MITRATECH

TeamConnect® SSO-SAML Add-In

© 2017 Mitratech

User Guide

TeamConnect® SSO-SAML User Guide

Document ID: tc_ss_user_1, published on 9/11/2017

Copyright © 2017, Mitratech Holdings, Inc. All rights reserved.

Disclaimer of Warranty

Mitratech Holdings, Inc. (Mitratech) makes no representations or warranties, either expressed or implied, by or with respect to anything in this document, and shall not be liable for any implied warranties of merchantability or fitness for a particular purpose or for any indirect, special or consequential damages.

Mitratech reserves the right to not support non-standard or non-default functionality and extended functionality available in third-party software, unless specifically documented as supported or certified in the Mitratech product documentation. For further information regarding third-party non-standard or non-default functionality, please contact Mitratech Support.

This document, along with the software that it describes, is furnished under license and may be used or copied only in accordance with the terms of such license. The content of this document is furnished for informational use only, is subject to change without notice, and should not be construed as commitment by Mitratech.

The following document is for the TeamConnect™ Enterprise 4.0 release only. Though every effort was made to ensure that the information in this document is correct and reliable, Mitratech does not assume any liability for any errors encountered in this document.

If you need support for TeamConnect™ Enterprise 4.0, please contact the Mitratech support team by sending an email to: support@mitratech.com. For more information about Mitratech, visit our web site: http://www.mitratech.com.

"Mitratech", TeamConnect™ Enterprise, TeamConnect™ Legal, TeamConnect™ Legal Matter Management, Collaborati®, TeamConnect™ Collaborati Spend Management®, TeamConnect™ Deadlines, TeamConnect™ AP Link, TeamConnect™ Office Suite, TeamConnect™ Legal Reports, and TeamConnect™ SOP Manager are trademarks and products of Mitratech Holdings, Inc. All other products or services mentioned in this book are the trademarks or service marks of their respective companies or organizations.

GOVERNMENT RIGHTS LEGEND:
Use, duplication or disclosure by the U.S. Government is subject to restrictions set forth in the applicable Mitratech license agreement and as provided in DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013 (Feb 2012)FAR 12.212(a) (1995), FAR 52.227-19 (Dec 2007), or FAR 52.227-14, as applicable.

CONTACT US:
Mitratech Holdings, Inc.
5001 Plaza on the Lake Suite 111, Austin, TX 78746
Phone: (512) 382-7322

NOTE: Throughout Mitratech product publications, in addition to using full product names where necessary, we also use familiar and shorter terms to increase your ease of reading. You may find the following aliases for our product names:

TeamConnect for TeamConnect Enterprise
Matter Management for TeamConnect Legal Matter Management
TeamConnect Legal for TeamConnect Legal Matter Management
CSM for TeamConnect Collaborati Spend Management
Collaborati Spend Management for TeamConnect Collaborati Spend Management
SOP or SOP Manager for TeamConnect SOP Manager
Legal Hold for TeamConnect Legal Hold
Legal Reports for TeamConnect Legal Reports
Deadlines for TeamConnect Deadlines
AP Link for TeamConnect AP Link
Office Suite for TeamConnect Office Suite

Acknowledgements

This product includes software developed by the following organizations:

Apache Software Foundation (http://www.apache.org/)

OpenSymphony Group (http://www.opensymphony.com/).

The license agreements for these and other supplemental software packages can be found in your installation media in subfolder Supplemental_Software_Licenses. That subfolder also contains Open Source Components.pdf, which lists the locations, license types, and specific versions of components that are available on the web.

Table of Contents

Part I SSO-SAML Help 5

1 Installation Requirements 5
2 Setup and Installation 6
3 Testing 8
4 Troubleshooting/Common Issues 8

Index 0

1 SSO-SAML Help

Welcome to the *TeamConnect® SSO-SAML User Help*.

This documentation is meant for people who need an overview of how to use TeamConnect SSO-SAML. It describes the product requirements and the installation and setup process.

The topics are organized by the major tasks that you must perform when setting up TeamConnect SSO-SAML.

