Login with Active Directory Federation Services (ADFS)

Summary

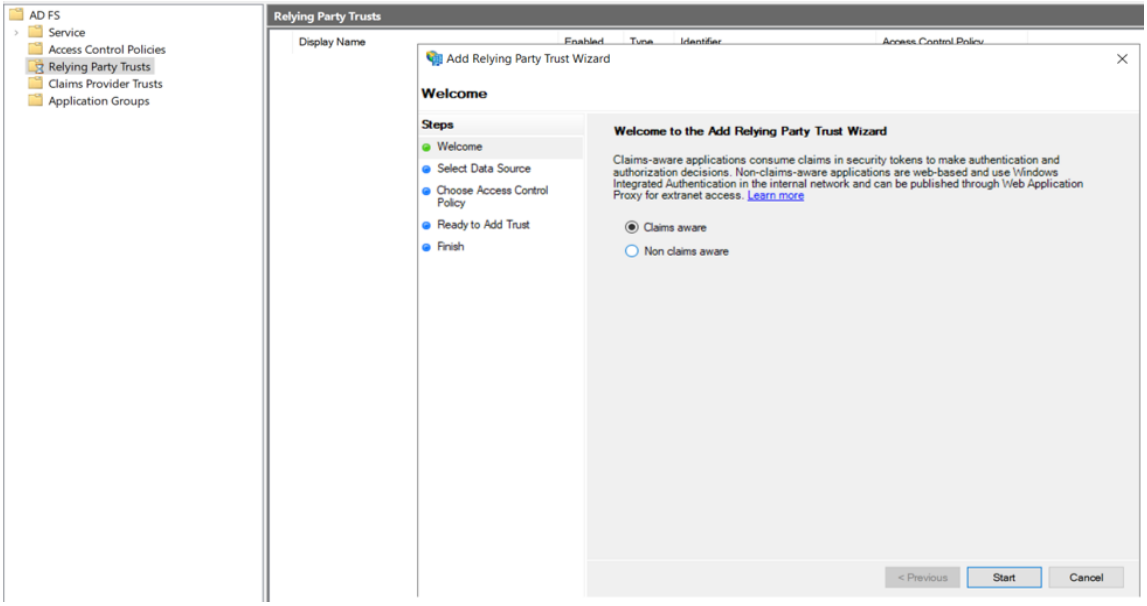
This article outlines and discusses the steps or actions required to enable Machpanel to authenticate via Active Directory Federation Services (ADFS).

ADFS setup

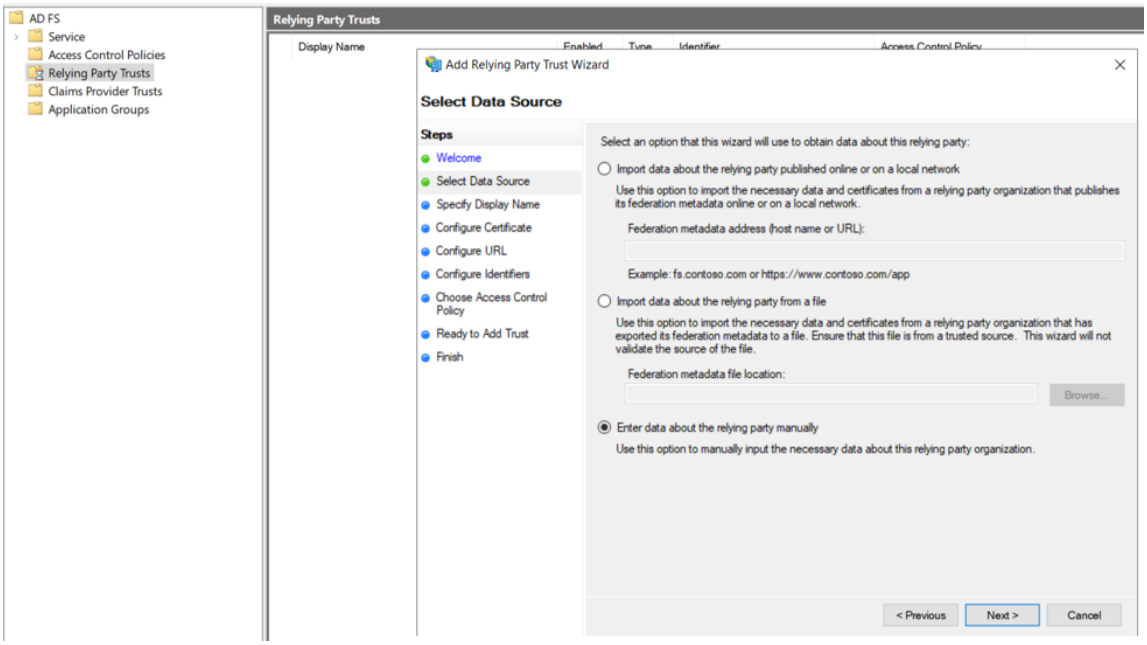
Functionality to login to Machpanel with ADFS account requires an ADFS server setup and shall be accessible from control panel server and also control panel shall be able to access ADFS server. Setting up ADFS machine is out of scope of this document. To setup the ADFS server please contact Machsol support.

