ABSTRACT
This white paper introduces and describes SAML authentication support in Documentum Connector for Microsoft SharePoint. It includes technical architecture, working, environment setup and troubleshooting steps.
December, 2016
# TABLE OF CONTENTS

## EXECUTIVE SUMMARY

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
</tr>
</tbody>
</table>

## AUDIENCE

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
</tr>
</tbody>
</table>

## INTRODUCTION

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
</tr>
</tbody>
</table>

- Documentum Connector for Microsoft SharePoint ............................................... 4
- What is SAML AUTHENTICATION? ............................................................................ 5
- DC4SP and SAML Authentication ............................................................................ 5
- Typical flow in DC4SP SAML Authentication ....................................................... 6

## PREREQUISITES

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
</tr>
</tbody>
</table>

## CONFIGURATION & DEPLOYMENT

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
</tr>
</tbody>
</table>

- Preparing CS and ADFS for SAML support .......................................................... 7
- Configuring ADFS for DC4SP SAML support ....................................................... 7
- Configuring Provider-Host .................................................................................... 8

## TROUBLESHOOTING TECHNIQUES AND LOG LOCATIONS

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
</tr>
</tbody>
</table>

## ASSUMPTIONS AND KNOWN LIMITATION

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
</tr>
</tbody>
</table>

## FUTURE WORK

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
</tr>
</tbody>
</table>

## REFERENCES

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

This white paper introduces and describes SAML authentication support in Documentum Connector for Microsoft SharePoint. It includes technical architecture, working, environment setup and troubleshooting steps.

AUDIENCE

This white paper is intended for Documentum Connector for Microsoft SharePoint Administrators, Architect and solution developers.

Introduction

Documentum Connector for Microsoft SharePoint

Documentum Connector for Microsoft SharePoint (DC4SP) is an Add-in to SharePoint (Office 365 SharePoint Online or SharePoint 2013/16 on premise). This Add-in allows secure access to Documentum repository anytime and anywhere.

The Add-in follows typical architecture of SharePoint Add-in. It consists of an app which is deployed onto SharePoint (online or on Premise) and a Provider Host web server which serves the Add-in. It uses Documentum Foundation Services (DFS) and DFSX to communicate with Content Server (CS) repository. The following diagrams shows the same.

DC4SP App Model

Currently DC4SP uses basic and Ticketed Authentication mechanism to authenticate with CS repository.

With 7.3 version DC4SP is supporting SAML Authentication also.

Figure 1. DC4SP high level architecture
What is SAML AUTHENTICATION?

SAML (Security Assertion Markup Language) is an xml based open standard data format protocol. It is used to exchange authentication and authorization information between the two parties

IDP (Identify Provider): It is responsible for authentication and generating SAML assertions.
SP (Service Provider): It is responsible for asserting (validating) the SAML assertions.

In SAML based SSO various entities have following roles

![Figure 2. SAML Entities Interaction](image)

Typically user request a resource from SP and then he/she is diverted to IDP, which authenticates the user. Since IDP and SP are trust relationship, IDP authenticated user is allowed to access the SP services.

DC4SP and SAML Authentication

DC4SP supports SAML 2.0 Authentication to authenticate with CS. With the support of SAML DC4SP now support web single sign on. This document has been written with ADFS (Active Directory Federation Services) as IDP and DC4SP Provider-Host as the SP.
DC4SP uses SP Initiated SAML authentication in which the SP initiates the login procedure. Also DC4SP uses HTTP-POST binding between SP and IDP.

- When client is trying to access CS resources e.g. list of cabinets and if the user is not authenticated already. DC4SP provider host creates the SAML request using issuer (specified in dctm.config) and send it to IDP.[1]
- IDP Will prompt a form to enter username and password to the client browser. User feeds in the username and password. The IDP form validates the username and password with LDAP.
- After the verification IDP send back the response with small assertion to the endpoint mention in respective issuer. [2] This is typically a SAML consumer page at Provider-Host.
- Client machine will store the SAML response in browser cookie.[3]
- DC4SP Provider host Consumer page parses the response to retrieve username and then uses the DFS SDK to create a connection with SAML response as password.[4]
- DFS server further sends the request to Content Server (out of scope for this document)[4]
- Content server then validates the response and return with a valid session to DC4SP through DFS server.[5][6]
- For all the operations the provider host will use the SAML response in the cookie to connect to content server until session expires with IDP or CS.
Prerequisites

Please refer Install guide for DC4SP base install. We are enlisting only DC4SP SAML support related prerequisite.

