INTEGRATING SINGLE SIGN-ON (SSO) WITH SUMMIT V6.2

SUMMIT
TRICKS AND TRAPS

SERIES - 1 / ARTICLE - 4
MAY 25, 2022

By **Ragavendran Ragothaman**

GreenPoint>
Summit

What is Single Sign-On (SSO)?

SSO is a session and user authentication service that permits a user to use a single set of login credentials across multiple applications in an organization.

Challenge cyber-attack through SSO

Advanced authentication can be easily and quickly deployed with SSO framework. Cyberintruders mainly target usernames and passwords, and they have a penetration opportunity every time a user logs in to a new application. Since users generally log in once every day and only use one set of credentials, SSO limits the number of attack surfaces. Enterprise security is enhanced by limiting the login process to one set of credentials.

Cost optimization through SSO

SSO also saves time and aggravation on password resets, lowering IT expenditures. When each program demands a unique login and password for each employee, there is a good risk that they will not recollect them, and support tickets for password resets will pile up. With SSO users only have to remember one set of credentials with SSO, which reduces the frequency of support tickets. Furthermore, most SSO solutions allow users to reset their passwords on their own, eliminating the need for IT intervention.

Introduction of SSO and its features from Summit v6.2

SSO is almost mandatory across financial institutions, and Finastra Summit supports it. Even so, the activation is not quite as seamless as the service it provides. GreenPoint Summit took on the challenge of implementing SSO for Summit at a large global bank, and encountered and resolved the hurdles. Up until Summit v6.1, an institution could implement their own authentication logic as a part of two-factor authentication. The workflow is described below.

› Summit v6.1 front-end passes user login credentials to the eToolkit server for authentication
› When a client customizes the extendable authentication process, the eToolkit server invokes a client-extendable authentication function, which is part of the Security Extendable API. Clients can implement their proprietary authentication logic in this function

From Summit v6.2 onwards, SSO functionality was implemented with the following capabilities:

› Supports for OpenID Connect (OIDC) Authentication workflow
› OIDC is an authentication protocol built on OAuth 2.0 that can be used to securely sign in a user into an application

Multiple challenges were faced while implementing the Azure SSO.

GreenPoint Summit, the Summit speciality services team at GreenPoint Financial, worked on a full upgrade to v6.2. As part of the upgrade project, the Azure SSO was implemented in a client environment.

There is an Azure ID and Summit User ID mismatch…

The first issue encountered was a difference in the way User IDs are used for authentication between Azure and Summit. To begin with, a basic setup of SSO was attempted. This revealed the initial differences between these systems.

› Summit v6.2 uses Azure preferred_username claim for user authentication. This claim represents the user in Azure. It can be an email address, phone number, or a generic username without any specified format. Its value is mutable and subject to change over time. The preferred_username claim was configured in the client Azure environment.

› In a client environment, this preferred_username is set to the email id of the user. However, the Summit login ID is already a specific User ID. This created a mismatch between the User ID returned by Azure and Summit User ID because of which the SSO was unsuccessful.

The next solution that was tried was to enable the SSO authentication through 'sso_mapper'.

The sso_mapper utility is used by the Open ID Connect feature to encrypt information from the input text file and add it to the dmSSOMAP table.

Unfortunately, the length of the generated value could not be stored in the table as the value by sso_mapper was greater than the column length. Therefore, the insertion into the dmSSOMAP table was unsuccessful.

To resolve this issue, an OIDC custom claim 'on_premises_account' was introduced in Summit, with the same being added to the Azure client environment.

This allows clients to add a User ID as the value of this claim. Summit fetches this value in the backend from the decrypted token and uses it to check in dmUSER if the user exists and allows authentication. The mismatch issue between the two systems was resolved using this approach, based on knowledge of Azure and Summit.

Find out about the other challenges encountered by GreenPoint Summit during SSO integration in our next release.

Be sure to check out this space for more interesting summit topics!

GreenPoint> Summit

GreenPoint> Financial

ABOUT
GREENPOINT SUMMIT

> - GreenPoint Summit is a comprehensive platform encompassing new implementations, version and module upgrades, product and application development, test automation, cloud migration, and system maintenance

> - Our quantitative services and platforms include Libor Replacement Simulation Tool (LRST), curve creation, recreation and management, model validation and documentation, and creation of challenger models for regulatory compliance.

