Windows Server 2012 R2 Microsoft

Windows Server 2012 R2: New Features in AD FS

Windows Server 2012 R2

Hands-on lab

Active Directory Federation Services (AD FS) uses claims-based authentication to provide users with single sign-on (SSO), web-based access to resources, whether located internally, in a federated partner organization, or in the cloud. In Windows Server 2012 R2, AD FS offers a number of new capabilities, including device registration (Workplace Join) for device authentication and SSO, enhancements for multi-factor authentication to manage risk, unified and simplified customization of the sign-in experience, and the ability to offer a user password change capability when using a registered device.

In this lab, you will configure AD FS to enable Workplace Join, configure a relying party trust, configure the Web Application Proxy server role to enable AD FS access for external clients, customize the AD FS sign-in page to improve the user experience, enable user password change for registered devices, and configure multi-factor authentication.

Produced by HynesITe, Inc
Version 2.0
12/20/2013

holSystems™
Learn. Experience. Collaborate.

This document is provided for informational purposes only and Microsoft makes no warranties, either express or implied, in this document. Information in this document, including URL and other Internet website references, is subject to change without notice. The entire risk of the use or the results from the use of this document remains with the user. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, 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, trademarks, 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.

Copyright 2013 © Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Hyper-V, Internet Explorer, Windows PowerShell, and Windows Server are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Introduction

Estimated time to complete this lab

45 minutes

Overview

Active Directory Federation Services (AD FS) uses claims-based authentication to provide users with single sign-on (SSO), web-based access to resources, whether located internally, in a federated partner organization, or in the cloud. In Windows Server 2012 R2, AD FS offers a number of new capabilities, including Workplace Join, enhancements for multi-factor authentication to manage risk, unified and simplified customization of the sign-in experience, and the ability to offer a change password capability for users when connecting with a registered device.

In this lab, you will configure AD FS to enable device registration, configure a relying party trust, configure the Web Application Proxy server role to enable AD FS access for external clients, customize the AD FS sign-in page to improve the user experience, enable user password change via a registered device, and configure multi-factor authentication.

Virtual machine Technology

This lab is completed using virtual machines that run on Windows Server 2012 Hyper-V technology. To log on to the virtual machines, press CTRL+ALT+END and enter your logon credentials.

Technical Architecture

This experience uses two servers and two clients.

Computer	Role	Configuration
DC	Domain controller and certification authority	Logon accounts server and Enterprise CA
Server2	AD FS server	Server that hosts the Active Directory Federation Services service
Server3	Application server	Server that hosts a web application used in the lab
Proxy	Web application proxy	Server that provides access to the web application and AD FS for external clients
Client1	Domain-joined Windows 8.1 client	Internal Windows 8.1 client
Client2	A standalone (non-domain-joined) Windows 8.1 client	External Windows 8.1 client

⚠ All user accounts in this lab use the password **Passw0rd!**

Note regarding pre-release software

Portions of this lab may include software that is not yet released, and as such may still contain active or known issues. While every effort has been made to ensure this lab functions as written, unknown or unanticipated results may be encountered as a result of using pre-release software.

Note regarding user account control

Some steps in this lab may be subject to user account control. User account control is a technology which provides additional security to computers by requesting that users confirm actions that require administrative rights. Tasks that generate a user account control confirmation are denoted using a shield icon. If you encounter a shield icon, confirm your action by selecting the appropriate button in the dialog box that is presented.

Note on activation

The virtual machines for these labs may have been built by using software that has not been activated. This is by design in the lab to prevent the redistribution of activated software. The unactivated state of software has been taken into account in the design of the lab. Consequently, the lab is in no way affected by this state. For operating systems other than Windows 8.1, please click Cancel or Close if prompted by an activation dialog box. If you are prompted by an Activate Screen for Windows 8.1, do the following:

1. Click **Go to PC Settings**.
2. Hover the mouse to one of the corners of the display, and then click the **Start** icon; alternatively, press the Windows key. The Start screen will appear.

Exercise 1: Enable Device Registration and Configure a Relying Party Trust

Workplace Join is made possible by the Device Registration Service (DRS) that is included as part of the AD FS role service on Windows Server 2012 R2. Workplace Join allows users to join Windows 8.1 and iOS devices to the network to provide access to resources. A workplace-joined (or registered) device represents a mid-state between non-domain joined and domain joined. Registered devices are known by the Active Directory administrator but are not affected by traditional domain membership characteristics such as Group Policy. Registered devices can be leveraged as a requirement for access to claims-aware applications.

In this lab exercise, you will first enable device registration in Active Directory to make it possible to workplace join devices. You will then configure a relying party trust for a sample claims-aware application. You will verify the configuration of the relying party trust. You will then configure the Web Application Proxy role service to enable device registration for an external client and provide access to claims-aware applications.

Enable device registration in Active Directory

The Device Registration Service provisions an object in Active Directory for devices that are workplace joined. In this task, you will examine the environment to learn about some of the prerequisites for enabling device registration and then enable device registration for Active Directory.