1. Content Server 7.3
   a. Content server 7.3 Support SAML 2.0
2. Identity Provider(IDP)
   a. Certified with Active Directory Federated Services(ADFS) only
3. DFS server
   a. DFS server should be configured to support SAML
   b. All above servers should be reachable by DC4SP provider host.

Configuration & Deployment

Below section shows the configuration’s needed for this setup

Preparing CS and ADFS for SAML support

Ensure all the machines such as Content Server, Provide host machine, SharePoint Server, App server, and Identity Provider are in the same time zone.

Do the below Configuration in the content server

- Copy the *.cer security certificate from the ADFS to the Content Server.
- On Content Server open C:\Documentum\wildfly9.0.1\server\DctmServer
  _MethodServer\deployments\ServerApps.ear\SAMLAuthentication.war\WEB-INF
  \classes\SAML.properties.
- Specify the location of the security certificate for certPath.
- Increase the value for responseSkew, to increase the timeout value.
- Restart JMS, which is Documentum Java method service in services.msc.
- SAML Authentication Logs for Content Server is logged in C:\Documentum\wildfly9.0.1
  \server\DctmServer_MethodServer\logs

Configuring ADFS for DC4SP SAML support

1. Adding Relying Party Rules

   - Open ADFS Management in the ADFS Server.
   - In the left pane, right-click the Relying Party Trusts folder, and then click Add Relying Party
   - Trust.
   - Click Start.
   - Select the Enter data about the relying party manually option.
   - Specify the display name such as <SAMLserver>.
   - Select AD FS Profile.
   - Retain the default values to configure certificate.
   - Select the options, Enable the support for the WS-Federation Passive protocol and Enable
   - Support for the SAML 2.0 Web SSO Protocol.
   - Specify the URL. For example: https://SAMLserver.emc.com/adfs/ls
   - Specify a unique identifier.
   - Click Add.
   - Select “I do not want to configure multi-factor authentication settings for this RP” option.
   - Select the Permit all users to access this relying party option.
   - Retain the default values for Ready to Add Trust screen.
   - Select Open the Edit Claim Rules dialog.
   - Click Close.

2. Adding Claim Rules

Add claim rules for the relying party rule that you added in Edit Claim Rules

- Open ADFS Management in the ADFS Server.
- In the left pane, right-click the Relying Party Trusts folder.
• Right-click on the Relying party rule and select Edit Claim Rules.
• Click Add Rule in Issuance Transform Rules.
• Select the Send LDAP Attributes as Claims option as the template.
• Specify a Claim rule name.
• Select Active Directory as the Attribute store and add the below mappings:
  • LDAP Attribute: Outgoing Claim Type
  • Display-Name: Windows account name
  • Display-Name: Name ID
• Click Finish and OK.

3. Post Relying Party Configuration

• Open ADFS Management in the ADFS Server.
• In the left pane, right-click the Relying Party Trusts folder.
• Right-click on the relying party rule added in the Adding Relying Party Rules, page 41 section.
• Select Properties.
• Select the Advanced tab and select SHA-1 for secure hash algorithm.
• Select Endpoints tab.
• Click Add SAML.
• Select the Endpoint Type as SAML Assertion Consumer.
• Select the Binding as POST.
• Specify a unique index value.
• Specify the Trusted URL as https://<host>/Auth/SAML/SAMLConsume.aspx, where
  • <Host> is the App domain name.
  • Note: Specify the App Domain name that is provided during the installation of Connector for
  • SharePoint.
• Restart ADFS services.

Configuring Provider-Host

In the dctm.config file, configure single sign on as the follows:

```xml
<SingleSignOn>
  <enabled value="true"></enabled>
  <mode value="SAML"></mode>
  <ignoreUserLoginNameCase value="true"></ignoreUserLoginNameCase>
</SingleSignOn>
```

The following are the details about the attributes:
• enabled: To enable SAML set this to true.
• mode: Set this to SAML.

