# PMS Revamp1.2.2.0 - Changes in API (NEW)

This document captures all the changes that have been made in the API endpoints during the PMS Revamp Release 1.2.2.0. These changes include addition of new endpoints, deprecation of a few endpoints and also some other changes.

Partner Management Service:

|  |  |  |  |
| --- | --- | --- | --- |
| **API Path** | **Method** | **Description** | **Changes done in release 1.2.2.0** |
| /oauth/client | GET | This endpoint retrieves a list of all OAuth clients created by the Auth Partners. It supports pagination, sorting, and and filtering based on optional query parameters. If the token used to access this endpoint, does not have the PARTNER\_ADMIN role, then it will fetch all the OAuth clients created by all the partners associated with the logged in user only. If the token used to access this endpoint, has PARTNER\_ADMIN role, then it will fetch all the OAuth clients created by all the partners. It is configured for **PARTNER\_ADMIN** and **AUTH\_PARTNER** roles. | Newly added in release 1.2.2.0 |
| /oauth/client | POST | This endpoint is used for creating OIDC Client. | 1. Added validation to check the partner id in the request body belongs to the user who’s token is being used to access this endpoint. This will ensure that PMS user can create OIDC client only for the partner id which belongs to the user. This validation is skipped if the user’s role is **PARTNER\_ADMIN**. 2. Added validation to check if the **Partner ID** used in the request body is active. This will ensure that OIDC client cannot be created for an inactive partner. ([MOSIP-34276](https://mosip.atlassian.net/browse/MOSIP-34276)) 3. If multiple policy requests were created by the partner for a policy, then while creating the OIDC client, this endpoint was checking the status of only the first policy request. So even if there was an approved policy request, it was still throwing an error. Fixed this bug ([MOSIP-34599](https://mosip.atlassian.net/browse/MOSIP-34599)) 4. Improved JWK validation for the public key by adding validation that n value (modulus value) of the JWK must be unique ([MOSIP-36219](https://mosip.atlassian.net/browse/MOSIP-36219)) 5. Updated client name to be a JSON string to support client name language map ([ES-836](https://mosip.atlassian.net/browse/ES-836)) |
| /oauth/client/{client\_id} | GET | This endpoint retrieves the OIDC client details by client id | 1. Added validation to check the partner id in the request belongs to the user who’s token is being used to access this endpoint. This will ensure that PMS user can access OIDC client only for the partner id which belongs to the user. This validation is skipped if the user’s role is **PARTNER\_ADMIN**. |
| /oauth/client/{client\_id} | PUT | This endpoint is used for updating OIDC Client based on client id | 1. Added validation to check the partner id in the request body belongs to the user who’s token is being used to access this endpoint. This will ensure that PMS user can update OIDC client only for the partner id which belongs to the user. This validation is skipped if the user’s role is **PARTNER\_ADMIN**. 2. Added validation to check if the **Partner ID** used in the request body is active. This will ensure that OIDC client cannot be updated for an inactive partner. This validation is skipped if the user’s role is **PARTNER\_ADMIN** and status in the request is changed to **INACTIVE**. ([MOSIP-34276](https://mosip.atlassian.net/browse/MOSIP-34276)) 3. If the status in the request is changed to **INACTIVE**, only the status is updated in the database other fields remain unchanged. This will ensure that PUT endpoint can be used to deactivate the OIDC client. 4. Added a bypass for a user with **PARTNER\_ADMIN** role. If the user with **PARTNER\_ADMIN** role is used to access this endpoint, then it will deactivate the OIDC client for any partner ID, even if the partner ID is deactivated. 5. Added a validation to check if the OIDC client is already deactivated.([MOSIP-34108](https://mosip.atlassian.net/browse/MOSIP-34108)) 6. Updated client name to be a JSON string to support client name language map ([ES-836](https://mosip.atlassian.net/browse/ES-836)) |
| /devicedetail | GET | This endpoint retrieves a list of all the Devices across all the Device Providers in PMS. It supports pagination, sorting, and filtering. It is configured for the role **PARTNER\_ADMIN**. | Newly added in release 1.2.2.0 |
| /devicedetail | PUT | Service to update Device Detail | This endpoint has been deprecated since the release-1.2.2.0. |
| /devicedetail | POST | Service to save Device Detail | This endpoint has been deprecated since the release-1.2.2.0. It has been replaced by the new POST /securebiometricinterface/{sbiId}/devices endpoint  This ensures that a device will always be created for a SBI and not without one. |
