< netPump >

Administration Guide

Contents

< netPump >

1   Overview

This document provides detail for administration of the netPump® Data service. Please refer to the netPump® Data User Guide for general details about setup and usage.

2   Configuring the netPump® service

2.1   Service settings

Service configuration settings can be changed by editing the appsettings.json file. This file is found in the top level of the installation directory. For example:

```json
"ServiceSettings": {
        "netPumpApiSecret": "",
        "ChunkRetrievalMaxParallelism": 8,
        "WriteChunksBatchSize": 50,
        "ChunkLengthBytes": 10485760,
        "DatabasePath": "logs/netpump.db",
        "FilesSequentiallyErroredLimit": 10,
        "DatabasePurgeSettings": {
                "RunIntervalUnit": "Days",
                "RunIntervalValue": 1,
                "SessionEndTimeUnit": "Days",
                "SessionEndTimeValue": 1
        }
        "TrustedCertificateThumbprints": [
                "23fb7a5ad36b30a7c07f1b2ebcae77fdd000c380"
        ],

},
```

A description of the configuration parameters are as follows:

Parameter Name	Description
netPumpApiSecret	String, mandatory. Shared secret used for netPump® services and clients to communicate with each other.
ChunkRetrievalMaxParallelism	Positive integer, optional. Specifies the degree of parallelism of file chunks being transferred. If not specified, the degree of parallelism will default to the number of logical processors supported by the server.
WriteChunksBatchSize	Positive integer, optional. The number of file chunks to be batched before writing to disk. If not specified, WriteChunksBatchSize will have a default value of 10.
ChunkLengthBytes	Positive integer, optional. The number of bytes of a file that the destination service requests from the origin service in a single request.
DatabasePath	String, mandatory. The absolute or relative file path (including the file name) of the database to be accessed (it will be created if it doesn't exist yet).
FilesSequentiallyErroredLimit	Positive integer, optional. The number of files which error in a row resulting in a transfer session being halted prematurely (faulted).

	If not specified, the FilesSequentiallyErroredLimit will have a default value of 10.
	Note: any files for which the user does not have access permissions will result in the files being errored. If a user attempts to transfer a whole directory containing many such files, the transfer session may be unintentionally halted before completion. In such cases, raising the FilesSequentiallyErroredLimit is recommended.
DatabasePurgeSettings	Object, optional. These settings control how often the database is purged of older transfer sessions meeting a sliding window data/time criteria. If the DatabasePurgeSettings object is omitted, transfer sessions will never be deleted.
DatabasePurgeSettings.RunIntervalUnit	String, mandatory. The time unit specifying the interval between purging of sessions. Supported values (case insensitive): "minutes", "hours", "days"
DatabasePurgeSettings.RunIntervalValue	Positive integer, mandatory. The quantity of the RunIntervalUnit to support the run interval. E.g. if RunIntervalUnit="hours" and RunIntervalValue="5" then the database purge will run every 5 hours.
DatabasePurgeSettings.SessionEndTimeUnit	String, mandatory. The time unit specifying the maximum age of sessions. Supported values (case insensitive): "minutes", "hours", "days".
DatabasePurgeSettings.SessionEndTimeValue	Positive integer, mandatory. The quantity of the SessionEndTimeUnit to support the maximum age of sessions. E.g. if SessionEndTimeUnit="days" and SessionEndTimeValue="7" then the maximum allowable age of sessions is one week. Sessions with an end date older than this will be purged.
TrustedCertificateThumbprints	Array of strings, optional. A list of certificate thumbprints (fingerprints) for which SSL/TLS validation errors will be ignored. Values are not case-sensitive. This will allow you to use certificates that are not trusted by your operating system. Each thumbprint is expected to be in SHA-1 format (40 byte hex string) e.g. " B7349730D41B9F5BF328AD7224ECBA2E3D1DCB83". Refer to section 10.2 for details on how to generate this thumbprint. NB: Mac OS X netPump® services does not currently support validation of untrusted certificates.

Restart the server to allow configuration changes to take effect.

The appsettings.json parameters are not case-sensitive.

Use regular double quotation marks ("") to wrap parameters and string values rather than curly quotes ("") to avoid runtime problems.

2.2   netPump® service configuration

Each netPump® service listens on a configurable port to communicate with other netPump® services and clients such as the netPump® UI.

A service can run independently or be configured behind a reverse proxy. A reverse proxy server can be configured to secure communication between the client and destination server and between the destination and origin servers. Use of a reverse proxy server in front of the netPump® service is the recommended approach.

2.2.1   With a reverse proxy

Commonly used web servers such as IIS or Nginx can be configured as a reverse proxy. Configuration of IIS on Windows is discussed in section 3 and configuration of Nginx on Linux/Mac is discussed in section 4.

The service ports (HTTP/HTTPS) on which the reverse proxy server listens are set up during configuration.

2.2.2   Without a reverse proxy

The netPump® service can run directly without a reverse proxy but is not recommended when communications will occur over public networks.

The default listening configuration is HTTP port 5000. To change this configuration, you will need to edit the appsettings.json file to add a "Kestrel" section. Refer to Microsoft documentation available at https://docs.microsoft.com/en-us/aspnet/core/fundamentals/servers/kestrel?view=aspnetcore-2.1 for details of the configuration format.

3   HTTPS support via IIS on Windows

The netPump® service can run independently and without SSL/TLS for security, however the recommended approach is to configure the netPump® service to use Internet Information Services (IIS) web server as a reverse proxy with SSL enabled.

3.1   Enable IIS

Enable IIS on the Windows desktop or server machine as follows.

Windows desktop

Navigate to Control Panel / Programs / Programs and Features / Turn Windows features on or off (left side of the screen).

