1. SSO - Admin Guide	2
1.1 Setting up Global SSO	2
1.1.1 Configuring IDP	2
1.1.1.1 ADFS configuration	2
1.1.1.1.1 Configuring ADFS for SSO	2
1.1.1.1.2 ADFS - Preparing certificate for SAML SSO Client	15
1.1.1.1.3 ADFS - configuring SAML sign-out	17
1.1.2 Step 1: Performing prerequisites check	19
1.1.3 Step 2: Preparing and configuring SAML SSO Client	19
1.1.4 Step 3: Installing and configuring Atlassian SSO add-ons	20
1.1.4.1 Configuring JIRA SSO add-on	21
1.1.4.2 Configuring Confluence SSO add-on	23
1.1.4.3 Configuring Bamboo SSO add-on	25
1.1.4.4 Configuring Bitbucket SSO add-on	27
1.1.4.5 Configuring FishEye SSO add-on	27

# SSO - Admin Guide

The content is intended for IDP Admins, Atlassian System Admins, thus we are assuming that the audience has sufficient and relevant technical knowledge.

The following pages describe how to prepare IDP, set up and configure Global SSO:

- Setting up Global SSO
  - Configuring IDP
    - ADFS configuration
  - Step 1: Performing prerequisites check
  - Step 2: Preparing and configuring SAML SSO Client
  - Step 3: Installing and configuring Atlassian SSO add-ons
    - Configuring JIRA SSO add-on
    - Configuring Confluence SSO add-on
    - Configuring Bamboo SSO add-on
    - Configuring Bitbucket SSO add-on
    - Configuring FishEye SSO add-on
- Upgrading Atlassian tools that have Global SSO

## Setting up Global SSO

To set up cPrime's Global SSO, perform the following operations:

- 1. Configure IDP
- 2. Step 1: Perform prerequisites check
- 3. Step 2: Prepare and configure SAML SSO Client
- 4. Step 3: Install and enable the Atlassian authenticators

## **Configuring IDP**

Depending on how your IDP is set up, the IDP Admin should work on one of the following IDP configurations in order to work with cPrime Global SSO:

- ADFS configuration
- OneLogin configuration
- Centrify configuration

We will use ADFS as an example to explain how to configure ADFS to work with Global SSO.

#### **ADFS configuration**

If you have ADFS IDP, here is additional information for ADFS configuration:

- 1. Configuring ADFS for SSO
- 2. ADFS Preparing certificate for SAML SSO Client
- 3. ADFS configuring SAML sign-out

After you are done with ADFS configuration, proceed with Step 1 for SSO setup - prerequisites check.

#### **Configuring ADFS for SSO**

On Your AD FS Server, perform the following operations:

- 1. Open the AD FS Management console.
- 2. In the Actions pane, click Add Relying Party Trust.
- 3. On the wizard introduction page, click Start.

<b>*</b>			10.00		
			AD FS		
File Action View Window Help					<u> </u>
AD FS Constraints of the service o	AD FS Over AD FS Lear C C C	Velcome Steps • Velcome • Select Data Source • Configue Multifactor Authentication Now? • Choose Issuance Authorization Rules • Ready to Add Trust • Finish	Add Relying Party Trust Wizard  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 authertication and authorization decisions. The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and user claims to b. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.	Ċ	Actions AD FS 1 Add Relying Party Trust ; Add Claims Provider Trust Add Claims Provider Trust Edit Federation Service Properties Edit Published Claims Revoke All Proxies View New Window from Here Refresh Help Help
			< Previous Start Cancel		

4. Select Enter data about the relying party manually and click Next.

<b>\$</b>	Add Relying Party Trust Wizard
Select Data Source	
Steps  Welcome  Select Data Source  Specify Display Name  Choose Profile  Configure Certificate  Configure URL  Configure Identifiers  Configure Multi-factor 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:          Import data about the relying party published online or on a local network         Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.         Federation metadata address (host name or URL):         Example: fs.contoso.com or https://www.contoso.com/app         Import data about the relying party from a file         Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.         Federation metadata file location:         Browse         Import data about the relying party manually         Use this option to manually input the necessary data about this relying party organization.
	< Previous Next > Cancel

