SilkRoad Life Suite Authentication Reference Guide

Version 2016.3

Copyright © 2017 SilkRoad Technology, Inc. All rights reserved.

This material is proprietary to SilkRoad Technology, Inc. It contains confidential information owned by SilkRoad and furnished pursuant to contracts between SilkRoad and its customers. This material is solely for customer's authorized use of SilkRoad hosted applications. This material may not be used, reproduced, copied, disclosed, or transmitted, in whole or in part, beyond the terms of customer's contract without the express written consent of SilkRoad Technology, Inc.

SilkRoad®, RedCarpet®, SilkRoad® Recruiting, SilkRoad® Onboarding, SilkRoad® Performance, SilkRoad® Learning, SilkRoad® HRMS, SilkRoad® Talent Apps, SilkRoad® Agile Performance and their respective tag lines, logos and marks are trademarks owned by SilkRoad Technology, Inc., registered in multiple jurisdictions. All other trademarks are owned by their respective owners.

This document was created using ***Author-it™*** (see Author-it Home - ***http://www.author-it.com***), the total component content management solution. Author-it™ is a trademark of Author-it Software Corporation Ltd.

SilkRoad Technology
100 S. Wacker Drive, Suite 425
Chicago, IL 60606
U.S.A.
1 (866) 329.3363 U.S. toll free
Email: ***info@silkroad.com***
Website: ***http://www.silkroad.com***

Contents

Getting started

In this section

About this guide

This guide provides background information and requirements for customers planning to implement SilkRoad's Identity Provider based Single Sign-on (SSO) and Single Logout (SLO) capabilities in Life Suite modules. It also provides customers with an overview of Identity Provider (IdP) based SSO/SLO.

Note: While this guide provides general information of what is expected from your Identity Provider, it is your responsibility to determine the requirements of your own IdP.

Introduction to Single Sign-On (SSO)

With Single Sign-On (SSO), an employee, using their existing credentials, can access the SilkRoad Life Suite solutions as if they are another piece of your corporate network. This approach increases security by keeping your employees' credentials on your network and makes system access easier for your employees. Benefits to using SSO include:

- Corporate control of password policies
- Centralized reporting for compliance adherence
- Reduces phishing
- Eliminates password fatigue
- Reduces support calls
- Keeps authentication data on corporate network
- Ability for you to add multi-factor authentication
- Widely accepted by users for ease-of-use

SilkRoad implements a Federated Single Sign-on solution, supporting Security Assertion Markup Language (SAML2.0). If an IdP is not an option, SilkRoad has documentation for an alternative solution for those customers still seeking to implement SSO (see SilkRoad Life Suite Authentication–Global GetSession Reference Guide).

Where SSO is not an option for all or some users, SilkRoad provides the Life Suite Login – a unified login to the Life Suite. With Life Suite Login, users log into the Life

Suite with their credentials and can move between Life Suite modules they have access to without having to log in again.

Customers can combine SSO with one or more IdPs, Global GetSession and Life Suite Login to cover their entire user population (e.g. some users via SSO and others via Life Suite Login).

Authentication Admin UI overview

Beginning in the Life Suite 2015.3 release, SilkRoad provides a user interface (UI) so you can manage your own Single Sign-on (SSO) configuration. Using the UI, you can:

- Access the SilkRoad Life Suite federation metadata URL, file, and related parameters
- Set group claim requirements to access a particular Life Suite module
- Add and manage your Identity Provider (IdP)
- Define, manage, and enable/disable your authentication sources: your IdP, Life Suite Login, and Global GetSession

Technical support

For technical assistance for any of our solutions, contact our support staff at:

Email: ***support@silkroad.com***
Web: ***https://silkroad.force.com/community***

Single Sign-on (SSO)/Single Logout (SLO) overview

All corporate networks maintain user/employee accounts, and many companies use special applications to help manage those accounts. These applications are called Identity Management applications. Most, if not all, have the ability to share your employees' identities with external resources such as the Life Suite. A system with the ability to share identities and keep details secured is referred to as an Identity Provider (IdP).

For SSO to work, your IT Department configures your IdP with certificates from SilkRoad and provides SilkRoad with certificates from your IdP. These certificates are used to sign and encrypt/decrypt data that is transferred between the systems. The exchange of certificates is known as creating a Trust Relationship or Federation. SilkRoad Life Suite Authentication will only trust information coming from your servers that have these specific certificates. Using this trusted connection, SilkRoad's servers communicate using the Security Assertion Markup Language (SAML 2.0). Using the SAML protocol, your servers assert who the user is and which groups they belong to. With that information, SilkRoad's Life Suite Authentication can then allow access to the Life Suite solutions for your employees.

