    | Scopes      |
|--|--------------|-------------|
| Access Control and Identity Management Service Suite | msa-identity | badges-auth |

**Note:** In the OAuth Settings section, Client ID and Client Secret appear. Use the same client ID and client secret for configuring TCP3 OAuth settings.

### OAuth Settings

#### Client ID

device-auth-3f263d8a-76e5-4dd4-94c7-e0b167462e96

#### Client secret

cb30d882e6459b48401a33dede01b51caa57f7437e293608f828f96aad1630ce

# Configuring the TCP3 device OAuth settings

## Configuring the OAuth settings from the TCP3 device EWS

If you have the TCP3 device IP address, then you can access the EWS to configure the OAuth settings. For more information, see [“Obtaining the IP address of the TCP3 device” on page 6](#).

- 1 Open a web browser, and then type **http://<TCP3\_device\_ip>:81** in the address field.

**Note:** <TCP3\_device\_ip> is the IP address of the TCP3 device.

- 2 Click **USB**.

- 3 In the TCP/IP CONFIGURATION section, select **TCPConv as Client**.

### TCP/IP CONFIGURATION

☐ **TCPConv as Server**

☒ **TCPConv as Client**

- 4 In the TCP CLIENT CONFIGURATION section, select **Connect to a Web Service**.

**Note:** The TCP CLIENT CONFIGURATION settings allow communication between the third-party printer and the Lexmark Cloud Services through the TCP3 device.

- 5 In the Authentication menu, make sure that **OAuth Client Credentials** is selected.

- 6 Type the client ID and client secret. For more information, see [“Obtaining the client ID and client secret” on page 14](#).

#### Notes:

- The client ID and client secret are specific to an organization.
- The client ID and client secret help Lexmark to identify the organization in which the TCP3 device is registered.

- 7 Configure the URLs for OAuth and web service. The TCP3 device prefixes the URLs with **https://**, which is retained when configuring the following values:

- **Token Grant Access**—**idp.<data\_center>.iss.lexmark.com/oauth/token**
- **Token Revoke Access**—**idp.<data\_center>.iss.lexmark.com/oauth/revoke**
- **Web Service Address**—**apis.<data\_center>.iss.lexmark.com/cpm/print-management-service/v3.0/documents/release?maxDocumentsToRelease=<integer>**

#### Notes:

- Replace **<data\_center>** with **eu** or **us**, depending on whether the organization is in Europe or North America.
- In the Web Service Address value, the value assigned to the optional parameter **maxDocumentsToRelease** sets the number of jobs to be released when the user authenticates. The default value is 10. Set the value to 1 to release the latest print job only.

- 8 In the TCP Unique Device ID field, type the serial number of the printer.



**9** Make sure that **Validate Server's Certificate** is selected.

**10** Click **Apply**.

**Note:** The client ID and client secret disappear to reduce the chances of disclosure.

**TCP CLIENT CONFIGURATION**

☐ **Connect to a Remote Host**

Remote Hostname or IP Address

Remote Port

**4** ☒ **Connect to a Web Service**

**5** Authentication

Credentials exist, enter new credentials to override.

**6** Client ID

Client Secret

Token Grant Address

**7** Token Revoke Address

Web Service Address

**8** TCP Unique Device ID

TCP Device Auth Code

☒ **Send Data via SSL/TLS**

**9** ☒ **Validate Server's Certificate**

**11** Click **REBOOT**.

## Configuring OAuth settings from TCP3 Config utility window

You can configure the TCP3 OAuth settings using the TCP3 Config utility window.

**1** Access the TCP3 Config utility window. For more information, see [“Accessing the TCP3 Config utility configuration window” on page 9](#).

**2** Click **USB**.

**3** In the TCP/IP Configuration section, select **TCP as Client**.

Configuration

Network **USB** System Password

Representation of Keyboard Newline

☐ Carriage Return ☐ Line Feed

☒ Carriage Return + Line Feed

TCP/IP Configuration

☐ TCP as Server **3** ☒ TCP as Client

TCP Client Configuration

☐ Connect to a Remote Host

Remote Hostname or IP 192.168.0.1

Remote Port 7777

**4** ☒ Connect to a Web Service

**5** Web Service Authentication OAuth Client Credentials

Credentials exist, enter new credentials to override.

**6** Client ID

Client Secret

**7** OAuth Token Grant Address https://idp.eu.iss.lexmark.com/oauth/token

OAuth Token Revoke Address https://idp.eu.iss.lexmark.com/oauth/revoke

Web Service Address https://apis.eu.iss.lexmark.com/cpm/print-management-service/v3.0.

