Configuring Salesforce

Complete the following steps to configure Salesforce:

- Step 1A: Download the SP metadata only (If IDP configuration already exists) OR
- Step 1B: Create IDP configuration and Download the metadata
- Step 2: Update the IDP configuration

Step 1A: Download metadata for existing IdP configuration

If you already have an IdP configuration set up, then use the below procedure to download the metadata for IdP:

Prerequisites

- Ensure that the IdP configuration is existing; else follow **Step 1B**.
- Ensure that you are in the classic view for Salesforce.

Procedure

1. Login to Salesforce account with admin privileges.



2. Under Administer, click Security Controls > Configure single-sign on for your organization.

salesforce	earch	\hat{Q} Soutch to Lightning Expensions bases minorshymine + Soutz Help Content	D
Home Chatter Libraries C	Content Subscriptions +		
Quick Find / Search () Q. Expand All Collapse All	Security Controls Developer Edition	Help for this Pag	je <mark>19</mark>
Lightning Experience Transition Assistant Nove to the new more productive Satisfice. Out Elastic	Security Controls - Manage your smaller constraints - Constraint constraints your set on your specification - Constraint constraints - Manage your smaller constraints - Constraint constraints - Manage your set on your specification - Constraint constraints - Constraint - Co	View auch teur of changes to your solution Prove and the out of several existence Designed administration of several existence Administration devices and control existence Administration devices Administration devices	
Home	- Company you remain a remain	- Lateral Providence	_
Administer Manage Users Manage Apps	Getting Started • Tips & Hints for Sharing Data • Security implementation Quide		
Monage Territories Monage Territories Company Profile Patal Castification Executing Costinue Beneting Costinue Login From Activations Beneting Access Activations Descond Monagement Light Access Activations Descond Monagement Light Access Activations Descond Act			

3. On the **Single Sign-On Settings** page, click on the IdP name to view the configuration.

Single Sign-On Settings							
2onfigure single sign-on in order to authenticate users in salesforce com from external environments. Your organization has the following options available for single sign-on:							
 Federated authentication, a single 	le sign-on method that uses SAML assert	ons sent to a Salesforce endpoint.					
		Edit SAML Assertion Validator					
Federated Single Sign-On Using SAN SAM	ML ML Enabled 🖌						
SAML Single Sign-On Settings		New New from Metadata File New from Metadata URL					
SAML Single Sign-On Settings Action Name	SAML Version	New New from Metadata File New from Metadata URL	Entity ID				
SAML Single Sign-On Settings Action Name Edit Del	SAML Version 2.0	New] New from Metadata File New from Metadata URL	Entity ID				
SAML Single Sign-On Settings Action Name Edit Del Edit Del	SAML Version 2.0 2.0	New New from Metadata File New from Metadata URL	Endty ID				
SAML Single Sign-On Settings Action Name Edt Del Edt Del Edt Del Edt Del	SAML Version 2.0 2.0 2.0	New Trom Metadata File New from Metadata URL	Entity ID				
SAML Single Sign-On Settings Action Name Edd [Del Edd [Del Edd [Del Edd [Del	SAML Version 2.0 2.0 2.0 2.0 2.0	New Trom Metadula File New from Metadata URL	Entity ID				
SAML Single Sign-On Settings Action Name Edit [Del Edit [Del Edit [Del Edit [Del Edit [Del	SAML Version 2.0 2.0 2.0 2.0 2.0 2.0 2.0	New from Metadata File New from Metadata URL Issuer	Entity ID				

4. Click Download Metadata and save the file as "sp-metadata.xml".

SAML Single Sign-On Settin Back to Single Sign-On Settings	ngs	
	Edit Delete Clone Download Metadata SAML Assertion Validator	
Name	adfs API Name	adfs
SAML Version	2.0	
Issuer	http://adfs .com/adfs/services/trust Entity IC	https:// my.salesforce.com
Identity Provider Certificate	CN=ADFS Signing - adts com Expiration: 4 Oct 2020 04:50:37 GMT	
Request Signing Certificate	SelfSignedCert 24Sep2019 230626	
Request Signature Method	RSA-SHA256	
Assertion Decryption Certificate	Assertion not encrypted	
SAML Identity Type	Username	
SAML Identity Location	Subject	
Service Provider Initiated Request Binding	HTTP POST	
Identity Provider Login URL	https://adfs com/adfs/is/	
Custom Logout URL		
Custom Error URL		
Single Logout Enabled	✓	
Identity Provider Single Logout URL	https://adfscom/adfs//s/	
Single Logout Request Binding	HTTP Redirect	
Just-in-time User Provisioning		
User Provisioning Enabled		
Endpoints		
View SAML endpoints for your organization, communit	es, or custom domains.	
Your Organization		
Login URL	https:// .salesforce.com?so=00D0b00000vMGs	
Logout URL	https:// my.salesforce.com/services/auth/sp/sami2/logout	
OAuth 2.0 Token Endpoint	https:// my.salesforce.com/services/oauth2/token?so=00D0b000000vMGs	
	Edit Delete Clone Download Metadata SAMI Assertion Validator	