Relaying Party setup

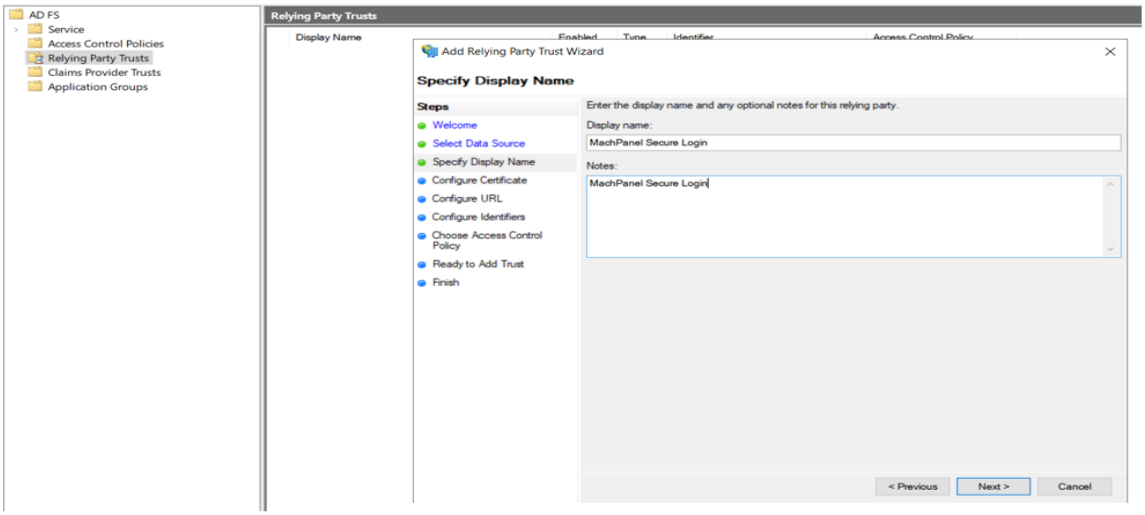
Once ADFS server is setup then we need to add our ‘ADFS login App’ as relying party in ADFS.In ADFS service console, navigate to ‘Relying Party Trust’, right click and select ‘Add new’, below dialog box appears, select ‘claim aware’ and click start.



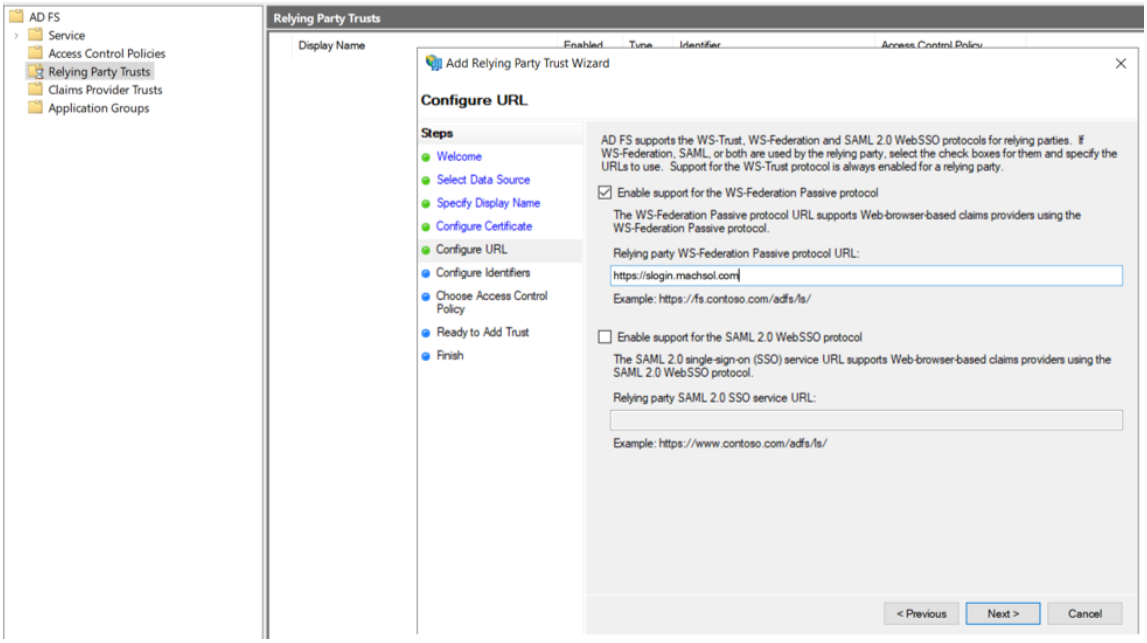
On next screen select ‘Enter data about relying party manually’ and click next as show below.



