ServicePRO
workflow management solution

ADFS Authentication and Configuration

January 2017

Help Desk Technology International Corporation http://www.servicepro.solutions

Table of Contents

1. Introduction

This document outlines ADFS Authentication and Configuration for use in ServicePRO.

Active Directory Federation Service (ADFS) is a software component provided by Microsoft that allows for login using active directory credentials.

From Microsoft's *Developer Network* page on AD FS:

> AD FS is a standards-based service that allows the secure sharing of identity information between trusted business partners (known as a federation) across an extranet. When a user needs to access a Web application from one of its federation partners, the user's own organization is responsible for authenticating the user and providing identity information in the form of "claims" to the partner that hosts the Web application. The hosting partner uses its trust policy to map the incoming claims to claims that are understood by its Web application, which uses the claims to make authorization decisions.

This user guide outlines:

- Details on changes made to the Configure Active Directory Synchronization feature in ServicePRO.
- How to configure Authentication Settings for Active Directory Federation Services (ADFS) in ServicePRO.
- Details on changes made to login functionality when ADFS authentication is enabled, for both ServicePRO and ServicePRO Web.

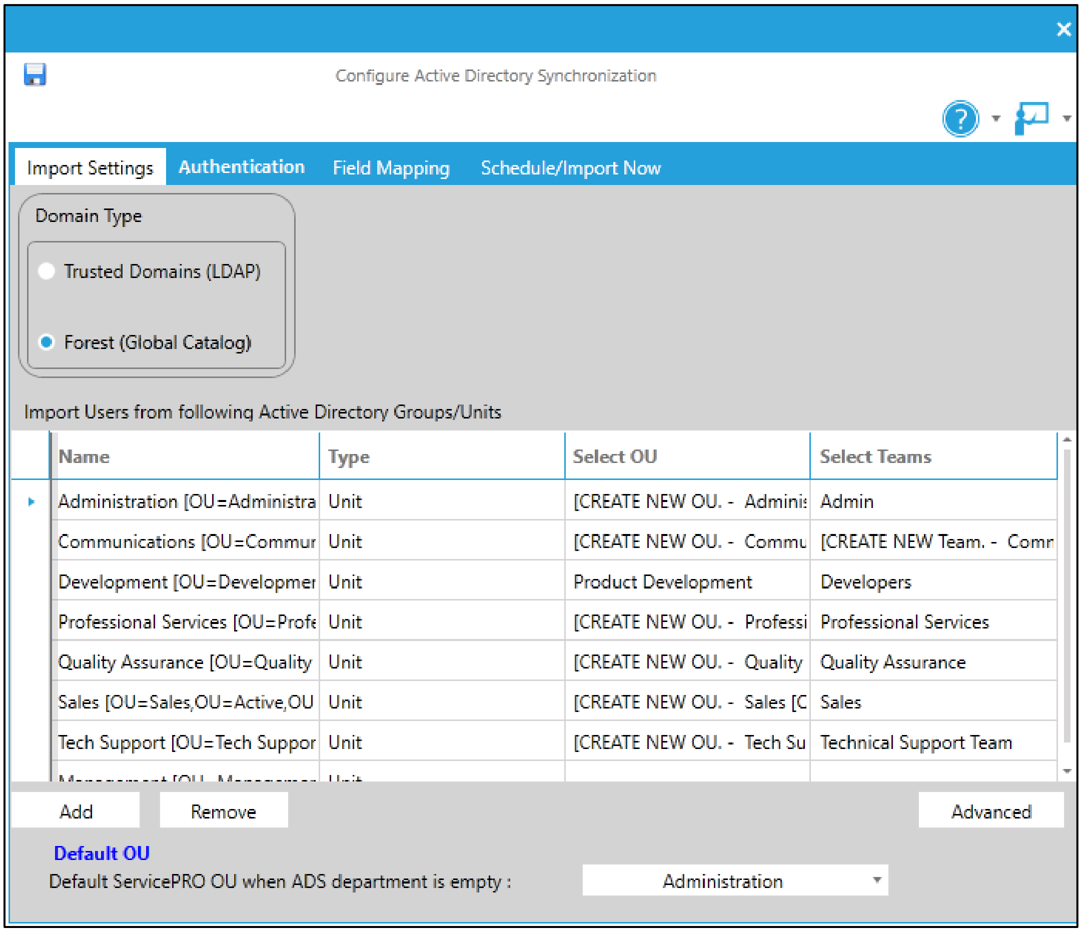
2. Changelog for Configure Active Directory Synchronization

2.1. Changes in Configure Active Directory Sync – 'Import Settings' Tab

Authentication settings for *AD Configuration* have been moved to a separate *Authentication* tab. Only import-related settings will remain in the *Import Settings* tab. No other changes in functionality have been made to this tab.

> **NOTE**: User Import is still possible only with AD, and not with Active Directory Federation Services (ADFS).