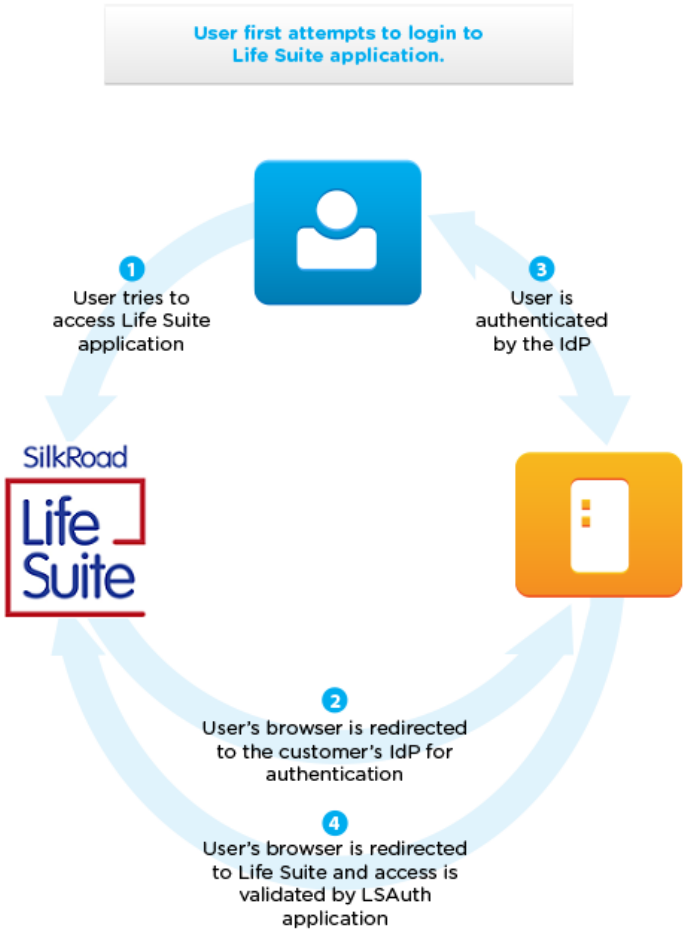
In this section

Single Sign-on (SSO)

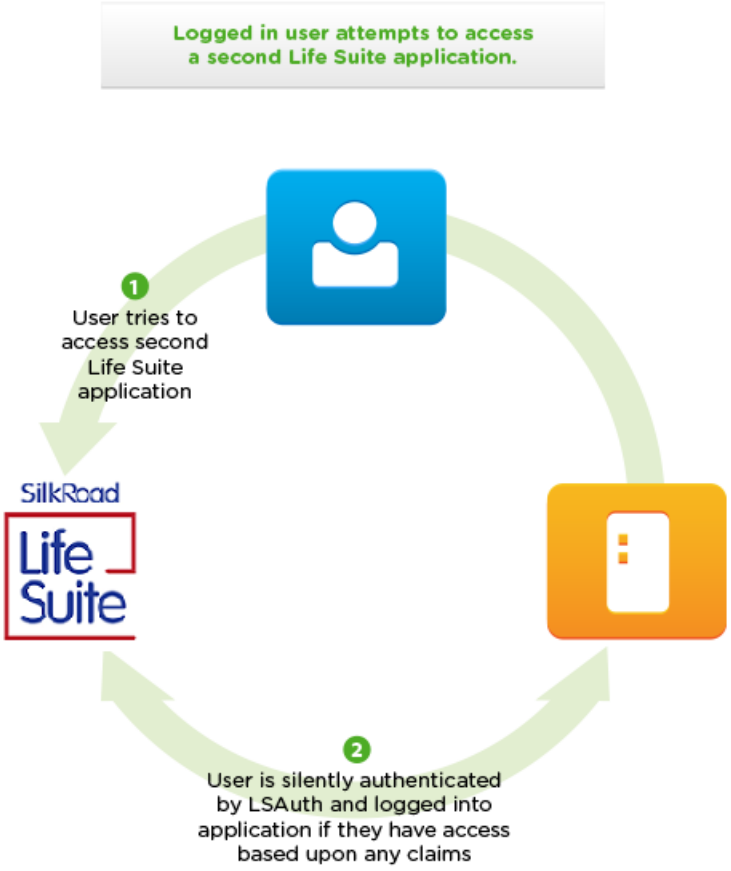
The SilkRoad Life Suite supports Service Provider initiated SSO and Identity Provider initiated SSO.