| /devicedetail | PATCH | Service to approve/reject Device Detail | This endpoint has been deprecated since the release-1.2.2.0. It has been replaced by the new POST devicedetail/{id}/approval endpoint |
| /devicedetail/{deviceId} | PATCH | This endpoint deactivates a Device based on the Device Id. It is configured for the roles **DEVICE\_PROVIDER** or **PARTNER\_ADMIN**. | Newly added in release 1.2.2.0 |
| /devicedetail/{id}/approval | POST | This endpoint is for the Partner Admin user to approve or reject a Device and activate the mapping between the Device and the SBI. It is configured for the role **PARTNER\_ADMIN** | Newly added in release 1.2.2.0 |
| /devicedetail/deviceSubType/filtervalues | POST | Service to filter Device Sub Types | No changes made in release 1.2.2.0 |
| /devicedetail/deviceType/filtervalues | POST | Service to filter Device Types | No changes made in release 1.2.2.0 |
| /devicedetail/deviceType/search | POST | Service to search Device Types | No changes made in release 1.2.2.0 |
| /devicedetail/filtervalues | POST | Service to filter Device Detail | This endpoint has been deprecated since the release-1.2.2.0. It has been replaced by the new GET /devicedetail endpoint |
| /devicedetail/search | POST | Service to search Device Detail | This endpoint has been deprecated since the release-1.2.2.0. It has been replaced by the new GET /devicedetail endpoint |
| /ftpchipdetail | GET | This endpoint retrieves a list of all FTM Chip details created by all the FTM Providers associated with the logged in user. It is configured for the roles **FTM\_PROVIDER** or **PARTNER\_ADMIN**. | Newly added in release 1.2.2.0 |
| /ftpchipdetail | PUT | Service to update ftp chip detail | This endpoint has been deprecated since the release-1.2.2.0 |
| /ftpchipdetail | POST | Service to save ftp chip detail | 1. Improved the validation check by trimming extra spaces in make and model to prevent duplicate entries. ([MOSIP-35788](https://mosip.atlassian.net/browse/MOSIP-35788)) |
| /ftpchipdetail | PATCH | Service to approve/reject ftp chip detail | No changes made in release 1.2.2.0 |
| /ftpchipdetail/{ftmId} | PATCH | This endpoint deactivates the ftp chip detail based on the ftp chip detail Id. It is configured for the roles **FTM\_PROVIDER** or **PARTNER\_ADMIN**. | Newly added in release 1.2.2.0 |
| /ftpchipdetail/{ftmId}/certificate-data | GET | This endpoint fetches both the CA signed certificate uploaded by the FTM Chip Provider and the MOSIP signed certificate generated by PMS. It is configured for the roles **FTM\_PROVIDER** or **PARTNER\_ADMIN**. | Newly added in release 1.2.2.0 |
| /ftpchipdetail/getPartnerCertificate/{ftpChipDetailId} | GET | Service to get certificate of ftp chip | 1. Improved Key Manager error handling, to capture the correct error code from Key Manager and send it in the endpoint’s response. |
| /ftpchipdetail/search | POST | Service to search ftp chip details | 1. This endpoint has been deprecated since the release-1.2.2.0. It has been replaced by the new GET /ftpchipdetail/v2 endpoint. |
| /ftpchipdetail/uploadcertificate | POST | Service to upload certificate of ftp chip | 1. Added validation to allow certificate upload only if the FTM chip details certificate status is **APPROVED** or **PENDING\_CERT\_UPLOAD**.([MOSIP-36283](https://mosip.atlassian.net/browse/MOSIP-36283)). So for Rejected or Deactivated FTM, a certificate cannot be uploaded. 2. Improved Key Manager error handling, to capture the correct error code from Key Manager and send it in the endpoint’s response. 3. Set isActive to false after certificate re-upload. This will ensure that after cert is reuploaded, partner admin will have to approve the FTM again. ([MOSIP-36285](https://mosip.atlassian.net/browse/MOSIP-36285)) |
| /ftpchipdetail/v2 | GET | This endpoint retrieves a list of all FTM Chip details created by all the FTM Providers. Also supports pagination, sorting, and filtering. It is configured for the role **PARTNER\_ADMIN**. | Newly added in release 1.2.2.0 |
| /admin-partners | GET | This endpoint retrieves a list of all Partners. Also supports pagination, sorting, and filtering. It is configured for the role **PARTNER\_ADMIN**. | Newly added in release 1.2.2.0 |
| /admin-partners/{partnerId} | GET | This endpoint retrieves all the details of the Partner based on Partner Id. It is configured for the role **PARTNER\_ADMIN**. | Newly added in release 1.2.2.0 |