5. Fill in the **Display name** field and click **Next**.

<b>\$</b>	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	test.adfs.com	
Specify Display Name	Notes:	
Choose Profile	test.adfs.com	~
Configure Certificate		
Configure URL		
<ul> <li>Configure Identifiers</li> </ul>		
<ul> <li>Configure Multi-factor Authentication Now?</li> </ul>		~
<ul> <li>Choose Issuance Authorization Rules</li> </ul>		
Ready to Add Trust		
• Finish		
	< Previous Next > Cancel	

6. Select the AD FS profile option and click Next.

<b>\$</b>	Add Relying Party Trust Wizard
Choose Profile	
Steps Welcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure Identifiers Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate configuration profile for this relying party trust. <ul> <li>AD FS profile</li> <li>This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol.</li> </ul> <ul> <li>AD FS 1.0 and 1.1 profile</li> <li>This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.</li> </ul> <ul> <li>AD FS 1.0 and 1.1 profile</li> <li>This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.</li> </ul>
	< Previous Next > Cancel

7. You will not need a token encryption certificate, so click Next to continue.

<b>\$</b>	Add Relying Party Trust Wizard	x
Configure Certificate		
<ul> <li>Configure Certificate</li> <li>Steps <ul> <li>Welcome</li> <li>Select Data Source</li> <li>Specify Display Name</li> <li>Choose Profile</li> <li>Configure Certificate</li> <li>Configure URL</li> <li>Configure Identifiers</li> <li>Configure Multi-factor Authentication Now?</li> <li>Choose Issuance Authorization Rules</li> <li>Ready to Add Trust</li> <li>Finish</li> </ul> </li> </ul>	Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to it. To specify the certificate, click Browse          Issuer:       Subject:         Effective date:       Expiration date:         View       Browse         Remove       Effective date:	
	< Previous Next > Cance	:

8. Select Enable support for the SAML 2.0 WebSSO protocol, paste the URL of your SAML Consumer service, and click Next. Example: https://test.adfs.com/SAMLssoclient/SAMLConsumer.

<b>\$</b>	Add Relying Party Trust Wizard
Configure URL	
<ul> <li>Steps</li> <li>Welcome</li> <li>Select Data Source</li> <li>Specify Display Name</li> <li>Choose Profile</li> <li>Configure Certificate</li> <li>Configure URL</li> <li>Configure Identifiers</li> <li>Configure Multi-factor Authentication Now?</li> <li>Choose Issuance Authorization Rules</li> <li>Ready to Add Trust</li> <li>Finish</li> </ul>	AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSD protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Federation Passive protocol The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol URL Relying party WS-Federation Passive protocol URL: Example: https://fs.contoso.com/adfs/ls/ I Enable support for the SAML 2.0 WebSSD protocol The SAML 2.0 single-sign-on (SSD) service URL supports Web-browser-based claims providers using the SAML 2.0 Single-sign-on (SSD) service URL supports Web-browser-based claims providers using the SAML 2.0 SAML 2.0 SSD service URL supports Web-browser-based claims providers using the Example: https://test.adfs.com/SAMLsoclient/SAMLConsume] Example: https://test.adfs.com/SAMLsoclient/SAMLConsume] Example: https://www.contoso.com/adfs/ls/
	< Previous Next > Cancel

9. In the **Relying party trust identifiers** field, enter the same URL (example: *https://test.adfs.com/SAMLssoclient/SAMLConsumer*).

Ensure that you include https:// here, and that you omit a slash at the end of the URL. Otherwise the integration will not work.

<b>\$</b> #	Add Relying Party Trust Wizard
Configure Identifiers	
Steps	Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying
Welcome	party trust.
Select Data Source	Relying party trust identifier:
Specify Display Name	Add
Choose Profile	Example: https://fs.contoso.com/adfs/services/trust
Configure Certificate	Relying party trust identifiers:
Configure URL	https://test.adfs.com/SAMLssoclient/SAMLConsumer Remove
Configure Identifiers	
<ul> <li>Configure Multi-factor Authentication Now?</li> </ul>	
<ul> <li>Choose Issuance Authorization Rules</li> </ul>	
Ready to Add Trust	
😑 Finish	
	ל ל <u>י</u>
	< Previous Next > Cancel

10. Select your desired multi-factor authentication option for users and click Next.

A Enabling multi-factor authentication requires additional steps that are outside the scope of this guide.

