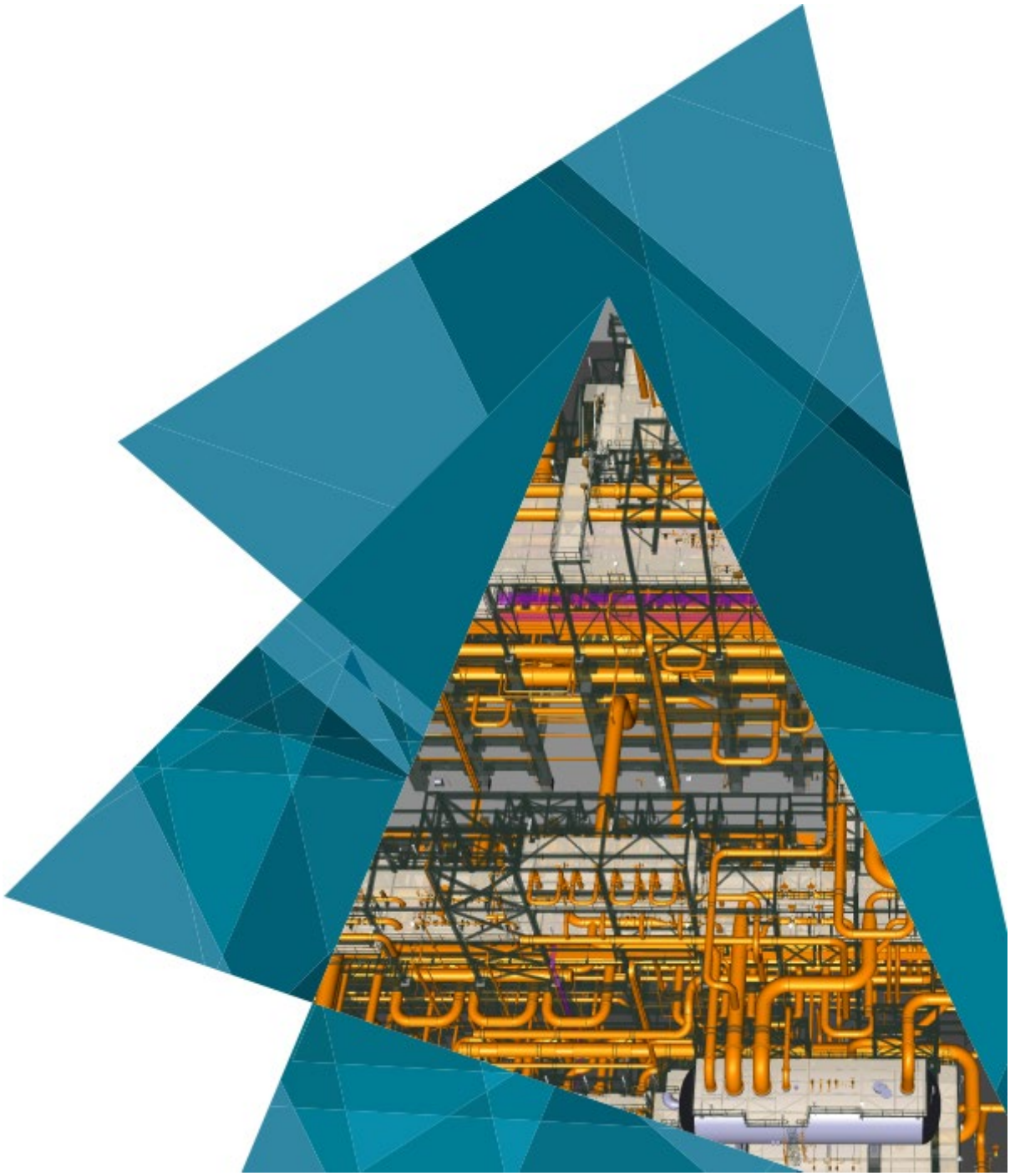
HxGN EAM Databridge Configuration for IMS via API Gateway Switch

Version 12.2.1
May 2025



Copyright

U.S. Government Restricted Rights Legend

Intergraph Corporation, Hexagon’s Asset Lifecycle Intelligence Division
305 Intergraph Way
Madison, AL 35758

Documentation

Documentation shall mean, whether in electronic or printed form, User's Guides, Installation Guides, Reference Guides, Administrator's Guides, Customization Guides, Programmer's Guides, Configuration Guides and Help Guides delivered with a particular software product.

Other Documentation

Other Documentation shall mean, whether in electronic or printed form and delivered with software or on Intergraph Smart® Support, SharePoint, box.net, or the Hexagon documentation web site, any documentation related to work processes, workflows, and best practices that is provided by Hexagon as guidance for using a software product.

Terms of Use

a. Use of a software product and Documentation is subject to the End User License Agreement ("EULA") delivered with the software product unless the Licensee has a valid signed license for this software product with Intergraph Corporation, Hexagon’s Asset Lifecycle Intelligence Division (“Hexagon”), a Hexagon Group Company. If the Licensee has a valid signed license for this software product with Hexagon, the valid signed license shall take precedence and govern the use of this software product and Documentation. Subject to the terms contained within the applicable license agreement, Hexagon gives Licensee permission to print a reasonable number of copies of the Documentation as defined in the applicable license agreement and delivered with the software product for Licensee's internal, non-commercial use. The Documentation may not be printed for resale or redistribution.

b. For use of Documentation or Other Documentation where end user does not receive a EULA or does not have a valid license agreement with Hexagon, Hexagon grants the Licensee a non-exclusive license to use the Documentation or Other Documentation for Licensee’s internal non-commercial use. Hexagon gives Licensee permission to print a reasonable number of copies of Other Documentation for Licensee’s internal, non-commercial use. The Other Documentation may not be printed for resale or redistribution. This license contained in this subsection b) may be terminated at any time and for any reason by Hexagon by giving written notice to Licensee.

Disclaimer of Warranties

Except for any express warranties as may be stated in the EULA or separate license or separate terms and conditions, Hexagon disclaims any and all express or implied warranties including, but not limited to the implied warranties of merchantability and fitness for a particular purpose and nothing stated in, or implied by, this document or its contents shall be considered or deemed a modification or amendment of such disclaimer. Hexagon believes the information in this publication is accurate as of its publication date.

The information and the software discussed in this document are subject to change without notice and are subject to applicable technical product descriptions. Hexagon is not responsible for any error that may appear in this document.

The software, Documentation and Other Documentation discussed in this document are furnished under a license and may be used or copied only in accordance with the terms of this license. THE USER OF THE SOFTWARE IS EXPECTED TO MAKE THE FINAL EVALUATION AS TO THE USEFULNESS OF THE SOFTWARE IN HIS OWN ENVIRONMENT.

Hexagon is not responsible for the accuracy of delivered data including, but not limited to, catalog, reference and symbol data. Users should verify for themselves that the data is accurate and suitable for their project work.

Limitation of Damages

IN NO EVENT WILL HEXAGON BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL INCIDENTAL, SPECIAL, OR PUNITIVE DAMAGES, INCLUDING BUT NOT LIMITED TO, LOSS OF USE OR PRODUCTION, LOSS OF REVENUE OR PROFIT, LOSS OF DATA, OR CLAIMS OF THIRD PARTIES, EVEN IF HEXAGON HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

UNDER NO CIRCUMSTANCES SHALL HEXAGON'S LIABILITY EXCEED THE AMOUNT THAT HEXAGON HAS BEEN PAID BY LICENSEE UNDER THIS AGREEMENT AT THE TIME THE CLAIM IS MADE. EXCEPT WHERE PROHIBITED BY APPLICABLE LAW, NO CLAIM, REGARDLESS OF FORM, ARISING OUT OF OR IN CONNECTION WITH THE SUBJECT MATTER OF THIS DOCUMENT MAY BE BROUGHT BY LICENSEE MORE THAN TWO (2) YEARS AFTER THE EVENT GIVING RISE TO THE CAUSE OF ACTION HAS OCCURRED.

IF UNDER THE LAW RULED APPLICABLE ANY PART OF THIS SECTION IS INVALID, THEN HEXAGON LIMITS ITS LIABILITY TO THE MAXIMUM EXTENT ALLOWED BY SAID LAW.

Export Controls

Intergraph Corporation, Hexagon's Asset Lifecycle Intelligence division ("Hexagon"), and a Hexagon Group Company's software products and any third-party Software Products obtained from Hexagon, its subsidiaries, or distributors (including any Documentation, Other Documentation or technical data related to these products) are subject to the export control laws and regulations of the United States. Diversion contrary to U.S. law is prohibited. These Software Products, and the direct product thereof, must not be exported or re-exported, directly or indirectly (including via remote access) under the following circumstances:

a. To Cuba, Iran, North Korea, Syria or the Crimean, "Donetsk People's Republic", "Luhansk People's Republic", or Sevastopol regions of Ukraine, or any national of these countries.

b. To any person or entity listed on any U.S. government denial list, including but not limited to, the U.S. Department of Commerce Denied Persons, Entities, and Unverified Lists, http://www.bis.doc.gov/complianceandenforcement/liststocheck.htm, the U.S. Department of Treasury Specially Designated Nationals List. Visit www.export.gov for more information or follow this link for the screening tool: https://legacy.export.gov/csl-search.

c. To any entity when Licensee knows, or has reason to know, the end use of the Software Product is related to the design, development, production, or use of missiles, chemical, biological, or nuclear weapons, or other un-safeguarded or sensitive nuclear uses.

d. To any entity when Licensee knows, or has reason to know, that an illegal reshipment will take place.

Any questions regarding export/re-export of relevant Hexagon software product, customized software, Technical Data and/or third-party software obtained from Hexagon, its subsidiaries or distributors, should be addressed to Hexagon's Export Compliance Department, 305 Intergraph Way, Madison, Alabama 35758 USA or at exportcompliance@intergraph.com. Customer shall hold harmless and indemnify Hexagon and a Hexagon Group Company for any causes of action, claims, costs, expenses and/or damages resulting to Hexagon or a Hexagon Group Company from a breach by Customer.

Trademarks

Intergraph®, the Intergraph logo®, Intergraph Smart®, SmartPlant®, SmartMarine, SmartSketch®, SmartPlant Cloud®, PDS®, FrameWorks®, I-Route, I-Export, ISOGEN®, SPOOLGEN, SupportManager®, SupportModeler®, SAPPHIRE®, TANK, PV Elite®, CADWorx®, CADWorx DraftPro®, GTSTRUDL®, CAESAR II®, and HxGN SDx® are trademarks or registered trademarks of Intergraph Corporation or its affiliates, parents, subsidiaries. Hexagon and the Hexagon logo are registered trademarks of Hexagon AB or its subsidiaries. Other brands and product names are trademarks of their respective owners.

The following are trademarks and service marks owned by Intergraph Corporation d/b/a Hexagon or its subsidiaries worldwide: hexagonppm.com/trademarks.