Service provider initiated Single Sign-on

When a user navigates to a Life Suite module that is configured for SSO, the user is routed to a log-in page hosted by your IdP if the user has not already been authenticated. After your IdP authenticates the user, the user is redirected back to the original page request within the Life Suite module via Life Suite Authentication to validate access.



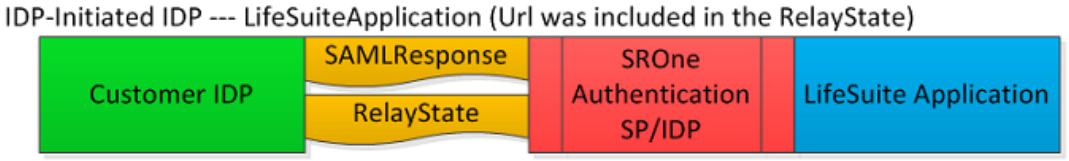
Any subsequent attempts to access other Life Suite applications are authenticated silently via the session generated by the customer IDP without the employee having to provide credentials again.



Identity provider initiated Single Sign-on

Identity provider initiated Single-sign on begins with the IDP authenticating a user. A SAML response is issued from the IDP to Life Suite Authentication. The user is then redirected to the Life Suite module.

A relaystate value is required either as part of the SAMLResponse or as a querystring variable. The relaystate value represents the Life Suite URL target. Life Suite Authentication uses the relaystate value to authorize and redirect the user to the appropriate Life Suite URL.



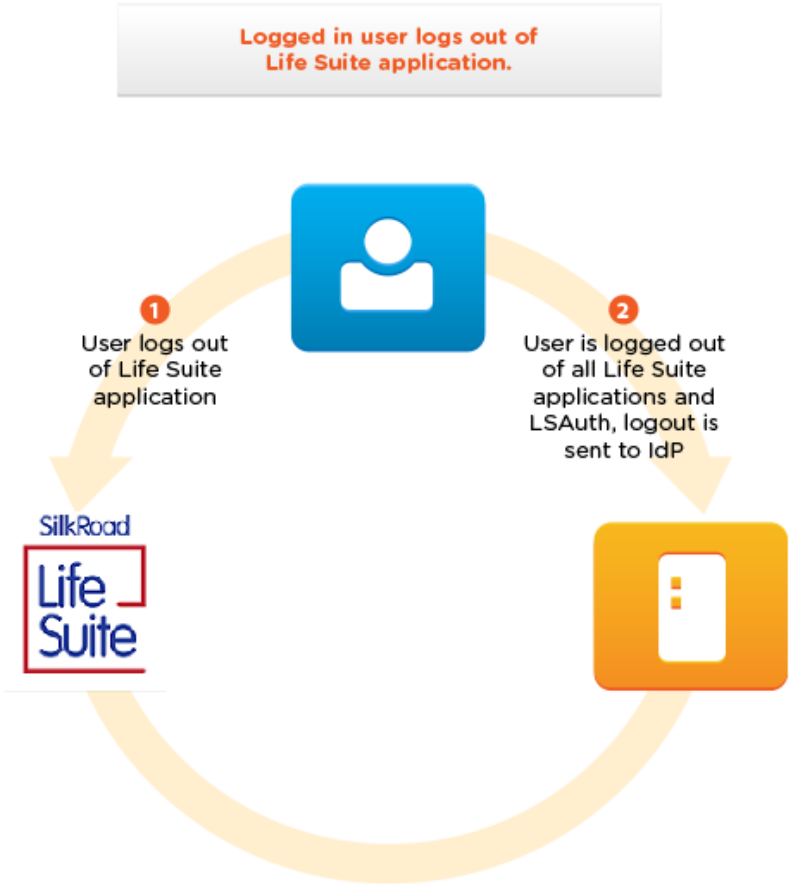
Recommendation: Service provider initiated Single Sign-on

SilkRoad strongly recommends Service provider initiated Single Sign-On (SP initiated SSO) for the following reasons:

- SP initiated SSO is more secure. It requires a SAMLRequest from SilkRoad to your IDP followed by a SAMLResponse from the IDP to the Life Suite. On the other hand, an IDP initiated SSO configuration is a one-way trust with only a SAMLResponse received by the Life Suite.
- Application links and deep links are easier to work with. With SP initiated SSO, any valid link or deep link to an application is accepted with the authenticated user arriving at the desired target. However, with IDP initiated SSO, a user must use a customer portal with appropriate links through the IDP, which generally makes deep links impossible.
- Single Logout (SLO) is only supported in a SP initiated SSO configuration. With IDP initiated SSO, there is no ability to log out in an application and log out of all the applications associated with the session.

Single Logout (SLO)

Single Logout (SLO) only applies to Service Provider Initiated Sign-on. When an employee logs out of a Life Suite module by clicking the module's logout link, the employee is automatically logged out of Life Suite Authentication and all Life Suite modules. If he subsequently attempts to access one of the other modules he will need to be re-authenticated. SLO is for Life Suite modules – any other third-party applications would need to construct their own SLO in conjunction with your IdP.



SLO is not supported with IDP-Initiated SSO. While a Life Suite module might logout, there is no logout at the IDP and therefore the original session might remain active. With IDP-Initiated, the only way to ensure termination of a session is to close the browser.

Life Suite solution variations

Each Life Suite solution has subtle differences in how an employee experiences Life Suite Login or SSO.

Note: From the perspective of the various Life Suite modules, Life Suite Login is also SSO – a single sign-on to the Life Suite. When a module is referred to as configured for SSO that means it is configured for both SSO and the Life Suite Login.

There are three modes related to how an employee can be authenticated:

- External/SSO: Employee must use SSO or the Life Suite Login to authenticate;
- Standard: Employee is authenticated within the Life Suite product using Life Suite application credentials
- Mixed Mode: Employee can use SSO or authenticate within the Life Suite application.

Solution	External/SSO Employee Authentication Option
HeartBeat	Authentication can be done using External/SSO or standard. There is no mixed mode within HeartBeat. This setting is applied to all employees. It is not set on an employee-by-employee basis like the other Life Suite applications.
SilkRoad HRMS	SilkRoad HRMS supports External SSO or Life Suite Login. SilkRoad HRMS does not have a native login process separate from SSO or the Life Suite.
SilkRoad Recruiting	Employees can be set up for External/SSO or standard authentication within SilkRoad Recruiting. There is no mixed mode. SilkRoad Recruiting can be set to force External/SSO so that all users must use the Life Suite Login or SSO. (Note: This does not apply to candidates.)
SilkRoad Onboarding	Employees use the Life Suite Login or SSO.
SilkRoad Learning	Employees can be set up for External/SSO or standard authentication within SilkRoad Learning. There is no mixed mode.
SilkRoad Performance	Employees can be set up for External/SSO or mixed mode authentication within SilkRoad Performance. There is also an option to force Life Suite Login or SSO for all users.

There are also variations in how an employee reaches the appropriate standard authentication log-in page or is redirected for Life Suite Login or SSO. The table below details these differences.

Product	How Employee is Redirected	Employee Has "Use SSO" Setting	With setting "On" – Auth. method	With setting"Off"– Auth. method
HeartBeat	Always redirects if External/SSO is turned on	No – it is SSO only once it's turned on.	N/A (set for all App)	N/A (set for all App)
SilkRoad HRMS	Always redirects to either customer's IDP for an SSO configuration or Life Suite Login.	N/A	N/A	N/A
SilkRoad Recruiting	Always have to click link on standard login page to select to use SSO	Yes	SSO or Life Suite Login only	Standard authentication
SilkRoad Onboarding	Always redirect to SSO or Life Suite Login	Yes	SSO only	Life Suite Login Only

Product	How Employee is Redirected	Employee Has "Use SSO" Setting	With setting "On" – Auth. method	With setting"Off"– Auth. method
SilkRoad Learning	Click link once to attempt SSO from the log-in page. (This sets a cookie so next time it redirects automatically.)	Yes	SSO or Life Suite Login only	Standard authentication
SilkRoad Performance	Click link once to attempt SSO from the log-in page. This sets a cookie so next time it redirects automatically.	Yes	SSO or Life Suite Login only	Mixed mode authentication

Customer requirements

This section provides details about primary customer requirements for setting up SSO with the SilkRoad Life Suite. The better prepared you are with the following requirements, the smoother your SSO implementation will be.