Add Relying Party Trust Wizard			
Steps Welcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure Identifiers Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	Add Relying Party Trust Wizard         Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required there is a match for any of the specified requirements.         Multi-factor Authentication       Global Settings         Requirements       Users/Groups       Not configured         Device       Not configured       Location         Location       Not configured         I do not want to configure multi-factor authentication settings for this relying party trust at this time.       Configure multi-factor authentication settings for this relying party trust at this time.         Configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see Configuring Authentication Policies.		

11. Select Permit all users to access this relying party and click Next.



12. Review your settings and click Next.

Ready to Add Trust
Stens
• Welcome         • Welcome         • Select Data Source         • Specify Display Name         • Choose Profile         • Configure Cetificate         • Configure Identifiers         • Configure Identifiers         • Configure Multi-factor Authentication Now?         • Choose Issuance Authentication Rules         • Finish

13. To exit the wizard, click Close.

<b>\$</b>	Add Relying Party Trust Wizard	x
Finish		
Steps	The reliving party trust was successfully added to the AD FS configuration database.	
Welcome	You can modify this relying party trust by using the Properties dialog box in the AD FS Management span	n-in
🥃 Select Data Source		
🥥 Specify Display Name		
Choose Profile	Open the Edit Claim Rules dialog for this relying party trust when the wizard closes	
Configure Certificate	i !i	
Configure URL		
Configure Identifiers		
Configure Multi-factor Authentication Now?		
<ul> <li>Choose Issuance Authorization Rules</li> </ul>		
🥥 Ready to Add Trust		
🥃 Finish		
	Close	е

14. In the Issuance Transform Rules tab of the dialog, click Add Rule.

Edit Claim Rules for test.adfs.com	_ 🗆 X			
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 Car	ncel Apply			

15. Configure the Send LDAP Attributes as Claims rule and click Next.

	Edit R	ul	e - Username	x
You car which to issued fi	n configure this rule to send the values of extract LDAP attributes. Specify how th rom the rule.	f L[ ne a	DAP attributes as claims. Select an attribute store from attributes will map to the outgoing claim types that will b	е
Claim ru	le name:			
NamelD		_		
Rule ter	nplate: Send LDAP Attributes as Claims			
Attribute	store:			
Active [	Directory		~	
Mapping	g of LDAP attributes to outgoing claim typ	bes	: :	
	LDAP Attribute (Select or type to add more)		Outgoing Claim Type (Select or type to add more)	
	Employee-ID	~	Name ID	~
<b>▶</b> ₩		~		~
		_		
View F	Rule Language		OK Cancel	