| /partner-api-keys | GET | This endpoint retrieves a list of all the API keys created by the Auth Partners. Also supports pagination, sorting, and and filtering based on optional query parameters. If the token used to access this endpoint, does not have the **PARTNER\_ADMIN** role, then it will fetch all the API keys created by all the partners associated with the logged in user only. If the token used to access this endpoint, has **PARTNER\_ADMIN** role, then it will fetch all the API keys created by all the partners. | Newly added in release 1.2.2.0 |
| /partner-policy-requests | GET | This endpoint fetches list of all the policy requests made by the partners. Also supports pagination, sorting, and filtering based on optional query parameters. If the token used to access this endpoint, does not have the **PARTNER\_ADMIN** role, then it will fetch all the policy requests made by all the partners associated with the logged in user only.If the token used to access this endpoint, has **PARTNER\_ADMIN** role, then it will fetch all the policy requests made by all the partners. | Newly added in release 1.2.2.0 |
| /partners | GET | Service to get partner details | 1. This endpoint has been deprecated since the release-1.2.2.0. It has been replaced by the new GET /partners/v3 endpoint. |
| /partners/{partnerId} | PATCH | Service to activate/de-activate partner | 1. Added a check to verify if the **partner** is already deactivated. If yes, partner cannot be deactivated again. ([MOSIP-37017](https://mosip.atlassian.net/browse/MOSIP-37017)) |
| /partners/{partnerId}/apikey/{apikey} | GET | Service to get policy for given API key | No changes made in release 1.2.2.0 |
| /partners/{partnerId}/apikey/{apikey}/policies | PUT | Service to update policies against to API key | No changes made in release 1.2.2.0 |
| /partners/{partnerId}/policy/{policyId}/apikey/status | PATCH | Service to activate/de-activate partner API key | 1. If the API key is already deactivated, it cannot be deactivated again.([MOSIP-34430](https://mosip.atlassian.net/browse/MOSIP-34430)) 2. Added a validation to check if the **Partner ID** used in the request body is active. This will ensure that API cannot be deactivated if partner has been deactivated. This validation is skipped if the user’s role is **PARTNER\_ADMIN**. ([MOSIP-34430](https://mosip.atlassian.net/browse/MOSIP-34430)) |
| /partners/apikey | GET | Service to get API key requests | This endpoint has been deprecated since the release-1.2.2.0. It has been replaced by the new GET /partner-policy-requests endpoint. |
| /partners/apikey/{apikey} | GET | Service to get API key request | No changes made in release 1.2.2.0 |
| /partners/policy/{mappingkey} | PUT | Service to approve/reject partner policy mapping | No changes made in release 1.2.2.0 |
| /partners/v2 | GET | Service to get partner details | This endpoint has been deprecated since the release-1.2.2.0. It has been replaced by the new GET /partners/v3 endpoint. |
| /trust-chain-certificates | GET | This endpoint retrieves a list of all the Trust Certificates uploaded by the Partner Admin. Also supports pagination, sorting, and filtering. It is configured for the role **PARTNER\_ADMIN**. | Newly added in release 1.2.2.0 |
| /trust-chain-certificates/{certificateId}/certificateFile | GET | This endpoint will download p7b file for a CA / Intermediate CA certificate along with the trust chain based on Certificate Id. It is configured for the role **PARTNER\_ADMIN**. | Newly added in release 1.2.2.0 |
| /partners | POST | partner self registration | No changes made in release 1.2.2.0 |
| /partners/{partnerId} | GET | Service to get details of partner | Corrected the version in the response body |
| /partners/{partnerId} | PUT | Service to update details of partner |  |
| /partners/{partnerId}/apikey/request | GET | Service to get API key requests of partner | Corrected the version in the response body |
| /partners/{partnerId}/certificate | GET | Service to get partner certificate | 1. Added validation to check the partner id in the request belongs to the user who’s token is being used to access this endpoint. This will ensure that PMS user can access the certificate only for the partner id which belongs to the user. This validation is skipped if the user’s role is **PARTNER\_ADMIN**. 2. Added a check to verify if the partner id in the request exists in the database.([MOSIP-37017](https://mosip.atlassian.net/browse/MOSIP-37017)) 3. Added validation to check if the certificate has been uploaded previously. |
| /partners/{partnerId}/certificate-data | GET | This endpoint retrieves both the CA signed certificate uploaded by the partner and the MOSIP-signed certificate generated by PMS. It is configured for role any of the partner type or **PARTNER\_ADMIN**. | Newly added in release 1.2.2.0 |
