TACHO MASTER

Single Sign On (SSO)



MASTER

Single Sign On - SAML2 Configuration

Parse metadata URL:

arsing a new URI, will overwrite the settings below if already set. You wil e able to review them before saving

dentity Provider (IdP) Entity ID

IdP Public Key

IdP Public Signing Key

Choose file No file chose Process File

etadata file will overwrite the settings below arsing a new set. You will be able to review them before saving.

Help

Parse URL

Identity provider (IdP) metadata URL: type the Identity Provider's (IdP) metadata URL.

Public Keys: Your IdP may be configure with a single public key or separate keys for signing and encryption. Fill in the appropriate fields with SHA-1 certificates provided by your IdP. Only RSA certificates are supported, DSA certificates are not

Sign-in URL: fill in the remote sign-in URL of your IdP. This is the URL where Tachomaster will redirect your users for signing-in. Sign-out URL: fill in the remote sign-out URL of your IdP. This is the U

Configuring Tachomaster for Single Sign-On (SSO)

Table of Contents

Login to Tachomaster	4
Create a Tachomaster default SSO user profile	4
Access the Tachomaster SSO configuration	5
Create and download Metadata file	6
Steps to configure ADFS	7
Add Relaying Party Trust	7
Import into Tachomaster	8

Please note that the following is a guide to point you in the right direction. Road Tech do not support AD FS, please refer to your provider for any help required.



 Calendar Modules Reports Tools Data Download 	Download Supplies Help 🔻 Invoi
Single Sign On - SAML2 Configuration	
Parse metadata URL: Parse URL Parsing a new LIRL will overwrite the settings below if already set You will be able to	Parse metadata file: Browse No file selected. Process File
review them before saving.	Parsing a new metadata file will overwrite the settings below if already set. You will be able to review them before saving.
Default User Profile for new users	Sign-on LIPI
SSO Default 🗸	The following URL should be used for single-sign-on:
Identity Provider (IdP) Entity ID *	https://www.tachomaster.co.uk/sso/signon/ROADTEDL/
http://sts.YOURDOMAIN.com/adfs/services/trust	For identifying User Attributes the following URL can be used to display available fields:
IdP Public Key	https://www.tachomaster.co.uk/sso/signon/RDADTEDL/2attr
^	Capital Devider Deta
TAeFw0yMjA0MDQxMTA3MDdaFw0yMzA0MDQxMTA3MDdaMCsxKTAnBgNV	Service Provider Data
IdP Public Signing Key	https://www.tachomaster.co.uk/sso/metadata/ROADTEDL/
	Your Identity Provider may require the following certificate information:
li.	BEGIN CERTIFICATE
Sign-in URL*	and a subscription of the second s
Sign-In Binding *	
	the start of the start start and the start start
Sign-out URL*	h6tgetWQmyCLPwT3ar312HaJ80zS0vz6ShPODq73eaFABUC6pjpo7A==
nups//sta.gistwonu.com/auts/is/	END CERTIFICATE
Sign-out Binding	
ur noasismamesticisAMEZ.0001ndingSH11P*Redirect	Help Identity provider (IdP) metadata (ID) - type the Identity Provider's (IdP) metadata (ID)
Name ID Format *	Public Keys: Your IdP may be configure with a single public key or separate keys for signing
or noososiemes.tc.pepetc.2.0.nemetrini mettransient	and encryption. Fill in the appropriate fields with SHA-1 certificates provided by your IdP. Only RSA certificates are supported, DSA certificates are not.
User Attributes	Sign-in URL: fill in the remote sign-in URL of your IdP. This is the URL where Tachomaster
_nameid	will redirect your users for signing-in.
-	will redirect your users when they sign-out.
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	User Attributes: fill in the attribute names for each of the fields as they will appear in the SAML2 response.
art Nama *	and a see of the second s
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	* Required field
Email	



1

Login to Tachomaster

To do any of the actions required in Tachomaster you must be logged in as a Tachomaster administrative user. If your user level is not administrator please contact one of your company's administrators or super user to upgrade your account. Please do not contact Road Tech support to do this.

Create a Tachomaster default SSO user profile

When setting up the SSO configuration you will be asked to apply a "Default User Profile for new users". All users can be moved to other profiles once created but we would suggest the initial default is a low access level (Departmental Manager is the lowest default profile but would still provide a lot of information). This will prevent users seeing data they should not have access before you allocate a specific profile and access for their roles.