**8** TCP Unique Device ID

TCP Device Auth Code

**9** ☒ Send Data via SSL/TLS

☒ Validate Server's Certificate

Standard operation is to connect and send all card data at once, then disconnect.

☒ Connect on any character

☐ Connect on this character 48 Decimal

☒ Send connect character

☒ Disconnect on this character 13 Decimal

☒ Send disconnect character

Disconnect timeout 10 Seconds

**10** Apply Save Cancel

**4** In the TCP CLIENT CONFIGURATION section, select **Connect to a Web Service**.

**5** In the Web Service Authentication menu, make sure that **OAuth Client Credentials** is selected.

**6** Type the client ID and client secret. For more information, see [“Obtaining the client ID and client secret” on page 14](#).

**Notes:**

- The client ID and client secret are specific to an organization.
- The client ID and client secret help Lexmark to identify the organization in the which the TCP3 device is registered.

**7** Configure the URLs for OAuth and web service. The TCP3 device prefixes the URLs with **https://**, which is retained when configuring the following values:

- **OAuth Token Grant Access**—`idp.<data_center>.iss.lexmark.com/oauth/token`
- **OAuth Token Revoke Access**—`idp.<data_center>.iss.lexmark.com/oauth/revoke`
- **Web Service Address**—`apis.<data_center>.iss.lexmark.com/cpm/print-management-service/v3.0/documents/release?maxDocumentsToRelease=<integer>`

**Notes:**

- Replace **<data\_center>** with **eu** or **us**, depending on whether the organization is in Europe or North America.
- In the Web Service Address value, the value assigned to the optional parameter **maxDocumentsToRelease** sets the number of jobs to be released when the user authenticates. The default value is 10. Set the value to 1 to release the latest print job only.

**8** In the TCP Unique Device ID field, type the serial number of the printer.

**9** Make sure that **Validate Server's Certificate** is selected.

**10** Click **Apply**.

**Note:** The client ID and client secret disappear to reduce the chances of disclosure.

**11** Click **REBOOT**.

## Managing certificates

The following certificates must be installed individually on each TCP3 device.

Download each certificate from the URLs listed:

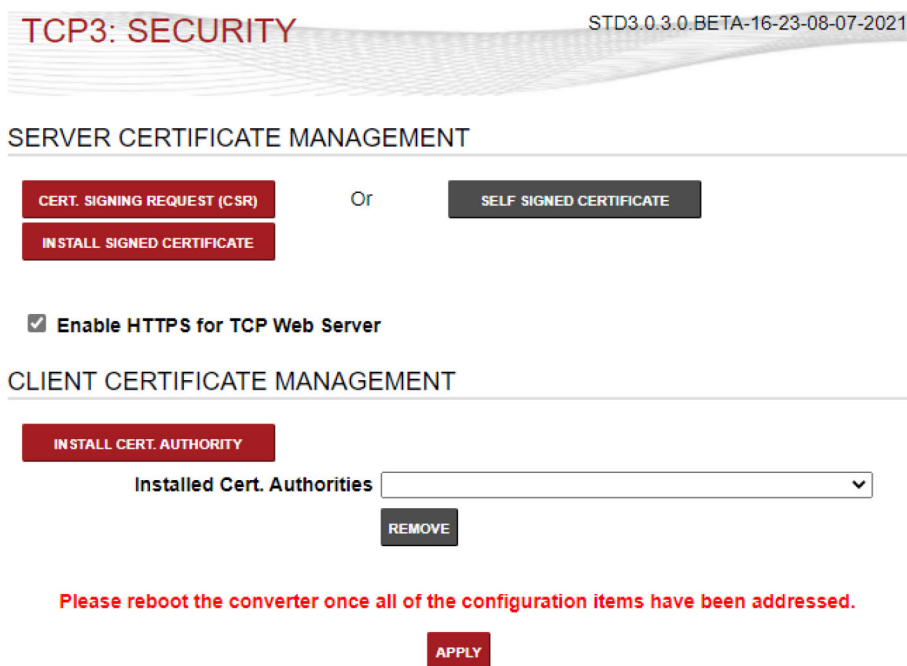
| Certificate name                              | URL   |
|---|---|
| Starfield Class 2 Certification Authority     | Go to <a href="https://crt.sh/?id=27">https://crt.sh/?id=27</a> .                 |
| DigiCert Global Root CA                       | Go to <a href="https://crt.sh/?id=853428">https://crt.sh/?id=853428</a> .         |
| Baltimore CyberTrust Root                     | Go to <a href="https://crt.sh/?id=76">https://crt.sh/?id=76</a> .                 |
| DigiCert Global Root G2                       | Go to <a href="https://crt.sh/?id=8656329">https://crt.sh/?id=8656329</a> .       |
| DigiCert Global Root G3                       | Go to <a href="https://crt.sh/?id=8568700">https://crt.sh/?id=8568700</a> .       |
| Microsoft RSA Root Certificate Authority 2017 | Go to <a href="https://crt.sh/?id=2565151295">https://crt.sh/?id=2565151295</a> . |
| Microsoft ECC Root Certificate Authority 2017 | Go to <a href="https://crt.sh/?id=2565145421">https://crt.sh/?id=2565145421</a> . |
| ISRG Root X1                                  | Go to <a href="https://crt.sh/?id=9314791">https://crt.sh/?id=9314791</a> .       |