In this section

Identity Provider

Before implementing SSO\SLO, you must have a valid SAML 2.0-compliant Identity Provider (IdP) that is a member of a federation that is responsible for managing the accounts of your users/employees. If you do not have this configured, you need to select and configure a valid IdP in your environment. This requires someone familiar with the complexities of configuring an IdP. If an IdP is not an option, SilkRoad has documentation for an alternative solution (see SilkRoad Life Suite Authentication – Global GetSession Reference Guide).

SilkRoad uses a SAML 2.0 compliant Service Provider. Setting up an IdP requires an understanding of using and configuring Active Directory, proxy servers, certificates and DNS entries at a minimum. Depending on the level of in-house knowledge, you may want to consider contracting with a third party to set up and implement your IdP. Setup and configuration of your chosen IdP is beyond the scope of SilkRoad's Service offerings.

SilkRoad supports the use of multiple IdPs even combined with the Global GetSession and Life Suite Login. This is useful in scenarios where your organization has disparate identity management processes across the organization.

Federation information

A federation is a circle of trust using a standardized, cross-domain, web-based, single sign-on framework. Establishing a trust between SilkRoad's Life Suite Authentication and your IdP allows your users to securely authenticate against your directory service using their current network credentials.

In most cases, all that is required to join the SilkRoad federation is to point to the location of our metadata file. The URL of your specific federation metadata is accessible in Authentication Admin UI (Service Provider>Federation Details page).

From there, you can also download SilkRoad's metadata or obtain the federation details as needed.

Identity Provider and Service Provider applications typically publish data about itself in an xml format to simplify configuration. This is provided by your IdP and should be hosted on a publicly accessible website so that it can be automatically updated. You can use the IdPs metadata URL when adding a new Authentication Source within the Authentication Admin UI. There are also options to upload the metadata file if a URL is not publicly accessible or enter the necessary information manually when defining a new authentication source. If you do not use a publicly available metadata URL, you must update your authentication source information in the Authentication Admin UI whenever a change is made because SilkRoad cannot update the trust automatically.

If you make a change to your IdP, the trust could be broken until you update your authentication source with those changes. In addition, if your IdP cannot be configured to point to our metadata URL and instead relies on an uploaded metadata file, the trust may be broken when a change occurs on our SilkRoad's side, such as the replacement of a security certificate. It is your responsibility to ensure you have the latest version of our metadata file if your IdP cannot refresh this automatically.

Using federation metadata is the preferred method to provide Life Suite Authentication with details of your IdP.

There have been documented, successful federations created between SilkRoad and the following:

- CA SiteMinder Federation
- IBM Tivoli Federated Identity Manager
- Microsoft ADFS 2.0 and 3.0
- Oracle Identity Federation
- Ping Identity PingFederate
- Shibboleth InCommon Federation
- SimpleSAMLPhp
- OneLogin
- Okta
- Salesforce IDP
- Microsoft Azure AD
- Box
- Juniper Networks

Group claim

A group claim is a class of users who have been granted access to a resource. This typically maps to a group in your directory service.

Using group claims is optional. If you want to control who can access to one or more of your Life Suite modules, you can create corresponding groups and provide them as part of a claim assertion.

To use group claims, enter the group name for the appropriate application within the Life Suite Authentication Admin UI. The group claim is the group name that identifies users who are allowed to access the particular Life Suite module. Having this group per module lets you control which users are allowed to log into each Life Suite module. For details, refer to the ***Customer recommendations*** (on page 20) section.

User Identity Claim

The User Identity Claim (UID) is the unique value that identifies an individual user within a Life Suite module. It is often referred to as the SSO ID within the Life Suite modules.

The UID is not the same as a user's login name for manually logging into Life Suite modules. It does not need to be called UID. You can select the appropriate UID claim after:

- You have defined your IdP as an authentication source within the Life Suite Authentication Admin UI
- At least one SAMLResponse has been received from that IdP

  (Life Suite displays a Claims button next to the authentication source with a list of possible claims to identify as the SSO ID/UID claim.

SilkRoad recommends the UID value be the employee number or HRISID. This may require that you add the employee number to your directory service.