16. In this case we will send the "Email" attribute to our consumer, so click Add Rule again, select "Send Claims Using a Custom Rule", and put in the following rule:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccou
ntname"]
=> issue(Type = "Email", Value = c.Value);
```



After these steps, proceed with configuring SAML sign-out.

**ADFS - Preparing certificate for SAML SSO Client** 

To prepare the certificate for SAML SSO Client, perform the following operations:

- 1. Export the Token Signing Certificate
- 2. Convert this certificate for our SAML SSO Client

Exporting the Token Signing Certificate

The Token Signing Certificate can be exported from the ADFS 2.0 Management, Services snap-in.

To export the Token Signing Certificate:

- 1. Go to ADFS Management.
- 2. Click Services to open the Service Snap-in.
- 3. In the Services Snap-in, click Certificates.
- 4. In Token-signing of the Certificates pane, select the Certificate and open it.
- 5. In the Details tab of the Certificate window, click Copy to File.
- 6. Click Next.

<b>Q</b> ii	AD FS	_ 0 X
🐐 File Action View Window Help		_ # ×
AD FS Certificat	Action Action	lons
AD FS Findmaints Certificate Claim Descriptions Claim Descriptions Claims Provider Truts Relying Party Truts A Authentication Policies Per Relying Party Trust Per Relying Party Trust	tes       Action         Issuer       Effective Date       Expiration Date       Status       Primary       Certificate         communications       Certificate       X       Certificate       Certif	ons tificates
	ОК	Next Cancel

7. Select Base-64 encoded X.509 (.CER), click Next, and save it.

📀 🍠 Certificate Export Wizard	×
<b>Export File Format</b> Certificates can be exported in a variety of file formats.	
Select the format you want to use:	
O DER encoded binary X.509 (.CER)	
Base-64 encoded X.509 (.CER)	
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
Include all certificates in the certification path if possible	
Personal Information Exchange - PKCS #12 (.PFX)	
Include all certificates in the certification path if possible	
Delete the private key if the export is successful	
Export all extended properties	
<ul> <li>Microsoft Serialized Certificate Store (.SST)</li> </ul>	
Next Cance	el

Converting the certificate for our SAML SSO Client

After these steps, convert this certificate for our SAML SSO Client. There are two ways to implement it:

openssl enc -base64 -A -in Example.cer -out finalBase64.ser	1.	Executing Linux command for converting					
		openssl enc -base64 -A -in Example.cer -out finalBase64.ser					

#### 2. Using a link

Use the following link for converting: http://www.mobilefish.com/services/base64/base64.php.

← → C 🗋 www.mobile	etish.com/services/base64/	base64.php
VCard generator	its character code of vice	versa.
European clothing standard	XML RSS FEED	
EN 13402 pictogram		
generator	Input base64 encoder and de	ecoder:
Favicon generator		
File checksum calculator		
Find the BIC numbers for		
Dutch IBAN numbers		
Free game sound effects		
Free game textures	Enter source data *:	
Free online practice exams		
Free online SEPA XML		
valdation		
Generate Dutch bank		
account numbers and		
numbers	Upload source file *:	
	Max 100 KB.	Выберите фаил base64.cer
button code generator	Conversion method *:	Encode to Base64 string
Coogle mana (ADL-O) and	Select output *:	Output to file
generator	Max characters per line *:	999 Allowed values 0 - 999. Use 0 for unlimited characters.
Google map distance	To prevent automated	
calculator	submissions an Access Code has been implemented for this	Y×N
Hide email address	tool.	
	Please enter the Access Code	YxN
HTML escape and	as displayed above".	
	* = required	Convert Clear
Hieroglyphs generator		
IBAN checker		

ADFS - configuring SAML sign-out

Inside your SaaS SSO configuration, define a sign-out URL. Example: https://test-adfs.com/adfs/ls/?wa=wsignout1.0.

- 1. On the ADFS side, go to **RP trust** for your app.
- 2. Configure a SAML logout endpoint.

Example:

🖗	AD FS
翰 File Action View Window Help	
adfsdev.com Properties	
Al Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints Proxy Endpoints Notes Advanced Specify the endpoints to use for SAML and WS-FederationPassive protocols.	Enabled Type Identifier No WS-T urn:ms-drs:adfsdev.com
