

## Contents

1	Introduction.....	2
2	Requirements .....	2
3	Installation.....	2
3.1	Niagara Software Module Installation .....	2
3.2	Niagara Software Licensing.....	2
4	Getting Started with OSS Webhook .....	3
5	OSS Webhook Palette.....	5
6	OssWebhook Component Reference .....	6
6.1	OssWebhookService .....	6
6.2	Endpoint .....	6
6.3	Authentication Definitions.....	7
7	Examples .....	9
7.1	URL API Key Authentication.....	9
7.2	HTTP Header API Key Authentication .....	10
7.3	Authentication Group .....	11
8	Appendix .....	12
8.1	End User License Agreement.....	12

## 1 Introduction

This document provides instructions on how to install and use the OSS Webhook server module. This module enables external services to send data to a Niagara station using a [Webhook](#).

## 2 Requirements

It is assumed that the user is trained in the use of Niagara 4.

The OSS Webhook software is only compatible with Niagara versions 4.10 or later.

You must read the [End User License Agreement](#) at the end of this document before using this software.

## 3 Installation

### 3.1 Niagara Software Module Installation

Before the OSS Webhook software can be used, the Niagara software modules must be installed on the user's PC and the target host.

The 'ossWebhook-rt.jar' and 'ossWebhook-wb.jar' files supplied by One Sight Solutions must be installed on the host using the Niagara platform software manager.

This software file must also be installed in the appropriate Niagara modules directory of any PC on which you intend to access the OSS Webhook software.

### 3.2 Niagara Software Licensing

The host running the OSS Webhook software must be licensed by One Sight Solutions before it will operate correctly.

The following information is required to generate the OSS Webhook license:

- Niagara host identifier (e.g. Qnx-TITAN-0000-XXXX-XXXX).
- Niagara host serial number (if the host is not a supervisor).

Please send this information to One Sight Solutions: [sales@onesight.solutions](mailto:sales@onesight.solutions)

It is recommended that the license is installed on the Niagara host using the platform license manager import capability to download the license directly from the Niagara license server over the internet.

If it is not possible for the host to download the license from the internet then One Sight Solutions can supply the necessary license files which can be installed manually.

Ensure that the One Sight Solutions certificate is also installed, so the Niagara platform license manager should show both of the following files:

- OneSightSolutions.license
- OneSightSolutions.certificate

The host should reboot during the license installation process.

## 4 Getting Started with OSS Webhook

The following is a basic introduction to using the OSS Webhook software.

First open the 'OSS Webhook' palette.

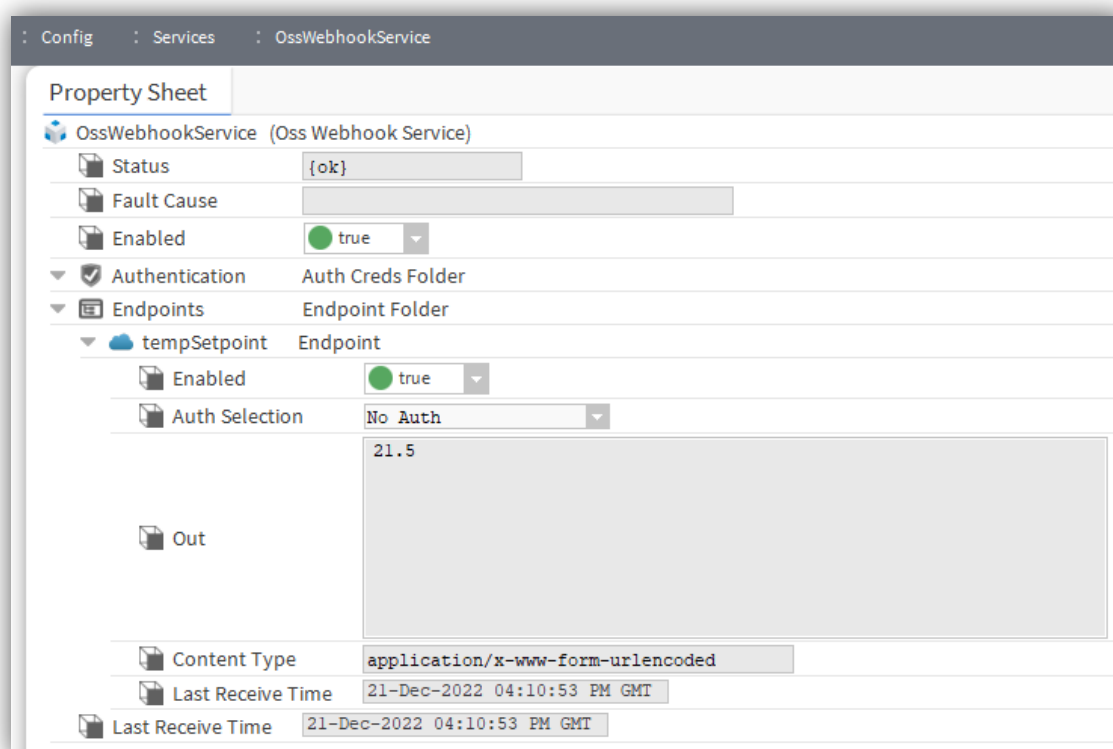
Drag the OssWebhookService component from the palette into the Niagara Services folder.