Step 1B: Creating IDP configuration and download the metadata

If you do not have the IdP configuration created, then follow the below procedure to add an IdP configuration and then download the metadata file:

Prerequisites

• You must have a Salesforce account with admin privileges.

Procedure

1. Login to Salesforce account with admin privileges.



2. Under Administer, click Security Controls > Configure single-sign on for your organization.

salesforce 👫 🔹	ard. Seed.	Satisti to Lipitolog Experience to one misentrycine Setup Help Constant
Home Chatter Libraries C	ontent Subscriptions +	
Quick Find / Search () Q Expand Al Collapse Al	Security Controls Developer Edition	Hadp for this Plage 🖯
Lightning Experience Transition Assistant Move to the new more produce Salesforce Mobile Quick Start	Security Control A Security for control A Security for a security of	Veer audit tosi of charges to since statu Force and for an orient to reset parameters Prove and for an orient and colone statuta Admitistic of Diritho data Admitistic of Diritho data
Home	Configure your identity Provider	Platform Encryption
Administer Manage Users Manage Apps	Getting Started - Tos & Hinto Strawng Data - Security Implementation Ouide	
Monage Territories Company Profile Data Classification Socurity Controls Security Controls		
Legin Flows Network Access Activations Session Management Login Access Policies Centricale and Key Management Single Sign-Cin Settings		

3. On the Single-sign on settings page, click New from Metadata File.

Single Sign-On Settings							
Configure single sign-on in order to authenticate users in salesforce.com from external environments. Your organization has the following options available for single sign-on:							
Federated authentication, a single sign-on m	nethod that uses SAML assert	ions sent to a Salesforce endpoint.					
		Edit SAML Assertion Validator					
Federated Single Sign-On Using SAML							
SAML Enabled	✓						
SAML Single Sign-On Settings		New New from Metadata File New from Metadata	JRL				
Action Name	SAML Version	Issuer			Entity ID		
Edit Del	2.0						
Edit Del	2.0						
Edit Del	2.0						
Edit Del	2.0						

4. On the **SAML single sign-on settings** page, click **Choose File** and upload the "**idp-metadata.xml**" downloaded when creating an application in IdP. Click **Create**. The settings for single-sign on displays.

SAML Single Sign-On Settings

Create configuration using an XML file (1 MB or smaller) containing SAML 2.0 settings from your identity provider. (Salesforce doesn't store this file.)

Create
Metadata File Choose File No file chosen
Create

- 5. On the **SAML single-sign on settings** page, provide the configuration in the following fields:
- a. Name
- b. API Name
- c. Select HTTP POST in "Service Provider Initiated Request Binding".
- d. Click Save.

SAML Single Sign-On Settin	lgs				Help for this Page 🔮
	Save Save & New Cancel				
Name	adfs		API Name	adfs	
SAML Version	2.0				
Issuer	http://adfs.com/adfs/		Entity ID	https:// r	
Identity Provider Certificate	Choose File No file chosen	Currer	nt Certificate	CN=ADFS Signing - adfs com Expiration: 4 Oct 2020 04:50:37 GMT	
Request Signing Certificate	SelfSignedCert_24Sep2019_230626 ·				
Request Signature Method	RSA-SHA256 V				
Assertion Decryption Certificate	Assertion not encrypted				
SAML Identity Type	Assertion contains the User's Salesforce username Assertion contains the Federation ID from the User object Assertion contains the User ID from the User object				
SAML Identity Location	Identity is in the Nameldentifier element of the Subject statement Identity is in an Attribute element				
Service Provider Initiated Request Binding	HTTP POST HTTP Redirect				
	Warning: The metadata file specifies multiple bindings for the login URL.				
Identity Provider Login URL	https://adfs com/adfs/ls/				
Custom Logout URL					
Custom Error URL					
Single Logout Enabled					
Identity Provider Single Logout URL	https://adfs.com/adfs/ls/				
Single Logout Request Binding	HTTP POST HTTP Redirect				
	Warning: The metadata file specifies multiple bindings for the single logout URL.				
Just-in-time User Provisioning					Required Information
User Provisioning Enabled					
	Save Save & New Cancel				

