



Select Survey .NET



SelectSurvey.NET Install Guide v5

Updated 5-31-2024 (v5.066.000) to add TWILIO SMS Texting features to web.config.

Updated 11-15-2023 to add Universal from email and 2 factor authentication info.

This guide has more detailed information and helpful points for hosted customers. See Appendix D of this document for common problems and solutions.

Contents

SelectSurvey.NET Install Guide v5	2
Requirements Summary.....	4
Installation Checklist	4
Detailed Instructions for above steps:	5
Place Files on Web Server and configure IIS.....	5
Configure the Production and Archive Databases.	10
SQL Server 2008R2 or later required	10
Create the production database:.....	11
Create the archive database:	13
Edit WEB.CONFIG file for SMTP EMAIL AND SMS TEXTING.....	14
Edit WEB.CONFIG set LICENSE KEY and remaining keys.	16
Configure Application Wide Settings.....	16
Configure Permissions for File upload and JS on Server.....	16
Support.....	18
SMTP Universal "From" email where all other "from" is "reply-to".....	19
2 Factor Login Authentication.....	21
Appendix A: Application Pooling	21
Appendix B: Notes for different culture/globalization settings	23



Appendix C: Integrating with Active Directory and other Login Integration Add-Ons.....	25
ADFS – Active Directory Federated Login Integration.....	26
Configuring a New ADFS Trust Relationship	32
Google Federated Login Integration	47
OpenID Connect Login Integration (AZURE Active Directory, Office 365, OAuth2.0, IdentityServer3,Azure AD ID).....	64
CAS Login Integration	70
Standard (AD) Active Directory Login Integration with Login box (Also options for AD + SSO, LDAP, SAML, NTLM)	71
Configure AD permissions on web folder in IIS 7 (or higher):.....	75
How to enable NTLM for IIS 7:.....	85
Windows Server 2008 or Windows Server 2008 R2 Install Windows Authentication	88
Windows Vista or Windows Install Windows Authentication	89
How to enable Windows authentication in IIS 7	89
How to enable NTLM:	90
Browser NTLM Configuration: IE Browser.....	92
Browser NTLM Configuration: Firefox Browser	97
Mapping AD User Fields to SUR_USER Survey User Fields	99
Appendix D: Common Errors/Solutions.....	101
Appendix E: Preferred Hosting Providers	102
Appendix F: Windows Sharepoint Services	102
Appendix G: Web Farm Configuration.....	104
Appendix H: Single Sign on with SQL Membership Provider.....	109
Appendix I: Minimizing File Upload Feature Vulnerability	112

Requirements Summary

The SelectSurvey.NET Server Software requires a dedicated server with the below basic requirements:

1. Dedicated Windows Server 2008 or later (Microsoft Internet Information Server IIS7 or later) with a minimum of 2 Gigabytes of RAM.
2. .NET Framework 4.6.1 must be installed on the server, this build targets 4.6.1 for the TLS 1.2 requirements. A .net 4.5 application pool is required (that targets 4.6.1). (See Appendix A for details)
3. Microsoft SQL 2008R2 or later is required.
4. SMTP services installed on web server (recommended) or access to external SMTP.

Installation Checklist

The steps to install SelectSurveyNET are as follows:

☒ 1. **[Download and Unzip files.](#)**

Copy "files to copy to IIS" to web server.

☒ 2. **[Place files on Web Server and Configure Web Server.](#)**

Configure IIS root folder as an application to use .Net 4.6.1 Framework application pool.

☒ 3. **[Configure your database.](#)**

Write down connection string for next step.

☒ 4. **[Edit the WEB.CONFIG.](#)**

Enter your database connection string into the web.config. Edit other keys with your customized information. Enter **LICENSE KEY** in space provided or you will see free trial message. License key is generated in your customer account page on classapps.com on the product download page.

☒ 5. **[Login to set Global Application Settings after logging in with the browser.](#)**

Adjust default settings in the "admin tools" > "application wide settings" with the

web browser.

Detailed Instructions for above steps:

Place Files on Web Server and configure IIS.

1. **Download and Unzip files.**

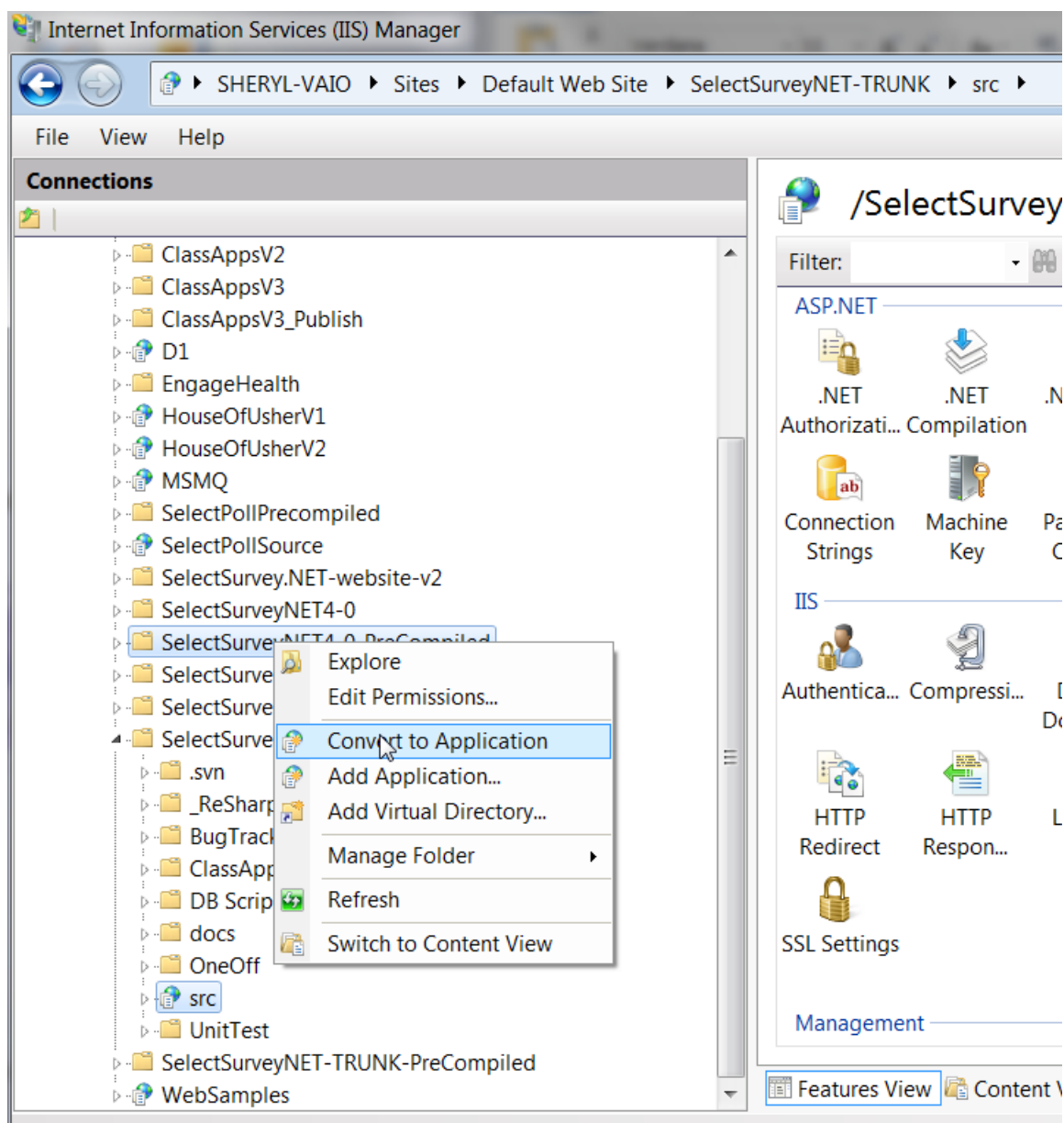
Unzip the files to a temporary directory. The zip file contains a folder of files to copy to the web server titled **"Files to copy to IIS"**, and a folder containing the solution project file and source code titled **"Source Code"** for development and customizations.

2. **Place files on Web Server and Configure Web Server.**

Copy the files inside the folder "Files to copy to IIS" to either your root web site folder or create a virtual directory in IIS that points to where you put the files, with whatever name you choose. Right click the folder in IIS 7 and click "convert to application". Select ".net 4.5 application pool".

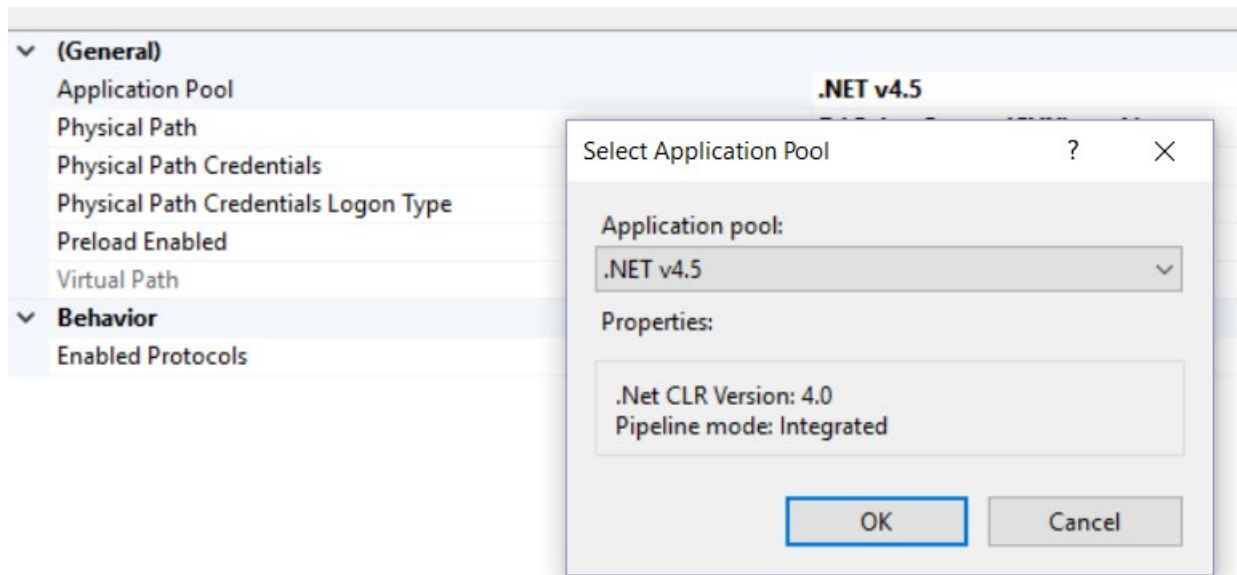
SelectSurvey.NET uses Microsoft .net 4.5 Framework.

Note for Hosted Environment: If your hosting provider does not allow you to configure a sub folder or virtual directory as an "application" you will have to put the application in the top or root folder of your web site or ask the hosting provider to configure the folder for you.



Convert the web folder to an application in IIS7

figure 1 (Internet Information Services (IIS) Manager 7)



Set Application Pool to .NET 4.6.1 in IIS7.

Also, make sure the Default.aspx page is set as the default document:

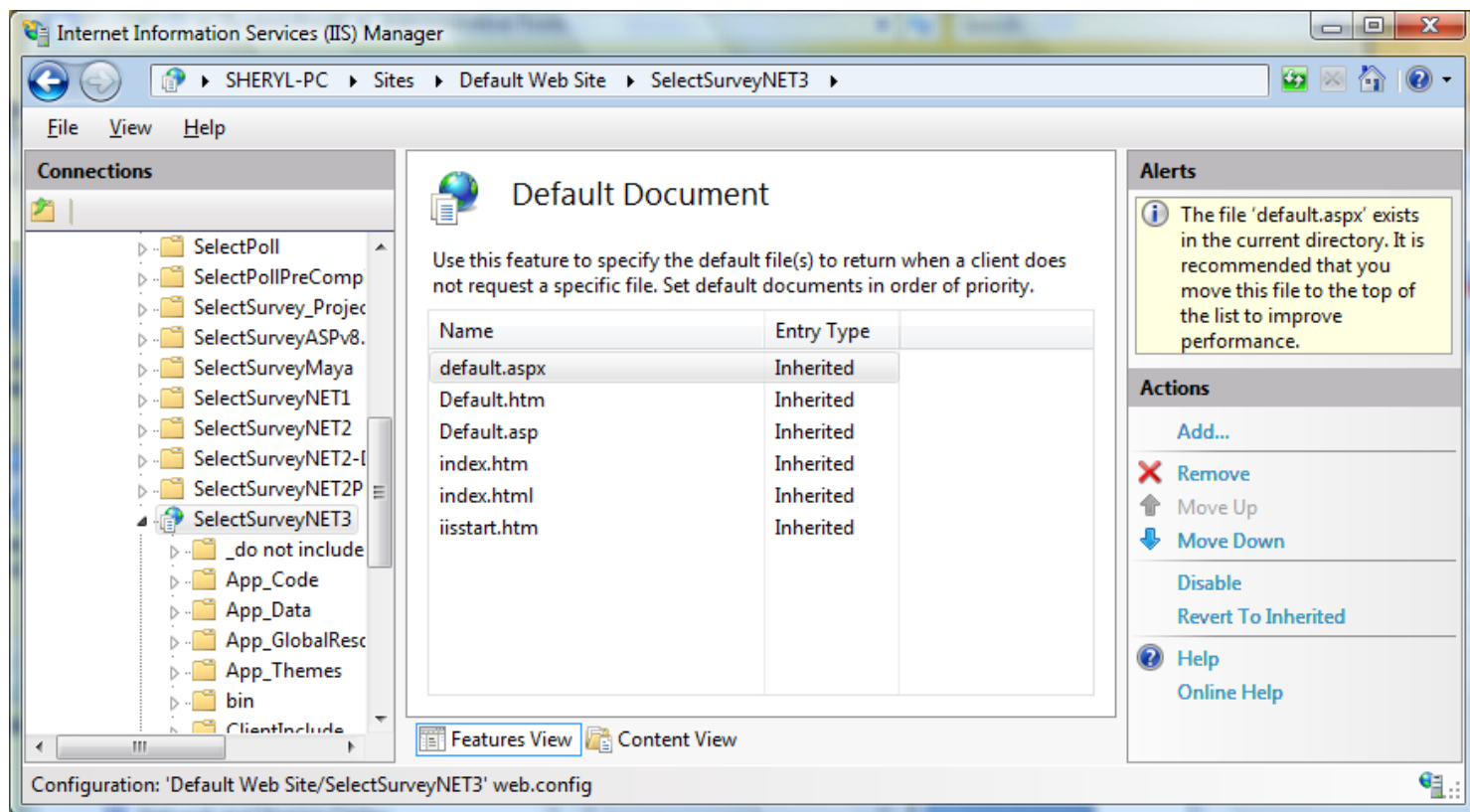


figure 2 (Internet Information Services (IIS) Manager 7)

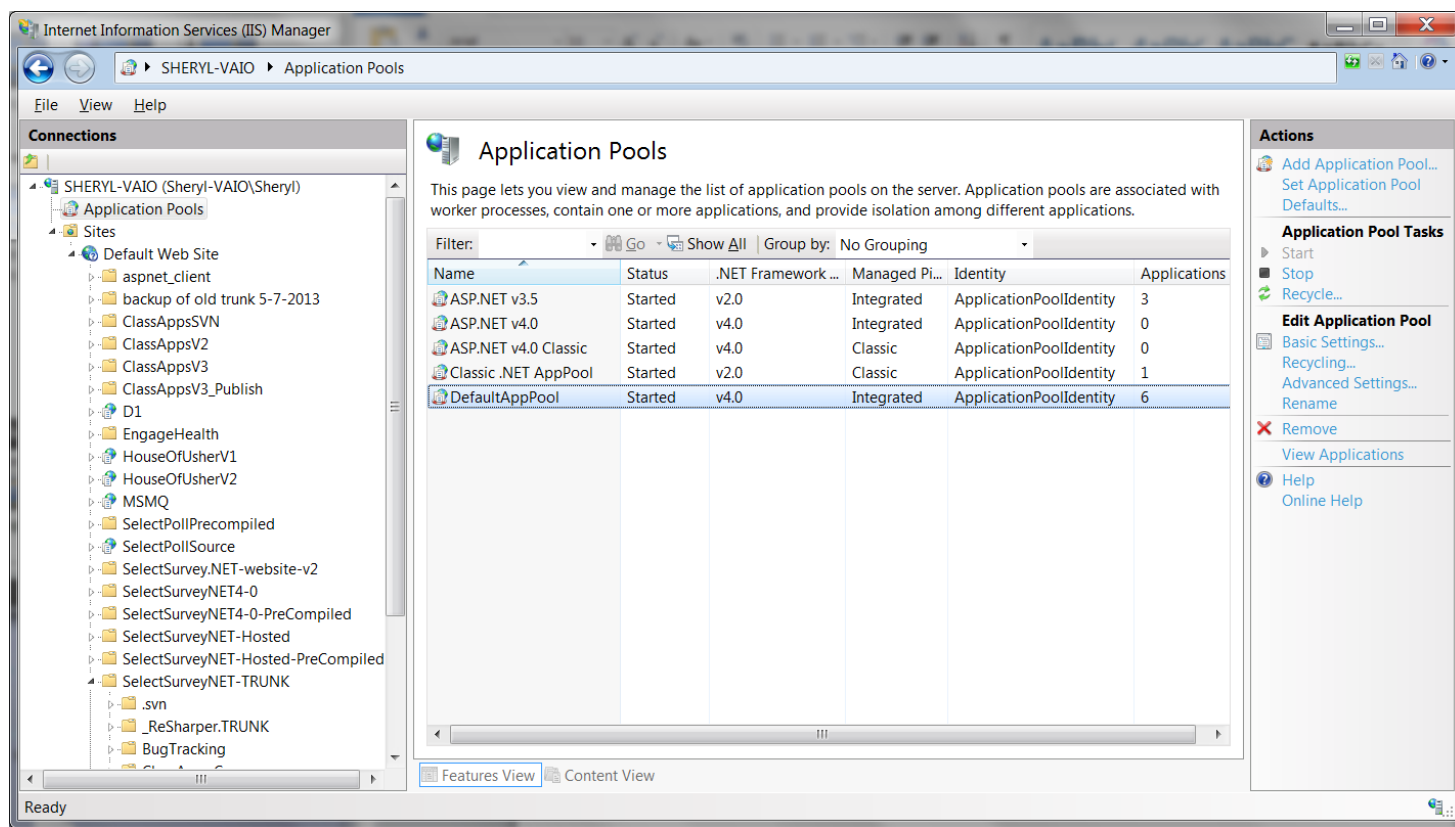
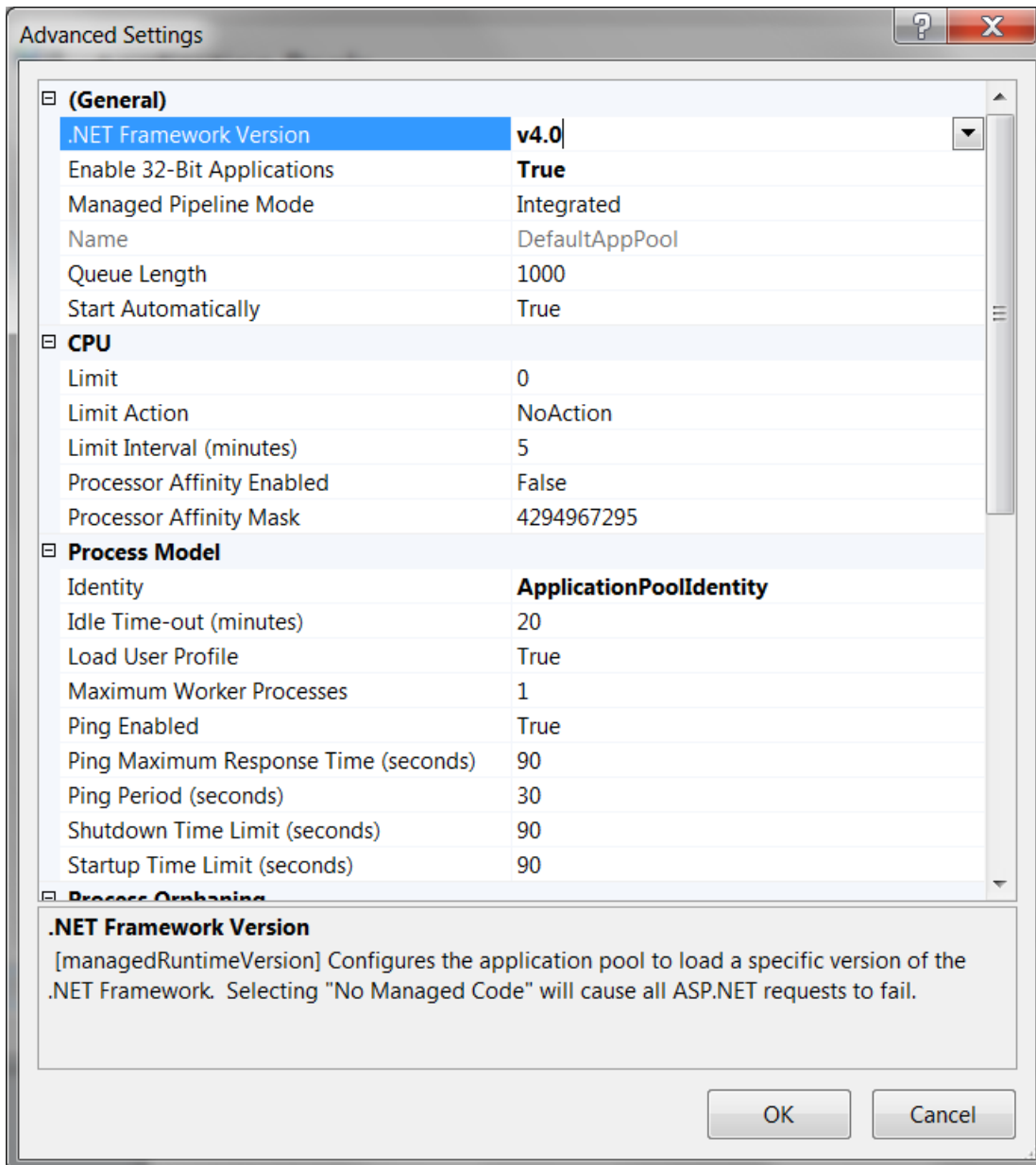


figure 3 (Internet Information Services (IIS) Manager 7)



Advanced Settings	
(General)	
.NET Framework Version	v4.0
Enable 32-Bit Applications	True
Managed Pipeline Mode	Integrated
Name	DefaultAppPool
Queue Length	1000
Start Automatically	True
CPU	
Limit	0
Limit Action	NoAction
Limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
Process Model	
Identity	ApplicationPoolIdentity
Idle Time-out (minutes)	20
Load User Profile	True
Maximum Worker Processes	1
Ping Enabled	True
Ping Maximum Response Time (seconds)	90
Ping Period (seconds)	30
Shutdown Time Limit (seconds)	90
Startup Time Limit (seconds)	90
.NET Framework Version [managedRuntimeVersion] Configures the application pool to load a specific version of the .NET Framework. Selecting "No Managed Code" will cause all ASP.NET requests to fail.	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

IIS7 Application pool settings for 64 bit servers: Set Enable 32-bit applications = True.

Configure the Production and Archive Databases.

SQL Server 2008R2 or later required

You will be creating 2 SQL server databases with the name of your choosing. One will be for production and one will be for archived surveys and responses.

NOTE: If you are upgrading from a prior version, please refer to the steps in the document found in the install folder of the zip file: "upgradeprocess2019-v5.pdf" and you do not need to follow this installation guide.

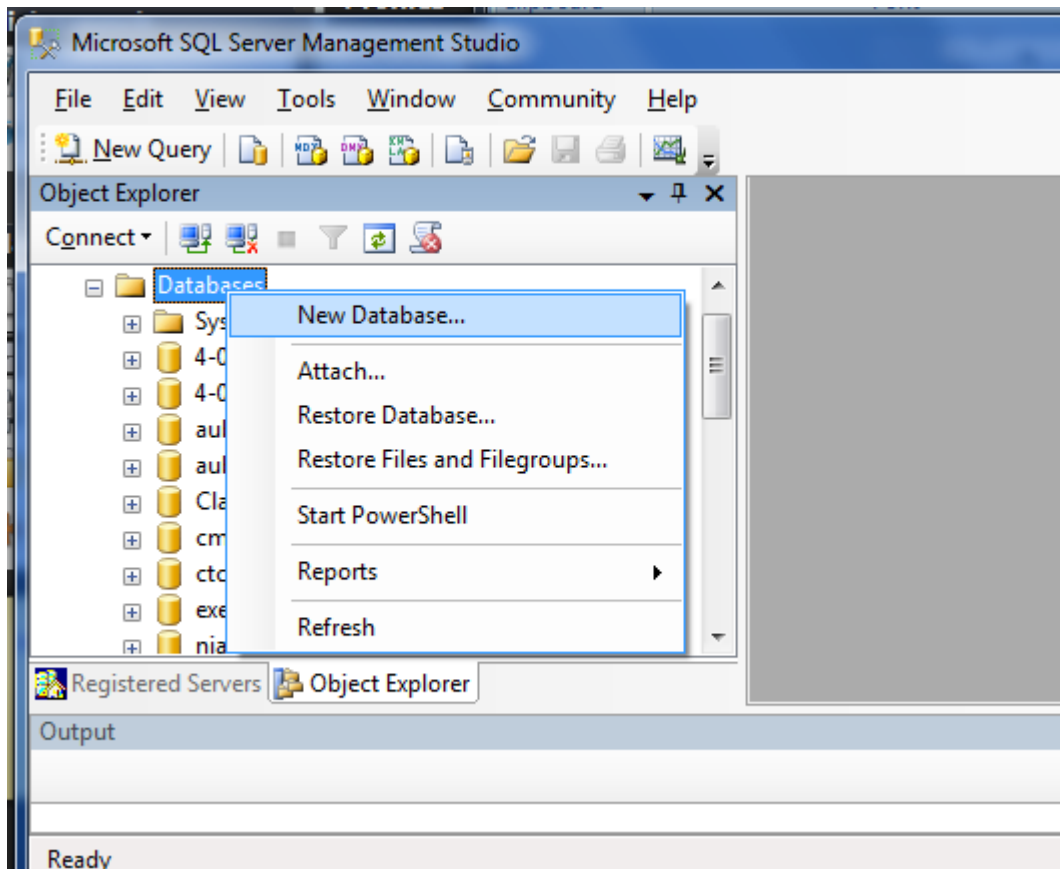
Create the production database:

You can name the database and archive database whatever name you choose in this format:

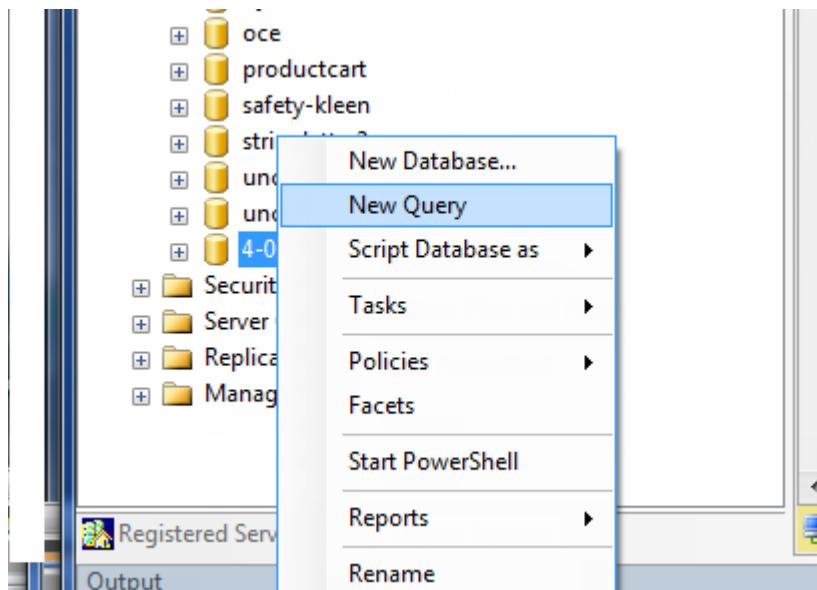
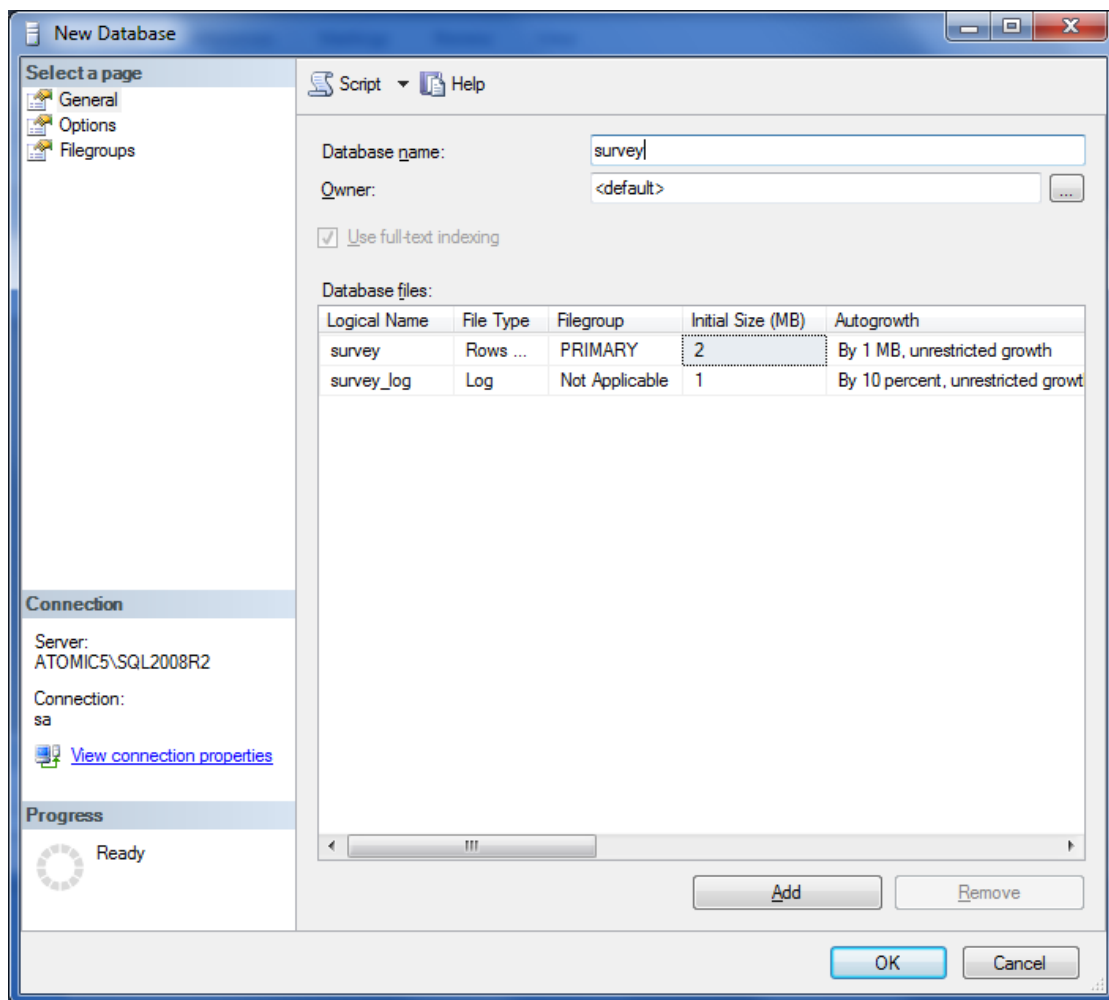
Acme_Production (production database)

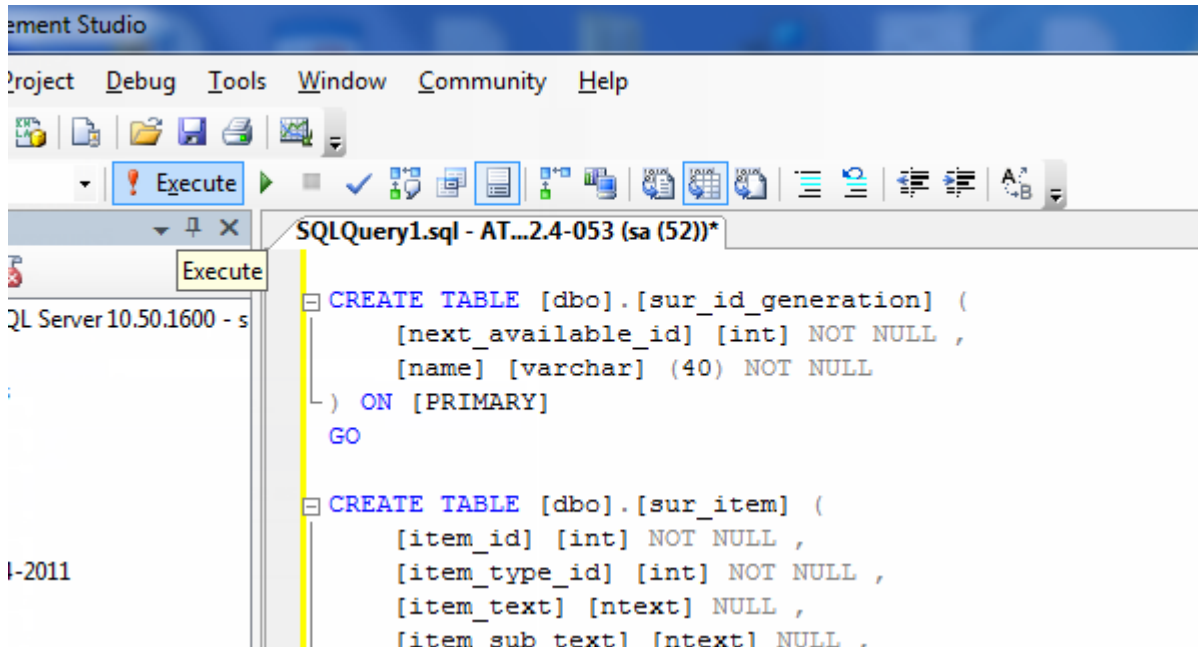
Acme_Archive (archive database)

Right click in SQL Server management studio New Database.



a.





- b. Load the tables into the database. The script for the tables is located in the file, "SelectSurveyNETTables.txt," which is located in the "SelectSurveyNET\Documentation\MSSQLScripts\MSSQL 2000 2005 and 2008\New Install " directory. The best way to load the tables is to open Microsoft Query Analyzer, open the file, "SelectSurveyNETTables.txt," from Query Analyzer, and execute.
- c. Load the required meta data into the database. The script for the meta-data is located in the file, "SelectSurveyNETData.sql," which is located in the "SelectSurveyNET\Documentation\MSSQLScripts\MSSQL 2000 2005 and 2008\New Install " directory. The best way to load the meta-data is to open the file, "SelectSurveyNETData.txt," from Microsoft Query Analyzer, and execute it.

- d. Update web.config:


```
<add key="SUR_DATABASE_TYPE" value="SQLServer" />
<add key="SURVEY_APP_DB_DRIVER" value="SqlClient" />
<add key="SURVEY_APP_ACTIVELY_CLOSE_CONNECTIONS" value="true" />
<add key="SURVEY_APP_CONNECTION"
value="Server=YourSQLServerNameOrIP;Database=SelectSurveyNET;Trusted_Connection=yes;"
/>
```

(use your connection string credentials, the above is an example only)

Create the archive database:

You can name the database and archive database whatever name you choose in this format:

Acme_Production (production database)

Acme_Archive (archive database)

NOTE: THE ARCHIVE DATABASE MUST BE ON THE SAME SQL SERVER AS THE PRODUCTION DATABASE FOR THE ARCHIVE AND RESTORE SCRIPTS TO RUN PROPERLY.

1. Create an “Archive Database” (optional but recommended in case someone deletes their survey and responses accidentally). This feature copies the survey and responses to an archive database and the user can restore it through the interface on the survey list page themselves without IT having to restore a database backup. When they archive a survey it deletes it from the production database after it is successfully copied to the archive database.
 - a. Create a separate empty database using the new db install TABLE script only. Call the database name the same as your production db name with “_Archive” after it. Such as:
 - i. Acme_Production (production database)
 - ii. Acme_Archive (archive database)
 - b. Add the archive connection string to your web.config:

```
<add key="SURVEY_ARCHIVE_CONNECTION"  
value="Server=yourserver;Database=Acme_Archive;UID=username;PWD=password;"/>
```

If you don't want to or can't create an archive database, make sure the archive connection string is EMPTY so that an error does not occur:

```
<add key="SURVEY_ARCHIVE_CONNECTION" value=""/>
```

NOTE: WHEN YOU UPGRADE PRODUCTION DATABASE YOU MUST ALSO RUN THE SAME UPGRADE SCRIPT ON YOUR ARCHIVE DATABASE, TO ENSURE THE ARCHIVE AND RESTORE SCRIPTS RUN SUCCESSFULLY AND THAT THE DATABASE STRUCTURE MATCHES.

Ensure your database connection string is correct before continuing. You should be able to bring up the login page of the application if your connection string is working. You can right click the app in IIS and click “browse” to see if the application comes up or not. If there is an error connecting to the database it will show an error if you are browsing on the server itself.

Edit WEB.CONFIG file for SMTP EMAIL AND SMS TEXTING.

3. **Edit the WEB.CONFIG file (required) with textpad or notepad to set email parameters.**
Also in the file, “Web.config,” there are several constants under the heading “EMAIL CONFIG VARIABLES”. SelectSurveyNET utilizes the System.Web.Mail namespace included in the .NET Framework for sending email. Read the comments in the web.config for how to set these values.

You will be setting the local or remote email server to be used for email list sending, SMS text messages, automatic response emails. The software supports local IIS6 SMTP, or remote SMTP services such as SendGrid or your company exchange server, or gmail.

