Overview

The Universal STAMP Local Web Server (LWS) is a web-based alternative to the Universal STAMP Windows App. It is designed for clients who cannot install native Windows applications due to IT policies, such as a blocked Microsoft Store.

Unlike the Windows App, LWS runs entirely inside a **Docker container** and is accessed through a standard web browser. All document processing remains strictly within your environment — no data is ever sent to Hampton's or Kemark's systems.

Prerequisites

System Requirements

Before proceeding, ensure your server environment meets the following requirements:

Requirement	Details
OS	Linux (recommended) - any distribution with Docker Engine support
Architecture	x64 (AMD64) or ARM64
Memory	2 GB RAM minimum (4 GB recommended)
Disk Space	2 GB minimum for the container image and temporary files
Docker	Docker Engine 20.10 or later
Network	Outbound HTTPS access on ports 443 and 8443

Network Requirements

The following firewall ports must be configured for the container to function correctly:

Direction	Port	Protocol	Purpose
Inbound	443	HTTPS	User access to the Web Frontend (via reverse proxy)
Outbound	443	HTTPS	Communication with U-STAMP Portal
Outbound	8443	Alt-HTTPS	GlobalSign Service
Optional	22	SSH	Required only if the Inbox feature is enabled

Note: Port 22 (SSH) is only required if the optional Inbox feature is enabled. Consult your Hampton contact before enabling this feature.

Installation Process

Step 1: Pull the Docker Image

The LWS container image is hosted in the Hampton Technologies' private Docker registry. Pull the latest image using the following command:

```
docker pull registry.hamptontech.net/universalstamp-local:latest
```

Step 2: Prepare the Temporary Files Directory

The LWS uses a temporary directory for intermediate document processing. While the container includes a built-in garbage collector that automatically removes stale files, it is **strongly recommended** to map this directory to a folder on the host server.

Mapping the temp folder provides the following benefits:

- Allows monitoring of temporary files for auditing and troubleshooting
- Provides visibility into container activity during document processing
- Ensures that temporary files are accessible outside the container if needed

Create the host directory before starting the container:

```
mkdir -p /opt/universalstamp/tmp
```

Step 3: Run the Container

Start the LWS container using the following command. This example maps the internal port 8080 to the host port 8080 and configures all recommended environment variables:

```
docker run -d --name universalstamp-local \
  --hostname=universalstamp-local \
  -e ASPNETCORE_URLS=http://0.0.0.0:8080 \
  -e ASPNETCORE_HTTP_PORTS=8080 \
  -e DOTNET_RUNNING_IN_CONTAINER=true \
  -e PDFHANDLER=tool/PdfHandler \
  -e PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin \
  --network=bridge \
  --workdir=/app \
  -p 8080:8080 \
  -v /opt/universalstamp/tmp:/tmp \
  --restart=always \
  registry.hamptontech.net/universalstamp-local:latest
```

Note: The container listens internally on port 8080. The -p 8080:8080 flag maps this to host port 8080. Adjust the host port as needed to avoid conflicts with other services on your server.

Reverse Proxy Configuration (Recommended)

It is strongly recommended to place a reverse proxy such as **NGINX** in front of the LWS container. The container itself does not handle SSL/TLS termination — this must be done at the reverse proxy layer.

A reverse proxy provides the following advantages:

- SSL/TLS termination with your own certificate (e.g., Let's Encrypt or an enterprise CA)
- Serves user traffic over standard HTTPS port 443 while the container runs on an internal port
- Enables access control, logging, and rate limiting at the network edge
- Allows multiple services to run on the same server with virtual host routing

Example NGINX Configuration

The following example configuration proxies HTTPS traffic on port 443 to the LWS container running on port 8080:

```
server {
    listen 443 ssl;
    server_name ustamp.yourdomain.com;

    ssl_certificate     /etc/ssl/certs/your_certificate.crt;
    ssl_certificate_key /etc/ssl/private/your_key.key;

    location / {
        proxy_pass         http://127.0.0.1:8080;
        proxy_http_version 1.1;
        proxy_set_header   Upgrade $http_upgrade;
        proxy_set_header   Connection keep-alive;
        proxy_set_header   Host $host;
        proxy_set_header   X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header   X-Forwarded-Proto $scheme;
        proxy_cache_bypass $http_upgrade;
    }
}
```

Note: Replace ustamp.yourdomain.com and the certificate paths with your actual domain and SSL certificate details. If you use a different host port in the docker run command, update the proxy_pass address accordingly.

Verifying the Installation

Check Container Status

After starting the container, verify it is running:

```
docker ps --filter name=universalstamp-local
```

The container should appear with a status of Up. If it is not running, inspect the logs:

```
docker logs universalstamp-local
```

Access the Web Interface

Open a web browser and navigate to your server's address:

```
# If accessed directly (no reverse proxy):
http://<your-server-ip>:8080

# If accessed through a reverse proxy with SSL:
https://ustamp.yourdomain.com
```

The Universal STAMP login page should be displayed. If you encounter issues, refer to the troubleshooting section below.

Maintenance

Updating the Container

To update to a newer version of the LWS image, pull the latest image and restart the container:

```
docker pull registry.hamptontech.net/universalstamp-local:latest
docker stop universalstamp-local
docker rm universalstamp-local
# Re-run the docker run command from Step 3
```

Monitoring Temporary Files

The container includes a built-in garbage collector that automatically removes old and unused temporary files from the `/tmp` directory. If you have mapped the temp folder to a host path (as recommended in Step 2), you can monitor it directly on the host:

```
# List files in the mapped temp directory
ls -lh /opt/universalstamp/tmp

# Check disk usage
du -sh /opt/universalstamp/tmp
```

Troubleshooting

Symptom	Recommended Action
Container exits immediately	Run docker logs universalstamp-local to inspect startup errors. Verify all environment variables are set correctly.
Cannot access web interface	Confirm the container is running (docker ps). Check that the host port is not blocked by a firewall. Verify the reverse proxy configuration if applicable.
Outbound connection failures	Ensure your firewall allows outbound HTTPS traffic on ports 443 and 8443 from the container host.
SSL certificate errors in browser	Verify the SSL certificate and key paths in your NGINX configuration. Ensure the certificate is valid and trusted by your clients.
Temp folder filling up	Check for processing errors causing files to be retained. The garbage collector should clean up automatically; verify the container is healthy.

Support

For technical support or questions regarding the LWS installation, please contact the Hampton support team at **support@hamptontech.net**.