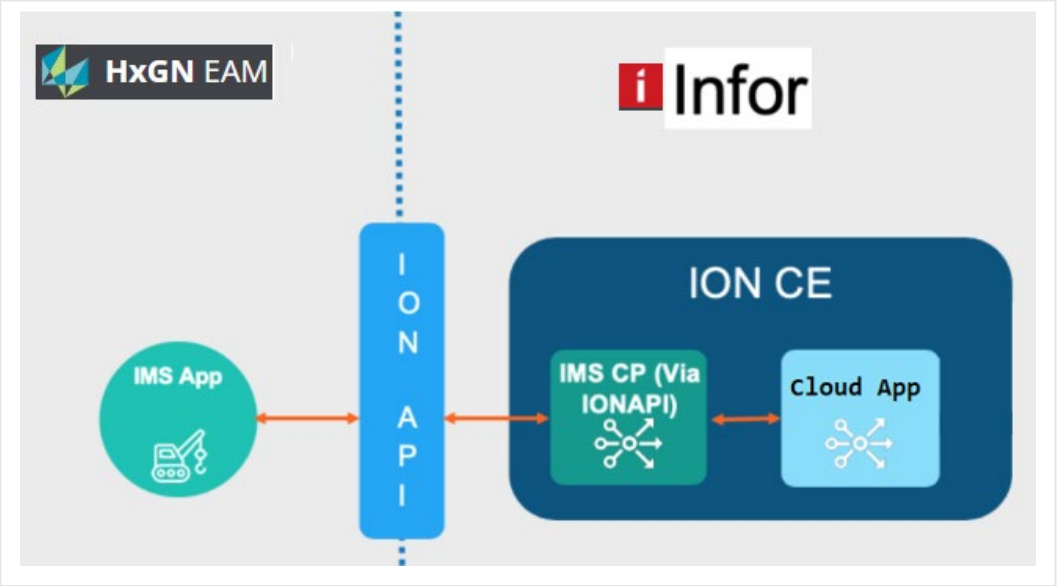
Contents

About this brief

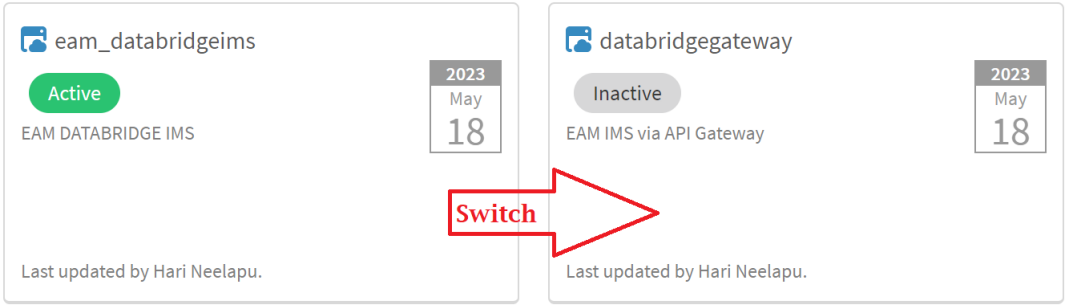
The purpose of this document is to guide the cloud EAM customers in Hexagon cloud to switch from the ION IMS connection point to the “IMS via ION API Gateway” connection point on Databridge BOD integration with ION. This document is applicable to cloud EAM customers in the Hexagon cloud who are currently using the Infor ION IMS connector for EAM Databridge BOD integration with ION.

Overview

As EAM is now a product of Hexagon, EAM tenants are gradually moving from the Infor cloud to the Hexagon cloud. While in the Hexagon cloud outside of the Infor cloud, EAM tenants may soon lose access to the Infor ION IMS end point inside the Infor cloud that is currently still exposed and may soon be restricted in its access inside the Infor cloud only. So, EAM as an external app outside the Infor cloud will need to access the ION IMS end point inside the Infor cloud via an API gateway called “IMS via API Gateway” Connector, which is a standard way provided by Infor for external apps to deal with this kind of scenario as shown in the below diagram.



For EAM in the Hexagon cloud to integrate with other Infor products via Infor ION inside the Infor cloud, customers must switch from their IMS Connector based data flows (involving either ‘eam.databridgeims’ IMS connection point or ‘eam’ IMS connection point) to “IMS via API Gateway” Connector based data flows



There are two phases for this transition or switch:

- Preparation before the transition: While EAM is still using the IMS end point/data flow to integrate with ION in run time, you will need to follow the guidelines to do all the necessary preliminary preparation work for the transition. This preparation work should not interrupt the production environment running on IMS based flows.
- Transition: This is the time when you will switch from the direct IMS approach to the IMS via ION API approach. You will need to follow the guidelines to switch from direct IMS based flows to “IMS via ION API Gateway” based flows.

If all the preliminary preparation is done correctly, the actual downtime for the transition is very minimal, say a few minutes, that is, the time between deactivation of the IMS based flow and activating the “IMS via API Gateway” based flow. So, before the transition or switch, ensure all the preparation work is done and done correctly.

Preparation before the transition

Follow the below steps as preparation for the transition. These preparation steps can be performed while the existing IMS based data flows are still running in the production environment.

1. Define a Non-Infor API suite in Infor OS to expose the EAM IMS endpoint by following the steps mentioned in Appendix A: API Gateway Configuration.

2. Once the Non-Infor API suite EAMIMS is successfully created, create a service account and Authorized App for EAM by following the steps mentioned in Appendix C: Service account and Client ID.

3. Once we have the service account and Client id, create the “IMS via API Gateway” connection point by following the steps mentioned in Appendix D: ION Configuration.

4. The user must configure tenant specific EAM security by following the steps mentioned in Appendix E: Tenant Specific EAM Security.

Transition

It is recommended to perform the transition on a non-business day(holiday/weekend) when the business impact is minimal.

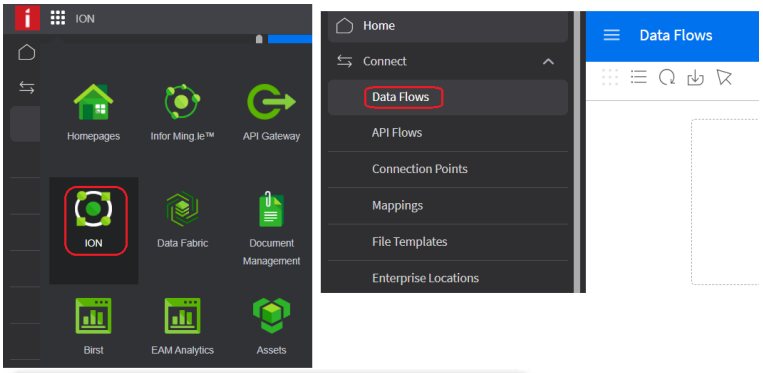
Before starting the transition, ensure all the steps mentioned in the Preparation for the Transition section are successfully executed.

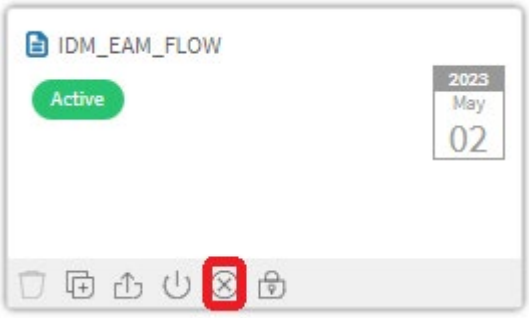
For the transition, follow the below steps in sequence.

Step 1: Go to EAM Administration | Security | Install Parameters screen, add/set below install parameter:

Field Name	Field Value
Install Parameter	***@IOBCONV***
Description	*Is Databridge IMS via API Gateway in progress? Y or N*
Value	*Y*

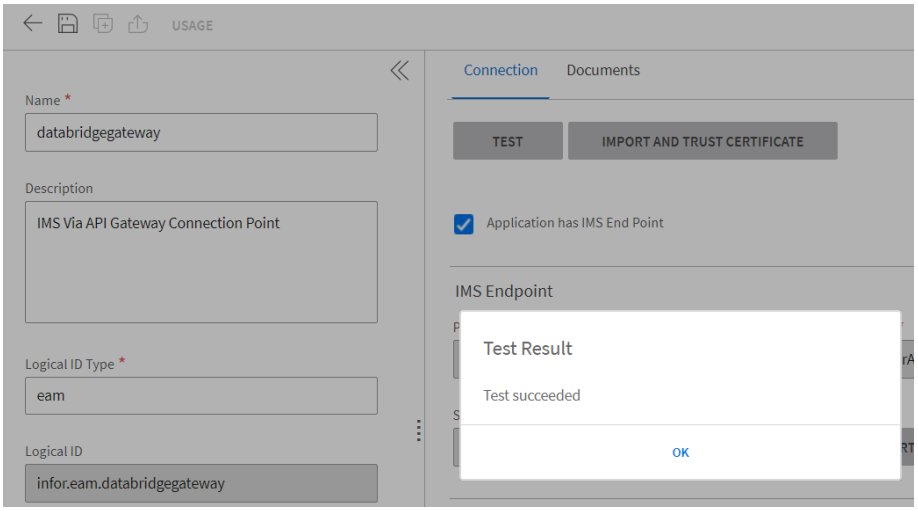
Step 2: Deactivate all ION Data flows referencing the EAM IMS connection point being used and make a note of which data flows were active and are now deactivated.



