WorkshopPLUS – Modern Authentication and Authorization – Active Directory Federation Services

Student Lab Manual

V1.0, January 2017

Information in this document is subject to change without notice. The example companies, organizations, products, people, and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarked, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2017 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, MS, Windows, Windows NT, MSDN, Active Directory, BizTalk, SQL Server, SharePoint, Outlook, PowerPoint, FrontPage, Visual Basic, Visual C++, Visual J++, Visual InterDev, Visual SourceSafe, Visual C#, Visual J#,  and Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names herein may be the trademarks of their respective owners.

Contents

[Objectives 4](#_Toc498683865)

[Prerequisites 5](#_Toc498683866)

[Task 1 – Create an application using ADFS for user authentication 5](#_Toc498683867)

[Task 2 – Configure ADFS to support an application using WS-Federation authentication 6](#_Toc498683868)

[Task 3 – Configure ADFS to support an application using OpenID Connect authentication. 7](#_Toc498683869)

## Objectives

After completing the exercises in this lab, you will be able to:

* Use AD FS management console to configure AD FS to provide security tokens to an application.
* Create an application using ADFS for authentication.

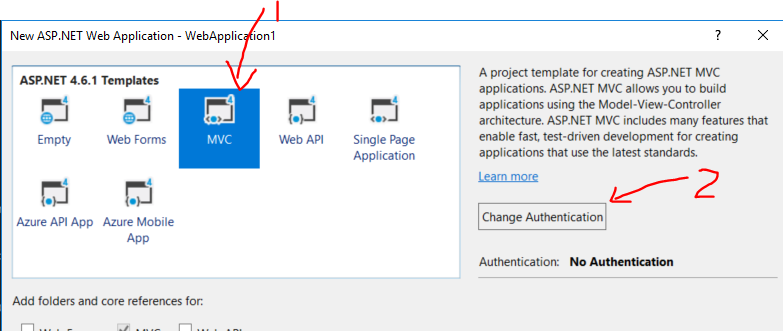
## Prerequisites

* None

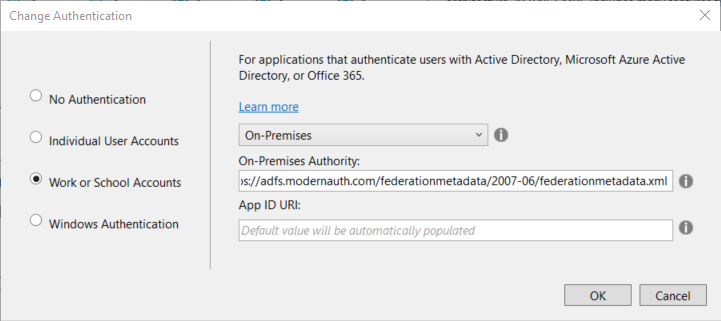
## Task 1 – Create an application using ADFS for user authentication

Using the Dev VM:

1. Open VS.NET
2. Create a new ASP.NET 4.x Web App using the MVC template (File->New project->C#->Web->ASP.NET Web Application (.NET Framework).
3. Click on Change Authentication button:



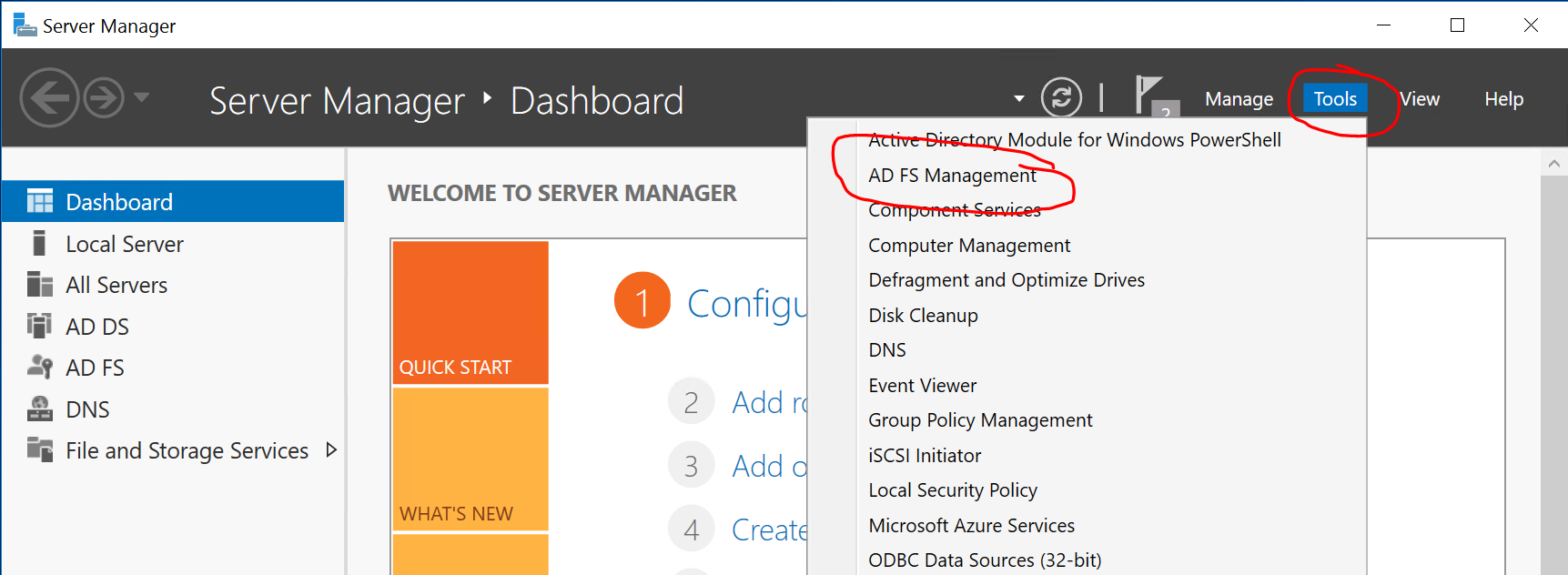
1. In the Change Authentication dialog select Work or School Accounts, On-premises application. In the On-premises Authority enter the metadata endpoint address of your ADFS server: <https://adfs.modernauth.com/federationmetadata/2007-06/federationmetadata.xml>. You can populate the App ID URI with your own ID or let the dialog choose one for you. Click OK and OK again to close the project creation dialog.



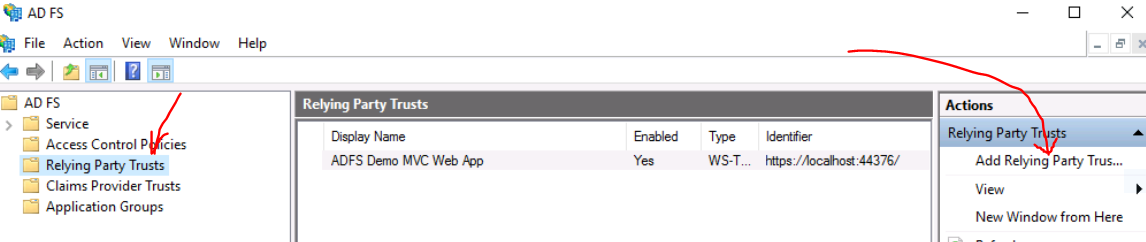
1. You should now have a new ASP.NET project. Open its web.config file – it will contain some values you will need in the next task.
2. Click on the Project name in the Solution explorer and note the SSL address on which the application will run locally, e.g. https://localhost:44359.