NOTE: THERE ARE 2 places in the web.config for email settings!

Place 1: Email

```
<add key="smtphost" value="smtp.gmail.com"/>
<add key="smtpport" value="587"/>
<add key="smtpusername" value="yourusername"/>
<add key="smtppassword" value="yourpassword"/>
```

Place 1: SMS TEXTING TWILIO OPTIONS

```
<!-- SMS TEXTING SMS GATEWAY PROVIDER SETTINGS -->
<!-- twilio goes into the smshost value field-->
<!--EXAMPLE:<add key="smshost" value="twilio" />-->
<add key="smshost" value=" " />

<!-- Twilio accountSid goes in smsuser value field-->
<!--EXAMPLE:<add key="smsuser" value="putyourTwilioaccountSidHere" />-->
<add key="smsuser" value=" " />

<!-- Twilio authToken goes in smspassword value field-->
<!--EXAMPLE:<add key="smspassword" value="putyourTwilioauthTokenHere" />-->
<add key="smspassword" value=" " />

<!-- Twilio from phone number goes in smssender value field-->
<!--EXAMPLE:<add key="smssender" value="+18161231234" />-->
<add key="smssender" value=" " />
<!-- END OF SMS TEXTING SMS GATEWAY PROVIDER SETTINGS -->
```

Place 2:

```
<mailSettings>
  <smtp>
    <!-- host should be "smtp.yourisp.com", some isp have different
port, check with them, update your username and pass below -->
    <!-- defaultCredentials="true" remove if error or timeout -->
    <network host="127.0.0.1" port="25" userName="username"
password="password" defaultCredentials="true" />
  </smtp>
</mailSettings>
```

Edit WEB.CONFIG set LICENSE KEY and remaining keys.

4. **Edit the WEB.CONFIG to add in license key settings.** Set values for all other web.config settings, which would include license keys for any add-ons you purchased. To obtain the license key for different add-ons or products, login to your customer account page on classapps.com and click "product downloads". Below each product is your license key. Some products require you to click a button "generate" to generate a license key based on your production URL which you type in on the customer account page. If you are seeing a "15 day trial" message then follow the "Configure Application Wide Settings" section below.

Configure Application Wide Settings

1. Update your application wide settings after you login the first time: All of the below settings are in "admin tools" > "application wide settings"
 - a. Enter your **CUSTOMER ID** so you don't get a license error.
 - b. Select a new responsive template as the **DEFAULT SURVEY TEMPLATE** (or create one branded for your company by copying a new one from "templates > create > from copy" choose any template that starts with the word "THEME"
 - c. **Enforce SSL**
 - d. **Allow X-Frames from trusted URL** (otherwise the respondent file upload will not work – it will be denied by security setting) If you DON'T want to use that question type, leave it set to DENY X-FRAMES for security.
2. **Set your logo in "Admin Tools" > "White label branding"** so it will show on the login page.
 - a. Click "admin tools" > "white label branding" upload your logo that is 290 pixels wide by clicking upload logo button. Make sure the path shows in the textbox as "UploadedImages/yourlogo.jpg" (make sure your image name does not contain spaces and special characters that would cause it to break in a URL.)

Configure Permissions for File upload and JS on Server.

5. **Additional web server configuration.** If you are installing the application on Windows 2003, you must make the following change:
 - a) By default, Windows 2003 locks down most file extensions, except for certain types of files. This is different than previous versions of Microsoft operating systems. The survey application contains a number of JavaScript routines, all of which are in a file with a .js extension. To enable the .js file type, you simply edit the MIME types either at the Global IIS level or the individual site or virtual directory level. Add the .js as an application/x-javascript type, and everything should work fine. If your application is hosted with an ISP, simply ask them to enable files with a .js extension, and they will readily understand the request and how to respond to it.
6. **Configure server for file upload.** Configure for maximum file upload if you are using the "file upload" feature of the "presentation image" question type which allows survey creators to upload images to the "UploadedImages" folder on the web server to be referenced in their surveys. Follow the below steps for

setting permissions on the UploadedImages folder and configuring the web.config to set the file size limitations.

Set permissions on the folder: In order for the survey creator to upload an image from their local workstation to the web server, the UploadedImages folder must have proper write permissions. You can also change the location of this folder by setting the web.config parameter:

```
<!-- IMAGE UPLOAD FOLDER FOR SURVEY TEMPLATES AND EMAIL MESSAGES FOR IMAGE UPLOAD FROM
HTML RICH TEXT BOX
      this folder must have correct permissions to allow image upload.
      reference article:
http://aspalliance.com/336_Upload_Files_Using_ASPNET_Impersonation_and_UNC_Share.all -->
      <add key="IMAGE_UPLOAD_FOLDER" value="~/UploadedImages"/>
```

First, right-click on the folder where the ASP.NET files should be uploaded and select Properties from the provided menu. The Properties dialog for the selected folder opens. Click the Security tab to make sure the ASP.NET Machine Account is included in the list and has the proper permissions to write to disk. If it is enabled, you see something similar to what is presented in Figure 2.

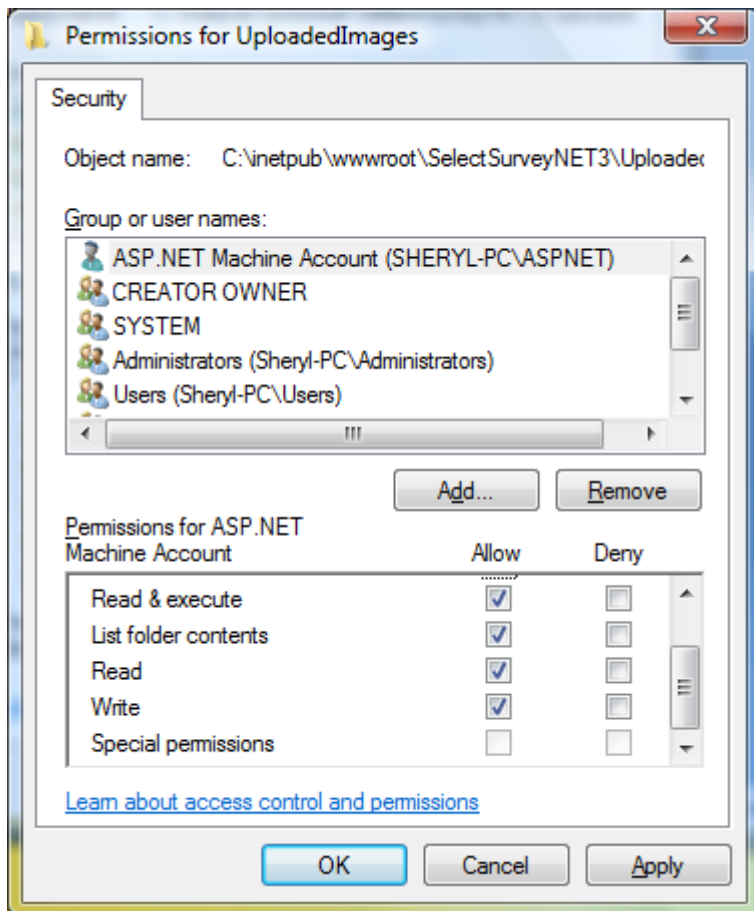


Figure 2 (IIS 7)

If you don't see the ASP.NET Machine Account in the list of users allowed to access the folder, add ASP.NET by clicking the Add button and entering ASPNET (without the period) in the text area provided (see Figure 3).

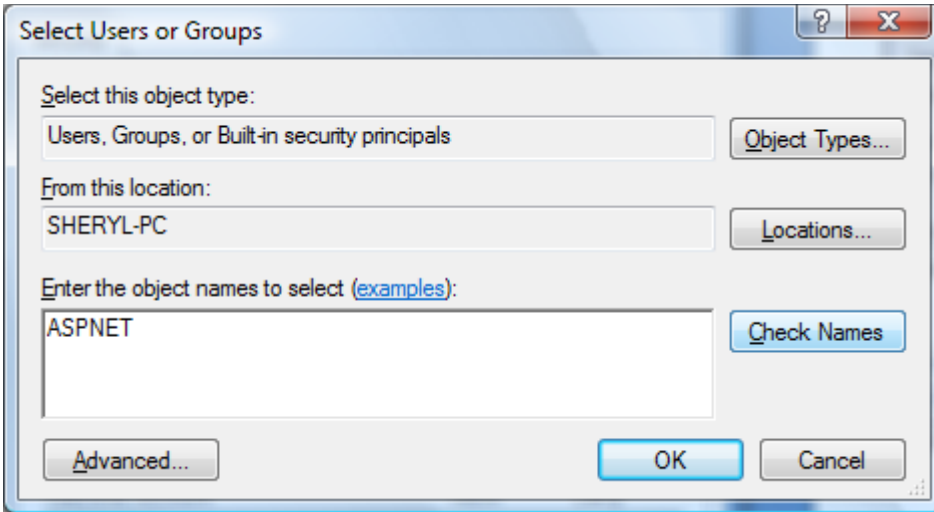


Figure 3 (IIS 7)

Click OK, and you can then click the appropriate check boxes to provide the permissions needed for your application.

Set maximum file size in admin tools “application wide settings”: Login as admin into the survey application with the browser. Click “admin tools”. Click “View Application wide settings”. Maximum file size setting is on this page along with all the other application wide settings.

Set file size limitation in the Web.Config file:

Note that any size of 4MB requires the below setting in web.config to also be changed since ASP.NET default file upload limit is 4MB. Set the `maxRequestLength` to the KB size limit you desire (20000 is approx 20MB). If you are setting to a large value, you must also raise the `executionTimeout` setting, which is in seconds, or it will timeout before the file is uploaded, causing an error on the server.

```
<httpRuntime executionTimeout="90" maxRequestLength="20000"
useFullyQualifiedRedirectUrl="false" requestLengthDiskThreshold="8192"/>
```

If you continue to get an error on uploading files over 4MB after changing the above setting, then you may need to also update the `machine.config` and `web.config.comments` file in the folder:

`C:\WINDOWS\Microsoft.NET\Framework\v3.5.50727\CONFIG`

Support

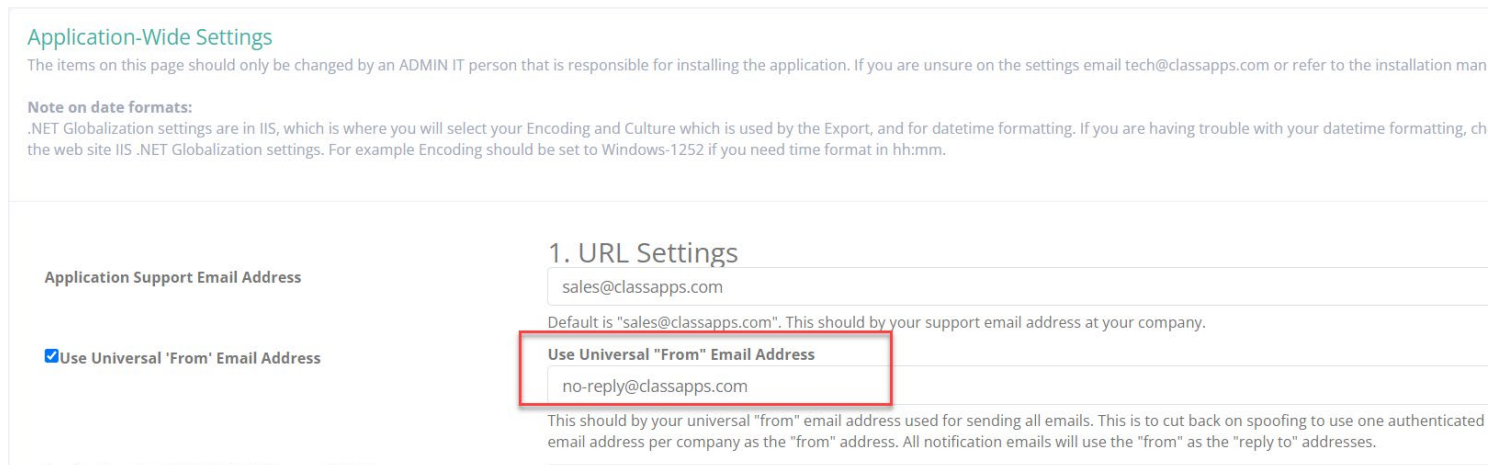
Go online to <http://www.classapps.com/support.asp> to the support page, where you can fill out a support ticket and find contact information.

SMTP Universal "From" email where all other "from" is "reply-to"

In admin tools > application wide settings > Universal from email you can set up an universal "from" email address. The universal "from" email is normally a "no-reply@yourdomain.com" email.

This helps with security so that you only have one from email for all emails sent from the survey application. If someone replies it will go to the "reply-to" email address which is whatever the survey owner put in as their address, or whatever was entered when sending to an email list on the form.

See the screenshot below.



Application-Wide Settings

The items on this page should only be changed by an ADMIN IT person that is responsible for installing the application. If you are unsure on the settings email tech@classapps.com or refer to the installation man

Note on date formats:
.NET Globalization settings are in IIS, which is where you will select your Encoding and Culture which is used by the Export, and for datetime formatting. If you are having trouble with your datetime formatting, ch the web site IIS .NET Globalization settings. For example Encoding should be set to Windows-1252 if you need time format in hh:mm.

Application Support Email Address
sales@classapps.com

☒ Use Universal 'From' Email Address

1. URL Settings
Default is "sales@classapps.com". This should by your support email address at your company.

Use Universal "From" Email Address
no-reply@classapps.com

This should by your universal "from" email address used for sending all emails. This is to cut back on spoofing to use one authenticated email address per company as the "from" address. All notification emails will use the "from" as the "reply to" addresses.

When this is activated, you will see the label "reply-to from email address" instead of "from email address" in the email list send forms. (See screenshot below).

Email Subject:*

Enter the subject of email

'From' Name:

YOUR NAME

'Reply-To' Email Address*

sbriggs@classapps.com|

'CC' Address(es):

Enter emails separated with Semicolon ';'

Warning! CC will get a copy of EVERY UNIQUE EMAIL. NO TOKEN

'BCC' Address(es):

Enter emails separated with Semicolon ';'

Warning! BCC will get a copy of EVERY UNIQUE EMAIL. NO TOKEN

Email Text:*

☒ Html ☐ Plain Text

Note: Make sure you check both email boxes, both HTML and F email client for recipient determines which message is displayed

File Edit View Insert Format Tools Table

↶ ↷ Paragraph ▼ **B** *I*  ▼    

Dear #FirstName#,

We are conducting a survey, and would appreciate your response.
The link to the survey is:

2 Factor Login Authentication

For non AD, non Azure AD, non owin login integration, you can turn on 2 Factor Authentication in admin tools > application wide settings > 2 step verification code.

See screenshot below with the available options.

Users must have email / phone numbers in the system in their accounts.

2 STEP VERIFICATION CODE - SMS/Email - RESPONDENTS ONLY -
Activate Response Approval Feature (for User Role Accounts only)

required to login again. Valid values are "session" and "cookie"

Regular Login (Default) - Choose this for AD/ADFS/Owin/OpenID/CAS where 3rd party auth handles 2 Factor Auth
2 FACTOR for Respondent Registration Logins only with Response Approval Feature
2 FACTOR Auth for every login attempt and all roles
Regular Login (Default) - Choose this for AD/ADFS/Owin/OpenID/CAS where 3rd party auth handles 2 Factor Auth
after using
activates a
that when
this is activated all new user registrations will require an SMS/email code to login. There is an additional review feature available without activating this feature. SMS settings are in the application web.config, if they are not filled in, an error may occur when trying to send an SMS text and an email will be sent instead.

Appendix A: Application Pooling

Platform: IIS6.0 with Windows Server 2003

Symptoms: Session timeout and session loss even when user is active.

Cause: Microsoft introduced several new features into Windows 2003/IIS6 web server that affect how sessions and application pools are handled. Most web hosting companies host multiple websites in the same application pool. When resources are maxed out for an application pool IIS 6 starts to recycle these sites causing application variables to be lost for those recycled sites.

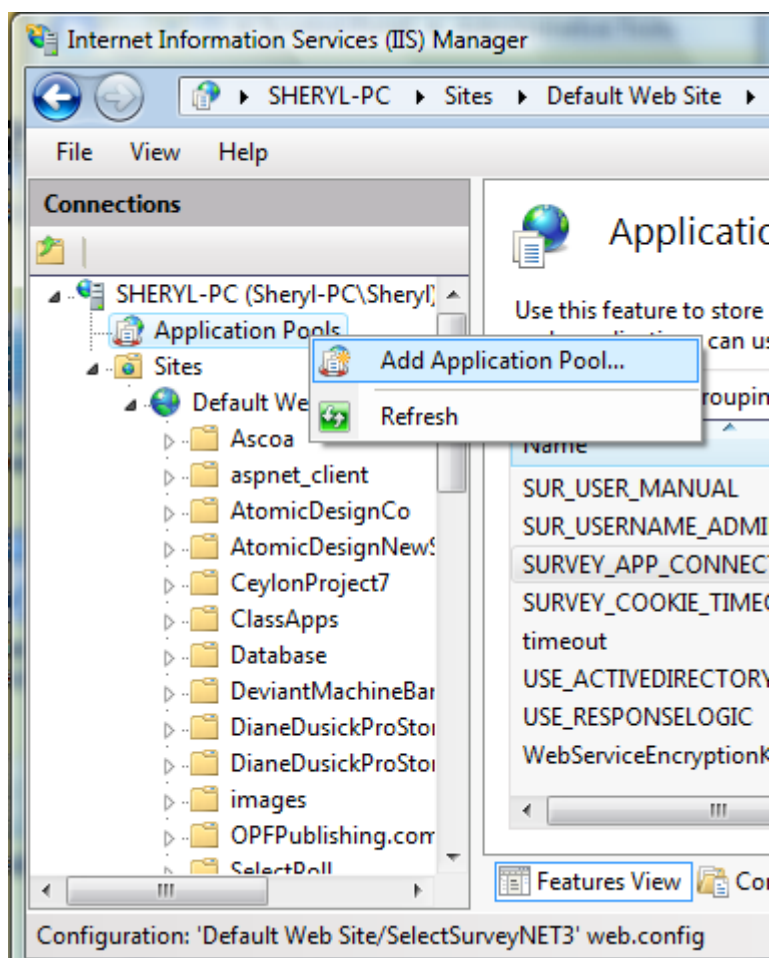
Solution:

If you are experiencing application/session loss symptoms then we would recommend asking your web hosting company to place you in your own application pool with all recycling options disabled and the recycle worker process set to recycle only once during the day at a set time.

Below are the instructions to do this:

Step 1:

Add new application pool for Select Survey Application.

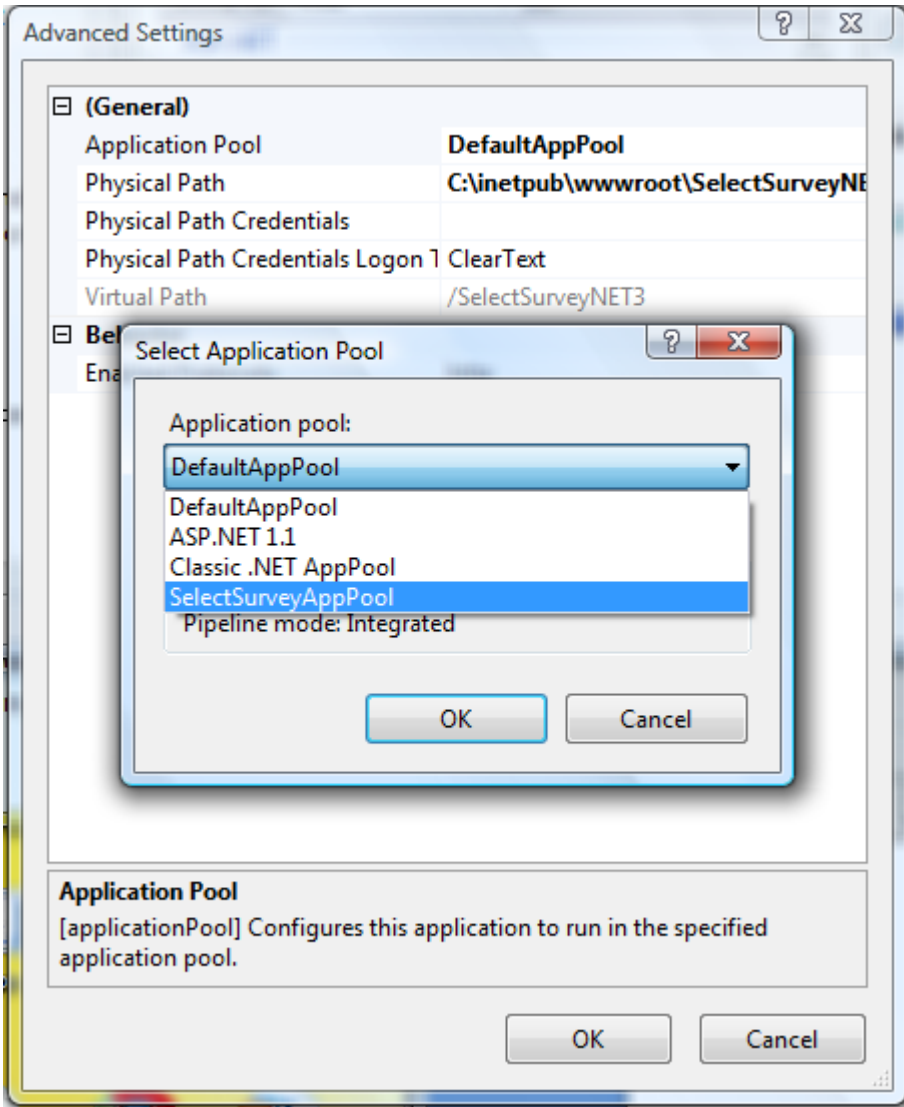


(IIS 7)

Step 2:

Choose your own application pool in the web site properties.

Done.



(IIS 7)

Appendix B: Notes for different culture/globalization settings

The provided application wide settings date format settings allow you to run the application even if your web server is a different language than your database server.

Click “admin tools” then “application wide settings”.

How to tell what language SQL is running under: Right click on the (local) SQL Server icon in enterprise manager and click “properties”. You will see a dialog box pop up similar to the below screenshot:



The default language here is how you determine how to set the “SERVER_DATE_FORMAT” value in the admin tools application wide settings. The above screenshot shows the server as value=“1” for the web.config.

If you need to work beyond the settings provided in the application, please note there are other settings in the machine.config when you install the .net framework and notes for these settings are below:

In order to display different languages and formatting for different parts of the world, there is a section in the machine.config on the web server as well as in the web.config file which contain settings for this.

1. Machine.config may be found on the web server in a directory similar to the following:
C:\WINDOWS\Microsoft.NET\Framework\v3.5\CONFIG\machine.config

search for the section "globalization Attributes" in the machine.config file that looks like the below and set the values for your country (they should be set as default when the framework is installed to your locale):
globalization Attributes:

requestEncoding="[Encoding value]" - Encoding to use for request

responseEncoding="[Encoding value]" - Encoding to use for response

fileEncoding="[Encoding value]" - Encoding to use for files

culture="[Culture]" - default Thread.CurrentCulture

uiCulture="[Culture]" - default Thread.CurrentUICulture

2. Web.config may be found in the web site root folder for SelectSurveyNET, edit the web.config to match your country language and culture:

```
<!--set culture to match datetime format you want for example "en-GB" is English Great Britain format -->  
<globalization requestEncoding="utf-8" responseEncoding="utf-8" culture="en-GB" />
```

Appendix C: Integrating with Active Directory and other Login Integration Add-Ons

This application has extra pages coded to work with active directory integration.

There are three modes for Active Directory:

- **NTLM Passthrough:** Application picks up logon_user identity from IE browser and the login screen is bypassed.
- **Active Directory Login:** Application shows the login page and user enters their network login as their survey login.
- **ADFS:** Active Directory Federated Claims based authentication.
- **COMBO:** SSO Single Sign On combined with NTLM Passthrough (Checks SSO, then NTLM)

There are also alternate login types available:

- **Google Federated Login:** Google openid owin based login authentication.
- **Office 365 Login:** Open ID OWIN based login authentication.

ADFS – Active Directory Federated Login Integration

Below are the steps for enabling ADFS WIF:

- 1) Make the below changes to the web.config. You can search for the text below – in some cases the text will be commented out (in green) and you will have to uncomment it as shown below. The yellow highlighted areas are where you would put your claims STS URL/information.

- a. Change "no" to "yes" on "USE_ADFS_LOGIN"
- b. Add STS url to "ADFS_FEDERATION_ISSUER"

```
<!--
*****
      ADFS ActiveDirectory Federated Login Claims Based Login Integration
*****
-->
<!-- values are "yes" or "no" -->
<add key="USE_ADFS_LOGIN" value="no"/>
<!-- value should be the URL of your STS -->
<add key="ADFS_FEDERATION_ISSUER" value="http://EmbeddedSts"/>
```

- 2) Test. That is the only thing you have to do. Note that if you cannot login, that you can turn on debug mode temporarily by changing the below web.config value, then open browser and try again.

```
<!--setting to turn on display of debug info on the login page to assist with setting up AD
integration (TURN THIS OFF WHEN YOU ARE DONE!-->
<!--valid values are "on" and "off" when "on" error stack trace and line # info will display on
bottom of AD login page when "off" no info will display. -->
<add key="AD_DEBUG_MODE" value="on"/>
```

How to setup ADFS with SSO

Prerequisites

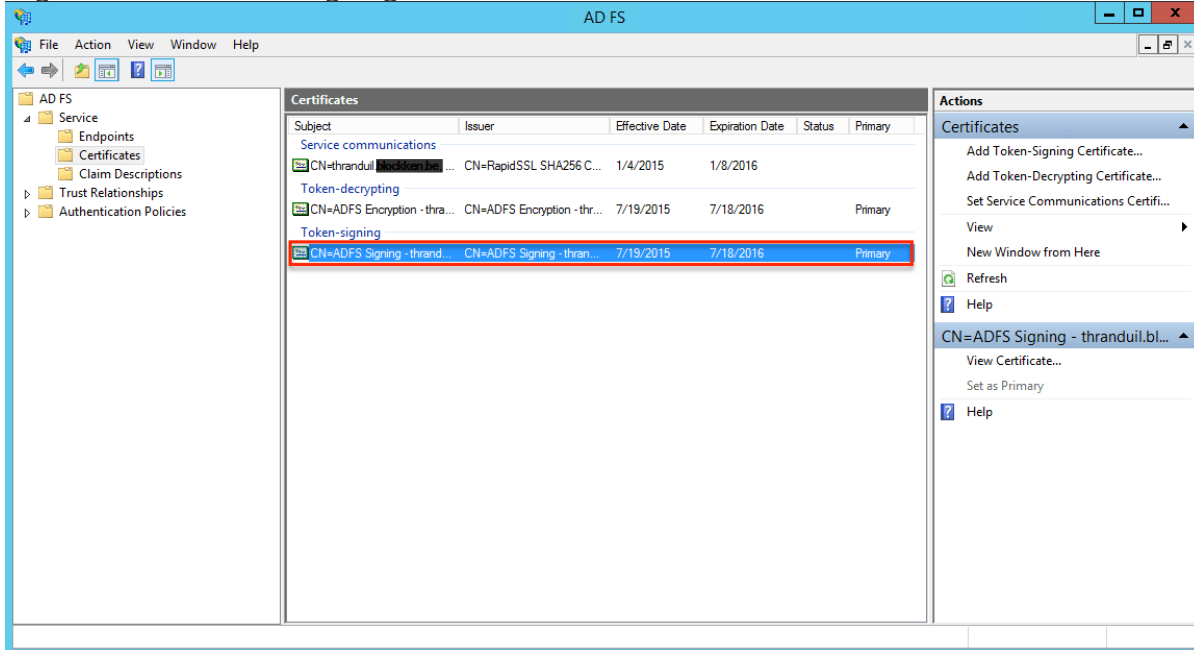
- The ADFS role should be installed and configured correctly. If you are unsure about this, please contact your network's system administrator to assist you.
- The following steps require administrator access to the ADFS server. If you do not have this access, you can provide this guide to your system administrator to perform the necessary steps.
- All users must have an email address added to their Active Directory account.

Steps to Complete

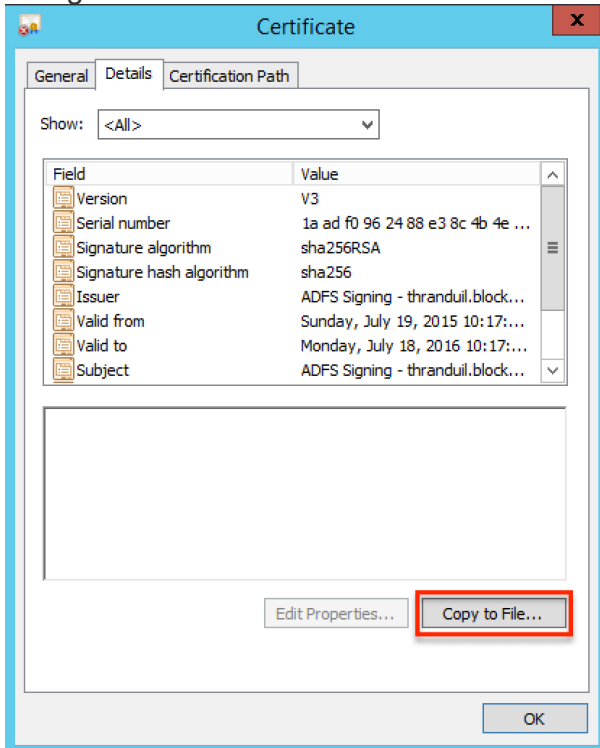
Exporting the Token-Signing Certificate

Use the following steps to export the token signing certificate.

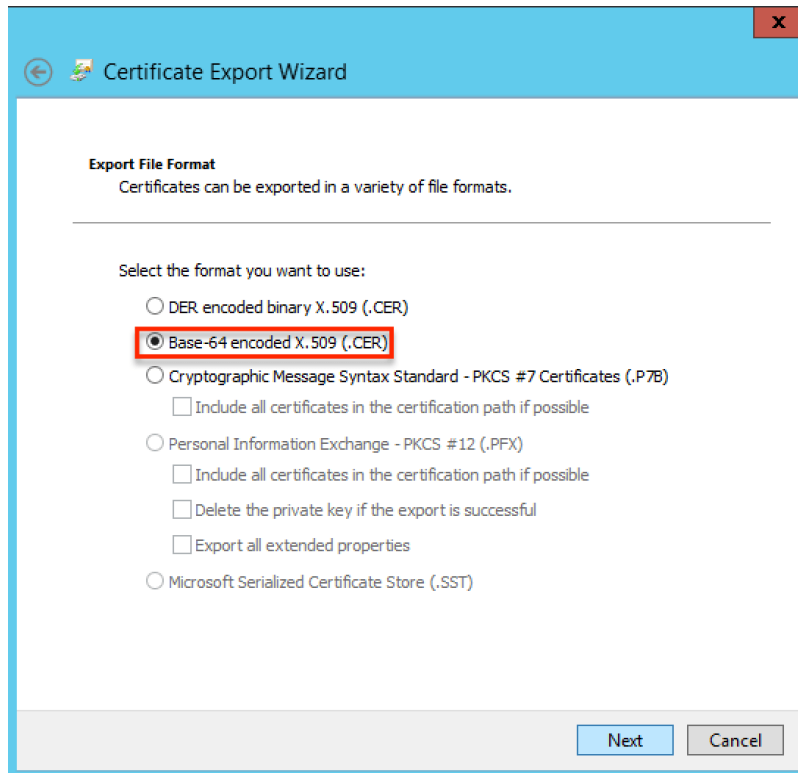
1. Open the ADFS Management console on the ADFS server.
2. In the tree view on the left, navigate to Service > Certificates.
3. Right-click the Token-signing certificate and chose "View Certificate".



4. Navigate to the Details tab and click the "Copy to File" button.



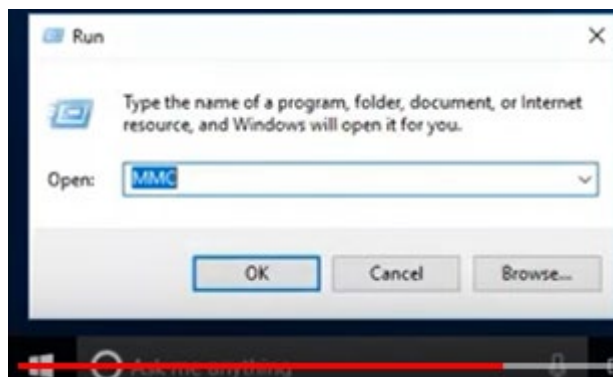
5. In the wizard, select "Base-64 encoded X.509 (.CER)" as the format and follow the wizard to store the certificate in an accessible location.



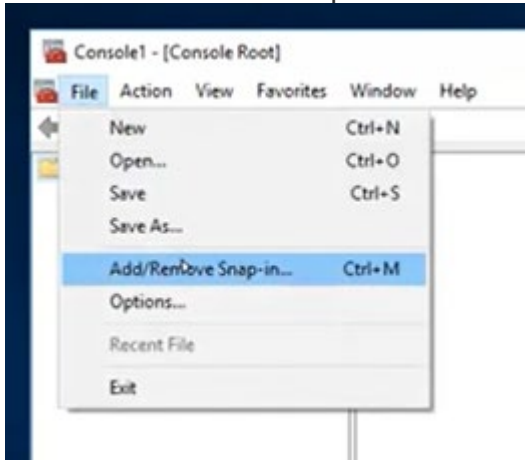
Install the token on the web server where the survey site will be running.

On the web server: (if you are using our cloud SaaS, we do this part – skip to the next step: “Configuring a New ADFS Trust Relationship”). If you are self hosting you would do this part on your web server.

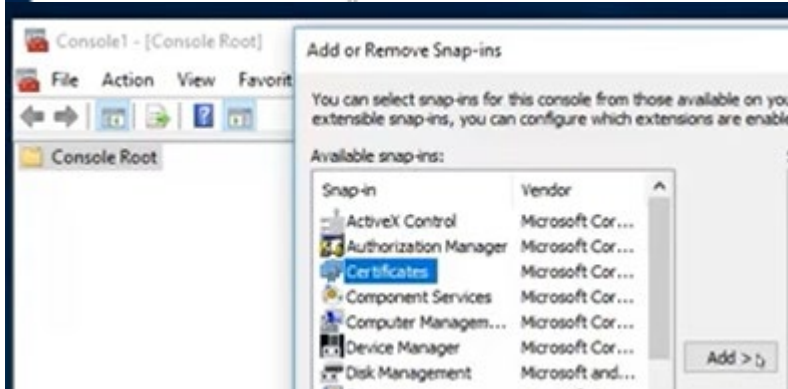
1. Click “Run” > “MMC” from the start menu.



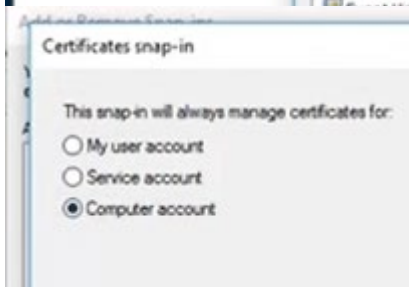
2. File > Add/Remove Snap-ins > Certificates



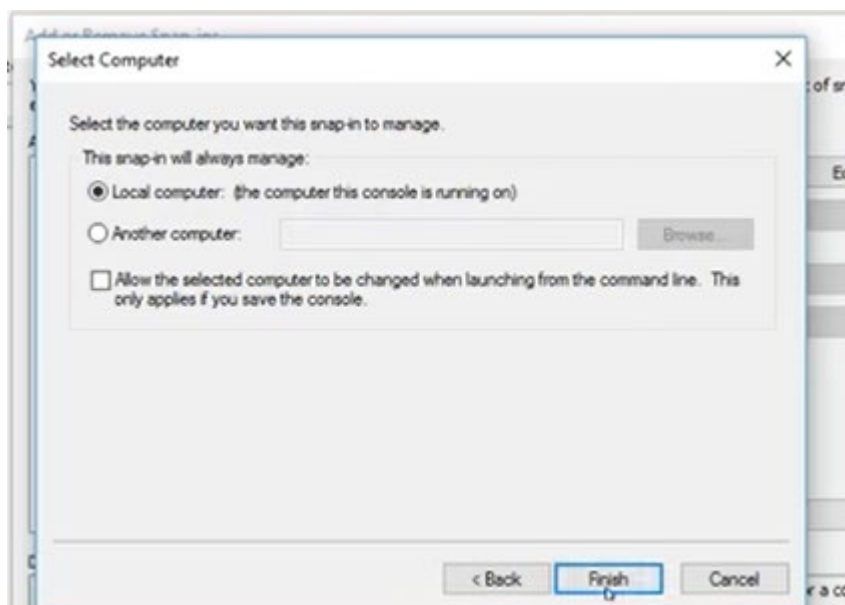
3.



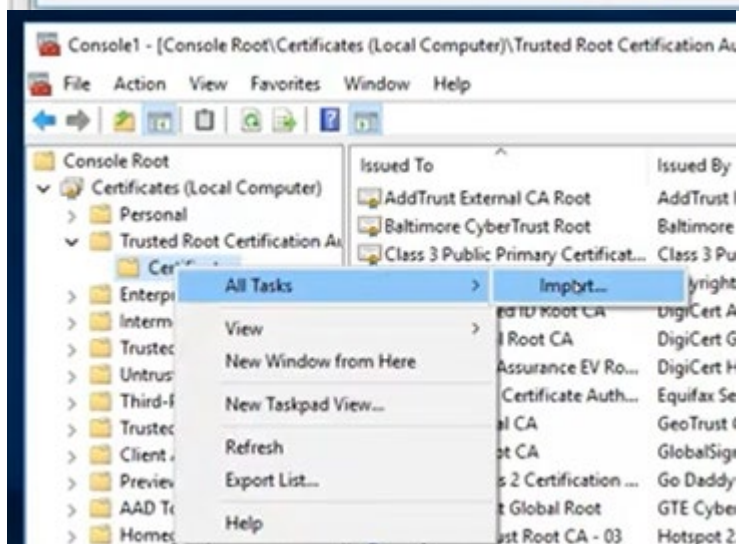
4.