URL         Index         Binding         Default         R∈           SAML Assertion Consumer Endpoints	Yes WS-T https://adfsdev.com/ADFSConsumer
A Contract of the second and the sec	Endpoint type: SAML Logout
Add SAML       Add WS-Federation       Remove       Edit       OK     Cancel	Binding: Redirect   Set the trusted URL as default  Index:   Trusted URL:  https://adfsdev.com/adfs/ls/?wa=wsignout1.0  Example: https://sts.contoso.com/adfs/ls  Response URL:  Example: https://sts.contoso.com/logout  OK Cancel

When configured, a proper logout will look like this:

	🕒 Sign out 🛛 🔪 🚺
← → C 🛛 🚱 https://adfsdev.com/adfs/ls/?v	va=wsignout1.0&SAMLRequest=IZJPb6QgGMa%2fivHOc 🛠 🖪 🔳
	>>
	adfsdev.com Sign out You have successfully signed out.
	© 2013 Microsoft

After you are done with ADFS configuration, proceed with step 1 for SSO setup.

## Step 1: Performing prerequisites check

#### Prerequisites before setting up Global SSO

- 1. For Global SSO, the Atlassian products must be accessible via HTTPS only.
- 2. SSO should only accept HTTPS SAML URL's.
- 3. IDP should support SAML 2.0 Assertions.
- 4. Global SSO works on the server implementations only.
- 5. We will need to have a signing certificate from IDP and will need to convert it to a Base64 encrypted string in preparation for our SAML SSO Client configuration.

After you are done with the prerequisites, proceed with SAML SSO Client configuration.

## Step 2: Preparing and configuring SAML SSO Client

To prepare and configure SAML SSO Client, perform the following operations:

- 1. Generate a public/private key pair
- 2. Convert the certificate from IDP to base64 string
- 3. Configure SAML SSO Client
- 4. Configure logout for the Atlassian applications

#### 1. Generating a public/private key pair

To generate a public/private key pair, execute the following commands in the Linux console:

- 1. openssl genrsa -out mykey.pem 2048
- 2. openssl pkcs8 -topk8 -inform PEM -outform PEM -in mykey.pem -out private\_key.pem -nocrypt
- 3. openssl rsa -in mykey.pem -pubout -outform DER -out public\_key.der

#### 2. Converting the certificate from IDP to base64 string

WARNING! In openssl, the base64 line length is limited to 76 characters by default. To be able to decode a base64 line without a line feed that exceeds the 76 characters, use -A option:

openssl enc -base64 -A -in Example.cer -out finalBase64.ser and put this certificate in the ../SAMLssoclient/WEB-INF/classes/ directory

#### 3. Configuring SAML SSO Client

- 1. Deploy the SAMLssoclient.war directly to a new Tomcat instance or to any Atlassian application.
- 2. Configure IDP.
- 3. Configure SAML SSO Client by using one of the following options:
  - a. Using SAML SSO Client Admin page: https://yourdomain.com/SAMLssoclient/SsoUpdate
  - b. Manually, by using a config file on your server: ../SAMLssoclient/WEB-INF/classes/config.properties

#### config.properties

unauthorizedPage=403.html EncryptionPrivateKey=..\path\_to\_your\private\_key.pem assertionConsumerServiceUrl=http\://domain.com/SAMLConsumer/SAML Consumer errorPage=error.html idpServerUrl=https\://domain.com/idpinitiatedsignon NameAttribute=Email certificate=converted\_certificate.ser cookiePath=/ loggingLevel=DEBUG cookieDomain=domain.com

#### Where:

Name (admin page)	Attribute(config.properties)	Description
_	unauthorizedPage	User failed validation page for redirecting
Private key	EncryptionPrivateKey	Full path to our private key for encryption
Assertion Consumer Service URL	assertionConsumerServiceUrl	Link to our SAML SSO Client page
Name Attribute	NameAttribute	Attribute name which we use for username encoding and then put to an SSO cookie
Certificate	certificate	Put your converted certificate to a folder, for example "\Tomcat 8.0\webapps\SAMLssoclient\WEB-INF\classes\", and enter the name of this certificate here.
—	errorPage	SAML error page for redirecting.
_	cookiePath	URL path for saving the SSO cookie
Log Level	loggingLevel	The logging level can be DEBUG, INFO, or ERROR
Cookie Domain	cookieDomain	Your server's domain
IDP Server URL	idpServerUrl	Link to your IDP
Issuer Application URL	issuerUrl	Issuer Application URL
Default target service	default.target.service	Default target service