Authentication

You need to configure your IdP to validate the user credentials on your side and also configure the IdP system to send the UID claim and claim group to our servers for authentication purposes. The user interface for logging in is also your responsibility and is typically a function of the IdP. For example most IdPs come with a basic web-based log-in page that you can customize to provide a log-in experience consistent with your corporate look and feel.

Time synchronization

It is important that the time is always correct on the machine running the IdP. You must use NTP or similar to keep your server clocks synchronized with nist.gov. Authentication requests can be rejected because of time differences between SilkRoad's servers and yours. This time sensitivity is built into the authentication process to increase security.

Single Logout endpoint

A Single Logout (SLO) endpoint is required to configure a complete federation between the Life Suite and your IdP. This endpoint must return a signed log-out response. If you do not have an SLO endpoint or implement IDP initiated SSO, the log-out functionality is not supported. However, in the absence of the log-out endpoint, Life Suite Authentication still proceeds with log out of Life Suite modules and redirects to a configurable "goodbye" page. A "reply" query string variable can also be provided to automatically redirect a user to the specified URL.

SSO only mode for non SLO IdPs

For IdPs that do not support SLO or if you implement IDP initiated SSO, your federation will be set up in an SSO only mode. In SSO only mode, once you logout of one of the Life Suite modules, you must close all browsers before re-authenticating into a Life Suite module. SilkRoad highly recommends you implement an IdP that supports SLO as we cannot guarantee functionality of logout without an SLO endpoint.

Life Suite requirements

This section outlines requirements of your SilkRoad Life Suite solutions to support Single Sign-On.

In this section

Product version requirements

You must be running a sufficiently recent version of the Life Suite application(s) to use SSO\SLO via an IdP. The SilkRoad Services or Support team will make sure you are running the correct version of your Life Suite product to perform SSO. If you are not running a suitable version, the implementation team will schedule and coordinate an upgrade before you can implement this functionality.

UID requirements

The UID (Unique User Identifier) corresponds to the unique identifier used by your organization to identify an individual employee. We recommend using an employee number or HRISID. It is important that you determine early in the process what this value will be since this value must be consistent across all of your Life Suite applications. It is important to note that this value also dictates additional employee data field values across the Life Suite applications based upon the following recommendations.

Note: If using the SilkRoad Data Integration Platform (also referred to as Integration Platform), it is a requirement that the Unique Employee ID match the SSO ID.

Module	Integration Platform ID		SSO Auth Param		Login ID	HB/HRMS Emp. ID
IdP	Login ID (ID Source)				N/A	N/A
HeartBeat	Username	=	Username	=	Username	EmployeeID
SilkRoad HRMS	Login ID	=	Login ID	=	Login ID	Employee HRISID
SilkRoad Onboarding	Auth Param	=	Auth Param	!=	LoginID *	N/A
SilkRoad Learning	EmpID	=	ExternalAuthenticationKey	= (if via SilkRoad Onboarding)	LoginCode	N/A
SilkRoad Performance	InternalID	=	SSOID	= (if via SilkRoad	Login	N/A

Module	Integration Platform ID		SSO Auth Param		Login ID	HB/HRMS Emp. ID
				Onboarding)		
SilkRoad Recruiting	EmployeeID	=	EmployeeID	= (if via SilkRoad Onboarding)	Username	N/A

*Non-editable and typically set prior to having a defined IdP login ID.

Selecting a value is important because it is possible that either of these values could later be consumed by a payroll or HR system that expects an HRISID and not, for example, a network log-in name. In addition, the chosen value will need to be in your directory service. It is possible that you will need to update your directory service to add this value to each employee record.

UID in Life Suite solutions

The UID is stored in the following fields in the Life Suite solutions. These fields must contain your chosen UID for SSO to work.

- SilkRoad Performance: The SSO ID in the user profile.
- SilkRoad Onboarding: The authentication parameter on the user profile.
- SilkRoad Recruiting: The employee ID on the user record.
- SilkRoad Learning: The authentication key under the **use external authentication** check box. This is in the external authentication section of the user edit.
- HeartBeat: The user name field of the employee.
- SilkRoad HRMS: The Login ID of the user.

User accounts

User names and password are maintained in your directory service; however you must still maintain a related account for each user in each Life Suite application. These accounts also need to be configured for SSO within each Life Suite application. There is no expectation or requirement that the credentials associated with the employee in the Life Suite application match what is in your directory service.

