

SUPPORT CONNECT KNOWLEDGE SERIES

Augment Your Problem-solving Capability

JULY | EDITION 149



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:

- **Asynchronous Balance Update for Customer Accounts**
- **Improper Cookie Path Attribute Configuration in FEBA Application**

So, let's start reading!

Asynchronous Balance Update for Customer Accounts

Product: Finacle Core Banking | Version: 10.2.25 and 11.13 onwards

In the conventional transaction flow, customer accounts are locked for a temporary period to perform validations and posting activities such as balance updates, lien or limit adjustments, and TOD processing. Consequently, transactions on the same account are processed sequentially, which can impact throughput in high-volume scenarios.

By minimizing processing within the lock window, **Asynchronous Balance Update** enhances transaction concurrency and performance.

A Detailed Explanation of How Functionality Works:

1. Debit Transactions:

For debit transactions, the system locks the account only for essential balance validation and releases it quickly after the required checks are completed. If sufficient balance is available, the amount is temporarily reserved in **BFT**, and the transaction is recorded in **CTGAM** instead of being synchronously updated in **GAM**.

The transaction is committed in the usual manner, and the balance becomes effective immediately after posting. Queued transactions are considered in the available balance to prevent excess debit, while the final update to **GAM** happens asynchronously. By end of day, there is no visible difference compared to the conventional synchronized flow.

2. Credit Transactions:

For credit transactions, the validated transaction is recorded in **CTGAM** and committed immediately, with the update to **GAM** completed asynchronously. During this period, queued credits are included in the available balance, allowing debit transactions to be honored appropriately. Balance and transaction details remain consistent throughout processing.

3. Eligible Accounts:

This feature is applicable to **SBA, ODA, CCA, and CAA** accounts that are expected to handle high volumes of concurrent debit and credit transactions. It is best suited for accounts with frequent concurrent activity and relatively fewer clearing, future-dated, TOD, or lien-related transactions.

This feature is **not recommended** for accounts linked to **balance-sharing (SWEEPS) pools** or accounts attached with **limits**.

Configuration Setup:

To enable the feature:

- 1. Update **GAM.ASYNCH_BAL_UPD_FLG** to:
 - **D** – enable asynchronous processing for both debit and credit transactions
 - **C** – enable asynchronous processing for credit transactions only
- 2. Create an entry in **ASACCT**.
- 3. Configure the required fund-blocking mechanism based on the deployment model:
 - **BALSER service** for non-docker environments
 - **HTTP route** for docker environments

Key Processing Tables

- **CTGAM** – stores asynchronous customer transaction entries
- **BFT** – temporarily stores blocked funds until posting is completed
- **BFFT** – records failures during blocked fund movement

Movement from **CTGAM to GAM** is carried out through **babx7703** exe.

For additional information or implementation guidance, please connect with the Support Team.

Improper Cookie Path Attribute Configuration in FEBA Application
Product: Finacle Online Banking | Version: 11.0.x, 11.2.x & 11.5

Session cookies generated in HTTP responses are scoped to the root path ("/"). Configuring cookies with the root path makes them accessible across the entire application, including unintended or less-trusted endpoints. This overly broad scope increases the application’s attack surface and may lead to unauthorized access to sensitive session information, thereby increasing the risk of session hijacking, privilege escalation, and other session-based attacks.

Recommendation:

The following corrective actions should be implemented to remediate the issue.
Note : A WebSphere Application Server (WAS) restart is required for the changes to take effect.

1. Server-Level Configuration

- 1. Log in to the **WebSphere Administrative Console**

- 2. Navigate to:
Servers → Server Types → WebSphere Application Servers → {Server Name} → Session Management
- 3. Click **Enable Cookies**
- 4. Ensure that the following options are enabled:
 - **Restrict cookies to HTTPS sessions**
 - **Set session cookies to HTTPOnly to help prevent cross-site scripting attacks**
- 5. Under the **Cookie Path** section, select the **"Use the context root"** radio button instead of **"Set cookie path"**
- 6. Click **Apply → Save**
- 7. In a clustered environment, repeat the above steps for **all servers and cluster members**

2. Application-Level (EAR/WAR) Configuration:

If the **"Override session management"** option is enabled for any application under the below navigation, the same secure settings mentioned above must be applied at the application level.

- 1. In the **WebSphere Administrative Console**, navigate to:
Applications → WebSphere Enterprise Applications → {Application Name}
- 2. Under **Web Module Properties**, click **Session Management**
- 3. Check whether the **"Override session management"** checkbox is enabled

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