



Document Version 3.2

(October 6, 2021)

Anaplan Informatica Connector

Document Version 3.2

Version Control

Version Number	Date	Changes
2.1	Mar 2017	New Template applied
2.2	Aug 2017	INTEGRA-1180 - New functionality and behaviors
2.3	Sep 2017	Added 3.1 Extract Import Action Dump File and Send to Target Connector section and added formatting.
2.3.1	Nov 2017	Added 3.2 File Isolation in Anaplan.
2.3.2	Jan 2018	Minor correction on page 20
2.4	Jan 2018	Updates to section 2.2.1. for version 2.4 of the connector.
2.5	May 2018	June 2018 Release Anaplan Connector
2.6	Oct 2018	Oct 2018 Release Anaplan Connector
2.7	Jan 2019	Updated Proxy Configuration instructions.
2.8	Dec2019	Included Proxy Configuration instructions for JVM options.
2.9	Feb 2020	Revised certificate language.
3.0	May 2020	Removed reference to Anaplan-issued certificates.
3.1	Oct 2020	October 2020 Release Anaplan Connector
3.2	Aug 2021	Workspace and Model name support added.
3.2	Oct 2021	Updates to domain and IP allow listings and bug fixes.

Anaplan Informatica Connector	0
1 Introduction	1
1.1 What's New	1
1.2 About the Anaplan Connector	1
1.3 About Version 2.0	1
1.4 Informatica Prerequisites	2
1.5 Anaplan Prerequisites	3
2 Anaplan Connector	4
2.1 Anaplan Connector Properties	5
2.2 Counts for Rows	7
2.2.1 Informatica Count behavior	7
2.3 Limitations and Testing Settings	8
2.4 Column Separator and Text Delimiter	9
2.5 Configure of an Anaplan Connection with Basic Authentication	10
2.6 Configure an Anaplan connection with authentication using a Certificate Authority (CA) certificate	12
2.6.1 Extract Private key and Public Certificate from the CA Certificate	13
2.6.2 Create a Java Keystore using your public certificate and private key	14
2.6.3 To configure an Anaplan connection with authentication using a CA Certificate	15
2.7 Proxy Access using JVM Options	17
2.7.1 Authenticated Proxy	17
2.7.2 Unauthenticated Proxy.....	18
2.7.3 Proxy Access using proxy.ini	19
2.7.4 Authenticated Proxy	20
2.7.5 Unauthenticated Proxy.....	20
2.8 Specify dump file location	22
3 Import synchronization task and Configuration	24
Step 1: Definition	24
Step 2: Source	24
Step 3: Target.....	25

Step 4: Data Filters.....	26
Step 5: Field Mapping	26
Step 6: Advanced Scheduling Options	27
3.1 Extract Import Action Dump File and Send to Target Connector.....	29
3.2 File Isolation in Anaplan.....	32
3.3 OPTION to USE API BASED FIELD MAPPING	33

1 Introduction

This guide explains how administrators and end users can configure and use the Anaplan Connector for Informatica Intelligent Cloud Services to:

- export data from Anaplan
- import data into Anaplan
- delete data from Anaplan
- run a process that contains any combination of model-to-model Import and Delete actions

1.1 What's New

- [Updates to domain and IP allow listings](#)
- Bug fix – Error with exports that contain commas within cells
- Bug fix – Error with export data with double quotation (") marks
- Bug fix – Error with exports with special characters or long character strings
- Bug fix – pagination of workspace models for API version 1.3

1.2 About the Anaplan Connector

The advantages of using the Anaplan Connector for Informatica Cloud include:

- **Automation:** no need to run actions manually from the Anaplan UI
- **Ease of configuration:** no need to write a batch file (Windows) or shell script (UNIX/Linux/macOS) for [Anaplan Connect](#)
- **Flexibility:** the mapping you create can take advantage of all the functionality that Informatica provides
- **Connectivity:** access hundreds of source connectors available to Informatica Cloud
- **Native Scheduling:** schedule integration jobs using Informatica Cloud

1.3 Informatica Prerequisites

Before you start, make sure you have:

1. An Informatica Cloud Secure Agent that is installed, registered, and running. See https://network.informatica.com/onlinehelp/IICS/prod/CDI/en/index.htm#page/bb-cloud-getting-started/Installing_Secure_Agents.html.
2. Knowledge of how to use Informatica Cloud, including:
 - (For synchronization task) how to use the synchronization task wizard
 - (For mapping) how to create a Connection using the Flat File Connector
3. On the same machine where the Informatica Secure Agent is installed:
 - Verify knowledge of your Informatica Connection properties, such as the Runtime Environment and the absolute path to a directory you can use as your output directory for Export.
 - Set the following in your operating system environment variables:
`JAVA_TOOLS_OPTIONS=-Dfile.encoding=UTF8`
This ensures greater usability for customers using non-English characters.

Create the following directory or file:

Import	A directory to hold the files you import
Export	The directory to hold the files you export (output directory)
Delete	A csv file with at least one column and one row of data
Process	A csv file with at least one column and one row of data

1.5 Anaplan Prerequisites

Make sure you have:

1. An Anaplan account with access to a model and workspace.
2. Knowledge of how to use and configure Anaplan actions.
3. Your Anaplan model must already have a corresponding action that you can run manually from the Anaplan graphical user interface:
 - For **Export**, an Export action that exports data from a model

✦ **Note:** Only exports that have a **Tabular Single Column** or **Tabular Multiple Column** layout are supported.

- For **Import**, an Import action that imports data into a model
- For **Delete**, another action that deletes data from a model
- For **Process**, a Process action that contains multiple actions

4. Certificates for authentication

Anaplan connector supports authentication with CA (Certificate Authority) certificates. Select API version 2.0 to use CA certificates.

If you're using a CA certificate, make sure you:

- Have the CA Certificate file in a JAVA keystore file. The keystore file must be present on the same machine as your Informatica Cloud Secure Agent.
- Know following information about the JAVA Keystore file:
 - Path to the keystore file
 - Alias of the Certificate saved in the keystore file
 - Password for the Certificate alias in the keystore file

5. Firewall and proxy access

Add api.anaplan.com and auth.anaplan.com to your company's allow (safe) URL list. Update domain and IP allow listings per this Anaplan Community [set of instructions](#).

- Add any firewall and any proxies your organization uses.
- Ensure that port 443 is open for two-way HTTPS connections between Anaplan Connect and Anaplan.

2 Anaplan Connector

Anaplan Operation	Connection Type		Informatica Operation Type must be:
	Source Connection	Target Connection	
Export	AnaplanV2	Flat File	INSERT
Import	Flat File	AnaplanV2	INSERT
Process	Flat File	AnaplanV2	INSERT
Delete	Flat File	AnaplanV2	INSERT

Each mapping requires two connections: one for the source, and one for the target. In this document, the two types are **Flat File** and **AnaplanV2**. The Flat File is used as an example, but any data source available in Informatica Cloud can be used.

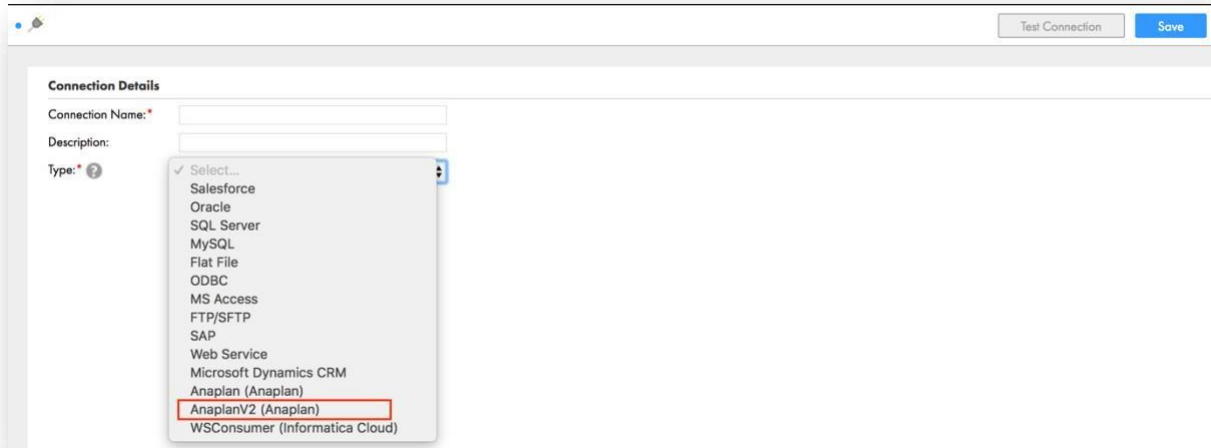


Fig. 1 : *New Connection Type*

2.1 Anaplan Connector Properties

Connection Details

Connection Name: *

Description:

Type: * ?

AnaplanV2 Connection Properties ?

Runtime Environment: * ?