#### 4. Configuring logout for the Atlassian applications

As a result, you can have one logout for all Atlassian applications:

To implement logout, set the cookiePath property ( ../SAMLssoclient/WEB-INF/classes/config.properties file): cookiePath=/



Note that the same value for path property should be set in all SSO authenticators.

Step 3: Installing and configuring Atlassian SSO add-ons

This step describes how to configure and enable the following Atlassian SSO add-ons:

- JIRA
- Confluence
- Bitbucket
- Bamboo
- FishEye

#### Configuring JIRA SSO add-on

This article describes how to configure SSO authenticator for JIRA.

WARNING! If you entered wrong parameters, use a "back door" functionality in order to avoid cyclic redirects and to access application bypass SSO.

Just add a GET parameter sso=off to the needed URL. Example: https://some.jira.com/?sso=off.

To configure SSO for JIRA:

1. Install JIRA SSO add-on.

Authentication-Redirect-Filters TRIAL EXPIRING Buy now								
This is the com.cprime.labs.jira:Authentication-Redirect-Filters plugin for Atlassian Jira.								
Your trial is expiring on 08/Jun/16. Buy a license for this add-on.								
Buy now Uninstall Disable								
No screenshots available	Version:	1.0.0-SNAPSHOT	14 of 14 modules enabled     14					
	Vendor:	cPrime						
	Add-on key:	com.cprime.labs.jira.Authentic ation-Redirect-Filters						
	License details:	Evaluation, Unlimited-user testing license, Standard, expires 08/Jun/16						
	License status:	Valid						
	License SEN:	Unknown						
	License key:	AAACLg0ODA 🖋						
› 🎄 Entity property conditions								
Filter Deletion Warning Plugin								
› 🎝 HipChat for JIRA		UPDATE	AVAILABLE	Update				
› 🎄 JIRA Feature Keys								
> 🎄 Soy Function Plugin								
› 💠 Support Tools Plugin		UPDATE	AVAILABLE	Update				
Audit log   JIRA update check   Settings   Enter safe mode								

- 2. Go to Administration > Add-Ons.
- 3. In the **FILTERS** section, click **Global SSO**.
- The Global SSO Configuration page opens.
- 4. Fill in the fields on this page. The field description is provided in the table below.

≡ <b>ŸJIRA</b> Dashboards •	Projects - Issues -	Agile	Structure -	Program	eazyBl	Create	Search	٩	@ -	۰.	
Administration ۹	Search JIRA admin										¢
APPLICATION LINKS	Global SSO	Confi	iguratior	ı							
BEHAVIOUR S Behaviours	Login URL:	* https://	//aag0677.my gin URL.	y.centrify.com	n/applogin/a	ppKey/8980f085	j-4d24-48a7-a701-bb13c4€	e90b0f/customeri	d/AAG06	77	
BUILDS Bamboo configuration	Logout URL:	* https://	//aag0677.my gout URL.	y.centrify.com	n/applogout						
JIRA AGILE LexoRank management	Cookie Domain:	* .cprim SAMLss	ne.com soclient Cookie	Domain.							
ISSUE COLLECTORS	Time Expiry:	* 14400 Live of \$	) SSO Token for a	authentication	in seconds. D	efault value is 1440	IO(4 hours).				
JIRA.AGNICIENT.COM mdsf.license.label	Path: Exclude paths:	/ Applica	tion Path. nks:/auth:/res	t:/oauth:/rpc	:/xml:L						
MONITORING Database Monitoring		inkCo nkJira	nfluencePage Issue;AjaxIss	e;ManageRa sueEditAction	nting;Li						
ADMIN HELPER		Exclude	Paths or part o	of URLs for filte	r(semicolon s	eparated values)). I	Example: /rest/usermanagemen	nt;/rest/api etc.			
Permission Helper Notification Helper	Public Key:	/var/a Please	tlassian/appli enter the full pa	th to your publ	lic key file on	ey.der server.					
FILTERS Global SSO	Exclude IP addresses:	107.1	70.234.49;12	7.0.0.1	) Jon separate	t values))					
Home Directory Browser Db Console		Save	Test SS	<b>O</b>	aopaidte	a vandoojj.					

## Field description for the Global SSO Configuration page

Attribute	Description
Login URL	IDP Login Page Examples: <ul> <li>https://adfs-test.com/adfs/ls/idpinitiatedsignon</li> <li>https://aa00677.mv.centrify.com/applogin/appKey/8980f085-4d24-48a7-a701-bb13c4e90b0f/customerId/AAG0677</li> </ul>
Logout URL	IDP Logout Page Examples: • https://aag0677.my.centrify.com/applogout • https://adfs-test.com/adfs/ls/?wa=wsignout1.0
Cookie Domain	Domain of your applications for SSO cookie
Path	Your application path. If you need to have one logout from all applications, enter "/" for this field.
Exclude paths	You can disable SSO from URLs which contain custom pieces of URL (semicolon separated values). Example: <b>/rest/usermanagement;/rest/api</b> Another case is to open REST API for using.