Begin this task logged onto **Server2** as **Contoso/Administrator** using the password **Passw0rd!**

1. On the desktop, double-click **Certificates**.
2. In the Certificates console, expand **Certificates (Local Computer)\Personal**, and then click **Certificates**.
3. In the details pane, double-click **adfs.contoso.com**.
4. In the Certificate dialog box, click the **Details** tab.
5. In the Details tab, note the values for the **Subject** and the **Subject Alternative Name** fields.

   This certificate is used as the SSL certificate for the AD FS role service to encrypt the session between the client and server. The subject name of the certificate must match the name used in the AD FS configuration, in this case, adfs.contoso.com. For device registration, you also need to add enterpriseregistration.contoso.com as a subject alternative name. The use of wildcard certificates is not recommended for AD FS.

6. In the Certificate dialog box, click **OK**.
7. Close the Certificates console, and then click **No** when prompted to save the settings.
8. Open **Windows PowerShell**.
9. Type the following commands, pressing ENTER after each one.

```
Ping adfs.contoso.com
Ping enterpriseregistration.contoso.com
```

Both names resolve to the same IP address. Two CNAME DNS resource records were created as part of the lab setup to resolve these names to the same IP address as Server2.contoso.com, where the AD FS role service is installed.

10. Type the following commands, pressing Y or ENTER, as appropriate, after each one.

```
Initialize-ADDeviceRegistration –ServiceAccountName Contoso\FsGmsa$
Enable-AdfsDeviceRegistration
```

The Contoso\FsGmsa$ service account is a group Managed Service Account that was created as part of the lab setup. Group Managed Service Accounts require a Microsoft Key Distribution Services root key created on the domain controller to enable automatic password generation for the group Managed Service Accounts.

11. Close **Windows PowerShell**.
12. Open **Internet Explorer**.
13. On the Favorites bar, click the shortcut **Device Registration Endpoint**.

The shortcut points to **https://enterpriseregistration.contoso.com/enrollmentserver/contract?api-version=1.0**.

IMPORTANT: You should receive a string value returned. This indicates that the device registration endpoints are working correctly.

Configure Web Application Proxy

In Windows Server 2012 R2, extranet access to AD FS is now provided by means of the new Web Application Proxy role service. In previous versions of AD FS, this functionality was provided by the AD FS Proxy, which is now a part of the Web Application Proxy. In this task, you will configure the Web Application Proxy role service to enable device registration for external, non-managed devices. Once configured, the Web Application Proxy will proxy requests for device registration to the AD FS server.

Begin this task logged onto **Proxy** as **Contoso/Administrator** using the password **Passw0rd!**

1. Open **Server Manager**.
2. In Server Manager, on the Tools menu, click **Remote Access Management**.
3. In the Remote Access Management Console, click **Web Application Proxy**.
4. Click **Run the Web Application Proxy Configuration Wizard**.
5. Click **Next**.
6. In Federation Service Name, type **adfs.contoso.com**.

7. In User Name, type **Contoso\Administrator**, and then in Password, type **Passw0rd!**
8. Click **Next**.
9. In AD FS Proxy Certificate, select **adfs.contoso.com**, and then click **Next**.
   - **NOTE:** The subject and subject alternative names (SAN) on this certificate are configured similar to the certificate you examined in a previous lab task. In this case, however, server3.contoso.com has been added as another SAN to support publishing the claims-aware application. You will publish this application in the next exercise.
10. Click **Configure**.
11. Click **Close**.
12. Leave the Remote Access Management console open for subsequent lab exercises.

Join a workplace from an unmanaged computer

When an unmanaged device is registered using Workplace Join, the Device Registration Service provisions a certificate on the device to represent the device identity. In this task, you will examine the user certificates personal store before joining a device this is outside the corporate network to the workplace, You will then workplace join the device and examine the certificate that is set on it.

✎ Begin this task logged onto **Client2** as **HomeUser** using the password **Passw0rd!**

1. On the desktop of Client2, double-click **Certificates**.
2. In the User Account Control dialog box, click **Yes**.
   - Notice that there is a single certificate issued to Ben Smith in the Personal certificate store. This certificate will be used for authentication in Exercise 4, after you configure multi-factor authentication.
3. Click the **Start** icon.
4. On the Start screen, type **Workplace**, and then press ENTER.
5. Click **Workplace Settings**.
6. In Workplace, type **bensmith@contoso.com**, and then click **Join**.
   - Access to the Device Registration Service occurs through the Web Application Proxy you configured in the previous task.
   - Client2 resolves enterpriseregistration.contoso.com and adfs.contoso.com, the DNS names required for device registration in the lab environment, to the IP address on external interface of PROXY.
7. In Contoso-ADFS, type **Passw0rd!** and then click **Sign in**.
   - Your computer is now joined to your workplace.
8. Move the mouse to the upper left corner, and then click the thumbprint for the Certificates console you opened previously.

9. In the Certificates console, click **Personal**, and then press F5.
10. Expand **Personal**, and then click **Certificates**.

    📌 The Device Registration Service has set a certificate.