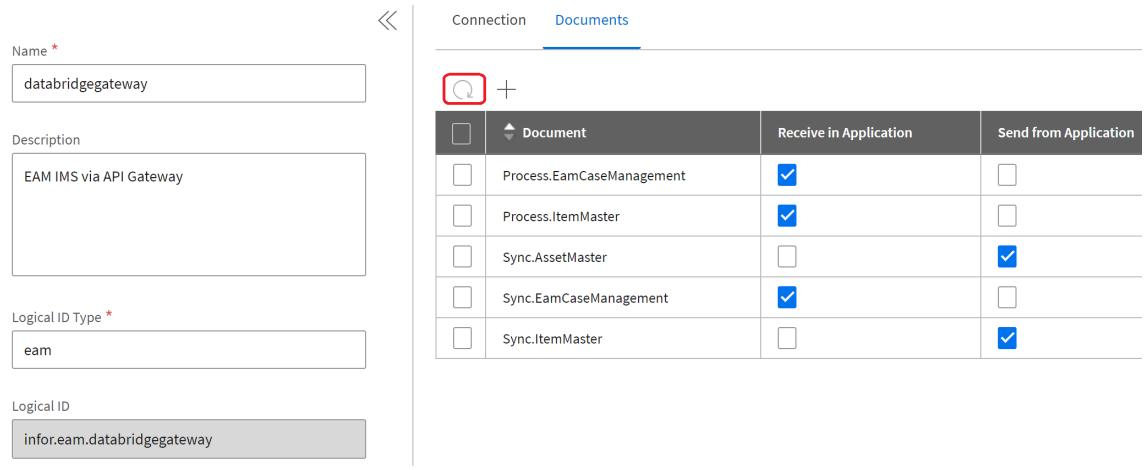


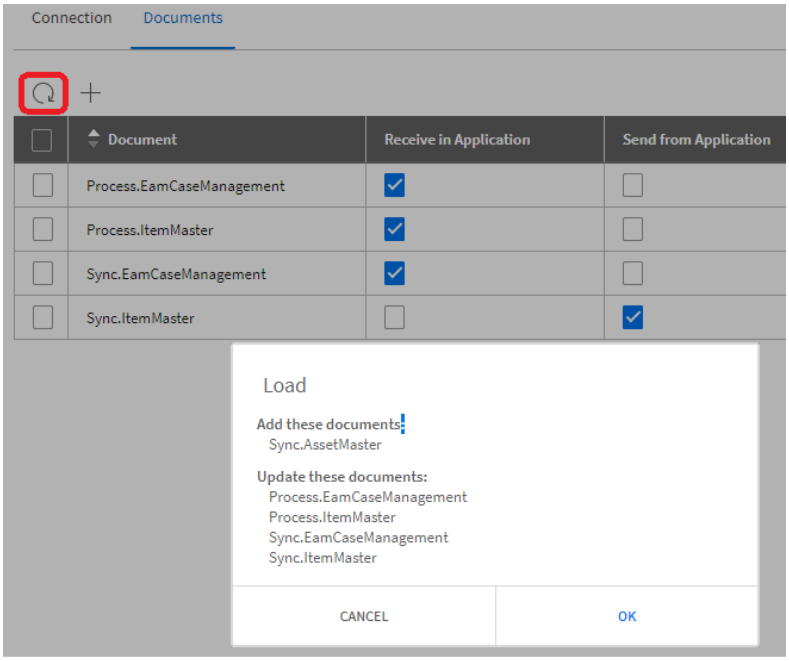
Step 3: Modify the INFOR-EAM partner in EAM by following the steps in Appendix F: EAM Configurations.

Step 4: On ION Desk | Connection Points, locate the new EAM “IMS via API Gateway” connection point, go to the Connection tab and click the ‘Test’ button to ensure you get a “Test succeeded” test result.

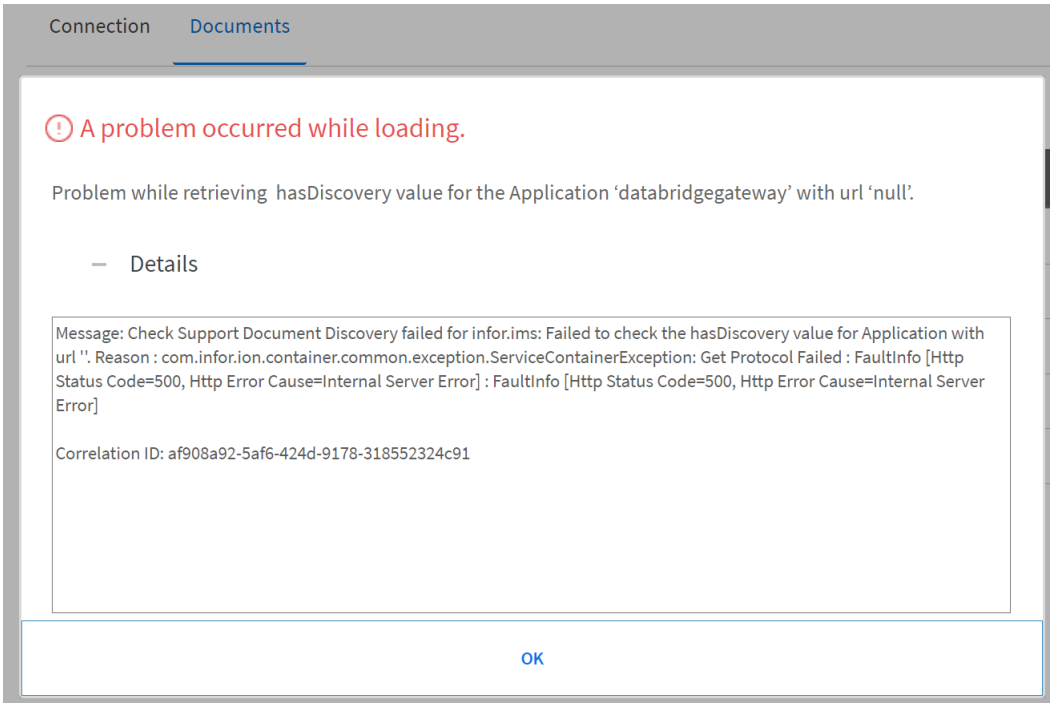


Then go to the Documents tab and click the Refresh button. The Documents tab will be updated with the partner subscriptions/inbound documents for the INFOR-IMS partner in EAM.





If you are not able to refresh the Document tab and get the error below, you will need to check the INFOR-IMS partner configuration done in Step 3 above, and also test the connection by clicking the 'Test Connection' button under the Connection tab on the new IMS via API Gateway connection point to ensure the EAM IMS URL and EAM oauth1.0 credentials are correctly configured for the API Gateway.



Step 5: Go to ION Desk | Connect | Data Flows, based on your previously active data flows that were deactivated in Step 2 (You have already made a note in Step 2), identify their corresponding duplicated data flows and activate these duplicated data flows one after another to ensure they are successfully activated.

Step 6: Go to EAM Administration | Security | Install Parameters screen, locate and set the install parameter ***@IOBCONV*** created in Step 1 to “N”.

Now the transition is complete. Verification that both EAM inbound and outbound BOD traffics work should be performed.

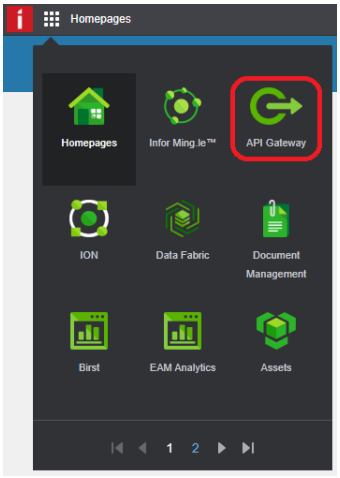
If there are issues encountered during or after the transition and you cannot resolve them in time, you can roll back to the original IMS configuration by following the steps defined in Appendix G: Roll back to IMS Connection point. After the issues are resolved, you can retry the transition later.

Appendix A: API Gateway Configuration

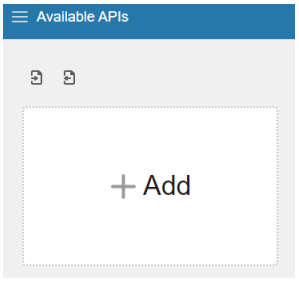
The prerequisite for defining the “IMS via API Gateway” connector is to add and define the Non-Infor API Suite in Cloud Multi-Tenant environment,

To add and define the Non-Infor Gateway suite, follow the steps below.

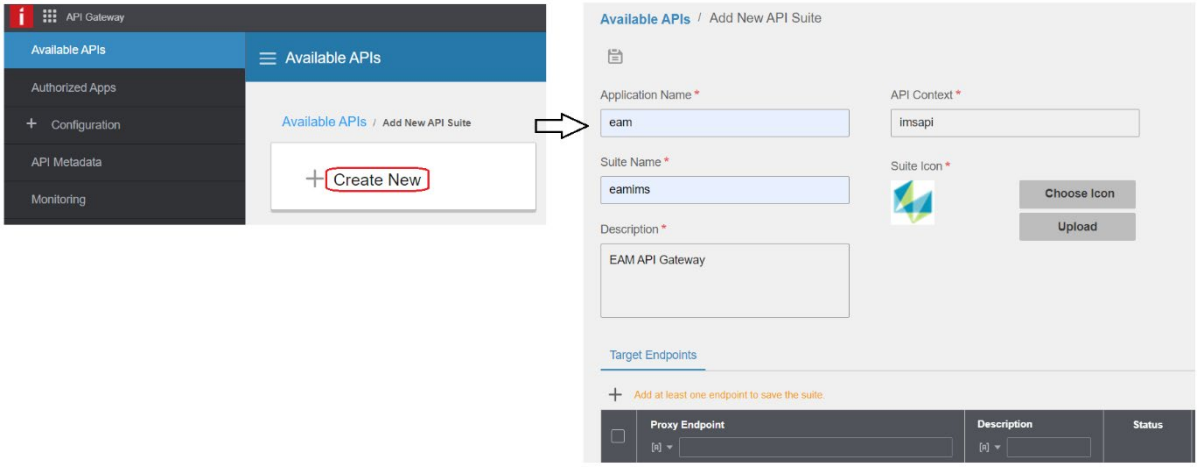
1. Go to API Gateway in the Infor OS menu,



2. Click Add for a new Non-Infor suite



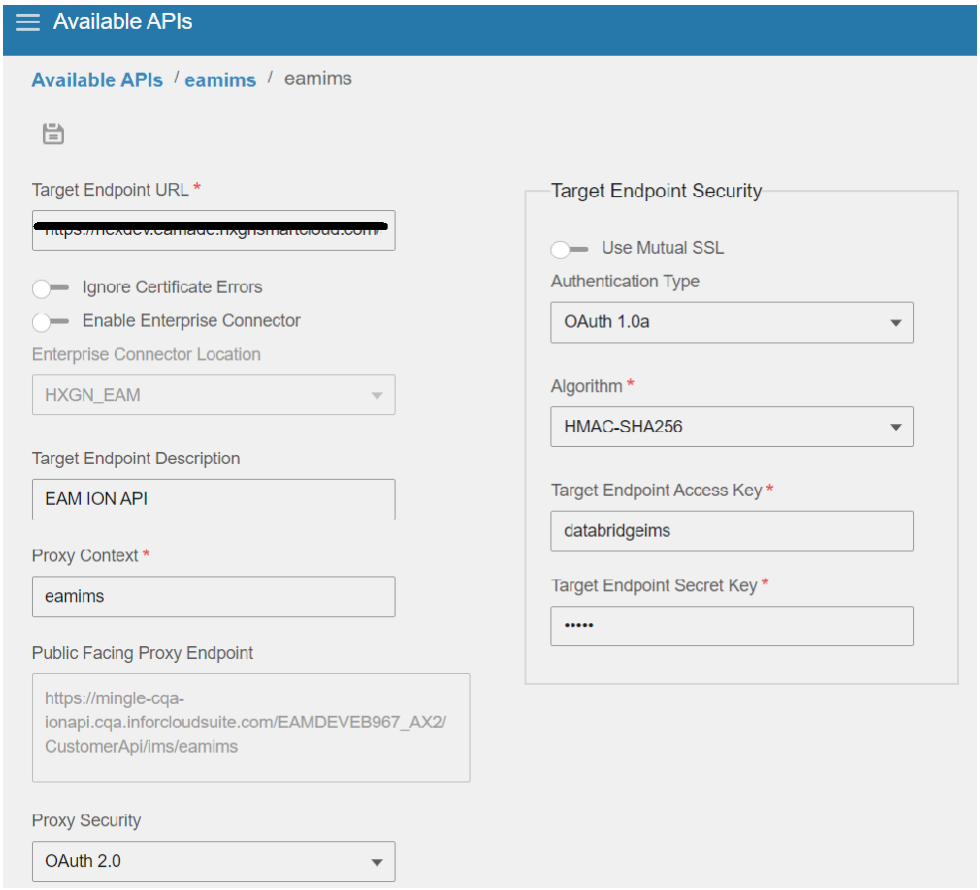
3. Click “Create New” to define a Non-Infor Api suite with below details.



