#### 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>Display Name</li> <li>Display Na</li></ul>	ad FS	Relying Party Trusts						
Welcome     Select Data Source     Onose Access Control     Poly     Ready to Add Trust     Pinish     Welcome     Cams aware applications consume claims in security tokens to make authentication and     authorization decisions. Non-claims aware applications are web-based and use Vindows     provy for extranet access. Learn more     Ono claims aware     Non claims aware	Access Control Policies Relying Party Trusts Claims Provider Trusts	Display Name	Nadd Relying Party Trust Wizard					
Crievious Statt Caliber			Welcome     Select Data Source     Choose Access Control     Policy     Ready to Add Trust	Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Vindows Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. Learn more © Claims aware	20			

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

AD FS	Relying Party Trusts							
<ul> <li>AD FS</li> <li>Service</li> <li>Access Control Policies</li> <li>Relying Party Trusts</li> <li>Claims Provider Trusts</li> <li>Application Groups</li> </ul>	Rolying Party Trusts Display Name	Final Select Data Source Select Data Source Select Data Source Select Data Source Select Data Source Select Data Source Configure Cetificate Configure URL Configure Identifiers Configure Identifiers Console Access Control Policy Ready to Add Trust Finish	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 it ts federation metadata andiress (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 it	e or on a local network certificates from a relying party organization that publishes k. aLJ: bio.com/app certificates from a relying party organization that has hat this file is from a trusted source. This wizard will not Browse				
				< Previous Next > Cancel				

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

ad FS	Relying Party Trusts				
Carrow Control Policies     Access Control Policies     Relying Party Trusts     Claims Provider Trusts     Application Groups	Display Name	En Specify Display Name			
Application Groups		Steps Welcome Stelect Data Source Specify Display Name Configure Certificate Configure URL Configure Vertifiers Choose 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.

	Relying Party Trusts					
A pplication Groups     Access Control Policies     Relying Party Trusts     Claims Provider Trusts     Application Groups		Add Relying Party Trust     Choose Access Cont     Seps     Welcome     Select Data Source     Secty Display Name     Configure Certificate     Configure URL     Configure URL     Configure URL     Configure URE	Tot Policy Choose an access control policy: Name Permit everyone Permit everyone and require MFA for extende acces Permit everyone and require MFA form extende acces Permit everyone and require MFA form unablenticat Permit everyone and require MFA form unablenticat Permit everyone and require MFA access and the form the everyone and require MFA access and the form the everyone and require MFA access Permit everyone for intranet access	Grant Grant s Grant d devices Grant rice registra Grant Grant	tiption access to everyor access to everyor access to the intra access to everyor access to everyor access to the intra	ne and require ne and require anet users an ne and require ne and require anet users.
		Configure URL     Configure Identifiers	Permit everyone and require MFA from extranet access Grant access to the intranet use Permit everyone and require MFA from unauthenticated devices Grant access to everyone and re Permit everyone and require MFA, allow automatic device registra Grant access to everyone and re			ne and require anet users an ne and require ne and require anet users.
			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	Relying Party Trusts					Actions
Service Access Control Policies	Display Name	Enabled	Type	Identifier	Access Control Policy	Relying Party Trusts
Relying Party Trusts	MachPanel Secu	Update from Federation Metadata	- un Tr	https://slogin.machsol.com	Permit everyone	Add Relying Party Trust
Claims Provider Trusts		Edit Access Control Policy				View
Application Groups		Edit Claim Issuance Policy				New Window from Here
		Disable				Refresh
		Properties				Help
		Delete				MachPanel Secure Login
		Help				Update from Federation Me
						Edit Access Control Policy_

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

AD FS	Relying Party Trusts			
<ul> <li>Service</li> <li>Access Control Policies</li> </ul>	Display Name	Enabled	Type Identifier	
Claims Provider Trusts	MachPanel Secure Log	jin Yes	WS-Tr https://slo	gin.ma
Application Groups	Edit Claim Issuance Policy for MachPan	el Secure Login	×	
	Issuance Transform Rules	-		
	The following transform rules specify the	claims that will be sent to the relying party		
	Order Rule Name	Issued Claims		
			1	
			-	
	Add Rule Edit Rule Ren	move Rule		
		OK Cancel	Apply	
		OK Cancel	Apply	

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.	machsol.com	Permit everyone	
Claims Provider Trusts		National Character Claim Rule	e Wizard					$\times$
Edit Cl	aim Issuance Pol	Configure Rule						
Issuan	ce Transform Rule	Steps	You can	configure this ru	ule to send the values of L	DAP attributes as claims	s. Select an attribute sto	ore from which
The	following transform	Choose Rule Type	to extract from the	t LDAP attribute rule.	s. Specify how the attribut	tes will map to the outgo	ing claim types that will	be issued
	der Rule Name	<ul> <li>Configure Claim Rule</li> </ul>	Claim rule	e name:				
On	der Rule Name		User Pri	incipal Name				
			Rule terr	plate: Send LD/	AP Attributes as Claims			
			Attribute	store:				
			Active D	Directory			~	
			Mapping	of LDAP attribu	tes to outgoing claim type	s:		
				LDAP Attribute add more)	e (Select or type to	Outgoing Claim Type	(Select or type to add	more)
			<u>۲</u>	User-Principal-	Name ~	UPN		~
			• •		~			~
			_					
Ac	dd 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 Parentee Sector Sate (MTF1) and
C:\Program Files\MachSol\ADFS Login App Pass-through authentication	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Connect as Test Settings Binding	Connect As ? ×
Type:         IP address:         Port:           https         10.1.210.123         443	Path credentials: O Specific user:
Host name: slogin.machsol.com	Set      Application user (pass-through authentication)
Require Server Name Indication	
Disable HTTP/2	OK Cancel
Disable OCSP Stapling	
SSL certificate:	
MachSolWildCard2024 V Select	View
Start Website immediately	
ОК	Cancel



## 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	3rd Party Authentication Two Factor Authentication Settings					
Company Profile	*Enable login using Microsoft account:					
Menu Settings	*Enable login using ADFS:					
Built-in Modules	*ADFS Login App Url: https://slogin.machsol.com					
Reseller Settings						
Configure Alerts	*Sigout from ADFS on panel signout:					
Authentication	Save Settings					
SMS Settings						
ά.						

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