11. Note the first and last four digits in the GUID that appears in the Issued To field.

    📌 Note that the GUID that appears in the Issued To field is the subject of the certificate.

Verify device registration in Active Directory

In this step, you will verify device registration in Active Directory.

✏ Begin this task logged onto **DC** as **Administrator** using the password **Passw0rd!**

1. In Server Manager, on the Tools menu, click **Active Directory Administrative Center**.
2. In Active Directory Administrative Center, navigate to **Contoso\RegisteredDevices**, and then click **RegisteredDevices**.

    📌 The name of the device that appears is in the form a GUID that matches the subject of the certificate issued to the newly workplace-joined device.

3. Double-click the device entry.
4. In Extensions, click **Attribute Editor**.

    📌 The display name indicates that this is the Client2 device.

    📌 Attributes of the device can be retrieved to issue claims in secure tokens to provide conditional access to resources.

5. Click **Cancel**.

Exercise 2: Configure Relying Party Trust Web Application Proxy for a Claims-Aware Application

In AD FS, a relying party is a website, application, or service that relies on an external AD FS to verify information about the identity of an entity requesting access to it. When an entity requests access to the relying party, the entity is redirected to an identity provider where it is authenticated using Active Directory or some other authentication mechanism. Once the entity is authenticated, claims about the identity of the entity are sent to AD FS. AD FS ultimately sends these claims in a digitally-signed token to the relying party. The token is digitally signed to ensure the integrity of the data. Based on the claims presented in the token, the entity requesting access is either allowed or denied access to the relying party. The relying party trust is the trust object that is configured to create and maintain the relationship between the relying party and an identity provider, in this case AD FS.

In this exercise, you will configure the relying party trust for a pre-installed sample claims-aware application and create a custom issuance authorization rule to allow access to the protected page of the application from our client devices. You will publish the application using the Web Application Proxy using an AD FS pre-authentication configuration, verify that both internal and external devices can access the protected application, and then compare the claims issued to both the internal and external devices. You will then reconfigure the Web Application Proxy to use pass-through authentication, and perform additional configuration steps in AD FS to ensure that claims specific to the workplace-joined device are issued.

Create a relying party trust on the federation server

In this step, you will configure your AD FS server to trust your claims application.

✎ Begin this task logged on to **Server2** as **Contoso\Administrator** using the password **Passw0rd!**

1. Open **Server Manager**.
2. In Server Manager, on the Tools menu, click **AD FS Management**.
3. In AD FS, expand **Trust Relationships**, and then click **Relying Party Trusts**.
4. In the Actions pane, click **Add Relying Party Trust**.
5. Click **Start**.
6. On the Select Data Source page, ensure that **Import data about the relying published online or on a local network** is selected.

   📌 This selection is the preferred method for creating relying party trust. When the data is published by the organization that maintains the relying party (either the internal organization or an external organization), it can be communicated and maintained more easily. Manually creating a relying party trust with a partner organization would require that a fairly significant amount of information would need to be collected from the partner organization.

7. In Federation metadata address (Host name or URL), type **https://server3.contoso.com/claimsapp**, and then click **Next**.

   As part of the lab setup, a federation.xml file contain the relying party data was created and copied to the claims-aware application to facilitate the creation and maintenance of the relying party trust for this lab by allowing you to import the data from the application URL.

8. On the Specify Display Name page, click **Next**.
9. On the Configure Multi-factor Authentication Now page, click **Next**.

   You will configure multi-factor authentication in a later lab step.

10. On the Choose Issuance Authorization Rules, page, click **Next**.
11. On the Ready to Add Trust page, click **Next**, and then click **Close**.
12. In the Edit Claims Rules for server3.contoso.com dialog box, click **Add Rule**.
13. In Claim rule template, select **Send Claims Using a Custom Rule**, and then click **Next**.

    Claim rules are defined as a property of claims provider trusts (for incoming claims) and relying party trusts (for outgoing claims). They define which claims are accepted, processed, and ultimately sent to the relying party.

14. In Claim rule name, type **All Claims**.
15. In Custom Rule, type the following text, and then click **Finish**.

    IMPORTANT: There is a space between **[** and **]** in the code below.

    ```
    c:[ ]
    => issue(claim = c);
    ```

    The text above is a custom definition language used by AD FS. You are usually not expected to know AD FS claims language syntax, as this syntax is automatically created using the configuration wizards. In this example, the syntax means to check for ***all*** incoming claims and then issue the same claims to the relying party. This example uses a custom language statement to display all claims for our lab purposes, which is not a normal scenario.

16. Click **OK**.

Configure forms-based authentication

In this task, you will configure AD FS to use forms-based authentication for Intranet users to facilitate testing.

Begin this task logged on to **Server2** as **Contoso\Administrator** using the password **Passw0rd!**

1. In AD FS, click the **Authentication Policies** node.
2. Under Primary Authentication, in the Global Settings area, click **Edit**.

