

# **Sage ID SSO Notifications via Sage Secure Gateway**

Sage (UK) Central R&D SSDP Team

Revision History

Revision	Author	Notes
1.0	GD	<ul style="list-style-type: none"><li>Initial version.</li></ul>



Table of Contents

- 1. Introduction.....4
  - 1.1. SSO Notifications.....4
  - 1.2. Sage Secure Gateway .....4
  - 1.3. Pre-requisites.....5
  - 1.4. Limitations .....5
- 2. Installation and Configuration .....7
  - 2.1. Overview .....7
  - 2.2. Gateway Client Installation .....7
  - 2.3. Proxy Configuration .....8
  - 2.4. Installing the Notification Data Service .....9
  - 2.5. Configuring the SSO Notifications Data Service .....11
- 3. Monitoring and Troubleshooting.....13
  - 3.1. Monitoring .....13
  - 3.2. Troubleshooting .....14

## 1. Introduction

### 1.1. SSO Notifications

Sage ID sends messages known as “SSO notifications” to web applications to inform them in real-time of important events in the session lifecycle.

In the current version of Sage ID, the following notifications are sent:

- Session.ExpiryDue

This notification is sent three minutes before an application’s participation in an SSO session expires. It provides an opportunity for an application to extend an SSO session to match your application session.

- Session.Ended

This notification is sent after an application’s participation in an SSO session has expired. An application should, in response, immediately close the application session associated with the SSO session.



*These messages and how to handle them are described in more detailed in the SSO developer guide section “Understanding the Session Lifecycle”.*

It is important that web applications handle notifications properly so that the correct behaviour with respect to single sign-out can be achieved.

Notifications are a “push” from Sage ID to the web application. That is, Sage ID makes an HTTP POST over the Internet to the web application.

For hosted production web applications this is not problematic since they are already open to the Internet. During development, however, testing notifications can be tricky for the following reasons:

- Applications in development are typically not exposed to the Internet for security reasons.
- There may be several developers working on an application, each running an instance of the same application on their desktop machine. Since notification URIs are configured inside Sage ID for each web application, only one developer’s instance would be able to receive notifications, at most.

In order to make testing the handling of notifications feasible for web applications in development, Sage ID supports relaying notifications via the Sage Secure Gateway.

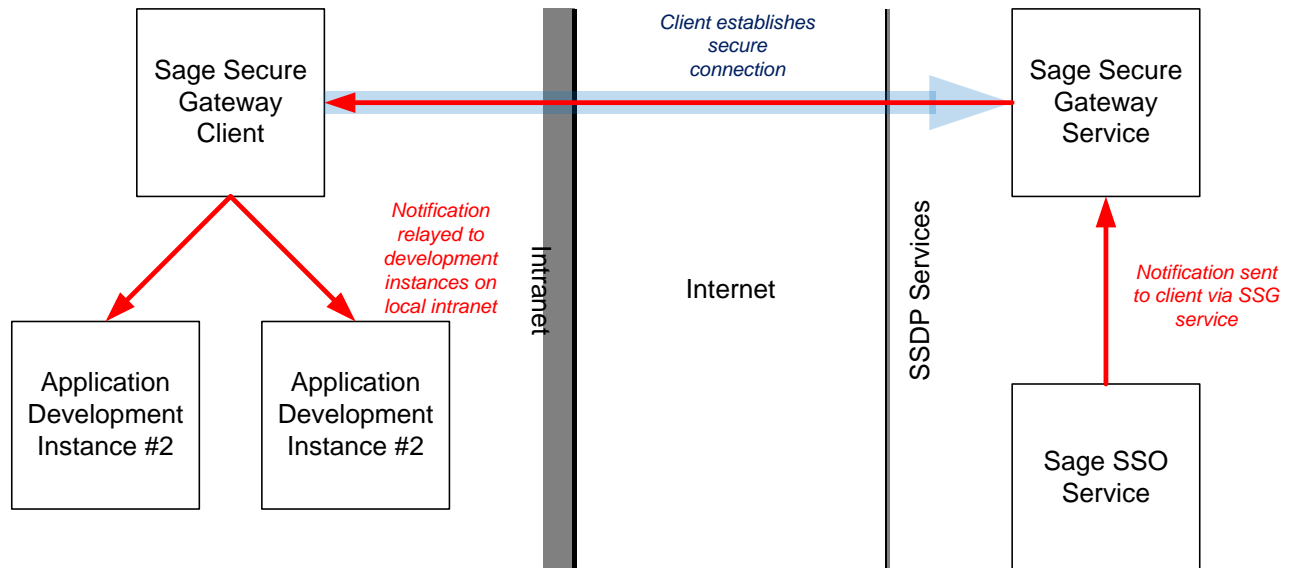
### 1.2. Sage Secure Gateway

The Sage Secure Gateway is a technology which allows external applications such as Sage ID to send messages in real-time to endpoints inside private networks without having to make any changes to firewall or port forwarding which might expose the private network directly to the Internet.