Expand the installed OssWebhookService component so the 'Endpoints' sub-folder is visible.

Drag an 'Endpoint' component from the palette into the 'Endpoint' folder.

Name the new endpoint component the identifier you wish to use for the webhook endpoint URL.

This should look something like **Figure 1**.



**Figure 1: OssWebhook example**

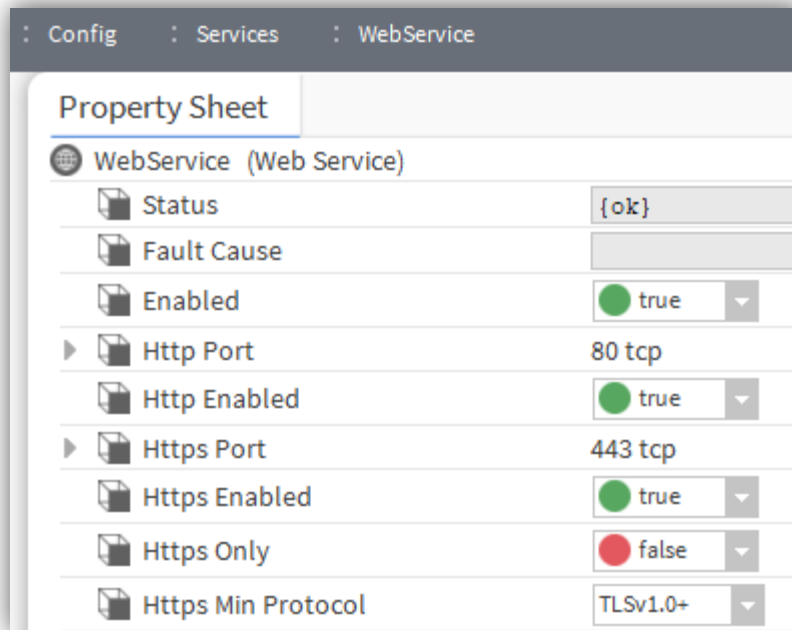
This now makes an unauthenticated HTTP webhook endpoint available that external systems can post data to.

To test the endpoint you have to send a HTTP POST request to the Niagara web server with the URL path starting with 'ossWebhook' followed by the name you gave your endpoint.

For example, if you called the endpoint 'tempSetpoint' and were accessing it from the same machine then the URL would be:

<http://localhost/ossWebhook/tempSetpoint>

**Note** that by default Niagara is configured to disable all insecure HTTP requests, so for this test to work you would need to enable insecure access in the Niagara Web Service by enabling HTTP ('Http Enabled' to true) and disabling HTTPS only ('Https only' to false). This is shown in **Figure 2**.



**Figure 2: Test WebService Settings**

As these settings put the Niagara station in an insecure state, make sure you change these settings back to the secure defaults when you have finished testing.