3. In Intranet, uncheck **Windows Authentication**, and then check **Forms Authentication**.
4. Click **OK**.

Publish claims-aware application using the Web Application Proxy

In this task, you will publish the claims-aware application using the Web Application Proxy using AD FS pre-authentication. Once configured, the Web Application Proxy will proxy requests for the claims-aware application.

✎ Begin this task logged onto **Proxy** as **Contoso/Administrator** using the password **Passw0rd!**

1. On Proxy, in the Remote Access Management console, click **Web Application Proxy**, and then in the Tasks pane, click **Publish**.
2. On the Welcome page, click **Next**.
3. On the Preauthentication page, ensure that **Active Directory Federation Services (AD FS)** is selected, and then click **Next**.
4. On the Relying Party page, select **server3.contoso.com**, and then click **Next**.
   - 📌 This page appears only if you select AD FS as a preauthentication mechanism.
5. On the Publishing Settings page, in Name, type **Server3.contoso.com**.
6. In External URL, type **https://server3.contoso.com/**.
7. In External certificate, select **adfs.contoso.com**.
8. On the Publishing Settings page, click **Next**.
9. Click **Publish**, and then click **Close**.

Verify internal and external application access and compare issued claims

In this task, you will verify that you can access the sample Claimsapp application from both an internal and an external (workplace-joined) client. You also compare the claims that are issued to both the internal and external client.

✎ Begin this task logged on to **Client1** as **Contoso\BenSmith** and **Client2** as **HomeUser** using the password **Passw0rd!**

1. On **Client2**, open **Internet Explorer**.
   - 📌 Client1 and Client2 are the internal (domain-joined) and external (workplace-joined) clients, respectively.
2. Navigate to **https://server3.contoso.com/claimsapp**.
   - 📌 On both Client1 and Client2, you can use the shortcut, labeled Contoso ClaimsApp, on the Favorites bar to navigate to the application.
3. Log on as **bensmith@contoso.com** using the password **Passw0rd!**

- You are required to log on ***before*** you can gain access to the application.

4. Click **Contoso sign-in page**.
    - A list of all available claims is presented. This is the primary purpose of the sample application. The sample application also contains a number of links to related information and the ContosoDemo.com site. Unless the virtual machine has Internet access, these links will not be accessible.
5. Switch to **Client1**.
6. On Client1, open **Internet Explorer**.
7. Navigate to **https://server3.contoso.com/claimsapp**.
    - You are allowed access to the application without preauthenticating with AD FS. Client1 does not access the application through the Web Application Proxy.
8. Click **Contoso sign-in page**.
9. Log on as **bensmith@contoso.com** using the password **Passw0rd!**
    - A list of all available clams is presented.
10. Compare the claims that are displayed in both clients.
    - Note that there is no difference in the claims that are being displayed. In particular, there is no indication in the issued claims that Client2 is a workplace-joined device. The reason for this is that additional configuration is required in AD FS to ensure that the claim is issued. You will perform this configuration in subsequent lab steps.
11. On both Client1 and Client2, close **Internet Explorer**.
12. On **Client1**, open **Internet Explorer**, and then navigate to **https://server3.contoso.com/claimsapp**.
13. Click **Contoso sign-in page**.
14. On **Client1**, close **Internet Explorer**.
15. On **Client2**, open **Internet Explorer**, and then navigate to **https://server3.contoso.com/claimsapp**.
    - On both clients, it is necessary to log in manually each time to access the claims-aware application. This behavior will change after making some additional configuration changes in a subsequent task.
16. On **Client2**, close **Internet Explorer**.

Modify a Web Application Proxy published application

In this task, you will replace the published application configuration with one that uses pass-through authentication.

✎ Begin this task logged on to **Proxy** as **Contoso\Administrator** and **Client2** as **HomeUser** using the password **Passw0rd!**

1. In the Remote Access Management console, in the Published Web Applications tile, right-click **Server3.contoso.com**, click **Remove**, and then click **Yes**.
2. In the Remote Access Management console, click **Web Application Proxy**, and then in the Tasks pane, click **Publish**.
3. On the Welcome page, click **Next**.
4. On the Preauthentication page, click **Pass-through**, and then click **Next**.
5. On the Publishing Settings page, in Name, type **Server3.contoso.com**.
6. In External URL, type **https://server3.contoso.com/**.
7. In External certificate, select **adfs.contoso.com**.
8. On the Publishing Settings page, click **Next**.
9. Click **Publish**, and then click **Close**.
10. On **Client2**, open **Internet Explorer**, and then navigate to **https://server3.contoso.com/claimsapp**.

    📌 Because Client2 no longer preauthenticates with AD FS, the process for signing in is the same as for Client1.

    📌 If you see a message saying the page could not be displayed, you likely performed the steps too quickly. Verify the configuration of the published application on Proxy and try again.

11. Click **Contoso sign-in page**, and then log on as **bensmith@contoso.com** using the password **Passw0rd!**

    📌 You are now required to log in to view the protected page showing the claims.