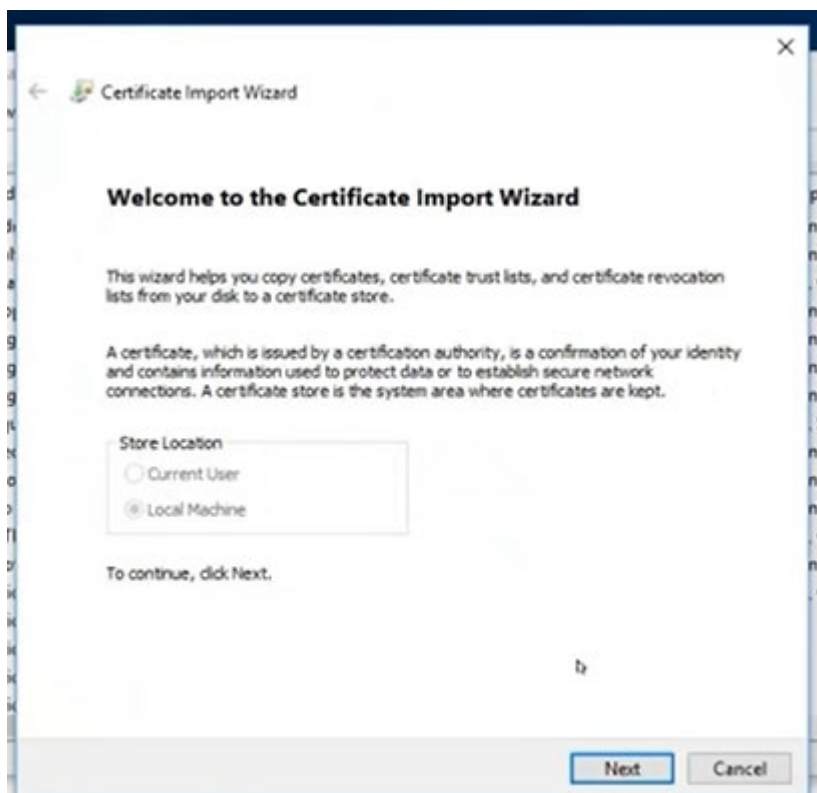
5.



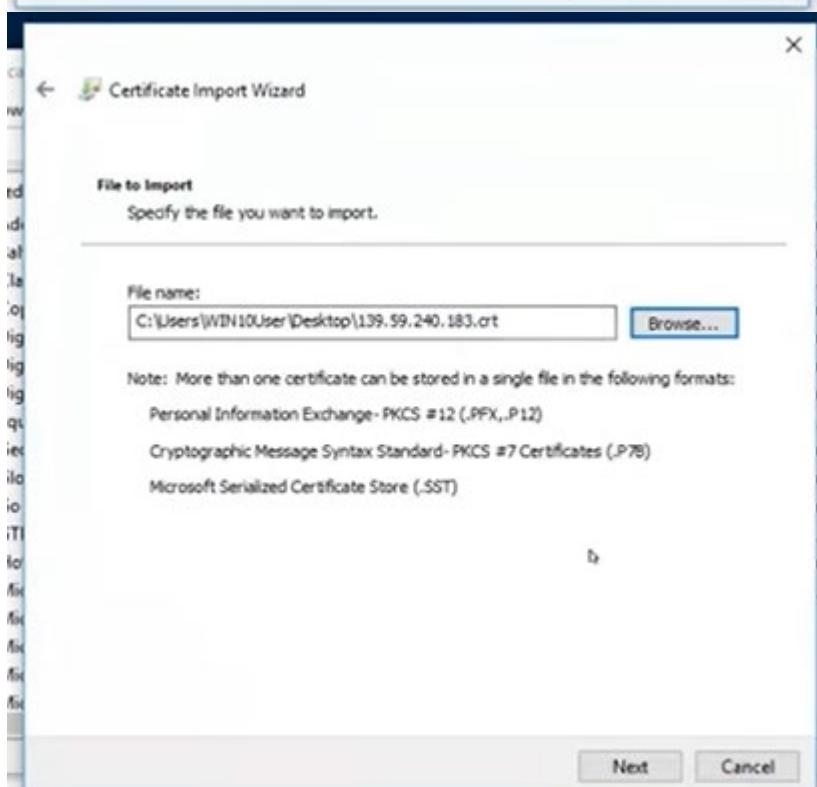
6.



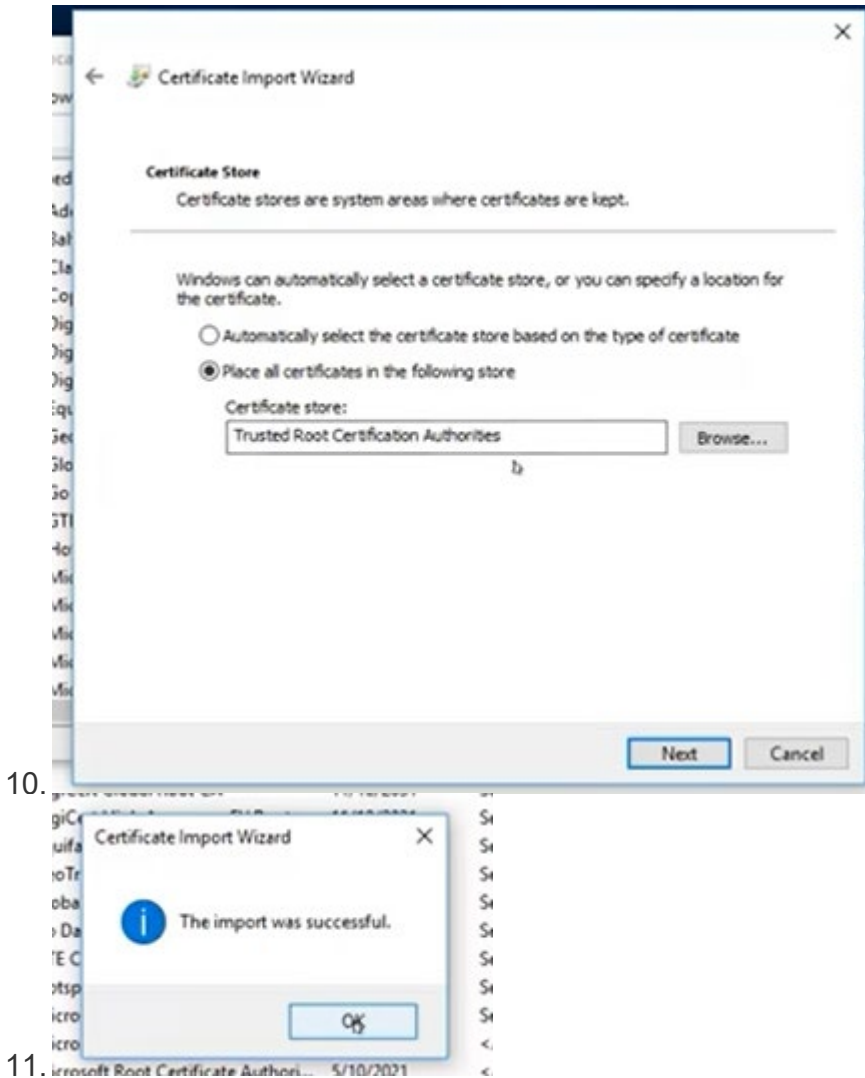
7.



8.



9.

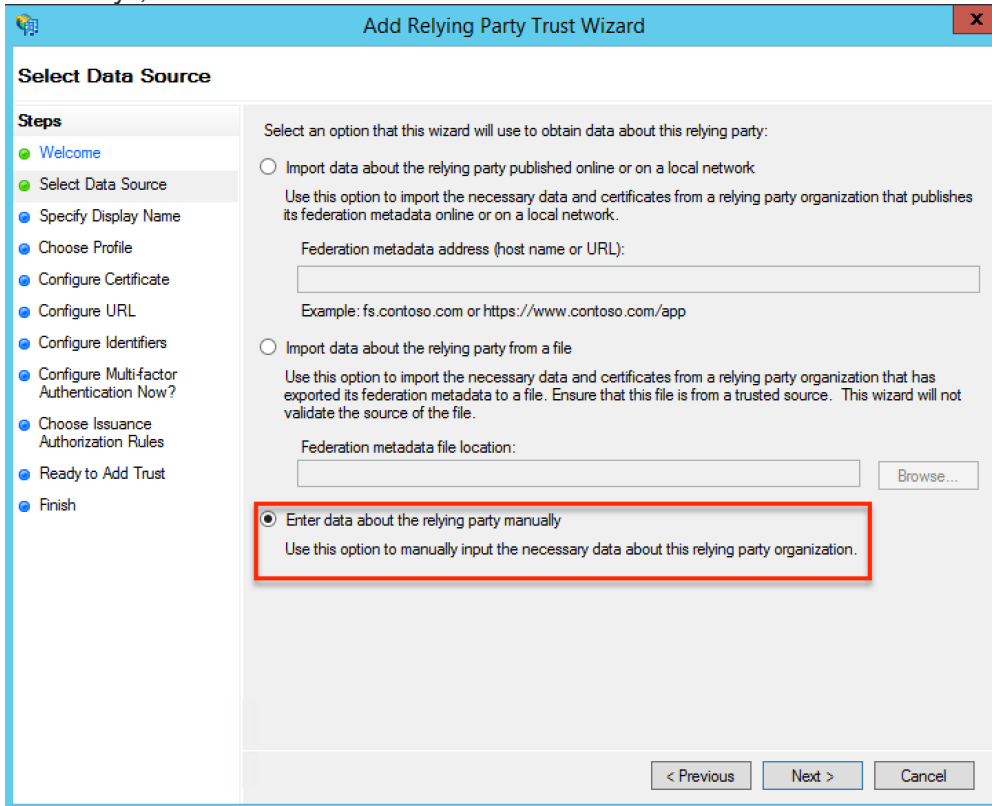


Configuring a New ADFS Trust Relationship

Use the following steps to configure a new trust relationship between SelectSurvey.NET and ADFS. This allows for communication between the two services.

1. In the ADFS Management console, navigate to Trust Relationships > Relying Party Trusts in the tree view.
2. Right-click on "Relying Party Trusts" and chose "Add Relying Party Trust".
3. A wizard will appear. Click "Start" to continue to the next screen.

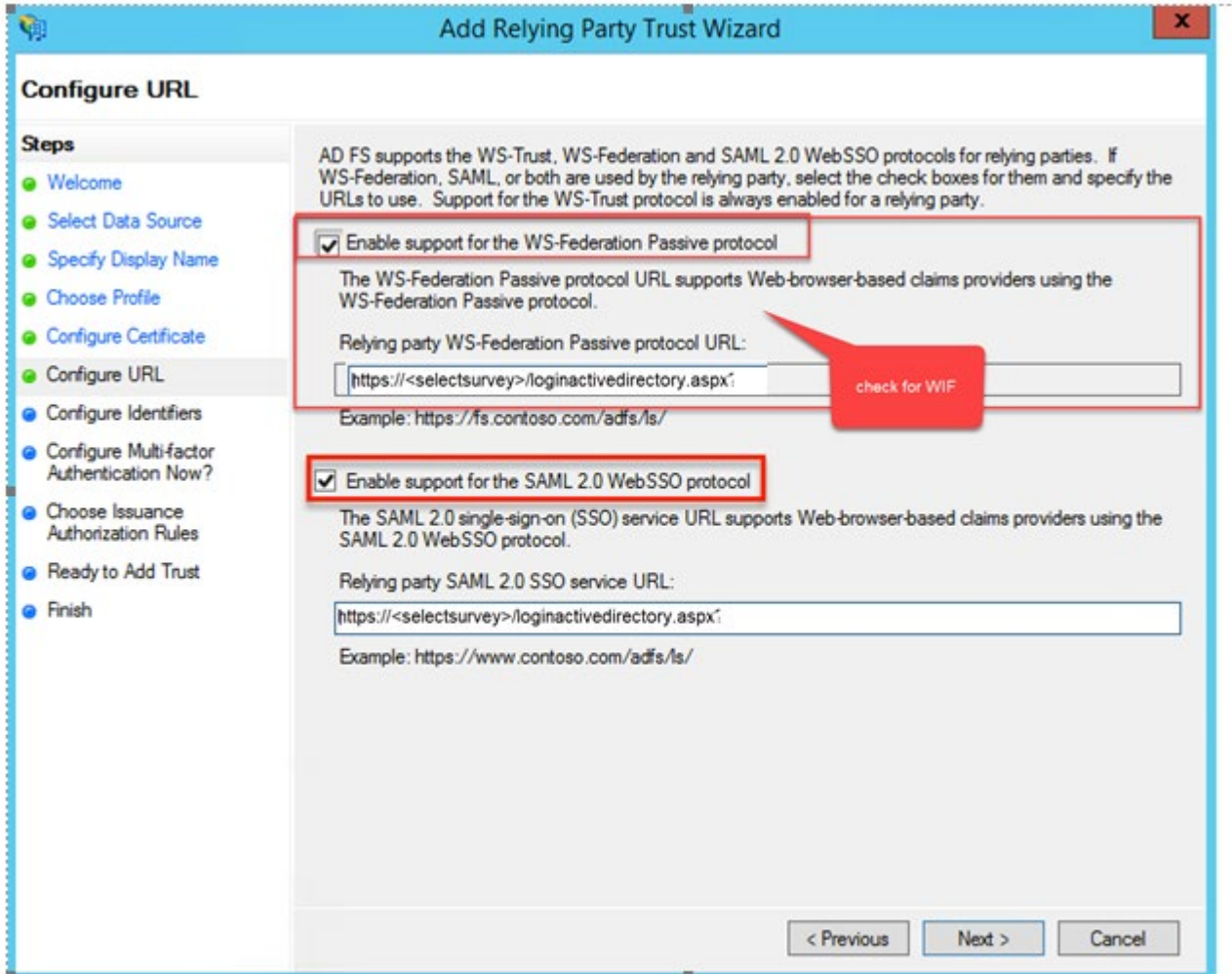
4. On the Select Data Source screen, choose the last option, "Enter data about the relying party manually", and click "Next".



The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar says 'Add Relying Party Trust Wizard'. The main window has a 'Select Data Source' header. On the left, there is a 'Steps' list with the following items: Welcome, Select Data Source (highlighted), Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains the following text: 'Select an option that this wizard will use to obtain data about this relying party:'. There are three radio button options: 1. 'Import data about the relying party published online or on a local network' with a description and a text field for 'Federation metadata address (host name or URL)'. 2. 'Import data about the relying party from a file' with a description and a text field for 'Federation metadata file location' with a 'Browse...' button. 3. 'Enter data about the relying party manually' (selected and highlighted with a red box) with a description. At the bottom, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

5. Enter a display name that will allow you to identify the newly configured trust relationship (e.g "SelectSurvey " or "SelectSurvey - Production" if you are planning on adding multiple SelectSurvey.NET instances). Click "Next".
6. In the profile selection, leave "AD FS profile" selected. Click "Next".
7. Optionally, configure a token encryption certificate. For the purpose of this guide, we will skip this step and click "Next".
8. To configure the SelectSurvey endpoint, select "Enable support for SAML 2.0 WebSSO protocol" and select "Enable support for the **WS-Federation** Passive protocol" enter the following URL in the field:

`https://<SelectSurvey.NET url>/LoginActiveDirectory.aspx`



Add Relying Party Trust Wizard

Configure URL

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL**
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

☒ **Enable support for the WS-Federation Passive protocol**

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: `https://fs.contoso.com/adfs/ls/`

☒ **Enable support for the SAML 2.0 WebSSO protocol**

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

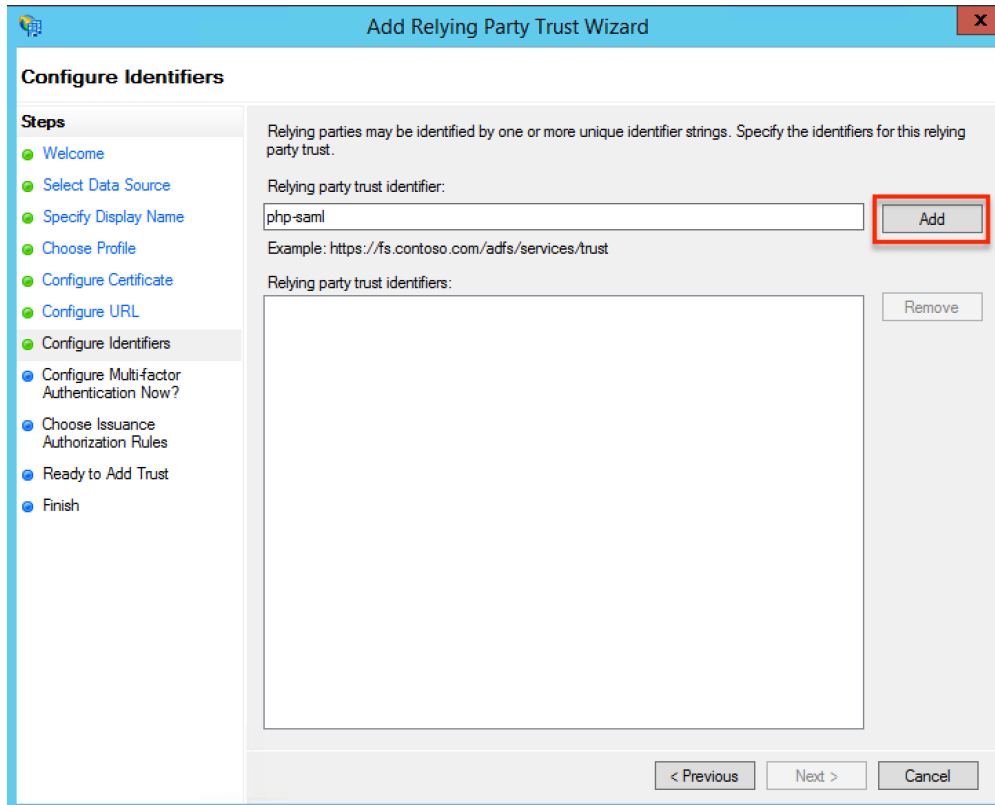
Relying party SAML 2.0 SSO service URL:

Example: `https://www.contoso.com/adfs/ls/`

< Previous Next > Cancel

Note: It is important that your instance is protected by SSL and your web server listens on HTTPS. This is required by ADFS, and the wizard will not allow you to continue if this requirement is not met.

- Click "Next" to display the Configure Identifiers page. You will need to configure a unique identifier if you are planning to add multiple SelectSurvey.NET instances with an individual trust relationship for each. Click "Add" to add the identifier to the list, then click "Next".



Add Relying Party Trust Wizard

Configure Identifiers

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers**
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

Relying party trust identifier:

php-saml

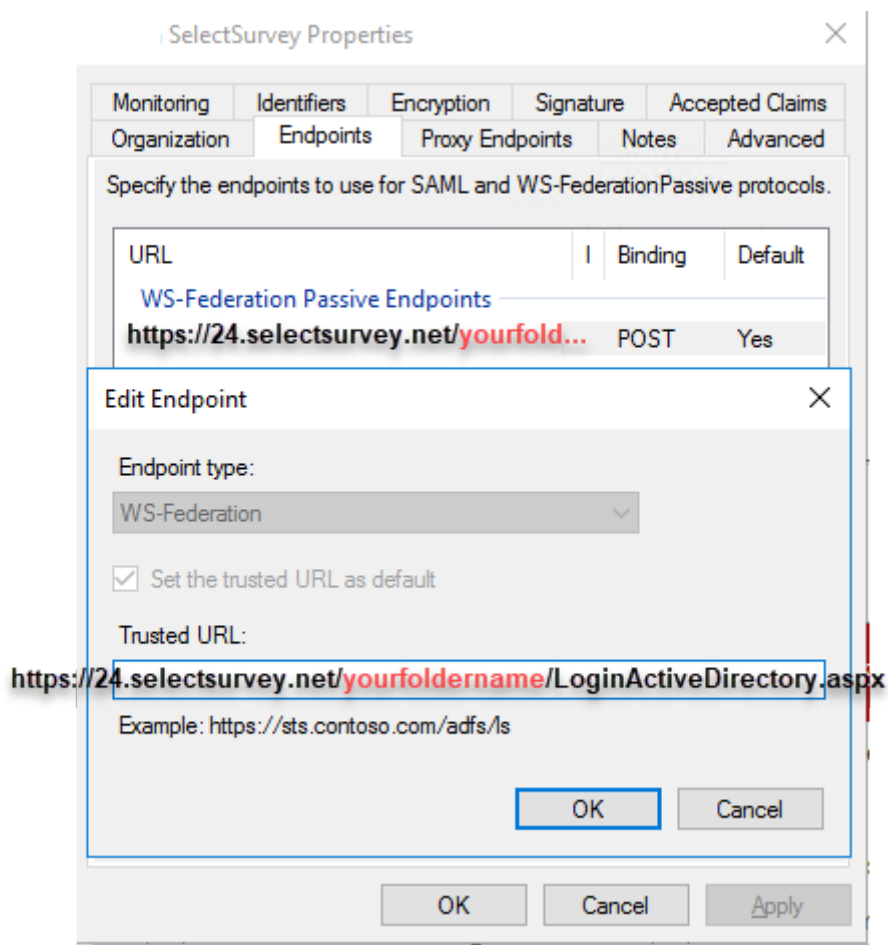
Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers:

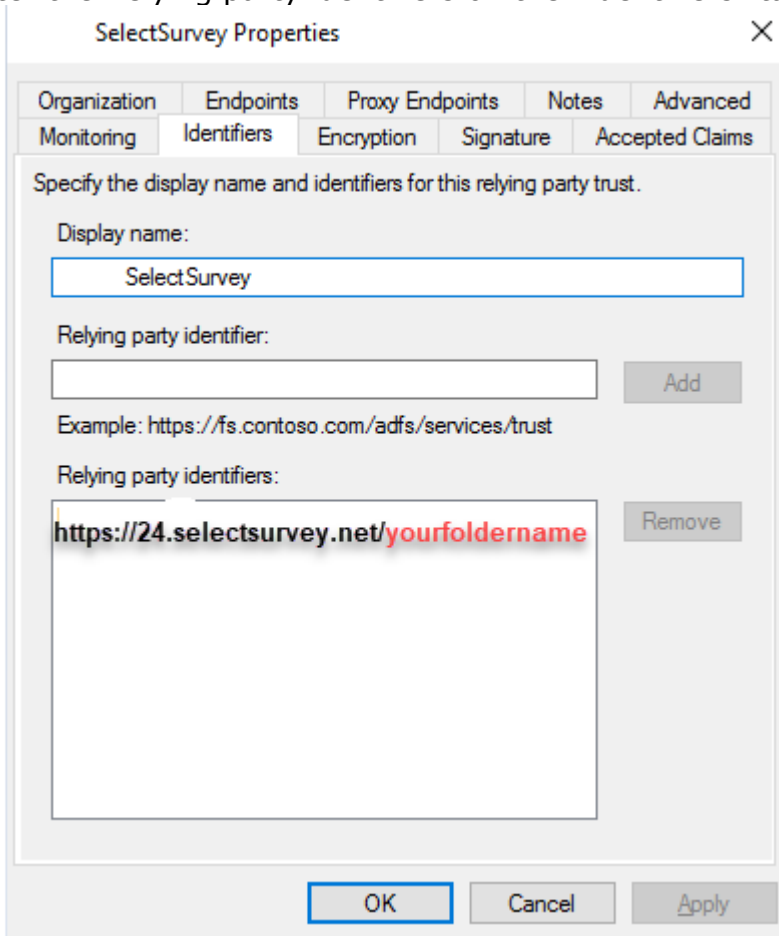
Remove

< Previous Next > Cancel

10. The wizard will ask to configure multi-factor authentication. If this is required by your organization, you can configure this now.
11. Enter the WS-Federation Passive endpoint trusted URL per below screenshot:



12. Enter the Relying party identifiers on the "Identifiers" tab per the below screenshot:



SelectSurvey Properties

Organization Endpoints Proxy Endpoints Notes Advanced
Monitoring Identifiers Encryption Signature Accepted Claims

Specify the display name and identifiers for this relying party trust.

Display name:
SelectSurvey

Relying party identifier:
Add

Example: https://fs.contoso.com/adfs/services/trust

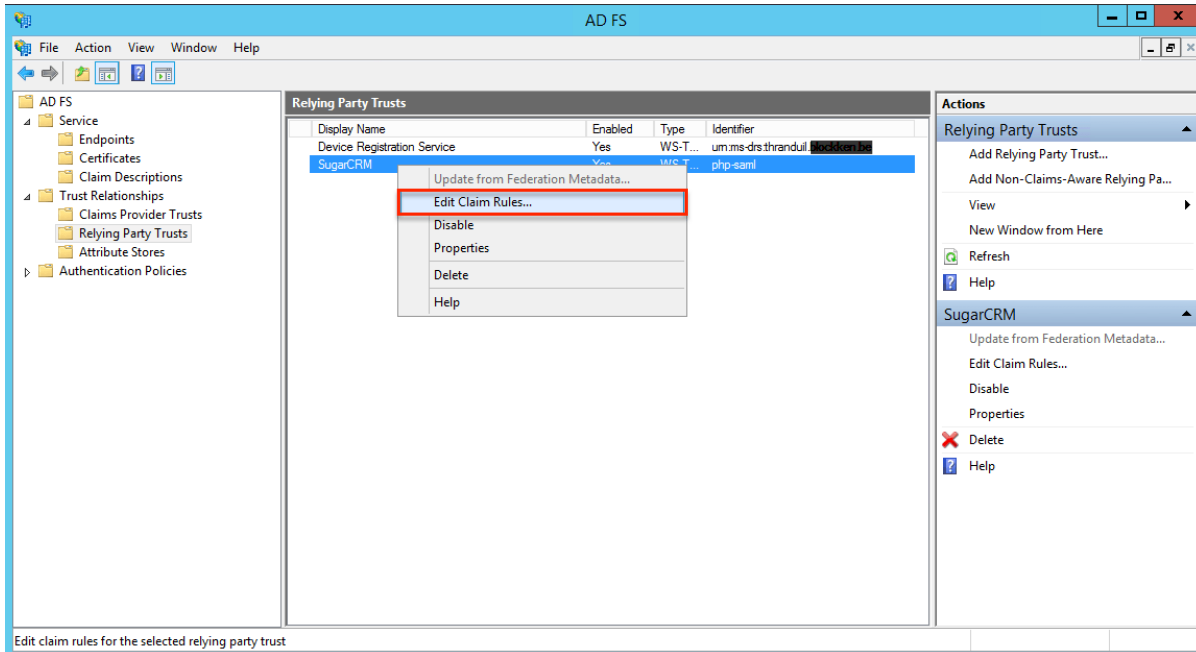
Relying party identifiers:
https://24.selectsurvey.net/yourfoldername Remove

OK Cancel Apply

13. Click "Next" again to display the Issuance Authorization Rules page. Here you can configure the default behavior of either allowing access to all users or no users. You can change this later, too. Leave the default selection to permit all users to log in.

14. Click "Next" to display an overview of the configured settings. Then click "Next" followed by "Close". This will create a new entry in the "Relying Party Trusts" list. Right-click the entry you just created and

select "Edit Claim Rules".



15. On the "Issuance Transform Rules" tab, add two rules which allow ADFS to work with SelectSurvey.NET. Name ID is what is used in SelectSurvey to match up with survey usernames. If your survey usernames are in email format, then setup per the screenshot below. If they are not email addresses then leave Name ID on the left and the right to synch regular usernames with SelectSurvey. If you are upgrading the survey app and switching from non AD logins to AD logins, then you must update your existing database to convert those existing usernames to match your AD usernames that are coming in, in order for the permissions to remain in tact from your previous survey usage. Jump to Step 19 for how to update your database.
16. Enter the Claims that you want to transfer from the AD to Survey App per the below screenshot:
 - (Note that if you are using email addresses for logins or UPN logins, set the "SAM-Account Name" to "UPN" on the left side and leave the right side as "Name ID")

Issuance Transform Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	Send AD attributes to SelectSurvey	Name ID,E-Mail Address,...

Edit Rule - Send AD attributes to SelectSurvey ✕

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

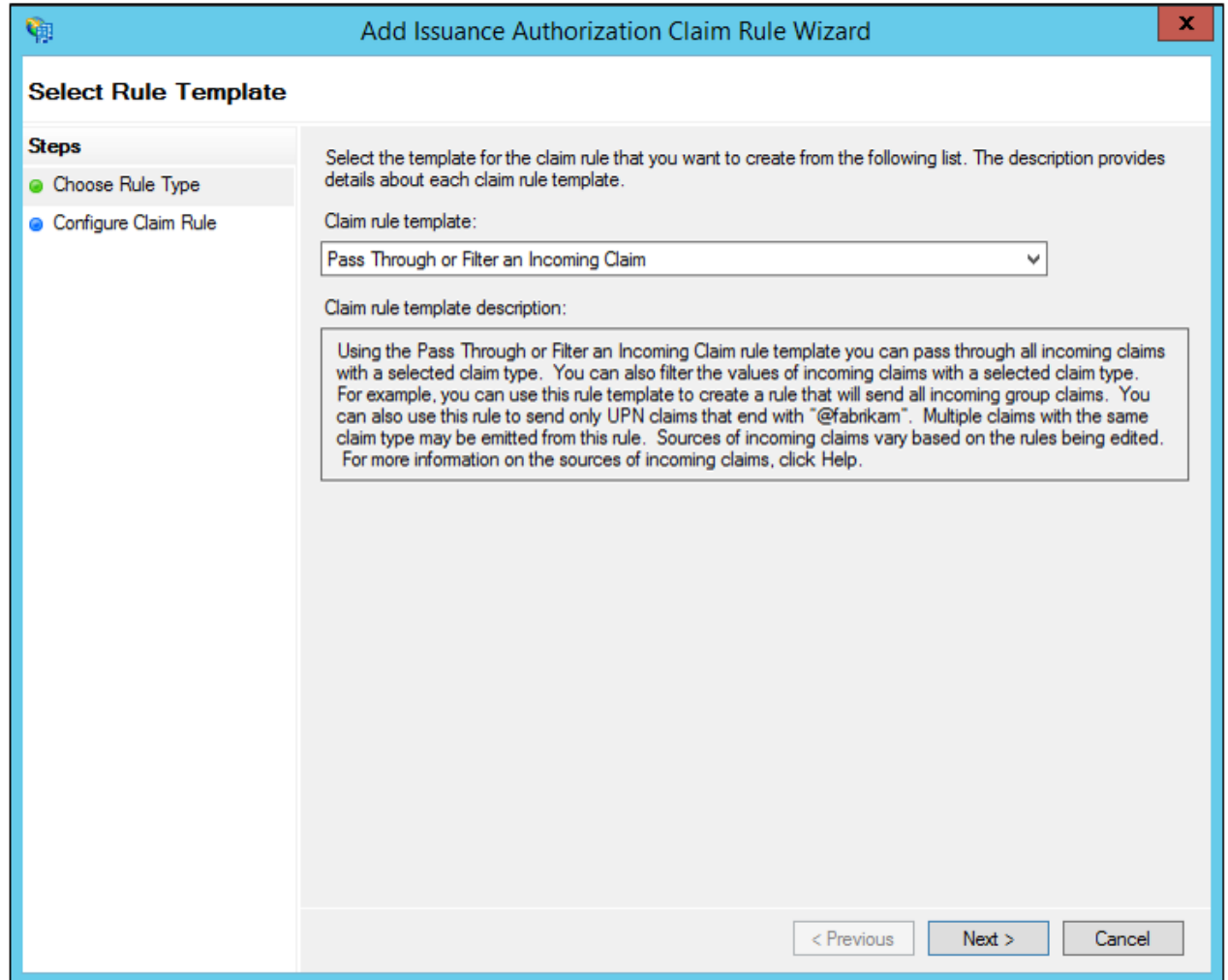
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	SAM-Account-Name ▾	Name ID ▾
	E-Mail-Addresses ▾	E-Mail Address ▾
	Given-Name ▾	Given Name ▾
	Surname ▾	Surname ▾
*	▾	▾

make sure
set to
passthrough
all claims

○

○

On the **Select Rule Template** page, under **Claim rule template**, select **Pass Through or Filter an Incoming Claim** from the list, and then click **Next**.



The screenshot shows a window titled "Add Issuance Authorization Claim Rule Wizard" with a close button (X) in the top right corner. The window has a light blue header and a white body. On the left side, there is a "Steps" section with two items: "Choose Rule Type" (marked with a green dot) and "Configure Claim Rule" (marked with a blue dot). The main area of the wizard is titled "Select Rule Template". It contains a paragraph of instructions: "Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template." Below this is a label "Claim rule template:" followed by a dropdown menu that currently displays "Pass Through or Filter an Incoming Claim". Underneath the dropdown is a label "Claim rule template description:" followed by a text box containing the following text: "Using the Pass Through or Filter an Incoming Claim rule template you can pass through all incoming claims with a selected claim type. You can also filter the values of incoming claims with a selected claim type. For example, you can use this rule template to create a rule that will send all incoming group claims. You can also use this rule to send only UPN claims that end with '@fabrikam'. Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited. For more information on the sources of incoming claims, click Help." At the bottom right of the wizard, there are three buttons: "< Previous", "Next >", and "Cancel".

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to pass through or filter an incoming claim. You can also configure this rule to filter claims that are generated by previous rules. Specify the claim type and whether only some claim values or all claim values should pass through.

Claim rule name:

Rule template: Pass Through or Filter an Incoming Claim

Incoming claim type:

Incoming name ID format:

☒ Pass through all claim values

☐ Pass through only a specific claim value

Incoming claim value:

☐ Pass through only claim values that match a specific email suffix value:

Email suffix value:

Example: fabrikam.com

☐ Pass through only claim values that start with a specific value:

Starts with:

Example: FABRIKAM\

< Previous Finish Cancel

Example only – please refer to this for your specific server version:

<https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/create-a-rule-to-pass-through-or-filter-an-incoming-claim>

- Create the second rule with "Transform an Incoming Claim" as the type and "Email Claim" as the name, "E-Mail Address" as the Incoming claim type, "Name ID" as the Outgoing claim type, "Email" as the Outgoing name ID format, and "Pass through all claim values" selected.

Edit Rule - email claim
✕

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type:

E-Mail Address ▼

Incoming name ID format:

Unspecified ▼

Outgoing claim type:

Name ID ▼

Outgoing name ID format:

Email ▼

☒ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

Browse...

☐ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

View Rule Language...

OK
Cancel

Update: no additional claims are necessary than from the original screenshot unless you want to add more (see AD to survey user field mapping page)

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	SAM-Account-Name ▼	Name ID ▼
	E-Mail-Addresses ▼	E-Mail Address ▼
	Given-Name ▼	Given Name ▼
	Surname ▼	Surname ▼
*	▼	▼

To map custom data fields to AD fields you can do that in SelectSurvey.NET on the AD mapping page here:

“Admin tools” > “ActiveDirectory User Property mapping”

These passthrough claims will get passed from ADFS to SelectSurvey and update the survey user account information each time they login.

- Dashboard
- Workspace
- Help
- Surveys
- Survey Folders
- Libraries
- Templates
- Email Lists
- Reports
- Users
- Admin Tools
- Account Usage
- Client Portal

ActiveDirectory User Property Mapping

This page is for administrators to map AD properties to survey user fields. When mapping is set, the AD properties will overwrite the survey user properties.

Enter the proper AD property for each survey user field. CASE SENSITIVE! Then click save at bottom of page.