Installation Requirements

Setup and Installation

Testing

Troubleshooting/Common Issues

1.1 Installation Requirements

INSTALLATION REQUIREMENTS

You must be running one of the following TeamConnect versions in order to install the TeamConnect SSO-SAML Add-In:

- TCE 3.3 SP3 U19 (or later 3.3 SP3 update)
- TCE 3.4 SP1 U17 (or later 3.4 SP1 update)
- TCE 4.0 U3 (or later 4.0 update)

Additionally, the user implementing the TeamConnect SSO-SAML add-in must be familiar with the following technologies:

- SAML concepts

- Custom Authentication Plug-Ins in TeamConnect
- Java KeyStore and Keytool
- Java Cryptography Extension (JCE)

1.2 Setup and Installation

SETUP AND INSTALLATION

Before You Begin

Contact your IDP Administrator to obtain the XML metadata for the IDP. ***Note:*** *If you use Siteminder for your IDP, you will not be able to specify the "type" of attribute. Use NameID instead for this case.*

The SAML Gateway requires a key pair to use for encryption and signing. Obtain the key pair from your administrator or use Java keytool to create a new one.

Installing the SAML gateway application

1. Replace the file named *idp.xml* in the *WEB-INF/classes/metadata* folder of the application with the metadata for your Identity Provider (IDP).

2. Import the encryption key pair into the provided keystore located at *WEB-INF/classes/security/samlKeystore.jceks*. You will need to provide the `-storetype jceks` option to Java keytool when importing. The default keystore password is teamconnect.

   Alternatively, you can replace the provided keystore with your own and update saml.properties (see below) accordingly.

3. Edit the *saml.properties* file in the *WEB-INF/classes* folder of the application.

Property	Description
idp.tcUsernameIdentifier	SAML response element that will contain the TeamConnect username. Supported values are *NameID* and *Attribute*. Contact your Identity Provider for this information.
idp.nameIDFormat	Required only when idp.tcUsernameIdentifier is *NameID* e.g. urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

idp.attributeName	The name of the response Attribute containing the TeamConnect username. Required only when idp.tcUsernameIdentifier is *Attribute*.Contact your Identity Provider for this information.
sp.entityID	Service Provider entity ID. This is the value used to generate service provider metadata in Step 6. If you are using an existing metadata file, enter the value of the *entityID* attribute from the metadata file.
gateway.admin.username	Defines the credentials to access the SAML gateway administration interface. Default is *admin*.
gateway.admin.password	Defines the credentials to access the SAML gateway administration interface. Default is *admin*.
gateway.supportIdpInitializedSSO	Indicates whether IDP-initialized SSO should be supported. Supported values are *true* and *false*.
teamconnect.loginUrl	The login URL for the TeamConnect application.
keystore.file	Name of the Java keystore file containing the private key for encrypting and optionally signing SAML messages. This file must be located in the *WEB-INF/classes/security* folder of the application. You may use the provided sample keystore (*samlKeystore.jceks*) or replace it with your own.
keystore.type	Type of the keystore. Supported values are *jceks* and *jks*.
keystore.password	Keystore password
keystore.privatekey.alias	Keystore alias for the private key. For security reasons, the default private key should not be used in production.
keystore.privatekey.password	Password for the private key

4. Deploy the SAML gateway application.
5. In a web browser, go to `<SAML gateway>/saml/web/metadata/generate`.
6. Log in using the credentials defined in step 3.
7. On the *Metadata generation* page, enter the Entity ID defined in step 3. The choices for Service Provider (SP) metadata generation depend on the environment and configuration, as agreed on by the IDP and SP admins.
8. Click the *Generate metadata* button. The *Metadata detail* page is displayed.
    a. Replace the contents of the file named *sp.xml* in the *WEB-INF/classes/metadata* folder of the application with the content of the *Metadata* field.
    b. Edit the *securityContext.xml* file in the *WEB-INF/classes* folder of the application and update the `ExtendedMetadata` of `<bean>` with `id="sp"` to include the property values from the *Configuration* field.
9. Restart the SAML gateway application.
10. Provide service provider metadata to your IDP administrator for upload to the IDP.

INSTALLING THE TEAMCONNECT CUSTOM AUTHENTICATION PLUGIN FOR SAML

1. Update the URLs in *badCredentials.html* and *logout.html* based on your SAML gateway deployment.

2. Create the following Document folder structures in your TeamConnect instance:
   a. System/Authentication/SAML/classes
   b. System/Authentication/SAML/pages

3. Upload the *authenticationDescriptor.properties*, *SAMLAuthenticator.class* and *Crypto.class* files to the *System/Authentication/SAML/classes* folder created in step 2.

4. Upload the *badCredentials.html*, *logout.html* and *sessionTimeout.html* files to the *System/Authentication/SAML/pages* folder created in step 2.

5. Restart the TeamConnect application and select *SAML Single Sign-On* as the *Default Authentication Method* under *Admin Settings -> Security.*

1.3 Testing

TESTING

1. Create a TeamConnect user configured to use default authentication (the default authentication was set to SAML SSO during installation of the SAML authentication plugin). This user must have a corresponding IDP account.

2. In a web browser, navigate to the TeamConnect login URL.

3. If the installation was successful, the browser will be redirected to the IDP for authentication and will eventually display the TeamConnect home page.

To log into TeamConnect without using SAML authentication, follow these steps:

1. Create a TeamConnect user configured to use *Standard Authenticator* as the authentication type.

2. Use `/standardLogin` for the login URL instead of `/login` and log in using the user created in Step 1.

1.4 Troubleshooting/Common Issues

TROUBLESHOOTING

LOGGING

Use the TeamConnect and SAML Gateway log files to troubleshoot issues.

TEAMCONNECT

Set the TeamConnect Authentication logger to DEBUG

SAML GATEWAY

Debug logging can be enabled on the *Logging* tab of the administrative console accessible via a web browser at `<SAML gateway>/saml/web/logging`

Note: *Use different browsers when accessing the SAML Gateway administration console and logging into TeamConnect via SAML at the same time.*

COMMON ISSUES

Issue	Resolution
When generating new metadata, the dropdowns for the 'Signing key' and 'Encryption key' fields are blank.	Verify that the keystore alias for the encryption key was created using lowercase letters and that the default keystore values in saml.properties have been changed to reflect the keystore being used.
TeamConnect login fails with the following exception in the SAML Gateway log: 'org.opensaml.saml2.metadata.provider.MetadataProviderException: Metadata for entity <name> and role {urn:oasis:names:tc:SAML:2.0:metadata} SPSSODescriptor wasn't found'.	Verify that the value of `sp.entityID` in *saml.properties* matches the entity ID of the Service Provider.
TeamConnect login fails with the following exception in the SAML Gateway log: ArtifactResolutionProfileBase.resolveArtifact | Could not decode artifact response message. org.opensaml.ws.message.decoder.MessageDecodingException: Error when sending request to artifact resolution service. Caused by: javax.net.ssl.SSLHandshakeException: org.springframework.security.saml.trust.UntrustedCertificateException: Peer SSL/TLS certificate	Check the certificate details in the log file. If the exception is for the IDP domain, import the root certificate for the IDP domain into the SAML Gateway application's keystore. The IDP URL is defined in *idp.xml* in the *WEB-INF/classes/metadata* folder of the application.
On login, TeamConnect displays an error message stating 'A system error occurred during authentication. Please contact your administrator to check the system logs.'	Verify that *SAMLAuthenticator.class* has been uploaded to the *System/Authentication/SAML/classes* folder and the application server was restarted after upload.
On login, the browser redirects endlessly.	Verify that: • There is an active TeamConnect user whose username matches the IDP response credential.

Issue	Resolution
	• *Crypto.class* has been uploaded to the *System/Authentication/SAML/classes* folder and the application server was restarted after upload.
On login, TeamConnect displays a Page Not Found error page instead of the home page.	Verify that the TeamConnect login URL in saml.properties is correct and does not have a '/' at the end i.e. the URL should end with /login and not /login/.
Persistent URLs do not work -- the user is logged into TC successfully but the home page is displayed instead of the requested record.	Verify that the TeamConnect URL in *saml.properties* has the same hostname as the user requested URL e.g. if the user accesses TeamConnect using http://example.com/TeamConnect/entityrecord/CONT_3, then the URL in *saml.properties* should be http://example.com/TeamConnect/login and not http://<ip address>/TeamConnect/login