One simple way to test this insecure webhook is to use the Microsoft Windows built-in 'curl' PowerShell command.

Open a PowerShell prompt and enter the following command:

```
curl -URI "http://localhost/ossWebhook/tempSetpoint" -Method "POST" -Body "21.5"
```

This will send the value '21.5' to the endpoint 'Out' property (as shown in **Figure 1**).

The PowerShell output should look like **Figure 3**.

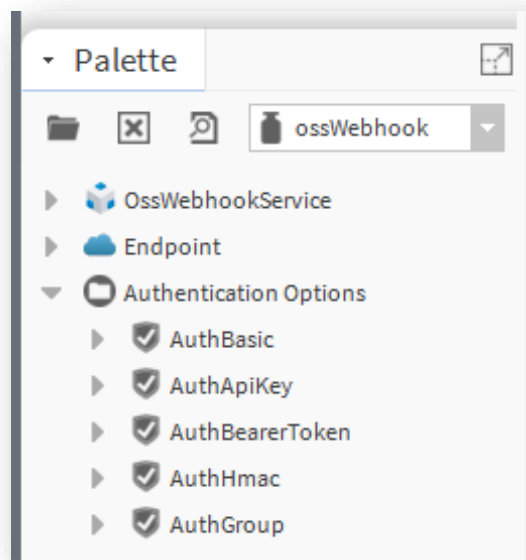
```
PS C:\Users\Adrian> curl -URI "http://localhost/ossWebhook/tempSetpoint" -Method "POST" -Body "21.5"

StatusCode      : 200
StatusDescription : OK
Content         : {"success":true}
RawContent      : HTTP/1.1 200 OK
                  x-frame-options: sameorigin
                  x-xss-protection: 1; mode=block
                  x-content-type-options: nosniff
                  Content-Length: 18
                  Content-Type: application/json
                  Expires: Thu, 01 Jan 1970 00:00:00 G...
Forms           : {}
Headers         : [[x-frame-options, sameorigin], [x-xss-protection, 1; mode=block], [x-content-type-
Images          : {}
InputFields     : {}
Links           : {}
ParsedHtml      : mshtml.HTMLDocumentClass
RawContentLength : 18
```

**Figure 3: PowerShell Test Output**

## 5 OSS Webhook Palette

**Figure 4** shows the OSS Easy API palette.



**Figure 4: OSS Webhook Palette**

**Table 1** has a brief description of each item in the palette.

Component	Function	Section	Page
OssWebhookService	The OssWebhook software service.	6.1	6
Endpoint	The component used to represent a Webhook endpoint.	6.2	6
AuthBasic	A Basic authentication definition.	6.3.1	7
AuthApiKey	An API key authentication definition.	6.3.2	7
AuthBearerToken	A Bearer Token authentication definition.	6.3.3	8
AuthHmac	A <a href="#">HMAC authentication</a> definition.	6.3.4	8
AuthGroup	A group of authentication definitions.	6.3.5	8

**Table 1: OSS Webhook Palette Items**

## 6 OssWebhook Component Reference

### 6.1 OssWebhookService

The OssWebhookService is the container for all elements that define the webhook endpoints and authentication credentials.

#### 6.1.1 Authentication Folder

The 'Authentication' folder contains all the authentication credential definitions that can be used by the webhook endpoints.

Note that each authentication definition can be used by more than one endpoint.

Authentication definitions can be added to the folder by dragging from the palette or using the folder actions.

These authentication credential components are described further in the following sections.

#### 6.1.2 Endpoints Folder

The 'Endpoints' folder contains all the endpoints definitions.

A new endpoint definition can be dragged from the palette or added using the folder action.

The endpoint definition component is described further in section 6.2.

### 6.2 Endpoint

The 'Endpoint' component is used to define an endpoint available from the webhook service when placed in the service endpoint folder.

A new endpoint definition can be dragged from the palette or added using the folder action.

#### 6.2.1 Endpoint URL

The name of the endpoint component is used as the suffix to the endpoint URL.

All OSS Webhook endpoint URLs start with the 'ossWebhook' prefix (after the host name).

The name of the endpoint component is placed after this prefix (separated by a forward slash).

