

SilkRoad Onboarding

(RedCarpet)

Single Sign On Authentication Guide

Version 2016.1

SilkRoad technology, inc. PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. In no event shall SilkRoad be liable for any loss of profits, loss of business, loss of use of data, interruption of business, or for indirect, special, incidental, or consequential damages of any kind, even if SilkRoad has been advised of the possibility of such damages arising from this publication. SilkRoad may revise this publication from time to time without notice. Some states or jurisdictions do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

Copyright © 2014 SilkRoad technology, inc. All rights reserved.

RedCarpet and Eprise are trademarks or registered trademarks of SilkRoad technology, inc. in the United States and other countries.

You may not download or otherwise export or reexport this Program, its Documentation, or any underlying information or technology except in full compliance with all United States and other applicable laws and regulations, including without limitations the United States Export Administration Act, the Trading with the Enemy Act, the International Emergency Economic Powers Act and any regulations thereunder. Any transfer of technical data outside the United States by any means, including the Internet, is an export control requirement under U.S. law. In particular, but without limitation, none of the Program, its Documentation, or underlying information of technology may be downloaded or otherwise exported or reexported (i) into (or to a national or resident, wherever located, of) Cuba, Libya, North Korea, Iran, Iraq, Sudan, Syria, or any other country to which the U.S. prohibits exports of goods or technical data; or (ii) to anyone on the U.S. Treasury Departments Specially Designated Nationals List or the Table of Denial Orders issued by the Department of Commerce. By downloading or using the Program or its Documentation, you are agreeing to the foregoing and you are representing and warranting that you are not located in, under the control of, or a national or resident of any such country or on any such list or table. In addition, if the Program or Documentation is identified as Domestic Only or Not-for-Export (for example, on the box, media, in the installation process, during the download process, or in the Documentation), then except for export to Canada for use in Canada by Canadian citizens, the Program, Documentation, and any underlying information or technology may not be exported outside the United States or to any foreign entity or foreign person as defined by U.S. Government regulations, including without limitation, anyone who is not a citizen, national, or lawful permanent resident of the United States. By using this Program and Documentation, you are agreeing to the foregoing and you are representing and warranting that you are not a foreign person or under the control of a foreign person.

SilkRoad RedCarpet Single Sign On Authentication Guide

Document Version: November 2015

Product Version: RedCarpet v 2016.1

Technical Support

SilkRoad technology, inc.

Web: <http://support.silkroadtech.com>

Phone: 866-329-3363

Headquarters

20 West Kinzie Street, Suite 1220

Chicago, IL 60654

1 (866) 329.3363 toll free (U.S. only)

+1 (336) 201.5100 phone

+1 (336) 201.5141 fax

www.silkroad.com

RedCarpet Single Sign On Authentication

Overview

RedCarpet allows you to use an external application to authenticate your RedCarpet users. The “standard” (default) installation of RedCarpet uses the user profile stored in the RedCarpet database to authenticate a user’s credentials.

Any SAML IDP can be used to perform the authentication requirements. RedCarpet authentication is defined as verifying a valid user and password.

Authentication vs. Authorization

Using your application to authenticate a user has *no impact* on the user’s authorization to content. All RedCarpet content is targeted (and specific) to the current user. For example, RedCarpet menu options, RedCarpet content, and what content is available in a user’s RedCarpet portals are all a result of user authorization. Content authorization is handled 100% by RedCarpet.



Establishing RedCarpet Users as SSO Authenticated Users

Each employee in RedCarpet has an authentication type of Standard or External.

- Use Standard if: your organization does not have an identity provider established. Setting an employee to Standard authentication type indicates the login credentials (login id and password) are stored in the RedCarpet database.
 - All SilkRoad LifeSuite applications can authenticate against a Standard employee. This is called “LifeSuite Login”.
- Use External if: your organization has an identity provider established. Setting an employee to External authentication type indicates the login credentials (login id and password) are stored in the IDP configured in the LifeSuite Authentication site.