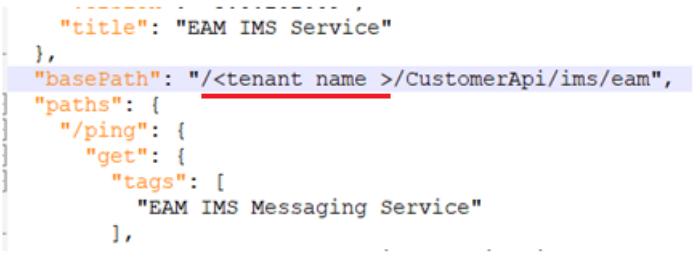
4. Add a target endpoint and then populate the EAM target endpoint with the below details,

- **EAM target Endpoint URL**: https://<eam host>:<port>/axis/imsservice. See Appendix B: How to find EAM IMS end point URL
- **Proxy Context**: eamims
- **Proxy Security**: OAuth 2.0
- **Target Endpoint Security**: OAuth 1.0a
- **Algorithm**: HMAC-SHA256
- **Target Endpoint Access Key**: tenant-specific databridge IMS access key you will define in EAM in Appendix E: Tenant Specific EAM Security, EAM Inbound Oauth1 Security Configuration section
- **Target Endpoint Secret Key**: tenant-specific databridge IMS secret key you will define in EAM in Appendix E: Tenant Specific EAM Security, EAM Inbound Oauth1 Security Configuration section

Note: You will need to determine the EAM IMS access/secret key values now to finish the above steps although EAM IMS access/secret keys are not yet configured in EAM at this point. EAM IMS access/secret key configuration is done in Appendix E: Tenant Specific EAM Security.



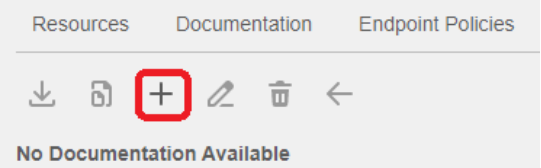
5. Add the attached(EAMIMS.json) documentation to the API Suite so the services defined in the IMS endpoint are available for the 'IMS via ION API' Connector. The user will need to edit the file to provide the tenant information in the documentation json before importing it into API Gateway as shown below



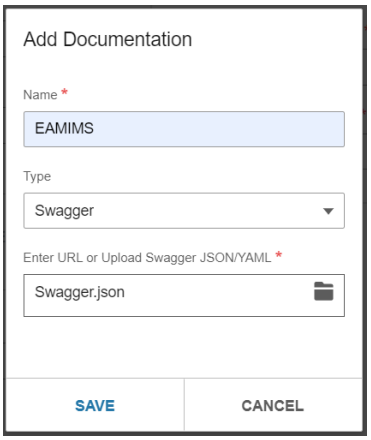

EAMIMS.json

Tip: The **EAMIMS.json** document is attached to this PDF in the **Attachments** pane. To access this file, browse to the left-hand menu for this page, and then click **1 attachment**. The attachments view opens with the selected document available for downloading.

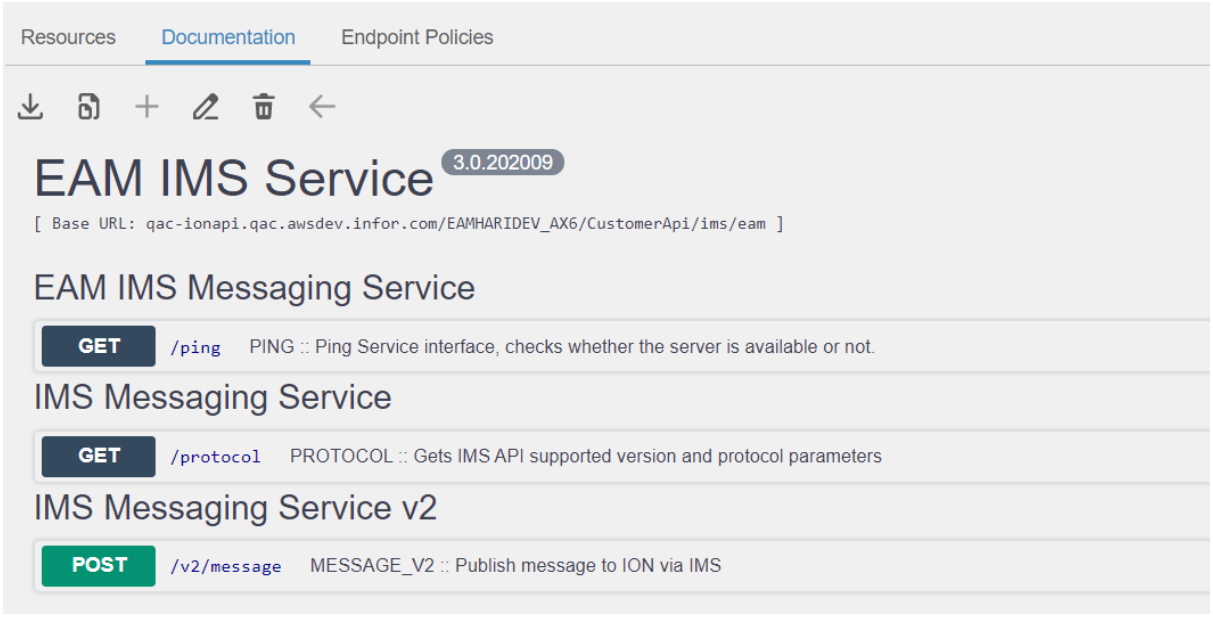
6. The Edited swagger documentation should be imported into the API endpoint by clicking on the “+” in the documentation section as shown below.



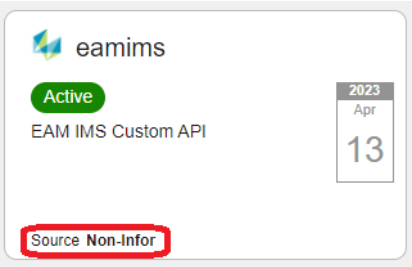
7. Provide the Name and Type as shown below and then browse to the edited EAMIMS.json file and click SAVE.



8. After importing the json file, the user should see the below swagger documentation with ping, protocol, and v2/message operations as shown below,



9. Once the Non-Infor API suite with documentation is successfully created, verify it is active. This will complete the API Gateway configuration.



Appendix B: How to find EAM IMS end point URL

Go to EAM Administration | Security | Install Parameters screen and locate *AXISURL* install parameter. Copy the value of this install parameter to any text editor and then replace "*services/EWSConnector*" with "*imsservice*". The result will be the EAM IMS end point URL.

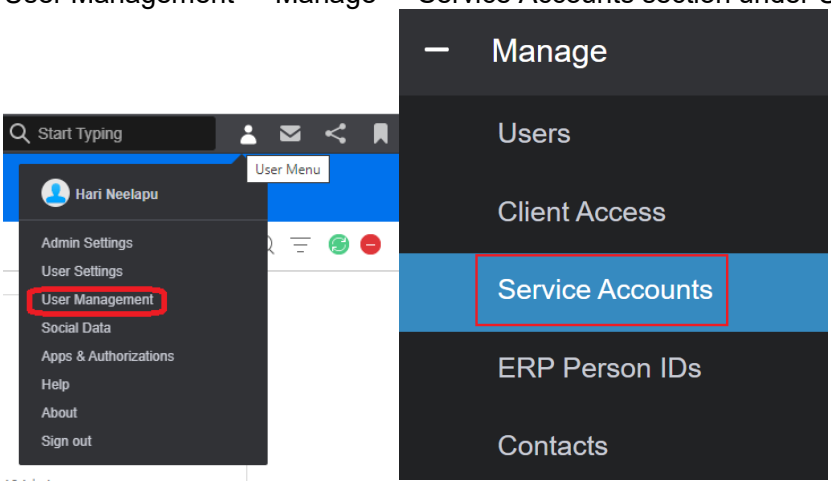
For example, when AXISURL="*https://hexdev.eamade.hxgnsmartcloud.com/axis/services/EWSConnector*",

EAM IMS URL will be "*https://hexdev.eamade.hxgnsmartcloud.com/axis/imsservice*".

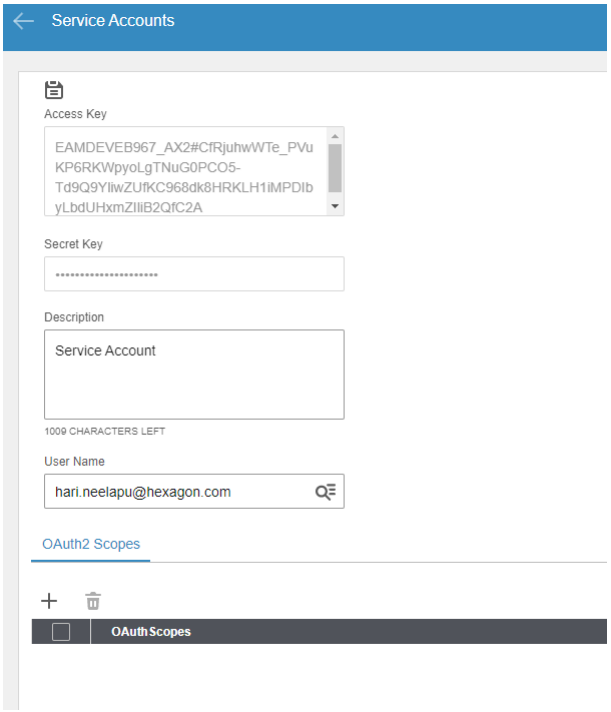
Appendix C: Service Account and Client ID

"Service Account" Creation ⚠ **CAUTION: If you have already finished this step while configuring Infor API Gateway for Hexagon EAM integration with Infor Datalake, please skip this step as both integrations share the same Infor API Gateway configuration.**

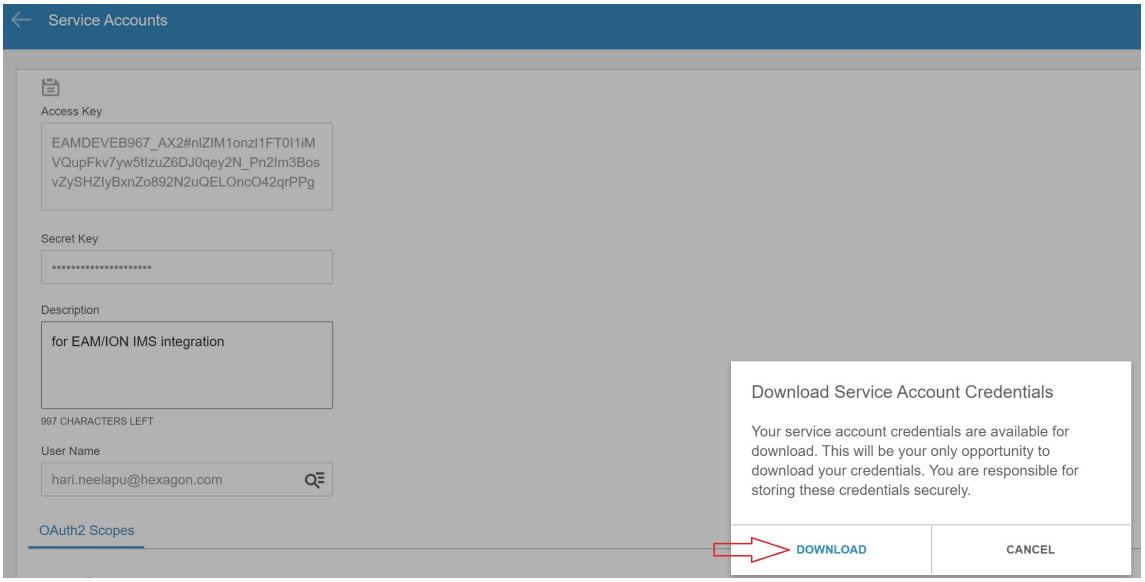
Create a service account for the user who is used to run the integration in the User Management -> Manage -> Service Accounts section under User Menu in Infor OS.