Open the group for Internet Information Services and Web Management Tools and check the following:

- IIS Management Console
- World Wide Web Services

Accept the default features for World Wide Web Services or customise IIS to suit your needs.
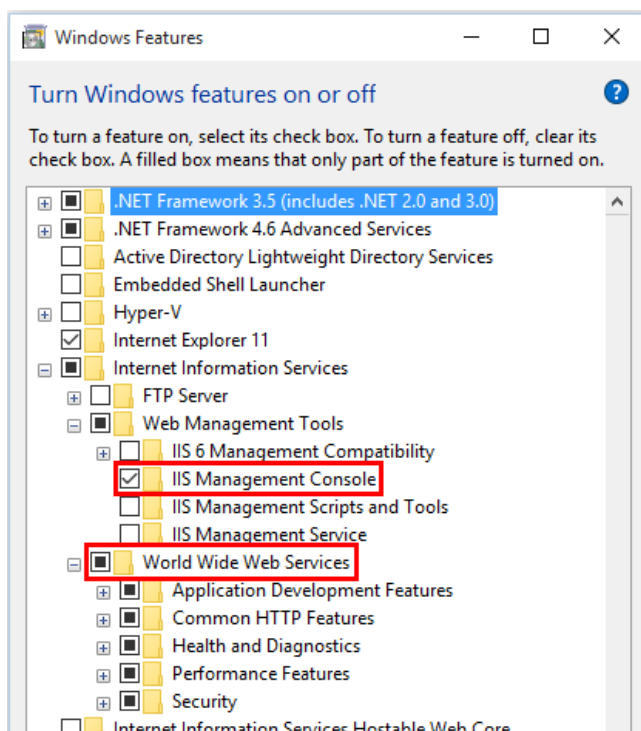
Windows Server

For server operating systems, use the Add Roles and Features wizard via the Manage menu or the link in Server Manager. On the Server Roles step, check the box for Web Server (IIS).
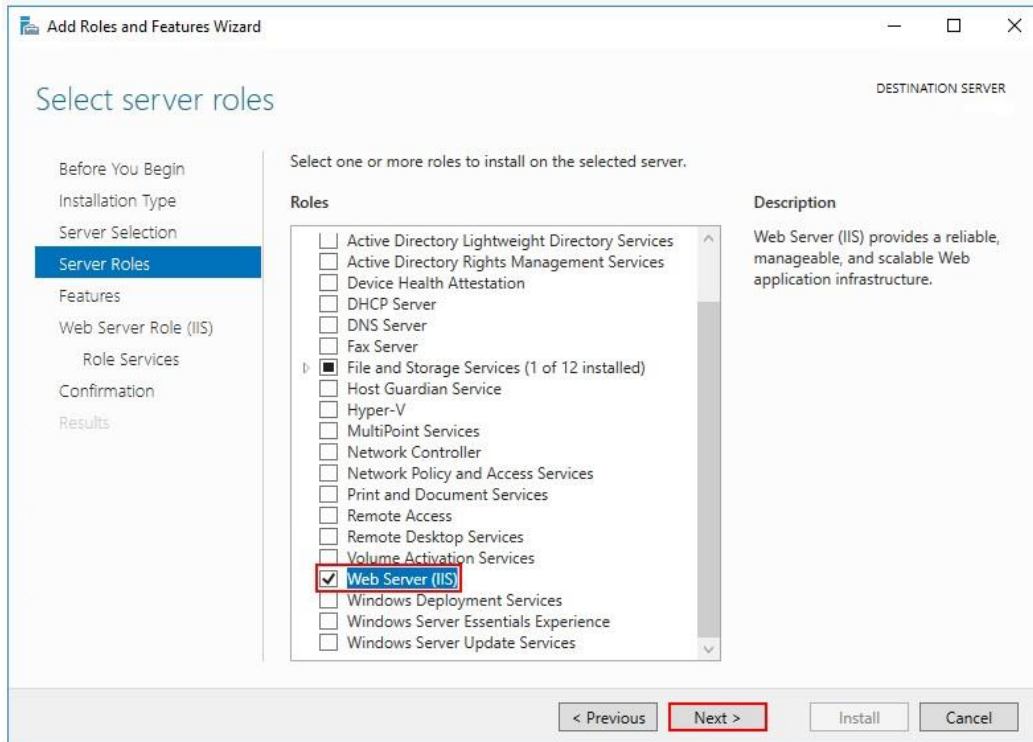
On the Role services step, select the IIS role services you desire or accept the default role services provided.

Source: https://docs.microsoft.com/en-us/aspnet/core/publishing/iis

3.2   Install the ASP.NET Core Windows Server Hosting bundle on IIS

The bundle contains the ASP.NET Core Module (ANCM) which creates and manages the reverse proxy communications between IIS and the netPump® service. A link to download the bundle can be found at: https://dotnet.microsoft.com/download/archives - download the "Runtime & Hosting Bundle".

3.3   Set up publish directory

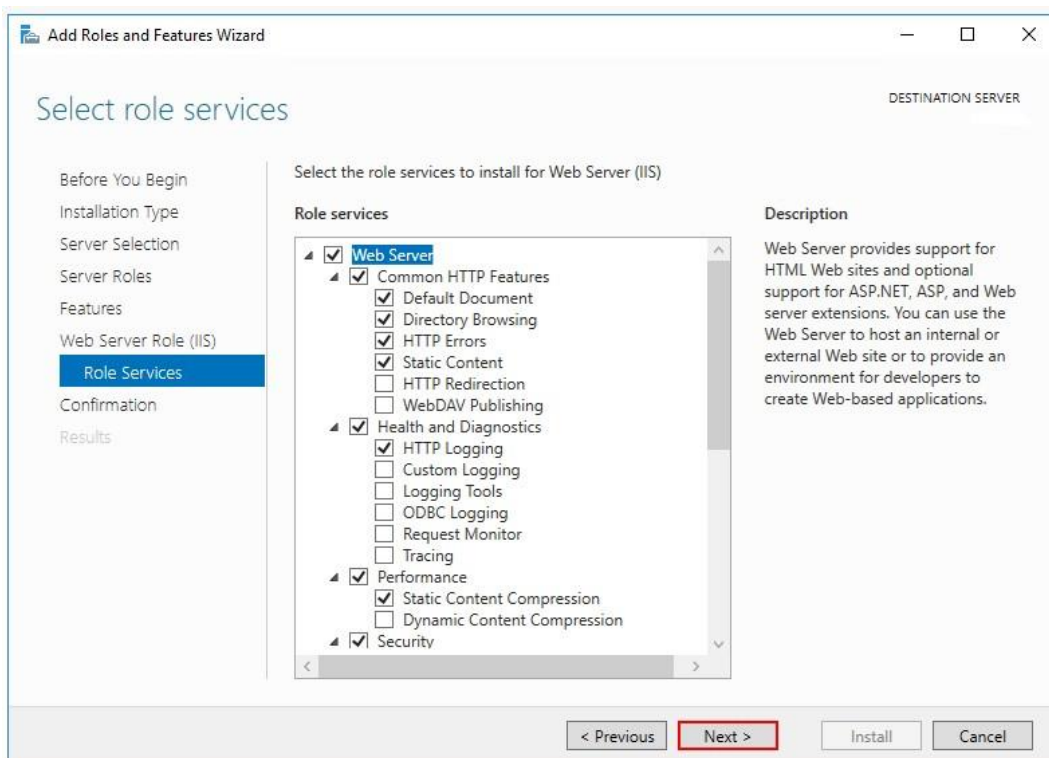The netPump® service installation directory will also be the publish directory where IIS will source netpump® web resources from.