Auth Type: *

Username:

Password:

Certificate Path Location:

Workspace ID: *

Model ID: *

API Base URL: *

Auth URL: *

API Major Version: *

API Minor Version:

Max Task Retry Count: *

Error Dump Path Location:

Use API Based Metadata: * ☐

KeyStore Path Location:

KeyStore Alias:

Keystore Password:

Fig. 2 : *Anaplan Connector Properties*

Connection Property	Description
Connection Name *	A name that distinguishes this connection from other connections.
Description	Indicate the purpose or explain who will use this connection.
Type *	Select Anaplan from the list.
Runtime Environment *	Select your Informatica Secure Agent.
Auth Type *	Select either Basic Auth or Cert Auth from the list.

Username	An Anaplan user name, such as <i>firstname.lastname@anaplan.com</i>
Connection Property	Description
Password	You must enter a password if you've selected Basic Auth on the Auth Type list.
Certificate Path Location	<p>You must enter the certificate path if:</p> <ul style="list-style-type: none"> You've selected Cert Auth on the "Auth Type" list, AND Set "API Major Version" = 1, and "API Minor Version" = 3 <p>Leave this field blank if any of the above conditions is false.</p>
Workspace name or ID*	Enter name or ID of your Anaplan workspace. You can get the ID of the workspace by clicking on Help -> About on Anaplan UI.
Model name or ID*	Enter name or ID of your Anaplan model. You can get the ID of the model by clicking on Help -> About on Anaplan UI.
API Base URL*	Enter the following URL: https://api.anaplan.com .
Auth URL *	Enter the following URL for authentication with v2 APIs: https://auth.anaplan.com
API Major Version*	<p>Anaplan supports 2 API versions:</p> <ul style="list-style-type: none"> v1.3 (Major version=1, Minor version=3) Newer v2.0 version (Major version=2, Minor version=0) <p>By default, the API major version is set to 1.</p> <ul style="list-style-type: none"> Select 1 if you want to use v1.x API Select 2 if you want to use v2.x API (for using CA Certificates)
API Minor Version	<p>By default, the API minor version is set to 3.</p> <ul style="list-style-type: none"> Select 3 if you want to use x.3 API (e.g. v1.3) Select 0 if you want to use x.0 API (e.g. v2.0).

Max Task Retry Count*	By default, the Max Task Retry count is set to 2. Note that if you select a greater value, this will slow down the integration.
Error Dump Path Location	Path to save Dump files generated from Anaplan Import actions. See section "SPECIFY DUMP FILE LOCATION" for more details.
Connection Property	Description
Use API Based Metadata	Select this to use API based metadata for Import actions. See section "OPTION TO USE API BASED FIELD MAPPING" for more details.
KeyStore Path Location KeyStore Alias Keystore Password	Use these fields if you select Auth Type = Cert Auth, and set API Major Verion = 2. These fields specify: <ul style="list-style-type: none"> Path to JAVA keystore file on machine with secure agent Alias of the Certificate saved in the KeyStore file Password for the Certificate alias in the KeyStore file

* Mandatory fields

2.2 Counts for Rows

2.2.1 Informatica Count behavior

Anaplan Operation	Connector Version 2	Connector Version 1
Export	Export (Lists): Informatica Success rows = count of rows exported Informatica Error rows = 0 Export (Modules): Informatica Success rows = count of rows exported Informatica Error rows = 0	Export (Success Scenario) - Success Rows: 1, Failure Rows: 0 Export (Failure Scenario) - Success Rows: 0, Failure Rows: Actual count of rows Failed
Anaplan Operation	Connector Version 2	Connector Version 1

Import*	<p>(Modules)</p> <p>Informatica Success rows = Number of Anaplan cells successfully updated/inserted + Number of Anaplan cells updated/inserted with warning</p> <p>Informatica Error rows = Number of failed Anaplan cells</p> <p>(List)</p> <p>Informatica Success rows = Number of rows successfully updated/inserted + Number of rows updated/inserted with warning</p> <p>Informatica Error rows = Number of failed rows</p> <p>(Cells with Anaplan Ignored status are not included in the count above.)</p>	<p>Import (Success Scenario) - Success Rows: Actual count of rows imported, Failure Rows: 0</p> <p>Import (Failure Scenario) - Success Rows: Actual count of rows imported, Failure Rows: Actual count of rows Failed</p>
Delete	<p>Delete (Success Scenario) - Success Rows: 1, Failure Rows: 0</p> <p>Delete (Failure Scenario) - Success Rows: 0, Failure Rows: 0</p>	<p>Delete (Success Scenario) - Success Rows: 0, Failure Rows: 0</p> <p>Delete (Failure Scenario) - Success Rows: 0, Failure Rows: 0</p>
Process	<p>Process (Success Scenario) - Success Rows: Actual count of actions executed successfully, Failure Rows: 0</p> <p>Process (Warning Scenario) – Success rows: Actual count of action executed successfully, Failure Rows: Actual count of failed actions</p>	<p>Process (Success Scenario) - Success Rows: 0, Failure Rows: 0</p> <p>Process (Failure Scenario) - Success Rows: 0, Failure Rows: 0</p>

2.3 Limitations and Testing Settings

- Model-to-model import is supported in a Process, not an Import.
- A Process is limited to any combination of model-to-model Import actions and/or Delete actions.
- Characters in the Anaplan column and field names must be alphanumeric because Informatica doesn't support names that contain spaces or special characters (`, ~, !, @, #, \$, %, ^, & *, (,), +, =, <, >, [,], {, })
- Import and Export actions must use any of the following as a column separator:

- a comma (,)
- Semi-colon (;)
- Tab, or
- Pipe (|)
- Import and Export actions must use a double quote (") as a Text Delimiter.
- Exports must include a header row. If you filter header rows in Anaplan, the export will fail in Informatica and must be canceled manually.

Imports and Exports of 1000 MB have been tested with the following settings:

- Informatica Secure Agent: 6 GB of RAM
- DTM JVM: -Xmx1024m

Note: Review the Informatica documentation for more information about increasing the field buffer size and increasing Secure Agent memory.

2.4 Column Separator and Text Delimiter

The Connector uses the **Column Separator** and **Text Delimiter** values that were set in the model through the **File Import Data Source Definition**.

The screenshot displays the 'File Import Data Source Definition' dialog box. At the top, the 'Actions' bar contains buttons for 'View', 'New Action', 'Run...', 'Edit...', 'Delete...', 'Reorder...', and 'Manage Import Data Sources...'. Below this, the 'Select Source' section offers options to 'Upload New File...' or 'Connect to Anaplan Model...', and a list of existing sources with 'Income Statement.txt' selected and an 'Edit...' button. The 'File Options' section is divided into two columns. The left column includes 'Text Encoding' (ISO-8859-1), 'Column Separator' (Tab), and 'Other:'. The right column includes 'Text Delimiter' (None), 'Decimal Separator' (Dot), 'Header Row' (1), and 'First Data Row' (2). Red boxes highlight the 'Manage Import Data Sources...' button, the 'Edit...' button, the 'Column Separator' section, and the 'Text Delimiter' dropdown.

Fig. 3 : *File Import Data Source Definition - Column Separator and Text Delimiter*

2.5 Configure of an Anaplan Connection with Basic Authentication

To configure an Anaplan connection with basic authentication:

1. Log in to your Informatica Cloud.
2. Go to **Data Integrations > Home > Connections**.
3. In the **Connections** section, click **New Connection**.
4. In the Connection Details section:
 - a. Enter a **Connection Name**.
 - b. On the **Type** list, click **AnaplanV2**.

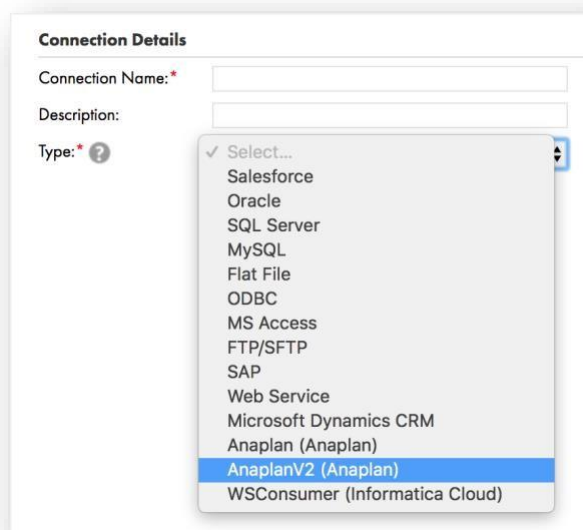
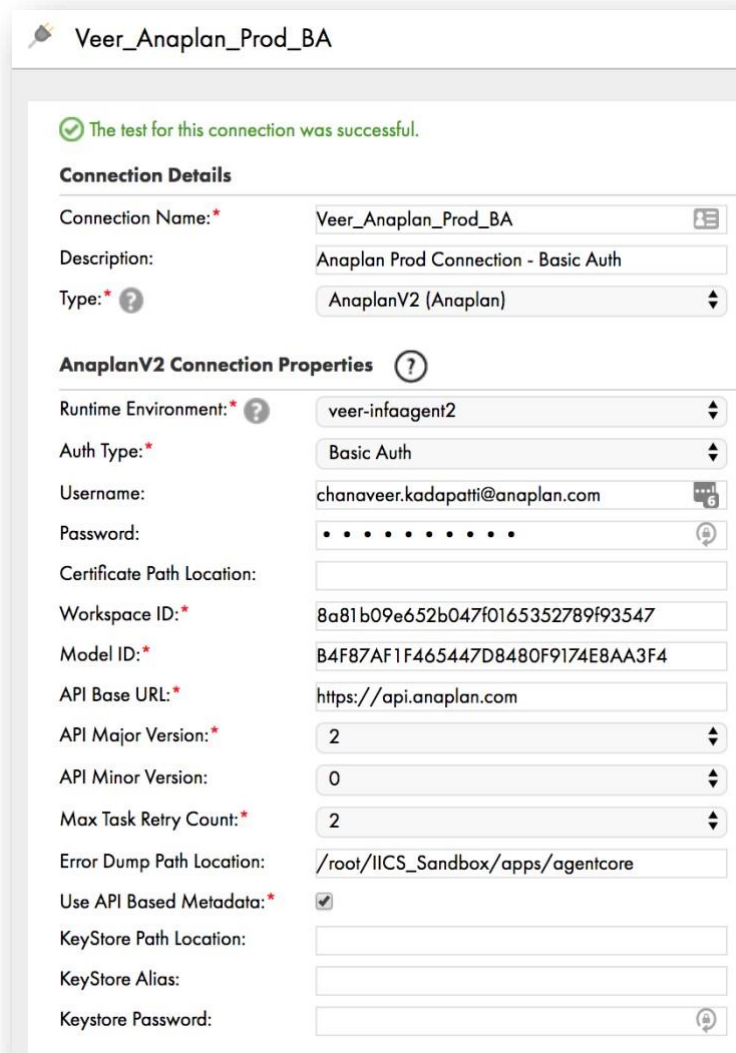