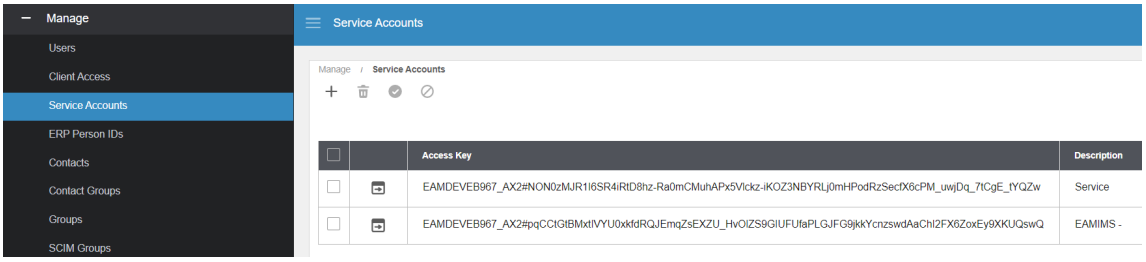


Add a new service account by clicking '+' button, and then select the user name and click save button.



You will be prompted with the below 'Download Service Account Credentials' windows. Click the DOWNLOAD button to download the service account information (.csv file) which will be used in Appendix D: ION Configuration



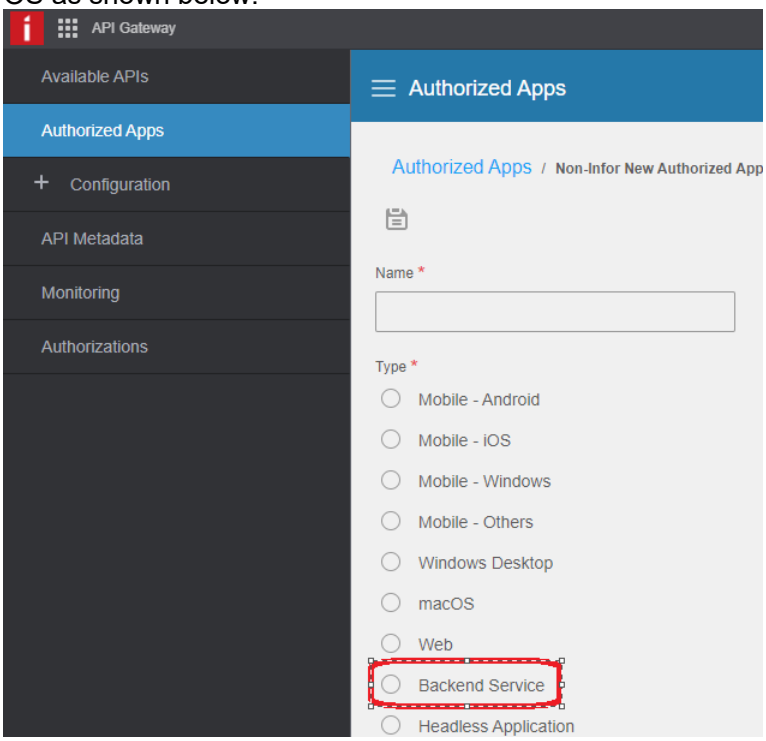


It is recommended to create a user not associated with an individual person and then create service account for that user.

Authorized App Creation

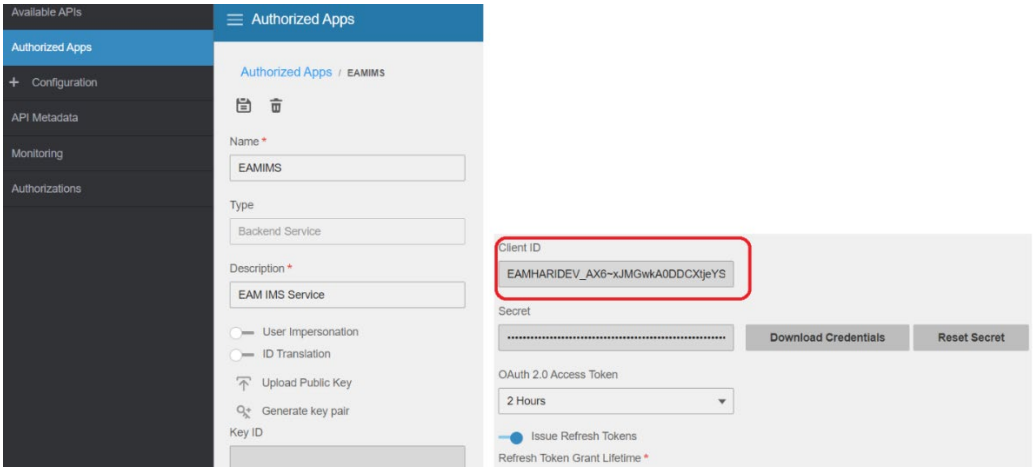
⚠ CAUTION: If you have already finished this step while configuring Infor API Gateway for Hexagon EAM integration with Infor Datalake, please skip this step as both integrations share the same Infor API Gateway configuration.

Create a Backend Service in the Authorized Apps section of the API Gateway menu in Infor OS as shown below.

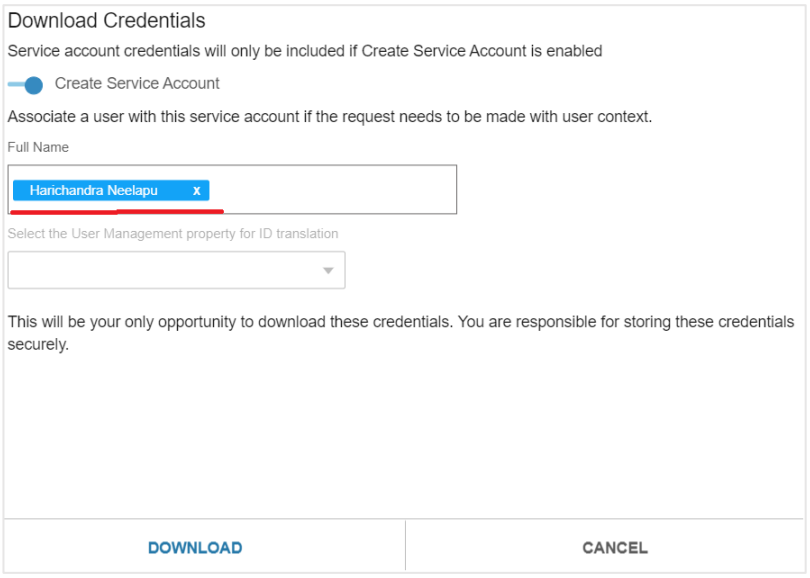


The user will be using this Backend Service in the configuration in Appendix D: ION Configuration, Also download the Oauth2 credentials file *.ionapi file by using the same account that was used to define a service account.

Make note of the “Client ID”, this client id will be used in the Connection point creation in Appendix D: ION Configuration,



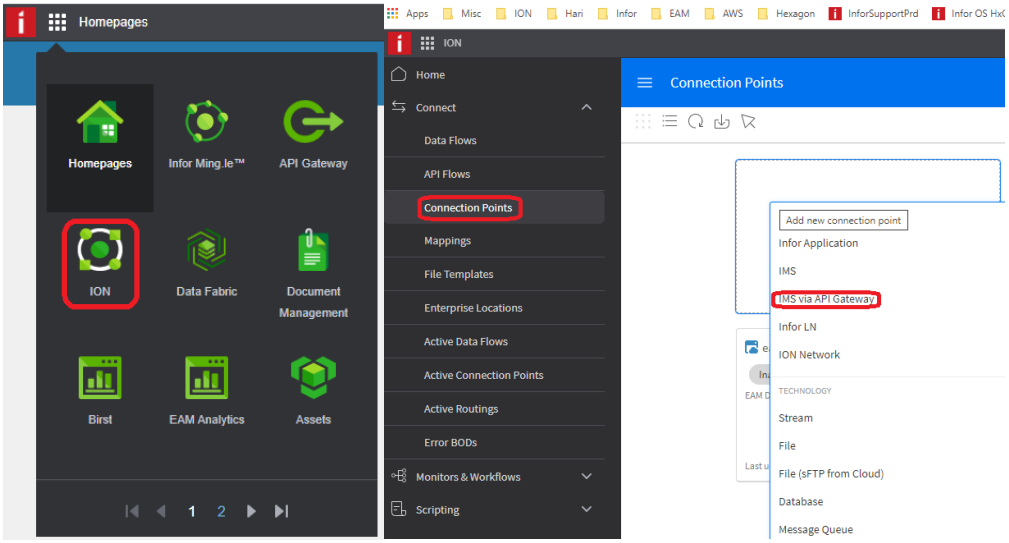
While downloading the Credentials, in the pop up, enable “Create Service Account” toggle button and enter the full name of the user that was used in “service account” creation on the Full Name field. The content of the downloaded file (EAMIMS.ionapi file) will be used in Appendix E: Tenant specific EAM Security.



This completes the Service account and Client ID configurations.

Appendix D: ION Configuration

Create an “IMS via API Gateway” connection point in ION -> Connect -> Connection points in Infor OS

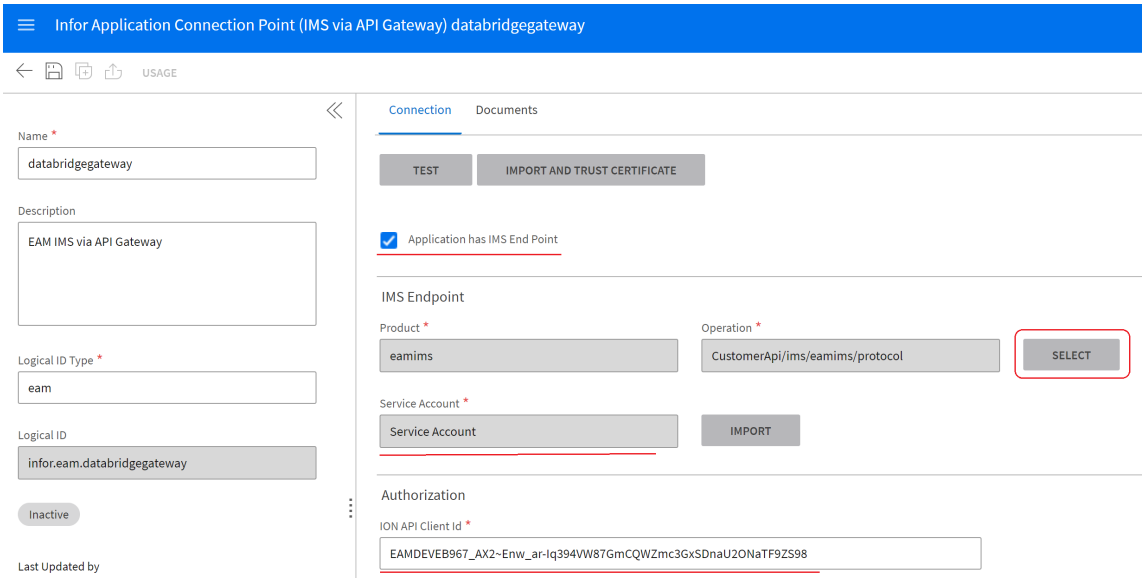


Provide the flowing values for the connection point .

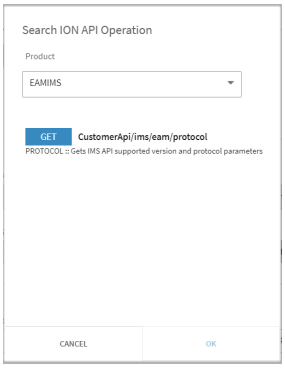
- **Name**: *databridgegateway*
- **Desc**: IMS Via API Gateway Connection point
- **Logical ID Type**: *eam*
- **Logical ID**: *infor.eam. databridgegateway*(read only)

Note: Use the same name “*databridgegateway*” for the partner id field while configuring the INFOR-IMS partner in EAM Databridge Partners during the transition time. The names “eam” or “eam:databridgeims” should not be used as the connection point name as they are already reserved or used for other purposes.

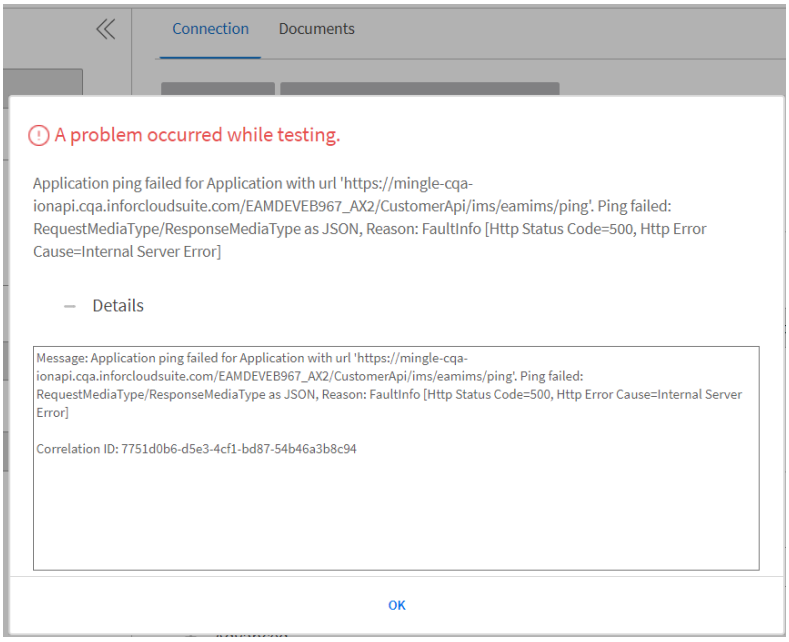
Connection Tab



- Check the Application has IMS Endpoint check box
- For Product and Operation, select the IONAPI Non-Infor Suite that we created in Appendix A: API Gateway Configuration section using the “SELECT” button provided in the above screen. Click the GET button before you click OK button in below screen.



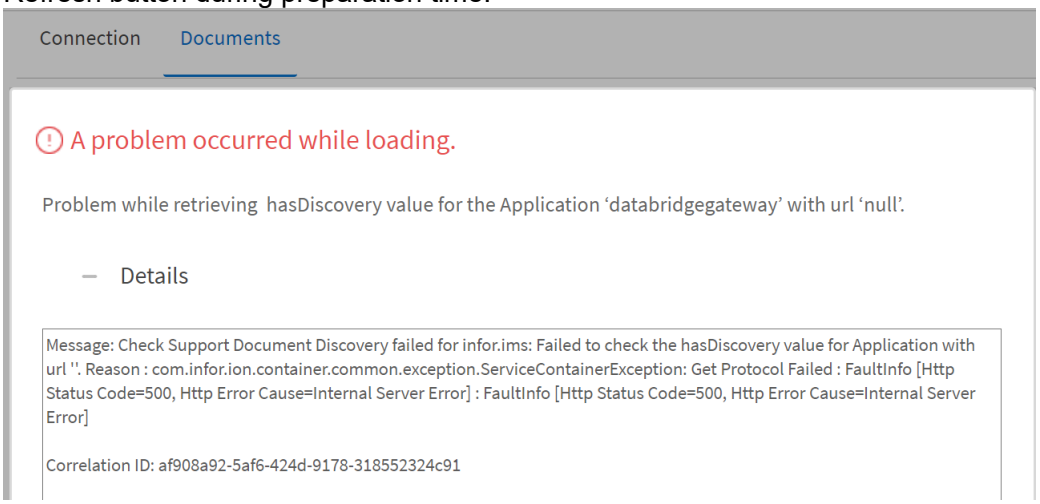
- Service Account: Import the account with the .csv file created in Appendix C: Service Account and Client ID
- ION API Client ID: Provide the Client ID value generated in Appendix C: Service Account and Client ID
- Since the EAM IMS access/secret keys and INFOR-IMS partner are not yet configured for the new IMS via API Gateway connector in EAM, when you click the “Test Connection” button at this point, the test connection will fail with below error:



You will wait to test connection at transition time.

Documents Tab

Since the EAM INFOR-IMS partner configuration is not done during the preparation time, users cannot use the Refresh button on the Document Tab to load the documents configured in EAM during preparation time. The below error will occur when clicking the Refresh button during preparation time.

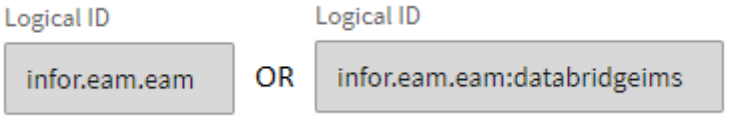


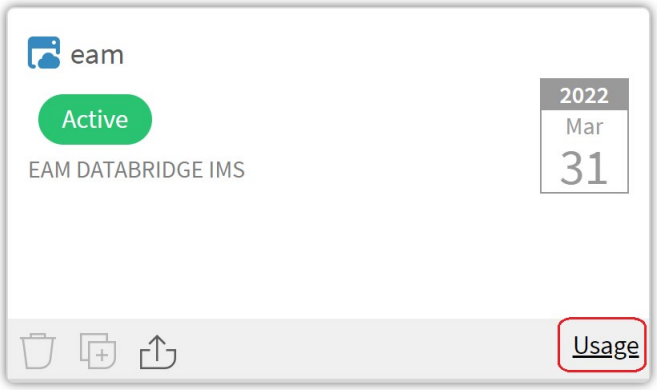
It is ok not to configure the Document tab during preparation. The Document tab will be refreshed during transition (see details in Transition section).

Users have the option to manually add these documents to the Document tab temporarily during preparation time to avoid the warning messages when configuring and saving the duplicated data flows as mentioned below in the same Appendix.

Identify, Duplicate the ION data flow, and Switch the connection point

Identify the EAM IMS connection point that is being used (either **infor.eam.eam** or **infor.eam.eam:databridgeims**). On ION Desk, Connect | Connection Points, click 'Usage' of that connection point and you will see all the data flows referencing that connection point. Make a note of these data flows.



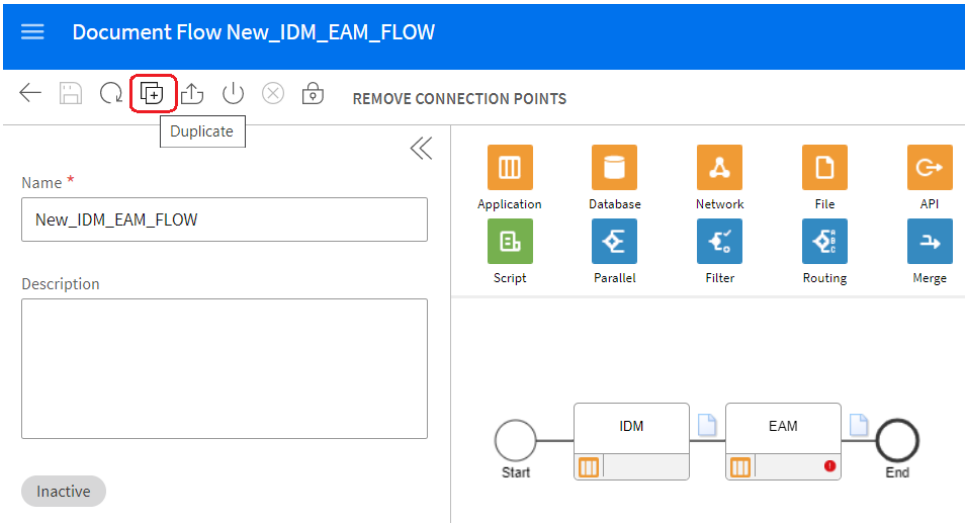


Usage

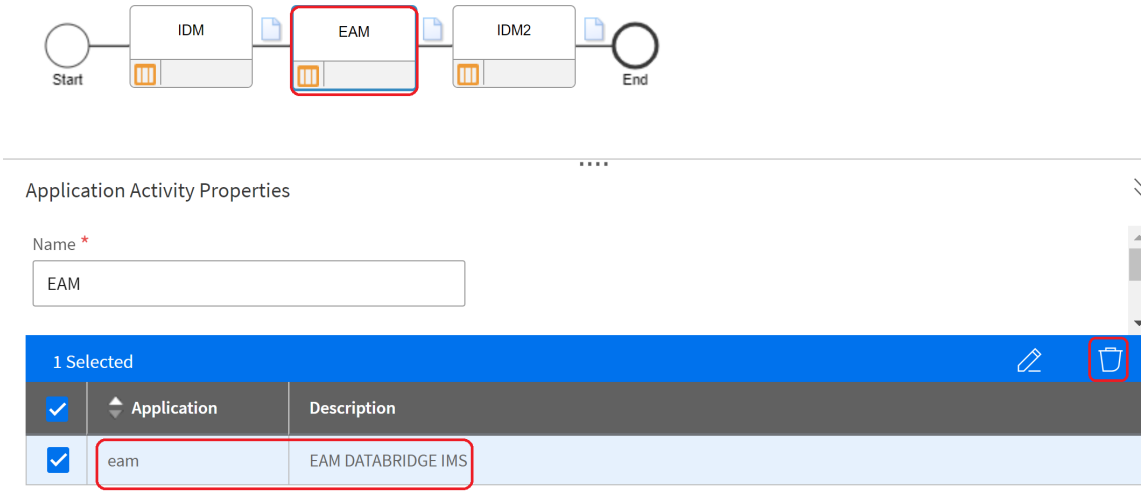
Type	Name	Description	Status
	CustomerSurveyEmail	Document Flow for Customer Survey Emails	Active
	EAM_IDM_Integration		Active
	EAMTOGFC	From EAM to GFC	Active
	EAMtoMingle		Inactive
	FoldertoEAM		Inactive

