FSBOA – IMS Security Level Access Request (Permanent) for Cloud Support/Operations Employee(s) or Contractor(s)

1. Overview

This document outlines steps on how to submit a "FSBOA – IMS Security Level Access Request" in the Softlayer Internal Portal (IMS Commercial). FSBOA Access is granted with proper justification and approvals.

The FSBOA flag in IMS can *'only'* be requested for Employee(s)/Contractor(s) within Hamilton Countries of Executions (CoEs) or with approved PCE

> **Australia, Canada, France, Germany, India, Ireland, Israel, Italy, Netherlands, Singapore, Switzerland, South Africa, United Kingdom, United States and Japan**

2. Prerequisites

- FSBOA access request in IMS can *only* be requested by the following individuals who have appropriate permissions to submit the request:

  Manager(s) of employee(s)/Contractor(s)

  OR

  'Proxy Manager(s) within respective group – IaaS, PaaS, Support and SOC'

  Note: See the next section for information on how to determine whether you have permissions to submit a request.
- You must already have a SoftLayer account (i.e., a SoftLayer Active Directory userid).
- You need to be able to VPN into SoftLayer using Global Protect VPN (GP VPN) and Yubikey

3. Verifying You Have Permissions to Submit an Access Request

1. Log into the Softlayer Internal Portal.
2. After you are logged in, click **username** in the top left-hand corner, under user information.

3. When the employee information page loads, click the **View Employee Permissions** link.

4. Under the "Employee permission" page, click the Actions tab, and look for the following permission:

   SECURITY_LEVEL_REQUEST_PERMANENT_ACCESS_OTHERS

If you see this permission under your username, you should be able to submit FSBOA access requests for your employees.

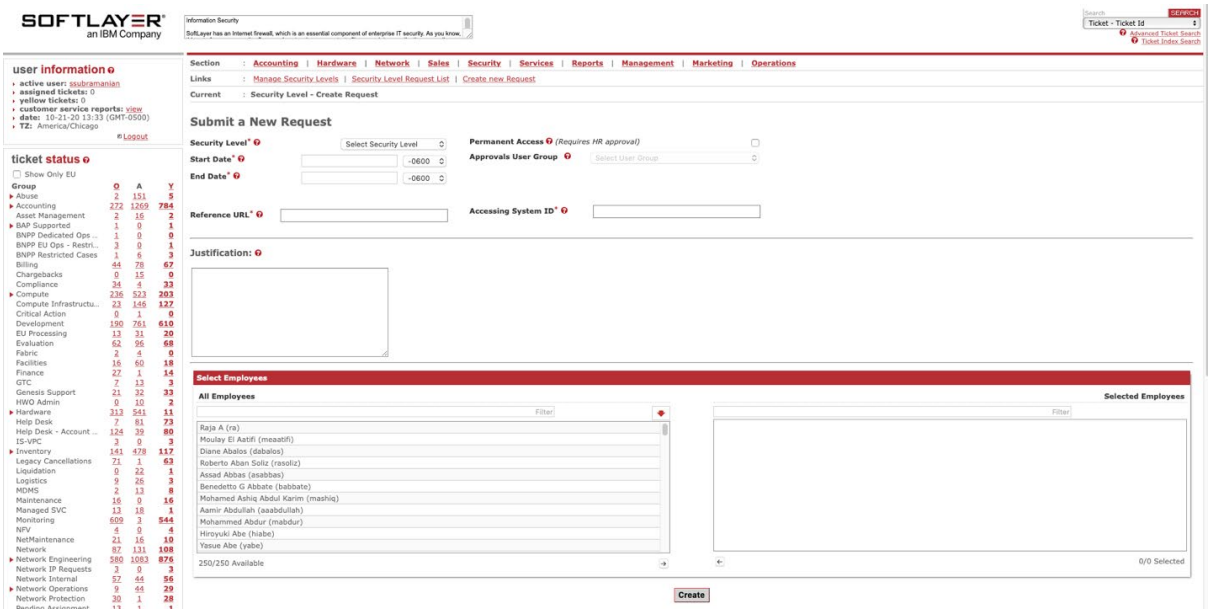
4. Use Case Process Workflow

Use Case	Step #1	Step #2
Manager with security level permissions	Go to Section 5: How-To Request FSBOA Access.	N/A
Manager without security level permissions	Go to Section 6: Manager emails 'Proxy Requestor'.	Go to Section 7: How to Request Necessary Permissions.

5. How-To Request FSBOA Access

Functional/First-Line Manager can "*only*" submit the FSBOA Permanent Access request.