Fig. 4 : **Configuration - Connection Type List**

5. In the AnaplanV2 Connection Properties section:
 - c. Select a Runtime Environment.
 - d. On the **Auth Type** list, click **Basic Auth**.
 - e. Enter a Username and Password.
 - f. From the URL of an Anaplan model, copy and paste the **Workspace name or ID** and **Model name or ID**.
 - g. Set the **API Base URL** to <https://api.anaplan.com>.

Note: By default, the **API Major Version** and **API Minor Version** are set to 1 & 3 respectively.

Note: The **Max Task Retry Count** is set to 2 by default. If you select a greater value, this will slow down the integration.



Connection Details

Connection Name: * Veer_Anaplan_Prod_BA

Description: Anaplan Prod Connection - Basic Auth

Type: * ? AnaplanV2 (Anaplan)

AnaplanV2 Connection Properties ?

Runtime Environment: * ? veer-infaagent2

Auth Type: * Basic Auth

Username: chanaveer.kadapatti@anaplan.com

Password:

Certificate Path Location:

Workspace ID: * 8a81b09e652b047f0165352789f93547

Model ID: * B4F87AF1F465447D8480F9174E8AA3F4

API Base URL: * https://api.anaplan.com

API Major Version: * 2

API Minor Version: 0

Max Task Retry Count: * 2

Error Dump Path Location: /root/IICS_Sandbox/apps/agentcore

Use API Based Metadata: * ☒

KeyStore Path Location:

KeyStore Alias:

Keystore Password:

Fig. 5 : *Connection Properties*

6. Click **Test Connection** to verify that the connection is successful and then click **OK**.

2.6 Configure an Anaplan connection with authentication using a Certificate Authority (CA) certificate

If you choose to authenticate using CA Certificate, note that:

1. Customers must purchase CA Certificates on their own. Your internal IT teams should be able to guide you in obtaining these Certificates.
2. The type of Certificates & list of supported root CA Certificates is given here:

[https://help.anaplan.com/anapedia/Content/Administration and Security/Tenant Administration/Security/Certificates.htm](https://help.anaplan.com/anapedia/Content/Administration%20and%20Security/Tenant%20Administration/Security/Certificates.htm)

3. Once you've obtained CA Certificate, it is under your control and Anaplan Inc. is not responsible for keeping it secure. Under no circumstance should you share your Private Key with anyone.
4. Informatica Cloud assumes that the location of any files (including certificates) that are referenced are located on a directory that the Cloud Secure Agent can access.

Note: *Your Tenant Admin must register your Public Certificate on Anaplan Tenant Admin page before you can use it with Integrations. Refer to [Manage your Certificates](#) in Anapedia.*

Follow these steps to use CA Certificates for authentication with Anaplan Connector:

1. Review this video for an example of how to create a JAVA Keystore:
<https://community.anaplan.com/t5/Videos/Certificate-Authentication-Process/bap/36468>
2. Obtain CA Certificate with assistance from your IT team.

When you obtain Certificate from your CA (Certificate Authority), the Certificate may be issued as 2 files: A Public Certificate (Public Cert) and the Private Key. Alternately, the Public Cert and Private Key may be issued in a single file by your CA. Contact your CA or internal IT team for details and process to obtain Certificate.
3. Extract Private key and Public Certificate from the CA Certificate. These are 2 separate files. Keep the Private key secure.
4. Create a JAVA keystore using your Private key and Public Certificate 5. Use the JAVA keystore in your Anaplan Connection

2.6.1 Extract Private key and Public Certificate from the CA Certificate

Note: *You need openssl and keytool command-line tools for below steps. Download appropriate openssl version for your operating system. Keytool is included with your JAVA distribution.*

If you obtain both the Public Cert and Private Key in a single file, use openssl commands to extract and save both files separately in PEM format.

Example

Note: *The exact command depends on the type and format of your certificate. Refer to the file type and openssl documentation for more details. This example assumes you have been issued a single PKCS12 formatted file containing both Public Cert and Private Key.*

Extracting Public Cert: `openssl pkcs12 -in Client_certificate.p12 -nokeys -out`

`CERTIFICATE.pem` Extracting Private Key:

`openssl pkcs12 -in Client_certificate.p12 -nocerts -out PRIVATE_KEY.pem -nodes`

Edit your Public Cert in a text editor and delete all text before “-----BEGIN CERTIFICATE-----” part. Ensure your Public Cert file begins with “-----BEGIN CERTIFICATE-----” and ends with “-----END CERTIFICATE-----”. Your Public Cert will look like this:

```
Chanaveers-MacBook-Pro:Test chanaveerkadapatti$ more publiccert.pem
-----BEGIN CERTIFICATE-----
MIIFi jCCBHKgAwIBAgIQBIInOKZCSMQCK0xf08aepETANBgkqhkiG9w0BAQsFADBl
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGl naUNL cnQgSW5jMRkwFwYDVQLExB3
d3
SU
Bh
Y2
YW
cG
87
46
vJ
kx
cY
Ax
dD
BA
MA
Qw
d3
Y3
MD
dX
cD
cy
SI
+L
3u
ZWQg
A1UE
Y2lz
ciBL
.YW5h
.QRCp
9jaL
6b3N
0wz0
SqI0
Xf4V
C9k/
AQH/
Y29t
AwQw
Oi8v
Oi8v
Y3Js
QXNz
aHR0
ZXJ0
CSqG
bBl+
RbiD
AJXG
183mqktk5fA26gMdX+zXwHB rnB8W+ko+uEp/WovWDL+l jFNDAmOiK5xpg6tcWXRX
yJWvew4GbiBa2rck5sfrUmT67tga8GfIM3XRAIsiSYMRcGt9nLsmMHbs/VKeS0uc
EJ1++yXPWjZ0yB1SkQazud33EHrXtP00MYAKKCLu
-----END CERTIFICATE-----
Chanaveers-MacBook-Pro:Test chanaveerkadapatti$
```

2.6.2 Create a Java Keystore using your public certificate and private key

1. First, run this command to create a pkcs12 bundle from your Public Certificate & Private Key. Both should be in PEM format.

```
$ openssl pkcs12 -export -in <CERTIFICATE.pem> -inkey <PRIVATE_KEY.pem> -out  
keystore_bundle.p12 -name <KEYSTORE_ALIAS> -CAfile <CERTIFICATE.pem> -caname  
root
```

Note:

- a. CERTIFICATE.pem is your Public certificate
 - b. PRIVATE_KEY.pem is your Private key
 - c. Keystore_bundle.p12 is the generated pkcs12 formatted file
 - d. KEYSTORE_ALIAS is the alias of your Public certificate in the pkcs12 bundle
 - e. You will be prompted for password when creating the pkcs12 bundle. USE THE SAME PASSWORD FOR THE NEXT STEP BELOW.
2. Next, create the JAVA keystore with above pkcs12 file. JAVA keystore are created & managed by JAVA keytool utility.

```
$ keytool -importkeystore -deststorepass <KEYSTORE-PASSWORD> -destkeystore  
my_keystore.jks -srckeystore keystore_bundle.p12 -srcstoretype PKCS12
```

Note:

- a. my_keystore.jks is the generated JAVA Keystore file
- b. keystore_bundle.p12 is the pkcs12 bundle used to create JAVA Keystore. This is the pkcs12 bundle created in previous step.
- c. KEYSTORE-PASSWORD is the password for your pkcs12 bundle in the JAVA Keystore. USE THE SAME PASSWORD AS YOU DID TO CREATE THE PKCS12 BUNDLE IN PREVIOUS STEP.

