AURORA Unified Identity Security Platform X Series

Feature List 2021

DISCLAIMER

Silverlake Sheaf Pte Ltd. ("Silverlake") does not make any representation or warranty, express or implied, as to the accuracy, timeliness or completeness of this document or the information contained herein and none of such parties shall have any direct or consequential liability for the information contained in, or any omissions from, this document.

The information contained herein is subject to change without notice. Silverlake reserve the right to amend or replace the information at any time, and undertake no obligation to update or correct the information set forth herein or to provide the recipient with access to any additional information. This information may not be modified, redistributed or reproduced by the recipient whether such information is in electronic or hard copy form.

The information contained herein is preliminary and does not purport to contain all the information that interested parties may desire.

Neither the receipt of this information by any person, nor any information contained herein constitutes, or shall be used or relied upon as constituting, the giving of advice by Silverlake to any such person.

AURORA Unified Identity Security Platform X Series – An Overview

Full end-to-end Unified Identity Security Platform features

Feature categories	X3 Series	X5 Series	X7 Series
Accounts Management	✓	✓	✓
User Provisioning	✓	✓	✓
Social Login	●	✓	✓
Self Service	✓	✓	✓
Broker Trust with external IdPs	●	●	✓
Identity Federation	●	●	✓
Adaptive Authentication	●	✓	✓
Analytics	✓	✓	✓

AURORA Unified Identity Platform X Series – Features in detail

Features	X3 Series	X5 Series	X7 Series
Account Management: Managing User Accounts			
User Registration			
• User Registration with Password Entry	✓	✓	✓
• User Registration with Email Verification	✓	✓	✓
• User Self-Registration	●	✓	✓
Password Policies			
• Password Patterns	✓	✓	✓
• Password History	✓	✓	✓
• Password Expiry	✓	✓	✓
Password Reset			
• Password Reset with Email	✓	✓	✓
• Password Reset with Challenge Question	✓	✓	✓
User Name Recovery			
• matching the **user claims** that are related to user attributes. The user will be prompted to enter values for these user attributes. If the value entered by the user matches with the claims, the corresponding username will be emailed to the user's registered email ID.	✓	✓	✓
Account Locking			
• Admin-Initiated Account Locking	✓	✓	✓
• Account Locking due to Failed Login Attempts	✓	✓	✓

Account Disabling			
• Enables the privileged users to disable user accounts for longer durations. These disabled user accounts can only be unlocked by privileged users.	✓	✓	✓
Account Pending Status			
• Places users in a pending status when the process of self-registration, email verification or ask password has been initiated and the confirmation mail has been sent, but the email has not been verified yet.	✓	✓	✓
Provisioning Provisioning is the process of creating, maintaining, and deleting digital identities (accounts) for users of a system(s) and linking appropriate rights to identities in the form of rules and roles. Identity provisioning is key for Identity Federation. Identity federation is a mechanism that allows authentication across different enterprises in different trust domains based on a trust factor. This makes access easy, as users do not have to remember a different set of credentials for every application they use.			
Inbound provisioning provisions users or groups into AURORA Unified Identity Server by an external application. These external applications are referred to as service providers. AURORA Unified Identity Server supports the SCIM API and SOAP-based Web service API standards for inbound provisioning.	✓	✓	✓
Outbound Provisioning	✓	✓	✓

Use case: Salesforce as the identity provider to provision users from AURORA Unified Identity Server. This means that once this is configured, new users that are added to AURORA Unified Identity Server are added to Salesforce as well.			
Account Syncing Exporting User Data from AURORA Unified Identity Server			
• Sync Accounts to ARION applications	✓	✓	✓
• Sync Accounts to HubSpot	✓	✓	✓
• Sync Accounts to MailChimp	✓	✓	✓
• Sync Accounts to Pardot	✓	✓	✓
• Sync Accounts to Pipedrive CRM	✓	✓	✓
• Sync Accounts to Salesforce	✓	✓	✓
• Sync Accounts to Sendgrid	✓	✓	✓
• Sync Accounts to Zoho CRM	✓	✓	✓
Social Login	●	✓	✓
Self-Service	●	✓	✓
Broker Trust with external IdPs	●	●	✓
Single Sign-On Single sign-on is a key feature of the AURORA Unified Identity Server that enables users to access multiple applications using the same set of credentials.			
• Single Sign-On Using SAML2	✓	✓	✓

