SETTING UP ADFS

AMANUAL

	Company settings			
å	Account Users Em	ail settings Theme Advanced		
*	On this page you can set up Single Sign-on options). The unique nam name.	: Sign-on for your company. Enter a title for your own refer e will be used to log in on the alternative Single Sign-on log	ence (this is mostly handy for those wishing to use m in page. You can only use lower case letters and numi	ultiple Single bers for this
å	The Entity ID from the Provider N setting up Single Sign-on on this p Service.	fetadata XML and the Provider Metadata XML can be four age, use the url (visible by clicking 'edit' on the overview yo	nd in the Provider Service you wish to use for Single S ou see after saving) to add this service as trusted in yo	ign-on. After ur Provider
å ^ÿ å	If you need help setting up Single	Sign-on for your company, feel free to download our manu	al.	
	Title	Name		
				Please f
	Entity	Metadat	a	
-				



Contents

Before configuring the settings on the ADFS server	3
Set up ADFS	6
Add Relying Party Trust	7
Set the Claim Rules	
Rule 1	17
Rule 2	17
Rule 3	18
What SSO looks like for messenger users	

Before configuring the settings on the ADFS server

Sign in on the messenger with an account with administrator rights. When using the web version, you will find the option 'Company settings' under the dropdown menu at the top right corner of your screen.

Click on 'Company settings'.



Then click on the tab on the right: 'Advanced'.

	Messenger info@messenger.com	New	Jane Doe	≡
-	Company settings			
Å	Account Users Email setting	Theme Advanced		
i	On this page you can specify what functionaliti	es users within your organization h	ave access to.	^
Å	Alternative sign in Applications	Alarm service		
	Coworkers can only be invited on approv	ed company domains	Pin login code mandatory for mobile users (Android only)	
Å ^ÿ Å	Ves No		Ves O No	
-	User can export conversations to a PDF		User can create a group chat by sending a email	
	Ves No		• Yes No	
				_
	Show message content in mobile notifica	tions	Show message content in emails	
?	Ves No		Ves No	
Ŀ	K			×

Here you will see three buttons at the top of the page. Choose the left one: 'Alternative sign in'. Then you will see the option 'Add Provider' in the top right corner. Click on it to show the fields necessary to start setting up ADFS.

	Messenger info@messenger.com	New		Jane Doe	≡
-	Company settings				
Å	Account Users Email settings	Theme	Advanced		
	back to advanced		Å	Add Provider Download manual	
å	On this page you can set up Single Sign-on for y Sign-on options). The unique name will be used name.	our company. Ente to log in on the alt	er a title for your own reference (this is mostly handy fo ternative Single Sign-on login page. You can only use lo	or those wishing to use multiple Single wer case letters and numbers for this	
å [†] å	The Entity ID from the Provider Metadata XMI setting up Single Sign-on on this page, use the u Service.	. and the Provider ırl (visible by clicki	Metadata XML can be found in the Provider Service yon ng 'edit' on the overview you see after saving) to add th	ou wish to use for Single Sign-on. After nis service as trusted in your Provider	
	If you need help setting up Single Sign-on for yo	our company, feel f	ree to download our manual.		
?					
. ●					

Enter the following information:

Title: This is what you will see as Administrator – choose a title that is clear to you.

Name: This is the name end users will use to connect to the ADFS infrastructure.

Entity: This is the URL from the ADFS server, for example: <u>https://adfs.COMPANY.com/adfs/services/trust</u>

Metadata: Here you can paste the information from federationmetadata.xml, retrieved from the ADFS server. The direct URL will have this format: https://adfs.COMPANY.com/federationmetadata/2007-06/federationmetadata.xml

After saving these settings, the messenger will generate a URL for you, which you can use to configurate the ADFS on the ADFS server.

Title	Name
Entity	Metadata

Save Cancel

Set up ADFS

Open the ADFS management console on the ADFS server.