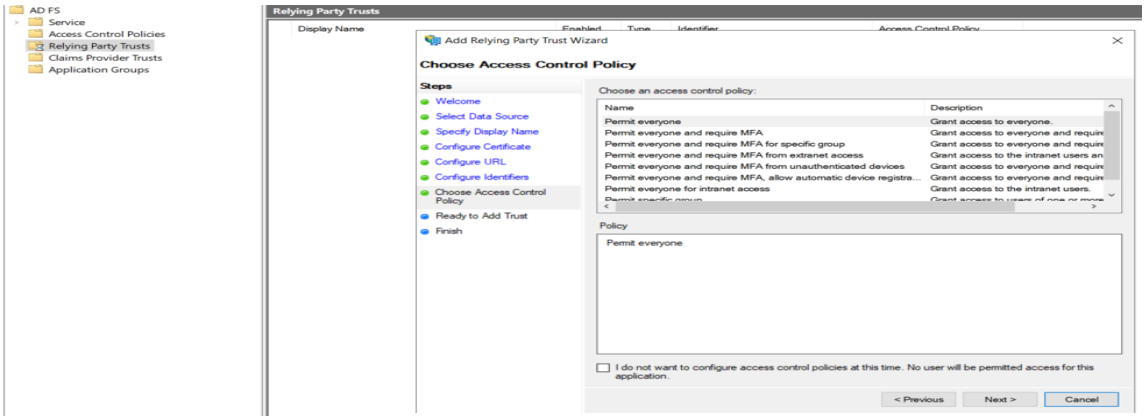
On next screen provide ‘Display name’ and ‘Notes’ for Relying party as below and click next.



On next screen ‘Configure certificate’ no change and click next and configure ‘Configure URL’ as show below and click next. Set the bridging/intermediate application url and select ‘WS Federation Passive protocol’



On ‘Configure identifiers’ steps no change, just click next. And on ‘Choose Access Control Policy’ screen select ‘Permit Everyone’ and click next as shown below.

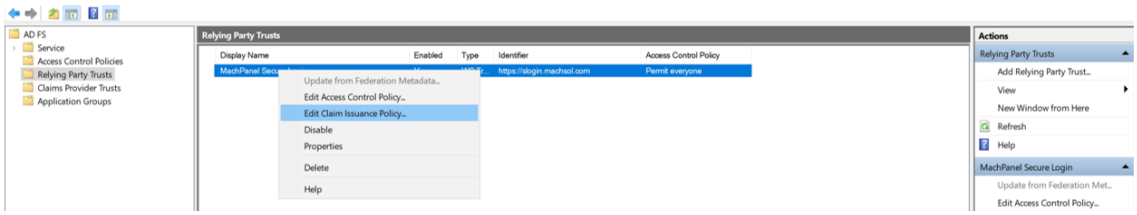


Navigate to last step by clicking ‘next’ and finish the setup.

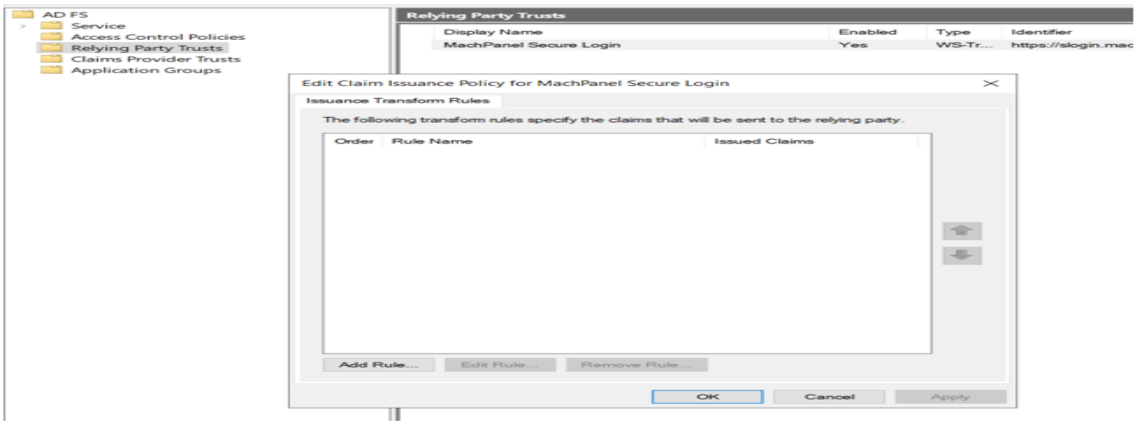
Configure Claim

Once a relying party is added successfully, we need to configure the ‘Claim Issuance Policy’ for relying party so that required claim is returned by ADFS to middle-ware application.