In the dctm.config file, configure the SAML properties as the follows:

```xml
<SAMLProperties>
  <IDPurl value="https://SAMLServer.com/adfs/ls" />
  <ACSurl value="https://localhost:8443/SAML/CreateRequest"/>
  <Issuer value="<Issuer ID as mentioned in ADFS>" />
  <cert_path value="<Path>\tokensign.cer " />
</SAMLProperties>
```

The following are the details about the attributes:
• IDPurl: Specify the URL provided in the Adding Relying Party Rules, page 41 for IDPurl.
• Issuer: Specify the unique identifies provided in Adding Relying Party Rules, page 41 for Issuer.
• cert_path: Copy the certificate from the ADFS server to the provider host server. Provide this Certificate path for cert_path.

Troubleshooting techniques and log locations

• Please make sure IDP, content server and application server are reachable by provider host.
  • In case of ADFS, Please note that the format of endpoint url should be similar to one used while registering SDFOntline app i.e. either it should be FQDN or IP
    • For e.g. https://10.30.85.34/Auth/SAML/SAMLConsume.aspx or https://dcsphightrust.com/Auth/SAML/SAMLConsume.aspx
  • To avoid frequent logouts, please increase the “skew time” in SAML.properties file on content server. It will improve the DC4SP app part performance as well.
SAML Responses have issued time stamp and validity time stamp. Once we send the SAML response to Content
Server through DFS, content server validates the response before providing a session. Since there can be a
possibility of the clocks on different servers
• SAML response/ticket can be cleared from browser by clearing the cookies. Once the DC4SP logins in successful, the
SAML response/token is stored in Browser cookie. Please note that cookies are not shared across browsers of different
vendors e.g. Chrome, IE and Firefox.
• If Pages failed to load with “too many redirects”, please refresh the page or restart the browse. It will refresh the SAML
token. Restarting the browser will remove all the SAML response/token from browser cookie and will again redirect the
user to IDP login page.
• Log can be found at ~\SDFOnlineWeb\_layouts\DocumentumLog\log.txt
• To enable debug level, change the Level to “DEBUG” in ~\SDFOnlineWeb\_layouts\Documentum\DC4SP.LogConfig.xml
• SAML Authentication logs w.r.t. Content Server can be found in SAMLAuthentication.log on Content server. For e.g. -
C:/Documentum/wildfly9.0.1/server/DctmServer_MethodServer/logs/SAMLAuthentication.log
• In case IDP Login dialog is not coming up, please check if the IDP server is up or if the respective issuer is properly
configured at IDP.
• After the IDP login page if app part or any of the DC4SP pages are not coming up then possible reasons may be:
  o SAML response is invalid
    DC4SP log file can be checked to find if there is any failure related to SAML response validation. If no
    error/debug information is found in DC4SP log, please refer to SAML authentication log on Content server for
    respective information.
  o No Response received from IDP.
    Please refer to DC4SP debug log to confirm whether DC4SP has received the SAML response.
  o SAML Consumer page is not reachable.
    In Case error of “Page not found”, the possible reason might be:
    • SAMLConsume.aspx is missing in DC4SP installed location.
    • You do not have permission to access the page.
    • Improper host name resolution. In case FQDN is used for SAML Consume page, please update the host
      file with DC4SP host name.
  o SAML Consumer endpoint URL and DC4SP SAML consumer page URL does not match.
  o SAML Assertion validation fails at Content Server.
  o Check if the user has permission in Content Server.

Assumptions and Known Limitation
• Internet Explorer does not work with clickonce content transfer mode.
  o To invoke clickonce, client machine invokes URL of clickonce application with SAML response and request
    parameter. The total URL length increases more than 5000. IE thus fail to invoke the URL since it has a limit of
    2083 characters (KB208427).
• D2/D2FS does not support SAML Authentication and thus it’s not supported for DC4SP D2 app parts as well.
• SAML Authentication is not supported for WebDirect data transfer mode.
• Shared Search and Browse app part does not depend on SAML Authentication.
• In S2S (server to server high trust environment), the windows logged in user should be same for the data services to work.

Future work
• UCF and WebDirect content transfer support.
• SAML assertion validation at Provider-Host.
• SP metadata xml support from provider host for easier ADFS relay party configuration.
• Single logout Use
  o Currently the SAML authentication provides session affinity till browser session only.
  o If user needs to logout, he should do either of the following
    • Close all instances of browser.
    • Delete cookies from browser.
  o To avoid this a logout functionality is required from within respective webpart. Which will invalidate login session
    from IDP itself.

References
• https://en.wikipedia.org/wiki/Active_Directory_Federation_Services