Add Relying Party Trust

Click on 'Add Relying Party Trust' in the column on the right. You will then see the following intro screen – click 'Start'.

Ŷ	Add Relying Party Trust Wizard
Welcome	
Steps Welcome Select Data Source Configure Multifactor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	Welcome to the Add Relying Party Trust Wizard This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions. The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.
	< Previous Start Cancel

The 'xxxx' key consists of a unique code that is different for each company and can be generated based on the contents of the MetaData field.

If you have followed the first steps of this manual correctly, you will have already generated this URL.

Fill in the Relying Party Trust URL and click 'Next'.

\$	Add Relying Party Trust Wizard
Select Data Source	
Steps Welcome Select Data Source Configure Multifactor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	Select an option that this wizard will use to obtain data about this relying party:
	< Previous Next > Cancel

On the next screen you can enter a name and notes according to your own preferences. Click 'Next'.

\$	Add Relying Party Trust Wizard	x
Specify Display Name		
Steps	Enter the display name and any optional notes for this relying party.	
Welcome	Display name:	
Select Data Source	Enter messenger name	
Specify Display Name	Notes:	
Configure Multi-factor Authentication Now?		<u>^</u>
 Choose Issuance Authorization Rules 		
Ready to Add Trust		
• Finish		~
	< Previous Next > Cancel	

Next you will see the following screen – for our messenger, you can ignore this one. Click 'Next'.

\$	Add Relying Party Trust Wizard
Steps	Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.
Select Data Source	Multifactor Authentication Global Settings
Specify Display Name Configure Multi-factor Authentication Now?	Requirements Users/Groups Not configured
Choose Issuance Authorization Rules Postute Add Taut	Device Not configured Location Not configured
 Finish 	
	 I do not want to configure multifactor authentication settings for this relying party trust at this time. Configure multifactor authentication settings for this relying party trust. You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see <u>Configuring Authentication Policies</u>.
	< Previous Next > Cancel

Next you will see the screen below. For our messenger, the default settings are correct. Click 'Next'.

\$	Add Relying Party Trust Wizard
Choose Issuance Auth	orization Rules
Steps Velcome Select Data Source Specify Display Name Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	 Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules. Permit all users to access this relying party The issuance authorization nules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access. Deny all users access to this relying party The issuance authorization nules will be configured to deny all users access to this relying party. You must later add issuance authorization nules to enable any users to access this relying party. You must later add issuance authorization nules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.
	< Previous Next > Cancel

You will then see a little summary. Click 'Next'.

\$	Add Relying Party Trust Wizard	x		
Ready to Add Trust				
Ready to Add Trust Steps • Welcome • Select Data Source • Specify Display Name • Configure Multi-factor Authentication Now? • Choose Issuance Authorization Rules • Ready to Add Trust • Finish				
	This relying party was last updated from federation metadata on: 16-6-2016 <pre></pre>	ancel		

You have now reached the 'Finish' screen. Keep the check mark for 'Edit Claim Rules' on – you will need to configure these next. Click 'Close'.

\$	Add Relying Party Trust Wizard	x
Finish		
Steps Welcome Select Data Source Specify Display Name Configure Multifactor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust	The relying party trust was successfully added to the AD FS configuration database. You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in. Implicit Open the Edit Claim Rules dialog for this relying party trust when the wizard closes	
Finish		
	Close	

Set the Claim Rules

The 'Edit Claim Rules' screen will be opened after you close the previous screen.

🖗 Edit Claim Rules for iml.alterdesk.com 🗖 🗖 🗙			
Issuance Transform Rules Issuance Authorization Rules Delegation Authorization Rules			
The following transform rules specify the claims that will be sent to the relying party.			
Order Rule Name Issued Claims			
Add Rule Edit Rule Remove Rule			
OK Cancel Apply			

In the 'Claim Rules settings', you will need to create three rules.

The first two serve to change the unique account name of the user into a format that can be used by the messenger. Start for both Rule 1 and Rule 2 with 'Add Rule'.