This is achieved by installing a small application – the Sage Secure Gateway Client – on a machine inside the private network. The Sage Secure Gateway Client makes a secure outbound connection over HTTP (via a proxy, if required) to the Sage Secure Gateway service and maintains this connection while the machine is running. When Sage ID sends a notification it checks to see if it should be delivered via the Sage Secure Gateway and, if so, dispatches the

notification accordingly. When the notification is received by the Sage Secure Gateway client, it is relayed to a list of endpoints configured locally.

The following diagram illustrates how Sage ID uses the Sage Secure Gateway to send notifications to web applications under development:



*The Sage Secure Gateway is a general purpose mechanism which can be used for remote access via SOAP or SData to systems and data within customer networks. For more details, please contact [ssdpdevelopersupport@sage.com](mailto:ssdpdevelopersupport@sage.com).*

### 1.3. Pre-requisites

In order to use notifications via the Sage Secure Gateway:

- Your application must be configured to receive notifications via the Sage Secure Gateway on the Sage ID server. Please contact [ssdpdevelopersupport@sage.com](mailto:ssdpdevelopersupport@sage.com) to have this done.
- You must install the Sage Secure Gateway client on a Windows machine inside your development network where it can:
  - Access the Internet using HTTP over port 80 and 443 either directly or via a proxy.
  - Relay notifications to your application development instances.

The Sage Secure Gateway client is supported on 32- and 64-bit versions of Windows XP and above. The client is lightweight and a small virtual instance of Windows is all that is required if a physical Windows machine is not available.

### 1.4. Limitations

There are some minor limitations to be aware of when using notifications via the Sage Secure Gateway:

- Each web application configuration on the SSO server can be configured for one Gateway client only.



You may request more than one web application configuration if you need to support separate development or test environments (for example: dev, pre-prod, UAT) and these can be configured individually as required but will each require a new certificate. *For more details, please contact **[ssdpdevelopersupport@sage.com](mailto:ssdpdevelopersupport@sage.com)**.*

- Notifications will only be relayed while the machine which has the Sage Secure Gateway client installed on it is running and has a connection to the Internet. The client runs as a Windows service, so there is no need to be logged in to receive notifications.
- There is a small amount of additional latency added by the Sage Secure Gateway, so notifications may not arrive as quickly as when delivered directly.
- Notifications via Sage Secure Gateway are supported by the Sage ID pre-production service only.

## 2. Installation and Configuration

### 2.1. Overview

This section describes how to install and configure the Sage Secure Gateway client.


### 2.2. Gateway Client Installation

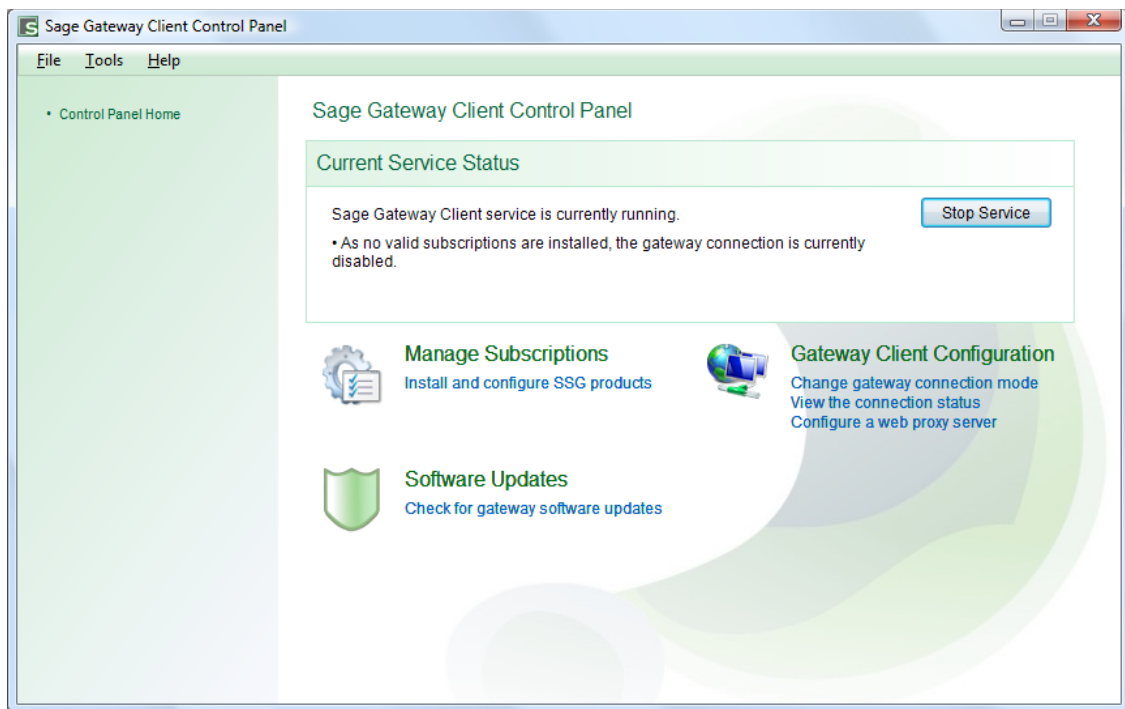
Double-click the Gateway Client installer executable to begin the installation.



