

# Completing the Security Architecture Review (SAR)

This document explains how to complete the Application Security Architecture Review (SAR) form when you need to deploy your application. The form is located at <http://ssdlc.lzd.co/>.

Test form to play with

View and edit a [test SAR form](#) provided by Security team.

### Completed form

View a [completed SAR form](#) for `lazada-partner-integrations`. The form was completed by the team in August 2020.

## 1. Business scenario security audit

business scenario security audit

\* application Name :

lazada-partner-integrations

\* Business Background :

bridging membership in an online store to the same store in Lazada. Details: https://yuque.antfin-inc.com/liveup/tech-docs/aq1wr5

\* access domain name list :

Staging (pre): https://partners-p.lazada.co.th  
Production: https://partners.lazada.co.th

\* target user :

External users ×

in the internal small 2 scenario, please select the office network cluster first. If you continue to apply, you are likely to be rejected.

\* product/application introduction :

git@gitlab.alibaba-inc.com:lazada-loyalty/lazada-partner-integrations.git::master/

\* trunk code branch address :

lazada-partner-integrations

\* current system test account/password :

no\_test\_account

no\_test\_account

## Application name

Enter "lazada-partner-integrations".

## Business background

Business logic of the application. Enter: "Bridging membership in an offline store to the same store in Lazada. Details: <https://yuque.antfin-inc.com/liveup/tech-docs/aq1wr5>".

### \* Business Background :

Bridging membership in an offline store to the same store in Lazada. Details: <https://yuque.antfin-inc.com/liveup/tech-docs/aq1wr5>.

## Access domain name list

This list should contain domain names that were published for the app on Aserver (hence, listed publically), both staging and production. These are the domain names of the application and not the domains that the application wants to access.

The values are as follows:

- MY:
  - Staging (pre): <https://partner-integ-p.lazada.com.my/>
  - Production: <https://partner-integ.lazada.com.my/>
- TH:
  - Staging (pre): <https://partners-p.lazada.co.th>
  - Production: <https://partners.lazada.co.th>

### \* access domain name list :

Staging (pre): <https://partners-p.lazada.co.th>  
Production: <https://partners.lazada.co.th>

## Target user

This is to choose what category of users is going to access the app when it's deployed to production. "Internal" users are employees of Lazada. "External" users are people outside Lazada. "Agents" are Customer Support agents. "Outsourced user" are other outsourced contractors whose IPs have been whitelisted.

Choose "External users".

\* target user :

External users ✕

in the internal small 2 scenario, please select the office network cluster first. If you continue to apply, you are likely to be rejected.

## Product/application introduction

This is for a free text overview of the application. For Partner Integration, enter "The application handles business logic for linking customer's membership in offline store and customer account in Lazada.

Enter: "Two external entities are involved: 1. Partner system (authenticated via Lazada Open API) and 2. Lazada user (authenticated via MTOP)."

\* product/application introduction :

Two external entities are involved: 1. Partner system (authenticated via Lazada Open API) and 2. Lazada user (authenticated via MTOP).

## Trunk code branch address

This field contains an automatically populated Git master branch address: "git@gitlab.alibaba-inc.com:lazada-loyalty/lazada-partner-integrations.git::master/"

## Current system test account/password

Many Lazada applications have a dedication user account module. Security team in this case would need a test account for pentesting the app. Skip this field if no test account is provided.

## 2. Core session authentication review

core session authentication audit

\* whether the current system involves user login :

☒ yes
☐ no

\* system permission model :

ACL

▼

\* how to use system permissions :

Method

▼

\* access permission system selection :

lazop ×

lazada-session-api ×

mtop ×

\* Application Interface authentication function

view examples

```
1 @GetMapping("/store")
```

\* application data authentication function

view examples

```
1 @GetMapping("/store")
```

## Whether the current system involves user login

If you provide username and password for your application users, then choose "yes". If users log in to the application using the existing login pages of Lazada, then also choose "yes".

For lazada-partner-integrations, choose "yes".

\* whether the current system involves user login :

☒ yes
☐ no

## System permission model

These are authentication and authorization modules. The values "RBAC", "BAC", "MAC", "ACL" are the modules provided by Alibaba, so if you're using these modules, then it's acceptable for Security team with no further review. Otherwise if you're implementing your own model, then choose "other". Note that internal applications of Alibaba group, such as AliWork, use "ACL".

Choose "ACL".