The revised *Import Settings* tab will appear as shown below:



Domain Type

○ Trusted Domains (LDAP)

● Forest (Global Catalog)

Import Users from following Active Directory Groups/Units

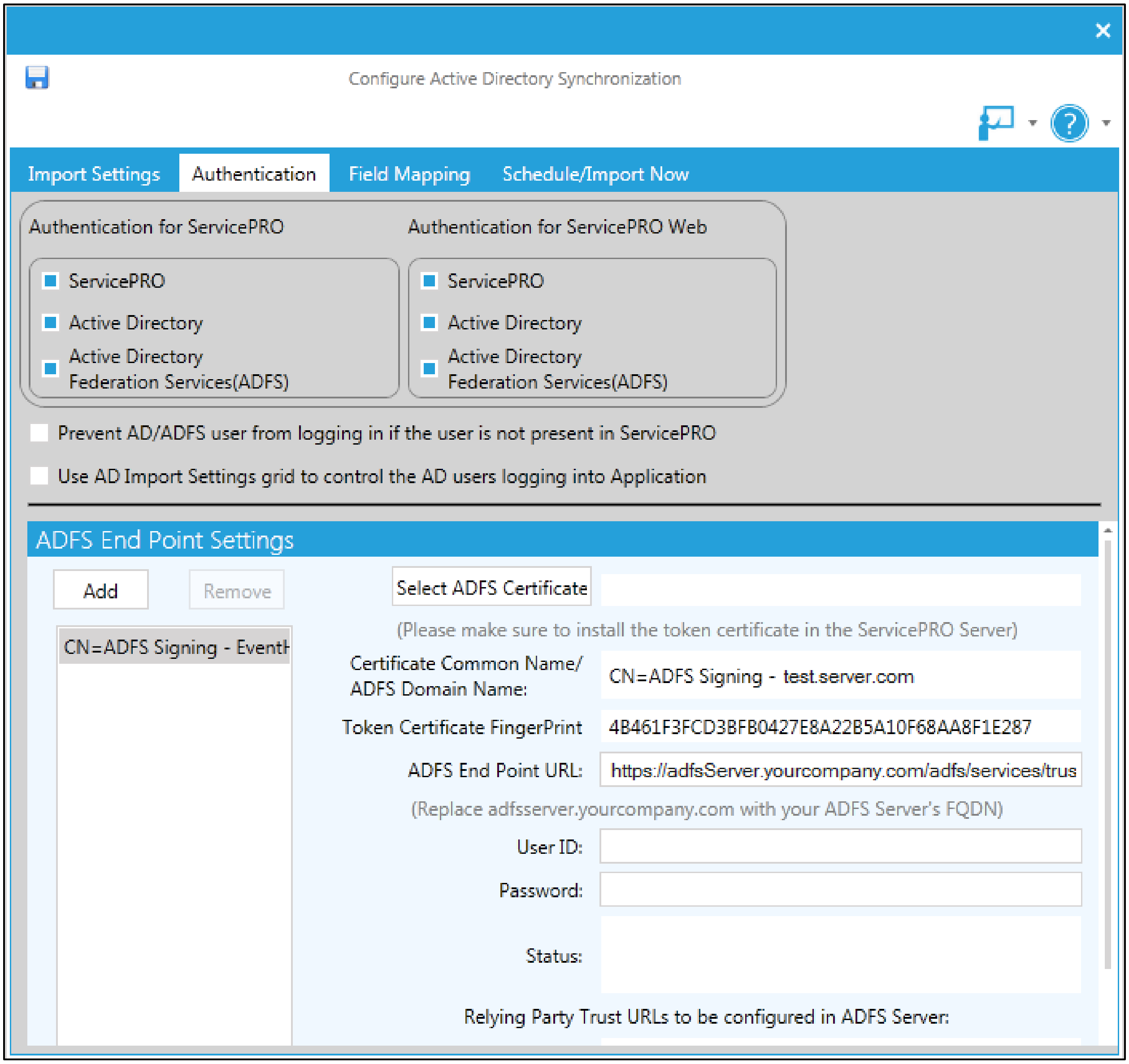
Name	Type	Select OU	Select Teams
Administration [OU=Administra	Unit	[CREATE NEW OU. - Adminis	Admin
Communications [OU=Commur	Unit	[CREATE NEW OU. - Commu	[CREATE NEW Team. - Comr
Development [OU=Developmer	Unit	Product Development	Developers
Professional Services [OU=Profe	Unit	[CREATE NEW OU. - Professi	Professional Services
Quality Assurance [OU=Quality	Unit	[CREATE NEW OU. - Quality	Quality Assurance
Sales [OU=Sales,OU=Active,OU	Unit	[CREATE NEW OU. - Sales [C	Sales
Tech Support [OU=Tech Suppor	Unit	[CREATE NEW OU. - Tech Su	Technical Support Team
Management [OU=Manageme	Unit		

Default OU

Default ServicePRO OU when ADS department is empty : Administration

2.2. Configure Active Directory Synchronization – ‘Authentication’ tab

The image below depicts settings that are now available in the *Authentication* tab in *Active Directory* configuration. *Authentication* related settings which existed previously in the *Import Settings* tab are moved to this new tab. In addition, ADFS-related settings have been implemented in this tab.