• Single Sign-On Using OpenID Connect	✓	✓	✓
• Single Sign-On Using Integrated Windows Authentication	●	✓	✓
• Single Sign-On Using WS-Federation	●	✓	✓
• Configuring reCAPTCHA for Single Sign On By configuring reCAPTCHA, you can mitigate or block brute force attacks.	✓	✓	✓
• Single Sign-On for Native iOS Applications with AURORA Unified Identity Server	●	✓	✓
• SAML 2.0 Web SSO	✓	✓	✓
• WS-Trust Security Token Service	●	✓	✓
• WS-Federation SSO	●	✓	✓
• Integrated Windows Authentication IWA SSO	●	✓	✓
• Oauth2-OpenID Connect SSO ○ OpenID Connect Single Logout ○ OpenID Connect Back-Channel Logout	✓	✓	✓
• Logging into WordPress using the Identity Server	●	✓	✓
• Logging into OpenCart using the Identity Server	●	✓	✓
• Logging into Drupal using the Identity Server	●	✓	✓
Access Delegation			
• Access Delegation with Oauth 2.0	●	✓	✓
• Access Delegation with UMA	●	✓	✓

Identity Federation

Identity federation is a mechanism that allows authentication across different enterprises in different trust domains based on a trust factor. This makes access easy, as users do not have to remember a different set of credentials for every application they use. However, the users have to provide their credentials to each one of the applications separately although the credentials used

are the same. On the other hand, SSO enables users to provide their credentials once and obtain access to multiple applications. In SSO, the users are not prompted for their credentials when accessing each application until their session is terminated.			
Federated Authentication • SAML 2.0 Web SSO	●	●	✓
• Oauth2-OpenID Connect	●	●	✓
• WS-Federation	●	●	✓
• Facebook	●	●	✓
• Yahoo	●	●	✓
• Google	●	●	✓
• Microsoft Windows Live	●	●	✓
• IWA on Linux	●	●	✓
• AD FS as a Federated Authenticator	●	●	✓
• Twitter	●	●	✓
• Apple	●	●	✓
Multi-Factor Authentication Multi-factor authentication is an authentication mechanism that enhances security by granting access to users only after they have successfully passed two or more layers of authentication to prove their identity. For example, in addition to providing a username and password to login, an application can be configured to request users to provide a one-time password (OTP) or fingerprint verification as an extra authentication step.			
MFA in AURORA Unified Identity Security Platform:			
• MFA using FIDO	✓	✓	✓
• Configuring SMS OTP	✓	✓	✓
• Configuring Email OTP	✓	✓	✓
• Configuring TOTP	✓	✓	✓
• MFA for Management Console	✓	✓	✓

• Configuring X509Certificate Authenticator	✓	✓	✓
AURORA Unified Identity Security Platform has comprehensive support for MFA, with authenticators available for SMSOTP, FIDO, MEPin and more* (See attached list)			
MFA with federated authenticators	✓	✓	✓
Identity Server enables configuring MFA in the following ways when a federated identity provider (IdP) is configured as the first factor.			
• Configuring MFA based on the claims that are provided by the locally provisioned/associated user of the federated IdP in the first factor. **(Recommended)**	✓	✓	✓
• Configuring the second factor based on the claims that are provided by the federated IdP in the first factor. *(Not recommended)*	✓	✓	✓
Fine-grained access control with extensible Access Control Markup Language (XACML) 3.0.	✓	✓	✓
Multi-Tenancy	✓	✓	✓
Analytics	✓	✓	✓
• Identity Analytics	✓	✓	✓
• Web Analytics Solutions	●	✓	✓
Authentication			
• Password-less authentication using FIDO2	●	✓	✓
• Logging in to your application via Identity Server using Facebook Credentials	●	✓	✓