Public Key	Full path to your public key file for decrypting the SSO username
Exclude IP addresses	To support deep linking between applications, specify a list of application's IP addresses for linking
Time Expiry	Life length of SSO Token (cookie) for authentication in seconds. Default value is 14400 (4 hours).

You can test your SSO cookie by using the  $\ensuremath{\text{Test}}\xspace$  button:

	Exclude IP addresses for filter(semicolon separated values)).           Save         Test SSO
0	Info! SSO login is - telcorp-admin   Cookie will expire in 232(minutes).

#### Configuring Confluence SSO add-on

This article describes how to configure SSO authenticator for Confluence.

WARNING! If you entered wrong parameters, use a "back door" functionality in order to avoid cyclic redirects and to access application bypass SSO.

Just add a GET parameter sso=off to the needed URL. Example: https://some.confluence.com/?sso=off.

#### To configure SSO for Confluence:

1. Install Confluence SSO add-on.

A CUITTUETICE Opaces - Fe	eople Create •••		
Confluence administration			
CONFIGURATION General Configuration Further Configuration Backup Administration Manage Referrers Languages Shortcut Links External Gadgets	Image add-ons         Image add-ons         Image add-ons         Image add-ons         Image add-ons         Image add-ons	e. To avoid problems when loading this page, you can	disable the connection to the Marketplace
Global Templates and Blueprints Import Templates Recommended Updates Email Mail Servers User Macros In-app Notifications HipChat Integration	User-installed add-ons  Authentication-Redirect-Filters  This is the com.cprime.labs.confluence:Authentication-f Try Authentication-Redirect-Filters free for 30 days  Free trial Buy now Uninstall Disable	Redirect-Filters plugin for Atlassian Confluence.	Free trial
Attachment Storage Spam Prevention PDF Export Language Support Configure Code Macro Office Connector Global SSO WebDAV Configuration ATLASSIAN MARKETPLACE Find new add-ons Manage add-ons USERS & SECURITY	No screenshots available	Version: 1.0.0-SNAPSHOT Vendor: cPrime Add-on key: com.cprime.labs.confluence.Au thentication-Redirect-Filters License details: Unlicensed License key: Update	E 13 of 13 modules enabled

- 2. Go to Administration > Add-Ons.
- 3. In the CONFIGURATION section, click Global SSO. The Configuration page for SSO opens.
- 4. Fill in the fields on this page. The field description is provided in the table below.



#### Field description for the Global SSO Configuration page

Attribute	Description
Login URL	IDP Login Page Examples: • https://adfs-test.com/adfs/ls/idpinitiatedsignon • https://aag0677.my.centrify.com/applogin/appKey/8980f085-4d24-48a7-a701-bb13c4e90b0f/customerId/AAG0677
Logout URL	IDP Logout Page Examples: • https://aag0677.my.centrify.com/applogout • https://adfs-test.com/adfs/ls/?wa=wsignout1.0
Cookie Domain	Domain of your applications for SSO cookie
Path	Your application path. If you need to have one logout from all applications, enter "/" for this field.
Exclude paths	You can disable SSO from URLs which contain custom pieces of URL (semicolon separated values). Example: <b>/rest/usermanagement;/rest/api</b> Another case is to open REST API for using.
Public Key	Full path to your public key file for decrypting the SSO username
Exclude IP addresses	To support deep linking between applications, specify a list of application's IP addresses for linking
Time Expiry	Live of SSO Token for authentication in seconds. Default value is 14400(4 hours).

You can test your SSO cookie by using the Test SSO button.

### **Configuring Bamboo SSO add-on**

This article describes how to configure SSO authenticator for Bamboo.

WARNING! before installing this add-on, check whether you can receive the SSO cookie.

#### To configure SSO for Bamboo:

1. Install Bamboo SSO add-on.

<ul> <li>点 Authentication-Redirect-Filters</li> </ul>		TRIAL E	XPIRING	Buy now
This is the com.cprime.labs.jira:Authentication-Redirect-Filters plugin for Atlassian Jira.				
Your trial is expiring on 08/Jun/16. Buy a lic	ense for this add-on.			
Buy now Uninstall Disable				