Authentication for ServicePRO

■ ServicePRO

■ Active Directory

■ Active Directory Federation Services(ADFS)

Authentication for ServicePRO Web

■ ServicePRO

■ Active Directory

■ Active Directory Federation Services(ADFS)

□ Prevent AD/ADFS user from logging in if the user is not present in ServicePRO

□ Use AD Import Settings grid to control the AD users logging into Application

ADFS End Point Settings

CN=ADFS Signing - EventH

(Please make sure to install the token certificate in the ServicePRO Server)

Certificate Common Name/ ADFS Domain Name: CN=ADFS Signing - test.server.com

Token Certificate FingerPrint 4B461F3FCD3BFB0427E8A22B5A10F68AA8F1E287

ADFS End Point URL: https://adfsServer.yourcompany.com/adfs/services/trus

(Replace adfsserver.yourcompany.com with your ADFS Server's FQDN)

User ID:

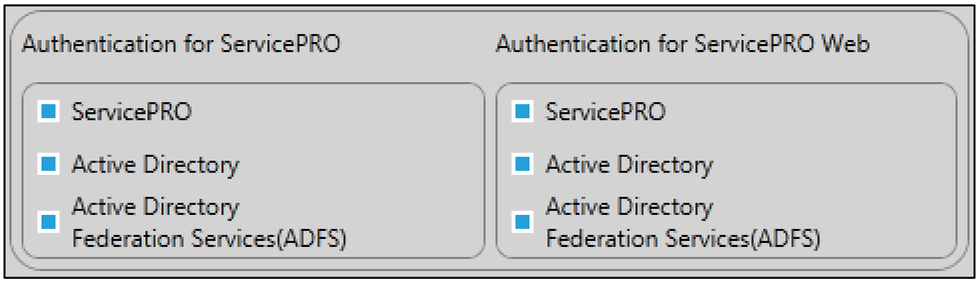
Password:

Status:

Relying Party Trust URLs to be configured in ADFS Server:

2.2.1. Authentication Check boxes

- Existing radio button options for authentication have been changed to new checkbox options in the *Authentication* tab.
- There is now a checkbox to specify if ‘Active Directory Federation Services (ADFS)' will be enabled for authentication.



Authentication for ServicePRO

☑ ServicePRO

☑ Active Directory

☑ Active Directory Federation Services(ADFS)

Authentication for ServicePRO Web

☑ ServicePRO

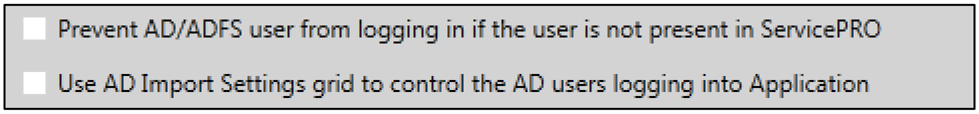
☑ Active Directory

☑ Active Directory Federation Services(ADFS)

2.2.2. Check-boxes that control user creation during login authentication

The two check-boxes that control user creation during login authentication have been moved to the *Authentication* tab from the *'Import Settings*' tab.

- **‘Prevent AD/ADFS user from logging in if the user is not present in ServicePRO’** – This checkbox option controls the user creation with both AD Authentication and ADFS Authentication
- **‘Use AD Import Settings grid to control the AD users logging into Application’** – This checkbox option controls the user creation only with AD Authentication (not with ADFS Authentication)



□ Prevent AD/ADFS user from logging in if the user is not present in ServicePRO

□ Use AD Import Settings grid to control the AD users logging into Application

2.2.2.1. <u>When user not present while authenticating using ADFS</u>

If the checkbox option labelled ‘*Prevent AD/ADFS user from logging in if the user is not present in ServicePRO*’ is not checked, new users will be generated if the authenticated user is not already present in ServicePRO. The following steps outline user creation:

1) Settings configured in AD Field Mapping settings will be applied.

> **NOTE**: The administrator needs to set up claims in the ADFS Server for all the Active Directory fields that are mapped in the Active Directory Field Mapping Settings. Please refer to Appendix sections 5.2 and 5.3.

2) If not all claims are set as per AD Field mapping settings, the user will be created with the minimal data available based on the claims present. Details on minimum requirements for claims for authentication have been provided in Section 5.3 of this document.

As ADFS claims cannot be set for the ADS department, the generated user will always be assigned to the ‘*Default Department’* set in the ‘*Import Settings’* tab.

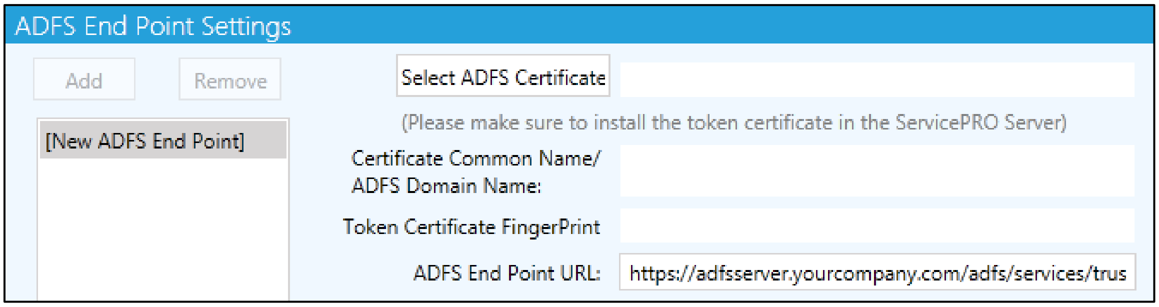
2.2.3. ADFS Endpoint Settings

- When the client chooses **Active Directory Federation Services (ADFS)** from the *Authentication* settings, they will need to set up ADFS Endpoints with names for each of the Endpoints. . These Endpoints will provide access to the federation server functionality of Active Directory Federation Services, such as token issuance, and the publishing of federation metadata.
    - For more details on ADFS Endpoints, please consult the Microsoft Server documentation on this subject. https://technet.microsoft.com/en-us/library/adfs2-help-endpoints(v=ws.10).aspx
- If the administrator has selected '**ADFS'**, but has not added at least one ADFS Endpoint setting, then the user will not be allowed to save authentication settings. ServicePRO facilitates the client to set up multiple ADFS Endpoints.
- Saving ADFS Endpoints is disallowed until each of the Endpoints are validated successfully.
- During login, if ADFS authentication is enabled, the name of these configured Endpoints will be listed in the login dialog. Based on the selected Endpoint/domain name, authentication will be performed using the specific Endpoint.

2.2.3.1. ADFS Endpoint Settings – Adding & Validation

This section outlines the setting up of the ADFS Endpoints in detail.

When a new ADFS Endpoint is added, the left panel will contain a placeholder item with the label, '**New ADFS Endpoint**'. This placeholder name will be updated and replaced with the contents of the '*Certificate Common Name/ADFS Domain Name*' field when a certificate is selected, and Endpoint Settings have been validated.



[New ADFS End Point]

(Please make sure to install the token certificate in the ServicePRO Server)

Certificate Common Name/ ADFS Domain Name:

Token Certificate FingerPrint

ADFS End Point URL: https://adfsserver.yourcompany.com/adfs/services/trus

The following field data should be entered by the user:

1) **Select ADFS Certificate** – When this option is selected, the user will be prompted with a file selection dialog to select the ADFS token certificate. When the certificate file is chosen by the user, the application parses the certificate file to retrieve the following information:
    - Certificate Common Name (Issuer Name)/ADFS domain name
    - Token Certificate Fingerprint

   The 2 display fields in ADFS Endpoint settings will be populated with information retrieved from the certificate.

NOTE: The Client's System Administrator should make sure to install the ADFS Token Certificate into the trusted store in the client's Web Server which hosts the ServicePRO and ServicePRO Web portal. This is required for validation as well as the actual authentication.

2) **ADFS Endpoint URL** – Field to enter the ADFS Endpoint URL that will be used for user authentication. This field will be populated with a URL with masked information (one shown below). The user will need to change the highlighted part of this URL to specify their company's ADFS server name with domain name (FQDN – Fully Qualified Domain Name); once resolved correctly, it will be reachable from the application:

   https://adfsServer.yourcompany.com/adfs/services/trust/13/UsernameMixed

3) **User ID, Password** – The administrator setting up ADFS Endpoint settings should enter a valid AD user and password in these fields. This is to validate the ADFS Endpoint settings being configured.

   For more details, please refer to the ADFS Server setup guide for the settings required in AD FS server for the relying party trust.

NOTE: The AD user that is used to authenticate must already exist in ServicePRO Database.

4) **"Relying Party Trust URLs to be configured in the ADFS Server" Display Only field** – Users will be able to copy the URLs from these fields to use in setting up relying party trust in the ADFS server.

   - **ServicePRO Service URL** – Displays the ServicePRO Service URL
   - **ServicePRO Web URL** – Displays the ServicePRO Web URL

   After filling in the fields listed above, the user should click on 'Validate' button in order to validate the settings before saving. The following actions will be performed when the user clicks on the 'Validate' button at the end of the '*ADFS Endpoint Settings*' section:

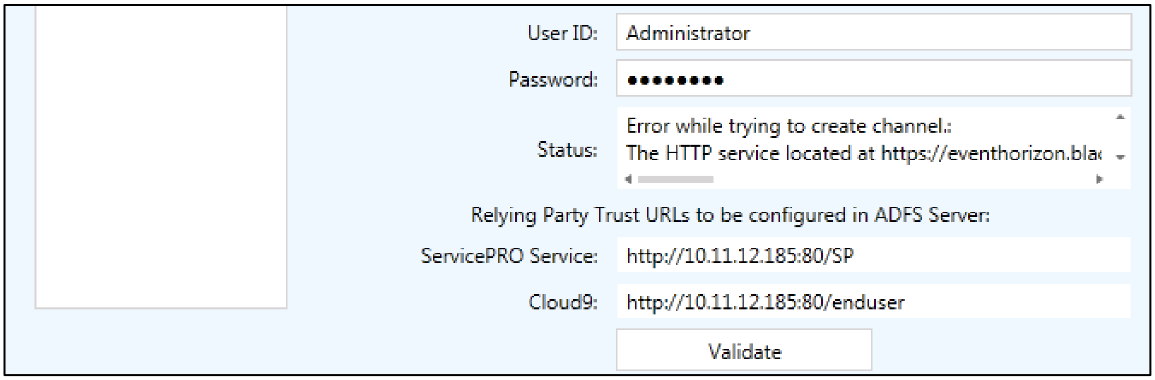
   1) Validate and ensure that fields in this section are not empty.
   2) Make the required call to ADFS by passing the following parameters: *Endpoint URL*, *Token Certificate Finger Print*, *User ID* and *Password*.

If validation fails:

- It may potentially be due to one of the exceptions listed in Section 5.1. Section 5.1 provides details on the possible exceptions as well as how to resolve them. When validation fails, details of the failure will be listed in the '*Status*' box.

If validation is successful:

- The current ADFS Endpoint will be marked as '*Validated'.* This information will not be saved until the user clicks on the '*Save'* menu option.



User ID: Administrator

Password: ••••••••

Status: Error while trying to create channel.:
The HTTP service located at https://eventhorizon.blac

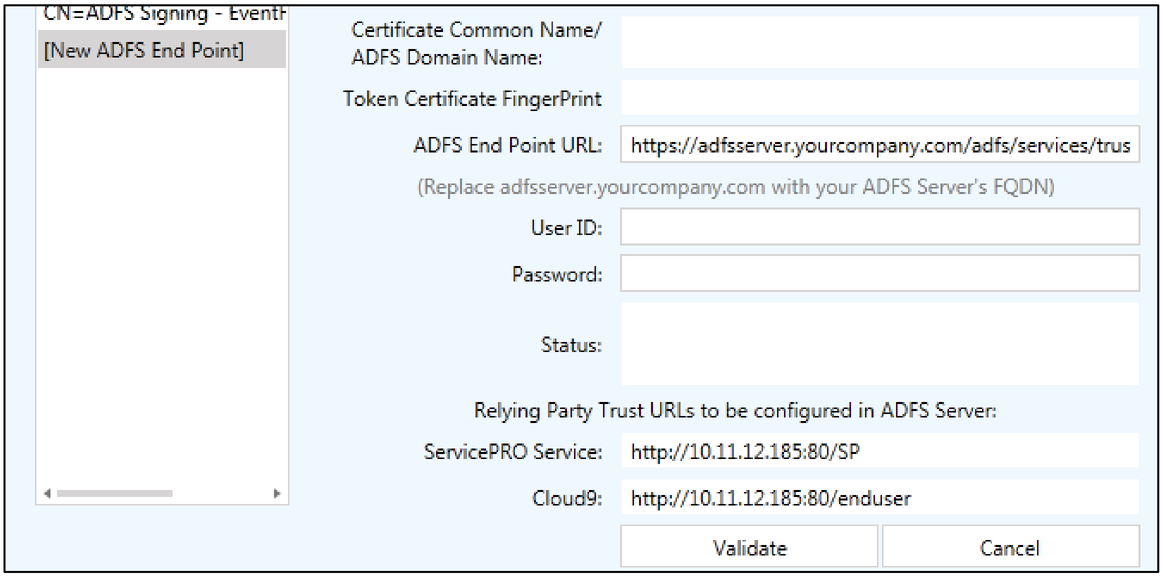
Relying Party Trust URLs to be configured in ADFS Server:

ServicePRO Service: http://10.11.12.185:80/SP

Cloud9: http://10.11.12.185:80/enduser

Cancel

The ‘**Cancel’** button in *Add/Edit of ADFS Endpoint* settings will be visible only when there are multiple ADFS Endpoint settings. When there is only one Endpoint setting, the ‘**Cancel’** button will not be visible, and only ‘**Validate’** will be present.



CN=ADFS Signing - EventH

[New ADFS End Point]

Certificate Common Name/ ADFS Domain Name:

Token Certificate FingerPrint

ADFS End Point URL: https://adfsserver.yourcompany.com/adfs/services/trus

(Replace adfsserver.yourcompany.com with your ADFS Server's FQDN)

User ID:

Password:

Status:

Relying Party Trust URLs to be configured in ADFS Server:

ServicePRO Service: http://10.11.12.185:80/SP

Cloud9: http://10.11.12.185:80/enduser

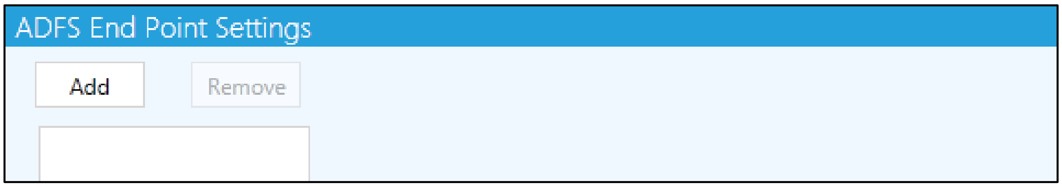
Remove

The **‘Remove’** Endpoint button will be available only under certain circumstances:

A. If ADFS authentication is checked off for either SP or ServicePRO Web:

i. The **Remove** option will be disabled when there is only one Endpoint exists.

ii. The **Remove** option will be enabled if there are multiple Endpoints.



ADFS End Point Settings

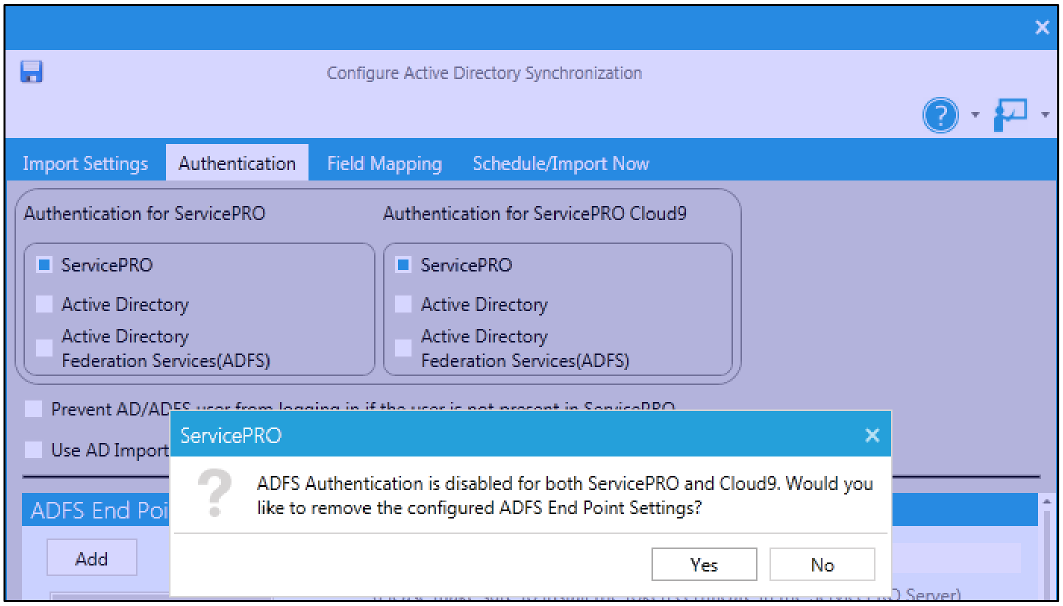
B. When either of the ADFS authentication options is unchecked, the user will be asked if they would like to remove the configured ADFS Endpoint Settings. The following actions will result:

i. If the user says **YES** to remove ADFS Endpoint settings:

- ADFS Endpoint items and settings will be removed. Users will be required to create new Endpoint entries and search for an appropriate ADFS certificate.

ii. If the user says **NO** to the removal of ADFS Endpoint settings:

- The **Remove** option will be enabled, regardless of one or more existing Endpoints.



Authentication for ServicePRO

- ■ ServicePRO
- □ Active Directory
- □ Active Directory Federation Services(ADFS)

Authentication for ServicePRO Cloud9

- ■ ServicePRO
- □ Active Directory
- □ Active Directory Federation Services(ADFS)

□ Prevent AD/ADFS user from logging in if the user is not present in ServicePRO

□ Use AD Import

ServicePRO

ADFS Authentication is disabled for both ServicePRO and Cloud9. Would you like to remove the configured ADFS End Point Settings?

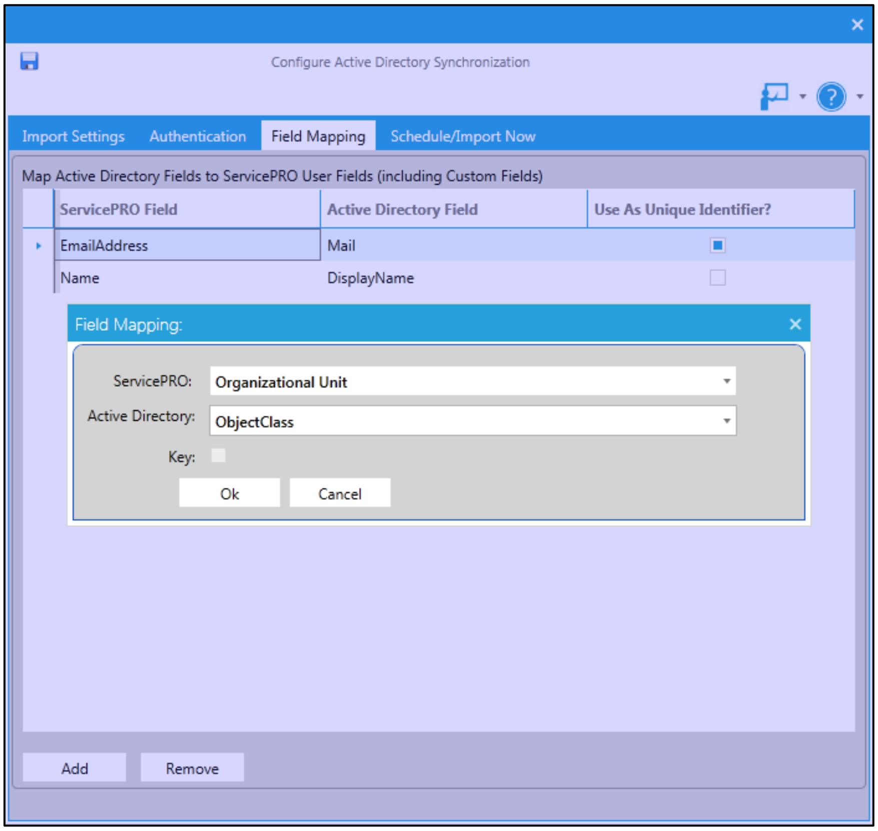
2. If the User has saved settings with ADFS authentication unchecked for both ServicePRO and ServicePRO Web, and if they have retained the Endpoint settings that were configured previously:

   When the user launches the *AD Sync Settings* window:

   - ADFS Endpoint settings will not be visible in the UI, though they are still in the Database (because both the ADFS authentication options are unchecked)
   - If the user now enables ADFS authentication for SP or ServicePRO Web, the UI will show the previously configured ADFS Endpoint settings.

2.3. Changes in Configure Active Directory Sync – ‘Field Mapping’ tab

- In the ‘Field Mapping’ tab, all mentions of ‘ADS’ in text have been changed to ‘Active Directory’.



Map Active Directory Fields to ServicePRO User Fields (including Custom Fields)

ServicePRO Field	Active Directory Field	Use As Unique Identifier?
EmailAddress	Mail	☑
Name	DisplayName	□

ServicePRO: Organizational Unit

Active Directory: ObjectClass

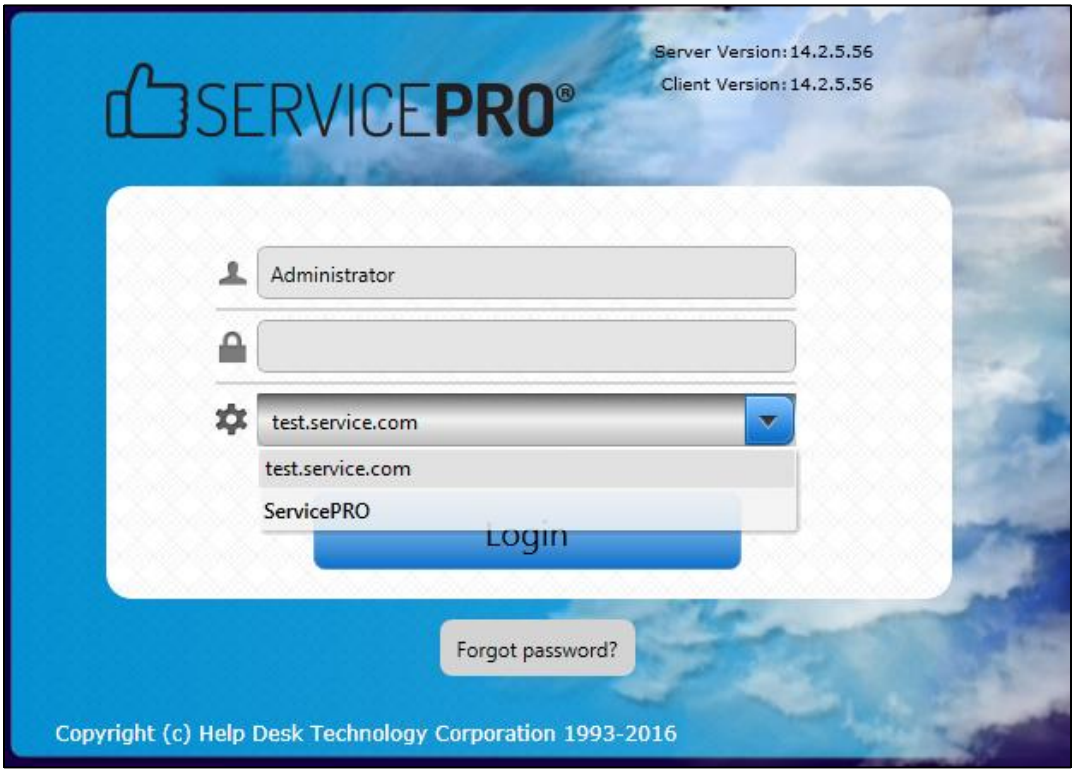
Key: □

- In the 'Field Mapping' view, if the application cannot connect to "AD", such as when the Web server is not connected to the AD domain (public cloud as well as on-premise but application cannot access AD), ServicePRO will display the predefined list of Active Directory fields in the drop down for selecting Active Directory fields.
- In the ‘Field Mapping’ pop-up, drop-down fields will fetch all relevant ServicePRO fields, irrespective of whether the application can connect to AD or not.
- In the ‘Field Mapping’ pop-up view, in the Active Directory drop-down field, the existing behavior will continue to work if the application can connect to AD. If the application cannot connect to AD, it will show the pre-defined list of Active Directory fields in the drop-down for setting up the mapping.

NOTE: The administrator needs to set up claims for all the Active Directory fields that are mapped in the Active Directory Field Mapping Settings in the ADFS Server.

3. Changes in the ServicePRO 'Login' function with respect to ADFS Authentication

- **ServicePRO Login** – If 'Active Directory Federation Services (ADFS)' authentication has been enabled for ServicePRO, the configured ADFS Endpoint(s) or domain name(s) will be listed first in the drop-down list.



Server Version: 14.2.5.56
Client Version: 14.2.5.56

Administrator

test.service.com

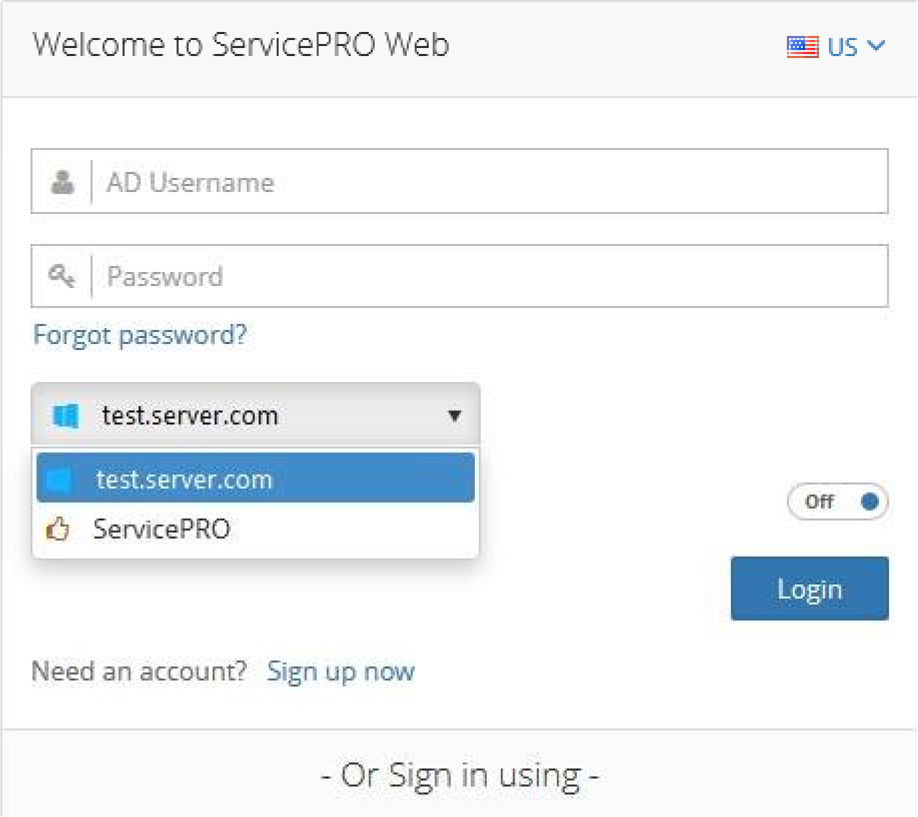
- When **ADFS Endpoint** is selected from the domains drop down:

  1) The User Name can be entered in one of the following ways:
     a. Email Address
     b. Domain\AD User Name [i.e. Domain\SAM Account Name]
     c. AD User Name [i.e. SAM Account Name]
  2) AD Passwords should be entered in the password field.

- User-entered credentials will be authenticated using the selected ADFS Endpoint/ Domain. When the user does not belong to the Primary domain, but belongs to the Trusted domain, then the user name must be entered either using option **a)** or **b)**.
- If the authentication fails, the reason for failure will be logged in a log file and the user will be shown a generic login failed message stating that the 'User Name or Password is incorrect' (Similar to OneLogin Single Sign-On).
- If the authenticated ADFS user is already present in ServicePRO, the user will be logged in immediately.

4. Changes in the ServicePRO Web 'Login' function with respect to ADFS Authentication

- **ServicePRO Web Login** – If 'Active Directory Federation Services (ADFS)' authentication has been enabled for ServicePRO Web, Configured ADFS Endpoint(s) / domain name(s) will be listed first in the drop-down.



- When the ADFS Endpoint is selected in the domain drop down:
  1) User Names can be entered in one of the following ways:
     - Via Email Address
     - Domain\AD User Name (i.e. Domain\SAM Account Name)
     - AD User Name (i.e. SAM Account Name)
  2) AD Password should be entered into the password field.

- User entered credentials will be authenticated using the selected ADFS Endpoint/Domain. When the user belongs to the Trusted domain, and does not belong to the Primary domain, the user name must be entered either using option A or B.
- If the authentication fails, the reason for failure will be logged in a log file, and the user will be shown a generic login failed message stating that 'User Name or Password is incorrect'.
- If the user is already present in ServicePRO, the user will be logged in immediately.

5. Appendix

5.1. Table of Possible ADFS Authentication Exceptions

Sl.No.	Exception Details	Possible reason for Exception	Solution
1	ServerTooBusyException	Turned off the server / ADFS was not running	Log in to the ADFS server and check the relying party URL’s are able to “update from federation metadata”.
2	System.ServiceModel.FaultException	When the Relay Party is disabled / when relay party is missing in the ADFS.	Test MetaData URLs.
3	TimeOutException		Increase the Factory Timeout interval of OpenTimeout property if this happens. Default is one minute. (Used when opening channels when no explicit timeout value is specified)
4	SecurityTokenException	When the thumbprint has Unicode characters or certificate is not in the certificate store.	1. Please check if the clock set correctly (i.e. so that the UTC time is correct [ignore local time, it is largely irrelevant]) - this certainly matters for WCF. 2. Is the certificate still valid? 3. Are you using the correct name from the certificate? 4. Is there a certificate trust chain issue?
5	SecurityNegogationException	When there is some issue with the certificate	Check the certificate is installed in the trusted root store and also check if there is a certificate in the ADFS configuration window (AD FS -> Service -> Certificates) ensure you have a valid certificate that is used for singing the token.
6	The request scope is not valid or is unsupported.	Relying Party URLs are not configured in ADFS	Check the certificate is installed in the trusted root store and Relying Party Trust URLs are configured in ADFS Server

5.2. Pre-defined list of Active Directory fields

The following is a list of pre-defined Active Directory fields that will be shown in drop-down when the application cannot connect to AD. Only the first 6 fields have matching ADFS claims:

Fields with Matching ADFS Claims

Field	Matching ADFS Claim
mail	emailaddress
Name	name
givenName	givenName
telephoneNumber	homephone
pager	otherphone
mobile	mobilephone

Fields *without* Matching ADFS Claims

Field
FacsimiletelephoneNumber
samAccountName
displayName
department
userPrincipalName
StreetAddress
NetworkAddress
UserWorkstations
employeeID

NOTE: For a list of all AD User Object attributes, please consult this page:

http://www.kouti.com/tables/userattributes.htm

5.3. Minimum Claims to be configured for successful ADFS SSO authentication

The following are the minimum claims needed to be configured for successful ADFS SSO authentication:

1. LDAP Attribute -> Outgoing Claim
2. SAM-Account-Name -> Name,
3. User-Principal-Name -> Email Address,
4. Display-Name -> Given Name.