Survey User Field

Username (sur_user.username)

Username (sur_user.username)

Username (sur_user.username)

Username (sur_user.username)

Register Date (sur_user.register_date)

User Password (sur_user.password)

Password Hint (sur_user.password_hint)

First Name (sur_user.first_name)

Last Name (sur_user.last_name)

Email Address (sur_user.email_address)

Current Position (sur_user.current_position)

Company (sur_user.company)

Location (sur_user.location)

Custom Data 1 (sur_user.custom_data_1)

Custom Data 2 (sur_user.custom_data_2)

Custom Data 3 (sur_user.custom_data_3)

Custom Data 4 (sur_user.custom_data_4)

ActiveDirectory User Property

SAMAccountName (Default AD setting)

userPrincipalName (Default AD setting if 1st returns null)

HttpContext.Current.User.Identity.Name (Default NTLM setting)

Request.ServerVariables["LOGON_USER"] (Default NTLM setting if 1st returns null)

n/a (User registration feature is not used with AD)

n/a (User password is not stored with AD integration)

n/a (Password hint is not used with AD integration)

givenName

search.PropertiesToLoad.Add("givenName")

sn

search.PropertiesToLoad.Add("sn")

mail

search.PropertiesToLoad.Add("mail")

Title

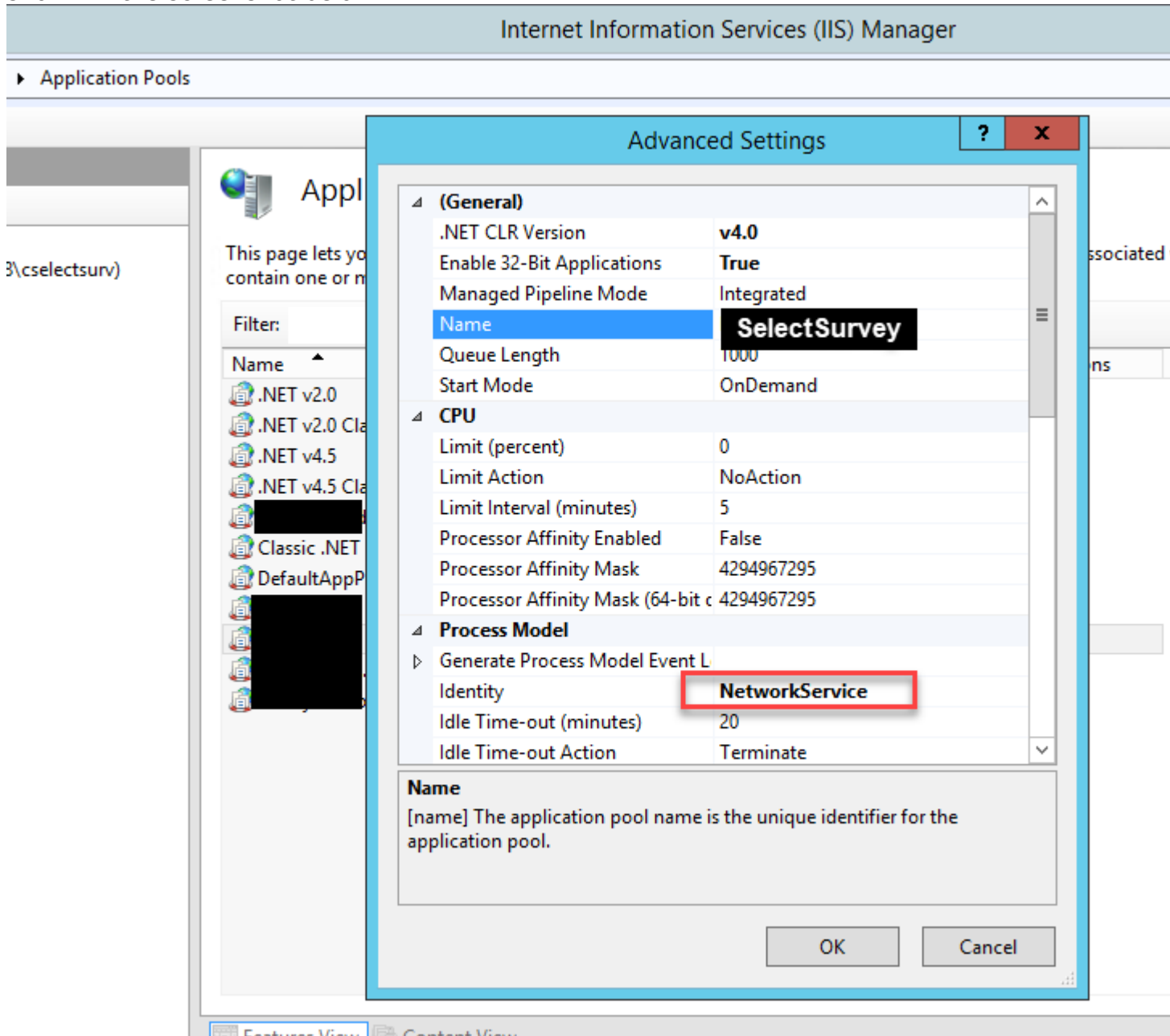
company

search.PropertiesToLoad.Add("company")

StreetAddress

search.PropertiesToLoad.Add("StreetAddress")

17. In IIS change the application pool used for the survey application to "NetworkService" as shown in the screenshot below:



That is it! You can now test and ADFS login should now be working.

Open your browser to <https://<your url>/Login.aspx> and click "LOGIN" button and it will now use ADFS and you will be logged in automatically.

Converting pre-existing Survey accounts to match ADFS user accounts

If you are converting from non AD to AD and already have users in the system that you need to synch to AD users, below is an example of the scripts that you need to run on the database to convert those user permissions on all objects to their new usernames.

You will have to modify these scripts for every single user you have in the system that you are converting.

```
--update survey owner permissions
```

```
update sur_survey set owners = replace(cast(owners as varchar(max)),'jdoe','jane.doe@yourcompany.com;')
```

```
--update template owner permissions
```

```
update sur_template set owners = replace(cast(owners as varchar(max)),' jdoe;', ' jane.doe@yourcompany.com;')
```

```
--update email list owner permissions
```

```
update sur_email_list set owners = replace(cast(owners as varchar(max)),' jdoe;', ' jane.doe@yourcompany.com;')
```

```
--update email template owner permissions
```

```
update sur_email_template set owners = replace(cast(owners as varchar(max)),' jdoe;', ' jane.doe@yourcompany.com;')
```

```
--update library owner permissions
```

```
update sur_library set owners = replace(cast(owners as varchar(max)),' jdoe;', ' jane.doe@yourcompany.com;')
```

```
--update survey folder owner permissions
```

```
update sur_survey_folder set survey_folder_owners = replace(cast(survey_folder_owners as varchar(max)),' jdoe;', 'jane.doe@yourcompany.com;')
```

```
--update existing response users
```

```
update sur_response set username = replace(username, ' jdoe ', 'jane.doe@yourcompany.com ')
```

```
--update existing users
```

```
update sur_user set username = replace(username, ' jdoe', 'jane.doe@yourcompany.com')
```

Google Federated Login Integration

Google Apps Federated Login Single Sign-On Service Overview

SelectSurvey.NET provides optional Google Apps Single Sign-On using Google Apps Federated Login Service.

For the Enterprise and the organization that use Google Apps, the Google Apps OpenID API enables a Universal Single Sign-on service that is integrated with **SelectSurvey.NET** survey software.

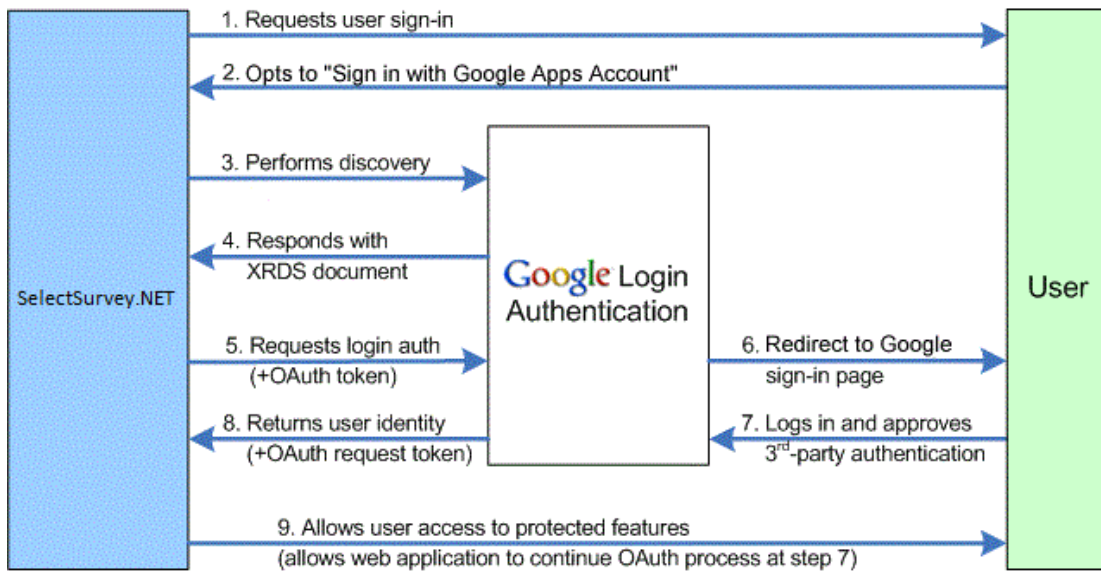
Note: The Federated Login Service is disabled by default for Google Apps for Business and Education. The domain admin can enable it from the Control Panel at <http://www.google.com/a/cpanel/<your-domain>/SetupIdp>.

Google Apps offers an OpenID API that allows end users to securely sign in to **SelectSurvey.NET** using their Google Apps user account. The [OpenID](http://openid.net) (<http://openid.net>) standard frees users from having to set up separate login accounts for different web sites--and conversely, frees web site developers from the task of managing login information and security measures. OpenID achieves this goal by providing a framework in which users can establish an account with an OpenID provider, such as a Google Apps hosted domain, and use that account to sign into any web site that accepts OpenIDs.

Google Apps API supports the OpenID 2.0 Directed Identity protocol, allowing any hosted domain to provide authentication support as an OpenID provider. On request from **SelectSurvey.NET**, Google authenticates users who are signing in with an existing Google Apps account, and returns to **SelectSurvey.NET** an identifier that the site can use to recognize the user. This identifier is consistent, enabling **SelectSurvey.NET** to recognize the user across multiple sessions.

Interaction Sequence

OpenID login authentication for web applications involves a sequence of interactions between **SelectSurvey.NET**, the Google Apps hosted domain, Google domain, Google's login authentication service, and the end user. The diagram and sequence below describe the process as recommended by Google. For simplicity, the diagram covers the flow in which discovery is done on the Google domain.



This image illustrates the following steps.

1. SelectSurvey.NET asks the end user to log in by offering a set of log-in options, including Google Apps accounts.
2. The user selects to sign in using a Google Apps account.
3. SelectSurvey.NET performs discovery as [defined in the documentation](#) to find location of the XRDS document.
4. Google returns an XRDS document, which contains the Google Apps (hosted) domain endpoint address.
5. SelectSurvey.NET sends a login authentication request (optionally with OAuth parameters) to the provided endpoint address.
6. This action redirects the user to a Google Apps account Federated Login page.
7. The user signs into their Google Apps account. Google Apps then displays a confirmation page and asks the user to confirm or reject a set of authentication requests by the web application.

Note: In some circumstances the login step or the approval step (or both) may be skipped dependent upon SelectSurvey.NET survey options for survey response types that are set to be anonymous.

8. If the user approves the authentication, Google returns the user to SelectSurvey.NET, and supplies a persistent, opaque identifier that the application can use to recognize the user.
9. SelectSurvey.NET uses the Google-supplied identifier to recognize the user and allow access to SelectSurvey.NET features and data.

Setup Step 1: Obtaining a Google Token

1. Register with Google to Obtain your Token.

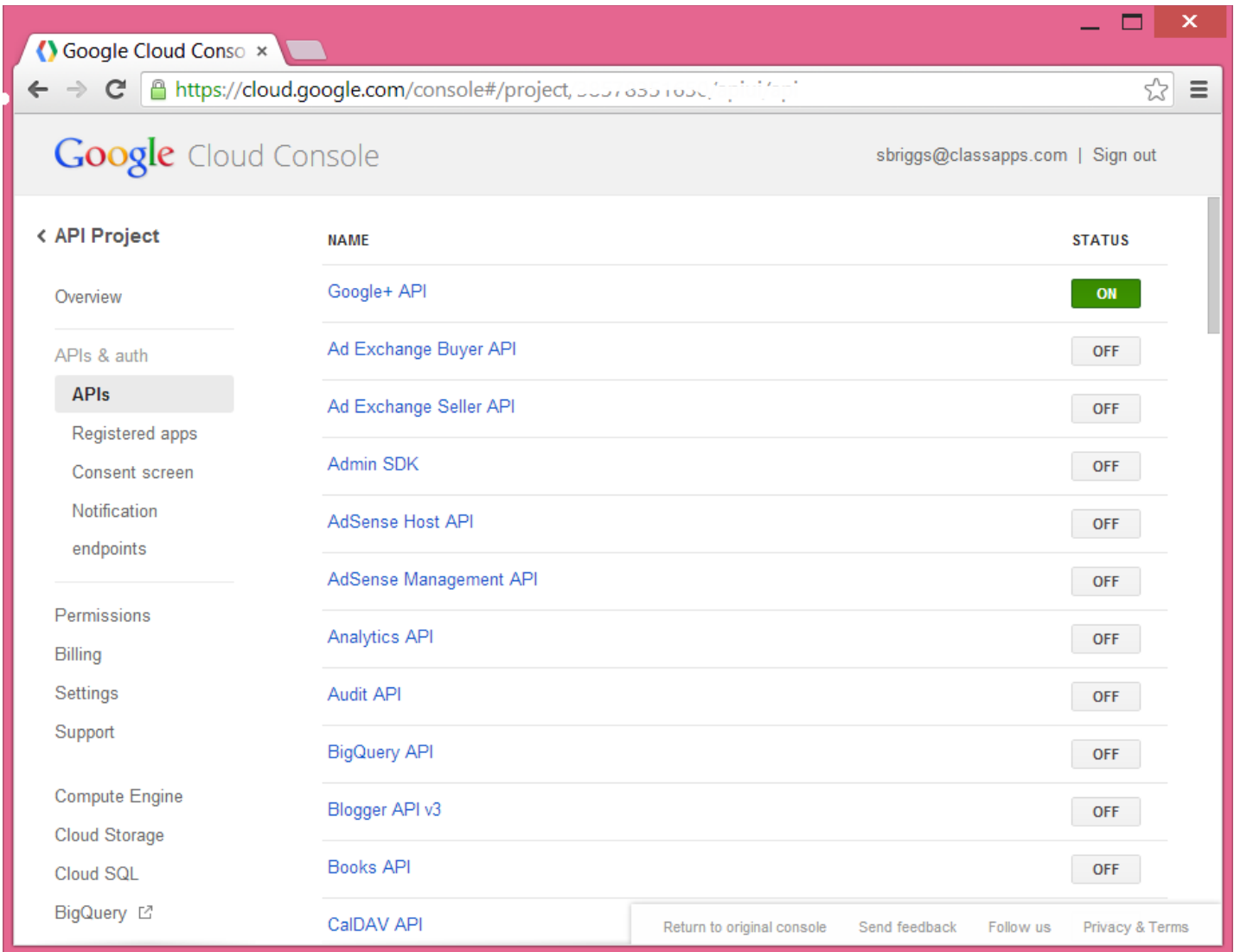
SelectSurvey.NET Server Software that is installed on a client's own Domain must be registered with Google and have its own domain token registration. SelectSurvey.NET hosted service already has a token registration with Google because it is hosted on the **SelectSurvey.NET** domain, which has been approved for this.

All applications that access a Google API must be registered through the [Google Cloud Console](https://cloud.google.com/console) (<https://cloud.google.com/console>). The result of this registration process is a set of values (such as a client ID and client secret) that are known to both Google and **SelectSurvey.NET**.

Please refer to the directions from GOOGLE, because they can change this process at any time at their discretion. Below are the general directions for the process at the date of this writing 11-12-2013.

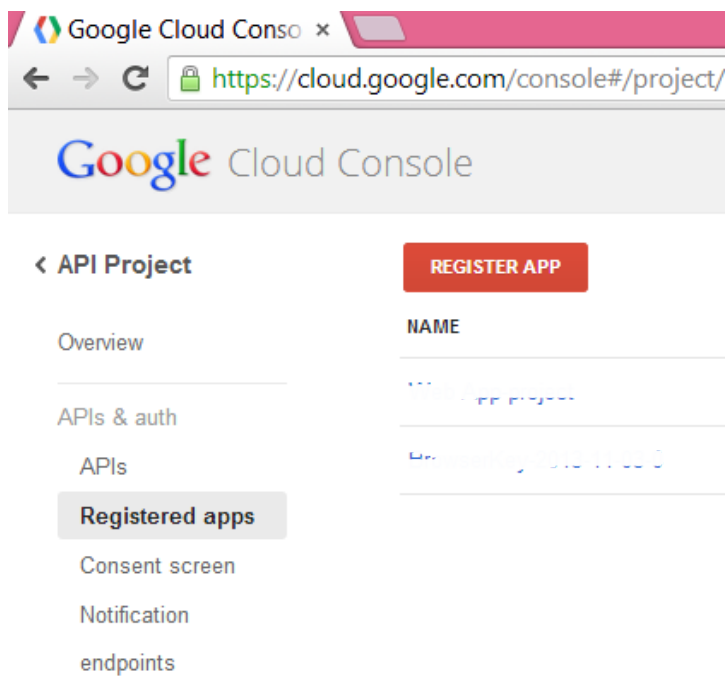
1. Select API's you need access to.

Select **"GOOGLE + API"** as shown in the screenshot below, so that it shows status "ON". This is the only API you need access to for SelectSurvey.NET to utilize the Google Apps Login feature. All other API status will show "OFF".

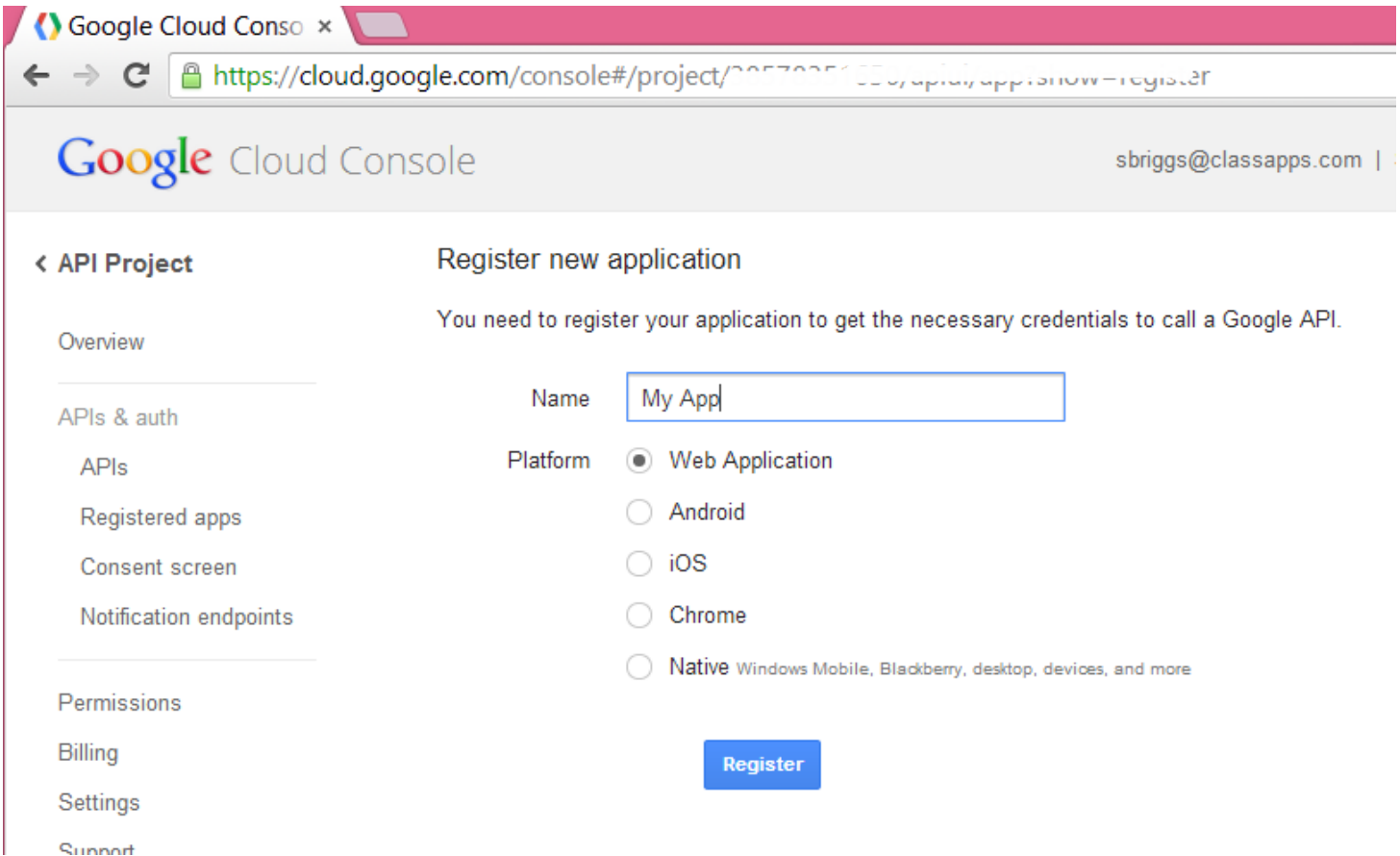


2. Register the Web App.

After logging in to the cloud.google.com/console, click “REGISTER APP” it is a red button at the top of the screen as shown in the screenshot below:



Then fill in the form with whatever name you want, and select "Web Application" as the Platform as shown in the screenshot below.



Google Cloud Console x

← → ↻ <https://cloud.google.com/console#/project/28578251-020/api/appl/show-register>

Google Cloud Console sbriggs@classapps.com |

< API Project

Register new application

You need to register your application to get the necessary credentials to call a Google API.

Overview

APIs & auth

APIs

Registered apps

Consent screen

Notification endpoints

Permissions

Billing

Settings

Support

Name

Platform

☒ Web Application

☐ Android

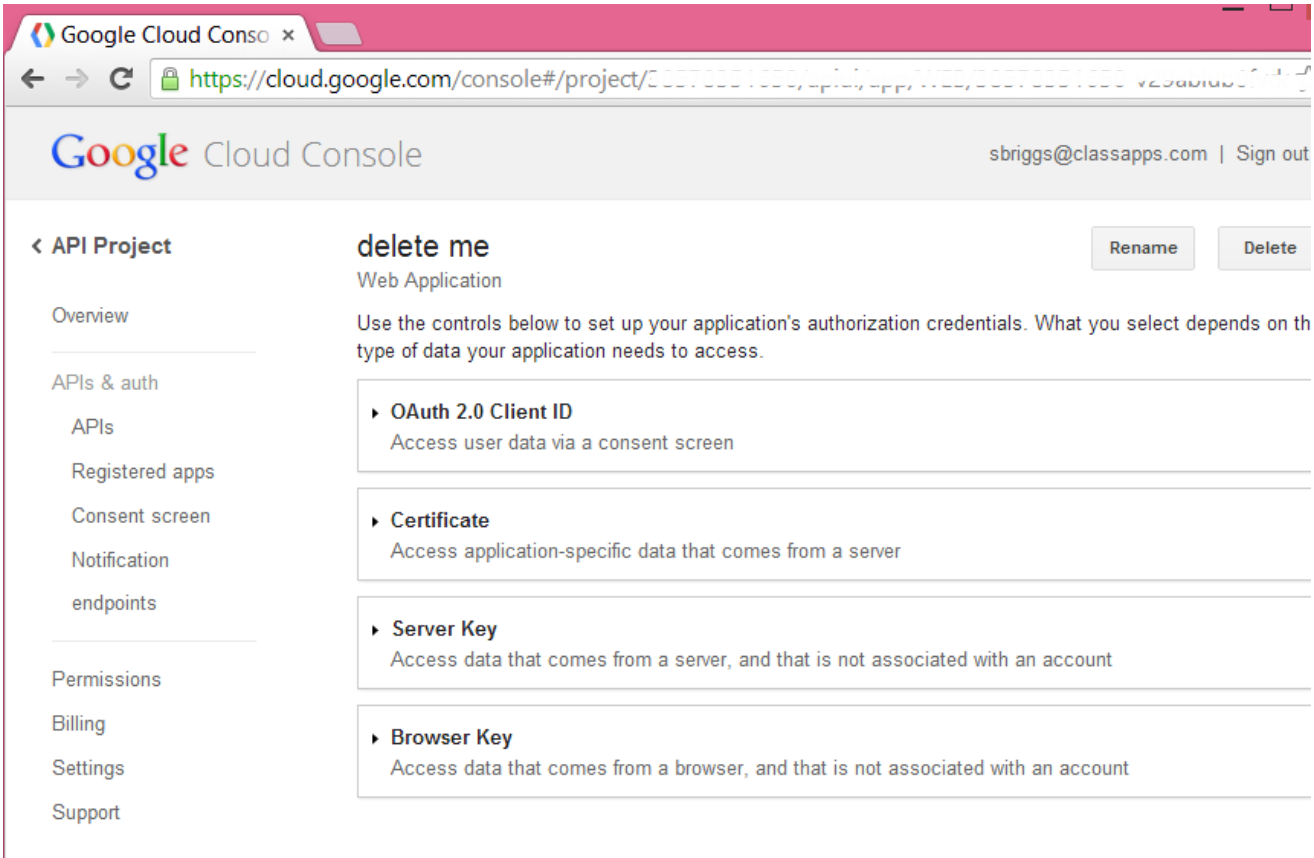
☐ iOS

☐ Chrome

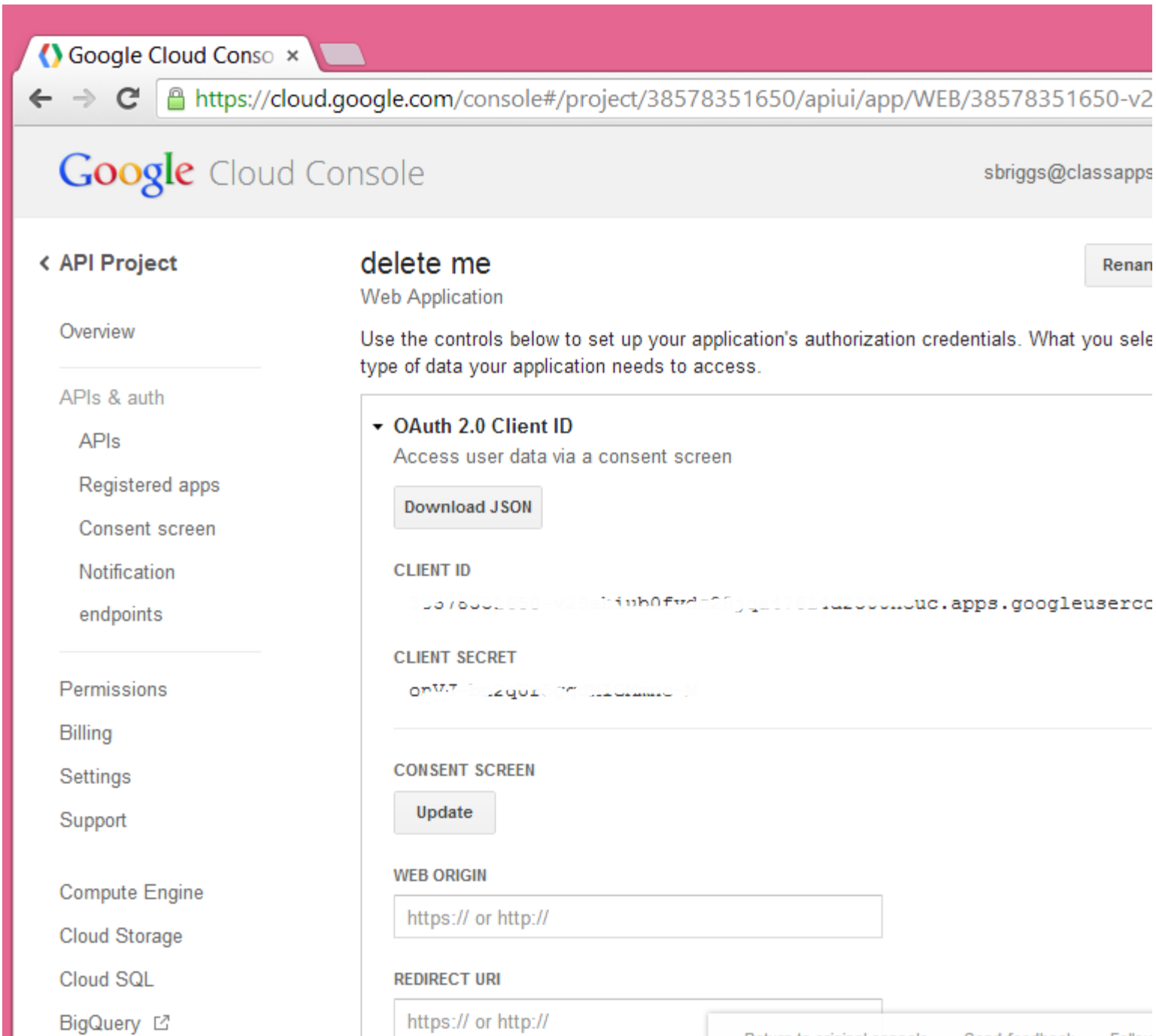
☐ Native Windows Mobile, Blackberry, desktop, devices, and more

Register

Click "Register".
You will then see the below screen where you will click OAUTH2.0 Client ID.



Click OAUTH2.0 Client ID on screen above. Then in screenshot below, copy the values of “CLIENT ID” and “CLIENT SECRET” into the SelectSurvey.NET Web.config as described in “Setup Step 2” of this manual.



3. Enter Web Origin and Redirect URI

Type in the fields "WEB ORIGIN" and "REDIRECT URI" the below, then click "GENERATE".

WEB ORIGIN:

<http://yourdomain.com> (this would be your domain where the survey application is installed).

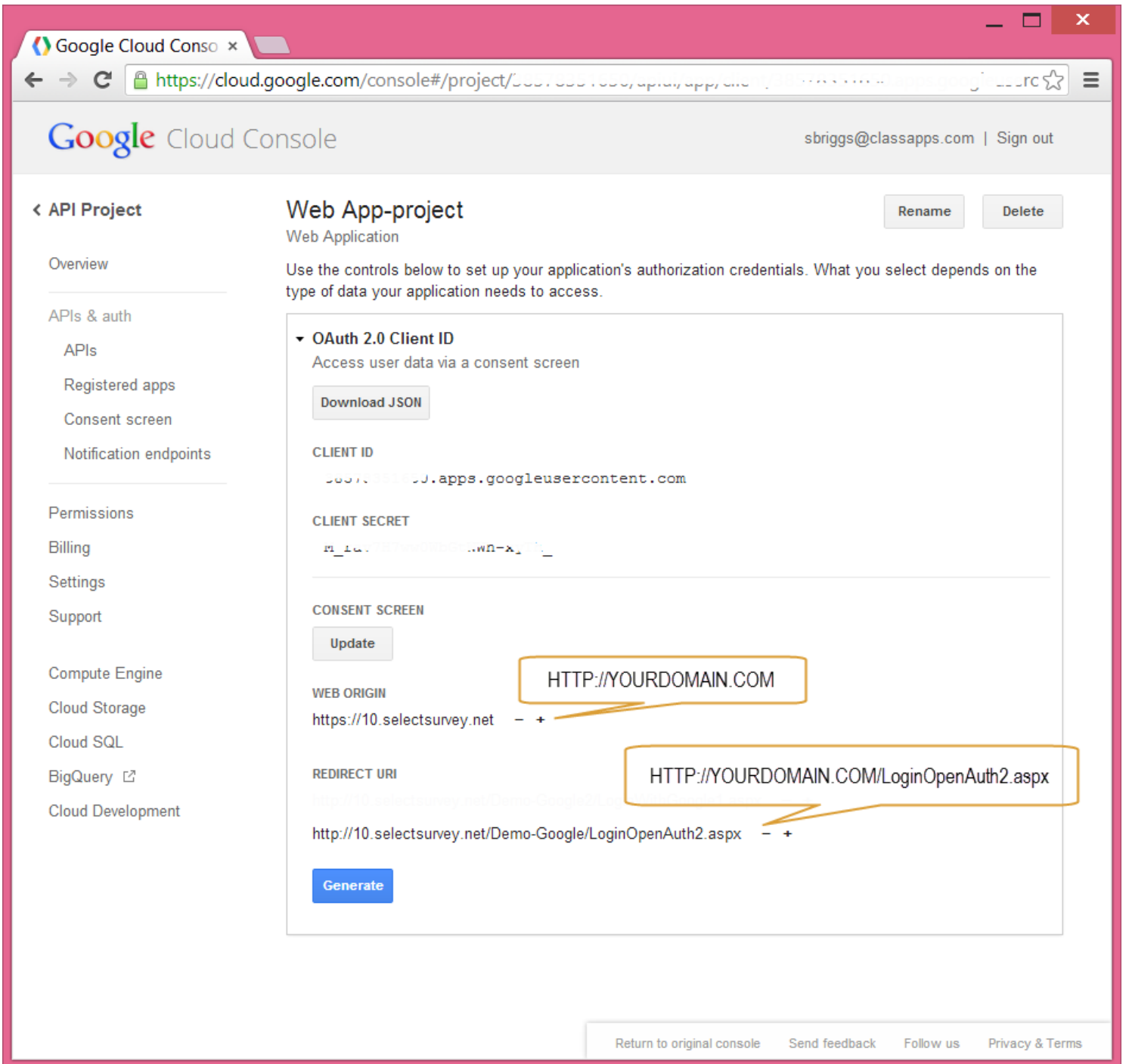
REDIRECT URI:



<http://yourdomain.com/LoginOpenAuth2.aspx> (this would be your domain where the survey application is installed and should contain "LoginOpenAuth2.aspx" which is the survey page that handles the google login callbacks. This URL must be correct or the login will not work. If you have your survey application in a sub folder it would be like this:

<http://yourdomain.com/surveyfolder/LoginOpenAuth2.aspx>

Click the "GENERATE" Blue button.
You are done with the Google Registration.



Google Cloud Console

sbriggs@classapps.com | Sign out

< API Project

Overview

APIs & auth

- APIs
- Registered apps
- Consent screen
- Notification endpoints

Permissions

Billing

Settings

Support

Compute Engine

Cloud Storage

Cloud SQL

BigQuery

Cloud Development

Web App-project

Web Application

Use the controls below to set up your application's authorization credentials. What you select depends on the type of data your application needs to access.

OAuth 2.0 Client ID

Access user data via a consent screen

[Download JSON](#)

CLIENT ID

6637655100.apps.googleusercontent.com

CLIENT SECRET

AIzaSyB7wG8B0C0wN-x1...

CONSENT SCREEN

[Update](#)

WEB ORIGIN

https://10.selectsurvey.net - + **HTTP://YOURDOMAIN.COM**

REDIRECT URI

http://10.selectsurvey.net/Demo-Google2/... - + **HTTP://YOURDOMAIN.COM/LoginOpenAuth2.aspx**

[Generate](#)

[Return to original console](#) [Send feedback](#) [Follow us](#) [Privacy & Terms](#)

Setup Step 2: Adding Google Token to SelectSurvey.NET web.config

2. Put your Google Token in your SelectSurvey.NET WEB.CONFIG file.

It is a requirement by Google for domains that access the Google API for Google Apps Federated Login to obtain a token from Google with their domain in it. This domain will need to match the settings in the web.config of SelectSurvey.NET as shown below. After registering with Google (To register with Google go here: <https://accounts.google.com/ServiceLogin?service=devconsole&passive=1209600&continue=https://code.google.com/apis/console/&followup=https://code.google.com/apis/console/>), you copy the token values from your Google account to the SelectSurvey.NET web.config. SelectSurvey.NET Server Software has a web.config file with placeholders for the google tokens as shown below.

These tags will be found inside the <appSettings> section as below:

```
<!-- replace the x's and YOUR-DOMAIN with your own values -->
<add key="google_clientId" value="xxxxxxx.apps.googleusercontent.com" />

<add key="google_clientEmail" value="xxxxxxxxx@developer.gserviceaccount.com" />

<add key="google_clientSecret" value="xxxxxxxxxxx" />

<!--change the url value to where the application is installed. Example:
http://10.selectsurvey.net/Demo-Google/LoginOpenAuth2.aspx -->
<add key="google_RedirectUrl" value="http://YOUR-DOMAIN.com/LoginOpenAuth2.aspx" />

<!-- change the value to where the application is installed. Example: http://10.selectsurvey.net/Demo-
Google -->
<add key="google_JavaScriptOrigin" value="http://YOUR-DOMAIN.com" />
```

Edit the web.config in notepad or text editor to change the value="x" to the values you were assigned by Google.

You will also be required to set two other settings in the same web.config with the license key, and the switch to turn on or off Google Apps login integration:

```
<!-- License Key for Google Apps/Open ID Integration Add-On -->
<add key="GOOGLE_APPS_LOGIN_LICENSE_KEY" value="paste in license key from purchase"/>

<!-- set to "yes" or "no" whether you want to use Google Apps/Open ID Integration-->
<add key="USE_GOOGLE_APPS_LOGIN" value="yes"/>

<!-- set to your domain for google apps so no other google domain users can authenticate. Example:
"yourdomain.com" If left empty, ANYONE with a google login can login.-->
<add key="GOOGLE_APPS_DOMAIN" value="yourdomain.com"/>
```



The license key is emailed and also displayed on your customer account product downloads page on classapps.com. You would copy the license key into the value=" [paste in license key from purchase](#)" above.

If you want all google users with a login (all domains) to be able to take surveys, then leave the "GOOGLE_APPS_DOMAIN" value="". If you leave the value empty, all domains can login. In most cases you want to restrict login to your own domain for Google Apps.