| /partners/{partnerId}/generate/apikey | PATCH | To generate API Key for approved policies | Added a check to remove extra spaces in the API key label before saving to the database, preventing the creation of duplicate API key labels with extra spaces.([MOSIP-35788](https://mosip.atlassian.net/browse/MOSIP-35788)) |
| /partners/{partnerId}/policy/map | POST | To request for policy mapping | Updated error messages to indicate if the policy is already mapped and its status is **Approved** or **In Progress**.([MOSIP-33803](https://mosip.atlassian.net/browse/MOSIP-33803)) |
| /partners/{partnerId}/policygroup/{policygroupName} | PUT | Service to update the policy group for partner | No changes made in release 1.2.2.0 |
| /partners/apikey/request/filtervalues | POST | Service to filter API key requests | This endpoint has been deprecated since the release-1.2.2.0. It has been replaced by the new GET /partner-policy-requests endpoint. |
| /partners/apikey/request/search | POST | Service to search API key requests | This endpoint has been deprecated since the release-1.2.2.0. It has been replaced by the new GET /partner-policy-requests endpoint. |
| /partners/apikey/search | POST | Service to search API key | This endpoint has been deprecated since the release-1.2.2.0. It has been replaced by the new GET /partner-api-keys endpoint. |
| /partners/certificate/ca/upload | POST | Service to upload ca certificate | No changes made in release 1.2.2.0 |
| /partners/certificate/upload | POST | Service to upload partner certificate | 1. Added a validation to check if the **Partner ID** used in the request body is active. This will ensure that certificate cannot be uploaded if partner has been deactivated. ([MOSIP-34498](https://mosip.atlassian.net/browse/MOSIP-34498)) 2. If domain is **FTM**, do not call the uploadOtherDomainCertificate endpoint of KeyManager.([MOSIP-35797](https://mosip.atlassian.net/browse/MOSIP-35797)) |
| /partners/email/verify | PUT | Service to verify partner email | No changes made in release 1.2.2.0 |
| /partners/filtervalues | POST | Service to filter partner details | This endpoint has been deprecated since the release-1.2.2.0. It has been replaced by the new GET /partners/v3 endpoint. |
| /partners/partner-certificates-details | GET | This endpoint retrieves a list of all Partner Certicates uploaded by the logged in user | Newly added in release 1.2.2.0 |
| /partners/partnerType/search | POST | Service to search partner types | No changes made in release 1.2.2.0 |
| partners/search | POST | Service to search partner details | This endpoint has been deprecated since the release-1.2.2.0. It has been replaced by the new GET /partners/v3 endpoint. |
| partners/v2 | POST | Registers partner details | No changes made in release 1.2.2.0 |
| partners/v2/{partnerId} | PUT | Service to update details of partner | No changes made in release 1.2.2.0 |
| partners/v3 | GET | This endpoint retrieves a list of Partners associated with the logged in user, based on the query parameters. It is configured for role any of the partner type or **PARTNER\_ADMIN**. | Newly added in release 1.2.2.0 |
| /roles | GET | Service to get required roles | No changes made in release 1.2.2.0 |
| /securebiometricinterface | GET | This endpoint retrieves a list of all SBIs created by the Device Providers. Also supports pagination, sorting, and and filtering based on optional query parameters. If the token used to access this endpoint, does not have the **PARTNER\_ADMIN** role, then it will fetch all SBIs created by all the partners associated with the logged in user only. If the token used to access this endpoint, has **PARTNER\_ADMIN** role, then it will fetch all the SBIs created by all the partners. | Newly added in release 1.2.2.0 |
| /securebiometricinterface | PUT | Service to update SecureBiometricInterface | This endpoint has been deprecated since the release-1.2.2.0 |
| /securebiometricinterface | POST | Service to save SecureBiometricInterface details | Added a check to remove extra spaces in the SBI version before saving to the database, preventing the creation of duplicate SBI versions with extra spaces.([MOSIP-35788](https://mosip.atlassian.net/browse/MOSIP-35788)) |
| /securebiometricinterface | PATCH | Service to approve/reject SecureBiometricInterface | Added separate error codes for cases when SBI is already **approved** or **rejected**.([MOSIP-38973](https://mosip.atlassian.net/browse/MOSIP-38973)) |
| /securebiometricinterface/{sbiId} | PATCH | This endpoint deactivates an SBI along with associated Devices. It is configured for the roles **DEVICE\_PROVIDER** or **PARTNER\_ADMIN**. | Newly added in release 1.2.2.0 |