## Task 2 – Configure ADFS to support an application using WS-Federation authentication

1. Connect to your ADFS VM and use the Server Manager – Dashboard Tools option to start the ADFS management console:



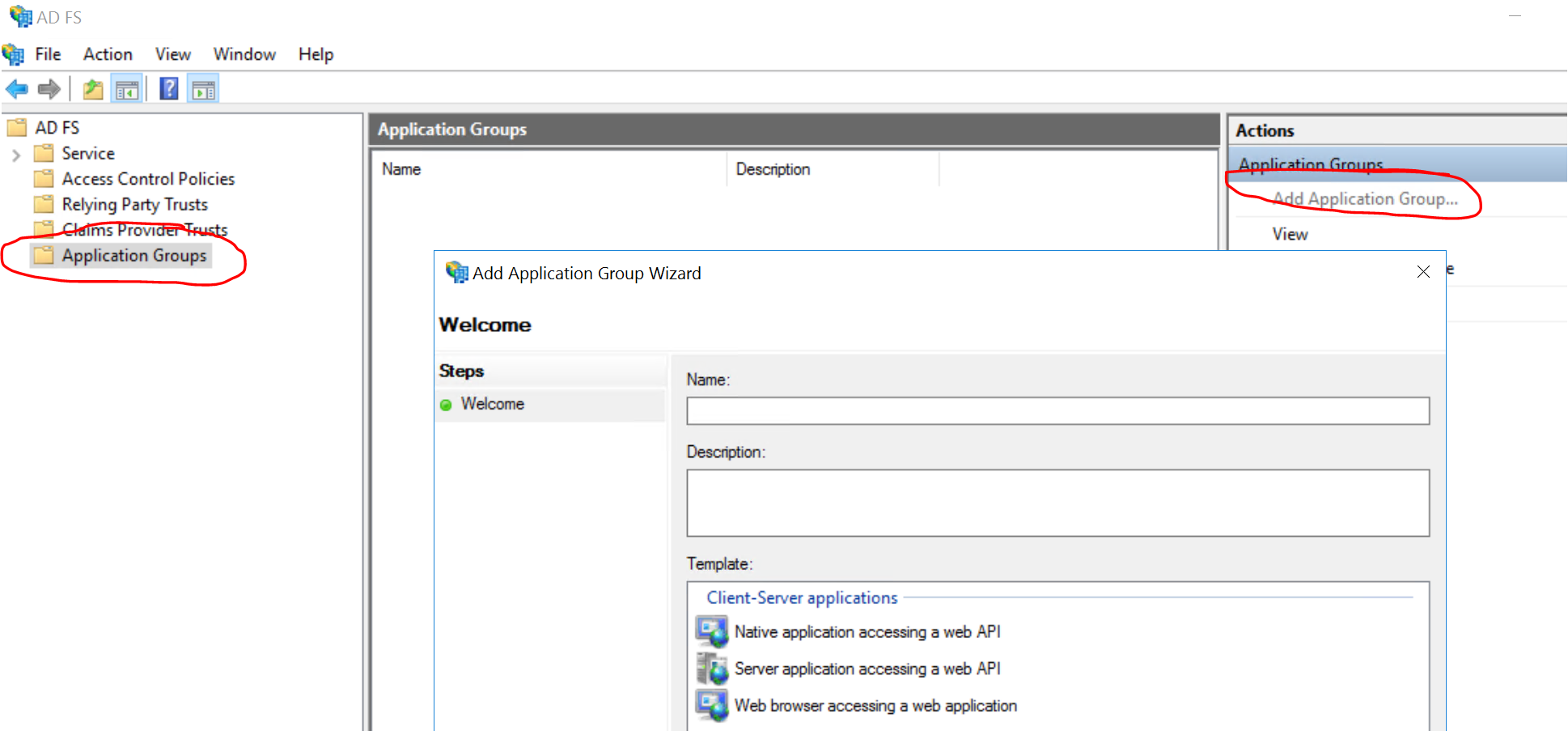
1. In the ADFS Management Console select the Relying Party Trusts folder on the left and Add Relying Party… option on the right of the screen:



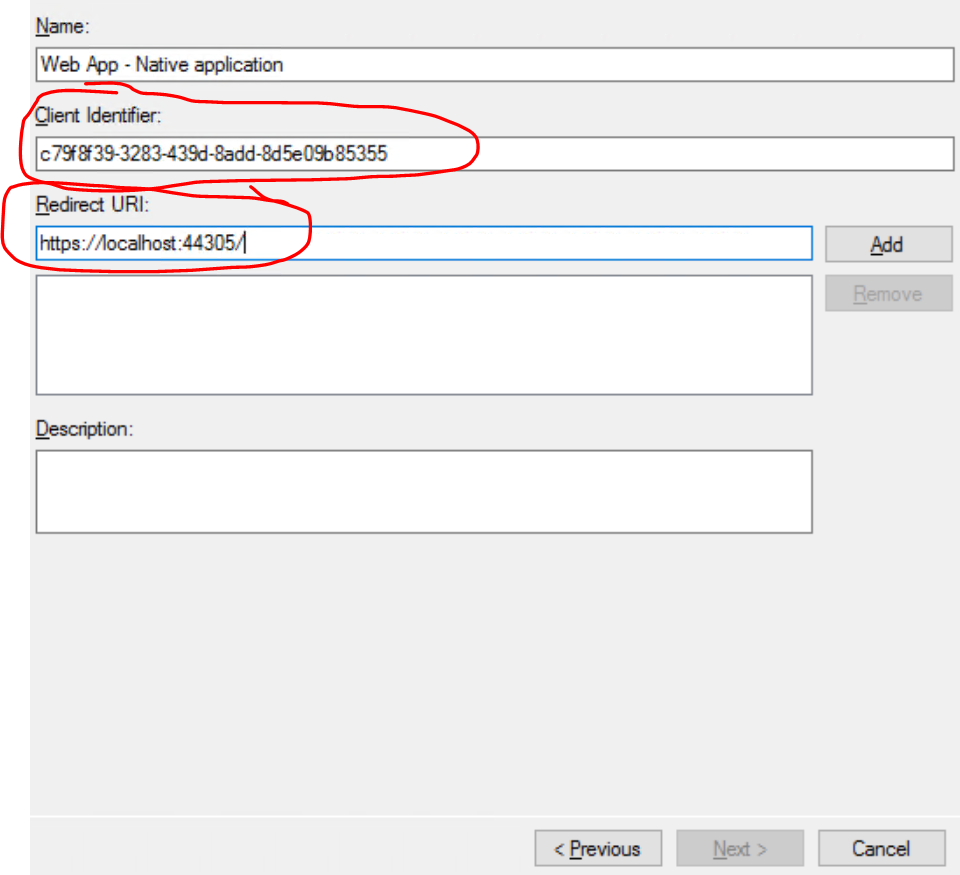
1. Connect to your VM and use the Server Manager – Dashboard Tools option to start the ADFS management console:
   1. Leave the Claims aware option on and click Start
   2. On the Select Data Source page select ‘Enter data about the relying party manually’ and click Next
   3. Enter a name for your application, e.g. ‘My WSFed app’ and click Next.
   4. Click Next on the Configure Certificate page (we are not encrypting our token requests).
   5. Select ‘Enable support for the WS-Federation Passive protocol’ on the Configure URL page. In the ‘Relying part WS-Federation Passive protocol URL enter the URL address on which your application will run (step 6 in the previous task), e.g. ‘https://localhost:44379. Click Next.
   6. On the Configure Identifiers page enter the value of the ‘ida:Wtrealm’ parameter from the web.config file (see step 5 in the previous Task), e.g. <https://webapp1>. Click Add and Next.
   7. Click Next several times till you can close this wizard. Click Close.
2. Edit Claim Issuance Policy dialog should open automatically. If not, select that option from the right side of the ADFS Management Console.
   1. Click Add Rule… and Next.
   2. Enter a name for the rule, e.g. ‘Send AD attributes’. Select Active Directory from the Attribute store dropdown.
   3. Select User-Principal-Name from the first column and UPN from the second.
   4. Click Finish and OK to close the dialog.
3. Switch to the Dev machine and run the application. Press OK if asked to install an SSL certificate.
4. When challenged for credentials enter those of a user defined in the AD (on the ADFS VM), e.g. administrator@modernauth.com/Pass@word#1. You should then be authenticated to your application. Note as the url in the browser changes for a while to indicate use of ADFS. You have successfully configured ADFS to authenticate to your application.

## Task 3 – Configure ADFS to support an application using OpenID Connect authentication.

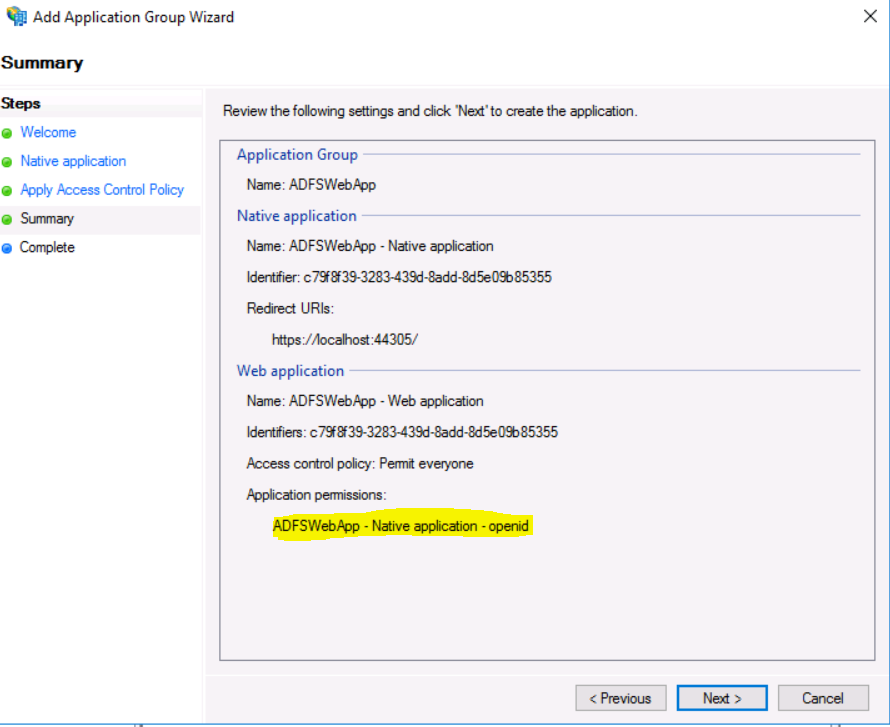
1. On the Dev VM, open the ADFSWebApp project in VS.NET from the C:\Users\Student\Desktop\Modern Auth\ ADFS\Lab folder.
2. Open the /App\_start/Startup.auth.cs source file.
3. Connect to your ADFS VM and use the Server Manager – Dashboard Tools option to start the ADFS management console:
4. Select the Application Groups option on the left panel and Add Application Group…