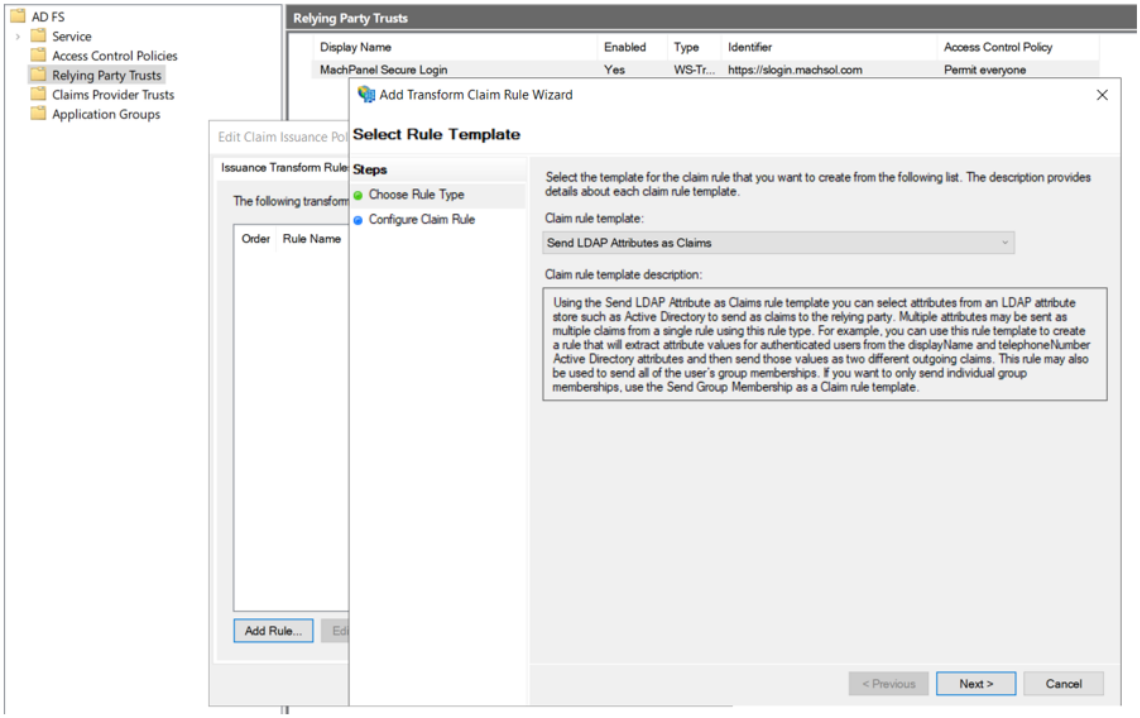
Right click on relying party name in ADFS service console and select ‘Edit claim issuance policy’ as shown below.



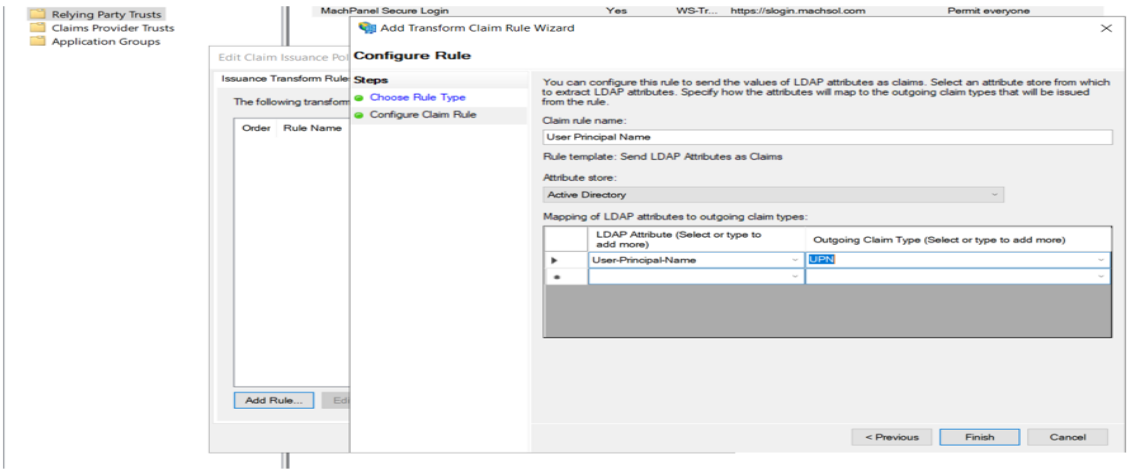
In claim issuance policy dialog click ‘Add Rule’ button as shown below.



On ‘Select Rule Template’ step verify ‘Send LDA attributes as Claims’ is selected and click ‘next’.