1. Go to the [CreateRequest page] in the Softlayer Internal Portal.

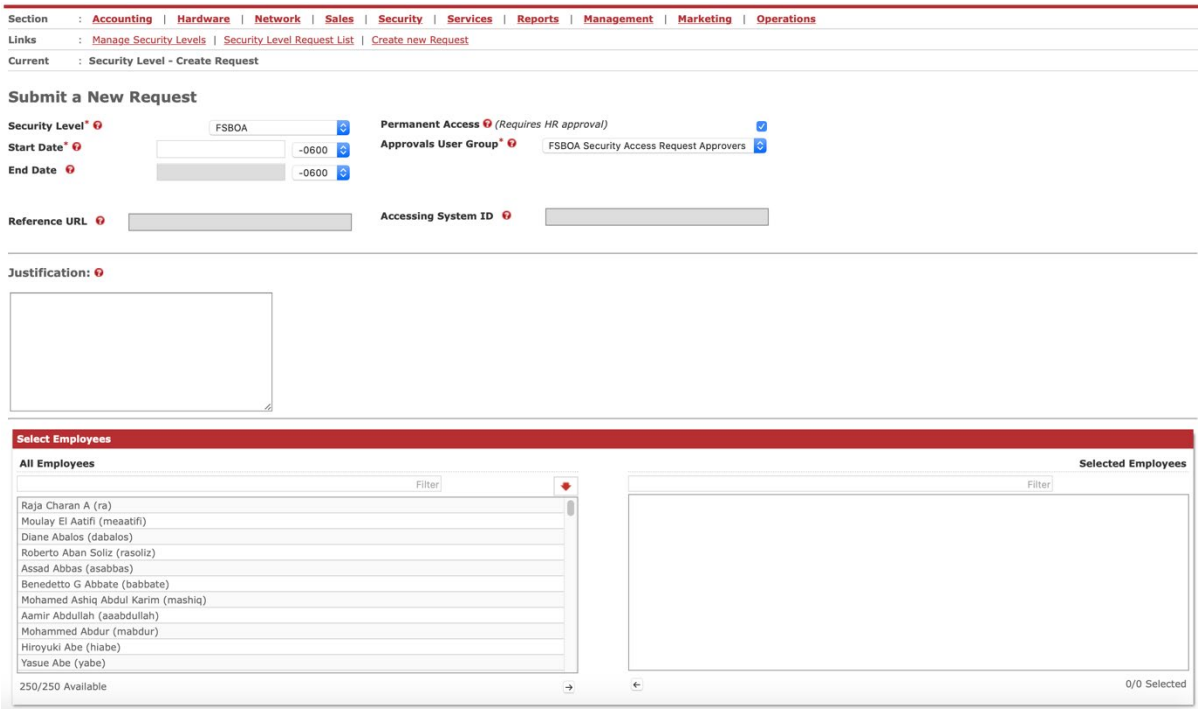


2. Provide the following information:
    - Security Level: FSBOA
    - **Start Date/End Date**: This is not applicable to FSBOA. Check the Permanent check box
    - **Approval User group**: FSBOA Security Access Request Approvers
    - **Accessing System ID**: Not applicable for Permanent request
    - **Reference URL**: Not applicable for Permanent request
    - **Justification**: Line Manager's to follow the guideline for Countries of Executions restrictions (see link below) – Go to section highlighted below in the link and follow the steps provided for justification.

"Verbiage to be used for FSBOA IMS, ServiceNow & AccessHub Requests for in-scope services"

https://pages.github.ibm.com/ibmcloud/Security/BoA/BoA-Access-Control-COE.html#verbiage-to-be-used-for-fsboa-ims-servicenow--accesshub-requests-for-in-scope-services

3. **Select Employee:** Type in atleast part of the employee name to search for an employee. Select the name of correct employee (in the 'filter' box) that need access by clicking on the name, and use the arrows to move their names to the right.



4. Click the **Create** button. An email is generated for each employee for which access was requested.
5. Once the request is submitted, the approval or rejection may take up to 2-3 business days. Notification will be sent to your email.

6. Manager Emails to ‘Proxy Requestor’

The Proxy Requestor is the Manager who is active in IMS with adequate permissions to submit security level access requests.

Managers who need to submit a request for IMS FSBOA permission for one of their team members and who themselves are not already in IMS system will:

1. Select one of the proxy requestors listed for their org (see designated proxy requestors below)
2. Email their formal request for user FSBOA permission (using the specified manager attestation template already documented) to the selected proxy requestor

"Verbiage to be used for FSBOA IMS, ServiceNow & AccessHub Requests for in-scope services

In the following examples, the verbiage in ***bold italics*** must be replaced with proper information in order for a valid request to be submitted and approved

Citizens in Approved Countries

"I am requesting access for ***Jane Doe*** that will give this person access to Bank of America client data for the purposes of ***[insert purpose for access, i.e., specific job function]***. I confirm that Jane Doe works in ***[insert name of country]***, which is an approved country for Bank of America"

Non-Citizens in Approved Countries

"I am requesting access for ***Jane Doe*** that will give this person access to Bank of America client data for the purposes of ***[insert purpose for access, i.e., specific job function]***. I confirm that Jane Doe has provided proof of identity and has all required permissions/certifications and related paperwork to work in ***[insert name of country]***, which is an approved country for Bank of America."

Access Being Requested Under an Approved Public Cloud Security Exception (PCE)

"I am requesting access for ***Jane Doe*** that will give this person access to Bank of America client data for the purposes of ***[insert purpose for access, i.e., specific job function]***. I confirm that Jane Doe does not reside an approved country for Bank of America but that they are covered under approved Public Cloud Security Exception ***[PCE-XXX-999999]***, located at ***[INSERT PCE GITHUB URL]***."