Open each of the data flow that reference the EAM IMS connection point and duplicate the data flow by clicking Duplicate button shown in below screen shot, and give a name that can be easy to identify as a duplicate. For example, if the original data flow name is *EAM_IDM_Integration*, give the name ***New**_EAM_IDM_Integration* to the duplicated data flow. Configure the duplicated data flow by following the below steps. All the duplicated data flows that are referencing EAM IMS connection point should be switched to EAM “IMS via API Gateway” connection point,

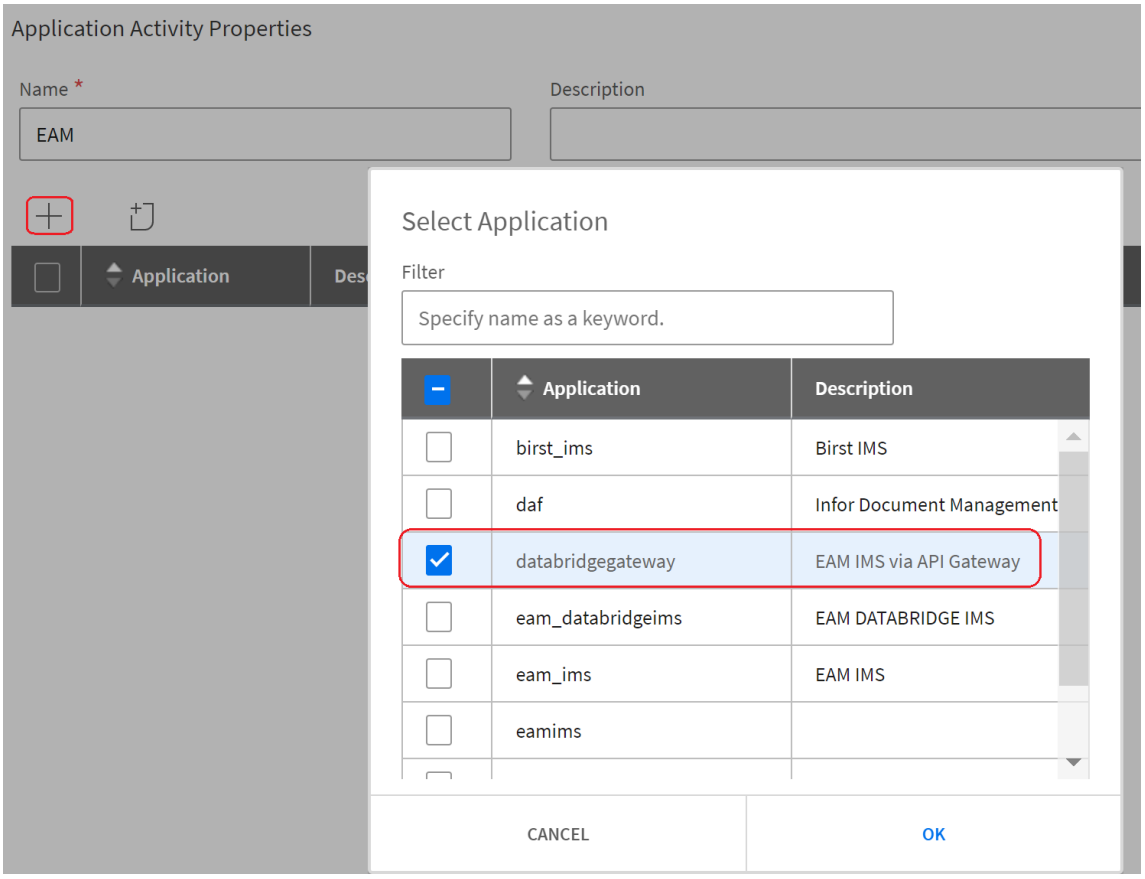
For example, in the above Usage screenshot there are 5 flows with references for the EAM IMS connection point, so all of these 5 flows have to be duplicated and the EAM IMS connection point has to be switched to the new “IMS via API Gateway” connection point.



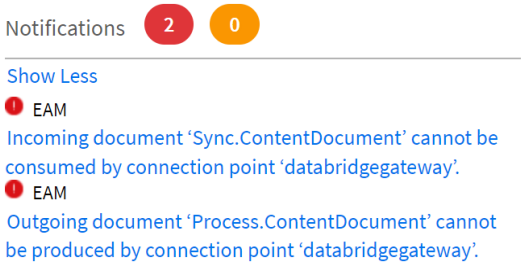
Open the duplicated flow and identify where the EAM IMS connection point is in the data flow. Select the EAM IMS connection point in the lower pane of the screen and click 'Remove'.



Then click 'Add' or '+', and select the new IMS Via API Gateway connection point in the lower pane of the screen. Save the duplicated data flow.



Note: Since the Document tab of the new IMS Via API Gateway connection point is not configured during preparation, you will get warning messages like below when saving duplicated data flows, which is ok for the preparation stage, and these warning messages will be gone at transition when the Document tab refreshes and loads from the EAM Configuration. You have the option to manually add the referenced documents to the Documents tab to avoid the warning messages.



Note: The duplicated data flow may contain other connection points also as part of the flow, change the EAM IMS connection point only to the new IMS Via API Gateway connection point, and do not alter other connection points in the duplicated data flows.

Do not activate the duplicated data flows at this time when doing preparation for transition. At the transition time, the original data flows will be deactivated and then these duplicated data flows will be activated (See Transition section for details).

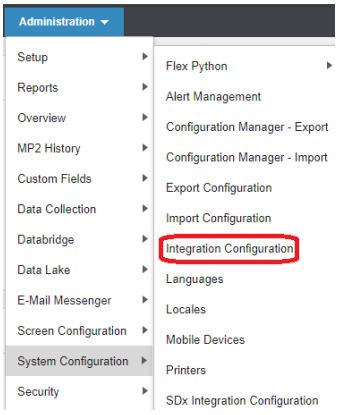
Appendix E: Tenant Specific EAM Security

EAM Outbound oauth2 Security Configuration Associated with IMS via API Gateway Connection Point

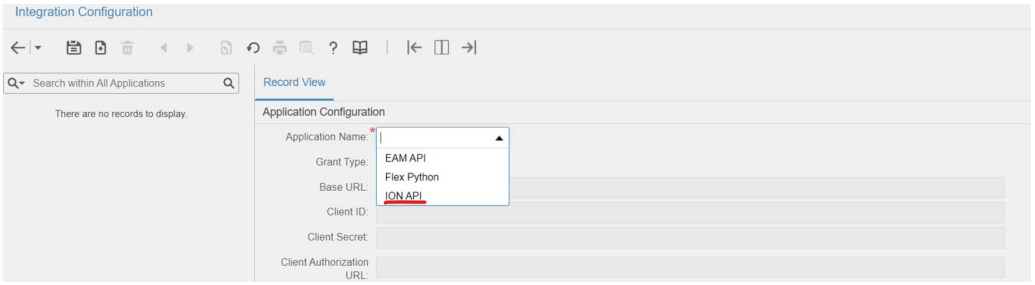
⚠ CAUTION: If you have already finished this step while configuring Infor API Gateway for Hexagon EAM integration with Infor Datalake, please skip this step as both integrations share the same Infor API Gateway configuration.

Since we are using the API Gateway for EAM outbound communication, it uses Tenant specific oauth2.0 for authentication of the request from EAM, so we need to provide the oauth2 credentials to EAM that will be used for the generation of the oauth access token to communicate with the API gateway.

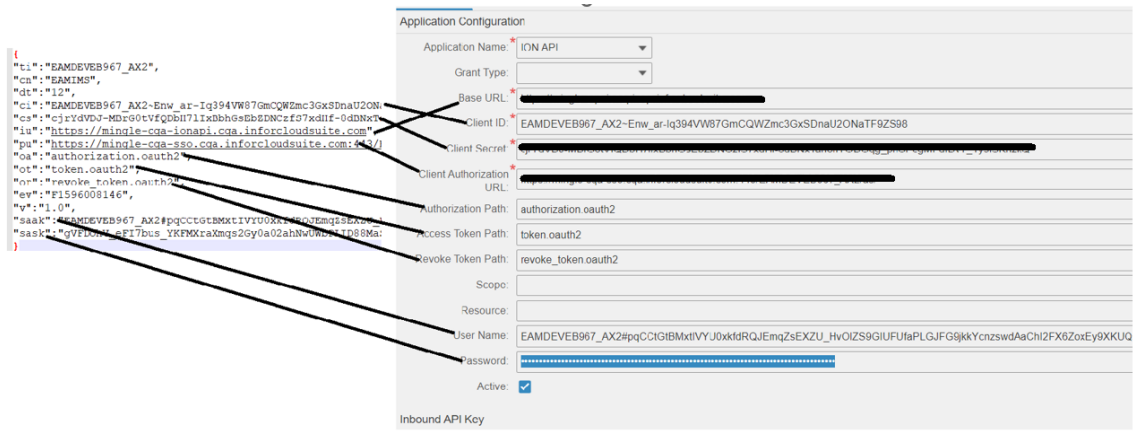
The Contents from the EAMIMS.ionapi file downloaded in the Appendix C: Service Account and Client Id, should be provided to EAM using the Integration Configuration screen in EAM, Administration -> System Configuration -> Integration Configuration screen as shown below.



In the Application Configuration, select “ION API” for application type as we are using an ION API based integration,



Provide the contents from the EAMIMS.ionapi file in the EAM screen as shown in the below field mapping, the fields that are not mapped are optional fields and they can be ignored.

