SilkRoad Onboarding

(RedCarpet)

Single Sign On Authentication Guide

Version 2016.1

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.

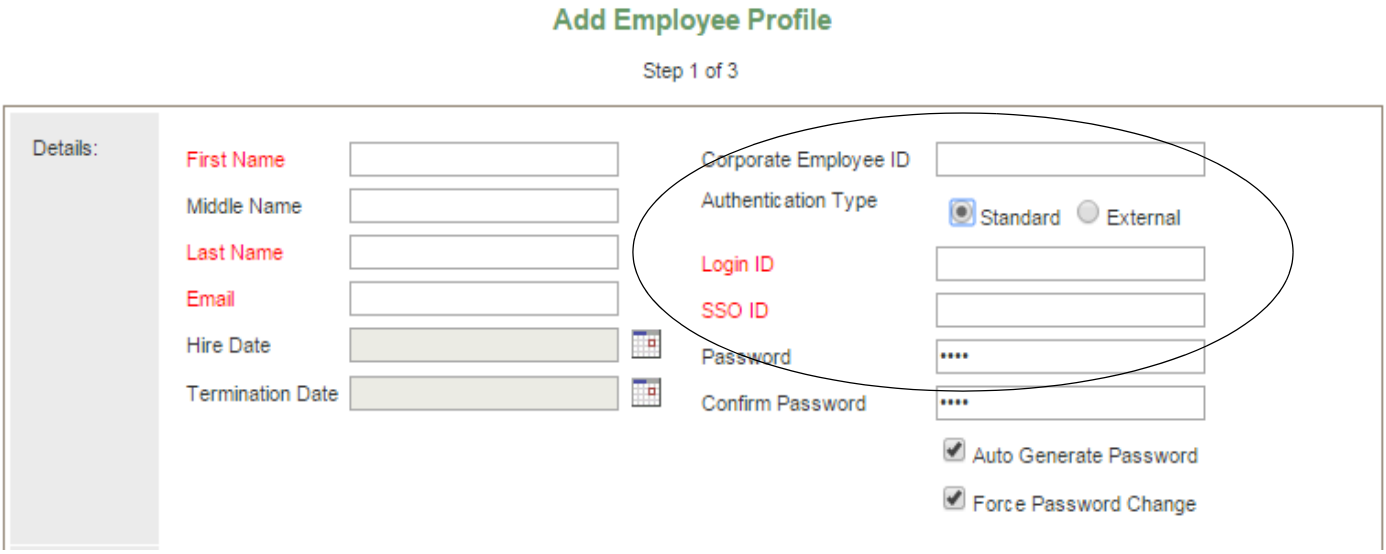
Authentication vs. Authorization

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.



- 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.

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 appplication. 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 recieving 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.