12. Close **Internet Explorer**.

Modify AD FS to issue claims for registered users

Previously, when you examined the claims issued to Client2, you saw that AD FS did not issue claims that are specific to workplace-joined (registered) devices. In this task, you will modify the authentication policies and add an issuance authorization to ensure that these claims are issued. You will then view the claims on Client1 and Client2 and note the differences.

✎ Begin this task logged on to **Server2** as **Contoso\Administrator** using the password **Passw0rd!**

1. In Server Manager, on the Tools menu, click **AD FS Management**.
2. In AD FS, navigate to **Authentications Policies**.
3. In AD FS, click the **Authentication Policies** node.

4. Under Primary Authentication, in the Global Settings area, click **Edit**.
5. In the Edit Global Authentication Policy, check **Enable device authentication**.
6. Click **OK**
7. In AD FS, navigate to **Relying Party Trusts**, right-click **Server3.contoso.com**, and then click **Edit Claim Rules**.
8. In the Edit Claim Rules for server3.contoso.com dialog box, click the **Issuance Authorization Rules** tab.

   📌 Issuance authorization rules specify the criteria a user must meet to be granted access to the resource. This allows you to enforce requirements such as group membership, department, or device registration.

9. Click **Add Rule**.
10. Click **Next**.
11. In Claim rule name, type **Registered User**.
12. In Incoming claim type, click the drop-down list, and then spend a few minutes examining the incoming claim types.

    📌 Note that a number of these claim types, such as Device Identifier and Inside Corporate Network, are new to AD FS in Windows Server 2012 R2.

13. In Incoming claim types, select **Is Registered User**.
14. In Incoming claim value, type **True**.
15. Click **Finish**.
16. In the Edit Claim Rules for server3.contoso.com dialog box, click **OK**.

Verify registered device claims

In this task, you will verify that claims that are relevant to workplace-joined devices are issued to Client2. You will compare these claims with those that are issued to Client1.

✎ Begin this task logged on to **Client1** as **Contoso\BenSmith** and **Client2** as **HomeUser** using the password **Passw0rd!**

1. On **Client1**, open **Internet Explorer**.
2. Navigate to **https://server3.contoso.com/claimsapp**.
3. Click **Contoso sign-in page**.
4. Log on as **bensmith@contoso.com** using the password **Passw0rd!**

   📌 Under Claim Type, note the claims types that are displayed after the block of claim types for https://schemas.microsoft.com/ws2008/identity/claims/groupsid.

5. Close **Internet Explorer**.

6. On **Client2**, open **Internet Explorer**.
7. Navigate to **https://server3.contoso.com/claimsapp**.
8. Click **Contoso sign-in page**.
9. Log on as **bensmith@contoso.com** using the password **Passw0rd!**

   📌 Under Claim Type, note the addition of claim types for http://schemas.microsoft.com/ws2012/01/devicecontext/claims/... that are displayed after the block of claim types for http://schemas.microsoft.com/ws2008/identity/claims/groupsid.

   📌 Also examine the additional claim types that follow the name pattern, http://schemas.microsoft.com/2012/01... For example, note the claim type that indicates whether the client is inside or outside the corporate network. These additional claim types allow AD FS in Windows Server 2012 R2 to use enhanced multi-factor access controls to allow or deny access based on network location, workplace join status, and other factors. You will explore multi-factor access control in more detail in Exercise 4 of this lab.

10. Close **Internet Explorer**.
11. On **Client2**, open **Internet Explorer**.
12. Navigate to **https://server3.contoso.com/claimsapp**.
13. Click **Contoso sign-in page**.

    📌 You were not required to log on again. This is the default behavior for registered (workplace-joined) devices.

Modify relying party trust to require a log in every time a user connects

As you saw in the previous task, device registration enables a seamless login experience for users who connect to applications or services from workplace-joined devices. Because you will learn about the customization of sign-in pages in the next exercise, you will disable this feature so that a sign-in page will be presented when a user on Client2 attempts to access the application.

✏ Begin this task logged on to **Server2** as **Contoso\Administrator** and **Client2** as **HomeUser** using the password **Passw0rd!**

1. In AD FS, click the **Authentication Policies** node.
2. Under Primary Authentication, in the Custom Settings area, click **Manage**.
3. In Per Relying Party Trust, right-click **server3.contoso.com**, and then click **Properties**.
4. In the Edit Authentication Policy for server3.contoso.com dialog box, check **Users are required to provide credentials each time at sign in**.
5. Click **OK**.
6. Switch to **Client2**.

7. Right-click the **Start** icon, point to **Shutdown or sign out**, and then click **Sign out**.
8. Log in as **HomeUser** using **Passw0rd!** as the password.
9. Open **Internet Explorer**, and navigate to **https://server3.contoso.com/claimsapp**.
10. Click **Contoso sign-in page**.

    📌 You now see the sign-in page again.

11. Leave Internet Explorer open at the sign-in page for the next exercise.

Exercise 3: Customize AD FS Sign-in Pages

In the version of AD FS included with Windows Server 2012 R2, the dependency on IIS is removed. Instead, AD FS is built directly on top of HTTP.SYS. Consequently, instead of modifying files used by IIS to customize sign-in pages, you use the provided Windows PowerShell cmdlets to perform the same tasks. Furthermore, because the changes are stored in the AD FS configuration store, it is no longer necessary to perform the customizations on each AD FS server in a farm. The changes are executed once and are implemented across all servers.