2.6.3 To configure an Anaplan connection with authentication using a CA Certificate

1. Log in to your Informatica Cloud.
2. Go to **Data Integration > Home > Connections**.
3. In the **Connections** section, click **New Connection**.
4. In the Connection Details section:
 - a. Enter a Connection Name.
 - b. On the **Type** list, click **AnaplanV2**.

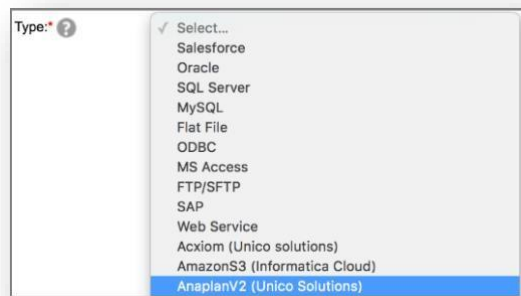
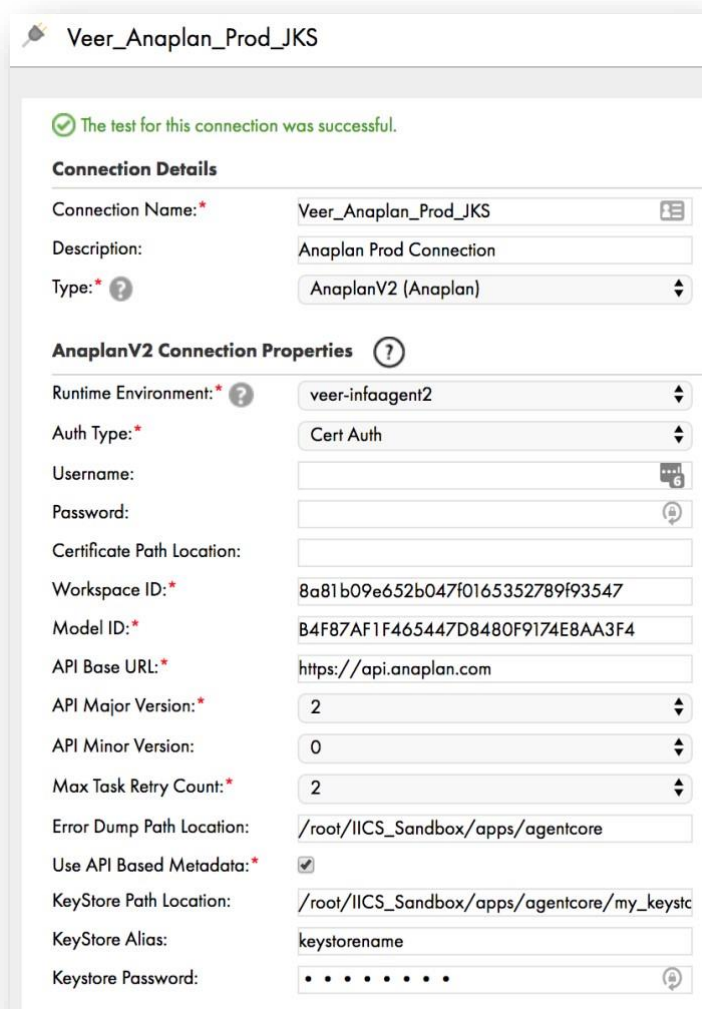


Fig. 6 : **CA Certificate Based Authentication – Connection Type List**

5. In the AnaplanV2 Connection Properties section:
 - a. Select a Runtime Environment.
 - b. On the **Auth Type** list, click **Cert Auth**.
 - c. From the URL of an Anaplan model, copy and paste the **Workspace name or ID** and **Model name or ID**.
 - d. Set the **API Base URL** to <https://api.anaplan.com>.
 - e. Set API Major Version = 2 and API Minor Version = 0
 - f. In the **Keystore Path Location** box, enter the path to the JAVA keystore (e.g. “/root/IICS/apps/agentcore/my_keystore.jks”)
 - g. Enter the keystore alias in the **KeyStore Alias** field, and keystore password in the **Keystore Password** field.



Note: The **Max Task Retry Count** is set to 2. If you select a greater value, this will slow down the integration.



✓ The test for this connection was successful.

Connection Details

Connection Name: * Veer_Anaplan_Prod_JKS

Description: Anaplan Prod Connection

Type: * ? AnaplanV2 (Anaplan)

AnaplanV2 Connection Properties ?

Runtime Environment: * ? veer-infaagent2

Auth Type: * Cert Auth

Username:

Password:

Certificate Path Location:

Workspace ID: * 8a81b09e652b047f0165352789f93547

Model ID: * B4F87AF1F465447D8480F9174E8AA3F4

API Base URL: * https://api.anaplan.com

API Major Version: * 2

API Minor Version: 0

Max Task Retry Count: * 2

Error Dump Path Location: /root/IICS_Sandbox/apps/agentcore

Use API Based Metadata: * ☒

KeyStore Path Location: /root/IICS_Sandbox/apps/agentcore/my_keystc

KeyStore Alias: keystorename

Keystore Password:

Fig. 7 : *JAVA keystore Location*

6. Click **Test** to verify that the connection is successful and then click **OK**.

2.7 Proxy Access using JVM Options

You can use Informatica's Administrator service to configure proxy access on the secure agent which the Anaplan Connector uses to send and receive data.

Follow these steps for configuring proxy access, depending on if you use authenticated proxy or unauthenticated proxy. If you are unsure, contact your integration support staff.

Informatica's Administrator service uses Java Virtual Machine (JVM) options to configure proxy access.

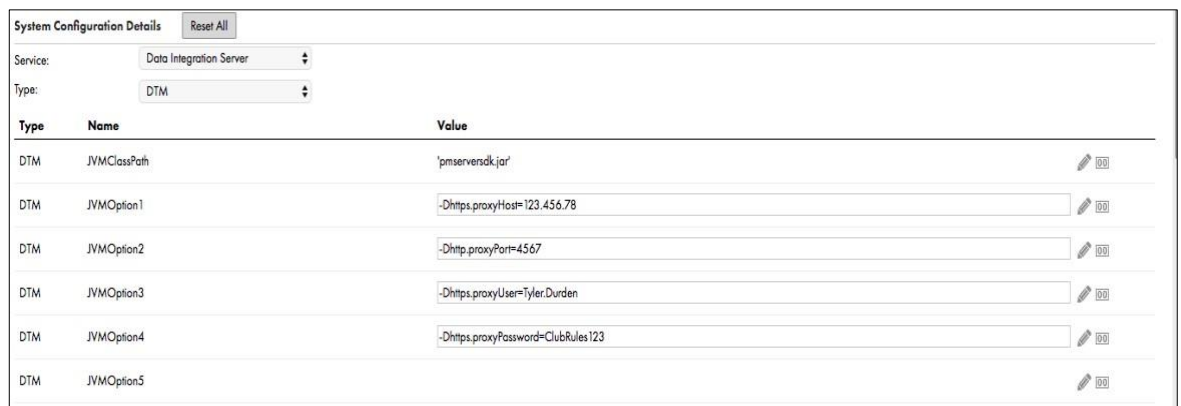
When you configure your proxy using JVM options, changes take place a few minutes after you save your configuration. You do not need to restart your Informatica agent. If you

have a **proxy.ini** file configured on your system, the JVM options override any settings in your **proxy.ini** file.

You can test your proxy setup by either running a task or viewing your proxy logs.

2.7.1 Authenticated Proxy

1. In Informatica's **Administrator** interface, navigate to **Runtime Environments**.
2. Select your environment name, then click **Edit**.
3. Under **System Configuration Details**, select *DTM* from the **Type** drop-down menu.
4. Define the JVM options.



Type	Name	Value
DTM	JVMClassPath	'pmserverjdk.jar'
DTM	JVMOption1	-Dhttps.proxyHost=123.456.78
DTM	JVMOption2	-Dhttp.proxyPort=4567
DTM	JVMOption3	-Dhttps.proxyUser=Tyler.Durden
DTM	JVMOption4	-Dhttps.proxyPassword=ClubRules123
DTM	JVMOption5	

JVM Option	Description	Value
JVMOption1	The proxy host.	-Dhttps.proxyHost= <i>IP address of your proxy host</i>
JVMOption2	The proxy port.	-Dhttps.proxyPort= <i>the port number used by your proxy host</i>
JVMOption3	<p>The proxy user name.</p> <p>This setting is only used for an authenticated proxy. Leave blank for an unauthenticated proxy.</p>	-Dhttps.proxyUser= <i>User name</i>

JVMOption4	<p>The password associated with the user name.</p> <p>This setting is only used for an authenticated proxy. Leave blank for an unauthenticated proxy.</p>	- Dhttps.proxyPassword= <i>Password</i>
JVMOption5	Not used	Leave blank

- Click **Save**.

2.7.2 Unauthenticated Proxy

- In Informatica's **Administrator** interface, navigate to **Runtime Environments**.
- Select your environment name, then click **Edit**.
- Under **System Configuration Details**, select *DTM* from the **Type** drop-down menu.
- Define the JVM options.

System Configuration Details
Reset All

Service: Data Integration Server
Type: DTM

Type	Name	Value
DTM	JVMClassPath	'pmserversdk.jar'
DTM	JVMOption1	-Dhttps.proxyHost=123.456.78
DTM	JVMOption2	-Dhttp.proxyPort=4567
DTM	JVMOption3	
DTM	JVMOption4	
DTM	JVMOption5	

JVM Option	Description	Value
JVMOption1	The proxy host.	-Dhttps.proxyHost= <i>IP address of your proxy host</i>
JVMOption2	The proxy port.	-Dhttps.proxyPort= <i>the port number used by your proxy host</i>

JVMOption3	Not used	Leave blank
JVMOption4	Not used	Leave blank
JVMOption5	Not used	Leave blank

5. Click **Save**.

2.7.3 Proxy Access using proxy.ini

You can manually configure the **proxy.ini** file with the proxy details on the secure agent which the Anaplan Connector will use to send and receive data.

Note: *Anaplan v2 connector utilizes Informatica Cloud's native proxy capabilities via configuration in conf/proxy.ini file. Anaplan v2 connector currently does not include custom proxy logic of its own. Refer to Informatica help pages for proxies supported by Informatica Cloud & steps on configuration using conf/proxy.ini.*

Follow these steps for using a **proxy.ini** file to configure proxy access, depending on if you use authenticated proxy or unauthenticated proxy. If you are unsure, contact your integration support staff.

The **proxy.ini** file contains these parameters:

- InfaAgent.ProxyPassword=
- InfaAgent.ProxyNtDomain=
- InfaAgent.ProxyHost=
- InfaAgent.ProxyPasswordEncrypted=true
- InfaAgent.NonProxyHost=localhost|127.*|[\:\:1]
- InfaAgent.ProxyUser=
- InfaAgent.ProxyPort=
- InfaAgent.AuthenticationOrder=

2.7.4 Authenticated Proxy

1. Stop the Informatica Secure Agent.
2. Go to Informatica *Secure Agent* folder.
3. Open file **proxy.ini** in the **conf/** sub-folder.

4. Edit the proxy.ini file and define the following parameters:

Parameter	Description
InfaAgent.ProxyHost=	The proxy host name
InfaAgent.ProxyPort=	The proxy port number
InfaAgent.ProxyUser=	The proxy user ID
InfaAgent.ProxyPassword=	The proxy password
InfaAgent.ProxyPasswordEncrypted=	Change to false.

- You should obtain this information from your Network Administrator or IT Department, or use a command line detector tool.
5. Save the file.
 6. Start and stop the Informatica Secure Agent Service.
 7. From your Windows Start menu, select **Control Panel -> Administrative Tools -> Services**. Locate the *Informatica Secure Agent* service, right-click and select **Restart**:

2.7.5 Unauthenticated Proxy

1. Stop the Informatica Secure Agent.
2. Go to Informatica *Secure Agent* folder.
3. Open file **proxy.ini** in the **conf/** sub-folder.
4. Edit the proxy.ini file and define the following parameters:

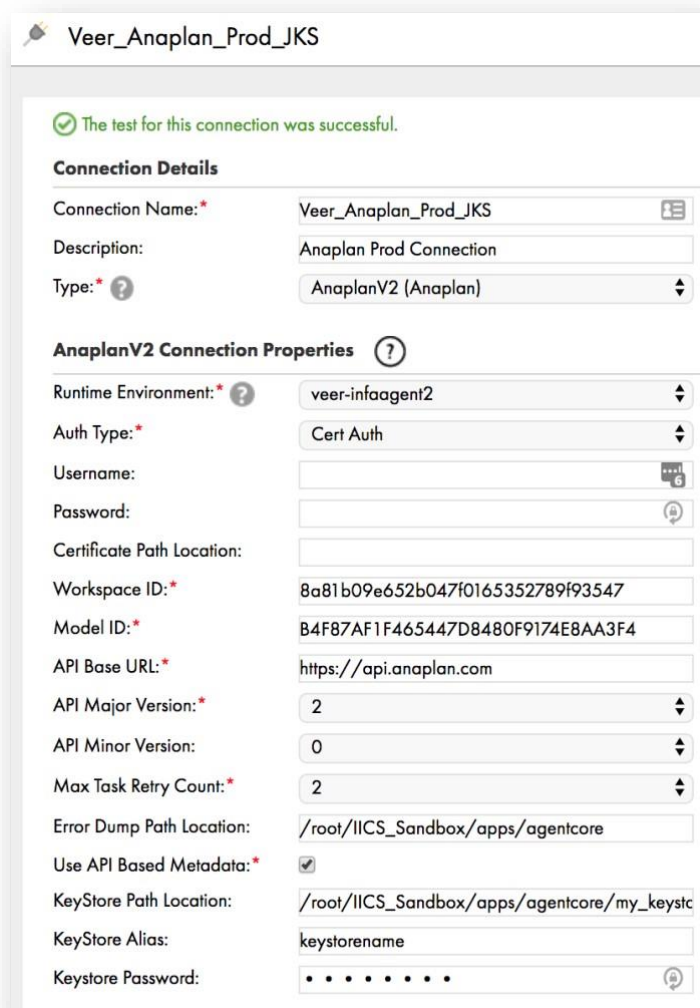
Parameter	Description
InfaAgent.ProxyHost=	The proxy host name
InfaAgent.ProxyPort=	The proxy port number

- You should obtain this information from your Network Administrator or IT Department, or use a command line detector tool.
5. Save the file.
 6. Start and stop the Informatica Secure Agent Service.
 7. From your Windows Start menu, select **Control Panel -> Administrative Tools -> Services**. Locate the *Informatica Secure Agent* service, right-click and select **Restart**:

2.8 Specify dump file location

You can specify where on the agent server you want Connector to automatically save the error dump file, if a process or import action generates a dump file on Anaplan. Note that a process action generates a dump file only if it contains an import action.

Enter the absolute path for the dump file folder in **Error Dump Path Location** field of Anaplan Connection configuration.



Veer_Anaplan_Prod_JKS

✓ The test for this connection was successful.

Connection Details

Connection Name: * Veer_Anaplan_Prod_JKS

Description: Anaplan Prod Connection

Type: * ? AnaplanV2 (Anaplan)

AnaplanV2 Connection Properties ?

Runtime Environment: * ? veer-infaagent2

Auth Type: * Cert Auth

Username:

Password:

Certificate Path Location:

Workspace ID: * 8a81b09e652b047f0165352789f93547

Model ID: * B4F87AF1F465447D8480F9174E8AA3F4

API Base URL: * https://api.anaplan.com

API Major Version: * 2

API Minor Version: 0

Max Task Retry Count: * 2

Error Dump Path Location: /root/IICS_Sandbox/apps/agentcore

Use API Based Metadata: * ☒

KeyStore Path Location: /root/IICS_Sandbox/apps/agentcore/my_keystc

KeyStore Alias: keystorename

Keystore Password:

Fig. 8 : **Anaplan Connection configuration – Connection Details**

- INFO** Anaplan v2 connector also provides an option to send Dump file to a target connector. Refer to section **EXTRACT IMPORT ACTION DUMP FILE AND SEND TO TARGET CONNECTOR**.

The connector creates a sub-folder in the **Error Dump Path Location** for each process action that results in a dump file. The naming convention for the folders is:

Dump_files_<process name>

Dump files for Process dumps use this naming convention:

<import Action name>.<file extension – either txt or csv>

Dump files for Import dumps use this naming convention:

Error_Dump_IMPORT_<import ID>_<task ID>_<timestamp>.<file extension – either txt or csv>

For example:

Error_Dump_IMPORT_112000000003_5540AC30461F4C2CA94845BD7D928444_1600191958023.csv

As some processes can be quite large, ensure you have sufficient space for dump files.

3 Import synchronization task and Configuration

You can use a synchronization task to automate the import of a Flat File into Anaplan using the **synchronization task Wizard**.

Make sure there is a .csv file in the Flat File connection. This is the .csv file that will be imported into Anaplan.

For more information, see [Informatica Prerequisites](#) and [Anaplan Prerequisites](#).

Step 1: Definition

1. Log in to Informatica Cloud and go to **Data Integration > New > Tasks > Synchronization Task**.
2. Click **Create**.
3. In the **Task Name** box, enter a name.
4. On the **Task Operation** list, click **Insert**.
5. Click **Next**.

New Synchronization Task1

1 Definition 2 Source 3 Target 4 Data Filters 5 Field Mapping 6 Schedule

Task Details

Task Name: * New Sync Task ?

Location * Anaplan\V2-Prod Browse ?

Description: New Sync Task ?

Task Operation: * Insert ?

? Save < Back Next > Finish Cancel

Fig. 9 : *Synchronization Task Wizard – Import Task Definition*

Step 2: Source

1. On the **Connection** list, select an existing Flat File connection.
2. Optionally, click **View** next to the **Connection** list to see more information on the Flat File connection properties.

3. Next to the **Source Object** list, click **Select**.
4. Select the .csv file you want to import and click **Select**.
- Warning:** If the column names in the .csv file contain spaces, then the Import action might fail because they can't be mapped. To solve this, remap the server file in Anaplan and run the import again.
5. Optionally, click **Preview All Columns** to see a preview of the .csv file.
- Warning:** Loading large imports can take some time.
6. Click **Next**.

New New Sync Task

1 Definition 2 **Source** 3 Target 4 Data Filters 5 Field Mapping 6 Schedule

Source Details

Connection: * Nayana_FlatFile_Imports_Connection View... New... Sample... ?

Source Type: * ☒ Single ☐ Multiple ☐ Saved Query

Source Object: * List With Errors.csv Select... Formatting Options... ?

☐ Display source fields in alphabetical order

Data Preview

List With Errors.csv Preview All Columns (Total columns: 14)

List_With_Errors	Parent	Code	Number1	Text2	...
Valid			90	jhijhjhjh	...
InValid1			abc	sdsdsd	...
InValid2			90	sdsdsd	...
InValid3			90	sdsdsd	...
InValid4			90	jhijhjhjh	...
InValid5			90	jhijhjhjh	...
Valid			90	jhijhjhjh	...

Save < Back **Next >** Finish Cancel

Fig. 10 : Synchronization Task Wizard – Import Task Connection Source

Step 3: Target

1. On the **Connection** list, select an existing Anaplan connection.
2. Optionally, click **View** next to the **Connection** list to see more information on the **AnaplanV2 Connection Properties**.
3. Next to the **Target Object** list, click **Select**.
4. Select the Anaplan Import action and click **Select**.
5. Optionally, click **Show Data Preview** to see the columns that will be imported. Click **Preview All Columns** to see more information.
- Warning:** Loading large imports can take some time. We advise you not to use the **Show Data Preview** option if the file size is over 5MB.

- Info:** If the first column header in your Anaplan server file is blank, it's automatically populated with the “_DUMMY” placeholder.
- 6. Click **Next**.

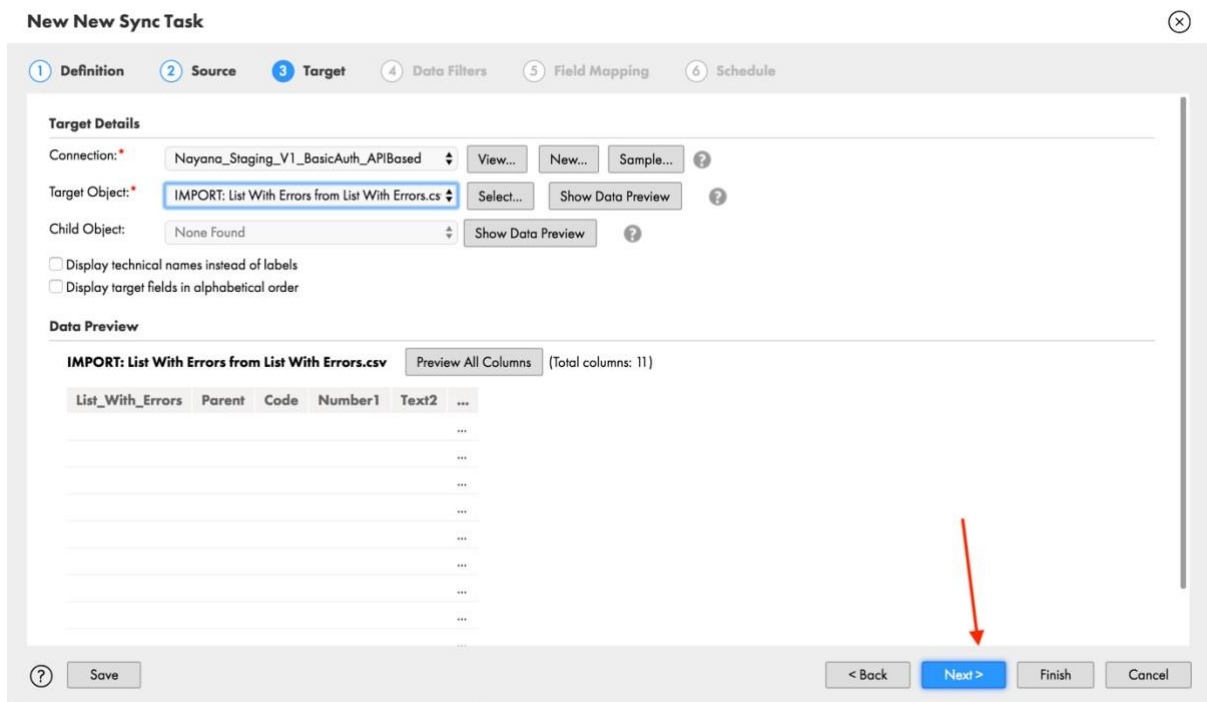


Fig. 11 : *Synchronization Task Wizard – Import Task Target Details*

Step 4: Data Filters

1. Optionally, click **New** to create data filters and follow the instructions. For more information, refer to the Informatica documentation.

Note: *It's not possible to apply a Row Limit to a synchronization task with a Flat File connector.*

2. Click **Next**.

Step 5: Field Mapping

1. Drag-and-drop the fields of your local Flat File connection (shown on the left) to the relevant fields in Anaplan (on the right). Some fields may already be auto-matched.

Note: *Map the first field in your Flat File to the first field in Anaplan. If you don't map one or more Anaplan fields, they won't appear in Informatica when you update the import file.*

Info: If you're importing a file that contains Header1, Header2, and Header3, and you only map the two first headers. When you update the import file, Header3 won't be listed as an available field.

- Optionally, click **Validate Mapping** to make sure the mapping is correct before running the task.
- Click **Save > Save and Run**. The **Monitor > Running Jobs** page opens with details of the tasks that are in progress. The task you've created will disappear from the list once complete.
- Go to **Monitor > All Jobs**. The status of the task is displayed in the **State** column. Click on a particular task in the **Instance Name** column for task details. For more information, see [Informatica Count behavior](#).
- If the import fails, click the **Instance Name** of the job, click **Download Session Log**, then download the `log.txt` file to find out what went wrong.

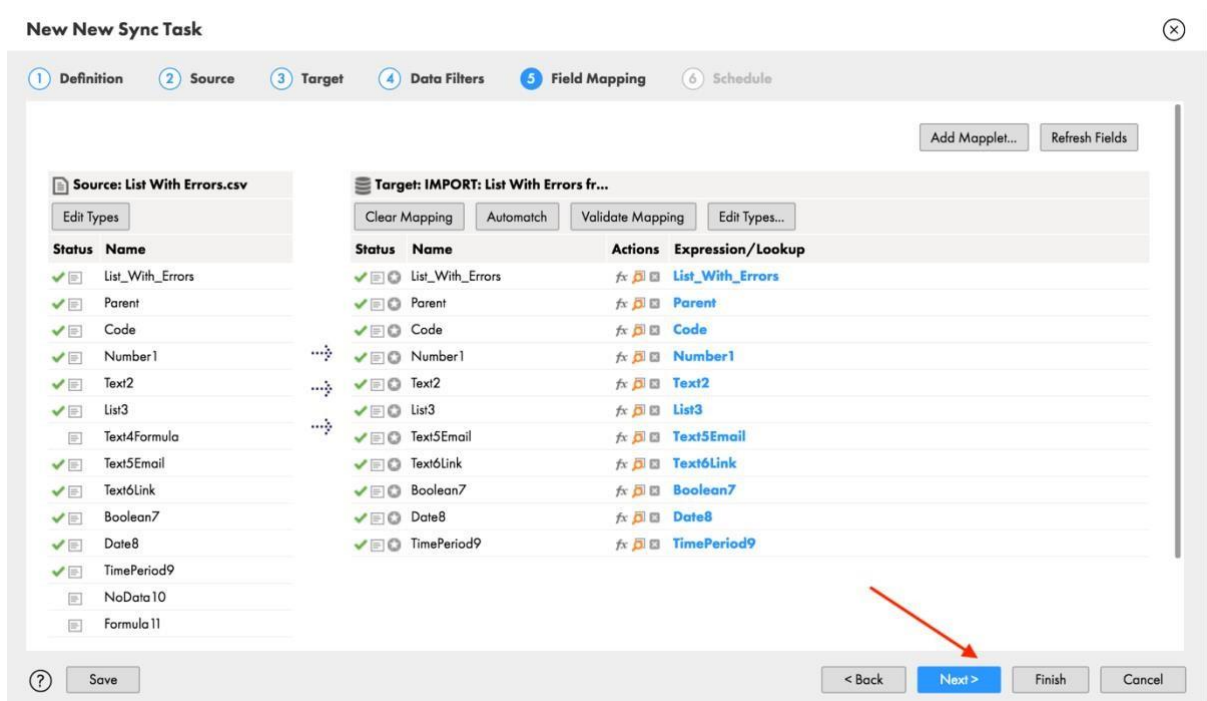


Fig. 12 : Synchronization Task Wizard – Import Task Field Mapping

Step 6: Advanced Scheduling Options

CONFIGURE CHUNK SIZE

You can specify the **Chunk Size** for Imports or Exports on the **Schedule** tab in **Advanced Target Properties**.

- Enter a whole number from 1 to 50MB. The default is 1.

Edit New Sync Task ✕

1 Definition 2 Source 3 Target 4 Data Filters 5 Field Mapping 6 Schedule

Advanced Options

Preprocessing Commands: ?

Post-processing Commands: ?

Parameter File Name: ?

Maximum Number of Log Files: 10 ?

Advanced Target Properties

Chunk Size:

Upload Only Import: ☐

Success File Directory:

Error File Directory:

Execution Mode

Mode: ☒ Standard ? ☐ Verbose ?

?

Fig. 13 : *Chunk Size setting*

CONFIGURE SYNCHRONIZATION TASK TO UPLOAD FILE WITHOUT INVOKING ACTION

You can configure a synchronization task to upload a file only and not invoke an Action.

1. To do this, on the **Schedule** tab, in **Advanced Target Properties**, enable **Upload Only Import**.

The screenshot shows the 'Edit New Sync Task' dialog box with the 'Schedule' tab selected. The 'Advanced Options' section includes fields for 'Preprocessing Commands', 'Post-processing Commands', 'Parameter File Name', and 'Maximum Number of Log Files' (set to 10). The 'Advanced Target Properties' section includes 'Chunk Size' (set to 1), 'Upload Only Import' (checked), 'Success File Directory', and 'Error File Directory'. The 'Execution Mode' section has 'Mode' set to 'Standard'. At the bottom, there are 'Save', '< Back', 'Next >', 'Finish', and 'Cancel' buttons.

Fig. 14 : *Upload without Invoking Action*

3.1 Extract Import Action Dump File and Send to Target Connector

You can configure the Anaplan connector to extract the dump file created during an import action and send it to a target connector. This enables you to export the dump file to a flat file, database table or other connector with a field mapping.

1. Create a normal Import Action synchronization task. See **Import synchronization task and Configuration**.

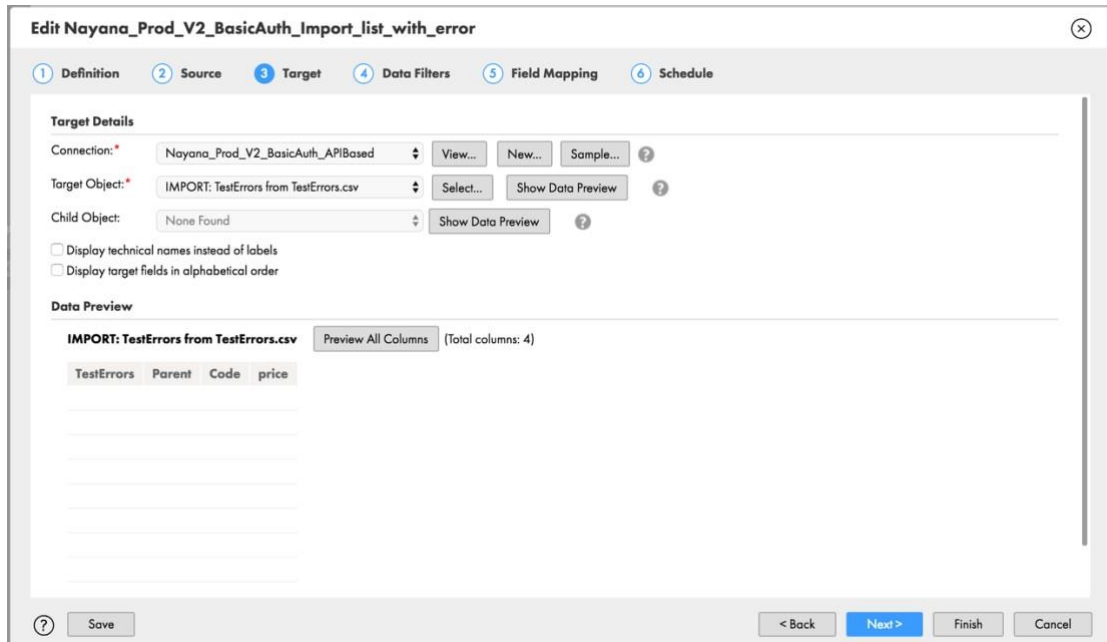


Fig. 15 : Options to select on the 'normal Import Action synchronization task'

2. Create a second synchronization task to extract the dump file from the first synchronization task and send to a target connector. See **Import synchronization task and Configuration**.



Note: When creating the second synchronization task, select an import action from Source Object with the text "ERRORDUMP".

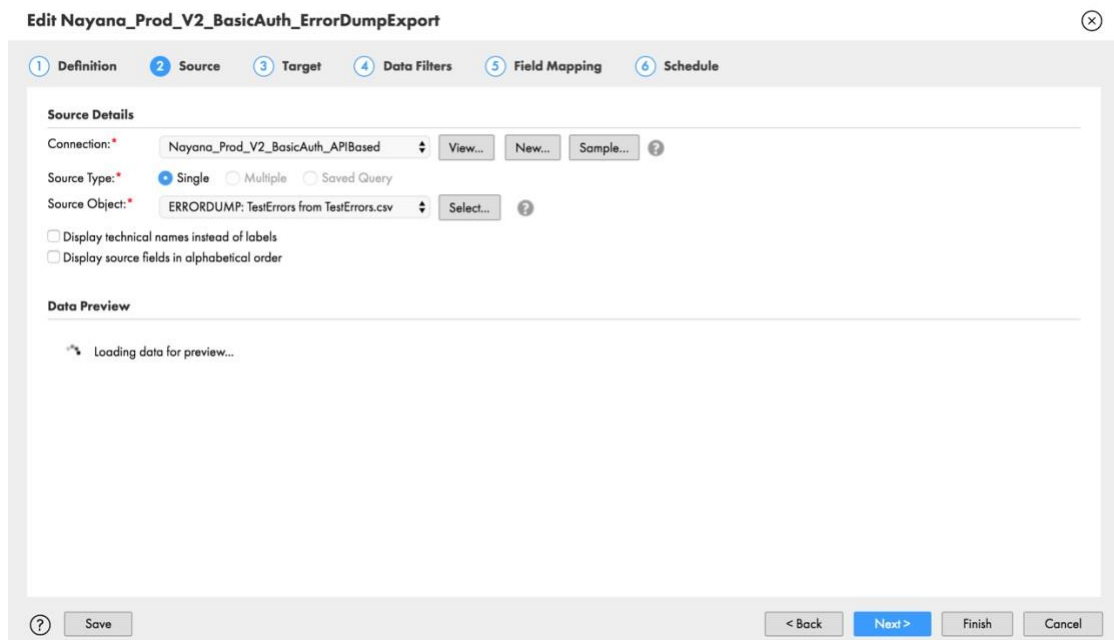


Fig. 16 : Source Object options on 'second synchronization task'.

3. On the second synchronization task, configure a target connection and mapping to receive the dump file. There are additional '_Error_N_' fields available for mapping. These fields correspond to the error description columns in Anaplan dump file.

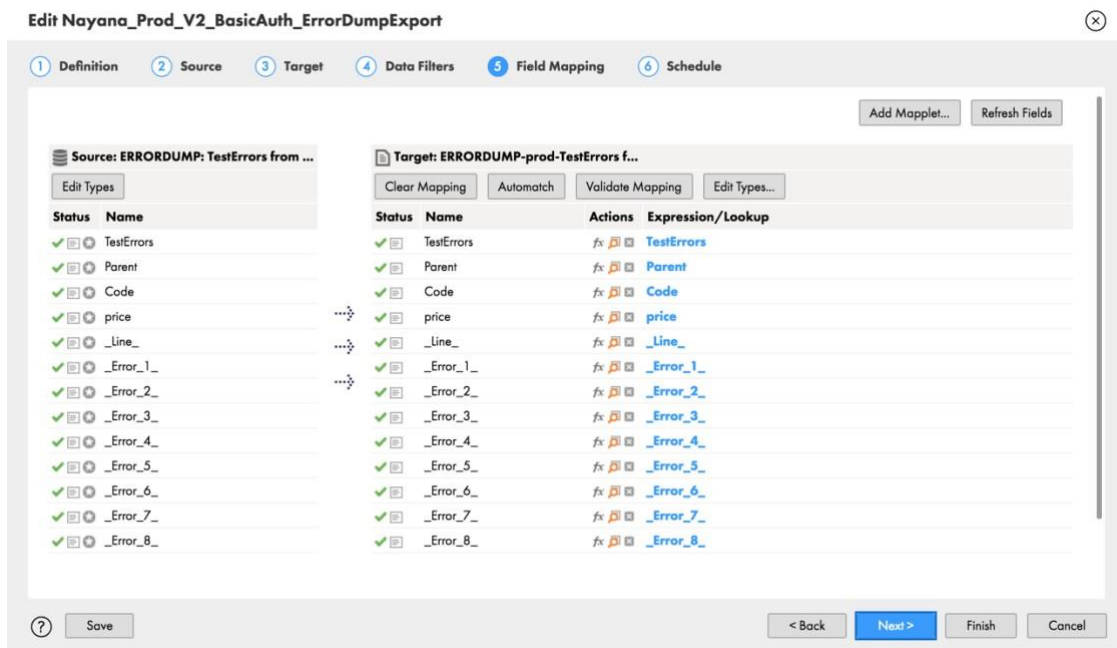


Fig. 17 : 'Second synchronization task' Field mappings.