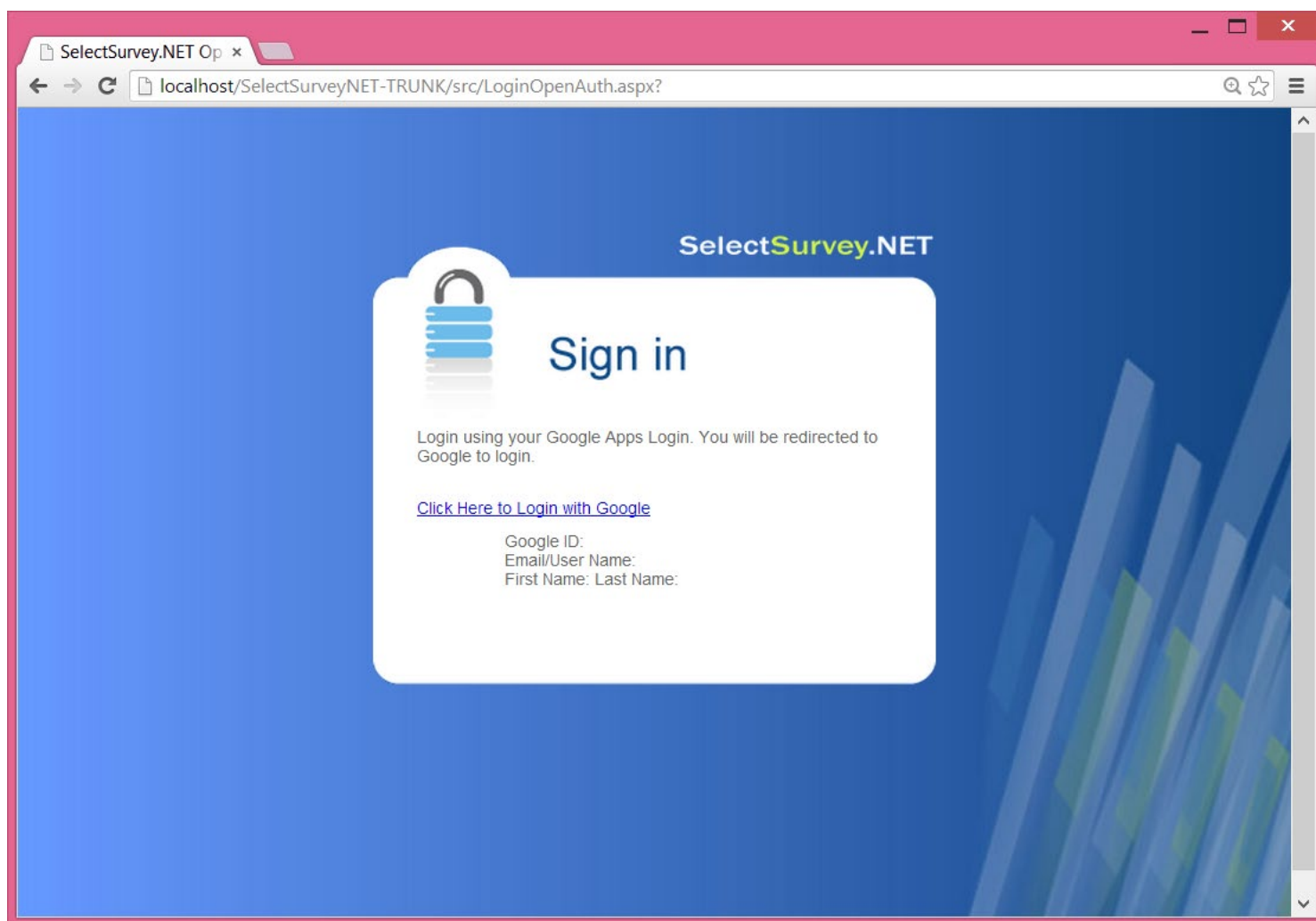
Setup Step 3: Enable Federated Login Service in Google Apps Account

3. The Federated Login Service is disabled by default for Google Apps.

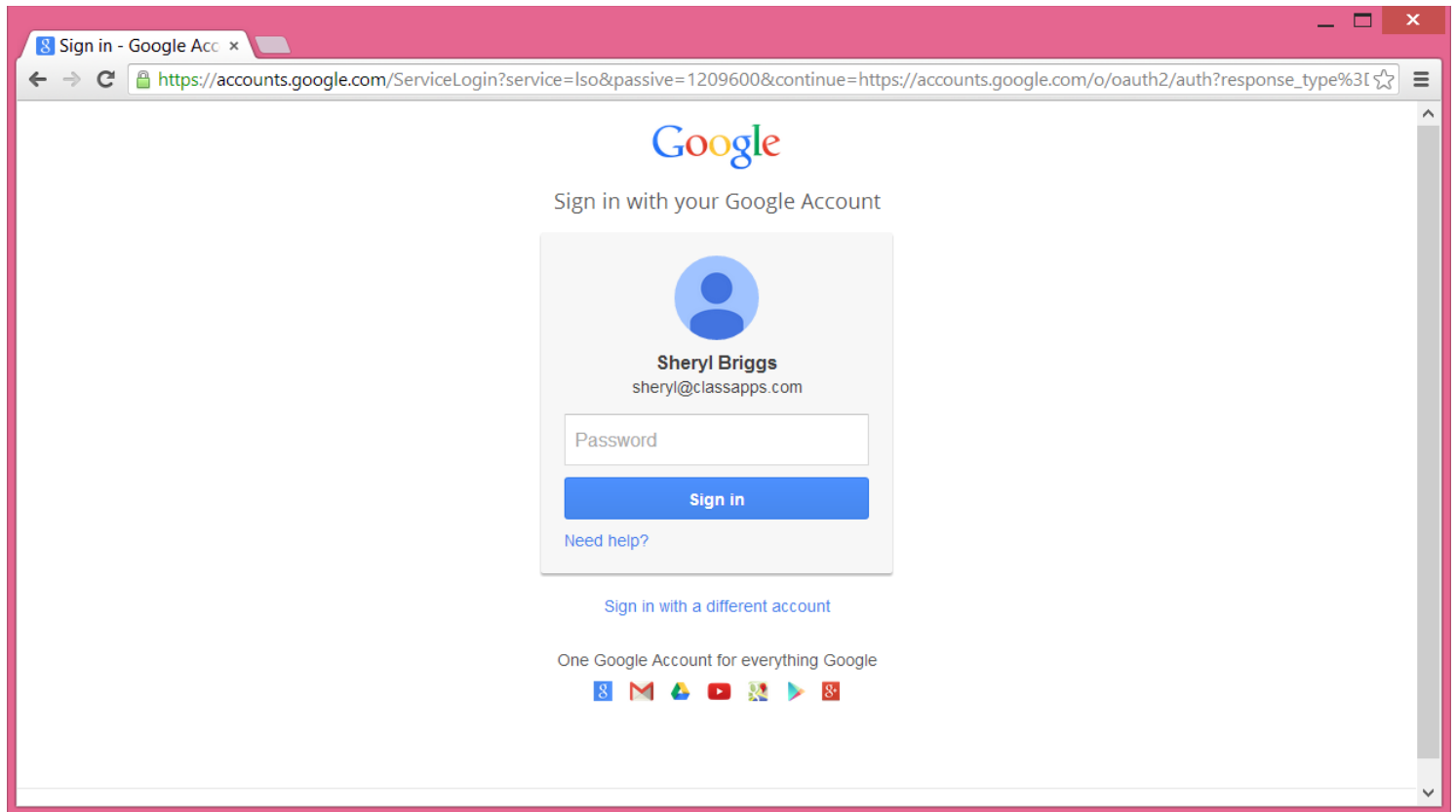
The domain admin with Google Apps can enable Federated Login Service from the Google Apps Control Panel at <http://www.google.com/a/cpanel/<your-domain>/SetupIdp>.

Step 4: Login with Google Apps Account and set Admin account

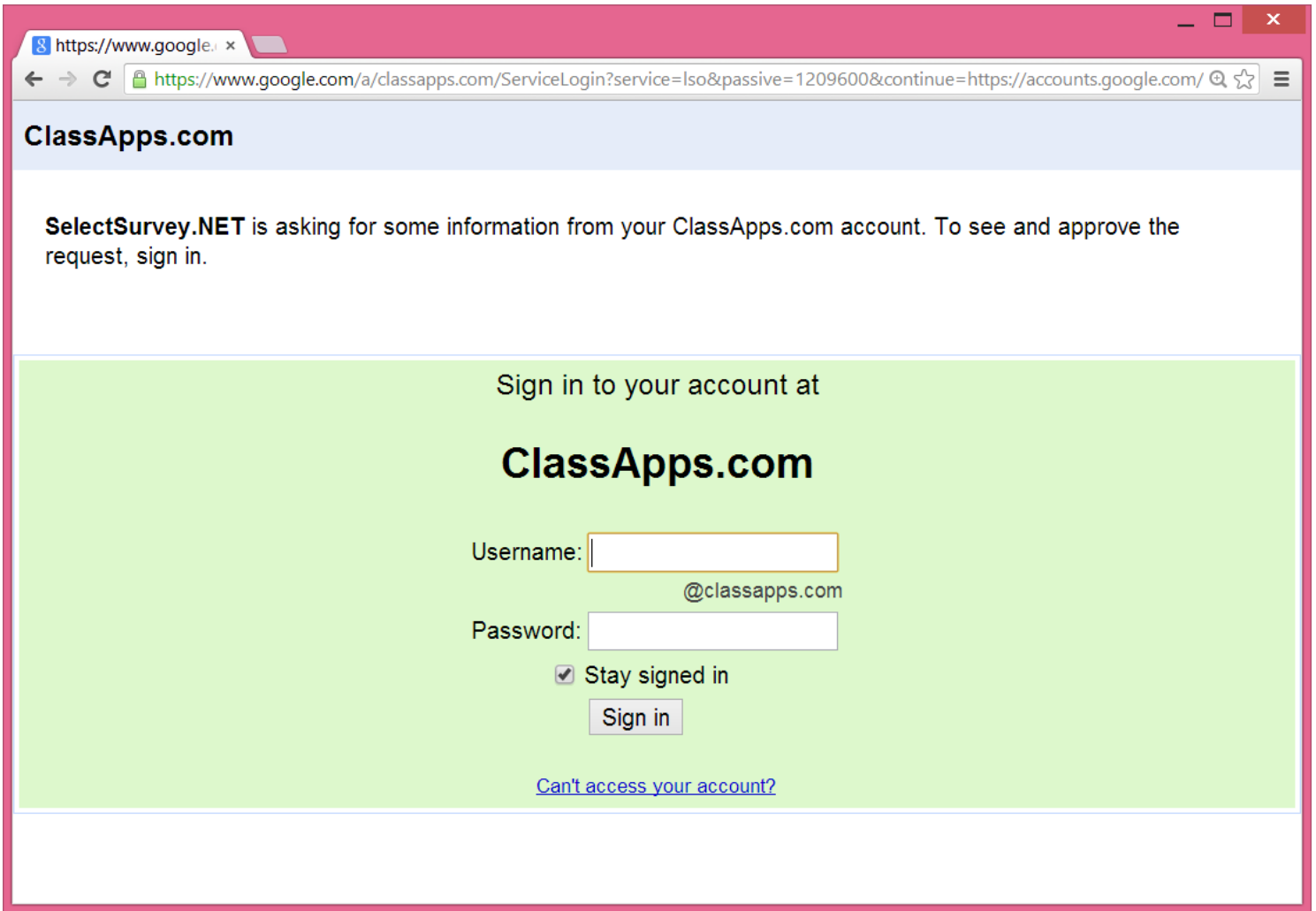
The first time any user logs in they are inserted into the sur_user table with the lowest role level (for taking surveys). If the user already exists in the survey database, it uses the existing user account. After installing the survey software, you will need at least one admin user. Login with the Google Apps account that you want to set as the survey admin account. In the database find that user ID that was created with that username in the sur_user table. The sur_user.username should be the same as the Google Apps username. Open the Survey SQL database and find the row in the sur_user_to_role_mapping table that has that user_id and update the role from role "1" to role "3" so that user will be set as the survey admin. Now logout and back in with the new admin user. You will be able to set other users that are automatically synched to admin or create role as well, by clicking "Users" then "Edit", then selecting the user role from the drop down box in the survey interface.



If no domain has been entered into the web.config you will see the general google login as below:



If you have specified a domain in the web.config you will see the login for that domain as below:



https://www.google.com/a/classapps.com/ServiceLogin?service=iso&passive=1209600&continue=https://accounts.google.com/

ClassApps.com

SelectSurvey.NET is asking for some information from your ClassApps.com account. To see and approve the request, sign in.

Sign in to your account at

ClassApps.com

Username:

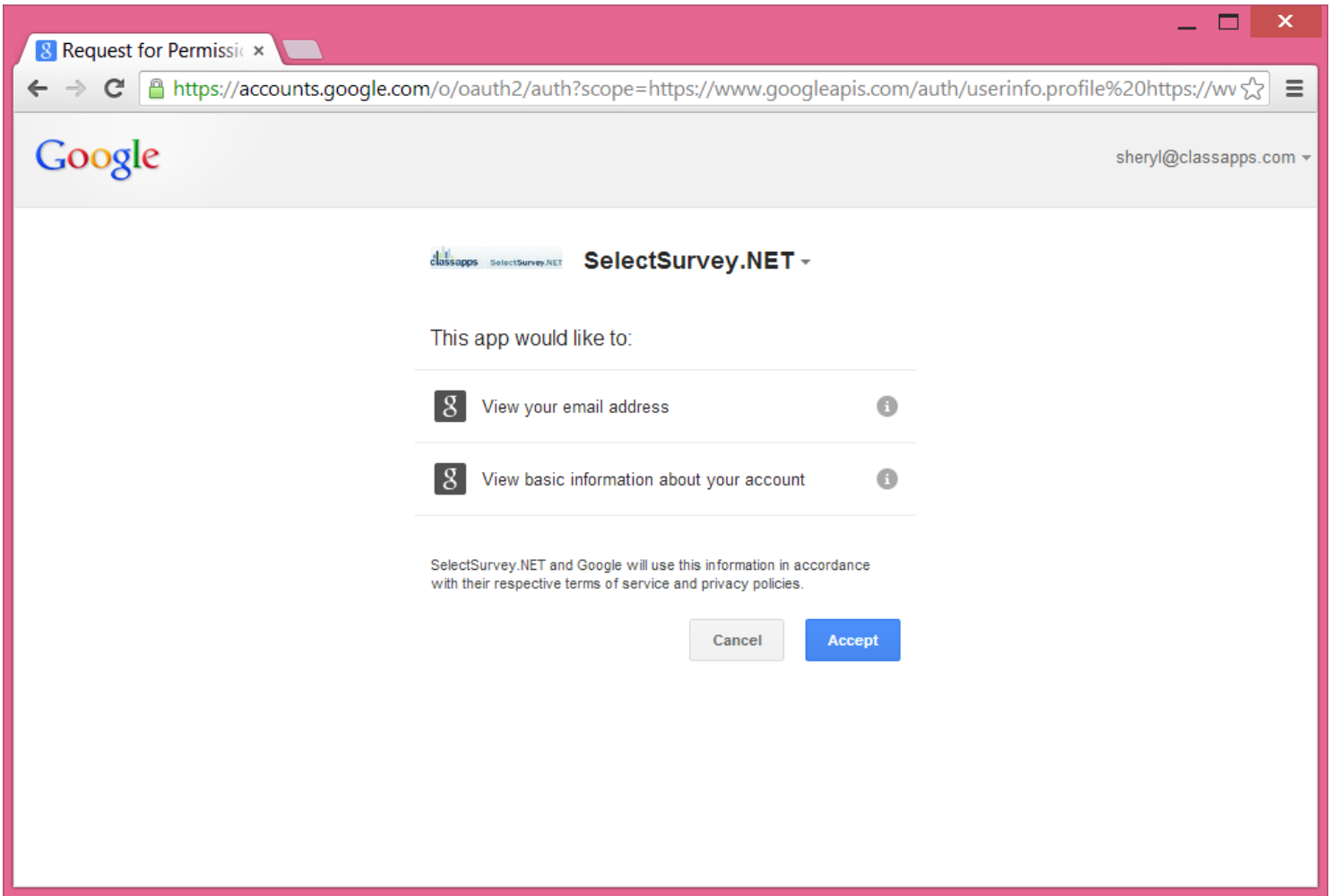
@classapps.com

Password:

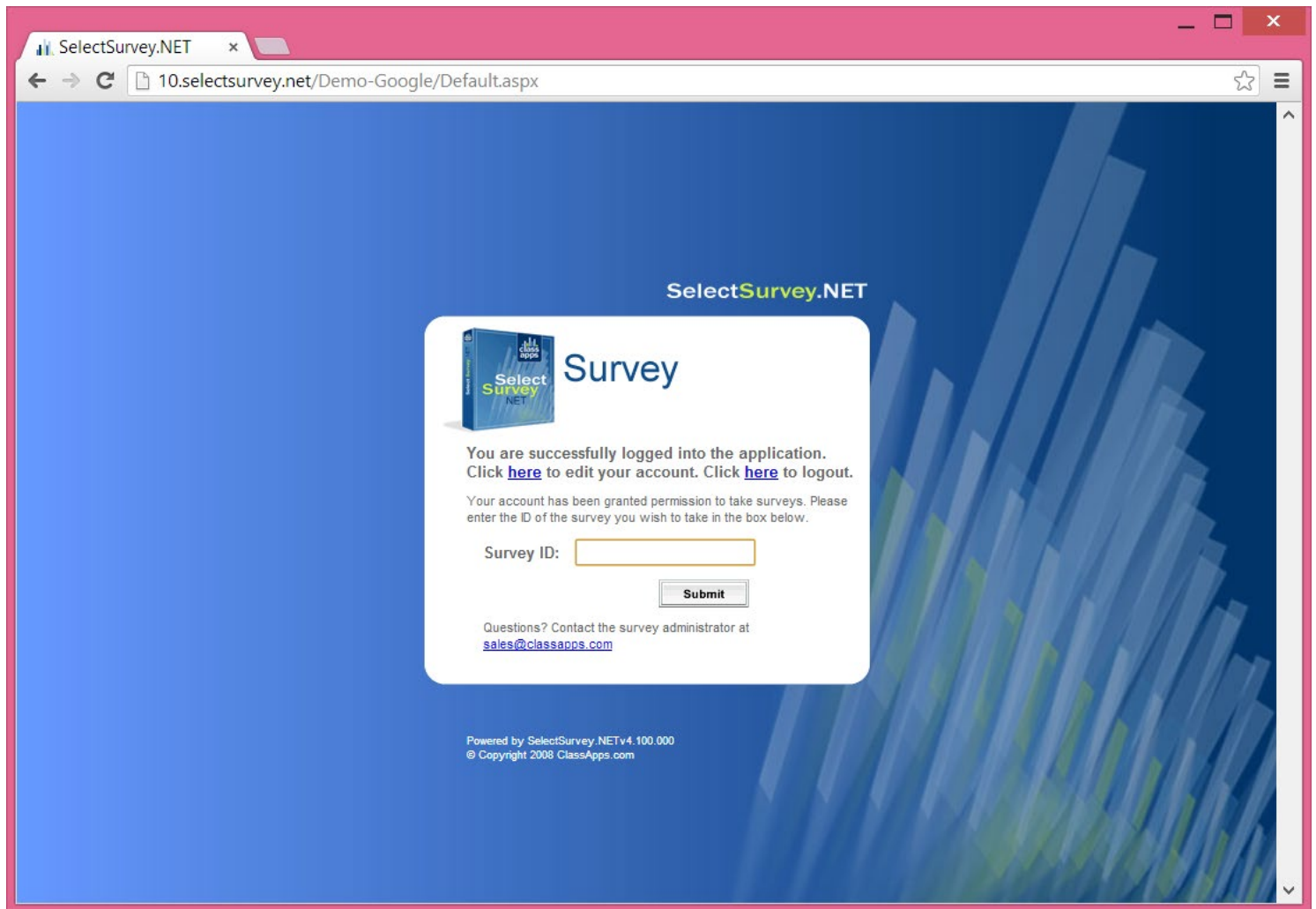
☒ Stay signed in

[Can't access your account?](#)

The user will be asked for permission to share their login and name with the application, the user needs to click "Accept" on the screen below:



If the user has never logged in before, they are logged in as user role=1, or “user” role, so that they can only take surveys, or edit their account as below:



Reference Documentation:

Reference documentation from google is located here:

https://developers.google.com/google-apps/sso/openid_reference_implementation

[OpenID](http://openid.net) (<http://openid.net>)

OpenID Connect Login Integration (AZURE Active Directory, Office 365, OAuth2.0, IdentityServer3, Azure AD ID)

OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It allows Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.

Fill in the Web.config section for Open ID login integration with the information from the app you want to integrate with.

```
<!--
*****
Owin/IdentityServer3/OpenID Connect/Social Authentication
*****
-->
<!-- replace the x's and YOURDOMAIN with your own values -->
<!-- set to "yes" or "no" whether you want to use identityserver3 with azure AD ID Integration, which
uses openauth2-->
<add key="USE_OPENID_APPS_LOGIN" value="no"/>

<!--client id: to get client id, login to your Azure AD portal, copy "application id" and paste below -->
<add key="openid_clientId" value="000000000-0000-0000-0000-000000000000"/>

<!--tenant id: (to get tenant id, login to your Azure AD portal, copy "Tenant ID" and paste below -->
<add key="openid_authority" value="https://login.microsoftonline.com/000000000-0000-0000-0000-
000000000000"/>

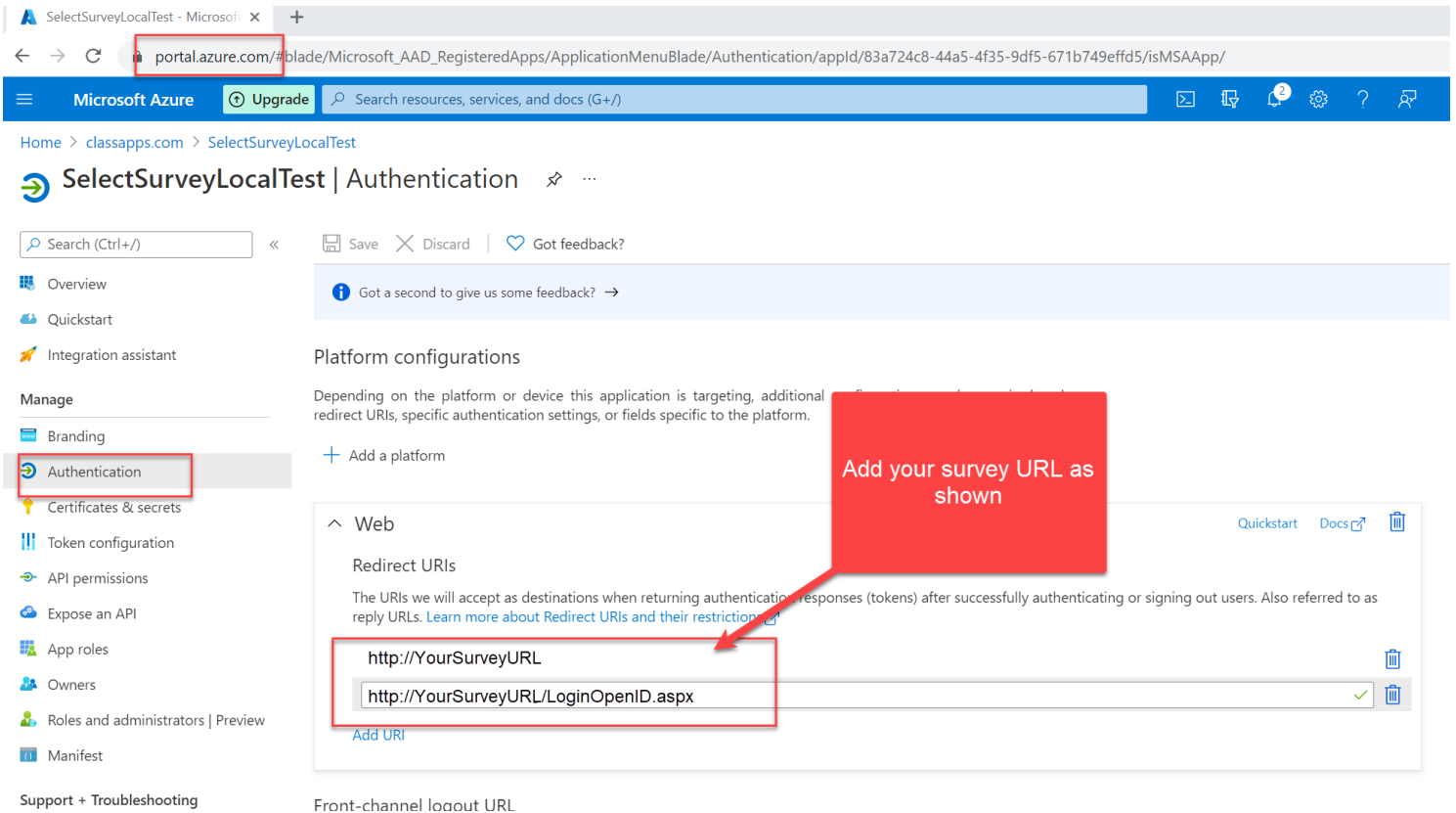
<!--Replace with your survey URL followed by "/LoginOpenID.aspx": -->
<add key="openid_RedirectUri" value="http://yoururl.com/LoginOpenID.aspx />

<!--this is the text that will show on the login page button they click to login to Azure AD etc.: -->
<add key="openid_LoginButtonText" value="Perseus Azure AD"/>

<!--the below is optional and not required-->
<!--leave values blank for azure AD -->
<add key="openid_clientSecret" value=""/>
<add key="openid_metadataAddress" value=""/>
```

Azure AD setup in the Azure AD portal: (see screenshots below)

- Add the application in Azure AD portal.
- Click "authentication" and add the acceptable end point URLs as shown. This must match the URL in the web.config for "openid_RedirectUri". If it does not, then you will get a login error.
- Click "ID Tokens" checkbox.



SelectSurveyLocalTest - Microsoft

portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/Authentication/applid/83a724c8-44a5-4f35-9df5-671b749effd5/isMSAApp/

Microsoft Azure Upgrade Search resources, services, and docs (G+)

Home > classapps.com > SelectSurveyLocalTest

SelectSurveyLocalTest | Authentication

Search (Ctrl+/) Save Discard Got feedback?

Overview Quickstart Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

Front-channel logout URL

Platform configurations

Depending on the platform or device this application is targeting, additional redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Web

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

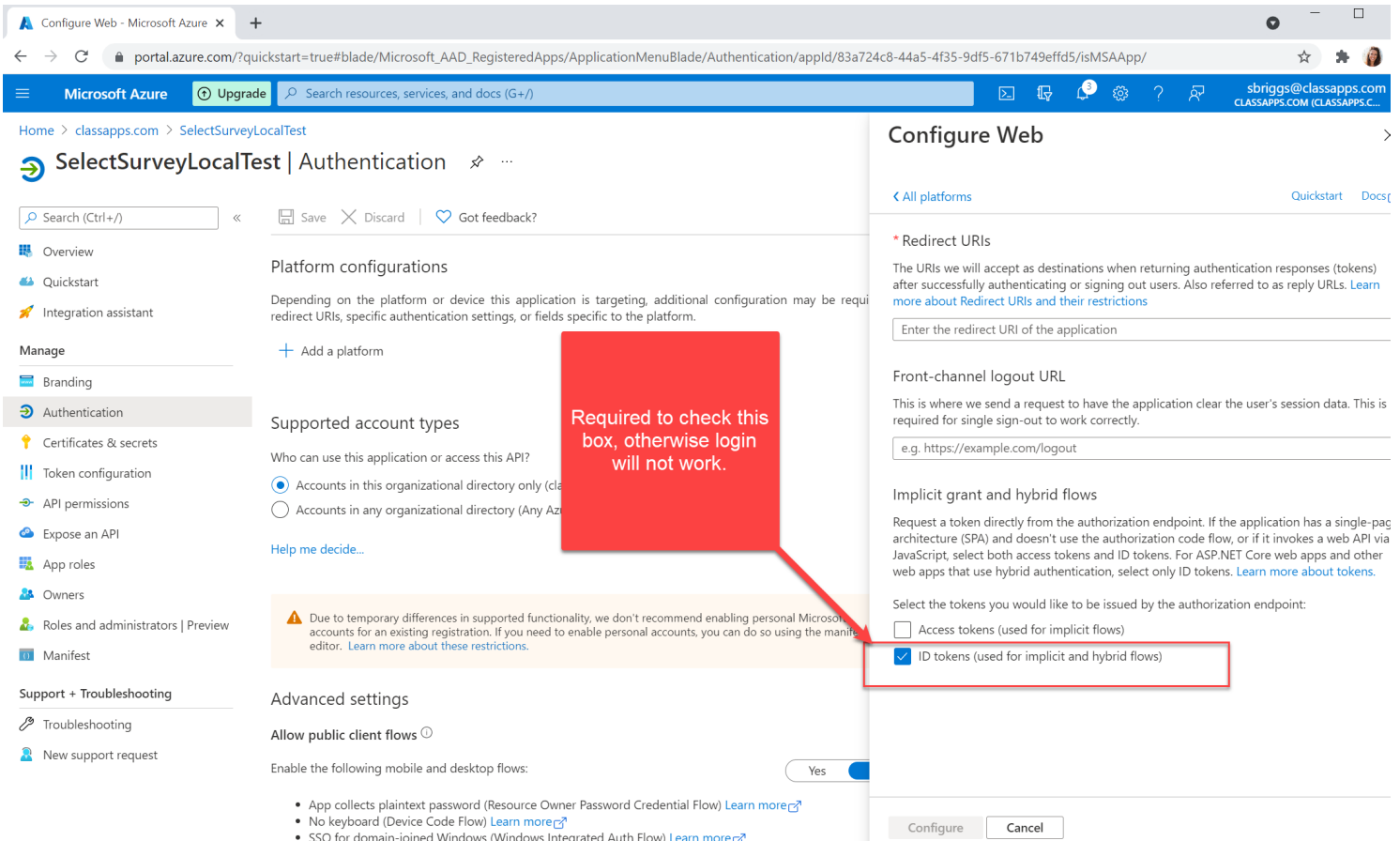
- http://YourSurveyURL
- http://YourSurveyURL/LoginOpenID.aspx

Add URI

Quickstart Docs

Add your survey URL as shown

Also you must set to allow ID tokens as shown in the screenshot below:



Configure Web - Microsoft Azure

portal.azure.com/?quickstart=true#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/Authentication/appld/83a724c8-44a5-4f35-9df5-671b749effd5/isMSAApp/

Microsoft Azure Upgrade Search resources, services, and docs (G+)

Home > classapps.com > SelectSurveyLocalTest

SelectSurveyLocalTest | Authentication

Search (Ctrl+/) Save Discard Got feedback?

Overview Quickstart Integration assistant

Manage

Branding Authentication Certificates & secrets Token configuration API permissions Expose an API App roles Owners Roles and administrators | Preview Manifest

Support + Troubleshooting Troubleshooting New support request

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required. For example, for mobile apps, you may need to configure redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (classic)

☐ Accounts in any organizational directory (Any Azure AD directory - Single sign-on)

Help me decide...

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. [Learn more about these restrictions.](#)

Advanced settings

Allow public client flows ☐

Enable the following mobile and desktop flows:

Yes

- App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#)
- No keyboard (Device Code Flow) [Learn more](#)
- SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#)

Configure Web

< All platforms Quickstart Docs

* Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

Enter the redirect URI of the application

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. https://example.com/logout

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more about tokens.](#)

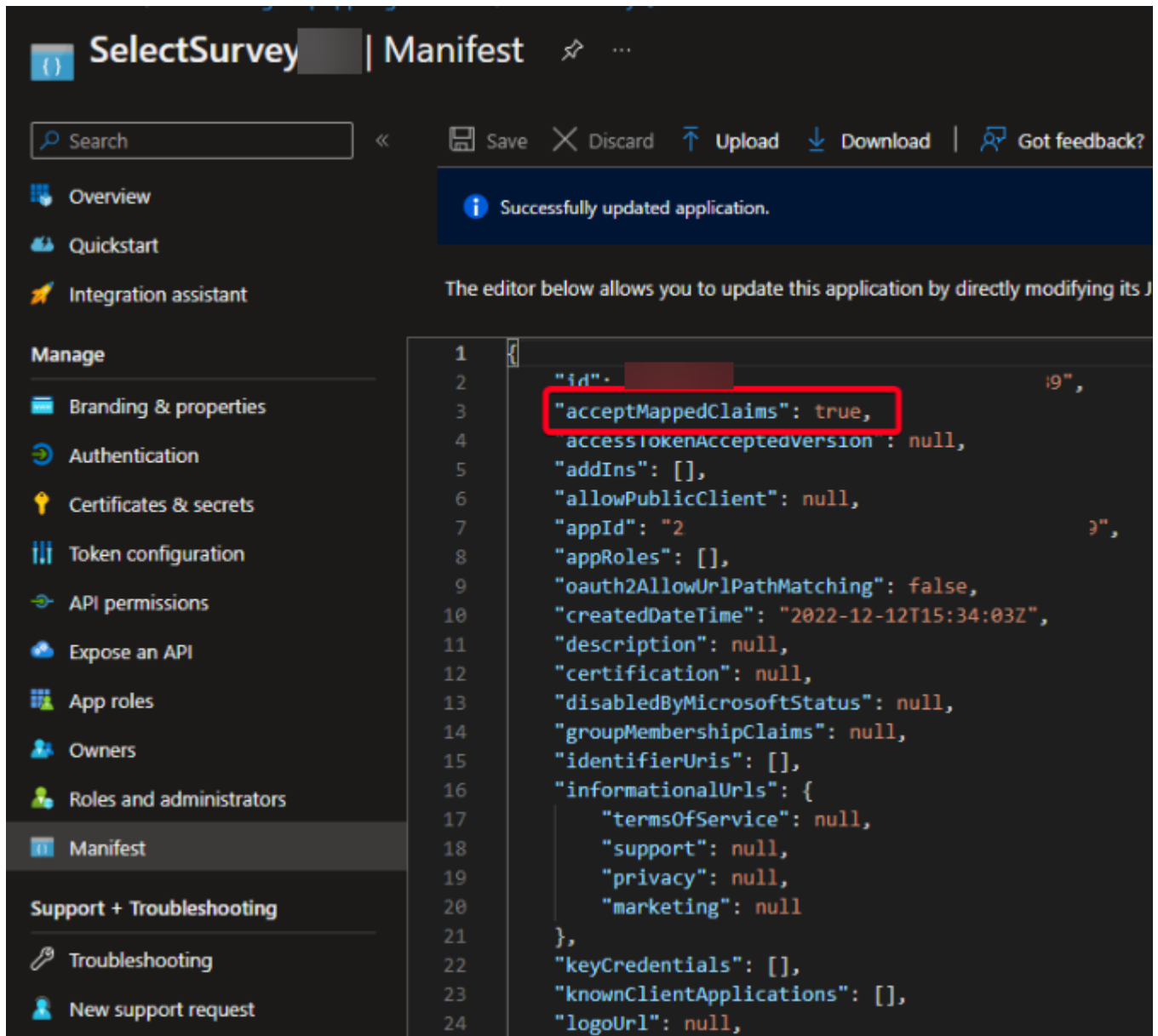
Select the tokens you would like to be issued by the authorization endpoint:

☐ Access tokens (used for implicit flows)

☒ ID tokens (used for implicit and hybrid flows)

Configure Cancel

Set the "Manifest" > "acceptMappedClaims": true,



SelectSurvey | Manifest

Search Save Discard Upload Download Got feedback?

Overview Quickstart Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest**

Support + Troubleshooting

- Troubleshooting
- New support request

Successfully updated application.

The editor below allows you to update this application by directly modifying its J

```

1 {
2   "id": "9",
3   "acceptMappedClaims": true,
4   "accessTokenAcceptedVersion": null,
5   "addIns": [],
6   "allowPublicClient": null,
7   "appId": "2",
8   "appRoles": [],
9   "oauth2AllowUrlPathMatching": false,
10  "createdDateTime": "2022-12-12T15:34:03Z",
11  "description": null,
12  "certification": null,
13  "disabledByMicrosoftStatus": null,
14  "groupMembershipClaims": null,
15  "identifierUri": [],
16  "informationalUrls": {
17    "termsOfService": null,
18    "support": null,
19    "privacy": null,
20    "marketing": null
21  },
22  "keyCredentials": [],
23  "knownClientApplications": [],
24  "logoUrl": null,

```

To find the values to put in the web.config:

Get Client ID

Login into your azure account.

Select azure active directory in the left sidebar.

Click Enterprise applications.

Click All applications.



Select the application which you have created.

Click Properties.

Copy the Application ID .

Find tenant ID through the Azure portal

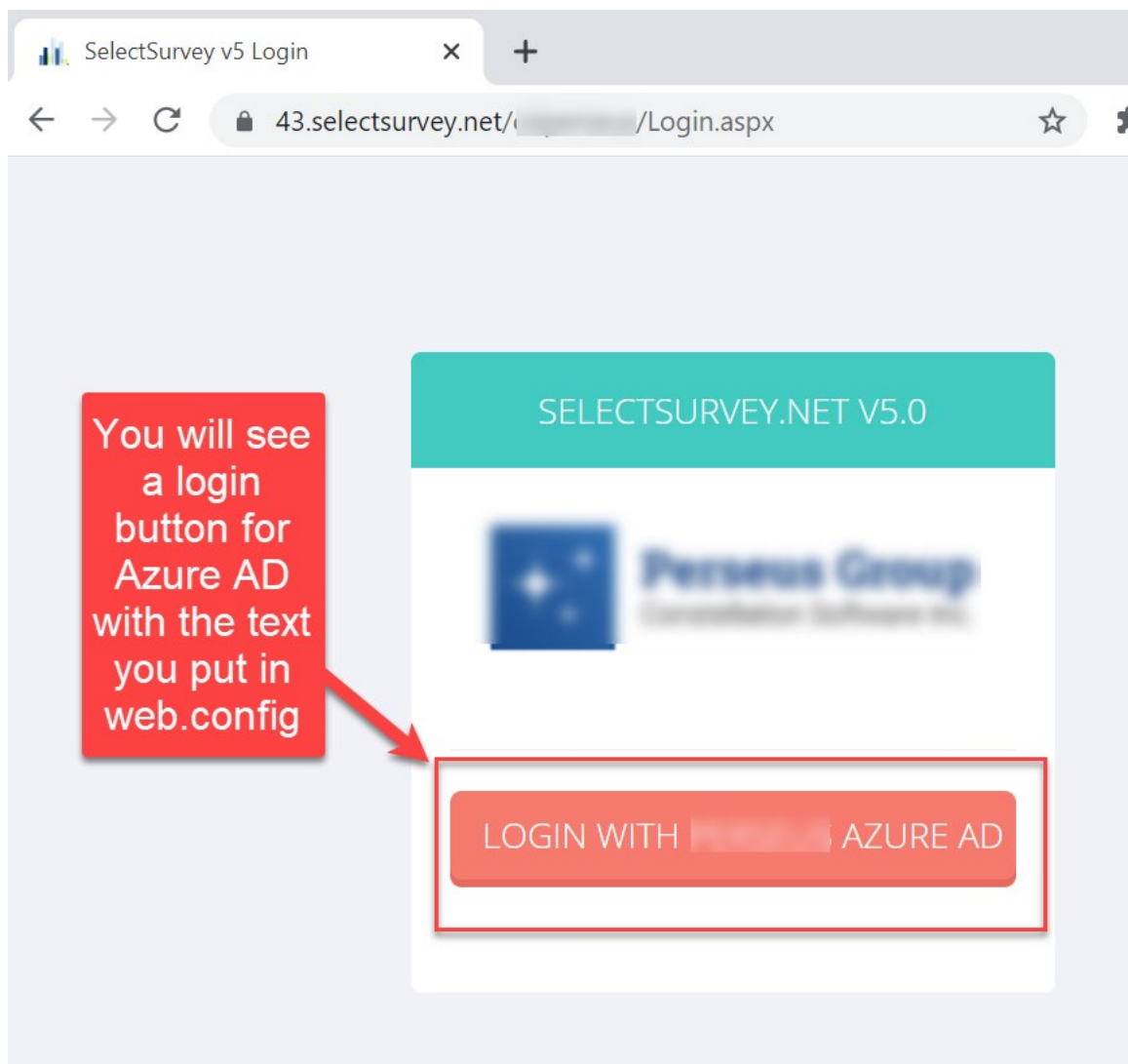
Sign in to the Azure portal.