For example, if an endpoint component is named 'meterData' then the OSS Webhook endpoint URL would be:

`https://<host-name>/ossWebhook/meterData`

#### 6.2.2 Endpoint Properties

##### 6.2.2.1 Enable

If the 'Enable' property is set to false then any requests to this endpoint will return an error (400, bad request). Otherwise the endpoint will operate normally.

##### 6.2.2.2 Auth Selection

The 'Auth Selection' property defines the authentication to be used for the endpoint.

A drop down list of options is provided.

When the default 'No Auth' option is selected no authentication is required to access the endpoint.

All other options are obtained from the list of authentication credential definitions that have been added to the service 'Authentication' folder.

#### 6.2.2.3 Post Data

The 'Post Data' property contains the data that has been sent to the endpoint in a POST request.

This data can be cleared by using the 'Clear Post Data' endpoint action.

#### 6.2.2.4 Post Content Type

The 'Post Content Type' property contains the HTTP header 'Content-Type' MIME type that was sent with the endpoint POST request. This usually describes the post data format.

#### 6.2.2.5 Last Request Time

The 'Last Request Time' contains the time of the last request to this endpoint.

### 6.3 Authentication Definitions

Authentication definitions are taken from the authentication options section of the OSS Webhook palette and placed in the service Authentication folder.

Various types of authentication credentials are available as described in the following sections.

Each endpoint can select a single authentication definition or a 'AuthGroup' component can be used to allow an endpoint to support multiple different authentication definitions.

Each authentication definition can be used by more than one endpoint.

All authentication definitions have an expiry mechanism which is described in section 6.3.6.

All authentication definitions also have an enable property which when disabled makes the authentication entry invalid.

It should be noted that these authentication mechanisms do not provide any encryption capability. If data encryption is required then the application should enforce HTTPS connections to provide this.

#### 6.3.1 AuthBasic

The AuthBasic component provides [HTTP basic access authentication \(RFC 7617\)](#).

This allows simple user, password information to be stored in HTTP header of the webhook endpoint request.

#### 6.3.2 AuthApiKey

The AuthApiKey component provides an API key authentication capability.

The API key may be provided in an endpoint client request either as a HTTP header or as a URL query.

The component has properties to control whether a header entry, URL query or both are allowed.

The 'Key Name' property defines a name that is either used as the HTTP header name or the URL query parameter key.

The 'Key Value' property defines the value that the endpoint client must set the key value to.

For example, if the Key Name is set to 'XToken' and the Key Value is set to '123456' then a client can be authorised by including the following HTTP header:

XToken: 123456

Or by adding the following URL query to the end of the endpoint URL:

?XToken=123456

### 6.3.3 AuthBearerToken

The AuthBearerToken component provides support for an OAuth 2.0 compatible bearer token HTTP header ([RFC 6750](#)).

The 'Token Value' property is used to specify the bearer token value.

This token value must then be included in the endpoint request HTTP header in the usual format by adding a 'Authorization' HTTP header entry with the value 'Bearer' followed by a space and then the required token value:

```
Authorization: Bearer <Token-Value>
```

### 6.3.4 AuthHmac

The AuthHmac component provides support for using a [HMAC cryptographic hash function](#) to validate the integrity of the data posted to the endpoint using a secret key.

The 'Header Name' property defines the HTTP header name that will be used to store the generated hash value.

The 'Hash Algorithm' property defines the hash algorithm that is used to generate the hash value from the secret key and the post data.

The 'Secret Key' property defines the secret value that will be combined with the post data to generate the hash value.

This authentication mechanism has the advantage that the contents of the data posted to the endpoint can be verified as well as providing an authentication capability. But this does require additional work by the client to generate the hash value for every request.

### 6.3.5 AuthGroup

The AuthGroup component allows an endpoint to support more than one authentication definition.

Authentication definitions are placed inside the AuthGroup component and then if an endpoint chooses the AuthGroup for its Auth Selection then any of the nested authentication definitions will be valid for that endpoint.

### 6.3.6 Authentication Definition Expiry

All authentication definitions have expiry properties.