To create a profile go to Tools> Add/Amend> User Profiles (https://www.tachomaster.co.uk/userprofile.php)

If you require help in setting up the profiles, please see the Road Tech knowledge base User Profiles video from Help> Tutorials and Videos (https://kb.roadtech.co.uk/en/tachomaster/tutorials)

0	MAS										Q, Sear	ch for Driver	r/Vehicle	Find
lome	List 🔻	Calendar 🔻	Modules 🔻	Reports 🔻	Tools 🔻	Data Dow	nload		ſ	Download	Supplies	Help 🔻	Invoices	Logout
			User	Profiles										
			Chan	ges saved!										
			Prot	ile Name	Create	View	Amend	Delete	View	Edit				
			Adn	inistrator	All	All	All	All	B.	-				
			Dep	artmental Manager	Some	Some	Some	Some		-				
			Rea	d Only	-	All	-	-	E.					
			SSO	Default	-	Some	-	-						
			Traf	fic Manager	Some	Some	Some	Some						
			<u>» Ac</u>	d new profile										
			Help											
			A User (Admin each of	Profile defines a set o strator and Departm these profiles have.	f permission ental Manag	s for use in er), click th	Tachomaste e View icon	r. By default above to see	2 User Pro what perm	files exist hissions				
			Click 'A	dd new profile' to cre	ate a custom	User Profi	le to fit the r	ole you want	t to assign t	o a user.				
			A User	Profile can be assigne	d to one or n	nany users	through the	Add/Amend	Users scre	en.				
											J			



Access the Tachomaster Single Sign On (SSO) configuration

Once logged in, change your browser URL to

https://tachomaster.co.uk/sso/configure (and then hit enter)

The "Single Sign On—SAML2 Configuration" page is now shown.



Download the Service Provider Metadata file by clicking on the "Metadata" link.

If you need to download again, the form now presented on the configuration form.

Single Sign On - SAML2 Configuration	
Configure your Identity Provider (IdP) Your IdP metadata will be available either by a public URL or from an XML download - or b Enter your JdP metadata URL: Parse URL Parse URL Parse URL will overwrite the settings below if already set. You will be able to review them before saving.	oth. Use the options below to populate the configuration. Select a metalate filter how our computer and click Process File: <u>Choose Rin</u> No. Bio chosen Proses File Paraling a new metadata file will overwrite the settings below if already set. You will be able to review them before saving.
Default User Profile for new users Departmental Manager	Sign-on URL The following URL should be used for single-sign-on:
IdP Entity ID *	https://www.tachomaster.co.uk/sso/signon/ROADTEDL/
IdP Public Key	For identifying User Attributes the following URL can be used to display available fields: https://www.tachowaster.co.uk/sso/sEgnon/ROADTEDL/Tattr Service Provider Data
IdP Public Signing Key	Metadata:
IdP Public Encryption Key	Help Identity provider (IdP) metadata URL: type the Identity Provider's (IdP) metadata URL. Public Kow: Your IdP may be configure with a single public key or separate keys for signing
Sign-in URL *	and encryption. Fill in the appropriate fields with SHA-1 certificates provided by your IdP.

Select your SSO default User Profile.



The follow steps are carried out within ADFS—if you require any support on ADFS please contact your provider.

Add Relying Party Trust

👾 🔶 🏟 🖄 🚾 🛙					
AD 55 Service Attribute Sto Anthenicasi Celificate Claim Decri Device Regis Endpoints Scope Decr Access Control Relying Party Claim Service Access Control Relying Party Application	res on Methods ptions tration tration ToTotes Add Relying Party Trus View New Window from He Refresh Help	Relying Party Trusts Declay Name Tachomaster 1	Enabled Yes	Type WS-T	ldertifier https://www.tachomaster.co.uk/isso/metadat.

🖬 Add Relying Party Trust V	Vizard	×				
Welcome						
Steps	Welcome to the Add Relying Party Trust Wizard					
Welcome	Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use \Vindows					
Select Data Source						
 Choose Access Control Policy 	Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. Learn more					
Ready to Add Trust	Caims aware					
G Finish	O Non claims aware					
	< Previous Start Canor	el				





Using the metadata XML file created on page 6 and import as above.

Steps	Enter the display name and any optional notes for this relying party.	
Welcome	Display name:	
Select Data Source	Tachomaster 2	
Specify Display Name	Notes:	
 Choose Access Control Policy 		^
Ready to Add Trust		
Finish		
		~



Dana			
Helpe Welcome Select Data Source Specify Display Name Choose Access Control Policy Ready to Add Trust Finish	Choose an access control policy: Name Permit everyone and require MFA Permit everyone and require MFA for spocific group Permit everyone and require MFA form extrante access Permit everyone and require MFA form unsufferticitated devices Permit everyone and require MFA form unsufferticitated devices Permit everyone and require MFA form unsufferticitated devices Permit everyone for intransf access Permit epecific group Policy Permit everyone	Description Grant access to everyone and requit Grant access to everyone and requit Grant access to the intranet users and Grant access to everyone and requit Grant access to everyone and requit Grant access to everyone and requit Grant access to users of one or more >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	~