| /securebiometricinterface/{sbiId}/devices | GET | This endpoint fetches the list of Devices associated with a given SBI Id. It is configured for the roles **DEVICE\_PROVIDER** or **PARTNER\_ADMIN**. | Newly added in release 1.2.2.0 |
| /securebiometricinterface/{sbiId}/devices | POST | This endpoint adds a new Device and creates an inactive mapping between the device and the given SBI. It is configured for the roles **DEVICE\_PROVIDER** or **PARTNER\_ADMIN**. | Newly added in release 1.2.2.0 |
| /securebiometricinterface/devicedetails/map | PUT | Service to map device details with sbi | This endpoint has been deprecated since the release-1.2.2.0. It has been replaced by the new POST /securebiometricinterface/{sbiId}/devices endpoint. |
| /securebiometricinterface/devicedetails/map/remove | PUT | Service to remove mapped device details with sbi | This endpoint has been deprecated since the release-1.2.2.0. |
| /securebiometricinterface/devicedetails/map/search | POST | Service to search mapped device details and SecureBiometricInterface details | This endpoint has been deprecated since the release-1.2.2.0. It has been replaced by the new GET /securebiometricinterface/{sbiId}/devices endpoint. |
| /securebiometricinterface/filtervalues | POST | Service to filter SBI's | This endpoint has been deprecated since the release-1.2.2.0. It has been replaced by the new GET /securebiometricinterface endpoint. |
| /securebiometricinterface/search | POST | Service to search SecureBiometricInterface details | This endpoint has been deprecated since the release-1.2.2.0. It has been replaced by the new GET /securebiometricinterface endpoint. |
| /system-config | GET | This endpoint fetches the configurations for PMS and sends them to the UI. No roles are required for access. | Newly added in release 1.2.2.0 |
| /users | POST | Service to register user | No changes made in release 1.2.2.0 |
| /users/user-consent | GET | This endpoint fetches the user's consent related to the data captured by PMS. The consent is requested only once after the user's first login, and won't be asked again if already given. It is configured for all Partner Type roles. | Newly added in release 1.2.2.0 |
| /users/user-consent | POST | This endpoint saves the user's consent related to data captured by the PMS portal, which is requested only once after the user's first login. Once provided, the consent will not be asked again. It is configured for all Partner Type roles. | Newly added in release 1.2.2.0 |

Policy Management Service:

|  |  |  |  |
| --- | --- | --- | --- |
| **API Path** | **Method** | **Description** | **Changes done in release-1.2.2.0** |
| /policies | GET | Service to get policies | No changes made in release 1.2.2.0 |
| /policies | POST | Service to create a new authentication, data sharing, or credential policy. | Handled missing 'Empty Array and Empty String' Schema Validation |
| /policies/{policyId} | GET | Service to retrieve the details of a specific policy by its ID. | No changes made in release 1.2.2.0 |
| /policies/{policyId} | PUT | Service to update policy details | No changes made in release 1.2.2.0 |
| /policies/{policyId} | PATCH | This endpoint deactivates a policy based on the Policy Id. It checks if any policy requests are associated with the policy: it can be deactivated if there are no requests or if there are rejected requests. It cannot be deactivated if there are approved or pending requests, returning error codes PMS\_POL\_063 or PMS\_POL\_064, respectively. This endpoint is configured for the **POLICYMANAGER** or **PARTNER\_ADMIN** roles. | Newly added in release 1.2.2.0 |
| /policies/{policyId}/group/{policygroupId}/publish | POST | Service to publish policy | No changes made in release 1.2.2.0 |
| /policies/active/group/{groupName} | GET | Service to get active policy details for policy group name | No changes made in release 1.2.2.0 |
| /policies/group/{policygroupId} | GET | Service to get policy group | No changes made in release 1.2.2.0 |
| /policies/group/{policyGroupId} | PATCH | Service for Partner Admin users to deactivate a Policy Group based on the Policy Group Id. It is configured for the **POLICYMANAGER** or **PARTNER\_ADMIN** roles. | Newly added in release 1.2.2.0 |
| /policies/group/new | POST | Service to create a new policy group | No changes made in release 1.2.2.0 |
| /policies/group/search | POST | Service to search policy group | No changes made in release 1.2.2.0 |
| /policies/policy-groups | GET | Service to retrieve details about all active Policy Groups | Newly added in release 1.2.2.0 |
| /policies/v2 | GET | Service to retrieve the list of all Policies. It is configured for the **POLICYMANAGER** or **PARTNER\_ADMIN** roles. | Newly added in release 1.2.2.0 |