In this exercise, you will explore some of the new Windows PowerShell cmdlets to customize the AD FS sign-in pages. You will change the logo, add custom error messages, and enable the update change password functionality for workplace-joined devices.

Customize sign-pages and verify changes

In this task, you will enter a series of Windows PowerShell commands that update the Sign-in page with a number of useful links and update the logo and company name. At the end of this task you will verify the changes.

Begin this task logged on to **Server2** as **Contoso\Administrator**, **Client1** as **Contoso\BenSmith**, and **Client2** as **HomeUser** using the password **Passw0rd!**

1. On **Client2**, at the sign-in page for the sample claims app, note the name on the page and the absence of links, descriptive texts, or graphic logos.
2. Switch to **Server2**.
3. Open **Windows PowerShell**.
4. At the Windows PowerShell prompt, type the following command, and then press ENTER.

   ```
   Get-AdfsGlobalWebContent
   ```

   Nothing is displayed in the output. This is an expected result.

5. At the Windows PowerShell prompt, type the following commands, pressing ENTER after each one.

   These Windows PowerShell commands, as well as others you will use subsequently, are found in a text file at **C:\Labfiles\ADFS-config.txt**. If you prefer, you can copy and paste these commands into the Windows PowerShell prompt or a Windows PowerShell ISE console.

   ```
   Set-AdfsGlobalWebContent -CompanyName "Contoso.Com"
   Set-AdfsGlobalWebContent -ErrorPageSupportEmail "Report this error"
   Set-AdfsGlobalWebContent -ErrorPageDescriptionText "Access Denied"
   Set-AdfsGlobalWebContent -HelpDeskLink
   "https://adfs.contoso.com/adfs/portal/updatepassword/"
   Set-AdfsGlobalWebContent -HelpDeskLinkText "Change Password"
   ```

```
↪ Set-AdfsGlobalWebContent -Homelink "http://server3.contoso.com"
↪ Set-AdfsGlobalWebContent -HomelinkText "Website"
↪ Set-AdfsGlobalWebContent -PrivacyLink
  "http://server3.contoso.com/privacy.html"
↪ Set-AdfsGlobalWebContent -PrivacyLinkText "Privacy Statement"
```

6. Switch to **Client2**.
7. In Internet Explorer, press F5 to refresh the sign-in page you left open in the previous exercise.
   - Notice that the company name changes. Also, notice that a number of new links are added to the bottom of the page.
8. At the bottom of the page, click **Change Password**.
   - An access denied message is displayed. You have just added the link to the change password application. However, it is necessary to enable this functionality in AD FS. You will enable the change password functionality in a subsequent task.
9. In Internet Explorer, click the back arrow to return to the sign-in page.
10. Switch to **Server2**.
11. At the Windows PowerShell prompt, type the following commands, pressing ENTER after each one:
    - These commands will replace the company name with a logo and add a different illustration to the left side of the sign-in page.

```
↪ Set-AdfsWebTheme -TargetName default -Logo
  @{path="C:\inetpub\images\ContosoLogo.jpg"}
↪ Set-AdfsWebTheme -TargetName default -Illustration
  @{path="C:\inetpub\images\illustration.png"}
```

12. Switch to **Client2**.
13. In Internet Explorer, press F5 to refresh the sign-in page you left open in the previous exercise.
    - The illustration and the logo changes.
14. Switch to **Server2**.
15. At the Windows PowerShell prompt, type the following commands, pressing ENTER after each one.
    - Because of the length of these commands, you may wish to copy and paste them from C:\Labfiles\adfs-config.txt.

```
↪ Set-AdfsGlobalWebContent -SignInPageDescriptionText "<p>Access to
  Contoso.Com resources may require device registration.<br><br>You
  can change your password using the 'Change Password' link below
  after you have registered your device.</p>"
```

```
↪ Set-AdfsGlobalWebContent -UpdatePasswordPageDescriptionText "Please
  enter your user account, old password and your new desired password
  twice. Note that your new password must meet the Contoso.com
  password complexity requirements."
↪ Set-AdfsRelyingPartyWebContent -Name "server3.contoso.com" -
  ErrorPageAuthorizationErrorMessage "<p style='font-
  size:0.9em'>Contoso.com requires you to workplace join your device
  to access this resource.</p><br><p>On your <b>Windows 8.1
  device</b>, use <b>PC Settings<b> to join your device to the
  workplace</p><br><p?On your <b>iOS</b> device, click <a
  href=https://adfs.Contoso.com/enrollmentserver/otaprofile>here</a>
  to join your device to the workplace</p><br><p style='font-
  size:1.0em'>Please close the browser and access the application
  after you have workplace joined your device.<p>"
↪ Set-AdfsGlobalWebContent -ErrorPageDeviceAuthenticationErrorMessage
  "We were unable to authenticate your device. Either your device is
  not registered or the certificate your device presented is invalid.
  Please register your device and try again."
↪ Set-AdfsGlobalWebContent -ErrorPageGenericErrorMessage "An
  unexpected error has occurred, please let the administrators know"
↪ Set-AdfsGlobalWebContent -ErrorPageAuthorizationErrorMessage "Sorry,
  we were unable to authorize your access, please try again. If this
  error persists, please contact the administrators."
```

16. At the Windows PowerShell prompt, type the following command, and then press ENTER.

```
↪ Get-AdfsGlobalWebContent
```

The output is populated with the settings changes you have made.

