

SUPPORT CONNECT KNOWLEDGE SERIES

Augment Your Problem-solving Capability

JULY | EDITION 127



Welcome to the Finacle Global Support fortnightly knowledge bulletin! We're here to offer solutions for common challenges, share valuable tips, provide knowledge bytes, and keep you updated. Each edition is meticulously curated to ensure we share best practices and known resolutions. In this issue, you'll find the following articles:

- **Significance of COHTTP Timeout Parameters**
- **Password Policy**

So, let's start reading!

Significance of COHTTP Timeout Parameters

Product: Finacle Core Banking | Version: 10.2.25 (part of DA module) and above

COHTTP service handles the client requests over the **HTTP** protocol and accesses all services (**SRVs**) like APIs for executing business transactions. The payloads are generally in **JSON** or other supported formats.

To ensure efficient request handling and prevent issues such as database deadlocks or client-side timeouts, two critical timeout parameters are available:

1. **COHTTP_TIMEOUT_MS**: This parameter defines the maximum allowable time (in milliseconds) for a transaction to be completed. If the processing time exceeds this limit, the system will not commit the transaction. Using **COHTTP_TIMEOUT_MS** helps prevent scenarios where the channel or client times out while the service continues processing in the background.
2. **COHTTP_SIGALARM_LIMIT**: This parameter sets a hard timeout (in milliseconds) for request processing. If the request is not completed within this limit, the process is forcibly terminated. The service then initiates a new process to handle subsequent requests.

These parameters must be configured such that **COHTTP_SIGALARM_LIMIT** is set slightly higher than **COHTTP_TIMEOUT_MS**. This ensures the system has sufficient time to gracefully handle timeout conditions and respond appropriately before forcibly terminating the request process. It prevents scenarios where the channel or client times out while the service continues processing in the background.

Password Policy

Product: Finacle Online Banking | Version: 11.x and DEH

Password policy defines the guidelines that users should follow while creating a password for the application. The Online Banking application has the following configuration options that can be maintained by the bank admin in **PRPM**:

- **PRPM** configuration can be created or updated from the navigation below in the admin application

General Administration: [Property Manager](#) > Property Manager Maintenance

PROPERTY MANAGER MAINTENANCE Create New

Search Criteria

Bank ID: 024

Property Name:

Property Description:

Search Clear

- After create or update of password property configuration, run **CommonCodeCache** and restart services

Configuration Options:

- The application enables two passwords for a user: the sign-on password and the transaction password. The application forces you to change the sign-on and transaction passwords at first instance.
- To allow the same password for sign-on and transaction
 - **SIGNON_TXN_PWD_SAME_FLAG**: Set the value as
 - Y – if both Sign on and Transaction passwords must be the same
 - N – if Sign On and Transaction passwords must be different
- The password should comprise special characters
 - **SPWD_PWD_SPECIAL_CHARSET**: Special characters to be included in sign-on password
 - **TPWD_PWD_SPECIAL_CHARSET**: Special characters to be included in the transaction password
- The length of the password should be a minimum of six characters and a maximum of 20 characters.
 - **SPWD_MAX_LENGTH_OF_PASSWORD**: Maximum length of sign-on password
 - **TPWD_MAX_LENGTH_OF_PASSWORD**: Maximum length of transaction password
 - **TPWD_MIN_LENGTH_OF_PASSWORD**: Minimum length of transaction password
 - **SPWD_MIN_LENGTH_OF_PASSWORD**: Minimum length of sign-on password
- The password should contain at least four distinct characters
 - **SPWD_PWDFOURCHARMAND**: Four characters mandatory in sign-on password
 - **TPWD_PWDFOURCHARMAND**: Four mandatory characters in transaction password
 - **SPWD_PWDALPHAMAND**: Whether alphabet is mandatory in the sign-on password
 - **TPWD_PWDALPHAMAND**: Whether alphabet is mandatory in transaction password
 - **SPWD_PWDDIGITMAND**: Whether digit is mandatory in the sign-on password
 - **TPWD_PWDDIGITMAND**: Whether digit is mandatory in transaction password
 - **SPWD_PWD_SPECIAL_CHAR_MANDATORY**: Special character is mandatory in sign-on password
 - **TPWD_PWD_SPECIAL_CHAR_MANDATORY**: Special character is mandatory in transaction password
- The duration after which the password expires can be configured by the bank. One grace log-on is allowed after the password expires. In such a situation, the Change Password screen is displayed immediately after you log on
 - **PWD_EXPIRY_PERIOD**: The Corporate/ Retail user password expires in these many days
 - **TXN_PWD_EXPIRY_PERIOD**: Transaction Password expires in these many number of days for the Retail or Corporate User
- The application allows you to enforce a password history, i.e., it displays an error message if the user the previously used passwords as per **DEFAULT_MAX_PWD_HISTORY_ALLOWED** value
 - **DEFAULT_MAX_PWD_HISTORY_ALLOWED**: Maximum Password history allowed

The revamped Finacle Support Center is now accessible through these URLs. Bookmark them for easy access and login!

- **Customer Access and Login:** <https://support.finacle.com>
- **Finacle Knowledge Center:** <https://docs.finacle.com/en/signin>

What would like to learn about?
Write to us:
finaclesupport@edgeverve.com



Better Inspires Better
www.finacle.com