Select Azure Active Directory.

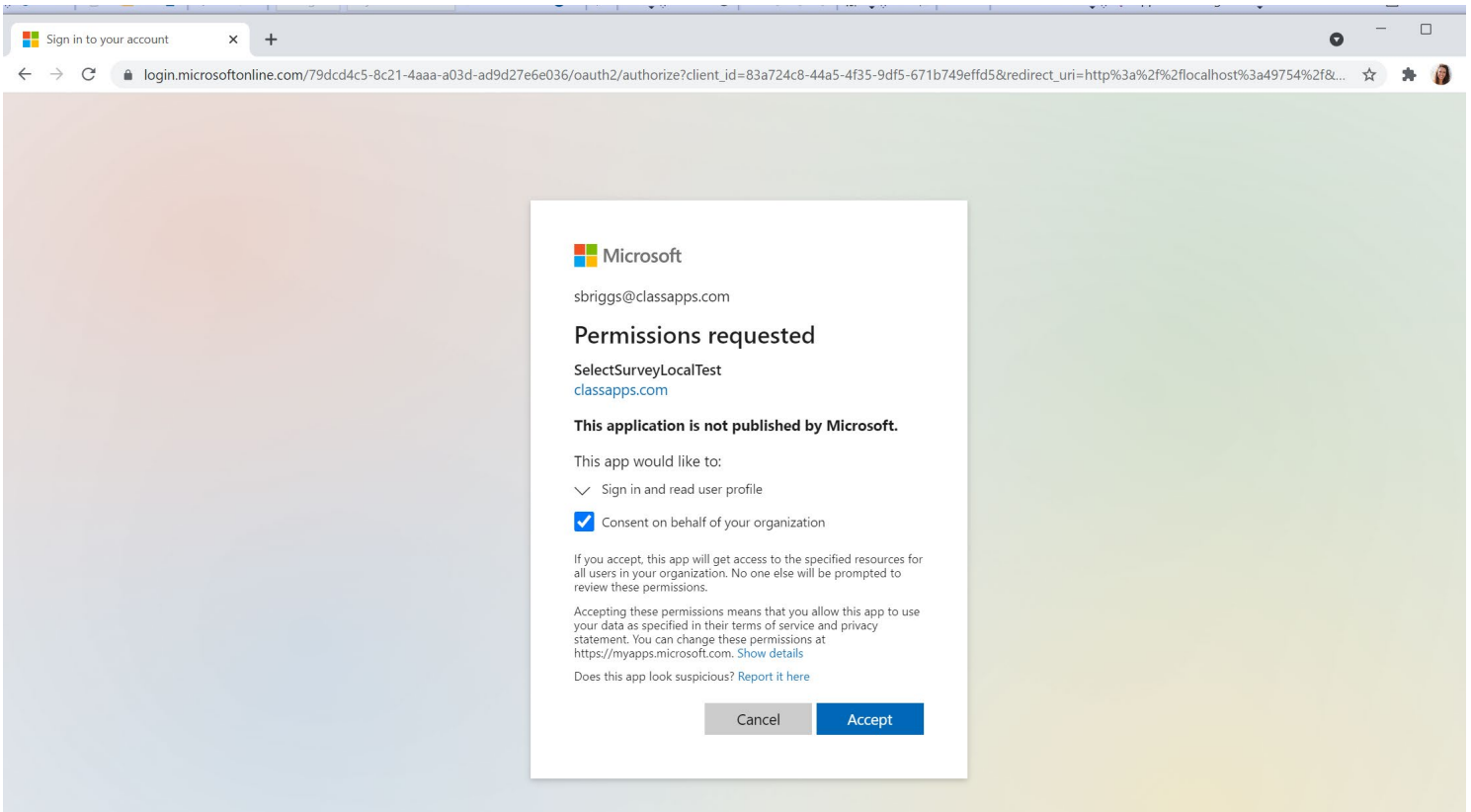
Select Properties.

Then, scroll down to the Tenant ID field. Your tenant ID will be in the box.

Test.



The first time you login you will see this screen, click “Accept”:



CAS Login Integration

The Central Authentication Service (**CAS**) is a single sign-on protocol. **SelectSurvey.NET** provides additional alternative login integrations.

Fill in the Web.config section for CAS login integration with the information from the app you want to integrate with.

```
<!--
*****
CAS Authentication
*****
-->
<!-- values: yes or no-->
<add key="USE_CAS_AUTHENTICATION" value="no"/>
<!-- example value="https://centrallogin.yourschool.edu/"-->
<add key="CAS_URL" value="https://centrallogin.yourschool.edu"/>
<!-- AD User Account -->
```



```
<add key="CAS_UserName" value="XXXX"/>
<add key="CAS_Password" value="****"/>
```

Standard (AD) Active Directory Login Integration with Login box (Also options for AD + SSO, LDAP, SAML, NTLM)

Each time a user logs in with their network Active Directory login, their data is imported or updated into the survey application (nothing is every updated in Active Directory), therefore it is synched at every login (survey roles and survey related info is maintained through the synchs) and no import of data is necessary. No Active Directory passwords are stored in the survey application or its database. If no Active Directory data exists for survey required fields such as email address, an administrator must fill those in within the survey application in the user edit page. These values will not be over-written by the synch if they remain empty in Active Directory.

The following pages are different or only used for active directory integration:

- Web.config
- LoginActiveDirectory.aspx/cs
- Other pages may be disabled or coded to behave differently:
 - forgot my password (disabled)
 - user edit
 - user add
 - user registration (disabled)
 - user buttons in the app
 - edit my account

Step 1:

Login to admin tools with non AD login (default admin/admin) click “admin tools”.

Click “Application wide settings”

Select “yes” from the drop down box next to “Use ActiveDirectory for login”

Click “Save”

Logout and delete cookies so that the next time you login it will use your AD login.

Edit the web.config to contain your active directory settings.

```
<!--
*****
AD FS ActiveDirectory Federated Login Claims Based Login Integration
```



```

*****
-->
<add key="USE_ADFS_LOGIN" value="no"/>

<!--
*****
LDAP Authentication
*****
-->
<!--ACTIVE DIRECTORY SETTINGS (CASE SENSITIVE!) UPDATED in v4.069.004 PLEASE CHECK VALUES-->

<!-- the below setting is for using the old AD code versus the new AD code that uses the new .net
AD classes -->
<!-- default is "no" -->
<add key="USE_OLD_AD_CODE" value="no"/>

<!--Prepopulate domain text box on login page? yes/no -->
<add key="POPULATE_DOMAIN_TXTBOX" value="yes" />

<!-- disable domain text box-->
<add key="DISABLE_DOMAIN_TXTBOX" value="no" />

<!--Domain = "test.com"; -->
<!--For multiple domains in drop down box, separate with a semicolon:
domain.com;domain2.com;domain3.com -->
<add key="Domain" value="test.com" />

<!--if using NEW: Default Root OU = "DC=test,DC=com" -->
<!--if using OLD: Default Root OU = "LDAP://test.com" -->
<add key="ADPath" value="DC=localhost" />

<!--Service User -->
<add key="ADUser" value="administrator" />

<!--Service User Password -->
<add key="ADPassword" value="123" />

<!--if using NEW: Default OU = "DC=test,DC=com" (no longer used in NEW)-->
<!--if using OLD: Default OU = "OU=DeveloperDepartment," -->
<add key="ADUsersPath" value="" />

<!-- (only used in NEW) -->
<!-- list of group name restrictions separated by comma (leave empty for no user group
restrictions): Test Users, Administrators-->
<add key="ADUserGroupRestriction" value="" />

<!--the below allows login with UPN. acceptable values are yes/no default is no-->
<!--setting to yes will hide domain text box and you must use domain email address for login -->
<add key="USE_AD_UPN_LOGIN" value="no" />

<!--setting to turn on display of debug info on the login page to assist with setting up AD
integration (TURN THIS OFF WHEN YOU ARE DONE!-->
<!--valid values are "on" and "off" when "on" error stack trace and line # info will display on
bottom of AD login page when "off" no info will display. -->
<add key="AD_DEBUG_MODE" value="off"/>

```



```

<!--If NTLM passthrough is activated the identity will be picked up by the browser (IE only) and
the user will never see the login page. They will be automatically logged in with their network identity
username in which all their survey activity will be stored. -->
<!-- valid values are "yes" and "no" -->
<add key="USE_NTLM_PASSTHROUGH_AUTHENTICATION" value="no"/>

<!-- required for NTLM passthrough to work otherwise regular AD login will show -->
<add key="FORCE_NTLM_PASSTHROUGH_AUTHENTICATION" value="no"/>

<!-- first checks SSO service (checks for ServerVariables["HTTP_SM_USER"]), then NTLM (checks for
ServerVariables["LOGON_USER"] internal uses NTLM auth for above AD network-->
<!-- possible values "yes" or "no"-->
<add key="SSO_EXTERNAL_NTLM_INTERNAL_PASSTHROUGH_AUTHENTICATION" value="no"/>

<!-- the below setting is the user role that is assigned to all users that are automatically
created via AD login-->
<!-- valid values are "1" for user or "2" for create role or "3" for admin role with the default
being 1 (user role) -->
<add key="DEFAULT_USER_ROLE_FOR_LOGIN_SYNC" value="1"/>

<!--END OF ACTIVE DIRECTORY SETTINGS -->
<!--
*****
-->

```

Config settings for both at bottom of web.config:

By default the web.config is set to use regular forms authentication and the various login types are handled via code. In order to switch authentication type from regular forms authentication (survey login page handled) to Active Directory/NTLM you uncomment the Active Directory section, and comment out the non Active Directory authentication section.

Below is the default web.config authentication section set for Non Active Directory:

```

<!--NON ACTIVE DIRECTORY: -->
    <authentication mode="Forms">
        <forms name=".ASPXAUTH" protection="All" timeout="240" loginUrl="Login.aspx"
slidingExpiration="true"/>
    </authentication>

<!--ACTIVE DIRECTORY: -->

    <!--<authentication mode="Forms"><forms name=".ASPXAUTH" timeout="240"
loginUrl="LoginActiveDirectory.aspx" path="/" slidingExpiration="true" /></authentication>-->

<!--END OF ACTIVE DIRECTORY -->

```

Below is the default web.config authentication section set for Active Directory:

```
<!--NON ACTIVE DIRECTORY: -->
<!--   <authentication mode="Forms">
           <forms name=".ASPXAUTH" protection="All" timeout="240" loginUrl="Login.aspx"
slidingExpiration="true"/>
           </authentication> -->

<!--ACTIVE DIRECTORY: -->

           <authentication mode="Forms"><forms name=".ASPXAUTH" timeout="240"
loginUrl="LoginActiveDirectory.aspx" path="/" slidingExpiration="true" /></authentication>
```

Non Active Directory Setting:

- Regular Forms Authentication using survey logins,
- Google federated login
- Middleware or Identity Server 3 login
- CAS login
- Automated 3rd party login
- Social Login (facebook, linked in, google, etc.)
- Azure

Active Directory Setting:

- Active Directory domain login using survey login page with domain drop down
- Active Directory NTLM/pass through login which authenticates to an Active Directory domain
- Azure Active Directory.

Step 2:

Add one admin user to your database.

Make sure nulls are allowed in the sur_user.password field.

Open the sur_user table and add a row with the AD username and AD password for the admin user. Then open sur_user_to_role_mapping table and add role 3 for that user. (use the existing admin user that is already in both

of these tables as an example but do not delete the admin user that is there) This is because the first time users login to the survey application with AD authentication, if the user is not already in the database, they will be set at the lowest permission level in the survey app which is “user” role, which they can only take surveys, not create them. So you need to set the one admin role so you can login with that to modify users that need admin or create roles later.

Open the sur_user table and make sure the “password” column allows null.

If this is not set you will get the error: Error:Field 'sur_user.user_password' cannot be a zero-length string when you attempt to login with AD.

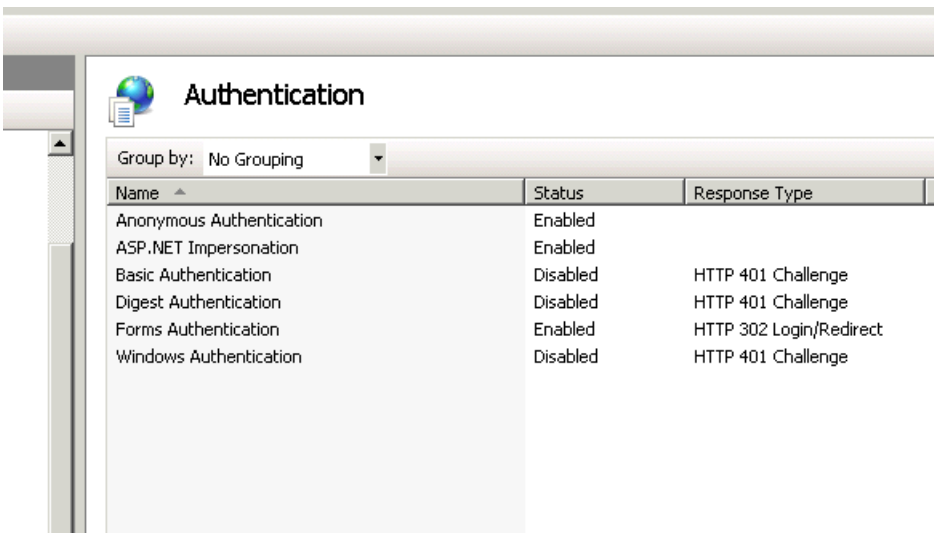
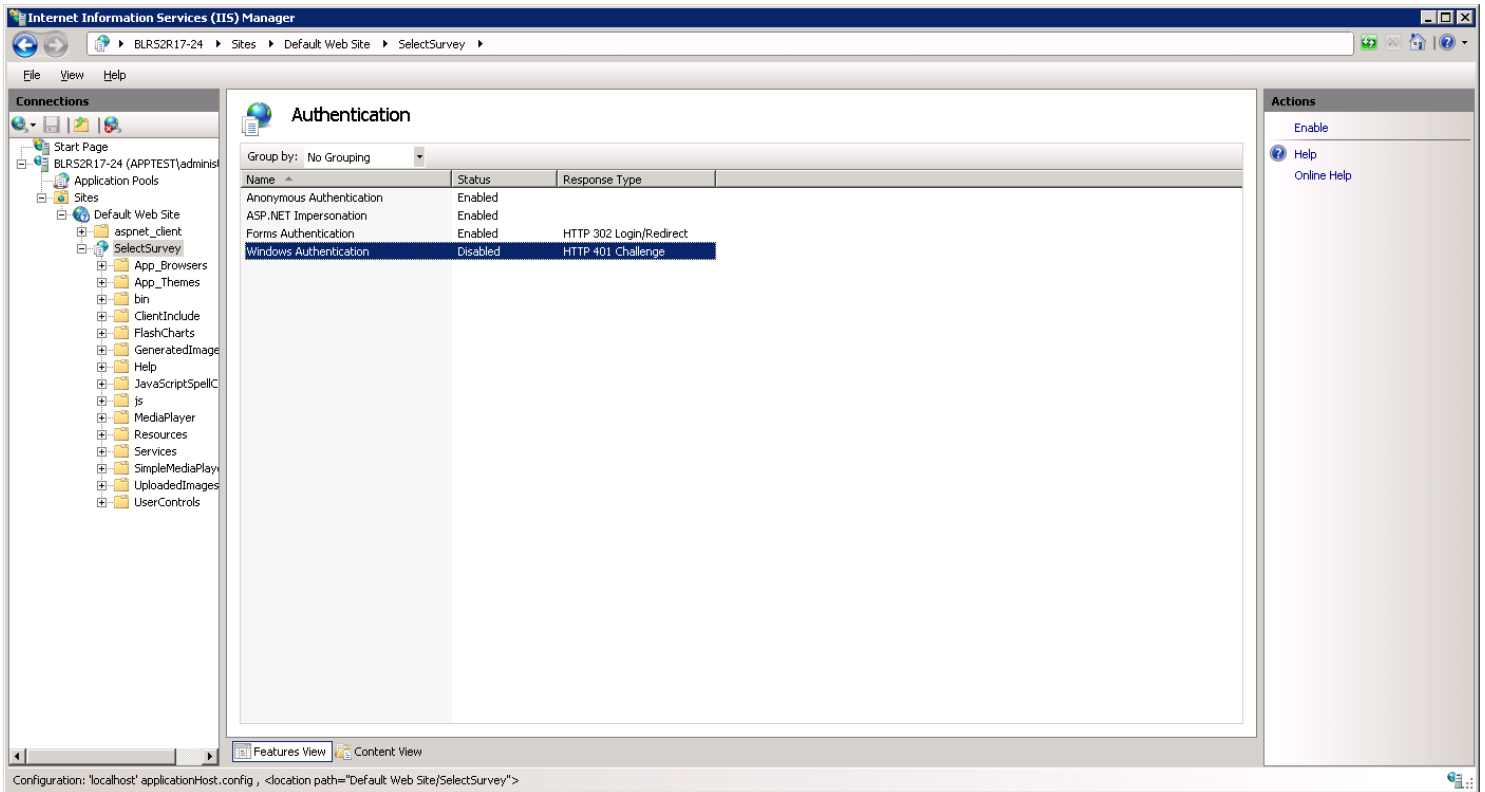
Step 3 IIS 6:

Configure AD permissions on web folder in IIS 7 (or higher):

Authentication tab in IIS 7:

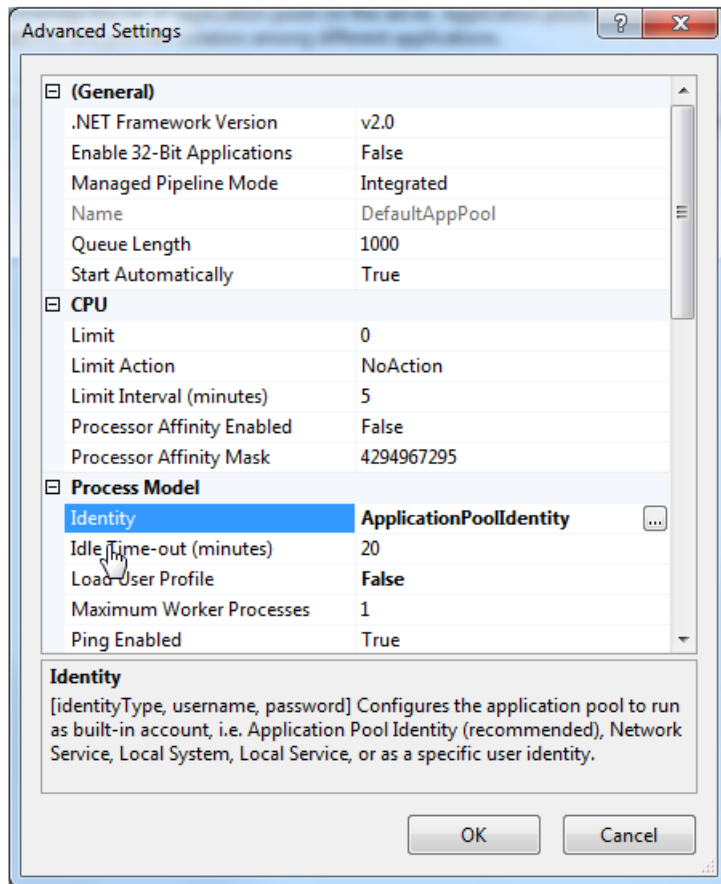
For Regular AD integration where it will display a login box the IIS 7 settings should look exactly like this screenshot:

- Anonymous is Enabled
- ASP.NET Impersonation is Enabled
- Forms Authentication is Enabled
- Windows Authentication is Disabled



IIS authentication screen should look exactly like this (unless you are using NTLM in which anonymous needs to be disabled):

If you cannot find the option for windows authentication in IIS, see below “Install Windows Authentication” sections.

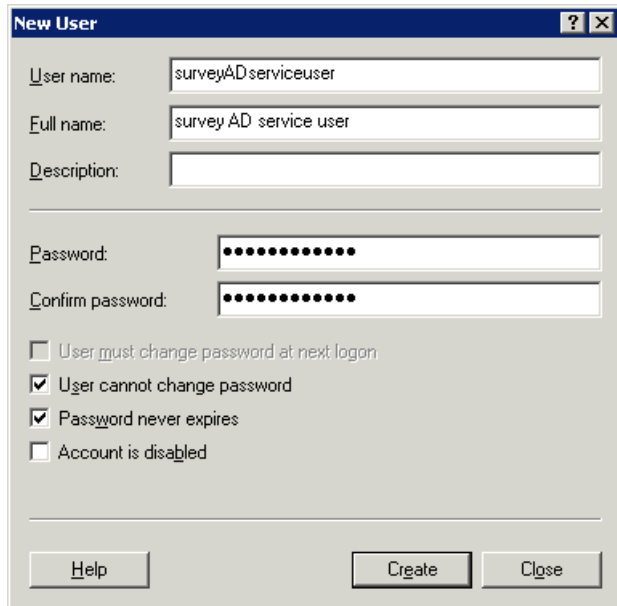


- Select the "Identity" list item and click the ellipsis (the button with the three dots).

Set the Process Model Identity to ApplicationPoolIdentity instead of Network Service.

Create an AD service user account:

When authenticating to single or multiple domains, create a user in all domains with the same username and password and also on the local IIS machine with the same username and password. In IIS set this user as the "anonymous IIS" user account.

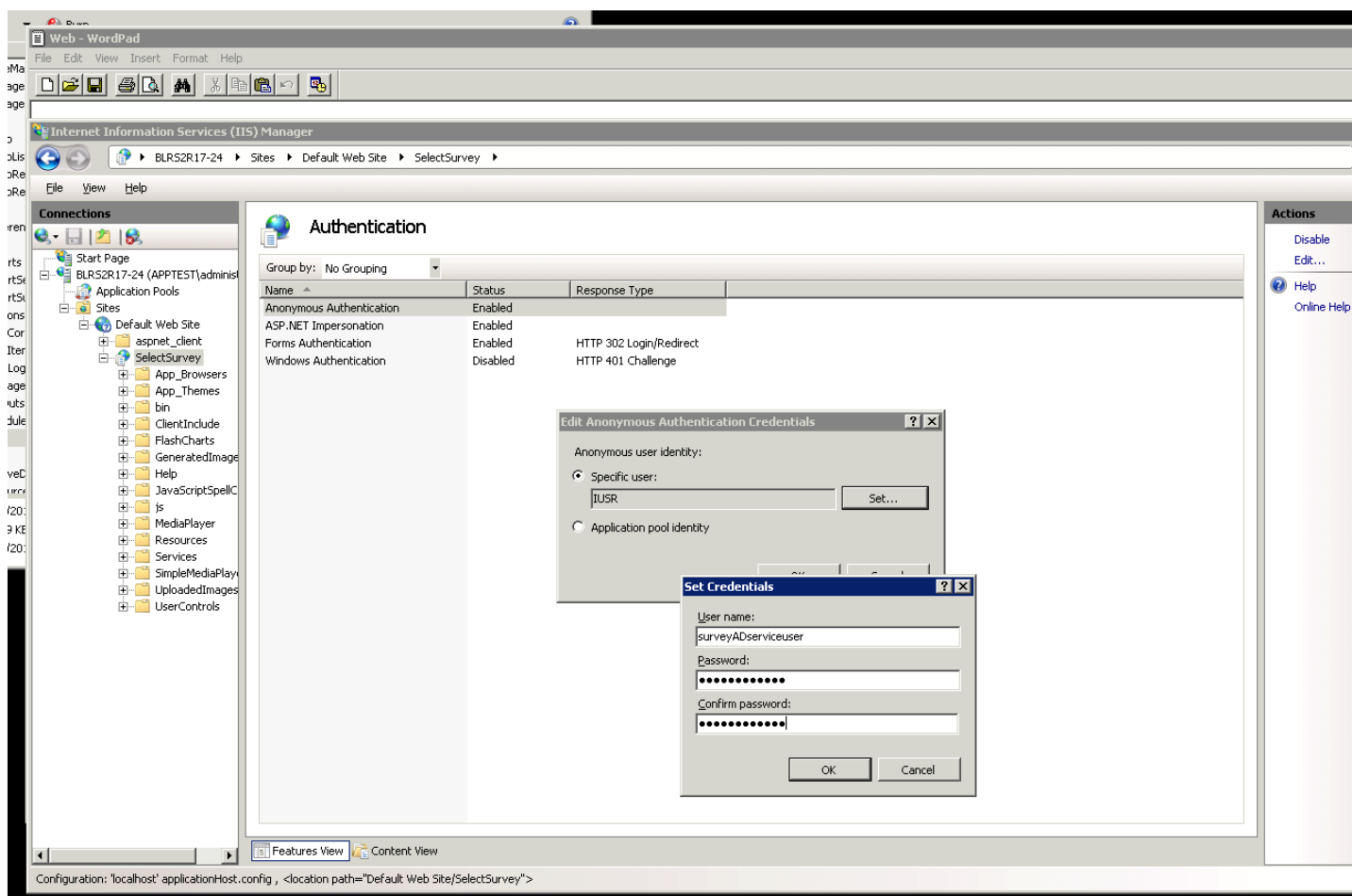


The image shows a 'New User' dialog box with the following fields and options:

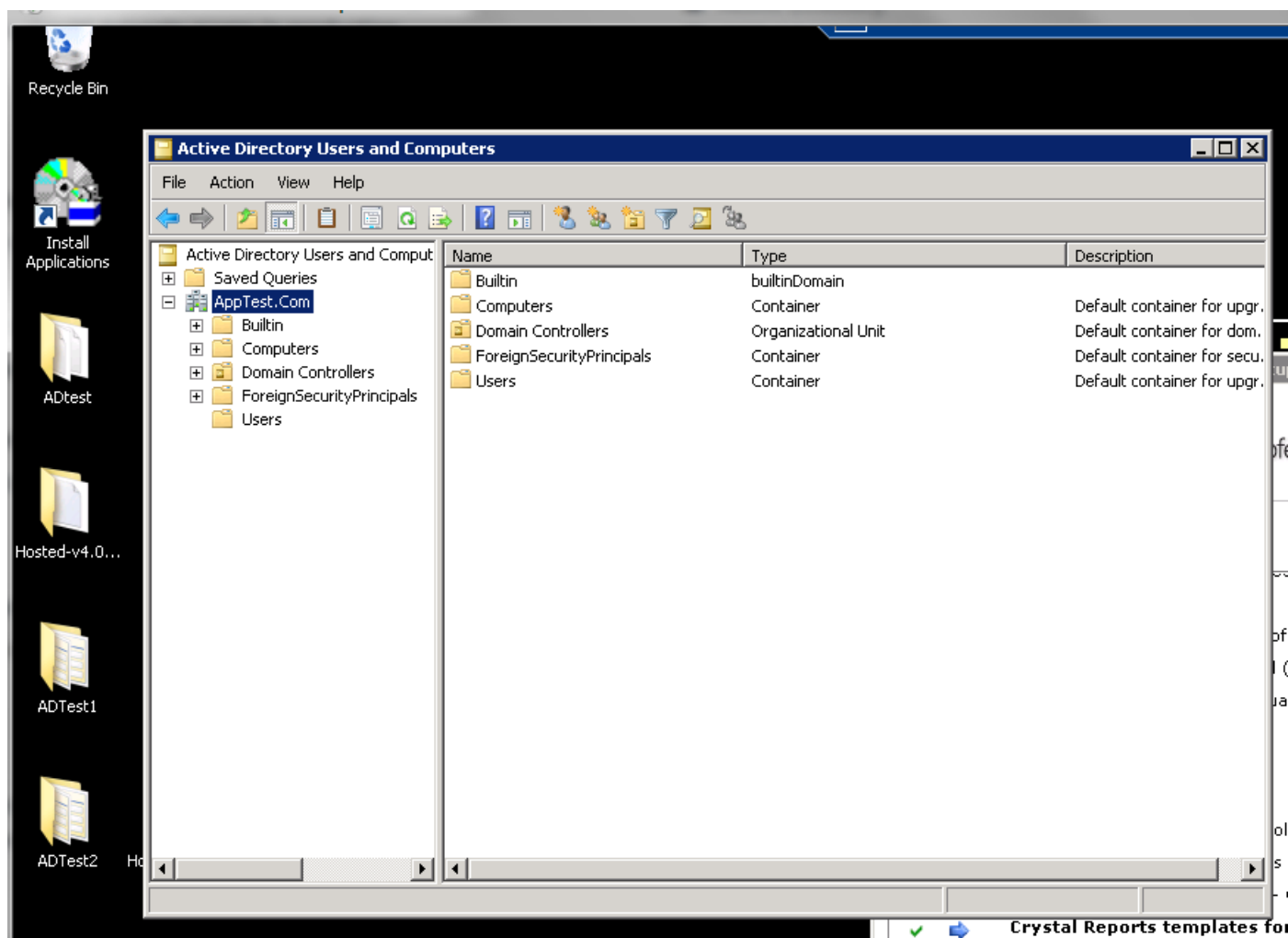
- User name:** surveyADserviceuser
- Full name:** survey AD service user
- Description:** (empty)
- Password:** (masked with dots)
- Confirm password:** (masked with dots)
- ☐ User must change password at next logon
- ☒ User cannot change password
- ☒ Password never expires
- ☐ Account is disabled

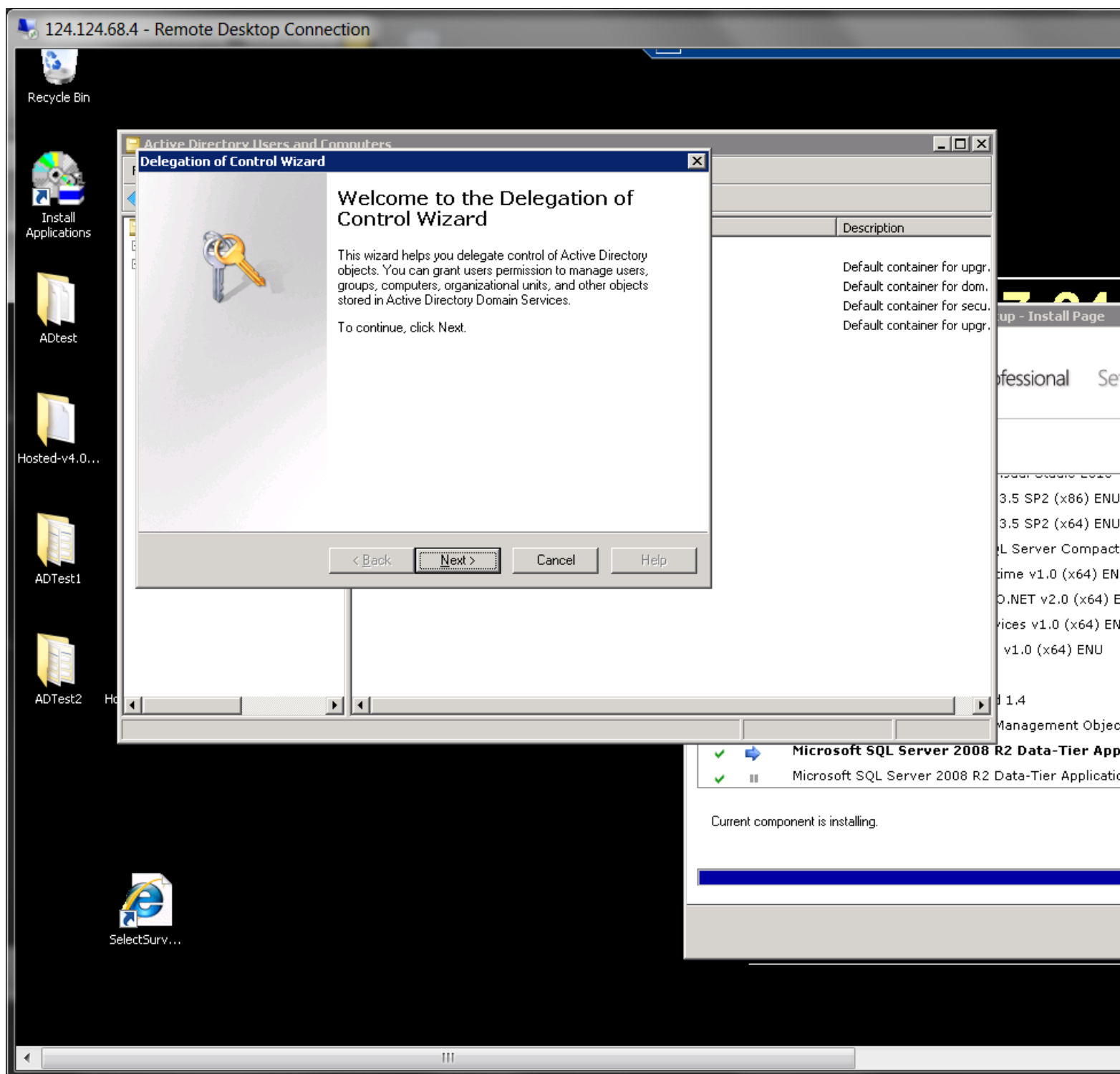
Buttons at the bottom: Help, Create, Close.

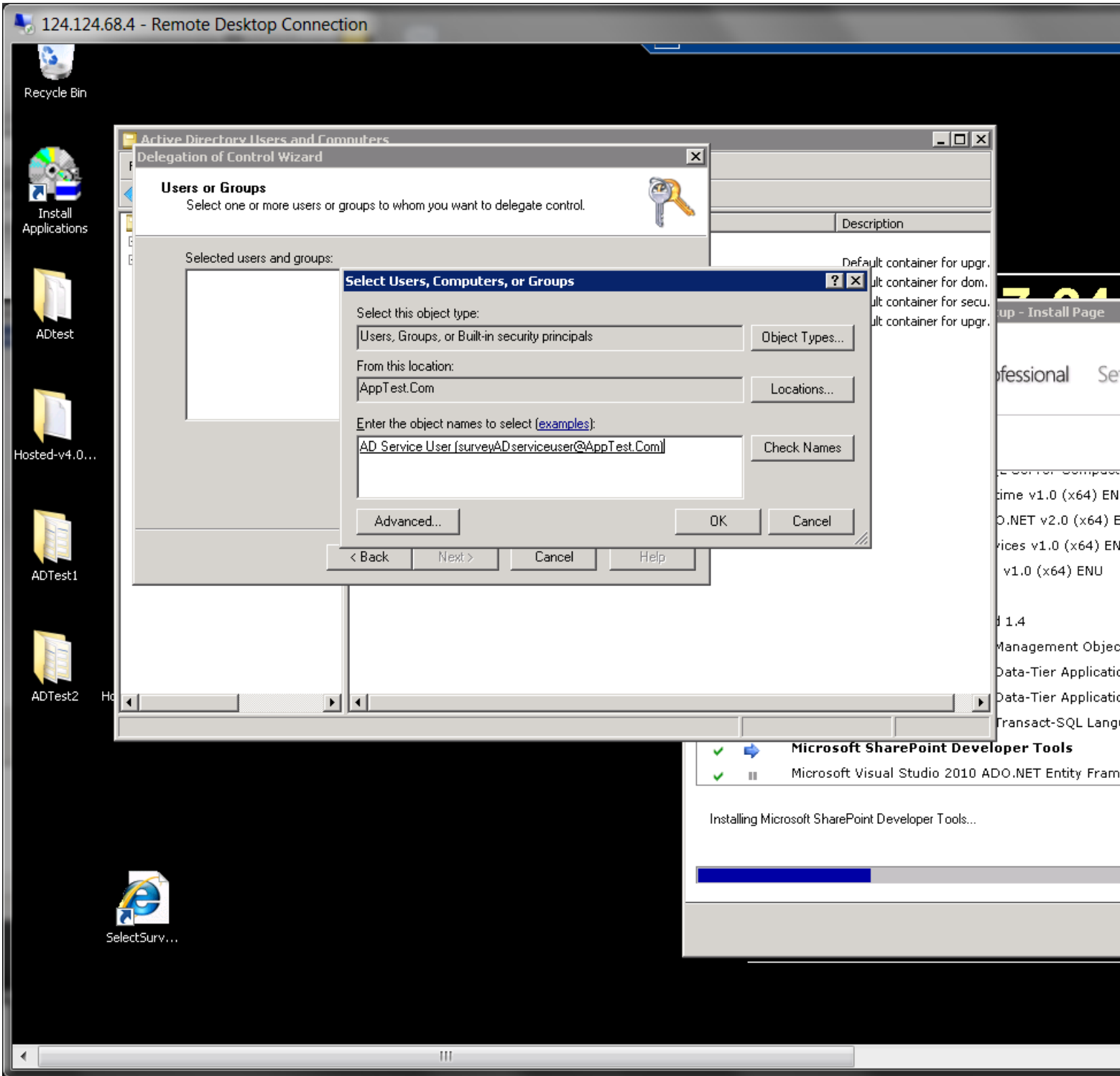
In IIS set this user as the “anonymous IIS” user account.