Steps	The solving party taut has been configured. Devices the following cattings, and they shall Next to add the						
Welcome	relying party trust to the AD FS configuration database.						
Select Data Source	Monitoring Identifiers Encountion Stanature Accented Claims Organization Endoprinte Note 1						
Specify Display Name	Specify the display name and identifiers for this relying party trust.						
Choose Access Control Policy	Display name:						
Ready to Add Trust	Tachomaster 2						
Finish	Relving party identifiers:						
	https://www.tachomaster.co.uk/sso/metadata/TONYTESU/						
	https://www.tachomaster.co.uk/sso/metadata/TONYTESU/						



Display Name	Enabled	Туре	Identifier	Access Control Policy
Tachomaster 1	Update Edit Acc	from Fede	ration Metadata	Permit everyone
	Edit Clai	m Issuand	e Policy	
	Disable			
	Properti	es		
	Delete			
	Help			

Right click the "Relaying Party Trust" and click "Edit Claim Issuance Policy". Click "Add Rule" and create as follows in *fig* 1/2







achomaster		
le template: Send LDAP Attributes as C	Claims	
tribute store:		
ctive Directory		~
apping of LDAP attributes to outgoing cl	laim types	
LDAP Attribute (Select or type t add more)	to	Outgoing Claim Type (Select or type to add more)
SAM-Account-Name	~	SAMAccountName ~
Given-Name	~	Given Name 🗸 🗸
Sumame	~	Sumame ~
E-Mail-Addresses	~	E-Mail Address ~
•	~	~



Note, it may be necessary to add "SAMAccountName" in "Claim Descriptions".

Obtain Federation Metadata XML

Inside the ADFS Management application, locate the Federation Metadata xml file. This can be found by clicking on ADFS > Service > Endpoints then locate the URL path in the "Metadata" section. The path is typically **/FederationMetadata/2007-06/FederationMetadata.xml** as seen below:





Fig 10

Metad	ata	
Yes	Yes	/adfs/services/trust/mex
Yes	Yes	/FederationMetadata/2007-06/FederationMetadata.xml
Yes	No	/adfs/fs/federationserverservice.asmx

Fig 11

Export the file and send to Road Tech Computer Systems to be imported in to Tachomaster.

Once you have configured your ADFS:

- Visit https://www.tachomaster.co.uk/sso/configure/ again



- Upload/Parse the metadata file from ADFS (this pre-populates all fields except for the User Attributes)

Single Sign On - SAML2 Configuration

Configure your Identity Provider (IdP)	
Your IdP metadata will be available either by a public URL or from an XML download - or bot	h. Use the options below to populate the configuration.
Enter your IdP metadata URL: Parse URL	Select a metadata file from your computer and click Process File: Choose file No file chosen
Parsing a new URL will overwrite the settings below if already set. You will be able to review them before saving.	Process File Parsing a new metadata file will overwrite the settings below if already set. You will be able to review them before saving.
Default User Profile for new users	Sign-on URL
Departmental Manager 🗸	The following URL should be used for single-sign-on:
dP Entity ID *	https://www.tachomaster.co.uk/sso/signon/ROADTEDL/
	For identifying User Attributes the following URL can be used to display available fields:
dP Public Key	https://www.tachomaster.co.uk/sso/signon/ROADTEDL/?attr
	Service Provider Data
dP Public Signing Key	Metadata: 🛓
	https://www.tachomaster.co.uk/sso/metadata/ROADTEDL/
//////////////////////////////////////	Help
	Identity provider (IdP) metadata URL: type the Identity Provider's (IdP) metadata URL.
Sign-in URL*	Public Keys: Your IdP may be configure with a single public key or separate keys for signing and encryption. Fill in the appropriate fields with SHA-1 certificates provided by your IdP.

- If you don't know the User Attribute names populate them with *something* temporarily

- Save- The metadata URL will show on the right, ADFS will need that - do that part in ADFS

If you don't know the User Attributes, use the URL listed in the SSO configure page with <code>?attr</code> at the end:

You should see something like this—the company code (shown as TONYTESU will be your own company code).

4		
TONYTESU		
Name	Value	
<pre>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/SAMAccountName http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname </pre>	t*****e T**y J*****e t*****e	







Tachomaster copyright © 2022 – Road Tech Computer Systems Ltd All rights reserved AD FS is a Microsoft Product

Road Tech Computer Systems Ltd, Shenley Hall, Rectory Lane, Shenley, Radlett, Hertfordshire, UK: T: 01923 460000 E:crm@roadtech.co.uk

Version: 2.2