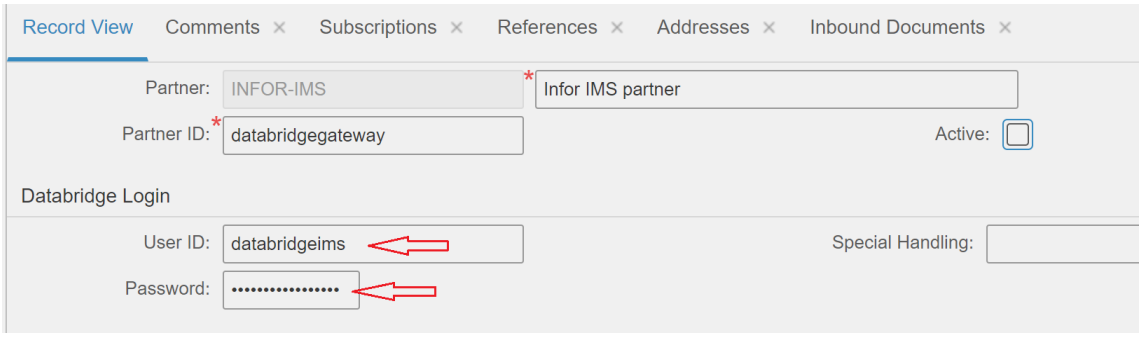


Field on Application Configuration screen	Field in EAMIMS.ionapi file	Other Values
Application Name		“ION API”
Grand Type		Null
Base URL	“iu”	
Client ID	“ci”	
Client Secret	“cs”	
Client Authorization URL	“pu”	
Authorization Path	“oa”	
Access Token Path	“ot”	
Revoke Token Path	“or”	
Scope		Null
Resource		Null
User Name	“saak”	
Password	“sask”	
Active		Checked

EAM outbound security configurations are now completed.

EAM Inbound oauth1 Security Configuration Associated with IMS via API Gateway Connection Point

Go to the EAM Databridge Partners screen, locate the INFOR-IMS partner and go to the record view tab, in the Databridge login section, input the IMS access key in the User ID field and input the IMS secret key in the Password field and then save the partner record. These values will be populated into the R5MGPROVISIONINGCONFIG table in the EAM database which are used for validation with incoming IMS requests to EAM.



The IMS access key and secret key you defined here are used when you configure the ION API gateway in Appendix A: API Gateway Configuration.

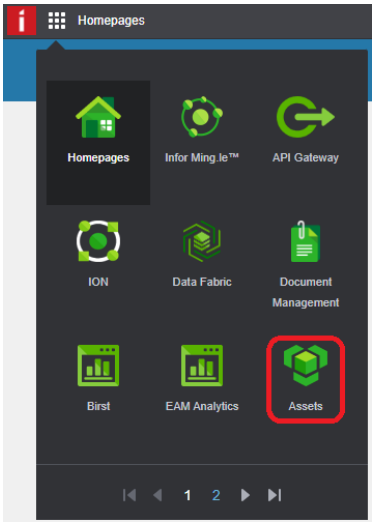
Note: Adding the IMS access key and secret key in the Databridge login section (for IMS via API Gateway connection point) for the INFOR-IMS partner will not disrupt the EAM/ION integration with the direct IMS connection point that is still running.

Appendix F: EAM Configurations

Databridge Configuration

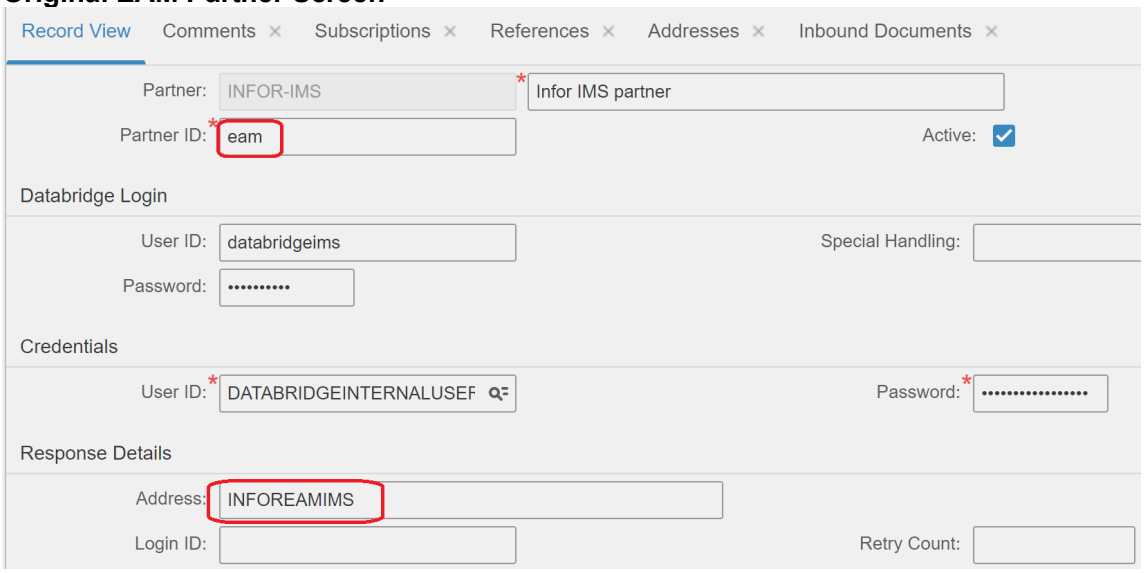
On the Infor OS screen, select Assets, In the EAM Menu, Select Administration -> Databridge -> Databridge Partners

We must use Infor-IMS partner for this integration, and since the user is already using the Infor-IMS partner, the user needs to change certain values on the partner screen as mentioned below;

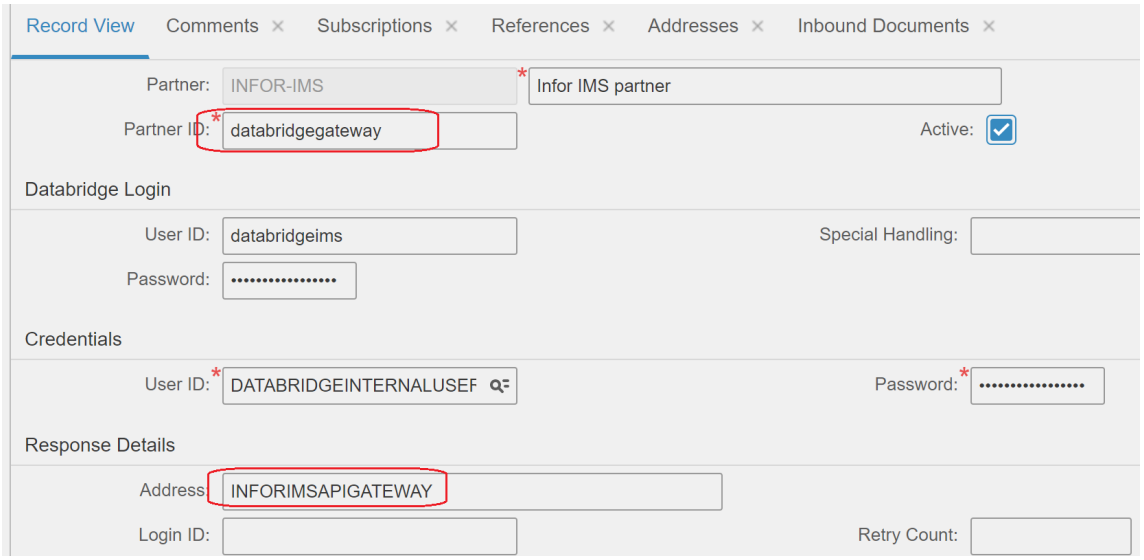


- **Partner-ID**:databridgegateway,
  - Keep track of the original value for partner id which is “eam” or “eam:databridgeims” before updating it to the new value, if the user wants or needs to roll back to the original IMS setup using Appendix G: Rollback to IMS Connection point then the value should be “eam” or “eam:databridgeims”.
- **Address**: “*INFORIMSAPIGATEWAY*”, this needs to be set to make the IMS partner be used for the “IMS via API Gateway” based integration
  - Keep track of the original value for Address which is “*INFOREAMIMS*” before updating it to the new value. In case the transition is not successful, and the user wants to roll back to the original IMS setup, you will need to set it back using Appendix G: Rollback to IMS Connection point then the value should be “*INFOREAMIMS*”.
- **User ID and Password** (in the Databridge Login section): These are EAM IMS access/secret keys configured during preparation time in Appendix E: Tenant specific EAM security. Leave these values as they are.

Original EAM Partner Screen



New Updated Partner screen



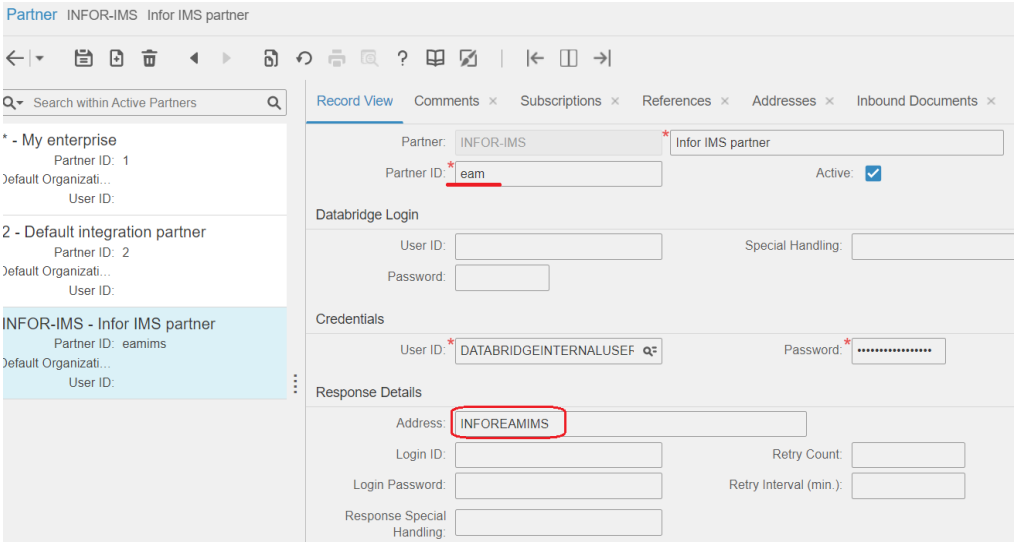
Appendix G: Rollback to IMS Connection Point

If there are issues encountered during or after transition and you cannot resolve them in time, you can roll back to the original IMS configuration with the below steps.

1. In ION Desk | Connect | Data Flows, deactivate the duplicated data flows that were activated in Step 5 during the transition if your transition has progressed that far.

2. On the EAM Databridge Partners screen, locate the INFOR-IMS partner and go to the Record View, change the Partner ID back to what it was before the transition, and change the Address under the Response Details section to INFOREAMIMS and then save the record.

   Partner ID: *eam or eam:databridgeims*
   Address: *INFOREAMIMS*



3. In ION Desk | Connect | Data Flows, identify and activate the original dataflows that were used/active before the transition, and were deactivated during the transition. You should have taken notes for these data flows during the transition.

4. Go to the EAM Administration | Security | Install Parameters screen, locate and set the install parameter ***@IOBCONV*** to “N”.

5. Check and verify that both inbound and outbound BOD traffics are working with the original IMS configuration.

You may need to contact Infor ION support for ION or API Gateway related issues you encounter if these issues cannot be resolved on your own.