\* system permission model :

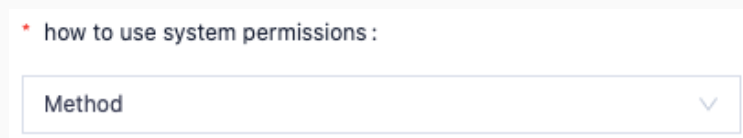
ACL

▼

## How to use system permissions

How do you integrate or embed the authorization system (ACL) in your application, which determines the way that roles and permissions are granted to your users.

Choose "Method".



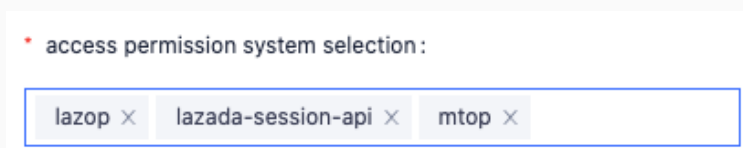
## Access permission system selection

This setting indicates what system your application is using for permission management. Alibaba created custom access management systems for authorization:

- "Xspace" is for Customer Care agents.
- "Hema Rex" used by [Hema](#), an Alibaba business that operates new retail supermarkets.
- "New Retail" is for New Retail business unit.
- "Mozi" is for Apollo applications.
- "Group Internal ACL" is for internal apps in Alibaba which we use every day.
- "Supply Chain Division" is for supply chain employees.
- "After logon, all content is accessible without permission."
- "Self-Built Permission Control System"

If you choose one of the last two options, it will require a separate review.

The lazada-partner-integrations application uses three different identity/authentication system for the APIs exposed to the internet from three different gateways: LAZOP: http, MTOP: native and h5, and ASERVER: http. You need to enter "lazop, lazada-session-api, mtop". This field supports free text input.



## App interface authentication function

This is an application-level authentication parameter. Paste the fragment of code that performs authentication. When the user submits user name and password, how is it processed?

Use this code snippet.

```

1 @GetMapping("/store")
2     @ResponseBody
3     public String store(@RequestParam("seller_id") Long sellerId,
4                         HttpServletResponse response,
5                         Device device) {
6
7         if (shouldShowComingSoonPage(device)) {
8             response.addHeader(ACCEL_REDIRECT_HEADER, ICMS_ROUTE_
9             PREFIX + cmsComingSoonPage);
10            response.setStatus(HttpStatus.NO_CONTENT.value());
11            return "";
12        }
13
14        Response<PartnerDTO> partnerDTOResponse = partnerQueryFac
15        ade.findPartnerById(sellerId);
16        if (partnerDTOResponse == null || partnerDTOResponse.isNo
17        tSuccess()) {
18            BizLogger.log(BIZ_CODE, "Could not find partner {0}",
19            sellerId);
20            Optional.ofNullable(partnerDTOResponse).map(Response:
21            :getErrorCode).ifPresent(BizLogger::error);
22            return "";
23        }
24
25        PartnerDTO partnerDTO = partnerDTOResponse.getModule();
26        if (!PartnerStatus.ENABLED.equals(partnerDTO.getStatus())
27        ) {
28            BizLogger.log(BIZ_CODE, "Partner is not enabled: {0}"
29            , partnerDTO);
30            return "";
31        }
32
33        Response<ProgramDTO> programDTOResponse = programQueryFac
34        ade.findProgramByPartner(sellerId);
35        if (programDTOResponse == null || programDTOResponse.isNo
36        tSuccess()) {
37            BizLogger.log(BIZ_CODE, "Could not find program by pa
38            rtner {0}", sellerId);
39            Optional.ofNullable(programDTOResponse).map(Response:

```

```

        :getErrorCode().ifPresent(BizLogger::error);
30         return "";
31     }
32
33     ProgramDTO programDTO = programDTOResponse.getModule();
34
35
36
37     //////////// USER AUTHENTICATION
38     Long memberId = UserWebLoginUtils.getLoginUserId();
39     ////////// <<<<----- USER AUTHENTICATION <<<<<<<<
40     //////////// END USER AUTHENTICATION
41
42
43
44
45     BizLogger.log(BIZ_CODE, "MemberID: {0}", "" + memberId);
46
47
48
49     ////////// AUTHORIZATION
50     MembershipDTO membershipDTO = null;
51     if (memberId != null) {
52         List<MembershipDTO> memberships = membershipService.f
indMemberships(memberId); ////////////// AUTHORIZATION for getting
membership data
53         if (CollectionUtils.isNotEmpty(memberships)) {
54             membershipDTO = memberships.stream()
55                 .filter(membership ->
56                     "ACTIVE".equalsIgnoreCase(members
hip.getStatus())
57                     && membership.getProgramC
ode() != null
58                     && membership.getProgramC
ode().equalsIgnoreCase(programDTO.getCode()))
59                 .findFirst()
60                 .orElse(null);
61         }
62     }

