



Happy New Year

2021

From all of us at Finacle Support, we wish you all a very happy and prosperous New Year 2021! May this new year bring peace, harmony, and success in each of your endeavors.

Finacle Support brings you this fortnightly knowledge bulletin to augment your problem-solving capability. There is more to it. Every edition is put together with utmost diligence to ensure that best practices and known resolutions are shared. In this edition you will find the following articles:

- **PRPM Parameter to Prevent Phishing**
- **Penalty Calculation in Top-Up Deposits**
- **Masking Sensitive Data in FI Logs**
- **Webinar Announcement: Audit Framework in FEBA**

So let's start reading!



PRPM Parameter to Prevent Phishing

Product: Finacle Online Banking Version: 11.x onwards

SITE_TO_USER_ENABLED is a security feature provided in Finacle Online Banking. Banks may implement this feature to ensure that bank website users are accessing a genuine site, and not any phishing or fake website, before entering their secret code or password.

Functionality & Features

Once the PRPM parameter **SITE_TO_USER_ENABLED** is set as **Y**, users are prompted to enter only the **User ID** in the first screen and in the subsequent screen, i.e. the **Password** screen, a preselected image and phrase will be shown. Users must confirm the phrase and the image

along with the password for logging in to the application. This way, the users can be sure that they are accessing the authentic bank site instead of a phishing site

- By default, the image and phrase-configuration is present in the **data/Bankaway.properties** file:
 - **DEFAULT_PERSONAL_PHRASE=Welcome**
 - **DEFAULT_PERSONAL_IMAGE=SITE_TO_USER_IMAGE_0**
- A set of images are configured in the **data/CMSLookup.xml** file by the admin user
- The user can set or update their image from the pre-configured images and phrase details once they have logged in to the online banking application through **Security Settings** → **Update Image/Phrase Details**. Image details will be updated in column **IMAGE_ID** of the **IUSR** table
- Cache Refresh should be carried out after the **PRPM** change for the changes to take effect

Penalty Calculation in Top-Up Deposits

Product: Finacle Core Banking Version: 10.x onwards

A penalty is applicable in Top-up deposits when the customer misses to pay installments. The penalty calculation in Top-up deposit accounts is based on the **HTUGSPM** setup for TUA scheme type. Unlike TD accounts, TU accounts can apply a penalty, based on the number of days, months, or missed installments.

Under the **HTUGSPM** (Scheme tab → **Penalty** parameters), the penalty parameters are



defined as- **Penalty Charge Code**, **Penalty Based On**, and **Penalty Placeholder**. The penalty to be applied can be based on the number of days, months, or installments.

- a. If the **Penalty Based On** field is set as **No. of Months**, then the delay is calculated as the number of months for which it got delayed
 - If the number of months is less than 0, then the delay is 0
 - If the number of months is more than 0, then the number of complete months + 1 (if days > = 1)
 - b. If the **Penalty Based On** field is set as **No. of Days** then the delay is calculated as number of days the installment got delayed
 - c. If the **Penalty Based On** field is set as **No. of Installments**, then the delay is calculated with the missed number of installments
- Once the delay is calculated then the penalty amount is calculated as: (**Installment Amount * Delay * Percentage** as mentioned in HPTTM).



Masking Sensitive Data in FI Logs

Product: Finacle Core Banking Version: 10.2.16 onwards

The parameter **LOG_FILTER_ENABLED** and **DISABLE_PATTERN** is introduced in **FIMASTER.FI_CONFIG_DATA** to mask the sensitive data while recording the debug statements into log files located in the FI layer.

This parameter is mandatory for **FI SSO Real User Login** APIs, where the **User ID** and the password tag values are displayed as such in the **FI** logs leading to the data exposed to anyone viewing the logs.

To avoid it, the **LOG_FILTER_ENABLED** parameter value should be set to **Y**, and the pattern configured to mask the particular tag value with its name under the parameter **DISABLE_PATTERN**. The **DISABLE_PATTERN** can be configured for an individual API, based on the service request ID value as below.

BankInq={<Name>.*</Name>}, FISSOLogin={<pwd>.*</pwd>}

If the **DISABLE_PATTERN** parameter is set as above, then it will mask the entire nametag along with its value in FI logs for BankInq API and the password tag, along with its value in FISSOLogin API.

Multiple tags of the same service request can be configured with a comma separator inside the braces “{}”, Similarly, multiple service requests can be configured with a comma separator outside the braces “{ }”.

The **DISABLE_PATTERN** parameter can also be configured for all APIs for a particular tag name as below:

All={<Name>.*</Name>}

Webinar Announcement: Audit Framework in FEBA

Finacle Online Banking Support team is hosting a webinar on **Audit Framework in FEBA**. The session will give an insight to the setup and features of Audit in FEBA. Commonly faced problems and solutions will also be discussed. You can also mention any specific areas related to Audit Module that you would like us to cover in the upcoming session.

Click [here](#) to register today!

Date: Thursday, January 7, 2021

Time: 3:00 PM to 4:00 PM IST

Hope you like this edition. Is there anything that you'd like to see in the forthcoming series? We'd love to hear from you!

Write to us at finaclesupport@edgeverve.com