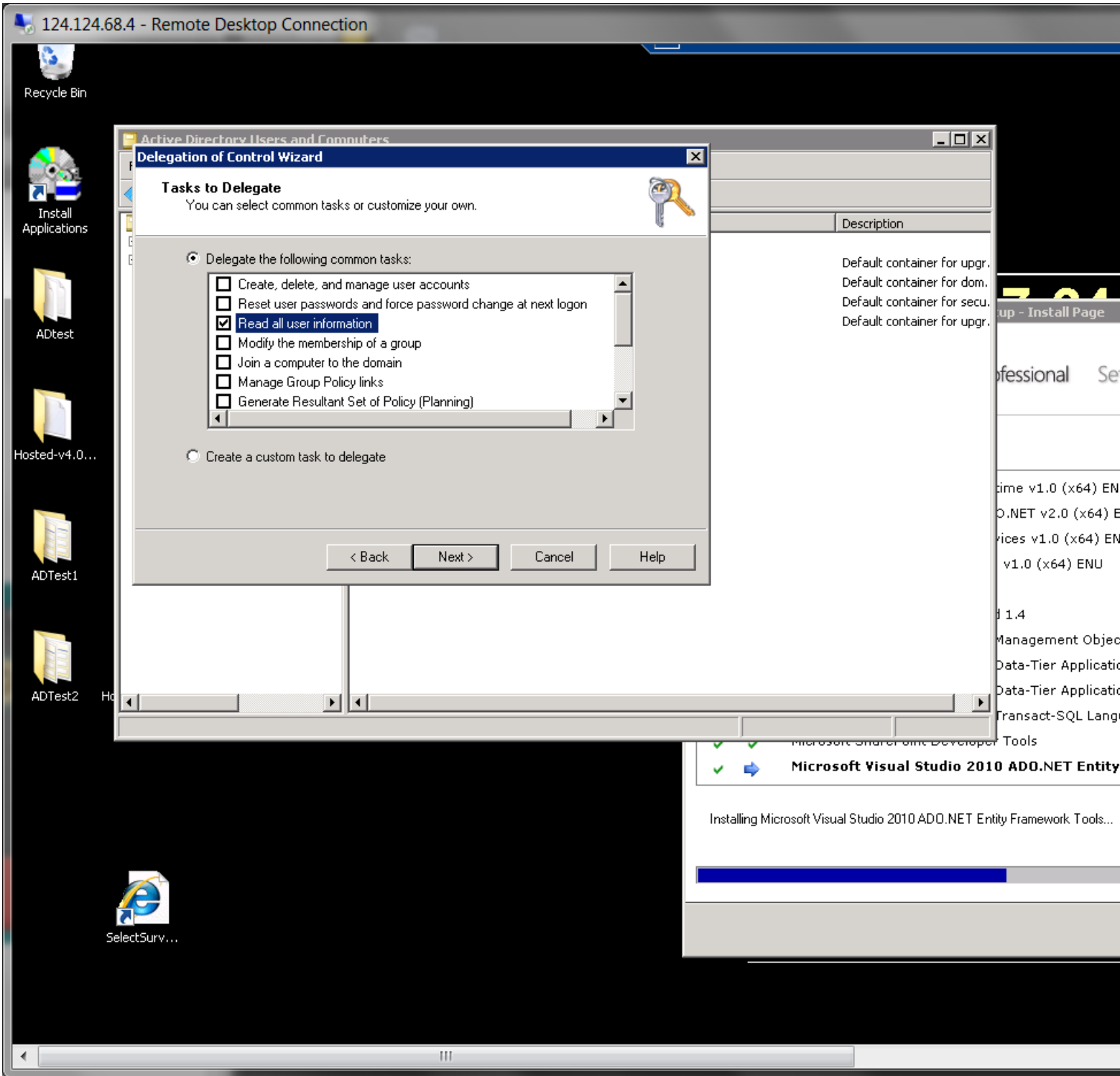


Delegate this user to “read all user info” in AD.

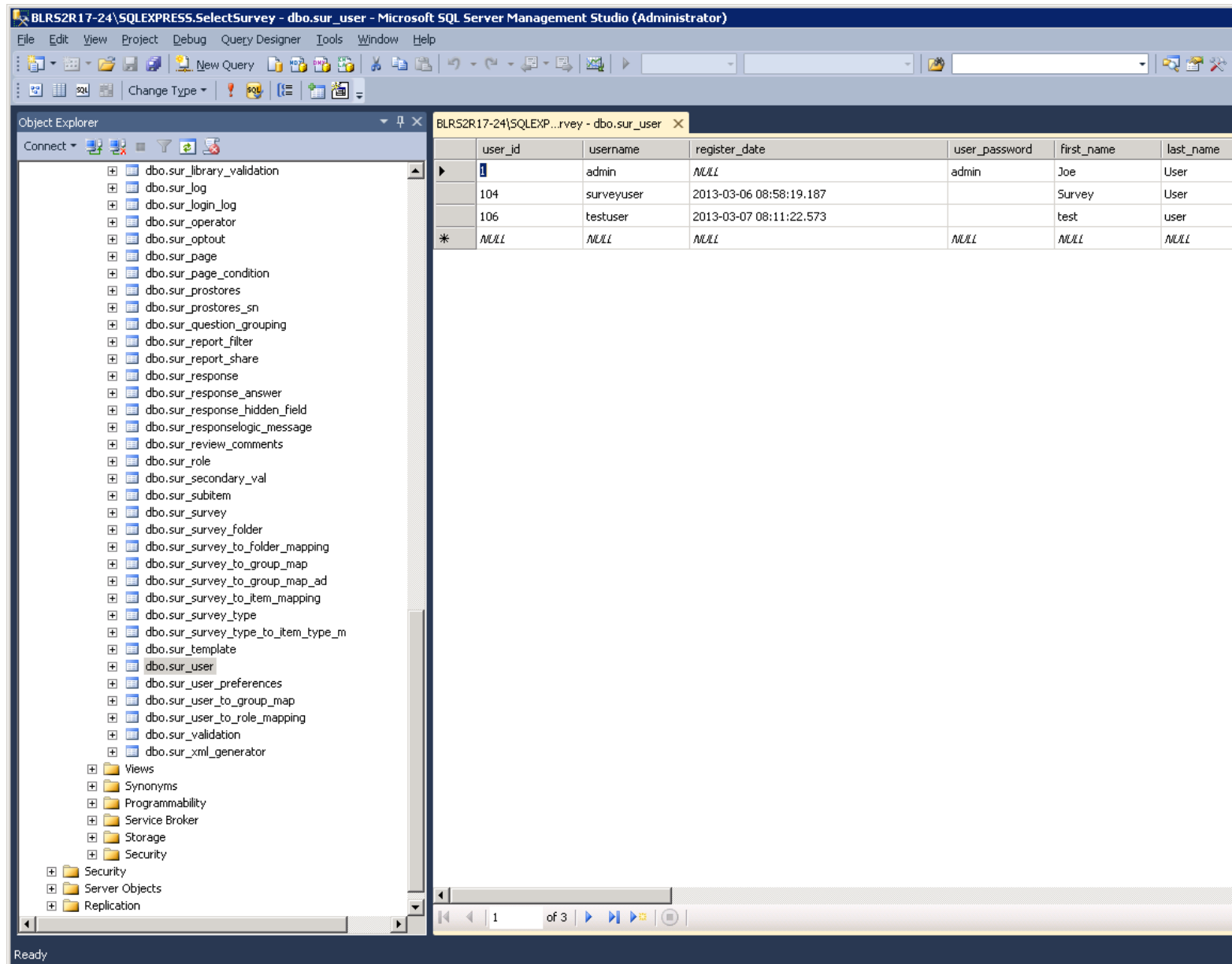








Now all domains users properties synch in SelectSurvey.NET when logging in from any trusted domain.



The screenshot shows the Microsoft SQL Server Management Studio interface. The Object Explorer on the left lists various database objects, including tables like dbo.sur_library_validation, dbo.sur_log, and dbo.sur_user. The main window displays the data for the dbo.sur_user table, which includes columns for user_id, username, register_date, user_password, first_name, and last_name. The data is as follows:

user_id	username	register_date	user_password	first_name	last_name
1	admin	NULL	admin	Joe	User
104	surveyuser	2013-03-06 08:58:19.187		Survey	User
106	testuser	2013-03-07 08:11:22.573		test	user
*	NULL	NULL	NULL	NULL	NULL

How the Active Directory Integration behaves:

When user logs in, their active directory info is automatically added to the sur_user table as the lowest role user (can take surveys).



This means there is no import necessary and nothing else required to synch the data between Active Directory and the survey app.

Each time the user logs in, the data is synched from the Active Directory data to the survey tables except for survey specific properties like survey role.

When survey role (user/create/admin) is edited in the survey app this will stay until edited from within the survey app.

User edit/delete in survey app does not edit or delete user in Active Directory.

How to enable NTLM for IIS 7:

When NTLM is enabled, users will not see the AD login page, but will be directed either into a survey or into the survey list page depending on their user role.

Make sure you do not use debug mode with the force NTLM passthrough authentication setting, as this would cause an infinite loop of redirects.

1. Set the NTLM specific settings in the web.config:

```
<!--If NTLM passthrough is activated the identity will be picked up by the browser (IE only) and the user will never see the login page. They will be automatically logged in with their network identity username in which all their survey activity will be stored. -->
```

```
<!-- valid values are "yes" and "no" -->
```

```
<add key="USE_NTLM_PASSTHROUGH_AUTHENTICATION" value="yes"/>
```

```
<!-- required for NTLM passthrough to work otherwise regular AD login will show -->
```

```
<add key="FORCE_NTLM_PASSTHROUGH_AUTHENTICATION" value="yes"/>
```

(lower portion below:)

```
<authorization>
```

```
    <allow users="*" />
```

```
</authorization>
```

```
<!--NTLM Integrated Windows Authentication -->
```

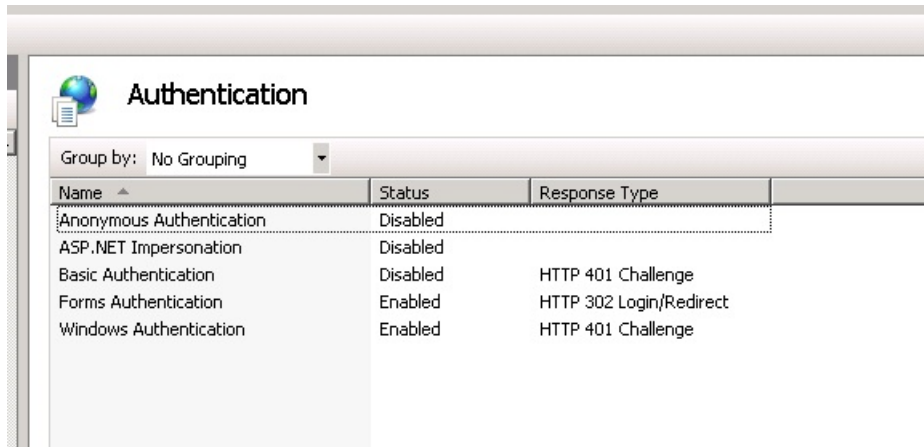
```
<identity impersonate="false" />
```

```
<authentication mode="Windows">
```

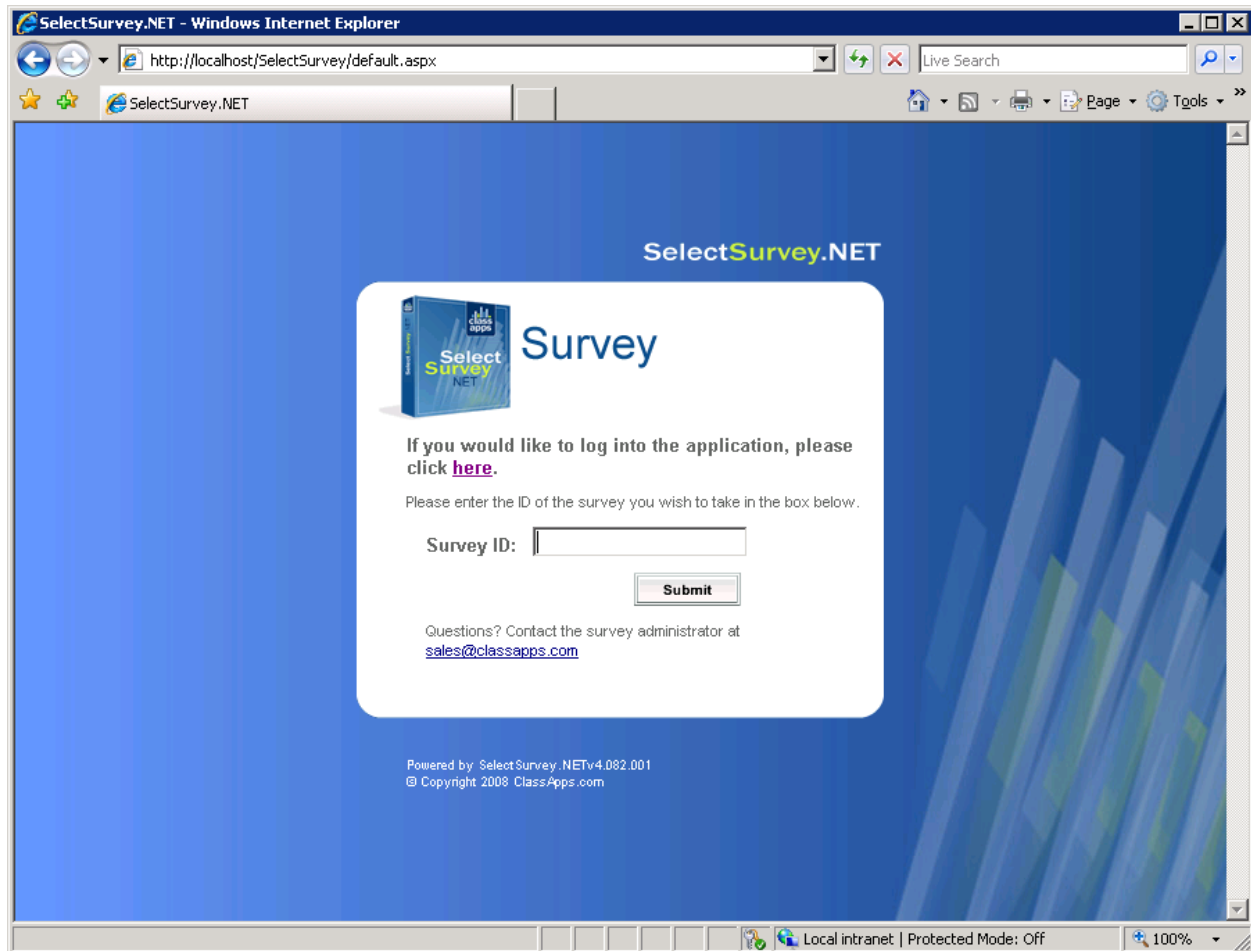
2. Set the Authentication in IIS:

NTLM requires that anonymous authentication be disabled in IIS, and windows authentication must be enabled with application user passthrough authentication set in IIS.

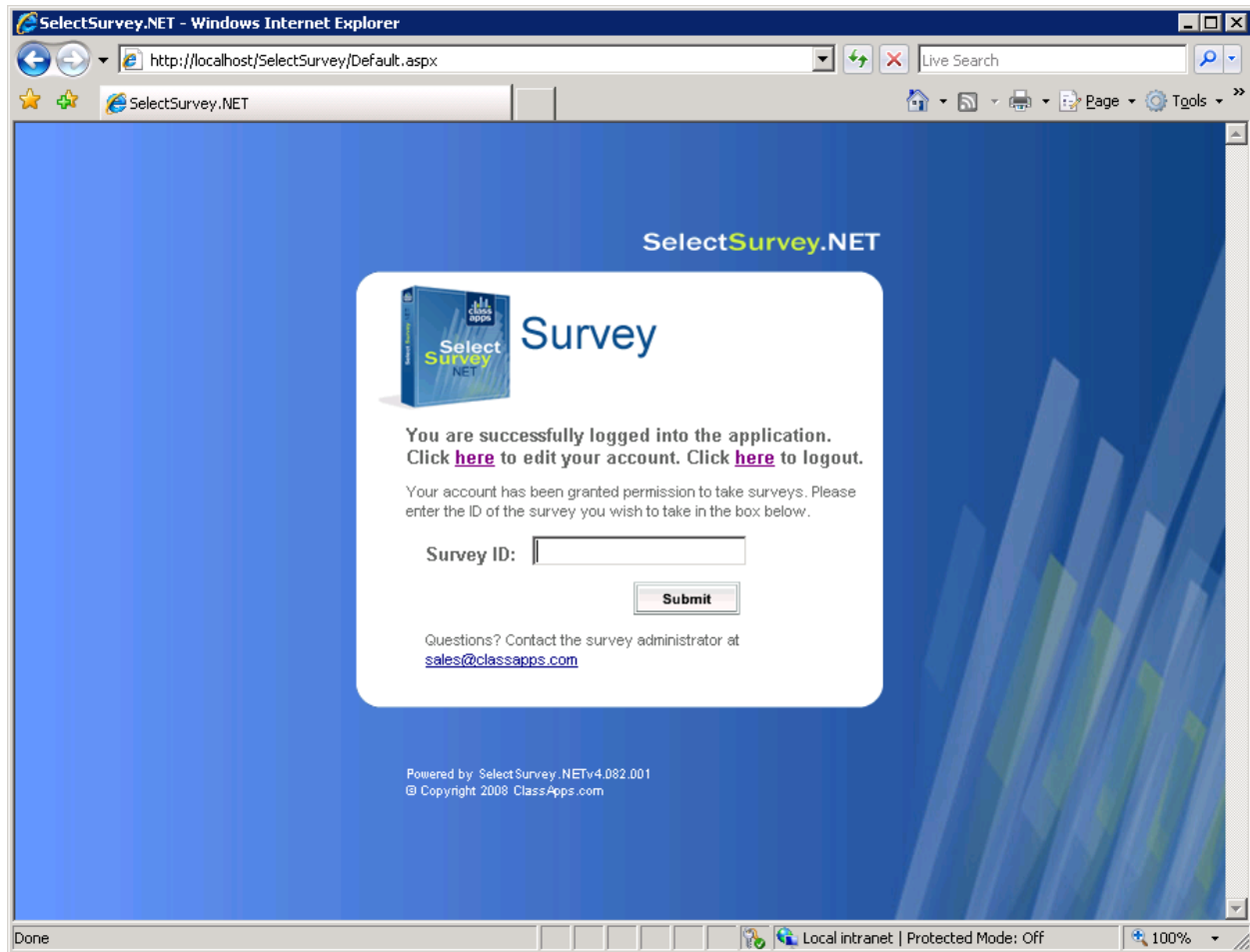
NTLM authentication should match the below screenshot exactly:



When clicking to login the user is redirected straight into the survey or into the survey list page depending on permissions.



Or if the user is user role 1, then they can only take surveys or logout.



The default installation of IIS 7 does not include the Windows authentication role service. To use Windows authentication on IIS, you must install the role service, disable Anonymous authentication for your Web site or application, and then enable Windows authentication for the site or application.

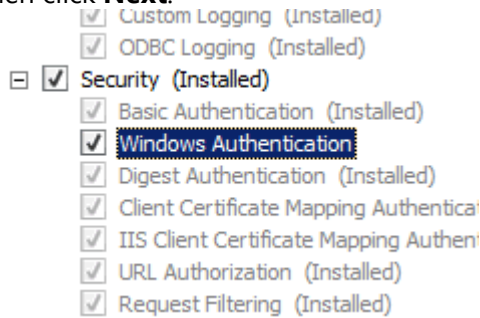
Note: After you install the role service, IIS 7 commits the following configuration settings to the ApplicationHost.config file.

```
<windowsAuthentication enabled="false" />
```

Windows Server 2008 or Windows Server 2008 R2 Install Windows Authentication

1. On the taskbar, click **Start**, point to **Administrative Tools**, and then click **Server Manager**.

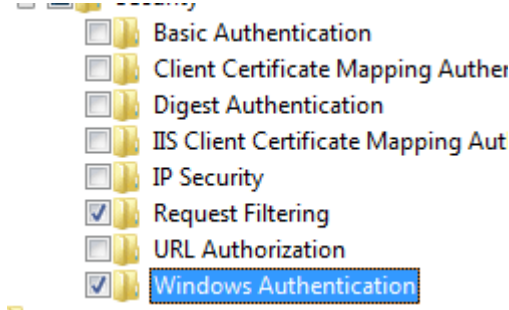
2. In the **Server Manager** hierarchy pane, expand **Roles**, and then click **Web Server (IIS)**.
3. In the **Web Server (IIS)** pane, scroll to the **Role Services** section, and then click **Add Role Services**.
4. On the **Select Role Services** page of the **Add Role Services Wizard**, select **Windows Authentication**, and then click **Next**.



5. On the **Confirm Installation Selections** page, click **Install**.
6. On the **Results** page, click **Close**.

Windows Vista or Windows Install Windows Authentication

1. On the taskbar, click **Start**, and then click **Control Panel**.
2. In **Control Panel**, click **Programs and Features**, and then click **Turn Windows Features on or off**.
3. Expand **Internet Information Services**, then **World Wide Web Services**, then **Security**.
4. Select **Windows Authentication**, and then click **OK**.

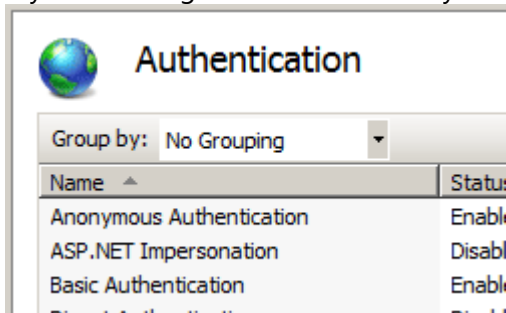


How to enable Windows authentication in IIS 7

1. Open **Internet Information Services (IIS) Manager**:
 - If you are using Windows Server 2008 or Windows Server 2008 R2:
 - On the taskbar, click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.

- If you are using Windows Vista or Windows 7:
 - On the taskbar, click **Start**, and then click **Control Panel**.
 - Double-click **Administrative Tools**, and then double-click **Internet Information Services (IIS) Manager**.
- 2. In the **Connections** pane, expand the server name, expand **Sites**, and then the site, application, or Web service for which you want to enable Windows authentication.
- 3. Scroll to the **Security** section in the **Home** pane, and then double-click **Authentication**.
- 4. In the **Authentication** pane, select **Windows Authentication**, and then click **Enable** in the **Actions** pane.

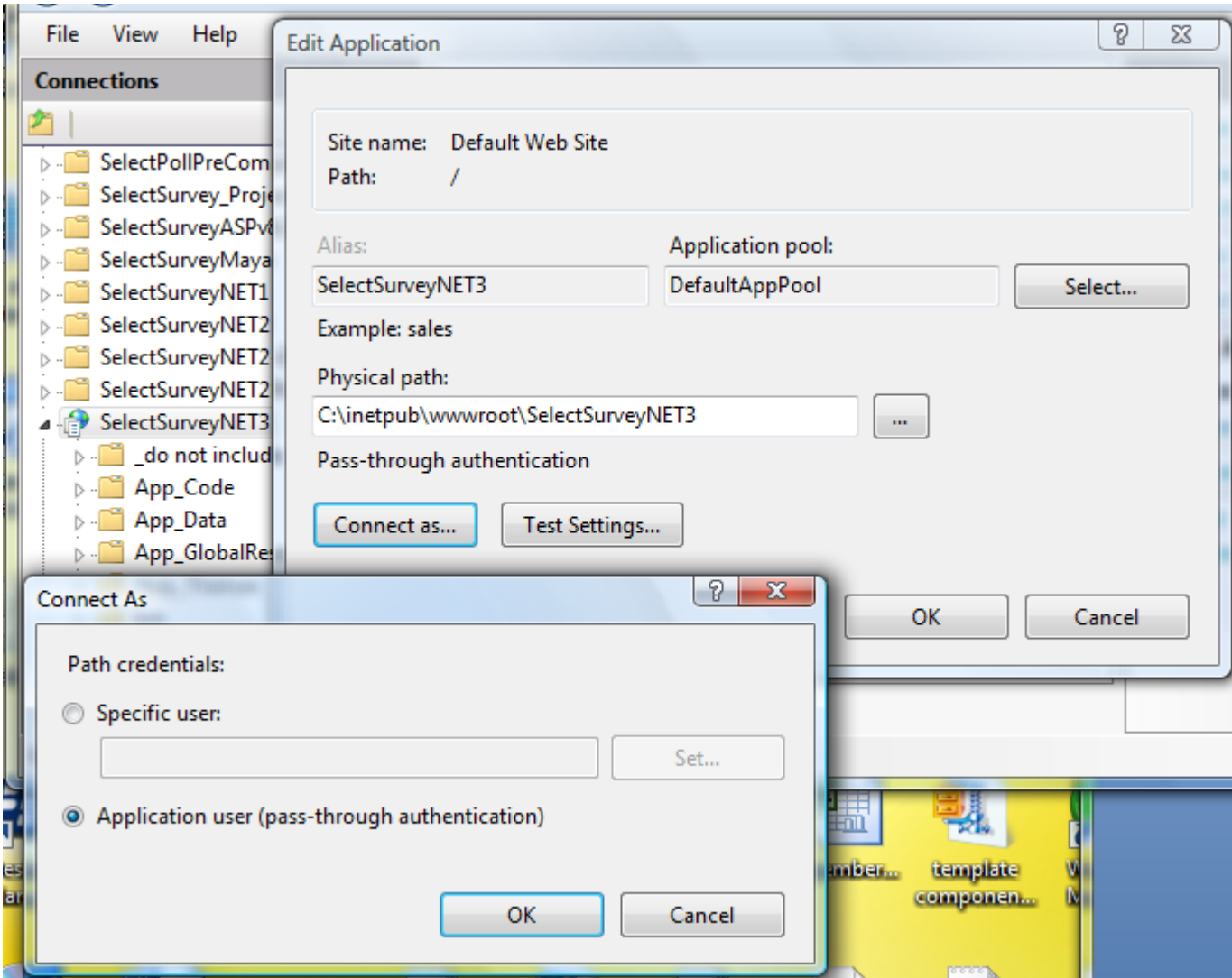
If you are using NTLM disable anonymous authentication, otherwise leave it enabled.



How to enable NTLM:

Disable anonymous authentication in IIS7 authentication screen for this web site.

Enable pass through authentication in IIS7 for this web site (see screenshot below).



(IIS 7)

Step 4:

Test.

How the Active Directory Integration behaves:

When user logs in, their active directory info is automatically added to the sur_user table as the lowest role user (can take surveys).

This means there is no import necessary and nothing else required to synch the data between Active Directory and the survey app.

Each time the user logs in, the data is synched from the Active Directory data to the survey tables except for survey specific properties like survey role.

When survey role (user/create/admin) is edited in the survey app this will stay until edited from within the survey app.

User edit/delete in survey app does not edit or delete user in Active Directory.

Browser NTLM Configuration: IE Browser

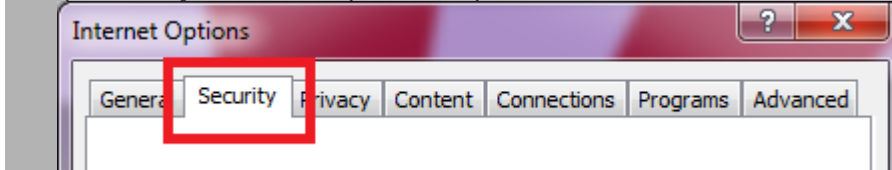
IE:

- 1) from IE browser select Tools menu, choose "Internet Options"
- 2) click the security tab
- 3) select the local intranet icon
- 4) click the "Sites" button
- 5) click the "Advanced " button
- 6) add your selectsurvey installation URL to the local intranet zone.
- 7) click the add button then click ok.

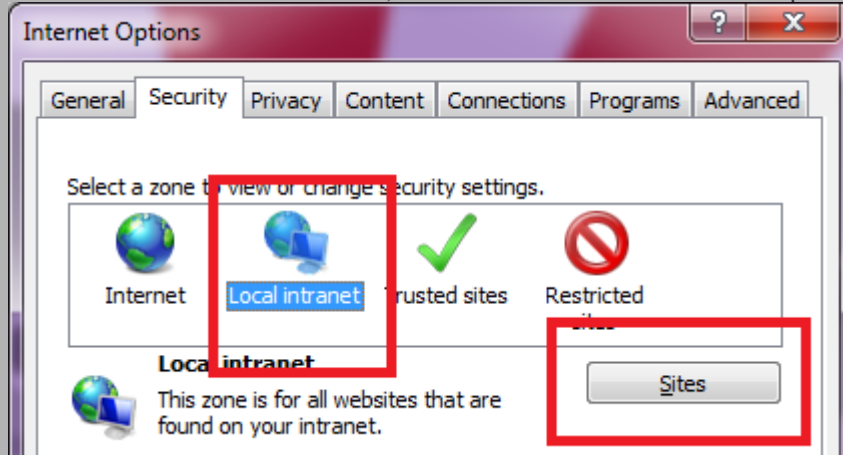
Internet Explorer Local Machine Trusted Sites Setup

So you may not have a domain, with an Active Directory Server to do your bidding. Don't worry though, as this is just as easy to setup on your local machine. If you're on a domain, you'll need to complete the following on your active directory server before skipping to the next section anyway.

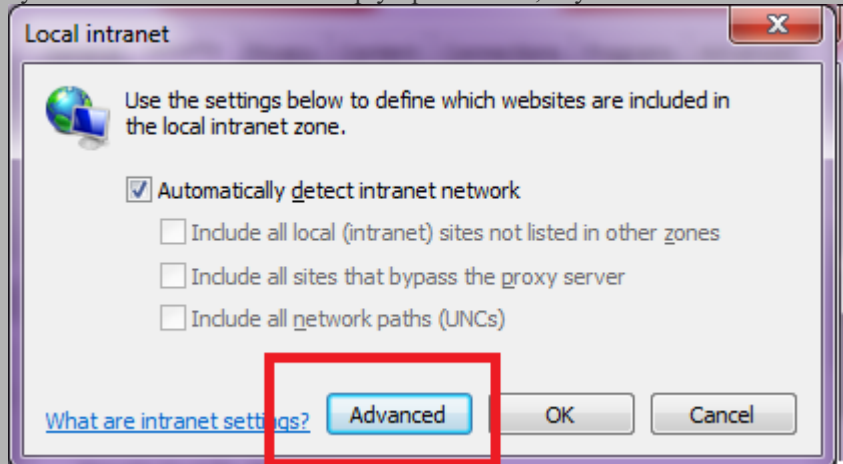
1. Open IE on your local computer and open **TOOLS > INTERNET OPTIONS**, then choose the Security tab up the top.



- Click on the 'Local Intranet' icon, and then click the **Sites** button to open the list of Trusted Sites for the Intranet zone.

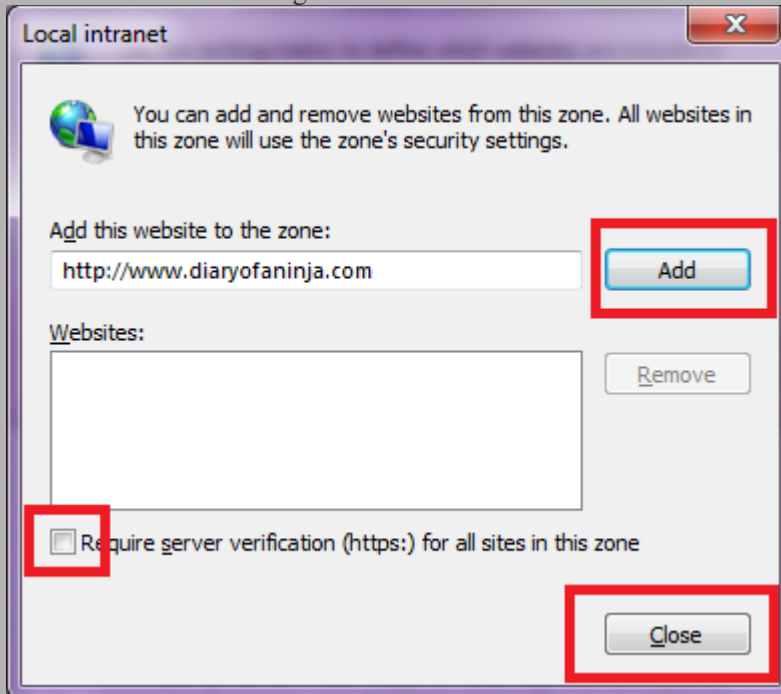


- If you're in IE 6-7 This will simply open the list, If you're in IE 8 it will show the window below. Click **Advanced**.

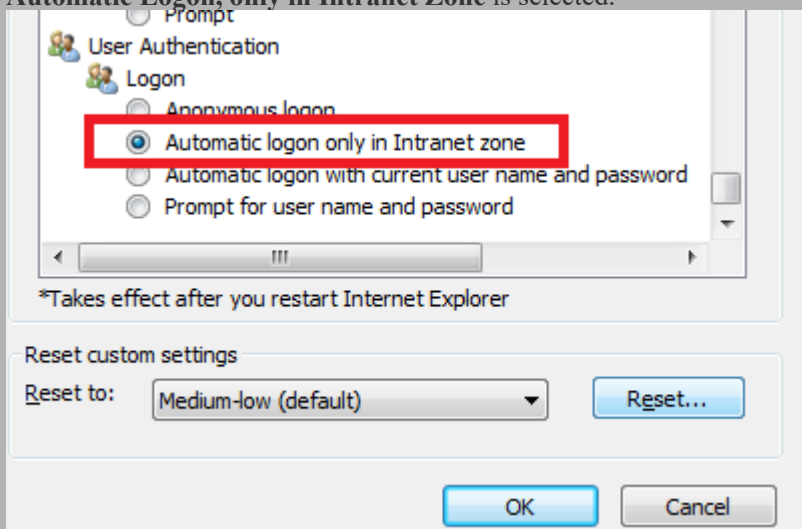


- If your site ASP.Net, SharePoint or TFS site is not on an HTTPS connection (*I'm assuming it isn't*) un-tick the box marked "Require secure connection", and then enter your site's address in the box. Then click **Add**. Do this for every site you

want to have automatic sign-on for and then click close



5. Now back at the main settings screen, make sure the intranet zone is still selected and click the **custom level** button. On the next screen scroll right to the bottom and make sure that under **User Authentication > Logon**, that the option **Automatic Logon, only in Intranet Zone** is selected.



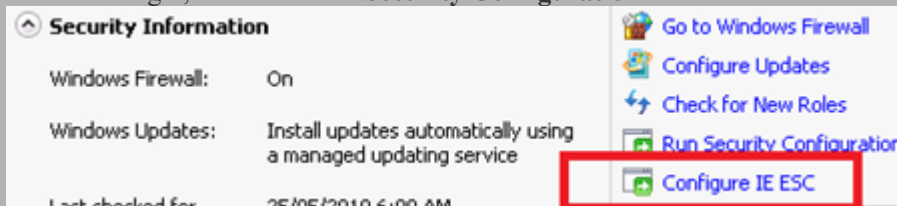
6. Close by clicking OK, and you're done!

Internet Explorer Domain Group Policy Trusted Sites Setup

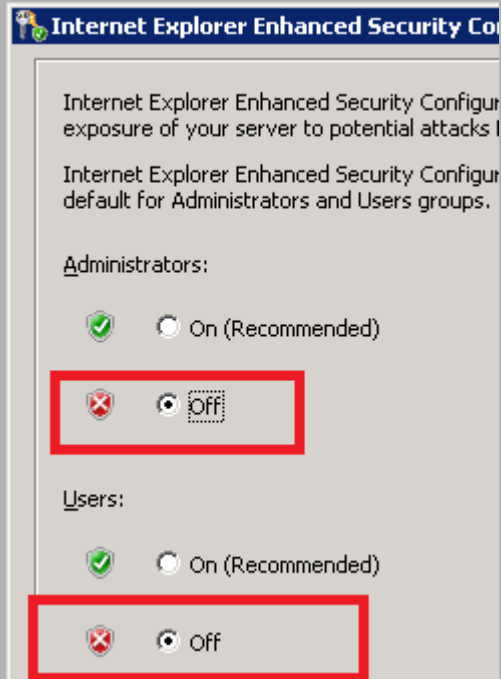
If you're on a domain, and want to allow all your users to have automatic sign-on, Group Policy is your friend. If you don't you're already done.

1. Login to your Active Directory Domain Controller, using a domain admin account, and perform the steps listed above to setup the local Internet Explorer settings on the server. You will want to repeat the following for two separate policies. One with Enhanced Security Configuration turned on, and one with it turned off, so that you can support workstations with both configuration.

