

KB 160130

Modifications to the logon form in the DIGIPASS Authentication for Microsoft ADFS

Creation date: 11/04/2017

Last Review: 12/09/2017

Revision number: 1

Document type: How To

Security status: EXTERNAL

Summary

This paper outlines the process for customizing the ADFS logon form that is installed with the DIGIPASS Authentication for Microsoft ADFS product.

Problem symptoms / details

When installing the DIGIPASS for Microsoft ADFS product module, the default logon theme used by ADFS is replaced with a DIGIPASS branded form. In many cases, clients do not want to make major changes to the end-user federated logon experiences. Alternatively, some clients have previously customized their ADFS logon form to meet internal objectives and provide a desired experience for end-users. Both of these require a post-install steps be taken to remove the VASCO ADFS logon form modifications.

Solution

1 Overview

ADFS logon forms are known as 'themes'. The ADFS management Console has some theme management, but most of the Theme management occurs using Microsoft documented PowerShell commands.

The DIGIPASS Authentication for Microsoft ADFS installation includes the DPAAuth4ADFS theme, which it sets to be the active, 'default', theme; effectively replacing any previous default customizations with the VASCO provided form.

This is done during the installation process by executing an installed PowerShell script; i.e.:

- VdsAddNativeModule.ps1

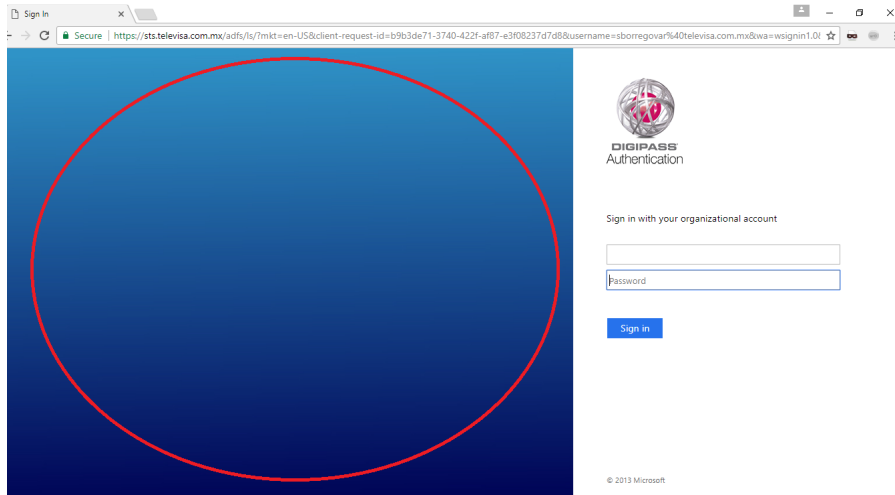
After the installation, the script is installed (for reference) in the ADFS folder created for this new DPAAuth4ADFS theme¹.

¹ usually c:\Windows\ADFS\DPAAuth4ADFS

2 PowerShell cmdlet review

The PowerShell scripts use a variety of ADFS specific PowerShell cmdlets to manage the ADFS logon form. While this document is not intended to provide a comprehensive review of the ADFS PowerShell management cmdlets, it will review key cmdlets used in the scripts executed during installation and others that are available to modify the logon form.

