



CA SiteMinder

Authentication Method Group

Alternative User Experience

Contents

Change History	1
Summary.....	2
Intended Audience	3
Prerequisites.....	3
Required Information.....	3
Create Authentication Method Group	3
Create Authentication Partnerships	3
Create Federation Partnerships	3
Deploy Customization.....	6
sps-chs-overlay.....	6

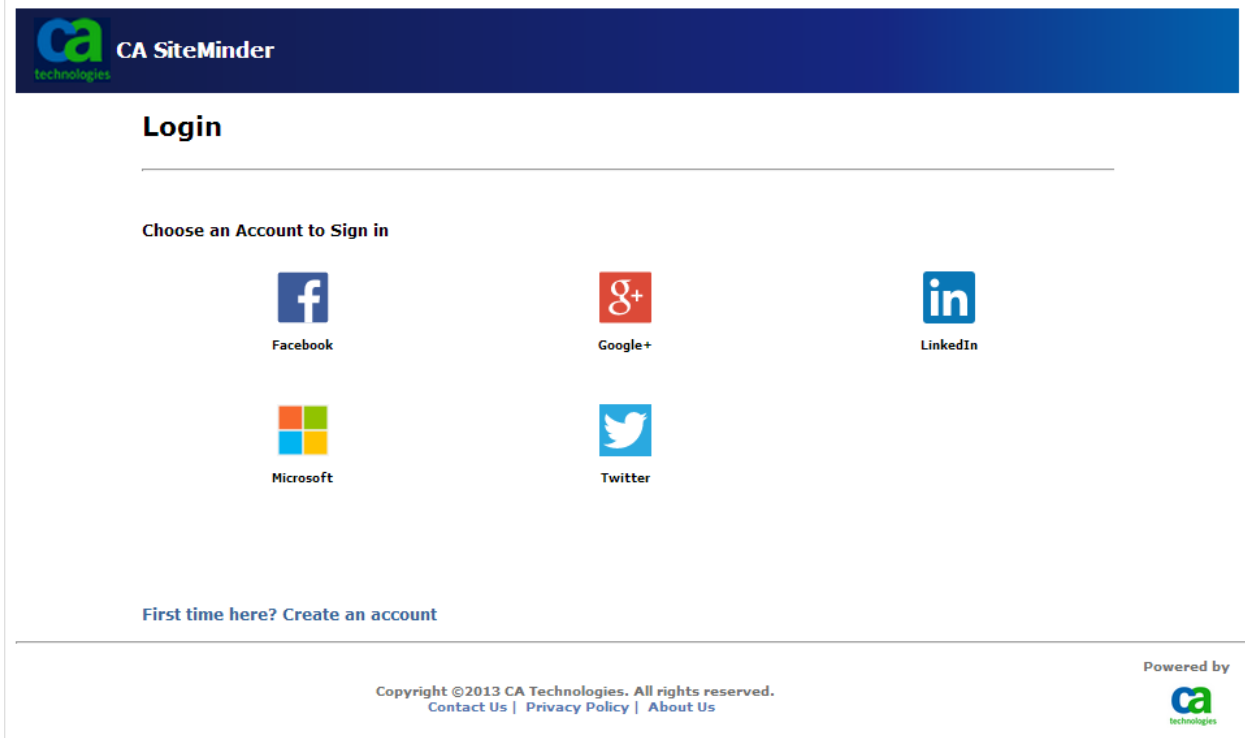
Change History

Revision	Name	Email	Reason for Change
1.0	Tim Hobbs	Timothy.Hobbs@ca.com	Initial draft