```

```

63          //////////
64
65
66
67
68
69          //
70          // todo: check membership status, what todo if disconnect
ed !?
71          //
72
73          String icmsPage;
74          if (membershipDTO != null) {
75              //
76              // is membership
77              //
78              icmsPage = cmsIsMembership.replace("[membershipId]",
String.valueOf(membershipDTO.getId()));
79          } else {
80              BizLogger.log(BIZ_CODE, "[cmsNonMembership] Partner:
{0}, Program: {1}", partnerDTO, programDTO);
81              icmsPage = cmsNonMembership.replace("[partnerCode]",
Optional.ofNullable(partnerDTO.getCode()).orElse("null"))
82                  .replace("[programId]", String.valueOf(progra
mDTO.getId()));
83          }
84
85          BizLogger.log(BIZ_CODE, "Accel redirect to {0}", icmsPage
);
86
87          response.addHeader(ACCEL_REDIRECT_HEADER, ICMS_ROUTE_PREF
IX + icmsPage);
88          response.setStatus(HttpStatus.NO_CONTENT.value());
89
90          return "";
91      }

```

## App data authentication function



This is an application-level authentication parameter. When the user has access to the application, Lazada also checks whether the user has access to the data, whether the user is authorized to see the data. What data can and cannot be seen was defined as a result of data classification in Lazada data warehouse (ODPS).

Use the same code snippet as in [App interface authentication function](#).

### 3. Application function API audit

List all internet-facing APIs (REST, MTOP and [LAZOP](#)) so that they can be reviewed by a security engineer. Note that the default API list is automatically populated by bootstrap. You need to edit as "N/A" if you don't plan on using a default API, and it will be removed from the release.

接口URL	批注
<a href="#">/youpin-api/priceSetting/downloadExcelTemplate</a> <a href="#">查看示例</a>	
<a href="#">/status.taobao</a>	
<a href="#">/membership/link</a>	
<a href="#">/membership/store</a>	
<a href="#">/membership/linking/result</a>	
<a href="#">/membership/partner/link</a>	
<a href="#">/checkpreload.htm</a>	
<a href="#">/\${server.error.path:\${error.path:/error}}</a>	
<a href="#">MTOP: mtop.lazada.partnerinteg.program.list</a>	
<a href="#">MTOP: mtop.lazada.partnerinteg.program.detail</a>	
<a href="#">MTOP: mtop.lazada.partnerinteg.membership.detail</a>	
<a href="#">MTOP: mtop.lazada.partnerinteg.membership.disconnect</a>	
<a href="#">MTOP: mtop.lazada.partnerinteg.program.link</a>	
<a href="#">MTOP: mtop.lazada.partnerinteg.membership.number</a>	
<a href="#">LAZOPS: /membership/balance/update</a>	
<a href="#">LAZOPS: /membership/update</a>	
<a href="#">LAZOPS: /membership/unlink</a>	
<a href="#">LAZOPS: /membership/updatecopy</a>	
<a href="#">LAZOPS: /membership/link</a>	

Note that the `/status.Taobao` endpoint is a health check endpoint generated by PandoraBoot framework. When a project is created, PandoraBoot automatically creates this URL to check if the app starts up successfully. This endpoint API always returns a "success" string.

/status.taobao
✕

接入URL: /status.taobao

接口说明: health check endpoint provided by pandore

鉴权方法:

1 none

接口入参:

1 none

接口出参:


1 success

## 4. Application architecture security audit

Attach the architecture diagrams from product and technical viewpoints.

application Architecture security audit


• product architecture diagram :



+  
product  
architecture  
diagram

Include the call relationship among applications inside different products and highlight the location of the current application in the product.  
[View template](#)

• technical architecture diagram :



+  
Technical  
architecture  
diagram

Including internal components of the application, interactions with other middleware and other content.  
[View template](#)

### Product architecture diagram

Attach a diagram that describes user flows among screens or components of the application.

Use this diagram: <https://yuque.antfin-inc.com/liveup/membership-integration/xipd49>.

### Technical architecture diagram

Attach a diagram that describes how the servers are connected, how the code is deployed, which systems are involved.

Use this diagram: <https://yuque.antfin-inc.com/liveup/membership-integration/say4ws>.