6. The configuration is complete. Click **Download Metadata** and save the file as "**sp-metadata.xml**".

SAML Single Sign-On Settings

Back to	Single	Sign-On	Settings

	Edit	Delete	Clone	Download Metadata	SAML Assertion Validator			
News				()		A DI Marris		
Name	adis					APIName	adis	
SAML Version	2.0					5-11-1D	http://	
Issuer	nttp://adfs .com/adfs/services/trust					Entity ID	https:// my.salesto	prce.com
identity Provider Certificate	Expiration: 4 Oct 2020 04:50:37 GMT							
Request Signing Certificate	SelfSignedCert 24Sep2019 230626							
Request Signature Method	RSA-SHA256							
Assertion Decryption Certificate	Assertion not encrypted							
SAML Identity Type	Username							
SAML Identity Location	Subject							
Service Provider Initiated Request Binding	HTTP POST							
Identity Provider Login URL	https://adfs com/adfs/ls/							
Custom Logout URL								
Custom Error URL								
Single Logout Enabled	✓							
Identity Provider Single Logout URL	https://adfs.com/adfs/ls/							
Single Logout Request Binding	HTTP Redirect							
Just-in-time User Provisioning								
User Provisioning Enabled								
Endpoints								
View SAML endpoints for your organization, communit	es, or custom domains.							
Your Organization								
Login URL	https:// v.salesforce.	com?so=00	D0b000	000vMGs				
Logout URL	https:// my.salesforce.	com/service	s/auth/s	p/saml2/logout				
OAuth 2.0 Token Endpoint	https:// my.salesforce.	com/service	s/oauth	2/token?so=00D0b000	000vMGs			
	Edit	Delete	Clone	Download Metadata	SAML Assertion Validator			

Next Steps: Create a Federated Pair in Access. For more information, see Overview.

Step 2: Updating IdP configuration

Prerequisites

• The IdP configuration is updated after creating a federated pair in MobileIron Access. You must download the proxy metadata files from Access.

Procedure

- 1. Login to Salesforce account with admin privileges.
- 2. Under Administer, click Security Controls > Configure single-sign on for your organization.

🥮 🕼 . e	et. Man	
Home Chatter Libraries C	ontent Subscriptions +	
Quick Find / Search (D Q, Expand M Collapse M	Security Controls Developer Edition	mag to the Page G
⇔ ∮ Lightning Experience Transition Assistant More to the nex. more productive Sensitives Get Stande	Second Controll Versionage room content chambers - Software and chambers - So	View with Net / dampie Ity par wine - Prova of your wants from dampieson - Antonizati mana Prova - Antonizati (2019) and dampieson - Antonizati (2019) and dampieson - Vieway watchingto (2010) anyon - View
Salesforce Mobile Quick Start	Configure single-sign on for your organization Manage authentication providers	Manage Sessions Manage OAuth-pustom scopes
Home	Configure your identity Provider	Pallom Encypton
Administer	Cetting Surted Tring Surted Tri	
Manage Learning August Company Profile Data Classification Executly Alerts Feachty Nets Health Check Sharing Settings		
Part Accessibility Pressource Parkies Bession Settings Login Flows Network Access Session Management Copfication Management Conflicted and Kay Management Single Spic On Settings		