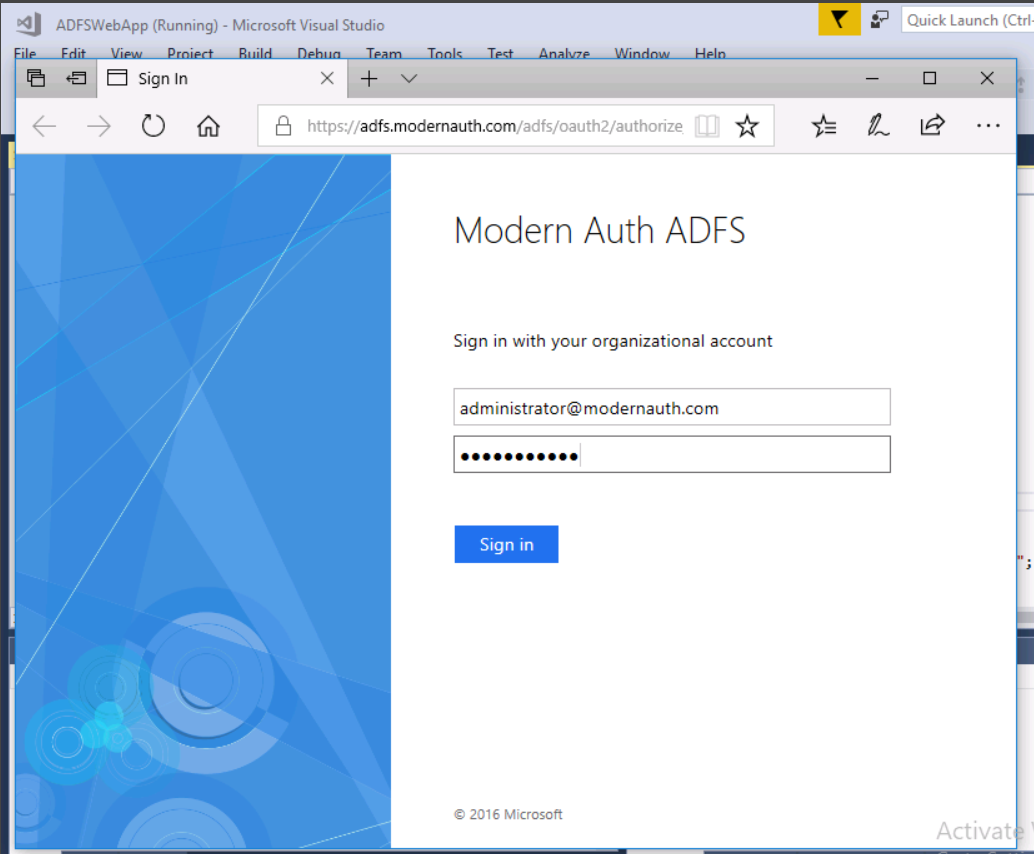
1. Select the *Web browser accessing a web application* option.
2. Give the application a descriptive name (e.g. *Web App*) and select Next.
3. Copy the Client Identifier (see below) to clipboard and paste it into the clientId field in the Startup.auth.cs class.
4. Enter <https://localhost:44305/> into the Redirect URI field and press Add. Click Next.



1. Click Next two more times and close the dialog. Note that the last panel tells you that ADFS will be configured to use OpenID Connect (OIDC) with this application:



1. Run the application on your local machine. You should be prompted for credentials. Enter credentials to authenticate with the ADFS server, you may authenticate with the administrator set of credentials.



1. You should be redirected to your application home page. Verify that the application knows who you are and shows the authenticated user:

