SSO (Single Sign-On)

Configuration Guide

DocuPhase 6.2 (or later)

Last Revised: November 5, 2019

DISCLAIMER

These recommendations are only provided as a general point of reference for system installations, and may need to be adjusted to meet the demands of your specific situation.

DocuPhase has made every effort to ensure that this document is accurate;
DocuPhase disclaims liability for any inaccuracies or omissions.

Information in this document is subject to change without notice and
does not represent commitment on the part of DocuPhase.

If you find information in this document that is incorrect, misleading, or incomplete,
we would appreciate your comments and suggestions.

Table of Contents

1. Revision History

Item #	Release #	Revision Date	Description	Tracking Notes
005	6.3 and later	11/05/19	Removed commenting that was inadvertently left in.	kb
004		10/14/19	Complete re-work of the document to include more specific information about Authentication set up.	FLopez/Dev Authentication Article - Confluence
003	ALL	09/23/19	Update styles as per new style guide (all pages)	KBennett
002			Add checklist for correct configuration (on page 15)	AWay
001	6.3 and later	05/01/19	Added instructions for workaround for enabling IIS App Pool Anonymous Authentication (see page16)	US29923/ EAllen/TW 4
000	ALL	04/25/18	Original	US29396

Introduction

Purpose of this Guide

As more and more organizations require a single sign-on solution, DocuPhase has continued to develop its product to accommodate this growing need – in all its variations. This document has been created and is intended for technical software professionals who want to perform configuration Single Sign-On capability for a client, as well as for Clients who want to do their own SSO configuration.

IMPORTANT!
As of version 6.1, the name of the iSynergy platform was changed to DocuPhase. You may notice some updates and revised files paths have been updated to reflect this change.

Please review the 6.1 Release Notes (in online help or via the DocuPhase Learning Library: https://training.docuphase.com/lesson/docuphase-platform-6-1-release-notes) for more information about the name change.

Overview

SSO (Single Sign-On) refers to the ability to log into one place, then have those same credentials automatically applied to another software system: preventing users from having to re-authenticate every time the secondary site is accessed.

DocuPhase currently offers the following SSO options and configuration information for the following:

- ✓ **Microsoft Windows** (with/without ADIS)
- ✓ **Active Directory Federated Services (ADFS)** – Version 6.1 and later
- ✓ **Security Assertion Markup Language (SAML)** – Version 6.2 and later

TIPS
In this document, you will see the following two terms:

- *Identity Provider (IdP) refers to a software system that performs an authentication, then passes a token to the system: providing access to the user (e.g., Onelogin, ADFS/INOVA, Okta, and AzureAD are all Identity Providers).*
- *Service Provider (SP) refers to the Target software system the user wants to access (e.g., DocuPhase is the Service Provider).*

Assumptions

The following must be true in order to successfully configure and implement SSO:

- ✓ Personnel assigned to this task is **familiar with ADFS Configuration** (if not, go to www.microsoft.com for details).
- ✓ **Server Prerequisites** have been installed (refer to DocuPhase Standard Requirements Specification Guide.
- ✓ The **DocuPhase platform** is installed and successfully tested as http.
- ✓ An **SSL certificate** has been purchased and configured for DocuPhase.
- ✓ **Notepad ++ (run as an administrator)** is to be used when editing config files.

**Go to https://en.wikipedia.org/wiki/Certificate_authority for more information about certificates and how to obtain them*

.

MS Windows Authentication

DocuPhase Supports Windows Authentication via IIS Configuration, as described below.

IMPORTANT!

- ***Make sure DocuPhase has been configured for SSO (see Appendix A, on page 18).***
- ***Once authentication has been configured, be sure to synchronize DocuPhase Users (see Appendix B, on page 18)***

In IIS Manager

1) Find and select the appropriate Web Site (usually the Default).

In the IIS Section:

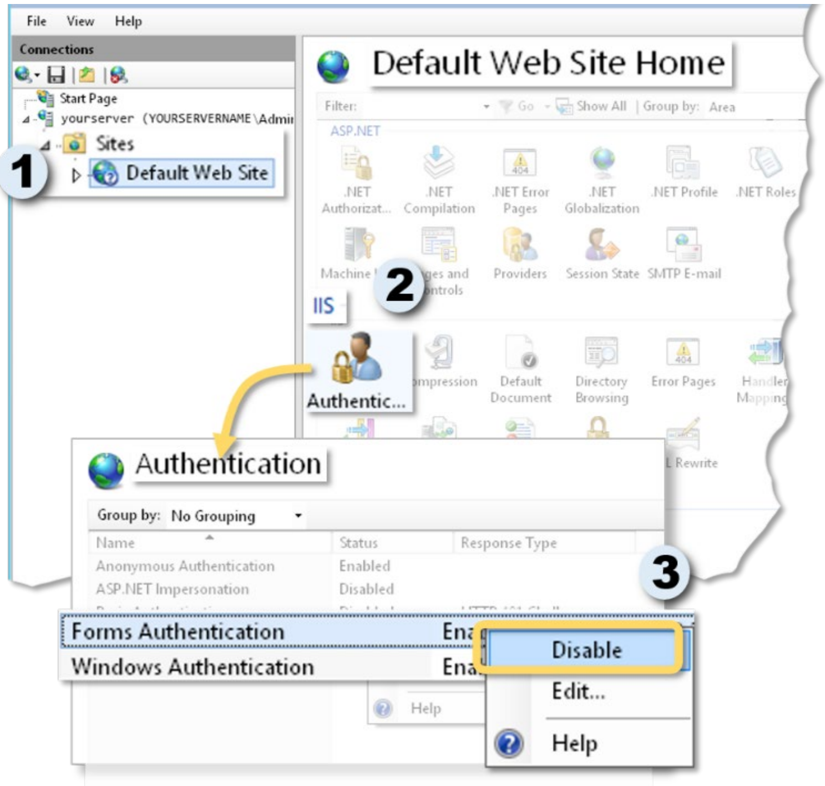
2) Double-click (Authentication) to display the Authentication settings window.

In the Authentication settings window:

3) Make the following settings:
   - ✓ Disable the Forms Authentication
   - ✓ Enable the Windows Authentication

NOTE

Option: If ADS is being used, configure DocuPhase ADS Syncing via ADIS Manager

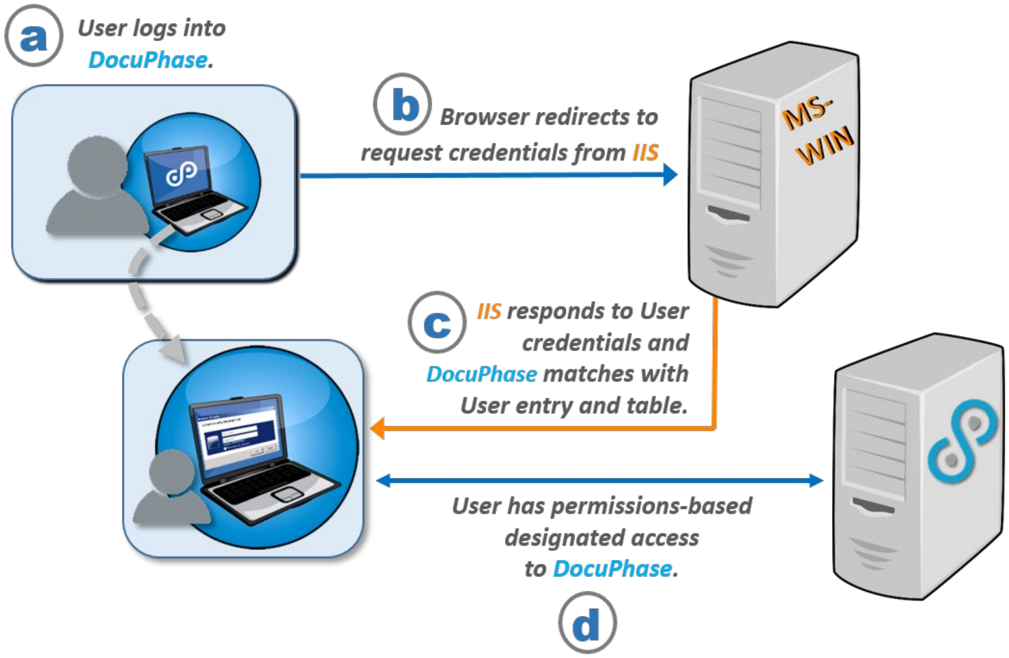


Authentication

Group by: No Grouping

Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Forms Authentication	Ena	
Windows Authentication	Ena	

Summary: When DocuPhase is Configured Correctly for Windows


a
User logs into DocuPhase.
b
Browser redirects to request credentials from IIS
MS-WIN
c
IIS responds to User credentials and DocuPhase matches with User entry and table.
User has permissions-based designated access to DocuPhase.
d

a) The User navigates to, and logs into the DocuPhase web application (i.e., Service Provider) via HTTPS in browser

b) The browser redirects the log in information/credentials to the Windows server for authentication.

c) If/when the Windows server verifies the credentials, a token is sent to notify the DocuPhase server that the User is authorized to use DocuPhase.

d) Once DocuPhase receives the token, the User then has the pre-defined, permissions-based access to DocuPhase.

Claims Authentication – Active Directory Federation Services (ADFS)

DocuPhase supports WS-Federation Claims-based authentication (i.e., authenticating that users are who they claim to be) through ADFS. Active Directory Federation Services (ADFS) is a software component developed by Microsoft, and run on Windows Server operating systems: providing single sign-on access to systems and applications used across an organization. It authenticates users by a combination of usernames and passwords.

IMPORTANT!

- ***Make sure DocuPhase has been configured for SSO (see Appendix A, on page 18).***
- ***Make sure you have at least 1 valid SSL certificate before proceeding (please refer to the DocuPhase SSL Configuration Guide).***
- ***Once authentication has been configured, be sure to synchronize DocuPhase Users (see Appendix B, on page 18)***

The process for configuring DocuPhase to work with ADFS as a WS-Federation claims authentication service includes the following:

A) Set up ADFS in SQL Server (see page 4)

B) Add Relying Party Trusts Identifier (see page 5)

C) Add Passive Endpoint (see page 6)

D) Add a Claim Rule (see page 7)

E) Set the Authentication (see page 8)

F) Make Changes in DocuPhase Directory (see page 9)

G) Add sso.htm to Root Directory (see page 10)

H) Edit the DocuPhase Web Application Config File (see page 10)

I) Match Certificate Thumbprint (see page 12)

A) Set Up ADFS for SQL Server:

Set up ADFS, and make sure you have at least 1 valid SSL certificate before proceeding.

TIPS

For more information, refer to the following:

- *https://docs.microsoft.com/en-us/windows-server/identity/active-directory-federation-services*
- *The current DocuPhase SSL Configuration and Implementation Guide).*

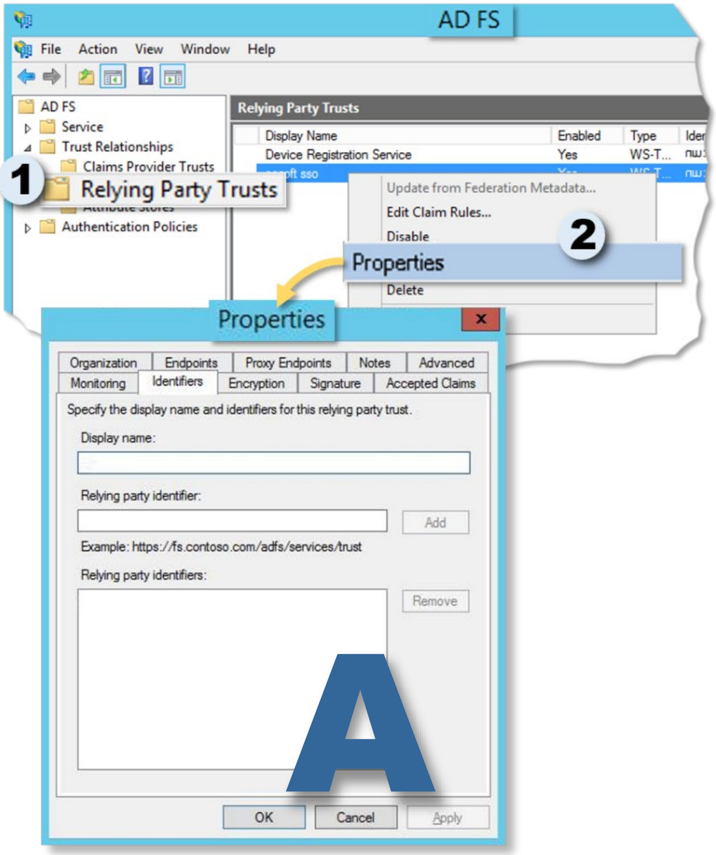
Once ADFS is Set Up with a Valid SSL Certificate:

In the ADFS Directory ⦣

1) Select the **Relying Party Trusts** folder to display the ***Relying Party Trusts*** window.

In the Relying Party Trusts window:

2) Right-click to display a **Properties** dialog, then complete sections B through J, as shown below.



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

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

B) Add Relying Party Trusts Identifier

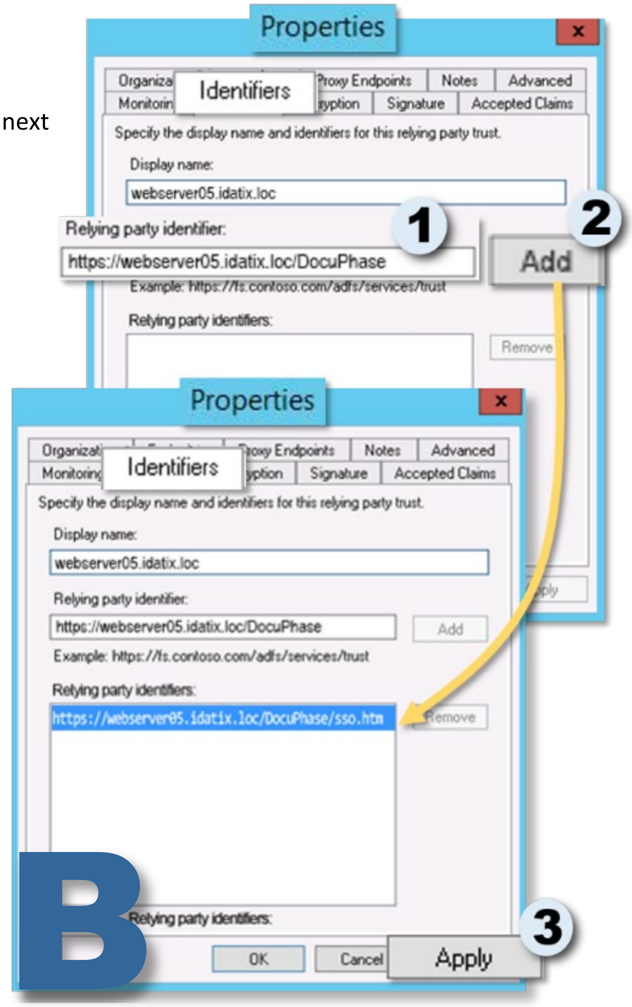
, On the Identifiers tab of the Properties Dialog:

In the Relying Party Identifier field:

1) Enter the URL of the DocuPhase web server.

2) Click Add to add the URL to the list of Relying Party Identifiers.

3) Click Apply to save the setting before you to onto the next tab without closing the ***Properties*** dialog.



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

Display name: webserver05.idatix.loc

Relying party identifier: https://webserver05.idatix.loc/DocuPhase

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

Relying party identifiers: https://webserver05.idatix.loc/DocuPhase/sso.htm

NOTE

If you click OK, settings are saved, but the Properties dialog closes

For more information about Relying Party Trusts, refer to the following:

- *https://docs.microsoft.com/en-us/windows-server/identity/active-directory-federation-services*
- *The current DocuPhase SSL Configuration and Implementation Guide).*

C) Add Passive Endpoint

On the Endpoints tab of the Properties dialog:

1) Click Add WS-Federation... to display the Edit Endpoint dialog.

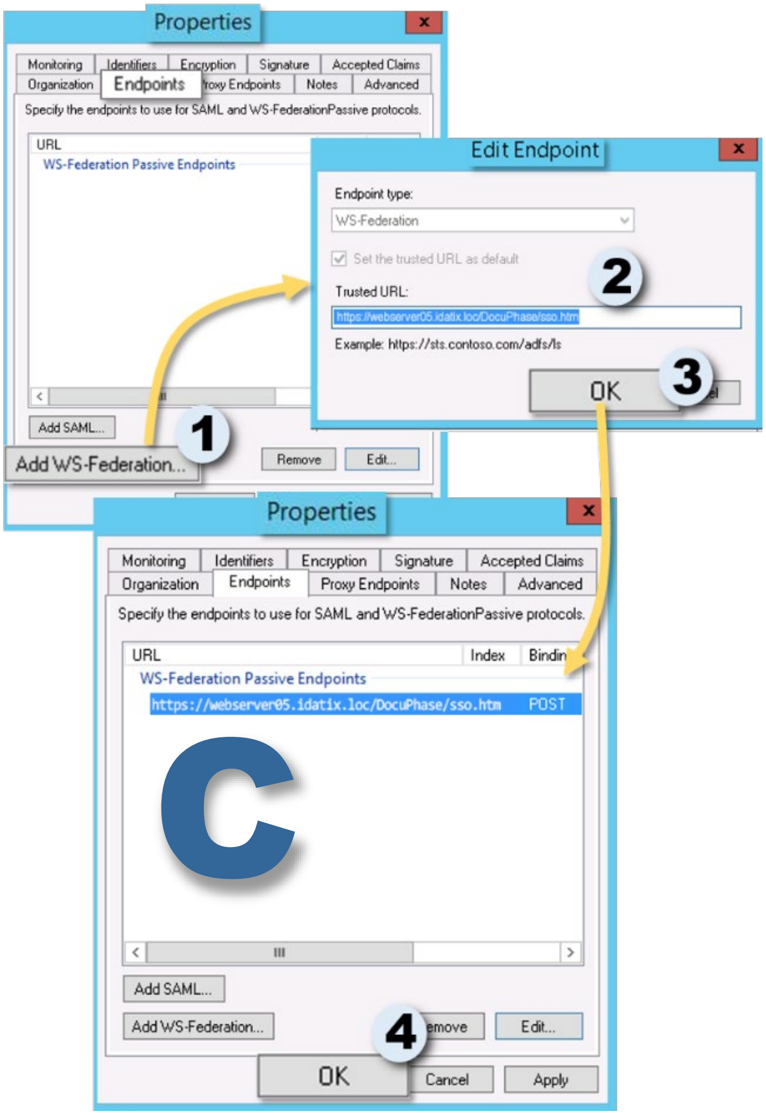
In the Edit Endpoint dialog:

2) Enter the designated sso.htm page (see page 10 for more information).

3) Click OK to close the **Edit *Endpoint*** dialog and return to the ***Endpoints*** tab of the ***Properties*** dialog, with the newly added URL now in the list.

On the Endpoints tab of the Properties dialog:

4) Click OK to save the setting, close the ***Properties*** dialog.



Endpoint type: WS-Federation

☑ Set the trusted URL as default

Trusted URL: https://webserver05.idatix.loc/DocuPhase/sso.htm

Example: https://sts.contoso.com/adfs/ls

Specify the endpoints to use for SAML and WS-FederationPassive protocols.

URL	Index	Binding
WS-Federation Passive Endpoints		
https://webserver05.idatix.loc/DocuPhase/sso.htm		POST

D) Add a Claim Rule

In the list of Relying Party Trust in the ADFS directory:

1) Right-click on the **Trust Identifier** you added previously (see page 5) to display a list of options.

From the list of options:

2) Select Edit Claim Rules… to display the *Edit Claim Rules* dialog.

On the Issuance Authorization Rules tab of the Edit Claim Rules dialog:

3) Click Add Rule... .to display the ***Edit Rule*** dialog.

On the Edit Rule dialog:

4) Make sure **Name** and **UPN** are selected as the ***Outgoing Claim Type*** for the ***User Principal Name***.

5) Select the E-Mail Address for the *Outgoing Claim Type* for the *E-Mail Address*.

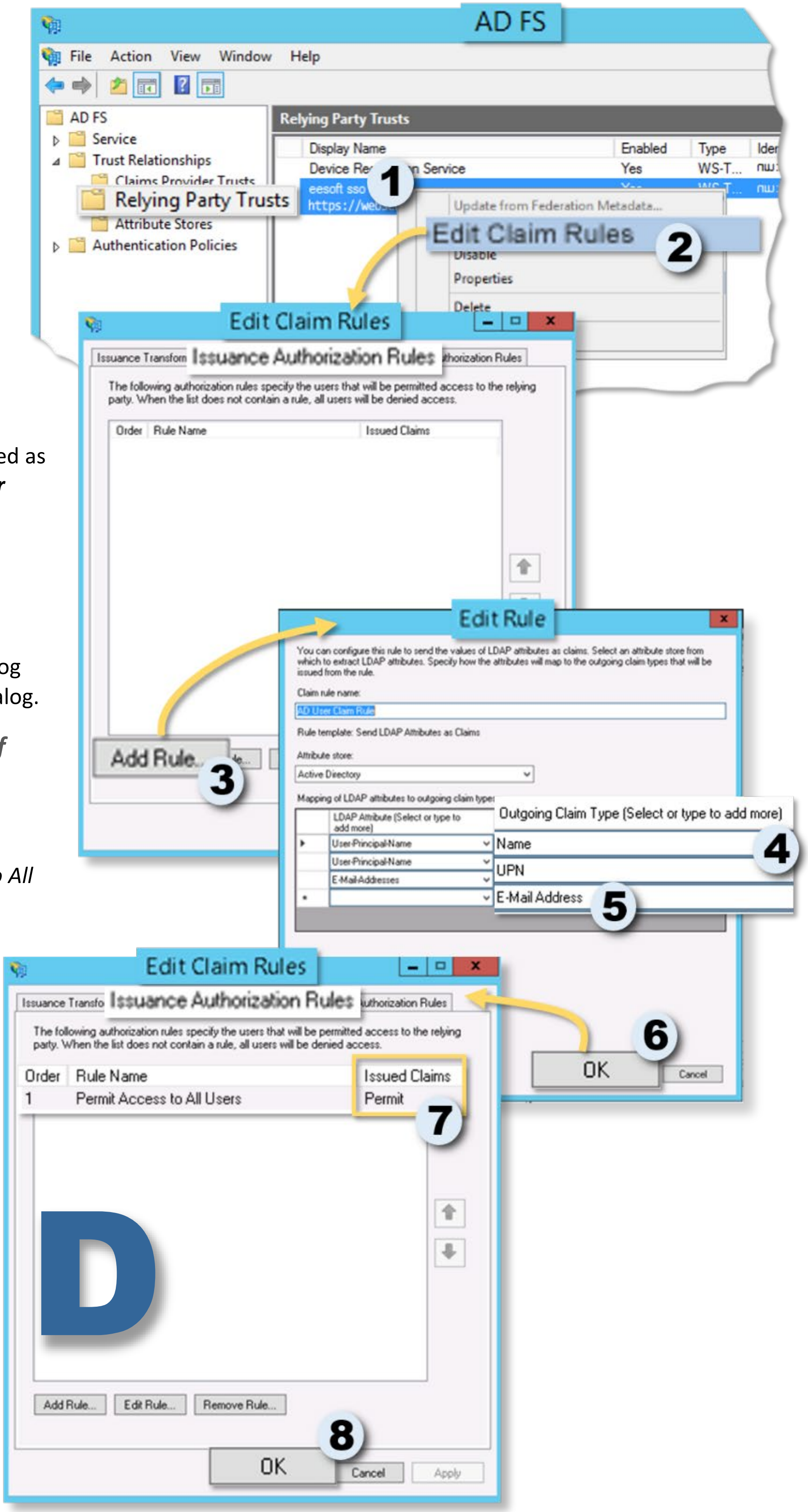
6) Click OK to close the ***Edit Rule*** dialog and return to the ***Edit Claim Rules*** dialog.

On the Issuance Authorization Rules tab of theEdit Claim Rules dialog:

In the Issued Claims field:

7) Select Permit for the *Permit Access to All Users* rule.

8) Click OK to save the settings and close the ***Edit Claims Rules*** dialog.



The following authorization rules specify the users that will be permitted access to the relying party. When the list does not contain a rule, all users will be denied access.

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:

AD User Claim Rule

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

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)
▸	User-Principal-Name	Name
	User-Principal-Name	UPN
	E-Mail-Addresses	E-Mail Address
*		

Order	Rule Name	Issued Claims
1	Permit Access to All Users	Permit

E) Set Authentication

There are two Authentication policies that must be set:

- ✓ **Authentication Policies**
- ✓ **Anonymous Authentication**

E1) Setting Authentication Policies

In order to make the ADFS authentication work within windows applications and with Internet Explorer, you must set the authentication policies within ADFS as follows:

In the ADFS Directory ⦥

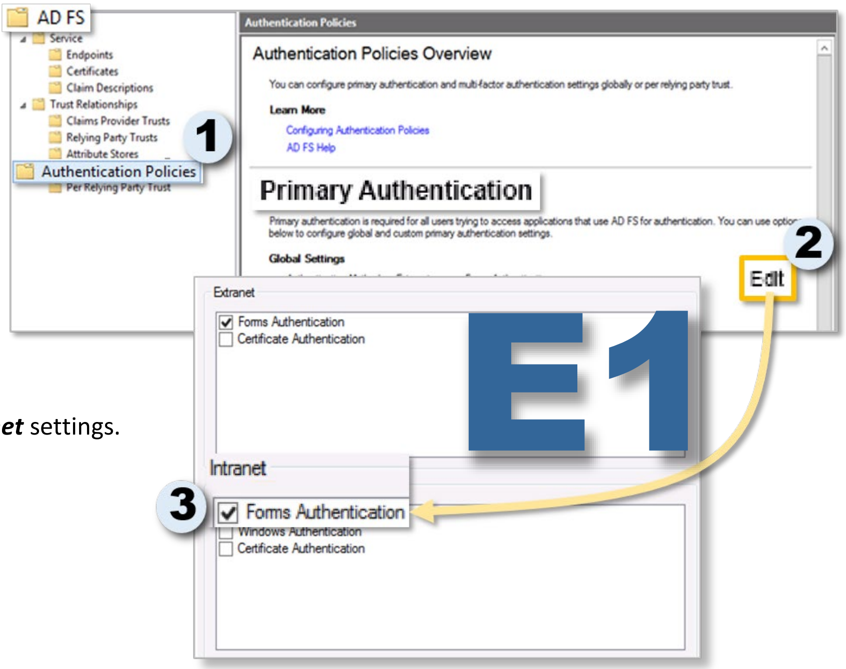
1) Select the Authentication Policies folder to display the *Authentication Policies Overview* window

In the Authentication Policies Overview window:

2) Click **Edit** to display the ***Extranet*** and ***Intranet*** settings.

In the Intranet section:

3) Enable (☑) Forms Authentication.



Authentication Policies Overview

You can configure primary authentication and multi-factor authentication settings globally or per relying party trust.

Primary Authentication

Primary authentication is required for all users trying to access applications that use AD FS for authentication. You can use options below to configure global and custom primary authentication settings.

Extranet
☑ Forms Authentication
☐ Certificate Authentication

Intranet
☑ Forms Authentication
☐ Windows Authentication
☐ Certificate Authentication

E2) Enabling Anonymous Authentication

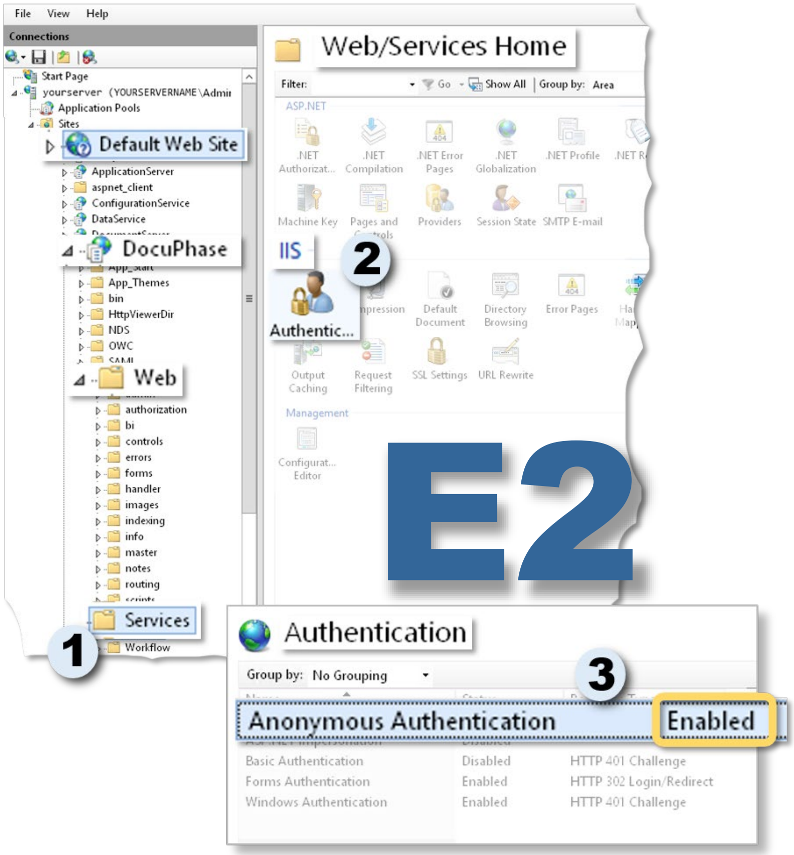
The Anonymous Authentication must be enabled so that DocuPhase server IIS app pool can accept the DocuPhase windows service login for HTML5 cache clearing:

1) Go to Web Site ▶ DocuPhase ▶ Web ▶ Services.

Under the DocuPhase Server name in IIS Manager, in the Web Services Home window:

2) Double-click **Authentication** to display corresponding settings.

3) Make sure that the **Anonymous Authentication** is **Enabled**, but all other Authentication settings are Disabled.



Anonymous Authentication	Enabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Enabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

F) Change Default Document(s)

Changing the Default Document (as described below) is necessary to force all incoming traffic through the Access.aspx page (by default).

1) Go to Web Site ▶ DocuPhase ▶ Web ▶ Services.

Under the DocuPhase Server name in IIS Manager, in the Web Services Home window:

2) Double-click Default Document to display the corresponding window.

In the Default Document window:

3) Right-click on the ***Default Document*** to display a list of options, then click **X Remove** to display a confirmation prompt.

In the confirmation prompt:

4) Click Yes to delete the selected default document, close the prompt, and return to the ***Default Document*** window.

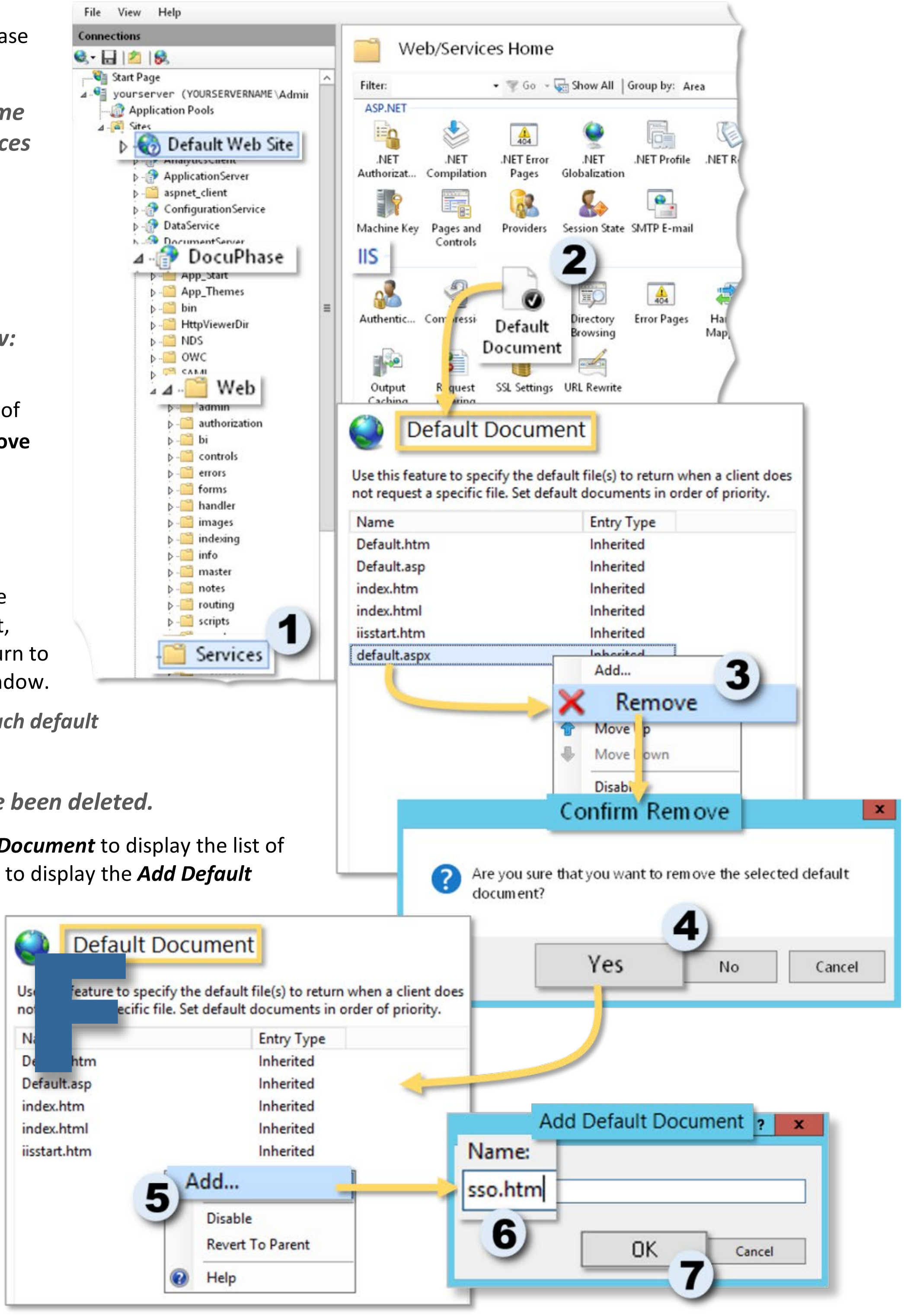
Repeat steps 5 and 6 for each default document in the list.

Once all default documents have been deleted.

5) Right-click on the ***Default Document*** to display the list of options, then select **Add...** to display the ***Add Default Document*** dialog.

6) Enter **"sso.htm"** as the default document

7) Click OK to save the new default document, and close the dialog**.**



Default Document

Use this feature to specify the default file(s) to return when a client does not request a specific file. Set default documents in order of priority.

Name	Entry Type
Default.htm	Inherited
Default.asp	Inherited
index.htm	Inherited
index.html	Inherited
iisstart.htm	Inherited
default.aspx	Inherited

Are you sure that you want to remove the selected default document?

Name: sso.htm

G) Create and add an sso.htm to Root Directory of DocuPhase Server

1) Create the sso.htm file with the following contents:

```
<!DOCTYPE HTML>
<html lang="en-US">
    <head>
        <meta charset="UTF-8">
        <meta http-equiv="refresh" content="0; url=web/authorization/Access.aspx">
        <script type="text/javascript">
            window.location.href = "web/authorization/Access.aspx"
        </script>
        <title>Page Redirection</title>
    </head>
    <body>
    </body>
</html>
```

2) Add the **sso.htm** file to the root directory for DocuPhase Server (e.g., C:\Program Files\DocuPhase\DocuPhase Server).

H) Edit the DocuPhase Web Application Config File

In the DocuPhase Server web.config file (generally located here: C:\Program Files\DocuPhase\DocuPhase Server):

Make the following changes:

	Starting at Line(s)	Action	Content for Change

1)	10
	and
	11
		Uncomment lines 10 and 11	`<!--****************************************************`
			`** Sections needed for Claims Authentication *`
			`****************************************************-->`
			`<section name="system.identityModel" type="System.IdentityModel.Configuration.SystemIdentityModelSection, System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=B77A5C561934E089" />`
			`<section name="system.identityModel.services" type="System.IdentityModel.Services.Configuration.SystemIdentityModelServicesSection, System.IdentityModel.Services, Version=4.0.0.0, Culture=neutral, PublicKeyToken=B77A5C561934E089" />`

2)	99	Set the following:
		✓ authentication mode = none
		✓ defaultUrl to Access.aspx:
			`<!--****************************************************`
			`** For Claims Authentication set the mode to None **`
			`****************************************************-->`
			`<authentication mode="None">`
			`<forms loginUrl="web/authorization/Access.aspx" defaultUrl="web/authorization/Access.aspx" protection="Validation" timeout="120" slidingExpiration="true" requireSSL="false" />`
			`</authentication>`

Edit the DocuPhase Web Application Config file (continued on next page)

Edit the DocuPhase Web Application Config file (continued)

	Starting at Line(s)	Action	Content for Change

3)	269	Uncomment to include modules	`<!--`
			`****************************************************************`
			`** When enabling Claims authentication uncomment these modules. **`
			`****************************************************************-->`
			`<add name="RedirectFederationAuthenticationModule" type="iDatix.Web.RedirectFederationAuthenticationModule" />`
			`<add name="SessionAuthenticationModule" type="System.IdentityModel.Services.SessionAuthenticationModule, System.IdentityModel.Services, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" preCondition="managedHandler" />`

4)	300	Uncomment the section and edit the data*
		(highlighted in yellow)
		*
			`<!--****************************************************`
			`** For Claims Authentication set the mode to None **`
			`****************************************************-->`
			`<location path="FederationMetadata">`
			`<system.web>`
			`<authorization>`
			`<allow users="*" />`
			`</authorization>`
			`</system.web>`
			`</location>`
			`<system.identityModel>`
			`<identityConfiguration>`
			`<audienceUris>`
			`<add value="https://idatix056.idatix.loc/DocuPhase/" />`
			`</audienceUris>`
			`<issuerNameRegistry type="System.IdentityModel.Tokens.ConfigurationBasedIssuerNameRegistry, System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">`
			`<trustedIssuers>`
			`<add thumbprint="da72de2b19ae0786ee782ee9330637a67dfd59ef" name="https://domain.idatix.loc/ADFS/services/trust" />`
			`</trustedIssuers>`
			`</issuerNameRegistry>`
			`<certificateValidation certificateValidationMode="None" />`
			`</identityConfiguration>`
			`</system.identityModel>`
			`<system.identityModel.services>`
			`<federationConfiguration>`
			`<cookieHandler requireSsl="false" />`
			`<wsFederation passiveRedirectEnabled="true" issuer="https://domain.idatix.loc/ADFS/ls" realm="https://idatix056.idatix.loc/DocuPhase/" requireHttps="false" />`
			`</federationConfiguration>`
			`</system.identityModel.services>`

**domain.idatix.loc is the host name of the ADFS server and idatix056.idatix.loc is the host name of the DocuPhase web server .*

I) Confirm that the ADFS Certificate Thumbprint Matches

ADFS Single Sign-on only works when the ADFS Thumbprint matches the one that's in the DocuPhase Server web.config file :

1) Go to ***AD FS Manager*▶*ADFS Service*▶*Certificates***.

In the Certificates window:

2) Right-click the primary token signing certificate to display a list of options, then choose **View Certificate** to display the **Certificates** dialog.

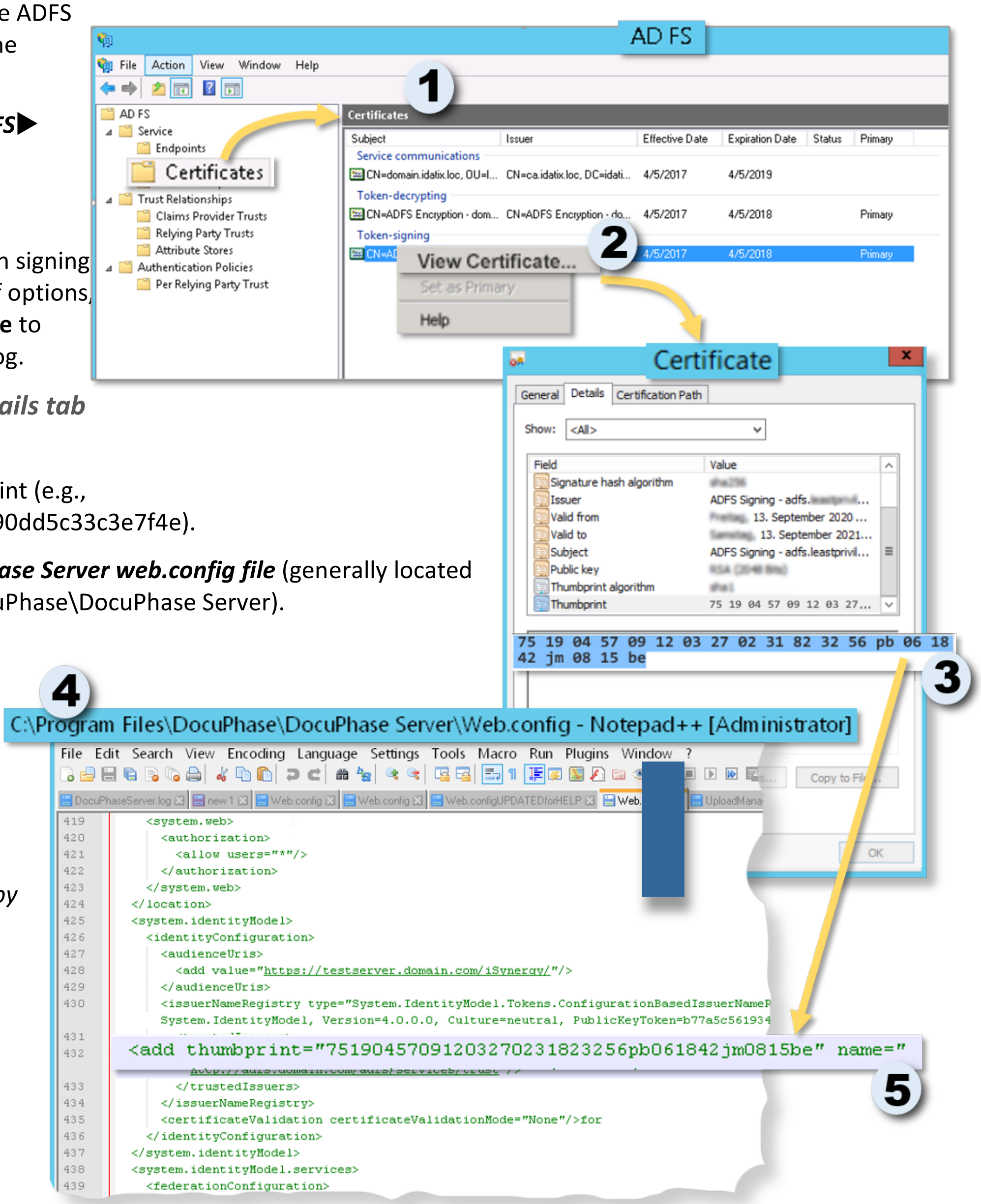
In the Thumbprint field of the Details tab of the Certificates dialog:

3) View and copy the thumbprint (e.g., 5730d7cd5d4003c468120590dd5c33c3e7f4e).

4) Go to and open the ***DocuPhase Server web.config file*** (generally located here: C:\Program Files\DocuPhase\DocuPhase Server).

DocuPhase Server web.config file

5) Find the thumbprint value and make sure it matches the thumbprint of the ADFS Token Signing certificate you just viewed (step 2 above).
   - *If it does not match, copy and paste the thumbprint from the **Certificates Details** tab (step 2 above).*


AD FS
File Action View Window Help
1
AD FS
Service
Endpoints
Certificates
Trust Relationships
Claims Provider Trusts
Relying Party Trusts
Attribute Stores
Authentication Policies
Per Relying Party Trust
Certificates
2
View Certificate...
Set as Primary
Help
Certificate
General Details Certification Path
Show: <All>
3
4
C:\Program Files\DocuPhase\DocuPhase Server\Web.config - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
DocuPhaseServer.log new 1 Web.config Web.config Web.configUPDATEDforHELP Web. UploadMana
Copy to File...
OK
5

Subject	Issuer	Effective Date	Expiration Date	Status	Primary
Service communications					
CN=domain.idatix.loc, OU=I...	CN=ca.idatix.loc, DC=idati...	4/5/2017	4/5/2019		
Token-decrypting					
CN=ADFS Encryption - dom...	CN=ADFS Encryption - do...	4/5/2017	4/5/2018		Primary
Token-signing					
CN=AD		4/5/2017	4/5/2018		Primary

Field	Value
Signature hash algorithm	
Issuer	ADFS Signing - adfs....
Valid from	13. September 2020 ...
Valid to	13. September 2021...
Subject	ADFS Signing - adfs.leastprivil...
Public key	
Thumbprint algorithm	
Thumbprint	75 19 04 57 09 12 03 27...

```
75 19 04 57 09 12 03 27 02 31 82 32 56 pb 06 18
42 jm 08 15 be
```

```
    <system.web>
      <authorization>
        <allow users="*"/>
      </authorization>
    </system.web>
  </location>
  <system.identityModel>
    <identityConfiguration>
      <audienceUris>
        <add value="https://testserver.domain.com/iSynergy/"/>
      </audienceUris>
      <issuerNameRegistry type="System.IdentityModel.Tokens.ConfigurationBasedIssuerNameR
      System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934
<add thumbprint="751904570912032702318232 56pb061842jm0815be" name="
        </trustedIssuers>
      </issuerNameRegistry>
      <certificateValidation certificateValidationMode="None"/>for
    </identityConfiguration>
  </system.identityModel>
  <system.identityModel.services>
    <federationConfiguration>
```

IMPORTANT!

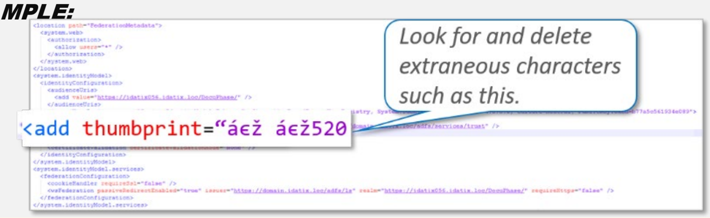
- ***Remember, if the Thumbprint does not match, ADFS Single Sign-on-will not work.***
- ***When you copy and paste the Thumbprint from the Windows Certificate window, there may be extra characters/elements that get copied as well. To make sure you have just the appropriate information copied, use the following procedure to verify that you have the appropriate code copied and pasted.***

a) Open the file in Notepad++.

b) Go to Select Encoding▶ Encode in ANSI.

c) Remove any extraneous characters (see Example below)

EXAMPLE:

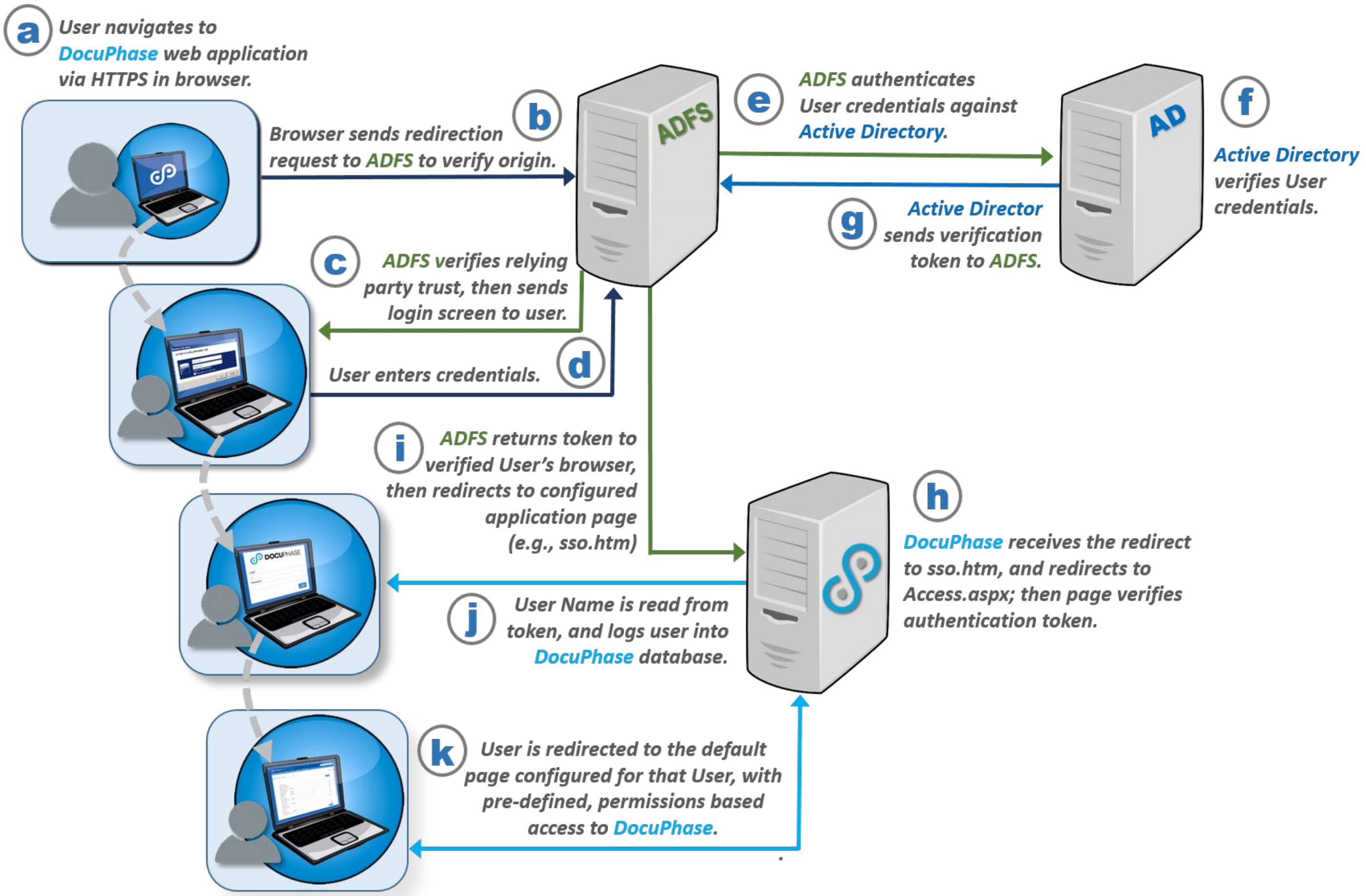


Look for and delete extraneous characters such as this.

```
<location path="FederationMetadata">
  <system.web>
    <authorization>
      <allow users="*" />
    </authorization>
  </system.web>
</location>
<system.identityModel>
  <identityConfiguration>
    <audienceUris>
      <add value="https://idatix056.idatix.loc/DocuPhase/" />
    </audienceUris>
<add thumbprint="áєž áєž520
  </identityConfiguration>
</system.identityModel>
<system.identityModel.services>
  <federationConfiguration>
    <cookieHandler requireSsl="false" />
    <wsFederation passiveRedirectEnabled="true" issuer="https://domain.idatix.loc/adfs/ls" realm="https://idatix056.idatix.loc/DocuPhase/" requireHttps="false" />
  </federationConfiguration>
</system.identityModel.services>
```

Summary Diagram: When DocuPhase is Configured Correctly for ADFS

The flow of control for DocuPhase authentication with ADFS properly configured looks like this:


a
User navigates to DocuPhase web application via HTTPS in browser.
b
Browser sends redirection request to ADFS to verify origin.
ADFS
e
ADFS authenticates User credentials against Active Directory.
AD
f
Active Directory verifies User credentials.
g
Active Director sends verification token to ADFS.
c
ADFS verifies relying party trust, then sends login screen to user.
d
User enters credentials.
i
ADFS returns token to verified User's browser, then redirects to configured application page (e.g., sso.htm)
h
DocuPhase receives the redirect to sso.htm, and redirects to Access.aspx; then page verifies authentication token.
j
User Name is read from token, and logs user into DocuPhase database.
k
User is redirected to the default page configured for that User, with pre-defined, permissions based access to DocuPhase.

a) The User Navigates to DocuPhase web application (i.e., Service Provider) via HTTPS in browser

b) ADFS receives a redirection request from the browser, and verifies the origin of the request

c) If the origin of the request is configured as a relying party trust within ADFS (– see Section B, on page 5), ADFS displays the login screen to the user; otherwise an error appears.

d) When the ADFS Login screen appears, the User logs in with credentials.

e) ADFS sends credentials to Active Directory for authentication.

f) Active Directory checks and authenticates the User's credentials.

g) If the user is authenticated, ADFS sends an authentication token (in the form of a cookie) to the User's browser; then issues a redirect to the application page configured within ADFS (e.g., for DocuPhase it redirects to sso.htm – see Section G, on page 10)

h) When DocuPhase receives the redirect to sso.htm, the application immediately redirects to Access.aspx; the page then verifies that a valid authentication token exists.

i) If the authentication is verified, ADFS sends the token to the verified User's browser, after which the browser is redirected to configured application page (e.g., sso.htm – see Section G, on page 10), and attempts to log in that user to the DocuPhase database.

j) DocuPhase reads the User Name is read from token, User entry existence in the DocuPhase Database is verified, and the User is logged into DocuPhase.

k) The User is redirected to the default page configured, and then has to pre-defined and permissions-based access to DocuPhase.

SAML Configuration - Version 6.2 (and later)

The Security Assertion Markup Language (SAML) is used to allow security log in information to be shared between two or more computers across a network: letting one computer perform certain security functions for one or more devices. It performs two roles:

- ✓ **Authentication**: Confirming that users are who they say they are
- ✓ **Authorization**: Confirming that users have rights/permissions to access certain systems or content

DocuPhase has developed SAML integration for customers who require Commercial Off-The-Shelf (COTS) packages to support single sign-on: giving their IT staff a centralized way to manage users and permissions.

IMPORTANT!
SAML must be configured for DocuPhase BEFORE any SAML-based Identity Provider can be configured to work with DocuPhase for Single Sign-On.

NOTE

References to "{mycompany}.docuphase.com" indicate a general pattern (not literal use) when setting configurations.

EXAMPLE

If your company's DocuPhase address is orgname.docuphase.com/docuphase, then use "orgname" in place of {mycompany} in the instructions on the following pages.

The process for configuring DocuPhase to work with SAML includes the following:

A) **SAML Configuration for the Identity Provider System (see below))**

B) **DocuPhase Service Provider Configuration (see page 28)**

A) Identity Provider Configuration

For Single Sign-on in DocuPhase, you can configure any of the Identity Providers listed below:

- **Azure AD (see page Appendix B1 on page 19)**
- **Okta (see page Appendix B2 on page 21)**
- **onelogin (see page Appendix B3 on page 24)**

IMPORTANT!
For any Identity Provider not listed above, please contact DocuPhase for assistance (see page 17).

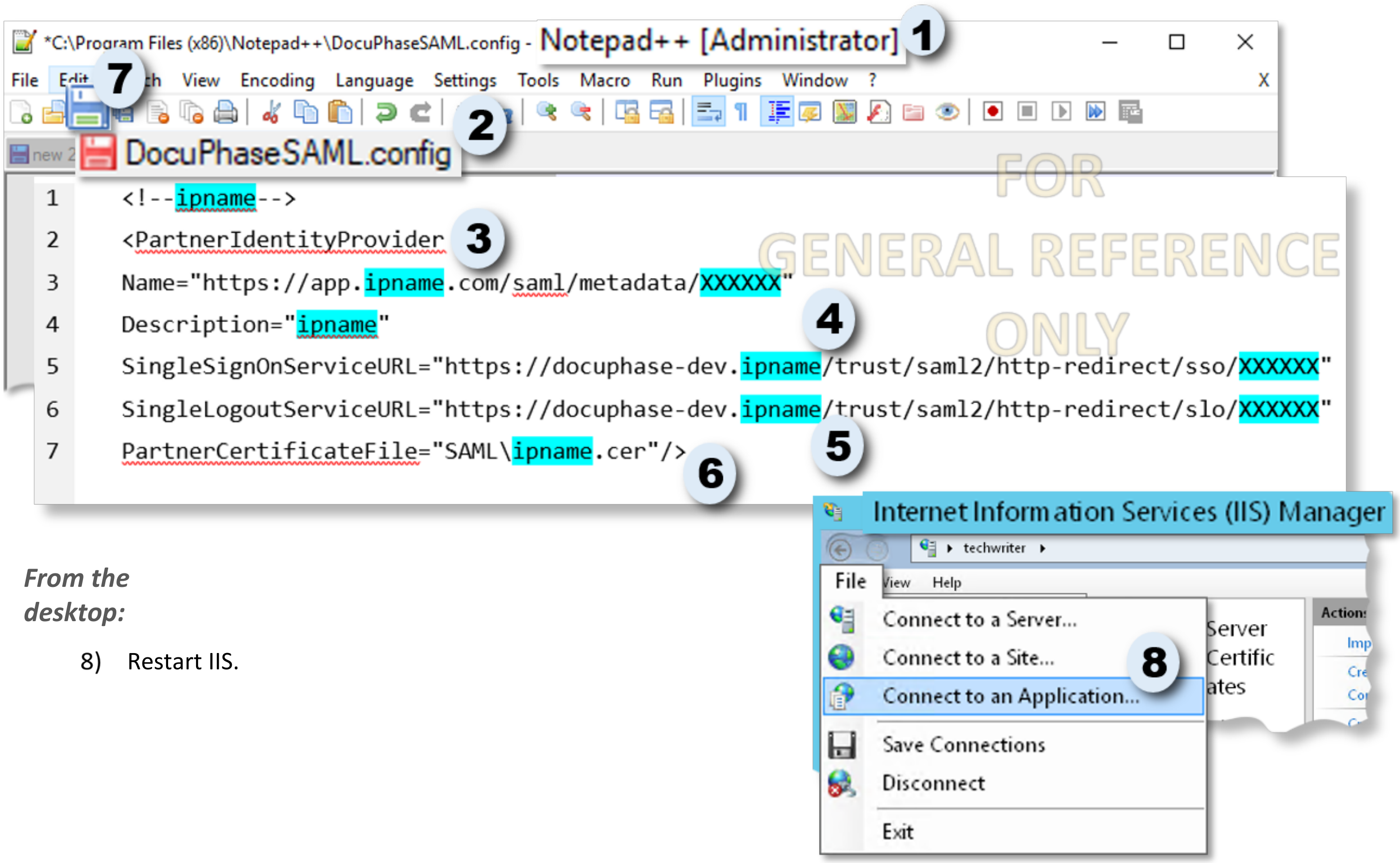
Remember that when you have finished the Identity Provider configuration, there is information used there, that must also be used in the DocuPhase SSO configuration. Therefore, please make a note of the following for use in the DocuPhase SAML configuration:

- ✓ *PartnerIdentityProvider*
- ✓ *Metadata entityID*
- ✓ *Identity Provider Url*
- ✓ *Partner certificate (in the Identity Provider's metadata)*

B) DocuPhase Configuration (Service Provider)

In Notepad ++:

1) Browse to and open the DocuPhase saml.config file.
2) Add a <PartnerIdentityProvider> entry for the Identity Provider.
3) Set Name value to the metadata entityID.
4) Set the Identity Provider Url to the Identity Provider single sign-on URL.
5) Set the SingleLogoutServiceURL to the Identity Provider single logout URL.
6) Copy the partner certificate information (from the Identity Provider metadata), then paste it into the SAML config file (as shown below).
7) Save the saml.config file.


*C:\Program Files (x86)\Notepad++\DocuPhaseSAML.config - Notepad++ [Administrator]
1
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
7
2
new 2
DocuPhaseSAML.config
3
4
5
6
Internet Information Services (IIS) Manager
techwriter
File View Help
Connect to a Server...
Connect to a Site...
Connect to an Application...
8
Save Connections
Disconnect
Exit
Server Certificates
Actions
Imp
Cre
Cor

```
<!--ipname-->
<PartnerIdentityProvider
Name="https://app.ipname.com/saml/metadata/XXXXXX"
Description="ipname"
SingleSignOnServiceURL="https://docuphase-dev.ipname/trust/saml2/http-redirect/sso/XXXXXX"
SingleLogoutServiceURL="https://docuphase-dev.ipname/trust/saml2/http-redirect/slo/XXXXXX"
PartnerCertificateFile="SAML\ipname.cer"/>
```

From the desktop:

8) Restart IIS.

Configuration Checklist for All Options

Use the following checklist to make sure all necessary settings are in place for any successful configuration of SSO.

✓ Make sure Single Sign On is enabled in the ***dob DocuPhase Database (SQL) config table***

✓ Make sure ADIS is enabled in ***DocuPhase Service Config file***

✓ Make sure **IIS authentication** is set up as follows:

- ***Server ▶sites ▶default web sites ▶Docuphase ▶authentication*** *(only need Windows Authentication enabled)*
- ***Server ▶sites ▶default web sites ▶Docuphase ▶web->services->****authentication (only need Anonymous Authentication enabled)*
- *Check **IE Trusted Sites Custom config** for correct authentication*

Troubleshooting

Issue: If a 401 Error Occurs...

When setting up DocuPhase to use SSO, the DocuPhase site ***only uses Windows Authentication***. This disables ***Anonymous and Forms authentications***: preventing DocuPhase Service from calling on the subdirectory DocuPhase/Web/Services, and causing a 401 error.

However, there is a simple workaround for this issue as shown below:

> ***IMPORTANT!***
> ***The procedure described below is only necessary AFTER enabling SSO using the DocuPhase SSO Configuration Guide.***

The workaround for this issue is to configuring the DocuPhase server IIS app pool to accept the DocuPhase windows service login attempts for HTML5 cache clearing, as shown below.

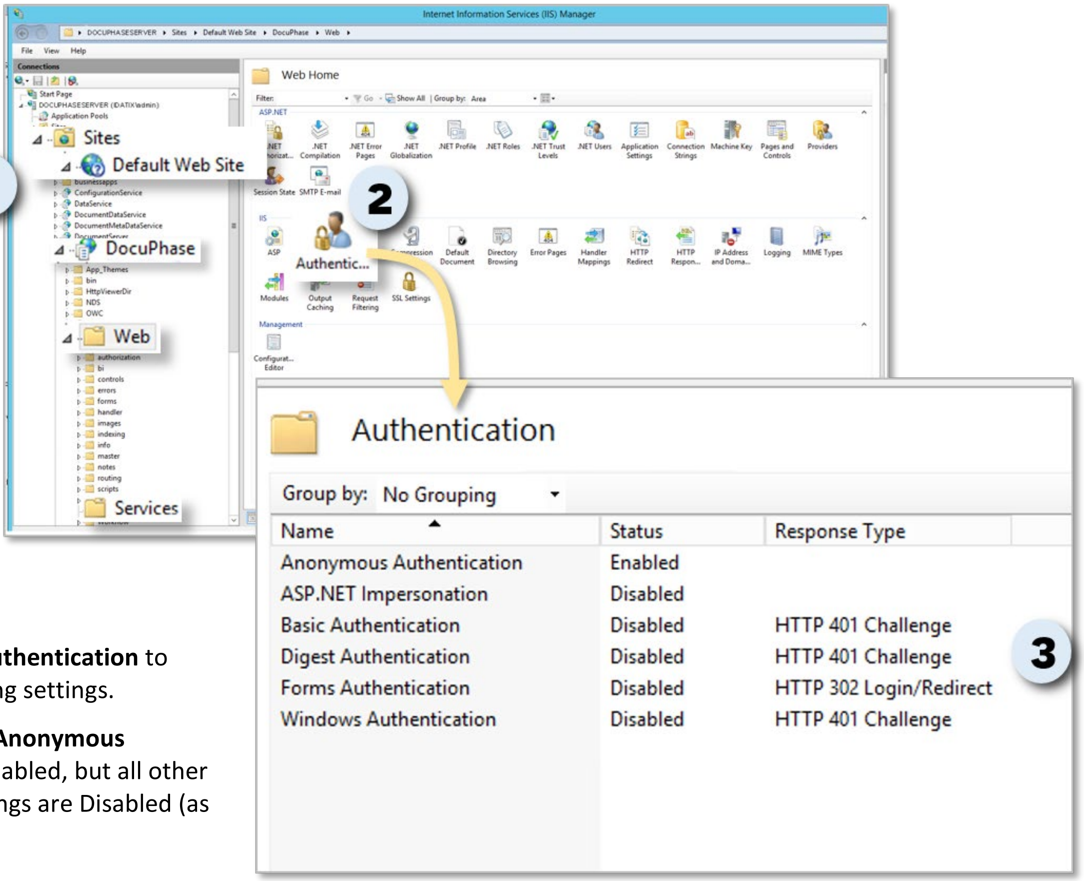
Under the DocuPhase Server name in IIS Manager:

1) Go to Sites ▶Default Web Site ▶DocuPhase ▶Web ▶Services.

In the Services window:

2) Double-click **Authentication** to display corresponding settings.

3) Make sure that the **Anonymous Authentication** is Enabled, but all other Authentication settings are Disabled (as shown in image).


Internet Information Services (IIS) Manager
DOCUPHASESERVER ▸ Sites ▸ Default Web Site ▸ DocuPhase ▸ Web ▸
File View Help
Connections
1
Sites
Default Web Site
DocuPhase
Web
Services
Web Home
2
Authentic...
3

Authentication

Group by: No Grouping

Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

Questions or Need Assistance?

If you have specific questions or need assistance with the configuration of SSO and/or a specific Identity Provider, please contact DocuPhase at any of the following:

Email: support@docuphase.com

Phone: (727) 441-8228

Website: https://www.docuphase.com/contact-us

BEST PRACTICE

When sending an email please use the following format:

- ***In the Subject line:*** *"Request for information about 6.3 Upgrade"*
- ***In the Body of the email:***
  - *Give a brief description of the information you are looking to obtain.*
  - *Provide the best contact name, phone number, and email address.*

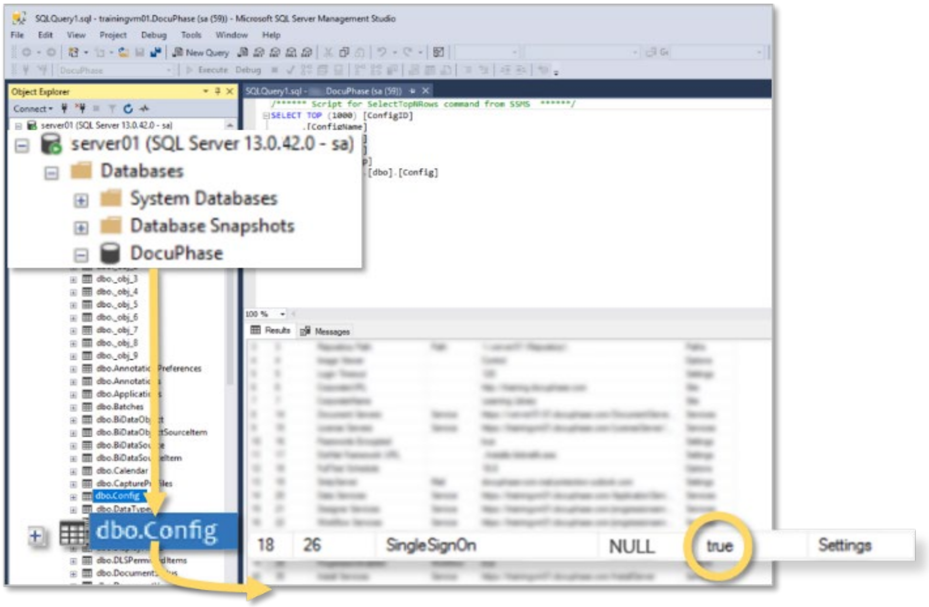
Appendices

Appendix A: Prepare the DocuPhase Database for SSO

Regardless of the Authentication type that you are configuring, you MUST make the following setting:

In the DocuPhase SQL Config table:

Make sure the Single Sign-on setting is set to "**true**".


SQLQuery1.sql - trainingvm01.DocuPhase (sa (59)) - Microsoft SQL Server Management Studio
File Edit View Project Debug Tools Window Help
New Query
Execute Debug
Object Explorer
Connect
server01 (SQL Server 13.0.42.0 - sa)
Databases
System Databases
Database Snapshots
DocuPhase
dbo.Config
Results
Messages

```
/****** Script for SelectTopNRows command from SSMS  ******/
SELECT TOP (1000) [ConfigID]
      ,[ConfigName]
  [dbo].[Config]
```

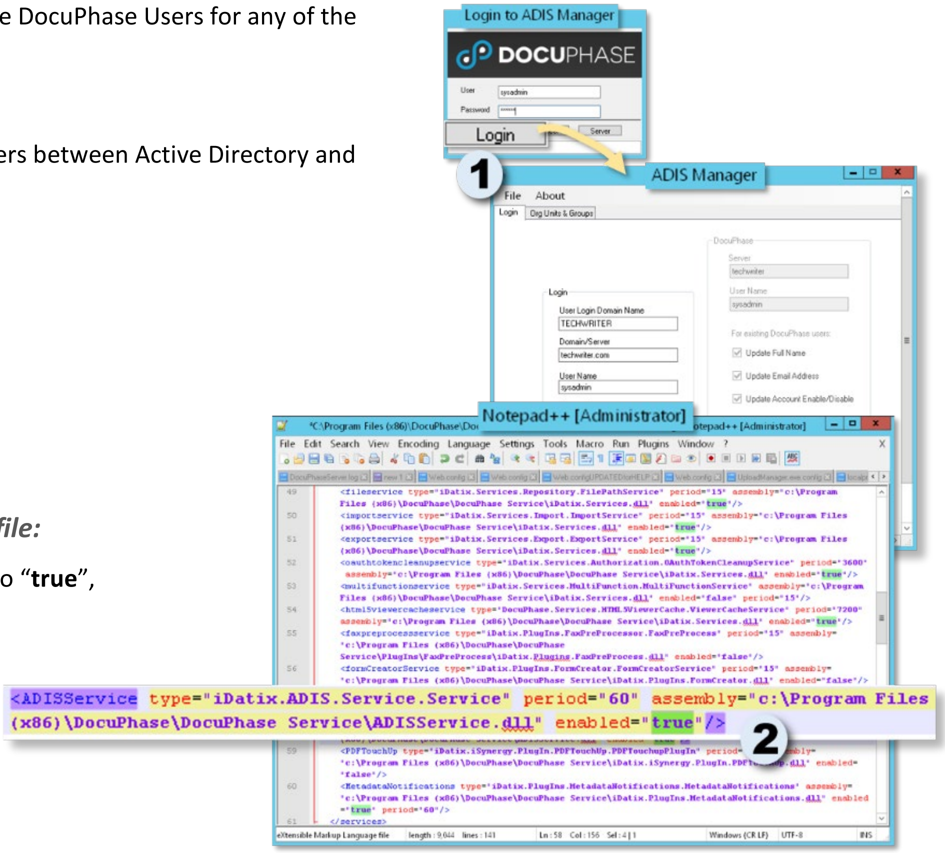
18	26	SingleSignOn	NULL	true	Settings

Appendix B: Set Up and Synchronize DocuPhase Users

You must be sure to Set Up and Synchronize DocuPhase Users for any of the Authentication Configurations:

In ADIS Manager:

1) Synchronize Active Directory users between Active Directory and DocuPhase database users.