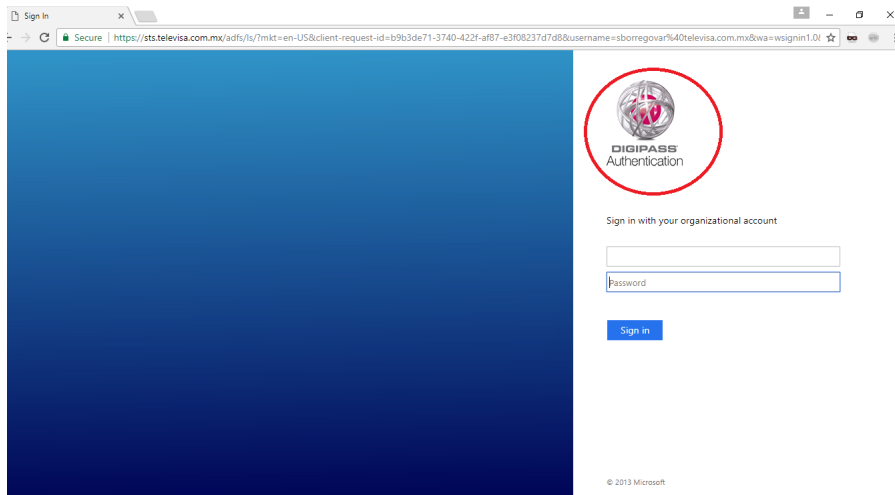
2.1 Set DIGIPASS theme illustration



The DIGIPASS DPAAuth4ADFS theme does not contain any illustration graphics, but changing the left side illustration on the logon form can be achieved with the following PowerShell cmdlet:

```
Set-AdfsWebTheme -TargetName default -Illustration @"{path=" <illustration path>"}"
```

2.2 Set DIGIPASS theme logo



² Recommended dimensions for this is 1420x1080 pixels @ 96 DPI and no greater than 200KB

To modify the logo displayed on the logon form use the PowerShell cmdlet:

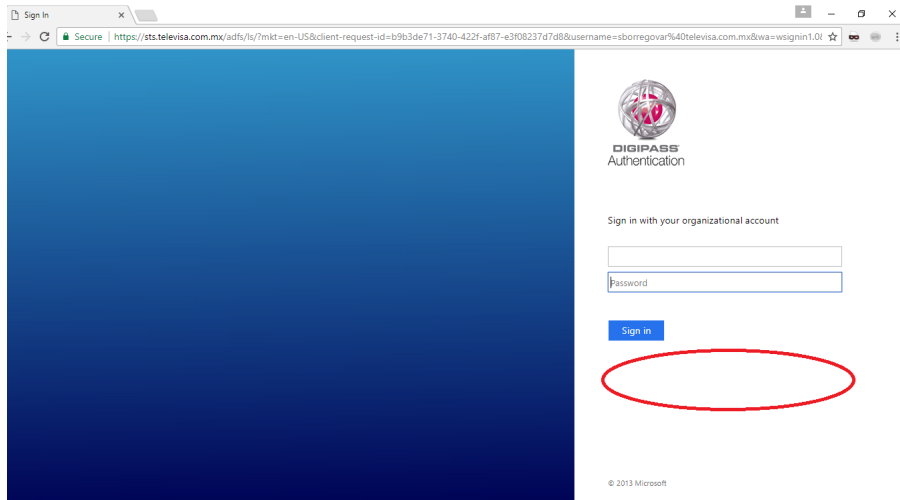
```
Set-AdfsWebTheme -TargetName DPAAuth4ADFS -Logo @"{path="<logo image path³>"}
```

2.3 Set DIGIPASS theme company name

There is no company name defined in the DIGIPASS ADFS theme (since the logo image is provided). However, to define a company name that would be displayed on the sign-in form when the logo is not available, execute the PowerShell cmdlet:

```
Set-AdfsGlobalWebContent -CompanyName "<company name>"
```

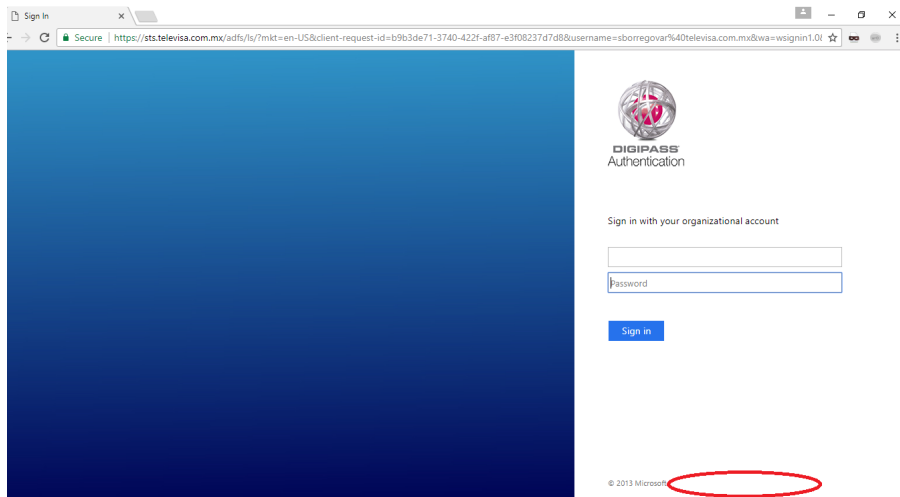
2.4 Set DIGIPASS theme description text



By default, no sign-in description text is defined in the DIGIPASS ADFS logon form, however to add one, the following PowerShell can be executed:

```
Set-AdfsGlobalWebContent -SignInPageDescriptionText "<description text⁴>"
```

