



## **Single Sign-on in Enterprise Configuration Guide**

**Revised June 15, 2020**

COPYRIGHT 2020 Riskconnect, Inc. All rights reserved.

This document contains confidential and proprietary information of Riskconnect, Inc. and is protected by copyright, trade secret and other State and Federal laws. This document and the contents within are for the sole use of Riskconnect, Inc. and its clients only. By accessing or otherwise using these materials, you acknowledge that this information is proprietary and confidential to Riskconnect, Inc.

All rights are reserved. The receipt or possession of this document does not convey any rights and no part of this document may be reproduced or retransmitted, in any form or by any means, electronic, photocopying, mechanical recording or any other means, now known or hereafter invented, without the prior written permission from Riskconnect, Inc.'s CEO. Permitted reproductions, in whole or in part, shall bear this notice.

Riskconnect, Inc.  
1701 Barrett Lakes Blvd, Suite 500  
Kennesaw, GA 30144  
Phone (770) 790-4700

## Contents

1	Single Sign-on in Enterprise .....	4
1.1	Overview .....	4
1.2	Purpose .....	4
1.3	Customer Side Responsibilities .....	4
1.4	Riskconnect ClearSight Side .....	4
2	Configuration of SSO for ClearSight and Enterprise .....	5
2.1	Conditions/Restrictions .....	5
2.2	Implementation Activities .....	5
2.2.1	Step 1 – Action Party: Riskconnect ClearSight .....	5
2.2.2	Step 2 – Action Party: Client .....	6
2.2.3	Step 3 – Action Party: Riskconnect ClearSight .....	6
2.2.4	Step 4 – Riskconnect ClearSight and Client .....	6
3	Troubleshooting .....	7
3.1	Client ID or User Id Provided Does Not Match Our Records .....	7
3.2	RelayState Cannot Be Found in The SSO Message .....	7
3.3	Assertion is Encrypted .....	7
3.4	Single Sign On Assertion Is Not Current .....	8
3.5	Signature Description Could Not Be Created .....	8
3.6	SIGNATURE_NOT_VERIFIED .....	8

# 1 Single Sign-on in Enterprise

## 1.1 Overview

Single Sign-on (SSO) is a session and user authentication service that permits a user to access multiple applications with one set of login credentials (for example, name and password). The benefit of using SSO is that a user must only be authenticated once to gain access to Riskconnect ClearSight or Enterprise and other systems in their organization

## 1.2 Purpose.

The purpose of this document is to serve as reference guide for customers working with Riskconnect to configure SSO for the ClearSight or Enterprise app

## 1.3 Customer Side Responsibilities

1. **Identity Provider (IDP)** – The customer should have an Identity Provider . The IDP provides local authentication services to the user (aka Principal) facilitating access through an HTML page (containing the target Riskconnect URL, SAML assertion, and RelayState) to ClearSight. The IDP should be accessible via private line or internet.
2. **Enterprise User IDs** – A user must have a corresponding user id in Enterprise before the application can be accessed via SSO.
3. **User Mapping** – The client is responsible for maintaining the mapping between user ids in their local security implementation and Enterprise security.

**NOTE:** If a client is using the **Name ID** element in their assertion, the value must be identical to the Enterprise user id. The user id from the client will be sent in a SAML response to Riskconnect ClearSight

4. **Resource Mapping** – The client's SSO configuration must include lists of any resources (for example, Enterprise URLs) they will be requesting access to. The resource must include the variable ssoClient in the URL. This will help identify the target, Enterprise client resource.
5. **Digital Certificate** – This will be used to sign the SAML response.

**NOTE:** The client must provide Riskconnect ClearSight with the public key to the digital certificate. This will be used to validate user access to Enterprise. The client's public key details will be entered in the **Admin** section of Enterprise.

## 1.4 Riskconnect ClearSight Responsibilities

**Service Provider (SP)** – Riskconnect ClearSight supplies the Service Provider. The SP receives a SAML assertion from the client's IDP. Depending on the contents of the assertion, Riskconnect ClearSight's SP will decide whether to fulfill the IDP's request (grant or deny user access to Enterprise).