Life Suite Login

The Life Suite Login is an optional, add-on feature that allows for a unified login to all Life Suite solutions. When installed and enabled, users can use their Life Suite Login credentials to access any Life Suite solution they have permission to without re-authenticating. Users have only one set of Life Suite credentials to remember, eliminating the need to remember multiple passwords or request support for forgotten passwords.

Unlike SSO with your own IdP or Global GetSession, Life Suite Login can only provide access to Life Suite modules and Talent Apps. There is no ability with Life Suite Login to give access to other non-SilkRoad-affiliated applications as you would be able to with your own authentication.

The Life Suite Login can be combined with one or more IdPs as need to provide an authentication mechanism for all users. As an example, a customer might have all employees using SSO with a SAML 2.0 supported IdP and then have all contractors authenticate via Life Suite Login. Another example might have all US employees using SSO while non-US employees use the Life Suite Login because they are not stored in a US-based IdP.

In this section

Life Suite Login vs. Single Sign–On (SSO)

Life Suite Login is an alternative to Single Sign-On (SSO), the preferred SilkRoad single sign-on solution. Both solutions allow users to access Life Suite solutions using a single login. However, unlike SSO, Life Suite Login does not require any hardware, software or IT resources on the customer side. It is a great for customers who lack the resources or desire to implement SSO.

Life Suite Login and Life Suite Integration Platform

To use Life Suite Login, the Life Suite Integration Platform (formerly known as SilkRoad Connect) must be first implemented and enabled. The Integration Platform keeps all employees in sync across the Life Suite. In addition, the Integration Platform optionally allows an external system to indicate what Life Suite modules an individual employee can log into. These access values passed by the Integration Platform are merged with any Group Claims specified for that employee from an IDP.

Note: Although Life Suite Login allows for a unified login to Life Suite solutions, user permissions and roles are still controlled within the individual Life Suite solutions.

Life Suite Login and passwords

With the Life Suite Login, authentication is fully managed on the SilkRoad side via the setting of a loginID and password. Generally the first time users access the Life Suite Login, they will need to reset or set their password. (For optimal security, the Life Suite Login does not email passwords to users.) Be sure to send instructions to your new users to instruct them to click on the *Did you forget your password?* link (or equivalent link if you customized your login page).

Note: Upon resetting the password, if a valid referrer (initial browser destination) is detected, the user is first prompted to authenticate with the new password and then is directed to the original browser destination.

Password strength is configurable with the Life Suite Login and includes options to:

- Set minimum password length
- Set maximum password length
- Force new password upon any update to password
- Prevent a password change if it matches a defined number of previous passwords
- Require password contain:
- Upper and lowercase
- Alpha and non-alpha
- Upper and lowercase and alpha and non-alpha
- Three of four – upper and lowercase, alpha and non-alpha

The Life Suite Login stores passwords using a SHA256-bit hash that makes password values secure and irretrievable.

Using Life Suite Login to access Life Suite applications

As a customer administrator, you can use Life Suite Login to access Life Suite applications. You might need to do this in the event of a federation failure between the IDP and a Life Suite application. Use this URL:

`https://{domain}/Authentication/Admin/LifeSuite`

This URL lets you use any Life Suite Login account (that has Authentication permissions) to gain access.

Customer recommendations

In this section

Group Claim recommendations

While optional, SilkRoad recommend that you create a group claim for each of the Life Suite modules to limit access to each module appropriately. Group Claims are just claims using the claimtype: http://schema.xmlsoap.org/claims/Group

It is assumed that your users are stored in a directory service and these group claims would be the equivalent of a directory group in your directory service, for example Active Directory. Users still need to have an account in each Life Suite module, but the addition of group claims provides an additional level of control.

It is recommended that you create a group claim for each product as follows:

- **EpriseUsers**: A group for all users that can use SSO for Eprise (for standalone Eprise).
- **GL_Access**: A group for all users that can use SSO for SilkRoad Learning (GreenLight).
- **HB_Access**: A group for all users that can use SSO for HeartBeat.
- **HR_Access**: A group for all users that can use SSO for SilkRoad HRMS.
- **OH_Access**: A group for all users that can use SSO for SilkRoad Recruiting (OpenHire).
- **PortalStudioUsers**: A group for all users that have access to a Recruiting-only PortalStudio.
- **RC_Access**: A group for all users that can use SSO for SilkRoad Onboarding (RedCarpet).
- **WS_Access:**A group for all users that can use SSO for SilkRoad Performance (WingSpan).
- **CD_Access**: A group for all users that can use SSO for the Life Suite Integration Platform (Connect).
- **PT_Access**: A group for all users that can use SSO for Talent Portal.