**Notes:**

- The TCP3 device accepts certificate files only in PEM format. Use the **Download Certificates: PEM** option on each certificate page.
- Certificates can be installed only using the TCP3 device EWS.

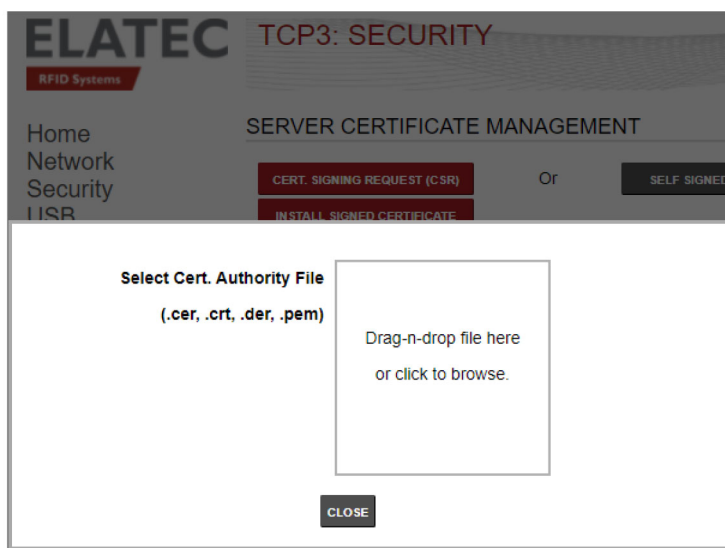
## Installing certificates

- 1 From the TCP3 device EWS, click **Security**.
- 2 In the CLIENT CERTIFICATE MANAGEMENT section, click **INSTALL CERT. AUTHORITY**.



The screenshot shows the 'TCP3: SECURITY' interface with the version 'STD3.0.3.0.BETA-16-23-08-07-2021'. The 'SERVER CERTIFICATE MANAGEMENT' section has buttons for 'CERT. SIGNING REQUEST (CSR)', 'INSTALL SIGNED CERTIFICATE', and 'SELF SIGNED CERTIFICATE'. The 'CLIENT CERTIFICATE MANAGEMENT' section has an 'INSTALL CERT. AUTHORITY' button, a dropdown for 'Installed Cert. Authorities', and a 'REMOVE' button. A red message states: 'Please reboot the converter once all of the configuration items have been addressed.' Below this is an 'APPLY' button.

- 3 Select the certificates or drag each certificate, and then click **CLOSE**.



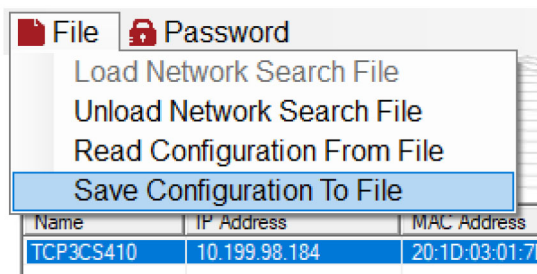
The screenshot shows a dialog box titled 'Select Cert. Authority File' with the file types '(cer, .crt, .der, .pem)'. It contains a large box with the text 'Drag-n-drop file here or click to browse.' and a 'CLOSE' button at the bottom.

- 4 Click **APPLY**.
- 5 Click **REBOOT**.

## Saving a TCP3 device configuration

A TCP3 device configuration can be saved for future deployment only if the configuration is performed using the TCP3 Config utility window.

To save a configuration for future deployment, from the File menu, click **Save Configuration To File**.