• Configuring Shibboleth IdP as a Trusted Identity Provider	●	✓	✓
• Logging in to SimpleSAMLphp using Identity Server	●	✓	✓
• Enabling SSO for Management Console using OpenSSO as the IDP	●	✓	✓
• Logging in to Salesforce using the Identity Serve	●	✓	✓
• Logging in to Salesforce with Facebook	●	✓	✓
• Logging in to Salesforce with Integrated Windows Authentication	●	✓	✓
• Logging in to AURORA Products via the Identity Server	✓	✓	✓
• Logging in to Workday using the Identity Server	●	✓	✓
• Logging in to Microsoft Dynamics CRM with WS-Federation	●	✓	✓
• Logging in to Microsoft Sharepoint Web Applications using Identity Server	●	✓	✓
• Logging in to Office365 Using AURORA Unified Identity Server	●	✓	✓
• Logging in to Office365 with WS Federation	●	✓	✓
• Logging in to Office365 with WS-Trust	●		
• Logging in to a .NET application using the Identity Server	●	✓	✓
• Using REST APIs via XACML to Manage Entitlement	●	✓	✓
• Logging in to Google using the Identity Server	●	✓	✓

• Logging in to an Application Using Google	●	✓	✓
Adaptive Authentication provides an authentication script editor that allows you to define authentication scripts using JavaScript. The script editor provides a set of predefined templates that you can use to easily set up adaptive authentication for some of the most common authentication scenarios. You can define scripts that can consider the following evaluation criteria:			
• User attributes	●	✓	✓
• User behaviour	●	✓	✓
• Level of assurance of the access request	●	✓	✓
• Risk analysis statistics	●	✓	✓
• Machine learning algorithms	●	✓	✓
Define dynamic authentication sequences that can perform actions similar to the following:			
• Control the authentication step selection	●	✓	✓
• Change user attributes	●	✓	✓
• Send email notifications	●	✓	✓
• Redirect users to an error page etc	●	✓	✓
Pre-defined templates for common adaptive authentication use cases			
• Role-Based	●	✓	✓
• User-Age-Based	●	✓	✓
• Tenant-Based	●	✓	✓
• User Store-Based	●	✓	✓
• IP-Based	●	✓	✓
• New-Device-Based	●	✓	✓
• ACR-Based	●	✓	✓
• Risk-Based	●	✓	✓

• Criterial-Based	●	✓	✓
• With Function Library	●	✓	✓
My Account Users can manage their user account-related preferences with more convenience. The latest set of features:			
• User profile management • Linked accounts • Export user profile • Reset password • Account recovery • Multi-factor authentication • Monitor active user sessions • Consent management • Review pending approvals	✓	✓	✓

* LIST OF READILY AVAILABLE AUTHENTICATORS

WS-Trust Authenticator	Passive-STS Federated Authenticator
OPA	OpenID Connect Authenticator
Evident Identity Verification	Windows-Live Authenticator
JWT SSO Inbound Authenticator	Yahoo Authenticator
Cognito	Google Authenticator
CASQUE SNR	Facebook Authenticator
AWS User Store	JWT
Office365 Provisioning Connector	Token2
Nuxeo	Basecamp
Private Key JWT Client Authenticator	Duo Security
Mutual TLS Client Authenticator	Foursquare
SAML Authenticator	Twitter
CAS	Instagram
SCIM 2.0 Inbound Provisioning Connector	LinkedIn
Mobile Connect	Dropbox
Pinterest Authenticator	Wordpress
FIDO Authenticator	MailChimp
X509	Office365
SCIM Provisioning Connector	MePIN
Salesforce Provisioning Connector	Yammer
SPML Provisioning Connector	Github
Google Provisioning Connector	EmailOTP
Reddit	Bitly
Inwebo	SMSOTP
RSA	TOTP
Amazon	Password Policy

--- END OF DOCUMENT ---

About Silverlake Sheaf

Founded in 2017, the Silverlake Sheaf Group (Sheaf) is a subsidiary of the Silverlake Group of Private Entities (SPE). Headquartered in Singapore, Sheaf specializes in two core business activities:

1) Wholesale of Cyber Security software, hardware and peripheral equipment including development of software in areas of payment, enterprise integration, cyber security; and

2) Information Technology Consulting services related to Cyber Security and Digital Transformation.

Sheaf is headquartered in Singapore, has an office in Malaysia; and representative offices in Thailand, Vietnam and India. Sheaf is an authorized reseller/distributor for Silverlake MasterSAM worldwide. Sheaf offers a spectrum of market-ready solutions ranging from cyber security, payment and enterprise integration. For enquiries, please visit www.silverlakesheaf.com or write to sheaf_sales@silverglobe.com.