2.5 Set DIGIPASS theme home, privacy and help links



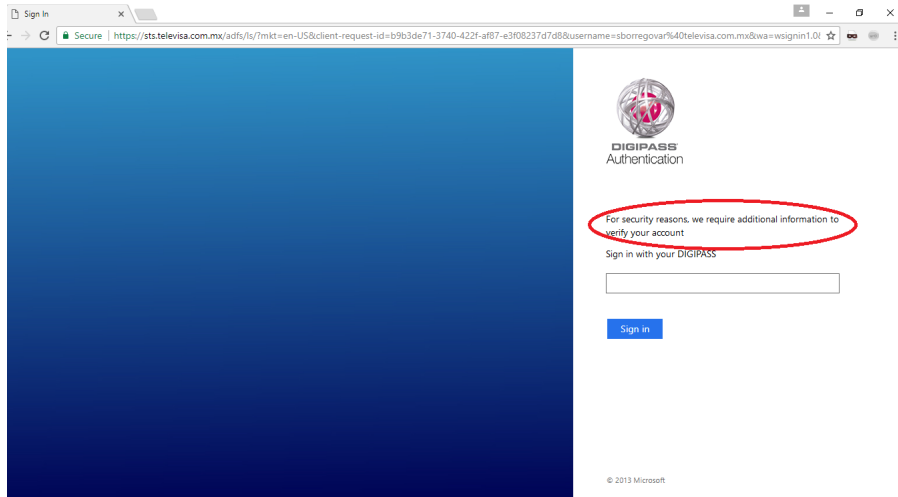
³ Recommended dimensions for this is 260x35 pixels @ 96 DPI and no greater than 10KB

⁴ Description text supports HTML with or without tags

By default, no links are defined on the DIGIPASS ADFS logon form, however to add these, the following PowerShell cmdlets can be used:

```
Set-AdfsGlobalWebContent -HelpDeskLink <helpdesk link> -HelpDeskLinkText Help5
Set-AdfsGlobalWebContent -HomeLink <home page link> -HomeLinkText Home5
Set-AdfsGlobalWebContent -PrivacyLink <privacy link> -PrivacyLinkText Privacy5
```

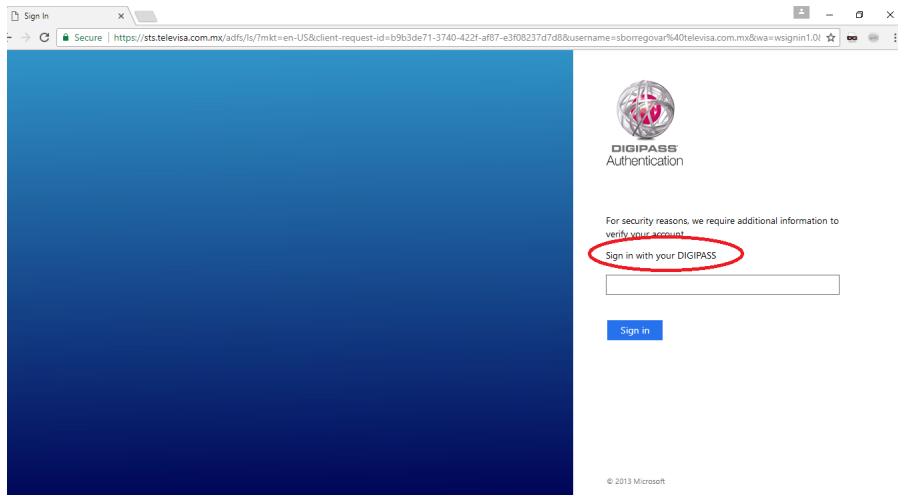
2.6 Set description on secondary logon form