2. To turn off Internet Explorer Enhanced Security Configuration on a Windows 2008 server do the following. Open up Server manager, scroll down to **Security Configuration** and click the link that says **Configure IE ESC**

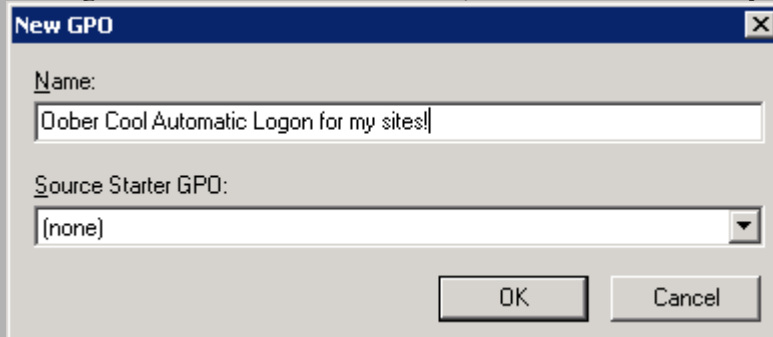


3. Turn it off for **Administrators** and close the window



4. Open up **Group Policy Management**

5. Right-click your domain name (or whichever OU contains the users you wish to apply this to), and create a new Policy by clicking “**Create a GPO in this domain, and link it here**”. Give your new policy a name (preferably better than mine)

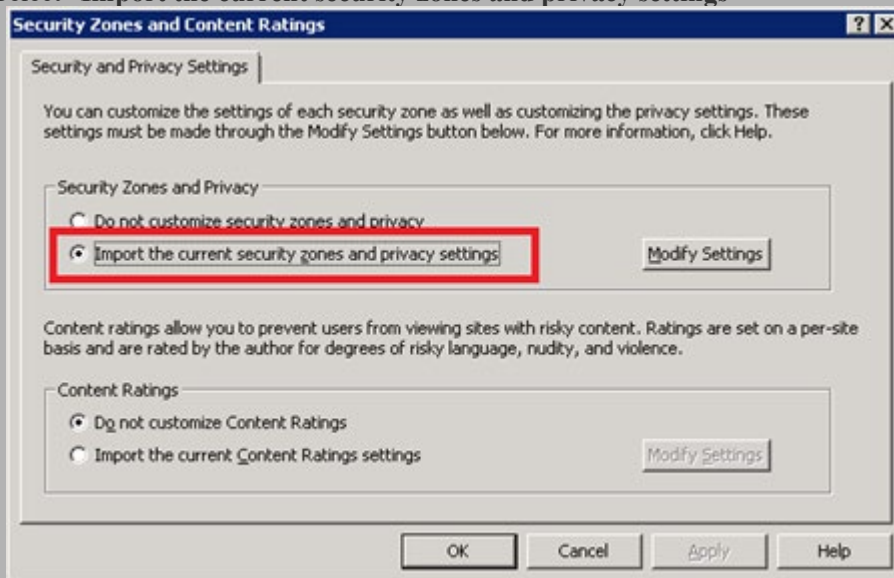


The 'New GPO' dialog box has a title bar with a close button. It contains two text input fields. The first is labeled 'Name:' and contains the text 'Dober Cool Automatic Logon for my sites!'. The second is labeled 'Source Starter GPO:' and has a dropdown menu currently showing '(none)'. At the bottom right are 'OK' and 'Cancel' buttons.

6. Right click on your newly created policy and select **Edit**

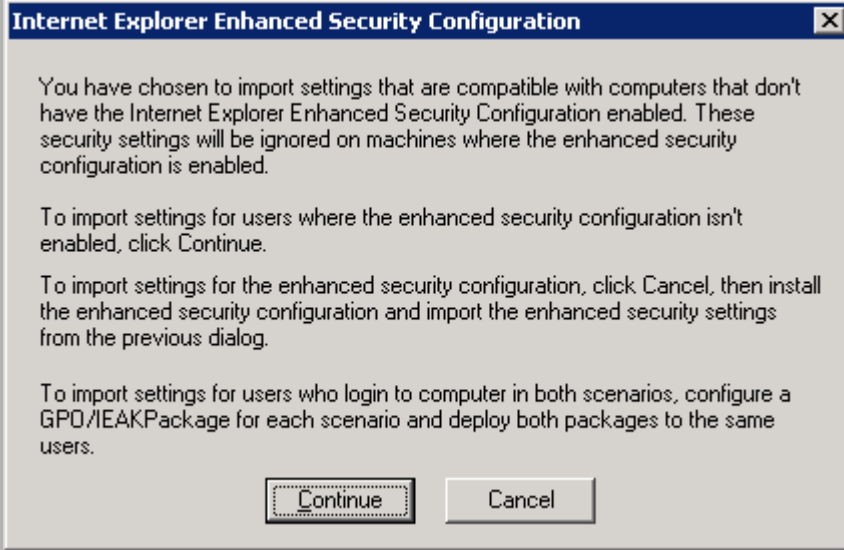
7. Open down to **User Configuration > Policies > Windows Settings > Internet Explorer Maintenance > Security > Security Zones and Content Ratings**

8. Select “**Import the current security zones and privacy settings**”



The 'Security Zones and Content Ratings' dialog box has a title bar with a help button and a close button. It features a tab labeled 'Security and Privacy Settings'. Below the tab is a text block explaining that settings must be made through the 'Modify Settings' button. There are two main sections: 'Security Zones and Privacy' and 'Content Ratings'. In the 'Security Zones and Privacy' section, the radio button for 'Import the current security zones and privacy settings' is selected and highlighted with a red rectangle; a 'Modify Settings' button is to its right. In the 'Content Ratings' section, the radio button for 'Do not customize Content Ratings' is selected, with a 'Modify Settings' button to its right. At the bottom are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

9. When you select this option you will probably receive a warning about ‘Internet Explorer Enhanced Security Configuration’.



This is why we disabled the enhanced configuration in step 3, so that this policy will apply to workstations without Enhanced security turned on. Click **Continue**.

10. Close all open windows.

The changes will take time to replicate through your AD topology, depending on your setup. You may see the changes take effect within 15 mins to an hour. If you have a Multi-site AD setup it may take a day or two.

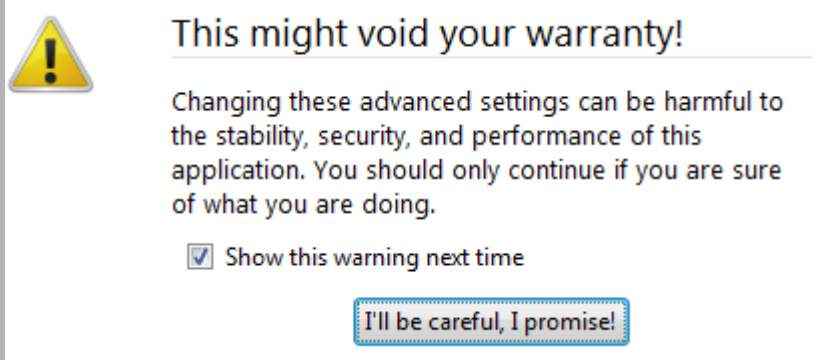
Browser NTLM Configuration: Firefox Browser

Firefox:

About > Config

network.automatic-ntlm-auth.trusted-urls Value: SurveyServername

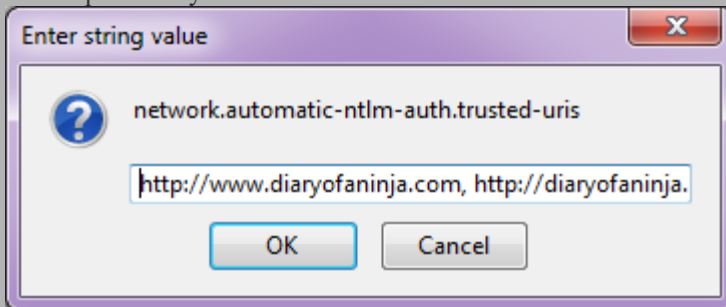
1. Open FireFox and type **about:config** in the address bar. Click **I'll be careful, I promise!** to the warning and you'll open the FireFox advanced configuration page.



2. Search for **ntlm** by typing it into the filter box.
3. Select the option **network.ntlm.send-lm-response** and double click it to toggle it to **on**

Filter: ntlm				
Preference Name	Status	Type	Value	
network.auth.force-generic-ntlm	default	boolean	false	
network.automatic-ntlm-auth.allow-proxies	default	boolean	true	
network.automatic-ntlm-auth.trusted-uris	default	string		
network.ntlm.send-lm-response	default	boolean	false	

4. Next double click the item marked **network.automatic-ntlm-auth.trusted-uris** in the next box enter each URL of your sites seperated by a comma – click OK



5. Close the tab and you're done!

Firefox Domain Group Policy Trusted Sites Setup

Firefox is Mozilla's beast, and therefore what they say and do goes in the world of FireFox. Sadly this means that there is no clear cut way to setup group policy's for FireFox.

Click the link to go to the selectsurvey login.aspx page and the page will never show you will automatically be logged in and forwarded to the survey list page, or if a user, to the survey.

Mapping AD User Fields to SUR_USER Survey User Fields

SelectSurvey.NET has a built in capability of mapping custom fields from AD to the Survey User. To access this feature, login as admin user, then click "Admin Tools", "ActiveDirectory User Map". See the screenshots below for an idea of the fields that you can map between AD and Survey.



- Dashboard
- Workspace
- Help
- Surveys
- Survey Folders
- Libraries
- Templates
- Email Lists
- Reports
- Users
- Admin Tools
- Account Usage
- Client Portal

ActiveDirectory User Property Mapping

This page is for administrators to map AD properties to survey user fields. When mapping is set, the AD properties will overwrite the survey user properties

Enter the proper AD property for each survey user field. CASE SENSITIVE! Then click save at bottom of page.

Survey User Field

Username (sur_user.username)

Username (sur_user.username)

Username (sur_user.username)

Username (sur_user.username)

Register Date (sur_user.register_date)

User Password (sur_user.password)

Password Hint (sur_user.password_hint)

First Name (sur_user.first_name)

Last Name (sur_user.last_name)

Email Address (sur_user.email_address)

Current Position (sur_user.current_position)

Company (sur_user.company)

Location (sur_user.location)

Custom Data 1 (sur_user.custom_data_1)

Custom Data 2 (sur_user.custom_data_2)

Custom Data 3 (sur_user.custom_data_3)

Custom Data 4 (sur_user.custom_data_4)

ActiveDirectory User Property

SAMAccountName (Default AD setting)

userPrincipalName (Default AD setting if 1st returns null)

HttpContext.Current.User.Identity.Name (Default NTLM setting)

Request.ServerVariables["LOGON_USER"] (Default NTLM setting if 1st returns null)

n/a (User registration feature is not used with AD)

n/a (User password is not stored with AD integration)

n/a (Password hint is not used with AD integration)

givenName

search.PropertiesToLoad.Add("givenName")

sn

search.PropertiesToLoad.Add("sn")

mail

search.PropertiesToLoad.Add("mail")

Title

company

search.PropertiesToLoad.Add("company")

StreetAddress

search.PropertiesToLoad.Add("StreetAddress")

Appendix D: Common Errors/Solutions

Below are some common errors and how to resolve them.

There is a variable in web.config "Show admin tools" yes/no. When this is set to yes, a tool icon will display in the upper right corner of application when logged in as admin user. Click the tool icon, then there is a variety of admin tools to help with install and configuration.

Error: Ambiguous match found.

Solution: You are using the wrong version of the .net framework, right click the web site folder in iis and check on the .net framework tab to make sure it is pointing to the correct version 3.5 of the .net framework.

Error: Database error.

Solution: Click browse in IIS on the server to see if there is an error connecting to the database. If the login page comes up and is functioning, then normally this means everything is working. If you get an error, then check the web.config connection string for typos, and check the security of the SQL user to make sure the user is database owner of your survey database and archive database.

Error: Object reference not set to an instance of an object.trace: at
SelectSurveyNET.SurveyListPage.Page_Load

Solution 1: Make sure you have upgraded your database to add new columns. See releasenotes.txt in the upgrade zip file, check all database changes from version you were using, to new version.

Solution 2: If you are running the application on a sharepoint server, you need to add variables to the web.config so that login authentication will retain user.context.

Sharepoint variables: (add to system.web section in web.config.)

```
<trust level="Full" originUrl="" />

<httpHandlers>

    <add verb="*" path="*.aspx" type="System.Web.UI.PageHandlerFactory, System.Web,
Version=1.0.5000.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />

</httpHandlers>

<httpModules>
```

```
<add name="Session" type="System.Web.SessionState.SessionStateModule"/>

<add name="FormsAuthentication" type="System.Web.Security.FormsAuthenticationModule"/>

<add name="PassportAuthentication"
type="System.Web.Security.PassportAuthenticationModule"/>

<add name="UrlAuthorization" type="System.Web.Security.UrlAuthorizationModule"/>

<add name="FileAuthorization" type="System.Web.Security.FileAuthorizationModule"/>

</httpModules>

<pages enableSessionState="true" enableViewState="true" enableViewStateMac="true"
validateRequest="false"/>
```

Appendix E: Preferred Hosting Providers

Hosting provider must allow control panel ability to add asp.net application folder. If they don't, then you will most likely have to create a support ticket to wait for them to add it for you.

The below hosting providers have asp.net permissions and asp.net application folders that you can configure through the control panel: (this is not a complete list)

Intermedia.net

Godaddy.com

Appendix F: Windows Sharepoint Services

Hosting the survey application on a server that has Microsoft Sharepoint Services installed will require some tweaking for security to work.

Sharepoint security will over-ride security to the Survey application (or any other 3rd party application) without following the below steps:

(The below is an excerpt from <http://support.microsoft.com/kb/828810>)

Add Sharepoint information to Select Survey web.config:

You'll have to both add an excluded path and clear out the HTTP handlers in

web.config. In your web.config file, add these directives immediately after

<system.web>.

Example 1: (default)

```
<!--SHAREPOINT START:  DEFAULT SHAREPOINT ADDITIONS -->

<trust level="Full" originUrl="" />

<httpHandlers>

<add verb="*" path="*.aspx" type="System.Web.UI.PageHandlerFactory, System.Web,
Version=1.0.5000.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />

</httpHandlers>

<pages enableSessionState="true" enableViewState="true" enableViewStateMac="true"
validateRequest="false"/>

<!--SHAREPOINT END -->
```

Here is another example of a more complicated sharepoint addition to the survey web.config (add directly under system.web section in web.config):

Example 2: (complex)

```
<!--SHAREPOINT START -->

<trust level="Full" originUrl="" />

<httpHandlers>

<add verb="*" path="*.aspx" type="System.Web.UI.PageHandlerFactory, System.Web,
Version=1.0.5000.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />

</httpHandlers>

<httpModules>

<add name="Session" type="System.Web.SessionState.SessionStateModule"/>

<add name="FormsAuthentication" type="System.Web.Security.FormsAuthenticationModule"/>

<add name="PassportAuthentication"
type="System.Web.Security.PassportAuthenticationModule"/>

<add name="UrlAuthorization" type="System.Web.Security.UrlAuthorizationModule"/>
```

```
<add name="FileAuthorization" type="System.Web.Security.FileAuthorizationModule"/>

</httpModules>

<pages enableSessionState="true" enableViewState="true" enableViewStateMac="true"
validateRequest="false"/>

<!--SHAREPOINT END -->
```

You can also find more information on google groups and the Microsoft support site.

Appendix G: Web Farm Configuration

SelectSurvey.NET can be configured for web farms or web gardens by following the instructions below to make a simple change to the web.config file. ASP.NET session state lets you share session data user-specific state values across all machines in your Web farm. Now a user can hit different servers in the web farm over multiple requests and still have full access to her session.

The default setting for session state in the SelectSurvey.NET web.config is “inProc” session state because its performance is faster than all the different types of session states. For SelectSurvey.NET to run without session errors on a web farm or web garden scenario, the session state must be changed from “inProc” to “StateServer” in the web.config as described below:

To configure an ASP.NET application to use **StateServer** mode, in the application's Web.config file do the following:

- Set the **mode** attribute of the [sessionState](#) element to **StateServer**.
- Set the **stateConnectionString** attribute to **tcpip=serverName:42424**.

The following example shows a configuration setting for **StateServer** mode where session state is stored on a remote computer named `SampleStateServer`:

```
<configuration>
  <system.web>
    <sessionState mode="StateServer"
      stateConnectionString="tcpip=SampleStateServer:42424"
      cookieless="false"
      timeout="20"/>
  </system.web>
</configuration>
```

Read the items below concerning proper setup of the servers on the webfarm.

StateServer

- - In a web farm, make sure you have the same <machineKey> in all your web servers. See [KB 313091](#) on how to do it.
- - Also, make sure your objects are serializable. See [KB 312112](#) for details.
- - For session state to be maintained across different web servers in the web farm, the Application Path of the website (For example \LM\W3SVC\2) in the IIS Metabase should be identical in all the web servers in the web farm. See [KB 325056](#) for details

Additional information on Microsoft.com:

More information can be found here: <http://www.eggheadcafe.com/articles/20021016.asp>

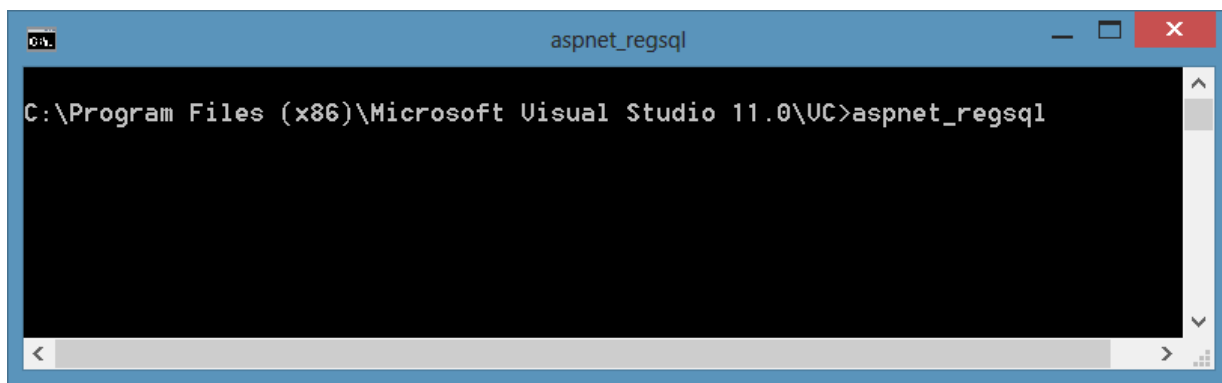
Web-Farm Session State ASP.NET session state lets you share session data user-specific state values across all machines in your Web farm. Now a user can hit different servers in the web farm over multiple requests and still have full access to her session.

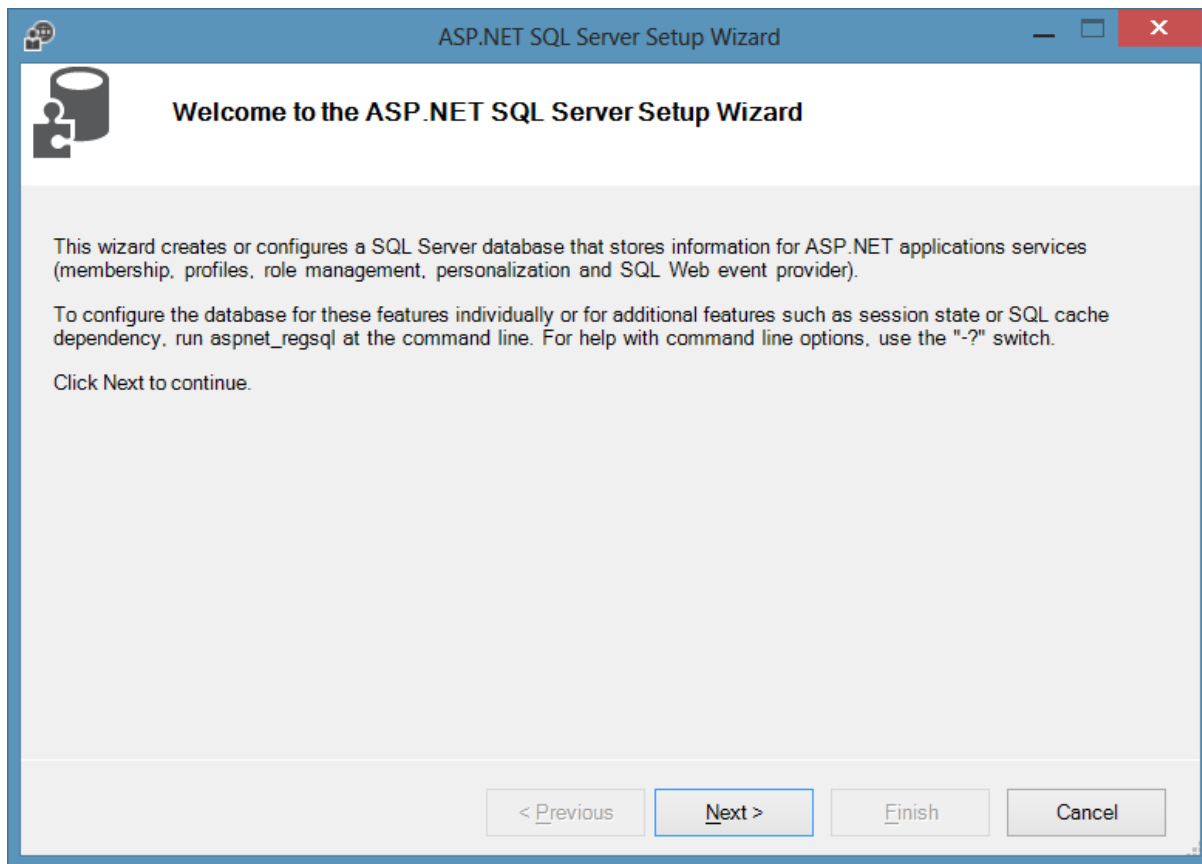
<http://msdn2.microsoft.com/en-us/library/ms178586.aspx>

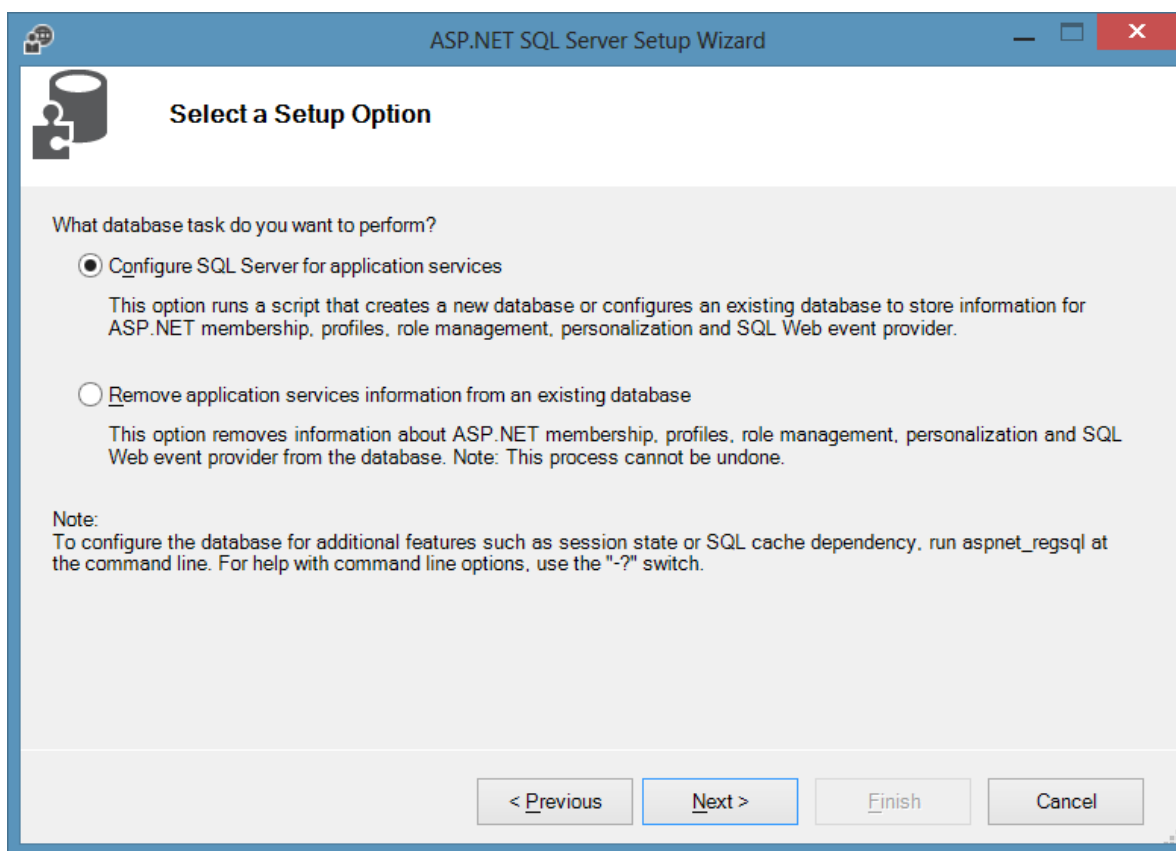
SQLServer Session store

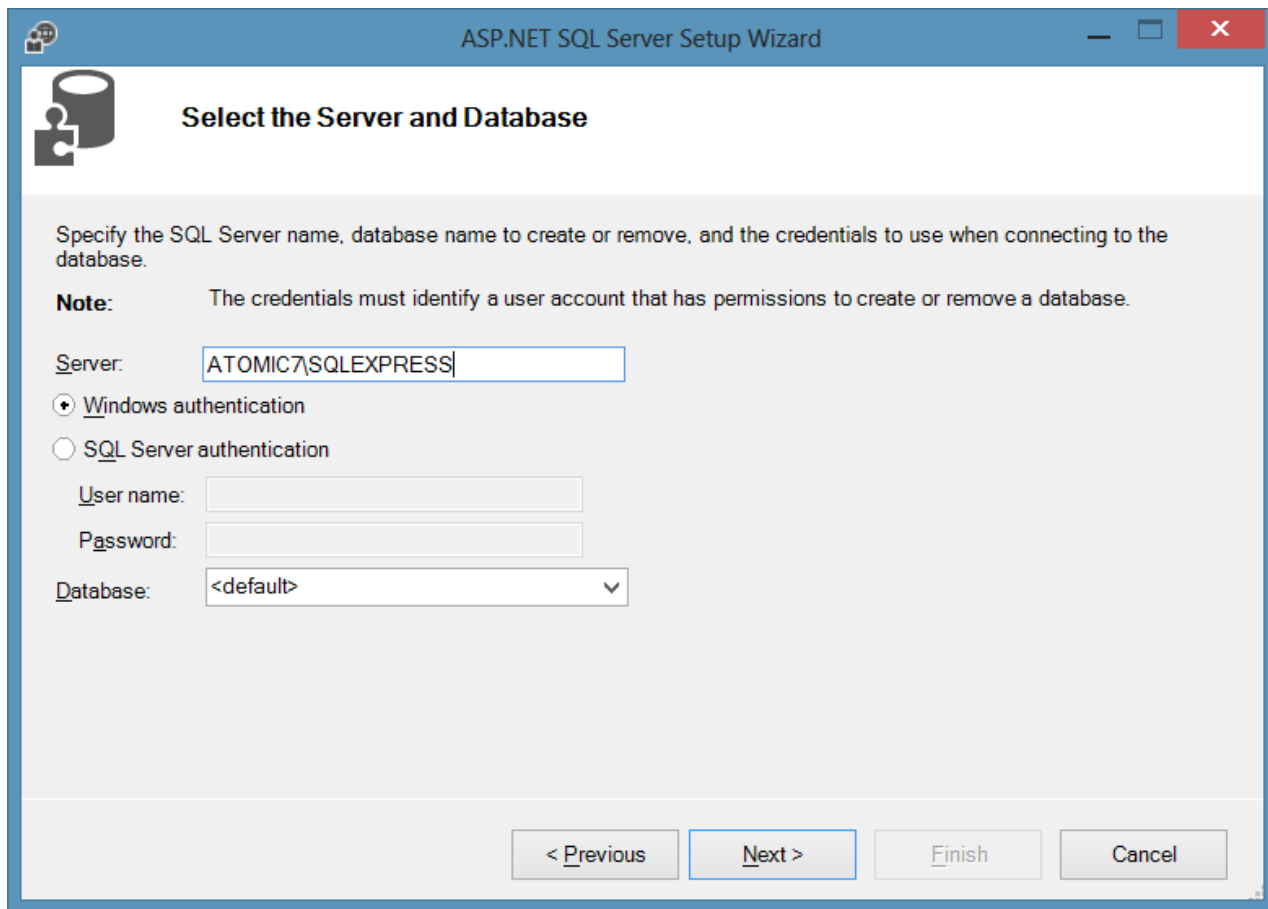
To enable storage of session state in SQL Server, update the web.config, and configure the SQL Server database to store the session state.

- 1) Update the web.config by changing the “mode” from “InProc” to “SQLServer”: `<sessionState mode="SQLServer" stateConnectionString="tcpip=127.0.0.1:42424" sqlConnectionString="data source=127.0.0.1;Trusted_Connection=yes" cookieless="false" timeout="20"/>`
- 2) Open the visual studio command prompt and type in “aspnet_regsql” to open the wizard for configured SQL to store session data:









ASP.NET SQL Server Setup Wizard

Select the Server and Database

Specify the SQL Server name, database name to create or remove, and the credentials to use when connecting to the database.

Note: The credentials must identify a user account that has permissions to create or remove a database.

Server:

☒ Windows authentication

☐ SQL Server authentication

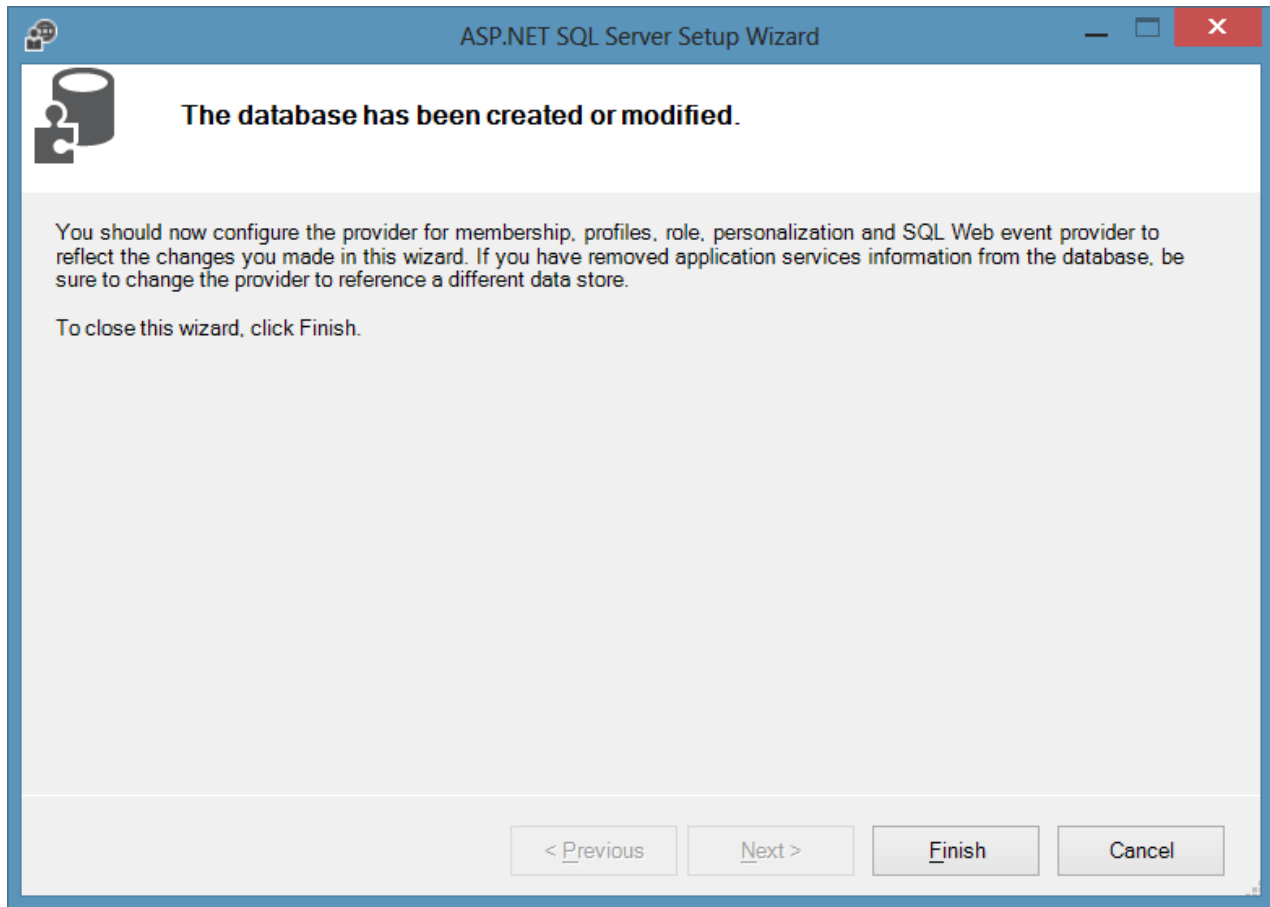
User name:

Password:

Database:

< Previous Next > Finish Cancel

A new database called “aspnetdb” will be created on the SQL server.



Developer reference: <http://www.codeproject.com/Articles/416137/Understanding-Session-Management-Techniques-in-ASP>

Appendix H: Single Sign on with SQL Membership Provider

SelectSurvey.NET provides integration with Single Sign on using MS SQL Membership Provider as an optional feature. Below are instructions for configuring the Single Sign on feature.

When the membership provider is activated, the application authenticates to the membership provider database, and then tries to find the user with the same “username” in the `sur_user` table in the survey database. If it finds it, the user is redirected into the survey list page.

The user enters their username and password into the `survey login.aspx` page, it authenticates to your membership provider database, then looks in the survey database for the matching user and redirects them into the survey list page (depending on the user’s role level).

The users in the survey database still need to synch with whatever single sign on you are using. You can either write a custom provider to do the synching or you can modify the source code of the survey application to add in the synching upon login if membership provider is used on the `login.aspx.cs` page the same way we wrote the

synching for the AD/NTLM page LoginActiveDirectory.aspx.cs. Source code must be purchased to make this edit in the survey application side. If the synching happens from your custom provider, it can create the user directly in the database upon authentication.

1) Edit the web.config file section below:

<!-- If you are using the survey app in a single sign on environment, enter the details of the membership provider in the <membership> node further down in this file. -->

```
<add key="UseMembershipProvider" value="no" />
```

2) Edit the web.config section as follows: Include a <membership> configuration in the <system.web> section as shown:

```
<membership defaultProvider="SqlMembershipProvider">
```

```
<providers>
```

```
<add name="SqlMembershipProvider"
```

```
type="System.Web.Security.SqlMembershipProvider" connectionStringName="ASPNETDB"
requiresUniqueEmail="true" maxInvalidPasswordAttempts="25" minRequiredPasswordLength="4"
minRequiredNonalphanumericCharacters="0" requiresQuestionAndAnswer="false"
applicationName="/SelectSurveyNET"/>
```

```
</providers>
```

```
</membership>
```

3) Configure a <connectionString> element with the name "ASPNETDB".

That is the connection string to the authentication database. It is required in addition to the connection string to the SelectSurvey.NET database. Below is a condensed version of what the web.config file should look like:

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<configuration>
```

```
<connectionStrings>
```

```
<add name="ASPNETDB" connectionString="Data
Source=xxx.xxx.xxx.xxx;Initial
Catalog=xxxxxx;UID=xxxxxxx;Password=xxxxxx"
providerName="System.Data.SqlClient" />
```

```
</connectionStrings>
```

```
<appSettings>
```

```
--all your app settings go in here. along with your existing SelectSurveyNET
connection string
```

```
<add key="UseMembershipProvider" value="yes" />
```

```
<add key="SURVEY_APP_DB_DRIVER" value="OleDb" />
```

```
<add key="SURVEY_APP_CONNECTION" value="Provider=SQLNCLI;Data
Source=xxx.xxx.xxx.xxx;Initial
Catalog=SelectSurveyNET;UID=xxxxxx;Password=xxxxxx" />
```

```
-- other settings...
```

```
</appSettings>
```

```
<system.web>
```

```
<membership defaultProvider="SqlMembershipProvider">
```

```
    <providers>
```

```
        <add name="SqlMembershipProvider"
type="System.Web.Security.SqlMembershipProvider" connectionStringName="ASPNETDB"
requiresUniqueEmail="true" maxInvalidPasswordAttempts="25" minRequiredPasswordLength="4"
minRequiredNonalphanumericCharacters="0" requiresQuestionAndAnswer="false"
applicationName="/SelectSurveyNET"/>
```

```
    </providers>
```

```
</membership>
```

```
</system.web>
```

Appendix I: Minimizing File Upload Feature Vulnerability

The "Respondent File Upload" feature and all features that allow uploading of images or files pose a potential risk for malicious files to be uploaded.

How to Allow File Upload while minimizing risk:

- Make sure you are using the latest version of SelectSurvey.NET v4.077.012 or later OR you have disabled the file upload question type AND removed write permissions on the "UploadedImages" folder.
- Make sure you have antivirus installed and running on the web server and that it is scanning the UploadedImages folder, or the folder you have specified for the "Respondent File Upload" question type.
- Make sure the folder specified for respondent file uploads is isolated and permissions on that folder are limited only to that folder.
- Train survey designers to specify file restrictions when adding the "Respondent File Upload" question type on a survey (the edit item page has checkboxes to restrict files to specific types)
- Make sure the web.config that only allows static files in the UploadedFiles folder (or whatever folder you have specified in admin tools>application wide settings for this) is there (can be copied from v4.077.012 or later from UploadedImages folder)
- Remove any files from the UploadedImages folder that are not static. That includes .html, .htm, .asp, .aspx, etc.
- Make sure you run windows updates on the web server
- Follow Microsoft Security Recommended Best Practices
- Make sure you are doing daily backups of files and databases on the server.

How to Disable file uploading and eliminate risk:

Remove folder and file permissions on the file upload folder designated in Admin Tools > Application Wide Settings. By default this is the "UploadedImages" folder on the web server right beneath the survey web folder itself.

How to Disable the "Respondent File Upload" Question Type:

To disable the ability for survey designers and administrators from adding the "Respondent File Upload" question type to a survey, login as an admin user, click "Admin Tools" > "Activate/De-Activate Question Types". Select the "Respondent File Upload" question type from the drop down list and click the arrow to move it to the disabled list of questions. If you are disabling file upload, you should also disable the question type, so that it does not show up as an option in the application.