If the 'Enable Expiry' property is set to false then the definition will never expire.

Otherwise the definition will remain valid until after the date/time defined by the 'Expiry' property.



## 7 Examples

### 7.1 URL API Key Authentication

This example shows the use of an endpoint with URL API key authentication.

This mechanism places the user defined API key at the end of the endpoint URL.

The OssWebhookService properties are shown in the following screenshot:

The screenshot displays the 'Property Sheet' for 'OssWebhookService (Oss Webhook Service)'. The configuration is as follows:

- Status:** {ok}
- Fault Cause:** (empty)
- Enabled:** true
- Authentication:** Auth Creds Folder
  - loraKey:** Auth Api Key
    - Enabled:** true
    - Key Name:** token
    - Key Value:** zPShY8Uh0LidgL2j
    - Allow Http Header:** false
    - Allow Url Param:** true
    - Enable Expiry:** false
    - Expiry:** 01-Jan-2050 12:00 AM GMT
- Endpoints:** Endpoint Folder
  - loraData:** Endpoint
    - Enabled:** true
    - Auth Selection:** loraKey
    - Post Data:** {'devEUI':'12345678abcdefgh','temperature':20.7}
    - Post Content Type:** application/x-www-form-urlencoded
    - Last Request Time:** 11-Jan-2023 10:51:36 AM GMT

The PowerShell curl command for sending data to this endpoint would look like following:

```
curl -URI "http://localhost/ossWebhook/loraData?token=zPShY8Uh0LidgL2j"
      -Method "POST"
      -Body "{ 'devEUI': '12345678abcdefgh', 'temperature': 20.7 }"
```

## 7.2 HTTP Header API Key Authentication

This example shows the of use an endpoint with HTTP header API key authentication.

This mechanism places the user defined API key in the HTTP header.

The OssWebhookService properties are shown in the following screenshot:

The screenshot displays the 'Property Sheet' for 'OssWebhookService (Oss Webhook Service)'. It is organized into sections: 'Authentication' and 'Endpoints'. Under 'Authentication', the 'alarmCreds' section is expanded, showing 'Auth Creds Folder' as 'Auth Api Key'. Properties include 'Enabled' (true), 'Key Name' (X-Token), 'Key Value' (xUatYu7ytM9LjSYa), 'Allow Http Header' (true), 'Allow Url Param' (false), 'Enable Expiry' (false), and 'Expiry' (01-Jan-2050 12:00 AM GMT). Under 'Endpoints', the 'alarmStatus' endpoint is expanded, showing 'Enabled' (true), 'Auth Selection' (alarmCreds), 'Post Data' (a JSON object), 'Post Content Type' (application/x-www-form-urlencoded), and 'Last Request Time' (11-Jan-2023 10:54:15 AM GMT).

Property Sheet	
OssWebhookService (Oss Webhook Service)	
Status	{ok}
Fault Cause	
Enabled	<input checked="" type="radio"/> true
Authentication	Auth Creds Folder
alarmCreds	Auth Api Key
Enabled	<input checked="" type="radio"/> true
Key Name	X-Token
Key Value	xUatYu7ytM9LjSYa
Allow Http Header	<input checked="" type="radio"/> true
Allow Url Param	<input type="radio"/> false
Enable Expiry	<input type="radio"/> false
Expiry	01-Jan-2050 12:00 AM GMT
Endpoints	Endpoint Folder
alarmStatus	Endpoint
Enabled	<input checked="" type="radio"/> true
Auth Selection	alarmCreds
Post Data	{'alarmId':'1234abcd','state':'offnormal'}
Post Content Type	application/x-www-form-urlencoded
Last Request Time	11-Jan-2023 10:54:15 AM GMT
Last Request Time	11-Jan-2023 10:54:15 AM GMT

The PowerShell curl command for sending data to this endpoint would look like following:

```
curl -URI "http://localhost/ossWebhook/alarmStatus"  
      -Headers @{ 'X-Token' = 'xUatYu7ytM9LjSYa' }  
      -Method "POST"  
      -Body "{ 'alarmId':'1234abcd','state':'offnormal' }"
```

### 7.3 Authentication Group

This example shows the use of an endpoint with an authentication group which contains multiple authentication options.