Click through the wizard to accept the licence agreement and to install to the default location.

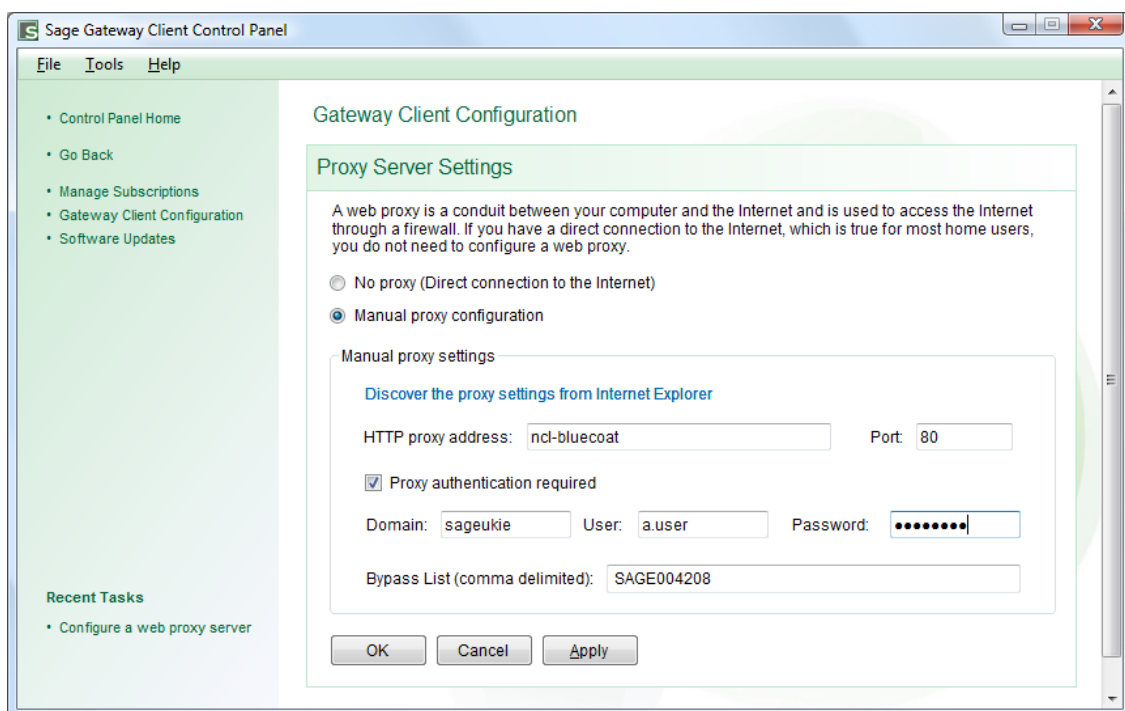
## 2.3. Proxy Configuration

When the Gateway Client has installed, open the Gateway Client control panel by double-clicking the  icon in the task tray, or from the start menu:



If the machine upon which the Gateway Client is installed is behind a proxy, click "Configure a web proxy server" on the displayed dialog to review your proxy information.

The installer configures the Gateway Client with proxy information from Internet Explorer. If your required proxy is not shown or is different, or if your proxy requires user credentials you should enter the required information here:

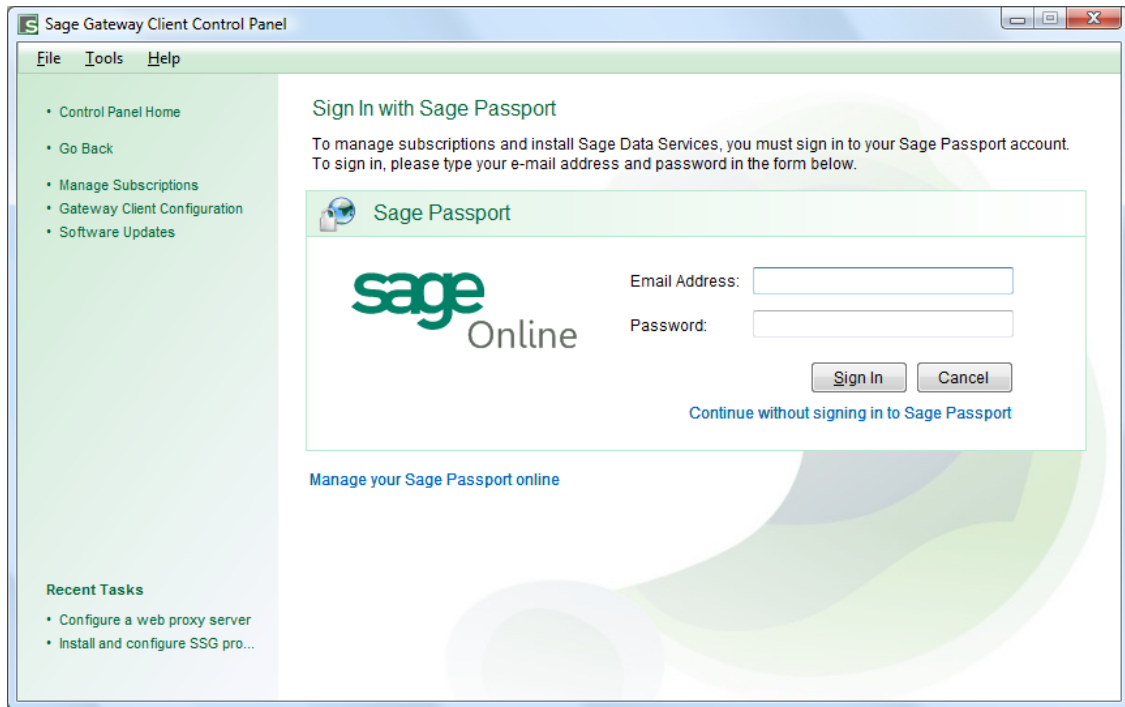




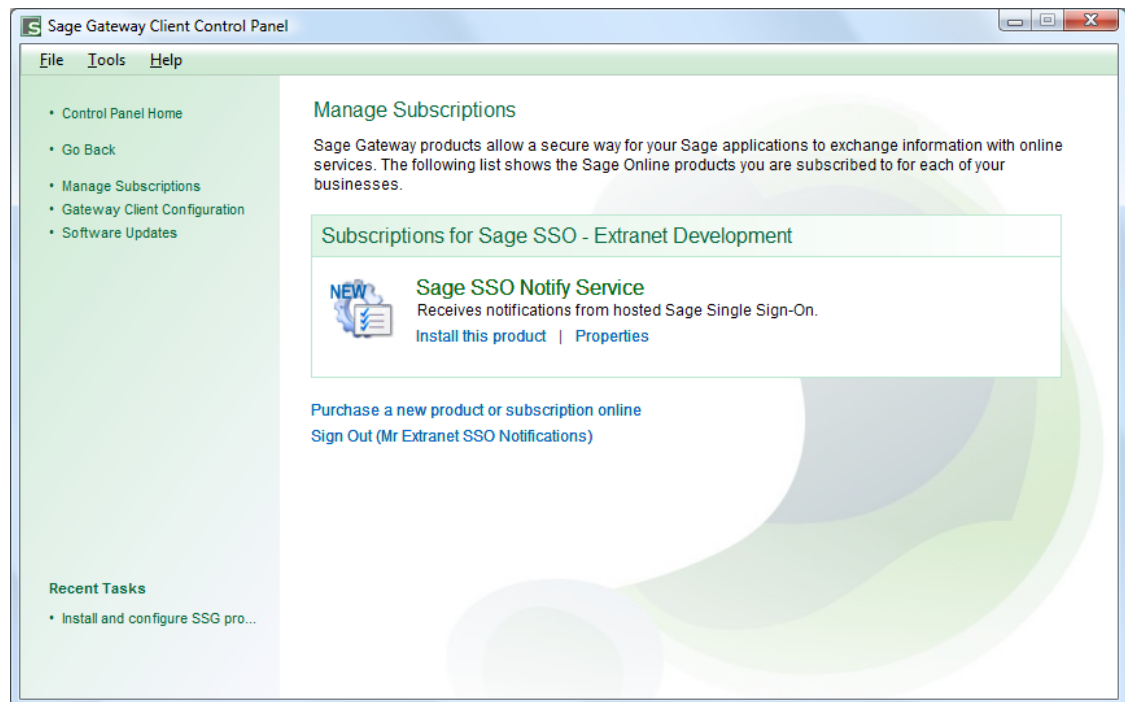
## 2.4. Installing the Notification Data Service

The Gateway Client hosts plug-ins called "data services". SSO notifications are received and delivered by a data service which must now be installed on the Gateway client.