No screenshots available	Version:	1.0.0-SNAPSHOT		
	Vendor:	cPrime		
	Add-on key:	com.cprime.labs.jira.Authentic ation-Redirect-Filters		
	License details:	Evaluation, Unlimited-user testing license, Standard, expires 08/Jun/16		
	License status:	Valid		
	License SEN:	Unknown		
	License key:	AAACLg00DA 🖋		
> 🎄 Entity property conditions				
> 🎄 Filter Deletion Warning Plugin				
> & HipChat for JIRA UPDATE AVAILABLE Update				
> 💠 JIRA Feature Keys				
> 🤹 Soy Function Plugin				
› 🎄 Support Tools Plugin		UPDATE	AVAILABLE	Update
Audit log   JIRA update check   Settings	Enter safe mode			

2. Go to Administration > Add-Ons.

3. Click Global SSO on the left panel.

Click Global SSC on the left parter.
 The Configurationpage for Global SSO opens.
 Fill in the fields on this page. The field description is provided in the table below.
 WARNING! Before you enter login / logout URL, test your SSO!

≡ <b>⊜Bamboo</b> <sup>My Bamb</sup>	oo Build - Deploy -	Reports - Create -	
Bamboo administration			
BUILD RESOURCES Agents	Configuration	n page for Glob	al SSO
Agent matrix Executables	Login URL:*	https://aag0677.my.cen	tı
JDKs Server capabilities Global variables	Logout URL:*	https://aag0677.my.cen SSO Logout URL.	tı
Linked repositories Shared credentials	Cookie Domain:*	.cprime.com SAMLssoclient Cookie Doma	in.
Repository settings	Path:*	/ Application Path.	
Configuration PLANS	Exclude paths:	servlet/applinks/auth;/p oauth Exclude Paths or part of URI	lugins/servlet/
Concurrent builds Quarantine settings	Public Key:*	/opt/atlassian/bamboo-	5. Jour public key file on server.
Bulk action Build monitoring	Exclude IP addresses:	107.170.234.49;127.0.1	0.1
Remove plans Move plans		Save Test SSO	n (sennoonori separateu Vallues)).
Bulk edit plan permissions SECURITY	(i) Info! SSO login	is - telcorp-admin	
Users			

You can test your SSO cookie by using the **Test SSO** button:

	Save Test SSO	
6	Info! SSO login is - username	

## Field description for the Global SSO Configuration page

Attribute	Description
Login URL	IDP Login Page Examples: • https://adfs-test.com/adfs/ls/idpinitiatedsignon • https://aag0677.my.centrify.com/applogin/appKey/8980f085-4d24-48a7-a701-bb13c4e90b0f/customerld/AAG0677
Logout URL	IDP Logout Page Examples: • https://aag0677.my.centrify.com/applogout • https://adfs-test.com/adfs/ls/?wa=wsignout1.0
Cookie Domain	Domain of your applications for SSO cookie

Path	Your application path. If you need to have one logout from all applications, enter "/" for this field.
Exclude paths	You can disable SSO from URLs which contain custom pieces of URL (semicolon separated values). Example: <b>/rest/usermanagement;/rest/api</b> Another case is to open REST API for using.
Public Key	Full path to your public key file for decrypting the SSO username
Exclude IP addresses	To support deep linking between applications, specify a list of application's IP addresses for linking

## Configuring Bitbucket SSO add-on

To configure Bitbucket SSO Authenticator, perform the following operations:

- 1. Intstall the Bitbucket SSO add-on.
- 2. Configure the **BITBUCKET\_WORK\_DIR/shared/bitbucket.properties** file. As a result, you will have a configuration like this:

#### bitbucket.properties

plugin.global-sso.login.url=https://aag0677.my.centrify.com/applogin/ appKey/6c7c624e-b80d-447d-8b0a-c9e9ef3lc73c/customerId/AAG0677 plugin.global-sso.logout.url=https://aag0677.my.centrify.com/applogout plugin.global-sso.public.key.file=/var/atlassian/application-data/bit bucket/public\_key.der plugin.global-sso.path=/ plugin.global-sso.domain=.cprime.com plugin.global-sso.expiry.time=14400

#### Where:

Property	Description
plugin.global-sso.login.url	IDP Login URL.
plugin.global-sso.logout.url	IDP Logout URL.
plugin.global-sso.public.key.file	Full path to the public key on the server(for decription the cookie).
plugin.global-sso.path	Cookie path.
plugin.global-sso.domain	Cookie domain.
plugin.global-sso.expiry.time	Live of SSO Cookie for authentication in seconds. Default value is 14400(4 hours).

3. Generate **public\_key.der** and specify a path to this key.

4. Restart Bitbucket instance.

5. Install the Bitbucket-SSO-Authenticator add-on.

#### Configuring FishEye SSO add-on

Content in development, please wait a bit.