FINASTRA

Global PAYplus

Security

Business Guide

Product Version: 4.5
Catalog ID: GPP4.5-00-B45-02-201511

Copyright

Disclaimer

Finastra does not guarantee that any information contained herein is and will remain accurate or that use of the information will ensure correct and faultless operation of the relevant software, services or equipment. This document contains information proprietary to Finastra. Finastra does not undertake mathematical research but only applies mathematical models recognized within the financial industry. Finastra does not guarantee the intrinsic theoretical validity of the calculation models used.

Finastra, its agents, and employees shall not be held liable to or through any user for any loss or damage whatsoever resulting from reliance on the information contained herein or related thereto. The information contained in this document and the general guidance of Finastra staff does not take the place of qualified compliance personnel or legal counsel within your institution.

FINASTRA CANNOT RENDER LEGAL, ACCOUNTING OR OTHER PROFESSIONAL SERVICES TO YOUR INSTITUTION. THE INFORMATION CONTAINED HEREIN IS GENERAL IN NATURE AND DOES NOT CONSTITUTE LEGAL ADVICE OR A LEGAL OPINION. CONSULT YOUR LEGAL COUNSEL FOR LEGAL ADVICE SPECIFIC TO YOUR SITUATION OR CIRCUMSTANCES OR TO ANSWER ANY LEGAL QUESTIONS.

This document is not intended as a substitute for formal education in the regulatory requirements of banking, banking operations, lending, lending operations, or other topics generally applicable to financial institutions. Your financial institution is solely responsible for configuring and using the software or services in a way that meets policies, practices, and laws applicable to your institution, including, without limitation: (1) options and selections made on prompts; (2) entries in the software program; (3) program setup; and (4) documents produced by the software or services. It is the obligation of the customer to ensure that responsible decisions are taken when using Finastra products. Information in this document is subject to change without notice and does not represent a commitment on the part of Finastra.

Feedback

Do you have comments about our guides and online help? Please address any comments and questions to your local Finastra representative.
Need more information? Read more about our products at http://www.finastra.com or contact your local Finastra office at http://www.finastra.com/contact.

Version Control

Version	Date	Summary of Changes
1.0	August 2015	Document created
2.0	November 2015	Updated for Rebranding
3.0	September 2018	Document rebranded to Finastra.

Table of Contents

1 Introduction

Note: This Business Guide has not yet been certified for GPP V4.5; therefore, there may be inaccuracies in this document that may require amendments in the future. For more information, please contact your D+H Project Manager.

Global PAYplus (GPP) uses integrated security and access control procedures and a mechanism, which are designed to guarantee the integrity and confidentiality of application data and limit access to the application to authorized users.

At this stage this Business Guide includes only information related to Single Sign On (SSO).

1.1 Target Audience

This business guide is intended for system administrators, IT personnel, and GPP users who need to know about security within GPP.

2 Single Sign On (SSO)

2.1 Overview

Single Sign On (SSO) is a user authentication process that permits a user to enter one name and password to access multiple applications. It allows users to be authenticated only once with no further authentications required when accessing any applications protected in the same security federation.

GPP supports the use of SSO authentication using a combination of GPP system parameters, WebSphere configuration, and the use of a GPP URL designed for use with SSO.

When using the SSO mode, two approaches are supported:

- The external authentication system supplies both a valid GPP user ID and a valid GPP role (which is defined as the user's role in GPP). The user is allowed to login to GPP using SSO.
- An external authentication system supplies the user ID and role information which are not found in GPP. In this case, GPP determines if the unknown user is allowed to login to GPP according to the server configuration. When the unknown user is allowed to login to GPP, GPP creates the user based on the predefined user and entitlement templates to login to GPP using SSO.

SSO in a nutshell:

- User ID and User role are provided to GPP in the http header fields, or the principal object is provided in the request from an external authentication system.
- When an unknown user logs in to GPP, the new user is created with the office predefined in the Entitlement profile.
- Unknown user creation is supported when the financial institution creates an Entitlement profile.
- Financial institution creates a default Entitlement profile. In this case an unknown user is created using the default Entitlement profile.
- Financial institution is responsible to create and maintain the GPP User and Entitlement profiles.

2.2 Processing

When GPP uses SSO it needs to be configured for SSO login mode. GPP can be configured to accept both User ID's that exist and do not exist in the GPP database. For more information, see Server Configuration.