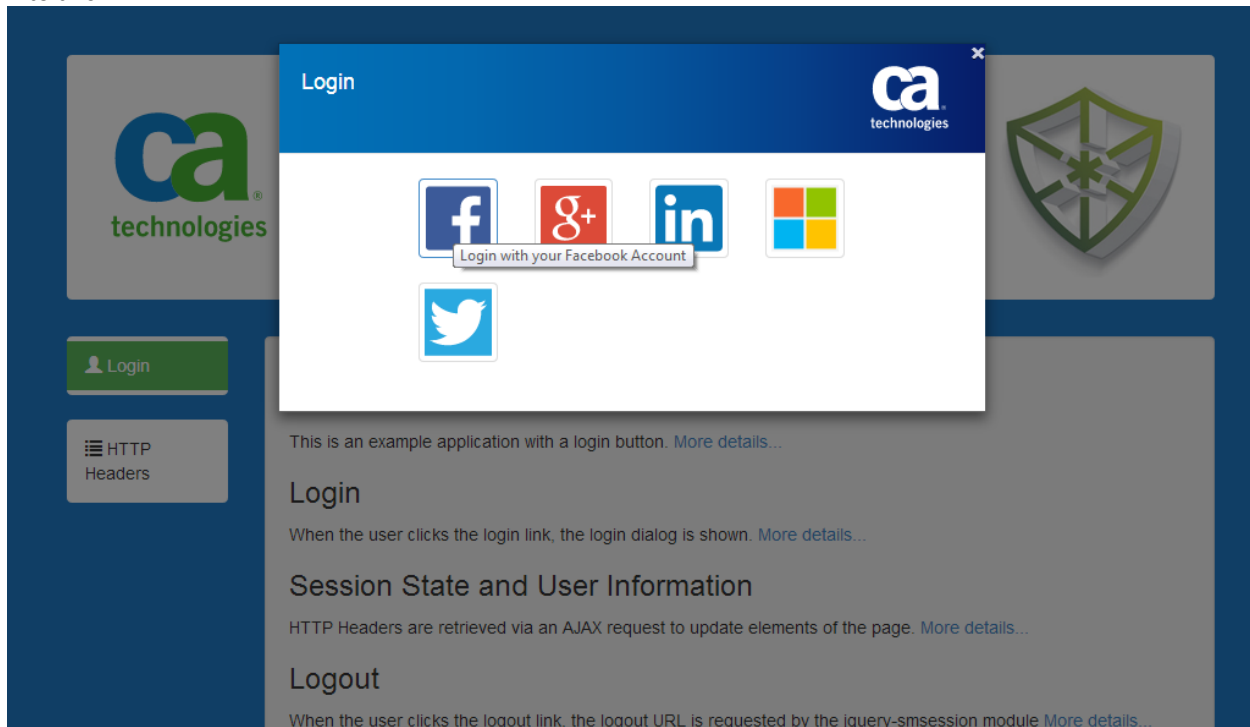


Summary

How to modify the user experience for SiteMinder Authentication Method Groups.
Change this:



Into this:





Intended Audience

This document is for CA SiteMinder Administrators.

Prerequisites

To complete this integration you need:

1. SiteMinder 12.52 or later
 - a. SiteMinder Service Provider Partnership (at least one)
 - b. SiteMinder User Directory (at least one)

Required Information

The following information is needed:

Placeholder	Example	Source	Description
[baseUrl]	https://siteminder.example.com	SiteMinder Administrator	Base URL of SiteMinder Federation
[spPartnership]	facebook-partnership	SiteMinder Administrator	Name of the service provider partnership
[spUserDirectory]	Facebook Users	SiteMinder Administrator	Name of the user directory used to disambiguate users in the partnership
[userDirectory]	My Users	SiteMinder Administrator	Name of the user directory

Create Authentication Method Group

An Authentication Method Group cannot be created until after at least one service provider partnership is created. Create an Authentication Method Group.

1. Navigate to Infrastructure, Authentication, Authentication Method Groups, Create Authentication Method Group
 - a. Group Name: MyAuthMethodGroup
 - b. Add a service provider partnership
 - i. SP Partnership Name: [spPartnership]
 - ii. Authentication URL: [accept the default]
 - iii. Logo URL: An http or https static URL. If your [baseUrl] is https, use https.
 - iv. Display Name: A short name to be used as an alternative to an image, e.g. Facebook
 - v. Description: A longer description, e.g. Login with your Facebook Account
 - c. Save the Authentication Method Group

Create Authentication Partnerships

User selection of an Identity Provider for login requires the configuration of a local federation partnership. This requires a user directory, four federation entities and two partnerships. SAML Artifact binding must be used to allow the AJAX request to receive data.

Create Federation Partnerships

This step requires:

[baseUrl]

[userDirectory]