In ‘Configure Rule’ screen set the claim rule name, select attribute store as ‘Active Directory’, select ‘User-Principal-Name’ in LDAP attribute and ‘UPN’ in Outgoing claim type and click finish as shown below.



Bridging/Middleware App setup

Website Configuration in IIS

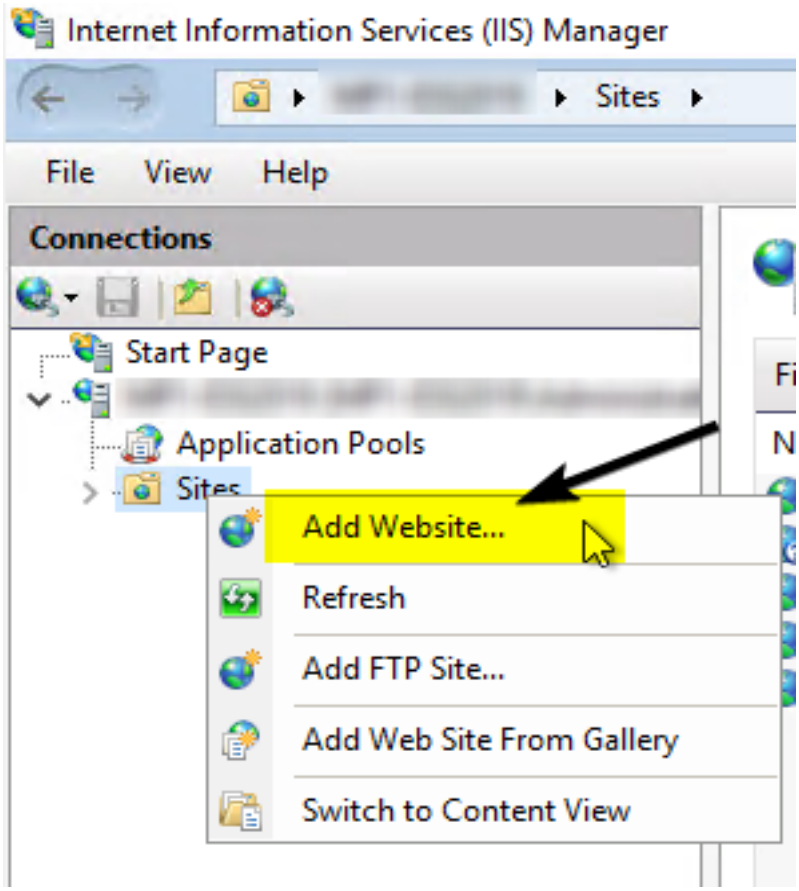
Download the "MachPanel ADFS Middleware App".

Right Click and "Unblock" the zip file before extracting files.

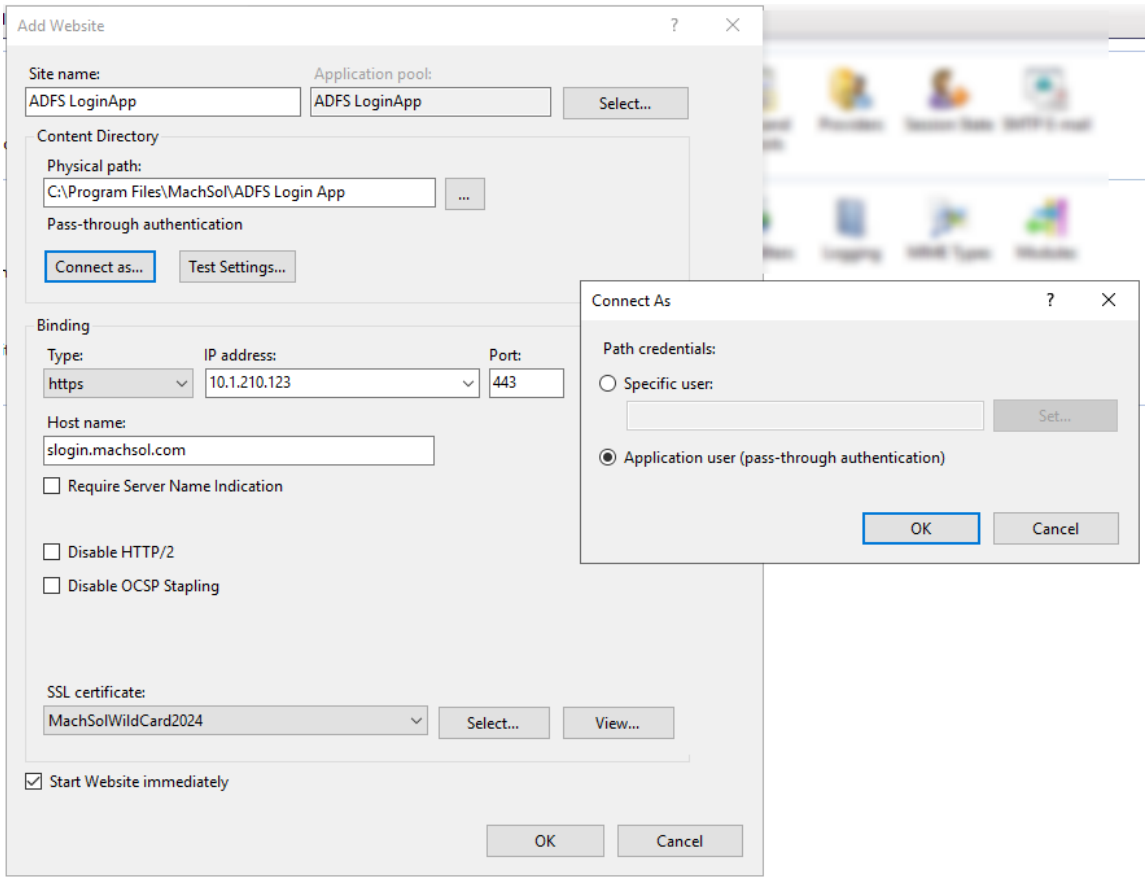
Copy the extracted 'ADFS Login App' folder and place at location which shall be configured for IIS website.

