#### 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.

<ul> <li>Service</li> <li>Access Control Policies</li> <li>Relying Petry Trusts</li> <li>Claims Provider Trusts</li> <li>Application Groups</li> <li>Display Name</li> <li>Paubled</li> <li>Tune</li> <li>Identifier</li> <li>Access Control Policy</li> <li>X</li> <li>Welcome</li> <li>Service</li> <li>Service</li> <li>Relying Petry Trust Wizard</li> <li>Welcome</li> <li>Service</li> <li>Service</li> <li>Service</li> <li>Relying Petry Trust Wizard</li> <li>Welcome</li> <li>Service</li> <li>Service</li> <li>Service</li> <li>Relying Petry Trust Wizard</li> <li>Welcome</li> <li>Service</li>     &lt;</ul>	> Service	
Steps       Welcome to the Add Relying Party Trust Wizard <ul> <li>Select Data Source</li> <li>Obose Access Control Polcy</li> <li>Ready to Add Trust</li> <li>Finish</li> <li>Claims aware</li> <li>Claims aware</li> <li>Claims aware</li> <li>Non claims aware</li> </ul>	Access Control Policies     Display Name     Enabled     TuneIdentifier	Access Control Policy
Providence Start Canad	Steps       Welcome            • Select Data Source        Claims-aware applications consume claims in s authorization discisions. Non-claims-aware appli Pology             • Ready to Add Trust           • Claims aware             • Frish           • Claims aware	Vizad expriny takens to make authentication and cations are web-based and use Windows and can be published through Web Application

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

AD FS	Relying Party Trusts			
AD FS Service Carrol Policies Cairns Provider Trusts Cairns Provider Trusts Application Groups	Relying Party Trusts Display Name	Ena Ena Ena Ena Ena Ena Ena Ena	New         Lidentifier           izard         Select an option that this wizard will use to obtain dat           Import data about the relying party published onlin         Use this option to import the necessary data and the federation metadata online or on a local network           Federation metadata address (host name or UF         Example: fs contoso com or https://www.conto           Import data about the relying party from a file         Use this option to import the necessary data and or exported fa federation metadata to a file. Ensure the validate the source of the file.           Federation metadata file location:         Federation metadata file location:           Import data about the relying party manually         Use this option to manually input the necessary data and or exported fals about the relying party manually	Access Control Policy.
				< Previous Next > Cancel

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

ad FS	Relying Party Trusts						
Claims Provide Trusts     Claims Provider Trusts     Claims Provider Trusts     Application Groups	Display Name	Enabled Tune Identifier Access Control Policy  Specify Display Name					
Application Groups		Steps Welcome Steps Specify Display Name Configure Certificate Configure Certificate Configure Certificate Configure Certificate Choise Access Control Ready to Add Trust Finish	Erter the display name and any optional notes for Display name: MachPanel Secure Login Notes: MachPanel Secure Login	r this relying party.	X		
				< Previous Next >	Cancel		

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.

AD FS	Relying Party Trusts					
A OF 5 Costs Control Policies Claims Provider Trusts Claims Provider Trusts Application Groups	Relying Party Trusts	E Choose Access Cont Seps Wilsone Select Data Source Secoty Diploy Name Configure Centicate Configure URL Configure VRL Configure Montentions Configure Access Control	Anablert Tone Identifier Wizard Choose an access control policy: Name Permit everyone and require MFA Permit everyone and require MFA Permit everyone and require MFA form extranet access Permit everyone and require MFA form extranet access Permit everyone and require MFA form extranet access Permit everyone and require MFA allow automatic de Permit everyone for intanet access	Access Control P Descr Grant Grant devices Grant devices Grant Grant Grant Grant Grant	iption access to everyor access to everyor access to everyor access to the intra access to the intra access to everyor access to the intra	te. te and requir te and requir te and requir te and requir te and requir te and requir te and requir to rea or more to rea or more to rea or more te and require
		Configure Certificate     Configure Certificate     Configure (Certificate     Configure (Certificate     Choose Access Control     Paloy     Ready to Add Trust     Finish	Permit everyone and require MFA for specific group. Permit everyone and require MFA form substanet acces Permit everyone and require MFA form unauthenticat Permit everyone and require MFA, allow automatic de Permit everyone for intranet access Permit everyone de la substance access Policy Permit everyone	d avices Grant d devices Grant kos registra Grant Grant	access to everyor access to the intra access to the intra access to everyor access to everyor access to everyor access to the intra access to the intra	te and requiri net users an te and requiri te and requiri te and requiri final tusers. final tusers.
			I do not want to configure access control policies at application.	this time. No user wi	Il be permitted acc	cess for this

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.