1. Navigate to Federation, Partnership Federation, Entities, Create Entity
 - a. Location: Local
 - b. Type: SAML2 IDP
 - c. Entity ID: authidp
 - d. Entity Name: authidp-local
 - e. Base URL: [baseUrl]
 - f. Supported NameID Formats: Unspecified
 - g. Confirm and Finish
2. Navigate to Federation, Partnership Federation, Entities, Create Entity
 - a. Location: Remote
 - b. Type: SAML2 SP
 - c. Entity ID: authsp
 - d. Entity Name: authsp-remote
 - e. Remote Assertion Consumer Service URLs
 - i. Binding: HTTP-Artifact
 - ii. URL: [baseUrl]/affwebservices/public/saml2assertionconsumer
 - f. Supported NameID Formats: Unspecified
 - g. Confirm and Finish
3. Navigate to Federation, Partnership Federation, Entities, Create Entity
 - a. Location: Local
 - b. Type: SAML2 SP
 - c. Entity ID: authsp
 - d. Entity Name: authsp-local
 - e. Base URL: [baseUrl]
 - f. Supported NameID Formats: Unspecified
 - g. Confirm and Finish
4. Navigate to Federation, Partnership Federation, Entities, Create Entity
 - a. Location: Remote
 - b. Type: SAML2 IDP
 - c. Entity ID: authidp
 - d. Entity Name: authidp-remote
 - e. Remote SSO Service URLs
 - i. Binding: HTTP-Redirect
 - ii. URL: [baseUrl]/affwebservices/public/saml2sso
 - f. Supported NameID Formats: Unspecified
 - g. Confirm and Finish
5. Navigate to Federation, Partnership Federation, Partnerships, Create Partnership, SAML2 IDP -> SP
 - a. Configure Partnership
 - i. Partnership Name: authidp-authsp
 - ii. Local IDP: authidp-local
 - iii. Remote SP: authsp-remote
 - iv. User Directory:
 1. [spUserDirectory]
 2. [userDirectory]



- b. User Identification
 - i. Each User Directory: All Users in Directory
- c. Assertion Configuration
 - i. Name ID Format: Unspecified
 - ii. Name ID Type: User Attribute
 - iii. Value: uid

Note: If your user directories do not use the same uid, then choose an appropriate attribute.

- iv. Assertion Attributes: Any
- d. SSO and SLO
 - i. Authentication Mode: Credential Selector
 - ii. Authentication Base URL: [baseUrl]
 - iii. Authentication Method Group: MyAuthMethodGroup
 - iv. Authentication Request Binding: HTTP-Redirect
 - v. SSO Binding: HTTP-Artifact
 - vi. The remaining values are supplied from the entities.
- e. Signature and Encryption
 - i. Disable Signature Processing: Any
- f. Confirm and Finish
- g. Activate the Partnership
- 6. Navigate to Federation, Partnership Federation, Partnerships, Create Partnership, SAML2 SP -> IDP
 - a. Configure Partnership
 - i. Partnership Name: authsp-authidp
 - ii. Local SP: authsp-local
 - iii. Remote IDP: authidp-remote
 - iv. User Directory: [userDirectory]
 - b. User Identification
 - i. Use Name ID: checked
 - ii. LDAP Search Specification: uid=%s

Note: If your user directories do not use the same uid, then choose an appropriate search.

- c. SSO and SLO
 - i. Authentication Request Binding: HTTP-Redirect
 - ii. SSO Profile: HTTP-Artifact
 - iii. Enforce Single-Use Assertion: checked
 - iv. Use Persistent Session: checked
 - v. Add a row for a Remote SOAP Artifact Resolution URL:
 - 1. [baseUrl]/affwebservices/public/saml2ars
 - 2. Select the row by checking the box under Select
 - vi. The remaining values are supplied from the entities.
- d. Signature and Encryption
 - i. Disable Signature Processing: Any
- e. Application Integration
 - i. Redirect Mode: Persist Attributes
 - ii. Target: [baseUrl]/static/html/application.html



- iii. Relay State Overrides Target: checked
- iv. Persist Authentication Session Variables: unchecked
- v. Enable Attribute Mapping: unchecked
- f. Confirm and Finish
- 7. Activate the Partnership

Deploy Customization

The modification to the Credential Handler Service (CHS) is not a supported configuration.

[sps-chs-overlay](#)

The sps-chs-overlay webapp modifies the tenantlogin.jsp and errorpage.jsp to provide a JSON formatted response for AJAX clients. Deploy the application according to the included readme.md.



Copyright © 2014 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. This document is for your informational purposes only. CA assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA provides this document “as is” without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill or lost data, even if CA is expressly advised in advance of the possibility of such damages.

This publication may contain sample application programming code and/or language which illustrate programming techniques on various operating systems. Notwithstanding anything to the contrary contained in this publication, such sample code does not constitute licensed products or software under any CA license or services agreement.

You may copy, modify and use this sample code for the purposes of performing the installation methods and routines described in this document. These samples have not been tested. CA does not make, and you may not rely on, any promise, express or implied, of reliability, serviceability or function of the sample code.