Ensure the netPump® service user has read permissions to this directory.

Details about further configuration (optional) can be found at: https://docs.microsoft.com/en-us/aspnet/core/host-and-deploy/aspnet-core-module?view=aspnetcore-2.1.

3.4   Obtain an SSL/TLS certificate

Request an SSL certificate from a Certificate Authority.

Following is an example of creating a self-signed certificate for testing purposes on Windows using makecert.

At the command line:

```
"C:\Program Files (x86)\Windows Kits\10\bin\x64\makecert.exe" -sv netpump.pvk -n
"CN=ExampleCorp" netpump.cer -r
```

to generate the .pvk and .cer files. When prompted, enter a secure password and store it for future reference.

Then type:

```
"C:\Program Files (x86)\Windowzs Kits\10\bin\x64\pvk2pfx.exe" -pvk netpump.pvk -spc
netpump.cer -pfx netpump.pfx -pi
```
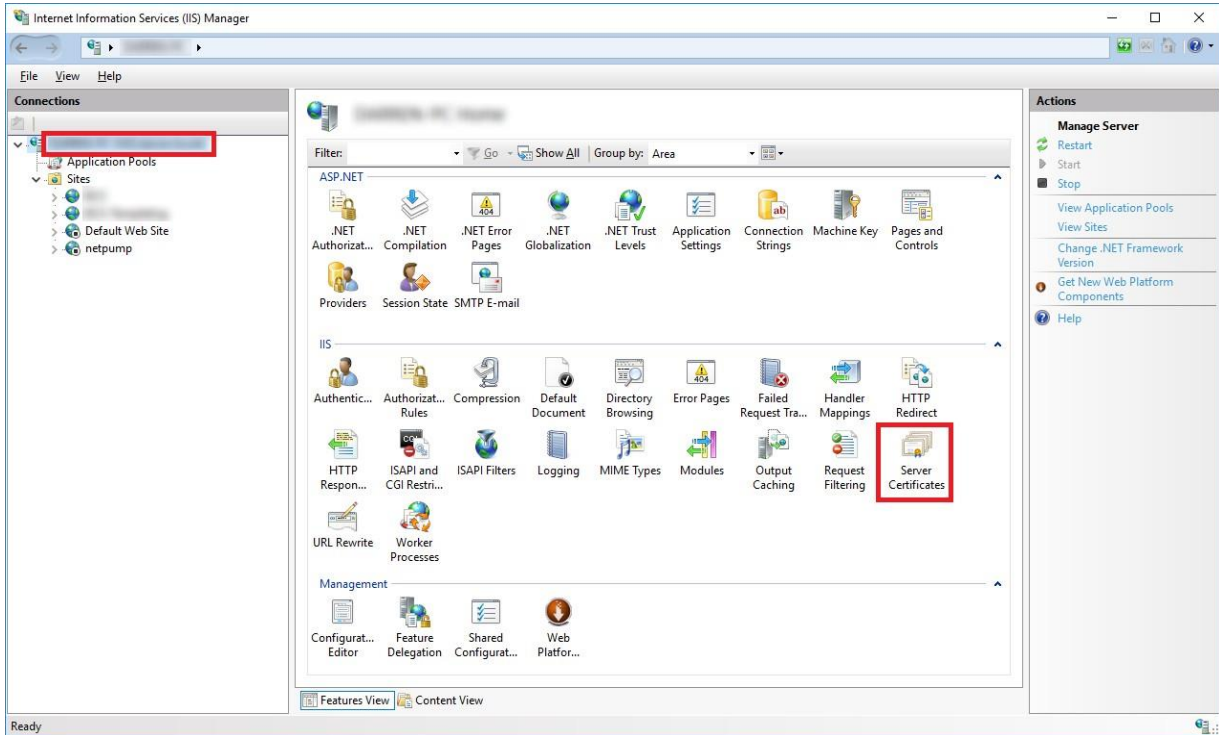
providing the password created above. This creates the `netpump.pfx` archive file containing the private key and certificate generated above.

3.5   Install the certificate

Click Start and type 'inetmgr' to open the IIS Manager.

Click on the localhost connection, double click on Server Certificates

On the right-hand side in the Actions pane, select Import.

Browse for the .pfx file and provide the password used when created the certificate.

3.6 Deploy the netPump® service with IIS

To deploy the service, first create a website. In IIS Manager, right-click on Sites, Add Website
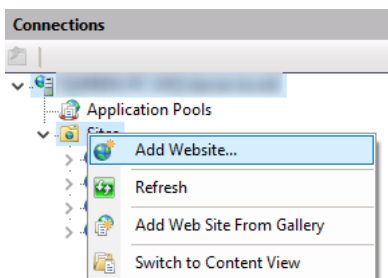
Provide the following:

- Site name: a unique name for the service
- Physical path: point it to the publish directory discussed above
- Binding: Type: 'https', IP address: 'All Unassigned', Port : 443
- Host name: this will be used when specifying the origin and destination service
- SSL certificate: add the relevant certificate from the dropdown list
- Connect As: specify the Specific user who will be accessing the service
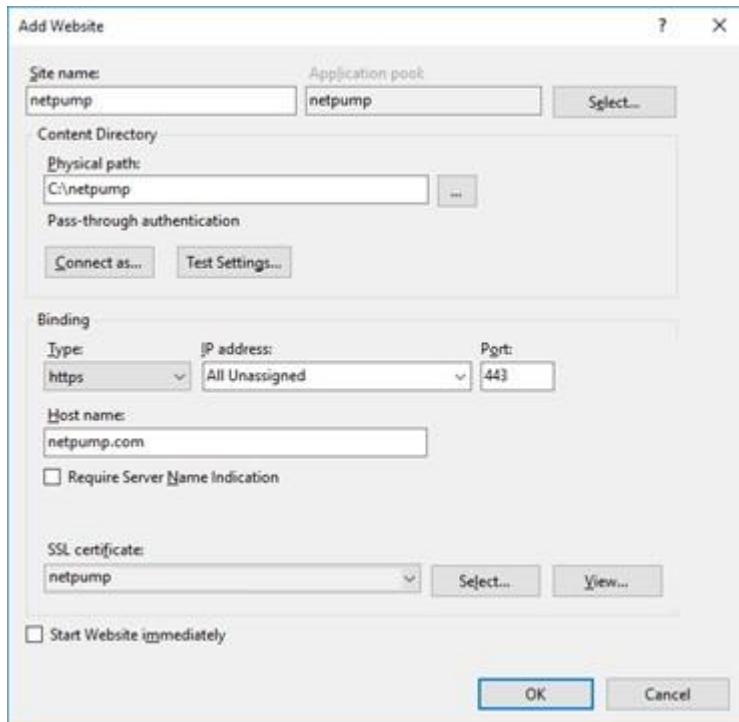
Once the website has been created, check the binding has been created. On right-hand side: Actions/Bindings.

3.7   To always use secure communications

To require requests use SSL only, click on the site then SSL Settings:
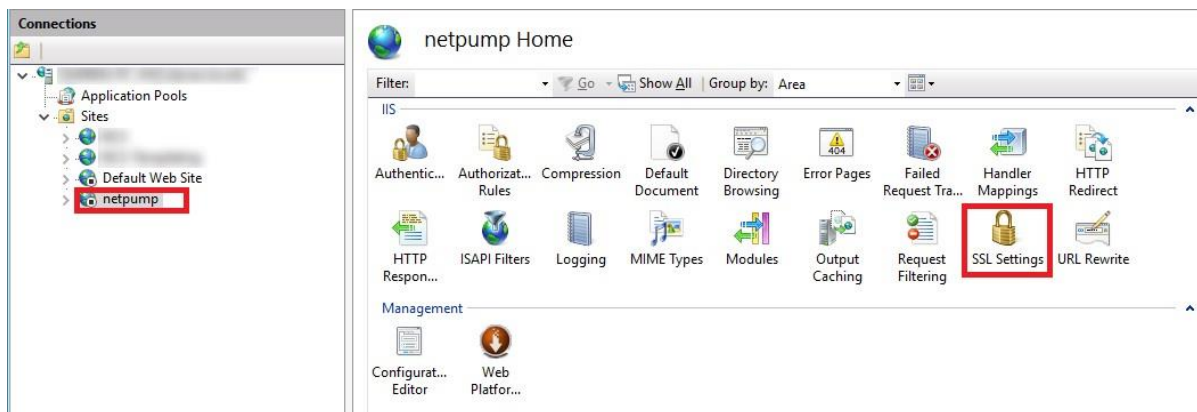
If the server communications should always be secure, check the 'Require SSL' box:

If left unchecked, users can switch seamlessly between secure (HTTP) and unsecure (HTTPS) communication via the netPump® UI.

3.8   Configure the application pool

In IIS Manager, on the left-hand side, click on 'Application Pools'. Right-click on the service site name in the centre then Basic Settings.
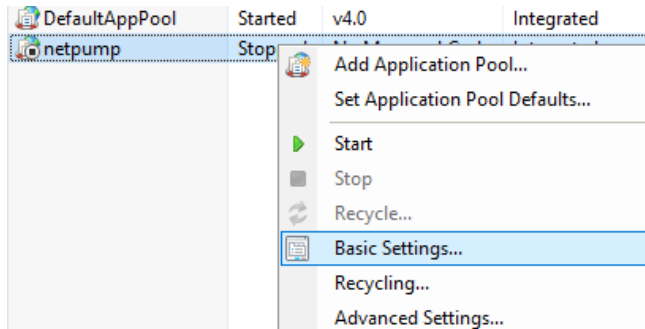
For .NET CLR version, select 'No Managed Code' and Managed pipeline mode: 'Integrated':
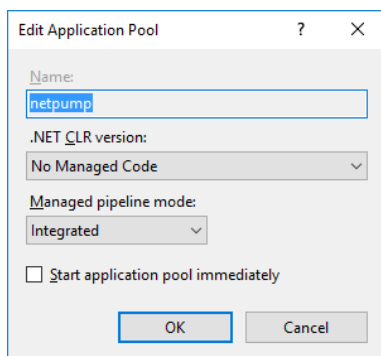
Right-click on the service site name in the centre then Advanced Settings:
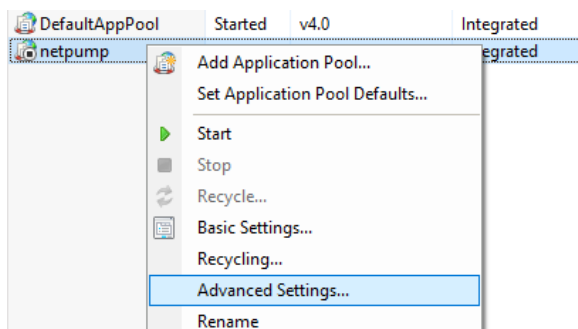
Locate the Identity setting in the Process Model group and set a Custom account for the user which the service will be run under. This user should be the same as the one nominated above for the website.

Source: https://docs.microsoft.com/en-us/aspnet/core/host-and-deploy/aspnet-core-module?view=aspnetcore-2.1.
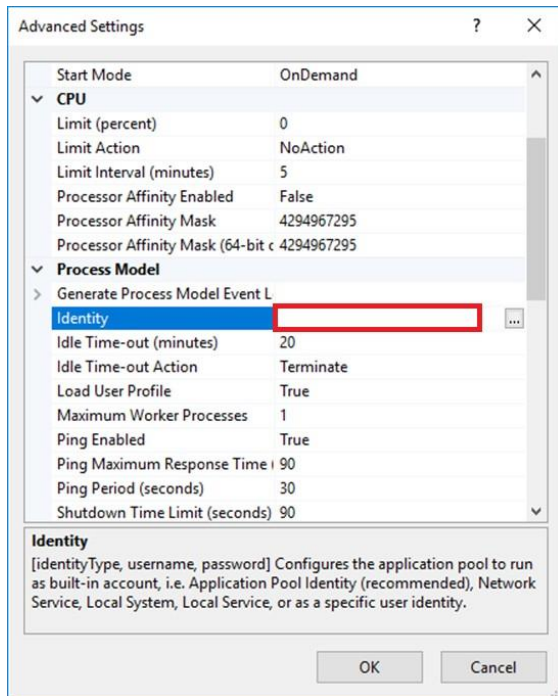
To test everything is ok, on the right-hand side, click on 'Basic Settings'. Click 'Test Settings'. Green ticks should appear beside the Authentication and Authorization tests.

3.9   Start IIS and the website

In IIS Manager:

- Click on the server connection at top left. Under Actions, click 'Start'.
- Click on the Application Pools/<site name>. Under Actions, click 'Start'.
- Click on Sites/<site name>. Under Actions, click 'Start'.

3.10 Running the netPump® service with/without HTTPS support

Depending on circumstances you may wish to toggle between running the netPump® service with or without HTTPS support.

3.10.1 Running the service with HTTPS

To enable HTTPS handling of requests:

- Stop netPump® service running on Kestrel in the console.
- Start IIS, the application pool and the website as described above. The ANCM will start the netPump® service when the first request is received.

When providing the service in the GUI enter only `<hostname>` in the service field, the HTTP/HTTPS prefix is not required, and the `<port>` in the default secure port field

E.g.

```
netpump.com
```

3.11 Running the service with HTTP only

To disable HTTPS handling of requests:

- Stop the relevant IIS application pool and the website. Stop IIS if no other websites are being hosted
- Start the netPump® service in the console

When providing the service in the GUI enter only `<hostname>` in the service field, and `<port>` in the default unsecure port field.

E.g.

Service: `netpump.com`
Default unsecure port field: `5000`

4 HTTPS support via Nginx

It is recommended that the netPump® service is configured as a local service with a reverse proxy such as Nginx providing access and SSL/TLS termination.

The following is an example of the requirements to run the netPump® service on a Linux/Mac host with the Nginx http server configured as a reverse proxy.

4.1 Set up the netPump® service as a daemon

A daemon is used in this example to manage the lifecycle of the netPump® service.

4.1.1 Linux

We use systemd init system to manage the lifecycle of the netPump® service.

Create a unit configuration file `/etc/systemd/system/netpump.service`:

```
[Unit]
Description=netPumpDataService

[Service]
WorkingDirectory=/home/netpump.service/service/
ExecStart=/usr/bin/dotnet
/home/netpump.service/service/netPump.Service.dll
Restart=always
RestartSec=30
SyslogIdentifier=netpump-service
User=netpump

[Install]
WantedBy=netpump.target
```

Note: This assumes an appropriately privileged user 'netpump' exists, and the netPump® service has been extracted to /home/netpump/netpump.service.

Enable, start and check the status of the service:

```
sudo systemctl enable netpump.service
sudo systemctl start netpump.service
sudo systemctl status netpump.service
```

4.1.2   Mac OS X

The launchd service management framework can be used to manage the lifecycle of the netPump®
service daemon.

For example, to define a global daemon under the `/Library/LaunchAgents` directory, create a
property list file `netpump.service.plist` with the contents:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
   <dict>
      <key>Label</key>
      <string>netPumpDataService</string>
      <key>ProgramArguments</key>
         <array>
            <string>/usr/bin/dotnet</string>
            <string>/home/netpump.service/service/netPump.Service.dll</string>
         </array>
      <key>WorkingDirectory</key>
      <string>/home/netpump.service/service</string>
      <key>RunAtLoad</key>
      <true/>
      <key>UserName</key>
      <string>netpump</string>
   </dict>
</plist>
```

Note: This assumes an appropriately privileged user 'netpump' exists, and the netPump® service has
been extracted to /home/netpump/netpump.service.

Enable, start and check the status of the service:

```
launchctl load netpump.service.plist

launchctl start netPumpDataService

launchctl list | grep netPump
```

> This yields: <pid> <status code> <label of service>
>
> A status code of 78 indicates an error with the configuration
>
> If errors are encountered, install and run the LaunchControl application to help diagnose and
> fix errors in the property list file.

4.2   Confirm the netPump® service is running correctly

Check the status endpoint:

```
curl http://localhost:<port>/status
```

The port should be as is configured in hosting.json.

The response body should contain 'Running'.

4.3   Configure Nginx to proxy requests to netPump®

Update the Nginx configuration file `nginx.conf` to take requests on port 443 (or another port as required) and proxy them to the netPump® service on port 5000 (or as configured in hosting.json).

For example:

```
server {
   listen 443 ssl http2 default_server;
   ssl_certificate /etc/nginx/cert.pem;
   ssl_certificate_key /etc/nginx/cert.key;
   location / {
      proxy_pass http://netpump;
      proxy_set_header Host $host;
      proxy_http_version 1.1;
      proxy_set_header Connection keep-alive;
   }
}
upstream netpump {
   server 127.0.0.1:5000;
}
```

`cert.pem` is the full certificate chain in PEM format.

`cert.key` is the un-encrypted key for the server certificate (an alternative to storing an un-encrypted certificate key is the Nginx ssl_password_file option).

For full Nginx configuration details refer to the documentation for your distribution at https://nginx.org/en/docs/.

When the *destination* netPump® service is on a Linux/Mac host, in order for it to contact any *origin* netPump® service, that origin must serve a full certificate chain.

The following error returned by a Mac destination server:

```
System.Net.Http.CurlException: Peer certificate cannot be authenticated with given
CA certificates at System.Net.Http.CurlHandler.ThrowIfCURLEError
```

is due to a problem with the certificate chain on the origin server. Ensure the origin serves the full certificate chain.

In the above example, cert.pem contains the root, intermediates and server certificates.

For example, to extract the server (client) and CA certs from a PKCS12 archive and combine in the appropriate order:

```
openssl pkcs12 -in example.pfx -clcerts -nokeys -out client.pem
openssl pkcs12 -in example.pfx -out cas.pem -nodes -nokeys -cacerts
cat client.pem cas.pem > cert.pem
```

To obtain a certificate key in unencrypted form from a PKCS12 archive:

```
openssl pkcs12 -in example.pfx -nocerts -out encrypted.key
openssl rsa -in encrypted.key -out decrypted.key
```

Note: If using an un-encrypted key pair due care should be taken to ensure it is not stored in an unsafe location.

Validate Nginx configuration using `sudo nginx -t` before reloading with `sudo nginx -s reload.`

To validate that a full certificate chain is being served check `openssl s_client -connect <hostname or ip address>:443.`

4.4   Check the status endpoint via the reverse proxy port

To confirm that requests are being proxied to the netPump® service correctly:

`curl https://localhost:443/status`

The response body should contain 'Running'.

5 Bash scripting

To assist with scripting and cron job scheduling of file transfers on Linux/Mac, a shell script is provided in the installation directory: `startTransfer.sh`

5.1 Permissions

Ensure the script has permissions 755.

5.2 Running the script

Usage details can be found by running the script with the -h switch:

```
./startTransfer.sh -h
```

Examples:

```
./startTransfer.sh -a AUTH_SECRET -p
/path/to/a.log,/another/path/b.log -l /home/data -r
http://12.1.130.1:5000 -D http://12.1.131.1:5000
```

```
./startTransfer.sh -a AUTH_SECRET -p C:/files/a.log -l /home/data -r
https://machine-origin -D https://machine-destination:5555 -m
```

5.3 Support for trusted certificates

If the security certificate installed on the destination server has errors but should be explicitly trusted by the client (e.g. self-signed) and adding it to a local certificate store is not possible, the startTransfer.sh script can be amended in the following ways:

1. Certificates can be explicitly validated by providing the certificate file with the cURL `-cacert` option.

2. Certificate validation can be disabled using the cURL `-k` (or `--insecure`) switch.

5.4 DOS/Linux line endings

If the following error is received:

```
-bash: ./startTransfer.sh: /bin/bash^M: bad interpreter: No such
file or directory
```

This indicates the script has 'Windows' line endings CR LF which is inconsistent with Linux which uses the LF character.

Convert the script to a Linux-compliant format. For example, using the dos2unix utility:

```
sudo apt-get install dos2unix
```

```
dos2unix startTransfer.sh
```

6 Powershell scripting

Scripting support is available for users who wish to initiate files transfers via Powershell.

The script: startTransfer.ps1 is available in the root directory of the netPump® service. It is suitable to use for scheduling purposes. Because this script is intended for administrators running the script in non-interactive mode, the listing of directory contents, pause and resume scripting capabilities are not supported at this time.

6.1 Installation of Powershell

For operating systems without a current installation of Powershell, Powershell can be installed from https://microsoft.com/powershell or https://github.com/PowerShell/PowerShell for cross platform support.

Follow the instructions provided for the platform on which you are installing Powershell. For example, for an Ubuntu machine, download the .deb file and install using the Ubuntu Software Centre.

6.2 Running Powershell

Ensure the netPump® service is running.

In Windows:

Click Start

Type: `Powershell`

   Select Windows Powershell

In Linux:

Open a console and type:

```
> powershell
```

6.3 Running the script

After Powershell has been started, go to the netPump® service installation directory:

```
cd <installation directory>
```

To see high-level instructions of how to run the script, type:

```
help .\startTransfer.ps1
```

From here, you may wish to get detailed help:

```
get-help .\startTransfer.ps1 -detailed
```

Or see examples:

```
get-help .\startTransfer.ps1 -examples
```

6.4 Examples

To transfer files, provide a list of files delimited by a comma ',':

```
.\startTransfer.ps1
      -DestinationService http://localhost:5000
      -DestinationFolder C:\temp\receiver
      -OriginService http://localhost:5000
      -AuthSecret AUTH_SECRET
      -Paths C:\path\to\files\a.log,C:\another\path\to\files\b.log
      -DeleteOnTransfer
```

To transfer a directory with a pattern, provide both a directory and a pattern:

```
.\startTransfer.ps1
      -DestinationService http://localhost:5000
      -DestinationFolder C:\temp\receiver
      -OriginService http://localhost:5000
      -AuthSecret AUTH_SECRET
      -Directories C:\path\to\dir
      -Pattern 20170?01_*.txt
```

Alternatively, the script can be run in interactive mode by only specifying the files or directories to transfer. The script will prompt for the mandatory fields to be entered:

```
.\startTransfer.ps1 -Paths C:\files\a.log

cmdlet startTransfer.ps1 at command pipeline position 1
Supply values for the following parameters:
DestinationService: http://localhost:5000
DestinationFolder: C:\receiver
OriginService: http://localhost:5000
AuthSecret: AUTH_SECRET
```

On successful initiation of the transfer, the session ID (a GUID) will be returned in the response:

```
Guid
----------
64baa412-a4a5-4b87-9ee4-0c453c17035b
```

6.5 Support for trusted certificates

If the security certificate installed on the destination server has errors but should be explicitly trusted (e.g. self-signed) and adding it to a local certificate store is not possible, the startTransfer.ps1 script can be amended.

Powershell provides a callback which can be set prior to the `Invoke-WebRequest` call. This allows the script caller to accept errored certificates:

```
[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true};
```

7 Starting transfers using cURL

cURL is a command line tool for requesting files using URLs. It supports common Internet protocols, notably HTTP which is required to call the netPump® service. cURL commands can be integrated into scripts for convenience.

7.1 Installation

On Windows, check if cURL is installed. Click the Start menu, type 'cmd' to open a command line window. Type:

```
curl
```

If cURL has been installed, a message similar to this should be displayed:

```
curl: try 'curl --help' or 'curl --manual' for more information
```

If not, look for a local installation of cURL on the machine.

If still not found, download cURL from:

```
https://curl.haxx.se/download.html
```

Select the installation to install or use the cURL download wizard link for assistance.

Once the package has been downloaded, add the installation directory (where curl.exe resides) to the environment variable %PATH%.

cURL commands can then be issued from the command line.

7.2 Walkthrough

The sequence of steps to call the service API is as follows.

7.2.1 Get a directory listing

To request the content of a directory on the origin machine, issue a POST request via a cURL command with the following format of the example:

Windows:

```
curl ^
     -X POST ^
     --header "Content-Type: application/json" ^
     --header "Authorization: AUTH_SECRET" ^
     --header "Accept: application/json" ^
     -d "{ \"remoteService\": \"http://localhost:5000\",  \"path\": \"C:\\files\"
}" ^
     "http://localhost:5000/controlapi/directory/listing"
```

Linux/Mac:

```
curl \
     -X POST \
     --header 'Content-Type: application/json' \
     --header 'Authorization: AUTH_SECRET' \
```

```
--header 'Accept: application/json' \
-d '{
   "remoteService": "http://localhost:5000",
   "path": "/home/netpump/sender"
 }' \
'http://localhost:5000/controlapi/directory/listing'
```

Replace AUTH_SECRET with the actual Authorization secret as configured in appsettings.json.

Note: the caret character '^' in Windows and backslash '\' in Linux have been used to split the request over multiple lines for better readability.

Note: '-H' can be used interchangeably with '--header'.

7.2.2   Initiate a file transfer

To initiate a file transfer, an HTTP PUT request can be made to the transfer/start API endpoint.

To transfer files, use the 'paths' parameter with one or more paths representing files on the origin service:

Windows:

```
curl ^
      -X PUT ^
      --header "Content-Type: application/json" ^
      --header "Authorization: AUTH_SECRET" ^
      --header "Accept: application/json" ^
      -d   "{   \"paths\":   [   \"C:\\files\\a.log\",   \"C:\\files\\b.log\"   ],
\"localFolder\": \"C:\\receiver\", \"remoteService\": \"http://localhost:5000\" }" ^
      "http://localhost:5000/controlapi/transfer/start"
```

Linux/Mac:

```
curl \
      -X PUT \
      --header 'Content-Type: application/json' \
      --header 'Authorization: AUTH_SECRET' \
      --header 'Accept: text/html' -d '{
            "paths": [
            "/home/netpump/sender/a.log",
            "/home/netpump/sender/b.log"
            ],
            "localFolder": "/home/netpump/receiver",
            "remoteService": "http://localhost:5000"
}' \
      'http://localhost:5000/controlapi/transfer/start'
```

To transfer one or more directories, use the 'directories' parameter:

```
curl ^
      -X PUT ^
      --header "Content-Type: application/json" ^
      --header "Authorization: AUTH_SECRET" ^
      --header "Accept: application/json" ^
      -d   "{ \"directories\": [ \"C:\\files\\dir1 \", \"C:\\files\\dir2 \" ],
\"localFolder\": \"C:\\receiver\", \"remoteService\": \"http://localhost:5000\" }" ^
```

```
                 "http://localhost:5000/controlapi/transfer/start"
```

To transfer files with a wildcard filter on a single directory, the pattern parameter should be provided, and the directories collection should only contain a single item:

```
curl ^
      -X PUT ^
      --header "Content-Type: application/json" ^
      --header "Authorization: AUTH_SECRET" ^
      --header "Accept: application/json" ^
      -d "{ \"directories\": [ \"C:\\files\\logs\" ], \"pattern\":  \"2017010?.*\",
\"localFolder\": \"C:\\receiver\", \"remoteService\": \"http://localhost:5000\" }" ^
      "http://localhost:5000/controlapi/transfer/start"
```

Replace `AUTH_SECRET` with the actual Authorization secret as configured in appsettings.json.

If conflicting options are provided (e.g. providing both paths and directories), the service returns a HTTP 400 status code with an error message indicating the problem.

8 Resumability

The netPump® service can handle a disruption to the service (either at the origin or destination) and will resume outstanding file transfers if the service is restarted.

To support resumability, the netPump® destination service maintains transfer session progress information in a local database (see 'DatabasePath' in the configuration section).

When the service resumes it will identify any incomplete sessions and attempt to retrieve outstanding files from the origin service in order to complete the requested transfer.

9   Trouble-shooting guide

Errors may arise from time to time and trouble-shooting them is an important step towards diagnosing and fixing the problem.

Logging captures warnings such as when a file is not available for transfer or more serious problems from which the service cannot recover from.

9.1   netPump® service

Log output is sent to standard out/error of the shell hosting the service by default.

To change the logging levels for debugging purposes, modify the logging level in appsettings.json in the installation folder of the service.

E.g. on a Windows server, change the level to "Debug":

```
"Logging": {
        "IncludeScopes": false,
        "LogLevel": {
                "Default": "Debug",
                "System": "Information",
                "Microsoft": "Debug"
        }
},
```

then restart the server.

The logging levels from least to highest severity are:

- Trace
- Debug
- Information
- Warning
- Error
- Critical

Note: the lower the level of logging, the more verbose and larger the log files will be.

If running in standalone mode, or without a reverse proxy which provides access to logs from stdout/err, logging data may also be written directly to a file as configured in the logging adaptor section of the netPump® service configuration file (see appsettings.example.json for an example):

```
"Serilog": {
        "Using": [
                "Serilog.Extensions.Logging.File",
                "Serilog.Enrichers.Thread",
                "Serilog.Enrichers.Environment"
        ],
        "MinimumLevel": "Verbose",
        "WriteTo": [
                {
                        "Name": "RollingFile",
                        "Args": {
                                "pathFormat": "logs/service-{Date}.log",
                                "outputTemplate": "{Timestamp:yyyy-MM-dd
HH:mm:ss.fff zzz} [H:{MachineName}] [T:{ThreadId}] [L:{Level}]
{Message}{NewLine}{Exception}"
```

```
                        }
                }
        ],
        "Enrich": [ "FromLogContext", "WithMachineName", "WithThreadId" ]
    }
```

9.2   Client-side

Logging is also present on the client side when interacting with the netPump® services.

9.2.1   netPump® UI

Errors are displayed in the status bar at the bottom of the application.

9.2.2   cURL and Powershell

Limited information is provided via these interfaces. Error messages returned by the service may be useful for diagnostic purposes.

10 Obtaining thumbprints for security certificates

It may be necessary to generate the thumbprint (fingerprint) of a security certificate to enable either the netPump® service or the UI to accept the certificate.

10.1 Obtaining the thumbprint from IIS

If IIS is used as the reverse proxy server for SSL/TLS security, the certificate store will contain the certificate.

Inside the IIS Manager, click on Server Certificates and select the certificate being used by the netPump® service. The thumbprint will look similar to this:
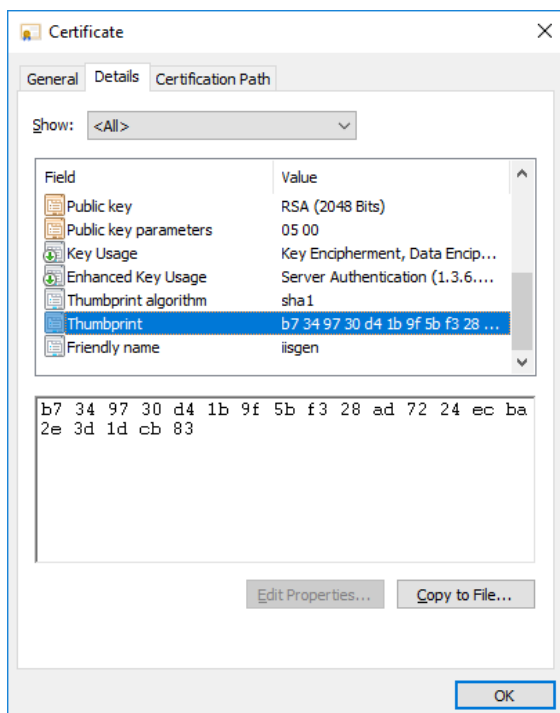
Remove the spaces from the thumbprint if it is to be added to the TrustedCertificateThumbprints list in appsettings.json.

10.2 Steps to generate a thumbprint

If the SHA-1 or SHA256 thumbprint is not readily available it can be generated as follows:

1. Install OpenSSL

2. Convert the certificate to an appropriate format

> For example, to convert a pkcs12 file to a .pem:

```
openssl pkcs12 -in example.pfx -out example.pem
```

3. Generate the thumbprint

SHA-1 (used in the netPump® service configuration file appsettings.json)

< netPump >

```
openssl x509 -noout -in example.pem -fingerprint -sha1
```

This will produce the output:

```
SHA1
Fingerprint=B7:34:97:30:D4:1B:9F:5B:F3:28:AD:72:24:EC:BA:2E:3D:1D:CB:83
```

The fingerprint is:

```
B7349730D41B9F5BF328AD7224ECBA2E3D1DCB83
```

< netPump™ >

11 Known limitations and restrictions of file transfers

Restrictions pertaining to individual platforms mean that the transfer of certain files may not be possible. In this event, the individual files will be errored and the session will end with a status of Completed With Errors.

11.1 Reserved file names

Windows has a series of reserved names such as CON, COM and LPT. Files having these names cannot be transferred to Windows.

11.2 Reserved characters

Windows has a wider set of reserved characters than Linux/Mac hence the netPump® service may not be able to transfer a file from Linux/Mac to Windows which contains special characters. For example, the file *name* 'C:\server.log' is valid on Linux but it cannot be transferred to Windows as a file *name* when joined with the destination folder. The reserved characters on Windows for a file *name* are generally:

'\', '/', ':', '*', '?', '"', '<', '>', '|' and ASCII control codes 0 to 31

11.3 File attributes

Due to differences in how file attributes and permissions are supported on different operating systems, limited support is available for the preservation of owner/group/other attributes and permissions in file transfers.

11.3.1 Linux/Mac to Windows

Read-write attributes are preserved. Linux/Mac read-write permissions are governed by the permissions on the file and the user of the netPump® service.

For example, if the netPump® service is set up by a user X and a client wishes to transfer a file for which user X has 'Other' permissions, then the 'Other' permissions on the file apply when the file is transferred by the netPump® service. In this case, the file will be transferred to Windows with the read-only attribute set.

Hidden or 'dot' files on Linux/Mac which start with a period '.' are transferred to Windows with the hidden file attribute set and the dot prefix retained.

11.3.2 Windows to Linux/Mac

Read-write attributes are preserved during the transfer for the user (owner) but preservation of group/other attributes is not supported.

Windows files lose the hidden attribute on transfer to Linux since the definition of a hidden file in Linux/Mac is a file name starting with a period '.'. The exception is where the Windows file name starts with a period.

< netPump >

11.3.3 Linux/Mac to Linux/Mac

The preservation of read-write file attributes is not supported at present.

11.3.4 All platforms

Timestamps such as Date Created and Date Modified are not persisted during transfers.

11.4 File name length and total path length

Each operating system imposes its own restriction on file name length and possibly th etotal path length. For example, Windows has a path length restriction of 260 chars for path and file name combined whereas Linux imposes a 255 char limit for the file name and a maximum of 4096 chars for the file path on Ext4 file systems.

For this reason, errors may be encountered when transferring a file from one operating system to another if a file path limit is breached while attempting writing the file to disk.

11.5 Case sensitivity

File names are case sensitive in Linux. Two files named a.log and A.LOG can co-exist in the same Linux directory. If both files are transferred to Windows in the same session, the first file will be overwritten by the second.

Windows superficially supports case sensitive file names but internally they are stored without reference to case. As such, a user is not permitted to create say a.log then A.LOG in the same directory. Hence, it is not possible to send two files with the same name but differing cases (from the same directory) from Windows to Linux. Windows files transferred to Linux will preserve case sensitivity.

Mac is similar to Windows with respect to case sensitivity of file names.

11.6 Links and shortcuts

Windows provides shortcuts and links to files/directories. Both types of shortcuts can be transferred, in the case of a link (hard or otherwise) the content of the linked file will be transferred, for shortcuts the shortcut (.lnk) file itself will be transferred without the linked content.

Linux has soft (symbolic) links to files/directories and hard links to files. Both types of links can be specified in a transfer request. The name of the file/directory link will be reflected in the file/directory transferred to Windows.

Mac OS X has aliases, soft links and hard links. Only files represented by hard links can be successfully transferred by the netPump® service.

11.7 File path collisions

11.7.1 Transfers from multiple origin filesystems

When transferring files from two separate filesystems attached to an origin service, if the files share a common path aside from their drive letter, share root, etc, one file will be transferred and any remaining 'collisions' will be flagged and not transferred.

For example, a transfer of:

C:\Data\Files\Example.dat
D:\Data\Files\Example.dat

Will result in one of the above files only being written to the nominated folder on the destination service filesystem, for example:

C:\TransferIn\Data\Files\Example.dat

The file which is not transferred will be marked as errored.

11.7.2 Transfer to a destination filesystem having an existing file

If an attempt is made to transfer a file to a location on the destination filesystem having the same path as an existing file with the same name, the transfer file will be marked as errored.

12 Legal

The netPump® Data service is copyright © Pacbyte Limited 2020. All rights reserved.

The netPump® Data service includes certain third-party software, the licence terms of which are included in this section.

Atom / Electron

MIT License

Copyright (c) 2011-2017 GitHub Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Dapper

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%)

or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform,

sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and
You must cause any modified files to carry prominent notices stating that You changed the files; and
You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

FluentAssertions

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and
You must cause any modified files to carry prominent notices stating that You changed the files; and
You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

Serilog

make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and
You must cause any modified files to carry prominent notices stating that You changed the files; and
You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.