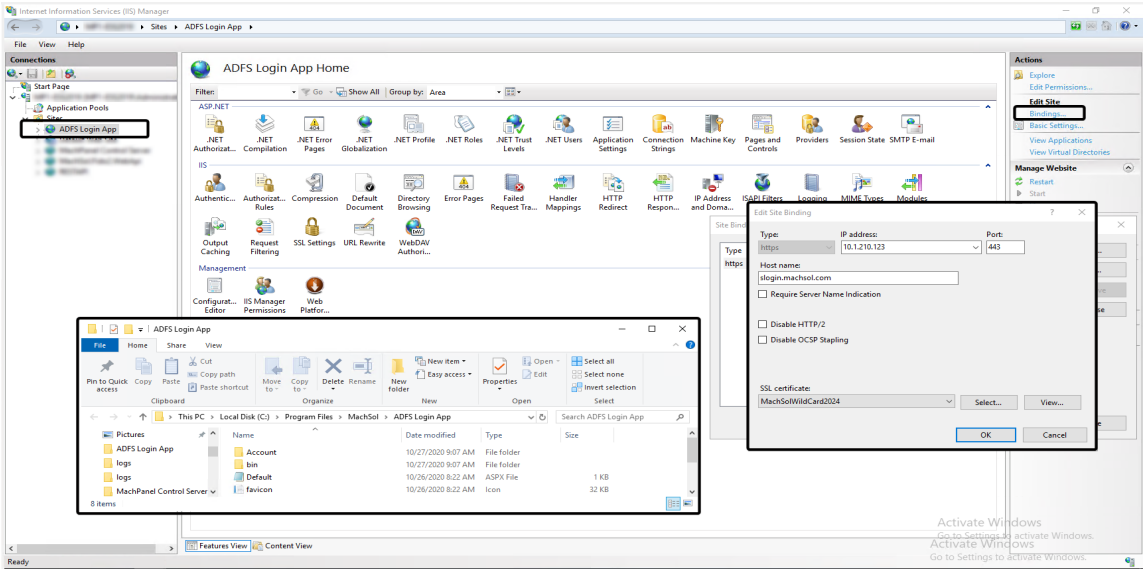
Add a new website in IIS and point the application directory to "ADFS Login App" folder. Define bindings for https protocol over 443 port and assign a valid certificate and host name.

This hostname shall be same as 'Relying party identifier' specified when creating relying party.



Login with Active Directory Federation Services (ADFS)





Configuration variable setup in config file

There are some custom keys in the website configuration file (Web.config inside application directory) which are required to be set and are shown below.

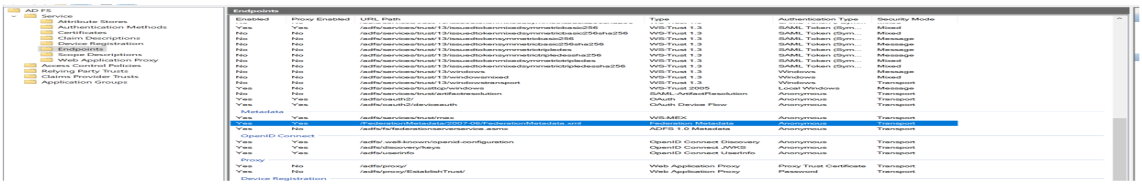
```
<?xml version="1.0" encoding="utf-8"?>
<!--
  For more information on how to configure your ASP.NET application, please visit
   https://go.microsoft.com/fwlink/?LinkId=301880

  -->
<configuration>
  <appSettings>
    <add key="ida:ADFSMetadata" value="https://adfs.machsol.com/federationmetadata/2007-06/federationmetadata.xml" />
    <add key="ida:Wtrealm" value="https://slogin.machsol.com" />
    <add key="ida:claimType" value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"/>
    <add key="ida:signoutUrl" value="" />
    <add key="panelUrl" value="http://10.2.200.112:8088"></add>
    <add key="loginAsADUserOnly" value="0" />
  </appSettings>
```

Ida:ADFSMetadata

This is the Url of ADFS metadata endpoint, metadata for ADFS service can be found in ‘Endpoints’ section in ADFS service console, see below screenshot.