3. The Proxy Requestor will submit in IMS that request using the managers attestation email (including date/time) supplied in the previous step.
4. The Proxy Requestor will provide the request ID # back to manager
5. The Proxy Requestor will receive an email with request outcome and relay back to the manager.

Designated "Proxy Requestors" based on Group

IaaS	**PaaS**	**Support**	**SOC**
Ken Cooper Ken.Cooper@ibm.com	Brian Countryman - brianjc@us.ibm.com	Todd Burns burnsto@us.ibm.com	Jake Gordy jake.gordy@ibm.com
John Eaves eavesj@us.ibm.com		Bobby Burrow bburrow@us.ibm.com	Jason Riggs jriggs@us.ibm.com

7. How to Request Necessary Permissions (for Security Level Access Request) in IMS

Your IMS account needs to be in “active” state to follow the steps below. If your role in IMS is a “Manager” or any other role, but don’t have the necessary permission SECURITY_LEVEL_REQUEST_PERMANENT_ACCESS_OTHERS:

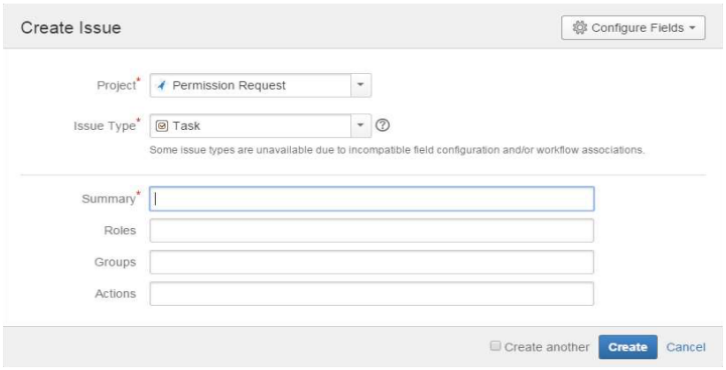
1. Open a PERMREQ ticket for compliance team (per instructions attached from Compliance).

Request Permission Addition/Changes

Changes to permissions (new role, new action, or changed action) require two levels of manager approval and confirmation by compliance.

Note: Permission requests cannot span multiple departments. Each department will need it's own set of manager approvals

The request should be initiated by someone at managerial level or above by opening a new JIRA issue under the Permission Request project:



Summary is a short explanation of the request, ex: "Add Contract Management permission to members of the NOC group"

Roles is the roles or role to add the permission to. Your role should generally correspond to your title. If you are unsure about what the name of the role is, just put the names of the people you wish the permission to be added to.

Groups is optional, if you know what permission group that is part of the roles the permission is being added to, put it here. Otherwise just leave it blank.

Actions is the specific permissions to be added. The easiest way to find out the name of the permission is just to try to go to the page and you will be presented with an error message detailing the action keyname (will be in all caps separated by underscores)

Example:

https://jira.softlayer.local/browse/PERMREQ-1199 (for requesting permissions added to your existing role OR add a new role) - Handled by Compliance team

Once a new role created, the user needs to create helpdesk ticket (IMS ticket, for example -https://internal.softlayer.com/Ticket/ticketEdit/126249896)

8. How to Retrieve Users with Security Level Requests in Your Team

From the GetRequests page in the Softlayer Internal Portal, you can revoke/remove/close security level permission for your associates when employee(s) leaves the company or switch roles.

9. Maintaining Your Access

Contact Information

Slack Channel - #sl-helpdesk
Phone - 281-714-4500 or extension 44500

Passwords

Passwords are changed every 90 calendar days.
Password can only be changed once every 24hrs, unless employee contacts Softlayer Help Desk to enable the password to be changed again. Passwords can be changed in either of the below locations:

IBM VPN (Must be connected to IBM's network/VPN) -
https://apr.inside.softlayer.com/pwreset/apr.dll?cmd=change
Softlayer VPN (Must be connected to the Softlayer GlobalProtect VPN) -
https://apr.softlayer.local/pwreset/apr.dll?cmd=change

Password Requirements

- Must not match one of your last 24 passwords
- Must not be similar to your current password
- Must not be similar to your logon name
- Must not be similar to your name
- Must contain at least 15 characters

Must Contain 1 char of each 4, and at least 4 char of 1 of the Following:

- an upper alpha character (A - Z)
- a lower alpha character (a - z)
- a numeric value (0 - 9) a special character (All characters not included above)

Logging in:

Employee accounts will disable every 30 calendar days if there is no activity such as VPN login.

If account is soft-disable, employee will need to contact Softlayer Help Desk to have the account re-enabled. Once re-enabled, you will need to wait 15min before attempting to login. Logging in will need to be done before 9am CST the following morning.

Note: Setup calendar reminder to login to the Softlayer VPN (GlobalProtect) every 25 calendar days to prevent account being soft-disabled.

Employee accounts will be terminated if there is no activity in 120+ calendar days.