The OssWebhookService properties are shown in the following screenshot:

The screenshot displays the 'Property Sheet' for the 'OssWebhookService (Oss Webhook Service)'. The interface is organized into a tree view on the left and a corresponding configuration area on the right.

- OssWebhookService (Oss Webhook Service)**
  - Status**: {ok}
  - Fault Cause**: (empty field)
  - Enabled**: ☒ true
  - Authentication** (Auth Creds Folder)
    - credsGroup** (Auth Group)
      - secureCreds** (Auth Hmac)
        - Enabled**: ☒ true
        - Header Name**: X-HmacSha256
        - Hash Algorithm**: HmacSHA256
        - Secret Key**: se2wJ4gew6GhxxVpvuPNxqmy
        - Enable Expiry**: ☐ false
        - Expiry**: 01-Jan-2050 12:00 AM GMT
      - temporaryCreds** (Auth Basic)
        - Enabled**: ☒ true
        - Username**: guest
        - Password**: (masked with dots)
        - Enable Expiry**: ☒ true
        - Expiry**: 01-Mar-2023 12:00 AM GMT
      - otherAccess** (Auth Api Key)
    - Endpoints** (Endpoint Folder)
      - tempSetpoint** (Endpoint)
        - Enabled**: ☒ true
        - Auth Selection**: credsGroup
        - Post Data**: 20.5
        - Post Content Type**: application/x-www-form-urlencoded
        - Last Request Time**: 11-Jan-2023 10:41:45 AM GMT
    - Last Request Time**: 11-Jan-2023 10:41:45 AM GMT

## 8 Appendix

### 8.1 End User License Agreement

#### 8.1.1 License

By receiving, opening the file package, and/or using OSS Webhook ("Software") containing this software, you agree that this End User License Agreement (EULA) is a legally binding and valid contract and agree to be bound by it. You agree to abide by the intellectual property laws and all of the terms and conditions of this Agreement.

Unless you have a different license agreement signed by One SightSolutions Ltd your use of OSS Webhook indicates your acceptance of this license agreement and warranty.

Subject to the terms of this Agreement, One SightSolutions Ltd grants to you a limited, non-exclusive, non-transferable license, without right to sub-license, to use OSS Webhook in accordance with this Agreement and any other written agreement with One SightSolutions Ltd. One SightSolutions Ltd does not transfer the title of OSS Webhook to you; the license granted to you is not a sale. This agreement is a binding legal agreement between One SightSolutions Ltd and the purchasers or users of OSS Webhook.

If you do not agree to be bound by this agreement, remove OSS Webhook from your computer now and, if applicable, promptly return to One SightSolutions Ltd by mail any copies of OSS Webhook and related documentation and packaging in your possession.

#### 8.1.2 Distribution

ossEasyAPI and the license herein granted shall not be copied, shared, distributed, re-sold, offered for re-sale, transferred or sub-licensed in whole or in part except that you may make one copy for archive purposes only. For information about redistribution of OSS Webhook contact One SightSolutions Ltd.

#### 8.1.3 User Agreement

##### 8.1.3.1 Use

Your license to use OSS Webhook is limited to the number of licenses purchased by you. You shall not allow others to use, copy or evaluate copies of OSS Webhook.

##### 8.1.3.2 Use Restrictions

You shall use OSS Webhook in compliance with all applicable laws and not for any unlawful purpose. Without limiting the foregoing, use, display or distribution of OSS Webhook together with material that is pornographic, racist, vulgar, obscene, defamatory, libellous, abusive, promoting hatred, discriminating or displaying prejudice based on religion, ethnic heritage, race, sexual orientation or age is strictly prohibited.

Each licensed copy of OSS Webhook may be used on one single computer location by one user. Use of OSS Webhook means that you have loaded, installed, or run OSS Webhook on a computer or similar device. If you install OSS Webhook onto a multi-user platform, server or network, each and every individual user of OSS Webhook must be licensed separately.