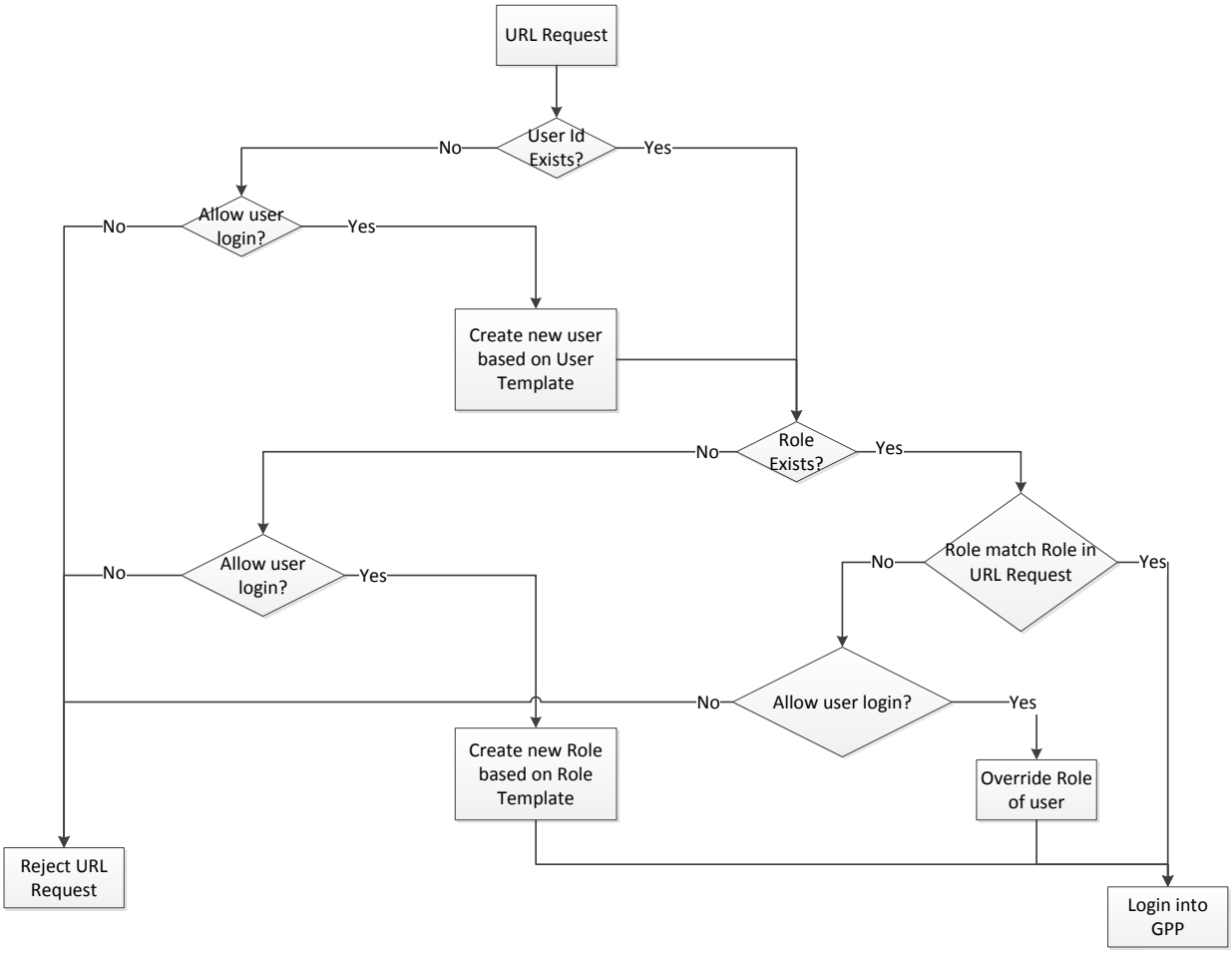
When the user navigates to the login page, GPP receives the authentication information from the http header fields, or the principal object from an authentication system configured as a reverse proxy to GPP.

There are two methods for GPP to identify the User ID. The financial institution determines which method they will use for SSO.

- By Java Authentication and Authorization Service (JAAS) principal object. The user name is obtained from the principal object and GPP checks that the user has the required existing GPP entitlements. For more information, see GPP Online Help, Entitlement Classes.
- HTTP request headers. GPP receives the user name and the user role as values of the HTTP request headers. GPP determines whether the User ID exists in the GPP database.

Note: For both methods the workflow is the same.

2.2.1 SSO Workflow



2.2.2 URL Request

When a user accesses the path to the GPP environment, a request on behalf of the user is sent to the financial institution's server.

Any communication error is handled by the financial institution. If the URL is not available then an error defined by the financial institution is displayed.

2.2.3 User ID Exists

When the URL is opened, the GPP Login page is displayed and the user is prompted to enter their User ID and Password.

GPP determines whether the user exists in the GPP database.

- If the user is found, GPP continues with the process and checks if the role exists.
- If the user is not found, GPP checks the Server Configuration option and determines whether the unknown user is allowed to login to GPP.
  - When the user is allowed:
    - GPP creates a new user based on the User template
    - GPP continues with the process and checks if the role exists
  - When the user is not allowed:
    - GPP rejects URL request and the user is not allowed to login to GPP
    - GPP prompts a failed login message

2.2.4 Role Exists

GPP determines whether the user role exists in the GPP database.