Syntax is: https://<ADFS Server Pointer>/federationmetadata/2007-06/federationmetadata.xml

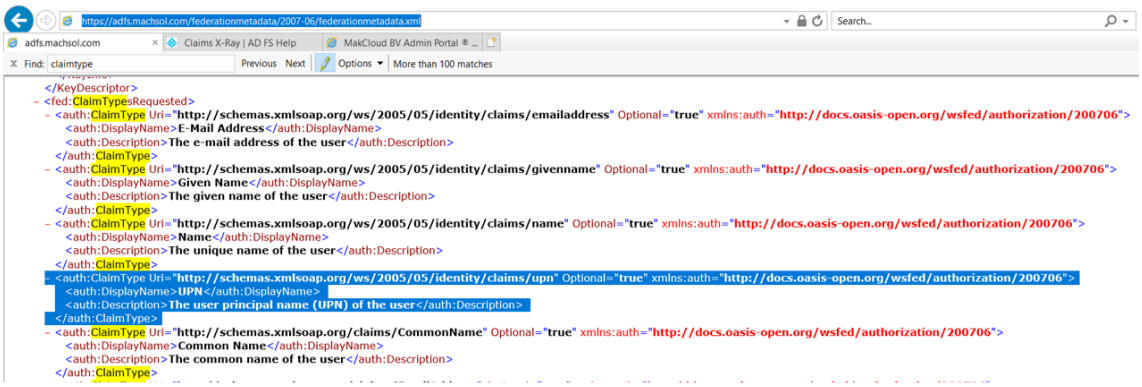


Ida:Wtrealm

This is the Url of the application/Relying party identifier configured in ADFS.

Ida:claimType

This is claim type value identifier whose value is returned to panel and is matched with panel account. This can be found by browsing/opening the metadata Url in any web browser, seen below screenshot.



Ida:singoutUrl

This is **optional** key, it can be used to redirect user to some specific page on sign-out from ADFS, This Url shall be added in Relying party rusted endpoints, otherwise the redirection to the Url on sign-out will not work.

panelUrl

This is the control panel URL.

loginAsADUserOnly

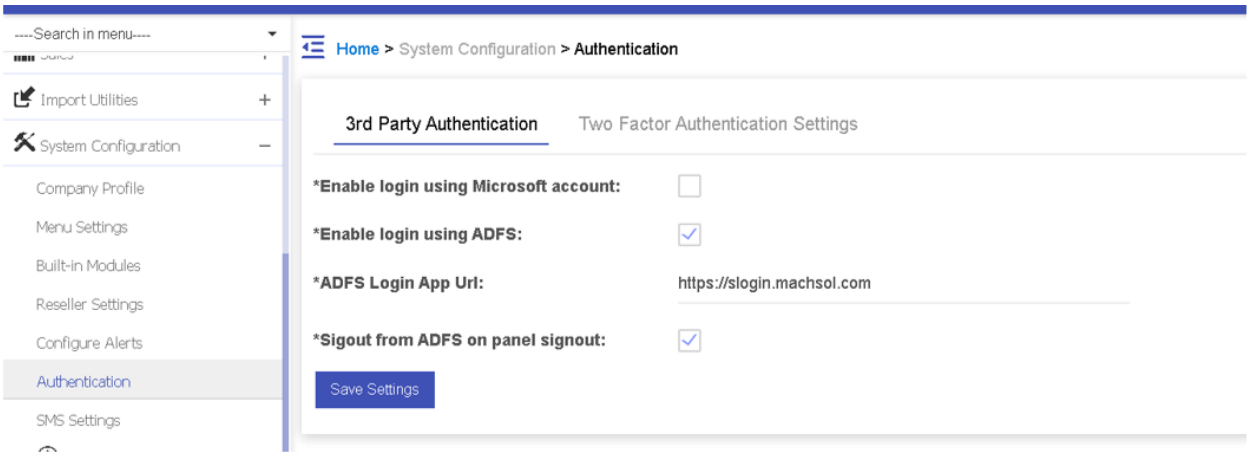
When set to ‘0’ this will allow to login to panel with any of the authentication accounts i.e. can

sign-in with customer, reseller, staff/employee, contact or AD user.

When set to 1 this will allow to login to panel as AD user only (4th level user login).

Configuration in Machpanel

To enable login with ADFS, navigate to Home > System Configuration > Authentication and on first tab '3rd Party Authentication' enable the option as shown below.

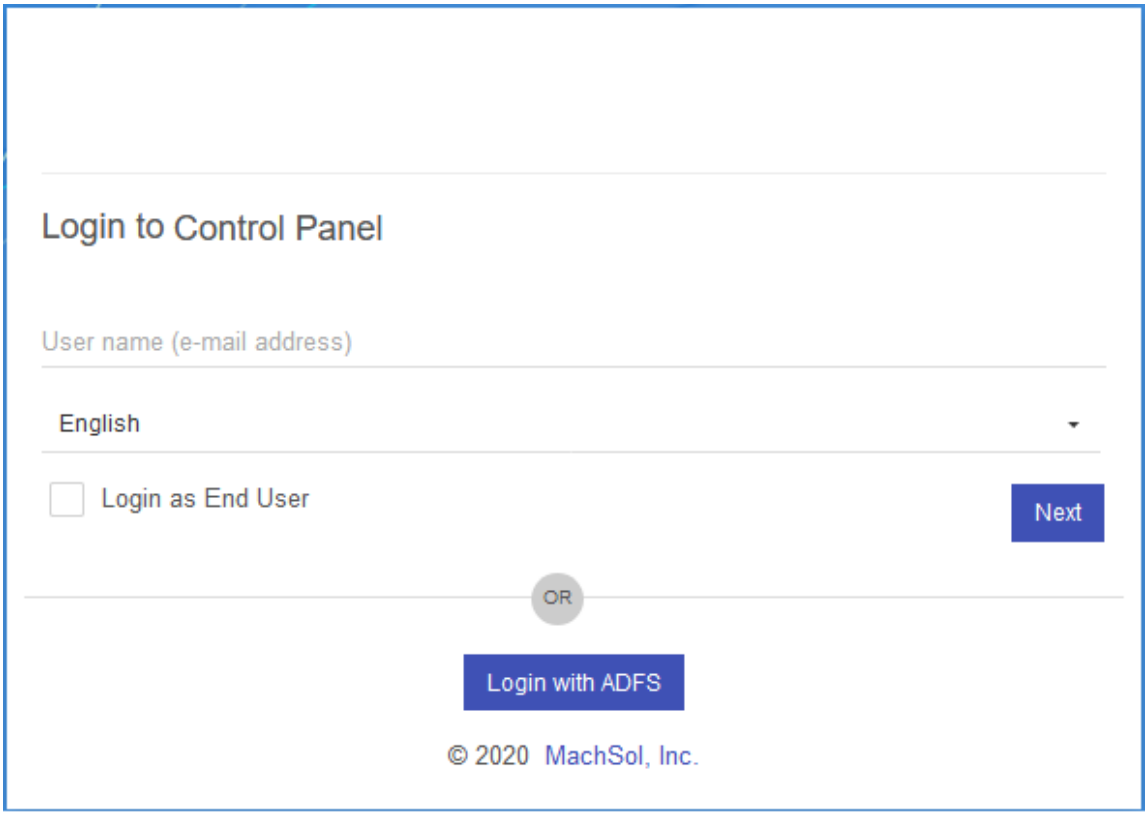


ADFS Login App Url

This shall be the bridging/intermediate application (shipped with control panel) URL configured in previous step.

Sign-out from ADFS on panel sign-out

This option specified whether it is required to sign-out from ADFS account when signing out of control panel, when enabled this will sign-out from ADFS and will effect any other applications signed in with same ADFS account.



When selected, the button redirects to ADFS for authentication and if already signed in with ADFS account in same browser to any other app the panel logs in with same account, otherwise sign-in screen of ADFS appears as below.

Login with Active Directory Federation Services (ADFS)

The name shown above on Sigin-In page is the name set for ADFS service.

Supported Authentication Scenarios

As Customer:

When claim value (UPN in this case) returned by ADFS matches with the login of customer account.

As Customer via linked AD account:

When claim value returned by ADFS matches with UPN of the AD user account in panel and is linked with customer account for authentication.

As Customer contact:

When claim value returned by ADFS matches with customer contact login.

As Customer contact via linked AD account:

When claim value returned by ADFS matches with UPN of the AD user account in panel and is linked with customer contact for authentication.

Reseller:

When claim value returned by ADFS matches with login of reseller account.

Staff/Employee:

When claim value returned by ADFS matches with login of employee/staff account.

Staff/Employee via linked AD account:

When claim value returned by ADFS matches with UPN of the AD user account in

panel and is linked with staff/employee for authentication.

AD user (4th level login):

When claim value returned by ADFS matches with AD user account in panel and logs in as AD user for self service.