To modify the descriptive text on the secondary 'child' logon form that gets displayed with the DIGIPASS ADFS use to collect the OTP, use the PowerShell cmdlet:

```
Set-AdfsGlobalWebContent -SignInPageAdditionalAuthenticationDescriptionText "<description text>"
```

2.7 Set label text on DIGIPASS secondary logon form



This involves advanced customization, which requires modification to the onload.js script that is executed with all ADFS theme pages. To get a copy of the existing

⁵ The 'LinkText' parameters (-HelpDeskLinkText, -HomeLinkText and -PrivacyLinkText) are required only if the link text being displayed is being changed.

onload.js logic (changes should be added to this so as not to lose existing advanced features) perform the following:

```
Export-AdfsWebTheme -Name default -DirectoryPath <path to theme folder6>
```

This will create the onload.js file from the default theme in the specified theme folder, which can then be modified with the desired logic changes.

To change the login message on the second page, you can edit the following lines:

```
// change login message string in the child logon form if it is present.
var loginMessageNode = document.getElementById('loginForm');
if (loginMessageNode)
{
    // Check whether first child of loginForm element is text
    var loginMessageChild = loginMessageNode.firstChild;
    if (loginMessageChild.nodeType == Node.TEXT_NODE
        && loginMessageChild.nodeValue.trim().length > 0)
    {
        // Replace/Create input instructions on loginForm child document with new text
        loginMessageNode.replaceChild(document.createTextNode("<label text>"),
            loginMessageChild);
    }
}
```

Finally, to associate the modified onload.js script with the specific theme (DPAAuth4ADFS), execute the PowerShell cmdlet:

```
Set-AdfsWebTheme -TargetName DPAAuth4ADFS7 -AdditionalFileResource
@{Uri='adfs/portal/script/onload.js';path="<theme folder path>"}
```

⁶ The theme folder should be created beforehand and must be accessible to the ADFS server when running.

⁷ Changes to the onload.js file cannot be associated directly to the 'default' theme.

3 Conclusion

The simplest way to make all but the advanced modifications to the installed DIGIPASS ADFS theme forms is to edit and modify the VdsAddNativeModule.ps1 script and rerun that script (along with onload.js edits if advanced modifications are required). Some of these changes can be made in existing PowerShell cmdlet calls; others require the introduction of new cmdlets.

The following is an example (*italics* indicate new/changed lines):

```

$iCnt = 0
do {
    $arrService = Get-Service -Name 'adfssrv'
    if ($arrService.Status -eq "Running") {
        break
    }
    Start-Service -Name 'adfssrv'
    Start-Sleep -Seconds 3
    $iCnt++
} while($iCnt -lt 3)

[System.Reflection.Assembly]::Load("System.EnterpriseServices, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a")
$publish = New-Object System.EnterpriseServices.Internal.Publish
$publish.GacInstall("C:\Windows\ADFS\DPAuth4ADFS\DPAuth4ADFS.dll")

##### Register#####
$typeName = "DPAuth4ADFS.ADFSAuthenticationAdapter, DPAuth4ADFS, Version=3.6.0.12,
Culture=neutral, PublicKeyToken=47635ea377e360dd"
Register-AdfsAuthenticationProvider -TypeName $typeName -Name "DPAuth4ADFS" -
Verbose
## Create a new ADFS theme basd on the default
New-AdfsWebTheme -Name DPAuth4ADFS -SourceName default
## Set this new DPAuth4ADFS as the active theme
Set-AdfsWebConfig -ActiveThemeName DPAuth4ADFS
## Change text shown on DPAuth4ADFS logon form when image is not available
Set-AdfsGlobalWebContent -CompanyName "<company name>"
## Change image shown on DPAuth4ADFS logon form
Set-AdfsWebTheme -TargetName DPAuth4ADFS -Logo @{path="<logo image path>"}
## if custom changes are required in second page - run script to detect and implement
these
## NOTE - export this for theme to the path folder first and modify javascript onload.js file
with appropriate logic
## Set-AdfsWebTheme -TargetName DPAuth4ADFS -AdditionalFileResource
@{Uri='adfs/portal/script/onload.js';path="<theme folder path>"}

Set-AdfsProperties -SsoLifetime 10
Set-AdfsGlobalAuthenticationPolicy -AdditionalAuthenticationProvider "DPAuth4ADFS"
Restart-Service "Active Directory Federation Services" -Force

```