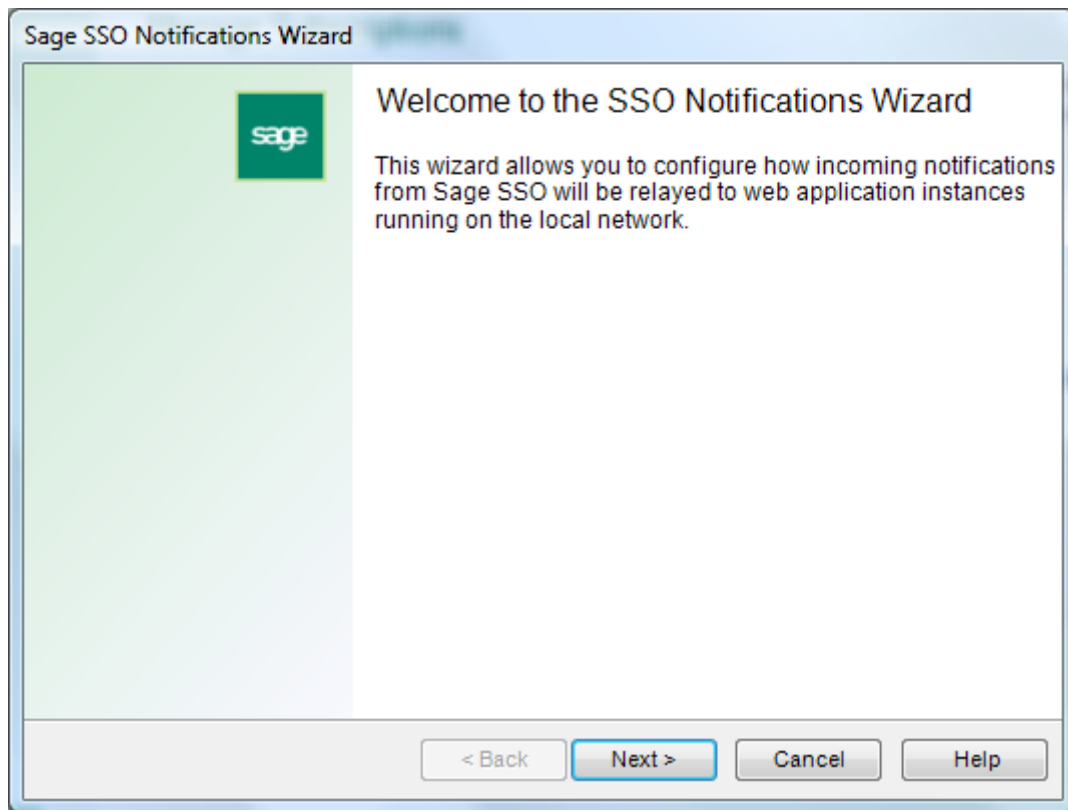
On the Gateway Client control panel home page, click "Manage Subscriptions". This will display the sign-in page:



Enter the username and password supplied to you by SSDP developer support and click sign-in. After a short delay, the subscriptions page will be displayed:

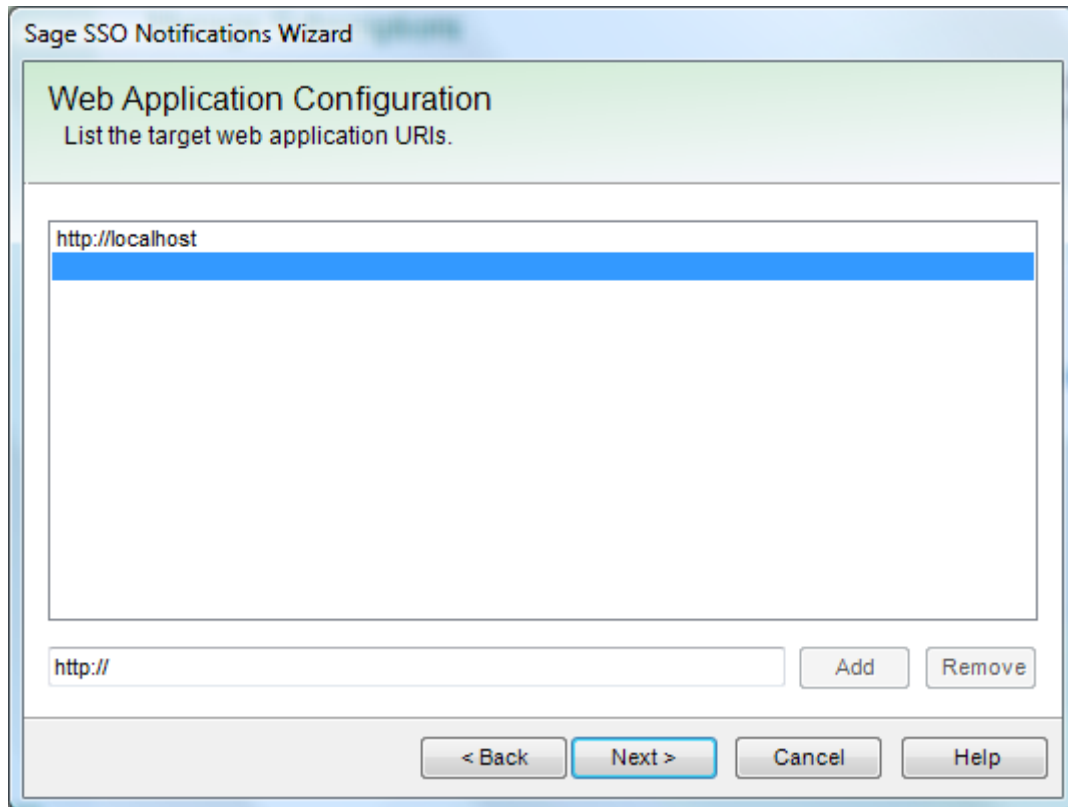


Click the "Sage SSO Notify Service" link to install the data service. The latest version of the data service is downloaded and installed automatically. When installation is complete, the configuration wizard will be displayed:



## 2.5. Configuring the SSO Notifications Data Service

Click "next" on the first page of the wizard to display the web application configuration page:



On this page, enter the notification URI for each local instance of your web application which is to receive SSO notifications.

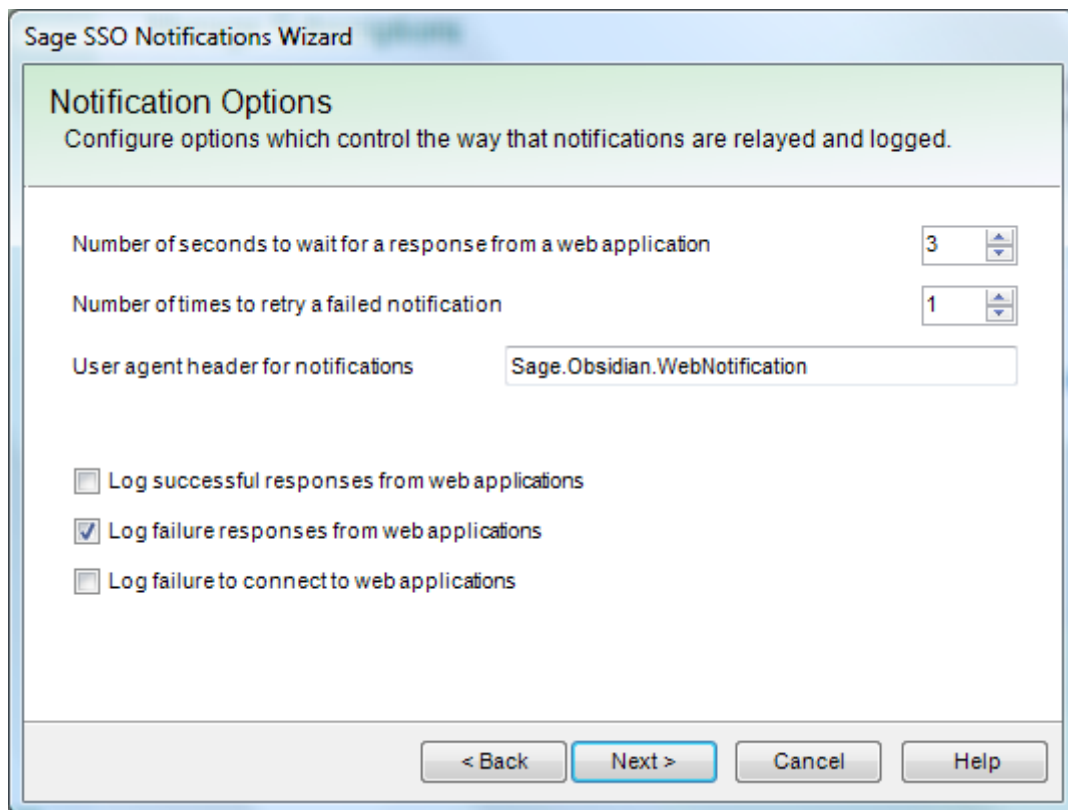
For example, if your application receives notifications posted to `notify.aspx` you would use <http://localhost/mywebapp/notify.aspx> to relay notifications to the application running on the local machine.

You can enter as many URIs as you require here. *All* notifications sent to your web application (as configured in Sage ID) will be relayed to *all* the URIs you specify.