Select 'Send Claims Using a Custom Rule' and click 'Next'.

\$	Add Transform Claim Rule Wizard	x
Select Rule Template		
Steps • Choose Rule Type • Configure Claim Rule	Select the template for the claim rule that you want to create from the following list. The description provide details about each claim rule template. Claim rule template: Send Claims Using a Custom Rule Claim rule template description: Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are written in the AD FS claim rule language. Capabilities that require custom rules include: Sending claims from a SQL attribute store Sending claims from a custom attribute store Sending claims only when 2 or more incoming claims are present Sending claims only when 2 or more incoming claim value matches a complex pattern Sending claims for use only in later rules	25
	< Previous Next > Cancel	

Next you will see the screen below, in which you can enter your Custom Rules. You can find these Custom Rules on the next page.

\$	Add Transform Claim Rule Wizard	x
Configure Rule		
Steps Choose Rule Type Configure Claim Rule	You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language. Claim rule name:	
		<
	< Previous Finish Cancel	

Rule 1

Rule 1 consists of the following 'Custom Rule':

c:[Type ==

"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname ", Issuer == "AD AUTHORITY"]

=> issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/windowsaccountname"
), query = ";samaccountname;{0}", param = c.Value);

Rule 2

Rule 2 consists of the following 'Custom Rule': c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/windowsaccountname"]

=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient");

Rule 3

To configure Rule 3, start with 'Add Rule'. Then select 'Send LDAP Attributes as Claims' and click 'Next'.

\$	Add Transform Claim Rule Wizard		
Select Rule Template			
Steps	Select the template for the claim rule that you want to create from the following list. The description provides		
Choose Rule Type	details about each claim rule template.		
Configure Claim Rule	Claim rule template:		
	Send LDAP Attributes as Claims 🗸		
	Claim rule template description:		
	Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.		
	< Previous Next > Cancel		

Give the rule a name. In the example we have entered 'Attributes'. Select 'Active Directory' as your Attribute store.

\$		Add Transform Claim Rule	Wizard
Configure Rule			
Steps • Choose Rule Type • Configure Claim Rule	You ca which t issued Claim n Atmbut Rule te Attribut Active Mappir	In configure this rule to send the values of L to extract LDAP attributes. Specify how the from the rule. ule name: es mplate: Send LDAP Attributes as Claims e store: Directory ig of LDAP attributes to outgoing claim type LDAP Attribute (Select or type to add more)	DAP attributes as claims. Select an attribute store from attributes will map to the outgoing claim types that will be s: Outgoing Claim Type (Select or type to add more)

Configure the next screen the same as the example in the screen-print below:

E-Mail-Addresses	E-Mail address
Given-Name	Given Name
Surname	Surname
Display-Name	Display Name
objectGUID*	objectGUID

*The objectGUID attribute might need to be entered manually, because it's not selectable by default. Sometimes the manually entered entry disappears, but then it needs to be entered again to make it visible.

		Edit Rule - Attributes				
You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.						
laim rule name:						
ttributes						
ule template: Send LDAP Attributes as Claims	3					
ttribute store:						
ctive Directory						
lapping of LDAP attributes to outgoing claim ty	ypes		_			
LDAP Attribute (Select or type to add more)		Outgoing Claim Type (Select or type to add more)	Â			
E-Mail-Addresses	~	E-Mail Address 🗸				
Given-Name	~	Given Name 🗸 🗸]≡			
Sumame	~	Sumame 🗸 🗸				
Display-Name	~	Display Name 🗸 🗸				
objectGUID	~	objectGUID 🗸				
View Rule Language		OK				

What SSO looks like for messenger users

At the bottom of the login screen, choose 'Alternative sign in'.



You will then see this screen:

Alternative sign in			
Sign in			
	_		
Sign in	Alternative sign in		

Enter your chosen Provider Name in the 'Provider' field (this will usually be the company name). You have set this in the messenger company settings.