- Info:** While importing a Module with Line Items in a column or Importing a List, at a maximum, all input columns could have incorrect input data. In this scenario, Anaplan creates one error description column in the Dump file for each error column. Hence, the number of '_Error_X_' columns available for mapping is twice the number of data columns in the Import file.

Create a Taskflow with the two synchronization tasks that you created earlier.

- Run the 'Import Action synchronization task'.
- Run the second synchronization task to push the first dump file to a target connector.

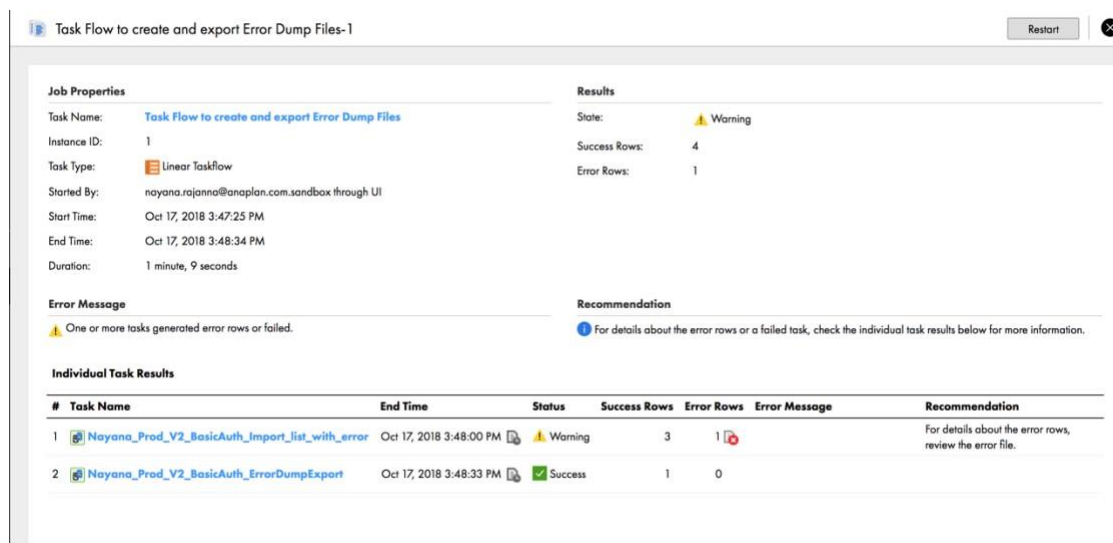


Fig. 18 : Taskflow with the two synchronization tasks.

3.2 File Isolation in Anaplan

Anaplan now provides a mechanism for Workspace Administrators to set the privacy level of files associated with Import and Export Actions. This is referred to as file isolation. In summary:

- Data files set as *private files* can be accessed only by the user who originally uploaded or exported the data.
- Data files can be set as *default files* for Administrators, to be accessible only by Workspace Administrators. Alternately, they can be set as Default for all users (Everyone), including standard end users.

The ability for users to maintain unique private files has an effect on data integrations with Anaplan, including the Anaplan Connector for Informatica Cloud. When working with the Anaplan Connector, you must ensure that:

- The Import Action file exists in the model and can be accessed by the user ID that will be used to run the integration with the Action. If this user ID is different from the user ID that created the Action, the data file *must* be set as a default file.
- The Export Action file exists in the model. If it doesn't exist, you can't view the Informatica DSS Data Preview for an export.

For more details on file isolation, see the “Overview of Private and Default Files” article in Anapedia and the release notes in [Platform Releases](#).

3.3 OPTION to USE API BASED FIELD MAPPING

The Anaplan connector now provides an option to use API based field mapping in place of Anaplan file-based mapping. Previously, the Anaplan connector referred to Anaplan files (Import data source) for fetching column header information. This method could potentially break Informatica Import action synchronization tasks in scenarios where the Anaplan file has been deleted or overwritten. With the new option, users can elect to use API based mapping where Anaplan connector makes an API call to determine headers and remove dependency on files.

- To elect to use API based field mapping, select your Anaplan connection and edit it. Note the option: **Use API Based Metadata**.

Veer_Anaplan_Prod_JKS

The test for this connection was successful.

Connection Details

Connection Name: * Veer_Anaplan_Prod_JKS
Description: Anaplan Prod Connection
Type: ? AnaplanV2 (Anaplan)

AnaplanV2 Connection Properties ?

Runtime Environment: ? veer-infaagent2
Auth Type: * Cert Auth
Username:
Password:
Certificate Path Location:
Workspace ID: * 8a81b09e652b047f0165352789f93547
Model ID: * B4F87AF1F465447D8480F9174E8AA3F4
API Base URL: * https://api.anaplan.com
API Major Version: * 2
API Minor Version: 0
Max Task Retry Count: * 2
Error Dump Path Location: /root/IICS_Sandbox/apps/agentcore
Use API Based Metadata: * ☒
KeyStore Path Location: /root/IICS_Sandbox/apps/agentcore/my_keystc
KeyStore Alias: keystorename
Keystore Password:

Note: The **Use API Based Metadata** option is unchecked by default to enable you to run existing Integrations as-is and use File based mapping. To switch to API based mapping, check the checkbox and save the connection. ALL SYNCHRONIZATION TASKS USING THIS CONNECTION WILL START USING API BASED MAPPING.

Note: The Anaplan recommendation is to use API based mapping for all new Anaplan Connections, making import action synchronization tasks more robust. Anaplan's long-term strategy is to move all Import mapping functionality to use API based mapping. File-based mapping is planned to be disabled in mid-2019 (Anaplan will provide advanced notification when this change takes place). As a best practice, your organization should use API based mapping as soon as possible.

Info:

- When you view an existing Anaplan connection the new option does not display, except in **Edit** mode. Save the edited connection to view option in **View** mode.
- The API based mapping does not return read-only columns from Anaplan, such as Parent level aggregate members of a hierarchy, columns with formulas, and similar columns. As a result, read-only Anaplan columns are not available for mapping.
- API based mapping may NOT work if your Import action has custom Date formats

Import:

Mapping Time HUB18 Demo - Employees Versions

How to map the source data into the timescale

☐ Dates Source file contains dates
☒ Periods Source file contains periods
☐ Periods in specific year Source file contains period without year
☐ Match names Match names from the source file against

Patterns with Separators

Y-M
 M-Y

Separator can be any non-alphabetic character
 Y represents year number (1, 2, 3)
 M represents month number (1, 2, 3)

Fixed-position Patterns

YYYYMM
 YYMM
 MMYYYY
 MMY

Fixed-position patterns look for the following patterns

Custom fixed-position pattern

DD MMM YYYY

Custom patterns are like the fixed-position patterns, but they are not ignored

As of May 2018, Informatica Cloud (ICS) does not natively handle columns headers starting with numbers. With API based mapping, Anaplan connector has implemented following workaround for handling numeric headers or headers starting with numbers:

- If you are trying to Export data from Anaplan where column headers start with a number, the connector attaches a unique tag “_NUMHDR_” to the beginning of such headers. These tags remain in the exported data (see image below) due to technical Informatica limitations in removing the tags.

1	"Versions"	"Line_Items"	"_NUMHDR_1_Jan_18"	"_NUMHDR_2_Jan_18"	"_NUMHDR_3_Jan_18"
2	"Actual"	"number1"	"123456"	"123456"	"123456"
3	"Actual"	"text2"	"changed2"	"changed2"	"changed2"
4	"Forecast"	"number1"	"123456"	"123456"	"123456"
5	"Forecast"	"text2"	"changed2"	"changed2"	"changed2"
6					

- If you are trying to Import data into Anaplan where source column headers start with a number, the connector attaches and displays tag “_NUMHDR_” in the DST Field Mapping section. Go ahead with the mapping, save, and run the DST. The tags are automatically removed when writing data to Anaplan, so that Anaplan Import Data Source file has the original headers.

Synchronization task Field Mapping tab

Source: ModuleWithTimeHeadersP2.csv

Status	Name
✓	Line_Items
✓	__Jan_18
✓	__Jan_18_1
✓	__Jan_18_2
✓	__Jan_18_3
✓	__Jan_18_4

Target: IMPORT: Module With Time H...

Status	Name	Actions	Expression/Lookup
✓	Line_Items	fx	Line_Items
✓	_NUMHDR_1_Jan_18	fx	__Jan_18
✓	_NUMHDR_2_Jan_18	fx	__Jan_18_1
✓	_NUMHDR_3_Jan_18	fx	__Jan_18_2
✓	_NUMHDR_4_Jan_18	fx	__Jan_18_3
✓	_NUMHDR_5_Jan_18	fx	__Jan_18_4
	_NUMHDR_6_Jan_18	fx	
	_NUMHDR_7_Jan_18	fx	
	_NUMHDR_8_Jan_18	fx	
	_NUMHDR_9_Jan_18	fx	

Anaplan Import Data Source file after DST is run

1	Line Items,1 Jan 18,2 Jan 18,3 Jan 18,4 Jan 18,5 Jan 18
2	number1,8787,8787,8787,8787,8787
3	text2,sample,sample,sample,sample,sample
4	

- The Anaplan recommendation is to avoid using numeric column headers or column headers starting with numbers to avoid confusion with the “_NUMHDR_” tags.