AD FS	<b>Relying Party Trusts</b>					Actions	
Service     Access Control Policies	Display Name	Enabled	Туре	Identifier	Access Control Policy	Relying Party Trusts	-
Relying Party Trusts Claims Provider Trusts Application Groups	MachPanel Secu	Update from Federation Metadata Edit Access Control Policy Edit Claim Issuance Policy Disable Properties		https://slogin.mechsol.com	Permit everyone	Add Relying Party Trus View New Window from He Refresh	st 🕨
		Delete Help				MachPanel Secure Login Update from Federatio Edit Access Control Po	on Met

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

AD FS	Relying Party Trusts			
Service Access Control Policies	Display Name	Enabled	Туре	Identifier
Claims Provider Trusts	MachPanel Secure Login	Yes	WS-Tr	https://slogin.ma
Application Groups	Edit Claim Issuance Policy for MachPane	l Secure Login	×	
	Issuance Transform Rules			
	The following transform rules specify the o	laims that will be sent to the relying party.		
	Order Rule Name	Issued Claims		
			141	
			-0-	
	Add Rule Edit Rule Rem	ove Rule		
		OK Cancel	Apply	
			Pog	

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.

Relying Party Trusts	Mach	Panel Secure Login	Yes	WS-Tr https://slogin.r	machsol.com	Permit everyone
Claims Provider Trusts Application Groups		Ndd Transform Claim Rul	e Wizard			×
	Edit Claim Issuance Po	Configure Rule				
	Issuance Transform Rule	Steps	You can configure this	rule to send the values of Li	DAP attributes as claims.	Select an attribute store from which
	The following transform	Choose Rule Type	from the rule.	ites. Specify how the attribute	es will map to the outgoin	ig claim types that will be issued
	Order Rule Name	<ul> <li>Configure Claim Rule</li> </ul>	Claim rule name:			
	Cider Rule Name		User Principal Name			
			Rule template: Send L	DAP Attributes as Claims		
			Attribute store:			
			Active Directory			~
			Mapping of LDAP attri	butes to outgoing claim types	10	
			LDAP Attrib add more)	ute (Select or type to	Outgoing Claim Type (	Select or type to add more)
			User-Principa	al-Name ~	UPN	~
			·	Ŷ		~
	Add Rule Ed					
					< Previous	Finish Cancel
		1				

### **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.



🛀 Internet Information Services (IIS) Manager

Add Website	? ×
Site name: Application pool: ADFS LoginApp ADFS LoginApp	Select
Content Directory Physical path:	and Providen Sector halo 2017 5 real
C:\Program Files\MachSol\ADFS Login App Pass-through authentication	1 10 (20) 44
Connect as Test Settings	Connect As 7 X
Binding	
Type: IP address: Port:	Path credentials:
https v 10.1.210.123 v 443	O Specific user:
Host name:	Set
slogin.machsol.com	Application user (pass-through authentication)
Require Server Name Indication	
Disable HTTP/2	OK Cancel
Disable OCSP Stapling	
SSL certificate:	
MachSolWildCard2024 Y Select	View
Start Website immediately	



## 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.



# 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.

# IoginAsADUserOnly

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

### Login with Active Directory Federation Services (ADFS)

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 <u>Home > System Configuration > Authentication</u> and on first tab '3rd Party Authentication' enable the option as shown below.

Search in menu	► Home > System Configuration > Authentication	
ピ Import Utilities	+ 3rd Party Authentication Two Easter Authentication Settings	
🛠 System Configuration		
Company Profile	*Enable login using Microsoft account:	
Menu Settings	*Enable login using ADFS:	
Built-in Modules	*ADES Login Ann Life https://slogin.machsol.com	
Reseller Settings		
Configure Alerts	*Sigout from ADFS on panel signout:	
Authentication	Save Settings	
SMS Settings		

#### 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.

Login to Control Panel	
User name (e-mail address)	
English	•
Login as End User	Next
OR	
Login with ADFS	
© 2020 MachSol, Inc.	

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.

Sign in someone@example.com Password	MachPanel   Security Token Service
someone@example.com Password	Sign in
Password	someone@example.com
	Password

### 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

### Login with Active Directory Federation Services (ADFS)

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.

#### MachPanel Knowledgebase

https://kb.machsol.com/Knowledgebase/55648/Login-with-Active-Directory-Fede...