*A given local instance of your web application may receive notifications for sessions which were not started by that instance (if you have multiple instances configured for the same web application). Your application should ignore notifications which don't relate to an existing application session. For more details, see the section "Understanding the Session Lifecycle" in the Sage ID Developer Guide.*

On the next page of the wizard, you can configure various options which govern *how* each message will be relayed to the URIs you specified:



The screenshot shows a window titled "Sage SSO Notifications Wizard" with a sub-header "Notification Options". Below the sub-header is the instruction "Configure options which control the way that notifications are relayed and logged." The main area contains three settings: "Number of seconds to wait for a response from a web application" set to 3, "Number of times to retry a failed notification" set to 1, and "User agent header for notifications" set to "Sage.Obsidian.WebNotification". There are three checkboxes: "Log successful responses from web applications" (unchecked), "Log failure responses from web applications" (checked), and "Log failure to connect to web applications" (unchecked). At the bottom are four buttons: "< Back", "Next >", "Cancel", and "Help".

For a detailed explanation of an option, move your mouse pointer over the corresponding label. After choosing your options, click "next" and then "finish" to save the changes. You may then close the Gateway Client control panel. You may also log off the machine, if required. Notifications will still be received and relayed while the machine is running.

You can return to the wizard at any time using the Gateway Client control panel.

## 3. Monitoring and Troubleshooting

### 3.1. Monitoring

The Gateway Client writes an activity log which includes information about notification forwarding. If the client is installed to the default location, the log directory is:

%programfiles%\Sage\SecureGatewayClient\Logs

Log entries related to notifications are prefixed with [ DataService:SSONotifyDataService ], as shown in the sample log output below.

```
16/12/2010 15:23:52 - [ DataService:SSONotifyDataService ] [ INFO ] Received notification 1 from SageSSO:

<Notification xmlns="http://sso.sage.com"><NotificationId>e9c92ee6-56f6-49c8-86b9-52e8264d41e6</NotificationId><Issued>2010-12-16T15:23:50.5267031Z</Issued><Type>Session.Ended</Type><Parameters><Parameter><Name>SessionId</Name><Value>3bc43079-6cc4-459e-9558-5cd63c0a8196</Value></Parameter><Parameter><Name>EmailAddress</Name><Value>ssouser1@mailinator.com</Value></Parameter><Parameter><Name>Reason</Name><Value>ApplicationControlled</Value></Parameter><Parameter><Name>Timestamp</Name><Value>2010-12-16T15:23:50.5267031Z</Value></Parameter></Parameters><Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo><CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" /><SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" /><Reference URI=""><Transforms><Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" /></Transforms><DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" /><DigestValue>qDTTrFPZISluSwnYF1Muh0WWD2vg=</DigestValue></Reference></SignedInfo><SignatureValue>ssrSHCmQ+jj9Q9i8EKkQaYmGiZNawFBB040oMDrFvxqW87sUHk9Lq7/o0U9ISV1Ii3zLYa/p/alitTgUzrCGXBGghlRzmMtZ2dXkdbGpxlKGnF0lBGACJkKmpFigVZ+gm1kyQ8SsXgjAGOCeqjI/KhAkIiaKzlvEjv71P4TmxMU=</SignatureValue></Signature></Notification>

16/12/2010 15:23:52 - [ DataService:SSONotifyDataService ] [ INFO ] Posting notification 1 to http://webappa.dev.sage.com/notify.aspx. Attempt = 1.
16/12/2010 15:23:52 - [ DataService:SSONotifyDataService ] [ INFO ] Success response received for notification 1 to http://webappa.dev.sage.com/notify.aspx on attempt 1. Status code = OK. Response headers:
Connection: close
Content-Length: 0
Cache-Control: private
Date: Thu, 16 Dec 2010 15:23:52 GMT
Server: Microsoft-IIS/7.0
X-AspNet-Version: 2.0.50727
X-Powered-By: ASP.NET

No response data.
```

If several notifications are received at the same time, messages in the log for a single notification may not be grouped together. For this reason, the Gateway Client numbers each notification so that related messages can be correlated in the log. The number resets back to 1 if the Gateway Client is restarted.