User sysadmin
Password *****

Login
User Login Domain Name: TECHWRITER
Domain/Server: techwriter.com
User Name: sysadmin

DocuPhase
Server: techwriter
User Name: sysadmin
For existing DocuPhase users:
☑ Update Full Name
☑ Update Email Address
☑ Update Account Enable/Disable

*C:\Program Files (x86)\DocuPhase\Do... - Notepad++ [Administrator]

```
<fileservice type="iDatix.Services.Repository.FilePathService" period="15" assembly="c:\Program Files (x86)\DocuPhase\DocuPhase Service\iDatix.Services.dll" enabled="true"/>
<importservice type="iDatix.Services.Import.ImportService" period="15" assembly="c:\Program Files (x86)\DocuPhase\DocuPhase Service\iDatix.Services.dll" enabled="true"/>
<exportservice type="iDatix.Services.Export.ExportService" period="15" assembly="c:\Program Files (x86)\DocuPhase\DocuPhase Service\iDatix.Services.dll" enabled="true"/>
<oauthtokencleanupservice type="iDatix.Services.Authorization.OAuthTokenCleanupService" period="3600" assembly="c:\Program Files (x86)\DocuPhase\DocuPhase Service\iDatix.Services.dll" enabled="true"/>
<multifunctionservice type="iDatix.Services.MultiFunction.MultiFunctionService" assembly="c:\Program Files (x86)\DocuPhase\DocuPhase Service\iDatix.Services.dll" enabled="false" period="15"/>
<html5viewercacheservice type="DocuPhase.Services.HTML5ViewerCache.ViewerCacheService" period="7200" assembly="c:\Program Files (x86)\DocuPhase\DocuPhase Service\iDatix.Services.dll" enabled="true"/>
<faxpreprocessservice type="iDatix.PlugIns.FaxPreProcessor.FaxPreProcess" period="15" assembly="c:\Program Files (x86)\DocuPhase\DocuPhase Service\PlugIns\FaxPreProcess\iDatix.Plugins.FaxPreProcess.dll" enabled="false"/>
<formCreatorService type="iDatix.PlugIns.FormCreator.FormCreatorService" period="15" assembly="c:\Program Files (x86)\DocuPhase\DocuPhase Service\iDatix.PlugIns.FormCreator.dll" enabled="false"/>
<ADISService type="iDatix.ADIS.Service.Service" period="60" assembly="c:\Program Files (x86)\DocuPhase\DocuPhase Service\ADISService.dll" enabled="true"/>
<PDFTouchUp type="iDatix.iSynergy.PlugIn.PDFTouchUp.PDFTouchupPlugIn" period= [illegible] assembly="c:\Program Files (x86)\DocuPhase\DocuPhase Service\iDatix.iSynergy.PlugIn.PDFTouchUp.dll" enabled="false"/>
<MetadataNotifications type="iDatix.PlugIns.MetadataNotifications.MetadataNotifications" assembly="c:\Program Files (x86)\DocuPhase\DocuPhase Service\iDatix.PlugIns.MetadataNotifications.dll" enabled="true" period="60"/>
</services>
```

eXtensible Markup Language file | length : 9,044 lines : 141 | Ln : 58 Col : 156 Sel : 4 | 1 | Windows (CR LF) | UTF-8 | INS

In the DocuPhaseService.exe.config file:

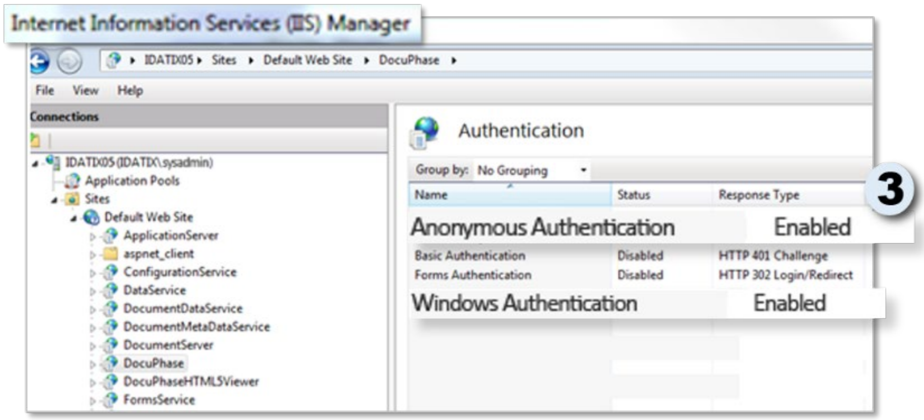
2) Make sure **ADIS Service** is set to "**true**", then **Save** the file.

Appendix B: Set Up and Synchronize DocuPhase Users (continued)

Appendix B: Set Up and Synchronize DocuPhase Users (continued)

For IIS Manager under the designated Server:

3) Enable both of the following items:
   - ✓ Anonymous Authentication
   - ✓ Windows Authentication



Name	Status	Response Type
Anonymous Authentication	Enabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	

Appendix C: Configure Specific SAML-Based Identity Providers

The following information provides a description of how to configure the following Identity Providers for DocuPhase Single Sign-on

C1) Azure AD (see below)

C2) Okta (see page 21)

C3) onelogin (see page 24)

C1) Configure Azure AD

Use the following information (both sections A and B) to configure Azure AD as a SAMLE Identity Provider for DocuPhase.

NOTE

When you see the term "Service Provider" referred to in any Identity Provider-specific instruction information, remember that DocuPhase is the Service Provider

a) Set up basic SAML Configuration for Azure AD as an Identity Provider

Please go to the Microsoft Azure AD for Single Sign-on Configuration documentation found via the following link:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-single-sign-on-non-gallery-applications

C1) Configure Azure AD (continued on next page)

b) Make changes to the web.config and saml.config files

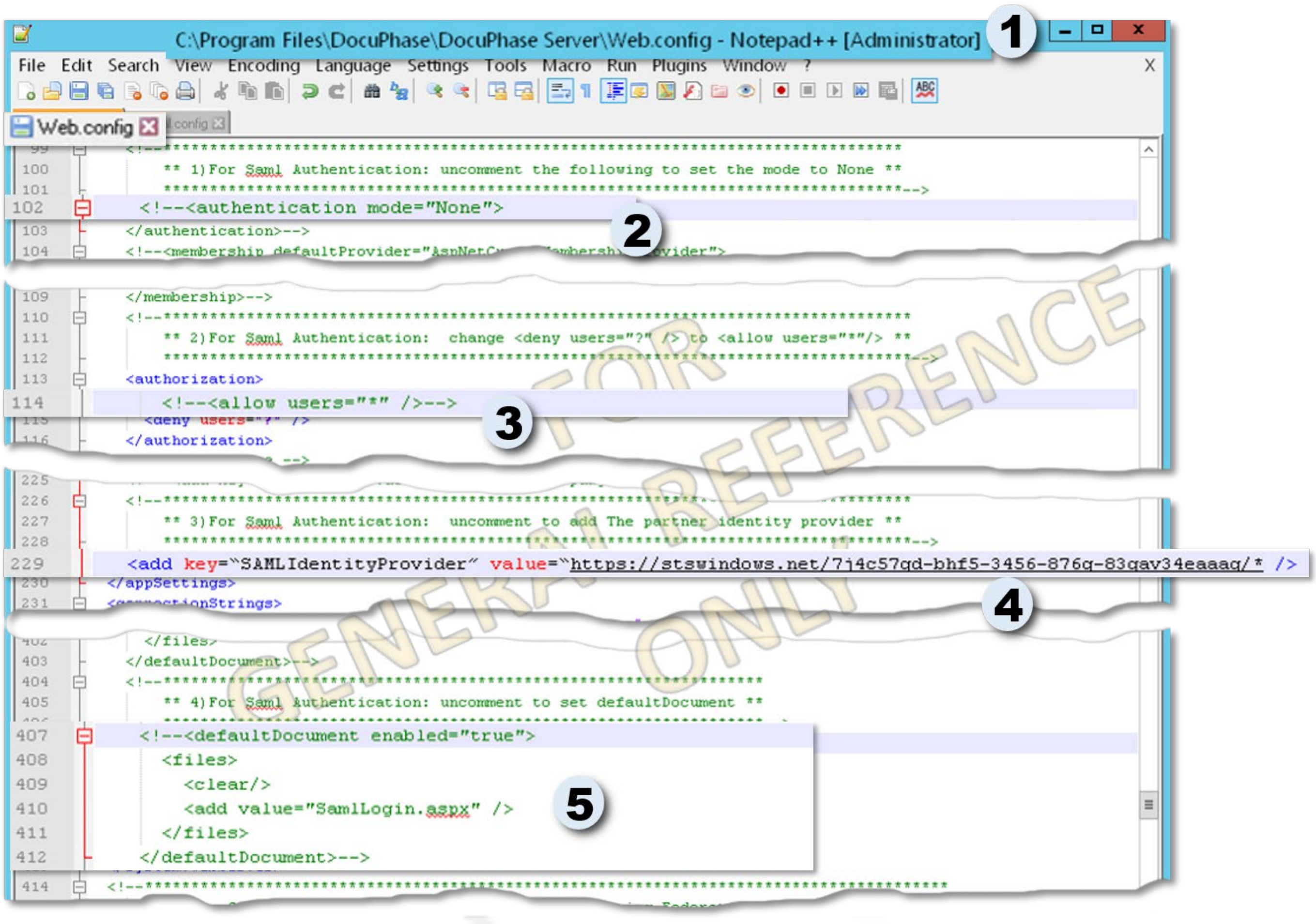
Once you have complete the procedure detailed in the link in Section A, you'll need to use Note++ as an Administrator to make changes in both the web.config and SAML.config files, as described below:

> ***TIPS***
>
> *The web.config and saml.config files are generally located at: C:\Program lFiles\DocuPhase\DocuPhase Server\Web.config).*

✓ ***Web.config***

In Notepad++:

1) Open the web.config file.
2) Set the Authentication Mode to "None".
3) Set Authentication access to "Allow Users".
4) Enter the Azure AD Identifier/PartnerIdentityProvider (used in section A) as the URL for the SAMLIdentityProvider key.
5) Uncomment to set the "defaultDocument".



```
<!--**********************************************************************
    ** 1)For Saml Authentication: uncomment the following to set the mode to None **
    **********************************************************************-->
  <!--<authentication mode="None">
</authentication>-->
<!--<membership defaultProvider="AspNetC          embersh    vider">

</membership>-->
<!--**********************************************************************
    ** 2)For Saml Authentication:  change <deny users="?" /> to <allow users="*"/> **
    **********************************************************************-->
<authorization>
    <!--<allow users="*" />-->
  <deny users="?" />
</authorization>

<!--**********************************************************************
    ** 3)For Saml Authentication:  uncomment to add The partner identity provider **
    **********************************************************************-->
  <add key="SAMLIdentityProvider" value="https://stswindows.net/7j4c57qd-bhf5-3456-876q-83qav34eaaaq/* />
</appSettings>
<connectionStrings>

    </files>
</defaultDocument>-->
<!--****************************************************************
    ** 4)For Saml Authentication: uncomment to set defaultDocument **
  <!--<defaultDocument enabled="true">
    <files>
      <clear/>
      <add value="SamlLogin.aspx" />
    </files>
  </defaultDocument>-->
<!--**********************************************************************
```

C1) Configure Azure AD (continued on next page)

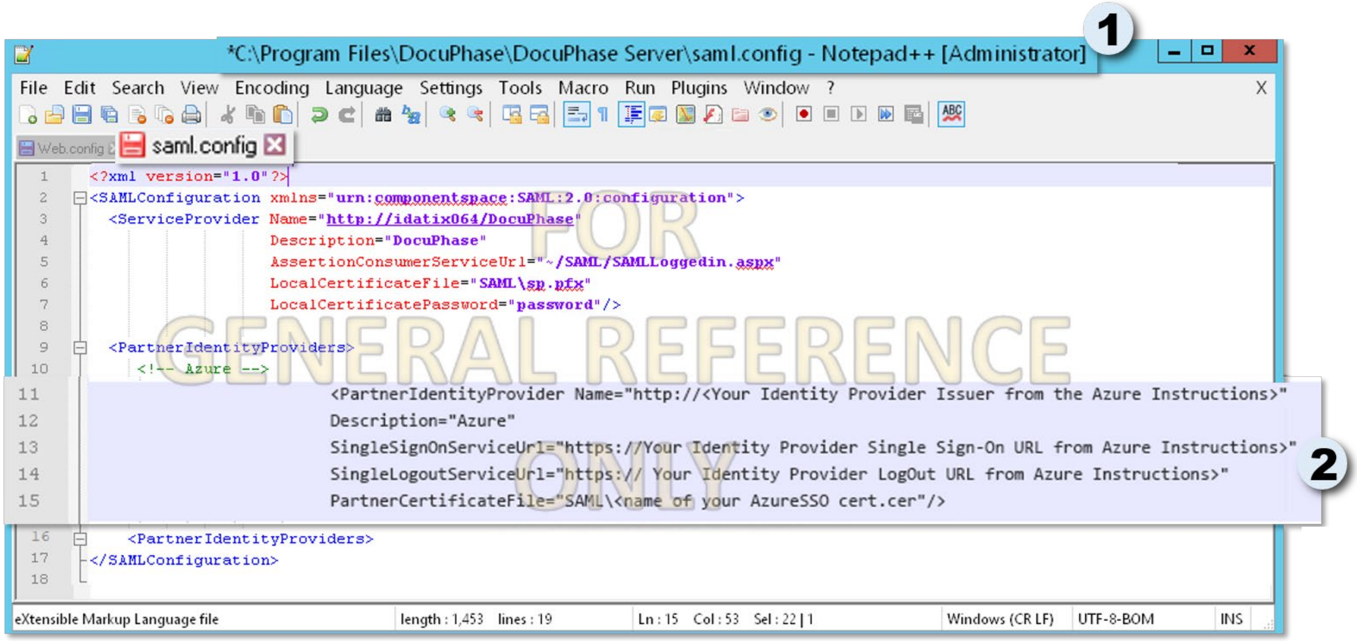
C1) Configure Azure AD (continued)

✓ ***Saml.config***

In Notepad++:

1) Open the saml.config file.
2) Use the information entered in the Azure Instructions (see section A on page 19) to enter the following in the saml.config file:
   - Partner Identity Provider
   - SingleSignOn and SingleLogout URLs

> ***NOTE***
>
> *For DocuPhase, the Single Sign URL and the Single Logout URL are the same.*


*C:\Program Files\DocuPhase\DocuPhase Server\saml.config - Notepad++ [Administrator]
1
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Web.config
saml.config
2
eXtensible Markup Language file
length : 1,453 lines : 19
Ln : 15 Col : 53 Sel : 22 | 1
Windows (CR LF)
UTF-8-BOM
INS

```
<?xml version="1.0"?>
<SAMLConfiguration xmlns="urn:componentspace:SAML:2.0:configuration">
  <ServiceProvider Name="http://idatix064/DocuPhase"
                   Description="DocuPhase"
                   AssertionConsumerServiceUrl="~/SAML/SAMLLoggedin.aspx"
                   LocalCertificateFile="SAML\sp.pfx"
                   LocalCertificatePassword="password"/>

  <PartnerIdentityProviders>
    <!-- Azure -->
                        <PartnerIdentityProvider Name="http://<Your Identity Provider Issuer from the Azure Instructions>"
                        Description="Azure"
                        SingleSignOnServiceUrl="https://Your Identity Provider Single Sign-On URL from Azure Instructions>"
                        SingleLogoutServiceUrl="https:// Your Identity Provider LogOut URL from Azure Instructions>"
                        PartnerCertificateFile="SAML\<name of your AzureSSO cert.cer"/>
    <PartnerIdentityProviders>
</SAMLConfiguration>
```

> ***IMPORTANT!***
>
> ***Once both the web.config and saml.config files are edited (as described above), restart both DocuPhase and IIS.***

C2) Configure Okta

Use the following information (both sections A and B) to configure Okta as a SAMLE Identity Provider for DocuPhase.

> ***NOTE***
>
> *When you see the term “Service Provider” referred to in any Identity Provider-specific instruction information, remember that DocuPhase is the Service Provider*

a) Set up basic SAML Configuration for Okta as an Identity Provider

Please go to the Okta Single Sign-on Configuration documentation found via the following link:

https://developer.okta.com/docs/guides/saml-application-setup/overview/

C2) Configure Okta (continued on next page)

b) Make changes to web.config and saml.config files

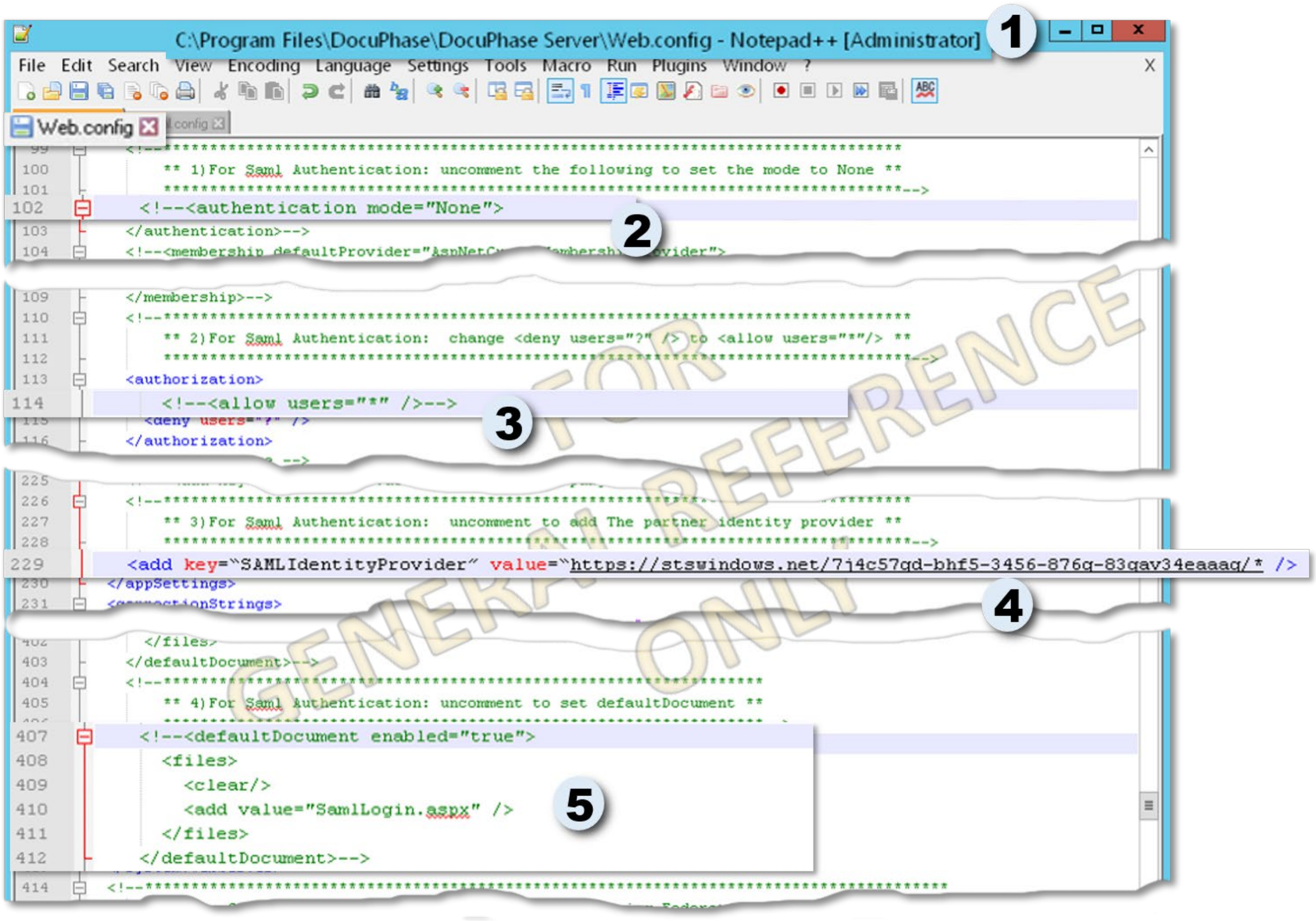
Once you have complete the procedure detailed in the link in Section A on the previous page, you'll need to use Note++ as an Administrator to make changes in both the web.config and SAML.config files, as described below:

> ***TIPS***
> *The web.config and saml.config files are generally located at: C:\Program Files\DocuPhase\DocuPhase Server\Web.config).*

✓ ***Web.config***

In Notepad++:

1) Open the web.config file.
2) Set the Authentication Mode to "None".
3) Set Authentication access to "Allow Users".
4) Enter the Okta Identifier/PartnerIdentityProvider (used in section A) as the URL for the SAMLIdentityProvider key.
5) Uncomment to set the "defaultDocument".


C:\Program Files\DocuPhase\DocuPhase Server\Web.config - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Web.config
1
2
3
4
5

```
<!--*************************************************************************
    ** 1)For Saml Authentication: uncomment the following to set the mode to None **
    *************************************************************************-->
 <!--<authentication mode="None">
</authentication>-->
<!--<membership defaultProvider="AspNetC...Membership...ovider">

</membership>-->
<!--*************************************************************************
    ** 2)For Saml Authentication:  change <deny users="?" /> to <allow users="*"/> **
    *************************************************************************-->
<authorization>
  <!--<allow users="*" />-->
  <deny users="?" />
</authorization>

<!--*************************************************************************
    ** 3)For Saml Authentication:  uncomment to add The partner identity provider **
    *************************************************************************-->
<add key="SAMLIdentityProvider" value="https://stswindows.net/7j4c57gd-bhf5-3456-876g-83gav34eaaag/* />
</appSettings>
<connectionStrings>

  </files>
</defaultDocument>-->
<!--*************************************************************
    ** 4)For Saml Authentication: uncomment to set defaultDocument **
 <!--<defaultDocument enabled="true">
   <files>
     <clear/>
     <add value="SamlLogin.aspx" />
   </files>
 </defaultDocument>-->

<!--*************************************************************************
```

C2) Configure Okta (continued on next page)

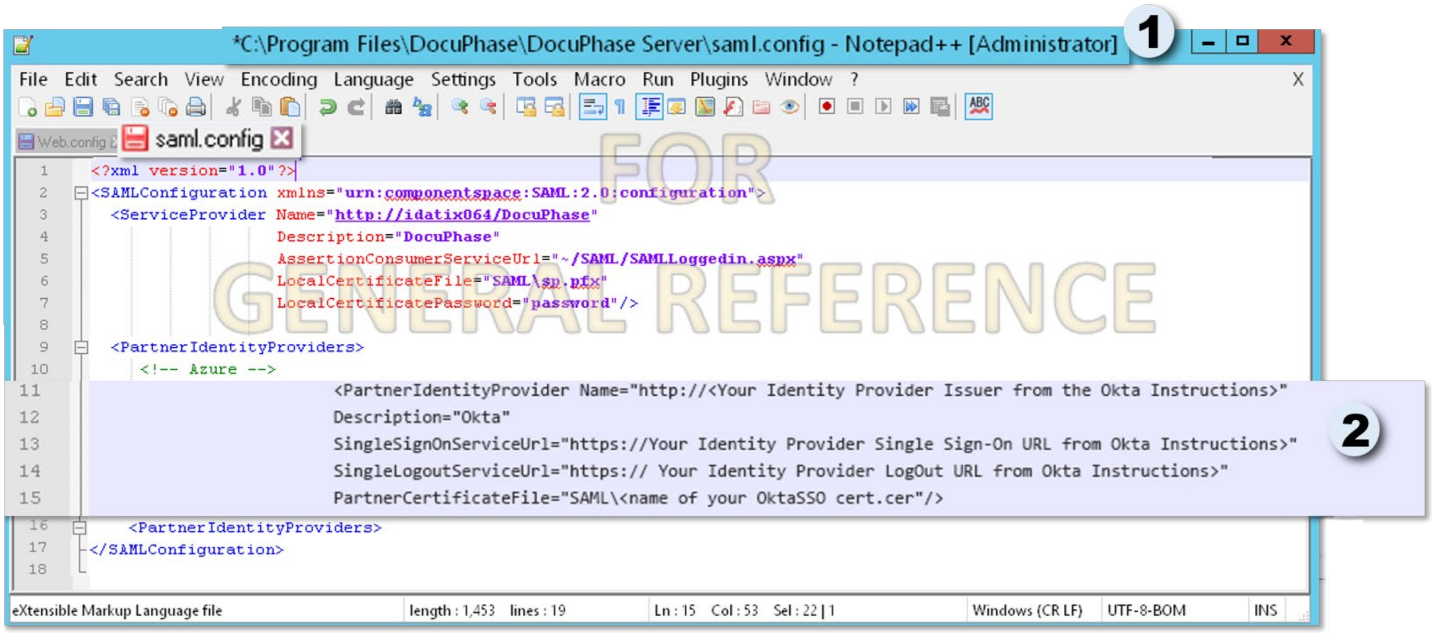
C2) Configure Okta (continued)

✓ ***Saml.config***

In Notepad++:

1) Open the saml.config file.
2) Use the information entered in the Okta Instructions (see section A on page 21) to enter the following in the saml.config file:
   - Partner Identity Provider
   - SingleSignOn and SingleLogout URLs

> ***NOTE***
>
> *For DocuPhase, the Single Sign URL and the Single Logout URL are the same.*


*C:\Program Files\DocuPhase\DocuPhase Server\saml.config - Notepad++ [Administrator]
1
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Web.config
saml.config
2
eXtensible Markup Language file
length : 1,453 lines : 19
Ln : 15 Col : 53 Sel : 22 | 1
Windows (CR LF)
UTF-8-BOM
INS

```
<?xml version="1.0"?>
<SAMLConfiguration xmlns="urn:componentspace:SAML:2.0:configuration">
  <ServiceProvider Name="http://idatix064/DocuPhase"
                   Description="DocuPhase"
                   AssertionConsumerServiceUrl="~/SAML/SAMLLoggedin.aspx"
                   LocalCertificateFile="SAML\sp.pfx"
                   LocalCertificatePassword="password"/>

  <PartnerIdentityProviders>
     <!-- Azure -->
                          <PartnerIdentityProvider Name="http://<Your Identity Provider Issuer from the Okta Instructions>"
                          Description="Okta"
                          SingleSignOnServiceUrl="https://Your Identity Provider Single Sign-On URL from Okta Instructions>"
                          SingleLogoutServiceUrl="https:// Your Identity Provider LogOut URL from Okta Instructions>"
                          PartnerCertificateFile="SAML\<name of your OktaSSO cert.cer"/>
    <PartnerIdentityProviders>
</SAMLConfiguration>
```

> ***IMPORTANT!***
>
> ***Once both the web.config and saml.config files are edited (as described above), restart both DocuPhase and IIS.***

Appendix C: Configure Specific SAML-Based Identity Providers (continued on next page)

C3) Configure onelogin

Once you are logged into Onelogin:

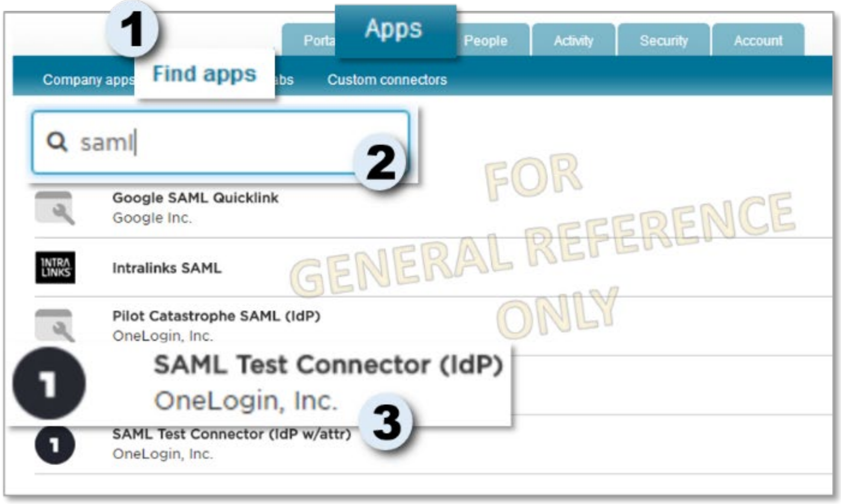
1) Go Apps▶ Find Apps do display the applications search screen.

In the search field at the top of the Find Apps screen:

2) Enter “**SAML**” to find related applications.

From the search results:

3) Select **SAML Test Connector (IdP)** to display the Portal settings.



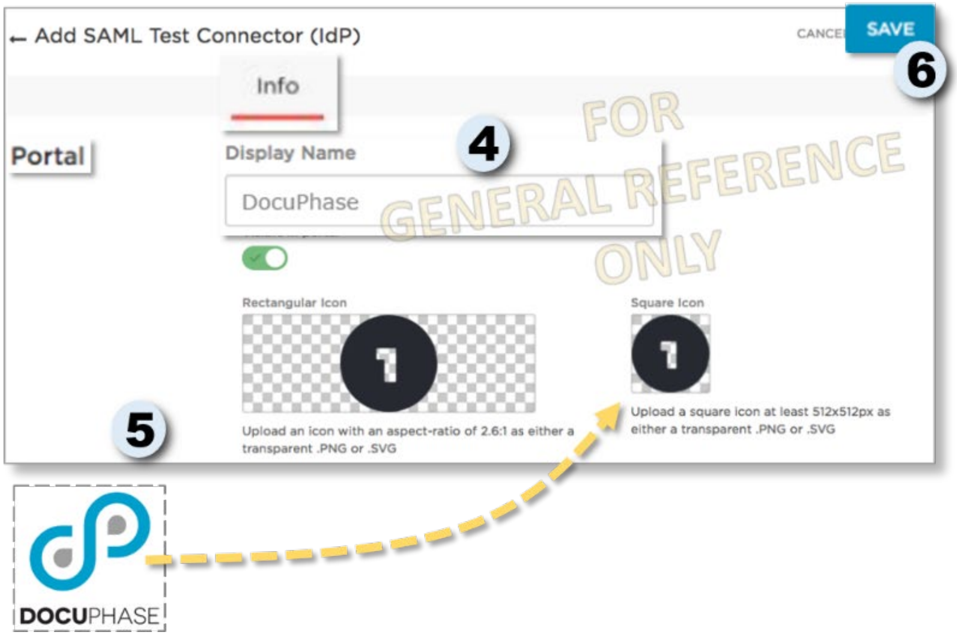
Set Display Name and Add the DocuPhase Logo for Portal

For Portal settings:

4) Enter “DocuPhase” as the Display Name; make sure the ***Visible in portal*** option is green (i.e., on).

5) Drag and drop the **DocuPhase logo** from its location into the appropriate location (i.e., either rectangular or square).

6) Click SAVE to store the settings.


← Add SAML Test Connector (IdP)
CANCEL
SAVE
6
Info
Portal
Display Name
4
DocuPhase
Rectangular Icon
Upload an icon with an aspect-ratio of 2.6:1 as either a transparent .PNG or .SVG
Square Icon
Upload a square icon at least 512x512px as either a transparent .PNG or .SVG
5
DOCUPHASE
FOR GENERAL REFERENCE ONLY

C3) Configure onelogin (continued on next page)

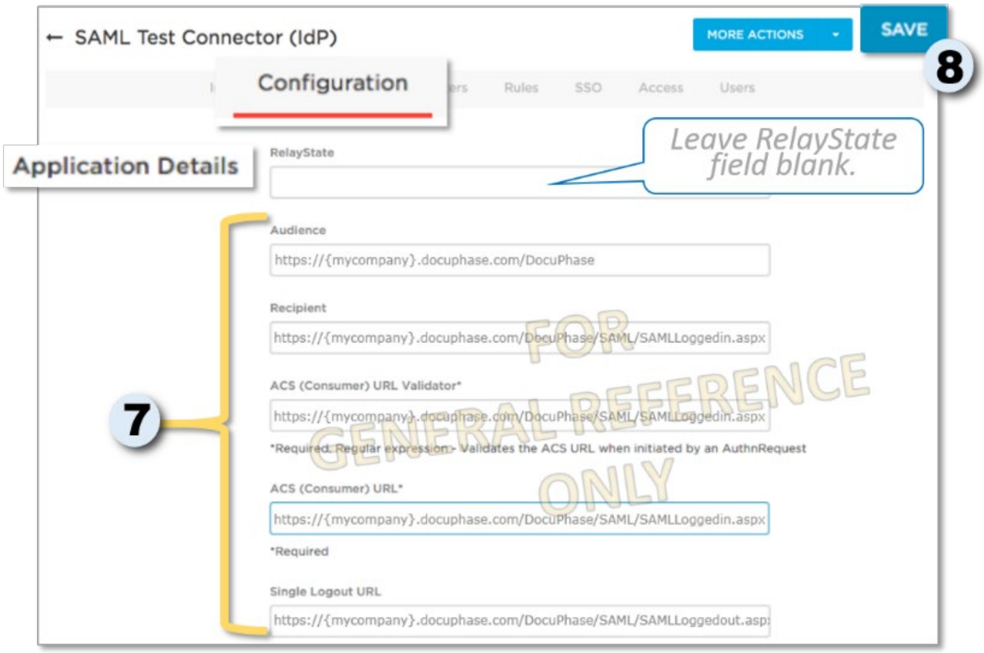
Set Application Details

On the Application page:

7) Make the following settings:

In this field…	Enter this…
Audience	https://{mycompany}.docuphase.com/DocuPhase
Recipient	https://{mycompany}.docuphase.com/DocuPhase/SAML/SAMLLoggedin.aspx
ACS (Consumer) URL Validator	
ACS (Consumer) URL	
Single Logout URL	https://{mycompany}.docuphase.com/DocuPhase/SAML/SAMLLoggedout.aspx

8) Click SAVE to store the settings.



RelayState

Audience: https://{mycompany}.docuphase.com/DocuPhase

Recipient: https://{mycompany}.docuphase.com/DocuPhase/SAML/SAMLLoggedin.aspx

ACS (Consumer) URL Validator*: https://{mycompany}.docuphase.com/DocuPhase/SAML/SAMLLoggedin.aspx

*Required. Regular expression - Validates the ACS URL when initiated by an AuthnRequest

ACS (Consumer) URL*: https://{mycompany}.docuphase.com/DocuPhase/SAML/SAMLLoggedin.aspx

*Required

Single Logout URL: https://{mycompany}.docuphase.com/DocuPhase/SAML/SAMLLoggedout.asp

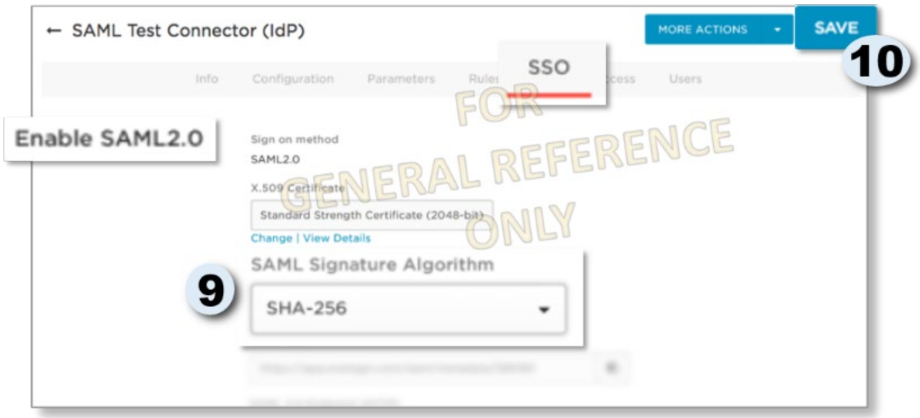
C3) Configure onelogin (continued on next page)

Configure Signature Algorithm

In the SAML Signature Algorithm field on the SSO link page:

9) Select **SHA-256**.

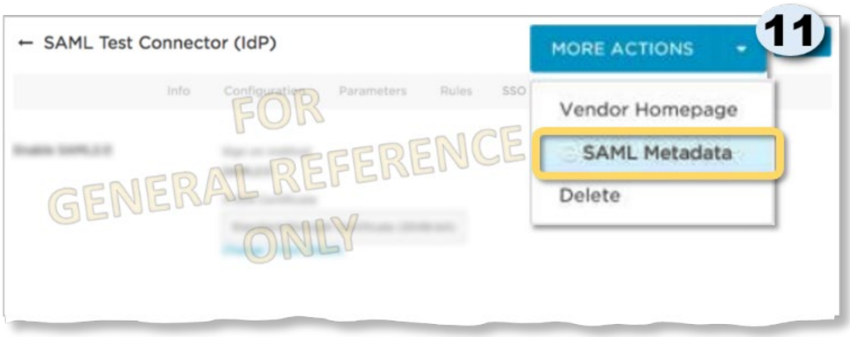
10) Click SAVE to store the settings.



Download the Identity Provider Metadata

In the More Actions drop down:

11) Select SAML Metadata* to download the Identity Provider metadata that is used to configure the Service Provider (DocuPhase).



IMPORTANT!
You need to make any necessary configuration changes for users or roles within the Identity Provider's system to allow users to access the DocuPhase application.

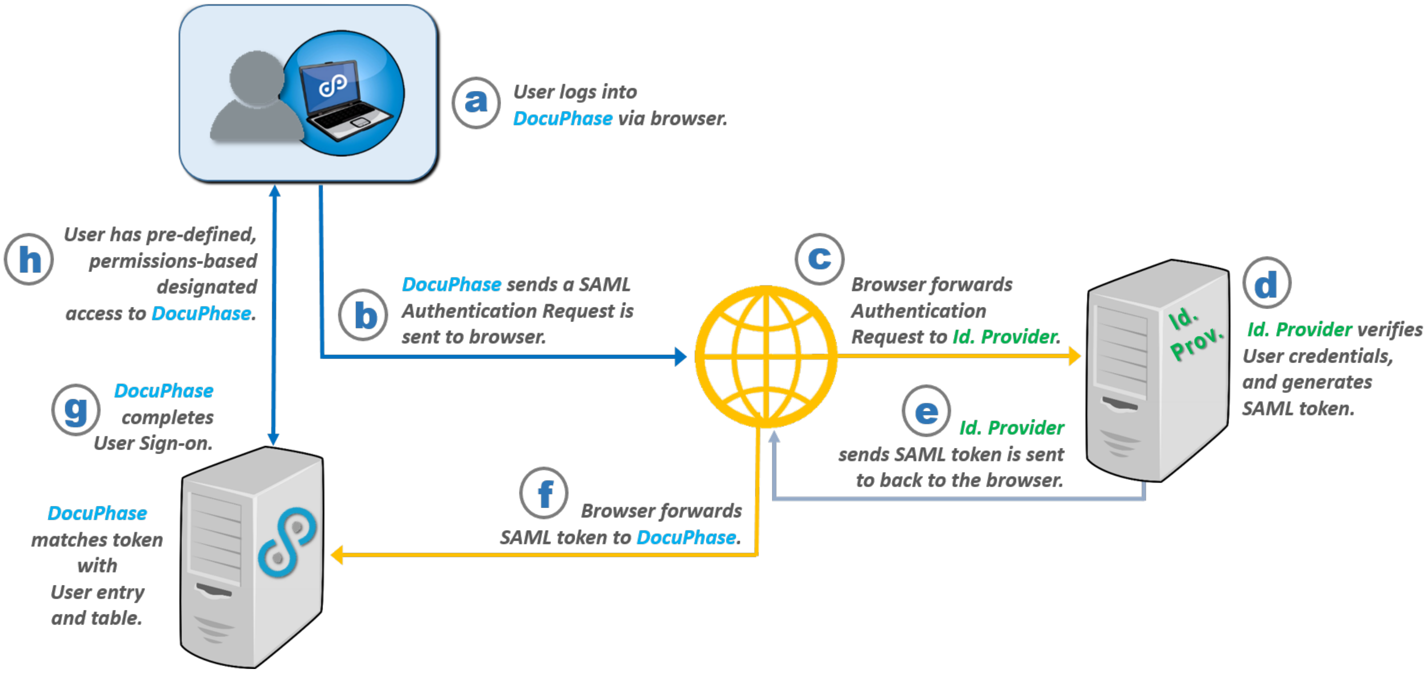
Onelogin - Download the Identiry Provider Metadata (continued on next page)

Sample metadata.xml:

```
<?xml version="1.0"?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="https://app.onelogin.com/saml/metadata/764180">
<IDPSSODescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>MIIEHTCCAwWgAwIBAgIUWOK5y1IXpcktUcXLJoBJvNR3Av8wDQYJKoZIhvcNAQEF
BQAwWjELMAkGA1UEBhMCVVMxEjAQBgNVBAoMCURvY3VQaGFzZTEVMBMGA1UECwwM
T25lTG9naW4gSWRQMSAwHgYDVQQDDBdPbmVMb2dpbiBBY2NvdW50IDEyMjI3NTAe
...
IHr0RvHc++gvIpU+hhX/eAwuD7WZwlKTJIuHGG6yIflDFjAHm1ycjEC17X6JLl3o
9hk+Pnw3jQH1mYJ5i2C7xpKokJl0qjqMzYeKJtEyJLrTAJuFiG37ZbWfsArqkzsM
PJeyDhDf/AcM2ZzxLhf+BapU6yvCWxHyR8Y39R/aTwLJD7eunbQ8o5cQsNtjJUvT
Sw==</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</KeyDescriptor>
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://docuphase-dev.onelogin.com/trust/saml2/http-redirect/slo/764180"/>
<NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://docuphase-dev.onelogin.com/trust/saml2/http-redirect/sso/764180"/>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://docuphase-dev.onelogin.com/trust/saml2/http-post/sso/764180"/>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://docuphase-
dev.onelogin.com/trust/saml2/soap/sso/764180"/>
</IDPSSODescriptor>
</EntityDescriptor>
```

Appendix D: Summary Diagram of Successful SAML Configuration

The following diagram shows successful single sign-on for any of the SAML Identity Providers described in Appendix C.


a
User logs into DocuPhase via browser.
h
User has pre-defined, permissions-based designated access to DocuPhase.
b
DocuPhase sends a SAML Authentication Request is sent to browser.
c
Browser forwards Authentication Request to Id. Provider.
d
Id. Prov.
Id. Provider verifies User credentials, and generates SAML token.
g
DocuPhase completes User Sign-on.
e
Id. Provider sends SAML token is sent to back to the browser.
f
Browser forwards SAML token to DocuPhase.
DocuPhase matches token with User entry and table.

a) The User navigates to, and logs into the DocuPhase web application (i.e., Service Provider) via HTTPS in browser

b) DocuPhase then sends a request for SAML Authentication to the browser.

c) The browser forwards the authentication request to the Identity Provider.

d) Identity Provider verifies the User's credentials, and generates a SAML token based on successful verification.

e) Identity Provider then sends the SAML token to the browser.

f) The browser then forwards the SAML token from Identity Provider to DocuPhase.

g) DocuPhase reads the User Name is read from the token, User entry existence in the DocuPhase Database is verified, and the User is logged into DocuPhase.

h) The User then has pre-defined, permissions-based access to DocuPhase.