## 2 Configuration of SSO for ClearSight and Enterprise

### 2.1 Conditions/Restrictions

Please note the following stipulations:

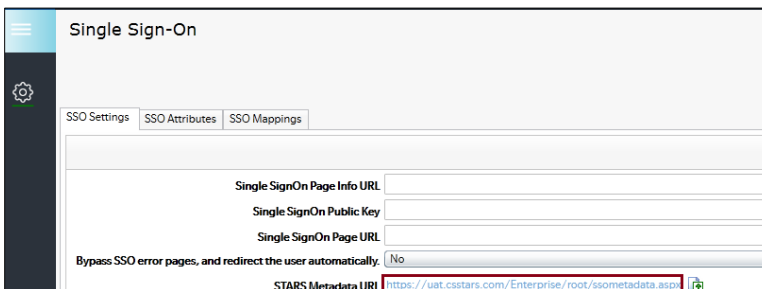
1. ClearSight and Enterprise only support SAML 2.0 SSO.
2. Since https is used, the SAML assertion does not need to and should not be encrypted. However, it can be encoded or signed.
3. ClearSight and Enterprise will not work if embedded in an iFrame element (an HTML document embedded inside another one in a website).
4. The default signature algorithm used in Enterprise is SHA-1 and signing is not required in this case. If a different algorithm (for example, SHA-256, SHA-384, and SHA-512) will be used, please notify Riskconnect ClearSight so that support can be enabled for the chosen algorithm within Enterprise.

### 2.2 Implementation Activities

Below is a high-level breakdown of tasks associated with SSO implementation.

#### 2.2.1 Step 1 – Action Party: Riskconnect ClearSight

6. **Provide SSO metadata from ClearSight or Enterprise to client.** Navigate to **Admin > Single Sign-On > SSO Settings**. Click on **STARS Metadata URL**, copy the contents of the Metadata URL, and send to the client (sample screenshot below for **Enterprise SSO** section in **Admin**).



7. **Provide X.509 public certificate (included in above metadata) to client.**
8. **Provide Entity ID to client.** Included in metadata file
9. **Create Enterprise User IDs (or use existing ones) to be associated with client's SSO IDs.** If users already exist in the system, this step can be skipped.
10. **Provide Enterprise User IDs to client (if new user ids created).** Ask the client to designate a handful of Enterprise for testing SSO.
11. **Provide client with Enterprise Client IDs for UAT and Live respectively.**
12. **Provide client with RelayState URLs for UAT and Live respectively.**

13. **Confirm with customer that their systems are appropriately time-synched to low-stratum time server.** If the client uses the **Not before Date** and **Not On Or After Date** conditions in their SAML assertions, ascertain what these values are.

### 2.2.2 Step 2 – Action Party: Client

**You will need to update the following values in your SSO application:**

- **Sign On URL** – RelayState URL.
- **Identifier** – Entity ID from the metadata file provided by Riskconnect.
- **Reply URL** – AssertionConsumerService (ACS) from the metadata provided to client

Ensure SAML RelayState URL (as provided by Riskconnect ClearSight) is correct and contains the Enterprise Client ID for the target environment.

**Complete other configurations in you SSO application.** For example, mapping of local AD credentials to Enterprise User IDs or provisioning users to the application

**Provide error page(s) URL if client will be creating these.** This is to enable Riskconnect ClearSight redirect users upon authentication denial.

**Provide Digital Certificate (MD5 if possible) containing public key to Riskconnect ClearSight.** Key Length must be less than 2000 characters.

**Inform Riskconnect whether users will bypass Enterprise Error URLs and be redirected to client's pages.**

Provide Bypass Error URL if applicable.

Provide Single Sign-On Page URL (if no special error pages will be required).

### 2.2.3 Step 3 – Action Party: Riskconnect ClearSight

- Import Client's SSO settings from the Digital Certificate containing the client's Public Key in Enterprise.
- Configure error URLs provided by Client (if applicable), the **Bypass Error** setting, and **Single Sign on Page** URLs in Enterprise.
- If signing algorithm used by Client is not SHA-1, enable support for the designated algorithm in Enterprise.
- If required, configure **Clock Drift Global** setting in **Admin**.
- If the client provided URL to metadata location.

### 2.2.4 Step 4 – Riskconnect ClearSight and Client

**Run initial SSO trials and troubleshoot as necessary.** Test a disabled user account and confirm authentication denial. The client's IDP (not Enterprise) is responsible for identifying disabled accounts; therefore, not supplying the affected user with a valid SAML assertion. Enterprise is only responsible for declining invalid SAML assertions.