**Note:** For security reasons, when the configuration is saved, the client ID and client secret are not saved. They must be manually edited in the configuration file or manually entered in the TCP3 device after pushing the configuration.

## Restoring a client ID and client secret

- 1 Open the saved configuration file (JSON).
- 2 Locate the "**client\_id**" and "**client\_secret**" entries.
- 3 Type the "**<clientid>**", and "**<clientsecret>**" entries.
- 4 Save the file.

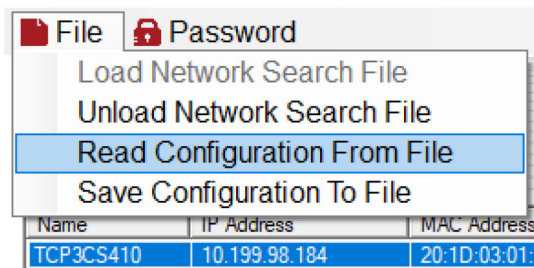
### Sample JSON file

```
"webservice_authentication": "oauthcc"
"client_ID": "e60044a1-8c73-9ec7-c53351a886cc"
"client_secret": "3939f4f7dcf18f8b87f0a18a7fa9a8845c22f5307a8af6e0b83f090b4320fb6"
```

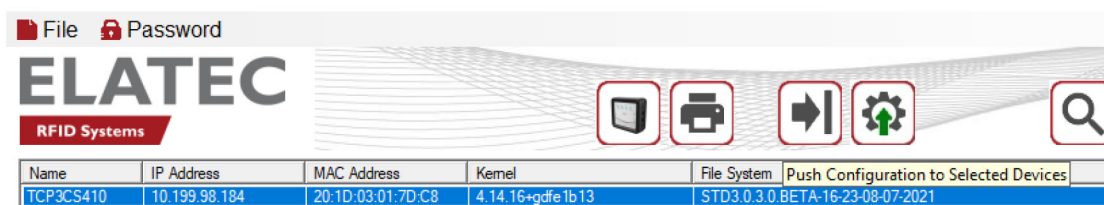
**Installation warning:** Make sure that you do not modify other elements of the file.

## Pushing a TCP3 configuration

- 1 From the File menu, click **Read Configuration From File**.



- 2 Select one or more TCP3 devices to receive the saved configuration, and then click **Push Configuration to Selected Devices**.



## Getting help

If you encounter an error, then contact your Lexmark representative.

# Notices

## Edition notice

May 2022

**The following paragraph does not apply to any country where such provisions are inconsistent with local law:** LEXMARK INTERNATIONAL, INC., PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in later editions. Improvements or changes in the products or the programs described may be made at any time.

References in this publication to products, programs, or services do not imply that the manufacturer intends to make these available in all countries in which it operates. Any reference to a product, program, or service is not intended to state or imply that only that product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any existing intellectual property right may be used instead. Evaluation and verification of operation in conjunction with other products, programs, or services, except those expressly designated by the manufacturer, are the user's responsibility.

For Lexmark technical support, go to <http://support.lexmark.com>.

For information on Lexmark's privacy policy governing the use of this product, go to [www.lexmark.com/privacy](http://www.lexmark.com/privacy).

For information on supplies and downloads, go to [www.lexmark.com](http://www.lexmark.com).

© 2021 Lexmark International, Inc.

All rights reserved.

## GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4, as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

## Trademarks

Lexmark and the Lexmark logo are trademarks or registered trademarks of Lexmark International, Inc. in the United States and/or other countries.

All other trademarks are the property of their respective owners.



# Index

## C

- certificates
  - installing 19
  - managing 19
- checklist
  - deployment readiness 4
- client ID and client secret
  - obtaining 14
  - restoring 21
- Client secret
  - getting 14
- configuring the TCP3 OAuth Settings 16

- TCP3 device
  - accessing 6
- TCP3 device configuration
  - saving 21
- TCP3 device EWS
  - logging in to 6
- TCP3 EWS
  - configuring 10
- TCP3 OAuth Settings
  - configuring 16

## D

- deployment readiness checklist 4

## E

- ELATEC
  - overview 3
- ELATEC TCP3 device
  - setting up 5

## G

- getting help 23

## L

- Lexmark Cloud Services authentication
  - setting up 14

## O

- obtaining the client ID and client secret 14
- Overview 3

## S

- setting up the ELATEC TCP3 device 5

## T

- TCP3 Config utility
  - configuring 12
- TCP3 configuration
  - pushing 21