The above names are not required and are only provided as samples and recommendations. If any groups are defined, you need to associate them with the appropriate Life Suite module within the Authentication Admin UI.

Life Suite Authentication reviews these claims and looks for a specific (configurable) value before allowing access to each Life Suite module. Most IDPs have the option to include Domain Group Membership into the authentication token they create. This

means you can manage access to our modules by simply managing membership to Domain Groups.

When the IDP includes these group claims, they appear in the AttributeStatement portion of the SAMLResponse. The following sample AttributeStatement shows the inclusion of three groups. If an application had a RequiredGroupClaim set as 'GroupTest', then the owner of this AttributeStatement would be allowed access to the application.

```
  <saml:AttributeStatement>
      <saml:Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue
xsi:type="xs:string">test</saml:AttributeValue>
      </saml:Attribute>
   <saml:Attribute Name="http://schemas.xmlsoap.org/claims/LoginId"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue
xsi:type="xs:string">test2</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="http://schemas.xmlsoap.org/claims/Email"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">HYPERLINK
"mailto:test@silkroadtech.com</saml:AttributeValue"
test@silkroadtech.com</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="UID"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue
xsi:type="xs:string">1</saml:AttributeValue>
      </saml:Attribute>
    <saml:Attribute Name="http://schemas.xmlsoap.org/claims/Group"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue
xsi:type="xs:string">AllowDiagnostics</saml:AttributeValue>
        <saml:AttributeValue
xsi:type="xs:string">DomainAdmin</saml:AttributeValue>
        <saml:AttributeValue
xsi:type="xs:string">GroupTest</saml:AttributeValue>
      </saml:Attribute>
    </saml:AttributeStatement>
```

Another benefit of using groups is the ability to remove an employee's access to specific modules. For example, when an employee gives notice that they are leaving your organization, you may want to remove access to all modules except Onboarding (the employee may still need Onboarding access to complete their off-boarding events.) Prior to using SSO, you would have been required to log into each Life Suite module and disable the user, but that is not necessary if you have the appropriate groups defined.

Note: It is recommended you still disable these accounts in the Life Suite modules manually or programmatically for tracking purposes and to reduce the

possibility that the employee may attempt to log-in manually if your modules are configured to allow this.

Glossary

Active Directory (AD) is Microsoft's directory service.

Group Claim is a collection of users that have been granted access to an application or resource. In Active Directory this is the equivalent of a group. Group Claims are just claims using the claimtype: http://schema.xmlsoap.org/claims/Group

Extensible Markup Language (XML) A set of rules for encoding documents in machine-readable form. XML emphasize simplicity, generality, and usability over the Internet.

External Authentication (EA) is validation of a user's credentials outside of an application to grant access to said application.

Federated Identity/federation of identity, describes the technologies, standards and use-cases which serve to enable the portability of identity information across otherwise autonomous security domains.

Human Resource Information Services ID (HRISID) The employee's unique ID to identify him/her; this is often used across multiple systems to identify the same employee.

Identity Provider (IdP) Provides local authentication services to the principal (typically a user) to a service provider such as SilkRoad. The service provider relies on the identity provider to identify the principal.

Network Time Protocol (NTP) is a means of synchronizing clocks over a computer network.

Proxy Server A server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers.

Security Assertion Markup Language (SAML) A version of the SAML OASIS standard for exchanging authentication and authorization data between security domains.

SAML 2.0 An XML-based protocol that uses security tokens containing assertions to pass information about a principal (usually an end-user) between an identity provider and a web service. SAML 2.0 enables web-based authentication and authorization scenarios including single sign-on (SSO).

Single Logout (SLO) allows a single action of signing out to terminate access to multiple applications.

Single Sign-on (SSO) allows a user to log-in once and gain access to multiple applications without being prompted to log-in again for each of them.

Security Domains are considered to be an application or collection of applications that all trust a common security token for authentication, authorization, or session management.

Security Tokens are used to prove one's identity electronically. Think of tokens as an electronic key to access a resource.

Trust is a system that is relied upon to a specified extent to enforce a specified security policy. As such, a trusted system is one whose failure may break a specified security policy.