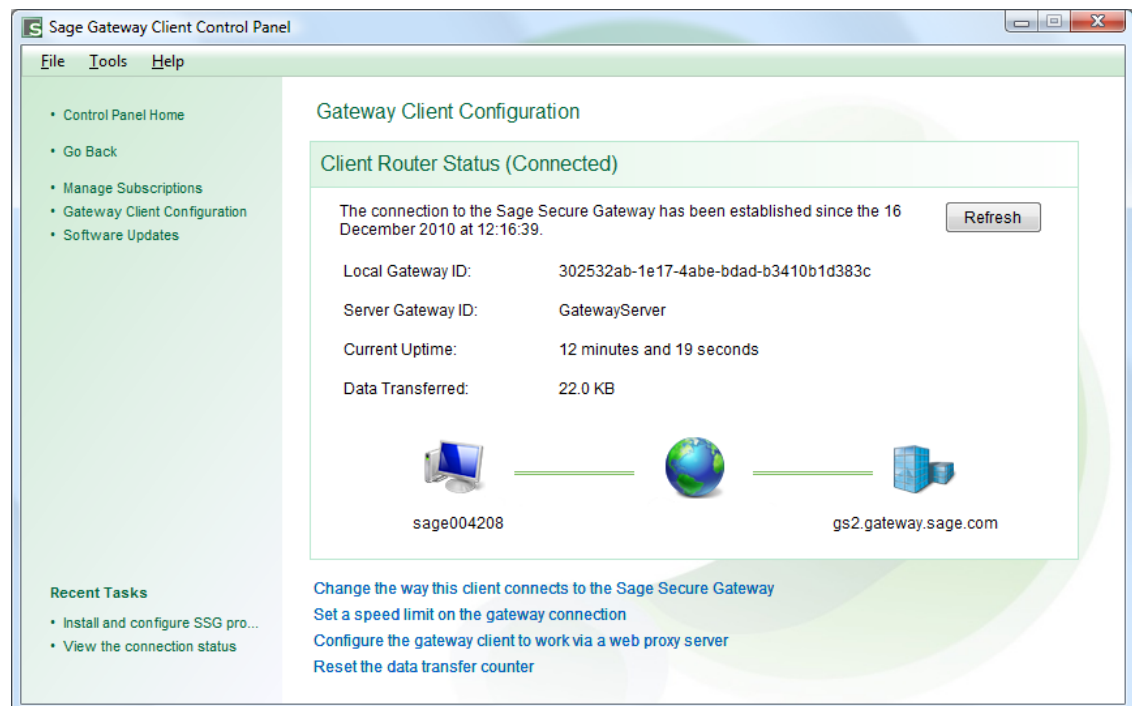
*It's a good idea to open a fileshare to the logs directory on the Gateway Client machine for easy remote access to the logs during development.*

### 3.2. Troubleshooting

If you are not receiving the notification messages you think you should be receiving, the following diagnostic actions may help:

- Check that the Gateway Client is running and has a connection to the Gateway Server.

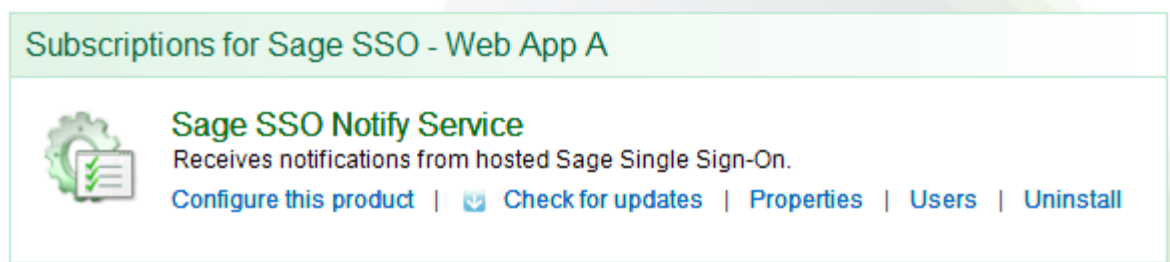
This can be checked using "View the connection status" from the Gateway Client control panel home page, as shown below:



- Check that the SSO Notify Service is installed.

Click "Manage subscriptions" and sign-in to the Gateway Client using the username and password supplied to you by SSDP developer support.

If the service is installed, it will appear like this:





*If the service is listed as "Currently installed on another Gateway Client" please check that no-one else on your team has installed the service on a different machine. The data service for a given web application configured in Sage ID may be installed on a single Gateway Client only.*

*Note that this message is normal if you have previously installed the data service on another machine and wish to re-install it on a different machine.*

- Check that the target web application URIs you have configured are correct.



*If you are targeting HTTPS URIs, the certificate presented by the web application must be trusted on the machine on which the Gateway Client is installed. If your certificate is self-signed you may need to install it or its root as a trusted root certification authority on the Gateway Client machine.*

- Ensure that all logging options are enabled, as show below:

- ☒ Log successful responses from web applications
- ☒ Log failure responses from web applications
- ☒ Log failure to connect to web applications

Review the Gateway Client log output. Most failures are readily apparent in the log.



*If you are still unable to resolve the problem please contact **[ssdpdevelopersupport@sage.com](mailto:ssdpdevelopersupport@sage.com)** for additional help.*