3. On the **Single Sign-On Settings** page, click on the IdP name to view the configuration.

Single Sign-On Settings						
Configure single sign-on in order to aut	henticate users in salesforce.com from	external environments. Your organization has the following options available f	or single sign-on:			
 Federated authentication, a sing 	gle sign-on method that uses SAML assert	ions sent to a Salesforce endpoint.				
		Edit SAML Assertion Validator				
Federated Single Sign-On Using SA	ML					
SAI	ML Enabled 🖌					
SAML Single Sign-On Settings		New New from Metadata File New from Metadata URL				
SAML Single Sign-On Settings	SAML Version	New from Metadata File New from Metadata URL		Entity ID		
SAML Single Sign-On Settings Action Name Edit Del	SAML Version 2.0	New Trom Metadata File New from Metadata URL		Entity ID		
SAML Single Sign-On Settings Action Name Edit Del Edit Del	SAML Version 2.0 2.0	New) New from Metadata File) New from Metadata URL		Entity ID		
SAML Single Sign-On Settings Action Name Edit Del Edit Del Edit Del	SAML Version 2.0 2.0 2.0	New New from Metadata File New from Metadata URL		Entity ID		
SAML Single Sign-On Settings Action Name Edit Del Edit Del Edit Del Edit Del	SAML Version 2.0 2.0 2.0 2.0 2.0	New) New from Metadata File New from Metadata URL		Entity ID		
SAML Single Sign-On Settings Action Name Edit (Del Edit (Del Edit (Del Edit (Del Edit (Del Edit (Del Edit (Del Edit (Del Edit (Del	SAML Version 2.0 2.0 2.0 2.0 2.0 2.0 2.0	New New from Metadata File New from Metadata URL Issuer http://adfs		Entry ID		

4. Click **Edit** in the configuration page.

SAML Single Sign-On Settin Back to Single Sign-On Settings	ngs	Printable View Help for this Page 🥹
	Edit Delete Clone Download Metadata SAML Assertion Validator	
Name	adfs APi Name adfs	
SAML Version	2.0	
Issuer	http://adfscom/adfs/services/trust Entity ID https:// ny.salesforce.com	
Identity Provider Certificate	CN=ADFS Signing - addit mimext.com Expiration.4 Co2020 04:50:37 GMT	
Request Signing Certificate	SelfSignedCert_24Sep2019_230626	
Request Signature Method	RSA-SHA256	
Assertion Decryption Certificate	Assertion not encrypted	
SAML Identity Type	Username	
SAML Identity Location	Subject	
Service Provider Initiated Request Binding	HTTP POST	
Identity Provider Login URL	https://adfs com/adfs/ls/	
Custom Logout URL		
Custom Error URL		
Single Logout Enabled		
Identity Provider Single Logout URL	https://adfs com/adfs/is/	
Single Logout Request Binding	HTTP Redirect	
Just-in-time User Provisioning		
User Provisioning Enabled		
Endpoints		
View SAML endpoints for your organization, communit	ies, or custom domains.	
Your Organization		
Login URL	https:// my.salesforce.com?so=00D0b000000MGs	
Logout URL	https:// my.salesforce.com/services/auth/sp/sam12/logout	
OAuth 2.0 Token Endpoint	https:// my.salesforce.com/services/oauth21token?so=00D0b000000MGs	
	Editi Delete Clone Download Metadata SAML Assertion Validator	

a. Open the "Access IDP Metadata" in a viewer that is available in MobileIron Access after creating a federated pair.



b. Copy "X.509Certificate" value.

c. Open the certificate format site and paste the "X.509 cert" in the text area: <u>https://www.samltool.com/format_x509cert.php</u>

d. Click "Format X.509 Certificate".

onelogin SAML DEVELOP	ER TOOLS	ONLINE TOOLS	DOCUMENTATION	PLUGINS	TOOLKITS	GET ONELOGIN
X.509 CERTS	Format a	X.509 cer	tificate			
Obtain Self-Signed Certs	Sometimes we co this tool we can g SAML Toolkits.	py and paste the X. let certificates form	509 certificates from do ated in different ways, w	cuments and t hich will be re	flies, and the for ady to be used i	mat is lost. With n the OneLogin
Format X.509 Certificate		MEEDOS				
Format Private Key	CEDAR POR	TTTLED B				
CODE/DECODE	X.509 cert					0
ENCRYPT / DECRYPT	PASTE HERE	- 10				
III SIGN						
VALIDATE						
ATTRIBUTE EXTRACTOR						
XML PRETTY PRINT					-	
BUILD METADATA					FORMAT	LSOS CERTIFICATE
EXAMPLES	X.509 cert with h	eader				0
💢 EXTERNAL SAML TOOLS						

- e. Copy the value in "X.509 cert with header" text area after formatting.
- f. Open a text editor and paste the value in a new text file.
- g. Save the file as "access-idp-certificate.crt".

