

Sisukord

- Novitus Fiscal Printer Configuration for Directo** 3
- Introduction** 3
- Fiscal Printer Preparation 3
- Printer Port Settings 3
- Enable "NOVITUS" Protocol 3
- Enable NoviAPI 3
- Testing the HTTP Connection 4
- Enabling HTTPS 4
- HTTPS Certificate 4
- Example HTTPS Configuration 4
- Testing the HTTPS Connection 7
- Troubleshooting** 7

Novitus Fiscal Printer Configuration for Directo

Introduction

The Directo web application communicates with the Novitus fiscal printer over TCP/IP using HTTP requests sent to the printer's IP address. This guide provides instructions for configuring the printer to communicate securely over HTTPS, ensuring that sensitive data remains encrypted during transmission.

Fiscal Printer Preparation

Printer Port Settings

To begin, you must configure the communication settings for the printer. Press the green square button on the printer to access the configuration menu. Use the directional buttons to navigate to the following menu:

Ustawienia → Konfiguracja → Połączenia → Ustawienia Portow → PC

- Ensure that the „Interfejs“ option is set to TCP.

Enable "NOVITUS" Protocol

The Directo web application uses the „NOVITUS“ protocol to transmit messages between the fiscal printer and the web application. To verify that the printer is configured to use this protocol, navigate to the following menu:

Ustawienia → Konfiguracja → Połączenia → Protokół Komunikacji

- Use the up/down arrows to confirm that `NOVITUS` is selected. Press the green square button to confirm your selection.

Enable NoviAPI

Next, you need to enable NoviAPI, which will allow the printer to receive HTTP requests. To enable NoviAPI, follow these steps:

1. Navigate to the following menu on the printer: Ustawienia → Konfiguracja → Połączenia → NOVIAPI → OPCJE.
2. Ensure that there is a green checkmark next to Aktywna (use the right/left arrows to toggle the setting).
3. Leave the „Protokół“ option set to HTTP for now, as we will switch to HTTPS later.

4. You will be prompted to configure an IP address and port number. Write down these details, as they will be required later in the process.
5. Restart the printer by holding down the red button (marked with a red circle) and selecting Wylaczenie (Shutdown).

Testing the HTTP Connection

At this point, it's important to test whether the fiscal printer is ready to accept HTTP connections. Open PowerShell or any other shell application and issue an HTTP request to the IP address and port you configured in the previous step. For example, using PowerShell, you might issue the following command:



The response should indicate a StatusCode of 200, which confirms that the request was received successfully and the printer responded.



Enabling HTTPS

Now that the basic configuration is complete, you can enable HTTPS to secure the communication between the printer and the Directo web application. To do this:

1. Return to the NoviAPI configuration menu: Ustawienia → Konfiguracja → Polaczenia → NOVIAPI → OPCJE.
2. Follow the steps as outlined previously (the settings you configured earlier will remain unchanged).
3. When prompted for „Protokol,“ select HTTPS instead of HTTP.
4. Restart the printer once again to apply the changes.

HTTPS Certificate

In order to use HTTPS, the fiscal printer requires an SSL/TLS certificate to establish a secure connection. This certificate must be uploaded using Novitus's „Wiking2“ printer management software.

Important Note: Directo does not provide SSL certificates or manage certificate installation. You will need to obtain and configure a certificate for your printer. Due to the wide variety of network configurations, it is not feasible for Directo to provide a one-size-fits-all certificate solution.

Example HTTPS Configuration

Here is an example configuration for enabling HTTPS communication with the fiscal printer. This example assumes that the printer is set up with a static IP on the local area network and uses a custom, self-signed certificate for encryption:

1. The printer's NoviAPI is configured to run on IP address `10.10.10.78` and port `8888`.
2. A custom Root Certificate Authority (CA) is created, and a self-signed certificate is generated using this CA. This certificate is then uploaded to the fiscal printer using the „Wiking2“ software.

To generate a self-signed certificate and custom Root CA, you can use the following PowerShell script:

[script.ps1](#)

```
# Useful variables
$caCn = "Novitus Printer Root CA"
$fiscalPrinterIp = "10.10.10.78"

#
# Custom Root CA
#
# Generate custom Root CA
openssl genrsa -out rootCA.key 4096

# Generate custom Root CA certificate
openssl req -x509 -new -noenc `
    -key rootCA.key -sha256 `
    -days 3650 `
    -out rootCA.crt `
    -subj "/CN=$caCn/O=Directo/C=EE"

# Generate private key for specific fiscal printer
openssl genrsa -out server.key 2048

#
# Fiscal Printer Server Certificate
#
# Create config file for SAN
@"
[req]
default_bits = 2048
prompt = no
default_md = sha256
distinguished_name = dn
req_extensions = req_ext

[dn]
CN = $fiscalPrinterIp
O = Directo
C = EE

[req_ext]
subjectAltName = @alt_names

[alt_names]
IP.1 = $fiscalPrinterIp
"@ | Out-File -FilePath "server.conf" -Encoding utf8
```

```
# Generate CSR using the config
openssl req -new `
  -key server.key `
  -out server.csr `
  -config server.conf

# Generate certificate using the CSR
openssl x509 -req -in server.csr `
  -CA rootCA.crt `
  -CAkey rootCA.key `
  -CAcreateserial `
  -out server.crt `
  -days 3650 `
  -sha256 `
  -extensions req_ext `
  -extfile server.conf

# Use certutil (requires administrator privileges) to add the custom
Root CA
# to the computers certificate store otherwise the HTTPS connection
will not
# work as the computer does not recognize the certificate presented
by the
# fiscal printer.
certutil -delstore -enterprise root $caCn
certutil -addstore -enterprise "Root" rootCA.crt

# Convert our server.crt and server.key into a .pfx which will then
be given
# to Wiking2
openssl pkcs12 -export `
  -out server.pfx `
  -inkey server.key `
  -in server.crt `
  -passout pass: `
  -certfile rootCA.crt
```

Next, open the „Wiking2“ software and follow the instructions pictured below to upload the certificate to the printer:



After the certificate has been uploaded, restart the fiscal printer.

Testing the HTTPS Connection

To verify that HTTPS is working correctly, follow the same steps as before, but use the `https` protocol instead of `http`.

For example:



The response should again indicate a `StatusCode` of 200, confirming a successful connection.



Additionally, open a web browser and navigate to https://printerip:configured_port/api/v1. **Note:** If you are using a custom Root CA, you may need to restart your browser. This ensures that the browser recognizes the newly installed Root CA and does not display certificate warnings. You should see a blank white page, indicating that the printer's API is accessible via HTTPS without any security warnings.

Troubleshooting

If you encounter issues during the setup, here are a few common troubleshooting steps:

- **Is the printer connected to the local network via an Ethernet cable?** Ensure that the printer is properly connected and powered on.
- **Can the printer's IP address be reached from your computer?** Use tools like ping or telnet to check the connectivity between your computer and the printer.
- **Are you able to access the printer's configuration menu?** If not, check the physical connections and restart the printer.

From:

<https://wiki.directo.ee/> - Directo Help

Permanent link:

https://wiki.directo.ee/et/novitus_fp_config

Last update: **2024/12/09 10:07**