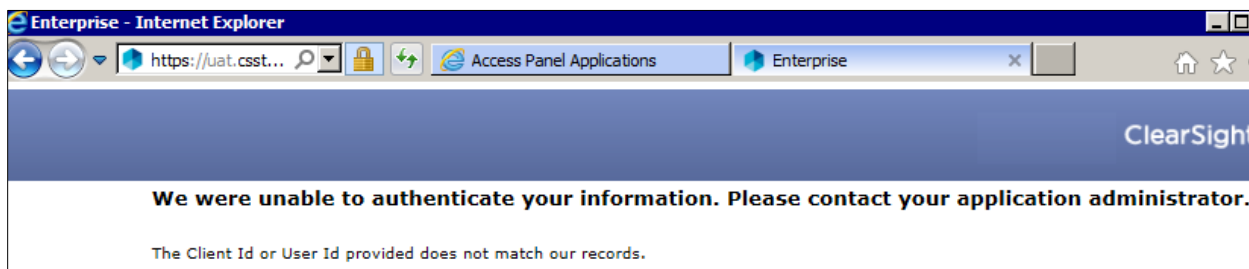
## 3 Troubleshooting

Below are a few errors that may be encountered during and post – SSO configuration and suggestions for resolving them.

### 3.1 Client ID or User Id Provided Does Not Match Our Records

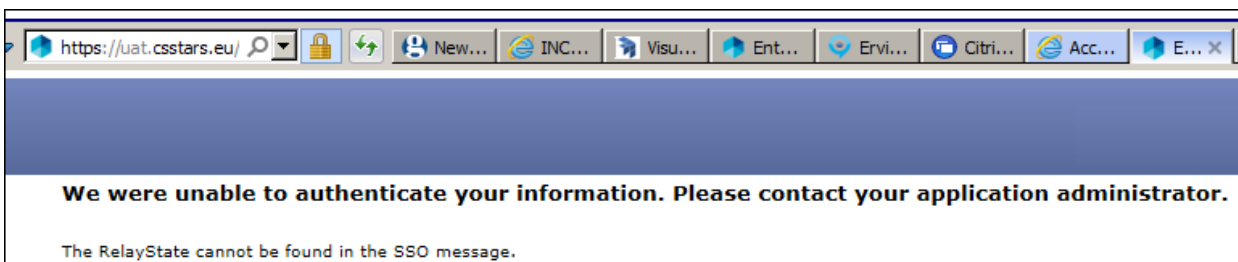
The value for the **NameID** element in the assertion does not match the Enterprise User ID.

Both values must be identical.



### 3.2 RelayState Cannot Be Found in The SSO Message

The **RelayState** form variable within the HTML page is empty. In which case in ACS (Assertion Consumer Service), the SSO client and company parameter needs to be added (For example, <https://www.csstars.eu/enterprise/default.cmdx?ssoClient=Z277>).



### 3.3 Assertion is Encrypted

Ensure that the IDP is set to generate unencrypted assertions. Assertions can be encoded, but not encrypted in order to work with Enterprise.

### 3.4 Single Sign On Assertion Is Not Current

The server time of x is not between the **Not Before Date** of y and the **Not On Or After Date** of z.

For example, the single sign on assertion is not current. The server time of 2016-06-07T11:07:14Z is not between the **Not Before Date** of 2016-06-07T11:07:29Z and the **Not On Or After Date** of 2016-06-07T11:17:29Z. "

This indicates disparities between our server clocks and those of the client. To resolve, set **Clock Drift for Single Sign on (In Minutes)** to 10 in **Enterprise Admin (Configure Screens > Global Settings > Login section)**.

### 3.5 Signature Description Could Not Be Created

**SignatureDescription** could not be created for the signature algorithm supplied. This indicates that the client is not using (Enterprise default) SHA-1 as their signing algorithm. If the client provides the SAML assertion, then this will be noted in the **Signature Method** section. In the example (assertion) below, SHA-256 has been used.

```
<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
```

To enable support for other signing algorithms (SHA-256, SHA-384, SHA-512), navigate to **Admin > Global Settings > Login** section. Set the value to **YES** for **Support SHA2 in Assertion Signatures** (SHA256, SHA384, SHA512).

### 3.6 SIGNATURE\_NOT\_VERIFIED

- The public key is malformed.
- The public key did not come from the same certificate used to sign the assertion.
- The assertion was created without preserving white spaces.