17. Switch to **Client2**.
18. In Internet Explorer, on the sign-in page, press F5 to refresh the page.

Additional descriptive text is added. In the next task, you will change the issuance authorization rules so that Client1 will be denied access. This will allow you to see other messages you have added by means of the Windows PowerShell cmdlets.

Temporarily deny access to unregistered devices

In this task, you will modify the issuance authorization rules to deny access to Client1. This configuration change serves two purposes: it allows you to see some of the customizations that you made in the previous task and it demonstrates the compound (multi-factor) authentication available in this version of AD FS. At the end of this task, you will set the configuration back to its original state.

Begin this task logged on to **Server2** as **Contoso\Administrator** using the password **Passw0rd!**

1. On **Server2**, in the AD FS console, in the tree pane, navigate to **Relying Party Trusts**, right-click **server3.contoso.com**, and then click **Edit Claim Rules**.

2. In the Edit Claim Rules for server3.contoso.com dialog box, click the **Issuance Authorization Rules** tab.
3. Click **Permit Access to All Users**, click **Remove Rule**, and then click **Yes**.
4. Click **Apply**.

    By removing this rule, only users who log in from workplace-joined devices (that is, where the claim "Is Registered User" evaluates to True), will be allowed access. This is an example of seamless compound or multi-factor authentication, whereby two or more conditions must be met in order to allow access. As you saw in the previous exercise, the new claim types, such as "Is Registered User", that are available with AD FS in Windows Server 2012 R2 provide richer and more nuanced controls for multi-factor access.

5. Leave the dialog box open for subsequent steps.
6. Switch to **Client1**.
7. On **Client1**, open **Internet Explorer**.
8. Navigate to **https://server3.contoso.com/claimsapp**.
9. Click **Contoso sign-in page**.
10. Log on as **bensmith@contoso.com** using the password **Passw0rd!**

    You receive a message stating that your device must be workplace joined in order to gain access to the page.

11. Close **Internet Explorer**.
12. Switch to **Client2**.
13. In Internet Explorer, on the sign-in page, log on as **bensmith@contoso.com** using the password **Passw0rd!**

    You can log on because you are doing so from a registered device.

14. In Internet Explorer, click the back arrow to return to the sign-in page.
15. Switch to **Server2**.

    You are going to return the issuance authorization rules to their previous state so that users on Client1 can log on.

    IMPORTANT: Make sure you perform the steps below; otherwise, subsequent lab steps will fail.

16. In the Edit Claim Rules for server3.contoso.com dialog box you left open in a previous step, click the **Issuance Authorization Rules**, and then click **Add Rule**.
17. On the Select Rule template page, select **Permit All Users**, and then click **Next**.
18. Click **Finish**.
19. In the Edit Claim Rules for server3.contoso.com dialog box, click **OK**.

Enable change user password on registered devices

In this task, you will enable the update password capability so that users on workplace-joined devices will be able to change their passwords.

✎ Begin this task logged on to **Server2** and **Proxy** as **Contoso\Administrator** using the password **Passw0rd!**

1. On **Server2**, in AD FS, navigate to **Service/Endpoints**.
2. In Endpoints, scroll to the bottom of the list, right-click **adfs/portal/updatepassword**, and then click **Enable**.
3. In the AD FS Management dialog box, click **OK** to acknowledge the message about restarting the service.
4. Right-click **adfs/portal/updatepassword** again, and then click **Enable on Proxy**.
5. In the AD FS Management dialog box, click **OK** to acknowledge the message about restarting the service.
6. On **Server2**, open **Windows PowerShell**.
7. At the Windows PowerShell prompt, type **restart-service –name adfssrv –force**, and then press ENTER.
8. Switch to **Proxy**.
9. On Proxy, open **Windows PowerShell**.
10. At the Windows PowerShell prompt, type **restart-service –name adfssrv –force**, and then press ENTER.

Verify update password functionality

In this task, you will verify that you ~~cannot access Claimsapp, as you are not on a registered device~~change a password from a registered device.

✎ Begin this task logged on to **Client1** as **Contoso\BenSmith** and **Client2** as **HomeUser** using the password **Passw0rd!**

1. On **Client2** in Internet Explorer, on the AD FS **Contoso sign-in page**, click **Change Password**.
2. In the first field, type **bensmith@contoso.com**.
3. In Old Password, type **Passw0rd!**
4. In New Password, and Confirm New Password, type **Passw0rd1**.
5. Click **Submit**.
6. Close **Internet Explorer**.