Add Employee Profile

Step 1 of 3

Details:	First Name	<input type="text"/>	Corporate Employee ID	<input type="text"/>
	Middle Name	<input type="text"/>	Authentication Type	<input checked="" type="radio"/> Standard <input type="radio"/> External
	Last Name	<input type="text"/>	Login ID	<input type="text"/>
	Email	<input type="text"/>	SSO ID	<input type="text"/>
	Hire Date	<input type="text"/> 	Password	<input type="password"/>
	Termination Date	<input type="text"/> 	Confirm Password	<input type="password"/>
			<input checked="" type="checkbox"/> Auto Generate Password	
			<input checked="" type="checkbox"/> Force Password Change	

- Figure 1: Establishing an externally authenticated user

For most implementations the Login ID and the SSO ID should match. Sometimes the RedCarpet Login ID is established before a corporate login id is established.

In the example in Figure 1 - the “SSO Authentication Parameter Label” has been configured (via Settings) to display “SSO ID”.

The “Corporate Employee ID” is not used for log in. The employee ID is optional and applies for organizations that have employee ids that differ from an SSO id.

- the employee id is use for:
 - integrations with other applications (via the RedCarpet web methods) where the other application uses this id
 - an alternate search criteria for locating employees in RedCarpet.

In the example in Figure 1 - the “Employee HRSID Label” has been configured (via Settings) to display “Corporate Employee ID”.

◁ The “SSO Authentication Parameter” is populated with the user id used in the external application. This must match the “UID” passed in the GetSession method call.

Eprise Version: 2015.3.2.041

Employees	UI	Reporting	Notification	I-9	Tasks	APIs	Logos	O
SSO Authentication Parameter Label The display label for the Single Sign On identifier field. SSO ID								
Employee HRISID Label The display label for the Employee HRIS ID field. Corporate Employee ID								

Configuring your IDP

There are three ways you can set up a Single Sign-on experience:

- Global GetSession
- Life Suite Login
- SAML 2.0 supported IdP

Global GetSession and Life Suite Login authentication sources are added for you by SilkRoad staff.

You can reference the information SilkRoad Staff will collect by referencing the [online help for the Life Suite Authentication](#) application.

What to Provide to Your SilkRoad Implementation Team

Your SilkRoad implementation team will be configuring your RedCarpet application to work with the LifeSuite Authentication application. Our Authentication application requires a secure handshake with your IDP to validate the user's credentials.

You will need to provide:

- 1 A URL to the login page of your IDP.
- 2 The ip address of your server running the application. RedCarpet will establish a secure "back channel" with your application. A back channel is established to identify what ip addresses are allowed request a RedCarpet session. The

trusted handshake will be valid only between **your** RedCarpet implementation and **your** server.

- 3 In addition to configuring RedCarpet to establish a trusted back channel with an application server (or servers), RedCarpet also offers application level security through a Blowfish encryption key. Using Blowfish encryption is not required but we recommend it.

RedCarpet is easily configured to accept an encrypted application key (instead of clear text) to validate the data in the method call.

Your application and your RedCarpet installation must be configured with a matching encryption key. The key will be used to encrypt and decrypt the “ApplicationKey” value to insure the method call is from a valid source. See “Setting up the WebConfig Code Example” for additional information.

If you want to use an encrypted key (recommended), you must also provide a string to be used as the Blowfish encryption key.

An example string value is “FEDCBA9876543210”.

<Note: Blowfish encryption functions use code placed in the public domain. See <http://www.schneier.com/blowfish.html> if you are unfamiliar with the Blowfish encryption algorithm.

How RedCarpet works with External Authentication

At a very high level, the logical process flow of authenticating a user through your application is as follows:

- 1 Any RedCarpet or permissioned RedCarpet portal page is requested but instead of prompting the user for their credentials, the request is redirected to Life Suite Authentication. Life Suite Authentication redirects to the configured service provider.
- 2 The service provider receives the redirected authentication request, authenticates the user, and responds to Life Suite Authentication.
- 3 After receiving confirmation of a valid user, LifeSuite Authentication makes an Eprise web service call over a secure channel and returns a valid RedCarpet session identifier.
- 4 LifeSuite Authentication responds passing the session identifier as a query string on the (requested) referred URL.
- 5 The browser redirects the request for the RedCarpet page. RedCarpet serves the page in response to a fully authenticated and authorized RedCarpet user.