> - Our summit professionals also provide data porting, migration and management as well as cloud services.

> - Over the last year we have completed several projects including full system upgrades, Libor/RFR migration, replacement of valuation frameworks, and custom code creation and testing for large global banks and insurers.

ABOUT
GREENPOINT FINANCIAL

> - GreenPoint Financial is a division of GreenPoint Global, which provides software-enabled services, content, process and technology services, to financial institutions and related industry segments.

> - GreenPoint is partnering with Finastra across multiple technology and services platforms.

> - Founded in 2006, GreenPoint has grown to over 500 employees with a global footprint. Our production and management teams are in the US, India, and Israel with access to subject matter experts.

> - GreenPoint has a stable client base that ranges from small and medium-sized organizations to Fortune 1000 companies worldwide. We serve our clients through our deep resource pool of subject matter experts and process specialists across several domains.

> - As an ISO certified company by TÜV Nord, GreenPoint rigorously complies with ISO 9001:2015, ISO 27001:2013, and ISO 27701:2019 standards.

Product Implementation and Upgrade

Curve Construction and Management

Portfolio Archiving and Cloud Services

Valuation Model Validation and Documentation

GreenPoint> Summit

Support Services

Product Development

Test Automation Tool

Managed Services

Sanjay Sharma, PhD
FOUNDER AND CHAIRMAN

Sanjay provides strategic and tactical guidance to GreenPoint senior management and serves as client ombudsman. His career in the financial services industry spans three decades during which he has held investment banking and C-level risk management positions at Royal Bank of Canada (RBC) Goldman Sachs, Merrill Lynch, Citigroup, Moody's, and Natixis. Sanjay is the author of "Risk Transparency" (Risk Books, 2013), Data Privacy and GDPR Handbook (Wiley, 2019), and co-author of "The Fundamental Review of Trading Book (or FRTB) - Impact and Implementation" (Risk Books, 2018).

Sanjay was the Founding Director of the RBC/Hass Fellowship Program at the University of California at Berkeley and has served as an advisor and a member of the Board of Directors of UPS Capital (a Division of UPS). He has also served on the Global Board of Directors for Professional Risk International Association (PRMIA).

Sanjay holds a PhD in Finance and International Business from New York University and an MBA from the Wharton School of Business and has undergraduate degrees in Physics and Marine Engineering. As well as being a regular speaker at conferences, Sanjay actively teaches postgraduate level courses in business and quantitative finance at EDHEC (NICE, France), Fordham, and Columbia Universities.

Ragavendran Ragothaman
TECHNICAL MANAGER

Ragavendran has over 15 years of experience across various derivatives trading systems. He has worked in trading systems such as Summit, Sophis Risqué, and Murex. He has extensively worked on Interest Rate and Equity Derivatives and Fixed Income Products, mainly as a Techno Functional Expert. He has been responsible for customizing and extending the functionality of Summit and Sophis products. Ragavendran has developed the business-critical utilities, reports and feeds for front and back offices. He has also supported Summit business users across different geographical locations (UK, USA, Europe, and Singapore). Ragavendran has expertise in Summit upgrade projects which involves upgrading to Summit v6.2 from lower versions of Summit. He has sound knowledge in setting up and configuration of Summit Insight. He has expertise in setting up client environment in the Finastra servers. Ragavendran has earlier worked in Cognizant, Infosys, TCS, and HCL Technologies.

Ragavendran holds a BTech in Information Technology from Anna University. He holds Python certifications and is currently pursuing Data Science related certifications.

He is an ardent carom board player and has played inter-college tournaments during his graduation days. He also loves playing the Mridangam.

Ragavendran lives with his family in Chennai, India.

Marcus Cree
MANAGING DIRECTOR AND CO-HEAD

Mothiram K
DELIVERY HEAD - TCM

Maraimani Chakkaravarthy
DELIVERY HEAD - GREENPOINT SUMMIT

Yu Dai
SENIOR QUANTITATIVE MANAGER