onelogin SAML DEVELO	PERTOOLS ONLINE TOOLS DOCUMENTATION PLUGINS TOOLKITS	ELOGIN
👷 X.509 CERTS		
Obtain Self-Signed Certs	Format a X.509 certificate	
Calculate Fargerprint	Sometimes we copy and paste the X.509 certificates from documents and files, and the format is lost,	With
Format X.508 Certificate	SAML Toolkits.	ogin
Format Private Key	CLEAR FORM FIELDS	
CODE/DECODE		
ENCRYPT / DECRYPT	X.509 cert	0
📑 SIGN	MILDIJCLAOSQAVIIBAQILAVZI KQVANAUGCSQGSIDSDDEBLWUAMIGHMCBWCOTUVUGUEWUV MBEG ATUECAWKQ2FsaWZvcm5pYTEWMBQGATUEBwwNU2FuIEZyYW5jaXNjb2ENMAsGATUECgwl YTFLU	ET2t0
VALIDATE	MBIGA1UECwwLUINPUHJvdmikZXixEDAOBgNVBAMMB3Rob2xvbnMxHDAaBgkqhkiG9w0BC Wiu 2000 Ab200YEEIb 2004bb abidZwybbabwUZ7WBkobbb abidizwbbabwUZ7WbieEW/2015E1 MAk52 Ab	QEWD
ATTRIBUTE EXTRACTOR	C VVMxEzARBgNVBAgMCkNhbGimb3JuaWExFjAUBgNVBAcMDVNhbiBGcmFuY2lzY28xDTALE	IgNVB
XML PRETTY PRINT	AoM BE94GExFDASBgNVBAsMCINTTIByb3ZpZGVyMRAwDgYDVQQDDAd0aG9sb25zMRwwGgY. vcN	JKoZlh
BUILD METADATA		
EXAMPLES	Paint S	CATE
	X.509 cert with header	10
ETTENNEL SAML TOOLS	BEGIN CERTIFICATE MIDIO[CC:05ag4wiBag1dx2VTkq3AMA0GC5qGSIb3DQEBCwUAMIGPMGswCQYDVQQG EwJVU2ETMBEGA1UECAwKQ2FEaW2×cm5pYTEWMBGAGAUEBwwNU2EUIE2yYW5jaXNj bzENMA5AG1UECgwET20YTEUMBIGAUECewuLUNPUHJvJmitZXLtCADBgNVBAMM B3Rob2vbmHzhDaBgdrahiG9w0BCQEWDWU2m9Ab2t0Y55b20wHhchHTcwHzhW mTNINjMwHchNI(wcHXHWHTINI5WCJE)ELEAAKGAUEBMCV/WtcZARBgNVBAAM CKhhbGimb3LauWErFJAUBgNVBACMDVNIbiBGcmFu72itY28b2TALBgNVBAAMBE9r dGE+rDa5BgNVBAAMTTINI5W2CyWHRAWD2DYU20D2DAdGa0525xHR8wvGgYI Ko2TihvcAAGkFg1abm2vGG9dGEuY29HIMBIANBgknhiG9w0BAQEFAADCAABA MIBGQKCADEAgda55b1WHT10345TCU20U20HAB9kG9DV02DDAB4C65575T87m3d HIBGgTW07bUXDJHyuV9cOD2XGSJRIHqg15amWCV7TDX5x49BiSMY/FhwkFASGfy L0567b2020H201JHyuV9cD02XGSJRIHqg15amWCV7TDX5x49BiSMY/FhwkFASGfy L0567b2020H201JHg1V202DD2101b2020H201HBISM57H7m3cb2HI	

5. In Salesforce, on Edit SAML Sign on Settings page, do the following:

a. Copy "**entityId**" attribute value from "EntityDescriptor" Element from "**access-idp-metadata.xml**" and paste in the "issuer" text box.

b. Copy "**Location**" attribute value from "**SingleSignOnService**" Element from "access-idp-metadata.xml" and paste in the "Identity Provider Login URL" text box.

c. Copy "Location" attribute value from "SingleLogoutService" Element from "access-idp-metadata.xml" and paste in "Identity Provider Single Logout URL" text box.

d. Click on "Browse" in the "Identity Provider Certificate" to open a file upload

dialog. Upload "access-idp-certificate.crt" formatted in above step. e. Click **Save**.



Updating IDP Configuration in Salesforce can be error prone if copy/paste is required.

Alternative is to create another entry in Salesforce 'Single-Sign-on Settings' 'by uploading the proxy-metadata file from Access and using the new entry in Domain Management in My Domain.

Procedure

- 1. Click Administer > Domain Management > My domain.
- 2. Edit Authentication configuration.
- 3. Enable the authentication service.
- 4. Click save.

This enables the service with Salesforce domain.