7. Switch to **Client1**.
8. Open **Internet Explorer**.
9. Navigate to **https://server3.contoso.com/claimsapp**.
10. Click **Contoso sign-in page**.
11. On the sign-in page, click **Change Password**.

    📌 You are denied access since the update password functionality is available only from workplace-joined devices.

12. Close **Internet Explorer**.

Exercise 4: Enable Multi-Factor Authentication for Sensitive Applications

A final feature that you will explore in this lab is the enhancement of multi-factor authentication (MFA) in AD FS. The general function of AD FS is to issue a secure token that contains a set of claims containing information about an entity that is requesting access to a resource. Within AD FS, claim rules determine what claims AD FS will accept and issue. Issue authorization rules set on relying party trusts provide access control to applications or services based on what claims are accepted or denied.

In Windows Server 2012 R2, AD FS includes a greater variety of claim types, for example, those that are related to Workplace Join. The additional claim types allow for richer and more nuanced multi-factor access controls over previous versions of AD FS, as you have seen previously in the lab.

In addition to this, AD FS in Windows Server 2012 R2 allows you to configure multi-factor access controls on a global basis or a per-application/service (relying party trusts) basis. In addition, it is possible for 3rd-party authentication vendors, such as Windows Azure Multi-Factor Authentication, to be used as a multi-factor authentication method. That is, multi-factor authentication is extensible.

Enable certificate-based multi-factor access control

Out of the box, Windows Server 2012 R2 includes certificate-based multi-factor access control for certificates. Typically, in a production environment, the certificates would be on a smart-card that is issued to the users. In this task, you will enable multi-factor access control for a certificate that is installed in the user profile.

✎ Begin this task logged on to **Server2** as **Contoso\Administrator**

1. In AD FS, navigate to **Authentication Policies**.
2. In Authentication Policies, under Multi-factor Authentication, in the Global Settings area, click **Edit**.

   📌 Global settings for MFA affect all relying party trusts and are used as a fallback in the absence of application-specific MFA configurations.

3. In Edit Global Authentication Policy, in the Users/Groups area, click **Add**.
4. In the Select Users or Groups, type **MFA**, and then click **OK**.

   📌 This group contains a single user, Alice Ciccu.

5. In the Locations area, check **Extranet**.

   📌 If either of these two conditions (membership in the MFA-users group or logging on from an external device) is met, certificate authentication will be required in addition to user name and password.

6. In the Select additional authentication methods area, check **Certificate Authentication**.
7. Click **OK**.

Verify certificate-based multi-factor access control

In this task, you will verify the MFA settings you configured in the previous exercise.

✎ Begin this task logged on to **Client1** as **Contoso\BenSmith** using a **Password1** as the password and logged on to **Client2** as **HomeUser** using **Passw0rd!** as the password.

- **IMPORTANT**: In the previous exercise you changed the password of the Contoso\BenSmith account. Please ensure you use the appropriate password for this object.

1. On **Client1**, open **Internet Explorer**.
2. Navigate to **https://server3.contoso.com/claimsapp**.
3. Click **Contoso sign-in page**.
4. Log in as **bensmith@contoso.com** using **Passw0rd1** as the password.
   - Ben Smith is not a member of the MFA-Users group and is logging in from an internal client; therefore, no additional authentication methods are required.
   - Spend a few moments reviewing the claim types that are shown on the web page.
5. On the taskbar, right-click the **Start** icon, point to **Shut down or sign out**, and then click **Sign out**.
6. On **Client1**, log on as **Contoso\AliceCiccu** using the password **Passw0rd!**
7. Open **Internet Explorer**.
8. Navigate to **https://server3.contoso.com/claimsapp**.
9. Click **Contoso sign-in page**.
10. Log on as **aliceciccu@contoso.com** using the password **Passw0rd!**
11. In the Windows Security dialog box, click **OK**.
    - The AliceCiccu account is a member of the MFA-users group, which triggers certificate authentication according the settings you configured earlier.
12. In the Windows Security dialog box, click **Allow**.
    - After approximately 10-30 seconds, the protected page showing the claim types should appear.
    - Additional claims types related to the certificate authentication are present in the token.
13. Switch to **Client2**.
14. Open **Internet Explorer**.
15. Navigate to **https://server3.contoso.com/claimsapp**.
16. Click **Contoso sign-in page**.
17. Log on as **bensmith@contoso.com** using the password **Passw0rd1**.

- 📌 You will briefly see the page informing you that a certificate is required. You are seeing this page because Ben is logging in from an external client. After a few moments, the protected page showing the claim types is presented. If you were in a production environment, you would be using a smart card that requires a PIN. You would be prompted for the PIN.
- 📌 Note the claim types that are present to indicate certificate-based authentication. As part of the lab setup, a certificate for Ben Smith was enrolled and then imported into the certificates store of Client2. This certificate was automatically used to provide a seamless login experience for the workplace-joined device.

This is the end of the lab