- When the user role is found, GPP continues with the process and matches the user role with the user entitlement in the GPP database.
- When the user role is not found, GPP checks the Server Configuration option and determines whether the unknown role is allowed to login to GPP.
  - When a role is allowed:
    - GPP creates a new role based on the Role template
    - GPP authorizes the user login
  - When a role is not allowed:
    - GPP rejects URL request and the user is not allowed to login to GPP
    - GPP prompts a failed login message

2.2.5 Match Role in URL Request

GPP determines whether the user role matches the user entitlement in the GPP database.

- When the user role matches the user entitlement, GPP authorizes the user login.
- When the user role does not match the user entitlement, GPP checks the Server Configuration option and determines whether the user is allowed to login to GPP.
  - When a user is allowed:
    - GPP updates the user record with a new role
    - GPP authorizes the user login
  - When a user is not allowed:
    - GPP rejects URL request and the user is not allowed to login to GPP
    - GPP prompts a failed login message

2.2.6 Login to GPP

When a user is authorized to login to GPP, the main GPP page is displayed.

2.2.7 LDAP Authentication Over SSO

In addition to the SSO process, GPP also supports LDAP Authentication Over SSO. A financial institution can use SSO with LDAP, in order to authenticate the User.

When GPP is configured for the LDAP Authentication Over SSO mode, the user navigates to the SSO login page to enter GPP. In this mode, the SSO login page expects authentication information (user name and password) to be supplied in the http header fields from LDAP. The server then logs on to

the LDAP server on behalf of the user by providing the LDAP server with the user's ID and password. If successful, the security server then proceeds with any authorization procedure and/or lets the user proceed to GPP.

2.3 System Configuration and Business Setup

2.3.1 Business Setup

2.3.1.1 System Parameters

System Parameter	Description
WEBLOGMODE	Specifies the WEB login mode according to which authentication is done. Possible options: • INTEGRATED - User authentication is done via GPP; all users are managed through the USERS table. In this mode, User profiles can be created and edited. • SSO - User authentication is done via an outside application, (e.g. WebSEAL), where the USERS table is used only for storing the users that use the application in order to display the list of logged in users in the Users profile. In this mode, User profiles cannot be created and edited. Note: If the value is not one of the above values, GPP assumes the value to be INTEGRATED.
IV_USER	Specifies the name of the mandatory header field that contains the user ID when operating in SSO mode. This header field must be present in the login request, and its associated value must be a valid GPP user.
IV_CREDS	Specifies the name of the optional header field that contains the user's GPP role. If this field is not present, GPP determines the user's role. If this header field is present, its value must be a valid GPP role (an entitlement name, in GPP terminology). Use of this optional header field is useful to control privileges from the authentication server.
SSO_USER_PROVISIONING	Specifies whether user authorization by an external SSO service and not defined in the internal GPP repository can be created. • Yes - Unknown user request is created using predefined default template and the user logs in to GPP. • No - Unknown user request is rejected. Note: If the value is not one of the above values, GPP assumes it is No.

2.3.1.2 Profiles

These are the details of the setup in GPP profiles that are related to SSO. For more information, see GPP Online Help.

- System Users Profile: Create a user with the **User ID** name TEMPLATE
- Roles Profile: Create a role with the **User Entitlement Profile** name TEMPLATE

2.3.2 Server Configuration

If the user does not exist in the database, GPP determines whether the unknown user is allowed to login to GPP, based on the server configuration.

To allow a user to use SSO, when they do not exist in the GPP database:

1. Set the WEBLOGMODE system parameter with the value SSO.

   The user authentication is done via an outside application, where the Users table is used only for storing the users that use the application in order to display the list of logged in users in the Users profile. In this mode, User profiles cannot be created and edited.

2. Set the IV_USER system parameter to the value of the HTTP request header that contains the User name.

   Note: This step is not relevant if using the JAAS method. For more information, see Processing.

3. Set the IV_CREDS system parameter to the value of the HTTP request header that contains the User role.

   Note: This step is not relevant if using the JAAS method. For more information, see Processing.

4. Set the SSO_USER_PROVISIONING system parameter to Yes. The default value is No.

   - Yes - Unknown user request is created using predefined default template and the user logs in to GPP.

2.3.3 WebSphere Configuration to Support SSO

When the authentication system uses an agent to protect the site, the agent setup takes care of intercepting the login requests and sending them to the authentication system. When the authentication system does not include an agent, it is required to perform WebSphere configuration to intercept login requests and send them to the authentication system.

Appendix A: Glossary

Term	Description
SSO	Single Sign On
JAAS	Java Authentication and Authorization Service
URL	Uniform Resource Locator
LDAP	Lightweight Directory Access Protocol

Registered in England & Wales
No. 01360027

Registered Office
One Kingdom Street Paddington
London W2 6BD