You may make one copy of OSS Webhook for backup purposes, providing you only have one copy installed on one computer being used by one person. Other users may not use your copy of OSS Webhook. The assignment, sublicense, networking, sale, or distribution of copies of OSS Webhook are strictly forbidden without the prior written consent of One SightSolutions Ltd. It is a violation of this agreement to assign, sell, share, loan, rent, lease, borrow, network or transfer the use of OSS

Webhook. If any person other than yourself uses OSS Webhook registered in your name, regardless of whether it is at the same time or different times, then this agreement is being violated and you are responsible for that violation!

#### *8.1.3.3 Copyright Restriction*

This Software contains copyrighted material, trade secrets and other proprietary material. You shall not, and shall not attempt to, modify, reverse engineer, disassemble or decompile OSS Webhook. Nor can you create any derivative works or other works that are based upon or derived from OSS Webhook in whole or in part.

One SightSolutions Ltd's name, logo and graphics file that represents OSS Webhook shall not be used in any way to promote products developed with OSS Webhook. One SightSolutions Ltd retains sole and exclusive ownership of all right, title and interest in and to OSS Webhook and all Intellectual Property rights relating thereto.

Copyright law and international copyright treaty provisions protect all parts of OSS Webhook, products and services. No program, code, part, image, audio sample, or text may be copied or used in any way by the user except as intended within the bounds of the single user program. All rights not expressly granted hereunder are reserved for One SightSolutions Ltd.

#### *8.1.3.4 Limitation of Responsibility*

You will indemnify, hold harmless, and defend One SightSolutions Ltd, its employees, agents and distributors against any and all claims, proceedings, demand and costs resulting from or in any way connected with your use of One SightSolutions Ltd's Software.

In no event (including, without limitation, in the event of negligence) will One SightSolutions Ltd, its employees, agents or distributors be liable for any consequential, incidental, indirect, special or punitive damages whatsoever (including, without limitation, damages for loss of profits, loss of use, business interruption, loss of information or data, or pecuniary loss), in connection with or arising out of or related to this Agreement, OSS Webhook or the use or inability to use OSS Webhook or the furnishing, performance or use of any other matters hereunder whether based upon contract, tort or any other theory including negligence.

One SightSolutions Ltd's entire liability, without exception, is limited to the customers' reimbursement of the purchase price of the Software (maximum being the lesser of the amount paid by you and the suggested retail price as listed by One SightSolutions Ltd) in exchange for the return of the product, all copies, registration papers and manuals, and all materials that constitute a transfer of license from the customer back to One SightSolutions Ltd.

#### *8.1.3.5 Warranties*

Except as expressly stated in writing, One SightSolutions Ltd makes no representation or warranties in respect of this Software and expressly excludes all other warranties, expressed or implied, oral or written, including, without limitation, any implied warranties of merchantable quality or fitness for a particular purpose.

#### *8.1.3.6 Governing Law*

This Agreement shall be governed by the law of the United Kingdom applicable therein. You hereby irrevocably attorn and submit to the non-exclusive jurisdiction of the courts of United Kingdom therefrom. If any provision shall be considered unlawful, void or otherwise unenforceable, then that provision shall be deemed severable from this License and not affect the validity and enforceability of any other provisions.

#### 8.1.3.7 Termination

Any failure to comply with the terms and conditions of this Agreement will result in automatic and immediate termination of this license. Upon termination of this license granted herein for any reason, you agree to immediately cease use of OSS Webhook and destroy all copies of OSS Webhook supplied under this Agreement. The financial obligations incurred by you shall survive the expiration or termination of this license.

#### 8.1.4 Disclaimer Of Warranty

**This software and the accompanying files are sold "as is" and without warranties as to performance or merchantability or any other warranties whether expressed or implied. this disclaimer concerns all files generated and edited by OSS Webhook as well.**

#### 8.1.5 Consent Of Use Of Data

You agree that One SightSolutions Ltd may collect and use information gathered in any manner as part of the product support services provided to you, if any, related to OSS Webhook. One SightSolutions Ltd may also use this information to provide notices to you which may be of use or interest to you.

End of license agreement